Cisco Identity Services Engine リリース 3.5 リリースノート

コンテンツ

Cisco Identity Services Engine リリース 3.5

Cisco Identity Services Engine（ISE）リリース 3.5 では、セキュリティとユーザー体験の向上に焦点を当て、ネットワーク管理が大幅に強化されました。このリリースでは、シングルスタック IPv6 の完全なサポートが導入され、ポータル、RADIUS サービス、API などの設定やサポートされる機能の範囲が拡張されます。新しい pxGrid API によりエンドポイントアクセスが強化され、pxGrid クラウドは追加のリージョンをサポートするように拡張され、統合カタログを介した統合が容易になりました。Active Directory 参加ポイントへの専用リソース割り当ては、新しいアラームおよびモニタリング機能とともに、Cisco ISE のモニタリング機能を強化します。このリリースから、Cognitive Threat Analytics（CTA）アダプタは脅威中心型ネットワーク アクセス コントロール（TC-NAC）フローではサポートされなくなりました。これは、セキュリティの重点が戦略的に変更されたことを示しています。

セキュリティとコンプライアンスは、OAuth2 認証のサポート、リモート TAC サポートの承認、および DoDIN APL、FIPS 140-3、コモンクライテリア認定用の Network Device Collaborative Protection Profile（NDcPP）v3.0e などの連邦認定との連携によってさらに強化されます。このリリースでは、SNMP ベースのデバイスプロファイリングと、EAP-TLS および TEAP-TLS を使用したユーザー/デバイスの承認により、プロファイリングと承認の機能が強化されています。TACACS over TLS の追加と、さまざまなワークフローでの TLS 1.3 サポートの拡張により、セキュリティが強化されます。ユーザー体験の向上には、ゲストパスワードのリセット用の国コードドロップダウンや時間制限付きデバッグ設定などの機能が含まれます。さらに、Cisco ISE ライセンス戦略の変更は、pxGrid、pxGrid Direct、プロファイリングサービス、TrustSec などの機能がアクティブなエンドポイントの数に基づいてライセンスを消費するようになることを意味します。ただし、コンプライアンス違反のライセンスに対する適用はまだ実装されていません。これらの機能拡張により、包括的で安全かつ使いやすいネットワーク管理ソリューションが提供されます。

このドキュメントでは、Cisco ISE リリース 3.5 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
2026-04-13	Cisco ISE リリース 3.5 累積パッチ 3 の正式版
2026-02-26	Cisco ISE リリース 3.5 累積パッチ 2 の正式版
2025-12-15	Cisco ISE リリース 3.5 累積パッチ 1 の正式版
2025-09-22	Cisco ISE リリース 3.5 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 3.5 パッチ 3 の新機能

表 2. Cisco ISE リリース 3.5 累積パッチ 3 の新機能

製品への影響	機能	説明
使いやすさ	継続的な再評価	継続的な再評価により、Cisco Secure Client を使用してエンドポイントの正常性とポスチャをリアルタイムでモニターできます。このオプションを有効にすると、Cisco Secure Client は継続的な再評価を実行し、特定のイベントで発生するポスチャの変更を 10 分間隔で検出します。この機能により、動的なポスチャの変更を迅速に特定し、継続的なモニタリングとレポート作成によってエンドポイントの動作の可視性を向上させます。
	Cisco ISE の TC-NAC ノードの高可用性とフェールオーバーのサポート	TC-NAC ノードの高可用性およびフェールオーバーのサポートが利用可能になり、プライマリ TC-NAC ノードで障害が発生した場合の継続的な Cisco ISE サービスが保証されます。展開ごとに最大 2 つの TC-NAC ノード（プライマリノードとセカンダリノード）を設定でき、プライマリノードがアクティブな TC-NAC ロールを担います。TC-NAC ノードが 1 つだけ存在する場合、そのノードは自動的にプライマリになり、アクティブなロールを実行します。すべてのロール変更は、コンプライアンスのために **変更設定監査** で追跡されます。
	グローバル展開内の複数の IP アドレスを使用した FQDN から SGT へのマッピング	Cisco ISE で IP とホスト名 SGT の静的マッピングを使用すると、TrustSec 環境全体に SGT 情報を展開できます。これらのマッピングを Cisco ISE で設定すると、特定のホスト名のすべての解決済み IP アドレスがキャプチャされ、正しい SGT にマッピングされます。この機能は、単一のホスト名が場所によって異なる IP アドレスに解決される場合があるグローバル展開で特に役立ちます。
	MDM ベンダーの OAuth サポート	OAuth 2.0 を使用して MDM ベンダーと統合することで、セキュリティを強化できます。サーバーを追加すると、次の 2 つの新しい認証タイプを選択できます。**OAuth - Client Credentials - Intune**（特に Microsoft Intune の場合）または **OAuth - Client Credentials - Generic**（Jamf Pro や Omnissa などのベンダーの場合）。このサポートにより、非準拠エンドポイントのセッションを自動的に再承認でき、基本認証に変わる安全な方法が提供されます。
	TrustSec ポリシー管理用の強化されたユーザーインターフェイス	Cisco ISE の [TrustSecポリシー（TrustSec Policy）] ページでは、ユーザー体験が向上するように再設計されたレイアウトと最新のビジュアル要素が使用されています。合理化されたインターフェイスにより視覚的に明確であるため、ポリシー設定を簡単に参照および理解できます。 直感的なコントロールと適切に編成されたポリシーコンポーネントにより複雑さが軽減され、ポリシー管理タスクがシンプルになります。最適化の機能により、ポリシーを効率的に作成、変更、確認できます。TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）とポリシーマトリックスを管理する際のエクスペリエンスが向上します。
	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。[シンタックス検証（Validate Syntax）] ボタンをクリックすると、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。
	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）] の [ワークロード コネクタ エンドポイント（Workload Connector Endpoints）] タブでは、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。このタブには、[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。

