CHAPTER 1

Cisco ISE のアップグレード

Cisco ISE の古いリリースはすべて、新しいリリースにアップグレードできます。以前のリリースは、パッチがインストールされているか、メンテナンス リリースである場合があります。

次のリリースはすべて、Cisco ISE メンテナンス リリース 1.1.1 に直接アップグレードできます。

- Cisco ISE リリース 1.0.3.377
- Cisco ISE リリース 1.0.4.573

上記の Cisco ISE 1.0 リリースのいずれかからのアップグレードを行う場合、「有効なライセンスの取得」（P.1-2）に記載された指示に従う必要があります。

ただし、現在 Cisco ISE リリース 1.1 を起動している場合は、Cisco ISE リリース 1.1.1 へのアップグレード前に Cisco ISE 1.1 パッチ 3 を適用する必要があります。Cisco ISE 1.1 パッチ 3 は、Cisco ISE リリース 1.1、1.1 パッチ 1、または 1.1 パッチ 2 に直接適用することができます。このパッチを適用すると、アップグレード手順中にセカンダリ Cisco Administration ISE ノードのライセンスが失われるのを防ぐことができます。

この章は、次の項で構成されています。

（注） Cisco ISE リリース 1.1.1 にアップグレードする場合、Cisco ISE の以前のリリースでは使用していなかったネットワーク ポートの開放を求められる場合があります。『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1*』の付録の「Cisco ISE 3300 Series Appliance Ports Reference」で Cisco ISE での開放が必要なポートの表を確認してください。

作業前の準備

展開をアップグレードする前に、次を実行する必要があります。

- リリース 1.0 からアップグレードする場合は、「有効なライセンスの取得」（P.1-2）に記載された手順に従います。
- Cisco ISE リリース 1.1 を起動している場合は、Cisco ISE リリース 1.1.1 へのアップグレード前に Cisco ISE 1.1 パッチ 3 を適用する必要があります。このパッチを適用すると、アップグレード手順中にセカンダリ Cisco Administration ISE ノードのライセンスが失われるのを防ぐことができます。
- 分割展開アップグレードを実行していて、展開内にセカンダリ Cisco ISE Administration ノードが存在する場合、セカンダリ Cisco ISE 管理ノード（ISE ノード B）の UDI に基づいた有効なライセンスが必要です。

  セカンダリ Administration ノードが 90 日以上稼働していた場合、そのライセンスは登録解除後に失われます。この場合、セカンダリ Cisco ISE Administration ノード（ISE ノード B）用の有効なライセンスを UDI（シリアル番号、バージョン ID、製品 ID）に基づいて取得する必要があります。詳細については、「有効なライセンスの取得」（P.1-2）を参照してください。

  ランタイム中は、セカンダリ Cisco ISE Administration ノードにライセンスをプリインストールまたはインストールすることはできません。ライセンスは、ノードがプライマリ Cisco ISE Administration ノードに設定された後にインストールできます。すべてのライセンスはプライマリ Administration ISE ノードにのみ適用されます。
- Cisco ISE 設定データおよび Cisco ADE オペレーティング システム データのバックアップを取得します。詳細については、「オンデマンド バックアップの実行」（P.1-3）を参照してください。

この項では、次のトピックを扱います。

有効なライセンスの取得

ライセンスは、Cisco Global Licensing Organization（GLO）に要求します。GLO では 24 時間 365 日スタッフが常駐しているため、オンラインでライセンス処理を行う場合はいつでも次のアドレスから問い合わせることができます。

http://www.cisco.com/go/license

GLO へのライセンス要求には次の 3 つの方法があります。

- http://cisco.com/tac/caseopen でのオンライン ポータル テクノロジーおよびサブテクノロジーの選択後、必ず [問題のタイプ（Type of Problem）] リスト ボックスから [ライセンス（Licensing）] を選択してください。このオプションは、重大度が 3 のサービス リクエストを行う場合に最も効率が良く、推奨される方法です。
- 電話：800-553-2447（米国およびカナダ）その他の地域の番号については、次のリンクを使用します。

  http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html. このオプションは、ネットワークの停止または重大な劣化などの素早い対処が必要な状況で使用します。
- GLO への E メール：licensing@cisco.com. 新しいライセンスを要求する場合に備えて、セカンダリ管理ノードの UDI を通知する必要があります。UDI は次のコマンドを入力して取得できます。

psn1/admin# show udi

さらにセールス オーダー番号と可能な場合には元のライセンスの PAK 番号を通知する必要があります。

オンデマンド バックアップの実行

Cisco ISE 設定データおよび Cisco ADE オペレーティング システム データのオンデマンド バックアップを実行できます。バックアップには次の 2 つの方法があります。

