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

コンテンツ

Cisco Identity Services Engine リリース 3.4

Cisco ISE リリース 3.4 では、パフォーマンス、拡張性、およびセキュリティを強化する重要な改善が多数行われています。このリリースでは、Duo 接続へのアイデンティティ同期設定などの機能が導入されており、管理者は初期セットアップ後にユーザーデータの同期を柔軟に管理できます。パフォーマンスの向上には、アップグレード時の自動ログバンドルの生成やバックアップログ機能の改善が含まれます。これにより、障害対応プロセスがよりスムーズかつ効率になります。FIPS 140-3 規格に沿って、ネイティブ IPSec を使用する仮想トンネルインターフェイスの設定を導入し、機密情報がプレーンテキストで伝送されることを防ぐパスワードセキュリティ対策を強化することで、セキュリティの有効性が強化されます。

新しい認証局診断ツール、Cisco ISE GUI から TAC サポートケースを直接開く機能、承認応答の信頼性を高めるダイナミック アクセス コントロール リストの動作の改善など、使いやすく展開しやすくするためのさまざまな拡張機能が優先順位に応じて導入されています。このリリースでは、TrustSec 統合用の PAC レス RADIUS 通信もサポートされています。これにより、セキュアな通信を維持しながら、設定の負担が軽減されます。GUI の機能拡張と API の改善（show version コマンドへのホットパッチの詳細の追加や、pxGrid を使用して使用可能な新しいセッション ディレクトリ トピックなど）。これにより、ユーザー体験がさらに合理化され、業務効率が向上します。さらに、複数の Cisco Application Centric Infrastructure コネクタのサポートにより、さまざまなネットワーク環境でアクセスポリシーを管理する範囲が拡張され、ピボタル セキュリティおよび管理ソリューションとしての Cisco ISE のロールが強化されます。

このドキュメントでは、Cisco ISE リリース 3.4 の機能、問題、および制限事項について説明します。

表 1. 新機能および変更情報

日付	説明
2026-04-23	Cisco ISE リリース 3.4 累積パッチ 6 の正式版。
2026-02-23	Cisco ISE リリース 3.4 累積パッチ 5 の正式版。
2025-11-04	Cisco ISE リリース 3.4 累積パッチ 4 の正式版。
2025-08-05	Cisco ISE リリース 3.4 累積パッチ 3 の正式版。
2025-06-20	Cisco ISE リリース 3.4 累積パッチ 2 の正式版。
2024-12-18	Cisco ISE リリース 3.4 累積パッチ 1 の正式版。
2024-08-04	Cisco ISE リリース 3.4 の一般可用性

新しいソフトウェア機能

このセクションでは、このリリースで導入された新しいソフトウェア機能について簡単に説明します。

Cisco ISE リリース 3.4 パッチ 6 の新機能

表 2. Cisco ISE リリース 3.4 累積パッチ 6 の新機能

製品への影響	機能	説明
ソフトウェアの信頼性	Cisco pxGrid および IMS のサーバー EKU 証明書を許可する	Cisco ISE は、Cisco pxGrid および IMS 用にサーバー認証 EKU のみを含むサーバー証明書の使用をサポートします。この更新により、サービスは新しいパブリック CA 標準との互換性が維持されます。内部サービスの場合、Cisco ISE 内部 CA を使用して外部証明書の依存関係を回避してください。
使いやすさ	SGACL シンタックスの検証	Cisco ISE のシンタックス検証機能を使用して、セキュリティグループ ACL（SGACL）コマンドを確認して、正確なポリシー設定を確認できます。**シンタックスの検証** オプションを使用して、ACL を作成または編集する際に、SGACL シンタックスを検証できます。標準の IPv4 および IPv6 形式に対してコマンドを検証できます。

Cisco ISE リリース 3.4 パッチ 5 の新機能

Cisco ISE リリース 3.4 パッチ 5 には新機能はありません。

Cisco ISE リリース 3.4 パッチ 4 の新機能

表 3. Cisco ISE リリース 3.4 累積パッチ 4 の新機能

製品への影響	機能	説明
使いやすさ	Active Directory ユーザーのロックアウトを防止するための TACACS+ のサポート	[Active Directoryユーザーロックアウトの防止（Prevent Active Directory User Lockout）] オプションを使用すると、パスワードが正しくないログイン試行が繰り返し失敗することによるユーザーロックアウトを減らすことができます。この機能は、RADIUS プロトコルと TACACS+ プロトコルの両方でサポートされています。Cisco ISE はこれらのプロトコルを使用して、認証要求を管理して過剰な試行失敗を制限することで Active Directory でのアカウントロックアウトを最小限に抑えます。
	ワークロード コネクタ エンドポイント ダッシュボード	[コンテキストの可視性（Context Visibility）] ページの [ワークロード コネクタ エンドポイント（Workload Connector Endpoints）] ダッシュボードでは、ワークロードコネクタに関連するデータを効率的に収集、分析、およびレポートできます。このダッシュボードには、**ワークロードコネクタ（Workload Connectors）** ページで収集されたエンドポイント属性情報が表示されます。エンドポイントの IP アドレスをクリックすると、エンドポイント分析用の詳細な属性情報にアクセスまたはダウンロードできます。
	低速な外部リソースと過剰な TACACS+ アクティビティの新しいアラーム	Cisco ISE でのシステムモニタリングと障害対応を強化するために、新しいアラームが導入されました。これらの新しいアラームにより、外部システムへのアクセスの遅延や TACACS+ デバイスからの過剰な通信トラフィックなどの問題を検出し、問題の特定と対処に役立ちます。これらのアラームは以下を検出します。 • Cisco ISE ノード間での ping または通信の大きな遅延 • Active Directory（AD）接続での速度低下。 • Lightweight Directory Access Protocol（LDAP）接続での速度低下。 • オープン データベース接続（ODBC）接続での速度低下。 • 過剰な TACACS 通信

