Cisco Identity Services Engine リリース 2.4 リリース ノート

初版：2018 年 4 月 30 日

最終更新：2019 年 3 月 28 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。

概要

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。

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 2.4 には、次のプラットフォームが必要です。

表 *1*: サポート対象のハードウェア プラットフォームおよびペルソナ

ハードウェア プラットフォーム	ペルソナ	設定
Cisco SNS-3515-K9（小規模）	任意	アプライアンス ハードウェア仕様については、『Cisco Identity Services Engine Hardware Installation Guide 2.4』の「Cisco SNS-3500 Series Appliances」の章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）		
Cisco ISE-VM-K9（VMware、Linux KVM、Microsoft Hyper-V）		• CPU およびメモリの推奨事項については、『Cisco Identity Services Engine Installation Guide, Release 2.4』の「VMware Appliance Sizing Recommendations」のセクション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, Release 2.4』の「Disk Space Requirements」のセクション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。 • サポート対象のサポートされる仮想環境。

（注） 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。

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。

（注）

- 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 6.0（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。

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（5.1 U2 以降は RHEL 7 をサポート）、6.x
- Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V
- RHEL 7.3 の KVM

（注） ESXi 5.x サーバに Cisco ISE をインストールまたはアップグレードしている場合に、ゲスト OS として RHEL 7 をサポートするには、VMware のハードウェア バージョンを 9 以降にアップデートしてください。

サポートされているブラウザ

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 リリース 2.4 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、および 2016 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 2.4 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、大規模な企業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 2.4 は最大 50 個のドメイン参加ポイントをサポートします。

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、次の場所にある Cisco AnyConnect ISE ポスチャのサポート表を参照してください。

https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html

Cisco ISE リリース 2.4 の新機能

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

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。

ビジネスの成果

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。

プロキシ経由で外部接続を開始するときのデフォルトの TLS バージョンは TLS 1.2

Cisco ISE がクライアントとして機能する場合、そのクライアントから外部エンティティへの接続に使用されるデフォルトのプロトコルは TLS 1.2 です。この場合、サポート対象プロトコルは TLS 1.2 のみになります。下位バージョンをサポートする場合（安全でない場合があります）、次のページ（[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）]）に移動して、これらのバージョンを Cisco ISE から明示的に有効にする必要があります。

ビジネスの成果

SSL 接続のセキュリティが向上しました。

Cisco ISE は Cisco IND から IoT デバイス コンテキストとセッション データを取得できる

ISE は、Cisco Industrial Network Director（IND）に接続されたデバイスの状態をプロファイル化して表示できます。Cisco Platform Exchange Grid（pxGrid）は、Cisco ISE と Cisco IND 間でエンドポイント（Internet of Things（IoT））データを通信するために使用されます。pxGrid は、Cisco IND からコンテキストを受信し、Cisco IND を照会してエンドポイント タイプを更新するために使用されます。

ビジネスの成果

ネットワーク上の IoT デバイスの分類を自動化します。

pxGrid クライアントの権限の制御

PxGrid 認証ルールを作成し、pxGrid クライアントの権限を制御することができます（[管理（Administration）] > [pxGridサービス（pxGrid Services）] > [権限（Permissions）]）。

これらのルールは、pxGrid クライアントが使用できるサービスとそのサービスの動作を制御できます。Cisco ISE は、個々のクライアントではなくグループにルールを適用します。[権限（Permissions）] ウィンドウの [グループの管理（Manage Groups）] 見出しをクリックすると、グループを管理できます。[権限（Permissions）] ウィンドウには、事前定義されたグループ（EPS や ANC など）を使用する事前定義された認証ルールが表示されます。事前定義されたルールで更新できるのは [グループ（Groups）] フィールドのみです。

ビジネスの成果

pxGrid 下位互換性の向上：

- さまざまな pxGrid サービスの認可を制御する機能。
- 同様の権限を持つ pxGrid クライアントを簡単にグループ化。

カスタマイズ可能な SSH 暗号方式および暗号化アルゴリズム

`service sshd encryption-algorithm` および `service sshd encryption-mode` グローバル コンフィギュレーション コマンドを Cisco ISE 2.4 で使用すると、ISE SSH サーバを強化し、使用する暗号スイートを指定できます。AES-CTR 暗号および AES-CBC 暗号を使用できます。

Cisco ISE 2.3 以前のリリースでは、AES-CBC 暗号のみが許可されていました（アクセス コントロール デバイスおよびシステムに共通する基準保護プロファイルが原因）。Cisco ISE 2.4 では、CTR 暗号と AES-CBC 暗号の両方を使用できます。

ビジネスの成果

- SSH アクセスのセキュリティが向上しました。
- 暗号化アルゴリズムを選択できます。
- セキュアなアクセスの強化に使用する暗号を選択できます。

MDM 属性のエンドポイント API の機能拡張

モバイル デバイス管理（MDM）属性はエンドポイント API を介して使用可能になり、Cisco ISE とサードパーティ MDM サーバ間に同期機能が追加されます。

ビジネスの成果

サードパーティ システムと ISE を適切に統合し、MDM サーバで管理されているモバイル デバイスを使用するエンド ユーザにより優れたユーザ エクスペリエンスを提供できます。

RADIUS の IPv6 サポート

IPv6 アドレスが RADIUS 設定でサポートされるようになりました。[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] ページの [IPアドレス（IP Address）] フィールドと [管理（Administration）] > [ネットワークリソース（Network Resources）] > [外部RADIUSサーバ（External RADIUS Server）] ページの [ホストIP（Host IP）] フィールドの RADIUS 設定で、IPv4 と IPv6 の両方のアドレスをサポートできるようになりました。

ビジネスの成果

IPv6 アドレッシングの追加サポート：

- ネットワークを IPv6 ベースのネットワークに移行することができます。ネットワークがフラグメント化されているか、または IPv4 アドレスが枯渇している場合は、IPv6 アドレッシングに移行できます。
- 効率的なルーティング、パケット処理、セキュリティ、および簡素化されたネットワーク設定が簡単になります。

ペルソナ モニタリング用の大規模な仮想マシン

Cisco ISE では、モニタリング ノードに大規模 VM が導入されました。

このフォーム ファクタは、リリース 2.4 以降での VM としてのみ使用可能で、大規模 VM ライセンスが必要です。

ビジネスの成果

大規模 VM にモニタリング ペルソナを展開すると、次の利点があります。

- 以前サポートされていたデータ量の最大 3 倍。
- ライブ ログ クエリへの応答とレポート完了の面でパフォーマンスが向上しました。

ポスチャの機能拡張

- 非準拠デバイスの猶予期間：Cisco ISE には、適合しなくなったデバイスの猶予時間を設定するオプションが用意されています。Cisco ISE は、設定可能な時間にわたってポスチャ評価の結果をキャッシュします。デバイスが適合していないことが判明した場合、Cisco ISE はキャッシュ内で以前の正常な状態を検索し、デバイスに猶予時間を与えて、その間はネットワーク アクセスが許可されます。分、時、または日単位（最大 30 日）で猶予期間を設定できます。エンドポイント別のポスチャ アセスメント レポートが更新され、現在準拠していないけれども猶予期間内のエンドポイントの猶予準拠ステータスが表示されます。
- ポスチャの再スキャン：AnyConnect ユーザは、いつでも手動でポスチャを再実行できるようになりました。
- AnyConnect ステルス モード通知：ユーザが VPN 接続に関する問題を特定できるように、AnyConnect ステルス モードの展開にいくつかの新しい失敗通知が追加されました。
- Windows での UAC プロンプトの無効化：AnyConnect ポスチャ プロファイルから Windows エンドポイントのユーザ アクセス コントロール（UAC）プロンプトを無効にすることができます。

  （注） デフォルトでは、この値は AnyConnect プロファイルの設定時に [いいえ（No）] に設定されます。これを [はい（Yes）] に変更すると、UAC プロンプトは無効になり、Windows ユーザはこれらのプロンプトを受信しなくなります。UAC プロンプトを再度有効にする場合は、AnyConnect プロファイルでこの設定を [いいえ（No）] に変更する必要があります。この設定は、Windows エンドポイントが再起動された場合にのみ有効になります。

- クライアント プロビジョニングとポスチャ更新をダウンロードするための新しい URL：クライアント プロビジョニングとポスチャ フィードの URL が変更されました。ポスチャ更新の新しい URL は https://www.cisco.com/web/secure/spa/posture-update.xml、クライアント プロビジョニングの新しい URL は https://www.cisco.com/web/secure/spa/provisioning-update.xml です。
- ファイル条件の機能拡張：ファイル条件下に新しい演算子が導入され、一定期間内のファイルの変更が確認されます。

- クライアント プロビジョニングとポスチャ ポリシーの証明書属性：証明書属性がクライアント プロビジョニングとポスチャ ポリシー ページで使用可能になりました。
- [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディスク暗号化条件（Disk Encryption Condition）] ウィンドウの [ロケーション（Location）] フィールドの下に、次のオプションが新しく追加されました。
  - すべての内部ドライブ：内部のドライブをチェックします。マウントおよび暗号化されたすべてのハードディスクと、すべての内部パーティションが含まれます。読み取りのみのドライブ、システム リカバリ ディスク/パーティション、ブート パーティション、ネットワーク パーティション、およびエンドポイント外のさまざまな物理ディスク ドライブ（USB およびサンダーボルトを介して接続されたディスク ドライブを含むがこれに限定されない）は除外されます。検証済みの暗号化ソフトウェア製品には次のものがあります。
    - Bit-locker-6.x/10.x
    - Windows 7 上の Checkpoint 80.x

（注） [すべての内部ドライブ（All Internal Drives）] オプションは、AnyConnect バージョン 4.6.01098 以降でサポートされています。

ビジネスの成果

セキュリティ アラートおよび適用が改善されました。

- 猶予期間固有のメッセージング シナリオを含む、ポスチャ条件の失敗についてエンドユーザを教育するために柔軟性に優れたオプションを管理者ユーザに提供します。
- 追加の権限を必要とする一部のポスチャ チェックおよび修復を効率的に管理し、そのような権限のユーザにプロンプトを表示します。

プロファイラの機能拡張

- AudioCode、BlackBerry、Brother、Hewlett Packard、Lexmark、NetApp、Samsung、Xerox といったベンダーの 190 個の新しいプロファイル ポリシーが追加されました。
- 追加のプローブをサポートするために新たな条件が 185 個のプロファイル ポリシーに追加されました。たとえば、SNMP に基づいて Xerox デバイスをプロファイリングしないユーザが DHCP を使用して Xerox デバイスをプロファイリングできるように、DHCP 条件を Xerox デバイスに追加します。
- 新しいデバイスを正確に識別できるようにプロファイルをファミリに再編成します。たとえば、HP-LaserJet-4350 は HP-Device 下ですでに直接プロファイリングされています。ここで HP-LaserJet 下でプロファイリングされ、次に HP-Device 下でプロファイリングされ

