Cisco Identity Services Engine リリース 3.4 リリースノート

最終更新：2025 年 4 月 25 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 3.4 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 3.4 - 累積パッチ 1 の新機能

将来の Cisco Identity Services Engine（ISE）リリースおよびパッチでのお客様のライセンスの使用は、Cisco ISE のライセンス階層に合わせて調整されます。ライセンス階層を確認して、コンプライアンスを確保します。

参加ポイントの専用リソースの割り当て

Cisco ISE リリース 3.4 パッチ 1、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 3.4』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。

pxGrid Direct を使用したディクショナリ属性の認可変更（CoA）

Cisco ISE リリース 3.4 パッチ 1 以降では、pxGrid ダイレクトを使用したディクショナリ属性の認可変更（CoA）を有効にできます。CoA 対応ディクショナリ属性の値が変更されると、影響を受けるエンドポイントで CoA **ポートバウンス**または**再認証**が実行されます。詳細については、『Cisco ISE Administrator Guide, Release 3.4』の「Asset Visibility」 にある「Change of Authorization (CoA) for dictionary attributes using pxGrid Direct」を参照してください。

Cisco pxGrid Cloud の新しいリージョンのサポート

Cisco pxGrid Cloud は、米国に加えてヨーロッパ、アジア太平洋、および日本でサポートされるようになりました。詳細については、『pxGrid Cloud Solution Guide』および『pxGrid Cloud Onboarding Guide』を参照してください。

ダイナミック再認証スケジューラ

Cisco ISE リリース 3.4 パッチ 1 リリース以降では、各セッションに事前に定義された有効期限の日時を設定することでアクセス制御を強化できます。これにより、指定された有効期限の間のみセッションがアクティブになるため、不正アクセスを防止できます。

詳細については、『Cisco Identity Services Engine Admin Guide, Release 3.4』の「Segmentation」の章にある「Dynamic Reauthorization Scheduler」を参照してください。

FIPS モードでの PAP/ASCII の有効化

Cisco ISE リリース 3.4 パッチ 1 以降、Cisco ISE では FIPS モードで PAP/ASCII プロトコルを設定できます。FIPS モードで PAP/ASCII プロトコルをサポートするようネットワークデバイスを設定する際に、RADIUS DTLS 設定を有効にできます。

パッチのフルアップグレードおよび分割アップグレードのサポート

新しい Cisco ISE リリースを、そのリリースに対応するパッチの有無にかかわらずアップグレードできます。Cisco ISE リリースのパッチをすでにインストールしている場合は、[Patch] オプションを使用して、現在のリリースのパッチのみをアップグレードできます。

パッチのアップグレードには、フルアップグレードか分割アップグレードのオプションを選択できます。

- **フルアップグレード**：フルアップグレードは、同時に Cisco ISE 展開のすべてのノードの完全なパッチ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**：分割アップグレードは、アップグレードプロセス中にサービスを引き続き利用できるようにしながら、Cisco ISE 展開のパッチ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。

詳細については、『Cisco Identity Services Engine Upgrade Guide, Release 3.4』の「Install Latest Patch」の章にある「Software Patch Upgrade」を参照してください。

インバウンドおよびアウトバウンド SGT ドメインルール

インバウンド SGT ドメインルールを作成して、着信 SGT バインディングを特定の SGT ドメインにマップできます。ルールが定義されていない場合、ワークロードコネクタから受信したバインディングはデフォルトの SGT ドメインに送信されます。

アウトバウンド SGT ドメインルールを作成して、特定の SGT バインディングのターゲット宛先を指定できます。

詳細については、『Cisco ISE Administrator Guide, Release 3.4』の「Segmentation」の章にある「Add Inbound SGT Domain Rules」と「Add Outbound SGT Domain Rules」を参照してください。

統合カタログを使用した Cisco pxGrid Cloud アプリケーションの統合

Cisco ISE リリース 3.4 パッチ 1 以降では、Cisco ISE のネイティブ統合カタログインターフェイスを使用して Cisco pxGrid Cloud アプリケーションと統合でき、統合エクスペリエンスが簡素化されます。Cisco pxGrid Cloud アプリケーションを Cisco ISE と統合するには、[Integration Catalog] を使用します（**[Administration]** > **[System]** > **[Deployment]** > **[Integration Catalog]**）。シングルインスタンスとマルチインスタンスの両方の Cisco pxGrid Cloud アプリケーションを統合できます。詳細については、『Cisco pxGrid Cloud Solution Guide』を参照してください。

新しい pxGrid API：エンドポイントトピック

エンドポイントトピックは、Cisco ISE 管理対象ネットワークデバイスに接続されているエンドポイントへのアクセスを提供します。詳細については、『Cisco pxGrid API Guide』を参照してください。

ポータルのカスタマイズのプレビュー

[Portal Page Customization] ページで変更を加えた後、[Render Preview] をクリックしてコンテンツをプレビューする必要があります。更新されたコンテンツを表示するたびに [Refresh Preview] をクリックする必要があります。

（注） アクティブなコンテンツまたはスクリプトを使用してポータルのカスタマイズをレンダリングすると、セキュリティ上のリスクが生じる可能性があります。レンダリングの前にスクリプトを慎重に確認することを強くお勧めします。

詳細については、『Cisco ISE Administrator Guide, Release 3.4』の「Guest and Secure WiFi」の章にある「Preview Portal Customization」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 3.4 パッチ 1 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 3.4 パッチ 1 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 3.4』[英語] を参照してください。

グローバル セキュリティ グループの ACI のサポート

Cisco ISE リリース 3.4 と Cisco ISE リリース 3.4 パッチ 1 とでは、外部 EPG（EEPG）の命名規則が変更されています。Cisco ISE リリース 3.4 では、EEPG の名前は「ISE_SGT_<SGT_TAG>」という形式で、「ISE_SGT_」という固定プレフィックスの後にセキュリティグループタグ (SGT) が続きます。一方 Cisco ISE リリース 3.4 パッチ 1 では、この形式が「ISE_<SG_NAME>」に変更されます。「ISE_」が固定プレフィックスで、その後にセキュリティグループ（SG）名が続きます。

（注） 今回の更新では移行がサポートされていないため、EFT をご利用のお客様は、Cisco ISE リリース 3.4 パッチ 1 をインストールする前にアウトバウンドルールを無効にし、パッチのインストール完了後に再度有効にする必要があります。

ワークロード分類ルール

ワークロード分類ルールを使用してワークロードを分類し、プライマリおよびセカンダリ SGT をワークロードに割り当てることができます。プライマリ SGT は pxGrid セッショントピックで “Security Group” とマークされ、SXP を介して IP から SGT へのマッピングを公開するために使用されます。セカンダリ SGT は、“Secondary Security Groups” という名前の順序付き配列として pxGrid セッショントピックに含まれています。

分類ルールの実行順序を指定できます。ルールをドラッグアンドドロップして順序を変更できます。

詳細については、『Cisco ISE Administrator Guide, Release 3.4』の「Segmentation」の章にある「Add Workload Classification Rules」を参照してください。

ワークロードコネクタ

共通ポリシーは、ドメインに関係なく、一貫したアクセスポリシーとセグメンテーションポリシーを構築し、適用するためのフレームワークです。ワークロードコネクタは、このフレームワークで使用され、オンプレミスおよびクラウドのデータセンターとのセキュアな接続を構築し、アプリケーション ワークロード コンテキストをインポートし、そのコンテキストを SGT に正規化し、ポリシーを構築するために他のドメインとコンテキストを共有します。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.4』の「Segmentation」の章にある「Workload Connectors」を参照してください。

ワークロード ライブ セッション

[Workloads Live Session] ページには、ライブ ワークロード セッションに関する詳細が表示されます。このページを表示するには、Cisco ISE GUI で [Menu] アイコンをクリックし、[Operations] > [Workloads] > [Workloads Live Session] の順に選択します。

詳細については、『Cisco ISE Administrator Guide, Release 3.4』の「Segmentation」の章にある「Workloads Live Session」を参照してください。

Cisco ISE リリース 3.4 の新機能

アップグレード時の自動ログバンドル生成

Cisco ISE リリース 3.4 以降、アップグレードに固有のデバッグログのみを含むミニログバンドルは、アップグレードプロセス中に自動的に生成されます。このログバンドルはアップグレードが開始されたリポジトリにコピーされ、障害発生時のアップグレードのトラブルシューティングに使用できます。自動ログバンドル生成は、Cisco ISE の 3 つのアップグレードオプション（フルアップグレード、分割アップグレード、およびCLIを使用したアップグレード）すべてで使用できます。

詳細については、『Cisco Identity Services Engine Upgrade Guide, Release 3.4』の「Perform the Upgrade」の章を参照してください。

Cisco ISE CLI からのバックアップログの改善

backup-logs CLI コマンドが更新され、core-files、date-from、date-to、db-logs、debug-logs、local-logs、mnt-report-logs、policy-cache-logs、policy-conf-logs、および system-logs など、Cisco ISE GUI で使用可能なすべてのバックアップログオプションが含まれるようになりました。出力オプションが含まれていない場合は、すべてのバックアップログが生成されます。

この CLI コマンドの詳細については、『Cisco ISE CLI Reference Guide, Release 3.4』の「Cisco ISE CLI Commands in EXEC Mode」の章にある「backup-logs」を参照してください。

認証局診断ツール

証明書管理に関するの問題を診断するには、**application configure ise** コマンドで [CA Diagnostic Tool] オプション（オプション 37）を使用します。このツールは、特定された問題の考えられる理由と修復方法を提案します。問題の修正に役立ち、障害対応の関連ログを提供します。

詳細については、『Cisco Identity Services Engine CLI Reference Guide, Release 3.4』の「Cisco ISE CLI Commands in EXEC Mode」の章にある「Diagnose Certificate Management Related Issues」を参照してください。

