



Cisco ISE アップグレードの概要

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で Cisco Identity Services Engine (Cisco ISE) ソフトウェアをリリース 3.0 にアップグレードする方法について説明します。
(『Cisco Identity Services Engine リリース 3.0 リリースノート』の「[Cisco ISE リリース 3.0 の新機能](#)」を参照してください。)



- (注) Cisco ISE リリース 2.3 以降では、すべての既存のネットワーク アクセス ポリシーとポリシー セットを置き換える、新しい拡張された [ポリシーセット (Policy Sets)] ページが用意されています。以前のリリースからリリース 2.3 以降にアップグレードすると、すべてのネットワーク アクセス ポリシーの設定 (認証および認可の条件、ルール、ポリシー、プロファイル、および例外を含む) が Cisco ISE GUI の新しい [ポリシーセット (Policy Sets)] ウィンドウに移行されます。ポリシーモデルの詳細については、『[Cisco Identity Services Engine リリース 2.6 管理者ガイド](#)』の「新規ポリシー モデル」のセクション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。
- アップグレードパス (2 ページ)
- 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 (3 ページ)
- ライセンスの変更 (4 ページ)
- その他の参考資料 (5 ページ)
- 通信、サービス、およびその他の情報 (6 ページ)

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 3.0 に直接アップグレードできます。



- (注) 永久ライセンス予約がある場合、またはアップグレード元のリリースで SSM オンプレミス接続方式が有効になっている場合は、まずこれらの機能を無効にする必要があります。その後、Cisco ISE リリース 3.0 パッチ 2 以降にアップグレードして、Cisco ISE でこれらの機能を再び有効にします。

永久ライセンス予約および SSM オンプレミス接続方式は、次のリリースで使用可能です。

- Cisco ISE リリース 2.6 パッチ 10 以降
- Cisco ISE リリース 2.7 パッチ 4 以降

• Cisco ISE、リリース 2.4

• Cisco ISE リリース 2.6

• Cisco ISE リリース 2.7

アップグレードバンドルは Cisco.com からダウンロードすることができます。リリース 3.0 では、次のアップグレードバンドルを使用できます。

[ise-upgradebundle-2.4.x-2.7.x-to-3.0.0.458.SPA.x86_64.tar.gz](#) : リリース 2.4、2.6、または 2.7 から 3.0 にアップグレードするには、このバンドルを使用します

2段階のアップグレード

Cisco ISE リリース リリース 2.4 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 3.0 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 3.0 では、ADE-OS は RHEL 7.6 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 3.2	RHEL 8.4

Cisco ISE リリース 3.0 以降のリリースでは、VMware ESXi 7.0.3 以降のリリースに更新することを推奨します。

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

デバイス管理ライセンス

Cisco ISE リリース 2.x に使用されている Base、Plus、Apex などのライセンスが新しいライセンスタイプに置き換えられました。Cisco ISE リリース 3.0 では、Essentials、Advantage、Premier のライセンスを使用します。『[Cisco Identity Services Engine 管理者ガイド](#)』の「ライセンス」の章を参照してください。ライセンスの移行の詳細については、『[ISE 3.0 License Migration Guide](#)』を参照してください。

Cisco ISE リリース 3.0 でライセンスの消費を有効にするには、Cisco Smart Software Manager (CSSM) を使用して既存のスマートライセンスか従来のライセンスを新しいライセンスタイプに変換する必要があります。

Cisco ISE 2.4 以降、デバイス管理ライセンスの数は、展開環境のデバイス管理ノード（デバイス管理サービス用に設定された PSN）の数と同じである必要があります。

現在、デバイス管理ライセンスを使用していてリリース 2.4 以降へのアップグレードを計画している場合、TACACS+ 機能はリリース 2.4 以降で 50 デバイス管理ノードに対しサポートされます。