るようになりました。Hewlett Packard が新しい Hewlett Packard LaserJet プリンタ モデルを導入すると、Cisco ISE は、その正確な LaserJet プリンタ モデルの新しいプロファイル ポリシーが追加されるまで、HP-Device としてではなく、HP-LaserJet として新しいモデルを分類します。

ビジネスの成果

デバイスの効率的な分類：

- プロファイラの効率性を向上した Xerox プリンタや Vista リンク プリンタなど、これまで不明であったデバイスの可視性を向上することができます。

個別の SNMP CoA パケットの送信のサポート

[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイスプロファイル（Network Device Profiles）] > [認可変更（CoA）（Change of Authorization (CoA)）] ウィンドウで [SNMP COAの個別リクエストの送信（Send SNMP COA Separate Request）] チェックボックスを選択し、SNMP CoA パケットを NAD に 2 つのパケットとして送信できます。

ビジネスの成果

デバイスの互換性の向上：

- SNMP CoA パケットを 2 つのパケットとして送信することを義務付けている、以前のシスコおよびサードパーティ製の NAD をサポートします（shutdown および no shutdown インターフェイス コンフィギュレーション コマンドの場合）。

RADIUS NAD クライアントでの IP ごとの 2 つの共有秘密のサポート

ネットワーク デバイスと Cisco ISE で使用される 2 つの共有秘密（鍵）を指定できます。Cisco ISE の [管理（Administration）] > [ネットワークリソース（Network Resources）] > [ネットワークデバイス（Network Devices）] ページの NAD の [RADIUS認証（RADIUS authentication）] セクションで共有秘密を設定できます。

ビジネスの成果

ネットワーク デバイスの共有秘密を置き換えます。

- ネットワーク デバイスの共有秘密を個別に置き換え、共有秘密がネットワーク デバイスで置き換えられるまで、ISEは古い共有秘密と新しい共有秘密の両方をサポートします。これで、RADIUS の秘密の変更が簡単になり、ネットワーク デバイスを更新する前に新しい共有秘密を入力できるようになりました。

TrustSec の機能拡張

ネットワーク デバイスを追加する際に、ネットワーク デバイスに設定変更を送信する必要がある ISE ノードを選択できます（[高度なTrustSec設定（Advanced TrustSec Settings）] セクションの下）。PAN または PSN ノードを選択できます。選択した PSN ノードがダウンした場合、PAN を使用してこのデバイスに設定変更が送信されます。

IP SGT スタティック マッピングを展開する場合は、選択したマッピングを展開する必要があるデバイスまたはデバイス グループを選択できます。必要に応じて、すべてのデバイスを選択できます。フィルタ オプションを使用して必要なデバイスを検索できます。デバイスを何も選択しない場合は、選択したマッピングがすべての TrustSec デバイスに展開されます。

[ステータスを確認（Check Status）] オプションを使用して、特定のデバイスの同じ IP アドレスに複数の異なる SGT が割り当てられているかどうかを確認します。このオプションを使用すると、競合するマッピングを使用するデバイス、複数の SGT にマッピングされている IP アドレス、および同じ IP アドレスに割り当てられている複数の SGT を見つけることができます。展開でデバイス グループ、FQDN、ホスト名、または IPv6 アドレスが使用される場合でも、このオプションを使用できます。競合するマッピングを展開する前に、それらのマッピングを削除するか、展開の範囲を変更する必要があります。

[一般TrustSecの設定（General TrustSec Settings）] オプションの [TrustSec展開の検証（Verify TrustSec Deployment）] オプションでは、すべてのネットワーク デバイスに最新の TrustSec ポリシーが展開されているかどうかを検証できます。Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合、[アラーム（Alarms）] ダッシュレットにアラームが表示されます（**[ワークセンター（Work Centers）] > [TrustSec] > [ダッシュボード（Dashboard）]**）。TrustSec ダッシュ ボードに、以下のアラームが表示されます。

- 検証プロセスが開始または完了するたびに、情報アイコンとともにアラームが表示されます。
- 新しい展開要求のために検証プロセスがキャンセルされた場合、情報アイコンとともにアラームが表示されます。
- 検証プロセスの結果がエラーになった場合（たとえばネットワーク デバイスとの SSH 接続を開けない、ネットワーク デバイスが使用不可など）、または Cisco ISE で設定されたポリシーとネットワーク デバイスの間に相違がある場合、これらのネットワーク デバイスごとに警告アイコンとともにアラームが表示されます。

[展開の検証（Verify Deployment）] オプションは、次のページでも使用できます。

- **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ ACL（Security Group ACLs）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [マトリックス（Matrix）]**

- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [送信元ツリー（Source Tree）]**
- **[ワークセンター（Work Centers）] > [TrustSec] > [TrustSecポリシー（TrustSec Policy）] > [出力ポリシー（Egress Policy）] > [宛先ツリー（Destination Tree）]**

それぞれの展開後に、Cisco ISE ですべてのネットワーク デバイス上の更新を検証するには、[すべての展開後に自動検証（Automatic Verification After Every Deploy）] チェックボックスをオンにします。展開プロセスが完了したら、[展開プロセス後の時間（Time after Deploy Process）] フィールドに指定した時間が経過した後に、検証プロセスが開始されます。待機期間中または検証の進行中に新しい展開要求を受信した場合、現在の検証プロセスはキャンセルされます。検証プロセスをすぐに開始するには、[今すぐ検証（Verify Now）] をクリックします。

IP SGT 静的マッピングでではIPv6アドレスを使用できます。SSH またはSXP を使用して、特定のネットワーク デバイスまたはネットワーク デバイス グループにこれらのマッピングを伝達できます。

FQDN とホスト名が使用される場合、Cisco ISE はマッピングを展開して展開ステータスを検査する際に、PAN および PSN ノード内の対応する IP アドレスを検索します。[一般TrustSecの設定（General TrustSec Settings）] ウィンドウの次のいずれかのオプション（[ホスト名のIP SGT スタティックマッピング（IP SGT Static Mapping of Hostnames）] の下）を使用すると、DNS クエリによって返される IP アドレス用に作成されるマッピング数を指定できます。

- **DNSクエリによって返されるすべてのIPアドレスに対してマッピングを作成する（Create mappings for all IP addresses returned by DNS query）**
- **DNSクエリによって返される最初のIPv4アドレスおよび最初のIPv6アドレスに対してのみマッピングを作成する（Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query）**

ビジネスの成果

- ネットワーク デバイスの TrustSec ポリシーを検証します。
- 拡張 IP-SGT マッピング ワークフロー：
  - [ステータスの確認（Check Status）] オプションを使用してネットワーク デバイスの設定ミスのエラー処理と運用効率を改善します。
  - IP SGT スタティック マッピングを選択的に展開します。
  - IPv6 アドレスを使用して IP スタティック マッピングを作成します。
  - DNS FQDN クエリに基づいて最初または既知のすべての IP アドレスのマッピングを作成します。

廃止したダッシュレット

パフォーマンス問題の解決のために削除された一部のダッシュレット

次のダッシュレットは、大規模なデータセットを表示する際のパフォーマンスの問題を防ぐために廃止されました。

- **[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoint）] > [コンプライアンス：ステータストレンド（Compliance: Status Trend）]**
- **[ホーム（Home）] > [エンドポイント（Endpoints）] > [エンドポイントキャパシティ（Endpoint Capacity）]**

多数のエンドポイントで一部のダッシュレットにパフォーマンスの問題が発生しました。

スポンサー ポータルの Kerberos 認証

ISE を設定して、Windows にログオンしているスポンサー ユーザのスポンサー ポータルへのアクセスの認証に Kerberos を使用することができます。このプロセスは、Kerberos チケットでログインしているスポンサー ユーザの Active Directory クレデンシャルを使用します。ブラウザが ISE との SSL 接続を確立した後、セキュア トンネル内で Kerberos SSO が実行されます。

スポンサー認証の追加セキュリティ。

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。

ビジネスの成果

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。

既知の制限事項と回避策

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。パッチ バンドルは正しい MD5 チェックサムを使用してダウンロードする必要があることに注意してください。

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。

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。

Cisco Temporal Agent

Cisco Temporal Agent は、クライアント プロビジョニング ポータルからエージェントをダウンロードしてから 2 分以内に実行することをお勧めします。それ以外の場合は、「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 メッセージが表示されます。

モバイル サービス エンジン（MSE）デバイス

Cisco ISE に MSE デバイスを追加する場合は、許可が簡単になるように MSE デバイスから ISE に証明書をコピーする必要があります。ISE は MSE デバイスからこれらの証明書を直接受信することはありません。

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。

アップグレード情報

（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 2.4 へのパッチの適用

Cisco ISE リリース 2.4 のパッチ 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（http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm）にログインし（Cisco.com ログイン クレデンシャル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, Release 2.4*』の「Installing a Software Patch」のセクション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手順については、『*Cisco Identity Services Engine CLI Reference Guide, Release 2.4*』の「Install Patch」のセクションを参照してください。

（注） 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、CLI に次のエラーが表示されます。「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）」。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。

パッチは、上記のパッチ バージョンで提供されるすべての修正が含まれるように累積されます。Cisco ISE バージョン 2.4.0.357 は Cisco ISE 2.4 リリースの初期バージョンでした。パッチのインストール後、Cisco ISE GUI の **[設定（Settings）] > [Identity Services Engineについて（About Identity Services Engine）] ** ページから、および次の形式「2.4.0.357 パッチ N」（N はパッチ番号）で CLI からバージョン情報を表示できます。

（注） バグ データベース内では、パッチで解決された問題に、形式が異なるバージョン番号「2.4(0.9NN)」が使用されます。ここで、NN は 2 桁の数字として表示されるパッチ番号です。たとえば、バージョン「2.4.0.298 パッチ 1」はバグ データベース「2.4(0.901)」の次のバージョンに対応しています。

（注） Cisco ISE リリース 2.4 にパッチをインストールした後、ブラウザのキャッシュをクリアすることをお勧めします。

リリース 2.4 へのアップグレード

次の Cisco ISE リリースからリリース 2.4 に直接アップグレードできます。

- 2.0
- 2.0.1
- 2.1
- 2.2
- 2.3

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。

Cisco ISE リリース 2.0 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 2.4 にアップグレードする必要があります。