Cisco ISE のレジリエンシのユースケース

Cisco ISE リリース 3.4 以降、Cisco ISE のレジリエンシを維持するために、**過剰な RADIUS ネットワークデバイス通信**アラームと**過剰なエンドポイント通信**アラームが追加されています。詳細については、『Cisco ISE Administrator Guide, Release 3.4』の「Troubleshoot」の章にある「Cisco ISE Alarms」を参照してください。

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 3.4 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 3.4』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。

URL プッシャ pxGrid Direct コネクタタイプの作成

Cisco ISE GUI および OpenAPI（REST API）を使用して、pxGrid Direct コネクタを作成できます。Cisco ISE リリース 3.4 以降では、[URL Fetcher] の pxGrid Direct コネクタタイプまたは [URL Pusher] の pxGrid Direct コネクタタイプのいずれかを選択できます。[URL Pusher] pxGrid Direct コネクタを使用すると、pxGrid Direct Push API を使用して JSON データを Cisco ISE データベースにプッシュできます。[URL Pusher] pxGrid Direct コネクタタイプを使用して、サーバーまたは CMDB なしでデータをプッシュできます。このデータは Cisco ISE データベースに残り、認証ポリシーで使用できます。

詳細については、『Cisco ISE Administrator Guide, Release 3.4』および『Cisco ISE API Reference Guide』の「Asset Visibility」の章にある「Create a URL Pusher Connector Type」を参照してください。

デバッグログの設定

各デバッグログコンポーネントに許可される最大ファイルサイズと最大ファイル数を設定できます。[Debug Level Configuration] ページに現在のディスク容量の使用率と、[Max File Size] と [File Count] に設定された値に基づいた容量の使用率の推定値を表示できます。これらの値をデフォルトにリセットする必要がある日時を指定することもできます。

詳細については、『Cisco ISE Administration Guide, Release 3.4』の「Troubleshoot」の章の「Configure Debug Log Settings」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 3.4』の「Segmentation」の章にある「Configure Security Settings」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 3.4』の「Secure Access」の章にある「Network Devices Import Template Format」の表を参照してください。

Cisco ISE リリース 3.4 の GUI の機能拡張

Cisco ISE リリース 3.4 では、ユーザー体験をより直感的にするために、Cisco ISE GUI に次の拡張機能があります。

- **エンドポイント情報へのシングルクリックアクセス**

  Cisco ISE GUI のエンドポイントの属性詳細など、[Context Visibility] ページのオブジェクトの詳細情報を、ユーザーが 1 回のクリックで使用できるようになりました。

  すべてのエンドポイント属性が 1 つのタブに表示されるようになり、使いやすさと可視性が向上しました。

  次の操作を実行できます。

  - エンドポイントの MAC アドレスをクリックすると、すべてのエンドポイント属性を 1 つのページに表示します。
  - このページの右上隅にある [See full detail] オプションをクリックすると、すべてのエンドポイントの詳細が新しいブラウザタブに表示され、共有することもできます。
  - エンドポイントの MAC アドレスの横にあるリンクアイコンをクリックすると、すべてのエンドポイント詳細のフルページビューが開きます。

  次のページが更新され、次の拡張機能が追加されました。

  - **[Context Visibility]** > **[Endpoints]**。
  - **[Work Center]** > **[Guest Access]** > **[Identities]** > **[Endpoints]**。
  - **[Work Center]** > **[BYOD]** > **[Identities]** > **[Endpoints]**。
  - **[Work Center]** > **[Network Access]** > **[Identities]** > **[Endpoints]**。
  - **[Work Center]** > **[Profiler]** > **[Endpoint Classification]**。

- 列表示のユーザー設定の保持：Cisco ISE GUI でテーブルの列表示を変更する（列幅の調整、列の表示/非表示、列の並べ替えなど）と、その設定が保持されます。

Show Version コマンドに追加されたホットパッチの詳細

show version CLI コマンドで、特定の Cisco ISE リリースのホットパッチ詳細（ある場合）が表示されるようになりました。詳細については、『Cisco ISE CLI Reference Guide, Release 3.4』の「Cisco ISE CLI Commands in EXEC Show Mode」の章にある「show version」を参照してください。

Cisco ISE GUI でホットパッチの詳細を表示するには、  アイコンをクリックし、[About ISE and Server] を選択します。

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 25）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 3.4』の「Cisco ISE CLI Commands in EXEC Mode」の章にある「Localized ISE Installation」を参照してください。

「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 3.4*』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 3.4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 3.4』の「Troubleshoot」の章の「Open TAC Support Cases」[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 3.4』の「Segmentation」章にある「Integrate Cisco Duo With Cisco ISE for Multifactor AuthenticationIntegrate Cisco Duo With Cisco ISE for Multifactor Authentication」[英語] を参照してください。

優先順位によるドメインコントローラの選択の強制

優先ドメインコントローラのフェールオーバーが発生した場合に、Cisco ISE のドメインコントローラ選択をオーバーライドすることを選択できるようになりました。これを行うには、**[Administration]** > **[Identity Management]** > **[External Identity Sources]** > **[Active Directory]** > **[Advanced Tools]** > **[Advanced Tuning]**の順に選択します。[Name] フィールドに **REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\PreferredDcAndGc\Priority\Enabled** レジストリキーを入力し、[Value] フィールドに **1** を入力します。これにより、ドメインコントローラのフェールオーバーの発生時に、Cisco ISE は既存の優先順位値をオーバーライドし、左から右への入力順序で優先リスト内の次のドメインコントローラを選択します。このレジストリキーの値は、デフォルトで **0** に設定されています。

REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\PreferredDcAndGc\Priority\Enabled レジストリキーが有効になっている場合は、フェールバック間隔（秒単位）を設定することもできます。フェールバック間隔の値は 60 ～ 86400 です。デフォルトのフェールバック間隔は 180 秒です。

（注） この機能は、ドメインコントローラが設定された直接ドメインに対してのみ機能し、信頼関係ドメインに対しては機能しません。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.4』の「Asset Visibility」の章にある「Active Directory Advanced Tuning」を参照してください。

TrustSec 統合用の PAC なしの RADIUS 通信

Cisco ISE リリース 3.4 以降、TrustSec 統合用の PAC なしの RADIUS 通信をサポートします。この PAC なしを適用すると、PAC ベースの RADIUS 認証が置き換えられ（サポートされている場合）、Cisco ISE と TrustSec デバイス間のセキュアな通信を保証する共有秘密を介して適用されます。この機能には、Cisco ISE での設定変更は必要ありません。展開内のネットワークデバイスでは、設定の変更が必要な場合があります。PAC なしの RADIUS 通信は、IOS-XE バージョン 17.15.1 以降のネットワークデバイスでのみサポートされます。

ユーザーごとの動的アクセス制御リストの動作変更

ユーザーごとの動的アクセス制御リスト（DACL）を使用して認証プロファイルを評価するときに、DACL が Cisco ISE 設定に存在しない場合、認証は失敗し、Cisco ISE はそのユーザーに Access-Reject 応答を送信します。この情報は、[Live Log Details] ページと [AAA Diagnostics] レポートで確認できます。Cisco ISE リリース 3.4 以降では、Cisco ISE ダッシュボードの [Alarms] ダッシュレットにも認証失敗アラームが表示されます。

詳細については、『Cisco ISE Administrator Guide, Release 3.4』の「Segmentation」の章にある「Downloadable ACLs」を参照してください。

認証ポリシーのディクショナリグループ内の配列に対する pxGrid Direct のサポート

Cisco ISE リリース 3.4 以降では、ディクショナリ属性として配列とともに pxGrid Direct コネクタのデータを使用して、認証ポリシーを設定することもできます。ポリシーの設定時には、「Contains」または「Matches」の演算子（正規表現の場合）を使用する必要があります。配列がある場合、「Equals」と「In」の演算子は機能しません。「AND」または「OR」条件を使用して、複数の属性をネストできます。詳細については、『Cisco ISE Administrator Guide, Release 3.4』の「Segmentation」の章にある「Authorization Policies」を参照してください。

pxGrid フィルタリング

Cisco ISE リリース 3.4 以降、pxGrid はクライアントの特定の要件に基づいた情報のフィルタリングをサポートします。pxGrid フィルタリング機能を使用すると、クライアントはサブスクリプションごとにパブリッシャから関連情報のみを受信できます。情報のフィルタリングは、pxGrid サーバーのフィルタリング API を使用して実現されます。詳細については、『Cisco ISE Administrator Guide, Release 3.4』の「Cisco pxGrid」の章にある「pxGrid Filtering」を参照してください。

RADIUS 抑制およびレポートの機能拡張

Cisco ISE リリース 3.4 以降、RADIUS の抑制とレポートに関する機能が拡張され、RADIUS（**[Administration]** > **[System]** > **[Settings]** > **[Protocols]** > **[RADIUS]** > **[RADIUS Settings]**）設定の運用が容易になっています。詳細については、『Cisco ISE Administrator Guide, Release 3.4』の「Segmentation」の章にある「RADIUS Settings」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

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。

複数の Cisco Application Centric Infrastructure コネクタのサポート

Cisco ISE を使用すると、複数のドメイン間で一貫したアクセスポリシーを作成して適用できます。Cisco ISE では、Cisco Application Centric Infrastructure（Cisco ACI）を使用して SGT および SGT バインディングを共有できます。また、Cisco ACI からエンドポイントグループ（EPG）、エンドポイント セキュリティ グループ（ESG）、およびエンドポイント情報を学習することもできます。Cisco ISE に複数の Cisco ACI 接続を追加できます。

Cisco ISE で学習したコンテキストを管理し、Cisco ISE コネクタと Cisco ACI コネクタ間のコンテキストフローを最適化するルールを設定できます。

