新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

次の表に、新機能および変更された機能の要約と参照先を示します。

表 *1 : Cisco ISE* リリース *3.2* の新機能および変更された機能

機能	説明
Cisco ISE リリース 3.2 パッチ 4	
Cisco Catalyst 9800 ワイヤレス LAN コントローラからの Wi-Fi デバイス分析データ	Cisco ISE に統合されたシスコ ワイヤレス LAN コントローラからのデバイス分析データを使用して、Apple、Intel、および Samsung エンドポイントのプロファイリングポリシー、許可条件、および認証条件とポリシーを作成できます。 Cisco Catalyst 9800 ワイヤレス LAN コントローラからの Wi-Fi デバイス分析データを参照してください
カスタマー エクスペリエンス アンケート	Cisco ISE では、管理ポータル内でユーザーに顧客満足度アンケートが表示されるようになりました。顧客満足度アンケートを定期的に実施することで、シスコではお客様の Cisco ISE のエクスペリエンスをより深く理解し、何が良好に機能しているかを追跡し、改善すべき領域を特定することができます。アンケートを送信すると、その後 90 日間は別のアンケートは表示されません。 アンケートは、すべての Cisco ISE の展開においてデフォルトで有効になっています。アンケートはユーザーレベルで、あるいは Cisco ISE の展開に対して無効にできます。 カスタマー エクスペリエンス アンケートを参照してください
Cisco ISE リリース 3.2 パッチ 3	

新機能および変更された機能に関する情報

機能	説明
外部 LDAP ユーザーを Cisco ISE エンドポイントグループにリンクする	Cisco ISE リリース 3.2 パッチ 3 以降では、[Dynamic] オプションを使用して、外部 LDAP ユーザーグループをゲストデバイスのエンドポイント ID グループに割り当てることができます。詳細については、『*Cisco Identity Services Engine Administrator Guide, Release 3.2*』の「Guest and Secure WiFi」の章の「Create or Edit Guest Types」を参照してください。
ポータルでのウクライナ語のサポート	ゲスト、スポンサー、デバイス、およびクライアントプロビジョニング ポータルに、サポートされるローカリゼーション言語としてウクライナ語が含まれるようになりました。
Cisco ISE リリース 3.2 パッチ 2	
pxGrid Direct の機能拡張	pxGrid Direct は、制御された導入機能ではなくなりました。Cisco ISE リリース 3.2 または 3.2 パッチ 1 から Cisco ISE リリース 3.2 パッチ 2 にアップグレードする前に、設定済みのすべての pxGrid Direct コネクタと、pxGrid Direct コネクタからのデータを使用する認証プロファイルおよび認証ポリシーを削除することを推奨します。Cisco ISE リリース 3.2 パッチ 2 にアップグレードした後、pxGrid Direct コネクタを再設定してください。 Cisco pxGrid Directを参照してください （注） 設定済みの pxGrid Direct コネクタを削除しない場合、コネクタはアップグレード中に自動的に削除されます。この削除により、編集も使用も不可能な認証プロファイルと認証ポリシーが作成されます。これらを削除して新しいものに置き換える必要があります。
Cisco ISE リリース 3.2 パッチ 1	
Cisco ISE の Meraki コネクタ	Cisco ISE 3.2 パッチ 1 以降のリリースは、Cisco ISE と Cisco Meraki の統合をサポートしています。Cisco ISE およびクラウドベースの Cisco Meraki は、TrustSec ポリシーのポリシー管理ポイントである TrustSec 対応システムです。Cisco と Meraki の両方のネットワークデバイスを使用している場合、1 つ以上の Cisco Meraki ダッシュボードを Cisco ISE に接続して、TrustSec ポリシーおよび要素を Cisco ISE から各組織に属する Cisco Meraki ネットワークに複製できます。 Meraki コネクタの設定の詳細については、『*Cisco Identity Services Engine Administrator Guide, Release 3.2*』の「Segmentation」の章にある「Connect Cisco Meraki Dashboards with Cisco ISE」を参照してください。