（注） 次のバージョンの Cisco ISE にアップグレードする前に、既存のバージョンの最新パッチにアップグレードすることをお勧めします。

GUI または CLI からリリース 2.4 にアップグレードできます。『Cisco Identity Services Engine Upgrade Guide, Release 2.4』を参照してください。

仮想マシンのオペレーティング システムの確認

ISE リリース 2.4 は Red Hat Enterprise Linux（RHEL）7.0 で実行されます。VMware VM で Cisco ISE ノードをアップグレードする場合は、アップグレード後、ゲスト オペレーティング システムを Red Hat Enterprise Linux（RHEL）7 に変更します。これを行うには、VM の電源をオフにし、RHEL 7 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。

外部 RADIUS トークン サーバのタイムアウト

外部 Radius トークン サーバのタイムアウトの最大値が 120 秒から 60 秒に変更されました。このリリースにアップグレードすると、最大値が 60 秒を超える場合に既存の設定が変更されます。

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。展開に評価、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。

インストールまたはアップグレードの後、展開済みの VM ノードの数とインストール済みの VM ライセンスの数の間に不一致がある場合、アラームが 14 日ごとに [アラーム（Alarms）] ダッシュレットに表示されます。アラームは、VM ノードのリソースに変化がある場合や、VM ノードが登録または登録解除されるたびにも表示されます。

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, Release 2.4*』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。アップグレードの失敗のほとんどは、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、実際のアップグレードの前にデータを検証し、問題をレポートして、可能な限り問題を解決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、Windows および Mac OS X 用 CISCO NAC Agent、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。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ために、初期展開時に Cisco ISE でこのライブ アップデート ポータルを設定する必要があります。

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 サーバが必要になる場合は、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）]** を選択してプロキシを設定します。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を許可するようにプロキシ設定を有効にした場合、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失われます。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, Release 2.4』の「Specify Proxy Settings in Cisco ISE」のセクション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 EngineAdministrator Guide, Release 2.4』の「Configure Client Provisioning」の章の「Download Client Provisioning Resources Automatically」セクション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, Release 2.4』の「Download Posture Updates Automatically」のセクション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。

また、オフライン更新はプロファイラ フィード サービスでも使用できます。詳細については、「」を参照してください。

オフライン 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/2.4.0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
- **nacagent-**<*version*>**-isebundle.zip**：オフライン NAC 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。

オフラインでポスチャ更新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 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 ライセンス料金を指定する必要があります。

- 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。
- Cisco Identity Services Engine の対応するリリースのリリース ノート ドキュメントを参照してください。

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。

- Cisco ISE の概要
- Cisco ISE YouTube チャンネルに関するビデオ
- 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 の詳細な発注情報については、『Cisco Identity Services Engine Ordering Guide』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 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（https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/tsd-products-support-series-home.html）を参照してください。

Cisco ISE のバージョンと Cisco DNA Center のバージョンのそれぞれの互換性については、https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html?wcmmode=disabledを参照してください。

移行情報

ACS から ISE への移行の詳細については、『Cisco Identity Services Engine Migration Tool Guide』を参照してください。

不具合

このセクションでは、重大度 1 および 2 の未解決の不具合について説明し、重大度 3 の不具合を選択します。「未解決の不具合」セクションには、現在のリリースに適用され、以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。バグ ID は英数字順にソートされます。「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、バグ検索ツールを使用する必要があります。

シスコのバグ検索ツール（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、キーワードに基づいてバグを検索できます。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 2.4.0.357 の解決済みの不具合 - 累積パッチ 9

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。

次の表は、Cisco ISE 2.4 パッチ 9 で解決済みの不具合のリストです。

パッチ 9 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。

（注） パッチが正常にインストールされた後、再起動しようとすると、パッチのインストールが失敗したことを示すアラームがエラーとともに表示される場合があります。これは誤ったアラームです。このアラームは無視できます。

不具合 ID 番号	説明
CSCvd88480	ERS ネットワーク デバイス get-all API のロケーション フィルタが失敗した
CSCvf17323	正規化された Radius：SSID が同じセッション ID の CoA の後に一致しない
CSCvf33851	ISE 2.1+ RBAC：エンドポイントを管理し、スタティック ID グループを割り当てることができない

不具合 ID 番号	説明
CSCvh64185	pxGrid を介して ISE から FMC にセッションの詳細が送信されると、一部の情報が欠落する
CSCvi27613	プロファイリングが無効になっていても、エンドポイントはプロファイリングを維持する
CSCvi65932	customField フィールドに「null」値が含まれている場合、スポンサー ポータルで空白のポップアップが表示される
CSCvj02829	SCCM MDM 属性 LastPolicyRequest が ISE で正しく変換されていない
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	SCCM MDM 属性 LastPolicyRequest が ISE で正しく変換されていない
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
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
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
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」
CSCvn66198	ユーザを削除してもスポンサー ポータルでアカウントが更新されず、手動で更新する必要がある
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削除される
CSCvo48975	ISE が BYOD の不要な RA 証明書をダウンロードする
CSCvo56989	Json SearchResult は href 値を NULL として提供する
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
CSCvo75376	FMC の pxGrid ノード名の制限が短すぎる
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
CSCvo82021	GUI と show tech のメモリ使用率が一致しない
CSCvo90393	Radius+PassiveID フローでの COA 障害

不具合 ID 番号	説明
CSCvo92284	IP SGT スタティック マッピングの変更を保存する場合、「実施した変更を破棄しますか（Discard changes you have mad）」というメッセージが表示される
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
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
CSCvp05936	DEFCON マトリックスの追加ポップアップ タイトルを変更する必要がある
CSCvp07591	Active Directory マシン認証が失敗し、エラー「22040パスワードが不正か、または共有秘密が無効です（22040 Wrong password or invalid shared secret）」が表示される
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
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]
CSCvp13378	PassiveID フローでユーザの SamAccountName と ExplicitUPN を送信する必要がある
CSCvp14725	一部のセッションで 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
CSCvp17444	[アクセス（Access）] > [管理者（Administrators）] にアカウントが存在しない場合、ISE 管理者ポータルにログインすると、有効なアカウントとクレデンシャルを使用する RSA または RADIUS トークン ユーザに空白ページが表示される
CSCvp18692	AD ユーザ情報が [コンテキストの可視性（Context Visibility）] ページに表示されない
CSCvp19632	XML としてエクスポートする場合、ポリシー セット順序が一致しない
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
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 プローブ設定の有効化が正常に機能しない

不具合 ID 番号	説明
CSCvp33593	ISE がエンドポイント ID グループ「不明（unknown）」との認証ポリシーの照合に失敗する
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
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	[管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] > [Active Directory] で GUI を介して AD Join 操作が試行されると、アプリケーション サーバのクラッシュが発生する
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
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
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
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
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
CSCvp50557	最大ユーザ グローバル設定を変更すると、変更設定の監査にログが記録されない
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
CSCvp52201	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
CSCvp54949	IOS 12.2 で BYOD フローが破損している
CSCvp54992	BYOD のプロビジョニング プロファイルでは、IOS 12.2 で EAP TLS が自動的に設定されない
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 Failed 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

不具合 ID 番号	説明
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
CSCvp65711	エンドポイントが 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
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
CSCvp76911	複数マトリックス ワークフローが有効な場合、[マトリックス（Matrix）] ページに [展開（Deploy）] ボタンが表示されない
CSCvp77008	カスタム属性が設定されている場合、ISE LogicalProfile が [コンテキストの可視性（Context Visibility）] ページの [カスタム（Custom）] 属性の下に表示される
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
CSCvp93901	pxGrid を介して次の属性をパブリッシュする拡張機能：ADUserSamAccountName、ADUserQualifiedName、ADHostSamAccountName、ADHostQualifiedName
CSCvq15329	スケジュール バックアップの復元に失敗した

Cisco ISE リリース 2.4.0.357 の解決済みの不具合 - 累積パッチ 8

次の表は、リリース 2.4 累積パッチ 8 で解決済みの不具合のリストです。

パッチ 8 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。

（注） パッチが正常にインストールされた後、再起動しようとすると、パッチのインストールが失敗したことを示すアラームがエラーとともに表示される場合があります。これは誤ったアラームです。このアラームは無視できます。

不具合 ID 番号	説明
CSCvj83362	ポスチャ評価レポートにホスト名が含まれる

不具合 ID 番号	説明
CSCvk34232	ポスチャ修復ファイルが 50 MB に制限されている
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
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
CSCvn52886	WMI 情報のユーザ名が同じエンドポイントの DHCP カスタム syslog を受信すると削除される
CSCvn55560	EOB ゲスト ユーザのパッチ 5 作成の適用後に ISE 2.3 が機能しない
CSCvn56648	個々のポリシー セットがリセットされると、他のポリシー セットのヒット カウンタが 0 にリセットされる
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
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
CSCvn61139	スマート ライセンス エージェントのスレッド ロックにより、ISE 2.2 の GUI ログイン遅延が発生する
CSCvn64652	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvn65317	ISE は、以前のユーザに使用されたのと同じゲストタイプにゲストアカウントを割り当てることができない
CSCvn67160	プロキシバイパス リストにキャリッジリターン記号が含まれている場合、ISE 2.4 はプロキシ設定を変更できない
CSCvn67199	「/」文字を使用すると、「NAD ポート ID」別にコンテキストの可視性をフィルタリングできない
CSCvn69854	ISE にサポート バンドルで prrt-server ファイルが 1 つだけ含まれる
CSCvn70558	MDMServerReachable が SCCM MDM に対して再度機能しない
CSCvn70680	Base ライセンスと Wired ライセンスの数が一致しない場合、ISE の期限切れライセンスを削除できない
CSCvn72150	VM パフォーマンス レポートでノードの IO スパイクが頻繁に発生する
CSCvn72918	ISE TrustSec ポリシー相違のアラームの説明にアクセスできない
CSCvn75396	認証が「失敗の理由別上位 N の認証（Top N Authentication by Failure Reason）」レポートに誤って表示される

不具合 ID 番号	説明
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
CSCvn79043	ISE 2.4 ライブ ログがフィルタリングされない
CSCvn79557	ISE：カスタム ユーザ属性の変更に設定変更監査レポートの変更が反映されない
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
CSCvn85498	ISE 2.4：InactiveDays 属性が無効なプロファイルで更新される
CSCvn87918	IPV6 ベースのクライアント プロビジョニング ポータルがデフォルト ポート 8443 で動作していない
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
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
CSCvo13269	ISE で SGT の追加が許可されていない
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
CSCvo17704	ISE 2.4：CLI パスワードに 3 $ を指定できない
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
CSCvo23340	[ワークセンター（Work Centers）]>[デバイス管理（Device Admin）]>[ID（Identities）] への移動時に TACACS+ 管理者グループへのアクセスが拒否される
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
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