Cisco ISE は、Cisco ACI マルチテナントおよび Multi-Virtual Routing and Forwarding の展開をサポートしています。複数の接続を介してマルチファブリックを定義できます。この統合では、マルチポッドおよび個々の Cisco ACI ファブリックがサポートされます。

詳細については、『Cisco ISE Administration Guide, Release 3.4』の「Segmentation」の章にある「Connect Cisco Application Centric Infrastructure with Cisco ISE」を参照してください。

（注） 複数の Cisco Application Infrastructure（Cisco ACI）コネクタに対するサポートは、制御された導入（ベータ）機能です。この機能を実稼働環境で使用する前に、テスト環境で十分にテストすることを推奨します。このベータ機能を最大限に活用するには、このホットパッチをインストールします。

Cisco ISE ワークフローの TLS 1.3 サポート

Cisco ISE リリース 3.4 では、TLS 1.3 が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 3.4 の時点では、TLS 1.3 の TEAP が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 3.4 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 3.4』の「Segmentation」の章にある「Configure Security Settings」 [英語] を参照してください。

ソフトウェア ダウンロード サイトで Cisco ISE リリース 3.4 ISO、アップグレードバンドル、および Cisco ISE-PIC 3.4 ISO ファイルが置き換えられました。

「Cisco ISE Software Download」サイトで Cisco ISE リリース 3.4 ISO、Cisco ISE リリース 3.4 アップグレードバンドル、および Cisco ISE-PIC 3.4 ISO ファイルが置き換えられました。新しいファイルのファイル名は次のとおりです。

- ise-3.4.0.608a.SPA.x86_64.iso
- ise-upgradebundle-3.1.x-3.3.x-to-3.4.0.608a.SPA.x86_64.tar.gz
- Cisco-ISE-PIC-3.4.0.608a.SPA.x86_64.iso

新しい ISO ファイルからブート可能な USB デバイスを作成するには、Rufus に加えて Fedora Media Writer および BalenaEtcher USB ツールを使用します。

新しい ISO ファイルを使用してブート可能な USB デバイスを作成する場合、次の手順は必要ありません。

- 次のファイルの「cdrom」という単語を「hd:sdb1」に置き換えます。
  - isolinux/isolinux.cfg または syslinux/syslinux.cfg
  - EFI/BOOT/grub.cfg
- ks.cfg ファイルで、「cdrom」という単語を「harddrive --partition=/dev/disk/by-label/ADEOS --dir=/」に置き換えます。

詳細については、『Cisco Identity Services Engine Installation Guide, Release 3.4』の「Additional Installation Information」の章にある「SNS Appliance Reference」を参照してください。

Cisco ISE リリース 3.4 または Cisco ISE-PIC 3.4 の以前のファイル（ise-3.4.0.608.SPA.x86_64.iso など）を使用した場合は、Cisco ISE または Cisco ISE-PIC を再インストールする必要はありません。新しいファイルには、インストールプロセスを改善するための変更のみが含まれています。

廃止された機能

レガシー IPSec（ESR）のサポート終了

Cisco ISE リリース 3.4 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 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。

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 3.4 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 3.4 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 3.4 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。

GUI の廃止

次のページは、Cisco ISE リリース 3.4 の Cisco ISE GUI から削除されました。

- Location Services（**[Administration]** > **[Network Resources]** > **[Location Services]**）。
- NAC Managers（**[Administration]** > **[Network Resources]** > **[NAC Managers]**）。

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 3.4 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）	

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。

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 3.0 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。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。

  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 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 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。

- 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 20230302.100169

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 Infrastrucure（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 3.4 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 123、124、125、および 127 以降
- Google Chrome バージョン 122、123、124、および 126 以降
- Microsoft Edge バージョン 123、124、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	

外部 ID ソース	バージョン
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 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 3.4 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。

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。

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 3.4 へのアップグレード

次の Cisco ISE リリースからリリース 3.4 に直接アップグレードできます。

- 3.1
- 3.2
- 3.3

Cisco ISE リリース 3.1 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 3.4 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。

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 Catalyst Center

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。

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 3.4 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 3.4 の解決済みの不具合：累積パッチ 1

次の表は、Cisco ISE 3.4 パッチ 1 で解決済みの不具合のリストです。

問題 ID 番号	説明
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。
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くときにデータが一致しない。
CSCwk98467	REST ID ストアがサフィックスなしで設定されている場合、Cisco ISE リリース 3.3 から Cisco ISE リリース 3.4 へのデータのアップグレードまたは復元が失敗する。
CSCwm12300	内部アイデンティティユーザー認証設定で Cisco ISE のパスワードポリシーを変更できない。
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。
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。
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。
CSCwk93711	Cybervision が Cisco ISE 統合後に DDOS getAssets コールを受信する。
CSCwj77930	pxGrid JMESPath フィルタの一括ダウンロードクライアントがタイムアウトする。
CSCwm05976	ODBC 認証用の Active Directory プローブを介して RPC コールが行われる。

問題 ID 番号	説明
CSCwm00336	ボンドが設定されている場合、システムファイル（etc/hosts）でドメイン名が更新されない。
CSCwk24032	UDP サイズ制限（長さ = 548）により、一部の Cisco ISE SRV レコードに IP がない。
CSCwk71111	バックアップの復元が 75% でスタックする。
CSCwm36268	Cisco ISE リリース 3.3 パッチ 2 では、リリース後にエンドポイントが「Rejected Endpoint」と誤って表示される。
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。
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。
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。
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。
CSCwm38826	Cisco ISE リリース 3.4 では、RADIUS パケットが誤って重複とマークされる。
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。
CSCwm59777	IP ドメイン名の検証が厳密すぎるため、有効なドメインが受け入れられない。
CSCwj44649	Cisco ISE リリース 3.3 で TACACS データが保持されず、すべてが消去される。
CSCwj82240	Cisco ISE リリース 3.2 で、Cisco ISE のセカンダリノードのカウンタレポートが空になる。
CSCwk79595	インバウンドおよびアウトバウンドの [SGT Domain Rules] ページのページレベルのヘルプが機能しない。
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。
CSCwk07454	Cisco ISE リリース 3.2 パッチ 6 では、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。
CSCwk15719	Cisco ISE プロファイラは、SNMP プロー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。

問題 ID 番号	説明
CSCwi01581	複数の VN 間のエンドポイントの再認証中に、SXP バインディングが Cisco ISE でスタックする。
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。
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。
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。
CSCwm13930	エージェントレスポスチャおよび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。
CSCwm43231	カスタムポータルファイルのプレビューが正しくロードされない。
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。
CSCwk97231	バックアップファイルが GUI 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。
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と、説明フィールドが閉じる。
CSCwm63628	Cisco ISE GUI の TrustSec ポリシーにある送信元ツリーと宛先ツリーのルールの一部が表示されない。
CSCwk91347	RADIUS DTLS 互換性のために FIPS が有効になっている場合に、PAP の有効化が許可される。
CSCwk38205	ACI 接続が削除されても、SGT が削除されない。
CSCwk55333	デバッグモードでは ise.psc.log に着信 API 要求の URI が出力されない。
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。

問題 ID 番号	説明
CSCwk74068	SXP ノードのリロード後に、SXP が欠落しているエントリを一括ダウンロードする。
CSCwm50409	ERS API エンドポイントコールの遅延。
CSCwk33597	SMNT がプライマリ PAN と同じノード上にある場合、TACACS 認可の詳細が機能しない。
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。
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。
CSCvy74903	Cisco ISE 管理に証明書ベースの認証を使用すると、IP アドレス 169.254.4.3 が表示される。
CSCwk64227	認証ポリシーの ODBC クエリが Postgres で結果を返さない。
CSCwk38245	Cisco ISE リリース 3.2 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。
CSCwm37824	提案されたプロファイルルールのダウンロードボタンで 400 エラーがスローされる。
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。
CSCwm60583	IPv6 を有効または無効にすると、sysctl.conf ファイルに複数の空白行が作成される。
CSCwm58686	Cisco ISE がセッションを常に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。
CSCwm40047	「Unable to send email」という誤解を招くエラープロンプトが表示される。
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。
CSCwk80338	CDP で Cisco ACI から Cisco ISE への複数の SGT IP バインディングが欠落する。Cisco ACI に mdpEps がある。
CSCwm02519	LSD クラスに対する追加の修正。
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。

問題 ID 番号	説明
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。
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。
CSCwj29473	Cisco ISE のフォーミュラ インジェクション
CSCwm47768	ブラウザの言語がロシア語の場合、Cisco ISE ポータルにウクライナ語が表示される。
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。
CSCwk56154	RBAC 管理者ユーザーが、静的割り当てグループなしでユーザーを追加できる。
CSCwm36039	スポンサー権限を持つ管理者アカウントで Cisco ISE リリース 3.4 GuestAPI クエリが失敗する。
CSCwm63134	Cisco ISE リリース 3.2 パッチ 6 で、MDM サーバーから 404 応答を受信した場合、Cisco ISE は断続的に MDM を照会しなくなる。
CSCwm44513	Cisco ISE 管理者アクセスの PIV/CAC 認証により、System 360 権限の問題が発生する。
CSCwm53456	Cisco ISE リリース 3.3 パッチ 2 で、証明書の詳細を取得するとエラーが発生する。
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。
CSCwm67805	CoA 再認証がスタックしているため、デバイスが登録されている場合でも、BYOD デバイスは WebAuth 保留状態になる。
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。
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。
CSCwm03837	Cisco ISE リリース 3.2 パッチ 6 のヘルスチェックの入力または出力帯域幅は、サポートされているガイドラインの範囲内であっても失敗する。
CSCwk73315	Cisco ISE 360 モニタリングダッシュボードに、レート合計でなはく平均 CPU 時間のパーセンテージが表示される。
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。

