Cisco Identity Services Engine リリース 3.0 リリースノート

初版：2020 年 9 月 18 日

最終更新：2021 年 7 月 27 日

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

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

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

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

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、5GaaS 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 TrustSec ソリューションのポリシーマネージャとして機能し、TrustSec ソフトウェアによって定義されたセグメンテーションをサポートします。

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

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

Cisco ISE の詳細な発注およびライセンス情報については、 *Cisco IdentityServices 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。

Cisco ISE リリース 3.0 の新機能

Cisco ISEリリース 3.0 では、Essentials、Advantage、Premier のライセンスを使用します。

この Cisco ISE リリースでサポートされているライセンスの詳細については、『Cisco Identity Services Engine 管理者ガイド』の「ライセンス」の章を参照してください。

新しい機能は、その機能に必要なライセンスに従って分類されます。

Essential ライセンス

次の機能には Cisco ISE Essentials ライセンスが必要です。

機能別のデバッグウィザード

デバッグウィザードには、ISE ノードの問題のトラブルシューティングに使用できる事前に定義されたデバッグテンプレートが含まれています。デバッグプロファイルとデバッグログを設定できます。

ビジネス成果：Cisco TACは、Cisco ISE 展開の複数のノードでデバッグログを簡単に有効にできるようになりました。この機能は、迅速なトラブルシューティングに役立ちます。

多要素認証用の SAML SSO

多要素認証をサポートするように SAML 要求見出しの認証コンテキスト値を編集します。

ビジネス成果：SAML 認証で多要素認証がサポートされるようになります。

Amazon Web サービスの VMware クラウドおよび Azure VMware ソリューションにおける Cisco ISE のサポート

VMware クラウドに Cisco ISE をインストールするプロセスは、VMware 仮想マシンに Cisco ISE をインストールするプロセスとまったく同じです。サポートされる仮想環境 （8 ページ） を参照してください。

ビジネス成果：Cisco ISE は、Amazon Web Services（AWS）と Azure VMware ソリューション（AVS）の VMware クラウド上でホストできます。

ODBC アイデンティティストアに対する複数の属性ルックアップ

次のディクショナリの属性を（ユーザー名とパスワードに加えて）[Fetch Attributes] ストアドプロシージャの入力パラメータとして使用するには、ODBCアイデンティティストアを追加した上で [Advanced Settings] オプションをクリックします。

- RADIUS
- Device

- ネットワークアクセス（AuthenticationMethod、デバイス IP アドレス、EapAuthentication、EapTunnel、ISE ホスト名、プロトコル、UserName、VN、および WasMachineAuthenticated）

ODBC データベースから次の出力パラメータを取得するようにストアドプロシージャを設定できます。

- ACL
- セキュリティ グループ（Security Group）
- VLAN（名前または番号）
- Web リダイレクト ACL
- Web リダイレクトポータル名

ビジネス成果：これらの属性を使用して認証プロファイルを設定できます。たとえば、認可プロファイルごとに VLAN を手動で指定するのではなく、指定された入力属性（MAC アドレス、ユーザー名、着信側ステーション ID、デバイスの場所など）に基づいて ODBC データベースから返された VLAN を使用するように認証プロファイルを設定できます。

Cisco ISE API ゲートウェイ

Cisco ISE API ゲートウェイは、複数の Cisco ISE サービス API への単一のエントリポイントとして機能する API 管理ソリューションであり、セキュリティとトラフィック管理を向上させます。外部クライアントからの API 要求は、Cisco ISE の API ゲートウェイにルーティングされます。その後、要求は API ゲートウェイで設定されたルールに基づいてサービス API が実行されている Cisco ISE ノードに転送されます。

ビジネス成果：Cisco ACI インフラストラクチャと組み合わせることで、Cisco Software-Defined Access（SDA）ファブリックの情報交換とクロスドメイン自動化の変換が強化されました。

証明書フィンガープリント

信頼できる証明書で即時発行者フィンガープリント SHA256 証明書を評価するには、証明書のフィンガープリントプロセスを使用します。これにより、複数の証明書が異なるドメインをサポートするためのセキュアなメカニズムが適用されます。証明書フィンガープリントでは、802.1x プロトコルの信頼できる証明書をロックすることもできます。

ビジネス成果：複数の信頼できる証明書によって複数のドメインがサポートされます。

パッシブ ID のサービス用の MSRPC プロトコル

Cisco ISE リリース 3.0 以降では、パッシブ ID に MS-Eventing API または Microsoft Remote Procedure Call（MSRPC）プロトコルを使用できます。MSRPC プロトコルを使用してノード通信を確立し、Cisco ISE のノード間のハートビートをモニターします。このオプションは、パッシブ ID サービス用の WMI プロトコルに加えて使用できます。

MSRPC プロトコルは、Cisco ISE または Cisco ISE-PIC が複数のドメインコントローラからイベントを収集およびモニターするときに、信頼性の高いメカニズムが助長されます。また、Active Directory ドメインコントローラのユーザーログインイベントの遅延も減少します。

ビジネス成果：DC イベントを監視するための信頼性の高いメカニズムを提供します。

ヘルス チェック

展開内のすべてのノードを診断するオンデマンドのヘルスチェックオプションが導入されています。運用の前にすべてのノードでヘルスチェックを実行すると、ダウンタイムやブロッカーを引き起こす可能性のある重大な問題を特定できます。ヘルスチェックは、すべての依存コンポーネントの動作ステータスを提供します。コンポーネントに障害が発生すると、問題を解決するためのトラブルシューティングの推奨事項が即座に提供され、シームレスな操作が実行されます。

アップグレードプロセスを開始する前に、ヘルスチェックを実行するようにしてください。

ビジネス成果：重要な問題を特定し、ダウンタイムやブロッカーを回避します。

ヘルスチェックの詳細については、『Cisco Identity Services Engine Administrator Guide』の「Troubleshooting」の章を参照してください。

テレメトリの更新

追加のネットワーク統計情報が収集されます。

ビジネス成果：顧客ネットワークについて収集できる情報が多くなればなるほど、製品の改善方法を分析できるようになります。

TCP ダンプの機能拡張

TCP ダンプファイルをより詳細に制御できるようになりました。その他のインターフェイスで TCP ダンプを実行することもできます。

ビジネス成果：TCP トラフィックに関するデータの収集が簡単になりました。

Azure Active Directory でユーザーを認証するためのリソース所有者パスワード クレデンシャル フロー

リソース所有者パスワードクレデンシャル（ROPC）フローでは、Cisco ISE がクラウドベースのアイデンティティプロバイダーを使用してネットワーク内で認可と認証を実行できます。これは制御された導入機能です。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。

ビジネス成果：ROPC フローでは、Cisco ISE で Azure Active Directory ユーザーを認証および認証できます。

インタラクティブヘルプ

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

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

Advantage ライセンス

次の機能には Cisco ISE Advantage ライセンスが必要です。

新しい pxGrid のページ

新しい pxGrid インターフェイスには、pxGrid v1 と pxGrid v2を 分離する新しいページがあります。セッションとクライアントの情報を含む新しい [Summary] ウィンドウもあります。

ビジネス成果：pxGrid セッションを管理する際のワークフローが向上しました。

（注） pxGrid 1.0 はレガシー Extensible Messaging and Presence Protocol（XMPP）を使用します。この実装はメンテナンスモードになっており、間もなく削除されます。Cisco ISE リリース 2.4 で pxGrid 2.0 が導入されました。 pxGrid 2.0 は REST プロトコルと Websocket プロトコルを使用します。これらのプロトコルは、標準化されたシンプルなアプリケーション間通信インターフェイスです。パートナーは pxGrid クライアントの実装をこれらの新しいプロトコルに切り替えることを推奨します。

pxGrid 2.0 へのスイッチを推奨する理由については、『Welcome to Learning Cisco Platform Exchange Grid (pxGrid)』を参照してください。

Desktop Device Manager からのベースラインポリシーの設定

Cisco ISE リリース 3.0 にアップグレードするときに、接続されている Desktop Device Manager サーバーから設定のベースラインポリシーを選択するのにルートパッチを使用しないことをお勧めします。

また、ドングル、ドッキングステーション、または MAC アドレスのランダム化技術が使用されている場合、MAC アドレスの代わりにデバイス識別子を使用して Windows エンドポイントを検証し、精度を高めることもできます。

ビジネス成果：Desktop Device Manager サーバーで作成された設定のベースラインポリシーを使用して、エンドポイントのコンプライアンスを確認できます。エンドポイント識別の精度を高めるには、MAC アドレスではなくデバイス識別子を使用します。

Cisco ISE ACI-SDA と VN 認識の統合

Cisco ISE リリース 3.0 は、Cisco ACI インフラストラクチャと組み合わせることで、Cisco Software Defined Access（SDA）ファブリックの情報交換とクロスドメイン自動化の変換が強化されます。この実装により、IP-SGT バインディングの交換や pxGrid ドメインと SXP ドメインへのバインディングの送信とともに、EPG および SGT 情報の交換と変換、Cisco ACI ファブリックへの SDA 仮想ネットワーク（VN）の拡張、SDA および ACI ファブリックデータプレーンの自動化をサポートします。

ビジネス成果：セキュリティとトラフィック管理が向上しました。

ウイルス対策とマルウェア対策の最小バージョン

Cisco ISE リリース 3.0 以降では、ポスチャポリシーを作成して、ネットワーク内のエンドポイントにウイルス対策とマルウェア対策の最小バージョンを設定できます。このポリシーは、エンドポイントがネットワークポリシーのウイルス対策とマルウェア対策の最小バージョンに確実に準拠するようにします。また、新しいバージョンのウイルス対策とマルウェア対策で状態を自動的に更新するため、状態を修正するために必要な手作業が軽減されます。

ビジネス成果：エンドポイントがネットワークポリシーに準拠しているため、セキュリティが強化されました。

ポスチャセッションの共有

ポスチャステータスはPSN間で共有されます。ステータスは設定できません。常にオンです。

ビジネス成果：異なる PSN に切り替えると、クライアント接続でポスチャを再実行する必要はありません。

エージェントレスポスチャ

この新しいポスチャタイプは、SSH を介してクライアントにエージェントを配信し、必要に応じてポスチャが完了したときにクライアントを削除します。AnyConnect は必要ありません。

ビジネス成果：フットプリントが低く、一時的なポスチャエージェントが顧客に表示されません。

マルチ **DNAC** のサポート

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

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

Premier ライセンス

次の機能には Cisco ISE Premier ライセンスが必要です。

エンドポイント スクリプト ウィザード

エンドポイント スクリプト ウィザードを使用すると、接続されているエンドポイントでスクリプトを実行して、組織の要件に準拠した管理タスクを実行できます。これには、使用されていないソフトウェアのアンインストール、プロセスやアプリケーションの開始または終了、特定のサービスの有効化または無効化などのタスクが含まれます。

ビジネス成果：接続されたエンドポイントで管理タスクを簡単に実行し、組織の要件に準拠します。

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 リリース 3.0 は、次の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-3515-K9（小規模）	アプライアンスハードウェアの仕様については、『*Cisco Secure Network Server* アプライアンスハードウェアの設置ガイド』を参照してください。
Cisco SNS-3595-K9（大規模）	
Cisco SNS-3615-K9（小規模）	
Cisco SNS-3655-K9（中規模）	
Cisco SNS-3695-K9（大規模）	

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

注意

- Cisco ISE 3.1 以降のリリースは、Cisco Secured Network Server（SNS）3515 アプライアンスをサポートしていません。
- Cisco SNS 3400 シリーズ アプライアンスは、Cisco ISE リリース 2.4 以降ではサポートされていません。
- 16 GB 未満のメモリの割り当ては、VM アプライアンスの設定ではサポートされていません。Cisco ISE の動作に問題が発生した場合、すべてのユーザーは、Cisco Technical Assistance Center に連絡する前に割り当てメモリを 16 GB 以上に変更する必要があります。
- レガシー アクセス コントロール サーバー（ACS）およびネットワーク アクセス コントロール（NAC）アプライアンス（Cisco ISE 3300 シリーズを含む）は、Cisco ISE リリース 2.0 以降ではサポートされていません。

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。

- VMware ESXi 5.x、6.x、7.x
  - Cisco ISE は、VMware ESXi 6.5 を搭載したCisco HyperFlex HX シリーズで検証済みです。
  - 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 1.5.3-160 上の KVM
- Nutanix AHV 20201105.2096

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。

（注） Cisco ISE リリース 3.0 以降、Cisco ISE 仮想マシンをホストする仮想化プラットフォームの CPU は、ストリーミング SIMD 拡張（SSE）4.2 手順セットをサポートしている必要があります。そうでない場合、特定の ISE サービス（ISE API ゲートウェイなど）が機能せず、Cisco ISE GUI を起動できません。2011 年以降は、Intel プロセッサと AMD プロセッサの両方が SSE バージョン 4.2 をサポートしています。

連邦情報処理標準（FIPS）モードのサポート

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

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

- すべての FIPS 非準拠暗号スイートは無効になります。

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

対応ブラウザ

管理者ポータルでサポートされているブラウザは次のとおりです。

- Mozilla Firefox 96 以前のバージョン（バージョン 82 以降）
- Mozilla Firefox ESR 91.3 以前のバージョン
- Google Chrome 97 以前のバージョン （バージョン 86 以降）
- Microsoft Edge の最新バージョンと最新バージョンより 1 つ前のバージョン

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 [12]	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 [3]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019 [4]	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
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
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	

外部 ID ソース	バージョン
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 OCSP 機能は Microsoft Windows Active Directory 2008 以降でのみ使用できます。

