Cisco Identity Services Engine リリース 2.6 リリースノート

初版：2019 年 2 月 18 日

最終更新：2020 年 6 月 16 日

（注） content.cisco.com のコンテンツハブに移動します。ここでは、ファセット検索機能を使用して、必要なコンテンツを正確に拡大できます。参照用にカスタマイズした PDF ブックを簡単に作成するなど、数多くのことが可能です。

早速始めましょう。content.cisco.com をクリックしてください。

また、コンテンツハブをすでに体験したことがある場合は、ご意見をお聞かせください。

ページの[フィードバック（Feedback）]アイコンをクリックして、ご意見をお寄せください。

はじめに

Cisco Identity Services Engine（ISE）は、ネットワークリソースへのセキュアなアクセスを提供するセキュリティポリシー管理プラットフォームです。企業は、Cisco ISE を使用して、ネットワーク、ユーザ、およびデバイスからコンテキスト情報をリアルタイムで収集できます。その後、管理者はこの情報を使用して、積極的に管理上の決定を下すことができます。これを行うには、アクセススイッチ、シスコ ワイヤレス コントローラ、バーチャル プライベート ネットワーク（VPN）ゲートウェイ、データセンタースイッチなどのさまざまなネットワーク要素のアクセス コントロール ポリシーを作成します。Cisco ISE は、Cisco TrustSec ソリューションのポリシーマネージャとして機能し、TrustSec ソフトウェアによって定義されたセグメンテーションをサポートします。

Cisco ISE は、異なるパフォーマンス特性を持つセキュアなネットワーク サーバ アプライアンス上で、および仮想マシン（VM）で実行可能なソフトウェアとして使用できます。パフォーマンス向上のためにアプライアンスを展開に追加できます。

Cisco ISE は、スタンドアロンおよび分散展開をサポートする拡張性の高いアーキテクチャを使用しますが、設定および管理は一元化されています。また、ペルソナとサービスの設定と管理を個別に行うこともできます。このため、ネットワーク内で必要なサービスを作成して適用することができますが、Cisco ISE 展開を完全な統合システムとして運用することもできます。

この Cisco ISE リリースでサポートされている機能の詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

cisco.com のマニュアルにアクセスするには、End-User Documentation [英語] にアクセスしてください。

システム要件

Cisco ISE の設定を継続使用する場合は、次のシステム要件が満たされていることを確認してください。

この Cisco ISE リリースのハードウェア プラットフォームおよびインストールの詳細については、『Cisco Identity Services Engine Hardware Installation Guide』を参照してください。

サポート対象ハードウェア

Cisco ISE リリース 2.6 は、次のプラットフォームにインストールして実行できます。

⚠

注意 Cisco Secure Network Server（SNS）3600 シリーズ アプライアンス サポート（SNS-3615-K9、SNS-3655-K9、SNS-3695-K9）の場合は、新しい ISO ファイル（ise-2.4.0.357.SPA.x86_64_SNS-36x5_APPLIANCE_ONLY.iso）のみを使用する必要があります。Cisco ISE 2.4 パッチ 9 以降はインストール後に適用する必要があります。SNS 3500 シリーズ アプライアンス、VMware、KVM、または Hyper-V のインストールでは、この ISO ファイルを使用しないことをお勧めします。

表 *1:* サポートされるプラットフォーム

ハードウェア プラットフォーム	設定
Cisco SNS-3515-K9（小規模）	アプライアンスハードウェアの仕様については、Cisco Secure Network Server アプライアンスハードウェアの設置ガイド [英語] を参照してください。
Cisco SNS-3595-K9（大規模）	
Cisco SNS-3615-K9（小規模）	
Cisco SNS-3655-K9（中規模）	
Cisco SNS-3695-K9（大規模）	

ハードウェア プラットフォーム	設定
Cisco ISE-VM-K9（VMware、Linux KVM、Microsoft Hyper-V） ESXi 5.x、6.x、7.x	• CPU とメモリの推奨事項については、『*Cisco Identity Services Engine Installation Guide*』の「VMware Appliance Sizing Recommendations」の項を参照してください。 • ハードディスクのサイズに関する推奨事項については、『*Cisco Identity Services Engine Installation Guide*』の「Disk Space Requirements」の項を参照してください。 • NIC—1-GB NIC インターフェイスが必要です。最大 6 つの NIC をインストールできます。

インストール後、上記の表に記載されているプラットフォームで、管理、モニタリング、pxGrid などの特定のコンポーネントペルソナを使用して Cisco ISE を設定できます。これらのペルソナに加えて、Cisco ISE では、プロファイリングサービス、セッションサービス、脅威中心型 NAC サービス、TrustSec 用の SXP サービス、TACACS+ デバイス管理サービス、およびパッシブ ID サービスなど、ポリシーサービス内に他のタイプのペルソナが含まれています。

⚠

注意

- Cisco Secured Network Server（SNS）3400 シリーズアプライアンスは、Cisco ISE リリース 2.4 以降ではサポートされていません。
- 16 GB 未満のメモリの割り当ては、VM アプライアンスの設定ではサポートされていません。Cisco ISE の動作に問題が発生した場合、すべてのユーザは、Cisco Technical Assistance Center に連絡する前に割り当てメモリを 16 GB 以上に変更する必要があります。
- レガシー アクセス コントロール サーバ（ACS）およびネットワーク アクセス コントロール（NAC）アプライアンス（Cisco ISE 3300 シリーズを含む）は、Cisco ISE リリース 2.0 以降ではサポートされていません。

連邦情報処理標準モードサポート

Cisco ISE は、組み込みの連邦情報処理標準（FIPS）140-2 検証済み暗号化モジュール、Cisco FIPS オブジェクト モジュール バージョン 6.2（証明書 #2984）を使用します。FIPS コンプライアンス要求の詳細については、Global Government Certifications を参照してください。

Cisco ISE で FIPS モードが有効になっている場合は、次の点を考慮してください。

- すべての FIPS 非準拠暗号スイートは無効になります。
- 証明書と秘密キーには、FIPS 準拠ハッシュと暗号化アルゴリズムのみを使用する必要があります。
- RSA 秘密キーには、2048 ビット以上を指定する必要があります。

- 楕円曲線デジタル署名アルゴリズム（楕円曲線DSA）の秘密キーには、224ビット以上を指定する必要があります。
- Diffie–Hellman Ephemeral（DHE）暗号方式は2048ビット以上のDiffie–Hellman（DH）パラメータを使用して動作します。
- SHA1は、ISEローカルサーバ証明書の生成を許可されていません。
- EAP-FASTの匿名PACプロビジョニングオプションは無効です。
- ローカルSSHサーバはFIPSモードで動作します。
- RADIUSの場合、次のプロトコルはFIPSモードではサポートされていません。
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

サポートされる仮想環境

Cisco ISEは次の仮想環境プラットフォームをサポートしています。

- ESXi 5.x、6.x、7.x
  - Cisco ISEは、ESXi 6.5を搭載したCisco HyperFlex HXシリーズで検証済みです。
  - 仮想マシンはVMwareクラウドが提供するソフトウェア定義型データセンター（SDDC）でホストできます。VMwareクラウドにCisco ISEをインストールするプロセスは、VMware仮想マシンにCisco ISEをインストールするプロセスとまったく同じです。オンプレミス展開へのアクセスを可能にするために、セキュリティグループポリシーがVMwareクラウドで設定されていることを確認します（[ネットワーキングとセキュリティ（Networking & Security）] > [セキュリティ（Security）] > [ゲートウェイ ファイアウォール（Gateway Firewall）]）。
- Microsoft Windows Server 2012 R2以降のMicrosoft Hyper-V
- RHEL 7.1、7.3、および7.5上のKVM

詳細については、Cisco Identity Services Engine互換性ガイド [英語] を参照してください。

注意 Cisco ISE は、ISE データのバックアップ用の VMware スナップショットをサポートしていません。これは、VMware スナップショットが特定の時点で VM のステータスを保存するためです。マルチノード Cisco ISE 環境では、すべてのノードのデータは、現在のデータベース情報と継続的に同期されます。スナップショットを復元すると、データベースのレプリケーションと同期の問題を引き起こす可能性があります。データのバックアップおよび復元用に、Cisco ISE に含まれるバックアップ機能を使用することを推奨します。

VMware スナップショットを使用して ISE データをバックアップすると、Cisco ISE サービスが停止します。ISE ノードを起動するには、再起動が必要です。

サポートされるブラウザ

管理者ポータルでサポートされているブラウザは次のとおりです。

- Mozilla Firefox 96 以前のバージョン（バージョン 82 以降）
- Mozilla Firefox ESR 91.3 以前のバージョン
- Google Chrome 96 以前のバージョン （バージョン 86 以降）
- Microsoft Internet Explorer 11.x
- Microsoft Edge の最新バージョンと最新バージョンより 1 つ前のバージョン

Microsoft Active Directory のサポート

Cisco ISE は、すべての機能レベルで Microsoft Active Directory サーバ 2003、2003 R2、2008、2008 R2、2012、 2012 R2、2016、および 2019 と連携して動作します。

（注）
- Windows サーバをサポート対象バージョンにアップグレードすることをお勧めします。Microsoft は Windows サーバ 2003 および 2003 R2 のサポートを終了しています。
- Microsoft Active Directory バージョン 2000 またはその機能レベルは、Cisco ISE ではサポートされていません。

Cisco ISE は、マルチドメインフォレストと Active Directory インフラストラクチャとの統合をサポートし、大規模なエンタープライズネットワーク全体の認証および属性の収集をサポートしています。Cisco ISE は最大 50 個のドメイン参加ポイントをサポートしています。

ユーザ識別の改善

Cisco ISE は、ユーザ名が一意でなくても Active Directory ユーザを識別できます。マルチドメインの Active Directory 環境で短いユーザ名を使用する場合、一般的にユーザ名が重複します。ソフトウェア資産管理（SAM）、顧客名（CN）、またはその両方を使用してユーザを識別できます。Cisco ISE は、ユーザを一意に識別するために属性を使用します。

次の値を更新します。

- SAM：クエリで SAM のみを使用するには、この値を更新します（デフォルト）。
- CN：クエリで CN のみを使用するには、この値を更新します。
- CNSAM：クエリで CN および SAM を使用するには、この値を更新します。

Active Directory ユーザの識別用に上記の属性を設定するには、Active Directory を実行しているサーバのレジストリで **IdentityLookupField** パラメータを更新します。

```
REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField
```

サポート対象のウイルス対策およびマルウェア対策製品

ISE ポスチャエージェントでサポートされているウイルス対策およびマルウェア対策製品の詳細については、Cisco Identity Services Engine 互換性ガイド [英語] の Cisco AnyConnect ISE ポスチャのサポート表を参照してください。

サポート対象の暗号方式

Cisco ISE のクリーンインストールまたは新規インストールでは、SHA1 暗号はデフォルトで無効になっています。ただし、既存のバージョンの Cisco ISE からアップグレードする場合、SHA1 暗号は以前のバージョンのオプションのままです。SHA1 暗号の設定は、[SHA1暗号を許可する（Allow SHA1 Ciphers）] フィールド（[管理（Administration）]>[システム（System）]>[設定（Settings）]>[セキュリティ設定（Security Settings）]）を使用して表示および変更できます。

（注） この暗号は、管理者ポータルには適用されません。連邦情報処理標準モード（FIPS）で実行している場合、アップグレードでは管理者ポータルから SHA1 暗号が削除されません。

Cisco ISE は、TLS バージョン 1.0、1.1、および 1.2 をサポートします。

Cisco ISE は、RSA および ECDSA サーバ証明書をサポートしています。次の楕円曲線をサポートしています。

- secp256r1
- secp384r1
- secp521r1

次の表に、サポートされている暗号スイートが表示されています。

暗号スイート	**Cisco ISE** が **EAP** サーバとして設定されている場合 **Cisco ISE** が **RADIUS DTLS** サーバとして設定されている場合	**Cisco ISE** が、**HTTPS** またはセキュア **LDAP** サーバから **CRL** をダウンロードする場合 **Cisco ISE** がセキュアな **LDAP** クライアントとして設定されている場合 **Cisco ISE** が **CoA** の **RADIUS DTLS** クライアントとして設定されている場合
TLS 1.0 のサポート	TLS 1.0 が許可されている場合 （DTLS サーバは DTLS 1.2 のみをサポート） Cisco ISE 2.3 以上では、[TLS 1.0 を許可（Allow TLS 1.0）] オプションがデフォルトで無効になっています。このオプションが無効の場合、TLS 1.0 では、TLS ベースの EAP 認証方式（EAP-TLS、EAP-FAST/TLS）および 802.1 X サプリカントがサポートされません。TLS ベースの EAP 認証方式を TLS 1.0 で使用するには、[セキュリティ設定（Security Settings）] ウィンドウの [TLS 1.0 を許可（Allow TLS 1.0）] チェックボックスをオンにします。このウィンドウを表示するには、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [セキュリティ設定（Security Settings）] を選択します。	TLS 1.0 が許可されている場合 （DTLS クライアントは DTLS 1.2 のみをサポート）

TLS 1.1 のサポート	TLS 1.1 が許可されている場合 Cisco ISE 2.3 以上では、[TLS 1.1 を許可（Allow TLS 1.0）] オプションがデフォルトで無効になっています。このオプションが無効の場合、TLS 1.1 では、TLS ベースの EAP 認証方式（EAP-TLS、EAP-FAST/TLS）および 802.1 X サプリカントがサポートされません。TLS ベースの EAP 認証方式を TLS 1.1 で使用するには、[セキュリティ設定（Security Settings）] ウィンドウ（[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [セキュリティ設定（Security Settings）]）で [TLS 1.1を許可（Allow TLS 1.1）] チェック ボックスをオンにします。	TLS 1.1 が許可されている場合
ECC DSA 暗号方式		
ECDHE-ECDSA-AES256-GCM-SHA384	Yes	○
ECDHE-ECDSA-AES128-GCM-SHA256	Yes	○
ECDHE-ECDSA-AES256-SHA384	Yes	○
ECDHE-ECDSA-AES128-SHA256	Yes	○
ECDHE-ECDSA-AES256-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
ECDHE-ECDSA-AES128-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
ECC RSA 暗号方式		
ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES256-SHA384	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合

ECDHE-RSA-AES128-SHA256	ECDHE-RSA が許可されている場合	ECDHE-RSA が許可されている場合
ECDHE-RSA-AES256-SHA	ECDHE-RSA/SHA-1 が許可されている場合	ECDHE-RSA/SHA-1 が許可されている場合
ECDHE-RSA-AES128-SHA	ECDHE-RSA/SHA-1 が許可されている場合	ECDHE-RSA/SHA-1 が許可されている場合
DHE RSA 暗号方式		
DHE-RSA-AES256-SHA256	×	可
DHE-RSA-AES128-SHA256	×	可
DHE-RSA-AES256-SHA	×	SHA-1 が許可されている場合
DHE-RSA-AES128-SHA	×	SHA-1 が許可されている場合
RSA 暗号方式		
AES256-SHA256	Yes	○
AES128-SHA256	Yes	○
AES256-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
AES128-SHA	SHA-1 が許可されている場合	SHA-1 が許可されている場合
3DES 暗号方式		
DES-CBC3-SHA	3DES/SHA-1 が許可されている場合	3DES/DSS および SHA-1 が有効になっている場合
DSS 暗号方式		
DHE-DSS-AES256-SHA	×	3DES/DSS および SHA-1 が有効になっている場合
DHE-DSS-AES128-SHA	×	3DES/DSS および SHA-1 が有効になっている場合
EDH-DSS-DES-CBC3-SHA	×	3DES/DSS および SHA-1 が有効になっている場合
弱い RC4 暗号方式		