問題 ID 番号	説明
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。
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。
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正常に機能しない。
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。
CSCwj57668	アップグレード後の MFC プロファイラダッシュボードにデータが表示されない。
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。
CSCwj35581	Cisco ISE にレート制限保護がない。
CSCwk40725	ConfD が localhost:9888.access.1.1.1.1... などをエンドレスに生成する。
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。
CSCwk38327	MDM フローの正常性チェックでエラーが発生する。
CSCwm13073	SGT が 3000 未満の場合に、Cisco ISE は「This Custom View has exceeded the maximum number of SGTs (3000)」エラーをスローする。
CSCwk61938	Cisco ISE は OpenSSH CVE-2024-6387「regreSSHion」を評価する必要がある。
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。
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。
CSCwm61668	TC-NAC_Tenable が「Scan Failed: Error in connecting to host: 403 Forbidden」エラーをスローする。
CSCwk36095	pxGrid ライブログの有用性。
CSCwk33023	アプリケーションサーバーの再起動なしで pi-profiler Prometheus 設定を更新する。
CSCwk73305	Cisco ISE XDR 統合の変更をコミットするための包括的なバグ。
CSCwk57231	CDP のマルチ ACI レポートを追加するための包括的なバグ。

問題 ID 番号	説明
CSCwk47423	Cisco ISE の反射型クロスサイト スクリプティングの脆弱性。
CSCwk47454	Cisco ISE の反射型クロスサイト スクリプティングの脆弱性。
CSCwk47465	Cisco ISE XML 外部エンティティ インジェクションの脆弱性。
CSCwk47475	Cisco ISE の任意のファイルの読み取りおよび削除の脆弱性。
CSCwk47489	Cisco ISE の任意のファイルの読み取りおよび削除の脆弱性。
CSCwk59325	ダングリング LOCK_FILE が原因で、Cisco ISE サービスが初期化される。
CSCwk59449	Cisco ISE リダイレクションのバイパスが、XSS につながる可能性がある。
CSCwm07116	SMS ゲートウェイの GET 要求の場合、URL マッピングが guest.log に表示されない。
CSCwm31590	Cisco ISE リリース 3.3 パッチ 3 との FMC の統合が、Azure セッションで中断される。
CSCwm34442	Cisco ISE リリース 3.4 Active Directory 診断ツールのテストが失敗する。
CSCwn07737	CDP または CSDAC で、ワークロード分類ルールの変更後、SXP デバイスへのバインディングが送信されなくなる。
CSCwn18814	CDP で PSN のリロードまたは SXP の移動後に、データセンターへの IPv6 トラフィックの損失が発生する。
CSCwn21297	インストール時間の延長によって CI が影響を受けた。
CSCwn21374	Cisco ISE リリース 3.3 において、TCP ポート 443 で応答しないため、非同期モードのときに PAN にログインすると遅延が発生する。
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。
CSCvy74903	Cisco ISE 管理に証明書ベースの認証を使用すると、IP アドレス 169.254.4.3 が表示される。
CSCwm58017	Cisco ISE リリース 3.4 のポート 80 がリスニング状態にならない。
CSCwm65529	エンドポイントのスタティック ID グループを変更できない。

Cisco ISE リリース 3.4 の解決済みの不具合

Cisco ISE リリース 3.4 で解決済みの不具合は、Cisco ISE パッチリリース（3.3 パッチ 3、3.2 パッチ 6、3.1 パッチ 9）と同等です。

次の表は、リリース 3.4 で解決済みの不具合のリストです。

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。
CSCwf80509	Cisco ISE パッシブ ID のエージングタイムは、設定に関係なく常に 1 時間である。
CSCwf32641	Cisco ISE リリース 3.3：自動生成された SNMPv3 エンジン ID は、すべてのノードで同一になる。表示される ID は AKHGCM5MKGF になる。
CSCwi59868	スポンサーベースのゲストポータルでアカウント拡張が正しく定義されない。
CSCwh81035	Cisco ISE PAN で Cisco ISE 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。
CSCwh89520	Cisco ISE CLI のアップグレードが「Internal error during command execution」というエラーで失敗する。
CSCwj42214	Cisco ISE MnT 消去イベントの Syslog の形式が正しくない。
CSCwi59216	Cisco ISE GUI で [Contact Support] オプションをクリックすると、スポンサーポータルに「400 Bad Request」というエラーが表示される。
CSCwi18917	Cisco ISE SNMP ポーリングが、プライバシープロトコル AES 192 または AES 256 で機能しない。
CSCwf16588	2 番目の NTP 認証キーを追加すると、Cisco ISE GUI からすべての認証キーが削除される。
CSCwh84446	アカウントの有効期限通知に特殊文字が含まれている場合、ゲストタイプを保存できない。
CSCwb63834	MnT ログプロセッササービスが、他の Cisco ISE 管理ノードで実行されることがある。
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。
CSCwi58421	ポスチャリースが有効になっている場合、Cisco ISE PSN 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。
CSCwe74135	Cisco ISE リリース 3.1 パッチ 5 においてゲストポータルの削除の失敗および完全性の制約。
CSCwd28431	Cisco ISE コードからの EPS の削除。
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 TLS 暗号を使用する。
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 で検出されない。

問題 ID 番号	説明
CSCwi57950	Cisco ISE リリース 3.2 では、厳密なトランスポートセキュリティの形式が正しくない。
CSCwh95587	NFS リポジトリが、Cisco ISE リリース 3.2 の分散展開の単一ノードで突然動作を停止する。
CSCwi57812	Cisco ISE リリース 3.2 で、ポート TCP および 67 にリスニングが表示される。
CSCwf72037	Cisco ISE リリース 3.1 で管理者ログインレポートに 5 分ごとに「Administrator authentication failed」エラーが表示される。
CSCwj48359	Cisco ISE の pxGrid データベース同期テストで、「Out of Sync」というエラーが表示される。
CSCwh47601	Cisco ISE リリース 3.2 パッチ 2 および 3 で 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ーを作成できない。
CSCwj04049	LDAP 接続を使用して AD に接続する場合、Cisco ISE は AD 属性「msRASSavedFramedIPAddress」または「msRADIUSFramedIPAddress」の値を変換できない。
CSCwc64144	属性 TotalAuthenLatency と ClientLatency が、Cisco ISE の TACACS+ で機能しない。
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 アドレスをエンドポイント ID グループに追加できない。
CSCwi15914	SXP ADD 操作によってリンクローカルアドレスに IPV6 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。
CSCwf10516	Cisco ISE リリース 3.2 で、認証ポリシー機能が動作しない。
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。
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。
CSCwf80292	Cisco ISE が EAP-TLS 認証中にピア証明書を取得できない。
CSCvo60450	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	Cisco ISE で「no ip name-server」というエラーが表示され、プロンプトなしでサービスが直接再起動される。
CSCvw81130	Cisco ISE リリース 2.7 で Active Directory 診断ツールのスケジュール済みテストを無効にできない。

問題 ID 番号	説明
CSCwj84815	Cisco ISE リリース 3.3 パッチ 2 でエラー「No session available」が表示される。
CSCvv90394	Cisco ISE リリース 2.6 パッチ 7 で、認証ポリシーの「identityaccessrestricted equals true」と一致できない。
CSCwj14217	[Device Network Conditions] GUI ページがロードされない。
CSCwi61700	「iselocalstore」ログが、Cisco ISE CLI から取得したサポートバンドルログに収集されない。
CSCwh23986	pxGrid getUserGroups API 要求が空の応答を返す。
CSCwk25064	Cisco ISE PSN で SXP ロールを有効にすると、CPU の負荷と使用率が高くなる。
CSCwj06401	属性セクションに null のキーと値のペアがあるエンドポイントによってパージフローが中断される。
CSCwh61339	[Network Devices] ページの [Export All] オプションを使用して 90,000 を超えるネットワークデバイスをエクスポートすると、Cisco ISE がタイムアウトする。
CSCwf47838	コマンドセットが CSV ファイルとしてエクスポートされた後、コマンド引数のスペース「 」文字がスラッシュ「/」文字に置き換えられる。
CSCwi60778	エンドポイントが再認証後にスタティック ID グループの割り当てを失う。
CSCwj91517	Cisco ISE の起動時に unbound-anchor を無効にする必要がある。
CSCwi18005	Cisco ISE 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。
CSCwh24754	スポンサーグループにマッピングされる AD グループの数が多すぎるため、スポンサーログインで遅延が発生する
CSCwh70275	以前に展開に登録されたノードの登録中に、その展開のすべての証明書が削除され、展開内のすべてのノードが再起動される現象が確認された。
CSCwi05445	Cisco ISE リリース 3.1 パッチ 7 で Cisco ISE GUI からサポートバンドルを削除できない。
CSCwk14636	Cisco ISE リリース 3.2 パッチ 6 において AWS 上で仮想マシンリソース不足アラームの問題が発生する。
CSCwi59555	Cisco ISE 3.2 パッチ 4 でフォーマット内の MAC アドレスの検索が無視される。
CSCwd49321	Cisco ISE で 2 つのノードで pxGrid が有効になっている場合、統合が失敗し、「pxGrid not enabled on ISE」というエラーが表示される。
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。