製品への影響	機能	説明
	Entra ID EAP-TLS および TEAP-TLS を使用したユーザーおよびデバイスの認証	Cisco ISE では、EAP または TEAP チェーンを介してデバイスとユーザーを承認できるようになりました。証明書ベースの認証と Microsoft Entra ID からのリアルタイム情報を組み合わせることにより、セキュアなネットワーク アクセス コントロールが可能になります。 認証中、Cisco ISE は Microsoft Entra ID に直接アクセスせずに、デバイスまたはユーザーによって提示された証明書を評価します。認証では、ポリシーの REST ID ストア属性条件または REST ID ストアグループが設定できます。承認中、Cisco ISE は Microsoft Entra ID をクエリし、関連するユーザー、グループ、デバイスの属性を取得します。この情報は、Cisco ISE が情報に基づいて承認するかどうかを判断するために使用します。
	SMTP に向けた OAuth のサポート	Cisco ISE GUI で Simple Mail Transfer Protocol（SMTP）サーバーの認証設定を有効または無効にできます。このリリースでは、基本パスワード認証に加えて、Microsoft OAuth 認証のサポートも追加されています。
ハードウェアの信頼性	Cisco Secure Network Server 3800 シリーズ アプライアンスのサポート	Cisco Secure Network Server（Cisco SNS）3800 シリーズ アプライアンスは、Cisco Unified Computing System（Cisco UCS）C225 M8 ラックサーバーに基づいており、特に Cisco ISE をサポートするように構成されています。Cisco SNS 3800 シリーズ アプライアンスは、幅広いワークロードで高いパフォーマンスと効率性を提供するように設計されています。 Cisco SNS 3800 シリーズ アプライアンスには次のモデルがあります。 • Cisco SNS 3815（SNS-3815-K9） • Cisco SNS 3855（SNS-3855-K9） • Cisco SNS 3895（SNS-3895-K9） Cisco SNS 3815 アプライアンスは、小規模な展開に適しています。Cisco SNS 3855 および Cisco SNS 3895 アプライアンスには、ハードディスクや電源などの複数の冗長コンポーネントがあり、信頼性の高いシステム構成を必要とする大規模な展開に適しています。PAN および MnT ペルソナには Cisco SNS 3895 が推奨されます。 Cisco SNS 3800 アプライアンスには、次の OVA、ISO、およびアップグレード バンドル ファイルのみを使用する必要があります。 • Cisco-vISE-300-3.4.0.608b.ova • Cisco-vISE-600-3.4.0.608b.ova • Cisco-vISE-1200-3.4.0.608b.ova • Cisco-vISE-2400-3.4.0.608b.ova • ise-3.4.0.608b.SPA.x86_64.iso • ise-upgradebundle-3.1.x-3.3.x-to-3.4.0.608b.SPA.x86_64.tar.gz • ise-urtbundle-3.4.0.608b-1.0.0.SPA.x86_64.tar.gz Cisco SNS 3800 アプライアンスは、Cisco ISE リリース 3.4 パッチ 4 以降でサポートされています。 **注**：Cisco SNS 3855 アプライアンスは、1 つのハードディスクまたは 4 つのハードディスクで構成できます。Cisco SNS 3855 アプライアンスが 1 つのハードディスクのみで構成されている場合は、PSN または pxGrid のペルソナのみを有効にすることを推奨します。

製品への影響	機能	説明
ソフトウェアの信頼性	Red Hat OpenShift プラットフォームのサポート	Cisco ISE リリース 3.4 パッチ 4 は、Red Hat OpenShift プラットフォームをサポートしています。Red Hat OpenShift Virtualization プラットフォームに Cisco ISE VM を展開できます。これにより、単一のプラットフォームで VM とコンテナのワークロードを実行および管理することが可能になります。 **注**：Red Hat OpenShift プラットフォームのサポートでは、この ISO ファイル（ise-3.4.0.608b.SPA.x86_64.iso）のみを使用する必要があります。
	プロファイラ トラフィック プローブのモニタリング	次の拡張機能により、Cisco ISE プロファイラサービスのレジリエンスと安定性が向上します。 • チャットのエンドポイントに対するプローブ関連の処理は、事前定義されたクールオフ期間中一時停止されます。これにより、トラフィックの多い環境でのシステム負荷が軽減されます。 • プロファイラのキューの使用率は、定義されたしきい値（中、高、および最大の負荷）に基づいて管理されるため、重要なタスクが優先され、ピーク負荷時のシステムの安定性が維持されます。
	USB ディスク暗号化条件	[すべての外部USBドライブ（）] オプション（ [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [条件（Conditions）] > [ポスチャ（Posture）] > [ディスク暗号化条件（Disk Encryption Condition）]）を使用して、選択した製品で外部ディスクドライブが暗号化されているかどうかを確認できます。 USB ドライブが挿入されると、Cisco ISE は挿入を動的に検出し、ただちに USB ドライブ条件を評価して、エンドポイントの適合性ステータスを確認します。このプロセスにより、エンドポイントが Cisco ISE 制御ネットワーク内にとどまったまま、USB デバイスに関連するポスチャポリシーの継続的なモニタリングと適用が保証されます。

