

Cisco Identity Services Engine リリース 3.3

リリースノート

最終更新：2025 年 3 月 24 日

Cisco Identity Services Engine の概要

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、ユーザー、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、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、ローカル 5G ネットワーク、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 グループ ベース ポリシー 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 Cisco Secure Network Server アプライアンス、仮想マシン (VM)、およびパブリッククラウドで使用できます。

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。

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 注文ガイド](#) [英語] を参照してください。

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 管理者ガイド](#)』の「Cisco ISE のモニタリングとトラブルシューティング サービス」のセクションを参照してください。

このリリースの新機能

このセクションでは、Cisco ISE 3.3 およびそのパッチの新機能と変更された機能をすべて示します。

Cisco ISE リリース 3.3 - 累積パッチ 4 の新機能

Tenable Security Center の API キーと証明書認証のサポート

Cisco ISE 3.3 パッチ 4 以降では、Tenable Security Center で次の認証方式が追加でサポートされています。

- [API Keys] : Tenable Security Center のアクセス権限を持つユーザーアカウントのアクセスキーと秘密鍵を入力します。

API キー認証は、Tenable Security Center 5.13.x 以降のリリースでサポートされています。



- (注) Cisco ISE でこのオプションを選択する前に、管理者ユーザーとしてログインして、Tenable Security Center で API キー認証を有効にする必要があります。

- [Certificate Authentication] : [Authentication Certificate] ドロップダウンリストから必要な証明書を選択します。

認証に成功すると、Cisco ISE はカスタマーが設定したテンプレートを Tenable Security Center から取得します。



- (注) Cisco ISE でこのオプションを有効にする前に、SSL クライアント証明書認証を許可するように Tenable Security Center を設定する必要があります。

詳細については、『Cisco Identity Services Engine Administration Guide, Release 3.3』の「Threat Containment」の章にある「[Configure Tenable Adapter](#)」[英語]を参照してください。

参加ポイントの専用リソースの割り当て

Cisco ISE リリース 3.3 パッチ 4、以降では、各 PSN の参加ポイントのリソースを予約できます。このリソースセグメンテーションは、参加ポイント間のリソース共有によって引き起こされるパフォーマンスへの影響を軽減するのに役立ちます。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Asset Visibility」の章にある「[Assign dedicated resources for join points](#)」[英語]を参照してください。

証明書のセキュリティ識別子が認証で使用されない

Cisco ISE リリース 3.3 パッチ 4 以降では、セキュリティ識別子 (SID) を使用した新しいフォーマットの証明書がサポートされます。

[Subject Alternative Name (SAN)] フィールド内の SID は、Cisco ISE での認証には使用されません。この機能拡張により、認証プロセスでの誤った SID 解析が原因で発生する認証エラーを防ぐことができます。

SSHD サービス暗号化アルゴリズムの機能拡張

Cisco ISE リリース 3.3 パッチ 4 以降では、**service sshd** にある新しいアルゴリズムを使用して、Cisco ISE CLI でサービスを管理できます。次のアルゴリズムが新しく追加されます。

- **MAC-algorithm**
- **Hostkey**
- **Hostkey-algorithm**
- **Key-exchange-algorithm**
- **SSH-client-hostkey-algorithm**

詳細については、『[Cisco ISE CLI Reference Guide, Release 3.3](#)』[英語] を参照してください。

osquery 条件のサポート

Cisco ISE 3.3 パッチ 4 以降では、osquery 条件を作成してエンドポイントのポスチャ コンプライアンス ステータスを確認したり、エンドポイントから必要な属性を取得したりできます。

詳細については、『[Cisco Identity Services Engine Administrator Guide, Release 3.3](#)』の「Compliance」の章にある「[Add an osquery condition](#)」[英語] を参照してください。



(注) osquery 条件をサポートするには、コンプライアンスモジュール 4.3.3394 以降および Cisco Secure Client 5.1.7 以降のバージョンを使用する必要があります。

usgv6 コマンドのサポート

usgv6 コマンドを EXEC モードで使用すると、基盤となるオペレーティングシステムで Cisco ISE ノードの usgv6 コンプライアンスステータスを有効化、無効化、または確認できます。

詳細については、『[Cisco Identity Services Engine CLI Reference Guide, Release 3.3](#)』の「Cisco ISE CLI Commands in EXEC Mode」の章にある「[usgv6](#)」[英語] を参照してください。

Cisco ISE リリース 3.3 - 累積パッチ 3 の新機能

明示的な曲線の検証を有効または無効にするための CLI オプション

Cisco ISE リリース 3.3 パッチ 3 以降、管理者は **application configure ise** CLI コマンドで次のオプションを使用して、楕円曲線デジタル署名アルゴリズム（楕円曲線 DSA）の明示的な曲線証明書を検証できます。

[39]Enable/Disable Explicit EC Check

証明書の検証は、EAP TLS サーバーモード、Secure Syslog、およびセキュア LDAP に適用されます。

詳細については、『Cisco Identity Services Engine CLI Reference Guide, Release 3.3』の「Cisco ISE CLI Commands in EXEC Mode」の章にある「[Application Configure ISE](#)」[英語]を参照してください。

Duo 接続の作成後にアイデンティティ同期を追加するオプション

Duo 接続の作成中に Active Directory と Duo 間のユーザーデータ同期を設定しない場合は、[Identity Sync] ページで [Skip] をクリックします。[Summary] ページに直接移動します。

Duo 接続を作成した後は、いつでもアイデンティティ同期設定を追加できます。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Segmentation」章にある「[Integrate Cisco Duo With Cisco ISE for Multifactor Authentication](#)」[英語]を参照してください。

Cisco ISE リリース 3.3 - 累積パッチ 2 の新機能

ネイティブ IPsec を使用した仮想トンネルインターフェイス (VTI) の設定

Cisco ISE リリース 3.3 パッチ 2 からは、ネイティブ IPsec 設定を使用して VTI を設定できます。IKEv1 および IKEv2 プロトコルを使用して、IPsec トンネルを介した Cisco ISE PSN と NAD 間のセキュリティアソシエーションを確立するためにネイティブ IPsec を使用できます。ネイティブ IPsec の設定により、Cisco ISE は FIPS 140-3 に準拠します。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Secure Access」の章にある「[Configure Native IPsec on Cisco ISE](#)」[英語]を参照してください。

レガシー IPsec (ESR) のサポート終了

Cisco ISE リリース 3.3 パッチ 2 以降、レガシー IPsec (ESR) は Cisco ISE でサポートされません。Cisco ISE のすべての IPsec 設定が、ネイティブ IPsec 設定になります。トンネルとトンネルの設定が失われないように、Cisco ISE リリース 3.3 累積パッチ 2 にアップグレードする前に、レガシー IPsec (ESR) からネイティブ IPsec に移行することを推奨します。詳細については、『Cisco ISE Administrator Guide』の「Secure Access」の章にある「[Migrate from Legacy IPsec to Native IPsec on Cisco ISE](#)」[英語]を参照してください。

強化されたパスワードセキュリティ

Cisco ISE では、次の機能拡張によりパスワードのセキュリティが向上しています。

- 次のフィールド値の [Show] ボタンを非表示にして、編集集中にプレーンテキストで表示されないようにすることができます。

[Network Devices] で、

- RADIUS Shared Secret
- Radius Second Shared Secret

[Native IPsec]で、

- Pre-shared Key

これを行うには、[Administration] > [Settings] > [Security Settings]の順に選択し、[Show Password in Plaintext] チェックボックスをオフにします。

詳細については、『Cisco ISE Administrator Guide, Release 3.3』の「Segmentation」の章にある「Configure Security Settings」[英語]を参照してください。

- ネットワークデバイスのインポートおよびエクスポート中に RADIUS の共有秘密と 2 番目の共有秘密がプレーンテキストで表示されないようにするために、[PasswordEncrypted:Boolean(true|false)] というヘッダーを持つ新しい列が [Network Devices Import Template Format] に追加されました。この列に必要なフィールド値はありません。

Cisco ISE リリース 3.3 パッチ 1 以前のリリースからネットワークデバイスをインポートする場合は、インポートする前に、このヘッダーを含む新しい列を [Authentication:Shared Secret:String(128)] 列の右側に追加する必要があります。この列を追加しないとエラーメッセージが表示され、ファイルをインポートできません。インポート時にパスワードを復号するための有効なキーが指定されていない場合、暗号化されたパスワードを持つネットワークデバイスは拒否されます。

詳細については、『Cisco ISE Administrator Guide, Release 3.3』の「Secure Access」の章にある「Network Devices Import Template Format」の表を参照してください。

ローカライズされた ISE のインストール

Cisco ISE の再インストール中に、**application configure ise** コマンドで [Localized ISE Install] オプション（オプション 38）を使用して、インストール時間を短縮できます。このオプションは、Cisco Secure Network Server と仮想アプライアンスの両方に使用できますが、Cisco Secure Network Server の再インストール時間を大幅に短縮します。

詳細については、『Cisco Identity Services Engine CLI Reference Guide, Release 3.3』の「Cisco ISE CLI Commands in EXEC Mode」の章にある「Localized ISE Installation」[英語]を参照してください。

認証失敗が繰り返される場合のアイデンティティのロック

アイデンティティをロックしなければならなくなるまでの認証失敗の回数を指定して、EAP-TLS プロトコルを介した認証中にアイデンティティ（ユーザー名またはホスト名）が失敗できる認証試行の最大回数を制限できるようになりました。アイデンティティは、永続的にロックすることも、特定の期間ロックすることもできます。ロックされたアイデンティティによる認証の成功も、アイデンティティのロックが再び解除されるまで拒否されます。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Segmentation」の章にある「RADIUS Settings」[英語]に記載されている表を参照してください。



- (注) Cisco ISE リリース 3.3 パッチ 4 以降、[Identity Lock Settings] は、[RADIUS Settings] ページ ([Administration] > [System] > [Settings] > [Protocols] > [RADIUS]) で使用できません。

「今すぐ同期」を使用したオンデマンドの pxGrid 直接データ同期

[Sync Now] 機能を使用して、pxGrid Direct URL フェッチャコネクタのデータのオンデマンド同期を実行できます。完全同期と増分同期の両方をオンデマンドで実行できます。オンデマンドのデータ同期は、Cisco ISE GUI または OpenAPI を使用して実行できます。

詳細については、『Cisco ISE Administrator Guide, Release 3.3』の「Asset Visibility」の章にある「[On-demand pxGrid Direct Data Synchronization using Sync Now](#)」[英語] を参照してください。

Cisco ISE での TAC サポートケースのオープン

Cisco ISE リリース 3.3 パッチ 2 以降では、Cisco ISE GUI から直接 Cisco ISE の TAC サポートケースを開くことができます。

詳細については、『Cisco ISE Administrator Guide, Release 3.3』の「Troubleshoot」の章の「[Open TAC Support Cases](#)」[英語] を参照してください。

pxGrid を使用して登録できる新しいセッションディレクトリについて

Cisco ISE リリース 3.3 パッチ 2 以降では、pxGrid を使用して Session Directory All トピックに登録できます。sessionTopicAll は、既存の sessionTopic（引き続きサポート）に似ていますが、重要な違いが 1 つあります。sessionTopicAll は、IP アドレスのないセッションのイベントもパブリッシュします。詳細については、『[pxGrid API Guide](#)」[英語] を参照してください。

トランスポートゲートウェイのサポート終了

Cisco ISE ではトランスポートゲートウェイがサポートされなくなりました。次の Cisco ISE 機能では、接続方法としてトランスポートゲートウェイが使用されていました。

- Cisco ISE スマート ライセンス

スマートライセンス設定の接続方法としてトランスポートゲートウェイを使用している場合は、Cisco ISE リリース 3.3 パッチ 2 にアップグレードする前に設定を編集する必要があります。Cisco ISE リリース 3.3 パッチ 2 ではトランスポートゲートウェイがサポートされていないため、別の接続方法を選択する必要があります。接続方式を更新せずに Cisco ISE リリース 3.3 パッチ 2 にアップグレードすると、アップグレードプロセス中に HTTPS 直接接続方式を使用するようにスマートライセンス設定が自動的に更新されます。接続方法は、アップグレード後にいつでも変更できます。

- Cisco ISE テレメトリ

Cisco ISE テレメトリを使用する場合、トランスポートゲートウェイは接続方法として使用できなくなりました。テレメトリワークフローは、この変更の影響を受けません。

Cisco ISE ワークフローの TLS 1.3 サポート

Cisco ISE リリース 3.3 パッチ 2 以降のリリースでは、TLS 1.3 は次のワークフローでピアと通信できます。

- Cisco ISE は、EAP-TLS サーバーとして設定されます
- Cisco ISE は、TEAP サーバーとして設定されます



注目 Cisco ISE リリース 3.3 パッチ 2 リリースの時点では、TEAP TLS 1.3 は使用可能なクライアント OS でサポートされていないため、TEAP サーバーとして設定された Cisco ISE の TLS 1.3 サポートは、内部テスト条件下でテストされています。

- Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます



(注) Cisco ISE リリース 3.3 パッチ 2 については、[Manually Configure Ciphers List] オプションが TLS 1.3 でサポートされていません。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Segmentation」の章にある「[Configure Security Settings](#)」[英語]を参照してください。

Cisco ISE リリース 3.3 - 累積パッチ 1 の新機能

多要素認証のための Cisco Duo の統合

Cisco ISE リリース 3.3 パッチ 1 以降では、多要素認証（MFA）ワークフローの外部 ID ソースとして Cisco Duo を直接統合できます。Cisco ISE の以前のリリースでは、Cisco Duo は外部 RADIUS プロキシサーバーとしてサポートされていましたが、この設定は引き続きサポートされます。

この Cisco Duo 統合では、次の多要素認証のユースケースがサポートされています。

1. VPN ユーザー認証
2. TACACS+ 管理者アクセス認証

この機能の詳細については、『Cisco ISE Administration Guide, Release 3.3』の「Segmentation」の章にある「[Integrate Cisco Duo With Cisco ISE for Multifactor Authentication](#)」[英語]を参照してください。

カスタマー エクスペリエンス アンケート

Cisco ISE では、管理ポータル内でユーザーに顧客満足度アンケートが表示されるようになりました。顧客満足度アンケートを定期的実施することで、シスコではお客様の Cisco ISE のエクスペリエンスをより深く理解し、何が良好に機能しているかを追跡し、改善すべき領域を特定することができます。アンケートを送信すると、その後 90 日間は別のアンケートは表示されません。

アンケートは、すべての Cisco ISE の展開においてデフォルトで有効になっています。アンケートはユーザーレベルで、あるいは Cisco ISE の展開に対して無効にできます。

詳細については、『[Cisco ISE Administrator Guide, Release 3.3](#)』の「Basic Setup」の章にある「Customer Experience Surveys」[英語]を参照してください。

Microsoft Intune が MDM 統合における UDID ベースのクエリのサポートを終了

2024 年 3 月 24 日以降、Microsoft Intune では MDM 統合の UDID ベースのクエリのサポートを終了します。詳細はこの [Field Notice](#) をご確認ください。このサポート終了に対応して、Microsoft Intune MDM 統合から必要なエンドポイント情報を取得するための Cisco ISE API が変更されました。

Cisco ISE リリース 3.3 パッチ 1 以降、Microsoft Intune ではコンプライアンス API に対応して次のエンドポイントの詳細のみを提供します。

- デバイス コンプライアンス ステータス
- Intune による管理
- MAC アドレス
- 登録ステータス

変更の詳細については、『[Integrate MDM and UEM Servers with Cisco ISE](#)』を参照してください。

Cisco ISE リリース 3.3 の新機能

HTTPS と TLS 1.3 を使用した Cisco ISE 管理 GUI へのアクセス

Cisco ISE リリース 3.3 からは、TLS 1.3 バージョンで HTTPS を使用して Cisco ISE 管理 GUI にアクセスできます。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Secure Access」の章にある「[Configure Security Settings](#)」を参照してください。

pxGrid Cloud でのコンテキストイン API の一括更新と一括削除のサポート

Cisco ISE リリース 3.3 から、pxGrid Cloud でコンテキストイン API がサポートされ、エンドポイントの一括更新および一括削除が可能になります。詳細については、『[Cisco ISE API Reference Guide](#)』を参照してください。

API コールの証明書ベースの認証

Cisco ISE Release 3.3 から、[管理 (Admin)] > [システム (System)] > [管理アクセス (Admin Access)] > [認証 (Authentication)] > [認証方式 (Authentication Method)] ウィンドウで、API 管理や OpenAPI 管理などの API 管理ユーザーの認証を設定できます。[API 認証タイプ (API Authentication Type)] セクションでは、パスワードベースまたは証明書ベースの認証、あるいはその両方を許可できます。これらの認証設定は、pxGrid REST、MnTREST、およびその他の REST の管理ユーザーなどの REST 管理ユーザーには適用されません。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Basic Setup」の章にある「[Enable API Service](#)」を参照してください。

エンドポイントプロファイリングのための Cisco AI-ML ルール提案

Cisco ISE は、ネットワークからの継続的な学習に基づいてプロファイリングの提案を行い、エンドポイントプロファイリングと管理を強化するのに役立ちます。このような提案を使用し

て、ネットワーク内の不明なエンドポイントやプロファイリングされていないエンドポイントの数を減らすことができます。

詳細については、『Cisco Identity Services Engine Administration Guide, Release 3.3』の「Asset Visibility」の章にある「[Cisco AI-ML Rule Proposals for Endpoint Profiling](#)」[英語]を参照してください。

Cisco ISE でのネイティブ IPsec の設定

Cisco ISE リリース 3.3 からは、ネイティブ IPsec 設定を使用して IPsec を設定できます。IKEv1 および IKEv2 プロトコルを使用して、IPsec トンネルを介した Cisco ISE PSN と NAD 間のセキュリティアソシエーションを確立するためにネイティブ IPsec を使用できます。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Secure Access」の章にある「[Configure Native IPsec on Cisco ISE](#)」を参照してください。

