



Cisco Identity Services Engine アップグレード ガイド リリース 1.1.1

2012 年 7 月

**【注意】シスコ製品をご使用になる前に、安全上の注意
(www.cisco.com/jp/go/safety_warning/)をご確認ください。**

**本書は、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。**

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Identity Services Engine アップグレードガイド リリース 1.1.1

© 2012 Cisco Systems, Inc.

All rights reserved.

Copyright © 2012, シスコシステムズ合同会社.

All rights reserved.



CONTENTS

はじめに v

Cisco Identity Services Engine の概要 v

目的 vi

対象読者 vi

マニュアルの構成 vii

表記法 vii

関連資料 viii

リリース固有のドキュメント viii

プラットフォーム固有のマニュアル viii

マニュアルの更新 ix

マニュアルの入手方法およびテクニカル サポート ix

CHAPTER 1

Cisco ISE のアップグレード 1-1

作業前の準備 1-2

有効なライセンスの取得 1-2

オンデマンド バックアップの実行 1-3

Cisco ISE UI からのバックアップ 1-3

Cisco ISE CLI からのバックアップ 1-4

CLI からのアプリケーション アップグレードの使用 1-5

アップグレード プロセスの検証 1-6

アップグレードに関する既知の問題 1-6

Cisco ISE 1.0.4 から Inline Posture のある 1.1.1 へのアップグレード 1-7

Cisco ISE リリース 1.0.3.377 からのアップグレード 1-8

CHAPTER 2

スタンドアロン ノードのアップグレード 2-1

Cisco ISE スタンドアロン ノードのアップグレード 2-1

リリース 1.1 を実行する Cisco ISE スタンドアロン アプライアンスとリリース 1.1.1 を実行するアプライアンスの交換 2-3

CHAPTER 3

2 Admin ノード展開のアップグレード 3-1

2 Admin ノード展開のアップグレードの実行 3-1

CHAPTER 4

分散展開のアップグレード 4-1

分散展開のアップグレードの実行 4-1

分散展開での Cisco ISE ノードのアップグレード 4-2

分散展開での、Cisco ISE リリース 1.1 を実行するアプライアンスとリリース 1.1.1 を実行するアプライアンスとの交換 4-5

分散展開での、既存の Cisco ISE 1.1 ノードのサブセットとリリース 1.1.1 を実行する Cisco ISE アプライアンスとの交換 4-5

分散展開での、リリース 1.1 を実行するすべての Cisco ISE アプライアンスとリリース 1.1.1 を実行するアプライアンスとの交換 4-6

CHAPTER 5

アップグレードの障害からの復旧 5-1

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 5-1

シナリオ 1: データベース スキーマまたはデータモデル アップグレード中のアップグレードの障害 5-1

シナリオ 2: バイナリ インストール中のアップグレードの障害 5-1

アップグレード中に SSH セッションが中断した場合のアプライアンスの復元 5-2

INDEX



はじめに

ここでは、Cisco Identity Services Engine (ISE) 3300 シリーズ アプライアンスについて、以下の情報を示します。

- 「[Cisco Identity Services Engine の概要](#)」 (P.v)
- 「[目的](#)」 (P.vi)
- 「[対象読者](#)」 (P.vi)
- 「[マニュアルの構成](#)」 (P.vii)
- 「[表記法](#)」 (P.vii)
- 「[関連資料](#)」 (P.viii)
- 「[マニュアルの更新](#)」 (P.ix)
- 「[マニュアルの入手方法およびテクニカル サポート](#)」 (P.ix)

Cisco Identity Services Engine の概要

Cisco Identity Services Engine (ISE) は、企業でのコンプライアンスの順守、インフラストラクチャのセキュリティの強化、サービス オペレーションの合理化を実現する、次世代のアイデンティティおよびアクセス コントロール ポリシーのプラットフォームです。Cisco ISE は、その独自のアーキテクチャによってネットワーク、ユーザ、デバイスからリアルタイムのコンテキスト情報を収集し、ID をアクセス スイッチ、ワイヤレス LAN コントローラ (WLC)、仮想プライベート ネットワーク (VPN) ゲートウェイ、データセンター スイッチなどの様々なネットワーク要素に結びつけることで、企業が積極的な管理上の決定を下せるようにします。

Cisco ISE は Cisco Security Group Access Solution のキー コンポーネントです。Cisco ISE は、統合されたポリシーベースのアクセス コントロール ソリューションで以下を実現します。

