

Cisco ISE 3.1 アップグレードガイド：概要

初版：2022年12月28日

最終更新：2022年12月28日

Cisco ISE アップグレードの概要

Cisco Identity Services Engine (Cisco ISE) リリース 3.1 以降、すべての pxGrid 接続は pxGrid 2.0 に基づく必要があります。pxGrid 1.0 ベース (XMPP ベース) の統合は、リリース 3.1 以降の Cisco ISE では動作しなくなります。

WebSocket に基づく pxGrid バージョン 2.0 は、Cisco ISE リリース 2.4 で導入されました。統合の中断を防ぐために、他のシステムを計画して pxGrid 2.0 準拠バージョンにアップグレードすることをお勧めします。

このマニュアルでは、Cisco ISE アプライアンスおよび仮想マシン (VM) で Cisco ISE ソフトウェアをリリース 3.1 にアップグレードする方法について説明します。(『[Release Notes for Cisco Identity Services Engine, Release 3.1](#)』の「[What is New in Cisco ISE, Release 3.1](#)」を参照してください。)

Cisco ISE 展開環境のアップグレードは複数段階のプロセスであり、このマニュアルで指定されている順序で実行する必要があります。このマニュアルで示されている推定所要時間を使用して、最小限のダウンタイムでのアップグレードを計画してください。展開環境に含まれる複数のポリシーサービスノード (PSN) が1つの PSN グループに属している場合、ダウンタイムは発生しません。アップグレード対象の PSN で認証されるエンドポイントがない場合、要求はノードグループ内の別の PSN で処理されます。エンドポイントは、認証の成功後に再認証されて、ネットワークアクセス権が付与されます。



注意 スタンドアロン展開環境または単一の PSN のみの展開環境の場合は、その PSN がアップグレードされている間、すべての認証にダウンタイムが発生する可能性があります。



(注) Cisco ISE リリース 3.2 以降にアップグレードすると、ルート CA の再生成がアップグレードフローで自動的に行われます。したがって、アップグレード後のルート CA の再生成は必要ありません。

さまざまなタイプの展開

- スタンドアロンノード：管理、ポリシーサービスおよびモニタリングのペルソナを担当する単一の Cisco ISE ノード
- マルチノード展開：複数の ISE ノードによる分散展開。

Cisco ISE のネイティブクラウド展開の違い

Cisco ISE アップグレードワークフローは、AWS 上の Cisco ISE では使用できません。新規インストールのみがサポートされています。ただし、設定データのバックアップと復元は実行できます。Cisco ISE AWS インスタンスでデータを復元すると、データは Cisco ISE リリース 3.1 バージョンにアップグレードされます。

ルート CA チェーンの再生成

次のイベントが発生した場合は、ルート CA チェーンを再生成する必要があります。

- PAN または PSN のドメイン名またはホスト名の変更。
- 新しい展開でのバックアップの復元。
- アップグレード後に古いプライマリ PAN を新しいプライマリ PAN に昇格。

ルート CA チェーンを再生成するには、次のように選択します。

1. Cisco ISE GUI で [メニュー (Menu)] アイコン (☰) をクリックして、[管理 (Administration)] > [システム (System)] > [証明書 (Certificates)] > [証明書の管理 (Certificate Management)] > [証明書署名要求 (Certificate Signing Requests)] の順に選択します。
2. [証明書署名要求 (CSR) の生成 (Generate Certificate Signing Request (CSR))] をクリックします。
3. [証明書の使用先 (Certificate(s) will be used for)] ドロップダウンリストから、[ISE ルート CA (ISE Root CA)] を選択します。
4. [ISE ルート CA 証明書チェーンの置き換え (Replace ISE Root CA Certificate Chain)] をクリックします。

アップグレードパス

シングルステップアップグレード

次のリリースはすべて、Cisco ISE リリース 3.1 に直接アップグレードできます。

- Cisco ISE リリース 2.6
- Cisco ISE リリース 2.7
- Cisco ISE リリース 3.0
- Cisco ISE リリース 3.1

2段階のアップグレード

Cisco ISE リリース 2.6 より前のバージョンを現在使用している場合は、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 3.1 にアップグレードする必要があります。

仮想マシンでサポートされるオペレーティングシステム

Cisco ISE は、Red Hat Enterprise Linux (RHEL) に基づく Cisco Application Deployment Engine オペレーティングシステム (ADE-OS) で動作します。Cisco ISE 3.1 では、ADE-OS は RHEL 8.2 に基づいています。

