AsyncOS 13.7 for Cisco Email Security Appliances リリースノート

発行日:2020 年 12 月 3 日
改定日:2024 年 1 月 30 日

目次

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

機能	説明
AsyncOS API を使用したログ情報の取得	AsyncOS API を使用して、電子メールゲートウェイから次のログ詳細を取得できるようになりました。 • サブスクリプションの詳細を記録します。 • 特定のログサブスクリプションのすべてのログファイル。 • ファイル名または URL を使用したログファイル。 詳細については、『*AsyncOS 13.7 API for Cisco Email Security Appliances - Getting Started Guide*』の「Logging APIs」セクションを参照してください。
監査ログを使用した認証、許可、アカウンティングのイベント（AAA: Authentication、Authorization、および Accounting）の記録	Cisco E メール セキュリティ ゲートウェイは、AAA（認証、許可、アカウンティング）のイベントを記録する新しいタイプのログサブスクリプション「監査ログ」をサポートしています。 監査ログの詳細の一部を次に示します。 • ユーザ - ログオン • ユーザ - ログオンに失敗しました、パスワードが正しくありません • ユーザ - ログオンに失敗しました、ユーザ名が不明です • ユーザ - ログオンに失敗しました、アカウントの有効期限が切れています • ユーザ - ログオフ • ユーザ - ロックアウト • ユーザ - アクティブ化済み • ユーザ - パスワードの変更 • ユーザ - パスワードのリセット • ユーザ -セキュリティ設定/プロファイルの変更 • ユーザ - 作成済み • ユーザー - 削除または変更 • ユーザ設定 - ユーザが行った設定変更。 • グループ/ロール - 削除/変更済み • グループ/ロール - アクセス許可の変更 • 隔離 - 隔離内のメッセージに対して実行されるアクション。 詳細は、ユーザガイドまたはオンラインヘルプの「ログ」の章を参照してください。

AsyncOS API 向けの電子メールゲートウェイでの OpenID Connect 1.0 の設定	Cisco E メール セキュリティ ゲートウェイは、OpenID Connect 1.0 認証で ID プロバイダー（IDP）を使用するアプリケーションまたはクライアントとの統合をサポートし、電子メールゲートウェイで使用可能な AsyncOS API とシームレスに接続します。現在、お使いの電子メールゲートウェイは、Microsoft AD FS のみを使用して OpenID Connectで認定されています。 詳細については、ユーザガイドまたはオンラインヘルプの「System Administration」の章と『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。
新しいアクセス権限：委任管理者のログサブスクリプション	新しいアクセス権限オプションである [ログサブスクリプション（Log Subscription）] が、アプライアンスの Web インターフェイスの [システム管理（System Administration）] > [ユーザロール（User Role）] ページに追加されました。[ログサブスクリプション（Log Subscription）] オプションを使用して、カスタムユーザロールに割り当てられている委任管理者がログサブスクリプションまたはログ API にアクセスしてログファイルを表示またはダウンロードできるかどうかを定義します。 詳細については、ユーザ ガイドまたはオンライン ヘルプの「Distributing Administrative Tasks」の章を参照してください。
クラウドコネクタロギングのサポート	アプライアンスは、新しいタイプのログサブスクリプション（**クラウドコネクタログ**）をサポートするようになりました。このログサブスクリプションを使用して、Cisco Aggregator Server からの Web インタラクション トラッキング データに関する情報を表示します。ほとんどの情報は、[情報（Info）] または [警告（Warning）] レベルです。
電子メールゲートウェイで SecureX Threat Response フィードの使用を設定	Cisco SecureX Threat Response ポータルから脅威フィードを使用するように電子メールゲートウェイを設定できるようになりました。 Cisco SecureX Threat Response ポータルでは、監視対象を継続的に収集するためのカスタムフィードを作成し、フィード URL を使用して電子メールゲートウェイでそれらを利用できます。フィードは、JSON 形式の監視対象の単純なリストです。フィードは、SecureX Threat Response ポータルの [インテリジェンス（Intelligence）] > [フィード（Feeds）] ページで作成および管理されます。 詳細については、以下を参照してください。 • このリリースに関連するユーザーガイドの「Configuring Email Gateway to Consume External Threat Feeds」の章の「How to Configure Email Gateway to Consume External Threat Feeds」および「Configuring SecureX Threat Response Feeds Source」のセクション。 • このリリースに関連する CLI リファレンスガイドの「The Commands: Reference Examples」の章の「Configuring Email Gateway to Consume External Threat Feeds」のセクション。

