CHAPTER 5

Cisco ISE のアップグレード

Cisco Identity Services Engine（ISE）は、以前のメジャー リリースまたはメンテナンス リリースから最新の Cisco ISE メンテナンス リリース 1.0.4 にアップグレードできます。また、Cisco Secure Access Control System（ACS）5.1 および 5.2 リリースから最新の Cisco ISE メンテナンス リリース 1.0.4 に移行することもできます。

Cisco Secure ACS 4.x 以前のバージョンまたは Cisco Network Admission Control（NAC）アプライアンスから最新の Cisco ISE リリースに移行することはできません。

Cisco Secure ACS 5.1 および 5.2 リリースから最新の Cisco ISE リリースへの移行に関する情報については、『*Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.0.4*』を参照してください。

（注） 最新の Cisco ISE リリースには、最新の ACS 5.x リリースからのみ移行できます。最新の Cisco ISE リリースへの移行を計画する前に、最新の ACS 5.x リリースにアップグレードする必要があります。

ここでは、次の手順について説明します。

Cisco ISE ノードのアップグレード

（注） Cisco ISE リリース 1.0.3.377 から Cisco ISE メンテナンス リリース 1.0.4.573 へのアップグレード後のデフォルト「admin」管理者ユーザ インターフェイス アクセスに関する、既知の問題があります。詳細については、『*Release Notes for Cisco Identity Service Engine, Release 1.1*』の「Known Issues」を参照してください。

Cisco ISE は以前のリリースから次のリリースにアップグレードできます。以前のリリースには、すでにインストールされているパッチが含まれる場合があります。また、任意のメンテナンス リリースになる場合があります。

たとえば、Cisco ISE リリース 1.0 を最新の Cisco ISE メンテナンス リリースにアップグレードし、メンテナンス リリースを次の将来のリリースに後でアップグレードすることができます。

次のアップグレード オプションを使用できます。

- CLI からアプリケーション アップグレードを実行する。詳細については、「CLI からのアプリケーション アップグレードの実行」（P.5-2）を参照してください。

- 分割展開アップグレードを実行する。詳細については、「分割展開アップグレードの実行」（P.5-4）を参照してください。
- 以前の Cisco ISE リリース 1.0 または Cisco ISE メンテナンス リリース 1.0.4 アプライアンスを、最新の Cisco ISE リリース 1.1 を実行する新しい Cisco ISE アプライアンスに置き換える。詳細については、「ISE 1.1 を実行する Cisco ISE アプライアンスによる ISE 1.0 ソフトウェアを実行する Cisco ISE アプライアンスの置換」（P.5-6）を参照してください。

（注） ノード ペルソナの変更、システム同期、ノードの登録または登録解除などの展開設定の変更は、展開内のすべてのノードが完全にアップグレードされるまで遅延することを強く推奨します。（ただし、この推奨の例外の 1 つに、「スタンドアロン ノードでのアップグレード障害からの回復」（P.5-8）に記載されている、失敗したアップグレードからの回復に必要な手順が含まれます）。

（注） 以前のバージョンの Cisco ISE から Cisco ISE 1.1 に Cisco ISE モニタリング ノードがアップグレードまたは復元されると、アクティブ セッションは保持されず、「0」にリセットされます。

CLI からのアプリケーション アップグレードの実行

Cisco ISE では、Cisco ISE リリース 1.0 および Cisco ISE メンテナンス リリース 1.0.4 から最新の Cisco ISE メンテナンス リリース 1.1 に CLI から直接アプリケーション アップグレードすることもできます。このオプションにより、アプライアンス上に新しい Cisco ISE ソフトウェアをインストールし、同時に設定およびモニタリング情報データベースをアップグレードすることができます。

アプリケーション アップグレードを実行するには、Cisco ISE CLI から次のコマンドを入力します。

application upgrade *application-bundle repository-name*

それぞれの説明は次のとおりです。

- *application-bundle* は、Cisco ISE アプリケーションをアップグレードするアプリケーション バンドルの名前です。
- *repository-name* はリポジトリの名前です。

詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4*』を参照してください。

（注） 手順を進める前に、異なる種類のノード上でアップグレードを実行する方法に関する次の項の情報をすべて確認することを推奨します。

次の場合、CLI から **application upgrade** コマンドを使用して Cisco ISE を以前のバージョンから現在のバージョンにアップグレードできます。

- 管理、ポリシー サービス、および監視ペルソナを担当しているスタンドアロン ノード上の Cisco ISE をアップグレードする場合。
- 分散展開で Cisco ISE をアップグレードする場合。