製品への影響	機能	説明
ソフトウェアの信頼性	**すべての Cisco ISE RADIUS 応答パケットに Message-Authenticator を含める**	Cisco ISE では、**すべての応答パケット（アクセス受け入れ、アクセス拒否、およびアクセスチャレンジ）に Message-Authenticator RADIUS 属性** を含めることができるようになりました。この設定は、NAD ごとに、またはデフォルトのデバイス設定を介して有効にできます。
	RADIUS 経由の TrustSec ポリシーダウンロードおよび サーバーリストで IPv6 をサポート	Cisco ISE は、IPv4 に加えて、TrustSec AAA サーバーで IPv6 をサポートするようになりました。この機能拡張により、TrustSec デバイスが IPv6 アドレスを使用して Cisco ISE サーバーに対して認証できるようになり、ネットワークの柔軟性と展開オプションが向上します。
	SXP での IPv6 のサポート	[展開（Deployment）] 設定の下で [SXPサービスの有効化（Enable SXP Service）] チェックボックスをオンにすることによって、IPv6 ノードの SXP サービスを有効にできるようになりました。[IPv6アドレス（IPv6 Address）] フィールドは、ネットワークインターフェイスを選択すると自動的に入力され、[ノードID（Node ID）] という新しいフィールドが追加されています。ノード ID は、ネットワーク内の SXP ノードを一意に識別する IPv4 アドレスです。インターフェイスに IPv4 アドレスがあるか、デュアルスタックとして設定されている場合、ノード ID は自動的に入力されます。ただし、インターフェイスが IPv6 アドレスのみを使用する場合は、ノード ID の IPv4 アドレスを手動で入力する必要があります。
	HTTP 2.0 のサポート	API ゲートウェイは、Cisco ISE リリース 3.5 パッチ 3 以降で HTTP 2.0 ベースの要求をサポートします。
	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 のサーバー認証 EKU のみを含むサーバー証明書の使用をサポートするようになりました。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。
セットアップの容易さ	Windows Server 2025 のサポート	アイデンティティ管理のニーズを満たすために、Cisco ISE の外部アイデンティティソースとして Windows Server 2025 Active Directory ドメインを使用できます。このサポートにより、最新の Windows サーバー インフラストラクチャと統合して、ユーザー認証とマシン認証を管理できます。Windows Server 2025 のセキュリティ設定が強化されたため、EAP-MS-CHAPv2 および EAP-GTC を介して行われるパスワードの変更はデフォルトで無効になっています。

Cisco ISE リリース 3.5 パッチ 2 の新機能

Cisco ISE リリース 3.5 パッチ 2 に新機能はありません。

Cisco ISE リリース 3.5 パッチ 1 の新機能

表 3. Cisco ISE リリース 3.5 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	CoA のユーザー属性モニタリングの拡張機能	Microsoft Entra ID 属性の更新に基づいて、認可変更（CoA）によるユーザー属性のモニタリングに次の拡張機能を使用できるようになりました。 • 新しい日付および時刻属性が、既存のユーザー属性のリストに追加されます。 • extension_<GUID>_<attributeName> 形式で [ユーザー属性（User Attributes）] タブからカスタムディレクトリ拡張属性を選択できるようになりました。