[2] 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
```

[3] 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。

[4] 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 は、OpenSSL 1.0.2.x（CiscoSSL 6.0）を使用して検証されます。

既知の制限事項と回避策

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

誤ったハッシュ値が原因で SNMP ユーザーの認証がアップグレード後に失敗する可能性

Cisco ISE 2.7 以前のリリースから Cisco ISE 3.0 にアップグレードする場合は、アップグレード後に SNMP ユーザーの設定を再設定する必要があります。そうしないと、誤ったハッシュ値が原因で SNMP ユーザーの認証が失敗する可能性があります。

SNMPv3 ユーザーの設定を再設定するには、次のコマンドを使用します。

no snmp-server user <*snmp user*> <*snmp version*> <*auth password*> <*priv password*>

snmp-server user <*snmp user*> <*snmp version*> <*auth password*> <*priv password*>

日本語のオンラインヘルプ

Cisco ISE で日本語を有効にするようにローカリゼーションを設定している場合は、オンラインヘルプにこのリリースで導入された新機能に関する情報が含まれていないことに注意してください。これらの機能の詳細については、『*Cisco ISE リリース3.0 管理者ガイド*』を参照してください。

認証の Radius ログ

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

アップグレード後の LDAP サーバーの再設定

制限事項

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

条件

[Connection] ウィンドウで [Specify server for each ISE node] オプションを有効にした場合。このウィンドウを表示するには、[メニュー（Menu）] アイコン（☰）をクリックして選択します **[Administration]** > **[Identity Management]** > **[External Identity Sources]** > **[LDAP]** > **[Add]** の順に選択します。または既存のサーバーを選択した後、PSN がある Cisco ISE 展開をアップグレードすると、展開 ID がリセットされる傾向があります。

回避策

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

有効なユーザーエージェントヘッダー

Cisco ISE では、Cisco ISE リリース 2.7 以降、Cisco ISE スポンサーポータルなどの Cisco ISE エンドユーザー向けポータルで正常な応答またはリダイレクト応答を受信するため、Web 要求で送信される有効なユーザーエージェントヘッダーが必要です。

応答ステータス行

Cisco ISE リリース 2.7 以降、Cisco ISE Web サービスおよびポータルは、HTTP バージョンとステータスコードのみを含む応答ステータス行を返しますが、対応する理由フレーズは返しません。

Trustsec AAAサーバーリストのサーバー IP の更新

Cisco ISE インスタンスの IP アドレスを CLI を使用して変更すると、Cisco ISE サービスは再起動されます。サービスが起動した後、Trustsec AAA サーバーの IP アドレスを変更する必要があります。Cisco ISE GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。**[ワークセンター（Workcenters）]** > **[TrustSec]** > **[コンポーネント（Components）]** > **[Trustsec サーバー（Trustsec Servers）]** > **[TrustSec AAAサーバー（Trustsec AAA Servers）]** を選択します。

アップグレード情報

- ライセンスの変更 （14 ページ）
- アップグレード手順の前提条件

リリース 3.0 へのアップグレード

次の Cisco ISE リリースからリリース 3.0 に直接アップグレードできます。

- 2.4
- 2.6
- 2.7

Cisco ISE リリース 2.4 より前のバージョンの場合は、はじめに上記のリリースのいずれかにアップグレードしてから、リリース 3.0 にアップグレードする必要があります。

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

Cisco ISE リリース 3.0 には、Cisco ISE パッチリリース（2.4 パッチ 13、2.6 パッチ 7、2.4 パッチ 10、および 2.7 パッチ 2）とのパリティがあります。

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 から入手できます。

ライセンスの変更

Cisco ISE リリース 2.x に使用されている Base、Plus、Apex などのライセンスが新しいライセンスタイプに置き換えられました。Cisco ISEリリース 3.0 では、Essentials、Advantage、Premier のライセンスを使用します。『*Cisco Identity Services Engine* 管理者ガイド』の「ライセンス」の章を参照してください。

Cisco ISE リリース 3.0 でライセンスの消費を有効にするには、Cisco Smart Software Manager（CSSM）を使用して既存のスマートライセンスか従来のライセンスを新しいライセンスタイプに変換する必要があります。

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。

テレメトリ

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

テレメトリは、Cisco ISE のステータスと機能に関する貴重な情報を提供します。シスコは、Cisco ISE を導入した IT チームのアプライアンス ライフサイクル管理を改善するためにテレメトリを使用します。このデータを収集することで、製品チームは顧客により優れたサービスを提供できるようになります。このデータと関連する分析情報により、シスコは潜在的な問題をプロアクティブに特定し、サービスとサポートを改善し、ディスカッションを促進して新規お

よび既存の機能からより多くの価値を収集し、IT チームによるライセンス権限のインベントリレポートと今後の更新を支援します。

Cisco ISE でテレメトリ機能が無効になり、テレメトリデータの共有が停止するまでに最大 24 時間かかる場合があります。

収集されるデータのタイプには、製品使用状況テレメトリや Cisco Support Diagnostics などがあります。

Cisco Support Diagnostics

Cisco Support Diagnostics Connector は、Cisco Technical Assistance Center（TAC）とシスコのサポートエンジニアがプライマリ管理ノードから展開の情報を取得するのに役立つ。デフォルトでは、この機能は無効になっています。この機能を有効にする手順については、『Cisco Identity Services Engine 管理者ガイド』を参照してください。

Cisco ISE ライブアップデートポータル

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

デフォルトのアップデートポータル URL にアクセスできず、ネットワークにプロキシサーバーが必要な場合は、プロキシを設定します。ライブアップデートポータルにアクセスする前に、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）] の順に選択します。Cisco ISE GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。プロキシ設定でプロファイラ、ポスチャ、およびクライアント プロビジョニング フィードへのアクセスが許可されている場合、Cisco ISE は MDM 通信のプロキシサービスをバイパスできないため、モバイルデバイス管理（MDM）サーバーへのアクセスがブロックされます。これを解決するには、MDM サーバーとの通信を許可するようにプロキシサービスを設定できます。プロキシ設定の詳細については、『Cisco Identity Services Engine Administrator Guide』の「Specify Proxy Settings in Cisco ISE」の項を参照してください。

クライアント プロビジョニングとポスチャのライブアップデートポータル

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

Cisco ISE GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。**[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアアップデート（Software Updates）] > [クライアント プロビジョニング（Client Provisioning）]**。

次のソフトウェア要素は、次の URL から入手できます。

- Windows および Mac OS X ネイティブサプリカント向けのサプリカント プロビジョニング ウィザード

- 最新の Cisco ISE の永続的なエージェントおよび一時的なエージェントの Windows バージョン
- 最新の Cisco ISE の永続的なエージェントの Mac OS X バージョン
- ActiveX および Java アプレット インストーラ ヘルパー
- AV/AS コンプライアンス モジュール ファイル

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

次の場所からポスチャ更新をダウンロードできます。

Cisco ISE GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。 **[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアアップデート（Software Updates）] > [ポスチャ更新（Posture Updates）]**

次のソフトウェア要素は、次の URL から入手できます。

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

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

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

Cisco ISE オフライン更新

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

オフラインのクライアント プロビジョニング リソースをアップロードするには、次の手順を実行します。

手順

ステップ 1 https://software.cisco.com/download/home/283801620/type/283802505/release/3.0.0に進みます。

ステップ 2 ログインクレデンシャルを入力します。

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

次のオフライン インストール パッケージをダウンロードできます。

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

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

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

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

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

オフラインのポスチャ更新をダウンロードするには、次のようにします。

手順

ステップ 1 https://www.cisco.com/web/secure/spa/posture-offline.htmlに進みます。

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

ステップ 3 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）]。Cisco ISE GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。

ステップ 4 矢印をクリックすると、ポスチャの設定が表示されます。

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

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

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

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

ステップ 8 [今すぐ更新（Update Now）] をクリックします。

設定要件

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

Cisco ISE を設定するには、次のリソースを参照してください。

- Getting started with Cisco ISE
- YouTube の Cisco ISE チャンネルのビデオ
- *ISE* セキュリティ エコシステム統合ガイド
- *Cisco Identity Services Engine* 管理者ガイド

モニタリングおよびトラブルシューティング

システムのモニタリングおよびトラブルシューティングに関する詳細については、『*Cisco Identity Services Engine* 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。

発注情報

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

Cisco ISE と Cisco Digital Network Architecture Center との統合

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

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

Cisco AI エンドポイント分析

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

Cisco AI エンドポイント分析は、人工知能（AI）と機械学習機能を使用して、同様の属性を持つエンドポイントを直感的にグループ化します。IT 管理者は、これらのグループを確認してラベルを割り当てることができます。割り当てられたエンドポイントラベルは、Cisco ISE アカウントがオンプレミスの Cisco DNA Center に接続されている場合、Cisco ISE で使用できます。

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

新しいパッチのインストール

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

システムへのパッチの適用方法については、『Cisco Identity Services Engine 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 リファレンスガイド*』の「Patch Install」セクションを参照してください。

（注） Cisco ISE リリース 3.0 パッチ 2 以降のリリースでは、SSM オンプレミス接続方式のライセンス機能がサポートされています。この機能を有効にした後、Cisco ISE 3.0 パッチ 1 以前にロールバックする必要がある場合は、ライセンス機能を含むパッチをアンインストールする前にライセンス機能を無効にする必要があります。

ルート CA 証明書の自動再生成

Cisco ISE リリース 3.0 パッチ 6 以降では、新しいパッチをインストールするときにルート CA 証明書を再生成する必要があります。

- スタンドアロンノードでは、CLI または GUI を使用してパッチをインストールすると、ルート CA 証明書が自動的に再生成されます。

- 分散型展開では、CLI を使用してパッチをインストールする場合、パッチのインストール後にルート CA 証明書を再生成する必要があります。Cisco ISE GUI を使用してパッチをインストールすると、ルート CA 証明書が自動的に再生成されます。

Cisco ISE リリース 3.0 パッチ 6 以降のリリースから Cisco ISE リリース 3.0 パッチ 5 以前のリリースにロールバックする場合は、ロールバックする Cisco ISE リリースでルート CA 証明書を再生成する必要があります。

ルート CA 証明書を生成する方法については、『Cisco ISE Administrator Guide』の「Basic Setup」の章の「Generate Root CA and Subordinate CAs on the Primary PAN and PSN」のトピック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。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、現在のリリースに適用され、Cisco ISE 3.0 よりも前のリリースにも適用されている可能性のある未解決の不具合が記載されています。これまでのリリースで未解決で、まだ解決されていない不具合は、解決されるまで、今後のすべてのリリースに適用されます。

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

Cisco ISE リリース 3.0 の新機能：累積パッチ 7

Cisco Secure Client の延長サポート

Cisco ISE 3.0 パッチ 7 は、Windows、MacOS、Linux オペレーティングシステム用の AnyConnect（バージョン 4.10.5075 以降）と Cisco Secure Client の両方をサポートしています。これらのオペレーティングシステムでは、次の Cisco Secure Client バージョンがサポートされています。

- Windows：Cisco Secure Client バージョン 5.00529 以降
- MacOS：Cisco Secure Client バージョン 5.00556 以降
- Linux：Cisco Secure Client バージョン 5.00556 以降

これらのオペレーティングシステムではエンドポイントに対して AnyConnect と Cisco Secure Client の両方を構成できますが、エンドポイントでの実行時に考慮されるのは 1 つのポリシーのみです。

Cisco ISE リリース 3.0 の解決済みの不具合：累積パッチ 7

次の表に、リリース 3.0 累積パッチ 7 の解決済みの不具合を示します。

問題 ID 番号	説明
CSCwc71060	削除されたネットワーク デバイス グループがポリシーセットに引き続き表示される
CSCwc51239	[Make a Wish] リンクの場所を新しい場所に更新
CSCwd10864	XML 外部エンティティ インジェクションの脆弱性
CSCwd30994	Gig 0 以外のインターフェイスのゲートウェイを使用した静的デフォルトルートにより、ネットワーク接続が切断される
CSCwc61320	[Download Logs] ページがバックグラウンドで読み込まれるため、[Support Bundle] ページの読み込みが遅くなる
CSCwc09435	携帯電話番号フォーマットのエラー処理/メッセージが明確でない
CSCwc24126	[Profiler Condition] に [Attribute Value] が表示されない
CSCwc57294	設定の読み取りに例外がある場合、Duplicate Manager でパケットが削除されない
CSCwc00162	クライアントまたはブラウザから複数の証明書が送信されると、証明書ベースの管理者ログインが機能しない
CSCwd27506	ISE 3.0 パッチ 6：スケジュールされたレポートが欠落している
CSCvw51787	ISE で、自己署名証明書の上への CA 署名付き証明書のインポートが許可されない
CSCwc30811	ゲストポータルでアンダースコアが脆弱である
CSCwb24002	ERS SDK の認証設定が API コールを介して無効化されていない
CSCwd94235	31p5：アプリサーバーと API ゲートウェイサービスが実行されない
CSCwc52685	ENH：SMS ゲートウェイ用の Twilio MessagingServiceSid を使用した ISE
CSCwb56878	複製停止アラームはトリガーされない
CSCwb55232	ERS API を使用してネストされたエンドポイントグループを作成する
CSCvv87286	ISE 2.7P2 ～ 3.0 で内部 CA とキーをインポートできない

問題 ID 番号	説明
CSCwc64346	ERS SDK ネットワークデバイスの一括要求のドキュメントが正しくない
CSCwc30019	CIAM：openssl 1.0.2n
CSCwd42311	GUI のダウンロードログから rest-id-store をダウンロードできない
CSCwc12303	インスタンスが使用する PGA メモリが MNT ノードで PGA_AGGREGATE_LIMIT を超えている
CSCwc31482	NetworkSetupAssistance.exe デジタル署名証明書が Windows SPW を使用した BYOD フローで期限切れになる
