Cisco Identity Services Engine リリース 3.3 リリースノート

初版：2023 年 7 月 5 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セキュアなネットワーク サーバー アプライアンス、仮想マシン（VM）、または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 Ordering Guide』[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 Administrator Guide』の「Monitoring and Troubleshooting Cisco ISE」のセクション [英語] を参照してください。

Cisco ISE リリース 3.3 の新機能

このセクションでは、Cisco ISE 3.3 の新機能と変更された機能をすべて示します。

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 呼び出し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、MnT REST、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 ISE Administration Guide, Release 3.3』の「Asset Visibility」の章にある「Cisco AI-ML Rule Proposals for Endpoint Profiling」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 ISE Administrator Guide, Release 3.3』の「Deployment」の章にある「Data Replication from Primary to Secondary Cisco ISE Nodes」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」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」の章の「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、[ネットワークアクセスユーザー（Network Access Users）] ウィンドウの [ネットワークアクセスユーザー（Network Access User）] テーブルに [作成日（Date Created）] 列と [変更日（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」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）を取得します。

詳細については、『Cisco ISE Administration Guide, Release 3.3』の「Asset Visibility」の章にある「Multi-Factor Classification for Enhanced Endpoint Visibility」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**
- **ポリシー**
- **管理（Administration）**
- **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」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。[TLS_RSA_With_AES_128_CBC_SHAのみを許可（Allow Only TLS_RSA_WITH_AES_128_CBC_SHA）] オプションが選択されている場合、このリストのこの SHA1 暗号方式のみが有効になります。[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 ISE Administration Guide, Release 3.3』の「Asset Visibility」の章にある「pxGrid Direct」「」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 ISE Administration Guide, Release 3.3』の「Maintain and Monitor」の章にある「Log Analytics」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 ISE Administration Guide, Release 3.3』の「Basic Setup」の章にある「Schedule Application Restart After Admin Certificate Renewal」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」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 ISE Administrator Guide, Release 3.3』の「Asset Visibility」の章にある「Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller」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』[英語] 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
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

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 以降および ESXi 7.*x* の VMware バージョン 14 以降。
  - ISO ファイルは ESXi 6.7 以降のリリース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。

- Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V
- QEMU 2.12.0-99 上の KVM
- 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
- Oracle Cloud Infrastrucure（OCI）

（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 とも呼ばれます。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。

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、次のブラウザで検証済みです。

- Mozilla Firefox バージョン 113 および 114
- Google Chrome バージョン 112 および 114
- Microsoft Edge バージョン 112

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。

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 [1]	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 [2]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019 [3]	Windows Server 2019
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
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	最新
Oracle Access Manager（OAM）	バージョン 11.1.2.2.0

外部 ID ソース	バージョン
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	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
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 には最大 200 のドメインコントローラのみを追加できます。制限を超えると、次のエラーが表示されます：

`<DC FQDN> の作成エラー：許可される DC の数が最大数 200 を超えています（Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200）`

[2] 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。

[3] Cisco ISE 2.6 パッチ 4 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。

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

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 1.1.1t および Cisco SSL 7.3.265 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。

アップグレード情報

（注） 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。

Cisco ISE リリース 3.3 には、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 以前のパッチ）と同等な機能があります。

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 [英語] から入手できます。

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 [英語] 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』[英語] を参照してください。

Cisco ISE と Cisco Digital Network Architecture Center との統合

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

Cisco ISE と Cisco DNA Center との互換性については、『Cisco SD-Access Compatibility Matrix』[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 [英語] 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） Cisco ISE 3.1 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。

警告

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

（注） 「未解決の不具合」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。

BST は Bug Toolkit の後継オンラインツールであり、ネットワークリスク管理およびデバイスのトラブルシューティングにおいて効率性を向上させるように設計されています。製品、リリース、またはキーワードに基づいてソフトウェアのバグを検索し、バグの詳細、製品、バー

ジョンなどの主要データを集約することができます。ツールの詳細については、http://www.cisco.com/web/applicat/cbsshelp/help.html のヘルプページ [英語] を参照してください。

Cisco ISE リリース 3.3 の解決済みの不具合

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。

不具合 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。
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。

不具合 ID 番号	説明
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 Giganet 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。
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。

不具合 ID 番号	説明
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。
CSCwe54466	Cisco ISE のスポンサーポータルの印刷の問題により、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サーバー順序（RADIUS server sequence）] ページに「no data available（使用可能なデータがありません）」と表示される。
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。

不具合 ID 番号	説明
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。
CSCwe92640	Cisco ISE リリース 3.1 および 3.2 では、CLI 設定時に既存のルートの検証が行われない。
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。
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。

不具合 ID 番号	説明
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。

不具合 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 tterrors.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。
CSCwc91917	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。
CSCwc85920	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。

不具合 ID 番号	説明
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。
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。
CSCwc74531	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。
CSCwc48311	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 ー 40% 低下する。

不具合 ID 番号	説明
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と、後続のすべての RADIUS/TACACS+ 認証が失敗する。
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。
CSCwf10004	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にこのマッピングが 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。
CSCwe11676	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。
CSCwe13780	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。
CSCwe38610	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。

不具合 ID 番号	説明
CSCwe24589	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。
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。
CSCwe44886	Cisco ISE リリース 2.7 パッチ 8 により、CLI からの読み取りテスト速度が低下し、「Insufficient Virtual Machine Resources」エラーが発生する。
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。

不具合 ID 番号	説明
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 パストラバーサルの脆弱性。
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 ウェブ展開パッケージのアップロードに失敗する。
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。
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。

不具合 ID 番号	説明
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。
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。

不具合 ID 番号	説明
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。
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 プロー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。

不具合 ID 番号	説明
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。
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。

不具合 ID 番号	説明
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 DB 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。

不具合 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。
CSCwf19039	エージェントレスポスチャの失敗により、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。

不具合 ID 番号	説明
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。
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。

不具合 ID 番号	説明
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。
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。

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。

不具合 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。
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。

不具合 ID 番号	説明
CSCwf69829	Cisco ISE リリース 3.3：Wi-Fi 分析の場合、MFC_EPType 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、ノードエクスポータ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。

その他の参考資料

次のリンクには、Cisco ISE で作業するときに使用できる追加のリソースが含まれています。
https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

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、シスコサービスにアクセスしてください。
- サービス リクエストを送信するには、シスコサポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet 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 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

シスコのテクニカルドキュメント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。

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。