RC4-SHA	[許可されているプロトコル（Allowed Protocols）] ページで [脆弱な暗号を許可（Allow weak ciphers）] オプションが有効になっていて、SHA-1 が許可されている場合	×
RC4-MD5	[許可されているプロトコル（Allowed Protocols）] ページで [脆弱な暗号を許可（Allow weak ciphers）] オプションが有効になっている場合	×
EAP-FAST 匿名プロビジョニングのみの場合： ADH-AES-128-SHA	Yes	×
ピア証明書の制限		
KeyUsage の検証	クライアント証明書では、以下の暗号に対し、KeyUsage=Key Agreement および ExtendedKeyUsage=Client Authentication が必要です。 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-ECDSA-AES256-SHA384	

ExtendedKeyUsage の検証	クライアント証明書では、以下の暗号に対し、KeyUsage=Key Encipherment および ExtendedKeyUsage=Client Authentication が必要です。 • AES256-SHA256 • AES128-SHA256 • AES256-SHA • AES128-SHA • DHE-RSA-AES128-SHA • DHE-RSA-AES256-SHA • DHE-RSA-AES128-SHA256 • DHE-RSA-AES256-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES128-SHA256 • ECDHE-RSA-AES256-SHA • ECDHE-RSA-AES128-SHA • EDH-RSA-DES-CBC3-SHA • DES-CBC3-SHA • RC4-SHA • RC4-MD5	サーバ証明書では ExtendedKeyUsage=Server Authentication が必要です

Cisco ISE リリース 2.6 の新機能

基本ライセンス

以下に示す機能を使用するには、Cisco ISE 基本ライセンスが必要です。

外部 ID ストアによる CLI アクセス

ISE は、Active Directory などの外部 ID ソースによる CLI 管理者の認証をサポートしています。

ビジネス成果：複数のパスワードポリシーを管理したり、ISE 内で内部ユーザを管理したりする必要なしに、パスワードの単一ソースを管理できるため、時間の節約と労力の軽減を実現できます。

IPv6 のサポート

Cisco ISE リリース 2.6 では、IPv4 のサポートに加えて、次の機能や項目に対して IPv6 のサポートが拡張されています。

- ISE 管理

IPv6 アドレスを介して Cisco ISE ノードにアクセスして管理し、セットアップウィザードおよび CLI で IPv6 アドレスを Eth0（インターフェイス）に設定できます。

（注） IPv6 アドレスを設定する場合は、Cisco ISE ノード通信用に（IPv6 アドレスに加えて）IPv4 アドレスも設定する必要があります。したがって、デュアルスタック（IPv4 と IPv6 の両方の組み合わせ）が必要です。

また、IPv6 アドレスを使用してセキュアソケットシェル（SSH）を管理することもできます。Cisco ISE では、任意のインターフェイス上で複数の IPv6 アドレスを利用でき、CLI を使用してこれらの IPv6 アドレスを設定および管理できます。

- Network Time Protocol のサポート

  IPv4、FQDN、IPv6 アドレス、またはこれらの組み合わせを使用して、Network Time Protocol（NTP）サーバにアクセスし、設定および管理できます。

  また、Cisco ISE は、IPv6 アドレスを介した NTP サーバのフォールバックメカニズムおよびサーバ認証もサポートしています。

- ドメインネームシステムのサポート

  IPv4 と IPv6 のドメインネームシステム（DNS）サーバを組み合わせて設定し、CLI および GUI を使用して IPv4 ベースまたは IPv6 ベースの DNS サーバを管理することもできます。スタティックホスト名を IPv6 アドレスにマッピングできます。

  詳細については、『ISE Cisco Identity Services Engine CLI Reference Guide, Release 2.6』を参照してください。

- 外部リポジトリ

  IPv6 アドレスを使用して、Cisco ISE に外部リポジトリを追加できます。Cisco ISE ノードの IPv6 アドレスが Eth0 に設定されている場合は、ノードと IPv6 外部リポジトリとの間で通信できます。

  詳細については、『ISE Cisco Identity Services Engine CLI Reference Guide, Release 2.6』を参照してください。

- 監査ログとレポート

  IPv6 アドレスを使用して Cisco ISE にアクセスしながら、ユーザによるログインとログアウトのアクティビティ、パスワードの変更、操作上の変更に関するレポートを表示できます。これらのイベントは、Cisco ISE ダッシュボードで使用可能な監査レポートで確認できます。

- Simple Network Management Protocol

  Simple Network Management Protocol（SNMP）トラップと MIB は IPv6 アドレスを介して通信できます。IPv4 ベースの SNMP サーバ、IPv6 ベースの SNMP サーバ、または複数の SNMP サーバ（IPv4 と IPv6 の組み合わせ）を設定できます。

- アクセスコントロールリストと動的アクセスコントロールリスト

  Cisco ISE リリース 2.6 以降では、IPv6 アドレスを使用してアクセスコントロールリスト（ACL）、動的アクセスコントロールリスト（DACL）、Cisco Airespace ACL を定義できます。

- Active Directory

  Cisco ISE から IPv6 Active Directory に接続できます。

- 外部 Restful サービスポータル

  IPv6 クライアントでは外部 Restful サービスを使用できます。

- syslog クライアントまたはロギングターゲット

  IPv6 ベースの syslog ターゲットを設定できます。

- ポスチャ

  IPv6 アドレスを使用して RADIUS サーバにアクセスできます。

Cisco ISE リリース 2.6 での IPv6 のサポートに関する詳細については、『Cisco Identity Services Engine Administrator Guide, Release 2.6』を参照してください。

ビジネス成果：IPv6 ベースのネットワークに移行すると、上記の項目を達成できます。

管理者ポータルの日本語表示または英語表示

管理コンソールは、現在、日本語と英語の 2 つの言語に対応しています。[アカウント設定（Account Settings）] で、日本語表示または英語表示を選択できます。

ビジネス成果：日本語または英語がわかる管理者は Cisco ISE を適切に設定および使用できます。

ポリシーサービスノードとライト セッション ディレクトリ

ライト セッション ディレクトリ機能を使用すると、ユーザセッション情報を保存し、展開のポリシーサービスノード（PSN）全体で複製できるため、ユーザセッションの詳細について、プライマリ管理ノード（PAN）またはモニタリングとトラブルシューティング（MnT）ノードから完全に独立できます。ライト セッション ディレクトリ機能では、認可変更（CoA）に必要なセッション属性のみが保存されます。ライト セッション ディレクトリ機能を有効にするには、[管理（Administration）] > [設定（Settings）] > [ライトセッションディレクトリ（Light Session Directory）] を選択し、[ライトセッションディレクトリの有効化（Enable Light Session Directory）] チェックボックスをオンにします。

ビジネス成果：Cisco ISE ノードのパフォーマンスと拡張性が向上しました。

外部管理者向けの REST のサポート

Cisco ISE 2.6 から、外部 RESTful サービス（ERS）ユーザは、内部ユーザとなることも、外部 Active Directory に属することもできます。外部ユーザが所属する Active Directory グループは、ERS 管理者または ERS オペレータのいずれかのグループにマッピングする必要があります。

この機能強化により、管理者は、ERS サービスにアクセスする必要がある外部ユーザに対応する内部ユーザを作成する必要がなくなりました。

ビジネス成果：外部管理者による RESTful サービスへのアクセスを可能にするプロセスが簡素化されます。

Manufacturer Usage Descriptor のサポート

製造元使用率記述子（MUD）は IETF 標準で、オンボード IoT デバイスに対する方法を定義します。IoT デバイスのシームレスな可視化とセグメンテーションの自動化を提供します。MUD は IETF プロセスで承認されており、RFC8520 としてリリースされています。

https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/.

Cisco ISE リリース 2.6 では、IoT デバイスの識別がサポートされています。Cisco ISE は、プロファイリングポリシーとエンドポイント ID グループを自動的に作成します。MUD は、IoT デバイスのプロファイリング、プロファイリングポリシーの動的作成、ポリシーとエンドポイント ID グループの作成プロセス全体の自動化をサポートします。管理者はこれらのプロファイリングポリシーを使用して、許可ポリシーおよびプロファイルを手動で作成できます。DHCP と LLDP のパケットで MUD URL を出力する IoT デバイスは、これらのプロファイルとポリシーを使用して登録されています。システム内での適用を含む完全な自動化は、今後のリリースに追加される予定です。

Cisco ISE は IoT デバイスを符号なしで分類し、プロファイラポリシーを使用してアクセスします。ISE は MUD 属性を保存しません。属性は現在のセッションのみで使用されます。[コンテキストと可視性（Context and Visibility）] > [エンドポイント（Endpoints）] ウィンドウの [エンドポイントプロファイル（Endpoint Profile）] フィールドで、IoT デバイスをフィルタリングできます。

次のデバイスは、Cisco ISE への MUD データの送信をサポートしています。

- Cisco Identity Services Engine 2.6
- Cisco IOS XE バージョン 16.9.1 と 16.9.2 を実行している Cisco Catalyst 3850 シリーズ スイッチ
- Cisco IOS バージョン 15.2(6)E2 を実行している Cisco Catalyst デジタル ビルディング シリーズ スイッチ
- Cisco IOS バージョン 15.2(6)E2 を実行している Cisco Industrial Ethernet 4000 シリーズ スイッチ
- MUD 機能が組み込まれた Internet of Things（IoT）デバイス

プロファイラのサポート

Cisco ISE は、次のプロファイリングプロトコルおよびプロファイリングプローブをサポートします。

- LLDP と RADIUS - TLV 127
- DHCP - オプション 161

ビジネス成果：エンタープライズ ネットワークに接続される Internet of Things（IoT）デバイスの数は増え続けています。これまで、Cisco ISE では、これらのデバイスを分類できませんでした。リリース 2.6 から、Cisco ISE では、自動プロセスを使用して、組織のネットワークに接続されている IoT デバイスを分類して表示できます。

ISE メッセージングを介した syslog

Cisco ISE リリース 2.6 から、モニタリングとトラブルシューティング（MnT）WAN 存続可能性を UDP syslog 収集に利用できます。syslog は ISE メッセージングサービスを使用して記録されます。syslog が収集および保存される**リモートロギングターゲット**では、ポート TCP 8671 とセキュアな Advanced Message Queuing Protocol（AMQP）を使用して、syslog を MnT に送信します。

Cisco ISE リリース 2.6 パッチ 1 まで、[ISEメッセージングサービス（ISE Messaging Service）] オプションはデフォルトで無効になっています。

Cisco ISE リリース 2.6 パッチ 2 以降では、[ISEメッセージングサービス（ISE Messaging Service）] オプションはデフォルトで有効になっています。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 2.6』を参照してください。

ビジネス成果：MnT ノードにアクセスできない場合でも、運用データが一定期間保持されます。

強化するための改善

Cisco ISE を強化するための改善として、次の不具合が修正されています。

- CSCvj85532：管理者の認証失敗に対するセキュリティの適用が簡素化されました。
- CSCvk46033：Cisco ISE SSH サーバへの接続のセキュリティを強化するように改善されました。
- CSCvk09565：RFC 3164 標準に準拠しました。
- CSCvj96345：Cisco ISE 管理アプリケーションへの接続のセキュリティが強化されました。

TrustSec 展開の検証レポート

このレポートを使用すると、最新の TrustSec ポリシーがすべてのネットワークデバイスに展開されているかどうか、および Cisco ISE で設定されたポリシーとネットワークデバイスに展開されたポリシーに不一致があるかどうかを確認できます。

ビジネス成果：最新の TrustSec ポリシーがネットワークデバイスに展開されているかどうかや、不一致があるかどうかを簡単に確認できます。

NFS リポジトリのクレデンシャル

リポジトリを追加し、プロトコルとして [NFS] を選択しても、リポジトリ接続用のクレデンシャルを入力できなくなりました。

ビジネス成果：クレデンシャルを使用して NFS リポジトリに接続すると、問題が発生しました。

Apex ライセンス

以下に示す機能を使用するには、Cisco ISE Apex ライセンスが必要です。

ダイナミック MAC アドレスを使用した管理対象デバイスの識別

AnyConnect 4.7 は、接続ユーザを識別するための固有デバイス ID（UDID）を提供するようになりました。UDID 値はモバイル デバイス管理（MDM）プロバイダーからの情報にマッピングできるため、同じ MAC アドレスを持つユーザを識別しやすくなります。MAC アドレス共有は、複数の人がドックまたは USB ドングルを共有しているオープンオフィスでは一般的です。

ビジネス成果：デバイス接続が共有されている場合に UDID を使用してユーザを一意に識別するソリューションを開発できます。

柔軟な修復通知

Cisco ISE リリース 2.6 以降では、猶予期間の一定割合が経過するまで、猶予期間の通知をユーザに表示するのを遅らせることができます。

たとえば、[ポリシー（Policy）]>[ポスチャ（Posture）]>[ポスチャポリシー（Posture Policy）] ウィンドウの [通知の遅延（Delay Notification）] フィールドが 50 パーセントに設定され、設定されている猶予期間が 10 分の場合、Cisco ISE は、5 分後にポスチャステータスをチェックし、エンドポイントが準拠していないと判断したときは猶予期間通知を表示します。エンドポイントのステータスが準拠している場合、猶予期間通知は表示されません。通知遅延期間が 0 パーセントに設定されている場合は、猶予期間の開始時に直ちに問題の解決を促すメッセージが表示されます。ただし、エンドポイントは、猶予期間の有効期限が切れるまで、アクセス権が付与されます。

ビジネス成果：JAMF ソフトウェアや Microsoft System Center Configuration Manager（SCCM）の更新を待っているエンドポイントに対して不必要に修復を求めることを避けられます。

Cisco AnyConnect を介した汎用またはカスタムメッセージング

Cisco AnyConnect は、Cisco ISE ポスチャサービスに関連して使用する場合、より詳しい情報メッセージを表示できるようになりました。エンドユーザはポスチャステータスやエラーに関するメッセージを表示できるようになりました。AnyConnect のポスチャプロファイルに表示される内容は変更できます。この機能を使用するには Cisco AnyConnect バージョン 4.7 が必要であることに注意してください。

ビジネス成果：エンドユーザとの通信が改善します。

プラットフォーム

Cisco Secure Network Server 3600 シリーズ アプライアンスのサポート

Cisco ISE 2.6 は、Cisco Secure Network Server 3615、Secure Network Server 3655、および Secure Network Server 3695 アプライアンスをサポートしています。