新機能および変更された機能に関する情報

機能	説明
Cisco AI 分析のサポート	Cisco ISE 3.2 パッチ 1 以降は Cisco AI 分析をサポートしています。Cisco AI Analytics エージェントは、Cisco ISE からエンドポイントのデータに対してクエリを実行し、そのデータを定期的に AI クラウドに送信します。このデータを使用して、AI ベースのエンドポイントグループ化、自動化されたカスタムプロファイリングルール、クラウドソーシングされたエンドポイントラベルを提供することにより、ネットワーク内の不明なエンドポイントの数を減らすことができます。詳細については、『*Cisco ISE Administrator Guide, Release 3.2*』の「Asset Visibility」の章にある「Cisco ISE Administrator Guide, Release 3.2」を参照してください。
Cisco ISE リリース 3.2	
ポスチャ条件スクリプトのサポート	ポスチャ条件スクリプトを作成し、アップロードして、エンドポイントのコンプライアンスステータスを確認できます。この機能は、Windows、MacOS、および Linux プラットフォームでサポートされています。
Cisco AnyConnect のブランド変更	Cisco AnyConnect は、Cisco Secure Client としてブランド変更されました。Cisco ISE 3.2 は、ブランド変更された用語を使用するように Cisco ISE GUI が更新されている場合でも、ブランド変更されたエージェントとレガシーエージェントの両方をサポートします。 コンプライアンス を参照してください。

新機能および変更された機能に関する情報

機能	説明
システム 360	システム 360 には、[モニタリング（Monitoring）] と [Log Analytics] が含まれています。 [モニタリング（Monitoring）] 機能を使用すると、一元化されたコンソールから、展開内のすべてのノードの幅広いアプリケーションとシステム統計、および主要業績評価指標（KPI）を監視できます。KPI は、ノード環境の全体的な状態を把握するのに役立ちます。統計は、システム構成と使用率固有のデータを簡略化して表示します。 Cisco ISE 3.2 以降のリリースは、Grafana および Prometheus と統合されています。Grafana は、サードパーティのメトリクスダッシュボードおよびグラフエディタです。これは、Prometheus データベースで収集された統計とカウンタをグラフィックまたはテキストベースで表示します。Prometheus は、KPI を時系列形式で格納するためのデータストアとして使用されます。 [Log Analytics] は、エンドポイントの認証、許可、アカウンティング（AAA）およびポスチャ syslog データを詳細に分析するための柔軟な分析システムを提供します。ISE 正常性サマリーと ISE プロセスステータスを分析することもできます。 オープンソースのデータ可視化プラットフォームである Kibana を使用して、syslog データを分析および可視化します。Elasticsearch は、syslog データの保存とインデックス作成に使用されます。
モバイルデバイス管理の機能拡張	エンドポイントがプライマリ MDM または UEM サーバーに登録されていない場合、またはプライマリ MDM もしくは UEM サーバーに到達できない場合、[General MDM or UEM Settings] を構成して、複数の MDM サーバーにクエリを実行できます。
ERS API の Open API 仕様	ERS API の Open API 仕様（JSON ファイル）は、Cisco ISE GUI の **[API 設定（API Settings）]** ウィンドウの **[概要（Overview）]** セクションでダウンロードできます（**[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** > **[API設定（API Settings）]** > **[概要（Overview）]**）。 この Open API JSON ファイルは、Python、JAVA などのプログラミング言語を使用した API クライアントコードの自動生成に使用できます。Open API の仕様とツールの詳細については、https://openapi.tools/ [英語] を参照してください。
ERS API PATCH 要求のサポート	Cisco ISE は、ERS API の PATCH 要求をサポートするようになりました。PATCH 要求は、リソースの属性のサブセットを更新するのに役立ちます。そのリソースの構成全体ではなく、要求の一部として送信された属性のみが更新されます。詳細については「API Reference Guide」を参照してください。