問題 ID 番号	説明
CSCwf26951	プロファイラ CoA が誤ったセッション ID で送信される。
CSCwi38644	エージェントルールが、既存のエージェントを編集している間にデフォルトのルール設定にデフォルト設定される。
CSCwh38464	Cisco ISE CLI 管理者ユーザーが 2 か月以上ログインしていないと、ログインできなくなる。
CSCwf35760	ct_engine ルートが CPU を 100% 使用している。
CSCwi37079	Cisco ISE URT バンドルのアップグレードが「RADIUS dictionary attribute duplicate entry exists」というエラーで失敗する。
CSCwi54325	エンドポイントがポスチャリース内にある場合、PRA が失敗する。
CSCwi03961	ポリシーセットにロケーショングループ情報がない。
CSCwh71157	JavaScript コードの携帯電話番号の形式フィールドで、100 文字を超える文字はサポートされない。
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試行されない。
CSCwi29623	スケジュールされたバックアップ設定の詳細が、Cisco ISE リリース 3.1 パッチ 7 の読み取り専用ユーザーに表示されない。
CSCwf36285	[Manage SXP Domain filters] の行に、最大 25 のフィルタしか表示されない。
CSCwi48806	ポータルエントリが重複しているため、認証ポリシーをロードできない。
CSCwj09890	Cisco ISE リリース 3.4 にアップグレードすると、Duo Seeder がアップグレード後の MnT テーブルにない。
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。
CSCwh83323	Cisco ISE リリース 3.2 でカスタム「SMTP API Destination Address」を使用している場合、「Reset Password」フローで SMS が送信されない。
CSCwf92635	Cisco ISE リリース 3.3 で、PAN フェールオーバー コンポーネントがデバッグログ設定にない。
CSCwa15336	Cisco ISE PIC リリース 3.1 で、ライブセッションに終了したセッションが表示されてしまう。
CSCwi04514	ディクショナリ属性に「-」が含まれている場合、ポスチャ クライアント プロビジョニング リソースに HTTP エラーが表示される。
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している。

問題 ID 番号	説明
CSCwh60726	Cisco ISE の自動クラッシュデコーダが機能を正しくデコードしていない。
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。
CSCwh16289	転送中にCLIバックアッププロセスが失敗した場合、「/opt/backup」から一時ファイルを削除するオプションが追加される。
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。
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
CSCwh69466	Cisco ISE リリース 3.1 で、詳細レポートに EAP チェーンのユーザー認証ポリシーとマシン認証ポリシーの両方が表示されない。
CSCwk13212	Cisco ISE リリース 3.2 以降のリリースでは、System 360 モニタリングのデバッグログレベルを下げる必要がある。
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。
CSCwi73984	Cisco ISE リリース 3.1 パッチ 8 の [Installed Patches] メニューに一部のパッチが表示されない。
CSCwi73981	大文字の FQDN を使用して追加された ID ストアを、CLI から削除できない。
CSCwf03445	Cisco ISE リリース 3.1 で、ライブログの詳細の表示に断続的な障害が発生し、「No Data available for this record」というエラーが表示される。
CSCwf66781	ERS を介した出力マトリックスポリシーの一括作成がエラーで失敗する
CSCwf42496	「Is IPSEC Device」NDG を削除しようとすると、後続のすべての RADIUS および TACACS+ 認証が失敗する。
CSCwi17694	設定された synflood-limit が 10000 を超えている場合、制限が機能しない。
CSCwh90691	show CLI コマンドで、ログレベルを 5 に設定すると、例外をスローする。
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。
CSCwi89689	Cisco ISE で「Invalid IP or hostname」エラーが表示される。
CSCwi46648	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。
CSCwi45131	シスコ製品に影響を与える Apache Struts の脆弱性：2023 年 12 月
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。

問題 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 からの応答が表示されない。
CSCwj01310	Cisco ISE リリース 3.4 で SXP コンポーネントがノードの寿命の問題を引き起こすために集中的に GC が発生する。
CSCwh51136	Cisco ISE が RADIUS 要求をドロップし、「Request from a nonwireless device was dropped」というエラーメッセージが表示される。
CSCwj77067	内部ユーザーの編集中に「Provide a comprehensible description for the error」が表示される。
CSCwf59310	Cisco ISE リリース 3.1 パッチ 7 で pxGrid ContextIn の [Context Visibility] にカスタム属性が存在しない。
CSCwh25160	スワップメモリの使用率が高い。
CSCwh64195	Cisco ISE でデータ破損により FailureReason=11007 または FailureReason=15022 が発生する。
CSCwf23271	展開 SEC_TRNREP_STATUS が「In Progress」状態から更新されない。
CSCwf22527	[Context Visibility] ページで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。
CSCwh71273	Cisco ISE リリース 3.2 で Essentials ライセンスが無効になっている場合、GUI アクセスが制限され、ルート CA を再生成できない。
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、Cisco ISE GUI がロードされない。
CSCwi57761	Cisco ISE の OpenSSH で CVE-2023-48795 が発生する。
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。
CSCwj83460	CV と Oracle データベース間で ID グループ数の不一致が発生する。
CSCwh71117	「User Services」のみを有効にすると、管理 GUI アクセスも有効になる。
CSCwi61491	メタスペースが枯渇した結果、アプリケーションサーバーがクラッシュする。
CSCwh77574	証明書のインポート中に Cisco ISE がパスワード内の特殊文字を許可しない。
CSCwf22794	VLAN ID または名前の不一致により、「Error: Not a valid ODBC dictionary」エラーが発生する。
CSCwh69045	Cisco ISE リリース 3.1 パッチ 5 で、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。

問題 ID 番号	説明
CSCwj44649	Cisco ISE リリース 3.3 で TACACS データが保持されず、消去される。
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。
CSCwi10922	メッセージコード 13036 のメッセージの説明に、スペル間違いの単語がある。
CSCwk30610	Cisco ISE リリース 3.2 で、コンソールで 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。
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。
CSCwh36544	pxGrid にトピック登録の詳細が表示されない。
CSCwi69659	TrustSec 展開の検証時、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トリガーされる。
CSCwe12974	[Out of Compliance for 30 days] アラームのテキストを更新する必要がある。
CSCwh97876	Cisco Identity Services Engine の任意のファイルのアップロードの脆弱性。
CSCwd57628	Cisco ISE リリース 3.1 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。
CSCwh70696	Cisco Identity Services Engine のストアドクロスサイトスクリプティングの脆弱性。
CSCwj21203	「Dashboard System Status」クエリが原因で 1000 件のデータベース接続が使い果たされる。
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と表示される。
CSCwj39533	RMQforwarder が原因で CPU 使用率が高くなる。
CSCwj60125	ユーザーアカウント検索とアカウントの管理機能が強化された。
CSCwf89224	クライアントから受信したセッションチケットの復号が Cisco ISE で失敗する。
CSCwi43166	CoA または CoA プッシュでの TrustSec 更新が破損している。
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。
CSCwi79159	Cisco ISE リリース 3.2 パッチ 4 で「deleteCertFromStore:- Failed to parse certificate」エラーが表示される。
CSCwk07483	入力の文字列に「0-255」を含めると、プロファイラ NetworkDeviceEventHandler がデバイスを追加できない。

問題 ID 番号	説明
CSCwj05508	特定の手順で設定された IP ホストに到達しようとすると、「Name or service not known」というエラーが表示される。
CSCwc39545	Docker メトリックレポートを変更する必要がある。
CSCwf31073	OpenAPI を使用してデバイス管理ネットワーク条件を取得するときに Cisco ISE に 400 エラーが表示される。
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 VPM フローでトリガーされる必要がある。
CSCwj43362	Cisco ISE リリース 3.2 へのアップグレードが「integrity constraint (CEPM.REF_HOSTCONFIG_HA_PEER1) violated」エラーで失敗する。
CSCwh28528	TACACS 着信レコードが 1 日あたり 4,000 万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。
CSCwc85211	Cisco ISE パッシブ ID エージェントでエラー「id to load is required for loading」が表示される。
CSCwf51766	Cisco ISE で、OpenAPI を使用して DenyAccess アイデンティティソースで認証ポリシーを作成できない。
CSCwj85626	API コールを使用してエンドポイントの IP アドレスを取得できない。
CSCwi67639	コマンド「show cpu usage」が Cisco ISE 3.x リリースで情報を表示しない。
CSCwj35581	Cisco ISE にレート制限保護がない。
CSCwj05881	Cisco ISE で認証が失敗し、詳細オプションが無視される。
CSCwh14249	Cisco ISE 3.x リリースで API ゲートウェイ設定のスペルミスがある。
CSCvz86688	Aruba-MPSK-Passphrase に暗号化のサポートが必要。
CSCwf09364	ユーザーおよびエンドポイント ID グループの説明フィールドは、長いテキストを使用すると編集できない。
CSCwh10401	Cisco ISE リリース 3.1 パッチ 5 で CSR を利用して pxGrid クライアント証明書を生成できない。
CSCwj12489	ネットワーク デバイス グループを削除できない。
CSCwh04251	Cisco ISE エージェントレスポスチャで、「:」文字を含むパスワードがサポートされない。
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。

問題 ID 番号	説明
CSCwf66237	Cisco ISE リリース 2.7 以降、Cisco ISE の「Get All Endpoints」要求の実行に時間がかかる。
CSCwk04644	Cisco ISE リリース 3.2 以降のリリースでは、System 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。
CSCwi38377	COA をトリガーできず、ディスパッチャキューでスタックする。
CSCwi92655	Cisco ISE リリース 3.3 パッチ 1 でサブタイトルをロード中に、[Context Visibility] ページのドロワを開くアクションでエラーが表示される。
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セキュリティグループとコントラクトは、Cisco ISE に同期できない。
CSCwd67833	この Cisco ISE 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。
CSCwj35602	パスワードの更新時に現在のパスワードを入力するという要件を、Cisco ISE でバイパスできる。
CSCwf96294	「not allowed domains」リスト内のドメインへの接続試行が、Cisco ISE リリース 3.0 で発生する。
CSCwd14523	'accountEnabled' 属性により、Azure AD での EAP-TLS の認証問題が発生する。
CSCwd34467	Cisco ISE で EAP チェーンおよび Azure AD グループを使用した認証の試行で、認証ルールの評価の失敗と見られる現象が発生する。
CSCwj80589	[Log Analytics] ページの起動中にエラーが表示される。
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や VN 値が表示される。
CSCwh64394	[Import] ボタンをクリックした後、.csv ファイルを選択すると [Import] ボタンが機能しない。
CSCvt75833	FQDN がトークンサーバーの場合、Cisco ISE は NSLookup を再度実行する必要がある。
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。
CSCwj66951	ネットワーク アクセス ユーザーの名と姓のフィールドでは、名前に「OR」を使用できない。
CSCwc53824	Cisco ISE で、AMP - AMQP サービスへの接続が TLSv1.0 に制限される。
CSCwf82055	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 で「$」が含まれている管理者パスワードを変更できない。