Cisco Secure Network Server（SNS）3600 シリーズ アプライアンス サポート（SNS-3615-K9、SNS-3655-K9、SNS-3695-K9）の場合は、新しい ISO ファイル（ise-2.4.0.357.SPA.x86_64_SNS-36x5_APPLIANCE_ONLY.iso）のみを使用する必要があります。Cisco ISE 2.4 パッチ 9 以降はインストール後に適用する必要があります。SNS 3500 シリーズ アプライアンス、VMware、KVM、または Hyper-V のインストールでは、この ISO ファイルを使用しないことをお勧めします。

ビジネス成果：SNS 35xx シリーズ アプライアンスでのパフォーマンス、拡張性、プラットフォームの管理性が向上しました。

既知の制限事項と回避策

アップグレード後の LDAP サーバの再設定

制限事項

プライマリホスト名または IP が更新されないため、認証が失敗します。これは、Cisco ISE 展開のアップグレード中に、展開 ID がリセットされる傾向があるためです。

条件

[接続（Connection）] ウィンドウ（**[管理（Administration）] > [ID 管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [LDAP] > [追加（Add）]**）で [各 ISE ノードのサーバの指定（Specify server for each ISE node）] オプションを有効にするか、既存のサーバを選択し、PSN を使用して Cisco ISE 展開をアップグレードすると、展開 ID がリセットされる傾向があります。

回避策

各ノードの LDAP サーバ設定を再設定します。詳細については、Cisco Identity Services Engine 管理者ガイド、リリース 2.4 [英語] の「Administrative Access to Cisco ISE Using an External Identity Store」の章の「LDAP Identity Source Settings」の項を参照してください。

アップグレード GUI 通知

制限事項

アップグレード GUI に、アップグレードが 100% になるまでセカンダリ PAN のアップグレードが 0% で進行していることが示されます。アップグレードプロセスはバックグラウンドで続行され、アップグレードには影響しません。

条件

Cisco ISE 2.4 パッチ 8 から新しいリリースにアップグレードする場合。

回避策

ade.log ファイルでアップグレードプロセスを確認します。ade.log ファイルを表示するには、Cisco ISE CLI から次のコマンドを入力します。

```
show logging system ade/ADE.log
```

詳細については、CSCvp78781 を参照してください。

pxGrid 証明書の問題

制限事項

pxGrid のデフォルトの自己署名証明書が失敗します。

条件

Cisco ISE 2.7 パッチ 7 から新しいリリースにアップグレードする場合。

回避策

別の証明書を使用するか、または既存の証明書に「SSLクライアント」を追加します。

特定の条件下で IP-SGT バインディングが伝播されない

次の条件下では、IP-SGT マッピングは ACI に伝播されません。

ISE 管理者コンソールで、[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] の順に移動します。

1. セキュリティグループを作成します。ただし、[ACIに伝播（Propagate to ACI）] はオンにしないでください。
2. 前の手順で作成したセキュリティグループを使用して、IP-SGTバインディングを作成します。これは、スタティックバインディング、セッションバインディング、SXPバインディングのいずれかになります。
3. セキュリティグループで、[ACIに伝播（Propagate to ACI）] をオンにします。
4. [保存（Save）] をクリックします。
5. セキュリティグループは、ACI と同期しますが、セキュリティグループにマッピングされている SGT とは同期しません。

回避策

次のいずれかを行います。

1. ISE で ACI 伝播を再開し、IP-SGT マッピングを再作成します。
    1. [ワークセンター（Work Centers）] > [TrustSec] > [設定（Settings）] > [ACIの設定（ACI Settings）] で、[TrustSec-ACIポリシー要素の交換（TrustSec-ACI Policy Element Exchange）] をオフにし、保存します。

2. [TrustSec-ACIポリシー要素の交換（TrustSec-ACI Policy Element Exchange）] をオンにし、保存します。
3. Cisco ISE と ACI との間の接続が再確立されます。

2. 古い IP-SGT バインディングを削除し、[ACIに伝播（Propagate to ACI）] をオンにして再作成します。

（注） ACI と ISE との間の接続は 24 時間ごとに再認証されるため、同様にこの問題が修正されます。

SXP プロトコルセキュリティ標準

制限：Security Group Exchange Protocol（SXP）は、暗号化されていないデータを転送し、draft-smith-kandula-sxp-06 ごとのメッセージ整合性チェックに脆弱なハッシュアルゴリズムを使用します。
回避策：回避策はありません。

詳細については、https://tools.ietf.org/html/draft-smith-kandula-sxp-06 を参照してください。

Chrome ブラウザを使用したパッチビルドのダウンロード

制限：整合性チェックサムの問題は、Google Chrome ブラウザを使用してパッチビルドをダウンロードする場合に発生します。
条件：Message Digest 5（MD5）の合計値が一致しません。
回避策：FireFox ブラウザを使用してパッチビルドをダウンロードします。ダウンロードしたパッチバンドルの MD5 チェックサムが正しいことを確認します。

認証の Radius ログ

認証イベントの詳細は、[Radius認証（Radius Authentications）] ウィンドウの [詳細（Details）] フィールドで確認できます。認証イベントの詳細を使用できるのは7日間のみで、その後は認証イベントのデータを表示することはできません。すべての認証ログデータは、パージがトリガーされると削除されます。

プロファイラ RADIUS プローブ

制限：エンドポイントはプロファイリングされません。認証され、データベースに追加されるだけです。
条件：RADIUS プローブは無効になっています。
回避策：プロファイリングサービスを完全に無効にします。

NAM TLS 1.2 非互換警告

制限：EAP-FAST の ISE 実装では、TLS 1.2 でのキー生成はサポートされていません。
条件：EAP-FAST を使用してエンドポイントを認証するために NAM 4.7 を使用している場合は、ISE の特定のバージョンしか EAP-FAST に必要な TLC 1.2 をサポートしていないことに注

意してください。適切でないバージョンのISEを使用している場合、認証が失敗し、エンドポイントからネットワークにアクセスすることはできません。
回避策：この問題を解決するには、次のリリースに示すようにCisco ISEソフトウェアをアップグレードします。

- Cisco ISEリリース2.4：パッチ5以降。
- Cisco ISEリリース2.0、2.0.1、2.1。ホットパッチを適用する前に、Struts2-CVE-2018-11776 PSIRT修正プログラムをインストールします。Struts2-CVE-2018-11776 PSIRT修正プログラムはCiscoソフトウェアダウンロードからダウンロードできます。

（注） リリース2.4よりも前のCisco ISEリリースのホットパッチを入手するには、Cisco Technical Assistance Center（TAC）にお問い合わせください。ホットパッチを適用する前に、ISEソフトウェアに最新のパッチが適用されていることを確認してください。

詳細については、https://www.cisco.com/c/en/us/support/docs/field-notices/703/fn70357.html を参照してください。

メモリ使用率が高い

制限：Cisco ISEバージョン1.3以降へのインストールまたはアップグレード後にメモリ使用率が高くなります。
条件：カーネルがキャッシュメモリを管理する方法が原因で、Cisco ISEでより多くのメモリが使用される可能性があるため、メモリ使用率が高くなり（80 ～ 90%）、アラームが発生することがあります。
回避策：回避策はありません。

詳細については、CSCvn07836 を参照してください。

Diffie-Hellman 最小キー長

制限：LDAPサーバへの接続に失敗しました。
条件：LDAPサーバに設定されているDiffie-Hellman最小キー長が1024未満の場合、LDAPサーバへの接続に失敗します。
回避策：LDAPサーバのDiffie-Hellmanキーのサイズを変更します。

詳細については、CSCvi76985 を参照してください。

ECDSA 証明書

制限：Cisco ISEは、キー長が256および384のみの楕円曲線デジタル署名アルゴリズム（ECDSA）証明書をサポートします。
条件：EAP認証に使用されるECDSA証明書は、Androidバージョン6.x以降のエンドポイントでのみサポートされます。

（注） Apple iOS は、ECDSA をシステム証明書として使用する場合はサポートされません。ECDSA 証明書は、Android 6.x および Android 7.x でのみサポートされます。

回避策：[管理（Administration）]>[システム（System）]>[証明書（Certificates）]>[証明書の管理（Certificate Management）]>[システム証明書（System Certificates）] ウィンドウでキー長を選択できます。

サプリカント プロビジョニング ウィザード参照の再作成

制限：BYOD 証明書のプロビジョニングフローは内部証明書と外部証明書の両方で破損しています。
条件：新しいリリースにアップグレードする場合、またはパッチを適用する場合、サプリカント プロビジョニング ウィザード（SPW）は更新されません。
回避策：新しい SPW を参照する新しいネイティブ サプリカント プロファイルと新しいクライアント プロビジョニング ポリシーを作成します。

エンドポイント保護サービス API

Cisco ISE 1.4 現在、ANC はエンドポイント保護サービスを置き換えます。ANC は、追加の分類を提供し、パフォーマンスを向上させます。Cisco ISE SDK には、ANC 用の新しい API が備わっています。ERS API がまだ機能する場合もありますが、ANC に移行することを強く推奨します。

アップグレード情報

- リリース 2.6 へのアップグレード
- ライセンスの変更
- アップグレード手順の前提条件

（注） ホットパッチをインストールしている場合は、アップグレードパッチを適用する前にホットパッチをロールバックします。

リリース 2.6 へのアップグレード

次の Cisco ISE リリースからリリース 2.6 に直接アップグレードできます。

- 2.1
- 2.2
- 2.3

- 2.4

（注） Cisco ISE 2.6 パッチ 7 にアップグレードすると、ANC ポリシーで RE_AUTHENTICATE を使用していた場合にエラーメッセージが表示されます。既存のポリシーは引き続き機能します。

パッチ 2 を適用すると、エラーメッセージが表示されなくなります。または、アップグレードする前にこれらのポリシーを削除できます。

Cisco ISE リリース 2.1 より前のバージョンの場合は、はじめに上記のリリースのいずれかにアップグレードしてから、リリース 2.6 にアップグレードする必要があります。

（注） アップグレードの開始前に、既存のバージョンで最新のパッチにアップグレードすることをお勧めします。

Cisco ISE リリース 2.6 には、2.0 パッチ 7、2.1 パッチ 8、2.2 パッチ 13、2.3 パッチ 5、および 2.4 パッチ 5 とのパリティがあります。

仮想マシンでサポートされるオペレーティングシステム

GUI または CLI のいずれかからリリース 2.6 にアップグレードできます。

Cisco ISE は、Red Hat Enterprise Linux（RHEL）に基づく Cisco Application Deployment Engine オペレーティングシステム（ADEOS）で動作します。Cisco ISE リリース 2.6 では、ADEOS は RHEL 7.5 に基づいています。詳細については、Cisco Identity Services Engine アップグレードプロセス [英語] を参照してください。

VMware 仮想マシンの Cisco ISE ノードをアップグレードする場合は、アップグレードの完了後に、Red Hat Enterprise Linux（RHEL）のサポートされるバージョンにゲスト オペレーティング システムを変更します。これを行うには、VM の電源をオフにし、サポートされる RHEL バージョンにゲスト オペレーティング システムを変更し、変更後に VM の電源をオンにする必要があります。

パッチの互換性

このパッチは、次のパッチリリースと互換性があります。

- 2.2 パッチ 15
- 2.3 パッチ 7
- 2.4 パッチ 10
- 2.6 パッチ 2

アップグレードパッケージ

アップグレードパッケージおよびサポートされているプラットフォームに関する情報は、Cisco ISE Software Download から入手できます。

ライセンスの変更

デバイス管理ライセンス

デバイス管理ライセンスには、クラスタとノードの2つのタイプがあります。クラスタライセンスでは、Cisco ISE クラスタ内のすべてのポリシーサービスノードでデバイス管理を使用できます。ノードライセンスでは、1つのポリシーサービス ノードでデバイス管理を使用できます。ハイ アベイラビリティ スタンドアロン展開では、ノードライセンスによって、ハイアベイラビリティペアの 1 つのノードでデバイス管理を使用することが許可されます。

デバイス管理ライセンスキーは、プライマリおよびセカンダリポリシー管理ノードに対して登録されます。クラスタ内のすべてのポリシーサービスノードは、ライセンス数に達するまで必要に応じてデバイス管理ライセンスを消費します。

クラスタライセンスは Cisco ISE 2.0 のデバイス管理のリリースで導入され、Cisco ISE 2.0 以降のリリースで適用されています。ノードライセンスは後でリリースされ、リリース 2.0 ～ 2.3 で部分的にのみ適用されています。Cisco ISE 2.4 以降では、ノードライセンスはノード単位で完全に適用されています。

クラスタライセンスは廃止されました。現時点ではノードライセンスのみを販売しています。

ただし、有効なクラスタライセンスでこのリリースにアップグレードする場合は、アップグレード時に既存のライセンスを引き続き使用できます。

評価ライセンスを使用すると、1 つのポリシーサービスノードでデバイスを管理できます。

仮想マシンノードのライセンス

Cisco ISE は仮想マシン（VM）としても販売されています。このリリースでは、展開に VM ノードの適切な VM ライセンスをインストールすることをお勧めします。VM ノードの数と CPUやメモリなどの各VMノードのリソースに基づいて、VMライセンスをインストールします。そうでない場合、VM ライセンスキーを調達してインストールする警告と通知が表示されます。ただし、インストールプロセスは中断されません。Cisco ISE リリース 2.4 以降、GUI から VM ライセンスを管理できます。

VM ライセンスは、小、中、大の 3 つのカテゴリで提供されます。たとえば、8 コアと 64 GB RAM を備えた 3595 相当の VM ノードを使用している場合、VM で同じ機能をレプリケートするには、中カテゴリのVMライセンスが必要になります。展開の要件に応じて、VM とそのリソースの数に基づいて、複数の VM ライセンスをインストールできます。

VMライセンスはインフラストラクチャ ライセンスです。このため、展開で使用可能なエンドポイントライセンスに関係なく、VMライセンスをインストールできます。展開にEvaluation、Base、Plus、Apex ライセンスのどれもインストールされていない場合でも、VM ライセンスをインストールできます。ただし、Base、Plus、または Apex ライセンスによって有効になる機能を使用するには、適切なライセンスをインストールする必要があります。

VM ライセンスは永久ライセンスです。VM ライセンスの変更は、Cisco ISE GUI にログインするたびに表示され、通知ポップアップウィンドウで [今後、このメッセージを表示しない（Do not show this message again）] チェックボックスをオンにすると表示されなくなります。

以前に ISE VM ライセンスを購入していない場合、『Cisco Identity Services Engine Ordering Guide』を参照して購入する適切な VM ライセンスを選択します。

（注） PAK を使用せずに ISE VM ライセンスを購入した場合は、licensing@cisco.com に電子メールを送信して VM PAK を要求できます。電子メールに ISE VM の購入を示す SO 番号とシスコ ID を記載してください。購入した各 ISE VM ごとに 1 つの中規模 VM ライセンスキーを提供します。

使用中の Cisco ISE バージョンと VM の互換性に関する詳細については、該当するリリースの『Cisco Identity Services Engine Installation Guide』の「Hardware and Virtual Appliance Requirements」の章を参照してください。