Cisco ISE リリース 3.4 パッチ 3 の新機能

表 4. Cisco ISE リリース 3.4 累積パッチ 3 の新機能

製品への影響	機能	説明
ソフトウェアの信頼性	セキュリティサービスの挿入	セキュリティサービスの挿入により、定義済みのポリシーに基づいてファイアウォールを介してトラフィックをステアリングすることで、ネットワークセキュリティが強化されます。これにより、ゼロトラスト セキュリティ ソリューションがサポートされます。セキュリティサービスの挿入は、有線展開とワイヤレス展開をサポートし、オンプレミスおよびクラウドホスト ソリューションを含む、シスコおよびサードパーティのファイアウォールと互換性があります。 Cisco ISE API は、ポリシーの作成を容易にし、設定された送信元セキュリティグループに基づいてネットワークデバイスがポリシーを取得および適用できるようにすることで、セキュリティサービスの挿入において重要な役割を果たします。

Cisco ISE リリース 3.4 パッチ 2 の新機能

表 5. Cisco ISE リリース 3.4 累積パッチ 2 の新機能

製品への影響	機能	説明
使いやすさ	強化された [エンドポイントトピック設定（Endpoint Topics Settings）] を使用した Cisco ISE データの共有	強化された [Endpoint Topics Settings] 機能を使用して、エンドポイント属性データを Cisco AI エンドポイント分析および Cisco pxGrid Cloud と共有することで、ネットワークの可視性とセキュリティを強化できます。[トピックのエンドポイント属性の有効化（Enable Endpoint Attributes to Topics）] オプションを使用すると、統合を介して Cisco ISE から分析プラットフォームにエンドポイント属性を転送できます。また、[AI エンドポイント分析からエンドポイントプロファイルを消費（Consume Endpoint Profiles from AI Endpoint Analytics）] オプションを使用して、ネットワークアクセス認証およびエンドポイント制御のために AI エンドポイント分析プロファイルデータを Cisco ISE にパブリッシュすることもできます。
	osquery 条件のサポート	Cisco ISE リリース 3.4 パッチ 2 以降では、osquery 条件を作成してエンドポイントのポスチャ コンプライアンス ステータスを確認したり、エンドポイントから必要な属性を取得したりできます。 注：osquery 条件をサポートするには、コンプライアンスモジュール 4.3.3394 以降および Cisco Secure Client 5.1.7 以降のバージョンを使用する必要があります。
ソフトウェアの信頼性	リモートサポート許可	リモートサポート許可により、Cisco ISE 管理者は、特定の Cisco TAC スペシャリストが、CLI と UI のいずれかまたは両方を介して Cisco ISE 展開に安全にリモートアクセスし、トラブルシューティングや情報収集を行うことを許可できます。このアクセスは、Cisco ISE 管理者によって明示的に許可される必要があり、Cisco ISE 展開内の 1 つ以上のノードに提供できます。
	時間制限付きデバッグの有効化	Cisco ISE リリース 3.4 パッチ 2 から導入された時間制限付きデバッグの有効化機能を使用すると、ドロップダウンリストからログレベルを選択し、デフォルト設定に戻すためのリセットタイマーを設定することができます。タイマーが期限切れになると、選択されたノードはデフォルト状態に戻ります。
	Blast RADIUS の脆弱性の修正	CSCwk67747で報告された Blast RADIUS の脆弱性に対処するために、[External RADIUS Server]、[RADIUS Token ID Store]、および [Device Profile] に [Message Authenticator Required On Response] チェックボックスが導入されました。 アップグレード後、このチェックボックスはデフォルトでは有効になりませんが、新しいリソースが追加されると自動的に有効になります。チェックボックスを有効にすると、Cisco ISE は応答内に **Message-Authenticator** 属性のないパケットを無効にするため、フローで障害が発生します。
	TACACS+ over TLS のサポート	ネットワークデバイスの TACACS over TLS 認証を有効にして、セキュリティを強化できます。Cisco ISE は、証明書の IP アドレス（iPAddress）、DNS 名（dNSName）、およびディレクトリ名（directoryname）属性の検証をサポートしています。 いずれかの属性が一致した場合は検証が成功し、一致しない場合は検証が失敗します。SAN 属性ごとに、複数の値がサポートされています。 ネットワークデバイスに対して TACACS 認証または TACACS over TLS 認証が有効になっているかどうかは、**Network Devices** ページで確認できます。
	Tenable Security Center の API キーと証明書認証のサポート	Cisco ISE リリース 3.4 パッチ 2 以降では、Tenable Security Center で次の認証方式が追加でサポートされています。 • [API Keys]：Tenable Security Center のアクセス権限を持つユーザーアカウントのアクセスキーと秘密鍵を入力します。API キー認証は、Tenable Security Center 5.13.x 以降のリリースでサポートされています。Cisco ISE でこのオプションを選択する前に、管理者ユーザーとしてログインして、Tenable Security Center で API キー認証を有効にする必要があります。