不具合 ID 番号	説明
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
CSCvo35516	デバイス センサーが RADIUS プローブ経由で DHCP 属性を正しく解析できない
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
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
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
CSCvo49521	ISE が OperatingSystemVersion の末尾に別の文字を追加する
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
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 P6 から利用できない
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
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
CSCvi21737	ISE 2.2 のジャーナル ファイルが多すぎる
CSCvi29759	Samsung S7 および S8 プロファイル
CSCvi51291	初回認証から 2 日後に ISE CoA が動作しなくなる
CSCvi68744	不要なライセンス ファイルがあるため、過剰なログイン遅延が発生する：ISE
CSCvi80094	CSRF トークンを必要とする ERS API が 403 の代わりに HTTP 404 を返す

不具合 ID 番号	説明
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
CSCvj08392	snmp-server ユーザの削除後も ISE SNMPv3 ユーザが「show snmp user」で表示される
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
CSCvj72647	EAP チェーンで ODBC 属性の取得が適切に機能しない
CSCvj75478	デバイス ネットワーク条件が見つからない
CSCvj81752	ORA-31684 が原因でインポート時に URT が失敗する
CSCvj90273	マルチ NIC Windows/macOS：ISE ポスチャ モジュールが、接続されていないインターフェイスの MAC アドレスに VPN IP をマッピングする
CSCvk13569	ISE ADRT が子ドメイン名をルート フォレスト ドメインと誤認するため「ERROR_NO_SUCH_USER」が表示される
CSCvk29087	マスター ゲスト レポートの表示に 30 分以上かかる
CSCvk50720	ISE 2.2：[ネットワークデバイス（Network Device）] ページがロードされていない
CSCvk59716	ドメイン管理者がスポンサー アカウントを正しく編集できない
CSCvk61386	フィルタリングされた NAD が ISE に表示されない
CSCvk70748	PSN ノードにおける CPU と認証の高遅延および OOM 条件
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
CSCvm07718	TACACS/RADIUS 共有秘密キーが、強調表示してコマンド/コントロール + C を押すと消える
CSCvm63427	Cisco Identity Services Engine のパスワード回復の脆弱性
CSCvm87060	ISE 2.x：リモート フォレストの Active Directory コントローラのフェールオーバー時間が長くなる
CSCvm87292	Tenable アダプタを ISE 2.4 & 2.5 2.2 2.3 に統合できない
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」
CSCvn01551	ISE Agent リソースで 50 MB を超えるファイル サイズの AC パッケージをアップロードできない

不具合 ID 番号	説明
CSCvn10971	ISE：関連付けられているサイト固有のGCを再起動すると、他のGCへのフェールオーバーが発生しない
CSCvn12229	log4j.appender.ACS-FILE.MaxBackupIndex が ISE で動作していない
CSCvn15670	SL サーバが ISE 認証更新によって過負荷になっている
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
CSCvn24392	特定の文字が正しく解析されていない
CSCvn24568	複数の範囲が設定されている場合、ネットワーク デバイス フィルタリングが最初の IP 範囲のみを返す
CSCvn27022	NADへのアクセス時に[ネットワークデバイスグループの取得に失敗しました（failed to fetch network device group）] が制限付きアクセス ユーザに表示される
CSCvn27325	条件でトンネル グループ名が指定されているポスチャ ポリシーがヒットしていない
CSCvn39504	TACACS 認証の詳細に空白ページが表示される
CSCvn39998	認証サマリー レポートの引き出しレポートに空のレポートが表示されている
CSCvn40822	パッチ 5 以降の ISE 2.3 でゲストの作成に失敗する
CSCvn52114	外部 radius トークン サーバ認証を使用したプロセスが失敗する
CSCvn56754	新しいユーザ名（および/または）新しい IP アドレスを使用すると、ライブ セッション レコードが更新されない
CSCvo41052	ISE が新しく作成された IP-SGT マッピングを削除する
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
CSCvo11090	ISE で ACI IEPG を削除できる
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
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

不具合 ID 番号	説明
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
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
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
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
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

Cisco ISE リリース 2.4.0.357 の解決済みの不具合 - 累積パッチ 7

次の表は、リリース 2.4 累積パッチ 7 で解決済みの不具合のリストです。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
CSCvn90651	これは Cisco ISE のマルチ DNAC サポートにマスター ノード API を実装するための機能拡張です。

Cisco ISE リリース 2.4.0.357 の解決済みの不具合 - 累積パッチ 6

次の表は、リリース 2.4 累積パッチ 6 で解決済みの不具合のリストです。

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 2.2.0.53 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
CSCux55288	ゲスト ユーザ情報保存機能により ISE ゲスト アクティビティ ロギングが中断される
CSCuy41309	ISE 2.x がエンドポイント グループからエンドポイントを削除できない
CSCuz00603	重複するマッピングを複数の SXP VPN に追加できない
CSCvb17967	ISE が特殊文字を使用して MDM から応答を読み取ることができない
CSCvb45390	ユーザ名を使用して設定された収集フィルタが TACACS の作成者/アカウントに対して機能しない

不具合 ID 番号	説明
CSCvc06629	[ISE] HTML タグを含む英語以外の SMS 通知
CSCvd79952	分散展開でのセッション マージ後に EasyConnect CoA が送信されない
CSCvf03310	ゲストへの ISE 電子メール通知で承認とゲスト ユーザ用に電子メールが 2 回送信される
CSCvf19364	ネットワーク サブネットのスタティック マッピングを作成しようとしたときに ISE 2.2 パッチなしの SXP プロセスが失敗する
CSCvf30591	ISE 2.2：パスワードの有効期間が無効にされる。ただし、アカウントの有効期限の通知は受信する。
CSCvf75225	ISE 2.1-P3 || redis で 100K に制限されているため、PAN の高 CPU が検出される
CSCvg86743	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
CSCvh09779	ISE 2.x TACACS ログが非常に遅い
CSCvh11308	Cisco Identity Services Engine のログ クロスサイト スクリプティングの脆弱性
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
CSCvh31565	接続の切断後に ISE が TCP syslog 接続を再確立できない
CSCvh54905	ID 管理者の [ID（Identities）] タブの下にユーザを表示できない
CSCvh83222	ISE：一意のエンドポイントの総数に関するレポート/ダッシュボードが必要
CSCvh91118	認証を失敗したユーザ名を開示するタイムインターバルを選択するために必要な柔軟性
CSCvh97544	クライアントが応答せず、ISE が RADIUS プロキシとして使用されている場合、短時間の CPU スパイクが検出されることがある
CSCvi21043	ポリシー内で参照されるライブラリ コマンドが削除されている。評価は拒否アクセスである
CSCvi23542	ストレス認証中に予期しないエラーが発生する。RPC ログオン要求が失敗した。STATUS_ACCESS_DENIED
CSCvi30462	SAML プロバイダーを使用してスポンサー ポータルにログインすると、一括ゲスト インポートが機能しない

不具合 ID 番号	説明
CSCvi37480	HP スイッチを使用した ISE での SNMPv3 COA の障害
CSCvi41678	コンテキストの可視性のエンドポイント属性が更新されない
CSCvi42404	ERS が作成したゲストで、validDays が fromDate から toDate の期間と一致しない
CSCvi43687	ISE 2.2 エンドポイントのエクスポートに重複するエントリが含まれている場合がある
CSCvi48298	[更新（REFRESH）] ボタンをクリックすると、ポリシー ヒット カウント値が無効になる
CSCvi50320	ISE iseca フォルダが欠落している場合、EST サービスが実行されない
CSCvi61204	ISE 2.1 エンドポイントの消去ポリシーは一致したけれども、実行中にジョブが停止する
CSCvi67780	ISE 内部 CA：CSR の RequestedExtensions の最初のエントリでない場合、SAN 外部検証が失敗する
CSCvi68271	ドキュメントに記載されているように、[説明（description）] フィールドを返さないすべてのエンドポイントを ERS API が取得する
CSCvi97332	管理者ユーザの作成時に、サポートされていない文字のバックスラッシュを UI エラー メッセージに追加する必要がある
CSCvi99561	AC 4.6 アプリケーションの適用が Torrent で機能していない
CSCvj01047	32 文字の [PassiveID] セクションに DC を追加する場合のパスワード長の制限
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
CSCvj24095	ExternalIdStoreDictionary の更新時に不明な Radius フローが RadiusFlowType に設定される
CSCvj25696	ドラッグ アンド ドロップして保存した後、ユーザの顧客属性の順序が変更されない
CSCvj31243	ポリシーで参照されているグループで ISE 2.3 AD グループ SID の更新に失敗する
CSCvj50257	アクティブなエンドポイントが予想された値と一致しない
CSCvj57593	SNMP CoA が正しい SNMP トラップを送信していない
CSCvj62592	Cisco Identity Services Engine（ISE）の Java 逆シリアル化の脆弱性

不具合 ID 番号	説明
CSCvj62599	Adobe Action Message Format（AMF）での Cisco Identity Service Engine（ISE）の安全でない逆シリアル化
CSCvj62614	Cisco Identity Services Engine（ISE）のファイル アップロード コード実行の脆弱性
CSCvj63376	ISE 2.2 VPN MDM コンプライアンスがアクティブ セッションの MDM コンプライアンス チェッカーから更新されない
CSCvj64763	DNAC-ISE：Pxgrid フェールオーバーが DNAC と ISE を統合した 2.4 パッチ 1 で失敗する
CSCvj65552	ISE 2.4 バックアップの入力検証がバックアップ名の文字に対して行われない
CSCvj67414	ISE HSTS の Max-Age パラメータが includedDomains フラグでアグレッシブすぎる
CSCvj72699	ISE が SXP マッピングのパブリッシュを停止する
CSCvj73152	ISE 2.4 の VLAN DHCP リリースの有効化により、ゲスト フローが切断される
CSCvj77878	pxgrid：XMPP クリアテキスト認証
CSCvj92976	ISE：ネットワーク デバイス プロファイルの下にアイコンをインポートすると、不完全なエラー メッセージが表示される
CSCvj95709	FIPS モードによる pxGrid の有効化
CSCvj99698	スポンサーがゲスト パスワードを表示する権限を持っていない場合、ゲスト パスワードがリセットされない
CSCvk01682	ISE でポータル セットアップに同じ言語の複数のインスタンスをインポートできる
CSCvk04424	[マイ レポート（My Reports）] の名前をポリシー セットに一致にするように変更すると、[マイ レポート（My Reports）] から削除オプションが削除される
CSCvk10156	ネットワーク デバイス グループの読み取り専用データ アクセスによって RBAC SuperAdmin データ アクセスが上書きされる
CSCvk13724	ISE で EPG マッピングが作成されない
CSCvk23161	ISE が TACACS 要求への応答を停止する

