Cisco Identity Services Engine リリース 1.1 ハードウェア インストレーション ガイド

2012 年 5 月

Text Part Number: OL-25540-01-J

【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。

FCC クラス A 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 準拠装置に関する記述：このマニュアルに記載された装置は、無線周波エネルギーを生成および放射する可能性があります。シスコの指示する設置手順に従わずに装置を設置した場合、ラジオおよびテレビの受信障害が起こることがあります。この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。これらの仕様は、住宅地で使用したときに、このような干渉を防止する適切な保護を規定したものです。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。

シスコの書面による許可なしに装置を改造すると、装置がクラス A またはクラス B のデジタル装置に対する FCC 要件に準拠しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で矯正するように求められることがあります。

装置の電源を切ることによって、この装置が干渉の原因であるかどうかを判断できます。干渉がなくなれば、シスコの装置またはその周辺機器が干渉の原因になっていると考えられます。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。

- 干渉がなくなるまで、テレビまたはラジオのアンテナの向きを変えます。
- テレビまたはラジオの左右どちらかの側に装置を移動させます。
- テレビまたはラジオから離れたところに装置を移動させます。
- テレビまたはラジオとは別の回路にあるコンセントに装置を接続します （装置とテレビまたはラジオがそれぞれ別個のブレーカーまたはヒューズで制御されるようにします）。

シスコでは、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

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 Identity Services Engine リリース 1.1 ハードウェア インストレーション ガイド

CONTENTS

はじめに

この章では、Cisco Identity Services Engine（ISE）3300 シリーズ アプライアンスに関する次の情報を提供します。

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、およびサービス運用の合理化を実現する次世代 ID およびアクセス コントロール ポリシー プラットフォームです。Cisco ISE の固有のアーキテクチャにより、企業はリアルタイム状況情報をネットワーク、ユーザ、およびデバイスから収集し、アクセス スイッチ、ワイヤレス LAN コントローラ（WLC）、バーチャル 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 スイッチなどのさまざまなネットワーク要素に ID を関連付けることにより、ガバナンスに関する決定を事前に行うことができます。

Cisco ISE は、Cisco Security Group Access Solution の主要なコンポーネントです。Cisco ISE は、次のことを行う統合ポリシーベース アクセス コントロール ソリューションです。

- 認証、許可、アカウンティング（AAA）、ポスチャ、プロファイラ、およびゲスト管理サービスを 1 つのアプライアンスに統合します。
- 802.1X 環境を含むネットワークにアクセスするすべてのエンドポイントのデバイス ポスチャを確認して、エンドポイントのコンプライアンスを順守します。
- ネットワーク上のエンドポイント デバイスの検索、プロファイリング、ポリシーベース配置、および監視をサポートします。
- 一元化された展開と分散された展開で一貫したポリシーを実現し、必要な場所にサービスを提供できるようにします。

- セキュリティ グループ タグ（SGT）とセキュリティ グループ（SG）アクセス コントロール リスト（ACL）を使用して、セキュリティ グループ アクセス（SGA）を含む高度な順守機能を提供します。
- 小規模なオフィスから大規模な企業の環境まで、複数の展開シナリオをサポートするスケーラビリティを提供します。

Cisco ISE ソフトウェアは、さまざまなパフォーマンス特性を持つ広範な物理アプライアンスに事前にインストールされています。Cisco ISE が本来備えているスケーラビリティによって、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 アーキテクチャは、スタンドアロン展開と分散展開をハイ アベイラビリティ オプションとともにサポートします。Cisco ISE では、一元化されたポータルからネットワークを設定および管理でき、効率性と使いやすさが実現されます。

また、Cisco ISE には設定可能である特徴的なロールとサービスが組み込まれているため、ネットワークで必要な場所に、Cisco ISE サービスを作成および適用できます。結果として、全機能を備えた統合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

このインストール マニュアルでは、Cisco ISE リリース 1.1 に関する次のような情報が提供されます。

- インストールの前提条件
- サポートされる Cisco ISE アプライアンスへの Cisco ISE ソフトウェアのインストール手順
- サポートされる VMware 仮想マシンへの Cisco ISE ソフトウェアのインストール手順
- サポートされるシスコ ネットワーク アドミッション コントロール（NAC）アプライアンスまたは Cisco Secure Access Control System（ACS）アプライアンスへの Cisco ISE ソフトウェアのインストール手順

Cisco ISE リリース 1.1 では、展開のサイズに応じて、次の 3 つのアプライアンス プラットフォームが提供されます。

- 小規模ネットワーク：Cisco ISE 3315
- 中規模ネットワーク：Cisco ISE 3355
- 大規模ネットワーク ：Cisco ISE 3395

Cisco ISE ソフトウェアは、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）で稼働します。Cisco ADE-OS と Cisco ISE ソフトウェアは、専用 Cisco ISE 3300 シリーズ アプライアンスまたは VMware サーバ（Cisco ISE VM）のいずれかで実行します。

VMware ベースのインストールの場合は、VMware 環境がシステムの特定の最小要件を満たすよう設定し、Cisco ISE リリース 1.1 ソフトウェアをインストールします。サポートされる VMware バージョンは次のとおりです。

- VMware Elastic Sky X（ESX）バージョン 4.0、4.0.1、および 4.1
- VMware ESXi バージョン 4.0、4.0.1、および 4.1

（注） VMware ベースのインストールの詳細については、第 4 章「VMware 仮想マシンにおける Cisco ISE 3300 シリーズ ソフトウェアのインストール」を参照してください。

（注） VMware サーバ（バージョン 2.0）は、Cisco ISE リリース 1.1 の機能をデモするためにのみサポートされ、実稼働環境向けにはサポートされていません。

対象読者

このマニュアルは、Cisco ISE ソフトウェアを Cisco ISE 3300 シリーズ アプライアンスまたは VMware サーバにインストールし、設定するネットワーク管理者、システム インテグレータ、またはネットワーク展開担当者を対象としています。このハードウェア インストール マニュアルを使用する前提条件として、ネットワーク装置やケーブル配線に精通し、電気回路、電気配線方法、および装置ラックの取り付けについて基本的な知識を持っている必要があります。

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 ハードウェア インストレーション ガイド リリース 1.1*』の構成を示します。

表 1 Cisco ISE ハードウェア インストレーション ガイドの構成

章または付録とタイトル	説明
第 1 章「Cisco ISE ネットワーク展開について」	Cisco ISE 3300 シリーズ アプライアンス展開およびそのコンポーネントの概要を紹介します。新しい Cisco ISE 3300 シリーズ展開を計画する前に、この章をお読みください。
第 2 章「Cisco ISE 3300 シリーズ ハードウェアについて」	Cisco ISE 3300 シリーズ ハードウェアの概要を紹介します。
第 3 章「Cisco ISE 3300 シリーズ アプライアンスの設定」	Cisco ISE 3300 シリーズ ハードウェアへの Cisco ISE ソフトウェアの初期インストールを実行する方法について説明します。
第 4 章「VMware 仮想マシンにおける Cisco ISE 3300 シリーズ ソフトウェアのインストール」	VMware ESX または ESXi 仮想マシンに Cisco ISE ソフトウェアをインストールする方法について説明します。
第 5 章「Cisco ISE のアップグレード」	Cisco ISE ソフトウェアおよびアプライアンスをアップグレードする方法について説明します。
第 6 章「インストール後のタスクの実行」	Cisco ISE 3300 シリーズ ライセンスのインストールに関する情報を提供し、次のインストールを実行するために必要な設定タスクを示します。
付録 A「Cisco ISE 3300 シリーズ ハードウェアの設置準備」	必要な安全手順、設置場所の要件、および Cisco ISE 3300 シリーズ ハードウェアをインストールする前に実行する必要があるタスクについて説明します。
付録 B「Cisco ISE 3300 シリーズ ハードウェアの設置」	Cisco ISE 3300 シリーズ アプライアンスのラック取り付けの実行、すべてのケーブルの接続、アプライアンスの電源投入、およびアプライアンスの取り外しまたは交換に関する詳細な手順について説明します。
付録 C「Cisco ISE 3300 シリーズ アプライアンスのトラブルシューティング」	Cisco ISE 3300 シリーズ アプライアンスの初回起動をトラブルシューティングする方法について説明します。

表 1　Cisco ISE ハードウェア インストレーション ガイドの構成 （続き）

章または付録とタイトル	説明
付録 D「Cisco ISE 3300 シリーズ アプライアンスの保守」	インストール後に Cisco ISE 3300 シリーズ アプライアンスを保守する場合の推奨事項について説明します。
付録 E「Cisco ISE 3300 シリーズ アプライアンスのポート リファレンス」	Cisco ISE 3300 シリーズ アプライアンス サービス、アプリケーション、およびデバイスによって使用されるポートのリファレンス リストを提供します。
付録 F「Cisco NAC および Cisco Secure ACS アプライアンス上の Cisco ISE 3300 シリーズ ソフトウェアのインストール」	サポートされる Cisco NAC アプライアンスまたは Cisco Secure ACS アプライアンスに Cisco ISE ソフトウェアをインストールする方法について説明します。

インストール参考資料

表 2 に、Cisco ISE 3300 シリーズ リリース 1.1 ソフトウェアをインストールする前に参照すると役に立つと思われる参考資料を示します。各インストール プロセスについては、対応する章、付録、またはマニュアルを参照してください。

表 2　Cisco ISE 3300 シリーズ インストール シナリオ

インストール プロセス	参考資料
Cisco ISE アプライアンスおよび事前展開の要件について	1. 第 2 章「Cisco ISE 3300 シリーズ ハードウェアについて」 2. 付録 A「Cisco ISE 3300 シリーズ ハードウェアの設置準備」
初期 Cisco ISE アプライアンスのインストールと Cisco ISE ソフトウェアの設定	1. 付録 B「Cisco ISE 3300 シリーズ ハードウェアの設置」 2. 第 3 章「Cisco ISE 3300 シリーズ アプライアンスの設定」
VMware サーバへの初期 Cisco ISE ソフトウェアのインストール	1. 第 4 章「VMware 仮想マシンにおける Cisco ISE 3300 シリーズ ソフトウェアのインストール」
ログインする Web インターフェイスのライセンス取得と使用	1. 第 6 章「インストール後のタスクの実行」
Cisco NAC アプライアンスまたは Cisco Secure ACS アプライアンスへの Cisco ISE ソフトウェアのインストール	1. 付録 F「Cisco NAC および Cisco Secure ACS アプライアンス上の Cisco ISE 3300 シリーズ ソフトウェアのインストール」

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**フォント
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*フォント
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**

項目	表記法
ユーザが入力する変数	*イタリック体の* `screen` フォント
選択するメニュー項目を、選択する順序で示します。	[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、このマニュアル以外の参考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

リリース固有ドキュメント

表 3 に、Cisco ISE リリースで利用可能な製品ドキュメントを示します。Cisco ISE の一般的な製品情報は、http://www.cisco.com/go/ise で入手できます。エンドユーザ ドキュメントは、Cisco.com で入手できます（http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html）。

表 3　Cisco Identity Services Engine（ISE）の製品ドキュメント

ドキュメント名	場所
『Release Notes for the Cisco Identity Services Engine, Release 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』	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
『Cisco Identity Services Engine User Guide, Release 1.1』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
『Cisco Identity Services Engine リリース 1.1 ハードウェア インストレーション ガイド』	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』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
『Cisco Identity Services Engine CLI Reference Guide, Release 1.1』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
『Cisco Identity Services Engine API Reference Guide, Release 1.1』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
『Cisco Identity Services Engine Troubleshooting Guide, Release 1.1』	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html

表 3　Cisco Identity Services Engine（ISE）の製品ドキュメント （続き）

ドキュメント名	場所
『*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ドキュメント

Policy Management Business Unit ドキュメントへのリンクは、www.cisco.com の次の場所で利用可能です。

- 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 アプライアンス
  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 ゲスト サーバ
  http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html

マニュアルの更新

表 4 に、この Cisco ISE 製品リリース向けマニュアルの更新の一覧を示します。

表 4　Cisco Identity Services Engine リリース 1.1 ハードウェア インストレーション ガイドの更新

日付	説明
2012 年 4 月 20 日	CSCtz41716 の解決
2012 年 4 月 19 日	CSCtz41736 の解決
2012 年 4 月 6 日	CSCtz11001 の解決
2012 年 4 月 3 日	CSCty98730 の解決
2012 年 3 月 19 日	『Cisco Identity Services Engine リリース 1.1 ハードウェア インストレーション ガイド』

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、およびその他の有用な情報については、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 ネットワーク展開について

この章では、Cisco Identity Services Engine (ISE) 3300 シリーズ アプライアンスとその関連コンポーネントを展開する方法、複数のネットワーク展開シナリオ、および Cisco ISE をサポートするのに必要なスイッチ設定について説明します。この章は、次の内容で構成されています。

Cisco ISE を展開する前に

この項では、Cisco ISE アプライアンスをネットワーク環境に展開する前に必要なことを理解するのに役立つ次の情報を提供します。

ノード タイプ、ペルソナ、ロール、およびサービスについて

Cisco ISE は、スタンドアロン展開と分散展開の両方をサポートする、ハイ アベイラビリティを備えたスケーラブルなアーキテクチャを提供します。分散環境では、1 つのプライマリ管理 ISE ノードを設定し、残りはセカンダリ ノードになります。この項のトピックでは、Cisco ISE の用語、サポートされるノード タイプ、分散展開、および基本的なアーキテクチャに関する情報を提供します。

Cisco ISE 展開の用語

表 1-1 で、Cisco ISE 展開シナリオで使用される一般的な用語の一部について説明します。

表 1-1　Cisco ISE 展開の用語

用語	説明
サービス	サービスは、ネットワーク アクセス、プロファイラ、ポスチャ、セキュリティ グループ アクセス、監視などの、ペルソナが提供する固有の機能です。
ノード	ノードは、Cisco ISE ソフトウェアを実行する個別インスタンスです。Cisco ISE はアプライアンスとして使用でき、VMware サーバで実行できるソフトウェアとしても使用できます。Cisco ISE ソフトウェアを実行する各インスタンス（Cisco ISE アプライアンスまたは VMware サーバのいずれかで実行されます）はノードと呼ばれます。
ノード タイプ	ノードには、ISE ノードとインライン ポスチャ ノードの 2 つの種類があります。ノード タイプとペルソナによって、そのノードにより提供される機能の種類が決まります。
ペルソナ	ノードのペルソナによって、ノードにより提供されるサービスが決まります。ISE ノードは、管理、ポリシー サービス、および監視のペルソナのいずれかまたはすべてを担当することができます。
ロール	ノードがスタンドアロンであるか、プライマリ ノードであるか、またはセカンダリ ノードであるかを決定します。管理 ISE ノードと監視 ISE ノードにのみ適用されます。
ノード グループ	ロード バランサの背後にある、要求を均等に分散する複数のポリシー サービス ISE ノード。ノード障害を検出し、障害が発生したノードで保留状態のセッションをリセットするために、2 つ以上のポリシー サービス ISE ノードを同じノード グループに配置できます。

ノードの種類

Cisco ISE ネットワークには、次の 2 つの種類のノードしかありません。

- ISE ノード：ISE ノードは、次の 3 つのペルソナのいずれかを担当することができます。
  - 管理：ISE ですべての管理操作を実行できます。システム関連のすべての設定と、認証、許可、監査などの機能に関連する設定を処理します。分散環境では、1 つのノードのみ、または最大 2 つのノードで管理ペルソナを実行できます。管理ペルソナは、スタンドアロン、プライマリ、またはセカンダリのロールのいずれかを担うことができます。プライマリ管理 ISE ノードがダウンした場合は、セカンダリ管理 ISE ノードを手動で昇格する必要があります。管理ペルソナには自動フェールオーバーがありません。

（注）　分散セットアップでは、少なくとも 1 つのノードが管理ペルソナを担当する必要があります。

  - ポリシー サービス：ネットワーク アクセス、ポスチャ、ゲスト アクセス、クライアント プロビジョニング、およびプロファイリング サービスを提供します。このペルソナはポリシーを評価し、すべての決定を行います。複数のノードがこのペルソナを担うことができます。通常は、分散展開に複数のポリシー サービス ペルソナが存在します。ロード バランサの背後にあるすべてのポリシー サービス ISE ノードは、マルチキャスト アドレスを共有し、1 つのノー

ド グループを形成するようグループ化できます。ノード グループのいずれかのノードで障害が発生した場合に、その他のノードは障害を検出し、保留中のすべてのセッションをリセットします。

（注）　分散セットアップでは、少なくとも 1 つのノードがポリシー サービス ペルソナを担当する必要があります。

- 監視 : ISE はログ コレクタとして機能し、環境内の ISE ノード上にあるすべての管理ペルソナとポリシー サービス ペルソナからのログ メッセージを格納します。このペルソナは、ネットワークとリソースを効果的に管理するために使用できる高度な監視およびトラブルシューティング ツールを提供します。

このペルソナのノードは、収集するデータを集約して関連付けて、意味のある情報をレポートの形で提供します。Cisco ISE では、プライマリ ロールまたはセカンダリ ロールを担うことができるこのペルソナを持つノードを最大 2 つ使用してハイ アベイラビリティを実現できます。プライマリ監視ペルソナおよびセカンダリ監視ペルソナの両方は、ログ メッセージを収集します。プライマリ監視ペルソナがダウンした場合は、セカンダリ監視ペルソナがプライマリ監視ペルソナのロールを自動的に担当します。

（注）　分散セットアップでは、少なくとも 1 つのノードが監視ペルソナを担当する必要があります。

- インライン ポスチャ ノード : ネットワーク上のワイヤレス LAN コントローラ（WLC）やバーチャル プライベート ネットワーク（VPN）コンセントレータなどのネットワーク アクセス デバイスの背後にあるゲートキーパー ノード。インライン ポスチャにより、ユーザが認証され、アクセス権が与えられた後にアクセス ポリシーが適用され、WLC または VPN が処理できない認可変更（CoA）要求が処理されます。Cisco ISE では、1 つの展開で 10,000 のインライン ポスチャ ノードを使用できます。2 つのインライン ポスチャ ノードをフェールオーバーのペアとして設定し、ハイ アベイラビリティを実現できます。

（注）　インライン ポスチャ ノードはそのサービス専用となり、他の ISE サービスを同時に稼働できません。同様に、そのサービスの特性のため、インライン ポスチャ ノードはどのペルソナも担当することができません。インライン ポスチャ ノードは、VMware サーバ システムでサポートされません。

（注）　展開の各 ISE ノードは、一度に 3 つのペルソナ（管理、ポリシー サービス、または監視）の内 1 つ以上のペルソナを担当することができます。対照的に、各インライン ポスチャ ノードは、1 つの専用ゲートキーパー ロールでのみ稼働します。

分散展開では、ネットワーク上で次の組み合わせのノードを使用できます。

- プライマリ管理 ISE ノードとセカンダリ管理 ISE ノード
- プライマリ監視 ISE ノードとセカンダリ監視 ISE ノード
- 1 つまたは複数のポリシー サービス ISE ノード
- 1 つまたは複数のインライン ポスチャ ノード

分散展開について

ISE 分散展開は、1 つのプライマリ管理 ISE ノードと複数のセカンダリ ノードから構成されます。展開の各 ISE ノードは、管理、ポリシー サービス、および監視のペルソナのいずれかを担当することができます。

（注）　インライン ポスチャ ノードは、その特性のため、他のいずれのペルソナも担当することができません。インライン ポスチャ ノードは、専用ノードである必要があります。インライン ポスチャ ノードは、VMware サーバ システムでサポートされません。詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』を参照してください。

このマニュアルで説明されているように ISE をすべてのノードにインストールした後に、ノードはスタンドアロン状態で稼働します。次に、1 つのノードをプライマリ管理 ISE ノードとして定義する必要があります。プライマリ管理 ISE ノードの定義後に、そのノードでポリシー サービスや監視などの他のペルソナを設定できます。プライマリ管理 ISE ノードでペルソナを定義したら、プライマリ管理 ISE ノードで他のセカンダリ ノードを登録し、そのセカンダリ ノードにペルソナを定義できます。

ISE ノードをセカンダリ ノードとして登録した直後に、ISE によってプライマリ ノードからセカンダリ ノードへのデータベース リンクが作成され、プライマリ ノードからセカンダリ ノードへの ISE 設定データの複製プロセスまたは共有プロセスが開始されます。このプロセスでは、展開の一部であるすべての ISE ノードに存在する設定データ間で整合性が保たれます。

通常、最初に ISE ノードをセカンダリ ノードとして登録したときに、完全な複製が実行されます。完全な複製の実行後は差分複製が実行され、プライマリ管理 ISE ノードでの設定データに対する新しい変更（追加、変更、削除など）がセカンダリ ノードに反映されます。複製のプロセスでは、展開内のすべての ISE ノードが同期されます。複製のステータスは、ISE 管理ユーザ インターフェイスの展開ページで確認できます。

ロード バランサの背後の 1 つの場所にあり、複数のマルチキャスト アドレスを共有するポリシー サービス ISE ノードはグループ化できます。このようなシナリオでは、ノード グループを定義し、特定のグループにノードを割り当てることができます。

展開からノードを削除するには、ノードの登録を解除する必要があります。プライマリ管理 ISE ノードからセカンダリ ノードの登録を解除すると、登録解除されたノードのステータスがスタンドアロンに変わり、プライマリ ノードとセカンダリ ノード間の接続が失われます。複製のアップデートは、登録解除されたセカンダリ ノードに送信されなくなります。

（注）　プライマリ管理 ISE ノードの登録は解除できません。

（注）　[展開（Deployment）] ページでプライマリ ノードをスタンドアロンとして維持できます。プライマリ ノードを編集し、[スタンドアロンにする（Make Standalone）] をクリックします。これは、展開ですべてのセカンダリ ノードの登録を解除した場合にのみ実行できます。

次のいずれかの変更を行うと、ISE ノードのアプリケーション サーバが再起動されます。

- ノードの登録（スタンドアロンからセカンダリへ）
- ノードの登録解除（セカンダリからスタンドアロンへ）
- プライマリ ノードからスタンドアロンへの変更（他のノードが登録されていない場合は、プライマリからスタンドアロンに変更されます）
- 管理 ISE ノードの昇格（セカンダリからプライマリへ）

- ペルソナの変更（ノードからポリシー サービスまたは監視ペルソナを割り当てたり、削除したりする場合）
- ポリシー サービス ISE ノードでのサービスの変更（セッションとプロファイラ サービスをイネーブルまたはディセーブルにします）
- プライマリでのバックアップの復元（同期操作がトリガーされ、プライマリ ノードからセカンダリ ノードにデータが複製されます）

（注） たとえば、展開に 2 つのノードがあり、セカンダリ ノードの登録を解除した場合は、このプライマリとセカンダリのペアのノード両方が再起動されます。（以前のプライマリ ノードとセカンダリ ノードはスタンドアロンになります）。

（注） これらのいずれかの変更を行うと、アプリケーション サービスが再起動されます。これらのサービスが再起動されるまで遅延が発生します。

（注） 展開では 1 つのプライマリ ノードのみを使用できます。他の Cisco ISE ノードは、以前に説明した 1 つまたは複数のロールに設定できるセカンダリ ノードです。プライマリ ノードが失われた場合は、セカンダリ ノードのいずれかを昇格させてプライマリ ノードにする必要があります。Cisco ISE では、任意のセカンダリ アプライアンスを昇格させてプライマリ ノードとして使用できます。

Cisco ISE インストールが完了したら、Cisco ISE インスタンスのいずれかをプライマリ ノードとして設定する必要があります。プライマリ ノードを編集し、プライマリ ノードで実行するサービスをイネーブルにできます。

セカンダリ ノードを登録する前に

前提条件：

- 登録するスタンドアロン ノードの完全修飾ドメイン名（FQDN）（たとえば、*ise1.cisco.com*）は、プライマリ管理 ISE ノードからドメイン ネーム システム（DNS）を使用して解決できる必要があります。解決できない場合は、ノード登録が失敗します。DNS サーバに、分散展開の一部である ISE ノードの IP アドレスと FQDN を入力する必要があります。
- プライマリ管理 ISE ノードと、セカンダリ ノードとして登録するスタンドアロン ノードでは、同じバージョンの Cisco ISE が実行されている必要があります。
- 初期セットアップ中に作成したユーザ名とパスワード（または、後で変更したパスワード）を使用します。
- プライマリ ノードとセカンダリ ノードのデータベース パスワードは同じである必要があります。ノード インストール中にこれらのパスワードが異なって設定された場合は、次のコマンドを使用してパスワードを変更できます。
  - application reset-passwd ise internal-database-admin
  - application reset-passwd ise internal-database-user

  CLI コマンドの使用方法の詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.1*』を参照してください。
- または、登録するノードで管理者アカウントを作成し、ノードの登録にそれらのクレデンシャルを使用することもできます。各 ISE 管理者アカウントには、1 つまたは複数の管理ロールが割り当てられています。セカンダリ ノードを登録および設定するには、Super Admin、System Admin、ま

たは RBAC Admin のいずれかのロールを割り当てる必要があります。さまざまな管理ロールとそれらの各ロールに関連付けられた権限の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の第 4 章「Cisco ISE Admin Group Roles and Responsibilities」を参照してください。

- ハイ アベイラビリティを実現するためにセカンダリ管理 ISE ノードを登録する場合は、他の Cisco ISE ノードを登録する前に、最初にプライマリでセカンダリ管理 ISE ノードを登録することを推奨します。Cisco ISE ノードがこの順序で登録された場合は、セカンダリ管理 ISE ノードをプライマリとして昇格した後にセカンダリ ISE ノードを再起動する必要はありません。
- セッション サービスを実行する複数のポリシー サービス ISE ノードを登録し、これらのノード間で相互フェールオーバーが必要な場合は、ノード グループにポリシー サービス ISE ノードを配置する必要があります。登録ページで使用するノード グループを選択する必要があるため、ノードを登録する前にノード グループを最初に作成する必要があります。詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の第 9 章「Creating, Editing, and Deleting Node Groups」を参照してください。
- プライマリ ノードの証明書信頼リスト（CTL）に、（セカンダリ ノードとして登録する）スタンドアロン ノードの HTTPS 証明書を検証するために使用できる適切な認証局（CA）証明書が含まれ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*』の第 12 章「Creating Certificate Trust Lists in the Primary Cisco ISE Node」を参照してください。
- セカンダリ ノードをプライマリ ノードに登録した後で、登録されたセカンダリ ノードで HTTPS 証明書を変更した場合は、セカンダリ ノードの HTTPS 証明書を検証するために使用できる適切な CA 証明書を取得し、プライマリ ノードの CTL にインポートする必要があります。詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の第 12 章「Creating Certificate Trust Lists in the Primary Cisco ISE Node」を参照してください。

（注） すべての Cisco ISE ノードを UTC 時間帯に設定することを推奨します。この手順では、展開内にあるさまざまなノードからのレポートとログのタイムスタンプが常に同期されます。

プライマリ ノードのユーザ インターフェイスを使用して、セカンダリ ノードを登録し、設定プロファイルを編集できます。セカンダリ ノードのインストール直後に、Cisco ISE は、すべての変更を複製および同期するためにプライマリ ノードとセカンダリ ノード間のデータベース リンクを作成します。また、ノードを選択解除することにより、展開からノードを削除できます。このアクションにより、ノードは展開から削除されます。

プライマリからノードの登録を解除すると、登録解除されたノードのステータスがスタンドアロンに変わります。プライマリ ノードとセカンダリ ノード間の接続が失われ、複製アップデートはセカンダリ ノードに送信されません。

次の手順：

Cisco ISE ノードの設定の詳細については、次を参照してください。

- *『Cisco Identity Services Engine User Guide, Release 1.1』*
  - 第 9 章「Setting Up ISE in a Distributed Environment」と「Registering and Configuring a Secondary Node」

分散展開を設定する場合のガイドライン

分散展開で Cisco ISE アプライアンスを設定する前に、次のガイドラインに従ってください。

- 分散展開のために適切に設定された DNS が正しく動作している必要があります。

- Cisco ISE ノードは、同時にどの ISE ノード ペルソナでも実行できます。
- Cisco ISE ノードは、構成と設定に応じて、スタンドアロン ノード、あるいはプライマリとセカンダリのペアのプライマリ ノードまたはセカンダリ ノードとして実行するよう指定できます。
- 展開では 1 つのプライマリ Cisco ISE ノードのみを使用できます。

（注） 他の Cisco ISE ノードは、ライセンスと設定に応じて、1 つまたは複数の他のロールに設定できるセカンダリ ノードと見なされます。プライマリ ノードが失われた場合は、有効なセカンダリ ノードを昇格させてプライマリ ノードにする必要があります。Cisco ISE は、管理ペルソナを持つセカンダリ ノード アプライアンスの「新しい」プライマリ ノードへの昇格のみをサポートします。また、Cisco ISE は管理者ペルソナを持つセカンダリ ノードとして有効なライセンスを所有している必要があります。

- プライマリ Cisco ISE ノードは管理ペルソナを実行する必要があります。
- すべての Cisco ISE システム関連の設定と、機能関連の設定は、プライマリ Cisco ISE ノードでのみ行う必要があります。
- プライマリ ノードで行った設定の変更は、展開内のすべてのセカンダリ ノードに複製されます。
- インライン ポスチャ ノードは、専用 Cisco ISE ノードを必要とします。他のサービスは、インライン ポスチャ ノードとして指定されたノードで実行できません。

（注） インライン ポスチャ ノードは、VMware サーバ システムでサポートされません。

- ノード間の時間帯の問題を回避するために、各ノードのセットアップ モード中に同じ NTP サーバ名を指定する必要があります。

Cisco ISE インストールが完了したら、Cisco ISE ノードのいずれかをプライマリ ノードとして設定する必要があります。プライマリ ノードを編集し、プライマリ ノードで実行するサービスをイネーブルにできます。プライマリ ノードのユーザ インターフェイスを使用して、セカンダリ ノードを登録し、設定を編集できます。セカンダリ ノードのインストール直後に、Cisco ISE は、すべての変更を複製および同期するためにプライマリ ノードとセカンダリ ノード間のデータベース リンクを作成します。

プライマリからノードの登録を解除すると、登録解除されたノードのステータスがスタンドアロンに変わります。登録解除されたノードを再びプライマリで登録するには、最初にノード上のデータベース設定をリセットし、新しくインストールされたノードの状態に戻して、ノードを再び登録する必要があります。

詳細情報：

次の項目の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』を参照してください。

- Cisco ISE 管理グループ ロールおよび役割
- Cisco ISE ノード サービス
- ノードの設定のリセット

Cisco ISE アーキテクチャの概要

図 1-1 に、次のコンポーネントを含む Cisco ISE アーキテクチャの基本的な概要を示します。

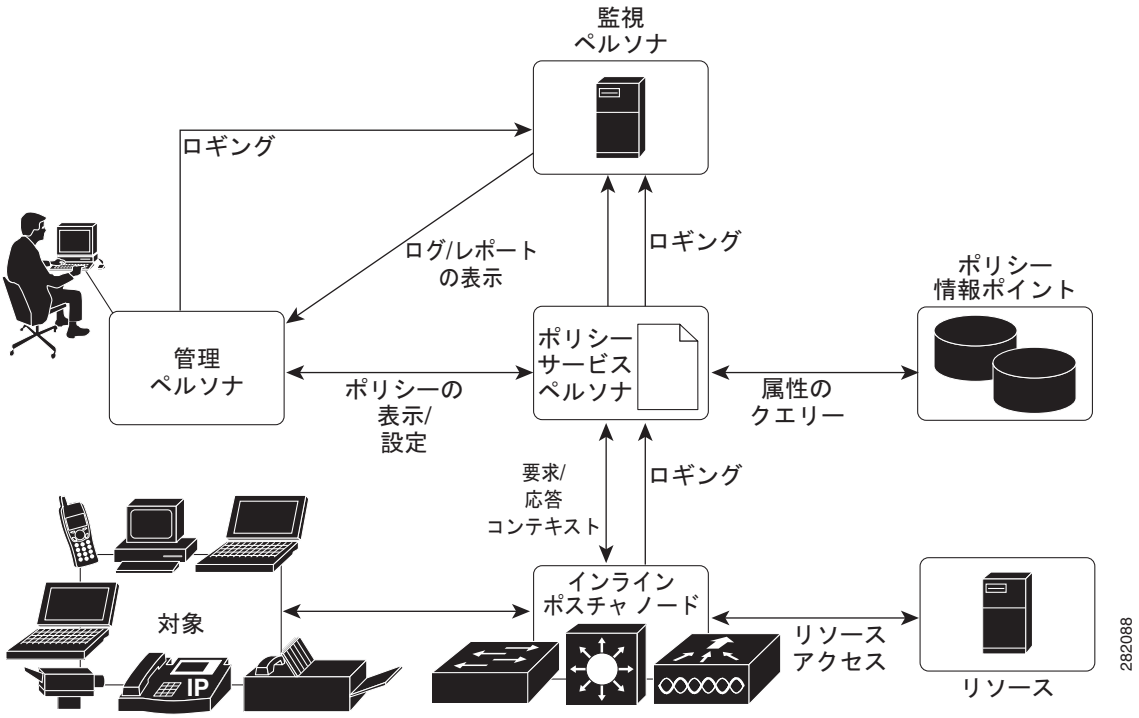
- ノードおよびペルソナの種類

  - ISE ノード：管理、ポリシー サービス、監視
  - インライン ポスチャ ノード：ゲートキーパーおよびアクセス ポリシー適用
- ネットワーク リソース
- エンドポイント

（注）　図 1-1 に、ISE ノードおよびペルソナの種類（管理、ポリシー サービス、および監視）、インライン ポスチャ ノード、およびポリシー情報ポイントを示します。

ポリシー情報ポイントは、外部の情報がポリシー サービス ペルソナに伝送されるポイントを表します。たとえば、外部情報は Lightweight Directory Access Protocol（LDAP）属性になります。

図 1-1　Cisco ISE のアーキテクチャ



展開シナリオ

この項では、Cisco ISE を分散展開で展開できる 3 つのシナリオについて説明します。

- 「小規模な Cisco ISE ネットワーク展開」（P.1-9）
- 「中規模な Cisco ISE ネットワーク展開」（P.1-10）
- 「大規模な Cisco ISE ネットワーク展開」（P.1-11）

小規模な Cisco ISE ネットワーク展開

最も小規模な Cisco ISE 展開は、図 1-2 で示されているように 2 つの Cisco ISE ノードから構成されます（小規模なネットワークでは 1 つの Cisco ISE ノードがプライマリ アプライアンスとして動作します）。

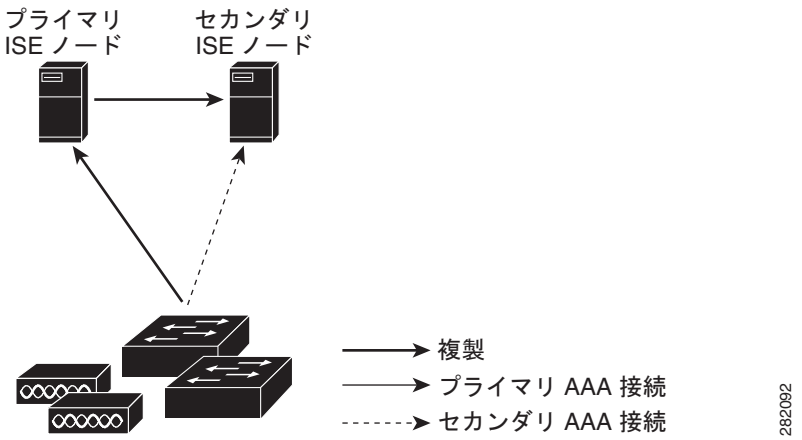
（注）　同時エンドポイントは、サポートされるユーザとデバイスの合計数を表します。これには、ユーザ、パーソナル コンピュータ、ラップトップ、IP 電話、スマート フォン、ゲーム コンソール、プリンタ、ファクス機、またはその他のネットワーク デバイスを組み合わせることができます。

プライマリ ノードが、このネットワーク モデルに必要なすべての設定、認証、およびポリシー機能を提供する一方で、セカンダリ Cisco ISE ノードはバックアップ ロールで稼働します。セカンダリ ノードはプライマリ ノードをサポートし、セカンダリ ネットワーク アプライアンス、ネットワーク リソース、または RADIUS の間で接続が失われたときにネットワークを稼働し続けます。

RADIUS は、一元化された AAA 操作がクライアントとプライマリ Cisco ISE ノード間で実行される場所です。結果として、プライマリ Cisco ISE ノードにあるすべての内容をセカンダリ Cisco ISE ノードと同期したり、その内容をセカンダリ ノードに複製したりできることが主な要件になります。

プライマリ ノードとセカンダリ ノード間で同期を行えるため、セカンダリ ノードをプライマリ ノードの最新の状態に保つことができます。小規模なネットワーク展開では、このような設定モデルでこのような展開または同様の方法を使用して、すべての RADIUS クライアントでプライマリ ノードとセカンダリ ノードの両方を設定できます。

図 1-2　小規模な Cisco ISE ネットワーク展開



ネットワーク環境でデバイス、ネットワーク リソース、ユーザ、および AAA クライアントの数が増えた場合に、図 1-3 で示されているように、基本的な小規模モデルから展開設定を変更し、分割または分散された展開モデルを使用することを推奨します。

（注）　図 1-2 は、AAA 機能を実行するポリシー サービス ペルソナとして動作するセカンダリ Cisco ISE ノードを示しています。セカンダリ Cisco ISE ノードは、監視または管理ペルソナとして動作することもできます。

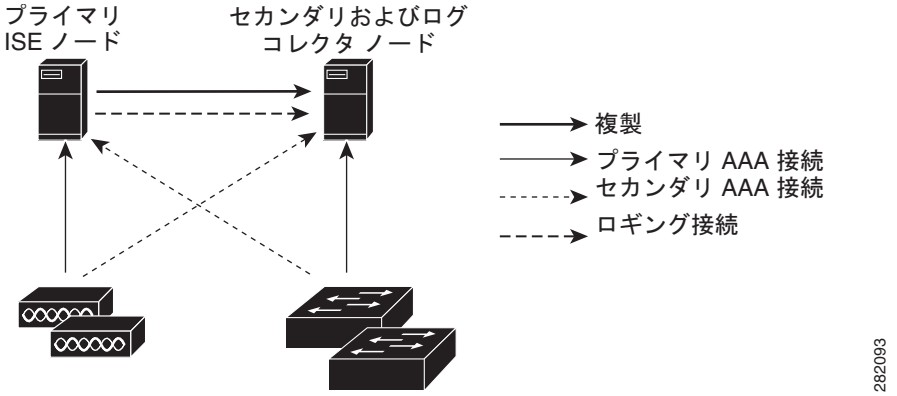
分割 Cisco ISE 展開

分割 Cisco ISE 展開の場合は、小規模な Cisco ISE 展開で説明されたようにプライマリ ノードとセカンダリ ノードを維持し続けます。ただし、AAA ロードは、AAA ワークフローを最適化するためにこれらの 2 つの Cisco ISE ノード間で分割されます。AAA 接続で問題がある場合は、各 Cisco ISE アプライアンス（プライマリまたはセカンダリ）がすべてのワークロードを処理できる必要があります。通常のネットワーク運用で稼働している場合は、プライマリ ノードとセカンダリ ノードのどちらも AAA 要求を処理するすべてのロードを引き受けません。これは、このワークロードが 2 つのノード間で分散されるためです。

このようにロードを分割できるため、システムの各 Cisco ISE ノードに対する負荷は減少します。また、ロードの分割により優れた負荷の制御を実現しつつ、通常のネットワーク運用中のセカンダリ ノードの機能ステータスはそのまま保持します。

別の利点は、各ノードが、ネットワーク アドミッションやデバイス管理などの独自の固有操作を実行でき、障害発生時でもすべての AAA 機能を実行できることです。認証要求を処理し、アカウンティング データを AAA クライアントから収集する 2 つの Cisco ISE ノードがある場合は、Cisco ISE ノードのいずれかがログ コレクタとして動作するよう設定することを推奨します。図 1-3 に、このロールのセカンダリ Cisco ISE ノードを示します。

図 1-3　分割 Cisco ISE ネットワーク展開



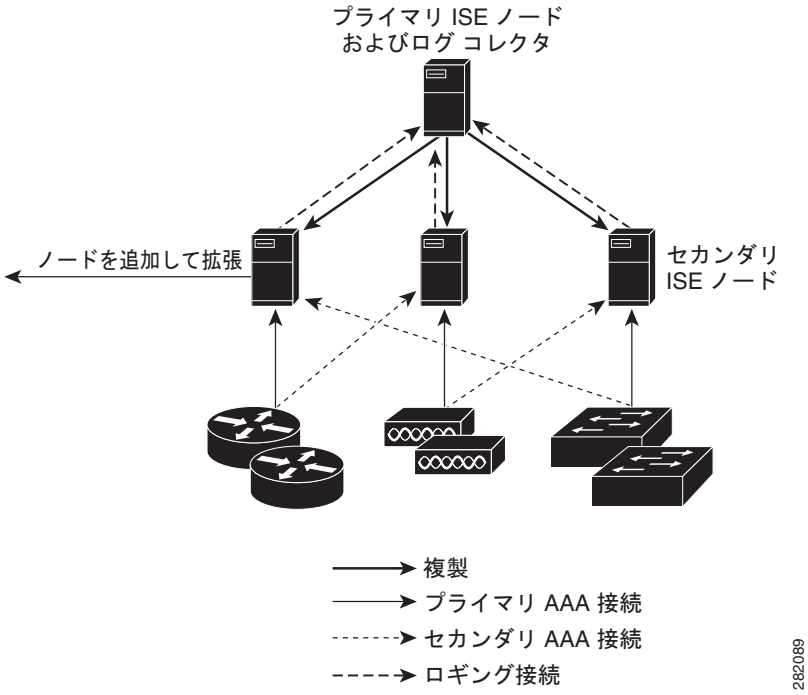
また、分割 Cisco ISE ノード展開の設計により、拡大が可能になる利点も提供されます（図 1-4 を参照）。

中規模な Cisco ISE ネットワーク展開

小規模なローカル ネットワークが大きくなった場合に、Cisco ISE ノードを追加して中規模なネットワークを作成し、素早くネットワークの拡大に対応できます。中規模なネットワーク展開では、すべての設定サービスを処理するために 1 つの Cisco ISE ノードを昇格させてプライマリとして実行し、すべての AAA 機能を管理するためにセカンダリ Cisco ISE ノードを使用できます。

ネットワークでログ トラフィックの量が増加した場合に、プライマリ Cisco ISE ノードを集中ログ コレクタとして使用するか、セカンダリ Cisco ISE ノードのいずれかをネットワークのこの機能のための専用ノードにするかを選択できます。

図 1-4　中規模な Cisco ISE ネットワーク展開



大規模な Cisco ISE ネットワーク展開

大規模な Cisco ISE ネットワークには集中ロギング（図 1-5 を参照）を使用することを推奨します。集中ロギングを使用するには、大規模で通信量の多いネットワークが生成することがある大きい syslog トラフィックを処理する監視ペルソナ（監視およびロギング用）として動作する専用ロギング サーバを設定する必要があります。

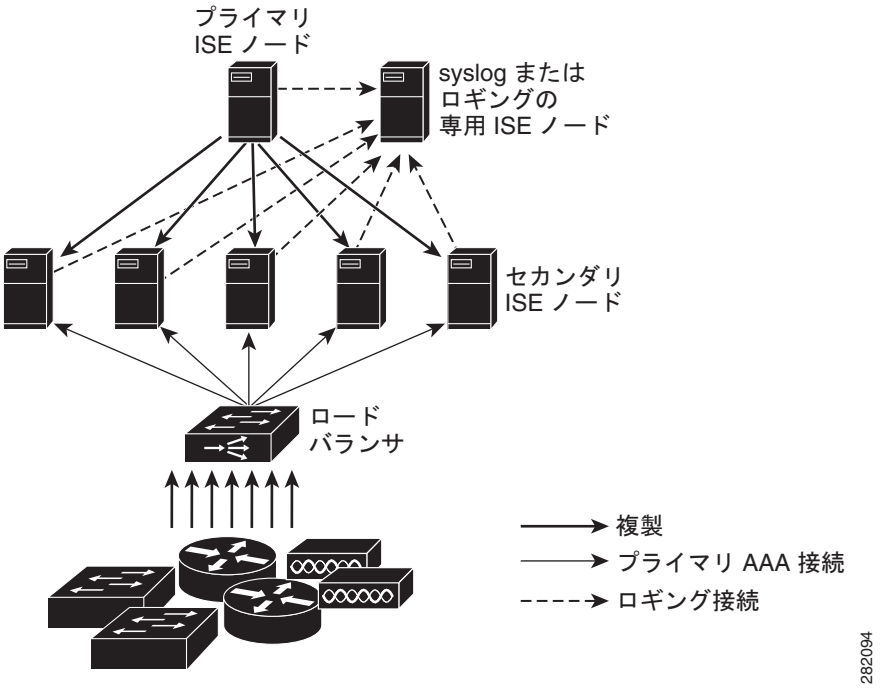
syslog メッセージは発信ログ トラフィックに対して生成されるため、どの RFC-3164 準拠 syslog アプライアンスでも、発信ロギング トラフィックのコレクタとして動作できます。専用ロギング サーバでは、すべての Cisco ISE ノードをサポートするために Cisco ISE で使用できるレポート機能およびアラート機能を使用できます。Cisco ISE ソフトウェアが専用ロギング サーバをサポートするよう設定する場合は、「セットアップ プログラムのパラメータについて」（P.3-3）を参照してください。