ライセンスの詳細については、『Cisco Identity Services Engine Administrator Guide』の「Cisco ISE Licenses」の章を参照してください。

アップグレード手順の前提条件

- 設定されたデータを必要な ISE バージョンにアップグレードできるかどうかを確認するには、ISE ソフトウェアアップグレードの前にアップグレード準備ツール（URT）を実行します。ほとんどのアップグレードの失敗は、データのアップグレードの問題が原因で発生します。URT は、可能な場合は、必ず実際のアップグレード前にデータを検証し、問題を報告または修正するように設計されています。URT は *Cisco ISE Download Software Center* からダウンロードできます。
- アップグレードの開始前に関連するすべてのパッチをインストールすることをお勧めします。

詳細については、『*Cisco Identity Services Engine Upgrade Guide*』を参照してください。

Cisco ISE ライブアップデートポータル

Cisco ISE ライブアップデートポータルは、**サプリカント プロビジョニング** ウィザード、AV/AS サポート（コンプライアンスモジュール）、およびクライアントプロビジョニングとポスチャポリシーサービスをサポートするエージェントインストーラパッケージを自動的にダウンロードするのに役立ちます。このライブアップデートポータルは、Cisco ISE を使用して Cisco.com から該当するデバイスに最新のクライアントプロビジョニングおよびポスチャソフトウェアを直接取得するように、初期展開時に Cisco ISE で設定します。

デフォルトのアップデートポータル URL にアクセスできず、ネットワークにプロキシサーバが必要な場合は、プロキシを設定します。ライブアップデートポータルにアクセスする前に、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）] の

順に選択します。プロキシ設定でプロファイラ、ポスチャ、およびクライアントプロビジョニング フィードへのアクセスが許可されている場合、Cisco ISE は MDM 通信のプロキシサービスをバイパスできないため、モバイルデバイス管理（MDM）サーバへのアクセスがブロックされます。これを解決するには、MDM サーバとの通信を許可するようにプロキシサービスを設定できます。プロキシ設定の詳細については、『Cisco Identity Services Engine Administrator Guide』の「Specify Proxy Settings in Cisco ISE」の項を参照してください。

クライアント プロビジョニングとポスチャのライブアップデートポータル

次の場所からクライアント プロビジョニング リソースをダウンロードできます。

[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアアップデート（Software Updates）] > [クライアント プロビジョニング（Client Provisioning）]。

次のソフトウェア要素は、次の URL から入手できます。

- Windows および Mac OS X ネイティブサプリカント向けのサプリカント プロビジョニング ウィザード
- 最新の Cisco ISE の永続的なエージェントおよび一時的なエージェントの Windows バージョン
- 最新の Cisco ISE の永続的なエージェントの Mac OS X バージョン
- ActiveX および Java アプレット インストーラ ヘルパー
- AV/AS コンプライアンス モジュール ファイル

クライアント プロビジョニング アップデート ポータルで利用可能なソフトウェアパッケージを Cisco ISE に自動的にダウンロードする方法については、『Cisco Identity Services Engine Administrator Guide』の「Configure Client Provisioning」の章の「Download Client Provisioning Resources Automatically」の項を参照してください。

次の場所からポスチャ更新をダウンロードできます。

[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアアップデート（Software Updates）] > [ポスチャ更新（Posture Updates）]

次のソフトウェア要素は、次の URL から入手できます。

- シスコで事前定義されたチェックとルール
- Windows および Mac OS X の AV/AS サポート表
- Cisco ISE オペレーティングシステムのサポート

このポータルで利用可能なソフトウェアパッケージを Cisco ISE に自動的にダウンロードする方法については、『Cisco Identity Services Engine Administrator Guide』の「Download Posture Updates Automatically」の項を参照してください。

自動ダウンロード機能を有効にしていない場合、更新をオフラインでダウンロードすることができます。

Cisco ISE オフライン更新

このオフライン更新オプションを使用すると、Cisco ISE を使用してデバイスから Cisco.com にインターネット経由で直接アクセスできない場合、またはセキュリティポリシーによって許可されていない場合に、クライアントプロビジョニングおよびポスチャ更新をダウンロードできます。

オフラインのクライアント プロビジョニング リソース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 https://software.cisco.com/download/home/283801620/type/283802505/release/2.6.0 に進みます。

ステップ 2 ログインクレデンシャルを入力します。

ステップ 3 Cisco Identity Services Engine のダウンロードウィンドウに移動し、リリースを選択します。

次のオフライン インストール パッケージをダウンロードできます。

- **win_spw-**<*version*>**-isebundle.zip**：Windows 向けのオフライン SPW インストールパッケージ
- **mac-spw-**<*version*>**.zip**：Mac OS X 向けのオフライン SPW インストールパッケージ
- **compliancemodule-**<*version*>**-isebundle.zip**：オフライン コンプライアンス モジュール インストール パッケージ
- **macagent-**<*version*>**-isebundle.zip**：オフライン Mac エージェント インストール パッケージ
- **webagent-**<*version*>**-isebundle.zip**：オフライン Web エージェント インストール パッケージ

ステップ 4 [ダウンロード（Download）] または [カートに追加（Add to Cart）] のいずれかをクリックします。

ダウンロードしたインストールパッケージを Cisco ISE に追加する方法については、『Cisco Identity Services EngineAdministrator Guide』の「Add ClientProvisioning Resources from a Local Machine」のセクションを参照してください。

ポスチャ更新を使用して、ローカルシステムのアーカイブから Windows および Mac オペレーティングシステムのチェック、オペレーティングシステム情報、ウイルス対策とスパイウェア対策サポート表を更新できます。

オフライン更新の場合は、アーカイブファイルのバージョンが設定ファイルのバージョンと一致していることを確認します。Cisco ISE を設定した後にオフラインでポスチャ更新を使用し、ポスチャポリシーサービスの動的更新を有効にします。

オフラインのポスチャ更新をダウンロードするには、次のようにします。

手順

ステップ 1 https://s3.amazonaws.com/ise-public/posture-offline.zipに進みます。

ステップ 2 ローカルシステムに **posture-offline.zip** ファイルを保存します。このファイルを使用すると、WindowsおよびMacオペレーティングシステムのオペレーティングシステム情報、チェック、ルール、ウイルス対策とスパイウェア対策サポート表が更新されます。

ステップ 3 Cisco ISE 管理者ユーザインターフェイスを起動し、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] を選択します。

ステップ 4 矢印をクリックすると、ポスチャの設定が表示されます。

ステップ 5 [更新（Updates）] をクリックします。
[ポスチャ更新（Posture Updates）] ウィンドウが表示されます。

ステップ 6 [オフライン（Offline）] オプションをクリックします。

ステップ 7 [参照（Browse）] をクリックし、システムのローカルフォルダからアーカイブファイル（posture-offline.zip）を検索します。

（注） [更新するファイル（File to Update）] フィールドは必須フィールドです。適切なファイルを含むアーカイブファイル（.zip）を 1 つだけ選択できます。.zip、.tar、.gz 以外のアーカイブファイルはサポートされていません。

ステップ 8 [今すぐ更新（Update Now）] をクリックします。

設定要件

- 関連する Cisco ISE ライセンス料金を支払う必要があります。
- 最新のパッチをインストールする必要があります。
- Cisco ISE ソフトウェア機能がアクティブになっている必要があります。

ISE の設定を開始するには、次のリソースを参照してください。

- Getting started with Cisco ISE
- YouTube の Cisco ISE チャンネルのビデオ
- *Cisco ISE Design and Integration Guides*
- *Cisco Identity Services Engine Administrator Guide*

モニタリングおよびトラブルシューティング

システムのモニタリングおよびトラブルシューティングに関する詳細については、『*Cisco Identity Services Engine Administrator Guide*』の「Monitoring and Troubleshooting Cisco ISE」のセクションを参照してください。

発注情報

Cisco ISE の詳細な発注およびライセンス情報については、Cisco Identity Services Engine 発生ガイド [英語] を参照してください。

Cisco ISE と Cisco Digital Network Architecture Center との統合

Cisco ISE は Cisco DNA Center と統合できます。Cisco DNA Center と連携するように Cisco ISE を設定する方法については、*Cisco DNA Center* のドキュメントを参照してください。

Cisco ISE と Cisco DNA Center との互換性については、「*Cisco SD-Access Compatibility Matrix*」を参照してください。

新しいパッチのダウンロードとインストール

Cisco ISE にパッチを適用するために必要なパッチファイルを取得するには、Cisco ダウンロードソフトウェア サイト（https://software.cisco.com/download/home）にログインし（Cisco.com ログイン情報の入力が必要になる場合があります）、[セキュリティ（Security）] > [アクセス制御およびポリシー（Access Control and Policy）] > [Cisco Identity Services Engine] > [Cisco Identity Services Engine ソフトウェア（Cisco Identity Services Engine Software）] に移動し、ローカルマシンにパッチファイルのコピーを保存します。

システムへのパッチの適用方法については、『Cisco Identity Services Engine Administrator Guide』の「Install a Software Patch」の項を参照してください。

CLI を使用したパッチのインストール方法については、『Cisco Identity Services Engine CLI Reference Guide』の「Patch Install」セクションを参照してください。

（注） リリース 2.4 パッチ 4 以降をインストールする場合、カーネルのアップグレード中に CLI サービスが一時的に使用できなくなります。この間に CLI にアクセスすると、「スタブライブラリを開くことができませんでした（Stub Library could not be opened）」というエラーメッセージが CLI に表示されます。ただし、パッチのインストールが完了すると、CLI サービスが再び利用可能になります。

注意事項

「不具合」セクションには、バグ ID とそのバグの簡単な説明が含まれています。特定の不具合の症状、条件、および回避策に関する詳細については、シスコのバグ検索ツール（BST）を使用してください。バグ ID は英数字順にソートされます。

（注） 「未解決の不具合」の項には、現在のリリースに適用され、Cisco ISE 2.6 よりも前のリリースにも適用されている可能性のある未解決の不具合が記載されています。これまでのリリースで未解決で、まだ解決されていない不具合は、解決されるまで、今後のすべてのリリースに適用されます。

BST は Bug Toolkit の後継オンラインツールであり、ネットワークリスク管理およびデバイスのトラブルシューティングにおいて効率性を向上させるように設計されています。製品、リリース、またはキーワードに基づいてソフトウェアのバグを検索し、バグの詳細、製品、バージョンなどの主要データを集約することができます。ツールの詳細については、http://www.cisco.com/web/applicat/cbsshelp/help.html のヘルプ ページを参照してください。

Cisco ISE リリース 2.6.0.156 の新機能 - 累積パッチ 7

ANC 拡張機能

MAC アドレスは、エンドポイントの一意の識別子とは限りません。USB NIC ドングルは、複数のユーザが同じ MAC アドレスを持てることを意味します。さらに、一部のエンドポイントは同じ MAC アドレスを持ちます。MAC スプーフィングには、重複する MAC アドレスも表示されます。

ANC サービスのエンドポイントをより適切に識別するために、Cisco ISE は、エンドポイントが接続されているスイッチの IP アドレスを使用します。スイッチの IP アドレスは `NAS-IPAddress` 属性です。

エンドポイントセッションは、ANC ポリシーで MAC アドレスと `NAS-IPAddress` を使用できます。

MDM ベンダーは、pxGrid v2 API で `NAS-IPAddress` を使用できます。

新しい API で `NAS-IPAddress` を使用するには、PxGrid v2 が必要です。既存の API は引き続き動作します。ただし、新旧両方の API を一緒に使用できません。

Cisco ISE のアップグレードに関する考慮事項

Cisco ISE 2.6 パッチ 7 にアップグレードすると、ANC ポリシーで RE_AUTHENTICATE を使用していた場合にエラーメッセージが表示されます。既存のポリシーは引き続き機能します。

Cisco ISE 2.6 パッチ 2 を適用すると、エラーメッセージが表示されなくなります。または、アップグレードする前にこれらのポリシーを削除できます。

プローブデータパブリッシャの有効化

プローブデータパブリッシャは、プライマリポリシー管理ノード（PAN）で pxGrid パブリッシャを開始します。プライマリ PAN が接続されたエンドポイントの属性の変更を識別すると、更新された属性データが Cisco ISE の関連する pxGrid トピックにパブリッシュされます。

デフォルトでは、このオプションは無効になっています。このオプションは、外部データコンシューマが設定されている場合にのみ有効にすることをお勧めします。

プローブデータパブリッシャを有効にするには、**[ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [設定（Settings）]** に移動し、[プローブデータパブリッシャの有効化（Enable Probe Data Publisher）] チェックボックスをオンにします。

テレメトリ

インストール後の管理者ポータルへの初回ログイン時には、Cisco ISE テレメトリバナーが表示されます。この機能を使用して、Cisco ISE は、ユーザの展開、ネットワーク アクセス デバイス、プロファイラ、およびユーザが使用している他のサービスに関する非機密情報を安全に収集します。このデータは、今後のリリースでサービスを向上させ、より多くの機能を提供するために使用されます。デフォルトでは、テレメトリは有効になっています。アカウント情報を無効または変更するには、[管理（Administration）] > [設定（Settings）] > [ネットワーク設定診断（Network Settings Diagnostics）] > [テレメトリ（Telemetry）] の順に選択します。アカウントは、各展開に固有です。各管理者ユーザが個別に提供する必要はありません。

テレメトリは、Cisco ISE のステータスと機能に関する貴重な情報を提供します。シスコは、Cisco ISE を導入した IT チームのアプライアンス ライフサイクル管理を改善するためにテレメトリを使用します。このデータを収集することで、製品チームは顧客により優れたサービスを提供できるようになります。このデータと関連する分析情報により、シスコは潜在的な問題をプロアクティブに特定し、サービスとサポートを改善し、ディスカッションを促進して新規および既存の機能からより多くの価値を収集し、IT チームによるライセンス権限のインベントリレポートと今後の更新を支援します。

Cisco ISE で、機能が無効になり、テレメトリデータの共有が停止するまでに最大 24 時間かかる場合があります。 パッチ 6 以降では、テレメトリはすぐに無効になります。

インタラクティブヘルプ

インタラクティブヘルプを使用すると、タスクを簡単に実行するためのヒントと段階的なガイダンスが表示されます。

ビジネス成果：これにより、エンドユーザは作業フローを容易に理解し、タスクを簡単に実行できるようにします。

Cisco ISE リリース 2.6.0.156 の解決済みの不具合 - 累積パッチ 7

次の表に、リリース 2.6 累積パッチ 7 の解決済みの不具合を示します。

パッチ 7 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCvb55884	ISE RBAC ネットワークデバイスタイプ/ロケーションビューが機能しない
CSCvd38796	AD が authC と authZ の両方に使用されている場合、RA-VPN/CWA に対して AD ドメイン属性が取得されない