CSCwc74531	毎時 cron では、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がクリーンアップされる必要がある
CSCwc91917	TACACS 認証プロファイルに引用文字を追加できない
CSCwd71574	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
CSCwc21890	専用 MnT ノードを使用する ISE でパッシブ Easy Connect が機能しない
CSCwb29498	高稼働時の DB 使用率アラームのパーセンテージを設定可能にする必要がある。
CSCwc69492	メタスペースを使い果たすと ISE ノードでクラッシュが発生する
CSCwb75959	保存されたクロスサイト スクリプティングの脆弱性
CSCwc87670	SAML が使用されている場合、ISE 3.1 パッチ 3 で csv ファイルからエンドポイントをインポートできない
CSCwb82141	復元操作後に、コンテキストの可視性のエンドポイントと NAD が既存の展開から削除されない
CSCwc72251	アカウンティング終了のために変更された pxGrid パブリッシング
CSCwc18751	DomainName\UserName 形式を使用してログインしている場合、作成したサポートバンドルを GUI からダウンロードできない
CSCvy32277	ポート 8084 で TLSv1.1 が有効になっている
CSCwd03009	2.7 p7 の platform.properties でハードウェアアプライアンスに基づいて制御する RMQForwarder スレッド
CSCwb52396	PRA フェールオーバー
CSCwc59570	SXP バージョン 4 で、ISE から 4,096 バイトのサイズの SXP メッセージが送信される

問題 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
CSCvz57222	ISE 3.0：セカンダリインターフェイス GigabitEthernet 1 および Bond 1 で ISE GUI に管理アクセスが許可される
CSCwc75572	3.2：Maxscale：PPAN アプリケーションサーバーが初期化状態でスタックする
CSCwd45843	GC 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
CSCwc74206	新しいインスタンスの使用時に機能する、新しいパスワードを持つSCCM MDM サーバーオブジェクトが ISE 3.0 で保存されない
CSCwb88851	VN 値が変更されている場合、複数の再認証後に IP から SGT へのマッピングの一貫性がなくなる
CSCwb26965	ISE 3.1：REST API を介してネットワーク デバイス グループを作成中にエラーが発生する
CSCwc57939	ISE が大規模な VM をサポート対象外として検出する
CSCwc62413	クロスサイト スクリプティングの脆弱性
CSCwb79056	ISE 3.1 ERS コール /ers/config/sgmapping/{id} でカスタム SGT の SGT 値が返されない
CSCwc98828	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
CSCwc07283	ISE 3.1：[Context Visibility Endpoint Authentication] タブにデータが表示されない
CSCwc98823	コマンドインジェクションの脆弱性
CSCwc57240	カスタム属性の追加中に GUI でデフォルト値が検証されない
CSCwb59162	SNMP パスワードパラメータの ISE 3.1 REST API のタイプミス
CSCwc26241	ISE 3.2 で次のエラーが表示される：「TypeError：未定義のプロパティを読み取れません（「attr」の読み取り）（TypeError: Cannot read properties of undefined (reading 'attr')）」
CSCwa95889	新しいホストキーアルゴリズム（rsa-sha2-512 など）を使用したホストに SSH/SFTP を追加できない
CSCwb26227	CIAM：jackson-databind 2.9.8
CSCwb88360	アップグレードされたノードで一時的な MnT ペルソナを無効化すると、分割アップグレードで失敗する

問題 ID 番号	説明
CSCwb85456	CIAM：openssl を 1.0.2ze および 1.1.1o にアップグレード
CSCwc65802	SAML 構成の保存ボタンがグレー表示される
CSCwc12693	ERS 検証エラー：必須フィールドの欠落：[validDays]
CSCwb91392	サードパーティの CA 証明書が管理者用に使用されている場合、ヘルスチェックとフルアップグレードの事前チェックがタイムアウトする
CSCwc65711	MAC：CSC 5.0554 Web 展開パッケージのアップロードに失敗する
CSCwc09104	認証 VLAN を使用したゲストリダイレクトが ISE 3.1 で機能しなくなった
CSCvv10712	Sec_txnlog_master テーブルは、レコード数が 200 万を超えたら切り捨てる必要がある
CSCwb86283	不正な証明書の有効期限チェックの結果として、すべてのノードから OUT_OF_SYNC がスローされる
CSCvx49736	containerd.io RPM パッケージ openssl 1.0.2r CIAM CVE-2021-23841 + その他
CSCwc64275	PPAN の ise-psc.log でオプティミスティックロックが失敗すると、事前チェックがタイムアウトすることがある
CSCwc98833	クロスサイト スクリプティングの脆弱性
CSCwc98831	保存されたクロスサイト スクリプティングの脆弱性
CSCwb47255	サポートされる HTTP メソッドが表示される
CSCwd74560	Digital Network Architecture Center から ISE（ERS）へのペイロードでの PUT 操作が失敗する
CSCwc42712	ISE RADIUS および PassiveID セッションのマージ
CSCwc15013	有用性を追加し、ISE 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
CSCwd31405	Session.PostureStatus のクエリ中に遅延が発生する
CSCvz65945	非 TACACS トラフィックのライブログ内の「無効な長さ」による TACACS 認証の失敗
CSCwc85867	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
CSCwb27894	EAP-TLS を使用した EAP-TEAP が「CERTIFICATE.Issuer - Common Name」を持つ条件に一致しない

問題 ID 番号	説明
CSCvz91479	3.1 および 3.2.0.804 のアップグレードに関する制約を変更中にスキーマのアップグレードが失敗する
CSCwb81416	ISE 3.1 GUI がログイン後にロードされない
CSCwc23593	LSD によって CPU が高くなる
CSCwc93451	プロファイラは、デフォルトの RADIUS プローブからの転送について、否定的な RADIUS Syslog メッセージを無視する必要がある
CSCvv54351	RADIUS を使用したデバイス管理が基本ライセンスを使用しない
CSCwa59924	ISE から FIPS 対応デバイスへの SSH が機能しない
CSCwc44614	[Network Devices] の [Export Selected] を使用し、X 回以上選択するとログイン画面が中断される
CSCwc27765	SYS_EXPORT_SCHEMA_01 が原因で ISE 設定のバックアップが失敗する
CSCwb62192	ISE インデックスエンジンのバックアップが失敗するとスケジュール済みバックアップが失敗する
CSCwc65821	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
CSCwa37580	ISE 3.0 NFS 共有がスタックする
CSCwb84779	親 ID グループ名を変更すると、認証リファレンスが壊れます
CSCwc80574	結合操作中に ISE AD コネクタでエラーが発生する
CSCwc51219	RADIUS 共有秘密の先頭に += 文字がある場合、CSV NAD インポートが拒否される
CSCwd13555	サードパーティ Syslog サーバーからの PassiveID セッションの使用を ISE が突然停止する
CSCwd24304	ISE 3.2 ERS POST /ers/config/networkdevicegroup が失敗する：破損した属性 othername/type/ndgtype
CSCwb84440	エンドポイントグループの削除後にスポンサーポータルが中断する
CSCvx94685	CIAM：rpm 4.11.3 CVE-2021-20271
CSCwc39844	eth 1 での IP アドレスの変更中に、ISE 3.1 サービスの自動再起動が内部エラーで失敗する
CSCwa55866	シングル接続が有効になっていると、TACACS 応答が送信されないことがある

問題 ID 番号	説明
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）」と表示される
CSCwb93156	TrustCertQuickView がすべての信頼できる証明書について同じ情報を提供する
CSCwc60997	ISE での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	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
CSCwd32758	名前を変更後、[Export Summary] ページでリポジトリ名が更新されない
CSCwc30643	CRUD を実行しないと、ノードのリロード後に [My Devices] ポータルが開かない
CSCwc11613	証明書署名要求では大文字と小文字を区別すべきでない

Cisco ISE リリース 3.0 の未解決の不具合：累積パッチ 7

Cisco ISE リリース 3.0 パッチ 7 には未解決の不具合はありません。

Cisco ISE リリース 3.0 の解決済みの不具合：累積パッチ 6

ID	見出し
CSCwa80359	CIAM：sqlite 3.7.17
CSCwb09045	正しくない cryptoLib 初期化が原因で Cisco ISE PSN ノードがクラッシュする
CSCwb22662	64 文字の制限は、ユーザープリンシパル名などの外部ユーザー ID に対応するには小さすぎる
CSCwa80547	CIAM：unixodbc 2.3.0
CSCwa37040	ISE CLI の公開キー暗号化を使用するバックアップログで、コアファイルのキャプチャが許可されない
CSCwb64656	ISE GUI で Essential ライセンスが無効になっている場合、スマートライセンスポータルがライセンスの使用を報告しない。
CSCwa61347	ISE-PIC が特殊文字で始まるライブセッションを転送しない
CSCwa96229	ISE で、ユーザーが現在のパスワードを検証せずに管理者パスワードを変更可能

ID	見出し
CSCwb36849	ISE で空の Cisco AV-Pair を access-accept パケットで送信しないようにする必要がある
CSCwb29140	nss rpm が更新された最新のパッチに移行した後、スレッドが使い果たされる（3.0p5 と 2.7p7、3.1P1 のみ）
CSCvz95478	P5 のインストール後、ISE 2.7 EST サービスが実行されず、CA サービスが初期化状態でスタックする
CSCwa35293	ISE 2.7：認証成功設定が成功/成功 URL を示す
CSCwb39964	ISE で外部 ID ソースを持つ無効なシャドウ管理アカウントを使用して GUI にログインできる。
CSCwa80553	CIAM：samba 4.8.3
CSCwb53455	内部 Docker IP 169.254.2.2 に関連する RMQ TLS syslog が監査ログに送信される
CSCwa53499	[コネクタ設定（connector settings）] ページが開くと、REST ID がクラウドからグループを取得する
CSCwa78479	CVE-2021-4034 Polkit の Cisco Identity Services Engine 評価
CSCwa55996	条件スタジオに新しいオブジェクトが存在しない
CSCwb14106	CIAM：cyrus-sasl 2.1.27
CSCwa16401	Get-By-Id サーバーシーケンスが GUI を介してシーケンスで最初の変更を行った後に空のサーバーリストを返す
CSCwa48465	複数の値を持つフィールドの処理ミスが原因でレポートが使用できない
CSCvx54894	スポンサーポータル管理者が 60 分/1 時間以下のランダムゲストアカウントを作成できない
CSCwa89443	DNA Center - ISE 統合：ISE で pxGrid エンドポイントの古い DNAC 証明書が表示される
CSCvx58736	3.1：Maxscale：/opt/CSCOcpm/prrt/diag/bin/diagRunner によって生成されたコアが開始される
CSCwa97123	2 つ以上の NTP サーバーが設定されている NTP 同期エラーアラーム。
CSCwa40040	セッションディレクトリの書き込みに失敗する。SQLException：ISE3.0P4 で文字列データの右側が切り捨てられる
CSCwa80710	CIAM：jszip 2.5.0

ID	見出し
CSCwa06912	認証ポリシーに日時条件がある Tacacs+ 要求で高遅延が発生する
CSCwb33727	ISE 3.1：属性の特殊文字がサポートされていない
CSCvz75902	ISE 内部 CA の生成時に ISE が pxGrid 証明書を置き換える
CSCwa57705	IP-SGT マッピングが新しいネットワークアクセスのデバイスグループとリンクしない
CSCwa80520	CIAM：libpng 1.6.20
CSCwa80679	CIAM：net-snmp 5.7.2
CSCwb61614	ゲストユーザー（AD または内部）が特定のノードで自分のデバイスを削除または追加できない
CSCwa33462	RADIUS 共有シークレットの先頭にある特殊記号 @ により、CSV NAD インポートが拒否される
CSCvz85074	CSCvu35802 の修正により、EAP チェーンのアイデンティティとして証明書属性をもつ AD グループの取得が中断される
CSCwb27857	ISE 3.0 P5：分散型展開で RSA 2FA を使用して MnT ノードの GUI にログインできない
CSCwa94984	長いカスタム属性文字列を使用した ISE API のユーザー追加操作に、Curl を使用して 4 分かかる
CSCwa13696	ISE 3.1 ゲストのユーザー名/パスワードポリシーを変更できない
CSCwa23207	メモリ割り当ての不整合が原因で複数のランタイムがクラッシュする
CSCwa47190	ポスチャポリシーで AD セキュリティグループの OU の末尾をドット文字にできない
CSCwa76896	RADIUS 認証レポートの「エラーの理由（Failure Reasons）」列が重複する
CSCwc06638	3.0P6：パッチロールバックおよびパッチインストール後にシステムサマリーが更新されない
CSCwa95892	間違った期間を示す ui_time_left 変数
CSCwb19256	Pingnode 呼び出しにより、CRL 検証中にアプリサーバーがクラッシュする（OOM は除く）
CSCwa57955	ポスチャファイアウォールの修復アクションを変更できない

ID	見出し
CSCwa17925	失敗したアップグレード前チェックを修正しても、[続行（Proceed）] ボタンが使用できない
CSCwa25731	レポートで過去 7 日間のフィルタが機能しない
CSCwb21669	オンプレミス SSM サーバーの IPv6 アドレスを入力できない
CSCwa49859	属性値 dc-opaque がライブログの問題を引き起こす
CSCwa80484	CIAM：nss 3.44.0
CSCvy91805	ISE での EAP-FAST-Chaining で最大セッション数が適用されない
CSCwa83517	電子メールアドレスにアポストロフィが含まれている場合、ゲストポータル登録ページで「ページの読み込みエラー」が表示される
CSCwb34910	ISE ポータルでのゲスト SMS 通知の複数行の問題
CSCwa04454	ISE 3.0 および 3.1：デバイス管理ライセンスだけですべての TACACS 必須メニューへのアクセスが許可される必要がある
CSCwa26210	「GET /ers/config/radiusserversequence」API の JSON 応答に nextPage フィールドがない
CSCwa20309	「不明なNAD（Unknown NAD）」および「正しく設定されていないネットワークデバイスを検出（Misconfigured Network Device Detected）」アラーム
CSCwa80501	CIAM：perl 5.16.3
CSCwa18443	展開ノードのエンドポイントに 8 オクテット MAC が存在する場合、ポスチャの有効期限を処理する必要がある
CSCwb09861	CIAM：glib 2.56.4
CSCwa79799	sysodbcini ファイルに PermSize 属性がない
CSCwa15191	EP が不明なポスチャでスタックする：MAC で LSD のセッションが見つからない
CSCwa97357	ISE が SMTP API 本文で $mobilenumber$ 値を送信しない
CSCwa13877	ISE スマートライセンス認証更新の失敗：詳細 = ライセンスクラウドからの無効な応答
CSCwa46758	削除されたルート ネットワーク デバイス グループがネットワークデバイスでエクスポートされた CSV レポートで引き続き参照されている
CSCvz43123	CIAM：jspdf 2.3.0

ID	見出し
CSCwb67934	CIAM：openjdk - 複数のバージョン
CSCwa90930	3.x の RMQ にハード Q キャップが必要
CSCvz24558	Spring Hibernate TPS アップグレード（Hibernate 5.5.2、Spring 5.3.8）
CSCwa75348	ODBC 動作のフェールオーバーの問題
CSCwb04898	名前にスペースを含むグループがファイルを所有している場合、Linux SFTP リポジトリから CFG バックアップを復元できない
CSCvz94133	「EDF_DB_LOG」が原因で構成バックアップが失敗する
CSCvs55875	MTU の変更後、既存のルートがルーティングテーブルにインストールされない
CSCwa47566	ISE 条件スタジオ - [IDグループ（Identity Groups）] ドロップダウンを 1000 個に制限
CSCwa20152	マトリックスが変更されていないスイッチの ISE で CoA が開始されなかったため、ポリシーの同期に失敗した
CSCwb05532	「場所」と「デバイスタイプ」の場所が、[ネットワークデバイス（Network Devices）] > [追加（Add）] をクリックするたびに交換される
CSCwa91335	パッシブ Syslog プロバイダーのデフォルトのドメイン構成が ISE 3.1 で機能しない
CSCwb40349	ISE 3.X：外部 RADIUS トークン共有秘密の無効な文字。
CSCwb01854	3.0 に移行後、外部 RADIUS サーバーのアップグレードリストが表示されない
CSCwa43187	ISE キューリンクエラー：Message=From Node1 To Node2、Cause=Timeout in NAT'ed deployment
CSCwa59924	ISE 3.1 パッチ 1：SSH：FIPS：エラー：Xkey_sign：無効なダイジェスト
CSCvw90778	展開ページでデバイスの管理プロセスを無効にしても、T+ ポート（49）が開いている
CSCwb03231	テーブルが見つからないため、p5 または p6 をインストールするとアプリケーションサーバーが初期化中にスタックする
CSCwa52110	ネットワークデバイスに設定された SNMP 構成で SNMP レコードの処理中に 20 秒の遅延が発生する
CSCwb41741	ISE：管理者グループの無効な文字エラー

ID	見出し
CSCwb32466	ISE 3.1：説明が設定されていない場合、REST API を介して作成されたエンドポイント ID グループを削除できない
CSCwa59237	200 以上の内部証明書を持つ PAN ノードで、Deployment-RegistrationPoller がパフォーマンスの問題を引き起こす
CSCvw74930	CIAM：kafka CVE-2019-12399
CSCwb40942	電子メールの送信元アドレスが .com または .net で終わっていない場合は無効になる
CSCwa32814	15 のコレクションフィルタが設定された ISE で 15 番目のフィルタが非表示になる
CSCwa60873	PAN のパフォーマンスを向上させるために bouncy-castle クラスを最適化する
CSCwb11147	VN を使用した SGT-IP マッピングの競合処理で必要なログの改善
CSCwa77161	3.0P5 -> 3.0P3 で PLR が返される
CSCwa27766	ISE 3.0 P4 でのバックアップの復元後にコンテキストの可視性が壊れる
CSCwb23028	パスワードの不正確な辞書の単語評価
CSCwb03479	hotpatch.log をサポートバンドルに含める必要がある
CSCwa16291	ゲストポータルのボタンのテキスト要素により、Apple VoiceOver の単語が繰り返される
CSCwb01843	DST/TZ が自動的に更新される
CSCvz92898	管理者ログイン時の SCM js ファイルのブラウザダウンロード
CSCwb29357	ISE 3.0 の 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
CSCwa82247	ISE キューリンクエラー：ISE iptables の 169.254.2.0/25 による Cause=Timeout