Cisco ISE 展開内のすべてのノードに対するエンドポイント複製の無効化

Cisco ISE リリース 3.3 から、動的に検出されたエンドポイントは、Cisco ISE 展開内のすべてのノードに自動的に複製されません。Cisco ISE 展開内のすべてのノードで動的に検出されたエンドポイントの複製は、有効または無効にするかを選択できるようになっています。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Deployment」の章にある「[Data Replication from Primary to Secondary Cisco ISE Nodes](#)」[英語]を参照してください。

Data Connect

Cisco ISE リリース 3.3 から、Data Connect 機能は、管理者証明書を使用し、オープンデータベース コネクティビティ (ODBC) または Java Database Connectivity (JDBC) ドライバを使用して Cisco ISE へのデータベースアクセスを提供するため、データベースサーバーを直接照会して、選択したレポートを生成できます。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Basic Setup」の章にある「[Data Connect](#)」を参照してください。

ポスチャワークフローでの未検証のオペレーティング システム リリースのサポートの強化

Cisco ISE は、エージェントベースおよびエージェントレスのポスチャワークフローで、オペレーティングシステムの未検証バージョンをサポートするようになりました。Cisco ISE の以前のリリースでは、検証済みのオペレーティングシステムを実行するエンドポイントのみがポスチャ エージェント ポリシーを正常に満たしていました。

その結果、未検証のオペレーティングシステムを実行しているエンドポイントは、「**The operating system is not supported by the server**」というエラーメッセージが表示され、ポスチャ エージェント ワークフローに失敗します。

サポートされるオペレーティングシステムの詳細については、お使いの Cisco ISE リリースの「[Compatibility Matrix](#)」を参照してください。

たとえば、オペレーティング システム バージョン Windows 10 IoT Enterprise LTSC または Mac 14 を実行しているエンドポイントのポスチャエージェントフローは、これらのオペレーティングシステムのバージョンが検証されていない間は失敗しました。Cisco ISE がこれらのバージョ

ンを検証し、オペレーティングシステムのデータがフィードサービスにパブリッシュされると、ポストチャエージェントはこれらのエンドポイントを正常に照合しました。

Cisco ISE 管理ポータル の **[管理 (Administration)]** > **[システム (System)]** > **[ポストチャ (Posture)]** > **[更新 (Updates)]** ページ の **[フィードサービス (Feed Service)]** から Cisco ISE に最新のオペレーティングシステムのデータをダウンロードできます。

Cisco ISE リリース 3.3 から、未検証のオペレーティングシステムは、Cisco ISE 管理ポータル の **[ポリシー (Policy)]** ページ (**[ポストチャ (Posture)]**、**[要件 (Requirements)]**、**[条件 (Conditions)]** ページ) にリストされている既知のオペレーティングシステムと照合されるため、ポストチャエージェント ワークフローを正常に完了できます。たとえば、Mac xx が検証されず、エンドポイントがそれを実行している場合、ポストチャエージェントはエンドポイントを MacOSX と照合できるようになりました。Mac xx が検証され、フィードサービスに公開され、ポストチャエージェントがエンドポイントで再度実行されると、エンドポイントは Mac xx と照合されます。ポストチャレポートには、エンドポイントが一致するオペレーティングシステムが表示されます。

Cisco ISE リリース 3.3 でサポートされているすべてのポストチャエージェントが、この変更の影響を受けます。BYOD などの他の Cisco ISE 機能は影響を受けません。

LDAP プロファイル バインド アカウント パスワード への ERS API サポート

Cisco ISE リリース 3.3 から、LDAP プロファイル バインド アカウント パスワード は ERS API でサポートされます。ERS API を使用して、Cisco ISE GUI で新しい LDAP サーバーを設定できます。作成された LDAP サーバーは、他の Cisco ISE ポータルでアイデンティティ送信元を設定するために使用できます。詳細については、『[Cisco ISE API Reference Guide](#)』を参照してください。

エージェントレス ポスチャ への IPv6 サポート

Cisco ISE リリース 3.3 では、エージェントレス ポスチャ への IPv6 サポートが追加されています。現在、Windows および MacOS クライアントがサポートされています。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Compliance」の章にある「[Agentless Posture](#)」[英語]を参照してください。

ポータル および プロファイラ 機能 への IPv6 サポート

Cisco ISE リリース 3.3 では、次のポータル、ポータル機能、およびプロファイラ機能に対する IPv6 サポートが追加されています。

IPv6 をサポートする Cisco ISE ポータル

- スポンサー ポータル
- MyDevices ポータル
- 証明書プロビジョニング ポータル
- ホットスポット ゲスト ポータル
- アカウント登録ゲスト ポータル

IPv6 をサポートする Cisco ISE ポータル機能

- シングルクリックスポンサー承認
- 猶予期間
- ゲストポータルのログイン情報の検証
- Active Directory
- 一時エージェントを使用したゲスト ポータル ポスチャ フロー
- Active Directory ユーザー：AnyConnect を使用したポスチャフロー
- Dot1x ユーザー：AnyConnect を使用したポスチャフロー
- ゲストおよび Dot1x ユーザー：一時エージェントを使用したポスチャフロー

IPv6 をサポートするプロファイラ機能

- DHCP プローブ
- HTTP プローブ
- RADIUS プローブ
- コンテキストの可視性（Context Visibility）サービス
- エンドポイント プロファイリング



(注) Web リダイレクションの共通タスクの静的 IP/ホスト名/FQDN フィールドに IPv6 アドレスを指定することはできません。

外部 LDAP ユーザーを Cisco ISE エンドポイントグループにリンクする

Cisco ISE リリース 3.3 から、[ダイナミック（Dynamic）] オプションを使用して、外部 LDAP ユーザーグループをゲストデバイスのエンドポイント アイデンティティ グループに割り当てることができます。詳細については、『*Cisco Identity Services Engine Administrator Guide, Release 3.3*』の「Guest and Secure WiFi」の章にある「[Create or Edit Guest Types](#)」を参照してください。

Cisco ISE ユーザーのパスワードの管理

Cisco ISE リリース 3.3 から、Cisco ISE の内部ユーザーとして、[Network Access Users] ウィンドウの [Network Access User] テーブルに [Date Created] 列と [Date Modified] 列を追加するか選択できます。詳細については、『*Cisco Identity Services Engine Administrator Guide, Release 3.3*』の「Asset Visibility」の章にある「[Cisco ISE Users](#)」[英語]を参照してください。

多要素分類による拡張エンドポイントの可視化

ネットワークに接続しているエンドポイントからの4つの特定の属性を使用して、微妙な差異のある許可ポリシーを作成できるようになりました。多要素分類（MFC）プロファイラは、さ

まざまなプロファイリングプローブを使用して、Cisco ISE 認証ポリシー作成ワークフローに 4つの新しいエンドポイント属性（MFCエンドポイントタイプ、MFCハードウェアメーカー、MFC ハードウェアモデル、MFC オペレーティングシステム）を取り込みます。

詳細については、『Cisco Identity Services Engine Administration Guide, Release 3.3』の「Asset Visibility」の章にある「[Multi-Factor Classification for Enhanced Endpoint Visibility](#)」[英語]を参照してください。

ナビゲーションの改善

Cisco ISE ホームページ GUI は、ユーザー体験を向上させるために変更されました。ホームページの左隅にあるメニューアイコンをクリックすると、ペインが表示されます。ペインの各オプションにカーソルを合わせると、次のような選択可能なサブメニューが表示されます。

- コンテキストの可視性（Context Visibility）
- 動作（Operations）
- ポリシー（Policy）
- 管理（Administration）
- ワークセンター（Work Centers）

ホームページで [ダッシュボード（Dashboard）] をクリックします。

左ペインには、最近表示したページを保存できる [ブックマーク（Bookmarks）] タブもあります。メニューアイコンを再度クリックすると、ペインが非表示になります。

左ペインが表示されているときにログアウトし、再度ログインすると、ペインは引き続き表示されます。ただし、ペインが非表示になった後にログアウトし、再度ログインした場合、ペインを再度表示するには、メニューアイコンをクリックする必要があります。

ホームページの  アイコンを使用して [ページの検索（Search Pages）] オプションにアクセスし、新しいページを検索したり、最近検索したページにアクセスしたりできるようになりました。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Basic Setup」の章にある「[Administration Portal](#)」[英語]を参照してください。

特定の暗号方式を無効にするオプション

[セキュリティ設定（Security Settings）] ウィンドウの [暗号リストの手動設定（Manually Configure Ciphers List）] オプションを使用すると、Cisco ISE コンポーネント（管理 UI、ERS、OpenAPI、セキュア ODBC、ポータル、および pxGrid）との通信用暗号方式を手動で設定できます。

許可された暗号方式がすでに選択された状態で暗号方式リストが表示されます。たとえば、[SHA1暗号方式を許可（Allow SHA1 Ciphers）] オプションが有効になっている場合、このリストの SHA1 暗号方式が有効になります。[Allow Only TLS_RSA_WITH_AES_128_CBC_SHA] オプションが選択されている場合、この SHA1 暗号方式のみがこのリストで有効になります。[SHA1暗号方式を許可（Allow SHA1 Ciphers）] オプションが無効になっている場合、このリストの SHA1 暗号方式はどれも有効にできません。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Segmentation」の章にある「[Configure Security Settings](#)」[英語]を参照してください。

ARM64 バージョンのエージェントへのポスチャおよびクライアント プロビジョニングのサポート

Cisco ISE リリース 3.3 から、ポスチャポリシーとクライアント プロビジョニング ポリシーは ARM64 エンドポイントでサポートされます。ARM64 エンドポイント用の ARM64 バージョンのエージェントをアップロードできます。

ARM64 クライアント プロビジョニング ポリシーを設定する際は、次の点に注意してください。

- ARM64 ポスチャポリシーは、次でサポートされています。
 - Windows エージェント
 - Mac エージェント
 - Mac テンポラルエージェント
 - Mac エージェントレス

Windows ポリシーは、ARM64 アーキテクチャとインテルアーキテクチャで別のパッケージを実行します。Windows テンポラルと Windows エージェントレスは、ARM64 アーキテクチャではサポートされていませんが、インテルアーキテクチャではサポートされています。

macOS ポリシーは、両方のアーキテクチャで同じパッケージを実行します。

- ARM64 パッケージは、Cisco AnyConnect VPN および Cisco Secure Client でサポートされています。



(注) Cisco Secure Client 5.0.4xxx 以降のバージョンは、ARM64 エンドポイントのポスチャおよびクライアント プロビジョニング ポリシーをサポートしています。

ARM64 準拠モジュール 4.3.3583.8192 以降のバージョンは、Cisco Secure Client 5.0.4xxx 以降のバージョンと、ARM64 エンドポイント用の Cisco ISE 3.3 以降のバージョンで使用できます。コンプライアンスモジュールは、[ソフトウェア ダウンロード センター](#)からダウンロードできます。

- ARM64 エージェントの自動アップグレードとコンプライアンスモジュールのアップグレードがサポートされています。
- Google Chrome および Microsoft Edge 89 以降のバージョンでは、ARM64、64 ビット、32 ビットなどの OS アーキテクチャ条件の Web リダイレクトがサポートされています。

Firefox ブラウザは、ARM64、64 ビット、32 ビットなどの OS アーキテクチャ条件の Web リダイレクトをサポートしていません。したがって、ARM64 クライアント プロビジョニ

ング ポリシーの照合には使用できません。Firefox ブラウザを使用すると、次のメッセージが表示されます。

ARM64 endpoints do not support Firefox browser, and there may be compatibility issues if you continue downloading this agent. We recommend that you use Chrome or Microsoft Edge browser instead.

- BYOD と ARM64 クライアント プロビジョニング ポリシーを組み合わせることはできません。
- ARM64 条件ポリシーが条件リストの一番上にあることを確認します（ARM64 条件のないポリシーの上に表示されます）。これは、エンドポイントが [クライアントプロビジョニングポリシー（Client Provisioning Policy）] ウィンドウに一覧表示されているポリシーと順を追って照合されるためです。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.3』の「Compliance」の章にある「[Configure Client Provisioning Policy for ARM64 Version of Agent](#)」を参照してください。

pxGrid コンテキストインの機能拡張

Cisco ISE リリース 3.3 から、pxGrid でコンテキストイン API がサポートされます。エンドポイントのカスタム属性を作成し、コンテキストインサポートに OpenAPI を使用できます。詳細については、『[Cisco ISE API Reference Guide](#)』を参照してください。

コンテキストインの pxGrid Cloud サポート

Cisco ISE リリース 3.3 から、pxGrid Cloud でコンテキストイン API がサポートされます。エンドポイントのカスタム属性を作成し、コンテキストインサポートに OpenAPI を使用できます。詳細については、『[Cisco ISE API Reference Guide](#)』を参照してください。

pxGrid Direct の機能拡張

pxGrid Direct は、制御された導入機能ではなくなりました。Cisco ISE リリース 3.2 または 3.2 パッチ 1 から Cisco ISE リリース 3.3 にアップグレードする前に、設定済みのすべての pxGrid Direct コネクタと、pxGrid Direct コネクタからのデータを使用する認証プロファイルおよび認証ポリシーを削除することを推奨します。Cisco ISE リリース 3.3 にアップグレードした後、pxGrid Direct コネクタを再設定してください。



- (注) 設定済みの pxGrid Direct コネクタを削除しない場合、コネクタはアップグレード中に自動的に削除されます。この削除により、編集も使用も不可能な認証プロファイルと認証ポリシーが作成されます。これらを削除して新しいものに置き換える必要があります。

pxGrid Direct 機能の変更の詳細については、『Cisco Identity Services Engine Administration Guide, Release 3.3』の「Asset Visibility」の章にある「[pxGrid Direct](#)」[英語]を参照してください。

RADIUS ステップ遅延ダッシュボード

[RADIUS ステップ遅延 (RADIUS Step Latency)] ダッシュボード ([ログ分析 (Log Analytics)] > [ダッシュボード (Dashboard)]) には、指定された期間の RADIUS 認証フローステップの最大遅延と平均遅延が表示されます。また、Active Directory 認証フローステップ (Active Directory がそのノードで設定されている場合) の最大遅延および平均遅延、および最大遅延または平均遅延のうち上位 N 個の RADIUS 認証手順を表示することもできます。

詳細については、『Cisco Identity Services Engine Administration Guide, Release 3.3』の「Maintain and Monitor」の章にある「[Log Analytics](#)」[英語]を参照してください。

管理証明書更新後のアプリケーション再起動のスケジュール設定

プライマリ PAN で管理証明書を更新した後、展開内のすべてのノードを再起動する必要があります。各ノードをすぐに再起動することも、後での再起動をスケジュールすることもできます。この機能を使用すると、実行中のプロセスが自動再起動によって中断されないようにすることができ、プロセスをより詳細に制御できます。証明書の更新から 15 日以内にノードの再起動をスケジュールする必要があります。

詳細については、『Cisco Identity Services Engine Administration Guide, Release 3.3』の「Basic Setup」の章にある「[Schedule Application Restart After Admin Certificate Renewal](#)」[英語]を参照してください。

GUI からの Cisco ISE 展開の分割アップグレード

分割アップグレードは、ユーザーがサービスを引き続き利用できるようにしながら、Cisco ISE 展開のアップグレードを可能にするマルチステッププロセスです。分割アップグレードでは、ノードを反復またはバッチでアップグレードすることでダウンタイムを制限できます。

詳細については、『Cisco Identity Services Engine Upgrade Guide, Release 3.3』の「Perform the Upgrade」の章にある「[Split Upgrade of Cisco ISE Deployment from GUI](#)」[英語]を参照してください。

ポータルでのウクライナ語のサポート

ゲスト、スポンサー、デバイス、およびクライアント プロビジョニング ポータルに、サポートされるローカリゼーション言語としてウクライナ語が含まれるようになりました。

Cisco Catalyst 9800 ワイヤレス LAN コントローラからの Wi-Fi デバイス分析データ

Cisco ISE に統合されたシスコ ワイヤレス LAN コントローラからのデバイス分析データを使用して、Apple、Intel、および Samsung エンドポイントのプロファイリングポリシー、許可条件、および認証条件とポリシーを作成できます。

詳細については、『Cisco Identity Services Engine Administration Guide, Release 3.3』の「Asset Visibility」の章にある「[Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller](#)」[英語]を参照してください。

廃止された機能

認証失敗が繰り返される場合のアイデンティティのロック

Cisco ISE リリース 3.3 パッチ 4 以降、[Identity Lock Settings] は、[RADIUS Settings] ページ ([Administration] > [System] > [Settings] > [Protocols] > [RADIUS]) で使用できません。

Cisco ISE の新規および変更された API

新規、変更、および廃止された API の詳細については、Cisco DevNet の『[Cisco ISE API 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 プラットフォームと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 3.3 は、次の Secure Network Server (SNS) ハードウェア プラットフォームにインストールできます。

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-3615-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 Appliance Hardware Installation Guide 』を参照してください。
Cisco SNS-3655-K9 (中規模)	
Cisco SNS-3695-K9 (大規模)	
Cisco SNS-3715-K9 (小規模)	
Cisco SNS-3755-K9 (中規模)	
Cisco SNS-3795-K9 (大規模)	



(注) OVA テンプレートのファイル名は、Cisco ISE リリース 3.3 で変更されていることに注意してください。

SNS 3600 シリーズ アプライアンスには、次の OVA テンプレートを使用できます。

OVA テンプレート	ISE ノードサイズ
Cisco-vISE-300-3.3.0.430.ova	評価
	極小規模
	小規模
	中規模
Cisco-vISE-600-3.3.0.430.ova	小規模
	中規模
Cisco-vISE-1200-3.3.0.430.ova	中規模
	大規模
Cisco-vISE-1800-3.3.0.430.ova	大規模
Cisco-vISE-2400-3.3.0.430.ova	大規模