（注） Cisco ISE をアップグレードする前にプライマリ管理ノードのオンデマンド バックアップ（手動）を実行します。

アップグレード プロセスを検証するには、次のいずれかを実行します。

- アップグレード プロセスについて、*ade.log* ファイルを確認します。

  ade.log ファイルをダウンロードするには、『*Cisco Identity Services Engine User Guide, Release 1.1*』の第 23 章「Downloading Support Bundles」を参照してください。
- **show version** CLI コマンドを実行してビルド バージョンを確認します。

スタンドアロン ノードでの Cisco ISE のアップグレード

管理、ポリシー サービス、および監視ペルソナを担当しているスタンドアロン Cisco ISE ノードで CLI から **application upgrade** コマンドを実行できます。

スタンドアロン ノードで Cisco ISE をアップグレードするには

ステップ 1　管理ユーザ インターフェイスまたは CLI からプライマリ管理 ISE ノードのオンデマンド バックアップ（手動）を実行し、Cisco ISE をアップグレードする前に管理ユーザ インターフェイスからモニタリング ノードのオンデマンド バックアップを実行します。

オンデマンド バックアップの実行方法の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の「*On-Demand Backup*」を参照してください。

ステップ 2　Cisco ISE CLI から **application upgrade** コマンドを起動します。このプロセスは、アプリケーション バイナリ、データベース スキーマ、およびデータモデル モジュールを内部的にアップグレードします。また、Cisco Application Deployment Engine (ADE) リリース 2.0 オペレーティング システム（ADE-OS）アップデートのアップグレードも処理します。

アップグレード プロセスでシステムのリロードが必要な場合、Cisco ISE ノードは正常にアップグレードされると、自動的に再起動されます。

スタンドアロン ノードでの正常なアップグレードの CLI トランスクリプトは次のようになります。

```
ise-vm29/admin# application upgrade ise-appbundle-1.1.0.xxx.i386.tar.gz disk
Save the current ADE-OS running configuration? (yes/no) [yes]?
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Initiating Application Upgrade...
################################################################
NOTICE: ISE upgrade requires you to change the database
administrator and database user password. You will be
prompted to change these passwords after the system reboots.
################################################################
Stopping ISE application before upgrade...
Running ISE Database upgrade...
Upgrading ISE Database schema...
ISE Database schema upgrade completed.
Running ISE Global data upgrade as this node is a STANDALONE...
Running ISE data upgrade for node specific data...

This application Install or Upgrade requires reboot, rebooting now...
```

ステップ 3　Cisco ISE リリース 1.0.3.377 または Cisco ISE メンテナンス リリース 1.0.4.573 を Cisco ISE リリース 1.1 にアップグレードすると、**host-key host <sftpservername>** コマンドを使用してホスト キーを承認するまで SFTP リポジトリを使用できない場合があります。このコマンドの使用の詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.1*』を参照してください。

ステップ 4　リブートが完了すると、ログイン資格情報によるログインを求めるプロンプトが表示され、すぐに新しい Cisco ISE 内部データベースの管理者およびユーザ パスワードの入力が求められます。（プロセスのこの部分は、ログインに使用しているユーザ アカウントが管理者レベルのアクセス権限を持つ場合のみ成功します）。

```
login: admin
```

```
password:
% NOTICE: ISE upgrade requires you to change the database administrator and user
passwords, before you can start the application.
Enter new database admin password:
Confirm new database admin password:
Enter new database user password:
Confirm new database user password:
Starting database to update password...

Starting database to update password...
ISE Database processes already running, PID: 3323
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
```

アプリケーション バイナリおよび Cisco ADE-OS のアップグレード中に障害が発生した場合は、アプリケーション バンドルの以前のバージョンを削除して再インストールするだけでバックアップを復元できます。

アップグレードの障害からの回復方法の詳細については、「スタンドアロン ノードでのアップグレード障害からの回復」（P.5-8）を参照してください。

（注）　Cisco ISE リリース 1.0.3.377 または Cisco ISE メンテナンス リリース 1.0.4.573 を Cisco ISE リリース 1.1 にアップグレードすると、以前のジョブが正常に機能しないため、スケジュール設定されたバックアップ ジョブを再作成する必要があります。