新しい PID から生成された PAK をインストールすると、PAK ファイルで利用可能な数量に応じてデバイス管理ライセンス数が表示されます。必要なデバイス管理ノード数に基づいて、展開に複数のデバイス管理ライセンスを追加できます。Evaluation ライセンスでは、1 つのデバイス管理ノードをサポートします。

VM ノードのライセンス

Cisco ISE は、仮想アプライアンスとしても提供されています。リリース 2.4 以降では、展開に VM ノードの適切な VM ライセンスをインストールすることをお勧めします。VM ノードの数と CPU やメモリなどの各 VM ノードのリソースに基づいて、VM ライセンスをインストールする必要があります。そうでない場合、リリース 2.4 以降で VM ライセンスキーを調達してインストールする警告と通知が表示されますが、サービスは中断されません。

VM ライセンスは、インフラストラクチャライセンスなので、展開で使用可能なエンドポイントライセンスに関係なく VM ライセンスをインストールできます。展開に Evaluation、Base、Plus、Apex ライセンスのどれもインストールされていない場合でも、VM ライセンスをインストールできます。ただし、Base、Plus、または Apex ライセンスによって有効になる機能を使用するには、適切なライセンスをインストールする必要があります。

リリース 2.4 以降のインストールまたはアップグレードの後、展開済みの VM ノードの数とインストール済みの VM ライセンスの数の間に不一致がある場合、アラームが 14 日ごとに [A

ラーム (Alarms)] ダッシュレットに表示されます。アラームは、VM ノードのリソースに変化がある場合や、VM ノードが登録または登録解除されるたびにでも表示されます。

VM ライセンスは永続ライセンスです。VM ライセンスの変更は、Cisco ISE GUI にログインするたびに表示され、通知ダイアログボックスで [このメッセージを再度表示しない (Do not show this message again)] チェックボックスをオンにすると表示されなくなります。

以前に ISE VM ライセンスのいずれも購入していない場合は、『Cisco Identity Services Engine 発注ガイド』を参照して購入する適切な VM ライセンスを選択します。製品認証キー (PAK) が関連付けられていない ISE VM ライセンスを購入済みの場合、licensing@cisco.com で ISE VM 購入を反映する販売注文番号を使用して VM PAK を要求することができます。この要求は、過去に購入した ISE VM ごとに 1 つの中規模 VM ライセンスキーを提供するように処理されます。

VM ライセンスのカテゴリ

VM ライセンスは、小、中、大の 3 つのカテゴリで提供されます。これらのカテゴリは、ハードウェアアプライアンス、RAM 容量、CPU 数などのリソースによって異なります。たとえば、8 コアと 64 GB RAM を搭載した 3595 相当の VM ノードを使用している場合に、その VM で同じ機能をレプリケートするには、中カテゴリの VM ライセンスが必要になります。展開の要件に応じて、VM とそのリソースの数に基づいて、複数の VM ライセンスをインストールする必要があります。

次の表は、VM カテゴリに必要な VM 最小リソースを示しています。

VM カテゴリ	VM ライセンス仕様
小	<ul style="list-style-type: none"> • 最小 16GB RAM および CPU 12 コア (SNS-3515 相当)。 • 最小 32GB RAM および CPU 16 コア (SNS-3615 相当)。
中	<ul style="list-style-type: none"> • 最小 64GB RAM および CPU 16 コア (SNS-3595 相当)。 • 最小 96GB RAM および CPU 24 コア (SNS-3655 相当)。
大	<ul style="list-style-type: none"> • 最小 256GB RAM および CPU 16 コア (500,000 を超える同時セッションをサポートするクラスタの MnT)。 • 最小 256GB RAM および CPU 24 コア (SNS-3695 相当)。

ライセンスの詳細については、『Cisco Identity Services Engine 管理者ガイド』の「Cisco ISE ライセンス」の章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、[Cisco Services](#) [英語] 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、[Cisco Support](#) [英語] 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](#) [英語] 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](#) [英語] 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。

シスコバグ検索ツール

[シスコバグ検索ツール](#) (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。