製品への影響	機能	説明
	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。
	ポスチャポリシーの猶予期間設定	[ポスチャの一般設定（Posture General Settings）] ページ（[管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）] > [一般設定（General Settings）]）で、ポスチャポリシーの [猶予期間設定（Grace period settings）] を設定するオプションが追加されました。この機能拡張により、次の2つのオプションのいずれかを選択して、ポリシー違反の時間しきい値を定義できます。 • 最小（Min）：すべての問題を解決するための最短の時間を表示します。 • 最大（Max）：すべての問題を解決するための最長時間を表示します。
ソフトウェアの信頼性	自己登録型ゲストポータル用 OpenID Connect	Cisco ISE は、自己登録ゲストポータルの OpenID Connect（OIDC）認証をサポートしています。ゲストフローでエンドポイントを認証するためのアイデンティティストアとして、Microsoft Entra ID または Okta などの汎用 OIDC アイデンティティ プロバイダーを設定できます。 アイデンティティ プロバイダーとして Microsoft Entra ID を選択した場合は、Microsoft Graph API を使用して、Microsoft Entra ID からグループと属性を取得できます。また、ID トークンまたは UserInfo エンドポイント API を使用して、Microsoft Entra ID からグループと属性を取得することもできます。
	USB ディスク暗号化条件	[すべての外部USBドライブ（All External USB Drives）] 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 3.5 の新機能

表 4. Cisco ISE リリース 3.5 の新機能

製品への影響	機能	説明
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。
セットアップの容易さ	Cisco ISE Data Grid サービスネットワークの要件	Cisco ISE Data Grid サービスでは、最適なパフォーマンスと接続を実現するために、次のネットワークポートを開いておく必要があります。 • ポート 47500：ノード検出とデプロイメント形成をサポートしています。 • ポート 47100：ノード間の内部通信を有効にします。 • ポート 10800：クライアント接続の確立をサポートします。

製品への影響	機能	説明
	シングルスタック IPv6 のサポート	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、新しい **`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。
	IPv6 シングルスタック構成のサポート	Cisco ISE リリース 3.5 より前は、一部の機能で IPv4 と IPv6 のデュアルスタック構成がサポートされていました。IPv6 シングルスタック構成で Cisco ISE を実行する場合は、次の機能がサポートされます。 • ポータル > 管理ポータルアクセス • ポータル > CAコンポーネント EST および SCEP • ポータル > My Devices • ポータル > 証明書プロビジョニング • ポータル > ゲスト - ホットスポット • ポータル > ゲスト - 自己登録 • ポータル > ゲストスポンサー • ポータル > スポンサー付きゲスト • ポータル > MDM • ポータル > ポスチャ - クライアント プロビジョニング • IPv6 シングル スタック サポート インフラストラクチャ > インフラ IPv6 シングルスタック • RADIUS > 認証、アカウンティング承認、属性、監査/デバッグログ、プロキシ、CoA、およびポリシー • RADIUS > OSCP • RADIUS > セキュア syslog ターゲット • RADIUS > DACL ダウンロード • CARS サービス > SSH サーバー、NTP • CARS サービス > 外部リポジトリ：FTP、SFTP、TFTP、NFS、HTTP、および HTTPS • CARS サービス > TCP ダンプ

製品への影響	機能	説明
		• CARS サービス > NNS • アイデンティティストア > Active Directory • アイデンティティストア > LDAP(S) • アイデンティティストア > EntraID • アイデンティティストア > EntraID モニター • 通信 > RMQ • 通信 > Cisco ISE ノード間 • 通信 > エンドポイント DB（ノード間通信） • API > ERS • API > オープン API • API > API ゲートウェイ • API > MnT REST API • 外部サービス > ポスチャフィード • 外部サービス > スマートライセンス • TrustSec > SGACL の定義 • TrustSec > SXP マッピング属性 • TrustSec > HTTP 経由のポリシーダウンロード • TrustSec > HTTP 経由の TrustSec サーバー • TrustSec > RADIUS 経由の CoA • pxGrid > サービス • ポスチャ > ポスチャフロー • ポスチャ > エージェントレス • オブザーバビリティ > ライブログまたはセッション • オブザーバビリティ > ログ分析、Kibana、および Grafana • オブザーバビリティ > MnT レポート • カスタム属性 > 内部ユーザー • カスタム属性 > 内部エンドポイント