製品への影響	機能	説明
		• [Certificate Authentication]：[Authentication Certificate] ドロップダウンリストから必要な証明書を選択します。認証に成功すると、Cisco ISE はカスタマーが設定したテンプレートを Tenable Security Center から取得します。Cisco ISE でこのオプションを有効にする前に、SSL クライアント証明書認証を許可するように Tenable Security Center を設定する必要があります。

Cisco ISE リリース 3.4 パッチ 1 の新機能

表 6. Cisco ISE リリース 3.4 累積パッチ 1 の新機能

製品への影響	機能	説明
使いやすさ	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。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。
	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。
	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、統合カタログ（[管理（Administration）] > [システム（System）] > [デプロイメント（Deployment）] > [統合カタログ（Integration Catalog）]）を使用します。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。
	TrustSec ポリシーマトリックス GUI の機能拡張	Cisco ISE の TrustSec ポリシーマトリックスは、多数の SGT があるデプロイメント向けに大幅に最適化されています。パフォーマンスの向上には、データの取得とレンダリングの効率化、大規模な SGT セットの高速処理のためのバックエンドクエリの最適化、およびスクロールやナビゲーションをスムーズにするための Cisco ISE GUI の改善が含まれます。これらの機能拡張により拡張性と応答性が向上し、広範なポリシーマトリックスを管理する際に効率的でシームレスなエクスペリエンスが提供されます。
ソフトウェアの信頼性	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。
	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。
	pxGrid Direct を使用したディクショナリ属性の 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。
	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。

製品への影響	機能	説明
	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
	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。
	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。
	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。
	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 では、サブジェクト代替名（SAN）フィールドにセキュリティ識別子（SID）が含まれる新しい証明書形式がサポートされます。SAN フィールドの SID は認証に使用されないため、誤った SID 解析による認証エラーを防止できます。 Cisco ISE は、証明書で次の SAN_URI フィールド形式をサポートしています。 • SID と ID または GUID をカンマで区切る形式（いずれかの順序）： <tag,sid>,<ID><GUID> または <ID><GUID>,<tag,sid> • SID と ID または GUID をコロンで区切る形式（いずれかの順序）： <tag,sid>:<ID><GUID> または <ID><GUID>:<tag,sid> • SID のみが存在する形式： <tag,sid> • ID と GUID のみが存在する形式： <ID><GUID> 新しいすべての Microsoft 証明書には、次の形式で SAN_URI に SID が含まれています。 **tag:microsoft.com,2022-09-14:sid:<SID>**.

製品への影響	機能	説明
	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。
	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。 これに対する移行が今回の更新では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。
API エクスペリエンス	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。
アップグレード	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。

Cisco ISE リリース 3.4 の新機能

表 7. Cisco ISE リリース 3.4 の新機能

製品への影響	機能	説明
ソフトウェアの信頼性	Cisco ISE のレジリエンスのユースケース	Cisco ISE リリース 3.4 以降、Cisco ISE のレジリエンスを維持するために、**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。
	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** 設定ページを使用して仮想トンネルインターフェイス（VTI） を設定できます。ネイティブ IPSec を使用すると、IKEv1 および IKEv2 プロトコルを用いた IPSec トンネルを介して、Cisco ISE PSN と NAD の間にセキュリティ アソシエーションを確立できます。ネイティブ IPSec の設定により、Cisco ISE は FIPS 140-3 への準拠を確保できます。
	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。[デバッグレベル設定（Debug Level Configuration）] ページに現在のディスク容量の使用率と、[最大ファイルサイズ（Max File Size）] と [ファイル数（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。

製品への影響	機能	説明
	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、[アイデンティティ同期（Identity Sync）] ページで [スキップ（Skip）] をクリックします。[サマリー（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。
	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。 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。
	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、[管理（Administration）] > [アイデンティティ管理（Identity Management）] > [外部アイデンティティソース（External Identity Sources）] > [Active Directory] > [拡張ツール（Advanced Tools）] > [高度な調整（Advanced Tuning）] を選択します。[名前（Name）] フィールドにレジストリキーの名前を入力し、**1** を[値（Value）] フィールドに入力します。 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。 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。 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。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。

製品への影響	機能	説明
	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 [表示（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 共有秘密 • Radius Second Shared Secret [ネイティブIPSec（Native IPsec）] で、 • 事前共有キー（Pre-Shared Key） これを行うには、[管理（Administration）] > [設定（Settings）] > [セキュリティ設定（Security Settings）] の順に選択し、[パスワードをプレインテキストで表示（Show Password in Plaintext）] チェックボックスをオフにします。 • 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 [ネットワークデバイスのインポートテンプレート形式（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。
	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。
	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。
	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（[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロトコル（Protocols）] > [RADIUS] > [RADIUS設定（RADIUS Settings）]）設定の運用が容易になっています。
	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。