また、アプライアンスが Cisco ISE ノードの監視ペルソナと汎用 syslog サーバの両方にログを送信するよう設定することもできます。汎用 syslog サーバを追加することにより、Cisco ISE ノード上の監視ペルソナがダウンした場合に冗長なバックアップが提供されます。

大規模な集中ネットワークでは、ロード バランサを使用する必要があります（図 1-5 を参照）。これにより、AAA クライアントの展開が簡略化されます。ロード バランサを使用するには、AAA サーバのエントリが 1 つだけ必要です。ロード バランサは、利用可能なサーバへの AAA 要求のルーティングを最適化します。

ただし、ロード バランサが 1 つだけしかないと、シングル ポイント障害が発生する可能性があります。この問題を回避するために、2 つのロード バランサを展開し、冗長性とフェールオーバーを実現します。この構成では、各 AAA クライアントで 2 つの AAA サーバ エントリを設定する必要があります（この設定は、ネットワーク全体で同じになります）。

図 1-5　大規模な Cisco ISE ネットワーク展開

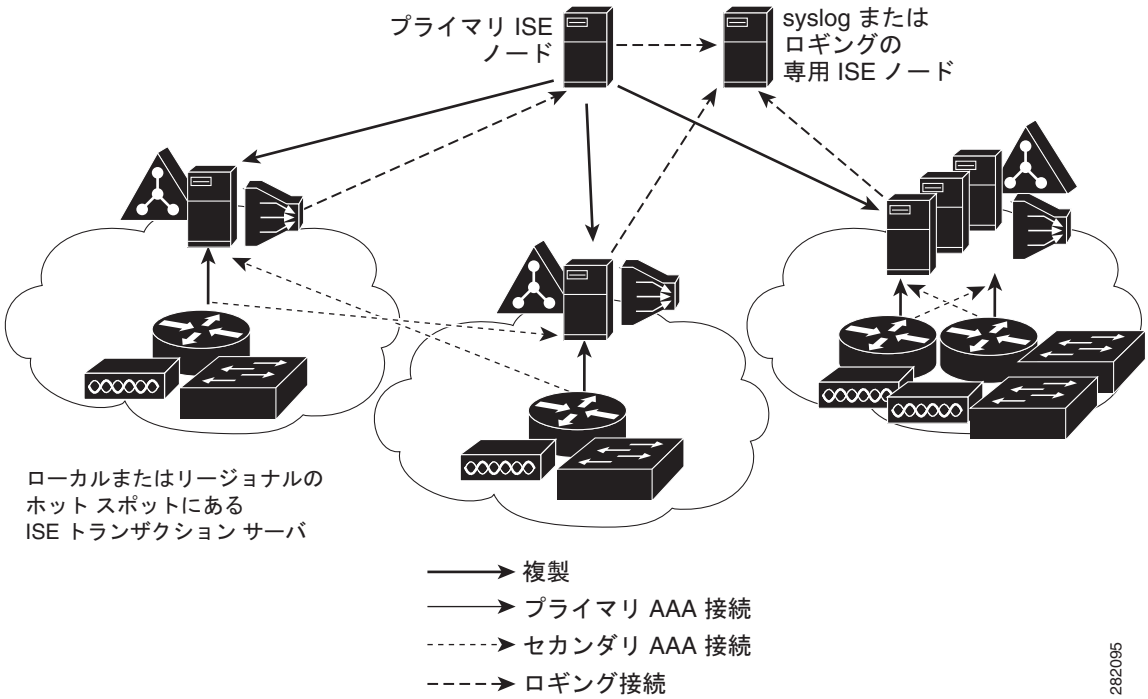


分散 Cisco ISE ネットワーク展開

分散 Cisco ISE ネットワーク展開は、主要な拠点があり、他の場所に地域、全国、またはサテライトの拠点がある組織に最も役に立ちます。主要な拠点は、プライマリ ネットワークが存在し、追加の LAN に接続される小規模から大規模にわたる場所であり、異なる地域や距離が離れた場所のアプライアンスとユーザをサポートします。

AAA パフォーマンスを最適化するために、各リモート サイトは独自の AAA インフラストラクチャを持つ必要があります（図 1-6 を参照）。集中管理モデルにより、同一の同期された AAA ポリシーが保持されます。集中設定モデルでは、プライマリ Cisco ISE ノードとセカンダリ Cisco ISE ノードを使用します。Cisco ISE ノードで個別の監視ペルソナを使用することを推奨しますが、リモートの場所それぞれで独自の固有なネットワーク要件を満たす必要があります。

図 1-6　分散 Cisco ISE 展開



複数のリモート サイトがあるネットワークを計画するときの一部の考慮事項は次のとおりです。

- Microsoft Active Directory や LDAP などの中央または外部データベースが使用されているかどうかを確認します。プロセスを最適化するために、各リモート サイトでは Cisco ISE がアクセスできる外部データベースの同期されたインスタンスが必要です。
- AAA クライアントの検索が重要になります。ネットワーク遅延の影響と WAN 障害により引き起こされるアクセス損失の可能性を減らすために、AAA クライアントのできるだけ近くに存在する Cisco ISE ノードを見つける必要があります。
- Cisco ISE では、バックアップなどの一部の機能にコンソールからアクセスできます。各サイトでターミナルを使用して、各ノードへのネットワーク アクセスをバイパスする直接的で安全なコンソール アクセスを行うことができます。
- 小規模な場合は、リモート サイトが近くにあるため、他のサイトに信頼できる WAN 接続を行えます。また、冗長性を提供するために、ローカル サイトのバックアップとして Cisco ISE ノードを使用できます。
- 外部データベースにアクセスできるようにするには、すべての Cisco ISE ノードで DNS を適切に設定する必要があります。

Cisco ISE ノードの設定

この項では、ネットワーク展開でさまざまな Cisco ISE アプライアンスが担うロールとそれらの設定方法について簡単に説明します。

- 「プライマリ ノード」（P.1-14）
- 「セカンダリ ノード」（P.1-14）
- 「ロギング サーバ」（P.1-15）

次の項目の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の「Setting Up Cisco ISE in a Distributed Environment」の章を参照してください。

- Cisco ISE ノードの設定
- 管理 Cisco ISE ノードでのハイ アベイラビリティの設定
- 展開内のノードの表示
- ノード グループの管理
- ノード ペルソナとサービスの変更
- 監視 ISE ノードでの自動フェールオーバーの設定
- 展開からのノードの削除
- Cisco ISE アプライアンス ハードウェアの交換

すべての Cisco ISE アプライアンスのインストール手順は似ています。詳細については、次の項を参照してください。

- 第 3 章「Cisco ISE 3300 シリーズ アプライアンスの設定」（Cisco ISE 3300 シリーズ アプライアンスへの Cisco ISE ソフトウェアのインストール）。
- 第 4 章「VMware 仮想マシンにおける Cisco ISE 3300 シリーズ ソフトウェアのインストール」（VMware ESX サーバへの Cisco ISE ソフトウェアのインストール）。

（注）　どの Cisco ISE ネットワーク展開でも、ネットワークのプライマリ ノードとして指定されたノードで、最初のハードウェアの取り付けを行う必要があります。

プライマリ ノード

Cisco ISE 展開では、1 つのアプライアンスのみ Cisco ISE プライマリ ノードとして稼働できます。このプライマリ ノードは設定機能を提供します。このプライマリ ノードからすべての複製操作を実行できます。

プライマリとセカンダリのペアでは、管理ペルソナとして動作するプライマリ ノードとセカンダリ ノードのみをライセンス ファイルで設定する必要があります。ライセンス ファイルをプライマリにインストールすると、セカンダリ ノードのライセンス要件が満たされます。

セカンダリ ノード

ネットワークでは 1 つのプライマリ Cisco ISE ノードしか使用できないため、他のすべての Cisco ISE ノードはセカンダリ ノードとして動作します。Cisco ISE セカンダリ ノードはプライマリ ノードからすべてのシステム設定を受け取りますが、各セカンダリ ノードでは次の項目を設定する必要があります。

- ライセンス：プライマリに基本ライセンスがインストールされると、複製機能により、展開内の各 Cisco ISE セカンダリ ノードにライセンスがコピーされます。
- 新しいローカル証明書：セカンダリ ノードでローカル証明書を設定するか、ローカル証明書をプライマリ ノードから各セカンダリ ノードにインポートできます。
- ロギング サーバ：プライマリ ノードまたはセカンダリ ノードが Cisco ISE ネットワークの専用ロギング サーバとして動作するよう設定できます。セカンダリ Cisco ISE ノードを専用ロギング サーバとして設定することを強く推奨します。

プライマリ ノードとセカンダリ ノードのペアでは、セカンダリ ノードは登録され、完全に同期された設定と複製アップデートをネットワーク内のプライマリ ノードから受け取ります。

ロギング サーバ

プライマリ ノードまたはいずれかのセカンダリ ノードをネットワークの専用ロギング サーバとして使用するよう設定できます。このロールでは、ロギング サーバは、Cisco ISE ネットワークに展開されたプライマリ ノードとすべてのセカンダリ ノードからログを受け取ります。Cisco ISE セカンダリ ノードのいずれかを監視ペルソナとして指定し、AAA のすべてのアクティビティからこの特定のセカンダリ ノードを除外することを推奨します。次の 3 つの主なロギング カテゴリが取得されます。

- 監査
- アカウンティング
- 診断

ロギング カテゴリと、ロギング サーバを設定するベスト プラクティスの詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の第 13 章「Logging」を参照してください。

Cisco ISE 機能をサポートするために必要なスイッチ設定

Cisco ISE をネットワーク スイッチと相互運用し、Cisco ISE の機能がネットワーク セグメント全体で正常に動作するようにするには、ネットワーク スイッチで、特定の必要な NTP、RADIUS/AAA、802.1X、MAB、およびその他の設定を指定する必要があります。

詳細情報：

- その他のスイッチ設定要件については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の付録 C「Switch Configuration Required to Support Cisco ISE Functions」を参照してください。

インライン ポスチャ展開の計画

この項は、Cisco ISE ネットワークでのインライン ポスチャの展開を計画するために必要なことの簡単な概要を提供することを目的としています。インライン ポスチャ展開で発生した問題について調べ、ネットワークのニーズと要件を満たすには何が最適かを判断することは、ネットワーク アーキテクトまたはシステム アーキテクトの責任です。

ネットワークでのインライン ポスチャの展開または設定を計画する前に、最初に、サポートされているインライン ポスチャ動作モードの種類と展開オプションについて理解する必要があります。

（注）　インライン ポスチャ動作モード、フィルタ、管理対象サブネット、およびインライン ポスチャのハイアベイラビリティ（これらのトピックは Cisco ISE ネットワークに対応します）の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の第 10 章「Setting Up an Inline Posture Node」を参照してください。

インライン ポスチャ計画の考慮事項

この項では、インライン ポスチャ ノードの展開を計画するときにネットワーク アーキテクトまたはシステム アーキテクトが対応する必要がある基本的ないくつかの問題と考慮事項について説明します。分散 Cisco ISE ネットワーク展開でインライン ポスチャ ノード設定を開始する前に、計画および展開に関する次の問題について理解する必要があります。

- インライン ポスチャ ノードの展開をどのように計画しますか。
- インライン ポスチャ ノードをどのように展開しますか。
- インライン ポスチャ ノードをスタンドアロン ノードとして実行しますか、またはインライン ポスチャ ノードのプライマリとセカンダリのペアの一部として実行しますか。

（注）　Cisco ISE ネットワークでは、ネットワークで一度に最大 2 つのインライン ポスチャ ノードを設定できます。ハイ アベイラビリティを備えたインライン ポスチャのプライマリとセカンダリのペアを展開する場合は、2 つのインライン ポスチャ ノードを設定する必要があります。このモードでは、一方のノードがプライマリとして指定され、他方のノードがセカンダリ ノードとして指定されます。両方のノードが同時に稼働された場合は、プライマリ ノードがプライマリ ロールを担当します。

- 展開計画にインライン ポスチャのプライマリとセカンダリのペアの設定を含めますか。含める場合、機能に関連するすべての設定はこのペアのプライマリ ノードからのみ行えることに注意してください（Cisco ISE ユーザ インターフェイスには、この設定のセカンダリ ノードに対する基本的な設定の表のみが表示されます）。
- インライン ポスチャ プライマリ ノード設定とそのピア セカンダリ ノードの同期は、このインライン ポスチャ ペアのプライマリ ノードの [フェールオーバー（Failover）] タブを使用して実行できることに注意してください。詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の第 10 章「Setting Up an Inline Posture Node」を参照してください。

この項の次のトピックでは、インライン ポスチャ ノードの基本的な情報の一部を提供します。ただし、これらのトピックは、ネットワークでの包括的な展開計画を完了するために必要なすべての情報を提供することを目的としていません。

インライン ポスチャ動作モードの選択

どのインライン ポスチャ動作モードを選択するかは、既存のネットワーク アーキテクチャに大きく依存します。選択によって、Cisco ISE 展開で使用できる他の多くの設定オプションが制限されます。したがって、次の各プライマリ インライン ポスチャ動作モードについて完全に理解する必要があります。

- ルーテッド モード：このモードは、ネットワーク接続でレイヤ 3 の「ホップ」として動作します。ルーテッド モードは、指定されたアドレスにパケットを転送します。ルーテッド モードでは、ネットワーク トラフィックを分離でき、選択された宛先アドレスにアクセスできるユーザにアクセス権を指定できます。
- ブリッジ モード：このモードは、ネットワーク接続でレイヤ 2 の「Bump In The Wire」として動作します。ブリッジ モードは、宛先アドレスに関係なくパケットを転送します。

（注）　また、インライン ポスチャ ノードはメンテナンス モードもサポートします。このモードでは、管理作業を実行できるようノードがオフラインになります。このモードは、インライン ポスチャ ノードがネットワークで最初にオンラインになったときのデフォルト値です。

インライン ポスチャ ルーテッド モード

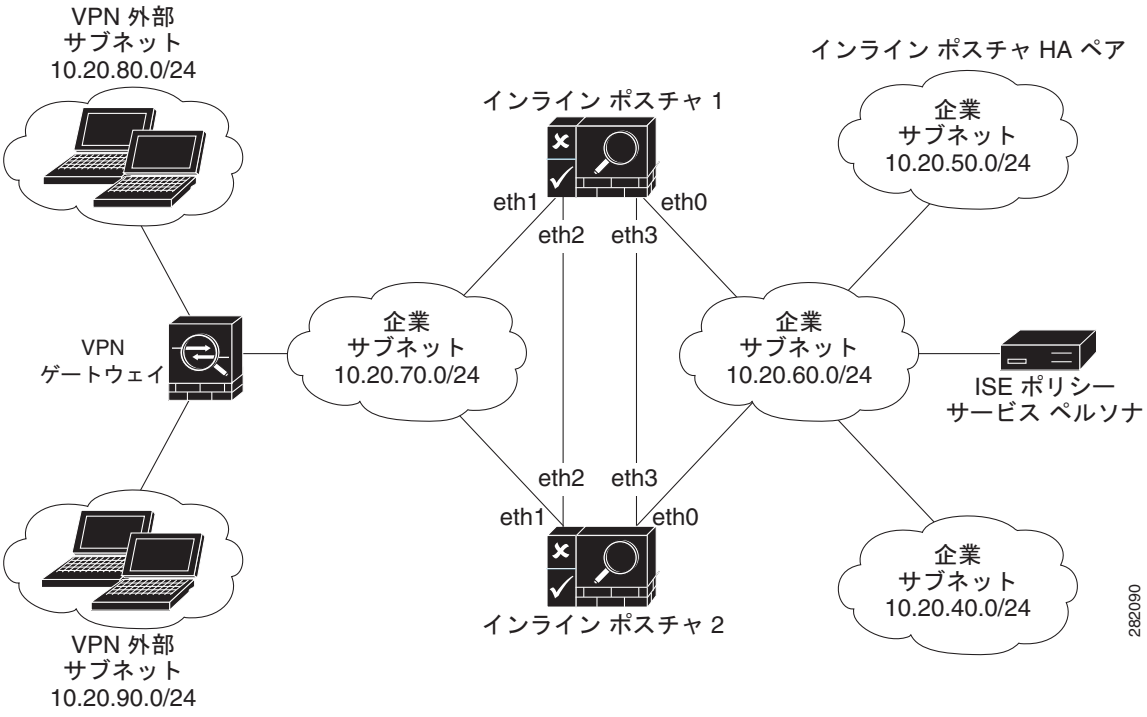
ルーテッド モードでは、インライン ポスチャ ノードはレイヤ 3 ルータとして動作し、信頼できない（Cisco ISE 外部）ネットワークと管理対象クライアントのデフォルト ゲートウェイとして機能します。信頼できないネットワークと信頼できるネットワーク間のすべてのトラフィックは、このインライン ポスチャ ルーテッド モードで渡されます。ルーテッド モードは、IP フィルタリング ルール、設定されたアクセス ポリシー、およびネットワークに設定した他のトラフィックベースのポリシーを適用します。

インライン ポスチャ ノードをルーテッド モードで設定する場合は、次の 2 つのインターフェイスの IP アドレスを指定します。

- 信頼できる（Eth0）
- 信頼できない（Eth1）

信頼できるアドレスと信頼できないアドレスは、異なるサブネットに属する必要があります。インライン ポスチャ ノードは、1 つまたは複数のサブネットを管理でき、信頼できないインターフェイスは管理対象サブネットのゲートウェイとして動作します。図 1-7 に、インライン ポスチャ ルーテッド モードの構成例を示します。

図 1-7　　インライン ポスチャ ルーテッド モードの構成



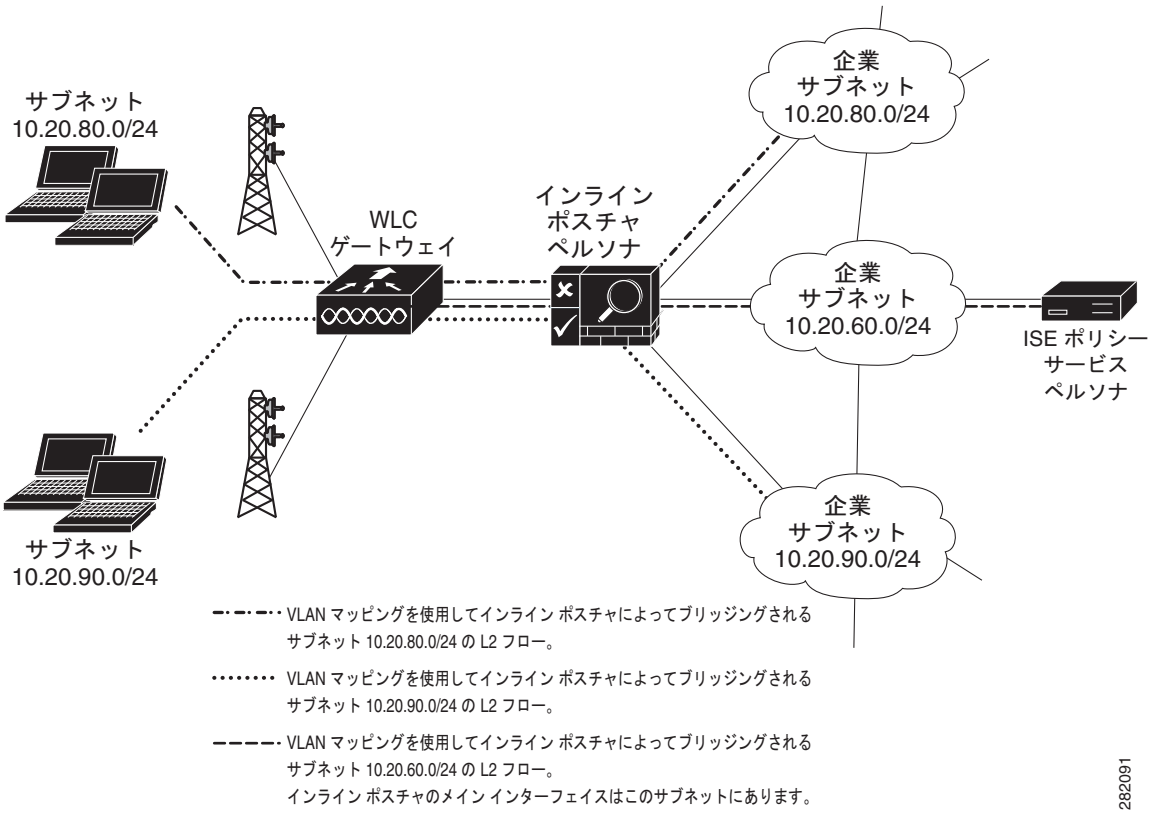
インライン ポスチャ ブリッジ モード

ブリッジ モードで動作する場合、インライン ポスチャ ノードは標準的なイーサネット ブリッジのように動作します。この設定は、信頼できないネットワークにすでにゲートウェイが含まれ、既存の設定に変更を行わない場合に最もよく使用されます。

図 1-8 に、WLC から Cisco ISE ネットワークへのレイヤ 2 クライアント トラフィックに対してブリッジとして動作するインライン ポスチャ ノードを示します。この構成では、インライン ポスチャ ノードで、ARP ブロードキャストに応答し、ARP ブロードキャストを適切な VLAN に送信できるサブネット エントリが必要です。

3 つのサブネット例（10.20.80.0/24、10.20.90.0/24、および 10.20.60.0/24）からのトラフィックのレイヤ 2 フローは、すべて VLAN マッピングによるインライン ポスチャ ノードでのブリッジ モードの使用を反映します。3 つのサブネット例の唯一の違いは、10.20.60.0/24 サブネットの場合に、インライン ポスチャ メイン インターフェイスがこのサブネット内に存在することです。

図 1-8　　インライン ポスチャ ブリッジ モードの設定



インライン ポスチャをスタンドアロンまたはハイ アベイラビリティとして展開

インライン ポスチャ展開で行う最も重要な決定は、インライン ポスチャを、単一のスタンドアロン インライン ポスチャ ノードとして展開するか、ハイ アベイラビリティを確保し、冗長性を提供してネットワークの信頼性を高めるためにプライマリとセカンダリのペアとして展開するかを決めることです。

スタンドアロン インライン ポスチャ ノードは、インライン ポスチャ サービスを提供する単一のインライン ポスチャ ノードであり、Cisco ISE ネットワークの他のすべてのノードとは独立して動作します。小規模な場所で使用するネットワークやネットワーク冗長性が大きな問題とはならない小規模なネットワークには、単一のスタンドアロン インライン ポスチャ ノードを展開することを決定できます。

ハイ アベイラビリティのためにインライン ポスチャ ノードのペアを設定する場合、追加の冗長性と信頼性を提供するために、これらはプライマリとセカンダリのペアとして動作します。このプライマリとセカンダリのペアにより、ペアのいずれかのノードで障害が発生した場合であってもネットワークが稼働し続けます。プライマリ ノードで障害が発生した場合は、セカンダリ ノードが引き継ぎ、必要なインライン ポスチャ機能を提供します。

インライン ポスチャのハイ アベイラビリティについて

インライン ポスチャのハイ アベイラビリティは、プライマリとセカンダリのペアとして設定された 2 つのインライン ポスチャ ノードから構成されます。この設定では、プライマリ ノードは RADIUS プロキシとして動作し、すべてのネットワーク パケットを転送します。プライマリ ノードで障害が発生すると、このペアのセカンダリ インライン ポスチャ ノードが引き継ぎます。

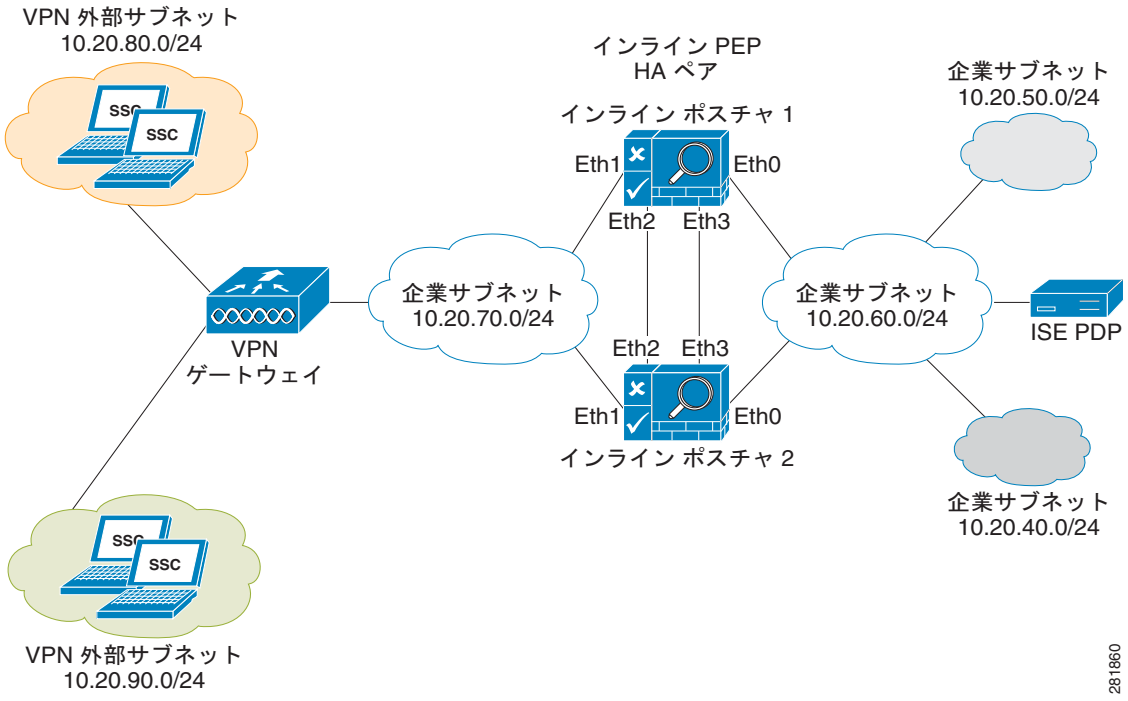
プライマリとセカンダリのペアが設定されたインライン ポスチャのステートレス ハイ アベイラビリティ展開では、セカンダリ ノードがバックアップ ユニットとして動作し、インターフェイス間でパケットを転送しません。ステートレスとは、プライマリ ノードにより認証および許可されたセッションがフェールオーバーの発生後に再び自動的に許可されることを意味します。

セカンダリ ノードは、(eth2 および eth3 インターフェイスで) ハートビート プロトコルを使用してプライマリ ノードを監視します。ハートビート プロトコルでは、2 つのノード間でメッセージを定期的に送信する必要があります。ハートビートが停止するか、割り当てられた時間内に応答がない場合は、フェールオーバーが発生し、復元アクションが実行されます。

ハートビート プロトコルがインライン ポスチャのハイ アベイラビリティ設定でアクティブな場合は、インライン ポスチャのプライマリとセカンダリのペアの eth2 インターフェイスと eth3 インターフェイス間でネットワーク接続が必要です。インライン ポスチャのハイ アベイラビリティ ペア（プライマリとセカンダリ）の各ノードの eth2 インターフェイスと eth3 インターフェイスは、2 つのノード間でのハートビート プロトコルの交換を使用するよう設定されています。このため、両方のインライン ポスチャ ノードの eth2 インターフェイス間でケーブルを直接接続する必要があります。同様に、冗長性を確保するために、両方のノードの eth3 インターフェイス間でケーブルを直接接続する必要があります。

（注） ハートビート プロトコルでは、ハイ アベイラビリティ ペアの両方のノードの eth2 インターフェイス間でケーブルを直接接続し、2 つのノードの eth3 インターフェイス間でケーブルを直接接続する必要があります。これらの接続には、どのイーサネット ケーブルでも使用できます。図 1-9 に、このケーブル要件を示します。

図 1-9　ハートビート プロトコル：eth2 および eth3 インターフェイスのイーサネット ケーブル接続



CHAPTER 2

Cisco ISE 3300 シリーズ ハードウェアについて

この章では、Cisco Identity Services Engine（ISE）3300 シリーズ アプライアンス ハードウェアを紹介し、サポート アプライアンス ハードウェア、主要なコンポーネント、コントロール、コネクタ、前面および背面パネルの LED インジケータについて説明します。この章で説明する内容は、次のとおりです。

Cisco ISE シリーズ アプライアンス

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）と Cisco ISE ソフトウェアは、専用 Cisco ISE 3300 シリーズ アプライアンスまたは VMware サーバ（Cisco ISE VM）のいずれかで実行します。Cisco ISE リリース 1.1 ソフトウェアは、この専用プラットフォームで他のパッケージまたはアプリケーションのインストールをサポートしません。追加のハードウェア互換性情報については、『*Release Notes for Cisco Identity Service Engine, Release 1.1*』を参照してください。

Cisco ISE 3300 シリーズ アプライアンス ハードウェアの概要

表 2-1、表 2-2、および 表 2-3 に、サポートされる各 Cisco ISE アプライアンスのハードウェア仕様の概要を示します。ネットワーク インターフェイス カード（NIC）ポート、電源装置ソケット、LED、および対応するパネルの重要なコントロールまたはボタンを示す詳細な図へのハイパーリンクについては、「図」カラムを参照してください。

表 2-1　Cisco ISE 3315 アプライアンス ハードウェアの概要

ハードウェアおよびサポートの仕様	図
• Cisco ISE 同時エンドポイント サポート：[1] – ポリシー サービス ノードのみ：最大 3,000 – その他のノード タイプまたは組み合わせ：最大 2,000 • シングル プロセッサ：クアッドコア Intel Xeon（コア 2 クアッド） • 4 ギガバイト（GB）RAM • 2 x 250 GB SATA[2] ハード ディスク ドライブ（HDD） • 4 つの 10/100/1000 LAN ポート（2 つの統合 NIC と 2 つのギガビット（Gb）NIC（PCI-E）） • CD/DVD-ROM ドライブ • 4 つの USB ポート（前面パネルに 2 つ、背面パネルに 2 つ） • 背面パネルに 2 つの Gb イーサネット ポート • 背面パネルに 1 つのシリアル ポート • 前面パネルに 1 つの Video Graphics Array（VGA）ポート • 重量：24.25 ポンド（11.0 kg）～ 28.0 ポンド（12.7 kg）。取り付けられたオプションによって異なります。 • 寸法：1.75 インチ H x 17.3 インチ W x 22.0 インチ D（44.5 mm x 440.0 mm x 559.0 mm）。これらの寸法にはラック ハンドルが含まれません。 • 冷却ファン：5 つ（さらに、電源装置に 2 つ）。 • ラック マウント：スライド レールを使用します（「スライド レールのラックへの取り付け」（P.B-4）を参照）。標準的な 19 インチ（48.3 cm）の 4 支柱装置ラックに取り付けます（提供されたラックマウント ブラケットを使用）。 • 最大動作高度：7000 フィート（2133 m）。 • 動作温度範囲：50 ～ 90 °F（10 ～ 35 °C）最大 3,000 フィート（914.4 m）。50 ～ 90 °F（10 ～ 32 °C）3000 ～ 7000 フィート（914.4 ～ 2133 m）。 • 電源：AC 入力電源用に設定されています。単一のオートレンジ AC 入力電源装置（350 ワット）が搭載されています。 **（注）** 通常、Cisco ISE 3315 アプライアンスは、4 支柱装置ラックに取り付けるためのブラケットまたはレールを含むラックマウント ハードウェア キットとともに出荷されます。詳細については、「Cisco ISE 3300 シリーズ アプライアンスの 4 支柱ラックへのマウント」（P.B-2）を参照してください。	• 図 2-2（P.2-6）、「Cisco ISE 3315 前面パネルの機能」 • 図 2-3（P.2-7）、「Cisco ISE 3315 前面パネルの LED とボタン」 • 図 2-4（P.2-8）、「Cisco ISE 3315 背面パネルの機能」 • 図 2-5（P.2-8）、「Cisco ISE 3315 の背面パネル LED」

1. 同時エンドポイントは、サポートされるユーザとデバイスの合計数を表します。これには、ユーザ、パーソナル コンピュータ、ラップトップ、IP 電話、スマート フォン、ゲーム コンソール、プリンタ、ファクス機、またはその他のネットワーク デバイスを組み合わせることができます。
2. SATA = Serial Advanced Technology Attachment（シリアル ATA）。

表 2-2　Cisco ISE 3355 アプライアンス ハードウェアの概要

ハードウェアおよびサポートの仕様	図
• Cisco ISE 同時エンドポイント サポート：[1] – ポリシー サービス ノードのみ：最大 6,000 – その他のノード タイプまたは組み合わせ：最大 2,000 • シングル プロセッサ：クアッドコア Intel Xeon（Nehalem） • 4 GB RAM • 2 x 300 GB SAS[2] RAID[3] HDD • 4 つの 10/100/1000 LAN ポート（2 つの統合 NIC と 2 つの Gb NIC（PCI-E）） • CD/DVD-ROM ドライブ • 4 つの USB ポート（前面パネルに 1 つ、内部に 1 つ、背面パネルに 2 つ） • 背面パネルに 2 つの Gb イーサネット ポート • 背面パネルに 1 つのシリアル ポート • 2 つの VGA ポート（前面パネルに 1 つ、背面パネルに 1 つ） • Cavium CN-1620-400-NHB-G アクセラレータ カード • 重量：28 ポンド（12.7 kg）～ 34.5 ポンド（15.6 kg）。取り付けられたオプションによって異なります。 • 寸法：1.7 インチ H x 17.3 インチ W x 28.0 インチ D（43 mm x 440.0 mm x 711.4 mm）。これらの寸法にはラック ハンドルが含まれません。 • 冷却ファン：シングルプロセッサ（Cisco ISE 3355）またはデュアルプロセッサ（Cisco ISE 3395）の場合は 6 つ。 • ラック マウント：スライド レールを使用します（「スライド レールのラックへの取り付け」（P.B-4）を参照）。標準的な 19 インチ（48.3 cm）の 4 支柱装置ラックに取り付けます（提供されたラックマウント ブラケットを使用）。 • 最大動作高度：7000 フィート（2133 m）。 • 動作温度範囲：50 ～ 90 °F（10 ～ 35 °C）最大 3000 フィート（914.4 m）。50 ～ 90 °F（10 ～ 32 °C）3000 ～ 7000 フィート（914.4 ～ 2133 m）。 • 電源：AC 入力電源用に設定されています。二重冗長化自動切り替え電源装置（675 ワット）が搭載されています。 **（注）** 通常、Cisco ISE 3355 アプライアンスと Cisco ISE 3395 アプライアンスは、4 支柱装置ラックに取り付けるためのブラケットまたはレールを含むラックマウント ハードウェア キットとともに出荷されます。詳細については、「Cisco ISE 3300 シリーズ アプライアンスの 4 支柱ラックへのマウント」（P.B-2）を参照してください。Cisco ISE 3300 シリーズ アプライアンス向けのラックマウント ハードウェア キットには、2 支柱装置ラックは含まれません。	• 図 2-7（P.2-9）、「Cisco ISE 3355 前面パネルの機能」 • 図 2-8（P.2-10）、「Cisco ISE 3355 前面パネルの LED とボタン」 • 図 2-9（P.2-11）、「Cisco ISE 3355 背面パネルの機能」 • 図 2-10（P.2-13）、「Cisco ISE 3355 の背面パネル LED」

1. 同時エンドポイントは、サポートされるユーザとデバイスの合計数を表します。これには、ユーザ、パーソナル コンピュータ、ラップトップ、IP 電話、スマート フォン、ゲーム コンソール、プリンタ、ファクス機、またはその他のネットワーク デバイスを組み合わせることができます。
2. SAS = Single-Attachment Station。
3. RAID = Redundant Array of Independent Disks。

表 2-3　Cisco ISE 3395 アプライアンス ハードウェアの概要

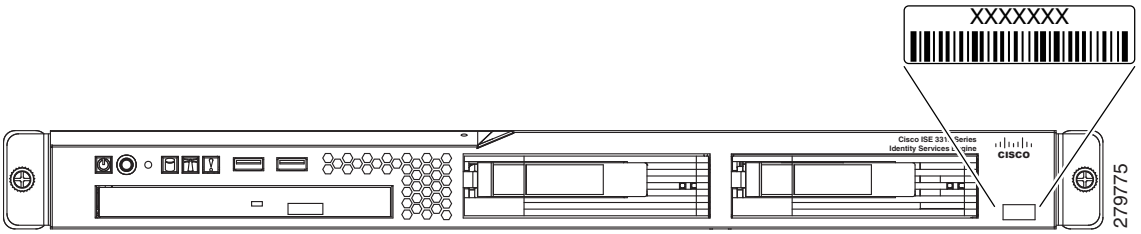
ハードウェアおよびサポートの仕様	図
• Cisco ISE 同時エンドポイント サポート：[1] – ポリシー サービス ノードのみ：最大 10,000 – その他のノード タイプまたは組み合わせ：最大 2,000 • デュアル プロセッサ：2 × クアッドコア Intel Xeon（Nehalem） • 4 GB RAM • 4 x 300 GB SAS RAID HDD • 4 つの 10/100/1000 LAN ポート（2 つの統合 NIC と 2 つの Gb NIC（PCI-E）） • CD/DVD-ROM ドライブ • 4 つの USB ポート（前面パネルに 1 つ、内部に 1 つ、背面パネルに 2 つ） • 背面パネルに 2 つの Gb イーサネット ポート • 背面パネルに 1 つのシリアル ポート • 2 つの VGA ポート（前面パネルに 1 つ、背面パネルに 1 つ） • Cavium CN-1620-400-NHB-G アクセラレータ カード • 重量：28 ポンド（12.7 kg）～ 34.5 ポンド（15.6 kg）。取り付けられたオプションによって異なります。 • 寸法：1.7 インチ H x 17.3 インチ W x 28.0 インチ D（43 mm x 440.0 mm x 711.4 mm）。これらの寸法にはラック ハンドルが含まれません。 • 冷却ファン：シングルプロセッサ（Cisco ISE 3355）またはデュアルプロセッサ（Cisco ISE 3395）の場合は 6 つ。 • ラック マウント：スライド レールを使用します（「スライド レールのラックへの取り付け」（P.B-4）を参照）。標準的な 19 インチ（48.3 cm）の 4 支柱装置ラックに取り付けます（提供されたラックマウント ブラケットを使用）。 • 最大動作高度：7000 フィート（2133 m）。 • 動作温度範囲：50 ～ 90 °F（10 ～ 35 °C）最大 3000 フィート（914.4 m）。50 ～ 90 °F（10 ～ 32 °C）3000 ～ 7000 フィート（914.4 ～ 2133 m）。 • 電源：AC 入力電源用に設定されています。二重冗長化自動切り替え電源装置（675 ワット）が搭載されています。	• 図 2-12（P.2-14）、「Cisco ISE 3395 前面パネルの機能」 • 図 2-13（P.2-15）、「Cisco ISE 3395 前面パネルの LED とボタン」 • 図 2-14（P.2-16）、「Cisco ISE 3395 背面パネルの機能」 • 図 2-15（P.2-17）、「Cisco ISE 3395 の背面パネル LED」

1. 同時エンドポイントは、サポートされるユーザとデバイスの合計数を表します。これには、ユーザ、パーソナル コンピュータ、ラップトップ、IP 電話、スマート フォン、ゲーム コンソール、プリンタ、ファクス機、またはその他のネットワーク デバイスを組み合わせることができます。

Cisco ISE 3315 のシリアル番号の場所

シリアル番号のラベルは、Cisco ISE 3315 の前面パネルの左下にあります（図 2-1 を参照）。

図 2-1　　Cisco ISE 3315 アプライアンスのシリアル番号の場所



（注） Cisco ISE 3315 のシリアル番号は、Cisco Unique Device Identifier（UDI）の仕様により定義され、この仕様に従います。

Cisco ISE 3315 の前面および背面パネル

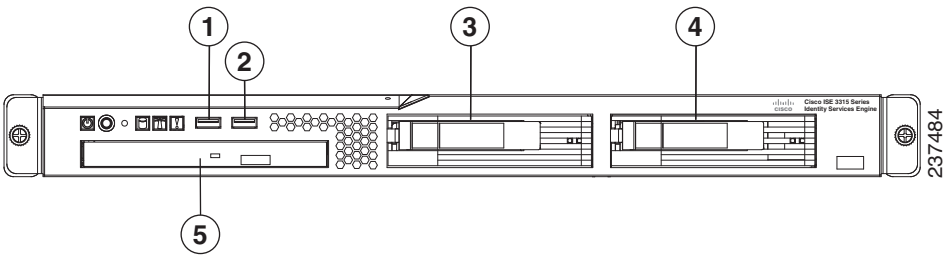
Cisco ISE 3315 プラットフォームは、最大 3 つの追加アプライアンスまたは 3 つのハイ アベイラビリティ ペアを管理する展開に推奨されます。Cisco ISE 3315 には、NIC インターフェイスの柔軟な選択や、ハイ アベイラビリティ構成での使用を実現する 4 つのネットワーク インターフェイスが搭載されています。詳細については、「Cisco ISE シリーズ アプライアンス」（P.2-1）を参照してください。

（注） 同時エンドポイントは、サポートされるユーザとデバイスの合計数を表します。これには、ユーザ、パーソナル コンピュータ、ラップトップ、IP 電話、スマート フォン、ゲーム コンソール、プリンタ、ファクス機、またはその他のネットワーク デバイスを組み合わせることができます。

Cisco ISE 3315 前面パネルの機能

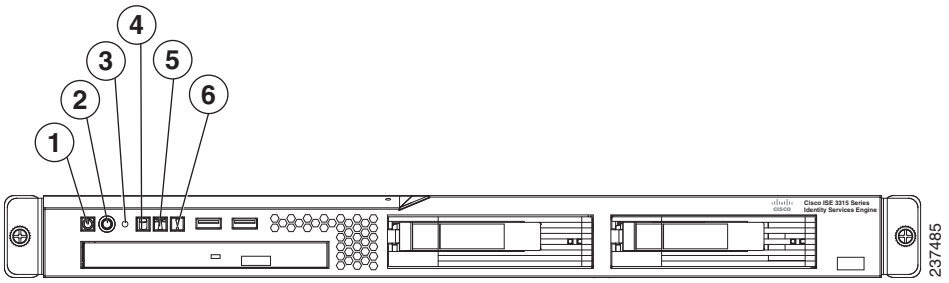
図 2-2、図 2-3、およびそれらの図とともに提供される表は、Cisco ISE 3315 前面パネルの機能、LED、およびボタンを示し、それらについて説明しています。

図 2-2　　Cisco ISE 3315 前面パネルの機能



1	前面 USB ポート 1	4	HDD ベイ 1
2	前面 USB ポート 2	5	CD-ROM/DVD ドライブ
3	ハード ディスク ドライブ（HDD）ベイ 0		

図 2-3　Cisco ISE 3315 前面パネルの LED とボタン

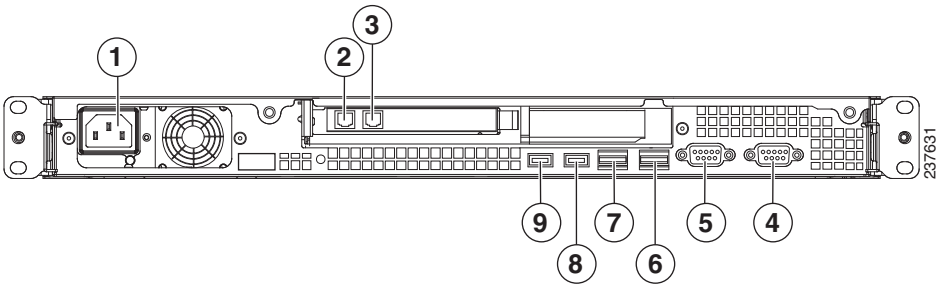


1	電源ステータス LED	緑色 = アプライアンスに AC 電源が接続され、電源が投入されています。 消灯 = アプライアンスの電源が入っていません（AC 電源の切断）。
2	電源ボタン	(埋め込み型)。
3	リセット ボタン	(埋め込み型)。
4	HDD アクティビティ LED	緑色の点滅 = ドライブが動作中です。 消灯 = ドライブが動作していません。
5	ロケータ ボタンまたは LED	青色の点滅 = ロケータ ボタンが押されました。
6	システム ヘルス LED	消灯 = システムが正常な状態です。 オレンジ色 = 障害予測システムしきい値に達しました。これは、次のいずれかの状況によって引き起こされることがあります。 • 少なくとも 1 つのファン（システム ファンまたはプロセッサ ファン）で障害が発生しました。 • 少なくとも 1 つの温度センサー（システム温度センサーまたはプロセッサ温度センサー）が危険なレベルに達しました。 • 少なくとも 1 つのメモリ モジュールで障害が発生しました。 • 電源装置ユニットでエラーが発生しました。