次の OVA テンプレートは、SNS 3600 および SNS 3700 シリーズ アプライアンスの両方に使用できます。

OVA テンプレート	ISE ノードサイズ	
Cisco-vISE-300-3.3.0.430a.ova	評価	300-Eval
	極小規模	300-ExtraSmall
	小規模	300-Small_36xx
		300-Small_37xx
	中規模	300-Medium_36xx
		300-Medium_37xx
Cisco-vISE-600-3.3.0.430a.ova	小規模	600-Small_36xx
		600-Small_37xx
	中規模	600-Medium_36xx
		600-Medium_37xx

OVA テンプレート	ISE ノードサイズ	
Cisco-vISE-1200-3.3.0.430a.ova	中規模	1200-Medium_36xx
		1200-Medium_37xx
	大規模	1200-Large_36xx
		1200-Large_37xx
Cisco-vISE-2400-3.3.0.430a.ova	大規模	2400-Large_36xx
		2400-Large_37xx

Cisco SNS 3595 は、Cisco ISE 3.3 以降のリリースではサポートされていません。詳細については、[サポート終了と販売終了のお知らせ](#)を参照してください。

Cisco SNS 3595 アプライアンスを使用して Cisco ISE 3.3 以降のリリースをインストールまたはアップグレードすることはできません。Cisco SNS 3595 プロファイルが設定された仮想アプライアンスは、Cisco SNS 3655 プロファイルに移行する必要があります。プロファイルを移行するには、ノードのバックアップを取得し、Cisco SNS 3655 プロファイルを使用して Cisco ISE 3.3 をインストールしてから、このノードで Cisco SNS 3595 プロファイルのバックアップを復元する必要があります。



(注) Cisco SNS 3595 プロファイルを使用して Cisco ISE 3.2 以前のリリースから Cisco ISE 3.3 にアップグレードする場合、ノードは Cisco ISE 3.3 で Cisco SNS 3615 としてプロファイリングされます。このため、ノードのパフォーマンスが低下します。

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。

- Cisco ISE リリース 3.3 は、VMware ESXi 6.7 をサポートする最後のリリースです。

Cisco ISE リリース 3.0 以降のリリースでは、VMware ESXi 7.0.3 以降のリリースに更新することを推奨します。

vTPM デバイスの場合は、VMware ESXi 7.0.3 以降のリリースにアップグレードする必要があります。

- OVA テンプレート : ESXi 6.7、ESXi 7.0、および ESXi 8.0 では VMware バージョン 14 以降。
- ISO ファイルは ESXi 6.7、ESXi 7.0、および ESXi 8.0 をサポートしています。

次のパブリック クラウド プラットフォーム上の VMware クラウドソリューションに Cisco ISE を展開できます。

- Amazon Web サービス (AWS) の VMware クラウド : Cisco ISE を AWS の VMware クラウドが提供するソフトウェアデファインドデータセンターでホストします。
- Azure VMware ソリューション : Azure VMware ソリューションは、Microsoft Azure 上でネイティブに VMware ワークロードを実行します。Cisco ISE を VMware 仮想マシンとしてホストできます。
- Google Cloud VMware Engine : Google Cloud VMware Engine は、Google Cloud 上の VMware によってソフトウェアデファインドデータセンターを実行します。VMware Engine によって提供されるソフトウェアデファインドデータセンターで、VMware 仮想マシンとして Cisco ISE をホストできます。



- (注) Cisco ISE 3.1 以降では、仮想マシン (VM) インスタンス (任意のペルソナを実行) のホスト間での移行に VMware マイグレーション機能を使用できます。Cisco ISE はホットマイグレーションとコールドマイグレーションの両方をサポートします。ホットマイグレーションは、ライブマイグレーションまたは vMotion と呼ばれます。ホットマイグレーション中に Cisco ISE をシャットダウンしたり、電源をオフにしたりする必要はありません。可用性を損なうことなく、Cisco ISE VM を移行できます。

- Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V

Cisco ISE は、Azure Stack HCI 23H2 以降のバージョンをサポートしています。Azure Stack HCI 内の Cisco ISE VM の仮想マシン要件とインストール手順は、Microsoft Hyper-V の場合と同じです。

- QEMU 2.12.0-99 以降の KVM



- (注) Cisco ISE は OpenStack にインストールできません。

- Nutanix AHV 20220304.392

次のパブリック クラウドプラットフォーム上に Cisco ISE をネイティブに展開できます。

- Amazon Web Services (AWS)
- Microsoft Azure クラウド
- Oracle Cloud Infrastructure (OCI)

仮想マシンの要件に関する情報については、お使いの Cisco ISE バージョンの『[Cisco Identity Services Engine インストールガイド](#)』を参照してください。

検証済みブラウザ

Cisco ISE 3.3 は、次のブラウザでサポートされています。

- Mozilla Firefox バージョン 113、114、119、123、125、および 127 以降
- Google Chrome バージョン 112、114、116、117、119、122、124、および 126 以降
- Microsoft Edge バージョン 112、115、117、119、122、125、および 126 以降



(注) 現在、モバイルデバイスで Cisco ISE GUI にアクセスすることはできません。

検証済み外部 ID ソース



(注) サポートされている Active Directory バージョンは、Cisco ISE と Cisco ISE-PIC の両方で同じです。

Cisco ISE は Microsoft Entra ID をサポートしています。

表 2: 検証済み外部 ID ソース

外部 ID ソース	バージョン
Active Directory	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 1	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019	Windows Server 2019
Microsoft Windows Active Directory 2022	Windows Server 2022 (パッチ Windows10.0-KB5025230-x64-V1.006.msu 適用済み)
Microsoft Windows Active Directory 2025	Windows Server 2025
LDAP サーバー	
SunONE LDAP ディレクトリサーバー	バージョン 5.2
OpenLDAP ディレクトリサーバー	バージョン 2.4.23
任意の LDAP v3 準拠サーバー	LDAP v3 準拠のすべてのバージョン

外部 ID ソース	バージョン
LDAP としての AD	Windows Server 2022 (パッチ Windows10.0-KB5025230-x64-V1.006.msu 適用済み)
トークンサーバー	
RSA ACE/サーバー	6.x シリーズ
RSA 認証マネージャ	7.x および 8.x シリーズ
Any RADIUS RFC 2865 準拠のトークン サーバー	RFC 2865 準拠のすべてのバージョン
セキュリティ アサーション マークアップ言語 (SAML) シングルサインオン (SSO)	
Microsoft Azure MFA	最新
Oracle Access Manager (OAM)	バージョン 11.1.2.2.0
Oracle Identity Federation (OIF)	バージョン 11.1.1.2.0
PingFederate サーバー	バージョン 6.10.0.4
PingOne クラウド	最新
セキュア認証	8.1.1
SAMLv2 準拠の ID プロバイダー	SAMLv2 準拠の任意の ID プロバイダバージョン
Open Database Connectivity (ODBC) アイデンティティソース	
Microsoft SQL Server	Microsoft SQL Server 2012 Microsoft SQL Server 2022
Oracle	Enterprise Edition リリース 12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3
ソーシャルログイン (ゲストユーザーアカウントの場合)	
Facebook	最新

¹ Cisco ISE は、Microsoft Windows Active Directory 2012 R2 のすべてのレガシー機能をサポートしていますが、保護ユーザーグループなどの Microsoft Windows Active directory 2012 R2 の新機能はサポートされていません。

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

Cisco 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 AnyConnect ISE ポスチャのサポート表](#)を参照してください。

検証済み OpenSSL のバージョン

Cisco ISE 3.3 は、OpenSSL 1.1.1x および CiscoSSL 7.3.375 with FOM 7.3a で検証済みです。

OpenSSL の更新には CA 証明書で CA:True であることが必要

証明書を CA 証明書として定義するには、証明書に次のプロパティが含まれている必要があります。

`basicConstraints=CA:TRUE`

このプロパティは、最近の OpenSSL 更新に準拠するために必須です。

既知の制限事項と回避策

このセクションでは、さまざまな既知の制限と対応する回避策に関する情報を提供します。

pxGrid Direct コネクタが無効になっている場合の Cisco ISE の再起動の制限

無効な pxGrid Direct コネクタがある状態で Cisco ISE を再起動すると、再起動後に pxGrid Direct コネクタを使用する同期操作をスケジュールする際に問題が発生します。Cisco ISE を再起動する前に、無効になっているすべての pxGrid Direct コネクタを有効にし、再起動してからコネクタを再度無効にすることをお勧めします。または、この問題の回避策として、Cisco ISE を再起動する前に、無効になっているコネクタの属性を編集する（アクティブなコネクタにする）こともできます。

この問題は、Cisco ISE リリース 3.2 累積パッチ 5 および Cisco ISE リリース 3.3 累積パッチ 2 で解決されています。

Cisco ISE リリース 3.3 - 累積パッチ 4 の既知の制限事項

osquery 可視性条件における特殊文字の使用方法

等号演算子を属性値の特殊文字とともに使用すると（たとえば、CPU@1.20GH）、osquery 可視性条件でエラーが発生します。回避策として、Like 演算子（is_containing）を使用して、特殊文字付きの osquery 可視性条件を設定できます。

ポスチャ修復スクリプトを要件に追加する

クライアントポスチャ要件にスクリプト条件を追加するには、[Client Posture Requirements] ページ ([Policy] > [Policy Elements] > [Results] > [Posture] > [Requirements]) から新しいスクリプト条件を作成し、[Save and Select] オプションを使用して、新しく作成したスクリプト条件を要件に追加する必要があります。

アップグレード情報



- (注) ネイティブクラウド環境では、アップグレードに Cisco ISE のバックアップおよび復元メソッドを使用する必要があります。ネイティブクラウド環境に展開された Cisco ISE ノードではアップグレードを実行できません。新しいバージョンの Cisco ISE を使用して新しいノードを展開し、古い Cisco ISE 展開の設定をそのノードに復元する必要があります。

リリース 3.3 へのアップグレード

次の Cisco ISE リリースからリリース 3.3 に直接アップグレードできます。

- 3.0
- 3.1
- 3.2

Cisco ISE リリース 3.0 より前のバージョンの場合は、まず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 3.3 にアップグレードする必要があります。

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。

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。

で Cisco ISE リリース 3.3 のアップグレードバンドル ファイルが置き換えられました。[Cisco ISE Software Download](#) サイト。

これには以下が含まれます。

- バグ [CSCwj43362](#) および [CSCwj55392](#) の解決。
- 新しいファイルのファイル名には、「b」がビルド番号に追加されます（たとえば、`ise-upgradebundle-3.0.x-3.2.x-to-3.3.0.430b.SPA.x86_64.tar.gz`）。
- 既存の Cisco ISE リリース 3.3 累積パッチは、この新しいアップグレードバンドルで引き続き機能します。

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 Cisco 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、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 により実際のアップグレード前にデータを検証し、問題があれば報告します。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 の Cisco Catalyst Center との統合

Cisco ISE は Cisco Catalyst Center との統合が可能です。Catalyst Center と連携するように Cisco ISE を設定する方法については、[Cisco Catalyst Center のドキュメント](#)を参照してください。

Cisco ISE と Catalyst Center との互換性については、「[Cisco SD-Access Compatibility Matrix](#)」[英語]を参照してください。

新しいパッチのインストール

システムへのパッチの適用方法については、『[Cisco Identity Services Engine Upgrade Journey](#)』の「Cisco ISE Software Patches」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方法については、『[Cisco Identity Services Engine CLI Reference Guide](#)』の「Patch Install」セクション [英語] を参照してください。



- (注) 以前の Cisco ISE リリースにホットパッチをインストールしている場合は、パッチをインストールする前にホットパッチをロールバックする必要があります。そうしないと、整合性チェックのセキュリティの問題により、サービスが開始されない可能性があります。

不具合

「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。



- (注) 「未解決の不具合」セクションには、現在のリリースに該当し、Cisco ISE 3.3 よりも前のリリースにも該当す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。

解決済みの不具合

Cisco ISE リリース 3.3 - 累積パッチ 4 の解決済みの不具合

ID	見出し
CSCWj57697	Cisco ISE でライブログまたはライブセッションの詳細を開いているときにデータが一致しない。
CSCWh01906	削除された MDM サーバーが引き続き MDMServerName 属性の許容値リストに表示される。
CSCWm13930	エージェントレス ポスチャ エンドポイント ログが zip ファイルではなく HTM としてエクスポートされる。
CSCWk45395	以前の必須ポリシーでエラーが発生すると、監査ポリシーエラーが発生して、スキップされた条件が表示される。
CSCWk07593	Get-All ゲストユーザー API がすべてのアカウント、特に他のスポンサーユーザーによって作成されたアカウントを取得しない。
CSCWj82278	古いロックファイルが API ゲートウェイとコンテキストの可視性をブロックする。
CSCWk76790	ネットワーク アクセス ユーザーの説明を編集または追加しようとする、説明フィールドが閉じる。
CSCWj76445	Cisco ISE ERS ゲストのドキュメントを更新して、Get コールからポータル ID を除外する必要がある。
CSCWk71111	バックアップの復元が 75% でスタックする。
CSCWj54376	設定バリデータの評価で、すべての NAD インターフェイスが解析されない。
CSCWk25206	消去するデータがない場合は、空の GPG ファイルがエクスポートされる。
CSCWj68795	レプリケーションエラー「オブジェクト同期エラー：EDF2EndPoint：操作：更新」。
CSCWm10693	Cisco ISE 内部ユーザーアカウントの無効化ポリシー機能は、非アクティブ状態が 1 日続くと機能しない。
CSCWk13234	古い Cisco ISE ノードが、復元後に TCP ダンプとデバッグプロファイル設定に表示される。
CSCWh54899	Cisco ISE GUI にログインできない。ログイン情報を入力した後、ログイン情報画面のチェック中にハングする。
CSCWj83460	CV と Oracle データベース間のアイデンティティグループ数の不一致。
CSCWf69715	パッチをインストールすると、TC-NAC アダプタに到達できなくなり、新しいアダプタを設定できない。
CSCWi58421	ポスチャリースが有効になっている場合、PSN ノードは正しいポスチャ有効期限でデータベースを更新しない。

ID	見出し
CSCwj58727	Cisco ISE では、プロトコルをチェックせずに許可されたプロトコルの保存は許可されない。
CSCwh49351	SAML 要求 PSN の除外。
CSCwj44649	TACACS データが保持されず、すべてが消去される。
CSCwj82240	セカンダリノードの Cisco ISE カウンタレポートが空になる。
CSCwfl1926	CLI ではリポジトリパスワードに %、<、>、? の文字を使用できるが、GUI では使用できない。
CSCwk74103	Cisco ISE EAP-FAST PAC なしセッションのタイムアウトが発生し、値が保存されない。
CSCwj09219	OpenSSL ライブラリを OpenSSL 1.1.1x (CiscoSSL 7.3.375 with FOM 7.3a) に更新。
CSCwk07454	PSN が正しいポスチャリースの有効期限でデータベースを更新しない。
CSCwk46855	ユーザー保留中のアカウントが [Sponsor Manage Account] ページに表示されない。
CSCwk30610	コンソール経由で NAD にアクセスしているときに、TACACS+ エンドステーション ネットワーク条件のステップの遅延が大きくなる。
CSCwk04493	Cisco ISE 3.1 パッチ 6 以降では、ポリシーの詳細を取得するために使用されるメソッドが内部メソッドを呼び出し、キャッシュされない。
CSCwk15719	Cisco ISE プロファイラは、SNMP プロブ応答を介して受信した LLDP ポート ID サブタイプ 7 から MAC を読み取ることができない。
CSCwi20027	TrustSec の展開要求に失敗し、NAD の取得中に CoA 要求がスタックする。
CSCwj94294	Cisco ISE REST API のブラインド SQL インジェクションの脆弱性。
CSCwj94297	Cisco ISE REST API のブラインド SQL インジェクションの脆弱性。
CSCvy30859	ACI からインポートされた EPG の静的 IP-SGT マッピングを Cisco ISE リリース 2.6 で作成できない。
CSCwj94305	Cisco ISE REST API のブラインド SQL インジェクションの脆弱性。
CSCwk38279	ea.log ファイルをサポートバンドルに含める必要がある。
CSCwk87768	デフォルトのデバイスが使用されている場合、プロファイル名を使用した認証に失敗する。
CSCwj84815	ポリシーセットでゲストタイプの名前を変更しようとする、「使用可能なセッションがありません」というエラーが表示される。
CSCwk67197	proxy-state 属性が欠落している場合、Cisco ISE が外部 RADUIS サーバーに接続しない。

ID	見出し
CSCwj97724	Cisco ISE では、ポリシーセットで許可されていない条件での既存のライブラリ条件の更新を許可しない必要がある。
CSCwk31930	AD フォレストがオフラインとマーク付けされているため、Cisco ISE が子ドメインコントローラに対する認証をスキップする。
CSCwk06043	MAB ポリシーにより割り当てられた SGT とのバインディングが、SGT バインディングテーブルに表示されない。
CSCwm00197	レプリケーション クライアントの再起動中に数値オーバーフロー例外が発生した。
CSCwk88239	MDM の重要な属性が原因で、認証フロー中にデータベース永続イベントが発生する。
CSCwk35573	ZAP の実行中に脆弱な JS ライブラリの問題が Cisco ISE リリース 3.3 で見つかった。
CSCwj97491	Cisco ISE のコマンドインジェクションの脆弱性。
CSCwk93711	Cybervision が Cisco ISE 統合後に DDOS getAssets コールを受信する。
CSCwj67089	ローカルディスク管理を介してセカンダリノードに大きなファイルをインポートすると、Cisco ISE アプリケーションサーバーがクラッシュする。
CSCwk07483	プロファイラ ネットワーク デバイス イベント ハンドラが入力文字列 0 ～ 255 のデバイスの追加に失敗する。
CSCwj23933	AD コネクタが参加ステータスになっていない。
CSCwk55333	デバックモードでは ise.psc.log に着信 API 要求の URI が出力されない。
CSCwi86762	ポスチャと MDM フローが一緒に設定されている場合に、正しい CoA が VPN フローでトリガーされるべきである。
CSCwk36095	pxGrid ライブログの有用性。
CSCwj85626	API コールを介してエンドポイントの IP アドレスを取得できない。
CSCwf79582	AD クレデンシャルで Cisco ISE と Cisco Catalyst Center 2.2.1.x 以降を統合できない。
CSCwk13244	ise.messaging.log がダウンロード対象として GUI に表示されない。
CSCwj95818	最大同時 CLI セッション数が機能しない。
CSCwk32078	エンドポイントチェックの結果が、passiveID ログインイベントの後に到達不能のままになる。
CSCwj35581	Cisco ISE にレート制限保護がない。
CSCwh39213	Cisco ISE AWS EC2 インスタンスの SSH キーを置き換えることができない。
CSCwk25839	syslog サーバーの外部アクティブディレクトリログでカウント数が上昇する。