製品への影響	機能	説明
セットアップの容易さ	URL プッシャ pxGrid Direct コネクタの作成	IPv6 アドレスを使用して Cisco ISE を設定できるようになり、IPv6 のみのセットアップが可能になりました。この機能拡張は、既存の IPv4 およびデュアルスタック構成オプションに加えて使用できます。**`reset-config`** コマンドを使用して、IPv4 構成と IPv6 構成を簡単に切り替えられます。また、新しく導入された **`ipv6 default-gateway`** コマンドでは、IPv6 アドレスを使用してデフォルトゲートウェイを指定できます。 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。
	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 • 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 Cisco ISE リリース 3.4 の時点では、使用可能なクライアント OS で TEAP TLS 1.3 が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。
使いやすさ	認証局診断ツール	証明書管理に関する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。
	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。 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、[ISEとサーバーの情報（About ISE and Server）] を選択します。
	「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。
	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、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。
	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。
	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。

製品への影響	機能	説明
	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。 • [コンテキストの可視性（Context Visibility）] > [エンドポイント（Endpoints）]。 • [ワークセンター（Work Centers）] > [ゲストアクセス（Guest Access）] > [アイデンティティ（Identities）] > [エンドポイント（Endpoints）]。 • [ワークセンター（Work Centers）] > [BYOD] > [アイデンティティ（Identities）] > [エンドポイント（Endpoints）]。 • [ワークセンター（Work Centers）] > [ネットワークアクセス（Network Access）] > [アイデンティティ（Identities）] > [エンドポイント（Endpoints）]。 • [ワークセンター（Work Centers）] > [プロファイラ（Profiler）] > [エンドポイントの分類（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。
API エクスペリエンス	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 **sessionTopicAll** 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。
アップグレード	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。

製品への影響	機能	説明
	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。

Cisco ISE の新規および変更された API

新たな API、変更された API、および廃止された API の詳細については、『Cisco ISE API リファレンスガイド』を参照してください。

動作における変更

Cisco ISE リリース 3.4 の廃止された機能

表 8. Cisco ISE リリース 3.4 の廃止された機能

機能	説明
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 に移行することをお勧めします。
API 認証用の RSA または RADIUS 外部データベースの設定	Cisco ISE リリース 3.4 以降、API 認証用の RSA または RADIUS 外部データベースの設定はサポートされなくなりました。
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設定 - 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。 • ロケーションサービス（Location Services）（[管理（Administration）] > [ネットワークリソース（Network Resources）] > [ロケーションサービス（Location Services）]）。 • NAC マネージャ（NAC Managers）（[管理（Administration）] > [ネットワークリソース（Network Resources）] > [NACマネージャ（NAC Managers）]）。

Cisco ISE リリース 3.4 の動作の変更

表 9. Cisco ISE リリース 3.4 の動作の変更

機能	既知の問題
Cisco ISE アップグレードの通知：RSA_PSS プロトコル設定の更新	RSA_PSS は、Cisco ISE GUI の [許可されたプロトコル（Allowed Protocols）] で管理されるようになりました。Cisco ISE リリース 3.4 にアップグレードすると、RSA_PSS はデフォルトで有効になります。Cisco ISE CLI を使用して以前に RSA_PSS を無効にした場合は、Cisco ISE リリース 3.4 にアップグレードした後、GUI の [許可されるプロトコル（Allowed Protocols）] で再度無効にする必要があります。

解決済みの問題

Cisco ISE リリース 3.4 パッチ 6：解決済みの問題

Cisco バグ検索ツールを使用して、特定のバグを検索したり、このリリースに含まれるすべての解決済みバグを検索したりできます。

Cisco ISE リリース 3.4 パッチ 5：解決済みの問題

Cisco バグ検索ツールを使用して、特定のバグを検索したり、このリリースに含まれるすべての解決済みバグを検索したりできます。

Cisco ISE リリース 3.4 パッチ 4：解決済みの問題

Cisco バグ検索ツールを使用して、特定のバグを検索したり、このリリースに含まれるすべての解決済みバグを検索したりできます。

Cisco ISE リリース 3.4 パッチ 3：解決済みの問題

シスコのバグ検索ツールを使用して、特定のバグを検索したり、このリリースに含まれるすべての解決済みバグを検索したりできます。

問題に関する追加情報を表示するには、バグ ID をクリックして、バグ検索ツール（BST）にアクセスしてください。

表 10. Cisco ISE リリース 3.4 累積パッチ 3 での解決済みの問題

不具合 ID	説明
CSCwp97554	Cisco ISE リリースパッチ 1 またはパッチ 2 をインストールした後に、Cisco ISE リリース 3.4 との Cisco Secure Network Analytics の統合が失敗します。
CSCwq14019	ASN1_get_object が原因で Cisco ISE リリース 3.4 パッチ 2 がクラッシュします。
CSCwp22511	Cisco ISE でピリオドがカンマに変換されるため、ファイル名の不一致が発生します。