- 認証、承認、アカウント (AAA)、ポスチャ、プロファイラ、ゲスト管理サービスを 1 つのアプライアンスに結合します。
- 802.1X 環境を含むネットワークにアクセスしているすべてのエンドポイントのデバイス ポスチャをチェックすることでエンドポイント コンプライアンスを徹底します。
- ネットワーク上のエンドポイント デバイスの検出、プロファイリング、ポリシーベースの配置、モニタリングのサポートを提供します。
- 集中型展開および分散型展開においてポリシーの一貫性が維持され、サービスを必要な場所に配信できるようになります。
- Security Group Tags (SGT) および Security Group (SG) Access Control List (ACL) によって Security Group Access (SGA) などの高度な強化機能を使用します。

- 小さな事務所から大企業まで様々な環境の展開シナリオに対応するスケーラビリティをサポートします。

Cisco ISE ソフトウェアは、様々なパフォーマンス特性化とともに様々な物理アプライアンスをプリインストールした状態で提供されます。Cisco ISE が本来備えている拡張性によってアプライアンスを展開に追加し、必要に応じてパフォーマンスと復元力を向上させることができます。Cisco ISE のアーキテクチャは、ハイアベイラビリティ オプションを備えたスタンドアロン展開および分散展開をサポートします。Cisco ISE により、集中型ポータルからネットワークを設定および管理して効率性と使いやすさを確保できます。

さらに Cisco ISE は設定可能な独自のルールを備え、ネットワークの必要な場所に Cisco ISE サービスを作成および適用できます。その結果、フル機能を備え統合されたシステムとして動作する包括的な Cisco ISE 展開が実現します。

目的

このマニュアルは、Cisco ISE シリーズ アプライアンスおよび VMware 仮想マシン上の Cisco Identity Services Engine ソフトウェア イメージをアップグレードする方法を説明します。

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 1.1.1 に更新できます。また、Cisco Secure Access Control System (ACS) リリース 5.1 および 5.2 から最新の Cisco ISE メンテナンス リリース 1.1.1 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 リリース 5.1 および 5.2 から最新の Cisco ISE リリースへの移行の詳細については、『[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 リリースへは、Cisco Secure ACS 5.1 および 5.2 リリースからのみ移行できます。最新の Cisco ISE リリースに移行する場合は、先に Cisco Secure ACS 5.1 または 5.2 リリースにアップグレードする必要があります。

対象読者

このガイドは、Cisco ISE 3300 シリーズ アプライアンスまたは VMware サーバで Cisco ISE ソフトウェアをアップグレードおよび設定するネットワーク管理者、システム インテグレータ、ネットワーク導入担当者を対象としています。このアップグレードガイドを使用する準備として、ネットワーク設備およびケーブル接続を理解し、電気回路、配線、装置ラックの取り付けに関する基礎知識を得ておく必要があります。



警告

この装置の設置、交換、または保守は、訓練を受けた相応の資格のある人が行ってください。ステートメント 1030

マニュアルの構成

表 1 に『Cisco ISE アップグレードガイドリリース』の構成を示します。

表 1 『Cisco ISE アップグレードガイド』の構成

章/付録およびタイトル	説明
第 2 章「スタンドアロン ノードのアップグレード」	Cisco ISE スタンドアロン ノードのアップグレード方法を説明します。
第 3 章「2 Admin ノード展開のアップグレード」	Cisco ISE 2 ノード展開のアップグレード方法を説明します。
第 4 章「分散展開のアップグレード」	分散展開の Cisco ISE のアップグレード方法を説明します。
第 5 章「アップグレードの障害からの復旧」	アップグレードの障害から復旧する方法を説明します。

表記法

このマニュアルでは、次の表記法を使用して手順および情報を表示しています。

項目	表記法
手順で選択する必要があるコマンド、キーワード、特殊な用語、およびオプション	太字
ユーザが値を指定する変数、および新しい用語や重要な用語	イタリック体
表示されるセッション情報、システム情報、パス、およびファイル名	screen フォント
ユーザが入力する情報	太字の screen フォント
ユーザが入力する変数	イタリック体の screen フォント
選択する順序で並べられたメニュー項目	[オプション (Option)] > [ネットワーク設定 (Network Preferences)]



(注)