動作における変更

ファイル レピュテーション サービスの設定変更	アプライアンスでファイル レピュテーション サービスを設定する場合、SSL 通信を有効または無効にするオプションはありません。アプライアンスは、デフォルトで SSL プロトコルを使用し、ファイアウォールポート 443 のみを使用してファイル レピュテーション サービスと通信します。 アプライアンスでファイル レピュテーション サービスの SSL 通信設定を構成する次のオプションは削除されました。 • アプライアンスの Web インターフェイスの [セキュリティ サービス(Security Services)] > [ファイルレピュテーションと分析(File Reputation and Analysis)] ページの [SSL(ポート 443)を使用する(Use SSL (Port 443))] チェックボックス。 • 「ファイルレピュテーション用の SSL 通信(ポート 443)を有効にしますか?[Y]>(Do you want to enable SSL communication (port 443) for file reputation? [Y]>)」というステートメント(CLI の ampconfig > advanced サブコマンド)。
外部脅威フィード:ファイルハッシュ設定の変更	アプライアンスは、外部脅威フィード(ETF)エンジンによって悪意のあるものとして分類されたファイルハッシュを大文字と小文字を区別せずに検出し、メッセージに対して適切に設定されたアクションを適用するようになりました。

アップグレードの方法

- リリース 13.7.0-093 へのアップグレード:GD(一般導入)(4 ページ)
- リリース 13.7.0-087 へのアップグレード:LD(限定的な導入)(5 ページ)

リリース 13.7.0-093 へのアップグレード:GD(一般導入)

(注) Cisco E メール セキュリティ アプライアンス向け AsyncOS 13.7.0-093 は、Cisco Cloud Email Security ユーザ向けの一般的な導入リリースです。

(注) アップグレード中は、デバイス(キーボード、マウス、管理デバイス(Raritan)など)をアプライアンスの USB ポートに接続しないでください。

次のバージョンから、リリース 13.7.0-093 にアップグレードできます。

- 12.1.0-087
- 12.5.0-066
- 12.5.2-011
- 13.0.0-392

- 13.5.1-177
- 13.5.1-277
- 13.5.1-352
- 13.5.2-036
- 13.5.2-204
- 13.5.3-010
- 13.7.0-087

リリース 13.7.0-087 へのアップグレード：LD（限定的な導入）

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから、リリース 13.7.0-087 にアップグレードすることができます。

- 13.5.1-277
- 13.5.1-352

（注） Cisco E メール セキュリティ アプライアンス向け AsyncOS 13.7 リリースは、オンデマンドでプロビジョニングされます。ソフトウェア メンテナンス リリースをさらに受け取るには、Cisco E メール セキュリティ アプライアンス向け AsyncOS 14.0 リリース（数ヶ月内に利用可能になる予定）へのアップグレードをお勧めします。

インストールおよびアップグレードに関する注意事項

このセクションに記載されているインストールとアップグレードの影響を把握および検討してください。

Web インターフェイスまたは CLI（コマンド ライン インターフェイス）から AsyncOS をアップグレードすると、設定は /configuration/upgrade ディレクトリ内のファイルに保存されます。FTP クライアントを使用して、アップグレード ディレクトリにアクセスできます。各設定ファイル名にはバージョン番号が付加され、設定ファイル内のパスワードは人間が判読できないようにマスクされます。

管理者権限を持つユーザーとしてログインして、アップグレードする必要があります。また、アップグレード後にアプライアンスを再起動する必要があります。

このリリースでサポートされているハードウェア

- すべての仮想アプライアンスモデル
- 次のハードウェア モデル
  - C190
  - C195

- C390
- C395
- C690
- C695
- C695F

（注） [C695 および C695F モデルの場合のみ]：アプライアンスをアップグレードまたは再起動する前に、接続されているファイバ スイッチ ポート インターフェイスで LLDP を無効にします。これにより、FCoE トラフィックが自動的に無効になります。