CSCwb75964	ISE 3.0：PAN 自動フェールオーバーアラームを編集できない
CSCwb07504	ユーザー ID グループに基づいた内部ユーザーの並べ替えが、[IDの管理（Identity Management）] > [ID] で機能しない
CSCvw85860	ISE pxGrid の例外のログレベルは DEBUG ではなく ERROR である必要がある
CSCwa56771	ISE 3.0p2：[すべてをモニター（Monitor All）] 設定が複数のマトリックスと異なるビューで正しく表示されない

ID	見出し
CSCwa60903	ISE で、CRL の nextUpdate の日付に 6 時間追加される
CSCwa41166	T+ コマンドの安全でない文字が 16 進数の文字参照に格納される
CSCwa47221	クライアント プロビジョニング ポリシーの AD セキュリティグループで OU の末尾をドット文字にできない
CSCvk25808	スケジュール設定されたレポートを作成した管理者が利用できなくなった場合、そのスケジュール設定されたレポートを編集または削除できない
CSCwa56934	エンドポイントグループに対する ERS API の並べ替えが一貫していない
CSCwa80477	CIAM：dom4j 1.6.1
CSCwb40131	Rest API を使用して外部パスワードタイプで内部ユーザーを有効にしているときに 400 Bad Request が発生する
CSCwa11633	ISE 3.0：APIC 統合：secGroup を作成できない
CSCwb32492	プライマリ PAN の管理証明書を変更した後、すべてのノードでアプリケーションサーバーが再起動する
CSCvz88327	PAN での CA の初期化中、ルート CA の再生成が「メッセージが定義されていません」というエラーで失敗する
CSCwa59621	ID グループに対する ERS API の並べ替えが一貫していない

Cisco ISE リリース 3.0 の未解決の不具合：累積パッチ 6

ID	見出し
CSCwc25830	[Open New Case] ウィンドウのフォーマットが正しく表示されません。

Cisco ISE リリース 3.0 の新機能：累積パッチ 5

Microsoft Graph の更新による Microsoft Intune の統合の変更

Microsoft は Azure Active Directory（Azure AD）Graph を廃止しており、2022 年 6 月 30 日以降、Azure AD Graph 対応の統合をサポートしません。Azure AD Graph を使用するすべての統合を Microsoft Graph に移行する必要があります。Cisco ISE は通常、エンドポイント管理ソリューション Microsoft Intune との統合に Azure AD Graph を使用します。

Azure AD Graph から Microsoft Graph への移行の詳細については、次のリソースを参照してください。

- Azure AD Graph アプリの Microsoft Graph への移行

- Azure AD Graph から Microsoft Graph への移行に関するよくある質問
- アプリケーションを Microsoft Authentication Library と Microsoft Graph API を使用するように更新する

Cisco ISE リリース 3.0 パッチ 5 は、Microsoft Graph を使用する Microsoft Intune 統合をサポートします。Cisco ISE と Microsoft Intune 間の統合の中断を回避するには、Cisco ISE を Cisco ISE リリース 3.0 パッチ 5 に更新します。次に、2022 年 6 月 30 日までに、Azure AD Graph の代わりに Microsoft Graph を使用するよう、Microsoft Azure の Cisco ISE 統合を更新します。Cisco ISE では、Microsoft Intune 統合を更新して、[自動検出URL（Auto Discovery URL）] フィールドを更新する必要があります。**https://graph.windows.net<*Directory (tenant) ID*>** を **https://graph.microsoft.com** に置き換えます。

設定手順の詳細については、「Connect Microsoft Intune to Cisco ISE as a Mobile Device Management Server」を参照してください。

Cisco ISE リリース 3.0 の解決済みの不具合：累積パッチ 5

問題 ID 番号	説明
CSCvo39514	コレクタログのアクセス許可が拒否されるため、MnT ログプロセッサが実行されない。
CSCvu58986	すべての ISE Syslog で「black list/blacklist」および「white list/whitelist」を適切な用語に置き換える。
CSCvz77905	Cisco Identity Services Engine RADIUS のサービス拒否の脆弱性
CSCvu94544	ISE 3.0 BH：TACACS ライブログにネットワークデバイス IP の選択オプションが表示されない
CSCvv43120	ISE-2.x：接続に関する Intune MDM アラーム || 401 未承認（401 Unauthorized）
CSCvv96532	DOC：ISE システム時間と OCSP 応答の間の最大時間差が不明。OCSP 応答の更新
CSCvw09460	/erc/config/authorizationprofile/{id} に対する PUT の更新されたフィールドリストは通常空になる
CSCvw65181	CIAM で POI の脆弱性が検出された
CSCvx43866	3.0P2：アカウンティングレポートのエクスポートの完了に時間がかかる
CSCvx48255	CIAM：画面 4.1.0 CVE-2021-26937
CSCvx59893	ISE の Syslog レベルとメッセージレベルの不一致
CSCvx98746	DOC：Windows のエージェントレス ポスチャ ドキュメントの要件が正しくない

問題 ID 番号	説明
CSCvy36887	TCP ポート 19444 が ISE 3.0 のみで開いている
CSCvy45345	マシン認証フラグが誤って「True」に設定されているため、EAP チェーン認証が失敗する
CSCvy53842	特定の証明書監査中に証明書の検証の Syslog メッセージが送信された - ISE
CSCvy56983	DOC：ISE：SAML 証明書は ISE 展開から削除すべきではない
CSCvy66537	ISE ドキュメントバグ：エージェントレスおよび一時的なポスチャの制限事項：説明が不完全
CSCvy71261	CIAM：nettle 3.4.1
CSCvy72028	ISE 2.7 パッチ 4 pxGrid の [サービス（Services）] > [すべてのクライアント（All Clients）] が java.lang.NullPointerException で終了する
CSCvy75191	Cisco Identity Services Engine の XML 外部エンティティ インジェクションの脆弱性
CSCvy82023	不適切なポスチャ複合条件のホットフィックス
CSCvy84989	POST /ers/config/internaluser/ の Cookie を有効にすると、「IDグループが存在しません（Identity Group(s) does not exist）」というエラーが発生する
CSCvy89317	ISE：DST ルート CA X3 認証局：2021 年 9 月 30 日で失効（90 日以内）
CSCvy92040	[ISE復元（ISE restore）] ポップアップメニューに誤ったテキストが表示される
CSCvy96761	EAP チェーンフローを実行して関連する ID を処理する際に、セッションキャッシュを更新する必要がある
CSCvz00034	ログ「この更新フィールドは現在の時刻よりも1週間以上前です（this update field is earlier than currunet time more than week）」のログレベルを変更する
CSCvz00617	PnSLongevity：3.0P3 で Longevity テストベッドのレプリケーション失敗エラーが発生する
CSCvz00706	「関心のあるグループ」が、改行が 1 つ入った単一文字列として返される
CSCvz07191	GUI アクセスに証明書ベースの認証を使用しているときに AD グループが存在しない場合、ISE GUI がロード中にスタックする
CSCvz17020	ISE GUI がすべてのライセンスをコンプライアンス違反として表示する：スマートライセンス
CSCvz18044	VN が作成者からリーダーに複製されない

問題 ID 番号	説明
CSCvz21417	CiscoSSL 1.0.2za を使用した ISE 3.0 以前のパッチのアップグレード
CSCvz22331	1 日の特定の時間（分）について時刻と日付の条件で設定されたポリシーで認証がブロックされない
CSCvz27791	ISE：MDM 設定が原因でバックアップの復元後にアプリケーションサーバーの初期化がスタックする
CSCvz28133	ユーザーがサポートバンドルを生成できない
CSCvz35550	MDM 検証時の ISE ヘルスチェックで誤ったアラームが発生する
CSCvz36192	/ers/config/downloadableacl を使用した DACL の GET で、存在する nextPage または previousPage が追加されない
CSCvz37241	キューリンクエラー：WARN:{socket_closed_unexpectedly;'connection.start'}
CSCvz37623	NTP（' - '）ソースの状態の説明が ISE CLI にない
CSCvz40708	NTP サーバーに到達する ISE が構成で定義されていない
CSCvz43183	「名前による」呼び出しの場合、スポンサーのアクセス許可がゲスト REST API に渡されない。
CSCvz44488	同じローカルユーザーが存在する場合、ISE 3.0 エージェントレスポスチャでドメイン認証が使用されない
CSCvz44655	ISE 管理アカウントの選択に関する問題
CSCvz46560	jquery v1.10.2 を使用する ISE が脆弱になっている
CSCvz46893	ISE ドキュメントの更新：Microsoft Intune 統合：権限
CSCvz46933	CIAM：jsoup 1.10.3
CSCvz48491	ISE CTS TLSv1.2 のサポート
CSCvz49871	ISE GUI：net::ERR_ABORTED 404 : /admin/ng/nls/fr-fr/
CSCvz50255	CIAM：bind 9.11.20
CSCvz55258	Cisco:cisco-av-pair AuthZ 条件の機能が停止した
CSCvz55293	セカンダリ PAN ISE ノードにより、プライマリ PAN ノードでサービスが再起動し、ドキュメントと一致しない
CSCvz56358	ISE 3.0 で最初の SAN エントリのみがチェックされる

問題 ID 番号	説明
CSCvz60870	TPS が高いときに Active Directory の遅延が大きいと、ADRT で HOL ブロッキングが発生する
CSCvz63405	ISE クライアントの pxgrid 証明書が DNAC に配信されない
CSCvz63643	ISE 2.7：EndpointPersister スレッドが停止する
CSCvz65057	[コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）] の [追加（Add）] ボタンをクリックして、[ゲスト（Guest）] タブを選択すると nullpoint エラーが発生する
CSCvz65576	CLI リポジトリまたはディスクリポジトリが使用されている場合、パッチでフルアップグレードが機能しない
CSCvz66279	7 日以上前の Radius レポートが空（CSCvw78289 の回帰）
CSCvz66577	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
CSCvz67479	すべてのフィールドの [ローカルログの設定（Local Log Settings）] ツールチップに、無関係で役に立たない「信頼できる証明書（Trust Certificates）」が表示される
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
CSCvz71284	SNMPv3 COA 要求が ISE 2.7 によって発行されない
CSCvz71872	CIAM：nss - 複数のバージョン
CSCvz72208	ISE 3.1：[認証（Authentication）] タブで、[コンテキストの可視性（Context Visivility）] に空白の結果が表示される
CSCvz72225	ディスカバリホストに FQDN を追加すると、ディスカバリホストの IP アドレスまたはホスト名が無効になる
CSCvz73445	エージェントレスポスチャがマルウェア対策チェックに合格しない
CSCvz74457	ERS API で「ネットワーク デバイス グループ」名にドット文字の使用または作成/更新が許可されていない
CSCvz77482	ISE 3.0 はゲストの自己登録ポータルの一部として「場所」設定を選択解除できません
CSCvz77836	登録された ISE での ISE 3.0 評価期限切れエラー
CSCvz80829	3.2 のフルアップグレードでバージョンの事前チェックが失敗する
CSCvz83204	ISE でポスチャフロー中に発生した不適切なインデックスから URL 属性値を取得できない

問題 ID 番号	説明
CSCvz83753	認証の高度な属性設定に含まれる空のユーザーカスタム属性により、誤った AVP が発生する
CSCvz85117	ISE ヘルスチェックの I/O 帯域幅パフォーマンスチェックで誤ったアラームが発生する
CSCvz86020	「開かれているファイルが多すぎます（too many files open）」というエラーにより、ライブログまたはセッションに最新のデータが表示されない
CSCvz87476	サポートされていないメッセージコード 91104 および 91105 アラーム
CSCvz88188	セッションキャッシュのユーザー名が null であるため、ユーザー名に対する TACACS 認証ポリシーのクエリ実行に失敗する
CSCvz90468	API フローを使用してユーザーを作成すると、外部パスワードストアを使用する内部ユーザーが無効になる
CSCvz91603	ISE を 3.0 パッチ 3 にアップグレードすると、ODBC から属性を取得できない
CSCvz93230	Gig0 とは異なるインターフェイスでホストされている場合に、ゲストポータルがロードされない
CSCvz95326	ISE で ACI 統合を有効にしようとすると、複数の ACI IP アドレスまたはホスト名を追加できなくなる
CSCwa00729	特定の NAD 削除により、すべての NAD が削除された
CSCwa03126	一部の言語で ISE CPP が正しくロードされない
CSCwa05404	「TACACSで確認された古いセッションで選択したサービスが見つかりませんでした（Stale Sessions observed for Tacacs Could not find selected service）」というエラー
CSCwa07580	ユーザー名に $ 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
CSCwa08484	セッションに IPv4 アドレスと IPv6 アドレスの両方がある場合に、IPv4 マッピングがない
CSCwa17718	専用の MNT を使用した PxGrid セッションディレクトリでセッションサービスを利用できない
CSCwa19573	SSL 監査イベントが原因で Catalina.out ファイルが巨大化する
CSCwa23393	ISE 2.7 p 4、5、6 で「デバイスのIPアドレスが重複しています（There is an overlapping IP Address in your device）」というエラーが報告される

問題 ID 番号	説明
CSCwa32312	セッションキャッシュが入力されていないため、RCM および MDM フローが失敗する
CSCwa35288	KONG が Postgres に到達できず、ISE GUI アクセスに影響を与える
CSCwa47133	ISE 評価 log4j CVE-2021-44228

Cisco ISE リリース 3.0 の未解決の不具合：累積パッチ 5

問題 ID 番号	説明
CSCwa36485	UDN pxGrid デバイス割り当て API で大きな遅延が発生する
CSCwa77161	3.0P5 -> 3.0P3 で PLR が返される

Cisco ISE リリース 3.0 の解決済みの不具合：累積パッチ 4

問題 ID 番号	説明
CSCvs66551	Apache log4j の複数の脆弱性。
CSCvu56753	CIAM：openjdk の複数の脆弱性。
CSCvv04957	GRUB2 の任意のコード実行の脆弱性。
CSCvv07101	メモリリーク：エンドポイントが Cisco ISE にある場合、PKCS11 キーストアによりメモリリークが発生する。
CSCvw78019	Cisco ISE：Cisco ISE リリース 2.7 へのアップグレード後に NTP が同期しなくなる。
CSCvy07088	Cisco ISE 3.0 エージェントレスポスチャがエンドポイントの信頼ストアに CA 証明書チェーンをインストールしない。
CSCvy11865	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性。
CSCvy14905	CTS-SXP-CONN：デバイスから Cisco ISE SXP 接続への ph_tcp_close：Hawkeye。
CSCvy42885	設定のバックアップがキャンセルされたために Cisco ISE アプリケーションサーバーがクラッシュまたは再起動する。
CSCvy43246	[CFD] ユーザーがポータルの作成手順でゲスト SSID を作成できない：Cisco ISE がビジーエラー。
CSCvy48766	all-numbers サブドメインが使用されている場合、Cisco ISE のインストールがデータベースのプライミング失敗エラーで失敗する。

問題 ID 番号	説明
CSCvy62875	Cisco ISE 2.7 p2：[400] Apple デバイスでの SAML SSO OKTA による不正な要求。
CSCvy71313	CIAM：cpio 2.12。
CSCvi53134	passive-id サービスが有効になった後、Cisco ISE AD 結合に使用されるアカウントがロックされることがある。
CSCvn27270	Cisco ISE：名前、場所、またはデバイスタイプを使用してネットワーク デバイス グループを作成できない。
CSCvp88242	Mydevice ポータルを更新する際の「[400]不正な要求（[400] Bad Request）」というエラー。
CSCvr76539	ネットワーク デバイス グループへの変更が変更監査ログに反映されない。
CSCvt94587	Plus ライセンスがコンプライアンス違反エラーのため、Cisco ISE ルート CA を再生成できない。
CSCvu58927	ISE UI およびコード内のいかなる場所においても「blacklist portal」を「blocked list portal」に更新する。
CSCvv09910	CSCvr96003 の修正にもかかわらず SYSAUX テーブルスペースが満杯である
CSCvw09827	PSN ノードの CPU 使用率が高い：CSCvt34876 の拡張機能。
CSCvw90586	ネットワーク デバイス グループの名前と説明を同時に変更できない。
CSCvx01272	証明書の一括生成に Cisco ISE の自己署名証明書が含まれていない。
CSCvx23375	編集/または保存中に Cisco ISE 認証プロファイルオプションが切り捨てられる（Chrome のみ）。
CSCvx43866	3.0P2：アカウンティングレポートのエクスポートの完了に時間がかかる。
CSCvx47691	セッションディレクトリのトピックで、ダイナミック認証後もユーザーの SGT 属性が更新されない。
CSCvx60818	ERS 自己登録ポータルの更新で PSN で期待されるようにフィールドが削除されない。
CSCvy90691	Radius ベンダー ID が重複している場合、ネットワークデバイスを変更すると PSN がクラッシュする場合がある。
CSCvy94427	Cisco ISE リリース 2.7 で EAP チェーンのポスチャリースが中断する。
CSCvz00258	TACACS 認証でセッションキャッシュがクリアされないエラーにより、ヒープの使用率が高くなり、認証の遅延が発生する。

問題 ID 番号	説明
CSCvz34849	DELETE /ers/config/networkdevicegroup/{id} が機能しない、CRUD の例外。
CSCvx91688	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。
CSCvx96190	Cisco ISE レポート：上位認証で、スケジュール済みレポートのフィルタが表示されない。
CSCvx97501	パスワードに Base64 以外の文字が含まれていると、Cisco ISE リリース 3.0 ROPC 認証が失敗する。
CSCvx99151	Cisco ISE 内部 ERS ユーザーが外部 ID ストア経由で認証を試行すると、REST の遅延が発生する。
CSCvx99675	バックアップ インターフェイスが設定されている場合に、Cisco ISE 2.7P3 が src add :169.254.2.2 で他のノードにパケットを送信する。
CSCvy04443	再認証用の MNT REST API が分散型展開（別の MnT）で使用されると失敗する。
CSCvy04665	完全な数値 ID エントリを照合すると、Cisco ISE リリース 2.6 とリリース 2.7 の TACACS レポートの詳細フィルタが機能しない。
CSCvy05954	[すべてのSXPマッピング（All SXP Mappings）] にセッション経由で学習した IPv6 マッピングが表示されない。
CSCvy10026	Cisco ISE 管理証明書 CN が FQDN と等しくない場合、Cisco ISE リリース 3.0 エージェントレスポスチャが失敗する。