不具合 ID 番号	説明
CSCvk23532	電子メール通知で $ui_start_date_time$ および $ui_end_date_time$ から GMT 部分が削除される
CSCvk27295	EP が管理者によって作成されたプロファイリング ポリシーと一致すると、NMAP の実行に失敗する
CSCvk28847	表示/印刷ゲストのパスワードが無効になっている場合、ISE スポンサーの電子メールが CC にない
CSCvk34232	ポスチャ修復ファイルが 50 MB に制限されている
CSCvk38374	ISE 2.4 スポンサー グループ OWN_ACCOUNTS 電子メール関連付け
CSCvk39421	ISE オフライン プロファイラ フィード サービスを利用できない（2018 年 7 月 17 年）
CSCvk40105	指名を java スクリプトを使用して作成した場合、ゲスト ユーザを編集するとポップアップ エラーが表示される
CSCvk48315	ライブ セッションが ISE 2.4 の ISE ライブ ログ ページには表示されない
CSCvk51906	DST の変更は、MNT ノードでデータ移動の問題が発生するシフト ジョブには適用されない
CSCvk55285	ISE がカスタム エンドポイント属性のデータ タイプの日付を検証しない
CSCvk58134	SAML 認証でスポンサーのログインおよび監査レポートに誤った ID ストアが表示される
CSCvk59357	新しいライセンスを追加しても、管理者にライセンス違反の警告が表示される
CSCvk65898	ISE 2.4：Facebook 側で行われた最近の変更が原因で、ソーシャル ログイン e2e フローが失敗する
CSCvk68196	SNMPv3 プロファイリングが DES または AES128 プライバシー プロトコルでのみ機能する
CSCvk70087	リモート ログ ターゲットの SecureSyslogCollectors はデフォルトで無効になっている必要がある
CSCvk71816	ISE ADE-OS：タイムゾーンを変更しようとすると、サポートされていないことを示す警告が表示される
CSCvk72606	ISE：無効にされた管理者アカウントを使用して GUI にログインできる
CSCvk74190	Radius トークン ID キャッシング タイムアウトが設定できない

不具合 ID 番号	説明
CSCvm00127	ISE スポンサー電子メールのカスタマイズによってイメージが正しく追加されない
CSCvm03842	PxGrid SSL/TLS 再ネゴシエーション ハンドシェイク MiTM プレーンテキスト データ インジェクション：CVE-2009-3555
CSCvm09377	電子メールに @ が含まれる場合、ISE の HTTP 要求ヘッダーが失敗する
CSCvm09493	ISE 2.4 | 複数のカスタム属性を一度に保存することができない
CSCvm11230	ライブ ログの [詳細（Details）] ページのこのレコードで利用可能なデータがユーザに表示されない
CSCvm12105	ISE 2.3 がセッション BYOD-Apple-MiniBrowser-Flow 条件を使用するポリシーにヒットしない
CSCvm12281	ISE 2.3 コンテキストの可視性の認証ポリシー列が空白である
CSCvm12443	ISE が ERS ヘッダーに存在しない「ERS-Media-Type」に関してアラームを送信しない
CSCvm14030	Struts リモート コード実行の脆弱性に関する positron の評価（2018 年 8 月）
CSCvm15059	ISE 2.1+：ID ソース順序の情報ボタンがスポンサー ポータルで誤っている
CSCvm16060	Telnet 変更パスワードを無効化できない
CSCvm16523	ISE 2.3 から 2.4 へのアップグレードが失敗し、「ノードのISEパッチバージョンが異なっています（nodes are not on the same ISE patch version）」というエラーが表示される
CSCvm16952	Oracle セキュリティ アラート アドバイザリ：CVE-2018-3110
CSCvm20561	ISE 2.x || シスコ デバイスのプロファイラ ポリシーで、tandberg OUI が条件として欠落している
CSCvm21147	ISE：ISE 2.4 へのアップグレード後、スケジュール バックアップが機能しない
CSCvm22262	AMQP クリアテキスト認証の脆弱性
CSCvm26334	設定の復元および新しいプロファイルのインポート後、エンドポイントが再プロファイリングされない
CSCvm27249	一時フォルダ内の PassiveID プローブ hprof ファイル
CSCvm29583	ホワイトリストに記載されていないドメイン ルックアップが失敗したため、ISE AD ルックアップが解除される

不具合 ID 番号	説明
CSCvm31919	IE11：コンテキストの可視性の MAC アドレス検索ボックスにリンクされている、ごみ箱アイコン
CSCvm32107	ルート ネットワーク デバイス グループを削除できない
CSCvm32303	Rest API：ToDate フィルタを使用してゲスト ユーザの詳細を取得できない
CSCvm33217	複数のスペースがある AD グループで authZ ポリシーを保存できない
CSCvm33673	説明に関する Oracle と ES の違い
CSCvm34694	新しく作成されたネットワーク デバイスのモデル名とソフトウェア バージョンが GUI に表示されない
CSCvm39902	再認証オプションが機能しなくても接続が維持される
CSCvm39909	ライブ ログの詳細レポートのセッション タイムアウトには秒単位ではなくミリ秒が表示される
CSCvm41485	ISE 2.3：NFS リポジトリを使用して機能していない NFS リポジトリおよびスケジュールされたレポートにアクセスできない
CSCvm41759	[ゲストアカウントの管理（Manage Guest Accounts）] ページで [サインアウト（Sing Out）] をクリックすると、「エラー400」が表示される
CSCvm45072	pxGrid Web アプリケーションでの OWASP ZAP レポートのクロスサイト スクリプティング（DOM ベース）
CSCvm45330	pxGrid 証明書を変更すると、onAuthzRequest が拒否される
CSCvm45941	先頭にゼロを使用すると、ISE 2.4 がプロファイルの「Framed-IP-Address」属性を送信しない
CSCvm47317	ISE 2.4 のアップグレードが成功しても、30 GB 以上のファイルが残っている
CSCvm47507	許可されたプロトコルに加えられた変更が変更設定監査レポートから欠落している
CSCvm47638	ゲストアカウントが一時停止または削除されると、ISE セカンダリ ノードが COA を送信しない
CSCvm48075	ユーザがライブ ログまたはライブ セッションにアクセスしたことがない場合、コンテキストの可視性で手動 CoA が失敗する
CSCvm49084	ISE PB ポータル ファイルは、古いバックアップを復元しても復元されない

不具合 ID 番号	説明
CSCvm49503	実行時に WasMachineAuthenticated EQUALS False が解析されなくなる：ISE 2.4
CSCvm57650	BYOD TLS が IOS 12 FCS リリースで動作しない
CSCvm61134	サービスが再起動されない限り、SXP デバッグ ログは sxp.log にダンプされない
CSCvm62783	「EST-CSR-Request」ディクショナリ条件が機能しない
CSCvm62862	Cisco Identity Services Engine のロギング クロスサイト スクリプティングの脆弱性
CSCvm66696	エンドポイント ID グループの変更時の ISE 2.4 条件付き CoA の障害
CSCvm66751	ゲスト AUP：AUP の承認がレプリケーション イベントをトリガーする
CSCvm67561	ASR1K のアカウンティング メッセージが保存されず、ISE レポートに表示されない
CSCvm69965	Chrome：新しい ByoD ポータルを作成できない
CSCvm70470	最大セッション値が 2.2p10 または 2.3p4 の適用後に GUI に適用できない
CSCvm71860	Cisco Identity Services Engine 反射型クロスサイト スクリプティングの脆弱性
CSCvm71871	Cisco ISE パス トラバーサルの問題
CSCvm72187	ISE 2.2 | ゲスト自己登録ポータルでタイムゾーン リストが正しくソートされない
CSCvm72309	AD プローブが FQDN を使用してコンピュータ オブジェクトを見つけられない
CSCvm73506	アラーム：プロファイラ キュー サイズの制限に到達
CSCvm73626	時間制限付きゲスト タイプでスポンサーがランダム アカウントの作成に失敗する
CSCvm74423	ISE 2.4：CSV からのインポート中にゲスト ユーザが電子メールを自動的に取得しない
CSCvm74605	ISE：アカウント OU の変更後、EAP-FAST が新しい DN 経由でキャッシュされた AD DN を優先する
CSCvm75687	MyDevices ポータル：セカンダリ PAN で実行されている PSN のデバイス ステータスを変更できない

不具合 ID 番号	説明
CSCvm75765	ISE：「ユーザの電子メールが有効ではありません（user's email is not valid）」：.com や .in 以外のトップ レベル ドメインのユーザを作成できない
CSCvm75790	ADFS を使用する SAML がサードパーティ NAD で解除されている
CSCvm76717	ISE 2.4 の複製に失敗し、ノードが LAN の自動化後に同期しなくなる
CSCvm79293	ISE 2.2 TACACS が長い正規表現引数の後にコマンド セットを適用しない
CSCvm79609	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
CSCvm79618	Cisco ISE ローカル権限昇格の脆弱性
CSCvm80914	ISE 2.4 のスケジュール バックアップが機能しない。GUI で確認できる
CSCvm81243	endpointcert/certRequest API コールにより、ISE で内部 CA サービスがクラッシュする
CSCvm82504	Radius トークン サーバのパスワード キャッシングを 900 秒以上に増やすように要求される
CSCvm86244	内部実行コンテキストが API 実行コンテキストから完全に更新されていない
CSCvm86699	ISE CAC または証明書のログインで新しい管理者グループの下に外部グループが入力されない
CSCvm87685	メニュー アクセスの重複がプラス記号を使用すると失敗する
CSCvm88149	アカウント無効化ポリシー「数日間の非アクティブ後にアカウントを無効にする（Disable accounts after days of inactivity）」が正しく計算されない
CSCvm89126	ISE 2.3 パッチ 5：NAD/AAA サーバ アドレスが指定されていない
CSCvm89837	日本語 GUI を使用すると、マイ デバイス ポータルで [紛失（Lost）] または [盗難（Stolen）] ボタンが無効のままになる
CSCvm90359	XCP の実行停止の原因となる pxGrid デバッグ「警告」レベル
CSCvm91034	pxGrid：EndpointProfileMetaData が Pxgrid V2 で伝搬されない
CSCvm91202	Cisco Identity Services Engine のパスワード回復の脆弱性
CSCvm92317	ISE Kerberos 認証で AD の不正なパスワード カウントが 2 ずつ増加する
CSCvm93698	2.2 P11/2.4 P4 の適用後に AD 認証が失敗する