アプライアンスがサポートされているかどうかを確認し、現在互換性がない場合にその状況を解決するには、http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html を参照してください。

このリリースでは、次のハードウェアはサポートされていません。

- C160、C360、C660、および X1060
- C170、C370、C370D、C670、および X1070
- C380 および C680 アプライアンス

仮想アプライアンスの展開またはアップグレード

仮想アプライアンスを展開またはアップグレードする場合は、『Cisco コンテンツセキュリティ仮想アプライアンス インストール ガイド』を参照してください。このドキュメントは https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-installation-guides-list.html から入手できます。

仮想アプライアンスのアップグレード

現在の仮想アプライアンスのリリースが 2 TB 以上のディスク領域をサポートしておらず、このリリースで 2 TB 以上のディスク領域を使用する場合は、仮想アプライアンスを単にアップグレードすることはできません。

代わりに、このリリース用に新しい仮想マシンインスタンスを導入する必要があります。

仮想アプライアンスをアップグレードしても、既存のライセンスは変更されません。

ハードウェアアプライアンスから仮想アプライアンスへの移行

ステップ 1 仮想アプライアンスの展開またはアップグレード (6 ページ)で説明されているマニュアルを使用して、この AsyncOS リリースで仮想アプライアンスをセットアップします。

ステップ 2 ハードウェアアプライアンスをこの AsyncOS リリースにアップグレードします。

ステップ 3 アップグレードされたハードウェアアプライアンスから設定ファイルを保存します。

ステップ 4 ハードウェアアプライアンスから仮想アプライアンスに設定ファイルをロードします。

ネットワーク設定に関連する適切なオプションを選択してください。

仮想アプライアンスのテクニカル サポートの取得

仮想アプライアンスのテクニカル サポートを受けるための要件は、http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-installation-guides-list.html にある『Cisco コンテンツセキュリティ仮想アプライアンス インストール ガイド』に記載されています。

以下のサービスとサポート (14 ページ) も参照してください。

仮想アプライアンスからの Cisco Registered Envelope Service 管理者のプロビジョニングとアクティブ化

仮想アプライアンスのプロビジョニングに必要な情報については、Cisco TAC にお問い合わせください。

アップグレード前の注意事項

アップグレードする前に、次の事項を確認してください。

Cisco Talos サービスにアクセスするためのファイアウォール設定

電子メールゲートウェイを Cisco Talos サービスに接続するには、次のホスト名または IP アドレス用にファイアウォール上で HTTPS (Out) 443 ポートを開く必要があります (以下の表を参照)。

(注) HTTPS アップデータプロキシ設定は、Cisco Talos サービスへの接続に使用されます。

ホスト名	IPv4	IPv6
grpc.talos.cisco.com	146.112.62.0/24	2a04:e4c7:ffff::/48
email-sender-ip-rep-grpc.talos.cisco.com	146.112.63.0/24	2a04:e4c7:fffe::/48
serviceconfig.talos.cisco.com	146.112.255.0/24	-
	146.112.59.0/24	-

詳細については、ユーザーガイドの「Firewall」の章を参照してください。

Cisco Advanced Phishing Protection クラウドサービスにアクセスするためのファイアウォールの設定

電子メールゲートウェイを Cisco Advanced Phishing Protection クラウドサービスに接続するには、次のホスト名用にファイアウォール上で HTTPS（Out）443 ポートを開く必要があります。

- kinesis.us-west-2.amazonaws.com
- sensor-provisioner.ep.prod.agari.com
- houston.sensor.prod.agari.com

詳細については、ユーザーガイドの「Firewall」の章を参照してください。

アプライアンスでのサービスログの有効化

サービスログは、Cisco E メール セキュリティ アプライアンス データ シートに基づいて個人データを収集するために使用されます。

サービスログは、フィッシング検出を改善するために Cisco Talos クラウドサービスに送信されます。

Cisco E メール セキュリティ ゲートウェイは、顧客の電子メールから限定された個人データを収集し、幅広く有用な脅威検出機能を提供します。この機能は、検出された脅威アクティビティを収集し、傾向を提示し、関連付けるための専用分析システムと組み合わせることができます。シスコでは、個人データを使用して、脅威の状況を分析し、悪意のある電子メールに脅威の分類ソリューションを提供し、スパム、ウイルス、ディレクトリ獲得攻撃などの新しい脅威から電子メールゲートウェイを保護するために、電子メールゲートウェイの機能を向上させています。