Cisco ISE 3315 背面パネルの機能

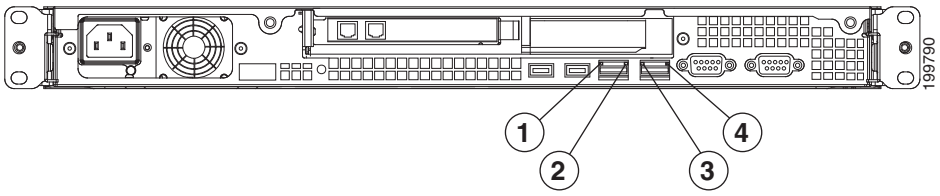
図 2-4、図 2-5、およびそれらの図とともに提供される表は、Cisco ISE 3315 背面パネルの機能および LED を示し、それらについて説明しています。

図 2-4　Cisco ISE 3315 背面パネルの機能



1	AC 電源装置ケーブル ソケット	6	NIC 2（eth1）ギガビット イーサネット インターフェイス
2	NIC 3（eth2）アドオン カード	7	NIC 1（eth0）ギガビット イーサネット インターフェイス
3	NIC 4（eth3）アドオン カード	8	背面 USB ポート 4
4	シリアル ポート	9	背面 USB ポート 3
5	ビデオ ポート		

図 2-5　Cisco ISE 3315 の背面パネル LED

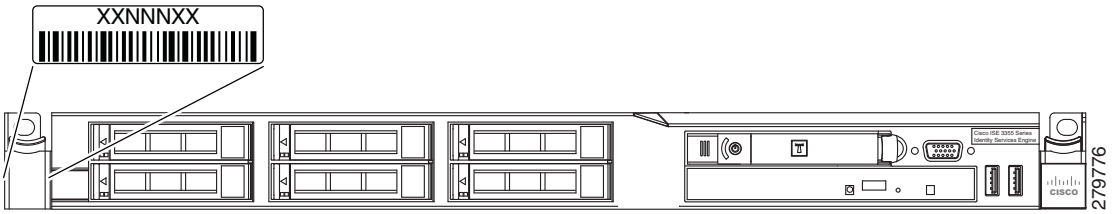


1	NIC 1（eth0）アクティビティ LED	緑色 = アクティビティが存在します。 緑色の点滅 = アクティビティが存在します。 消灯 = アクティビティが存在しません。
2	NIC 1（eth0）リンク LED	緑色 = リンクが存在します。 消灯 = リンクが存在しません。
3	NIC 2（eth1）アクティビティ LED	緑色 = アクティビティが存在します。 緑色の点滅 = アクティビティが存在します。 消灯 = アクティビティが存在しません。
4	NIC 2（eth1）リンク LED	緑色 = リンクが存在します。 消灯 = リンクが存在しません。

Cisco ISE 3355 のシリアル番号の場所

シリアル番号のラベルは、Cisco ISE 3355 の前面パネルの左下にあります（図 2-6 を参照）。

図 2-6　　Cisco ISE 3355 アプライアンスのシリアル番号の場所



（注）　Cisco ISE 3355 のシリアル番号は、Cisco UDI の仕様により定義され、この仕様に従います。

Cisco ISE 3355 の前面および背面パネル

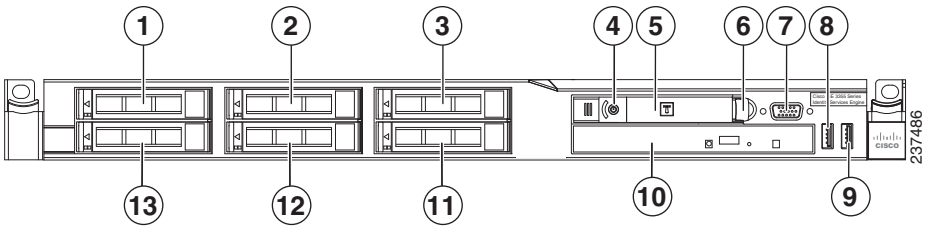
Cisco ISE 3355 プラットフォームは、最大 20 の他のアプライアンスまたはハイ アベイラビリティ ペアを管理する企業全体の展開に対して拡張機能を提供します。Cisco ISE 3315 と同様に、Cisco ISE 3355 には、NIC インターフェイスの柔軟な選択や、ハイ アベイラビリティ構成での使用を実現する 4 つのネットワーク インターフェイスが搭載されています。

また、Cisco ISE 3355 は、4 GB の RAM、RAID 0 および 1 で設定された 2 つの SAS ドライブ、デュアル電源装置、および大規模なネットワーク展開のために Secure Sockets Layer（SSL）をサポートする Cavium CN-1620-400-NHB-G アクセラレータ カードを提供し、ネットワーク コアでの展開の集中管理の信頼性を強化します。詳細については、「Cisco ISE シリーズ アプライアンス」（P.2-1）を参照してください。

Cisco ISE 3355 前面パネルの機能

図 2-7、図 2-8、およびそれらの図とともに提供される表は、Cisco ISE 3355 前面パネルの機能、LED、およびボタンを示し、それらについて説明しています。

図 2-7　　Cisco ISE 3355 前面パネルの機能

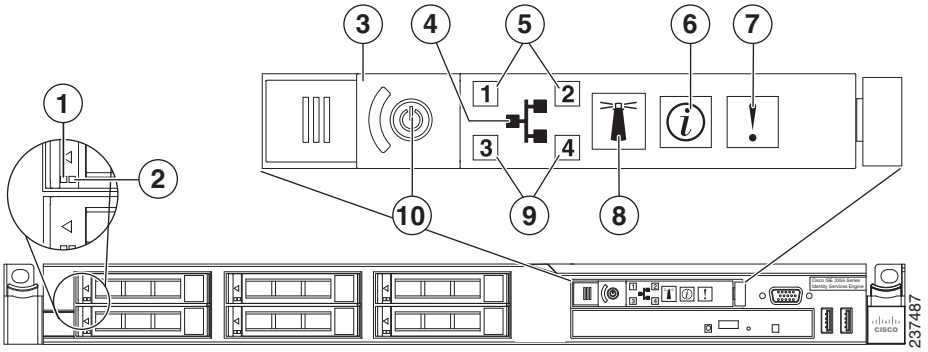


1	HDD ベイ 0	**8**	前面 USB ポート 1
2	空の（未使用）HDD ベイ[1]	**9**	前面 USB ポート 2
3	空の（未使用）HDD ベイ[1]	**10**	CD-ROM/DVD ドライブ
4	LED インジケータ付き電源ボタン （2 色：緑色またはオレンジ色）	**11**	空の（未使用）HDD ベイ[1]

5	オペレータ情報パネル	**12**	空の（未使用）HDD ベイ [1]
6	オペレータ情報パネル リリース スイッチ	**13**	HDD ベイ 1
7	ビデオ ポート		

1. Cisco ISE 3355 アプライアンスに追加のハード ドライブを取り付けることはできません。

図 2-8　　Cisco ISE 3355 前面パネルの LED とボタン



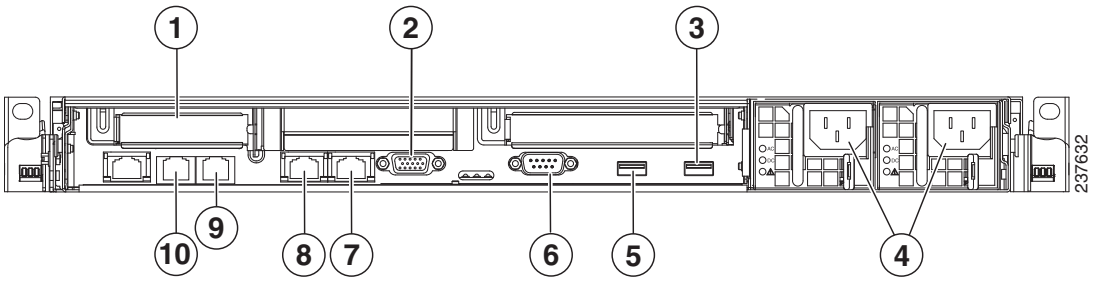
1	HDD アクティビティ LED	緑色 = ハード ディスク ドライブが動作しています。 緑色の点滅 = ハード ディスク ドライブが動作しています。 消灯 = ハード ディスク ドライブがアイドル状態か無効です。
2	HDD ステータス LED	オレンジ色 = ハード ディスク ドライブがエラー状態です。 消灯 = ハード ディスク ドライブが機能しているか、電源から切断されています。
3	電源スイッチ ボタン カバー	カバーを左または右にスライドして、電源スイッチを露出または保護します。
4	イーサネット アイコン LED	緑色 = イーサネット インターフェイスが設定され、アップ状態になっています。 消灯 = イーサネット インターフェイスが現在設定されていないか、すべてダウン状態になっています。
5	イーサネット インターフェイス アクティビティ LED（NIC 1 および NIC 2）	緑色 = アクティビティが存在します。 緑色の点滅 = アクティビティが存在します。 消灯 = アクティビティが存在しません。
6	情報 LED	オレンジ色 = 重大ではないシステム イベントが発生しました。 消灯 = システムは正常に動作しています。

7	システム ヘルス LED	消灯 = システムが正常な状態です。 オレンジ色 = 障害予測システムしきい値に達しました。これは、次のいずれかの状況によって引き起こされることがあります。 • 少なくとも 1 つのファン（システム ファンまたはプロセッサ ファン）で障害が発生しました。 • 少なくとも 1 つの温度センサー（システム温度センサーまたはプロセッサ温度センサー）が危険なレベルに達しました。 • 少なくとも 1 つのメモリ モジュールで障害が発生しました。 • 電源装置ユニットでエラーが発生しました。
8	前面ロケータ ボタンまたは LED	青色の点滅 = ロケータ ボタンが押されました。
9	イーサネット インターフェイス アクティビティ LED（NIC 3 および NIC 4）	緑色 = アクティビティが存在します。 緑色の点滅 = アクティビティが存在します。 消灯 = アクティビティが存在しません。
10	LED 付き電源ボタン	緑色 = アプライアンスに AC 電源が接続され、電源が投入されています。 緑色の短点滅 = アプライアンスはオフ状態であり、まだオンにすることができません。通常、アプライアンスのこの状態は 1 ～ 3 分間しか続きません。 緑色の長点滅 = アプライアンスは現在オフ状態であり、オンにすることができます。 徐々に退色する緑色の点滅 = アプライアンスはパワーセーブ モードであり、オンにすることができます。 消灯 = アプライアンスの電源が入っていません（AC 電源の切断）。

Cisco ISE 3355 背面パネルの機能

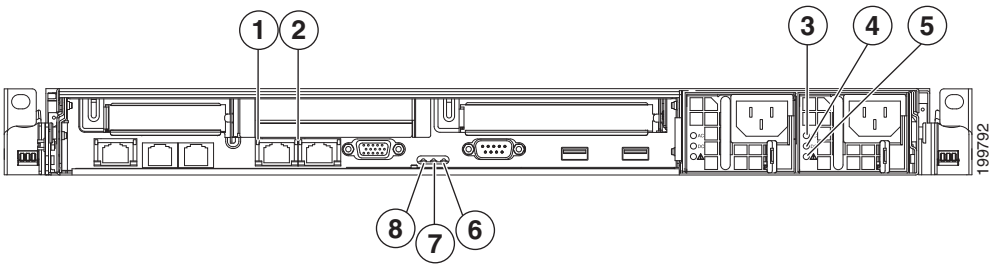
図 2-9、図 2-10、およびそれらの図とともに提供される表は、Cisco ISE 3355 背面パネルの機能および LED を示し、それらについて説明しています。

図 2-9　Cisco ISE 3355 背面パネルの機能



1	空き（未使用）PCI Express スロット	**6**	シリアル ポート（シリアル コンソール、DB9 接続）
2	ビデオ ポート	**7**	NIC 2（eth1）ギガビット イーサネット インターフェイス
3	背面 USB ポート 4	**8**	NIC 1（eth0）ギガビット イーサネット インターフェイス
4	AC 電源装置ケーブル ソケット	**9**	NIC 4（eth3）アドオン カード
5	背面 USB ポート 3	**10**	NIC 3（eth2）アドオン カード

図 2-10　Cisco ISE 3355 の背面パネル LED

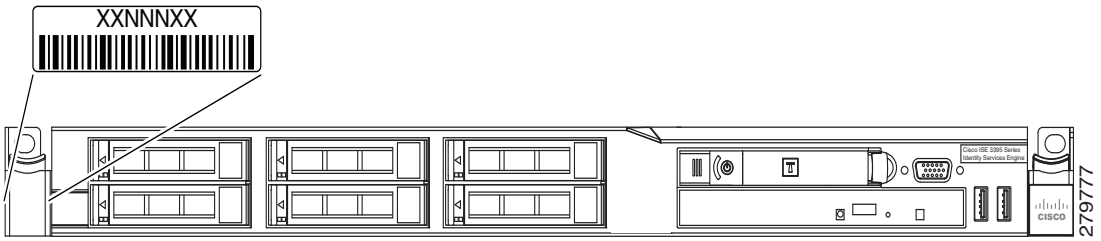


1	NIC 1（eth0）アクティビティ LED	緑色 = アクティビティが存在します。 緑色の点滅 = アクティビティが存在します。 消灯 = アクティビティが存在しません。
2	NIC 1（eth0）リンク LED	緑色 = リンクが存在します。 消灯 = リンクが存在しません。
3	AC 電源 LED	緑色 = AC 電源が電源装置に接続されています。 消灯 = AC 電源が電源装置に接続されていません。
4	DC 電源 LED	緑色 = DC 電源が電源装置に接続されています。 消灯 = DC 電源が電源装置に接続されていません。
5	電源装置エラー LED	オレンジ色 = 電源装置に電力が供給されていますが、電源装置がエラー状態です。 消灯 = 電源装置が正常に機能しているか（AC および DC 電源インジケータが緑色の場合）、または電源装置が切断されています。
6	システム エラー LED	オレンジ色 = システム エラーが発生したことを示しています。 消灯 = システムは正常に動作しています。
7	背面ロケータ LED	青色の点滅 = 前面ロケータ ボタンが押されました。
8	電源 LED	緑色 = アプライアンスに AC 電源が接続され、電源が投入されています。 緑色の短点滅 = アプライアンスはオフ状態であり、まだオンにすることができません。通常、アプライアンスのこの状態は 1 ～ 3 分間しか続きません。 緑色の長点滅 = アプライアンスは現在オフ状態であり、オンにすることができます。 徐々に退色する緑色の点滅 = アプライアンスはパワーセーブ モードであり、オンにすることができます。 消灯 = アプライアンスの電源が入っていません（AC 電源の切断）。

Cisco ISE 3395 のシリアル番号の場所

シリアル番号のラベルは、Cisco ISE 3395 の前面パネルの左下にあります（図 2-11 を参照）。

図 2-11　Cisco ISE 3395 アプライアンスのシリアル番号の場所



（注）　Cisco ISE 3395 のシリアル番号は、Cisco UDI の仕様により定義され、この仕様に従います。

Cisco ISE 3395 の前面および背面パネル

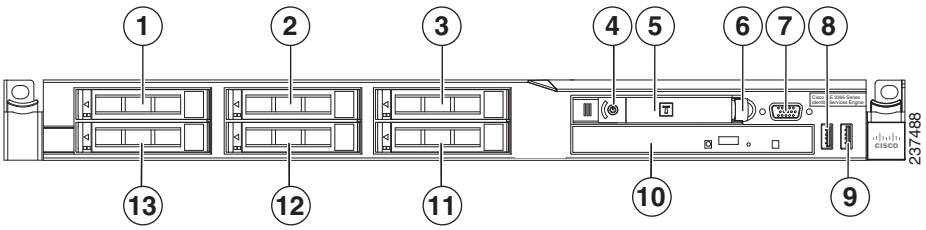
Cisco ISE 3395 アプライアンスは、拡張された処理、メモリ、および最大 40 の追加アプライアンスまたは HA ペアを管理する企業全体の展開に必要な電源を提供します。

Cisco ISE 3395 は、デュアル プロセッサ、デュアル電源装置、4 GB の RAM、4 つの HDD、4 つのネットワーク インターフェイス、および大規模なネットワーク展開のために SSL をサポートする Cavium CN-1620-400-NHB-G アクセラレータ カードを搭載し、ネットワーク コアでの展開の集中管理の信頼性を強化します。詳細については、「Cisco ISE シリーズ アプライアンス」（P.2-1）を参照してください。

Cisco ISE 3395 前面パネルの機能

図 2-12、図 2-13、およびそれらの図とともに提供される表は、Cisco ISE 3355 前面パネルの機能、LED、およびボタンを示し、それらについて説明しています。

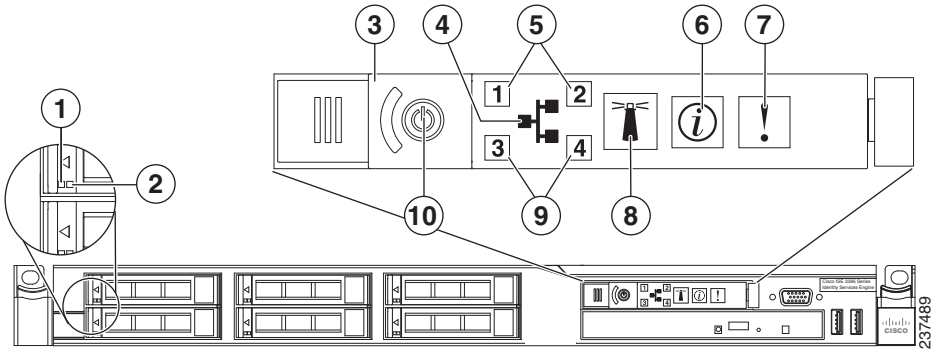
図 2-12　Cisco ISE 3395 前面パネルの機能



1	HDD ベイ 0	**8**	前面 USB ポート 1
2	HDD ベイ 2	**9**	前面 USB ポート 2
3	空の（未使用）HDD ベイ[1]	**10**	CD-ROM/DVD ドライブ
4	LED インジケータ付き電源ボタン （2 色：緑色またはオレンジ色）	**11**	空の（未使用）HDD ベイ[1]
5	オペレータ情報パネル	**12**	HDD ベイ 3
6	オペレータ情報パネル リリース スイッチ	**13**	HDD ベイ 1
7	ビデオ ポート		

1. Cisco ISE 3395 アプライアンスに追加のハード ドライブを取り付けることはできません。

図 2-13　　Cisco ISE 3395 前面パネルの LED とボタン



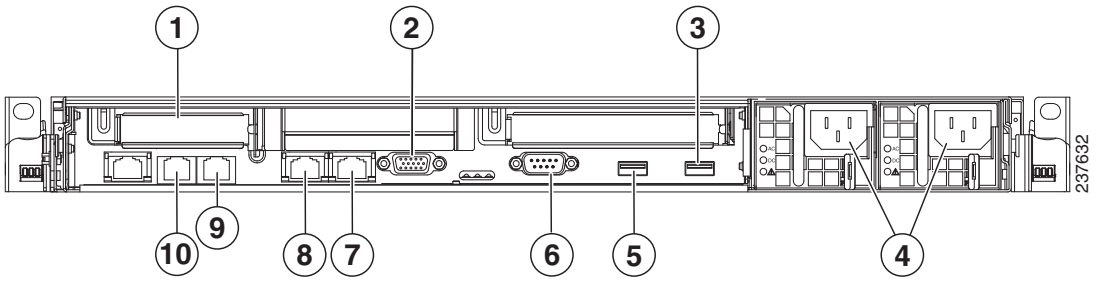
1	HDD アクティビティ LED	緑色 = ハード ディスク ドライブが動作しています。 緑色の点滅 = ハード ディスク ドライブが動作しています。 消灯 = ハード ディスク ドライブがアイドル状態か無効です。
2	HDD ステータス LED	オレンジ色 = ハード ディスク ドライブがエラー状態です。 消灯 = ハード ディスク ドライブが機能しているか、電源から切断されています。
3	電源スイッチ ボタン カバー	カバーを左または右にスライドして、電源スイッチを露出または保護します。
4	イーサネット アイコン LED	緑色 = イーサネット インターフェイスが設定され、アップ状態になっています。 消灯 = イーサネット インターフェイスが現在設定されていないか、イーサネット インターフェイスがすべてダウン状態になっています。
5	イーサネット インターフェイス アクティビティ LED（NIC 1 および NIC 2）	緑色 = アクティビティが存在します。 緑色の点滅 = アクティビティが存在します。 消灯 = アクティビティが存在しません。
6	情報 LED	オレンジ色 = 重大ではないシステム イベントが発生しました。 消灯 = システムは正常に動作しています。

7	システム ヘルス LED	消灯 = システムが正常な状態です。 オレンジ色 = 障害予測システムしきい値に達しました。これは、次のいずれかの状況によって引き起こされることがあります。 • 少なくとも 1 つのファン（システム ファンまたはプロセッサ ファン）で障害が発生しました。 • 少なくとも 1 つの温度センサー（システム温度センサーまたはプロセッサ温度センサー）が危険なレベルに達しました。 • 少なくとも 1 つのメモリ モジュールで障害が発生しました。 • 電源装置ユニットでエラーが発生しました。
8	ロケータ ボタンまたは LED	青色の点滅 = ロケータ ボタンが押されました。
9	イーサネット インターフェイス アクティビティ LED（NIC 3 および NIC 4）	緑色 = アクティビティが存在します。 緑色の点滅 = アクティビティが存在します。 消灯 = アクティビティが存在しません。
10	電源ボタンまたは LED	緑色 = アプライアンスに AC 電源が接続され、電源が投入されています。 緑色の短点滅 = アプライアンスはオフ状態であり、まだオンにすることができません。通常、アプライアンスのこの状態は 1 ～ 3 分間しか続きません。 緑色の長点滅 = アプライアンスは現在オフ状態であり、オンにすることができます。 徐々に退色する緑色の点滅 = アプライアンスはパワーセーブ モードであり、オンにすることができます。 消灯 = アプライアンスの電源が入っていません（AC 電源の切断）。

Cisco ISE 3395 背面パネルの機能

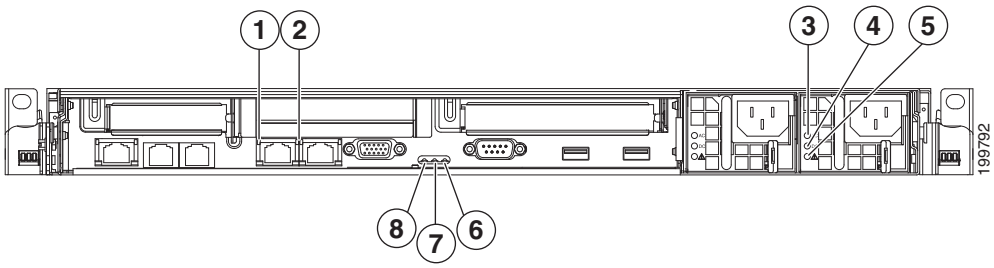
図 2-14、図 2-15、およびそれらの図とともに提供される表は、Cisco ISE 3395 前面パネルの機能、LED、およびボタンを示し、それらについて説明しています。

図 2-14　Cisco ISE 3395 背面パネルの機能



1	空き（未使用）PCI Express スロット	6	シリアル ポート（シリアル コンソール、DB9 接続）
2	ビデオ ポート	7	NIC 2（eth1）ギガビット イーサネット インターフェイス
3	背面 USB ポート 4	8	NIC 1（eth0）ギガビット イーサネット インターフェイス
4	AC 電源装置ケーブル ソケット	9	NIC 4（eth3）アドオン カード
5	背面 USB ポート 3	10	NIC 3（eth2）アドオン カード

図 2-15　Cisco ISE 3395 の背面パネル LED



1	NIC 1（eth0）アクティビティ LED	緑色 = アクティビティが存在します。 緑色の点滅 = アクティビティが存在します。 消灯 = アクティビティが存在しません。
2	NIC 1（eth0）リンク LED	緑色 = リンクが存在します。 消灯 = リンクが存在しません。
3	AC 電源 LED	緑色 = AC 電源が電源装置に接続されています。 消灯 = AC 電源が電源装置に接続されていません。
4	DC 電源 LED	緑色 = DC 電源が電源装置に接続されています。 消灯 = DC 電源が電源装置に接続されていません。
5	電源装置エラー LED	オレンジ色 = 電源装置に電力が供給されていますが、電源装置がエラー状態です。 消灯 = 電源装置が正常に機能しているか（AC および DC 電源インジケータが緑色の場合）、または電源装置が切断されています。

6	システム エラー LED	オレンジ色 = システム エラーが発生したことを示しています。 消灯 = システムは正常に動作しています。
7	背面ロケータ LED	青色の点滅 = 前面ロケータ ボタンが押されました。
8	電源 LED	緑色 = アプライアンスに AC 電源が接続され、電源が投入されています。 緑色の短点滅 = アプライアンスはオフ状態であり、まだオンにすることができません。通常、アプライアンスのこの状態は 1 ～ 3 分間しか続きません。 緑色の長点滅 = アプライアンスは現在オフ状態であり、オンにすることができます。 徐々に退色する緑色の点滅 = アプライアンスはパワーセーブ モードであり、オンにすることができます。 消灯 = アプライアンスの電源が入っていません（AC 電源の切断）。

CHAPTER 3

Cisco ISE 3300 シリーズ アプライアンスの設定

この章では、Cisco Identity Services Engine（ISE）3300 シリーズ アプライアンスの初期設定を実行する方法について説明します。内容は次のとおりです。

（注） Cisco ISE 3300 シリーズ アプライアンスで Cisco ISE ソフトウェアの設定を試みる前に、この章の設定の前提条件を確認する必要があります。

Cisco ISE 3300 シリーズ アプライアンスを設定する前に

Cisco ISE 3300 シリーズ アプライアンスには、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）および Cisco ISE リリース 1.1 ソフトウェアがあらかじめインストールされています。Cisco ADE-OS と Cisco ISE ソフトウェアは、専用の Cisco ISE アプライアンス（Cisco ISE 3300 シリーズ）にあらかじめインストールされています。また、このリリースでは VMware サーバにインストールすることもできます。

手順を進める前に、各アプライアンスまたは VMware インスタンスの以下のすべてのコンフィギュレーションの設定を特定していることを確認します。

- ホスト名
- ギガビット イーサネット 0（eth0）インターフェイスの IP アドレス
- ネットマスク
- デフォルト ゲートウェイ
- DNS ドメイン
- プライマリ ネーム サーバ
- プライマリ ネットワーク タイム プロトコル（NTP）サーバ
- システム時間帯

- ユーザ名（CLI 管理ユーザのユーザ名）
- パスワード（CLI 管理ユーザのパスワード）
- データベース管理者のパスワードおよびデータベース ユーザのパスワード（ワンタイム エントリのみ）

CLI 管理ユーザと Web ベース管理ユーザの権限の違いの詳細については、「CLI 管理ユーザと Web ベース管理ユーザの admin 権限の違い」（P.3-2）を参照してください。

CLI 管理ユーザと Web ベース管理ユーザの admin 権限の違い

Cisco ISE セットアップ プログラムを使用して設定したユーザ名およびパスワードは、Cisco ISE CLI および Cisco ISE Web インターフェイスでの管理アクセスでの使用を意図しています。Cisco ISE CLI にアクセスできる管理者を CLI 管理ユーザといいます。デフォルトでは、CLI 管理ユーザのユーザ名は **admin**、パスワードはセットアップ プロセスでユーザが定義したパスワードです。デフォルトのパスワードはありません。

CLI 管理ユーザのユーザ名、およびセットアップ プロセスで定義したパスワードを使用して、Cisco ISE Web インターフェイスに最初にアクセスできます。Web ベース admin のデフォルトのユーザ名およびパスワードはありません。

CLI 管理ユーザは、Cisco ISE の Web ベースの管理ユーザ データベースに *コピー*されます。最初の CLI 管理ユーザのみが Web ベースの管理ユーザとしてコピーされます。両方の管理ロールで同じユーザ名とパスワードを使用できるように、CLI と Web ベースの管理ユーザ ストアは同期を保持する必要があります。

追加の Web ベースの管理ユーザはユーザ インターフェイスから追加できます。さらに詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の「Configuring Cisco ISE Administrators」を参照してください。

Cisco ISE CLI 管理ユーザは、Cisco ISE Web ベースの管理ユーザとは異なる権限と機能を持ち、追加のタスクを実行できます。

CLI 管理ユーザおよび Web ベース管理ユーザによって実行されるタスク

CLI 管理ユーザおよび Web ベース管理ユーザは、次の Cisco ISE システム関連タスクを実行できます。

- Cisco ISE アプリケーション データをバックアップする。
- Cisco ISE アプライアンス上でシステム、アプリケーション、または診断ログを表示する。
- Cisco ISE ソフトウェア パッチ、メンテナンス リリース、およびアップグレードを適用する。
- NTP サーバ コンフィギュレーションを設定する。

CLI 管理ユーザによってのみ実行されるタスク

CLI 管理ユーザのみが、次の Cisco ISE システム関連タスクを実行できます。

- Cisco ISE アプリケーション ソフトウェアを起動および停止する。
- Cisco ISE アプライアンスをリロードまたはシャットダウンする。
- ロックアウトした場合、Web ベースの管理ユーザをリセットする。詳細については、「管理者のロックアウトによるパスワードの無効化」（P.6-15）を参照してください。

Cisco ISE CLI にアクセスするユーザのみを明示的に作成し、CLI 管理ユーザの資格情報を保護することを推奨します。

（注）　Cisco ISE ユーザ インターフェイスを使用して作成された Web ベース管理ユーザは、Cisco ISE CLI に自動的にログインできません。これらの権限を持つように明示的に作成された CLI 管理ユーザのみが、Cisco ISE CLI にアクセスできます。

詳細については、「Web ブラウザを使用した Cisco ISE へのアクセス」（P.6-7）を参照してください。

他の CLI 管理ユーザを作成するには、まず CLI 管理ユーザとして Cisco ISE CLI にログインし、次のタスクを実行します。

ステップ 1　セットアップ プロセスで作成した CLI 管理ユーザ名とパスワードを使用してログインします。

ステップ 2　**コンフィギュレーション** モードを開始します。

ステップ 3　**username** コマンドを実行します。

（注）　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。

セットアップ プログラムのパラメータについて

Cisco ISE セットアップ プログラムを実行して Cisco ISE ソフトウェアを設定する場合、対話形式の CLI が起動し、システムの設定に必要なパラメータの入力を求めるプロンプトが表示されます（表 3-1 を参照）。サポートされるハードウェア アプライアンスへの接続を確立してセットアップ プログラムを実行する方法は、いくつかあります。

- ハードウェア アプライアンスへのネットワークベースのコンソール接続を使用する。
- アプライアンスの背面パネルへのローカル シリアル コンソール ケーブル接続を使用する。
- アプライアンスへのローカル キーボードおよびビデオ（VGA）接続を使用する。

これらの方法により、アプライアンス管理者の資格情報の最初のセットを作成する初期ネットワークを設定できます。セットアップ プログラムの使用は一度だけ実行する設定作業です。

（注）　次の手順は、推奨手順に従って、サポートされているアプライアンスを適切にインストール、接続、および電源投入していることを前提としています。VMware サーバの設定については、「Cisco Identity Services Engine ISE ソフトウェア DVD を使用した VMware システムの設定」（P.4-12）を参照してください。

表 3-1　セットアップ用の Identity Services Engine ネットワーク設定パラメータ

プロンプト	説明	例
ホスト名（Hostname）	19 文字以下にする必要があります。有効な文字は、英数字（A ～ Z、a ～ z、0 ～ 9）とハイフン（-）で、最初の文字はアルファベット文字でなければなりません。	isebeta1
（eth0）イーサネット インターフェイス アドレス（(eth0) Ethernet interface address）	ギガビット イーサネット 0（eth0）インターフェイスの有効な IPv4 アドレスでなければなりません。	10.12.13.14
ネットマスク（Netmask）	有効な IPv4 ネットマスクでなければなりません。	255.255.255.0
デフォルト ゲートウェイ（Default gateway）	デフォルト ゲートウェイの有効な IPv4 アドレスでなければなりません。	10.12.13.1
DNS ドメイン名（DNS domain name）	IP アドレスは入力できません。有効な文字は、ASCII 文字、数値、ハイフン（-）、およびピリオド（.）です。	mycompany.com
プライマリ ネーム サーバ（Primary name server）	プライマリ ネーム サーバの有効な IPv4 アドレスでなければなりません。	10.15.20.25
別のネーム サーバの追加 / 編集（Add/Edit another name server）	追加のネーム サーバの有効な IPv4 アドレスでなければなりません。	（オプション）複数のネーム サーバを設定できます。これを行うには、**y** を入力して続行します。
プライマリ NTP サーバ（Primary NTP server）	NTP サーバの有効な IPv4 アドレスまたはホスト名でなければなりません。	clock.nist.gov
別の NTP サーバの追加 / 編集（Add/Edit another NTP server）	有効な NTP ドメインでなければなりません。	（オプション）複数の NTP サーバを設定できます。これを行うには、**y** を入力して続行します。
システム時間帯（System Time Zone）	有効な時間帯でなければなりません。詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4*』に記載されている Cisco ISE がサポートする時間帯のリストを参照してください。たとえば、太平洋標準時（PST）の場合は、PST8PDT（または UTC-8 時間）です。 **（注）** このハイパーリンクで参照される時間帯は、最も頻繁に使用される時間帯です。サポートされている時間帯のすべてのリストについては、Cisco ISE CLI から **show timezones** コマンドを実行できます。	UTC（デフォルト）
ユーザ名	Cisco ISE システムへの CLI アクセスに使用される管理者ユーザ名を特定します。デフォルト（**admin**）を使用しない場合は、新しいユーザ名を作成する必要があります。ユーザ名は 3 ～ 8 文字で、有効な英数字（A ～ Z、a ～ z、0 ～ 9）で構成されている必要があります。	admin（デフォルト）

表 3-1　セットアップ用の Identity Services Engine ネットワーク設定パラメータ （続き）

プロンプト	説明	例
パスワード	Cisco ISE システムへの CLI アクセスに使用される管理者パスワードを特定します。このパスワードは作成する必要があります（デフォルトはありません）。パスワードは最低 6 文字で、小文字（a ～ z）、大文字（A ～ Z）、数字（0 ～ 9）がそれぞれ 1 つ以上含まれている必要があります。	MyIseYP@@ss
データベース管理者のパスワード（Database Administrator Password）	Cisco ISE データベースのシステム レベルのパスワードを特定します。このパスワードは作成する必要があります（デフォルトはありません）。パスワードは最低 11 文字で、小文字（a ～ z）、大文字（A ～ Z）、数字（0 ～ 9）がそれぞれ 1 つ以上含まれている必要があります。使用可能な文字のリストには、アンダースコア（_）およびポンド（#）キーも含まれます。 （注）　分散環境のすべてのノードに同じパスワードが必要であるため、必ず同じエントリを使用してすべてのノードを設定してください。このパスワードの設定後、Cisco ISE はこれを「内部的に」使用します。つまり、システムのログイン時にこのパスワードを入力する必要はありません。	ISE4adbp_ss
データベース ユーザのパスワード（Database User Password）	Cisco ISE データベースのアクセス レベルのパスワードを特定します。このパスワードは作成する必要があります（デフォルトはありません）。パスワードは最低 11 文字で、小文字（a ～ z）、大文字（A ～ Z）、数字（0 ～ 9）がそれぞれ 1 つ以上含まれている必要があります。使用可能な文字のリストには、アンダースコア（_）およびポンド（#）キーも含まれます。 （注）　分散環境のすべてのノードに同じパスワードが必要であるため、必ず同じエントリを使用してすべてのノードを設定してください。このパスワードの設定後、Cisco ISE はこれを「内部的に」使用します。つまり、システムのログイン時にこのパスワードを入力する必要はありません。	ISE5udbp#ss

（注）　Web ベースの管理者のユーザ名およびパスワードの詳細については、「Web ブラウザを使用した設定の確認」（P.6-10）を参照してください。

VMware サーバに Cisco ISE ソフトウェアをインストールしている場合は、Cisco ISE は初期セットアップ中に VMware ツールもインストールおよび設定します。Cisco ISE は VMware ツール バージョン 8.3.2 をインストールします。VMware ツールが正しくインストールされたことを確認するには、「VMware ツールのインストールの確認」（P.6-12）を参照してください。

Cisco ISE 3300 シリーズ ハードウェア アプライアンスの設定

この項では、サポートされているハードウェア アプライアンス用に Cisco ISE 3300 シリーズ ソフトウェアを設定するための Cisco ISE セットアップ プログラムの実行について説明します。

セットアップ プログラムを使用して Cisco ISE 3300 シリーズ アプライアンスを設定するには、次の手順を実行します。

ステップ 1　キーボードと VGA モニタを Cisco ISE 3300 シリーズ アプライアンスに接続します。

ステップ 2　電源コードが Cisco ISE 3300 シリーズに接続されており、アプライアンスがオンであることを確認します。

（注） Cisco ISE ソフトウェアはすでにアプライアンスにあらかじめインストールされています。*Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD を挿入しないでください。DVD は、アプライアンスのイメージ再適用の実行、または CLI パスワードのリカバリの目的にのみ提供されています。

約 2 分で、次のプロンプトが表示されます。これはブート シーケンスが完了したことを意味します。

```
**********************************************
Please type 'setup' to configure the appliance
**********************************************
```

ステップ 3　プロンプトで、**setup** と入力し、セットアップ プログラムを起動します。ネットワーキング パラメータおよび最初の資格情報の入力を求めるプロンプトが表示されます。次に、セットアップ プログラムとデフォルト プロンプトの例を示します。

（注） Cisco ISE アプライアンスは、UTC 時間帯を使用して内部的に時間を追跡します。特定の時間帯が不明の場合は、Cisco ISE アプライアンスがある都市、地域、または国に基づいて入力します。時間帯の例については、表 3-2、表 3-3、および表 3-4 の表を参照してください。インストール中に、セットアップによりこの設定を求めるプロンプトが表示された時に、希望する時間帯（デフォルトは UTC）を設定することをお勧めします。

注意　インストール後に Cisco ISE アプライアンス上で時間帯を変更すると、そのノード上で Cisco ISE アプリケーションを使用できなくなります。時間帯の変更による影響の詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4*』の付録 A の「clock time zone」を参照してください。

```
Enter hostname[]: ise-server-1
Enter IP address[]: 10.1.1.10
Enter Netmask[]: 255.255.255.0
Enter IP default gateway[]: 172.10.10.10
Enter default DNS domain[]: cisco.com
Enter Primary nameserver[]: 200.150.200.150
Add/Edit another nameserver? Y/N: n
Enter primary NTP domain[]: clock.cisco.com
Add/Edit another NTP domain? Y/N: n
Enter system time zone[]: UTC
Enter username [admin]: admin
Enter password:
Enter password again:
Bringing up the network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use `Ctrl-C' from this point on...
```

```
Virtual machine detected, configuring VMware tools...
Appliance is configured
Installing applications...
Installing ISE...
Application bundle (ise) installed successfully

===Initial Setup for Application: ise===

Welcome to the ISE initial setup. The purpose of this setup is to provision the
internal ISE database. This setup requires you to create database administrator
password and also create a database user password.

Please follow the prompts below to create the database administrator password.

Enter new database admin password:
Confirm new database admin password:
Successfully created database administrator password.

Please follow the prompts below to create the database user password.

Enter new database user password:
Confirm new database user password:
Successfully created database user password.
Running database cloning script...

Generating configuration...
Rebooting...

Welcome to the ISE initial setup. The purpose of this setup is to provision the
internal database. This setup is non-interactive and will take roughly 15
minutes to complete. Please be patient.

Running database cloning script...
Running database network config assistant tool...
Extracting ISE database contents...
Starting ISE database processes...

...
```

（注）「Virtual machine detected, configuring VMware tools...」メッセージは、Cisco ISE が仮想マシンにインストールされている場合のみ表示されます。このメッセージは、Cisco ISE が物理マシンにインストールされている場合は表示されません。

Cisco ISE ソフトウェアの設定後、Cisco ISE システムは自動的にリブートします。Cisco ISE CLI にログインし直すには、セットアップ時に設定した CLI 管理ユーザの資格情報を入力する必要があります。

ステップ 4　Cisco ISE のリブート後、新しいデータベース管理者およびデータベース ユーザのパスワードの入力および確認を求めるプロンプトが表示されます。（分散環境のすべてのノードに同じパスワードが必要であるため、必ず同じエントリを使用してすべてのノードを設定してください）。このプロンプトが表示されます。

```
Welcome to the ISE initial setup. The purpose of this setup is to
provision the internal database. This setup requires you to create
a database administrator password and also create a database user password.

Please follow the prompts below to create the database administrator password.
```

```
Enter new database admin password:
Confirm new database admin password:
Successfully created database administrator password.

Please follow the prompts below to create the database user password.

Enter new database user password:
Confirm new database user password:
Successfully created database user password.

Running database cloning script...
Running database network config assistant tool...
Extracting ISE database contents...
Starting ISE database processes...

...
```

ステップ 5　Cisco ISE CLI シェルにログインし直したら、次の CLI コマンドを実行して、Cisco ISE アプリケーション プロセスのステータスを確認することができます。

```
ise-server/admin# show application status ise

ISE Database listener is running, PID: 4845
ISE Database is running, number of processes: 27
ISE Application Server is running, PID: 6344
ISE M&T Session Database is running, PID: 4502
ISE M&T Log Collector is running, PID: 6652
ISE M&T Log Processor is running, PID: 6738
ISE M&T Alert Process is running, PID: 6542
ise-server/admin#
```

ステップ 6　Cisco ISE アプリケーション サーバが実行中であることを確認した後、次のサポートされている Web ブラウザのいずれかを使用して Cisco ISE ユーザ インターフェイスにログインできます（「Web ブラウザを使用した Cisco ISE へのアクセス」（P.6-7）を参照）。

Web ブラウザを使用して Cisco ISE ユーザ インターフェイスにログインするには、アドレス フィールドに次のように入力します。

```
https://<your-ise-hostname or IP address>/admin/
```

ここで、「your-ise-hostname or IP address」はセットアップ時に Cisco ISE 3300 シリーズ アプライアンスに対して設定したホスト名または IP アドレスを表します。

ステップ 7　Cisco ISE のログイン ウィンドウで、Cisco ISE ユーザ インターフェイスにアクセスするための Web ベース admin ログイン資格情報（ユーザ名およびパスワード）を求めるプロンプトが表示されます。CLI 管理ユーザのユーザ名、およびセットアップ プロセスで定義したパスワードを使用して、Cisco ISE Web インターフェイスに最初にアクセスできます。

Cisco ISE ユーザ インターフェイスにログインしたら、続いて、デバイス、ユーザ ストア、ポリシー、およびその他のコンポーネントを設定できます。

Cisco ISE ユーザ インターフェイスへの Web ベースのアクセスに使用するユーザ名とパスワードの資格情報は、Cisco ISE CLI インターフェイスへのアクセス用にセットアップ時に作成した CLI 管理ユーザの資格情報と同じではありません。これらの 2 種類の管理ユーザの違いの説明については、「CLI 管理ユーザと Web ベース管理ユーザの admin 権限の違い」（P.3-2）を参照してください。

サポートされている時間帯

この項では、欧州、米国およびカナダ、オーストラリア、アジアの共通の UTC 時間帯の詳細を 3 つの表で示しています。

（注）　時間帯の形式は、POSIX または System V です。POSIX 時間帯形式の構文は America/Los_Angeles、一方、System V 時間帯の構文は PST8PDT のようになります。