CSCvy11617	Windows ユーザー名にスペースが含まれている場合、Cisco ISE リリース 3.0 エージェントレスポスチャが中断する。
CSCvy16894	一部の記号を使用すると、認証プロファイルでエラーが発生する。
CSCvy18560	[RADIUSアカウンティングの詳細（RADIUS Accounting Details）] レポートにアカウンティングの詳細が表示されない。
CSCvy20277	一部のオブジェクトの [説明（Descriptions）] フィールドで以前は許可されていた特殊文字が使用できない。
CSCvy24370	Cisco ISE で RADIUS シーケンス属性において 7 個以上の属性を変更できない。
CSCvy25533	Cisco ISE：CLI バックアップ中に「/opt/CSCOcpm/config/cpmenv.sh:line 396:<ipv6>:command not found」というエラーが表示される。
CSCvy25550	Cisco ISE が認証プロファイルで Framed-IPv6-Address のカスタム属性名を受け入れない。

問題 ID 番号	説明
CSCvy30119	オプションに他の変更を加え、保存すると、LDAP グループがスポンサーグループから消える。
CSCvy30295	Cisco ISE が管理者ポータルで証明書チェーンを送信しない。
CSCvy34977	証明書テンプレートの曲線タイプ P-192 が原因でアプリケーションサーバーが「初期化（initializing）」状態でスタックする。
CSCvy36868	Cisco ISE リリース 2.3 以降のリリースはコマンドセットで「改行」<cr> 文字をサポートしていない。
CSCvy36887	TCP ポート 19444 が Cisco ISE リリース 3.x で開いている。
CSCvy38459	Cisco ISE リリース 2.7 P3 GUI にすべてのデバイス管理認証ポリシーが表示されない。
CSCvy40845	ERS リクエストで 1 つのカスタム属性を更新すると、別のカスタム属性が削除される。
CSCvy41066	ポリシーの条件としての TACACS カスタム AV ペアが機能していない。
CSCvy45015	[電話番号をユーザー名として使用（Use Phone number as username）] が有効な場合に、重複ユーザーの Cisco ISE ゲスト自己登録エラーが発生する。
CSCvy46504	Cisco DNA Center からポリシーを展開しようとしているときに、Cisco DNA Center で断続的なエラーが発生する。
CSCvy51073	Cisco ISE 認証プロファイル ERS の更新で accessType 属性の変更が無視される。
CSCvy51210	Cisco ISE リリース 2.7 で NAD の IP デフォルトラベルを GUI で削除しようとすると、エラーが表示される。
CSCvy58771	NAD の編集中に、間違ったデバイスプロファイルがマッピングされる。
CSCvy60752	セットアップウィザードのパスワードはハイフンをサポートしているが、CLI を使用して設定をリセットすると、ウィザードがハイフンをサポートしなくなる。
CSCvy60865	エンドポイントが新しいスイッチポートに変更され、EP IdGroup で EP の削除またはすべて削除が実行されると、Cisco ISE リリース 2.4 CoA が失敗する。
CSCvy61564	Cisco ISE リリース 2.7 パッチ 3 の ERS コールが 3 文字の RADIUS 共有秘密を受け入れない。
CSCvy61894	UI：キーペアの生成でスペースを使用できるが、そのキーをエクスポートできない。

問題 ID 番号	説明
CSCvy63778	CoA の REST API が任意のサーバー IP で動作する。
CSCvy65786	PassiveID：% を含む AD アカウントパスワードを使用して WMI を設定すると、エラーになる。
CSCvy71690	ゲストポータルの [顧客（Customer）] フィールドに & - $ # が含まれる。
CSCvy74919	非アクティブタイマーに達した後も Cisco ISE 内部ユーザーが無効にならない。
CSCvy76262	Cisco ISE DACL 構文バリデータが ASA のコード要件に準拠していない。
CSCvy76328	[ネットワークデバイス（Network device）] タブの [複製（duplicate）] オプションを使用すると、IPv6 のサブネットが /128 に変更される。
CSCvy76617	Cisco ISE：NAD ページのフィルタの有無にかかわらず、デバイスの [すべて選択（Select All）] チェックボックスをオンにする必要がある。
CSCvy81435	Cisco ISE ゲスト SAML 認証が [アクセス権が検証されました（Access rights validated）] HTML ページで失敗する。
CSCvy82114	[ネットワークアクセスユーザー（Network Access Users）] の [姓名（First/Last name）] に誤った中国語の Unicode が表示される。
CSCvy89317	ISE：DST ルート CA X3 認証局：2021 年 9 月 30 日で失効（90 日以内）
CSCvy92536	Cisco ISE リリース 3.0 デバイス管理ライセンスだけで、[管理（Administration）] > [システム（System）] > [ログ記録（Logging）] メニューへのアクセスが許可される必要がある。
CSCvy93847	NAD でポリシーペルソナなしでセカンダリ PAN を選択し、設定変更をデバイス CoA に送信できる。
CSCvy94511	EPOCH 時間が Null になっているため、TACACS レポートに重複したエントリが表示される。
CSCvy94553	TACACS 認証レポートに重複したエントリが表示される。
CSCvy94818	NMAP が積極的な推測を実行するため、エンドポイントが「cisco-router」として不適切にプロファイリングされる。
CSCvy99582	外部 RADIUS サーバーが設定されている場合に、Cisco ISE リリース 2.4 パッチ 13 から Cisco ISE リリース 2.7 へのアップグレードプロセスが失敗する。
CSCvz00659	バナーで特殊文字を使用すると、SFTP リポジトリがブロックされる。

問題 ID 番号	説明
CSCvz01485	Cisco ISE リリース 2.7 パッチ 4 で Umbrella セキュリティプロファイルの .json ファイルをアップロードできない。
CSCvz05704	ディスクサイズが 1 TB を超える Cisco ISE のプラットフォームチェックが失敗する。
CSCvz05966	Cisco ISE リリース 2.6 パッチ 9：新しいグループを追加した後、デフォルトの権限がデフォルトのグループ内部に戻らない。
CSCvz07823	Cisco ISE リリース 2.7：エンドポイントをグループに追加できない。
CSCvz18627	PEAP セッションのタイムアウト値が最大で 604800 に制限されている。
CSCvv55602	ポリシーエンジンの機能強化。
CSCvz33839	メニューアクセスのカスタマイズが機能していない。
CSCvz49086	SQLException 発生時に Cisco ISE リリース 3.0 TimesTen 接続が終了する。
CSCvy32461	[電話（phone）] フィールドまたは [電子メール（email）] フィールドが入力されている場合に、スポンサーユーザーはデータを編集できない。
CSCvv63395	Cisco ISE リリース 3.0 でサービスの再起動後に REST ID ストアが見つけられない。
CSCvy88861	Cisco ISE のフェールオーバー後にポリシーの変更がネットワークデバイスにプッシュされない。
CSCvs95495	再認証の問題：Aruba：サードパーティのデバイス。
CSCvz08813	[発行された証明書（Issued Certficates）] ページで別のページにスクロールできない。
CSCvy29454	パスワードリセットの携帯電話番号検証が e.164 形式を満たしていない。

Cisco ISE リリース 3.0 の未解決の不具合：累積パッチ 4

Cisco ISE リリース 3.0 パッチ 4 には未解決の不具合はありません。

Cisco ISE リリース 3.0 の新機能：累積パッチ 3

Cisco ISE GUI に追加されたフルアップグレードと分割アップグレードのオプション

[管理（Administration）] > [システム（System）] > [アップグレード（Upgrade）] > [アップグレードを選択（Upgrade Selection）] ウィンドウで次のオプションのいずれかを選択して、Cisco ISE 展開をアップグレードできます。

- [フルアップグレード（Full Upgrade）]：フルアップグレードは、Cisco ISE 展開の連続した完全な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。この方法により、すべてのノードが並行してアップグレードされ、分割アップグレードプロセスよりも短時間でアップグレードされます。すべてのノードが並行してアップグレードされるため、アップグレードプロセス中にアプリケーションサービスがダウンします。

（注） フルアップグレード方法は、Cisco ISE 3.1 以降でサポートされています。フルアップグレード方法の詳細については、「Cisco Identity Services Engine Upgrade Journey, Release 3.1」を参照してください。

- [分割アップグレード（Split Upgrade）]：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。このアップグレード方法では、展開時にアップグレードする Cisco ISE ノードを選択できます。

Cisco ISE リリース 3.0 の解決済みの不具合：累積パッチ 3

問題 ID 番号	説明
CSCuo73496	ISE RADIUS session-timeout 値が 65535 までに制限される
CSCvh04231	「ゲストユーザー情報を保存」の RADIUS アカウンティングおよびアクセス許可でゲストユーザー名が送信されない
CSCvi59005	スクロールバーを使用すると、AD グループの完全なリストを表示できない。
CSCvn25548	アラームの受信：認証の失敗が多すぎるため、アカウントが一時的に停止される
CSCvn31249	GNU gettext default_add_message ダブルフリーの脆弱性
CSCvo04728	MIT Kerberos 5 KDC krbtgt チケット S4U2Self リクエストのサービス妨害 ...
CSCvo56767	ISE-PIC GUI 管理者ユーザー設定を変更しようとするとエラーが発生する
CSCvq26124	ISC BIND managed-keys トラストアンカーのサービス妨害の脆弱性
CSCvq58506	show running-config を完了できない
CSCvr47716	Info-ZIP UnZip ファイルの重複したサービス拒否の脆弱性 CVSS v3.0 Base 7.5
CSCvr55906	cURL および libcurl tftp_receive_packet() 関数ヒープ バッファ オーバーフローの脆弱性 CVSS v3.1 Base：9.8

問題 ID 番号	説明
CSCvr77653	cURL および libcurl tftp_receive_packet() 関数ヒープ バッファ オーバーフロー ...
CSCvr77655	GNU パッチ pch_write_line 関数のサービス妨害の脆弱性
CSCvr80914	SSSD グループ ポリシー オブジェクトの実装における不適切なアクセス制御の脆弱性
CSCvr80921	ISC BIND Dynamically Loadable Zones における不正アクセスの脆弱性
CSCvr81463	libssh2 packet.c の整数オーバーフローの脆弱性 CVSS v3.1 Base：8.1
CSCvr97388	Samba ファイル名パス区切り文字の不正アクセスの脆弱性
CSCvs29611	ISE 2.4 p5 が深夜に継続的にクラッシュし、コアファイルが生成される
CSCvs39800	gllibc LD_PREFER_MAP_32BIT_EXEC 環境変数の ASLR バイパスの脆弱性
CSCvs45350	ユーザー認証が失敗しマシン認証が成功すると、ライブログと NAD に Anonymous が表示される
CSCvs76914	libxml2 xmlParseBalancedChunkMemoryRecover メモリリークの脆弱性
CSCvs85273	libcurl の複数の脆弱性
CSCvs91984	systemd button_open のメモリリークの脆弱性
CSCvt30558	python の複数の脆弱性
CSCvt85370	ポスチャ条件が「vc_visInst_v4_CiscoAnyConnectSecureMobilityのチェックでClient_4_xが見つかりません（Check vc_visInst_v4_CiscoAnyConnectSecureMobility Client_4_x is not found）」で失敗する
CSCvu04874	io.netty.buffer.PoolChunk での疑わしいメモリリーク
CSCvu13139	2.4.50 より前の OpenLDAP の slapd の filter.c では、LDAP 検索で wit がフィルタリングされる
CSCvu14215	AD グループの追加/削除中にスポンサー グループ メンバーシップが削除される
CSCvu22058	DUO を外部 RADIUS プロキシとする ISE で access-reject がドロップされる
CSCvu22259	CIAM：batik 1.7
CSCvu24402	CIAM：cups 1.6.3
CSCvu30439	CIAM：ksh

問題 ID 番号	説明
CSCvu31098	CIAM：libssh
CSCvu37728	CIAM：perl 5.14.1
CSCvu37765	CIAM：procps 3.3.10
CSCvu37775	CIAM: python（version 2.7.5、2.7.14、3.7.1）
CSCvu38141	CIAM：vim 7.4.160
CSCvu58927	ISE UI およびコード内のいかなる場所においても「blacklist portal」を「blocked list portal」に更新する
CSCvu62938	プライマリ PSN/PAN に到達できない場合にポスチャが失敗する
CSCvu72744	すべての認証および認可のルール/プロファイルで「blacklist」を「blocked list」に置き換える
CSCvu81838	CIAM：d-bus 1.10.24
CSCvu84184	証明書チェーンがポータルで送信されない
CSCvu84773	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvu91859	CIAM：libjpeg と libjpeg-turbo
CSCvv10683	ドロップされたセッションのセッションキャッシュがクリアされず、PSN で高い CPU 使用率が発生する
CSCvv14390	最大セッション数制限がユーザーとグループに対して機能しない
CSCvv18317	データベース内の無効なオブジェクト
CSCvv19065	ISE ユーザーが [DNACアシュアランス（DNAC Assurance）] ページでゲスト ID を確認できない
CSCvv27690	ISE 2.4 で HTTPS、EAP、DTLS、および PORTAL の ISE 証明書を更新すると、PORTAL ロールと Admin ロールのみが適用される
CSCvv29737	Cisco DNA の ACA SG 同期が「JDBCException：ステートメントを準備できませんでした（JDBCException:could not prepare statement）」で失敗する
CSCvv30161	ライブセッション詳細レポートで、VPN ポスチャシナリオについて誤った認証プロファイルと認証ポリシーが表示される
CSCvv30226	Livelog セッションで、VPN ポスチャシナリオに誤った認証ポリシーが表示される
CSCvv43383	NFS リポジトリが GUI から機能しない

問題 ID 番号	説明
CSCvv44401	自己署名証明書を生成すると、CSR のデフォルトパラメータが事前にインストールされた証明書に対応していない
CSCvv45063	ノードが展開から削除されたときに内部 CA 証明書が削除されない
CSCvv45340	running-config の保存エラーにより、スタートアップ設定が失われる
CSCvv46958	NDG 列が 255 文字を超えると、TrustSec が有効になった NAD が TrustSec マトリックスに表示されない
CSCvv47849	[CFD] Cisco DNA Center で SG 名が変更された場合、マッピングされた SGT エントリが ISE で認証ルールからクリアされる
CSCvv50028	ISE ノードのリセット設定後にヒープダンプの生成が失敗する
CSCvv52637	ISE ホットスポット ゲスト ポータルのフローが中断する
CSCvv60353	合計レコード数が 500 万を超えると、認証概要レポートがスタックする
CSCvv60686	ISE SXP にはセッションから学習した古いマッピングをクリアするメカニズムが必要である
CSCvv60923	ISE に内部ユーザーのカスタム属性の IP データ型にスラッシュを使用する機能を追加する
CSCvv61732	異なる SNMP サーバーに対して一意のコミュニティストリングを作成できない
CSCvv62382	プロキシバイパス設定で大文字を使用できない
CSCvv63548	メモリリーク：PSN rmi GC の収集が正しく機能せず、パッシブ ID フローでメモリリークが発生する
CSCvv64012	アクションの使用頻度が高すぎると ISE 3.0 REST ID プロセスが失敗する
CSCvv66302	ドメインが SXP ピアに割り当てられない
CSCvv67091	Cisco Identity Services Engine の信頼できないファイルアップロードの脆弱性
CSCvv68293	ローカルまたはグローバルの例外を使用する場合、ISE がプラスライセンスを使用しない
CSCvv72418	ISE 3.0 REST ID ログファイルがサポートバンドルに含まれていない
CSCvv77007	ISE が内部の「ネットワーク管理者」ユーザーのリクエストを外部の RADIUS トークンサーバーに絶えず送信する

問題 ID 番号	説明
CSCvv77928	RMA'd pPAN の後、「予期しないエラーが発生しました（An unexpected error occurred）」というメッセージと共に証明書の一括生成が失敗する
CSCvv79940	ISE で SAN の hostname-x を使用して CSR を生成するとエラーになる
CSCvv80297	ROPC の CTL に DigitCert グローバルルート G2 が必要
CSCvv80307	ropc.log の REST エラーにはエンドポイント URL を含める必要がある
CSCvv82625	任意の認証ルールにセキュリティグループのみがあり、認証プロファイルがない場合、ポリシーセットが保存されない
CSCvv85588	メモリリーク：PassiveID ストレス時の使用者 CAD_ValidateUser で割り当てが高くなる
CSCvv90612	WebUI の復元が IE11 で機能しない
CSCvv91268	新しいウィンドウで PxGrid サービスメニューを開くと、ISE 3.0 で「PxGrid が無効になっています（PxGrid disabled）」と表示される
CSCvv93442	ISE 2.6p3 で SFTP サーバーのファイルパスに二重のスラッシュ「//」が追加される
CSCvv94791	[CFD] ACA 同期の中断：「移行中にエラーが発生しました：同期ランタイムの待機がタイムアウトしました（Error occurs during migration: Waiting for Sync Runtime timed out）」
CSCvv95150	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
CSCvw00375	ISE 2.7p2 のカスタムビューの [コンテキストの可視性（Context Visibility）] ページをロードできない
CSCvw01225	ISE Config Restore が 40% で失敗し、「IMPDPを使用したDBの復元が失敗しました（DB Restore using IMPDP failed）」というエラーメッセージが表示される
CSCvw01818	ISE 管理 Web UI および CLI のキーワード kong を API GW に置き換える
CSCvw01829	Chrome 85/86 での ISE 管理者またはポータルログインで「問題が発生しました（Oops. Something went wrong）」というエラーが発生する場合がある。
CSCvw02887	AD グループの追加後にパッシブ ID フローでメモリリークが発生する
CSCvw06722	スポンサーが自身のユーザー ID でポータルにアクセスしたときに、作成されたゲストユーザーのリストを表示できない

問題 ID 番号	説明
CSCvw08330	サードパーティの NAD のダイナミック リダイレクションでポスチャが機能しない
CSCvw10671	GNU.org bash rbash BASH_CMDS の変更特権昇格の脆弱性
CSCvw16237	PMNT のリロード後にスケジュール済みの OPS のバックアップがトリガーされない
CSCvw17908	デフォルトルートがタグ付けされている場合、IP から SGT へのマッピングを ISE からスイッチにプッシュできない
CSCvw19785	外部データ ソースのポスチャ条件を編集すると、常に間違った AD が表示される
CSCvw20021	NAD の場所が [コンテキストの可視性のエラスティック検索（Context Visibility ElasticSearch）] で更新されない
CSCvw20060	Windows ネットワーク インターフェイスよりも先にエージェントサービスが起動した場合、ISE 2.6 p5 エージェントで DC がダウンとしてマークされる
CSCvw20636	NAD プロファイルが削除された後、認証プロファイルに「データがありません（No data available）」と表示される