アップグレードプロセス中に、次のいずれかからアプライアンスのサービスログを有効にする方法を選択できます。

- Web インターフェイスの [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] ページで、[サービスログ（Service Logs）] に [同意する（I Agree）] オプションを選択します。
- upgrade CLI コマンドの「*サービスログをデフォルトで有効にして続行しますか？[Y]（Do you agree to proceed with Service Logs being enabled by default? [y]）*」に「**Yes**」と入力します。

詳細については、ユーザーガイドの「Improving Phishing Detection Efficacy using Service Logs」の章を参照してください。

クラスタレベルでのインテリジェント マルチスキャンとグレイメール設定のアップグレード

AsyncOS 13.7 にアップグレードする前に、インテリジェント マルチスキャンとグレイメールの設定が同じクラスタレベルに存在していることを確認します。クラスタレベルが異なっている場合は、アップグレード後にインテリジェント マルチスキャンとグレイメールの設定を確認する必要があります。

FIPS の準拠性

AsyncOS 13.7 リリースは、FIPS 準拠のリリースではありません。アプライアンスで FIPS モードを有効にしている場合は AsyncOS 13.7 にアップグレードする前に FIPS モードを無効にする必要があります。

AsyncOS の以前のバージョンへの復元

次の AsyncOS バージョンは、内部テストインターフェイスの脆弱性（http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa）の影響を受けます。

- 9.1.2-023
- 9.1.2-028
- 9.1.2-036
- 9.7.2-046
- 9.7.2-047
- 9.7-2-054
- 10.0.0-124
- 10.0.0-125

集中管理（クラスタ化されたアプライアンス）を使用した展開のアップグレード

クラスタに C160、C360、C660、X1060、C170、C370、C670、C380、C680、または X1070 ハードウェアアプライアンスが含まれている場合は、アップグレードの前に、これらのアプライアンスをクラスタから削除してください。

クラスタ内のすべてのマシンが同じバージョンの AsyncOS を実行している必要があり、x60、x70、および x80 ハードウェアをこのリリースにアップグレードすることはできません。必要に応じて、x60、x70、および x80 アプライアンス用に別のクラスタを作成してください。

直前のリリース以外のリリースからのアップグレード

このリリースの直前のリリース以外のメジャー（AsyncOS X.0）またはマイナー（AsyncOS X.x）リリースからアップグレードする場合は、現在のリリースとこのリリースの間にあるメジャー リリースとマイナー リリースのリリース ノートを確認する必要があります。

メンテナンス リリース（AsyncOS X.x.x）には、バグ修正のみが含まれています。

設定ファイル

通常、シスコは、以前のメジャーリリースに関して、設定ファイルの下位互換性をサポートしていません。マイナーリリースのサポートが提供されています。以前のバージョンの設定ファイルは以降のリリースで動作する可能性がありますが、ロードするために変更が必要になる場合があります。設定ファイルのサポートについて不明な点がある場合は、シスコカスタマーサポートでご確認ください。

アップグレード中の IPMI メッセージ

CLI を使用してアプライアンスをアップグレードする場合、IPMI に関連するメッセージが表示されることがあります。これらのメッセージは無視しても差し支えありません。これは既知の問題です。

障害 ID：CSCuz28415

このリリースへのアップグレード

はじめる前に

- ワークキュー内のすべてのメッセージをクリアします。ワークキューをクリアせずにアップグレードを実行することはできません。
- Known Issues（8 ページ）とインストールおよびアップグレードに関する注意事項（5 ページ）を確認してください。
- 仮想アプライアンスをアップグレードする場合は、仮想アプライアンスのアップグレード（6 ページ）を参照してください。