- 欧州、米国およびカナダの時間帯については、表 3-2 を参照してください。
- オーストラリアの時間帯については、表 3-3 を参照してください。
- アジアの時間帯については、表 3-4 を参照してください。

表 3-2　共通の時間帯

略語または名前	時間帯名
欧州	
GMT、GMT0、GMT-0、GMT+0、UTC、Greenwich、Universal、Zulu	グリニッジ標準時（UTC）
GB	英国
GB-Eire、Eire	アイルランド
WET	西ヨーロッパ時間（UTC）
CET	中央ヨーロッパ標準時（UTC + 1 時間）
EET	東ヨーロッパ時間（UTC + 2 時間）
米国およびカナダ	
EST、EST5EDT	東部標準時、UTC - 5 時間
CST、CST6CDT	中央標準時、UTC - 6 時間
MST、MST7MDT	山岳部標準時、UTC - 7 時間
PST、PST8PDT	太平洋標準時、UTC - 8 時間
HST	ハワイ標準時、UTC - 10 時間

表 3-3　オーストラリアの時間帯

オーストラリア[1]			
ACT[2]	Adelaide	Brisbane	Broken_Hill
Canberra	Currie	Darwin	Hobart
Lord_Howe	Lindeman	LHI[3]	Melbourne

表 3-3　オーストラリアの時間帯 （続き）

オーストラリア[1]			
North	NSW[4]	Perth	Queensland
South	Sydney	Tasmania	Victoria
West	Yancowinna		

1. 国と都市をスラッシュ（/）で区切って入力します（例：Australia/Currie）。
2. ACT = Australian Capital Territory（オーストラリア首都特別地域）
3. LHI = Lord Howe Island（ロード・ハウ諸島）
4. NSW = New South Wales（ニュー サウス ウェールズ）

表 3-4　アジアの時間帯

アジア[1]			
Aden[2]	Almaty	Amman	Anadyr
Aqtau	Aqtobe	Ashgabat	Ashkhabad
Baghdad	Bahrain	Baku	Bangkok
Beirut	Bishkek	Brunei	Kolkata
Choibalsan	Chongqing	Columbo	Damascus
Dhakar	Dili	Dubai	Dushanbe
Gaza	Harbin	Hong_Kong	Hovd
Irkutsk	Istanbul	Jakarta	Jayapura
Jerusalem	Kabul	Kamchatka	Karachi
Kashgar	Katmandu	Kuala_Lumpur	Kuching
Kuwait	Krasnoyarsk		

1. アジアの時間帯には、東アジア、南アジア、東南アジア、西アジア、および中央アジアがあります。
2. 地域と都市または国をスラッシュ（/）で区切って入力します（例：Asia/Aden）。

（注）　Cisco ISE CLI **show timezones** コマンドを使用すると、追加の時間帯を使用できます。この CLI コマンドを実行すると、使用可能なすべての時間帯が表示されます。ネットワークの場所に最適な時間帯を選択します。

設定プロセスの確認

設定プロセスが正しく完了したことを確認するには、次の 2 つの方法のいずれかを使用して Cisco ISE 3300 シリーズ アプライアンスにログインします。

- Web ブラウザ
- Cisco ISE CLI

（注）　インストール後の設定の確認を実行するには、第 6 章「インストール後のタスクの実行」を参照してください。

CHAPTER 4

VMware 仮想マシンにおける Cisco ISE 3300 シリーズ ソフトウェアのインストール

この章では、VMware 仮想マシンにおける Cisco Identity Services Engine（ISE）3300 シリーズ アプライアンス ソフトウェアのインストールのシステム要件について説明します。次のトピックで、インストール プロセスに関する情報を提供します。

（注） インライン ポスチャ ノードは、Cisco ISE 3300 シリーズ アプライアンスでのみサポートされています。VMware サーバ システムではサポートされません。その他の指定されたロールはすべて、VMware 仮想マシン上での使用がサポートされています。

仮想マシン要件

仮想マシンの最小システム要件は、Cisco ISE 3300 シリーズ アプライアンス ハードウェアの設定と同様である必要があります。表 4-1 に、VMware 仮想マシンに Cisco ISE 3300 シリーズ ソフトウェアをインストールするための最小システム要件を示します。

表 4-1　最小 VMware システム要件

要件のタイプ	最小要件
CPU	Intel デュアルコア、2.13 GHz 以上
メモリ	4 GB RAM

表 4-1　最小 VMware システム要件 （続き）

要件のタイプ	最小要件
ハード ディスク	60 ～ 600 GB のディスク ストレージ（サイズは配置およびタスクによって異なります） （注）　Cisco ISE は、VMware 内の単一のディスクにインストールする必要があります。インストールのディスク領域要件を満たすために複数の小さいディスクを使用すると、予期せぬ動作が発生する場合があります。
ディスク コントローラ	SCSI コントローラ
NIC	1 GB の NIC インターフェイスが必要（4 つの NIC を推奨） （注）　設定する任意の NIC のネットワーク接続の作成時は、必ず [アダプタ（Adapter）] ドロップダウン リストから対応する Flexible ネットワーク アダプタを選択してください。このリリースでは、Cisco ISE はすべての NIC の Flexible ネットワーク アダプタをサポートしています。「VMware サーバの設定」（P.4-7）のステップ 9 を参照してください。
ハイパーバイザ	サポートされている VMware のバージョンは次のとおりです。 • VMware ESX 4.0、4.0.1、4.1 • VMware ESXi 4.0、4.0.1、4.1

（注）　VMware サーバ バージョン 2.0 は、Cisco ISE リリース 1.0 の機能のデモンストレーションでのみサポートされており、実稼働環境ではサポートされていません。

（注）　VMware サーバ上で Cisco ISE ソフトウェアを実行する際、評価と実稼働の目的では異なる種類のライセンスが必要になります。ライセンスの詳細については、「ライセンスのインストール」（P.6-1）を参照してください。

表 4-2 に、実稼働環境の配置で VMware サーバを実行するために必要な、最小 Cisco ISE ハード ディスク領域割り当て要件を示します。実稼働環境の配置では、Cisco ISE ソフトウェアの実行に表 4-1 にリストされている、サポートされている VMware ESX および ESXi サーバ バージョンを使用してください。

表 4-2　実稼働環境での最小 VMware ディスク領域要件

ISE ペルソナ	実稼働環境での最小ディスク領域要件
スタンドアロン ISE	200 GB
管理	200 GB
監視	200 GB
管理および監視	200 GB
ポリシー サービス	60 GB

（注）　VMware サーバで監視ペルソナをイネーブルにして Cisco ISE ソフトウェアを実行している場合、小規模、中規模および大規模の実稼働環境の配置でサポートされる最小ハード ディスク領域割り当ては 200 GB です。
Cisco ISE は、VMware 内の単一のディスクにインストールする必要があります。インストールのディスク領域要件を満たすために複数の小さいディスクを使用すると、予期せぬ動作が発生する場合があります。

Cisco ISE リリース 1.0 インストーラは、Cisco ISE ハードウェア アプライアンスでサポートされる最大と等しい最大まで、VMware サーバに割り当てられているすべてのディスク領域を使用するように設計されています。つまり、600 GB を超える VMware サーバを作成する場合、Cisco ISE がすべての配置タイプに割り当てる最大ディスク領域は 600 GB になります。

残りのディスク領域はパーティション化されないままです。次に例を示します。

- VMware サーバが 200 GB のディスク領域割り当てで作成された場合、Cisco ISE インストーラは 200 GB を使用に割り当てます。
- VMware サーバが 1 テラバイト（TB）のディスク領域割り当てで作成された場合、Cisco ISE インストーラは許可される最大（600 GB）まで割り当てます。
- VMware サーバが 40 GB のディスク割り当てで作成された場合、サイズ割り当てがサポートされているディスク領域割り当ての 60 GB を下回っているため、Cisco ISE インストーラは失敗します。

（注）　100 ユーザのみをサポートする評価環境で VMware サーバを実行するための Cisco ISE のハード ディスク領域割り当ての要件は 60 GB です。ただし、VMware サーバを多数のユーザをサポートする実稼働環境に移動する場合は、必ず表 4-2 にリストされている推奨される最小ディスク サイズ以上（許可される最大の 600 GB まで）に Cisco ISE のインストールを再構成してください。

Cisco ISE リリース 1.1 の評価

評価目的の場合、Cisco ISE リリース 1.0 は「仮想マシン要件」（P.4-1）を満たし、サポートされている任意の VMware サーバ仮想マシンにインストールできます。Cisco ISE リリース 1.0 を評価する際に、仮想マシンにあまり多くのディスク領域を設定する必要はありませんが、少なくとも 60 GB の最小ディスク領域を割り当てる必要があります。

評価のために Cisco ISE リリース 1.0 ソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1　次のリンクに移動します。

http://www.cisco.com/go/ise（このリンクにアクセスするには、有効な Cisco.com ログイン クレデンシャルを持っている必要があります）。

ステップ 2　[ソフトウェアのダウンロード（Download Software）] をクリックします。

Cisco ISE リリース 1.0 ソフトウェア イメージには、90 日間の評価ライセンスがすでにインストールされた状態で付属しているため、設置および初期設定が完了すると、すべての Cisco ISE サービスのテストを開始できます。

（注）　評価環境での VMware サーバのインストールがサポートされています。評価環境と実稼働環境の配置で、使用する VMware サーバに必要な最小ディスク領域要件の違いはありません。Cisco ISE でサポートされる最小の VMware サーバのインストールには 60 GB のディスク領域が必要です。

評価システムから完全ライセンスを持つ実稼働環境のシステムに Cisco ISE 設定を移行するには、次のタスクを実行する必要があります。

- 評価版の設定をバックアップする
- 実稼働環境への展開ライセンスをインストールする
- 実稼働環境のシステムに設定を復元する
- インストール用のディスク領域を増やす（可能な場合）

（注）　100 ユーザのみをサポートする評価環境で VMware サーバを実行するための Cisco ISE のハード ディスク領域割り当ての要件は 60 GB です。ただし、VMware サーバを多数のユーザをサポートする実稼働環境に移動する場合は、必ず表 4-2 にリストされている推奨される最小ディスク サイズ以上（許可される最大の 600 GB まで）に Cisco ISE のインストールを再構成してください。

VMware ESX または ESXi サーバの設定

サポートされている VMware サーバに Cisco ISE をインストールするには、VMware 仮想マシンに 60 GB の最小ディスク領域を割り当てる必要があります。この項では、VMware 仮想マシン上で必要な最小ディスク領域を設定する（VMware 仮想マシン上でディスク領域サイズを変更し、VMware ESX サーバにログインする）方法について説明します。この項では、重要な設定に関連するタスクの実行手順を示します。

注意　ストレージ タイプとして VMware シン プロビジョニングを選択しないでください。Cisco ISE ソフトウェアの本リリースでは、サポートされている VMware サーバ（VMware バージョン ESX 4.x または ESXi 4.x）でのストレージ タイプとしての VMware シン プロビジョニングの使用はサポートされていません。これはデフォルトではなく、ステップ 10 のシン プロビジョニングのチェック ボックスの選択について助言しています（図 4-11 を参照）。

（注）　次の手順を実行するには、ログインする必要があります。最初のログインの実行の詳細については、「ログイン」（P.6-8）を参照してください。

ディスク割り当てを確認または変更するには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [メモリ（Memory）] を選択し、[プロパティ（Properties）] を選択します。

ブロック サイズが 256 MB の場合は、4 GB に変更する必要があります。

ステップ 2　ブロック サイズを 4 GB に変更するには、[設定（Configuration）] > [メモリ（Memory）] を選択します。

（注）　VMware 仮想ファイル システム（VMFS）が、VMware ホストで設定されている各ストレージ ボリュームに設定されていることに注意することが重要です。つまり、VMFS ブロック サイズの選択では、VMware ホスト上でホストされる最大の仮想ディスク サイズを考慮する必要があります。ブロック サイズを設定すると、VMFS パーティションを再フォーマットしないと変更することができません。

デフォルト設定を削除するには、次の手順を実行します。

ステップ 1　[削除（Remove）] をクリックします。

確認ウィンドウが表示されます。

ステップ 2　[はい（Yes）] をクリックします。

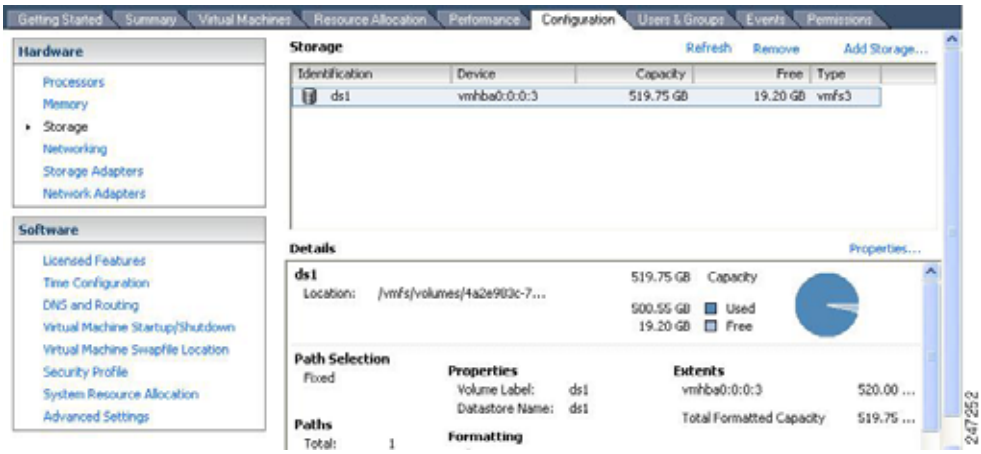
デフォルト設定が削除されます。

新しい仮想ファイル サイズを作成するには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ストレージ（Storage）] > [ストレージの追加ウィザード（Add Storage Wizard）] を選択します。

[ストレージの追加（Add Storage）] ウィザードは [設定（Configuration）] ウィンドウの右上隅にあります。

図 4-1　[設定（Configuration）] ウィンドウ



ステップ 2　[ストレージ タイプ（Storage Type）] ドロップダウン リストから、[ディスク /LUN（Disk/LUN）] を選択して、[次へ（Next）] をクリックします。

ステップ 3　ディスク領域サイズに [60 GB]、VMFS ブロック サイズに [2 MB] を選択し、[次へ（Next）] を選択します。

60 GB は、VMware と Cisco ISE のインストールに必要な最小ディスク領域です。ただし、VMware システムで余分な領域を割り当てた場合でも、Cisco ISE は最大 600 GB のみを使用します。設定する値は、展開に応じて、60 ～ 600 GB でなければなりません。

（注）　デフォルトの VMFS 1 MB ブロック サイズを選択した場合、VMware ホスト上の仮想マシンに 600 GB のディスク領域を作成することはできません。VMFS ファイル システムの作成中に 2 MB の VMFS ブロック サイズを選択することによってのみ、最大 600 GB の仮想マシンのディスク領域を設定できます。

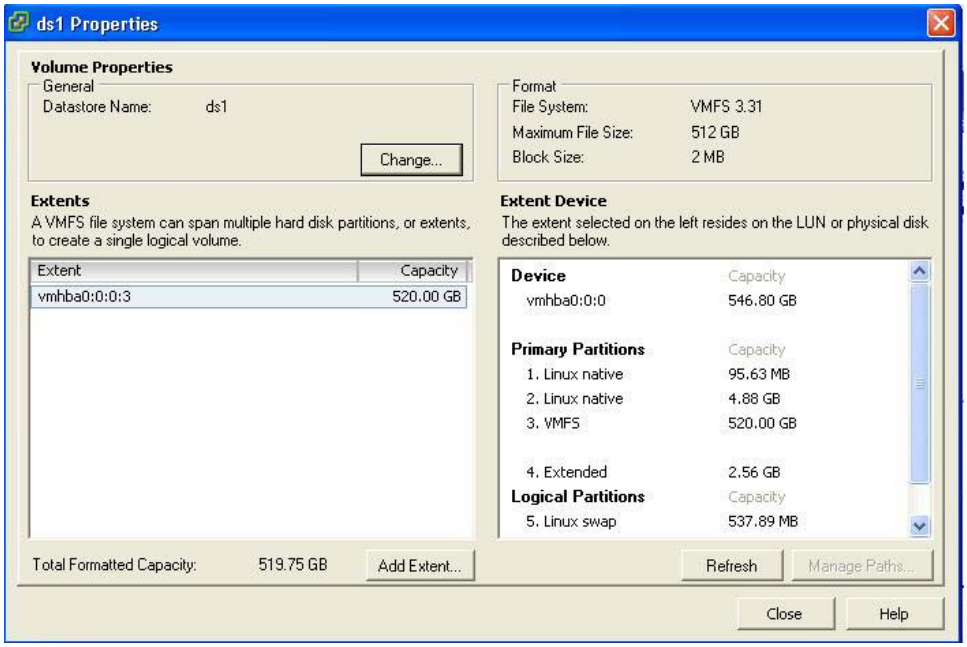
ステップ 4　[終了（Finish）] をクリックします。

60 GB の仮想ディスク サイズと 2 MB のブロック サイズを持つ新しい VMware システムが正常に作成されます。

新しいファイル サイズを確認するには、[設定（Configuration）] > [メモリ（Memory）] を選択して [プロパティ（Properties）] をクリックします。

図 4-2 に、ds1 という名前で作成されるディスク領域のプロパティを示します。

図 4-2　ディスク領域のプロパティ ウィンドウ



VMware システム上で Cisco ISE Profiler サービスを適切に動作させるには、VMware ESX または ESXi サーバ上で VMswitch0 および VMswitch1 インターフェイスを設定する必要があります（図 4-3（P.4-7）を参照）。

Cisco ISE Profiler サービスをサポートするように VMware サーバ インターフェイスを設定するには、次の手順を実行します。

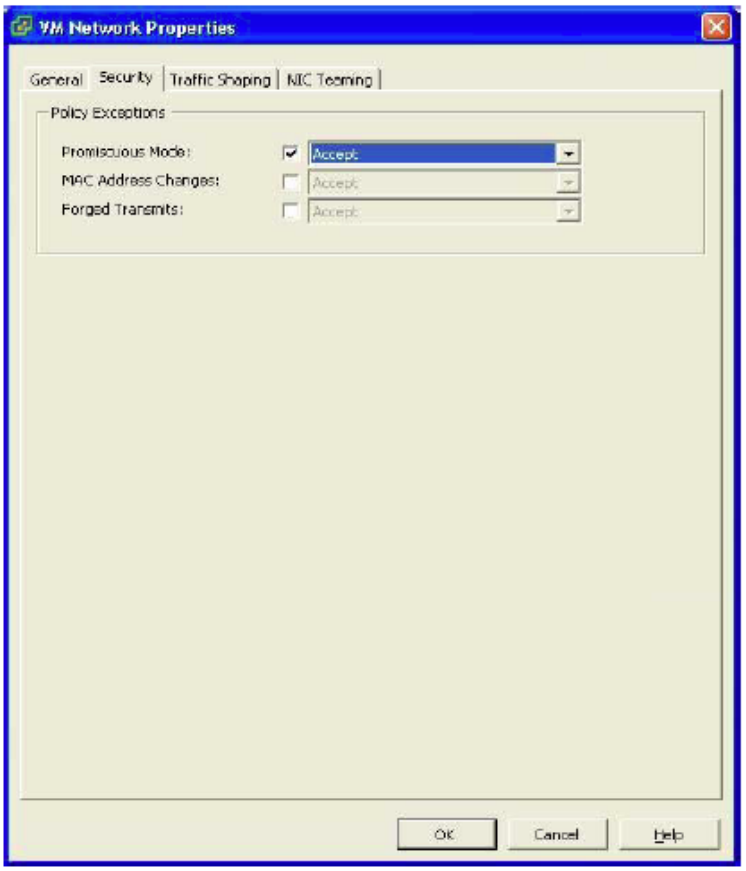
ステップ 1　[設定（Configuration）] > [ネットワーキング（Networking）] > [プロパティ（Properties）] > [VMNetwork]（VMware サーバ インスタンスの名前）> [VMswitch0]（VMware ESX サーバ インターフェイスの 1 つ）> [プロパティ（Properties）] > [セキュリティ（Security）] を選択します。

ステップ 2　[セキュリティ（Security）] タブの下の [ポリシー例外（Policy Exceptions）] ペインで [無差別モード（Promiscuous Mode）] チェックボックスをオンにします。

ステップ 3　隣接するドロップダウン リスト ボックスで [承認（Accept）] を選択して、[OK] をクリックします。

VMswitch1 上で同じ手順を繰り返します（もう一方の VMware ESX サーバ インターフェイス）。

図 4-3　[VMNetwork プロパティ（VMNetwork Properties）] ウィンドウ



VMware サーバの設定

この項では、VMware Infrastructure Client を使用して VMware サーバを設定する方法について説明します。

前提条件

Cisco ISE ソフトウェアのインストール前に、VMware 仮想マシンに最小で 60 GB の割り当てられたディスク領域があることを確認します。詳細については、「VMware ESX または ESXi サーバの設定」（P.4-4）を参照してください。

VMware Infrastructure Client を使用して VMware サーバを設定するには、次の手順を実行します。

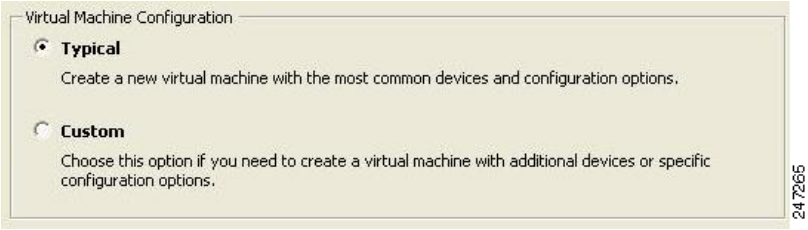
ステップ 1　ESX サーバにログインします。

ステップ 2　VMware Infrastructure Client の左側のペインで、ホスト コンテナを右クリックして、[新規仮想マシン（New Virtual Machine）] を選択します。

[新規仮想マシン（New Virtual Machine）] ウィザードが表示されます。

ステップ 3　[設定タイプ（Configuration Type）] ダイアログボックスで、図 4-4 に示すように VMware 設定として [標準（Typical）] を選択して、[次へ（Next）] をクリックします。

図 4-4　[仮想マシンの設定（Virtual Machine Configuration）] ダイアログボックス



[名前と場所（Name and Location）] ダイアログボックスが表示されます。（図 4-5）。

ステップ 4　VMware システムを参照するための名前を入力して、[次へ（Next）] をクリックします。

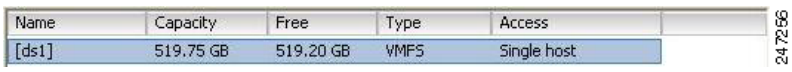
図 4-5　[名前と場所（Name and Location）] ダイアログボックス

ヒント　VMware ホストに使用するホスト名を使用します。

[データストア（Datastore）] ダイアログボックスが表示されます。（図 4-6）。

ステップ 5　最小で 60 GB の空きスペースが使用可能なデータストアを選択して、[次へ（Next）] をクリックします。

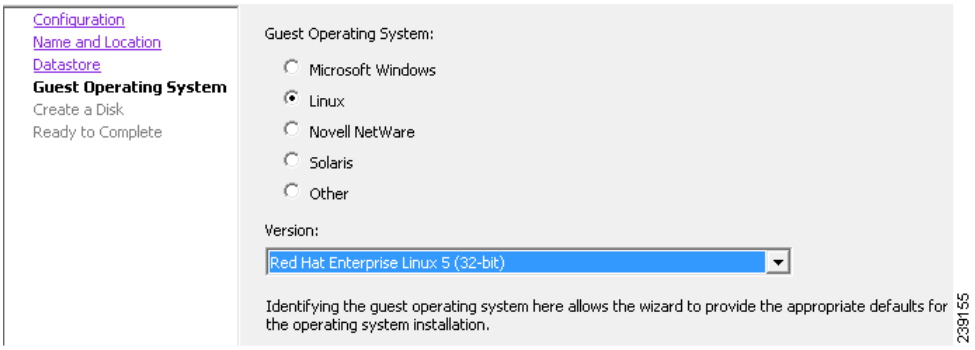
図 4-6　[データストア（Datastore）] ダイアログボックス



[ゲスト オペレーティング システム（Guest Operating System）] ダイアログボックスが表示されます。（図 4-7）。

ステップ 6　[Linux] をクリックし、[バージョン（Version）] ドロップダウン リストから [Red Hat Enterprise Linux 5（32 ビット）（Red Hat Enterprise Linux 5 (32-bit)）] を選択します。

図 4-7　[ゲスト オペレーティング システム（Guest Operating System）] ダイアログボックス



[仮想プロセッサの数（Number of Virtual Processors）] ダイアログボックスが表示されます。（図 4-8）。

ステップ 7　[仮想プロセッサの数（Number of Virtual Processors）] ドロップダウン リストから [2]（2 が使用可能な場合）を選択します。1 を選択することもできます。[次へ（Next）] をクリックします。

図 4-8　[仮想プロセッサの数（Number of Virtual Processors）] ダイアログボックス

[メモリ設定（Memory Configuration）] ダイアログボックスが表示されます。（図 4-9）。

ステップ 8　**4096 MB** と入力して、[次へ（Next）] をクリックします。

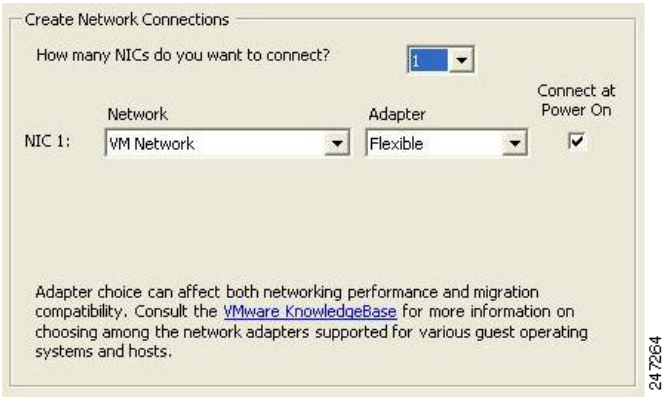
図 4-9　[メモリ設定（Memory Configuration）] ダイアログボックス

[NIC 設定（NIC Configuration）] ダイアログボックスが表示されます。（図 4-10）。

ステップ 9　[NIC 1] を選択して [次へ（Next）] をクリックします。

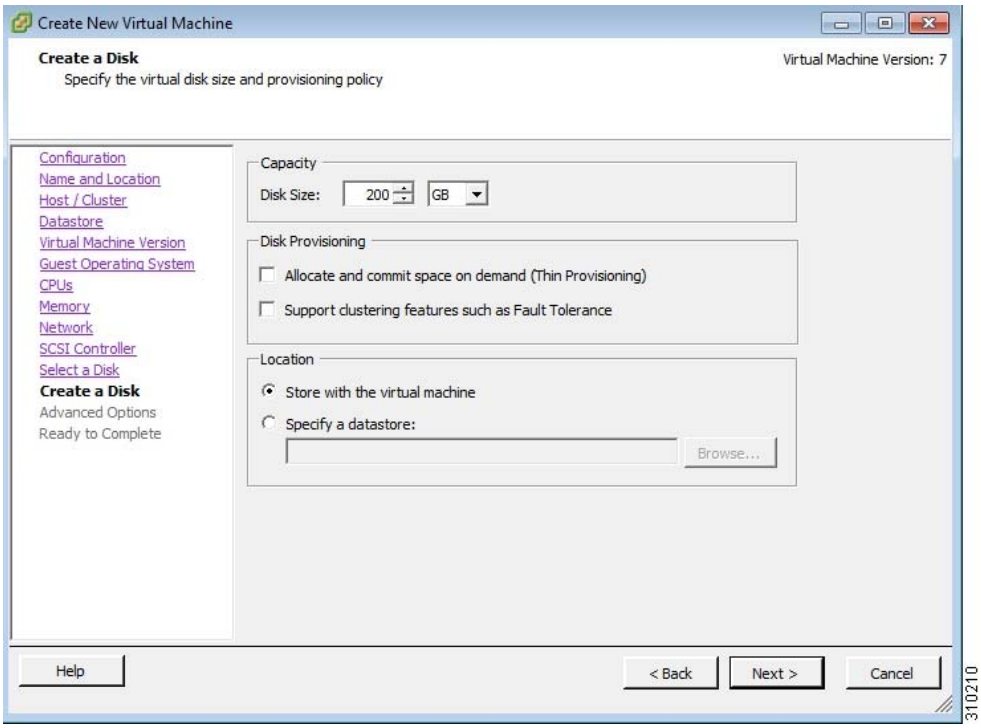
（注）　設定する任意の NIC のネットワーク接続の作成時は、必ず [アダプタ（Adapter）] ドロップダウン リストから対応する Flexible ネットワーク アダプタを選択してください。このリリースでは、Cisco ISE はすべての NIC の Flexible ネットワーク アダプタをサポートしています。

図 4-10　[NIC 設定（NIC Configuration）] ダイアログボックス



[仮想ディスク容量（Virtual Disk Capacity）] ダイアログボックスが表示されます。（図 4-12）。

図 4-11　[ディスク プロビジョニング（Disk Provisioning）] ダイアログ ボックス



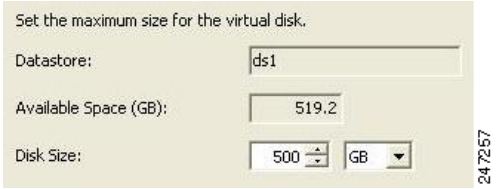
ステップ 10　[ディスク プロビジョニング（Disk Provisioning）] ダイアログボックスで [スペースをオンデマンドで割り当てて確定（シン プロビジョニング）（Allocate and commit space on demand (Thin Provisioning)）] チェックボックスをオンにしないでください（図 4-11）。[次へ（Next）] をクリックして続行します。

[仮想ディスク容量（Virtual Disk Capacity）] ダイアログボックスが表示されます。（図 4-12）。

注意　ストレージ タイプとして VMware シン プロビジョニングを選択しないでください。Cisco ISE ソフトウェアの本リリースでは、サポートされている VMware サーバ（VMware バージョン ESX 4.x または ESXi 4.x）でのストレージ タイプとしての VMware シン プロビジョニングの使用はサポートされていません。これはデフォルト設定ではありません。図 4-11 では、シン プロビジョニングのチェックボックスの選択について助言しています。

ステップ 11　[ディスク サイズ（Disk Size）] フィールドに **500 GB** と入力して、[次へ（Next）] をクリックします。

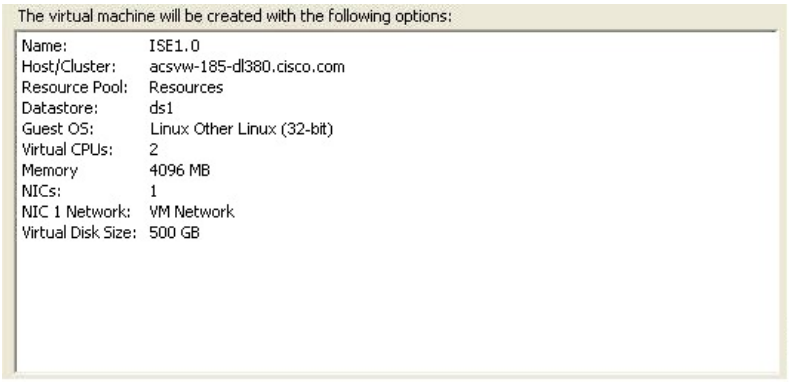
図 4-12　[仮想ディスク容量（Virtual Disk Capacity）] ダイアログボックス



[新規仮想マシンを完了する準備ができました（Ready to Complete New Virtual Machine）] ダイアログボックスが表示されます。（図 4-13）。

ステップ 12　新規作成された VMware システムの名前、ゲスト OS、仮想 CPU、メモリ、および仮想ディスク サイズなど、設定の詳細を確認します。

図 4-13　　[完了する準備ができました（Ready to Complete）] ダイアログボックス



ステップ 13　[終了（Finish）] をクリックします。

これで、VMware システムがインストールされました。

新たに作成した VMware システムをアクティブにするには、左側のペインで VM を右クリックして、[電源オン（Power On）] を選択します。

Cisco ISE ソフトウェアのインストールのための VMware システムの準備

VMware システムを設定すると、Cisco ISE ソフトウェアをインストールする準備ができる状態になります。*Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD から Cisco ISE ソフトウェアをインストールするには、VMware システムを Cisco ISE DVD からブートするように設定する必要があります。これには、VMware システムが仮想 DVD ドライブを使用して *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD からブートするように設定する必要があります。

これは、ご使用のネットワーク環境に応じて異なる方法を使用して実行できます。VMware ESX サーバ ホストの DVD ドライブを使用して VMware システムを設定するには、「Cisco Identity Services Engine ISE ソフトウェア DVD を使用した VMware システムの設定」（P.4-12）を参照してください。

Cisco Identity Services Engine ISE ソフトウェア DVD を使用した VMware システムの設定

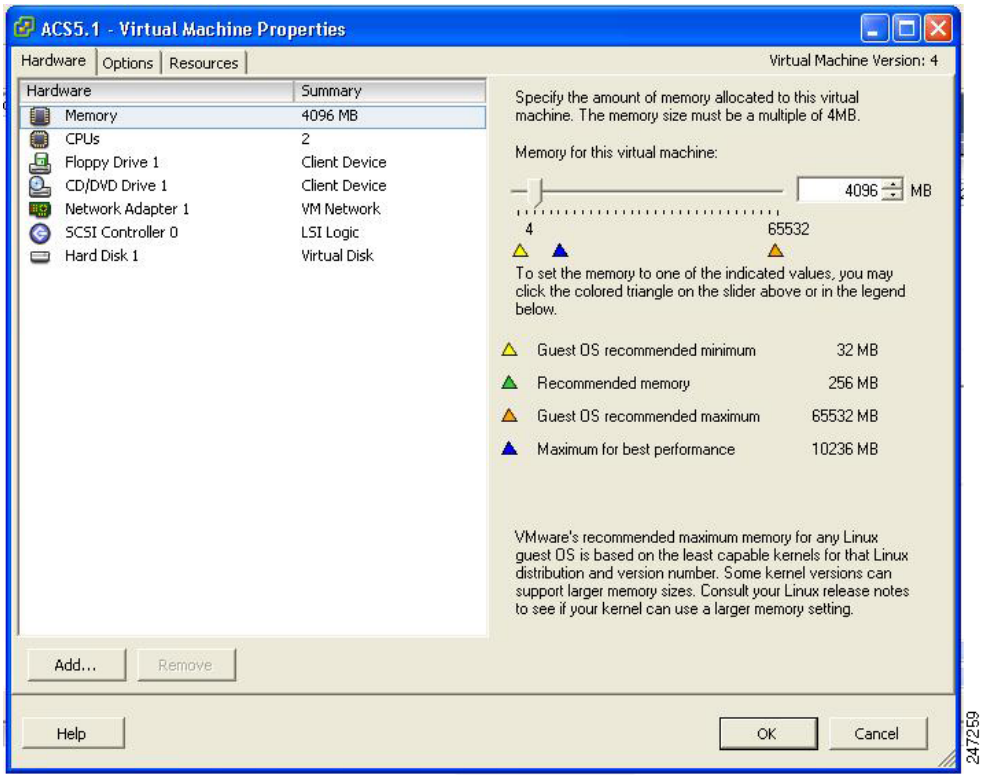
この項では、VMware ESX サーバ ホストの DVD ドライブを使用して、*Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD から VMware システムを起動するように設定する方法について説明します。

DVD ドライブを使用して VMware システムを設定するには、次の手順を実行します。

ステップ 1　VMware Infrastructure Client で、新たに作成した VMware システムを強調表示して、[仮想マシン設定の編集（Edit Virtual Machine Settings）] を選択します。

[仮想マシンのプロパティ（Virtual Machine Properties）] ウィンドウが表示されます。図 4-14 に、Cisco ISE リリース 1.0 の名前で作成される VMware システムのプロパティを示します。

図 4-14　[仮想マシンのプロパティ（Virtual Machine Properties）] ダイアログボックス



ステップ 2　[仮想マシンのプロパティ（Virtual Machine Properties）] ダイアログボックスで、[CD/DVD ドライブ 1（CD/DVD Drive 1）] を選択します。

[CD/DVD ドライブ 1 のプロパティ（CD/DVD Drive1 properties）] ダイアログボックスが表示されます。

ステップ 3　[ホスト デバイス（Host Device）] オプションを選択して、ドロップダウン リストからご使用の DVD ホスト デバイスを選択します。

ステップ 4　[電源オンで接続（Connect at Power On）] オプションを選択して、[OK] をクリックして設定を保存します。

これで、VMware ESX サーバの DVD ドライブを使用して、Cisco ISE ソフトウェアをインストールできるようになりました。

設定が完了したら、[コンソール（Console）] タブをクリックして、左側のペインから [VM] を右クリックして、[電源（Power）]、[リセット（Reset）] の順に選択して、VMware システムを再起動します。

VMware システムへの Cisco ISE ソフトウェアのインストール

この項では、VMware ESX 4.x への Cisco ISE ソフトウェアのインストール プロセスについて説明します。

VMware システムに Cisco ISE ソフトウェアをインストールするには、次の手順を実行します。

ステップ 1　VMware Infrastructure Client にログインします。

ステップ 2　BIOS で協定世界時（UTC）が設定されていることを確認します。

a. VMware システムの電源がオンになっている場合は、システムの電源をオフにします。

b. VMware システムの電源をオンにします。

c. F1 を押して、BIOS セットアップ モードにします。

d. 矢印キーを使用して、[日付と時刻（Date and Time）] に移動し、Enter を押します。

e. アプライアンスの時刻を UTC/ グリニッジ標準時（GMT）時間帯に設定します。

（注） すべての Cisco ISE ノードを UTC 時間帯に設定することを推奨します。この時間帯設定により、展開におけるさまざまなノードからのレポートおよびログが、タイムスタンプで常に同期されるようになります。

f. Esc を押して、メイン BIOS メニューを終了します。

g. Esc を押して、BIOS セットアップ モードを終了します。

（注） インストール後に、永続ライセンスをインストールしない場合、Cisco ISE は自動的に最大 100 エンドポイントをサポートする 90 日間の評価ライセンスをインストールします。

ステップ 3　VMware ESX ホストの CD/DVD ドライブに *Cisco ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD を挿入し、仮想マシンの電源をオンにします。

（注） この DVD へのアクセス権がない場合は、Cisco Software Download サイト（http://www.cisco.com/public/sw-center/index.shtml）から Cisco ISE リリース 1.1 ソフトウェアをダウンロードします。Cisco.com クレデンシャルの提供が求められます。

Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx) DVD のブート時に、コンソールが表示されます。

```
Welcome to Cisco ISE
To boot from the hard disk press <Enter>
Available boot options:
[1] Cisco Identity Services Engine Installation (Monitor/Keyboard)
[2] Cisco Identity Services Engine Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
```

```
Please enter boot option and press <Enter>.
boot: 1
```

初期セットアップを実行するには、モニタとキーボード ポートまたはコンソール ポートのいずれかを選択できます。

ステップ 4　システム プロンプトで、**1** と入力してモニタとキーボード ポートを選択するか、**2** と入力してコンソール ポートを選択し、Enter を押します。

これで、VMware システムへの Cisco ISE ソフトウェアのインストールが開始します。

（注）　インストール プロセスが完了するまで、20 分かかります。

インストール プロセスが終了すると、仮想マシンは自動的に再起動されます。

VM の再起動時に、コンソールに次のように表示されます。

```
Type 'setup' to configure your appliance
localhost:
```

ステップ 5　システム プロンプトで、**setup** と入力し、Enter を押します。

セットアップ ウィザードが表示され、ウィザードに従って初期設定を実行します。セットアップ プロセスの詳細については、「セットアップ プログラムのパラメータについて」（P.3-3）を参照してください。

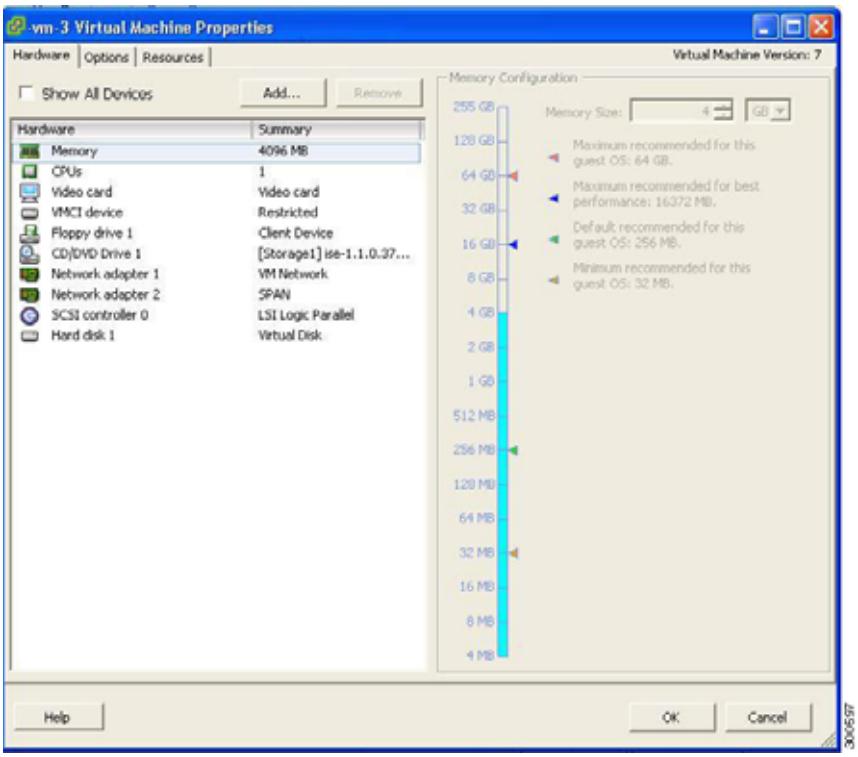
シリアル コンソールを使用した Cisco ISE VMware サーバへの接続

シリアル コンソールを使用して Cisco ISE VMWare サーバに接続するには、次の手順を実行します。

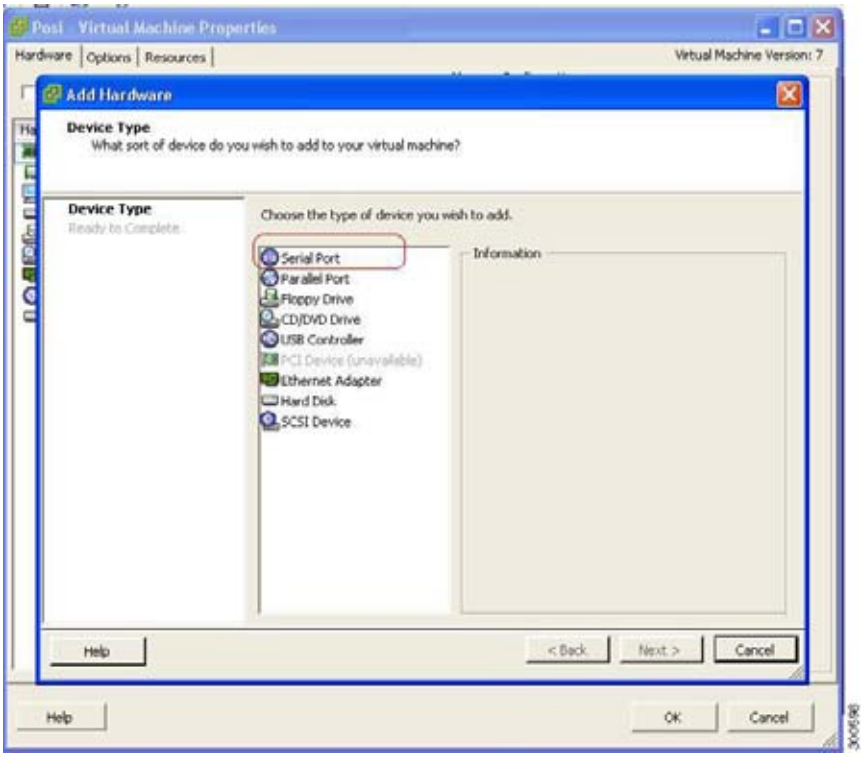
ステップ 1　特定の VMware サーバ（たとえば ISE-120）の電源をオフにします。