不具合 ID 番号	説明
CSCvj47301	ノードグループメンバーが到達不能の場合、ISE はアクティブ準拠のセッションに CoA を送信する
CSCvn12644	AD 属性のポリシー評価中に ISE がクラッシュする
CSCvn50531	tcpdump print_prefix 関数スタックベースのバッファオーバーリードの脆弱性
CSCvo15781	Logwatch ファイルのサイズの上限が定められていない
CSCvo28970	Cisco 経時的エージェントを使用すると、AnyConnect に Cisco NAC エージェントエラーが表示される
CSCvo51415	ISE 2.4 URT が証明書エラーで失敗する
CSCvo68357	ISE 復元オプションに暗号キーなしの <cr> 改行がない
CSCvo73749	「MAR キャッシュ配布が有効にならない」（有効にしていた場合でも）
CSCvp16483	古いジャーナルログファイルを削除する
CSCvp17458	libssh2 SSH_MSG_CHANNEL_REQUEST パケット処理が領域外メモリ参照の...
CSCvp40398	スケジュール設定と運用バックアップを当日と同じ開始日に設定することができない
CSCvq07619	GnuPG ファイル名ステータスメッセージのスプーフィングの脆弱性
CSCvq13431	ポスチャと RADIUS フロー中、コンテキスト属性を取得している間に ISE PSN ノードがクラッシュする
CSCvq19646	TCP_SACK のポジションの評価
CSCvq48396	レプリケーション失敗アラームが生成され、ise-psc.log に ORA-00001 例外が表示される
CSCvq61089	SAML 認証を使用した BYOD オンボーディング後、デバイスポータルにデバイスが表示されない
CSCvq73677	GNU パッチ OS シェル コマンド インジェクションの脆弱性
CSCvq86741	FasterXML jackson-databind logback-core クラスのポリモーフィック型逆シリアル化...
CSCvq86746	jquery の複数の脆弱性 - ゲストポータル
CSCvr09749	GNU パッチ do_ed_script OS シェルコマンドの実行の脆弱性

不具合 ID 番号	説明
CSCvr19392	Apache Commons Beanutils PropertyUtilsBean クラスプロパティの抑制の脆弱性
CSCvr39943	脅威イベントに対するアクションの空白のコースが CTA クラウドから TC-NAC アダプタに受信された
CSCvr40545	秘密キーの暗号化に失敗したときに、共有暗号がないためEAP-FAST認証に失敗した
CSCvr47732	FasterXML jackson-databind ポリモーフィック型入力の脆弱性 CVSS v3.1 Base：9.8
CSCvr47790	Apache Commons Compress ファイル名のエンコーディング アルゴリズム DoS の脆弱性 CVSS v3.0 Base：7.5
CSCvr56785	大きなコアファイルに対応するためにローカルディスクサイズを拡大する必要がある
CSCvr77676	libmspack chmd_read_headers 関数サービス妨害の脆弱性
CSCvr84753	ISE 2.2 パッチ 14 AD ステータスが「更新しています...（updating ..）」と表示され、プロセスがハングしていることを示す
CSCvr85363	ユーザ API による ISE アプリのクラッシュ
CSCvr87373	ACI マッピングは SXP pxGrid トピックにパブリッシュされない
CSCvs05260	App server と EST サービスが毎朝 1 時にクラッシュ/再起動する
CSCvs09981	ISE のグループノード間の MAR キャッシュチェックが原因で失敗した COA を除外する機能を追加する
CSCvs19481	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvs23628	ルールが一致した後でも、ポリシーエンジンがすべてのポリシーセットの評価を続行する
CSCvs25569	無効なルート CA 証明書が受け入れられた
CSCvs36758	ISE 2.6 で 2 つのカッコを使用して CRL URL を設定できない
CSCvs38883	古いデータをプッシュする TrustSec マトリックス
CSCvs39880	Xms 値を持つ Mnt ノードの高負荷
CSCvs40406	信頼できる CA 証明書の削除中に SEC_ERROR_BAD_DATABASE がシステム/アプリデバッグログに表示される
CSCvs42758	CRL が特定の条件で期限切れになる

不具合 ID 番号	説明
CSCvs44006	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvs44795	ISE が SGT を正しく更新しない
CSCvs46399	URL リダイレクトの AuthZ プロファイルの詳細プロファイルでカスタム HTTPS 宛先が許可されない
CSCvs46853	DNA-C との統合中に、信頼できるストアから削除されたものと同じ CN の ISE 2.6 CA 証明書
CSCvs46998	条件はライブラリから削除されたが、DB 内にある
CSCvs47941	ISE2.6 で内部 CA とキーをインポートできない
CSCvs51519	NFS マウントが原因でクラッシュする
CSCvs52031	MACAdress API が機能していない（API/mnt/Session/MACAddress）
CSCvs55464	スポンサーポータルで新しいユーザを作成すると、「無効な入力（invalid input）」が表示される
CSCvs55594	ランダム認証の場合、期限切れまでの日数が 0 としてマークされる
CSCvs58106	NAD CSV のインポートでは、サポートされているすべての文字を TrustSecDeviceID に許可する必要がある
CSCvs60518	ISE 管理者ユーザが内部ユーザのグループを変更できない
CSCvs62081	コレクタログが pxgid および dnac メッセージとともにダンプされる
CSCvs62586	REST API を使用すると Tacacs プロファイルが正しく取得されない
CSCvs65467	Cisco Identity Services Engine のストアド クロスサイト スクリプティングの脆弱性
CSCvs65989	ネットワークデバイス/グループをインポートした後、新しいロケーションを追加できない
CSCvs67042	ISE 2.2+ がメモリリークの影響を受ける Inflater() によってネイティブメモリが毎日 1 ー 2% 増加する
CSCvs67785	セルフ登録ポータルのポータルページのカスタマイズで、日数が更新されない
CSCvs68914	DNAC から送信された _（アンダースコア）を使用して SG が作成されたときにエラーが発生する
CSCvs69726	ISE 2.2+ がメモリリークの影響を受ける PORT_Alloc_Util() によってネイティブメモリが毎日 1 ー 2% 増加する

不具合 ID 番号	説明
CSCvs70863	ISE 2.6：デフォルトのデバイス管理者が変更されていると FIPS を有効にできない
CSCvs70997	ISE：SCEP RA の設定時に 2.4p9 CA 中間証明書がインストールされない
CSCvs75274	「証明書プロビジョニングポータル」のポータルカスタマイズを実行できない
CSCvs76257	RadiusProxyFlow::stripUserName() にユーザ名ではなく空の文字列があるために ISE がクラッシュする
CSCvs77182	ISE：属性「url-redirect」を HTTPS で使用できず、HTTP を使用する同じ URL は正常に機能する
CSCvs78160	INetworkAuthZCheck の ConditionsData 句で URT が失敗する
CSCvs83303	中間更新が DB に保存されていない場合、API がデータを取得しない
CSCvs84948	binutils の複数の脆弱性
CSCvs85970	AD join-point に文字列「TACACS」があると、AuthZ 条件で AD joinpoint が表示されない
CSCvs86344	ゲストユーザ名に @ 記号（guest@example.com）が含まれていると、ISE 2.4 Guest ERS Call Get-By-Name が失敗する
CSCvs86686	パッチの複数の脆弱性
CSCvs86690	python の複数の脆弱性
CSCvs86697	sudo の複数の脆弱性
CSCvs86775	ISE 2.6 インストール：検証の入力 - IP ドメイン名の確認
CSCvs88222	パッケージ展開の脆弱性 - RHEL 7
CSCvs88368	ハッシュパスワードを使用すると ISE SNMP サーバがクラッシュする
CSCvs91808	特殊文字を含むメタデータ XML ファイルをインポートすると、サポートされていないタグエラーが発生する
CSCvs96541	ISE 2.4 P11 で、OP バックアップの復元時に EPOCH_TIME 列が削除される
CSCvs97302	.dmp ファイルが ISE の reset-config の後でも /opt/oracle/base/admin/cpm10/dpdump から削除されない
CSCvt00283	ゲストスポンサーポータルの成功ページ更新時の 404 エラー

不具合 ID 番号	説明
CSCvt01161	NMAP：ISE のバージョン 2.6 で MCAFeeEPROOrchestratorClientscan を実行できない
CSCvt03094	ISE の期限切れの tacacs セッションがセッションキャッシュからタイムリーにクリアされない
CSCvt03292	Cert Revoke と CPP が APEX ライセンスなしで機能しない
CSCvt03935	TrustSec ポリシーマトリックス -- ISE の [表示（View）] オプションの表現を変更する
CSCvt04047	バックアップ/復元メニューに移動した後、すべての ISE ページで POST getBackupRestoreStatus が発生する
CSCvt04144	アラーム設定での高ディスク使用率のしきい値オプションがない
CSCvt05201	トンネルグループポリシー評価によるポスチャが Java Mem を減らしている
CSCvt07230	ISE がインポート時にイーグレスポリシーで ANY を許可しない
CSCvt08143	ISE 2.6 の時差
CSCvt10214	[ENH] ネットワークデバイスの API を使用して「GET|PUT|DELETE by Name」機能を追加する
CSCvt12236	IP SGT スタティックマッピングのインポートがホスト名で正しく動作しない
CSCvt13198	FasterXML jackson-databind xbean-reflect/JNDI のブロッキングの脆弱性
CSCvt13707	pxGrid 2.0 WebSocket 分散アップストリーム接続の問題
CSCvt13719	pxGrid 2.0 WebSocket ping pong がアイドル状態のスタンドアロンでも遅すぎる
CSCvt13746	追加の authz ポリシーと例外がある場合、ISE はすべてのデバイス管理 authz ルールを表示しない
CSCvt14248	EST サービスを初期化する認証局サービスが ISE 2.6 へのアップグレード後に実行しない
CSCvt15256	「ゲストユーザ」ID ストアを使用すると、認証プロセスが失敗する。
CSCvt15893	ISE 2.6 へのアップグレード後、エラーサプリカント/不良構成サプリカントの Radius テーブルが存在しない
CSCvt15935	JDK8 のメタスペースの代わりに PERMGEN が設定された

不具合 ID 番号	説明
CSCvt16882	Apple CNA と AUP をリンクとして使用して iPad にアクセスすると、400 Bad 要求エラーが発生する。
CSCvt17335	WMI と REST を同時に使用すると Pxgrid でバッチロジックをパブリッシュする
CSCvt17783	ISE では、SGT のインポートまたはエクスポートで ANY SGT または値 65535 を公開できない
CSCvt19657	多数のエンドポイントが存在する場合、ISE ERS API エンドポイントの更新が遅い
CSCvt24276	許可された値をシステム使用ディクショナリへの 7 つ以上の属性に追加/変更できない
CSCvt35044	EP ルックアップに時間がかかり、ゲストフローの遅延が大きくなる
CSCvt36117	アイデンティティグループが ISE の内部ユーザを更新する
CSCvt36322	リダイレクト値が URL に存在する場合、ISE 2.6 MDM フローが失敗する
CSCvt36324	ホスト名が CARS 設定から欠落している
CSCvt37910	[ENH] /ers/config/internaluser の API を使用して「GET|PUT|DELETE by Name」機能を追加する
CSCvt38308	ISE：min pwd の長さを増やすと、既存の短い pwd の GUI を使用したログインがエラーなしで失敗する
CSCvt40534	MNT ノード選択プロセスが適切に設計されない。
CSCvt49961	FQDN を使用して設定された Syslog ターゲットによってネットワークが停止する可能性がある
CSCvt57027	ISE 2.6p5 の認証ステータス API コールが空白の出力を返す
CSCvt57571	IP-access がエントリなしで送信された場合、App-server がクラッシュする
CSCvt57805	REST API 更新操作の断続的なパスワードルールエラー
CSCvt61181	ISE ERS API：SNMP 設定の処理中のネットワークデバイスの GET コールが遅い
CSCvt71559	アラームダッシュレットに「データが見つかりません（No Data Found）」と表示される
CSCvt85722	動作していない MNT ウィジェットのデバッグログがない
CSCvt87409	ISE DACL 構文チェックで IPv4 形式エラーが検出されない

不具合 ID 番号	説明
CSCvu10009	req 格納ファイルの /ers/config/internaluser/name/{username}makes id&password&name mandatory の PUT verb
CSCvu14634	2.6p3 からのバックアップ復元後、2.6p5 /p6 で EAP TLS 認証が失敗する
CSCvu42244	EAP-TLS を介したマシン認証が、ユーザが見つからないというエラーを示して許可フロー中に失敗する

Cisco ISE リリース 2.6.0.156 の未解決の不具合：累積パッチ 7

不具合 ID 番号	説明
CSCvv41074	2.6p7 で ojdbc の複数のバージョンを使用すると、ライセンス/管理/展開の問題が発生します。

Cisco ISE リリース 2.6.0.156 の解決済みの不具合 - 累積パッチ 6

次の表に、リリース 2.6 累積パッチ 6 の解決済みの不具合を示します。

パッチ 6 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCvi35647	マルチノード展開では、ポスチャセッション状態を PSN 間で共有する必要がある
CSCvp05303	プロビジョニングされた証明書が失効後に削除されない
CSCvs82557	SXP バインディングが pxGrid 2.0 クライアントに公開されない

Cisco ISE リリース 2.6.0.156 の新機能：累積パッチ 5

Cisco AI エンドポイント分析サポート

Cisco AI エンドポイント分析は、エンドポイント プロファイリングの忠実度を改善する Cisco DNA Center のソリューションです。きめ細かいエンドポイント識別を提供し、さまざまなエンドポイントにラベルを割り当てます。ディープ パケット インスペクション、および Cisco ISE、Cisco SD-AVC、ネットワークデバイスなどのソースからのプローブによって収集された情報は、エンドポイント プロファイリングのために分析されます。

Cisco AI エンドポイント分析は、人工知能と機械学習機能を使用して、同様の属性を持つエンドポイントを直感的にグループ化します。IT 管理者は、これらのグループを確認してラベルを

割り当てることができます。割り当てられたエンドポイントラベルは、Cisco ISE アカウントがオンプレミスの Cisco DNA Center に接続されている場合、Cisco ISE で使用できます。

Cisco AI エンドポイント分析の結果割り当てられたエンドポイントラベルは、Cisco ISE 管理者がカスタム認証ポリシーを作成するために使用できます。それらの認証ポリシーを使用して、エンドポイントまたはエンドポイントグループに適切なアクセス権限のセットを提供できます。

Cisco ISE リリース 2.6.0.156 の未解決の不具合 - 累積パッチ 5

Cisco ISE 2.6 パッチ 5 をインストールすると、CSCvt36324 によって追跡されている問題が原因で、SSID に基づくゲスト認証が失敗することがあります。失敗した場合は、次のコマンドを実行します。

```
show running-config
```

ホスト名が使用可能かどうかを確認します。ホスト名が使用できない場合は、Cisco TAC に連絡してこの問題をトラブルシューティングします。

不具合 ID 番号	説明
CSCvt36324	CARS 設定からホスト名が欠落しているため、リダイレクトしない
CSCvt36452	ISE の評価プロファイラライセンスが期限切れになると、デフォルトの radius プローブが有効になる