製品への影響	機能	説明
		• エンドポイント プロファイリング > DHCPv6 • エンドポイント プロファイリング > RADIUS 属性 • エンドポイント プロファイリング > エンドポイントへの SNMP プローブ • エンドポイント プロファイリング > NAD への SNMP プローブ • テレメトリ > テレメトリ
使いやすさ	Cisco ISE ライセンス戦略の拡張機能	プロファイリングサービス、TrustSec、pxGrid、および pxGrid Direct のライセンス使用量が、機能の使用状況に基づいてライセンス階層ごとに正確に追跡されるようになりました。各階層の消費量は、その特定の階層に関連付けられた機能を使用しているアクティブなエンドポイントの数によって決まります。ただし現時点では、コンプライアンス違反ライセンスに対するライセンスの適用は実装されていないことにご注意ください。 ライセンスに関する質問は、ise-license-escalation@external.cisco.com にお問い合わせください。
	Cisco pxGrid Cloud の新しいリージョンのサポート	Cisco pxGrid Cloud は、米国に加えてヨーロッパ、アジア太平洋、および日本でサポートされるようになりました。
	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 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）]**）を使用して Cisco ISE と統合できます。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。
	Cisco ISE での OCSP のホストヘッダーのサポート	Cisco ISE は、オンライン証明書ステータスプロトコル（OCSP）サーバーで必要な場合に、HTTP 1.1 プロトコルで指定されるホストヘッダーフィールドをサポートするようになりました。この機能拡張により、基盤となるプロトコルとして HTTP 1.0 を維持しながら、このようなサーバーとの互換性が確保されます。
	Microsoft Active Directory 参加ポイントの専用リソースの割り当て	各 PSN の Microsoft Active Directory 参加ポイントのリソースを予約できます。このリソースのセグメンテーションは、Microsoft Active Directory 参加ポイント間で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します。
	ゲストパスワードをリセットする際の国コードドロップダウンの追加	自己登録したゲストのパスワードリセットプロセスには、新しい国コードが記載されたドロップダウンリストが含まれます。自己登録したゲストが **[電話（Phone）]** オプションを選択してパスワードをリセットすると、国コードのドロップダウンが表示されるようになりました。ゲストユーザーは、電話番号を入力する前に適切な国コードを選択できます。

製品への影響	機能	説明
	NTP 認証キーのサポート	Cisco ISE CLI 設定モードの **`ntp authentication-key`** コマンドは、特に AES128 や AES256 などの暗号化タイプをサポートします。このコマンドでは、ハッシュとプレーンテキストの両方のキー値がサポートされます。NTP を認証と正常に同期させるには、設定したキーを NTP サーバーに関連付ける前に信頼できるリストに追加する必要があります。
	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。
	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。
	Simple Network Management Protocol スキャンを使用したネットワークと IoT デバイスのプロファイル	Simple Network Management Protocol（SNMP）スキャンは、IoT とネットワークデバイスを分類し、プロファイリングポリシーを作成します。プローブデータを使用して、特定のサブネットまたは IP アドレス範囲に対してスケジュールされた SNMP スキャンまたはオンデマンドの SNMP スキャンを実行します。SNMP を使用して、詳細な OS とハードウェアの情報を収集します。このスキャンはシスコおよびサードパーティのデバイスをサポートしており、資産管理システムなしでのデプロイメントに役立ちます。
	管理インターフェイスの選択	初期セットアッププログラムを実行してアプライアンスを設定するときに、そのアプライアンスの管理インターフェイスとして設定するインターフェイスを選択できるようになりました。使用可能なインターフェイスが 1 つだけの場合は、Gig0 がデフォルトの管理インターフェイスとして設定されます。また、Cisco ISE CLI から **`application reset-config ise`** コマンドを使用して管理インターフェイスを変更することもできます。 このオプションは、Cisco SNS 3700 シリーズおよび Cisco SNS 3800 シリーズのアプライアンスで使用できます。Cisco SNS 3700 および 3800 シリーズ アプライアンスでは、管理インターフェイスとして eth0 ～ eth5 のイーサネット インターフェイスを選択できます。たとえば、eth2 を管理インターフェイスとして選択すると、eth2 がすべてのポータルのデフォルトインターフェイスになります。また、管理インターフェイスをこれらのアプライアンスのファイバポートに割り当てることもできます。このオプションは仮想マシンには適用されません。

製品への影響	機能	説明
	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
	[Probe Status] ダッシュボード	[Operations] > [System 360] > [Log Analytics] > [Dashboards] の [Probe Status] ダッシュボードには、Cisco ISE が受信したすべてのアクティブなプロファイリングプローブ、ネットワーク アクセス デバイス（NAD）プローブステータス、およびエンドポイントプローブの詳細が表示されます。より詳細な結果を得るには、フィルタを使用して特定の PSN、PSN グループ、または NAD を選択します。 各 PSN または NAD に対して生成されたプローブを分析することで、NAD が適切に設定されているかどうかを確認できます。生成されたプローブパケットを分析し、それに応じてプローブと NAD の設定を更新することができます。
	時間制限付きデバッグの有効化	時間制限付きデバッグ有効化機能を使用すると、ログレベルを選択し、デフォルト設定に戻すタイマーを設定できます。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。
	新しい TrustSec テレメトリ属性	展開のモニタリングを強化し、TrustSec と Cisco ISE の使用方法に関するデータを収集するために、新しい TrustSec テレメトリ属性が追加されました。その一部を以下に示します。 • 作成された SGACL の数 • セキュリティグループの数 • TrustSec が設定されているネットワークデバイスの数 • SGT を割り当てるポリシーの数、SGT を使用するポリシーの数 • その他の関連する TrustSec モニタリングテレメトリ属性など