「注釈」です。役立つ情報や、このガイド以外の参照資料などを紹介しています。



注意

「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

リリース固有のドキュメント

表 2 に Cisco ISE Release で利用可能な製品マニュアルを示します。Cisco ISE の全般的な製品情報は <http://www.cisco.com/go/ise> で確認できます。エンドユーザ マニュアルは、Cisco.com の http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html から入手できます。

表 2 Cisco Identity Services Engine の製品マニュアル

ドキュメント名	参照先
『Release Notes for the Cisco Identity Services Engine, Release 1.1.1』	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
『Cisco Identity Services Engine Network Component Compatibility, Release 1.1.1』	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
『Cisco Identity Services Engine User Guide, Release 1.1.1』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
『Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Upgrade Guide, Release 1.1.1』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
『Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
『Cisco Identity Services Engine API Reference Guide, Release 1.1.x』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
『Cisco Identity Services Engine Troubleshooting Guide, Release 1.1.x』	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
『Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card』	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html

プラットフォーム固有のマニュアル

ポリシー管理ビジネス ユニットのマニュアルは www.cisco.com の次の場所で入手できます。

- 『Cisco ISE』
http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html

- 『Cisco Secure ACS』
http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
- 『Cisco NAC Appliance』
http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html
- 『Cisco NAC Profiler』
http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- 『Cisco NAC Guest Server』
http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html

マニュアルの更新

表 3 に Cisco ISE 製品リリースのマニュアルの更新情報を示します。

表 3 『Cisco Identity Services Engine アップグレード ガイド リリース 1.1.1』の更新

日付	説明
2012年7月10日	『Cisco Identity Services Engine, Release 1.1.1』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



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。

- 「[作業前の準備](#)」(P.1-2)
- 「[CLI からのアプリケーションアップグレードの使用](#)」(P.1-5)
- 「[アップグレードプロセスの検証](#)」(P.1-6)
- 「[アップグレードに関する既知の問題](#)」(P.1-6)



(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ブライ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。

- 「オンデマンドバックアップの実行」(P.1-3)
 - 「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)

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 ユーザー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。
<i>backup-name</i>	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。
<i>repository-name</i>	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。

<code>application</code>	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)。
<code>application-name</code>	アプリケーション名。255 文字までの英数字で指定します。
<code>encryption-key</code>	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。
<code>hash</code>	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。
<code>plain</code>	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。
<code>encryption-key name</code>	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が必要）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 out-of-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、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、管理者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。



CHAPTER 2

スタンドアロンノードのアップグレード

ここでは、次の内容について説明します。

- 「Cisco ISE スタンドアロンノードのアップグレード」(P.2-1)
- 「リリース 1.1 を実行する Cisco ISE スタンドアロンアプライアンスとリリース 1.1.1 を実行するアプライアンスの交換」(P.2-3)

Cisco ISE スタンドアロンノードのアップグレード

Administration、Policy Service、Monitoring のペルソナを担当するスタンドアロン Cisco ISE ノードの 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の Cisco ISE を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 ISE のアップグレード前に、管理ユーザ インターフェイスまたは CLI から、スタンドアロン ISE ノードのオンデマンドバックアップ（手動）を実行し、管理ユーザ インターフェイスから Monitoring 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詳細な実行方法については、「[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。

- 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、データモデルモジュールを内部で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) の更新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を完了するためにシステムのリロードが必要な場合、アップグレードの成功後に Cisco ISE ノードは自動的に再起動します。

スタンドアロンノードでアップグレードを成功させるための CLI トランスクリプトは次のとおりです。

```
ise-vm29/admin# application upgrade ise-appbundle-1.1.1.xxx.i386.tar.gz myrepository
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 から Cisco ISE リリース 1.1.1 へのアップグレードの後、**host-key host <sftp servername>** コマンドを使用してホストキーを受け入れるまで、**SFTP** リポジトリを使用することができます。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.x*』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 から Cisco ISE リリース 1.1.1 へのアップグレードの後、古いジョブは適切に機能しないため、スケジュール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。



- (注)** 次の **ステップ 4** は Cisco ISE リリース 1.0.3.377 から新しいリリースへのアップグレードを実行している場合にのみ適用されます。それ以外の場合にはこの手順は無視することができます。

- ステップ 4** リポート プロセスの完了後、ログイン資格情報によるログインが指示され、すぐに Cisco ISE 内部データベース管理者パスワードおよびユーザパスワードを入力するように求められます。(このプロセスは、ログインに使用しているユーザ アカウントに管理者レベルのアクセス権限がある場合にのみ成功します)。