分割展開アップグレードの実行

分散展開で Cisco ISE ノードをリリース 1.1 にアップグレードするには、分割展開アップグレードの方法を使用する必要があります。

プライマリ管理 ISE ノード データベースに行われた設定の変更は、セカンダリ管理 ISE ノード、インライン ポスチャ ノード、および展開内のすべてのセカンダリ ノードに適用されます。これにより、各ノードが設定のローカル コピーを持つようにプライマリ管理 ISE ノードからすべてのノードにデータベースを複製することができます。すべてのノード間での設定データの複製により、最新バージョンで実装された機能変更および必要な設定が複雑になる場合があります。

分散展開での Cisco ISE ノードの中央集中型の設定および管理の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の第 10 章「Setting Up ISE in a Distributed Environment」を参照してください。

（注）　完全な Cisco ISE 展開をアップグレードするには、ドメイン ネーム システム（DNS）サーバの解決が必須です。そうでない場合、アップグレードは失敗します。

（注）　分割展開アップグレード中に、ノードを新しいプライマリ管理ノードに登録する前に、次のことを実行する必要があります。

- 自己署名証明書を使用する場合、すべてのノードの自己署名証明書を新しいプライマリ管理ノードにインポートする必要があります。
- ノードに異なる CA 証明書を使用する場合、すべての CA 証明書を新しいプライマリ管理ノードにインポートする必要があります。
- ノードに同じ CA 証明書を使用する場合、その CA 証明書を新しいプライマリ管理ノードにインポートする必要があります。

Cisco ISE の展開でプライマリ管理 ISE ノード、セカンダリ管理 ISE ノード、インライン ポスチャ ノード、および複数のポリシー サービスノードがある場合、分割展開アップグレードの方法を使用して Cisco ISE をアップグレードして、この展開の問題を解決できます。展開を分割することにより、Cisco ISE 展開でアップグレードするバージョンの新しい展開を作成できます。

まず、セカンダリ管理 ISE ノードを新しい展開に移動し、その後、すべてのポリシー サービス ノードを新しい展開に段階的方法で移動します。すべてのポリシー ノードを新しい展開にアップグレードしたら、Cisco ISE の展開は完了します。

完全な Cisco ISE 展開を次のリリースにアップグレードする際、Cisco ISE をアップグレードするバージョンに基づいて新しい展開を作成し、すべてのノードを新しい展開に移行します。

分割展開アップグレードは 2 つの段階で行われます。

- 「セカンダリ管理 ISE ノードから新しい展開へのアップグレード」（P.5-5）
- 「新しい展開へのポリシー サービス ノードのアップグレード」（P.5-6）

セカンダリ管理 ISE ノードから新しい展開へのアップグレード

（注）　展開でノードをアップグレードする前に、プライマリ管理 ISE ノードおよびモニタリング ノードのオンデマンド バックアップを取得する必要があります。また、アップグレードする前にインライン ポリシー エンフォースメント ポイント（IPEP）ノードを記録して、アップグレード後に IPEP ノードを再設定できるようにする必要があります。

上位のリリースにアップグレードする際、最初にセカンダリ管理 ISE ノードのみを上位バージョンにアップグレードする必要があります。

たとえば、1 つのプライマリ管理ノード（ノード A）、1 つのセカンダリ管理ノード（ノード B）、1 つの IPEP ノード（ノード C）、および 2 つの PDP（ノード D およびノード E）による展開セットアップがある場合、アップグレード手順は次のように進めることができます。

ステップ 1　展開セットアップからセカンダリ ノード（ノード B）を登録解除します。登録解除すると、スタンドアロン ノードになります。このスタンドアロン ノードを Cisco ISE リリース 1.1.x.x にアップグレードします。

ステップ 2　展開セットアップから PDP ノード（ノード D）を登録解除します。登録解除すると、スタンドアロン ノードになります。このスタンドアロン ノードを Cisco ISE リリース 1.1.x.x にアップグレードします。

ステップ 3　ノード B を新しい展開のプライマリ ノードとして昇格させ、ノード D を PDP ノードとして登録します。

ステップ 4　展開セットアップから IPEP ノード（ノード C）を登録解除し、スタンドアロン ノードにします。この IPEP ノードを Cisco ISE リリース 1.1.x.x にアップグレードします。

（注）　アップグレード プロセスにより、IPEP ノードの設定が削除されます。アップグレード後、IPEP ノードを再設定する必要があります。

ステップ 5　展開から 2 番目の PDP ノード（ノード E）を登録解除し、Cisco ISE リリース 1.1.x.x にアップグレードします。ノード B に PDP ノードとして登録します。