問題 ID 番号	説明
CSCwi45090	フィルタフィールド 'name' は、Cisco ISE ERS API を介したダウンロード可能な ACL ではサポートされない。
CSCwi59567	COA 再試行カウントを「0」に更新すると問題が発生する。
CSCwe82004	TCP ソケットの枯渇。
CSCwj82298	割り当てられた論理プロファイルが、[Context Visibility] ページのエンドポイント属性とレポートで繰り返される。
CSCwh48978	Open VM ツール（CVE-2023-20900）の評価。
CSCwj83459	Cisco ISE GUI で新しい内部ユーザーを作成できず、「couldn’t execute statement; SQL [n/a]; constraint [CEPM.BKUPSLASTAUTHTIMEENTRY]」というエラーが表示される。
CSCwf71870	スマートライセンスの登録後、TACACS 展開をゼロデイで評価しても機能しない。
CSCvy34255	[Require Admin Password] を有効にして機密データを表示すると、RADIUS および 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。
CSCwi36040	Cisco ISE リリース 3.2 の IP アクセスリスト制御が表示されない。
CSCwj97449	SNMPv3 設定中に snmp-server ホストの誤った engineID 形式について、Cisco ISE 管理者にアラートが表示されない。
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。
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中にエラーが発生する。
CSCwh88801	すべてのインターフェイスで設定されている 0.0.0.0 のデフォルト スタティック ルートが Cisco ISE のリロード後に削除される。
CSCwk07230	Cisco ISE リリース 3.3 パッチ 2 でネットワークデバイスを複製すると、RADIUS 設定なしでデバイスが再作成される。
CSCwf72123	pxGrid Direct 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 はそれらを取得できず、[Context Visibility] ページの pxGrid Direct Connector 情報に表示されない。
CSCwi66105	Cisco ISE リリース 3.1 パッチ 7 でカスタム属性のエラーが発生する。
CSCwh41693	メタデータ（IMDS）バージョン値 [V2 only] が選択されている場合、AWS 上の Cisco ISE が機能しない。

問題 ID 番号	説明
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。
CSCwh96376	Cisco ISE リリース 3.3 で、管理証明書ロールを切り替えることができない。
CSCwf34596	ユーザーカスタム属性がレンダリング段階でスタックする。
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。
CSCwj31619	Cisco ISE リリース 3.2 以降のリリースで、[Condition Studio] の条件の情報ポップアップに、デフォルトの無効アイコンが表示される。
CSCwi52264	Cisco ISE SAML アイデンティティ プロバイダーの設定属性が別の場所で参照されているにもかかわらず削除される。
CSCwh00049	Cisco Identity Services Engine のストアドクロスサイト スクリプティングの脆弱性。
CSCwf59005	Cisco ISE リリース 3.2 パッチ 3 で PEAP および EAP-TLS が FIPS モードで機能しない。
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。
CSCwh01022	IPv6 アドレスを変更すると、IPv6 デフォルトルートがルーティングテーブルから消える。
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。
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。
CSCwf38083	Cisco ISE サービスが、Secure SysLog で初期化状態のままになる。
CSCwi28131	[Never Purge] ルールで使用されているカスタム属性によって、エンドポイントが依然として消去される。
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。
CSCwj67980	外部リポジトリにエクスポートすると、プライマリゲストレポートにタイトルの重複エントリが表示される。
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。
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。
CSCwh17386	Cisco ISE の専用 MnT ノードが SMTP 設定を複製しない。

問題 ID 番号	説明
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のスクリプトが間違っている。
CSCwf25955	SGT、VN 名および VLAN によるマッチング認証プロファイルで、PRRT 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。
CSCwj82278	古いロックファイルが API ゲートウェイと [Context Visibility] ページをブロックする。
CSCwb77915	[Allowed Protocols] のポリシーに基づいて RSA PSS 暗号の有効/無効を切り替える。
CSCwh52589	ゲストユーザーが Cisco ISE に初めて接続した場合、Cisco ISE はゲストユーザー名で ACS.Username フィールドを更新しない。
CSCwh42442	Cisco ISE リリース 3.2 パッチ 3 で CRL のダウンロードに失敗する。
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。
CSCwj68795	Cisco ISE でレプリケーション時にレプリケーションエラー「Error synchronizing object: EDF2EndPoint: Operation: Update」が表示される。
CSCwh93498	Cisco ISE リリース 3.1 で、Cisco ISE BYOD 設定でデバイスポータルを複製した後、エンドポイント消去ルールが自動的に作成され、これにより 30 日後に Cisco ISE データベースからエンドポイントが削除される。
CSCwh90610	Cisco ISE で放棄された Jedis 接続がスレッドプールに返送されない。
CSCwf91508	CLI から取得された Cisco ISE GUI パケットキャプチャが削除できない。
CSCwe07822	Cisco ISE の最後の消去日付のタイムスタンプが正しくない。
CSCwh55667	Cisco ISE で Premier ライセンスが無効になっている場合、ポスチャの内部システムエラーが発生する。
CSCvz48764	起動プログラムの修復に一定の順序を設定できる。
CSCwi19460	サポートされていないメッセージコード 91092 と 91103、およびそれぞれのアラームが syslog に表示される。
CSCwj14231	TACACS レポートの Cisco ISE リリース 3.2 のカスタムフィルタが正常に機能しない。
CSCwh06081	Cisco ISE ノードの登録を解除すると、このプロセスがプライマリ PAN によって開始されたかどうかを確認する必要がある。

問題 ID 番号	説明
CSCwi17200	トラブルシューティングのために Active Directory との通信の復号に、「TROUBLESHOOTING.EncryptionOffPeriod」の高度な調整を分単位のゼロ以外の値で設定すると、その Cisco ISE ノードのすべての Active Directory 認証で RPC ネットログオンが失敗する。
CSCuz65708	DACL エントリの番号付けが、Mozilla Firefox 45 以降でオフになる。
CSCwh51548	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。
CSCwi66608	Cisco ISE リリース 3.2 で RMQ が APIPA IP 169.254.2.2 を使用して発信 RST パケットを送信する。
CSCwj25817	デフォルトゲートウェイと設定された IP アドレスが異なるサブネット上にある場合、初期セットアップが失敗する。
CSCwf39620	ユーザー名が $（ドル記号）で始まる場合、Windows エージェントレスポスチャが機能しない。
CSCwh17448	Cisco ISE リリース 3.1 で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。
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。
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。
CSCwi42412	Cisco ISE 3.x リリースでインタラクティブヘルプがコンソールとログにエラーをスローする。
CSCwh81943	ポータル名と結果のフィルタが、プライマリゲストレポートで機能しない。
CSCwh03740	CRL の取得に失敗する。
CSCwj81776	Cisco ISE リリース 3.2 で、[Empty] および [Not Empty] フィルタに高度なフィルタを使用できない。
CSCwj27469	クラウド（Azure、AWS、OCI）上の Cisco ISE リリース 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。
CSCwh96018	同じ名前で大文字と小文字が異なる新しいモバイルデバイス管理を作成すると、大文字と小文字を区別するチェックが原因で失敗する。
CSCwk07593	Get-All ゲストユーザー API が一部のアカウントを取得しない。

問題 ID 番号	説明
CSCwh99772	子項目がいずれかのグループから削除されると、すべてのネットワーク デバイス グループが削除される。
CSCwf44906	設定のバックアップを復元した後、新しいログイン情報でリポジトリを再設定する必要がある。
CSCwj35576	Cisco ISE サーバー側の検証が実行されていない。
CSCwi57903	スケジュール済みバックアップが失敗してもアラームが生成されない。
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表示される。
CSCwe12961	[Evaluation Period Expired] アラームが、過剰消費が原因で SLR ライセンスがコンプライアンス違反になっている場合に表示される。
CSCwj23933	未参加の AD コネクタのステータスが更新される。
CSCwi11762	[Context Visibility] ページの韓国語サポートの問題。
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ユーザーのみがエンドポイントを編集または削除できる。
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 でセッション統合が行われない。
CSCwi57069	NA PRRT は、メインスレッドプールを使用してロギングから分離する必要がある。
CSCwk13244	ise-messaging.log が、Cisco ISE GUI でのダウンロードに表示されない。
CSCwf14365	[Log Analytics] ページに移動すると、「Configuration Missing」という警告が表示される。
CSCwh24823	非必須属性が Update PUT 要求の本文に含まれていない場合、それらの値が空またはデフォルト値にリセットされる。
CSCwi53884	OpenSSL 1.0.2o での脆弱性。
CSCwe25050	プライマリ PAN 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。
CSCwc04447	Cisco ISE リリース 2.7 パッチ 6 において、IP アドレスで NAD IP をフィルタリングできない。
CSCwh30893	プロファイリングで、「XXXXXXXXXXXX」の形式の発信側ステーション ID の値が処理されない。