次の表に、Cisco ISE のさまざまなバージョンで使用される RHEL バージョンを示します。

表 1: RHEL リリース

Cisco ISE リリース	RHEL リリース
Cisco ISE 1.3	RHEL 6.4
Cisco ISE 1.4	RHEL 6.4
Cisco ISE 2.0	RHEL 7.0
Cisco ISE 2.1	RHEL 7.0
Cisco ISE 2.2	RHEL 7.0
Cisco ISE 2.3	RHEL 7.0
Cisco ISE 2.4	RHEL 7.3
Cisco ISE 2.6	RHEL 7.5
Cisco ISE 2.7	RHEL 7.6
Cisco ISE 3.0	RHEL 7.6
Cisco ISE 3.1	RHEL 8.2
Cisco ISE 3.2	RHEL 8.4



(注) RHEL 8.2 以降は、次の VMware ESXi バージョンをサポートしています。

- VMware ESXi 6.5
- VMware ESXi 6.5 U1
- VMware ESXi 6.5 U2
- VMware ESXi 6.5 U3
- VMware ESXi 6.7
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2
- VMware ESXi 7.0 U3

上記に加えて、RHEL 8.2 は、互換性のある新しい VMware ESXi バージョンもサポートします。

VMware 仮想マシン (VM) の Cisco ISE ノードをアップグレードする場合は、アップグレード後に、RHEL のサポートされるバージョンにゲスト オペレーティング システムを変更する必要があります。これを行うには、VM の電源をオフにし、サポートされる RHEL バージョンにゲスト オペレーティング システムを変更してから VM の電源をオンにする必要があります。



(注) [ゲスト OS RHEL 8 (Guest OS RHEL 8)] および [ファームウェア EFI (Firmware EFI)] を選択した場合は、[VM オプション (VM Options)] タブで [UEFI セキュアブートの有効化 (Enable UEFI Secure Boot)] オプションが無効になっていることを確認する必要があります。このオプションは、ゲスト オペレーティング システム RHEL 8 VM ではデフォルトで有効になっています。Cisco ISE VM の [UEFI セキュアブートの有効化 (Enable UEFI Secure Boot)] オプションが無効であることを確認してください。

RHEL オペレーティング システム アップグレードを使用した Cisco ISE アップグレードは、通常のアップグレードプロセスよりも時間がかかる場合があります。また、Oracle データベース バージョンに変更がある場合は、オペレーティング システムのアップグレード時に新しい Oracle パッケージがインストールされるため、アップグレードにさらに時間がかかる場合があります。

ライセンスの変更

この項では、Cisco ISE リリース 3.1 のライセンスの変更点について説明します。

Cisco ISE ライセンスの詳細については、次の資料を参照してください。

- [Cisco ISE 発注ガイド](#)
- [Cisco ISE 移行ガイド](#)
- [Cisco ISE ライセンス FAQ](#)

Cisco ISE GUI でのライセンスのアクティブ化については、「[Licensing](#)」を参照してください。

仮想アプライアンスのライセンス

Cisco ISE リリース 3.1 以降は ISE VM ライセンスをサポートしています。これは、リリース 3.1 以前にサポートされていた VM Small、VM Medium、および VM Large ライセンスに代わるものです。新しい ISE VM ライセンスは、オンプレミス展開とクラウド展開の両方の Cisco ISE VM ノードを対象としています。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「[Licensing](#)」の章にある「[Cisco ISE Licenses](#)」を参照してください。

特定ライセンス予約

特定のライセンス予約は、組織のセキュリティ要件で Cisco ISE と Cisco Smart Software Manager (CSSM) 間の永続的な接続が許可されていない場合にスマートライセンスを管理するためのスマートライセンス方式です。特定のライセンス予約では、Cisco ISE ノードで特定のライセンス権限を予約できます。

予約する必要があるライセンスのタイプと数を定義して特定のライセンス予約を作成し、Cisco ISE ノードで予約をアクティブ化します。登録して予約を有効にした Cisco ISE ノードは、ライセンスの使用を追跡し、ライセンス消費のコンプライアンスを適用します。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「[Licensing](#)」の章にある「[Specific License Reservation](#)」を参照してください。

その他の参考資料

次のリンクには、Cisco ISE で作業するときを使用できる追加のリソースが含まれています。

https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

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、[シスコサービス](#) 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 DevNet](#) にアクセスしてください。
- 一般的なネットワーク、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。

Cisco バグ検索ツール

[Cisco バグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

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。