ステップ 2　VMware サーバを右クリックし、[編集（Edit）] を選択します。

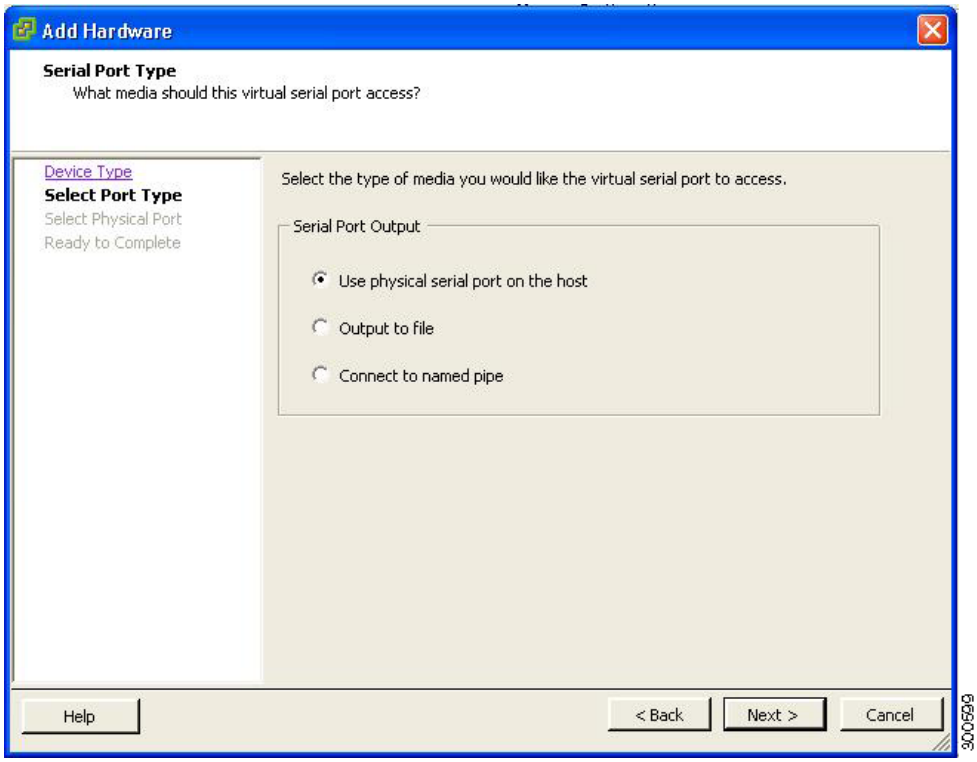
ステップ 3　[ハードウェア（Hardware）] タブを選択し、[追加（Add）] をクリックします。



ステップ 4　[シリアル ポート（Serial Port）] を選択し、[次へ（Next）] をクリックします。



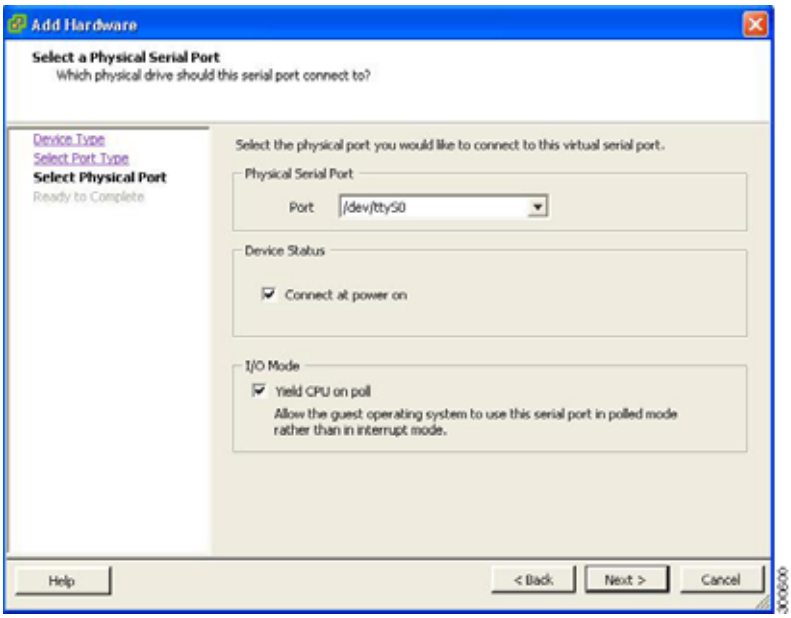
ステップ 5　シリアル ポート出力の場合は、[ホストで物理シリアル ポートを使用する（Use physical serial port on the host）] を選択します。[次へ（Next）] をクリックします。



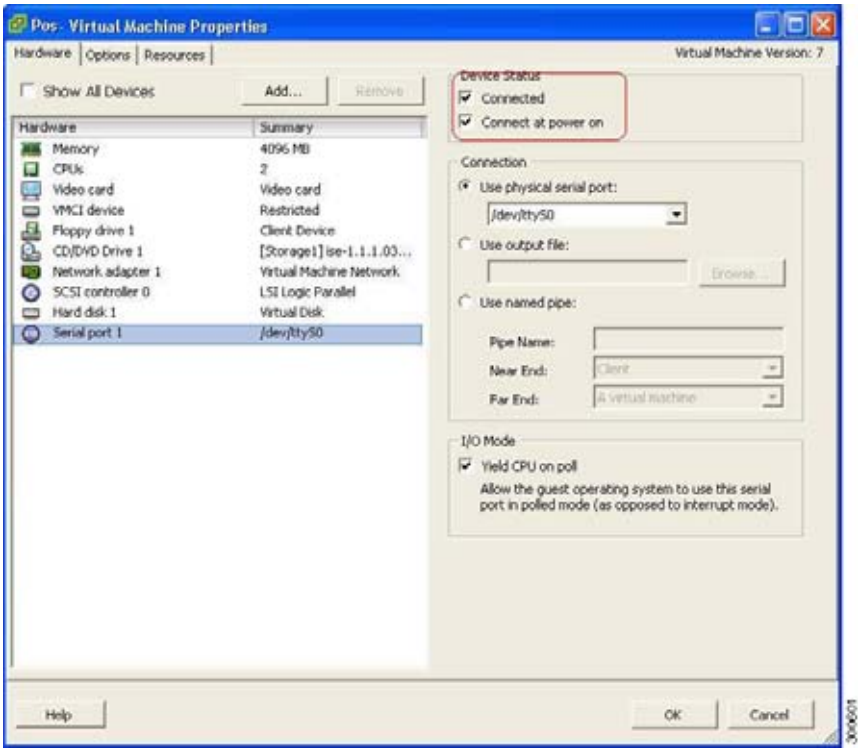
ステップ 6　ポートを選択します。次の 2 つのいずれかのオプションを選択できます。

- **/dev/ttyS0**（DOS または Windows オペレーティング システムで、これは COM1 として表示されます）。
- **/dev/ttyS1**（DOS または Windows オペレーティング システムで、これは COM2 として表示されます）。

ステップ 7　[次へ（Next）] をクリックします。



ステップ 8　デバイスのステータスを確認します。これは [接続済み（Connected）] と表示されます。



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

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。

CHAPTER 6

インストール後のタスクの実行

この章では、Cisco Identity Services Engine（ISE）3300 シリーズ アプライアンスのインストールおよび設定が正常に完了した後に実行が必要ないくつかの作業について説明します。この章で説明する内容は、次のとおりです。

ライセンスのインストール

Cisco ISE システムを管理するには、有効なライセンスが必要です。ライセンスは、Cisco ISE ネットワーク リソースを使用できる同時エンドポイントの数など、アプリケーションの機能の使用やアクセスを制限する機能を提供します。

（注） 同時エンドポイントは、サポートされるユーザとデバイスの合計数を表します。エンドポイントには、ユーザ、パーソナル コンピュータ、ラップトップ、IP 電話、スマート フォン、ゲーム コンソール、プリンタ、ファクス機、またはその他のネットワーク デバイスを組み合わせることができます。

Cisco ISE ソフトウェア機能サポートは、2 つの機能セットに分けられます。

- 基本パッケージ：ネットワーク アクセス、ゲスト、およびリンク暗号化の基本サービスをイネーブルにします。
- 拡張パッケージ：プロファイラ、ポスチャ、およびセキュリティ グループ アクセスなど、より高度なサービスをイネーブルにします。

各ライセンス パッケージは、対応するサービスの接続および使用が可能な特定の数の同時エンドポイントをサポートしています。各パッケージ タイプのサービスは、対応するライセンスをインストールすることによってイネーブルになります。2 通りのライセンス インストールのアプローチの可能性が考えられます。

- **基本および拡張ライセンス**：基本および拡張ライセンスをインストールし、インストールに応じて対応する機能サポートをイネーブルにできます。各ライセンスは個別にインストールできます。また、同じタイプの複数のライセンスをインストールして、対応するパッケージのエンドポイント数を累積的に増やすことができます。
- **ワイヤレス ライセンス**：ワイヤレス ライセンスは、基本および拡張パッケージの両方で同じ数のエンドポイントをイネーブルにします。ただし、このタイプのライセンスでサポートされているデバイスはワイヤレス デバイスに制限されます。その後、すべてのタイプのデバイスの基本および拡張パッケージ機能のサポートをイネーブルにするワイヤレス アップグレード ライセンスをインストールすることにより、この制限を削除することができます。

これらのトピックに関する詳細については、次の各項を参照してください。

- 「ライセンスのタイプ」（P.6-3）
- 「ライセンスの取得」（P.6-6）
- 「評価ライセンスの自動インストール」（P.6-7）

組み込みライセンス

Cisco ISE システムには、基本および拡張の両方のパッケージ サービスをフィーチャする評価ライセンスが含まれます。これは 90 日間有効で、システムの基本および拡張パッケージのユーザ数を 100 に制限します。Cisco ISE システムにより、評価ライセンスの期限が切れる前に、有効な製品ライセンスのダウンロードを求めるプロンプトが表示されます。

90 日間の最後に評価ライセンスの期限が切れると、管理 Web アプリケーションにより、基本、基本および拡張、またはワイヤレスの有効な製品ライセンスのインストールを求めるプロンプトが表示されます。（評価ライセンスは有線およびワイヤレスの両方のユーザのサポートを提供できますが、ワイヤレス ライセンス オプションを購入および適用すると、評価期間中にサポートされていた可能性のあるサポートが切り捨てられます）。管理ユーザ インターフェイスを使用したライセンス ファイルの追加および変更の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の「Managing Licenses」の章を参照してください。

中央集中型ライセンス

ライセンスは Cisco ISE ネットワーク内の管理 ISE ノードによって集中管理され、展開内のすべての他の Cisco ISE ノード（インライン ポスチャ ノードを除く）に自動的に分散されます。たとえば、分散展開では、プライマリおよびセカンダリとして展開されている 2 つの管理ペルソナ インスタンスがあります。ライセンス ファイルのインストールが正常終了すると、プライマリ管理 ISE ノードからのライセンス情報はセカンダリ管理 ISE ノードに伝播されます（これにより、展開内の各管理 ISE ノードに同じライセンスをインストールする必要はありません）。

（注）　Cisco ISE ライセンスは、MAC アドレスではなく、プライマリ管理 ISE ノード ハードウェア ID に基づいて生成されます。

同時エンドポイント カウント

各 Cisco ISE ライセンスには、Cisco ISE サービスを使用できる同時エンドポイントの数を制限する、基本、基本および拡張、またはワイヤレス パッケージのカウント値が含まれます。カウントには、ネットワークに同時接続されており、サービスにアクセスしている全体の展開間のエンドポイントの合計数が含まれます。エンドポイントの数がサポートされているライセンス カウントを超えて増えた場

合、Cisco ISE 内でのライセンス強制はソフトで、エンドポイントはサービスのアクセスからブロックされないままです。エンドポイントがライセンスされている値を超えたときに生成されるアラームに関する詳細については、「ライセンスの強制」（P.6-3）を参照してください。

ライセンスの強制

Cisco ISE はネットワーク上で同時エンドポイントを追跡し、エンドポイント カウントがライセンスされている量を超えるとアラームを生成します。

- 80 % 情報
- 90 % 警告
- 100 % 重大

注意　正確なエンドポイント アカウンティングは RADIUS アカウンティングに依存します。

ライセンスの期限切れ

ライセンスの期限切れの通知のためのアラームは送信されません。期限切れのライセンスで Cisco ISE ノードにログインすると、管理者は Cisco ISE ダッシュボードまたはその他のサービスにアクセスできず、www.cisco.com のライセンス ページにリダイレクトされます。

Cisco ISE ライセンス アプリケーションの動作

- デフォルトの評価ライセンスの上にワイヤレス ライセンスをインストールすると、ワイヤレス ライセンスにより、評価ライセンスのパラメータがワイヤレス ライセンスに関連付けられている特定の期間とユーザ カウントで上書きされます。
- デフォルトの評価ライセンスの上に基本ライセンスをインストールすると、基本ライセンスにより、評価ライセンスの「基本」部分のみが上書きされます。このため、拡張ライセンスの機能はデフォルトの評価ライセンス期間によって許可されている残りの期間のみ使用可能なままになります。
- デフォルトの評価ライセンスの上に拡張ライセンスをインストールすると、拡張ライセンスにより評価ライセンスの「拡張」部分のみが上書きされます。このため、基本ライセンスの機能はデフォルトの評価ライセンス期間によって許可されている残りの期間のみ使用可能なままになります。

（注）　Cisco ISE の基本または拡張機能に関連する期限切れの問題を回避するため、デフォルトの評価ライセンスを同時に基本と拡張の両方のライセンスに置き換えることを推奨します。

ライセンスのタイプ

この項では、Cisco ISE 3300 シリーズ アプライアンスでの使用がサポートされている 4 種類のライセンスについて説明します。

- 「評価ライセンス」（P.6-4）
- 「基本ライセンス」（P.6-5）
- 「拡張ライセンス」（P.6-5）
- 「ワイヤレス ライセンス」（P.6-5）

一般的に、基本および拡張ライセンスは主に Cisco ISE サービスの提供に重点が置かれており、ワイヤレス ライセンス オプションは純粋にワイヤレス エンドポイント環境でより迅速かつ容易に Cisco ISE を確実に展開できるようにすることに重点が置かれています。

Cisco ISE の基本、拡張、ワイヤレスおよびワイヤレス アップグレード ライセンスで使用可能な機能および Stock-Keeping Unit（SKU）の詳細については、『Cisco Identity Services Engine Ordering Guidelines』（http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/guide_c07-656177.html）を参照してください。

ライセンスに関するガイドライン

次に、遵守する必要があるライセンスに関するガイドラインをいくつか示します。

- 展開ごとにすべてのライセンスは Cisco ISE ノード（管理 ISE ノード）で集中管理されます。
- すべてのライセンスは管理 ISE ノードにのみ適用されます。
- 展開に、基本ライセンスなしで拡張ライセンスを持たせることはできません。
- ワイヤレス ライセンスは、管理 ISE ノード上で基本ライセンス、または基本および拡張ライセンスと共存することができません。
- 管理 ISE ノードで、基本エンドポイント ライセンスより多い拡張エンドポイント ライセンスを追加できないことを確認する必要があります。
- インライン ポスチャ ノードに個別のライセンスは必要ありません。
  - インライン ポスチャ ノードは Cisco ISE 3300 シリーズ アプライアンスでのみサポートされます。VMware サーバ システムではサポートされません。
  - 特定のワイヤレス LAN コントローラ（WLC）バージョンのみがインライン ポスチャでサポートされます。（詳細については、『*Cisco Identity Services Engine Network Component Compatibility, Release 1.1*』を参照してください）。

（注）　インライン ポスチャ ノードは、VMware サーバ システムでサポートされません。

- ライセンスが適用される前に Cisco ISE を起動すると、ライセンス ページのみが含まれるブートストラップ設定のみが表示されます。
- 評価ライセンスが期限切れに近づくと、Cisco ISE システムに Web ベースのアクセスを試みたときに製品ライセンス（基本、基本および拡張、またはワイヤレス）のダウンロードおよびインストールを求めるプロンプトが表示されます。
- 基本ライセンスが適用されると、基本的なネットワーク アクセスおよびゲスト アクセスのための Cisco ISE ユーザ インターフェイス画面およびタブが表示されます。
- 拡張ライセンスが適用されると、プロファイラ、ポスチャ、およびセキュリティ グループ アクセスのための Cisco ISE ユーザ インターフェイス画面およびタブが表示されます。

評価ライセンス

評価ライセンスは、基本と拡張の両方のライセンス パッケージで構成されます。評価ライセンスでは、サポートが 100 エンドポイントに制限され、90 日で期限が切れます。この期間はリアルタイム クロックではなく、Cisco ISE システム クロックに基づいています。評価ライセンスは事前インストールされているため、別途インストールする必要はありません。

評価ライセンスが 90 日間の終わりに近づくと、Cisco ISE システムはライセンスのアップグレードのアラームを生成することにより、ユーザに有効な製品ライセンス（基本または拡張）のダウンロードとインストールを求めるプロンプトを表示します。正規ライセンスのインストールでは、サービスは選択したパッケージに基づいて継続されます。

基本ライセンス

基本ライセンスはデバイス上で Cisco ISE 管理インターフェイスを使用してインストールされます。評価ライセンスと異なり、基本ライセンスでは使用状況もデバイスに記録されます。基本ライセンスは永続ライセンスです。基本パッケージには認証、許可、ゲスト、およびスポンサー サービスが含まれ、このライセンスの期限が切れることはありません。

拡張ライセンス

拡張ライセンスは、基本ライセンスの上にのみインストールできます。最初に基本ライセンスをインストールせずに、評価ライセンスを拡張ライセンスにアップグレードすることはできません。基本ライセンス パッケージで使用可能な機能に加え、拡張ライセンスでは Cisco ISE のプロファイラ、ポスチャ、およびセキュリティ グループ アクセス サービスがアクティブになります。

拡張ライセンスでサポートされるエンドポイントの合計数は、常に基本ライセンスのカウントを上回ることができません（基本ライセンス カウント以下にすることができます）。

（注）　拡張ライセンスはサブスクリプション ベースで、3 年と 5 年の 2 つの有効サブスクリプション期間があります。

ワイヤレス ライセンス

ワイヤレス ライセンスは、基本的なネットワーク アクセス（認証および許可）、ゲスト サービス、およびリンク暗号化など基本的な基本ライセンス機能だけでなく、プロファイラ、ポスチャ、セキュリティ グループ アクセス サービスを含むすべての拡張ライセンス機能も提供するワイヤレス専用のサービス プロバイダに、柔軟なオプションを提供するように設計されています。Cisco ISE は、ワイヤレス専用の顧客のみがワイヤレス LAN コントローラ（WLC）からの RADIUS ワイヤレス認証要求のみを許可することによりワイヤレス ライセンス オプションを活用できることを保証します（他の認証リクエスト メソッドはドロップされます）。さらに、LiveLogs エントリにも、「Request from a non-wireless device was dropped due to installed Wireless license」と表示し、ドロップされた要求の理由を示します。

（注）　拡張ライセンス パッケージと同様に、ワイヤレス ライセンスはサブスクリプション ベースです。

現在展開にワイヤレス ライセンス モデルをサブスクライブしており、その後、前述の基本および拡張ライセンス スキームに戻さずに、ネットワーク上の非ワイヤレス エンドポイントの Cisco ISE サポートを提供することを決定した場合、ワイヤレス アップグレード ライセンスに移行できます。これらのライセンスは、Cisco ISE 機能、および有線および VPN コンセントレータ アクセスを含むすべてのワイヤレスおよび非ワイヤレス クライアント アクセス メソッドの全範囲を提供するように設計されています。

（注）　ワイヤレス アップグレード ライセンス オプションは、同じ許容エンドポイント カウントを持つ既存のワイヤレス ライセンスの上にのみインストールできます。ワイヤレス アップグレードを基本プラス拡張ライセンス パッケージの上にインストールすることはできません。

ライセンスの取得

90 日間の評価ライセンスの期限が切れた後、引き続き Cisco ISE サービスを使用して、100 を超える同時エンドポイントをネットワーク上でサポートするには、Cisco ISE で固有の基本または基本および拡張ライセンス パッケージを取得してインストールする必要があります。ライセンス ファイルは、Cisco ISE ハードウェア ID と製品認証キー（PAK）の組み合わせに基づいています。Cisco ISE を購入した時点で、または 90 日間のライセンスの期限が切れる前に、Cisco.com にアクセスして基本または基本および拡張ライセンスを注文することができます。

Cisco.com からライセンス ファイルを注文して 1 時間以内に、シスコの補遺エンド ユーザ ライセンス契約書および注文した各ライセンスの PAK を含む権利証明書が添付された電子メールを受信するはずです。権利証明書の受信後、シスコの製品ライセンス登録サイト（http://www.cisco.com/go/license）にログインおよびアクセスし、適切なハードウェア ID 情報および PAK を入力してライセンスを生成できます。

ライセンス ファイルを生成するには、次の固有の情報を指定する必要があります。

- 製品 ID（PID）
- バージョン ID（VID）
- シリアル番号（SN）
- 製品認証キー（PAK）

シスコの製品ライセンス登録サイトでライセンス情報を送信した翌日に、ライセンス ファイルが添付された電子メールを受信します。ローカル マシン上の既知の場所にライセンス ファイルを保存し、『*Cisco Identity Services Engine User Guide, Release 1.1*』の「Managing Licenses」の章の手順に従って、Cisco ISE での製品ライセンスの追加およびアップデートを行います。

プライマリ管理 ISE ノード ハードウェア ID を決定するには、次の手順を実行します。

ステップ 1　ダイレクト コンソール CLI にアクセスし、**show inventory** コマンドを入力します。次のような行を含む出力が表示されます。

```
PID: NAC3315, VID: V01, SN: ABCDEFG
```

ステップ 2　（オプション）ライセンスの期限が切れていない場合は、次の手順を実行してプライマリ管理 ISE ノードを表示できます。

a. [管理（Administration）] > [システム（System）] > [ライセンス（Licensing）] を選択します。

[ライセンスの操作（License Operations）] ナビゲーション ペインと [現在のライセンス（Current Licenses）] ページが表示されます。

b. [ライセンスの操作（License Operations）] ナビゲーション ペインで [現在のライセンス（Current Licenses）] をクリックします。

[現在のライセンス（Current Licenses）] ページが表示されます。

c. プライマリ管理 ISE ノード ハードウェア ID をチェックする Cisco ISE ノードに対応するボタンを選択して、[管理ノード（Administration Node）] をクリックします。

製品 ID、バージョン ID、およびシリアル番号が表示されます。

（注）　Cisco ISE ライセンスは、MAC アドレスではなく、プライマリ管理 ISE ノード ハードウェア ID に基づいて生成されます。

詳細、および新しいインストールのライセンス オプションや Cisco Secure Access Control System などのシスコの既存のセキュリティ製品を含む、Cisco ISE で使用可能なライセンス製品番号については、Cisco Identity Services Engine の注文ガイドライン（http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/guide_c07-656177.html）を参照してください。

評価ライセンスの自動インストール

ディスク領域が 60 ～ 600 GB の Cisco ISE で仮想マシンを使用する場合は、Cisco ISE によって評価ライセンスが自動的にインストールされます。すべての Cisco ISE 3300 シリーズ アプライアンスには 90 日間および 100 エンドポイントに制限される評価ライセンスが付属しています。

Cisco ISE ソフトウェアをインストールし、アプライアンスをプライマリ管理 ISE ノードとして初期設定した後、「ライセンスの取得」（P.6-6）の手順に従って、Cisco ISE のライセンスを取得および適用する必要があります。プライマリ管理 ISE ノード ハードウェア ID を使用して、すべてのライセンスを Cisco ISE プライマリ管理 ISE ノードに適用します。その後、プライマリ管理 ISE ノードは展開にインストールされているすべてのライセンスを集中管理します。

Cisco ISE ライセンスは、MAC アドレスではなく、プライマリ管理 ISE ノード ハードウェア ID に基づいて生成されます。ライセンス管理のプロセスは、デュアル管理 ISE ノードの場合もシングル管理 ISE ノードの場合も同じです。

次の手順：

Cisco ISE ユーザ インターフェイスを使用してライセンスを管理するには、『*Cisco Identity Services Engine User Guide, Release 1.1*』の「Managing Licenses」の章を参照し、次のタスクを実行します。

- ライセンスの追加およびアップグレード
- ライセンスの編集

Web ブラウザを使用した Cisco ISE へのアクセス

Cisco ISE 3300 シリーズ アプライアンスは、次の HTTPS が有効なブラウザを使用した Web インターフェイスをサポートしています。

- Mozilla Firefox バージョン 3.6
- Mozilla Firefox バージョン 9
- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 9（Internet Explorer 8 互換モード）

（注） Cisco ISE ユーザ インターフェイスは Microsoft IE8 ブラウザの IE7 互換モードの使用をサポートしていません（Microsoft IE8 は IE8 モードのみがサポートされています）。

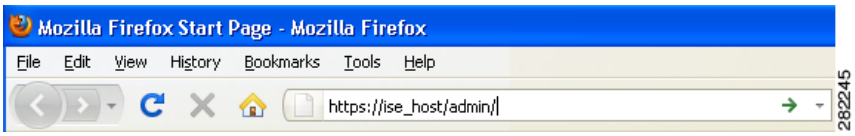
この項では、次の内容について説明します。

ログイン

初めて Cisco ISE Web ベース インターフェイスにログインするときは、事前インストールされている評価ライセンスを使用します。前の項で挙げたサポートされている HTTPS が有効なブラウザのみを使用する必要があります。本マニュアルで説明するとおりに Cisco ISE をインストールしたら、Cisco ISE Web ベース インターフェイスにログインできます。

Web ベース インターフェイスを使用して Cisco ISE にログインするには、次の手順を実行します。

ステップ 1　Cisco ISE アプライアンスのリブートが完了したら、サポートされている Web ブラウザの 1 つを起動します。



ステップ 2　アドレス フィールドに、Cisco ISE アプライアンスの IP アドレス（またはホスト名）を次のフォーマットを使用して入力し、Enter を押します。

```
http://<IP address or host name>/admin/
```

たとえば、`http://10.10.10.10/admin/` と入力すると Cisco ISE のログイン ページが表示されます。

ステップ 3　Cisco ISE のログイン ページで、セットアップ時に定義したユーザ名とパスワードを入力します。

ステップ 4　[ログイン（Login）] をクリックすると Cisco ISE のダッシュボードが表示されます。

（注）　Cisco ISE CLI 管理ユーザ名またはパスワードを回復またはリセットするには、「管理者パスワードのリセット」（P.6-14）を参照してください。

（注）　CLI 管理ユーザ名またはパスワードを忘れた場合は、*Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD を使用して [パスワードの回復（Password Recovery）] を選択します。このオプションにより、CLI 管理ユーザ名およびパスワードをリセットできます。

ヒント　Cisco ISE GUI を表示しより良いユーザ エクスペリエンスのために必要な最小画面解像度は 1280 X 800 ピクセルです。

Cisco ISE へのログイン時、CLI ベースと Web ベースでは、ユーザ名とパスワードの値は同じではありません。Cisco ISE CLI 管理ユーザと Cisco ISE Web ベース管理ユーザとの違いの詳細については、「CLI 管理ユーザと Web ベース管理ユーザの admin 権限の違い」（P.3-2）を参照してください。

（注）　ライセンス ページは、評価ライセンスの期限が切れた後、初めて Cisco ISE にログインするときにだけ表示されます。

（注）　Cisco ISE システムに正常にログインした後、Cisco ISE ユーザ インターフェイスを使用して管理者ログイン パスワードを定期的にリセットすることを推奨します。管理者パスワードのリセットの詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の「Configuring Cisco ISE Administrators」を参照してください。

ログインの試行に失敗した後の管理者のロックアウト

指定した管理者ユーザ ID に対して誤ったパスワードを十分な回数入力した場合、Cisco ISE ユーザ インターフェイスにより「ロックアウト」され、ログ エントリが [モニタ（Monitor）] > [レポート（Reports）] > [カタログ（Catalog）] > [サーバ インスタンス（Server Instance）] > [サーバ管理者ログイン（Server Administrator Logins）] レポートに追加され、「管理者のロックアウトによるパスワードの無効化」（P.6-15）に従ってその管理者 ID に関連付けられたパスワードをリセットする機会を得るまで、その管理者 ID の資格情報が一時停止されます。管理者アカウントをディセーブルにするのに必要な失敗試行数は、『*Cisco Identity Services Engine User Guide, Release 1.1*』の「Managing Identities」の章に記載されているガイドラインに従って設定できます。管理者ユーザ アカウントがロックアウトされると、関連する管理ユーザに電子メールが送信されます。

ログアウト

Cisco ISE Web ベース インターフェイスをログアウトするには、Cisco ISE メイン ウィンドウ ツールバーで [ログアウト（Log Out）] をクリックします。これにより、管理セッションが終了してログアウトされます。

注意　セキュリティ上の理由から管理セッションを完了した場合は、Cisco ISE からログアウトすることを推奨します。ログアウトしない場合、30 分間何も操作しないと Cisco ISE の Web インターフェイスからログアウトされ、送信されていない設定データは保存されません。

Cisco ISE Web ベースの Web インターフェイスの使用の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』を参照してください。

Cisco ISE 設定の確認

この項では、ログインおよび Cisco ISE 設定の確認にそれぞれ異なるユーザ名とパスワードの資格情報を使用する 2 つの方法を提供しています。

- 「Web ブラウザを使用した設定の確認」（P.6-10）
- 「CLI を使用した設定の確認」（P.6-11）

（注）　Cisco ISE システムに初めて Web ベースでアクセスする場合、管理者のユーザ名とパスワードはセットアップ時に設定した CLI ベースのアクセスと同じです。Cisco ISE システムに CLI ベースでアクセスする場合、管理者のユーザ名はデフォルトで **admin**、管理者パスワード（デフォルトがないため、ユーザ定義）はセットアップ時に設定した値を表します。

CLI 管理ユーザと Web ベース管理ユーザの権限の違いの詳細については、「CLI 管理ユーザと Web ベース管理ユーザの admin 権限の違い」（P.3-2）を参照してください。

Web ブラウザを使用した設定の確認

Cisco ISE 3300 シリーズ アプライアンスが正常に設定されたことを確認するには、Web ブラウザを使用して次の手順を実行します。

ステップ 1　Cisco ISE アプライアンスのリブートが完了したら、サポートされている Web ブラウザの 1 つを起動します。

ステップ 2　**アドレス** フィールドに、Cisco ISE アプライアンスの IP アドレス（またはホスト名）を次のフォーマットを使用して入力し、Enter を押します。

```
http://<IP address or host name>/admin/
```

たとえば、`http://10.10.10.10/admin/` と入力すると Cisco ISE のログイン ページが表示されます。

ステップ 3　Cisco ISE のログイン ページで、セットアップ時に定義したユーザ名とパスワードを入力し、[ログイン（Login）] をクリックします。

Cisco ISE ダッシュボードが表示されます。

（注）　Cisco ISE システムに正常にログインした後、Cisco ISE ユーザ インターフェイスを使用して管理者ログイン パスワードを定期的にリセットすることを推奨します。管理者パスワードのリセットの詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』の「Configuring Cisco ISE Administrators」を参照してください。

CLI を使用した設定の確認

Cisco ISE 3300 シリーズ アプライアンスが正常に設定されたことを確認するには、Cisco CLI を使用して次の手順を実行します。

ステップ 1　Cisco ISE アプライアンスのリブートが完了したら、ISE アプライアンスへのセキュア シェル（SSH）接続の確立にサポートされている製品を起動します（たとえば、PuTTY、オープン ソース Telnet/SSH クライアントを使用します）。

ステップ 2　ホスト名（または IP アドレス）のフィールドに、ホスト名（またはドット付き 10 進形式を使用して Cisco ISE の IP アドレス）を入力し、[開く（Open）] をクリックして Cisco ISE アプライアンスのシステム プロンプトを表示します。

ステップ 3　ログイン プロンプトで、セットアップ時に設定した CLI 管理ユーザ名（**admin** がデフォルト）を入力し、Enter を押します。

ステップ 4　パスワード プロンプトで、セットアップ時に設定した CLI 管理パスワード（これはユーザ定義でデフォルトはありません）を入力し、Enter を押します。

ステップ 5　アプリケーションが適切にインストールされていることを確認するには、システム プロンプトで **show application version ise** と入力し、Enter を押します。

コンソールに次の画面が表示されます。

```
ise-4/admin# show application version ise

Cisco Identity Services Engine
------------------------------------------
Version      : 1.0.2.303
Build Date   : Mon Oct  4 04:44:18 2010
Install Date : Mon Oct  4 22:51:55 2010
```

282247

（注）　ビルド番号は、現在インストールされている Cisco ISE ソフトウェアのバージョンを反映します。

ステップ 6　Cisco ISE プロセスのステータスを確認するには、システム プロンプトで **show application status ise** と入力し、Enter を押します。

コンソールに次の画面が表示されます。

```
ise-4/admin# show application status ise

ISE Database listener is running, PID: 4014
ISE Database is running, number of processes: 29
ISE Application Server is running, PID: 4310
ISE Monitoring Session Database is running, PID: 3815
ISE Monitoring Log Collector is running, PID: 4369
ISE Monitoring Log Processor is running, PID: 4425
ISE Monitoring Alert Process is running, PID: 4331
```

282248

（注）　最新の Cisco ISE パッチを入手し Cisco ISE を最新に保つには、http://www.cisco.com/public/sw-center/index.shtml を参照してください。

ステップ 7　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）のバージョンを確認するには、システム プロンプトで **show version** と入力し、Enter を押します。

コンソールに次の出力が表示されます。

```
Cisco Application Deployment Engine OS Release: 2.0
ADE-OS Build Version: 2.0.2.083
ADE-OS System Architecture: i386
```

VMware ツールのインストールの確認

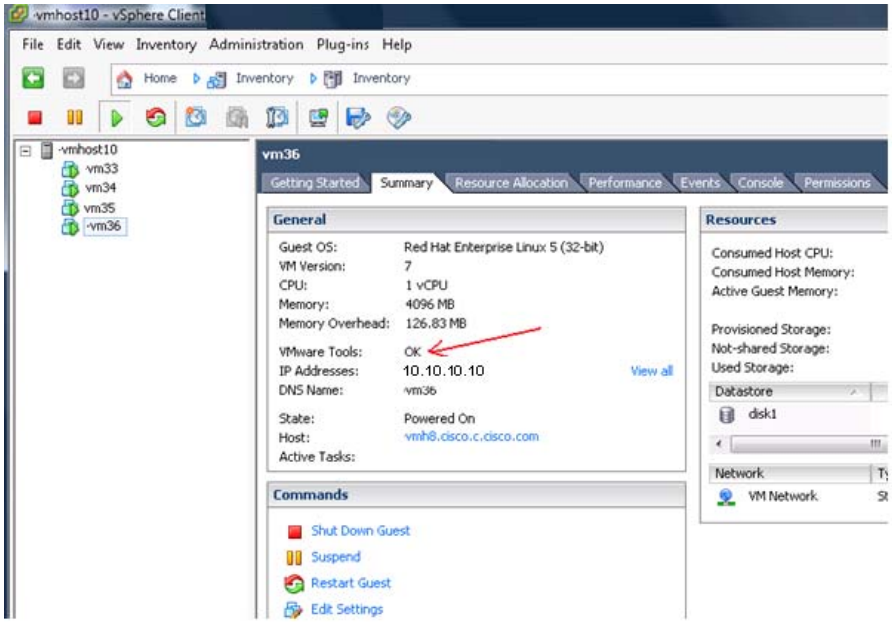
VMware ツールのインストールは次の 2 つの方法で確認できます。

- vSphere Client での [サマリー（Summary）] タブの使用
- CLI の使用

vSphere Client での [サマリー（Summary）] タブの使用

vSphere Client の [サマリー（Summary）] タブに移動します。[VMware ツール（VMware Tools）] の値は「OK」であるはずです。図 6-1 の赤色の矢印は、値が「OK」であるため、VMware ツールがインストールされていることを示しています。

図 6-1　vSphere Client での VMware ツールの確認



CLI の使用

show inventory CLI コマンドを使用して VMware ツールがインストールされているかどうかを確認することもできます。このコマンドは NIC ドライバ情報をリストします。VMware ツールがインストールされた仮想マシンでは、ドライバ情報が「VMware 仮想イーサネット ドライバ」としてリストされます。次の例を参照してください。

```
vm36/admin# show inv

NAME: "ISE-VM-K9          chassis", DESCR: "ISE-VM-K9          chassis"
PID: ISE-VM-K9         , VID: V01 , SN: 8JDCBLIDLJA
Total RAM Memory: 4016564 kB
CPU Core Count: 1
CPU 0: Model Info: Intel(R) Xeon(R) CPU           E5504  @ 2.00GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /dev/sda
Disk 0: Capacity: 64.40 GB
Disk 0: Geometry: 255 heads 63 sectors/track 7832 cylinders
NIC Count: 1
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:0C:29:BA:C7:82
NIC 0: Driver Descr: VMware Virtual Ethernet driver

(*) Hard Disk Count may be Logical.
vm36/admin#
```

管理者パスワードのリセット

Cisco ISE の管理者パスワードをリセットする方法は 2 つあります。特定のパスワードの紛失の性質に応じて、次の一連の手順の 1 つを使用します。

- 「紛失、失念、または侵害されたパスワード」（P.6-14）：管理者パスワードの紛失、失念、または侵害により、誰も Cisco ISE にログインできない場合、この手順を使用します。
- 「管理者のロックアウトによるパスワードの無効化」（P.6-15）：管理者 ID の行で指定された回数のログインを失敗したためにパスワードが使用できなくなった場合、この手順を使用します。

紛失、失念、または侵害されたパスワード

管理者パスワードが紛失、失念、または侵害により誰も Cisco ISE システムにログインできない場合は、*Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD を使用して管理者パスワードをリセットできます。

前提条件：

Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx) DVD を使用して Cisco ISE アプライアンスの起動を試みる場合、問題が発生する可能性のある次の接続関連の状況を理解していることを確認する必要があります。

- 次の状況で *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD を使用して Cisco ISE アプライアンスの起動を試みると、エラーが発生する場合があります。
  - *exec* 行設定を含む Cisco ISE アプライアンスへのシリアル コンソール接続に関連付けられているターミナル サーバがある（*no exec* 行設定を使用していない場合）。
  - Cisco ISE アプライアンスへのキーボードおよびビデオ モニタ（KVM）接続がある（これはリモート KVM または VMware vSphere クライアント コンソール接続のいずれかになります）。

  および

  - Cisco ISE アプライアンスへのシリアル コンソール接続がある。

（注） *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD を使用して Cisco ISE アプライアンスを起動する場合、「no exec」設定を使用するシリアル コンソール行のターミナル サーバ設定を指定することにより、これらの接続関連の問題を回避することができます。これにより、KVM 接続とシリアル コンソール接続の両方を使用できます。

Cisco ISE アプライアンスの管理者パスワードのリセット

管理者パスワードをリセットするには、次の手順を実行します。

ステップ 1　Cisco ISE アプライアンスの電源がオンになっていることを確認します。

ステップ 2　アプライアンスの CD/DVD ドライブに *Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)* DVD を挿入します。

コンソールに次のメッセージが表示されます（これは Cisco ISE 3355 の例です）。

```
Welcome to Cisco Identity Services Engine - ISE 3355
To boot from hard disk press <Enter>
Available boot options:
```

```
[1] Cisco Identity Services Engine Installation (Keyboard/Monitor)
[2] Cisco Identity Services Engine Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
boot:
```

ステップ 3　管理者パスワードをリセットするには、システム プロンプトで、アプライアンスへのキーボードおよびビデオ モニタ接続を使用している場合は、**3** と入力し、ローカル シリアル コンソール ポート接続を使用している場合は **4** と入力します。

コンソールにパラメータのセットが表示されます。

ステップ 4　表 6-1 にリストされている説明に従って、パラメータを入力します。

表 6-1　パスワード リセット パラメータ

パラメータ	説明
管理ユーザ名（Admin username）	パスワードをリセットする管理者に対応する番号を入力します。
パスワード（Password）	指定された管理者の新しいパスワードを入力します。
パスワードの確認（Verify password）	再度パスワードを入力します。
変更を保存してリブート（Save change and reboot）	保存するには **Y** と入力します。

コンソールに次のメッセージが表示されます。

```
Admin username:
[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4
Enter number of admin for password recovery:2
Password:
Verify password:
Save change and reboot?[Y/N]:
```

DB パスワードをリセットするコマンドおよびその他の CLI コマンドについては、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.0.4*』を参照してください。

管理者のロックアウトによるパスワードの無効化

管理者ユーザ ID に対して誤ったパスワードを十分な回数入力すると、管理者パスワードが無効になる場合があります。最小およびデフォルトの回数は 5 です。Cisco ISE のユーザ インターフェイスによりシステムから「ロックアウト」され、その管理者 ID に関連付けられたパスワードをリセットする機会を得るまでその管理者 ID の資格情報が一時停止されます。

（注）　次のコマンドにより、管理者ユーザ インターフェイス パスワードをリセットします。指定された管理者 ID の CLI パスワードへの影響はありません。

管理者 ID のロックアウト後、パスワードをリセットするには、次の手順を実行します。

ステップ 1　ダイレクト コンソール CLI にアクセスし、次のコマンドを入力します。

```
admin# application reset-passwd ise <administrator ID>
```

ステップ 2　この管理者 ID に使用した前の 2 つのパスワードと異なる新しいパスワードを指定します。

```
Enter new password:
Confirm new password:

Password reset successfully
```

管理者パスワードが正常にリセットされると、Cisco ISE で資格情報がすぐにアクティブになり新しいパスワードでログインできます。システムをリブートする必要はありません。

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

Cisco ISE 3300 シリーズ アプライアンスの IP アドレスの変更

Cisco ISE 3300 シリーズ アプライアンスの IP アドレスを変更するには、次の手順を実行します。

ステップ 1　Cisco ISE CLI にログインします。

ステップ 2　次を入力します。

```
cofigure terminal
interface GigabitEthernet 0
ip address <new_ip_address> <new_subnet_mask>
exit
```

（注）　Cisco ISE アプライアンスの IP アドレスを変更する場合は、**no ip address** コマンドを使用しないでください。

（注）　Cisco ISE アプライアンスの IP アドレスを変更した後、すべての Cisco ISE サービスを再起動する必要はありません。

Cisco ISE 3300 シリーズ アプライアンスのイメージ再適用

Cisco ISE 3300 シリーズ アプライアンスのイメージ再適用、または以前に Cisco Secure ACS リリース 5.1 インストールで使用したイメージ再適用が必要な場合があります。たとえば、Cisco Secure ACS データを Cisco ISE に移行し、アプライアンスで再使用することを計画している場合です。

Cisco ISE 3300 シリーズ アプライアンスのイメージ再適用を行うには、次の手順を実行します。

ステップ 1　Cisco Secure ACS アプライアンスの電源がオンになっている場合は、アプライアンスの電源をオフにします。

ステップ 2　Cisco Secure ACS アプライアンスの電源をオンにします。

ステップ 3　F1 を押して、BIOS セットアップ モードにします。

ステップ 4　矢印キーを使用して [日付と時刻（Date and Time）] に移動し、Enter を押します。

ステップ 5　アプライアンスの時刻を UTC/GMT 時間帯に設定します。

（注）　すべての Cisco ISE ノードを UTC 時間帯に設定することを推奨します。この時間帯設定により、展開におけるさまざまなノードからのレポートおよびログが、タイムスタンプで常に同期されるようになります。

ステップ 6　Esc を押して、メイン BIOS メニューを終了します。

ステップ 7　Esc を押して、BIOS セットアップ モードを終了します。

ステップ 8　「Cisco ISE 3300 シリーズ アプライアンスを設定する前に」（P.3-1）で説明されている手順を実行します。

ステップ 9　「セットアップ プログラムのパラメータについて」（P.3-3）で説明されている手順を実行します。

ステップ 10　アプライアンスの CD/DVD ドライブに ***Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)*** DVD を挿入します。

コンソールが表示されます（これは Cisco ISE 3315 の例です）。

```
Welcome to Cisco Identity Services Engine - ISE 3315
To boot from hard disk press <Enter>
Available boot options:
[1] Cisco Identity Services Engine Installation (Keyboard/Monitor)
[2] Cisco Identity Services Engine Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
boot:
```

ステップ 11　コンソール プロンプトで、キーボードとビデオ モニタを使用している場合は **1** と入力し、シリアル コンソール ポートを使用している場合は **2** と入力して、Enter を押します。

イメージの再適用プロセスにより、既存の Cisco ADE-OS とソフトウェアバージョンがアンインストールされ、最新の Cisco ADE-OS と Cisco ISE ソフトウェア バージョンがインストールされます。

インストールおよび設定プロセスの詳細については、「Cisco ISE 3300 シリーズ アプライアンスを設定する前に」（P.3-1）および「セットアップ プログラムのパラメータについて」（P.3-3）を参照してください。