ステップ 6　以前の展開のプライマリ モード（ノード A）をスタンドアロン ノードに変換します。ノード A を Cisco ISE リリース 1.1.x.x にアップグレードし、Cisco ISE リリース 1.1 展開セットアップ内のノード B にセカンダリ ノードとして登録します。

ステップ 7　IPEP ノード証明書を新しいプライマリ管理ノード（ノード B）証明書と交換します。同様に、IPEP ノード証明書を新しいセカンダリ管理ノード（ノード A）証明書と交換します。

（注）　管理インターフェイス証明書を信頼できるようにするため、プライマリとセカンダリ管理ノードの両方の証明書を、各 IPEP ノードにインストールする必要があります。証明書のプロビジョニングの詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の「Deploying an Inline Posture Node」セクションを参照してください。

ステップ 8　IPEP ノード（ノード C）を新しい展開セットアップ、つまりノード B に登録します。

新しい展開へのポリシー サービス ノードのアップグレード

以前の展開のプライマリ管理 ISE ノードに適用された設定は、新しい展開のセカンダリ管理 ISE ノードにも適用する必要があります。これにより、新しい展開でセカンダリ管理 ISE ノードからポリシー サービス ノードを複製できます。これらのノードは新しい展開で動作させることができます。

設定の変更は、以前のバージョンに現在適用しているアップグレードされた展開バージョンに適用する必要があります。アップグレードされたバージョンに適用された設定の変更は、以前のバージョンに戻って適用する必要はありません。

ISE 1.1 を実行する Cisco ISE アプライアンスによる ISE 1.0 ソフトウェアを実行する Cisco ISE アプライアンスの置換

（注）　Cisco Identity Services Engine メンテナンス リリース 1.0.4.558 を実行する Cisco ISE アプライアンスを、Cisco Identity Services Engine メンテナンス リリース 1.0.4.573 を実行する新しい Cisco ISE で置き換えるには、データベースのバックアップ イメージを作成する前にバージョン 1.0.4.558 を実行するアプライアンスを 1.0.4.573 にアップグレードする必要があります。その後、バージョン 1.0.4.573 を実行する新しいアプライアンス上で復元することができます。

（注）　以前のバージョンのバックアップからデータを復元する際、既存の設定は、古いまたは新しい機能に関係なく、復元後にクリアされます。

この項では、次の内容について説明します。

- 「Cisco ISE リリース 1.1 を実行する Cisco ISE アプライアンスによる ISE 1.0 ソフトウェアを実行する Cisco ISE スタンドアロン アプライアンスの置換」（P.5-7）
- 「分散展開でのリリース 1.1 を実行する Cisco ISE アプライアンスによる既存の Cisco ISE ノードのサブセットの置換」（P.5-7）
- 「分散展開での Cisco ISE 1.1 を実行する Cisco ISE アプライアンスによる ISE 1.0 ソフトウェアを実行するすべての Cisco ISE アプライアンスの置換」（P.5-8）

Cisco ISE リリース 1.1 を実行する Cisco ISE アプライアンスによる ISE 1.0 ソフトウェアを実行する Cisco ISE スタンドアロン アプライアンスの置換

このアップグレード シナリオは、Cisco ISE リリース 1.0 または Cisco ISE メンテナンス リリース 1.0.4 ソフトウェアを Cisco ISE リリース 1.1 にアップグレードしており、同時に既存の Cisco ISE シャーシを置換している場合にのみ必要です。

同じ物理アプライアンスまたは仮想マシンを使用している場合、バックアップの復元ではなく、CLI からのアプリケーション アップグレードの実行を使用することを推奨します。

Cisco ISE 1.0 ソフトウェアを実行する Cisco ISE スタンドアロン アプライアンスを Cisco ISE リリース 1.1 を実行する Cisco ISE アプライアンスで置き換えるには、次の手順を実行します。

ステップ 1　Cisco ISE 1.0 アプライアンスをバックアップします。

ステップ 2　新しい Cisco ISE 1.1 アプライアンスを起動および設定します。

ステップ 3　Cisco ISE 1.0 バックアップを復元します。

バックアップおよび復元の方法の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の第 14 章「Backing Up and Restoring Cisco ISE Data」を参照してください。