手順

E メール セキュリティ アプライアンスをアップグレードするには、次の手順を実行します。

ステップ 1 アプライアンスから、XML 設定ファイルを保存します。

ステップ 2 セーフリスト/ブロックリスト機能を使用している場合は、アプライアンスからセーフリスト/ブロックリストデータベースをエクスポートします。

ステップ 3 すべてのリスナーを一時停止します。

ステップ 4 ワークキューが空になるまで待ちます。

ステップ 5 [システム管理（System Administration）] タブで、[システムアップグレード（System Upgrade）] ページを選択します。

ステップ 6 [利用可能なアップグレード（Available Upgrades）] ボタンをクリックします。ページが更新され、使用可能な AsyncOS アップグレード バージョンのリストが表示されます。

ステップ 7 [アップグレードの開始（Begin Upgrade）] ボタンをクリックすると、アップグレードが開始されます。表示される質問に答えます。

ステップ 8 アップグレードが完了したら、[今すぐリブート（Reboot Now）] ボタンをクリックしてアプライアンスを再起動します。

ステップ 9 すべてのリスナーを再開します。

次の作業

- アップグレード後、SSL の設定を確認し、使用する正しい GUI HTTPS、インバウンド SMTP、およびアウトバウンド SMTP 方式が選択されていることを確認します。[システム管理（System Administration）] > [SSL 構成（SSL Configuration）] ページを使用するか、CLI で `sslconfig` コマンドを使用します。手順については、ユーザーガイドまたはオンラインヘルプの「System Administration」の章を参照してください。
- 「パフォーマンスアドバイザリ（11 ページ）」を確認してください。
- SSH キーを変更した場合は、アップグレード後に Cisco E メールセキュリティアプライアンスと Cisco セキュリティ管理アプライアンス間の接続を再認証します。

アップグレード後の注意事項

- AsyncOS 13.x へのアップグレード後のクラスタレベルでの DLP 設定の不整合（11 ページ）
- インテリジェント マルチスキャンおよびグレイメールのグローバル設定の変更（11 ページ）

AsyncOS 13.x へのアップグレード後のクラスタレベルでの DLP 設定の不整合

AsyncOS 13.x にアップグレードした後、アプライアンスがクラスタモードになっていて、DLP が設定されている場合、CLI を使用して clustercheck コマンドを実行すると、DLP 設定の不整合が表示されます。

この不整合を解決するには、クラスタ全体でクラスタ内の他のいずれかのマシンの DLP 設定を使用するように強制します。次の例に示すように、clustercheck コマンドで「この不整合をどのように解決しますか？(How do you want to resolve this inconsistency?)」というプロンプトを使用します。

```
(Cluster)> clustercheck
Checking DLP settings...
Inconsistency found!
DLP settings at Cluster test:
mail1.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
mail2.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
How do you want to resolve this inconsistency?
1. Force the entire cluster to use the mail1.example.com version.
2. Force the entire cluster to use the mail2.example.com version.
3. Ignore.
[3]>
```

インテリジェント マルチスキャンおよびグレイメールのグローバル設定の変更

AsyncOS 13.7 にアップグレードした後のインテリジェント マルチスキャン(IMS)およびグレイメールのグローバル設定の変更点は次のとおりです。

- IMS およびグレイメールのグローバル設定が異なるクラスタ レベルで設定されている場合、アプライアンスはグローバル設定を最も低い設定レベルにコピーします。たとえば、クラスタ レベルで IMS を設定し、マシン レベルでグレイメールを設定すると、アプライアンスは IMS グローバル設定をマシン レベルにコピーします。
- スキャンメッセージの最大メッセージサイズとタイムアウト値が異なる場合、アプライアンスは [最大タイムアウト(maximum timeout)] および [最大メッセージ(maximum message size)] の値を使用して、IMS およびグレイメールのグローバル設定を行います。たとえば、IMS およびグレイメールの最大メッセージサイズの値がそれぞれ 1M と 2M である場合、アプライアンスは IMS とグレイメールの両方の最大メッセージサイズ値として 2M を使用します。

パフォーマンスアドバイザリ

アウトブレイクフィルタ

アウトブレイクフィルタは、コンテキスト適応スキャンエンジンを使用してメッセージの脅威レベルを判定し、アダプティブルールとアウトブレイクルールの組み合わせに基づいてメッセージにスコアを付けます。一部の設定では、中程度のパフォーマンス低下が発生する可能性があります。