Cisco Secure ACS リリース 5.1/5.2 データから Cisco ISE リリース 1.0 アプライアン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。

Cisco ISE システムの設定

Cisco ISE の Web ベースのユーザ インターフェイス メニューを使用して、Cisco ISE システムをニーズに合わせて設定できます。認証ポリシー、許可、ポリシーの設定、およびすべての機能、メニュー、およびオプションの使用の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』を参照してください。

Cisco ISE の操作および監視やレポートなどのその他の管理機能の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.1*』を参照してください。

本リリースの最新情報については、『*Release Notes for Cisco Identity Service Engine, Release 1.1*』を参照してください。

Cisco ISE でのシステム診断レポートのイネーブル化

初めて Cisco ISE をインストールまたはアプライアンスのイメージ再適用を行った後、Cisco ISE CLI を使用してシステム レベルの診断レポートをイネーブルにすることができます（システム診断でのレポートを行うロギング機能は、デフォルトでは Cisco ISE でイネーブルになりません）。

システム診断レポートをイネーブルにするには、次のことを実行します。

ステップ 1　デフォルトの管理者ユーザ ID およびパスワードを使用して Cisco ISE CLI コンソールにログインします。

ステップ 2　次のコマンドを入力します。

```
admin# configure terminal
admin# logging 127.0.0.1:20514
admin# end
admin# write memory
```

Cisco ISE UI（[管理（Administration）] > [システム（System）] > [ロギング（Logging）] > [ロギング カテゴリ（Logging Categories）] > [システム診断（System Diagnostics）]）からシステム診断設定を指定できます。

新しい Cisco ISE ソフトウェアのインストール

各 Cisco ISE 3300 シリーズ アプライアンスには Cisco ISE ソフトウェアが事前インストールされています。事前インストールされている Cisco ISE ADE-OS および Cisco ISE ソフトウェアを新しいバージョンにアップグレードすること、既存のシステム設定情報を必ず保持することを推奨します。アプライアンス上で Cisco ISE の新しいインストールを実行すると、復元が必要な設定データの量によって、（展開された Cisco ISE ノードにつき）10 分から 60 分またはそれ以上がかかることがあります。

（注）　新しいソフトウェア インストールが完了したら、このインストール プロセスの前に、Cisco ISE へのアクセスに使用していたアクティブ ブラウザのキャッシュをクリアします。

詳細情報

Cisco 3300 シリーズ アプライアンスと新しい Cisco ISE リリース 1.0 ソフトウェアのインストールの詳細については、『*Release Notes for Cisco Identity Service Engine, Release 1.1*』の「Installing Cisco ISE Software」を参照してください。

APPENDIX A

Cisco ISE 3300 シリーズ ハードウェアの設置準備

この付録では、安全に関するガイドライン、設置場所の要件、および Cisco Identity Services Engine（ISE）3300 シリーズ アプライアンスを設置する前に、従う必要のあるイーサネット コネクタとコンソール ポートのガイドラインについて簡単に説明します。この情報については、次のトピックを参照してください。

安全に関するガイドライン

Cisco ISE 3300 シリーズ アプライアンスの設置を開始する前に、人身事故または機器の損傷を防ぐために、この付録の安全に関するガイドラインと、「ラックマウント構成のガイドライン」（P.B-1）を確認してください。

さらに、アプライアンスの交換、設定、または保守を行う前に、「関連資料」（P.xiii）に示されている安全上の警告を確認してください。この項では、次のトピックを扱います。

一般的な注意事項

アプライアンスの使用および取り扱いには、次の一般的な注意事項を守ってください。

- サービスに関するマーキングに従ってください。アプライアンス マニュアルで説明されている場合を除き、シスコ製品の保守を行わないでください。稲妻が描かれた三角形の印がついたカバーを開閉するときは、感電のおそれがあります。このような区画内にあるコンポーネントの修理は、認定されたサービス技術者だけが行う必要があります。

- 次のいずれかの状態が発生した場合は、電源コンセントから製品を取り外してパーツを交換するか、許可された保守技術者にご連絡ください。
  - 電源ケーブル、延長コード、またはプラグが損傷している。
  - 何かの物体が製品に入り込んだ。
  - 製品に水がかかった。
  - 製品が落下または損傷した。
  - 操作指示に従っているのに、製品が正しく動作しない。
- アプライアンスをラジエータや熱源の近くに置かないでください。また、通気口をふさがないでください。
- アプライアンスの上に食べ物や液体をこぼさないでください。また、水気のある環境で本製品を操作しないでください。
- アプライアンスの開口部に物を押し込まないでください。内部コンポーネントがショートして火災や感電の原因となる可能性があります。
- 製品は、シスコによって承認されている他の機器だけで使用してください。
- カバーを取り外すか、内部コンポーネントに触れる前に、製品を冷却できます。
- 正しい外部電源を使用してください。製品の電気定格ラベルに表示されている、電源のタイプからのみ製品を操作してください。必要な電源の種類が不明な場合は、サービス担当者または現地の電力会社にお問い合わせください。
- 認定された電源ケーブルだけを使用してください。ご使用のアプライアンス用、またはご使用のアプライアンス向けの AC 電源オプション用の電源ケーブルが付属していない場合は、国で使用が承認された電源ケーブルを購入してください。

  電源ケーブルが、製品と、製品の電気定格ラベルに記載された電圧および電流に適合することを確認してください。ケーブルの電圧と電流の定格は、製品に記載されている定格よりも大きい必要があります。
- 感電事故を予防するため、アプライアンスおよび電源ケーブルは、適正に接地されたコンセントに接続してください。これらのケーブルには適切な接地を可能にする 3 極プラグが装着されています。アダプタ プラグを使用したり、ケーブルから接地極を外したりしないでください。延長コードを使用する必要がある場合は、適切に接地されたプラグが装着された 3 線コードを使用してください。
- 延長コードとテーブル タップの定格を遵守してください。延長コードまたはテーブル タップに差し込まれたすべての製品の合計アンペア定格が、延長コードまたはテーブル タップのアンペア定格限度の 80 % を超えないようにしてください。
- アプライアンス電圧変換器、またはアプライアンス用に販売されているキットを、製品とともに使用しないでください。
- 一時的に急激に起こる電源電圧の上昇または下降からアプライアンスを保護するには、サージ抑制装置、パワー コンディショナ、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に配置してください。ケーブルと電源コードは、人に踏まれたり、それによって人が躓いたりしないように配線して差し込んでください。また、アプライアンスのケーブルまたは電源ケーブルの上に物を置かないように注意してください。
- 電源ケーブルとプラグを改造しないでください。場所を変更する場合は、ライセンスを待つ電気技術者または電力会社にお問い合わせください。現地または該当国の配線規定に必ず従ってください。

機器を扱う場合の注意

安全を確保して、機器を保護するため、次のガイドラインに従ってください。ただし、このリストには、生じる可能性のある危険な状況がすべて網羅されているわけではありません。絶えず*注意*してください。

警告　設置手順を読んでから、システムを電源に接続してください。ステートメント 1004

- アプライアンスを移動する前に、必ずすべての電源コードおよびインターフェイス ケーブルを外してください。
- 回路の電源が切断されていると思い込まないで、*必ず*確認してください。
- 設置作業前および作業後は、アプライアンスのシャーシの設置場所を整理し、埃のない状態に保ってください。
- 工具とアセンブリ コンポーネントは、通行の邪魔にならない場所に保管してください。
- 危険を伴う作業は、1 人では行わないでください。
- 人身事故や装置障害を引き起こす可能性のある作業は行わないでください。
- ゆったりとした衣服は身につけず、アプライアンスのシャーシに引っかかることがないようにしてください。
- 目が危険にさらされる状況で作業する場合は、保護眼鏡を着用してください。

電気製品を扱う場合の注意

警告　この装置は、出入りが制限された場所に設置されることを想定しています。出入りが制限された場所とは、特殊なツール、ロックおよびキー、または他のセキュリティ手段を使用しないと入室できない場所を意味します。
ステートメント 1017

警告　感電を防ぐため、安全超低電圧（SELV）回路を電話網電圧（TNV）回路に接続しないでください。LAN ポートには SELV 回路が、WAN ポートには TNV 回路が組み込まれています。一部の LAN ポートおよび WAN ポートは RJ-45 コネクタを使用しています。ステートメント 1021

警告　電源コードが接続されている場合は、電源に触れないでください。電源スイッチを備えたシステムの場合、電源スイッチがオフになっていても、電源コードが接続されていれば、電源装置内部に入力電圧がかかっています。電源スイッチのないシステムの場合、電源コードが接続されていれば、電源装置内部に入力電圧がかかっています。ステートメント 4

警告　電力系統に接続された装置で作業する場合は、事前に、指輪、ネックレス、腕時計などの装身具を外してください。金属は電源やアースに接触すると、過熱して重度のやけどを引き起こしたり、金属類が端子に焼き付いたりすることがあります。ステートメント 43

警告　シャーシの作業や電源モジュール周辺の作業を行う前に、AC 装置の電源コードを外し、DC 装置の回路ブレーカーの電源を切ってください。ステートメント 12

警告　雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

警告　この機器は接地されることを前提にしています。通常の使用時にホストが接地されていることを確認してください。ステートメント 39

警告　装置を設置または交換する際は、必ずアースを最初に接続し、最後に取り外します。ステートメント 1046

電気で動く機器を操作する場合は、次のガイドラインに従ってください。

- 部屋の緊急電源遮断スイッチを確認します。これにより、電気事故が発生した場合に、ただちに電源をオフにすることができます。
- 次のタスクを実行する前にすべての電源を切ってください。
  - 電源付近で作業する場合
  - アプライアンスの取り付けまたは取り外しを行う場合
  - ほとんどのハードウェア アップグレードを行う場合
- 故障していると思われる機器は取り付けないでください。
- 床が濡れていないか、接地されていない電源延長コードや保護アースの不備などがないかどうか、作業場所の安全を十分に確認してください。
- 回路の電源が切断されていると思い込まないで、*必ず*確認してください。
- 人を危険にさらしたり、装置の安全性を損なったりする可能性のある作業は、いっさい行わないでください。
- 危険を伴う作業は、1 人では行わないでください。
- 電気事故が発生した場合は、次の手順に従ってください。
  - 十分注意して、自分自身が被害者にならないようにしてください。
  - アプライアンスの電源を切ってください。
  - 可能であれば、医療を受けるために別の人を呼びます。それができないときは、被害者の状態を判別してから助けを呼んでください。
  - 被害者が人工呼吸、心臓マッサージ、またはその他の治療を必要としているかどうか判断して、適切な処置を施してください。

さらに、電源は切断されているが、電話回線またはネットワーク ケーブルにはまだ接続されている機器を取り扱う場合は、次のガイドラインに従ってください。

- 雷が発生しているときには、電話線の接続を行わないでください。
- ジャックが特別に設計されている場合を除き、電話のジャックを水気のある場所では設置しないでください。

- 電話回線がネットワーク インターフェイスから切り離されていない限り、絶縁されていない電話ケーブルや端子には、触れないでください。
- 電話回線の設置または変更は、十分注意して行ってください。

静電破壊の防止

静電放電は、機器に損傷を与えたり、電気回路を損なったりする可能性があります。静電放電は、電気プリント基板の取り扱いが不適切な場合に生じ、障害あるいは断続的障害を引き起こします。モジュールの取り外しまたは交換を行うときは、必ず次の静電気防止手順に従ってください。

- 静電放電を受けやすいコンポーネントを輸送用ボックスから取り出すときは、アプライアンスにそのコンポーネントを取り付ける準備が整うまで、静電気防止用梱包材からコンポーネントを取り出さないでください。静電気防止用の梱包材を取り外す直前に、必ず身体から静電気を放電します。
- 精密なコンポーネントを輸送する場合、まずそのコンポーネントを静電気防止用の容器または包装材に配置します。
- 精密なコンポーネントは必ず耐静電気の安全な区域で処理します。可能な限り、静電気防止のフロア パッドおよび作業台パッドを使用します。
- Cisco ISE 3300 シリーズ アプライアンスが電気的に接地されていることを確認してください。
- 静電気防止用リスト ストラップを肌に密着させて着用してください。クリップをアプライアンスの塗装されていない表面に止めて、不要な静電気がアースに流れるようにします。静電破壊と感電を防ぐために、リスト ストラップとコードは効果的に使用する必要があります。
- リスト ストラップがない場合は、アプライアンスの金属部分に触れて、身体を接地してください。

注意　機器の安全を確保するために、静電気防止用リスト ストラップの抵抗値を定期的にチェックしてください。抵抗値は、1 ～ 10 Mohm でなければなりません。

持ち上げ時のガイドライン

Cisco ISE 3300 シリーズ アプライアンスは、アプライアンスに取り付けられているハードウェア オプションに応じて、15 ～ 33 ポンド（9.071 ～ 14.96 kg）の重さがあります。アプライアンスは、頻繁に移動されることを想定していません。アプライアンスを設置する前に、電源とネットワーク接続に対応するためにアプライアンスを後で移動する必要性が生じないように、設置場所が正しく準備されていることを確認してください。

アプライアンスまたは重い物を持ち上げる場合は、以下のガイドラインに従ってください。

- アプライアンスを持ち上げたり移動したりする前に、必ずすべての外部ケーブルを外してください。
- 足元を安定させ、両足で均等にシャーシの重量を支えるようにします。
- アプライアンスをゆっくり持ち上げます。突然移動したり、持ち上げるときに体をひねったりしないでください。
- 背中をまっすぐに保ち、背中ではなく脚で持ち上げます。アプライアンスを持ち上げるためにかがむ必要がある場合は、腰ではなく膝を曲げて、腰部の筋肉への負担を軽減してください。
- アプライアンスは下部から持ち上げてください。両方の手でアプライアンス外部の下側をつかみます。

設置場所の準備

ここでは、設置場所の計画、設置場所の準備、および Cisco ISE 3300 シリーズ アプライアンスの設置の準備について、次のトピックで説明します。

Cisco ISE 3300 シリーズ アプライアンスを設置する前に、次のステップを完了してください。

ステップ 1　設置場所を準備して（「設置場所の計画」（P.A-6）を参照）、設置計画や導入場所の調査資料があれば確認します。

ステップ 2　アプライアンスを開梱して調べます。

ステップ 3　アプライアンスを正しく設置するために必要な工具とテスト機器を収集します。

設置場所の計画

警告　**この装置は、出入りが制限された場所に設置されることを想定しています。出入りが制限された場所とは、特殊なツール、ロックおよびキー、または他のセキュリティ手段を使用しないと入室できない場所を意味します。**
ステートメント 1017

通常、設置場所を事前に準備しておく必要があります。準備の一環として、設置場所および Cisco ISE 3300 シリーズ アプライアンスが収容される装置ラックの見取り図を入手してください。

既存のアプライアンスの場所、および通信と電源を含む相互接続を判別します。通気に関するガイドライン（「通気に関するガイドライン」（P.A-8）を参照）に従って、アプライアンスに十分な冷気を行きわたらせてください。

アプライアンスの設置に関与するすべての担当者（設置担当者、エンジニア、監督者）が、お客様による承認のために Method of Procedure（MOP）の準備に参加する必要があります。詳細については、「Method of Procedure」（P.A-10）を参照してください。

次の項では、アプライアンスを設置する前に考慮する必要がある設置場所の要件に関するガイドラインについて説明します。

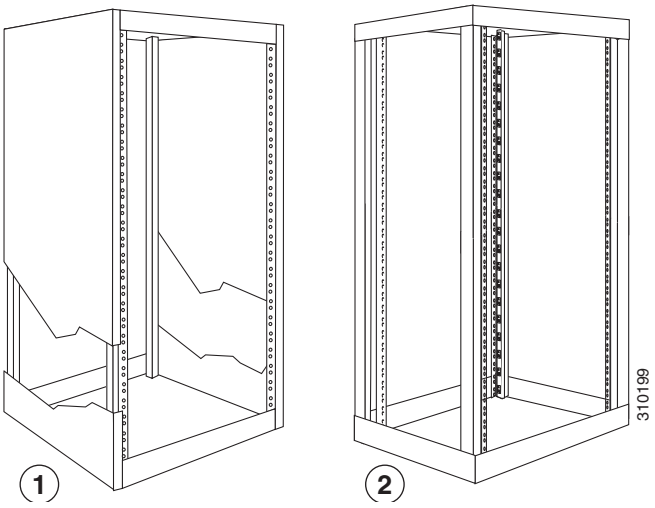
ラックへの設置の安全に関するガイドライン

Cisco ISE 3300 シリーズ アプライアンスは、装置ラックに関する EIA 標準（EIA-310-D）に準拠する、ほとんどの 4 支柱、電話会社タイプ（Telco タイプ）の 19 インチ装置ラックに設置できます。2 つの支柱にある取り付け穴の中心線間の距離は、18.31 インチ +/- 0.06 インチ（46.50 cm +/- 0.15 cm）でなければなりません。アプライアンスに付属のラック取り付けハードウェアは、ほとんどの 19 インチの装置ラックまたは Telco タイプのフレームに適しています。

（注）　可能な限り 4 支柱ラックを使用することが強く推奨されますが、ラックには、アプライアンスを取り付けるためにマウント フランジを提供する支柱が少なくとも 2 つ*必要です*。

図 A-1 に、4 支柱装置ラックの一般的な 2 つの例を示します。

図 A-1　　4 支柱装置ラックのタイプ



4 支柱（部分的に密閉）ラック

図 A-1 の図「1」に、前面に 2 つの支柱があり、背面にさらに 2 つの支柱がある、自立型の部分的に密閉されたラックを示します。Cisco ISE 3300 シリーズ アプライアンスは、このような閉鎖型ラックに設置できます。これは、このアプライアンスでは、内部コンポーネントの許容動作温度を保持するために、冷気が妨げられずにシャーシの前面に流れ、背面から出て行くようにする必要があるためです。

4 支柱（オープン）ラック

図 A-1 の図「2」に、前面に 2 つの支柱があり、背面に 2 つの支柱がある、自立型の 4 支柱のオープン ラックを示します。このタイプのラックの支柱は、多くの場合調整可能であるため、ラックの前面と面一に取り付けるのではなく、ラックの奥にラック取り付け型の装置を配置できます。

Cisco ISE 3300 シリーズ アプライアンスをラックに取り付ける前に、次のガイドラインを確認してください。

- ラックにアプライアンスを設置するには、2 人以上が必要です。
- 室温が 95 °F（35 °C）を下回っていることを確認します。
- 通気孔をふさがないでください。通常、6 インチ（15 cm）のスペースで通気が行きわたります。
- アプライアンスの設置の際は、ラックの下部から考慮してください。

- 複数のアプライアンスをラックの外側に同時に延ばさないでください。
- アプライアンスは、正しく接地されたコンセントに接続してください。
- ラックに複数のデバイスを設置する場合は、電源コンセントの過負荷が発生しないようにしてください。
- 110 ポンド（50 kg）を超える重さの物をラック取り付け型デバイスの上部に置かないでください。

設置場所の環境

正常に動作させるには、アプライアンスの配置、装置ラックまたは配線室のレイアウトが非常に重要です。配置が近すぎる機器、不適切な通気、およびアクセスできないパネルによって、誤動作やシャットダウンが生じ、メンテナンスが困難になる可能性があります。アプライアンスの前面パネルと背面パネルへのアクセスを計画します。

次の注意事項を考慮することで、アプライアンスに適した動作環境を確保し、環境による装置の故障を防ぐことができます。

- アプライアンスを使用する室内で、十分な換気が可能であることを確認してください。電子機器は放熱します。十分に空気循環されていないと、室内の温度が高くなり、機器を許容動作温度に冷却できなくなる場合があります。詳細については、「通気に関するガイドライン」（P.A-8）を参照してください。
- ラックの設置に、AC 電源、アース接続、およびネットワーク ケーブルのプロビジョニングも含まれていることを確認します。
- 十分なスペースを確保して、設置中にラックの周囲で作業できるようにします。次のことが必要です。
  - アプライアンスを移動、位置合わせ、および挿入するために、ラックに隣接する少なくとも 3 フィート（9.14 m）。
  - 設置後のメンテナンスのために、アプライアンスの前面と背面に少なくとも 24 インチ（61 cm）の空間。
- 2 つの支柱またはレールの間にアプライアンスを取り付けるには、使用可能な開口（2 つのマウント フランジの*内*端間の幅）は少なくとも 17.7 インチ（45.0 cm）でなければなりません。

（注） ラックマウント キットには、2 支柱の装置ラックは含まれていません。

- ケーブルと機器の接続を保護するには、適切なストレインレリーフ方法を使用してください。
- ネットワーク インターフェイス ケーブルでのノイズの干渉を回避するには、電源コード間または電源コードに沿って直接配置しないでください。
- 機器の破損を防ぐため、「静電破壊の防止」（P.A-5）に記載されている静電放電の防止手順に必ず従ってください。静電放電による損傷によって、即時または断続的な機器障害が発生する可能性があります。

通気に関するガイドライン

装置ラック内で十分な通気を確保するには、ラックの前面と背面に少なくとも 6 インチ（15.24 cm）の空間を維持することを推奨します。装置ラックと、ラックに配置されているアプライアンス内の通気が、ブロックまたは制限されている場合、またはラックに流れる換気の温度が高すぎると、装置ラック内の温度が上がり過ぎてアプライアンスが過熱する可能性があります。

また、設置場所では、可能な限り埃のない状態にする必要があります。埃はアプライアンスのファンに詰まる傾向があり、装置ラックと、ラックに配置されているアプライアンス内で冷気の流れが低下します。この種の通気の低下によって、温度が上がり過ぎて、アプライアンスがオーバーヒートするリスクが高まります。

さらに、次のガイドラインは、装置ラックの構成を計画する場合に役立ちます。

- 通気の他に、ラックの周囲に、メンテナンスに必要な空間を確保する必要があります。
- オープンラックにアプライアンスを設置する場合、ラックのフレームで前面の吸気口や背面の排気口をふさがないように注意してください。

温度と湿度に関するガイドライン

表 A-1 に、Cisco ISE 3300 シリーズ アプライアンスの稼働環境の設置場所と非稼働環境の設置場所の要件をリストします。アプライアンスは通常、リストされている範囲内で稼働します。ただし、最小パラメータまたは最大パラメータに近い温度の測定は、問題の可能性を示しています。

アプライアンスを設置する前に設置場所を正しく計画して準備して、臨界値に近づく前に、環境の異常を予期して修正することで、正常な動作を維持してください。

表 A-1　稼働環境仕様と非稼働環境仕様

仕様	最小	最大
動作時の温度	50 °F（10 °C）	95 °F（35 °C）
非動作時および保管時の温度	-40 °F（°C）	158 °F（70 °C）
動作時の湿度（結露しないこと）	10 %	90 %
非動作時および保管時の湿度（結露しないこと）	5 %	95 %
動作時の振動	5–500 Hz、2.20 g RMS ランダム	—

電源に関する考慮事項

Cisco ISE 3300 シリーズ アプライアンスは、AC 入力電源のみで構成します。すべての電源接続が National Electrical Code の規則と規制、および地域の規定に準拠していることを確認します。アプライアンスへの電源接続を計画する際には、次の注意事項と推奨事項に従う必要があります。

- 設置する前と、設置後に定期的に、設置場所の電源を調べ、質の良い（スパイクやノイズのない）電力が供給されていることを確認してください。必要に応じて、電力調整器を取り付けてください。
- AC 電源には次の機能があります。
  - 110 V または 220 V 運用の自動選択機能。
  - すべてのアプライアンスの電気コード （電源コードの近くにあるラベルは、アプライアンスの正しい電圧、周波数、電流引き込み、および消費電力を示しています）。

警告　この製品は設置する建物に回路短絡（過電流）保護機構が備わっていることを前提に設計されています。120 VAC、15 A（米国）（240 VAC、10 A（国際規格））以下のヒューズまたは回路ブレーカーが、相導体（すべての電流コンダクタ）で使用されていることを確認してください。ステートメント 13

- 装置ラックで適切に接地し、雷や電力サージによる損傷を防止してください。

警告　**この装置は、接地させる必要があります。絶対にアース導体を破損させたり、アース線が正しく取り付けられていない装置を稼働させたりしないでください。アースが適切かどうかはっきりしない場合には、電気検査機関または電気技術者に確認してください。ステートメント 1024**

- オペレータによる調整の必要がない、100 ～ 240 VRMS と 50 ～ 60 Hz の範囲内の入力電圧と周波数で AC 入力電源モジュールが稼働することを確認してください。表 A-2 に、電気入力に関する追加情報を示します。

表 A-2　電気入力の仕様

仕様	最小	最大
正弦波入力	50 Hz	60 Hz
入力電圧の低範囲	100 VAC	127 VAC
入力電圧の高範囲	200 VAC	240 VAC
おおよその入力キロボルト アンペア（kVA）	0.102 kVA	0.55 kVA

Method of Procedure

以前に説明したように、準備には設置計画または MOP の確認が含まれます。MOP は、設置前のチェックリストや作業のリスト、ガイドライン、または設置に進む前に対処して同意する必要がある考慮事項です。次に MOP がガイドラインとして機能する例を示します。

ステップ 1　担当者を割り当てます。

ステップ 2　担当者、機器、および工具の保護要件を決定します。

ステップ 3　保守に影響する可能性がある事故を評価します。

ステップ 4　設置の時期をスケジュールします。

ステップ 5　スペースの要件を決定します。

ステップ 6　所要電力を決定します。

ステップ 7　必要な手順またはテストを特定します。

ステップ 8　装置の計画において、設置する各 Cisco ISE 3300 シリーズ アプライアンスの配置の予備決定を行います。

ステップ 9　このハードウェア設置ガイドを確認します。

ステップ 10　設置のために交換可能なパーツ（ネジ、ボルト、ワッシャなど）のリストを確認して、特定します。

ステップ 11　必要な工具とテスト機器が使用可能であることを確認するために、必要な工具リストを調べます。詳細については、「必要な工具と部品」（P.A-13）を参照してください。

ステップ 12　設置を実行します。

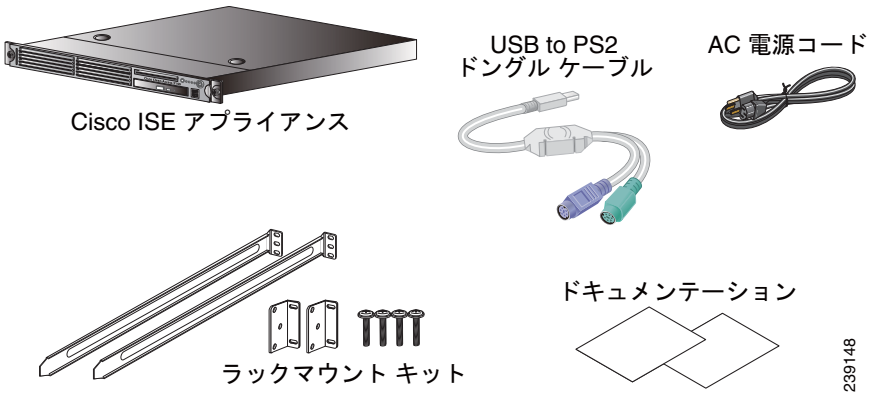
出荷内容の開梱と確認

Cisco ISE 3300 シリーズ アプライアンスの出荷パッケージは、出荷中の通常の運搬に関連する製品損傷の可能性を減らすように設計されています。製品の損傷の可能性を減らすには、アプライアンスを元のシスコの梱包材で移送してください。そうしないと、アプライアンスが損傷を受ける可能性があります。また、設置の準備ができるまでは、アプライアンスを出荷容器から出さないでください。

アプライアンス、ケーブル、および注文したオプションの機器は、複数の容器で出荷されることがあります。損傷を受けたり、足りなかったりする項目を記録するために、*Notes* セクションがあります。図 A-2 に、Cisco ISE 3300 シリーズ アプライアンスでの出荷項目を表示します。

（注）　Cisco ISE 3300 シリーズ アプライアンスの出荷時に使用される梱包材料を廃棄しないでください。アプライアンスを移動または出荷する場合に、将来梱包材料が必要になります。

図 A-2　　Cisco ISE 3300 シリーズ アプライアンスと一緒に出荷される項目



出荷時の損傷がないかどうか、すべての項目を調べます。損傷を受けている物がある場合、またはアプライアンスの設置または構成の問題が発生した場合は、カスタマー サービス担当者にお問い合わせください。

（注）　ラックマウント キットには、2 支柱の装置ラックは含まれていません。

『Cisco Information Packet』と保証

『*Cisco Information Packet*』には、保証、保守、およびサポート情報が記載されています。次の手順を実行して、ブラウザで次の場所を指定して Cisco.com から『*Cisco Information Packet*』、保証、およびライセンス契約書にアクセスし、これらをダウンロードしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/cetrans.htm

Warranties and License Agreements ページが表示されます。

『*Cisco Information Packet*』を表示するには、次の手順を完了します。

ステップ 1　[情報パケット番号（Information Packet Number）] フィールドをクリックし、製品番号 78-5235-03D0 が選択されていることを確認します。

ステップ 2　文書を表示する言語を選択します。

ステップ 3　[実行（Go）] をクリックします。

Information Packet の [Cisco Limited Warranty and Software License] ページが表示されます。

ステップ 4　このページから文書をオンラインで見ることも、[PDF] アイコンをクリックして、文書をダウンロードし、印刷することもできます。

PDF ファイルを表示し、印刷するには、Adobe Acrobat Reader が必要です。Adobe の Web サイトからこれをダウンロードできます。

お手持ちの製品について、翻訳またはローカライズされた保証情報を表示するには、次の手順を完了します。

ステップ 1　[保証文書番号（Warranty Document Number）] フィールドに、次の製品番号を入力します。

```
78-5236-01C0
```

ステップ 2　文書を表示する言語を選択します。

ステップ 3　[実行（Go）] をクリックします。

Cisco warranty ページが表示されます。

ステップ 4　このページから文書をオンラインで見ることも、[PDF] アイコンをクリックして、文書を PDF 形式でダウンロードし、印刷することもできます。

また、Cisco Service and Support の Web サイトにアクセスして、サポートを受けることもできます。

http://www.cisco.com/en/US/support/

ハードウェア保証期間

90 日間です。

ハードウェアに関する交換、修理、払い戻しの手順

シスコ、またはその代理店では、Return Materials Authorization（RMA）要求を受領してから、10 営業日以内に交換部品を出荷するように商業上合理的な努力を致します。お届け先により、実際の配達所要日数は異なります。

（注）　シスコは購入代金を払い戻すことにより一切の保証責任とさせて頂く権利を留保します。

RMA 番号の入手

製品を購入されたシスコの代理店にお問い合わせください。製品を直接シスコから購入された場合は、シスコの営業担当者にお問い合わせください。

次の項目を記入して、参照用に保管してください。

製品情報	説明
製品の購入先	
購入先の電話番号と Web サイトのロケーション	
製品モデル番号：	
製品シリアル番号：[1]	
保守契約番号	

1. 詳細については、「Cisco ISE 3300 シリーズ アプライアンス ハードウェアの概要」（P.2-1）、「Cisco ISE 3355 のシリアル番号の場所」（P.2-9）、「Cisco ISE 3395 のシリアル番号の場所」（P.2-14）、および「アプライアンスのシリアル番号の確認」（P.C-5）を参照してください。

必要な工具と部品

注意　ラックマウント キットの固定器具パックには、8 個のラック用ネジが含まれています。これらのネジを調べて、ラックの穴に合った適切なサイズであることを確認する必要があります。ラックのネジ穴に誤ったサイズのネジを使用すると、ラックが損傷を受ける可能性があります。

4 支柱ラックに Cisco ISE 3300 シリーズ アプライアンスを設置するために必要な工具および部品は、次のとおりです。

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**

- 静電気防止用コードとリスト ストラップ。
- No.2 プラス ドライバ。
- メモリまたはその他のコンポーネントをアップグレードする場合は、カバーを取り外すためにマイナス ドライバ（小型の 3/16 インチ（0.476 cm）と中型の 1/4 インチ（0.625 cm））。
- ラックマウント キット。キットの内容の詳細については、「4 支柱ラックマウント ハードウェア キットの使い方」（P.B-3）を参照してください。
- LAN ポートに接続するためのケーブル（構成によって異なる）。
- イーサネット（LAN）ポートへの接続用にイーサネット スイッチ。

Cisco ISE 3300 シリーズ アプライアンスの初期構成を行うには、次の物のいずれかが必要です。

- USB キーボードおよび VGA モニタ。

  または

- 9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、およびハードウェア フロー制御なし用に構成されたコンソール端末（ASCII 端末または端末エミュレーション ソフトウェアが実行されている PC）。
- シリアル（コンソール）ポートに接続するためのコンソール ケーブル。ヌルモデム ケーブルが推奨されます。

インストレーション チェックリスト

設置を支援し、行った作業の履歴レコードを提供するには、次のインストレーション チェックリストを使用してください。このチェックリストのコピーを作成し、各タスクの完了時にエントリにマーク付けします。

チェックリストの記入が完了したら、各 Cisco ISE 3300 シリーズ アプライアンスのチェックリストのコピーを、新しいアプライアンスのその他のレコードとともに、サイト ログに含めます（サイト ログの作成については、「サイト ログの作成」（P.A-14）を参照してください）。

設置場所のインストレーション チェックリスト：Cisco ISE 3300 シリーズ アプライアンス：

タスク	確認者	日付
インストレーション チェックリストをコピーする		
サイト ログに背景説明を含める		
設置場所の電源電圧を確認する		
設置場所の電源チェック完了		
必要な工具が使用可能であることを確認する		
追加の機器が使用可能であることを確認する		
Cisco ISE 3300 シリーズ アプライアンスを受け取る		
資料『*Cisco Information Packet*』を受け取る		
アプライアンス コンポーネントを確認する		
最初の電源投入成功		
ASCII 端末（ローカル設定用）を確認する		
信号の距離制限を確認する		
起動シーケンス手順完了		
初期動作を確認する		

サイト ログの作成

Cisco ISE 3300 シリーズ アプライアンスに対して実行されるすべての設置、メンテナンス、アップグレード、交換、および変更のレコードとして機能するサイト ログを保持できます。ログは、アプライアンスの近くの場所で利用できる状態にして、タスクを実行する人がアクセスできるようにします。

インストレーション チェックリスト（「インストレーション チェックリスト」（P.A-14）を参照）を使用して、アプライアンスの設置とメンテナンスの手順を確認します。サイト ログに記録する内容は次のとおりです。

- 設置の進行：アプライアンスのインストレーション チェックリストのコピーを作成して、サイト ログに挿入します。各タスクの完了時に、エントリを作成します。
- アップグレード、取り外し、およびメンテナンス手順：進行中のアプライアンスのメンテナンスと拡張履歴のレコードとして、サイト ログを使用します。アプライアンスでタスクを実行するたびに、サイト ログを更新して、次の情報を反映させます。
  - 新規アダプタ カードの取り付け
  - アダプタ カードの取り外しまたは交換と、その他のアップグレード

- 設定変更
- メンテナンスのスケジュールと要件
- 実行したメンテナンス手順
- 間欠的な問題
- コメントとメモ

イーサネット コネクタおよびコンソール ポートのガイドライン

この項では、Cisco ISE 3300 シリーズ アプライアンス用のイーサネット コネクタおよび非同期シリアル コンソール ポートについて、次のガイドラインを示します。

- 各 Cisco ISE 3300 シリーズ アプライアンスは、背面パネル上でイーサネット コネクタを提供し、ギガビット イーサネット 0 ポートは非シールドより対線（UTP）ケーブル接続を使用します（カテゴリ 6 UTP ケーブルが推奨されます）。セグメントの最大距離は 328 フィート（100 m）です。

  UTP ケーブルは、通常の電話に使用されるケーブルと似ています。ただし、UTP ケーブルは、電話ケーブルでは満たされない電気規格を満たします（これらの UTP ケーブルは、インストレーション パッケージには含まれていません）。

- 各 Cisco 3300 シリーズ アプライアンスは、背面パネル上で、（コンソール端末を使用して）アプライアンスにローカルでアクセスできるようにする非同期シリアル コンソール ポートを提供します。コンソール端末（ASCII 端末または端末エミュレーション ソフトウェアが実行されている PC のいずれか）をコンソール ポートに接続する前に、正しいタイプのケーブル接続を確認して使用することが重要です。

注意　ネットワーク セキュリティの潜在的な脅威を回避するために、接続を使用していないときは、Cisco ISE のコンソール管理ポートから物理的に切断しておくことを強く推奨します。詳細については、http://seclists.org/fulldisclosure/2011/Apr/55 を参照してください（Cisco ISE、Cisco NAC アプライアンス、および Cisco Secure ACS ハードウェア プラットフォームに適用されます）。

（注）　コンソール ケーブルは Cisco ISE 3300 シリーズ アプライアンスに含まれていません。

APPENDIX B

Cisco ISE 3300 シリーズ ハードウェアの設置

この付録では、Cisco Identity Services Engine（ISE）3300 シリーズ アプライアンスを設置する方法、および 3 つのサポートされるアプライアンス（Cisco ISE 3315、Cisco ISE 3355、および Cisco ISE 3395）のいずれかをネットワークに接続する方法について説明します。この情報は次のトピックに含まれています。

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**

警告 **この装置は、出入りが制限された場所に設置されることを想定しています。出入りが制限された場所とは、特殊なツール、ロックおよびキー、または他のセキュリティ手段を使用しないと入室できない場所を意味します。**
ステートメント 1017

ラックマウント構成のガイドライン

各 Cisco ISE 3300 シリーズ アプライアンスはラック ハンドル セットを備えています（出荷時取り付け）。アプライアンスを 4 支柱ラックに設置する際にこれらのハンドルを使用します。4 支柱ラック仕様に準拠した 19 インチ（48.3 cm）装置ラックに、アプライアンスをフロント（フラッシュ）マウントまたはミッドマウントできます。

（注） 内側の幅は 17.5 インチ（44.45 cm）であることが必要です。

実行する必要がある最初のタスクは、アプライアンスをブラケットにマウントすることです。アプライアンスをラックに設置した後は、マウントのために 1 つ分の EIA 1.75 インチ（4.4 cm）垂直マウント スペースまたは 1 ラック ユニット（RU）が必要です。

注意　冷却用の空気が前面から取り込まれ、アプライアンス内を循環してアプライアンスの背面から排出されるように、Cisco ISE 3300 シリーズ アプライアンスの前後に十分な空間を確保する必要があります。詳細については、「通気に関するガイドライン」（P.A-8）を参照してください。

「ラックへの設置の安全に関するガイドライン」（P.A-7）および次の情報は、装置ラックの構成を計画するために役立ちます。

- アプライアンスを装置ラックにマウントする際には、必ずラックを床にボルトでしっかりと固定してください。
- 1 つまたは複数のアプライアンスをラックに設置できるため、設置された全アプライアンスの重さがラックの可搬重量を超えないことを確認してください。さもないと、ラックが不安定になります。

注意　ラック内の装置の重さのため、一部の装置ラックでは、天井のブラケットにも固定するようになっています。このタイプの設置では、アプライアンスを設置するために使用するラックを建物の構造に必ずしっかりと固定してください。

- 「通気に関するガイドライン」（P.A-8）で推奨されているように、吸気および排気のための適切なスペースを確保するために、アプライアンスの前後に 6 インチ（15.2 cm）の間隔を確保してください。
- アプライアンスを過密状態のラックに設置することはやめてください。ラック内の他のアプライアンスとの間で空気が循環することにより、アプライアンスを通じた正常な冷却空気の流れが妨げられる可能性があり、その結果、アプライアンスの過熱を引き起こすリスクが高まります。
- 任意のアプライアンスのメンテナンス操作の実行のために、ラックの前後に 24 インチ（61 cm）以上の空間を確保してください。

注意　アプライアンスが過熱状態にならないようにするため、閉鎖型ラックや、適切に換気または適切な空調のサポートがない部屋にアプライアンスを設置しないでください。

- ケーブル管理については、各地のベスト プラクティスに従ってください。アプライアンスに接続されたケーブルが、装置の保守やアップグレードを行うために必要なアクセスの妨げにならないようにしてください。

（注）　ラック マウント ハードウェア キットには、2 支柱装置ラックは含まれていません。

Cisco ISE 3300 シリーズ アプライアンスの 4 支柱ラックへのマウント

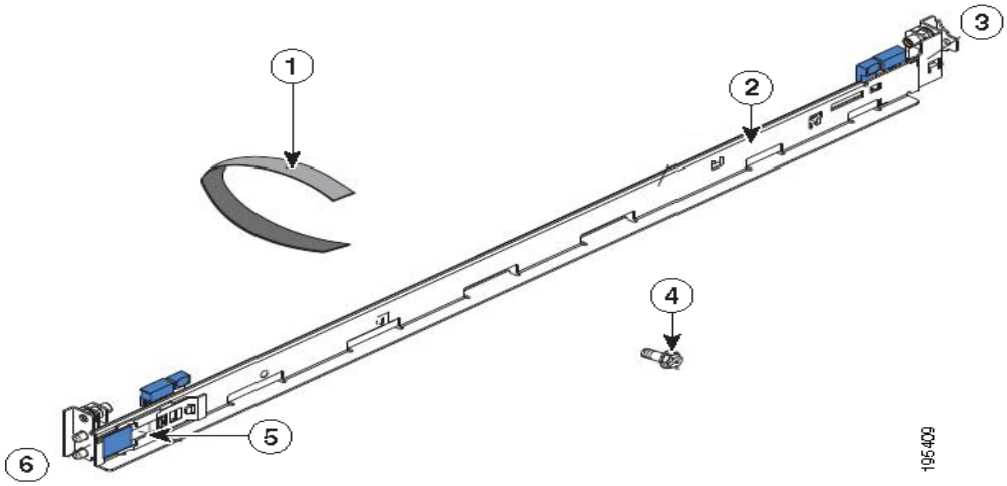
警告　**アプライアンスをラックに取り付け、サイド レール上で一杯に伸ばした場合、ラックが不安定になって転倒し、重大なけがを負うおそれがあります。レールを伸ばした場合や地震が発生した場合でもラックが不安定にならないようにするには、ラックを床に固定してください。**

ここでは、次のトピックについて説明します。

4 支柱ラックマウント ハードウェア キットの使い方

図 B-1 に、Cisco ISE 3300 シリーズ アプライアンスを 4 支柱ラックに設置するのに必要な項目を示します。

図 B-1　スライド レール ハードウェア上のリリース レバー



次の表で、図 B-1 の各コンポーネントについて説明します。

1	ケーブル ストラップ	**4**	M6 ネジ
2	スライド レール	**5**	輸送用ブラケット
3	レールの前面	**6**	レールの背面

表 B-1 に、ラックマウント ハードウェア キットの内容を示します。

表 B-1　ラックマウント ハードウェア キット

項目	数量
スライド レール	2
ケーブル ストラップ	6
M6 ネジ	6

スライド レールのラックへの取り付け

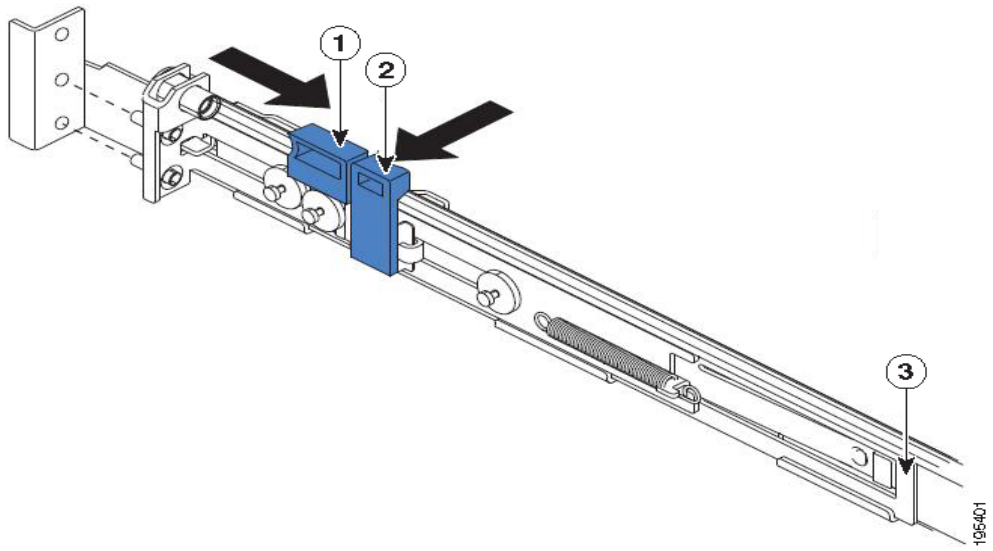
Cisco ISE 3300 シリーズ アプライアンスをラックへ取り付けるには、次の手順を実行します。