Cisco ISE リリース 2.6.0.156 の解決済みの不具合：累積パッチ 5

次の表に、リリース 2.6 累積パッチ 5 の解決済みの不具合を示します。

パッチ 5 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCux25333	ISE ダッシュボードでは、特殊文字の < > ? " を使用できます。
CSCux25342	[ライブセッション（Live Sessions）] ウィンドウの [セッションステータス（Session Status）] 列でカスタムフィルタが機能しない
CSCuz18895	CoA REST API が ASA VPN セッションで動作していない
CSCvc71503	エンドポイントはスタティック グループの割り当てを失う
CSCve89689	MNT API が特殊文字をサポートしない

不具合 ID 番号	説明
CSCvf59076	ライブセッションで、VPN とポスチャシナリオに誤った認証プロファイルと認証ポリシーが表示される
CSCvf94942	シェルプロファイルに VSA がある場合、ルールに定義されたコマンドセットがないときは、明確な説明なしに TACACS 認証ルールが失敗する
CSCvh86082	解析する NMAP smb-os-discovery データの削除または \x00 を実行する必要がある
CSCvj43999	自己署名アカウントの作成エラー：「アカウント情報のテキストを入力しようとしましたが、失敗しました（An attempt to text your account information to you has failed）」
CSCvj67437	procps-ng の複数の脆弱性
CSCvj88164	リモートアクセス VPN を使用したポスチャ済みセッションのライセンスの使用が誤っている
CSCvk48115	ISE 2.3 RSA SecurID 認証が失敗する
CSCvk50684	ホスト名の変更後に証明書を削除できない
CSCvm46997	openssh の複数の脆弱性
CSCvm56657	AnyConnect が誤ったユーザエージェントを送信しているため、ポスチャフロー後に Windows 7 が誤ってプロファイリングされる
CSCvn55560	ISE 2.3 パッチ 5 の適用後、EOB ゲストユーザが作成されない
CSCvn73729	AMP アダプタを使用した脅威イベントのパブリッシュ中にエラーが発生した
CSCvo02285	isemntlogproc について /var/log/secure にエラーが 10 秒ごとに表示される
CSCvo22887	ISE 2.4 URT は、ノードがサポートされているアプライアンス上にあるかどうかを確認しない
CSCvo28578	ISE 2.3：一部の NAD のネットワーク デバイス グループでロケーション情報と IPSEC 情報の順序が逆になる
CSCvo47391	krb5 の複数の脆弱性
CSCvo49755	CLI clock timezone コマンドを有効にする
CSCvo82930	ProfilerCoA：Profiler.log に getting Policy details Exception の例外が表示される
CSCvo87602	バージョン 2.4.44 を実行している openldap rpm を使用した ISE ノードでのメモリリーク

不具合 ID 番号	説明
CSCvo90281	Web GUI を介したアップロードが中断された場合、アップグレード中に 1 GB を超えるパッチアップロードファイルが削除されない
CSCvo90380	アカウントの拡張時に、スポンサー承認型ゲストアカウントの開始日が調整されない
CSCvp07591	UTF-8 検証チェックの失敗により、EAP-GTC マシン認証がパスワードの不一致で失敗する
CSCvp12685	クロスサイト リクエスト フォージェリ（CSRF）[OWASP_CSRFTOKEN バイパス]
CSCvp19539	ゲストポータルの第 2 要素の Radius トークンサーバ認証を使用した ISE 2.2 サインインボタンがグレー表示される
CSCvp19738	認証または認証ポリシーに基づいて ISE 2.4 のライブセッションをフィルタリングできない
CSCvp20910	ISE 2.2 で、シスコスマートライセンスのクライアントエージェントが待機状態の場合、GUI のログイン遅延が発生する
CSCvp24085	セカンダリ管理者ノードの ISE 2.4 の CPU 使用率が高い
CSCvp35021	外部 CA がシステム証明書に署名すると、信頼できるページから CA を削除できるようになる
CSCvp40509	PrRTCpmBridge が検出したユーザを返しても、prrt-server で内部ユーザが断続的に検出されない
CSCvp52008	IETF ディクショナリ属性の Ascend-Client-Primary-DNS がアップグレード後に破損する
CSCvp70644	期限切れのゲストアカウントの消去がサマータイムの変更後に停止する
CSCvp73335	calling-station-id に CLIENTVPN が含まれている場合、Radius セッション詳細レポートが破損する
CSCvp91987	不正なジョブ（HOURLY_STATS_JOB）が実行されている
CSCvq07756	IPv6 アドレスが含まれている場合、ISE へのネットワークデバイスのインポートに時間がかかる
CSCvq30417	リポジトリをエクスポートするためのオプションを使用した MnT の消去が機能していない
CSCvq40899	中間 CA CSR で外部 CA 証明書をバインドすると、証明書チェーンが CA ページで破損する

不具合 ID 番号	説明
CSCvq49292	30 日よりも前の ISE TACACS 認証とアカウンティングのレポートが欠落している
CSCvq50182	CTS pac が期限切れになると、ISE がロギングを表示しない
CSCvq61878	CVE-2018-20685 の ISE の評価
CSCvq69138	90140 INFO PassiveID のロギングレベルの変更：デバッグのためのメッセージ解析済みの syslog
CSCvq80132	ページをまたがる IP SGT の静的マッピングのトラッシングが完了しない
CSCvq83410	最大スレッド値の制限が低すぎるため、「管理スレッドプールがしきい値に到達しました（Admin thread pool reached threshold value）」というアラームがトリガーされる
CSCvq88821	アクセスポイントに接続されたアクセススイッチ上の SNMP トラップによって不正なプロファイリングが発生する
CSCvq96801	すべての SNMP パケットが /var/log/messages ファイルに記録される
CSCvq97641	ISE 2.4 localhost-<date>.log ファイルのサイズが 8 Gb 以上に増加している
CSCvq98277	ASA CLI を介して ISE 内部ユーザ有効化パスワードをユーザが変更するとパスワード監査が生成されない
CSCvq99963	アクティブセッション数が 200K を超えた場合にしばらくすると、パッシブ ID ダッシュボードでアプリケーションサーバのクラッシュが確認される
CSCvr00348	条件別ポスチャ評価レポートに空のレコードが表示される
CSCvr06487	ISE ポスチャエージェントのプロファイルで空の修復タイマーを使用できない
CSCvr07263	消去ルールを作成すると、plus ライセンスがない場合は Radius ディレクトリがハングする
CSCvr07464	IP アドレスまたはポートが使用されている場合、ISE 2.6 MUD URL が正しく解析されない
CSCvr08988	外部 Radius のシナリオで、アクセスチャレンジを NAD に転送する前に、ISE が状態属性を置換する必要がある
CSCvr09759	証明書が Oracle から NSSDB に適切にロードされていない
CSCvr11769	ISE 2.4：高度なカスタムフィルタオプションと、レポートのエクスポートが予期したとおりに機能しない

不具合 ID 番号	説明
CSCvr12350	「MDM：MDM サーバへの接続に失敗しました（MDM: Failed to connect to MDM server）」というログエントリにエンドポイント情報を含める必要がある
CSCvr13218	IPv6 アドレスが ::xx 形式の場合、Framed-Interface-Id RADIUS 属性が access-accept に送信されない
CSCvr13464	ISE ERS SDK NetworkDeviceGroup PUT が API コールの ID 配置を表示しない
CSCvr13481	ISE ERS SDK NetworkDeviceGroup の削除で ID の場所が指定されない
CSCvr13649	pxGrid XMPP GCL 再接続の失敗
CSCvr24458	ネットワークデバイスの POST API ではデバイスのモデル名に文字とスペースを使用できるが、GUI では使用できない
CSCvr25197	UCP を使用してパスワードを変更した後、「ユーザ変更パスワードの監査（User change password audit）」レポートに「ID（Identity）」がない
CSCvr29863	ISE と Cisco DNA Center を統合すると、特殊文字の & と \ の両方が秘密値に含まれている場合はネットワークデバイスが ISE に表示されない
CSCvr31312	IP/マスクでのフィルタリング中に ISE がネットワークデバイスのページをロードできない
CSCvr32199	Systemd 脆弱性 RHEL 7 RHSA-2019:0049
CSCvr35154	読み取り専用管理者ユーザが TrustSec デバイス設定クレデンシャルを表示できない
CSCvr35719	すべての tenable アダプタリポジトリを取得できない
CSCvr36392	日本語でのネットワークデバイスの説明
CSCvr38857	カスタマーフィルタを使用すると、Radius認証レポートにログが欠落する
CSCvr40359	ISE がエンドポイントデータベースで device-public-mac 属性を使用していない
CSCvr40574	秘密キーの暗号化に失敗すると、ISE GUI でエクスポートが失敗する
CSCvr46529	カイブパスワードを持つ内部ユーザのパスワードライフタイムの期限切れリマインダが表示される
CSCvr47215	ACS 5.7 から ISE 2.6 への移行で authzation プロファイルがインポートされない

不具合 ID 番号	説明
CSCvr48043	エクスポートされた TACACS デバイスの場合、複数共有の秘密フィールドが入力される
CSCvr48101	予期しない CoA が SCCM MDM で観測される場合がある
CSCvr48729	マイデバイスポータルにアクセスできない
CSCvr50921	類似の内部ユーザが無効になっている場合に、AD ユーザとの GUI ログインに失敗する
CSCvr51940	ISE が AD でマシンアカウントを正しく検索していない
CSCvr51959	ISE 2.4：誤った FQDN の一致が原因でユーザに誤ったスポンサーポータルが提示される
CSCvr53428	パッチ 2.3 p7 のインストール後に ISE サービスが起動しない
CSCvr57378	DHCP メッセージによってエンドポイントがアクティブとしてマーキングされるため、アクティブなエンドポイント数が増加する
CSCvr60339	[カウンタの時間制限（Counter Time Limit）] タブの [最大セッション数（Max Sessions）] ウィンドウに入力ミスがある
CSCvr61108	セッション ID に対する PxGrid ANC API のサポート
CSCvr62517	ISE 2.4 p9：セッションディレクトリの書き込みに失敗した：文字列インデックスが範囲外：-1 アラームが展開に表示された
CSCvr63504	システム証明書を参照しているため、SCEP プロファイルを削除できない
CSCvr64067	ISE MnT が 90% の消去後にライブログの表示を停止する
CSCvr67988	ゲストのパスワードの表示/印刷が無効になっている場合でも、ISE スポンサーの電子メールがゲストクレデンシャルの電子メールに CC される
CSCvr68971	ISE IP ルーティングの優先順位の問題
CSCvr70581	RADIUS 認証詳細レポートに Called-Station-ID がない
CSCvr71796	SCCM フローに SCCMException と表示され、MDMServerReachable 値が MDMServersCache に false として更新される
CSCvr77321	WSA が AD グループではなく SID を ISE から受信する
CSCvr81522	McAfee や Symantec など、一部の AM 製品の定義日が誤表示される
CSCvr83696	アカウント OU の変更後、ISE がキャッシュ済みの AD OU を新しい OU よりも優先させる

不具合 ID 番号	説明
CSCvr84125	あるプラットフォームから別のプラットフォームへの設定の復元で、sec_hostconfig テーブルの UDI 設定が誤っている
CSCvr84143	ISE ゲスト OS で tzdata を更新する必要がある
CSCvr84978	ISE LDAP バインドテストでは、ノードごとに定義されている場合は正しいサーバが使用されない
CSCvr86380	TrustSec マトリックス CSV が、すでに GUI で EMPTY になっている EMPTY SGACL でインポートされたときのレプリケーションアラーム
CSCvr87936	有効な Base ライセンスと Plus ライセンスのコンプライアンス違反が表示される
CSCvr90773	ライブログの「5436 通知 RADIUS：RADIUS パケットはすでにプロセスにあります（5436 NOTICE RADIUS: RADIUS packet already in the process）」というメッセージに誤ったユーザ名が表示される
CSCvr95948	接続の切断後に ISE が外部 syslog 接続を再確立できない
CSCvr96003	SYSAUX テーブルスペースが AWR および OPSSTAT データでいっぱいになる
CSCvr96189	NDG デバイスの参照が ISE DB から削除されないため、NDG の削除が妨げられる
CSCvr98395	IP ベースのプロファイルポリシーのプロファイル CoA がない
CSCvs01924	パスワードの期限切れのため、ERS 管理者アカウントが不適切に無効になる
CSCvs01949	ISE メッセージングサービスが basic_cancel という理由でキューリンクエラーのアラームをトリガーする
CSCvs02166	API コールと GUI に異なる結果が表示される
CSCvs03195	最大セッションカウンタの有効期限オプションが機能しない
CSCvs03810	ユーザ名の入力が 2 回異なると、ISE は RADIUS レポートに正しいユーザを表示しない
CSCvs03998	ISE 2.3 p6 LDAP テストの GUI フロー（複数の結果を含む）では、実行時に観測されたエラーが生成されない
CSCvs04047	ERS API を使用して作成した認証プロファイルが GUI の「ASA VPN」フィールドと一致しない
CSCvs04433	TACACS+ の PSN クラッシュ

不具合 ID 番号	説明
CSCvs05104	エンドポイントのデフォルトの間隔を無効にすると、最大時間フレームが 60 分に設定される
CSCvs07344	正常に終了しているにもかかわらず、2.4 パッチ 9 のリセット設定がいくつかのエラーをスローする
CSCvs12409	ゲストユーザの有効日数の ISE ゲスト作成 API 検証に時間が考慮されない
CSCvs14297	PassiveID：$ 文字を含む AD アカウントパスワードを使用して WMI を設定するとエラーがスローされる
CSCvs24704	LDAP ID ストアの破損アラーム：機能拡張
CSCvs25258	ブルートフォースのパスワード攻撃に対する動作を改善する
CSCvs27310	ISE 2.6 と 2.7：dACL の説明フィールドに ' の文字を追加できない
CSCvs36036	ISE 2.6 では、ユーザが IPv4 または IPv6 を選択しても、dACL シンタックスに複数の空白行が許可される必要がある
CSCvs36150	ISE 2.x ネットワーク デバイス スタックのローディング
CSCvs41571	自己登録済みゲストポータルがゲストタイプの設定を保存できない
CSCvs42072	静的グループの割り当てを編集できない
CSCvs51296	ISE では、コマンドセットのコマンドの前にスペースを挿入できる
CSCvs51537	暗号化キーの特殊文字でバックアップがトリガーされない
CSCvs53148	複数のエンドポイントが 1 秒ごとにプロファイリングされ、ISE ノードが同期しなくなる
CSCvs59955	ポート 15672 が使用中のとき、RabbitMQ コンテナを起動できない
CSCvr76574	内部ユーザが外部パスワードで設定されていると、認証機能の有効化が中断する
CSCvp54240	HSTS がルートフォルダに実装されていない
CSCvr70044	高負荷時に ISE ポスチャモジュールに「ポリシーサーバなし（No policy server）」エラーが表示される
CSCvt18276	破損したエンドポイント：不正なエンドポイントに関連付けられている属性