Cisco ISE リリース 3.4 パッチ 2：解決済みの問題

シスコのバグ検索ツールを使用して、特定のバグを検索したり、このリリースに含まれるすべての解決済みバグを検索したりできます。

Cisco ISE リリース 3.4 パッチ 1：解決済みの問題

シスコのバグ検索ツールを使用して、特定のバグを検索したり、このリリースに含まれるすべての解決済みバグを検索したりできます。

Cisco ISE リリース 3.4：解決済みの問題

バグ検索ツールを使用して、特定のバグを検索したり、このリリースに含まれるすべての解決済みバグを検索したりできます。

未解決の問題

Cisco ISE リリース 3.4 パッチ 6：未解決の問題

以前のリリースで未解決の問題は、解決されるまで後続のリリースに残ります。

文書化されたシスコ製品の問題を検索するには、ブラウザに次のように入力します。<bug_number> site:cisco.com。

Cisco ISE リリース 3.4 パッチ 5：未解決の問題

以前のリリースで未解決の問題は、解決されるまで後続のリリースに残ります。

表 11. Cisco ISE リリース 3.4 累積パッチ 5 の未解決の問題

不具合 ID	説明
CSCwt16625	Cisco ISE で Facebook ソーシャル ログイン プロバイダーを作成または変更すると、ルート CA チェーンが見つからないか、信頼されていないことを示すエラーが発生することがあります。これは、Facebook（Meta）が 2025 年 11 月に SSL 証明書チェーンを DigiCert Global Root G2 に更新したためです。デフォルトで Cisco ISE が信頼するのは CISCO_SERVICES のみです。これを解決するには、Cisco ISE の信頼できる証明書を編集し、「DigiCert Global Root G2 CA」証明書に対して、[ISE 内の認証用に信頼（Trust for authentication within ISE）] をオンにします。

文書化されたシスコ製品の問題を検索するには、ブラウザに次のように入力します。<bug_number> site:cisco.com。

Cisco ISE リリース 3.4 パッチ 4：未解決の問題

以前のリリースで未解決の問題は、解決されるまで後続のリリースに残ります。

表 12. Cisco ISE リリース 3.4 累積パッチ 4 の未解決の問題

不具合 ID	説明
CSCws52326	Cisco ISE で、[コンテキストの可視性（Context Visibility）] ページに表示されるエンドポイントのカスタム属性が正しく評価されません。その結果、カスタム属性を使用する認証ルールが不正確に照合され、誤った認証プロファイルが割り当てられる可能性があります。
CSCws30603	Entra AD ユーザーが 20 を超えるグループに属している場合、ユーザー グループ メンバーシップを取得できないという問題が発生する可能性があります。Cisco ISE で使用される Microsoft Graph API は各ユーザーの最初の 20 グループのみを返すため、承認が失敗します。ポリシーに必要なグループが最初の 20 に含まれていない場合、グループメンバーシップの評価は失敗します。

不具合 ID	説明
CSCws18653	スタンドアロン展開で Cisco ISE リリース 3.4 パッチ 3 から Cisco ISE リリース 3.4 パッチ 4 にアップグレードした場合、 **RADIUS 認証詳細レポートで** 、属性、結果、手順などのセクションが欠落することがあります。この問題が起きるのは、想定されるデータベースパッチスクリプト（mntpatchinstall_v4.sql）が実行されず、デバッグログファイル（collector.log）でテーブルまたはビューが存在しないことを示すエラーが発生したためです。パッチ 4 とパッチ 3 の両方をロールバックし、パッチ 4 を再度適用して、欠落したレポートの詳細を復元することを推奨します。

文書化されたシスコ製品の問題を検索するには、ブラウザに次のように入力します。<bug_number> site:cisco.com。

Cisco ISE リリース 3.4 パッチ 3：未解決の問題

以前のリリースで未解決の問題は、解決されるまで後続のリリースに残ります。

文書化されたシスコ製品の問題を検索するには、ブラウザに次のように入力します。<bug_number> site:cisco.com。

Cisco ISE リリース 3.4 パッチ 2：未解決の問題

以前のリリースで未解決の問題は、解決されるまで後続のリリースに残ります。

表 13. Cisco ISE リリース 3.4 累積パッチ 2 での未解決の問題

不具合 ID	説明
CSCwh77618	Cisco ISE RMQ Full：EPO が有効になっている場合、ISE ノード間の遅延が大きくなります。
CSCwn97980	TrustSec ポリシーマトリックスのセルが断続的に応答しなくなります。
CSCwo05386	Cisco ISE が、内部証明書「Baltimore CyberTrust Root」の期限切れに関するアラームを受信しています。
CSCwo99311	Cisco ISE リリース 3.4 パッチ 2 では、EPO PSN1 到達不能シナリオでエンドポイントがオンボードされません。
CSCwp22511	新しいパッチアップロード UI により、ピリオドがカンマに変換され、ファイル名の不一致が発生します。
CSCwp60343	証明書ベースの認証中に、クライアント検証エラーが原因で内部ユーザーの ERS 後操作が失敗します。