製品への影響	機能	説明
	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。
	Cisco ISE 統合機能の強化	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。
	すべてのネットワークデバイスのリポジトリへのエクスポート	Cisco ISE でネットワークデバイスをエクスポートするときに、**[すべてをリポジトリにエクスポート（Export All to Repository）]** を選択し、すべてのネットワークデバイスをリポジトリにエクスポートできます。登録済みの電子メールアドレスに、エクスポートされたデータにアクセスする方法が記載された電子メールが送信されます。
	TACACS+ 向けの ROPC サポート	Cisco ISE は、リソース所有者パスワードログイン情報（ROPC）フローを設定するための TACACS+ ワークフローをサポートするようになりました。これにより、Microsoft Entra ID によるユーザー認証が可能になります。これは、これまでサポートされていた EAP-TLS および TEAP ワークフローに追加されます。
	USGv6 コマンドのサポート	`usgv6` コマンドを EXEC モードで使用して、基盤となるオペレーティングシステムで Cisco ISE ノードの U.S. Government IPv6（USGv6）コンプライアンスステータスを有効化、無効化、または確認できます。
	osquery 条件のサポート	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。
	pxGrid Direct の OAuth2 認証のサポート	Cisco pxGrid Direct は、Cisco ISE GUI を介して URL Fetcher pxGrid Direct コネクタを作成するときに、Basic、API Key、および OAuth2 の 3 つの認証方式をサポートするようになりました。URL Fetcher pxGrid Direct コネクタは、データ同期用に設定した URL を使用します。 Cisco pxGrid Direct OAuth2 では、アクセストークンを取得するために [Client Credentials] と [Password] の両方がサポートされています。[Client Credentials] フローではクライアント ID とシークレットが使用され、[Password] フローではクライアントのログイン情報とユーザー名およびパスワードの両方が必要です。トークンが期限切れになると、更新トークンを使用して新しいアクセストークンが取得されます。

製品への影響	機能	説明
	EntraID 属性変更後の CoA の送信	Cisco ISE を使用すると、Microsoft Entra ID インスタンス内のユーザーまたはデバイス属性の変更をモニターできます。事前定義されたルールで変更が検出されると、Cisco ISE は影響を受けるエンドポイントセッションの再認証をトリガーし、更新されたネットワーク アクセス ポリシーが適用されるようにします。特定の属性をモニターするように認証ポリシーを設定し、SAML を使用してそれらを取得することで、Cisco ISE は属性の変更を特定し、認可変更（CoA）を発行し、再認証後に更新されたアクセス権限を再適用できます。このプロセスにより、承認判断に常に最新の属性情報が反映されます。
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。 **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	Tenable Security Center の API キーと証明書認証のサポート	Cisco ISE リリース 3.5 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。 • [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を許可するように Tenable Security Center を設定する必要があります。
	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	[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 [メニュー（Menu）] アイコンをクリックし、**[操作（Operations）] > [ワークロード（Workloads）] > [ワークロード（Workloads）] > [ワークロードライブセッション（Workloads Live Session）]** の順に選択します。
	ワークロード分類ルール	ワークロード分類ルールを使用してワークロードを分類し、プライマリおよびセカンダリ SGT をワークロードに割り当てることができます。プライマリ SGT は pxGrid セッショントピックで “Security Group” とマークされ、SXP を介して IP から SGT へのマッピングを公開するために使用されます。セカンダリ SGT は、“Secondary Security Groups” という名前の順序付き配列として pxGrid セッショントピックに含まれています。 分類ルールの実行順序を指定できます。ルールをドラッグアンドドロップして順序を変更できます。