```
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 バンドルの前のバージョンを削除または再インストールしてバックアップから復元を行うしかありません。

アップグレードの障害から復旧する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の障害からの復旧](#)」(P.5-1) を参照してください。



(注) Cisco ISE リリース 1.0.3.377、Cisco ISE メンテナンス リリース 1.0.4.573 または Cisco ISE リリース 1.1 から Cisco ISE リリース 1.1.1 へのアップグレードの後、古いジョブは適切に機能しないため、スケジュール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。

リリース 1.1 を実行する Cisco ISE スタンドアロン アプライアンスとリリース 1.1.1 を実行するアプライアンスの交換

このアップグレードシナリオは、既存の Cisco ISE シャーシの交換と同時に、Cisco ISE リリース 1.0、Cisco ISE メンテナンス リリース 1.0.4 または Cisco ISE リリース 1.1 ソフトウェアを Cisco ISE リリース 1.1.1 にアップグレードす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は、バックアップからの復元ではなく [CLI からのアプリケーションアップグレードの使用](#)を使用することを推奨します。

Cisco ISE 1.1 を実行する Cisco ISE スタンドアロン アプライアンスと Cisco ISE リリース 1.1.1 を実行する Cisco ISE アプライアンスを交換するには、次の手順を実行します。

- ステップ 1** Cisco ISE 1.1 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 1.1.1 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 1.1 のバックアップを復元します。



(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場合、古い機能も新しい機能も関係なく、既存の設定はすべて復元後に消去されます。

バックアップと復元の実行方法の詳細については、『[Cisco Identity Services Engine User Guide, Release 1.1.1](#)』の 14 章、「Backing Up and Restoring Cisco ISE Data」を参照してください。

データの復元後は、すべてのアプリケーション サーバ プロセスが作動するまで待機する必要があります。

Cisco ISE アプリケーション サーバ プロセスの起動を確認するには、Cisco ISE CLI 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 1.1.x](#)』を参照してください。



CHAPTER 3

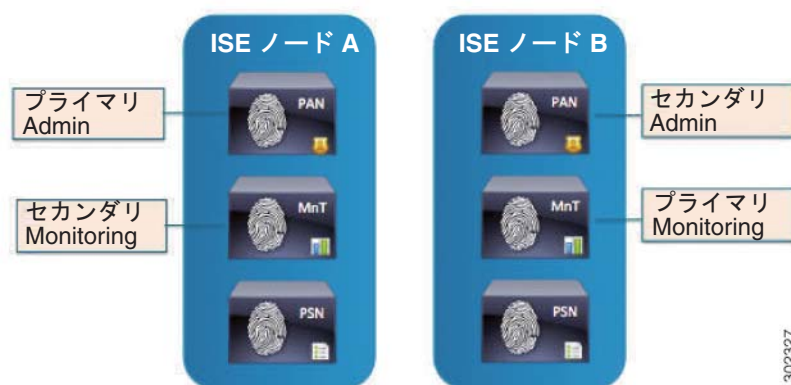
2 Admin ノード展開のアップグレード

2 Admin ノード展開のアップグレードの実行

上位のリリースにアップグレードする場合は、先にセカンダリ Administration ISE ノードのみを上位の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、[図 3-1](#) に示すようなプライマリ Administration ノード（ノード A）1 つとセカンダリ管理ノード（ノード B）1 つを備えた展開セットアップの場合、次のアップグレード手順に進むことができます。

図 3-1 Cisco ISE リリース 1.1.2 ノード管理展開



Cisco ISE リリース 1.0 または 1.1 から Cisco ISE リリース 1.1.1 への分割ドメインのみのアップグレードをサポートするため、アップグレード前には展開からセカンダリ ISE ノードを個別に登録解除する必要があります。