CSCvw22228	pxGrid ANC applyEndpointPolicy ですべての MAC アドレス形式を正しく扱われない
CSCvw24227	例外が原因でエンドポイントが消去されない
CSCvw24268	Cisco Identity Services Engine の信頼できないファイルアップロードの脆弱性
CSCvw25615	ISE TACACS ロギングタイムスタンプに将来の日付が表示される
CSCvw26415	ISE 3.0 で CN および SAN が欠落している証明書が信頼できる証明書ストアにインポートされない
CSCvw28084	DOC：ISE：ISE 2.7 インストールガイドに OVA テンプレート予約テーブルを追加する必要がある
CSCvw28441	API の使用中に NAD の共有秘密がログに表示される
CSCvw29490	内部ユーザーのカスタム属性が CoA プッシュで送信されない
CSCvw31269	SAML グループがスポンサーポータルグループで適用した場合に機能しない

問題 ID 番号	説明
CSCvw33115	VPN のユースケースで ISE MNT ライブセッションのステータスが「ポスチャ済み」に変わらない
CSCvw36190	スケジュールされた運用バックアップが「バックアップが進行中です...（Backup is in progress...）」でスタックする
CSCvw36486	IP アクセス制限を適用した後、GUI にアクセスできない
CSCvw36743	パスワードに特殊文字を使用すると、ISE サービスアカウントがロックされ、WMI が確立されない
CSCvw37844	ISE で内部コールにホスト名が使用されるため ANC CoA が機能しない
CSCvw38530	SBET：[バックアップと復元（Backup & Restore）] ページのロード中に ise-psc.log のリポジトリに関する例外が発生する。
CSCvw44120	機能：ISE 3.0 でゲストポータル作成が失敗する
CSCvw46096	ISE 3.0 Syslog プロバイダーが設定を適用できない
CSCvw47011	同じ ID グループが複数回作成され、ERS REST API 送信を使用すると UI に表示される
CSCvw48396	Cisco ADE-OS のローカル ファイル インクルードの脆弱性
CSCvw48403	SNMPv3 | エンドポイントについて収集された SNMP 情報が ISE で処理されない：ストリングインデックスが範囲外：8
CSCvw48697	API IP SGT マッピングが [No Devices] の結果を返さない
CSCvw49938	TACACS コマンドの前にスペースを含むサードパーティデバイスについて、TACACS コマンド アカウンティング レポートがない
CSCvw50381	猶予アクセスの期限が切れたときに Aruba WLC に対する CoA-disconnect が ISE で発行されない
CSCvw50829	RBAC ポリシーで AD セキュリティグループの OU の末尾をドット文字にできない
CSCvw51801	ISE ライブセッションの「ポスチャ済み」セッションが暫定アップデート時に「開始済み」に 切り替わる
CSCvw53187	ACI エンドポイントのライブログが情報を表示せずに「ロード中（loading）」でスタックする
CSCvw53412	SB で Hibernate.log を収集する必要がある
CSCvw54878	日本語の GUI に 50 以上のルールがある場合、ISE は完全認可のルールを表示しない

問題 ID 番号	説明
CSCvw55793	ISE が PSN からの CoA の送信に「識別子割り当てに失敗しました（Identifier Allocation Failed）」というエラーで失敗する
CSCvw58538	GNOME GLib file_copy_fallback 関数の不適切な権限の脆弱性
CSCvw58824	バージョン 1.4.15 より前の XStream の複数の脆弱性
CSCvw59312	Freetype の CVE-2020-15999 および CVE-2018-6942 のヒープ バッファ オーバーフロー
CSCvw59314	moment モジュールの日付文字列の正規表現に関するサービス妨害の脆弱性
CSCvw59855	6.1.0 より前の Highcharts JS の js/parts/SvgRenderer.js での使用 ...
CSCvw59920	c3p0 の複数の脆弱性
CSCvw60197	glibc の複数の脆弱性
CSCvw61589	ISE ポリシー評価：ポリシーセットの削除後に RADIUS 要求がドロップされる
CSCvw61786	スキーマオブジェクトをドロップする前に復元プロセスのすべてのプロセスを停止する必要がある
CSCvw63264	ISE 3.0 ポリシー条件スタジオ GUI バグ
CSCvw64840	CIAM で mariadb の脆弱性が検出された
CSCvw65262	CIAM：go 1.12 CVE-2019-9634 など
CSCvw66468	Doc：syslog カテゴリに関する ISE 3.0 のドキュメントがない
CSCvw66483	選択した外部サーバーのリストが変更された後に RADIUS サーバーの順序が間違った順序になる
CSCvw66601	CIAM で jspdf の脆弱性が検出された
CSCvw68480	ISE の [合計（TOTAL）] フィールドに正しくない数値が表示される
CSCvw68512	ゲスト ユーザーが誤った有効期間で作成される
CSCvw69977	「すべての SXP マッピング（All SXP Mapping）」表に、ISE で終了したセッションが含まれる
CSCvw73928	関連のない NTP 同期失敗アラームを変更する必要がある
CSCvw74703	CIAM：libssh2 CVE-2019-17498 など

問題 ID 番号	説明
CSCvw74712	CIAM：libcurl CVE-2016-8622 など
CSCvw74932	CIAM：json-sanitizer 1.2.0 CVE-2020-13973
CSCvw75397	MNTHA：IP アクセスが有効な場合に、MnT ノード名が NULL に設定される。
CSCvw75563	パスコードフィールドに特殊文字が含まれていると、ホットスポット ゲスト ポータルでページロードエラーが表示される
CSCvw77219	Dot1x 認証がマネージャの重複で失敗する：add=false
CSCvw78269	CWE-20：ノードグループの作成の入力検証が正しくない
CSCvw78289	50 文字を超えるプロファイル名を使用している場合、認証に成功したことを示すライブログが表示されない
CSCvw80520	IMS（ISE メッセージングサービス）が無効になっている場合、「Radius認証の詳細（Radius Authentication Details）」レポートに時間がかかる
CSCvw82774	ISE 2.6/2.7 のユーザー ID グループでユーザー名に基づくソートが機能しない
CSCvw82784	ISE 3.0 で TACACS+ のエンドステーション ネットワーク条件のスクロールバーが機能しない
CSCvw82815	認証プロファイルの CWA オプションが一部のネットワーク デバイス プロファイルで正しく機能しない
CSCvw84127	ISE：設定監査の詳細にどのポリシーセットが変更されたかが表示されない
CSCvw85599	TACACS+ N/W 条件および PORT N/W 条件のスクロールバーが機能しない
CSCvw87147	ライブセッションで正しいアクティブセッションが表示されない
CSCvw87173	ISE 2.4 p13 で MAB 認証済みエンドポイントの AD 許可ルックアップが中断される
CSCvw87175	Active Directory を使用した MAB 認証が AD オブジェクトが無効でも成功する
CSCvw88881	DB クリーンアップの毎時 cron で DB ロックが取得される結果、展開の登録に失敗する
CSCvw89326	PKI ベースの SFTP の場合、MnT ノードの GUI キーのエクスポートは PAN に昇格した場合にのみ可能となる
CSCvw90961	RBAC ルールが 2.7 で適用されない

問題 ID 番号	説明
CSCvw93570	ISE 2.4 パッチ 8 でゲストポータルを編集、複製、削除できない
CSCvw94096	ISE BYOD ポータルで iPod がオプションとして表示されない
CSCvw94603	外部 MDM サーバー（Microsoft_intune）でポーリング間隔の変更が反映されない
CSCvw96371	API からカスタム属性を更新すると、EP から静的ポリシーとグループの割り当てが失われる
CSCvw97905	内部ユーザーエクスポート機能でパスワードに無効な文字が含まれていてもエラーが表示されない
CSCvx01798	ISE RBAC：ネットワークデバイスを追加すると、「ネットワークデバイスをロードできません（Unable to load NetworkDevices）」というエラーが表示される
CSCvx03047	ACI が学習したマッピングが xgrid 一括ダウンロードに表示されない
CSCvx04512	login.jsp に直接アクセスすると証明書ベースの認証による管理アクセスがバイパスされる
CSCvx09383	ISE 2.7：コンテキストの可視性：実行中のプロセスでエンドポイントアプリケーションをソートすると、すべてのシャードが失敗する
CSCvx10186	スマートライセンスに登録した後も ISE が評価期限切れ状態のままになる
CSCvx14332	CIAM：json-sanitizer 1.2.0 CVE-2021-23899 など
CSCvx15010	CLI を介した 2.7 P3 から 3.1.236 へのアップグレードフローがマルチノード展開の証明書の問題で失敗する
CSCvx15427	ヘルスチェック：DNS 解決可能性：CNAME（エイリアス）として ISE FQDN を使用時に誤ったエラーが発生する
CSCvx15448	ヘルスチェック：ディスク容量：不十分な障害情報
CSCvx18730	シスコ製品に影響する Sudo 権限昇格の脆弱性：2021 年 1 月
CSCvx22229	結合インターフェイスの IP アドレスを変更すると、ISE の「ipv6 address autoconfig」が削除される
CSCvx22594	ISE 3.0 GUI 証明書認証：サポートされていない証明書の目的
CSCvx23205	IdenTrust Commercial Root CA 1 証明書を ISE トラストストアに追加
CSCvx27632	認証では [ODBCストアドプロシージャ（ODBC Stored-Procedures）] ページで設定された形式で MAC アドレスを検索する必要がある

問題 ID 番号	説明
CSCvx28402	ISE 2.7 以降のバージョンのサポートバンドルで ise-jedis.log ファイルがキャプチャされない
CSCvx30276	ISE 2.7：ルート CA の再作成時に Jedis DB 接続プールが再作成されない
CSCvx32666	NetworkAccess：ポリシーセットのエントリの評価で認証方式の条件が照合されない
CSCvx32764	予期しない電源イベントの後に TC-NAC サービスが実行されない
CSCvx34413	Azure AD からのページングが ROPC に実装されない
CSCvx36013	ISE ヘルスチェック プラットフォーム サポートが結果に従って UI を直接更新する
CSCvx37149	すべてのペルソナを同じノードで実行している SNS3515 の SGA 値が Under-Provisioned になる
CSCvx37297	シングルサインオン/Kerberos ユーザーによるスポンサーポータルへの認証でエラー 400 が発生する。
CSCvx37467	ポータル設定で「携帯電話番号（mobile number）」フィールドにチェックが付いていない場合、スポンサーポータルが「無効な入力」を提供する
CSCvx41826	Tenable SC 5.17 ですべての tenable アダプタリポジトリを取得できない
CSCvx43566	外部のユーザー名を使用している場合に、パスワードの誤りによるログインの失敗がログに記録されない
CSCvx43825	NAS-IP アドレスが指定されていない acct stop を受信した場合にセッションが開始状態のままになる
CSCvx44815	ISE AD ランタイムで a1-a2-a3-a4-a5-a6 から a1a2a3a4a5a6 への書き換えをサポートする必要がある
CSCvx45481	ISE 2.4 でエンドポイントを新規スイッチポートに変更し、エンドポイント ID グループを変更した場合、CoA が失敗する
CSCvx46638	EAP チェーンの場合に、ポスチャポリシーでマシン AD グループメンバーシップを取得できない
CSCvx47891	ISE で新しいエンドポイントの AMP イベントが正しくマッピングされない
CSCvx48922	TACACS フローのメモリリーク
CSCvx49538	CIAM：bind：複数のバージョン CVE-2020-8625

問題 ID 番号	説明
CSCvx50752	Smart Call Home およびスマートライセンス用に IdenTrust Commercial Root CA 1 証明書を追加
CSCvx51738	Network Success Diagnostics 用に IdenTrust Commercial Root CA 1 証明書を追加
CSCvx53205	NIC ボンディングにより、MAR キャッシュが複製されない
CSCvx53905	ISE 3.0 で認証ポリシー条件の形式が正しくない
CSCvx54213	[ネットワークデバイス（Network Devices）] > [デフォルトのデバイス（Default Device）] ページで設定のために Plus ライセンスが要求される
CSCvx57433	TrustSec ポリシーマトリックスにより、ISE 3.0 での制限付きスクロールが許可される
CSCvx57545	isedailycron temp1 のトラッキングにより AWR レポートで遅延が発生する
CSCvx58456	ユーザーは、所定の時点で完全アップグレードか分割アップグレードのどちらか 1 つのオプションのみを選択できる。
CSCvx58516	ネットワークデバイス別上位 N の認証の詳細が表示されない
CSCvx58520	PLR でプロファイラオンライン更新エラー：ライセンスファイルデータの取得に失敗：Null
CSCvx61462	ISE ログ収集エラー「セッションディレクトリの書き込みに失敗しました（Session directory write failed）」
CSCvx61664	ISE で AnyConnect 出力設定ファイルの Json ファイルの情報が更新されない
CSCvx64247	国コードのドロップダウンを使用すると、モバイルデバイスで「無効な電話番号形式（Invalid phone number format）」が表示される
CSCvx69701	PnSLongevity：データベース接続が利用できないため、展開で同期ができない
CSCvx70633	ISE の Adv Trustsec の構成展開で EXEC またはイネーブルモードのパスワードに % を使用できない
CSCvx72642	バックアップインターフェイスが設定されている場合、REST 認証サービスは無効になる
CSCvx78643	ISE 2.7 | 電子メールアドレスが設定されていない場合でも、すべてのシステムアラームについて電子メールが送信される
CSCvx79693	ISE との Qualys の統合が失敗する

問題 ID 番号	説明
CSCvx85391	ログイン文字の大文字小文字が原因で内部ユーザーの非アクティブタイマーが更新されない
CSCvx85675	ISE が、競合状態が原因の SXP-IP マッピング伝搬の削除/追加を処理できない
CSCvx85807	ISE および ISE-PIC で、登録解除フローのスマートライセンスが機能しない
CSCvx86571	ログインページのメッセージが空の場合は説明のボックスを削除する必要がある
CSCvx86915	TrustSec のページの UI に問題がある
CSCvx86921	RADIUS トークン ID のソースプロンプトと TACACS 認証の内部ユーザープロンプト
CSCvx94452	2/7 p2 以降で EST サービスが実行されない
CSCvx96915	XStream 1.4.16 で修正された脆弱性
CSCvx99176	ISE で「-」または「*」を使用した NAD IP 定義がパッチ適用後に完全な IP 比較を実行しない
CSCvy06719	「手動アクティブセッション（Manual Active Session）」レポートが空になっている
CSCvy08724	読み取り専用管理者によるアップグレードの実行は許可されないようにする
CSCvy14259	アップグレードサポートから 3515 を削除する
CSCvy14342	PIP クエリ評価が原因で ISE 2.6P3 以降の PSN ノードで CPU 使用率が高くなる
CSCvy15058	API 経由でドメインを「ブロック/許可する」に更新できない
CSCvy15172	Cisco Identity Services Engine のセルフ クロスサイト スクリプティングの問題
CSCvy17893	ISE REST API が IP-SGT マッピングに重複する値を返す。
CSCvy23354	FF 88 で最大高さが小さすぎる
CSCvy37878	任意の認証ルールにセキュリティグループのみがあり、認証プロファイルがない場合、アクセスが拒否される
CSCvy38896	Framed-IP 値のない AAA 要求により、SXP プロセスで例外が発生する

問題 ID 番号	説明
CSCvy42972	データサイズが全体で 40GB を超える場合、フルアップグレードで警告がスローされる必要がある
CSCvy76601	コンテキストの可視性で「All」関数を削除し、CAPTCHA ポップアップに {0} 個のエンドポイントを表示する

Cisco ISE リリース 3.0 の未解決の不具合：累積パッチ 3

問題 ID 番号	説明
CSCvz00617	PnSLongevity：3.0P3 で Longevity テストベッドのレプリケーション失敗エラーが発生する

Cisco ISE リリース 3.0 の新機能：累積パッチ 2

エアギャップネットワークのライセンス方式

Cisco ISE リリース 3.0 パッチ 2 は、エアギャップネットワークの次のライセンスソリューションをサポートしています。

- **Smart Software Manager（SSM）オンプレミス接続方式**

  SSM オンプレミスは、Cisco ISE 対応ネットワークでスマートライセンスを管理する SSM オンプレミスサーバーを設定する接続方式です。この接続方法では、Cisco ISE はインターネットへの永続的な接続を必要としません。

『*Cisco Identity Services Engine リリース3.0 管理者ガイド*』の「ライセンス」の章を参照してください。

DNS キャッシュ

ホストの DNS 要求をキャッシュできるため、DNS サーバーの負荷が軽減されます。

この機能は、次のコマンドを使用してコンフィギュレーション モードで有効にできます。

service cache enable hosts ttl *ttl*

この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

no service cache enable hosts ttl *ttl*

管理者は、キャッシュを有効にしながら、キャッシュ内のホストの存続可能時間（TTL）値を秒単位で設定できます。ttl のデフォルト設定はありません。1 ～ 2147483647 の範囲の値を指定できます。

（注） TTL 値は、否定応答に対して受け入れられます。DNS サーバーで設定された TTL 値は、肯定応答に対して受け入れられます。DNS サーバーで TTL が定義されていない場合は、コマンドで設定された TTL が受け入れられます。機能を無効にするとキャッシュも無効になります。

ビジネス成果：DNS サーバーの負荷が軽減されます。

Cisco ISE リリース 3.0 の解決済みの不具合：累積パッチ 2

問題 ID 番号	説明
CSCvq44063	DNS の不正な設定により、TACACS 認証または RADIUS 認証に失敗する
CSCvu94025	ISE が syslog ターゲットに対してのみ IP を許可するか、DNS キャッシングを提供する
CSCvv02998	MacOS 11 で BYOD 証明書のプロビジョニングフローが失敗する
CSCvv27690	HTTPS、EAP、DTLS、および PORTAL の ISE 証明書を更新すると、PORTAL ロールと Admin ロールのみが適用される
CSCvv30274	[Context Visibility] には、VPN ポスチャシナリオの誤った認可プロファイルとポリシーが表示される
CSCvv46034	TACACS 設定の更新中はデバイス管理サービスが無効になる
CSCvv53221	ISE_EST_Local_Host の RADIUS 共有秘密が見つからない場合、ISE アプリケーションサーバーが初期化状態になる
CSCvv54798	CLI からエクスポートされたコンテキストの可視性の CVS に IP アドレスが表示されない
CSCvv55663	ISE ノードのリロード後に ISE 2.6/2.7 リポジトリが削除される
CSCvv57628	一時停止されたゲストユーザーがエンドポイントグループから自動的に削除されない
CSCvv74361	ISE 3.0 ヘルスチェックライセンス検証の誤ったアラーム
CSCvv91007	接続に失敗すると、[Smart Licensing Entitlement] タブが [Refreshing] でスタックする
CSCvw08602	IP オーバーラップの場合にエラーがスローされない
CSCvw25285	パッシブ ID がマルチ接続 syslog クライアントで安定して動作しない
CSCvw34491	Essentials ライセンスを有効にすると、[Network Devices] タブの [Add/Modify] へのアクセスのみがブロックされる

問題 ID 番号	説明
CSCvw54878	日本語の GUI に 50 以上のルールがある場合、ISE は完全認可のルールを表示しない
CSCvw61537	cisco.com から取得する ISE 3.0 評価仕様
CSCvw73529	スマートライセンスと永久ライセンスの予約に [OnPrem Satellite] オプションがない
CSCvw76847	侵入テスト時に ISE 条件ライブラリが破損する