製品への影響	機能	説明
	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。
	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 3.5 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 には「ISE_SGT_<SGT_TAG>」というフォーマットを使用して名前が付けられていました。この「ISE_SGT_」は定数プレフィックスであり、<SGT_TAG> はセキュリティグループタグを指します。 Cisco ISE リリース 3.5 から、命名規則は「ISE_<SG_NAME>」に変更されます。現在は「ISE_」が定数プレフィックスであり、その後にセキュリティグループ（SG）名が続きます。 この命名変更の自動移行サポートはありません。既存の EFT のお客様は、潜在的な問題を回避するため、Cisco ISE リリース 3.5 にアップグレードする前にアウトバウンドルールを無効にし、アップグレードが完了したら再度有効にする必要があります。
	リモート TAC サポート承認	リモートサポート承認により、Cisco ISE 管理者は、特定の Cisco TAC スペシャリストが、CLI と GUI のいずれかまたは両方を介して Cisco ISE デプロイメントに安全にリモートアクセスし、トラブルシュート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。
	クラウド多要素分類プロファイラ	クラウド多要素分類（MFC）プロファイラは、観測された属性を分析のためにクラウドと共有することで、エンドポイント分類を強化します。これによりエンドポイントのラベリング、グループ化、およびポリシーの適用が改善され、スタンドアロン展開と分散型展開の両方がサポートされています。Cisco ISE リリース 3.4 と比較して、クラウドオンボーディング中の分類ラベルが改善され、カスタムルールとダイレクトルールの両方のサポートが追加されます。 クラウド MFC プロファイラを有効にするには、**[管理（Administration）] > [フィードサービス（Feed Service）] > [クラウド多要素分類プロファイラ（Cloud Multi-Factor Classification Profiler）]** に移動し、リージョンを選択して **[有効化（Enable）]** をクリックします。その後、シスコの認証ポータルにリダイレクトされ、シスコのログイン情報の入力を求められます。
	証明書検証のプロトコルエンジン	プロトコルエンジンという別個のサービスが、運用効率を向上させるために選択したシナリオで証明書を検証します。プロトコルエンジンは、API コールを介して Cisco ISE アプリケーションサーバーと通信します。CLI で **show application status ise** コマンドを入力すると、**プロトコルエンジン**と呼ばれる新しいサービスが実行されます。
	ダイナミック再認証スケジューラ	ダイナミック再認証スケジューラを使用して、各セッションに事前に定義された有効期限の日時を設定することでアクセス制御を強化できます。これにより、指定された有効期限の間のみセッションがアクティブになるため、不正アクセスを防止できます。

製品への影響	機能	説明
	連邦およびセキュリティ認定	連邦およびセキュリティ認定は、コモンクライテリア認定のネットワーク デバイス コラボレーション保護プロファイル（NDcPP）v3.0e と連携して強化され、これにはセキュアシェル（SSH）や認証サーバー PP モジュールなどのテストが含まれます。 さらに、Cisco ISE リリース 3.5 では次のものが計画されています。 • DoDIN APL 認定 • FIPS 140-3 コンプライアンスレビュー • ホストカテゴリの USGv6 認定および IPv6 対応ロゴ認定
	DoDIN APL サポート	Cisco ISE リリース 3.5 は、ネットワーク アクセス コントローラ（NAC）カテゴリにおける米国国防総省認定製品リスト（DoDIN APL）認定のテストを受けています。テストが完了して認定を受けた後、シスコは DoDIN APL の Web サイトに認定の詳細を掲載します。
	FIPS 140-3 サポート	Cisco ISE は FIPS 140-3 モードをサポートしています。このモードにより、暗号のセキュリティとコンプライアンスが強化され、FIPS 準拠のプロトコル、アルゴリズム、およびキーサイズが適用されます。FIPS モードでは、IPsec、SSHv2、LDAPS、EAP-TLS、EAP-FAST、pxGrid、pxGrid Direct、TC-NAC Tenable、および pxGrid クラウドコンポーネントの非準拠の暗号スイートおよびプロトコルが無効になります。
	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 プロファイラのレジリエンシ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。

製品への影響	機能	説明
	プロファイリングポリシーの機能拡張	Cisco ISE で MFC ベースのプロファイリングポリシーを作成し、ルールベースの分類を使用して、識別できないエンドポイントを分類することができます。カスタムルールまたは直接マッピングルールを通じて自動的にラベルが割り当てられるため、エンドポイント分類プロセスの一貫性が保たれます。 • カスタムルール：特定の組織のニーズのプロファイリング基準を定義し、カスタマイズされた属性に基づいて分類を正確に制御できます。 • 直接マッピングルール：特定の属性または識別子（mdmOSVersion や mdmManufacturer など）を使用して、デバイスを直接分類できます。 Cisco ISE は、以前のリリースから AI/ML およびシステムルールをサポートし続けており、高度なプロファイリング機能と、強化されたユーザー体験およびインターフェイスを提供します。
	SSHD サービス暗号化アルゴリズムの機能拡張	これらの新しいアルゴリズムを **`service sshd`** で使用し、次のような Cisco ISE CLI を使用してサービスを管理できます。 • MAC-algorithm • Hostkey • Hostkey-algorithm • Key-exchange-algorithm • SSH-client-hostkey-algorithm
	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、**外部 RADIUS サーバー**、**RADIUS トークン ID ストア**、および**ネットワーク デバイス プロファイル**に **[応答にメッセージ オーセンティケータが必要（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**メッセージ オーセンティケータ**属性のないパケットを無効にするため、フローが失敗します。
	pxGrid Direct を使用したディクショナリ属性の CoA	pxGrid Direct 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。