新機能および変更された機能に関する情報

機能	説明
[Endpoints] コンテキストの可視性ウィンドウの GUID を持つエンドポイントの単一エントリ	Cisco ISE GUI の **[コンテキストの可視性（Context Visibility）]** > **[エンドポイント（Endpoints）]** ウィンドウで、GUID を持つエンドポイントは、最新のランダム MAC アドレスとともに 1 回だけリストされます。
デフォルトモードまたはダークモードで Cisco ISE を表示する	Cisco ISE をデフォルト（ライト）モードまたはダークモードで表示できるようになりました。Cisco ISE 管理者ポータルの [アカウント設定（Account Settings）] ダイアログボックスから、デフォルトモードまたはダークモードを選択します。
Microsoft Entra ID を使用した EAP-TLS および TEAP 認証	Cisco ISE は、証明書ベースの認証と Microsoft Entra ID 認証をサポートしています。Microsoft Entra ID から属性を選択し、それらを Cisco ISE ディクショナリに追加して、認証ポリシーで使用できます。
Cisco ISE ユーザーのパスワードの管理	Cisco ISE リリース 3.2 以降、Cisco ISE の内部ユーザーとして、[パスワードのライフタイム（Password Lifetime）] オプションを使用して、有効化パスワードとログインパスワードのライフタイムを管理できます。 Cisco ISE ユーザー を参照してください。
Cisco Private 5G	Cisco ISE リリース 3.2 以降、Cisco ISE は Cisco Private 5G およびセッション管理機能（SMF）ソフトウェアをサポートします。Cisco ISE は、RADIUS 認証のみおよびアカウンティングフローで導入される 5G 認証のポリシー設定を提供します。
Data Connect	Data Connect 機能は、オープン データベース コネクティビティ（ODBC）または Java Database Connectivity（JDBC）ドライバを使用して Cisco ISE へのアクセスを提供するため、データベースサーバーを直接照会して、選択したレポートを生成できます。データへの読み取りアクセスのみが提供されます。 ビジネス要件に応じて、ネットワークに関する構成または運用データを抽出し、それを使用して洞察に富んだレポートとダッシュボードを生成できます。 （注） Cisco ISE リリース 3.2 限定提供リリースで Data Connect 機能がアクティブになっている場合、Cisco ISE リリース 3.2 一般提供リリースにアップグレードするときに、Data Connect 機能を無効にしてから有効にする必要があります。

新機能および変更された機能に関する情報

機能	説明
PassiveID ログインユーザーの認証ポリシーの構成	PassiveID ログインユーザーの認証ポリシーを設定する場合は、[Active Directoryの詳細設定（Active Directory Advanced Settings）] ウィンドウの [認証フロー（Authorization Flow）] チェックボックスをオンにします。 Active Directory グループメンバーシップに基づいて SGT をユーザーに割り当てる認証ポリシーを設定できます。設定すると、PassiveID認証に対しても TrustSec ポリシールールを作成できるようになります。
セキュリティ設定の機能拡張	[SHA-1暗号の許可（Allow SHA-1 Ciphers）] オプション（**[管理（Administration）] > [システム（System）] > [設定（Settings）] > [セキュリティ設定（Security Settings）]**の下）が有効になっている場合、Cisco ISE は次の Cisco ISE コンポーネントとの通信に SHA-1 暗号を許可します。 • 管理者アクセス UI • Cisco ISE ポータル • ERS • pxGrid このオプションはデフォルトでは無効になっています。 Cisco ISE リリース 3.2 にアップグレードすると、アップグレード前に有効にした場合でも、[Allow SHA-1 Ciphers] オプションは無効になります。クライアントが SHA-1 暗号化のみを使用して Cisco ISE と通信できるようにする場合は、アップグレード後にこのオプションを有効にできます。このオプションを有効または無効にした後、展開内のすべてのノードを再起動する必要があります。 セキュリティ設定の構成 を参照してください。
エンドポイントプロファイルと論理プロファイルの概要レポート	このレポートには、論理プロファイルとエンドポイントプロファイル、およびそれらのプロファイルに一致するエンドポイントの数が表示されます。
pxGrid Direct	Cisco pxGrid Direct は、エンドポイント属性の JSON データを提供する外部 REST API に接続するのに役立ちます。収集されるデータは、pxGrid Direct 構成で指定した属性に基づいています。次に、pxGrid Direct は収集したデータを Cisco ISE データベースに保存します。 このデータは、認証ポリシーで使用できます。pxGrid Direct はエンドポイントをより迅速に評価および認証するのに役立ちます。取得されたデータが認証ポリシーで使用されるためです。これにより、エンドポイントを承認する必要があるたびにエンドポイント属性データをクエリする必要がなくなります。

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。