警告

この警告は、Cisco ISE リリース 1.1 パッチ 3 からのアップグレードを行う場合には当てはまりません。

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。

2 Admin ノード展開を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 ISE リリース 1.1.1 へのアップグレード前に、管理ユーザ インターフェイスまたは CLI から、プライマリ Administration ISE ノードのオンデマンド バックアップ（手動）を実行し、管理ユーザ インターフェイスから Monitoring 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 バックアップの詳細な実行方法については、「[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。
- ステップ 2** 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。登録解除後、このノードはスタンドアロン 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 1.1.1 にアップグレードします。
- アップグレード後にノード B にログインする際にシステムがライセンスについてのプロンプトを表示する場合、UDI に基づくセカンダリ ノード用の有効なライセンスをインストール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。
- 登録解除後、以前の展開のプライマリ ノード（ノード A）もスタンドアロン ノードになります。
- ステップ 3** ノード B を新しい展開のプライマリ ノードに設定します。
- ステップ 4** ノード A を Cisco ISE リリース 1.1.1 にアップグレードし、Cisco ISE リリース 1.1.1 展開セットアップでセカンダリ ノードとしてノード B に登録します。
- 展開のアップグレード後、以前の展開のすべてのポリシーとその他のデータは新しい展開で維持されます。



CHAPTER 4

分散展開のアップグレード

この章は、次の内容で構成されています。

- 「分散展開のアップグレードの実行」(P.4-1)
- 「分散展開での、Cisco ISE リリース 1.1 を実行するアプライアンスとリリース 1.1.1 を実行するアプライアンスとの交換」(P.4-5)

分散展開のアップグレードの実行

分散展開で Cisco ISE ノードのリリース 1.1.1 へのアップグレードを実行するには、分割展開のアップグレード方法を使用する必要があります。

プライマリ Administration ISE ノード データベースに対する設定の変更は、セカンダリ管理 ISE ノード、Inline Posture 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、すべてのノードでプライマリ Administration ISE ノードからデータベースを複製し、各ノードに設定のローカル コピーを作成することができます。すべてのノードにまたがる設定データの複製は、最新バージョンで実装された機能変更の点では複雑化し、設定が必要となる場合があります。

分散展開における Cisco ISE ノードの一元的な設定と管理についての詳細は、『[Cisco Identity Services Engine User Guide, Release 1.1.1](#)』の 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場合、ドメイン ネーム システム (DNS) サーバのリゾリューションが必須になります。実施しなかった場合はアップグレードは失敗します。



(注) 分割展開のアップグレード中、ノードを新しいプライマリ Administration ノードに登録する前に次を実行する必要があります。

- 自己署名証明書を使用している場合、すべてのノードの自己署名証明書を新しいプライマリ Administration ノードにインポートする必要があります。
- ノードごとに異なる CA 証明書を使用している場合、すべての CA 証明書を新しいプライマリ Administration ノードにインポートする必要があります。
- 各ノードで共通の CA 証明書を使用している場合、そのノードを新しいプライマリ Administration ノードにインポートする必要があります。

完全な Cisco ISE 展開を新しいリリースにアップグレードする場合、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。

分割展開のアップグレードは 2 つの段階で実施されます。

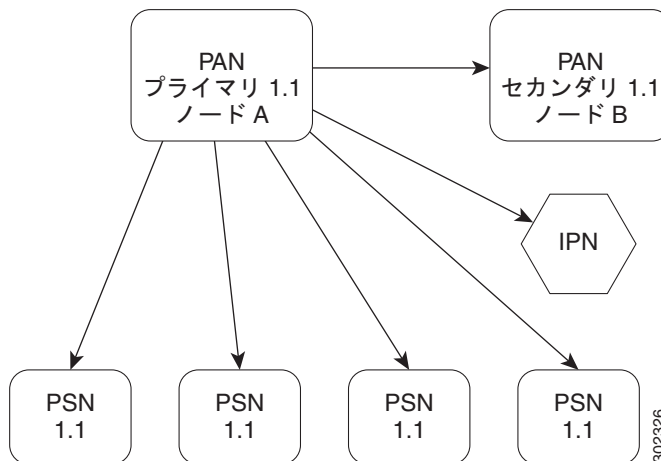
1. 分散展開の Cisco ISE Administration ノードをアップグレードします。
2. Policy Service ノードと Inline Posture ノードを新しい展開にアップグレードします。

分散展開での Cisco ISE ノードのアップグレード

上位のリリースにアップグレードする場合は、先にセカンダリ Administration ISE ノードのみを上位の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、図 4-1 に示すようなプライマリ Administration ノード 1 つ (ノード A)、セカンダリ Administration ノード 1 つ (ノード B)、Inline Posture ノード (IPN) 1 つ (ノード C)、Policy Service ノード (PSN) 4 つ (ノード D、ノード E、ノード F、ノード G) の展開セットアップの場合、次のアップグレード手順に進むことができます。