不具合 ID 番号	説明
CSCvm93821	ID グループを条件として使用すると、認証ポリシーの評価が断続的に失敗する
CSCvm98407	show members により、NDG ページでの N/w デバイスの取得に遅延が発生する
CSCvm99398	大規模 NAD 環境での SGACL プッシュにより、PAN の CPU が高くなる
CSCvn01019	既存のネットワーク デバイス プロファイルの変更、灰色の [保存（SAVE）] ボタン
CSCvn04051	ISE 2.4：パッチ 1 のインストール後、REST API クエリに「エラー 500」の詳細が表示されない
CSCvn09504	Qualys で設定された TC-NAC が到達不能であると表示される
CSCvn11424	PassiveID 管理ログが DC 名の代わりにデータベース ID を表示する
CSCvn12114	証明書認証プロファイルに内部ユーザ グループを追加する必要がある
CSCvn12442	高負荷時、ISE 2.3 の ISE ライブ ログが動作を停止する
CSCvn13802	ISE 2.4：共有秘密に「<」が含まれている場合、ネットワーク デバイスをインポートできない
CSCvn17210	trustsec マトリックスで空のセルをインポートする ISE がセルの既存のコンテンツを上書きしない
CSCvn18758	OSX Mojave（10.14）のプロファイラ定義が ISE 2.4 の最新のパッチでは使用できない
CSCvn21316	ISE：logwatch プロセスが ::1 の致命的なエラーにより失敗する
CSCvn22251	ISE 2.4 パッチ 4 により I/O 読み取り速度が低下する
CSCvn23570	ISE：インポート ネットワーク デバイスが管理者アクセス権限に準拠していない
CSCvn24356	パブリッシュおよびダウンロードで無効な xml 文字を処理しない pxGrid
CSCvn25367	VCS ページの認証/エンドポイント タブに空白のポップアップ メッセージが表示される
CSCvn29633	ISE がリスナーの機能に従っていない
CSCvn31277	ISE：Trustsec アラームに重大度レベルが表示されず、グレー表示されている
CSCvn31755	スポンサー ポータルのログアウト時の 400 不正な要求

不具合 ID 番号	説明
CSCvn33441	RBAC 権限が AD を使用して ISE にログインする管理者ユーザに伝播されない
CSCvn33534	レポート ログが「過去 30 日間」で完全に表示されない
CSCvn35579	ISE と IOS デバイス間の SXP 接続が DeleteHoldDown 状態でスタックする
CSCvn36029	コンテキストの可視性のエクスポート時の Unix エポック形式の日付
CSCvn37048	ISE 2.x || ISE syslog メッセージ コード（59200-59208）が ISE で現在使用されていない
CSCvn40645	2.4P5：P5 PSN のロールバック後の 3 ノード展開でダウンする
CSCvn50203	ISE 2.4p5：ACI 統合：ACI 上のすべての IP_EPG マッピングが ISE でインポートされないことがある
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
CSCvn52114	外部 radius トークン サーバ認証を使用したプロセスが失敗する
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
CSCvn56648	個々のポリシー セットがリセットされると、他のポリシー セットのヒット カウンタが 0 にリセットされる
CSCvn59383	特殊文字を使用してスポンサー ポータルでゲスト ユーザを作成する場合の ISE 2.3 パッチ 5 の問題
CSCvn59502	ISE DACL 構文チェックでエラーが正しく検出されない
CSCvn62164	ISE では、ACS の一部である特殊文字コロン「:」を使用して内部ユーザをサポートする必要がある
CSCvn62788	Qualys で設定された TC-NAC が到達不能であると表示される
CSCvn67968	IPv6 ルートの追加後、ISE が独自のサブネット内の IPv6 ホストへの応答を停止する
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
CSCvn79861	ResetAll ヒットカウント ボタンで Firefox ブラウザのヒットカウント値がリセットされない
CSCvn81631	ISE 2.4 から 2.5 へのアップグレード後にすべてのノードで一貫して生成されるコア

不具合 ID 番号	説明
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

Cisco ISE リリース 2.4.0.357 の新機能 - 累積パッチ 6

RADIUS トークンおよび RSA SecurID サーバの ID キャッシング

ID キャッシングは、サーバに対する認証を実行しない要求の処理を許可するために使用されます。ID キャッシング オプションを有効にし、エージング タイムを分単位で設定できます。デフォルト値は 120 分です。有効な範囲は、1 ～ 1440 分です。最後に成功した認証から取得された結果が、指定された時間、キャッシュ内で使用可能になります。

このオプションはデフォルトでは無効になっています。

Cisco ISE リリース 2.4.0.357 の未解決の不具合 - 累積パッチ 6

不具合 ID 番号	説明
CSCvo75376	Cisco Firepower Management Center（FMC）の pxGrid ノード名の制限が短すぎる

Cisco ISE リリース 2.4.0.357 の解決済みの不具合 - 累積パッチ 5

次の表は、リリース 2.4 累積パッチ 5 で解決済みの不具合のリストです。

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 2.2.0.53 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
CSCvj62599	Adobe Action Message Format（AMF）での Cisco Identity Service Engine（ISE）の安全でない逆シリアル化
CSCvb45390	ユーザ名を使用して設定された収集フィルタが TACACS の作成者/アカウントに対して機能しない
CSCvj86877	SFTP 接続エラー
CSCvm03681	EAP-FAST が TLS 1.2 で正しいキー生成をサポートしていない
CSCvm91034	pxGrid：EndpointProfileMetaData が Pxgrid V2 で伝搬されない
CSCvm93698	2.2 P11/2.4 P4 の適用後に AD 認証が失敗する
CSCvn09504	Qualys で設定された TC-NAC が到達不能であると表示される

不具合 ID 番号	説明
CSCvk13724	ISE で EPG マッピングが作成されない
CSCvn17524	ISE Apache Struts CVE-2016-1000031 の脆弱性

Cisco ISE リリース 2.4.0.357 の解決済みの不具合 - 累積パッチ 4

次の表は、リリース 2.4 累積パッチ 4 で解決済みの不具合のリストです。

パッチ 4 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 2.2.0.53 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
CSCuq95531	診断ツール：DNS の場合、レコード テストの変更ステータスが失敗して警告に変わる
CSCuz52877	ISE21：15 分ごとの認証非アクティブ アラーム
CSCvf75225	ISE 2.1-P3 || redis で 100K に制限されているため、PAN の高 CPU が検出される
CSCvh25718	ポータルではなく 802.1x でクレデンシャルが使用されている場合、ISE はゲスト ユーザ名を小文字に変換しない
CSCvh54905	ID 管理者の [ID（Identities）] タブの下にユーザを表示できない
CSCvh74979	設定のリセットにより、パッチの修正が復元され、問題が発生する
CSCvi10363	ISE：アクセス許可パケットから状態属性を削除する
CSCvi23542	ストレス認証中に予期しないエラーが発生する。RPC ログオン要求が失敗した。STATUS_ACCESS_DENIED
CSCvi50536	2018 年 2 月 Apache Tomcat 用 ISE の評価の脆弱性
CSCvi58316	ISE：ACS を ISE 移行セットアップにアップグレードするため、URT が失敗する
CSCvi85159	Cisco Identity Services Engine クロスサイト リクエスト フォージェリの脆弱性
CSCvi88520	メッセージ コード 89006 のみを表示し、残りは表示しないメッセージ カタログ
CSCvj36442	共有秘密がプレーンテキストであるため、[ネットワークデバイス（Network devices）] ページのページネーションが失敗する

不具合 ID 番号	説明
CSCvj44088	ISE：登録時、「ノード<fqdn>バージョン:0.0.0.0. を登録できない（Unable to register the node <fqdn> Version: 0.0.0.0.）」というメッセージが表示される。
CSCvj57771	一般的なパッチ管理：Red Hat Linux（クリティカル/高）
CSCvj57967	アプリケーション チェックが反対のロジックで動作する
CSCvj70896	sgt タグ 5 の sgt 名の取得に失敗したり、sgt が読み取り専用であったり、isPropgateToAPIC が false であったりする
CSCvj97277	CSCvf68738 の修正で正当な CA 証明書の更新が許可されていない
CSCvk07631	ISE 2.2：ホット スポット ポータル ユーザが AUP を複数回許可するように要求される
CSCvk09597	VM ライセンスのしきい値の不一致プラットフォームの定義
CSCvk10303	ISE 2.4 Trustsec ダッシュボード クエリのパフォーマンス
CSCvk10454	展開にノードを追加しても、プロファイリング OUI データが追加されない
CSCvk10674	IP フォン内の ISE 2.4 Windows PC が Cisco-IP-Phone-8851 としてプロファイリングされる
CSCvk12450	回帰：Windows 8/10 クライアントがフィード ポリシーにより誤って windows7 としてプロファイリングされる
CSCvk13569	ISE ADRT が子ドメイン名をルート フォレスト ドメインと誤認するため「ERROR_NO_SUCH_USER」が表示される
CSCvk16959	ISE 2.4 パッチなし：[ネットワークデバイス（network devices）] ページをロードできない
CSCvk19766	ISE 2.4 MnT セッション と Auth API 応答が「other_attributes」セクションを指定しない
CSCvk40421	信頼できるページから証明書を削除できない
CSCvk43032	COLLATIONDAILY_PURGE、HOURLY_STATS_JOB へのコールで間違った番号または引数のタイプが存在する
CSCvk48315	ライブ セッションが ISE 2.4 の ISE ライブ ログ ページには表示されない
CSCvk51667	ISE：スポンサー ポータルが SAML 認証用に設定されている場合、「アカウントの管理」で 400 HTTP エラーが表示される
CSCvk55065	セカンダリ MNT に対する ISE 2.4 PxGrid クエリにより、コレクタがクラッシュする

