Cisco Emergency Responder 8.6 アドミニストレーション ガイド

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Emergency Responder 8.6 アドミニストレーション ガイド

CONTENTS

はじめに

この項では、このマニュアルの対象読者および構成について説明します。

また、次のトピックについて取り上げます。

概要

『*Cisco Emergency Responder 8.6 Administrator Guide*』には、Cisco Emergency Responder（Emergency Responder）8.6 を理解し、インストール、設定、管理、および使用するために必要な情報が記載されています。

対象読者

ネットワーク エンジニア、システム管理者、および電気通信エンジニアはこのガイドを読み、ネットワークで Emergency Responder を適切に設定するために必要な手順について習得する必要があります。また、Emergency Responder と Cisco Unified Communications Manager 間には密接なやり取りがあるため、Emergency Responder を導入する前に、Cisco Unified Communications Manager に精通しておく必要があります。

セキュリティ担当者は、『*Cisco Emergency Responder 8.6 User Guide*』を読む必要があります。

マニュアルの構成

次の表に、このマニュアルの構成を示します。

トピック	説明
第 1 章「Cisco Emergency Responder 8.6 の計画」	緊急コールの規定、Cisco ER を使用してこれらの規定を順守する方法、および Cisco ER を適切に導入するために行う必要あることを理解するために役立つ情報を提供します。
第 2 章「Cisco Emergency Responder 8.6 のインストール」	Emergency Responder 8.6 のインストールまたはアップグレードに関する詳細情報を提供します。
第 3 章「Cisco Emergency Responder 8.6 向けの Cisco Unified Communications Manager Versions 6.1 以降の設定」	Emergency Responder 8.6 向けに Cisco Unified CM 4.1、4.2、および 4.3 を設定する手順について説明します。
第 4 章「Cisco Emergency Responder 8.6 の設定」	緊急コールの管理が開始されるように Cisco ER を設定する方法について説明します。
第 5 章「Cisco Emergency Responder の Intrado V9-1-1 Enterprise Services との併用」	Cisco ER を設定して Intrado V-9-1-1 Enterprise と相互運用する方法について説明します。
第 6 章「Cisco Emergency Responder 8.6 Serviceability の設定」	Emergency Responder 8.6 Serviceability 機能を設定および使用する方法について説明します。
第 7 章「Cisco Emergency Responder 8.6 向けの Cisco Unified Operating System の設定」	Cisco ER 8.6 に付属の Cisco Unified Communications Operating System を設定および使用する方法について説明します。
第 8 章「Cisco Emergency Responder 8.6 Disaster Recovery System の設定」	Cisco ER 8.6 Disaster Recovery System を設定する方法について説明します。
第 9 章「Cisco Emergency Responder 8.6 Admin Utility の使用」	Cisco ER Admin Utility を使用する方法について説明します。
第 10 章「Cisco Emergency Responder のためのユーザの準備」	Cisco ER ユーザのさまざまなロールについて説明します。
第 11 章「Cisco Emergency Responder のトラブルシューティング」	Cisco ER で発生する可能性がある問題に対処し、解決方法を提示します。また、問題の特定と解決に関連するその他の作業も示します。
第 12 章「ALI フォーマット ツールの使用」	ALI フォーマット ツール（AFT）について説明し、AFT の使用方法およびトラブルシューティング方法に関する情報を提供します。
付録 A「Cisco Emergency Responder の管理 Web インターフェイス」	Cisco ER Administrator Web インターフェイスのページ上のフィールドについて説明します。
付録 B「Cisco Emergency Responder のサービスアビリティ Web インターフェイス」	Cisco ER Serviceability Web インターフェイスのページ上のフィールドについて説明します。
付録 C「Cisco Emergency Responder の Cisco Unified Operating System Administration Web インターフェイス」	Cisco Unified Operating System（OS）Administration Web インターフェイスのページ上のフィールドについて説明します。
付録 D「Cisco Emergency Responder の Disaster Recovery System Web インターフェイス」	Cisco ER Disaster Recovery System Administration Web インターフェイスのページ上のフィールドについて説明します。

トピック	説明
付録 E「Cisco Emergency Responder の Admin Utility Web インターフェイス」	Cisco ER Admin Utility Web インターフェイスのページ上のフィールドについて説明します。
付録 F「コマンド ライン インターフェイス」	使用可能なコマンド、コマンド構文、パラメータなどの、Cisco Unified OS Administration コマンドライン インターフェイスに関する情報を提供します。
付録 G「特定のサービス プロバイダーに対する AFT の使用」	AFT と組み合わせて使用する、サービス プロバイダー固有の情報を提供します。
付録 H「イベント ログ メッセージ」	Emergency Responder ベースのイベント ログ メッセージおよび管理アラートについて説明します。
付録 I「Emergency Responder でのポートの使用」	Cisco Emergency Responder によって使用されるポートに関する情報を提供します。

関連資料

Cisco Emergency Responder（Cisco ER）、Cisco Unified CallManager、および Cisco Unified Communications Manager の詳細については、次の資料を参照してください。

- すべての Cisco ER マニュアルは、次の URL で入手できます。

  http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

- Cisco Unified Communications Manager および Cisco Unified CallManager のインストールに関するマニュアルは、次の URL で入手できます。

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

- Cisco Unified Communications Manager および Cisco Unified CallManager オペレーティング システムのインストールに関するマニュアル、ならびにバックアップと復元に関するマニュアルは次の URL で入手できます。

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

- Cisco Unified Operations Manager 1.0 に関する情報は、次の URL で入手できます。

  http://www.cisco.com/en/US/products/ps6535/index.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

シスコ製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、および

ユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、次の URL で参照できます。
http://www.access.gpo.gov/bis/ear/ear_data.html

通知

This product includes software developed by Justin Wells and Semiotek Inc. for use in the WebMacro Servlet Framework (http://www.webmacro.org).

You may use WebMacro for use under the GNU General Public License.You may also use WebMacro under the terms of the Semiotek Public License.The terms of the Semiotek Public License are as follows:

Copyright (c) 1997, 1998, 1999, 2000 Semiotek Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Justin Wells and Semiotek Inc. for use in the WebMacro Servlet Framework (http://www.webmacro.org)."
4. The names "Semiotek Inc." and "WebMacro" must not be used to endorse or promote products derived from this software without prior written permission.For written permission, please contact justin@webmacro.org
5. Products derived from this software may not be called "WebMacro" nor may "WebMacro" appear in their names without prior written permission of Justin Wells.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Justin Wells and Semiotek Inc. for use in the WebMacro Servlet Framework (http://www.webmacro.org)."

THIS SOFTWARE IS PROVIDED BY SEMIOTEK INC. ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES OR CONDITIONS, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL SEMIOTEK INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

CHAPTER 1

Cisco Emergency Responder 8.6 の計画

『Cisco Emergency Responder 8.6 Administrator Guide』（Emergency Responder 8.6）は、緊急コールに効率的に応答したり、緊急コールの処理について地方自治体の規定を順守したりできるように、テレフォニー ネットワークで緊急コールを管理するのに役立ちます。北米では、その法令は、「Enhanced 911（E911）」と呼ばれています。同様の規定が他の国やロケールにも存在します。

緊急コールの規定は、国、地域、州、場合によっては首都圏内の場所ごとに異なることがあるため、Emergency Responder は、緊急コールの設定を特定の地域の要件に適合させるために必要な柔軟性を備えています。ただし、場所ごとに規定が異なり、さらに企業ごとにセキュリティ要件が異なるため、Emergency Responder を法的なニーズやセキュリティのニーズに適合する方法で配置するには、事前に広範囲の計画と調査を行っておく必要があります。

次のトピックは、緊急コールの規定、それらの規定を満たすために Emergency Responder がどのように役立つか、および Emergency Responder を正常に配置するために行う必要があることを理解するのに役立ちます。

Enhanced 911（E911）について

Enhanced 911（E911）は、北米の標準的な緊急コールである基本型 911 の拡張版です。次のトピックでは、E911 の要件および用語について説明します。

Enhanced 911 の要件の概要

Enhanced 911（E911）は、標準的な緊急コールである基本型 911 を拡張し、信頼性をさらに高めたものです。

北米で基本型 911 を使用している場合、発信者が 911 をダイヤルすると、コールが Public Safety Answering Point（PSAP）にルーティングされ、911 オペレータが呼び出されます。PSAP は発信者と話をし、警察、消防署、または救急車チームの派遣などの、適切な緊急応答を手配します。

E911 では、次の要件によってこの標準が拡張されています。

- 発信者のロケーションに基づいて緊急コールをローカル PSAP にルーティングする必要がある。（基本型の 911 では、コールは任意の PSAP にルーティングされる必要があるだけで、必ずしもローカル PSAP にルーティングされるわけではありません）。
- 発信者のロケーション情報を緊急オペレータの端末に表示する必要がある。この情報は、*自動ロケーション情報*（ALI）データベースを照会することによって取得されます。

E911 では、発信者のロケーションは緊急ロケーション識別番号（ELIN）によって特定されます。これは、緊急コールが切断された場合、または PSAP が発信者と再度話す必要がある場合に、PSAP が緊急発信者に再度連絡を取るためにダイヤルできる電話番号です。緊急コールは、この番号に関連付けられたロケーション情報に基づいて PSAP にルーティングされます。オフィス システムなどのマルチラインの電話システムの場合、電話機を Emergency Response Location（ERL; 緊急応答ロケーション）にグループ化することで、複数の電話機を ELIN と関連付けることができます。この場合、PSAP が受信するロケーションはオフィス ビルの住所となります。大規模なビルの場合は、このロケーションに、フロアやフロア上の領域などの追加情報が含まれます。各 ERL には、一意の ELIN が必要です。

これらの一般的な E911 の要件に加え、地域ごとにこれらの要件をさらに広げたり、抑えたりすることができます。たとえば、都市の規定において、ERL のサイズ（2,133.6 平方メートルを超えないなど）、ERL に設置できる電話機の台数（48 台を超えないなど）について特定の制限が含まれている場合があります。サービス プロバイダーおよび地方自治体と連携して、エリアに適切な E911 の要件を決定します。

関連項目

- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）
- 「Cisco Emergency Responder について」（P.1-3）

E911 および Cisco Emergency Responder の用語について

表 1-1 には、このマニュアルに使用される重要な用語の一部が定義されています。

表 1-1　E911 および Cisco Emergency Responder の用語

用語	定義
ALI	自動ロケーション情報。これは ELIN をロケーションに結び付ける情報です。この情報を使用して、緊急コールをその ELIN から正しいローカル PSAP にルーティングされます。この情報は PSAP に表示され、PSAP で緊急の発信者を探すのに役立ちます。Emergency Responder では、ERL ごとに ALI データを入力し、ALI データベースに含めるために ALI データをサービス プロバイダーに送信します。
ANI	自動番号識別。ANI は、ELIN の別名です。このマニュアルでは、ANI の代わりに ELIN を使用します。
CAMA	集中型自動メッセージ アカウンティング。公衆電話機交換網（PSTN）を迂回して、E911 選択ルータに直接接続されるアナログ電話トランクです。
DID	直通社内通話。電話ネットワークへのダイヤルインに使用できる、サービス プロバイダーから取得された電話番号です。DID 番号は、ELIN に使用されます。

表 1-1　E911 および Cisco Emergency Responder の用語（続き）

用語	定義
ELIN	Emergency Location Identification Number（緊急ロケーション識別番号）。これは、緊急コールをローカル PSAP にルーティングする電話番号です。PSAP は、この電話番号を使用して緊急の発信者にコールバックできます。緊急コールが切断された場合、または緊急コールを通常通り終了した後に PSAP が追加情報を必要とする場合、PSAP はこの番号が必要になることがあります。ALI を参照してください。
緊急コール	911 などの現地の緊急番号に発信されるコール。Emergency Responder がコールをサービス プロバイダーのネットワークにルーティングし、そこからそのコールがローカル PSAP にルーティングされます。
緊急発信者	緊急コールを発信する人。発信者は、個人的な緊急に助けを求めたり、一般的な緊急（火災、盗難、事故など）を報告したりします。
ERL	Emergency Response Location（緊急応答ロケーション）。これは、緊急コールの発信元エリアです。ERL は、必ずしも緊急のロケーションであるとは限りません。緊急の発信者が一般的な緊急を報告した場合、実際の緊急が別のエリアであることがあります。Emergency Responder では、スイッチ ポートおよび電話機を ERL に割り当てます。ERL 定義には ALI データが含まれています。
ESN	緊急サービス番号。
ESZ	緊急サービス ゾーン。特定の PSAP によってカバーされるエリアです。このエリアには通常、複数の警察署と消防署が含まれます。たとえば、都市とその郊外は 1 つの PSAP によってカバーされる可能性があります。 各 ESZ には、識別するために一意の ESN が割り当てられます。
MSAG	マスター住所録。これは、緊急コールを正しい PSAP に正確にルーティングできる ALI のデータベースです。Emergency Responder では、ALI 定義をエクスポートし、MSAG の更新を確認するサービス プロバイダーにその定義を送信します。このサービスをサービス プロバイダーとネゴシエートする必要があります。このサービスは、Emergency Responder を介して直接提供されるサービスではありません。
NENA	National Emergency Number Association。ALI 定義や、米国におけるその他の緊急コール要件のためのデータ形式およびファイル形式を推奨する組織です。Emergency Responder では、ALI データのエクスポート ファイルに NENA 形式を使用します。サービス プロバイダーによってデータ形式に制限が追加されているため、ALI エントリがそのサービス プロバイダーの規則に従っていることを確認してください。
PSAP	Public Safety Answering Point。PSAP は、緊急コールを受信する組織（たとえば、911 オペレータ）です。PSAP には、緊急コール処理の訓練を受けたスタッフが配置されます。PSAP は緊急発信者と話をし、適切な公共サービス組織（警察、消防署、救急車など）に緊急事態とそのロケーションを通知します。

関連項目

- 「Enhanced 911 の要件の概要」（P.1-1）
- 「Cisco Emergency Responder について」（P.1-3）

Cisco Emergency Responder について

次のトピックでは、Emergency Responder の概要と、ネットワークで Emergency Responder を使用する方法について説明します。

- 「Cisco Emergency Responder 8.6 の機能」（P.1-4）

Cisco Emergency Responder 8.6 の機能

Emergency Responder 8.6 の主な新機能および拡張機能を次に示します。

- 第 4 章「EnergyWise の使用」

Emergency Responder 8.6 でサポートされているハードウェアとソフトウェアのリストについては、『*Release Notes for Cisco Emergency Responder 8.6*』を参照してください。

ネットワークのハードウェアおよびソフトウェアの要件

Emergency Responder 8.6 では、さまざまなハードウェアおよびソフトウェア コンポーネントがサポートされています。サポートされているハードウェアとソフトウェアの完全なリストについては、『*Release Notes for Cisco Emergency Responder 8.6* 』を参照してください。このマニュアルは、http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_release_notes_list.html にあります。

Cisco Emergency Responder 8.6 のライセンス

Emergency Responder 8.6 では、製品ライセンスの要求、作成、および配布に Web ベースのシステムを使用します。Cisco.com の Web サイトで Emergency Responder 製品を登録すると、サーバ ライセンスを含むファイルが、電子メールにテキスト ファイル形式で添付されて送信されます。

この項は、次のトピックで構成されています。

初期インストールまたはアップグレードのライセンス

Emergency Responder 8.6 では、初期インストールのため、またはアップグレードの実行のためにライセンス キーは必要ありません。新規インストールまたは Emergency Responder 7.1 からのアップグレードから 60 日以内に新しいサーバ ライセンスをインストールする必要があります。Emergency Responder 8.0 以降からのアップグレードには、新しいサーバ ライセンスは必要ありません。ライセンス供与されていない Emergency Responder 8.6 ソフトウェアは、インストール後 60 日間、電話機 100 台のキャパシティで正常に動作します。追加のユーザ ライセンスは、サーバ ライセンスをインストールしてから有効になります。60 日以内にサーバ ライセンスをインストールしないと、Emergency Responder 8.6 システムはシャットダウンされます。

サーバ ライセンス

サーバ グループ内の Emergency Responder サーバごとにサーバ ライセンスを取得するには、サーバ ソフトウェアを注文する必要があります。1 つのライセンス ファイルに Emergency Responder パブリッシャと Emergency Responder サブスクライバの両方のライセンスを含めるか、または Emergency Responder サブスクライバの個別のライセンス ファイルを後で Emergency Responder パブリッシャにインストールすることができます。パブリッシャ サーバでイーサネット カードの MAC アドレスを使用して、パブリッシャおよびサブスクライバのライセンスを生成する必要があります。Emergency Responder サブスクライバの MAC アドレスは使用しないでください。

Emergency Responder サーバ ライセンスを注文するには、次の手順を実行します。

手順

ステップ 1　ご希望の注文方法で Emergency Responder 8.6 を注文します。Emergency Responder 8.6 と一緒に製品認証キー（PAK）を受け取ります。

ステップ 2　https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet に進み、PAK とパブリッシャの Emergency Responder サーバのメディア アクセス コントロール（MAC）アドレスを入力して Emergency Responder を登録します。Emergency Responder サブスクライバの MAC アドレスは使用しないでください。

パブリッシャの Emergency Responder サーバの MAC アドレスを取得するには、次の手順を実行します。

a.　Cisco Unified OS Administration の Web サイトにログインします。

b.　[Show] > [Network] の順に進みます。

c.　[Ethernet Details] セクションに MAC アドレスが表示されます。

処理後、電子メールにテキスト ファイル形式で添付されたサーバ ライセンス ファイルを受信します。

（注）　VMware のインストールの場合は、<Hardware MAC> の代わりに HOSTNAME=<License MAC> を使用してライセンス ファイルを生成してください。

ステップ 3　サーバ ライセンス ファイルをローカル サーバに保存して、そのファイルを Emergency Responder サーバにアップロードできるようにします。

ステップ 4　Emergency Responder Administration Web インターフェイスを使用して、サーバ ライセンス ファイルをアップロードします。サーバ ライセンス ファイルをアップロードする方法の手順については、「Cisco Emergency Responder ライセンス ファイルのアップロード」（P.4-25）を参照してください。

ユーザ ライセンス

ユーザ ライセンスは通常、プライマリ Emergency Responder サーバにインストールされますが、ユーザ ライセンスのインストール先に関係なく、プライマリとセカンダリの両方の Emergency Responder サーバでサーバ ライセンスが共有されます。

サーバ グループで使用できるユーザ ライセンス総数は、サーバ グループの両方のサーバで使用できるユーザ ライセンスの合計です。

Emergency Responder でサポートされているすべての Cisco Unified CM クラスタによって制御されたエンドポイント（IP ハードフォン、IP ソフトフォン、アナログ電話機を含む）ごとにユーザ ライセンスを購入する必要があります。Cisco Unified CM クラスタ内の一部のエンドポイントのみのライセンスを取得することはサポートされていません。

追加の Emergency Responder ユーザ ライセンス、またはアップグレードされた Emergency Responder ユーザ ライセンスを注文するには、次の手順を実行します。

手順

ステップ 1　追加の Cisco ER ユーザ ライセンス、またはアップグレードされた Cisco ER ユーザ ライセンスを注文します。追加のユーザ ライセンスごとに製品認証キー（PAK）を受け取ります。

ステップ 2　Cisco.com に進み、PAK とプライマリ Emergency Responder サーバのメディア アクセス コントロール（MAC）アドレスを入力して Emergency Responder を登録します。ユーザ ライセンスがプライマリ Emergency Responder サーバにインストールされます。Emergency Responder サブスクライバの MAC アドレスは使用しないでください。

（注）　VMware のインストールの場合は、<Hardware MAC> の代わりに HOSTNAME=<License MAC> を使用してライセンス ファイルを生成してください。

処理後、電子メールにテキスト ファイル形式で添付されたサーバ ライセンスを受信します。

ステップ 3　サーバ ライセンス ファイルをローカル サーバに保存して、そのファイルをプライマリ Emergency Responder サーバにアップロードできるようにします。

ステップ 4　ユーザ ライセンス ファイルをアップロードします。ユーザ ライセンスのアップロード方法の手順については、「Cisco Emergency Responder ライセンス ファイルのアップロード」（P.4-25）を参照してください。

（注）　Emergency Responder 8.0 以降は、プライマリ サーバでのみライセンス ファイルをアップロードできます。

（注）　Emergency Responder 8.0 以降は、サーバ ライセンスに暗黙的なライセンスは含まれません。ユーザ ライセンスを明示的に購入する必要があります。

ライセンス要件の決定

サーバ ライセンスの場合：

- Emergency Responder グループ内のサーバ（プライマリおよびセカンダリ）ごとにサーバ ライセンスを取得するには、サーバ ソフトウェアを注文します。サーバ ソフトウェアの 2 つのコピーをまとめて注文すると、ノード カウントが 2 のサーバ グループに対して 1 つのサーバ ライセンスを取得できます。Emergency Responder ソフトウェアの追加のコピーを個別に注文することによって、既存の Emergency Responder グループにセカンダリ サーバを追加できます。
- すべてのサーバ ライセンスは、プライマリ Emergency Responder サーバのメディア アクセス コントロール（MAC）に基づきます。Emergency Responder サブスクライバの MAC アドレスは使用しないでください。

- パブリッシャ サーバとサブスクライバ サーバ間では、サーバ ライセンスを共有できません。既存の Emergency Responder グループにセカンダリ サーバを追加するには、Emergency Responder ソフトウェアの個別のコピーを注文する必要があります。

ユーザ ライセンスの場合：

- Emergency Responder グループごとに 1 つ以上（必要に応じて）のユーザ ライセンスを注文します。
- 各 Emergency Responder グループ内のパブリッシャ サーバとサブスクライバ サーバ間でユーザ ライセンスを共有できます。
- Emergency Responder ユーザ ライセンスを Emergency Responder クラスタ内の異なる Emergency Responder グループ間で、または異なる Emergency Responder クラスタ間で共有することはできません。（クラスタの詳細については、「Cisco Emergency Responder のクラスタおよびグループについて」（P.1-14）を参照してください）。

例

Emergency Responder 設定で 500 ユーザをサポートする場合は、次のライセンスを購入する必要があります。

- Emergency Responder パブリッシャ サーバのサーバ ライセンスを取得するための、Emergency Responder ソフトウェアの 1 つコピー。
- Emergency Responder サブスクライバ サーバのサーバ ライセンスを取得するための、Emergency Responder ソフトウェアの 1 つコピー。このライセンスは、プライマリ Emergency Responder サーバのメディア アクセス コントロール（MAC）に基づきます。
- 最大 500 ユーザのユーザ ライセンスを購入します。
- Emergency Responder ソフトウェアの 2 つのコピーをまとめて注文すると、ノード カウントが 2 のサーバ グループに対して 1 つのサーバ ライセンスを取得できます。Emergency Responder ソフトウェアの追加のコピーを個別に注文することによって、既存の Emergency Responder グループにセカンダリ サーバを追加できます。

ライセンス ファイルのアップロード

Emergency Responder Administration Web インターフェイスを使用して、ライセンス ファイルを Emergency Responder サーバにアップロードできます。パブリッシャ サーバを起動して実行している場合、パブリッシャ サーバからのみすべてのライセンス ファイルをアップロードする必要があります。ライセンス ファイルをアップロードするには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration Web サイトにログインします。

ステップ 2　[System] > [License Manager] の順に選択します。[License Manager] ページが表示されます。

ステップ 3　[Upload license] をクリックします。[Upload File] ページが表示されます。

ステップ 4　[Browse...] ボタンを使用して、ローカル システムからアップロードするライセンス ファイルを選択します。

ステップ 5　[Upload] をクリックします。選択したライセンス ファイルが Emergency Responder サーバにアップロードされます。

（注）　Emergency Responder 8.0 以降は、プライマリ Emergency Responder サーバからのみサーバ ライセンスをアップロードできます。

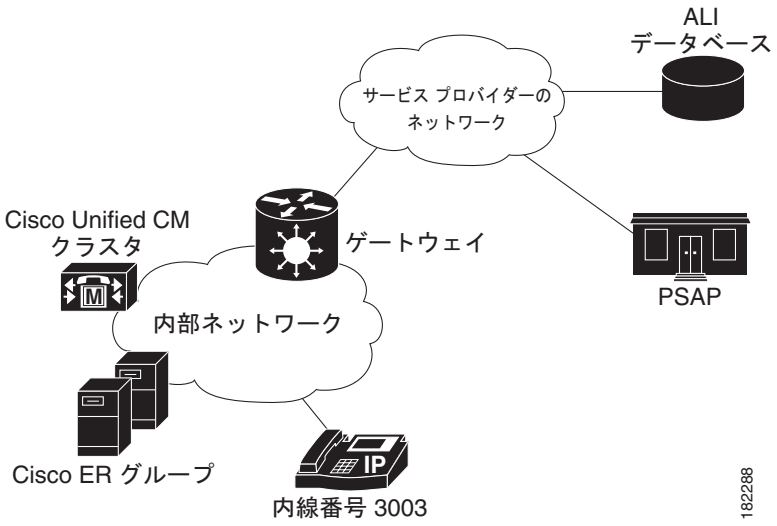
関連項目

- 「License Manager」（P.A-9）

Cisco Emergency Responder をご使用のネットワークに適合させる方法

図 1-1 に、Cisco Emergency Responder（Emergency Responder）をご使用のネットワークに適合させる方法を示します。

図 1-1　Cisco Emergency Responder をご使用のネットワークに適合させる方法



Emergency Responder は、緊急コールを Emergency Responder グループに送信するために変更する必要のある、会社のダイヤル プランの Cisco Unified Communications Manager に依存します。必要な Cisco Unified Communications Manager の設定の詳細については、第 3 章「Cisco Emergency Responder 8.6 向けの Cisco Unified Communications Manager Versions 6.1 以降の設定」を参照してください。

電話機を追跡するために、Emergency Responder では、クラスタに登録されている電話機のリストについて Cisco Unified Communications Manager に照会します。その後、Emergency Responder では、電話機が接続されているポートを特定するためにネットワーク上のスイッチ（Emergency Responder のものであると識別されたスイッチ）に照会します。移動された電話機を識別できるように、Emergency Responder では、日中に定期的にこの追跡を行います。Emergency Responder でのスイッチの設定の詳細については、「Cisco Emergency Responder のスイッチの設定」（P.4-44）を参照してください。Emergency Responder で緊急コールをポートと電話機ロケーションに基づいて正しい PSAP に送信できるようにスイッチ ポートを設定する方法については、「電話機の管理」（P.4-54）を参照してください。

オプションとして、ご使用のネットワークまたはサービス プロバイダーに SMTP 電子メール サーバを設定することもできます。電子メールをオンサイト アラート（セキュリティ）担当者に送信するように Emergency Responder を設定し、それらの担当者に緊急コールを通知することができます。サーバを電子メールベースのページング サービスとして設定するとそれらの担当者がページングされます。

最後に、Emergency Responder で緊急コールを現地の Public Safety Answering Point（PSAP）にルーティングできるように、サービス プロバイダーのネットワークへの PRI または CAMA リンクを備えたゲートウェイが必要です。

図 1-1 に、1 つの Cisco Unified Communications Manager クラスタをサポートしている 1 つの Emergency Responder グループを示します。Cisco Unified CM で同一バージョンのソフトウェアを実行している限り、1 つの Emergency Responder グループで複数の Cisco Unified Communications Manager クラスタをサポートできます。より大規模なネットワークでは、複数の Emergency Responder グループをインストールし、Emergency Responder クラスタを作成することができます。このインストールの説明については、「Cisco Emergency Responder のクラスタおよびグループについて」（P.1-14）を参照してください。

Emergency Responder で管理される場合に緊急コールで取得するパスの説明については、「緊急コールの発信時に発生するプロセス」（P.1-9）を参照してください。

関連項目

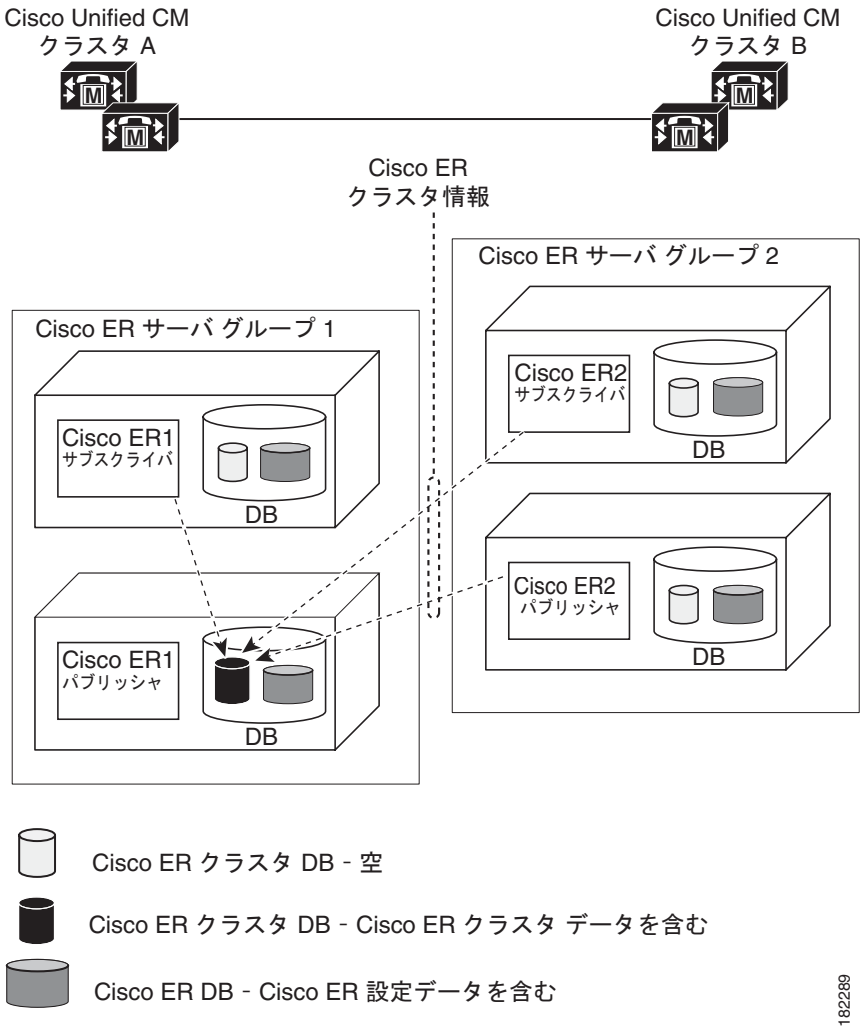
- 「Cisco Emergency Responder のクラスタおよびグループについて」（P.1-14）
- 「必要な Cisco Emergency Responder グループ数の決定」（P.1-17）
- 「Cisco Emergency Responder の配置」（P.1-24）

緊急コールの発信時に発生するプロセス

このトピックでは、緊急コールを処理するために Cisco Emergency Responder（Emergency Responder）で使用するプロセスについて説明します。このプロセスを理解すると、Emergency Responder を正しく設定し、発生する可能性のある問題のトラブルシューティングを実行することができます。

図 1-2 は、Emergency Responder で緊急コールをルーティングする方法を示します。

図 1-2　Cisco Emergency Responder で緊急コールをルーティングする方法



誰かが内線 3003 を使用して緊急コールを発信した場合：

1. Cisco Unified Communications Manager によって、そのコールが Emergency Responder にルーティングされます。
2. Emergency Responder では、発信者の緊急応答ロケーション（ERL）に設定されているルート パターンを取得します。コール ルーティングの順序については、「Cisco Emergency Responder のコール ルーティングの順序」（P.1-11）を参照してください。
3. Emergency Responder によって、発信者番号が発信者の ERL に設定されているルート パターンに変換されます。このルート パターンは、適切な緊急ロケーション識別番号（ELIN）を Public Safety Answering Point（PSAP）に渡すために設定されます。ELIN は、緊急の発信者にコールバックするために PSAP で使用できる電話番号です。
4. デフォルトでは、Emergency Responder によって、発信者の内線番号と ELIN の間のマッピングが最大 3 時間保存されます。エントリのタイムアウト前にマッピングが後続のコールで上書きされる場合があります。タイムアウトの設定を 3 時間よりも長くしたり、短くしたりすることもできます（「Cisco Emergency Responder Group Settings」（P.A-3）を参照）。

5. Emergency Responder では、発信者の ERL に設定されているルート パターンを使用してコールがルーティングされます。次に、このルート パターンでは、設定されたルート リストを使用して、緊急コールを適切なサービス プロバイダーのネットワークに送信します。サービス プロバイダーは、自動ロケーション情報（ALI）で ELIN を検索し、コールを適切なローカル PSAP にルーティングします。PSAP では、電話コールを受信し、ALI データベースで ALI を検索します。
6. 同時に、Emergency Responder によって、Web アラートが Emergency Responder ユーザに送信されます。さらに、Emergency Responder では、ERL に割り当てられているオンサイト アラート（セキュリティ）担当者にコールします。その担当者の電子メール アドレスを設定している場合、Emergency Responder によって、電子メールも送信されます。そのアドレスが電子メールベースのページング サービス用である場合には、その担当者に電子メールではなく、ページが送信されます。
7. 緊急コールが突然切断された場合、PSAP は ELIN を使用して緊急の発信者にコールバックできます。ELIN のコールは Emergency Responder にルーティングされ、Emergency Responder によって、ELIN が ELIN と関連付けられているキャッシュされた最後の内線番号に変換されます。その後、コールがその内線にルーティングされます。

適切なパフォーマンスを確保し、障害点をなくすには、次の内容を確認します。

- 緊急コールが正しくルーティングされるようにするためには、発信者の電話機を正しい ERL に割り当てる必要があります。電話機に関連付けられている ERL が正しいかを確認するには、ERL デバッグ ツールを使用します。
- コールの正確なルーティングについて他に考えられる問題としては、ELIN 定義があります。ELIN ルート パターンを誤ったゲートウェイに割り当てた場合、緊急コールが誤ったネットワークにルーティングされる可能性があります。これにより、緊急コールが間違った PSAP に送信される可能性があります。

  サービス プロバイダーと連携して、必要なゲートウェイ数とゲートウェイを接続する場所を決定します。これらの要件は、ご使用のネットワーク トポロジよりもサービス プロバイダーのネットワーク トポロジに基づきます。米国では、緊急コール ネットワークは PSTN に直列に接続するため、PSTN に接続しただけでは、緊急コールは正しくルーティングされません。
- ALI データベースの情報が正しくないと、サービス プロバイダーのネットワークでコールが正しくルーティングされない可能性があります。ALI データをエクスポートしてそのデータをサービス プロバイダーに送信し、ELIN またはロケーションの情報を変更した場合には必ず ALI データを再送信します。
- ERL から多数の緊急コールが発信されると、PSAP では、緊急の発信者に正常にコールバックできない可能性があります。Emergency Responder では、ELIN-to-extension マッピングが最大 3 時間キャッシュされます。ERL に 2 つの ELIN を定義し、3 時間の間に 3 つの緊急コールが発信された場合、最初の ELIN が 2 回使用されます。つまり、1 回目は最初の発信者に、2 回目は 3 番目の発信者に使用されます。PSAP で最初の ELIN をコールした場合、PSAP は最初の発信者ではなく、3 番目の発信者に到達します。この問題が発生する可能性は、ELIN に定義する ELIN の数と ERL における標準的な緊急コール率で決まります。

Cisco Emergency Responder のコール ルーティングの順序

Emergency Responder では、緊急コールが発信された電話機のロケーションに基づいて緊急コールを転送します。電話機のロケーションは、優先順位に従って次の方法によって判断されます。

- 擬似電話：電話の MAC アドレスは、擬似電話の MAC アドレスと一致し、テスト用の緊急応答ロケーション（ERL）に割り当てられます。「擬似電話機の追加」（P.4-67）および「テスト ERL の設定」（P.4-40）を参照してください。

- スイッチ ポートの背後で追跡される IP 電話 : IP 電話の MAC アドレスは、ERL に割り当てられているスイッチ ポートの背後で追跡されます。「スイッチ ポートの設定」（P.4-54）を参照してください。
- IP サブネットを使用して追跡される IP 電話 : IP 電話の IP アドレスは、ERL に割り当てられている IP サブネットワークに属します。「IP サブネットベースの ERL の設定」（P.4-38）を参照してください。
- 同じ Emergency Responder クラスタ内の別の（リモートの）Emergency Responder サーバ グループによって追跡される IP 電話 : リモート サーバ グループでは、スイッチ ポートの背後で、または IP サブネットで IP 電話を追跡します。緊急コールを受信すると、リモートの Emergency Responder サーバ グループでカバーされている Cisco Unified Communications Manager クラスタに緊急コールが転送されます。「クラスタ間の電話機の移動」（P.11-24）を参照してください。
- 手動で設定された電話 : 電話の回線番号は、手動で ERL に割り当てられます。「電話機の手動での定義」（P.4-63）を参照してください。
- 位置未確認の電話 : IP 電話の MAC アドレスは、ERL に割り当てられます。「位置未確認の電話の識別」（P.4-62）を参照してください。
- デフォルト ERL : 電話機ロケーションを特定するために、前のどの基準も使用されません。コールは、デフォルト ERL にルーティングされます。「デフォルト ERL の設定」（P.4-33）を参照してください。

（注）　Cisco Unified IP Phone には、MAC または IP アドレスの追跡が推奨されます。MAC または IP アドレスによって追跡されない IP 電話は、手動の回線番号設定でロケーションが割り当てられている場合でも、位置未確認の電話機として表示されます。

（注）　手動で設定された電話機には、Emergency Responder で、先頭に「+」を含む回線番号に基づいてロケーションを割り当てることができません。Emergency Responder で回線番号に基づいてアナログ電話機にロケーションを割り当てる場合は、Cisco Unified CM で、先頭に「+」を付けてその電話機を設定しないでください。

お客様は、[Unlocated Phones] ページから IP 電話が削除されることがないように、IP 電話が MAC または IP アドレスによって追跡されない問題を解決するようにしてください（「位置未確認の電話機が多すぎる」（P.11-2）を参照）。[Unlocated Phones] ページで ERL を IP 電話に直接割り当てることはできますが、その電話機に手動の回線番号設定でロケーションが割り当てられていると、この割り当ては有効になりません。ERL Debug Tool を使用して、[Unlocated Phones] ページに表示される IP 電話に有効な ERL 割り当てを決定します。

位置未確認の電話の識別

Emergency Responder では、位置未確認の電話機を、次のすべての基準を満たす Cisco Unified IP Phone として定義します。

- IP 電話が、Emergency Responder グループに認識される Cisco Unified Communications Manager に登録されていること。
- IP 電話の MAC アドレスがスイッチ ポートの背後で追跡されていないこと。
- IP 電話の IP アドレスが IP サブネットを使用して追跡されていないこと。
- IP 電話の MAC アドレスが Emergency Responder で模擬電話機として定義されていないこと。

（注）　リモートの Emergency Responder サーバ グループによって追跡される Cisco Unified IP Phone と ERL に手動で回線番号が割り当てられている IP 電話機も [Unlocated Phones] 画面に表示されます。

位置未確認の電話への ERL の割り当て

Emergency Responder では、ERL を [Unlocated Phones] 画面に表示される IP 電話機に割り当てる手順を提供します。この割り当てによって、位置未確認の電話の MAC アドレスが管理者によって選択される ERL に関連付けられます。この関連付けには、次の規則が適用されます。

- [Unlocated Phones] ページでの ERL の IP 電話機への関連付けによって、IP 電話機のステータスは変更されません。つまり、IP 電話機が前に説明されているように位置未確認の電話機の基準と一致しているため、IP 電話は [Unlocated Phones] ページに表示されたままです。
- ERL の関連付けが使用されるのは、前の規則を使用して（Emergency Responder で特定されるように）IP 電話機の位置が確認できない場合だけです。

たとえば、電話 A は現在検出されず、[Unlocated Phones] ページに表示されます。位置未確認の電話に ERL 割り当て機能を使用して、この電話の ERL としてロケーション A が割り当てられます。後続の電話の追跡サイクルによって、スイッチ ポートの背後で電話 A が検出されると、[Unlocated Phones] ページに電話 A が表示されなくなります。電話 A のロケーション A への割り当ては無効になります。関連付けは不変であるため、その後も IP 電話機の位置が不明である場合でも、その割り当ては有効です。

CTI アプリケーションによって転送されるコールのロケーション情報

Cisco Unity などのコンピュータ テレフォニー インテグレーション（CTI）アプリケーションによって緊急コールが 911 に転送される場合、コール ルーティングおよび PSAP レポートで使用されるロケーションは、元の発信者のロケーションではなく、アプリケーション サーバのロケーションです。これについては、Cisco Unified CM 4.2(3) および 4.3、Cisco Unified CM 5.1、6.0、および 6.1 で可能であるように、アプリケーションによって元の発信側回線が保持される場合でも引き続き適用されます。このため、911 を直接ダイヤルする必要があります。

関連項目

- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）
- 「データの整合性および信頼性に関する考慮事項」（P.1-18）
- 「ERL について」（P.4-30）
- 「 •「ERL の作成」（P.4-33）」（P.3-10）
- 「PSAP への接続に使用されるゲートウェイに対するコーリング サーチ スペースの設定」（P.3-18）
- 「Cisco Emergency Responder 用のネットワークの準備」（P.1-20）

Cisco Emergency Responder のクラスタおよびグループについて

ご使用のネットワークに Cisco Emergency Responder（Emergency Responder）を一対の冗長サーバとして配置します。1 つのサーバはパブリッシャ サーバとして指定し、もう 1 つのサーバはサブスクライバ サーバとして指定します。Emergency Responder のパブリッシャ サーバとサブスクライバ サーバは、それぞれ 1 つの Emergency Responder サーバ グループを構成します。サーバ グループの設定データは、パブリッシャのデータベースに保存されます。このデータは、サブスクライバに複製されます。

Emergency Responder クラスタは、正しい緊急コール処理機能を提供するためにデータを共有する一連の Emergency Responder サーバ グループです。Emergency Responder クラスタ情報は、クラスタ内のクラスタ データベースと呼ばれる中央の場所に保存されます。Emergency Responder サーバ グループは、そのグループがクラスタ内の他のサーバ グループと同じクラスタ データベースを指している場合、そのクラスタの一部であると見なされます。

Emergency Responder 8.6 では、次の 2 つの個別のデータベースを使用します。

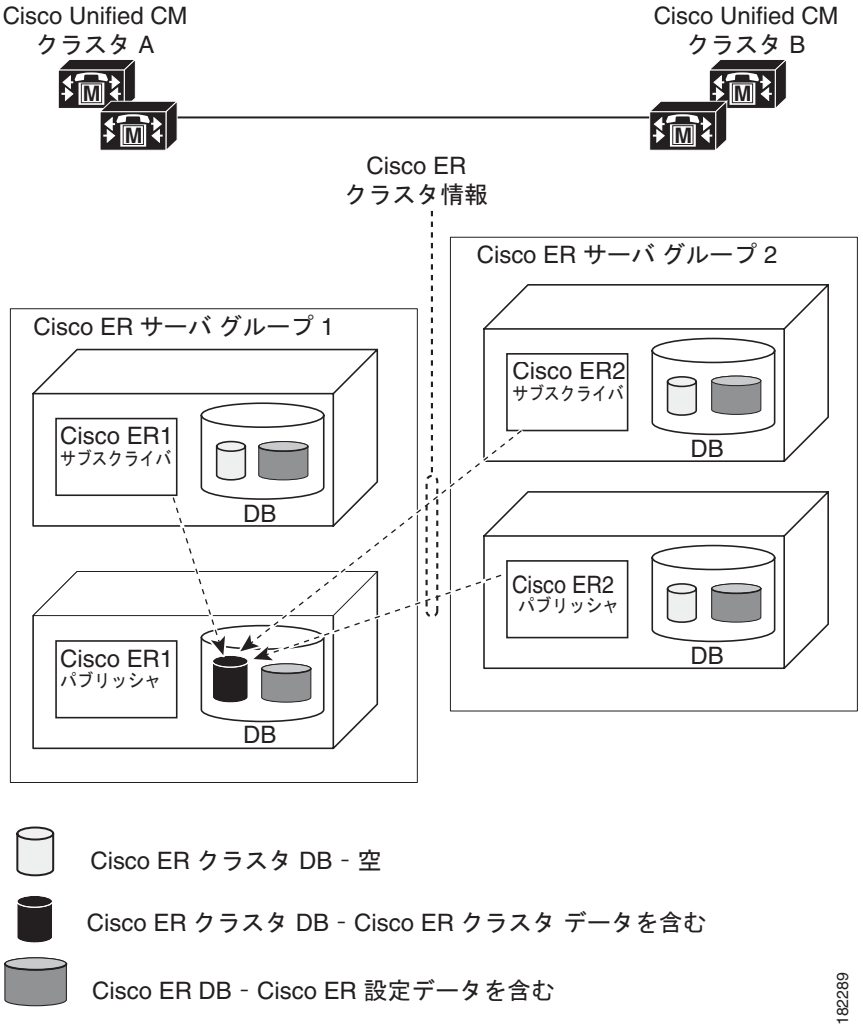
- 1 つのデータベースには、Emergency Responder の設定情報が保存されます。
- 2 つ目のデータベースには、Emergency Responder のクラスタ情報が保存されます。

インストール時に、両方のデータベースが各 Emergency Responder サーバに作成されます。ただし、クラスタ データは、1 つの Emergency Responder サーバにのみ含まれます。

（注） 同一の Emergency Responder グループには、バージョンが異なる Emergency Responder を配置できません。Emergency Responder 8.6 にアップグレードする場合は、両方の Emergency Responder サーバをバージョン 8.6 にアップグレードするようにしてください。Cisco Unified CM 8.5 または 8.6 に登録されている電話機が EnergyWise Power Save Plus モードに設定されている場合は、EnergyWise が以前のバージョンの Emergency Responder でサポートされていないため、クラスタ内のすべての Emergency Responder サーバ グループが Emergency Responder 8.6 である必要があります。Emergency Responder 8.6 の大規模検出では、EnergyWise Power Save Plus モードにある電話機は削除されません。

図 1-3 は、Cisco Emergency Responder（Emergency Responder）グループを 1 つの Emergency Responder クラスタに結合する方法を示します。

図 1-3　Cisco Emergency Responder グループと Cisco Emergency Responder クラスタ間の関係について



この例では、次のようになります。

- 2 つの Cisco Unified Communications Manager クラスタ、Cisco Unified CM クラスタ A および Cisco Unified CM クラスタ B があります。
- Emergency Responder サーバ グループ 1 と Emergency Responder サーバ グループ 2 で 1 つの Emergency Responder クラスタが形成されています。
- Emergency Responder サーバ グループ 1 は Cisco Unified CM クラスタ A をサポートし、Emergency Responder サーバ グループ 2 は Cisco Unified CM クラスタ B をサポートしています。
- Cisco ER1 パブリッシャのクラスタ データベースに、両方の Emergency Responder サーバ グループの Emergency Responder クラスタ情報が保存されます。点線は、Emergency Responder サーバとクラスタ データベース ホストとの通信を示します。
- 各 Emergency Responder サーバには、Emergency Responder の設定情報が含まれたデータベースがあります。

（注）　Emergency Responder クラスタ内の電話機の追跡が正確に動作するように、クラスタ内の Emergency Responder サーバがそのホスト名で検出され、その他すべての Emergency Responder サーバからネットワーク上のクラスタ内の Emergency Responder サーバに到達できるようにする必要があります。

（注）　Emergency Responder サーバ グループの設定を設定するときに、[System Administrator Mail ID] フィールドにシステム管理者の電子メール アカウントを入力した場合、スタンバイ サーバによってコールが処理されるときに、またはスタンバイ サーバがプライマリ サーバを継承するときに、システム管理者は電子メール通知を受信します。（「Cisco Emergency Responder サーバ グループの設定」（P.4-22）を参照）。

Emergency Responder クラスタの作成を完了するには、クラスタ内トランクとルート パターンを作成することにより、Emergency Responder グループがグループ間で緊急コールを渡したり（「Cisco Emergency Responder グループ間の通信に対するルート パターンの作成」（P.3-19）を参照）、Emergency Responder でこれらのルート パターンを設定したり（「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）を参照）できるようにする必要があります。

注意　Emergency Responder クラスタの作成前に、Emergency Responder クラスタによってサポートされるすべての Cisco Unified Communications Manager クラスタのダイヤル プランを一意にする必要があります。たとえば、1 つの Cisco Unified Communications Manager クラスタには、内線 2002 のみを設定できます。ダイヤル プランが重複している場合は、Emergency Responder クラスタを分離しておく必要があります。その場合、これらの Cisco Unified Communications Manager クラスタ間の電話機の動的な移動をサポートできません。

注意　E.164 ダイヤル プランのユーザは、Cisco Emergency Responder が、先頭の桁として「+」が含まれる数字列で使用されるようには設計されていないことに注意してください。

クラスタ間の電話機の移動

次のシナリオは、Emergency Responder でクラスタ間の電話機の移動を処理する方法について示します。

- Server Group A（SGA）には、SGA 以外に移動する電話機（Phone_1）があります。
  - Emergency Responder は Server Group B（SGB）で Phone_1 を検出します。
  - SGA の [Unlocated Phones] ページに SGB の電話機が表示されます。
- SGB の両方の Emergency Responder サーバ（パブリッシャとサブスクライバ）が停止しても、SGA には SGB の Phone_1 が表示されたままになります。
  - このときに Phone_1 から発信されたコールは SGB にリダイレクトされ、Emergency Responder サーバがその SGB 内に存在しない場合、Emergency Responder は同じ手順を実行してこの緊急コールをルーティングします。
  - また、両方の SGB Emergency Responder サーバが停止している場合、Phone_1 は、SGB 内の他の電話機と同様に扱われます。

- Phone_1 が Server Group C（SGC）に移動した場合：
  - SGA、SGC の順で次回の増分電話機のトラッキングが実行されると検出されます。
  - [Unlocated Phones] ページでは、Phone_1 から SGC への関連付けが変更されます。
- Phone_1 が元の SGA に移動すると、次回の増分電話機トラッキングで検出され、対応するスイッチ ポートの下に表示されます。

Emergency Responder システムを計画する際には、次のことに留意してください。

- 1 つの Emergency Responder *グループ*で、Cisco Unified Communications Manager バージョンが混在しているクラスタをサポートすることはできません。たとえば、Emergency Responder は、すべての Cisco Unified Call Manager 4.2 クラスタ**または**すべての Cisco Unified Call Manager 5.1 クラスタをサポートできます。

  ただし、Emergency Responder クラスタには、異なるバージョンの Cisco Unified Communications Manager をサポートする Emergency Responder グループを含めることができます。この方法により、Emergency Responder で、テレフォニー ネットワーク内の Cisco Unified Communications Manager バージョンの混在をサポートできます。
- Emergency Responder 86 サーバ グループは、他の Emergency Responder 8.6 サーバ グループまたは Emergency Responder 1.3 サーバ グループとともに動作できます。

（注） 共用回線を使用して Cisco Unified IP Phone から緊急コールを発信すると、コールがクラスタを介して間違った ERL に終端する可能性があります。

（注） 検出されて ERL に関連付けられている電話機を、同じ Emergency Responder クラスタに属する別の Emergency Responder サーバ グループによって追跡される別の Cisco Unified CM クラスタに移動するには、現在の Emergency Responder サーバ グループから ERL の関連付けを削除する必要があります。現在の Emergency Responder サーバ グループから ERL の割り当てを解除するには、「位置未確認の電話の識別」（P.4-62）のステップ 7 を参照してください。

関連項目

- 「Cisco Emergency Responder をご使用のネットワークに適合させる方法」（P.1-8）
- 「緊急コールの発信時に発生するプロセス」（P.1-9）

必要な Cisco Emergency Responder グループ数の決定

Cisco ER の効率的なパフォーマンスを実現するには、Emergency Responder の配置を計画する際に各 Emergency Responder グループでサポートできる制限を考慮する必要があります。1 つの Emergency Responder グループは複数の Cisco Unified Communications Manager クラスタをサポートできますが、1 つの Cisco Unified Communications Manager クラスタは 1 つの Emergency Responder グループでしかサポートできないことに注意してください。

設定を含む 1 つの Emergency Responder グループのキャパシティについては、『*Release Notes for Cisco Emergency Responder 8.6*』を参照してください。別の数値に達していなくても、1 つの制限に関して最大数値を満たすことができることに留意してください。たとえば、1,000 個のスイッチを定義できますが、スイッチ ポートは 30,000 個未満です。

追加のグループをインストールすることにより、さらに大規模なネットワークを管理できます。各 Emergency Responder グループは、1 つ以上の Cisco Unified Communications Manager クラスタと連携できます。

これらのグループごとの制限に加えて、サービス プロバイダーの ALI データベース プロバイダーによってカバーされる管轄区域も考慮する必要があります。ネットワークが複数の ALI データベース プロバイダーの管轄区域に及ぶ場合は、ALI フォーマット ツール（AFT）を使用して、ALI レコードを複数の ALI データベース形式でエクスポートしてください。

1 つの Emergency Responder グループで複数の LEC をサポートするには、次の手順を実行します。

手順

ステップ 1　Emergency Responder からの ALI レコード ファイル出力を標準の NENA 形式で取得します。このファイルには、複数の LEC に宛てられたレコードが含まれています。

ステップ 2　必要な ALI フォーマットごとに元のファイルの 1 つのコピーを作成します（LEC ごとに 1 つのコピー）。

ステップ 3　最初の LEC（たとえば、LEC-A）の AFT を使用して、NENA 形式のファイルのコピーをロードし、他の LEC に関連付けられているすべての ELIN のレコードを削除します。（AFT の使用方法については、第 12 章「ALI フォーマット ツールの使用」を参照してください）。削除する情報は、通常、NPA（またはエリア コード）によって識別できます。

ステップ 4　結果として生成されたファイルを、LEC-A に必要な ALI フォーマットで保存し、適宜ファイル名を付けます。

ステップ 5　各 LEC に対してステップ 3 と 4 を繰り返します。

各 LEC に AFTs を使用できない場合、テキスト エディタで NENA 形式のファイルを編集することで、同じ結果をアーカイブできます。

関連項目

- 「Cisco Emergency Responder のクラスタおよびグループについて」（P.1-14）
- 「Cisco Emergency Responder の配置」（P.1-24）
- 「ALI 提出要件に関するサービス プロバイダーとの交渉」（P.1-22）
- 「サービス プロバイダー向け ALI 情報のエクスポート」（P.4-42）
- 第 12 章「ALI フォーマット ツールの使用」
- 「ALI Formatting Tool」（P.A-80）

データの整合性および信頼性に関する考慮事項

ローカル PSAP への緊急コールの正しいルーティングは、ERL 設定に基づきます。ご使用のネットワーク内では、正しい電話機の識別によって、サービス プロバイダーのネットワークへの接続に使用するゲートウェイが決定されます。サービス プロバイダーのネットワークでは、ルーティングは ELIN に基づきます。ELIN は、発信者の ALI の検索にも使用されます。そのため、正確な ELIN が緊急コールに割り当てられるように、ERL 設定の信頼性を確保する必要があります。

ERL 設定の信頼性を維持するために考慮する事項を次に示します。

- ERL は、ポート自体のロケーションではなく、ポートに接続されているデバイスのロケーションに基づいてスイッチ ポートに割り当てられます。したがって、ポートに接続されているワイヤを変更すると（たとえば、2 つ以上のポート間でワイヤを切り替えることによって）、ポートに現在接続されているデバイスが実際には別の ERL に配置されている可能性があります。ポートに割り当てられている ERL を変更しない場合、誤った ELIN がポートに使用され、間違った ALI が PSAP に送信されてしまいます。

  1 つの LAN スイッチが別の PSAP によってカバーされる ERL に接続される可能性は低いため、通常、この種の変更によって、コールが誤ってルーティングされることはありません。ただし、送信された ALI は間違っているため、発信者が実際に 4 階にいる場合の緊急に対してセキュリティ スタッフは 3 階を調べる可能性があります。

  この問題を防止するには、ワイヤリング クローゼットが安全に配置されていることを確認し、スイッチ ポート間のワイヤを交換しないようにネットワーキング スタッフに指導します。

- Emergency Responder で自動的に追跡できない電話機の場合は、これらの電話機に対して何らかの移動、追加、または変更を行うと、Emergency Responder の設定も更新されることを確認します。このようなタイプの電話機の定義については、「電話機の手動での定義」（P.4-63）を参照してください。

（注）　スイッチ ポートのマッピングが変更された場合、電子メール アラートが送信されます。

- Emergency Responder 1.2 よりも前は、登録された電話機がスイッチ ポートの背後で検出されなかった場合、Emergency Responder によって、[Unlocated Phones] ページに電話機のリストが表示されます。

  Emergency Responder 1.2 以降では、これらの電話機は次のように検索されます。

  - 登録された電話がスイッチ ポートの背後で検出されない場合、設定された IP サブネットの 1 つで見つけることができます。
  - 登録された電話機がスイッチ ポートの背後で検出されない場合、電話機の IP サブネットが設定されていない場合、あるいは電話機が模擬電話機として設定されていない場合、Emergency Responder によって、[Unlocated Phones] ページに電話機のリストが表示されます。

    Emergency Responder でコール ルーティングに使用する ERL を決定するには、ERL デバッグ ツールを使用して電話機を検索します。この検索により、この電話機からの緊急コールのルーティングで使用される現在の ERL と、Emergency Responder がその ERL を選択した理由が得られます。詳細については、「Cisco Emergency Responder Admin Utility の使用」（P.11-19）を参照してください。

- Emergency Responder 8.6 をインストールする際に、パブリッシャ サーバ（プライマリ）と、そのパブリッシャを指定するサブスクライバ サーバ（バックアップ）を設置します。パブリッシャ サーバおよびサブスクライバ サーバは、それぞれ 1 つの Cisco ER サーバ グループを構成します。この冗長性は、1 つのサーバの障害が緊急コールの発信機能に影響しないようにするのに役立ちます。WAN リンクで分離されていない別のサブネット上にある、プライマリ サーバと物理的に離れた場所にスタンバイ サーバを設置することを検討してください。この分離は、プライマリ サーバを設置しているビルの火災、プライマリ サーバのホストとなるサブネットとの接続切断などのような中断から保護することができます。

- スイッチの（たとえば、モジュールの追加や変更による）追加、削除、または更新時に Emergency Responder の設定が定期的に更新されることを確認します。スイッチを変更したら、Emergency Responder でスイッチを表示し、[Locate Switch Ports] をクリックして、スイッチ上でスイッチ ポートおよび電話機更新プロセスを実行します。詳細については、「LAN スイッチの指定」（P.4-48）を参照してください。

未定義のスイッチに接続されている電話機は、Emergency Responder に位置未確認の電話機としてリストに表示されます。定義されたスイッチを変更した場合、新しいポート、または変更されたポートは、ERL の関連付けのないポートになります。新しいスイッチ ポート、または追加されたスイッチ ポートに対して ERL を割り当てる必要があります。ネットワーク変更に関係する反復的な作業については、「ネットワーク管理者のロールについて」（P.10-3）および「ERL 管理者のロールについて」（P.10-2）を参照してください。

- ERL/ALI 設定を変更する際には、その情報をエクスポートし、ALI データベースに含めるためにサービス プロバイダーにその情報を送信する必要があります。これにより、緊急コールが正しい PSAP にルーティングされ、PSAP に正しい ALI が提示されるようになります。詳細については、「ERL 情報のエクスポート」（P.4-41）および「サービス プロバイダー向け ALI 情報のエクスポート」（P.4-42）を参照してください。

関連項目

- 「緊急コールの発信時に発生するプロセス」（P.1-9）
- 「Cisco Emergency Responder のクラスタおよびグループについて」（P.1-14）
- 「必要な Cisco Emergency Responder グループ数の決定」（P.1-17）
- 「Cisco Emergency Responder のためのユーザの準備」（P.10-1）

Cisco Emergency Responder 用のネットワークの準備

次のトピックでは、Cisco Emergency Responder を配置する前にネットワークの準備に必要な手順について説明します。

- 「PSTN に対する CAMA トランクまたは PRI トランクの取得」（P.1-20）
- 「サービス プロバイダーからの DID 番号の入手」（P.1-21）
- 「ALI 提出要件に関するサービス プロバイダーとの交渉」（P.1-22）
- 「スイッチおよび電話機のアップグレード」（P.1-22）

PSTN に対する CAMA トランクまたは PRI トランクの取得

緊急コールを処理するには、PRI トランクまたは CAMA トランクを取得してサービス プロバイダーに接続する必要があります。ご使用のサービス プロバイダーでサポートされているトランクのタイプが 1 つだけである可能性があります。サービス プロバイダーに問い合わせて、最適に機能する接続のタイプを決定します。

次の問題について検討してください。

- PRI：緊急コールに PRI 接続を使用する場合、標準電話トラフィックで接続を共有できます。標準トラフィックにトランクを使用する場合、トランク使用率を監視して、緊急コールの処理に利用可能な帯域幅が十分にあることを確認します。キャパシティが不十分である場合、緊急の発信者はコールを発信したときにビジー信号を受け取る可能性があります。キャパシティ プランニングが緊急コールの要件に基づいていることを確認します。

  PRI トランクを設定する際に、汎用番号（サイトのメイン番号など）ではなく、実際の発信者番号が送信されるように設定する必要があります。そのように設定しないと、PSAP では、予測される ELIN が受信されず、緊急コールが正しい PSAP にルーティングされない可能性があります。

- CAMA：CAMA トランクは、緊急コール専用であり、ほとんどのエリアで使用できます。CAMA トランクは、標準音声トラフィックによって使用されることはないため、CAMA トランクにキャパシティを計画する必要はありません。

サービス プロバイダーと連携して、ご使用のネットワークに必要なトランク数を決定します。たとえば、一部のサービス プロバイダーでは、10,000 台の電話機に対して 2 つの CAMA トランクを使用するガイドラインを採用しています。

また、トランク数は、ローカル PSAP に対するオフィスの分配に応じて異なる可能性があります。たとえば、ニューヨークとシカゴにオフィスがある場合は、電話機の総数に必要なトランク数がニューヨークにだけオフィスがあったとした場合より少なくても、両方の都市にトランクが必要です。PSAP のアクセシビリティに基づいたトランクの要件について、緊急コール ネットワークのレイアウトを把握するサービス プロバイダーによる指示を受けることができます。

関連項目

- 「PSAP への接続に使用されるゲートウェイに対するコーリング サーチ スペースの設定」（P.3-18）

サービス プロバイダーからの DID 番号の入手

緊急応答ロケーション（ERL）の緊急ロケーション識別番号（ELIN）として使用するために、サービス プロバイダーからダイヤルイン（DID）番号を入手する必要があります。

一般に、ERL ごとに少なくとも 1 つの一意な番号が必要です。緊急コールは ERL の ELIN に基づいてローカル PSAP にルーティングされるため、一意の ELIN がないと、コールが正しくルーティングされません。また、ALI データベース プロバイダーによって、重複する ELIN が含まれている ALI が受け入れられない可能性があります。

ERL ごとに複数の ELIN が必要になることがあります。ERL に複数の電話機がある場合、短時間（3 時間未満）の間に ERL から複数の緊急コールが発信される可能性があります。ERL に ELIN を 1 つだけ割り当てると、各緊急コールにその ELIN が再利用されます。したがって、1 時間の間に 4 人が緊急コールを発信した場合、PSAP で ELIN をコールすると、最後の発信者に接続されます。PSAP でそれよりも前の発信者の 1 人に接続しようとする場合に、これが問題となることがあります。

ERL ごとに複数の ELIN を定義した場合、Emergency Responder では、すべての ELIN が使用されるまで順にそれらの ELIN を使用します。その後、それらの ELIN を順に再利用します。Emergency Responder では、ELIN 間のリンクと実際の緊急発信者の内線番号が最大 3 時間まで保持されます。

サービス プロバイダーからそれらの DID を購入する必要があるため、予算の必要性と正しい発信者に到達するために PSAP の機能を維持する必要性のバランスを取る必要があります。

（注） 取得する DID 数は、Emergency Responder で処理できる緊急コール数とは関係しません。Emergency Responder はユーザが定義した ELIN を再利用するため、すべての緊急コールが処理され、正しい PSAP にルーティングされます。ELIN の数が影響するのは、PSAP が目的の緊急の発信者にコールバックする成功率に対してだけです。

関連項目

- 「 •「ERL の作成」（P.4-33）」（P.3-10）
- 「ERL の作成」（P.4-33）

ALI 提出要件に関するサービス プロバイダーとの交渉

緊急コールは、緊急の発信者の緊急ロケーション識別番号（ELIN）に基づいて適切な PSAP にルーティングされます。緊急コールをルーティングするには、テレフォニー ネットワークで、それらの ELIN をロケーションにマップする自動ロケーション情報（ALI）が必要です。緊急コールの適切なルーティングに加え、ALI データベースによって、PSAP 画面に表示されるロケーション情報も提供され、発信者の特定に役立ちます。

Emergency Responder には、ALI を作成する機能と、サービス プロバイダーに受け入れ可能な各種形式で ALI をエクスポートする機能が含まれています。ERL/ALI 設定を作成した後、ALI データをエクスポートし、そのデータを ALI データベース プロバイダーに送信する必要があります。

データの送信方法は、ロケーション間またはサービス プロバイダー間で異なる場合があります。サービス プロバイダーと連携して、ALI データの提出に選択できるサービスを決定する必要があります。最低限でも、予測されるデータ形式と必要な転送方法を把握する必要があります。

Emergency Responder には、ALI を自動的に送信する機能は含まれていません。

ヒント　ご使用のネットワーク全体に Emergency Responder を配置する前に、サービス プロバイダーと一緒に ALI 提出プロセスをテストしてください。サービス プロバイダーと協力して、PSAP で ALI データを使用してご使用のネットワークに正常にコールバックできることをテストします。各サービス プロバイダーや ALI データベース プロバイダーの ALI 情報に関する規則は少し異なります。Emergency Responder では、一般的な NENA 標準に従って ALI データを作成できますが、ご使用のサービス プロバイダーまたはデータベース プロバイダーにはより厳しい規則があります。

関連項目

- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）
- 「ERL の作成」（P.4-33）
- 「ERL 情報のエクスポート」（P.4-41）

スイッチおよび電話機のアップグレード

Emergency Responder の最も強力な機能は、ご使用のネットワークで電話機の追加および移動を自動的に追跡できることです。ユーザが都市間で電話機を移動しても、この動的な機能により、緊急コールがローカル PSAP に確実にルーティングされます。これによって、移動、追加、または変更が簡素化され、電話ネットワークの維持コストを削減することができます。

ただし、Emergency Responder で電話機の移動を自動的に追跡できるのは、特定のタイプの電話機、および特定のタイプのスイッチ ポートに接続された電話機の場合だけです。これらの電話機およびスイッチのリストについては、「ネットワークのハードウェアおよびソフトウェアの要件」（P.1-4）を参照してください。

完全な自動化を実現するには、ご使用のスイッチをサポートされているモデルまたはソフトウェア バージョンにアップグレードするか、ご使用の電話機をサポートされているモデルと交換してください。

関連項目

- 「Cisco Emergency Responder のスイッチの設定」（P.4-44）
- 「電話機の管理」（P.4-54）

Cisco Emergency Responder 用のスタッフの準備

Emergency Responder は、既存の緊急手順に置き換わるものではありません。それよりむしろ、Emergency Responder はそれらの手順の強化に使用できるツールです。Emergency Responder を配置する前に、Emergency Responder をどのように手順に適合させるか、および Emergency Responder システムの機能をどのように使用するかを検討してください。

Emergency Responder をどのように使用するかを決定する際に検討する主な内容を次に示します。

- 誰かが緊急コールを発信すると、Emergency Responder によって、割り当てられたオンサイト アラート（セキュリティ）担当者（緊急応答チーム）に発信者のロケーションが通知されます。この情報の大部分は ERL 名です。緊急応答チームと協力して、緊急応答チームが緊急に対して迅速に応答するのに役立つ ERL 命名方法を策定することを検討してください。検討する内容の種類は、ビルの名前、階数、およびその名前に含まれている理解しやすいその他のロケーション情報です。
- Emergency Responder では 3 つのタイプの管理ユーザを定義できるため、Emergency Responder システム管理、ネットワーク管理、および ERL 管理全体の責任を分割できます。1 人でこれらの作業に必要なスキルおよび知識を持っていることはめったにありません。それらのスキルに従って Cisco ER 設定の責任を分割することを検討してください。
- 緊急コールのルーティングと正確な ALI の送信は、まさにサービス プロバイダーに提出する ALI 定義の信頼性とネットワーク トポロジの安定性を意味します。ERL 管理者が ALI データを最新の状態にしておく重要性を理解し、ネットワーク管理者が安定したネットワークを維持する重要性を理解していることを確認してください。データの整合性に関する詳細については、「データの整合性および信頼性に関する考慮事項」（P.1-18）を参照してください。

関連項目

- 「Cisco Emergency Responder のためのオンサイト アラート（セキュリティ）担当者の準備」（P.10-1）
- 「ERL 管理者のロールについて」（P.10-2）
- 「ネットワーク管理者のロールについて」（P.10-3）
- 「Cisco Emergency Responder システム管理者のロールについて」（P.10-4）

Cisco Emergency Responder の配置

次のトピックでは、さまざまなタイプのネットワークの配置モデルについて説明します。さらに大規模で複雑なネットワークを形成するために、次の例を組み合わせ、それらの例をモジュールとして使用できます。

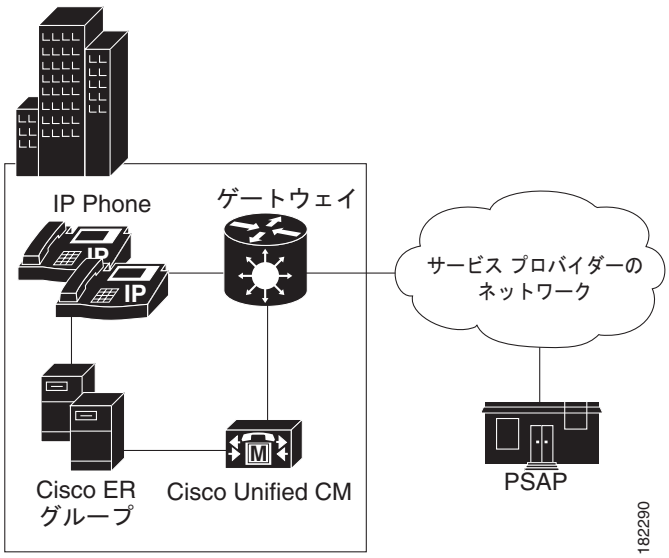
1 つの PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置

1 つの Cisco Unified Communications Manager クラスタで構成される単純なテレフォニー ネットワークをサポートするには、2 つの Emergency Responder サーバを設置し、1 つのサーバをパブリッシャとして、もう 1 つのサーバをそのパブリッシャを指すサブスクライバとして設定します。

ローカル PSAP が 1 つだけであるため、テレフォニー ネットワークのキャパシティ プランニングで複数のゲートウェイが必要になる可能性がある場合でも、サービス プロバイダーのネットワークへの必要なゲートウェイは 1 つだけです。このゲートウェイを使用するために、すべてのルート パターンを設定します。

図 1-4 は、1 つの Cisco Unified Communications Manager クラスタを含む単純なテレフォニー ネットワークに Emergency Responder を適合させる方法を示します。

図 1-4　1 つの PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置



これらの例をより複雑なネットワークに拡張するには、次の例を参照してください。

- 「2 つ以上の PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-26）
- 「サテライト オフィスがある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-27）
- 「2 つ以上のサイトをカバーする 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-29）
- 「2 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-31）

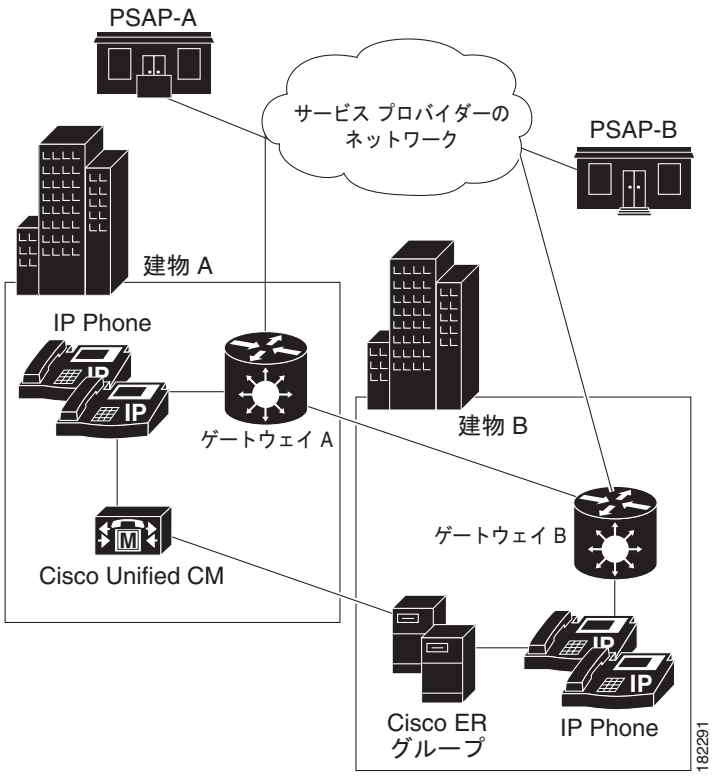
関連項目

- 「緊急コールの発信時に発生するプロセス」（P.1-9）
- 「Cisco Emergency Responder をご使用のネットワークに適合させる方法」（P.1-8）
- 「必要な Cisco Emergency Responder グループ数の決定」（P.1-17）
- 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）
- 「Cisco Emergency Responder 8.6 向けの Cisco Unified Communications Manager Versions 6.1 以降の設定」（P.3-1）

2 つ以上の PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置

図 1-5 は、2 つ以上の PSAP でカバーされている 1 つのメイン サイトを含む Emergency Responder の設定を示します。この例では、1 つの Cisco Unified Communications Manager クラスタがあることを前提とします。複数のクラスタがある場合、設定は論理的に「2 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-31）で説明されている設定と同じです。

図 1-5　2 つ以上の PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置



このタイプのネットワークをサポートするには、2 つの Cisco ER サーバを設置し、1 つをパブリッシャとして、もう 1 つをパブリッシャを指定するサブスクライバとして設定します。

ロケーションをカバーする PSAP が 2 つあるため、サービス プロバイダーのネットワークの別の部分に接続している複数のゲートウェイが必要になる場合があります。ただし、これは、サービス プロバイダーのネットワークのレイアウトによって決まります。つまり、PSAP が、緊急コールをインテリジェントに複数の PSAP にルーティングできる選択ルータに接続される場合、必要なゲートウェイが 1 つだけである可能性があります。サービス プロバイダーと話し合い、ビルの要件を決定します。この例では、2 つのゲートウェイが必要であることが前提です。当然ながら、ご使用のテレフォニー ネットワークのキャパシティ プランニングでは、各リンクに複数のゲートウェイが必要な場合があります。

ゲートウェイを設定してサービス プロバイダーのネットワークに正しく接続した後、ゲートウェイ A を使用するためにビル A の ERL で使用されるすべてのルート パターンを設定し、ゲートウェイ B を使用するためにビル B の ERL で使用されるすべてのルート パターンを設定します。ビル間で電話機を移動すると、Cisco ER によって、それらの ERL が動的に更新され、緊急コールが目的のゲートウェイからルーティングされるようになります。

これらの例を他のネットワークに拡張するには、次の例を参照してください。

- 「1 つの PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-24）
- 「サテライト オフィスがある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-27）
- 「2 つ以上のサイトをカバーする 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-29）
- 「2 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-31）

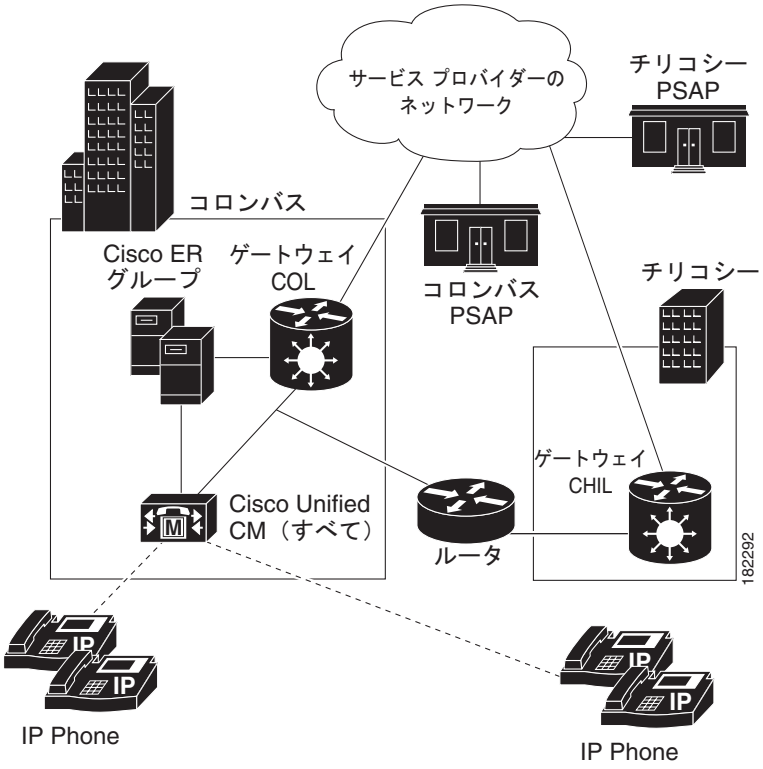
関連項目

- 「緊急コールの発信時に発生するプロセス」（P.1-9）
- 「Cisco Emergency Responder をご使用のネットワークに適合させる方法」（P.1-8）
- 「必要な Cisco Emergency Responder グループ数の決定」（P.1-17）
- 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）
- 「Cisco Emergency Responder 8.6 向けの Cisco Unified Communications Manager Versions 6.1 以降の設定」（P.3-1）

サテライト オフィスがある 1 つのメイン サイトでの Cisco Emergency Responder の配置

図 1-6 は、1 つのメイン サイトで 1 つ以上のサテライト オフィスをカバーしている場合、つまり、サテライト オフィス内の電話機がメイン サイト上の Cisco Unified Communications Manager クラスタから稼動されている場合の Emergency Responder 設定を示します。サテライト オフィスに独自の Cisco Unified Communications Manager クラスタがある場合には、「2 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-31）を参照してください。

図 1-6　サテライト オフィスがある 1 つのメイン サイトでの Cisco Emergency Responder の配置



注意　この設定では、オフィス間の WAN リンクが故障した場合、サテライト オフィスにいる人々は Emergency Responder のサポートを使用して緊急コールを発信できません。WAN が故障した場合には、サテライト オフィスの SRST によって、緊急コールの基本的なサポートが提供されます。

このタイプのネットワークをサポートするには、2 つの Cisco ER サーバを設置し、1 つをパブリッシャとして、もう 1 つをパブリッシャを指定するサブスクライバとして設定します。両方のサーバをメイン オフィスに設置します。

ほとんどの場合、メイン オフィス（コロンバス）とサテライト オフィス（チリコシー）をカバーする個別の PSAP があります。したがって、サービス プロバイダーのネットワークの別の部分（サービス プロバイダーが異なることもあります）に接続している複数のゲートウェイが必要になる場合があります。ただし、これは、サービス プロバイダーのネットワークのレイアウトによって決まります。つまり、PSAP に共有スイッチを使用する場合、必要なゲートウェイが 1 つだけである可能性があります。サービス プロバイダーと話し合い、ビルの要件を決定します。この例では、2 つのゲートウェイが必要であることが前提です。当然ながら、ご使用のテレフォニー ネットワークのキャパシティ プランニングでは、各リンクに複数のゲートウェイが必要な場合があります。

ゲートウェイを設定してサービス プロバイダーのネットワークに正しく接続した後、ゲートウェイ COL を使用するためにコロンバスの ERL で使用されるすべてのルート パターンを設定し、ゲートウェイ CHIL を使用するためにチリコシーの ERL で使用されるすべてのルート パターンを設定します。サイト間で電話機を移動すると、Cisco ER によって、それらの ERL が動的に更新され、緊急コールが目的のゲートウェイからルーティングされるようになります。

また、SNMP のパフォーマンスを WAN リンクのアカウントに合わせなければならない場合があります。Cisco ER では、そこで電話機の移動を追跡するためにリモート サイトのスイッチの SNMP クエリーを実行する必要があります。SNMP クエリーを正常に実行するために十分な時間がない、または再試行できない場合には、SNMP タイムアウトの問題が発生する可能性があります。詳細については、「SNMP 接続の設定」（P.4-45）を参照してください。

これらの例を他のネットワークに拡張するには、次の例を参照してください。

- 「1 つの PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-24）
- 「2 つ以上の PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-26）
- 「2 つ以上のサイトをカバーする 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-29）
- 「2 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-31）

ヒント　サテライト オフィスの規模が小さく（電話機 50 台未満）、Survivable Remote Site Telephony（SRST）を使用している場合、メイン オフィスの Cisco ER ではなく、ローカル PSAP に対して CAMA トランクが設定されている FXO ポートに 911 コールを送信するようにリモート オフィスにゲートウェイを設定することで、緊急コールの直接サポートが容易になる可能性があります。

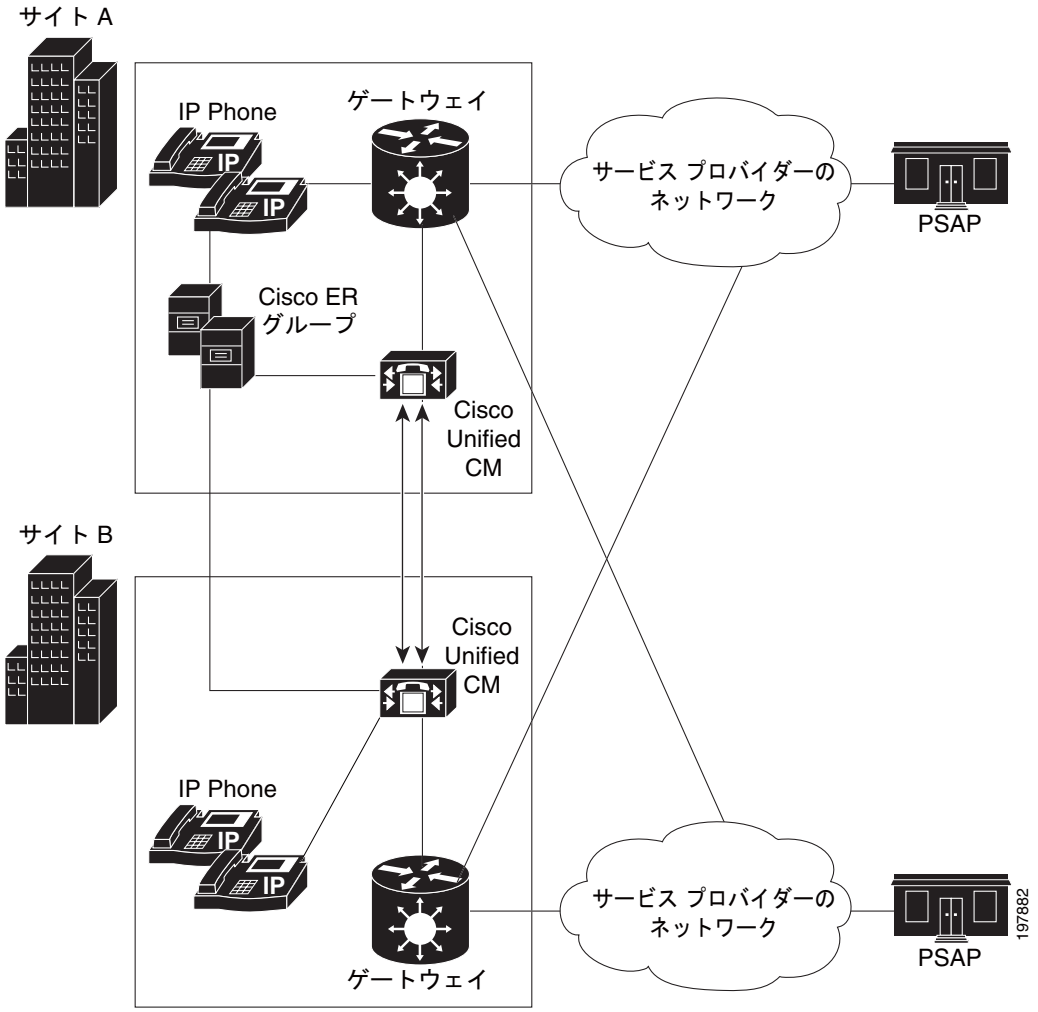
関連項目

- 「緊急コールの発信時に発生するプロセス」（P.1-9）
- 「Cisco Emergency Responder をご使用のネットワークに適合させる方法」（P.1-8）
- 「必要な Cisco Emergency Responder グループ数の決定」（P.1-17）
- 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）
- 「Cisco Emergency Responder 8.6 向けの Cisco Unified Communications Manager Versions 6.1 以降の設定」（P.3-1）

2 つ以上のサイトをカバーする 1 つのメイン サイトでの Cisco Emergency Responder の配置

図 1-7 は、2 つ以上のメイン サイトが 2 つ以上の PSAP でカバーされており、さらにサイトごとに 1 つの Cisco Unified CM クラスタがある場合の Emergency Responder 設定を示します。

図 1-7　2 つ以上のサイトをカバーする 1 つのメイン サイトでの Emergency Responder の配置



このタイプのネットワークをサポートするには、2 つの Emergency Responder サーバを設置し、1 つのサーバをパブリッシャとして、もう 1 つのサーバをそのパブリッシャを指すサブスクライバとして設定します。

ロケーションをカバーする PSAP が 2 つあるため、サービス プロバイダーのネットワークの別の部分に接続している複数のゲートウェイが必要になる場合があります。ただし、これは、サービス プロバイダーのネットワークのレイアウトによって決まります。つまり、PSAP が、緊急コールをインテリジェントに複数の PSAP にルーティングできる選択ルータに接続される場合、必要なゲートウェイが 1 つだけである可能性があります。サービス プロバイダーと話し合い、ビルの要件を決定します。この例では、サイトごとに 1 つのゲートウェイが必要であることが前提です。当然ながら、ご使用のテレフォニー ネットワークのキャパシティ プランニングでは、各リンクに複数のゲートウェイが必要な場合があります。

ゲートウェイを設定してサービス プロバイダーのネットワークに正しく接続した後、ローカル サイトのゲートウェイを使用するために、サイト A の ERL で使用されるすべてのルート パターンとサイト B の ERL で使用されるすべてのルート パターンを設定します。ビル間で電話機を移動すると、Emergency Responder によって、それらの ERL が動的に更新され、緊急コールが目的のゲートウェイからルーティングされるようになります。

この例では、Emergency Responder が 2 つの Cisco Unified CM クラスタをカバーすることにより、サイト間の電話機の移動が容易になります。サイト A とサイト B の両方の Cisco Unified CM クラスタで、サイト A の ERL とサイト B の ERL のルート パターンを設定する必要があります。

EMCC を使用する 2 つ以上のサイトをカバーする 1 つのサイトでの Emergency Responder

2 つの Cisco Unified CM クラスタ間で Extension Mobility Cross Cluster（EMCC）を使用すると、Emergency Responder で 911 コールの拡張サポートを提供できるようになります。

図 1-7 は、Emergency Responder が 1 つのサイトに配置され、各サイトに Cisco Unified CM が存在する 2 つ以上のサイトをカバーしているようすを示します。

このシナリオでは、Emergency Responder サーバは EMCC ユーザのホーム クラスタと Cisco Unified CM の Visiting クラスタの両方で共有されます。Emergency Responder で処理する場合、911 コールが EMCC にログインしたユーザによって発信されても、Cisco Unified CM ホーム クラスタでは、911 コールをユーザの Visiting クラスタに転送するために付属コーリング サーチ スペース（CSS）を使用できません。

その代わりに、両方のクラスタをサポートしている共有 Emergency Responder サーバによって、ユーザのホーム クラスタにある 911 コールが処理されます。

これらの例を他のネットワークに拡張するには、次の例を参照してください。

- 「1 つの PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-24）
- 「2 つ以上の PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-26）
- 「サテライト オフィスがある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-27）
- 「2 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-31）

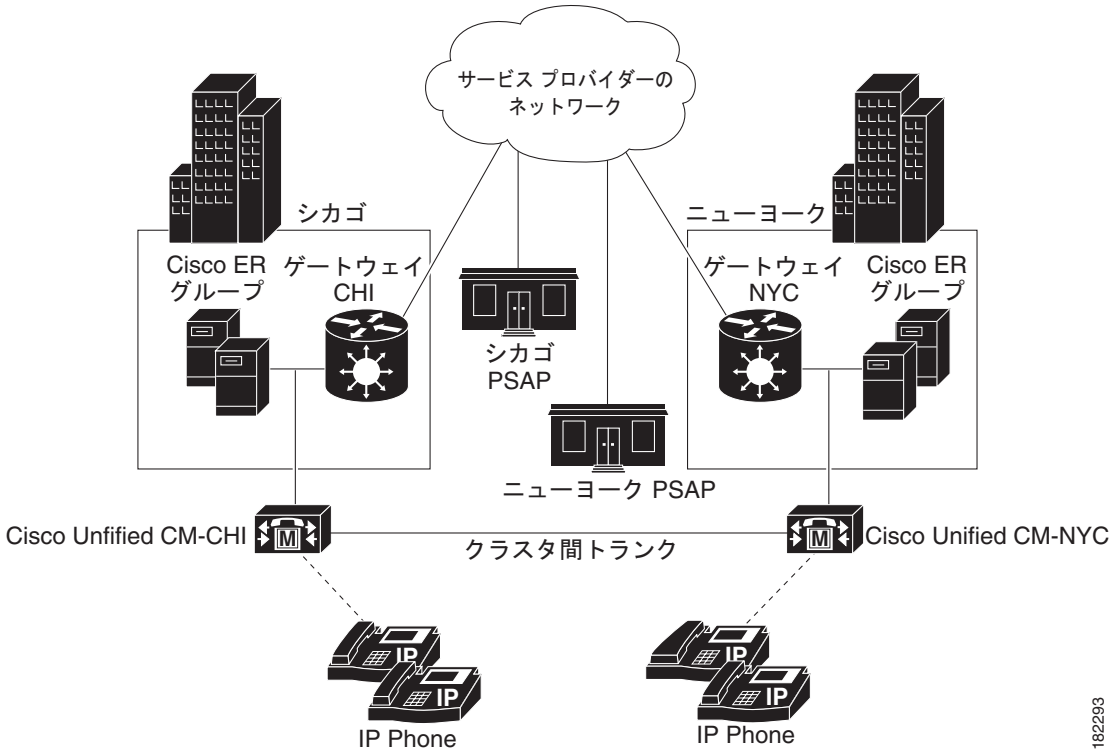
関連項目

- 「緊急コールの発信時に発生するプロセス」（P.1-9）
- 「Cisco Emergency Responder をご使用のネットワークに適合させる方法」（P.1-8）
- 「必要な Cisco Emergency Responder グループ数の決定」（P.1-17）
- 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）
- 「Cisco Emergency Responder 8.6 向けの Cisco Unified Communications Manager Versions 6.1 以降の設定」（P.3-1）

2 つのメイン サイトでの Cisco Emergency Responder の配置

図 1-8 は、それぞれが個別の PSAP でカバーされている 2 つ（以上）のメイン サイトを含む Emergency Responder の設定を示します。

図 1-8　2 つのメイン サイトでの Cisco Emergency Responder の配置



この例の説明と次の例を組み合わせることで、この例をより複雑な設定に適用させることができます。

- 一部のメイン サイトにサテライト オフィスがある場合のそれらのオフィスでの Cisco ER の配置については、「サテライト オフィスがある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-27）を参照してください。

1 つのメイン サイトが複数の PSAP でカバーされている場合のそのサイトでの Cisco ER の配置については、「2 つ以上の PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-26）を参照してください。このタイプのネットワークをサポートするには、

- シカゴに 2 つの Cisco ER サーバを設置し、1 つのサーバをパブリッシャとして、もう 1 つのサーバをパブリッシャを指定するサブスクライバとして設定します。設置後、クラスタ データベースとして使用するためにシカゴの Cisco ER グループにある Cisco ER パブリッシャ サーバを選択します。「8.6 Cisco Emergency Responder クラスタおよびクラスタ DB ホスト」（P.4-28）を参照してください。
- ニューヨークに 2 つの Cisco ER サーバを設置し、1 つのサーバをパブリッシャとして、もう 1 つのサーバをパブリッシャを指定するサブスクライバとして設定します。設置後、クラスタ データベースとして使用するためにシカゴの Cisco ER グループにある Cisco ER パブリッシャ サーバを選択します。「8.6 Cisco Emergency Responder クラスタおよびクラスタ DB ホスト」（P.4-28）を参照してください。

ほとんどの場合、メイン オフィスをカバーする個別の PSAP があります。この例では、シカゴとニューヨークで異なる PSAP を使用します。サービス プロバイダーのネットワークの別の部分（サービス プロバイダーが異なることもあります）に接続するには、シカゴとニューヨークにそれぞれ、少なくとも 1 つのゲートウェイが必要です。サービス プロバイダーと話し合い、ビルの要件を決定します。当然ながら、ご使用のテレフォニー ネットワークのキャパシティ プランニングでは、各サイトに複数のゲートウェイが必要な場合があります。

ゲートウェイを設定してサービス プロバイダーのネットワークに正しく接続した後、ゲートウェイ CHI を使用するためにシカゴの ERL で使用されるすべてのルート パターンを設定し、ゲートウェイ NYC を使用するためにニューヨークの ERL で使用されるすべてのルート パターンを設定します。

シカゴとニューヨーク間で電話機の移動を可能にするには、Cisco ER で個別の Cisco ER グループがある Cisco Unified Communications Manager クラスタ間のコール転送を行うことができるように、クラスタ間トランクを設定して Cisco Unified Communications Manager クラスタをリンクし、Cisco ER グループ間のルート パターンを作成する必要もあります。この状況において Cisco ER で電話機の移動を処理する方法の詳細については、「Cisco Emergency Responder グループ間の通信に対するルート パターンの作成」（P.3-19）を参照してください。

サイト間で電話機を移動すると、Cisco ER によって、それらの ERL が動的に更新され、緊急コールが目的のゲートウェイからルーティングされるようになります。ただし、WAN リンクを使用不能になった場合、Cisco ER でサイト間の電話機の移動を追跡できません。

EMCC を使用した 2 つのメイン サイトでの Emergency Responder クラスタとしての Cisco Emergency Responder の配置

2 つの Cisco Unified CM クラスタ間で Extension Mobility Cross Cluster（EMCC）を使用した場合、Emergency Responder は 911 コールの拡張サポートを提供できます。

図 1-8 は、それぞれが個別の PSAP でカバーされている 2 つ（以上）のメイン サイトを含む Emergency Responder の設定を示します。

このシナリオでは、EMCC に 2 つのクラスタを設定する必要があります。911 コールが EMCC にログインしたユーザによって発信されると、そのコールは、そのユーザのホーム クラスタにある Emergency Responder グループに転送されます。

ユーザのホーム クラスタおよび Visiting クラスタにある Emergency Responder グループは、Emergency Responder クラスタを形成します。ホーム クラスタにある Emergency Responder グループによって、コールが 2 つの Cisco Unified CM クラスタ間のクラスタ内トランク（ICT）を経由して Visiting の Emergency Responder グループにリダイレクトされ、Visiting の Emergency Responder によって、そのコールが適切な PSAP にルーティングされます。

（注）　このシナリオでは、Cisco Unified CM に付属 CSS は設定されていません。

これらの例を他のネットワークに拡張するには、次の例を参照してください。

- 「1 つの PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-24）
- 「2 つ以上の PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-26）
- 「サテライト オフィスがある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-27）
- 「2 つ以上のサイトをカバーする 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-29）

関連項目

- 「緊急コールの発信時に発生するプロセス」（P.1-9）
- 「Cisco Emergency Responder をご使用のネットワークに適合させる方法」（P.1-8）
- 「必要な Cisco Emergency Responder グループ数の決定」（P.1-17）
- 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）

- 「Cisco Emergency Responder 8.6 向けの Cisco Unified Communications Manager Versions 6.1 以降の設定」（P.3-1）

付属 CSS 設定を使用した 2 つのメイン サイトでの Emergency Responder クラスタとしての Cisco Emergency Responder の配置

2 つの Cisco Unified CM クラスタ間で Extension Mobility Cross Cluster（EMCC）を使用した場合、Emergency Responder は 911 コールの拡張サポートを提供できます。

図 1-8 は、それぞれが個別の PSAP でカバーされている 2 つ（以上）のメイン サイトを含む Emergency Responder の設定を示します。

このシナリオでは、EMCC に 2 つのクラスタが設定されます。2 つの Cisco Unified CM クラスタには、さまざまな緊急パターンがあるため、付属 CSS を設定する必要があります。緊急コールが EMCC にログインしたユーザによって発信されると、そのコールはホーム クラスタから Cisco Unified CM の Visiting クラスタにリダイレクトされた後、そのユーザの Visiting クラスタにある Emergency Responder グループに転送されます。

ユーザの Visiting クラスタにある Visitng の Emergency Responder グループによって、コールが適切な PSAP にルーティングされます。

（注）　ホーム クラスタと Visiting クラスタで同じ緊急パターンを共有しない場合、Cisco Unified CM クラスタに付属 CSS を設定しておく必要があります。ホーム クラスタと Visiting クラスタで同じ緊急パターンを共通する場合には、付属 CSS を設定せずに前の使用例を使用できます。

これらの例を他のネットワークに拡張するには、次の例を参照してください。

- 「1 つの PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-24）
- 「2 つ以上の PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-26）
- 「サテライト オフィスがある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-27）
- 「2 つ以上のサイトをカバーする 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-29）

関連項目

- 「緊急コールの発信時に発生するプロセス」（P.1-9）
- 「Cisco Emergency Responder をご使用のネットワークに適合させる方法」（P.1-8）
- 「必要な Cisco Emergency Responder グループ数の決定」（P.1-17）
- 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）
- 「Cisco Emergency Responder 8.6 向けの Cisco Unified Communications Manager Versions 6.1 以降の設定」（P.3-1）

ワイドエリア ネットワーク配置でのローカル ルート グループの設定

ワイドエリア ネットワーク（WAN）を経由して複数のロケーションにまたがって Emergency Responder と Cisco Unified Communications Manager を配置する場合は、Emergency Responder と Cisco Unified Communications Manager の間の接続が故障した状況でもユーザが緊急コールを発信できるように、ローカル ルート グループ（LRG）を設定することを推奨します。

LRG を設定するには、次の手順を実行します。

1. Cisco Unified Communications Manager Administration で、911 緊急コール ルーティング用に LRG のルート パターンおよびルート ポイントを設定します。
2. Cisco Unified Communications Manager Administration で、LRG のルート パターンを使用して緊急コールのルート ポイントで転送されている接続先のルート ポイントを設定します。
3. Emergency Responder Administration で、LRG のルート パターンをデフォルト ERL として設定します。

Emergency Responder と Cisco Unified Communications Manager の間に通信障害が発生している間、次の Emergency Responder 機能はサポートされません。

- オンサイト アラート
- Web アラート
- 電子メール アラート
- PSAP コールバック
- デバイス モビリティ。

  デバイス モビリティをサポートするには、あるロケーションから別のロケーションに電話機を移動する際に 911 コールが新しい LRG ロケーションにルーティングされるように Cisco Unified Communications Manager でデバイス モビリティを設定する必要があります。

関連項目

- 「緊急コールの発信時に発生するプロセス」（P.1-9）
- 「Cisco Emergency Responder をご使用のネットワークに適合させる方法」（P.1-8）
- 「必要な Cisco Emergency Responder グループ数の決定」（P.1-17）
- 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）
- 「Cisco Emergency Responder 8.6 向けの Cisco Unified Communications Manager Versions 6.1 以降の設定」（P.3-1）

CHAPTER 2

Cisco Emergency Responder 8.6 のインストール

Cisco Emergency Responder（Emergency Responder）は、Cisco Unified Communications Operating System ソフトウェアを含む、Emergency Responder 8.6 をインストールするために必要なすべてが含まれたインストール用 DVD で配布されます。

Emergency Responder 8.6 には、Emergency Responder 7.1 または Emergency Responder 8.0 からアップグレードできます。これ以外のバージョンの Emergency Responder（Emergency Responder 1.x、Emergency Responder 2.x、Emergency Responder 7.0 など）からは、Emergency Responder 8.6 に直接アップグレードすることはできません。

次のトピックでは、Cisco ER のハードウェア要件、ソフトウェア要件、およびアップグレード手順について説明します。

（注） Emergency Responder には Cisco Unified Communications Manager 8.6（Cisco Unified CM 8.6）との互換性があります。すべての機能を保証するため、Cisco Unified CM 8.6 にアップグレードすることをお勧めします。

ハードウェアおよびソフトウェア要件

Cisco ER を適切に実行するには、特定のハードウェアおよびソフトウェアが必要です。Emergency Responder 8.6 のインストールまたはアップグレードを続行する前に、次の項を参照してください。

- 『*Release Notes for Cisco Emergency Responder 8.6*』を参照して、Emergency Responder をインストールために必要なすべてのハードウェアおよびサポートされているバージョンのソフトウェアがあるか検証し、Cisco MCS Unified Communications Manager Appliance プラットフォームに、必要とする設定を満たす Emergency Responder 機能が用意されているか確認してください。（また、シスコが認定する同等のサーバを使用することもできます）。
- 「ライセンス要件の決定」（P.1-6）を参照して、インストール処理を開始する前に、必要なライセンス キーがすべて使用できることを確認してください。

インストールまたはアップグレードの前に

Emergency Responder 8.6 のインストール プロセスでは、プラットフォーム ソフトウェアと Emergency Responder 8.6 ソフトウェアの両方がインストールされます。インストール中には、インストールを完了するためにシステムで必要な情報の入力を求めるプロンプトが表示されます。

（注）　インストールまたはアップグレードは、オフピーク時間中に実行することをお勧めします。インストールおよびアップグレード手順により、ハード ディスクが完全に再フォーマットされます。したがって、インストールまたはアップグレード中は、Emergency Responder 8.6 を使用できません。

システムに Emergency Responder 8.6 をインストールまたはアップグレードする前に、次の情報を確認してください。

- Emergency Responder 8.6 へのアップグレード：
  - Emergency Responder 8.6 にアップグレードする前に、既存のバージョンの Cisco Unified CM との互換性があることを確認する必要があります。Cisco Unified Communications Compatibility Tool を使用して、この問題を調べることができます。http://tools.cisco.com/ITDIT/vtgsca/VTGServlet
  - Cisco Unified CM をアップグレードする前に、Emergency Responder をアップグレードする必要があります。新しいバージョンの Emergency Responder をインストールした後にのみ、Cisco Unified CM をアップグレードできます。
  - Emergency Responder と Cisco Unified CM の両方をアップグレードしたら、Emergency Responder 上で Cisco Unified CM のバージョンを更新する必要があります。
  - アップグレードの正しい順序およびこの内容に関する追加情報については、表 2-1 を参照してください。
- Emergency Responder のバージョン：
  - 別のバージョンの Emergency Responder を同じ Emergency Responder グループ内に配置することはできません。プライマリ Emergency Responder サーバとスタンバイ Emergency Responder サーバで同じバージョンの Emergency Responder を実行する必要があります。Emergency Responder 8.6 にアップグレードする場合は、両方の Emergency Responder サーバをバージョン 8.6 にアップグレードしてください。

（注）　Emergency Responder 8.6 では、異なるバージョンの Emergency Responder を実行している 2 つのサーバ グループ間での相互運用性がサポートされます。クラスタの 1 つのサーバ グループで Emergency Responder 8.6 を実行し、もう 1 つのサーバ グループで Emergency Responder 1.3、Emergency Responder 2.0.x、Emergency Responder 7.x、および Emergency Responder 8.0 を実行することができます。ただし、Emergency Responder 8.6 には、Emergency Responder 1.3 以前のバージョンとの相互運用性はありません。

- Emergency Responder のホスト名とパスワードを決め、リストを作成します。
  - Emergency Responder をインストールする前に、Emergency Responder サーバでずっと使用するホスト名、ユーザ インターフェイス管理者名およびパスワードを決定します。インストール後に Emergency Responder サーバのホスト名を変更すると、問題が発生する場合があります。
  - Emergency Responder 8.6 の Publisher および Subscriber のホスト名には、アンダースコア文字（_）を使用しないでください。既存の Emergency Responder サーバで、ホスト名にアンダースコアを使用している場合は、Emergency Responder 8.6 をインストールする前にホスト名を変更してください。

– Cisco ER 管理ユーザのパスワードを決定します。

（注）　Emergency Responder 管理ユーザのパスワードは、長さ 6 文字以上にしてください。パスワードには英数字、ハイフン、アンダースコアを使用できます。また、英数字から始まるパスワードにしてください。

- イーサネット NIC 速度とデュプレックス モード
  - イーサネット NIC 速度およびデュプレックスのオートネゴシエーションをイネーブルにするかどうかを決定します。
  - する場合、追加の情報は必要ありません。
  - イネーブルにしない場合は、使用するイーサネット NIC 速度およびデュプレックス モードを決定します。
- DHCP の設定
  - IP アドレスの割り当てにダイナミック ホスト コンフィギュレーション プロトコル（DHCP）を使用するかどうかを決定します。
  - する場合、追加の情報は必要ありません。
  - 使用しない場合は、[Static Network Configuration] で入力するホスト名、IP アドレス、IP マスク、およびゲートウェイ アドレスが必要になります。
- NTP クライアントの情報
  - 外部ネットワーク タイム プロトコル（NTP）サーバの設定を求めるプロンプトが表示されます。システム時刻を正確に保つため、外部 NTP サーバを使用することをお勧めします。
  - 外部 NTP サーバを使用する場合は、サーバの IP アドレスまたはホスト名を入力する必要があります。
  - 外部 NTP サーバを使用しない場合は、システムの日付と時刻の情報を手動で入力する必要があります。

（注）　UCS サーバに Emergency Responder 8.6 をインストールする場合は、NTP サーバの使用が必須です。

- Database Access Security パスワードを決定します
  - servergroup のノードが通信できるようにするには、データベース アクセス セキュリティ パスワードが必要です。パスワードは、servergroup のすべてのノードで共有されます。
  - パスワードは、長さ 6 文字以上にしてください。パスワードには英数字、ハイフン、アンダースコアを使用できます。また、英数字から始まるパスワードにしてください。
- SMTP ホストの設定（任意）
  - SMTP ホストを使用するかどうかを決定します。
  - 使用する場合は、SMTP ホストのホスト名または IP アドレスを決めます。
- 警告：
  - インストールの前に、次の URL にある Emergency Responder 8.6 のリリース ノートを参照してください。

    http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_release_notes_list.html

表 2-2 に示す順序で、Emergency Responder 8.6 のコンポーネントをインストールしてください。

表 2-1　アップグレード作業

インストール作業	参照先
Emergency Responder 8.6 のアップグレード	「ソフトウェア アップグレードの実行」（P.7-19）
Unified CM のアップグレード	「Cisco Unified Communications Manager のバージョンの変更」（P.9-1）
Cisco Unified CM のバージョンの更新	「Cisco Unified CM のバージョンの更新」（P.E-1）

表 2-2　インストール作業

インストール作業	参照先
Cisco Unified Communications Manager のインストール	http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
新規インストールとしての Emergency Responder 8.6 のインストール	「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）

Cisco UCS サーバの Cisco Emergency Responder のインストールおよび移行

次の項では、Cisco UCS サーバの Cisco Emergency Responder のインストール、アップグレード、および移行に関する変更について説明します。

- 「システム要件」（P.2-4）
- 「Cisco UCS サーバへの Cisco Emergency Responder のインストール」（P.2-5）
- 「Cisco UCS サーバの Cisco Emergency Responder のライセンス」（P.2-10）
- 「Cisco UCS サーバの Cisco Emergency Responder への移行」（P.2-11）
- 「VMware のサポート」（P.2-12）
- 「Cisco UCS サーバの Cisco Emergency Responder の日常業務の実行」（P.2-13）

システム要件

Cisco UCS サーバで Cisco Emergency Responder を実行するには、システムが**表 2-3（P.2-4）**で示している要件を満たしている必要があります。

表 2-3　システム要件

システム パラメータ	システム パラメータのオプション
Supported Virtual Machine Configuration	次の URL にあるドキュメントを参照 http://www.cisco.com/go/uc-virtualized
IOPS per virtual machine (VM)	次の URL にあるドキュメントを参照 http://www.cisco.com/go/uc-virtualized

表 2-3　システム要件（続き）

システム パラメータ	システム パラメータのオプション
VMware version	ESXi 4.0 Update 1 （注）　ESX ではなく、ESXi を使用して Cisco UCS サーバ上で Cisco Emergency Responder を実行していることを確認してください。ただし、サーバを ESX ホストを含む VMware vCenter の一部にすることはできます。
VMware—vMotion	No （注）　シスコでは、実行中の VM 上での vMotion はサポートされません。ただし、VM の電源を切断し、異なるラック サーバで VM をリブートした場合は、サポートされます。ラック サーバをメンテナンス モードに設定する場合、これが役立つことがあります。
VMware—Site Recovery Manager	Yes
VMware—High Availability	Yes
VMware—Data Recovery (VDR)	Yes
リストに含まれていない他のすべての VMware 機能	サポートなし

Cisco Emergency Responder を Cisco UCS サーバで正常に動作させるには、VMware ESXi を実行しているホスト サーバ管理の経験とスキルが必要です。この経験がなく、必要な情報をすぐに取得したい場合は、VMware を簡単に動かせる Web ベースのアプリケーションである VMware GO の使用を検討してください。

（注）　VMware GO を使用する場合でも、Cisco UCS サーバの Cisco Emergency Responder でサポートする VMware 設定が必要です。この設定については、http://www.cisco.com/go/swonly および http://www.cisco.com/go/uc-virtualized で説明しています。

Cisco UCS サーバへの Cisco Emergency Responder のインストール

次の項では、Cisco UCS サーバへの Cisco Emergency Responder の新規インストールを実行する方法について説明します。

サーバのインストールおよび設定に関する設定チェックリスト

表 2-4（P.2-6）に、Cisco Emergency Responder を Cisco UCS サーバにインストールして設定するために必要な、主な手順のチェックリストを示します。

表 2-4　サーバのインストールおよび設定に関する設定チェックリスト

	設定手順	関連資料
ステップ 1	サーバの設置を準備します。	*「設置の準備」（P.2-7）*
ステップ 2	サーバを物理的に設置し、接続します。	—
ステップ 3	サーバで電源を投入し、リモート管理用の Cisco Integrated Management Controller（CIMC）の設定を行います。	—
ステップ 4	UCS サーバを別に購入した場合、RAID 設定の仕様を次のように設定します。 • 最初の 2 つのドライブは、RAID 1（ミラー化）ドライブとして設定されます。このドライブは、ESXi のインストール用です。 • 次の 4 つのドライブは、RAID 5 ドライブとして設定されます。このドライブは VM 用です。 **（注）** ドライブの数は、UCS サーバの各バージョンによって異なる場合があります。	*「RAID の設定」（P.2-7）*
ステップ 5	UCS サーバを別に購入した場合、BIOS の仕様を次のように設定します。 • Quiet モードを無効にします。 • CDROM アクセスの拡張 SATA を有効にします。 • 次のブート順序を設定します。 – 1 番目に SATA5:Optiarc DVD – 2 番目に PCI RAID アダプタ	—
ステップ 6	2 台の使用可能なディスクのより小さい方（約 130 GB）に VMware EXSi 4.0.0 Update 1 をインストールし、設定します。	VMware ESXi の資料
ステップ 7	vSphere クライアントをインストールします。	「vSphere クライアントのインストール」（P.2-8） vSphere Client の資料
ステップ 8	VM のデータストアをアラインします。	「VM に使用されるデータストアのアライン」（P.2-8）
ステップ 9	802.1q トランキングを使用する場合、MTU サイズを 1472 に設定します。	—

表 2-4　サーバのインストールおよび設定に関する設定チェックリスト（続き）

	設定手順	関連資料
ステップ 10	仮想マシン（VM）をインストールし、設定します。	「仮想マシンの作成」（P.2-9） 「仮想マシン テンプレート（OVA テンプレート）のダウンロード」（P.2-9）
ステップ 11	VM に Cisco Emergency Responder をインストールします。	「Cisco Emergency Responder の VM へのインストール」（P.2-10）

設置の準備

この項では、スタンドアロン構成（つまり、データセンターにはない状態）での、Cisco UCS サーバへの Cisco Emergency Responder のインストールを準備する方法について説明します。

設置前に、次のリソースを確保する必要があります。

- 2 RU の UCS サーバを設置するラック内のスペース
- 次のような、UCS サーバに近いスイッチ上のイーサネット ポート：
  - 1 つのポートは CIMC 用。
  - 2 つのポートは LAN on motherboard（LOM）NIC 用。
- CIMC 管理ポートの IP アドレス。
- 仮想ホストの IP アドレス。これは、UCS サーバの IP アドレスで、ESXi によって使用されます。
- ホスト名と、仮想ホストのホスト名で任意に設定する DNS
- VM の IP アドレス。

RAID の設定

UCS サーバを別に購入した場合、RAID 設定の仕様を次のように設定します。

- 最初の 2 つのドライブは、RAID 1（ミラー化）ドライブとして設定されます。このドライブは、ESXi のインストール用です。
- 次の 4 つのドライブは、RAID 5 ドライブとして設定されます。このドライブは VM 用です。

（注）　ドライブの数は、UCS サーバの各バージョンによって異なる場合があります。

次の手順に従って、この作業を実行します。

ステップ 1　サーバのブート中に、Ctrl+Y を押し、プリブート CLI を開始します。

ステップ 2　次のコマンドを入力し、現在の RAID 設定を特定します。

-ldinfo -l0 -a0

-ldinfo -l1 -a0

必要な設定は、論理ドライブ 0 の RAID 1 アレイに 2 つのドライブ、論理ドライブ 1 の RAID 5 アレイに 4 つのドライブがある設定です。

RAID 設定が誤っている場合は、この手順を続行します。

（注）　RAID が正しく設定されている場合は、この手順は続行しないでください。

ステップ 3　**-cfgclr -a0** コマンドを入力して、RAID 設定をクリアします。

注意　RAID 設定をクリアすると、ハード ドライブ上のすべてのデータが削除されます。

ステップ 4　次のコマンドを入力して、RAID を設定します。

-cfgldadd -r1 [252:0, 252:1] -a0

-cfgldadd -r5 [252:2, 252:3, 252:4, 252:5] -a0

以前、ハード ドライブに RAID 設定がなかった場合は、RAID を設定したことになります。

ハード ドライブに RAID 設定がすでにあった場合は、この手順を続けてください。

ステップ 5　次のコマンドを入力して、論理ボリュームを初期化します。

-ldinit -start -full -l0 -a0（l0 は、文字の l と番号の 0 で、番号の 10 ではありません）

-ldinit -start -full -l1 -a0（l1 は、文字の l と番号の 1 で、番号の 11 ではありません）

これによって、ドライブ上のデータがクリアされ、新しいアレイが初期化されます。

ステップ 6　プリブート CLI を終了する前に、これらのコマンドの実行を終了できるようにします。次のコマンドを入力して、コマンドの進行状況を表示します。

-ldinit -showprog -l0 -a0

-ldinit -showprog -l1 -a0

両方のコマンドによって、初期化が実行されていないことがレポートされた場合、プリブート CLI を安全に終了できます。

ステップ 7　2 つの論理ボリュームを設定後、**q** を入力すると、プリブート CLI を終了できます。

vSphere クライアントのインストール

ネットワーク上で仮想ホストが使用可能な場合、その IP アドレスにアクセスして、Web ベース インターフェイスを開始できます。vSphere クライアントは Windows ベースのため、Windows PC からダウンロードとインストールを実行する必要があります。

vSphere クライアントがインストールされると、設定した仮想ホストの名前または IP アドレス、root ログイン ID、およびパスワードを使用して実行し、ログインできます。

vCenter を使って管理する場合、ホストを vCenter に結合できます。

VM に使用されるデータストアのアライン

VMWare ESXi をインストールするとき、2 つ目の論理ボリュームはアラインされない状態で自動的にインポートされます。VM では、すべてのパーティション（物理、ESXi、および VM）が同じバウンダリで開始されると、より優れたディスク パフォーマンスが得られます。

これによって、異なるバウンダリ間でディスク ブロックが断片化することを防ぐことができます。

VM に使用される ESXi パーティションがアラインされるようにするには、アラインされていないデータストア（より大きなディスク パーティション（407 GB））を削除し、vSphere クライアントを使用してデータストアを再作成する必要があります。

仮想マシンの作成

Cisco では、仮想ホストをダウンロードして転送するための VM テンプレートを提供しています。このテンプレートを使用して、Cisco UCS サーバのインストール上に Cisco Emergency Responder の VM を作成します。

テンプレートを導入し、VM を作成する前に、ホスト名および IP アドレスを新しい VM に割り当てる必要があります。

次の手順に従って VM を作成し、Cisco UCS サーバに Cisco Emergency Responder をインストールする準備を行います。

ステップ 1　アプリケーションに VM テンプレートをダウンロードします。

詳細については、「仮想マシン テンプレート（OVA テンプレート）のダウンロード」（P.2-9）を参照してください。

ステップ 2　UCS サーバにあるデータストアにテンプレートをアップロードします。

この場合には、より小さいデータストア（ESXi をインストール済み）を使用することを推奨します。

ステップ 3　このテンプレートを UCS サーバで使用できるようにします。

ステップ 4　vSphere クライアントを使用してテンプレート ファイルを配置します。新しい VM に次の情報を入力します。

- hostname
- datastore：十分なリソースがあるデータストアを選択します。

ステップ 5　VM の作成を完了します。

これで、アプリケーションの使用に適した容量のメモリ、CPU の数、およびディスクのサイズと数で、新しい VM が作成されます。

ステップ 6　Cisco Emergency Responder を VM 上の Cisco UCS サーバにインストールします。

詳細については、「Cisco Emergency Responder の VM へのインストール」（P.2-10）を参照してください。

仮想マシン テンプレート（OVA テンプレート）のダウンロード

Cisco Emergency Responder および仮想マシンの構成は、サポート対象の仮想マシン テンプレートと一致している必要があります。

次の手順を実行して、Cisco UCS サーバの Cisco Emergency Responder 用の仮想マシン テンプレートを取得します。

ステップ 1　ブラウザで、次の URL を選択します。

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

ステップ 2　ブラウザで指示された場合は、Cisco.com の [User Name:] および [Password:] をテキスト ボックスに入力し、[Log In] ボタンをクリックします。

ステップ 3　[IP Telephony] > [Call Control] > [Cisco Unified Communications Manager (Cisco Unified CM)] > [Cisco Unified Communications Manager Version 8.0] の順に選択します。