CSCvw78269	CWE-20：ノードグループの作成の入力検証が正しくない
CSCvw81454	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCvw82927	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCvw83296	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCvw83334	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCvw89818	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCvx00245	保存中に Itune 統合がエラーをスローするが、テスト接続は正常に動作している
CSCvx00345	Azure AD グループを取得できない

Cisco ISE リリース 3.0 の未解決の不具合：累積パッチ 2

問題 ID 番号	説明
CSCvz00617	PnSLongevity：3.0P3 で Longevity テストベッドのレプリケーション失敗エラーが発生する

Cisco ISE 3.0 パッチ 2 の既知の制限事項

[名前（Name）] および [説明（Description）] フィールドでの特殊文字の使用に関する制限

- TACACS+ プロファイルおよびデバイス管理ネットワーク条件の [説明（Description）] フィールドでは、特殊文字 [%\<>*^:"|',=/()$.@;&-!#{}.?] は使用できません。サポートされる文字は、英数字、アンダースコア（_）、およびスペースです。
- 認証プロファイルの [名前（Name）] および [説明（Description）] フィールドでは、特殊文字 %\<>*^:\"|',= は使用できません。[名前（Name）] および [説明（Description）] フィールドでサポートされる文字は、英数字、ハイフン（-）、ドット（.）、アンダースコア（_）、およびスペースです。

- 時刻と日付の条件の [名前（Name）] および [説明（Description）] フィールドでは、 特殊文字 [%\#$&()~+*@{}!/?;:',=^`]"<>" は使用できません。[名前（Name）] および [説明（Description）] フィールドで サポートされる文字は、英数字、ハイフン（-）、ドット（.）、アンダースコア（_）、およびスペースです。

Cisco ISE リリース 3.0 の解決済みの不具合：累積パッチ 1

問題 ID 番号	説明
CSCvf61114	「認証プロファイル」に対する ERS の更新/作成で XML スキーマの検証が失敗する
CSCvm47584	ポスチャリースが原因で 1 日を超えた猶予期間を設定できない
CSCvr22065	共有秘密キーに特殊文字が含まれていると、サポートされていないエラーによりインポート NAD が失敗する
CSCvt64739	アプリケーションサーバーの初期化に時間がかかる
CSCvu05121	SMTP サーバーの変更後にゲスト電子メールが送信されない
CSCvu58892	ISE GUI のすべてで「マスターゲストレポート」を「プライマリゲストレポート」に更新
CSCvu58927	ISE GUI 内のいかなる場所においても「blacklist portal」を「blocked list portal」に更新する
CSCvu58954	ISE GUI 内のいかなる場所においても「blacklist identity group」を「blocked list identity group」に更新する
CSCvu59038	「show interface」コマンドの「master/slave」という用語を「primary/subordinate」に更新する
CSCvu72744	すべての認証および認可のルール/プロファイルで「blacklist」を「blocked list」に置き換える
CSCvu87758	ゲストパスワードポリシー設定がアルファベットまたは数字で設定されていると保存できない
CSCvu90761	ISE の [Radius Live Sessions] ページで [No Data Found] と表示される
CSCvu91039	ISE 2.6 パッチ 7 が MAC リスト内のすべての MAC アドレスのルックアップを実行しないため、リダイレクトなしのポスチャが失敗する
CSCvu97657	エンドポイントのデバッグを有効にすると、ISE 2.4 アプリケーションサーバーが初期化状態になる
CSCvv00951	停止状態への移行中にアプリケーションサーバーがクラッシュする

問題 ID 番号	説明
CSCvv04416	エンドポイントデータがセカンダリ管理ノードに表示されない
CSCvv08466	ログ収集エラーアラームが表示される
CSCvv14001	共通タスクでセキュリティグループを選択すると、認可プロファイルが適切な属性で保存されない
CSCvv16401	pxGrid 内部クライアントを ping できない
CSCvv25102	ISE で TACACS+ および TCP を強化するための TCP 設定の変更
CSCvv29190	iOS 14 beta で BYOD フローが破損している
CSCvv30133	ディスカバリホストの説明テキストが紛らわしい
CSCvv35921	内部 ID ストア内の選択したユーザーに対して CSV エクスポートを開始できない
CSCvv36189	無効な IPv6 アドレスが原因で RADIUS に認証済みライブログが送信されない
CSCvv38249	カスタムポートのみが有効な場合、手動 NMAP が動作しない
CSCvv39000	LANDESK のポスチャ条件を作成できない
CSCvv41935	キーに < 記号または > 記号が含まれていると、PSK cisco-av-pair がエラーをスローする
CSCvv45174	スタティックホスト名 SGT マッピングの作成で SXP ドメインを選択できない
CSCvv48544	ISE で NIC チーミングが有効になっていると、ヘルスチェックが機能しない
CSCvv50721	Aruba ダイナミック URL リダイレクトを使用して NetworkSetupAssistant.exe のダウンロードリンクを取得できない
CSCvv52637	ISE ホットスポット ゲスト ポータル フローが破損している
CSCvv54761	現在のアクティブセッションのレポートのエクスポートでは、午前 0 時以降に更新されたセッションのみが表示される
CSCvv57639	TACACS コマンドセットでカッコ付きのコマンドを保存するとエラーが発生する（ISE 2.7 パッチ 2）
CSCvv57822	TRACE レベルのデバッグによって pxGrid ノードでデッドロックが発生する
CSCvv57830	コンテキストに空の値が追加され、グループの検索に失敗する

問題 ID 番号	説明
CSCvv58629	EST サービスを初期化する認証局サービスが ISE 2.7 パッチ 2 へのアップグレード後に実行しない
CSCvv59233	ISE RADIUS ライブログの詳細で、[Other Attributes] セクションに AD グループ名がない
CSCvv62549	エンドポイントの GUI ページに Clinda のカスタム属性が表示されない
CSCvv62729	存在しないネットワークデバイスを照会すると、ネットワークデバイス API コールがエラー 500 をスローする
CSCvv64190	ユーザー アイデンティティ グループで大文字と小文字が区別されると、[Select Sponsor Group Members] ウィンドウがロードされない
CSCvv67051	[RADIUS Server Sequences] ページに「no data available」と表示される
CSCvv67101	TAC サポートケースのリダイレクションの問題
CSCvv67743	状態別ポスチャ アセスメント レポートに、状態ステータスフィルタのあるデータが表示されない
CSCvv67935	認証プロファイルのセキュリティグループの値が取得直後に表示されない
CSCvv68028	AUP テキストを変更できない
CSCvv74373	ISE 3.0 DNS 解決可能性の誤アラーム
CSCvv74517	SAML アイデンティティ プロバイダーでの ISE 3.0 GUI の不具合
CSCvv77530	バインドパスワードで % 文字が 2 回以上使用されている場合、LDAP グループ/サブジェクト属性を取得できない
CSCvv77894	アップグレードおよびデータベースでの偏向のないテキスト/コード
CSCvv78097	ローカルリポジトリの使用状況情報が表示されない
CSCvv80113	ISE ポスチャ自動更新が実行されていない
CSCvv82806	ネットワークデバイス IP フィルタがサブネット内の IP と一致しない
CSCvv83510	RuleResultsSGTUpgradeService ステップで ISE 3.0 アップグレードが失敗する
CSCvv91234	プライマリ MNT がダウンしていると、ISE 2.6 のスケジュール済みレポートが機能しない
CSCvv91684	収集フィルタが [Logging] ページに表示されない

問題 ID 番号	説明
CSCvv92203	ISE 2.6 パッチ 6：「Employees」という名前で SGT を作成しようとすると「NetworkAuthZProfile with entered name exists」というエラーメッセージが表示される
CSCvv92613	スポンサーグループに属していないユーザーはスポンサーポータルにログインできない
CSCvw01829	Chrome 85/86で ISE GUI ログインページに次のエラーが表示される：問題が発生しました
CSCvw08292	削除メッセージの送信後も ACI マッピングが削除されない
CSCvw38853	ISE 2.6 パッチ 7：MAC OSX のマルウェア対策条件に Sophos 10.x の定義がない
CSCvw61595	ステップ UPSUpgradeHandler で ISE 3.0 の設定バックアップの復元が失敗する

Cisco ISE リリース 3.0 の未解決の不具合：累積パッチ 1

問題 ID 番号	説明
CSCvw73529	スマートライセンスのオンプレミスサテライトオプションのポーティングの変更

Cisco ISE リリース 3.0 の解決済みの不具合

問題 ID 番号	説明
CSCuo02920	ISE が access-reject で設定済みの Radius AVP 18 を返さない
CSCuz02795	ホームページの更新時に GET-BY-ID が実装されない例外
CSCva44035	ライブ認証で ISE が VPN ユーザーの MAC アドレスではなく IP アドレスを表示することがある
CSCvb55884	ISE RBAC ネットワークデバイスタイプ/ロケーションビューが機能しない
CSCvd38796	AD が authC と authZ の両方に使用されている場合、RA-VPN/CWA に対して AD ドメイン属性が取得されない
CSCve89689	MNT API が特殊文字をサポートしない
CSCvf30470	3.6.11362.2 コンプライアンスモジュールへのアップグレード後に MAC OX が失敗する

問題 ID 番号	説明
CSCvg50777	nas-update＝true アカウンティング属性により、セッションが削除されない
CSCvh77224	ENH // HTTPS プロキシを使用したスマートライセンスの登録が失敗する
CSCvi35647	マルチノード展開では、ポスチャセッション状態を PSN 間で共有する必要がある
CSCvi62805	CSCvi62805 ISE ODBC が設定されたストアドプロシージャに従って MAC アドレスを変換しない
CSCvj47301	ノードグループメンバーが到達不能の場合、ISE はアクティブ準拠のセッションに CoA を送信する
CSCvj59836	IOS デバイスのオンボードポータルでの入力ミス
CSCvj77817	OS のアップグレード時に 2.3P4、2.4P3 のアップグレードが失敗する
CSCvk04307	ISE ゲスト/BYOD ポータルの再試行が 1.1.1.1 にリダイレクトされる
CSCvk50684	ホスト名の変更時に、RADIUS DTLS とポータルの使用が新しい自己署名証明書に割り当てられない
CSCvn02461	Cisco IP Phone のプロファイラ更新を含める：8832、7832
CSCvn12644	AD 属性のポリシー評価中に ISE がクラッシュする
CSCvn48096	コンテキストの可視性のページ全体のすべてのエンドポイントのチェックボックスを選択しても機能しない
CSCvn73740	エンドポイントプロファイルが不明に設定されていない EAP-TLS 認証は、2 番目の認証で失敗する。
CSCvn99149	要求キャッシュの制御が private、no-cache、および no-store に設定される
CSCvo15770	コンテキストの可視性でアドレスが HTML コードとして表示される
CSCvo22887	ISE 2.4 URT は、ノードがサポートされているアプライアンス上にあることを確認しない
CSCvo28970	Cisco 経時的エージェントを使用すると、AnyConnect に Cisco NAC エージェントエラーが表示される
CSCvo84056	ページのカスタマイズで [Self-Reg Success] ページの [Username/password] を有効または無効にしてもページのカスタマイズに保持されない
CSCvo87602	バージョン 2.4.44 を実行している openldap rpm を使用した ISE ノードでのメモリリーク
CSCvp42493	ゲスト ERS API の「SearchResult」の合計が他の API と一致しない

問題 ID 番号	説明
CSCvp59038	ISE セカンダリ PAN ノードが送信元アドレス 169.254.2.2 で RST を他の ISE ノードに送信する
CSCvp61452	（機能拡張）パッチのインストールフェーズ中にアーカイブが削除される
CSCvp85813	特定の NAS IP アドレスを使用してフィルタ処理するオプションが ISE TACACS ライブログにない
CSCvp88443	新しい論理プロファイルが認証ポリシーの例外で使用されている場合でも、ISE CoA が送信されない
CSCvp93322	有効期限テスト中に MNT でメモリが大幅に増加する
CSCvq12204	リロード後に ISE 2.4 SNMPv3 ユーザーが誤ったハッシュで追加され、SNMPv3 認証が失敗する
CSCvq13431	ポスチャと RADIUS フロー中、コンテキスト属性を取得している間に ISE PSN ノードがクラッシュする
CSCvq43600	PSN ペルソナが無効になっていても、TACACS ポート 49 が開いたままになる
CSCvq48396	レプリケーション失敗アラームが生成され、ise-psc.log に ORA-00001 例外が表示される
CSCvq61089	SAML 認証を使用した BYOD オンボーディング後、デバイスポータルにデバイスが表示されない
CSCvq70247	自己登録ゲストポータルのプレビューに「Registration Code」ラベルが表示されない
CSCvq88821	AP に接続されたアクセススイッチ上の SNMP トラップによって不正なプロファイリングが発生する
CSCvq90601	EAP チェーン：動的属性値が使用できない
CSCvr07294	RADIUS 認証と RADIUSアカウントレポートのパフォーマンスが遅い
CSCvr22373	機能拡張：ネイティブイベントログ API、パッシブ ID 機能の EVT API をサポート
CSCvr39943	脅威イベントに対するアクションの空白のコースが CTA クラウドから TC-NAC アダプタに受信された
CSCvr40545	秘密キーの暗号化に失敗したときに、共有暗号がないため EAP-FAST 認証に失敗した

問題 ID 番号	説明
CSCvr40574	秘密キーの暗号化で ISE GUI にエラーメッセージがあったときに、ISE GUI でエクスポートに失敗した
CSCvr44495	pxGrid が MnT イベントをパブリッシュしない
CSCvr48726	（機能拡張）SCCM の対応デバイス再認証クエリの時間間隔の範囲を拡大
CSCvr68432	REST を介して追加された 2.4P10 エンドポイントには「編集」モードでのみポリシーの割り当てが表示される
CSCvr68971	ISE IP ルーティングの優先順位の問題
CSCvr70044	高負荷時に ISE ポスチャモジュールに「No policy server detect」が表示される
CSCvr81384	ネットワークデバイスの CSV インポートが失敗し、理由なくサイレントにプロセスが終了される
CSCvr83696	ISE：アカウント OU の変更後、キャッシュ済みの AD OU を新しい OU よりも優先させる
CSCvr84143	ISE ゲスト OS で tzdata を更新する必要がある
CSCvr85363	ユーザー API による ISE アプリのクラッシュ
CSCvr87373	ACI マッピングは SXP pxGrid トピックにパブリッシュされない
CSCvr95948	接続の切断後に ISE が外部 syslog 接続を再確立できない
CSCvr96003	SYSAUX テーブルスペースが AWR および OPSSTAT データでいっぱいになる
CSCvs03810	ユーザーの入力が 2 回異なると、ISE は RADIUS レポートに正しいユーザーを表示しない
CSCvs04433	ISE：TACACS：TACACS+ の PSN クラッシュ
CSCvs05260	App server と EST サービスが毎朝 1 時にクラッシュ/再起動する
CSCvs07344	ISE：正常に終了しているにもかかわらず、2.4 パッチ 9 のリセット設定がいくつかのエラーをスローする
CSCvs09981	ISE のグループノード間の MAR キャッシュチェックが原因で失敗した COA を除外する機能を追加する
CSCvs19481	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvs23628	ルールが一致した後でも、ポリシーエンジンがすべてのポリシーセットの評価を続行する

問題 ID 番号	説明
CSCvs25258	ブルートフォースのパスワード攻撃に対する動作を改善する
CSCvs25569	無効なルート CA 証明書が受け入れられた
CSCvs36036	ISE 2.6 では、ユーザーが IPv4 または IPv6 を選択しても、dACL シンタックスに複数の空白行が許可される必要がある
CSCvs36150	ISE 2.x ネットワーク デバイス スタックのローディング
CSCvs36758	ISE 2.6 で 2 つのカッコを使用して CRL URL を設定できない
CSCvs38883	古いデータをプッシュする TrustSec マトリックス
CSCvs39633	NAD グループ CSV のインポートでは、説明フィールドにサポートされているすべての文字を許可する必要がある
CSCvs39880	Xms 値を持つ Mnt ノードの高負荷
CSCvs40406	信頼できる CA 証明書の削除中に SEC_ERROR_BAD_DATABASE がシステム/アプリデバッグログに表示される
CSCvs41571	自己登録済みゲストポータルがゲストタイプの設定を保存できない
CSCvs42072	静的グループの割り当てを編集できない
CSCvs42441	SMS と LDAP ページでサーバーから返されたサービス アカウント パスワード
CSCvs42758	CRL が特定の条件で期限切れになる
CSCvs44006	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvs44795	ISE が SGT を正しく更新しない
CSCvs46274	RADIUS アカウンティングレポートが機能しない：アカウンティングレコードが表示されない
CSCvs46399	URL リダイレクトの AuthZ プロファイルの詳細プロファイルでカスタム HTTPS 宛先が許可されない
CSCvs46853	DNA-C との統合中に、信頼できるストアから削除されたものと同じ CN の ISE 2.6 CA 証明書
CSCvs46998	条件はライブラリから削除されたが、DB 内にある
CSCvs47941	ISE2.6 で内部 CA とキーをインポートできない
CSCvs50437	ISE バージョンが新しい Oracle データベースと互換性のない古い JDBC バージョン（11.2.0.3）を使用する

問題 ID 番号	説明
CSCvs51296	ISE では、コマンドセットのコマンドの前にスペースを挿入できる
CSCvs51519	NFS マウントが原因でクラッシュする
CSCvs51537	暗号化キーの特殊文字でバックアップがトリガーされない
CSCvs52031	MACAdress API が機能していない（API/mnt/Session/MACAddress）
CSCvs53606	ISE 2.4：管理者ログインレポートが証明書ベースの管理者認証を使用すると認証に失敗する
CSCvs55464	スポンサーポータルで新しいユーザーを作成すると、「invalid input」が表示される
CSCvs55594	ランダム認証の場合、期限切れまでの日数が 0 としてマークされる
CSCvs56617	キャプティブポータルでユーザーが自由に電子メールの送信をトリガーできる
CSCvs58106	NAD CSV のインポートでは、サポートされているすべての文字を TrustSecDeviceID に許可する必要がある
CSCvs60518	ISE 管理者ユーザーが内部ユーザーのグループを変更できない
CSCvs62081	コレクタログに pxGrid メッセージと DNAC メッセージが繰り返し入力される
CSCvs62586	REST API を使用すると Tacacs プロファイルが正しく取得されない
CSCvs62597	認証プロファイルが REST API を使用して正しくプルされていない（改ページがない）
CSCvs65467	Cisco Identity Services Engine のストアドクロスサイト スクリプティングの脆弱性
CSCvs65989	ネットワークデバイス/グループをインポートした後、新しいロケーションを追加できない
CSCvs67042	ISE 2.2+ がメモリリークの影響を受ける Inflater() によってネイティブメモリが毎日 1 ー 2% 増加する
CSCvs68914	ERS API を介して下線を使用してセキュリティグループを作成すると、ISE エラーが発生する