Cisco ISE リリース 2.6.0.156 の新機能：累積パッチ 3

マルチ DNAC のサポート

Cisco DNA Center システムは、25,000 ー 100,000 のエンドポイントの範囲を超えて拡張できません。Cisco ISE は 200 万エンドポイントまで拡張できます。現在、1 つの Cisco DNA Center システムと 1 つの Cisco ISE システムのみを統合できます。大規模な Cisco ISE 展開では、複数の DNA Center のクラスタを 1 つの Cisco ISE に統合することでメリットが得られます。シスコは、Cisco ISE 展開ごとに複数の Cisco DNA Center のクラスタ（マルチ DNAC とも呼ばれる）をサポートするようになりました。

ビジネス成果：Cisco DNA Center のアクセス制御アプリケーションのこの機能を使用すると、1 つの Cisco ISE システムに最大 4 つの Cisco DNA Center クラスタを統合できます。

Cisco ISE リリース 2.6.0.156 の解決済みの不具合：累積パッチ 3

次の表に、リリース 2.6 累積パッチ 3 の解決済みの不具合を示します。

パッチ 3 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCvd16468	「不明な SGT がプロビジョニングされました（Unknown SGT was provisioned）」というメッセージに NAD 情報がない
CSCvd48081	ソフトウェアが ISE ノードでの pxGrid 証明書の削除を許可すべきではない
CSCvf45991	AD での疑似二重認証要求
CSCvg60477	ISE 2.3+ に認証条件 Network Access:AuthenticationMethod がない
CSCvg65262	ISE の簡単なワイヤレスセットアップ：SAW のセキュアなアクセスウィザードが wlc コード >8.3 で機能しない
CSCvi72862	ISE：抑制のためのアカウンティング更新の許容度の効率を引き上げる必要がある
CSCvj67166	TLSv1.2 でサポートされるサーバ暗号には 2048 ビットオプションが必要
CSCvk52874	EAP チェーンのコンテキストで想定される値が ISE から提供されない
CSCvk53782	ISE ENH：RADIUS ディクショナリの VSA で 2 バイトの ベンダー属性サイズフィールド長が許可される
CSCvm73337	SSL 接続に 1024 ビット以下の Diffie-Hellman 係数を持つ暗号を削除する

不具合 ID 番号	説明
CSCvm81230	Cisco Identity Services Engine（ISE）の任意のクライアント証明書作成時の脆弱性
CSCvn21926	ise バージョンに関係なく、脅威中心型 NAC CTA 設定でパーサー エラーが検出される
CSCvn66106	cloudpost IND からプッシュされた場合、ISE カスタム属性がエンドポイントに適用されない
CSCvn70558	MDMServerReachable が SCCM MDM に対して再度機能しない
CSCvn79043	ISE 2.4 ライブ ログがフィルタリングされない
CSCvo04342	ackson-databind の複数の脆弱性
CSCvo07993	パッチの適用前に追加した場合、tc-nac を無効/有効にすると Qualys が接続済み状態を表示する
CSCvo24097	[次の条件で無効なユーザ名を開示（Disclose invalid username by）] が常に動作していない無効な名前設定を表示する
CSCvo29478	参照されていないのに ISE 2.3 P5 ISE は GUI から SGT タグを削除することができない
CSCvo30170	ゲスト ポータルのクライアント プロビジョニング カスタマイズ テキストが保存されない
CSCvo33696	内部ユーザがネットワーク デバイスに正常にログインした後、ISE 2.4 が failedLoginAttempts をリセットしない
CSCvo51295	ISE 2.2 スポンサー：承認リンクを 2 回クリックすると、シングル クリック承認で誤ったメッセージが表示される
CSCvo64085	MnT のバックアップに必要なスペースの計算を再検証する必要がある
CSCvo94666	ISE 2.4 P5：プロファイリング：Netflow プローブが ISE の結合されたインターフェイスで動作していない
CSCvp00421	ISE プロファイラの SNMP 要求失敗アラームに失敗の理由が表示される
CSCvp01553	大規模な NAD（>300）を MatrixA と MatrixB 間で移動すると、シリアル化またはバッチ処理されない
CSCvp02082	TrustSec-ACI の統合が有効になっていると、Env データが欠落する
CSCvp03249	ISE：電子メール通知を送信する SMTP サーバが枯渇する
CSCvp22075	CSRF トークンを必要とする ERS API が PUT/POST/DELETE で常に失敗する

不具合 ID 番号	説明
CSCvp28377	外部管理者権限の変更が展開内の他のノードに反映されない
CSCvp33598	MACアドレスが同時に2回削除されると、ISEがすべてのエンドポイントを削除する
CSCvp45598	SystemTest：SCEP RA プロファイルの削除中にエラーが発生する
CSCvp46165	AnyConnect_ISEPosture.txt でポスチャのリダイレクトが「ピアを確認できません（unable to determine peer）」エラーで失敗する
CSCvp47029	CTA の脅威情報を備えた ISE 2.4 で、脅威エンドポイントが検出されない
CSCvp51033	GUI コンテキストの可視性レポートのエクスポートの速度が低下する
CSCvp54424	AD 診断ツールが低レベルの API クエリに失敗したことを表示するが、応答に回答が含まれていないDNS 設定の確認
CSCvp56265	設定されたサーバに到達できない場合に MDM サーバを無効にできない
CSCvp58616	SQLite FTS3 クエリ処理整数がオーバーフローする脆弱性
CSCvp62113	NMAP スキップ ホスト ディスカバリおよびNMAP スキャン タイムアウトが適用される
CSCvp63038	システムテスト：Temporial Agentのインストールが内部システムエラーで失敗する
CSCvp65586	[pxGrid XMPP サーバ] TCP/5222 のセキュアでない Diffie-hellman プライム p 1024 ビット
CSCvp73076	ログ収集エラー：AD プローブ セッションが挿入されると、セッション ディレクトリの書き込みに失敗する
CSCvp73385	AD で KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN がスローされると、認証の開始が失敗する
CSCvp74154	権限エラーのためエンドポイントデータベースからエンドポイントを削除できない
CSCvp75207	2.4 P8/P9 証明書チェーンがパッチ 8 とパッチ 9 にインポートされない
CSCvp77008	有効なカスタム属性の後に設定すると、CV のカスタム属性の下に ISE LogicalProfile が表示される
CSCvp77014	ISE TrustSec カスタムビューが手動順序で正しく並べ替えられない
CSCvp83214	API を介した ISE ERS の作成では指定された ID が使用されない

不具合 ID 番号	説明
CSCvp88443	新しい論理プロファイルが認証ポリシーの例外で使用されている場合でも、ISE CoA が送信されない
CSCvp88940	認証プロファイルの実行中にエンドポイントグループの説明を使用できない
CSCvp96921	Cisco Identity Services Engine のストアドクロスサイトスクリプティングの脆弱性
CSCvp98834	Cisco Identity Services Engine のストアドクロスサイトスクリプティングの脆弱性
CSCvp98851	Cisco Identity Services Engine クロスサイトスクリプティングの脆弱性
CSCvq04802	ISE が SAML 認証応答トークンを処理できない
CSCvq08423	SubCA と PKCS12（単一ファイル）としての ISE による証明書プロビジョニングポータルのエラー
CSCvq14925	更新された自己署名証明書が信頼ストアで更新されない
CSCvq15329	スケジュール バックアップの復元に失敗した
CSCvq17464	ERS--ISE 経由で外部パスワード ID ストアを使用して内部ユーザを更新できない
CSCvq19039	ISE が大規模なポリシーセットの設定変更を保存できない
CSCvq21272	パスワードのリセット後に誤ったパスワードが通知される（SMS でのみ）
CSCvq24877	グループ ID の前または後ろにスペースがある場合、CEPM.REF_ROLE_MASTER で ORA-02291 を使用すると作成できない
CSCvq27110	PSN サーバのコアファイルによってディスク使用率が高いというエラーが発生する
CSCvq29336	セッション ID に「-」が含まれていると、「問題が発生しました（Oops. Something went wrong）」と ISE に表示される
CSCvq33194	オプションの [常に使用（Always use）] を使用してゲストポータルの言語を変更できない
CSCvq35826	[最大セッション数（Max Sessions）]ページの [カウンタの時間制限（Counter Time Limit）] を更新している間に不正な監査レポートが生成される
CSCvq38085	プライマリ PAN に到達できないときに「サーバの問題によりポスチャが失敗しました（Posture failed due to server issues）」というエラーでポスチャが失敗する

不具合 ID 番号	説明
CSCvq38610	pxGrid 単独ペルソナの pxGrid の場合、証明書信頼チェーンが完全にならない
CSCvq39759	ISE PAN フェールオーバーの非アクティブ日数 = 経過日数によって EP が誤って消去される
CSCvq42847	ISE：MAC OSX でのシステムスキャン時に「サーバの問題によりポスチャが失敗しました（Posture failed due to server issues）」というエラーが発生する
CSCvq45008	ISE が設定済みのカスタムグループに自己登録エンドポイントを保存しない
CSCvq46232	ISE 2.6 ACI 統合 Trustesec ACI レポートが ip-sgt のマッピングを ACI に送信しない
CSCvq50088	RBAC を使用すると、ネットワーク デバイス グループのエクスポート機能が失敗する
CSCvq51955	ネットワーク条件が短縮された IPv6 では機能しない
CSCvq52317	Cisco Identity Services Engine のストアド クロスサイト スクリプティングの脆弱性
CSCvq52340	ネットワーク アクセス ユーザの [すべて削除（Deleting All）] が監査レポートに表示されない
CSCvq52402	Cisco Identity Services Engine 情報の開示の脆弱性
CSCvq54061	MNT ノードでシステムの概要を使用できない
CSCvq54153	Cisco Identity Services Engine のポリシー設定名のクロスサイト スクリプティングの脆弱性
CSCvq54533	管理者または pxGrid の使用率での ECDSA 署名済み証明書を使用すると pxGrid が破損する
CSCvq56241	ユーザ名に無効な文字が含まれていると ISE ユーザのインポートが失敗する
CSCvq56281	ISE ゲストポータルが 2 つの疑問符を持つ http 要求を解析できない
CSCvq58785	一部のシナリオで、静的グループ情報が EP から失われる
CSCvq62367	MNT への接続がない場合は、PSN がスケジュール設定されたレポートを生成する
CSCvq63279	パッチポップアップの実装

不具合 ID 番号	説明
CSCvq65220	ISE 2.6：CSCvi89085 の修正で detectMACAuthenticationOnPAP フローが中断する
CSCvq66846	[マッピンググループに移動（Move to Mapping Group）] ドロップダウンメニューで SGT マッピンググループを 25 に制限する
CSCvq69142	PassiveID エージェント：エージェントモニタリング DC がダウンすると、MnT に syslog メッセージが送信されない
CSCvq69228	pxGrid コントローラが terracotta.org に接続している
CSCvq71264	ゲストフローからの静的グループ割り当てが失われる
CSCvq71844	すべてのプロファイラポリシーで「キャッシュが正しく初期化されません（Cache not properly initialized）」メッセージが表示され、プロファイラフィードを更新できない
CSCvq72760	管理ユーザのパスワードを更新すると、現在のパスワードの入力をバイパスできる
CSCvq73316	ISE 2.4 p9 の猶予期間が VPN ユースケースの PRA で機能しない
CSCvq74649	ISE スポンサーポータル：作成日による並べ替えが機能しない
CSCvq74995	名前に「/」が含まれている場合の ISE 2.4 による証明書属性メッセージ内の XSS 入力の可能性
CSCvq77051	Restful API を介して追加されたネットワークデバイスが「ネットワークデバイスが見つかりません（'Network Device not located）」というエラーで認証に失敗する
CSCvq78489	ACS から ISE への migtool が意図した認証ポリシーの結果を変更する
CSCvq79598	IPv6 RADIUS 属性を外部属性にマッピングできない
CSCvq80211	マッピングデータのないエントリの場合、IP SGT 静的マッピングのエクスポートが失敗する
CSCvq81381	トークンパスワードを使用している内部ユーザがパスワードの期限切れにより無効になる
CSCvq83678	ise.messaging.log がサポートバンドルまたは GUI に表示されない
CSCvq83700	不要な JQUERY-UI ファイルを ISE から削除する
CSCvq85414	iOS CNA ブラウザでリンクが機能しない場合のログインページ AUP
CSCvq86848	アクセスが NDG に制限されている場合は、[別のグループへのデバイスの移動（Move devices to another group）] ボタンを無効にする必要がある

不具合 ID 番号	説明
CSCvq97680	ISE 2.6 パッチ 2：エンドポイントグループに一致しない EAP-TLS 認証
CSCvr13444	REST API：パスワードフィールドでの特殊文字（「/」）を使用したネットワークデバイスの作成は UTF と解釈される
CSCvr27905	ISE が NMAP スキャン情報の解析に失敗する
CSCvr39672	ISE 2.7 ベータ：エンドポイントの説明に無効な文字があるため、マイデバイスポータルのロードに失敗する
CSCvr41265	ISE 3695 アプライアンスに、Super MNT に設定されている Oracle パラメータに関する問題がある
CSCvr43077	Day0：iPad OS 13.1 BYOD フローが失敗した
CSCvr64000	ホスト名の変更によって ISE メッセージングの問題が発生する：MNT Failover and Queue Link Error-basic_cancel

Cisco ISE リリース 2.6.0.156 の未解決の不具合：累積パッチ 3

不具合 ID 番号	説明
CSCvs04092	pxGrid V2 クライアントで SGT 通知が欠落している

Cisco ISE リリース 2.6.0.156 の新機能 - 累積パッチ 2

ISE メッセージングサービスを介した syslog

UDP syslog（組み込みの UDP syslog ターゲットの LogCollector および LogCollector2）は、デフォルトで現在有効になっている既存の **ISE メッセージング サービス** インフラストラクチャを使用して、モニタリングノードに配信されます。これにより、syslog メッセージの WAN 存続可能性が高くなります。この機能を使用するには、すべてのノード間のファイアウォール（存在する場合）で TCP ポート 8671 を開いていることを確認してください。

このオプションを無効にすると、UDP ポート経由で UDP syslog を配信できます。これを行うには、Cisco ISE GUI で [管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ログ設定（Log Settings）] ページに移動し、[UDP syslogをMnTに配信するためにISEメッセージサービスを利用する（Use ISE messaging Service for UDP syslog delivery to MnT）] オプションをオフにします。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 2.6』を参照してください。

ビジネスの成果

モニタリングノードにアクセスできない場合でも、運用データが一定期間保持されます。

Elevated System Administrator ロールのサポート

Elevated System Administrator ロールは、既存の System Administrator ロールに似ています。加えて、このロールでは、ネットワーク管理者ユーザを除く管理者ユーザを作成、削除、および更新できます。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 2.6』を参照してください。