ステップ 4　[Unified Communications Manager Virtual Machine Templates] リンクをクリックします。

ステップ 5　Latest Releases フォルダで、[1.0(1)] リンクをクリックします。

ステップ 6　[Download Now] ボタンをクリックします。プロンプトに従い、必要な情報を入力し、ソフトウェアをダウンロードします。

ステップ 7　[Download Cart] ウィンドウが表示されたら、[Readme] リンクをクリックして、仮想マシン テンプレートのリリース情報を参照します。

Cisco Emergency Responder の VM へのインストール

次の手順に従って、新しい VM に Cisco Emergency Responder をインストールします。

ステップ 1　vSphere クライアントで、次に VM がリブートされたときに BIOS 設定が適用されるよう、VM を編集します。

ステップ 2　VM DVD-ROM ドライブで、Emergency Responder インストール メディアを使用できるようにします。

ステップ 3　VM の電源を投入し、次に BIOS 設定で、ハード ドライブの前に CD ROM からブートするように設定します。

ステップ 4　VM のブートを完了します。

Cisco Emergency Responder のインストール プログラムが起動します。インストールの詳細については、『*Installing Cisco Emergency Responder*』を参照してください。

Cisco UCS サーバの Cisco Emergency Responder のライセンス

次の項で、Cisco UCS サーバの Cisco Emergency Responder のライセンシングについて説明します。

- 「新しいライセンス付与手順によるお客様への影響」（P.2-10）
- 「サポート対象仮想マシンの構成とライセンス」（P.2-11）

新しいライセンス付与手順によるお客様への影響

Cisco UCS サーバの Cisco Emergency Responder は、MCS サーバの Cisco Emergency Responder とは異なるライセンシング モデルを使用します。NIC カードの MAC アドレスは、ライセンスのサーバへの関連付けには使用されなくなりました。

代わりに、ライセンスはライセンス MAC に関連付けられます。ライセンス MAC は、サーバ上に設定する次のパラメータを合わせて作成される、12 桁の 16 進数の値です。

- Time zone
- NTP server 1（または「none」）
- NIC speed（または「auto」）
- Hostname
- IP Address（または「dhcp」）
- IP Mask（または「dhcp」）
- Gateway Address（または「dhcp」）
- Primary DNS（または「dhcp」）
- SMTP server（または「none」）
- Certificate Information（Organization、Unit、Location、State、Country）

ライセンス MAC を取得する方法は、次のとおりです。

- インストール後、[Cisco Emergency Responder OS Administration] Web ページで [Show] > [Network] を選択します。
- インストール後、CLI コマンド **show status** を使用します。

新しいライセンスの取得

https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet でライセンスの Product Activation Key（PAK; 製品アクティベーション キー）を再取得する手順が、ライセンス MAC では変更されました。この URL でライセンス MAC の PAK を回復するときには、取得するライセンスのタイプを選択するプロンプトが表示されます。

- 物理 MAC アドレス：Cisco Emergency Responder を MCS サーバにインストールするときに使用します。
- ライセンス MAC アドレス：Cisco Emergency Responder を Cisco UCS サーバにインストールするときに使用します。

この選択を行う場合、ライセンス ファイルの生成とインストールでは、同じプロセスが使用されます。

ライセンス MAC パラメータの変更時の再ホスト ライセンスの取得

ライセンス MAC を作成するパラメータを変更する場合、一緒に取得したライセンスは無効になります。有効なライセンスを取得するため、ライセンスの再ホストを要求してください。古いライセンスは、30 日間の猶予期間、動作します。

ライセンスを再ホストするには、ライセンス チームに問い合わせる必要があります。ライセンス チームのメール アドレス licensing@cisco.com までお問い合わせください。

サポート対象仮想マシンの構成とライセンス

シスコからのサポートを受けるには、Cisco UCS サーバ上で Cisco Emergency Responder を実行する仮想マシンの構成が、「システム要件」（P.2-4）に記載されている仕様を満たしている必要があります。

Cisco Emergency Responder は他の仮想マシン設定でもインストールし、ライセンスを得ることができますが、シスコではこのような設定をサポートしません。

Cisco UCS サーバの Cisco Emergency Responder への移行

Media Convergence Server（MCS サーバ）から Cisco UCS サーバの Cisco Emergency Responder への移行では、サーバ ハードウェアを交換する手順に類似した手順を実行します。

表 2-5 に、移行プロセスの概要およびその他の印刷資料を示します。

表 2-5　Cisco UCS サーバの Cisco Emergency Responder への移行プロセスの概要

	設定手順	関連手順とトピック
ステップ 1	MCS サーバを Cisco Emergency Responder 8.6 にアップグレードします。	『*Cisco Emergency Responder Admin Guide Release 8.6*』を参照してください。
ステップ 2	MCS サーバと異なる IP アドレスまたはホスト名が、Emergency Responder VM で使用されている場合、MCS サーバの IP アドレスおよびホスト名を、Emergency Responder VM で使用されている値に変更します。これは、DRS のバックアップおよび復元を動作させるために必要です。	『Cisco Emergency Responder Admin Guide Release 8.6』を参照してください。
ステップ 3	MCS サーバで DRS バックアップを実行します。	『Cisco Emergency Responder Admin Guide Release 8.6』を参照してください。
ステップ 4	MCS ノードの代替として使用する Cisco UCS サーバに仮想マシン（VM）を作成します。	「Cisco UCS サーバへの Cisco Emergency Responder のインストール」(P.2-5)
ステップ 5	Cisco UCS サーバに Cisco Emergency Responder 8.6 をインストールします。	「Cisco UCS サーバへの Cisco Emergency Responder のインストール」(P.2-5)
ステップ 6	DRS の復元を実行して、MCS サーバからバックアップされたデータを Cisco UCS サーバに復元します。	『Cisco Emergency Responder Admin Guide Release 8.6』を参照してください。
ステップ 7	新しいライセンスを Cisco UCS サーバの Cisco Emergency Responder にアップロードします。	『*Cisco Emergency Responder Admin Guide Release 8.6*』を参照してください。

VMware のサポート

Cisco UCS サーバで Cisco Emergency Responder を使用する場合、次の事項を考慮してください。

- サーバに DVD ドライブがない場合は、インストール、アップグレード、復元手順には ISO や Virtual Floppy（FLP; 仮想フロッピー）などの「ソフト メディア」を使用します。
- USB テープのバックアップはサポートされません。
- VMware 仮想スイッチでは、NIC チーミングが設定されています。
- ハードウェア SNMP および Syslog は、VMware および UCS Manager に移動されます。
- インストール ログは、仮想シリアル ポートのみに書き出されます。
- ユーザ介入なしのインストールでは、USB の代わりに仮想フロッピーが使用されます。
- 基本的な UPS 統合はサポートされません。
- ブート順序は、VMware VM の BIOS によって制御されます。
- ハードウェア BIOS、ファームウェア、ドライバは必要なレベルでなければなりません。また、VMware 製品およびバージョンをサポートする Cisco Emergency Responder と互換性があるよう設定する必要があります。

UCS C シリーズ サーバの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/gui/config/guide/1.1.1/b_Cisco_UCS_C-Series_Servers_Integrated_Management_Controller_Configuration_Guide_1_1_1.html

Cisco UCS C シリーズの Integrated Management Controller の製品インストールおよび設定のガイドについては、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html

Cisco UCS Manager の製品インストールおよび設定のガイドについては、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

Cisco UCS サーバの Cisco Emergency Responder の日常業務の実行

Cisco UCS サーバの Cisco Emergency Responder ソフトウェア アプリケーションの日常業務は、アプリケーションを MCS サーバにインストールした場合と同様です。

ただし、ハードウェアの管理と監視の一部に違いがあります。これは、Cisco UCS サーバの Cisco Emergency Responder は仮想環境で動作しているためです。ここでは、これらの作業の実行方法について説明します。

- 「VM からのハードウェアのモニタリング」（P.2-13）
- 「CIMC からの監視」（P.2-13）
- 「vSphere クライアントおよび vCenter からのモニタリング」（P.2-13）

VM からのハードウェアのモニタリング

VM で実行されているアプリケーションには、物理ハードウェアをモニタする機能はありません。ハードウェアのモニタリングは、CIMC、ESXi プラグイン、vCenter、または物理的な点検（LED の点滅など）から行う必要があります。

CIMC からの監視

CIMC では次のハードウェア モニタリング機能が提供されています。

- CPU、メモリ、および電源の状況の概要
- CPU、メモリ、電源、およびストレージなどのハードウェア インベントリの概要
- 電源、ファン、温度、および電圧のセンサーのモニタリング
- BIOS およびセンターのエントリが含まれているシステム イベント ログ

vSphere クライアントおよび vCenter からのモニタリング

vSphere クライアントでは次のモニタリング機能が提供されています。

- vCenter にログインしているとき、vSphere クライアントでは、[Alarms] タブで定義されているハードウェア アラームおよびシステム アラームが表示されます。
- VM リソースの使用状況が、[Virtual Machines] タブおよび各 VM の [Performance] タブで表示されます。

- ホストのパフォーマンスおよびリソースの使用状況が、そのホストの [Performance] タブで表示されます。
- ESXi がスタンドアロン（vCenter なし）で使用される場合、ハードウェア ステータスおよびリソースの使用状況は使用できますが、アラーム機能は使用できません。

関連資料

『UCS RAID Controller SMI-S Reference Guide』では、Cisco UCS サーバでの Storage Management Initiative Specification（SMI-S）サポートについて説明しています。これは、次の URL にあります。

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/utilities/raid/reference/guide/ucs_raid_smis_reference.html

新しいシステムへの Cisco Emergency Responder 8.6 のインストール

この手順では、新規インストールとして Emergency Responder 8.6 をインストールする方法について説明します。

Emergency Responder グループ設定は、次のトピックで説明するように、Publisher（プライマリ）および Subscriber（セカンダリ）サーバのペアに基づいて、Emergency Responder Administration Web インターフェイスを使用して入力します。

- 「Cisco Emergency Responder Publisher のインストール」（P.2-14）
- 「Cisco Emergency Responder Subscriber のインストール」（P.2-19）

Cisco Emergency Responder Publisher のインストール

Emergency Responder 8.6 をインストールするには、Publisher（プライマリ）を最初にインストールしてから、Subscriber（バックアップ）を別のサーバにインストールします。Emergency Responder は、Cisco Unified Communications Manager またはすべての Cisco Unified Communications アプリケーションとは別のサーバにインストールする必要があります。

新しくインストールするには、約 1 時間かかります。

Publisher をインストールするには、次の手順を実行します。

手順

ステップ 1　Emergency Responder 8.6 インストール用 DVD を挿入します。

システムで DVD が検出されると、DVD に何らかの問題があるかどうか確認するため、インストールの前にメディア チェックを実行するかどうか尋ねられます。DVD のチェックサムが表示され、このチェックサムを Emergency Responder 8.6 の Web サイトで確認するよう指示されます。

画面の下部に、要素間を移動したり要素を選択する手順が、次のように表示されます。

- 次の要素に進むには Tab キーを使用します。
- 前の要素に戻るには Alt キーを押した状態で Tab キーを押します。
- 強調表示した要素を選択するには、スペース キーを使用します。

メディア チェックの実行を選択した場合は、システムによってメディア チェックが実行され、結果が表示されます。

メディア チェックの結果が [PASS] の場合、[OK] をクリックします。インストールが開始されます。ステップ 2 に進みます。

メディア チェックの結果が [FAIL] の場合、シスコから新しいインストール用 DVD を入手してください。

ステップ 2　Cisco Unified Communications システムのインストールが開始されます。[Product Deployment Selection] 画面に、Cisco Emergency Responder 製品スイートがインストールされることを示すメッセージが表示されます。[OK] をクリックして続行します。

ステップ 3　[Proceed with Install] ページに、ハード ドライブにある現在のソフトウェア バージョンとインストール用 DVD のソフトウェア バージョンが表示されます。

新規インストールを実行する場合、ハード ドライブにはソフトウェアがなく、インストールを進めてよいか確認するメッセージが表示されます。[Yes] をクリックして進みます。

アップグレードを実行する場合、現在のソフトウェア バージョンが表示され、ハード ドライブを上書きしてよいか確認するメッセージが表示されます。[Yes] をクリックして進みます。

[Yes] をクリックした場合は、インストールが続行され、[Platform Configuration Wizard] が表示されます。

[No] をクリックすると、インストールは終了します。

ステップ 4　[the Platform Configuration Wizard] ページで、[Proceed] をクリックしてプラットフォームのインストールを続行します。[Import Windows Data] ページが表示されます。ステップ 5 に進みます。

[Skip] をクリックした場合は、プラットフォームと Emergency Responder ソフトウェアの両方がインストールされ、情報の提供を求めるプロンプトはインストール中に表示されません。インストールが完了してシステムがリブートすると、必要な設定情報の入力を求めるプロンプトが表示されます。

ステップ 5　[Import Windows Data] ページに、Emergency Responder からのデータのインポートを求めるプロンプトが表示されます。このページは、新規インストールや Linux ベースの旧バージョンの Emergency Responder からのアップグレードでは使用しません。[No] をクリックして、新規インストールを続行します。[Basic Install] ページが表示されます。

ステップ 6　[Continue] をクリックして進みます。[Timezone Configuration] ページが表示されます。

ステップ 7　表示されるリストから、正しい時間帯を選択します。

次のキーを使用して、[Timezone Configuration] ページの要素間を移動します。

- 上矢印または下矢印を使用して、リストから時間帯を選択
- Tab キーで他のフィールドに移動

正しい時間帯を選択したら、[OK] をクリックします。[Auto Negotiation Configuration] ページが表示されます。

ステップ 8　[Yes] をクリックして、イーサネット NIC 速度およびデュプレックスのオートネゴシエーションをイネーブルにします。[DHCP Configuration] ページが表示されます。[Yes] をクリックした場合は、ステップ 11 に進みます。

[No] をクリックした場合、[NIC Speed and Duplex Configuration] ページが表示されます。

ステップ 9　[NIC Speed and Duplex Configuration] ページで、次を行います。

a.　[NIC Speed] を選択します。選択肢は [10 Megabit]、[100 Megabit]、[1000 Megabit] です。

b.　[NIC Duplex] 設定を選択します。選択肢は [Full] または [Half] です。

c.　[OK] をクリックします。[DHCP Configuration] ページが表示されます。

ステップ 10　[MTU Configuration] ページでは、次の手順に従って、ネットワークで送信できる最大伝送ユニット（MTU）を設定できます。

- 1500 バイト未満の MTU 値を設定する場合は、[Yes] をクリックします。
- デフォルトの MTU 値の 1500 バイトを使用する場合は [No] をクリックします。

ステップ 11　Dynamic Host Configuration Protocol（DHCP）を使用する場合は [Yes] をクリックします。[Administration Login Configuration] ページが表示されます。ステップ 15 に進みます。

[No] をクリックした場合は、[Static Network Configuration] ページが表示されます。

ステップ 12　DHCP を使用しない場合は、[Static Network Configuration] ページに関する次の情報を入力します。

- Host Name
- IP Address
- IP マスク
- Gateway (GW) Address

[OK] をクリックします。[DNS Client Configuration] ページが表示されます。

ステップ 13　[DNS Client Configuration] ページで、Domain Name System（DNS; ドメイン ネーム システム）クライアントを設定するかたずねられます。

（注）　DNS 設定の詳細については、[Help] ボタンをクリックしてください。

[Yes] を選択すると、2 つ目の [DNS Client Configuration] ページが表示されます。

[No] を選択すると、[Administration Login Configuration] ページが表示されます。ステップ 15 に進みます。

ステップ 14　2 つ目の [DNS Client Configuration] ページで、次の情報を入力するよう求められます。

- Primary
- Secondary DNS（任意）
- Domain

[OK] をクリックします。[Administration Login Configuration] ページが表示されます。

ステップ 15　[Administration Login Configuration] ページで、管理者アカウントの ID およびパスワードを入力します。このパスワードは、CLI と、Cisco Unified OS Administration および Disaster Recovery System（DRS）の Web サイトにアクセスするために使用されます。[Help] をクリックすると、このパスワードを作成するガイドラインが表示されます。

入力が終わったら、[OK] をクリックします。[Certificate Information] ページが表示されます。

ステップ 16　[Certificate Information] ページに関する次の情報を入力します。

- マニュアルの構成
- Unit
- Location
- State
- Country（スクロールダウン メニューから選択）。

[OK] をクリックします。[Publisher Configuration] ページが表示されます。

ステップ 17　実行するインストールのタイプに基づき、次のいずれかを行います。

- 設定しているサーバがサーバ グループの Publisher である場合は、[Yes] をクリックします。[Network Time Protocol Client Configuration] ページが表示されます。ステップ 18 に進みます。
- インストールしているサーバがサーバ グループの Publisher ではない場合、次に進む前に Publisher で最初にこのサーバを設定する必要があります。また、このサーバは、インストールが正常に完了するよう、稼動中の Publisher にネットワークでアクセスする必要があります。Subscriber を設定している場合のみ、[No] をクリックします。Subscriber のインストールの詳細については、「Cisco Emergency Responder Subscriber のインストール」（P.2-19）を参照してください。

ステップ 18　[Network Time Protocol Client Configuration] ページで、外部 Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバを設定するかたずねられます。

（注）　Cisco では、システム時刻を正確にしておくために、外部 NTP サーバを使用することを強くお勧めします。

注意　UCS サーバに Emergency Responder をインストールする場合は、NTP サーバの設定が必須になります。

[Yes] をクリックした場合は、2 つ目の [Network Time Protocol Client Configuration] ページが表示されます。表示されたフィールドに、外部 NTP サーバの IP アドレスまたはホスト名を入力し、[OK] をクリックします。[Database Access Security Configuration] ページが表示されます。ステップ 19 に進みます。

[No] をクリックした場合は、[Hardware Clock Configuration] ページが表示されます。次の情報を入力します。

- Year（*yyyy*）
- Month（*mm*）
- Day（*dd*）
- Hour（*hh*）
- Minute（*mm*）
- Second（*ss*）

この情報を入力したら、[OK] をクリックします。[Database Access Security Configuration] ページが表示されます。

ステップ 19　[Database Access Security Configuration] ページで、表示されるフィールドにセキュリティ パスワードを入力し、パスワードを確認します。

（注）　セキュリティ パスワードは、長さ 6 文字以上にしてください。パスワードには英数字、ハイフン、アンダースコアを使用できます。また、英数字から始まるパスワードにしてください。このセキュリティ パスワードは、インストール/アップグレード、DRS のバックアップまたは復元、および「新しい Publisher の指定」操作を実行する際に Emergency Responder サーバ グループ間で安全に通信するために使用されます。

[Help] をクリックするとガイドラインが表示されます。終了したら、[OK] をクリックします。[SMTP Host Configuration] ページが表示されます。

ステップ 20　Simple Mail Transport Protocol（SMTP; シンプル メール転送プロトコル）ホストを設定するかたずねられます。この手順は任意です。

- [Yes] をクリックした場合、2 つ目の [SMTP Host Configuration] ページが表示されます。[Help] をクリックするとガイドラインが表示されます。表示されたフィールドに SMTP ホスト名または IP アドレスを入力します。入力が終わったら、[OK] をクリックします。[Platform Configuration Confirmation] ページが表示されます。
- [No] をクリックした場合、[Platform Configuration Confirmation] ページが表示されます。

ステップ 21　[Platform Configuration Confirmation] ページで、次のいずれかを行います。

- [OK] を選択してプラットフォーム設定情報を保存し、インストールを続行します。[Cisco Emergency Responder Configuration] ページが表示されます。

（注）　[OK] を選択すると、プラットフォーム設定情報は変更できません。

- 前のページに戻って変更する場合、[Back] を選択します。[Back] を続けて選択すると、各プラットフォーム設定ページをスクロールします。
- [Cancel] を選択すると、インストールがキャンセルされます。

ステップ 22　[Cisco Emergency Responder Configuration] ページで、次を行います。

- 緊急電話番号（**911** など）を入力します。
- Cisco Unified Communications Manager のバージョンを選択します。↑キーまたは↓キーを使用してバージョン番号を選択し、[OK] をクリックします。

ステップ 23　[Security End User Language Selection] ページで、Cisco Emergency Responder の Web ページの言語を選択します。デフォルトは英語です。

[Application User Password Configuration] ページが表示されます。

ステップ 24　[Application User Configuration] ページで、ユーザ名とパスワードを入力します。このユーザ名とパスワードはデフォルトの管理アカウントに関連付けられ、[Emergency Responder Administration] Web ページへのログインに使用されます。ガイドラインを表示するには、[Help] をクリックします。

入力が終わったら、[OK] をクリックします。[Cisco Emergency Responder Configuration Confirmation] ページが表示されます。

ステップ 25　[Cisco Emergency Responder Configuration Confirmation] ページで、次のいずれかを行います。

- [OK] を選択して Cisco Emergency Responder の設定情報を保存し、インストールを続行します。インストール プロセスが続行され、システムがリブートします。

注意　[OK] を選択すると、Cisco Emergency Responder の設定情報は変更できません。

- 前のページに戻って変更する場合、[Back] を選択します。[Back] を続けて選択すると、各 [Emergency Responder Application User Configuration] ページをスクロールします。
- [Cancel] を選択すると、インストールがキャンセルされます。

ステップ 26　システムが再起動された後、各種システム コンポーネントのステータスがチェックされます。問題が見つかった場合は、問題の修正を求めるプロンプトが表示されます。

問題が見つからなかった場合、インストール処理が続行されます。インストール用 DVD が排出され、システムがリブートし、インストールが終了します。インストールが完了すると、コマンドライン インターフェイス プロンプトが表示されます。

（注）　このプロセス中に、Publisher の MAC アドレスが表示されます。表示された MAC アドレスを書き留めます。この MAC アドレスは、後で Emergency Responder ライセンスを取得する際に使用します。インストール中に MAC アドレスを取得できなかった場合、後で確認できます。サーバの MAC アドレス確認の詳細については、「サーバ ライセンス」（P.1-5）を参照してください。

ステップ 27　Emergency Responder 8.6 の Web サイトを表示するには、ネットワーク上の Windows システムで、サポートされている Web ブラウザを起動して次の URL を入力します。

http://*your Emergency Responder hostname*

または

http://*your Emergency Responder IP address*

（注）　ホスト名が IP アドレスに解決されるよう、Emergency Responder は DNS を使用して設定されていることを確認してください。

Cisco Emergency Responder Subscriber のインストール

Publisher のインストール後に、Emergency Responder Subscriber をインストールする必要があります。Subscriber は Emergency Responder Publisher とは別のサーバにインストールする必要があります。

注意　Subscriber のインストールを開始する前に、Publisher のインストールを完了する必要があります（これには、リブートが含まれます）。

Emergency Responder 8.6 Subscriber をインストールするには、次の手順を実行します。

手順

ステップ 1　Publisher サーバで、次を行って Subscriber サーバの詳細を追加します。

a. Publisher の [Emergency Responder 8.6 Administration] Web サイトにログインします。

b. [System] > [Add Subscriber] を選択します。[Add Server] ページが表示されます。

c. 新しい Subscriber のホスト名を入力して [Insert] をクリックします。[Add Subscriber] が再度表示されます。

d. [Configured Servers] リストで、新しい Subscriber のホスト名と IP アドレスが表示されているか確認します。

ステップ 2　「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」のステップ 1 からステップ 16 までを行ってください。ステップ 16 が完了すると、[Publisher Configuration] ページが表示されます。

ステップ 3　[Publisher Configuration] ページで、[No] を選択して Publisher ではなく Subscriber をインストールするよう指定します。Publisher ではない場合は、続行する前に、Publisher の管理 Web インターフェイスを使用して最初にこのサーバを設定する必要があることを知らせる警告が表示されます（詳細については、この手順のステップ 1 を参照してください）。また、追加しているこのサーバは、インストールが正常に完了するよう、稼動中の Publisher にネットワークでアクセスする必要があります。

[OK] をクリックして警告を閉じます。

ステップ 4　[Network Connectivity Test Configuration] ページが表示されます。システムの接続性の検証が試行されます。[No] をクリックしてインストールを続行します。

ステップ 5　[Publisher Access Configuration] ページが表示されます。次の内容を入力します。

- Publisher のホスト名
- Publisher の IP アドレス
- Publisher のデータベース / セキュリティ パスワード

ステップ 6　Publisher 情報が正しいか確認して [OK] をクリックします。

ステップ 7　[SMTP Host Configuration] ページが表示されます。SMTP ホストを設定する場合は [Yes] を選択します。

ステップ 8　[Platform Configuration Complete] ページが表示されます。次のオプションのうちいずれかを選択します。

- Publisher 情報が正しい場合、[OK] をクリックします。
- 情報が正しくない場合、[Back] ボタンをクリックして、[Publisher Access Configuration] ページで必要な変更を行います。[OK] をクリックします。

Emergency Responder Subscriber のインストールが開始され、完了するまでに 20 ～ 30 分かかります。

ステップ 9　インストールが完了したら、Subscriber の [Emergency Responder Administration] Web サイトを表示して Subscriber が正常にインストールされているか確認します。正常にインストールされた場合は、「Primary Cisco Emergency Responder is active」というメッセージが表示されます。このメッセージは Subscriber が正常にインストールされたことを示します。

（注）　Subscriber のインストールで Publisher を検証できなかった場合は、トラブルシューティングの章の「パブリッシャを確認できない」（P.11-16）を参照してください。

Emergency Responder 8.6 へのアップグレード

7.1(1) または 8.0(1) から、新しいバージョンの Emergency Responder 8.6 にアップグレードするには、Cisco Unified OS Administration Web インターフェイスを使用します。Emergency Responder 7.1 から新しいバージョンの Emergency Responder 8.6 へのアップグレードの詳細については、「ソフトウェアアップグレードの実行」（P.7-19）を参照してください。

CHAPTER 3

Cisco Emergency Responder 8.6 向けの Cisco Unified Communications Manager Versions 6.1 以降の設定

この章では、Cisco Emergency Responder（Emergency Responder）8.6 向けに Cisco Unified Communications Manager（Cisco Unified CM）6.1、7.1、8.0、8.5、および 8.6 を設定する手順について説明します。

（注） Cisco Emergency Responder（Emergency Responder）8.6 では、Cisco Unified CM 7.0(x) はサポートされません。

次のトピックでは、Emergency Responder が電話ネットワークで動作できるように、Cisco Unified CM 6.1、7.1、8.0、8.5、および 8.6 において設定する必要がある項目について説明します。

次のトピックでは、Cisco Unified CM の設定例について説明します。選択された名前（パーティション名、コーリング サーチ スペース名などは必須ではありません。

- 「電話機のルート プランの設定」（P.3-2）
- 「Cisco Emergency Responder で緊急コールを処理するための Cisco Unified Communications Manager の設定」（P.3-4）
- 「Cisco Emergency Responder Cisco Unified CallManager ユーザの作成」（P.3-21）

Cisco Unified CM の例について

これらの項では、参考用に設定および値の例を示します。特定の設定は、ご使用のネットワークと命名方法のニーズに応じて異なります。

これらの例では、次のコーリング サーチ スペースおよびパーティションを使用します。

- PhoneCSS：Phones パーティションが含まれています。
- E911CSS：E911 および Phones のパーティションが含まれています。

例は、単一の Cisco Unified CM クラスタに基づきます。複数のクラスタを設定する場合、緊急ロケーション識別番号（ELIN）のトランスレーション パターンを除き、クラスタごとに設定を繰り返します。ELIN トランスレーション パターンは、ゲートウェイが Public Safety Answering Point（PSAP）から着信コールを送信する Cisco Unified CM クラスタでのみ定義されます。

電話機のルート プランの設定

Emergency Responder を設定する前に、緊急コールの発信に使用される電話機（通常、すべての電話機）が Cisco Unified CM に追加および登録されていることを確認する必要があります。サポートが必要な場合は、Cisco Unified CM に付属のマニュアルまたはオンライン ヘルプを参照してください。

次の項では、Emergency Responder を追加する*前*のネットワークの設定例について説明します。

- 「電話機のパーティション」（P.3-2）
- 「電話機のコーリング サーチ スペースの作成」（P.3-2）
- 「電話機へのパーティションおよびコーリング サーチ スペースの割り当て」（P.3-3）

電話機のパーティション

電話機にパーティションをまだ作成していない場合には、ここで作成します。

電話機のパーティションを作成するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CM で [Route Plan] > [Partition] の順に選択します。

[Find and List Partitions] ページが表示されます。

ステップ 2　[Add a New Partition] をクリックします。

[Partition Configuration] ページが表示されます。

ステップ 3　[Partition Name and Description] フィールドに **Phones** などの記述的な名前を入力します。さらに、説明を入力することもできます。

ステップ 4　[Insert] をクリックして、新しいパーティションを追加します。

関連項目

- 「Cisco Unified CM の例について」（P.3-1）
- 「電話機のコーリング サーチ スペースの作成」（P.3-2）
- 「電話機へのパーティションおよびコーリング サーチ スペースの割り当て」（P.3-3）

電話機のコーリング サーチ スペースの作成

電話機にすでに定義されたコーリング サーチ スペースがない場合は、次の手順に従ってコーリング サーチスペースを作成します。

定義されたコーリング サーチ スペースを作成するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CM で [Route Plan] > [Calling Search Space] の順に選択します。

[Find and List Calling Search Spaces] ページが表示されます。

ステップ 2　[Add a New Calling Search Space] をクリックします。

[Calling Search Space Configuration] ページが表示されます。

ステップ 3　[Calling Search Space Name] フィールドに **PhoneCSS** などの記述的な名前を入力します。

ステップ 4　[Available Partitions] リスト ボックスで **Phones** パーティションを選択し、2 つのリスト ボックスの間にある矢印ボタンをクリックして、そのパーティションを [Selected Partitions] リスト ボックスに追加します。

ステップ 5　[Insert] をクリックして、新しいコーリング サーチ スペースを追加します。

関連項目

- 「Cisco Unified CM の例について」（P.3-1）
- 「電話機のパーティション」（P.3-2）
- 「電話機へのパーティションおよびコーリング サーチ スペースの割り当て」（P.3-3）

電話機へのパーティションおよびコーリング サーチ スペースの割り当て

Phones パーティション（「電話機のパーティション」（P.3-2））と PhonesCSS コーリング サーチ スペース（「電話機のコーリング サーチ スペースの作成」（P.3-2））を作成した後、それらを使用するために電話機を設定します。

はじめる前に

Bulk Administration Tool (BAT) を使用して、複数の電話機のパーティションおよびコーリング サーチ スペースを変更することができます。この場合、所要時間が各電話を個々に変更するよりもかなり短くなります。次の手順では、電話機を 1 台ずつ変更する手順について説明します。

BAT を使用してパーティションおよびコーリング サーチ スペースを変更するには、次の手順を実行します。

手順

ステップ 1　[Device] > [Phone] の順に選択します。

Cisco Unified CM に [Find and List Phones] ページが表示されます。

ステップ 2　検索フィールドで [Device name is not empty] を選択し、[Find] をクリックします。

Cisco Unified CM の下部のフレームにすべての電話機が表示されます。

ステップ 3　設定を変更する電話機をクリックします。

Cisco Unified CM に [Phone Configuration] ページが表示されます。

ステップ 4　コーリング サーチ スペースを **PhoneCSS** に変更し、[Update] をクリックします。

ステップ 5　左側の列で設定する回線番号をクリックします。

Cisco Unified CM に [Directory Number Configuration] ページが表示されます。

ステップ 6　パーティションを **Phones** に、コーリング サーチ スペースを **PhoneCSS** に変更します。

ステップ 7　[Insert] をクリックして変更を保存します。

関連項目

- 「Cisco Unified CM の例について」（P.3-1）
- 「電話機のパーティション」（P.3-2）
- 「電話機のコーリング サーチ スペースの作成」（P.3-2）

Cisco Emergency Responder で緊急コールを処理するための Cisco Unified Communications Manager の設定

緊急コールを処理するには、緊急コール番号（911 など）を設定して、Emergency Responder で緊急コール番号を傍受できるようにする必要があります。その後、Emergency Responder は、緊急コールを適切な Public Safety Answering Point（PSAP）にルーティングし、必要に応じて緊急コールを変換して、コールをルーティングしたり、初回コールが切断された場合に PSAP オペレータが緊急の発信者にコールバックできるようにします。

次のトピックでは、Emergency Responder に必要な Cisco Unified CM の要素を定義する方法について説明します。

- 「Cisco Emergency Responder のパーティションの作成」（P.3-4）
- 「Cisco Emergency Responder のコーリング サーチ スペースの作成」（P.3-5）
- 「緊急コールのルート ポイントの作成」（P.3-6）
- 「必要な CTI ポートの作成」（P.3-8）
- 「エラー メッセージおよびシステム メッセージ」（P.3-10）
- 「ERL の作成」（P.4-33）
- 「代替緊急コール番号の作成」（P.3-17）
- 「PSAP への接続に使用されるゲートウェイに対するコーリング サーチ スペースの設定」（P.3-18）
- 「Cisco Emergency Responder グループ間の通信に対するルート パターンの作成」（P.3-19）

Cisco Emergency Responder のパーティションの作成

Emergency Responder のパーティション E911 を作成する必要があります。このパーティションには、ネットワークにコールするために PSAP によって使用される番号とその他特定の CTI ルート ポイントが含まれます。

Emergency Responder のパーティション E911 を作成するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CM で [Route Plan] > [Partition] の順に選択します。

[Find and List Partitions] ページが表示されます。

ステップ 2　[Add a New Partition] をクリックします。

[Partition Configuration] ページが表示されます。

ステップ 3　[Partition Name] フィールドに **E911** などの記述的な名前を入力します。

ステップ 4　[Insert] をクリックして、新しいパーティションを追加します。

関連項目

- 「Cisco Unified CM の例について」（P.3-1）
- 「Cisco Emergency Responder のコーリング サーチ スペースの作成」（P.3-5）
- 「電話機のルート プランの設定」（P.3-2）
- 「緊急コールのルート ポイントの作成」（P.3-6）
- 「 •「ERL の作成」（P.4-33）」（P.3-10）
- 「Cisco Emergency Responder グループ間の通信に対するルート パターンの作成」（P.3-19）

Cisco Emergency Responder のコーリング サーチ スペースの作成

Emergency Responder のコーリング サーチ スペースを作成するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CM で [Route Plan] > [Calling Search Space] の順に選択します。

[Find and List Calling Search Spaces] ページが表示されます。

ステップ 2　[Add a New Calling Search Space] をクリックします。

[Calling Search Space Configuration] ページが表示されます。

ステップ 3　[Calling Search Space Name] フィールドに **E911CSS** などの記述的な名前を入力します。

ステップ 4　[Available Partitions] リスト ボックスで [E911] パーティション、[Phones] パーティション*の順に*選択し、2 つのリスト ボックスの間にある矢印ボタンをクリックして、これらを [Selected Partitions] リスト ボックスに追加します。E911 がリストの最上位に表示されるようにパーティションを配置します。

他のパーティションを使用している場合には、E911 パーティション*の後に*それらのパーティションをこのリストに追加します。

（注）　ユーザがトランスレーション パターン 911 または 9.911 を設定した場合（「9.911 のトランスレーション パターンの作成」（P.3-14）を参照）、911 ルート ポイントが E911 パーティションに追加され、電話機が E911 パーティションを認識できなくなるため、Phones パーティションの前に E911 パーティションを配置する必要があります。911 トランスレーション パターンは Phones パーティションにあり、E911CSS を取得します。E911 パーティションを最初に配置すると、911 ルート ポイントと一致し、目的通りにコールが Emergency Responder サーバに発信されます。誤って Phones パーティションを最初に配置すると、トランスレーション パターンが検索し続けるため、速いビジー信号が発生してしまいます。

ステップ 5　[Insert] をクリックして、新しいコーリング サーチ スペースを追加します。

関連項目

- 「Cisco Unified CM の例について」（P.3-1）
- 「Cisco Emergency Responder のパーティションの作成」（P.3-4）

- 「電話機のルート プランの設定」（P.3-2）
- 「緊急コールのルート ポイントの作成」（P.3-6）
- 「 •「ERL の作成」（P.4-33）」（P.3-10）
- 「代替緊急コール番号の作成」（P.3-17）
- 「PSAP への接続に使用されるゲートウェイに対するコーリング サーチ スペースの設定」（P.3-18）

緊急コールのルート ポイントの作成

Cisco Unified CM で次の CTI ルート ポイントを設定する必要があります。

- 911 などのロケールの緊急コール番号。

（注）　アクセス コードとして 9 を使用する場合の Emergency Responder の設定については、「9.911 のトランスレーション パターンの作成」（P.3-14）を参照してください。

- Emergency Responder スタンバイ サーバでリッスンする必要がある 912 などの番号。
- Public Safety Answering Point（PSAP）からの着信コールで使用する番号。PSAP が切断され、発信者にコールする必要がある場合、Emergency Responder は、ELIN 設定に基づいてコールを変更し、そのコールを緊急コールを発信した人にルーティングします。その他の ELIN 設定については、「 •「ERL の作成」（P.4-33）」（P.3-10）を参照してください。

はじめる前に

次の手順では、メインの緊急コール番号として 911 を使用していることを前提とします。ロケールで別の番号を使用する場合、「911」をその番号に置き換え、同様に「911」に基づいて「912」などの他の番号に置き換えます。たとえば、ロケールの緊急コール番号が 112 である場合、112、および場合によっては 113、114 を使用します。

Emergency Responder をインストールする際には、緊急コール番号を入力する必要があります。次の手順では、インストール時に指定する同一の番号を設定します。

表 3-1 では、緊急コールのルート ポイントについて説明します。

表 3-1　緊急コールのルート ポイント

ルート ポイントの設定	ルート ポイント		
	プライマリ番号（911）	バックアップ番号（912）	ELIN（913）
Device Name	RP911	RP912	RPELIN913
Description	エリアの緊急コール番号。Emergency Responder では、この番号へのすべてのコールを処理します。	Emergency Responder スタンバイ サーバのルート ポイント。プライマリ サーバでコールを処理できない場合には、このルート ポイントを経由してスタンバイ サーバでコールを処理します。	PSAP からのすべての着信コールの接続先。Emergency Responder によって、これらのコールが緊急の発信者に転送されます。ルート パターンはプレフィクス（913）と 10 個の X です。X の数は、番号計画に基づいてロケールで使用されている標準電話番号と同じにする必要があります。 この番号は、数字と X のみで構成する必要があります。 **注：**E.164 ダイヤル プランの場合、X の数には先頭の「+」が含まれません。

表 3-1　緊急コールのルート ポイント（続き）

ルート ポイントの設定	ルート ポイント		
	プライマリ番号（911）	バックアップ番号（912）	ELIN（913）
Directory Number	911	912	913XXXXXXXXX
Partition	電話機	E911	E911
Calling Search Space	E911CSS	E911CSS	E911CSS
Forward Busy	[Destination]：912 [CSS]：E911CSS	[Destination]：次のいずれかです。[1] • デフォルト ERL のルート パターン。 • オンサイトのセキュリティ番号。 [CSS]：E911CSS	[Destination]：オンサイトのセキュリティ番号。[2] [CSS]：E911CSS
Forward No Answer	[Destination]：912 [CSS]：E911CSS	[Destination]：次のいずれかです。 • デフォルト ERL のルート パターン。 • オンサイトのセキュリティ番号。 [CSS]：E911CSS	[Destination]：オンサイトのセキュリティ番号。 [CSS]：E911CSS
Forward On Failure	[Destination]：912 [CSS]：E911CSS	[Destination]：次のいずれかです。 • デフォルト ERL のルート パターン。 • オンサイトのセキュリティ番号。 [CSS]：E911CSS	[Destination]：オンサイトのセキュリティ番号。 [CSS]：E911CSS
Voice Mail Mask	このルート ポイントの場合は、ボイスメール マスクを設定しないでください。	このルート ポイントの場合は、ボイスメール マスクを設定しないでください。	このルート ポイントの場合は、ボイスメール マスクを設定しないでください。

1. スタンバイ サーバにコール転送番号を設定すると、スタンバイ サーバでコールを処理できない場合にコールがデフォルト ERL を担当する PSAP、またはオンサイトのセキュリティにルーティングされるようになります。スタンバイ サーバを設置しない場合には、プライマリ サーバにそれらの設定を使用します。
2. ELIN ルート ポイントにコール転送番号を設定すると、Cisco ER でコールを処理できない場合に PSAP のコールバックがオンサイトのセキュリティに転送されるようになります。

表 3-1 に説明されている緊急コールのルート ポイントを作成するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CM で [Device] > [CTI] の順に選択します。

[Find and List CTI Route Points] ページが表示されます。

ステップ 2　[Add a new CTI Route Point] をクリックします。

[CTI Route Point Configuration] ページが表示されます。

ステップ 3　次のように CTI ルート ポイントのプロパティを入力します。

- [Device Name] フィールドに **RP911** などの一意な名前を入力し、この名前が緊急コール番号であることを認定します。表 3-1 に推奨される名前を示していますが、任意の名前を使用できます。
- [Device Pool] メニューから適切なデバイス プールを選択します。
- 表 3-1 に示すように、ルート ポイントのコーリング サーチ スペースを選択します。

ステップ 4　[Insert] をクリックして新しい CTI ルート ポイントを追加します。

Cisco Unified CM によって、ルート ポイントが追加され、回線 1 を設定するかどうかが尋ねられます。[OK] をクリックして回線 1 を設定します。

Cisco Unified CM に [Directory Number Configuration] ページが表示されます。

ステップ 5　表 3-1 の情報を利用して作成している回線に設定を入力します。

ステップ 6　[Insert] をクリックします。

Cisco Unified CM によって、回線がデバイスに追加されます。表 3-1 で説明されているすべてのデバイスが設定されるまで、この手順を繰り返します。

さらにサポートが必要な場合は、Cisco Unified CM に付属のマニュアルおよびオンライン ヘルプを参照してください。

関連項目

- 「Cisco Emergency Responder のパーティションの作成」（P.3-4）
- 「Cisco Emergency Responder のコーリング サーチ スペースの作成」（P.3-5）
- 「 •「ERL の作成」（P.4-33）」（P.3-10）
- 「Cisco Emergency Responder グループ間の通信に対するルート パターンの作成」（P.3-19）
- 「代替緊急コール番号の作成」（P.3-17）
- 「Cisco Emergency Responder Cisco Unified CallManager ユーザの作成」（P.3-21）
- 「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）
- 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）

必要な CTI ポートの作成

Emergency Responder では、誰かが緊急コールを発信すると、CTI ポートを使用してオンサイトのアラート（セキュリティ）担当者にコールします。ERL に割り当てられている各担当者がコールを受信できるように、十分な CTI ポートを設定する必要があります。設定するポート数は、Emergency Responder がこれらの担当者に発信できる同時コール数です。このコール数は、Emergency Responder が処理できる、または PSAP に転送できる緊急コール数とは関連していません。Emergency Responder が処理できる同時緊急コール数に設定可能な制限はありません。

はじめる前に

Emergency Responder では、CTI ポートの内線番号は連続していなければならないため、未使用の内線のブロックを探す必要があります。たとえば、3001 から始まる 4 つの CTI ポートを作成する場合、3001、3002、3003、および 3004 を使用できるようにする必要があります。

必要な CTI ポート作成するには、次の手順を実行します。

手順

ステップ 1　[Device] > [Phone] の順に選択します。

Cisco Unified CM に [Find and List Phones] ページが表示されます。

ステップ 2　[Add a New Phone] をクリックします。

Cisco Unified CM に [Add a New Phone] ページが表示されます。

ステップ 3　[Phone Type] で [CTI Port] を選択し、[Next] をクリックします。

Cisco Unified CM に [Phone Configuration] ページが表示されます。

ステップ 4　次の情報を入力し、CTI ポートを設定します。

- [Device Name]：CTI3001 などの意味のある名前を入力します。
- [Device Pool]：適切なデバイス プールを選択します。このデバイス プールでは、G.711 リージョンを使用する必要があります。
- [Calling Search Space]：[PhoneCSS] を選択します。

ステップ 5　[Insert] をクリックします。

Cisco Unified CM によって、CTI ポートが追加され、回線 1 を設定するかどうかが尋ねられます。[OK] をクリックします。Cisco Unified CM に [Directory Number Configuration] ページが表示されます。

ステップ 6　次の情報を入力し、CTI ポートに回線 1 を設定します。

- [Partition]：[Phones] を選択します。
- [Calling Search Space]：[PhoneCSS] を選択します。

（注）　各 CTI ポートには回線を 1 つだけ設定します。オンライン アラート通知がそれらのポートを介して開始されると、1 つ以上の回線からオンサイトのセキュリティのアラート プロンプトが表示されない場合があります。

ステップ 7　[Insert] をクリックします。

Cisco Unified CM によって、回線がデバイスに追加されます。この手順を繰り返して、必要な各 CTI ルート ポイントを作成します。

（注）　続けて作成するすべての CTI ポートは、最初の CTI ポート DN から連続している必要があります。

関連項目

- 「Cisco Emergency Responder のパーティションの作成」（P.3-4）
- 「Cisco Emergency Responder のコーリング サーチ スペースの作成」（P.3-5）

- 「Cisco Emergency Responder Cisco Unified CallManager ユーザの作成」（P.3-21）
- 「Cisco Unified Communications Manager クラスタの指定」（P.4-26）
- 「ERL の作成」（P.4-33）

エラー メッセージおよびシステム メッセージ

Cisco Unified CM は複数のアラームを生成して、Emergency Responder の問題のトラブルシューティングを支援します。重要なイベントに関する電子メール通知でのアラートを使用するためには、Emergency Responder イベントの通知を設定する必要があります。

表 3-2 に、関連アラームを示します。

表 3-2　Cisco Unified CM の関連アラーム

関連アラーム	アラーム レベル	説明	推奨処置
CtiProviderOpened	Informational	アプリケーションが正常にプロバイダーをオープンしました。	このアラームは情報提供だけを目的としているため、処置は必要ありません。
CtiProviderClosed	Informational	アプリケーションによってプロバイダーが閉じられました。	Cisco Emergency Responder が稼動していることを確認し、アプリケーション サーバと Unified CM の間のネットワーク接続を確認し、アプリケーション サーバと Unified CM の CPU 使用率が安全な範囲にあることを確認します。
ApplicationConnectionDropped	Warning	CTIManager とアプリケーションの間の TCP 接続または TLS 接続が切断されています。	Cisco Emergency Responder が稼動していることを確認し、アプリケーション サーバと Unified CM の間のネットワーク接続を確認して、アプリケーション サーバと Unified CM の CPU 使用率が安全な範囲にあることを確認します。
CtiIncompatibleProtocolVersion	Warning	Cisco Emergency Responder のバージョンまたはその Unified Communications Manager の設定に、CTIManager のバージョンとの互換性がありません。	正しいバージョンの Cisco Emergency Responder が使用されていて、その Cisco Unified CM のバージョン設定が正しいことを確認します。Cisco Unified CM のバージョンを更新するには、第 9 章「Cisco Unified Communications Manager のバージョンの変更」を参照してください。

デフォルトでは、エラー イベントのみがイベント ログに書き込まれます。警告が書き込まれるようにイベント レベルを変更するか、または Emergency Responder ユーザがアプリケーション/ポートを閉じた場合のカスタマー アラートを設定する必要があります。

これを行うには、[Alarm] > [Configuration] > [Server] > [Service Group (CM Services)] > [Service (Cisco CTI Manager)] を選択して Serviceability Web ページに移動します。表 3 の最後の 3 つのアラームすべてが SysLog に書き込まれるように、[Alarm Event Level] を [Error] に変更します。

これらのアラームはシステム全体のアラームであり、Emergency Responder 固有のアラームではないことに注意してください。つまり、Emergency Responder だけではなく、警告メッセージをトリガーするすべての CTI アプリケーションがイベント ログへの書き込みを行います。プロバイダーがアウトオブ サービスになった場合に、電子メールまたは他の通知イベントによるアラートを使用できるように、Emergency Responder に関連する Cisco Unified CM イベントを設定する必要があります。

緊急コールのルーティングと PSAP コールバックの有効化を実現するための ELIN 番号の設定

緊急コールは、着信者番号ではなく、発信者番号に基づいてルーティングされます。何らかの理由により緊急コールが切断された場合（発信者がコールを切るなど）、PSAP は発信者番号を使用して緊急の発信者にコールバックできるようにする必要があります。緊急コールを通常通り終了した後に、更新された情報を入手するために PSAP がコールバックすることもあります。

Emergency Responder によって、発信者の内線が緊急ロケーション識別番号（ELIN）に変更されます。この番号を使用して緊急コールのルーティングと PSAP コールバックの有効化を実現します。Emergency Responder では、同じ番号セットを再利用し、最大 3 時間の間に発信されたコールから電話機の内線番号を記録します。

ELIN 番号を設定するには、まずサービス プロバイダーからダイヤルイン（DID）番号を入手する必要があります。各番号の料金を支払う必要があるため、取得する DID の数は ERL ごとに 2 つまたは 3 つに制限することを推奨します。DID は ERL ごとに一意にする必要があります。

Emergency Responder では、必要に応じて ERL に割り当てられている ELIN 番号を再利用します。たとえば、1 つの ERL に 2 つの番号を設定し、3 時間の間に 3 回の緊急コールが発信された場合、最初の緊急の発信者の ELIN マッピングが第 3 の発信者の内線に置き換えられます。したがって、PSAP は、最初の発信者にコールすると、第 3 の発信者に到達します。各 ERL 用に必要な DID の数を決定する際には、この点に留意してください。

次のトピックでは、ELIN 番号の設定に必要なルート パターンおよびトランスレーション パターンを設定する方法について説明します。

- 「ERL のルート パターンの作成」（P.3-11）
- 「ELIN のトランスレーション パターンの作成」（P.3-13）

これらの番号を使用して ERL を設定する方法の詳細については、「ERL の作成」（P.4-33）を参照してください。

ERL のルート パターンの作成

Emergency Responder は、ルート パターンを使用して緊急コールを適切な Public Safety Answering Point（PSAP）にルーティングします。ルート パターンでは、パターンを PSAP に接続するゲートウェイに関連付けます。選択するゲートウェイは、ルート パターンの割り当て先である緊急応答ロケーション（ERL）に応じて異なります。

ネットワークで ERL ごとに 1 つのルート パターンを作成する必要があります。それらの番号は、PSAP がネットワークにコールできるようにサービス プロバイダーから取得するダイヤルイン（DID）番号です。

はじめる前に

各 ERL には、ELIN に一意なルート パターンが必要です。ERL 管理者と協力して必要なルート パターンの数と ERL のロケールを把握し、適切なゲートウェイを選択できるようにします。ERL 管理者は、作成するルート パターンを ERL 定義に入力する必要があります。ERL については、「ERL の作成」（P.4-33）を参照してください。

ERL のルート パターンを作成するには、次の手順を実行します。

手順

ステップ 1　[Route Plan]>[Route Pattern] を選択します。

Cisco Unified CM に [Find and List Route Patterns] ページが表示されます。

ステップ 2　[Add a New Route Pattern] をクリックします。

Cisco Unified CM に [Route Pattern Configuration] ページが表示されます。

ステップ 3　次のようにルート パターンの情報を入力します。

- [Route Pattern]：緊急コール番号に変換できるパターン。通常、これは数字、ドット、および緊急コールです。たとえば、10.911、11.911 などです。パターンに含めることができるのは、数字とドットのみです。
- [Partition]：[E911] を選択します。
- [Numbering Plan]：エリアの番号計画を選択します。
- [Gateway/Route List]：ローカル PSAP への接続に使用するゲートウェイを選択します。
- [Route Option]：[Route this pattern] を選択します。
- [Use Calling Party's External Phone Number Mask]：これを選択します。
- [Discard Digits]：10.911 などのように提案されたパターンを使用する場合には、[PreDot] を選択します。別の方法を使用する場合、適切な設定を選択し、必要に応じて（緊急コール番号にダイヤルするために）[Called Party Transform Mask] に入力します。

（注）　+ が先頭に付く E.164 番号として ELIN が受信される場合は、トランスレーション パターンでも先頭の「+」および国番号（任意）を削除する必要があります。これにより、トランスレーション パターンが Emergency Responder で設定した北米番号計画または他の国内形式の番号と一致します。

ステップ 4　[Insert] をクリックします。

Cisco Unified CM によって、ルート パターンが保存されます。ルート パターンをさらに追加するには、ステップ 2 に戻ります。

ヒント　多数のルート パターンを作成することになる可能性があるため、ルート パターンについて詳細な命名方法の開発を検討してください。たとえば、*xyzzaaab*.911 などのパターンを使用するとします。この場合、*x* は Emergency Responder クラスタ ID であり、*y* は Emergency Responder グループ ID であり、*zz* は PSAP ID であり、*aaa* は ERL ID であり、*b* は ELIN ID（ERL 内の）です。

関連項目

- 「ELIN のトランスレーション パターンの作成」（P.3-13）
- 「Cisco Emergency Responder のパーティションの作成」（P.3-4）
- 「Cisco Unified CM の例について」（P.3-1）
- 「ERL について」（P.4-30）
- 「ERL の作成」（P.4-33）

ELIN のトランスレーション パターンの作成

ELIN 番号に使用しているダイヤルイン（DID）番号をカバーするトランスレーション パターンを作成します。PSAP では、それらの ELIN を使用してネットワークにコールします。Emergency Responder では、これらのコールを傍受し、コールを正しい緊急の発信者にルーティングできるようにする必要があります。「緊急コールのルート ポイントの作成」（P.3-6）で説明したように、ELIN にプレフィクスとして付けた番号を PSAP コールバックに設定したルート ポイントにするためには、トランスレーション パターンが必要です。

（注）　ELIN には、先頭に「+」が付いた E.164 番号を使用できません。10 桁の北米番号計画または他の国内形式の番号を使用してください。

ELIN に使用しているすべての DID のリストがあることを確認します。

ELIN のトランスレーション パターンを作成するには、次の手順を実行します。

手順

ステップ 1　[Route Plan] > [Translation Pattern] の順に選択します。

Cisco Unified CM に [Find and List Translation Patterns] ページが表示されます。

ステップ 2　[Add a New Translation Pattern] をクリックします。

Cisco Unified CM に [Translation Pattern Configuration] ページが表示されます。

ステップ 3　次のようにトランスレーション パターンを作成します。

- [Translation Pattern]：ELIN として使用している DID。可能な場合は、X 変数を使用して複数の DID をカバーするパターンを作成します（たとえば、5555551XXX）。パターンを作成できない場合は、DID ごとのトランスレーション パターンを個別に定義します。
- [Partition]：[E911] を選択します。
- [Numbering Plan]：エリアの番号計画を選択します。
- [Calling Search Space]：[E911CSS] を選択します。
- [Route Option]：[Route this pattern] を選択します。

- [Called Party Transformations, Prefix Digits (Outgoing Calls)]：番号に付けるプレフィクスの桁数を入力します。PSAP コールバックのルート ポイントを作成する際に使用した桁数を入力します。

ステップ 4　[Insert] をクリックします。

Cisco Unified CM によって、トランスレーション パターンが保存されます。トランスレーション パターンをさらに追加するには、ステップ 2 に戻ります。

関連項目

- 「ERL のルート パターンの作成」（P.3-11）
- 「Cisco Unified CM の例について」（P.3-1）
- 「ERL について」（P.4-30）
- 「ERL の作成」（P.4-33）

9.911 のトランスレーション パターンの作成

外部アクセス コードが 9 であるシステムでは、ユーザが外部の接続先にダイヤルすると、911 または 9.911 の CTI ルート ポイントがユーザのセカンダリ ダイヤルトーンのタイミングに干渉する可能性があります。911 および 9.911 のトランスレーション パターンを作成すると、セカンダリ ダイヤルトーンのタイミングが無視されます。

ユーザが外部アクセス コード 9 と 911 をダイヤルしたときに、前に「緊急コールのルート ポイントの作成」（P.3-6）で作成した単一の 911 パターンにコールが転送されるようにトランスレーション パターンを作成します。

はじめる前に

次の手順は、外部アクセス コードが 9 であるシステムに適用されます。外部アクセス コードが 9 以外である場合には、次の手順は適用されません。

次の手順を完了するために、Cisco Emergency Responder のインストール用にパーティションおよびコーリング サーチ スペースを追加しておく必要があります。

表 3-3 に、外部アクセス コード 9 のトランスレーション パターンを示します。

表 3-3　外部アクセス コード 9 のトランスレーション パターン

トランスレーション パターン	911	9.911
Partition	電話機	電話機
Calling Search Space	E911CSS	E911CSS
Route Option	Route this pattern	Route this pattern
Provide outside dial tone	このボックスをオンにする。	このボックスをオンにする。
Called Party Transformations, Discard Digits (Outgoing Calls)	なし	PreDo

表 3-3 に説明されているトランスレーション パターンを作成するには、次の手順を実行します。

手順

ステップ 1　[Route Plan] > [Translation Pattern] の順に選択します。

Cisco Unified CM に [Find and List Translation Patterns] ページが表示されます。

ステップ 2　[Add a New Translation Pattern] をクリックします。

Cisco Unified CM に [Translation Pattern Configuration] ページが表示されます。

ステップ 3　次のようにトランスレーション パターンを作成します。

- [Translation Pattern]：911
- [Partition]：Phones
- [Numbering Plan]：エリアの番号計画を選択します。
- [Calling Search Space]：[E911CSS] を選択します。
- [Route Option]：[Route this pattern] を選択します。
- [Provide Outside Dial Tone]：このボックスがオンになっていることを確認します。
- [Called Party Transformations, Discard Digits]：<*none*> を選択します。

ステップ 4　[Insert] をクリックします。

Cisco Unified CM によって、トランスレーション パターンが保存されます。

ステップ 5　次のように変更してステップ 2 からステップ 4 を繰り返します。

- [Translation Pattern]：9.911
- [Called Party Transformations, Discard Digits (Outgoing Calls)]：Predot

9.911 トランスレーション パターンの設定後に、ルート ポイントを作成する必要があります。表 3-4 は、9.911 の緊急コールのルート ポイントを示します。

（注）　次のルート ポイントは、「緊急コールのルート ポイントの作成」（P.3-6）で作成したルート ポイントとほぼ同じです。この場合、パーティションに Phones ではなく、E911 を入力します。

表 3-4　9.911 の緊急コールのルート ポイント

ルート ポイントの設定	ルート ポイント		
	プライマリ番号（911）	バックアップ番号（912）	ELIN（913）
Device Name	RP911	RP912	RPELIN913
Description	エリアの緊急コール番号。Emergency Responder では、この番号へのすべてのコールを処理します。	Emergency Responder スタンバイ サーバのルート ポイント。プライマリ サーバでコールを処理できない場合には、このルート ポイントを経由してスタンバイ サーバでコールを処理します。	PSAP からのすべての着信コールの接続先。Emergency Responder によって、これらのコールが緊急の発信者に転送されます。ルート パターンはプレフィクス（913）と 10 個の X です。X の数は、番号計画に基づいてロケールで使用されている標準電話番号と同じにする必要があります。 この番号は、数字と X のみで構成する必要があります。
Directory Number	911	912	913XXXXXXXXXX
Partition	E911	E911	E911
Calling Search Space	E911CSS	E911CSS	E911CSS

表 3-4　9.911 の緊急コールのルート ポイント（続き）

ルート ポイントの設定	ルート ポイント		
	プライマリ番号（911）	バックアップ番号（912）	ELIN（913）
Forward Busy	[Destination]：912 [CSS]：E911CSS	[Destination]：次のいずれかです。[1] • デフォルト ERL のルート パターン。 • オンサイトのセキュリティ番号。 [CSS]：E911CSS	[Destination]：オンサイトのセキュリティ番号。[2] [CSS]：E911CSS
Forward No Answer	[Destination]：912 [CSS]：E911CSS	[Destination]：次のいずれかです。 • デフォルト ERL のルート パターン。 • オンサイトのセキュリティ番号。 [CSS]：E911CSS	[Destination]：オンサイトのセキュリティ番号。 [CSS]：E911CSS
Forward On Failure	[Destination]：912 [CSS]：E911CSS	[Destination]：次のいずれかです。 • デフォルト ERL のルート パターン。 • オンサイトのセキュリティ番号。 [CSS]：E911CSS	[Destination]：オンサイトのセキュリティ番号。 [CSS]：E911CSS

1. スタンバイ サーバにコール転送番号を設定すると、スタンバイ サーバでコールを処理できない場合にコールがデフォルト ERL を担当する PSAP、またはオンサイトのセキュリティにルーティングされるようになります。スタンバイ サーバを設置しない場合には、プライマリ サーバにそれらの設定を使用します。
2. ELIN ルート ポイントにコール転送番号を設定すると、Cisco ER でコールを処理できない場合に PSAP のコールバックがオンサイトのセキュリティに転送されるようになります。

9.911 のルート ポイントを作成するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CM で [Device] > [CTI] の順に選択します。

[Find and List CTI Route Points] ページが表示されます。

ステップ 2　[Add a new CTI Route Point] をクリックします。

[CTI Route Point Configuration] ページが表示されます。

ステップ 3　次のように CTI ルート ポイントのプロパティを入力します。

- [Device Name] フィールドに **RP911** などの一意な名前を入力し、この名前が緊急コール番号であることを認定します。表 3-4 に推奨される名前を示していますが、任意の名前を使用できます。
- [Device Pool] メニューから適切なデバイス プールを選択します。
- 表 3-4 に示すように、ルート ポイントのコーリング サーチ スペースを選択します。

ステップ 4　[Insert] をクリックして新しい CTI ルート ポイントを追加します。

Cisco Unified CM によって、ルート ポイントが追加され、回線 1 を設定するかどうかが尋ねられます。[OK] をクリックして回線 1 を設定します。

Cisco Unified CM に [Directory Number Configuration] ページが表示されます。

ステップ 5　表 3-4 の情報を利用して作成している回線に設定を入力します。

ステップ 6　[Insert] をクリックします。

Cisco Unified CM によって、回線がデバイスに追加されます。表 3-4 で説明されているすべてのデバイスが設定されるまで、この手順を繰り返します。

さらにサポートが必要な場合は、Cisco Unified CM に付属のマニュアルおよびオンライン ヘルプを参照してください。

関連項目

- 「ERL のルート パターンの作成」（P.3-11）
- 「Cisco Unified CM の例について」（P.3-1）
- 「ERL について」（P.4-30）

代替緊急コール番号の作成

以前、9（または別の番号）をダイヤルして外線に接続していた場合、ユーザは、最初に外線のアクセス番号をダイヤルしてから緊急コール番号をダイヤルしてしまう可能性があります。たとえば、緊急コール番号が 911 である場合、ユーザは 9911 をダイヤルする可能性があります。このような可能性に対応する場合に、ユーザがダイヤルする可能性が高い番号のトランスレーション パターンを設定します。次の手順は、代替緊急コール番号として 9911 を設定する方法を示しています。

代替緊急コール番号を作成するには、次の手順を実行します。

手順

ステップ 1　[Route Plan] > [Translation Pattern] の順に選択します。

Cisco Unified CM に [Find and List Translation Patterns] ページが表示されます。

ステップ 2　[Add a New Translation Pattern] をクリックします。

Cisco Unified CM に [Translation Pattern Configuration] ページが表示されます。

ステップ 3　次のようにトランスレーション パターンを作成します。

- [Translation Pattern]：緊急番号として対応する番号。この例では、9.911 です。
- [Partition]：[Phones] を選択します。
- [Numbering Plan]：エリアの番号計画を選択します。
- [Calling Search Space]：[E911CSS] を選択します。
- [Route Option]：[Route this pattern] を選択します。
- [Provide Outside Dial Tone]：これを選択します。
- [Called Party Transformations, Discard Digits (Outgoing Calls)]：[Predot] を選択します。

ステップ 4　[Insert] をクリックします。

Cisco Unified CM によって、トランスレーション パターンが保存されます。トランスレーション パターンをさらに追加するには、ステップ 2 に戻ります。

関連項目

- 「Cisco Unified CM の例について」（P.3-1）
- 「電話機のパーティション」（P.3-2）
- 「電話機のコーリング サーチ スペースの作成」（P.3-2）

PSAP への接続に使用されるゲートウェイに対するコーリング サーチ スペースの設定

緊急ネットワークまたは PSTN への CAMA 接続または PRI 接続を使用するためにゲートウェイを設定し、緊急コールをローカル PSAP にルーティングできるようにする必要があります。ゲートウェイの設定の詳細については、ご使用のゲートウェイのマニュアルと Cisco Unified CM のマニュアルを参照してください。ゲートウェイの設定後、次の手順を実行してゲートウェイにコーリング サーチ スペースを設定できます。

PSAP への接続に使用されるゲートウェイにコーリング サーチ スペースを設定するには、次の手順を実行します。

手順

ステップ 1　[Device] > [Gateway] の順に選択します。

Cisco Unified CM に [Find and List Gateways] ページが表示されます。

ステップ 2　選択基準を入力せずに [Find] をクリックしてすべてのゲートウェイを表示するか、または設定するゲートウェイを表示するために必要な検索条件を入力して [Find] をクリックします。

基準に一致するゲートウェイが Cisco Unified CM に表示されます。

ステップ 3　設定するゲートウェイをクリックします。

Cisco Unified CM に [Gateway Configuration] ページが表示されます。

ステップ 4　[Calling Search Space] の [E911CSS] を選択します。

ステップ 5　[Update] をクリックします。

Cisco Unified CM によって、変更が保存されます。

関連項目

- 「Cisco Emergency Responder のコーリング サーチ スペースの作成」（P.3-5）
- 「PSTN に対する CAMA トランクまたは PRI トランクの取得」（P.1-20）
- 「Cisco Emergency Responder の配置」（P.1-24）
- 「Cisco Emergency Responder をご使用のネットワークに適合させる方法」（P.1-8）

Cisco Emergency Responder グループ間の通信に対するルート パターンの作成

Emergency Responder クラスタに複数の Emergency Responder グループが存在するときに、発信者の電話機が電話機の現在のロケーション外にある Cisco Unified CM クラスタにコールを発信する場合は、各 Emergency Responder グループで緊急コールを別の Emergency Responder グループにルーティングできるようにルート パターンを設定する必要があります。Emergency Responder クラスタ内で Emergency Responder グループ間の通信を行う方法の詳細については、「Cisco Emergency Responder のクラスタおよびグループについて」（P.1-14）を参照してください。

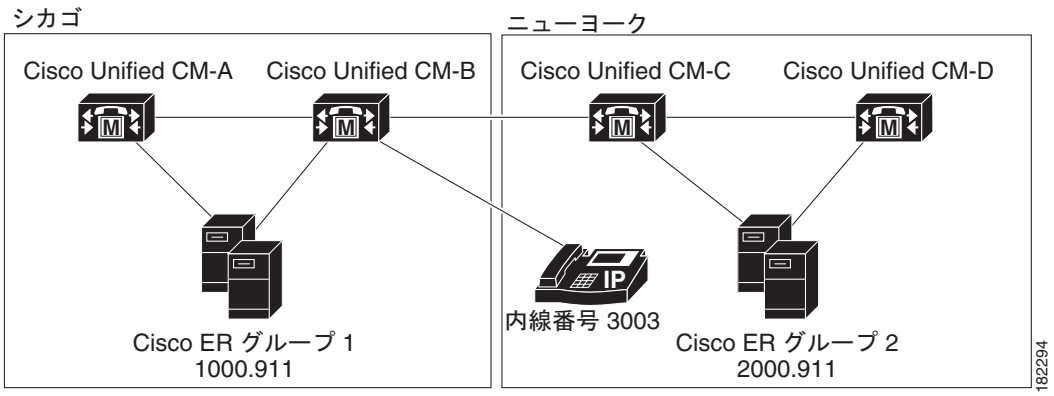
次の手順では、1 つの Emergency Responder グループのルート パターンを作成する方法について説明します。このようなパターンは、Emergency Responder グループによってサポート*されていない* Cisco Unified CM クラスタ内で作成する必要があります。図 3-1 のネットワークの設定について考えます。

グループ間の通信を可能にするには、次のように定義する必要があります。

- Cisco Unified CM クラスタ間の通信を可能にするために、各 Cisco Unified CM クラスタにクラスタ間トランクを定義する必要があります。このようなタイプのゲートウェイの作成の詳細については、Cisco Unified CM のマニュアルを参照してください。
- Cisco Unified CM クラスタ CCM-C および CCM-D にルート パターン 1000.911 を定義する必要があります。
- Cisco Unified CM クラスタ CCM-A および CCM-B にルート パターン 2000.911 を定義する必要があります。
- Emergency Responder グループ 1 に、Emergency Responder グループのルート パターンとして 1000.911 を定義します。
- Emergency Responder グループ 2 に、Emergency Responder グループのルート パターンとして 2000.911 を定義します。

これらの定義によって、Emergency Responder グループ 1 で運用されている Cisco Unified CM クラスタ CCM-B に電話機がコールを発信する場合でも、Emergency Responder グループ 2 で管理されている ERL のコールを Emergency Responder グループ 2 にルーティングすることができます。

図 3-1　　Cisco Emergency Responder グループのルート パターンについて



はじめる前に

ダイヤル プランは、Emergency Responder クラスタによってサポートされているすべての Cisco Unified CM クラスタ間で一意である必要があります。たとえば、図 3-1 に示すネットワークでは、Cisco Unified CM クラスタ CCM-B に内線 3003 のみを定義することができます。

1 つの Emergency Responder グループのルート パターンを作成するには、次の手順を実行します。

手順

ステップ 1　[Call Routing] > [Route/Hunt] > [Route Pattern] の順に選択します。

Cisco Unified CM に [Find and List Route Patterns] ページが表示されます。

ステップ 2　[Add a New] をクリックします。

Cisco Unified CM に [Route Pattern Configuration] ページが表示されます。

ステップ 3　次のようにルート パターンの情報を入力します。

- [Route Pattern]：緊急コール番号に変換できるパターン。通常、これは数字、ドット、および緊急コールです。1000.911、2000.911 などです。このパターンは、数字とドットのみで構成する必要があります。
- [Partition]：[E911] を選択します。
- [Numbering Plan]：エリアの番号計画を選択します。
- [Gateway/Route List]：Emergency Responder グループ間のルート パターンを定義している Emergency Responder グループによってサポートされている Cisco Unified CM クラスタに接続するために使用するクラスタ間トランク ゲートウェイを選択します。
- [Route Option]：[Route this pattern] を選択します。
- [Called Party Transformations, Discard Digits]：1000.911 などのように提案されたパターンを使用する場合には、[PreDot] を選択します。別の方法を使用する場合、適切な設定を選択し、必要に応じて（緊急コール番号にダイヤルするために）[Called Party Transform Mask] に入力します。

ステップ 4　[Save] をクリックします。

Cisco Unified CM によって、ルート パターンが保存されます。ルート パターンをさらに追加するには、ステップ 2 に戻ります。

ステップ 5　Emergency Responder グループ間のルート パターンを定義している Emergency Responder グループ以外の Emergency Responder グループで運用されている他すべての Cisco Unified CM クラスタに、ルート パターンを定義していることを確認します。

（注）　Cisco Unified CM 8.5 以降を使用する Emergency Responder クラスタの Emergency Responder ServerGroups 間で緊急コールをやり取りするには、[Unified CM Administration] Web サイトの [Device] > [Trunk Configuration] ページで、[Calling Party Selection] オプションを [Originator] に設定します。

関連項目

- 「Cisco Emergency Responder のパーティションの作成」（P.3-4）
- 「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）
- 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）

（注）　Cisco Unified CM 8.5 以降を使用する Emergency Responder クラスタの Emergency Responder ServerGroups 間で緊急コールをやり取りするには、[Cisco Unified CM Administration] Web サイトの [Device] > [Trunk Configuration] ページで、[Calling Party Selection] オプションを [Originator] に設定します。

Cisco Emergency Responder Cisco Unified CallManager ユーザの作成

Emergency Responder を Cisco Unified CM ユーザとして追加する必要があります。ここで入力する設定は、Emergency Responder 向けに Cisco Unified CM を設定する際に使用されます。

Emergency Responder を Cisco Unified CM ユーザとして追加するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CM で、[User Management] > [Application User] の順に選択します。[Add New] ボタンをクリックします。

Cisco Unified CM に [Application User Configuration] ページが表示されます。

ステップ 2　次の必須フィールドに入力します。

- [UserID] :「Emergency_Responder_User」などの記述的な名前を入力します。
- [Password] : このユーザのパスワードを入力します。
- [Confirm Password] : このユーザのパスワードを再入力します。

ステップ 3　[Device Information] セクションで、必要なルート ポイントおよび CTI ポートを選択してから、下矢印をクリックして選択したデバイスをユーザのコントロール リストに追加します。デバイスのリストが [Controlled Devices] 領域に表示されます。

ステップ 4　次のデバイスを選択します。

（注）　必要なデバイスの選択に、[Find Phones] または [Find Route Points] を使用しなければならない場合があります。

a. Cisco Emergency Responder で使用するために作成されているすべての CTI ポート。詳細については、「必要な CTI ポートの作成」の項を参照してください。

b. 911 などのプライマリ緊急コール番号。

c. 912 などのバックアップ緊急コール番号。

d. 913XXXXXXXXXX などの ELIN に使用されるルート ポイント。

ステップ 5　[Save] をクリックします。

ステップ 6　上部にある [Cisco Unified CM] メニューで、[User Management] > [User Group] の順にクリックします。

ユーザ グループの検索ページが表示されます。

ステップ 7　検索条件に standard を入力し、[Find] をクリックします。

名前が standard で始まるユーザ グループの一覧が表示されます。

ステップ 8　[Standard CTI Allow Calling Number Modification user group link] をクリックして、[User Group Configuration] ページを表示します。

ステップ 9　[Add Application Users to Group] をクリックします。

[Find and List Application Users] ポップアップ ウィンドウが表示されます。

ステップ 10　で作成したユーザ ID を検索条件として入力し、[Find] をクリックします。

アプリケーション ユーザの一覧が表示されます。

ステップ 11　ユーザ ID の隣にあるチェックボックスをオンにして [Add Selected] をクリックします。

Cisco Unified CM によって、選択したユーザが [Standard CTI Allow Calling Number Modification user group] に追加されます。

ステップ 12　[User Management] > [User Group] の順に選択します。

ユーザ グループの検索ページが表示されます。

ステップ 13　検索条件として **standard** を入力し、[Find] をクリックします。

名前が Standard で始まるユーザ グループの一覧が表示されます。

ステップ 14　[Standard CTI Enabled] グループをクリックします。

ユーザを Standard CTI Enabled グループに追加するには、ステップ 9 ～ 11 を繰り返します。

関連項目

- 「緊急コールのルート ポイントの作成」（P.3-6）
- 「必要な CTI ポートの作成」（P.3-8）

E.164 ダイヤル プランに基づくセキュリティ担当者の割り当て

Emergency Responder では、先頭に「+」が付いた E.164 番号はオンサイトのセキュリティ電話番号としてサポートされません。

Cisco Unified CM で設定されたオンサイトのセキュリティ電話番号が、先頭に「+」が付いた E.164 番号である場合は、まず、先頭に「+」が付かないオンサイトのセキュリティ電話番号を Emergency Responder で設定する必要があります。次に、Emergency Responder からオンサイトのセキュリティ電話番号が受信されるときに「+」が追加されるように、Cisco Unified CM でトランスレーション パターンを設定する必要があります。

次の手順を実行します。

- 電話機を Phones パーティションに配置します。
- 912, 913XXXXXXX を E911 パーティションに配置し、これに E911CSS を割り当てます。
- Phones パーティションを使用して PhoneCSS を作成し、これを電話回線に割り当てます。
- 911 を Phone パーティションに配置し、E911CSS を割り当てます。
- E911 パーティションおよび Phones パーティションを使用して E911CSS を作成します。

次に、次の手順を実行します。

- トランスレーション パターンを作成します。

- このトランスレーション パターンを、Emergency Responder で設定したオンサイト セキュリティ担当者の DN と一致する E911 パーティションに配置します。
- トランスレーション パターンのコーリング サーチ スペースを PhoneCSS に設定します。
- 着信側トランスフォーメーションで、[Prefix Digits] を [+] に設定します。

これで、トランスレーション パターンにより、これらの電話機に割り当てられたパーティションを含む CSS にコールがルーティングされます。

詳細については、「ERL のルート パターンの作成」（P.3-11）および「ELIN のトランスレーション パターンの作成」（P.3-13）を参照してください。

CHAPTER 4

Cisco Emergency Responder 8.6 の設定

Cisco Emergency Responder（Emergency Responder）のインストール、および Cisco Unified Communications Manager（Cisco Unified CM）の設定後に、緊急コールの管理を開始するように Emergency Responder を設定できます。

次のトピックでは、Emergency Responder 8.6 を設定する方法について説明します。

Cisco Emergency Responder 設定の概要

Emergency Responder 8.6 は、拡張管理 Web サイト インターフェイス、ロールベースのユーザ管理、およびユーティリティのアップロード/ダウンロードなど、いくつかの機能を提供します。

次のトピックでは、Emergency Responder の設定について概説します。

（注） Emergency Responder 8.6 は Cisco EnergyWise と互換性があります。これには、電源の切れている電話機のユーザ アクティビティを検出するプロビジョニングが含まれます。

Cisco Emergency Responder Web サイト インターフェイス

Emergency Responder 8.6 は、システムの異なる部分のアクセスおよび使用を可能にするいくつかの Web サイトを提供します。メインの Emergency Responder 8.6 Web ページから、次の領域にアクセスできます。

- Cisco ER Serviceability
- Cisco ER Administration（デフォルト ホーム）
- Cisco Unified OS Administration
- Disaster Recovery System
- Emergency Responder User
- Emergency Responder Admin Utility

これらの各 Web サイトを使用すると、システムの異なる部分へのユーザ アクセスが可能になり、別のログインおよびパスワードが必要になります。これらの Web サイトへのアクセスは、ロールベースのユーザ管理メカニズムにより制御します（詳細は、「ロールベースのユーザ管理」（P.4-2）を参照）。

Emergency Responder 8.6 システムが初めてインストールされると、デフォルトの Emergency Responder Administrator ユーザが作成されます。デフォルト Administrator は Cisco Unified OS Administration および Disaster Recovery System Web サイト以外のすべての Web サイトへのフル アクセスを持ち、ユーザ、ロール、およびユーザ グループを作成できます。デフォルトの Administrator は、システムから削除できません。

関連項目

- 付録 A「Cisco Emergency Responder の管理 Web インターフェイス」
- 付録 B「Cisco Emergency Responder のサービスアビリティ Web インターフェイス」
- 付録 C「Cisco Emergency Responder の Cisco Unified Operating System Administration Web インターフェイス」
- 付録 D「Cisco Emergency Responder の Disaster Recovery System Web インターフェイス」

ロールベースのユーザ管理

Emergency Responder 8.6 では、ロールベースのユーザ管理システムが使用されます。次のトピックでは、このシステムについて説明します。

- 「ユーザ管理」（P.4-2）
- 「ロールの管理」（P.4-3）
- 「ユーザ グループ管理」（P.4-5）

ユーザ管理

インストールで、システムはデフォルトのユーザ Emergency Responder Administrator を作成します。Emergency Responder Administrator は Platform Administration および Disaster Recovery System 画面以外のすべてのシステム管理画面にアクセスできます。デフォルトでは、Emergency Responder Administrator ユーザは、Emergency Responder System Administrator、Emergency Responder Serviceability、Emergency Responder Admin Utility、および Emergency Responder User ユーザ グループに割り当てられ、Emergency Responder System Admin、Emergency Responder Serviceability、Emergency Responder Admin Utility、および Emergency Responder User ロールに定義されたリソースにアクセスできます。

（注）　デフォルトの Emergency Responder Administrator ユーザは削除できません。

追加ユーザは追加できます。追加ユーザが追加されたら、ユーザ グループに割り当てます。新規ユーザは、そのユーザ グループに定義されているロールを継承します。

関連項目

- 「Cisco Emergency Responder ユーザの管理」（P.4-10）
- 「Find and List Users」（P.A-64）

ロールの管理

インストールで、システムは 6 つのデフォルト ロールを作成します。表 4-1 に、デフォルト ロールのリストと説明を示します。

（注）　デフォルト ロールは削除できません。

表 4-1　デフォルト ロール

ロール	説明
Emergency Responder System Admin	すべてのシステム管理画面にアクセスできます。
Emergency Responder Serviceability	すべてのサービスアビリティ画面にアクセスできます。
Emergency Responder Admin Utility	すべての Admin Utility 画面にアクセスできます。
Emergency Responder Network Admin	Cisco Unified Communications Manager、LAN スイッチ、および SNMP 設定画面にアクセスできます。
Emergency Responder ERL Admin	すべての ERL 関連の画面にアクセスできます。
Emergency Responder User	ユーザ画面にアクセスできます。

新しいロールを作成または既存のロールを変更した場合、ロールに割り当てられているシステム リソースを指定します。リソースは、Emergency Responder 8.6 Administration Web サイトの Web ページまたはメニュー項目と同じものです。たとえば、[Find and List Roles] Web ページは、[User Management]>[Role] メニュー項目であるため、リソースです。

表 4-2 に、各デフォルト ロールに使用できるリソースを示します。

（注）　一部のリソースは、メニュー項目のグループです。たとえば、Cisco ER Serviceability Web サイトの [Logs] メニューは 1 つのリソースですが、複数のサブメニューを含んでいます。

表 4-2　デフォルト ロールに割り当てられたリソース

リソース	Emergency Responder System Admin	Emergency Responder Network Admin	Emergency Responder ERL Admin	Emergency Responder Serviceability	Emergency Responder Admin Utility	Emergency Responder User
Add Subscriber	x					
Admin Utility	x					
ALI Formatting Tool	x					
All Logs				x		
Application User	x					
Call History	x					
Cisco Unified CM Details	x	x				
Emergency Responder Groups in Cluster	x					
Change Cisco Unified CM Version					x	
Cluster DBHost Setting					x	
Control Center				x		
CPU and Memory Usage				x		
Device SNMP Settings	x	x				
Disk Usage				x		
ERL	x		x			
ERL Audit Trail	x					
ERL Debug Tool	x					
ERL Migration	x		x			
Event Viewer				x		
File Management Utility	x					
Functional role	x					
Intrado ERL	x		x			
Intrado VUI Settings	x					
IP subnet	x		x			
License Management	x					
Mail Alert Configurations	x					
Manually Configured Phones	x		x			
MIB2 System Group Configuration				x		
Off-Premises ERL	x		x			
Onsite Contact	x		x			
Pager Alert Configurations	x		x			
Phone Search						x

表 4-2　デフォルト ロールに割り当てられたリソース（続き）

リソース	Emergency Responder System Admin	Emergency Responder Network Admin	Emergency Responder ERL Admin	Emergency Responder Serviceability	Emergency Responder Admin Utility	Emergency Responder User
Point to New Publisher					x	
Processes				x		
PS ALI Convert	x					
PS ALI Export	x					
Purge	x					
Run Tracking	x	x				
Tracking Schedule	x	x				
Server	x					
Server Group	x					
LAN Switches	x	x				
SNMP V1/V3c Configuration				x		
SNMP V3 Configuration				x		
Switch Port	x		x			
Synthetic Phone	x		x			
Telephony	x					
Unlocated Phones	x		x			
User Call History						x
User Group	x					
Web Alert						x

関連項目

- 「Cisco Emergency Responder ロールの管理」（P.4-14）
- 「Find and List Roles」（P.A-68）

ユーザ グループ管理

インストールで、システムは 6 つのユーザ グループを作成します。表 4-3 にデフォルト ユーザ グループのリストと説明を示します。

（注）　デフォルト ユーザ グループは削除できません。

表 4-3　デフォルト ユーザ グループ

ユーザ グループ	説明
Emergency Responder System Administrator	割り当てられたシステム管理ロール
Emergency Responder Network Administrator	割り当てられたネットワーク管理ロール
Emergency Responder ERL Administrator	割り当てられた ERL 管理ロール
Emergency Responder Serviceability	割り当てられたサービスアビリティ ロール
Emergency Responder Admin Utility	割り当てられた Admin Utility ロール
Emergency Responder User	割り当てられたユーザ ロール

追加のユーザ グループを作成できます。ユーザ グループを作成するとき、そのグループにロールを割り当て、ユーザを追加します。複数のロールを単一のグループに割り当て可能です。グループ内のユーザは、グループに割り当てられたロールで定義されたすべてのリソースにアクセスできます。

関連項目

- 「Cisco Emergency Responder ユーザ グループの管理」（P.4-16）
- 「Find and List User Groups」（P.A-70）

アップロードおよびダウンロード ユーティリティの使用

Emergency Responder 8.6 にはダウンロードおよびアップロード ユーティリティが含まれており、csv ファイル形式でCisco ER サーバからローカル システムへ（ダウンロード）およびローカル システムから Cisco ER サーバへ（アップロード）バルク データを転送できます。

たとえば、データベースの詳細を csv ファイルにエクスポートし、次にその csv ファイルをローカル システムにダウンロードできます。ローカル システムでは、csv ファイルを変更して Cisco ER サーバにアップロードする、および csv ファイル内のデータを Cisco ER データベースにインポートすることができます。

表 4-4 にアップロードおよびダウンロード ユーティリティを使用し、各ページへのナビゲーション パスを指定する Cisco ER Administrative Web ページを示します。

（注）　xml、csv、lic、および txt の 4 つのファイル タイプのみアップロードできます。ファイル名には、スペースを含めることはできません。

表 4-4　アップロードおよびダウンロード ユーティリティを含む Administrative Web ページ

ページ名	ナビゲーション パス
Find Conventional ERL Data	[ERL]>[Conventional ERL]
Find Off-Premises ERL Data	[ERL]>[Off-premises ERL]>[Off-premises ERL(Search and List)]
Find Intrado ERLs Data	[ERL]>[Intrado ERL]>[Intrado ERL (Search and List)]
LAN Switch Details	[Phone Tracking]>[LAN Switch Details]

表 4-4　アップロードおよびダウンロード ユーティリティを含む Administrative Web ページ（続き）

ページ名	ナビゲーション パス
Switch Port Details	[ERL Membership]>[Switch Ports]
Find and List IP subnets	[ERL Membership]>[IP subnets]
Find and List Manually Configured Phones	[ERL Membership]>[Manually Configured Phones]

ファイルのダウンロード

Emergency Responder 8.6 サーバからローカル システムにファイルをダウンロードするには、次の手順を実行します。

手順

ステップ 1　表 4-4 に一覧表示されているいずれかのページで、[Export] をクリックします。[Export] ページが表示されます。

ステップ 2　以前にデータをファイルにエクスポートした場合、ステップ 3 に進みます。以前にデータをファイルにエクスポートしていない場合、[Select Export Format] プルダウン メニューを使用し、作成するファイルの名前を [Enter Export File Name] フィールドに入力します。[Export] をクリックします。データが指定のファイルにエクスポートされます。

ステップ 3　[Select a File to Download] プルダウン メニューを使用してダウンロードするファイルを選択してから、[Download] をクリックします。ファイルがローカル システムにダウンロードされます。

ファイルのアップロード

ローカル システムから Emergency Responder 8.6 サーバにファイルをアップロードするには、次の手順を実行します。

はじめる前に

手順を開始する前に、アップロードするファイルがローカル システムに存在することを確認してください。ファイルは、以前に Emergency Responder 8.6 サーバからダウンロードしたファイルであるか、作成したファイルであることが必要です。

手順

ステップ 1　表 4-4 に一覧表示されているいずれかのページで、[Import] をクリックします。[Import] ページが表示されます。

ステップ 2　[Upload] をクリックします。[Upload File] ページが表示されます。

ステップ 3　[Browse] をクリックし、アップロードするファイルを選択します。[Choose File] ウィンドウが開き、ファイルがローカル システムに表示されます。

ステップ 4　アップロードするファイルを選択し、[Open] をクリックします。アップロードするファイルのパス名は [Upload File] ページの [Select the file to be uploaded] フィールドに表示されます。

ステップ 5　[Upload] をクリックします。Cisco ER サーバにファイルがアップロードされます。これで、ファイルからデータをインポートできるようになります。

関連項目

- 「Conventional ERL」（P.A-17）
- 「LAN Switch Details」（P.A-44）
- 「Switch Port Details」（P.A-48）
- 「Find and List IP Subnets」（P.A-52）
- 「Find and List Manually Configured Phone」（P.A-58）
- 「File Management Utility」（P.A-82）

Cisco Emergency Responder 8.6 設定作業チェックリスト

このチェックリストは、Emergency Responder を設定するために完了する必要がある作業の情報、作業を完了できるユーザ タイプを詳細情報へのポインタとともに示します。

（注） 以下に示す作業の一部は、並行して進めることができます。

表 4-5　設定作業チェックリスト

作業	説明およびロケーション情報
システム管理者の作業	Emergency Responder ユーザおよびグループを作成して設定する。
組織で Cisco ER 管理に必要なユーザを作成する。	「Cisco Emergency Responder ユーザの管理」（P.4-10）と「Cisco Emergency Responder へのログインおよびログアウト」（P.4-19）を参照してください。
Emergency Responder グループを作成する。	「Cisco Emergency Responder サーバ グループの設定」（P.4-22）を参照してください。
Emergency Responder グループ テレフォニー設定を設定する。	「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）を参照してください。
Emergency Responder サーバを Emergency Responder グループに更新する。	「Cisco Emergency Responder サーバの設定」（P.4-25）を参照してください。
製品ライセンス キーをアップロードする。	「Cisco Emergency Responder ライセンス ファイルのアップロード」（P.4-25）を参照してください。
この Emergency Responder グループが処理する緊急コールの Cisco Unified CM クラスタを特定および設定する。 **（注）** この手順は、ネットワーク管理者が実行することもできます。	「Cisco Unified Communications Manager クラスタの指定」（P.4-26）を参照してください。
反復的なシステム管理作業を理解する。	「Cisco Emergency Responder システム管理者のロールについて」（P.10-4）を参照してください。
Intrado V9-1-1 for Enterprise Service を使用する場合、Intrado V9-1-1 for Enterprise Service をサポートするように Emergency Responder を設定する。	「Intrado VUI 設定の実行」（P.5-3）を参照してください。
構外ユーザをサポートする場合、Cisco Unified CM で AXL 認証情報を設定する。	「AXL 認証の設定」（P.5-11）を参照してください。
ネットワーク管理者の作業	スイッチを識別し、スイッチへの接続を設定する。
SNMP read コミュニティ ストリングを入力する。	「SNMP 接続の設定」（P.4-45）を参照してください。

表 4-5　設定作業チェックリスト（続き）

作業	説明およびロケーション情報
Emergency Responder がスイッチからの情報更新を行うスケジュールを定義する。	「電話機トラッキングとスイッチ更新スケジュールの定義」（P.4-47）を参照してください。
電話機が接続されたスイッチを識別する。	「LAN スイッチの指定」（P.4-48）を参照してください。
Emergency Responder がスイッチのポートを識別し、電話機が接続されているかどうかを判断できるようにスイッチ ポートと電話機の更新プロセスを実行する。	「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）を参照してください。
反復的なネットワーク管理作業を理解する。	「ネットワーク管理者のロールについて」（P.10-3）を参照してください。
ERL 管理者作業	オンサイト アラート（セキュリティ）担当者を確認し、Emergency Response Location（ERL; 緊急応答ロケーション）を作成して、それを電話機に割り当て、ALI データをサービス プロバイダーに送信します。ERL 管理の概要については、「ERL について」（P.4-30）および「ERL 管理の概要」（P.4-31）を参照してください。
Emergency Responder からのアラートを受信するオンサイト アラート（セキュリティ）担当者を特定する。	「セキュリティ担当者（オンサイト アラート担当者）の指定」（P.4-32）を参照してください。
ERL を作成します。	「ERL の作成」（P.4-33）を参照してください。
ERL をスイッチ ポートに割り当てる。 **（注）** この作業を実行するには、ネットワーク管理者がスイッチを追加し、スイッチ ポートおよび電話機の更新プロセスを実行する必要があります。	「スイッチ ポートの設定」（P.4-54）を参照してください。
Emergency Responder が直接にはサポートしていない電話機を追加する。 **（注）** Emergency Responder では、電話機の移動は自動的には追跡されません。	「電話機の手動での定義」（P.4-63）を参照してください。
位置未確認の電話機を特定し、ネットワーク管理者と連携して、Emergency Responder がこれらの電話機を認識しない問題を解決する。残っている ERL を電話機に割り当てる。	「位置未確認の電話の識別」（P.4-62）を参照してください。
ALI データをエクスポートし、サービス プロバイダーに送信する。転送要件を判断するには、サービス プロバイダーにお問い合わせください。	「ERL 情報のエクスポート」（P.4-41）と「サービス プロバイダー向け ALI 情報のエクスポート」（P.4-42）を参照してください。
反復的な ERL 管理作業を理解する。	「ERL 管理者のロールについて」（P.10-2）を参照してください。
次の作業は、Intrado V9-1-1 for Enterprise Service とともに Emergency Responder を使用する場合に必要になります。	
Intrado ERL を作成し、その Intrado ERL の ALI データの Intrado TN データベースに対する妥当性および整合性を確認する。	「Intrado ERL の設定」（P.5-5）を参照してください。「ALI の不一致の調整」（P.5-6）も参照してください。

表 4-5　設定作業チェックリスト（続き）

作業	説明およびロケーション情報
Intrado ERL をスイッチ ポート、IP サブネット、および位置未確認の電話機に割り当てます。	ERL のスイッチ ポートへの割り当てについては、「スイッチ ポートの設定」（P.4-54）を参照してください。 ERL の IP サブネットへの割り当てについては、「IP サブネットベースの ERL の設定」（P.4-38）を参照してください。 ERL の位置未確認の電話機への割り当てについては、「位置未確認の電話の識別」（P.4-62）を参照してください。
構外ユーザをサポートする場合、Off-Premise ERL を作成し、IP サブネット、および位置未確認の電話機に割り当てます。 （注）　Off-Premise ERL をスイッチ ポートに割り当てることはできません。	Off-Premise ERL の作成については、「Off-Premise ERL の設定」（P.5-11）を参照してください。 ERL の IP サブネットへの割り当てについては、「IP サブネットベースの ERL の設定」（P.4-38）を参照してください。 ERL の位置未確認の電話機への割り当てについては、「位置未確認の電話の識別」（P.4-62）を参照してください。

Cisco Emergency Responder ユーザの管理

Emergency Responder 8.6 をインストールすると、システムには 1 つのデフォルト Emergency Responder Administrator ユーザが定義されます（詳細は「ユーザ管理」（P.4-2）を参照）。追加ユーザを定義したり、既存ユーザを変更したりすることもできます。

次のトピックでは、新規ユーザを追加する方法と、既存ユーザを変更または削除する方法について説明します。

- 「ユーザの追加」（P.4-10）
- 「ユーザの変更」（P.4-11）
- 「ユーザの削除」（P.4-13）
- 「一括でのユーザのリモートへの変更」（P.4-14）

ユーザの追加

システムに追加ユーザを追加し、そのユーザをユーザ グループに割り当てることができます。新規ユーザのセキュリティ レベルは、割り当てたユーザ グループによって決まります。

Emergency Responder 8.6 では、ユーザはローカル ユーザまたはリモート ユーザとして追加できます。リモート ユーザは、認証に Cisco Unified CM クレデンシャルまたは Active Directory クレデンシャルを使用する必要があります。

ユーザは、単一の Emergency Responder グループ内にあるプライマリ サーバとスタンバイ サーバのいずれかに追加できます。アクセス許可は 2 つのサーバに定義されているユーザ グループの組み合わせに基づいて行われるため、プライマリ サーバにのみ定義されているユーザは、バックアップ サーバにログインできます。

はじめる前に

各セキュリティ レベルのユーザのリストを作成します。すべてのオンサイト アラート担当者のユーザ名を把握する必要があります。また、それぞれの管理セキュリティ レベルへのアクセス権を付与するユーザを決定する必要があります。

ユーザを追加するには、次の手順を実行します。

（注）　この手順を使用して、ユーザの追加または削除を使用できます。ただし、Emergency Responder のインストール時に作成した管理ユーザは削除できません。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスから、[User Management]>[User] を選択します。

[Find and List Users] ページが表示されます。

ステップ 2　[Add New User] ボタンをクリックします。[User Configuration] ページが表示されます。

ステップ 3　[User Name]、[Authentication Mode]、[Password]、[Confirm Password]、[Cisco Unified CM Cluster] フィールドに、必要な情報を入力します。

ステップ 4　[Insert] をクリックします。

ステップ 5　ユーザを追加するには、これらの手順を繰り返します。

ステップ 6　セキュリティ レベルを新規ユーザに割り当てるには、ユーザを 1 つ以上のユーザ グループに追加する必要があります。詳細については、「Cisco Emergency Responder ユーザ グループの管理」（P.4-16）を参照してください。

ステップ 7　Emergency Responder サーバ グループの他の Emergency Responder サーバでこの手順を繰り返します。

（注）　グループからユーザを削除するには、プライマリ サーバおよびスタンバイ サーバの両方でグループからユーザを削除する必要があります。

ユーザの変更

ユーザを作成すると、次のことが実行できます。

- ユーザの認証モードの変更
- ローカル ユーザのパスワードの変更
- リモート ユーザの Cisco Unified CM Cluster の変更

ユーザの認証モードの変更

ユーザの認証モードを変更するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスから、[User Management]>[User] を選択します。

[Find and List Users] ページが表示されます。

ステップ 2　変更する特定のユーザを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのユーザを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 3　ユーザ名をクリックします。

ステップ 4　[User Configuration—Modify User] ページが表示されます。

ステップ 5　ユーザに割り当てる認証モードをドロップダウン ボックスから選択します。

- 認証モードとして [Remote] を選択した場合は、ドロップダウン ボックスから [Cisco Unified CM Cluster] を選択します。
- 認証モードとして [Local] を選択した場合は、パスワードを入力し、確認用にもう一度パスワードを入力します。

ステップ 6　[Update] をクリックします。

ローカル ユーザのパスワードの変更

ローカル ユーザのパスワードを変更するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスで、[User Management] > [User] を選択します。

[Find and List Users] ページが表示されます。

ステップ 2　変更する特定のユーザを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのユーザを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 3　ユーザ名をクリックします。

ステップ 4　ユーザの設定に使用する [Modify User] ページが表示されます。

ステップ 5　ユーザに割り当てる認証モードをドロップダウン ボックスから選択します。

認証モードとして [Local] を選択した場合は、新しいパスワードを入力し、確認用にもう一度新しいパスワードを入力します。

ステップ 6　[Update] をクリックします。

リモート ユーザの Cisco Unified CM Cluster の変更

Emergency Responder 8.6 では、既存のリモート ユーザの Cisco Unified CM クラスタを別の Cisco Unified CM クラスタに変更できます。

リモート Cisco Unified CM クラスタを変更するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスから、[User Management]>[User] を選択します。

[Find and List Users] ページが表示されます。

ステップ 2　変更する特定のユーザを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのユーザを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 3　認証モードとして [Remote] を選択した場合は、ドロップダウン ボックスから [Cisco Unified CM Cluster] を選択します。

ステップ 4　[User Configuration—Modify User] ページが表示されます。

ステップ 5　すべてのリモート ユーザの新しい Cisco Unified CM クラスタを選択します。

ステップ 6　[Update] をクリックします。

ユーザの削除

Emergency Responder 8.6 では、単一ユーザの削除や複数ユーザの一括削除など、バッチ処理を実行できます。

単一ユーザを削除、または複数のユーザを一括削除するには、次の手順を実行します。

（注）　Emergency Responder のインストール時に作成したデフォルトの管理ユーザは削除できません。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスから、[User Management]>[User] を選択します。

[Find and List Users] ページが表示されます。

ステップ 2　削除する特定のユーザを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのユーザを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 3　削除するユーザを見つけ、そのユーザの [Delete] アイコンをクリックします。

削除を確認する警告が表示されます。

ユーザを一括して削除するには、同様に、ローカルとリモートの両方のリストから複数のユーザを選択して（チェックボックスをオンにします）、[Delete Users] ボタンをクリックします。

削除を確認する警告が表示されます。

ステップ 4　[OK] をクリックします。システムからユーザが削除され、そのユーザに対するすべてのユーザ グループ アソシエーションが削除されます。

関連項目

- 「Cisco Emergency Responder へのログインおよびログアウト」（P.4-19）
- 「Cisco Emergency Responder のためのユーザの準備」（P.10-1）

一括でのユーザのリモートへの変更

Emergency Responder 8.6 では、ユーザはローカルまたはリモートに変更できます。リモート ユーザは、Cisco Unified CM クラスタを使用して、認証されます。

（注）　このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

ユーザの認証モードを変更するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスで、[User Management] > [User] を選択します。

[Find and List Users] ページが表示されます。

ステップ 2　削除する特定のユーザを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのユーザを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 3　ユーザ名をクリックします。ユーザの設定に使用する [Modify User] ページが表示されます。

ステップ 4　ユーザに割り当てる認証モードを選択します。ローカル ユーザをリモート ユーザに変更できます。

ステップ 5　ユーザをリモート ユーザに変更した場合は、ドロップダウン ボックスから [Cisco Unified CM Cluster] を選択します。

ステップ 6　[Update] をクリックします。

（注）　一括でユーザを変更するには、変更するユーザをチェックボックスで選択し、[Change to Remote Users] ボタンをクリックします。前述のステップ 6 で説明したように、ドロップダウン ボックスから [Cisco Unified CM] を選択します。

Cisco Emergency Responder ロールの管理

Emergency Responder 8.6 をインストールすると、システムには 6 つのデフォルト ロールが定義されます（デフォルト ロールの詳細については、「ロールの管理」（P.4-3）を参照してください）。追加ロールを定義したり、既存ロールを変更したりすることもできます。

次のトピックでは、新規ロールを追加する方法と、既存ロールを変更または削除する方法について説明します。

ロールの追加

システムに追加ロールを追加し、そのロールにリソースを割り当てることができます。

（注）　デフォルト ロールを削除または変更することはできません。

はじめる前に

はじめる前に、作成する追加ロールを決定し、既存のデフォルト ロールが要求を満たしているかどうかを判断する必要があります。

新規ロールを追加するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスから、[User Management]>[Roles] を選択します。

[Find and List Roles] ページが表示されます。

ステップ 2　[Add a New Role] をクリックします。

[Role Configuration] ページが表示されます。

ステップ 3　テキストボックスに、[Role Name]（必須）と [Description]（任意）を入力します。

ステップ 4　リソースのリストで、新しいロールにアクセス権を付与するリソースの隣にあるチェックボックスをオンにします。

ステップ 5　[Insert] をクリックし、新しいロールをシステムに追加します。

ステップ 6　新規ロールが正常に追加されたことを確認するには、[User Management]>[Roles] ページに戻ってロール検索を実行します。作成した特定のロールを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのロールを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。新規ロールがリストに表示されていることを確認します。

ロールの変更

既存ロールを変更するには、次の手順を実行します。

（注）　デフォルト ロールは変更できません。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスから、[User Management]>[Roles] を選択します。

[Find and List Roles] ページが表示されます。

ステップ 2　変更する特定のロールを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのロールを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 3　ロール名をクリックします。

[Role Configuration—Modify Role] ページが表示されます。

ステップ 4　必要に応じて、テキストボックスで [Role Name] と [Description] を変更します（表示されている場合）。

ステップ 5　リソースのリストで、変更したロールにアクセス権を付与するリソースの隣にあるチェックボックスをオンまたはオフにします。

ステップ 6　システムに更新したロール情報を追加するには、[Update] をクリックします。

ステップ 7　新規ロールが正常に変更されたことを確認するには、[User Management]>[Roles] ページに戻ってロール検索を実行します。変更した特定のロールを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのロールを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。ロール名をクリックし、変更されたロール情報が [Role Configuration—Modify Role] ページに表示されたことを確認します。

ロールの削除

既存ロールを削除するには、次の手順を実行します。

（注）　標準ロールは削除できません。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスから、[User Management]>[Roles] を選択します。

[Find and List Roles] ページが表示されます。

ステップ 2　削除する特定のロールを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのロールを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 3　削除するロールの [Delete] アイコンをクリックします。

ロールの削除を確認する警告メッセージが表示されます。

ステップ 4　ロールを削除するには、[OK] をクリックします。

[Find and List Roles] ページが更新され、ロールは [Role Names] リストに表示されなくなります。

Cisco Emergency Responder ユーザ グループの管理

Emergency Responder 8.6 をインストールすると、システムには 6 つのデフォルトのユーザ グループが定義されます（デフォルトのユーザ グループの詳細については、「ユーザ グループ管理」（P.4-5）を参照してください）。追加ロールを定義したり、既存ユーザ グループを変更したりすることもできます。

次のトピックでは、新規ユーザ グループを追加する方法と、既存ユーザ グループを変更または削除する方法について説明します。

- 「ユーザ グループの追加」（P.4-17）
- 「ユーザ グループの変更」（P.4-18）
- 「ユーザ グループの削除」（P.4-18）

ユーザ グループの追加

システムにユーザ グループを追加し、それぞれの新規ユーザ グループにユーザおよびロールを割り当てることができます。

はじめる前に

はじめる前に、作成する追加ユーザ グループを決定し、既存のデフォルト ユーザ グループが要求を満たしているかどうかを判断する必要があります。

新規ユーザ グループを追加するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスから、[User Management] > [User Group] を選択します。

[Find and List User Groups] ページが表示されます。

ステップ 2　[Add a User Group] をクリックします。

[User Group Configuration—Add User Group] ページが表示されます。

ステップ 3　テキストボックスに、[User Group Name]（必須）と [Description]（任意）を入力します。

ステップ 4　[Add Users] をクリックします。

[User Names] ページが表示されます。

ステップ 5　特定のユーザを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのユーザを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 6　追加したユーザ名の左側にあるチェックボックスをオンにし、[Add] をクリックします。

[User Name] ページが閉じ、追加した名前が [Configuration—Add User Group] ページの [Add User to Group] テキストボックスに表示されます。

（注）　リストからユーザを削除するには、ユーザ名を選択して [Remove Users] をクリックします。

ステップ 7　[Add Roles] をクリックします。

[Role Names] ページが表示されます。

ステップ 8　特定のロールを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのロールを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 9　追加したロールの左側にあるチェックボックスをオンにし、[Add] をクリックします。

[Role Names] ページが閉じ、追加されたロールが [User Group Configuration] ページの [Add Roles to Group] テキストボックスに表示されます。

（注）　リストからロールを削除するには、ユーザ名を選択して [Delete Roles] をクリックします。

ステップ 10　[Insert] をクリックし、新しいロールをシステムに追加します。

ユーザ グループの変更

既存ユーザ グループを変更するには、次の手順を実行します。

（注）　デフォルト ユーザ グループは変更できません。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスから、[User Management]>[User Group] を選択します。

[Find and List User Groups] ページが表示されます。

ステップ 2　変更する特定のユーザ グループを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのユーザ グループを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 3　ユーザ グループ名をクリックします。

[User Group Configuration—Modify User Group] ページが表示されます。

ステップ 4　必要に応じて、[Description] テキストボックスでユーザ グループ（表示されている場合）の説明を変更します。

ステップ 5　[Add Users to Group] テキストボックスには、対象のユーザ グループに現在割り当てられているユーザの名前が表示されます。追加ユーザを追加するには、「ユーザ グループの追加」（P.4-17）の手順に従います。

ユーザを削除するには、ユーザの名前を強調表示し、[Remove Users] をクリックします。

ステップ 6　[Assign Roles to Group] テキストボックスには、対象のユーザ グループに現在割り当てられているロールの名前が表示されます。追加ロールを追加するには、「ロールの追加」（P.4-14）の手順に従います。

ロールを削除するには、ロールの名前を強調表示し、[Remove Roles] をクリックします。

ステップ 7　完了したら、[Update] をクリックし、更新したユーザ グループをシステムに保存します。

ステップ 8　ユーザ グループが正常に変更されたことを確認するには、[User Management]>[User Group] ページに戻って検索を実行します。変更した特定のユーザ グループを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのユーザ グループを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。ユーザ グループ名をクリックし、変更されたユーザ グループ情報が [User Group Configuration—Modify User Group] ページに表示されます。

ユーザ グループの削除

既存ユーザ グループを削除するには、次の手順を実行します。

（注）　デフォルト ユーザ グループは削除できません。削除できるのは、作成したユーザ グループだけです。

手順

ステップ 1　Emergency Responder Administration Web インターフェイスから、[User Management]>[User Group] を選択します。

[Find and List User Groups] ページが表示されます。

ステップ 2　削除する特定のユーザ グループを見つけるための検索条件を入力し、[Find] をクリックします。または、設定したすべてのユーザ グループを表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 3　削除するユーザ グループの [Delete] アイコンをクリックします。

（注）　デフォルト ユーザ グループは削除できません。削除できるのは、作成したユーザ グループだけです。

ユーザ グループの削除を確認する警告メッセージが表示されます。

ステップ 4　ユーザ グループを削除するには、[OK] をクリックします。

[Find and List Roles] ページが更新され、削除したユーザ グループは [User Groups] リストに表示されなくなります。

Cisco Emergency Responder へのログインおよびログアウト

システム設定を表示または変更するには、Emergency Responder Web インターフェイスにログインする必要があります。システム管理者は、ロールベースのユーザ管理メカニズムを使用してアクセスを制御します。詳細については、「ロールベースのユーザ管理」（P.4-2）を参照してください。

はじめる前に

Emergency Responder にログインするには、有効なユーザ ID とパスワードが必要です。インターフェイスにログインできず、管理作業を行うためのアクセス権が必要な場合は、中心的な Cisco ER 管理者に問い合わせてください。

Emergency Responder にログインするには、次の手順を実行します。

手順

ステップ 1　サポートされるブラウザを使用して、http://*servername*/ceradmin を開きます。ここで、servername は Emergency Responder サーバの DNS 名または IP アドレスです。

ブラウザで [Emergency Responder Server Administration] ページが開きます。

ステップ 2　[Navigation] プルダウン メニューを使用して、ログインする Web サイトを選択します。Emergency Responder Web サイトには、次の領域があります。

- Emergency Responder Serviceability
- Emergency Responder Administration
- Cisco Unified OS Administration
- Disaster Recovery System
- Emergency Responder User
- Emergency Responder Admin Utility

ログイン ページを開くには、いずれかのリンクをクリックします。

ステップ 3　[Go] をクリックします。

選択した Web サイトのログイン画面が表示されます。

ステップ 4　ユーザ名とパスワードを入力し、[Login] をクリックします。

選択した Web サイトへのログインが行われます。システム管理者としてログインする場合を除き、メニューの一部のコマンドにロック アイコンが表示されることがあります。このロック アイコンは、付与されている承認レベルが理由で表示できないページであることを示します。

操作完了後、ログアウトするには、メニュー バーの上にある [Logout] をクリックします。

（注）　Emergency Responder 8.5 以降では、ユーザ名の検証では大文字と小文字は区別されません。

関連項目

- 「Cisco Emergency Responder ユーザの管理」（P.4-10）
- 「Cisco Emergency Responder ロールの管理」（P.4-14）
- 「Cisco Emergency Responder ユーザ グループの管理」（P.4-16）
- 「Cisco Emergency Responder のためのユーザの準備」（P.10-1）

同時セッション数の制限

Emergency Responder では、管理者は、任意のユーザに対して一度にアクティブにできる同時セッションの最大数を制限できます。この制限が有効になっていると、管理者は許可される同時セッションの数の最大数（1 ～ 15）を指定できます。

この制限は、Emergency Responder に設定されているすべてのユーザに適用されます。

ユーザは、指定された数を超える同時セッションを確立できなくなります。制限を超える数の同時セッションを追加で確立しようとしたユーザは、Emergency Responder にログインできなくなり、「Session limit exceeded. Please log out of any existing sessions and try again」というエラー メッセージが表示されます。

（注）　この制限は、Emergency Responder の制限を超えてセッションを追加したすべてのユーザに適用されます。

（注）　この制限は、各 Emergency Responder Web サイトに対して個別に強制されます。
– Emergency Responder Administration
– Emergency Responder Serviceability
– Emergency Responder User
– Emergency Responder Admin Utility

警告　**ユーザが Emergency Responder Web サイトにログインし、ログアウトせずにブラウザを閉じた場合、そのセッションは 30 分後にタイムアウトになるまでアクティブのまま維持されます。この間にユーザが事前設定された制限を超えて追加のセッションを確立しようとしても、その操作は成功しません。**

はじめる前に

Emergency Responder サーバ グループを設定するには、システム管理者権限が必要です。

Emergency Responder サーバ グループを設定するには、次の手順を実行します。

手順

ステップ 1　[System]>[Cisco ER Group Settings] を選択します。

[Emergency Responder Group Settings] ページが開きます。

ステップ 2　[Limit Concurrent Sessions] チェックボックスをオンにします。このチェックボックスによって、同時セッション数の制限が有効になり、[Max. number of concurrent sessions] ドロップダウン ボックスで選択できるようになります。

ステップ 3　Emergency Responder ユーザに適用する同時セッションの最大数を [Max. number of concurrent sessions] ドロップダウン ボックスで選択します。

ステップ 4　新しい変更を適用するには、[Update Settings] ボタンをクリックします。

（注）　同時セッションの最大数の設定を無効にするには、[System] > [Emergency Responder Group Settings] の順に選択し、[Limit Concurrent Sessions] チェックボックスをオフにします。

関連項目

- 「Cisco Emergency Responder Group Settings」（P.A-3）

サーバおよびサーバ グループの設定

次のトピックでは、Emergency Responder サーバおよびサーバ グループを設定する方法と、Emergency Responder グループと Cisco Unified CM 間のテレフォニー接続について説明します。

- 「Cisco Unified Communications Manager クラスタの指定」（P.4-26）

Cisco Emergency Responder サーバ グループの設定

Emergency Responder サーバ グループを設定するには、グループに含めるいずれかのサーバの管理インターフェイスに接続する必要があります。Emergency Responder サーバ グループは、最大 2 つの Emergency Responder サーバ（プライマリ サーバとスタンバイ サーバ、またはバックアップ サーバ）で構成されます。この冗長性により、いずれかのサーバが使用できなくなった場合でも Emergency Responder を継続して利用できるようにします。

1 つのグループ内に 2 つのサーバを配置し、WAN リンクは分断せず、物理的な位置を別個にすることを検討してください。このような構成では、片方のサーバに火災、洪水、ネットワーク中断などの問題が生じた場合でも、他方のサーバには影響しません。詳細については、「データの整合性および信頼性に関する考慮事項」（P.1-18）を参照してください。

はじめる前に

Emergency Responder サーバ グループを設定するには、システム管理者権限が必要です。

Emergency Responder サーバ グループを設定するには、次の手順を実行します。

手順

ステップ 1　[System]>[Cisco ER Group Settings] を選択します。

[Emergency Responder Group Settings] ページが開きます。

ステップ 2　「Cisco Emergency Responder Group Settings」（P.A-3）で説明したように、グループ設定を入力します。多くのフィールドには、大部分のネットワークで有効なデフォルトが設定されています。少なくとも、以下のフィールドは設定する必要があります。

- [Cisco ER Group Name]：グループの名前を入力します。この名前はシステムを使用するときに使われるため、わかりやすい名前を選択してください。
- [SMTP Mail Server] および [Source Mail ID]：Emergency Responder システム管理者やオンサイト アラート担当者（セキュリティ）に電子メール アラートが送信されるようにする場合は、メール サーバの IP アドレスまたは DNS 名、および電子メールの送信に使用するサーバのアカウント名を入力します。オンサイト アラート担当者の電子メール アドレスを設定すると（「セキュリティ担当者（オンサイト アラート担当者）の指定」（P.4-32）を参照）、担当者が割り当てられている領域で緊急コールが発生したときにこのアカウントから電子メール アラートが送信されます。電子メール アドレスが、電子メールベースのポケットベルの場合、ポケットベルが使用されます。
- [System Administrator Mail ID]：緊急なエラーの場合に電子メール アラートを送信するときは、システムの連絡先の電子メール アカウント情報を入力します。
- [Calling Party Modification flag]：Emergency Responder を Cisco Call Manager ユーザとして作成した場合、[Calling Party Modification] を有効にしたときは、このフラグを設定する必要があります。
- [Enable Syslog] および [Syslog Server]：CiscoWorks2000 をネットワーク管理ソフトウェアとして使用しているときは、syslog コレクタにログ メッセージを送信するように Emergency Responder を設定できます。syslog コレクタを使用するには、[Enable Syslog] を選択し、syslog サーバの完全修飾 DNS 名を入力します。
- [Security end user web interface language]：ページをフランス語（カナダ）で表示するには、ドロップダウン ボックスからこの言語を選択します。デフォルトの言語は英語です。

ステップ 3　設定が完了したら、[Update Settings] をクリックします。

Emergency Responder グループが作成されます。

関連項目

- 「Cisco Emergency Responder サーバの設定」（P.4-25）
- 「Cisco Emergency Responder Group Settings」（P.A-3）
- 「syslog からの情報収集」（P.11-33）

Cisco Emergency Responder サーバのグループ テレフォニー設定

Emergency Responder に緊急コールや ELIN に使用する電話番号を通知するには、テレフォニーを設定する必要があります。

はじめる前に

テレフォニーを設定するには、システム管理者権限が必要です。

これらの設定を行う前に、Cisco Unified CM で必要なルート ポイントおよびルート パターンを作成します。詳細については、次のトピックを参照してください。

- 「緊急コールのルート ポイントの作成」（P.3-6）
- Creating the Route Patterns for ELINs, page 4-10
- 「Cisco Emergency Responder グループ間の通信に対するルート パターンの作成」（P.3-19）

テレフォニーを設定するには、次の手順を実行します。

手順

ステップ 1　[System]>[Telephony Settings] を選択します。

[Telephony Settings] ページが開きます。

ステップ 2　「Telephony Settings」（P.A-5）に説明されているとおり、テレフォニー設定を入力します。

- [UDP Port Begin]：Emergency Responder の最初の UDP ポートは電話に使用できます。32000 などです。
- [Inter Cisco ER Group Route Pattern]：他の Emergency Responder グループがこのグループに緊急コールをルーティングするために使用するルート パターン（1000.911 など）。
- [PSAP Callback Route Point Pattern]：PSAP からのコールを受け取るために作成した CTI ルート ポイント。913XXXXXXXXXX（913 の後ろに 10 個の X）などです。
- [ELIN Digit Strip Pattern]：ELIN を表示するために PSAP コールバック ルート ポイントから受け取った数字。913 などです。
- [Route Point for Primary Cisco ER Server]：使用する Emergency Responder プライマリ サーバ用に作成したルート ポイント。711 などです。この数字は変更できます。「緊急電話番号の変更」（P.4-24）を参照してください。
- [Route Point for Standby Cisco ER Server]：使用する Emergency Responder スタンバイ サーバ用に作成したルート ポイント。912 などです。
- [IP Type of Service (00-FF)]：IP ヘッダーに含まれる Type of Service（TOS; タイプ オブ サービス）バイトの値。デフォルトの 0xB8 は、プライオリティ キューの TOS クラスを意味します。このデフォルト値は Emergency Responder 用として使用することをお勧めします。