文書化されたシスコ製品の問題を検索するには、ブラウザに次のように入力します。<bug_number> site:cisco.com。

Cisco ISE リリース 3.4 パッチ 1：未解決の問題

以前のリリースで未解決の問題は、解決されるまで後続のリリースに残ります。

文書化されたシスコ製品の問題を検索するには、ブラウザに次のように入力します。<bug_number> site:cisco.com。

Cisco ISE リリース 3.4：未解決の問題

以前のリリースで未解決の問題は、解決されるまで後続のリリースに残ります。

文書化されたシスコ製品の問題を検索するには、ブラウザに次のように入力します。<bug_number> site:cisco.com。

既知の問題

Cisco ISE リリース 3.4 パッチ 6：既知の問題

Cisco ISE リリース 3.4 パッチ 6 には既知の問題はありません。

Cisco ISE リリース 3.4 パッチ 5：既知の問題

表 14. Cisco ISE リリース 3.4 累積パッチ 5 の既知の問題

不具合 ID	既知の問題
CSCws61409	Cisco ISE リリース 3.4 パッチ 1 から Cisco ISE リリース 3.4 パッチ 3 に対して Cisco ISE リリース 3.4 パッチ 5 がインストールされている場合、**Secure System Diagnostics レポート** と **SXP バインディングレポート**に何も表示されません。 Cisco ISE リリース 3.4 パッチ 4 に対して Cisco ISE リリース 3.4 パッチ 5 がインストールされている場合、**設定監査の変更**、**ポスチャ関連レポート**、および **SXP バインディングレポート**に何も表示されません。 Cisco ISE リリース 3.3 パッチ 8 または Cisco ISE リリース 3.3 パッチ 9 から Cisco ISE リリース 3.4 パッチ 5 にアップグレードされた場合、**設定監査の変更**、**ポスチャ関連レポート**、および **Active Directory 操作レポート**に何も表示されません。

Cisco ISE リリース 3.4 パッチ 4：既知の問題

表 15. Cisco ISE リリース 3.4 累積パッチ 4 の既知の問題

機能	既知の問題
Cisco ISE クラウドの脆弱性修正	パッチ 1、パッチ 2、またはその他の Cisco ISE リリースから Cisco ISE リリース 3.4 パッチ 4 にアップグレードすると、Cisco ISE はログイン時に内部サービスを必ず再起動します。この再起動は、CSCwn63400で特定された脆弱性に対処するために必要です。この修正はクラウド展開にのみ適用されます。修正を完全に適用するには、次のいずれかのオプションを使用して、展開内のすべてのノードを PAN と同期する必要があります。 • 自動同期で続行（Proceed with Auto Sync）：修正を即時に同期および適用するために、すべてのノードが再起動されます。展開内のノードの同期ステータスは、[展開ノード（Deployment Nodes）] ページ（[管理（Administration）] > [システム（System）] > [展開（Deployment）]）で確認できます。すべてのノード間での自動同期を確実に行うために、このオプションを推奨します。 • **手動同期で続行（Proceed with Manual Sync）：再起動後、できるだけ早くすべてのノードを手動で同期し、非同期を防ぐ必要があります。**ノードが非同期になっている場合は、問題を解決するために登録解除して設定をリセットし、ノードを再度登録する必要があります。 • **後で決定（Decide Later）：次回のログイン時に、脆弱性を修正するためのオプションを使用できます。** **注**：この要件は、Cisco ISE リリース 3.4 パッチ 4 にアップグレードする前に、最新の Cisco ISE リリース 3.4 パッチ 3 AMIをインストールしている場合は適用されません。

Cisco ISE リリース 3.4 パッチ 3：既知の問題

表 16. Cisco ISE リリース 3.4 累積パッチ 3 の既知の問題

機能	既知の問題
Cisco ISE リリース 3.4 パッチ 3 へのアップグレード後におけるログ分析の初期化の問題	Cisco ISE リリース 3.3 パッチ 7 から Cisco ISE リリース 3.4 パッチ 3 にアップグレードした後に、アプリケーションサーバーが「初期化中（initializing）」の状態から進まないことがあります。これは、以前のリリースから認識されないテレメトリオブジェクトに到達すると、Kibana の移行が失敗するために発生します。問題のあるドキュメントを手動で削除し、移行を完了できるように Kibana 設定を一時的に変更することで、これを解決できます。CSCwt07284 の回避策セクションの手順を参照してください。

Cisco ISE リリース 3.4 パッチ 2：既知の問題

Cisco ISE リリース 3.4 パッチ 2 に既知の問題はありません。

Cisco ISE リリース 3.4 パッチ 1：既知の問題

表 17. Cisco ISE リリース 3.4 累積パッチ 1 の既知の問題

機能	既知の問題
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 [パッチロールバック（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。

Cisco ISE リリース 3.4：既知の問題

Cisco ISE リリース 3.4 に既知の問題はありません。

互換

ソフトウェア ダウンロード サイトで置き換えられた Cisco ISE 3.4 OVA、ISO、およびアップグレード バンドル ファイル

Cisco ISE ソフトウェア ダウンロード サイト [英語] で Cisco ISE 3.4 OVA、ISO、およびアップグレード バンドル ファイルが置き換えられました。Cisco SNS 3800 アプライアンスには、次のファイルのみを使用する必要があります。

- Cisco-vISE-300-3.4.0.608b.ova
- Cisco-vISE-600-3.4.0.608b.ova
- Cisco-vISE-1200-3.4.0.608b.ova
- Cisco-vISE-2400-3.4.0.608b.ova
- ise-3.4.0.608b.SPA.x86_64.iso
- ise-upgradebundle-3.1.x-3.3.x-to-3.4.0.608b.SPA.x86_64.tar.gz
- ise-urtbundle-3.4.0.608b-1.0.0.SPA.x86_64.tar.gz