問題 ID 番号	説明
CSCwi32576	CPMSessionID の割り当て中に PSN ノードがクラッシュする。
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。
CSCwi11965	Cisco Identity Services Engine のサーバー側リクエストフォージェリの脆弱性。
CSCvu56500	Cisco ISE のすべてのネットワークデバイスのエクスポートでファイルが空になる。
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。
CSCwk32104	agentprobeoom.sh と restprobeoom.sh の両方は、独自の OOM ヒープファイルをクリーンアップして、Cisco ISE データベースの使用率を最適化する必要がある。
CSCwf85644	PSK に % を使用すると、Cisco-av-pair がエラーをスローする。
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」エラーが表示される。
CSCwa82035	ガベージコレクタログ、スレッドダンプ、およびヒープダンプがサポートバンドルにない。
CSCwh45472	Cisco ISE GUI からの運用バックアップが、「Backup Failed; copy to repository failed」というステータスで失敗する。
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。
CSCwj07319	API ers/config/sessionservicenode が誤った合計を返す。
CSCwf83193	AD ログイン情報を使用してセカンダリ管理ノードの Cisco ISE GUI にログインできない。
CSCwk00439	ロックファイルが削除されないため、pxGrid Direct サービスが初期化状態でスタックする。
CSCwf61939	[First Name] と [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。
CSCwh18731	アップグレードワークフロー前に 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、プロファイラ例外が発生する。
CSCwh42009	Cisco ISE リリース 3.2 パッチ 3 で、アダプタログ情報が更新されない。
CSCwk20019	SMS HTTP メソッドを SMS ゲートウェイとして使用する場合、SMS HTTP URL の属性名によって問題が発生する。
CSCwk35172	Cisco ISE PSN ノードで DumpClearOnExceed ファイルが使用するディスク容量が大きすぎる。

問題 ID 番号	説明
CSCwf62744	「Disable EDR Internet Check」タグを追加する機能拡張。
CSCwf44736	Cisco Identity Services Engine のクロスサイト リクエスト フォージェリの脆弱性。
CSCwh26698	pxGrid コネクタのユーザーデータを取得する方法の追加。
CSCwb57672	Android 12 の認証要件である SHA384withRSA4096 証明書を使用した GCMP256 認証では、認証プロセスが失敗する。
CSCwh41977	Cisco ISE リリース 3.2 で Cisco ISE 設定にユーザーごとの DACL が存在することを確認する。
CSCwd21798	Cisco ISE-PIC ライセンスの期限切れアラーム。
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、データのないレポートが作成される。
CSCwj72680	HS_err ファイルが MnT ノードで生成される。
CSCvv77007	外部の RADIUS トークンサーバーへの応答として Cisco ISE が内部ネットワーク管理者ユーザーを絶えず要求する。
CSCwh46877	PORT_BOUNCE を持つ ANC ポリシーが削除された場合、COA ポートバウンスが発生する必要がある。
CSCwj72117	運用データの削除を実行すると、プライマリ モニタリング ノード名のみが表示される。
CSCwh32290	FQDN 値でリセット設定を実行すると、GUI と CLI で不一致が発生する。
CSCwc80574	結合操作中に Cisco ISE AD コネクタでエラーが発生する。
CSCvg54133	CLI での出力時にホスト名が変更される。
CSCvz62183	デバッグログ設定で「reset to default」オプションが使用されている場合、デバッグプロファイルは削除されない。
CSCwk13234	古い Cisco ISE ノードが、復元操作後に TCP ダンプとデバッグプロファイル設定に表示される。
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。
CSCwf44942	Cisco ISE PSN が、TACACS を使用したユーザーセッション認証フローに最大数のユーザーが含まれている場合にクラッシュする。
CSCwf22816	内部ユーザー ID グループに基づく承認が、VPN の RADIUS トークン承認がないため失敗する。
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。

問題 ID 番号	説明
CSCwh39802	スポンサーの承認後にゲストに電子メールを送信できない場合、Cisco ISE が誤解を招くメッセージを送信する。
CSCwi72309	Cisco ISE がプロファイリングループでスタックし、レプリケーションが遅延し、エラーが発生する。
CSCwe96739	TLS 1.0 または TLS 1.1 は、Cisco ISE リリース 3.0 の管理者ポータルで受け入れられる。
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。
CSCwj74175	restprobe-OOMHeap ダンプを圧縮する。
CSCwf60904	ANC の修復が AnyConnect VPN で適切に機能しない。
CSCvm56115	対応する ID ストアが別のブラウザタブから削除されても、Cisco ISE でポリシーを保存できる。
CSCwf56826	回帰セットアップのプライマリ PAN ノードで jstack に関連するコアを確認できる。
CSCwd20521	AD コネクタプロセスがシャットダウンしない。
CSCwh79938	高度な調整で優先ドメインコントローラのレジストリ値を設定できない。
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。
CSCwf78003	[pxGrid Endpoints] ページのエンドポイントの詳細が正しくない。
CSCwh42683	SAML 認証時に Cisco ISE 管理者のアクセスに読み取り専用権限が付与される。
CSCwi58699	Cisco ISE で Cisco Catalyst Center または Endpoint Analytics 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。
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。
CSCwi88583	erl_crash.dump をより適した方法で処理する必要がある。
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。
CSCwi75143	PriorityType が必須であるとき、プロファイリング設定を更新できない。
CSCwf97087	プロキシに問題がある場合、ポスチャフィード更新エラーが正しくない。
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。

問題 ID 番号	説明
CSCwi93050	管理アクセスに 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。
CSCwi12671	TCP ダンプ診断ツールで、ノードの複数のインターフェイスを同時にキャプチャすることができない。
CSCwi33361	サーバーへの接続に失敗すると、Cisco ISE CLI アクセスで問題が発生する。
CSCwh08440	ライブログイベント 5422 および 5434 では、[Authentication] 列と [Authorization] 列にデータが表示されない。
CSCwi34405	認証ポリシーに IdentityAccesssRestricted 属性を適用できない。
CSCwj58727	Cisco ISE では、プロトコルがチェックされていない場合、ユーザーが許可されたプロトコルを保存することを許可してはならない。
CSCwf59338	Cisco ISE でクロスオリジン HTTP セキュリティヘッダーがない。
CSCwh95022	日本語の 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。
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、障害理由 11007 および 15022 により承認がドロップされる。
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、自己登録電子メールの件名行の等号記号「=」以降がすべて切り捨てられる。
CSCvv85789	ポート 8084 における Cisco ISE HSTS ヘッダーの脆弱性。
CSCwj47769	Cisco ISE がパッシブ ID エージェントをダウンロードできない。
CSCwi27497	IP テーブルのエラーが原因で、Cisco ISE REST 認証サービスが実行されない。
CSCwj32716	クライアント証明書の GUID を使用してデバイスのコンプライアンスを検証すると、MDM 設定が失敗する。
CSCwf55795	ADE-OS 復元オプションを使用すると、Cisco ISE リリース 3.2 パッチ 1 以降のリリースで Cisco ISE GUI および CLI にアクセスできない。
CSCwi38912	デバッグ要素が、Cisco ISE リリース 3.3 のデバッグプロファイル設定で 3 回以上繰り返される。
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。
CSCwi20027	NAD 情報の取得中に CoA 要求がスタックすると、TrustSec の展開要求に失敗する。

問題 ID 番号	説明
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 2x 応答を返す。
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。
CSCwh17285	Cisco ISE リリース 3.2 パッチ 3 および Cisco ISE リリース 3.3 でインターフェイス上の IPV6 コマンドが「IPV6 is enable」のみの場合、ポータルが初期化されない。
CSCwj51329	VMware Workspace One がモバイルデバイス管理サーバーに設定されている 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。
CSCwf02093	Hyper-V で実行している Cisco ISE リリース 3.2 のノードに、初期セットアップ時に設定された静的 IP に加えて DHCP アドレスが割り当てられる。
CSCwi63725	SNMPD プロセスが原因で Cisco ISE でメモリリークが発生する。
CSCwf30570	コンピュータが 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。
CSCwh68651	Cisco ISE リリース 3.1 パッチ 7 で undo-tablespace を再作成すると、URT が失敗する。
CSCwf94289	Cisco ISE リリース 3.0 パッチ 6 において Policy export でポリシーのエクスポートに失敗する。
CSCwj48827	起動プログラム修復で、引用符（""）内に複数のタスクを追加できない。
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。
CSCwh88911	Cisco ISE データベースで、スポンサーアカウントの電子メールフィールドに 100 文字しか使用できない。
CSCwf09393	Cisco ISE リリース 3.1 で 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。
CSCwf79582	AD ログイン情報によって 2.2.1.x 以降のリリースで Cisco ISE を統合できない。
CSCwe99498	Cisco ISE に、Common Vulnerability and Exposures（CVE）の ID（CVE-2023-27536、CVE-2023-27535、CVE-2023-27538）によって識別される脆弱性の影響を受けるバージョンの libcurl が含まれている。
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しない。
CSCwh99534	エンドポイントプローブが SXP マッピングをクリーンアップしない。
CSCwj95818	最大同時 CLI セッションが、Cisco ISE リリース 3.4 で機能しない。

問題 ID 番号	説明
CSCwf61657	スポンサー FQDN の TCP ハンドシェイクに常に Gig 0 が関与する。
CSCwh92185	[Operational Data Purging] ページからエクスポートされた RADIUS 認証レポートが空になる。
CSCwi54722	IP アドレスで終わる FQDN を使用するリダイレクト URL で、IP アドレスが Cisco ISE ホスト名に置き換えられる。
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。
CSCwi89466	Cisco ISE リリース 3.2 パッチ 3 で Cisco ISE AD ユーザーの SamAccountName パラメータがユーザーセッションで null になる。
CSCwi78164	重複エントリ（IP、名前、FQDN）が原因で、Cisco ISE DNS の解決可能性ヘルスチェックが失敗する。
CSCwk04493	Cisco ISE リリース 3.1 パッチ 6 で、ポリシーの詳細を取得するために使用されるメソッドは、内部メソッドを使用し、キャッシュされない。
CSCwj03747	特定の論理グループの CoA を抑制するオプションが有効になっている場合でも、プロファイリングが CoA を抑制しない。
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セッションキャッシュに保存されない。
CSCwj80616	Cisco ISE の [Context Visibility] ページ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の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。
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。
CSCwh65018	Cisco ISE リリース 3.1 パッチ 5 のインストールが無期限に停止する。
CSCwj59848	[Log Analytics] ページが Cisco ISE で起動しない。
CSCwh08408	Cisco ISE リリース 3.3 で、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。
CSCwh72754	アイデンティティソースとして Active Directory を使用する認証への影響。
CSCwi66126	Cisco ISE ERS API で 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。
CSCwi98793	プロファイラが誤った値を持つ MDM 属性をキャッシュしている。