- [Onsite Alert Prompt Repeat Count]：オンサイト セキュリティ電話機に表示するプロンプトの回数。
- [Intrado Route Pattern]：Intrado の Emergency Response Location（ERL; 緊急応答ロケーション）のルート パターン。

ステップ 3　変更を保存するには、[Update Settings] をクリックします。

緊急電話番号の変更

インストール時に [Route Point for Primary Cisco ER Server] フィールドに数字を入力して自動的に設定された緊急電話番号を設定または変更できます。緊急電話番号を設定または変更する前に、新しいルート ポイントを設定し、Cisco Unified CM の Cisco ER ユーザに関連付ける必要があります。

注意　緊急電話番号の変更は、混雑していない時間に行ってください。

緊急電話番号を変更するには、次の手順を実行します。

手順

ステップ 1　新規ルート ポイントを、Cisco Unified CM の Emergency Responder ユーザに関連付けます。「Cisco Emergency Responder Cisco Unified CallManager ユーザの作成」（P.3-21）を参照してください。

ステップ 2　新しい番号のルート ポイントを変更します。[Route Point for Primary Cisco ER Server] フィールドに番号を入力します。

ステップ 3　[Update Settings] をクリックします。

（注）　Cisco ER でサポートされる緊急電話番号は現在も 1 つだけです。番号を変更すると、Cisco ER は、新しい緊急電話番号ルート ポイントで受け取ったコールをルーティングするようになります。

関連項目

- 「Telephony Settings」（P.A-5）
- 「緊急コールのルート ポイントの作成」（P.3-6）
- 「ERL のルート パターンの作成」（P.3-11）
- 「Cisco Emergency Responder グループ間の通信に対するルート パターンの作成」（P.3-19）
- 「Cisco Unified Communications Manager クラスタの指定」（P.4-26）

Cisco Emergency Responder サーバの設定

Emergency Responder グループを作成すると（「Cisco Emergency Responder サーバ グループの設定」（P.4-22）を参照）、[Server Settings] ページを使用して Cisco ER サーバ設定の更新（サーバ名の変更、トレースおよびデバッグ設定の変更など）や、サーバの削除を実行できます。

はじめる前に

Cisco ER サーバの更新または削除を行うには、システム管理者権限が必要です。

Cisco ER サーバを設定するには、次の手順を実行します。

手順

ステップ 1　[System]>[Server Settings] を選択します。

[Server Settings] ページが開きます。

ステップ 2　サーバ設定（[Server Name]、[Debug Package List]、または [Trace Package List] の設定）を変更するには、左側の [Servers] リストでサーバ名を選択します。編集ボックスに、サーバの設定が読み込まれます。変更を加えて、[Update] をクリックします。

ステップ 3　グループからサーバを削除するには、サーバを選択して [Delete] をクリックします。ネットワークからサーバを完全に削除する場合は、コールが誤って転送されたりドロップされたりすることのないように、テレフォニー ネットワークに必要な変更を行ってください。

ステップ 4　設定が完了したら、[Update] をクリックします。

変更が保存され、ページ上部のサーバ リストに表示されます。

関連項目

- 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）
- 「Cisco Emergency Responder サーバ グループの設定」（P.4-22）
- 「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）
- 「Cisco Unified Communications Manager クラスタの指定」（P.4-26）
- 「Server Settings for Emergency ResponderServerGroup」（P.A-7）

Cisco Emergency Responder ライセンス ファイルのアップロード

サーバ グループのライセンス ファイルのアップロードには、2 つのオプションがあります。

- Emergency Responder 8.6 を使用するため、パブリッシャ用の有効なサーバ ライセンス ファイルと、サブスクライバ用の 2 番目のサーバ ライセンス ファイルをアップロードできます。
- パブリッシャとサブスクライバ用の独立したライセンスを注文する代わりに、2 つのノードを備えたサーバ グループのライセンスをアップロードすることもできます。

詳細については、「Cisco Emergency Responder 8.6 のライセンス」（P.1-4）を参照してください。

この手順を開始する前に、すべてのサーバおよびユーザのライセンス ファイルを用意してください。

（注）　必要なライセンス ファイルが明らかでない場合は、「ライセンス要件の決定」（P.1-6）を参照してください。

はじめる前に

[License Manager] ページにアクセスするには、システム管理者権限が必要です。

Cisco ER ライセンス ファイルをアップロードするには、次の手順を実行します。

手順

ステップ 1　Cisco ER Administration Web サイトから、[System]>[License Manager] を選択します。

[License Manager] ページが開きます。サーバのライセンスの詳細が表示されます。

ステップ 2　ライセンス ファイルをアップロードするサーバに基づいてプルダウン メニューからサーバ名を選択し、[Upload License] をクリックして追加のライセンス ファイルをアップロードします。

[Upload File] ページが表示されます。

ステップ 3　[Browse] ボタンを使用してアップロードするライセンス ファイル（Cisco.com で Cisco ER システムを登録した後に電子メールの添付ファイルとして受信したファイル）に移動し、ファイル名を選択して、[Open] をクリックします。

選択したファイル名が [Select file to be uploaded] テキストボックスに表示されます。

ステップ 4　[Upload] をクリックします。追加ライセンス ファイルのアップロードとインストールが実行されます。

（注）　[License Manager] ページに、次の情報が表示されます。

- サーバ グループのサーバ ライセンス情報。
- 統合ユーザ ライセンス情報（パブリッシャおよびサブスクライバ）

関連項目

- 「Cisco Emergency Responder 8.6 のライセンス」（P.1-4）
- 「License Manager」（P.A-9）

Cisco Unified Communications Manager クラスタの指定

設定している Cisco ER グループで管理する Cisco Unified CM クラスタごとに、1 つの Cisco Unified CM サーバを指定する必要があります。Cisco ER は、これらの Cisco Unified CM サーバに登録されている電話機リストを取得し、電話機の移動を追跡します。

Cisco ER 8.6 は、3 つのレベルの CTI フェールオーバーを提供します。3 つのレベルの CTI フェールオーバーを有効にするには、プライマリ CTI Manager、バックアップ CTI Manager 1、バックアップ CTI Manager 2 の IP アドレスまたは DNS 名を入力します。

はじめる前に

Cisco Unified CM クラスタを指定するには、システム管理者またはネットワーク管理者の権限が必要です。

Cisco ER がサーバから必要な情報を取得できるように、Cisco Unified CM クラスタ内の各 Cisco Unified CM サーバで、SNMP サービスを実行する必要があります。

これらの設定を行う前に、必要なユーザと CTI ポートを作成します。この情報は、Cisco ER が Cisco ER クラスタを使用してプロバイダーを作成しようとする前に整っている必要があります。Cisco ER は、プロバイダーの作成時にユーザに関連付けられている CTI ポートとルート ポイントのみを登録します。詳細については、次のトピックを参照してください。

- 「Cisco Emergency Responder Cisco Unified CallManager ユーザの作成」（P.3-21）
- 「必要な CTI ポートの作成」（P.3-8）

設定している Cisco ER グループで管理する Cisco Unified CM クラスタごとに、1 つの Cisco Unified CM サーバを指定するには、次の手順を実行します。

手順

ステップ 1　[Phone Tracking]>[Cisco Unified Communications Manager Details] を選択します。

Cisco Emergency Responder により、[Cisco Unified CM Details] ページが表示されます。

ステップ 2　Cisco Unified CM サーバの詳細を入力します。

- [Cisco Unified Communications Manager]：サーバの IP アドレスまたは DNS 名。このサーバでは、Cisco Unified CM と SNMP サービスを実行する必要があります。Cisco ER 設定では、同じ Cisco Unified CM クラスタ内に複数の Cisco Unified CM サーバを定義しないでください。
- [CTI Manager]：サーバが属するクラスタの CTI Manager の IP アドレスまたは DNS 名。
- [CTI Manager User Name]：Cisco Emergency Responder で作成したユーザ。詳細については、「Cisco Emergency Responder Cisco Unified CallManager ユーザの作成」（P.3-21）を参照してください。
- [CTI Manager Password]：ユーザのパスワード。
- [Backup CTI 1 Manager]:クラスタの最初のバックアップ CTI Manager の IP アドレスまたは DNS 名。
- [Backup CTI 2Manager]：クラスタの 2 番目のバックアップ CTI Manager の IP アドレスまたは DNS 名。
- [Telephony Port Begin Address]：Cisco ER を使用するために作成した一連のポートの最初の CTI ポート アドレス。詳細については、「必要な CTI ポートの作成」（P.3-8）を参照してください。
- [Number of Telephony Ports]：Cisco ER を使用するために作成した一連の CTI ポートの数。

ステップ 3　セキュアな JTAPI 通信を確立するには、次の手順を実行します。

a. [Enable Secure Connection] チェックボックスをオンにします。

b. 次の必須情報を入力します。

- TFTP Server IP Address
- TFTP Server Port

（注） [TFTP Server Port] フィールドには、デフォルト値が設定されます。Cisco Unified CM に [TFTP Server Port] フィールドとは異なる値を入力した場合は、このフィールドにはデフォルト値ではなく、Cisco Unified CM と同じ値を入力する必要があります。

- CAPF Server IP Address
- CAPF Server Port

（注）　[CAPF Server Port] フィールドには、デフォルト値が設定されます。Cisco Unified Communications Manager に [CAPF Server Port] フィールドとは異なる値を入力した場合は、このフィールドにはデフォルト値ではなく、Cisco Unified Communications Manager と同じ値を入力する必要があります。

- Instance ID for Publisher
- Secure Authentication String for Publisher
- Instance ID for Subscriber
- Secure Authentication String for Subscriber

（注）　Cisco Unified Communications Manager クラスタにも、セキュアな JTAPI 通信を設定する必要があります。詳細については、“Configuring JTAPI Security” section on page 4-20 を参照してください。

ステップ 4　[Insert] をクリックします。

Cisco ER により、サーバ リストに Cisco Unified CM サーバが追加されます。この Cisco ER グループで他の Cisco Unified CM クラスタをサポートしている場合は、この手順を繰り返します。

ヒント

- Cisco Unified CM サーバの設定を表示または変更するには、サーバ リストでサーバをクリックします。設定が編集ボックスに読み込まれます。設定を変更するには、編集して [Update] をクリックします。
- Cisco ER 設定から Cisco Unified CM サーバを削除するには、サーバ リストでサーバをクリックし、[Delete] をクリックします。

関連項目

- 「Cisco Unified Communications Manager Clusters」（P.A-41）

8.6 Cisco Emergency Responder クラスタおよびクラスタ DB ホスト

Cisco ER クラスタおよびクラスタ DB ホストを設定するには、次の手順を実行します。

手順

ステップ 1　次のことを確認します。

- すべての Cisco ER グループを Cisco ER クラスタに追加している
- いずれかの Cisco ER パブリッシャを「クラスタ DB ホスト」として設定している
- クラスタ間で、「クラスタ パスワード」として同じパスワードを使用している

ステップ 2　Cisco ER Admin Utility Web インターフェイスを使用して、[Update]>[ClusterDB Host] に移動し、ステップ 1 の値を入力します。

ステップ 3　クラスタ内の Cisco ER サーバ グループごとにステップ 1 と 2 を繰り返します。

ステップ 4　Cisco ER サービスを再起動します。

（注） Emergency Responder 8.6 サーバ グループが、Emergency Responder クラスタ内にある Emergency Responder サーバ グループの Cisco ER 1.3、2.x、7.1、および 8.0 以降のバージョンと通信できるようになります。

関連項目

- 「Update Cluster DB Host」（P.E-2）
- 「Cisco Emergency Responder クラスタ データベース ホストの詳細の更新」（P.9-2）

Cisco Emergency Responder で指定された Cisco Unified Communications Manager クラスタの変更

Emergency Responder で指定された Cisco Unified CM クラスタの変更やアップグレードを行った場合は、Admin Utility を使用して、新しいバージョンの Cisco Unified CM を Cisco ER に指定する必要があります。

Cisco ER に指定された Cisco Unified CM クラスタを別のバージョンに変更する方法については、「Cisco Unified Communications Manager のバージョンの変更」（P.9-1）を参照してください。

ERL の使用

Emergency Response Location（ERL; 緊急応答ロケーション）は、緊急コールが発生する領域を定義します。セキュリティ担当者および緊急応答チームは、ERL 情報を使用して緊急の発信者の場所を特定します。

（注） Cisco Unified CM 6.x では、IP 電話に新たな Do-Not-Disturb 機能が導入されました。オンサイト セキュリティ電話機として指定された電話機でこの機能が有効になっていると、Cisco ER から電話機に緊急アラートが送信されても、オンサイト セキュリティ担当者へのアラート通知は行われません。オンサイト アラート機能を搭載した電話機では、Do-Not-Disturb 機能を無効にすることが重要です。

Cisco Unified CM 7.x では、Do-Not-Disturb 機能が有効になっている電話機で、Cisco ER 8.6 からオンサイト セキュリティ担当者にアラートを通知する機能がサポートされています。

ERL の作成や変更を実行できるのは、Emergency Responder システム管理者または ERL 管理者です。この項では、ERL について詳述し、Cisco ER での使用方法を説明します。

- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）

- 「セキュリティ担当者（オンサイト アラート担当者）の指定」（P.4-32）
- 「ERL の作成」（P.4-33）
- 「ERL 情報のエクスポート」（P.4-41）
- 「ERL 情報のエクスポート」（P.4-41）
- 「ERL の監査証跡の表示」（P.4-43）

ERL について

Emergency Response Location（ERL; 緊急応答ロケーション）は、建物、建物内の領域、または屋外（電話機サービスを屋外にも広げている場合）で、これらの領域は緊急応答を行うための単一ロケーションとして扱われます。ERL 内のすべての電話は、同じロケーションからかかってきたものとして認識されます。

そのため、緊急コールが発生すると、Public Safety Answering Point（PSAP）とオンサイト アラート（セキュリティ）チームに ERL が通知されます。緊急時に、緊急コールの発信者の場所を特定する必要がある場合、応答チームは ERL 内にいる個人を見つけなければなりません。各スイッチ ポートの [Phone Location] フィールドを使用して、より詳細な情報を含めることができます。このレベルの詳細情報は、自動的に追跡される電話機でのみ利用可能で、オンサイト アラート担当者の [Web Alert] 画面にのみ表示されます。

この方法は、ホーム ユーザの緊急コールの取り扱い方法と同様です。つまり、緊急応答チームはコールの発信場所は把握しますが、発信者がわかるまで各部屋を探す必要があります。家が大きいほど、探す時間が長くなります。同様に、ERL の領域が広いほど、応答チームが緊急の発信者を見つけるまでの時間が長くなります。

ERL の広さに関する法は、地域によって異なります。責任を持って、現地法に基づいた ERL の設定を行ってください。電話機のサービス プロバイダーと連携して作業してください。現地法の理解につながります。ERL からのコールが適切な PSAP にルーティングされるように、最終的には ERL の Automatic Location Information（ALI）をサービス プロバイダーに送信する必要があります。

考えられる ERL について、いくつか例を示します。

- 25 階建ての建物があり、各フロアのオフィス スペースは 10,000 平方フィート（3,048 平方メートル）です。1 フロアにつき 1 つずつ、全部で 25 の ERL を作成できます。各フロアを 2 つに分割して、1 フロアにつき 2 つずつ、全部で 50 の ERL を作成する方が望ましいといえます。
- 5 つの建物があります。いずれも以前は居住用に使用されていました。広さは約 3000 平方フィート（914.4 平方メートル）です。一部は数階建てですが、1 つの建物につき 1 つずつ、全部で 5 つの ERL を作成できます。
- 5 階建ての建物がありますが、この建物は規模が大きく、各フロアに 100,000 平方フィート（30,480 平方メートル）のオフィス スペースがあります。1 フロアに 20 ERL ずつ、全部で 100 ERL を作成できます。1 つの ERL で約 5,000 平方フィート（15,240 平方メートル）をカバーします。
- 電話機を集中して配置していますが、現地法では、1 つの ERL に配置する電話機は 48 機以内にすることが求められています。この場合、物理的なスペースではなく、電話機の可能なサービスエリアに基づいてゾーンを定義する必要があります。物理ロケーションとして認識可能なゾーンを作成してください（BldJFloor5Row3 など）。

関連項目

- 「ERL 管理の概要」（P.4-31）
- 「ERL の作成」（P.4-33）
- 「ERL 情報のエクスポート」（P.4-41）

- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）
- 「緊急コールの発信時に発生するプロセス」（P.1-9）

ERL 管理の概要

ERL の有効なセットを構築するため、次の手順に従うことを検討してください。

1. 緊急コールの要件について、現地法をよく理解します。現地法には、ERL の最大サイズに関する特定の要件や推奨事項が規定されていることがあります（7,000 平方フィート（2133.6 平方メートル）など）。
2. サービス プロバイダーと打ち合わせをして、ルールや推奨事項を把握します。
3. 組織のセキュリティ担当者と打ち合わせをして、緊急コールに効果的に応答するためにはどのようなことが必要と考えているかを把握します。各種ゾーンのサイズについて提案することに加え、セキュリティ担当者は ERL の命名方法についても検討する必要があります。ERL の名前は、緊急の発信者の場所の特定に使用する重要なデータの 1 つであるためです。

   セキュリティ担当者は、次のフィールドを使用して、発信者の場所を特定できます。

   - ALI の [Location] フィールド：このフィールドに建物の住所を入力するなど、ERL 名を明確にするために使用できます。セキュリティ担当者は Emergency Responder ユーザ インターフェイスで ALI を表示することもできますが、すべての ALI を表示するには追加の手順が必要になります。このため、[Location] フィールドに完全な住所を入力することで、応答の迅速化を図ることができます。
   - [Phone Location] フィールド：スイッチ ポートに関連付けられています。このフィールドを使用して、（たとえば、ポートがサービスを提供するオフィスの番号や仕切りスペース内の番号を指定して）ロケーションを微調整できます。
4. Cisco ER を使用して、セキュリティ（オンサイト アラート）担当者に関する情報を入力します。ERL を定義するときに各 ERL に担当者を割り当てるため、この情報は ERL を定義する前に入力する必要があります。詳細については、「セキュリティ担当者（オンサイト アラート担当者）の指定」（P.4-32）を参照してください。
5. Cisco ER を使用して、ERL とその ALI を定義します。詳細については、「ERL の作成」（P.4-33）を参照してください。
6. 正しい ERL にスイッチ ポートを割り当て、ポートの電話のロケーションを定義します。詳細については、「スイッチ ポートの設定」（P.4-54）を参照してください。この作業を完了するには、ネットワーク管理者の権限が付与されているユーザが、まず、Cisco ER 設定にスイッチを追加する必要があります。
7. Cisco ER では直接サポートされていない電話機を定義します。詳細については、「電話機の手動での定義」（P.4-63）を参照してください。
8. ERL と ALI の定義が完了したら、ALI 情報をエクスポートし、そのデータをサービス プロバイダーに送信します。サービス プロバイダーと協力して、ファイル形式と送信の要件を決定します。ERL からの緊急コールが正しい Public Safety Answering Point（PSAP）にルーティングされるように、この情報は必ず送信してください。詳細については、「ERL 情報のエクスポート」（P.4-41）および「サービス プロバイダー向け ALI 情報のエクスポート」（P.4-42）を参照してください。

   ここで説明した作業を完了すると、ERL からの緊急コールは、正しいオンサイト応答担当者に通知され、正しいローカル PSAP にルーティングされます。

（注）　必ず、作成したすべての ALI エクスポート ファイルを送信してください。ALI エクスポート レコードには、レコードが新規に作成されたものか、変更されたものであるかを示す情報が含まれます。ALI エクスポート ファイルを送信しないと、送信する後続のファイルのステータスが不正確になり、送信レコードの一部（場合によっては全部）がサービス プロバイダーで拒否される結果に陥るおそれがあります。

9. 以下の操作を行ったときは、必ず、ERL、ALI、スイッチ ポートの情報を更新してください。
   - スイッチまたはポートの追加/削除
   - 手動で定義した電話機の追加/削除
   - ERL の追加/削除
   - ALI の更新

   ERL の ELIN、または ALI を更新した場合は、ALI データを再エクスポートしてサービス プロバイダーに送信する必要があります。

関連項目

- 「ERL について」（P.4-30）
- 「ERL 管理者のロールについて」（P.10-2）

セキュリティ担当者（オンサイト アラート担当者）の指定

セキュリティ担当者またはオンサイト アラート担当者を指定して、緊急応答ロケーション（ERL）に割り当てる必要があります。ERL で緊急コールが発信されると、関係するオンサイト アラート担当者は以下を受け取ります。

- Emergency Responder エンドユーザ インターフェイスでの Web ベースのアラート。
- 電子メール メッセージ。電子メール アドレスが、電子メールベースのポケットベルの場合、ポケットベルが使用されます。
- 緊急コールが発信されたことを知らせる電話。

はじめる前に

システム管理者または ERL 管理者の権限で、Cisco ER にログインする必要があります。

名前、電話番号、電子メール アドレスなど、すべてのオンサイト アラート担当者に関する情報を収集します。さらに、各担当者に一意の識別名（バッジ番号など）を作成します（まだ作成していない場合）。

オンサイト セキュリティ担当者を追加するには、次の手順を実行します。

手順

ステップ 1　[ERL]>[Onsite Alert Settings] を設定します。

[Onsite Alert Settings] ページが開きます。

ステップ 2　セキュリティ担当者またはオンサイト アラート担当者の一意の ID、名前、電話番号、電子メール アドレス、ポケットベル アドレスを入力します。

一意の ID には、バッジ番号、電子メール名、その他のサイト固有の一意の名前を指定できます。この ID を使用して担当者を ERL に割り当て、有用な命名方法を構築できます。

電子メールベースのポケットベル アドレスを使用して、オンサイト アラート担当者が電子メールではなくポケットベルで受信するように設定できます。

ステップ 3　[Insert] をクリックします。

担当者が、オンサイト担当者のリストに追加されます。この手順を繰り返して、すべてのセキュリティ担当者またはオンサイト担当者を定義します。

ヒント

- 担当者を削除するには、まず、すべての ERL 定義から担当者を削除します。次に、[Onsite Alerts Settings] ページの [Available Onsite Alerts] リストで、担当者レコードに対応する [Delete] アイコンをクリックします。
- オンサイト アラート設定を変更するには、[Available Onsite Alerts] リストで、担当者の [Onsite Alert ID]、[Onsite Alert Name]、[Onsite Alert Number]、[Onsite Alert Email Address]、または [Onsite Alert Pager Address] をクリックします。担当者の情報は、このページの [Modify Onsite Alert Contact] セクションに表示されます。必要に応じて情報を変更し、[Update] をクリックします。担当者の [Onsite Alert ID] は変更できません。[Onsite Alert ID] を変更するには、担当者のエントリを削除して、新しく作成する必要があります。

ERL の作成

この項では、Emergency Response Location（ERL; 緊急応答ロケーション）を作成する方法について説明します。

- 「デフォルト ERL の設定」（P.4-33）
- 「ERL の設定（Non-PSAP 配置の場合）」（P.4-34）
- 「ERL と ALI の設定」（P.4-35）
- 「複数の ERL の一括インポート」（P.4-37）

デフォルト ERL の設定

Emergency Responder では、新しいスイッチ ポートや位置未確認の電話機をデフォルトの緊急応答ロケーション（ERL）に割り当てる処理は自動的には行われません。新しいスイッチ ポートおよび位置未確認の電話機は、「ERL は設定されていない」ものとして扱われます。

すべてのスイッチ ポート、位置未確認の電話機、手動で設定した電話機や IP サブネットに、必ずしもデフォルト ERL を設定する必要はありません。デフォルト ERL は、その電話機に設定されている他の ERL がない場合にのみ、Cisco ER によって内部的に使用されます。

Cisco ER では、Cisco ER サーバが初めて起動されたとき（またはスタンバイ Cisco ER サーバがない場合に再起動されたとき）、最初のスイッチ ポート更新が完了するまでの間、すべての緊急コールにデフォルト ERL が使用されます。（このプロセスは即座に起動されます）。

はじめる前に

システム管理者または ERL 管理者の権限で、Cisco ER にログインする必要があります。

最初に、Cisco Unified CM で必要な ELIN を設定する必要があります（「 •「ERL の作成」（P.4-33）」（P.3-10）を参照してください）。

デフォルト ERL を設定するには、次の手順を実行します。

手順

ステップ 1　[ERL]>[Conventional ERL] を選択します。

[Find Conventional ERL Data] ページが開きます。

ステップ 2　[Configure Default ERL] をクリックします。

[ERL Information for Default] ウィンドウが開きます。

ステップ 3　[ERL Information for Default] ウィンドウに情報を入力します。各フィールドの詳しい説明については、「Add New ERL」（P.A-18）を参照してください。

ステップ 4　[ALI Details] をクリックします。

[ALI Information] ウィンドウが開きます。

ステップ 5　[ALI Information] ウィンドウに情報を入力します。各フィールドの詳しい説明については、「ALI Information (for ERL Name)」（P.A-22）を参照してください。

ALI への情報入力が完了したら、[Update ALI Info] をクリックします。ALI が保存されます。ウィンドウを閉じるには、[Close] をクリックします。

ステップ 6　[ERL Information for Default] ウィンドウをアクティブ ウィンドウにして（アクティブになっていない場合）、[Update] をクリックします。

ERL とその ALI が保存されます。

ステップ 7　ウィンドウを閉じるには、[Close] をクリックします。

ヒント　デフォルト ERL は削除できません。また、デフォルト ERL を設定しないと、他の ERL を設定できません。

関連項目

- 「Conventional ERL」（P.A-17）
- 「Add New ERL」（P.A-18）
- 「ALI Information (for ERL Name)」（P.A-22）
- 「ERL と ALI の設定」（P.4-35）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）

ERL の設定（Non-PSAP 配置の場合）

Cisco ER の配置は、オンサイト アラートの場合にのみ実行できます。つまり、緊急コールを Public Safety Answering Point（PSAP）にルーティングする代わりに、指定のセキュリティ電話機に緊急コールをルーティングします。

Non-PSAP 配置の設定には、2 つの方法があります。

[Configure Security IDs Only] : このシナリオでは、任意の ERL のゾーンにセキュリティ ID を設定し、ルート/トランスレーション パターンは設定しません。すべての緊急コールは、ERL セキュリティにルーティングされます。この処理に失敗すると、コールはデフォルト ERL セキュリティにルーティングされます。次に、Cisco ER は設定されたセキュリティ電話機へのコールを開始し、アラート セキュリティ担当者に緊急コールのプロンプトを再生します。

セキュリティ ID のみを設定するには、次の手順を実行します。

手順

ステップ 1　緊急コールを通知するセキュリティ担当者を指定します（「セキュリティ担当者（オンサイト アラート担当者）の指定」（P.4-32）を参照してください）。

たとえば、セキュリティ A に電話番号 1000 を設定します。

ステップ 2　ルート パターン/ELIN は指定せず、ERL のセキュリティ ID を指定して、ERL を追加します（「ERL の作成」（P.4-33）を参照してください）。

たとえば、セキュリティ A を指定した ERL X を追加します。

ステップ 3　スイッチ ポート画面に移動し、検出されたスイッチ ポートを設定済みの ERL に割り当てます（「スイッチ ポートの設定」（P.4-54）を参照してください）。

たとえば、スイッチ IP Y のスイッチ ポートを ERL X に関連付けます。

スイッチ IP Y に接続された電話機からの緊急コールはすべて、ERL X を使用して、セキュリティ A の電話番号 1000 を呼び出します。

（注）　ワイヤレス アクセス ポイントの IP アドレスを使用する無線 IP 電話や無線電話機にレイヤ 3（IP）ローミングを使用すると、Cisco ER では、これらの電話機の移動は自動的には追跡できません。Cisco ER では、電話機の IP アドレスを使用して電話機の位置を特定するためです。Cisco ER を使用してネットワーク上で無線電話機の移動を自動的に追跡する必要がある場合は、レイヤ 3 ローミングを使用しないでください。

[Configure Security IDs and Route/Translation Patterns] : このシナリオでは、任意の ERL のゾーンにセキュリティ ID を設定し、ELIN 番号を指定せずにルート/トランスレーション パターンを設定します。Cisco ER には、このゾーンには ELIN が設定されないことを知らせるポップアップの警告メッセージが表示されます。緊急コールは、ルート/トランスレーション パターンを使用してルーティングされます。この処理に失敗すると、デフォルトのパターンが使用されます。次に、Cisco ER は設定されたセキュリティ電話機へのコールを開始し、アラート セキュリティ担当者に緊急コールのプロンプトを再生します。

（注）　このシナリオでは、各ゾーンに異なるルート/トランスレーション パターンを使用する必要があります。

ERL と ALI の設定

この項では、単一の ERL を定義する方法について説明します。複数の ERL に同様の情報が設定されることが多いため、同様の ERL の定義を簡素化するための方法について「複数の ERL の一括インポート」（P.4-37）を参照してください。

はじめる前に

システム管理者または ERL 管理者の権限で、Emergency Responder にログインする必要があります。

単一の ERL を定義するには、次の手順を実行します。

手順

ステップ 1　[ERL]>[Conventional ERL] を選択します。

[Find conventional ERLs] ページが開きます。

ステップ 2　[Add New ERL] をクリックします。

[Add New ERL] ウィンドウが開きます。

ステップ 3　[Add New ERL] ウィンドウに情報を入力します。各フィールドの詳しい説明については、「Add New ERL」（P.A-18）を参照してください。

ステップ 4　[Add ALI] ボタンをクリックします。

[ALI Information] ウィンドウが開きます。

ステップ 5　[ALI Information] ウィンドウに情報を入力します。各フィールドの詳しい説明については、「ALI Information (for ERL Name)」（P.A-22）を参照してください。

ALI への情報入力が完了したら、[Save and Close] をクリックします。

ステップ 6　[Add New ERL] ウィンドウをアクティブ ウィンドウにして（アクティブになっていない場合）、[Insert] をクリックします。

ERL とその ALI が保存されます。

ステップ 7　ウィンドウを閉じるには、[Close] をクリックします。

ヒント

- 既存 ERL に類似した ERL を作成するには、既存 ERL のリストで [Find] をクリックし、類似した ERL を選択して [Copy] をクリックします。ERL の一部の情報と ALI のすべての情報がコピーされます。これらの情報を変更して、新しい ERL を作成できます。
- ALI の定義プロセスを簡素化するため、タグの作成や更新を行うことができます。[ALI Information] ウィンドウに移動し、samplevalidate.txt ファイルのロケーションに関する情報を探します。サンプル ファイルに、タグの設定方法の説明が載っています。必要なタグを作成または更新したら、[ALI Information] ウィンドウでタグの名前を選択します。[ALI] フィールドに、選択したタグに関係のある設定が読み込まれます。

関連項目

- 「Conventional ERL」（P.A-17）
- 「Add New ERL」（P.A-18）
- 「ALI Information (for ERL Name)」（P.A-22）
- 「複数の ERL の一括インポート」（P.4-37）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）

複数の ERL の一括インポート

一度に 1 つの ERL を定義するのではなく、「ERL と ALI の設定」（P.4-35）で説明したように、複数の ERL 定義を含むファイルを作成して、これらの ERL を一度に Emergency Responder 設定にインポートできます。この方法は、スプレッドシートにすでに ERL 定義を作成している場合や、Cisco ER からエクスポートした ERL データを使用して Cisco ER 設定を復元する場合に特に便利です。

はじめる前に

システム管理者または ERL 管理者の権限で、Cisco ER にログインする必要があります。

インポート ファイルを準備します。Cisco ER の [Import ERL Data] ページで、必要なファイル形式に関する詳細情報を確認できます。このページには、インポートを実行するときにファイルを配置するロケーションに関する情報も示されます。

従来型の ERL、Off-Premise ERL、または Intrado ERL をインポートできます。[Import] リンクは、[Find Conventional ERL Data] ページ、[Find Off-Premises ERLs Data] ページ、および [Find Intrado ERLs Data] ページの右上にあります。

従来型の ERL の作成については、「ERL の作成」（P.4-33）を参照してください。

Intrado ERL の作成については、「Intrado ERL の設定」（P.5-5）を参照してください。

Off-Premise ERL の作成については、「Off-Premise ERL の設定」（P.5-11）を参照してください。

次の手順を使用して形式の表示、ファイルの作成 / 更新、必要なロケーションへのファイルのコピーを行い、次の手順に従ってファイルをインポートしてください。

一度に複数の ERL をインポートするには、次の手順を実行します。

手順

ステップ 1　[Find ERL] ページ（[Find Conventional ERL Data] ページ、[Find Off-Premises ERLs Data] ページ、または [Find Intrado ERLs Data] ページ）で、[Import] をクリックします。

[Import ERL Data] ページが開きます。

ステップ 2　プルダウン メニューからインポート ファイルの形式（csv または xml）を選択します。

ステップ 3　ローカル マシンからファイルをアップロードするには、[Upload] をクリックします。アップロード ユーティリティの使用については、「ファイルのアップロード」（P.4-7）を参照してください。

ステップ 4　インポート ファイルを選択します。

ステップ 5　[Import] をクリックします。

ERL と関連する ALI データのインポートが開始され、インポートの進捗状況が表示されます。Cisco ER 設定に既存のデータと競合するデータがある場合は、インポートされるデータによって上書きされます。

ステップ 6　[Close] をクリックして、[Import ERL Data] ウィンドウを閉じます。

関連項目

- 「Import ERL Data」（P.A-26）
- 「ERL と ALI の設定」（P.4-35）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）

ALI データの変換

PS-ALI Converter ツールを使用して、ERL のカンマ区切り形式（csv）のテキスト ファイルを生成します。この形式のファイルは、Cisco ER ERL で使用可能です。ファイルを変換する前に、既存の ALI ファイルを NENA 2.0 形式で Cisco ER にアップロードする必要があります。

はじめる前に

システム管理者または ERL 管理者の権限で、Cisco ER にログインする必要があります。

ALI データを変換するには、次の手順を実行します。

手順

ステップ 1　[Tools]>[PS-ALI Converter] を選択します。

[PS-ALI Converter] ページが開きます。

ステップ 2　NENA 2.0 形式の ERL ファイルをアップロードするには、[Upload PSALI file] ボタンをクリックします。[Upload File] ページが表示されます。

ステップ 3　「ファイルのアップロード」（P.4-7）の手順に従って、ERL ファイルをアップロードします。

ステップ 4　プルダウン メニューから、アップロードしたファイルを選択します。

ステップ 5　[Output file (in csv format) Name] フィールドに、変換後の csv ファイルの名前を入力します。

ステップ 6　csv ファイルを作成するには、[Convert] をクリックします。

生成された csv ファイルは、次のフォルダにあります。

```
%cerroot%/import
```

このファイルのインポートやダウンロードを行うには、ファイル マネージャ ユーティリティを使用します。

ステップ 7　必要に応じて、変換後の csv ファイルを変更します。たとえば、ERL 名、ルート パターン、セキュリティの詳細を追加して、ERL を更新します。

ステップ 8　ウィンドウを閉じるには、[Close] をクリックします。

関連項目

- 「Import ERL Data」（P.A-26）
- 「ERL と ALI の設定」（P.4-35）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）

IP サブネットベースの ERL の設定

Emergency Responder 8.6 では、スイッチ ポートベースの ERL だけでなく、IP サブネットベース（レイヤ 3）ERL もサポートされます。IP サブネットを設定し、この IP サブネットに ERL を割り当てることができます。設定された IP サブネットと ERL アソシエーションに基づいて、緊急コールのルーティングが行われます。

これは、無線電話機を使用した設定など、厳密な IP アドレッシング ルールに従い、仕切られたスペースごとの位置確認が不要な環境で有用です。

（注）　サブネットベースのトラッキングでは、IP サブネット レベルでのみ処理され、仕切りスペースごとのレベルでは処理されないことに注意してください。

IP サブネットベース ERL を使用して、802.11b エンドポイント（802.11b で実行中の Cisco Unified Wireless IP Phone 7920 デバイスや Cisco IP SoftPhone など）の位置を特定し、追跡します。Cisco ER では、Cisco アクセス ポイントに対する 802.11b ワイヤレス エンドポイントの位置を特定し、追跡することはできません。以下に推奨事項を記載します。

- 各アクセス ポイントにサブネット ERL を設定します。
- アクセス ポイントが接続されたスイッチ ポートを指定し、802.11b ワイヤレス エンドポイントを、そのアクセス ポイントに設定したサブネット ERL に割り当てます。

はじめる前に

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

IP サブネットベースの ERL を設定するには、次の手順を実行します。

手順

ステップ 1　[ERL Membership]>[IP Subnets] を選択し、[Find and List IP Subnets] ページの [Add new IP Subnet] リンクをクリックします。

[Configure IP Subnets] ページが開きます。

ステップ 2　[Subnet ID] フィールドに、定義するサブネットの IP アドレスを入力します（10.76.35.0 など）。

ステップ 3　[Subnet Mask] フィールドに、定義するサブネットのマスクを入力します（255.255.255.224 など）。

ステップ 4　サブネットに割り当てる ERL を選択するには、[ERL Name] フィールドの隣にある [Search ERL] ボタンをクリックします。[Find ERL] ページが表示されます。

ステップ 5　[ERL Search Parameters] を入力し、[Find] をクリックします。検索結果が表示されます。

ステップ 6　サブネットに割り当てる ERL の隣にあるオプション ボタンをクリックして、[Select ERL] をクリックします。[Find ERL] ページが閉じます。

ステップ 7　[Configure IP Subnet] ページで、[Insert] をクリックしてサブネットを追加します。

ポップアップ メッセージが表示され、スイッチ ポートを更新するように求められます。この処理は、すべての IP サブネットを追加してから行ってください。

ステップ 8　このページのフィールドの内容を、以前に保存した設定に戻すには、[Cancel Changes] をクリックします。

ステップ 9　[Find and List IP Subnets] ページに戻るには、[Back to IP Subnet Search] をクリックします。

関連項目

- 「Find and List Synthetic Phones」（P.A-62）
- 「Add New Synthetic Phone」（P.A-63）

テスト ERL の設定

Cisco Unified Operations Manager 2.01 を使用して、Cisco ER のヘルスと機能性をモニタできます。

Cisco ER とともに Cisco Unified Operations Manager を使用するには、従来型の ERL 用にテスト ERL を設定し、擬似電話機を追加して、擬似電話機をテスト ERL に関連付けます。擬似電話機で緊急コールが発信されると、Cisco ER は関連付けたテスト ERL を使用してコールのルーティングを行います。

（注） テスト ERL は、擬似電話機に対してのみ設定できます。

（注） Off-Premise ERL や Intrado ERL には、テスト ERL は設定できません。

Cisco ER のテストに使用する擬似電話機はすべて、設定したいずれかのテスト ERL に属する必要があります。テスト ERL に使用する電話機では、擬似電話機に割り当てられた MAC アドレスまたはアドレス範囲を入力します。

次の条件はテスト ERLS に適用されます。

- 模擬電話機からのコールは、Call History ログには記録されません。
- 模擬電話機から緊急コールが発信されても、Web アラートは生成されません。
- 模擬電話機から緊急コールが発信されても、電子メール アラートは生成されません。
- テスト ERLS の PS-ALI レコードは、NENA エクスポート ファイルにエクスポートされません。

ヒント テスト ERL の ALI データを入力する必要はありません。テスト ERL 以外の ERL には、ALI データが必要です。

はじめる前に

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

テスト ERL を設定するには、次の手順を実行します。

手順

ステップ 1　[ERL]>[Conventional ERL] を選択し、[ERL Configuration] ページの [Add New ERL] をクリックします。

ステップ 2　[ERL] フィールドに、テスト ERL の名前を入力します。

ステップ 3　[Test ERL] フィールドで、ボックスをオンにして選択します。

（注） この設定は、[ERL Information for Default] ページでは使用できません。デフォルト ERL はテスト ERL として使用できません。

（注） [ALI Details] をクリックして ALI データを入力しないでください。テスト ERL に ALI データの入力は不要です。テスト ERL 以外の ERL では、ALI データは必要です。

ステップ 4　[Insert] をクリックしてテスト ERL を保存し、[Close] をクリックしてウィンドウを閉じます。

ステップ 5　[ERL Membership>Synthetic Phones] を選択し、[Find and List Synthetic Phones] ページの [Add New Synthetic phone] をクリックします。

ステップ 6　[MAC Address] フィールドに、擬似電話機に割り当てられた MAC アドレスまたは MAC アドレス範囲を入力します。

MAC アドレスは次の形式で入力します。

xx-xx-xx-xx-xx-xx

または

xxxxxxxxxxxx

代用の MAC アドレスは、次の範囲内であることが必要です。

00059a3b7700 ～ 0059a3b8aff

ステップ 7　[ERL Name] フィールドに、擬似電話機に割り当てるテスト ERL を入力します。ドロップダウン リストから、設定したテスト ERL を選択するか、または有効なテスト ERL 名を入力します。

ステップ 8　定義した擬似電話機のリストに電話機を追加するには、[Insert] をクリックします。

ステップ 9　このページのフィールドの内容を、以前に保存した設定に戻すには、[Cancel Changes] をクリックします。

関連項目

- 「Find and List Synthetic Phones」（P.A-62）
- 「Add New Synthetic Phone」（P.A-63）

ERL 情報のエクスポート

ERL の設定のバックアップや移動などに使用するために ERL エクスポート ファイルを作成するには、[Export ERL] ページを使用します。従来型の ERL、Off-Premise ERL、または Intrado ERL をエクスポートできます。[Export] リンクは、[Find Conventional ERL Data] ページ、[Find Off-Premises ERLs Data] ページ、および [Find Intrado ERLs Data] ページの右上にあります。

従来型の ERL の作成については、「ERL の作成」（P.4-33）を参照してください。

Intrado ERL の作成については、「Intrado ERL の設定」（P.5-5）を参照してください。

Off-Premise ERL の作成については、「Off-Premise ERL の設定」（P.5-11）を参照してください。

（注）　ERL エクスポート ファイルはサービス プロバイダーに送信しないでください。サービス プロバイダーが使用できる形式ではエクスポートされません。

ALI 情報のエクスポートについては、「サービス プロバイダー向け ALI 情報のエクスポート」（P.4-42）を参照してください。

ERL で受け入れられるための ALI データの形式の変更については、「サービス プロバイダー向け ALI 情報のエクスポート」（P.4-42）を参照してください。

はじめる前に

システム管理者または ERL 管理者の権限で、Cisco ER にログインする必要があります。

ERL 情報をエクスポートするには、次の手順を実行します。

手順

ステップ 1　[Find ERL] ページ（[Find Conventional ERL Data] ページ、[Find Off-Premises ERLs Data] ページ、または [Find Intrado ERLs Data] ページ）で、[Export] をクリックします。

[Export ER Data] ウィンドウが開きます。

ステップ 2　プルダウン メニューからエクスポート ファイルの形式（csv または xml）を選択します。

ステップ 3　[Enter Export File Name] フィールドに、エクスポート先のファイル名を入力します。

ステップ 4　[Export] をクリックします。

エクスポート ファイルが作成され、ファイルが作成された場所とエクスポートされたレコード数が通知されます。

ステップ 5　エクスポートしたファイルをローカル マシンにダウンロードするには、プルダウン メニューから該当のファイルを選択し、[Download] をクリックします。

ステップ 6　[Close] をクリックして、[Export ERL Data] ウィンドウを閉じます。

関連項目

- 「Export ERL Data」（P.A-25）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）

サービス プロバイダー向け ALI 情報のエクスポート

サービス プロバイダーとデータベース プロバイダーは、Automatic Location Information（ALI）を必要とします。この情報を使用して、従来型の ERL から発信された緊急コールが正しい Public Safety Answering Point（PSAP）にルーティングされるようになります。PSAP では、この情報を使用して緊急応答チーム（警察、消防署、医療機関）を派遣し、緊急事態に対処します。ERL とその ALI の作成や更新を行うときは、必ず、データをエクスポートし、サービス プロバイダーまたはデータベース プロバイダーが指定する形式でデータをこれらのプロバイダーに送信してください。

サービス プロバイダーへの ALI の詳細情報の送信については、「ALI フォーマット ツールの使用」を参照してください。

はじめる前に

システム管理者または ERL 管理者の権限で、Emergency Responder にログインする必要があります。

注意　必ず、作成したすべての ALI エクスポート ファイルを送信してください。ALI エクスポート レコードには、レコードが新規に作成されたものか、変更されたものであるかを示す情報が含まれます。ALI エクスポート ファイルを送信しないと、送信する後続のファイルのステータスが不正確になり、送信レコードの一部（場合によっては全部）がサービス プロバイダーで拒否される結果に陥るおそれがあります。

サービス プロバイダーに送信する ALI 情報をエクスポートするには、次の手順を実行します。

手順

ステップ 1　[Tools]>[Export PS-ALI Records] を選択します。

[Export PS-ALI Records] ページが開きます。

ステップ 2　[Select the NENA Format] フィールドのドロップダウン リストから、サービス プロバイダーが必要とする形式を選択します。

ステップ 3　[File to Export] フィールドに、エクスポート先のファイル名を入力します。

ステップ 4　[Company Name] フィールドに、会社名を入力します。

ステップ 5　[Cycle Counter] は、データをエクスポートするたびに自動的に増分されます。以前のエクスポートを再実行する場合や修正する場合を除き、このカウンタを変更する必要はありません。ただし、シーケンス番号を変更してもファイル内のデータには影響しません。エクスポートをやり直す場合は、エクスポート ファイルを手動で編集して、レコード ステータス フィールドを変更する必要があります。

ステップ 6　[Export] をクリックします。

エクスポート ファイルが作成され、エクスポートされたレコード数が通知されます。

ステップ 7　ローカル マシンにファイルをダウンロードするには、[Download] をクリックします。

ステップ 8　[Close] をクリックして、[Export ALI Records] ウィンドウを閉じます。

ステップ 9　サービス プロバイダーのファイルの転送方法を使用して、サービス プロバイダーにファイルを送信します。

関連項目

- 「ALI Information (for ERL Name)」（P.A-22）
- 「Export ERL Data」（P.A-25）
- 「Export PS-ALI Records」（P.A-76）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）

ERL の監査証跡の表示

ERL の監査証跡を参照すると、ERL の作成や変更がどのように、いつ、だれによって実行されたかを確認できます。

はじめる前に

監査証跡を表示するには、システム管理者、ERL 管理者、またはネットワーク管理者の権限が必要です。

ERL の監査証跡を表示するには、次の手順を実行します。

手順

ステップ 1　[Reports]>[ERL Audit Trail] を選択します。

[ERL Audit Trail] ページが開きます。

ステップ 2　ERL の監査履歴を選択するための検索条件を入力します。

すべての ERL を表示するには、条件を入力せずに [Find] をクリックします。

検索を絞り込むには、次の手順に従います。

a. 検索するフィールドを選択し、検索関係を選択して、検索文字列を入力します。一部のフィールドでは、右端にあるドロップダウン リストから、有効な文字列を選択できます。

b. フィールドの組み合わせを検索するには、[More] をクリックして、検索フィールドを追加します。いずれかの検索条件に一致する ERL を表示するには、リスト上部で [Any] を選択します（OR 検索）。すべての検索条件に一致する ERL のみを表示するには、リスト上部で [All] を選択します（AND 検索）。

c. すべての検索条件を入力したら、[Find] をクリックします。

条件に一致する監査レコードが表示されます。一致するレコード数が多い場合は、結果は複数のページにわたって表示されます。リストの下部にあるリンクを使用して、ページを変更します。

ヒント　特定の ERL の監査証跡を表示するには、[Find and List ERLs] ページに表示される ERL リストの [Audit Trail] 列で [View] をクリックします。

関連項目

- 「ERL Audit Trail」（P.A-75）
- 「ERL の使用」（P.4-29）

Cisco Emergency Responder のスイッチの設定

スイッチ ポートを ERL に割り当てるには、ネットワークで使用するスイッチを Emergency Responder に指定する必要があります。次のトピックでは、スイッチ要件と、Cisco ER にスイッチを指定する方法について説明します。

- 「Cisco Emergency Responder のスイッチ要件について」（P.4-44）
- 「SNMP 接続の設定」（P.4-45）
- 「電話機トラッキングとスイッチ更新スケジュールの定義」（P.4-47）
- 「LAN スイッチの指定」（P.4-48）
- 「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）

Cisco Emergency Responder のスイッチ要件について

Emergency Responder は、Cisco Discovery Protocol（CDP）を使用して電話機を検出するため、すべてのスイッチで CDP を有効にする必要があります。CDP を有効にしないと、Cisco ER ではスイッチの Content Addressable Memory（CAM）テーブルを使用して電話機の追跡が行われます。CAM テーブルを使用すると、CDP を使用した場合と比較して効率性が低くなります。

ネットワーク上に CDP を使用しない電話機があると、Cisco ER では、CAM テーブルを使用した追跡が行われます。

電話機を接続しているスイッチが Cisco ER でサポートされていることと、そのスイッチで必要なソフトウェア バージョンを実行していることを確認してください。「ネットワークのハードウェアおよびソフトウェアの要件」（P.1-4）に、サポートされるスイッチとソフトウェア バージョンを示します。

Catalyst 3500 スイッチ クラスタを使用している場合は、各スイッチに IP アドレスを割り当てる必要があります。IP アドレスが設定されていないスイッチは、Cisco ER では機能しません。

関連項目

- 「SNMP 接続の設定」（P.4-45）
- 「電話機トラッキングとスイッチ更新スケジュールの定義」（P.4-47）
- 「LAN スイッチの指定」（P.4-48）
- 「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）

SNMP 接続の設定

Emergency Responder では、SNMP を使用して、スイッチ上のポートに関する情報を取得します。Cisco ER では、このポート情報は必須です。この情報を使用して、ポートの ERL への割り当て、ポートに接続されている電話機の特定、ERL 割り当ての更新などを実行できます。

Cisco ER では、SNMP 情報のみ読み込まれます。スイッチ設定への書き込みは行われないため、設定する必要があるのは SNMP read コミュニティ ストリングだけです。

はじめる前に

SNMP 設定を定義するには、システム管理者またはネットワーク管理者の権限が必要です。

Cisco ER に定義するすべてのスイッチの read コミュニティ ストリングを入手します。スイッチ セットごとに異なるストリングを使用する場合は、対象のセットに IP アドレス パターンを定義できるかどうか確認してください。たとえば、10.1 で開始するすべてのスイッチに同じストリングを使用し、10.2 で開始するスイッチに別のストリングを使用する場合、10.1.*.* と 10.2.*.* のパターンを使用できます。

1 つの IP アドレスに対して 2 つ以上のパターンが一致すると、Cisco ER では、最も近い一致パターンに関連付けられた SNMP ストリングが使用されます。たとえば、*.*.*.* と 10.1.*.* を定義した場合、IP アドレスが 10.1.12.24 であると、Cisco ER では 10.1.*.* に定義された SNMP 文字列が使用されます。このページのエントリの順序は、選択には影響しません。

スイッチに SNMP ストリングを設定した場合は、Cisco Unified CM サーバにも SNMP ストリングを設定する必要があります。Cisco ER では、サポート対象のクラスタにあるすべての Cisco Unified CM サーバについて SNMP クエリーを作成できなくてはなりません。

Cisco Emergency Responder サーバ、Cisco Unified CM サーバ、および Cisco IP 電話がスイッチとは別のサブネットにある場合は、サーバと電話機の両方のサブネットとスイッチのサブネットを設定するか、または *.*.*.* を使用する必要があります。

SNMP 接続を設定するには、次の手順を実行します。

手順

ステップ 1　[Phone Tracking]>[SNMP Settings] を選択します。

[SNMP Settings] ページが開きます。

ステップ 2　SNMP read コミュニティ ストリングを関連付ける IP アドレス パターンを入力します。ワイルドカード文字としてアスタリスク（*）を使用します。オクテットの範囲を使用することもできます（15-30 など）。Cisco ER では、[LAN Switch Details] ページで指定されたスイッチにのみアクセスを試行するため（詳細については「LAN スイッチの指定」（P.4-48）を参照）、指定する IP アドレス パターンがスイッチ以外のデバイスを対象としていても問題ありません。

- すべてのスイッチで同じ read コミュニティ ストリングを使用している場合は、*.*.*.* と入力します。作成する必要のあるエントリは 1 つだけです。
- スイッチのサブセットが同じストリングを使用しているときは、それらのサブセットをカバーするマスクを作成します（可能な場合）。簡略化するため、パターンの数は最小限に抑えてください。
- 各スイッチに別々のストリングを使用する場合は、このページにそれぞれのスイッチを入力する必要があります。

ステップ 3　タイムアウト値と再試行の回数を入力します。これらの値は、Cisco ER がスイッチからの SNMP 情報の取得を試みる回数と時間を決定するために組み合わせて使用されます。最初の試行は、タイムアウト値に指定された時間が経過するまで継続されます。再試行回数に 1 以上の値を入力すると、再試行されます。このときの試行時間は、前回の試行時間の 2 倍になります。たとえば、タイムアウト値に 10 を指定すると、最初の再試行は 20 秒、2 回目の再試行では 40 秒となります。

タイムアウトには 10 ～ 15 秒、再試行回数には 2 ～ 3 回が最適です。

ステップ 4　read コミュニティ ストリング（public など）を入力します。

ステップ 5　[Insert] をクリックします。

SNMP 設定が、設定のリストに追加されます。

ステップ 6　複数の設定を作成する必要がある場合は、ステップ 2 に戻って操作します。

ヒント

- スイッチの SNMP read コミュニティ ストリングを変更した場合は、Cisco ER の関連する設定を更新する必要があります。
- SNMP 設定を変更するには、リストで対象の設定を選択します。編集ボックスに、設定が読み込まれます。変更を加えて、[Update] をクリックします。SNMP 設定を更新したら、スイッチでスイッチ ポートと電話機の更新プロセスを実行します。[Phone Tracking]>[LAN Switch Details] を選択し、[LAN Switches] リストでスイッチを選択して、[Locate Switch Ports] をクリックします。多数のスイッチの設定を変更する場合は、[Phone Tracking]>[Run Switch-Port & Phone Update] を選択して、すべてのスイッチでプロセスを実行します。
- 設定を削除するには、設定のエントリの削除アイコンをクリックします。

関連項目

- 「SNMP Settings」（P.A-38）
- 「LAN スイッチの指定」（P.4-48）

電話機トラッキングとスイッチ更新スケジュールの定義

電話機を正常に追跡するため、Emergency Responder では、定期的にスイッチにアクセスしてポート情報とデバイス情報を取得する必要があります。Cisco ER は、次の 2 つのプロセスを使用してネットワーク情報を更新します。

- 電話機トラッキング：Cisco Unified CM に登録されている電話機の情報と、スイッチから取得したロケーション情報を定期的に比較します。電話機が移動した場合、Cisco ER によりその電話機の ERL が更新されます。位置を確認できない電話機は、「位置未確認の電話機」として分類されます（「位置未確認の電話の識別」（P.4-62）を参照してください）。

（注）　電話機のスイッチ ポートの更新スケジュールを設定しないと、デフォルトのスケジュールが午前 0 時に実行されます。

- スイッチ ポートと電話機の更新：電話機トラッキング プロセスに加え、ネットワーク スイッチのより広範なチェックが実行されます。このチェックにより、新規または変更されたスイッチ モジュール（追加または削除されたポート）を特定できます。新たに検出されたポートは、デフォルト ERL に割り当てられます。ERL 管理者により、新しいポートへの ERL 割り当てが更新されることを確認してください。

はじめる前に

スケジュールを定義するには、システム管理者またはネットワーク管理者の権限が必要です。

電話機トラッキングとスイッチ更新スケジュールを定義するには、次の手順を実行します。

手順

ステップ 1　[Phone Tracking]>[Schedule] を選択します。

[Schedule] ページが開きます。

ステップ 2　増分電話機トラッキング スケジュールを分単位で入力し、[Update] をクリックします。

Cisco ER では、前回の電話機トラッキング プロセスが完了した後、ここで指定した時間（分）が経過してから電話機トラッキング プロセスが実行されます。

ステップ 3　スイッチ ポートおよび電話機の更新プロセスのスケジュールを入力します。このプロセスは、1 日に 1 回以上実行する必要があります（ただし、1 日に 4 回を超えて実行しないでください）。

たとえば、月曜日から金曜日の午前 0 時と、土曜日と日曜日の午後 6 時にプロセスを実行するには、次のような 2 つのスケジュール エントリを作成します。

- [Mon]、[Tue]、[Wed]、[Thu]、[Fri] を選択し、[Hour] に [00]、[Minute] に [00] を選択して、[Insert] をクリックします。スケジュールが、リストに追加されます。
- [Sat] と [Sun] を選択し、[Hour] に [18]、[Minute] に [00] を選択して、[Insert] をクリックします。スケジュールが、リストに追加されます。

スケジュールを重複して定義しても、Cisco ER では 1 つのプロセスしか実行されません。

（注）　電話機トラッキングが効果的に変更されるようにするには、Emergency Responder 管理者は Cisco Unified CM の *ccmPhoneStatusUpdateStorePeriod*（CISCO-CCM-MIB）値が Emergency Responder の増分電話機トラッキング間隔よりも長い時間に設定されていることを確認する必要があります。

ヒント

- スイッチ ポートおよび電話機の更新スケジュールを変更するには、リストで該当するスケジュールをクリックします。Cisco ER のスケジュールのフィールドに、スケジュールの設定が読み込まれます。変更を加えて、[Update] をクリックします。
- スケジュールを削除するには、スケジュール リスト エントリの削除アイコンをクリックします。

関連項目

- 「Phone Tracking Schedule」（P.A-40）
- 「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）

LAN スイッチの指定

Cisco Emergency Responder（Cisco ER）で、管理するスイッチを指定する必要があります。Cisco ER では、ポートの変更が追跡されます。これには、ポートに接続されたデバイスの変更も含まれます。また、電話機が接続されたポートも認識されます。電話機が接続されたすべてのスイッチを指定します。基本的に、エッジ スイッチはすべて指定します。

Cisco ER ではスイッチからの情報を取得することが必要であるため、Cisco ER に入力した情報が正しいことと、最新情報に維持されていることを確認してください。初期のスイッチ リストを作成した後は、スイッチ定義のエクスポート、エクスポート ファイルの編集、ファイルの再インポートを行って、スイッチ定義をまとめて変更できます。

次のトピックでは、Cisco ER にスイッチを指定する方法とスイッチ情報をエクスポートする方法について説明します。

- 「LAN スイッチの指定（一度に 1 台）」（P.4-48）
- 「スイッチのグループのインポート」（P.4-50）
- 「スイッチ情報のエクスポート」（P.4-51）

LAN スイッチの指定（一度に 1 台）

Emergency Responder 設定に、一度に 1 台のスイッチの情報を入力できます。多数のスイッチを追加する場合は、ここで説明する手順を使用するのではなく、インポート ファイルを作成して追加することを検討してください。詳細については、「スイッチのグループのインポート」（P.4-50）を参照してください。

はじめる前に

スイッチ定義の追加、削除、変更を行うには、システム管理者またはネットワーク管理者の権限が必要です。

ネットワークに、Cisco Discovery Protocol（CDP）を使用して存在をネットワークアナウンスする機能を持たない電話機があるかどうかを確認します。CDP 電話機以外の電話では、Cisco ER はスイッチの CAM 情報を使用して電話機を特定しなければなりません。CAM アクセスが必要となる電話機の詳細については、「ネットワークのハードウェアおよびソフトウェアの要件」（P.1-4）を参照してください。

スイッチを追加する前に、必ず、SNMP read コミュニティ ストリングを設定してください。詳細については、「SNMP 接続の設定」（P.4-45）を参照してください。

（注）　Emergency Responder サーバのリブートまたはバージョンのアップグレードを実行すると、Emergency Responder はすべてのスイッチを対象に完全な検出スキャンを実行します。ネットワークサイズやスイッチの数に応じて、このプロセスには時間がかかることがあります。
スイッチがネットワークから削除されている場合は、必ず、[Emergency Responder Administration] > [Phone Tracking] > [LAN Switch Details] を使用して LAN スイッチを削除してください。

一度に 1 台の LAN スイッチを指定するには、次の手順を実行します。

手順

ステップ 1　[Phone Tracking]>[LAN Switch Details] を選択します。

[LAN Switch Details] ページが開きます。

ステップ 2　スイッチに関する情報を入力します。

- スイッチの IP アドレスまたは DNS 名を入力します。
- CDP が有効になっていない電話機がスイッチに接続されている場合は、[Enable CAM-based Phone Tracking] を選択します。
- Emergency Responder のロケーション フィールドに、スイッチに設定されているスイッチ ポートの説明を表示するには、[Use port description as port location] を選択します。

ステップ 3　Cisco ER 設定にスイッチを追加するには、[Insert] をクリックします。

Cisco ER により、スイッチ ポートおよび電話機の更新プロセスを実行するかどうかが尋ねられます。Cisco ER がスイッチ上のポートを特定し、ERL 管理者がポートを正しい ERL に割り当てることができるように、このプロセスを実行する必要があります。

複数のスイッチを追加する場合は、最後のスイッチを追加してからこのスイッチを実行してください。プロセスの実行を選択すると、スイッチ ポートおよび電話機の更新プロセスが最後に実行された後に追加されたすべてのスイッチに対して、このプロセスが実行されます。

プロセスを実行しないように選択した場合は、[Phone Tracking]>[Run Switch-Port & Phone Update] を選択して、後でこのプロセスを実行できます。

いずれの場合も、新たに検出されたポートは、デフォルト ERL に割り当てられます。

（注）　Emergency Responder では、1 つのシャーシには IP アドレス / ホスト名が 1 つだけ存在することを見込んでいます。また、次の MIB にアクセスできることが必要です。
– mib-2
– IF-MIB
– CISCO-CDP-MIB
– ENTITY-MIB
– CISCO-VLAN-MEMBERSHIP-MIB
– BRIDGE-MIB*
– CISCO-STACK-MIB
– Mib-2
– interface
– CISCO-2900-MIB

ヒント

- スイッチの Cisco ER 設定を表示するには、[LAN Switches] リストでスイッチをクリックします。設定を変更するには、変更を加えて [Update] をクリックします。
- 既存スイッチの設定を表示している場合に、別のスイッチを追加するには、[Add LAN Switch] をクリックします。
- スイッチを削除するには、[LAN Switches] リストから対象のスイッチを選択して [Delete] をクリックします。スイッチをネットワークから削除しないと、Cisco ER では、スイッチに接続された電話機は「位置未確認の電話機」として認識されます。

関連項目

- 「スイッチのグループのインポート」（P.4-50）
- 「スイッチ情報のエクスポート」（P.4-51）
- 「LAN Switch Details」（P.A-44）
- 「Cisco Emergency Responder のスイッチ要件について」（P.4-44）

スイッチのグループのインポート

必要なスイッチ情報を含むファイルをインポートすることで、一度に多数のスイッチを定義できます。このファイルを作成するには、ネットワーク管理ソフトウェアからスイッチ情報をエクスポートし、スプレッドシート プログラムを使用して Emergency Responder ファイル形式要件に一致するようにレコードに変更を加えます（列の削除、追加、再配置などを行います）。

大規模ネットワークの場合、スイッチ定義をインポートすることで、時間を大幅に節約できます。

はじめる前に

スイッチ定義をインポートするには、システム管理者またはネットワーク管理者の権限が必要です。

インポート ファイルを準備します。Cisco ER の [Import LAN Switch] ページで、必要なファイル形式に関する詳細情報を確認できます。このページには、インポートを実行するときにファイルを配置するロケーションに関する情報も示されます。次の手順を使用してページの移動、形式の表示、ファイルの作成、必要なロケーションへのファイルのコピーを行い、次の手順に従ってファイルをインポートしてください。

スイッチを追加する前に、必ず、SNMP read コミュニティ ストリングを設定してください。詳細については、「SNMP 接続の設定」（P.4-45）を参照してください。

スイッチのグループをインポートするには、次の手順を実行します。

手順

ステップ 1　[Phone Tracking]>[LAN Switch Details] を選択します。

[LAN Switch Details] ページが開きます。

ステップ 2　左側のスイッチ リストで、[Import] をクリックします。

[Import LAN Switch] ページが開きます。

ステップ 3　インポートするファイル形式とファイル名を選択します。

ステップ 4　[Import] をクリックします。

Cisco ER から、インポート先のスイッチ上で電話機トラッキングを実行するかどうかが尋ねられます。電話機トラッキングを実行しないとスイッチ ポートを設定することができないため、通常は、[OK] を選択する必要があります。[Cancel] を選択した場合は、Cisco ER によってスイッチはインポートされますが、電話機トラッキング プロセスは実行されません。

いずれかを選択すると、Cisco ER によりスイッチ設定が追加され、インポート状況が表示されます。

ステップ 5　ウィンドウを閉じるには、[Close] をクリックします。

ステップ 6　インポートしたスイッチ上で電話機トラッキングを実行しなかった場合は、[Phone Tracking]>[Run Switch-Port & Phone Update] を選択します。

Cisco ER は各スイッチにアクセスして、スイッチ上のポートおよびポートに接続されている電話機を検出します。

または、[LAN Switch Details] ページで [Locate Switch Ports] をクリックすると、各スイッチの設定を表示できます。このプロセスは、選択したスイッチ上でのみ実行されます。

関連項目

- 「LAN スイッチの指定（一度に 1 台）」（P.4-48）
- 「スイッチ情報のエクスポート」（P.4-51）
- 「LAN Switch Details」（P.A-44）
- 「Cisco Emergency Responder のスイッチ要件について」（P.4-44）

スイッチ情報のエクスポート

Cisco Emergency Responder（Cisco ER）設定をエクスポートできます。この機能により、データのバックアップを行ったり、Cisco ER で多数のスイッチ定義の更新に使用するファイルを作成したりすることができます。エクスポート ファイルを編集して変更を加え、ファイルを再インポートして Cisco ER の情報を上書きできます。

はじめる前に

スイッチ定義をエクスポートするには、システム管理者またはネットワーク管理者の権限が必要です。

スイッチ情報をエクスポートするには、次の手順を実行します。

手順

ステップ 1　[Phone Tracking]>[LAN Switch Details] を選択します。

[LAN Switch Details] ページが開きます。

ステップ 2　スイッチ リストで、[Export] をクリックします。

[Export LAN Switch] ページが開きます。

ステップ 3　ファイルのタイプを選択し、エクスポート ファイルのファイル名を入力します。ファイル拡張子を含めないでください。

ステップ 4　[Export] をクリックします。

エクスポート ファイルが作成されます。ウィンドウを閉じるには、[Close] をクリックします。

関連項目

- 「LAN スイッチの指定（一度に 1 台）」（P.4-48）
- 「スイッチのグループのインポート」（P.4-50）
- 「LAN Switch Details」（P.A-44）
- 「Cisco Emergency Responder のスイッチ要件について」（P.4-44）

スイッチ ポートおよび電話機更新プロセスの実行（手動）

ERL をスイッチ ポートに割り当てるには、スイッチ ポートおよび電話機更新プロセスを使用して、Emergency Responder にスイッチ上のポートを認識させる必要があります。Cisco ER では、設定したスケジュールに基づいてこのプロセスを実行しますが（詳細については、「電話機トラッキングとスイッチ更新スケジュールの定義」（P.4-47）を参照）、各スイッチ上で電話機トラッキングを実行せずにスイッチ設定に多数の変更を加えた場合は、このプロセスを手動で実行することをお勧めします。

スイッチ ポートおよび電話機更新プロセスでは広範なチェックが行われるため、Cisco ER のトラッキング結果全体をリフレッシュしたい場合にのみ、実行してください。一定のスイッチの結果のみを更新する場合には、各スイッチ上で電話機トラッキングを実行できます。[Phone Tracking]>[LAN Switch Details] を選択し、左側のリストでスイッチを選択して、[Locate Switch Ports] をクリックします。

各スイッチ上で電話機トラッキングを実行することが必要になるのは、次のような場合です。

- Cisco ER にスイッチを追加した場合。スイッチを追加するとき、Cisco ER により、プロセスを実行するかどうかが尋ねられます。このときにプロセスを実行するように選択した場合は、[Locate Switch Ports] を選択する必要はありません。Cisco ER では、完全なスイッチ ポートおよび電話機更新プロセスが最後に実行された後に追加されたすべてのスイッチを対象にプロセスが実行されるためです。
- Cisco ER にすでに定義されたスイッチにモジュールの追加、削除、または変更を行った場合。
- IP サブネットベースの ERL の追加や削除を行った場合。

次のような場合は、スイッチ ポートおよび電話機更新プロセスを手動で実行してください。

- Cisco ER のトラッキング結果をリフレッシュしたい場合。
- 「スイッチのグループのインポート」（P.4-50）で説明したとおりにスイッチ定義を Cisco ER にスイッチを追加したが、インポートするときに電話機トラッキングを実行しなかった場合。
- 位置未確認の電話機リストに多数のエントリが存在する場合（「位置未確認の電話の識別」（P.4-62）を参照）。このプロセスを実行すると、Cisco ER で一部の電話機が検出されるかどうかを確認できます。これらの問題については「位置未確認の電話機が多すぎる」（P.11-2）を参照し、スイッチ ポートおよび電話機更新プロセスを実行する前に、問題解決に役立ててください。

はじめる前に

スイッチ ポートおよび電話機更新プロセスを手動で実行するには、システム管理者またはネットワーク管理者の権限が必要です。

スイッチ ポートおよび電話機更新プロセスを手動で実行するには、次の手順を実行します。

手順

ステップ 1　[Phone Tracking]>[Run Switch-Port & Phone Update] を選択します。

Cisco ER により、プロセスが実行されます。表示しているページは変わりません。新たに検出されたポートは、デフォルト ERL に割り当てられます。

関連項目

- 「電話機トラッキングとスイッチ更新スケジュールの定義」（P.4-47）
- 「位置未確認の電話の識別」（P.4-62）
- 「Cisco Emergency Responder のスイッチ要件について」（P.4-44）

スイッチ IP アドレス変更の動的なトラッキング

Emergency Responder 8.6 では、Emergency Responder が管理する LAN スイッチ IP アドレスに変更が生じた場合、それを動的に追跡できます。この機能は、スイッチ ホスト名を使用して追加された LAN スイッチを対象に実行されます。

LAN スイッチ IP アドレスを動的に追跡するには、次の手順を実行します。

はじめる前に

LAN スイッチ IP アドレスの動的なトラッキングを有効にするには、システム管理者権限が必要です。

手順

ステップ 1　[System]>[Cisco ER Group Settings] を選択します。

[Emergency Responder Group Settings] ページが開きます。

ステップ 2　スイッチの IP アドレスを動的に追跡するには、[Dynamic Tracking of Switch IP Address] チェックボックスをオンにします。

ステップ 3　変更を適用するには、[Update Settings] ボタンをクリックします。

次の増分検出サイクルが開始するのを待機する必要があります。このサイクルで、Emergency Responder によって LAN スイッチの新しい IP アドレスが検出され、データベースが更新されます。変更が検出されたことは、Emergency Responder Event Viewer および管理者向けの電子メール アラートによって通知されます。

（注）　スイッチ IP アドレスの動的なトラッキングを有効にするのは、スケジュールしたメンテナンス時間内のみにすることをお勧めします（この時間にスイッチの IP アドレスが実際に変更されます）。この処理は CPU への負荷が高いため、通常の運用時間中はこのオプションを無効にすることをお勧めします。

（注）　IP アドレスを使用して追加された LAN スイッチの場合、Emergency Responder は IP アドレスの変更を追跡できません。このような場合は、スイッチを削除して、新しい IP アドレスを使用して追加し直す必要があります。

関連項目

- 「Cisco Emergency Responder Group Settings」（P.A-3）

- 「電話機トラッキングとスイッチ更新スケジュールの定義」（P.4-47）

電話機の管理

次のトピックでは、スイッチ ポートおよび電話機を適切な緊急応答ロケーション（ERL）に割り当てる方法と、Emergency Responder が処理した緊急コールの履歴を表示する方法について説明します。

- 「スイッチ ポートの設定」（P.4-54）
- 「位置未確認の電話の識別」（P.4-62）
- 「電話機の手動での定義」（P.4-63）
- 「緊急コール履歴の表示」（P.4-67）

スイッチ ポートの設定

ネットワーク管理者が Emergency Responder 設定にスイッチを追加してスイッチ ポートおよび電話機更新プロセスを実行すると、スイッチ ポートを緊急応答ロケーション（ERL）に割り当てることができます。ポートを ERL に割り当てるときは、必ず、ポート自体のロケーションではなく、ポートに接続されているデバイスのロケーションに基づいて ERL を割り当ててください。

たとえば、ワイヤリング クローゼットが Floor 1 にあるとします。半数のポートは Floor 1 にサービスを提供し、残りの半数は Floor 2 にサービスを提供しています。また、Floor1 と Floor2 の 2 つの ERL を定義しています。スイッチは Floor 1 にありますが、半数のポートは Floor1 ERL に属し、残りの半数は Floor2 ERL に属しています。

ポートを ERL に割り当てる前に、エンドポイント（仕切りスペース内の番号やオフィスの番号など）に対するスイッチ ポートのマッピングの信頼性が高いことを確認してください。このマッピングが固定されている場合（配線がスイッチ上のポート間で見境なく移動されない場合）にのみ、信頼性が高いと判断できます。ネットワーク管理者と協力して、ワイヤリング クローゼットの整合性を確実なものにしてください。詳細については、「データの整合性および信頼性に関する考慮事項」（P.1-18）を参照してください。

次のトピックでは、スイッチ ポートを ERL に割り当てる方法について説明します。

- 「少数のスイッチ ポートの一括設定」（P.4-54）
- 「少数のポートの一括設定」（P.4-56）
- 「スイッチ ポート情報のエクスポート」（P.4-57）
- 「Wired Cisco Unified IP Phone に関するスイッチ ポート変更報告」（P.4-58）

少数のスイッチ ポートの一括設定

少数のスイッチ ポートを一括して ERL に割り当てることができます。多数のポートをマップするには、ここで説明する手順ではなく、インポート ファイルを作成して追加する方法を使用するとより簡単に実行できます。詳細については、「少数のポートの一括設定」（P.4-56）を参照してください。

はじめる前に

ポートを ERL に割り当てるには、システム管理者または ERL 管理者の権限が必要です。

設定できるのは、ログインしている Emergency Responder グループに定義されているポートだけです。

スイッチ ポートを設定するには、次の手順を実行します。

手順

ステップ 1　[ERL Membership]>[Switch Ports] を選択します。

[Switch Port Details] ページが開きます。

ステップ 2　設定するポートを一覧表示するための検索条件を入力します。

- [Find] をクリックすると、最大 1,000 レコードが表示されます。必要に応じて検索結果を絞り込みます。表示するポートの数を制限するには、[Collapse search results] の隣にあるチェックボックスをオンにします。検索結果には、見つかったスイッチの IP アドレスまたは名前が表示されます。表示を展開してスイッチに関連付けられたすべてのポートを表示するには、スイッチの隣にある [+] ボタンをクリックします。リストを折りたたんでスイッチだけを表示するには、スイッチの隣にある [-] ボタンをクリックします。
- 特定のスイッチにあるすべてのポートを一覧表示するには、[Switch IP Address] または [Switch Host Name] を選択し、IP アドレスまたはホスト名を入力して、[Find] をクリックします。スイッチで検出されたすべてのポートが一覧表示されます。
- 複数の検索条件を使用して検索結果を絞り込むには、[+] ボタンをクリックして検索フィールドを追加します。いずれかの検索条件に一致するポートを表示するには、リスト上部で [Any] を選択します（OR 検索）。すべての検索条件に一致するポートのみを表示するには、リスト上部で [All] を選択します（AND 検索）。
- どの検索方法を使用する場合でも、検索対象とする Cisco ER グループを選択します。最初の検索で目的のポートが表示されない場合、そのポートは別の Cisco ER グループで管理されている可能性があります。一度に 1 つの Cisco ER グループしか検索できません。

（注）　Emergency Responder では、ログイン セッション中は前回の検索条件が記憶されます。

ステップ 3　ポートを ERL に割り当てます。

a.　ERL を割り当てるスイッチ ポートの隣にあるチェックボックスをオンにします。

スイッチに表示されているすべてのポートを割り当てるには、そのスイッチのチェックボックスをオンにします。一度に割り当てることができるのは、1 ページ内に表示されているポートだけです。このため、ポートが複数のページにわたって表示されている場合は、ページごとにこの操作を行う必要があります。

b.　ポートに割り当てる ERL を選択します。

c.　[Phone Location] フィールドにより詳細なロケーション情報を入力することもできます。情報を入力するウィンドウを開くには、[view] をクリックします。たとえば、ポートがサービスを提供する領域の番号やオフィスの番号を入力します。この情報はオンサイト アラート（セキュリティ）担当者に送信され、緊急の発信者の場所の特定に活用されます。電話機ロケーション情報を更新できるのは、Cisco ER グループのプライマリ Cisco ER サーバにログインしているときだけです。

d.　選択したポートに割り当てる ERL を選択するには、[ERL Name] フィールドの隣にある [Search ERL] ボタンをクリックします。[Find ERL] ページが表示されます。

e.　[ERL Search Parameters] を入力し、[Find] をクリックします。検索結果が表示されます。

f.　スイッチ ポートに割り当てる ERL の隣にあるオプション ボタンをクリックして、[Select ERL] をクリックします。[Find ERL] ページが閉じます。

g.　[Assign ERL] をクリックします。

Cisco ER により、選択したポートに ERL が割り当てられます。引き続き、ポート リストのこのページに表示されているポートを割り当てることができますが、この手順を完了するまでは、検索結果ページを変更しないでください。

Cisco ER により、ERL の割り当てがコミットされます。この手順まで実行したら、別のページに進むことができます。または [Find] をクリックして、新しい検索条件を入力し、別のポートのリストを表示できます。

ヒント

- ポート リストに表示されるフィールドの変更や再配置を行う場合は、[Edit View] をクリックします。標準ビューに戻るには、[Restore Defaults] をクリックします。
- プライマリ Cisco ER サーバに電話機ロケーション情報が保存されます。このデータは定期的にバックアップしてください。「データのバックアップと復元」（P.11-33）を参照してください。

関連項目

- 「Switch Port Details」（P.A-48）
- 「Import Switch Ports」（P.A-51）
- 「少数のポートの一括設定」（P.4-56）
- 「スイッチ ポート情報のエクスポート」（P.4-57）
- 「ERL の使用」（P.4-29）

少数のポートの一括設定

必要な情報を含むファイルをインポートすることで、一度に多数のポートを ERL に割り当てることができます。

大規模ネットワークの場合、ポートと ERL のマッピングをインポートすることで、時間を大幅に節約できます。

はじめる前に

スイッチ ポート定義をインポートするには、システム管理者または ERL 管理者の権限が必要です。

インポート ファイルを準備します。このファイルを作成する最も簡単な方法として、まず Cisco ER からスイッチ ポートの詳細をエクスポートし（「スイッチ ポート情報のエクスポート」（P.4-57）を参照）、スプレッドシート プログラムを使用して ERL を目的に合わせて変更して、電話機ロケーション情報を追加する方法があります。エクスポート ファイルを作成する前に、必ず、スイッチ ポートおよび電話機更新プロセスを実行してください。これにより、すべてのスイッチ ポートに関するレコードがファイルに含まれるようになります。

ファイルをインポートする前に、[Import Switch Port] ページで指定したロケーションにファイルをコピーする必要があります。このページの開き方については、次の手順で説明します。このページにあるリンクを使用して、インポート ファイルに必要なファイル形式に関する詳細情報を表示することもできます（必要な場合）。

ファイルをインポートする前に、Cisco ER にポートを認識させる必要があります。インポートするすべてのポートのロケーションが Cisco ER によって認識されていることを確認してください。

設定できるのは、ログインしている Cisco ER グループに定義されているポートだけです。

一度に多数のポートを設定するには、次の手順を実行します。

手順

ステップ 1　[ERL Membership]>[Switch Ports] を選択します。

[Switch Port Details] ページが開きます。

ステップ 2　[Import] をクリックします。

[Import Switch Ports] ページが開きます。

ステップ 3　プルダウン メニューからインポート ファイルの形式（csv）を選択します。

ステップ 4　ローカル マシンからファイルをアップロードするには、[Upload] をクリックします。アップロード ユーティリティの使用については、「ファイルのアップロード」（P.4-7）を参照してください。

ステップ 5　[Select File to Import] プルダウン メニューを使用して、インポート ファイルを選択します。

ステップ 6　[Import] をクリックします。

ファイルがインポートされ、インポートの結果が表示されます。Cisco ER 設定に既存のデータは、インポート ファイルの ERL とポートのマッピング情報およびポート ロケーション情報で上書きされます。

ステップ 7　[Close] をクリックして、[Import Switch Port] ページを閉じます。

関連項目

- 「Switch Port Details」（P.A-48）
- 「Export Switch Ports」（P.A-50）
- 「少数のスイッチ ポートの一括設定」（P.4-54）
- 「スイッチ ポート情報のエクスポート」（P.4-57）
- 「ERL の使用」（P.4-29）

スイッチ ポート情報のエクスポート

Emergency Responder のポート設定をエクスポートできます。この機能により、データのバックアップを行ったり、Cisco ER で多数のスイッチ ポート マッピングの更新に使用するファイルを作成したりすることができます。エクスポート ファイルを編集して変更を加え、ファイルを再インポートして Cisco ER の情報を上書きできます。

はじめる前に

スイッチ ポート定義をエクスポートするには、システム管理者または ERL 管理者の権限が必要です。

スイッチ ポート情報をエクスポートするには、次の手順を実行します。

手順

ステップ 1　[ERL Membership]>[Switch Ports] を選択します。

[Switch Port Details] ページが開きます。

ステップ 2　[Export] をクリックします。

[Export Switch Ports] ページが開きます。

ステップ 3　ファイル形式を選択し、目的のファイル名を入力して、[Export] をクリックします。

ファイルがエクスポート先にエクスポートされます。

ステップ 4　エクスポートしたファイルをローカル システムにダウンロードするには、[Select file to download] プルダウン メニューからファイル名を選択し、[Download] をクリックします。

ステップ 5　[Close] をクリックして、[Export Switch Port] ページを閉じます。

関連項目

- 「Switch Port Details」（P.A-48）
- 「少数のスイッチ ポートの一括設定」（P.4-54）
- 「少数のポートの一括設定」（P.4-56）
- 「ERL の使用」（P.4-29）

Wired Cisco Unified IP Phone に関するスイッチ ポート変更報告

Cisco ER は、Wired Cisco Unified IP Phone のスイッチ ポート アソシエーションに変更を検出します。増分または完全な検出サイクルでは、スイッチ ポート アソシエーションが変更された Cisco Unified IP Phone または新たに見つかった Cisco Unified IP Phone が検出されます。検出時に不明になった Cisco Unified IP Phone も報告されます。これらの変更内容について、Cisco ER からシステム管理者に電子メールで通知されます。

（注）　不明な Cisco Unified IP Phone とは、Cisco Unified Communications Manager に登録されているものの、Cisco ER が追跡するスイッチのポートに見つからないものを指します。Cisco ER Administration Web インターフェイスの [Unlocated Phones] ページに表示される Cisco Unified IP Phone は、不明リストにも含まれます。スイッチ ポート変更報告は、Cisco ER が追跡するスイッチに接続されたときに、Cisco Unified IP Communicator のロケーションの変更を報告します。

変更通知の電子メールには、次の情報が含まれています。

- 変更が検出された日時。変更が検出された検出サイクルのおおよその完了時刻です。
- Cisco Unified IP Phone の前回のスイッチの IP およびポート番号。新規の Cisco Unified IP Phone である場合、このフィールドは空白になります。
- Cisco Unified IP Phone の現在のスイッチの IP およびポート番号。不明な Cisco Unified IP Phone である場合、このフィールドは空白になります。
- Cisco Unified IP Phone の詳細。MAC アドレス、デバイス名、電話機のタイプ、IP アドレス、IP 電話の内線番号などが含まれます。

（注）　電子メールを読みやすくするために改行キーを使用できるようにするには、電子メール クライアントを設定します。電子メール クライアント設定の詳細については、「Cisco Emergency Responder サーバ グループの設定」（P.4-22）を参照してください。

[Supported Cisco Unified IP Phones]：この機能は、次の両方の条件を満たす Wired Cisco Unified IP Phone のみを対象とします。

- Cisco Discovery Protocol（CDP）トラッキングまたは Content-Addressable Memory（CAM）トラッキングを使用して LAN スイッチ ポートで検出された Wired Cisco Unified IP Phone。

- Cisco Unified CM にアクティブに登録されている Wired Cisco Unified IP Phone。ただし、以前に Cisco Unified CM に登録されている Cisco Unified IP Phone はこの規則の例外として扱われます。このような Cisco Unified IP Phone は不明として報告されます。

[Cluster Scenario] : クラスタ内の各サーバ グループにあるアクティブ サーバが、検出して追跡した Cisco Unified IP Phone ごとに通知を送信します。

[Server Group Scenario] : サーバ グループ内で、Cisco ER は、アクティブな Cisco ER サーバについてのみ、変更の検出と通知を行います。

[Feature Activation] : 変更の検出と通知を行う機能を、手動で有効にする必要があります。

変更の検出と通知を行う機能を有効にするには、次の手順を実行します。

手順

ステップ 1　[System]>[Mail Alert Configurations] を選択します。

[Email Alert Settings] ページが表示されます。

ステップ 2　[Misc parameters] セクションのプルダウン メニューを使用して、スイッチ ポートのロケーション変更報告を行うパラメータを [True] に設定します。

ステップ 3　[Update Settings] をクリックします。

[Change Notification conditions] : Cisco ER は、以下のいずれかの状況下で完全な検出サイクルを完了すると、変更を通知する電子メールを送信します。

- 通常のスケジュールされた検出を行うとき。
- Cisco ER Administrator Web インターフェイスから手動で起動されたとき。
- システム管理者が Web インターフェイスを使用して Cisco Unified CM を追加したとき。

同様に、以下のいずれかの状況下で部分的な検出サイクルを完了すると、変更を通知する電子メールを送信します。

- 通常のスケジュールされた検出を行うとき。
- LAN スイッチが Cisco ER に追加されたとき（システム管理者が検出プロセスを開始したとき）。
- システム管理者が [LAN Switch Details] ページで [Locate Switch Ports] ボタンを選択したとき。

（注）　増分検出で、検出サイクル中に電話機の登録が行われない場合は、Cisco Unified CM で不明な Cisco Unified IP Phone の位置の確認は行われません。完全な検出では、完全な検出が最後に実行された後の不明な Cisco Unified IP Phone はすべて検出されます。

次のイベントが発生しても、変更の通知は行われません。

- 最初の検出サイクルの後に、Emergency Responder Server が起動した場合。
- 最初の検出サイクルの後に、パブリッシャがオンライン状態に戻った場合。
- 検出サイクルの後に、電話のロケーション変更が発生しなかった場合。

EnergyWise の使用

Cisco EnergyWise を使用すると、管理者は IP フォンなどの、Cisco ネットワークに接続されたデバイスのエネルギー消費を測定および低減できます。各電話機は電力消費をスイッチまたはルータにレポートするため、ネットワーク全体でエネルギー消費をモニタできます。その後で、電力供給されたときに電源投入された電話機および供給された電力量を決定することで、電話機の電源ステータスを管理できます。

Cisco EnergyWise Phones ユーザ エクスペリエンス

電話機が Power Save Plus モードになると、Cisco Unified CM から登録解除され、EnergyWise スイッチとのネゴシエーション後に電源を切断します。管理者はスリープ時間とウェイクアップ時間を設定します。これは、電話機によってスイッチと通信します。

ユーザは 6900/8900/9900 シリーズの電話機を Power Save Plus モードから復帰できますが、7900 シリーズの電話機は復帰できません。

EnergyWise Power Save Plus モードでの電話機の検出のシナリオ

次の 3 つの電話機の検出シナリオは、EnergyWise ユーザに共通します。これらのシナリオを使用し、この機能をさらに理解します。

シナリオ 1 電話機が Emergency Responder で検出に設定されているスイッチに接続した場合:

- 電話機は、Cisco Unified CM で EnergyWise を使用して設定されます。
- 電話機は、スイッチに接続され、Emergency Responder によって検出されます。電話機は、[Switch Port] ページに表示され、スイッチ ポートに接続されます。
- 次の大規模検出の前に、電話機は Power Save Plus モードになり、Cisco Unified CM から登録解除されます。
- 次の大規模検出中に、Emergency Responder は電話機のロケーション情報を保持します。これは、同じスイッチ ポートに接続されているため、[Switch Port] ページに一覧表示されます。
- 電話機に再び電源を投入すると、次の増分検出または大規模検出を待たずに 911 コールを発信できる場合、正しいロケーションが利用できます。

（注） Power Save Plus モードの電話機を抜くと、スイッチの EnergyWise 設定は失われます。大規模検出を実行する場合、電話機情報も失われます。電話機を同じポートに再接続し、電源を入れスイッチに登録した場合でも、Emergency Responder は次の検出サイクルでこの電話機を新しく登録された電話機として扱います。

（注） EnergyWise 電話機が Emergency Responder で検出に設定されているサポートされたスイッチに接続されている場合、Power Save Plus モードにする前に少なくとも 1 度電話機を検出する必要があります。その結果、Emergency Responder は次の大規模検出に電話機のロケーションおよび設定情報を保持できるようになります。検出されずに電話機が Power Save Plus モードになると、[Switch] ページに一覧表示されません。ただし、代わりに、電話機は次の検出で [IP Subnet] ページ（設定されている場合）または [Unlocated Phone] ページに一覧表示されます。電源を投入し、スイッチに登録して検出された場合、電話機は [Switch Port] ページに一覧表示されます。

シナリオ 2 Emergency Responder での IP サブネット ベースの電話機検出:

- 電話機は、Cisco Unified CM で EnergyWise を使用して設定されます。
- 電話機は、IP サブネットに基づいて、Emergency Responder によって検出されます。これは [IP Subnet] ページに一覧表示されます。
- 次の大規模検出の前に、電話機は PowerSavePlus モードになり、Cisco Unified CM から登録解除されます。
- 次の大規模検出中に、Emergency Responder は電話機のロケーション情報を保持し、電話機は [IP Subnet] ページに一覧表示されます。
- 電話機に再び電源を投入すると、次の増分検出または大規模検出を待たずに 911 コールを発信できる場合、正しいロケーションが利用できます。

シナリオ 3 Emergency Responder での位置未確認の電話機:

- 電話機は、Cisco Unified CM で EnergyWise を使用して設定されます。
- 電話機は、検出後、Emergency Responder の [Unlocated Phones] ページに一覧表示されます。
- 次の大規模検出の前に、電話機は Power Save Plus モードになり、Cisco Unified CM から登録解除されます。
- 次の大規模検出中に、Emergency Responder は電話機のロケーション情報を保持します。これは [Unlocated Phones] ページに一覧表示されます。
- 電話機に再び電源を投入すると、ユーザは次の増分検出または大規模検出を待たずに 911 コールを発信できます。ただし、電話機は、デフォルト ERL または位置未確認の電話機スイッチに割り当てられた ERL にあります。

Power Save Plus モード使用時の制限

Power Save Plus モードの電話機から 911 コールを発信するユーザに対して、次の制限を考慮する必要があります。

- スリープおよびウェイク アップ時間は Cisco Unified CM で設定されるため、ユーザは Power Save Plus モードの 7900 シリーズの電話機を復帰できません。電話機のロケーション情報は Emergency Responder から削除されませんが、ユーザは設定されたウェイク アップ時間に電話機が達するまで 911 コールを発信できません。
- ユーザは Power Save Plus モードの 6900/8900/9900 シリーズの電話機をウェイク アップできます。ただし、電話機をウェイク アップして Cisco Unified CM で登録するまで数分かかるため、緊急時はこの遅延を考慮する必要があります。
- スイッチに接続されている電話機は [Emergency Responder] ページで追跡できます。検出されずに電話機が Power Save Plus モードになると、これらは位置未確認と見なされ、[Unlocated Phones] ページに一覧表示されます。
- ネットワークがスタンドアロン Emergency Responder でバックアップ サブスクライバがない場合、システムまたは Emergency Responder の再起動の影響を考慮する必要があります。バックアップ サーバがないため、システムを再起動すると、既存の検出データは消失します。検出が行われると、新しい検出と見なされ、Emergency Responder は再起動前に Power Save Plus モードになった電話機のスイッチ ロケーション情報を識別しません。Emergency Responder 8.5 以前では、Emergency Responder はこれらの電話機が消失したと見なします。ただし、Emergency Responder 8.6 では、これらは [Unlocated Phones] ページまたは [IP Subnet] ページ（設定されている場合）に一覧表示されます。電話機の電源を投入して検出された場合、電話機は [Switch Port] ページに一覧表示されます。ただし、ERL を割り当てる際はこれらのスリープ中の電話機とウェイク アップ時間を考慮してください。Emergency Responder が停止した場合に Power Save Plus モードの電話機を消失しないようにするため、バックアップ Emergency Responder サブスクライバを設定することをお勧めします。次にパブリッシャ Emergency Responder サービスが停止したまたはサー

バがダウンした場合、サブスクライバは Power Save Plus モードの電話機を含む、検出データのバックアップ バージョンにアクセスします。再起動されると、検出データがサブスクライバから取得され、Power Save Plus モードの電話機は消失しません。

位置未確認の電話の識別

Emergency Responder が電話機の位置を特定できないと、電話機をデフォルト ERL に配置し、「位置未確認の電話機」のリストに載せます。このリストを使用して、電話機を別の ERL に割り当て直したり、Cisco ER が電話機の位置を特定できない問題を確認することができます。

Cisco ER で電話機の位置を確認できない原因はいくつかあります。

- Cisco ER で定義されていないスイッチに電話機が接続されています。
- 電話機がサポート対象外のデバイスに接続されています。ルータ ポート、ルータに接続されるハブ、サポート対象外のスイッチなどです。
- SNMP クエリーに応答しないなど、電話機が接続されているスイッチが現時点で到達不能です。
- 電話機は、異なる Cisco ER グループで処理されているスイッチに移動しました。この場合、位置未確認の電話機リストで、その電話機について Cisco ER グループ名が表示されます。
- 電話機に IP サブネットが設定されていない。

Cisco ER は位置未確認の電話機を適切な ERL に割り当てることができないため、ネットワーク上でこれらの電話機の位置が検出されない原因となっている問題のすべてを特定し、解決してください。Cisco ER でスイッチを定義するか、電話機をサポートされているスイッチ ポートに移動しても問題が解決されない場合は、手動で電話機を ERL に割り当てることができます。これらの問題を解決する方法の詳細については、「位置未確認の電話機が多すぎる」（P.11-2）を参照してください。

また、Emergency Responder では、位置未確認の電話機のリストに次の情報を表示します。

- 手動で割り当てられた電話機。
- 位置未確認の電話機として特定され、ERL に割り当てられた電話機。

はじめる前に

位置未確認の電話機を表示または設定するには、システム管理者または ERL 管理者の権限が必要です。

位置未確認の電話機の位置を特定するには、次の手順を実行します。

手順

ステップ 1　[ERL Membership]>[Unlocated Phones] を選択します。

[Unlocated Phones] ページが開きます。

ステップ 2　位置未確認の電話機を一覧表示するための検索条件を入力します。

ステップ 3　ERL を割り当てる電話機の隣にあるチェックボックスをオンにします。

ステップ 4　選択した電話機に割り当てる ERL を選択するには、[ERL Name] フィールドの隣にある [Search ERL] ボタンをクリックします。[Find ERL] ページが表示されます。

ステップ 5　[ERL Search Parameters] を入力し、[Find] をクリックします。検索結果が表示されます。

ステップ 6　位置未確認の電話機に割り当てる ERL の隣にあるオプション ボタンをクリックして、[Select ERL] をクリックします。[Find ERL] ページが閉じます。

ステップ 7　[Assign ERL] ボタンをクリックします。

電話機が ERL に割り当てられます（ただし、この電話機はまだリストに表示されたままです）。Cisco ER がこの電話機の位置を特定できない問題を解決すると、Cisco ER によって、この電話機はリストから削除され、ポートの割り当てに基づいて正しい ERL が割り当てられます。

（注） ERL を割り当て解除するには、電話機を選択して [Unassign ERL] ボタンをクリックします。

ヒント

- リストのタイトルにあるチェックボックスをオンにすると、表示されたページのすべての電話機を選択できます。
- 電話機の ERL への割り当ては、一度に 1 ページでしか実行できません。電話機が複数のページにわたって表示されている場合は、リストの下部にあるリンクを使用して、ページ間を移動します。

（注） Cisco ER では、アナログ電話機や PBX に接続された電話機は自動的には検出されません。このため、これらの電話機は位置未確認の電話機のリストに表示されません。このような電話機は手動で設定する必要があります。詳細については、「電話機の手動での定義」（P.4-63）を参照してください。

関連項目

- 「IP Subnet Phones」（P.A-54）
- 「スイッチ ポートの設定」（P.4-54）
- 「電話機の手動での定義」（P.4-63）

電話機の手動での定義

ネットワーク内のすべての緊急コールを管理するには、コールが Cisco Unified CM によってルーティングされるすべての電話機について、Emergency Responder に認識させる必要があります。Cisco ER が直接サポートしない電話機についても同様です。Cisco ER では、手動で定義された電話機からの緊急コールは、サポートされるスイッチ ポートに接続された電話機の緊急コールと同様に扱われます。唯一の相違点は、手動で定義された電話機が移動されても、Cisco ER ではその ERL を動的には変更できないということです。

次の条件のいずれかが該当する場合は、電話機を手動で定義する必要があります。

- アナログのようなタイプの電話機。Cisco ER では、このような電話機の自動トラッキングはサポートしません。
- 電話機が、ルータ ポート、ルータに接続されたハブ、サポートされていないスイッチ上のポートなどのサポートされていないポート上でホストされている。
- 電話機に IP サブネットが設定されていない。

手動定義が必要な電話機については、定期的にそのロケーションを監査し、Cisco ER で電話機の ERL 割り当てを更新する必要があるかどうかを確認してください。

（注）　新しいスイッチ ポートや位置未確認の電話機は、自動的にはデフォルト ERL に関連付けられません。このような電話機は、「ERL は設定されていない」ものとして扱われます。デフォルト ERL は、その電話機に他の ERL が設定されていない場合に、Cisco ER で内部的に使用されます。Cisco ER では、デフォルト ERL に [Switch Ports]、[Unlocated Phones]、[Manually Configured Phones]、または [IP Subnets] を設定することはできません。

（注）　Cisco Unified CM エクステンション モビリティで使用されている電話機を手動で追加することはできません。Cisco Unified CM エクステンション モビリティを使用すると、ユーザは電話機にログインでき、電話機はユーザの内線番号に割り当てられます。ただし、手動で定義された電話機では、（デバイスではなく）内線番号に基づいて電話機を定義します。このため、ログインしたユーザの内線番号は適切な ERL に割り当てられません。Cisco Unified CM エクステンション モビリティで使用する電話機が、サポートされたスイッチ ポートに接続されていることを確認してください。

はじめる前に

電話機を手動で定義するには、システム管理者または ERL 管理者の権限が必要です。

電話機を手動で定義するには、次の手順を実行します。

手順

ステップ 1　[ERL Membership]>[Manually Configured Phones] を選択します。

新たに [Find and List Manually Configured Phones] ページが開きます。

ステップ 2　変更が必要な電話機を検索するには、内線番号を入力して [Find] をクリックします。検索が実行され、検索結果が表示されます。

[Find and List Manually Configured Phones] ページの検索結果を使用して、電話機の削除、既存の電話機の変更、または新しい電話機の追加を行うことができます。

ステップ 3　電話機を削除するには、電話機のエントリの削除アイコンをクリックします。

ステップ 4　既存の電話機を変更するには：

a.　リストで電話機のエントリをクリックします。[Add/Modify Phones] ページが開き、編集ボックスに電話機の情報が表示されます。

b.　変更を加えて、[Update] をクリックします。電話機が更新されます。

c.　[Find and List Manually Configured Phones] ページに戻るには、[Back to Phone Search] をクリックします。

ステップ 5　新しい電話機を追加するには：

a.　[Add New Manual Phone] をクリックします。[Add New Manual Phone] ページが開きます。

b.　定義する電話機の情報を入力します。回線番号を入力し、ERL を選択する必要があります。電話機が IP 電話である場合は、その電話機の IP アドレスと MAC アドレスの入力も必要です。その他のフィールドはオプションで、主にユーザ情報として使用できます。

c.　選択したポートに割り当てる ERL を選択するには、[ERL Name] フィールドの隣にある [Search ERL] ボタンをクリックします。[Find ERL] ページが表示されます。

d.　[ERL Search Parameters] を入力し、[Find] をクリックします。検索結果が表示されます。

e.　手動の電話機に割り当てる ERL の隣にあるオプション ボタンをクリックして、[Select ERL] をクリックします。[Find ERL] ページが閉じます。

f. [Insert] をクリックします。電話機が手動定義の電話機のリストに追加されます。

g. [Find and List Manually Configured Phones] ページに戻るには、[Back to Phone Search] をクリックします。

関連項目

- 「Add New Manual Phone」（P.A-59）
- 「位置未確認の電話の識別」（P.4-62）
- 「ネットワークのハードウェアおよびソフトウェアの要件」（P.1-4）
- 「多数の手動設定電話機の ERL への一括割り当て」（P.4-65）
- 「手動設定電話機情報のエクスポート」（P.4-66）

多数の手動設定電話機の ERL への一括割り当て

必要な情報を含むファイルをインポートすることで、一度に多数の手動設定電話機を ERL に割り当てることができます。

大規模ネットワークの場合、手動設定電話機と ERL のマッピングをインポートすることで、時間を大幅に節約できます。

はじめる前に

スイッチ ポート定義をインポートするには、システム管理者または ERL 管理者の権限が必要です。

インポート ファイルを準備します。このファイルを作成する最も簡単な方法として、まず Cisco ER から手動設定電話機の詳細をエクスポートし（「手動設定電話機情報のエクスポート」（P.4-66）を参照）、スプレッドシート プログラムを使用して ERL を目的に合わせて変更して、電話機ロケーション情報を追加する方法があります。エクスポート ファイルを作成する前に、必ず、手動設定電話機および電話機更新プロセスを実行してください。これにより、すべての手動設定電話機に関するレコードがファイルに含まれるようになります。

ファイルをインポートする前に、[Import Manual Phones] ページで指定したロケーションにファイルをコピーする必要があります。このページの開き方については、次の手順で説明します。このページにあるリンクを使用して、インポート ファイルに必要なファイル形式に関する詳細情報を表示することもできます（必要な場合）。

ファイルをインポートする前に、Cisco ER に手動設定電話機を認識させる必要があります。インポートするすべての手動設定電話機が Cisco ER によって認識されていることを確認してください。

設定できるのは、ログインしている Cisco ER グループに定義されている手動設定電話機だけです。

多数の手動設定電話機を ERL に一括して割り当てるには、次の手順を実行します。

手順

ステップ 1　[ERL Membership]>[Manually Configured Phones] を選択します。

[Find and List Manually Configured Phones] ページが表示されます。

ステップ 2　[Import] をクリックします。

[Import Manually Configured Phones] ページが表示されます。

ステップ 3　プルダウン メニューを使用して、[Import Format (csv)] を選択します。

ステップ 4　ローカル マシンからファイルをアップロードするには、[Upload] をクリックします。アップロード ユーティリティの使用については、「ファイルのアップロード」（P.4-7）を参照してください。

ステップ 5　[Select File to Import] プルダウン メニューを使用してインポート ファイルを選択します。

ステップ 6　[Import] をクリックします。

ファイルがインポートされ、インポートの結果が表示されます。Cisco ER 設定に既存のデータは、インポート ファイルの ERL とポートのマッピング情報および手動設定電話機のロケーション情報で上書きされます。

ステップ 7　[Close] をクリックして、[Import Manually Configured Phone] ページを閉じます。

関連項目

- 「Switch Port Details」（P.A-48）
- 「Export Switch Ports」（P.A-50）
- 「少数のスイッチ ポートの一括設定」（P.4-54）
- 「スイッチ ポート情報のエクスポート」（P.4-57）
- 「ERL の使用」（P.4-29）

手動設定電話機情報のエクスポート

Emergency Responder の手動設定電話機の設定をエクスポートできます。この機能により、データのバックアップを行ったり、Cisco ER で多数の手動設定電話機マッピングの更新に使用するファイルを作成したりすることができます。エクスポート ファイルを編集して変更を加え、ファイルを再インポートして Cisco ER の情報を上書きできます。

はじめる前に

スイッチ ポート定義をエクスポートするには、システム管理者または ERL 管理者の権限が必要です。

手動設定電話機についての情報をエクスポートするには、次の手順を実行します。

手順

ステップ 1　[ERL Membership]>[Manually Configured Phones] を選択します。

[Find and List Manually Configured Phones] ページが開きます。

ステップ 2　[Export] をクリックします。

[Export Manual Phones] ページが開きます。

ステップ 3　[Select Export Format] プルダウン メニューからエクスポート ファイルの形式（csv）を選択します。

ステップ 4　[Enter Export File Name] フィールドに目的のファイル名を入力し、[Export] をクリックします。

ファイルがエクスポート先にエクスポートされます。

ステップ 5　エクスポートしたファイルをローカル システムにダウンロードするには、[Select file to download] プルダウン メニューからファイル名を選択し、[Download] をクリックします。

ステップ 6　[Close] をクリックして、[Export Manual Phones] ページを閉じます。

関連項目

- 「電話機の手動での定義」（P.4-63）
- 「多数の手動設定電話機の ERL への一括割り当て」（P.4-65）
- 「ERL の使用」（P.4-29）
- 「擬似電話機の追加」（P.4-67）

擬似電話機の追加

Emergency Responder 8.6 では、Cisco Unified Operations Manager 1.0 を使用して、Cisco ER のヘルスと機能性をモニタできます。Cisco ER で Cisco Unified Operations Manager を使用するには、Cisco ER で模擬電話機を設定し、テスト ERL として使用する ERL に模擬電話機を関連付けます。擬似電話機で緊急コールが発信されると、Cisco ER は関連付けたテスト ERL を使用してコールのルーティングを行います。

（注） テスト ERL は、従来型の ERL にのみ設定できます。Off-Premise ERL や Intrado ERL には、テスト ERL は設定できません。

詳細については、「テスト ERL の設定」（P.4-40）を参照してください。

緊急コール履歴の表示

Emergency Responder が処理対象とするネットワークで発信された緊急コールの履歴を表示できます。Cisco ER により、ERL で指定したオンサイト アラート担当者に緊急コール通知が送信されます。これらの担当者は、この通知に対処します。管理者のインターフェイスを使用して、オンサイト アラート担当者が参照するのと同じコール履歴を表示できます。また、オンサイト アラート担当者が作成したコールに関するコメントも参照できます。使用状況の報告や、コールのルーティングに関する問題のトラブルシューティングを行う場合に、コール履歴の確認が必要になることがあります。

ヒント [Call History] ページでは、最近の 10,000 のコールについて詳細情報を参照できます。Cisco ER の raw コール ログ ファイルでは、それよりも古いレコードを検索できます。詳細については、「コール履歴ログの収集」（P.11-29）を参照してください。

緊急コール履歴を表示するには、次の手順を実行します。

手順

ステップ 1　[Reports] > [Call History] を選択します。

[Call History] ページが表示されます。

ステップ 2　[Find] をクリックします。

すべてのコールの概要が表示されます。

ステップ 3　緊急コール リストの作成に使用する検索条件を入力します。

すべてのコールのリストを表示するには、検索条件を指定せずに [Find] をクリックします。

検索を絞り込むには、検索する項目を選択し、[Find] をクリックします。たとえば、特定の ERL で作成されたコールや、特定の内線番号から発信されたコールを表示できます。複数の条件を指定して検索するには、[More] をクリックし、検索フィールドを追加します。すべての検索条件に一致するコールのみを表示するには、リスト上部で [All] を選択します（AND 検索）。いずれかの検索条件に一致するコールを表示するには、リスト上部で [Any] を選択します（OR 検索）。

ステップ 4　検索条件に応じて表示されたコールのリストで、次のことを実行できます。

- コールの特性を確認します。
- ERL 名をクリックすると、ERL の詳細が表示されます。ERL の詳細で、コールの ALI を参照することもできます。
- コメントのフィールドで [edit] をクリックして、コメントを変更できます。別のウィンドウが開くため、そこで編集できます。

ヒント　多数のコールが検索条件と一致した場合は、複数ページにわたって表示されます。リストの下部にあるリンクを使用して、ページ間を移動します。

関連項目

- 「コール履歴ログの収集」（P.11-29）

CHAPTER 5

Cisco Emergency Responder の Intrado V9-1-1 Enterprise Services との併用

Cisco Emergency Responder（Emergency Responder）8.6 は、地域通信事業者（LEC）との直接接続の代わりに、Cisco Unified Communications 環境で Intrado V9-1-1 for Enterprise Service をサポートしています。Intrado V9-1-1 for Enterprise Service は、Intrado のお客様にローカル ルーティングおよび緊急サービス応答を提供します。Emergency Responder は、Intrado と連携して、企業ネットワーク上に存在する（構内）電話機や、企業ネットワークから離れて設置されている（構外）電話機への緊急サービスを提供します。

Cisco ER の設定、Emergency Responder ユーザの管理、ERL の操作、およびその他の関連項目の詳細については、「関連項目」（P.5-13）を参照してください。

次のトピックでは、Emergency Responder と Intrado V9-1-1 for Enterprise Service の連携動作の概要や、Intrado V-9-1-1 Enterprise ユーザをサポートするための Emergency Responder の設定および使用方法について説明します。

Cisco Emergency Responder での Intrado V9-1-1 for Enterprise Service のサポート方法

IntradoV9-1-1 for Enterprise Service のサブスクライバである場合は、Emergency Responder を使用して緊急コールの管理を簡素化できます。Emergency Responder には、ロケーション情報を直接 Intrado データベースに入力し、同期させることができるインターフェイスが用意されています。Emergency Responder は、構内電話機と構外電話機の両方の緊急コールのためのロケーション情報を提供し、Intrado および Cisco Unified CM と連携して緊急コールを完了します。

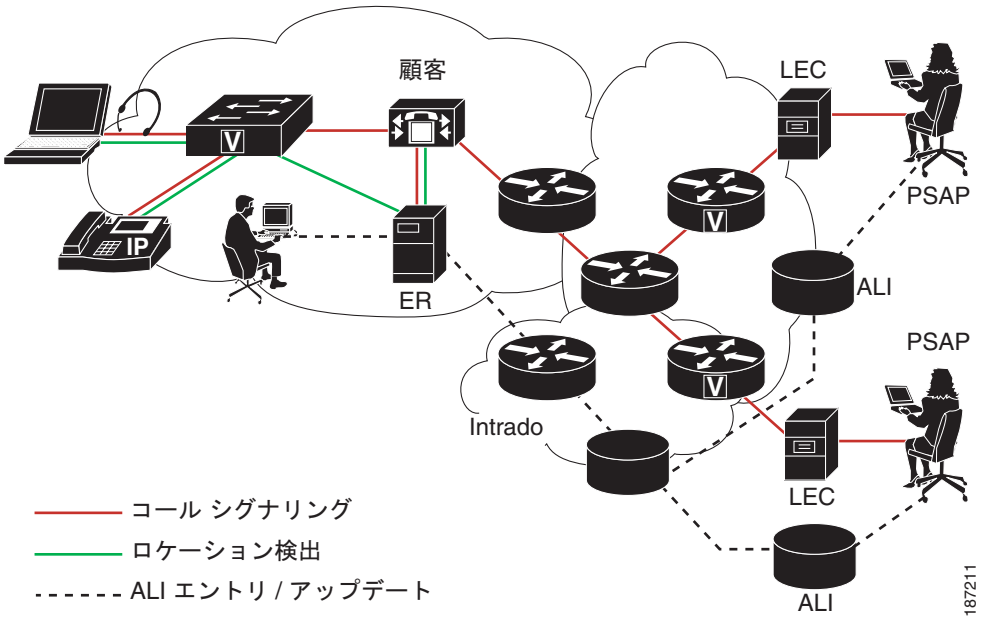
Emergency Responder は、IP サブネットまたは（誰かが手動で設定して割り当てた場合は）MAC アドレスを使用して IP 電話を追跡します。Emergency Responder は、電話機（構内、構外、位置未確認）のステータスを保持し、ALI/ELIN 情報をすべて Intrado に渡します。構内電話機のユーザは Cisco Unified Communication を使用して、緊急コールを Intrado および指定した緊急プロバイダーにルートします。

構外電話機を持つユーザは、自分のロケーションを入力し、この情報を各自のディレクトリ番号に関連付けるまで、緊急コールを発信することができません。ロケーション情報が確認されると、構外電話機から発信された緊急コールを完了できます。

（注）　ユーザは、構外ロケーションを DN ごとに 1 つしか設定できません。これは共有回線に適用されます。2 台の構外電話機で DN を共有している場合、ユーザはその DN に 1 つのロケーションしか関連付けることができません。

図 5-1 に、ユーザ、Emergency Responder、および Intrado の間の相互関係を示します。

図 5-1　ユーザ、Emergency Responder、および Intrado の間の相互関係について



Intrado V9-1-1 for Enterprise Service を使用して緊急コールが発信された場合の処理

ユーザが緊急コールを発信すると、次の処理が実行されます。

1. Cisco Unified CM が、そのコールを Emergency Responder にルーティングします。
2. Emergency Responder が、そのコールを Intrado にルーティングします。
3. Intrado は発信者の 10 桁の ELIN を受信し、この発信者番号から発信者の ALI データ取得します。
4. Intrado がコールを完了します。

Intrado V9-1-1 for Enterprise Service をサポートするための Cisco Emergency Responder の設定

Intrado での緊急サービスのサポートを確認したら、Intrado V9-1-1 for Enterprise Service をサポートするように Emergency Responder を設定する必要があります。

Intrado ERL を作成する前に、表 5-1 で説明されている作業を完了する必要があります。構外ユーザのサポートの詳細については、「構外ユーザをサポートするための Emergency Responder の設定」（P.5-8）を参照してください。

表 5-1　Intrado 用に Emergency Responder を設定するための作業一覧

作業	説明	注
1.	検証および更新インターフェイス（VUI）で、次の設定を行います。 a. Intrado によって提供された証明書をアップロードします。 b. 証明書を検証します。 c. Intrado アカウント情報を設定します。	「Intrado VUI 設定の実行」（P.5-3）を参照してください。
2.	Emergency Responder サーバで、コールを Intrado にルーティングするためのルート パターンを設定します。	「Cisco Emergency Responder 上での Intrado ルート パターンの設定」（P.5-4）を参照してください。
3.	Cisco Unified CM サーバで、コールを Intrado にルーティングするためのルート パターンとゲートウェイを設定します。	『Cisco Unified CM Administration Guide』の「Understanding Route Plans」の章および『Cisco Unified CM Administration Guide』の「Gateway Configuration」の章を参照してください。
4.	Intrado ERL を作成し、その Intrado ERL の ALI データの Intrado TN データベースに対する妥当性および整合性を確認します。	「Intrado ERL の設定」（P.5-5）と「ALI の不一致の調整」（P.5-6）を参照してください。
5.	Intrado ERL をスイッチ ポート、IP サブネット、および位置未確認の電話機に割り当てます。	ERL のスイッチ ポートへの割り当てについては、「スイッチ ポートの設定」（P.4-54）を参照してください。 ERL の IP サブネットへの割り当てについては、「IP サブネットベースの ERL の設定」（P.4-38）を参照してください。 ERL の位置未確認の電話機への割り当てについては、「位置未確認の電話の識別」（P.4-62）を参照してください。

Intrado VUI 設定の実行

Intrado VUI を設定するには、その前に Intrado のアカウント情報と証明書が必要です。

（注）　Emergency Responder サブスクライバへのフェールオーバーが発生した場合に緊急サービスのサポートを続行するには、証明書ファイルをその Emergency Responder サブスクライバに個別にアップロードする必要があります。

Intrado VUI 設定を行うには、次の手順を実行します。

手順

ステップ 1　Emergency Responder から、[System]>[Intrado VUI Settings] の順に選択します。

[Intrado VUI Settings] ページが表示されます。

ステップ 2　[Upload Certificate] をクリックします。[Upload Certificate] ウィンドウが開きます。[Browse] ボタンを使用して Intrado 証明書ファイルを見つけ、そのファイルを選択して [Upload] ボタンをクリックします。

ステップ 3　隣接するテキスト ボックスに、[Certificate Password] と [VUI URL] を入力します。[Test and Validate] をクリックします。

ステップ 4　次のアカウント情報を入力します。

- VUI Schema URL
- Intrado Account ID
- Max VUI Connections

ステップ 5　[Update] をクリックします。

Intrado VUI の設定の詳細については、「Intrado VUI Settings」（P.A-12）を参照してください。

関連項目

- 「Cisco Emergency Responder 上での Intrado ルート パターンの設定」（P.5-4）
- 「Intrado ERL の設定」（P.5-5）
- 「ALI の不一致の調整」（P.5-6）

Cisco Emergency Responder 上での Intrado ルート パターンの設定

Intrado V9-1-1 for Enterprise Service で何らかの緊急コールを完了できるようにするには、コールを Intrado にルーティングするためのルート パターンを設定しておく必要があります。

Intrado のルート パターンを作成するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder から、[System] > [Telephony Settings] の順に選択します。

[Telephony Settings] ページが表示されます。

ステップ 2　[Intrado Route Pattern Settings] で、Intrado のルート / トランスレーション パターンを入力して [Add] ボタンをクリックします。

Intrado ERL の設定

Intrado ERL を追加する前に、まず Intrado ルート パターンを設定する必要があります。

（注）　Intrado ERL は、次の点で、従来の ERL とは異なります。

- ルート パターンは、[Telephony Settings] Web ページ内の事前に設定されたリストからしか選択できません。
- Intrado Validation & Update Interface（VUI; 検証および更新インターフェイス）を使用して、Intrado から ALI データを照会し、検証できます。
- 緊急コールを正常にルーティングできるようにするには、Intrado VUI を使用して Intrado に ALI データ（TN アップデート）を送信しておく必要があります。

Intrado ERL を設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder から、[ERL] > [Intrado ERL] > [Intrado ERL(Search and List)] の順に選択します。

[Find Intrado ERL Data] ページが表示されます。

ステップ 2　[Add New ERL] ボタンをクリックします。

[Add New ERL] ウィンドウが開きます。各フィールドの詳細な説明については、「Intrado ERL (Search and List)」（P.A-31）を参照してください。

ステップ 3　[ERL Information] に情報を入力します。

ステップ 4　[ALI Details] をクリックします

[ALI Information] ウィンドウが開きます。

ステップ 5　ALI 情報を入力します。Intrados MSAG データベース内のアドレスを検索するには、[Query from Intrado] をクリックします。