図 4-1 Cisco ISE リリース 1.1 管理展開



Cisco ISE では、以前のリリースから Cisco ISE リリース 1.1.1 への分割ドメインアップグレードのみをサポートします。そのため、セカンダリ ISE ノードと Inline Posture ノードはアップグレード前に展開から個別に登録解除しておく必要があります。



警告

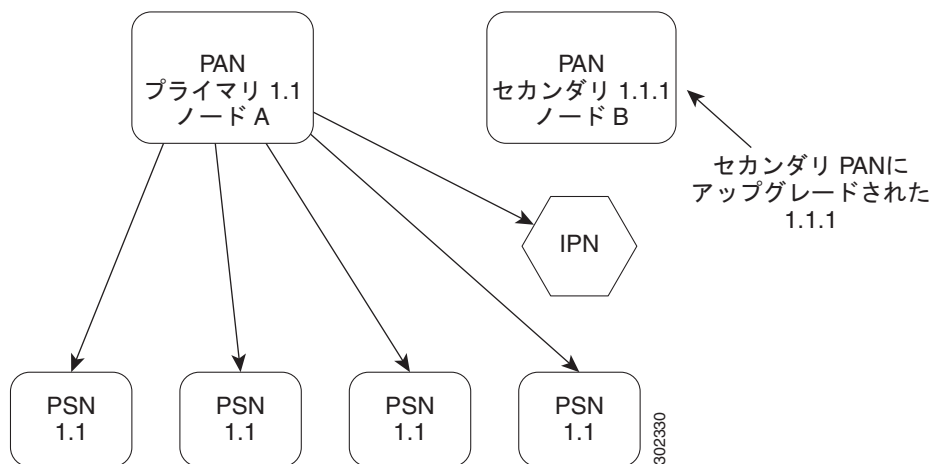
この警告は、Cisco ISE リリース 1.1 パッチ 3 からのアップグレードを行う場合には当てはまりません。

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。

分散展開を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 ISE のアップグレード前に、管理ユーザ インターフェイスまたは CLI から、プライマリ Administration ISE ノードのオンデマンド バックアップ（手動）を実行し、管理ユーザ インターフェイスから Monitoring 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 バックアップの詳細な実行方法については、「[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。
- ステップ 2** アップグレード前に Inline Posture ノード (IPN) 設定を記録し、アップグレード後に IPN ノードを再設定できるようにします。
- ステップ 3** 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。登録解除後、このノードはスタンドアロン 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 1.1.1 にアップグレードします。[図 4-2](#)を参照してください。

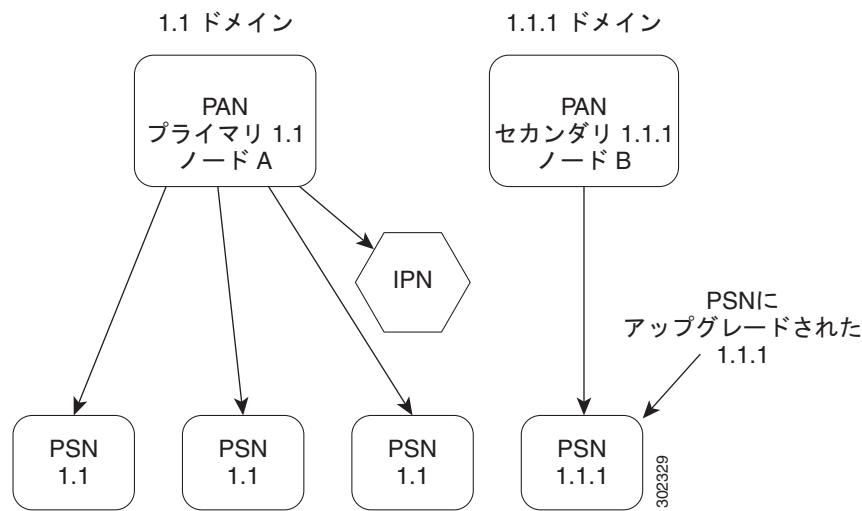
図 4-2 Cisco ISE セカンダリ ノードのアップグレード



アップグレード後にノード B にログインする際にシステムがライセンスについてのプロンプトを表示する場合、UDI に基づくセカンダリ ノード用の有効なライセンスをインストール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。

