Cisco ISE 3.0 アップグレードガイド：概要

Cisco ISE アップグレードの概要

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

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で Cisco Identity Services Engine（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 については、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存在する場合、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） 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。

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。分散展開をアップグレードする手順については、次の参照先で説明しています。

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。

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。 [証明書署名要求（CSR）の生成（Generate Certificate Signing Requests（CSR））] をクリックします。[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。[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、3.0 に直接アップグレードできます。

- 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 Release 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（ADEOS）で動作します。Cisco ISE 3.0 では、ADEOS 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

VMware 仮想マシンの Cisco ISE ノードをアップグレードする場合は、アップグレードの完了後に、Red Hat Enterprise Linux（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 システムを変更します。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、変更後に VM の電源をオンにする必要があります。

一般に、Cisco ISE のアップグレードに RHEL（Red Hat Enterprise Linux）OS（Red Hat の後継バージョン）のアップグレードが含まれている場合は、ISEインスタンスあたりのアップグレード所要時間が長くなります。さらに、ISE の Oracle データベースバージョンに変更がある場合は、OS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ます。このためアップグレードに時間がかかる場合があります。アップグレードの時間を最小限にするには、ISE のアップグレード中に基盤となる OS がアップグレードされるかどうかを確認する必要があります。

エアギャップ ネットワークのスマート ライセンス

Cisco ISEスマートライセンスでは、Cisco ISE をCSSMに接続する必要があります。ネットワークがエアギャップされている場合、Cisco ISE はライセンスの使用状況を CSSM に報告できません。このレポートの欠落により、Cisco ISE への管理アクセスと Cisco ISE 機能の制限が失われます。

エアーギャップされたネットワークでのライセンスの問題を回避し、Cisco ISE の全機能を有効にするには、Smart Software Manager（SSM）オンプレミスを設定します。このライセンス方式は、Cisco ISE リリース 3.0 パッチ 2 以降で利用できます。展開内のノードで SSM オンプレミスサーバを設定し、Cisco ISE がこのサーバに到達できることを確認できます。このサーバは、エアギャップされたネットワーク内でのCSSMのロールを引き継ぎ、必要に応じてライセンス権限を解放し、使用状況メトリックを追跡します。SSMオンプレミスサーバは、ライセンスの消費と有効性に関連する通知、アラーム、および警告メッセージも送信します。

ライセンスを購入するか、または購入したライセンスを変更する場合は、SSMオンプレミスをCSSM に接続し、ローカルサーバで変更を使用できるようにする必要があります。

（注）
- SSM オンプレミス ライセンス ソリューションを有効にすると、Cisco ISE でプロキシサービスを使用できなくなります。また、外部 CA 証明書によって有効にされている Cisco ISE サービスも使用できなくなります。
- ISE-PIC 3.0 はスマートライセンスをサポートしていません。

スマートライセンス用の Smart Software Manager オンプレミスの設定

始める前に

展開内のノードで SSM オンプレミスサーバを設定し、Cisco ISE が確実にこのサーバに到達できるようにします。このノードは専用サーバである必要があります。このノードで Cisco ISE ペルソナを有効にしないでください。

「Smart Software Manager オンプレミスのリソース」を参照してください。

手順

ステップ 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）] > [ライセンシング（Licensing）]**を選択します。

ステップ 2 [登録の詳細（Registration Details）] をクリックします

ステップ 3 表示される [登録の詳細（Registration Details）] 領域に、CSSM から [登録トークン（Registration Token）] フィールドで受信した登録トークンを入力します。

ステップ 4 [接続方式（Connection Method）] ドロップダウンリストから [SSM オンプレミスサーバ（SSM On-Prem Server）] を選択します。

SSM オンプレミスポータルの [証明書（Certificates）] に、接続されている SSM オンプレミスサーバの IP アドレスまたはホスト名（あるいは FQDN）のいずれかが表示されます。

ステップ 5 設定した IP アドレスまたはホスト名（あるいは FQDN）を [SSM オンプレミスサーバホスト（SSM On-Prem server Host）] フィールドに入力します。

ステップ 6 [階層（Tier）] 領域と [仮想アプライアンス（Virtual Appliance）] 領域で、有効にする必要があるすべてのライセンスのチェックボックスをオンにします。選択したライセンスがアクティブ化され、その使用量が CSSM によって追跡されます。

ステップ 7 [登録（Register）] をクリックします。

永久ライセンスの予約

Cisco ISE リリース 3.0 パッチ 2 以降では、永久ライセンス予約のライセンス方式がサポートされています。

インターネットへの永続的な接続がないと、Cisco ISE スマートライセンスはライセンスの使用状況に関するCSSMを更新できません。このように Cisco ISE と CSSM 間の通信が失われると、管理アクセスが失われ、Cisco ISE の機能が最適化されない可能性があります。永久ライセンス予約は、インターネットへの永続的な接続がない Cisco ISE 展開に適したライセンス方式です。

重要 永久ライセンス予約は、承認されなければ使用できないライセンス方式です。永久ライセンス予約を環境内で使用できるかどうかについては、シスコのアカウントマネージャにお問い合わせください。

永久ライセンス予約では、Cisco ISE にユニバーサル予約をインストールします。このライセンス方式では、ネットワークで任意の Cisco ISE ライセンス権限を使用できます。

このライセンス方式が有効になっている場合、Cisco ISE ライセンスは、対応する Cisco ISE 機能が使用されている場合はCSSMに接続してライセンスの消費を促進または報告する必要はありません。ライセンスの消費と使用に関する通知、警告、またはアラートは受信しません。

展開内のすべてのプライマリポリシー管理ノード（PAN）に永久ライセンス予約をインストールする必要があります。オプションですが、すべてのセカンダリ PAN でもこのライセンス方式を有効にすることを推奨します。

セカンダリ PAN で永久ライセンス予約を有効にすると、次のシナリオでサービスの中断を回避できます。

- プライマリ PAN のフェールオーバー
- ハイアベイラビリティのプライマリ PAN の設定

- プライマリ PAN がセカンダリ PAN として一時的に降格されるアップグレードのワークフロー

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 [アラーム（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	• 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	• 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	• 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。