- 「Cisco ISE UI からのバックアップ」（P.1-3）
- 「Cisco ISE CLI からのバックアップ」（P.1-4）

Cisco ISE UI からのバックアップ

Cisco ISE ユーザ インターフェイス（UI）にはプライマリ管理ノードのオンデマンド バックアップを取得するオプションがあります。Cisco ISE アプリケーション固有の設定データ、またはアプリケーションと Cisco ADE オペレーティング システムのデータのバックアップを取得できます。

前提条件：

1. この作業を実行する前に、Cisco ISE でのバックアップおよび復元操作の基礎を理解しておく必要があります。
2. リポジトリを設定していることを確認します。詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1.1*』の「Configuring Repositories」を参照してください。
3. すべての Cisco ISE 管理者アカウントには、1 つ以上の管理ロールが割り当てられています。次の手順で説明されている操作を実行するには、Super Admin または System Admin のいずれかのロールを割り当てられている必要があります。様々な管理ロールとそれぞれに関連する権限についての詳細は、『*Cisco Identity Services Engine User Guide, Release 1.1.1*』の「Cisco ISE Admin Group Roles and Responsibilities」を参照してください。

（注）　操作のバックアップおよび復元では、読み取り専用リポジトリである CDROM、HTTP、または HTTPS オプションを選択することはできません。

オンデマンド バックアップを行うには次の手順を実行します。

ステップ 1　[管理（Administration）] > [システム（System）] > [メンテナンス（Maintenance）] を選択します。

ステップ 2　左の [操作（Operations）] ナビゲーション ペインから　[データ管理（Data Management）] > [管理ノード（Administration Node）] > [オンデマンド フル バックアップ（Full Backup On Demand）] を選択します。

[オンデマンド バックアップ（Backup On Demand）] ページが表示されます。

ステップ 3　バックアップ ファイルの名前を入力します。

ステップ 4　バックアップ ファイルを保存するリポジトリを選択します。

ここにリポジトリ名を入力することはできません。ドロップダウン リストから利用可能なリポジトリのみを選択できます。バックアップの実行前にリポジトリを作成していることを確認してください。

ステップ 5　[OS システム データを除くアプリケーションのみのバックアップ（Application-Only Backup, Excludes OS System Data）] チェックボックスをオンにし、Cisco ISE アプリケーション データのバックアップを取得します。Cisco ADE オペレーティング システム データも必要な場合はこのチェックボックスをオフにします。

ステップ 6　[暗号化キー（Encryption Key）] を入力します。このキーは、バックアップ ファイルの暗号化および解読に使用されます。

ステップ 7　[すぐにバックアップ（Backup Now）] をクリックしてバックアップを実行します。

（注）　分散展開では、バックアップの実行中にノードのロールを変更したり、ノードの設定を行ったりすることはできません。バックアップの実行中にノードのロールを変更すると、すべての手順が中断し、データに不一致が生じる場合があります。ノードのロールを変更する際は、バックアップが完了するまで待機してください。

ステップ 8　[オンデマンド バックアップ（Backup On Demand）] ページを表示している場合、ページが更新されページの右下に次のメッセージが表示されます。

バックアップが正常に完了しました。（Backup is done successfully.）

バックアップのステータスの確認のために Cisco ISE ユーザ インターフェイスの他のページに移動している場合は、[バックアップ履歴（Backup History）] ページに移動する必要があります。詳細については、「Viewing Backup History」を参照してください。

Cisco ISE は、バックアップ ファイル名にタイムスタンプを追加し、このファイルを特定のリポジトリに保存します。バックアップ ファイルが指定したリポジトリ内に存在するかどうか確認してください。

Cisco ISE CLI からのバックアップ

Cisco ISE CLI からのバックアップを実行し（Cisco ISE および Cisco ADE OS データを含む）、リポジトリにバックアップを保存するには、EXEC モードで **backup** コマンドを使用します。Cisco ADE OS データのない Cisco ISE アプリケーションのみのバックアップを実行するには、**application** コマンドを使用します。

（注）　EXEC モードでの **backup** コマンドの使用を試みる前には、ネットワーク サーバなどの安全な場所に対する現在の設定をコピーするか、Cisco ISE サーバ スタートアップ設定として保存する必要があります。このスタートアップ設定は、バックアップおよびシステム ログから Cisco ISE アプリケーションを復元またはトラブルシューティングする際に使用できます。実行中の設定をスタートアップ設定にコピーする詳細な方法については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*』の「copy」コマンドを参照してください。

backup *backup-name* **repository** *repository-name* **application** *application-name* **encryption-key hash |plain** *encryption-key name*