ステップ 6　[ALI Information] への入力を完了したら、[Pre-validate from Intrado] をクリックします。

ステップ 7　[Add New ERL] ウィンドウをアクティブ ウィンドウにして（アクティブになっていない場合）、[Insert] をクリックします。

ERL とその ALI が保存されます。

Intrado ERL のインポート

複数の ERL があり、それらをすべて一度に追加したい場合は、複数の ERL 定義を含むファイルを作成し、すべての ERL を Emergency Responder 設定に一度にインポートすることができます。ERL のインポートの詳細については、「複数の ERL の一括インポート」（P.4-37）を参照してください。

Intrado ERL 情報のエクスポート

ERL の設定のバックアップや移動などに使用するために ERL エクスポート ファイルを作成するには、[Export ERL] ページを使用します。ERL のインポートの詳細については、「ERL 情報のエクスポート」（P.4-41）を参照してください。

関連項目

- 「Intrado VUI 設定の実行」（P.5-3）
- 「Cisco Emergency Responder 上での Intrado ルート パターンの設定」（P.5-4）
- 「ALI の不一致の調整」（P.5-6）

ALI の不一致の調整

Emergency Responder を使用すると、Intrado VUI のレコードをデータベース内のレコードと比較し、不一致を含む ALI レコードを表示することができます。各レコードを調べて、ローカル レコードを Intrado の情報で更新するか、または Intrado のレコードを更新するかを選択できます。

ALI の不一致のレコードを調整するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration で、[ERL] > [Intrado ERL] > [View ALI Discrepancies] の順に選択します。

[View Intrado ALI Discrepancies] ページが表示されます。

ステップ 2　特定の ELIN を見つけるための検索条件を入力し、[Find] をクリックします。または、Intrado ALI のすべての不一致を表示するには、検索条件を指定せずに [Find] をクリックします。検索結果が表示されます。

ステップ 3　表示する ELIN の横にあるオプション ボタンをクリックするか、または [View ALI Discrepancies] ボタンをクリックして [View Intrado ALI Discrepancies for a particular ELIN] を起動します。

[View Intrado ALI Discrepancies for a particular ELIN] ウィンドウが表示されます。

ステップ 4　ローカルの Emergency Responder データベースまたは Intrado のどちらかから正しいデータを選択します。

ステップ 5　ローカルの Emergency Responder データベースへの変更を保存するには、[Save] をクリックします。Intrado VUI への変更を保存するには、[Save Intrado ALI Info] をクリックします。

ステップ 6　このウィンドウを閉じるには、[Close] をクリックします。

関連項目

- 「Intrado VUI 設定の実行」（P.5-3）
- 「Cisco Emergency Responder 上での Intrado ルート パターンの設定」（P.5-4）
- 「Intrado ERL の設定」（P.5-5）

ERL データの移行

Emergency Responder は、既存の従来の ERL の Intrado ERL への移行と、その逆方向の移行をサポートしています。

従来の ERL データの Intrado ERL データへの移行

従来の ERL を Intrado ERL に移行するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration で、[ERL] > [ERL Migration Tool] の順に選択します。

[ERL Migration Tool] ページが表示されます。

ステップ 2　検索パラメータのドロップダウン ボックスで [Conventional ERL] を選択し、検索条件を入力して [Find] をクリックします。

ステップ 3　ERL 名の横にあるチェックボックスをオンにすることによって、移行する ERL を選択します。

[Enter Route Patterns for ERL Migration] ウィンドウが表示されます。

ステップ 4　ドロップダウン メニューから、更新されたルート パターンを選択します。

ステップ 5　[Migrate to Intrado ERL] をクリックします。

関連項目

- 「Intrado V9-1-1 for Enterprise Service をサポートするための Cisco Emergency Responder の設定」（P.5-3）
- 「Intrado ERL データの従来の ERL データへの移行」（P.5-7）

Intrado ERL データの従来の ERL データへの移行

Intrado ERL を従来の ERL に移行するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration で、[ERL] >[ERL Migration Tool] の順に選択します。

[ERL Migration Tool] ページが表示されます。

ステップ 2　検索パラメータのドロップダウン ボックスで [Intrado ERL] を選択し、検索条件を入力して [Find] をクリックします。

ステップ 3　ERL 名の横にあるチェックボックスをオンにすることによって、移行する ERL を選択します。

[Enter Route Patterns for ERL Migration] ウィンドウが表示されます。

ステップ 4　隣接するテキスト ボックスに、更新されたルート パターン / トランスレーション パターンを入力します。

ステップ 5　[Migrate to Conventional ERL] をクリックします。

関連項目

- 「従来の ERL データの Intrado ERL データへの移行」（P.5-7）
- 「ERL について」（P.4-30）

構外ユーザをサポートするための Emergency Responder の設定

Cisco Emergency Responder 8.6 では、企業ネットワークの外部（構外）にいるユーザが緊急コールを発信できます。構外からの緊急コールのサポートには、次のものが必要です。

- Cisco Emergency Responder 8.6
- Cisco Unified CM 7.1 以降のバージョン。
- Intrado V9-1-1 Enterprise Services

構外ユーザに対する Emergency Responder のサポートを設定するには、次の作業を完了します。

表 5-2　構外ユーザを設定するための作業一覧

作業	説明	注
1.	Intrado と併用するように Emergency Responder を設定します。	「Intrado V9-1-1 for Enterprise Service をサポートするための Cisco Emergency Responder の設定」（P.5-3）を参照してください。
2.	構外をサポートするように Cisco Unified CM で Emergency Responder Location Management を有効にします。	「Cisco Unified Communications Manager での Emergency Responder Location Management の設定」（P.5-9）を参照してください。
3.	Cisco Unified CM で Emergency Responder のための AXL アプリケーション ユーザを設定します。	「AXL アプリケーション ユーザの設定」（P.5-10）を参照してください。
4.	Cisco Unified Communications Manager を使用して AXL 認証を設定します。	「AXL 認証の設定」（P.5-11）を参照してください。
5.	Off-Premise ERL を設定します。	「Off-Premise ERL の設定」（P.5-11）を参照してください。
6.	Off-Premise ERL を IP サブネットおよび位置未確認の電話機に割り当てます。	ERL の IP サブネットへの割り当てについては、「IP サブネットベースの ERL の設定」（P.4-38）を参照してください。 ERL の位置未確認の電話機への割り当てについては、「位置未確認の電話の識別」（P.4-62）を参照してください。 **（注）** Off-Premise ERL をスイッチ ポートに割り当てることはできません。

Off-Premise ERL を設定すると、ユーザは [Cisco Unified CM User Option] ページから、自分の構外電話機用のロケーション情報を入力できます。

（注）　Emergency Responder 構外ロケーション管理機能を使用するエンドポイントのための DID として、ダイヤル可能な 10 桁の北米番号計画番号が必要です。ただし、Cisco Unified CM で短縮された回線番号と外部電話番号マスクを設定することによって、TN アップデートと Intrado への 911 コールの発信回線番号の両方で 10 桁の DID を作成できます。

関連項目

- 「Cisco Unified Communications Manager での Emergency Responder Location Management の設定」（P.5-9）
- 「AXL アプリケーション ユーザの設定」（P.5-10）
- 「AXL 認証の設定」（P.5-11）
- 「Off-Premise ERL の設定」（P.5-11）

Cisco Unified Communications Manager での Emergency Responder Location Management の設定

ユーザが Emergency Responder Location Management サーバを使用して自分の構外ロケーションを入力できるようにするには、Cisco Unified CM サーバでそのサーバを設定しておく必要があります。

Cisco Unified CM で Cisco Emergency Location Manager を有効にするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CM 管理から、[System] > [Application Server] の順に選択します。

ステップ 2　[Add New] ボタンをクリックします。

[Application Server Configuration] ページが表示されます。

ステップ 3　[Application Server Type] ドロップダウン ボックスから、[Application Server] を選択します。[Next] をクリックします。

ステップ 4　Emergency Responder Off-Premise アプリケーションを識別する名前を入力します。

この名前は、[User Option] ページのナビゲーション ドロップダウン ボックスに表示され、[Emergency Responder Off-Premise] ページに移動するためにユーザによって選択されます。

ステップ 5　[Emergency Responder Off-Premise] ページの URL を入力します。この URL の形式は http://*cer_host*/ofpuser です。ここで、*cer_host* は Emergency Responder パブリッシャまたは Emergency Responder サブスクライバの名前または IP アドレスです。

（注）　Cisco Unified CM 管理では、Emergency Responder パブリッシャと Emergency Responder サブスクライバの両方を個別のアプリケーション サーバとして入力する必要があります。

ステップ 6　[Save] をクリックします。

関連項目

- 「AXL アプリケーション ユーザの設定」（P.5-10）
- 「AXL 認証の設定」（P.5-11）

- 「Off-Premise ERL の設定」（P.5-11）

AXL アプリケーション ユーザの設定

構外ユーザが Emergency Responder の構外ユーザ Web サイトにログインできるように、Cisco Unified CM で Emergency Responder のための AXL アプリケーション ユーザを設定する必要があります。

AXL アプリケーションを設定するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager で、[User Management]>[Application User] の順に選択します。[Add New] ボタンをクリックします。

Cisco Unified Communications Manager によって [Application User Configuration] ページが表示されます。

ステップ 2　次の必須フィールドに入力します。

- [User ID]：「AXL Application User」などのわかりやすい名前を使用します。
- [Password]：このユーザのパスワードを入力します。
- [Confirm Password]：このユーザのパスワードを再入力します。

ステップ 3　[Save] をクリックします。

ステップ 4　上部にある [Cisco Unified Communications Manager] メニューで、[User Management]>[User Group] の順に選択します。

ユーザ グループの検索ページが表示されます。

ステップ 5　検索条件に standard を入力し、[Find] をクリックします。

名前が standard で始まるユーザ グループの一覧が表示されます。

ステップ 6　[Standard CCM Admin Users] リンクをクリックして、[User Group] 設定ページを表示します。

ステップ 7　[Add App Users to Group] をクリックします。

[Find and List Application Users] ポップアップ ウィンドウが表示されます。

ステップ 8　ステップ 2 で作成したユーザ ID を検索条件として入力し、[Find] をクリックします。

アプリケーション ユーザの一覧が表示されます。

ステップ 9　ユーザ ID の隣にあるチェックボックスをオンにして [Add Selected] をクリックします。

Cisco Unified CM によって、選択したユーザが [Standard CCM Admin Users] ユーザ グループに追加されます。

ステップ 10　[User Management]>[User Group] の順に選択します。

ユーザ グループの検索ページが表示されます。

ステップ 11　検索条件として **standard** を入力し、[Find] をクリックします。

名前が Standard で始まるユーザ グループの一覧が表示されます。

ステップ 12　[Standard TabSync User] グループをクリックします。

ステップ 13　ステップ 7 ～ 9 を繰り返して、ユーザを [Standard TabSync User] グループに追加します。

ステップ 14　[User Management]>[User Group] の順に選択します。

ユーザ グループの検索ページが表示されます。

ステップ 15　検索条件として **standard** を入力し、[Find] をクリックします。

名前が Standard で始まるユーザ グループの一覧が表示されます。

ステップ 16　[Standard RealtimeAndTraceCollection] グループをクリックします。

ステップ 17　ステップ 7 ～ 9 を繰り返して、ユーザを [Standard RealtimeAndTraceCollection] グループに追加します。

AXL 認証の設定

Emergency Responder と Cisco Unified CM の間の AXL 認証を設定するには、次の手順を実行します。

ステップ 1　Emergency Responder から、[Phone Tracking] > [Cisco Unified CM] の順に選択します。

ステップ 2　[AXL Setting] で、次の情報を入力します。

- AXL Username
- AXL パスワード
- AXL Port Number

ステップ 3　[Insert] をクリックします。

Off-Premise ERL の設定

従来の ERL とは異なり、Off-Premise ERL では ELIN または ALI 情報の入力は必要ありません。電話機の ERL は、IP サブネットおよび電話機の MAC アドレスの割り当てによって追跡されます。

（注）　Off-Premise ERL は、IP サブネット、位置未確認の電話機、および手動電話機にのみ割り当てることができます。Off-Premise ERL をスイッチ ポートに割り当てることはできません。

Off-Premise ERL を設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder から、[ERL] > [Off-Premise ERL] > [Off-Premises ERL (Search and List)] の順に選択します。

ステップ 2　[Add New ERL] ボタンをクリックします。

ステップ 3　[Add New ERL] ウィンドウで次の情報を入力し、[Insert] をクリックします。

- ERL 名
- 説明
- Intrado ルート パターン / トランスレーション パターン
- オンサイト アラート

[Add New ERL] ウィンドウで情報を入力します。各フィールドの詳細な説明については、「Off-Premises ERL (Search and List)」（P.A-27）を参照してください。

（注）　Off-Premise ERL を追加できるようにするには、まず Intrado ルート パターンを追加する必要があります。

Off-Premise ERL のインポート

複数の ERL があり、それらをすべて一度に追加したい場合は、複数の ERL 定義を含むファイルを作成し、すべての ERL を Emergency Responder 設定に一度にインポートすることができます。ERL のインポートの詳細については、「複数の ERL の一括インポート」（P.4-37）を参照してください。

Off-Premise ERL 情報のエクスポート

ERL の設定のバックアップや移動などに使用するために ERL エクスポート ファイルを作成するには、[Export ERL] ページを使用します。ERL のインポートの詳細については、「ERL 情報のエクスポート」（P.4-41）を参照してください。

Intrado アップデートのスケジューリング

Emergency Responder と Intrado の間で、ALI およびセカンダリ ステータスのアップデートのスケジュールを作成できます。スケジュールされた ALI アップデートは、新しく作成された TN レコードを Intrado に送信します。スケジュールされたセカンダリ ステータスのアップデートによって、クエリーが、修正されたエラーを含むレコードに関する情報を要求している Intrado に送信されます。

Emergency Responder と Intrado の間のスケジュールされたアップデートを追加するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder から、[ERL] > [Intrado ERL] > [Intrado Schedule] の順に選択します。

[Intrado Schedule] ページが表示されます。

ステップ 2　アップデートをスケジュールする曜日と時刻を選択します。

ステップ 3　このスケジュールをアクティブにする場合は、[Enable Schedule] ボックスをオンにします。

ステップ 4　[ALI Update Schedule] と [Secondary Status Update Schedule] のどちらかを選択します。

ステップ 5　スケジュールをスケジュールのリストに追加するには、[Add] をクリックします

Emergency Responder と Intrado の間のスケジュールされたアップデートを更新するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder から、[ERL] > [Intrado ERL] > [Intrado Schedule] の順に選択します。

[Intrado Schedule] ページが表示されます。

ステップ 2　更新するスケジュールの隣にある [Edit] リンクをクリックします。

ステップ 3　曜日と時刻を選択します。

ステップ 4　このスケジュールを有効にするには、[Enable Schedule] ボックスをオンにします。

ステップ 5　[Update] をクリックしてスケジュールの一覧のスケジュールを変更します。

関連項目

- 「Cisco Emergency Responder ユーザの管理」（P.4-10）
- 「Cisco Emergency Responder ロールの管理」（P.4-14）
- 「Cisco Emergency Responder ユーザ グループの管理」（P.4-16）
- 「Cisco Emergency Responder へのログインおよびログアウト」（P.4-19）
- 「サーバおよびサーバ グループの設定」（P.4-21）
- 「8.6 Cisco Emergency Responder クラスタおよびクラスタ DB ホスト」（P.4-28）
- 「Cisco Emergency Responder で指定された Cisco Unified Communications Manager クラスタの変更」（P.4-29）
- 「ERL の使用」（P.4-29）
- 「Cisco Emergency Responder のスイッチの設定」（P.4-44）
- 「電話機の管理」（P.4-54）
- 「Secondary Status」（P.A-33）
- 「Intrado Schedule」（P.A-34）

CHAPTER 6

Cisco Emergency Responder 8.6 Serviceability の設定

Cisco Emergency Responder（Emergency Responder）8.6 には、Emergency Responder 8.6 Serviceability 機能にアクセスできる Serviceability インターフェイスが含まれています。これらの機能は、[Tools]、[SNMP]、[System Monitor]、[Emergency Responder Logs] という、Serviceability Web インターフェイス上の 4 つのメイン メニューの下にグループ化されています。すべての Serviceability Web ページの詳細については、付録 B「Cisco Emergency Responder のサービスアビリティ Web インターフェイス」を参照してください。

次のトピックでは、Emergency Responder 8.6 Serviceability 機能を設定および使用する方法について説明します。

Serviceability ツールの使用

次のトピックでは、Emergency Responder 8.6 Serviceability ツールについて説明します。

Control Center の使用

Control Center を使用すると、選択された Emergency Responder 8.6 システム上で実行されているサービスに対するアクションを実行できます。

選択された Emergency Responder 8.6 システム上で実行されているサービスに対するアクションを実行するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[Tools]>[Control Center] の順に選択します。

[Control Center] ページが表示されます。

ステップ 2　サービスのステータスを変更するには、[Service Name] の左側にあるオプション ボタンをクリックし、必要なアクションに対応するボタンをクリックします。選択可能なアクションは次のとおりです。

- Start
- Stop
- Restart

（注）　Cisco Tomcat および Cisco IDS サービスは、Emergency Responder Serviceability Web サイトから開始、停止、または再開することはできません。これらのサービスは、CLI を使用してのみ開始、停止、または再開できます。詳細については、付録 F「コマンド ライン インターフェイス」を参照してください。

ステップ 3　ページを更新するには、[Refresh] をクリックします。

関連項目

- 「Control Center」（P.B-1）

Event Viewer の使用

Event Viewer を使用すると、過去 6 か月間のイベントを表示できます。

過去 6 か月間のイベントを表示するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[Tools]>[Event Viewer] の順に選択します。

[Event Viewer] ページが表示されます。

ステップ 2　過去 6 か月間に発生したすべてのイベントを検索するには、検索条件を入力せずに [Find] をクリックします。

特定の条件に一致するイベントを検索するには、検索条件を入力します。

- 特定の月を選択すると、その月のイベントだけが表示されます。
- [Type] を選択した場合は、検索に使用するタイプを右側のプルダウン メニューから選択できます。

  [Module] を選択した場合は、検索に使用するモジュールを右側のプルダウン メニューから選択できます。

（注）　使用可能なタイプとモジュールのリストについては、「Event Viewer」（P.B-2）を参照してください。

検索条件を入力したら、[Find] をクリックします。

ステップ 3　結果を昇順または降順でソートできます。ソートを実行するには、[Time]、[Type]、または [Module] 列見出しの横にある上矢印または下矢印をクリックします。

関連項目

- 「Event Viewer」（P.B-2）

SNMP の設定

Emergency Responder 8.6 は、SNMP V1/V2C および V3 をサポートしています。Serviceability Web インターフェイスを使用すると、SNMP V1/V2C（コミュニティ ストリングと通知先）および SNMP V3（ユーザと通知先）を設定できます。

各 SNMP バージョンには、セキュリティ モデルとセキュリティ レベルがあります。ユーザは、セキュリティ モデルと指定されたセキュリティ レベルで定義されたグループに割り当てられます。各グループには、MIB オブジェクトのセットに対する読み取りおよび書き込みについて定義されたセキュリティ アクセス レベルもあります。これらは *ビュー*と呼ばれます。スイッチには、デフォルト ビュー（すべての MIB オブジェクト）と、SNMP V1 および V2C セキュリティ モデル用に定義されたデフォルト グループがあります。SNMP V3 は、メッセージの整合性、認証、および暗号化をカバーする追加のセキュリティ機能を提供します。さらに、SNMP V3 では、MIB ツリーの特定の領域へのユーザ アクセスも制御されます。

次のトピックでは、SNMP V1/V2C および V3 の設定方法について説明します。

- 「SNMP コミュニティ ストリングの設定」（P.6-3）
- 「SNMP V1/V2C 通知ストリングの設定」（P.6-4）
- 「SNMP ユーザの設定」（P.6-5）
- 「SNMP V3 通知先の設定」（P.6-5）
- 「MIB2 の設定」（P.6-6）

SNMP コミュニティ ストリングの設定

SNMP を設定することによって、Emergency Responder SNMP エージェントへの SNMP アクセスを制御できます。管理ステーションは、まず認証のための有効なコミュニティ ストリングを送信する必要があります。

コミュニティ ストリングを設定するには、コミュニティ ストリング名、そのコミュニティ ストリングを使用して認証できるホストの IP アドレス、および許可されるアクセス権限を入力します。使用可能なアクセス権限は次のとおりです。

- ReadOnly
- ReadWrite
- ReadWriteNotify
- NotifyOnly
- None

SNMP コミュニティ ストリングを設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[SNMP]>[V1/V2C Configuration]>[Community String] の順に選択します。

[SNMP Community String Configuration] ページが表示されます。

ステップ 2　[Community String Name] テキスト ボックスに、コミュニティ ストリングの名前を入力します。

ステップ 3　SNMP パケットを受け入れる特定のホストを指定するには、[Accept SNMP Packets only from these hosts] オプション ボタンをクリックし、テキスト ボックスに IP アドレスを入力して [Insert] をクリックします。

任意のホストから SNMP パケットを受け入れるには、[Accept SNMP Packets from any host] オプション ボタンをクリックします。

ステップ 4　既存のホストを削除するには、ホストの IP アドレスを選択し、[Remove] をクリックします。

ステップ 5　[Access Privileges] プルダウン メニューから、ホストのアクセス権限を選択し、[Insert] をクリックします。

関連項目

- 「SNMP Community String Configuration」（P.B-4）

SNMP V1/V2C 通知ストリングの設定

SNMP V1/V2C 通知ストリングを使用すると、SNMP V1/V2C トラップ メッセージの送信先のホストとポートを選択できます。すべての通知ストリングを認証する必要があります。SNMP V1/V2C を使用する場合、認証はコミュニティ ストリングを使用して実行されます。

SNMP V1/V2C 通知ストリングを設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[SNMP]>[V1/V2C Configuration]>[Notification Destination] の順に選択します。

[SNMP Notification Destination Configuration] ページが表示されます。

ステップ 2　新しい SNMP 通知先を追加するには、[Add New] をクリックします。

ステップ 3　[Host IP Addresses] プルダウン メニューから、[Add New] を選択します。追加のフィールドが表示されます。

ステップ 4　テキスト ボックスに、ホストの IP アドレスとポート番号を入力します。

ステップ 5　[V1] または [V2C] オプション ボタンのどちらかをクリックして、SNMP バージョンを選択します。

[V1] をクリックすると、[Community String] プルダウン メニューが表示されます。ステップ 7 に進みます。

[V2C] をクリックすると、[Notification Type] プルダウン メニューが表示されます。

ステップ 6　[Notification Type] プルダウン メニューから、[Inform] または [Trap] を選択します。[Community String] プルダウン メニューが表示されます。

ステップ 7　[Community String] プルダウン メニューから、使用するコミュニティ ストリングを選択します。

ステップ 8　[Insert] をクリックします。

変更を有効にするには SNMP マスター エージェントを再起動する必要があることを知らせるメッセージが表示されます。[OK] をクリックして SNMP マスター エージェントを再起動するか、または [Cancel] をクリックしてマスター エージェントを再起動せずに続行します。

[SNMP Notification Destination Configuration] ページにある宛先のリストに通知先が追加されます。

ステップ 9　通知先を追加するには、ステップ 2 ～ステップ 8 を繰り返します。

関連項目

- 「SNMP V1/V2c Notification Destination Configuration」（P.B-6）

SNMP ユーザの設定

SNMP V3 は、メッセージの整合性、認証、および暗号化をカバーする追加のセキュリティ機能を提供します。さらに、SNMP V3 では、MIB ツリーの特定の領域へのユーザ アクセスも制御されます。

SNMP ユーザを設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[SNMP]>[V3 Configuration]>[User] の順に選択します。

[SNMP User Configuration] ページが表示されます。

ステップ 2　新しい SNMP ユーザを追加するには、[Add New] をクリックします。

ステップ 3　[User Name] テキスト ボックスに、新しいユーザの名前を入力します。

ステップ 4　認証を要求するには、[Authentication Required] チェックボックスをオンにして、[Password] テキスト ボックスにパスワードを入力し、[Reenter Password] テキスト ボックスにパスワードを再入力してから、[MD5] または [SHA] オプション ボタンのどちらかをクリックして使用するプロトコルを選択します。[Insert] をクリックして、ユーザを追加します。

ステップ 5　情報のプライバシーを要求するには、[Privacy Required] チェックボックスをオンにして、[Password] テキスト ボックスにパスワードを入力し、[Reenter Password] テキスト ボックスにパスワードを再入力してから、[DES] チェックボックスをクリックします。

（注）　変更を有効にするには SNMP マスター エージェントを再起動する必要があることを知らせるメッセージが表示されます。[OK] をクリックして SNMP マスター エージェントを再起動するか、または [Cancel] をクリックしてマスター エージェントを再起動せずに続行します。

[SNMP User Configuration] ページのユーザのリストに新しいユーザが追加されます。

ステップ 6　ユーザを追加するには、ステップ 2 ～ステップ 4 を繰り返します。

関連項目

- 「SNMP User Configuration」（P.B-7）

SNMP V3 通知先の設定

SNMP V3 の通知先ストリングでは、各通知ストリングがユーザと関連付けられるため強力なセキュリティを提供します。ユーザを設定する場合は、必要なレベルの認証とセキュリティを指定できます。

SNMP V3 通知ストリングを設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[SNMP]>[V3 Configuration]>[Notification Destination] の順に選択します。

[SNMP Notification Destination Configuration] ページが表示されます。

ステップ 2　新しい SNMP 通知先を追加するには、[Add New] をクリックします。

ステップ 3　[Host IP Addresses] プルダウン メニューから、[Add New] を選択します。追加のフィールドが表示されます。

ステップ 4　テキスト ボックスに、ホストの IP アドレスとポート番号を入力します。

ステップ 5　[Notification Type] プルダウン メニューから、[Inform] または [Trap] を選択します。

[Trap] を選択すると、[Security Level] プルダウン メニューが表示されます。ステップ 7 に進みます。

[Inform] を選択すると、リモート エンジン ID の入力を求めるプロンプトが表示されます。

ステップ 6　リモート エンジン ID を入力します。

ステップ 7　[Security Level] プルダウン メニューから、必要なセキュリティ レベルを選択します。

ステップ 8　[User Name] の左側にあるオプション ボタンをクリックして、通知先に関連付けるユーザを選択します。

ステップ 9　通知先を追加するには、ステップ 2 ～ステップ 8 を繰り返します。

関連項目

- 「SNMP V3 Notification Destination Configuration」（P.B-9）

MIB2 の設定

SNMP MIB2 ツールでは、MIB2 管理ノードの連絡先担当者、および管理ノードの物理ロケーションを指定できます。

MIB2 を設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[SNMP]>[System Group Configuration]>[MIB2 System Group Configuration] の順に選択します。

[SNMP MIB2 Configuration] ページが表示されます。

ステップ 2　[System Contact] テキストボックスに連絡先の名前を入力します。

ステップ 3　[Location] テキスト ボックスに、管理ノードのロケーションを入力します。

ステップ 4　ページの左上隅にある [Update] アイコンをクリックします。

ステップ 5　情報を変更するには、ページの左上隅にある [Clear] アイコンをクリックし、[System Contact] および [Location] テキスト ボックスに新しい情報を入力して、[Update] アイコンを再びクリックします。

関連項目

- 「MIB2 SystemGroup Configuration」（P.B-11）

System Monitor ツールの使用

次のトピックでは、System Monitor ツールの使用方法について説明します。

CPU and Memory Usage ツールの使用

CPU and Memory Usage ツールを使用して、この情報を監視し、記録できます。デフォルトでは、情報は 30 秒ごとに更新されます。この情報の更新頻度は変更できます。または、自動更新機能を無効にすることもできます。

CPU and Memory Usage ツールを使用するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[System Monitor]>[CPU & Memory Usage] の順に選択します。

[CPU and Memory Usage] ページが表示されます。

このページは、[Processors] と [Memory] の 2 つのセクションに分かれています。表示される情報の詳細については、表 B-12（P.B-12）を参照してください。

ステップ 2　ページの更新間隔を変更するには、[Set the screen refresh value] テキストボックスに値（秒）を入力し、[Set] をクリックします。入力できる最小値は 5 秒です。

ステップ 3　自動更新機能を無効にするには、左上隅にある [Disable Auto-Refresh] チェックボックスをオンにします。

ステップ 4　CPU の使用状況のログ ファイルを作成するには、ページの [Processors] セクションの [Start Log] ボタンをクリックします。

同様に、メモリ使用状況のログ ファイルを作成するには、ページの [Memory] セクションにある [Start Log] ボタンをクリックします。

最大 25 のログ ファイルを作成できます。

デフォルトのロギング間隔は 10 秒です。ロギング間隔を変更するには、次の手順を実行します。

a.　CPU のロギング間隔を変更するには、[Set CPU Logging Interval] テキストボックスに 5 ～ 600 秒の値を入力し、[Set] をクリックします。

b.　メモリのロギング間隔を変更するには、[Set Memory Logging Interval] テキストボックスに 5 ～ 600 秒の値を入力し、[Set] をクリックします。

ステップ 5　ログ ファイルをダウンロードするには、[Download CPU Log File] または [Download Memory Log File] をクリックします。

現在のすべてのログ ファイルを示す [Log Files] ページが表示されます。その後、ログ ファイルはリサイクルされます。新しいログ ファイルが追加されると、最も古いログ ファイルが削除されます。

ステップ 6　個々のファイルをダウンロードするには、ダウンロードするログ ファイル名の左側にあるチェックボックスをオンにします。すべてのログ ファイルをダウンロードするには、[File Name] 列見出しの左側にあるチェックボックスをオンにします。ファイルを選択したら、[Download] をクリックします。

ダウンロード用に複数のファイルを選択すると、CPULogs（プロセッサのログ ファイルの場合）および MemoryLogs（メモリのログ ファイルの場合）という名前の圧縮ファイルが作成され、ダウンロードされます。

ステップ 7　ログ ファイルをダウンロードせずに、オンラインで表示することもできます。その場合は、ファイル名をクリックします。ログ ファイルの内容が表示されます。

関連項目

- 「CPU and Memory Usage」（P.B-12）

Processes ツールの使用

Processes ツールを使用して、プロセス情報を監視し、記録できます。デフォルトでは、情報は 30 秒ごとに更新されます。更新の最小値は 5 秒です。この情報の更新頻度は変更できます。または、自動更新機能を無効にすることもできます。

Processes ツールを使用するには、次の手順を使用します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[System Monitor]>[Processes] の順に選択します。

[Processes] ページが表示されます。表示される情報の詳細については、表 B-13（P.B-13）を参照してください。

結果を昇順または降順でソートできます。ソートを実行するには、並べ替える列の見出しの横にある上向き矢印または下向き矢印をクリックします。たとえば、プロセスに基づいて降順のソートを実行するには、[Process] 列見出しの横にある下矢印をクリックします。同様に、プロセス ID に基づいて昇順のソートを実行するには、[PID] 列見出しの横にある上矢印をクリックします。

ステップ 2　ページの更新間隔を変更するには、左上隅にある [Set the screen refresh value] テキストボックスに値を入力し、[Set] をクリックします。入力できる最小値は 5 秒です。

ステップ 3　自動更新機能を無効にするには、左上隅にある [Disable Auto-Refresh] チェックボックスをオンにします。

ステップ 4　プロセスの詳細を表示するには、プロセス名の左側にあるチェックボックスをオンにして、[View Selected Processes] をクリックします。最大 10 のプロセスを選択できます。

[Selected Processes] に、プロセスの詳細が表示されます。このページで、更新頻度や自動更新機能の無効化の設定も行えます。プロセスのロギングを開始するには、[Start Log] をクリックします。ロギングを終了するには、[Stop Log] をクリックします。

プロセスのロギング間隔を変更するには、[Set Process Logging Interval] テキストボックスに 5 ～ 600 秒の値を入力し、[Set] をクリックします。

ステップ 5　ログ ファイルをダウンロードするには、[Process Log Files] ページから [Download Process Logs] をクリックします。（ログ ファイルをダウンロードするには、[Processes] ページから [Download Log File] をクリックします）。

ステップ 6　個々のファイルをダウンロードするには、ダウンロードするログ ファイル名の左側にあるチェックボックスをオンにします。すべてのログ ファイルをダウンロードするには、[File Name] 列見出しの左側にあるチェックボックスをオンにします。ファイルを選択したら、[Download] をクリックします。ダウンロード用に複数のファイルを選択すると、ProcessLogs という名前の圧縮ファイルが作成され、ダウンロードされます。

ステップ 7　ログ ファイルをダウンロードせずに、オンラインで表示することもできます。その場合は、ファイル名をクリックします。別ウィンドウにログ ファイルの内容が表示されます。

関連項目

- 「Processes」（P.B-14）

Disk Usage ツールの使用

Disk Usage ツールは、システム内のさまざまなパーティションで使用されている使用可能なディスク領域の割合を表示します。

Disk Usage ツールを使用するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[System Monitor]>[Disk Usage] の順に選択します。

[Disk Usage] ページが表示されます。[Disk Usage] ページの詳細については、表 B-17（P.B-16）を参照してください。

ステップ 2　昇順または降順のソートを実行するには、並べ替える基準にする列見出しの横にある上矢印または下矢印をクリックします。たとえば、パーティションに基づいて降順で並べ替えるには、[Partition] 列の見出しの横にある下向き矢印をクリックします。同様に、使用可能なディスク領域に基づいて昇順のソートを実行するには、[Available Space] 列見出しの横にある上矢印をクリックします。

関連項目

- 「Disk Usage」（P.B-15）

Cisco Emergency Responder ログの使用

Emergency Responder 8.6 には、システムやアプリケーションのログを収集するためのインターフェイスが用意されています。これらのログは同じユーザ インターフェイスを共有し、ログ ファイルは同じ方法で表示およびダウンロードできます。次の手順は、すべての Emergency Responder ログに適用されます。

Emergency Responder 8.6 ログは 3 つの種類に構成されます。これらの種類およびそれぞれに含まれるログは次のとおりです。

- Emergency Responder ログ
  - CER Admin
  - CER Server
  - CER Phone Tracking
  - JTAPI
  - Tomcat
  - Event Viewer

  - Audio Driver
- プラットフォーム ログ
  - CLI
  - CLM
  - Certificate Management/IPSec
  - DRS
  - Install/Upgrade
  - Remote Support
  - Syslog
  - Servm
- DB ログ
  - Cerdbmon
  - Install DB
- CLI 出力ファイル
  - Platform
  - DB

Emergency Responder ログを表示するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[System Logs]>[Log Type]>[Log Name] の順に選択します。

選択された [Log Files] ページが表示されます。これらの各ページの詳細については、次の関連項目の項を参照してください。

結果を昇順または降順でソートできます。ソートを実行するには、並べ替える列の見出しの横にある上向き矢印または下向き矢印をクリックします。

ステップ 2　[Download] ボタンを使用して、ログ ファイルをローカル システムにダウンロードします。

個々のファイルを選択するには、ダウンロードするログ ファイル名の左側にあるチェックボックスをオンにします。すべてのログ ファイルを選択するには、[File Name] 列見出しの左側にあるチェックボックスをオンにします。ファイルを選択したら、[Download] をクリックします。ダウンロード用に複数のファイルを選択すると、CPULogs という名前の圧縮ファイルが作成され、ダウンロードされます。圧縮ファイルの名前は、次のように、含まれるログの種類に基づきます。

- CER Admin
- CERr Server
- CER Phone Tracking
- Syslog
- JTAPI
- Tomcat
- Install
- DRS

- CLILogs
- CMILogs
- ServmLogs
- RemoteSupportLogs
- InstallDBLogs
- CertificateManagement&IPSecLogs
- CerdbmonLogs
- CLIOutputPlatform
- CLIOutputDB

ステップ 3　ログ ファイルをダウンロードせずに、オンラインで表示することもできます。その場合は、ファイル名をクリックします。別ウィンドウにログ ファイルの内容が表示されます。表示しているログ ファイルを更新するには、[Reload Log File] をクリックします。表示しているログ ファイルをダウンロードするには、[Download Log] をクリックします。

関連項目

- 「[System Logs] メニュー」（P.B-16）

CHAPTER 7

Cisco Emergency Responder 8.6 向けの Cisco Unified Operating System の設定

次のトピックでは、Cisco Emergency Responder（Emergency Responder）8.6 に付属の Cisco Unified Communications Operating System を設定および使用する方法について説明します。

Cisco Unified Communications Operating System の管理へのログイン

Cisco Unified Communications Operating System の管理にアクセスしてログインするには、次の手順に従います。

（注） Cisco Unified Communications Operating System の管理を使用する場合、ブラウザのコントロール（[Back] ボタンなど）は使用しないでください。

手順

ステップ 1 Emergency Responder にログインします。

ステップ 2 [Emergency Responder Administration] ページの右上にある [Navigation] メニューから、[Cisco Unified OS Administration] を選択し、[Go] をクリックします。

[Cisco Unified Communications Operating System Administration Logon] ウィンドウが表示されます。

（注） また、次の URL を入力して Cisco Unified Communications Operating System の管理に直接アクセスすることもできます。
http://*server-name***/cmplatform**

ステップ 3　管理者ユーザ名とパスワードを入力します。

（注） 管理者ユーザ名とパスワードは、インストール時に決めるか、CLI を使用して作成します。

ステップ 4　[Submit] をクリックします。

[Cisco Unified Communications Operating System Administration] ウィンドウが表示されます。

管理者パスワードとセキュリティ パスワードの復旧

管理者パスワードやセキュリティ パスワードがわからなくなった場合、次の手順に従ってパスワードをリセットします。

パスワード回復プロセスを実行するには、システム コンソール経由でシステムに接続している必要があります。つまり、キーボードとモニタをサーバに接続している必要があります。システムにセキュアシェル接続している状態ではパスワードを回復できません。

注意　サーバ グループのすべてのサーバのセキュリティ パスワードが一致する必要があります。すべてのマシンのセキュリティ パスワードを変更してください。変更しないと、互いに通信できなくなります。

注意　セキュリティ パスワードを変更した後に、サーバ グループ内の各サーバをリセットする必要があります。サーバをリブートできない場合は、システム サービスで問題が発生したり、サブスクライバ サーバ上の [Emergency Responder Administration] ページで問題が発生します。

（注） この手順中、物理的にシステムにアクセスできるか確認するため、有効な CD または DVD をディスク ドライブから取り出し、再挿入する必要があります。

手順

ステップ 1　次のユーザ名とパスワードを使用してシステムにログインします。

- ユーザ名：**pwrecovery**
- パスワード：**pwreset**

[Welcome to platform password reset] ウィンドウが表示されます。

ステップ 2　任意のキーを押して続行します。

ステップ 3　ディスク ドライブに CD または DVD が入っている場合は、ここで取り出します。

ステップ 4　任意のキーを押して続行します。

CD または DVD がディスク ドライブから取り出してあるかが確認されます。

ステップ 5　有効な CD または DVD をディスク ドライブに挿入します。

（注）　このテストでは、音楽 CD ではなくデータ CD を使用する必要があります。

ディスクを挿入したかが確認されます。

ステップ 6　ディスクが挿入されていることをシステムが確認した後、次のいずれかのオプションを入力して続行するよう要求されます。

- **a** を入力して、管理者パスワードをリセットする。
- **s** を入力して、セキュリティ パスワードをリセットする。
- **q** を入力して、終了する。

ステップ 7　選択したタイプの新しいパスワードを入力します。

ステップ 8　新しいパスワードを再入力します。

パスワードには 6 文字以上が必要です。システムが新しいパスワードの有効性を確認します。パスワードが有効性テストに合格しない場合、新しいパスワードを入力するよう要求されます。

ステップ 9　新しいパスワードの強度が検証された後、パスワードがリセットされ、任意のキーを押してパスワード リセット ユーティリティを終了するよう指示されます。

Cisco Unified OS 情報の表示

[Cisco Unified OS Administration] Web ページを使用すると、オペレーティング システム、プラットフォーム ハードウェア、およびネットワークのステータスを表示できます。次のトピックで、この情報の表示方法を説明します。

- 「ServerGroup 情報の表示」（P.7-3）
- 「ハードウェア ステータスの表示」（P.7-4）
- 「ネットワーク ステータスの表示」（P.7-4）
- 「インストールされているソフトウェアの表示」（P.7-4）
- 「システム ステータスの表示」（P.7-4）

ServerGroup 情報の表示

クラスタ情報を表示するには、次の手順を実行します。

手順

ステップ 1　メインの [Cisco Unified OS Administration] Web ページから、[Show]>[ServerGroup] を選択します。

[ServerGroup] ページが表示されます。

ステップ 2　[ServerGroup] ページのフィールドの説明については、表 C-1（P.C-2）を参照してください。

ハードウェア ステータスの表示

ハードウェア ステータスを表示するには、次の手順を実行します。

手順

ステップ 1　メインの [Cisco Unified OS Administration] Web ページから、[Show]>[Hardware] を選択します。

[Hardware Status] ページが表示されます。

ステップ 2　[Hardware Status] ページのフィールドの説明については、表 C-2（P.C-2）を参照してください。

ネットワーク ステータスの表示

表示されるネットワーク ステータス情報は、ネットワークの耐障害性がイネーブルになっているかどうかによって異なります。ネットワークの耐障害性が有効になっていると、イーサネット ポート 0 に障害が発生した場合、イーサネット ポート 1 が自動的にネットワーク通信を継承します。ネットワークの耐障害性がイネーブルになっている場合、ネットワーク ポートのイーサネット 0、イーサネット 1、および Bond 0 のネットワーク ステータス情報が表示されます。ネットワークの耐障害性がイネーブルになっていない場合、イーサネット 0 のステータス情報のみが表示されます。

ネットワーク ステータスを表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Show]>[Network] を選択します。

[Network Settings] ページが表示されます。

ステップ 2　[Network Settings] ページのフィールドの説明については、表 C-3（P.C-3）を参照してください。

インストールされているソフトウェアの表示

ソフトウェア バージョンとインストールされているソフトウェア オプションを表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Show]>[Software] を選択します。

[Software Packages] ページが表示されます。

ステップ 2　[Software Packages] ページのフィールドの説明については、表 C-4（P.C-4）を参照してください。

システム ステータスの表示

システム ステータスを表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Show]>[System] を選択します。

[System Status] ページが表示されます。

ステップ 2　[System Status] ページのフィールドの説明については、表 C-5（P.C-5）を参照してください。

IP 設定の表示

IP 設定を表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Show]>[IP Preference] を選択します。

[IP Preferences] ページが表示されます。

ステップ 2　データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3 に進みます。

レコードをフィルタまたは検索するには、次の手順を実行します。

- 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

（注）　検索条件をさらに追加するには、[+] ボタンをクリックします。条件を追加した場合、指定した条件をすべて満たしているレコードが検索されます。条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[Clear Filter] ボタンをクリックします。

ステップ 3　[Find] をクリックします。

条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[Rows per Page] ドロップダウン リスト ボックスで別の値を選択します。

Cisco Unified OS 設定の表示および変更

IP 設定、ホスト設定、およびネットワーク タイム プロトコル（NTP）設定を表示および変更するには、設定オプションを使用します。次のトピックでは、Cisco Unified OS 設定を表示および変更する方法について説明します。

- 「イーサネット設定の設定」（P.7-6）
- 「Emergency Responder サーバの IP アドレスの変更」（P.7-6）
- 「NTP サーバの設定」（P.7-8）
- 「SMTP 設定の設定」（P.7-9）

- 「時刻設定の設定」（P.7-9）
- 「ソフトウェア バージョンの再起動、シャットダウン、または切り替え」（P.7-10）

イーサネット設定の設定

[Ethernet Settings] オプションを使用すると、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）、ポート、およびゲートウェイの情報を表示および変更できます。

[Ethernet Configuration] ページでは、DHCP をイネーブルまたはディセーブルにしたり、イーサネット ポートの IP アドレスおよびサブネット マスクを指定したり、ネットワーク ゲートウェイの IP アドレスを指定できます。

（注）　イーサネット設定はすべて Eth0 にのみ適用されます。Eth1 を対象とした設定はできません。Eth0 の Maximum Transmission Unit（MTU; 最大伝送ユニット）のデフォルトは 1500 です。

イーサネット設定を表示または変更するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Settings]>[IP]>[Ethernet] を選択します。

[Ethernet Configuration] ページが表示されます。

ステップ 2　イーサネット設定を変更するには、目的のフィールドに新しい値を入力します。[Ethernet Configuration] ウィンドウのフィールドの説明については、表 C-7（P.C-6）を参照してください。

（注）　DHCP をイネーブルにすると、[Port Information] および [Gateway Information] の設定がディセーブルになり、変更できなくなります。

ステップ 3　変更を保存するには、[Save] をクリックします。

Emergency Responder サーバの IP アドレスの変更

Emergency Responder パブリッシャまたは Emergency Responder サブスクライバのいずれか、あるいは Cisco ER パブリッシャと Cisco ER サブスクライバの両方の IP アドレスを変更できます。

この項では、Emergency Responder サーバの IP アドレスを変更する方法について説明します。

- 「Emergency Responder パブリッシャ サーバの IP アドレスの変更」（P.7-7）
- 「Emergency Responder サブスクライバ サーバの IP アドレスの変更」（P.7-7）
- 「Emergency Responder パブリッシャ サーバと Emergency Responder サブスクライバ サーバの両方の IP アドレスの変更」（P.7-8）

Emergency Responder パブリッシャ サーバの IP アドレスの変更

インストール後に Emergency Responder パブリッシャの IP アドレスを変更するには、次の手順を実行します。

（注）　サーバの IP アドレスの変更を開始する前に、DNS サーバの IP アドレス情報を更新してください。

1. 次のいずれかのオプションを使用して、Emergency Responder パブリッシャの IP アドレスを変更します。
   - [Cisco Unified Operating System Administration] で、[Settings] > [IP] > [Ethernet] に新しい IP アドレスを入力します。「Ethernet Configuration」（P.C-6）を参照してください。
   - コマンドライン インターフェイス（CLI）で、set network ip コマンドを使用して新しい IP アドレスを設定します。「set network ip」（P.F-22）を参照してください。
2. Emergency Responder パブリッシャをリブートします。
3. Emergency Responder パブリッシャが完全に動作可能になったら、Emergency Responder Subscriber 上で [Cisco Unified Operating System Administration] にログインします。
4. [Settings] > [IP] > [Publisher] を選択します。[Cisco Unified Operating System Administration] に Publisher の古い IP アドレスが表示されます。パブリッシャの新しい IP アドレスを [Edit] ボックスに入力し、[Save] をクリックします。
5. Emergency Responder パブリッシャと Emergency Responder サブスクライバの通信が維持されるように、ただちに Emergency Responder サブスクライバをリブートします。
6. 「utils dbreplication status」（P.F-57）の説明に従って、utils dbreplication status CLI コマンドを使用して複製を確認します。各サーバの値が 2 と等しくなるようにしてください。
7. CTI ポートが Emergency Responder パブリッシャ サーバに登録されていることを確認します。CTI ポートが登録されていない場合は、ポートを削除してから再度追加して CTI ポートを再作成する必要があります。「必要な CTI ポートの作成」（P.3-8）を参照してください。

Emergency Responder サブスクライバ サーバの IP アドレスの変更

インストール後に Emergency Responder サブスクライバの IP アドレスを変更するには、次の手順を実行します。

（注）　サーバの IP アドレスの変更を開始する前に、DNS サーバの IP アドレス情報を更新してください。

1. 次のいずれかのオプションを使用して、Emergency Responder サブスクライバの IP アドレスを変更します。
   - [Cisco Unified Operating System Administration] で、[Settings] > [IP] > [Ethernet] に新しい IP アドレスを入力します。「Ethernet Configuration」（P.C-6）を参照してください。
   - コマンドライン インターフェイス（CLI）で、set network ip コマンドを使用して新しい IP アドレスを設定します。「set network ip」（P.F-22）を参照してください。
2. Emergency Responder サブスクライバをリブートします。
3. Emergency Responder サブスクライバが完全に動作可能になったら、Emergency Responder パブリッシャをリブートします。

4. 「utils dbreplication status」（P.F-57）の説明に従って、utils dbreplication status CLI コマンドを使用して複製を確認します。各サーバの値が 2 と等しくなるようにしてください。

Emergency Responder パブリッシャ サーバと Emergency Responder サブスクライバ サーバの両方の IP アドレスの変更

パブリッシャとサブスクライバ両方の IP アドレスを変更する場合、サーバの IP アドレスを続けて変更し、最初にサブスクライバを起動する必要があります。

注意　サブスクライバの IP アドレスの変更作業が完了するまで、パブリッシャ サーバの IP アドレスの変更は開始しないでください。

Emergency Responder パブリッシャと Emergency Responder サブスクライバの IP アドレスを変更するには、次の手順を実行します。

1. Emergency Responder パブリッシャ サーバの IP アドレス変更の詳細については、「Emergency Responder パブリッシャ サーバの IP アドレスの変更」（P.7-7）を参照してください。
2. Emergency Responder サブスクライバ サーバの IP アドレス変更の詳細については、「Emergency Responder サブスクライバ サーバの IP アドレスの変更」（P.7-7）を参照してください。

NTP サーバの設定

外部 NTP サーバが Stratum 9 以上（1 ～ 9）であることを確認してください。外部 NTP サーバの追加、削除、または変更を行うには、次の手順を実行します。

（注）　パブリッシャ上では NTP サーバ設定しか構成することができません。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Settings]>[NTP Servers] を選択します。

[NTP Server List] ページが表示されます。[NTP Server List] ページの詳細については、「NTP Server List」（P.C-8）を参照してください。

ステップ 2　NTP サーバの追加、削除、または変更ができます。

- NTP サーバを削除するには、当該のサーバの前にあるチェックボックスをオンにしてから [Delete Selected] をクリックします。
- NTP サーバを追加するには、[Add] をクリックします。[NTP Server Configuration] ページが表示されます。ホスト名または IP アドレスを入力し、[Save] をクリックします。
- NTP サーバを変更するには、IP アドレスをクリックします。[NTP Server Configuration] ページが表示されます。ホスト名または IP アドレスを変更し、[Save] をクリックします。

（注）　NTP サーバに対する変更は、完了するまで最大で 5 分かかる場合があります。NTP サーバを変更する場合、ページを更新して正しいステータスを表示する必要があります。

ステップ 3　[NTP Server Settings] ページを更新して正しいステータスを表示するには、[Settings]>[NTP] を選択します。

（注）　NTP サーバを削除、変更、または追加した後には、Publisher と Subscriber の両方を再起動して、変更を有効にする必要があります。

SMTP 設定の設定

[SMTP Settings] ウィンドウでは、SMTP ホスト名の表示や設定ができ、SMTP ホストがアクティブであるかどうかが表示されます。

SMTP ホスト設定を設定するには、次の手順を実行します。

ヒント　システムから E メールを送信する場合は、SMTP ホストを設定する必要があります。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Settings]>[SMTP] を選択します。

[SMTP Settings] ページが表示されます。[SMTP Settings] ページの詳細については、「SMTP Settings」（P.C-9）を参照してください。

ステップ 2　SMTP ホストのホスト名または IP アドレスを入力します。

ステップ 3　[Save] をクリックします。

時刻設定の設定

時刻を手動で設定するには、次の手順を実行します。

（注）　サーバ時刻を手動で設定するには、設定済みの NTP サーバをすべて削除する必要があります。NTP サーバの削除の詳細については、「NTP サーバの設定」（P.7-8）を参照してください。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Settings]>[Time] を選択します。[Time Settings] ページが表示されます。[Time Settings] ページの詳細については、「Time Settings」（P.C-10）を参照してください。

ステップ 2　システムの日付と時刻を入力します。

ステップ 3　[Save] をクリックします。

ソフトウェア バージョンの再起動、シャットダウン、または切り替え

このオプションは、より新しいソフトウェアにアップグレードする場合、または以前のソフトウェア バージョンにフォール バックする場合の両方で使用できます。

Cisco ER ソフトウェア バージョンの再起動、シャットダウン、または切り替えを行うには、次の手順を実行します。

注意　この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Settings]>[Version] を選択します。[Version Settings] ページが表示されます。[Version Settings] ページの詳細については、「Version Settings」（P.C-11）を参照してください。

ステップ 2　アクティブなパーティションで実行しているバージョンを再起動するには、[Restart] をクリックします。

[Restart] をクリックすると、現在のパーティションのシステムが、バージョンを切り替えずに再起動します。

ステップ 3　システムをシャットダウンするには、[Shutdown] をクリックします。

[Shutdown] をクリックすると、すべてのプロセスが中断され、システムがシャット ダウンします。

（注）　ハードウェアの電源は自動的には切れません。

注意　サーバの電源ボタンを押すと、システムがただちにシャット ダウンします。

ステップ 4　アクティブなディスク パーティションで実行中のシステムをシャットダウンし、非アクティブなパーティションのソフトウェア バージョンを使用してシステムを自動的に再起動するには、[Switch Versions] をクリックします。

[Switch Versions] をクリックするとシステムが再起動し、現在非アクティブであるパーティションがアクティブになります。

（注）　[Switch Version] ボタンは、非アクティブのパーティションにソフトウェアがインストールされている場合にのみ表示されます。

（注）　このオプションは、より新しいソフトウェアにアップグレードする場合、または以前のソフトウェア バージョンにフォール バックする必要がある場合の両方で使用できます。

セキュリティの管理

次のトピックでは、セキュリティおよび IPSec の管理作業を行う方法について説明します。

Internet Explorer のセキュリティ オプションの設定

サーバから証明書をダウンロードできるように Internet Explorer のセキュリティ設定が正しく設定されていることを確認するには、次の手順を実行します。

手順

ステップ 1　Internet Explorer を起動します。

ステップ 2　[Tools]>[Internet Options] を選択します。

ステップ 3　[Advanced] タブをクリックします。

ステップ 4　[Advanced] タブの [Security] セクションまでスクロール ダウンします。

ステップ 5　必要に応じて、[Do not save encrypted pages to disk] チェックボックスをオフにします。

ステップ 6　[OK] をクリックします。

証明書および証明書信頼リストの管理

次のトピックでは、[Certificate Management] を使用して実行できる機能について説明します。

証明書の表示

既存の証明書を表示するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Management] を選択します。

[Certificate List] ページが表示されます。[Certificate List] ページの詳細については、「Certificate List」（P.C-11）を参照してください。

ステップ 2　証明書のリストをフィルタするには、[Find] コントロールを使用します。

ステップ 3　証明書または信頼ストアの詳細を表示するには、ファイル名をクリックします。

[Certificate Configuration] ページに該当の証明書の情報が表示されます。

ステップ 4　[Certificate List] ページに戻るには、[Related Links] リストの [Back To Find/List] を選択し、[Go] をクリックします。

証明書または CTL のダウンロード

証明書または CTL を Cisco ER からローカル システムにダウンロードするには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。証明書または CTL のファイル名をクリックします。

ステップ 2　証明書のリストをフィルタするには、[Find] コントロールを使用します。

ステップ 3　証明書または CTL のファイル名をクリックします。

[Certificate Configuration] ページが表示されます。

ステップ 4　[Download] をクリックします。

ステップ 5　[File Download] ダイアログボックスで、[Save] をクリックします。

証明書の削除および再作成

次の各項では、証明書の削除と再作成について説明します。

- 「証明書の削除」（P.7-12）
- 「証明書の再作成」（P.7-13）

証明書の削除

信頼できる証明書を削除するには、次の手順を実行します。

注意　証明書を削除すると、システムの動作に影響する場合があります。[Certificate List] で選択する証明書については、システムから既存の CSR がすべて削除されるため、新しい CSR を生成する必要があります。詳細については、「証明書署名要求の生成」（P.7-15）の手順を参照してください。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　証明書のリストをフィルタするには、[Find] コントロールを使用します。

ステップ 3　証明書または CTL のファイル名をクリックします。

[Certificate Configuration] ページが表示されます。

ステップ 4　[Delete] をクリックします。

証明書の再作成

証明書を再作成するには、次の手順を実行します。

注意　証明書を再作成すると、システムの動作に影響する場合があります。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　[Generate New] をクリックします。

[Generate Certificate] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、証明書の名前を選択します。表示される証明書の名前の説明については、表 7-1 を参照してください。

ステップ 4　[Generate New] をクリックします。

表 7-1　証明書の名前と説明

名前	説明
tomcat	この自己署名ルート証明書は、HTTPS サーバのインストール中に作成されます。
ipsec	この自己署名ルート証明書は、MGCP ゲートウェイおよび H.323 ゲートウェイとの IPSec 接続のインストール中に生成されます。

証明書または証明書信頼リストのアップロード

注意　新しい証明書ファイルまたは証明書信頼リスト（CTL）ファイルをアップロードすると、システムの動作に影響する場合があります。新しい tomcat 証明書または証明書信頼リストをアップロードした後、CLI コマンドの **utils service restart Cisco Tomcat** を入力して、Cisco Tomcat サービスを再起動する必要があります。

（注）　システムが信頼証明書を他のクラスタ サーバに自動的に配信することはありません。複数のサーバで同じ証明書が必要な場合は、証明書を各サーバに個々にアップロードする必要があります。

次の項では、CA ルート証明書、アプリケーション証明書、または CTL ファイルをサーバにアップロードする方法について説明します。

- 「証明書のアップロード」（P.7-14）
- 「信頼できる証明書のアップロード」（P.7-14）

証明書のアップロード

CA ルート証明書、アプリケーション証明書、CTL ファイルをサーバにアップロードするには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　[Upload Certificate] をクリックします。

[Upload Certificate] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、証明書の名前を選択します。

ステップ 4　サード パーティの CA で発行されたアプリケーション証明書をアップロードする場合は、CA ルート証明書の名前を [Root Certificate] テキストボックスに入力します。CA ルート証明書をアップロードする場合は、このテキストボックスを空白のままにします。

ステップ 5　次のいずれかの手順で、アップロードするファイルを選択します。

- [Upload File] テキスト ボックスに、ファイルのパスを入力します。
- [Browse] ボタンをクリックしてファイルを選択し、[Open] をクリックします。

ステップ 6　ファイルをサーバにアップロードするには、[Upload File] ボタンをクリックします。

信頼できる証明書のアップロード

信頼できる証明書をアップロードするには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　[Upload CTL] をクリックします。

[Upload Certificate Trust List] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、証明書の名前を選択します。

ステップ 4　サード パーティの CA で発行されたアプリケーション証明書をアップロードする場合は、CA ルート証明書の名前を [Root Certificate] テキストボックスに入力します。CA ルート証明書をアップロードする場合は、このテキストボックスを空白のままにします。

ステップ 5　次のいずれかの手順で、アップロードするファイルを選択します。

- [Upload File] テキスト ボックスに、ファイルのパスを入力します。

- [Browse] ボタンをクリックしてファイルを選択し、[Open] をクリックします。

ステップ 6　ファイルをサーバにアップロードするには、[Upload File] ボタンをクリックします。

サード パーティ製の CA 証明書の使用

Cisco Unified OS は、サード パーティ製の Certificate Authority（CA; 認証局）が PKCS # 10 Certificate Signing Request（CSR; 証明書署名要求）によって発行した証明書をサポートしています。次の表に、このプロセスの概要および参考となる文書を示します。

	作業	参照先
ステップ 1	サーバに CSR を作成する。	「証明書署名要求の生成」（P.7-15）を参照してください。
ステップ 2	CSR を PC にダウンロードする。	「証明書または CTL のダウンロード」（P.7-12）を参照してください。
ステップ 3	CSR を使用して、CA からアプリケーション証明書を取得する。	アプリケーション証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、「サードパーティ製の CA 証明書の取得」（P.7-16）を参照してください。
ステップ 4	CA ルート証明書を取得する。	ルート証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、「サードパーティ製の CA 証明書の取得」（P.7-16）を参照してください。
ステップ 5	CA ルート証明書をサーバにアップロードする。	「証明書または証明書信頼リストのアップロード」（P.7-13）を参照してください。
ステップ 6	アプリケーション証明書をサーバにアップロードする。	「証明書または証明書信頼リストのアップロード」（P.7-13）を参照してください。
ステップ 7	新しい証明書に影響されるサービスを再起動する。	すべての証明書タイプで、対応するサービスを再起動します（たとえば、Tomcat の証明書を更新した場合は Tomcat サービスを再起動します）。さらに、CAPF または Cisco Unified CM の証明書を更新した場合は、TFTP サービスも再起動します。 サービスの再起動の詳細については、「Control Center の使用」（P.6-1）を参照してください。

証明書署名要求の生成

Certificate Signing Request（CSR; 証明書署名要求）を作成するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　[Generate CSR] をクリックします。

[Generate Certificate Signing Request] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、証明書の名前を選択します。

証明書署名要求をダウンロードするには、次の手順を実行します。

ステップ 4　[Generate CSR] をクリックします。

証明書署名要求のダウンロード

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2　[Download CSR] をクリックします。

[Download Certificate Signing Request] ダイアログボックスが表示されます。

ステップ 3　[Certificate Name] リストから、証明書の名前を選択します。

ステップ 4　[Download CSR] をクリックします。

ステップ 5　[File Download] ダイアログボックスで、[Save] をクリックします。

サードパーティ製の CA 証明書の取得

サードパーティの CA が発行するアプリケーション証明書を使用するには、署名付きのアプリケーション証明書と CA ルート証明書の両方を CA から取得する必要があります。これらの証明書の取得に関する情報は、CA から入手してください。入手の手順は、CA によって異なります。

CAPF および Cisco ER の CSR には、CA へのアプリケーション証明書要求に含める必要のある拡張情報が含まれています。CA が拡張要求メカニズムをサポートしていない場合は、CSR 作成プロセスの最後のページに表示される X.509 拡張を有効にする必要があります。

Cisco Unified OS では、証明書は DER および PEM 符号化フォーマットで、CSR は PEM 符号化フォーマットで生成されます。また、DER および DER 符号化フォーマットの証明書を受け入れます。

証明書の有効期限日の監視

証明書の有効期限日が近づいたときに、システムから自動的に E メールを送信できます。

証明書有効期限モニタを表示および設定するには、次の手順を実行します。

（注）　[Certificate Expiration Monitor] ページに関する情報を更新するには、Cisco Certificate Expiry Monitor サービスが実行されている必要があります。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[Certificate Monitor] を選択します。

[Certificate Monitor] ページが表示されます。

ステップ 2　必要な設定情報を入力します。[Certificate Monitor Expiration] フィールドの説明については、表 C-21（P.C-15）を参照してください。

ステップ 3　変更内容を保存するには、[Save] をクリックします。

IPSEC 管理

次のトピックでは、IPSec を管理する方法について説明します。

- 「既存の IPSec ポリシーの表示または変更」（P.7-17）
- 「新しい IPSec ポリシーの設定」（P.7-17）

（注）　IPSec は、インストール中にサーバ グループ内のサーバ間で自動的に設定されません。

既存の IPSec ポリシーの表示または変更

既存の IPSec ポリシーを表示または変更するには、次の手順を実行します。

（注）　システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを変更または作成しないでください。

注意　IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[IPSEC Configuration] を選択します。

[IPSEC Policy Configuration] ページが表示されます。

注意　既存の IPSec ポリシーを変更すると、システムの正常な動作に影響する場合があります。

ステップ 2　[Display Detail] リンクをクリックします。[Association Details] ページが表示されます。このページのフィールドの説明については、表 C-23（P.C-16）を参照してください。

新しい IPSec ポリシーの設定

新しい IPSec ポリシーとアソシエーションを設定するには、次の手順を実行します。

（注）　システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを変更または作成しないでください。

注意　IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Security]>[IPSEC Configuration] を選択します。

[IPSEC Policy List] ページが表示されます。

ステップ 2　[Add New] をクリックします。

[IPSEC Policy Configuration] ページが表示されます。

ステップ 3　[Next] をクリックします。

[Setup IPSEC Policy and Association] ページが表示されます。

ステップ 4　[IPSEC Policy Configuration] ページに関する適切な情報を入力します。このページのフィールドの説明については、表 C-23（P.C-16）を参照してください。

ステップ 5　新しい IPSec ポリシーを設定するには、[Save] をクリックします。

既存の IPSec ポリシーの管理

既存の IPSec ポリシーを表示、イネーブル/ディセーブル、または削除するには、次の手順を実行します。

（注）　システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを変更または作成しないでください。

注意　IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

注意　既存の IPSec ポリシーを変更すると、システムの正常な動作に影響する場合があります。

手順

ステップ 1　[Security] > [IPSEC Configuration] を選択します。

（注）　[Security] メニューの項目にアクセスするには、管理者パスワードを使用して Cisco Unified Communications Operating System の管理に再ログインする必要があります。

[IPSEC Policy List] ウィンドウが表示されます。

ステップ 2　ポリシーを表示、イネーブル、またはディセーブルにするには、次の手順を実行します。

a.　ポリシー名をクリックします。

[IPSEC Policy Configuration] ウィンドウが表示されます。

b. ポリシーをイネーブルまたはディセーブルにするには、[Enable Policy] チェックボックスを使用します。

c. [Save] をクリックします。

ステップ 3　1 つまたは複数のポリシーを削除するには、次の手順を実行します。

a. 削除するポリシーの隣にあるチェックボックスをオンにします。

[Select All] をクリックしてすべてのポリシーを選択することも、[Clear All] をクリックしてすべてのチェックボックスをオフにすることもできます。

b. [Delete Selected] をクリックします。

ソフトウェア アップグレードの実行

このトピックでは、ソフトウェア アップグレードを実行する方法について説明します。

- 「ソフトウェアのアップグレードとインストール」（P.7-19）

ソフトウェアのアップグレードとインストール

システムの動作中に、サーバにアップグレード ソフトウェアをインストールできます。システムにはアクティブで起動可能なパーティションと、非アクティブで起動可能なパーティションの 2 つのパーティションがあります。システムのブートと動作はすべてアクティブ パーティションとしてマークされているパーティションで実行されます。

アップグレード ソフトウェアをインストールする場合は、アクティブでないパーティションにインストールします。ソフトウェアのインストール中もシステムは通常通り動作します。準備ができたら、非アクティブ パーティションをアクティブにして、アップグレードしたソフトウェアでシステムをリブートします。現在アクティブなパーティションは、システムの再起動後に非アクティブなパーティションとして認識されます。現在のソフトウェアは、次のアップグレードまで、非アクティブのパーティションに保持されます。設定情報は自動的にアクティブ パーティションにあるアップグレード バージョンに移行されます。

[Software Upgrade] ページで、Cisco ER ソフトウェアをローカルまたはリモート ソースのいずれかからアップグレードできます。

ソフトウェア アップグレードの手順で、問題が発生した場合にアップグレードを取り消すこともできます。システムの非アクティブなパーティションにアップグレード用のソフトウェアをインストールし、再起動してシステムを新しいバージョンのソフトウェアに切り替えます。このプロセス中に、アップグレードされたソフトウェアがアクティブなパーティションになり、現在のソフトウェアが非アクティブなパーティションになります。設定情報は自動的にアクティブ パーティションにあるアップグレード バージョンに移行されます。

何らかの理由でアップグレードから元の状態に戻す場合、ソフトウェアの以前のバージョンがある非アクティブ パーティションでシステムを再起動できます。ただし、ソフトウェアのアップグレード以降に行った設定の変更はすべて失われます。

（注）　Cisco ER 8.5 から新しいバージョンにアップグレードする場合は、Publisher を最初にアップグレードした後に、Subscriber をアップグレードする必要があります。

アップグレード ファイルの取得

アップグレード プロセスを開始する前に、適切なアップグレード ファイルを Cisco.com から取得する必要があります。詳細については、該当する『Emergency Responder Release Notes』の「Installation and Upgrade」の項を参照してください。

（注） インストールする前に、パッチ ファイルの名前を変更しないでください。システムでそれが有効なファイルだと認識されなくなります。

（注） ファイルを解凍または untar しないでください。これを行うと、アップグレード ファイルを読み込めなくなる場合があります。

インストール プロセス中も、アップグレード ファイルにはローカル DVD かリモートの FTP または SFTP サーバからアクセスできます。アップグレード ファイルにアクセスする際に入力するディレクトリ名とファイル名は、大文字と小文字が区別されるため、注意してください。

ローカル ソースからのソフトウェアのインストールおよびアップグレード

ローカル ディスク ドライブの DVD からソフトウェアをインストールして、アップグレード プロセスを開始できます。

（注） ソフトウェアのアップグレード プロセスを開始する前にシステム データをバックアップしてください。詳細については、「Cisco Emergency Responder 8.6 Disaster Recovery System の設定」の章を参照してください。

ソフトウェアを DVD からインストールまたはアップグレードするには、次の手順を実行します。

手順

ステップ 1　Cisco.com から適切なアップグレード ファイルをダウンロードします。

ステップ 2　DVD を焼くための .iso ファイルを使用して DVD を作成します。.iso ファイルには、元の DVD ディスクの完全なイメージが含まれます。.iso ファイルは DVD にコピーできません。DVD 作成ソフトウェアを使用して、イメージに含まれているファイルを抽出し、これらを DVD に書き込む必要があります。これにより、DVD ディスクの正確な複製が作成されます。

ステップ 3　アップグレードするローカル サーバのディスク ドライブに新しい DVD を挿入します。

ステップ 4　[Cisco Unified OS Administration] Web ページから、[Software Upgrades]>[Install/Upgrade] を選択します。

[Software Installation/Upgrade] ページが表示されます。

ステップ 5　[Source] リストから [DVD/CD] を選択します。

ステップ 6　[Directory] フィールドに、DVD 上のパッチファイルのパスを入力します。

ファイルがルート ディレクトリにある場合は、スラッシュ（/）を入力します。

ステップ 7　[Next] をクリックしてアップグレード プロセスを続行します。

ステップ 8　インストールするアップグレード バージョンを選択して、[Next] をクリックします。

ステップ 9　次のページで、アップグレードの進行状況を監視します。これには、転送中のファイル名とメガバイト数が含まれます。

ステップ 10　アップグレードをインストールして、アップグレードされたパーティションに自動的に再起動するには、[Reboot to upgraded partition] を選択します。システムが再起動され、アップグレードされたソフトウェアが起動されます。

ステップ 11　アップグレードをインストールして、後でアップグレードされたパーティションに手動でリブートするには、次のいずれかの手順を実行します。

a. [Do not reboot after upgrade] を選択します。

b. [Next] をクリックします。

[Upgrade Status] ウィンドウにアップグレード ログが表示されます。

c. インストールが完了したら、[Finish] をクリックします。

d. システムを再起動して、アップグレードをアクティブにするには、[Settings] > [Version] を選択して、[Switch Version] をクリックします。

システムが再起動され、アップグレードされたソフトウェアが起動されます。

リモート ソースからのインストールとアップグレード

ソフトウェアをネットワーク ドライブまたはリモート サーバからインストールするには、次の手順を実行します。

（注）　ソフトウェアのアップグレード プロセスを開始する前にシステム データをバックアップしてください。詳細については、「Cisco Emergency Responder 8.6 Disaster Recovery System の設定」の章を参照してください。

（注）　Cisco Unified Operating System の管理にアクセスしている間は、ブラウザの制御機能（表示の更新や再読み込みなど）を使用しないでください。代わりに、管理インターフェイスのナビゲーション コントロールを使用してください。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Software Upgrades]>[Install/Upgrade] を選択します。

[Software Installation/Upgrade] ページが表示されます。

ステップ 2　[Source] リストから [Remote Filesystem] を選択します。

ステップ 3　[Directory] フィールドに、リモート システムのパッチファイルのパスを入力します。

アップグレード ファイルが Linux または UNIX サーバ上にある場合は、ディレクトリ パスの先頭にフォワード スラッシュを入力する必要があります。たとえば、アップグレード ファイルが patches ディレクトリに存在する場合は、`/patches` と入力する必要があります。

アップグレード ファイルが Windows サーバ上にある場合は、FTP サーバまたは SFTP サーバに接続することになるため、次のような適切な構文を使用してください。

- パスの先頭はフォワード スラッシュ（/）で始め、パス全体でフォワード スラッシュを使用します。

- パスは、サーバの FTP または SFTP ルート ディレクトリで始まる必要があります。「C:」などのドライブ レターで始まる Windows 絶対パスは入力できません。

ステップ 4　[Server] フィールドにサーバ名を入力します。

ステップ 5　[User Name] フィールドにユーザ名を入力します。

ステップ 6　[User Password] フィールドにパスワードを入力します。

ステップ 7　[Transfer Protocol] フィールドで、転送プロトコルを選択します。

ステップ 8　[Next] をクリックしてアップグレード プロセスを続行します。

ステップ 9　インストールするアップグレード バージョンを選択して、[Next] をクリックします。

ステップ 10　次のページで、アップグレードの進行状況を監視します。これには、転送中のファイル名とメガバイト数が含まれます。

ステップ 11　ダウンロードが完了したら、ダウンロードしたファイルのチェックサム値と、Cisco.com に表示されているチェックサム値を確認します。

注意　アップグレード ファイルの認証と整合性を保証するため、2 つのチェックサム値は一致している必要があります。チェックサム値が一致しない場合、Cisco.com から新しいバージョンのファイルをダウンロードして、再度アップグレードを試みてください。

（注）　アップグレード プロセスの進行中にサーバとの接続を失った場合、またはブラウザを閉じた場合は、[Software Upgrades] メニューに再度アクセスしようとすると、次のメッセージが表示されることがあります。

Warning: Another session is installing software, click Assume Control to take over the installation.

セッションを引き継ぐ場合は、[Assume Control] を選択します。

[Assume Control] が表示されない場合は、Real Time Monitoring Tool でアップグレードをモニタすることもできます。

ステップ 12　アップグレードをインストールして、アップグレードされたパーティションに自動的に再起動するには、[Reboot to upgraded partition] を選択します。システムが再起動され、アップグレードされたソフトウェアが起動されます。

ステップ 13　アップグレードをインストールして、後でアップグレードされたパーティションに手動でリブートするには、次のいずれかの手順を実行します。

a. [Do not reboot after upgrade] を選択します。

b. [Next] をクリックします。

[Upgrade Status] ウィンドウにアップグレード ログが表示されます。

c. インストールが完了したら、[Finish] をクリックします。

d. システムを再起動して、アップグレードをアクティブにするには、[Settings] > [Version] を選択して、[Switch Version] をクリックします。

システムが再起動され、アップグレードされたソフトウェアが起動されます。

アップグレードの途中停止

アップグレード ソフトウェアのインストール中に、アップグレードが途中停止したように見える場合があります。アップグレード ログには新しいログ メッセージが表示されなくなります。アップグレードが途中停止した場合は、アップグレードをキャンセルし、I/O スロットリングを無効にして、アップグレード手順を初めからやり直す必要があります。正常にアップグレードが完了した場合は、I/O スロットリングをイネーブルにする必要はありません。

I/O スロットリングを無効にするには、CLI コマンドの **utils iothrottle disable** を入力します。

I/O スロットリングのステータスを表示するには、CLI コマンドの **utils iothrottle status** を入力します。

I/O スロットリングを有効にするには、CLI コマンドの **utils iothrottle enable** を入力します。デフォルトでは、iothrottle は有効になっています。

システムがキャンセルに応答しない場合は、サーバをリブートし、I/O スロットリングをディセーブルにし、アップグレード プロセスの手順を再開してください。

以前のバージョンへの復帰

アップグレード後、ソフトウェア バージョンをアップグレードの実行前に戻すことができます。システムを再起動し、次の作業を実行して非アクティブなパーティションのソフトウェア バージョンに切り替えます。

	作業	詳細情報の参照先
1.	パブリッシャ ノードを以前のバージョンに戻します。	「パブリッシャ サーバの以前のバージョンへの復帰」（P.7-23）
2.	すべてのバックアップ サブスクライバ ノードを以前のバージョンに戻します。	「サブスクライバ サーバの以前のバージョンへの復帰」（P.7-24）

パブリッシャ サーバの以前のバージョンへの復帰

パブリッシャ サーバを以前のバージョンに復帰するには、次の手順を実行します。

手順

ステップ 1　次の URL を入力して、直接 Cisco Unified Communications Operating System の管理を表示します。

https://*server-name*/**cmplatform**

server-name は、Emergency Responder サーバのホスト名または IP アドレスです。

ステップ 2　管理者ユーザ名とパスワードを入力します。

ステップ 3　[Settings] > [Version] を選択します。

[Version Settings] ウィンドウが表示されます。

ステップ 4　[Switch Versions] ボタンをクリックします。

システムの再起動について確認すると、システムが再起動します。処理が完了するまでに、最大で 15 分かかることがあります。

ステップ 5　バージョンの切り替えが正常に完了したことを確認するには、次の手順を実行します。

a. 開いている [Cisco Unified Communications Operating System Administration] に再度ログインします。

b. [Settings] > [Version] を選択します。

[Version Settings] ウィンドウが表示されます。

c. アクティブなパーティションで、適切な製品バージョンが実行されていることを確認します。

d. アクティブにしたサービスがすべて動作していることを確認します。

e. 次の URL を入力し、ユーザ名とパスワードを入力して Emergency Responder にログインします。

https://*server-name***/ccmadmin**

f. ログインできること、および設定データが存在することを確認します。

サブスクライバ サーバの以前のバージョンへの復帰

サブスクライバ サーバを以前のバージョンに復帰するには、次の手順を実行します。

手順

ステップ 1　次の URL を入力して、直接 Cisco Unified Communications Operating System の管理を表示します。

https://*server-name***/cmplatform**

server-name は、Emergency Responder サーバのホスト名または IP アドレスです。

ステップ 2　管理者ユーザ名とパスワードを入力します。

ステップ 3　[Settings] > [Version] を選択します。

[Version Settings] ウィンドウが表示されます。

ステップ 4　[Switch Versions] ボタンをクリックします。

システムの再起動について確認すると、システムが再起動します。処理が完了するまでに、最大で 15 分かかることがあります。

ステップ 5　バージョンの切り替えが正常に完了したことを確認するには、次の手順を実行します。

a. 開いている [Cisco Unified Communications Operating System Administration] に再度ログインします。

b. [Settings] > [Version] を選択します。

[Version Settings] ウィンドウが表示されます。

c. アクティブなパーティションで、適切な製品バージョンが実行されていることを確認します。

d. アクティブにしたサービスがすべて動作していることを確認します。

ブリッジ アップグレード

ブリッジ アップグレードは、製造中止されたサーバから Emergency Responder-8.6(1) をサポートするサーバに移行するユーザに移行パスを提供します。

サポートが中止されたサーバは、ブリッジ アップグレード サーバとして機能することが許可され、アップグレードおよび起動できますが、Cisco Emergency Responder は正しく機能しません。

Emergency Responder-8.6(1) に正常にアップグレードすると、新しいバージョンの Cisco Emergency Responder で実行できるのは DRS バックアップのみであることを通知する警告がコンソールに表示されます（この警告は、CLI セッションと GUI セッションの両方で表示されます）。

ステップ 1　製造中止されたサーバで Emergency Responder-8.6(1) バージョンにアップグレードします。

ステップ 2　製造中止されたサーバの新しい Emergency Responder version バージョンを使用して、DRS バックアップを実行します。

（注）　Cisco Emergency Responder および Cisco Phone Tracking エンジンは、製造中止されたサーバでのブリッジ アップグレード後は、サービスとして表示されません。

ステップ 3　製造中止されたサーバと同じホスト名で、サポートされる新しいサーバに Emergency Responder-8.6(1) バージョンをインストールします。

ステップ 4　Emergency Responder-8.6(1) を実行しているサポートされる新しいサーバで、最初のノードの DRS 復元を実行します。

（注）　ブリッジ アップグレード可能なサーバのリストについては、『Emergency Responder 8.6(1) Release Notes』を参照してください。

カスタマイズされたログイン メッセージ

[Cisco Unified Communications Operating System Administration] ページ、[Cisco Unified CM Administration]、および CLI に表示されるカスタマイズされたログイン メッセージが含まれるテキスト ファイルをアップロードできます。

カスタマイズされたログイン メッセージをアップロードするには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified Communications Operating System Administration] ウィンドウで、[Upgrades] > [Customized Logon Message] の順に選択します。

[Customized Logon Message] ウィンドウが表示されます。

ステップ 2　アップロードするテキスト ファイルを選択するには、[Browse] をクリックします。

ステップ 3　[Upload File] をクリックします。

（注）　10KB を超えるファイルはアップロードできません。

システムにカスタマイズされたログイン メッセージが表示されます。

ステップ 4　デフォルトのログイン メッセージに戻すには、[Delete] をクリックします。

カスタマイズされたログイン メッセージが削除され、システムにデフォルトのログイン メッセージが表示されます。

Cisco Unified OS のサービスの使用

次のトピックで、Cisco Unified OS のサービスの使用方法を説明します。

ping ユーティリティの使用

[Ping Configuration] ページで、他のシステムがネットワーク経由でアクセスできるかを確認するため、ping 要求を送信できます。

別のシステムに ping を送信するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Services]>[Ping] を選択します。

[Ping Configuration] ページが表示されます。[Ping Configuration] ページの詳細については、「Ping Configuration」（P.C-19）を参照してください。

ステップ 2　ping の送信先となるシステムの IP アドレスまたはネットワーク名を入力します。

ステップ 3　ping 間隔を秒で入力します。

ステップ 4　パケット サイズを入力します。

ステップ 5　ping 回数（システムに ping を送信する回数）を入力します。

（注）　複数回の ping を指定した場合は、**ping** コマンドを入力してもリアルタイムでは ping の日時が表示されません。**ping** コマンドがデータを表示するのは、指定した回数だけ ping を送信した後です。

ステップ 6　IPSec を検証するかどうかを選択します。

ステップ 7　[Ping] をクリックします。

[Ping Results] テキスト ボックスに ping の統計情報が表示されます。

リモート サポートの設定

[Remote Support] ページで、シスコのサポート担当者が指定日時に Cisco ER システムにアクセスできるようにするためのリモート アカウントを設定できます。

リモート サポート プロセスは、次の手順で行われます。

1. ユーザがリモート サポート アカウントを設定します。このアカウントには、シスコの担当者がアクセスできる、設定可能な制限時間が含まれます。
2. リモート サポート アカウントの設定が完了すると、パス フレーズが生成されます。
3. ユーザはシスコのサポートに電話し、リモート サポート アカウント名とパス フレーズを伝えます。

4. シスコのサポート担当者はパスフレーズをデコーダ プログラムに入力し、パス フレーズからパスワードを生成します。
5. シスコのサポート担当者はデコードしたパスワードを使用して、お客様のシステムにリモート サポート アカウントでログインします。
6. アカウントの制限時間が経過すると、シスコのサポート担当者はリモート サポート アカウントにアクセスできなくなります。

リモート サポートを設定するには、次の手順を実行します。

手順

ステップ 1　[Cisco Unified OS Administration] Web ページから、[Services]>[Remote Support] を選択します。

[Remote Access Configuration] ページが表示されます。

ステップ 2　リモート サポート アカウントが設定されていない場合は、[Add] をクリックします。

ステップ 3　リモート アカウントのアカウント名と、アカウントの期限を、日単位で入力します。

（注）　アカウント名の長さが 6 文字以上で、すべて小文字のアルファベットであることを確認してください。

ステップ 4　[Save] をクリックします。

[Remote Access Configuration] ページが再度表示されます。[Remote Access Configuration] ページのフィールドの説明については、表 C-27（P.C-21）を参照してください。

ステップ 5　生成されたパス フレーズを使用してシステムにアクセスする方法については、シスコの担当者にお問い合わせください。

CHAPTER 8

Cisco Emergency Responder 8.6 Disaster Recovery System の設定

次のトピックでは、Cisco Emergency Responder（Emergency Responder）8.6 Disaster Recovery System を設定する方法について説明します。

Disaster Recovery System とは

メインの Cisco ER 8.6 Web インターフェイスから起動できる Disaster Recovery System（DRS）は、完全なデータ バックアップを行い、Emergency Responder サーバ グループのすべてのサーバの機能を復元します。Disaster Recovery System では、定期的にスケジュールされた自動データ バックアップまたはユーザ起動のデータ バックアップを実行できます。DRS では、複数のバックアップ スケジュールがサポートされます。

Cisco Disaster Recovery System は、サーバ グループ レベルのバックアップを実行します。つまり、Emergency Responder サーバ グループ内のすべてのサーバのバックアップを中央の場所に集め、バックアップ データを物理的なストレージ デバイスにアーカイブします。

DRS は、プラットフォームのバックアップ/復元の一環として、独自の設定（バックアップ デバイス設定およびスケジュール設定）を復元します。DRS は、drfDevice.xml ファイルおよび drfSchedule.xml ファイルをバックアップおよび復元します。これらのファイルとともにサーバを復元するときは、DRS バックアップ デバイスおよびスケジュールを再設定する必要がありません。

システム データ復元を実行するときには、サーバ グループ内のどのサーバを復元するかを選択できます。

Disaster Recovery System には、次の機能が含まれています。

- バックアップ タスクおよび復元タスクを実行するためのユーザ インターフェイス
- バックアップ機能および復元機能を実行するための分散システム アーキテクチャ
- スケジュール バックアップ
- 物理的なテープ ドライブまたはリモート sftp サーバへのバックアップのアーカイブ

（注） テープ ドライブが Publisher に接続されている必要があります。

Disaster Recovery System には、*マスター エージェント*（MA）と *ローカル エージェント*（LA）という 2 つの主要な機能が含まれています。マスター エージェントは、バックアップおよび復元アクティビティをすべてのローカル エージェントと調整します。

サーバ グループ内のすべてのサーバ上では、マスター エージェントとローカル エージェントの両方が自動的にアクティブになります。

（注） Disaster Recovery System は、Windows から Linux へ、または Linux から Linux へデータを移行しません。復元は、バックアップと同じ製品バージョンで実行する必要があります。Windows ベースのプラットフォームから Linux ベースのプラットフォームへのデータ マイグレーションの詳細については、『*Data Migration Assistant User Guide*』を参照してください。

注意 コール処理が中断してサービスに影響が及ばないように、バックアップはオフピーク時間中にスケジュールしてください。

バックアップ手順および復元手順のクイック リファレンス表

次の表に、バックアップ手順および復元手順のクイック リファレンスを示します。

バックアップのクイック リファレンス

表 8-1 に、Disaster Recovery System を使用してバックアップ手順を行う場合に実行する必要がある主要な手順と、その概要へのクイック リファレンスを発生順に示します。

（注）　Disaster Recovery System は、Windows から Linux へ、または Linux から Linux へデータを移行しません。復元は、バックアップと同じ製品バージョンで実行する必要があります。表 8-1 の手順を実行する前に、Windows ベースのプラットフォームから Linux ベースのプラットフォームへのデータ マイグレーションの詳細について、『*Data Migration Assistant User Guide*』を参照してください。

表 8-1　バックアップ手順を実行するための作業の概要

作業	参照先
データのバックアップ先となるバックアップ デバイスを作成する。	「バックアップ デバイスの追加」（P.8-5）
スケジュールに従ってデータをバックアップするためのバックアップ スケジュールを作成および編集する。 （注）　手動バックアップまたはスケジュール バックアップでは、サーバ グループがバックアップされます。	「バックアップ スケジュールの作成と編集」（P.8-6）
データをバックアップするためのバックアップ スケジュールをイネーブルまたはディセーブルにする。	「スケジュールのイネーブル化、ディセーブル化、および削除」（P.8-8）
手動バックアップを実行する（任意）。	「手動バックアップの開始」（P.8-8）
バックアップのステータスを確認する：バックアップの実行中、現在のバックアップ ジョブのステータスを確認できます。	「バックアップ ステータスの確認」（P.8-8）

復元のクイック リファレンス

表 8-2 に、Disaster Recovery System を使用して復元手順を行う場合に実行する必要がある主要な手順と、その概要へのクイック リファレンスを発生順に示します。

表 8-2　復元手順を実行するための作業の概要

作業	参照先
保存場所を選択する：まず、バックアップ ファイルの復元元となる保存場所を選択する必要があります。	「バックアップ ファイルの復元」（P.8-9）
バックアップ ファイルを選択する：使用可能なファイルのリストから、復元するバックアップ ファイルを選択します。	「バックアップ ファイルの復元」（P.8-9）
機能を選択する：使用可能な機能のリストから、復元する機能を選択します。	「バックアップ ファイルの復元」（P.8-9）
サーバを選択する：選択した機能が複数のサーバからバックアップされたものである場合には、復元するサーバを選択する必要があります。	「バックアップ ファイルの復元」（P.8-9）
復元のステータスを確認する：復元プロセスの実行中、現在の復元ジョブのステータスを確認できます。	「復元ステータスの表示」（P.8-13）

サポートされている機能およびコンポーネント

Emergency Responder 8.6 リリースでは、Emergency Responder のバックアップおよび復元を行えます。

バックアップの機能を選択すると、そのすべてのサブコンポーネントが自動的にバックアップされます。

システム要件

サーバ グループのすべてのサーバ上で Emergency Responder 8.6 が実行中であることを確認してください。

データをネットワーク上のリモート デバイスにバックアップするには、SFTP サーバを用意して必要な設定を行う必要があります。シスコは次の SFTP サーバのテストを実行しており、これらを推奨しますが、任意の SFTP サーバを使用できます。

（注）　シスコは、サード パーティのソフトウェアはサポートしていません。サポート上の問題については、SFTP ベンダーにお問い合わせください。

- Open SSH（Unix システム用）
- Cygwin
- freeFTPD
- Titan

（注）　バックアップまたは復元の実行中は、Disaster Recovery System によりプラットフォームの API がロックされ、すべての OA 管理要求がブロックされるため、OS 管理作業は行えません。一方、ほとんどの CLI コマンドはブロックされません。CLI ベースのアップグレード コマンドだけがプラットフォーム API ロッキング パッケージを使用するからです。

Disaster Recovery System へのアクセス方法

Disaster Recovery System にアクセスするには、メインの Emergency Responder 8.6 Web インターフェイスの [Navigation] プルダウン メニューから、[Disaster Recovery System] を選択します。
Cisco Unified OS Administration Web インターフェイスに使用するものと同じ管理者ユーザ名とパスワードを使用して、Disaster Recovery System にログインします。

（注）　管理者ユーザ名とパスワードは Emergency Responder のインストール時に設定したものであり、CLI を使用して、管理者パスワードを変更したり、新しい管理者アカウントを設定したりできます。「set password」（P.F-26）を参照してください。

マスター エージェントの役割とアクティブ化

マスター エージェントは、サーバ グループのすべてのサーバで自動的に起動されますが、完全にアクティブになるのはパブリッシャで実行されるマスター エージェントだけです。

マスター エージェント（MA）は、次の役割を果たします。

- MA は、システム全体のコンポーネント登録情報を保存します。
- MA は、スケジュールされた一連のタスクを Emergency Responder データベースに保持します。ユーザ インターフェイスから更新を受信すると、MA はスケジュールに従って、該当するローカル エージェントに実行可能なタスクを送信します。（ローカル エージェントは、遅滞なくただちにバックアップ タスクを実行します）。
- Disaster Recovery System ユーザ インターフェイスにアクセスして、バックアップのスケジュール、特定のサーバまたはサーバ グループの新しいバックアップ タスクの追加、既存のエントリの更新または表示、実行済みタスクのステータスの表示、システム復元の実行などのアクティビティを行います。
- MA は、ローカルに接続されたテープ ドライブまたはリモート ネットワーク上の場所にバックアップ セットを保存します。

ローカル エージェント

マスター エージェントが搭載されているサーバをはじめ、Emergency Responder サーバ グループ内の各サーバには、それぞれのサーバのバックアップ機能および復元機能を実行するための独自のローカル エージェントが搭載されている必要があります。

（注） デフォルトでは、ローカル エージェントはサーバ グループの各サーバ上で自動的にアクティブになります。

ローカル エージェントは、サーバ グループの各サーバ上でバックアップおよび復元スクリプトを実行します。

バックアップ デバイスの追加

Disaster Recover System を使用する場合は事前に、バックアップ ファイルを保存する場所を設定する必要があります。最大 10 個のバックアップ デバイスを設定できます。

バックアップ デバイスを設定するには、次の手順を実行します。

手順

ステップ 1　メインの [Disaster Recovery System] Web ページから、[Backup]>[Backup Device] を選択します。

[Backup Device List] ページが表示されます。

ステップ 2　新しいバックアップ デバイスを設定するには、[Add New] をクリックします。バックアップ デバイスを編集するには、[Backup Device] リストでそのデバイスを選択し、[Edit Selected] をクリックします。

[Backup Device] ウィンドウが表示されます。

ステップ 3　[Backup device name] フィールドにバックアップ デバイス名を入力します。

（注）　バックアップ デバイス名には、英数字、スペース（ ）、ダッシュ（-）、およびアンダースコア（_）だけを使用できます。その他の文字は使用できません。

ステップ 4　次のいずれかのバックアップ デバイスを選択し、[Select Destination] 領域で適切なフィールド値を入力します。

- [Tape Device]：ローカルに接続されたテープ ドライブにバックアップ ファイルを保存します。リストから目的のテープ デバイスを選択します。

  （注）　複数のテープに分散させたり、テープに複数のバックアップを保存したりすることはできません。

- [Network Directory]：SFTP 接続でアクセスするネットワーク ドライブにバックアップ ファイルを保存します。次の必須情報を入力します。
  - [Server name]：ネットワーク サーバの名前または IP アドレス
  - [Path name]：バックアップ ファイルの保存先となるディレクトリのパス名
  - [User name]：リモート システム上のアカウントの有効なユーザ名
  - [Password]：リモート システム上のアカウントの有効なパスワード
  - [Number of backups to store on Network Directory]：このネットワーク ディレクトリに保存するバックアップの数。

  （注）　ネットワーク上に保存先を設定するには、SFTP サーバにアクセスする必要があります。バックアップの前に SFTP パスが存在している必要があります。SFTP サーバへのアクセスに使用するアカウントには、選択したパスに対する書き込み権限が必要です。

ステップ 5　これらの設定を更新するには、[Save] をクリックします。

（注）　ネットワーク ディレクトリ バックアップの場合は、[Save] ボタンをクリックすると、DRS マスター エージェントが選択した SFTP サーバを検証します。ユーザ名、パスワード、サーバ名、またはディレクトリ パスが無効な場合は、保存に失敗します。

ステップ 6　バックアップ デバイスを削除するには、[Backup Device] リストでそのデバイスを選択し、[Delete Selected] をクリックします。

（注）　バックアップ スケジュールにバックアップ デバイスとして設定されているバックアップ デバイスは削除できません。

バックアップ スケジュールの作成と編集

最大 10 個のバックアップ スケジュールを作成できます。各バックアップ スケジュールには、自動バックアップのスケジュール、バックアップする機能セット、保存場所など、独自のプロパティがあります。

バックアップ スケジュールを管理するには、次の手順を実行します。

手順

ステップ 1　メインの [Disaster Recovery System] Web ページから、[Backup]>[Scheduler] を選択します。

[Schedule List] ウィンドウが表示されます。

ステップ 2　次のいずれかの手順を実行して、新規スケジュールを追加するか、または既存のスケジュールを編集します。

a.　新規スケジュールを作成するには、[Add New] をクリックします。

b.　既存のスケジュールを設定するには、[Schedule List] 列でその名前をクリックします。

スケジューラのウィンドウが表示されます。

ステップ 3　スケジュール名を [Schedule Name] フィールドに入力します。

（注）　デフォルトのスケジュールの名前は変更できません。

ステップ 4　[Select Backup Device] 領域でバックアップ デバイスを選択します。

ステップ 5　[Select Features] 領域でバックアップする機能を選択します。少なくとも 1 つの機能を選択する必要があります。

ステップ 6　[Start Backup at] 領域でバックアップを開始する日付と時刻を選択します。

ステップ 7　[Frequency] 領域でバックアップを行う頻度を選択します。[Once]、[Daily]、[Weekly]、[Monthly] のいずれかになります。[Weekly] を選択した場合は、バックアップを行う週の曜日も選択できます。

ヒント　バックアップ頻度を火曜日から土曜日までの [Weekly] に設定するには、[Set Default] をクリックします。

ステップ 8　これらの設定を更新するには、[Save] をクリックします。

ステップ 9　スケジュールを有効にするには、[Enable Schedule] をクリックします。

設定した時刻になると自動的に次のバックアップが実行されます。

（注）　サーバ グループのすべてのサーバが、Emergency Responder の同じバージョンを実行し、ネットワークからアクセスできることを確認してください。スケジュールされたバックアップの時刻にサーバが稼動していないと、そのサーバはバックアップされません。

ステップ 10　スケジュールをディセーブルにするには、[Disable Schedule] をクリックします。

スケジュールのイネーブル化、ディセーブル化、および削除

スケジュールのイネーブル化、ディセーブル化、または削除を行うには、次の手順を実行します。

手順

ステップ 1　メインの [Disaster Recovery System] Web ページから、[Backup]>[Scheduler] を選択します。
[Schedule List] ウィンドウが表示されます。

ステップ 2　変更するスケジュールの横にあるチェックボックスをオンにします。

- すべてのスケジュールを選択するには、[Select All] をクリックします。
- すべてのチェックボックスをオフにするには、[Clear All] をクリックします。

ステップ 3　選択したスケジュールをイネーブルにするには、[Enable Selected Schedules] をクリックします。

ステップ 4　選択したスケジュールをディセーブルにするには、[Disable Selected Schedules] をクリックします。

ステップ 5　選択したスケジュールを削除するには、[Delete Selected] をクリックします。

手動バックアップの開始

手動バックアップを開始するには、次の手順を実行します。

手順

ステップ 1　メインの [Disaster Recovery System] Web ページから、[Backup]>[Manual Backup] を選択します。
[Manual Backup] ページが表示されます。

ステップ 2　[Select Backup Device] 領域でバックアップ デバイスを選択します。

ステップ 3　[Select Features] 領域でバックアップする機能を選択します。

ステップ 4　手動バックアップを開始するには、[Start Backup] をクリックします。

バックアップ ステータスの確認

現在のバックアップ ジョブのステータスを確認し、現在のバックアップ ジョブをキャンセルできます。バックアップ履歴を表示するには、「バックアップ履歴および復元履歴の表示」（P.8-13）を参照してください。

現在のバックアップ ジョブのステータスを確認するには、次の手順を実行します。

手順

ステップ 1　メインの [Disaster Recovery System] Web ページから、[Backup]>[Current Status] を選択します。
[Backup Status] ページが表示されます。

ステップ 2　バックアップ ログ ファイルを表示するには、ログファイル名リンクをクリックします。

ステップ 3　現在のバックアップをキャンセルするには、[Cancel Backup] をクリックします。

（注）　現在のコンポーネントがバックアップ操作を完了した後、バックアップがキャンセルされます。

バックアップ ファイルの復元

Disaster Recovery System では厳格なバージョン チェックが行われ、Emergency Responder の一致するバージョンのみを復元できます。

復元ウィザードは、バックアップの復元に必要な手順を案内します。

ヒント　サーバ グループのすべてのサーバを復元するには、「サーバ グループの復元」（P.8-10）を参照してください。

注意　Emergency Responder を復元する場合は事前に、サーバにインストールされている Emergency Responder バージョンが、復元するバックアップ ファイルのバージョンと一致することを確認してください。Disaster Recovery System は、Emergency Responder のバージョンが一致する場合に限り復元をサポートします。たとえば、Disaster Recovery System ではバージョン 8.6.(1).10000-1 からバージョン 8.6(2).10000-1 への復元や、バージョン 8.6.(2).10000-1 からバージョン 8.6(2).10000-2 への復元は行えません。

要するに、Disaster Recovery System で Emergency Responder データベースを復元するには、製品バージョンが完全に一致する必要があります。

復元するには、次の手順を実行します。

手順

ステップ 1　メインの [Disaster Recovery System] Web ページから、[Restore]>[Restore Wizard] を選択します。

復元ウィザードの最初のページ（[Step1 Restore—Choose Backup Device]）が表示されます。

ステップ 2　[Select Backup Device] 領域で復元元となるバックアップ デバイスを選択します。

ステップ 3　[Next] をクリックします。

[Step 2 Restore—Choose the Backup Tar File] ページが表示されます。

ステップ 4　復元するバックアップ ファイルを選択します。

（注）　バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

ステップ 5　[Next] をクリックします。

[Step 3 Restore—Select the Type of Restore] ページが表示されます。

ステップ 6　復元する機能を選択します。

（注）　選択したファイルにバックアップされた機能だけが表示されます。

ステップ 7　[Next] をクリックします。[Step4 Restore—Final Warning for Restore] ページが表示されます。

ステップ 8　データの復元を開始するには、[Restore] をクリックします。

復元するサーバの選択を求めるプロンプトが表示されます。

ステップ 9　適切なサーバを選択します。

注意　データを復元するサーバを選択すると、そのサーバ上の既存のデータが上書きされます。

ステップ 10　選択したサーバにデータが復元されます。復元のステータスを表示するには、「復元ステータスの表示」（P.8-13）を参照してください。

ステップ 11　サーバを再起動します。

（注）　復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに 1 時間以上かかることがあります。

サーバ グループの復元

重大な障害やハードウェアのアップグレードが発生した場合は、サーバ グループ内のすべてのサーバの復元が必要になる場合があります。サーバ グループ全体を復元するには、次の手順を実行します。

（注）　サーバ グループを復元する前に、サーバ グループのサブスクライバ サーバが稼動していて、パブリッシャ サーバと通信していることを確認してください。復元時にダウンしているか、またはパブリッシャ サーバと通信していないサブスクライバ サーバについては、新規インストールを実行する必要があります。

ステップ 1　復元ウィザードを使用して両方のサーバを選択し、Emergency Responder Publisher と Emergency Responder Subscriber の両方を復元します。

ステップ 2　Publisher を再起動します。

ステップ 3　パブリッシャがオンラインに戻ったら、Subscriber を再起動します。

（注）　サーバ グループの両方のサーバを同時に再起動する必要があります。

次の項では、サーバ グループのサーバを復元する手順について説明します。

パブリッシャ サーバの復元

パブリッシャ サーバを復元するには、次の手順を実行します。

注意　Cisco ER を復元する場合は事前に、サーバにインストールされている Cisco ER バージョンが、復元するバックアップ ファイルのバージョンと一致することを確認してください。Disaster Recovery System は、Emergency Responder のバージョンが一致する場合に限り復元をサポートします。たとえば、Disaster Recovery System ではバージョン 8.6.(1).1000-1 からバージョン 8.6(2).1000-1 への復元や、バージョン 8.6.(2).1000-1 からバージョン 8.6(2).1000-2 への復元は行えません。

手順

ステップ 1　Publisher サーバ上で Cisco ER 8.6 の新規インストールを実行します。詳細については、「Cisco Emergency Responder Publisher のインストール」（P.2-14）を参照してください。

ステップ 2　メインの [Disaster Recovery System] Web ページから、[Restore]>[Restore Wizard] を選択します。

復元ウィザードの最初のページ（[Step 1 Restore—Choose Backup Device]）が表示されます。

ステップ 3　[Select Backup Device] 領域で復元元となるバックアップ デバイスを選択します。

ステップ 4　[Next] をクリックします。

[Step 2 Restore—Choose the Backup Tar File] ページが表示されます。

ステップ 5　復元するバックアップ ファイルを選択します。

（注）　バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

ステップ 6　[Next] をクリックします。

[Step 3 Restore—Select the Type of Restore] ページが表示されます。

ステップ 7　復元する機能を選択します。

（注）　選択したファイルにバックアップされた機能だけが表示されます。

ステップ 8　[Next] をクリックします。

[Step4 Restore—Final Warning for Restore] ページが表示されます。

ステップ 9　データの復元を開始するには、[Restore] をクリックします。

ステップ 10　復元するサーバの選択を求めるプロンプトが表示されたら、Publisher のみを選択します。

ステップ 11　パブリッシャ サーバにデータが復元されます。復元のステータスを表示するには、「復元ステータスの表示」（P.8-13）を参照してください。

（注）　復元プロセス中には、[Cisco ER Administration] ページまたは [User] ページに関するタスクを実行しないでください。

ステップ 12　サーバを再起動します。

（注）　復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに 1 時間以上かかることがあります。

ステップ 13　パブリッシャ サーバが再起動したら、「サブスクライバ サーバの復元」（P.8-12）に進みます。

サブスクライバ サーバの復元

サーバ グループのサブスクライバ サーバを復元するには、次の手順を実行します。

注意　サーバ グループを復元する際には、サブスクライバ サーバを復元する前にパブリッシャ サーバを復元する必要があります。

注意　Cisco ER を復元する場合は事前に、サーバにインストールされている Cisco ER バージョンが、復元するバックアップ ファイルのバージョンと一致することを確認してください。Disaster Recovery System は、Emergency Responder のバージョンが一致する場合に限り復元をサポートします。たとえば、Disaster Recovery System ではバージョン 8.6.(1).1000-1 からバージョン 8.6(2).1000-1 への復元や、バージョン 8.6.(2).1000-1 からバージョン 8.6(2).1000-2 への復元は行えません。

手順

ステップ 1　Subscriber サーバ上で Cisco ER 8.6 の新規インストールを実行します。詳細については、「Cisco Emergency Responder Subscriber のインストール」（P.2-19）を参照してください。

ステップ 2　メインの [Disaster Recovery System] Web ページから、[Restore]>[Restore Wizard] を選択します。

復元ウィザードの最初のページ（[Step 1 Restore—Choose Backup Device]）が表示されます。

ステップ 3　[Select Backup Device] 領域で復元元となるバックアップ デバイスを選択します。

ステップ 4　[Next] をクリックします。

[Step 2 Restore—Choose the Backup Tar File] ページが表示されます。

ステップ 5　復元するバックアップ ファイルを選択します。

注意　サーバ グループのサブスクライバ サーバを復元するには、Publisher の復元に使用した同じバックアップ ファイルを選択する必要があります。

ステップ 6　[Next] をクリックします。

[Step 3 Restore—Select the Type of Restore] ページが表示されます。

ステップ 7　復元する機能を選択します。

（注）　選択したファイルにバックアップされた機能だけが表示されます。

ステップ 8　[Next] をクリックします。

[Step4 Restore—Final Warning for Restore] ページが表示されます。

ステップ 9　データの復元を開始するには、[Restore] をクリックします。

ステップ 10　復元するサーバを選択するよう求められたら、サブスクライバのみを選択します。

ステップ 11　サブスクライバ サーバにデータが復元されます。復元のステータスを表示するには、「復元ステータスの表示」（P.8-13）を参照してください。

ステップ 12　サーバを再起動します。

（注）　復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに 1 時間以上かかることがあります。

ステップ 13　サブスクライバがリブートし、復元されたバージョンの Emergency Responder が実行されている状態になったら、パブリッシャをリブートします。

ステップ 14　「utils dbreplication status」（P.F-57）の説明に従って utils dbreplication status CLI コマンドを使用して、すべてのノードで [Restore Status] の値を確認します。各ノードの値が 2 と等しくなるようにしてください。

ヒント　複製が正しくセットアップされない場合は、「utils dbreplication reset」（P.F-58）の説明に従って utils dbreplication reset CLI コマンドを使用します。

復元ステータスの表示

現在の復元ジョブのステータスを確認するには、次の手順を実行します。

手順

ステップ 1　メインの [Disaster Recovery System] Web ページから、[Restore]>[Status] を選択します。

[Restore Status] ページが表示されます。

[Restore Status] ウィンドウの [Status] 列に、復元手順の完了率など進行中の復元のステータスが表示されます。

ステップ 2　復元ログ ファイルを表示するには、ログファイル名リンクをクリックします。

バックアップ履歴および復元履歴の表示

次のトピックでは、最新の 20 個のバックアップ ジョブおよび復元ジョブを表示する方法について説明します。

- バックアップ履歴
- 復元履歴

バックアップ履歴

バックアップ履歴を表示するには、次の手順を実行します。

手順

ステップ 1　メインの [Disaster Recovery System] Web ページから、[Backup]>[History] を選択します。

[Backup History] ページが表示されます。

ステップ 2　[Backup History] ページから、ファイル名、バックアップ デバイス、完了日付、結果、バックアップする機能など、実行したバックアップを表示できます。

（注）　[Backup History] ウィンドウには、最新の 20 個のバックアップ ジョブだけが表示されます。

復元履歴

復元履歴を表示するには、次の手順を実行します。

手順

ステップ 1　メインの [Disaster Recovery System] Web ページから、[Restore]>[History] を選択します。

[Restore History] ページが表示されます。

ステップ 2　[Restore History] ページから、ファイル名、バックアップ デバイス、完了日付、結果、復元されたた機能など、実行したバックアップを表示できます。

（注）　[Restore History] ページには、最新 20 件の復元ジョブのみ表示されます。

トレース ファイル

マスター エージェント、GUI、および各ローカル エージェントのトレース ファイルは、次の場所に書き込まれます。

- マスター エージェントのトレース ファイルは、*platform/drf/trace/drfMA0** です。
- 各ローカル エージェントのトレース ファイルは、*platform/drf/trace/drfLA0** です。
- GUI のトレース ファイルは、*platform/drf/trace/drfConfLib0** です。

トレース ファイルは CLI を使用して表示できます。詳細については、付録 F「コマンド ライン インターフェイス」を参照してください。

コマンド ライン インターフェイス

また、Disaster Recovery System では表 8-3 に示すように、バックアップ機能および復元機能のサブセットにコマンドラインからアクセスできます。これらのコマンドの詳細および CLI の使用の詳細については、付録 F「コマンド ライン インターフェイス」を参照してください。

表 8-3　Disaster Recovery System の CLI

コマンド	説明
utils disaster_recovery backup	Disaster Recovery System インターフェイスに設定されている機能を使用して、手動バックアップを開始します。
utils disaster_recovery restore	復元を開始します。復元するバックアップの場所、ファイル名、機能、およびサーバを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップ ジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップ ファイルを表示します。
utils disaster_recovery cancel_backup	進行中のバックアップ ジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。
utils disaster_recovery show_tapeid	テープ識別情報を表示します。

CHAPTER 9

Cisco Emergency Responder 8.6 Admin Utility の使用

Cisco Emergency Responder（Emergency Responder）8.6 では、Admin Utility は Emergency Responder 自体に統合されています。Admin Utility には、メインの Emergency Responder Web ページからアクセスできる専用の Web インターフェイスがあります。他の Emergency Responder Administration Web インターフェイスと同様に、Admin Utility Web インターフェイスはパスワードで保護されています。

次のトピックでは、Emergency Responder Admin Utility を使用する方法について説明します。

Cisco Unified Communications Manager のバージョンの変更

Admin Utility を使用して Cisco Unified Communications Manager（Cisco Unified CM）のバージョンを変更するには、次の手順を実行します。

手順

ステップ 1 Emergency Responder Admin Utility Web インターフェイスにログインします。

ステップ 2 メインの [Emergency Responder Admin Utility] ページで、[Update]>[CCM Version] の順に選択します。[Upgrade CCM Version] ページが表示されます。

ステップ 3 [Choose the CCM Version to Upgrade] プルダウン メニューから、Cisco Unified CM の新しいバージョンを選択し、[Go] をクリックします。

（注） パブリッシャおよびサブスクライバ ノードで個別に Cisco Unified CM バージョンを変更する必要があります。

（注） Emergency Responder 8.6 では、Cisco Unified CM 4.x ～ Cisco Unified CM 6.0 および Cisco Unified CM 7.0 はサポートされていません。Cisco Unified CM 6.1、7.1、8.0、8.5、8.6 のみがサポートされています。

L2 のアップグレード中に、Emergency Responder の低いバージョンで Cisco Unified CM バージョンが 6.0 以下として設定されている場合は、アップグレード後に Emergency Responder によって Cisco Unified CM が 6.1 バージョンに設定されます。

同様に、L2 のアップグレード中に Emergency Responder の低いバージョンで Cisco Unified CM バージョンが 7.0 に設定されている場合、アップグレード後、Emergency Responder で 7.1 バージョンに設定されます。

変更が行われると、[Upgrade CCM Version] ページの [Status] 領域に新しいバージョン番号が表示されます。

関連項目

- 「Cisco Unified CM のバージョンの更新」（P.E-1）

Cisco Emergency Responder クラスタ データベース ホストの詳細の更新

デフォルトでは、クラスタ内の各サーバは、自身のデータベースをクラスタ データベース ホストと見なします。各クラスタで保持するデータベースは 1 つのみでなければならないため、クラスタ設定をそれに従って更新する必要があります。

たとえば、2 つのサーバグループ（Servergroup A と Servergroup B）にそれぞれパブリッシャとサブスクライバが含まれている場合は、次の手順を実行してクラスタ データベース ホストの詳細を更新します。

1. Servergroup A の独自のホスト名を使用して、Servergroup A のクラスタ データベース ホストのパスワードを更新します。
2. IP アドレスと、Servergroup A のクラスタ データベース パスワードを入力して、Servergroup B のクラスタ データベース ホスト パスワードを更新します。
3. クラスタ内の他のサーバグループに対して、ステップ 2 を繰り返します。

（注） ホスト名を使用する場合は、DNS を使用してそのホスト名を解決できる必要があります。DNS が設定されていない場合や、DNS が何らかの理由で使用できない場合、ホスト名の解決が失敗し、クラスタは正常に機能しません。使用不可にならないように、DNS の設定に冗長なエントリを含めることをお勧めします。または、クラスタ データベース ホストの IP アドレスを、この画面で設定することもできます。

Admin Utility を使用して Emergency Responder クラスタ データベース ホストの詳細を更新するには、次の手順を実行します。

（注） Emergency Responder クラスタ DB ホストの詳細を更新するには、サーバをリブートする必要があります。他のサービスが IP アドレスをキャッシュしているため、Emergency Responder サービスを再起動するだけでは機能しません。
この手順では、このサーバ グループの Emergency Responder クラスタ DB ホストの詳細のみが更新されます。この Emergency Responder クラスタ内の他のサーバが自動的に更新されることはありません。

手順

ステップ 1　Emergency Responder Admin Utility Web インターフェイスにログインします。

ステップ 2　メインの [Emergency Responder Admin Utility] ページで、[Update]>[Cluster DBHost] の順に選択します。[Update Cluster DB Host] ページが表示されます。

ステップ 3　テキスト ボックスに、新しいクラスタ DBHost 名（DNS が設定されている場合）または IP アドレスを入力します。クラスタが複数のドメインに分散している場合、完全修飾ホスト名を入力します。

ステップ 4　[Password] テキスト ボックスに、新しいクラスタ DBHost のパスワードを入力します。

ステップ 5　[Confirm Password] テキスト ボックスに、新しいクラスタ DBHost のパスワードを再入力します。

ステップ 6　[Go] をクリックします。

関連項目

- 「Update Cluster DB Host」（P.E-2）

CHAPTER 10

Cisco Emergency Responder のためのユーザの準備

次のトピックでは、Cisco Emergency Responder（Emergency Responder）ユーザのさまざまな役割について説明します。これらのトピックは、ソフトウェアの使用について説明しているだけでなく、Emergency Responder を組織の緊急応答ニーズに適合させる方法を決定するために組織で行う必要のあるより大きなポリシーや手順の決定を理解するためにも役立ちます。

Cisco Emergency Responder のためのオンサイト アラート（セキュリティ）担当者の準備

緊急応答のポリシーや手順が、すでに設定されている場合があります。Cisco Emergency Responder（Emergency Responder）をこれらのポリシーや手順に適合させる方法について検討し、必要に応じて、緊急応答チーム（オンサイト アラートまたはセキュリティ担当者）と協力してこれらの手順を更新します。

Emergency Responder の次の側面に関して、これらの担当者のトレーニングを検討します。

- Emergency Responder Web インターフェイスの使用方法。これらのトピックについては、Emergency Responder ユーザ Web インターフェイスのオンライン ヘルプを参照してください。このオンライン ヘルプには、印刷してユーザに配布できる PDF 形式のユーザ ガイドが含まれています。このユーザ ガイドに含まれている情報は、オンライン ヘルプに含まれている情報と同じです。次の領域に関して、ユーザのトレーニングを行います。
  - ユーザ Web インターフェイスへのログイン方法。
  - 画面でのアラートの表示方法。
  - コールのロケーションに関する詳細情報の取得方法。概要情報には、発信者の実際の内線番号、PSAP が緊急発信者の番号として取得する電話番号である ELIN、スイッチ ポートに関連付けられた電話機ロケーション、および ALI のロケーション フィールドが含まれます。ユーザはまた、ALI 全体も表示できます。
  - コールを確認し、それにコメントを追加する方法。これらの手順で緊急応答チームの一貫した行動が保証されるようにするための規則の開発を検討します。

  - 緊急コール履歴の緊急コールの検索方法。
- 緊急コールの通知を受信する方法について説明します。
  - Emergency Responder ユーザ Web インターフェイスにログインしているすべてのユーザに対して、Web アラートが表示されます。
  - ERL からの緊急コールが発生すると、ERL に割り当てられているすべての担当者に電話がかかります。この電話には、発信者の内線番号に関する情報が含まれます。
  - 担当者の電子メール アドレスを設定した場合、これらの担当者はまた、電話コールより詳細な情報（ERL 名や電話機ロケーションなど）を含む電子メールも受信します。電子メール アドレスが電子メール ベースのポケットベルのものである場合は、ポケットベルが使用されます。ポケットベルは、自分のデスクにいないユーザに情報を通知するための最も効率的な方法です。

    スタンバイ Cisco ER サーバが緊急コールを処理した場合は、そのコール自体と、スタンバイ サーバによってコールが処理されたことがすべてのオンサイト アラート担当者に通知されます。各担当者がこれらの通知に応答する方法を決定します。
- 使用している ERL の名前と電話のロケーションを説明します。これは、担当者が緊急発信者のロケーションを識別するために保有する主要な情報です。
- 緊急コールに応答するための組織のポリシーについて説明します。まだポリシーがない場合は、緊急応答チームと協力して、受け入れ可能なポリシーを開発します。

関連項目

- 「Cisco Emergency Responder 用のスタッフの準備」（P.1-23）

ERL 管理者のロールについて

表 10-1 は ERL 管理者が担当する反復的な作業のリストです。システム管理者もまた、次の作業を実行できます。

表 10-1　Cisco Emergency Responder ERL 管理の反復的な作業

反復的な作業	説明	詳細情報
新規または変更されたスイッチ ポートに ERL を割り当てる。	スイッチがネットワークに追加された場合、または追加のポートを含むモジュールが既存のスイッチに追加された場合は、新しいポートに ERL を割り当てます。	「スイッチ ポートの設定」（P.4-54）
必要に応じて ERL を作成する。	ビジネスの拡張に伴い、必要に応じて新しい ERL を作成します。テレフォニー管理者と協力して ERL の ELIN を取得し、ネットワーク管理者と協力して Cisco ER で定義されている新しいスイッチを取得します。	• 「ERL の作成」（P.4-33） • 「スイッチ ポートの設定」（P.4-54）
ALI データをエクスポートしてサービス プロバイダーに送信する。	ALI データに変更を加えた場合、ERL を追加または削除した場合、または ERL に割り当てた ELIN を変更した場合（追加、削除など）は、ALI をエクスポートし、サービス プロバイダーに再提出します。	• 「ERL 情報のエクスポート」（P.4-41） • 「サービス プロバイダー向け ALI 情報のエクスポート」（P.4-42） • 「ERL の作成」（P.4-33） • 「ALI 提出要件に関するサービス プロバイダーとの交渉」（P.1-22）