IronPort スパム隔離

C シリーズのアプライアンスに対して IronPort スパム隔離オンボックスを有効にすると、公称水準の負荷がかかっているアプライアンスでは、システムスループットにわずかな低下が生じます。ピークスループット付近またはピークスループットで実行されているアプライアンスの場合、アクティブな隔離からの追加の負荷によって、スループットが 10 ～ 20% 低下する可能性があります。システムのキャパシティがいっぱいか、いっぱいに近いときに IronPort スパム隔離を使用する場合は、規模が大きい C シリーズ アプライアンスまたは M シリーズ アプライアンスへの移行を検討してください。

スパム対策ポリシーをスパムのドロップから隔離に変更する場合（オンボックスまたはオフボックス）、ウイルスおよびコンテンツセキュリティのために追加のスパムメッセージをスキャンする必要があるため、システムの負荷が増大します。インストールのサイジングを適切に行う際にサポートが必要な場合は、認定サポートプロバイダーにお問い合わせください。

既知および修正済みの問題

シスコのバグ検索ツールを使用して、このリリースの既知および修正済みの不具合に関する情報を検索します。

- バグ検索ツールの要件（12 ページ）
- 既知および修正済みの問題のリスト（12 ページ）
- 既知および解決済みの問題に関する情報の検索（12 ページ）

バグ検索ツールの要件

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

既知および修正済みの問題のリスト

既知の問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=13.7.0&prdNam=Cisco%20Secure%20Email%20Gateway
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=13.7.0-093&prdNam=Cisco%20Secure%20Email%20Gateway

既知および解決済みの問題に関する情報の検索

シスコのバグ検索ツールを使用して、既知および解決済みの不具合に関する最新情報を検索します。

はじめる前に

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

手順

ステップ 1 https://tools.cisco.com/bugsearch/ に移動します。

ステップ 2 シスコ アカウントのクレデンシャルでログインします。

ステップ 3 [リストから選択(Select from list)] > [セキュリティ(Security)] > [E メールセキュリティ(Email Security)] > [Cisco E メールセキュリティアプライアンス(Cisco Email Security Appliance)] の順にクリックし、[OK] をクリックします。

ステップ 4 [リリース(Release)] フィールドに、リリースのバージョン(たとえば、13.7)を入力します。

ステップ 5 要件に応じて、次のいずれかを実行します。

- 解決済みの問題のリストを表示するには、[バグの表示(Show Bugs)] ドロップダウンから、[これらのリリースで修正済み(Fixed in these Releases)] を選択します。
- 既知の問題のリストを表示するには、[バグの表示(Show Bugs)] ドロップダウンから [これらのリリースに影響(Affecting these Releases)] を選択し、[ステータス(Status)] ドロップダウンから [開く(Open)] を選択します。

ご不明な点がある場合は、ツールの右上にある [ヘルプ(Help)] または [フィードバック(Feedback)] リンクをクリックしてください。また、インタラクティブなツアーもあります。これを表示するには、[検索(search)] フィールドの上のオレンジ色のバーにあるリンクをクリックします。

関連資料

マニュアルの内容 (Cisco Content Security 製品)	参照先
ハードウェアおよび仮想アプライアンス	この表で該当する製品を参照してください。
Cisco Secure Email and Web Manager	http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Secure Web Appliance	http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email ゲートウェイ	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco コンテンツ セキュリティ アプライアンス用 CLI リファレンス ガイド	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html
Cisco Secure Email Encryption Service	http://www.cisco.com/c/ja_jp/support/security/email-encryption/tsd-products-support-series-home.html

サービスとサポート

（注） 仮想アプライアンスのサポートを受けるには、仮想ライセンス番号（VLN）をご用意の上 Cisco TAC に連絡してください。

Cisco TAC：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

従来の IronPort のサポートサイト：http://www.cisco.com/web/services/acquisitions/ironport.html

重大ではない問題の場合は、アプライアンスからカスタマー サポートにアクセスすることもできます。手順については、ユーザーガイドまたはオンラインヘルプを参照してください。