ID	見出し
CSCwk64227	認証ポリシーの ODBC クエリが postgres で結果を返さない。
CSCwk40725	ConfD が localhost:9888.access.1.1.1.1... などエンドレスに生成する。
CSCwk79546	Cisco ISE リリース 3.3 パッチ 3 でライブログに「22076 MFA 認証失敗」というメッセージが表示されて、Duo MFA 認証が即座に失敗する。
CSCwk59176	Cisco Prime Infrastructure の起動パッドで [Cisco ISE report] をクリックしても、グラフが表示されない。
CSCwj80616	Cisco ISE コンテキストの可視性のエンドポイント詳細が、MDM フロー内の RADIUS ライブログまたはセッションと一致しない。
CSCwj48625	EAP-TLS フローでエンドポイントログイン用に複数のドメインが設定されている場合に、エージェントレスポスチャに失敗する。
CSCwj35698	Cisco ISE ビジネスロジックの問題：ユーザーディクショナリ。
CSCwk04644	Cisco ISE リリース 3.2 以降では、システム 360 モニタリングのデバッグログローテーションが機能しない。
CSCwk14636	Cisco ISE 3.2 パッチ 6 では、AWS 上で仮想マシンリソース不足アラームがトリガーされる。
CSCwk40233	ポスチャ状態の同期機能の使用例と検証手順を文書化する必要がある。
CSCwk21895	Cisco ISE では、CLI のパスワードの最大文字数が 127 と表示される。
CSCwk32677	サポートバンドルの作成時に ise-duo.log ログが収集されない。
CSCwk09094	パスワードの有効期間が 365 日より長く設定されている場合、誤解を招くポップアップが表示される。
CSCwk38828	API NBAR アプリケーション管理設定で PUT オプションを使用すると、Swagger ツールのエラーが表示される。
CSCwk06817	既知の OS バグが原因で、Cisco ISE ノードでスワップが増加する。
CSCwj29473	Cisco ISE のフォーミュラ インジェクション
CSCwk91976	GUI がパスワードの変更時に古いパスワードの確認を求めない。
CSCwk32104	agentprobeoom.sh および restprobeoom の OOM ヒープファイルを削除する必要がある。
CSCwk38327	MDM フローの正常性チェックでエラーが発生する。
CSCwj66951	ネットワークアクセスユーザーを作成する際、「OR」の組み合わせを含む姓または名を持つユーザーを作成できない。
CSCwc64144	合計認証遅延とクライアント遅延が TACACS+ で機能しない。

ID	見出し
CSCwk20019	SMS HTTP URL の属性名が原因で、編集時に URL の更新に関する問題が発生する。
CSCwk35172	「DumpClearOnExceed」ファイルで Cisco ISE PSN ノードのディスクがいっぱいになっている。
CSCwj35576	Cisco ISE サーバー側の検証が実行されていない。
CSCwk07789	nslookup 要求で最初の文字に「_」を使用すると、無効な IP またはホスト名エラーが発生する。
CSCwi72309	Cisco ISE がプロファイリンググループでスタックし、レプリケーションの遅延エラーが発生する。
CSCwm29900	インポートされたエンドポイントに誤ったエンドポイントID が表示され、データの不一致が発生する。
CSCwj77501	インバウンド属性が 2 つ以上選択されている場合、ODBC 拡張属性が機能しない。
CSCwe54931	プライマリ Cisco ISE 以外の複数の DNS ドメイン名を持つ Cisco ISE ノードがシステム 360 で表示されない。
CSCwk75775	正常性チェックが入力または出力帯域幅のパフォーマンスチェックに失敗し、Null の結果を返す。
CSCwj82298	割り当てられた論理的なプロファイルが、コンテキスト可視性エンドポイント属性とレポートで繰り返される。
CSCwj83459	「could not execute statement; SQL [n/a]; constraint」エラーが原因で、新しい内部ユーザーを作成できない。
CSCwj72680	HS_err ファイルが MnT ノードで生成される。
CSCwk73315	Cisco ISE 360 モニタリングダッシュボードに、レート合計ではなく平均 CPU 時間のパーセンテージが表示される。
CSCwj72117	運用データの削除を実行すると、2 つの展開ノードの内、プライマリ モニタリング ノード名のみが表示される。
CSCwk25064	SXP スレッドにより Java ヒープに Null オブジェクトが格納されると、CPU の負荷と使用率が高くなる。
CSCwk53171	Cisco ISE /ers/config/endpoint/getrejectedendpoints にページネーションが設定されておらず、100 個のエンドポイントのみが返される。
CSCwj97449	snmp-server host の engineID フォーマットが正しくない場合に、SNMP v3 設定に基づき管理者にアラートが送信されない。
CSCwj38485	8 ノードの展開の <getAllTrustCerts> クラスで高いメモリ使用率が確認された。
CSCwj94315	Cisco ISE REST API のブラインド SQL インジェクションの脆弱性。

ID	見出し
CSCWj52362	Cisco ISE リリース 3.3 パッチ 1 から Cisco ISE リリース 3.4 への分割アップグレード中に、プライマリ管理ノードがディスク破損チェック段階でスタックする。
CSCWj33906	VPN クライアントの IPS-XP マッピングが作成されない。
CSCwk34825	不正な試行時の Cisco ISE 内部ユーザーのロックや一時停止カウンタが期待どおりに機能しない。
CSCwk69424	プロシージャコールで送信された ODBC 詳細設定はログに記録する必要がある。
CSCWj17975	IMS ロールが指定された証明書に EAP ロールを割り当てることができなかった。
CSCWj89479	複数の Cisco ISE ノードをドメインコントローラに同時に参加させると、重複アカウントが作成される。
CSCwk75761	Cisco ISE の [Endpoint Identity Groups] ページにアクセスする管理ノードポストで CPU 使用率が高くなる。
CSCwk66013	ローカルログの設定を変更しても、古いファイルの削除がトリガーされない。
CSCwi66105	Cisco ISE リリース 3.1 パッチ 7 でエンドポイント属性フィルタが無効になっている場合、カスタム属性が保持されない。
CSCWj40026	バックアップを GUI からスケジュールすると、バックアップの詳細でスケジュールステータスが「no」および「triggered from CLI」と表示される。
CSCwk38245	Cisco ISE リリース 3.2 パッチ 6 で、Cisco ISE_Internal_Operations_Diagnostics によって、localstore ディレクトリサイズの問題によりシステムがディスク容量の下限に達したことを示す致命的ロギングメッセージがトリガーされる。
CSCwc62131	mysql.proc テーブルが実装されていないため、Cisco ISE では MySQL 8.x をクエリできない。
CSCwm00497	Cisco ISE の passiveid-agent.log には、ログオンイベントが共有されている場合のユーザーに関する情報を含める必要がある。
CSCwk45006	Cisco ISE 管理者ユーザーがデバイス管理ライセンスを使用して初回ログインパスワードをリセットできない。
CSCWj74175	restprobeOOMHeap ダンプを圧縮する。
CSCwk90681	Cisco ISE リリース 3.3 パッチ 3 から複数のオプションが削除されたか、application configure ise コマンドで機能していない。
CSCWj80950	Cisco ISE が pxGrid を介してポスチャ準拠セッションを適切に共有していない。
CSCWj77067	内部ユーザー編集のエラーの説明を改善。
CSCwk29799	管理者証明書の問題が原因で、インストールされているパッチのリストがパッチ管理ページに表示されない。

ID	見出し
CSCwd61906	Sysaux テーブルスペースの割り当ては、ノードのプロファイルに基づいて行う必要がある。
CSCwk69537	ERS API を介して参加ポイントを削除すると、Cisco ISE リリース 3.2 API は参加ポイントが使用中かどうかを検証しない。
CSCwj12359	「show tech-support」の実行を中断すると、Cisco ISE でサービスが停止する。
CSCwh50924	変更の実行後に IPv6 ルートを削除できない。
CSCwk05023	アイデンティティの情報ページに未定義のデータがある。
CSCwj71638	オープン API GET コールによってポリシーが取得されると、ポリシーのヒット数が 0 と表示される。
CSCwk70500	Cisco ISE リリース 3.2 以降では、ボンドインターフェイスにはプライマリインターフェイスで設定されている MTU が必要である。
CSCwk80923	Cisco ISE CLI または SSH ユーザーがパスワードポリシーに従っていない。
CSCwm30212	pxGrid ダイレクトがスケジュール時刻ではなく、最後の再起動時刻に同期をトリガーする。
CSCwm48867	6 時間ごとに高負荷が発生するため、swapon または swapoff cron を削除する必要がある。
CSCwm35851	展開ページで PAN フェールオーバーが有効になっている場合、PAN- HA 事前チェックに失敗する。
CSCwj75183	Cisco ISE リリース 3.2 パッチ 5 でゲストのドキュメントを修正。
CSCwj87344	ホスト名の変更にキャプチャを削除できない。
CSCwm41230	Cisco ISE リリース 3.3 パッチ 3 で MnT データベースをリセットすると、すべてのデータベースが破損する。
CSCwk02837	メモリ使用率が高くなると、12 時間のパッシブトラフィックの後にアプリケーションサーバーが再起動する。
CSCwm53627	フルテーブルスキャンを排除するために、「EDF_MDM_GUID」の「EDF_MDM_GUID」ルックアップのインデックス作成を最適化。
CSCwk63923	DNS キャッシュタイムアウトが無視される。
CSCwm33110	ヒープスペースが RMQ コンシューマによってすべて使用される。
CSCwm72206	Cisco ISE リリース 3.3 パッチ 3 のインストール後、Cisco ISE リリース 3.3 パッチ 3 で、外部アイデンティティソースに「使用可能なデータがない」と表示される。
CSCwm58686	Cisco ISE がセッションをステッチしようとするため、パッシブセッションが FMC にパブリッシュされない。

ID	見出し
CSCwj72586	API ゲートウェイのメモリ制限により、Cisco ISE 管理 CLI で OOM Killer アラートが発生する。
CSCwm02519	LSD クラスに対する追加の修正。
CSCwm61668	TC-NAC_Tenable が「Scan Failed: Error in connecting to host: 403 Forbidden」エラーをスローする。
CSCwm44693	VM または SNS アプライアンスをシャットダウンして電源をオンにすると、Cisco ISE が古い CLI パスワードに戻る。
CSCwi89923	IPv6 が無効になった後のリンクローカル IPv6 アドレスを持つギガビットイーサネットまたはボンドインターフェイス。
CSCwm46079	VPN ユーザーのプライベート IP の SXP マッピングが学習されない。

Cisco ISE リリース 3.3 - 累積パッチ 3 の解決済みの不具合

問題 ID 番号	説明
CSCwi89720	Microsoft Azure AD は正式に Microsoft Entra ID に名前変更された。
CSCwi67639	コマンド show cpu usage が Cisco ISE リリース 3.X の情報を表示しない。
CSCwi60778	エンドポイントが再認証後にスタティック アイデンティティ グループの割り当てを失う。
CSCwj43912	アプリケーションの修復が編集後に表示されなくなる。
CSCwf24553	[Licensing] ページで使用する用語情報の提供に関する Cisco Umbrella の不具合。
CSCwj60692	Cisco ISE リリース 3.3 では TLS が一部の暗号のみを使用するように制限されているが、8905、9094、9095 ポートはすべての暗号を使用する。
CSCwi58699	Cisco ISE で Cisco Catalyst Center または EA ディクショナリ属性が更新されると、ゲストフローによって CoA がトリガーされる。
CSCwi62078	組み込みの認証プロファイル Block_Wireless_Access を使用すると、[404] Resource Not Found エラーが返される。
CSCwj48827	起動プログラムの修復時に、引用符で複数のタスクを追加できない。
CSCwj05508	ip host <ip> <fqdn> コマンドで、Cisco ISE に IP-FQDN エントリが作成されない。
CSCwk00439	ロックファイルが削除されないため、pxGrid ダイレクトサービスが初期化状態でスタックしたままになる。
CSCwj35698	ユーザーディクショナリの Cisco ISE ビジネスロジックの問題。

問題 ID 番号	説明
CSCwi94938	フィルタを使用すると、Cisco ISE リリース 3.2 ゲストユーザー API で誤った結果が返される。
CSCwh33160	Cisco ISE が、設定された SNMP サーバーに SNMPv3 ディスクトラップを送信できない。
CSCwi15793	Cisco ISE が特殊文字で始まる iPSK カスタム属性に対してエラーをスローする。
CSCwi59868	スポンサーゲストアカウントが許可されている最大日数を超えて延長されている。
CSCwi89082	Cisco ISE で SAML を設定するために必要な SAML デフォルトポータルがデータベースから削除される。
CSCvy34255	[require admin password] オプションを有効にすると、RADIUS または TACACS キーの表示中に追加のポップアップ画面が表示される。
CSCwi78164	/etc/hosts の重複エントリ (IP、名前、FQDN) が原因で、Cisco ISE DNS の正常性チェックが失敗する。
CSCwi61950	認証ポリシーの LDAP グループを照会するときに、Cisco ISE がプロキシフローのコンテキスト制限に達する。
CSCwj14217	デバイスネットワーク条件の GUI でロードに失敗する。
CSCwh67500	Cisco ISE リリース 3.2 で選択した認証プロファイルが見つからない。
CSCwj97620	pxGrid の直接同期が進行中にスタックする。
CSCwj12489	ネットワーク デバイス グループを削除できない。
CSCwi57903	スケジュール済みバックアップに失敗しても、アラームが生成されない。
CSCwj21203	「Dashboard System Status」のクエリで 1000 個のデータベース接続が使い果たされる。
CSCwj03747	特定の論理グループでは CoA が抑制されているにもかかわらず、プロファイリングで CoA が抑制されない。
CSCwh92366	Cisco ISE リリース 3.1 パッチ 8 の寿命設定で、仮想マシンリソース不足のアラームが発生する。
CSCwj06269	デバイス管理設定が変更されても、レポートやアラームが記録されない。
CSCwj51329	「VMware Workspace ONE」が MDM に設定されている MAC アドレスが複数ある場合、MDM コンプライアンスチェックに失敗する。
CSCwj39533	RMQ フォワーダにより、CPU または負荷平均が高くなる。
CSCwh01323	CoA 要求で IPv6 を使用するための修正。
CSCwj21403	/etc/hosts に複数のエントリがある場合に、REST API 認証サービスが有効にならない。

問題 ID 番号	説明
CSCwj36716	Cisco ISE の自己永続的クロスサイトスクリプティング (XSS) がレポートに表示される。
CSCwi59230	Cisco ISE に 1000 を超えるアイデンティティグループがある場合、ネットワーク管理者以外のユーザーはエンドポイントを編集または削除できない。
CSCwd49321	pxGrid が両方のノードで有効になっている場合でも、Cisco ISE で pxGrid が有効になっていないというエラーメッセージが表示され、Cisco ISE 統合に失敗する。
CSCwj43480	Cisco ISE リリース 3.3 がユーザープリンシパル名 (UPN) を持つユーザーに対して MFA を呼び出さない。
CSCwh36667	Cisco ISE モニタリング GUI ページが「Welcome to Grafana」のままになる。
CSCwi93050	管理者アクセスに Azure SAML を使用すると、RBAC でエンドポイントのインポートに失敗する。
CSCwh56565	MnT ノードへのプライマリ PAN REST API コールはロードバランシングしない必要がある。
CSCwi74567	データベース内の不整合により、Cisco ISE ポータルで破損が発生する。
CSCwa82035	Cisco ISE サポートバンドルにガベージコレクションログ、スレッドダンプ、ヒープダンプを含める必要がある。
CSCwj29392	Cisco ISE クロスサイト リクエスト フォージェリ。
CSCwi73981	大文字の FQDN を使用して追加されたアイデンティティストアを CLI から削除できない。
CSCwf36985	認証ポリシーの評価中に AD グループの取得に失敗する。
CSCwi98793	プロファイラが誤った値を持つ MDM 属性をキャッシュする。
CSCwj07319	API ers/config/sessionservice ノードが誤った合計を返す。
CSCwi79159	Cisco ISE リリース 3.2 パッチ 4 : deleteCertFromStore が証明書の解析に失敗する。
CSCwi61491	メタスペースの枯渇によりアプリケーションサーバーがクラッシュする。
CSCwi89689	無効な IP またはホスト名エラー。
CSCwi52041	ランクに変更があると、認証ルールがデータベーステーブルにコミットされ、UI からの保存コールがトリガーされる。
CSCwh00060	Cisco Identity Services Engine のコードインジェクションの脆弱性。
CSCwj16540	Cisco ISE リリース 3.2 パッチ 4 のコンテキスト可視性がライブログまたはセッションと一致しない。
CSCwj06401	エンドポイントの属性セクションに Null のキーと値のペアがあり、消去フローが中断される。