表 10-1　Cisco Emergency Responder ERL 管理の反復的な作業（続き）

反復的な作業	説明	詳細情報
手動で定義された電話機を監査する。	手動電話機の定義を定期的にチェックして、各電話機が引き続き正しい ERL に割り当てられていることを確認します。テレフォニー管理者と協力して、これらの電話機に関するすべての追加、移動、または変更の通知を取得します。必要に応じて電話機を追加します。	• 「電話機の手動での定義」（P.4-63）
位置未確認の電話機のリストを監査する。	位置未確認の電話機リストを定期的に監査し、ネットワーク管理者とともに、Cisco ER が電話機の位置を確認できない理由を突き止め、問題を解決します。	• 「位置未確認の電話の識別」（P.4-62） • 「位置未確認の電話機が多すぎる」（P.11-2）
新しいオンサイト担当者の追加、古い担当者の削除、電話番号の更新を行う。	オンサイトのアラート担当者が追加されたら、彼らを Cisco ER で定義し、適切な ERL に割り当てます。同様に、担当者が削除されたら、その担当者を ERL から削除し、次に Cisco ER から削除します。電話番号、電子メール アドレス、その他の連絡先情報が変更された場合は、これらを更新します。	• 「セキュリティ担当者（オンサイト アラート担当者）の指定」（P.4-32） • 「ERL の作成」（P.4-33）
IP サブネットを追跡対象の IP サブネットに追加する。	Cisco ER で検出する必要のある新しい IP サブネットが存在する場合は、次の作業を実行します。 • 新しい IP サブネットの地理的なロケーションにわたる ERL を設定します。 • この新しい IP サブネットとそれに対応するマスクを設定し、この IP サブネットを作成された ERL に割り当てます。	• 「IP サブネットベースの ERL の設定」（P.4-38）

関連項目

- 「ERL の使用」（P.4-29）
- 「電話機の管理」（P.4-54）
- 「Cisco Emergency Responder のトラブルシューティング」（P.11-1）

ネットワーク管理者のロールについて

表 10-2 は、ネットワーク管理者が担当する反復的な作業のリストです。システム管理者もまた、次の作業を実行できます。

表 10-2　Cisco Emergency Responder ネットワーク管理の反復的な作業

反復的な作業	説明	詳細情報
新しいスイッチを追加する。	ネットワークに追加するスイッチをすべて Cisco ER の設定に追加する。スイッチは、その IP アドレスが Cisco ER で定義されていない場合に新規であると見なされます。	• 「LAN スイッチの指定」（P.4-48） • 「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）
古いスイッチを削除する。	ネットワークからスイッチを削除した場合は、そのスイッチを Cisco ER の設定から削除します。スイッチが Cisco ER の設定に存在しなくても問題は発生しませんが、Cisco ER によるスイッチへの接続の試みがタイムアウトしないと次のスイッチに進むことができないため、電話機の追跡を行うために必要な時間が長くなります。	• 「LAN スイッチの指定」（P.4-48）
SNMP read コミュニティが変更された場合は更新する。	定義されたスイッチの read コミュニティ ストリングを変更する場合は、Cisco ER の SNMP 設定を更新する必要があります。設定が更新されるまで、Cisco ER は、そのスイッチに接続された電話機を追跡できません。	• 「SNMP 接続の設定」（P.4-45）
Cisco Unified CM サーバを更新または削除する	ネットワークに Cisco Unified CM クラスタが追加または削除された場合は、クラスタをサポートする Cisco ER グループの設定を更新します。これらの更新を行うための権限はありますが、組織で、主要な責任が Cisco ER システム管理者に割り当てられる可能性があります。	• 「Cisco Unified Communications Manager クラスタの指定」（P.4-26）
ERL 割り当てをチェックする。	ERL デバッグ ツールを使用して、選択された電話機に対して正しい、予測された ERL が使用されていることを確認します。	• 「Cisco Emergency Responder Admin Utility の使用」（P.11-19）

関連項目

- 「Cisco Emergency Responder のスイッチの設定」（P.4-44）
- 「Cisco Emergency Responder のトラブルシューティング」（P.11-1）

Cisco Emergency Responder システム管理者のロールについて

表 10-2 は、システム管理者が担当する反復的な作業のリストです。システム管理者もまた、「ERL 管理者のロールについて」（P.10-2）および「ネットワーク管理者のロールについて」（P.10-3）で説明されている、ERL 管理者とネットワーク管理者の作業の一部またはすべてを担当することがあります。

表 10-3　Cisco Emergency Responder システム管理の反復的な作業

反復的な作業	説明	詳細情報
Cisco ER グループを追加する。	電話機がネットワークに追加されると、追加の Cisco ER グループが必要になることがあります。これらをインストールおよび定義して、電話設定を行います。 テレフォニー管理者と協力して、必要な Cisco Unified CM の設定を完了します。	• 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14） • 「Cisco Emergency Responder サーバ グループの設定」（P.4-22） • 「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23） • 「Cisco Emergency Responder サーバの設定」（P.4-25） • 「Cisco Emergency Responder ライセンス ファイルのアップロード」（P.4-25） • 「Cisco Unified Communications Manager クラスタの指定」（P.4-26）
システムを監視し、発生するすべての問題をトラブルシューティングする。	発生するすべての問題の解決を支援します。必要に応じて、ネットワーク管理者、ERL 管理者、およびテレフォニー管理者と協力します。	• 「Cisco Emergency Responder のトラブルシューティング」（P.11-1）
新しい Cisco ER ユーザを作成し、古いユーザを削除する。	オンサイト アラート担当者が変更された場合や、Cisco ER システム、ネットワーク、および ERL 管理者が変更された場合は、必要に応じてそれらを追加または削除します。	• 「Cisco Emergency Responder ユーザの管理」（P.4-10）
Cisco Unified CM サーバを追加または削除する。	ネットワークに Cisco Unified CM クラスタが追加または削除された場合は、クラスタをサポートする Cisco ER グループの設定を更新します。これらの更新を行うための権限はありますが、組織で、主要な責任が Cisco ER ネットワーク管理者に割り当てられる可能性があります。	• 「Cisco Unified Communications Manager クラスタの指定」（P.4-26）
Cisco ER によって生成された電子メール アラートを監視する。	サーバ グループの設定に電子メール ID が設定されている場合は、Cisco ER から重大なエラーに関する電子メール アラートが送信されます。エラーを理解し、適切な措置を講じて問題を解決する必要があります。 この電子メール アラートの理解や問題の解決に役立つ情報については、「電子メール アラートのトラブルシューティング」（P.11-11）を参照してください。	• 「Cisco Emergency Responder サーバ グループの設定」（P.4-22）

関連項目

- 「サーバおよびサーバ グループの設定」（P.4-21）

- 「電子メール アラートのトラブルシューティング」（P.11-11）

CHAPTER 11

Cisco Emergency Responder のトラブルシューティング

ここでは、Cisco Emergency Responder（Emergency Responder）で発生する可能性がある問題に対処し、解決方法を示します。また、問題の特定の解決に関連する他の作業についても説明します。

電話機に関する問題のトラブルシューティング

ここでは、ERL への電話機の割り当ておよび電話機の管理に関する問題の解決に役立つ情報について説明します。

電話機が検出されない

Cisco Emergency Responder（Emergency Responder）が Cisco Unified Communications Manager（Cisco Unified CM）に対するホーミング処理中の電話機を検出していない場合、すべての Cisco Unified CM が SNMP で到達可能であり、NMP 設定が正しいことを確認します。Cisco Unified CM が SNMP で到達不能であっても Emergency Responder のログにはイベントが記録されます。

Cisco Unified CM の SNMP 設定を確認するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Administration CLI にログインし、次のコマンドを使用して Cisco Unified CM サーバに ping を送信します。

```
utils network ping <ipaddress of CUCM>
```

ステップ 2　Cisco Unified CM を正常に ping することができる場合、Cisco Unified CM 上で SNMP 設定が正しいことを次のように確認します。

- Cisco Unified CM（バージョン 6.0 以降）の Linux バージョンを使用している場合、Cisco Unified CM サービスアビリティ Web インターフェイスにログインし、SNMP Web ページを使用して SNMP コミュニティ ストリングの設定を確認します。
- Cisco Unified CM の Windows バージョンを使用している場合、Cisco Unified CM のサービスを開き、次を選択します。

  [Start]>[Settings]>[Control Panel]>[Administrative Tools]>[Services Properties]>[SNMP]>[Properties]>[Security] タブ

ステップ 3　Emergency Responder サーバで次の CLI コマンドを実行して、Cisco Unified CM が SNMP で到達可能かどうかを確認します。

```
utils snmp get <ccm ip-address/host name> <snmp-read-community-string> 1.3.6.1.2.1.1.2.0
```

Cisco Unified CM が SNMP で到達可能な場合、前述のコマンドの出力は次の例のようになります。

```
Variable = 1.3.6.1.2.1.1.2.0
value    = OBJECT IDENTIFIER <sys-oid-of-ccm>
```

位置未確認の電話機が多すぎる

Emergency Responder は Cisco Unified CM から登録済み電話機のリストを取得し、すべての電話機について位置確認を試行します。スイッチ ポートの背後や任意の設定済み IP サブネット内にある電話機の位置を Emergency Responder で確認できず、その電話機が設定済みの模擬電話機ではない場合、位置未確認の電話機のリストに表示されます。

位置未確認の電話機が数多く存在する場合は、まずスイッチ ポートおよび電話機更新プロセスを実行し、Emergency Responder が問題の一部を自動的に解決できるかどうか確認します。詳細については、「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）を参照してください。

Emergency Responder で電話機の位置を確認できない原因はいくつかあります。

- 電話機が CDP（Cisco Discovery Protocol）ネイバーであるとレポートするスイッチ ポートが複数ある場合、電話機は位置未確認の電話機に表示されます。電話機が CDP ネイバーであるとレポートするスイッチ ポートが 1 つのみの場合、この条件は次回の電話機トラッキング プロセスで修正されます。

- Emergency Responder で定義されていないスイッチに電話機が接続されています。スイッチの定義については、「LAN スイッチの指定」（P.4-48）を参照してください。
- 電話機がサポート対象外のデバイスに接続されています。ルータ ポート、ルータに接続されるハブ、サポート対象外のスイッチなどです。サポートされるスイッチの一覧については、「ネットワークのハードウェアおよびソフトウェアの要件」（P.1-4）を参照してください。このような種類の電話機をサポート対象のデバイスに接続できない場合の電話機の設定方法については、「電話機の手動での定義」（P.4-63）を参照してください。
- 電話機はハブに接続され、ハブはサポート対象のスイッチ ポートに接続されていますが、そのスイッチ ポートが CDP をサポートしていません。Emergency Responder では、（サポート対象のスイッチ ポートに接続された）ハブに接続されている CDP 対応の電話機を常に検出できますが、この方法で接続されている非 CDP 電話機は追跡できません。非 CDP 電話機の場合、サポート対象のスイッチ ポートに電話機を直接接続するようにしてください。
- SNMP クエリーに応答しないなど、電話機が接続されているスイッチが現時点で到達不能です。この理由はいくつか考えられます。
  - スイッチ上の SNMP の読み込みコミュニティ ストリングが、Emergency Responder に設定されているストリングと一致しません。Emergency Responder の設定を修正してください。「SNMP 接続の設定」（P.4-45）を参照してください。
  - 電話機から CAM テーブルへのアクセスが必要ですが、Emergency Responder のスイッチに対して CAM のトラッキングがイネーブルではありません。「LAN スイッチの指定」（P.4-48）を参照してください。
  - ネットワークが停止しているため、Emergency Responder サーバとスイッチ間で通信できません。ネットワークの停止の問題を突き止め、解決してください。

  Emergency Responder で次のスイッチ ポートと電話機全体の更新プロセスが実行されるまで、到達不能のスイッチは再試行されません。ただし、個々のスイッチに対して更新プロセスを実行すると再試行されます。
- 電話機は、異なる Emergency Responder グループで処理されているスイッチに移動しました。この場合、位置未確認の電話機リストで、その電話機について Emergency Responder グループ名が表示されます。移動後の次の増分電話機トラッキング プロセスでも電話機の位置が確認されない場合、この電話機がどの Emergency Responder グループに属していても、スイッチ ポートと電話機全体の更新プロセスが実行されるまで位置が確認されません。
- 電話機には CAM ベースのトラッキングが必要ですが、電話機が接続されているスイッチで CAM ベースのトラッキングがイネーブルではありません。Cisco IP SoftPhone とその他の一部の電話機モデルには、CAM ベースのトラッキングが必要です。CAM ベースのトラッキングについては、「LAN スイッチの指定」（P.4-48）を参照してください。また、CAM ベースのトラッキングが必要な電話機のリストについては、「ネットワークのハードウェアおよびソフトウェアの要件」（P.1-4）を参照してください。

Emergency Responder で電話機の位置を確認できない問題を解決した後は、影響があるスイッチまたはすべてのスイッチで、スイッチ ポートと電話機の更新プロセスを実行します。

- 特定のスイッチで更新プロセスを実行するには、[Phone Tracking]>[LAN Switch Details] を選択し、左側の列のスイッチを選択し、[Locate Switch Ports] を選択します。
- すべてのスイッチでプロセスを実行するには、[Phone Tracking]>[Run Switch-Port & Phone Update] を選択します。

関連項目

- 「位置未確認の電話の識別」（P.4-62）
- 「IP Subnet Phones」（P.A-54）
- 「Cisco Unified OS CLI コマンド」（P.F-4）

Cisco Emergency Responder に電話機が表示されなくなることがある

Emergency Responder が電話機トラッキング プロセス中で、電話機が異なる Cisco Unified CM クラスタに対するホーミング処理中の場合、電話機のレコードを保有する Cisco Unified CM クラスタはありません。そのため、Emergency Responder は電話機の存在を認識していません。また、Emergency Responder インターフェイスで電話機を検索できません。ただし、電話機が Cisco Unified CM クラスタへの接続に成功した場合、次回の増分電話機トラッキング プロセス時にその電話機が追跡されるため、電話機は Emergency Responder インターフェイスに表示されます。

Emergency Responder の電話機のトラッキング プロセス中に、電話機がバックアップ サーバからプライマリ Cisco Unified CM サーバに再接続している場合も、この問題が発生することがあります。

共有回線で誤った ERL が使用される

シェアド ライン アピアランスを使用する複数の電話機が、1 つの Emergency Responder グループにモニタされるスイッチから、異なる Emergency Responder グループにモニタされるスイッチに移動すると、このような電話機には、緊急コール時に誤った ERL が割り当てられることがあります。異なる Cisco Unified CM クラスタがある異なるキャンパスに電話機が移動し、移動した電話機が元の Cisco Unified CM クラスタにまだ登録されている場合、この問題が発生することがあります。また、複数の Cisco Unified CM クラスタに処理されている 1 つの大規模なキャンパス内に電話機が移動した場合にも発生することがあります。

移動した電話機はまだ元の Cisco Unified CM クラスタに登録されているため、その電話機からの緊急コールは、元の Emergency Responder グループにルーティングされます。この場合、異なる Emergency Responder グループがモニタしているスイッチに発信元の電話機が接続されていることを Emergency Responder グループが検出し、コールは H.323 インタークラスタ トランクを介して適切な Emergency Responder グループに転送されます。インタークラスタ トランクは発信元の電話機の MAC アドレスを渡さないため、受信 Emergency Responder グループは発信元の電話機の MAC アドレスを認識しておらず、発信者番号に基づいて電話機を ERL に関連付ける必要があります。

受信側の Emergency Responder グループがモニタしているスイッチに 1 台の電話機が接続されている場合、これは問題にはなりません。ただし、シェアド ライン アピアランスを使用する複数の電話機が、受信側の Emergency Responder グループにモニタされているスイッチに接続している場合、Emergency Responder は緊急コールを発信した電話機を推測する必要があります。シェアド ライン アピアランスを使用するすべての電話機が同じ ERL 内にある場合、推測は成功します。電話機の ERL が複数の場合、推測に失敗する可能性があります。

関連項目

- 「2 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-31）
- 「Cisco Emergency Responder グループ間の通信に対するルート パターンの作成」（P.3-19）

不適切な ERL を使用した 802.11b エンドポイント

802.11b エンドポイント（802.11b で実行される Cisco Wireless IP 7920 Phone や Cisco IP SoftPhone など）は、設定済みのサブネットベースの ERL ではなく、スイッチ ポートベースの ERL を使用しています。

Cisco Emergency Responder（Emergency Responder）では、コール ルーティングのスイッチ ポートの関連付けにより高いプライオリティが付与されます。Emergency Responder によって任意のエンドポイント（802.11b エンドポイントを含む）のスイッチ ポート マッピングが検出された場合、緊急

コールのルーティングにスイッチ ポートが使用されます。スイッチ ポート マッピングが検出されない場合、または対応するスイッチ ポートに ERL が設定されていない場合、Emergency Responder 1.2 はサブネット ERL 設定を使用して緊急コールをルーティングします。

Emergency Responder 8.6 は次のような状況下ではスイッチ ポートの背後で 802.11b エンドポイントを検出することに注意してください。

- 接続しているアクセス ポイントまたはスイッチ ポートで、Cisco Discovery Protocol（CDP）がディセーブルです。
- 特定のスイッチの CAM トラッキングが Emergency Responder でイネーブルです。

スイッチ ポート画面または ERL デバッグ ツール（「ERL Debug Tool を使用した Cisco Emergency Responder 設定の確認」（P.11-18）を参照）で、802.11b エンドポイントがスイッチ ポートに関連付けられていることを確認してください。

サブネットベースの ERL を使用して 802.11b エンドポイントを追跡することをお勧めします。そのため、緊急コールを 802.11b エンドポイントからサブネット ベースの ERL にルーティングするように、スイッチ ポートおよびアクセス ポイントで CDP を有効にします。

関連項目

- 「IP サブネットベースの ERL の設定」（P.4-38）

緊急コールに関する問題のトラブルシューティング

ここでは、緊急コールのルーティングに関する問題の解決に役立つ情報や、コール時に提供される情報について説明します。

緊急コールが Cisco Emergency Responder で代行受信されない

Emergency Responder で緊急コールが代行受信されない場合、Cisco Unified CM 設定の誤りか、Emergency Responder 設定での表現の誤りが原因の可能性があります。

- 緊急コール番号（911）は Phones パーティション内にあり、E911CSS コーリング サーチ スペースを使用します。Emergency Responder のインストール時に、この番号が識別されるようにします（「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）を参照）。その結果、ユーザは緊急番号にダイヤルできるようになります。Cisco Unified CM でこの番号を設定する方法については、「緊急コールのルート ポイントの作成」（P.3-6）を参照してください。

- スタンバイ Emergency Responder サーバのルート ポイント（912）は E911 パーティション内にあり、E911CSS コーリング サーチ スペースを使用します。Cisco Unified CM でこの番号を設定する方法については、「緊急コールのルート ポイントの作成」（P.3-6）を参照してください。Emergency Responder 設定で、この番号をスタンバイ サーバのルート ポイントとして定義します（「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）を参照）。
- PSAP コールバック ルート ポイント パターン（913XXXXXXXXXX）は、E911 パーティション内にあり、E911CSS コーリング サーチ スペースを使用します。Cisco Unified CM でこの番号を設定する方法については、「緊急コールのルート ポイントの作成」（P.3-6）を参照してください。Emergency Responder 設定で、この番号が PSAP コールバック ルート ポイント パターンとして定義されていること、および削除プレフィクス（913）も指定されていることを確認します（「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）を参照）。
- すべての ELIN ルート パターンは E911 パーティション内にあります。Cisco Unified CM でこれらの番号を設定する方法については、「ERL のルート パターンの作成」（P.3-11）を参照してください。
- すべての電話と CTI ポート（デバイスと回線の両方）は Phones パーティション内にあり、PhoneCSS コーリング サーチ スペースを使用します。追加のパーティションは使用できますが、Emergency Responder パーティションおよびコーリング サーチ スペースとの関係について、“Setting Up Cisco Emergency Responder to Handle Emergency Calls” section on page 4-4 に記載されている例のパーティションと同じ方法でパーティションを設定する必要があります。
- サービス プロバイダーのネットワークに対するすべてのゲートウェイは、E911CSS コーリング サーチ スペースを使用します。詳細については、「PSAP への接続に使用されるゲートウェイに対するコーリング サーチ スペースの設定」（P.3-18）を参照してください。
- 設定されている Cisco Unified CM バージョン（JTAPI jar）が適切です。Cisco Unified CM バージョンを確認するには、次の手順を実行します。
  1. Emergency Responder Admin Utility Web サイトにログインします。
  2. [Update]>[CCM Version] を選択します。
  3. [Status] セクションで、[Current Version of CCM] を確認します。

ELIN が PSAP に伝送されない

ELIN が PSAP に伝送されず、PSAP に対する緊急コールのルーティングに PRI 接続を使用している場合、ゲートウェイの設定を確認します。本社の番号などの固定番号ではなく、実際の発信者番号（ELIN）が送信されるように、PRI を設定する必要があります。「PSTN に対する CAMA トランクまたは PRI トランクの取得」（P.1-20）を参照してください。

他の ERL からのコールにデフォルトの ERL の ELIN が使用される

発信元の ERL に割り当てられている ELIN ではなく、デフォルトの ERL に定義されている ELIN が緊急コールに割り当てられる場合、次の点を確認してください。

- Cisco Unified CM で、使用されるはずの ELIN のルート パターンについて確認します。「ERL のルート パターンの作成」（P.3-11）を参照してください。
- Emergency Responder の ERL 定義で、その ERL について ELIN が正しく設定されていることを確認します。「ERL と ALI の設定」（P.4-35）を参照してください。

ERL のルート パターンが失敗する場合、デフォルト ERL に定義されているルート パターンが使用されます。

緊急コールが正しい PSAP にルーティングされない

緊急コールがどの PSAP にもルーティングされない場合、発信元の ERL とデフォルト ERL に使用されているルート パターンが設定されていること、および正しいパーティションとコーリング サーチ スペースを使用していることを確認します（「ERL のルート パターンの作成」（P.3-11）を参照）。ゲートウェイのパーティションとコーリング サーチ スペースが正しいことを確認します（「PSAP への接続に使用されるゲートウェイに対するコーリング サーチ スペースの設定」（P.3-18）を参照）。

緊急コールはローカル ネットワークから送出されますが、正しい PSAP にルーティングされない場合、問題の原因と考えられる次の点を確認してください。

- 電話機に割り当てられた ERL に、正しい ELIN を割り当てるように Emergency Responder を設定していますか。緊急コールは ELIN に基づいてルーティングされるため、誤った ELIN を割り当てると、コールは正しくルーティングされません。「ERL の作成」（P.4-33）を参照してください。
- ELIN が正しい場合、ELIN のルート パターンには正しいゲートウェイを使用するように設定されていますか。誤ったゲートウェイを選択すると、目的の PSAP に接続できないサービス プロバイダーのネットワークの部分にコールがルーティングされる可能性があります。ゲートウェイの要件を判断するには、サービス プロバイダーにお問い合わせください。

  次のトピックを参照してください。

  - 「 •「ERL の作成」（P.4-33）」（P.3-10）
  - 「2 つ以上の PSAP がある 1 つのメイン サイトでの Cisco Emergency Responder の配置」（P.1-26）
- サービス プロバイダーの ALI データベースに、ELIN の正しい情報が格納されていますか。外部ネットワークでの緊急コールは、ローカル ネットワークの情報ではなく、サービス プロバイダーのデータベースの情報に基づいてルーティングされます。「ERL 情報のエクスポート」（P.4-41）を参照してください。
- 緊急コールの電話機は、元のスイッチ ポートをサポートする Emergency Responder グループとは異なる Emergency Responder グループがサポートする Cisco Unified CM クラスタに登録されていますか。この場合、Emergency Responder クラスタの設定が正しくない可能性があります。次のトピックを参照してください。

  - 「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）
  - 「Cisco Emergency Responder グループ間の通信に対するルート パターンの作成」（P.3-19）
  - 「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）

（注） コールは PSAP に到達しますが、PSAP が発信者と通話できない場合、リモート Emergency Responder グループの Cisco Unified CM が、ゲートウェイとしてローカル Emergency Responder グループの Cisco Unified CM を定義していることを確認します。

緊急コールの発信者がビジー信号を受信することや、緊急コールがルーティングされないことがある

発信者が緊急コール番号に発信したときにビジー信号が聞こえる場合、または緊急コールがルーティングされないことがある場合、スタンバイ Emergency Responder サーバの設定が原因の可能性があります。

- プライマリ Emergency Responder サーバのみを設定している場合、スタンバイ Emergency Responder サーバのインストールおよび設定を行います。プライマリ サーバの CPU 使用率が 100% に達すると、Emergency Responder は緊急コールを処理できなくなります。この場合、スタンバイ サーバがあればコールを処理できます。
- スタンバイ サーバのルート ポイント設定を確認します。緊急コール ルート ポイントのコール転送設定で、この番号にコールが転送されるように指定します。Cisco Unified CM の設定については「緊急コールのルート ポイントの作成」（P.3-6）、Emergency Responder の設定については「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）を参照してください。

PSAP コールバック エラー

PSAP オペレータが、発信者 ID に指定されている ELIN を使用して緊急コールの発信者にコールバックしようとしたときに、この問題が発生することがあります。

症状　PSAP は、元の緊急コール内線番号に到達できないことがあります。

推奨処置　Emergency Responder は、発信者の実際の内線番号と、ERL に定義した ELIN とのマッピングを取得します。ERL に定義した ELIN の数よりもコール数が多いと、Emergency Responder は番号を再利用するため、元の発信者の内線番号は上書きされます。元の発信者の内線番号を判断するには、コール履歴を確認します。「緊急コールの発信時に発生するプロセス」（P.1-9）を参照してください。

これが問題ではない場合、Cisco Unified CM と Emergency Responder で PSAP コールバック ルート ポイントの設定（「緊急コールのルート ポイントの作成」（P.3-6）および「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）を参照）を確認し、Cisco Unified CM で ELIN トランスレーション パターンを確認します（「ELIN のトランスレーション パターンの作成」（P.3-13）を参照）。

症状　オンサイト アラート（セキュリティ）担当者は、PSAP からコールバックを受けます。

推奨処置　キャッシュにある緊急コールの ELIN から内線へのマッピングが期限切れになった場合、Emergency Responder はデフォルトの ERL のオンサイト アラート担当者に PSAP コールバックをルーティングします。デフォルトでは、これは 3 時間ですが、期限を 3 時間よりも長くしたり、短くしたりすることができます。「Cisco Emergency Responder Group Settings」（P.A-3）を参照してください。

オンサイト アラート担当者が電話機のアラートを受信できない

ERL で緊急コールが発信されたときに、オンサイト アラート担当者が電話機のアラートを受信できない場合、すべての電話機と CTI ポート（デバイスと回線の両方）が Phones パーティション内にあり、PhoneCSS コーリング サーチ スペースを使用していることを確認します。追加のパーティションは使用できますが、Emergency Responder パーティションおよびコーリング サーチ スペースとの関係について、“Setting Up Cisco Emergency Responder to Handle Emergency Calls” section on page 4-4 に記載されている例のパーティションと同じ方法でパーティションを設定する必要があります。

また、Cisco Unified CM クラスタの Emergency Responder 設定が正しいことを確認します。Emergency Responder 設定には、Cisco Unified CM で CTI ポートとして定義した電話ポートの正しい開始アドレスが表示されること、および電話ポートの番号が正しいことを確認します。コールが発生した場合、この番号は常に 0 より大きな値になります。Emergency Responder では、オンサイト アラート担当者への発信にこの CTI ポートを使用します。

Emergency Responder Serviceability Web インターフェイスの Event Viewer にエラー メッセージ「No port to place call」が表示された場合、オンサイト アラート担当者へのすべてのコールを開始するために定義された十分な CTI ポートが存在しません。そのため、追加のポートを定義する必要があります。Event Viewer にアクセスするには、Emergency Responder Serviceability Web インターフェイスにログインし、[Tools]>[Event Viewer] を選択します。

緊急コールの着信時にオンサイト アラート電話機の着信音が鳴らない

緊急コールの着信時にオンサイト アラート電話機の着信音が鳴らない場合、次の問題が発生している可能性があります。

症状　緊急コールの着信時にオンサイト アラート電話機の着信音が鳴らない。

考えられる原因　電話機の Do Not Disturb（DND）機能がイネーブルの場合、および Cisco Unified CM 6.x を使用して Emergency Responder を設定している場合、オンサイト アラート電話機の着信音は鳴りません。

推奨処置　オンサイト アラート電話機では、DND をイネーブルにしないでください。

電話機のアラートのプロンプトが再生されない

電話機のアラートのプロンプトが再生されない場合、次の問題が発生している可能性があります。

症状　コールが CTI ポートから発信された場合、オンサイト アラート電話機ではプロンプトは再生されません。

説明　この問題は、複数の回線に単一の CTI ポートが設定されている場合に発生する可能性があります。オンサイト アラートの通知コールがこのような 1 つまたは複数の回線を介して発信された場合、その回線からのプロンプトは再生されない可能性があります。

推奨処置　この問題を回避するには、Emergency Responder に設定されている Cisco Unified CM で、CTI ポートにつき 1 行のみ設定します。

オンサイト アラート担当者に電子メール（または呼び出し）通知が送信されない

オンサイト アラート担当者の電子メール アドレスを設定（「Onsite Alert Settings」（P.A-13）を参照）しても、電子メールまたは電子メールベースの呼び出しが送信されない場合、Emergency Responder 設定で SMTP の設定を確認します。SMTP サーバ アドレスと発信元メール ID が正しいことを確認し（「Cisco Emergency Responder Group Settings」（P.A-3）を参照）、SMTP サーバにそのメール ID のアカウントがあることを確認します。

誤った位置情報がオンサイト アラート担当者に送信される

オンサイト アラート（セキュリティ）担当者に送信される緊急コールの位置情報に誤りがある場合、次の問題の可能性を検討してください。

- ERL の ALI データは正しいですか。「ERL の作成」（P.4-33）を参照してください。
- スイッチ ポートの電話位置データは正しいですか。「スイッチ ポートの設定」（P.4-54）を参照してください。
- 電話が接続されるスイッチ ポートには、正しい ERL が割り当てられていますか。これらの条件に該当しない場合、次の 2 つの問題が考えられます。
  - 誰かがスイッチの配線を変更したため、以前は正しかった設定が無効になりました。配線を別のポートに移動すると、ERL の割り当てが無効になる可能性があります。「データの整合性および信頼性に関する考慮事項」（P.1-18）を参照してください。
  - ワイヤリング クローゼットは保護されており、単に ERL の割り当てが間違っています。「スイッチ ポートの設定」（P.4-54）を参照してください。
- （任意の永続的 ERL にデフォルトの ERL を使用していないという前提で）コールの発信元はデフォルトの ERL でしたか。この場合、次の問題が発生している可能性があります。
  - 電話機はサポート対象外のポートに接続され、手動電話機として定義されていません。「電話機の手動での定義」（P.4-63）を参照してください。
  - 電話機はサポート対象外であり、手動電話機として定義されていません。「電話機の手動での定義」（P.4-63）を参照してください。
  - 電話機はサポートされていますが、Emergency Responder で位置を確認できませんでした。この問題を解決できない場合、状況によっては手動で電話機を ERL に割り当てる必要があります。「位置未確認の電話機が多すぎる」（P.11-2）を参照してください。
- コールは手動で定義した電話機の内線番号から発信されましたか。その場合、おそらく電話が移動されたために、誤った ERL が割り当てられている可能性があります。「電話機の手動での定義」（P.4-63）を参照してください。

緊急コールの履歴に関する問題

ここでは、緊急コールの履歴情報を表示するとき（「緊急コール履歴の表示」（P.4-67）を参照）に発生する可能性があるいくつかの問題について説明します。

症状　緊急コール情報は、コール履歴にすぐには表示されません。

推奨処置　Emergency Responder では、15 秒ごとにデータベースへコール履歴情報が書き込まれます。そのため、コール履歴情報を表示できるのは、15 秒後の可能性があります。

症状　コール履歴には、コールに使用された ELIN とルート パターンは表示されません。

推奨処置　コールを PSAP にルーティングできなかった場合、ELIN またはルート パターンは表示されません。コールをルーティングできなかった理由を確認して判断してください。「緊急コールが正しい PSAP にルーティングされない」（P.11-7）を参照してください。

電子メール アラートのトラブルシューティング

ここでは、Emergency Responder で生成される電子メール アラートに関する問題の解決に役立つ情報について説明します。

Emergency Call Alert（緊急コール アラート）

ユーザが 911（緊急）コールを発信すると、Emergency Responder で電子メール アラートが生成されます。Emergency Responder から、コールが発信された ERL に設定されている電子メール ID を持つオンサイト アラート（セキュリティ）担当者全員に電子メール アラートが送信されます。（「Cisco Emergency Responder サーバ グループの設定」（P.4-22）を参照）。

セキュリティ担当者はそのユーザに応答します。詳細については、次の URL のマニュアルを参照してください。

http://<<*CERServer HostName*>>/ceruserreports

911 コールが発信され、バックアップ Emergency Responder サーバがコールを処理する場合、次のようなアラートが送信されます。

```
Subject: Emergency Call Alert -- Extn # 332101 (Generated by Backup Cisco ER)
Message: EMERGENCY CALL DETAILS (Generated by Emergency Responder)
Caller Extension:332101
Zone/ERL          :Z1
Location          :ddd
Call Time         :June 2, 2003 3:47:30 PM IST
```

Transition Alert（移行アラート）

スタンバイ Emergency Responder サーバがコールを制御し、アクティブ サーバになる場合、Transition Alert が Emergency Responder 管理者に送信されます。この状況は、次の条件で発生します。

- プライマリ Emergency Responder サーバが停止した場合。
- プライマリ Emergency Responder サーバで Emergency Responder サービスが停止した場合。
- プライマリおよびスタンバイの Emergency Responder サーバ間の接続が切断された場合。

管理者は原因を診断し、できるだけ早く問題を解決する必要があります。

Emergency Responder バックアップ サーバがコールを制御すると、次のようなアラートが送信されます。

```
Subject: Transition Alert: Cisco ER Backup is active
Message:
Backup Cisco ER <<CER HostName>> has taken control as Active Cisco ER.
Transition Time  :June 2, 2003 3:57:12 PM IST
```

マスター Emergency Responder サーバがコールを制御すると、次のようなアラートが送信されます。

```
Subject: Transition Alert: Cisco ER Master is active
Message:
Master Cisco ER <<Emergency Responder Server HostName>> has taken control as Active Cisco
ER.
Transition Time  :June 2, 2003 3:57:12 PM IST
```

Tracking Failure（トラッキング エラー）

スイッチ ポートと電話機のトラッキング プロセスが終了するときに、追跡できなかったデバイスがある場合、Emergency Responder から Emergency Responder 管理者に Tracking Failure の電子メールが送信されます。

管理者は Emergency Responder サーバのイベント ログを確認し、追跡されなかったデバイスのリストを探す必要があります。次に、以下の点を確認し、必要な修正を行います。

1. 正しい SNMP コミュニティ ストリングが Emergency Responder に設定されていることを確認します。
2. デバイスが接続されていることを確認します。
3. Emergency Responder サーバのホスト名が解決可能であること（つまり、検出可能であること）を確認します。
4. そのデバイス（スイッチや Cisco Unified CM）で SNMP サービスがイネーブルであることを確認します。

次に、Tracking Failure アラートの例を示します。

```
Subject: CER Phone Tracking failed to track some devices
Message:
CER Phone Tracking could not get information [using SNMP] from 2 Cisco Cisco Unified CM(s)
and 1 Switch(es)
Check Event Viewer on CER Server for details.
```

Failed To Get Provider（プロバイダーの取得に失敗しました）

Emergency Responder が、設定済みの Cisco Unified CM クラスタの 1 つに登録できない場合、Emergency Responder から Emergency Responder 管理者に Failed to Get Provider アラートが送信されます。Emergency Responder は、登録が成功するまで登録の試行を続けます。数回の再試行後、Emergency Responder からは Failed to Get Provider 電子メールが送信されます。

このメッセージでは、次の例のように、問題の解決方法に関する情報を提供します。

```
Subject: Failed to get JTAPI Provider for Cisco Unified CM <<CCM IP/Host Name>> (Generated
by Backup Cisco ER)
Message:
Please check the following:
1) Check if the Cisco Unified CM is connected to the CER server.
2) Check if the configured Call Manager is running a version supported by the CER server.
```

```
3) Check if the given login credentials are correct:
    CTI Manager Host Name:<<CCM IP/HostName>>
```

Failed to Establish Communication with Cisco Emergency Responder Phone Tracking Engine（Cisco Emergency Responder Phone Tracking Engine との通信の確立に失敗しました）

Emergency Responder サーバが Phone Tracking Engine との通信の確立に一定の期間失敗した場合、Emergency Responder から Emergency Responder 管理者にこのメッセージが送信されます。Emergency Responder Phone Tracking Engine サービスが停止した場合、この問題が発生する可能性があります。管理者は次の手順を実行する必要があります。

1. Emergency Responder Phone Tracking Engine サービスが停止した場合、そのサービスを開始します。
2. Emergency Responder サーバのホスト名にアンダースコア（_）文字が含まれないことを確認します。

次に、Tracking Failure アラートの例を示します。

```
Subject: CER Server failed to establish communication with CER Phone Tracking Engine.
Message:
CER Server could not communicate with CER Phone Tracking Engine.
```

Lost Communication with Cisco Emergency Responder Phone Tracking Engine（Cisco Emergency Responder Phone Tracking Engine との通信が失われました）

Emergency Responder サーバと Emergency Responder Phone Tracking Engine との通信が失われた場合、Emergency Responder から Emergency Responder 管理者にこの電子メール アラートが送信されます。この問題の最も可能性が高い原因は、Emergency Responder サービスの実行中に Emergency Responder Phone Tracking Engine サービスが停止した場合です。

管理者は Emergency Responder Phone Tracking Engine サービスを再開する必要があります。

次に、Tracking Failure アラートの例を示します。

```
Subject: CER Server lost communication with CER Phone Tracking Engine
Message:
CER Server could not communicate with CER Phone Tracking Engine.
```

Failed to Send Unlocated Phone Details to Remote Cisco Emergency Responder Server Group（位置未確認の電話機の詳細をリモートの Cisco Emergency Responder サーバ グループに送信できませんでした）

サーバ グループに対してすでにエントリの送信プロセスが実行されているために、Emergency Responder からそのサーバ グループに対して位置未確認エントリの送信に失敗した場合、このアラートが送信されます。

このアラートはほとんど発生しません。このアラートが発生するのは、1 つの Emergency Responder サーバが複数の Emergency Responder サーバ グループで検出される場合です。この問題を解決するには、古い設定のサーバ グループを確認し、そのサーバ グループを削除します。

```
Subject: CER Server failed to send Unlocated Phones details to Remote CER Server Group.
Message:
CER Server failed to send Unlocated Phones to Remote CER Server Group. Please ensure that
the CER servers are not found under more than one CER Server Group.
CER Servers in Remote Server Group:<< CERServer HostNames >>
```

Emergency Call Could Not be Routed（緊急コールをルーティングできませんでした）

ERL に設定されている一部のルート パターンに対する緊急コールのルーティングが失敗する場合、Emergency Responder からシステム管理者に電子メールが送信されます。

件名：Emergency call could not be routed using some route patterns (CERServer:<*server hostname*>)

*メッセージ本文：*Emergency call from: <Caller Extn> could not be routed using some Route Patterns.Check Event Log.

Event Log には次のメッセージが表示されます。

```
Emergency call from <extn> could not be routed using the following route patterns

<RoutePattern1>
<RoutePattern2>
*****************
Call Routed to <RoutePattern-X>

Please check the availability of the above routes. Also, check for the following error
conditions:

1. If FAC and/or CMC are configured on the route patterns used for Cisco ER, please
disable them.
2. If the "Calling Party Number Modification" flag on the CER user page in the Cisco
Unified CM is not enabled, please enable it.
```

ソリューション

1. Cisco Unified CM 4.2 または 4.3 を実行している場合、Emergency Responder ユーザ ページの [Calling Party Number] チェックボックスがオンであることを確認します。
2. Cisco Unified CM 5.x または Cisco Unified CM 6.x を実行している場合、ルートが使用可能であることを確認します。
3. Emergency Responder アプリケーション ユーザが「Standard CTI Allow Calling Number Modification」ユーザ グループに追加されます。

Calling Party Modification Failed（発信側の修正に失敗しました）

発信側の修正に失敗した場合、Emergency Responder からシステム管理者に次の電子メールが送信されます。

*件名：*Emergency Calling Party Modification Failed (Emergency ResponderServer: <*server*>)

*メッセージ本文：*Emergency call from: <Caller Extn> cannot be routed with calling party modification.Check Event Log.

Event Log には次のメッセージが表示されます。

```
Emergency Call from <Caller Extn> has been routed to default ERL because the calling party
modification failed.
Please make sure that the checkbox "Enable Calling Party Number Modification: is checked
on the Cisco Unified CM user page for the CER user. PSAP callbacks MAY NOT work correctly.
The CER service will need to be restarted once the flag is checked on the Cisco Unified CM
User page.
```

ソリューション　Cisco Unified CM 4.2 または 4.3 Administration の場合、Emergency Responder ユーザ ページの [Enable Calling Party Number Modification] チェックボックスをオンにします。このフラグをイネーブルにした後は、変更内容を反映するために Emergency Responder サービスを再起動します。

Web アラートのトラブルシューティング

Web アラートの受信時に次の問題が発生する可能性があります。

症状　Web アラートは 30 秒ごとに更新を続けます。この問題を確認するには、ブラウザでステータスを確認します。このモード中は、ステータスに更新までの残り時間（秒）が表示されます。

推奨処置　同じクライアント マシンで別の Web アラート画面が開いているかどうかを確認します。リアルタイム モードで 1 台のクライアント マシンから操作できるのは 1 つのブラウザのみです。余計なブラウザは削除します。

Cisco Emergency Responder システムおよび管理に関する問題のトラブルシューティング

ここでは、サーバと Web サーバの問題など、Emergency Responder システムとその管理に関する問題の解決に役立つ情報について説明します。

パブリッシャを確認できない

インストール処理でパブリッシャを確認できない場合（「Cisco Emergency Responder Subscriber のインストール」（P.2-19）のステップ 5）、次の点を確認してください。

1. パブリッシャのホスト名が正しいこと、およびホスト名でパブリッシャに到達可能であることを確認します。
2. パブリッシャとサブスクライバ サーバが同じバージョンの Emergency Responder を実行していることを確認します。
3. 入力したデータベースのパスワードが正しいことを確認します。これは、インストール時に [Database Access Security Configuration] ページで指定したパスワードです。
4. パブリッシャでサブスクライバが正しく設定されていることを確認します。

ログインに関する問題のトラブルシューティング

ここでは、Emergency Responder にログインするときに発生する可能性があるいくつかの問題について説明します。

症状　Emergency Responder Administration Web サイトにログインできません。

推奨処置　CLI にログインし、**utils service list** コマンドを実行します。ステータス「Cisco IDS」が STARTED かどうかを確認します。STARTED ではない場合、**utils service start** *service name* コマンドを使用してサービスを開始します。

症状　Netscape Navigator を使用して複数の Emergency Responder セッションを開くことはできません。

推奨処置　Netscape/Mozilla Navigator は同じセッション ID を複数のウィンドウにわたって使用します。そのため、異なる ID を使用して Emergency Responder にログインしようとすると問題が発生します。通常、システム管理者としてログインすると、複数のウィンドウを開くことができます。Internet Explorer を使用し、（既存のセッションから新しいウィンドウを開くのではなく）新しい IE インスタンスを開始して別の IE セッションを開いた場合、IE は異なるセッション ID を使用します。そのため、異なる ID を使用してログインできます（たとえば、ユーザと管理者として、LAN スイッチ管理者と ERL 管理者としてなど）。

関連項目

- 「ERL Debug Tool を使用した Cisco Emergency Responder 設定の確認」（P.11-18）

Cisco Unified Operations Manager の使用

Emergency Responder システムの動作状況を継続的にモニタするには、Cisco Unified Operations Manager 2.01 を使用します。

Cisco Unified Operations Manager を使用するように Emergency Responder を設定する方法については、「テスト ERL の設定」（P.4-40）を参照してください。

Cisco Unified Operations Manager のインストール方法と使用方法については、次のマニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/cscowork/index.html

Cisco Emergency Responder スイッチとポートの設定に関する問題のトラブルシューティング

Emergency Responder でスイッチまたはスイッチ ポートの設定するとき、次の問題が発生する可能性があります。

症状　Emergency Responder は Cisco Unified CM の情報を使用して設定されていますが、電話機が検出されません。

推奨処置　ネットワークで Cisco Unified CM サーバに到達可能であることを確認します。次に、スイッチおよび Cisco Unified CM サーバの SNMP 読み取りコミュニティ ストリングが正しく設定されていることを確認します（「SNMP 接続の設定」（P.4-45）を参照）。次に、スイッチ ポートと電話機の更新プロセスを手動で実行します（「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）を参照）。CLI ベースの **utils snmp** コマンドを使用して、Cisco Unified CM が SNMP で到達可能かどうかを確認します。

症状　Emergency Responder で、Emergency Responder に設定されているスイッチのポートが表示されません。

推奨処置　サポート対象のスイッチを Emergency Responder に追加し、追加後にスイッチで電話機のトラッキングを実行すると、スイッチでイーサネット ポートのリストを表示できます。Emergency Responder でポート リストが表示されない場合、スイッチの Emergency Responder で SNMP 設定を確認します（「SNMP 接続の設定」（P.4-45）を参照）。また、ネットワーク上でスイッチに到達可能であることを確認します。スイッチで特定の電話機のトラッキング プロセスを再試行します（スイッチの詳細情報を表示しているときに、[Locate Switch Ports] をクリックします。詳しくは「LAN Switch Details」（P.A-44）を参照してください）。

問題が解決しない場合、スイッチがサポート対象であることを確認します（「ネットワークのハードウェアおよびソフトウェアの要件」（P.1-4）を参照）。また、Event Viewer でエラー メッセージを確認します。

症状　一部の電話機がスイッチ ポート リストに表示されません。

推奨処置　設定済みの IP サブネットまたは擬似電話機内に電話機があるかどうかを確認します。いずれの場所でも見つからなかった場合、位置未確認の電話機として配置されます。電話機の位置を確認できなかった理由のリストについては、「位置未確認の電話機が多すぎる」（P.11-2）を参照してください。

症状　Emergency Responder の設定からスイッチを削除できません。

推奨処置　電話機のトラッキング プロセスが進行中の場合、スイッチは削除できません。プロセスの終了後に削除を再試行してください。これが問題ではない場合、Emergency Responder サーバが実行されていない可能性があります。コントロール センターを確認し、サーバを再起動してください（「Cisco Emergency Responder サーバの起動と停止」（P.11-25）を参照）。

症状　スイッチ ポートの詳細の読み込みまたは書き出しに失敗します。

推奨処置　スイッチ ポートの読み込みまたは書き込みの試行に失敗する場合、次の理由が考えられます。第 1 に、スイッチ ポートと電話機の更新プロセスがまだ終了していません（完了するまで待ってください）。第 2 に、Emergency Responder サーバが実行されていません（コントロール センターを使用して再起動します。「Cisco Emergency Responder サーバの起動と停止」（P.11-25）を参照してください）。第 3 に、Emergency Responder サーバの初期化が完了していません（初期化されるまで待ってください）。

症状　一部のスイッチ ポート設定の読み込みに失敗します。

推奨処置　スイッチ ポート設定を読み込むには、スイッチで Emergency Responder を設定済みであり、Emergency Responder はスイッチ ポートと電話機の更新プロセスを使用して、まずスイッチ上のポートを検出する必要があります。Emergency Responder でまだ検出されていないポートの設定を読み込もうとすると、設定の読み込みに失敗します。このプロセスについては、「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）を参照してください。ポート設定を読み込むことができないスイッチでこのプロセスを実行してから、読み込みを再試行してください。

症状　電話機が他の Emergency Responder グループからこの Emergency Responder グループに移動され、また元のグループに移動した場合、電話機は、この Emergency Responder グループのスイッチ ポートの詳細に表示されます。

推奨処置　このような電話機は、次回のスイッチ ポートと電話機全体の更新プロセスが実行されるまで、スイッチ ポートの詳細から削除されません。これが問題の場合、そのスイッチ（またはすべてのスイッチ）でプロセスを手動実行できません。「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）を参照してください。

ERL Debug Tool を使用した Cisco Emergency Responder 設定の確認

ERL Debug Tool は検索条件として電話機の内線番号を使用し、電話機の緊急コールのルーティングに現在使用されている ERL を表示します。

この診断ツールを使用して、ERL の作成および ERL の割り当てフェーズ時の Emergency Responder の設定を確認し、誤った ERL 宛てのコールの問題を解決します。

たとえば、手動設定した電話機として ERL_1 を設定したとします。ただし、設定を誤った IP サブネットがこの電話機の IP アドレスと一致し、ERL_2 と関連付けられています。この場合、Debug Tool を使用して設定の問題を検出し、修正できます。

ERL Debug Tool を使用するには、次の手順を使用します。

手順

ステップ 1　[Tools] > [ERL Debug Tool] を選択します。

Emergency Responder の [ERL Debug Tool] ページが表示されます。

ステップ 2　特定の電話のリストを表示するには、[Find Phones] フィールドで検索条件を選択し、[Find] をクリックします。

その電話機で緊急コールのルーティングに現在使用されている ERL が表示されます。

ステップ 3　設定が正しくない場合、必要に応じて修正します。

（注）　Emergency Responder には最大 1,000 レコードが表示されます。

パブリッシャ サーバとサブスクライバ サーバの交換

問題のあるパブリッシャ サーバまたはサブスクライバ サーバを交換する必要がある場合、次のように適切な手順を実行します。

- 「問題のあるサブスクライバの交換」（P.11-19）
- 「問題のあるパブリッシャの交換」（P.11-19）

問題のあるサブスクライバの交換

問題のあるサブスクライバを交換するには、Emergency Responder Administration を使用し、そのサブスクライバを削除します。パブリッシャの新しい Emergency Responder サブスクライバをインストールします（「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）を参照）。

（注）　新しい交換サブスクライバ サーバで同じホスト名を使用しない予定の場合、パブリッシャ サーバの Emergency Responder Administration の画面から、問題のあるサブスクライバを削除する必要があります。

問題のあるパブリッシャの交換

パブリッシャを復元できるのは、Emergency Responder の一部として使用できる Disaster Recovery System でパブリッシャをバックアップした場合のみです。「データのバックアップと復元」（P.11-33）を参照してください。

問題のあるパブリッシャを交換するには、次の手順を実行します。

手順

ステップ 1　以前に使用していたものと同じホスト名を持つ同じバージョンの Emergency Responder Publisher をインストールします。

ステップ 2　インストール時には同じ設定オプションを選択します（Cisco Unified CM のバージョンなど）。

ステップ 3　Disaster Recovery System を使用して、古い設定データを復元します。

Cisco Emergency Responder Admin Utility の使用

Emergency Responder Admin Utility Tool を使用して、次の作業を実行できます。

- Emergency Responder クラスタ データベース ホストの詳細を更新する

- CCM バージョンをアップグレードする

ここでは、次のトピックについて取り上げます。

- 「Cisco Emergency Responder Admin Utility Tool の使用方法」（P.11-20）

Cisco Emergency Responder Admin Utility Tool の使用方法

Emergency Responder Admin Utility Tool を使用するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Admin Utility Web インターフェイスにログインします。

ステップ 2　メニュー バーを使用して、実行するタスクを選択します。

a. サブスクライバ サーバが示すパブリッシャを変更するには、[Update]>[Publisher] を選択します。

b. Cisco Unified CM バージョンを更新するには、[Update]>[CCM Version] を選択します。

c. パブリッシャ サーバとサブスクライバ サーバの両方でクラスタ設定を更新するには、[Cluster]>[DBHost] を選択します。

（注）　このアクションで、このサーバ グループの Emergency Responder クラスタ DB の詳細のみが更新されます。この Emergency Responder クラスタの他のサーバは自動更新されません。

ステップ 3　変更内容を保存するには、パブリッシャ サーバとサブスクライバ サーバの両方を再起動します。

サブスクライバ データベースの設定のトラブルシューティング

（DB レプリケーションとは別の）サブスクライバに関する問題がある場合、パブリッシャとサブスクライバを設定し直すには、次の手順を実行します。

手順

ステップ 1　サブスクライバ サーバの Emergency Responder Admin Utility インターフェイスにログインします。

ステップ 2　[Update]>[Publisher] を選択します。

ステップ 3　同じパブリッシャのホスト名、IP アドレス（すでに指定済み）、およびデータベース アクセス セキュリティ パスワードを指定します。

ステップ 4　[Go] をクリックします。

この設定手順には時間がかかることがあります。

データベースおよびエンタープライズ レプリケーションのトラブルシューティング

Informix Dynamic Server（IDS）データベースのトラブルシューティングには、次の CLI コマンドを使用します。

- **utils service list**：IDS サービスが実行中かどうかを確認するために使用されます。
- **show tech dbstateinfo**：データベースに関する問題のデバッグに役立つ DB の状態情報を表示します。
- **show tech dbinuse**：現在使用されているデータベースを表示します。
- **show tech dbintegrity**：データベースの整合性情報を表示します。
- **show tech database**：データベースのすべてのテーブルのコンテンツを含む 1 つの .csv ファイルを作成します。

エンタープライズ レプリケーションのトラブルシューティングには、次の CLI コマンドを使用します。

- **utils dbreplication status**：データベース レプリケーションののステータスを表示するために使用されます。
- **utils dbreplication reset**：パブリッシャとサブスクライバ間のデータベース レプリケーションをリセットし、再起動します。
- **utils dbreplication repair**：レプリケーション サーバ（パブリッシャとサブスクライバ）上のデータを比較し、データの不統一を列挙したレポートを作成し、データの不統一を修復します。また、何らかの理由で .rhosts ファイルが破損した場合、このコマンドは、そのファイルを再構築してレプリケーションの修復も試行します。

ログを使用してデータベースに関する問題を解決するには、Emergency Responder Serviceability Web サイトまたは CLI を介してログをダウンロードします。

次のログは、データベースに関連する問題をデバッグするための情報を提供します。

- Install/Upgrade ログ：/var/log/install/
- Install DB ログ：/var/log/active/er/trace/dbl/sdi/
- CERDbMon ログ：/var/log/active/er/trace/dbl/sdi/cerdbmon/
- CLI ログ：/var/log/active/platform/log/

症状　DNS を使用してサブスクライバをインストールした後にレプリケーションの起動に失敗し、CLI コマンド **utils dbreplication status** でレプリケーションが動作していないと表示されます。

考えられる原因　.rhosts は、サブスクライバの FQDN（完全修飾ドメイン名）ではなく、サブスクライバのホスト名になります。

推奨処置　レプリケーションの問題を修復するには、CLI コマンド **utils dbreplication repair** を使用します。このコマンドは、破損した .rhosts ファイルを再構築して、レプリケーションの修復を試行します。

Cisco Emergency Responder システムに関する問題のトラブルシューティング

ここでは、Emergency Responder システムの通常の操作で発生する可能性があるいくつかの問題と、Emergency Responder サーバ、グループ、およびクラスタに関連する設定画面について説明します。

症状　Emergency Responder クラスタ内のコール ルーティングが失敗するか、Emergency Responder が電話機を正しく検出しません。

推奨処置　Emergency Responder クラスタ内のすべての Emergency Responder サーバをホスト名で検出できること、およびそのすべてのサーバに他のすべての Emergency Responder サーバからネットワーク上で到達可能であることを確認します。

推奨処置　すべての Emergency Responder が Emergency Responder クラスタ DB ホストに到達可能であること、およびクラスタ DB パスワードがクラスタ内のすべてのサーバで同じであることを確認します。

症状　Emergency Responder の起動後に終了します。

考えられる原因　すでに使用中の TCP ポートを使用するように Emergency Responder を設定しました。

推奨処置　Windows Event Viewer で、「CER could not open socket at port *peer-tcp-port*, Exiting」というメッセージを確認します。このメッセージがある場合、異なる TCP ポートを使用するように Emergency Responder グループ設定を変更します。手順については、「Cisco Emergency Responder サーバ グループの設定」（P.4-22）を参照してください。

症状　[Emergency Responder Groups in Cluster] 画面がロードされず、「Cannot connect to cluster DB host」というエラーが表示されます。

推奨処置　クラスタ DB ホストをホスト名で検出できることを確認します。

指定したクラスタの db ホスト パスワードが、クラスタ内のすべての Emergency Responder サーバ グループで同じであることを確認します。

詳細については、「8.6 Cisco Emergency Responder クラスタおよびクラスタ DB ホスト」（P.4-28）を参照してください。

関連項目

- 「Cisco Emergency Responder Cluster での Cisco Emergency Responder グループおよびサーバの特定」（P.11-24）
- 「Cisco Emergency Responder サーバの起動と停止」（P.11-25）
- 「イベント メッセージの表示」（P.11-31）
- 「パフォーマンスの管理」（P.11-31）
- 「データのバックアップと復元」（P.11-33）

Cisco Unified Communications Manager の設定に関する問題のトラブルシューティング

ここでは、Emergency Responder と Cisco Unified CM との通信で発生する可能性があるいくつかの問題について説明します。緊急コールの失敗に伴うその他の問題と現象については、「緊急コールに関する問題のトラブルシューティング」（P.11-5）を参照してください。

症状　Emergency Responder が、使用するために選択したルート ポイントと CTI ポートを使用して登録されません。

推奨処置　ルート ポイントと CTI ポートが Cisco Unified CM Cisco Emergency Responder ユーザと関連付けられていることを確認します（「Cisco Emergency Responder Cisco Unified CallManager ユーザの作成」（P.3-21）を参照）。また、Cisco Unified CM サーバ上の CTI Manager（または Windows ベースの Cisco Unified CM サーバ上の DC Directory）が適切に実行されていることを確認します。

症状　Cisco Emergency Responder 設定から Cisco Unified CM を削除しようとしても削除できず、「Phone tracking in progress」というメッセージが表示されます。

推奨処置　電話機のトラッキング プロセスの進行中は、Emergency Responder 設定から Cisco Unified CM サーバを削除できません。プロセスの終了後に削除を再試行してください。

デバイスの追加後の Cisco Emergency Responder の更新

Emergency Responder で Emergency Responder クラスタを使用してプロバイダーを作成する前に、ユーザに割り当てる必要がある Emergency Responder の使用と CTI ポートおよびルート ポイントについて、Cisco Unified CM ユーザを作成する必要があります。Emergency Responder は、プロバイダーの作成時にユーザに関連付けられている CTI ポートとルート ポイントのみを登録します。したがって、Emergency Responder の起動後にユーザに追加したデバイスは、Emergency Responder によって登録されません。

Cisco Unified CM で Emergency Responder にデバイスを追加する場合、Emergency Responder で次のいずれかの技術を使用して、プロバイダーの再作成を強制的に行うことができます。

- Emergency Responder サーバを再起動します。
- Emergency Responder の設定から Cisco Unified CM サーバを削除し、再入力します。
- Emergency Responder 設定で Cisco Unified CM サーバのバックアップ CTI Manager 設定を変更し、[Update] をクリックします。この操作で、強制的にプロバイダーからログオフされ、プロバイダーが再作成されます。
- Cisco Unified CM でユーザ名を変更するか、新しいユーザを作成して、すべてのデバイスをそのユーザに関連付けます。次に、新しいユーザを使用する Emergency Responder 設定を更新します。

Cisco Emergency Responder Cluster での Cisco Emergency Responder グループおよびサーバの特定

Emergency Responder サーバの管理者のインターフェイスに接続している場合、サーバと Emergency Responder グループのスタンバイ サーバの詳細を表示するには、[System]>[Cisco ER Group Settings] を選択します。

また、Emergency Responder グループと、同じ Emergency Responder クラスタ内にある Emergency Responder サーバを特定することもできます。クラスタ内の他の Emergency Responder グループを表示するには、[System]>[Cisco ER Groups in Cluster] を選択します。[Emergency Responder Groups in Cluster] ページで、表示するグループを選択します。グループ内の Emergency Responder サーバが表示されます。これらのサーバの詳細を表示するには、サーバのいずれかで実行されている Emergency Responder Administration インターフェイスにログインし、[System]>[Cisco ER Groups in Cluster] を選択し、グループのリストから表示するグループを選択します。

Emergency Responder グループをアンインストールする必要がある場合、まずこのページを使用して Emergency Responder クラスタからグループを削除します。グループを削除するには、システム管理者としてログインする必要があります。クラスタからグループを削除すると、Emergency Responder Cluster DB からグループのエントリのみが削除されます。グループのサーバから Emergency Responder は削除されません。

関連項目

- 「Cisco Emergency Responder Server Groups in Cluster」（P.A-2）

クラスタ間の電話機の移動

次のシナリオでは、Emergency Responder クラスタの動作と、クラスタ間で移動する電話機を Emergency Responder で扱う方法について説明します。

- Server Group A（SGA）には、SGA 以外に移動する電話機（Phone_1）があります。
  - Emergency Responder は Server Group B（SGB）で Phone_1 を検出します。
  - SGA の [Unlocated Phones] ページに SGB の電話機が表示されます。
- SGB の両方の Emergency Responder サーバ（パブリッシャとサブスクライバ）が停止しても、SGA には SGB の Phone_1 が表示されたままになります。
  - このときに Phone_1 から発信されたコールは SGB にリダイレクトされ、Emergency Responder サーバがその SGB 内に存在しない場合、Emergency Responder は同じ手順を実行してこの緊急コールをルーティングします。
  - また、両方の SGB Emergency Responder サーバが停止している場合、Phone_1 は、SGB 内の他の電話機と同様に扱われます。
- Phone_1 が Server Group C（SGC）に移動した場合：
  - SGA、SGC の順で次回の増分電話機のトラッキングが実行されると検出されます。
  - [Unlocated Phones] ページでは、Phone_1 から SGC への関連付けが変更されます。
- Phone_1 が元の SGA に移動すると、次回の増分電話機トラッキングで検出され、対応するスイッチ ポートの下に表示されます。

Cisco Emergency Responder サーバの起動と停止

Emergency Responder をインストールすると、コンピュータの電源投入またはリブート時に毎回自動的に Emergency Responder サーバが設定されます。ただし、コンピュータの電源オフやリブートを使用しなくても、Emergency Responder Serviceability Web インターフェイスを介して Emergency Responder サーバの停止と再起動を行うことができます。たとえば、問題のデバッグを試みる場合にこの操作が役立つことがあります。

Emergency Responder サーバを起動または停止するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスにログインし、[Tools]>[Control Center] を選択します。

[Control Center Services] ページが開き、すべての Emergency Responder サービスとそれぞれの現在のステータスが表示されます。

ステップ 2　サービス名の左側にあるオプション ボタンをクリックし、[Start]、[Stop]、または [Restart] をクリックして、サービスで目的のアクションを実行します。最新情報で画面を更新するには、[Refresh] をクリックします。

（注）　ボタンは、そのアクションを実行可能な場合にのみ表示されます。たとえば、[Start] は、サービスが現在停止している場合にのみ表示されます。

（注）　Cisco Tomcat および Cisco IDS サービスは、Control Center から開始または停止できません。これらのサービスを開始または停止するには、**utils service** コマンドを使用します。詳細については、「utils service」（P.F-79）を参照してください。

表 11-1 では、[Control Center Services] ページに表示されるアイコンの意味について説明します。

表 11-1　Cisco Emergency Responder の Control Center のアイコン

アイコン	意味
	Emergency Responder サーバまたは Emergency Responder Phone Tracking Engine が起動し、正常に機能しています。
	管理者が Emergency Responder サーバの Emergency Responder Phone Tracking Engine を停止しました。

関連項目

- 「Control Center」（P.B-1）

ALI データのアップロードのトラブルシューティング

定期的に、ALI データを書き出し、サービス プロバイダーに送信する必要があります。ALI データは、ローカル ネットワークから正しい PSAP に緊急コールをルーティングし、緊急コールの位置に関する情報を PSAP に提供するために使用されます。

Emergency Responder では、多様な NENA 形式で ALI データを書き出すことができます。使用すべき形式については、サービス プロバイダーにお問い合わせください。

アップロード プロセス時に、一部の ALI データ レコードが正しくアップロードされないことがあります。この場合、お使いのサービス プロバイダーはエラーのリストを提供できるはずです。また、サービス プロバイダーのデータ アップロード ソフトウェアの使用時にエラーが表示される可能性もあります。誤りのあるレコードを修正し、ALI データの書き出しファイルを再送信する必要があります。レコードを修正するには、場合によってはエラーのレコードを手動で編集する必要があります。

ここでは、ALI データ レコードを修正するための一般的な手順と、多様な NENE 形式ファイルの編集方法について説明します。

- 「ALI データ レコードの修正」（P.11-26）
- 「NENA 2.0 および 2.1 ファイル形式の編集」（P.11-27）
- 「NENA 3.0 ファイル形式」（P.11-28）

ALI データ レコードの修正

ALI レコードをサービス プロバイダーにアップロードするときに表示されることがあるデータ エラーを修正するには、次の手順を実行します。

はじめる前に

NENA またはサービス プロバイダーから、NENA Doc 02-010『*Recommended Formats and Protocols for Data Exchange*』を入手してください。この文書で、さまざまな NENA 形式が詳細に説明されています。

手順

ステップ 1　エラー レポートをよく読み、発生した問題について判断します。

ステップ 2　Emergency Responder Web インターフェイスで、失敗した ERL/ALI レコードのエラーになったフィールドを変更します。たとえば、[Street Suffix] の短縮表記が受け入れられなかった場合、受け入れられる表記に変更します。すべての変更を保存します。

ステップ 3　もう一度 ALI データを書き出します（オンライン ヘルプを参照）。

ステップ 4　エラー状態にあるすべてのレコードが新規だった場合、レコードのデータベース関数を変更する必要があります。Emergency Responder ではこれらのレコードを書き出し済みなので、新規の挿入ではなく更新というラベルが付けられます。ただし、これらのレコードはアップロード時に失敗したため、サービス プロバイダーのデータベースは新規と見なします。

テキスト エディタで ALI 書き出しファイルを開き、修正するレコードの関数コードを変更します。書式設定や他の余計な文字を追加しないエディタを使用してください。ファイルの編集の詳細については、次の項を参照してください。

- 「NENA 2.0 および 2.1 ファイル形式の編集」（P.11-27）
- 「NENA 3.0 ファイル形式」（P.11-28）

ステップ 5　編集したファイルをサービス プロバイダーに送信します。

NENA 2.0 および 2.1 ファイル形式の編集

NENA 2.0 および 2.1 ファイル形式には次の特徴があります。

- レコードは固定長です。
- フィールドは特定の順序です。
- 使用しないフィールドはスペースを入力して埋めます。
- レコードの末尾にはアスタリスク（*）が示されます。

各フィールドのバイト位置と長さを決定するには、NENA Doc 02-010『*Recommended Formats and Protocols for Data Exchange*』を参照してください。ファイルを編集する場合、レコード長を長くしないでください。追加した余計なスペースは削除します。アイテムの長さがフィールドの長さ未満の場合、フィールドにスペースをパディングします。フィールドに応じて、右側または左側にパディングします。

ファイルには 1 つのヘッダーと 1 つのトレーラー レコードが含まれます。これらのレコードの間に ALI データ レコードが含まれます。

表 11-2 に、編集することが多いフィールドについて説明します。他のフィールドを変更するには、Emergency Responder Web インターフェイスを使用する必要があります。

表 11-2　NENA 2.0 および 2.1 の一般的なフィールド

フィールド	説明
Function Code	**位置**：バイト 1。 **長さ**：1 文字。 **説明**：レコードのデータベース関数。次のいずれかになります。 • **I**：新しい ALI レコードを挿入します • **C**：既存のレコードを変更します。C を使用するには、レコードのアップロードに 1 回は成功している必要があります。アップロードに成功したことがないレコードを修正する場合、C を I に変更します。 • **D**：レコードを削除します。Emergency Responder は、Emergency Responder 設定から ALI を削除した後に作成される書き出しファイルに、削除レコードを 1 回だけ生成します。レコードを再生成する必要がある場合、以前の書き出しファイルからカット アンド ペーストする（そしてレコード カウントを調整する）か、Emergency Responder で ALI を再作成し、保存してデータを書き出してから、ALI を削除し、もう一度データを書き出します。
Cycle Counter	**位置**：バイト 62 ～ 67。 **長さ**：6 文字。 **説明**：サービス プロバイダーに送信するファイルのシーケンス番号（1、2 など）。番号は右寄せにし、先頭にスペースを付加します。サービス プロバイダーによっては、このフィールドを無視することがあります。

表 11-2　NENA 2.0 および 2.1 の一般的なフィールド（続き）

フィールド	説明
Record count	**位置**：トレーラー レコードのバイト 62 ～ 70。 **長さ**：9 文字。 **説明**：サービス プロバイダーに送信するファイルに含まれるレコードの合計数（1、2 など）。数は右寄せにし、先頭にスペースを付加します。

NENA 3.0 ファイル形式

NENA 3.0 ファイル形式には次の特徴があります。

- レコードは可変長です。
- フィールドはタグとデータの組み合わせであり、任意の順序にすることができます。
- 使用しないフィールドは含まれません。タグの有無は次の影響があります。
  - タグを含めない場合、その要素の前の値が何であっても、その値は未変更のままです。
  - タグの値が空の場合、その要素の前の値は削除されます。
  - タグに空ではない値が含まれる場合、要素の値はその新しい値に変更されます。
- タグはバーティカル バー（|）で区切られます。
- レコードの末尾は事前に定義した文字で示されます。

各フィールドのタグ名と値を決定するには、NENA Doc 02-010『*Recommended Formats and Protocols for Data Exchange*』を参照してください。値がフィールドの最大長を超えないようにしてください。余計なスペースをパディングする必要はありません。

ファイルには 1 つのヘッダーと 1 つのトレーラー レコードが含まれます。これらのレコードの間に ALI データ レコードが含まれます。

表 11-3 に、編集することが多いフィールドについて説明します。他のフィールドを変更するには、Emergency Responder Web インターフェイスを使用する必要があります。

表 11-3　NENA 3.0 の一般的なフィールド

フィールド	説明
Function Code	**タグ**：FOC。 **説明**：レコードのデータベース関数。次のいずれかになります。 • **I**：新しい ALI レコードを挿入します（FOCI）。 • **C**：既存のレコードを変更します（FOCC）。C を使用するには、レコードのアップロードに 1 回は成功している必要があります。アップロードに成功したことがないレコードを修正する場合、C を I に変更します。 • **D**：レコードを削除します（FOCD）。Emergency Responder は、Emergency Responder 設定から ALI を削除した後に作成される書き出しファイルに、削除レコードを 1 回だけ生成します。レコードを再生成する必要がある場合、以前の書き出しファイルからカット アンド ペーストする（そしてレコード カウントを調整する）か、Emergency Responder で ALI を再作成し、保存してデータを書き出してから、ALI を削除し、もう一度データを書き出します。

表 11-3　NENA 3.0 の一般的なフィールド（続き）

フィールド	説明
Cycle Counter	**タグ**：CYC。 **説明**：サービス プロバイダーに送信するファイルのシーケンス番号（CYC1、CYC2 など）。サービス プロバイダーによっては、このフィールドを無視することがあります。
Record count	**タグ**：ヘッダー レコードとトレーラー レコードの REC。 **説明**：サービス プロバイダーに送信するファイルに含まれるレコードの合計数（REC1、REC2 など）。

コール履歴ログの収集

Emergency Responder では大量のコール履歴ログが保守されます。ログには処理された各緊急コールのエントリが含まれます。コール履歴情報は、管理インターフェイスとユーザ インターフェイスから表示できます。

Emergency Responder では、発信された緊急コールの履歴がデータベースに保存されます。プライマリ Emergency Responder サーバ（パブリッシャ）がアクティブではない場合、緊急コールはバックアップ Emergency Responder サーバ（サブスクライバ）によって処理されます。これら両方のサーバがアクティブになると、レプリケーションによって両方のコール履歴レコードは同期されます。そのため、コール履歴はどちらの Emergency Responder サーバでも表示できます。

コール履歴レコードをダウンロードするには、コール履歴を表示するテーブルの上部にある [Download] ボタンをクリックします。これらのレコードは Excel（.xls）形式でダウンロードできます。

トレースおよびデバッグ情報の収集

Emergency Responder で発生した問題についてシスコ テクニカル サポートに問い合わせると、トレースおよびデバッグ情報の収集が求められることがあります。

トレースおよびデバッグ情報を収集すると Emergency Responder のパフォーマンスに影響があるため、シスコから求められた場合にのみ、トレースとデバッグを有効にしてください。生成される情報は、シスコが製品の問題を解決するために使用されます。

詳細については、次の項を参照してください。

- 「トレースおよびデバッグ情報の収集」（P.11-29）
- 「syslog のイネーブル化」（P.11-31）

Cisco Emergency Responder の詳細なトレースおよびデバッグ情報のイネーブル化

Emergency Responder の詳細なトレースおよびデバッグ情報をイネーブルにするには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Web インターフェイスから、[Cisco ER Group]>[Server Settings] を選択します。

[Server Settings] ページが開きます。

ステップ 2　左側の列から、デバッグまたはトレース情報を収集する必要があるサーバを選択します。

サーバの設定が表示されます。

ステップ 3　デバッグ パッケージとトレース パッケージのセクションまでスクロールし、シスコ テクニカル サポートから求められたパッケージを選択します。

各セクションのリストは同一です。シスコから求められたリストのパッケージを選択するようにしてください。[Debug] リストで選択したパッケージでは、トレース情報と追加のデバッグ データが生成されます。シスコからすべてのパッケージを選択するように求められた場合、適切なリストで [Select All] をクリックします。

使用できるパッケージには次が含まれます。

- CER_DATABASE：データベース サブシステム。データベース アクセス コードで生成されるログ情報を含みます。
- CER_REMOTEUPDATE：リモート更新サブシステム。サーバ間の更新を管理します。
- CER_PHONETRACKINGENGINE：電話機のトラッキング サブシステム。電話機のトラッキングとスイッチ ポートおよび電話機の更新プロセスを実行します。
- CER_ONSITEALERT：オンサイト アラート担当者に通知するためのオンサイト アラート サブシステム。
- CER_CALLENGINE：コール エンジン サブシステム。コールのルーティングとプロセスを行います。
- CER_SYSADMIN：システム管理者 Web インターフェイス サブシステム。
- CER_TELEPHONY：電話機サブシステム。Cisco Unified CM とのインタラクションに使用されます。
- CER_AGGREGATOR：アグリゲータ モジュールは、電話機のトラッキング エンジンを使用したすべての Emergency Responder サーバ通信とデータ処理を対象にします。このモジュールには、クラスタ、Administration、Cisco IP SoftPhone、コール ルーティングなど、サブシステムの追跡したデータの検索とルックアップが含まれます。
- CER_GROUP：Emergency Responder サーバ グループ サブシステム。グループ内のサーバ間の通信に使用されます。
- CER_CLUSTER：サーバ クラスタ サブシステム。クラスタ内の Emergency Responder グループ間の通信に使用されます。

ステップ 4　[Update] をクリックして、変更内容の保存とアクティブ化を行います。

要求したトレースおよびデバッグ情報の生成が開始されます。

（注）　Emergency Responder のトレースは、Emergency Responder Serviceability Web インターフェイスまたは CLI を使用して収集できます。

ステップ 5　デバッグおよびトレース情報の収集を完了したら、デバッグとトレースを無効にする選択を行ったセクションごとに、[Clear All] をクリックします。次に [Update] をクリックして変更を完了します。

関連項目

- 「Server Settings for Emergency ResponderServerGroup」（P.A-7）
- 付録 B「Cisco Emergency Responder のサービスアビリティ Web インターフェイス」
- 付録 F「コマンド ライン インターフェイス」

syslog のイネーブル化

トレースおよびデバッグ情報を収集するには、Emergency Responder の syslog をイネーブルにする必要があります。

Emergency Responder の syslog をイネーブルにするには、「syslog からの情報収集」（P.11-33）を参照してください。

イベント メッセージの表示

Emergency Responder Serviceability Web インターフェイスを使用して Emergency Responder イベント メッセージを確認すると、ソフトウェアの問題の診断に役立ちます。

Emergency Responder イベントの表示については、「Event Viewer の使用」（P.6-2）を参照してください。

[Find and List Events] ページの詳細については、「Event Viewer」（P.B-2）を参照してください。

パフォーマンスの管理

サポートされる Cisco MCS Unified CM Appliance プラットフォームとその Emergency Responder のスケーラビリティについては、『*Release Notes for Cisco Emergency Responder 8.6*』を参照してください。

Emergency Responder が WAN リンクのスイッチを管理している場合、Emergency Responder パフォーマンスに影響が出ることがあります。Emergency Responder は必ず管理対象のスイッチに SNMP 要求を送信するため、WAN の遅延が SNMP タイムアウトの原因になり、電話機とスイッチの変更を追跡するために必要な時間が増える可能性があります。場合によっては、SNMP パラメータの調整が必要です。詳細については、「SNMP 接続の設定」（P.4-45）を参照してください。

ネットワーク管理システムとの統合

CiscoWorks2000 または他の SNMP ベースのネットワーク管理システムを使用して、Emergency Responder サーバのステータスをリモート管理できます。CiscoWorks2000 は標準のシスコ ネットワーク管理システムですが、Emergency Responder には付属していません。CiscoWorks2000、Campus Manager、および Topology Service の詳細については、次の URL にあるマニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/netmgtsw/tsd_products_support_category_home.html

次のトピックでは、Emergency Responder をネットワーク管理システムと統合するときに役立つ情報について説明します。

- 「CDP サポートの概要」（P.11-32）

CDP サポートの概要

Cisco Emergency Responder では、アクティブなインターフェイスで、指定したマルチキャスト アドレス宛てに、Cisco Discovery Protocol（CDP）を使用して、CDP メッセージを定期的に送信します。これらのメッセージには、デバイスの識別、インターフェイス名、システム機能、SNMP エージェント アドレス、存続可能時間などの情報が含まれます。CDP をサポートするすべてのシスコ デバイスは、この定期的なメッセージをリッスンして、Cisco Emergency Responder サーバの位置を確認できます。

CiscoWorks2000 Server は、CDP を介して提供された情報を使用して、Cisco Emergency Responder サーバ、Campus Manager アプリケーション、および Topology Service を検出し、Cisco Emergency Responder サーバを表示するトポロジ マップを構築できます。

Cisco Emergency Responder サーバは、CDP メッセージの送出に加え、CDP をサポートする電話機の位置確認に CDP を使用します。Cisco Emergency Responder で、スイッチに対する SNMP クエリーを介してこの情報を入手できるように、スイッチで CDP をイネーブルにする必要があります。

表 11-4 に、Cisco Emergency Responder ハードウェア プラットフォームの SNMP OID を示します。

表 11-4　Cisco Emergency Responder ハードウェア プラットフォームの OID

ハードウェア プラットフォーム	SNMP OID
Cisco MCS-7815-I	1.3.6.1.4.1.9.1.582
Cisco MCS-7825-H	1.3.6.1.4.1.9.1.583
Cisco MCS-7825-I	1.3.6.1.4.1.9.1.746
Cisco MCS-7835-H	1.3.6.1.4.1.9.1.584
Cisco MCS-7835-I	1.3.6.1.4.1.9.1.585
Cisco MCS-7845-H	1.3.6.1.4.1.9.1.586
Cisco MCS-7845-I	1.3.6.1.4.1.9.1.587

Cisco Emergency Responder サブシステムのステータスの監視

Cisco Emergency Responder は SYSAPPL-MIB をサポートします。SYSAPPL-MIB を使用すると、CiscoWorks2000 またはサードパーティの SNMP ブラウザから次の Cisco Emergency Responder コンポーネントに関する情報にリモート アクセスできます。

- Cisco Emergency Responder Server
  - CERServer.exe
- Cisco PhoneTrackingEngine
  - CERPhoneTracking.exe
- MSQL Server 関連のサービス

SYSAPPL-MIB は SNMP を使用します。Emergency Responder は次の SYSAPPL-MIB テーブルをサポートします。

- SysApplInstallPkgTable：メーカー、製品名、インストールされているバージョン、インストールした日付、位置などのアプリケーション情報を提供します。これは、関連する [Application Administration Web] ページ（適用される場合）にアクセスする部分 URL です。
- SysApplRunTable：アプリケーションの起動時間と実行時のステータスが記述されます。
- SysApplInstallElmtTable：個々のアプリケーション要素、または関連する実行可能要素が記述されます。これは SysApplInstallPkgTable に定義されているアプリケーションから構成されます。
- SysApplElmtRunTable：ホスト システムで現在実行されているプロセス、または実行可能要素が記述されます。

syslog からの情報収集

Cisco Syslog Collector を使用するように Emergency Responder を設定できます。Cisco Syslog Collector と Cisco Syslog Analyzer は、Resource Management Essentials パッケージの一部として、CiscoWorks2000 と共に提供されます。また、Emergency Responder からの syslog の出力を採用して、他のネットワーク管理システムに使用することもできます。

Cisco Syslog Collector は、Emergency Responder にレポートされるメッセージの共通システム ログを保守します。

Cisco Syslog Analyzer は、すべてのイベントを効率的に制御および表示するため、読み取りや解釈が容易で、システム メンテナンスと問題解決にも簡単に利用できます。

Cisco Syslog Collector のインストールと設定については、CiscoWorks2000 のマニュアルを参照してください。

syslog をイネーブルにするには、次の手順を実行します。

手順

ステップ 1　[System]>[Cisco ER Group Settings] を選択します。

[Emergency Responder Group Settings] ページが開きます。

ステップ 2　[Enable Syslog] で [enable] を選択します。

ステップ 3　[Syslog Server] フィールドにサーバの完全修飾 DNS 名を入力します（server.domain.com など）。

ステップ 4　[Update Settings] をクリックして、変更を保存します。

直後に、syslog へのメッセージの書き込みが開始されます。

関連項目

- 「Cisco Emergency Responder Group Settings」（P.A-3）

データのバックアップと復元

Emergency Responder 8.6 は、システム データのバックアップと復元に Disaster Recovery System を使用します。

Disaster Recovery System の使用方法については、第 8 章「Cisco Emergency Responder 8.6 Disaster Recovery System の設定」を参照してください。

関連項目

- 「コール履歴ログの収集」（P.11-29）

Data Migration Assistant のトラブルシューティング

Data Migration Assistant（DMA）は 2 つのフェーズで動作します。第 1 フェーズの Database では、次のフォルダが tar ファイルにバックアップされます。

- export
- import
- etc
- nena_msag_records

第 2 フェーズでは、バックアップ Emergency Responder データベースのコンテンツが、Emergency Responder 8.6 データベース スキーマに対して検証されます。

症状　DMA のバックアップと検証に失敗しました。

推奨処置　次のチェック リストを確認します。

- MSDE が実行されているかどうかを確認します。データベースが実行されていない場合、バックアップは成功しません。
- バックアップ対象のノードが Sbscriber ノードではなく Publisher ノードであることを確認します。Subscriber ノードでは DMA バックアップを実行できません。
- CSA が実行されていないことを確認します。CSA が実行されている場合、停止してからバックアップを開始します。

症状　DMA のバックアップは成功しますが、検証に失敗します。

推奨処置　次のチェック リストを確認します。

- CSA が実行されていないことを確認します。CSA が実行されている場合、停止してからバックアップを開始します。CSA が DMA 操作に干渉します。
- 以降の分析ついて、データ検証ログを収集します。この場合、Emergency Responder 8.6 へのマイグレートが成功するには、場合によってはデータベースに含まれるデータを事前に変更する必要があります。

DMA ログは次の場所にあります。

- exportdb.log および migratecCERCSV.log は C:¥CiscoWebs¥DMA¥Bin にあります
- installdbw1.log、installdbw1.log.err、installdbccm.log、installdbccm.log.err、および dbl_INSTALLDBxxxxxx.txt は C:¥Program Files¥Cisco¥Trace¥DBL にあります
- ログ ファイルは C:¥Program Files¥Cisco¥Trace¥DMA にあります

検証ログ ファイルは次のとおりです。

- exportdb.log
- installdbw1.log
- installdbw1.log.err

- dbl_INSTALLEDBxxxxxx.txt

Linux アップグレードのトラブルシューティング

Emergency Responder 8.6 の今後のバージョンにアップグレードする場合、特定の問題が発生することがあります。ここでは、このような問題の原因と推奨されるアクションについて説明します。

症状　[Install / Upgrade] メニューの最初のページでアップグレード パッチの詳細を入力した後に、「No valid upgrade options found」というエラー メッセージが表示されます。

推奨処置　パブリッシャのアップグレード前に、サブスクライバはアップグレードしないでください。Emergency Responder サーバ グループのアップグレード時には、必ずパブリッシャからアップグレードします。

推奨処置　実際に指定したローカルまたはリモート パスに、有効で署名付きの ISO イメージが含まれ、拡張子が .sgn.iso であることを確認します。

症状　[Install / Upgrade] メニューの最初のページでリモートの場所にあるアップグレード パッチの詳細を入力すると、「Incorrect user name/password」というエラー メッセージが表示されます。

推奨処置　リモートの SFTP/FTP の場所について入力したユーザ名とパスワードが正しいことを確認します。

症状　ISO イメージを Emergency Responder サーバにダウンロードしましたが、チェックサム値が一致しません。

推奨処置　Cisco.com から新しく ISO イメージをダウンロードし、もう一度アップグレードを試行します。

症状　アップグレードはキャンセルされましたが、システムをリブートするように求める警告メッセージが表示されます。

推奨処置　アップグレード時に、Emergency Responder サーバ上の特定のサービス（アップグレードがキャンセルされたタイミングによって決まります）が停止した可能性があります。この場合、サーバをリブートすることが強く推奨されます。

CHAPTER 12

ALI フォーマット ツールの使用

次のトピックでは、自動ロケーション情報（ALI）フォーマット ツール（AFT）について説明した後、AFT の使用方法およびトラブルシューティング方法に関する情報を提供します。

ネットワーク エンジニア、システム管理者、および通信エンジニアは、これらのトピックを確認して、AFT の使用およびトラブルシューティングに必要な手順を習得してください。AFT を配置する前に、Cisco Emergency Responder（Emergency Responder）および
Cisco Unified Communications Manager（Cisco Unified CM）に精通するようにしてください。

サービス プロバイダー固有の情報については、付録 G「特定のサービス プロバイダーに対する AFT の使用」を参照してください。

ALI フォーマット ツールの概要

Emergency Responder は、テレフォニー ネットワーク内での緊急コールの管理に役立ちます。Emergency Responder は、システムの電話機およびロケーションを追跡し、これらの情報を National Emergency Number Association（NENA）2.0、2.1、および 3.0 形式に準拠した ALI レコードでエクスポートします。ただし、多くのサービス プロバイダーは NENA 標準を使用しません。AFT を使用すると、Emergency Responder で作成した ALI レコードを、サービス プロバイダーで使用されている形式と互換性のある形式に変更できます。これにより、サービス プロバイダーは、その再フォーマットされたファイルを使用して自身の ALI データベースを更新します。

AFT は Emergency Responder で生成された ALI ファイルを読み取り、AFT の Web ページにすべての ELIN レコードを表示します。AFT を使用して、次のことができます。

- ALI レコードの詳細を簡単に表示する。ALI ファイルは、NENA の固定長形式での読み取りが困難です。AFT は ALI ファイルを読み取り、読み取りが容易なインターフェイスで NENA フィールドを提供します。
- レコードを選択し、ALI フィールドの値を更新する。AFT では、ALI フィールドを編集して、さまざまなサービス プロバイダーの要件を満たすようにカスタマイズできます。これにより、サービス プロバイダーは、再フォーマットされた ALI ファイルを読み取り、そのファイルを使用して ELIN レコードを更新できます。
- 複数の ALI レコードに対するバルク更新を実行する。バルク更新機能を使用すると、選択したすべてのレコード、1 つのエリア コード、または 1 つのエリア コードと 1 つのシティ コードに対して共通の変更を適用できます。

- エリア コード、シティ コード、または 4 桁のディレクトリ番号に基づいて、ALI レコードを選択的にエクスポートする。たとえば、あるエリア コードのすべての ALI レコードを選択してエクスポートすることにより、各サービス プロバイダーのすべての ELIN レコードにすばやくアクセスできるため、複数のサービス プロバイダーを簡単にサポートできます。

ALI フォーマット ツールを使用したファイルの生成

ここでは、ALI フォーマット ツール（AFT）の使用方法について説明します。

• ALI フォーマット ツールのインターフェイスの使用

• AFT を使用したフォーマット済み ALI ファイルの生成

ALI フォーマット ツールのインターフェイスの使用

AFT を使用して、次のフィールドを編集できます。

- ヘッダー フィールドとトレーラ フィールド。ALI フォーマット ツール（AFT）は、すべての ALI レコード データを [ALI] タブに表示します。ALI ファイルは、1 つのヘッダー レコードと 1 つのトレーラー レコードのみで構成されています。ELIN レコードごとの個別のヘッダー レコードやトレーラー レコードは存在しません。
- [Function/Transaction Code] フィールド。
- サービス プロバイダー固有のフィールド。

AFT では、次のフィールドは編集できません。

- Emergency Responder を通して設定および編集する ALI レコード フィールド。これらは AFT では無効になっています。
- レコード カウント フィールド。AFT は、この数値をエクスポート用に選択されたレコード数に基づいて内部で計算するため、このトレーラ フィールドは編集できません。

表 12-1 に、AFT インターフェイスを使用して主な AFT 作業を実行する方法を示します。

表 12-1　AFT インターフェイスを使用した主な作業の実行

作業	手順	注
サービス プロバイダー用の AFT を開く。	[Tools]>[ALI Formatting Tool] の順に選択します。プルダウン メニューのサービス プロバイダーの名前をクリックします。	適切な特権を使用して Emergency Responder Administration Web サイトにログインする必要があります。
NENA ファイルを AFT への入力として指定する。	プルダウン メニューに表示されるファイルのリストから、AFT の入力ファイルを選択します。	NENA ファイルが表示されない場合は、[Tools]>[Export PS-ALI Record] を選択して、NENA 2.0 ファイルをエクスポートします。
特定の ELIN 番号を選択する。	AFT への入力として指定された NENA ファイル内のすべての ELIN が表示されます。特定の ELIN に絞り込むには、ELIN の検索を実行します。	

表 12-1　AFT インターフェイスを使用した主な作業の実行（続き）

作業	手順	注
ELIN に対する ALI の詳細を表示する。ELIN を選択してその ALI フィールドを編集する。	各 ELIN はリンクです。特定の ELIN リンクをクリックして、そのレコードを表示します。ELIN の詳細が画面の右側に表示されます。	その後、ALI の編集可能フィールドに新しい値を入力して ALI レコードを編集できます。
ALI ファイルに対するバルク更新を実行する。	バルク更新を実行する ELIN を選択します。ELIN のリストの上にある [Bulk Update] ボタンをクリックします。	
変更を確認する。	何らかの変更を行ったら、[Review Changes/Generate File] ボタンをクリックします。 変更されたすべての ELIN のリストが表示されます。	[Review Changes/Generate File] ページで [ELIN] リンクをクリックして、変更された情報を表示します。
ヘッダー レコードを表示または編集する。	[ALI Record Details for ELIN] ページでいずれかの ELIN を選択し、[Header Record] リンクをクリックします。 これで、ヘッダー レコードの編集可能フィールドを編集できます。	ヘッダー レコードは ALI ファイルに共通であり、ELIN に固有ではありません。
トレーラー レコードを表示または編集する。	[ALI Record Details for ELIN] ページでいずれかの ELIN を選択し、[Trailer Record] リンクをクリックします。 これで、トレーラー レコードの編集可能フィールドを編集できます。	トレーラー レコードは ALI ファイルに共通であり、ELIN に固有ではありません。
ELIN を追加する。	[Review Changes/Generate File] ページで、[Add More ELIN(s)] ボタンをクリックします。 変更されていない ELIN のリストが表示されます。最終的に生成されるファイル内に保持する ELIN を選択します。	

表 12-1　AFT インターフェイスを使用した主な作業の実行（続き）

作業	手順	注
ELIN を削除する。	[Review Changes/Generate File] ページで、削除する ELIN を選択し、[Remove ELIN(s)] ボタンをクリックします。	このレコードに対して行われた変更は失われ、この ELIN が、変更されていない ELIN のプールに追加されます。
フォーマット済みファイルを生成する。	[Review Changes/Generate File] ページで、次の手順を実行します。 1. フォーマット済みファイルに含める ELIN を選択します。 2. 生成するフォーマット済みファイルの名前を入力します。 3. [Generate File] ボタンをクリックします。	フォーマット済みファイルが正常に生成された後、そのファイルをダウンロードできます。 そのファイルを後でダウンロードする場合は、次の手順を実行します。 1. [Tools]>[File Management Utility] の順に選択します。 2. 検索パラメータで [ALI Formatting Tool] を選択した後、サービス プロバイダーを選択します。フォーマット済みファイルが表示されます。 3. フォーマット済みファイルを選択し、[Download] をクリックします。

フォーマット済み ALI ファイルの生成

AFT を使用してフォーマット済みファイルを生成するには、次の手順を実行します。

手順

ステップ 1　次の手順を実行して、Emergency Responder で生成された NENA 2.0 ファイルを AFT への入力として指定します。

a. Emergency Responder Administration Web ページから、[Tools]>[ALI Formatting Tool] の順に選択します。

b. メニューのサービス プロバイダー名をクリックします。

c. プルダウン メニューに表示されるファイルのリストから、ALI フォーマット ツールの入力ファイルを選択します。

AFT により、NENA ファイルのすべての ELIN が表示されます。

ステップ 2　ALI ファイルの詳細を表示するには、[ELIN] リンクをクリックします。画面の右側の [ALI Record Details for ELIN] に情報が挿入されます。

ステップ 3　編集可能なフィールドに新しい値を入力して、ALI フィールドを編集します。

ステップ 4　サービス プロバイダーにエクスポートする ELIN を、画面の左側にある対応するチェックボックスをオンにすることによって選択します。

ステップ 5　AFT でサービス プロバイダーのフィールドを更新します。

必要なサービス プロバイダー固有の情報の詳細については、付録 G「特定のサービス プロバイダーに対する AFT の使用」を参照してください。

ステップ 6　この時点で、多数の ELIN の一部のフィールドを同時に編集する場合は、AFT のバルク更新機能を使用できます。これを行うには、次の手順を実行します。

a. バルク更新を使用して編集する ELIN を選択します。

b. [Bulk Update] ボタンをクリックします。[Bulk Update] フォームが表示されます。

c. 必要なサービス プロバイダー固有の情報の詳細については、付録 G「特定のサービス プロバイダーに対する AFT の使用」を参照してください。

ステップ 7　次の手順を実行して、フォーマット済みファイルを生成します。

a. [Review Changes/Generate File] ボタンをクリックします。

編集された ELIN のリストが表示されます。変更されていない ELIN を追加したり、編集された ELIN をリストから削除したりすることができます。

b. 最終的なフォーマット済みファイルに含める ELIN を選択し、そのフォーマット済みファイルの名前を入力します。

c. [Generate File] をクリックして、ファイルを生成します。

AFT によって、ALI ファイルがサービス プロバイダーに固有の形式で生成され、その同じファイルをダウンロードするよう求められます。

（注）　フォーマット済みファイルを生成する前に、入力した詳細を確認してください。

ステップ 8　サービス プロバイダーから推奨されたファイルの送信方法を使用して、その ALI ファイルをサービス プロバイダーに送信することにより、サービス プロバイダーがその AFT ALI ファイルの ELIN で E911 データベースを更新できるようにします。

（注）　その AFT ALI ファイルのコピーを控えとして保存するようにしてください。これは、サービス プロバイダーからエラーが報告された場合に役立ちます。AFT フォーマットのすべての変更をやり直すことなく、ファイルに必要な変更を加えることができます。

ステップ 9　サービス プロバイダーから ALI ファイルのステータスが返されます。

サービス プロバイダーからエラーは存在しないと報告された場合は、そのまま AFT を使用して、さらにフォーマット済みのレコードを生成することも、プログラムを終了することもできます。

サービス プロバイダーから ALI エラーが報告された場合は、次の手順を実行します。

a. サービス プロバイダーに送信したフォーマット済みファイルを修正します。サービス プロバイダーのエラー コードはすべて、そのサービス プロバイダーの ALI フォーマットのマニュアルで定義されています。そのマニュアルを参照してファイル内のエラーを特定し、AFT を使用してエラーを修正します。

（注）　AFT を使用して編集できないフィールドでエラーが発生した場合は、Emergency Responder を使用してそのフィールドを修正する必要があります。訂正後、AFT を使用してファイルを再生成します。

b. 修正されたファイルをサービス プロバイダーに送信します。記録として、訂正したファイルのコピーを保存しておいてください。

c. サービス プロバイダーがフォーマット済みのファイルを読み取って、ELIN レコードの更新に使用できるようになるまでこのプロセスを繰り返します。

関連項目

- 「ALI データの変換」（P.4-38）
- 「ALI Formatting Tool」（P.A-80）

APPENDIX A

Cisco Emergency Responder の管理 Web インターフェイス

次のトピックで、Cisco Emergency Responder（Emergency Responder）管理者の Web インターフェイスのページ フィールドについて説明します。

Cisco Emergency Responder Server Groups in Cluster

[System]>[Cisco Emergency Responder Groups in Cluster] を選択すると、[Emergency Responder Server Groups in Cluster] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者、ERL 管理者、またはネットワーク管理者の権限が必要です。

説明

[Emergency Responder Server Groups in Cluster] ページは、Emergency Responder を構成する Emergency Responder グループを表示するために使用します。クラスタ内の各 Emergency Responder グループに属している Emergency Responder サーバを表示することができます。Emergency Responder クラスタ内のリモート サーバ グループのリンクをクリック（プライマリ サーバとバックアップ サーバのどちらかを選択）すれば、それらのサーバの Emergency Responder インターフェイスに直接移動することができます。

表 A-1 に、[Emergency Responder Server Groups in Cluster] ページの説明を示します。

表 A-1　[Cisco Emergency Responder Server Groups in Cluster] ページ

フィールド	説明	注
Emergency Responder Groups		
Emergency Responder Groups list	同じクラスタ データベース ホストを指している Emergency Responder サーバ グループのリスト。 グループ名をクリックすると、そのグループ内のサーバが表示されます。	Emergency Responder クラスタは、Emergency Responder グループのこのセットで構成されます。Emergency Responder サーバのインストール時にクラスタを作成します。「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）を参照してください。
Servergroup Details		
Emergency Responder Group Name	サーバ グループの名前。	サーバ グループ名をクリックすると、[Servergroup Details] ページ セクションにそのグループ内のサーバが表示されます。
Primary Host Name	グループ内のプライマリ サーバの DNS ホスト名または IP アドレス。	このホスト名（ローカル サーバ グループ以外）をクリックすると、そのサーバの Emergency Responder 管理ページが新しいウィンドウで開きます。
Standby Host Name	グループ内のスタンバイ サーバまたはバックアップ サーバの DNS ホスト名または IP アドレス。	このホスト名（ローカル サーバ グループ以外）をクリックすると、そのサーバの Emergency Responder 管理ページが新しいウィンドウで開きます。
[Delete] ボタン	表示している Emergency Responder グループを Emergency Responder クラスタから削除するには、[Delete] をクリックします。	クラスタから Emergency Responder グループを削除できるのはシステム管理者だけです。 Emergency Responder グループをアンインストールする前にクラスタからグループを削除します。

関連項目

- 「Cisco Emergency Responder Cluster での Cisco Emergency Responder グループおよびサーバの特定」（P.11-24）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Cisco Emergency Responder Group Settings

[System]>[Cisco ER Group Settings] を選択すると、[Emergency Responder Group Settings] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Emergency Responder Group Settings] ページは、Emergency Responder サーバ グループの運用特性を定義するために使用します。

表 A-2 に、[Emergency Responder Server Group Settings] ページの説明を示します。

表 A-2　[Cisco Emergency Responder Group Settings] ページ

フィールド	説明	注
Emergency Responder Group Name	サーバ グループの名前。この名前は情報としてしか使用されないため、わかりやすい名前にしてください。	
Peer TCP Port	サーバ グループ内の Emergency Responder サーバ間の通信に使用される TCP ポート。デフォルト ポートを使用しない場合は、未使用ポートが選択されていることを確認してください。	範囲は 1024 ～ 65535 です。
Heartbeat Count	Emergency Responder サーバが、応答しない Emergency Responder サーバを使用不可と見なすまでのカウント数。	デフォルトのカウント数は 3 です。範囲は 3 ～ 10 です。 カウント間の時間は [Heartbeat Interval] で定義されます。
Heartbeat Interval	サーバ グループ内の他の Emergency Responder サーバにハートビート メッセージを送信する時間間隔（秒数）。	デフォルトは 30 秒です。範囲は 30 ～ 300 秒です。
Active Call Timeout	PSAP が緊急通報者に電話をかけ直すことができるように、コール ルート マッピングを保存しておく時間。	デフォルトは 180 分（3 時間）です。範囲は 30 ～ 1440 分です。
SMTP Mail Server	メール サーバの IP アドレスまたは完全修飾名（email.domain.com など）。	緊急コールの受信時に Emergency Responder から警備員に電子メールまたは電子メールベースのページを送信する場合は、電子メール サーバを設定します。
Source Mail ID	メール サーバを設定する場合は、電子メールの送信に使用可能なサーバ上の電子メール アカウントを入力する必要があります。	警備員に送信される電子メールまたはページは、この電子メール アカウントから配信されます。
System Administrator Mail ID	Emergency Responder からシステムに関する重要情報が送信されるメール アカウント。	Emergency Responder からシステム管理者に送信される電子メールまたはページは、この電子メール アカウントに送信されます。
Enable Calling Party Modification	発信者番号の動的変更。1 つのルート パターンに対して複数の ELIN 番号を設定することによって、ルート パターンの数を減らすことができます。ELIN 番号は一意にする必要があります。	Cisco Unified CM 4.0 以降と Emergency Responder 1.2(2) 以降で使用することができます。 Emergency Responder を Cisco Unified CM ユーザとして作成したときに、発信者変更をイネーブルにした場合は、このフラグをセットする必要があります。
Syslog	CiscoWorks2000 Syslog Collector へのログ メッセージの書き込みをイネーブル/ディセーブルにするプルダウン メニュー。	
Syslog Server	CiscoWorks2000 Resource Manager Essentials Syslog Collector を実行しているサーバの名前。 サーバの完全修飾された DNS 名（cw2k.domain.com など）を入力します。	[Enable Syslog] を選択した場合は、サーバ名を入力するだけで済みます。
注	サーバ グループの使用目的を明確にするために入力するメモ。	

表 A-2　[Cisco Emergency Responder Group Settings] ページ（続き）

フィールド	説明	注
Dynamic Tracking of Switch IP Address	Emergency Responder でホスト名を使用して設定された LAN スイッチの IP アドレスを動的に更新します。	このアクションは、IP アドレスを使用して Emergency Responder に追加された LAN スイッチには適用されません。
Security end user web interface language	ユーザ Web ページに表示される言語を選択可能なプルダウン メニュー（[English] または [French (Canadian)]）。	言語を変更したら、次の作業を完了しないと、その言語がユーザ Web ページに表示されません。 • [Tools]>[Control Center] を選択して、Emergency Responder Serviceability で Emergency Responder サービスを再起動します。 • CLI コマンドの **utils service restart Cisco Tomcat** を使用して Cisco Tomcat サービスを再起動します。 • 現在の Emergency Responder ユーザ Web ページを更新します。
Limit Concurrent Sessions	ユーザ単位の同時セッション数を制限します。	このチェックボックスをオン / オフすると、[Max. number of concurrent sessions] ドロップダウン ボックスがイネーブル / ディセーブルになります。
Max. number of concurrent sessions	[Limit Concurrent Sessions] がイネーブルになっている場合は、この制限がすべてのユーザに適用されます。	この制限は、各 Emergency Responder Web サイトに対して個別に強制されます。 • Emergency Responder Administration • Emergency Responder Serviceability • Emergency Responder User • Emergency Responder Admin Utility
[Update Settings] ボタン	変更を保存してアクティブにするには、[Update Settings] をクリックします。	
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	

関連項目

- 「Cisco Emergency Responder サーバ グループの設定」（P.4-22）
- 「syslog からの情報収集」（P.11-33）
- 「同時セッション数の制限」（P.4-20）
- 「スイッチ IP アドレス変更の動的なトラッキング」（P.4-53）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Telephony Settings

[System]>[Telephony Settings] を選択すると、[Telephony Settings] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Telephony Settings] ページは、Emergency Responder グループによって使用される電話番号とテレフォニー ポートを定義するために使用します。

表 A-3 に、[Telephony Settings] ページの説明を示します。

表 A-3　[Telephony Settings] ページ

フィールド	説明	注
Specify telephony attributes		
Route Point for Primary Emergency Responder Server	プライマリ サーバで使用すべき CTI ルート ポイント（911 など）。	詳細については、「緊急コールのルート ポイントの作成」（P.3-6）を参照してください。
Route Point for Standby Emergency Responder Server	スタンバイ サーバで使用すべき CTI ルート ポイント（912 など）。この番号は、プライマリ緊急番号のコール転送番号として設定します。	詳細については、「緊急コールのルート ポイントの作成」（P.3-6）を参照してください。
PSAP Callback Route Point Pattern	Public Safety Answering Point（PSAP; 緊急応答機関）からのコールを受信するように定義した CTI ルート ポイント。たとえば、913XXXXXXXXXX（913 + 10 個の X）と入力します。 この番号は、数字と X のみで構成する必要があります。	詳細については、「緊急コールのルート ポイントの作成」（P.3-6）を参照してください。
ELIN Digit Strip Pattern	[PSAP Callback Route Point Pattern] の値の先頭から除外する数字（913 など）。パターンから除外する数字は、PSAP でネットワークへのコールに使用可能な ELIN 番号にする必要があります。	この文字列は、[PSAP Callback Route Point Pattern] の一部である必要があります。
UDP Port Begin	登録中に CTI ポートで使用されるポート番号。	範囲は 1024 ～ 65535 です。
Inter Emergency Responder Group Route Pattern	他の Emergency Responder グループがこのグループに緊急コールをルーティングするために使用するルート パターン（1000.911 など）。 このパターンは、数字とドットのみで構成する必要があります。	この番号の詳細については、「Cisco Emergency Responder グループ間の通信に対するルート パターンの作成」（P.3-19）を参照してください。
IP Type of service (00-FF)	IP ヘッダー内の Type Of Service（TOS; タイプ オブ サービス）バイトの値。デフォルトの 0xB8 は、プライオリティ キューの TOS クラスを意味します。このデフォルト値は Emergency Responder 用として使用することをお勧めします。	ここで入力した TOS 値は、Emergency Responder からオンサイト音声アラート機能に送信される RTP パケットにのみ適用されます。
Onsite Alert Prompt Repeat Count	オンサイト アラート電話機でプロンプトが再生される回数。	

表 A-3　[Telephony Settings] ページ（続き）

フィールド	説明	注
Use IP Address from call signaling	このパラメータがイネーブルになっている場合は、Emergency Responder が JTAPI から電話機の IP アドレスを取得します。このパラメータはコールのルーティングに使用されます。つまり、IP サブネットが電話機用に設定されている場合は、このパラメータ設定が他のどの手動設定より優先されます。 このパラメータがディセーブルになっている場合は、Emergency Responder が電話機の手動設定を使用してコールをルーティングします。	このフィールドは、Emergency Responder が Cisco Unified Communications Manager 6.x 以降を使用して設定されている場合のみ適用されます。
[Update Settings] ボタン	変更を保存してアクティブにするには、[Update Settings] をクリックします。	
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	
Intrado Route Pattern Settings		
Intrado Route/Translation Pattern	Intrado Emergency Response Location（ERL; 緊急応答ロケーション）のルート パターン / トランスレーション パターンを入力します。Intrado ERL は Intrado から提供される ERL です。Intrado ERL には、このページ上で設定されたルート パターンのみが表示されます。新しいルート パターン / トランスレーション パターンを追加することも、既存のルート パターン / トランスレーション パターンを更新または削除することもできます。	新しいルート パターンまたはトランスレーション パターンを追加するには、テキスト ボックスをクリックして、数字とワイルドカード（スペースは使用不可）を含むルート パターンを入力し、[Add] をクリックします。 既存のルート パターンを更新するには、該当するルート パターンをクリックして、パターンを変更し、[Update] をクリックします。 既存のルート パターンを削除するには、該当するルート パターンをクリックして、[Remove] をクリックします。 既存の変更をキャンセルして最後に保存された設定値に戻すには、[Cancel Changes] をクリックします。

関連項目

- 「Cisco Emergency Responder サーバのグループ テレフォニー設定」（P.4-23）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Server Settings for Emergency ResponderServerGroup

[System]>[Server Settings] を選択すると、[Server Settings for Emergency ResponderServerGroup] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

Emergency Responder サービスが開始されると、Emergency Responder サーバが Emergency Responder グループに追加されます。(「新しいシステムへの Cisco Emergency Responder 8.6 のインストール」（P.2-14）を参照)。

[Server Settings for Emergency ResponderServerGroup] ページは、サーバ設定を更新する、たとえば、サーバ名を変更したり、トレース/デバッグ設定を変更したり、サーバを削除したりするために使用します。

（注）　サーバのホスト名は変更することができません。

表 A-4 に、[Server Settings Emergency ResponderServerGroup] ページの説明を示します。

表 A-4　[Server Settings for the Emergency ResponderServerGroup] ページ

フィールド	説明	注
Status	[Server Settings Emergency ResponderServerGroup] ページのステータスが表示されます。	
Select Server		
Server	すでに作成されたサーバのリスト。サーバ名をクリックすると、そのサーバの設定が表示されます。	サーバ グループ当たり最大 2 つのサーバを設定することができます。
Modify Server Settings		
Server Name	サーバの名前。	この [Server Name] フィールドを必要な値に変更します。
Host Name	Emergency Responder サーバの DNS 名。	このフィールドは変更することができません。
[Debug Package] リスト	詳細なデバッグ情報を収集するサブシステムの選択肢。デバッグ情報には、トレース メッセージだけでなく、より詳細なメッセージも含まれています。シスコのテクニカル サポートから要求された場合にのみサブシステムを選択します。デバッグ情報は、シスコがお客様の問題解決を支援するために使用するものです。	各フィールドの説明については、「トレースおよびデバッグ情報の収集」（P.11-29）を参照してください。
[Select All] ボタン	[Debug Package] リスト内のすべてのサブシステムを選択します。	
[Clear All] ボタン	[Debug Package] リストで選択されているすべてのサブシステムをクリアします。	
[Trace Package] リスト	簡易なトレース情報を収集するサブシステムの選択肢。シスコのテクニカル サポートから要求された場合にのみサブシステムを選択します。トレース情報は、シスコがお客様の問題解決を支援するために使用するものです。 デバッグ用のサブシステムを選択した場合は、トレース用のサブシステムを選択する必要がありません。	各フィールドの説明については、「トレースおよびデバッグ情報の収集」（P.11-29）を参照してください。
[Select All] ボタン	[Trace Package] リスト内のすべてのサブシステムを選択します。	
[Clear All] ボタン	[Trace Package] リストで選択されているすべてのサブシステムをクリアします。	

表 A-4　[Server Settings for the Emergency ResponderServerGroup] ページ（続き）

フィールド	説明	注
[Update Settings] ボタン	設定に加えた変更を保存するには、既存のサーバの設定が表示されているときに [Update] をクリックします。	既存のサーバの設定が表示されている場合にのみ使用することができます。
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	

関連項目

- 「Cisco Emergency Responder サーバの設定」（P.4-25）
- 「トレースおよびデバッグ情報の収集」（P.11-29）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

License Manager

[System]>[License Manager] を選択すると、[License Manager] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[License Manager] ページは、サーバ グループのライセンスの詳細を表示したり、サーバ グループのライセンス ファイルをアップロードしたりするために使用します。Emergency Responder 8.6 のライセンス要件の詳細については、「Cisco Emergency Responder 8.6 のライセンス」（P.1-4）を参照してください。

表 A-5 に、[License Manager] ページの説明を示します。

表 A-5　[License Manager] ページ

フィールド	説明
Status	ステータス メッセージが表示されます。
[Upload license] ボタン	ドロップダウン メニューで選択したサーバにライセンス ファイルをアップロードすることができます。 **（注）** パブリッシャ サーバとサブスクライバ サーバで別々のライセンス ファイルを購入する必要がありますが、パブリッシャ サーバ上でのみ、Cisco Emergency Administration Web ページを使用して、パブリッシャとサブスクライバの両方のライセンス ファイルをアップロードすることができます。
Details of Emergency Responder Licenses	
Installation Date (MM/YY/DD)	サーバ ライセンスがインストールされた日付が表示されます。 **（注）** この日付は、評価ライセンスの場合にのみ表示されます。
Emergency Responder Server License	

表 A-5　[License Manager] ページ（続き）

フィールド	説明
Emergency Responder server license type	インストールされたサーバ ライセンスのタイプが表示されます。このフィールドに使用可能な値は 2 つあります。 • Evaluation：サーバ ライセンスはインストールされず、Emergency Responder が 60 日モードで動作します。 • Permanent：サーバ ライセンスがインストールされます。
Server license count	サーバ グループ内のライセンスされたサーバの数が表示されます。
Emergency Responder User License	インストールされた Emergency Responder ユーザ ライセンスに関する次の情報が表示されます。 • 累積ユーザ ライセンス カウント • パブリッシャ ユーザ ライセンス カウント • サブスクライバ ユーザ ライセンス カウント • 検出された電話機の台数 • 手動で設定された電話機の台数 • 現在追跡中のユーザの総数

関連項目

- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）
- 「Cisco Emergency Responder 8.6 のライセンス」（P.1-4）
- 「Cisco Emergency Responder ライセンス ファイルのアップロード」（P.4-25）

Email Alert Settings

[System]>[Mail Alert Configurations] を選択すると、[Email Alert Settings] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Email Alert Settings] ページは、Emergency Responder から電子メール アラートを送信するパラメータを指定するために使用します。各パラメータの右側にあるチェックボックスを使用して、そのパラメータの電子メール アラートをイネーブル（オン）またはディセーブル（オフ）にします。イベント ビューアからの詳細を電子メール メッセージに含める場合は、[Include event viewer contents in mail] チェックボックスをオンにします。

表 A-6 に、[Email Alert Settings] ページの説明を示します。

表 A-6　[Email Alert Settings] ページ

フィールド	電子メール アラートが送信されるタイミング
Discovery Parameters	
Discovery Engine Registration Failed	Discovery Engine の登録が失敗した場合
Discovery Engine goes out of connection	Discovery Engine の接続が失われた場合

表 A-6　[Email Alert Settings] ページ（続き）

フィールド	電子メール アラートが送信されるタイミング
For unreachable devices during recovery	スイッチや Cisco Unified Communications Managers などのデバイスが到達不能になった場合
Emergency Call Routing Parameters	
Call information	911 コールが発信された場合
Call routing session ended due to problems	コール ルーティングが次の原因のいずれかで停止された場合 • Invalid CMC • Invalid FAC • FAC and CMC needed • CMC needed • FAC needed • RESOURCE_BUSY
Re-Routing of call	緊急コールが再ルーティングされた場合
Routing failure	コール ルーティングが失敗した場合
Route Point out of Service	ルート ポイントがアウト オブ サービスになった場合
Cluster Parameters	
Cluster DB Failure	サーバがクラスタ データベース ホストと通信できなくなった場合
Intra Cluster Failure	クラスタ内のサーバグループへのクラスタ内通信が失敗した場合
Misc Parameters	
Subscriber becomes active	サブスクライバがアクティブになった場合
Publisher comes back online	パブリッシャがオンラインに戻った場合
Not able to get the JTAPI Provider	Emergency Responder が JTAPI プロバイダーを取得できなかった場合
Available user licenses get exhausted during phone tracking	電話機の追跡中にユーザ ライセンス数が 0 になった場合
Switch Port location change reporting	電話機に関するスイッチ ポート変更報告をイネーブルにした場合
Suppress IP Communicator location change reporting	ロケーション変更報告電子メール アラートから Cisco Unified IP Communicator を除外した場合
[Update Settings] ボタン	電子メール アラート設定を更新します。
[Cancel Changes] ボタン	電子メール アラート設定に対する変更をキャンセルします。

関連項目

- 「Onsite Alert Settings」（P.A-13）
- 「Cisco Emergency Responder サーバ グループの設定」（P.4-22）

Add Subscriber

[System]>[Add Subscriber] を選択すると、[Add Subscriber] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Add Subscriber] ページは、Emergency Responder サーバ グループにサブスクライバ サーバを追加するために使用します。サブスクライバ情報を追加したら、次の作業のいずれかを実行する必要があります。

- インストール中にプロンプトが表示された場合は、正しいパブリッシャ サーバ情報が入力されていることを確認してください。

はじめる前に

サブスクライバ サーバを設定する前に、パブリッシャ サーバを設定する必要があります。

表 A-7 に、[Add Subscriber] ページの説明を示します。

表 A-7　[Add Subscriber] ページ

フィールド	説明
Add Subscriber	
HostName	サブスクライバ サーバのホスト名
[Insert] ボタン	新しいサブスクライバ サーバを追加するには、[Insert] をクリックします。
[Cancel Changes] ボタン	[Add Subscriber] ページから入力を削除します。
Configured Servers	現在設定されているすべてのサーバのリストで、サーバごとにホスト名と IP アドレスが表示されます。

関連項目

- 「Cisco Emergency Responder Publisher のインストール」（P.2-14）
- 「Cisco Emergency Responder Subscriber のインストール」（P.2-19）

Intrado VUI Settings

[System]>[Intrado VUI Settings] を選択すると、[Intrado VUI Settings] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Intrado VUI Settings] ページは、Emergency Responder で Intrado Validation and Update Interface（検証および更新インターフェイス）を相互運用するために必要なアカウント情報を入力するために使用します。必要な情報を入力したら、このページから Intrado への接続をテストすることができます。