不具合 ID 番号	説明
CSCvk61086	ISE 2.4 2.3 2.2 2.1 2.0：NFS リポジトリ クレデンシャルが使用されない
CSCvk65898	ISE 2.4：Facebook 側で行われた最近の変更が原因で、ソーシャル ログイン e2e フローが失敗する
CSCvk71161	MNT に送信される ISE 2.4 の過剰なプロファイラ syslog
CSCvk74356	ISE 2.4 Cisco Prime クエリ ISE セッション API により、モニタリング ノードの CPU 使用率が高くなる可能性がある
CSCvk74989	DNAC 信頼の再確立後に証明書パラメータが永続的ではなくなる
CSCvk75544	認証サマリー レポートで Radius および TACACS の「使用可能なデータがありません（no data available）」と表示される
CSCvk76510	プライマリ ノードの ISE 2.4 コア ダンプ：GenericConfigObject::getAsNested(unsigned int) const の SIGSERV
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」
CSCvm02478	GooglePlay で CISCO Network Setup Assistant アプリが使用できない
CSCvm05439	同じチェーンが使用されている場合の DNAC 確立後の LDAP テスト サーバ上の ISE コア
CSCvm05499	ISE CoA が NAS-Port-Id に NULL 値を送信する
CSCvm11175	ISE カスタム エンドポイント属性タイプ文字列が数字のみを許可しない
CSCvm11230	ライブ ログの [詳細（Details）] ページのこのレコードで利用可能なデータがユーザに表示されない
CSCvm11595	ユーザ名に unicode 文字が含まれているため、LiveSessions が GUI に表示されない
CSCvm12575	ISE コンテキストの可視性エンドポイントのインポートがカスタム エンドポイント属性の日付で失敗する
CSCvm14030	Struts リモート コード実行の脆弱性に関する positron の評価（2018 年 8 月）
CSCvm17749	ポータル セッションの削除が原因でゲストおよびスポンサー ポータルで 400 エラーが表示される
CSCvm17795	GUI からトリガーされた設定バックアップが ES バックアップ中に 45% で終了する

Cisco ISE リリース 2.4.0.357 の未解決の不具合 - 累積パッチ 4

不具合 ID 番号	説明
CSCvm93698	ISE 2.4 パッチ 4 のインストール後に AD 認証が失敗する。ad_agent.log に次のエラーが表示される場合がある。`Identity resolution failed - ERROR_NO_SUCH_USER_SOME_DOMAINS_NOT_AVAILABLE`
CSCvm75266	ISE 2.4：利用可能なカーネル メモリのリーク
CSCvm72528	ISE 2.4 パッチ 3：CTS ロールベースのポリシーで COA が機能していない
CSCvm90852	ISE 2.4 パッチ 4 のリポジトリとして SFTP サーバを使用できない

Cisco ISE リリース 2.4.0.357 の解決済みの不具合 - 累積パッチ 3

次の表に、リリース 2.4 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 2.2.0.53 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
CSCvd78169	SNMP クエリを介して EP に追加されない CDP 属性
CSCvf75225	ISE 2.1-P3 || redis で 100K に制限されているため、PAN の高 CPU が検出される
CSCvf75968	httpasyncclient の複数の脆弱性
CSCvf82350	US27030：MAC マッピングへの VPN セッションを修正
CSCvg46899	ISE 2.2 ユーザがホットスポット ポータルでの AUP 承認後に再度リダイレクトされる場合がある
CSCvh54726	ISE：Intel AMT サプリカント ユーザ名形式の AD グループの取得に失敗する
CSCvh91996	GUID で表示されるが名前ではない、モニタ専用モードの AuthC および AuthZ ルールが一致した
CSCvi03093	ID グループ名が変更された場合/変更が消去ポリシーに反映されない場合、消去が機能しない
CSCvi06525	暗黙的/明示的 UPN を使用する自己登録ゲストが表示されないシングル クリック承認スポンサー
CSCvi31965	内部エンドポイントでのルックアップによる ISE 認証の高遅延

不具合 ID 番号	説明
CSCvi66786	MNT ノードでの timesten のクラッシュが原因でコアファイルが生成される
CSCvi74182	ログ収集エラー：null アラーム
CSCvj02644	RADIUS ライブ ログに空白の [詳細（Details）] ページが表示される
CSCvj37364	インポートされたゲスト通知テンプレートのコンテンツの変更が機能していない
CSCvj38428	ネットワーク アクセス ユーザのステータスの変更が監査レポートに表示されない
CSCvj41029	ISE のパッシブ ID AD エージェントまたは MS WEF を使用している場合、セッションのユーザ ドメイン名が空のままになることがある
CSCvk19766	ISE 2.4 MnT セッション と Auth API 応答が「other_attributes」セクションを指定しない
CSCvk48105	スポンサーが作成したゲストに以前のゲスト アカウントの電子メール CC が使用される
CSCvk57963	ISE 2.4 パッチ 2 インストールでは、整合性チェックサムの失敗が原因でアプリケーション サービスが終了する
CSCvm14030	Struts リモート コード実行の脆弱性に関する positron の評価（2018 年 8 月）
CSCvm17749	ポータル セッションの削除が原因でゲストおよびスポンサー ポータルで 400 エラーが表示される

Cisco ISE リリース 2.4.0.357 の解決済みの不具合 - 累積パッチ 2

次の表に、リリース 2.4 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 2.1.0.53 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
CSCvc71503	プールに戻る Jedis 接続：接続の切断（タイムアウトによる）
CSCvf20208	ISE ポスチャ PRA タイマーの期限が切れ、非準拠になる
CSCvf52213	ENH：インターフェイスでの MTU 設定に対する ISE CLI サポート

不具合 ID 番号	説明
CSCvg75818	ISE 2.2 から 2.3 へのアップグレードが「CREATE UNIQUE INDEX CEPM.PKUPSABSTRACTTYPE_ATTRIBUTES」で失敗する
CSCvh86466	PassiveID：WMI クエリ DC が原因で、DC のメモリが増える（Microsoft WMI メモリ リーク）
CSCvi29600	内部ユーザが AD パスワードを使用している場合、スポンサー グループが AD スポンサー グループと結果をマージしない
CSCvi50542	設定可能な ISE テレメトリ スケジューラ
CSCvi51021	plus/advanced ライセンス スタンドアロン ノードがない場合、コンテキストの可視性で利用可能なデータがない
CSCvi68271	ドキュメントに記載されているように、[説明（description）] フィールドを返さないすべてのエンドポイントを ERS API が取得する
CSCvi73782	DHCP プローブによりドロップされるスタティック グループの割り当て
CSCvi79632	アカウンティング アクティビティがない場合、ライブ セッションは 5 日間すべてのセッションを保持する
CSCvi82192	[pxGrid証明書の生成（Generate pxGrid Certificates）] ページに証明書テンプレートの RSA キー サイズが反映されない
CSCvi91353	NMAP はカスタム ポート 9100 をスキャンするけれども、nmap.log にはレポートしない
CSCvj08379	ISE 2.4 EPSStatus がコンテキストの可視性で適切に更新されない
CSCvj11319	ISE 2.4：2.3 のアップグレード後に EST サービスが実行されない
CSCvj11981	SNMP ポーリング時間の変更後、認証なしのセキュリティ レベルで NAD の SNMPv3 プロファイラが中断する
CSCvj13401	ネットワーク デバイスのインポート時の ISE [属性プロトコルの失敗値は必須です（Failed Value for attribute Protocol is mandatory）]
CSCvj20617	KEK の変更により 2.4 へのアップグレードが失敗する
CSCvj42529	ISE：ゲスト作成 POST の成功から 60 ～ 90 秒後の API POST 401 未認証
CSCvj47154	ISE 2.4 がデフォルトの認証ポリシーで plus 追加ライセンスを消費している
CSCvj52267	TACACS デバイス ネットワーク条件下の IPv6 サブネットに対する ISE 2.4 入力検証エラー

不具合 ID 番号	説明
CSCvj66943	ISE が「属性の取得」に LDAP で SSL を使用しないけれども、ポート 636 に接続する
CSCvj72180	ENH：ISE：RPC エラー 121 に関係なく、新しいパスワードが有効な場合、新しい m/c パスワードが ISE 側に保存される
CSCvj79271	セカンダリ MNT：フォルダ Timesten_Data の不適切な timesten 権限の問題
CSCvj88674	ISE 2.4 リリースでスマート ライセンスの有効化が失敗している
CSCvj90439	trustsec マトリックスで使用されている SGT を削除することができない
CSCvj92358	アップグレード後にセカンダリ ノードの UDI 値が sec_hostconfig テーブルから消える
CSCvk28377	MnT はデータベースを変更せずに頻繁なアカウンティングの Interim-updates を維持する
CSCvk31092	コア：SyslogSecureTCPConnection::updateConnectionData
CSCvk57963	ISE 2.4 パッチ 2 インストールでは、整合性チェックサムの失敗が原因でアプリケーション サービスが終了する
CSCvi44041	Cisco Identity Services Engine の権限昇格の脆弱性

Cisco ISE リリース 2.4.0.357 の解決済みの不具合 - 累積パッチ 1

不具合	説明
CSCvi36111	ライブ セッション：ipv6 で NAS IP アドレスのツールチップが重複する
CSCvi47074	SXP 接続のダウン中に SXP ノードでレプリケーションの障害が検出される
CSCvi48886	アップグレード後：GuestVLAN が omapi.key のキーを DHCP にコピーしない
CSCvi50979	マシン変更パスワードの間隔を高度な調整パラメータ（Kerberos SSO）から設定する必要がある
CSCvi56003	ISE 2.4 の自己登録フォームの AUP リンクが不正な要求をスローする

不具合	説明
CSCvi69286	[ダッシュボード（Dashboard）] > [検索（Search）]：エンドポイントの詳細画面が Internet Explorer で正常に動作しない
CSCvj11476	ISE：一部のリソースで参照されている証明書を削除すると、誤ったエラー メッセージが表示される
CSCvi53593	CoA を発行しようとした場合、MAC アドレスが選択されていない場合の誤ったメッセージ
CSCvj61368	2.4 P1：ISE インデックス サーバがセカンダリ PAN で実行されていない
CSCvi38373	ISE でコンテキストの可視性内のすべてのエンドポイントを削除する場合、リスクが非常に高い
CSCvh93370	ISE ゲスト：syslog の誤ったアカウンティングが原因で問題が発生する
CSCvi06647	Anyconnect の設定：コンプライアンス モジュールのドロップ メニューが空
CSCvi61330	Radius/DTL 認証後の不定期なアプリケーションの再起動
CSCvg90863	「Application Configure ISE」のアイドル時間が長くなると、SSHD が無効になる
CSCvj17258	ISE 2.4 が古い DNAC クライアント証明書を保持するため、ISE を使用した新しい DNAC pxGrid が失敗する
CSCvj33336	DNAC1.2：プロビジョニング後に ISE 2.4 に追加されないネットワーク デバイス
CSCvi49103	NAD CSV エクスポートで「Enable Multi Shared Secret:String(128)」のデータ タイプが正しくない
CSCvg19708	ゲスト アカウンティング レポートの破損

Cisco ISE リリース 2.4.0.357 の解決済みの不具合

（注） Cisco ISE 2.4 パッチ 0 には、Cisco ISE 2.0 パッチ 6、2.0.1 パッチ 5、2.1 パッチ 6、2.2 パッチ 6、および 2.3 パッチ 2 とのパリティがある