問題 ID 番号	説明
CSCwj72982	IP アドレス列フィルのパッシブ ID レポートに IPv4 または IPv6 の選択が表示されない。
CSCvt75833	トークンサーバーが FQDN の場合、Cisco ISE はルックアップを再度実行する必要がある。
CSCwh23986	pxGrid getUserGroups API 要求が空の応答を返す。
CSCwj32716	nsf は、複数の SAN -URI がある場合でも、index-0 SAN-URI を MDM に返す必要がある。
CSCvm56115	別のブラウザタブで ID ストアが削除されると、Cisco ISE でポリシーを保存できる。
CSCwi96581	3.4.2 に脆弱性があるため、CXF バージョンをアップグレードする。
CSCwj01310	SXP コンポーネントが原因で集中的なガベージコレクションが発生する。
CSCwh69267	ADE-OS の復元後、アプリケーションサーバーが初期化中にスタックする。
CSCwj07675	Cisco ISE リリース 3.2 が APIPA IP 169.254.4.x で発信 RST パケットを送信する。
CSCwi67503	API を使用して認証プロファイルを作成した場合、選択した認証プロファイルが Cisco ISE 3.2 で検出されない。
CSCwj47769	Cisco ISE リリース 3.2 パッチ 5 の無効な要求ページ。
CSCwi63725	SNMPD プロセスが原因で Cisco ISE でメモリリークが発生する。
CSCwi57761	Cisco ISE では、Common Vulnerability and Exposures (CVE) ID、CVE-2023-48795 で特定された脆弱性が、オープン SSH のサードパーティ製ソフトウェアに影響する。
CSCwh25160	スワップクリーンアップスクリプトがスワップ領域をドロップし、cron をプログラムする。
CSCwh95587	Cisco ISE リリース 3.2 パッチ 2 が断続的に NFS リポジトリをアンマウントしない。
CSCwd14523	Azure AD の「accountEnabled」属性により、EAP-TLS の認証問題が発生する。
CSCwh61339	90,000 を超えるネットワークデバイスのエクスポートがタイムアウトする。
CSCwj07717	Cisco ISE 監査レポートで、APIPA アドレスが API 要求の送信元としてログに記録される。
CSCwa32407	すべてまたは特定のゲストユーザーのユーザーアカウントの詳細をスポンサーに再送信する。
CSCwf56826	プライマリ PAN ノードで jstack に関連するコアが表示される。
CSCwj66777	Cisco ISE リリース 3.3 の ECDSA 明示的曲線テストが EAP、セキュア syslog、およびセキュア LDAP で失敗する。
CSCwj60125	ゲストユーザーアカウントの検索機能を強化。
CSCwk18638	プライマリ PAN にポリシーロールがない場合、TrustSec CoA がプライマリ PAN から送信されない。

問題 ID 番号	説明
CSCwi61950	認証ポリシーの LDAP グループを照会するときに、Cisco ISE がプロキシフローのコンテキスト制限に達する。
CSCwi38377	ディスパッチャキューでスタックした CoA をトリガーできない。
CSCwk07324	ACE サードパーティライブラリが原因で Cisco ISE のメインスレッドプールがスタックし、contextN のリークが発生する。
CSCwk61938	Cisco ISE は OpenSSH CVE-2024-6387 「regreSSHion」を評価する必要がある。
CSCwj44649	Cisco ISE 3.3 で TACACS データが保持されず、すべてが消去される。

Cisco ISE リリース 3.3 - 累積パッチ 2 の解決済みの不具合

問題 ID 番号	説明
CSCwf47838	コマンド引数のスペース文字が TACACS+ コマンドセットの CSV エクスポート後に保持されない。
CSCwi48806	認証ポリシーのロードに時間がかかり、Duo ポータルエントリで遅延が発生する。
CSCwf24554	SR-Insights で SL 登録失敗の詳細情報の表示に関する Cisco Umbrella の不具合を確認。
CSCwf93165	Cisco ISE 3.3 で [always show invalid usernames] オプションを有効にしても機能しない。
CSCwh99534	エンドポイントプローブが SGT 交換プロトコルマッピングをクリーンアップしない。
CSCwh24823	ERS を使用した内部ユーザーの更新で、必須ではない属性の値を保持する必要がある。
CSCwi53104	1 か月を超える期間のレポートをエクスポートすると、データが生成されない。
CSCwd67833	ERS API が単一のエンドポイントを更新するのに数秒かかる。
CSCwh83323	Cisco ISE 3.2 : カスタム SMTP API 宛先アドレスを使用している場合、「パスワードのリセット」フローで SMS が送信されない。
CSCwe25050	PPAN にインポートされたワイルドカード証明書が展開内の他のノードに複製されない。
CSCwi69659	TrustSec 展開の検証 : Cisco ISE と NAD でポリシーが同一であるにもかかわらず、ポリシー差異アラームが表示される。
CSCwh74135	不正なパスワードのエラーが原因で、Cisco Prime Infrastructure と統合できない。
CSCwi29253	Cisco ISE AD 診断ツールをアップグレードすると動作が停止し、使用可能なテストのリストを取得できない。
CSCvj75157	Cisco ISE API がユーザーアカウントの作成中にアイデンティティグループを認識しない。

問題 ID 番号	説明
CSCwf61673	Cisco ISE CLI 読み取り専用ユーザーは show CPU usage コマンドを実行できない。
CSCwi61491	メタスペースの枯渇によりアプリケーションサーバーがクラッシュする。
CSCwi54722	リダイレクト URL は IP で終わる FQDN を使用し、IP は Cisco ISE ホスト名で置き換えられる。
CSCwa15336	Cisco ISE PIC 3.1 では、ライブセッション機能は終了したセッションを表示しない。
CSCwi30707	Cisco ISE 3.1 パッチ 7 : 削除されたデバイスタイプをポリシーセットで引き続き選択できる。
CSCwi45090	Cisco ISE : REST API ERS : downloadablecl : フィルタフィールド「name」がサポートされない。
CSCwi42628	MAR キャッシュの複製が、NIC および非 NIC ボンディング インターフェイスの両方のピアノード間で失敗する。
CSCwh81035	PAN で PSN からのエンドポイントの重要ではない属性更新が欠落している。
CSCwi21020	Cisco ISE メッセージング証明書の生成では、セカンダリノードで完全な証明書チェーンが複製されない。
CSCwi04514	ディクショナリ属性に「-」が含まれている場合のポスチャクライアントプロビジョニングリソース HTTP エラー。
CSCwi36040	Cisco ISE 3.2 の IP アクセスリスト制御が表示されない。
CSCwi15914	SXP ADD 操作から IPv6 リンクローカルアドレス用の追加の IPv6-SGT セッションバインディングが作成される。
CSCwi66126	Cisco ISE ERS API : DACL を更新しても最終更新日のタイムスタンプが変更されない。
CSCwh87732	Antisamy 1.5.9 の脆弱性。
CSCvs77939	AnyConnect 設定およびポスチャ エージェント プロファイルの編集集中にエラーが発生する。
CSCwh21038	サードパーティのポスチャフロー中に、セッション情報が時間指定セッションキャッシュに保存されない。
CSCwh83482	Cisco ISE データベースがスポンサーアカウントの電子メールフィールドを更新しない。
CSCwh96018	同じ名前で大文字と小文字が異なる新しい MDM が作成された場合に、大文字と小文字を区別するチェックが原因で失敗する。
CSCwi54325	Linux の問題 : エンドポイントがポスチャリース内にある場合、PRA に失敗する。
CSCwi53915	高度なフィルタの [Save] オプションが、クライアントプロビジョニングリソースのフィルタリングで機能しない。

問題 ID 番号	説明
CSCwf89224	OU に & および @ 文字が含まれている場合、NAD から受信したセッションチケットの復号に失敗する。
CSCwh99772	子項目がいずれかのグループから削除された後、すべてのネットワーク デバイス グループが削除される。
CSCwh93498	デバイスポータルが重複している場合、Cisco ISE 3.1 のエンドポイント消去ルールが自動的に作成される。
CSCwh90610	Cisco ISE : 放棄された Jedis 接続がスレッドプールに返送されない。
CSCwh41977	Cisco ISE 3.2 : Cisco ISE 設定でのユーザーごとの dACL の存在の確認。
CSCwi40089	IP アドレスなしで pxGrid セッション更新の公開を許可する。
CSCwi45879	既存の認証プロファイルまたは重複した認証プロファイルが選択されている場合、ホットスポットポータルを選択できない。
CSCwh84446	アカウントの有効期限通知に特殊文字または改行文字が含まれている場合、ゲストタイプの保存が機能しない。
CSCwh71117	Cisco ISE 管理アクセス : 「User Services」のみを有効にすると、管理 GUI アクセスも有効になる。
CSCwi33361	Cisco ISE CLI のアクセスの問題 : サーバーへの接続に失敗しました。
CSCwi34117	Grafana UI と Kibana では Identity Services Engine に RBAC を実装する必要がある。
CSCwh55667	Cisco ISE ポスチャ障害 : Premier ライセンスが無効になっている場合の内部システムエラー。
CSCwi59555	Cisco ISE 3.2 パッチ4 : ODBC : フォーマット内の MAC アドレスの検索が無視される。
CSCwi18005	3.2 にアップグレードした後、外部 RADIUS サーバーリストが表示されない。
CSCwi17694	Cisco ISE : 10,000 以上に設定されている場合、synflood-limit が有効にならない。
CSCwf34596	ユーザーカスタム属性がレンダリングでスタックする。
CSCwe92640	Cisco ISE 3.1/3.2 : CLI 設定時に既存のルートの検証が実行されない。
CSCwi03961	ポリシーセットにロケーショングループ情報がない。
CSCwf61657	スポンサー FQDN の TCP ハンドシェイクに常に Gig0 が関与する。
CSCwh77574	証明書のインポート中に Cisco ISE がパスワードの特殊文字を許可しない。
CSCwi59312	Cisco ISE の認証プロファイルが「セキュリティグループ」と「再認証」の一般的なタスクでデータを保持しない。

問題 ID 番号	説明
CSCwh90691	show CLI コマンドが、ログレベルを 5 に設定した後に例外をスローする。
CSCwi59216	[Contact Support] をクリックすると、スポンサーポータルが 400 Bad Request を返す。
CSCwi45131	シスコ製品に影響を与える Apache Struts の脆弱性：2023 年 12 月。
CSCwh95022	日本語の UI を使用すると、スポンサーポータルの [Setting date] タブに誤った曜日情報が表示される。
CSCwi52264	Cisco ISE SAML アイデンティティプロバイダーの設定属性が参照されているにもかかわらず削除される。
CSCwf31073	Cisco ISE : OpenAPI を介してデバイス管理ネットワーク条件を取得するときに「Error 400」が表示される。
CSCwh92117	AUD\$ テーブルサイズの増加により、Sysaux テーブルスペースがいっぱいになる。
CSCwi25755	Cisco ISE 3.2 以降に SAML プロバイダーを追加できない。
CSCwi23166	パッチ管理条件の変更を保存できない。
CSCuz65708	Firefox 45 以降/Chrome 72 : DACL の行番号が正しくない。
CSCwi34405	認証中に IdentityAccessRestricted 属性を適用できない。
CSCwi05905	Cisco ISE ERS API/ers/config/deploymentinfo/getAllInfo がマルチノード展開で異なるデータを返す。
CSCwf80386	パッチのインストール時に、Disable_RSA_PSS 環境値の現在の値が保持されない。
CSCwi27497	iptables エラーが原因で Cisco ISE REST 認証サービスが実行されない。
CSCwi57950	Cisco ISE 3.2 : Nexpose Rapid 7 : Strict-Transport-Security 形式が正しくない。
CSCwc85211	Cisco ISE パッシブアイデンティティエージェントのエラー「id to load is required for loading」。
CSCwh93925	複数のスタティック デフォルト ルートが存在する場合、Cisco ISE が RADIUS トラフィックを誤ってルーティングする。
CSCwi28131	「消去なし」のルールで使用されているカスタム属性が依然としてエンドポイントを消去する。
CSCwi59567	CoA 再試行カウントを「0」に更新する際の問題。
CSCwh92185	[Operational Data Purging] ページからエクスポートされた RADIUS 認証レポートが空である。
CSCwi73984	Cisco ISE 3.1P8 の [Installed Patches] メニューにすべてのパッチが表示されない。
CSCwi78722	Azure VM : 展開にノードを登録できない。

問題 ID 番号	説明
CSCwh72754	Cisco ISE Active Directory プロセス (lwsmd) が「Updating」でスタックし、CPU を 90 ～ 100% 消費する。
CSCwi32576	CPMSessionID の割り当て中に PSN ノードがクラッシュする。
CSCwi19099	いずれかのコネクタが無効になっている場合、設定フォルダへのデータの挿入中に問題が発生する。
CSCwj27469	クラウド (Azure、AWS、OCI) 上の Cisco ISE 3.3 がディスクサイズを適切に読み取らず、サイズが常にデフォルトの 300 GB になる。

Cisco ISE リリース 3.3 の解決済みの不具合：累積パッチ 1

ID	見出し
CSCwf80509	Cisco ISE パッシブ ID セッションが常に 1 時間後にクリアされる。
CSCwh42683	読み取り専用の管理者グループのユーザーが、SAML 認証を介して Cisco ISE GUI にログインすると、フルアクセスできる。
CSCwh64195	データの破損により認証エラーが発生し、「FailureReason=11007」または「FailureReason=15022」というエラーメッセージが表示される。
CSCwf37679	プライマリ PAN ペルソナからアクセスすると、スポンサーポータルでスポンサー権限が無効になる。
CSCwf78003	[pxGrid Endpoints] ページで、エンドポイントの詳細が正確に表示されない。
CSCwh17386	Cisco ISE 展開の専用 MnT ノードが SMTP 設定を複製しない。
CSCwe89459	Cisco ISE REST API ドキュメントで、エンドポイントグループの作成時に誤ったスクリプトが提供される。
CSCwf25955	SGT、VN 名、VLAN フィールドが空の match 認証プロファイルを使用すると、ポートがクラッシュする。
CSCwh18487	期限切れのゲストアカウントが、アカウントを再アクティブ化しようとしても SMS を受信しない。
CSCwh71273	必須ライセンスを無効にすると Cisco ISE GUI ページへのアクセスが制限され、ルート CA を再生成できなくなる。
CSCwh52589	Acs.Username が最初のデバイス接続の際、ゲストユーザー名で更新されない。
CSCwd82539	ローカルまたはグローバルの例外ルールが認証ポリシーと一致しない。

ID	見出し
CSCwh06338	クライアント プロビジョニング ポータルの設定を編集しようとしても GUI がロードされない。
CSCwf68108	エンドポイントの OpenAPI が既存の IOT アセット属性で機能しない。
CSCwd79277	同期に最大数の TrustSec オブジェクトが選択されている場合、同期ステータスが失敗と表示される。
CSCwh79938	高度な調整中に PreferredDCs レジストリ値を設定できない。
CSCwe07822	最後の消去日付のタイムスタンプが正しくない。
CSCwb63834	MNT ログプロセッサが非 MNT 管理 Cisco ISE ノードで有効になっている。
CSCwe95624	Cisco ISE リリース 3.2 で、ノードの再起動後に SNMP が機能しない。
CSCvz48764	起動プログラムの修復に一定の順序を設定できる。
CSCwh95022	日本語の Cisco ISE GUI を使用すると、スポンサーポータルの [Setting date] タブに誤った曜日情報が表示される。
CSCwf22794	VLAN ID に不整合がある場合、「Not a valid ODBC dictionary.」というエラーメッセージが表示される。
CSCwh69045	Cisco ISE リリース 3.1 パッチ 5：一部の内部ユーザーのパスワードが、設定されたグローバルパスワードの期限を過ぎても期限切れにならない。
CSCwe74135	Cisco ISE リリース 3.1 パッチ 5：PAN の障害後にゲストポータルを削除しようとする、完全性制約 ORA-02292 が発生する。
CSCwd28431	Cisco ISE コードからの EPS の削除。
CSCvq79397	カスタム管理メニューのワークセンター権限で Cisco ISE GUI ページが正しくロードされない。
CSCwh51156	Cisco ISE が破損した NAD プロファイルをロードできず、次の認証エラーが発生する：failureReasons 11007 and 15022。
CSCwh47299	Cisco ISE アラームとダッシュボードの概要がロードされない。
CSCwh51548	Cisco ISE 3.2.0.542：パッチとホットパッチの両方が ZTP 設定にある場合、ホットパッチがインストールされない。
CSCwc26835	RADIUS サーバーのシーケンス設定が破損する。
CSCwf44906	設定バックアップの復元後、ログイン情報を使用してリポジトリを再設定する必要がある。
CSCwf72037	Cisco ISE リリース 3.1：管理者ログインレポートに 5 分ごとに「Administrator authentication failed」と表示される。

ID	見出し
CSCwh36544	pxGrid にトピック登録の詳細が表示されない。
CSCwf39620	ユーザー名が特殊文字「\$」で始まる場合、Windows でエージェントレスポスチャが機能しない。
CSCwd36753	スクリプトの条件名にピリオドが含まれている場合、AnyConnect ポスチャスクリプトが実行されない。
CSCwh17448	Cisco ISE リリース 3.1：ドメインユーザーがエンドポイントログイン用に設定されている場合、エージェントレス ポスチャ フローが失敗する。
CSCwf72918	Cisco ISE リリース 3.2 で、実行コンフィギュレーション内の IP ネームサーバーの順序に誤りがある。
CSCvj75157	Cisco ISE API がユーザーアカウントの作成中に ID グループを認識しない。
CSCwh63501	log4net 2.0.8.0 の脆弱性。
CSCwh47601	Cisco ISE リリース 3.2 パッチ 2 および 3：40 文字の認証パスワードとプライバシーパスワードを持つユーザを作成できない。
CSCwh58768	Cisco ISE リリース 2.7 からの復元後に、デバイスポータルで既存のデバイスを削除できない。
CSCwd57628	Cisco ISE リリース 3.1 パッチ 1、2、3、4、および 5 で、アポストロフィで始まる NAD RADIUS 共有秘密キーが正しくない。
CSCwh46669	管理証明書の変更後、ボンドインターフェイスが設定されている場合、Cisco ISE がサービスを再起動しない。
CSCwh17285	Cisco ISE リリース 3.2 パッチ 3 および Cisco ISE リリース 3.3：インターフェイス上の IPV6 コマンドが <i>IPV6 enable</i> のみの場合、ポータルの初期化が失敗する。
CSCwe10898	ゲストポータルで猶予アクセスを使用すると、エンドポイントの MAC アドレスがエンドポイント ID グループに追加されない。
CSCwf07855	コールが失敗した場合、Cisco ISE SXP バインディング API コールが 2xx 応答を返す。
CSCwh42009	Cisco ISE リリース 3.2 パッチ 3：Cisco ISE GUI 設定が [TRACE] または [DEBUG] であっても、adapter.log が INFO 状態のままとなる。
CSCwh03740	CRL の取得に失敗する。
CSCwf22527	Context visibility：エンドポイントのカスタム属性を特殊文字でフィルタリングできない。
CSCwf10516	Cisco ISE リリース 3.2 で、認証ポリシーの検索機能が動作しない。
CSCwh05599	ゲストタイプに特殊文字が使用されている場合、Cisco ISE スポンサーポータルに入力が無効である旨のエラーが表示される。