ビジネスの成果

Elevated System Administrator は管理者ユーザを管理できます。

Cisco ISE リリース 2.6.0.156 の解決済みの不具合 - 累積パッチ 2

次の表に、リリース 2.6 累積パッチ 2 の解決済みの不具合を示します。

パッチ 2 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCuw55841	カスタム管理者が他の制限付き管理者ユーザを作成できない
CSCvb56579	[SXPデバイス（SXP Devices）] ページで名前の 14 文字を超える部分が表示されない
CSCvc77960	承認されていないアクセスに対して、空白ページの代わりに、わかりやすい情報メッセージを表示する必要がある
CSCvg03526	パッチのインストールで「アプリケーションパッチのインストール失敗（Application patch installation failed）」というアラームが生成される場合がある
CSCvh22907	スポンサーポータルページのロードに 10 秒以上かかる
CSCvh64185	セッション通知で、ADNormalizedUsername、ADUserResolvedIdentities の各フィールドに不正な値が出力される場合がある
CSCvi51291	初回認証から 2 日後に ISE CoA が動作しなくなる
CSCvk76680	ISE-PIC 自己署名証明書の削除操作が、セキュアな Syslog サーバの参照エラーが原因で失敗する
CSCvm00481	Web UI で内部認証局を無効にしても、コマンドラインで CA サービスがまだ実行されている

不具合 ID 番号	説明
CSCvn15748	ISE ゲストフローの最大セッション制限で、サードパーティ NAD との CoA 接続解除が送信されない
CSCvn44171	外部パスワードを使用するネットワーク アクセス ユーザを ISE 管理者として使用できない
CSCvn51282	ISE が「ip:」を「ip:inacl」Cisco AV ペアの該当するホスト名に置き換える
CSCvn60787	アラーム固有の電子メール設定に電子メールが送信されない
CSCvn73740	エンドポイントプロファイルが不明に設定されていない EAP-TLS 認証は、2 番目の認証で失敗する。
CSCvn79569	ISE のアプリケーションステータスが初期化状態である
CSCvn92246	ISE：tacacs ユーザがグループなしで保存されている場合、管理者ユーザがグループを削除または変更できない
CSCvn92528	ISE 2.4：サプリカントクエリが誤って設定されているため、両方の MNT ノードの CPU 使用率が高くなる
CSCvo14624	ISE メッセージングサービスがオンになっている場合に、高い TPS レートで遅延が観測される
CSCvo17704	ISE 2.4：CLI パスワードに 3 $ を指定できない
CSCvo28092	ISE カスタムエンドポイント属性：保存も削除もされない
CSCvo45582	内部管理者のサマリーレポートで特定のカラムを選択できない
CSCvo45768	PSN フェールオーバーケースで PrA をサポートするための設定が追加される
CSCvo50638	TCNAC アダプタを 2.2 から 2.6 にアップグレードした後に設定できない
CSCvo59928	ISE 2.6 ANC ポリシーの適用時に SMC でエラー「microservice_unavailable」が表示される
CSCvo77219	スポンサーゲストポータルのレート制限時間が適用されない
CSCvo78051	許可されるプロトコル：[ポリシーセット（Policy Sets）] ページでインラインの許可されるプロトコルを作成する際のエラー
CSCvp07591	UTF-8 検証チェックの失敗により、EAP-GTC マシン認証がパスワードの不一致で失敗する
CSCvp12131	ISE 2.4 パッチ 6 をリロードすると、バックアップが中断される

不具合 ID 番号	説明
CSCvp13378	PassiveID フローでユーザの SamAccountName と ExplicitUPN を送信する必要がある
CSCvp14725	半数のセッションで ADNormalizedUserName フィールドが欠落している
CSCvp16734	Plus ライセンスが Plus 機能なしで消費される
CSCvp18692	AD_User_Fetch 情報が UI および Redis で表示されない
CSCvp28382	複数選択で複数の管理者グループを削除することができない
CSCvp29197	NAD IP アドレスが無効なため、ISE 2.4p3 Radius ライブログが表示されない
CSCvp29413	外部 RADIUS サーバへの要求で送信する Radius 属性の変更が ISE で機能しない
CSCvp29572	Pxgrid プロファイリングプローブの有効化を保存しても、有効にならない
CSCvp30958	外部サーバ遅延シナリオでの記述子割り当ての枯渇により ISE で要求がドロップされる
CSCvp33593	ISE がエンドポイント ID グループ「不明」との認証ポリシーの照合に失敗する
CSCvp33862	カスタム属性（CV の詳細フィルタ）がリスクスコア（整数値）でフィルタ処理できない
CSCvp37101	AD 接続の問題が発生し、コアファイルが同じ日に生成される
CSCvp37238	TACACS/AAA ライブログレポートに ACI から行われた設定変更が表示されない
CSCvp39842	ISE 2.6 SFTP リポジトリへのアクセスが失敗する
CSCvp43302	ゲストタイプを削除すると、エラーが表示されて同じ名前の新しいゲストタイプを作成できなくなる
CSCvp45528	外部ルート CA による ISE CA 証明書への署名後にキューリンクエラーアラームが生成される
CSCvp50450	ISE 2.4 および 2.6 で ise-elasticsearch.log ファイルがパージされない
CSCvp52201	ISE 2.4：レプリケーション：クラスタ情報テーブルに古い FQDN が含まれる
CSCvp54773	タイムアウト後にスポンサーポータルで ISE 2.4 p6 400 エラーが発生する
CSCvp54949	IOS 12.2 で BYOD フローが破損している

不具合 ID 番号	説明
CSCvp58945	ネットワーク デバイス テンプレートをインポートすると、「暗号化キーへの無効な値により失敗しました（Failed illegal value for Encryption key）」というエラーが表示される
CSCvp59286	struts2-core の複数の脆弱性
CSCvp60359	アップグレードされた ISE ノードに LDAP ID ストアのパスワードがプレーンテキストで表示される
CSCvp61880	ユーザへの警告やエラーの表示なしに、認証プロファイルのインポートが失敗する
CSCvp65699	CSCvp63136：US399914：2.6 P2 - サードパーティライセンスと通知の表示 - リンクの更新
CSCvp65711	dot1x で設定されていない有線ネットワークに切り替わると、ISE 2.4 P8 ポスチャスキャンが実行される
CSCvp65816	「Cisco Modified」プロファイルがプロファイラ フィード サービスによって上書きされる
CSCvp68285	サポートへの問い合わせリンクから戻る際に AUP ゲストポータルエラー 400 が発生する（iPhone キャプティブポータル）
CSCvp72966	ゲストのパスワードの表示/印刷が無効になっている場合に電子メールがゲストに届かない
CSCvp75101	cisco-av-pair=addrv6=0x7f8c0d588608 を受信する際の ISE MNT 例外
CSCvp76617	ISE カスタマーエンドポイントの属性タイプ文字列で特定の数字を使用できない
CSCvp76911	ISE で複数マトリックスを使用している場合に展開ボタンが表示されない
CSCvp77941	Plus ライセンスの [ライセンスの使用状況（License Usage）] に 0 または誤った値が表示される
CSCvp83006	[コンテキストの可視性（Context Visibility）] - [エンドポイント（Endpoints）] からのエクスポートでほとんどのエンドポイントのカスタム属性が含まれない
CSCvp86406	[ソフトウェアバージョン（Software Version）] フィールドに、任意の数字とその後に () を続けて組み合わせてネットワークデバイスを追加することができない
CSCvp88242	Mydevice ポータルを更新する際の「[400] 不正な要求（[400] Bad Request）」エラー

不具合 ID 番号	説明
CSCvp93901	pxGrid で ADUserSamAccountName、ADUserQualifiedName、ADHostSamAccountName、ADHostQualifiedName を公開
CSCvq13341	ISE 2.6 パッチ 1 - AD のユーザテストが 0 グループを返す

Cisco ISE リリース 2.6.0.156 の未解決の不具合 - 累積パッチ 2

不具合 ID 番号	説明
CSCvq54061	MNT ノードでシステムの概要を使用できない
CSCvq69343	特定のシナリオで IP-SGT マップが ACI に伝播されない

Cisco ISE リリース 2.6.0.156 の解決済みの不具合 - 累積パッチ 1

次の表に、リリース 2.6 累積パッチ 1 の解決済みの不具合を示します。

パッチ 1 は古いバージョンの SPW で機能しない可能性があります。MAC ユーザは SPW を MACOSXSPWizard 2.2.1.43 以降にアップグレードする必要があります。また、Windows ユーザはその SPW を WinSPWizard 2.2.1.53 以降にアップグレードする必要があります。

不具合 ID 番号	説明
CSCvg70813	バックアップ試行に失敗しても、ISE dmp ファイルが /opt/oracle/base/admin/cpm10/dpdump から削除されない
CSCvh19430	ISE 2.x：インポートしたアカウントのゲストアカウントのアクティベーション時間が一致しない
CSCvi80094	CSRF トークンを必要とする ERS API が HTTP 403 の代わりに HTTP 404 を返す
CSCvj05563	仮想ネットワークマッピングを使用するセキュリティグループを削除できない
CSCvj31598	同じサブジェクト名を持つ 2 つの CA 証明書がインポートされる
CSCvj83747	BYOD、セキュアアクセス、スポンサードゲストフローの ISE セキュアアクセスウィザード簡易ワイヤレス null AD グループ
CSCvm01627	ISE 2.4 ERS API - PUT および GET 内部ユーザの「ユーザ カスタム属性」
CSCvm05840	NAD CSV インポートでサポート対象のすべての文字を許可する必要がある
CSCvm90478	RBAC ユーザを使用して ID グループにエンドポイントを追加しようとしたときに「利用可能なデータがない（No Data Available）」

不具合 ID 番号	説明
CSCvn40822	パッチ 5 以降の ISE 2.3 でゲストの作成に失敗する
CSCvn55640	スポンサーユーザが権限 ALL&GROUP スポンサーグループで設定されている場合、ACC コールを無制限に管理する
CSCvn58964	500 個の認証ポリシーを使用すると、ISE 2.4 のデータベース応答が低下する
CSCvn76567	ISE 2.4：ユーザセッションの SXP から IP-SGT バインディングが消える
CSCvn85484	SCEP RA プロファイルを削除すると、関連付けられている CA チェーンが信頼済みストアからサイレントに削除される
CSCvn92778	未使用の論理プロファイルを削除すると、誤った認可結果が生成される場合がある
CSCvn98932	存在しない DACL が ISE で検証されない
CSCvo05269	[ISE 2.4] 認可条件で作成されたプロファイルポリシーを使用できない
CSCvo09945	SFTP リポジトリからバックアップすると、変更時刻に誤った年が表示される場合がある
CSCvo11090	ISE で ACI IEPG を削除できる
CSCvo13269	ISE で SGT の追加が許可されていない
CSCvo15770	コンテキストの可視性でアドレスが HTML コードとして表示される
CSCvo18247	ISE：移行中に重複した framed-pool 属性をスキップできない
CSCvo19076	ISE エンドポイント消去 ACTIVEDIRECTORY ディクショナリがロードされていない
CSCvo24593	ISE の [すべてのSXPマッピング（All SXP Mappings）] ページでページネーションが機能していない
CSCvo41052	ISE が新しく作成された IP-SGT マッピングを削除する
CSCvo43289	ISE が「-」文字以降の SGT 名を切り捨て、バージョン ID を割り当てる
CSCvo61900	ISE 2.4 パッチ 7 を使用した MAC 組み込み FW 修復でシステムスキャンが内部エラーをスローする
CSCvo74441	ポート 15672 がすでに使用されている場合、RabbitMQ Docker コンテナが起動しない
CSCvo78171	ISE 2.4 パッチ 6 をインストールすると、スポンサーと MyDevices ポータルの FQDN が切断される

不具合 ID 番号	説明
CSCvo84948	ACS 5.8 から ISE 2.6 への dACL の移行に失敗する
CSCvo90393	Radius+PassiveID フローでの CoA 障害
CSCvp07364	ISE 2.0.1 パッチ 4 から 2.4 パッチ 6 へのアップグレード後に、CoA が ISE から発行されない
CSCvp23869	ISE TLS 1.0 および 1.1 セキュリティ設定は PxGrid に適用されないため、WSA が統合に失敗する
CSCvp48710	AD グループ名に「/.」または「/..」が含まれている場合、AD グループを追加できない
CSCvo31313	2.6 へのアップグレード後に一部の内部ユーザのパスワードを変更できない
CSCvo32279	SXP ロギングが「DEBUG」に設定されている場合、sxp.log に APIC ログには表示されない
CSCvo35144	ISE での SXP マッピングのクリアで遅延が発生する
CSCvo36769	ISE 2.6 で [EAP-TTLS設定（EAP-TTLS Settings）] ページが保存されない
CSCvo36837	パッチ 5 のインストール後、管理者グループが [デバイス管理（Device Administration）] タブの [ユーザ（Users）] にアクセスできない
CSCvo42165	デフォルトの python 変更パスワードスクリプトで CRUD 操作の例外が返される
CSCvo45606	ISE：WMI-Passed 値によって ISE のセキュリティが損なわれる場合がある。悪意のあるスクリプト用語を削除してください
CSCvo48352	RADIUS 認証レポートの CSV ファイルに重複するレコードが含まれる場合がある
CSCvo48975	ISE が BYOD の不要な RA 証明書をダウンロードする
CSCvo61888	デバイス管理の現在アクティブなセッションレポートが 2.4 パッチ 6 から利用できない
CSCvo74766	ワイルドカード表記で ISE DACL 構文チェックの検証が失敗する
CSCvo75129	ランタイムでは、プロファイラに送信される syslog メッセージ内の dhcp-class-identifier の「;」の前に「\」が付加される
CSCvo75376	FMC の pxGrid ノード名の制限が短すぎる
CSCvo80291	pxGrid のスタートアップ順序でプロファイラコードが初期化に失敗する

不具合 ID 番号	説明
CSCvo80516	ISE 2.6 LiveLogs が表示されず、「ヘルスステータスを使用できません（Health Status is Unavailable）」というアラームが誤って表示される
CSCvo82021	ISE：GUI と show tech のメモリ使用率が一致しない
CSCvo98554	ISE PB を ISE にインポートすると、ログインページがロードされない
CSCvn35142	ISE 2.3：条件別のエンドポイントのポスチャレポートが予想どおりに動作しない
CSCvo13626	ISE：大量レコード（100 万）の条件レポートエクスポートレートでポスチャ評価が改善される
CSCvp17444	有効な RSA/RADIUS トークンクレデンシャルを使用していても、ISE 管理者 DB 内でない場合、[管理者アクセス（Admin Access）] はブランクページになる
CSCvp40082	ISE 2.3/2.4 を最新のパッチにアップグレードすると、サードパーティの NAD のダイナミック リダイレクションが中断される場合がある
CSCvo08406	[改善] 外部データソース条件の [Active Directory] フィールドを、参加ポイントと表示するように変更
CSCvo19377	CSV 制限を超えているため、RADIUS レポートに正常な認証エントリが表示されない
CSCvo33474	「サーバが到達不能です（Server not reachable）」による自動ログアウトを修正

Cisco ISE リリース 2.6.0.156 の解決済みの不具合

ISE 2.6 で解決済みのすべての不具合

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283801589&rls=2.6(0.901)&sb=afr&bt=null

Cisco ISE リリース 2.6.0.156 の未解決の不具合

Cisco ISE リリース 2.6 の未解決の不具合

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283801589&rls=2.6&sb=afr&sts=open&bt=null

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービスリクエストを送信するには、シスコサポート にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

【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。