Cisco SNS 3800 アプライアンスは、Cisco ISE リリース 3.4 パッチ 4 でサポートされています。Cisco SNS 3800 プロファイルを使用した Cisco SNS 3800 OVA および ISO のサポートは、Cisco ISE リリース 3.4 パッチ 4 からのみ使用できます。

Cisco ISE リリース 3.4 へのアップグレード

Cisco ISE リリース 3.3、3.2、および 3.1 から Cisco ISE リリース 3.4 に直接アップグレードできます。

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。

Cisco ISE パッチは累積的であるため、アップグレードを始める前に、既存のリリース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 アップグレードガイド』を参照してください。

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。

クラウド上の Cisco ISE

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。クラウド環境で Cisco ISE をネイティブに展開するには、「クラウドプラットフォームへの Cisco Identity Services Engine のネイティブな展開」を参照してください。サポートされている Cisco ISE インスタンスに関する詳細は、「Cisco ISE インスタンスと使用目的」を参照してください。

新しいパッチのインストール

システムへのパッチの適用方法については、『Cisco Identity Services Engine アップグレードプロセス』の「Cisco ISE ソフトウェアパッチ」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。

検証済みハードウェア

Cisco ISE リリース 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。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設置ガイド』を参照してください。

- Cisco SNS-3615-K9（小規模）
- 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-3815-K9（小規模）
- Cisco SNS-3855-K9（中規模）
- Cisco SNS-3895-K9（大規模）

注：Cisco SNS 3800 アプライアンスは、Cisco ISE リリース 3.4 パッチ 4 以降でサポートされています。

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 ハードウェア インストールガイド』を参照してください。

検証済み仮想環境

次の表にサポートされているプラットフォームをまとめ、Cisco ISE デプロイメントオプションに関する主な詳細を示します。

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

表 18. 検証済み仮想環境

仮想環境	サポートの詳細
VMware	• VMware 7.0.3 以降 • 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 テンプレートは、ESXi 7.0 および ESXi 8.0 で VMware バージョン 14 以降をサポートしています。 • 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。 • VMware の移行機能を使用して、VM インスタンス（任意のペルソナを実行）をホスト間で移行できます。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。
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	• AWS：VMware Cloud on AWS が提供するソフトウェア定義型データセンターで Cisco ISE をホストします。 • Azure VMware ソリューション：Microsoft Azure 上で VMware ワークロードをネイティブに実行します。 • Google Cloud VMware Engine：VMware on Google Cloud がソフトウェア定義型データセンターを実行します。
Microsoft Hyper-V	• Microsoft Windows Server 2012 R2 以降をサポートしています。 • 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。

仮想環境	サポートの詳細
QEM 上の KVM	• QEMU 2.12.0-99 以降をサポートしています。 • Cisco ISE リリース 3.4 パッチ 4 以降のリリースでは OpenStack がサポートされています。 注：OpenStackをサポートするには、次の ISO ファイルを使用する必要があります。 ise-3.4.0.608b.SPA.x86_64.iso
Nutanix	• Nutanix 20230302.100169 以降をサポートしています。
パブリック クラウド プラットフォーム	• Amazon Web Services（AWS）、Microsoft Azure Cloud、および Oracle Cloud Infrastructure（OCI）のネイティブサポート。
Red Hat OpenShift	• Red Hat OpenShift コンテナプラットフォーム 4.19 以降。 • Cisco ISE は、標準の Cisco ISE ISO イメージを使用して OpenShift プラットフォームに展開する必要があります。OVA テンプレートを使用した Cisco ISE の展開はサポートされていません。

ブラウザとの互換性

Cisco ISE GUI は、Chrome、Firefox、Edge などのほとんどの一般的なブラウザの最新のデスクトップバージョンと互換性を持つように設計されています。ほとんどの場合、最新リリースの 1 つ前のバージョンまで互換性があります。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。

Cisco ISE リリース 3.4 は、次の環境でサポートおよび検証されています。

- 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

検証済み外部 ID ソース

表 19. 検証済み外部 ID ソース

外部 ID ソース	詳細	バージョン
Active Directory	Microsoft Windows Active Directory 2012	Windows Server 2012
	Microsoft Windows Active Directory 2012 R2	Windows Server 2012 R2 注：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。
	Microsoft Windows Active Directory 2016	Windows Server 2016
	Microsoft Windows Active Directory 2019	Windows Server 2019

外部 ID ソース	詳細	バージョン
	Microsoft Windows Active Directory 2022	Windows Server 2022（パッチ Windows10.0-KB5025230-x64-V1.006.msu 適用済み）
LDAP サーバ	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 ID プロバイダーバージョン
オープン データベース コネクティビティ（ODBC）ID ソース	Microsoft SQL サーバー	Microsoft SQL サーバー 2012 および 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

検証済み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 リリース 3.4 は、OpenSSL 1.1.1za ベースの CiscoSSL 7.3.410 で検証されています。

関連技術情報

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、コレクションページを参照してください。

法的情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/go/trademarks をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)

このマニュアルで使用している IP アドレスと電話番号は、実際のアドレスと電話番号を示すものではありません。マニュアル内の例、コマンド表示出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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。

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。