ID	見出し
CSCwh18899	Cisco ISE Open API：「/certs/system-certificate/import」でマルチノード展開をサポートする必要がある。
CSCwf88944	ゲストポータル の FQDN がデータベース内のノードの IP アドレスにマッピングされる。
CSCwh23367	Cisco ISE リリース 3.2 のスポンサーゲストポータルにおいて、自己登録された電子メールの件名の等号記号 (=) 以降がすべて切り捨てられる。
CSCwf72123	pxGridDirect で、ユーザーデータ情報がデータ配列内のネストされたオブジェクトに保存されている場合、Cisco ISE によって処理されない。
CSCwf80292	Cisco ISE が EAP-TLS 認証中にピア証明書を取得できない。
CSCvo60450	Cisco ISE：MS-RPC コールの AES256 のみを送信するための暗号化の機能拡張。
CSCwf10773	「no ip name-server <IP_of_DNS_server>」コマンドを使用して複数の DNS サーバーの 1 つを削除すると、再起動プロンプトなしで Cisco ISE のサービスが再起動する。
CSCvw81130	Cisco ISE リリース 2.7：スケジュール済みの Active Directory 診断ツールのテストを無効にできない。
CSCwh26288	pxGridDirect：コネクタの追加に Premier ライセンスが必要となる。この機能を使用するには、Advantage ライセンスが必要です。
CSCwf30570	エンドポイントが AC 電源に接続されていない場合、エージェントレス ポスチャ スクリプトが実行されない。
CSCwf24158	Portal Builder を Cisco ISE リリース 3.0 以降のリリースで使用すると、[Terms and Conditions] チェックボックスが表示されない。
CSCwf94289	Cisco ISE リリース 3.0 パッチ 6：Policy export でポリシーのエクスポートに失敗する。
CSCwc39545	DockerMetrics：レポートを変更する必要がある。
CSCwa08802	AWS 上の Cisco ISE リリース 3.1 でヘルスチェックの DNS チェックの検出漏れが生じる。
CSCwf09393	Cisco ISE リリース 3.1：Cisco ISE リリース 2.7 からのバックアップの復元後、サービスを開始できない。
CSCwe15945	ゲストアカウントが特定のスポンサーグループのスポンサーに表示されない。
CSCwf34391	アクティブ認証 syslog の前に PassiveID syslog が MnT によって受信されると、Cisco ISE EasyConnect スティッチングが発生しない。
CSCwh42442	Cisco ISE リリース 3.2 パッチ 3：CRL のダウンロードに失敗する。
CSCwf79582	証明書 API (/admin/API/PKI/TrustCertificates) は公開されないが、Cisco DNA Center と AD ユーザー名の統合が中断される。

ID	見出し
CSCwf14365	ログ分析ページに移動すると、「Configuration Missing」という警告が表示される。
CSCwh24823	ERS API を使用した内部ユーザーの更新で、必須ではない属性の値を保持する必要がある。
CSCwh90691	show CLI コマンドが、ログレベルを 5 に設定した後に例外をスローする。
CSCwf66934	Cisco ISE リリース 3.2：新しい Context Visibility ダッシュボードを追加すると、Windows で GUI の問題が発生する。
CSCwh14249	Cisco ISE 3.x：API ゲートウェイ設定のスペルミス。
CSCvz86688	Aruba-MPSK-Passphrase に暗号化のサポートが必要。
CSCwf09364	ユーザー ID グループとエンドポイント ID グループの説明フィールドの文字数制限が 1199 文字である。
CSCwc04447	Cisco ISE リリース 2.7 パッチ 6：ネットワークデバイス IP で TACACS ライブログをフィルタリングできない。
CSCwh30893	プロファイリングで、次の形式の発信側ステーション ID の値が処理されない： XXXXXXXXXXXX。
CSCwh10401	Cisco ISE リリース 3.1 パッチ 5：CSR オプションを利用して pxGrid クライアント証明書を生成できない。
CSCwh70275	登録解除から残った証明書を使用してノードを登録すると、現在使用中の証明書が削除される。
CSCwf47038	pxGrid ポリシーの [Trash all] または [selected] オプションが、内部グループのエントリに影響しないようにする必要がある。
CSCwf07444	Cisco ISE パッチ GUI のインストールが、展開中に特定の Cisco ISE ノードでスタックする。
CSCwh04251	Cisco ISE エージェントレスポスチャで、コロンを含むパスワードがサポートされない。
CSCvu56500	Cisco ISE 上のすべてのネットワークデバイスをエクスポートすると、ファイルが空になる。
CSCwf66237	Cisco ISE：Get All Endpoints 要求の実行に時間がかかる（Cisco ISE リリース 2.7 以降）。
CSCwf59058	管理メニューが非表示の場合、カスタム権限を持つ RBAC ポリシーが機能しない。
CSCwd97984	Cisco ISE アプリケーションサーバーの再起動直後に Cisco Meraki 同期サービスが実行されない。
CSCwf66880	エンドポイントの .csv ファイルのインポートで、ファイルを選択した後に「no file chosen」と表示される。
CSCwh08408	Cisco ISE リリース 3.3 で、ノードエクスポートのパスワードが見つからないため、アップグレード後の展開に新しいノードを登録できない。

ID	見出し
CSCwf26951	プロファイラ CoA が誤ったセッション ID で送信される。
CSCwh45472	PKI キーペアのパスフレーズにプラス (+) 記号が含まれている場合、Cisco ISE GUI から SFTP リポジトリへの運用バックアップが失敗する。
CSCwh28528	着信 TACACS が 1 日あたり 40M レコードを超えると、TopN デバイス管理レポートが機能しなくなる。
CSCwf40265	Cisco ISE の最大セッションカウンタの有効期限が機能しない。
CSCwf97173	非同期ポリシーエンジンがアクティブな VPN クライアントの ANC 検疫の CoA に影響する。
CSCwh48026	pxgriddirect-connector.log で、実際のクロック時刻とログの出力時刻が一致しない。
CSCwf83193	AD ログイン情報を使用してセカンダリ管理ノードの GUI にログインできない。
CSCwf96294	Cisco ISE リリース 3.0：接続試行がドメインで許可されない。
CSCwd34467	EAP チェーンおよび Azure AD グループを使用した試行で、Cisco ISE 承認ルールの評価が失敗する。
CSCwf98849	クライアント プロビジョニング ポータルのカスタマイズで重大なエラーが発生する。
CSCwf61939	[First Name] または [Last name] フィールドにアポストロフィを使用すると、名前が無効である旨のエラーが表示される。
CSCwf64662	SXP で、IP アドレスと SGT 間にマッピングの不整合が発生する場合がある。
CSCwc36589	Intune からの MAC アドレスベースの API のサポート終了により、Cisco ISE Intune MDM 統合が中断される可能性がある。
CSCwh18731	アップグレード前に LSD を無効にして Cisco ISE リリース 3.2 にアップグレードすると、EP プロファイラ例外が発生する。
CSCwc53824	Cisco ISE で、AMP AMQP サービスへの接続が TLSv1.0 に制限される。
CSCwe53550	Cisco ISE および CVE-2023-24998。
CSCwf82055	Cisco ISE：パッシブ ID エージェントに関連付けられたポートの SHA1 を無効にできない。
CSCwh53159	Cisco ISE リリース 3.1 パッチ 7：特殊文字「\$」が含まれている管理者パスワードを変更できない。
CSCwf62744	「disable EDR internet check」タグの追加。
CSCwh26698	pxGrid コネクタのユーザーデータを取得する方法の追加。
CSCwh28098	Cisco ISE リリース 3.2 パッチ 3：RSD が無効になっているポスチャアセスメント中に、CoA プッシュの代わりに CoA 切断が送信される。

ID	見出し
CSCwb57672	SHA384 と RSA4096 証明書を備えた GCMP256 認証（Android 12 の要件）が失敗する。
CSCwe82004	TCP ソケットの枯渇。
CSCwf98944	axios 0.21.1 の脆弱性。
CSCwh38464	Cisco ISE CLI ユーザーが、Cisco ISE CLI を使用しない状態が約 2 か月続くとログインできなくなる。
CSCwd21798	Cisco ISE-PIC ライセンスの期限切れアラーム。
CSCwf71870	0 日間の評価期間で TACACS 展開を行った場合、スマートライセンスの登録後に動作しない。
CSCwh46877	PORT_BOUNCE を使用して ANC ポリシーを削除する際、CoA ポートバウンスが必要となる。
CSCwf62987	AntiSamy 1.5.9 の脆弱性。
CSCwh32290	リセット設定の実行後、GUI と CLI の FQDN 値が一致しない。
CSCwh60726	Cisco ISE 自動クラッシュデコーダの障害。
CSCwf31477	スイッチポートに複数のセッションが存在する場合、プロファイラがポートバウンスをトリガーする。
CSCwh71435	ERS API で指定されていない場合に、内部ユーザーのイネーブルパスワードが作成される。
CSCwf55641	ドイツ語とイタリア語の電子メールがゲストタイプのアカウント有効期限通知に保存できない。
CSCwf28452	クライアントプロビジョニングポリシーへの保存後、他の条件の順序が変更される。
CSCwh41693	ISEaaS : AWS : IMDS v2 をサポート。
CSCwh05647	IPv6 のスタティックルートが、Cisco ISE リリース 3.2 でのリロード後に削除される。
CSCwh44407	Cisco ISE リリース 3.2 API : システム証明書のインポートが、展開中の Cisco ISE ノードで機能しない。
CSCwf27484	100 以上のグループにユーザーが属している場合、Azure AD グループを照合できない。
CSCwe03624	スマートライセンスの登録に失敗し、「communication send error」アラームが断続的に発生する。
CSCwf81550	Cisco ISE で、MAC アドレスでない場合でも、選択した MAC アドレス形式に従って MAC アドレス形式が変更される。
CSCwf54680	名前に括弧が含まれている認証プロファイルを編集または削除できない。

ID	見出し
CSCwh38484	Cisco ISE リリース 3.0 パッチ 7 で、スタティックルートを手動で削除すると、Cisco ISE が誤った MAC アドレスのパケットを送信する。
CSCwf35760	ct_engine の CPU 使用率が 100% になる。
CSCwh39008	構成バックアップのスケジュールを設定または編集できない。
CSCwf60904	ANC の修復が AnyConnect VPN で機能していない。
CSCwh03227	認証プロファイルルールを使用せず認証すると、Cisco ISE がライセンスを消費しない。
CSCwf80951	「xwt.widget.repeater.DataRepeater」エラーにより、管理者ユーザーを編集または作成できない。
CSCwh51136	Cisco ISE が RADIUS 要求をドロップし、「Request from a non-wireless device was dropped」というメッセージが表示される。
CSCwh30723	Cisco ISE の Context Visibility で、コロンなどの区切り文字がない場合、スタティック MAC エントリが検証されない。
CSCwf59310	Cisco ISE リリース 3.1 パッチ 7 : Context Visibility と pxGrid コンテキストインにカスタム属性が存在しない。
CSCwf38083	Cisco ISE サービスが、Secure SysLog で初期化状態のままになる。
CSCwh35713	ユースケースに関する ERS SDK 開発者リソースが適切に読み込まれない。
CSCwh03306	ポート 1521 が使用できない場合、スレッドがプライマリ PAN でブロックされる。

Cisco ISE リリース 3.3 の解決済みの不具合

Cisco ISE リリース 3.3 で解決済みの不具合は、Cisco ISE パッチリリース（3.2 パッチ 2、3.1 パッチ 7、3.0 パッチ 7）と同等です。

次の表は、リリース 3.3 で解決済みの不具合のリストです。

問題 ID 番号	説明
CSCwe34204	パッチのインストール後に Cisco ISE の [アップグレード (Upgrade)] タブにアップグレードが進行中であると表示される。
CSCwd07345	Cisco ISE の特権昇格の脆弱性。
CSCwc50392	約 53,000 のグループを持つ ROPC グループの fetch コマンドが Cisco ISE GUI で機能しない。
CSCwf15717	Cisco ISE リリース 3.2 では、システム 360 機能はデバイス管理ライセンスで使用できない。
CSCwe37377	Cisco ISE CRL 取得失敗アラームには、CRL のダウンロードが失敗したサーバーを表示する必要がある。

問題 ID 番号	説明
CSCwc33290	Cisco ISE でカスタムエンドポイント属性を削除できない。
CSCvr79992	Cisco ISE でエンドポイントの認証時に Session.CurrentDate 属性が正しく計算されない。
CSCwd48787	Cisco ISE - SSL バッファにより、PAC 復号で問題が発生している。これは、Cisco ISE の EAP-FAST フローに影響する。
CSCwe68336	条件別ポスチャ評価で Cisco ISE GUI で次の無効な識別子が生成される : ORA-00904: "SYSTEM_NAME"
CSCwd07349	Cisco ISE のコマンドインジェクションの脆弱性。
CSCwd27865	Cisco ISE でエンドポイントをグループに割り当てるときに、[設定が変更されました (Configuration Changed)] フィールドが機能しない。
CSCwf14957	日本語の Cisco ISE GUI を使用している場合、TrustSec ステータスを変更できない。
CSCwe69085	デバイス管理ライセンスが有効になっている場合、Cisco ISE GUI でポリシーサービスノードにアクセスできない。
CSCwc33751	Cisco ISE リリース 3.1 では、TFTP プロトコルを使用した copy コマンドがタイムアウトする。
CSCwd97022	Cisco ISE リリース 3.2 パッチ 3 では、無効な Cisco ISE-PIC スマートライセンスが誤ってアップグレードに使用されている。
CSCwd46505	キューリンクエラーアラームが Cisco ISE-PIC ノードに表示されない。
CSCwd07340	Cisco ISE の特権昇格の脆弱性。
CSCwc39320	CLI を使用してアップグレードされた Cisco ISE ノードは、Cisco ISE GUI で [アップグレード中 (Upgrading)] ステータス以降に進まない。
CSCwd93719	Cisco ISE XML 外部エンティティ インジェクションの脆弱性。
CSCwe18359	Sudo 1.8.29 (サードパーティ製ソフトウェア) の脆弱性が修正された。
CSCwd63749	Cisco ISE リリース 3.1 では、多数の Active Directory グループをロードすると、[Active Directory グループの取得 (Active Directory Retrieve Groups)] ウィンドウに空白の画面が表示される。
CSCwd24089	セーフモードで Cisco ISE リリース 3.2 を起動できない。
CSCwb92655	Cisco ISE リリース 3.1 および 3.2 では、共通ポリシー (CDP) はデフォルトで有効になっていない。
CSCwb77915	Cisco ISE GUI の [許可されているプロトコル (Allowed Protocols)] のポリシーに基づいた RSA PSS 暗号の有効または無効をトグルボタンを使用して切り替える。
CSCwd30994	デフォルトスタティックルートが Gigaset 0 を除くインターフェイスのサブネットゲートウェイで設定されている場合、Cisco ISE へのネットワーク接続は失われる。

問題 ID 番号	説明
CSCwe55215	Cisco ISE スマートライセンスが Smart Transport を使用するようになった。
CSCwd35608	古い監査セッション ID が使用されているため、Cisco ISE で CoA が失敗する。
CSCwc61320	ログのダウンロードページがバックグラウンドで読み込まれるため、サポートバンドルページが低速になる可能性がある。
CSCwc58608	Cisco ISE リリース 3.2 では、EAP-FAST および EAP チェーンで RADIUS 要求を受信するとすぐにキャッシュが行われる。
CSCvt62460	ノードが未定義のサーバーを使用している場合、異なる LDAP からグループを取得できない。
CSCwd70902	IMS が有効になっている場合、PRRT はフラグメント化されていないメッセージをモニタリングノードに送信する必要がある。
CSCwe49261	Cisco ISE PassiveID エージェントは、すべてのドメイン（PassiveID が設定されていないドメインを含む）のステータスをプローブする。
CSCwc95878	アプリケーションのアクティベーションで断続的な問題が発生する。
CSCwd13201	Google Chrome および Microsoft Edge ブラウザで認証ポリシーをロードしているときに、Cisco ISE GUI がクラッシュする。
CSCwc57294	設定の読み取りに例外がある場合、Duplicate Manager で関連パケットが削除されない。
CSCwe07354	RADIUS トークンサーバー設定はセカンダリサーバーの空のホスト IP アドレスを受け入れる。
CSCwd57071	自己登録ポータルが、スポンサーに送信される承認/拒否リンクのノードの FQDN をサポートしない。
CSCwf26973	Cisco ISE 管理者アカウントが読み取り専用の場合、ネットワーク デバイス グループ情報が欠落している。
CSCwd27506	Cisco ISE リリース 3.0 パッチ 6 では、外部管理者によって作成されたスケジュール済みレポートがない。
CSCwc79321	ID ソースを RSA/RADIUS トークンサーバーの内部ソースから外部ソースに変更できない。
CSCwd41773	Cisco ISE リリース 3.1 では、5 MB 以上の CRL が頻繁にダウンロードされると、アプリケーションサーバーがクラッシュする。
CSCwd97606	異なるセッション ID を持つ同じ IP、VN、VPN の組み合わせに対する複数のリクエストにより、Cisco ISE で重複するレコードが作成される。
CSCwe63320	Cisco ISE リリース 3.2、3.1、および 3.0 では、[すべてのエンドポイントの取得（Get All Endpoints）] レポートに一致しない情報が表示される。