データを復元した後、すべてのアプリケーション サーバ プロセスが起動し、実行されるまで待つ必要があります。

Cisco ISE アプリケーション サーバ プロセスが実行中であることを確認するには、Cisco ISE CLI コマンドから次のコマンドを入力します。

show application status ise

CLI コマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4*』を参照してください。

分散展開でのリリース 1.1 を実行する Cisco ISE アプライアンスによる既存の Cisco ISE ノードのサブセットの置換

Cisco ISE 1.0 ノードのサブセットを分散展開で 1.1 を実行する Cisco ISE アプライアンスで置き換えるには、次の手順を実行します。

ステップ 1　既存の展開の各ノードで、Cisco ISE 1.1 へのアプリケーション アップグレードを実行します。「CLI からのアプリケーション アップグレードの実行」（P.5-2）を参照してください。

ステップ 2　新しい Cisco ISE 1.1 アプライアンスを展開で登録解除または登録します。

この場合、プライマリ管理 ISE ノードは元のハードウェア上にあるままです。新しい Cisco ISE 1.1 アプライアンスの 1 つを新しいプライマリ管理 ISE ノードに昇格できます。

分散展開での Cisco ISE 1.1 を実行する Cisco ISE アプライアンスによる ISE 1.0 ソフトウェアを実行するすべての Cisco ISE アプライアンスの置換

Cisco ISE メンテナンス リリース 1.0.4 ソフトウェアの Cisco ISE リリース 1.0 を実行するすべての Cisco ISE アプライアンスを、分散環境で Cisco ISE リリース 1.1 を実行する Cisco ISE アプライアンスで置き換えるには、次の手順を実行します。

ステップ 1　既存の展開の各ノードで、Cisco ISE 1.1 へのアプリケーション アップグレードを実行します。「CLI からのアプリケーション アップグレードの実行」（P.5-2）を参照してください。

ステップ 2　セカンダリ アプライアンスを登録解除し、最初の Cisco ISE 1.1 アプライアンスに登録します。

ステップ 3　Cisco ISE 1.0 ハードウェア展開から Cisco ISE 1.1 ハードウェア展開に移動する残りのセカンダリ ノードに対して、手順 2 を繰り返します。

ステップ 4　新しい Cisco ISE 1.1 アプライアンスの 1 つを新しいプライマリ管理 ISE ノードに昇格します。

ステップ 5　最後の Cisco ISE 1.0 アプライアンスを登録解除し、展開の最後の Cisco ISE 1.1 アプライアンスに登録します。

アップグレード障害からの回復

ここでは、次の内容について説明します。

スタンドアロン ノードでのアップグレード障害からの回復

アップグレードが失敗したノード上でロールバックまたはリカバリを試みる前に、**backup-logs** CLI コマンドを使用してアプリケーション バンドルを生成し、リモート リポジトリに置く必要があります。

シナリオ 1：データベース スキーマまたはデータモデルのアップグレード中にアップグレードが失敗する

検出：次のメッセージのいずれかが、コンソールおよび ADE.log に示されます。

- ISE Database schema upgrade failed!
- ISE Global data upgrade failed!
- ISE data upgrade for node specific data failed!

ロールバック方法：ロールバックするには、最後のバックアップから復元します。

アップグレードを再試行する方法：

- ログを分析します。

- 問題を特定および解決するには、生成したアプリケーション バンドルを Cisco Technical Assistance Center（TAC）に送信します。
- アップグレードを再試行するたびに新しいアプリケーション バンドルが必要になります。

シナリオ 2：バイナリ インストール中にアップグレードが失敗する

検出：データベース アップグレード後にアプリケーション バイナリ アップグレードが行われています。バイナリ アップグレードの障害が発生した場合、次のメッセージがコンソールおよび ADE.log に示されます。

% Application install/upgrade failed with system removing the corrupted install

ロールバック方法：以前の ISO イメージを使用して Cisco ISE アプライアンスのイメージを再適用し、バックアップを復元します。

アップグレードを再試行する方法：

- ログを分析します。
- 問題を特定および解決するには、生成したアプリケーション バンドルを Cisco Technical Assistance Center（TAC）に送信します。

アップグレードを再試行するたびに新しいアプリケーション バンドルが必要になります。

アップグレード中に SSH セッションが終了する場合のアプライアンスの回復

検出：アップグレード中に SSH セッションまたはコンソールが切断されるまたは終了する

ロールバック方法：以前の ISO イメージを使用してバックアップから復元することにより、Cisco ISE アプライアンスのイメージ再適用を行います。

アップグレードを再試行する方法：再びアップグレードを続行します。アプライアンスが新しい Cisco ISE バージョン 1.1 でセカンダリ ノードとして使用されている場合、新しいプライマリ管理 ISE ノードに新しい ISO バージョンを直接インストールし、登録します。