- ステップ 4** 展開セットアップから PSN ノード (ノード D) を登録解除します。登録解除後、このノードはスタンドアロン 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 1.1.1 にアップグレードします。[図 4-3](#)を参照してください。

図 4-3 新しい展開にアップグレードされた Policy Service ノード



ステップ 5 ノード B を新しい展開のプライマリ ノードとして昇格し、ノード D を PSN ノードとして登録します。

ステップ 6 展開セットアップから IPN ノード (ノード C) を登録解除し、スタンドアロン ノードとします。この IPN ノードを Cisco ISE リリース 1.1.1 にアップグレードします。



(注) アップグレードプロセスは IPN の設定を削除します。アップグレード後に IPN を再設定する必要があります。

ステップ 7 展開からセカンド PSN ノード (ノード E) を登録解除し、Cisco ISE リリース 1.1.1 にアップグレードします。このノードを PSN ノードとしてノード B に登録します。他の PSN ノード (ノード F および ノード G) に対してこの手順を繰り返します。

ステップ 8 以前の展開のプライマリ ノード (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 1.1.1 にアップグレードし、Cisco ISE リリース 1.1.1 展開セットアップでセカンダリ ノードとしてノード B に登録します。

ステップ 9 IPN 証明書を新しいプライマリ Administration ノード (ノード B) の証明書と交換します。同様に、IPN 証明書を新しいセカンダリ Administration ノード (ノード A) の証明書と交換します。

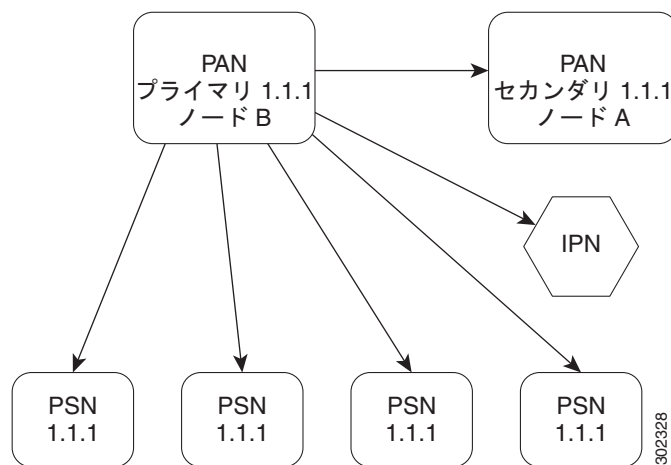


(注) プライマリおよびセカンダリの Administration ノードの証明書を各 IPN ノードにインストールして、管理インターフェイスの証明書を信頼済みとする必要があります。証明書のプロビジョニングの詳細については、『Cisco Identity Services Engine User Guide, Release 1.1.1』の「Deploying an Inline Posture Node」を参照してください。

ステップ 10 IPN ノード (ノード C) を新しい展開セットアップ (ノード B) に登録します。

すべての Policy Service ノードを新しい展開へとアップグレードすると、Cisco ISE 展開のアップグレードは完了となります (図 4-4 を参照)。

図 4-4 新しい Cisco ISE リリースへの移行が完了した展開



302328

分散展開での、Cisco ISE リリース 1.1 を実行するアプライアンスとリリース 1.1.1 を実行するアプライアンスとの交換

この項の構成は、次のとおりです。

- 「分散展開での、既存の Cisco ISE 1.1 ノードのサブセットとリリース 1.1.1 を実行する Cisco ISE アプライアンスとの交換」 (P.4-5)
- 「分散展開での、リリース 1.1 を実行するすべての Cisco ISE アプライアンスとリリース 1.1.1 を実行するアプライアンスとの交換」 (P.4-6)

分散展開での、既存の Cisco ISE 1.1 ノードのサブセットとリリース 1.1.1 を実行する Cisco ISE アプライアンスとの交換

分散展開で Cisco ISE 1.1 ノードのサブセットを 1.1.1 を実行する Cisco ISE アプライアンスと交換するには、次の手順を実行します。

- ステップ 1** 既存のセカンダリ Cisco ISE 1.1 アプライアンスを登録解除し、Cisco ISE 1.1.1 にアップグレードします。このアプライアンスを新しい展開のプライマリ ノードに設定します。
- ステップ 2** 新しい展開に移動する古い展開のその他のノードを登録解除し、アップグレードして新しい展開に登録します。
- ステップ 3** 新しい Cisco ISE 1.1.1 アプライアンスを新しい展開に登録します。
この場合、プライマリ Administration ISE ノードは元のハードウェアに維持されます。
- ステップ 4** 新しい Cisco ISE 1.1.1 アプライアンスの 1 つを新しいプライマリ Administration ISE ノードに設定します。