製品への影響	機能	説明
	TACACS+ over TLS 1.3 のサポート	ネットワークデバイスの TACACS+ over TLS 1.3 認証を有効にして、セキュリティを強化できます。NAD 証明書の検証について、Cisco ISE は次の SAN 属性の検証をサポートしています。 • IP アドレス（iPAddress） • DNS 名（dNSName） • ディレクトリ名（directoryName） 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（Network Devices）]** ページから、認証ステータスを確認し、TACACS+ over TLS 1.3 認証を設定できます。
	追加の Cisco ISE ワークフローの TLS 1.3 サポート	Cisco ISE リリース 3.5 では、次の項目に対して TLS 1.3 がサポートされます。 • ポータル（アカウント登録ゲストポータル、スポンサーポータル、およびホットスポットポータル） • pxGrid • TACACS+ • Cisco Catalyst Center の統合 • Cisco Meraki の統合 • Cisco Duo の統合 • PEAP ワークフロー • ポスチャフィードサービス通信
	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。
	Red Hat OpenShift プラットフォームのサポート	Cisco ISE リリース 3.5 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。

製品への影響	機能	説明
	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>**.
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 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 Reference Guide』を参照してください。

動作における変更

Cisco ISE リリース 3.5 パッチ 3：動作の変更

表 5. Cisco ISE リリース 3.5 パッチ 3 で動作が変更された機能

機能	説明
Cisco pxGrid および IMS 用 EKU のサポート	Cisco ISE では、Cisco pxGrid サービスと IMS サービスの両方について、サーバー認証拡張キー使用法（EKU）のみを含むサーバー証明書を使用できます。 Cisco ISE では、サーバー認証 EKU を含む Cisco pxGrid および IMS 証明書のインポートまたはバインドが可能です。さらに、Cisco ISE は、サーバー認証とクライアント認証 EKU の両方を含む証明書を引き続き受け入れます。両方の EKU が必要な古いバージョンの Cisco ISE にロールバックする場合、アップグレード後にサーバー専用 EKU 証明書に切り替えると、互換性の問題が発生する可能性があります。 これを回避するには、常に元の証明書をバックアップするか、変更を加える前にプライベート CA から再生成できるようにしてください。

Cisco ISE リリース 3.5 パッチ 2：動作の変更

Cisco ISE リリース 3.5 パッチ 2 では、動作が変更された機能はありません。

Cisco ISE リリース 3.5 パッチ 1：動作の変更

Cisco ISE リリース 3.5 パッチ 1 では、動作が変更された機能はありません。

Cisco ISE リリース 3.5：動作の変更

表 6. Cisco ISE リリース 3.5 で動作が変更された機能

機能	説明
Cognitive Threat Analytics（CTA）アダプタ	Cognitive Threat Analytics（CTA）アダプタは、脅威中心型ネットワーク アクセス コントロール（TC-NAC）フローではサポートされなくなりました。
エンドポイント レプリケーション ページの廃止	[エンドポイント レプリケーション（Endpoint Replication）] ページ（[管理（Administration）] > [システム（System）] > [設定（Settings）] > [エンドポイント レプリケーション（Endpoint Replication）]）は、Cisco ISE GUI で廃止されました。
API ゲートウェイ暗号サポートの変更	API ゲートウェイは最新バージョンの CiscoSSL を使用するようになりました。その結果、Cisco ISE で推奨されていない SHA1 暗号の一部は、Cisco ISE GUI で有効なままになっていたとしても、API ゲートウェイでブロックされます。このセキュリティ強化により、API 通信の暗号化規格が強化されます。
Cisco ISE リリース 3.5 アップグレードの証明書要件	最新の CiscoSSL セキュリティ要件では、管理サービスで SHA1 がサポートされなくなるため、Cisco ISE リリース 3.5 にアップグレードする前に、管理サービスで使用されている SHA1 証明書を、SHA256 以上の安全なアルゴリズムを使用した証明書に置き換えてください。これらの証明書が更新されていない場合、管理サービスが正しく機能しない可能性があります。SHA1 証明書は引き続き他のサービス用にインポートできますが、管理サービスに使用することはできません。
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 3.5 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 3.5 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。
Cisco ISE パスワード セキュリティの強化	Cisco ISE パスワードは、128 ビットソルトと組み合わせて使用される強力な SHA-512 ハッシュを使用して保護されます。