問題 ID 番号	説明
CSCwe54466	Cisco ISE のスポンサーポータル印刷の問題により、設定されている消去設定ではなく、最初のログインから (From-First-Login) ゲストアカウント設定に基づいてゲストユーザー設定が表示される。
CSCwc62419	Cisco ISE の不十分なアクセス制御の脆弱性。
CSCwe33360	Cisco ISE で変則的挙動の検出が期待どおりに機能しない。
CSCwe69179	最新の IP アクセス制限設定により、Cisco ISE で以前の設定が削除される。
CSCwd90613	[RADIUS server sequence] ページに「使用可能なデータがない」というメッセージが表示される。
CSCwd30433	ゲストアカウントの作成が拒否された場合の電子メール通知が管理者に送信されない。
CSCwc86067	Cisco ISE の承認バイパスの脆弱性。
CSCwd31524	Cisco ISE リリース 3.2 では、SFTP の設定の 16 文字のパスワードはサポートされていない。
CSCwd12357	9644 での例外が原因で、SXP サービスが初期セットアップでスタックする。
CSCwd41219	Cisco ISE のコマンドインジェクションの脆弱性。
CSCwf19811	Cisco ISE リリース 3.1 では、SXP バインディングレポートに「データが見つかりません (No data found)」エラーが表示される。
CSCwe70402	Cisco ISE 3.2 は、単一行の JavaScript コメントを含むポータル カスタマイズ スクリプトをサポートしない。
CSCwe15315	ネットワーク デバイスの CSV テンプレートファイルのインポート中に、TrustSec PAC 情報フィールドの属性値が失われる。
CSCwe37978	データサイズが大きいスケジュール済みレポートは、Cisco ISE リポジトリで「空」として表示される。
CSCwd87161	Cisco ISE リリース 3.1 で、デバイス管理ライセンスが有効になっている場合にのみ、証明書ベースのログインでライセンスファイルが要求される。
CSCwe22934	MAC アドレスを持たないデバイスが原因で、Cisco ISE 認証の遅延が発生する。
CSCwe43002	読み取り専用管理者を、Cisco ISE 管理 SAML 認証で使用できない。
CSCwe64558	ネットワーク アクセスユーザーから作成された Cisco ISE 管理者アカウントは、Cisco ISE GUI でダークモード設定を変更できない。
CSCwd30038	Cisco ISE のコマンドインジェクションの脆弱性。
CSCwd30039	Cisco ISE のコマンドインジェクションの脆弱性。

問題 ID 番号	説明
CSCwd07350	Cisco ISE パストラバーサルの脆弱性。
CSCwd28431	エンドポイント保護サービスが Cisco ISE コードから削除された。
CSCwc93253	フィルタが 1 つのネットワークデバイスに一致する場合にのみ、Cisco ISE ネットワークデバイス CAPTCHA が入力を要求する。
CSCwd51812	Cisco ISE GUI の証明書認証権限は、Cisco ISE リリース 3.1 パッチ 4 で変更された。
CSCwc64346	ネットワークデバイスのバルクリクエストについて Cisco ISE ERS SDK のドキュメントが正しくない。
CSCwd31137	Cisco ISE のスケジュール RADIUS 認証レポートが SFTP リポジトリへのエクスポート中に失敗する。
CSCwc48509	Windows Server 2022 はターゲット ドメイン コントローラとして機能していて、監視する必要がある。
CSCwc47015	CSCvz85074 の解決策により、Cisco ISE での AD グループの取得が中断される。
CSCwe52296	Cisco ISE MNT 認証ステータス API クエリを最適化する必要がある。
CSCvg66764	Cisco ISE-PIC エージェントは、セッションスティッチングのサポートを提供する。
CSCwf33128	Cisco ISE の RADIUS 使用スペースが誤った使用状況を報告する。これは、最終レポートで TACACS テーブルも考慮されるため。
CSCwf02093	Cisco ISE リリース 3.2 では、Hyper-V のインストールで DHCP が有効になっている。
CSCwb83304	カスタム セキュリティ グループが原因で Cisco ISE のアップグレードが失敗する。
CSCwc47799	Cisco ISE は、パスワードに「%」を含む証明書と秘密キーをインポートするときにエラーメッセージを表示しない。
CSCwd32591	Cisco ISE リリース 3.2 では、[キーペアの生成 (generate key pair)] オプションをクリックした後でも、Cisco ISE GUI から SFTP リポジトリを操作できない。
CSCwd42311	Cisco ISE GUI のダウンロードログから REST-ID ストアをダウンロードできない。
CSCwd48000	TomCat 9.0.14 の脆弱性。
CSCwc31482	Sierra Pacific Windows (Microsoft Windows の SPW ウィンドウ) を使用している場合、BYOD フローで NetworkSetupAssistance.exe デジタル署名証明書が期限切れになる。
CSCwd92324	Cisco ISE リリース 3.2 ROPC の基本的な有用性の改善。
CSCwe12098	Cisco ISE リリース 3.2 で、ゲストポータル設定用のポートが、AWS にインストールされた Cisco ISE ノードで開かない。

問題 ID 番号	説明
CSCwf21585	安全でない可能性のあるメソッドの使用：HTTP PUT メソッドが受け入れられた。
CSCwe49422	Cisco ISE リリース 3.2 以降で、identity-store コマンドにテキストパスワードを入力する必要がある。
CSCwe96633	サポートバンドルに terrors.log および times.log が含まれない。
CSCwd19529	Cisco ISE の保存されたクロスサイト スクリプティングの脆弱性。
CSCwf22799	コンプライアンスモジュールが Cisco Secure クライアントと互換性がない場合、遅延更新条件が機能しない。
CSCwe91917	ユーザーは TACACS 認証プロファイルに引用文字を追加できない。
CSCwe85920	Cisco ISE TrustSec ロギング：SGT 作成イベントが ise-psc.log ファイルに記録されない。
CSCwd97353	自動バックアップが 3 ～ 5 日後に停止する。
CSCwd71574	Cisco ISE でエージェントレスポスタチャが設定されている場合に CPU 使用率が高くなる。
CSCwe27146	Cisco ISE リリース 3.2 パッチ 1 で「-」（ハイフン/ダッシュ）を含む CLI ユーザー名を解析できない。
CSCwc69492	Cisco ISE リリース 3.1 で、メタスペースを使い果たすと Cisco ISE ノードでクラッシュが発生する。
CSCwe97989	Cisco ISE リリース 3.2 が認証プロファイルの VN でクラッシュする。
CSCwd24304	Cisco ISE リリース 3.2 ERS POST /ers/config/networkdevicegroup が失敗し、属性 othername/type/ndgtype が破損する。
CSCvz68091	ゲストタイプの設定変更が監査レポートで更新されない。
CSCwe70889	DB サービスのタイムアウトが原因で、Cisco ISE リリース 3.0 から Cisco ISE リリース 3.1 へのフルアップグレードに失敗した。
CSCwd92835	[ネットワークデバイスプロファイル (Network Device Profile)] に HTML コードが名前として表示される。
CSCwe50710	Cisco ISE リリース 3.2 では、クラウド上の Cisco ISE 展開インスタンスに DNS ドメインを入力するとエラーが表示される。
CSCwe49167	Cisco ISE リリース 3.2 では、設定の保存時に SAML 署名認証要求の設定がオフになる。
CSCwf33881	Cisco ISE リリース 3.2 パッチ 1 では、Cisco ISE ポート、リソース、またはリファレンスガイドに記載されていないサーバーへの接続が確立される。
CSCwc44580	Cisco ISE リリース 3.1 で IP 10.88.0.1 および 10.88.0.0/16 の IP ルートを持つ cni-podman0 インターフェイスが作成される。

問題 ID 番号	説明
CSCwe14808	Cisco ISE が msRASSavedFramedIPAddress の AD 属性の変換に失敗する。
CSCwe57764	CVE-2021-26414 の Windows DCOM サーバー強化後に Microsoft SCCM への MDM 接続が失敗する。
CSCwf17490	サービスライセンスの更新後、Cisco ISE ライセンスページに、消費されたライセンスの評価コンプライアンスステータスが表示される。
CSCwd78306	ROPC 認証機能は、Cisco ISE リリース 3.2 では機能しない。
CSCwf13630	モニタリング ログ プロセッサ サービスが毎晩停止する。
CSCwd38766	「-」または「_」文字が含まれる SNMPv3 ユーザー名を削除すると、Cisco ISE から 16 進数のユーザー名が削除されない。
CSCvy69943	{ } 文字を含むコンテンツヘッダーを含むゲストポータル HTTP リクエストが許可される。
CSCwe78540	Get All Endpoints を使用すると、iotAsset 情報が欠落する。
CSCwd07351	Cisco ISE のコマンドインジェクションの脆弱性。
CSCwd05697	ゲストロケーションが Cisco ISE ゲストポータルにロードされない。
CSCwd03009	Cisco ISE リリース 2.7 パッチ 7 のハードウェアアプライアンスのプラットフォームプロパティを制御する RMQForwarder スレッド。
CSCwe74531	Cisco ISE の毎時クリーンアップは、95% 使用されているメモリではなく、キャッシュされたバッファをクリーンアップする必要がある。
CSCwd41018	Cisco ISE のコマンドインジェクションの脆弱性。
CSCwd16837	ダイレクトリスティングが無効になっていると、Cisco ISE OpenAPI HTTP リポジトリパッチのインストールが失敗する。
CSCwa62202	ポータルアクセス用に 2 つのインターフェイスが設定されている Cisco ISE が破損している。
CSCwe24932	エンドポイントログイン設定で複数のドメインユーザーを使用すると、エージェントレスポスチャが失敗する。
CSCwe48311	IMS を使用した Cisco ISE vPSN のパフォーマンスが、UDP syslog と比較して 30 ~ 40% 低下する。
CSCwa55233	IMS にサードパーティの署名付き証明書を使用している場合に「不明な CA」キューリンクエラーが表示される。
CSCwf42496	「Is IPSEC Device」NDG を削除しようとする、後続のすべての RADIUS/TACACS+ 認証が失敗する。

問題 ID 番号	説明
CSCwd41651	Cisco ISE リリース 3.1 の [RBACデータとメニュー権限 (RBAC Data and Menu Permissions)] ウィンドウに垂直スクロールバーがない。
CSCwe86793	REST ID ストアグループの Cisco ISE フィルタに「Error Processing this request (このリクエストの処理中にエラーが発生しました)」と表示される。
CSCwe40577	API リソース要求の処理に失敗する：条件の変換に失敗する。
CSCwd16657	Cisco ISE の任意のファイルのダウンロードの脆弱性。
CSCwfl0004	ISE の IP SGT スタティックマッピングを別のマッピンググループに移動するときこのマッピングが SXP ドメインに送信されない。
CSCwc75572	プライマリ管理ノードのアプリケーションサーバーが初期化段階でスタックしたままになる。
CSCvv90394	Cisco ISE リリース 2.6 パッチ 7 は、許可ポリシーの「identityaccessrestricted equals true」と一致しない。
CSCwel1676	Cisco ISE ダッシュボード [TC-NACの脅威 (Threat for TC-NAC)] の [侵害を受けたエンドポイントの総数 (Total Compromised Endpoints)] にアクセスすると、データが失われる。
CSCwel3780	Cisco ISE は REST API によってノードを AD に参加できない。
CSCwd45843	Cisco ISE のガベージコレクション アクティビティによるポリシー評価の認証ステップの遅延。
CSCwd78028	Cisco ISE : Apache TomCat の脆弱性 CVE-2022-25762。
CSCwc74206	Cisco ISE 3.0 で SCCM MDM サーバーオブジェクトが新しいパスワードで保存されないが、新しいインスタンスの使用時は機能する。
CSCwe07406	Cisco ISE の自己登録ゲストポータルでゲストアカウントを作成すると、「Error Loading page (ページのロード中にエラーが発生しました)」エラーが出力される。
CSCwc38610	MDM API V3 証明書文字列で大文字と小文字が区別されないようにする。
CSCwc44614	[ネットワークデバイス (Network Devices)] の [選択したものをエクスポート (Export Selected)] を使用すると、さらに多くの選択肢が含まれるログイン画面が表示される。
CSCwc24589	Cisco ISE リリース 3.1 で Cisco ISE リリース 3.2 URT が「Failed (Import into cloned database failed) (クローンデータベースへのインポートに失敗しました)」で失敗する。
CSCwe92624	Cisco ISE アフリカまたはカイロのタイムゾーン DST。
CSCwd26845	Cisco ISE リリース 3.2 の APIC 統合に fvIP サブスクリプションがない。
CSCwc70197	Cisco ISE 証明書 API は、フレンドリ名フィールドにハッシュ文字を含む信頼できる証明書を返すことができない。

問題 ID 番号	説明
CSCwe12618	Cisco ISE リリース 3.2 の APIC 統合が EP の null の取得に失敗する (com.cisco.cpm.apic.ConfImporter:521)。
CSCwc98828	Cisco ISE インターフェイス機能の不十分なアクセス制御の脆弱性。
CSCwc98824	Cisco ISE でポスチャ要件はデフォルトエントリのみを表示する。
CSCwe41824	Cisco ISE リリース 3.2 には、PKI ベースの SFTP のセカンダリポリシー管理ノードキーがない。
CSCvo61351	Cisco ISE ライブセッションが「認証済み」状態でスタックする。
CSCwc88848	Cisco ISE リリース 3.1 パッチ 1 で Rest ID または ROPC フォルダログが作成されない。
CSCvy69539	CIAM : openjdk - 複数のバージョン。
CSCwc57240	カスタム属性の追加中に Cisco ISE GUI でデフォルト値が検証されない。
CSCvy88380	Cisco ISE GUI で既存の証明書の ISE メッセージングの使用状況を選択できない (グレー表示される)。
CSCwf05309	Cisco ISE SAML 証明書が他のノードに複製されない。
CSCwe94012	Cisco ISE で特殊文字を含むパスワードを使用すると、Evaluate Configuration Validator がスタックする。
CSCwa52678	Cisco ISE GUI TCP DUMP が「Stop_In_Progress」状態でスタックする。
CSCwc62716	IndexRebuild.sql スクリプトが Cisco ISE のモニタリングノードで実行された。
CSCwd63661	Cisco ISE GUI に誤ったパスワードを入力すると、Cisco ISE リリース 3.1 パッチ 1 のエンドユーザー契約が表示される。
CSCwc65802	Cisco ISE GUI で SAML 構成の保存ボタンがグレー表示される。
CSCwe17953	Cisco ISE パストラバーサル脆弱性。
CSCwe17338	AWS 経由で展開する場合、Cisco ISE のホスト名は 19 文字以下にする必要がある。
CSCwc65711	MAC : CSC 5.0554 Web 展開パッケージのアップロードに失敗した。
CSCwc62415	Cisco ISE の不正なファイルアクセスの脆弱性。
CSCwe43468	VN 参照を使用したスタティック IP-SGT マッピングにより、Cisco DNA Center グループベースのポリシーの同期が失敗する。
CSCwd71496	Cisco ISE が SXP マッピングテーブルからすべてのセッションを削除しない。
CSCvv10712	トランザクションテーブルは、200 万レコードカウント後に切り捨てる必要がある。

問題 ID 番号	説明
CSCwc62413	Cisco ISE のクロスサイト スクリプティングの脆弱性。
CSCwc13859	Cisco ISE の「System Admin」管理者グループの管理者ユーザーで、スケジュールされたバックアップを作成できない。
CSCwf26226	EP 消去呼び出しに伴うメモリリークによる CPU スパイク。
CSCwf40128	CiscoSSL ルールに則った KU 目的の検証なしでクライアント証明書を受け入れる。
CSCwc20314	Cisco ISE-PIC リリース 3.1 での PIC ライセンスの消費。
CSCwe00424	Cisco ISE : NAS-Port-ID の長さが原因で収集失敗アラームに SQLException が送信される。
CSCwc98833	Cisco ISE のクロスサイト スクリプティングの脆弱性。
CSCwc98831	Cisco ISE の保存されたクロスサイト スクリプティングの脆弱性。
CSCwe86494	Cisco ISE で特定の URL を使用すると、Tomcat スタックトレースが表示される。
CSCwd97582	Cisco ISE リリース 3.1 パッチ 5 で CA 証明書 EKU を検証すると「unsupported certificate」エラーが発生する。
CSCwe37041	元のプライマリ管理ノードが削除されると、内部 CA 証明書チェーンが無効になる。
CSCwe52461	Cisco ISE リリース 3.1 でファイアウォール条件を有効にできない。
CSCwa82521	Cisco ISE リリース 3.1 の [信頼できる証明書 (Trusted Certificates)] メニューに問題がある。
CSCwd41098	pxGrid の無効化後に ise-psc.log で pxGrid のエラーログが記録される。
CSCwd24286	Cisco ISE が Cisco DNA Center にホスト名属性を送信していない。
CSCwd74898	「Posture Configuration detection」アラームは「INFO」レベルであり、言い回しを変更する必要がある。
CSCwe36788	Cisco ISE リリース 3.2 では、ユーザーは IP アクセスルールの追加中に追加されたルールを削除できない。
CSCwc81729	フィルタ処理で特定の 1 つのネットワーク アクセス デバイスを削除しようとする、と、「すべてのデバイスが正常に削除されました (All devices were successfully deleted)」エラーが表示される。
CSCwd74560	Cisco DNA Center を介した Cisco ISE (ERS) へのペイロードで PUT 操作が失敗する。
CSCwc42712	Cisco ISE RADIUS および PassiveID セッションのマージ。
CSCwd15888	Cisco ISE ERS API で時刻設定構成のエクスポートにアクセスできない。