表 A-8 に、[Intrado VUI Settings] ページの説明を示します。

表 A-8　Intrado VUI Settings

フィールド	説明
Status	ステータス メッセージが表示されます。
Intrado VUI Settings	
Upload Certificate	ローカル ドライブから Emergency Responder サーバに証明書をアップロードします。 証明書をアップロードするには、次の手順を実行します。 1. [Upload Certificate] リンクをクリックします。 [Upload Certificate] ウィンドウが表示されます。 2. [Browse] ボタンをクリックして、ローカル マシン上の証明書ファイルを探します。 3. [Upload] ボタンをクリックして、証明書ファイルをアップロードします。
Validate Certificate	
Intrado Certificate Password	この証明書を使用して作成されたパスワード。
VUI URL	VUI URL は Intrado から提供されます。
Test and Validate Certificate	このボタンは、証明書の妥当性をテストするために使用します。
Configure Account Details	
VUI Schema URL	Intrado から提供された VUI スキーマ URL。
Intrado Account ID	Intrado から提供された Intrado アカウント ID。
Max VUI Connections	Emergency Responder がサーバ グループ全体で許可する同時 VUI 接続の最大数。
Test Connectivity	このリンクは、Emergency Responder から Intrado VUI に正常に接続できるかどうかを確認するために使用します。
Delete Account	Emergency Responder データベースから既存の Intrado アカウントを削除します。
Update	このページで加えた変更を保存するには、[Update] をクリックします。
Cancel	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel] をクリックします。

関連項目

- 「Cisco Emergency Responder の Intrado V9-1-1 Enterprise Services との併用」（P.5-1）

Onsite Alert Settings

[ERL]>[Onsite Alert Settings] を選択すると、[Onsite Alert Settings] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Onsite Alert Settings] ページは、オンサイト アラート担当者に関する情報を追加するために使用します。ERL を設定するときに、これらの担当者を ERL に割り当てます。Emergency Responder は、ゾーン内で緊急コールが発信されたときに、割り当てられた担当者に警告します。

表 A-9 に、[Onsite Alert Settings] ページの説明を示します。

表 A-9　[Onsite Alert Settings] ページ

フィールド	説明	注
Add New Onsite Alert Contact		
Onsite Alert ID	オンサイト アラート連絡先の ID。使用する ID は、サイトの識別方法（セキュリティ ID やバッジ番号）に基づいている必要があります。このフィールドは、連絡先を識別するために Emergency Responder 全体で使用されます。たとえば、連絡先をゾーンに割り当てるときに [Onsite Alert ID] から選択します。保存されたオンサイト アラート ID は変更することができません。	組織にとって有意義であると同時に、Emergency Responder でのゾーン設定に有効な命名方法を使用してください。
Onsite Alert Name	オンサイト アラート連絡先の名前。	
Onsite Alert Number	オンサイト アラート連絡先の電話番号。この番号は音声電話番号にする必要があります。ボイスメール システムまたは自動受付の番号は入力しないでください。	Emergency Responder が ERL から緊急コールを受信すると、ERL の連絡先のオンサイト アラート番号を呼び出して、緊急コールが発信された電話番号を含む事前に録音されたメッセージを再生します。 Emergency Responder では、先頭に「+」が付いた E.164 番号はオンサイトのセキュリティ電話番号としてサポートされません。Cisco Unified CM で設定されたオンサイトのセキュリティ電話番号が、先頭に「+」が付いた E.164 番号である場合は、まず、先頭に「+」が付かないオンサイトのセキュリティ電話番号を Emergency Responder で設定する必要があります。次に、Emergency Responder からオンサイトのセキュリティ電話番号が受信されるときに「+」が追加されるように、Cisco Unified CM でトランスレーション パターンを設定する必要があります。「E.164 ダイヤル プランに基づくセキュリティ担当者の割り当て」（P.3-22）を参照してください。

表 A-9　[Onsite Alert Settings] ページ（続き）

フィールド	説明	注
Onsite Alert Email Address	オンライン アラート連絡先の電子メール アドレス（email@domain.com など）。	Emergency Responder が ERL から緊急コールを受信すると、その ERL に関連付けられたオンサイト アラート連絡先に電子メールを送信します。電子メール ID が電子メール ページング システム用の場合は、電子メールの代わりにページが連絡先に送信されます。この電子メールまたはページには、緊急コールが発信された電話番号が含まれています。
Onsite Alert Pager Address	オンサイト アラート連絡先のポケットベル電子メール アドレス（<*pager_number*>@domain.com など）。	[Pager Alert Setting] ページ上のフィールドを設定することによって、ポケットベルに送信されるメッセージのサイズを制限することができます。「Pager Alert Settings」（P.A-16）を参照してください。
[Insert] ボタン	連絡先を連絡先のリストに追加するには、[Insert] をクリックします。そうすると、連絡先がページの [Available Onsite Alerts] セクションに一覧表示されます。	
[Cancel Changes] ボタン	このページに加えたすべての変更をキャンセルするには、[Cancel Changes] をクリックします。	
Available Onsite Alerts	すでに設定されているオンサイト アラート連絡先が表示されるページ セクション。設定済みのオンサイト アラート連絡先の場合は、次の情報が表示されます。 • Onsite Alert ID • Onsite Alert Name • Onsite Alert Number • Onsite Alert Email Address エントリを変更するには、そのエントリをクリックするか、[Edit] アイコンをクリックします。その人物の連絡先情報が編集ボックスにロードされます。変更を加えて、[Update] をクリックします。 エントリを削除するには、そのエントリと同じ行にある [Delete] アイコンをクリックします。	どの連絡先も設定されていない場合は、このセクションが空白になります。 連絡先のオンサイト アラート ID は変更することができません。 エントリを削除するには、その人物が割り当てられた ERL を更新して、ERL からその人物を削除できるようにする必要があります。
[Add New] ボタン	別の連絡先を追加するには、[Add New] をクリックします。	
[Update] ボタン	情報に加えた変更を保存するには、既存の連絡先の設定が表示されているときに [Update] をクリックします。	既存の連絡先に関する情報が表示されている場合にだけ使用することができます。

関連項目

- 「セキュリティ担当者（オンサイト アラート担当者）の指定」（P.4-32）
- 「ERL の作成」（P.4-33）

- 「Cisco Emergency Responder のためのオンサイト アラート（セキュリティ）担当者の準備」（P.10-1）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Pager Alert Settings

[ERL]>[Pager Alert Configurations] を選択すると、[Pager Alert Settings] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Pager Alert Configurations] ページは、ポケットベルに送信するフィールドを選択して、それらのラベルを編集することによって、システム全体のポケットベル メッセージのサイズを制限するために使用します。

表 A-10 に、[Pager Alert Settings] ページの説明を示します。

表 A-10　Pager Alert Settings

フィールド	説明
Pager Alert Settings	次のフィールドを選択して、それらに関連付けられたラベルを編集することによって、送信するポケットベル メッセージのサイズを制限することができます。 • Extension • ERL • Location • Time • Server ポケットベルに表示するフィールドを選択するには、フィールドの隣にあるボックスをオンにします。 ポケットベルに送信するラベルを編集するには、そのフィールドのテキスト ボックスをクリックします。
[Update Settings] ボタン	加えた変更を保存するには、[Update Settings] をクリックします。
[Restore Defaults] ボタン	デフォルトのポケットベルとラベルの設定を復元するには、[Restore Defaults] をクリックします。
Send Sample Message to a pager	ポケットベルにテスト メッセージを送信するには、テキスト ボックスにポケットベルのアドレスを入力して、[Send Test Message] ボタンをクリックします。

関連項目

- 「Onsite Alert Settings」（P.A-13）
- 「Cisco Emergency Responder のためのオンサイト アラート（セキュリティ）担当者の準備」（P.10-1）

Conventional ERL

[ERL]>[Conventional ERL] を選択すると、[Conventional ERL] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Conventional ERL Data] ページは、会社の ERL を定義するために使用します。ERL は、建物全体（小規模な場合）、建物のフロア、またはフロアの一区画にすることができます。コミュニティごとに ERL のサイズに関する法律が異なる可能性があるため、ERL を決定する前に、地元の条例を調べたり、サービス プロバイダーに相談したりしてください。作成された ERL は緊急応答チームが緊急事態を特定するために使用するため、ERL はそれらのチームが発信者を妥当な時間内に特定できる規模にする必要があります。

表 A-11 に、[Find and List ERLs] ページの説明を示します。

表 A-11　[Find and List ERLs] ページ

フィールド	説明	注
ERL Search Parameters		
Find Conventional ERL where...	検索条件を選択して、[Find] をクリックすると、既存の ERL が一覧表示されます。すべての ERL を一覧表示するには、条件を入力せずに [Find] をクリックします。ドロップダウン メニューから、検索ごとにページ単位で表示するレコード件数を選択することができます。 検索結果リストでは、次の操作を実行できます。 • エントリをクリックすると、その特性を表示して更新することができます。 • ALI データが同じ新しい ERL を作成するには、[Copy] アイコンをクリックします。 • ERL を削除するには、[Delete] アイコンをクリックします。 • ERL に加えられた変更履歴を表示するには、[Audit Trail] 列の [view...] をクリックします。詳細については、「ERL Audit Trail」（P.A-75）を参照してください。	ERL をコピーしても、ERL 内で一意にすべき情報はコピーされません。 詳細については、「Add New ERL」（P.A-18）を参照してください。
Configure Default ERL	デフォルト ERL を設定してから、他の ERL を設定する必要があります。 デフォルト ERL は、他に ERL 設定が見当たらない場合にコール ルーティングに使用されるシステム定義の ERL です。 （注）　アップグレード シナリオでのデータ移行で、デフォルト ERL に割り当てられた手動設定電話機が存在する場合は、その設定が変更されるまでその状態が維持されます。	詳細については、「Add New ERL」（P.A-18）を参照してください。

表 A-11　[Find and List ERLs] ページ（続き）

フィールド	説明	注
Add New ERL	新しい ERL を作成するには、[Add New ERL] をクリックします。	詳細については、「Add New ERL」（P.A-18）を参照してください。
Configure Default ERL	デフォルト ERL を設定するには、[Configure Default ERL] をクリックします。	
Export	ERL 設定を含むファイルを作成するには、[Export] リンクをクリックします。	ERL データのエクスポート方法については、「Export ERL Data」（P.A-25）を参照してください。
Import	別のファイルに保存された情報を使用して ERL を作成または更新するには、[Import] リンクをクリックします。ERL データをインポートすることによって、一度に複数の ERL を作成または更新することができます。	ERL データのインポート方法については、「Import ERL Data」（P.A-26）を参照してください。

関連項目

- 「Export PS-ALI Records」（P.A-76）
- 「ERL の作成」（P.4-33）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Add New ERL

[Add New ERL] ページと [ERL Information for ERL Name] ページは、次の点で、本質的に同じです。

（注）　[ERL Information for ERL Name] ページでは、*ERL Name* 変数がそのページに関連付けられた ERL の名前に置き換えられます。たとえば、デフォルト ERL をクリックすると、表示されていたページのタイトルが「**ERL Information for Default**」に変わります。同様に、ERL 名が First Floor の場合は、表示されていたページのタイトルが「**ERL Information for First Floor**」に変わります。

- [Add New ERL] ページは、[Find ERL Data] ページ（[ERL]>[Conventional ERL] を選択したときに表示される）で [Add New ERL] を選択すると表示されます。既存の ERL の場合は、[Copy] をクリックしてもこのページが表示されます。
- [ERL Information for Default] ページは、[Find ERL Data] ページで [Configure Default ERL] をクリックすると開きます。[ERL Information for ERL Name] ページは、[Find ERL Data] ページ（[ERL]>[Conventional ERL] を選択したときに表示される）でリスト内の既存の ERL に関連付けられたリンクをクリックしても表示されます。

（注）　デフォルト ERL はテスト ERL として使用できません。[ERL Information for Default] ページでは、[Test ERL] チェックボックスが使用できなくなっています。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Add New ERL] ページは、新しい ERL を作成するために使用します。また、別のファイルから事前に定義された ERL 情報をインポートすることによって、一度に複数の ERL を作成または更新することができます。詳細については、「Import ERL Data」（P.A-26）を参照してください。

Emergency Responder 8.6 を使用すれば、ERL をテスト ERL として選択することができます。

[Find ERL Data] ページは、既存の ERL を表示または更新するために使用します。

Cisco Unified Communications Manager での ELIN 番号の設定方法については、「 •「ERL の作成」（P.4-33）」（P.3-10）を参照してください。

緊急コールを PSAP の代わりにオンサイト セキュリティにルーティングする場合は、「ERL の設定（Non-PSAP 配置の場合）」（P.4-34）で、ルート / トランスレーション パターンと ELIN の設定方法を参照してください。

表 A-12 に、[Add New ERL] ページと [ERL Information] ページの説明を示します。

表 A-12　[Add New ERL] ページと [ERL Information] ページ

フィールド	説明	注
ERL Settings		
ERL Name	ERL の名前。使用する命名方法が重要です。ERL 名は、セキュリティ チームが緊急コールを受けたときに最初に目にするものの 1 つです。この名前がわかりやすければ、チームはすばやくコールに対処することができます。 たとえば、Building J という名前の 3 階建てのビルでフロアごとに 1 つずつの ERL を作成する場合は、それらの名前を BldgJ-Floor1、BldgJ-Floor2、BldgJ-Floor3 にします。 ERL 命名方法はセキュリティ チームと協力して策定してください。	既存の ERL の名前は変更することができません。ERL 名を変更するには、新しい ERL を作成してから、古い ERL を削除します。 先行スペースと後続スペースは削除されます。
Description	新しい ERL の説明を入力します（任意）。	
Test ERL (Used for Synthetic Testing)	この ERL がテストに使用される場合に、このチェックボックスをオンにします。テスト ERL は、Emergency Responder が CiscoWorks IP Telephony Environment Monitor（ITEM）によってモニタされている場合に使用することができます。 「テスト ERL の設定」（P.4-40）を参照してください。	この設定は、[ERL Information for Default] ページでは使用できません。デフォルト ERL はテスト ERL として使用できません。

表 A-12　[Add New ERL] ページと [ERL Information] ページ（続き）

フィールド	説明	注
ELIN Settings	緊急コールを PSAP にルーティングして、PSAP が電話を切ってから緊急発信者を呼び出す必要がある場合に PSAP にコールバック番号を提供するルート パターンと電話番号の組み合わせ。	ERL ごとに一意の ELIN を設定する必要があります。定義した ELIN の数によって、サポート可能なコールバック回数が決定されます。ELIN は、緊急コールの発信順に使用され、必要に応じて、再利用されます。たとえば、1 つの ERL に対して 2 つの ELIN を定義して、3 回の緊急コールが発信された場合は、PSAP が最初の緊急発信者にコールバックできません。 ただし、同時緊急コール数は ELIN の数に*左右されません*。ELIN が 2 つしかない場合でも、10 回のアクティブ緊急コールを受けることができます。ELIN の数は、PSAP のコールバック能力にしか影響しません。 **（注）** ELIN が Off-Premises Cisco ER ユーザの直通社内通話（DID）番号として設定されている場合は、Emergency Responder が ELIN と ERL の関連付けを制限します。DID 番号が、Emergency Responder 内で構外ロケーションに関連付けられたことのないユーザに属している場合は、この制限がかかりません。
Route/Translation Pattern	Cisco Unified Communications Manager 内のルート パターンとして定義された電話番号で、コールをルーティングするゲートウェイを使用して正しい PSAP に到達するように設定されます。この番号には、米国での 911 のような外部緊急番号を含める必要があります。たとえば、10.911 や 10911 を含めます。パターンに含めることができるのは、数字とドットのみです。	ELIN には、先頭に「+」が付いた E.164 番号を使用できません。10 桁の北米番号計画または他の国内形式の番号を使用してください。
ELIN Number	コールを正しいローカル PSAP にルーティングする一意の電話番号で、PSAP が電話を切った後で緊急発信者にかけ直すときに使用することができます。この番号は、サービス プロバイダーから提供された DID 番号にする必要があります。つまり、PSTN 上でルーティング可能な番号にする必要があります。4085551212、408-555-1212、408.5551212、(408)555-1212 のように、エリア コードを含めた番号全体を入力します。番号には、数字、シングル ハイフン、ドット、括弧以外を含めることができません。	
[Add] ボタン	ルート ポイントと ELIN の組み合わせを追加するには、情報を入力して [Add] をクリックします。	

表 A-12　[Add New ERL] ページと [ERL Information] ページ（続き）

フィールド	説明	注
[Update] ボタン	既存の組み合わせを変更するには、それをリストで選択して、編集ボックスで情報を変更し、[Update] をクリックします。	
[Remove] ボタン	組み合わせを削除するには、それをリストで選択して [Remove] をクリックします。	
Onsite Alert Settings		
Available Onsite Alert IDs	対応可能なすべてのオンサイト アラート担当者の ID が表示されるテキスト ボックス。	事前に、オンサイト アラート担当者のリストに連絡先を追加しておく必要があります。詳細については、「Onsite Alert Settings」（P.A-13）を参照してください。
[Add] ボタン	ERL に割り当てるオンサイト アラート（セキュリティ）連絡先を選択します。ERL から緊急コールが発信されると、これらの連絡先に通知されます。連絡先を追加するには、[Available Onsite Alert IDs] リストからオンサイト アラート ID を選択して [Add] をクリックします。そうすると、その連絡先の ID が [Onsite Alert IDs for the ERL] テキスト ボックスに表示されます。	
[Remove] ボタン	ERL の連絡先を削除するには、[Onsite Alert IDs for the ERL] テキスト ボックスで該当する ID を選択して [Remove] をクリックします。	
ERL Address		
[ALI Details] ボタン	ERL の Automatic Location Information（ALI）を表示または変更するには、[ALI Details] をクリックします。ALI は、所在地住所や電話番号などの ERL の場所に関する詳細情報を提供します。	ALI フィールドについては、「ALI Information (for ERL Name)」（P.A-22）を参照してください。
[Insert] ボタン	新しい ERL に加えた変更を保存するには、[Insert] をクリックします。	[Insert] ボタンは、新しい ERL を作成している場合にのみ使用可能になります。
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	
[Update] ボタン	ERL に加えた変更を保存するには、[Update] をクリックします。	[Update] ボタンは、既存の ERL を変更している場合にのみ使用可能になります。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。変更を保存するには、[Close] をクリックする前に、[Update] または [Insert] をクリックする必要があります。	

関連項目

- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）
- 「デフォルト ERL の設定」（P.4-33）
- 「ERL と ALI の設定」（P.4-35）

- 「テスト ERL の設定」（P.4-40）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

ALI Information (for ERL Name)

次のいずれかを実行すると、[ALI Information (for ERL Name)] ページが表示されます。

（注）　[ALI Information (for ERL Name)] ページの *ERL Name* 変数が該当する ERL 名に置き換えられます。たとえば、[ERL Information for Default] ページで [ALI Details] をクリックすると、表示されていたページのタイトルが「**ALI Information for Default**」に変わります。同様に、ERL 名が First Floor の場合は、表示されていたページのタイトルが「**ALI Information for First Floor**」に変わります。

- [Add New ERL] ページの [ERL Address] セクションで [Add/Edit ALI] をクリックします。

  （注）　[Add New ERL] ページは、[Find ERL Data] ページ（[ERL]>[Conventional ERL] を選択したときに表示される）で [Add New ERL] を選択すると表示されます。

- [ERL Information for ERL Name] ページで [Add/Edit ALI] をクリックします。[ERL Information for ERL Name] ページは、[Find ERL Data] ページ（[ERL]>[Details] を選択したときに表示される）で既存の ERL 名または [Configure Default ERL] をクリックすると表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Enter ALI Information] ページは、ERL に関する ALI を入力するために使用します。この情報は、必要なデータベースに届くことを保証しているサービス プロバイダーに送信されます。このサービス プロバイダーは、ELIN からのコールがローカル PSAP にルーティングされ、その PSAP で緊急コールが特定できるようにします。

これらのフィールドのデータ要件は、サービス プロバイダーによって異なります。要件の詳細については、サービス プロバイダーにお問い合わせください。表 A-13 のフィールドに関する説明は、National Emergency Number Association（NENA）バージョン 2 標準（米国）に基づいています。

注意　ここで入力する情報の質が重要です。この情報は、緊急コール オペレータとローカル対応チームに表示されます。彼らはこの情報を使用して緊急発信者を特定します。データが間違っていたり、わかりにくかったりすると、緊急対応が遅れて、防げた惨事が起きてしまう可能性があります。

表 A-13 に、[Enter ALI Information] ページの説明を示します。

表 A-13　[Enter ALI Information] ページ

フィールド	説明	注
Find all prevalidated fields from validation file by selecting a tag		
Select a Tag	ウィンドウにロードする ALI データが関連付けられたタグを選択します。そうすると、その ALI に関する情報を編集することができます。	validate.txt ファイル内にタグをセットアップすることによって、ALI データの入力を容易にすることができます。このページには、ファイルの格納場所、ファイルの形式が記載された samplevalidate.txt ファイルの検索場所が表示されます。 タグを作成するときに、会社名、市、州などの複数の ALI に共通する情報を入力します。たとえば、25 階建てのビルがあり、そのフロアごとに 1 つずつの ERL を作成する場合は、「25story」という名前のタグを作成することができます。そうすれば、そのビルに関する情報を 25 回繰り返し入力しなくても、1 つのタグを選択するだけで、そのタグに対して定義したデータと一緒に ALI データがロードされます。
ALI Data		
House Number	建物の所在地住所に含まれる番号（例：「170 West Tasman Dr.」の中の「170」）。	この番号は最大 10 桁にすることができますが、サービス プロバイダーが 8 桁の番号しかサポートしていない場合があります。
House Number Suffix	番地の番号拡張（/2 など）。	
Street Name	建物の住所に含まれる通り名。	60 文字以下に制限されています。
Prefix Directional	通り名に含まれている場合の先行方向指示（北を示す N など）。	N、S、E、W、NE、NW、SE、SW のいずれかにすることができます。
Street Suffix	通りの種類。ドロップダウン リストから種類を選択します。このフィールドには、U.S. Postal Service Publication 28 で許可されている略語の 1 つが入力されます（大通りを示す AVE など）。	サフィクスに入力することもできます。4 文字以下に制限されています。
Post Directional	通り名に含まれている場合の後続方向指示（北を示す N など）。	N、S、E、W、NE、NW、SE、SW のいずれかにすることができます。
Community Name	住所の地域名（市、町、区名など）。	32 文字以下に制限されています。
State	2 文字の州の略語。	2 文字以下に制限されています。
Main NPA	ERL に関連付けられた代表番号の 3 桁のエリアコード。	
Main Telephone No.	ERL に関連付けられた代表電話番号。これは、ERL の警察施設の番号にすることができます。	7 文字以下に制限されています。
Class of Service	ERL のサービス クラスを選択します。	サービス クラスが不明の場合は、サービス プロバイダーにお問い合わせください。
Type of Service	ERL のタイプ オブ サービスを選択します。	サービス クラスが不明の場合は、サービス プロバイダーにお問い合わせください。
Exchange	電話局を運営している Local Exchange Carrier（LEC; 地域通信事業者）の交換 ID。	4 文字以下に制限されています。この ID はサービス プロバイダーにお問い合わせください。

表 A-13　[Enter ALI Information] ページ（続き）

フィールド	説明	注
Customer Name	ERL に関連付けられた加入者名。通常は、会社名。	32 文字以下に制限されています。
Order Number	このレコードを設定または更新するアクティビティのサービス注文番号。	10 文字以下に制限されています。必要な場合は、有効な注文番号をサービス プロバイダーにお問い合わせください。
Extract Date	レコードが作成された日付。	これは、読み取り専用フィールドです。
County ID	ゾーンの国識別コード。米国では、国勢調査局によって国に割り当てられた FIPS コードを使用します。	4 文字以下に制限されています。
Company ID	NENA に登録されている国識別コード。	5 文字以下に制限されています。
Zip Code	住所の郵便番号。	5 文字以下に制限されています。
Zip Code Extension	ZIP+4 番号。	4 桁以下に制限されています。
Customer Code	顧客コード。コードが不明の場合は、サービス プロバイダーにお問い合わせください。	3 文字以下に制限されています。 このフィールドを変更すると、Emergency Responder によって、古いコードを持つ ALI を削除するための削除レコードと、新しいコードを持つ ALI を追加するための挿入レコードが生成されます。この削除/挿入シーケンスは、次に ALI をエクスポートするときにのみ生成されます。このエクスポート ファイルがサービス プロバイダーに提出されていることを確認する必要があります。
Comments	オプションのコメント。ERL から緊急コールが発信された場合に、これらのコメントが PSAP に表示されます。	30 文字以下に制限されています。
Longitude	ERL の経度。	9 桁以下に制限されています。
Latitude	ERL の緯度。	9 桁以下に制限されています。
Elevation	ERL の高度。	5 桁以下に制限されています。
TAR Code	課税区画レート コード。	6 文字以下に制限されています。
Location	電話の正確な場所を特定するために役立つ、自由形式の追加の場所情報。 この情報は、緊急コールが発信されたときに、ERL 名と一緒にセキュリティ担当者に表示されるため、このフィールドは発信者の特定を支援するために使用します。たとえば、定義された所在地住所を、このページの他のフィールドに繰り返し入力することができます。	60 文字以下に制限されています。

表 A-13　[Enter ALI Information] ページ（続き）

フィールド	説明	注
Reserved	サービス プロバイダーで有効な ALI ファイルを作成するために必要な情報。	予約領域への入力が必須かどうかは、サービス プロバイダーにお問い合わせください。 NENA 要件と CSV 要件が違う場合があることに注意してください。たとえば、ERL インポートでは、予約フィールドに何も入力する必要がありません。すべての ERL レコードを空にしても、Emergency Responder でそのファイルのインポートが許可されます。ただし、ファイルからフィールド自体を削除しないようにする必要があります。レコード内にフィールドが存在する必要があります。フィールドはカンマ区切りの空文字列にすることができます。
[Save and Close] ボタン	変更を保存して、[Enter ALI Information] ページを閉じるには、[Save and Close] をクリックします。	このボタンは、新しい ERL に関する情報を入力したときにのみ使用可能になります。
[Update ALI Info] ボタン。	変更を保存するには、[Update ALI Info] をクリックします。	このボタンは、設定済みの ERL が表示されている場合にのみ使用可能になります。
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。	

関連項目

- 「デフォルト ERL の設定」（P.4-33）
- 「ERL と ALI の設定」（P.4-35）
- 「複数の ERL の一括インポート」（P.4-37）
- 「Export PS-ALI Records」（P.A-76）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Export ERL Data

[Find ERL Data] ページ（[ERL]>[Conventional ERL] を選択したときに表示される）で [Export] リンクをクリックすると、[Export ERL Data] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Export ERL Data] ページは、個人的に使用する ERL エクスポート ファイルを作成するために使用します。ERL エクスポート ファイルはサービス プロバイダーに提出しないでください。たとえば、ERL エクスポート ファイルは、設定をバックアップしたり、設定を別の Emergency Responder サーバに移動したりするために使用します。

ALI データを更新するためにサービス プロバイダーに送信するファイルを作成するには、「Export PS-ALI Records」（P.A-76）を参照してください。

表 A-14 に、[Export ERL Data] ページの説明を示します。

表 A-14　[Export ERL Data] ページ

フィールド	説明
Select Export Format	エクスポート ファイルで使用すべきファイル形式。ERL データの場合は、comma separated value（csv; カンマ区切り値）か XML のどちらかです。
Enter Export File Name	作成するファイルの名前。ファイル拡張子を含めないでください。
[Export] ボタン	エクスポート ファイルを作成するには、[Export] をクリックします。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。

関連項目

- 「ALI 提出要件に関するサービス プロバイダーとの交渉」（P.1-22）
- 「ERL 情報のエクスポート」（P.4-41）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Import ERL Data

[Find ERL Data] ページ（[ERL]>[Conventional ERL] を選択したときに表示される）で [Import] リンクをクリックすると、[Import ERL Data] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Import ERL Data] ページは、ERL データが定義されたファイルから一度に複数の ERL を作成または更新するために使用します。このファイルは、必要な形式（csv または xml）のいずれかで情報を保存可能なスプレッドシートを使用して作成します。インポート ファイルを作成する前に、このページのサンプルを確認してください。

多数の ERL を更新する必要がある場合は、ERL データをエクスポートして、エクスポート ファイルを更新し、そのファイルを再度インポートします。

アップロード ユーティリティを使用して、ERL データを含むファイルをローカル システムからアップロードすることもできます。その後で、ERL データをインポートすることができます。詳細については、「ファイルのアップロード」（P.4-7）を参照してください。

表 A-15 に、[Import ERL Data] ページの説明を示します。

表 A-15　[Import ERL Data] ページ

フィールド	説明
Select Import Format	インポートするファイルに使用される形式を選択します。 形式を選択したら、[View sample file] をクリックして、予想される形式と値のシーケンスの例を確認します。このサンプル情報を使用して、スプレッドシートでインポート ファイルを作成します。
Select File to Import	ERL データをインポートするファイルを選択します。
[Upload] ボタン	ファイルをローカル システムからアップロードするには、[Upload] をクリックします。詳細については、「ファイルのアップロード」（P.4-7）を参照してください。
[Import] ボタン	インポート ファイルから Emergency Responder データベースに ERL データを追加するには、[Import] をクリックします。 （注）　インポートされた ERL データによって、Emergency Responder データベース内の競合するデータが上書きされます。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。

関連項目

- 「複数の ERL の一括インポート」（P.4-37）
- 「ERL 情報のエクスポート」（P.4-41）
- 「ファイルのアップロード」（P.4-7）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）
- 「Export PS-ALI Records」（P.A-76）

Off-Premises ERL (Search and List)

[ERL]> [Off-Premise ERL] > [Search And List] を選択すると、[Find Off-Premises ERL Data] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Off-Premise ERL Data] ページは、電話機が社内ネットワークの外部に設置された個人の ERL を定義するために使用します。

表 A-16 に、[Find and List Off-Premise ERLs] ページの説明を示します。

表 A-16　Find Intrado ERL Data (Off-Premise)

フィールド	説明	注
ERL Search Parameters		
Find Off-Premises ERL where...	既存の Off-Premise ERL を一覧表示するには、検索条件を選択して、[Find] をクリックします。すべての ERL を一覧表示するには、条件を入力せずに [Find] をクリックします。ドロップダウン メニューから、検索ごとにページ単位で表示するレコード件数を選択することができます。 検索結果リストでは、次の操作を実行できます。 • エントリをクリックすると、その特性を表示して更新することができます。 • ALI データが同じ新しい ERL を作成するには、[Copy] アイコンをクリックします。 • ERL を削除するには、[Delete] アイコンをクリックします。 • ERL に加えられた変更履歴を表示するには、[Audit Trail] 列の [view...] をクリックします。詳細については、「ERL Audit Trail」（P.A-75）を参照してください。	ERL をコピーしても、ERL 内で一意にすべき情報はコピーされません。
Add New ERL	新しい ERL を作成するには、[Add New ERL] をクリックします。	

関連項目

- 「Add New ERL」（P.A-28）
- 「Secondary Status」（P.A-30）
- 「構外ユーザをサポートするための Emergency Responder の設定」（P.5-8）

Add New ERL

[Find Intrado ERL Data] ページ（[ERL]>[Off-Premise ERL] > [Search and List] を選択したときに表示される）で、[Add New ERL] を選択すると、[Add New ERL (Off-Premise phones)] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Add New ERL] ページは、構外電話機の新しい ERL を作成するために使用します。また、別のファイルから事前に定義された ERL 情報をインポートすることによって、一度に複数の ERL を作成または更新することができます。詳細については、「Import ERL Data」（P.A-26）を参照してください。

[Find ERL Data] ページは、既存の ERL を表示または更新するために使用します。

表 A-17 に、[Add New ERL (Off-Premise Phones)] ページの説明を示します。

表 A-17　Add New ERL (Off-Premise Phones)

フィールド	説明	注意事項
ERL Settings		
ERL Name	ERL の名前。使用する命名方法が重要です。ERL 名は、セキュリティ チームが緊急コールを受けたときに最初に目にするものの 1 つです。この名前がわかりやすければ、チームはすばやくコールに対処することができます。 ERL 命名方法はセキュリティ チームと協力して策定してください。	既存の ERL の名前は変更することができません。ERL 名を変更するには、新しい ERL を作成してから、古い ERL を削除します。 先行スペースと後続スペースは削除されます。
Description	新しい ERL の説明を入力します（任意）。	
Route/Translation Pattern Settings		
Route/Translation Pattern	Cisco Unified Communications Manager 内のルート パターンとして定義された電話番号で、コールをルーティングするゲートウェイを使用して正しい PSAP に到達するように設定されます。この番号には、米国での 911 のような外部緊急番号を含める必要があります。たとえば、10.911 や 10911 を含めます。パターンに含めることができるのは、数字とドットのみです。	
[Add] ボタン	ルート ポイントを追加するには、ドロップダウン ボックスからルート ポイントを選択して [Add] をクリックします。	
[Remove] ボタン	組み合わせを削除するには、それをリストで選択して [Remove] をクリックします。	
Onsite Alert Settings		
Available Onsite Alert IDs	対応可能なすべてのオンサイト アラート担当者の ID が表示されるテキスト ボックス。	事前に、オンサイト アラート担当者のリストに連絡先を追加しておく必要があります。詳細については、「Onsite Alert Settings」（P.A-13）を参照してください。
[Add] ボタン	ERL に割り当てるオンサイト アラート（セキュリティ）連絡先を選択します。ERL から緊急コールが発信されると、これらの連絡先に通知されます。連絡先を追加するには、[Available Onsite Alert IDs] リストからオンサイト アラート ID を選択して [Add] をクリックします。そうすると、その連絡先の ID が [Onsite Alert IDs for the ERL] テキスト ボックスに表示されます。	
[Remove] ボタン	ERL の連絡先を削除するには、[Onsite Alert IDs for the ERL] テキスト ボックスで該当する ID を選択して [Remove] をクリックします。	
[Insert] ボタン	新しい ERL に加えた変更を保存するには、[Insert] をクリックします。	[Insert] ボタンは、新しい ERL を作成している場合にのみ使用可能になります。
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	

表 A-17　Add New ERL (Off-Premise Phones)（続き）

フィールド	説明	注意事項
[Update] ボタン	ERL に加えた変更を保存するには、[Update] をクリックします。	[Update] ボタンは、既存の ERL を変更している場合にのみ使用可能になります。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。変更を保存するには、[Close] をクリックする前に、[Update] または [Insert] をクリックする必要があります。	

関連項目

- 「Off-Premises ERL (Search and List)」（P.A-27）
- 「Secondary Status」（P.A-30）
- 「構外ユーザをサポートするための Emergency Responder の設定」（P.5-8）

Secondary Status

[ERL]> [Off-Premise ERL] > [Secondary Status] を選択すると、[Secondary Status] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Secondary Status] ページは、エラーでフラグが立てられた構外電話番号レコード更新トランザクションに関する情報を Intrado Secondary Status データベースに問い合わせるために使用します。これらのレコードには、次のデータが含まれています。

- 現在は Intrado データベース内に存在する修正済みレコード。
- 修正するために顧客に戻されたエラー レコード。
- Intrado データベースから削除されたエラー レコード。

Intrado Secondary Status データベースに、エラーを含む構外電話番号レコードを問い合わせることができます。

表 A-18 に、[Secondary Status for Off-Premise phones] ページの説明を示します。

表 A-18　Secondary Status (Off-Premise Phones)

フィールド	説明
Find DIDs where...	検索条件を選択して、[Find] をクリックすると、Intrado のセカンダリ ステータス サーバに対する問い合わせの結果が一覧表示されます。

関連項目

- 「Off-Premises ERL (Search and List)」（P.A-27）
- 「Add New ERL」（P.A-28）
- 「構外ユーザをサポートするための Emergency Responder の設定」（P.5-8）

Intrado ERL (Search and List)

[ERL] > [Intrado ERL] > [Intrado ERL (Search and List)] を選択すると、[Find Intrado ERL] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

Intrado V91-1-1 サービスを使用している場合は、[Intrado ERL Data] ページを使用して、会社の ERL を定義することができます。

表 A-19 に、[Find and List Intrado ERLs] ページの説明を示します。

表 A-19　Find Intrado ERL Data

フィールド	説明	注
ERL Search Parameters		
Find Intrado ERL where...	検索条件を選択して、[Find] をクリックすると、既存の Intrado ERL が一覧表示されます。すべての ERL を一覧表示するには、条件を入力せずに [Find] をクリックします。ドロップダウン メニューから、検索ごとにページ単位で表示するレコード件数を選択することができます。 検索結果リストでは、次の操作を実行できます。 • エントリをクリックすると、その特性を表示して更新することができます。 • ALI データが同じ新しい ERL を作成するには、[Copy] アイコンをクリックします。 • ERL を削除するには、[Delete] アイコンをクリックします。 • ERL に加えられた変更履歴を表示するには、[Audit Trail] 列の [view...] をクリックします。詳細については、「ERL Audit Trail」（P.A-75）を参照してください。	ERL をコピーしても、ERL 内で一意にすべき情報はコピーされません。 詳細については、「Add New ERL」（P.A-18）を参照してください。
Add New ERL	新しい ERL を作成するには、[Add New ERL] をクリックします。	詳細については、「Add New ERL」（P.A-18）を参照してください。
[Level of service] ボタン	ALI 詳細で設定された特定の住所に対して Intrado から指定されたサービス レベルを表示するには、[Level of service] をクリックします。Intrado は、次のサービス レベルをサポートします。 • No Coverage：Intrado は、選択的ルータにアクセスすることができず、コールバック番号と住所をその住所を担当している PSAP に提供することができません。 • Basic：現在サービスを提供している PSAP は、有線回線サービスまたは VoIP サービス プロバイダーを緊急支援できません。 • Enhanced：既存の E9-1-1 選択的ルータ ネットワーク経由でコールを PSAP にルーティングすることができ、Intrado はコールバック番号と住所を PSAP に提供することができます。	

表 A-19　Find Intrado ERL Data（続き）

フィールド	説明	注
[Bulk TN Update] ボタン	複数の ERL を選択して、[Bulk TN Update] をクリックすると、選択した ERL の ELIN が更新されます。	
Export	ERL 設定を含むファイルを作成するには、[Export] リンクをクリックします。	ERL データのエクスポート方法については、「Export ERL Data」（P.A-25）を参照してください。
Import	別のファイルに保存された情報を使用して ERL を作成または更新するには、[Import] リンクをクリックします。ERL データをインポートすることによって、一度に複数の ERL を作成または更新することができます。	ERL データのインポート方法については、「Import ERL Data」（P.A-26）を参照してください。

関連項目

- 「Default ALI Values」（P.A-32）
- 「Secondary Status」（P.A-33）
- 「Intrado Schedule」（P.A-34）
- 「View ALI Discrepancies」（P.A-35）
- 「Cisco Emergency Responder での Intrado V9-1-1 for Enterprise Service のサポート方法」（P.5-1）

Default ALI Values

[ERL]> [Intrado ERL] > [Default ALI Values] を選択すると、[Default ALI Values] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Default ALI Values] ページは、新しい Intrado ERL の作成時に、それぞれの ALI フィールドを自動的に生成するデフォルト値を設定するために使用します。

表 A-20 に、[Default ALI Information] ページの説明を示します。

表 A-20　Default ALI Values

フィールド	説明
Default ALI Values for Intrado ERLs	
Type of Service	発信者番号のタイプ オブ サービスを定義します（FX in 911 area や Non-Pub など）。 **（注）** Intrado では、デフォルトを Non-Pub に設定することを推奨しています。

表 A-20　Default ALI Values（続き）

フィールド	説明
Class of Service	発信者番号のサービス クラスを定義します（residential、business、VoIP など）。 （注）　Intrado では、デフォルトを VoIP に設定することを推奨しています。
Company ID	Intrado によって指定されます。
Customer Name	Intrado によって指定されます。
[Update] ボタン	[Update] をクリックして、変更を保存します。
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。

関連項目

- 「Intrado ERL (Search and List)」（P.A-31）
- 「Secondary Status」（P.A-33）
- 「Intrado Schedule」（P.A-34）
- 「View ALI Discrepancies」（P.A-35）
- 「Cisco Emergency Responder の Intrado V9-1-1 Enterprise Services との併用」（P.5-1）

Secondary Status

[ERL]> [Intrado ERL] > [Secondary Status] を選択すると、[Secondary Status] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Secondary Status] ページは、エラーでフラグが立てられた電話番号レコード更新トランザクションに関する情報を Intrado Secondary Status データベースに問い合わせるために使用します。これらのレコードには、次のデータが含まれています。

- 現在は Intrado データベース内に存在する修正済みレコード。
- 修正するために顧客に戻されたエラー レコード。
- Intrado データベースから削除されたエラー レコード。

Intrado Secondary Status データベースに、修正済みのエラーを含む電話番号レコードを問い合わせることができます。

表 A-21 に、Intrado がサービスを提供している電話機の [Secondary Status] ページの説明を示します。

表 A-21　Secondary Status (Intrado Phones)

フィールド	説明
Find ELINS where...	検索条件を選択して、[Find] をクリックすると、Intrado のセカンダリ ステータス サーバに対する問い合わせの結果が一覧表示されます。

関連項目

- 「Intrado ERL (Search and List)」（P.A-31）
- 「Default ALI Values」（P.A-32）
- 「Intrado Schedule」（P.A-34）
- 「View ALI Discrepancies」（P.A-35）
- 「Cisco Emergency Responder の Intrado V9-1-1 Enterprise Services との併用」（P.5-1）

Intrado Schedule

[ERL]> [Intrado ERL] > [Intrado Schedule] を選択すると、[Intrado Schedule] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Intrado Schedule] ページは、ALI 更新要求とセカンダリ ステータス更新要求が Intrado に送信される曜日と時刻を指定するために使用します。ALI 更新要求では、新しく作成された TN レコードが Intrado に送信されます。セカンダリ ステータス更新要求では、修正されたエラーを含むレコードに関する情報を要求するクエリーが Intrado に送信されます。

表 A-22 に、[Intrado Schedule] ページの説明を示します。

表 A-22　Intrado Schedule

フィールド	説明	注
Add New Schedule	更新をスケジュールする曜日と時刻を指定します。 1. スイッチ ポートおよび電話機更新プロセスを実行する曜日を選択します。 2. プロセスを実行する時刻を選択します。00 時 00 分が真夜中です。時刻は 24 時制に基づきます。 3. このスケジュールをアクティブにする場合は、[Enable Schedule] ボックスをオンにします。 4. [ALI Update Schedule] と [Secondary Status Update Schedule] のどちらかを選択します。	少なくとも 1 日 1 回は Intrado 更新プロセスを実行することをお勧めします。ネットワーク トラフィックが増加することから、通常の営業時間外にプロセスを実行することをお勧めします。
[Add] ボタン	スケジュールをスケジュールのリストに追加するには、[Add] をクリックします。	
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	
[Update] ボタン	スケジュールに加えた変更を保存するには、既存のスケジュールが表示されているときに [Update] をクリックします。	既存のスケジュールが表示されている場合にのみ使用可能になります。

関連項目

- 「Intrado ERL (Search and List)」（P.A-31）
- 「Default ALI Values」（P.A-32）

- 「Secondary Status」（P.A-33）
- 「View ALI Discrepancies」（P.A-35）
- 「Cisco Emergency Responder の Intrado V9-1-1 Enterprise Services との併用」（P.5-1）

View ALI Discrepancies

[ERL]> [Intrado ERL] > [View ALI Discrepancies] を選択すると、[View ALI Discrepancies] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[View ALI Discrepancies] ページは、ローカル Emergency Responder データベースに保存された ALI データと、Intrado データベース内のこの ELIN に関する ALI データのレコード内での不一致を確認するために使用します。

表 A-23 に、[Find ALI Discrepancies] ページの説明を示します。

表 A-23　ALI Discrepancies

フィールド	説明
Find ELIN where...	探している ELIN を選択するための検索条件を入力します。 すべての ELIN を検索する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、ドロップダウン リストから検索するフィールドを選択して、検索関係（[is contains] や [begins with] など）を選択し、検索文字列を入力します。[Find] をクリックします。

関連項目

- 「Intrado ERL (Search and List)」（P.A-31）
- 「Default ALI Values」（P.A-32）
- 「Secondary Status」（P.A-33）
- 「Intrado Schedule」（P.A-34）
- 「Cisco Emergency Responder の Intrado V9-1-1 Enterprise Services との併用」（P.5-1）

View ALI Discrepancies for a Specific ELIN

[ERL]> [Intrado ERL] > [View ALI Discrepancies] を選択して、不一致を検索します。結果から特定の ELIN を選択すると、[View ALI Discrepancies for a specific ELIN] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[View ALI Discrepancies for a Specific ELIN] ページは、ローカル Emergency Responder データベースに保存された ALI データと、Intrado データベース内のこの ELIN に関する ALI データのレコード内での不一致を確認するために使用します。

表 A-24 に、[Find ALI Discrepancies for a specific ELIN] ページの説明を示します。

表 A-24　ALI Discrepancies for Specific ELIN

フィールド	説明
View Intrado ALI Discrepancies	
ALI Fields	ローカル Emergency Responder データベースと Intrado データベースからの ALI フィールド情報のリスト： • House Number • House Suffix • Street Name • Prefix Directional • Street Suffix • Post Directional • Community Name • State • Main NPA • Class of Service • Type of Service • Exchange • Customer Name • Order Number • Extract Date • County ID • Company ID • Zip Code • Zip Code Extension • Customer Code • Comments • Longitude • Latitude • Elevation • TAR Code • Location • Reserved

表 A-24　ALI Discrepancies for Specific ELIN（続き）

フィールド	説明
[Save] ボタン	変更をローカル Emergency Responder データベースに保存するには、[Save] をクリックします。
[Save Intrado ALI Info] ボタン	Intrado VUI データベースを更新するには、[Save Intrado ALI Info] をクリックします。
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。

関連項目

- 「Intrado ERL (Search and List)」（P.A-31）
- 「Default ALI Values」（P.A-32）
- 「Secondary Status」（P.A-33）
- 「Intrado Schedule」（P.A-34）
- 「Cisco Emergency Responder の Intrado V9-1-1 Enterprise Services との併用」（P.5-1）

ERL Migration Tool

[ERL]> [ERL Migration Tool] をクリックすると、[ERL Migration Tool] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[ERL Migration Tool] ページは、従来の ERL データから Intrado ERL データに、またはその逆方向に ERL を移行するために使用します。

表 A-25 に、[ERL Migration Tool] ページの説明を示します。

表 A-25　ERL Migration Tool

フィールド	説明
Status	ステータス メッセージが表示されます。
ERL Search Parameter	
Find	検索条件を選択して、[Find] をクリックすると、既存の従来の ERL か Intrado ERL のどちらかが一覧表示されます。 検索結果リストから、移行する ERL を選択することができます。

表 A-25　ERL Migration Tool（続き）

フィールド	説明
[Migrate to Intrado ERL] ボタン	従来の ERL を検索するときに、Intrado に移行する ERL を選択することができます。 [Migrate to Intrado ERL] ボタンをクリックすると、選択したすべての ERL に関する Intrado ルート ポイントを選択することができます。
Migrate to Regular ERL	Intrado ERL を検索するときに、従来の ERL データに移行する ERL を選択することができます。 [Migrate to Regular ERL] ボタンをクリックすると、ルート ポイントを入力し、ERL がテスト ERL かどうかを指定して、ERL をテストできます。

関連項目

- 「Intrado ERL (Search and List)」（P.A-31）
- 「Default ALI Values」（P.A-32）
- 「Secondary Status」（P.A-33）
- 「Intrado Schedule」（P.A-34）
- 「View ALI Discrepancies」（P.A-35）
- 「Cisco Emergency Responder の Intrado V9-1-1 Enterprise Services との併用」（P.5-1）
- 「ERL データの移行」（P.5-7）

SNMP Settings

[Phone Tracking]>[SNMP Settings] を選択すると、[SNMP Settings] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者またはネットワーク管理者の権限が必要です。

説明

[SNMP Settings] ページは、スイッチで使用される SNMP read コミュニティ ストリングを定義するために使用します。

表 A-26 に、[SNMP Settings] ページの説明を示します。

表 A-26　[SNMP Settings] ページ

フィールド	説明	注
Add SNMP Community Setting		
IP Address/Host Name	SNMP read コミュニティ ストリングを定義するスイッチの IP アドレスまたはホスト名。 すべてのスイッチに対して同じ read コミュニティ ストリングを使用する場合は、*.*.*.*. というエントリを定義するだけで済みます。 スイッチのセットに対して別々の read コミュニティ ストリングを使用する場合は、変数と範囲を使用して、それぞれのセットを定義することができます。たとえば、10.1.115.0 ～ 10.1.125.0 の 10 台のスイッチがある場合は、IP アドレスとして 10.1.115-125.0 を使用することができます。*.*.115-125.* のように、範囲と変数を組み合わせることもできます。	このページでは、スイッチを定義するのではなく、read コミュニティ ストリングに IP アドレス パターンを関連付けるだけです。 Emergency Responder は、[LAN Switch Details] ページで特定されたスイッチと一緒にこのストリングを使用します。詳細については、「LAN Switch Details」（P.A-44）を参照してください。 1 つの IP アドレスに対して 2 つ以上のパターンが一致すると、Emergency Responder では、最も近い一致パターンに関連付けられた SNMP ストリングが使用されます。
Timeout	Emergency Responder で試行されたスイッチへの接続が失敗と見なされる秒単位の時間。詳細については、再試行の説明を参照してください。	デフォルトは 10 秒です。最適値は 10 ～ 15 秒です。
Maximum Retry Attempts	Emergency Responder がスイッチへの接続を試みる回数。 再試行ごとに、前回のタイムアウトが 2 倍され、スイッチが応答を返すのに十分な時間が確保されます。たとえば、タイムアウトとして 10 を指定した場合は、最初の試行が 10 秒でタイムアウトし、2 回目の試行が 20 秒でタイムアウトし、3 回目の試行が 40 秒でタイムアウトするといった具合です。	デフォルトは 2 回です。この数値には最初の試行が含まれません。つまり、再試行回数が 2 の場合は、Emergency Responder が最大で 3 回（最初の試行 + 2 回の再試行）スイッチへの接続を試みます。 最適値は 2 ～ 3 回です。
Read Community	スイッチの SNMP read コミュニティ ストリング。	デフォルトは、SNMP 設定リストでカバーされない IP アドレスを表す public です。
[Insert] ボタン	エントリを SNMP 設定のリストに追加するには、[Insert] をクリックします。	
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	
SNMP Settings	すでに定義された SNMP 設定のリスト。 エントリを変更するには、そのエントリに関連付けられたリンクのいずれかをクリックして、ページ上部にある編集ボックスに詳細をロードします。その後で、変更を加えて、[Update] をクリックします。 エントリを削除するには、そのエントリの [Delete] アイコンをクリックします。	
[Add New] ボタン	別の SNMP 設定を追加するには、[Add New] をクリックします。	
[Update] ボタン	既存の SNMP 設定に加えた変更を保存するには、[Update] をクリックします。	既存の設定が表示されている場合にのみ使用可能になります。

関連項目

- 「SNMP 接続の設定」（P.4-45）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Phone Tracking Schedule

[Phone Tracking]>[Schedule] を選択すると、[Phone Tracking Schedule] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者またはネットワーク管理者の権限が必要です。

説明

[Phone Tracking Schedule] ページは、ネットワークから電話機とスイッチに関する情報を更新する Cisco Emergency Responder（Emergency Responder）のスケジュールを定義するために使用します。Emergency Responder は、次の 2 つのプロセスを使用してネットワーク情報を更新します。

- 電話機トラッキング：Cisco Unified Communications Manager に登録された電話機とスイッチから取得されたロケーション情報の定期比較。電話機が移動した場合、Emergency Responder によりその電話機の ERL が更新されます。
- スイッチ ポートおよび電話機更新：電話機トラッキング プロセス + より広範囲のネットワーク スイッチのチェック。新しいまたは変更されたスイッチ モジュール（追加または削除されたポート）を特定することができます。ERL 管理者により、新しいポートへの ERL 割り当てが更新されることを確認してください。

表 A-27 に、[Phone Tracking Schedule] ページの説明を示します。

表 A-27　[Phone Tracking Schedule] ページ

フィールド	説明	注
Incremental Phone Tracking		
Incremental Phone Tracking Interval	既存の電話機ロケーションを更新する分単位の時間間隔。この定期更新によって、移動された電話機が特定され、正しい ERL に割り当てられることが保証されます。 このフィールドに加えた変更を保存するには、[Update] をクリックします。	デフォルトは 30 分です。 定義可能な時間間隔の範囲は 5 ～ 300 分です。
Add New Schedule	追加するスケジュールを入力します。 1. スイッチ ポートおよび電話機更新プロセスを実行する曜日を選択します。 2. プロセスを実行する時刻を選択します。00 時 00 分が真夜中です。時刻は 24 時制に基づきます。	スイッチ ポートおよび電話機更新プロセスを少なくとも 1 日 1 回実行することをお勧めします。ネットワーク トラフィックが増加することから、通常の営業時間外にプロセスを実行することをお勧めします。
[Insert] ボタン	スケジュールをスケジュールのリストに追加するには、[Insert] をクリックします。	
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	
[Update] ボタン	スケジュールに加えた変更を保存するには、既存のスケジュールが表示されているときに [Update] をクリックします。	既存のスケジュールが表示されている場合にのみ使用可能になります。

表 A-27　[Phone Tracking Schedule] ページ（続き）

フィールド	説明	注
Switch-Port and Phone Update Schedule	定義済みのスケジュールのリスト。 スケジュールを変更するには、[Hour] リンク、[Minute] リンク、または [Edit] アイコンをクリックして、そのスケジュールをリストの上部にある [Modify Schedule] エリアにロードします。その後で、変更を加えて、[Update] をクリックします。 スケジュールを削除するには、そのスケジュールの [Delete] アイコンをクリックします。	スケジュールがオーバーラップしている場合は、1 つのスケジュールしか実行されません。
[Add New] ボタン	別のスケジュールを追加するには、[Add New] をクリックします。	

関連項目

- 「電話機トラッキングとスイッチ更新スケジュールの定義」（P.4-47）
- 「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Cisco Unified Communications Manager Clusters

[Phone Tracking]>[Cisco Unified Communications Manager] を選択すると、[Cisco Unified Communications Manager Clusters] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者またはネットワーク管理者の権限が必要です。

説明

[Cisco Unified Communications Manager Clusters] ページは、この Emergency Responder グループが緊急コールを処理する Cisco Unified Communications Manager クラスタを特定するために使用します。1 つの Cisco Unified Communications Manager クラスタを 1 つの Emergency Responder グループに割り当てます。Emergency Responder は、これらの Cisco Unified Communications Manager サーバに登録された電話機のリストを入手して、それらの移動を追跡します。

表 A-28 に、[Cisco Unified Communications Manager Clusters] ページの説明を示します。

表 A-28　[Cisco Unified Communications Manager Clusters] ページ

フィールド	説明	注
Add New Cisco Unified Communications Manager Cluster		
Cisco Unified Communications Manager	Cisco Unified Communications Manager サービスと SNMP サービスを実行している Cisco Unified Communications Manager サーバの IP アドレスまたは DNS 名。 Cisco Unified Communications Manager クラスタごとに 1 つずつのサーバを追加します。Emergency Responder はクラスタ内の他のサーバを識別することができます。指定された Cisco Unified Communications Manager サーバが、属しているクラスタを表します。	定義済みの Cisco Unified Communications Manager サーバが表示されているときに、Emergency Responder に [CCM List] リンクが表示されます。[CCM List] をクリックすると、選択したサーバと同じクラスタに属している Cisco Unified Communications Manager サーバのリストが表示されます。 IP アドレス /DNS 名が設定されていれば、それを変更することができません。
CTI Manager	指定された Cisco Unified Communications Manager サーバで使用される CTI Manager の IP アドレスまたは DNS 名。	
CTI Manager User Name	Emergency Responder で使用するために Cisco Unified Communications Manager サーバで作成されたユーザの名前。	このユーザは、個別の特性とデバイス割り当てを持っている必要があります。詳細については、「Cisco Emergency Responder Cisco Unified CallManager ユーザの作成」（P.3-21）を参照してください。
CTI Manager Password	ユーザのパスワード。	
Backup CTI Manager 1	指定された Cisco Unified Communications Manager サーバで使用されるバックアップ CTI Manager の IP アドレスまたは DNS 名。	
Backup CTI Manager 2	指定された Cisco Unified Communications Manager サーバで使用されるバックアップ CTI Manager の IP アドレスまたは DNS 名。	
Telephony Port Begin Address	オンサイト アラート（セキュリティ）担当者の呼び出しに使用される最初の CTI ポートの番号。緊急コールが発信されると、Emergency Responder が、ここで設定されたテレフォニー ポートを使用して、発信 ERL のオンサイト アラート担当者を呼び出します。	事前に、Cisco Unified Communications Manager でこのポートを作成しておく必要があります。詳細については、「必要な CTI ポートの作成」（P.3-8）を参照してください。
Number of Telephony Ports	CTI ポートの数。Cisco Unified Communications Manager で作成した CTI ポートの数を入力します。ポートの数は、Emergency Responder からオンサイト アラート担当者に発信可能な同時コールの数です。	使用されるポートは、開始ポートから順番です。たとえば、開始ポートとして 3000 を、ポート数として 4 を入力した場合は、Emergency Responder によって 3000、3001、3002、および 3003 が使用されます。
Enable Secure Connection		
[Enable Secure Connection] チェックボックス	セキュア接続をイネーブルにするには、このチェックボックスをオンにします。セキュア接続をイネーブルにした場合にのみ、このセクションの他のフィールドにデータを入力することができます。	
TFTP Server IP Address	TFTP サーバの IP アドレス。	

表 A-28　[Cisco Unified Communications Manager Clusters] ページ（続き）

フィールド	説明	注
TFTP Server Port	TFTP サーバのポート。	
Backup TFTP Server IP Address	追加する Cisco Unified CM ノードのバックアップ TFTP サーバの IP アドレス。	
CAPF Server IP Address	CAPF サーバの IP アドレス。	
CAPF Server Port	CAPF サーバのポート。	
Instance ID for Publisher	パブリッシャ ノードのインスタンス ID。	
Secure Authentication String for Publisher	パブリッシャ ノードのセキュア認証文字列。	
Instance ID for Subscriber	サブスクライバ ノードのインスタンス ID。	
Secure Authentication String for Subscriber	サブスクライバ ノードのセキュア認証文字列。	
AXL Settings		
AXL Username	AXL クエリーの実行権限を持つ Cisco Unified Communications Manager 上のアプリケーション ユーザのユーザ名。	
AXL Password	AXL クエリーの実行権限を持つ Cisco Unified Communications Manager 上のアプリケーション ユーザのパスワード。	
AXL Port Number	Cisco Unified Communication Manger 上のアプリケーションによって使用されるポート番号。デフォルト値は 8443 です。	
[Insert] ボタン	新しい Cisco Unified Communications Manager サーバをサーバのリストに追加するには、[Insert] をクリックします。	
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	
[Update] ボタン	サーバに加えた変更を保存するには、既存のサーバが表示されているときに [Update] をクリックします。	既存のサーバが表示されている場合にのみ使用可能になります。既存のサーバが表示されているときに [Insert] ボタンの代わりに表示されます。
Cisco Unified Communications Manager Clusters		
[Add New] ボタン	別の Cisco Unified Communications Manager サーバを追加するには、[Add New] をクリックします。	
Cisco Unified Communications Manager list	この Emergency Responder グループに対して定義された Cisco Unified Communications Manager サーバのリスト。サーバの Emergency Responder 設定を表示して変更するには、サーバ リンクまたは [Edit] アイコンをクリックします。サーバを削除するには、[Delete] アイコンをクリックします。	

関連項目

- 「Cisco Unified Communications Manager クラスタの指定」（P.4-26）
- 「Cisco Emergency Responder Cisco Unified CallManager ユーザの作成」（P.3-21）
- 「必要な CTI ポートの作成」（P.3-8）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

LAN Switch Details

[Phone Tracking]>[LAN Switch Details] を選択すると、[LAN Switch Details] ページが表示されます。

（注） Cisco Emergency Responder は、LAN スイッチの SNMP バージョン 1、バージョン 2、およびバージョン 2C をサポートします。

許可の要件

このページにアクセスするには、システム管理者またはネットワーク管理者の権限が必要です。

説明

[LAN Switch Details] ページは、Emergency Responder によって管理されるスイッチを追加、削除、または変更するために使用します。電話機を接続するすべてのスイッチが特定されていることを確認してください。このページでスイッチを入力する場合は、スイッチ ポートを ERL にしか割り当てることができません。未定義のスイッチまたはポートに接続された電話機は Emergency Responder に位置未確認の電話機として一覧表示され、デフォルト ERL に割り当てられます。

表 A-29 に、[LAN Switch Details] ページの説明を示します。

表 A-29　[LAN Switch Details] ページ

フィールド	説明
LAN Switch Details	
Switch Host Name/IP Address	スイッチの IP アドレスまたは DNS 名。
Description	このスイッチの説明。
Enable CAM-based Phone Tracking	自らをネットワークにアナウンスするときに Cisco Discovery Protocol（CDP）を使用しない電話機をこのスイッチに接続する可能性がある場合に、このチェックボックスをオンにします。非 CDP 電話機の場合は、Emergency Responder がスイッチの Content Addressable Memory（CAM）情報を使用して電話機を特定します。
Use port description as port location	スイッチの [Location] フィールドに設定されたスイッチ ポートの説明を表示する場合に、このチェックボックスをオンにします。

表 A-29　[LAN Switch Details] ページ（続き）

フィールド	説明
[Insert] ボタン	スイッチをスイッチのリストに追加するには、[Insert] をクリックします。 [Insert] をクリックすると、Emergency Responder から、今すぐスイッチ上でスイッチ ポートおよび電話機更新プロセスを実行するかどうかが尋ねられます。今すぐプロセスを実行する場合は [OK] をクリックし、すぐにプロセスを実行せずに設定にスイッチを追加するだけの場合は [Cancel] をクリックします。 （注）　すぐにプロセスを実行しない場合のプロセスの実行方法については、「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）を参照してください。
[Update] ボタン	スイッチに加えた変更を保存するには、既存のスイッチが表示されているときに [Update] をクリックします。
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。
LAN Switches	
LAN Switch list	定義済みのスイッチのリスト。スイッチに関する設定を表示して変更するには、スイッチの IP アドレス /DNS 名をクリックするか、[Edit] アイコンをクリックします。スイッチを削除するには、[Delete] アイコンをクリックします。
[Add LAN Switch] ボタン	別のスイッチを追加するには、[Add LAN Switch] をクリックします。
Export	スイッチ定義を別のファイルにエクスポートするには、[Export] リンクをクリックします。詳細については、「Export LAN Switch」（P.A-45）を参照してください。
Import	スイッチのリストを Emergency Responder 設定にインポートするには、[Import] リンクをクリックします。このリストは、ネットワーク管理ソフトウェアからエクスポートすることができます。詳細については、「Import LAN Switch」（P.A-46）を参照してください。

関連項目

- 「LAN スイッチの指定」（P.4-48）
- 「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）
- 「位置未確認の電話の識別」（P.4-62）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Export LAN Switch

[LAN Switch Details] ページ（[Phone Tracking]>[LAN Switch Details] を選択したときに表示される）で [Export] をクリックすると、[Export LAN Switch] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者またはネットワーク管理者の権限が必要です。

説明

[Export LAN Switch] ページは、Emergency Responder スイッチ設定を含むファイルを作成するために使用します。

Emergency Responder 内のいくつかのスイッチ エントリを更新する必要がある場合は、スイッチ情報をエクスポートして、スプレッドシートを使用してエクスポート ファイルの内容を変更してから、そのファイルを再度インポートします。

ダウンロード ユーティリティを使用して、ファイルをローカル システムにダウンロードすることもできます。詳細については、「ファイルのダウンロード」（P.4-7）を参照してください。

表 A-30 に、[Export LAN Switch] ページの説明を示します。

表 A-30　[Export LAN Switch] ページ

フィールド	説明
Select Export Format	ファイルに使用される形式（CSV など）。
Enter Export File Name	作成するファイルの名前。ファイル拡張子を含めないでください。
[Export] ボタン	ファイルを作成するには、[Export] をクリックします。[Status] ボックスにエクスポートのステータスが表示されます。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。
Download	
Select a File to Download	ファイルをローカル システムにダウンロードするには、プルダウン メニューを使用して LAN スイッチ設定ファイルを選択し、[Download] をクリックします。

関連項目

- 「スイッチ情報のエクスポート」（P.4-51）
- 「ファイルのダウンロード」（P.4-7）
- 「スイッチのグループのインポート」（P.4-50）
- 「LAN Switch Details」（P.A-44）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Import LAN Switch

[LAN Switch Details] ページ（[Phone Tracking]>[LAN Switch Details] を選択したときに表示される）で [Import] をクリックすると、[Import LAN Switch] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者またはネットワーク管理者の権限が必要です。

説明

[Import LAN Switch] ページは、一度に複数のスイッチを Emergency Responder 設定に追加するために使用します。過去にエクスポートしたファイル、または、ローカル システム上で作成してアップロード ユーティリティを使用してアップロードしたファイルをインポートすることができます。詳細については、「ファイルのアップロード」（P.4-7）を参照してください。

表 A-31 に、[Import LAN Switch] ページの説明を示します。

表 A-31　[Import LAN Switch] ページ

フィールド	説明
Select Import Format	インポートするファイルに使用される形式を選択します。 形式を選択したら、[view sample file] をクリックして、予想される形式と値のシーケンスの例を確認します。このサンプル情報を使用して、スプレッドシートでインポート ファイルを作成したり、ネットワーク管理ソフトウェアで必要な形式が作成できるかどうかを判断したりします。
Select File to Import	データをインポートするファイルを選択します。 ファイルをインポートするには、このページで指定されたフォルダにファイルを配置する必要があります。
[Upload] ボタン	ファイルをローカル システムからアップロードするには、[Upload] をクリックします。詳細については、「ファイルのアップロード」（P.4-7）を参照してください。
[Import] ボタン	インポート ファイル内の情報から Emergency Responder 設定にデータを追加するには、[Import] をクリックします。 Emergency Responder から、インポート先のスイッチ上で電話機トラッキングを実行するかどうかが尋ねられます。電話機トラッキングを実行しないとスイッチ ポートを設定することができないため、通常は、[OK] を選択する必要があります。[Cancel] を選択した場合は、Emergency Responder によってスイッチはインポートされますが、電話機トラッキング プロセスは実行されません。 **（注）** 電話機トラッキング プロセスを実行しない場合は、ファイルのインポート後に、スイッチ ポートおよび電話機更新プロセスを実行してください。「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）を参照してください。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。
Import Status	ステータス情報が表示されるテキスト ボックス。

関連項目

- 「スイッチのグループのインポート」（P.4-50）
- 「スイッチ情報のエクスポート」（P.4-51）
- 「ファイルのアップロード」（P.4-7）
- 「LAN Switch Details」（P.A-44）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Run Switch-Port and Phone Update

[Phone Tracking/Run Switch-Port & Phone Update] を選択すると、ダイアログボックスが開いて「Press Okay to run Switch-Port and Phone update process on Emergency Responder」というプロンプトが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Run Switch-Port and Phone Update] ページは、スイッチ ポートおよび電話機更新プロセスを手動で実行するために使用します。

関連項目

- 「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）
- 「電話機トラッキングとスイッチ更新スケジュールの定義」（P.4-47）
- 「位置未確認の電話の識別」（P.4-62）
- 「Cisco Emergency Responder のスイッチ要件について」（P.4-44）

Switch Port Details

[ERL Membership]>[Switch Ports] を選択すると、[Switch Port Details] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Switch Port Details] ページは、スイッチ ポートを ERL に割り当てるために使用します。この割り当てを使用すれば、Emergency Responder が設定済みのポート経由でネットワークに接続している電話機に正しい ERL を割り当てることができます。

スイッチ ID、モジュール ID、およびポート ID の組み合わせで一意に識別可能なポートが実装された Cisco Catalyst 3750 などのスイッチをサポートするために、Emergency Responder 8.6 では次のポート命名規則が使用されます。

- IfName : スイッチ CLI と同様にポートに付けられた新しいフィールド表示名（Fa1/5 や Gi2/0/1 など）。
  - ポート ID : モジュール ID/ ポート ID の代わりに使用されます。{optional} <<スイッチ ID（Cisco Catalyst 3750 などのスタッカブル スイッチの場合）>>/ {optional} <<スイッチ内のモジュールの相対位置>> / <<モジュール内のポートの相対位置>> が含まれています。
- ポート IfName に対する検索が、モジュール ID/ ポート ID 検索の代わりに使用されます。

表 A-32 に、[Switch Port Details] ページの説明を示します。

表 A-32　[Switch Port Details] ページ

フィールド	説明	注
Switch Port Search Parameters		
Find ports where...	表示または設定するポートを選択するための検索条件を入力します。 すべてのポートを表示する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、次の手順に従います。 • すべての条件と一致するコールのみを選択するように指定する場合は [All] を選択します（AND 検索）。いずれかの検索条件と一致するコールを選択するように指定する場合は [Any] を選択します（OR 検索）。プルダウン メニューから、検索するフィールド（[ERL Name] や [Phone MAC Address] など）を選択して、検索関係（[contains] や [starts with] など）を選択し、検索文字列を入力して、1 ページに表示する結果数を選択します。 • フィールドの組み合わせを検索するには、**プラス** アイコン（+）をクリックして新しい検索パラメータを追加します。（検索パラメータを削除するには、**マイナス** アイコン（–）をクリックします）。 • すべての検索パラメータを入力したら、[Find] をクリックします。	ポートを設定する場合は、事前に、[Find] ボタンを使用してポートのリストを生成しておく必要があります。
Switch Ports	検索条件と一致するスイッチ ポートのリスト。1 行 1 ポートで表示されます。 選択したポートに ERL を割り当てるには、スイッチ詳細の左側にあるチェックボックスをオンにして、テキスト ボックスに ERL 名を入力するか、[Search ERL] をクリックして ERL を検索し、選択してから、[Assign ERL] をクリックします。 ポートの電話機ロケーションを表示して更新するには、そのポートの [Location] 列で [View] リンクをクリックします。 リストに表示されたフィールドを変更したり、その順序を変更したりするには、[Edit View] をクリックします。このアクションによって、別の [Edit View] ページが開きます。 • フィールドを追加するには、[Available Fields] リストでそれを選択して [>]（右矢印）をクリックします。 • フィールドを削除するには、[Selected Fields] リストでそれを選択して [<]（左矢印）をクリックします。 **（注）**　テーブル ビューから ERL 名は削除できません。 [Edit Table View] ページの変更を保存するには、[Apply] をクリックします。ウィンドウを閉じるには、[Close] をクリックします。	Emergency Responder には、一度に最大 1,000 件のスイッチ ポート レコードが表示されます。検索結果が 1,000 スイッチ ポートを超えた場合は、検索を絞り込むためのエラー メッセージが表示されます。 大量のポートが検索条件と一致した場合は、複数ページにわたって表示されます。ページの下部にある [First]、[Previous]、[Next]、および [Last] リンクを使用してページ間を移動します。[Page] フィールドに特定のページ番号を入力して Enter を押せば、そのページに移動することもできます。
Export	ERL とスイッチ ポート間の設定を別のファイルにエクスポートするには、[Export] をクリックします。詳細については、「Export Switch Ports」（P.A-50）を参照してください。	
Import	ERL/ポート マッピングのセットを Emergency Responder 設定にインポートするには、[Import] をクリックします。詳細については、「Import Switch Ports」（P.A-51）を参照してください。	

関連項目

- 「スイッチ ポートの設定」（P.4-54）
- 「LAN スイッチの指定」（P.4-48）
- 「スイッチ ポートおよび電話機更新プロセスの実行（手動）」（P.4-52）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Export Switch Ports

[Switch Port Details] ページ（[ERL Membership]>[Switch Ports] を選択したときに表示される）で [Export] をクリックすると、[Export Switch Ports] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Export Switch Ports] ページは、Emergency Responder スイッチ ポート設定を含むファイルを作成するために使用します。

大量のポート /ERL 割り当てを変更する必要がある場合は、ファイルをエクスポートして、スプレッドシートを使用してファイルの内容を変更してから、そのファイルを再度インポートします。

ダウンロード ユーティリティを使用してファイルをダウンロードして、それをローカル システム上で変更してから、アップロード ユーティリティを使用してアップロードすることもできます。詳細については、「ファイルのダウンロード」（P.4-7）を参照してください。

表 A-33 に、[Export Switch Ports] ページの説明を示します。

表 A-33　[Export Switch Ports] ページ

フィールド	説明
Select Export Format	ファイルに使用される形式（CSV など）。
Enter Export File Name	作成するファイルの名前。ファイル拡張子を含めないでください。
[Export] ボタン	ファイルを作成するには、[Export] をクリックします。[Status] ボックスにエクスポートのステータスが表示されます。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。
Download	
Select a File to Download	ファイルをローカル システムにダウンロードするには、プルダウン メニューを使用してファイルを選択し、[Download] をクリックします。

関連項目

- 「スイッチ ポート情報のエクスポート」（P.4-57）
- 「ファイルのダウンロード」（P.4-7）
- 「少数のポートの一括設定」（P.4-56）
- 「Switch Port Details」（P.A-48）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Import Switch Ports

[Switch Port Details] ページ（[ERL Membership]>[Switch Ports] を選択したときに表示される）で [Import] をクリックすると、[Import Switch Ports] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Import Switch Ports] ページは、一度に複数のスイッチ ポート設定を Emergency Responder 設定に追加または更新するために使用します。スイッチ ポート設定は、ポートと ERL のマッピングです。

スイッチ ポート インポート ファイルを作成するには、次の手順を実行します。

手順

ステップ 1　スイッチ ポート詳細をエクスポートします。

ステップ 2　これらのレコードの ERK フィールドを変更して、ファイルを保存します。

ステップ 3　スイッチ ポート インポートを使用してファイルをインポートします。

ローカル システム上でインポート ファイルを作成してから、そのファイルをアップロード ユーティリティを使用してアップロードすることもできます。詳細については、「ファイルのアップロード」（P.4-7）を参照してください。

表 A-34 に、[Import Switch Ports] ページの説明を示します。

表 A-34　[Import Switch Ports] ページ

フィールド	説明
Select Import Format	インポートするファイルに使用される形式を選択します。 形式を選択したら、[view sample file] をクリックして、予想される形式と値のシーケンスの例を確認します。このサンプル情報を使用してスプレッドシートでインポート ファイルを作成することができますが、Emergency Responder からスイッチ ポート情報をエクスポートして、スプレッドシート プログラムを使用してエクスポート ファイルを変更してから、そのファイルをインポートする方が簡単です。 **（注）**　スイッチ ポート情報のエクスポート方法については、「スイッチ ポート情報のエクスポート」（P.4-57）を参照してください。
Select File to Import	データをインポートするファイルを選択します。
[Upload] ボタン	ファイルをローカル システムからアップロードするには、[Upload] をクリックします。詳細については、「ファイルのアップロード」（P.4-7）を参照してください。
[Import] ボタン	インポート ファイル内の情報から Emergency Responder 設定にデータを追加するには、[Import] をクリックします。インポート ファイル内の ERL 割り当てによって、Emergency Responder 設定内にすでに存在する割り当てが上書きされます。 **（注）**　ポート ERL 設定は、ポート設定をインポートする前に Emergency Responder でポートが検出された場合にのみ更新されます。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。
Import Status	ステータス情報が表示されるテキスト ボックス。

関連項目

- 「少数のポートの一括設定」（P.4-56）
- 「ファイルのアップロード」（P.4-7）
- 「スイッチ ポート情報のエクスポート」（P.4-57）
- 「Switch Port Details」（P.A-48）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Find and List IP Subnets

[ERL Membership]>[IP Subnets] を選択すると、[Find and List IP Subnets] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Find and List IP Subnets] ページは、変更または削除する IP サブネットを検索して表示するために使用します。このページから新しい IP サブネットを追加するためにナビゲートすることもできます。

表 A-35 に、[Find and List IP Subnets] ページの説明を示します。

表 A-35　[Find and List IP Subnets] ページ

フィールド	説明
IP Subnet Search Parameters	
Find IP Subnets where...	特定の IP サブネットを一覧表示するには、検索条件を選択して [Find] をクリックします。すべての IP サブネットを一覧表示するには、条件を入力せずに [Find] をクリックします。
IP Subnets	
IP Subnets list	IP サブネット検索の結果が表示されます。IP サブネットが見つかった場合は、そのサブネット ID、サブネット マスク、ERL 名、およびロケーションが表示されます。 その IP サブネットを変更するには、上記のレコードのいずれかをクリックするか、[Edit] アイコンをクリックします。[Configure IP Subnets] ページが表示されます。[Location] フィールドまたは [ERL Name] フィールドを変更します。 **（注）** 既存の IP サブネットを変更するときに、サブネット ID またはサブネット マスクは変更できません。 IP サブネットに加えた変更を保存するには、[Update] をクリックします。 任意のレコード内で [View Phones] アイコンをクリックすると、すべての IP サブネット電話機が表示されます。[IP Subnet Phones] ページに、IP サブネット内で検出された電話機のリストが表示されます。「IP Subnet Phones」（P.A-54）を参照してください。 IP サブネットを削除するには、[Delete] アイコンをクリックします。[Delete] をクリックすると、Cisco Emergency Responder から、スイッチ ポートおよび電話機更新プロセスを今すぐ実行するかどうかが尋ねられます。すぐにプロセスを実行する場合は [OK] をクリックし、すぐにプロセスを実行せずに IP サブネットを削除する場合は [Cancel] をクリックします。
[Cancel Changes] ボタン	[Configure IP Subnets] ページに加えた変更をキャンセルするには、[Cancel Changes] をクリックします。 **（注）** [Cancel Changes] ボタンは、[Configure IP Subnets] ページにのみ表示されます。

表 A-35　[Find and List IP Subnets] ページ（続き）

フィールド	説明
Add New IP Subnet	新しい IP サブネットを設定するには、[Add New IP Subnet] をクリックします。[Configure IP Subnets] ページが表示されます。詳細については、「Configure IP Subnet」（P.A-53）を参照してください。
Export	IP サブネット設定情報を含むファイルを作成するには、[Export] をクリックします。[Export IP Subnet] ページが表示されます。詳細については、「Export IP Subnets」（P.A-54）を参照してください。
Import	ファイルから IP サブネット設定情報をインポートするには、[Import] をクリックします。[Import IP Subnet] ページが表示されます。詳細については、「Import IP Subnets」（P.A-55）を参照してください。

Configure IP Subnet

[Configure IP Subnet] ページにアクセスするには、[ERL Membership]>[IP Subnets] を選択して [Add New IP Subnet] リンクを選択します。[Configure IP Subnet] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Configure IP Subnet] ページは、IP サブネットとその ERL を手動で定義するために使用します。次の条件のいずれかが該当する場合は、IP サブネットを手動で定義する必要があります。

- Emergency Responder で、電話機が無線の場合などに、電話機のタイプを自動的に追跡できない。電話機のサポートについては、「ネットワークのハードウェアおよびソフトウェアの要件」（P.1-4）を参照してください。
- CiscoWorks IP Telephony Environment Monitor（ITEM）2.0 を使用して、Emergency Responder システムの動作状態を監視している。サブネットを作成し、テスト ERL を設定してそれらをサブネットに関連付け、模擬電話機をそのテスト ERL に属するように設定している。「IP サブネットベースの ERL の設定」（P.4-38）と「擬似電話機の追加」（P.4-67）を参照してください。

表 A-36 に、[Configure IP Subnet] ページの説明を示します。

表 A-36　[Configure IP Subnet] ページ

フィールド	説明
Add New IP Subnet	
Subnet ID	定義するサブネットの IP アドレス。
Subnet Mask	定義するサブネットのマスク。
Location（任意）	新しい IP サブネットのロケーション。
ERL Name	サブネットに割り当てる ERL。有効な ERL 名を入力するか、[Search ERL] をクリックして ERL を検索して選択します。

表 A-36　[Configure IP Subnet] ページ（続き）

フィールド	説明
[Insert] ボタン	サブネットを追加するには、[Insert] をクリックします。 [Insert] をクリックすると、Emergency Responder から、今すぐスイッチ上でスイッチ ポートおよび電話機更新プロセスを実行するかどうかが尋ねられます。今すぐプロセスを実行する場合は [OK] をクリックし、すぐにプロセスを実行せずに IP サブネットを設定に追加するだけの場合は [Cancel] をクリックします。
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。

関連項目

- 「IP サブネットベースの ERL の設定」（P.4-38）
- 「擬似電話機の追加」（P.4-67）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

IP Subnet Phones

[ERL Membership/ IP Subnets] を選択して、IP サブネット検索から返された任意のレコードに含まれる [View Phones] アイコンをクリックすると、[IP Subnet Phones] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[IP Subnet Phones] ページは、Emergency Responder によって検出されたすべての IP サブネット電話機を表示するために使用します。

[IP Subnet Phones] ページには、IP サブネットごとのサブネット ID とサブネット マスクが表示され、IP サブネット内で追跡されたすべての電話機と最後の電話機が追跡された時間が一覧表示されます。

関連項目

- 「Find and List IP Subnets」（P.A-52）
- 「Configure IP Subnet」（P.A-53）

Export IP Subnets

[Export IP Subnets] ページにアクセスするには、[ERL Membership]>[IP Subnets] を選択します。[Find and List IP Subnets] ページで、[Export] リンクをクリックします。[Export IP Subnets] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Export IP Subnets] ページは、Emergency Responder エクスポート IP サブネット設定を含むファイルを作成するために使用します。

大量のエクスポート IP サブネットを更新する必要がある場合は、電話機データをエクスポートして、スプレッドシートを使用してファイルの内容を変更してから、そのファイルを再度インポートします。

ダウンロード ユーティリティを使用してファイルをダウンロードして、それをローカル システム上で変更してから、アップロード ユーティリティを使用してアップロードすることもできます。詳細については、「ファイルのダウンロード」（P.4-7）を参照してください。

表 A-37 に、[Export IP Subnets] ページの説明を示します。

表 A-37　[Export IP Subnets] ページ

フィールド	説明
Select Export Format	インポートするファイルに使用される形式を選択します。 形式を選択したら、[view sample file] をクリックして、予想される形式と値のシーケンスの例を確認します。このサンプル情報を使用して、スプレッドシートでインポート ファイルを作成します。
Enter Export File Name	作成するファイルの名前。ファイル拡張子を含めないでください。
[Export] ボタン	インポート ファイルから Emergency Responder 設定にデータを追加するには、[Export] をクリックします。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。
Download	
Select a File to Download	ファイルをローカル システムにダウンロードするには、プルダウン メニューを使用してファイルを選択し、[Download] をクリックします。

関連項目

- 「ファイルのダウンロード」（P.4-7）
- 「Find and List IP Subnets」（P.A-52）
- 「Import IP Subnets」（P.A-55）

Import IP Subnets

[Import IP Subnets] ページにアクセスするには、[ERL Membership]>[IP Subnets] を選択します。[Find and List IP Subnets] ページで、[Import] リンクをクリックします。[Import IP Subnets] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Import IP Subnet] ページは、データが定義されているファイルから一度に複数の IP サブネット電話機を作成または更新するために使用します。このファイルは、必要な形式のいずれかで情報を保存可能なスプレッドシートを使用して作成します。インポート ファイルを作成または更新する前に、このページのサンプルを確認してください。

大量の IP サブネット電話機を更新する必要がある場合は、電話機データをエクスポートして、エクスポート ファイルを更新し、そのファイルを再度インポートします。

ローカル システムにダウンロードしたファイルを変更してアップロードすることもできます。詳細については、「ファイルのアップロード」（P.4-7）を参照してください。

表 A-38 に、[Import IP Subnets] ページの説明を示します。

表 A-38　[Import IP Subnets] ページ

フィールド	説明
Select Import Format	インポートするファイルに使用される形式を選択します。 形式を選択したら、[view sample file] をクリックして、予想される形式と値のシーケンスの例を確認します。このサンプル情報を使用して、スプレッドシートでインポート ファイルを作成または更新します。
Select File to Import	データをインポートするファイルを選択します。
[Upload] ボタン	ファイルをローカル システムからアップロードするには、[Upload] をクリックします。詳細については、「ファイルのアップロード」（P.4-7）を参照してください。
[Import] ボタン	インポート ファイルから Emergency Responder 設定にデータを追加するには、[Import] をクリックします。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。
Import Status	ステータス情報が表示されるテキスト ボックス。

関連項目

- 「Find and List IP Subnets」（P.A-52）
- 「Export IP Subnets」（P.A-54）
- 「ファイルのアップロード」（P.4-7）

Unlocated Phones

[ERL Membership]>[Unlocated Phones] を選択すると、[Unlocated Phones] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Unlocated Phones] ページは、Cisco Unified Communications Manager に登録されたが、Emergency Responder で検出されなかった電話機を特定するために使用します。この現象は次のような原因で発生する可能性があります。

- Emergency Responder で定義されていないスイッチに電話機が接続されています。
- 電話機がサポート対象外のデバイスに接続されています。ルータ ポート、ルータに接続されるハブ、サポート対象外のスイッチなどです。
- 電話機が接続されているスイッチが、現在、到達不能になっている。たとえば、SNMP クエリーに応答しない場合など。
- 電話機が設定済みのどの IP サブネットでも見つからず、電話機が模擬電話機として設定されていません。
- 手動で割り当てられた電話機。

- 位置未確認の電話機として特定され、ERL に割り当てられた電話機。

Emergency Responder は位置未確認の電話機を適切な ERL に割り当てることができないため、ネットワーク上でこれらの電話機の位置が検出されない原因となっている問題のすべてを特定し、解決してください。Emergency Responder でスイッチを定義するか、電話機をサポートされているスイッチ ポートに移動しても問題が解決されない場合は、このページを使用して手動で電話機を ERL に割り当てる必要があります。トラブルシューティング情報については、「位置未確認の電話機が多すぎる」（P.11-2）を参照してください。

表 A-39 に、[Unlocated Phones] ページの説明を示します。

表 A-39　[Unlocated Phones] ページ

フィールド	説明
Unlocated Phone Search Parameters	
Find phones where...	検索対象となる位置未確認の電話機を選択するための検索条件を入力します。 すべての位置未確認の電話機を検索する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、次の手順に従います。 • すべての条件と一致する電話機のみを選択するように指定する場合は [All] を選択します（AND 検索）。いずれかの検索条件と一致する電話機を選択するように指定する場合は [Any] を選択します（OR 検索）。プルダウン メニューから、検索するフィールド（[Phone Extension] や [Phone MAC Address] など）を選択して、検索関係（[is Exactly] や [Starts with] など）を選択し、検索文字列を入力します。 • フィールドの組み合わせを検索するには、**プラス** アイコン（+）をクリックして新しい検索パラメータを追加します。（検索パラメータを削除するには、**マイナス** アイコン（–）をクリックします）。 • すべての検索パラメータを入力したら、[Find] をクリックします。
Assign ERL	ERL を割り当てるには、電話機の隣にあるチェックボックスをオンにすることによって電話機を選択し、[Search ERL] をクリックして ERL を検索して選択し、[Assign ERL] をクリックします。
Unassign ERL	ERL を割り当て解除するには、電話機を選択して [Unassign ERL] ボタンをクリックします。
List of unlocated phones	Emergency Responder が特定の ERL に割り当てることができなかった電話機のリスト。次の情報が表示されます。 • Emergency Responder グループ • 電話機の IP アドレス • 電話機の MAC アドレス • 内線番号 • 割り当てられた ERL • 有効な ERL • ERL ルール 電話機が別の Emergency Responder グループによって制御されているスイッチに移動された場合は、その電話機の Emergency Responder グループ名がリストに表示されます。 **（注）** 位置未確認の電話機が数多く存在する場合は、複数ページにわたって表示されます。電話機の ERL への割り当ては、一度に 1 ページでしか実行できません。リストの下部にあるリンクを使用して、ページ間を移動します。

関連項目

- 「位置未確認の電話の識別」（P.4-62）
- 「位置未確認の電話機が多すぎる」（P.11-2）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）
- 「Find and List Manually Configured Phone」（P.A-58）

Find and List Manually Configured Phone

[ERL Membership]>[Manually Configured Phones] を選択すると、[Find and List Manually Configured Phones] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Find and List Manually Configured Phones] ページは、変更または削除する電話機を検索して表示するために使用します。このページから新しい電話機を追加するためにナビゲートすることもできます。

表 A-40 に、[Find and List Manually Configured Phones] ページの説明を示します。

（注）　E.164 ダイヤル プランの一部としてこの検索を実行する場合、「+」は有効な文字です。

表 A-40　[Find and List Manually Configured Phones] ページ

フィールド	説明
Manual Phone Search Parameters	
Find manual phones where Line Number...	探している手動設定電話機を選択するための検索条件を入力します。 すべての手動設定電話機を検索する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、プルダウン メニューを使用して、検索条件（[contains] や [Starts with] など）を選択して、テキスト ボックスに回線番号を入力します。プルダウン メニューから 1 ページに表示する結果数を選択することもできます。検索条件を指定したら、[Find] をクリックします。
Manually Configure Phones	
Manually Configured Phones list	検索結果が表示されます。見つかった電話機ごとに、回線番号、ERL 名、IP アドレス、およびロケーションが表示されます。電話機に関する情報を表示して変更するには、これらのレコードのいずれかをクリックするか、[Edit] アイコンをクリックします。[Modify Manual Phone] ページが表示されます。MAC アドレス、IP アドレス、電話機のタイプ、バージョン、ロケーション、および ERL 名を変更することができます。 （注）　手動電話機を変更するときに、サブネット ID または回線番号を変更することができません。 [Update] をクリックして、変更を保存します。

表 A-40　[Find and List Manually Configured Phones] ページ（続き）

フィールド	説明
Add new Manual Phone	手動設定電話機を追加するには、[Add new Manual Phone] をクリックします。[Add New Manual Phone] ページが表示されます。詳細については、「Add New Manual Phone」（P.A-59）を参照してください。 （注）　[Add new Manual Phone] ボタンは、[Modify Manual Phone] ページから使用することもできます。
Export	手動設定電話機情報をファイルにエクスポートするには、[Find and List Manually Configured Phones] ページで [Export] をクリックします。詳細については、「Export Manual Phones」（P.A-60）を参照してください。
Import	手動設定電話機情報をファイルにインポートするには、[Find and List Manually Configured Phones] ページで [Import] をクリックします。詳細については、「Import Manual Phones」（P.A-61）を参照してください。

関連項目

- 「IP Subnet Phones」（P.A-54）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）
- 「Add New Manual Phone」（P.A-59）
- 「Export Manual Phones」（P.A-60）
- 「Import Manual Phones」（P.A-61）

Add New Manual Phone

[Add New Manual Phone] ページにアクセスするには、[ERL Membership]>[Manually Configured Phones] を選択します。[Find and List Manually Configured Phones] ページで、[Add new Manual Phone] リンクをクリックします。[Add New Manual Phone] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Add New Manual Phone] ページは、電話機の ERL を手動で定義するために使用します。次の条件のいずれかが該当する場合は、電話機を手動で定義する必要があります。

- Emergency Responder で、電話機がアナログの場合などに、電話機のタイプを自動的に追跡できない。電話機のサポートについては、「ネットワークのハードウェアおよびソフトウェアの要件」（P.1-4）を参照してください。
- 電話機が、ルータ ポート、ルータに接続されたハブ、サポートされていないスイッチ上のポートなどのサポートされていないポート上でホストされている。

手動で定義された電話機の場合は、Emergency Responder が ERL 情報を自動的に検索して更新することができません。定期的に手動電話機設定を検査して、それらが正しいことを確認する必要があります。

表 A-41 に、[Add New Manual Phone] ページの説明を示します。

表 A-41　[Add New Manual Phone] ページ

フィールド	説明
Add New Manual Phone	
Line Number	定義する電話機の内線番号。
MAC Address	IP 電話の場合の MAC アドレス。
IP Address	IP 電話の場合の IP アドレス。
Phone Type	「analog」などの電話機のタイプ。このフィールドは情報提供のみに使用されます。
Version	電話機のソフトウェアのバージョン（存在する場合）。このフィールドは情報提供にのみ使用されます。
Location	電話機のロケーション。
ERL Name	電話機に割り当てる ERL。ERL を検索して選択するには、[Search ERL] をクリックします。
[Insert] ボタン	電話機を電話機のリストに追加するには、[Insert] をクリックします。 **（注）**　[Insert] ボタンは、電話機を追加している場合にのみ表示されます。
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。

関連項目

- 「電話機の手動での定義」（P.4-63）
- 「Import Manual Phones」（P.A-61）
- 「Export Manual Phones」（P.A-60）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Export Manual Phones

[Export Manual Phones] ページにアクセスするには、[ERL Membership]>[Manually Configured Phones] を選択します。[Find and List Manually Configured Phones] ページで、[Export] リンクをクリックします。[Export Manual Phones] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Export Manual Phones] ページは、Emergency Responder 手動電話機設定を含むファイルを作成するために使用します。

大量の手動設定電話機を更新する必要がある場合は、電話機データをエクスポートして、スプレッドシートを使用してファイルの内容を変更してから、そのファイルを再度インポートします。

ダウンロード ユーティリティを使用してファイルをローカル システムにダウンロードして、その内容を変更してから、アップロード ユーティリティを使用してそのファイルをアップロードすることもできます。詳細については、「ファイルのダウンロード」（P.4-7）を参照してください。

表 A-42 に、[Export Manual Phones] ページの説明を示します。

表 A-42　[Export Manual Phones] ページ

フィールド	説明
Export Manual Phones	
Select Export Format	インポートするファイルに使用される形式を選択します。 形式を選択したら、[view sample file] をクリックして、予想される形式と値のシーケンスの例を確認します。このサンプル情報を使用して、スプレッドシートでインポート ファイルを作成します。
Enter Export File Name	作成するファイルの名前。ファイル拡張子を含めないでください。
[Export] ボタン	ファイルをファイルにエクスポートするには、[Export] をクリックします。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。
Download	
Select a file to download	ファイルをローカル システムにダウンロードするには、プルダウン メニューを使用してファイルを選択してから、[Download] をクリックします。

関連項目

- 「電話機の手動での定義」（P.4-63）
- 「ファイルのダウンロード」（P.4-7）
- 「Import Manual Phones」（P.A-61）
- 「Find and List Synthetic Phones」（P.A-62）

Import Manual Phones

[Import Manual Phones] ページにアクセスするには、[ERL Membership]>[Manually Configured Phones] を選択します。[Find and List Manually Configured Phones] ページで、[Import] リンクをクリックします。[Import Manual Phones] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Import Manual Phones] ページは、データが定義されたファイルから一度に複数の手動設定電話機を作成または更新するために使用します。このファイルは、必要な形式のいずれかで情報を保存可能なスプレッドシートを使用して作成します。インポート ファイルを作成または更新する前に、このページのサンプルを確認してください。

大量の手動設定電話機を更新する必要がある場合は、電話機データをエクスポートして、エクスポート ファイルを更新し、そのファイルを再度インポートします。

アップロード ユーティリティを使用してファイルをローカル システムからアップロードしてから、データをファイルにインポートすることもできます。詳細については、「ファイルのアップロード」（P.4-7）を参照してください。

表 A-43 に、[Import Manual Phones] ページの説明を示します。

表 A-43　[Import Manual Phones] ページ

フィールド	説明
Select Import Format	インポートするファイルに使用される形式を選択します。 形式を選択したら、[view sample file] をクリックして、予想される形式と値のシーケンスの例を確認します。このサンプル情報を使用して、スプレッドシートでインポート ファイルを作成します。
Select File to Import	データをインポートするファイルを選択します。
Upload	ファイルをローカル システムからアップロードするには、[Upload] をクリックします。[Upload File] ページが表示されます。詳細については、「ファイルのアップロード」（P.4-7）を参照してください。
[Import] ボタン	インポート ファイルから Emergency Responder 設定にデータを追加するには、[Import] をクリックします。
[Close] ボタン	ウィンドウを閉じるには、[Close] をクリックします。
Import Status	ステータス メッセージが表示されます。

関連項目

- 「電話機の手動での定義」（P.4-63）
- 「ファイルのアップロード」（P.4-7）
- 「Find and List Synthetic Phones」（P.A-62）

Find and List Synthetic Phones

[ERL Membership]>[Synthetic Phones] を選択すると、[Find and List Synthetic Phones] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Find and List Synthetic Phones] ページは、変更または削除する電話機を検索して表示するために使用します。このページから新しい模擬電話機を追加するためにナビゲートすることもできます。

表 A-44 に、[Find and List Synthetic Phones] ページの説明を示します。

表 A-44　[Find and List Synthetic Phones] ページ

フィールド	説明
Synthetic Phone Search Parameters	
Find Synthetic phones where MAC Address	検索する模擬電話機を選択するための検索条件を入力します。 すべての模擬電話機を検索する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、プルダウン メニューを使用して、検索条件（[contains] や [Starts with] など）を選択して、テキスト ボックスに MAC アドレスを入力します。プルダウン メニューから 1 ページに表示する結果数を選択することもできます。検索条件を指定したら、[Find] をクリックします。
Synthetic Phones	
Synthetic Phones list	検索結果が表示されます。見つかった電話機ごとに、回線番号、ERL 名、IP アドレス、およびロケーションが表示されます。電話機に関する情報を表示して変更するには、これらのレコードのいずれかをクリックするか、[Edit] アイコンをクリックします。[Modify Synthetic Phone] ページが表示されます。MAC アドレス、IP アドレス、電話機のタイプ、バージョン、ロケーション、および ERL 名を変更することができます。 **（注）** 模擬電話機を変更するときに、サブネット ID または回線番号を変更することができません。 [Update] をクリックして、変更を保存します。
Add new Synthetic Phone	模擬電話機を追加するには、[Add new Synthetic Phone] をクリックします。[Add New Synthetic Phone] ページが表示されます。詳細については、「Add New Synthetic Phone」（P.A-63）を参照してください。 **（注）** [Add new Synthetic Phone] ボタンは、[Modify Synthetic Phone] ページから使用することもできます。

Add New Synthetic Phone

[Add New Synthetic Phone] ページにアクセスするには、[ERL Membership]>[Synthetic Phones] を選択します。[Find and List Synthetic Phones] ページで、[Add new Synthetic Phone] リンクをクリックします。[Add New Synthetic Phone] ページが表示されます。

（注） Off-Premise ERL や Intrado ERL には、テスト ERL は設定できません。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Add New Synthetic Phone] ページは、模擬電話機の ERL を手動で定義するために使用します。ERL 設定をテストするには、サブネット内に模擬電話機を設定する必要があります。CiscoWorks IP Telephony Environment Monitor（ITEM）2.0 と Emergency Responder のテスト ERL を組み合わせて使用することができます。

模擬電話機の場合は、Emergency Responder が ERL 情報を自動的に検索して更新することができません。定期的に模擬電話機設定を検査して、それらが正しいことを確認する必要があります。

表 A-45 に、[Add New Synthetic Phone] ページの説明を示します。

表 A-45　[Add New Synthetic Phone] ページ

フィールド	説明	注
MAC Address	模擬電話機の MAC アドレスまたは MAC アドレスの範囲。	疑似 MAC アドレスは 00059a3b7700 ～ 0059a3b8aff の範囲にする必要があります。 MAC アドレスは次の形式で入力します。 xx-xx-xx-xx-xx-xx または xxxxxxxxxxxx
ERL Name	模擬電話機に割り当てる ERL。有効な ERL 名を入力するか、ドロップダウン リストから ERL を選択します。	
[Insert] ボタン	模擬電話機を電話機のリストに追加するには、[Insert] をクリックします。	[Insert] ボタンは、電話機を追加している場合にのみ表示されます。
[New] ボタン	別の電話機を追加するには、[New] をクリックします。	[New] ボタンは、既存の電話機が表示されている場合にのみ表示されます。
[Update] ボタン	電話機に加えた変更を保存するには、既存の電話機が表示されているときに [Update] をクリックします。	[Update] ボタンは、既存の電話機が表示されている場合にのみ表示されます。
[Cancel Changes] ボタン	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。	

関連項目

- 「擬似電話機の追加」（P.4-67）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Find and List Users

[User Management]>[User] を選択すると、[Find and List Users] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Find and List Users] ページは、現在のユーザを検索して一覧表示したり、新しいユーザを追加したり、現在のユーザを変更または削除したりするために使用します。

表 A-46 に、[Find and List Users] ページの説明を示します。

表 A-46　[Find and List Users] ページ

フィールド	説明
User Search Parameters	
Find User where User Name	探しているユーザを選択するための検索条件を入力します。 すべてのユーザを検索する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、次の手順に従います。 • 選択した条件と一致するユーザのみを表示するように指定する場合は [All] を選択します（AND 検索）。 • いずれかの検索条件と一致するユーザを選択するように指定する場合は [Any] を選択します（OR 検索）。 • プルダウン メニューから、検索するフィールドを選択して、対応する関係を選択し、1 ページに表示する結果数を選択します。検索フィールドと対応する関係は次のとおりです。 – Authentication Mode：Both、Remote、または Local – User Name：Ends with、Starts with、contains、または Exactly。 – Unified CM Cluster：Ends with、Starts with、contains または Exactly。 • フィールドの組み合わせを検索するには、プラス アイコン（+）をクリックして新しい検索パラメータを追加します。（検索パラメータを削除するには、マイナス アイコン（–）をクリックします）。 • すべての検索パラメータを入力したら、[Find] をクリックします。
User	
Users list	このページ セクションには、検索結果が表示されます。検索後にユーザ名が表示されなかった場合は、まだ、どのユーザも設定されていません。
Username	選択条件に基づくユーザ名が表示されます。
Authentication Mode	ユーザの認証モードが表示されます。認証モードは [Remote] か [Local] のどちらかにすることができます。
Unified CM Cluster	この値は、ユーザが Unified CM サーバを経由してリモートで認証された場合にのみ表示されます。
[Edit] アイコン	ユーザ名または [Edit] アイコンをクリックすると [Modify User] ページが表示されます。このページでは、ユーザの認証モード、パスワード、および Unified CM クラスタを変更することができます。[Modify User] ページには、ユーザに割り当てられたグループとロールも表示されます。
[Delete] アイコン	ユーザをシステムから削除するには、[Delete] アイコンをクリックします。 **（注）**　管理者は削除することができません。
[Add New User] ボタン	[Add New User] ボタンをクリックすると、[Add User] ページが開きます。[Add User] ページについては、表 A-48 を参照してください。
[Delete Users] ボタン	ユーザをまとめて削除するには、[Delete Users] ボタンをクリックします。チェックボックスをオンにすることによって、リモートとローカルの両方のユーザを複数選択してから、[Delete Users] ボタンをクリックします。
[Change to Remote Users] ボタン	複数のローカル ユーザをまとめてリモート認証ユーザに変更するには、[Change to Remote Users] ボタンをクリックします。

Modify User

[User Management]>[User] を選択して、ユーザを検索し、[Find and List Users] ページでユーザ名をクリックするか、ユーザに関連付けられた [Edit] アイコンをクリックすると、[Modify User] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Modify User] ページは、現在のユーザのパスワードを変更するために使用します。

表 A-47 に、[Modify User] ページの説明を示します。

表 A-47　[Modify User] ページ

フィールド	説明
User Name	情報を変更するユーザの名前が表示されます。 **（注）** [Modify User] ページでは、ユーザ名を変更することができません。
Authentication Mode	ユーザの認証モードを変更します。ローカル ユーザをリモート ユーザに、リモート ユーザをローカル ユーザに変更することができます。
Password	ユーザの新しいパスワードを入力します。
Confirm Password	ユーザの新しいパスワードを再度入力します。
Cisco Unified CM Cluster	Cisco Unified CM クラスタを選択します。これは、ローカル ユーザをリモート ユーザに変更するときに必要です。既存のリモート ユーザの Cisco Unified CM クラスタを別の Cisco Unified CM クラスタに変更することもできます。 **（注）** [Cisco Unified CM Cluster] ドロップダウン ボックスは、認証モードがリモートとして選択されている場合にのみイネーブルになります。
[Update] ボタン	[Modify User] ページに加えられた変更を適用します。
[Cancel Changes] ボタン	[Modify User] ページに加えられた変更をキャンセルします。
Add new User	新しいユーザを追加する場合に、このボタンをクリックします。[Add User] ページが表示されます。詳細については、表 A-48 を参照してください。
User Groups for this user	ユーザが割り当てられたグループが表示されます。
User Roles for this user	ユーザに割り当てられたロールが表示されます。

Add User

[User Management]>[User] を選択して、[Find and List Users] ページで [Add new User] をクリックすると、[Add User] ページが表示されます。[Modify User] ページからも [Add User] ページにアクセスすることができます。詳細については、「Modify User」（P.A-66）を参照してください。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Add User] ページは、新しいユーザをシステムに追加するために使用します。

表 A-48 に、[Add User] ページの説明を示します。

表 A-48　[Add User] ページ

フィールド	説明
User Name	新しいユーザのユーザ名を入力します。
Authentication Mode	新しいユーザの認証モードを選択します。ユーザは、リモート ユーザかローカル ユーザのどちらかにすることができます。
Password	新しいユーザのパスワードを入力します。
Confirm Password	新しいユーザのパスワードを再度入力します。
Cisco Unified CM Cluster	このフィールドは、ユーザがリモート ユーザの場合にのみイネーブルになります。ドロップダウン ボックスから、リモート ユーザを認証する Cisco Unified CM クラスタを選択します。
[Insert] ボタン	新しいユーザを挿入します。
[Cancel Changes] ボタン	[Add User] ページに加えられた変更をキャンセルします。

関連項目

- 「ロールベースのユーザ管理」（P.4-2）
- 「Find and List Roles」（P.A-68）
- 「Find and List User Groups」（P.A-70）

Change to Remote User

[User Management]>[User] を選択して、[Find and List Users] ページで [Change to Remote Users] をクリックすると、[Change to Remote Users] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Change to Remote Users] ページは、ローカル ユーザの認証モードをリモート ユーザに変更するために使用します。

表 A-49 に、[Add User] ページの説明を示します。

表 A-49　[Change to Remote Users] ページ

フィールド	説明
Cisco Unified CM Cluster	ドロップダウン ボックスから、選択されたユーザをリモート認証する Cisco Unified CM クラスタを選択します。
Selected Users	リモート ユーザに変更するローカル ユーザが表示されます。

表 A-49　[Change to Remote Users] ページ（続き）

フィールド	説明
[Update] ボタン	[Change to Remote Users] ページに加えられた変更を適用します。
[Close] ボタン	ウィンドウを閉じます。

Find and List Roles

[User Management]>[Role] を選択すると、[Find and List Roles] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Find and List Role] ページは、現在のロールを検索、一覧表示、変更、および削除したり、新しいロールを追加したりするために使用します。

表 A-50 に、[Find and List Roles] ページの説明を示します。

表 A-50　[Find and List Roles] ページ

フィールド	説明
Role Search Parameters	
Find Role where Role Name is	探しているロールを選択するための検索条件を入力します。 すべてのロールを検索する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、プルダウン メニューを使用して、検索条件（[contains] や [Starts with] など）を選択して、テキスト ボックスにロールを入力します。プルダウン メニューから 1 ページに表示する結果数を選択することもできます。検索条件を指定したら、[Find] をクリックします。
Roles	検索結果が表示されるページ セクション。インストール中に 4 つのデフォルト ロールが作成され、ここに表示されます。ロールの種類は次のとおりです。 • Emergency Responder System Admin • Emergency Responder ERL Admin • Emergency Responder Network Admin • Emergency Responder User デフォルト ロールの [Role Name] リンクまたは [Description] リンクをクリックすると、そのロールの [Standard Role] ページが表示されます。このページには、次の情報が表示されます。 • ロール名 • 説明 • ロールに割り当てられたリソースのリスト **（注）** デフォルト ロールに関する情報は変更することができません。変更することができるのは、作成したロールに関する情報だけです。 新しいロールを作成すると、デフォルト ロールと一緒に一覧表示されます。作成したロールの名前、説明、または [Edit] アイコンをクリックすると、[Modify Role] ページが表示されます。[Modify Role] ページの詳細については、表 A-51 を参照してください。

表 A-50　[Find and List Roles] ページ（続き）

フィールド	説明
[Edit] アイコン	[Edit] アイコンをクリックすると、[Modify Role] ページが表示されます。[Modify Role] ページについては、表 A-51 を参照してください。
[Delete] アイコン	ロールをシステムから削除するには、[Delete] アイコンをクリックします。 （注）　デフォルト ロールは削除することができません。
[Add New Role] ボタン	[Add New Role] をクリックすると、[Add Role] ページが表示されます。このボタンは、[Modify Role] ページと [Add Role] ページでも使用することができます。[Add Role] ページについては、表 A-52 を参照してください。

Modify Role

[User Management]>[Role] を選択して、[Find and List Roles] ページで、ロールを検索して、ロール名、説明、またはロールに関連付けられた [Edit] アイコンをクリックすると、[Modify Role] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Modify Role] ページは、既存のロールに関する情報を変更するために使用します。

（注）　4 つのデフォルト ロールに関する情報は変更することができません。

表 A-51 に、[Modify Role] ページの説明を示します。

表 A-51　[Modify Role] ページ

フィールド	説明
Modify Role	
Role Name	変更する新しいロールの名前。 （注）　ロール名は変更することができません。
Description	変更するロールの説明。テキスト ボックスに新しいテキストを追加することによって説明を変更します。
Resource Permissions	このページ セクションには、使用可能なすべてのリソースのリストが表示されます。リソースの左側にあるチェックボックスは、このロールに割り当てられたリソースを示します。ボックスをオンまたはオフにすることによって、リソース割り当てを変更します。
[Select All] ボタン	一覧表示されたリソースのすべてを選択するには、[Select All] をクリックします。
[Clear All] ボタン	現在選択されているすべてのリソースを選択解除するには、[Clear All] をクリックします。
[Update] ボタン	[Modify Role] ページに加えた変更を保存するには、[Update] をクリックします。
[Cancel Changes] ボタン	[Modify Role] ページに加えた変更をキャンセルするには、[Cancel Changes] をクリックします。
[Add new Role] ボタン	新しいロールを追加することができます。新しいロールの追加方法については、「Add Role」（P.A-70）を参照してください。

Add Role

[User Management]>[Role] を選択して、[Find and List Roles] ページで [Add new Role] をクリックすると、[Add Role] ページが表示されます。[Add Role] ページには、[Modify Role] ページと [Standard Role] ページからもアクセスすることができます。詳細については、「Modify Role」（P.A-69）を参照してください。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Add Role] ページは、新しいロールをシステムに追加するために使用します。

表 A-52 に、[Add Role] ページの説明を示します。

表 A-52　[Add Role] ページ

フィールド	説明
Add Role	
Role Name	追加する新しいロールの名前。
Description	新しいロールの説明。
Resource Permissions	このページ セクションには、使用可能なすべてのリソースのリストが表示されます。各リソースの左側にあるチェックボックスを使用すれば、新しいロールに割り当てるリソースを選択または選択解除することができます。
[Select All] ボタン	一覧表示されたリソースのすべてを選択するには、[Select All] をクリックします。
[Clear All] ボタン	現在選択されているすべてのリソースを選択解除するには、[Clear All] をクリックします。
[Insert] ボタン	新しいロールを追加するには、[Insert] をクリックします。
[Cancel Changes] ボタン	ロールの追加操作をキャンセルするには、[Cancel Changes] をクリックします。

関連項目

- 「ロールベースのユーザ管理」（P.4-2）
- 「Find and List Users」（P.A-64）
- 「Find and List User Groups」（P.A-70）

Find and List User Groups

[User Management]>[User Group] を選択すると、[Find and List User Groups] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Find and List User Groups] ページは、現在のユーザ グループを検索、一覧表示、変更、および削除したり、新しいユーザ グループを追加したりするために使用します。

表 A-53 に、[Find and List User Groups] ページの説明を示します。

表 A-53　[Find and List User Groups] ページ

フィールド	説明
User Group Search Parameters	
Find User Group where User Group Name	探しているユーザ グループを選択するための検索条件を入力します。 すべてのユーザ グループを検索する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、プルダウン メニューを使用して、検索条件（[contains] や [Starts with] など）を選択して、テキスト ボックスにユーザ グループを入力します。プルダウン メニューから 1 ページに表示する結果数を選択することもできます。検索条件を指定したら、[Find] をクリックします。
User Groups	検索結果が表示されるページ セクション。[User Group Name] リンク、[Description] リンク、または [Edit] アイコンをクリックすると、[Modify User Group] ページが表示されます。詳細については、「Modify User Group」（P.A-71）を参照してください。
[Edit] アイコン	[Edit] アイコンをクリックすると、[Modify User Group] ページが表示されます。詳細については、「Modify User Group」（P.A-71）を参照してください。
[Delete] アイコン	ユーザ グループをシステムから削除するには、[Delete] アイコンをクリックします。 **（注）**　インストール中に作成されたデフォルト ユーザ グループは削除することができません。
[Add New User Group] ボタン	[Add New User Group] ボタンをクリックすると、[Add User Group] ページが表示されます。[Add User Group] ページについては、表 A-55 を参照してください。

Modify User Group

[User Management]>[User Group] を選択して、[Find and List User Groups] ページでユーザ グループを検索してから、ユーザ グループ名、説明、またはユーザ グループに関連付けられた [Edit] アイコンをクリックすると、[Modify User Group] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Modify Role] ページは、既存のユーザ グループに関する情報を変更するために使用します。

表 A-54 に、[Modify User Group] ページの説明を示します。

表 A-54　[Modify User Group] ページ

フィールド	説明
Modify User Group	
User Group Name	変更するユーザ グループの名前。 **（注）**　ユーザ グループ名は変更することができません。
Description	変更するユーザ グループの説明。テキスト ボックスにテキストを追加するか、テキスト ボックス内のテキストを修正することによって説明を変更します。
Add Users to the Group	このページ セクションには、ユーザ グループ内のユーザ名が表示されるテキスト ボックスがあります。

表 A-54　[Modify User Group] ページ（続き）

フィールド	説明
[Add Users] ボタン	新しいユーザをグループに追加することができます。[Add User] をクリックすると、[Add User] ページが表示されます。詳細については、「Add User」（P.A-66）を参照してください。
[Remove Users] ボタン	ユーザをグループから削除することができます。これを実行するには、テキスト ボックスでユーザ名を強調表示して [Remove Users] をクリックします。
Assign Roles to Group	このページ セクションには、ユーザ グループに割り当てられたロールが表示されるテキスト ボックスがあります。
[Add Roles] ボタン	新しいロールをグループに割り当てることができます。[Add Roles] をクリックすると、[Add Role] ページが表示されます。詳細については、「Add Role」（P.A-70）を参照してください。 **（注）** インストール中にデフォルト ユーザ グループに割り当てられたデフォルト ロールにロールは追加できません。変更するユーザ グループがデフォルト ユーザ グループの場合は、[Add Roles] ボタンが表示されません。
[Remove Roles] ボタン	ロールをグループから削除することができます。これを実行するには、テキスト ボックスでロール名を強調表示して [Remove Roles] をクリックします。 **（注）** インストール中にデフォルト ユーザ グループに割り当てられたデフォルト ロールは削除できません。変更するユーザ グループがデフォルト ユーザ グループの場合は、[Remove Roles] ボタンが表示されません。
[Update] ボタン	[Modify User Group] ページに加えた変更を保存するには、[Update] をクリックします。
[Add New User Group] ボタン	新しいユーザ グループを追加することができます。詳細については、「Add User Group」（P.A-72）を参照してください。

Add User Group

[User Management]>[User Group] を選択して、[Find and List User Groups] ページで [Add new User Group] をクリックすると、[Add User Group] ページが表示されます。[Modify User Group] ページからも [Add User Group] ページにアクセスすることができます。詳細については、「Modify User Group」（P.A-71）を参照してください。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Add User Group] ページは、新しいユーザ グループをシステムに追加するために使用します。

表 A-55 に、[Add User Group] ページの説明を示します。

表 A-55　[Add User Group] ページ

フィールド	説明
Add User Group	
User Group Name	追加する新しいユーザ グループの名前。
Description	新しいユーザ グループの説明。
Add Users to the Group	このページ セクションには、ユーザ グループに追加したユーザ名が表示されるテキスト ボックスがあります。

表 A-55　[Add User Group] ページ（続き）

フィールド	説明
[Add Users] ボタン	ユーザを新しいグループに追加することができます。[Add Users] をクリックすると、[Add Users] ページが表示されます。詳細については、「Add User」（P.A-66）を参照してください。
[Remove Users] ボタン	ユーザをグループから削除することができます。これを実行するには、テキスト ボックスでユーザ名を強調表示して [Remove Users] をクリックします。
Assign Roles to Group	このページ セクションには、新しいユーザ グループに割り当てたロールが表示されるテキスト ボックスがあります。
[Add Roles] ボタン	ロールを新しいグループに割り当てることができます。[Add Roles] をクリックすると、[Add Roles] ページが表示されます。詳細については、「Add Role」（P.A-70）を参照してください。
[Remove Roles] ボタン	ロールをグループから削除することができます。これを実行するには、テキスト ボックスでロール名を強調表示して [Remove Roles] をクリックします。
[Insert] ボタン	新しいロールを追加するには、[Insert] をクリックします。

関連項目

- 「ロールベースのユーザ管理」（P.4-2）
- 「Find and List Users」（P.A-64）
- 「Find and List Roles」（P.A-68）

Call History

[Reports]>[Call History] を選択すると、[Call History] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者、ERL 管理者、ネットワーク管理者、またはユーザの権限を持っている必要があります。

説明

[Call History] ページを使用して、このネットワークから発信された緊急コールの履歴を表示します。Emergency Responder 8.6 は、最新の 10,000 コール履歴レコードを保存します。これらのコールを発信した時間について制限はありません。