分散展開での、リリース 1.1 を実行するすべての Cisco ISE アプライアンスとリリース 1.1.1 を実行するアプライアンスとの交換

分散展開で Cisco ISE メンテナンス リリース 1.0.4 または Cisco ISE リリース 1.1 ソフトウェアを実行するすべての Cisco ISE アプライアンスと Cisco ISE リリース 1.1.1 を実行する Cisco ISE アプライアンスを交換するには、次の手順を実行します。

-
- ステップ 1** 既存のセカンダリ Cisco ISE 1.1 アプライアンスを登録解除し、Cisco ISE 1.1.1 にアップグレードします。このアプライアンスを新しい展開のプライマリ ノードに設定します。
 - ステップ 2** 新しい Cisco ISE 1.1.1 アプライアンスを新しい展開に登録します。
 - ステップ 3** すべての新しい Cisco ISE 1.1.1 アプライアンスが新しい展開に登録された後、新しい Cisco ISE 1.1.1 アプライアンスの 1 つを新しい展開のプライマリ ノードに昇格させます。
 - ステップ 4** 手順 1 でプライマリ ノードとして昇格された古いアプライアンスを登録解除します。
-



CHAPTER 5

アップグレードの障害からの復旧

この章は、次の内容で構成されています。

- 「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)
- 「アップグレード中に SSH セッションが中断した場合のアプライアンスの復元」(P.5-2)

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

アップグレードが失敗した場合にロールバックや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 リポジトリに保存する必要があります。

シナリオ 1：データベース スキーマまたはデータモデル アップグレード中のアップグレードの障害

検出内容：コンソールおよび ADE.log に次のいずれかのメッセージが表示されている。

- ISE データ スキーマのアップグレードが失敗しました (ISE Database schema upgrade failed!)
- ISE グローバル データのアップグレードが失敗しました (ISE Global data upgrade failed!)
- ノード固有データの ISE データのアップグレードが失敗しました (ISE data upgrade for node specific data failed!)

ロールバック方法：最後のバックアップから復元してロールバックします。

アップグレードの再試行方法：

- ログを分析します。
- 問題を特定し解決するためには、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には、毎回新しいアプリケーション バンドルが必要です。

シナリオ 2：バイナリ インストール中のアップグレードの障害

検出内容：アプリケーション バイナリのアップグレードはデータベースのアップグレード後に発生する。バイナリのアップグレードで障害が発生すると、コンソールと ADE.log に次のメッセージが表示されます。

% システムでアプリケーションのインストール/アップグレードが失敗しました。破損したインストールを削除します (% 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 アプライアンスを再イメージし、バックアップから復元します。

アップグレードの再試行方法 :

- ログを分析します。
- 問題を特定し解決するためには、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には、毎回新しいアプリケーションバンドルが必要です。

アップグレード中に SSH セッションが中断した場合のアプライアンスの復元

検出内容 : SSH セッションまたはコンソールがアップグレード中に切断または中断される。

ロールバック方法 : 以前の ISO イメージを使用して Cisco ISE アプライアンスを再イメージし、バックアップから復元します。

アップグレードの再試行方法 : アップグレードを再度実行します。新しい Cisco ISE リリース 1.1.1 でアプライアンスがセカンダリ ノードとして使用されている場合、新しい ISO バージョンを直接インストールして新しいプライマリ Administration ISE ノードとして登録します。



INDEX

数字

2 ノードのアップグレード [3-2](#)

あ

アプリケーションのアップグレード [1-5](#)

こ

交換

分散展開のサブセット [4-5](#)

コマンド

アプリケーションのアップグレード [1-6](#)

す

スタンドアロンのアップグレード [2-1](#)

ふ

復旧

アップグレード中に SSH セッションが中断した場合
のアプライアンス [5-2](#)

データベース スキーマ中のアップグレードの障
害 [5-1](#)

バイナリ インストール中のアップグレードの障
害 [5-1](#)

分割展開のアップグレード [4-1](#)

分散展開のアップグレード [4-2](#)