CSCvs69726	ISE 2.2+ がメモリリークの影響を受ける PORT_Alloc_Util() によってネイティブメモリが毎日 1 ー 2% 増加する
CSCvs70997	ISE：SCEP RA の設定時に 2.4p9 CA 中間証明書がインストールされない

問題 ID 番号	説明
CSCvs75068	エラーをスローするため、%または<を含むレジストリキー値条件を追加できない
CSCvs75274	「証明書プロビジョニングポータル」のポータルカスタマイズを実行できない
CSCvs76257	RadiusProxyFlow::stripUserName() にユーザー名ではなく空の文字列があるために ISE がクラッシュする
CSCvs77182	ISE：属性「url-redirect」を HTTPS で使用できず、HTTP を使用する同じ URL は正常に機能する
CSCvs78160	INetworkAuthZCheck の ConditionsData 句で URT が失敗する
CSCvs79836	期限切れの証明書が削除対象としてリストされていない
CSCvs82557	SXP バインディングが pxGrid 2.0 クライアントに公開されない
CSCvs83303	中間更新が DB に保存されていない場合、API がデータを取得しない
CSCvs85970	AD join-point に文字列「TACACS」があると、AuthZ 条件で AD joinpoint が表示されない
CSCvs86344	ゲストユーザー名に@記号（guest@example.com）が含まれていると、ISE 2.4 Guest ERS Call Get-By-Name が失敗する
CSCvs86775	ISE 2.6 インストール：検証の入力 - IP ドメイン名の確認
CSCvs88368	ハッシュパスワードを使用すると ISE SNMP サーバーがクラッシュする
CSCvs89440	PAN 専用ノードの CEPM スキーマ統計情報が収集/スケジュールされない
CSCvs89683	ADE-OS ログにプレーンテキストで出力する RabbitMQ ユーザーパスワードは、マスクするか削除する必要がある
CSCvs91026	設定リセット後に Docker イメージ ise-rabbitmq を正常にロードできない
CSCvs91408	LONG：耐用年数テストの PMNT ノードでメモリが大幅に増加する
CSCvs91808	特殊文字を含むメタデータ XML ファイルをインポートすると、サポートされていないタグエラーが発生する
CSCvs96516	複数ある 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
CSCvs96541	OP バックアップの復元後に TACACS の認証/アクセスレポートが表示されない

問題 ID 番号	説明
CSCvs96544	エンドポイント CSV ファイルを CV 2.4 パッチ 9 にインポートすると、[description] フィールドが保持されない
CSCvs96560	多数のエンドポイントが存在する場合、ISE ERS API ルックアップが遅くなる
CSCvs97302	.dmp ファイルが ISE の reset-config の後でも /opt/oracle/base/admin/cpm10/dpdump から削除されない
CSCvs98094	ISE 2.7 サーバーでのテスト中にファイル修復チェックが失敗する
CSCvt00283	ゲストスポンサーポータルの成功ページ更新時の 404 エラー
CSCvt00780	BYOD ウェルカムページで OS 検出メッセージのメッセージをローカライズできない
CSCvt01161	NMAP：ISE のバージョン 2.6 で MCAFeeEPROOrchestratorClientscan を実行できない
CSCvt03094	ISE の期限切れの TACACS セッションがセッションキャッシュからタイムリーにクリアされない
CSCvt03292	Cert Revoke と CPP が APEX ライセンスなしで機能しない
CSCvt03935	TrustSec ポリシーマトリックス -- ISE の [View] オプションの表現を変更する
CSCvt04047	バックアップ/復元メニューに移動した後、すべての ISE ページで POST getBackupRestoreStatus が発生する
CSCvt04144	アラーム設定での高ディスク使用率のしきい値オプションがない
CSCvt05201	トンネルグループポリシー評価によるポスチャが Java Mem を減らしている
CSCvt07230	ISE がインポート時にイーグレスポリシーで ANY を許可しない
CSCvt08143	ISE 2.6 の時差
CSCvt09164	ISE 2.2 P16 すでに拡張されたゲストユーザーを再拡張できない
CSCvt09434	SCCM サーバータイムアウトを処理するための適切なロギングとレポートを追加
CSCvt09458	ISE MDM 統合：デバッグでの誤解を招く COA タイプ
CSCvt10214	[ENH] ネットワークデバイスの API を使用して「GET|PUT|DELETE by Name」機能を追加する

問題 ID 番号	説明
CSCvt11130	sh version コマンドが ISE の管理者以外の CLI ユーザーで動作しない
CSCvt11179	この OS 属性が AD サーバーで変更されると「AD-Operating-System」属性が取得されない
CSCvt11366	CLI からエンドポイントをエクスポートすると Java の例外が発生する
CSCvt11380	DNAC が GBAC を管理しているとしても、ポリシーセット内で SGT を作成できる
CSCvt11664	「createLicenseSource」メソッド「FlexlmListException:Error」で ISE フィードサーバーが失敗する
CSCvt12236	IP SGT スタティックマッピングのインポートがホスト名で正しく動作しない
CSCvt13707	pxGrid 2.0 WebSocket 分散アップストリーム接続の問題
CSCvt13719	pxGrid 2.0 WebSocket ping pong がアイドル状態のスタンドアロンでも遅すぎる
CSCvt13746	追加の authz ポリシーと例外がある場合、ISE はすべてのデバイス管理 authz ルールを表示しない
CSCvt14248	EST サービスを初期化する認証局サービスが ISE 2.6/2.7 へのアップグレード後に実行されない
CSCvt15256	「ゲストユーザー」ID ストアを使用すると、認証プロセスが失敗する。
CSCvt15893	バグの防止：ISE 2.6 へのアップグレード後、エラーサプリカント/不良構成サプリカントの Radius テーブルが存在しない
CSCvt15935	システムサマリーダッシュボードと一致する高負荷アラームが一部のノードに表示されない
CSCvt16882	Apple CNA と AUP をリンクとして使用して iPad にアクセスすると、400 Bad 要求エラーが発生する。
CSCvt17283	AVC の有効化時に GUI の速度が低下する
CSCvt17783	ISE では、SGT のインポートまたはエクスポートで ANY SGT または値 65535 を公開できない
CSCvt18613	TEAP - EAP チェーニングの場合に AD グループでの AuthZ の条件が一致しない
CSCvt19657	多数のエンドポイントが存在する場合、ISE ERS API エンドポイントの更新が遅い

問題 ID 番号	説明
CSCvt22900	「*Endpoint Consumion Count Updated:」がライセンスで更新されない
CSCvt24276	許可された値をシステム使用ディクショナリへの7つ以上の属性に追加/変更できない
CSCvt25610	ISE2.7 コンプライアンスカウンタが 0 になっている
CSCvt26108	ISE 2.7 の Anyconnect の設定の遅延アップデートが保存されない
CSCvt34876	ISE で RADIUS と 高 CPU への対応が遅延する
CSCvt35044	EP ルックアップに時間がかかり、ゲストフローの遅延が大きくなる
CSCvt35239	clientMac が null の場合、ポスチャフロー時に catalina.out で NullpointerException がスローされる
CSCvt36117	アイデンティティグループが ERS を介して ISE の内部ユーザーを更新する
CSCvt36322	リダイレクト値が URL に存在する場合、ISE 2.6 MDM フローが失敗する
CSCvt36452	ISE の評価プロファイラライセンスが期限切れになると、デフォルトの radius プローブが有効になる
CSCvt37910	[ENH] /ers/config/internaluser の API を使用して「GET|PUT|DELETE by Name」機能を追加する
CSCvt38308	ISE：min pwd の長さを増やすと、既存の短い pwd の GUI を使用したログインがエラーなしで失敗する
CSCvt40534	MNT ノード選択プロセスが適切に設計されない。
CSCvt42064	ISE が SSH ログインとしてポスチャ セッション ルックアップ コールを誤って報告する
CSCvt43844	ISE：runtime-aaa デバッグでパケットの詳細が ASCII で出力されない。エンドポイントデバッグが中断される
CSCvt46584	ENDPOINTS_REJECT_RELEASE テーブルが消去さないディスク領域の問題でバックアップが失敗する
CSCvt46850	条件ライブラリを使用して保存された複合条件を編集できない
CSCvt49961	FQDN を使用して設定された Syslog ターゲットによってネットワークが停止する可能性がある
CSCvt53541	SMS over HTTPS でゲートウェイにユーザー名/パスワードが送信されていない

問題 ID 番号	説明
CSCvt55300	redis の IP 属性が削除されていても「現在の IP アドレス」が CV に表示される
CSCvt55312	Apple CNA を使用した ISE BYOD が 9800 で失敗する
CSCvt57274	昨日と今日の認証サマリーレポートにデータが表示されない
CSCvt57571	IP-access がエントリなしで送信された場合、App-server がクラッシュする
CSCvt57805	REST API 更新操作の断続的なパスワードルールエラー
CSCvt61181	ISE ERS API：SNMP 設定の処理中のネットワークデバイスで GET コールが遅くなる
CSCvt63793	ポスチャ：LSD が不一致の場合に、「No policy server detected」というメッセージが表示されてリダイレクション以外のフローが失敗する
CSCvt65332	2 行を使用した説明、または <Enter> が使用された場合、クライアント プロビジョニング リソースが errorA をスローする
CSCvt65719	誤解を招く NULL ポインタ例外。手動後同期が実行される
CSCvt65853	ISE-2.x：分散方展開で使用されると再認証の MNT REST API が失敗する
CSCvt67595	ユーザー認証に失敗したため、ライブログが表示されない
CSCvt69912	ISE が誤検出アラーム「Alarms：Patch Failure」を生成する
CSCvt70689	MAR キャッシュレプリケーションが有効になっていると、アプリケーションサーバーがクラッシュすることがある
CSCvt71355	pxGrid で INIT 状態のユーザーを削除できない
CSCvt71559	アラームダッシュレットに「No Data Found」と表示される
CSCvt73953	CLI エクスポートとコンテキストの可視性の情報が一致しない
CSCvt76509	SFTP リポジトリにスペースがないが、ISE バックアップファイル転送ログに [Success] と表示される
CSCvt80285	定義用のマルウェア対策条件の作成時に 45 以上の製品を選択できない
CSCvt81194	ポリシー HitCountCollector で CPU スパイクが観察される
CSCvt82384	diagnostics.log のローテーションが ISE で機能しない
CSCvt85722	動作していない MNT ウィジェットのデバッグログがない
CSCvt85757	スポンサーポータルで英語以外の文字が？と表示される

問題 ID 番号	説明
CSCvt85836	セッションキャッシュが不完全なセッションでいっぱいになる
CSCvt87409	ISE DACL 構文チェックで IPv4 形式エラーが検出されない
CSCvt89098	失敗したノードのワイルドカード複製が ISE で再試行されない
CSCvt91871	ISE RADIUS アカウンティングレポートの詳細で [Accounting Details] に [No data found] と表示される
CSCvt93117	ise-psc.log が「check TTConnection is valid」でいっぱいになり、関連するログがロールオーバーする
CSCvt93603	ISE 2.6p6 がカスタムエンドポイント属性を削除できない
CSCvt96594	ISE 2.6：ERS を介した外部スポンサーユーザーを使用したゲストユーザーの作成が 401 Unauthorized Error で失敗する
CSCvu04874	io.netty.buffer.PoolChunk での疑わしいメモリリーク
CSCvu05164	ISE で、NAD の Radius を API を使用して無効にできない
CSCvu10009	内部ユーザーで Update-By-Name メソッドを使用する場合の必須値
CSCvu15948	TC-NAC アダプタが nexpose（insiteVM）でスキャンを停止した
CSCvu16067	IP-TABLES ISE 2.6 の変更によってTCP 遅延、TACACS 遅延が発生する
CSCvu20359	ファイル名にドット（.）を含むファイルチェック条件を使用すると、マークアップ言語エラーが発生する
CSCvu21093	ISE 2.6p6：ポータルの背景が正しく表示されない
CSCvu25625	ISE が DNAC からの REST API コールに対して誤ったバージョンを返す
CSCvu25975	TACACS コマンドセットでインポートオプションが機能しない
CSCvu28305	ISE ロギングタイムスタンプに将来の日付が表示される
CSCvu29434	SNS 3655 PSN でのリロード後に ISE2.6P6 サービスを初期化できない
CSCvu30286	複数のマトリックスから単一のマトリックスへの移動後、ERS SGT の作成が許可されない
CSCvu31176	2.4P11 VPN + ポスチャ：Apex ライセンスが消費されない
CSCvu31853	ERS によって追加された NDG が、DB 内のすべてのネットワークデバイスに関連付けられる

問題 ID 番号	説明
CSCvu32240	内部ユーザーの更新に ISR ERS API を実行すると、既存の identityGroups 値が null に設定される
CSCvu32865	ISE 2.7 で CPU 使用率が高く、認証遅延が発生する
CSCvu33416	有効なライセンスでのライセンスのコンプライアンス違反アラーム
CSCvu33861	ISE 2.4 p6：MAC アドレスでデバイスを取得する REST API MnT クエリに 2 秒以上かかる
CSCvu34433	ISE 2.x：isehourlycron.sh cron スクリプトに従って Undo テーブルスペースの空き領域がクリアされない
CSCvu34895	レポートリポジトリのエクスポートが有効な専用 MnT で機能しない
CSCvu35802	AD ユーザーの共有電子メールがグループを取得できず、ISE がフォレストに複数のアカウントを表示する
CSCvu39653	MAC アドレスのセッション API が「Char 0x0 out of allowed range」を返す
CSCvu41815	（CFD）AuthZ プロファイルが異なる SG の同じ VN にマッピングされている場合、SG から VN を削除すると GBAC 同期が中断する
CSCvu42244	EAP-TLS を介したマシン認証が、ユーザーが見つからないというエラーを示して許可フロー中に失敗する
CSCvu47395	ISE 2.x、3.x：高メモリの問題があるシステムには Drop_Cache が必要となる
CSCvu48417	ISE ERS API DELETE デバイスが複数のコールでエラー 500 を返す
CSCvu49019	Elastic Search でメモリリークの疑いがある
CSCvu49724	DNAC で設定された SNMP v2c バージョンのデバイスが ISE のネットワークデバイスに表示されない
CSCvu53022	ISE：アカウント OU の変更後、キャッシュ済みの AD OU を新しい OU よりも優先させる
CSCvu53836	ISE 承認のみの要求が内部ユーザーグループに対して評価されない
CSCvu55332	REST API コールで、ポリシーセットで参照されているネットワーク デバイス グループを削除できる
CSCvu55557	RADIUS の 最小 4 文字の秘密の要件が REST API を使用して NAD を作成すると確認されない
CSCvu58476	アイデンティティストアに問題がある場合の My Device ポータルのエラーメッセージの改善

問題 ID 番号	説明
CSCvu58793	場所別でフィルタ処理すると、ERS REST API が重複する値を複数回返す
CSCvu59093	ISE から Session DB 列が欠落している（2.4 以上）
CSCvu59491	ISE が insiteVM（tc-nac サーバー）に新しいサイトを作成する
CSCvu63642	コンテキストの可視性により、ユーザー名の更新時にエンドポイントパラメータが融合される
CSCvu63833	AD がアイデンティティソースとして選択されている場合、監査レポートに ISE GUI への失敗したログインが表示されない
CSCvu67707	CWE-937 既知の脆弱性を含む JavaScript ライブラリの使用
CSCvu68700	無効なクレデンシャルを使用した ISE 2.6 p5 ERS API の XML または JSON 要求への応答が予期しない HTML 本文で HTTP 401 になる
CSCvu70683	ERS クエリでは、iselocalstore.log での抑制とともにアラーム抑制が必要
CSCvu70768	アラームとシステムの概要が ISE GUI に表示されない
CSCvu73387	「12308 Client sent Result TLV indicating failure」という理由で認証が失敗する
CSCvu74198	ISE：LDAP と ODBC のアイデンティティストア名にハイフンを使用できない
CSCvu83759	sftp リポジトリでの変更後に ISE がキーペアを削除する
CSCvu90107	ISE ではすべてのバージョンの ERS フローでデバイス ID の重複が許可される
CSCvu90703	CLDAP スレッドがハングし、無限に実行している
CSCvu91016	ATZ ポリシーの内部ユーザー属性が TACACS+ ASCII 認証に失敗する
CSCvu91601	ISE 認証ステータス API のコール期間が予想どおりに機能しない
CSCvu94733	不正なパスワードに対して「Account is not yet active」というメッセージが表示され、ゲスト認証が失敗する
CSCvv00377	サブネットと IP 範囲を使用しているネットワークデバイスの重複
CSCvv07049	ISE は、ポート番号を使用すると「Connection failed」で ODBC と接続できない
CSCvv09167	TACACS 集約テーブルが正しく消去されない

問題 ID 番号	説明
CSCvv15811	IP アドレスが割り当てられたシャットダウン インターフェイスがある場合、ISE TCP ポート 84xx が開かない
CSCvv23256	ISE 認証ステータス API コールが、指定された時間範囲のすべてのレコードを返さない
CSCvv26811	暗号化で保存された後、ポリシーのエクスポートが暗号化なしで保存されない
CSCvv44914	isedataupgrade.sh に失敗する。ISE グローバルデータの更新（ISE 2.6P6 から 2.7、3.0）が失敗した
CSCvr63698	セッションディレクトリに pxGrid 2.0 認証プロファイル属性がない
CSCvp93901	pxGrid で ADUser、ADHost、SamAccountName、および QualifiedName をパブリッシュする
CSCve58268	ベースラインステータスを確認するための SCCM クエリ機能を ISE に追加する
CSCve58212	設定項目ステータスを確認するための SCCM クエリ機能を ISE に追加する

Cisco ISE リリース 3.0 の未解決の不具合

問題 ID 番号	説明
CSCvq75448	SGT がある場合、ISE の FMC サブスクリプションを使用できない
CSCvr24059	送信元 SGT の相関が FMC および FTD 6.5 で機能しない
CSCvv45728	ISE 管理 GUI の一部のラベルが日本語に変換されない
CSCvv54305	[Support TrustSec Verification reports] チェックボックスを有効にすべきではない
CSCvv54754	IE の最新バージョン：DB 復元セットアップ時にゲストポータルページでポータルタイルが重複している
CSCvv55971	IE GUI：ヘルスチェックページのモジュール名が進捗バーと情報アイコンで重複しているか、または位置がずれている
CSCvv57822	TRACE レベルのデバッグによる pxGrid ノードのデッドロック
CSCvv58353	HTTPS サーバーリストの設定が 2.7 P1 から ISE 3.0 へのアップグレード後に永続的でなくなる
CSCvt97146	（ISE-3.0）ISED が WSA で継続的にクラッシュする

問題 ID 番号	説明
CSCvu78668	（ISE3.0）：セッションが存在しない場合に ISE-WSA 統合が失敗する
CSCvv66302	ドメインが SXP ピアに割り当てられない
CSCvv67101	TAC サポートケースのリダイレクションの問題
CSCwc83059	フルアップグレード後の VCS 情報がない

通信、サービス、およびその他の情報

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

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。