表 A-56 に、[Call History] ページの説明を示します。

表 A-56　[Call History] ページ

フィールド	説明
Call History Search Parameters	
Search criteria	探しているコールを選択するための検索条件を入力します。 すべてのコールを検索する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、次の手順に従います。 • すべての条件と一致するコールのみを選択するように指定する場合は [All] を選択します（AND 検索）。いずれかの検索条件と一致するコールを選択するように指定する場合は [Any] を選択します（OR 検索）。プルダウン メニューから、検索するフィールド（[ERL Name] や [Caller's Extension] など）を選択して、検索関係（[contains] や [begins with] など）を選択し、検索文字列を入力します。 • フィールドの組み合わせを検索するには、**プラス** アイコン（+）をクリックして新しい検索パラメータを追加します。検索パラメータを削除するには、**マイナス** アイコン（–）をクリックします。 • すべての検索パラメータを入力したら、[Find] をクリックします。
Call History Matching Records	検索条件と一致する緊急コールのリストが次の情報を伴って表示されます。 • ERL Name：名前をクリックすると、ERL の詳細とその ALI 情報が表示されます。設定フィールドについては、「Conventional ERL」（P.A-17）を参照してください。 • Caller Extension：緊急コールの発信に使用された内線番号。 • Time：緊急コールが発信された時刻。 • Date：コールが発信された日付。 • Route Pattern-ELIN No.：コールに使用されたルート パターンと ELIN の組み合わせ。これらのフィールドの詳細については、「Conventional ERL」（P.A-17）を参照してください。 • Location：電話の場所。電話が手動で設定されたか、スイッチ ポートまたは IP サブネットに基づいて設定されてかによって変わります。 • Call Acknowledged：[Web Alert] ページ上のコールの確認応答ステータス。 • Acknowledged By：コールを確認応答したユーザの ID。 • Time Acknowledged：コールが確認応答された時刻。 • Date Acknowledged：コールが確認応答された日付。 • Comments：コールに関して入力されたコメント。[Edit] アイコンをクリックすると、[Call Details] ページが表示されます。このページの [Comments about the call] テキスト ボックスで、コールに関するコメントを入力または変更することができます。 大量のコールが検索条件と一致した場合は、複数ページにわたって表示されます。ページの下部にある [First]、[Previous]、[Next]、および [Last] リンクを使用してページ間を移動します。[Page] フィールドに特定のページ番号を入力して Enter を押せば、そのページに移動することもできます。
Download	コール履歴データをスプレッドシートに保存して、ローカル システムで表示またはダウンロードできるようにするには、[Download] をクリックします。
Update	コールのコール履歴にコメントを含めるには、[Update] をクリックします。 **（注）**　[Call Details] ページからのみ表示できます。

表 A-56　[Call History] ページ（続き）

フィールド	説明
Cancel Changes	保存されていないコメントを削除するには、[Cancel Changes] をクリックします。それからコメントを再入力できます。 （注）　[Call Details] ページからのみ表示できます。
Close	[Close] をクリックして [Call Details] を閉じます。 （注）　[Call Details] ページからのみ表示できます。

関連項目

- 「緊急コール履歴の表示」（P.4-67）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

ERL Audit Trail

次のいずれかの操作を実行すると、[ERL Audit Trail] ページが表示されます。

- [Reports]>[ERL Audit Trail] を選択する。
- [ERL Configuration] ページ（[ERL]>[Conventional ERL] を選択したときに表示される）に表示された ERL に関する [Audit Trail] 列で [view] をクリックする。

許可の要件

このページにアクセスするには、システム管理者、ERL 管理者、またはネットワーク管理者の権限が必要です。

説明

[ERL Audit Trail] ページは、ERL の変更履歴を表示するために使用します。

表 A-57 に、[ERL Audit Trail] ページの説明を示します。

表 A-57　[ERL Audit Trail] ページ

フィールド	説明
ERL Audit Trail	
Search criteria	探している監査詳細を選択するための検索条件を入力します。 すべての監査詳細を検索する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、次の手順に従います。 • すべての条件と一致する監査詳細のみを選択するように指定する場合は [All] を選択します（AND 検索）。いずれかの検索条件と一致する監査詳細を選択するように指定する場合は [Any] を選択します（OR 検索）。プルダウン メニューから、検索するフィールド（[ERL Name] や [Modified By] など）を選択して、検索関係（[contains] や [begins with] など）を選択し、検索文字列を入力します。ERL 名で検索する場合は、ERL 名を入力することも、プルダウン メニューを使用して ERL を選択することもできます。 • フィールドの組み合わせを検索するには、**プラス** アイコン（+）をクリックして新しい検索パラメータを追加します。検索パラメータを削除するには、**マイナス** アイコン（–）をクリックします。 • すべての検索パラメータを入力したら、[Find] をクリックします。
Matching Records	検索条件と一致する ERL 変更レコードのリスト。ERL に対する変更ごとに別々のレコードに記録されるため、1 つの ERL に複数の監査レコードが含まれる場合があります。このリストには、レコードごとに次の情報が表示されます。 • ERL Name：変更された ERL の名前。 • Modified By：ERL を変更したユーザのログイン ID。 • Modified Time：ERL が変更された日付と時刻。 • Modification Details：ERL またはその ALI で変更されたフィールドのリスト。[Modification Details] テキスト ボックス内を上下に移動するには、スクロール バーを使用します。 **（注）** 大量のレコードが検索された場合は、複数のページにわたって表示されます。リストの下部にあるリンクを使用して、ページ間を移動します。[Page] フィールドに特定のページ番号を入力して Enter を押せば、そのページに移動することもできます。

関連項目

- 「ERL の監査証跡の表示」（P.4-43）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

Export PS-ALI Records

[Tools]>[Export PS-ALI Records] を選択すると、[Export PS-ALI Records] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Export PS-ALI Records] ページは、サービス プロバイダーに送信可能な NENA 形式でファイルを作成するために使用します。サービス プロバイダーは、このファイルを使用して、会社の ALI データを更新します。ERL からの緊急コールが正しい PSAP にルーティングされるためには、この情報がサービス プロバイダーに必要です。

サービス プロバイダーには、必ず、エクスポート ファイルを送信してください。エクスポート ファイルの送信を省略した場合は、以降のエクスポート ファイルにデータベース更新に関する正確なコマンド情報が格納されないため、エクスポート ファイルを手動で編集してアップロード可能にする必要があります。データベースのアップロードが失敗した場合に、サービス プロバイダーからエラー情報が提供されます。

（注） ALI レコード内の顧客コードを変更すると、Emergency Responder で、ALI のエクスポート時に、古いコードを持つ ALI を削除するための削除レコードと新しいコードを持つ ALI を追加するための挿入レコードが生成されます。この削除/挿入シーケンスは、コードの変更後初めて ALI をエクスポートするときにのみ生成されます。このエクスポート ファイルがサービス プロバイダーに送信されたことを確認する必要があります。ALI フィールドについては、「ALI Information (for ERL Name)」（P.A-22）を参照してください。

エクスポート ファイルを使用して ERL 設定をバックアップすることもできます。

表 A-58 に、[Export RS-ALI Records] ページの説明を示します。

表 A-58　[Export PS-ALI Records] ページ

フィールド	説明
Export PS-ALI Records	
Select NENA Format	エクスポート ファイルに使用すべきファイル形式（NENA 形式 3.0、2.1、または 2.0）。
File to Export	作成するファイルの名前。ファイル拡張子を含めないでください。
Company Name（NENA ヘッダー フィールド）	会社の名前。名前にスペースを含めることはできません。 **（注）**　データは NENA 要件に適合します。
Cycle Counter（NENA ヘッダー フィールド）	このエクスポートが作成されるシーケンス。このフィールドは、データをエクスポートするたびに自動的に増加されます。サービス プロバイダーに送信したシーケンスと同期がとれなくなった場合は変更することができます。ただし、シーケンス番号を変更してもファイル内のデータには影響しません。エクスポートをやり直す場合は、エクスポート ファイルを手動で編集して、レコード ステータス フィールドを変更する必要があります。 **（注）**　データは NENA 要件に適合します。
End of Line Format	ダウンロード用にエクスポートされる PS-ALI レコードの改行形式を選択することができます。次の 2 つの形式から選択することができます。 • Windows スタイル（¥r¥n） • Unix/Linux スタイル（¥n）
[Export] ボタン	エクスポート ファイルを作成するには、[Export] をクリックします。
Download File	エクスポートした PS-ALI ファイルをダウンロードするには、[Download File] をクリックします。
[Cancel] ボタン	エクスポート操作をキャンセルするには、[Cancel] をクリックします。

関連項目

- 「ALI Information (for ERL Name)」（P.A-22）
- 「ALI 提出要件に関するサービス プロバイダーとの交渉」（P.1-22）
- 「ERL 情報のエクスポート」（P.4-41）
- 「サービス プロバイダー向け ALI 情報のエクスポート」（P.4-42）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

PS-ALI Converter

[Tools]>[PS-ALI Converter] を選択すると、[PS-ALI Converter] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

PS-ALI Converter ツールは、Emergency Responder ERL で受け入れ可能な ERL ファイルを生成するために使用します。PS-ALI Converter ツールによって、ALI ファイルが NENA 2.0 形式から csv テキスト ファイルに変換されます。その後で、csv ファイルを変更（ERL 名を追加または変更するためなど）し、そのファイルを Emergency Responder にインポートすることによって、変更した ERL 詳細を保存することができます。

（注）　ALI レコード内の顧客コードを変更すると、Emergency Responder で、ALI のエクスポート時に、古いコードを持つ ALI を削除するための削除レコードと新しいコードを持つ ALI を追加するための挿入レコードが生成されます。この削除/挿入シーケンスは、コードの変更後初めて ALI をエクスポートするときにのみ生成されます。このエクスポート ファイルがサービス プロバイダーに送信されたことを確認する必要があります。ALI フィールドについては、「ALI Information (for ERL Name)」（P.A-22）を参照してください。

表 A-59 に、[PS-ALI Converter] ページの説明を示します。

表 A-59　[PS-ALI Converter] ページ

フィールド	説明
Export PS-ALI Records	
Select PS-ALI file（NENA 2.0 フォーマット）	変換する PS-ALI ファイルの名前。このファイルはデフォルト形式の NENA 形式 2.0 にする必要があります。
Output File（csv フォーマット）Name	作成する csv ファイルの名前。
[Convert] ボタン	csv ファイルを作成するには、[Convert] をクリックします。
[Cancel] ボタン	変換プロセスを停止してウィンドウを閉じるには、[Cancel] をクリックします。

関連項目

- 「ALI Information (for ERL Name)」（P.A-22）
- 「ALI 提出要件に関するサービス プロバイダーとの交渉」（P.1-22）
- 「ERL 情報のエクスポート」（P.4-41）
- 「サービス プロバイダー向け ALI 情報のエクスポート」（P.4-42）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）
- 「E911 および Cisco Emergency Responder の用語について」（P.1-2）

ERL Debug Tool

[Tools]>[ERL Debug Tool] を選択すると、[ERL Debug Tool] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[ERL Debug Tool] ページでは、内線番号を入力として、その電話機の緊急コールのルーティングに使用されている ERL が表示されます。

この診断ツールは、ERL の作成期間と ERL の割り当てフェーズで Emergency Responder 設定を検証したり、不正な ERL に転送されたコールをトラブルシューティングしたりするために使用します。

表 A-60 に、[ERL Debug Tool] ページの説明を示します。

表 A-60　[ERL Debug Tool] ページ

フィールド	説明
ERL Debug Tool	
Find Phones where extension	探している内線番号を選択するための検索条件を入力します。 すべての内線番号を検索する場合は、条件を入力せずに [Find] をクリックします。 検索を絞り込むには、プルダウン メニューを使用して、検索条件（[contains] や [Starts with] など）を選択して、テキスト ボックスに内線番号を入力します。プルダウン メニューから 1 ページに表示する結果数を選択することもできます。検索条件を指定したら、[Find] をクリックします。
Matching records	電話機の緊急コールのルーティングに使用されている ERL が表示されるページ セクション。見つかった内線番号ごとに、次の情報が表示されます。 • Phone extension • ERL • IP Address • MAC Address • Why this ERL is Used? 設定が間違っていた場合は、必要な変更を行います。

関連項目

- 「Cisco Emergency Responder Admin Utility Tool の使用方法」（P.11-20）
- 「ERL について」（P.4-30）
- 「ERL 管理の概要」（P.4-31）

ALI Formatting Tool

[Tools]>[ALI Formatting Tool] を選択すると、[ALI Formatting Tool] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[ALI Formatting Tool] ページは、サービス プロバイダーとの PS-ALI レコード トランザクションを正常に行えるように PS-ALI レコードの形式をカスタマイズするために使用します。

ALI フォーマット ツール（AFT）によって、Emergency Responder で生成された NENA ファイルが読み取られ、すべての ELIN レコードが表示されます。その後で、次のいずれかの操作を実行することができます。

- ALI レコードの詳細を表示する。
- レコードを選択して、AFT で編集できるように ALI フィールドの値を更新する。
- 複数の ALI レコードに対して一括更新処理を実行する。
- エリア コードやシティ コードに基づいて選択的に ALI レコードをエクスポートする。

表 A-61 に、[ALI Formatting Tool] ページの説明を示します。

表 A-61　[ALI Formatting Tool] ページ

フィールド	説明
Select a Service Provider	このプルダウン メニューは、サービス プロバイダーを選択するために使用します。
Select an Input File for the ALI Formatting Tool from the List Below	このプルダウン メニューは、入力ファイルを選択するために使用します。
[Submit] ボタン	[Submit] ボタンをクリックすると、[Search for ELINs] ページが表示されます。このページについては、表 A-62 を参照してください。

表 A-62 に、[Search for ELINs] ページの説明を示します。

表 A-62　[Search for ELINs] ページ

フィールド	説明
Use Search to Filter-out ELINs on Area, City and Local Code(last 4-digits).	ローカル コード、エリア コード、またはシティ コードで ELIN を検索することができます。

表 A-62　[Search for ELINs] ページ（続き）

フィールド	説明
追加（+）ボタン	新しい検索パラメータを追加します。
削除（-）ボタン	検索パラメータを削除します。

表 A-63 に、[Bulk Update] ページの説明を示します。

表 A-63　[Bulk Update] ページ

フィールド	説明
[Remove Changes/Generate File] ボタン	変更されたすべての ELIN を表示します。
Search for ELIN	ELIN 検索ページが表示されます。

表 A-64 に、[Review Changes/Generate File] ページの説明を示します。

表 A-64　[Review Changes/Generate File] ページ

フィールド	説明
Add More ELIN	変更されていない残りの ELIN を表示します。
Remove ELIN	選択された ELIN をリストから削除します。
Search for ELIN	ELIN 検索画面が表示されます。
[Generate File] ボタン	フォーマット済みファイルを生成します。

表 A-65 に、[Download Formatted File] ページの説明を示します。

表 A-65　[Download Formatted File] ページ

フィールド	説明
[Download Formatted File] ボタン	[Download File] ダイアログボックスを表示します。このダイアログボックスでは、フォーマット済みファイルをローカル システムにダウンロードすることができます。

関連項目

- 「ALI Information (for ERL Name)」（P.A-22）
- 「サービス プロバイダー向け ALI 情報のエクスポート」（P.4-42）
- 「Bell-Canada に対する ALI フォーマット ツールの使用」（P.G-1）
- 「SBC-Ameritech に対する ALI フォーマット ツールの使用」（P.G-3）
- 「SBC-PacBell に対する ALI フォーマット ツールの使用」（P.G-3）
- 「SBC-Southwestern Bell に対する ALI フォーマット ツールの使用」（P.G-4）
- 「Qwest に対する ALI フォーマット ツールの使用」（P.G-5）
- 「Verizon に対する ALI フォーマット ツールの使用」（P.G-6）

File Management Utility

[Tools]>[File Management Utility] を選択すると、[File Management Utility] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[File Management Utility] ページは、エクスポートされたファイルを検索、ダウンロード、または削除するために使用します。

表 A-66 に、[File Management Utility] ページの説明を示します。

表 A-66　[File Management Utility] ページ

フィールド	説明
Search Parameters	
Please Select:	プルダウン メニューから、検索するファイルのタイプを選択します。
[Search] ボタン	検索を実行するには、[Search] ボタンをクリックします。
Exported Files	検索結果が表示されるページ領域。見つかったファイルのファイル名、最終更新データ、およびファイル サイズが表示されます。
[Download] ボタン	選択されたファイルをダウンロードします。 **（注）** [Download] をクリックする前に、ファイル名の隣にあるボックスをオンにしてファイルを選択します。一覧表示されたすべてのファイルを選択するには、[File Name] 列見出しの隣にあるボックスをオンにします。
[Delete] ボタン	選択されたファイルを削除します。 **（注）** [Delete] をクリックする前に、ファイル名の隣にあるボックスをオンにしてファイルを選択します。一覧表示されたすべてのファイルを選択するには、[File Name] 列見出しの隣にあるボックスをオンにします。

関連項目

- 「アップロードおよびダウンロード ユーティリティの使用」（P.4-6）

Purge Call History

[Tools]>[Purge Utility] を選択すると、[Purge Utility for Call History] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者または ERL 管理者の権限が必要です。

説明

[Purge Call History Utility] ページは、指定した保存期間よりも古いコール履歴レコードを削除するために使用します。このユーティリティを使用すれば、レコードを直接パージしたり、コール履歴レコードの日次パージをスケジュールしたりすることができます。Emergency Responder は、パージの結果を Emergency Responder Administration ログに記録します。

表 A-67 に、パージ ユーティリティ ページの説明を示します。

表 A-67　Purge Utility for Call History

フィールド	説明
Status	ステータス メッセージが表示されます。
Purge Now	
Purge Data older than	削除するレコードの保存期間を指定します。
Schedule Purge	
Daily Purge at	古いレコードを削除する時刻（GMT）を指定します。
Purge Data older than	削除するレコードの保存期間を指定します。
Update	変更を保存してアクティブにするには、[Update] をクリックします。
Cancel	このページ上のフィールドを最後に保存された設定に戻すには、[Cancel Changes] をクリックします。

関連項目

- 「緊急コール履歴の表示」（P.4-67）
- 「コール履歴ログの収集」（P.11-29）

Purge Call History

APPENDIX B

Cisco Emergency Responder のサービスアビリティ Web インターフェイス

次のトピックでは、Cisco Emergency Responder（Emergency Responder）サービスアビリティ Web インターフェイスのページ上のフィールドについて説明します。

Control Center

[Tools] > [Control Center] を選択すると、[Control Center] ページが表示されます。

許可の要件

このページにアクセスするには、サービスアビリティ権限が必要です。

説明

[Control Center] ページを使用して、サーバで実行されているサービスを表示し、そのサービスの開始、停止、および再開を行います。このページには、サーバ上で現在実行されているサーバのリストが表示されます。各サービス名の前にあるオプション ボタンをクリックすると、目的のアクションを実行する各サービスを選択できます。

表 B-1 で [Control Center] ページについて説明します。

表 B-1　[Control Center] ページ

フィールド	説明
[Start] ボタン	選択したサービスを開始します。
[Stop] ボタン	選択したサービスを停止します。
[Restart] ボタン	選択したサービスを再開します。
[Refresh] ボタン	選択したサーバで現在実行されているサービスのリストを更新します。
Service Name	選択したサーバで現在実行されているサービスの名前。サービスを選択するには、サービス名の隣にあるオプション ボタンをクリックします。
Status	選択したサービスの現在のステータス。

関連項目

- 「Cisco Emergency Responder サーバの起動と停止」（P.11-25）

Event Viewer

[Tools]>[Event Viewer] を選択すると、[Event Viewer] ページが表示されます。

許可の要件

このページにアクセスするには、サービスアビリティ権限が必要です。

説明

[Event Viewer] ページは、以前の 6 か月の Emergency Responder イベントを表示するために使用します。

表 B-2 に、[Event Viewer] ページの説明を示します。

表 B-2　[Event Viewer] ページ

フィールド	説明
[Type] プルダウン メニュー	（注）　このプルダウン メニューには、[Type] と [Module] という 2 つのオプションがあります。[Type] または [Module] を選択すると、右側のプルダウン メニューが切り替わり、使用できる Type または Module のオプションが表示されます。 表示するイベントの種類を選択できます。使用できるタイプは次のとおりです。 • ALL • INFO • WARN • ERROR これらのオプションは、[Type] プルダウン メニューの右側にあるプルダウン メニューに表示されます。

表 B-2　[Event Viewer] ページ（続き）

フィールド	説明
[Module] プルダウン メニュー	**（注）** このプルダウン メニューには、[Type] と [Module] という 2 つのオプションがあります。[Type] または [Module] を選択すると、右側のプルダウン メニューが切り替わり、使用できる Type または Module のオプションが表示されます。 イベントを表示する Emergency Responder モジュールを選択できます。プルダウン メニューから [Module] を選択すると、右側のメニューが切り替わり、使用できるモジュールが表示されます。使用可能なオプションは次のとおりです。 • All • CER_DATABASE • CER_SYSADMIN • CER_REMOTEUPDATE • CER_TELEPHONY • CER_PHONETRACKINGENGINE • CER_AGGREGATOR • CER_ONSITEALERT • CER_GROUP • CER_CALLENGINE • CER_CLUSTER
[Items Per Page] メニュー	1 ページに表示するイベント数を選択できます。オプションは 10、20、30、40、または 50 イベントです。
Matching Records	検索結果が表示されます。 **（注）** ページのこの領域は、検索操作を実行するまで表示されません。
[Type] 列	イベントの種類が表示されます。[Type] 列には次のいずれかが表示されます。 • INFO • WARN • ERROR 上矢印および下矢印を使用して、結果の昇順または降順を実行できます。
[Time] 列	イベントの時刻が表示されます。上矢印および下矢印を使用して、結果の昇順または降順を実行できます。

表 B-2　[Event Viewer] ページ（続き）

フィールド	説明
[Module] 列	イベントの対象の Emergency Responder モジュールが表示されます。モジュールは次のとおりです。 • CER_DATABASE • CER_SYSADMIN • CER_REMOTEUPDATE • CER_TELEPHONY • CER_PHONETRACKINGENGINE • CER_AGGREGATOR • CER_ONSITEALERT • CER_GROUP • CER_CALLENGINE • CER_CLUSTER 上矢印および下矢印を使用して、結果の昇順または降順を実行できます。
[Message] 列	各イベントに関連付けられたメッセージが表示されます。テキスト ボックスの右側にある上矢印および下矢印を使用して、メッセージをスクロールします。

関連項目

- 「Event Viewer の使用」（P.6-2）

SNMP Community String Configuration

[SNMP] > [V1/V2c Configuration] > [Community String] を選択すると、[SNMP Community String Configuration] ページが表示されます。

許可の要件

このページにアクセスするには、サービスアビリティ権限が必要です。

説明

[SNMP Community String Configuration] ページを使用して、コミュニティ ストリングの表示、追加、更新、および削除を行います。コミュニティ ストリングは、SNMP V1 および V2c を使用するクライアントによる Emergency Responder へのアクセスを制御します。

表 B-3 で [SNMP Community String Configuration] ページについて説明します。

表 B-3　[SNMP Community String Configuration] ページ

フィールド	説明
[Community String Name] 列	選択したサーバに定義されているすべてのコミュニティ ストリングが表示されます。コミュニティ ストリングの名前をクリックすると、そのコミュニティ ストリングの情報が更新されます。

表 B-3　[SNMP Community String Configuration] ページ（続き）

フィールド	説明
[Add New] ボタンまたはアイコン	選択したサーバの新しいコミュニティ ストリングを追加します。このボタンをクリックすると、2 つ目の [SNMP Community String Configuration] ページが表示されます。 **（注）** [Add New] ボタンをクリックすると、[Add New] アイコンをクリックしたときと同じ画面が表示されます。
[Delete Selected] ボタンまたはアイコン	選択したコストを削除します。コミュニティ ストリングを削除するには、まずコミュニティ ストリングから選択する必要があります。コミュニティ ストリング名の左側にあるボックスをクリックして選択します。選択したサーバのすべてのコミュニティ ストリングを削除するには、[Community String Name] 列見出しの左側にあるボックスをクリックします。 **（注）** [Delete Selected] ボタンをクリックすると、ページの上部にある [Delete] アイコンをクリックしたときと同じアクションが開始されます。

2 つ目の [SNMP Community String Configuration] ページを使用して、新しい SNMP コミュニティ ストリングを追加し、既存の SNMP コミュニティ ストリングを更新します。

表 B-4 で 2 つ目の [SNMP Community String Configuration] ページについて説明します。

表 B-4　[SNMP Community String Configuration] ページ 2

フィールド	説明
Community String Name	新しいコミュニティ ストリングを追加する場合、このテキスト ボックスに新しいコミュニティ ストリングを入力します。既存のコミュニティ ストリングの情報を更新する場合、更新するコミュニティ ストリングの名前が表示されます。
Host IP Address Information	
Accept SNMP Packets from any host	任意のホストが SNMP を使用して Emergency Responder アクセスできるようにするには、このオプション ボタンをクリックします。
Accept SNMP Packets only from these hosts	SNMP を使用して Emergency Responder にアクセスできるホストを指定するには、このオプション ボタンをクリックします。SNMP アクセス権を持たせるホストを追加するには、新しいホストの IP アドレスを入力し、[Insert] をクリックします。SNMP アクセス権を持たせないホストを削除するには、そのホストの IP アドレスを入力し、[Remove] をクリックします。
[Access Privileges] プルダウン メニュー	新しいコミュニティ ストリングを追加すると、新しいコストのアクセス権を指定できます。コミュニティ ストリングを更新すると、現在のアクセス権限レベルが表示されます。使用できるアクセス権レベルは次のとおりです。 • ReadOnly • ReadWrite • ReadWriteNotify • NotifyOnly • None
[Insert] ボタンまたはアイコン	選択したサーバの新しいコミュニティ ストリングを挿入します。新しいコミュニティ ストリングを挿入するには、このページの他のフィールドを入力する必要があります。
[Clear] ボタンまたはアイコン	現在のページに表示されるコミュニティ ストリング情報をクリアします。

関連項目

- 「SNMP コミュニティ ストリングの設定」（P.6-3）

SNMP V1/V2c Notification Destination Configuration

[SNMP]>[V1/V2c Configuration]>[Notification Destination] を選択すると、[SNMP Notification Destination Configuration] ページが表示されます。

許可の要件

このページにアクセスするには、サービスアビリティ権限が必要です。

説明

[SNMP Notification Destination Configuration] ページを使用して、Emergency Responder SNMP エージェントからトラップ メッセージが送信される宛先を指定します。

表 B-5 で [SNMP Notification Destination Configuration] ページについて説明します。

表 B-5　[SNMP Notification Destination Configuration] ページ

フィールド	説明
[Server] プルダウン メニュー	SNMP 通知の宛先情報の表示、追加、更新、または削除を行うサーバの名前。サーバを選択すると、現在設定されている情報が次の形式で表示されます。 • Destination IP Address • Port Number • SNMP Version • Community String Name • Notification Type そのアドレスのデバイス情報を更新するには、[Destination IP Address] をクリックします。
[Destination IP Address] 列	選択したサーバに定義されているすべての通知先の IP アドレスが表示されます。このリストの IP アドレスをクリックすると、[Add/Update Notification Destination] ページが表示されます。
[Add New] ボタンまたはアイコン	選択したサーバの新しい通知先を追加します。このアイコンをクリックすると、[Add/Update Notification Destination] ページが表示されます。
[Delete Selected] ボタンまたはアイコン	選択した通知先を削除します。通知先を削除するには、まず通知先リストから選択する必要があります。通知先の左側にあるボックスをクリックして選択します。選択したサーバのすべての通知先を削除するには、[Destination IP Address] 列見出しの左側にあるボックスをクリックします。

2 つ目の [Add/Update Notification Destination] ページを使用して、新しい通知先を追加し、既存の通知先を更新します。

表 B-6 で [Add/Update Notification Destination] ページについて説明します。

表 B-6　[Add/Update Notification Destination] ページ

フィールド	説明
[Host IP Addresses] プルダウン メニュー	新しい通知先を追加するには、このプルダウン メニューから [Add New] を選択します。 **（注）** [SNMP Notification Destination Configuration] ページで既存の [Destination IP Address] をクリックしてこのページが表示された場合、[Host IP Address] および [Port Number] フィールドに、現在設定されている情報が表示されます。
[Host IP Address] フィールド	新しい通知先ホストの IP アドレス。

表 B-6　[Add/Update Notification Destination] ページ（続き）

フィールド	説明
[Port Number] フィールド	Emergency Responder SNMP エージェントから通知を受信する新しい通知先ホストのポート番号。
SNMP Version	SNMP V1 または V2c を指定するには、オプション ボタンのいずれかをクリックします。
[Notification Type] プルダウン メニュー	新しい通知先ホストの SNMP メッセージの種類を選択します。オプションは次のとおりです。 • Trap • Inform
[Community String] プルダウン メニュー	新しい通知先ホストのコミュニティ ストリングを選択します。
[Insert] ボタン	選択したサーバの新しい通知先を挿入します。
[Clear] ボタン	現在のページに表示される通知先情報をクリアします。

関連項目

- 「SNMP V1/V2C 通知ストリングの設定」（P.6-4）

SNMP User Configuration

[SNMP] > [V3 Configuration] > [User] を選択すると、[SNMP User Configuration] ページが表示されます。

許可の要件

このページにアクセスするには、サービスアビリティ権限が必要です。

説明

[SNMP User Configuration] ページを使用して、新しい SNMP V3 ユーザを設定します。

表 B-7 で [SNMP User Configuration] ページについて説明します。

表 B-7　[SNMP User Configuration] ページ

フィールド	説明
[Server] プルダウン メニュー	ユーザの表示、追加、更新、または削除を行うサーバの名前。サーバを選択すると、現在設定されている情報が次の形式で表示されます。 • User Name • Authentication Required • Authentication Protocol • Privacy Required • Privacy Protocol • Access Privileges [User Name] をクリックして [Add/Update SNMP User Configuration] ページを表示します。このページからそのユーザの情報を更新できします。
[Add New User] ボタンまたはアイコン	選択したサーバの新しいユーザを追加します。このアイコンをクリックすると、[Add/Update SNMP User Configuration] ページが表示されます。

表 B-7　[SNMP User Configuration] ページ（続き）

フィールド	説明
[Delete Selected] ボタンまたはアイコン	ユーザを削除します。ユーザを削除するには、まずユーザのリストから選択する必要があります。ユーザ名の左側にあるボックスをクリックして選択します。選択したサーバのすべてのユーザを削除するには、[User Name] 列見出しの左側にあるボックスをクリックします。

2 つ目の [SNMP User Configuration] ページを使用して、新しい SNMP V3 ユーザを設定します。

表 B-8 で [Add/Update SNMP User Configuration] ページについて説明します。

表 B-8　[SNMP User Configuration] ページ 2

フィールド	説明
[User Name] フィールド	新しい SNMP V3 ユーザの名前を入力します。 **（注）** [SNMP User Configuration] ページの既存のユーザ名をクリックしてこのページが表示された場合、このページには現在設定されている情報が表示されます。
Authentication Information	このセクションを使用して、次の情報を設定します。 • このユーザの認証が必要な場合、[Authentication Required] というチェックボックスをクリックします。 • [Password] および [Reenter Password] テキスト ボックスに新しいユーザの認証パスワードを入力します。 • 新しいユーザの認証プロトコルを選択するには、[MD5] または [SHA] のオプション ボタンをクリックします。
Privacy Information	このセクションを使用して、次の情報を設定します。 • このユーザのプライバシーが必要な場合、[Privacy Required] というチェックボックスをクリックします。 • [Password] および [Reenter Password] テキスト ボックスに新しいユーザのプライバシー パスワードを入力します。 • 新しいユーザのプライバシー プロトコルを選択するには、[DES] というオプション ボタンをクリックします。
Host IP Addresses Information	ページのこのセクションのオプション ボタンを使用して、次の操作を実行します。 • SNMP を使用して Emergency Responder にアクセスできるホストを指定します。Emergency Responder に対する SNMP アクセス権を持たせる新しいホストの IP アドレスを挿入できます。または、Emergency Responder に対する SNMP アクセス権を持たせないホストの IP アドレスを削除できます。 • 任意のホストが SNMP を使用して Emergency Responder にアクセスできるようにします。
[Access Privileges] プルダウン メニュー	新しいユーザを追加すると、このプルダウン メニューを使用して、その新しいユーザのアクセス プライバシーを指定できます。ユーザの情報を更新すると、このフィールドには最新のアクセス権限レベルが表示されます。使用できるアクセス権レベルは次のとおりです。 • ReadOnly • ReadWrite • ReadWriteNotify • NotifyOnly • None

表 B-8　[SNMP User Configuration] ページ 2（続き）

フィールド	説明
[Insert] ボタンまたはアイコン	選択したサーバの新しいユーザ情報を挿入します。
[Clear] ボタンまたはアイコン	現在のページに表示されるユーザ情報をクリアします。

関連項目

- 「SNMP ユーザの設定」（P.6-5）

SNMP V3 Notification Destination Configuration

[SNMP]>[V3 Configuration]>[Notification Destination] を選択すると、[SNMP Notification Destination Configuration] ページが表示されます。

許可の要件

このページにアクセスするには、サービスアビリティ権限が必要です。

説明

[SNMP V3 Notification Destination Configuration] ページを使用して、Emergency Responder SNMP エージェントからトラップ メッセージが送信される宛先を指定します。各通知ストリングは特定のユーザに関連付けられているため、[SNMP V3 Notification Destination] 情報のセキュリティは強化されています。

表 B-9 で [SNMP V3 Notification Destination Configuration] ページについて説明します。

表 B-9　[SNMP V3 Notification Destination Configuration] ページ

フィールド	説明
[Server] プルダウン メニュー	SNMP 通知の宛先情報の表示、追加、更新、または削除を行うサーバの名前。サーバを選択すると、現在設定されている情報が次の形式で表示されます。 • Destination IP Address • Port Number • Security Model • Security Name • Security Level • Notification Type そのアドレスのデバイス情報を更新するには、[Destination IP Address] をクリックします。このリストの IP アドレスをクリックすると、[Add/Update Notification Destination] ページが表示されます。
[Destination IP Address] 列	選択したサーバに定義されているすべての通知先の IP アドレスが表示されます。このリストの IP アドレスをクリックすると、[Add/Update Notification Destination] ページが表示されます。
[Add New] ボタンまたはアイコン	選択したサーバの新しい通知先を追加します。このアイコンをクリックすると、[Add/Update Notification Destination] ページが表示されます。

表 B-9　[SNMP V3 Notification Destination Configuration] ページ（続き）

フィールド	説明
[Delete Selected] ボタンまたはアイコン	選択した通知先を削除します。通知先を削除するには、まず通知先リストから選択する必要があります。通知先の左側にあるボックスをクリックして選択します。選択したサーバのすべての通知先を削除するには、[Destination IP Address] 列見出しの左側にあるボックスをクリックします。

2 つ目の [SNMP V3 Notification Destination] ページを使用して、新しい通知先を追加し、既存の通知先を更新します。

表 B-10 で 2 つ目の [SNMP V3 Notification Destination Configuration] ページについて説明します。

表 B-10　[SNMP V3 Notification Destination Configuration] ページ 2

フィールド	説明
[Host IP Addresses] プルダウン メニュー	新しい通知先を追加するには、このプルダウン メニューから [Add New] を選択します。 **（注）** [SNMP V3 Notification Destination Configuration] ページで既存の [Destination IP Address] をクリックしてこのページが表示された場合、[Host IP Address] および [Port Number] フィールドに、現在設定されている情報が表示されます。
[Host IP Address] フィールド	新しい通知先ホストの IP アドレス。
[Port Number] フィールド	Emergency Responder SNMP エージェントから通知を受信する新しい通知先ホストのポート番号。
[Notification Type] プルダウン メニュー	新しい通知先ホストの SNMP メッセージの種類を選択します。オプションは次のとおりです。 • Trap • Inform
Remote SNMP Engine ID	新しいリモート SNMP エンジン ID を追加するには、このプルダウン メニューから [Add New] を選択します。[Add New] を選択すると、新しい [Remote SNMP Engine ID] フィールドが表示されます。このフィールドに新しい Remote SNMP Engine ID を入力します。 **（注）** [Notification Type] プルダウンの通知の種類として [Inform] を選択した場合にのみ表示されます。 **（注）** [SNMP V3 Notification Destination Configuration] ページで既存の [Destination IP Address] をクリックしてこのページが表示された場合、[Remote SNMP Engine ID] フィールドに、現在設定されている情報が表示されます。
[Security Level] プルダウン メニュー	新しい V3 通知先のセキュリティ レベルを選択することができます。使用可能なオプションは次のとおりです。 • noAuthNoPriv • AuthNoPriv • authPriv

表 B-10　[SNMP V3 Notification Destination Configuration] ページ 2（続き）

フィールド	説明
User Information	現在設定されているユーザに関する情報が表示されます。また、ユーザを新しい V3 通知先に関連付けることができます。ページのこのセクションには、次の情報が含まれます。 • User Name • Authentication Protocol • Privacy Protocol 新しい V3 通知先に関連付けるユーザを選択するには、[User Name] 列の左側にあるオプションボタンをクリックします。
[Insert] ボタンまたはアイコン	選択したサーバの新しい通知先を挿入します。
[Clear] ボタンまたはアイコン	現在のページに表示される通知先情報をクリアします。

関連項目

- 「SNMP V3 通知先の設定」（P.6-5）

MIB2 SystemGroup Configuration

[SNMP] > [System Group Configuration] > [MIB2 System Group Configuration] を選択すると、[MIB2 System Group Configuration] ページが表示されます。

許可の要件

このページにアクセスするには、サービスアビリティ権限が必要です。

説明

[MIB2 System Group Configuration] ページを使用して、MIB2 管理モードの連絡先担当者の名前と所在地を指定します。

表 B-11 で [MIB2 System Group Configuration] ページについて説明します。

表 B-11　[MIB2 System Group Configuration] ページ

フィールド	説明
[Server] プルダウン メニュー	MIB2 の連絡先情報を更新するサーバの名前。サーバを選択すると、連絡先の名前と所在地を入力するフィールドが表示されます。
System Contact	MIB2 の連絡先の名前。
System Location	管理ノードの所在地。
[Update] ボタンまたはアイコン	更新した MIB2 の連絡先情報を保存します。
[Clear] ボタンまたはアイコン	現在のページに表示される MIB2 連絡先情報をクリアします。

関連項目

- 「MIB2 の設定」（P.6-6）

CPU and Memory Usage

[System Monitor] > [CPU & Memory Usage] を選択すると、[CPU and Memory Usage] ページが表示されます。

許可の要件

このページにアクセスするには、サービスアビリティ権限が必要です。

説明

[CPU and Memory Usage] ページを使用して、Emergency Responder システムの CPU とメモリ使用量を表示します。

表 B-12 で [CPU and Memory Usage] ページについて説明します。

表 B-12　[CPU and Memory Usage] ページ

フィールド	説明
Disable Auto-Refresh	このページに表示される情報の自動更新をディセーブルにするには、このチェックボックスをクリックします。
Set the screen reset value	このページを更新する頻度（秒）を指定します。
Set CPU Logging Interval	CPU 使用量をログに記録する頻度（秒）を指定します。5 ～ 600 秒の間隔を指定する必要があります。
Processors	このセクションには、多様なシステム コンポーネントが使用している CPU 時間の割合が表示されます。
Download CPU Log File	現在表示されている CPU およびメモリの使用量情報をファイルにダウンロードするには、このリンクをクリックします。このリンクをクリックすると、新しいページが開き、保存されているすべての CPU ログ ファイルが表示されます。この画面の詳細については、表 B-13 を参照してください。
Processor	プロセッサの名前。
%User	User モードに使用されているプロセッサ時間の割合。
%System	System モードに使用されているプロセッサ時間の割合。
%Nice	Nice タスクに使用されているプロセッサ時間の割合。 **（注）**　Nice は、プロセスの実行時を決定する、プロセスに関連付けられた値です。Nice タスクは、Nice 値が正のタスクのみです。
%Idle	プロセッサがアイドル状態の時間の割合。
%Irq	Interrupt Request（IRQ）に使用されているプロセッサ時間の割合。
%Softirq	ソフト IRQ に使用されているプロセッサ時間の割合。 **（注）**　ソフト IRQ は、延期できる割り込み要求です。
%I/O Wait	プロセッサが読み取りまたは書き込み操作を実行している時間の割合。
%CPU	最後の更新から経過した CPU 時間のプロセッサの共有。CPU 時間の割合として表現されます。
[Start Log] ボタン	現在の CPU 使用量のログ ファイルを開始します。 **（注）**　最大で 25 CPU ログ ファイルを作成できます。
Memory	このセクションには、異なる用途に割り当てられたメモリの割合が表示されます。

表 B-12　[CPU and Memory Usage] ページ（続き）

フィールド	説明
Download Memory Log File	現在表示されている CPU およびメモリの使用量情報をファイルにダウンロードするには、このリンクをクリックします。このリンクをクリックすると、新しいページが開き、保存されているすべての CPU ログ ファイルが表示されます。この画面の詳細については、表 B-14 を参照してください。
Total (KB)	使用できるメモリの合計（KB）。
Used (KB)	現在使用されているメモリの合計（KB）。
Free (KB)	使用できる空きメモリの合計（KB）。
Shared (KB)	共有プロセスに使用されているメモリの合計（KB）。
Buffers (KB)	バッファに使用されているメモリの合計（KB）。
Cached (KB)	キャッシュに使用されているメモリの合計（KB）。
Total Swap (KB)	合計スワップ領域（KB）
Used Swap (KB)	現在使用されているスワップ領域の合計（KB）。
Free Swap (KB)	使用できるスワップ領域の合計。
%VM Used	使用されている仮想メモリの合計。
[Start Log] ボタン	現在のメモリ使用量のログ ファイルを開始します。

[CPU Log Files] ページを使用して、CPU ログ ファイルを表示およびダウンロードします。

表 B-13 で [CPU Log Files] ページについて説明します。

表 B-13　[CPU Log Files] ページ

フィールド	説明
[Download] ボタン	選択したログ ファイルをダウンロードします。ファイルをダウンロードするには、まずファイルを選択します。選択するには、[File Name] の左側にあるボックスをクリックします。[File Name] 列見出しの左側にあるボックスをクリックすると、すべてのファイルがダウンロード対象として選択されます。
CPU Log Files	このセクションには、保存されている CPU ログ ファイルの詳細が表示されます。
File Name	保存されている CPU ログ ファイルの名前。ファイル名をクリックすると、新しい画面が開き、ログ ファイルの内容が表示されます。
Last Modified	CPU ログ ファイルの最終変更日時。
File Size (KB)	CPU ログ ファイルのサイズ（KB）。

[Memory Log Files] ページを使用して、メモリ ログ ファイルを表示およびダウンロードします。

表 B-14 で [Memory Log Files] ページについて説明します。

表 B-14　[Memory Log Files] ページ

フィールド	説明
[Download] ボタン	選択したログ ファイルをダウンロードします。ファイルをダウンロードするには、まずファイルを選択します。選択するには、[File Name] の左側にあるボックスをクリックします。[File Name] 列見出しの左側にあるボックスをクリックすると、すべてのファイルがダウンロード対象として選択されます。
Memory Log Files	このセクションには、保存されているメモリ ログ ファイルの詳細が表示されます。

表 B-14　[Memory Log Files] ページ（続き）

フィールド	説明
File Name	保存されているメモリ ログ ファイルの名前。ファイル名をクリックすると、新しい画面が開き、ログ ファイルの内容が表示されます。
Last Modified	メモリ ログ ファイルの最終修正日時。
File Size (KB)	メモリ ログ ファイルのサイズ（KB）。

関連項目

- 「CPU and Memory Usage ツールの使用」（P.6-7）

Processes

[System Monitor] > [Processes] を選択すると、[Processes] ページが表示されます。

許可の要件

このページにアクセスするには、サービスアビリティ権限が必要です。

説明

[Processes] ページを使用して、現在実行されているプロセスに関する情報を表示およびダウンロードします。

（注）　カテゴリごとに情報を並べ替えるには、[Processes] ページの各列見出しの隣にある上矢印と下矢印を使用します。

表 B-15 で [Processes] ページについて説明します。

表 B-15　[Processes] ページ

フィールド	説明
Disable Auto-Refresh	このページに表示される情報の自動更新をディセーブルにするには、このチェックボックスをクリックします。
Refresh Rate	このページを更新する頻度（秒）を指定するには、テキスト ボックスに数値を入力し、テキスト ボックスの右側にある [Set] ボタンをクリックします。
Download Log File	作成したログ ファイルをダウンロードするには、このリンクをクリックします。作成済みのログ ファイルがない場合、ログ ファイルをダウンロードできません。
Select	表示またはダウンロードするファイルを選択するには、チェックボックスをオンにします。
Process	プロセスの名前。
PID	プロセスの ID 番号。
%CPU	プロセスに使用されているプロセッサ時間の割合。
Status	タスクのプロセス ステータス。Running（R）、Sleeping（S）、Uninterruptible disk sleep（D）、Zombie（Z）、4 Traced（T）、Paging（P）。
Nice (Level)	プロセスのスケジューリング優先度を示します。Nice 値の 20 は最も高いプライオリティ、19 は最も低いプライオリティです。ほとんどのプロセスでデフォルトの Nice 値は 0 です。
Vm RSS (KB)	物理メモリに現在常駐している、コード、データ、およびスタックなどのサイズ（KB）。

表 B-15　[Processes] ページ（続き）

フィールド	説明
Vm Size (KB)	仮想メモリのサイズ（KB）。
Vm Data (KB)	仮想メモリに現在格納されているデータの合計（KB）。
Thread Count	現在実行されているプログラム スレッドの数。
Data Stack (KB)	データ スタックのサイズ（KB）。
Page Fault Count	メモリのロードが必要になったタスクの主要なページ エラーの数。

[View Selected Processes] ページを使用して、選択したプロセスを表示し、プロセス ログ ファイルをダウンロードします。

表 B-16 で [View Selected Processes] ページについて説明します。

表 B-16　[View Selected Processes] ページ

フィールド	説明
Disable Auto-Refresh	このページに表示される情報の自動更新をディセーブルにするには、このチェックボックスをクリックします。
Refresh Rate	このページを更新する頻度（秒）を指定するには、テキスト ボックスに数値を入力し、テキスト ボックスの右側にある [Set] ボタンをクリックします。
[View All Processes] ボタン	前の [Processes] 画面に戻ります。この画面には、実行されているすべてのプロセスが表示されます。
[Start Log] ボタン	このページに表示されている選択したプロセスのログを作成します。
[Download Log File] リンク	選択したプロセス ログ ファイルをダウンロードします。
Processes	このセクションには、選択したプロセスの詳細が表示されます。デフォルトは表 B-15 に表示されている値と同じです。

関連項目

- 「Processes ツールの使用」（P.6-8）

Disk Usage

[System Monitor] > [Disk Usage] を選択すると、[Disk Usage] ページが表示されます。

許可の要件

このページにアクセスするには、サービスアビリティ権限が必要です。

説明

[Disk Usage] ページを使用して、システムのさまざまなパーティションに使用されているディスク領域の割合を表示します。

（注）　カテゴリごとに情報を並べ替えるには、[Disk Usage] ページの各列見出しの隣にある上矢印と下矢印を使用します。

表 B-17 で [Disk Usage] ページについて説明します。

表 B-17　[Disk Usage] ページ

フィールド	説明
Disk Usage Details	
Partition	パーティションの名前。
Size	パーティションのサイズ。
Percentage Used	パーティションが使用しているディスク領域（割り当てられている合計ディスク領域の割合）。
Available Space	パーティションで現在使用できるディスク領域サイズ。
Used Space	使用しているパーティションのディスク領域サイズ。

関連項目

- 「Disk Usage ツールの使用」（P.6-9）

[System Logs] メニュー

[System Logs] メニューには、すべてのシステム ログがグループ化されている 3 つのサブメニューが含まれます。3 つのサブメニューは次のとおりです。

- [System Logs] > [Emergency Responder Logs]
- [System Logs] > [Platform Logs]
- [System Logs] > [DB Logs]
- [System Logs] > [CLI Output Files]

許可の要件

[System Logs] ページにアクセスできるサービスアビリティ権限が必要です。

（注） カテゴリごとに情報を並べ替えるには、各列見出しの隣にある上矢印と下矢印を使用します。

表 B-18 で [System Logs] ページについて説明します。

表 B-18　[System Logs] ページの一般的な説明

フィールド	説明
[Download] ボタン	選択したログ ファイルをダウンロードします。ファイルをダウンロードするには、まずファイルを選択します。選択するには、[File Name] の左側にあるボックスをクリックします。[File Name] 列見出しの左側にあるボックスをクリックすると、すべてのファイルがダウンロード対象として選択されます。 **（注）** 複数のログ ファイルを選択すると、ダウンロードするログ ファイルを含む Zip ファイルが作成されます。

表 B-18　[System Logs] ページの一般的な説明（続き）

フィールド	説明
File Name	ログ ファイルの名前。ファイル名をクリックすると、ログ ファイルの内容が新しい画面に表示されます。 **（注）** 内容の表示後にブラウザの [Back] ボタンをクリックすると、ログ ファイル ページに戻ります。
[Reload Log File] ボタン	すべての更新が表示されるように、現在表示されているログ ファイルを再ロードします。 **（注）** このボタンを使用できるのは、ファイル名をクリックし、特定のログ ファイルの内容を表示している場合のみです。
Last Modified	ログ ファイルの最終変更日。
File Size (KB)	ログ ファイルのサイズ（KB）。

表 B-19 に、3 つの [System Logs] サブメニューの各ログ一覧とその説明を示します。

表 B-19　個々の [System Log File] ページの説明

[Menu/Log File] ページ	説明
[CER Logs] > [CER Admin]	Emergency Responder Admin ログを表示またはダウンロードします。
[CER Logs] > [CER Server]	Emergency Responder Server ログを表示またはダウンロードします。
[CER Logs] > [CER Phone Tracking]	Emergency Responder Phone Tracking ログを表示またはダウンロードします。
[CER Logs] > [JTAPI]	JTAPI ログを表示またはダウンロードします。
[CER Logs] > [Tomcat]	Tomcat ログを表示またはダウンロードします。
[CER Logs] > [Event Viewer]	Emergency Responder Event ログを表示またはダウンロードします。
[CER Logs] > [Audio Driver]	Emergency Responder Audio Driver ログを表示またはダウンロードします。
[Platform Logs] > [CLI]	CLI 操作ログを表示またはダウンロードします。
[Platform Logs] > [CLM]	CLM（Cluster Manager）ログを表示またはダウンロードします。
[Platform Logs] > [Certificate Management/IPSec]	Certificate Management および IPSec ログを表示またはダウンロードします。
[Platform Logs] > [DRS]	DRS（Disaster Recovery System）ログを表示またはダウンロードします。
[Platform Logs] > [Install/Upgrade]	Installation および Upgrade ログを表示またはダウンロードします。
[Platform Logs] > [Remote Support]	Remote Account の作成および操作ログを表示またはダウンロードします。
[Platform Logs] > [Syslog]	Syslog ログを表示またはダウンロードします。
[Platform Logs] > [Servm]	Servm（Services Manager）ログを表示またはダウンロードします。
[DB Logs] > [Cerdbmon]	Cerdbmon ログを表示またはダウンロードします。
[DB Logs] > [Install DB]	InstallDB Utility ログを表示またはダウンロードします。
[CLI OutputFiles] > [Platform]	Platform ログ ファイルを表示またはダウンロードします。
[CLI OutputFiles] > [DB]	DB ログ ファイルを表示またはダウンロードします。

関連項目

- 「Cisco Emergency Responder ログの使用」（P.6-9）

APPENDIX C

Cisco Emergency Responder の Cisco Unified Operating System Administration Web インターフェイス

次のトピックでは、Cisco Emergency Responder（Emergency Responder）の Cisco Unified Operating System（OS）Administration Web インターフェイスについて説明します。

ServerGroup

[Show]>[ServerGroup] を選択すると、[ServerGroup] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[ServerGroup] ページは、サーバ グループの Emergency Responder サーバに関する情報を表示するために使用します。

表 C-1 に、[ServerGroup] ページの説明を示します。

表 C-1　[ServerGroup] ページ

フィールド	説明
ServerGroup	
Hostname	ホスト名が表示されます。
IP Address	ホストの IP アドレスが表示されます。
Alias	ホストのエイリアスが表示されます。
Type of Node	ホストのノード タイプが表示されます。

関連項目

- 「ハードウェア ステータスの表示」（P.7-4）

Hardware Status

[Show]>[Hardware] を選択すると、[Hardware Status] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Hardware Status] ページは、Emergency Responder ハードウェアに関する情報を表示するために使用します。

表 C-2 に、[Hardware Status] ページの説明を示します。

表 C-2　[Hardware Status] ページ

フィールド	説明
Hardware Resources	
Platform Type	プラットフォーム サーバのモデル ID
Processor Speed	プロセッサの速度
CPU Type	プラットフォーム サーバのプロセッサのタイプ
Memory	メモリの総量（MB 単位）
Object ID	プラットフォーム サーバのオブジェクト ID
OS Version	プラットフォーム サーバ上で実行しているオペレーティング システムのバージョン
RAID Details	プラットフォーム ハードウェアの詳細な概要

関連項目

- 「ハードウェア ステータスの表示」（P.7-4）

Network Configuration

[Show]>[Network] を選択すると、[Network Configuration] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Network Configuration] ページは、ネットワーク設定に関する情報を表示するために使用します。

（注）　表示されるネットワーク ステータス情報は、ネットワークの耐障害性がイネーブルになっているかどうかによって異なります。ネットワークの耐障害性が有効になっていると、イーサネット ポート 0 に障害が発生した場合、イーサネット ポート 1 が自動的にネットワーク通信を継承します。ネットワークの耐障害性がイネーブルになっている場合、ネットワーク ポートのイーサネット 0、イーサネット 1、および Bond 0 のネットワーク ステータス情報が表示されます。ネットワークの耐障害性がイネーブルになっていない場合、イーサネット 0 のステータス情報のみが表示されます。

表 C-3 に、[Network Configuration] ページの説明を示します。

表 C-3　[Network Configuration] ページ

フィールド	説明
Ethernet Details	
DHCP Status	イーサネット ポート 0 に対して DHCP がイネーブルになっているかどうかを表します。
Status	イーサネット ポート 0 および 1 について、ポートがアップまたはダウンのどちらであるかを表します。
IP Address	イーサネット ポート 0 の IP アドレス（ネットワーク耐障害性（NFT）がイネーブルの場合はイーサネット ポート 1 も）が表示されます。
IP Mask	イーサネット ポート 0 の IP マスク（NFT がイネーブルの場合はイーサネット ポート 1 も）が表示されます。
Link Detected	アクティブ リンクが存在するかどうかが示されます。
Queue Length	キューの長さが表示されます。
MTU	最大伝送ユニットが表示されます。
MAC Address	ポートのハードウェア アドレスが表示されます。
RX Stats	受信したバイト数およびパケット数に関する情報が表示されます。
TX Stats	送信したバイト数およびパケット数に関する情報が表示されます。
DNS Details	
Primary DNS	プライマリ ドメイン ネーム サーバの IP アドレスが表示されます。
Secondary DNS	セカンダリ ドメイン ネーム サーバの IP アドレスが表示されます。
Options	試行回数およびタイムアウト回数が表示されます。

表 C-3　[Network Configuration] ページ（続き）

フィールド	説明
Domain	サーバのドメインが表示されます。
Gateway	イーサネット ポート 0 のネットワーク ゲートウェイの IP アドレスが表示されます。

関連項目

- 「ネットワーク ステータスの表示」（P.7-4）

Software Packages

[Show]>[Software] を選択すると、[Software Packages] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Software Packages] ページは、ソフトウェアのバージョンおよびインストールされているソフトウェア オプションを表示するために使用します。

表 C-4 に、[Software Packages] ページの説明を示します。

表 C-4　[Software Packages] ページ

フィールド	説明
Partition Versions	アクティブ パーティションと非アクティブ パーティションで実行中のソフトウェアのバージョンが表示されます。
Active Version Installed Software Options	アクティブ バージョンにインストールされたソフトウェア オプションのバージョンが表示されます。
Inactive Version Installed Software Options	非アクティブ バージョンにインストールされたソフトウェア オプションのバージョンが表示されます。

関連項目

- 「インストールされているソフトウェアの表示」（P.7-4）

System Status

[Show]>[System] を選択すると、[System Status] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[System Status] ページは、Emergency Responder システムのステータスを表示するために使用します。

表 C-5 に、[System Status] ページの説明を示します。

表 C-5　[System Status] ページ

フィールド	説明
Host Name	Emergency Responder システムがインストールされている Cisco MCS ホストの名前
Date	オペレーティング システムのインストール時に指定された大陸と地域に基づく日付および時刻
Time Zone	インストール時に選択された時間帯
Locale	システムのロケール
Product Version	オペレーティング システムのバージョン。
Platform Version	プラットフォームのバージョン
Uptime	システムのアップタイム情報が表示されます。
CPU	CPU のキャパシティのうち、アイドル状態である割合、システム プロセスを実行している割合、ユーザ プロセスを実行している割合がそれぞれパーセント単位で表示されます。
Memory	メモリの使用状況に関する情報（メモリの合計量、メモリの空き容量、メモリの使用量）がそれぞれ KB 単位で表示されます。
Disk/active	アクティブなディスクの容量の合計、空き容量、使用量が表示されます。
Disk/inactive	非アクティブなディスクの容量の合計、空き容量、使用量が表示されます。
Disk/logging	ディスク ロギング用のディスクの容量の合計、空き容量、使用量が表示されます。

関連項目

- 「システム ステータスの表示」（P.7-4）

IP Preferences

[Show]>[IP Preferences] を選択すると、[IP Preferences] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[IP Preferences] ページは、システムで使用可能な登録済みポートのリストを表示するために使用します。表 C-6 に、[IP Preferences] ページの説明を示します。

表 C-6　[IP Preferences] ページ

フィールド	説明
Application	ポートを使用（リッスン）しているアプリケーションの名前。
Protocol	このポートで使用されているプロトコル（TCP や UDP など）。
Port Number	数字のポート番号。

表 C-6　[IP Preferences] ページ（続き）

フィールド	説明
Type	このポートで許可されるトラフィックのタイプ。 • [Public]：すべてのトラフィックが許可される • [Translated]：すべてのトラフィックが許可されるが、別のポートに転送される • [Private]：定義済みの一連のリモート サーバ（サーバ グループの他のサーバなど）からのトラフィックのみが許可される
Translated Port	このポートを宛先とするトラフィックは、[Port Number] 列に表示されているポートに転送されます。このフィールドが適用されるのは、[Translated] タイプのポートのみです。
Status	ポートの使用状況。 • [Enabled]：アプリケーションで使用されており、ファイアウォールで開かれている • [Disabled]：ファイアウォールでブロックされていて、未使用状態
Description	ポートの使用状況に関する簡単な説明。

関連項目

- 「IP 設定の表示」（P.7-5）

Ethernet Configuration

[Settings]>[IP]>[Ethernet] を選択すると、[Ethernet Configuration] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Ethernet Configuration] ページは、イーサネット設定を表示および変更するために使用します。

（注）　イーサネット設定はすべて Eth0 にのみ適用されます。Eth1 を対象とした設定はできません。Eth0 の Maximum Transmission Unit（MTU; 最大伝送ユニット）のデフォルトは 1500 です。

表 C-7 に、[Ethernet Configuration] ページの説明を示します。

表 C-7　[Ethernet Configuration] ページ

フィールド	説明
DHCP Information	
DHCP	DHCP がイネーブルまたはディセーブルであるかが示され、プルダウン メニューを使用して DHCP 設定を変更できます。
Host Information	
Hostname	サーバ名が表示されます（表示のみで設定は不可）。
Port Information	
IP Address	システムの IP アドレスが表示されます。テキスト ボックスに新しい IP アドレスを入力して、IP アドレスを変更できます。

表 C-7　[Ethernet Configuration] ページ（続き）

フィールド	説明
Subnet Mask	IP サブネット マスク アドレスが表示されます。テキスト ボックスに新しいサブネット マスクを入力して、マスクを変更できます。
Gateway Information	
Default Gateway	デフォルトのネットワーク ゲートウェイのゲートウェイ IP アドレスが表示されます。テキスト ボックスに新しい IP アドレスを入力して、ゲートウェイ IP アドレスを変更できます。
[Save] ボタンまたはアイコン	[Ethernet Configuration] ページのすべての変更内容を保存します。 **注意**　[Save] をクリックすると、マシンがリブートします。システムをシャットダウンしてリブートしない場合は [Save] をクリックしないでください。 **（注）**　すべての新しい IP アドレスを認識するには、サーバ グループの両方のサーバを手動でリブートする必要があります。

関連項目

- 「イーサネット設定の設定」（P.7-6）

サブスクライバ上でのパブリッシャ設定の設定

[Settings] > [IP] > [Publisher] を選択すると、[Publisher Settings] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

パブリッシャ設定ページは、パブリッシャのホスト名または IP アドレスを表示または変更するために使用します。

（注）　パブリッシャのホスト名 IP アドレスは、Emergency Responder Subscriber 上でのみ表示および変更でき、Emergency Responder パブリッシャ自体ではこれらを行えません。これらのフィールドの変更後には、Subscriber をただちにリブートする必要があります。

表 C-8

フィールド	説明
Hostname	この Subscriber の Emergency Responder Publisher のホスト名が表示されます。ホスト名を変更するには、テキスト ボックスに新しいホスト名を入力して、[Save] をクリックします。
IP Address	この Subscriber の Emergency Responder Publisher の IP アドレスが表示されます。IP アドレスを変更するには、テキスト ボックスに IP アドレスを入力し、[Save] をクリックします。
[Save] ボタンまたはアイコン	[Publisher Configuration Settings] ページの情報を保存します。

関連項目

「Emergency Responder サーバの IP アドレスの変更」（P.7-6）

NTP Server List

[Settings]>[NTP Servers] を選択すると、[NTP Server List] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[NTP Server List] ページは、NTP サーバを追加、変更、または削除するために使用します。パブリッシャ上では NTP サーバ設定しか構成することができません。

（注） 外部 NTP サーバが Stratum 9 以上（1 ～ 9）であることを確認してください。

（注） NTP サーバに対する変更は、完了するまで最大で 5 分かかる場合があります。NTP サーバを変更する場合、ページを更新して正しいステータスを表示する必要があります。

注意 NTP サーバを追加、変更、または削除した場合は、Publisher と Subscriber の両方をリブートする必要があります。

表 C-9 に、[NTP Server List] ページの説明を示します。

表 C-9　[NTP Server List] ページ

フィールド	説明
Status	見つかった設定済みの NTP サーバの台数が表示されます。
NTP Server	
[Hostname] または [IP Address] フィールド	設定済みの NTP サーバのホスト名または IP アドレスが表示されます。ホスト名または IP アドレスを変更するには、それをクリックして、新しいホスト名または IP アドレスを入力し、[Save] をクリックします。
[Add New] ボタンまたはアイコン	新しい NTP サーバを追加します。[Add New] をクリックした後に、新しい NTP サーバの IP アドレスのホスト名を入力し、[Save] をクリックします。
[Select All] ボタンまたはアイコン	一覧表示されたすべての NTP サーバを選択します。このボタンまたはアイコンをクリックすると、それぞれの NTP ホスト名または IP アドレスの左側と [Hostname] または [IP Address] 列見出しの左側にあるボックスにチェック マークが表示されます。 **（注）** [Select All] ボタンまたはアイコンは、1 つ以上の NTP サーバが以前に設定されている場合にのみ表示されます。
[Clear All] ボタンまたはアイコン	リストに表示されたすべての NTP サーバを選択します。このボタンまたはアイコンをクリックすると、すべてのチェック マークがオフになります。 **（注）** [Clear All] ボタンまたはアイコンは、1 つ以上の NTP サーバが以前に設定されている場合にのみ表示されます。

表 C-9　[NTP Server List] ページ（続き）

フィールド	説明
[Delete Selected] ボタンまたはアイコン	選択された NTP サーバを削除します。NTP サーバを削除するには、最初に、NTP サーバのリストから NTP サーバを選択する必要があります。NTP サーバ名の左側にあるボックスをクリックするとそれが選択されます。リストに表示されたすべての NTP サーバを選択するには、[Hostname] 列または [IP Address] 列の見出しの左側にあるボックスをクリックするか、または [Select All] をクリックします。 （注）　[Delete Selected] ボタンまたはアイコンは、1 つ以上の NTP サーバが以前に設定されている場合にのみ表示されます。

表 C-10 に、[NTP Server Configuration] ページの説明を示します。

表 C-10　[NTP Server Configuration] ページ

フィールド	説明
Status	見つかった設定済みの NTP サーバの台数が表示されます。
NTP Server Settings	
[Hostname] または [IP Address] フィールド	設定済みの NTP サーバのホスト名または IP アドレスが表示されます。ホスト名または IP アドレスを変更するには、それをクリックして、新しいホスト名または IP アドレスを入力し、[Save] をクリックします。
[Save] ボタンまたはアイコン	新しい NTP サーバに関する情報を保存します。

関連項目

- 「NTP サーバの設定」（P.7-8）

SMTP Settings

[Settings]>[SMTP] を選択すると、[SMTP Settings] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[SMTP Settings] ページは、SMTP ホストを手動で設定するために使用します。

表 C-11 に、[SMTP Settings] ページの説明を示します。

表 C-11　[SMTP Settings] ページ

フィールド	説明
Status	[SMTP Settings] ページのステータスが表示されます。
SMTP Host	
[Hostname] または [IP Address]	SMTP サーバのホスト名または IP アドレスをテキスト ボックスに入力します。

表 C-11　[SMTP Settings] ページ（続き）

フィールド	説明
Host Status	SMTP ホスト サーバのステータスが表示されます。
[Save] ボタンまたはアイコン	[SMTP Settings] ページの変更内容を保存します。

関連項目

- 「SNMP 接続の設定」（P.4-45）

Time Settings

[Settings]>[Time] を選択すると、[Time Settings] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Time Settings] ページは、サーバ時刻を手動で設定するために使用します。

（注）　サーバ時刻を手動で設定するには、設定済みの NTP サーバをすべて削除する必要があります。詳細については、「NTP Server List」（P.C-8）を参照してください。

注意　サーバ時刻を変更した場合は、パブリッシャとサブスクライバの両方をリブートする必要があります。

表 C-12 に、[Time Settings] ページの説明を示します。

表 C-12　[Time Settings] ページ

フィールド	説明
Date	プルダウン メニューを使用して、月、日、年、時、分、および秒を設定できます。
[Save] ボタンまたはアイコン	[Time Settings] ページの変更内容を保存します。

関連項目

- 「NTP Server List」（P.C-8）
- 「NTP サーバの設定」（P.7-8）
- 「時刻設定の設定」（P.7-9）

Version Settings

[Settings]>[Version] を選択すると、[Version Settings] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Version Settings] ページは、システムを再起動またはシャットダウンしたり、ソフトウェア バージョンを切り替えたりするために使用します。

（注） バージョンを切り替えるには、別のソフトウェア バージョンを非アクティブなパーティションにインストールしておく必要があります。

注意 このアクションを開始すると、システムが再起動して、一時的に使用できなくなります。

表 C-13 に、[Version Settings] ページの説明を示します。

表 C-13　[Version Settings] ページ

フィールド	説明
Status	現在のステータスが表示されます。
Installed Versions	
Active Version	アクティブなパーティションで実行しているバージョンが表示されます。
Inactive Version	非アクティブ パーティションのバージョンが表示されます。
[Restart] ボタンまたはアイコン	システムを再起動します。
[Shutdown] ボタンまたはアイコン	システムをシャットダウンします。
[Switch Versions] ボタンまたはアイコン	非アクティブなパーティション上のソフトウェア バージョンをアクティブにします。 **（注）** [Switch Versions] ボタンまたはアイコンは、非アクティブ パーティションにソフトウェア バージョンがインストールされている場合にのみ表示されます。

関連項目

- 「ソフトウェア バージョンの再起動、シャットダウン、または切り替え」（P.7-10）

Certificate List

[Security]>[Certificate Management] を選択すると、[Certificate List] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Certificate List] ページは、次を行うために使用します。

- 既存の証明書を検索する
- 新しい証明書を生成する
- 証明書をアップロードする
- CTL をアップロードする
- CSR を作成する

表 C-14 に、[Certificate List] ページの説明を示します。

表 C-14　[Certificate List] ページ

フィールド	説明
Status	現在のステータスが表示されます。
Certificate List	
Find certificate list where	検索する証明書リストの検索条件を入力します。 すべての証明書リストをファイル名で検索するには、プルダウン メニューから [File Name] を選択して、何も条件を入力せずに [Find] をクリックします。 すべての証明書リストを証明書名で検索するには、プルダウン メニューから [Certificate Name] を選択して、何も条件を入力せずに [Find] をクリックします。 検索を絞り込むには、次の手順に従います。 • プルダウン メニューから検索関係（[begins with] や [contains] など）を選択して、テキスト ボックスに検索文字列を入力します。 • フィールドの組み合わせを検索するには、**プラス** アイコン（+）をクリックして新しい検索パラメータを追加します。検索パラメータを削除するには、**マイナス** アイコン（–）をクリックします。追加したすべての検索パラメータを削除するには、[Clear Filter] をクリックします。 • [Rows per Page] プルダウン メニューを使用して、ページ単位で表示する行数を選択します。 すべての検索パラメータを入力したら、[Find] をクリックします。 検索で既存の証明書が見つかった場合は、その証明書に関する情報（[File Name]、[Certificate Name]、および [Certificate Type]）が [Certificate List] に表示されます。 [File Name] リンクをクリックすると、[Certificate Configuration] ページが表示されます。[Certificate Configuration] ページの詳細については、表 C-20 を参照してください。
[Generate New] ボタンまたはアイコン	新しい証明書を生成できます。[Generate New] をクリックすると、[Generate Certificate] ページが表示されます。[Generate Certificate] ページの説明については、表 C-15 を参照してください。
[Upload Certificate] ボタンまたはアイコン	リモート サーバから証明書をアップロードすることができます。[Upload Certificate] をクリックすると、[Upload Certificate] ページが表示されます。[Upload Certificate] ページの説明については、表 C-16 を参照してください。

表 C-14　[Certificate List] ページ（続き）

フィールド	説明
[Upload CTL] ボタンまたはアイコン	リモート サーバから証明書信頼リスト（CTL）をアップロードすることができます。[Upload CTL] をクリックすると、[Upload Certificate Trust List] ページが表示されます。[Upload Certificate Trust List] ページの説明については、表 C-17 を参照してください。
[Generate CSR] ボタンまたはアイコン	新しい Certificate Signing Request（CSR; 証明書署名要求）を作成することができます。[Generate CSR] をクリックすると、[Generate Certificate Signing Request] ページが表示されます。[Generate New] ページの説明については、表 C-18 を参照してください。
[Download CSR] ボタンまたはアイコン	CSR をダウンロードすることができます。[Download CSR] をクリックすると、[Download Certificate Signing Request] ページが表示されます。[Download Certificate Signing Request] ページの説明については、表 C-19 を参照してください。

表 C-15 に、[Generate Certificate] ページの説明を示します。

表 C-15　[Generate Certificate] ページ

フィールド	説明
Status	[Generate Certificate] ページの現在のステータスが表示されます。
Generate Certificate	
Certificate Name	プルダウン メニューから証明書名を選択することができます。
[Generate New] ボタンまたはアイコン	新しい証明書を作成します。最初に、プルダウン メニューから証明書名を選択する必要があります。
[Close] ボタンまたはアイコン	[Generate Certificate] ページを閉じます。

表 C-16 に、[Upload Certificate] ページの説明を示します。

表 C-16　[Upload Certificate] ページ

フィールド	説明
Status	[Upload Certificate] ページの現在のステータスが表示されます。
Upload Certificate	
Certificate Name	プルダウン メニューを使用して、アップロードする証明書の名前を選択します。
Root Certificate	ルート証明書の名前を入力します。
Upload File	[Browse] ボタンを使用して、アップロードするファイルを選択します。
[Upload File] ボタンまたはアイコン	[Upload Certificate] セクションで指定した証明書ファイルをアップロードします。
[Close] ボタンまたはアイコン	[Update Certificate] ページを閉じます。

表 C-17 に、[Upload CTL] ページの説明を示します。

表 C-17　[Upload CTL] ページ

フィールド	説明
Status	[Upload CTL] ページの現在のステータスが表示されます。
Upload Certificate	
Certificate Name	プルダウン メニューを使用して、アップロードする CTL ファイルの名前を選択します。
Root Certificate	ルート証明書の名前を入力します。
Upload File	[Browse] ボタンを使用して、アップロードするファイルを選択します。
[Upload File] ボタンまたはアイコン	[Upload Certificate Trust List] セクションで指定した証明書ファイルをアップロードします。
[Close] ボタンまたはアイコン	[Update CTL] ページを閉じます。

表 C-18 に、[Generate CSR] ページの説明を示します。

表 C-18　[Generate CSR] ページ

フィールド	説明
Status	[Generate CSR] ページの現在のステータスが表示されます。
Generate Certificate Signing Request	
Certificate Name	プルダウン メニューを使用して、生成する CTL ファイルの名前を選択します。
[Generate CSR] ボタンまたはアイコン	新しい CSR を生成します。
[Close] ボタンまたはアイコン	[Generate CSR] ページを閉じます。

表 C-19 に、[Download CSR] ページの説明を示します。

表 C-19　[Download CSR] ページ

フィールド	説明
Status	[Download CSR] ページの現在のステータスが表示されます。
Download Certificate Signing Request	
Certificate Name	プルダウン メニューを使用して、ダウンロードする CTL ファイルの名前を選択します。
[Download CSR] ボタンまたはアイコン	[Download Certificate Signing Request] セクションで指定した CSR をダウンロードします。
[Close] ボタンまたはアイコン	[Download CSR] ページを閉じます。

表 C-20 に、[Certificate Configuration] ページの説明を示します。

表 C-20　[Certificate Configuration] ページ

フィールド	説明
Status	[Certificate Configuration] ページの現在のステータスが表示されます。
Certificate Settings	証明書に関する次の情報が表示されます。 • ファイル名 • 証明書の名前 • 証明書タイプ • 証明書グループ • 説明
Certificate File Data	証明書ファイルの内容が表示されます。
[Delete] ボタンまたはアイコン	現在の証明書を削除します。
[Download] ボタンまたはアイコン	証明書をローカル システムにダウンロードします。

関連リンク

- 「証明書および証明書信頼リストの管理」（P.7-11）

Certificate Monitor

[Security]>[Certificate Monitor] を選択すると、[Certificate Monitor] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Certificate Monitor] ページは、次を行うために使用します。

- 開始時刻を指定する
- 頻度を指定する
- 電子メール通知をイネーブルにし、通知先の電子メール アドレスを指定する

表 C-21 に、[Certificate Monitor] ページの説明を示します。

表 C-21　[Certificate Monitor] ページ

フィールド	説明
Status	[Certificate Monitor] ページの現在のステータスが表示されます。
Certificate Monitor Configuration	
Notification Start Time	証明書が無効になる何日前に通知を送信してもらうかを入力します。
Notification Frequency	通知の頻度を入力し、いずれかのオプション ボタンをクリックして日数または時間数を指定します。

表 C-21　[Certificate Monitor] ページ（続き）

フィールド	説明
Enable Email Notification	このボックスをオンにすると、電子メール通知がイネーブルになります。 （注）　システムから通知を送信するようにするには、SMTP ホストを設定する必要があります。
Email ID	テキスト ボックスに通知先の電子メール アドレスを入力します。
[Save] ボタンまたはアイコン	[Certificate Monitor] に入力された情報を保存します。

関連項目

- 「証明書および証明書信頼リストの管理」（P.7-11）

IPSec Policy List

[Security]>[IPSec Configuration] を選択すると、[IPSec Policy List] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[IPSec Policy List] ページは、既存の IPSec ポリシーを表示したり、新たな IPSec ポリシーを追加したり、既存の IPSec ポリシーを変更したりするために使用します。

表 C-22 に、[IPSec Policy List] ページの説明を示します。

表 C-22　[IPSec Policy List] ページ

フィールド	説明
Status	[IPSec Policy List] ページの現在のステータスが表示されます。
IPSec Policy List	現在設定されている IPSec ポリシーが表示されます。ポリシーに関する [IPSec Policy Configuration] ページへのポリシー名リンクをクリックします。
[Add New] ボタンまたはアイコン	新しい IPSec ポリシーを追加します。[Add New] をクリックすると、[IPSec Policy Configuration] ページが表示されます。[IPSec Policy Configuration] ページの詳細については、表 C-23 を参照してください。

表 C-23 に、[IPSec Policy Configuration] ページの説明を示します。

表 C-23　[IPSec Policy Configuration] ページ

フィールド	説明
Status	[IPSec Policy Configuration] ページの現在のステータスが表示されます。
IPSec Policy Details	
Policy Group Name	
Policy Name	IPSec ポリシーの名前を指定します。
Authentication Method	認証方式を指定します。

表 C-23　[IPSec Policy Configuration] ページ（続き）

フィールド	説明
Preshared Key	[Authentication Method] フィールドで [Pre-shared Key] を選択した場合は、事前共有キーを指定します。
Peer Type	ピアのタイプが同じか異なるかを指定します。
Certificate Name	
Destination Address	宛先の IP アドレスまたは FQDN を指定します。
Destination Port	宛先のポート番号を指定します。
Source Address	ソースの IP アドレスまたは FQDN を指定します。
Source Port	ソースのポート番号を指定します。
Mode	[Tunnel] または [Transport] のモードを指定します。
Remote Port	宛先で使用されるポート番号を指定します。
Protocol	次のプロトコルまたは [Any] を指定します。 • TCP • UDP • Any
Encryption Algorithm	ドロップダウン リストから、暗号化アルゴリズムを選択します。選択肢は次のとおりです。 • DES • 3DES
Hash Algorithm	ハッシュ アルゴリズムを指定します。 • SHA1：フェーズ 1 IKE ネゴシエーションで使用されるハッシュ アルゴリズム • MD5：フェーズ 1 IKE ネゴシエーションで使用されるハッシュ アルゴリズム
ESP Algorithm	ドロップダウン リストから、ESP アルゴリズムを選択します。選択肢は次のとおりです。 • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
Phase 1 DH Group	
Phase One Life Time	フェーズ 1 の IKE ネゴシエーションのライフタイムを秒単位で指定します。
Phase One DH	ドロップダウン リストから、フェーズ 1 の DH 値を選択します。選択肢には、2、1、5、14、16、17、および 18 があります。
Phase 1 DH Group	
Phase Two Life Time	フェーズ 2 の IKE ネゴシエーションのライフタイムを秒単位で指定します。
Phase Two DH	ドロップダウン リストから、フェーズ 2 の DH 値を選択します。選択肢には、2、1、5、14、16、17、および 18 があります。
IPSec Policy Configuration	

表 C-23　[IPSec Policy Configuration] ページ（続き）

フィールド	説明
Enable Policy	チェックボックスをオンにすると、そのポリシーがイネーブルになります。
[Save] ボタンまたはアイコン	[IPSec Policy List] ページの変更内容を保存します。

関連項目

- 「IPSEC 管理」（P.7-17）

Software Installation/Upgrade

[Software Upgrades]>[Install/Upgrade] を選択すると、[Software Installation/Upgrade] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Software Installation/Upgrade] ページは、ソフトウェアを DVD/CD またはリモート サーバ上のファイルシステムからインストールまたはアップグレードするために使用します。

表 C-24 に、[Software Installation/Upgrade] ページの説明を示します。

表 C-24　[Software Installation/Upgrade] ページ

フィールド	説明
Status	[Software Installation/Upgrade] ページの現在のステータスが表示されます。
Software Location	
Source	インストール/アップグレードのソースを指定するために使用されるプルダウン メニュー。オプションは [DVD/CD] と [Remote Filesystem] です。
Directory	ファイルが保存されているディレクトリの名前。 （注）　アップグレード ファイルが Linux または Unix サーバ上にある場合は、ディレクトリ パスの先頭にフォワード スラッシュを入力する必要があります。たとえば、アップグレード ファイルが **patches** ディレクトリに存在する場合は、**/patches** と入力する必要があります。アップグレード ファイルが Windows サーバ上にある場合は、システム管理者に正しいディレクトリ パスを確認してください。
Server	ソフトウェアをダウロードするリモート サーバのホスト名または IP アドレス。
User Name	リモート サーバ上で設定されているユーザの名前。
User Password	リモート サーバ上でこのユーザ用に設定されたパスワード。
Transfer Protocol	使用される転送プロトコルを指定するために使用されるプルダウン メニュー。オプションは [ftp] と [sftp] です。 （注）　これらのオプションは、[Source] プルダウン メニューから [Remote Filesystem] を選択した場合にのみ使用することができます。[DVD/CD] を選択した場合は、このプルダウン メニューがグレー表示されます。

表 C-24　[Software Installation/Upgrade] ページ（続き）

フィールド	説明
[Cancel Install] ボタンまたはアイコン	インストール/アップグレード手順をキャンセルします。
[Next] ボタンまたはアイコン	インストール/アップグレード手順を継続します。

関連項目

- 「ソフトウェアのアップグレードとインストール」（P.7-19）

Ping Configuration

[Services]>[Ping] を選択すると、[Ping Configuration] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Ping Configuration] ページは、ping 要求を送信して他のシステムがネットワーク上で到達可能かどうかをテストするために使用します。

表 C-25 に、[Ping Configuration] ページの説明を示します。

表 C-25　[Ping Configuration] ページ

フィールド	説明
Status	[Ping Configuration] ページの現在のステータスが表示されます。
Ping Settings	
[Hostname] または [IP Address]	ping するシステムの IP アドレスまたはネットワーク名を入力するテキスト ボックス。
Ping Interval	ping 要求間の時間を秒単位で入力するテキスト ボックス。
Packet Size	ping 要求のパケット サイズを入力するテキスト ボックス。
Ping iterations	他のシステムに ping 要求を送信する回数を選択可能なプルダウン メニュー。使用可能なオプションは 1、5、25、または 100 回です。 **（注）** 複数回の ping を指定した場合は、**ping** コマンドを入力してもリアルタイムでは ping の日時が表示されません。**ping** コマンドでデータが表示されるのは、指定した ping の回数が完了した後です。
Validate IPSec	このチェックボックスをオンにすると、システムで IPSec が検証されます。
Ping Results	ping の結果が表示されるテキスト ボックス。
[Ping] ボタンまたはアイコン	ping 要求を送信します。

関連項目

- 「ping ユーティリティの使用」（P.7-26）

Remote Access Configuration

[Services]>[Remote Support] を選択すると、[Remote Access Configuration] ページが表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Remote Access Configuration] ページは、シスコのサポート担当者が、指定された期間にシステムにアクセスするために使用するリモート アカウントをセットアップするために使用します。アカウント有効期間が経過すると、シスコのサポート担当者はリモート サポート アカウントにアクセスできなくなります。

リモート アカウントを設定すると、システムでパス フレーズが生成されます。

次の手順に従って、リモート アカウント セットアップを完了します。

ステップ 1　シスコのサポート担当者に連絡して、リモート サポート アカウント名とパス フレーズを提供します。

ステップ 2　シスコのサポート担当者はパスフレーズをデコーダ プログラムに入力し、パス フレーズからパスワードを生成します。

ステップ 3　シスコのサポート担当者はデコードしたパスワードを使用して、お客様のシステムにリモート サポート アカウントでログインします。

まだリモート アカウントを作成していない場合は、[Remote Access Configuration] ページに移動したときに、新しいアカウントを作成できます。

表 C-26 に、[Remote Access Configuration] ページの説明を示します。

表 C-26　[Remote Access Configuration] ページ

フィールド	説明
Status	[Remote Access Configuration] ページの現在のステータスが表示されます。
Remote Access Account Information	
Account Name	新しいリモート アカウントの名前。アカウント名は、6 文字以上にし、すべて小文字のアルファベットにする必要があります。
Account Duration	リモート アカウントが存在する期間（日数）。
[Save] ボタンまたはアイコン	新しいリモート アカウントを作成します。[Add] をクリックする前に、[Account Name] と [Account Duration] を入力する必要があります。[Remote Access Configuration] ページが再表示されます。[Remote Access Configuration] ページのフィールドの説明については、表 C-27 を参照してください。
[Delete] ボタンまたはアイコン	現在設定されているリモート アカウントを削除します。 **（注）** [Delete] ボタンまたはアイコンは、既存のリモート アカウントが存在する場合にのみ表示されます。

すでにリモート アカウントを作成していた場合は、[Remote Access Configuration] ページに移動したときに、リモート アカウントが表示され、削除することができます。

表 C-27 に、[Remote Access Configuration] ページの説明を示します。

表 C-27　[Remote Access Configuration] ページ

フィールド	説明
Remote Access Account Information	
Account Name	リモート サポート アカウントの名前が表示されます。
Expiration	リモート アカウントが無効になる日時が表示されます。
Passphrase	生成されたパス フレーズが表示されます。
Decode Version	使用中のデコーダのバージョンが示されます。
[Delete] ボタンまたはアイコン	リモート アクセス アカウントの情報を削除します。

関連項目

- 「リモート サポートの設定」（P.7-26）

APPENDIX D

Cisco Emergency Responder の Disaster Recovery System Web インターフェイス

次のトピックでは、Cisco Emergency Responder（Emergency Responder）の Disaster Recovery System Administration Web インターフェイスのページのフィールドについて説明します。

Backup Device List

[Backup Device List] ページは、[Backup]>[Backup Device] を選択すると表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Backup Device List] ページを使用して、バックアップ デバイスの一覧表示、追加、および削除を行います。

表 D-1 は [Backup Device List] ページの説明です。

表 D-1　[Backup Device List] ページ

フィールド	説明
Backup Device List	設定済みのバックアップ デバイスを一覧表示し、デバイス名、デバイス タイプ、デバイス パスを表示します。そのデバイスの [Backup Device] ページを表示するには、[Device Name] リンクをクリックします。
[Add New] ボタン	新しいバックアップ デバイスを追加します。[Add] アイコンをクリックすると、[Backup Device] ページが表示されます。[Backup Device] ページについては、表 D-2 を参照してください。

表 D-1　[Backup Device List] ページ（続き）

フィールド	説明
[Select All] ボタンおよびアイコン	一覧表示されているすべてのバックアップ デバイスを選択します。
[Clear All] ボタンおよびアイコン	選択されているすべてのバックアップ デバイスの選択を解除します。
[Delete Selected] ボタンおよびアイコン	選択されているバックアップ デバイスを削除します。

表 D-2 は、新しいバックアップ デバイスの追加に使用する [Backup Device] ページの説明です。

表 D-2　[Backup Device] ページ

フィールド	説明
Backup Device Name	テキスト ボックスにデバイス名を入力します（必須）。
Select Destination	バックアップ先を選択するには、[Tape Device] または [Network Directory] オプション ボタンをクリックします（必須）。
Tape Device	プルダウン メニューからテープ デバイスの名前を選択します。
Network Directory	表示されたフィールドに、ネットワーク ディレクトリのサーバ名、パス名、ユーザ名、およびパスワードを入力します。
Number of backups to store on the Network Directory	プルダウン メニューを使用して、バックアップの数を選択します。
[Save] ボタンおよびアイコン	新しいバックアップ デバイスに関する情報を保存します。
[Back] ボタンおよびアイコン	[Backup Device List] ページに戻ります。

関連項目

- 「バックアップ デバイスの追加」（P.8-5）

Schedule List

[Schedule List] ページは、[Backup]>[Scheduler] を選択すると表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Schedule List] ページを使用して、現在スケジュールされているバックアップの一覧表示、新しいスケジュールの追加、スケジュールの有効化および無効化を行います。バックアップは、指定された日時に開始するようにスケジュールでき、1 回だけ実行するか、または指定された頻度で実行するかを設定したり、バックアップする機能を指定したりすることができます。

表 D-3 は [Schedule List] ページの説明です。

表 D-3　[Schedule List] ページ

フィールド	説明
Schedule List	スケジュールされたすべてのバックアップを一覧表示します。スケジュール リスト名、デバイス パス、およびスケジュールのステータスが表示されます。スケジュール リスト名のリンクをクリックすると、そのスケジュールの詳細が表示されます。 **（注）** スケジュール バックアップの作成後、スケジュールを有効にする必要があります。それには、[Schedule List] でスケジュールを選択し、[Enable Selected Schedules] ボタンまたはアイコンをクリックします。
[Add New] ボタンまたはアイコン	新しいスケジュールを追加します。[Add] ボタンまたはアイコンをクリックすると、[Scheduler] ページが表示されます。[Scheduler] ページについては、表 D-2 を参照してください。
[Select All] ボタンまたはアイコン	一覧表示されているすべてのスケジュールを選択します。 **（注）** [Select All] ボタンは、スケジュールが設定されていない場合にのみ表示されます。
[Clear All] ボタンまたはアイコン	選択されているすべてのスケジュールの選択を解除します。 **（注）** [Clear All] ボタンは、スケジュールが設定されていない場合にのみ表示されます。
[Delete Selected] ボタンまたはアイコン	選択されたスケジュールを削除します。 **（注）** [Delete Selected] ボタンは、スケジュールが設定されていない場合にのみ表示されます。
[Enable Selected Schedules] ボタンまたはアイコン	選択されているスケジュールを有効にします。 **（注）** [Enable Selected Schedules] アイコンは、スケジュールが設定されていない場合にのみ表示されます。
[Disable Selected Schedules] ボタンまたはアイコン	選択されたスケジュールを無効にします。 **（注）** [Disable Selected Schedules] ボタンは、スケジュールが設定されていない場合にのみ表示されます。

表 D-4 は [Scheduler] ページの説明です。

表 D-4　[Scheduler] ページ

フィールド	説明
Status	[Scheduler] ページのステータスを表示します。
Schedule Name	テキスト ボックスにスケジュールの名前を入力します。
Select Backup Device	プルダウン メニューからバックアップ デバイスの名前を選択します。
Select Features	バックアップする機能として [Emergency Responder] を選択します。
Start Backup at	
Date	プルダウン メニューから、バックアップを開始する年、月、および日を入力します。
Time	プルダウン メニューから、バックアップを開始する時間と分を入力します。
Frequency	
Once	1 回のバックアップをスケジュールするには、このオプション ボタンをクリックします。
Daily	毎日のバックアップをスケジュールするには、このオプション ボタンをクリックします。
Weekly	週単位のバックアップをスケジュールするには、このオプション ボタンをクリックします。 チェックボックスをオンにして、週単位のバックアップをスケジュールする日を指定します。
Monthly	月単位のバックアップをスケジュールするには、このオプション ボタンをクリックします。

表 D-4　[Scheduler] ページ（続き）

フィールド	説明
[Save] ボタンまたはアイコン	バックアップ スケジュール情報を保存します。
[Set Default] ボタンまたはアイコン	入力された情報を、スケジュールされたバックアップのデフォルトとして保存します。
[Disable Schedule] ボタンまたはアイコン	スケジュールを無効にします。スケジュールが現在無効になっている場合、このボタンはグレー表示されます。
[Enable Schedule] ボタンまたはアイコン	スケジュールを有効にします。スケジュールが現在有効になっている場合、このボタンはグレー表示されます。
[Back] ボタンまたはアイコン	[Scheduler List] ページに戻ります。

関連項目

- 「[Backup History] および [Restore History]」（P.D-5）
- 「Backup Status」（P.D-6）
- 「バックアップ スケジュールの作成と編集」（P.8-6）
- 「スケジュールのイネーブル化、ディセーブル化、および削除」（P.8-8）

Manual Backup

[Manual Backup] ページは、[Backup]>[Manual Backup] を選択すると表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Manual Backup] ページを使用して、手動バックアップを開始します。

（注）　手動バックアップを開始する前に、クラスタ内のすべてのサーバが実行されており、ネットワーク経由で到達可能なことを確認してください。実行されていないサーバや、ネットワーク経由で到達不可能なサーバはバックアップされません。

表 D-5 は [Manual Backup] ページの説明です。

表 D-5　[Manual Backup] ページ

フィールド	説明
Select Backup Device	プルダウン メニューからバックアップ デバイスの名前を選択します。
Select Features	バックアップする機能として [Emergency Responder] をオンにします。
[Start Backup] ボタンまたはアイコン	手動バックアップを開始します。

表 D-5　[Manual Backup] ページ（続き）

フィールド	説明
[Select All] ボタンまたはアイコン	一覧表示されているすべての機能を選択します。
[Clear All] ボタンまたはアイコン	選択されたすべての機能の選択を解除します。

関連項目

- 「Schedule List」（P.D-2）
- 「手動バックアップの開始」（P.8-8）

[Backup History] および [Restore History]

[Backup History] ページは、[Backup]>[History] を選択すると表示されます。[Restore History] ページは、[Restore]>[History] を選択すると表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

過去のバックアップに関する情報を表示するには、[Backup History] ページを使用します。過去の復元操作に関する情報を表示するには、[Restore History] ページを使用します。

表 D-6 は [Backup History] ページの説明です。

表 D-6　[Backup History] ページ

フィールド	説明
Backup History information	過去のバックアップに関する次の情報が表示されます。 • Tar ファイル名 • バックアップ デバイス • 完了日 • 結果 • バックアップされた機能
[Refresh] ボタンまたはアイコン	[Backup History] ページの情報を更新します。

表 D-7 は [Restore History] ページの説明です。

表 D-7　[Restore History] ページ

フィールド	説明
Restore History information	過去のバックアップに関する次の情報が表示されます。 • Tar ファイル名 • バックアップ デバイス • 完了日 • 結果 • 復元された機能
[Refresh] ボタンまたはアイコン	[Restore History] ページの情報を更新します。

関連項目

- 「Schedule List」（P.D-2）
- 「Manual Backup」（P.D-4）
- 「Backup Status」（P.D-6）
- 「Restore Wizard」（P.D-7）
- 「Restore Status」（P.D-9）
- 「バックアップ履歴および復元履歴の表示」（P.8-13）

Backup Status

[Backup Status] ページは、[Backup]>[Current Status] を選択すると表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Backup Status] ページを使用して、現在のバックアップに関するステータス情報を表示します。

表 D-8 は [Backup Status] ページの説明です。

表 D-8　[Backup Status] ページ

フィールド	説明
Status	現在のバックアップのステータスに関する情報を表示します。
Backup Details	現在のバックアップに関する次の情報が表示されます。 • Tar ファイル名 • バックアップ デバイス • 操作 • 完了率 • 機能 • サーバ • コンポーネント • ステータス • 結果[1] • 開始時間 • ログ ファイル[2]
[Refresh] ボタンまたはアイコン	現在のバックアップに関する情報を更新します。
[Cancel Backup] ボタンまたはアイコン	現在のバックアップをキャンセルします。

1. [Result] 列は、個々のコンポーネントのステージングの結果を示します。[Status] セクションは、全体的なバックアップ ステータスを示します。
2. ログ ファイルを表示するには、ファイル名をクリックします。

関連項目

- 「Schedule List」（P.D-2）
- 「バックアップ ステータスの確認」（P.8-8）

Restore Wizard

[Restore Wizard] ページは、[Restore]>[Restore Wizard] を選択すると表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Restore Wizard] ページを使用して、サーバのバックアップ ファイルまたはクラスタの前サーバの復元を行います。復元ウィザードは 4 つの Web ページで構成されています。

バックアップに使用するバックアップ デバイスを選択するには、[Step1 Restore—Choose Backup Device] ページを使用します。

表 D-9 は [Step1 Restore—Choose Backup Device] ページの説明です。

表 D-9　[Step1 Restore—Choose Backup Device] ページ

フィールド	説明
Status	復元操作の現在のステータスを示します。
Select Backup Device	プルダウン メニューを使用して、バックアップ デバイスを選択します。
[Next] ボタンまたはアイコン	復元ウィザードの次のページに進みます。
[Cancel] ボタンまたはアイコン	復元操作をキャンセルします。

復元するバックアップ tar ファイルを選択するには、[Step2 Restore—Choose Backup Tar File] ページを使用します。

表 D-10 は [Step2 Restore—Choose Backup Tar File] ページの説明です。

表 D-10　[Step2 Restore—Choose the Backup Tar File] ページ

フィールド	説明
Status	復元操作の現在のステータスを示します。
Select Backup File	プルダウン メニューを使用して、バックアップする tar ファイルを選択します。
[Back] ボタンまたはアイコン	復元ウィザードの前のページに戻ります。
[Next] ボタンまたはアイコン	復元ウィザードの次のページに進みます。
[Cancel] ボタンまたはアイコン	復元操作をキャンセルします。

復元する機能を選択するには、[Step3 Restore—Select the Type of Restore] ページを使用します。

表 D-11 は、[Step3 Restore—Select the Type of Restore] ページの説明です。

表 D-11　[Step3 Restore—Select the Type of Restore] ページ

フィールド	説明
Status	復元操作の現在のステータスを示します。
Select Features	バックアップする Emergency Responder 機能を選択するには、Emergency Responder 機能名の左側にあるボックスをクリックします。
[Back] ボタンまたはアイコン	復元ウィザードの前のページに戻ります。
[Next] ボタンまたはアイコン	復元ウィザードの次のページに進みます。
[Cancel] ボタンまたはアイコン	復元操作をキャンセルします。

復元するサーバを選択するには、[Step4 Restore—Final Warning for Restore] ページを使用します。

表 D-12 は [Step4 Restore—Final Warning for Restore] ページの説明です。

表 D-12　[Step4 Restore—Final Warning for Restore] ページ

フィールド	説明
Status	復元操作の現在のステータスを示します。
Warning	復元操作によって、選択されたサーバにある既存のデータすべてが上書きされることを伝える警告メッセージが表示されます。
Select the Servers to be restored for each Feature	Emergency Responder 機能名の下で、復元するサーバを選択します。それには、サーバ名の左側にあるチェックボックスをオンにします。
[Back] ボタンまたはアイコン	復元ウィザードの前のページに戻ります。
[Restore] ボタンまたはアイコン	復元操作を開始します。[Restore] をクリックする前に、復元するサーバを選択する必要があります。復元するパブリッシャまたはサブスクライバを選択できますが、その両方は選択できません。 **注意**　復元操作により、選択されたサーバ上の既存のデータはすべて上書きされます。
[Cancel] ボタンまたはアイコン	復元操作をキャンセルします。

関連項目

- 「[Backup History] および [Restore History]」（P.D-5）
- 「Restore Status」（P.D-9）
- 「バックアップ ファイルの復元」（P.8-9）
- 「サーバ グループの復元」（P.8-10）

Restore Status

[Restore Status] ページは、[Restore]>[Status] を選択すると表示されます。

許可の要件

このページにアクセスするには、プラットフォーム管理者の権限が必要です。

説明

[Restore Status] ページを使用して、復元操作のステータスを表示します。

表 D-13 は [Restore Status] ページの説明です。

表 D-13　[Restore Status] ページ

フィールド	説明
Status	現在の復元操作のステータスに関する情報を表示します。
Restore Details	現在の復元操作に関する次の情報が表示されます。 • Tar ファイル名 • バックアップ デバイス • 操作 • 完了率 • 機能 • サーバ • コンポーネント • ステータス • 結果[1] • 開始時間 • ログ ファイル[2]
[Refresh] ボタンまたはアイコン	現在の復元操作に関する情報を更新します。

1. [Result] 列は、個々のコンポーネントのステージングの結果を示します。[Status] セクションは、全体的な復元ステータスを示します。
2. ログ ファイルを表示するには、ファイル名をクリックします。

関連項目

- 「Restore Wizard」（P.D-7）
- 「[Backup History] および [Restore History]」（P.D-5）
- 「復元ステータスの表示」（P.8-13）
- 「バックアップ履歴および復元履歴の表示」（P.8-13）

Restore Status

APPENDIX E

Cisco Emergency Responder の Admin Utility Web インターフェイス

次のトピックでは、Cisco Emergency Responder（Emergency Responder）Admin Utility Web インターフェイスのページ上のフィールドについて説明します。

Cisco Unified CM のバージョンの更新

[Update]>[CUCM] を選択すると、[Update Unified CM Version] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Upgrade Unified CM Version] ページは、異なるバージョンの Cisco Unified Communications Manager にアップグレードするために使用します。

表 E-1 で [Upgrade CCM Version] ページについて説明します。

表 E-1　[Upgrade CCM Version] ページ

フィールド	説明
Status	現在の Cisco Unified Communications Manager バージョンが表示されます。
Cisco Unified CM Version Details	
Choose the Cisco Unified Communications Manager Version to Upgrade	プルダウン メニューを使用して、アップグレード対象の Cisco Unified Communications Manager version を選択します。

表 E-1　[Upgrade CCM Version] ページ（続き）

フィールド	説明
[Go] ボタン	[Go] をクリックしてアップグレード プロセスを開始します。 （注）　Publisher ノードと Subscriber ノードで個別に Cisco Unified CM バージョンを変更します。
[Cancel] ボタン	Cisco Unified Communications Manager のアップグレードをキャンセルします。

関連項目

- 「Cisco Unified Communications Manager のバージョンの変更」（P.9-1）

Update Cluster DB Host

[Update]>[Cluster DB Host] を選択すると、[Update Cluster DB Host] ページが表示されます。

許可の要件

このページにアクセスするには、システム管理者権限が必要です。

説明

[Update Cluster DB Host] ページは、新しいサーバを Emergency Responder のクラスタ データベース ホスト サーバとして指定するために使用します。

表 E-2 で [Update Cluster DB Host] ページについて説明します。

表 E-2　[Update Cluster DB Host] ページ

フィールド	説明
Status	現在のクラスタ データベース ホストの名前が表示されます
Cluster DB Host Details	
ClusterDB Hostname/IP Address	新しいクラスタ データベース ホストのホスト名（DNS が設定されている場合）または IP アドレスを入力します。 （注）　クラスタが複数のドメインに分散している場合、完全修飾ホスト名を入力します。
Password	新しいクラスタ データベース ホストのパスワードを入力します
Confirm Password	新しいクラスタ データベース ホストのパスワードを再入力します。

表 E-2　[Update Cluster DB Host] ページ（続き）

フィールド	説明
[Go] ボタン	[Go] ボタンをクリックし、新しいサーバをクラスタ データベース ホストとして指定します。 （注）　Emergency Responder Cluster DB ホストの詳細が更新されます。この変更を有効にするには、Emergency Responder サービスを再起動する必要があります。Emergency Responder のパブリッシャ サーバおよびサブスクライバ サーバをリブートして、Emergency Responder サービスを再起動してください。他のサービスが IP アドレスをキャッシュしているため、Emergency Responder サービスを再起動するだけでは機能しません。 これにより、このサーバ グループの Emergency Responder Cluster DB ホストの詳細のみが更新されます。この Emergency Responder クラスタの他のサーバは自動的に更新されません。詳細については、「Cisco Emergency Responder クラスタ データベース ホストの詳細の更新」（P.9-2）を参照してください。
[Cancel] ボタン	Update Cluster DB Host 操作をキャンセルします。

関連項目

- 「8.6 Cisco Emergency Responder クラスタおよびクラスタ DB ホスト」（P.4-28）
- 「Cisco Emergency Responder クラスタ データベース ホストの詳細の更新」（P.9-2）

Update Cluster DB Host

APPENDIX F

コマンド ライン インターフェイス

この付録では、Cisco Emergency Responder（Emergency Responder）プラットフォームで使用できる、基本的なオペレーティング システム機能を実行するための Cisco Unified Operating System（OS）コマンドについて説明します。Cisco Unified OS Administration Web インターフェイスからでも、これらの機能を使用できます。通常、コマンドライン インターフェイス（CLI）は、Cisco Unified OS Administration Web インターフェイスの使用中に問題が発生した場合にのみ使用します。

次のトピックでは、CLI を使用する方法について説明します。

CLI セッションの開始

CLI には、次の方法でリモートまたはローカルからアクセスできます。

- SSH セキュア シェルを使用して Emergency Responder に安全にアクセスすることで、Emergency Responder の管理に使用するワークステーションなど、Web クライアント ワークステーションからリモートで CLI にアクセスできます。
- インストールに使用したモニタとキーボードを使用して、またはシリアル ポートに接続されているターミナル サーバを使用して、CLI にローカルにアクセスすることができます。IP アドレスに問題がある場合は、この方法をご使用ください。

はじめる前に

インストール時に定義した次の情報を準備します。

- 主に使用する IP アドレスとホスト名
- 管理者 ID
- 管理者パスワード

この情報は、Emergency Responder プラットフォームにログインする際に必要になります。

CLI セッションを開始するには、次の手順を実行します。

手順

ステップ 1　アクセス方法に応じて、次のうち 1 つを実行します。

- リモート システムから、SSH セキュア シェルを使用して Emergency Responder プラットフォームにセキュアに接続します。SSH クライアントで、次のように入力します。

  ssh *adminname@hostname*

  ここで、*adminname* は管理者 ID、*hostname* はインストール時に定義したホスト名です。

  たとえば、**ssh admin@cer-1** と入力します。

- 直接接続の場合は、次のプロンプトが自動的に表示されます。

  ```
  cer-1 login:
  ```

  ここで、**cer-1** はシステムのホスト名を表します。

  インストール時に定義した管理者 ID を入力します。

いずれの場合にも、パスワードの入力を求めるプロンプトが表示されます。

ステップ 2　インストール時に定義したパスワードを入力します。

CLI プロンプトが表示されます。プロンプトは、次のように管理者 ID で表示されます。

```
admin:
```

これで、任意の CLI コマンドを使用できます。

CLI の基礎

次のトピックでは、CLI を使用して基本機能を実行する方法について説明します。

- 「コマンドのオートコンプリート」（P.F-2）
- 「ヘルプの利用方法」（P.F-3）
- 「CLI セッションの終了」（P.F-4）

コマンドのオートコンプリート

コマンドを補完するには、次のように Tab を使用します。

- コマンドの先頭部分を入力し、**Tab** を押してコマンドを完成させます。たとえば、**se** と入力して **Tab** キーを押すと、**se** が **set** コマンドに拡張されます。
- コマンド名全体を入力してから **Tab** を押すと、使用できるすべてのコマンドまたはサブコマンドが表示されます。たとえば、**set** と入力してから Tab を押すと、**set** のすべてのサブコマンドが表示されます。アスタリスク（*）は、サブコマンドが存在するコマンドを表します。
- コマンドが出現したら、そのまま Tab を押し続けます。現在のコマンド ラインが繰り返されます。これは、それ以上拡張できないことを示しています。

ヘルプの利用方法

どのコマンドについても次の 2 種類のヘルプを利用できます。

- コマンドの定義と、その使用例を含む詳細なヘルプ
- コマンドの構文だけを含む短いクエリ

コマンドのヘルプを利用するには、次の手順を実行します。

手順

ステップ 1　詳細なヘルプを表示するには、CLI プロンプトで次のように入力します。

help *command*

ここで、*command* にはコマンド名かコマンドとパラメータを指定します。例 F-1 を参照してください。

ステップ 2　コマンドの構文だけを表示するには、CLI プロンプトで次のように入力します。

*command***?**

ここで、*command* はコマンド名かコマンドとパラメータを表します。例 F-2 を参照してください。

（注）　疑問符（**?**）を **set** などのメニュー コマンドの後ろに入力すると、**Tab** キーと同様に機能して、使用できるコマンドのリストが表示されます。

例 F-1　詳細ヘルプの例

```
admin:help file list activelog

activelog help:
This will list active logging files

options are:
page - pause output
detail - show detailed listing
reverse - reverse sort order
date - sort by date
size - sort by size

file-spec can contain '*' as wildcards

Example:
admin:file list activelog platform detail
02 Dec,2004 12:00:59 <dir> drf
02 Dec,2004 12:00:59 <dir> log
16 Nov,2004 21:45:43 8,557 enGui.log
27 Oct,2004 11:54:33 47,916 startup.log
dir count = 2, file count = 2
```

例 F-2　クエリの例

```
admin:file list activelog?
Syntax:
file list activelog file-spec [options]
file-spec mandatory file to view
```

```
options optional page|detail|reverse|[date|size]
```

CLI セッションの終了

CLI セッションを終了するには、CLI プロンプトで **quit** を入力します。リモートからログインしている場合は、ログオフされ、**ssh** セッションが切断されます。ローカルでログインしている場合は、ログオフされ、ログイン プロンプトに戻ります。

Cisco Unified OS CLI コマンド

次の項では、Emergency Responder プラットフォーム上で実行されている Cisco Unified OS で使用できる CLI コマンドのリストと説明を示します。

（注） File I/O Reporting Service（FIOR）は、プロセスごとにファイル I/O を収集するカーネル ベースのデーモンを提供します。これは CLI から有効にする必要があります。デフォルトでは無効になっています。

delete account

このコマンドを使用すると、管理者のアカウントを削除できます。

コマンド構文

delete account *account-name*

パラメータ

- *account-name* は、管理者アカウントの名前を表します。

要件

コマンド特権レベル：4

アップグレード時の使用：不可

delete dns

このコマンドを使用すると、DNS サーバの IP アドレスを削除できます。

コマンド構文

delete dns *ip-address*

パラメータ

- *ip-address* は、削除する DNS サーバの IP アドレスを表します。

使用上のガイドライン

このコマンドの実行を続けるかどうかが尋ねられます。

注意　続行すると、ネットワーク接続が一時的に切断されます。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

delete ipsec

このコマンドを使用すると、IPSec ポリシーとアソシエーションを削除できます。

コマンド構文

delete ipsec

policy {**ALL** | *policy-name*}

association *policy-name* {**ALL** | *association-name*}

パラメータ

- *policy-name* は IPSec ポリシーを表します。
- *association-name* は IPSec アソシエーションを表します。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

delete process

このコマンドを使用すると、特定のプロセスを削除できます。

コマンド構文

delete process ***process-id*** [**force** | **terminate** | **crash**]

パラメータ

- *process-id* はプロセス ID 番号を表します。

オプション

- **force**：プロセスに停止を指示します。
- **terminate**：プロセスを停止するオペレーティング システムを表します。
- **crash**：プロセスをクラッシュさせ、クラッシュ ダンプを生成します。

使用上のガイドライン

（注）　**force** オプションは、コマンドだけではプロセスを削除できない場合にのみ使用してください。また、**terminate** オプションは、**force** によってプロセスを削除できない場合にのみ使用してください。

要件
コマンド特権レベル：1

アップグレード時の使用：可能

delete smtp

このコマンドを使用すると、SMTP ホストを削除できます。

コマンド構文
delete smtp

要件
コマンド特権レベル：1

次の場合に使用可能

file check

このコマンドは、/usr ディレクトリ ツリー内で、最新の新規インストールまたはアップグレードの後で追加、削除、またはサイズが変更されたファイルまたはディレクトリがないかどうかを調べ、結果を表示します。

コマンド構文
file check [*detection-size-kb*]

オプション
detection-size-kb：ファイルのサイズがこれ以上変化したときに、ファイルが変更されたとして表示される値です。

使用上のガイドライン
システムのパフォーマンスに影響が出る可能性があることが通知され、続行するかどうかが質問されます。

注意　このコマンドを実行するとシステムのパフォーマンスが影響を受ける可能性があるため、ピーク時間帯以外の時間にコマンドを実行することをお勧めします。

削除されたファイルと新しいファイルの両方が表示されます。

デフォルト
detection-size-kb のデフォルト値は 100 KB です。

要件
コマンド特権レベル：0

アップグレード時の使用：不可

file delete

このコマンドは、1 つまたは複数のファイルを削除します。

コマンド構文

file delete

activelog *directory/filename* [**detail**] [**noconfirm**]

inactivelog *directory/filename* [**detail**] [**noconfirm**]

install *directory/filename* [**detail**] [**noconfirm**]

パラメータ

- **activelog** はアクティブ側のログを指定します。
- **inactivelog** は、非アクティブ側のログを指定します。
- **install** は、インストール ログを指定します。
- *directory/filename* は、削除するファイルのパスとファイル名を指定します。*filename* には、ワイルドカード文字（*）を使用できます。

オプション

- **detail**：削除されたファイルと、日付および時刻のリストが表示されます。
- **noconfirm**：削除のたびに確認を求めることなくファイルを削除します。

使用上のガイドライン

注意　削除されたファイルを復旧させることはできません。Disaster Recovery System を使用すると、復旧できる可能性があります。

コマンドを入力した後、確認のためのプロンプトが表示されます。使用中のディレクトリやファイルは削除できません。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

例

次の例では、インストール ログを削除します。

```
file delete install install.log
```

file dump

このコマンドは、ファイルの内容を 1 ページずつ画面にダンプします。

コマンド構文

file dump

activelog *directory/filename* [**detail**] [**hex**]

inactivelog *directory/filename* [**detail**] [**hex**]

install *directory/filename* [**detail**] [**hex**]

パラメータ

- **activelog** はアクティブ側のログを指定します。
- **inactivelog** は、非アクティブ側のログを指定します。
- **install** は、インストール ログを指定します。
- *directory/filename* は、ダンプするファイルのパスとファイル名を指定します。*filename* では、1 つのファイルを表す場合に限り、ワイルドカード文字（*）を使用できます。

オプション

- **detail**：日付および時刻とともにリスト表示されます。
- **hex**：出力が 16 進数で表示されます。
- **regexp** *expression*：ファイル中の正規表現 *expression* に一致する行だけを表示します。
- **recent**：ディレクトリ内で最後に変更されたファイルを表示します。

要件

コマンド特権レベル：ログの場合は 1

アップグレード時の使用：可能

例

このコマンドは、ファイル _cdrIndex.idx の内容をダンプします。

```
file dump activelog cm/cdr/_cdrIndex.idx
```

file get

このコマンドは、SFTP を使用してファイルを別のシステムに送ります。

コマンド構文

file get

activelog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

inactivelog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

install *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

partBsalog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

salog *directory/filename* [**reltime**] [**abstime**] [**match**] [**recurs**]

パラメータ

- **activelog** はアクティブ側のログを指定します。
- **inactivelog** は、非アクティブ側のログを指定します。
- **install** は、インストール ログを指定します。
- **partBsalog** には、partBsalog ログ ディレクトリを指定します。
- **salog** には、salog ログ ディレクトリを指定します。

- *directory/filename* は、削除するファイルのパスを指定します。*filename* では、1 つのファイルを表す場合に限り、ワイルドカード文字（*）を使用できます。

オプション

- **abstime**：絶対的な時間。*hh:mm:MM/DD/YY hh:mm:MM/DD/YY* 形式で表します。
- **reltime**：相対的な時間。**months** | **weeks** | **days** | **hours** | **minutes** *値*で表します。
- **match**：ファイル名の中で、*文字列値* で表される特定の文字列との一致を検索します。
- **recurs**：サブディレクトリを含め、すべてのファイルを取得します。

使用上のガイドライン

指定したファイルが特定された後、SFTP ホスト、ユーザ名、パスワードの入力を求めるプロンプトが表示されます。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

例

次のコマンドは、オペレーティング システムの activelog ディレクトリ内で文字列「plat」に一致するすべてのファイルを取得します。

```
file get activelog platform match plat
```

次のコマンドは、特定の期間内のすべてのオペレーティング システム ログ ファイルを取得します。

```
file get activelog platform/log abstime 18:00:9/27/2005 18:00:9/28/2005
```

file list

このコマンドは、使用できるログ ディレクトリ内のログ ファイルをリスト表示します。

コマンド構文

file list

activelog *directory* [**page**] [**detail**] [**reverse**] [**date** | **size**]

inactivelog *directory* [**page**] [**detail**] [**reverse**] [**date** | **size**]

install *directory* [**page**] [**detail**] [**reverse**] [**date** | **size**]

partBsalog *directory* [**page**] [**detail**] [**reverse**] [**date** | **size**]

salog *directory* [**page**] [**detail**] [**reverse**] [**date** | **size**]

パラメータ

- **activelog** はアクティブ側のログを指定します。
- **inactivelog** は、非アクティブ側のログを指定します。
- **install** は、インストール ログを指定します。
- **partBsalog** には、partBsalog ログ ディレクトリを指定します。
- **salog** には、salog ログ ディレクトリを指定します。

- *directory* は、リスト表示するディレクトリのパスを指定します。1 つのディレクトリに解決される限り、*directory* にワイルドカード文字（*）使用できます。

オプション

- **detail**：日付および時刻を含む長いリスト
- **date**：日付によるソート
- **size**：サイズによるソート
- **reverse**：反対方向のソート
- **page**：出力を一度に 1 画面ずつ表示します。

要件

コマンド特権レベル：ログの場合は 1

アップグレード時の使用：可能

例

この例では、オペレーティング システム ログ ファイルの詳細がリスト表示されます。

```
file list activelog platform/log page detail
```

この例では、Emergency Responder ログに対して作成されたディレクトリがリスト表示されます。

```
file list activelog er/logs
```

この例では、サイズ指定したディレクトリ内の Emergency Responder ログがリスト表示されます。

```
file list activelog er/logs size
```

file search

このコマンドは、ログの内容を検索し、一致した行を一度に 1 ページずつ表示します。

コマンド構文

file search

activelog *directory/filename reg-exp* [**abstime** *hh:mm:ss mm/dd/yyyy hh:mm:ss mm/dd/yyyy*] [**ignorecase**] [**reltime** {**days** | **hours** | **minutes**} *timevalue*]

inactivelog *directory/filename reg-exp* [**abstime** *hh:mm:ss mm/dd/yyyy hh:mm:ss mm/dd/yyyy*] [**ignorecase**] [**reltime** {**days** | **hours** | **minutes**} *timevalue*]

install *directory/filename reg-exp* [**abstime** *hh:mm:ss mm/dd/yyyy hh:mm:ss mm/dd/yyyy*] [**ignorecase**] [**reltime** {**days** | **hours** | **minutes**} *timevalue*]

パラメータ

- **activelog** はアクティブ側のログを指定します。
- **inactivelog** は、非アクティブ側のログを指定します。
- **install** は、インストール ログを指定します。
- *reg-exp* は、正規表現を表します。
- *directory/filename* は、検索するファイルのパスを表します。ワイルドカード文字（*）を使用して、ファイル名の全体または一部を表すことができます。

オプション

- **abstime**：ファイルの作成時刻に基づいて、検索するファイルを指定します。開始時刻と終了時刻を入力してください。
- **days|hours|minutes**：ファイルの経過時間を日数、時間、または分によって指定します。
- **ignorecase**：検索時に大文字と小文字の違いを無視します。
- **reltime**：ファイルの作成時刻に基づいて、検索するファイルを指定します。検索するファイルの経過時間を入力します。
- *hh:mm:ss mm/dd/yyyy*：絶対時刻。形式は、時:分:秒 月/日/年。
- *timevalue*：検索するファイルの経過時間。この値の単位は、{**days** | **hours** | **minutes**} オプションで指定します。

使用上のガイドライン

検索条件は正規表現の形で記述します。正規表現とは、検索パターンを表す特殊なテキスト文字列です。

検索条件が 1 つのファイル内にのみ見つかった場合は、そのファイル名が出力の一番上に表示されます。検索条件が複数のファイル内に見つかった場合は、出力の各行の先頭に、一致が見つかったファイルの名前が示されます。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

例

```
file search activelog platform/log/platform.log Err[a-z] ignorecase
```

file tail

このコマンドは、ログ ファイルをテイル（最後の数行を出力）します。

コマンド構文

file tail

activelog *directory/filename* [**detail**] [**hex**] [**lines**]

inactivelog *directory/filename* [**detail**] [**hex**] [**lines**]

install *directory/filename* [**detail**] [**hex**] [**lines**]

パラメータ

- **activelog** はアクティブ側のログを指定します。
- **inactivelog** は、非アクティブ側のログを指定します。
- **install** は、インストール ログを指定します。
- *directory/filename* は、テイルするファイルのパスを指定します。filename では、1 つのファイルを表す場合に限り、ワイルドカード文字（*）を使用できます。

オプション

- **detail**：日付および時刻を含む長いリスト

- **hex**：16 進数リスト
- **lines**：表示する行数

要件

コマンド特権レベル：ログの場合は 1

アップグレード時の使用：可能

例

この例では、オペレーティング システムの CLI ログ ファイルがテイルされます。

```
file tail activelog platform/log/cli00001.log
```

file view

このコマンドは、ファイルの内容を表示します。

コマンド構文

file view

activelog *directory/filename*

inactivelog *directory/filename*

install *directory/filename*

system-management-log

パラメータ

- **activelog** はアクティブ側のログを指定します。
- **inactivelog** は、非アクティブ側のログを指定します。
- **install** は、インストール ログを指定します。
- **system-management-log** は、Integrated Management Log（IML）の内容を表示します。
- *directory/filename* は、表示するファイルのパスを指定します。*filename* では、1 つのファイルを表す場合に限り、ワイルドカード文字（*）を使用できます。

使用上のガイドライン

注意　このコマンドは、バイナリ ファイルを表示するためには使用しないでください。ターミナル セッションが終了することがあります。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

例

この例では、インストール ログが表示されます。

```
file view install install.log
```

この例では、特定の CDR ファイルが表示されます。

```
file view activelog er/logs/CERAdmin01.log
```

run sql

このコマンドを使用すると、SQL コマンドを実行できます。

コマンド構文
run sql *sql_statement*

パラメータ
- *sql_statement* は、実行する SQL コマンドを表します。

要件
コマンド特権レベル：1

アップグレード時の使用：不可

例
この例では、SQL コマンドが実行されます。

```
run sql select * from cerserver
```

set account

このコマンドは、オペレーティング システム上に新規アカウントを設定します。

コマンド構文
set account *name*

パラメータ
- *name* は、新規アカウントのユーザ名を表します。

使用上のガイドライン
ユーザ名を入力すると、この新規アカウントの特権レベルおよびパスワードの入力を求められます。

要件
コマンド特権レベル：0

アップグレード時の使用：不可

set account enable

このコマンドは、パスワードの非アクティブ化機能のためアカウントがディセーブルになっている場合、ユーザ アカウントをイネーブルにするために使用します。

パスワード非アクティビティ期間は、パスワードの有効期限が切れてからアカウントがディセーブルになるまでの、アクティビティがなかった日数です。

このコマンドを実行すると、現在のシステム設定でユーザ アカウントがイネーブルになります。システム設定は、パスワードの最小日数、パスワードの最大日数、パスワード非アクティビティ期間です。

コマンド構文
set account enable *userid*

パラメータ
userid はユーザ アカウントの名前です。

例
set account enable test

Enabling the account 'test' with current settings....