下の表に構文を説明します。

backup	Cisco ISE および Cisco ADE OS のバックアップを実行し、バックアップをリポジトリに保存するコマンド。
backup-name	バックアップ ファイルの名前。100 文字までの英数字で指定します。
repository	リポジトリ コマンド。
repository-name	ファイルをバックアップする場所。80 文字までの英数字で指定します。

application	アプリケーション コマンド（Cisco ODE OS システム データを除くアプリケーションのみのバックアップ）。
application-name	アプリケーション名。255 文字までの英数字で指定します。
encryption-key	バックアップを保護するユーザ定義の暗号化キーを指定します。
hash	バックアップを保護するハッシュ化された暗号化キー。使用する*暗号化された*（ハッシュ化された）暗号化キーを指定します。40 文字までで指定します。
plain	バックアップを保護するプレーンテキストの暗号化キー。使用する*暗号化されたプレーンテキストの暗号化キーを指定します。15 文字までで指定します。
encryption-key name	バックアップ用の暗号化キーをハッシュ /プレーン フォーマットで指定します。

このコマンドは Cisco ISE および Cisco ADE OS データのバックアップを実行し、バックアップを暗号化（ハッシュ化）されたまたは暗号化されていないプレーンテキストのパスワードとともにリポジトリに保存します。

ユーザ定義の暗号化キーを使用してバックアップを暗号化および解読できます。

例 1

```
ise/admin# backup mybackup repository myrepository encryption-key plain Lab12345
% Creating backup with timestamped filename: backup-111125-1252.tar.gpg
ise/admin#
```

例 2

```
ise/admin# backup mybackup repository myrepository application ise encryption-key plain
Lab12345
% Creating backup with timestamped filename: backup-111125-1235.tar.gpg
ise/admin#
```

CLI からのアプリケーション アップグレードの使用

Cisco ISE では Cisco ISE リリース 1.0、1.0.4、または 1.1 パッチ 3 から最新の Cisco ISE メンテナンス リリース 1.1.1 へのアプリケーション アップグレードを CLI から直接実行できます。このオプションによりアプライアンスの新しい Cisco ISE ソフトウェアをインストールし、同時に情報データベースの設定とモニタリングをアップグレードできます。

Cisco ISE CLI からアプリケーション アップグレードを実行するには次を入力します。

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ためのアプリケーション バンドルの名前です。
- *repository-name* はリポジトリの名前です。

スタンドアロン ノードでのアップグレードを成功させるための CLI トランスクリプトについての詳細は、「Cisco ISE スタンドアロン ノードのアップグレード」（P.2-1）を参照してください。

（注） 先に進む前に、このマニュアルのすべての章を見直して様々なタイプのノードでアップグレードを実行する方法を確認しておくことをお勧めします。

次の場合には 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。

- Administration、Policy Service、Monitoring の各ペルソナを担当するスタンドアロン ノードで Cisco ISE をアップグレードする場合。第 2 章「スタンドアロン ノードのアップグレード」を参照してください。
- 2 ノード展開で Cisco ISE をアップグレードする場合。第 3 章「2 Admin ノード展開のアップグレード」を参照してください。
- 分散展開で Cisco ISE をアップグレードする場合。第 4 章「分散展開のアップグレード」を参照してください。

（注） Cisco ISE のアップグレード前には、プライマリ管理ノードのオンデマンド バックアップを（手動で）実行します。「オンデマンド バックアップの実行」（P.1-3）を参照してください。

（注） ノードのペルソナの変更、システム同期、ノード登録または登録解除（分割ドメイン アップグレードで必要）などの展開設定の変更は、展開内のすべてのノードのアップグレードが完了してから行うことを強く推奨します。（ただし、この推奨事項は、「スタンドアロン ノードでのアップグレードの障害からの復旧」（P.5-1）で説明する失敗したアップグレードからの復旧時に必要な手順にはあてはまりません）。

（注） Cisco ISE の古いバージョンから Cisco ISE 1.1.1 に Cisco ISE Monitoring ノードをアップグレードまたは復元する場合、アクティブなセッションは維持されず、「0」にリセットされます。

アップグレード プロセスの検証

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。

- *ade.log* ファイルでアップグレード プロセスを確認します。

  ade.log ファイルを表示するには、CLI から次のコマンドを発行します。

  ```
  show logging system
  ```

- **show version** CLI コマンドを実行し、ビルド バージョンを検証します。

アップグレードに関する既知の問題

ここではアップグレードに関する以下の問題を説明します。

- 「Cisco ISE 1.0.4 から Inline Posture のある 1.1.1 へのアップグレード」（P.1-7）
- 「Cisco ISE リリース 1.0.3.377 からのアップグレード」（P.1-8）

