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

（注） Cisco ISE リリース 3.4 および対応するガイドは、段階的なロールアウトで入手できます。ソフトウェアの一般提供が開始されるまでは、シスコのアカウントマネージャに連絡して、このリリースをリクエストしてください。段階的なロールアウトが完了すると、Cisco ISE リリース 3.4 および対応するガイドがすべてのお客様に一般提供されます。

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 *3.4* の新機能および変更された機能

特長	説明
Cisco ISE のレジリエンシ	Cisco ISE リリース 3.4 以降、Cisco ISE のレジリエンシを維持するために、**過剰な RADIUS ネットワークデバイス通信**アラームと**過剰なエンドポイント通信**アラームが追加されています。 「Cisco ISE アラーム」を参照してください。
デバッグログの設定	各デバッグログコンポーネントに許可される最大ファイルサイズと最大ファイル数を設定できます。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。 デバッグログの設定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

特長	説明
URL プッシャ pxGrid Direct コネクタタイプの作成	Cisco ISE GUI を使用して、pxGrid Direct コネクタを作成できます。pxGrid Direct コネクタタイプには、[URLフェッチャ（URL Fetcher）] と [URLプッシャ（URL Pusher）] の 2 種類があります。Cisco ISE リリース 3.4 以降では、[URLフェッチャ（URL Fetcher）] の pxGrid Direct コネクタタイプまたは [URLプッシャ（URL Pusher）] の pxGrid Direct コネクタタイプのいずれかを選択できます。pxGrid Direct プッシュ API を使用して、エンドポイントデータを Cisco ISE にプッシュすることができます。 Cisco ISE リリース 3.4 以降では、配列を含むコネクタ属性を使用して認証プロファイルを設定することもできます。 URL プッシャコネクタタイプの作成を参照してください。
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。 Cisco ISE でのレガシー IPSec からネイティブ IPSec への移行を参照してください。
優先順位によるドメインコントローラの選択の強制	優先ドメインコントローラのフェールオーバーが発生した場合に、Cisco ISE のドメインコントローラ選択をオーバーライドすることを選択できるようになりました。このオプションを有効にすると、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。 優先ドメインコントローラの設定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

特長	説明
拡張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。 [ネットワークデバイス（Network Devices）] で、 • RADIUS共有秘密（RADIUS Shared Secret） • Radiusの2番目の共有秘密（Radius Second Shared Secret） [ネイティブIPSec（Native IPSec）] で、 • 事前共有キー（Pre-shared Key） セキュリティ設定の構成を参照してください。 • ネットワークデバイスのインポートおよびエクスポート中に RADIUS の共有秘密と 2 番目の共有秘密がプレーンテキストで表示されないようにするために、[PasswordEncrypted:Boolean(true|false)] というヘッダーを持つ新しい列が [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。 ネットワーク デバイスのインポート テンプレート形式を参照してください。
「今すぐ同期」を使用したオンデマンドのpxGrid直接データ同期	Cisco ISE リリース 3.4 以降では、[Sync Now（今すぐ同期）] 機能を使用して、pxGrid Direct 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。 「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

特長	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。 多要素認証のための Cisco Duo と Cisco ISE の統合を参照してください。
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、[ライブログの詳細（Live Log Details）] ページと [AAA 診断（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 [アラーム（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。 ダウンロード可能 ACL を参照してください。
複数の Cisco Application Centric Infrastructure コネクタのサポート	Cisco ISE を使用すると、複数のドメイン間で一貫したアクセスポリシーを作成して適用できます。Cisco ISE では、Cisco Application Centric Infrastructure（Cisco ACI）を使用して SGT および SGT バインディングを共有できます。また、Cisco ACI からエンドポイントグループ（EPG）、エンドポイント セキュリティ グループ（ESG）、およびエンドポイント情報を学習することもできます。Cisco ISE に複数の Cisco ACI 接続を追加できます。 Cisco ISE で学習したコンテキストを管理し、Cisco ISE コネクタと Cisco ACI コネクタ間のコンテキストフローを最適化するルールを設定できます。 Cisco ISE は、Cisco ACI マルチテナントおよび Multi-Virtual Routing and Forwarding の展開をサポートしています。複数の接続を介してマルチファブリックを定義できます。この統合では、マルチポッドおよび個々の Cisco ACI ファブリックがサポートされます。 Cisco ISE でのシスコ アプリケーション セントリック インフラストラクチャ接続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

特長	説明
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。 許可ポリシーの設定を参照してください。
RADIUS 抑制およびレポートの機能拡張	Cisco ISE リリース 3.4 以降、RADIUS の抑制とレポートに関する機能が拡張され、RADIUS（**[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。 「RADIUS 設定」を参照してください。
トランスポートゲートウェイのサポートの削除	Cisco ISEではトランスポートゲートウェイがサポートされなくなりました。次の Cisco ISE 機能では、接続方法としてトランスポートゲートウェイが使用されていました。 • Cisco ISE スマート ライセンス スマートライセンス設定の接続方法としてトランスポートゲートウェイを使用している場合は、Cisco ISE リリース 3.4 にアップグレードする前に設定を編集する必要があります。Cisco ISE リリース 3.4 ではトランスポートゲートウェイがサポートされていないため、別の接続方法を選択する必要があります。接続方法を更新せずに Cisco ISE リリース 3.4 に更新すると、アップグレードプロセス中に HTTPS 直接接続方法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。

新機能および変更された機能に関する情報

特長	説明
Cisco ISE ワークフローの TLS 1.3 サポート	Cisco ISE リリース 3.4 では、TLS 1.3 が次のワークフローでピアと通信できます。 • Cisco ISE は、EAP-TLS サーバーとして設定されます • Cisco ISE は、TEAP サーバーとして設定されます **注目** Cisco ISE リリース 3.4 の時点では、TEAP TLS 1.3 が使用可能なクライアント OS でサポートされていないため、TEAP サーバーとして設定された Cisco ISE の TLS 1.3 サポートは、内部テスト条件下でテストされています。 • Cisco ISE は、セキュアな TCP syslog クライアントとして設定されます 「セキュリティ設定の構成」を参照してください。

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。