.....

Successfully enabled account 'test'

要件
コマンド特権レベル：1

アップグレード時の使用：可能

show accountlocking

現在のアカウントのロック設定を表示します。

コマンド構文
show accountlocking

要件
コマンド特権レベル：1

アップグレード時の使用：可能

set accountlocking disable

このコマンドは、現在の管理アカウントのアカウントロックをディセーブルにします。

コマンド構文
set accountlocking disable

要件
コマンド特権レベル：1

アップグレード時の使用：可能

set accountlocking enable

このコマンドは、現在の管理アカウントのアカウントロックをイネーブルにします。

コマンド構文
set accountlocking enable

要件
コマンド特権レベル：0
アップグレード時の使用：可能

set accountlocking unlocktime

このコマンドは、Emergency Responder OS 管理アカウントのロック解除時間を秒で設定するために使用します。

有効な値は、300 秒以上 3600 秒（60 分）未満です。

コマンド構文
set accountlocking unlocktime *seconds*

パラメータ
seconds は秒でのロック解除時間です。

要件
コマンド特権レベル：1
アップグレード時の使用：可能

set cert delete

ユニットの IPSec の証明書 test.pem を削除します。

コマンド構文
set cert delete [*unit*] [*name*]

パラメータ
unit は信頼カテゴリの名前です。
name は証明書ファイルの名前です。

例：
set cert delete ipsec test.pem

要件
コマンド特権レベル：1
アップグレード時の使用：不可

set cert import

タイプ own | trust のユニット名の証明書をインポートします。

コマンド構文
set cert import [*unit name*]

パラメータ
name はユニット名です。

例：
set cert import trust tomcat
Successfully regenerated certificate for tomcat.
Please restart services related to tomcat for the new certificate to become active.

要件
コマンド特権レベル：1
アップグレード時の使用：可能

set csr gen

ユニット名の証明書を再生成します。

コマンド構文
set csr gen [*name*]

パラメータ
name は tomcat などのユニット名です。

例
set csr gen tomcat
Successfully regenerated certificate for tomcat.
Please restart services related to tomcat for the new certificate to become active.

要件
コマンド特権レベル：1
アップグレード時の使用：不可

set cert regen

ユニット名の証明書を再生成します。

コマンド構文
set cert regen [*name*]

パラメータ
Name はユニット名です。

例：
set cert regen tomcat
Successfully regenerated certificate for tomcat.

Please restart services related to tomcat for the new certificate to become active.

要件
コマンド特権レベル：1
アップグレード時の使用：不可

show csr list

選択した独自の CSR ファイルを表示します。

コマンド構文
show csr list type

例
show csr list own
tomcat/tomcat.csr
Vipr-QuetzalCoatl/Vipr-QuetzalCoatl.csr

set commandcount

このコマンドは、CLI コマンド プロンプトを変更して、実行済みの CLI コマンドの数が表示されるようにします。

コマンド構文
set commandcount {**enable** | **disable**}

パラメータ
- *unit-name* は、再生成する証明書の名前を表します。

要件
コマンド特権レベル：1
アップグレード時の使用：不可

set cli pagination

現在の CLI セッションに対し、自動的なページ分割を**オン**または**オフ**にします。

コマンド構文
set cli pagination {on | off}

パラメータ
- **on** を指定すると、ページ分割がオンになります。
- **off** を指定すると、ページ分割がオフになります。

要件

レベル特権：1

コマンド特権：1

アップグレード時の使用：不可

例

```
admin:set cli pagination off
Automatic pagination is turned off
```

set date

このコマンドは、システムで日付を設定します。

コマンド構文

set date HH:mm:ss:MM/DD/YY

HH:mm:ss: 時間形式（24 時間形式）

MM/DD/YY：日付形式。

（注）　次の形式も指定できます。

MM/DD/YYYY：日付形式。

例

日時を 2008 年 2 月 13 日午後 2:10:33 に設定する場合

set date 14:10:33:02/13/08

要件

コマンド特権レベル：1

アップグレード時の使用：不可

set ipsec

IPSec ポリシーとアソシエーションを設定します。

コマンド構文

set ipsec

policy {**ALL** | *policy-name*}

association *policy-name* {**ALL** | *association-name*}

パラメータ

- *policy-name* は IPSec ポリシーを表します。
- *association-name* は IPSec アソシエーションを表します。

要件
コマンド特権レベル：1
アップグレード時の使用：不可

set logging

このコマンドを使用すると、ロギングをイネーブルまたはディセーブルにすることができます。

コマンド構文
set logging {**enable** | **disable**}

要件
コマンド特権レベル：0
アップグレード時の使用：不可

set network cluster publisher hostname

このコマンドは、クラスタ パブリッシャのホスト名を設定します。
ネットワークが新しい構成で再起動している間、ネットワーク接続が一時的に失われます。

コマンド構文
set network cluster publisher hostname *name*
name は割り当てられるホスト名です。

set network cluster publisher ip

このコマンドは、クラスタ パブリッシャの IP アドレスを設定します。
ネットワークが新しい構成で再起動している間、ネットワーク接続が一時的に失われます。

コマンド構文
set network cluster publisher ip addr

set network dhcp

このコマンドは、イーサネット インターフェイス 0 の DHCP をイネーブルまたはディセーブルにします。イーサネット インターフェイス 1 は設定できません。

コマンド構文
set network dhcp eth0

enable

disable *node_ip net_mask gateway_ip*

パラメータ

- **eth0** はイーサネット インターフェイス 0 を指定します。
- **enable** を指定すると DHCP がイネーブルになります。
- **disable** を指定すると DHCP がディセーブルになります。
- *node_ip* は、サーバの新しい固定 IP アドレスです。
- *net_mask* は、サーバのサブネット マスクです。
- *gateway_ip* は、デフォルト ゲートウェイの IP アドレスです。

使用上のガイドライン

このコマンドの実行を続けるかどうかが尋ねられます。

注意　続行すると、システムが再起動されます。いずれかの IP アドレスを変更した場合は、必ずすべてのノードを再起動することをお勧めします。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

set network dns

プライマリまたはセカンダリ DNS サーバの IP アドレスを設定します。

コマンド構文

set network dns {**primary** | **secondary**} *ip-address*

パラメータ

- *ip-address* は、プライマリまたはセカンダリ DNS サーバの IP アドレスを表します。

使用上のガイドライン

このコマンドの実行を続けるかどうかが尋ねられます。

注意　続行すると、ネットワーク接続が一時的に切断されます。DNS サーバの IP アドレスを変更する場合、Cisco Tomcat を再起動する必要があります。詳細については、「utils service」（P.F-79）を参照してください。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

set network dns options

DNS オプションを設定します。

コマンド構文
set network dns options [**timeout** *seconds*] [**attempts** *number*] [**rotate**]

パラメータ
- **timeout** には、DNS 要求タイムアウトを設定します。
- **attempts** には、DNS 要求を試みる回数を設定します。
- **rotate** を指定すると、設定されている DNS サーバのローテーションを行い、負荷を分散させます。
- *seconds* には、DNS タイムアウト時間を秒単位で指定します。
- *number* には試行回数を指定します。

要件
コマンド特権レベル：0

アップグレード時の使用：可能

set network domain

システムのドメイン名を設定します。

コマンド構文
set network domain *domain-name*

パラメータ
- *domain-name* は、割り当てるシステム ドメインを表します。

使用上のガイドライン
このコマンドの実行を続けるかどうかが尋ねられます。

注意　続行すると、ネットワーク接続が一時的に切断されます。

要件
コマンド特権レベル：1

アップグレード時の使用：不可

set network failover

このコマンドは、ネットワーク耐障害性をイネーブルまたはディセーブルにします。

コマンド構文
failover {**enable** | **disable**}

パラメータ
- **enable** は、Network Fault Tolerance をイネーブルにします。
- **disable** を指定すると、ネットワーク耐障害性がディセーブルになります。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

set network gateway

ネットワーク ゲートウェイの IP アドレスを設定します。

コマンド構文

set network gateway *ip-address*

パラメータ

- *ip-address* は、割り当てるネットワーク ゲートウェイの IP アドレスを表します。

使用上のガイドライン

このコマンドの実行を続けるかどうかが尋ねられます。

注意　続行すると、システムが再起動されます。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

set network ip

イーサネット インターフェイス 0 の IP アドレスを設定します。イーサネット インターフェイス 1 は設定できません。

コマンド構文

set network ip eth0 *ip-address ip-mask*

パラメータ

- **eth0** はイーサネット インターフェイス 0 を指定します。
- *ip-address* は、割り当てる IP アドレスを表します。
- *ip-mask* は、割り当てる IP マスクを表します。

使用上のガイドライン

このコマンドの実行を続けるかどうかが尋ねられます。

注意　続行すると、システムが再起動されます。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

set network mtu

最大 MTU 値を設定します。

コマンド構文
set network mtu *mtu_max*

パラメータ
- *mtu_max* には、最大 MTU 値を指定します。

（注） システムのデフォルトの MTU 値は 1500 です。

使用上のガイドライン
このコマンドの実行を続けるかどうかが尋ねられます。

注意 続行すると、システムのネットワーク接続が一時的に失われます。

要件
レベル特権：1

コマンド特権：1

アップグレード時の使用：不可

例
```
admin:set network mtu 576
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue?

Enter "yes" to continue or any other key to abort

yes
executing...
```

set network max_ip_contrack

このコマンドは ip_conntrack_max 値を設定します。

コマンド構文
set network max_ip_conntrack *ip_conntrack_max*

パラメータ
- *ip_conntrack_max* には、ip_conntrack_max の値を指定します。

set network nic

このコマンドは、イーサネット インターフェイス 0 のプロパティを設定します。イーサネット インターフェイス 1 は設定できません。

コマンド構文

set network nic eth0 [**auto en** | **dis**] [**speed 10** | **100**] [**duplex half** | **full**]

パラメータ

- **eth0** はイーサネット インターフェイス 0 を指定します。
- **auto** には、自動ネゴシエーションをイネーブルにするかディセーブルにするかを指定します。
- **speed** には、イーサネット接続の速度を 10 Mbps にするか 100 Mbps にするかを指定します。
- **duplex** には半二重または全二重を指定します。

使用上のガイドライン

このコマンドの実行を続けるかどうかが尋ねられます。

（注） 一度にアクティブにできる NIC は 1 つだけです。

注意 続行すると、NIC がリセットされる間ネットワーク接続が一時的に失われます。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

set network pmtud

パス MTU ディスカバリをイネーブルまたはディセーブルにします。

コマンド構文

set network pmtud [**enable** | **disable**]

パラメータ

- **enable** を指定すると、パス MTU ディスカバリがイネーブルになります。
- **disable** を指定すると、パス MTU ディスカバリがディセーブルになります。

使用上のガイドライン

このコマンドの実行を続けるかどうかが尋ねられます。

注意 続行すると、システムのネットワーク接続が一時的に失われます。

要件

レベル特権：1

コマンド特権：1

アップグレード時の使用：不可

例

```
admin:set network pmtud enable
          ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity

          Do you want to continue?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

set network restore

指定したイーサネット ポートで指定したスタティック IP アドレスを使用するように設定します。

注意　このコマンド オプションは、他の **set network** コマンドを使用してネットワーク接続を復元できない場合にのみ使用します。このコマンドでは、指定されたネットワーク インターフェイスに関する今までのネットワーク設定が、Network Fault Tolerance も含めてすべて削除されます。このコマンドを実行した場合は、後から以前のネットワーク設定を手動で復元する必要があります。

注意　このコマンドを実行すると、サーバのネットワーク接続が一時的に失われます。

コマンド構文

set network restore eth0 *ip-address network-mask gateway*

パラメータ

- **eth0** はイーサネット インターフェイス 0 を指定します。
- *ip-address* には IP アドレスを指定します。
- *network-mask* にはサブネット マスクを指定します。
- *gateway* にはデフォルト ゲートウェイの IP アドレスを指定します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

set network status

このコマンドは、イーサネット 0 のステータスをアップまたはダウンにします。イーサネット インターフェイス 1 は設定できません。

コマンド構文

set network status eth0 {**up** | **down**}

パラメータ

- **eth0** はイーサネット インターフェイス 0 を指定します。

使用上のガイドライン

このコマンドの実行を続けるかどうかが尋ねられます。

注意　続行すると、システムのネットワーク接続が一時的に失われます。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

set password

このコマンドを使用すると、管理者のパスワードを変更できます。

コマンド構文

set password {**admin** | **security**}

パラメータ

- **eth0** はイーサネット インターフェイス 0 を指定します。

使用上のガイドライン

以前のパスワードと新しいパスワードの入力を求められます。

（注）　パスワードは 6 文字以上でなければならず、システムがパスワードの強度を確認します。

クラスタ内のサーバ間の通信は、セキュリティ パスワードを使用して認証されます。セキュリティ パスワードを変更した後に、クラスタをリセットする必要があります。

手順

ステップ 1　パブリッシャ サーバでセキュリティ パスワードを変更し、サーバをリブートします。

ステップ 2　すべてのサブスクライバ サーバで、パブリッシャ サーバで作成したのと同じパスワードにセキュリティ パスワードを変更し、サブスクライバ サーバを再起動してパスワードの変更を伝えます。

（注）　各サーバでパスワードを変更した後、そのサーバを再起動することをお勧めします。

注意　サーバをリブートしない場合、システム サービスで問題が発生するほか、サブスクライバ サーバ上の Emergency Responder Administration で問題が発生します。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

set password history

履歴に保存するパスワードの数を設定します。

コマンド構文

set password history *number*

パラメータ

- *number* は履歴に保持されるパスワードの数を表します。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

set password inactivity disable

OS アカウントのパスワード非アクティビティをディセーブルにします。

コマンド構文

set password inactivity *disable*

set password inactivity enable

デフォルト値を 10 日間に設定して、OS アカウントのパスワード非アクティビティをイネーブルにします。

コマンド構文

set password inactivity *enable*

set password inactivity period

OS アカウントのパスワード非アクティビティを設定値に設定します。

許容可能な値は 1 ～ 99 日です。

コマンド構文

set password inactivity period *days*

パラメータ

days は、非アクティビティを設定する必要がある日数を表します。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

set password expiry maximum-age enable

OS アカウントのパスワードの有効期限切れをイネーブルにします。Emergency Responder OS 管理者アカウントの最大パスワード経過時間が 3650 日（10 年）に設定されます。

コマンド構文

set password expiry maximum-age *enable*

set password expiry maximum-age disable

OS アカウントのパスワードの有効期限切れをディセーブルにします。

つまり Emergency Responder OS 管理者アカウントのパスワードは有効期限切れにならなくなります。

コマンド構文

set password expiry maximum-age *disable*

set password expiry minimum-age enable

OS アカウントのパスワードの有効期限切れをイネーブルにします。

OS 管理者アカウントの最小パスワード経過時間が 1 日（24 時間）に設定されます。

コマンド構文

set password expiry minimum-age *enable*

set password expiry minimum-age disable

OS アカウントの最小パスワード経過時間をディセーブルにします。

つまり、OS 管理者アカウントのパスワードはいつでも変更できます。

コマンド構文

set password expiry minimum-age *disable*

set password expiry user maximum-age disable

特定の OS カウントのパスワードの有効期限切れをディセーブルにします。

コマンド構文

set password expiry user maximum-age disable *userid*

パラメータ
userid は、最大パスワード経過時間設定をディセーブルにするアカウントの名前です。

set password expiry user maximum-age enable

特定の OS アカウントのパスワードの有効期限切れをイネーブルにします。

コマンド構文
set password expiry user maximum-age enable *userid*

パラメータ
userid は、最大パスワード経過時間設定をイネーブルにするアカウントの名前です。

set password expiry user minimum-age disable

特定の OS アカウントの最小パスワード経過時間をディセーブルにします。

コマンド構文
set password expiry user minimum-age disable *userid*

パラメータ
userid は、最小パスワード経過時間設定をディセーブルにするアカウントです。

set password expiry minimum-age enable

特定の OS アカウントの最小パスワード経過時間をイネーブルにします。

コマンド構文
set password expiry user minimum-age enable *userid*

パラメータ
userid は、最小パスワード経過時間設定をイネーブルにするアカウントです。

要件
コマンド特権レベル：1
アップグレード時の使用：可能

set password age minimum

OS 管理者アカウントの最小パスワード経過時間の値を、日数単位で変更します。
有効な値は、0 日以上 10 日以下です。

コマンド構文
set password age minimum *days*

パラメータ
days は最小パスワード経過時間（日数）です。

要件
コマンド特権レベル：1

アップグレード時の使用：可能

set password age maximum

Emergency Responder OS 管理者アカウントの最大パスワード経過時間の値を、日数単位で変更します。

有効な値は、10 日以上 3650 日（10 年）未満です。

コマンド構文
set password age maximum days

パラメータ
days は、最大パスワード経過時間（日数）です。

要件
コマンド特権レベル：1

アップグレード時の使用：不可

set password complexity character disable

パスワードの複雑度をディセーブルにします。変更内容は、次回パスワードを変更するときに有効になります。

ディセーブルにすると、コマンド実行後に作成または変更したパスワードは、強固ではなくなります。つまり、パスワードに必ず大文字、小文字、数字、特殊文字が含まれるわけではなくなります。

コマンド構文
set password complexity character disable

要件
コマンド特権レベル：1

アップグレード時の使用：可能

set password complexity character enable

パスワード中の文字の種類に対するパスワード複雑さルールをイネーブルにします。

イネーブルにした場合、パスワードは次のガイドラインに従う必要があります。

1. 少なくとも 1 つの小文字を含むこと。

2. 1 文字以上の大文字、数字、特殊文字が含まれている必要があります。

3. キーボード上のすべての隣接する文字は許可されません。

4. 過去 10 回以内に使用したパスワードを再使用することはできません。
5. 管理者ユーザ パスワードは、24 時間以内に一度しか変更できません。
上記のいずれのルールに違反すると失敗します。

コマンド構文
set password complexity character enable

要件
コマンド特権レベル：1
アップグレード時の使用：不可

set password complexity minimum-length

Cisco Unified CM OS アカウントの最低パスワード長の値を変更します。
有効な値は 6 以上です。このコマンドは、
パスワードの文字の複雑度をイネーブルにした後にのみ使用してください。

コマンド構文
set password complexity minimum-length l*ength*

パラメータ
length はパスワード長さの最小値です。

要件
コマンド特権レベル：1
アップグレード時の使用：不可

set password user admin

新しい Admin パスワードを設定します。

コマンド構文
set password user admin

例：
set password user admin
Please enter the old password :********
Please enter the new password:********
re-enter new password to confirm:********

要件
コマンド特権レベル：1
アップグレード時の使用：不可

set password user security

新しいプラットフォーム セキュリティ パスワードを設定します。

コマンド構文
set password user security

例：
set password user security
Please enter the password:********
re-enter the password to confirm: ********

要件
コマンド特権レベル：1
アップグレード時の使用：不可

utils import config

platformConfig.xml ファイル中のすべての設定をインポートし、システムをリブートします。

コマンド構文
utils import config

set smtp

このコマンドは、SMTP サーバのホスト名を設定します。

コマンド構文
set smtp *hostname*

パラメータ
- *hostname* は、SMTP サーバ名を表します。

要件
コマンド特権レベル：0
アップグレード時の使用：不可

set timezone

このコマンドを使用すると、システムの時間帯を変更できます。

コマンド構文
set timezone *timezone*

パラメータ

- *timezone* には、新しい時間帯を指定します。

使用上のガイドライン

新しい時間帯を一意に識別するために十分な文字を入力します。時間帯名では大文字と小文字が区別されることに注意してください。

注意　時間帯を変更した後はシステムを再起動する必要があります。

要件

コマンド特権レベル：0

アップグレード時の使用：不可

例

この例では、時間帯を Pacific 時間に設定します。

```
set timezone Pac
```

set trace

このコマンドは、指定されたタスクにトレース アクティビティを設定します。

コマンド構文

set trace

enable Error *tname*

enable Special *tname*

enable State_Transition *tname*

enable Significant *tname*

enable Entry_exit *tname*

enable Arbitrary *tname*

enable Detailed *tname*

disable *tname*

パラメータ

- *tname* は、トレースをイネーブルまたはディセーブルにするタスクを表します。
- **enable Error** を指定すると、タスク トレース設定が error レベルに設定されます。
- **enable Special** を指定すると、タスク トレース設定が special レベルに設定されます。
- **enable State_Transition** を指定すると、タスク トレース設定が state transition レベルに設定されます。
- **enable Significant** を指定すると、タスク トレース設定が significant レベルに設定されます。
- **enable Entry_exit** を指定すると、タスク トレース設定が entry_exit レベルに設定されます。
- **enable Arbitrary** を指定すると、タスク トレース設定が arbitrary レベルに設定されます。
- **enable Detailed** を指定すると、タスク トレース設定が detailed レベルに設定されます。

- **disable** を指定すると、タスク トレース設定が解除されます。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

set web-security

このコマンドは、オペレーティング システムに Web セキュリティ証明書情報を設定します。

コマンド構文

set web-security *orgunit orgname locality state country alternate-host-name*

パラメータ

- *orgunit* は組織単位を表します。
- *orgname* は組織名を表します。
- *locality* は組織の場所を表します。
- *state* は組織の状態を表します。
- *country* は組織の国を表します。
- *alternate-host-name*（任意）には、Web サーバ（Tomcat）証明書を生成するときの、ホストの代替名を指定します。

（注） **set web-security** コマンドで alternate-host-name パラメータを設定すると、tomcat の自己署名証明書には、alternate-host-name が指定された Subject Alternate Name 拡張が含まれます。Emergency Responder の CSR には、CSR に代替ホスト名が指定された Subject Alternate Name Extension が含まれます。

要件

コマンド特権レベル：0

アップグレード時の使用：不可

set workingdir

このコマンドは、アクティブ、非アクティブ、およびインストールの各ログの作業ディレクトリを設定します。

コマンド構文

set workingdir

activelog *directory*

inactivelog *directory*

install *directory*

パラメータ

- **activelog** を指定すると、アクティブ ログの作業ディレクトリが設定されます。
- **inactivelog** を指定すると、非アクティブ ログの作業ディレクトリが設定されます。
- **install** を指定すると、インストール ログの作業ディレクトリが設定されます。
- *directory* は、現在の作業ディレクトリを表します。

要件

コマンド特権レベル：ログに対して 0

アップグレード時の使用：可能

show account

このコマンドは、マスター管理者アカウント以外の現在の管理者アカウントをリスト表示します。

コマンド構文

show account

要件

コマンド特権レベル：4

アップグレード時の使用：可能

show cert

このコマンドは、証明書の内容および証明書信頼リストを表示します。

コマンド構文

show cert

own *filename*

trust *filename*

list {**own** | **trust**}

パラメータ

- *filename* は証明書ファイルの名前を表します。
- **own** には所有している証明書を指定します。
- **trust** には信頼できる証明書を指定します。
- **list** には証明書信頼リストを指定します。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

例

このコマンドは、所有している証明書信頼リストを表示します。

```
show cert list own
```

show cli pagination

このコマンドは、CLI 自動改ページのステータスを配置します。

コマンド構文
show cli pagination

パラメータ
なし

要件
レベル特権：0

コマンド特権：0

アップグレード時の使用：可能

例

```
admin: show cli pagination
Automatic Pagination: Off.
```

show ctl

このコマンドは、サーバ上の証明書信頼リスト（CTL）ファイルの内容を表示します。CTL が有効でない場合は、そのことが通知されます。

コマンド構文
show ctl

show date

システムの日付を表示します。

コマンド構文
show date

要件
コマンド特権レベル：1

アップグレード時の使用：可能

show diskusage

このコマンドは、サーバのディスクの使用状況情報を表示します。

コマンド構文

show diskusage

activelog {**filename** *filename* | **directory** | **sort**}

common {**filename** *filename* | **directory** | **sort**}

inactivelog {**filename** *filename* | **directory** | **sort**}

install {**filename** *filename* | **directory** | **sort**}

tmp {**filename** *filename* | **directory** | **sort**}

パラメータ

- **activelog** を指定すると、アクティブログ ディレクトリに関するディスク使用量情報が表示されます。
- **common** を指定すると、共通ディレクトリに関するディスク使用量情報が表示されます。
- **inactivelog** を指定すると、非アクティブログ ディレクトリに関するディスク使用量情報が表示されます。
- **install** を指定すると、インストール ディレクトリに関するディスク使用量情報が表示されます。
- **tmp** を指定すると、tmp ディレクトリに関するディスク使用量情報が表示されます。

オプション

- **filename** *filename* : *filename* で指定したファイルに出力を保存します。これらのファイルは、**platform/cli** ディレクトリに格納されます。保存されたファイルを表示するには、**file view activelog** コマンドを使用します。
- **directory**：ディレクトリのサイズだけを表示します。
- **sort**：ファイル サイズに基づいて出力をソートします。ファイル サイズは 1024 バイト ブロック単位で表示されます。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

show environment

サーバ ハードウェアに関する情報を表示します。

コマンド構文

show environment

fans

power-supply

temperatures

オプション

- **fans**：ファン プローブによって収集された情報を表示します。
- **power-supply**：電源プローブによって収集された情報を表示します。
- **temperatures**：温度プローブによって収集された情報を表示します。

show firewall list

サーバのシステムの各側面を表示します。

コマンド構文

show firewall list [**detail**] [**page**] [**file** *filename*]

オプション

- **detail**：システムで使用可能なデバイスごとに詳細な統計情報を表示します。
- **page**：出力を一度に 1 ページずつ表示します。
- **file** *filename*：情報をファイルに出力します。

（注）　file オプションを指定すると、情報が platform/cli/*filename*.txt に保存されます。ファイル名に「.」文字が含まれていないことを確認してください。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

show hardware

このコマンドは、プラットフォーム ハードウェアに関する次の情報を表示します。

コマンド構文

show hardware

使用上のガイドライン

このコマンドは、プラットフォーム ハードウェアに関する次の情報を表示します。

- プラットフォーム
- シリアル番号
- BIOS のビルド レベル
- BIOS のメーカー
- アクティブなプロセッサ
- RAID コントローラのステータス

要件

コマンド特権レベル：0

アップグレード時の使用：可能

show ipsec

IPSec ポリシーとアソシエーションを表示します。

コマンド構文

show ipsec

policy

association *policy*

information *policy association*

status

パラメータ

- **policy** を指定すると、ノード上のすべての IPSec ポリシーが表示されます。
- **association** は、ポリシーのアソシエーション リストとステータスを表示します。
- **information** を指定すると、ポリシーのアソシエーションの詳細とステータスが表示されます。
- **status** を指定すると、システムで定義されているすべての IPSec トンネルのステータスが表示されます。
- *policy* は、特定の IPSec ポリシーの名前を表します。
- *association* はアソシエーション名を表します。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

例

次のコマンドは IPSec ポリシーを表示します。

```
show ipsec policy
```

show logins

このコマンドは、サーバへの最近のログインをリスト表示します。

コマンド構文

show logins *number*

パラメータ

- *number* には、表示する最近のログインの数を指定します。デフォルトは 20 です。

show memory

サーバ メモリに関する情報を表示します。

コマンド構文

show memory

count

module [**ALL** | *module_number*]

size

オプション

- **count**：システム上のメモリ モジュールの数を表示します。
- **module**：各メモリ モジュールに関する詳細情報を表示します。
- **size**：メモリの総量を表示します。

パラメータ

ALL を指定すると、搭載されているすべてのメモリ モジュールに関する情報が表示されます。

module_number は表示するメモリ モジュールを指定します。

show myself

このコマンドは、現在のアカウントに関する情報を表示します。

コマンド構文

show myself

要件

コマンド特権レベル：0

アップグレード時の使用：可能

show network

このコマンドは、ネットワーク情報を表示します。

コマンド構文

show network

eth0 [**detail**]

failover [**detail**] [**page**]

route [**detail**]

status [**detail**] [**listen**] [**process**] [**all**] [**nodns**] [**search stext**]

ip_conntrack

max_ip_conntrack

dhcp eth0 status

all [**detail**]

パラメータ

- **eth0** は、イーサネット 0 を指定します。
- **failover** は、ネットワークの耐障害性情報を指定します。
- **route** は、ネットワークのルーティング情報を表示します。
- **status** は、アクティブなインターネット接続を指定します。
- **ip_conntrack** は、ip_conntrack の使用状況情報を表示します。
- **max_ip_conntrack** は、max_ip_conntrack 情報を指定します。

- **dhcp eth0 status** は、DHCP ステータス情報を表示します。
- **all** は、すべての基本ネットワーク情報を表示します。

オプション

- **options**：追加情報を表示します。
- **detail**：追加情報の詳細を示します。
- **page**：情報を一度に 1 ページずつ表示します。
- **listen**：受信ソケットのみを表示します。
- **process**：各ソケットが属するプロセス ID とプログラム名を表示します。
- **all**：リッスンしているソケットとリッスンしていないソケットの両方を表示します。
- **nodns**：DNS 情報なしで、数値によるアドレスを表示します。
- **search stext**：出力中で stext を検索します。

使用上のガイドライン

eth0 パラメータは、イーサネット ポート 0 の設定を、DHCP および DNS の設定とオプションも含めて表示します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

例

この例では、アクティブなインターネット接続が表示されます。

```
show network status
```

show network ipprefs

ファイアウォールでオープンまたは変換することを要求されたポートの一覧を表示します。

コマンド構文

ipprefs {all | enabled | public}

パラメータ

all：製品で使用されている可能性があるすべての着信ポートを表示します。

enabled：現在オープンされているすべての着信ポートを表示します。

public：リモート クライアント向けに現在オープンされているすべての着信ポートを表示します。

要件

レベル特権：0

コマンド特権：0

アップグレード時の使用：可能

例

```
admin:show network ipprefs public
```

```
Application  IPProtocol   PortValue    Type         XlatedPort   Status       Description
-----------  -----------  -----------  -----------  -----------  -----------  -----------
sshd         tcp          22           public       -            enabled      sftp and ssh
access
tomcat       tcp          8443         translated   443          enabled      secure web
access
tomcat       tcp          8080         translated   80           enabled      web access
clm          udp          8500         public       -            enabled      cluster
manager
clm          tcp          8500         public       -            enabled      cluster
manager
ntpd         udp          123          public       -            enabled      network time
sync
snmpdm       udp          161          public       -            enabled      SNMP
ccm          tcp          2000         public       -            enabled      SCCP-SIG
ctftp        udp          6969         translated   69           enabled      TFTP access
to CUCM TFTP Server
ctftp        tcp          6970         public       -            enabled      HTTP access
to CUCM TFTP Server
admin:
```

show open

このコマンドは、システム上の開いているファイルおよびポートを表示します。

構文の説明

show open

files [**all**] [**process** *processID*] [**regexp** *reg_exp*]

ports [**all**] [**regexp** *reg_exp*]

パラメータ

- **files** を指定すると、システムでオープンされているファイルが表示されます。
- **ports** を指定すると、システムでオープンされているポートが表示されます。

オプション

- **all**：開いているすべてのファイルまたはポートを表示します。
- **process**：開いているファイルのうち、指定されたプロセスに属するものを表示します。
- *processID*：プロセスを指定します。
- **regexp**：開いているファイルまたはポートのうち、指定された正規表現に一致するものを表示します。
- *reg_exp*：正規表現を表します。

show packages

このコマンドは、インストールされているパッケージの名前およびバージョンを表示します。

コマンド構文

show packages

active *name* [**page**]

inactive *name* [**page**]

パラメータ

name は、パッケージ名を表します。アクティブまたは非アクティブなすべてのパッケージを表示するには、ワイルドカード文字（*）を使用します。

オプション

- **page**：出力を一度に 1 ページずつ表示します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

show password expiry maximum-age

設定されているパスワード有効期限パラメータを表示します。

コマンド構文

show password expiry maximum-age

show password expiry minimum-age

設定されているパスワード有効期限パラメータを表示します。

コマンド構文

show password expiry minimum-age

show password expiry user maximum-age

特定の OS ユーザに対して設定されているパスワード有効期限パラメータを表示します。

コマンド構文

show password expiry user maximum-age userid

show password expiry user minimum-age

特定の OS ユーザに対して設定されているパスワード有効期限パラメータを表示します。

コマンド構文

show password expiry user minimum-age userid

show password history

このコマンドは、OS 管理者アカウントの、履歴に保持されるパスワードの数を表示します。

コマンド構文
show password history

要件
コマンド特権レベル：0

アップグレード時の使用：可能

show password inactivity

OS アカウントのパスワード非アクティビティのステータスを表示します。

パスワード非アクティビティは、パスワードの有効期限が切れてからアカウントがディセーブルになるまでの、アクティビティがなかった日数です。

コマンド構文
show password inactivity

例
show password inactivity

Password Inactivity: Enabled and is currently set to 10 days

要件
コマンド特権レベル：0

アップグレード時の使用：可能

show process

システムで動作しているプロセスに関する情報を表示します。

構文
show process

list [**file** *filename*] [**detail**]

load [**cont**] [**clear**] [**noidle**] [**num** *number*] [**thread**] [**cpu** | **memory**| **time**] [**page**]

name *process* [**file** *filename*]

open-fd *process-id* [**,** *process-id2*]

search *regexp* [**file** *filename*]

using-most cpu [*number*] [**file** *filename*]

using-most memory [*number*] [**file** *filename*]

パラメータ

- **list** を指定すると、すべてのプロセスと各プロセスに関する重要な情報の一覧が表示され、プロセス間の親子関係が視覚的に示されます。
- **load** を指定すると、システムの現在の負荷が表示されます。
- **name** を指定すると、同じ名前を共有する複数のプロセスの詳細とその親子関係が表示されます。
- **open-fd** を指定すると、カンマ区切りのプロセス ID のリストに対する、オープンされているファイル記述子の一覧が表示されます。
- **search** を指定すると、オペレーティング システム固有のプロセス リストの出力中で、正規表現 *regexp* で指定されたパターンを検索します。
- **using-most cpu** を指定すると、最も CPU 消費が激しいプロセスの一覧が表示されます。
- **using-most memory** を指定すると、最もメモリ消費が激しいプロセスの一覧が表示されます。

オプション

- **file** *filename*：結果を *filename* で指定したファイルに出力します。
- **detail**：詳細な出力を表示します。
- **cont**：コマンドを連続的に繰り返します。
- **clear**：出力を表示する前に画面をクリアします。
- **noidle**：アイドル プロセスまたはゾンビ プロセスを無視します。
- **num** *number*：*number* で指定された数のプロセスを表示します。デフォルトのプロセス数は 10 です。*number* を **all** に設定すると、すべてのプロセスが表示されます。
- **thread**：スレッドを表示します。
- [**cpu** | **memory** | **time**]：出力を CPU 使用率、メモリ使用量、または使用時間でソートします。デフォルトでは CPU 使用率でソートされます。
- **page**：出力をページ単位で表示します。
- *process*：プロセスの名前を指定します。
- *process-id*：プロセスのプロセス ID 番号を指定します。
- *regexp*：正規表現。
- *number*：表示するプロセスの数。デフォルトは 5 です。

show smtp

このコマンドは、SMTP ホストの名前を表示します。

コマンド構文

show snmp

要件

コマンド特権レベル：0

アップグレード時の使用：可能

show stats io

システム I/O 統計情報を表示します。

コマンド構文

show stats io [**kilo**] [**detail**] [**page**] [**file** *filename*]

オプション

- **kilo**：キロバイト単位で統計情報を表示します。
- **detail**：システムで使用できる各デバイスについて、詳細な統計情報を表示します。kilo オプションはオーバーライドされます。
- **page**：一度に 1 ページずつ表示します。
- **file** *filename*：情報をファイルに出力します。

（注）　file オプションを指定すると、情報が platform/cli/*filename*.txt に保存されます。ファイル名には「.」文字は使用できません。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

show status

このコマンドは、基本的なプラットフォーム ステータスを表示します。

コマンド構文

show status

使用上のガイドライン

このコマンドは、次の基本的なプラットフォーム ステータスを表示します。

- ホスト名
- 日付
- タイムゾーン
- ロケール
- 製品バージョン
- プラットフォームのバージョン
- CPU 使用率
- メモリおよびディスクの使用状況

要件

コマンド特権レベル：0

show tech all

すべての **show tech** コマンドの出力を組み合わせた内容を表示します。

コマンド構文
all [**page**] [**file** *filename*]

オプション
- **page**：一度に 1 ページずつ表示します。
- **file** *filename*：情報をファイルに出力します。

（注）　file オプションを指定すると、情報が platform/cli/*filename*.txt に保存されます。ファイル名には「.」文字は使用できません。

要件
コマンド特権レベル：1
アップグレード時の使用：可能

show tech database

データベース全体の CSV ファイルを作成します。

コマンド構文
show tech database
dump
sessions

パラメータ
- **dump** は、データベース全体の CSV ファイルを作成します。
- **sessions** を指定すると、現在のセッション ID のセッションと SQL 情報がファイルにリダイレクトされます。

要件
コマンド特権レベル：1
アップグレード時の使用：可能

show tech database dump

データベース全体の CSV ファイルを作成します。

コマンド構文
show tech database dump

show tech dbintegrity

データベースの整合性を表示します。

コマンド構文
show tech dbintegrity

show tech dbinuse

使用中のデータベースを表示します。

コマンド構文
show tech dbinuse

要件
コマンド特権レベル：1
アップグレード時の使用：可能

show tech dbschema

CSV ファイル中のデータベース スキーマを表示します。

コマンド構文
show tech dbschema

要件
コマンド特権レベル：1
アップグレード時の使用：可能

show tech dbstateinfo

データベースの状態を表示します。

コマンド構文
show tech dbstateinfo

show tech network

サーバのネットワークの各側面を表示します。

コマンド構文
show tech network [**page**] [**file** *filename*]
show tech network
　all [**page**] [**search** *text*] [**file** *filename*]

hosts [**page**] [**search** *text*] [**file** *filename*]

interfaces [**page**] [**search** *text*] [**file** *filename*]

resolv [**page**] [**search** *text*] [**file** *filename*]

routes [**page**] [**search** *text*] [**file** *filename*]

sockets {**numeric**}

パラメータ

- **all** を指定すると、すべてのネットワーク技術情報が表示されます。
- **hosts** を指定すると、ホストの設定に関する情報が表示されます。
- **interfaces** を指定すると、ネットワーク インターフェイスに関する情報が表示されます。
- **resolv** を指定すると、ホスト名の解決に関する情報が表示されます。
- **routes** を指定すると、ネットワーク ルートに関する情報が表示されます。
- **sockets** を指定すると、オープンされているソケットの一覧が表示されます。

オプション

- **page**：一度に 1 ページずつ表示します。
- **search** *text*：出力中の *text* で指定した文字列を検索します。検索では大文字と小文字は区別されません。
- **file** *filename*：情報をファイルに出力します。
- **numeric**：シンボリックなホストを特定する代わりに、ポートの数値のアドレスを表示します。これは、Linux のシェル コマンド netstat [-n] を実行するのと同等です。

使用上のガイドライン

file オプションを指定すると、情報が platform/cli/*filename*.txt に保存されます。ファイル名には「.」文字は使用できません。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

show tech prefs

Emergency Responder とそのデータベースのすべての環境設定ファイルを表示します。この情報はファイルに書き込まれ、**file view** CLI を使用して表示できます。

コマンド構文

show tech prefs

show tech runtime

サーバの実行時の各側面を表示します。

コマンド構文

show tech runtime

all [**page**] [**file** *filename*]

cpu [**page**] [**file** *filename*]

disk [**page**] [**file** *filename*]

env [**page**] [**file** *filename*]

memory [**page**] [**file** *filename*]

パラメータ

- **all** を指定すると、すべての実行時情報が表示されます。
- **cpu** を指定すると、コマンドを実行した時点での CPU 使用率情報が表示します。
- **disk** を指定すると、システム ディスク使用量情報が表示されます。
- **env** を指定すると、環境変数が表示されます。
- **memory** を指定すると、メモリ使用量情報が表示されます。

オプション

- **page**：一度に 1 ページずつ表示します。
- **file** *filename*：情報をファイルに出力します。

使用上のガイドライン

file オプションを指定すると、情報が platform/cli/*filename*.txt に保存されます。ファイル名には「.」文字は使用できません。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

show tech systables

sysmaster データベース内のすべてのテーブルの名前を表示します。

コマンド構文

show tech systables

要件

コマンド特権レベル：1

アップグレード時の使用：可能

show tech system

サーバのシステムの各側面を表示します。

コマンド構文

show tech system

all [**page**] [**file** *filename*]

bus [**page**] [**file** *filename*]

hardware [**page**] [**file** *filename*]

host [**page**] [**file** *filename*]

kernel [**page**] [**file** *filename*]

software [**page**] [**file** *filename*]

tools [**page**] [**file** *filename*]

パラメータ

- **all** を指定すると、すべてのシステム情報が表示されます。
- **bus** を指定すると、サーバ上のデータ バスに関する情報が表示されます。
- **hardware** を指定すると、サーバ ハードウェアに関する情報が表示されます。
- **host** を指定すると、サーバに関する情報が表示されます。
- **kernel** を指定すると、インストールされているカーネル モジュールの一覧が表示されます。
- **software** を指定すると、インストールされているソフトウェアのバージョンに関する情報が表示されます。
- **tools** を指定すると、サーバ上のソフトウェア ツールに関する情報が表示されます。

オプション

page：一度に 1 ページずつ表示します。

file *filename*：情報をファイルに出力します。

使用上のガイドライン

file オプションを指定すると、情報が platform/cli/*filename*.txt に保存されます。ファイル名には「.」文字は使用できません。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

show tech table

指定したデータベース テーブルの内容を表示します。

コマンド構文

show tech table *table_name* [**page**] [**csv**]

パラメータ

table_name は、表示するテーブルの名前を表します。

オプション

- **page**：出力を一度に 1 ページずつ表示します。
- **csv**：出力をカンマ区切り形式ファイルに送ります。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

show tech version

インストールされているコンポーネントのバージョンを表示します。

コマンド構文

show tech version [**page**]

オプション

page：出力を一度に 1 ページずつ表示します。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

show timezone

時間帯情報を表示します。

コマンド構文

show timezone

config

list [**page**]

パラメータ

- **config** を指定すると、現在の時間帯設定が表示されます。
- **list** を指定すると、使用可能な時間帯が表示されます。

オプション

- **page**：出力を一度に 1 ページずつ表示します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

show trace

このコマンドは、特定のタスクのトレース情報を表示します。

コマンド構文
show trace [*task_name*]

パラメータ
task_name は、トレース情報を表示するタスクの名前を表します。

（注）　パラメータを入力しないと、使用可能なタスクのリストが返されます。

要件
コマンド特権レベル：0

アップグレード時の使用：可能

例
次に、CDP のトレース情報を表示する例を示します。

```
show trace cdps
```

show ups status

USB 接続された APC スマート UPS デバイスの現在のステータスを表示し、すでに開始されていなければモニタリング サービスを開始します。

このコマンドによる完全なステータスの表示は、7835-H2 サーバと 7825-H2 サーバのみで利用できます。

コマンド構文
show ups status

show version

このコマンドは、アクティブなパーティションまたは非アクティブなパーティション上のソフトウェアのバージョンを表示します。

コマンド構文
show version

active

inactive

パラメータ
active を指定すると、アクティブ パーティションで動作しているバージョンが表示されます。

inactive を指定すると、非アクティブ パーティション上のバージョンが表示されます。

要件
コマンド特権レベル：0
アップグレード時の使用：可能

show web-security

このコマンドは、現在の Web セキュリティ証明書の内容を表示します。

コマンド構文
show web-security

要件
コマンド特権レベル：0
アップグレード時の使用：可能

show workingdir

アクティブログ、非アクティブログ、インストールの現在の作業ディレクトリを取得します。

コマンド構文
show workingdir

要件
コマンド特権レベル：0
アップグレード時の使用：可能

unset ipsec

IPSec ポリシーとアソシエーションをディセーブルにします。

コマンド構文
unset ipsec
policy {**ALL** | *policy-name*}
association *policy-name* {**ALL** | *association-name*}

パラメータ
- *policy-name* は IPSec ポリシーの名前を表します。
- *association-name* は IPSec アソシエーションの名前を表します。

要件
コマンド特権レベル：1
アップグレード時の使用：不可

unset network

このコマンドは、DNS オプションの設定を解除します。

コマンド構文
unset network dns options [**timeout**] [**attempts**] [**rotate**]

パラメータ

- **timeout** を指定すると、DNS クエリを失敗したと見なすまでの待ち時間がデフォルトに設定されます。
- **attempts** を指定すると、失敗と見なす前に試行する DNS クエリの回数がデフォルトに設定されます。
- **rotate** を指定すると、ネーム サーバを選択する方法がデフォルトに設定されます。これは、ネームサーバ間での負荷分散方法に影響します。

使用上のガイドライン
このコマンドの実行を続けるかどうかが尋ねられます。

注意　続行すると、システムのネットワーク接続が一時的に失われます。

unset network domain

ドメイン名を設定解除し、サーバを再起動します。

コマンド構文
unset network domain

要件
コマンド特権レベル：1
アップグレード時の使用：可能

utils core list

このコマンドは、既存のコア ファイルをすべてリスト表示します。

コマンド構文
utils core list

utils core analyze

指定したコア ファイルのバックトレース、スレッド リスト、すべての CPU レジスタの現在の値を生成します。

コマンド構文
utils core analyze *core file name*

パラメータ
- *core file name* にはコア ファイルの名前を指定します。

使用上のガイドライン
コア ファイルと同じ名前で、拡張子が .txt のファイルが、コア ファイルと同じディレクトリに作成されます。このコマンドはアクティブ パーティションのみに対して使用できます。

utils create report

このコマンドは、サーバに関するレポートを platform/log ディレクトリ内に作成します。

コマンド構文
utils create report

hardware

platform

csa

パラメータ
- **hardware** を指定すると、ディスク アレイ、リモート コンソール、診断、環境データを含むレポートが作成されます。
- **platform** を指定すると、プラットフォーム コンフィギュレーション ファイルが TAR ファイルに収集されます。
- **csa** を指定すると、CSA 診断で必要なすべてのファイルが収集され、単一の CSA 診断ファイルが作成されます。このファイルは、**file get** コマンドを使用して取得できます。

使用上のガイドライン
コマンドを入力すると、続行を求めるプロンプトが表示されます。

レポート作成後にレポートを取得するには、**file get activelog platform/log/***filename* を使用します。ここで、*filename* は、コマンドが完了した後に表示されるレポート ファイル名です。

要件
レベル特権：1

コマンド特権レベル：0

アップグレード時の使用：可能

utils csa disable

Cisco Security Agent（CSA）を停止します。

コマンド構文
utils csa disable

要件
コマンド特権レベル：1
アップグレード時の使用：不可

utils csa enable

Cisco Security Agent（CSA）をイネーブルにします。

コマンド構文
utils csa enable

使用上のガイドライン
CSA をイネーブルにすることを確認するプロンプトが表示されます。

注意　CSA の開始後、システムを再起動する必要があります。

要件
コマンド特権レベル：1
アップグレード時の使用：不可

utils csa status

Cisco Security Agent（CSA）の現在のステータスを表示します。

コマンド構文
utils csa status

使用上のガイドライン
CSA が実行中であるかどうかが示されます。

要件
コマンド特権レベル：0
アップグレード時の使用：不可

utils dbreplication status

データベース レプリケーションのステータスを表示します。このコマンドは、クラスタの最初のパブリッシャ サーバのみで実行する必要があります。

コマンド構文
utils dbreplication status

utils dbreplication repair

データベース レプリケーションを修復します。

コマンド構文
utils dbreplication repair

utils dbreplication reset

データベース レプリケーションをリセットして再起動します。

コマンド構文
utils dbreplication reset

（注）　**utils dbreplication reset** コマンドを実行した後は、CUOS Administration を使用するか CLI コマンド **utils system restart** を実行して、Emergency Responder サブスクライバ ノードを再起動する必要があります。詳細については、CLI コマンド **help utils dbreplication reset** を参照してください。

utils diagnose

このコマンドを使用すると、システムの問題を診断し、自動修復を試行できます。

コマンド構文
utils diagnose

fix

list

module *module_name*

test

version

パラメータ

- **fix** を指定すると、すべての診断コマンドを実行し、問題の修復を試みます。
- **list** を指定すると、使用可能なすべての診断コマンドの一覧が表示されます。
- **module** を指定すると、単一の診断コマンドまたは一連のコマンドが実行され、問題の修復が試みられます。
- **test** を指定すると、すべての診断コマンドが実行されますが、問題の修復は試みられません。
- **version** を指定すると、診断フレームワークのバージョンが表示されます。
- *module_name* は診断モジュールの名前です。

utils disaster_recovery backup tape

バックアップ ジョブを開始し、得られた tar ファイルをテープに格納します。

コマンド構文
utils disaster_recovery backup tape *featurelist tapeid*

パラメータ
- *featurelist* には、バックアップする機能のリストを、カンマ区切りで指定します。
- *tapeid* は、使用可能なテープ デバイスの ID を表します。

要件
コマンド特権レベル：1

アップグレード時の使用：可能

utils disaster_recovery backup network

バックアップ ジョブを開始し、得られた tar ファイルをリモート サーバに格納します。

コマンド構文
utils disaster_recovery backup network *featurelist path servername username*

パラメータ
- *featurelist* には、バックアップする機能のリストを、カンマ区切りで指定します。
- *path* は、リモート サーバ上のバックアップ ファイルの場所を表します。
- *servername* は、バックアップ ファイルを格納するサーバの IP アドレスまたはホスト名を表します。
- *username* は、リモート サーバにログインするために必要なユーザ名を表します。

使用上のガイドライン

（注）　リモート サーバ上のアカウントのパスワードを入力するように要求するプロンプトが表示されます。

要件
コマンド特権レベル：1

アップグレード時の使用：可能

utils disaster_recovery cancel_backup

このコマンドは、進行中のバックアップ ジョブをキャンセルします。

コマンド構文
utils disaster_recovery cancel_backup

使用上のガイドライン
バックアップ ジョブをキャンセルすることを確認するプロンプトが表示されます。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

utils disaster_recovery device add local

バックアップ ローカル デバイスを追加します。

コマンド構文

utils disaster_recovery device add local *device_name Number_of_backups*

パラメータ

device_name はバックアップ デバイスの名前です。

Number_of_backups は必要なバックアップの数です。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

utils disaster_recovery device add network

バックアップ ネットワーク デバイスを追加します。

コマンド構文

utils disaster_recovery device add network *device_name path server_name/ip_address username Number_of_backups*

パラメータ

device_name は、追加するバックアップ デバイスの名前です。

path は、この場所からバックアップ デバイスを取得するためのパスです。

server_name/ip_address は、バックアップ ファイルを格納するサーバのホスト名または IP アドレスです。

username はリモート マシンに接続するためのユーザ ID です。

オプション パラメータ

Number_of_backups は、ネットワーク ディレクトリに格納するバックアップの数です（デフォルトは 2）。

例：

utils disaster_recovery device add network networkDevice /root 10.77.31.116 root 3

要件

コマンド特権レベル：1

アップグレード時の使用：不可

utils disaster_recovery device add tape

バックアップ テープ デバイスを追加します。

コマンド構文
utils disaster_recovery device add tape *device_name tapeid*

パラメータ
device_name は、追加するバックアップ デバイスの名前です。
tapeid はテープ ID です。

例：
utils disaster_recovery device add tape tapeDevice /dev/nst0

要件
コマンド特権レベル：1
アップグレード時の使用：不可

utils disaster_recovery device delete

デバイスを削除します。

コマンド構文
utils disaster_recovery device delete *device_name*|*

パラメータ
device_name は、削除するデバイスの名前です。
* は、スケジュールに関連付けられているデバイス以外のすべての既存のデバイスを削除することを意味します。

要件
コマンド特権レベル：1
アップグレード時の使用：不可

utils disaster_recovery device list

すべてのバックアップ デバイスのデバイス名、デバイス タイプ、デバイス パスを表示します。

コマンド構文
utils disaster_recovery device list

例：
utils disaster_recovery device list
sftpdevice　　NETWORK　　10.77.31.116 : /root
tapedevice　　TAPE　　/dev/nst0

localdevice　　LOCAL　　/common/drfbackup

要件
コマンド特権レベル：1
アップグレード時の使用：可能

utils disaster_recovery history

以前のバックアップまたはリストアの履歴を表示します。

コマンド構文
utils disaster_recovery history *operation*

パラメータ
operation は、操作の名前（backup または restore）です。

例：
utils disaster_recovery history backup

Tar Filename:　　Backup Device:　Completed On:　　Result:　Backup Type:　Features Backed Up:

2009-10-30-14-53-32.tar　TAPE　　Fri Oct 30 14:55:31 CDT 2009　ERROR　MANUAL

2009-12-10-10-30-17.tar　TAPE　　Thu Dec 10 10:35:22 CST 2009　SUCCESS　MANUAL　CDR_CAR,CCM

utils disaster_recovery schedule add

これは、設定されているスケジュールを追加します。

コマンド構文
utils disaster_recovery schedule add *schedulename devicename featurelist datetime frequency*

パラメータ
schedulename はスケジューラの名前です。

devicename はスケジュールするデバイスの名前です。

featurelist はバックアップ対象の機能のカンマ区切りのリストです。

datetime はスケジューラを設定する日付です。形式は yyyy/mm/dd-hh:mm で、24 時間制です。

frequency は、バックアップを取得するために設定するスケジューラの頻度です。ONCE、DAILY、WEEKLY、MONTHLY などを指定します。

例：
utils disaster_recovery schedule add schedulename devicename featurelist datetime frequency

Schedule has been saved successfully.

要件
コマンド特権レベル：1

アップグレード時の使用：可能

utils disaster_recovery schedule delete

指定したスケジュールを削除します。

コマンド構文
utils disaster_recovery schedule delete *schedulename*|*

パラメータ
schedulename は、削除するスケジュールの名前です。
* を指定すると、既存のスケジュールがすべて削除されます。

例：
utils disaster_recovery schedule delete schedule1|*
Schedules deleted successfully.

要件
コマンド特権レベル：1
アップグレード時の使用：不可

utils disaster_recovery schedule disable

指定したスケジュールをディセーブルにします。

コマンド構文
utils disaster_recovery schedule disable *schedulename*

パラメータ
schedulename は、ディセーブルにするスケジュールの名前です。

例：
utils disaster_recovery schedule disable schedule1
Schedule disabled successfully.

要件
コマンド特権レベル：1
アップグレード時の使用：不可

utils disaster_recovery schedule enable

指定したスケジュールをイネーブルにします。

コマンド構文
utils disaster_recovery schedule enable *schedulename*

パラメータ
schedulename は、イネーブルにするスケジュールの名前です。

例：
utils disaster_recovery schedule enable schedule1

Schedule enabled successfully.

要件
コマンド特権レベル：1

アップグレード時の使用：不可

utils disaster_recovery schedule list

設定されているすべてのスケジュールを表示します。

コマンド構文
utils disaster_recovery schedule list

要件
コマンド特権レベル：1

アップグレード時の使用：不可

utils disaster_recovery restore tape

リストア ジョブを開始し、テープからバックアップ tar ファイルを取得します。

コマンド構文
utils disaster_recovery restore tape *server tarfilename tapeid*

パラメータ
- *server* には、リストアするサーバのホスト名を指定します。
- *tarfilename* には、リストアするファイルの名前を指定します。
- *tapeid* には、リストア ジョブを実行するテープ デバイスの名前を指定します。

要件
コマンド特権レベル：1

アップグレード時の使用：可能

utils disaster_recovery restore network

リストア ジョブを開始し、リモート サーバからバックアップ tar ファイルを取得します。

コマンド構文
utils disaster_recovery restore network *restore_server tarfilename path servername username*

パラメータ

- *restore_server* には、リストアするサーバのホスト名を指定します。
- *tarfilename* には、リストアするファイルの名前を指定します。
- *path* は、リモート サーバ上のバックアップ ファイルの場所を表します。
- *servername* は、バックアップ ファイルを格納するサーバの IP アドレスまたはホスト名を表します。
- *username* は、リモート サーバにログインするために必要なユーザ名を表します。

使用上のガイドライン

（注）　リモート サーバ上のアカウントのパスワードを入力するように要求するプロンプトが表示されます。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

utils disaster_recovery show_backupfiles tape

テープに格納されているバックアップ ファイルに関する情報を表示します。

コマンド構文

utils disaster_recovery show_backupfiles tape *tapeid*

パラメータ

- *tapeid* は、使用可能なテープ デバイスの ID を表します。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

utils disaster_recovery show_backupfiles network

リモート サーバに格納されているバックアップ ファイルに関する情報を表示します。

コマンド構文

utils disaster_recovery show_backupfiles network *path servername username*

パラメータ

- *path* は、リモート サーバ上のバックアップ ファイルの場所を表します。
- *servername* は、バックアップ ファイルを格納するサーバの IP アドレスまたはホスト名を表します。
- *username* は、リモート サーバにログインするために必要なユーザ名を表します。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

utils disaster_recovery show_registration

このコマンドは、指定されたサーバに登録されているフィーチャおよびコンポーネントを表示します。

コマンド構文

utils disaster_recovery show_registration *hostname*

パラメータ

- *hostname* には、登録情報を表示するサーバを指定します。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

utils disaster_recovery show_tapeid

このコマンドは、テープ デバイス ID のリストを表示します。

コマンド構文

utils disaster_recovery show_tapeid

要件

コマンド特権レベル：1

アップグレード時の使用：不可

utils disaster_recovery status

このコマンドは、現在のバックアップまたは復元ジョブのステータスを表示します。

コマンド構文

utils disaster_recovery status *operation*

パラメータ

- *operation* には、進行中の操作の名前（**backup** または **restore**）を指定します。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

utils fior

このコマンドを使用すると、サーバの I/O をモニタリングできます。ファイル I/O レポート サービスには、プロセスごとのファイル I/O を収集するためのカーネルベースのデーモンが用意されています。

コマンド構文

utils fior

disable

enable

list [**start=***date-time*] [**stop=***date-time*]

start

status

stop

top *number* [**read** | **write** | **read-rate** | **write-rate**] [**start=***date-time*] [**stop=***date-time*]

オプション

- **disable**：マシンの起動時にファイル I/O レポーティング サービスが自動的に起動しないようにします。このコマンドでは、リブートするまでサービスは停止しません。ただちにサービスを停止するときは、**stop** オプションを使用します。
- **enable**：マシンの起動時にファイル I/O レポーティング サービスが自動的に起動するようにします。このコマンドでは、リブートするまでサービスは開始しません。ただちにサービスを開始するときは、**start** オプションを使用します。
- **list**：このコマンドは、ファイル I/O イベントを古いものから新しいものの順番にリスト表示します。
- **start**：停止してあったファイル I/O レポーティング サービスを開始します。サービスは、手動で停止されるかマシンがリブートされるまで起動状態が保たれます。
- **status**：ファイル I/O レポーティング サービスのステータスを表示します。
- **stop**：ファイル I/O レポーティング サービスを停止します。サービスは、手動で開始されるかマシンがリブートされるまで停止状態が保たれます。
- **top**：発生させているファイル I/O が多いプロセスのリストを表示します。この一覧は、合計読み込みバイト数、合計書き込みバイト数、読み込み速度、書き込み速度でソートできます。
- **start**：開始日時を指定します。
- **stop**：終了日時を指定します。
- *date-time*：日時を、*H*:*M*、*H*:*M*:*S a*、*H*:*M*、*a*、*H*:*M*:*S Y-m-d*、*H*:*M*、*Y-m-d*、*H*:*M*:*S* のいずれかの形式で指定します。
- *number*：上位何件のプロセスをリストに表示するかを指定します。
- **[read | write | read-rate | write-rate]**：上位のプロセスの一覧をソートするために使用するメトリックを指定します。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

utils firewall

ノード上のファイアウォールを管理します。

コマンド構文

utils firewall

disable {*time*}

enable

list

status

パラメータ

- **disable** を指定すると、ファイアウォールがディセーブルになります。
- *time* には、ファイアウォールをディセーブルにする期間を、次のいずれかの形式で指定します。
  - [0-1440]**m**：分単位で期間を指定します。
  - [0-24]**h**：時間単位で期間を指定します。
  - [0-23]**h**[0-60]**m**：時間および分単位で期間を指定します。

  時間を指定しないと、デフォルトでは 5 分になります。
- **list** を指定すると、現在のファイアウォール設定が表示されます。
- **status** を指定すると、ファイアウォールのステータスが表示されます。

使用上のガイドライン

ファイアウォールをディセーブルにする場合、Web インターフェイスにログインするため、次の形式で Cisco Unified Communications Manager サーバの URL を入力する必要があります。

https://*server***:8443/**

ここで、*server* はサーバのサーバ名または IP アドレスです。

ファイアウォールをディセーブルにすることはお勧めしません。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils iostat

このコマンドは、指定された回数と間隔で iostat 出力を表示します。

コマンド構文

utils iostat [*interval*] [*iterations*] [*filename*]

パラメータ

- *interval* は、2 回の iostat の読み取りの間の秒数を表します（繰り返し回数を指定する場合は必須）。
- *interations* は、iostat の繰り返し回数を表します（間隔を指定する場合は必須）。

- filename を指定すると、出力がファイルにリダイレクトされます。

要件

レベル特権：0

コマンド特権：1

アップグレード時の使用：不可

utils iothrottle enable

I/O スロットリング拡張をイネーブルにします。イネーブルにすると、I/O スロットリング拡張により、アクティブなシステムにアップグレードが与える影響が低下します。

コマンド構文

utils iothrottle enable

utils iothrottle disable

I/O スロットリング拡張をディセーブルにします。このコマンドは、アップグレード時のシステムのパフォーマンスを低下させる可能性があります。

コマンド構文

utils iothrottle disable

utils iothrottle status

I/O スロットリング拡張のステータスを表示します。

コマンド構文

utils iothrottle status

utils netdump client

netdump クライアントを設定します。

コマンド構文

utils netdump client

start *ip-address-of-netdump-server*

status

stop

パラメータ

- **start** を指定すると、netdump クライアントが開始されます。
- **status** を指定すると、netdump クライアントのステータスが表示されます。

- **stop** を指定すると、netdump クライアントが停止されます。
- *ip-address-of-netdump-server* には、クライアントが診断情報を送信する netdump サーバの IP アドレスを指定します。

使用上のガイドライン

カーネル パニックがクラッシュした場合、netdump クライアントはクラッシュの診断情報を netdump サーバに送信します。

要件

コマンド特権レベル：0

アップグレード時の使用：不可

utils netdump server

netdump サーバを設定します。

コマンド構文

utils netdump server

add-client *ip-address-of-netdump-client*

delete-client *ip-address-of-netdump-client*

list-clients

start

status

stop

パラメータ

- **add-client** を指定すると、netdump クライアントが追加されます。
- **delete-client** を指定すると、netdump クライアントが削除されます。
- **list-clients** を指定すると、この netdump サーバに登録されているクライアントの一覧が表示されます。
- **start** を指定すると、netdump サーバが開始されます。
- **status** を指定すると、netdump サーバのステータスが表示されます。
- **stop** を指定すると、netdump サーバが停止されます。
- *ip-address-of-netdump-client* には、netdump クライアントの IP アドレスを指定します。

使用上のガイドライン

カーネル パニックがクラッシュした場合、netdump がイネーブルになっているクライアント システムは、クラッシュの診断情報を netdump サーバに送信します。

netdump 診断情報は netdump サーバの *crash/* に格納されます。クライアントの IP アドレスと日付から名前が構成されるサブディレクトリに、この netdump 情報が格納されます。

各 Emergency Responder サーバを netdump クライアントおよびサーバの両方として設定できます。

サーバが別の Emergency Responder サーバ上にある場合、カーネル パニック トレースのシグニチャだけがサーバに送信されます。それ以外の場合は、コア ダンプ全体が送信されます。

要件

コマンド特権レベル：0

アップグレード時の使用：不可

utils network arp

Address Resolution Protocol（ARP; アドレス解決プロトコル）テーブルのエントリを一覧表示、設定、または削除します。

コマンド構文

utils network arp

list [**host** *host*] [**page**] [**numeric**]

set {*host*} {*address*}

delete *host*

パラメータ

- **list** を指定すると、アドレス解決プロトコル テーブルの内容が一覧表示されます。
- **set** を指定すると、アドレス解決プロトコル テーブル中にエントリが設定されます。
- **delete** を指定すると、アドレス解決プロトコル テーブル中のエントリが削除されます。
- *host* は、テーブルに追加または削除するホストのホスト名または IP アドレスを表します。
- *address* は追加するホストの MAC アドレスを表します。MAC アドレスは、XX:XX:XX:XX:XX:XX という形式で入力します。

オプション

- **page**：出力を一度に 1 ページずつ表示します。
- **numeric**：ホストをドット区切りの IP アドレスで表示します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils network capture eth0

このコマンドは、指定されたイーサネット インターフェイス上の IP パケットを取得します。

コマンド構文

utils network capture eth0 [**page**] [**numeric**] [**file** *fname*] [**count** *num*] [**size** *bytes*] [**src** *addr*] [**dest** *addr*] [**port** *num*]

パラメータ

- **eth0** はイーサネット インターフェイス 0 を指定します。

オプション

- **page**：出力を一度に 1 ページずつ表示します。

page オプションまたは file オプションを使用した場合、コマンドが完了する前に、要求されたすべてのパケットの完全なキャプチャが完了する必要があります。

- **numeric**：ホストをドット区切りの IP アドレスで表示します。
- **file** *fname*：情報をファイルに出力します。

  file オプションは、情報を platform/cli/*fname*.cap に保存します。ファイル名には「.」文字は使用できません。
- **count** *num*：キャプチャするパケット数を設定します。

  画面出力の場合、上限は 1000 です。ファイル出力の場合、上限は 10,000 です。
- **size** *bytes*：取得するパケットのバイト数を設定します。

  画面出力の場合の最大バイト数は 128 であり、ファイル出力の場合の最大バイト数は任意の数または **ALL** です。
- **src** *addr*：パケットの送信元アドレスをホスト名または IPV4 アドレスで指定します。
- **dest** *addr*：パケットの宛先アドレスをホスト名または IPV4 アドレスで指定します。
- **port** *num*：パケットの送信元または宛先のポート番号を指定します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils network connectivity

サーバのパブリッシャ サーバへのネットワーク接続を確認します。サブスクライバ サーバのみで有効です。

コマンド構文

utils network connectivity

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils network host

このコマンドは、ホスト名をアドレスに、またはアドレスをホスト名に名前解決します。

コマンド構文

utils network host *hostname* [**server** *server-name*] [**page**] [**detail**] [**srv**]

パラメータ

- *hostname* は、解決するホスト名または IP アドレスを表します。

オプション

- *server-name*：代替のドメイン ネーム サーバを指定します。

- **page**：出力を一度に 1 画面ずつ表示します。
- **detail**：詳細なリストを表示します。
- **srv**：DNS SRV レコードを表示します。

要件
コマンド特権レベル：0
アップグレード時の使用：可能

utils network ping

別のサーバに ping を実行します。

コマンド構文
utils network ping *destination* [*count*]

パラメータ
- *destination* は、ping を行うサーバのホスト名または IP アドレスを表します。

オプション
- *count*：外部のサーバに対する ping の回数を指定します。デフォルトの回数は 4 です。

要件
コマンド特権レベル：0
アップグレード時の使用：可能

utils network tracert

リモートの宛先に送信される IP パケットを追跡します。

コマンド構文
utils network tracert *destination*

パラメータ
- *destination* は、トレースの送信先のサーバのホスト名または IP アドレスを表します。

要件
コマンド特権レベル：0
アップグレード時の使用：可能

utils ntp

このコマンドは、NTP のステータスまたは設定を表示します。

コマンド構文
utils ntp {**status** | **config**}

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils ntp restart

NTP サービスを再起動します。

コマンド構文

utils ntp restart

パラメータ

なし

要件

レベル特権：0

コマンド特権：0

アップグレード時の使用：可能

utils ntp server add

指定した NTP サーバを最大 5 台まで追加します。

norestart を指定すると、サーバを追加した後で NTP サービスが再起動されません。

（注） norestart オプションを使用する場合、変更内容を有効にするには、NTP サービスを明示的に再起動する必要があります。

コマンド構文

utils ntp server add s1 [s2 s3 s4 s5] [norestart]

パラメータ

必須パラメータ：追加する 1 台以上の NTP サーバ

オプション パラメータ：最大 4 台の追加の NTP サーバと norestart オプション。

例 1：誤ったコマンド ライン パラメータを使用したサーバの追加

---

admin:utils ntp server add s1 s2 s3 s4 s5 s6 s7 s8

Incorrect number of parameters entered for add

usage: utils ntp server add s1 [s2 s3 s4 s5] [norestart]

admin:

例 2：サーバを指定せず norestart を使用した追加

---

admin:utils ntp server add norestart
At least one NTP server must be specified for add operation.
usage: utils ntp server add s1 [s2 s3 s4 s5] [norestart]

例 3：norestart を使用しないサーバの追加

---

admin:utils ntp server add clock1.cisco.com clock2.cisco.com
clock1.cisco.com : added successfully.
clock2.cisco.com : added successfully.
Restarting NTP on the server.

例 4：norestart を使用しない、すでに追加されているサーバの追加

---

admin:utils ntp server add clock1.cisco.com clock2.cisco.com
clock1.cisco.com : [The host has already been added as an NTP server.]
clock2.cisco.com : [The host has already been added as an NTP server.]
admin:

例 5：norestart を使用しない、自身へのサーバの追加

---

admin:utils ntp server add bglr-ccm26
bglr-ccm26 : [This server cannot be added as an NTP server.]
admin:

例 6：norestart を使用しない、アクセス不能なサーバの追加

---

admin:utils ntp server add clock3.cisco.com
clock3.cisco.com : [Inaccessible NTP server.Not added.]
admin:

例 7：norestart を使用したサーバの追加

---

admin:utils ntp server add ntp01-syd.cisco.com ntp02-syd.cisco.com clock.cisco.com norestart
ntp01-syd.cisco.com: added successfully.
ntp02-syd.cisco.com: added successfully.
clock.cisco.com: added successfully.
The NTP service must be restarted for the changes to take effect.

例 8：すでに 5 台設定済みの場合のサーバの追加

---

admin:utils ntp server add clock3.cisco.com
The maximum permissible limit of 5 NTP servers is already configured

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils ntp server delete

設定されている NTP サーバのいずれかまたはすべてを削除するための選択肢を表示します。

ユーザが選択内容を入力すると、NTP サービスを再起動するかどうかを質問されます。

No と答えると、サーバを削除した後で NTP サービスが再起動されません。

（注） NTP サービスを再起動しないことを選択した場合、変更内容を有効にするには、NTP サービス明示的に再起動する必要があります。

コマンド構文

utils ntp server delete

例 1：誤ったコマンド ライン パラメータを使用したサーバの削除

---

admin:utils ntp server delete clock1.cisco.com clock2.cisco.com

Incorrect number of optional parameters entered for delete

usage: utils ntp server delete

admin:

例 2：NTP を再起動し 1 台のサーバを削除

---

admin:utils ntp server delete

1: clock1.cisco.com

2: clock2.cisco.com

3: ntp01-syd.cisco.com

4: ntp02-syd.cisco.com

5: clock.cisco.com

a: all

q: quit

Choice: 1

Restart NTP (y/n): y

clock1.cisco.com is deleted from the list of configured NTP servers.

Continue (y/n)?y

clock1.cisco.com: deleted successfully.

Restarting NTP on the server.

admin:

例 3：NTP を再起動せずすべてのサーバを削除

```
admin:utils ntp server delete
1: clock1.cisco.com
2: clock2.cisco.com
3: ntp01-syd.cisco.com
4: ntp02-syd.cisco.com
5: clock.cisco.com
a: all
q: quit
Choice: a
Restart NTP (y/n): n
This results in all the configured NTP servers being deleted.
Continue (y/n)?y
clock1.cisco.com:  deleted successfully.
clock2.cisco.com:  deleted successfully.
ntp01-syd.cisco.com:  deleted successfully.
ntp02-syd.cisco.com:  deleted successfully.
clock.cisco.com:  deleted successfully.
The NTP service must be restarted for the changes to take effect.
admin:
```

例 4：サーバが設定されていない場合のすべてのサーバの削除

```
admin:utils ntp server delete
There are no NTP servers configured to delete.
```

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils ntp server list

設定されている NTP サーバの一覧を表示します。

コマンド構文

utils ntp server list

例 1：誤ったコマンド ライン パラメータを使用したサーバの一覧表示

```
admin:utils ntp server list all
```

Incorrect optional parameter entered for list

usage: utils ntp server list

admin:

例 2：サーバの一覧表示

---

admin:utils ntp server list

clock1.cisco.com

clock2.cisco.com

ntp01-syd.cisco.com

ntp02-syd.cisco.com

clock.cisco.com

admin:

例 3：サーバが設定されていない場合のサーバの一覧表示

---

admin:utils ntp server list

There are no NTP servers configured.

要件

コマンド特権レベル：1

アップグレード時の使用：可能

utils ntp start

NTP サービスが動作していない場合、NTP サービスを開始します。

（注）　CLI からは NTP サービスを停止できません。このコマンドは、**utils ntp status** コマンドで **stopped** が返される場合に使用します。

コマンド構文

utils ntp start

パラメータ

なし

要件

レベル特権：0

コマンド特権：0

アップグレード時の使用：可能

utils remote_account

このコマンドを使用すると、リモート アカウントのステータスをイネーブルまたはディセーブルにしたり、作成または確認したりすることができます。

コマンド構文

utils remote_account

status

enable

disable

create *username life*

パラメータ

- *username* には、リモート アカウントの名前を指定します。username は小文字だけを使用でき、7 文字以上でなければなりません。
- *life* には、アカウントの有効期限を日単位で指定します。指定した日数が過ぎると、アカウントは使用できなくなります。

使用上のガイドライン

リモート アカウントは、パス フレーズを生成します。シスコのサポート担当者はこれを使用することにより、アカウントの指定有効期間の間、システムにアクセスできます。同時に有効にできるリモート アカウントは 1 つだけです。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

例

```
utils remote_account status
```

utils reset_ui_administrator_password

Emergency Responder Administration のパスワードをリセットします。

コマンド構文

utils reset_ui_administrator_password

utils service

サービスを停止、開始、または再起動します。

コマンド構文

utils service

start *service-name*

stop *service-name*

restart *service-name*

auto-restart {**enable** | **disable** | **show**} *service-name*

パラメータ

- *service-name* は、開始または停止するサービスの名前を、次のいずれかで指定します。
  - System NTP
  - System SSH
  - Cisco IDS
  - Cisco Tomcat
  - Cisco Database Layer Monitor
  - Cisco Emergency Responder
  - Cisco Phone Tracking Engine
- **auto-restart** を指定すると、サービスが自動的に再起動されます。
- **enable** を指定すると、自動再起動がイネーブルになります。
- **disable** を指定すると、自動再起動がディセーブルになります。
- **show** を指定すると、自動再起動ステータスが表示されます。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

utils service list

すべてのサービスとそのステータスの一覧を取得します。

コマンド構文

utils service list [**page**]

オプション

- **page**：出力を一度に 1 ページずつ表示します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils sftp handshake

クラスタのすべてのメンバと SFTP SSH キーを交換します。

コマンド構文

utils sftp handshake

utils snmp

このコマンドは、サーバ上の SNMP を管理します。

コマンド構文

utils snmp

get *version community ip-address object* [*file*]

hardware-agents [**status** | **restart**]

test

walk *version community ip-address object* [*file*]

パラメータ

- **get** を指定すると、指定した SNMP オブジェクトの値が表示されます。
- **hardware-agents status** を指定すると、サーバ上のハードウェア エージェントのステータスが表示されます。
- **hardware-agents stop** を指定すると、ハードウェア ベンダーから提供されているすべての SNMP エージェントが停止します。
- **hardware-agents restart** を指定すると、サーバ上のハードウェア エージェントが再起動されます。
- **test** を指定すると、ローカル syslog、リモート syslog、SNMP トラップにサンプル アラームを送信することで、SNMP ホストがテストされます。
- **walk** を指定すると、指定した SNMP オブジェクトから始めて、SNMP MIB 内を移動します。
- *version* には SNMP バージョンを指定します。有効な値は 1 または 2c です。
- *community* には、SNMP コミュニティ ストリングを指定します。
- *ip-address* には、サーバの IP アドレスを指定します。ローカル ホストを指定するには 127.0.0.1 と入力します。クラスタ内の別のノードの IP アドレスを入力し、そのノード上でコマンドを実行できます。
- *object* には、取得する SNMP Object ID（OID; オブジェクト ID）を指定します。
- *file* には、コマンド出力を保存するファイルを指定します。

要件

コマンド特権レベル：1

アップグレード時の使用：可能

utils snmp walk 3

このコマンドは、指定した OID から始めて、SNMP MIB 内を移動するために使用します。

コマンド構文

utils snmp walk 3

（システムによりパラメータの入力が求められます）

例：

MIB のリーフに対して snmp walk を実行すると、基本的に「utils snmp get ...」コマンドで得られるのと同じ内容が得られます。次に、OID 1.3.6 に対して得られる walk の出力例を示します。

iso.3.6.1.2.1.1.1.0 = STRING: "Hardware:7825H, 1 Intel(R) Pentium(R) 4 CPU 3.40GHz, 2048 MB Memory: Software:UCOS 2.0.1.0-62"

iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.583

iso.3.6.1.2.1.1.3.0 = Timeticks: (15878339) 1 day, 20:06:23.39

iso.3.6.1.2.1.1.4.0 = ""

iso.3.6.1.2.1.1.5.0 = STRING: "bldr-ccm34.cisco.com"

iso.3.6.1.2.1.1.6.0 = ""

iso.3.6.1.2.1.1.7.0 = INTEGER: 72

iso.3.6.1.2.1.2.1.0 = INTEGER: 3

iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1

iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2

iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3

iso.3.6.1.2.1.2.2.1.2.1 = STRING: "lo"

iso.3.6.1.2.1.2.2.1.2.2 = STRING: "eth0"

iso.3.6.1.2.1.2.2.1.2.3 = STRING: "eth1"

iso.3.6.1.2.1.2.2.1.3.1 = INTEGER: 24

iso.3.6.1.2.1.2.2.1.3.2 = INTEGER: 6

iso.3.6.1.2.1.2.2.1.3.3 = INTEGER: 6

iso.3.6.1.2.1.2.2.1.4.1 = INTEGER: 16436

iso.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500

iso.3.6.1.2.1.2.2.1.4.3 = INTEGER: 1500

iso.3.6.1.2.1.2.2.1.5.1 = Gauge32: 0

iso.3.6.1.2.1.2.2.1.5.2 = Gauge32: 100000000

iso.3.6.1.2.1.2.2.1.5.3 = Gauge32: 10000000

iso.3.6.1.2.1.2.2.1.6.1 = Hex-STRING: 00 00 00 00 00 00

iso.3.6.1.2.1.2.2.1.6.2 = Hex-STRING: 00 16 35 5C 61 D0

iso.3.6.1.2.1.2.2.1.6.3 = Hex-STRING: 00 16 35 5C 61 CF

iso.3.6.1.2.1.2.2.1.7.1 = INTEGER: 1

.....

リモート ホストの IP アドレスを指定した場合、コマンドはそのリモート ホスト上で実行されます。ドメイン名ではなく IP アドレスを指定する必要があることに注意してください。

要件

コマンド特権レベル：1

アップグレード時の使用：不可

utils snmp get 3

指定した MIB OID の SNMP データを取得します。

コマンド構文
utils snmp get 3

（システムによりパラメータの入力が求められます）

例：
MIB 内の特定の OID（リーフ）に対して実行した場合、その MIB の値が得られます。システム アップタイムの snmp get の出力例は、iso.3.6.1.2.1.25.1.1.0 = Timeticks: (19836825) 2 days, 7:06:08.25 となります。

リモート ホストの IP アドレスを指定した場合、コマンドはそのリモート ホスト上で実行されます。ドメイン名ではなく IP アドレスを指定する必要があることに注意してください。

要件
コマンド特権レベル：1

アップグレード時の使用：不可

utils system

このコマンドを使用すると、同じパーティションでのシステムの再起動、非アクティブなパーティションでのシステムの再起動、またはシステムのシャットダウンを実行できます。

コマンド構文
utils system {**restart** | **shutdown** | **switch-version**}

パラメータ
restart を指定すると、システムが再起動されます。

shutdown を指定すると、システムがシャットダウンされます。

switch-version を指定すると、非アクティブ パーティションにインストールされている製品リリースに切り替えられます。

使用上のガイドライン
utils system shutdown コマンドには 5 分間のタイムアウトがあります。システムが 5 分以内にシャットダウンしない場合、強制的にシャットダウンするかどうかを質問されます。

要件
コマンド特権レベル：1

アップグレード時の使用：不可

utils system boot

システム ブート出力の送信先をリダイレクトします。

コマンド構文
utils system boot {console | serial | status}

パラメータ
- **console** を指定すると、システム ブート出力がコンソールにリダイレクトされます。
- **serial** を指定すると、システム ブート出力が COM1（シリアル ポート 1）にリダイレクトされます。
- **status** を指定すると、シリアル ブート出力の現在の送信先が表示されます。

要件
レベル特権：1

コマンド特権：1

アップグレード時の使用：可能

utils system upgrade

このコマンドを使用すると、アップグレードおよび Cisco Option Package（COP）ファイルを、ローカルとリモートの両方のディレクトリからインストールできます。

コマンド構文
utils system upgrade {initiate | cancel | status}

パラメータ
- **cancel** を指定すると、アクティブなアップグレードがキャンセルされます。
- **initiate** を指定すると、新しいアップグレード ウィザードを開始するか、既存のアップグレード ウィザードを制御します。ウィザードによりアップグレード ファイルの場所を入力するよう求められます。
- **status** を指定すると、アップグレードのステータスが表示されます。

使用上のガイドライン
システムをアップグレードするには、次の概略手順を実行します。

1. **utils system upgrade list** コマンドを使用して、アップグレード元として計画している、ローカル ディスクまたはリモート サーバ上にある .iso アップグレード ファイルの一覧を表示します。
2. **utils system upgrade get** コマンドを使用して、使用するアップグレード ファイルを取得します。
3. **utils system upgrade start** コマンドを使用して、取得したアップグレード ファイルからのアップグレードを開始します。

utils vmtools status

現在動作している VMware Tools のバージョンを表示します。

コマンド構文
utils vmtools status

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils vmtools upgrade

現在インストールされている VMware Tools を、その VM 用の ESXi ホストによって指示されている最新版に更新します。

コマンド構文

utils vmtools upgrade

VMWare でサポートされていないコマンド

- show environment fans
- show environment power-supply
- show environment temperatures
- show memory size
- show memory count
- show memory modules all
- utils create report hardware
- utils snmp hardware-agents restart
- utils snmp hardware-agents start
- utils snmp hardware-agents status
- utils snmp hardware-agents stop

APPENDIX G

特定のサービス プロバイダーに対する AFT の使用

次のトピックでは、特定のサービス プロバイダーに ALI フォーマット ツール（AFT）を使用する方法について説明します。

Bell-Canada に対する ALI フォーマット ツールの使用

次のトピックでは、Bell-Canada に AFT を使用する方法について説明します。

トランザクション コードの変更

サービス プロバイダーの Bell Canada に AFT を使用する場合、Bell Canada のトランザクション コードが A または D であることを確認してください。それ以外の場合、Bell Canada はレコードを拒否し、エラー メッセージとともにレコードを Error Return ファイルに入れて返します。

表 G-1 は、NENA レコードの [Function Code] フィールドに表示される値と、Bell Canada レコードの [Transaction Code] の対応する値を示しています。

表 G-1　NENA および Bell Canada の [Function] および [Transaction Code] フィールド

NENA の [Function Code] フィールド	Bell Canada の [Transaction Code] フィールド
新規レコード挿入の場合 I	新規レコード追加の場合 A
レコード変更の場合 C	レコード変更の場合 A。 （注）　NENA のファンクション コード C は、Bell Canada のトランザクション コード A にマッピングされます。
レコード削除の場合 D	レコード削除の場合 D

Bell-Canada 固有データの入力

表 G-2 に、残りの Bell Canada 固有フィールドを示します。一部のフィールドでは、Bell Canada の ALI データのサポート資料で指定された形式で ALI ファイルを生成するためのデータが必要です。他のフィールドは空白にできます。

これらのフィールドでエラーが発生した場合、Bell Canada はレコードを拒否し、エラー コードとともに Error Return ファイルを返します。

（注）　[Language Indicator] フィールドは AFT を使用して設定しません。AFT はフィールドを英語の E に設定します。

表 G-2　Bell Canada 固有のフィールドの変更

フィールド	説明	書式	注
Service Class	顧客の端末番号の電話サービスの種類	3 文字の英数字	必須フィールド。
Postal Code	顧客のサービス アドレスの郵便番号	6 文字の英数字	必須フィールド。最初の文字はアルファベットにする必要があります。
Municipality Code	各地方自治体に割り当てられた固有のコード	3 文字の英数字	必須フィールド。
Class of Service	サービスのグレード、クラス、およびタイプを識別するコード	5 文字の英数字	必須フィールド。
System Source	トランザクション レコードのソース データベースを識別	1 文字の英数字	必須フィールド。
Location Type	建物内の場所のタイプ（例：アパート）	15 文字の英数字	オプション フィールド。
Location Number	[Location Type] フィールドで識別されたロケーションの番号（アパート 2、フロア 2、など）	6 文字の英数字	オプション フィールド。

表 G-2　Bell Canada 固有のフィールドの変更（続き）

フィールド	説明	書式	注
Service Municipality	市町村、区、地域	35 文字の英数字	必須フィールド。
LSP ID	Bell Canada が PS ALI 顧客に提供した、ローカル電話サービスのプロバイダーを示す固有コード。	5 文字の英数字	必須フィールド。 Bell Canada が PS ALI 顧客に提供した有効な LSP 識別子である必要があります。

SBC-Ameritech に対する ALI フォーマット ツールの使用

SBC Ameritech（Ameritech）には、AFT を使用して変更する必要のあるサービス プロバイダー固有のフィールドはありません。しかし、AFT を使用して Ameritech のレコードをフォーマットする場合、ファンクション コードを変更する必要があります。

Emergency Responder は、ファンクション コードを次の 1 つに設定します。

- 新規 ALI レコードの挿入の場合 I（デフォルト）
- 番地の変更など ALI レコード更新の場合 C
- ALI 削除の場合 D

Emergency Responder で ALI レコードを変更して、Ameritech から報告されたエラーを訂正した場合、AFT を使用して、ELIN レコードのファンクション コードを変更しなければならない場合があります。

たとえば、Emergency Responder では、まず挿入のファンクション コード I で ALI レコードが生成されます。AFT を使用してファイルをフォーマットし、Ameritech にエクスポートした後、番地のサフィクスが誤っているなどのエラーにより Ameritech がファイルを拒否する可能性があります。このフィールドは無効になっているため、AFT で番地のサフィクスを変更できません。代わりに、Emergency Responder を使用して ALI レコードを変更する必要があります。

Emergency Responder が、変更後再び ALI レコードを生成すると、最初のファイルが受け入れられたと想定して、ファンクション コードは C に設定されます。AFT を使用して、ELIN レコードのファンクション コードを C から I に変更します。その後、AFT を使用してフォーマットを生成し、再フォーマットしたファイルを Ameritech に送信します。

SBC-PacBell に対する ALI フォーマット ツールの使用

次のトピックでは、SBC-PacBell に AFT を使用する方法について説明します。

- 「[Call Back For This ELIN] の有効化」（P.G-3）
- 「ファンクション コードの変更」（P.G-4）

[Call Back For This ELIN] の有効化

Emergency Responder は PSAP で ELIN を表示します。緊急コールがなんらかの理由で切断された場合、または単に PSAP が発信者ともう一度話す必要がある場合、PSAP は緊急コールの発信者にダイヤルして再接続できます。

[Call Back for this ELIN] オプションでは、架空の番号から 911 に通報があった場合に PSAP が使用できる Direct Inward Dial（DID; ダイヤルイン）番号を指定できます。

[Call Back for this ELIN] オプションは、2 つの重要な機能を果たします。

- PSAP に、コールバック先の電話が 911 コールを生成しなかった可能性があることを警告します。
- PSAP は、実際に通報した架空の電話番号の近くにある電話にコールバックできます。

[Call Back for this ELIN] フィールドをオンにして、このオプションを常に有効にしておくことをお勧めします。（デフォルトでは、フィールドを空白、No です）。

ファンクション コードの変更

Emergency Responder は、ファンクション コードを次の 1 つに設定します。

- 新規 ALI レコードの挿入の場合 I（デフォルト）
- 番地の変更など ALI レコード更新の場合 C
- ALI 削除の場合 D

Emergency Responder で ALI レコードを変更して、サービス プロバイダーから報告されたエラーを訂正した場合、AFT を使用して ELIN レコードのファンクション コードを変更しなければならない場合があります。

たとえば、Emergency Responder では、まず挿入のファンクション コード I で ALI レコードが生成されます。AFT を使用してファイルをフォーマットし、SBC Pacific Bell（PacBell）にエクスポートした後、PacBell はファイルを拒否する可能性があります。エラーの原因としては、たとえば番地のサフィクスが誤っていることが考えられます。このフィールドは無効になっているため、AFT で番地のサフィクスを変更できません。Emergency Responder を使用して ALI レコードを変更する必要があります。

Emergency Responder が、変更後再び ALI レコードを生成すると、最初のファイルが受け入れられたと想定して、ファンクション コードは C に設定されます。AFT を使用して、ELIN レコードのファンクション コードを C から I に変更します。その後、AFT を使用してフォーマットを生成し、再フォーマットしたファイルを PacBell に送信します。

SBC-Southwestern Bell に対する ALI フォーマット ツールの使用

次のトピックでは、SBC-Southwestern Bell に AFT を使用する方法について説明します。

- 「SBC-Southwestern Bell の PS コードの変更」（P.G-4）
- 「ファンクション コードの変更」（P.G-5）

SBC-Southwestern Bell の PS コードの変更

Southwestern Bell で ELIN レコードを変更するには、AFT を使用して、PS Code フィールドを使用する必要があります。このフィールドは Southwestern Bell に特有です。PS コードは、新規 PS サイトが設定されるたびに Southwestern Bell が割り当てる 4 桁のコードです。このコードは、PS ユーザのログインおよびソースに関連付けられます。

PS コードは、正しい PS コードを持つレコードだけが PS サイトのテーブルに処理されるようにする機能です。PS コードが PS サイトに割り当てられた設定済みのソース名と一致しない場合、レコードは処理されません。AFT を使用してフォーマット済みファイルを生成する前に、PS Code と Source Name が一致することを確認します。詳細については、Southwestern Bell のマニュアルを参照してください。

ファンクション コードの変更

Emergency Responder は、ファンクション コードを次の 1 つに設定します。

- 新規 ALI レコードの挿入の場合 I（デフォルト）
- 番地の変更など ALI レコード更新の場合 C
- ALI 削除の場合 D

Emergency Responder で ALI レコードを変更して、サービス プロバイダーから報告されたエラーを訂正した場合、AFT を使用して ELIN レコードのファンクション コードを変更しなければならない場合があります。

たとえば、Emergency Responder では、まず挿入のファンクション コード I で ALI レコードが生成されます。AFT を使用してファイルをフォーマットし、Southwestern Bell にエクスポートした後、Southwestern Bell はファイルを拒否する可能性があります。エラーの原因としては、たとえば番地のサフィクスが誤っていることが考えられます。このフィールドは無効になっているため、AFT で番地のサフィクスを変更できません。Emergency Responder を使用して ALI レコードを変更する必要があります。

Emergency Responder が、変更後再び ALI レコードを生成すると、最初のファイルが受け入れられたと想定して、ファンクション コードは C に設定されます。AFT を使用して、ELIN レコードのファンクション コードを C から I に変更します。その後、AFT を使用してフォーマットを生成し、再フォーマットしたファイルを Southwestern Bell に送信します。

Qwest に対する ALI フォーマット ツールの使用

Qwest には、AFT を使用して変更する必要のあるサービス プロバイダー固有のフィールドはありません。しかし、AFT を使用して Qwest のレコードをフォーマットする場合、ファンクション コードを変更する必要があります。

Cisco Emergency Responder（Emergency Responder）は、ファンクション コードを次の 1 つに設定します。

- 新規 ALI レコードの挿入の場合 I（デフォルト）
- 番地の変更など ALI レコード更新の場合 C
- ALI 削除の場合 D

Emergency Responder で ALI レコードを変更して、Qwest から報告されたエラーを訂正した場合、AFT を使用して、ELIN レコードのファンクション コードを変更しなければならない場合があります。

たとえば、Emergency Responder では、まず挿入のファンクション コード I で ALI レコードが生成されます。AFT を使用してファイルをフォーマットし、Qwest にエクスポートした後、エラーにより Qwest がファイルを拒否する可能性があります。エラーの原因としては、たとえば番地のサフィクスが誤っていることが考えられます。このフィールドは無効になっているため、AFT で番地のサフィクスを変更できません。Emergency Responder を使用して ALI レコードを変更する必要があります。

Emergency Responder が、変更後再び ALI レコードを生成すると、最初のファイルが受け入れられたと想定して、ファンクション コードは C に設定されます。AFT を使用して、ELIN レコードのファンクション コードを C から I に変更します。その後、AFT を使用してフォーマットを生成し、再フォーマットしたファイルを Qwest に送信します。

Verizon に対する ALI フォーマット ツールの使用

次のトピックでは、Verizon に AFT を使用する方法について説明します。

ファンクション コードの変更

Verizon には、AFT を使用して変更する必要のあるサービス プロバイダー固有のフィールドはありません。しかし、AFT を使用して Verizon のレコードをフォーマットする場合、ファンクション コードを変更する必要があります。

Emergency Responder は、ファンクション コードを次の 1 つに設定します。

- I：新規 ALI レコードの挿入（デフォルト）
- C：番地の変更など、ALI レコードの更新
- D：ALI レコードの削除
- U：ALI レコードのロック解除（市内番号ポータビリティをサポートするために含まれる）
- M：ALI レコードの移行（市内番号ポータビリティをサポートするために含まれる）

Emergency Responder で ALI レコードを変更して、Verizon から報告されたエラーを訂正した場合、AFT を使用して、ELIN レコードのファンクション コードを変更しなければならない場合があります。

たとえば、Emergency Responder では、まず挿入のファンクション コード I で ALI レコードが生成されます。AFT を使用してファイルをフォーマットし、Verizon にエクスポートした後、エラーにより Verizon がファイルを拒否する可能性があります。エラーの原因としては、たとえば番地のサフィクスが誤っていることが考えられます。このフィールドは無効になっているため、AFT で番地のサフィクスを変更できません。Emergency Responder を使用して ALI レコードを変更する必要があります。

Emergency Responder が、変更後再び ALI レコードを生成すると、最初のファイルが受け入れられたと想定して、ファンクション コードは C に設定されます。AFT を使用して、ELIN レコードのファンクション コードを C から I に変更します。その後、AFT を使用してフォーマットを生成し、再フォーマットしたファイルを Verizon に送信します。

Verizon のニューイングランド諸州の Disability Indicator の変更

Verizon のニューイングランド諸州（MA、ME、NH、RI、VT）で ELIN を読み取り可能にするには、AFT を使用して、Verison に固有の [Disability Indicator] フィールドを更新する必要があります。Disability Indicator は、事業者が身体障がい者情報を入力するために使用できる 20 文字の予約フィールドです。

表 G-3 は、ALI レコードのロケーション フィールドへの読み込みに使用できる Disability Indicator を示しています。

表 G-3　Disability Indicator の説明

Disability Indicator	説明
LSS	ライフ サポート システム
MI	運動障がい
B	目が見えない
DHH	聴覚障がい
TTY	テレタイプライタ
SI	言語障がい
DD	発達障がい

AFT は、ニューイングランド諸州をインテリジェントに識別し（ALI レコードの州フィールドから）、[Disability Indicator] フィールドの個別更新（ツリーから New England の ELIN レコードを選択）または一括更新（バルク更新機能）できるようにします。

Verizon の西部諸州の顧客名の変更

Verizon の西部諸州（CA、HI、ID、IL、IN、MI、NC、OH、OR、SC、TX、WA、WI）は、姓と名の間にカンマとスペースを入れる次のフォーマットで [Customer Name] フィールドを読み取ります。

姓, 名

このフォーマットで、PSAP での表示エラーを防ぎます。Verizon の西部諸州で使用されている書式に従うように、AFT を使用してフィールドを更新できます。

AFT は、西部諸州をインテリジェントに識別し（ALI レコードの州フィールドから）、[Customer Name] フィールドの個別更新（ツリーから Verizon West の ELIN レコードを選択）または一括更新（バルク更新機能）できるようにします。

AFT を使用して更新すると、[Customer Name] フィールドには、2 つの異なるエントリ（Emergency Responder データベースに 1 つ、サービス プロバイダーのデータベースに 1 つ）が作成されます。将来不一致が発生するのを防ぐために、Emergency Responder GUI の [Customer Name] フィールドで同じ更新を行ってください。

ニュージャージーのロケーションの変更

Verizon のニュージャージー（NJ）システムは、ロケーション データをすべての PSAP で一様に表示するという州の要件に基づくキーワード型のシステムです。1 つ以上のキーワード、関連データ、デリミタが所定の正確な書式で存在する場合のみ、ロケーション フィールドからデータが抽出されます。NJ システムのロケーションには、PSAP で同時に表示できる 4 つの異なるロケーション タイプ フィールドがあります。ロケーション タイプ フィールドは次のとおりです。

- Unit Type（APT、BOX、LOT、PIER、RM、ROOM、RU、SUIT、SUITE、UNIT、WING）
- Floor Number（FLR）
- Building Description（BLDG）
- Coin Location Description（DES）

AFT は、ロケーションに関する NJ システム固有の要件をインテリジェントに識別し（ALI レコードの州フィールドから）、ロケーションの個別更新（ニュージャージーの ELIN を選択）およびバルク更新（バルク更新機能）できるようにします。

AFT を使用して更新すると、[Customer Name] フィールドには、2 つの異なるエントリ（Emergency Responder データベースに 1 つ、サービス プロバイダーのデータベースに 1 つ）が作成されます。将来不一致が発生するのを防ぐために、Emergency Responder GUI の [Location] フィールドで同じ更新を行ってください。

APPENDIX H

イベント ログ メッセージ

イベント ログ メッセージは、次のモジュールで使用できます。

CER_DATABASE

表 H-1　CER_DATABASE のイベント ログ メッセージ

タイプ	メッセージ
INFO	Failed to get the fully qualified host name.DNS might not be enabled.Putting Ipaddress in Cluster database.
ERROR	CER Server Memory Usage is HIGH, above threshold value of 80%.Memory Figures: <MEMORY USAGE INFO>.
ERROR	Database replication broken.
ERROR	Number of <NUM> limit exceeded.Fetching only a maximum of *** <NUM> *** entries.

CER_SYSADMIN

表 H-2　CER_SYSADMIN のイベント ログ メッセージ

タイプ	メッセージ
ERROR	Failed to add this CER group to CER cluster
WARNING	CER cluster functionality fails until this problem is fixed. 1. Check if "CERCluster password" is same as in CER ClusterDB. 2. Check if Cisco Tomcat and Database services are running on CER ClusterDB. 3. Check if CER ClusterDB Hostname is correct and accessible
ERROR	Failed to initialize LDAP.

CER_TELEPHONY

表 H-3　CER_TELEPHONY のイベント ログ メッセージ

タイプ	メッセージ
WARNING	Emergency call from <CALLING ADDRESS> has been routed to default ERL because calling party modification failed. Please make sure that the checkbox "Enable Calling Party Number Modification" is checked on the Call Manager user page for the CER user.PSAP callbacks MAY NOT work correctly.The CER service must be restarted once the flag is checked on the Call Manager User page.
WARNING	Emergency call from <calling address> could not be routed using the following Routepatterns. <LIST OF RP's> Call Routed to <RP/NUMBER> Please check the availability of the above routes. Also, you must check for the following error conditions: 1. If FAC or CMC are configured on the route patterns used for CER, please disable them. 2. If the "Calling Party Number Modification" flag on the CER user page in the call manager is not enabled, please enable it.
ERROR	Failed to load class <CLASS NAME>.
ERROR	CCMString is empty can't load telephony classes.
WARNING	Got OutOfService event from provider: <PROVIDER_NAME>.
INFO	Got InService event from provider: <PROVIDER_NAME>.
WARNING	Logged out of the duplicate provider - <CTI_Manager> from CER.Specify the CTI Ports (if any) of this provider, in a different CCM node.

表 H-3　CER_TELEPHONY のイベント ログ メッセージ（続き）

タイプ	メッセージ
ERROR	Cannot register media terminal for port: <PORT_NUMBER>.
WARNING	CTI Port: <PORT_NUMBER> is in OUTOFSERVICE, trying after 10 seconds.
ERROR	Mediachannel creation failed: <ERROR>.
WARNING	Failed to create media channel for: <PORT_NUMBER>.
ERROR	Failed to initiate call to security: <NUMBER> <ERROR>. <ERROR> corresponds to: • PrivilegeViolationException • InvalidPartyException • MethodNotSupportedException • InvalidArgumentException • InvalidStateException • E911CallRouterException • <Other Exceptions (if any)>
ERROR	Failed to register route point: <ROUTE_PATTERN> with Provider: <PROVIDER_NAME>.
ERROR	RouteAddress: <ADDRESS> is in OUTOFSERVICE.
WARNING	<ADDRESS> Route Point received IN_SERVICE event from Provider <NAME>.
WARNING	<ADDRESS> Route Point received OUT_OF_SERVICE event from Provider <NAME>.

表 H-3　CER_TELEPHONY のイベント ログ メッセージ（続き）

タイプ	メッセージ
ERROR	PSAP Callback failed for: <NUMBER> "Address = "+callingAddress+" ; Terminal = "+callingTerminal; because, routeEndEvent returned: < EXCEPTION> Exception can be: • CAUSE_INVALID_DESTINATION • CAUSE_ROUTING_TIMER_EXPIRED • CAUSE_PARAMETER_NOT_SUPPORTED • CAUSE_STATE_INCOMPATIBLE • CAUSE_UNSPECIFIED_ERROR ERROR_RESOURCE_BUSY.Please check availability of the Routes CAUSE_CTIERR_FAC_CMC_REASON_FAC_NEEDED.Please Uncheck the Requirement of FAC/CMC codes on the Route points used by the Cisco ER. CAUSE_CTIERR_FAC_CMC_REASON_CMC_NEEDED.Please Uncheck the Requirement of FAC/CMC codes on the Route points used by the Cisco ER. CAUSE_CTIERR_FAC_CMC_REASON_FAC_CMC_NEEDED.Please Uncheck the Requirement of FAC/CMC codes on the Route points used by the Cisco ER. CAUSE_CTIERR_FAC_CMC_REASON_FAC_INVALID.Please Uncheck the Requirement of FAC/CMC codes on the Route points used by the Cisco ER. CAUSE_CTIERR_FAC_CMC_REASON_CMC_INVALID.Please Uncheck the Requirement of FAC/CMC codes on the Route points used by the Cisco ER.

表 H-3　CER_TELEPHONY のイベント ログ メッセージ（続き）

タイプ	メッセージ
ERROR	Call failed to reach PSAP for: <NUMBER> "Address = "+callingAddress+" ; Terminal = "+callingTerminal; because, routeEndEvent returned: <EXCEPTION> Exception can be: • CAUSE_INVALID_DESTINATION • CAUSE_ROUTING_TIMER_EXPIRED • CAUSE_PARAMETER_NOT_SUPPORTED • CAUSE_STATE_INCOMPATIBLE • CAUSE_UNSPECIFIED_ERROR ERROR_RESOURCE_BUSY.Please check availability of the Routes CAUSE_CTIERR_FAC_CMC_REASON_FAC_NEEDED.Please Uncheck the Requirement of FAC/CMC codes on the Route points used by the Cisco ER. CAUSE_CTIERR_FAC_CMC_REASON_CMC_NEEDED.Please Uncheck the Requirement of FAC/CMC codes on the Route points used by the Cisco ER. CAUSE_CTIERR_FAC_CMC_REASON_FAC_CMC_NEEDED.Please Uncheck the Requirement of FAC/CMC codes on the Route points used by the Cisco ER.CAUSE_CTIERR_FAC_CMC_REASON_FAC_INVALID.Please Uncheck the Requirement of FAC/CMC codes on the Route points used by the Cisco ER. CAUSE_CTIERR_FAC_CMC_REASON_CMC_INVALID.Please Uncheck the Requirement of FAC/CMC codes on the Route points used by the Cisco ER.
WARNING	Call from <CALLER_ID> could not be routed to the Intrado ERL.Possible reasons: The TN Update to Intrado for the Intrado ERL may not yet happened or has met with errors.
WARNING	Call from <CALLER ID> could not be routed to the Offpremies ERL.Possible reasons: The phone-location association has not yet happened or has met with errors.
WARNING	Failed to get the JTAPI Provider for: <NAME_STRING> trying infinitely.
WARNING	Not registering the provider: <PROVIDER_NAME> as is already registered/in the same CCM Cluster as that of:<element>.
WARNING	JTAPI logs are not enabled as the logs path is empty in E911Bootstrap properties.
ERROR	Failed to get the JTAPI Provider for: <IP Address/Host Name> after <NUMBER> attempts.
WARNING	Currently, no CTI Ports are available to place the call for <CallingAddress>.Phone notification is retried in the next 60 seconds.

CER_AGGREGATOR

表 H-4　CER_AGGREGATOR のイベント ログ メッセージ

タイプ	メッセージ
WARNING	Device <IP Address> is SNMP unreachable. Please check SNMP settings in CER and on this CCM. Please confirm proper access privilege (READ_ONLY) set on this box for SNMP service.Also, verify n/w connectivity.
WARNING	During discovery some devices are unreachable. List of Unreachable Switches <List>.
WARNING	WARNING During discovery some devices are unreachable. List of Unreachable CCMs <List>.
WARNING	CER Server could not communicate with CERPhoneTrackingEngine.
WARNING	CERServer could not communicate with CERPhoneTrackingEngine.
INFO	Device <IP Address> is SNMP unreachable. Please check SNMP settings in CER and on this CCM. Please confirm proper access privilege (READ_ONLY) set on this box for SNMP service.Also, verify n/w connectivity.
INFO	Error in resolving HostName -> IPAddress through DNS, ignoring the seed from DE <IP Address>.
INFO	IP Address mismatch detected,OLD_IP <IP Address> NEW_IP <IP Address> SEED <IP Address> for any changed configuration, deletion and re addition of seed device is recommended.
INFO	Device <IP Address> is not a valid switch.
INFO	Device <IP Address> is SNMP Un-reachable.
INFO	Device <IP Address> is not supported.
INFO	This Device <IP Address> is identified for a different device family than earlier discovered, ignored for this discovery cycle.
INFO	Failed to retrieve SysOid of a device <IP Address> Please check if device is SNMP reachable.
INFO	This device is not supported <seed>.
INFO	This Device <IP Address> is earlier discovered with different device family. Please note, for changed device config.(ipAddress, deviceFamily, dnsName), delete and re-add the device is must, also you must re-enter SNMP community string if changed from earlier one.
INFO	The device <IP Address> is not a valid switch...please confirm.
INFO	This device not a valid CCM to discover <IP Address>.
INFO	Error in resolving HostName -> IPAddress, ignoring the seed for discovery <IP Address>.

表 H-4　CER_AGGREGATOR のイベント ログ メッセージ（続き）

タイプ	メッセージ
INFO	IP Address mismatch detected,OLD_IP <IP Address> NEW_IP <IP Address> SEED <IP Address> for any changed configuration, deletion and re addition of seed device is recommended.
INFO	Device <IP Address> is not a valid CCM.

CER_GROUP

表 H-5　CER_GROUP のイベント ログ メッセージ

タイプ	メッセージ
INFO	Active Cisco ER set to: <Server Details>.
INFO	Connection established with Cisco ER: <PEER>.
WARNING	Disconnected from Cisco ER: <PEER>.
ERROR	Cisco ER Couldn't open socket at port <NUMBER>, Exiting.
WARNING	Failed to open connection with Cisco ER: <_remoteAddress> / <_remotePort>.

CER_CALLENGINE

表 H-6　CER_CALLENGINE のイベント ログ メッセージ

タイプ	メッセージ
INFO	Cisco ER Exiting: <MSG> Graceful shutdown.
ERROR	Problem in initializing SERVER (Server Group).Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing Database (E911ServerGroupParameters).Retried... <COUNT> times.
ERROR	Problem in initializing SERVER (Server).Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing Database (Server).Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing Database (CERServers).Retried... <COUNT> times.
ERROR	Problem in initializing SERVER (License).Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (Zone).Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (DiscoveryEngine).Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (CERIPSubnetManager).Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (CERVHMPhoneManager).Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (CCM Cluster - No Call Manager seeds configured).Cannot continue... <EXCEPTION>.

表 H-6　CER_CALLENGINE のイベント ログ メッセージ（続き）

タイプ	メッセージ
ERROR	Problem in initializing SERVER (Seed Switch).Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (Discrepant entry).Cannot continue... <EXCEPTION>C96.
ERROR	Problem in initializing SERVER (Security Contact).Cannot continue... <EXCEPTION>.
ERROR	Problem in refreshing LDAP (Server Group).Cannot continue...
ERROR	Problem in refreshing LDAP (Zone).Cannot continue...
ERROR	Problem in refreshing LDAP (Server).Cannot continue...
ERROR	Problem in refreshing LDAP (Seed Switch).Cannot continue...
ERROR	Problem in refreshing LDAP (CCM Cluster).Cannot continue...
ERROR	Problem in refreshing LDAP (Discrepant entry).Cannot continue...
ERROR	Problem in refreshing LDAP (Security Contact).Cannot continue...
ERROR	Problem in refreshing LDAP (Security Contact).Cannot continue...
ERROR	Problem in refreshing zone port tree (Switchport to zone map).Cannot continue...
ERROR	LicenseManager: End Of 60 Day Evaluation Period.CER Will not work.Please upload a valid License file".
ERROR	End Of 30 Day Grace Period.Please upload a valid license file for CER to function.Current License MAC: <License MAC value>
WARNING	Warning!!!You have exhausted all your user licenses.Please purchase additional user licenses. Number of phones being tracked/configured: <num> Total user license: <num>
INFO	License MAC change is detected in the system.System will now operate in 30 day grace period.Please upload a valid license before grace period expires.
INFO	user license count could not be read.
INFO	Reason:
WARNING	License manager Init: Error loading license, Possibly there is no license file.
WARNING	License checkout failed: <message>.

CER_CLUSTER

表 H-7　CER_CLUSTER のイベント ログ メッセージ

タイプ	メッセージ
WARNING	IntraCluster Communication failed to ServerGroup with servers Master:<SERVER DETAILS> StandBy: <SERVER DETAILS>.

CER_ONSITEALERT

表 H-8　CER_ONSITEALERT のイベント ログ メッセージ

タイプ	メッセージ
WARNING	Backup Cisco ER <hostname> has taken control as Active Cisco ER. Transition time: <timestamp>.
WARNING	Master Cisco ER <hostname> has taken control as Active Cisco ER. Transition Time: <timestamp>.
WARNING	Emergency call Details Caller Extension: <num> Call Time: <time>
WARNING	Emergency call Details Caller Extension: <num> Zone/ERL: <zone> LOCATION: <location> Call Time: <time>

CER_ONSITEALERT

APPENDIX I

Emergency Responder でのポートの使用

Emergency Responder では次のポートが使用されます。

表 I-1　Emergency Responder でのポートの使用

プロトコル	TCP/UDP	ポート範囲	このプロトコルにおけるアプリケーション/ボックスの識別（Client、Server、または Peer）	相手側	製品との関連性	機能（機能このポートの使用が必須）
SNMP	UDP	161				SNMP ベースの管理アプリケーションにサービスを提供します。
SNMP	UDP	6161				ネイティブ SNMP エージェントは、SNMP マスター エージェントによって転送される要求をリッスンします。
SNMP	UDP	6162				SNMP マスター エージェントは、管理アプリケーションに転送されるネイティブ SNMP エージェントからのトラップをリッスンします。
TCP	TCP	7161				SNMP マスター エージェントとサブエージェントとの通信に使用されます。
TCP	TCP	1500				IDS DB
TCP	TCP	1501				IDS DB
XML	TCP	1515				IDS DB
Proprietary	TCP	8500				Ipsec クラスタ マネージャ

表 I-1　Emergency Responder でのポートの使用（続き）

プロトコル	TCP /UDP	ポート範囲	このプロトコルにおけるアプリケーション/ボックスの識別（Client、Server、または Peer）	相手側	製品との関連性	機能（機能このポートの使用が必須）
N/A	TCP	22				セキュア ファイル転送プロトコル
TCP	TCP	22				リモート アクセスの SSH ポート
N/A	UDP	123				Cisco Unified CM サーバ上で使用される NTP ポート
HTTPS	TCP	443				HTTPS
N/A	UDP	500				Internet Security Association and Key Management Protocol。
N/A	UDP	514				システム ロギング サービス
Proprietary	TCP	2444				CTL Client が CTL Provider と通信し、クラスタのセキュリティ モードを設定して CTL ファイルを管理するために使用されます
TCP	TCP	3804				エンドポイントからの着信要求をリッスンする Certificate Authority Proxy Function（CAPF）ポート
XML	TCP	5555				License Manager は、このポートでのライセンス要求をリッスンします
TCP	TCP	7070				Certificate Manager デーモン
TCP	TCP	7999				Cellular Digital Packet Data Protocol
N/A	UDP	253、752、537、625、393				Compaq 管理エージェント拡張（cmaX）
HTTPS	TCP	50000 ～ 50004				HTTPS から HP SIM

表 I-1　Emergency Responder でのポートの使用（続き）

プロトコル	TCP/UDP	ポート範囲	このプロトコルにおけるアプリケーション/ボックスの識別（Client、Server、または Peer）	相手側	製品との関連性	機能（機能このポートの使用が必須）
N/A	UDP	67 および 68				Cisco Unified CM サーバ上で使用される DHCP ポート
N/A	UDP	エフェメラル				パッケージ管理ツール
N/A	UDP	エフェメラル				DNS
N/A	IP	GRE：IP 47、ESP：IP 50、AH：IP 51、IPSec：UDP 500。				IPSec 設定
SNMP	UDP	61441				内部 SNMP トラップ レシーバ
SMTP	TCP	25	client	SMTP Mail Server（*）	必須	電子ページ、電子メール通知の送信
CDP			client		必須	CDP 対応電話機の検出
CLM	UDP	8500	server	clm	必須	クラスタ マネージャ
SYSLOGD	UDP	514	server	syslog サーバ	オプション	syslog ポート
SYSLOG	UDP	8888	client	syslog クライアント	オプション	syslog ポート
HTTPS	TCP	8443	server	ブラウザ	必須	セキュア Web アクセス（Tomcat）
HTTP	TCP	8080	server	ブラウザ	必須	Web アクセス（Tomcat）
NTPD	UDP	123	client	NTP サーバ	オプション	ネットワーク時間の同期
Peer TCP	TCP	17001*	peer	Emergency Responder サーバ	必須	Emergency Responder のマスター バックアップ フェールオーバー
Peer RMI	TCP	7777	server	Emergency Responder サーバ	必須	Emergency Responder サーバの RMI ポート
Peer RMI	TCP	7778	server	Emergency Responder Admin	必須	Emergency Responder Admin の RMI ポート
Applet	TCP	55000	server	Applets	必須	Web アラート

表 I-1　Emergency Responder でのポートの使用（続き）

プロトコル	TCP /UDP	ポート範囲	このプロトコルにおけるアプリケーション/ボックスの識別（Client、Server、または Peer）	相手側	製品との関連性	機能（機能このポートの使用が必須）
SNMP	UDP	162	server	SNMP エージェント	オプション	ネットワーク管理
DBLRPC	TCP	1515	server	dblrpc	必須	DB 複製
RACOON	ESP		client	Emergency Responder サーバ	オプション	ipsec トラフィック
RACOON	UDP	500	client	Emergency Responder サーバ	オプション	ipsec 設定ポート
IDS	TCP	1500	server	IDS		Informix データベース サーバ

INDEX

数字

A

B

C

D

E

F

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

つ

て

と

ね

は

ひ

ふ

ほ

ゆ

よ

ら

り

る

れ

ろ

わ