ステップ 1　スライド レールの背面にあるレール調整ブラケット（図 B-2 を参照）を押して、ブラケットが動かないようにします。

ステップ 2　調整タブ 1 と 2（図 B-2 を参照）を押し、レールロック キャリアを、カチッとはまるまでスライド レールの前面に向けてスライドさせます。

ステップ 3　調整タブ 1 と 2 を押し、レールロック キャリアを、カチッとはまるまでスライド レールの背面に向けてスライドさせます。

図 B-2　スライド レールのラックへの取り付け



次の表で、図 B-2 の各コンポーネントについて説明します。

1	調整タブ 1	**3**	レール調整ブラケット
2	調整タブ 2		

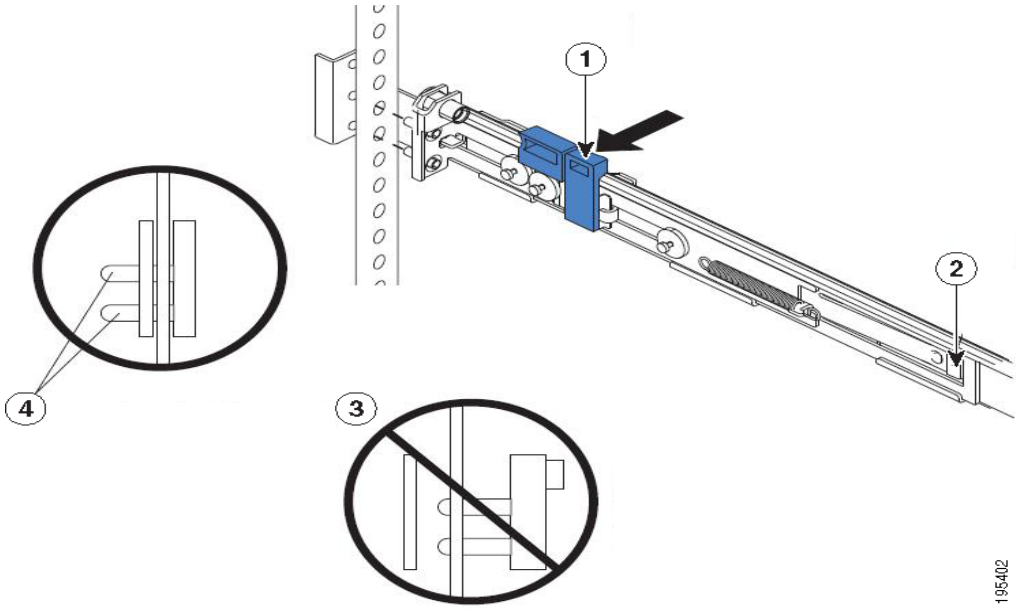
スライドレールの長さを調整する必要がある場合は、リリース タブ（図 B-3 を参照）を持ち上げ、カチッとはまるまでスライド レールの背面からレール調整ブラケットを完全に伸ばします。

ステップ 4　背面レールロック キャリアのピンを、後面マウント フランジの穴に合わせます。

ステップ 5　調整タブ（図 B-3 を参照）を押して、スライド レールの背面を背面マウント フランジに固定します。

（注）　ピンは、マウント フランジとスライド レールに完全に差し込んでください。

図 B-3　　スライドレール長の調整



次の表で、図 B-3 の各コンポーネントについて説明します。

1	調整タブ	**3**	ピン（マウント フランジとスライド レールに完全に差し込まれていない）
2	リリース タブ	**4**	ピン（マウント フランジとスライド レールに完全に差し込まれている）

ステップ 6　前面レールロック キャリア上のピン（図 B-4 を参照）を、前面マウント フランジに合わせます。

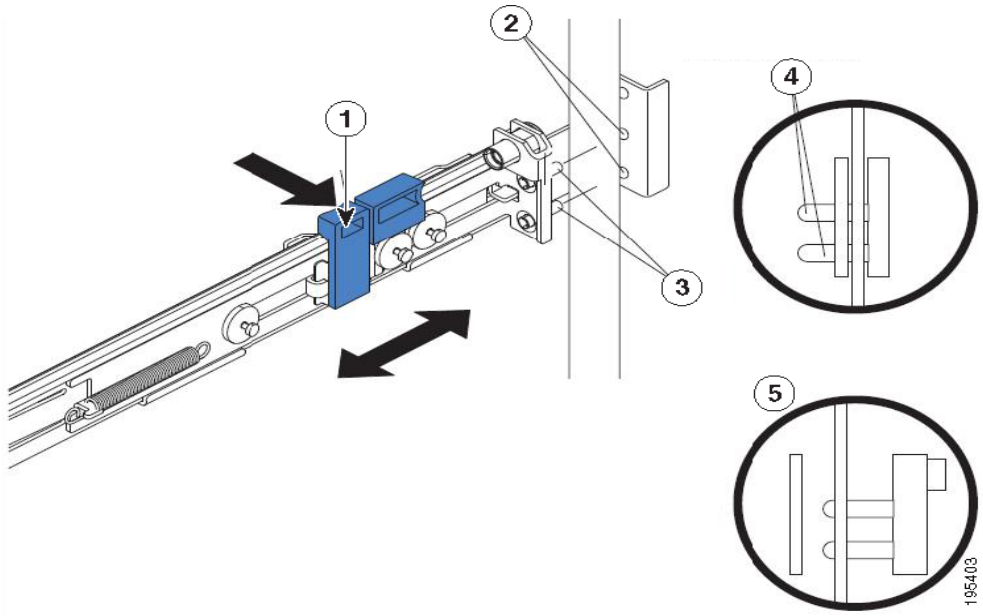
レール長を調整した場合は、レールロック キャリアをスライド レールの背面に向けて押し、スライド レールをマウント フランジに合わせます。

ステップ 7　調整タブを押して、スライド レールの前面を前面マウント フランジに固定します。

（注）　ピンは、マウント フランジとスライド レールに完全に差し込んでください。

ステップ 8　もう 1 つのスライド レールに対してこれらのステップを繰り返します。

図 B-4　スライド レールとマウント フランジの位置合わせ



次の表で、図 B-4 の各コンポーネントについて説明します。

1	調整タブ	4	ピン（マウント フランジとスライド レールに完全に差し込まれている）
2	マウント フランジ	5	ピン（マウント フランジとスライド レールに完全に差し込まれていない）
3	ピン		

アプライアンスのスライド レールへの取り付け

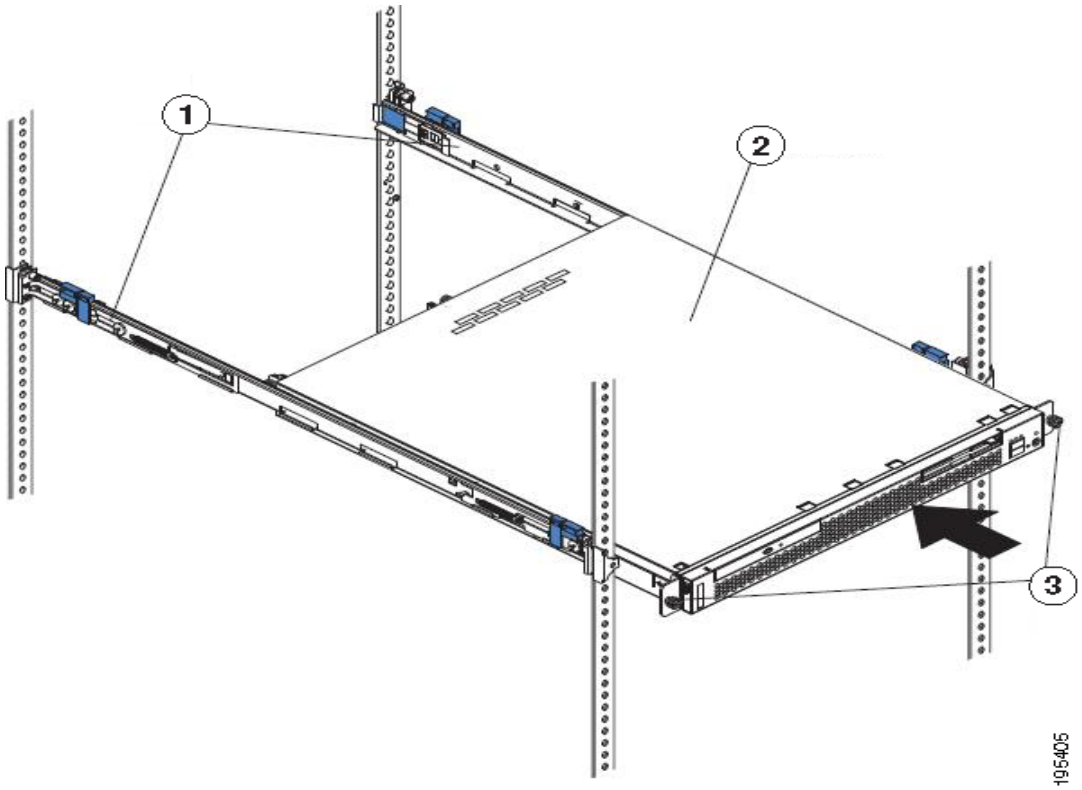
Cisco ISE 3300 シリーズ アプライアンスをスライド レールに取り付けるには、次の手順を実行します。

ステップ 1　サーバをスライド レールに合わせ、ラック キャビネットに完全に収まるまで押します。

ステップ 2　取り付けネジで、サーバを前面マウント フランジに固定します（図 B-5 を参照）。

（注）　スライド レールに取り付けられている輸送用ブラケットは、それが邪魔になってサーバをラック キャビネットに完全にスライドできない場合を除き、そのままにします。輸送用ブラケットを取り外す必要がある場合は、ステップ 3 を参照してください。

図 B-5　スライド レール上でのサーバの位置合わせ



次の表で、図 B-5 の各コンポーネントについて説明します。

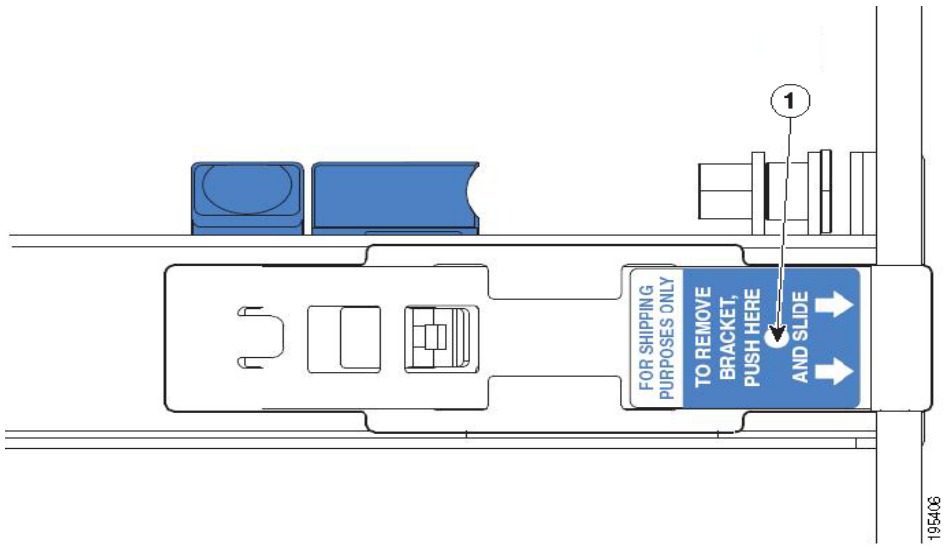
1	輸送用ブラケット	3	取り付けネジ
2	Cisco ISE 3300 シリーズ アプライアンス		

ステップ 3　輸送用ブラケット上で、図のようにリリース タブ（図 B-6 を参照）を押し、スライド レールから輸送用ブラケットを取り外します。

ステップ 4　もう一方の輸送用ブラケットに対してステップ 3 を繰り返します。輸送用ブラケットは、将来使用するために保管しておきます。

（注）　サーバが取り付けられた状態でラック キャビネットを輸送する場合は、その前に輸送用ブラケットをスライド レールに再度取り付ける必要があります。輸送用ブラケットを再度取り付けるには、逆の手順を実行します。

図 B-6　輸送用ブラケットの取り外し



次の表で、図 B-6 のコンポーネントについて説明します。

1	リリース タブ	

ケーブルの接続

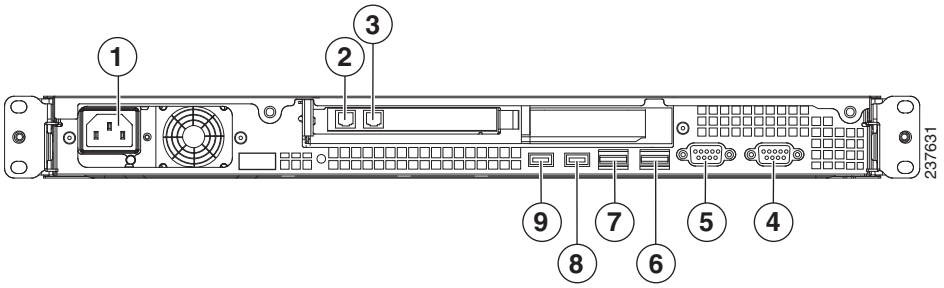
ここでは、Cisco ISE 3300 シリーズ アプライアンスをネットワークおよびアプライアンス コンソールに接続する方法について説明します。次の例では、図 B-7 に Cisco ISE 3315 アプライアンスを示します。他の Cisco ISE 3300 シリーズ アプライアンスの背面パネルの機能の具体的な位置については、次のトピックを参照してください。

- 「Cisco ISE 3355 背面パネルの機能」（P.2-11）
- 「Cisco ISE 3395 背面パネルの機能」（P.2-16）

次のトピックでは、ケーブルの接続および管理の方法について説明します。

- 「ネットワーク インターフェイスの接続」（P.B-10）
- 「コンソールの接続」（P.B-11）
- 「キーボードとビデオ モニタの接続」（P.B-13）
- 「ケーブル管理」（P.B-14）

図 B-7　Cisco ISE 3315 アプライアンスの背面パネル ビュー

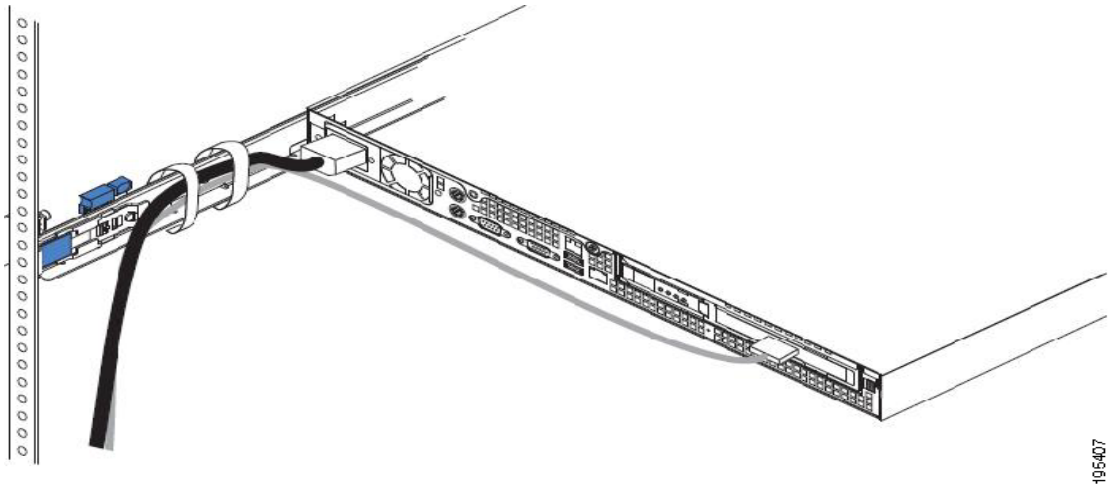


次の表で、図 B-7 の各コンポーネントについて説明します。

1	AC 電源装置ケーブル ソケット	6	NIC 2（eth1）ギガビット イーサネット インターフェイス
2	NIC 3（eth2）アドオン カード	7	NIC 1（eth0）ギガビット イーサネット インターフェイス
3	NIC 4（eth3）アドオン カード	8	背面 USB ポート 4
4	シリアル ポート	9	背面 USB ポート 3
5	ビデオ ポート		

ケーブル（必要に応じてキーボード、モニタ ケーブルなど）をサーバの背面に接続します。ケーブルはサーバの左隅にまとめ（図 B-8 に示すように背面パネルから見た場合）、ケーブル ストラップを使用してスライド レールに固定します。

図 B-8　ケーブルの接続



ネットワーク インターフェイスの接続

警告　**雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001**

ここでは、Cisco ISE 3300 シリーズ アプライアンス イーサネット ポートを接続する方法について説明します。RJ-45 ポートは、標準的なストレートおよびクロス カテゴリ 5 UTP ケーブルをサポートしています。

（注）　シスコではカテゴリ 5 UTP ケーブルを販売していません。市販のケーブルを使用してください。

ケーブルを Cisco ISE 3300 シリーズ アプライアンスのイーサネット ポートに接続するには、次の手順を実行します。

ステップ 1　アプライアンスの電源がオフになっていることを確認します。

ステップ 2　ケーブルの一方の端を、アプライアンス上のギガビット イーサネット 0 ポートに接続します。

ステップ 3　他方の端をネットワークのスイッチに接続します。

イーサネット ポート コネクタ

サポートされる各 Cisco ISE 3300 シリーズ アプライアンスには、2 個の内蔵デュアルポート イーサネット コントローラが搭載されています。これらのイーサネット コントローラは、10、100、または 1000 Mb/s ネットワークに接続するためのインターフェイスと全二重（FDX）機能を提供し、イーサネット LAN 上でデータを同時に送受信できます。各アプライアンスのイーサネット ポート コネクタの正確な位置については、次を参照してください。

- 「Cisco ISE 3315 背面パネルの機能」（P.2-8）
- 「Cisco ISE 3355 背面パネルの機能」（P.2-11）
- 「Cisco ISE 3395 背面パネルの機能」（P.2-16）

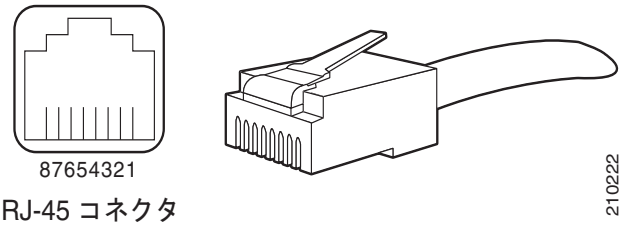
イーサネット ポートにアクセスするには、少なくともカテゴリ 5 または 5E（カテゴリ 6 の使用が推奨されます）UTP ケーブルをアプライアンスの背面にある RJ-45 コネクタに接続します。表 B-2 に、UTP ケーブルのカテゴリを示します。

表 B-2　UTP ケーブル接続カテゴリに対するイーサネットのガイドライン

タイプ	説明
10BASE-T	EIA カテゴリ 5 または 5E 以上の UTP（2 または 4 ペア）、最大 328 フィート（100 m）
100BASE-TX	EIA カテゴリ 5 または 5E 以上の UTP（2 ペア）、最大 328 フィート（100 m）
1000BASE-T	EIA カテゴリ 6 UTP（推奨）、カテゴリ 5E UTP または 5 UTP（2 ペア）、最大 328 フィート（100 m）

図 B-9 に、イーサネット RJ-45 ポートとプラグを示します。

図 B-9　RJ-45 ポートとプラグ



RJ-45 コネクタ

表 B-3 では、イーサネット コネクタで使用される RJ-45 ピン信号について説明します。

警告　**感電を防ぐため、安全超低電圧（SELV）回路を電話網電圧（TNV）回路に接続しないでください。LAN ポートには SELV 回路が、WAN ポートには TNV 回路が組み込まれています。一部の LAN ポートおよび WAN ポートは RJ-45 コネクタを使用しています。ケーブルを接続する際は、注意してください。ステートメント 1021**

表 B-3　イーサネット ポート（RJ-45）のピン割り当て

イーサネット ポートのピン	信号	説明
1	TxD+	送信データ +
2	TxD–	送信データ –
3	RxD+	受信データ +
4	終端ネットワーク	接続なし
5	終端ネットワーク	接続なし
6	RxD–	受信データ –
7	終端ネットワーク	接続なし
8	終端ネットワーク	接続なし

コンソールの接続

警告　**雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001**

注意　ネットワーク セキュリティの潜在的な脅威を回避するために、接続を使用していないときは、Cisco ISE のコンソール管理ポートから物理的に切断しておくことを強く推奨します。詳細については、http://seclists.org/fulldisclosure/2011/Apr/55 を参照してください（Cisco ISE、Cisco NAC アプライアンス、および Cisco Secure ACS ハードウェア プラットフォームに適用されます）。

各 Cisco ISE 3300 シリーズ アプライアンスには、コンソール端末をお使いのアプライアンスに直接接続できるようにする、データ回線終端装置モードのコンソール ポートがあります。アプライアンスのコンソール ポートでは、DB-9 シリアル コネクタが使用されています。

各 Cisco ISE 3300 シリーズ アプライアンス上のコンソール ポートには、EIA/TIA-232 非同期シリアル（DB-9）コネクタが含まれています。このシリアル コンソール コネクタ（ポート）を使用することで、端末（ターミナル エミュレーション ソフトウェアが動作する PC か ASCII 端末）をコンソール ポートに接続し、アプライアンスにローカルにアクセスできます。これは、次の方法のいずれかを使用して実行できます。

- 両端が DB-9 メスのストレート ケーブルの使用による、端末エミュレーション ソフトウェアが実行されている PC のコンソール ポートへの接続。
- 片方が DB-9 メスでもう一方が DB-25 オスのストレート ケーブルと、DB-25 メスから DB-25 メスへの変換アダプタの使用による、ASCII 端末のコンソール ポートへの接続。
- 端末またはターミナル エミュレーション ソフトウェアが動作する PC の、Cisco ISE 3300 シリーズ アプライアンスのコンソール ポートへの接続。

コンソール端末をお使いのアプライアンスに接続するには、次の手順を実行します。

ステップ 1　ストレート ケーブルを使用して端末をコンソール ポートに接続します。

ステップ 2　端末またはターミナル エミュレーション ソフトウェアを設定して、次の設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット
- ハードウェア フロー制御なし

シリアル（コンソール）ポート コネクタ

Cisco ISE 3300 シリーズ アプライアンスでは、1 個のシリアル ポート コネクタが、各アプライアンスの背面パネルにあります。各アプライアンスにおける各シリアル ポート コネクタの正確な位置については、次を参照してください。

- 「Cisco ISE 3315 背面パネルの機能」（P.2-8）
- 「Cisco ISE 3355 背面パネルの機能」（P.2-11）
- 「Cisco ISE 3395 背面パネルの機能」（P.2-16）

図 B-10 に、各 Cisco ISE 3300 シリーズ アプライアンスの背面パネルにある 9 ピン、オス、D シェル シリアル ポート コネクタのピン番号の割り当てを示します。定義されたピン番号の割り当ては、RS-232-C の業界標準に準拠しています。

図 B-10　　シリアル ポート コネクタ

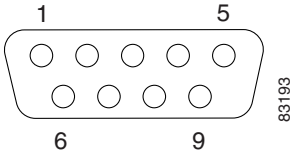


表 B-4 では、シリアル（コンソール）ポートのピン割り当てについて説明します。

表 B-4　DB-9 シリアル（コンソール）ポートのピン割り当て

シリアル ポート ピン	信号	説明
1	DCD	データ キャリア検出
2	RXD	受信データ
3	TXD	送信 / 転送データ
4	DTR	データ ターミナル レディ
5	GND	信号用接地
6	DSR	データ セット レディ
7	RTS	送信要求
8	CTS	送信可
9	RI	リング インジケータ

キーボードとビデオ モニタの接続

警告　雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

この項では、Cisco ISE 3300 シリーズ アプライアンスにキーボードとビデオ モニタを接続する方法について説明します。キーボードやビデオ モニタを接続する代わりに、Cisco ISE 3300 シリーズ アプライアンスにシリアル コンソール接続を確立できます。次のガイドラインに注意してください。

- Cisco ISE 3300 シリーズ アプライアンスは、マウス デバイスの使用をサポートしていません。
- Cisco ISE 3300 シリーズ アプライアンスは、各アプライアンスで前面パネルと背面パネルの両方に USB ポートを提供します。このポートは、キーボード（USB ポート）またはビデオ モニタ（ビデオ ポート）接続を確立するのに使用できます。

各アプライアンスの USB およびビデオ ポートの具体的な位置については、次を参照してください。

- 「Cisco ISE 3315 背面パネルの機能」（P.2-8）
- 「Cisco ISE 3355 背面パネルの機能」（P.2-11）
- 「Cisco ISE 3395 背面パネルの機能」（P.2-16）

お使いのアプライアンスにキーボードおよびビデオ モニタを接続するには、次の手順を実行します。

ステップ 1　アプライアンスの電源がオフになっていることを確認します。

ステップ 2　PS/2（キーボード）用のキーボード ケーブルの端を、アプライアンスの背面パネルにあり、提供される USB to PS/2 ドングル アダプタに接続します。

ステップ 3　ビデオ モニタ ケーブルの端を、アプライアンスにある PS/2 VGA ポートに接続します。Cisco ISE 3315 には、背面パネルにビデオ ポートが 1 つあります。Cisco ISE 3355 および Cisco ISE 3395 では、前面パネルと背面パネルに 1 つずつビデオ ポートがあります。

ステップ 4　アプライアンスの電源をオンにします。

ケーブル管理

ケーブル管理は、アプライアンスのセットアップの一部である最も視覚的な要素です。しかし、ケーブル管理の問題は費やした時間に対してプライオリティが高いタスクと見なされないため放置しがちです。今日のラックとエンクロージャは通常従来よりも多くの装置を収納するようになっているため、ラックごとの装置の取り付けの増加は、装置ラックの内側と外側のケーブル配線をより上手くまとめて、送り、管理する必要があることを意味しています。

ケーブル管理が適切でないと、ケーブルの損傷があったり、ケーブルのリルーティングまたは変更に時間がかかったりする可能性があるだけでなく、アプライアンスを冷却する重要な通気やアクセスを妨げる可能性もあります。これらの種類の問題は、装置のパフォーマンスが低下したり、ダウンタイムが長くなったりするおそれがあります。しかし、ケーブル管理の問題に対処するソリューションは、単純なケーブル管理リングから、垂直または水平収納容器、ケーブル トラフやはしごの使用まで、さまざまなものがあります。

すべての Cisco ISE 3300 シリーズ アプライアンスのケーブルは、ラック内のケーブル同士や装置の他の部分と干渉しないように、適切に整理する必要があります。各地のベスト プラクティスまたは電気プラクティスを使用して、アプライアンスに接続されているケーブルを適切に整理するようにします。これで、次のセクション「Cisco ISE 3300 シリーズ アプライアンスの電源投入」（P.B-14）に進んで、設置手順を続行できます。

Cisco ISE 3300 シリーズ アプライアンスの電源投入

警告　電源コードが接続されている場合は、電源に触れないでください。電源スイッチを備えたシステムの場合、電源スイッチがオフになっていても、電源コードが接続されていれば、電源装置内部に入力電圧がかかっています。電源スイッチのないシステムの場合、電源コードが接続されていれば、電源装置内部に入力電圧がかかっています。ステートメント 4

警告　この機器は接地されることを前提にしています。通常の使用時にホストが接地されていることを確認してください。ステートメント 39

この項では、次のトピックを扱います。

電源投入チェックリスト

次の条件を満たす場合、Cisco ISE 3300 シリーズ アプライアンスの電源投入に進むことができます。

- アプライアンスがしっかりとマウントされている。
- アプライアンスが適正に接地されている。
- すべての電源、ネットワーク、およびインターフェイス ケーブルが適切に接続されている。

電源投入手順

Cisco ISE 3300 シリーズ アプライアンスの電源を投入し、その初期化とセルフテストを確認するには、次の手順を実行します。次の手順が完了すると、アプライアンスを設定する準備ができます。図 B-12 に Cisco ISE 3315 アプライアンスを示します。他の Cisco ISE 3300 シリーズ アプライアンスの具体的な前面および背面パネルのビューと制御の説明については、次を参照してください。

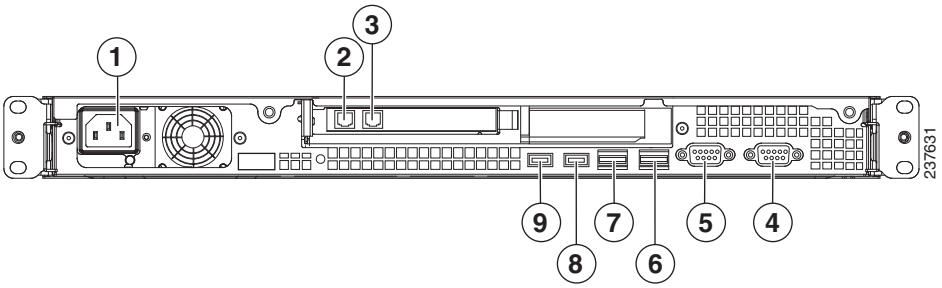
- Cisco ISE 3355 アプライアンス：
  - 「Cisco ISE 3355 前面パネルの機能」（P.2-9）
  - 「Cisco ISE 3355 背面パネルの機能」（P.2-11）
- Cisco ISE 3395 アプライアンス：
  - 「Cisco ISE 3395 前面パネルの機能」（P.2-14）
  - 「Cisco ISE 3395 背面パネルの機能」（P.2-16）

Cisco ISE 3300 シリーズ アプライアンスを電源投入するには、次の手順を実行します。

ステップ 1　「安全に関するガイドライン」（P.A-1）の情報を確認してください。

ステップ 2　AC 電源コードをアプライアンスの背面にある AC 電源ソケットに差し込みます。（Cisco ISE 3315 アプライアンスを示す図 B-11 の 1 番）。

図 B-11　　Cisco ISE 3315 アプライアンスの背面パネル ビュー



他の Cisco ISE 3300 シリーズ アプライアンスの AC 電源ソケットの位置については、以下を参照してください。

- 「Cisco ISE 3355 背面パネルの機能」（P.2-11）
- 「Cisco ISE 3395 背面パネルの機能」（P.2-16）

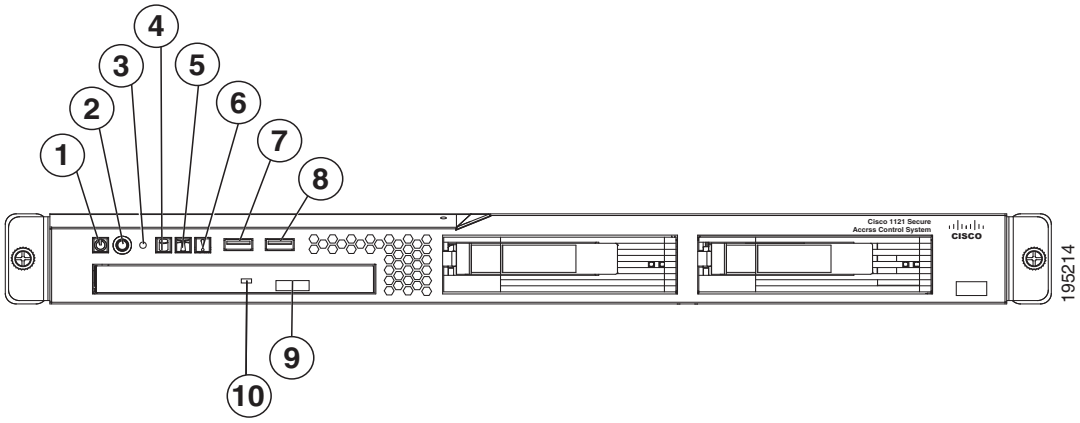
ステップ 3　AC 電源コードの他方の端を、設置場所で認定された AC 電源に接続します。

ステップ 4　アプライアンスの前面パネルで、AC 電源ボタン **On** を押してブート プロセスを開始します。Cisco ISE 3315 アプライアンスを示す図 B-12 の 2 番です。他の Cisco ISE 3300 シリーズ アプライアンスの AC 電源ボタンの位置については、以下を参照してください。

- 「Cisco ISE 3355 前面パネルの機能」（P.2-9）
- 「Cisco ISE 3395 前面パネルの機能」（P.2-14）

ステップ 5　Cisco ISE 3300 シリーズ アプライアンスの前面パネルの LED を確認します。例として、Cisco ISE 3315 アプライアンスが図 B-12 に示されています。「LED の確認」（P.B-16）に、3 つの Cisco ISE 3300 シリーズ アプライアンスすべての LED のステータスの一覧を示しています。

図 B-12　Cisco ISE 3315 アプライアンスの前面パネル ビュー



次の表に、図 B-12 に示す前面パネル機能と LED を定義します。

1	アプライアンス電源 LED	**6**	システム エラー LED
2	AC 電源制御ボタン	**7**	USB 1 コネクタ
3	リセット ボタン	**8**	USB 2 コネクタ
4	HDD アクティビティ LED	**9**	CD 取り出しボタン
5	ロケータ LED	**10**	CD ドライブ アクティビティ LED

LED の確認

Cisco ISE 3300 シリーズ アプライアンスが起動して動作中のときに、前面パネルの LED の状態を確認します。表 B-5 に、Cisco ISE 3300 シリーズ アプライアンスごとに表示される、LED カラー、電源の状態、アクティビティ、およびその他の重要なステータス インジケータを説明します。

表 B-5　Cisco ISE 3300 シリーズ アプライアンスの LED

LED タイプ	LED カラー	説明
Cisco ISE 3315 アプライアンスの前面パネルの LED		
電源ステータス	グリーン	• アプライアンスに AC 電源が接続され、電源がオンになっている場合、点灯します。 • アプライアンスの電源がオフになっている、AC 電源が切断されている、または動作電圧内でエラー条件が検出された場合、消灯します。

LED タイプ	LED カラー	説明
HDD アクティビティ	グリーン	• 進行中の HDD アクティビティがある場合、グリーンに点滅します。 • アクティビティが存在しない、アプライアンスがまだ起動していない、または起動プロセスでエラー条件が検出された場合、消灯します。
ロケータ（LED ボタン）	ブルー	• ロケータ ボタンが押された場合、ブルーに点滅します。
システム ヘルス	オレンジ	• システムが正常に動作している場合、消灯します。 • 点灯は、障害予測システムの次のようなしきい値条件を示します。 – 少なくとも 1 つのファン（システム ファンまたはプロセッサ ファン）で障害が発生しました。 – 少なくとも 1 つの温度センサー（システム温度センサーまたはプロセッサ温度センサー）が危険なレベルに達しました。 – 少なくとも 1 つのメモリ モジュールで障害が発生しました。 – 電源装置ユニットでエラーが発生しました。
Cisco ISE 3355 アプライアンスの前面パネルの LED		
HDD アクティビティ	グリーン	• 持続的な HDD アクティビティがある場合、点灯します。 • 進行中の HDD アクティビティがある場合、グリーンに点滅します。 • アクティビティが存在しない、HDD がアイドル状態、または HDD が無効な場合、消灯します。
HDD ステータス	オレンジ	• HDD がエラー状態である場合、点灯します。 • HDD が正常に動作しているか、システムが AC 電源から切断された場合、消灯します。
イーサネット（アイコン）	グリーン	• イーサネット インターフェイスが設定されて、アップ状態の場合、点灯します。 • イーサネット インターフェイスが現在設定されていないか、イーサネット インターフェイスがすべてダウン状態になっている場合、消灯します。

LED タイプ	LED カラー	説明
イーサネット インターフェイス アクティビティ（NIC 1 および NIC 2）	グリーン	• NIC 1 または NIC 2 にアクティビティが存在する場合、点灯します。 • NIC 1 または NIC 2 で進行中のアクティビティがある場合、グリーンに点滅します。 • NIC 1 または NIC 2 にアクティビティがない場合、消灯します。
情報	オレンジ	• 重大でないシステム イベントが発生した場合、点灯します。 • システムが正常に動作している場合、消灯します。
システム ヘルス	オレンジ	• システムが正常に動作している場合、消灯します。 • 点灯は、障害予測システムの次のようなしきい値条件を示します。 – 少なくとも 1 つのファン（システム ファンまたはプロセッサ ファン）で障害が発生しました。 – 少なくとも 1 つの温度センサー（システム温度センサーまたはプロセッサ温度センサー）が危険なレベルに達しました。 – 少なくとも 1 つのメモリ モジュールで障害が発生しました。 – 電源装置ユニットでエラーが発生しました。
ロケータ（ボタン）	ブルー	• ロケータ ボタンが押された場合、ブルーに点滅します。
イーサネット インターフェイス アクティビティ（NIC 3 および NIC 42）	グリーン	• NIC 3 または NIC 4 にアクティビティが存在する場合、点灯します。 • NIC 3 または NIC 4 で進行中のアクティビティがある場合、グリーンに点滅します。 • NIC 3 または NIC 4 にアクティビティがない場合、消灯します。

LED タイプ	LED カラー	説明
電源（ボタン）	グリーン	• アプライアンスに AC 電源が接続され、電源がオンになっている場合、点灯します。 • グリーンの短点滅は、アプライアンスの電源がオフになっていて、まだオンにすることができないことを示します。通常、アプライアンスのこの状態は 1 ～ 3 分間しか続きません。 • グリーンの長点滅は、アプライアンスの電源が現在オフになっていて、オンにすることができることを示します。 • 徐々に退色する点滅は、アプライアンスがパワーセーブ モードであることを示します（オンにすることができます）。 • アプライアンスの電源がオフになっている場合、消灯します（AC 電源が切断されています）。

LED タイプ	LED カラー	説明
Cisco ISE 3395 アプライアンスの前面パネルの LED		
HDD アクティビティ	グリーン	• 持続的な HDD アクティビティがある場合、点灯します。 • 進行中の HDD アクティビティがある場合、グリーンに点滅します。 • アクティビティが存在しない、HDD がアイドル状態、または HDD が無効な場合、オフになります。
HDD ステータス	オレンジ	• HDD がエラー状態である場合、点灯します。 • HDD が正常に動作しているか、システムが AC 電源から切断された場合、消灯します。
イーサネット（アイコン）	グリーン	• イーサネット インターフェイスが設定されて、アップ状態の場合、点灯します。 • イーサネット インターフェイスが現在設定されていないか、イーサネット インターフェイスがすべてダウン状態になっている場合、消灯します。
イーサネット インターフェイス アクティビティ（NIC 1 および NIC 2）	グリーン	• NIC 1 または NIC 2 にアクティビティが存在する場合、点灯します。 • NIC 1 または NIC 2 で進行中のアクティビティがある場合、グリーンに点滅します。 • NIC 1 または NIC 2 にアクティビティがない場合、消灯します。
情報	オレンジ	• 重大でないシステム イベントが発生した場合、点灯します。 • システムが正常に動作している場合、消灯します。

LED タイプ	LED カラー	説明
システム ヘルス	オレンジ	• システムが正常に動作している場合、消灯します。 • 点灯は、障害予測システムの次のようなしきい値条件を示します。 – 少なくとも 1 つのファン（システム ファンまたはプロセッサ ファン）で障害が発生しました。 – 少なくとも 1 つの温度センサー（システム温度センサーまたはプロセッサ温度センサー）が危険なレベルに達しました。 – 少なくとも 1 つのメモリ モジュールで障害が発生しました。 – 電源装置ユニットでエラーが発生しました。
ロケータ（ボタン）	ブルー	• ロケータ ボタンが押された場合、ブルーに点滅します。
イーサネット インターフェイス アクティビティ（NIC 3 および NIC 42）	グリーン	• NIC 3 または NIC 4 にアクティビティが存在する場合、点灯します。 • NIC 3 または NIC 4 で進行中のアクティビティがある場合、グリーンに点滅します。 • NIC 3 または NIC 4 にアクティビティがない場合、消灯します。
電源（ボタン）	グリーン	• アプライアンスに AC 電源が接続され、電源がオンになっている場合、点灯します。 • グリーンの短点滅は、アプライアンスの電源がオフになっていて、まだオンにすることができないことを示します。通常、アプライアンスのこの状態は 1 ～ 3 分間しか続きません。 • グリーンの長点滅は、アプライアンスの電源が現在オフになっていて、オンにすることができることを示します。 • 徐々に退色する点滅は、アプライアンスがパワーセーブ モードであることを示します（オンにすることができます）。 • アプライアンスの電源がオフになっている場合、消灯します（AC 電源が切断されています）。

Cisco ISE 3300 シリーズの LED の詳細については、「トラブルシューティングの概要」（P.C-1）を参照してください。オペレーティング システムが起動したら、基本的なソフトウェアの設定を初期化できます。設定手順については、第 3 章「Cisco ISE 3300 シリーズ アプライアンスの設定」を参照してください。

APPENDIX C

Cisco ISE 3300 シリーズ アプライアンスのトラブルシューティング

Cisco Identity Services Engine（ISE）3300 シリーズ アプライアンスでは、出荷前に精密なテストを実施しています。問題が発生した場合は、この付録を使用して問題を特定するか、そのアプライアンスが問題の原因であるかどうかを調べてください。

初期起動時に過度の温度または過度の消費電力の状態になることはまれですが、「サイト環境とアプライアンスの保守」（P.D-1）に記載されている、Cisco ISE 3300 シリーズ アプライアンスをサポートするために必要な一般的な環境条件を参照してください。

（注） この付録の手順では、Cisco ISE 3300 シリーズ アプライアンスの初期起動時におけるトラブルシューティングについて、アプライアンスが工場出荷時の設定のままであることを前提に解説します。コンポーネントを削除または交換している、もしくはデフォルト設定を変更している場合は、この付録の推奨事項を適用できない場合もあります。

この付録では、アプライアンスに起こりうる問題すべてを網羅するのではなく、お客様で頻繁に確認されている問題を中心に取り上げます。この付録では、次のトピックについて説明します。

トラブルシューティングの概要

初期システム起動時、次の事項を確認します。

- 外部電源ケーブルが接続されており、正しい電源が供給されている。詳細については、「電源に関する考慮事項」（P.A-9）、「Cisco ISE 3300 シリーズ アプライアンスの電源投入」（P.B-14）、および「電源および冷却システムのトラブルシューティング」（P.C-3）を参照してください。
- アプライアンスのファンとブロワーが稼働していることを確認する。「通気に関するガイドライン」（P.A-8）および「電源および冷却システムのトラブルシューティング」（P.C-3）を参照してください。
- アプライアンスのソフトウェアが正常に起動している。

- アダプタ カード（インストールされている場合）がスロット内に正しく設置されており、それぞれのカードが問題なく初期化（およびアプライアンス ソフトウェアによってイネーブル化）されている。

以上の条件がそれぞれ満たされており、ハードウェアの設置が完了している場合は、基本設定に移ります。Cisco ISE のこのリリースが提供する機能を理解するには、『*Cisco Identity Services Engine User Guide, Release 1.1*』を参照してください。Cisco ISE の機能を正しく設定するには、第 3 章「Cisco ISE 3300 シリーズ アプライアンスの設定」を参照してください。

問題の原因を特定できない場合は、問題の解決の最善の進め方についてシスコ カスタマー サービス担当者にお問い合わせください。Cisco Technical Assistance Center（TAC）の詳細については、アプライアンスに付属の『*Cisco Information Packet*』マニュアルを参照するか、次の Web サイトにアクセスしてください。

http://www.cisco.com/tac/

Cisco TAC にお問い合わせいただく前に、次の情報をお手元にご用意ください。

- アプライアンスのシャーシ タイプおよびシリアル番号。
- 保守契約または保証書（『*Cisco Information Packet*』を参照）。
- ソフトウェアの名前、タイプ、およびバージョンまたはリリース番号（該当する場合）。
- 新規アプライアンスの入手日。
- 発生した問題または状況の簡単な説明、問題の特定または再現のために行った手順、および問題解決のために行った手順の説明。

（注） カスタマー サービス担当者には、必ず Cisco ISE 3300 シリーズ アプライアンスの初期インストール後に行ったアップグレードまたはメンテナンスの情報をすべてお伝えください。サイト ログ情報については、「サイト ログの作成」（P.A-14）を参照してください。

問題解決

問題解決のキーは、問題を特定の箇所またはタスクに絞り込むことです。Cisco ISE 3300 シリーズ アプライアンスの動作と実行されるべき動作とを比較します。トラブルシューティングを行う場合は、特定の症状を定義し、症状を引き起こしうる潜在的な問題を認識する必要があります。次に、それぞれの潜在的な問題を体系的に実行し、症状や状況が消えるまでその問題を（最も起こりやすいものから最も起こりにくいものまで）排除することを試みます。