Cisco ISE 1.0.4 から Inline Posture のある 1.1.1 へのアップグレード

ISE 1.1.1 では、Inline Posture ノードが証明書に基づく承認を行うため、管理 ISE ノードに接続できません。そのため、アップグレード手順を開始する前に展開から Inline Posture ノードを取り外し、アップグレード後に Inline Posture ノードを再設定する必要があります。そのためには、ここに説明されている手順に従います。

警告　**相互承認のために Inline Posture 展開用の適切な証明書を設置する必要があります。**

前提条件

ノードを登録解除する*前に* Inline Posture ノードのすべての設定データを記録します。または、（Admin ユーザ インターフェイス内の）各 [インライン ポスチャ（Inline Posture）] タブのスクリーンショットを保存してデータを記録することもできます。このデータを保持しておくことで、後続の作業を完了するための Inline Posture ノードの再登録を素早く行うことができます。

Inline Posture のある Cisco ISE 1.1.1 にアップグレードするには、次の手順を実行します。

ステップ 1　Cisco Administration ISE ノードから Cisco Inline Posture ノードを登録解除します。

（注）　CLI に移動してコマンド **show application status ise** を入力すると、Inline Posture ノードが ISE ノード ステータスに戻ったことを確認できます。ノードが ISE ノードに戻っていないことがわかった場合は、コマンド プロンプトに **pep switch outof-pep** を入力できます。ただし、この方法は最終手段であると考えてください。

ステップ 2　『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1*』の説明に従って Cisco Administration ISE ノードを 1.1.1 にアップグレードします。

ステップ 3　Administration ISE ノードで CA ルート証明書のインポート、CSR の生成、証明書の作成を行います。

（注）　証明書では、クライアント承認とサーバ承認の両方のキー使用が延長されている必要があります。このタイプのキー使用の延長の例については、Microsoft CA コンピュータ テンプレートを参照してください。

ステップ 4　『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1*』の説明に従って、ISE ノード（以前の Inline Posture ノード）で ISE 1.1.1 の新規インストールを実行します。

ステップ 5　スタンドアロン モードになっている ISE ノード（以前の Inline Posture ノード）で、CA ルート証明書のインポート、CSR の生成、証明書の作成を行います。

（注）　証明書では、クライアント承認とサーバ承認のキー使用が延長されている必要があります。たとえば、Microsoft CA からコンピュータ テンプレートを選択します。

ステップ 6　新しくアップグレードした ISE ノードを Inline Posture ノードとして登録します。

ステップ 7　Cisco Inline Posture ノードを再設定します。

Cisco ISE リリース 1.0.3.377 からのアップグレード

Cisco Identity Services Engine リリース バージョン 1.0.3.377 からのアップグレード後の、デフォルトの「admin」管理者ユーザ インターフェイス アクセスについての既知の問題があります。この問題は、Cisco Identity Services Engine リリース 1.0.3.377 を初めてインストールしてから、管理者ユーザ インターフェイスへのログイン用のデフォルトの「admin」アカウント パスワードを変更していない Cisco ISE の顧客に影響を与える可能性があります。

パスワードが元のデフォルト値から変更されていない場合、アップグレード時にデフォルトの「admin」アカウントからログインしようとすると、管理者は Cisco ISE 管理者ユーザ インターフェイスから「ロック アウト」される場合があります。

この問題を避けるため、Cisco は次の手順を 1 つ以上実行することを推奨します。

1. アップグレードの*前に*、『*Cisco Identity Services Engine User Guide, Release 1.1.1*』の「Managing Identities」の章の指示に従ってパスワードが変更されていることを確認します。
2. アップグレードの*前に*、管理者ユーザ インターフェイスの [管理（Administration）] > [システム（System）] > [管理アクセス（Admin Access）] > [パスワード ポリシー（Password Policy）] ページでパスワードの有効期間をディセーブル化または変更し、アップグレードされたポリシーがデフォルトの「admin」アカウントに影響を与えないようにします。
3. [管理（Administration）] > [システム（System）] > [管理アクセス（Admin Access）] > [パスワード ポリシー（Password Policy）] ページでパスワードの有効期間の通知をイネーブル化し、管理ユーザに期限切れを警告します。通知を受けた管理者はパスワードを変更する必要があります。

（注）　上記の条件はすべての管理者アカウントに適用しますが、Cisco ISE バージョン 1.0.3.377 からの動作の変更は、デフォルトの「admin」アカウントにのみ影響します。