次の表は、リリース 2.4 で解決済みの不具合のリストです。

表 *2 : Cisco ISE* リリース *2.4*、解決済みの不具合、パッチ *0*

不具合	説明
CSCvf69805	Cisco Identity Services Engine クロスサイト リクエスト フォージェリの脆弱性
CSCvf49844	Cisco Identity Services Engine のローカル コマンド インジェクションの脆弱性
CSCvf63414	Cisco Identity Services Engine によって認証された CLI のサービス拒否の脆弱性
CSCvh51992	Cisco Identity Services Engine によって認証された CLI のサービス拒否の脆弱性
CSCvf69753	Cisco Identity Services Engine によって認証された権限昇格の脆弱性
CSCvf69963	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvg95479	Cisco Identity Services Engine の基盤となる OS へのコマンドインジェクションの脆弱性
CSCvd38467	BYOD が Apple iOS 10.3.x で動作しない
CSCvf29467	複数のクライアント プロビジョニング ポリシーを同時に編集すると、結果列が非表示になる
CSCvf33475	同じブラウザでの設定と運用の同時バックアップが非常に遅い
CSCvi45925	新しく作成されたダッシュボードが 2.4 342 ビルドには表示されない
CSCvf28877	ISE 2.3 TACACS+：編集中にコマンドセットにコマンドを追加できない

CSCvf32298	ISE 2.3 スポンサー ポータル：ユーザ名テーブルの更新とカウンタの更新の間に 1 分間の遅延がある
CSCvf32394	ISE 2.3：SMS プロバイダーの自己登録ゲストポータル：他の属性が変更されると、グローバル デフォルトが常に再選択される
CSCvf34216	ISE 2.3：詳細レポートを開くと、[ワークセンター（Work Center）]>[ゲストアクセス（Guest Access）]>[IDグループ（Identity Group）] を選択できない
CSCvh05703	ユーザ情報を保存（Remember Me）：RADIUS ライブ セッション ビューにゲスト デバイスのユーザ名が表示されない

Cisco ISE リリース 2.4.0.357 の未解決の不具合

次の表は、リリース 2.4 で未解決の不具合のリストです。

不具合 ID 番号	説明
CSCvf30591	ISE 2.2：パスワードの有効期間が無効にされる。ただし、アカウントの有効期限の通知は受信する。
CSCvg80657	ディスク メンテナンス。ESR 5921 IOS crashinfo ファイルの自動およびオンデマンド クリーンアップが必要
CSCvg80766	「application configure ise」コマンドによりすべての CLI セッションが突然終了する
CSCvh20790	[レポートの更新（Update Report）] ページ移動しても、「データが見つかりません」
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
CSCvh22984	複数のスポンサー アカウントを一度に削除することができない
CSCvh65530	NDG フラット テーブル ページで動作していないデバイスの数ごとのフィルタ
CSCvh69481	一部のオブジェクトで filtertype=OR を指定した Get-All が機能しない
CSCvh77969	VSW 後にユーザの可視性が機能しない
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

不具合 ID 番号	説明
CSCvh93771	HTTPS://<IP>:<port-non-443> で PAT/NAT を使用する 管理 Web UI アクセスが切断される
CSCvh95370	AlcatelWired へのネットワーク デバイスのデフォルト デバイス プロファイルの作成
CSCvi48276	ISE の AMP がクラウドからの登録解除後も接続されたままになる
CSCvi48298	特定のケースで新しいポリシーを作成している間にポリシー ヒット カウント値が無効になる
CSCvi60160	Active Directory 診断ツールで [実行中のすべてのテストを停止（Stop All Running Tests）] が正しく機能しなくなる
CSCvi85015	Vlan 更新用の Anyconnect プロファイル：注意事項がわかりにくい
CSCvi88520	メッセージ コード 89006 のみを表示し、残りは表示しないメッセージ カタログ
CSCvi90269	ピアの接続がオンにもかかわらず、ISE UI の SXP デバイス接続ページで ISE がオフになっていると表示される
CSCvj06916	ISE 2.3+：ext radius 順序を使用すると、ポリシーセット内の認証/許可ポリシーを設定できない
CSCvj13757	ISE 2.4：AD 診断失敗アラームを確認応答できない
CSCvj22303	エンドポイント OS が外部のモバイル デバイス管理レポートで誤って更新される
CSCvj28192	ISE 2.4 GUI tcpdump に -s 0 オプションが組み込まれていない
CSCvj29551	実在しないカスタム属性に基づいてポリシーをインポートする場合に警告/エラーが表示されない
CSCvj31598	機能拡張要求：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
CSCvj50085	コンテキストの可視性からエンドポイントを削除した後、ホームページにアクティブなエンドポイントが 0 と表示される
CSCvj50257	アクティブなエンドポイントが予想された値と一致しない
CSCvj54057	NAD ホスト名と IP アドレスを指すように、アラーム [TrustSec PACの検証の失敗（Trustsec PAC validation failed）] を拡張する必要がある
CSCvj73152	ISE 2.4 の VLAN DHCP リリースの有効化により、ゲスト フローが切断される

不具合 ID 番号	説明
CSCvj73550	スイッチと ISE 間の EAP-FAST 通信が失敗するため、CTS PAC の更新に失敗する
CSCvj77125	Cisco Wave 2（別名 COS）AP 1800/2800/3800 で cdpCachePlatform ルールが一致しない
CSCvj83961	非管理インターフェイスを使用する CWA がゲスト フローのセカンダリ インターフェイス fqdn を置き換えられない
CSCvj88164	リモート アクセス VPN ポスチャ セッションで Apex ではなく基本ライセンスが消費されていると表示される
CSCvj93331	次のページへのリンクが REST 応答に存在しない
CSCvk06884	REST コールに誤ったデータを指定した場合、ISE は 500 ではなく 400 HTTP エラーを返す必要がある
CSCvk09565	ISE 2.x 以降の RFC 3164 に完全には準拠していない
CSCvk12450	回帰：Windows 8/10 クライアントがフィード ポリシーにより誤って windows7 としてプロファイリングされる
CSCvk25549	オフラインのプロファイラ フィード更新 web ページでオフライン フィード オプションが見つからない
CSCvk34422	プロファイラ：フィードのダウンロード：FeedEndpointPolicy を更新できない
CSCvk40421	信頼できるページから証明書を削除できない
CSCvk48315	ライブ セッションが ISE 2.4 の ISE ライブ ログ ページには表示されない
CSCvk55076	プロファイラ AD プローブが原因で ISE 2.4 がスタティック グループ マッピングを失う
CSCvk55285	ISE がカスタム エンドポイント属性のデータ タイプの日付を検証しない
CSCvk59357	新しいライセンスを追加しても、管理者にライセンス違反の警告が表示される
CSCvk65179	証明書の使用に証明書を割り当てる場合のエラー。ログイン ポータルにアクセスできない
CSCvk65898	ISE 2.4：Facebook 側で行われた最近の変更が原因で、ソーシャル ログイン e2e フローが失敗する
CSCvk67692	ISE 2.x：REST API Get-All 内部ユーザ結果で XML と JSON 出力に「next-page」リンクが見つからない

不具合 ID 番号	説明
CSCvk68196	SNMPv3 プロファイリングが DES または AES128 プライバシー プロトコルでのみ機能する
CSCvk71555	アプリケーション条件の逆ロジックを設定できない
CSCvk72920	ISE で CDP の SNMP 一括要求を一度送信すると、再度送信しない
CSCvk74989	DNAC 信頼の再確立後に証明書パラメータが永続的ではなくなる
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」
CSCvm03411	カーネル側：L1 端末障害を使用したチャネル攻撃：CVE-2018-3620 および CVE-2018-3646（Foreshadow-NG）
CSCvm03842	PxGrid SSL/TLS 再ネゴシエーション ハンドシェイク MiTM プレーンテキスト データ インジェクション：CVE-2009-3555
CSCvm05439	同じチェーンが使用されている場合の DNAC 確立後の LDAP テスト サーバ上の ISE コア
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
CSCvm06464	ISE：SNMPv3 がトラップを送信しない
CSCvm06688	GUI からのインストール後にパッチのインストールに問題がある場合、CLI からのパッチのロールバックが失敗する
CSCvm07566	ISE 2.4 への ACS 移行により、ID ソースの順序付けが中断される
CSCvm09377	電子メールに @ が含まれる場合、ISE の HTTP 要求ヘッダーが失敗する
CSCvm10559	ISE 2.4 で仮想ネットワークに関連付けられている未使用の SGT を削除できない
CSCvm11175	ISE カスタム エンドポイント属性タイプ文字列が数字のみを許可しない
CSCvm11230	ライブ ログの [詳細（Details）] ページのこのレコードで利用可能なデータがユーザに表示されない
CSCvm12215	データベースのリセット時にパッチのインストールで SQL 修正を再適用する必要がある
CSCvm12484	信頼確立中にクロックが同期していない場合、ISE が DNAC に誤ったメッセージを送信する
CSCvm17795	GUI からトリガーされた設定バックアップが ES バックアップ中に 45% で終了する

不具合 ID 番号	説明
CSCvm19797	ホットフィックスのインストールで誤ったエラー メッセージが生成される
CSCvm19803	ISE 2.4 のエンドポイントが誤った論理プロファイルに関連付けられている
CSCvm20561	ISE 2.x || シスコ デバイスのプロファイラ ポリシーで、tandberg OUI が条件として欠落している
CSCvm22838	エンドポイントのプロファイルを変更すると、最初のプロファイラ CoA の後に CoA が送信されない
CSCvm23096	PSN がダウンし、初期化状態のままになる
CSCvm26207	ISE メトリック。コンプライアンスの割合で、実際のエンドポイントがポスチャを介せず、エンドポイントの総数から計算される
CSCvm26372	セカンダリ PAN で 2.4 パッチ 3 をインストールした後、ISE Indexing Engine が実行されない
CSCvm29083	論理プロファイルを使用すると、ISE 2.4 で設定された認可ポリシーが適切なポリシーと一致しない
CSCvm29136	Windows7：ワークステーション ポリシーがルール WinPlatform 確実度係数で誤っている、または 40 になる
CSCvm29577	ISE 2.4：コンテキストの可視性ユーザ：Active Directory 属性が保存されない
CSCvm31919	IE11：コンテキストの可視性の MAC アドレス検索ボックスにリンクされている、ごみ箱アイコン
CSCvm32107	ルート ネットワーク デバイス グループを削除できない
CSCvm32303	Rest API：ToDate フィルタを使用してゲスト ユーザの詳細を取得できない
CSCvm33217	外部ドメイン ユーザ グループを条件として使用する認証ポリシーを保存する場合にエラーが発生する
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 P6 から利用できない

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、Cisco Support 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。

Cisco バグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

【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。