問題 ID 番号	説明
CSCwc15013	有用性を追加し、Cisco ISE リリース 3.0 の「プールが枯渇しているためリソースを取得できませんでした (Could not get a resource since the pool is exhausted)」エラーを修正する。
CSCwf26482	Cisco ISE リリース 3.1 から Cisco ISE リリース 3.2 にアップグレードした後、REST AUTH サービスが実行されない。
CSCwe37018	Cisco ISE 信頼ストアに無効な証明書がある場合、Cisco ISE の Cisco DNA Center との統合が失敗する。
CSCwd05040	展開への登録後にセカンダリノードに証明書をインポートできない。
CSCwd31405	Session.PostureStatus のクエリ中に遅延が発生する。
CSCwe36242	TACACS コマンド アカウンティング レポートのエクスポートが機能しない。
CSCwe15576	KRON ジョブを設定できない。
CSCwb18744	説明に複数のバックスラッシュ文字が連続して含まれる SG とコントラクトは、Cisco ISE に同期できない。
CSCwe70975	Cisco ISE では、SMS JavaScript のカスタマイズが SMS 電子メールゲートウェイで機能しない。
CSCwc85867	Cisco ISE の変更構成監査レポートに、SGT の作成および削除イベントが明確に表示されない。
CSCwc66841	CIAM : openjdk - 複数のバージョン。
CSCwd51409	Cisco ISE は Tenable Security Center のリポジトリとスキャンポリシーを取得できない。
CSCwd79921	Cisco ISE の任意のファイルのダウンロードの脆弱性。
CSCwd13555	Cisco ISE がサードパーティの syslog サーバーからの passive-id セッションの使用を突然停止する。
CSCwe13110	Cisco ISE リリース 3.1 の設定バックアップは、プライマリ モニタリング ノードで実行される。
CSCwd70658	「There is an overlapping IP Address in your device (デバイスに重複する IP アドレスがあります)」というエラーにより、ネットワーク アクセス デバイスを追加できない。
CSCwd63717	PKI 対応の SFTP リポジトリが Cisco ISE リリース 3.2 で機能しない。
CSCwe45245	スマートライセンスの登録が機能していない。
CSCwe99961	ドイツのスポンサードポータル - カレンダーに木曜日 (Donnerstag) が Di not Do と表示される。
CSCwf23981	Cisco ISE 認証プロファイルに誤ったセキュリティグループまたは VN 値が表示される。

問題 ID 番号	説明
CSCwd73282	Cisco ISE リリース 3.1 パッチ 3 で、スポンサーポータル：セッション Cookie の SameSite 値が none に設定される。
CSCwc80243	リポジトリが選択されていない場合、Cisco ISE TCP DUMP がエラー「COPY_REPO_FAILED」状態でスタックする。
CSCwe54318	バインディングのクエリでの H2 DB の遅延が原因で、SXP サービスが初期化中にスタックする。
CSCwc23593	LSD によって CPU 使用率が高くなる。
CSCwf09674	登録済みエンドポイントレポートに、未登録のゲストデバイスが表示される。
CSCwc93451	プロファイラは、デフォルトの RADIUS プロブからのメッセージの転送中に否定的な RADIUS Syslog メッセージを無視する必要がある。
CSCwc85546	Cisco ISE リリース 3.1 で、エラー「Illegal hex characters in Escape (%) pattern ? For input string: ^F」が表示される。
CSCwf40861	Cisco ISE GUI に、コマンドセット内の文字の HTML 16 進数コードが表示される。
CSCwf36285	[SXP ドメインフィルタの管理 (Manage SXP Domain filters)] の行には、最大 25 しか表示されない。
CSCwe53550	Cisco ISE および CVE-2023-24998。
CSCwe30235	jszip 3.0.0 の脆弱性。
CSCwf44942	最大ユーザーセッション認証フロー中に Cisco ISE TACACS プライマリサービスノードがクラッシュした。
CSCwc80844	Cisco ISE VMSA-2022-0024 : VMware ツールの更新は、ローカル権限昇格の脆弱性に対処する。
CSCwe84210	LicenseConsumptionUtil.java の NullPointerException が原因で、認証ポリシーの評価が失敗する。
CSCwd10864	Cisco ISE XML 外部エンティティ インジェクションの脆弱性。
CSCwe36063	[事前調整 (Advanced Tuning)] ページで PBIS 登録キー設定が検証されない。
CSCwe25138	ユーザーのカスタム属性に \$ または ++ が含まれている場合、アイデンティティユーザーを作成できない。
CSCwd13425	Cisco ISE GUI からのパッチのインストールが失敗する。
CSCwe69189	LSD により、帯域幅の使用率が高くなる。
CSCwd98296	ネットワークデバイスのポート条件：IP アドレスまたはデバイスグループに有効なポート文字列を入力できない。

問題 ID 番号	説明
CSCwc36987	Cisco ISE BETA 証明書が古い証明書として表示され、クリーンアップする必要がある。
CSCwd31414	[訪問の理由 (Reason for Visit)] フィールドに特殊文字が含まれていると、[ゲストポータル (Guest portal)] ページで「Error Loading Page (ページのロード中にエラーが発生しました)」が表示される。
CSCwd39056	Cisco ISE リリース 3.1 パッチ 4 のパッシブ DC 設定でユーザー名が正しく保存されない。
CSCwd45783	P-PIC がダウンしている間に FMC を再統合すると、pxGrid セッションのパブリッシュが停止する。
CSCwf21960	アップグレード中、登録解除コールでデータベースからのすべてのノードの削除に失敗する。
CSCwd82119	Cisco ISE リリース 3.1 で ECDSA 証明書を使用した EAP-TLS 認証が失敗する。
CSCwc53895	Cisco ISE リリース 3.1 パッチ 3 では、アクティブなポリシーサービスノードがダウンした場合、SAML SSO は機能しない。
CSCwe61215	16 文字を超えるパスワードが設定されている場合、CLI を介した SFTP および FTP 検証が失敗する。
CSCvz08319	eapTLS のバッファ長が 0 であるため、Cisco ISE のアプリケーション サーバー プロセスが Dot1X 時に再起動する。
CSCwc99178	アクティブセッションのアラーム設定で多数の認証プロファイルを追加できない。
CSCwd10997	ノードの syncup が、ポータルロールでワイルドカード証明書の複製に失敗する。
CSCwe63873	Qualys アダプタがナレッジベースをダウンロードできない。「knowledge download in progress (ナレッジのダウンロードが進行中)」エラーでスタックする。
CSCwc65821	Cisco ISE ERS API で、「ネットワーク デバイス グループ」名にマイナス文字を使用できない。
CSCwd12453	Cisco ISE リリース 3.1 ポータルタグには、特殊文字の検証に関する問題がある。
CSCwa37580	Cisco ISE リリース 3.0 の NFS 共有がスタックする。
CSCwe53921	RADIUS 属性の長さを超える場合の AD グループ属性の連結のサポート。
CSCwc44622	セッションは、Cisco ISE が再起動されるまで無期限にスタックする。
CSCwd84055	Cisco ISE リリース 3.1 で MDM API V3 の Azure AD 自動検出が正しくない。
CSCwe92177	Cisco ISE では、メキシコのタイムゾーンが誤って夏時間に変更される。
CSCwd68070	SAML メタデータのインポートが失敗する。

問題 ID 番号	説明
CSCwe71804	Cisco ISE リリース 3.1 で、サードパーティのネットワーク デバイス プロファイルが使用されている場合、SessionCache に特定のキー属性が欠落している。
CSCwc76720	Cisco ISE リリース 3.1 では、SNMPv3 プライバシーパスワードを使用するとエラーが表示される。
CSCvx15522	FQDN syslog ポップアップの DNSCache 有効化コマンドを修正する必要がある。
CSCwc99664	macOS 12.6 のサポート。
CSCwe71729	Cisco ISE リリース 3.2 では、Data Connect 機能が無効になっている場合でも、Data Connect パスワードの有効期限アラームが常に表示される。
CSCwd57978	NDG の場所と IP アドレスに基づいてフィルタリングすると、すべてのネットワーク アクセス デバイスが削除される。
CSCwe39781	CoA 後に SGT が変更されると、Cisco ISE は SXP マッピングを削除しない。
CSCwc64480	ゲストポータルに新しい証明書がインポートされると、Cisco ISE はセキュアな接続を確立できない。
CSCwd38137	Cisco ISE XML 外部エンティティ インジェクションの脆弱性。
CSCwf28229	VLAN 検出間隔を 30 秒以下にする必要がある。
CSCwc26482	展開にレプリケーションの問題がある場合、プライマリ管理ノードの Replogns テーブルスペースが増加する。
CSCwfl9039	エージェントレスポスタの失敗により、Cisco ISE リリース 3.1 パッチ 5 で TMP フォルダのサイズが増加する。
CSCwd57752	DB 接続の寿命は長くなり、最大 DB 接続は Cisco ISE リリース 3.1 パッチ 5 では 994 である。
CSCwe44750	フィールドの増分更新後、再プロファイリングの結果が Oracle/VCS に更新されない。
CSCwd54844	ネットワーク デバイス グループ作成のための Cisco ISE ERS API スキーマ。
CSCwe49183	署名付き認証要求の Cisco ISE SAML 宛先属性がない。
CSCwd39746	MS が ADAL を廃止しているため、SCCM と Cisco ISE の統合に MSAL のサポートが必要。
CSCwc87670	Cisco ISE リリース 3.1 パッチ 3 では、SAML が使用されている場合、ユーザーは csv ファイルからエンドポイントをインポートできない。
CSCwd82134	Cisco ISE で不正な SLR コンプライアンス違反エラーが報告される。
CSCwe80760	パラメータに二重引用符 ("") が含まれている場合、プログラム起動修復を保存できない。
CSCwd64649	内部 CA 証明書の増加による Cisco DNA Center 統合の問題。

問題 ID 番号	説明
CSCwd69072	ユーザー定義 NAD プロファイルを使用した Cisco NAD でのセッションディレクトリ書き込み失敗アラーム。
CSCvz86446	Cisco ISE レプリケーション中に SyncRequest タイムアウト モニター スレッドがタイムアウト後もファイル転送を終了しない。
CSCwc55529	証明書の秘密キーが見つからないため、認証に失敗する。
CSCwc07082	csv ファイルからユーザーをインポートしようとすると、「電話番号が無効です (The phone number is invalid)」エラーが表示される。
CSCwe37826	ポスチャポリシー条件で条件演算子を AND から OR に変更できない。
CSCwe34566	ROPC ID ストアに対する認証が RSA キー生成エラーで失敗する。
CSCwf22816	誤った条件評価が原因で認証ポリシーが失敗した。
CSCwc91923	Cisco ISE GUI から AnyConnect エージェントをアップロードすると、プライマリ管理ノードで CPU 使用率が高くなり、完了までに 7 時間近くかかった。
CSCvw59025	ログとレポートに PassiveID のスペルミスエラーが表示される。
CSCwc60997	Cisco ISE でトークンの処理が正しくないため、ロードバランサを使用した SAML フローが失敗する。
CSCwc49580	適応型ネットワーク制御 (ANC) CoA がデバイス IP アドレスではなく NAS IP アドレスに送信される。
CSCwe87660	Cisco ISE リリース 3.1 では、以前のバージョンのホットパッチが引き続き DB に表示される。
CSCwe49504	Cisco ISE リリース 3.2 の identity-store コンフィギュレーション コマンドで、16 文字を超えるパスワードはサポートされない。
CSCwb72948	Cisco ISE リリース 3.0 パッチ 4 で登録済みノードのシステム証明書ページにアクセスできない。
CSCwf32255	Cisco ISE リリース 3.2 パッチ 2 で「snmp-server host」が設定されている場合、SNMP サーバーから応答を受信しない。
CSCwe96739	TLS 1.0/1.1 は、Cisco ISE リリース 3.0 管理者ポータルで受け入れられる。
CSCwe98676	ZAP の実行中に脆弱な JS ライブラリの問題が見つかった。
CSCwe39262	パッシブ ID エージェントが誤った時刻形式のイベントを送信する。
CSCwf15130	collector.log ファイルの権限が、自動的に root に設定される。
CSCwe30606	Cisco ISE GUI から 1GB を超えるサイズのサポートバンドルをダウンロードできない。

問題 ID 番号	説明
CSCvv99093	Cisco ISE ノードが断続的にキューリンクアラームをトリガーする。
CSCwd61906	Sysaux テーブルスペースの割り当ては、ノードのプロファイルに基づいて行う必要がある。
CSCwf16165	15 文字を超える NTP 認証キーで「% ERROR: Bad hashed key」エラーが発生する。
CSCwc98823	Cisco ISE のコマンドインジェクションの脆弱性。
CSCwf19463	Conditions Studio でのドラッグ アンド ドロップ アクションの階層化。
CSCwc03220	Cisco ISE から IP アクセスリストを削除すると、分散展開が破棄される。
CSCwe59587	日本語の Cisco ISE GUI で、一部の項目に「Test」と表示される。

未解決の不具合

Cisco ISE 3.3 リリースの未解決の不具合：累積パッチ 4

問題 ID 番号	説明
CSCwn34778	MDM 属性があるにもかかわらず、認証セッションが MDM ポリシーに一致しない

Cisco ISE リリース 3.3 - 累積パッチ 3 の未解決の不具合

問題 ID 番号	説明
CSCwf79582	AD クレデンシャルで Cisco ISE と Cisco Catalyst Center 2.2.1.x 以降を統合できない。
CSCwk67747	RADIUS プロトコルスプーフィングの脆弱性 (Blast- RADIUS)。
CSCwk79546	Cisco ISE 3.3 パッチ 3 でライブログに「22076 MFA 認証失敗」というメッセージが表示されて、Duo MFA 認証が即座に失敗する。 この問題を修正するには、ホットパッチ HP_3.3P3.zip をインストールする必要があります。

Cisco ISE リリース 3.3 - 累積パッチ 2 の未解決の不具合

問題 ID 番号	説明
CSCwf36985	認証ポリシーの評価中に AD グループの取得に失敗する。

問題 ID 番号	説明
CSCwh25160	スワップクリーンアップスクリプトがスワップ領域をドロップし、cron をプログラムする。
CSCwh69267	Adeos の復元後、アプリケーションサーバーが初期化中にスタックする。
CSCwh92366	Cisco ISE 3.1 パッチ 8 の寿命設定で、仮想マシンリソース不足のアラームが発生する。
CSCwi61950	Cisco ISE でコンテキスト N が不足している。
CSCwi89725	PAN の消去ルーティンで消去中のみ、DB からエンドポイントを受け入れるように PAN を作成。
CSCwj12359	「show tech-support」の実行を中断すると、Cisco ISE でサービスが停止する。
CSCwj38688	プロファイラの Null ポインタ例外により、アイデンティティグループでホストが検出されない。
CSCwj44649	Cisco ISE 3.3 で TACACS データが保持されず、すべてが消去される。

Cisco ISE リリース 3.3 の未解決の不具合：累積パッチ 1

問題 ID 番号	説明
CSCwe92640	Cisco ISE リリース 3.1 および 3.2：CLI 設定時に既存のルートの検証が行われない。
CSCwf55795	Cisco ISE リリース 3.2 パッチ 1 で、ADE-OS を使用した設定の復元後、Cisco ISE GUI および CLI にアクセスできない。
CSCwh92366	3.1 パッチ 8：3.1 パッチ 8 の寿命設定で、不十分な仮想マシンリソースのアラームが発生。

Cisco ISE リリース 3.3 の未解決の不具合

次の表は、リリース 3.3 で未解決の不具合のリストです。

問題 ID 番号	説明
CSCwf78050	下位モデル 3615/3715 でログ分析を有効にすると、Cisco ISE が応答しなくなる可能性がある。
CSCwf02597	Cisco ISE リリース 3.3：Cisco ISE 上の ML：クロックの差が 5 分を超える場合、Cisco ISE クラスタは ML クラウドに接続できない。
CSCwf49520	Cisco ISE リリース 3.3：ML 提案ルールのラベル付けに、特殊文字と重複に関する問題がある。

問題 ID 番号	説明
CSCwf76160	MFC プロファイラで、grafana ダッシュボードのすべてのメトリックに対して「No data（データなし）」と表示される。
CSCwf69829	Cisco ISE リリース 3.3 : Wi-Fi 分析の場合、MFC_EPTType が iPhone の電話として表示されない。
CSCwf14365	ログ分析ページを参照すると、「Configuration Missing」という警告が表示される。
CSCwh36667	Cisco ISE モニタリング GUI ページが「Welcome to Grafana」のままになる。
CSCwh08408	Cisco ISE リリース 3.3 では、ノードエクスポートのパスワードが見つからないため、アップグレード後の展開に新しいノードを登録できない。
CSCwh92366	3.1 パッチ 8 : 3.1 パッチ 8 の寿命設定で、不十分な仮想マシンリソースのアラームが発生
CSCwm05210	ISE 9060/ers/config/endpoint/{MAC address}/releaserejectedendpoint の送信時に「500 内部エラー」が発生する。

その他の参考資料

Cisco ISE を使用するときには活用できるその他のリソースについては、『[Cisco ISE End-User Resources](#)』[英語]を参照してください。

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](#) [英語] 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](#) [英語] 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 DevNet](#) [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) [英語] 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。

シスコのバグ検索ツール

[シスコのバグ検索ツール](#) (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シスコバグ追跡システムへのゲートウェイです。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。

マニュアルに関するフィードバック

シスコの技術マニュアルに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

【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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.

翻訳について

このドキュメントは、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。