問題 ID 番号	説明
CSCwf37679	プライマリ PAN 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。
CSCwi30707	Cisco ISE リリース 3.1 パッチ 7 で、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。
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、GUI からの保存コールがトリガーされる。
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。
CSCwi59312	Cisco ISE の認証プロファイルが「Security Group」と「Reauthentication」の一般的なタスクでデータを保持しない。
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。
CSCwf17714	Cisco ISE リリース 3.3 でレポートに DockerMetric の複数のエントリが表示される。
CSCwc36589	Intune での MAC アドレスベースの API のサポート終了により、Cisco ISE と Intune MDM の統合が中断される可能性がある。
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が順守されない。
CSCwf67438	作成者ノードの一部の VN が、リーダーノードに同期されない。
CSCwj52266	[Context Visibility] ページのエンドポイントの説明が、スタティック ID グループの説明で更新される。
CSCwi94938	Cisco ISE リリース 3.2 でフィルタを使用すると、ゲストユーザー API で誤った結果が返される。
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。
CSCwh28098	Cisco ISE リリース 3.2 パッチ 3 で RSD が無効になっているポスチャアセスメント中に、CoA プッシュコールの代わりに CoA 切断コールが送信される。
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。
CSCwj43480	Cisco ISE リリース 3.3 が UPN（ユーザープリンシパル名）を持つユーザーに対して MFA を呼び出さない。
CSCwe53550	Cisco ISE および CVE-2023-24998。
CSCwi15793	Cisco ISE のカスタム属性の特殊文字に関するエラー。

問題 ID 番号	説明
CSCwi89082	Cisco ISE のデフォルトポータルはデータベースから削除されるが、SAML 設定では必要になる。
CSCwh92366	Cisco ISE リリース 3.1 パッチ 8 で、仮想マシンリソース不足のアラームが発生する。
CSCwj06269	[Device Administration] 設定を変更しても、レポートまたはアラームがトリガーされない。
CSCwj33906	VPN クライアントの IP または SXP マッピングが作成されない。
CSCwj21403	ホストに複数のエントリがある場合に、REST 認証サービスが有効にならない。
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。
CSCwh56565	ライブログとレポートの MnT ノードへのプライマリ PAN REST コールがロードバランシングされない。
CSCwk61938	Cisco ISE は OpenSSH CVE-2024-6387 を評価する必要がある。
CSCwh95232	Cisco ISE でインターフェイス IP アドレスの重複が許可される。
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。
CSCwf05178	URT を実行すると、表面的な警告またはエラーが表示される。
CSCwi26921	DumpClearOnExceed ファイルを、Cisco ISE CLI で「dir」コマンドを使用して表示できる。
CSCwj40026	Cisco ISE GUI でトリガーされたバックアップに、バックアップが CLI からトリガーされたというエラーが表示される。
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トリガーされる。
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。
CSCwh36667	Cisco ISE モニタリング GUI が [Welcome to Grafana] ページでスタックする。
CSCwk07324	ACE サードパーティライブラリ ContextIn のリークが原因で Cisco ISE のメインスレッドプールがスタックする。
CSCwh74236	TACACS+ 認証フローの詳細な [Live Log] ページがロードされない。
CSCwi25755	Cisco ISE リリース 3.2 以降のリリースでは、SAML プロバイダーを追加できない。

問題 ID 番号	説明
CSCwi23166	パッチ管理条件の変更を保存できない。
CSCwh03227	Cisco ISE で、認証時にライセンスが使用されない。
CSCwh71435	ERS API で指定されていない場合でも、内部ユーザーの「Enable Password」が作成される。
CSCwh44407	Cisco ISE リリース 3.2 の展開内の Cisco ISE ノードでシステム証明書のインポートが機能しない。

未解決の不具合

Cisco ISE リリース 3.4 の未解決の不具合：累積パッチ 1

次の表は、Cisco ISE 3.4 パッチ 1 で未解決の不具合のリストです。

問題 ID 番号	説明
CSCwm40972	AWS ワークロードコネクタを設定する場合、パブリックおよびプライベート IPv4 アドレスのみが検出され、IPv6 アドレスは認識されない。
CSCwm61368	「Contains」演算子を使用してソース属性としてワークロード分類ルールでワークロードコネクタを使用する場合、コネクタを削除することができない。
CSCwn08908	バージョン Cisco ISE リリース 3.4 パッチ 1 にロールバックすると、セッションデータのみがパブリッシュされ、SXP データはパブリッシュされない。
CSCwn46625	接続先 ACI でエンドポイントグループ（EPG）を一括削除した後、設定のばらつきアラームメッセージがダッシュボードに表示されない。
CSCwn50666	pxGrid Direct 同期に基準よりも時間がかかっており、メモリの問題も発生している。
CSCwm75692	ACI 接続が一時停止した場合、SXP ノードを展開から登録解除し、ACI 接続を再接続する必要がある。
CSCwn12955	SGT をインポートする場合、そのプロセスは、ACI によって作成された名前で失敗するのではなく、既存の名前を上書きする。
CSCwn13021	「Contains」フィルタを大規模なデータに適用すると、保存に時間がかかりすぎる。
CSCwn14897	CDP または CSDAC において、[SGT Bindings] ページで IPv6 アドレスの部分検索に問題が発生する。
CSCwn33420	デフォルトの分類ページからの SGT が、他のルールからのバインディングに追加される。

問題 ID 番号	説明
CSCwn45653	CDP または CSDAC において、[SGT Bindings] ページでセカンダリ セキュリティ グループ フィルタが機能しない。
CSCwn47826	ログ分析で、[Radius Step latency] ダッシュボードにエラーが表示される。
CSCwn50156	デフォルトの分類ルールが PSN のデータベースで作成されない。
CSCwk39635	Cisco ISE リリース 3.3 パッチ 2 では、多要素認証が MSCHAPv2 で機能しない。
CSCwn54074	アップグレードされたセットアップで Cisco ISE リリース 3.4 パッチ 1 にロールバックすると、レガシーパッチページのロードに失敗する。
CSCwn21814	CDP では、アウトバウンドフィルタで「Purge Endpoint」操作を実行した後、IPv6 プレフィックスが削除されない。
CSCwn54494	プロキシを介した CRL 情報のダウンロードが失敗する。

Cisco ISE リリース 3.4 の未解決の不具合

次の表は、リリース 3.4 で未解決の不具合のリストです。

問題 ID 番号	説明
CSCwj57668	アップグレード後、MFC プロファイラダッシュボードにデータが表示されない。
CSCwk38205	ACI 接続が削除されても、SGT が削除されない。
CSCwk39635	VPN ログインを使用した Duo MFA が、MS-CHAP-v2 で機能しない。
CSCwk67747	RADIUS プロトコルスプーフィングの脆弱性（Blast- RADIUS）。
CSCwk74068	SXP ノードのリロード後に、SXP が欠落しているエントリを一括ダウンロードする。
CSCwk78054	スタンドアロンノードに PPAN と PSN の両方のペルソナが割り当てられている場合、エンドポイントは [Context Visibility] ページに表示されないが、[Live Logs] ページと [Live Sessions] ページには表示される。
CSCwk79595	[Inbound and Outbound SGT Domain Rules] ページのページレベルのヘルプが機能しない。
CSCwk85207	ISE 設定で DACL が見つからない場合、承認が失敗する。
CSCwk98200	[Administration] > [Identity Management] > [External Identity Sources] > [SAML Id Providers] で次のエラーが発生する。 `Signing certificate validation failed, error: The IdP signing certificate is self signed and cannot be found in Trusted Certificates. Check Trusted Certificates contain the IdP signing certificate.`

問題 ID 番号	説明
CSCwk98467	ユーザー名サフィックスが REST ID ストアで設定されていない場合、Cisco ISE 3.3 から 3.4 へのデータのアップグレードと復元が失敗する。
CSCwm35551	Cisco ISE GUI からネットワークデバイスをエクスポートした後、CSV ファイルの [Network Device Groups] の値が Cisco ISE GUI の値と異なる。
CSCwm38203	MacOS 15.1 Beta 2 での Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）ワークフローでは、Cisco Network Setup Assistant アプリケーションをダウンロードして開こうとすると、次のエラーが生成される。 `Unable to check for updates`
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。

Cisco ISE リリース 3.4 - 累積パッチ 1 の既知の制限事項

ACI 接続での IPv6 アドレスの使用

IPv6 アドレスが統合全体で同じ形式で維持されるように、Cisco ISE リリース 3.4 パッチ 1 をインストールする前に ACI 接続を一時停止する必要があります。

新しくサポートされた演算子を使用したパッチのロールバックフロー

Cisco ISE リリース 3.4 パッチ 1 以降、**IP Equals**、**IP Not Equals**、**In**、**Not In**、**Contains**、および **Not Contains** 演算子は、ワークロード分類ルールとインバウンド SGT ドメインルールでサポートされます。Cisco ISE リリース 3.4 パッチ 1 の [Patch Rollback] オプションを使用すると、これらの演算子を含むワークロード分類ルールとインバウンド SGT ドメインルールは、Cisco ISE リリース 3.4 ではサポートされていないため、パッチロールバックフロー中に削除されます。

その他の参考資料

Cisco ISE を使用するときに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。