機能	説明
pxGrid クラウド接続向け証明書検証および SAN の要件を強化	pxGrid クラウドは Go 1.24.x を使用するようにアップグレードされたため、セキュリティが向上し、FIPS 準拠が保証されます。この更新の一環として、TLS 証明書の検証が拡張され、pxGrid クラウド接続に使用されるすべての証明書にサブジェクト代替名（SAN）が含まれている必要があります。SAN のない証明書は、FIPS モードまたは非 FIPS モードでもセキュアな接続では受け入れられなくなります。 Cisco ISE サービスの中断を回避するには、Cisco ISE ノードのホスト名と一致する SAN を含めるように pxGrid サービス証明書を更新します。証明書を生成してインストールする方法については、自己署名証明書の生成を参照してください。

解決済みの問題

Cisco ISE リリース 3.5 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。

Cisco ISE リリース 3.5 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 3.5 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 3.5：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 3.5 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。

Cisco ISE リリース 3.5 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。

Cisco ISE リリース 3.5 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。

表 7. Cisco ISE リリース 3.5 累積パッチ 1 の未解決の問題

不具合 ID	説明
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
CSCws46345	OIDC へのポータル参照を削除せずに Cisco ISE リリース 3.5 パッチ 1 をロールバックして再インストールした後、OIDC ワークフローを使用しようとすると、リダイレクト中に「400 Bad Request」エラーが発生することがあります。これは、パッチプロセス後も OIDC の設定と参照が存在する場合に発生します。問題を修正するには、ロールバックしてパッチのインストールが完了した後に、関連するポータルページを保存します。ポータルページを保存すると、リダイレクトが期待どおりに機能するようになります。

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 3.5：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 8. Cisco ISE リリース 3.5：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。

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 3.5 パッチ 3：既知の問題

Cisco ISE リリース 3.5 パッチ 3 に既知の問題はありません。

Cisco ISE リリース 3.5 パッチ 2：既知の問題

Cisco ISE リリース 3.5 パッチ 2 に既知の問題はありません。

Cisco ISE リリース 3.5 パッチ 1：既知の問題

Cisco ISE リリース 3.5 パッチ 1 に既知の問題はありません。

Cisco ISE リリース 3.5：既知の問題

表 9. Cisco ISE リリース 3.5 の既知の問題

不具合 ID	説明
CSCwq03326	SNS アプライアンスのインストール後に、Cisco ISE リリース 3.5 から Cisco ISE リリース 3.3 または 3.4 にダウングレードすると、失敗します。
CSCwq49897	アカウンティングの更新要求が抑制されると、**設定が誤っている NAS** レポートにエントリが表示されません。
CSCwr86578	圧縮した IPv6 アドレス表記（fd00::103/64 など）を使用すると、セットアップおよびリセット設定操作が失敗します。完全な IPv6 アドレス表記（fd00:0:0:0:0:0:0:103/64 など）のみがサポートされています。設定エラーを避けるために、セットアップ時とリセット時の両方で完全な IPv6 アドレス表記を使用します。

互換

Cisco ISE リリース 3.5 へのアップグレード

Cisco ISE リリース 3.4、3.3、および 3.2 から Cisco ISE リリース 3.5 に直接アップグレードできます。

Cisco ISE リリース 3.2 より前のリリースを使用している場合は、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、Cisco ISE リリース 3.5 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 ISE 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、「Deploy Cisco ISE Natively on Cloud Platforms」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 instances and intended usage」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 ISE 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 ISE CLI Reference Guide』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 3.5 は、次の Cisco 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 Appliance Hardware Installation Guide』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）

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詳細は、お使いの Cisco ISE バージョンの『Cisco ISE Installation Guide』を参照してください。

表 10. 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。
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。
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。

仮想環境	サポートの詳細
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 3.5 は、次のサポートブラウザで検証されています。

- Mozilla Firefox バージョン 136、138、139、および 140 以降
- Google Chrome バージョン 134、135、137 以降
- Microsoft Edge バージョン 134、135 以降

検証済み外部 ID ソース

表 11. 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
	Microsoft Windows Active Directory 2022	Windows Server 2022（パッチ Windows10.0-KB5025230-x64-V1.006.msu 適用済み）
	Microsoft Windows Active Directory 2025 **注**：現在、Cisco ISE と Microsoft Windows Active Directory 2025 を統合するには、Active Directory ドメインコントローラの設定を変更する必要があります。詳細については、CSCwn62873 を参照してください。	Windows Server 2025
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

外部 ID ソース	詳細	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 3.5 は、OpenSSL 1.1.1za ベースの CiscoSSL 7.3.410 で検証されています。

関連資料

Cisco ISE を使用するときに活用できるその他のリソースについては、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。

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。