トラブルシューティングを実行する際は、次の手順を実行してこれらのガイドラインに従ってください。

ステップ 1　問題を分析し、明確に問題を記述したものを定義します。症状と潜在的な原因を定義します。

ステップ 2　考えられる原因または潜在的な原因を特定するための事実を収集します。

ステップ 3　収集した事実に基づいて考えられる原因または潜在的な原因を検討します。

ステップ 4　それらの原因に基づいて処置プランを作成します。最も起こりうる問題から始めて、1 つの変数だけをテストする計画を考えます。

ステップ 5　実行計画を実施します。各手順を慎重に実行し、症状が消えたか確かめます。

ステップ 6　結果を分析し、問題が解決したかどうかを確認します。問題が解決していれば、プロセスは完了です。

問題が解決していない場合は、リストで次に可能性の高い原因に基づいて処置プランを作成します。

ステップ 4 に戻り、問題が解決するまでプロセスを繰り返します。処置プランを実施するときは、変更をすべて元に戻してください。

ヒント　一度に変更する変数は、1 つだけです。

（注）　アプライアンスの前面および背面パネルにある LED は、アプライアンスのパフォーマンスと動作を確認するためのものです。これら LED の詳細については、「LED の読み取り方」（P.C-5）を参照してください。

トラブルシューティングの際は、まず、次に示すアプライアンスのサブシステムを確認してください。

- 電源および冷却システム：外部電源、電源ケーブル、およびアプライアンス ファンを確認してください。さらに、不十分な通気、阻害された換気、過度の埃や汚れ、ファン障害、または電源および冷却システムに影響を与える可能性のある環境条件を確認してください。
- アダプタ カード：アダプタ カードの LED を確認することで、障害を検知できます。
- ケーブル：アプライアンスをネットワークに接続している外部ケーブルがすべてしっかりと順序正しく装着されているかを確認します。

電源および冷却システムのトラブルシューティング

電源 LED およびファンは、電源の問題のトラブルシューティングを行う際に役立ちます。次の項目を確認し、問題を特定します。

- Cisco ISE 3300 シリーズ アプライアンスが電源に接続されているとき、アプライアンスの前面パネルにある電源 LED が点灯しているかを確認します。点灯していない場合、AC 電源コードの接続を確認します。それでも電源 LED が消灯している場合は、電源に障害が発生している可能性があります。
- アプライアンスがオンになっても、すぐにシャットダウンする場合は、
  - これが環境的に誘発されたシャットダウンかどうかを確認します。詳細については、「環境レポート機能」（P.C-4）の項を参照してください。
  - 冷却ファンを確認します。冷却ファンが動作していない場合、アプライアンスは過熱されて自動的にシャットダウンします。

    冷却ファンが動作していないのであれば、冷却ファンの電源接続を確認します。

    電源接続を確認する際は、アプライアンスをシャットダウンして外部ケーブルを取り除いてから、アプライアンスを開けます。
  - アプライアンスの吸気口と排気口に何もないことを確認します。
  - 環境に関連する設置場所の要件を満たしているかを確認します（「温度と湿度に関するガイドライン」（P.A-9）を参照）。
- アプライアンスの一部は起動しても、LED が点灯しない場合は、アプライアンスの前面パネルにある電源 LED を確認して電源障害の有無を確認します。
  - LED が点灯している場合は、電源は機能しています。
  - LED が点灯していない場合は、『*Cisco Information Packet*』で保証情報を確認するか、シスコ カスタマー サービス担当者にお問い合わせください。

環境レポート機能

Cisco ISE 3300 シリーズ アプライアンスは、過度の電流、電圧、および温度の状態をモニタして検出する保護回線を備えています。

電源がシャットダウンまたは停止状態になった場合、AC 電源の再投入は 15 秒間オフの状態になってから、1 秒間オンの状態になって電源をリセットします。次の条件によって、アプライアンスが異常な高温状態になる可能性があります。

- 冷却ファンの障害
- アプライアンスが設置されている室内の空調の障害
- 冷却ベントへの通気の阻害（吸気または排気）

発見した問題を修正するための手順を実行します。環境における動作条件の情報については、「温度と湿度に関するガイドライン」（P.A-9）を参照してください。

アダプタ カード、ケーブル、接続のトラブルシューティング

ネットワーク障害は、アダプタ カード、ケーブルまたはケーブル接続、もしくはハブやウォール ジャック、WAN インターフェイス、ターミナルなどの外部デバイスが原因になることがあります。次の症状を確認して、問題を特定します。

- Cisco ISE 3300 シリーズ アプライアンスがアダプタ カードを認識しない。
  - アダプタ カードがスロット内に確実に挿入されているかを確認する。
  - アダプタ カードの LED を確認する。各アダプタ カードにはそれぞれ固有の LED のセットが当てられています。
  - ソフトウェア リリースがアダプタ カードをサポートしているかを確認する。アダプタ カード付属の資料を参照してください。
- アダプタ カードは認識されるが、インターフェイス ポートが初期化されない。
  - アダプタ カードがスロット内に確実に挿入されているかを確認する。
  - 外部ケーブルの接続を確認する。
  - ソフトウェア リリースがアダプタ カードをサポートしているかを確認する。アダプタ カード付属の資料を参照してください。
- Cisco ISE 3300 シリーズ アプライアンスが正常に起動しない、または常時もしくは断続的に再起動する。
  - アダプタ カードがスロット内に確実に挿入されているかを確認する。
  - アプライアンス シャーシまたはアプリケーション ソフトウェアを確認する。保証情報については、アプライアンスに付属の『*Cisco Information Packet*』マニュアルを参照するか、シスコ カスタマー サービス担当者にお問い合わせください。
- ターミナルでコンソール ポートを使用しており、Cisco ISE 3300 シリーズ アプライアンスが起動してもコンソール画面がフリーズする。
  - 外部コンソールの接続を確認する。
  - ターミナルのパラメータが次のとおり設定されていることを確認する。

    (a) ターミナルとアプライアンスのデータ レートが同じに設定されている（デフォルトは 9600 bps）

    (b) 8 データ ビット

    (c) パリティ生成またはパリティ チェックを実行していない

（d）1 ストップ ビット

- Cisco ISE 3300 シリーズ アプライアンスでは、アダプタ カードが取り除かれた場合にだけ、電源がオンになり、起動します。アダプタ カードを確認してください。保証情報については、アプライアンスに付属の『*Cisco Information Packet*』マニュアルを参照するか、カスタマー サービス担当者にお問い合わせください。
- Cisco ISE 3300 シリーズ アプライアンスでは、特定のケーブルが切断された場合にだけ、電源がオンになり、起動します。ケーブルに問題がある可能性があります。保証情報については、アプライアンスに付属の『*Cisco Information Packet*』マニュアルを参照するか、シスコ カスタマー サービス担当者にお問い合わせください。

LED の読み取り方

Cisco ISE 3300 シリーズ アプライアンスの LED は、次の役割を果たします。

- アプライアンスで利用可能な基本電源を示す。
- ハード ディスク ドライブ、CD/DVD ドライブ、およびネットワーク アクティビティのステータスを示す。

前面パネルの LED

サポートされる Cisco ISE 3300 シリーズ アプライアンスの前面パネルの LED は、次の場所でサポート図とともに表で説明されています。

- 「Cisco ISE 3315 前面パネルの機能」（P.2-6）
- 「Cisco ISE 3355 前面パネルの機能」（P.2-9）
- 「Cisco ISE 3395 前面パネルの機能」（P.2-14）

背面パネルの LED

サポートされる Cisco ISE 3300 シリーズ アプライアンスの背面パネルの LED は、次の場所でサポート図とともに表で説明されています。

- 「Cisco ISE 3315 背面パネルの機能」（P.2-8）
- 「Cisco ISE 3355 背面パネルの機能」（P.2-11）
- 「Cisco ISE 3395 背面パネルの機能」（P.2-16）

アプライアンスのシリアル番号の確認

Cisco ISE 3300 シリーズ アプライアンスで、シリアル番号のラベルは各アプライアンスの前面パネルで見つかります。これらは、次の場所で示されています。

- 「Cisco ISE 3315 のシリアル番号の場所」（P.2-6）
- 「Cisco ISE 3355 のシリアル番号の場所」（P.2-9）
- 「Cisco ISE 3395 のシリアル番号の場所」（P.2-14）

APPENDIX D

Cisco ISE 3300 シリーズ アプライアンスの保守

Cisco Identity Services Engine (ISE) 3300 シリーズ アプライアンスはすべて、注文時に設定でき、インストールできる状態で工場から出荷されます。アプライアンスを所有するネットワーク環境にインストールおよび設定した後、アプライアンスが正常に稼働すること、およびネットワークに統合されていることを確認するため、特定のメンテナンス手順や操作を実行する必要がある場合もあります。この種の予防手順は、アプライアンスの正常稼働を維持し、コストがかかる上に時間のかかるサービス手順を最小限に抑えることができます。

注意 問題発生を防止するためには、この付録の手順を実行する前に、「関連資料」（P.-xiii）、および「安全に関するガイドライン」（P.A-1）をすべて確認してください。

次の項では、アプライアンスのパフォーマンスや寿命に悪影響を与える可能性のあるさまざまな環境要因について説明します。

サイト環境とアプライアンスの保守

適切な予防保守とは、外面の清掃や検査など、定期的に目視でアプライアンスを検査することです。この付録では、次のトピックでサイトとアプライアンスの保守についてベスト プラクティスを説明します。

一般的な外面清掃と検査

この項では、アプライアンスの外面清掃の要件について説明します。また、ケーブルおよびアダプタ カードの検査についてのガイドラインも提供します。

注意　アプライアンスの表面に洗浄液を吹きかけないでください。スプレーのしぶきがアプライアンスに入り、電気的な問題や内部コンポーネントの腐食の可能性が高まります。

アプライアンス

研磨剤が入っていない、表面を削らない柔らかい布で清掃します。溶剤、研磨剤入りの洗浄剤、およびティッシュ ペーパーは*使用しないでください*。アプライアンスが（大量の埃などで）汚れている場合は、湿らせた柔らかい布でアプライアンスの表面をやさしく拭きとります。水や液体は、必ずすぐにアプライアンスから拭きとってください。

埃と微粒子

稼働環境が清潔であれば、埃やその他の微粒子による悪影響を大幅に減らすことができます。埃や微粒子は絶縁体として作用したり、アプライアンスの機械コンポーネントの動作を妨害したりすることがあります。日常の定期的な清掃を実行する他に、アプライアンスの汚れを防ぐために、次のガイドラインに従ってください。

- アプライアンスの近くでの喫煙を禁止する。
- アプライアンスの近くでの飲食を禁止する。

ケーブルとコネクタ

アプライアンスに接続されているケーブルとコネクタをすべて定期的に検査します。この作業で、ケーブルとコネクタが正しく接続されていることを確認し、損耗および状態の目視検査し、接続のゆるみがあれば問題になる前に検出します。

アダプタ カード

アダプタ カードの接続を確認します。アプライアンスにアダプタ カードがしっかり装着されており、緩んだり機械的に損傷していたりしないかを確認してください。

腐食

指や手の皮脂や、高温または多湿の環境に長時間さらされると、アダプタ カードの金メッキされたエッジ コネクタやピン コネクタが腐食する可能性があります。アダプタ カードのコネクタの腐食は、徐々に進むため、最終的には電気回路が断続的に障害を起こす事態へと発展する場合があります。

腐食を防ぐため、アダプタ カードの端子には触れないでください。湿気や塩分の多い環境はすべて腐食が進みやすいため、腐食要素からアプライアンスを保護することは特に重要となります。また、腐食を防止する方法として、極端に温度差のある環境でアプライアンスを使用しないでください。詳細については、「温度」（P.D-3）を参照してください。

冷却

電源装置およびアプライアンス自体の内部の排気ファンは、アプライアンスの前面にあるいくつかの吸気口から空気を吸い込んで背面の排気口から吐き出すことで、電源装置とアプライアンスを冷却します。

ただし、これらのファンは埃やその他の微粒子もアプライアンス内に取り込みます。この結果、汚れが蓄積され、アプライアンスの内部温度上昇の直接の原因になる可能性があります。上昇した温度と汚れは、さまざまなアプライアンスのコンポーネントの正常な動作を妨げます。

このような状況を回避するには、作業環境を可能な限り清潔に保ち、アプライアンス周辺の埃や汚れの量を減らすことを推奨します。このベスト プラクティスは、ファンによってアプライアンス内に引き込まれる汚染物質の量を減らします。

温度

極端な温度差は、集積回路の経年劣化の促進や障害、またはデバイスの機械的な故障など、さまざまな障害の原因となります。

極端な温度変動によってソケット内の集積回路が緩むと、ディスク ドライブ プラッタでは膨張収縮が起こり、データの読み取りエラーや書き込みエラーの直接の原因になる可能性があります。Cisco ISE アプライアンスの熱放射の範囲は、341 ～ 1024 BTU（100 ～ 300 W）です。

温度によってアプライアンスのパフォーマンスが受ける悪影響を最小限に抑えるため、次のガイドラインに従ってください。

- 表 D-1 に、Cisco ISE アプライアンスの設置場所の高度に基づき、維持されるべき気温を示します。

表 D-1　　気温のメンテナンス

アプライアンスの状態	高度	気温
On	3000 フィート（0 ～ 914.4 m）	50.0 ～ 95.0 °F（10 ～ 35 °C）
On	3000 ～ 7000 フィート（914.4 ～ 2133.6 m）	50.0 ～ 89.6 °F（10 ～ 32 °C）
Off	最高高度：7000 フィート（2133.6 m）	50.0 ～ 109.4 °F（10 ～ 43 °C）
Shipping	最高高度：7000 フィート（2133.6 m）	-40 ～ 140 °F（-40 ～ 60 °C）

- アプライアンスの換気が適切であることを確認してください。閉鎖型の壁面ユニット内や布の上にアプライアンスを設置しないでください。熱がこもる原因となります。直射日光があたる場所にアプライアンスを置くことは避けてください（特に午後）。冬場の暖房の吹き出し口を含め、あらゆる種類の熱源の側にアプライアンスを設置しないでください。

高地では、特に適切な換気が重要となります。標高の高い場所の他、高温の環境でアプライアンスを稼働させる場合も最適なパフォーマンスが得られない可能性があります。次のガイドラインに従ってください。

- アプライアンスのすべてのスロットおよび開口部で、特にアプライアンス背面パネルにあるファンの吹き出し口が塞がれていないことを確認する。
- 定期的にアプライアンスを掃除して、過熱の一因になる可能性がある埃やゴミの蓄積を防ぐ。

- アプライアンスが異常な低温にさらされた場合、2 時間のウォームアップ時間をとって、通常の動作温度範囲に戻ってから電源を入れる。このプラクティスに従わないと、内部コンポーネント、特にハード ディスク ドライブに損傷を与える可能性があります。

湿度

湿度の高い状況では、アプライアンス内に水分が入り込み、湿気に犯される可能性があります。この湿気が原因で、内部コンポーネントの腐食と、電気抵抗、熱伝導性、物理的強度、サイズなどの特性の劣化が起こることがあります。アプライアンス内で極度に湿気が溜まると、電気的短絡が発生し、アプライアンスに甚大な被害を与える可能性があります。

各アプライアンスは、相対湿度 8 ～ 80 %、1 時間あたり 10 % の温度変化で動作するよう規定されています。温暖期には冷房で、寒冷期には暖房で室温が管理されているビル内では、一般的にアプライアンスが許容できる湿度が維持されます。

ただし、異常に湿度の高い場所にアプライアンスが設置されている場合は、除湿機で許容範囲内の湿度に保ってください。

高度

高度の高い（低気圧の）場所でアプライアンスを稼働させると、強制対流冷却の効率が低下し、アーク放電やコロナ効果に関連した電気的な問題が発生する可能性があります。また、このような状況では、電解コンデンサなどの、内部圧力がかかっている密閉コンポーネントが動作しなかったり、その効率が低下したりする場合もあります。

静電放電

静電放電は、人体やその他の特定の物質に静電気が蓄積することで発生します。通常、この静電気はカーペットの上を歩くなどの単純な動作で発生します。

静電放電は、静電気が放電する現象です。帯電した人がアプライアンスのコンポーネントに触れることで発生します。こうした静電放電は、特に集積回路（IC）などのコンポーネント故障の原因になります。特に相対湿度が 50 % 未満の乾燥した環境で、静電放電は問題となります。静電放電の影響を軽減するには、次のガイドラインに従ってください。

- 静電気防止用リスト ストラップを着用する。静電気防止用リスト ストラップが用意できない場合は、アプライアンスの塗装されていない金属面を定期的に触れて静電気を逃がします。
- コンポーネントは、取り付けるまで静電気防止用パッケージに入れたままにする。
- ウールまたは合成繊維の衣服を着用しない。

EMI および RFI

アプライアンスからの EMI および RFI は、アプライアンスの近くで稼働しているラジオやテレビの受信機などのデバイスに悪影響を与える可能性があります。また、アプライアンスから放出される無線周波数がコードレス電話や低出力の電話に影響をおよぼすこともあります。

RFI は、10 kHz を超える周波数を発生させる EMI として定義されます。この種の干渉は、電源ケーブルや電源、または無線電波のように空気を介して、アプライアンスから他のデバイスへと伝播します。米国連邦通信委員会（FCC）は、コンピュータ装置が放出する EMI および RFI の量を制限する固有の規制を公表しています。各アプライアンスは、これら FCC の規制に準拠します。

EMI および RFI の可能性を低減するには、次のガイドラインに従ってください。

- 必ずカバーを取り付けた状態でアプライアンスを稼働する。
- すべての周辺ケーブル コネクタのネジがアプライアンス背面の対応するコネクタにしっかりと取り付けられていることを確認する。
- アプライアンスに周辺機器を接続する際は、必ず金属製のコネクタ シェル付きシールド ケーブルを使用する。

磁気

ハードディスク ドライブはデータを磁気で記憶するため、磁気の影響を受けやすくなっています。ハードディスク ドライブは、次のタイプの磁気を発生させるもののそばに保管しないでください。

- モニタ
- プリンタ
- 電話（電動ベル使用）
- 蛍光灯

電源の中断

アプライアンスは、特に AC 電源から供給される電圧の変動の影響を受けやすくなっています。過電圧、低電圧、または過渡電圧（またはスパイク）の問題は、メモリからデータを消去するだけでなく、コンポーネントの障害を発生させることもあります。このような種類の問題からアプライアンスを保護するには、電源ケーブルを常に正しく接地し、次のいずれかの方法、または両方の方法を使用します。

- アプライアンスを専用の電力回路に設置する（他の電気機器と回路を共有させない）。
- ベスト プラクティスで、アプライアンスの電力回路を次の装置と**共有させない**こと。
  - コピー機
  - テレタイプ
  - レーザー プリンタ
  - ファクス機
  - その他の電動装置

記述された機器に加え、アプライアンスの電源に対する最大の脅威は、落雷によるサージまたは停電です。

アプライアンスに電源が入っているときに停電が発生した場合、停電が一時的なものであったとしても、すぐにアプライアンスの電源を切り、電源コードから外してください。アプライアンスを接続したままにしていると、電力が復旧した際に問題が発生する可能性があります。

お使いの Cisco ISE 3300 シリーズ アプライアンスの保守

この項では、次のアプライアンス関連の内容について説明します。

ラック キャビネットの輸送の準備

Cisco ISE 3300 シリーズ アプライアンスをインストールした後、別の場所にそれを輸送しようとする前に、必要な輸送前のタスクをすべて実行していることを確認してください。

輸送用に Cisco ISE 3300 シリーズ アプライアンスを準備するには、次の手順を実行してください。

ステップ 1　大きなネジ（図 D-1 を参照）を取り外し、廃棄します。

ステップ 2　前面ネジを取り外して保管します。

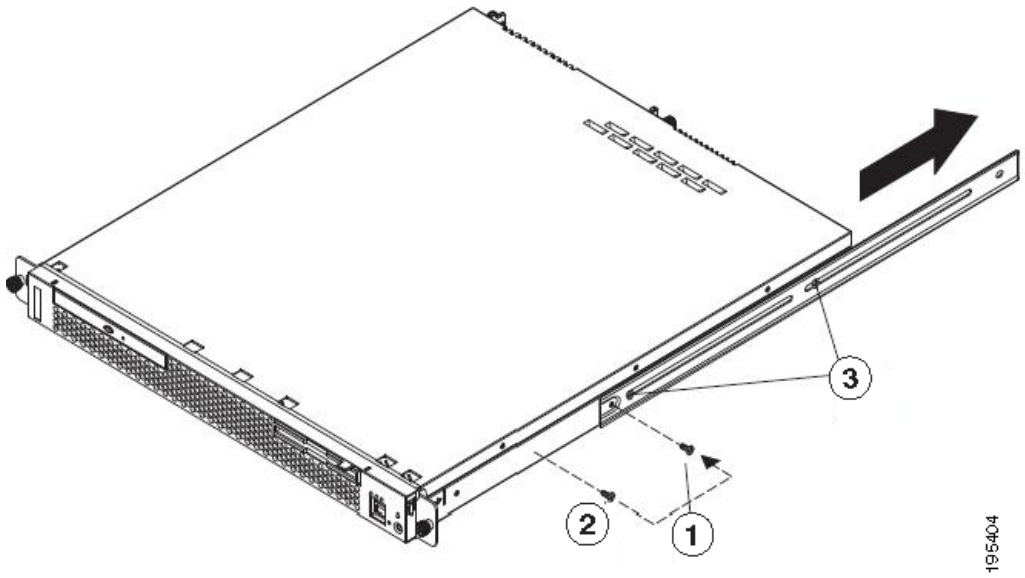
ステップ 3　残り 2 本の背面のネジを緩めます。

ステップ 4　レールを一杯に伸ばし、保管しておいたネジを大きなネジがあった場所に挿入します。

ステップ 5　すべてのネジを締めてレールを固定します。

ステップ 6　反対側のレールに対してステップ 1 ～ 5 を繰り返します。

図 D-1　　ラック キャビネットの輸送の準備



次の表で、図 D-1 の各コンポーネントについて説明します。

1	大きなネジ	3	背面ネジ（2）
2	前面ネジ		

ステップ 7　サーバをラックに固定します。

a. 必要に応じて、サーバの背面からケーブルを外します。

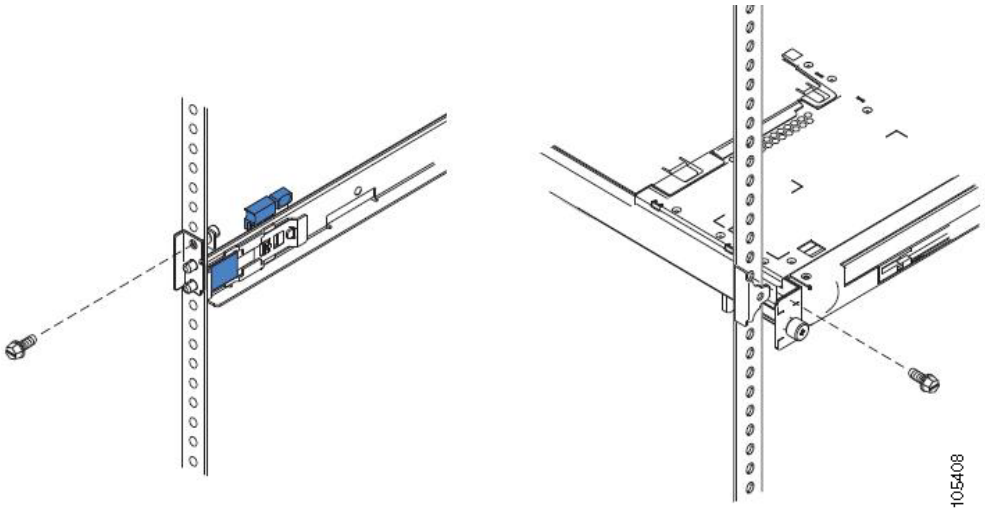
b. サーバをラックの外に 150 mm（6 インチ）スライドさせ、M6 ネジを各スライド レールに挿入します。

c. M6 ネジでサーバをラック キャビネットに固定します（図 D-2 を参照）。

ステップ 8　レールがラック キャビネットの背面に向けて完全に伸びていることを確認します。

スライド レールから輸送用ブラケットを取り外してある場合は、サーバが取り付けられた状態でラック キャビネットを輸送する前に、輸送用ブラケットを再度取り付ける必要があります。図 B-6（P.B-8）に示した手順と逆の手順を実行して、輸送用ブラケットを取り付けます。

図 D-2　ラック キャビネットを別の場所に移動するための準備



Cisco ISE 3300 シリーズ アプライアンスの取り外しまたは交換

警告　**オン/オフ スイッチのあるシステムを扱う際は、事前に AC 電源をオフにして、電源コードを外しておいてください。ステートメント 1**

警告　**本製品の最終処分は、各国のすべての法律および規制に従って行ってください。ステートメント 1040**

ここでは、次のトピックについて説明します。

- 「Cisco ISE 3300 シリーズ アプライアンスの取り外し」（P.D-8）
- 「Cisco ISE 3300 シリーズ アプライアンスの交換」（P.D-8）

Cisco ISE 3300 シリーズ アプライアンスの取り外し

Cisco ISE 3300 シリーズ アプライアンスをネットワークから取り外すには、次の手順を実行してください。

ステップ 1　取り外すアプライアンスの電源を切ります。

ステップ 2　電源コードとネットワーク ケーブルを外します。

ステップ 3　アプライアンスをラックから物理的に取り外します。

通常、Cisco ISE 3300 シリーズ アプライアンスは、ネットワーク上で定期的に通信しているため、ネットワークは、アプライアンスが応答しなくなったことを検出すると、アプライアンスへの要求の送信をすべて停止します。この変更は、ユーザが確認できます。

（注）　別のアプライアンスがネットワークに接続されている場合、ネットワークは別のアプライアンスに要求を送信し続けます。

Cisco ISE 3300 シリーズ アプライアンスの交換

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　交換しようとしているアプライアンスがネットワークから取り外されていることを確認します。

ステップ 2　取り外したアプライアンスに対して使用したのと同じ設置手順を使用して、新しいアプライアンスを設置します。

ステップ 3　取り外したアプライアンスに使用したのと同じ設定パラメータを使用して、新しいアプライアンスを設定します。

APPENDIX E

Cisco ISE 3300 シリーズ アプライアンスのポート リファレンス

この付録では、Cisco ISE が外部アプリケーションやデバイスとのイントラネットワーク通信に使用する、伝送制御プロトコル（TCP）およびユーザ データグラム プロトコル（UDP）のポートの一覧を示します。

表 E-1 に、ポートの一覧を TCP および UDP のポート番号ごとに表示して、関連機能、サービス、またはプロトコルを示し、またすべての特定のポートに関連する情報を説明します。これは、4 つのギガビット イーサネット ポート（GbEth0、GbEth1、GbEth2、および GbEth3）に適用されます。この表に示される Cisco ISE ポートは、対応するファイアウォールでオープンになっている必要があります。ポートのリストは、ファイアウォールの設定、アクセス コントロール リスト（ACL）の作成、および Cisco ISE ネットワーク上でのサービスの設定の際に役立つ可能性のある情報を提供します。

表 E-1　Cisco ISE のサービスとポート

Cisco ISE ノード	ISE サービス	ギガビット イーサネット 0 のポート	ギガビット イーサネット 1 のポート	ギガビット イーサネット 2 のポート	ギガビット イーサネット 3 のポート
管理 ISE ノード	管理	• TCP：22（セキュア シェル [SSH] サーバ） • TCP：80[1]（HTTP） • TCP：443[1]（HTTPS） **（注）** ポート 80 は、ポート 443 にリダイレクトされます（設定不可）。 **（注）** ポート 80 および 443 は、管理 Web アプリケーションをサポートしていて、デフォルトでイネーブルになっています。	Cisco ISE 管理は、ギガビット イーサネット 0 でのみ使用できます。	Cisco ISE 管理は、ギガビット イーサネット 0 でのみ使用できます。	Cisco ISE 管理は、ギガビット イーサネット 0 でのみ使用できます。
	複製および同期	• TCP：443（HTTPS SOAP） • TCP：1521[2]（データベース リスナーおよび AQ） • インターネット制御メッセージ プロトコル（ICMP）（ハートビート）	• TCP：1521[2]（データベース リスナーおよび AQ）	• TCP：1521[2]（データベース リスナーおよび AQ）	• TCP：1521[2]（データベース リスナーおよび AQ）
	監視	• UDP：161（Simple Network Management Protocol [SNMP] クエリー） **（注）** このポートは、ルート テーブルによって異なります。			

表 E-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	ISE サービス	ギガビット イーサネット 0 のポート	ギガビット イーサネット 1 のポート	ギガビット イーサネット 2 のポート	ギガビット イーサネット 3 のポート
モニタリング ISE ノード	管理	• TCP：22（SSH サーバ） • TCP：80[1]（HTTP） • TCP：443[1]（HTTPS）			
	複製および同期	• TCP：443（HTTPS） • TCP：1521[2]（データベース リスナーおよび AQ） • ICMP（ハートビート）	• TCP：1521[2]（データベース リスナーおよび AQ）	• TCP：1521[2]（データベース リスナーおよび AQ）	• TCP：1521[2]（データベース リスナーおよび AQ）
	ロギング	• UDP：20514（syslog） （注）　デフォルト ポートは、外部ログ用に設定できます。	• UDP：20514（syslog） （注）　デフォルト ポートは、外部ログ用に設定できます。	• UDP：20514（syslog） （注）　デフォルト ポートは、外部ログ用に設定できます。	• UDP：20514（syslog） （注）　デフォルト ポートは、外部ログ用に設定できます。
ポリシー サービス ISE ノード	管理	• TCP：22（SSH サーバ） • TCP：80[1]（HTTP） • TCP：443[1]（HTTPS）			
	複製および同期	• TCP：443（HTTPS） • TCP：1521[2]（データベース リスナーおよび AQ） • ICMP（ハートビート）	• TCP：1521[2]（データベース リスナーおよび AQ）	• TCP：1521[2]（データベース リスナーおよび AQ）	• TCP：1521[2]（データベース リスナーおよび AQ）

表 E-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	ISE サービス	ギガビット イーサネット 0 のポート	ギガビット イーサネット 1 のポート	ギガビット イーサネット 2 のポート	ギガビット イーサネット 3 のポート
ポリシー サービス ISE ノード（続き）	セッション	• UDP：1645、1812（RADIUS 認証） • UDP：1646、1813（RADIUS アカウンティング） • UDP：1700、3799（RADIUS 認可変更 [CoA]） （注） UDP ポート 1700 は、設定できません。 • TCP：88、389、464（アウトバウンド AD および Lightweight Directory Access Protocol [LDAP]） • UDP：30514（syslog） （注） これは、セッション サービスを介した内部サービスです。 • UDP：45588、45590 （注） UDP ポート 45588 および 45590 は、クラスタリング サポートに対するポリシー サービス通信をサポートします。	• UDP：1645、1812（RADIUS 認証） • UDP：1646、1813（RADIUS アカウンティング） • UDP：1700、3799（RADIUS 認可変更 [CoA]） （注） UDP ポート 1700 は、設定できません。 • TCP：88、389、464（アウトバウンド AD および Lightweight Directory Access Protocol [LDAP]） • UDP：30514（syslog） （注） これは、セッション サービスを介した内部サービスです。 • UDP：45588、45590 （注） UDP ポート 45588 および 45590 は、クラスタリング サポートに対するポリシー サービス通信をサポートします。	• UDP：1645、1812（RADIUS 認証） • UDP：1646、1813（RADIUS アカウンティング） • UDP：1700、3799（RADIUS 認可変更 [CoA]） （注） UDP ポート 1700 は、設定できません。 • TCP：88、389、464（アウトバウンド AD および Lightweight Directory Access Protocol [LDAP]） • UDP：30514（syslog） （注） これは、セッション サービスを介した内部サービスです。 • UDP：45588、45590 （注） UDP ポート 45588 および 45590 は、クラスタリング サポートに対するポリシー サービス通信をサポートします。	• UDP：1645、1812（RADIUS 認証） • UDP：1646、1813（RADIUS アカウンティング） • UDP：1700、3799（RADIUS 認可変更 [CoA]） （注） UDP ポート 1700 は、設定できません。 • TCP：88、389、464（アウトバウンド AD および Lightweight Directory Access Protocol [LDAP]） • UDP：30514（syslog） （注） これは、セッション サービスを介した内部サービスです。 • UDP：45588、45590 （注） UDP ポート 45588 および 45590 は、クラスタリング サポートに対するポリシー サービス通信をサポートします。

表 E-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	ISE サービス	ギガビット イーサネット 0 のポート	ギガビット イーサネット 1 のポート	ギガビット イーサネット 2 のポート	ギガビット イーサネット 3 のポート
ポリシー サービス ISE ノード（続き）	ゲストおよびスポンサー ポータル	• TCP：8443（HTTPS） **（注）** TCP ポート 8443 は、デフォルトでイネーブルになっていて、設定可能です。	• TCP：8443（HTTPS） **（注）** TCP ポート 8443 は、デフォルトでイネーブルになっていて、設定可能です。	• TCP：8443（HTTPS） **（注）** TCP ポート 8443 は、デフォルトでイネーブルになっていて、設定可能です。	• TCP：8443（HTTPS） **（注）** TCP ポート 8443 は、デフォルトでイネーブルになっていて、設定可能です。
	クライアント プロビジョニング	• TCP：80、8443（Web または Cisco NAC エージェントのインストール） **（注）** TCP ポート 8443 は、デフォルトでイネーブルになっていて、設定可能です。ゲストの設定にも対応しています。 • TCP：8905（Cisco NAC エージェントのアップデート）	• TCP：8905（Cisco NAC エージェントのアップデート）	• TCP：8905（Cisco NAC エージェントのアップデート）	• TCP：8905（Cisco NAC エージェントのアップデート）
	ポスチャおよびハートビート	• TCP：8905 検出（HTTPS） • UDP：8905（レイヤ 2）検出（SWISS） • UDP：8905 PRA/Keep-alive（SWISS）	• TCP：8905 検出（HTTPS） • UDP：8905（レイヤ 2）検出（SWISS） • UDP：8905 PRA/Keep-alive（SWISS）	• TCP：8905 検出（HTTPS） • UDP：8905（レイヤ 2）検出（SWISS） • UDP：8905 PRA/Keep-alive（SWISS）	• TCP：8905 検出（HTTPS） • UDP：8905（レイヤ 2）検出（SWISS） • UDP：8905 PRA/Keep-alive（SWISS）

表 E-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	ISE サービス	ギガビット イーサネット 0 のポート	ギガビット イーサネット 1 のポート	ギガビット イーサネット 2 のポート	ギガビット イーサネット 3 のポート
ポリシー サービス ISE ノード（続き）	Profiler	• UDP：9996（NetFlow） （注）このポートは、設定可能です。 • UDP：67、68（DHCP） （注）このポートは、設定可能です。 • TCP：80、8080（DHCPSPAN プローブおよび HTTP） • UDP：30514（RADIUS） （注）これは、セッション サービスを介した内部サービスです。 • NMAP は、ポート 0 ～ 65535[3] を使用します（アウトバウンド）。 • UDP：53（DNS ルックアップ） （注）このポートは、ルート テーブルによって異なります。 • UDP：161（SNMP クエリー） （注）このポートは、ルート テーブルによって異なります。 • UDP：162（SNMP トラップ） （注）このポートは、設定可能です。	• UDP：9996（NetFlow） （注）このポートは、設定可能です。 • UDP：67、68（DHCP） （注）このポートは、設定可能です。 • TCP：80、8080（DHCPSPAN プローブおよび HTTP） • UDP：30514（RADIUS） （注）これは、セッション サービスを介した内部サービスです。 • NMAP は、ポート 0 ～ 65535[3] を使用します（アウトバウンド）。 • UDP：53（DNS ルックアップ） （注）このポートは、ルート テーブルによって異なります。 • UDP：161（SNMP クエリー） （注）このポートは、ルート テーブルによって異なります。 • UDP：162（SNMP トラップ） （注）このポートは、設定可能です。	• UDP：9996（NetFlow） （注）このポートは、設定可能です。 • UDP：67、68（DHCP） （注）このポートは、設定可能です。 • TCP：80、8080（DHCPSPAN プローブおよび HTTP） • UDP：30514（RADIUS） （注）これは、セッション サービスを介した内部サービスです。 • NMAP は、ポート 0 ～ 65535[3] を使用します（アウトバウンド）。 • UDP：53（DNS ルックアップ） （注）このポートは、ルート テーブルによって異なります。 • UDP：161（SNMP クエリー） （注）このポートは、ルート テーブルによって異なります。 • UDP：162（SNMP トラップ） （注）このポートは、設定可能です。	• UDP：9996（NetFlow） （注）このポートは、設定可能です。 • UDP：67、68（DHCP） （注）このポートは、設定可能です。 • TCP：80、8080（DHCPSPAN プローブおよび HTTP） • UDP：30514（RADIUS） （注）これは、セッション サービスを介した内部サービスです。 • NMAP は、ポート 0 ～ 65535[3] を使用します（アウトバウンド）。 • UDP：53（DNS ルックアップ） （注）このポートは、ルート テーブルによって異なります。 • UDP：161（SNMP クエリー） （注）このポートは、ルート テーブルによって異なります。 • UDP：162（SNMP トラップ） （注）このポートは、設定可能です。

表 E-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	ISE サービス	ギガビット イーサネット 0 のポート	ギガビット イーサネット 1 のポート	ギガビット イーサネット 2 のポート	ギガビット イーサネット 3 のポート
ポリシー サービス ISE ノード（続き）	クラスタリング	• UDP：45588、45590	• UDP：45588、45590	• UDP：45588、45590	• UDP：45588、45590
インライン ポスチャ ISE ノード	管理	• TCP：22（SSH サーバ） • TCP：8443（HTTPS） （注）　管理 ISE ノードによって使用されます。	—	—	—
	インライン ポスチャ	• UDP：1645、1812（認証用 RADIUS プロキシ） • UDP：1646、1813（アカウンティング用 RADIUS プロキシ） • UDP：1700、3799（RADIUS CoA）	• UDP：1645、1812（認証用 RADIUS プロキシ） • UDP：1646、1813（アカウンティング用 RADIUS プロキシ） • UDP：1700、3799（RADIUS CoA）	—	—
（注）　ハイ アベイラビリティおよび管理サービスは、インライン ポスチャ固有のものであり、他の Cisco ISE ノード タイプには適用されません。					
	ハイ アベイラビリティ	—	—	UDP：694（ハートビート）	UDP：694（ハートビート）
	管理	TCP：9090（リダイレクト）	TCP：9090（リダイレクト）	—	—

1. インライン ポスチャ ノードは、管理ペルソナをサポートしていないため、このポートへのアクセスはありません。
2. インライン ポスチャ ノードは、データベース リスナー機能をサポートしていないため、このポートへのアクセスはありません。
3. NMAP OS スキャンは、ポート 0 ～ 65535 を使用して、エンドポイントのオペレーティング システムを検出します。

APPENDIX F

Cisco NAC および Cisco Secure ACS アプライアンス上の Cisco ISE 3300 シリーズ ソフトウェアのインストール

この付録では、次のサポートされる Cisco Secure ACS および Cisco NAC アプライアンス プラットフォームに『*Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)*』DVD から、Cisco ISE 3300 シリーズ ソフトウェアの初期（または新規）インストールを実行するプロセスについて説明します。

- Cisco Secure ACS-1121
- Cisco NAC-3315
- Cisco NAC-3355
- Cisco NAC-3395

Cisco Secure ACS または Cisco NAC アプライアンス上の Cisco ISE 3300 シリーズ ソフトウェアのインストールでは、Cisco ISE ソフトウェアがインストールされる基礎となるハードウェアが同じ物理デバイス タイプであるため、プロセスは簡易化されています。

- Cisco Secure ACS-1121 および Cisco NAC-3315 アプライアンスは、小規模の Cisco ISE ネットワーク配置（Cisco ISE 3315 アプライアンス）に使用されるものと同じ物理ハードウェアを基にしています。
- Cisco NAC-3355 および Cisco NAC-3395 アプライアンスは、中規模および大規模な Cisco ISE ネットワーク配置（Cisco ISE 3355 と Cisco ISE 3395 アプライアンスのそれぞれ）に使用されるものと同じ物理ハードウェアを基にしています。

（注） Cisco ISE 3300 シリーズ ハードウェア プラットフォームの具体的な詳細については、表 2-1（P.-Reference 2）を参照してください。

この付録では、次の手順について説明します。

- 「イメージを再適用した Cisco Secure ACS アプライアンスでの Cisco ISE ソフトウェアのインストール」（P.F-2）：『*Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)*』DVD を使用する Cisco ISE ソフトウェアのインストール、セットアップ プログラムの使用によるアプライアンスの設定、および設定プロセスの確認の手順について説明します。

- 「イメージを再適用した Cisco NAC アプライアンスでの Cisco ISE ソフトウェアのインストール」（P.F-3）：『*Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)*』DVD を使用する Cisco ISE ソフトウェアのインストール手順について説明します。イメージの再適用プロセスを終了する前に Cisco NAC アプライアンスの RAID 設定をリセットする方法が含まれます。

（注） Cisco ISE 3300 シリーズ アプライアンスとして、Cisco Secure ACS または Cisco NAC アプライアンスのイメージ再適用を行うには、Cisco ISE ソフトウェアをインストールし、セットアップ プログラムを使用してアプライアンスを設定します。

イメージを再適用した Cisco Secure ACS アプライアンスでの Cisco ISE ソフトウェアのインストール

この項では、Cisco ISE 3300 シリーズ（リリース 1.0）アプライアンスとして、既存の Cisco Secure ACS アプライアンスのイメージ再適用を行う手順を説明します。

Cisco ISE 3300 シリーズ アプライアンスとして、Cisco Secure ACS アプライアンスのイメージ再適用を行うには、次の手順を実行します。

ステップ 1　Cisco Secure ACS アプライアンスがオンである場合は、そのアプライアンスをオフにします。

ステップ 2　Cisco Secure ACS アプライアンスの電源をオンにします。

ステップ 3　F1 を押して、BIOS セットアップ モードにします。

ステップ 4　矢印キーを使用して [日付と時刻（Date and Time）] に移動し、Enter を押します。

ステップ 5　アプライアンスの時刻を UTC/GMT 時間帯に設定します。

（注） すべての Cisco ISE ノードを UTC 時間帯に設定することを推奨します。この時間帯設定により、展開におけるさまざまなノードからのレポートおよびログが、タイムスタンプで常に同期されるようになります。

ステップ 6　Esc を押して、メイン BIOS メニューを終了します。

ステップ 7　Esc を押して、BIOS セットアップ モードを終了します。

ステップ 8　「Cisco ISE 3300 シリーズ アプライアンスを設定する前に」（P.3-1）で説明されている手順を実行します。

ステップ 9　「セットアップ プログラムのパラメータについて」（P.3-3）で説明されている手順を実行します。

ステップ 10　「設定プロセスの確認」（P.3-10）で説明されている手順を実行します。

イメージを再適用した Cisco NAC アプライアンスでの Cisco ISE ソフトウェアのインストール

この項では、Cisco ISE 3300 シリーズ（リリース 1.0）アプライアンスとして、既存の Cisco NAC アプライアンスのイメージを再適用する手順を説明します。

Cisco ISE アプライアンスとして、Cisco NAC アプライアンスのイメージ再適用を行うには、次の手順を実行します。

ステップ 1　Cisco NAC アプライアンスがオンである場合は、そのアプライアンスをオフにします。

ステップ 2　Cisco NAC アプライアンスをオンにします。

ステップ 3　F1 を押して、BIOS セットアップ モードにします。

ステップ 4　矢印キーを使用して、[日付と時刻（Date and Time）] に移動し、Enter を押します。

ステップ 5　アプライアンスの時刻を UTC/GMT 時間帯に設定します。

（注）　すべての Cisco ISE ノードを UTC 時間帯に設定することを推奨します。この時間帯設定により、展開におけるさまざまなノードからのレポートおよびログが、タイムスタンプで常に同期されるようになります。

ステップ 6　Esc を押して、メイン BIOS メニューを終了します。

ステップ 7　Esc を押して、BIOS セットアップ モードを終了します。

（注）　Cisco ISE DVD インストール プロセスが、「The installer requires at least 600GB disk space for this appliance type（このアプライアンス タイプの場合、インストーラは、少なくとも 600 GB のディスク領域を必要とします）」というメッセージを返す場合、Cisco NAC アプライアンスの既存の RAID 設定のリセットに記載されているようにインストールを進めるために、アプライアンスで RAID 設定のリセットが必要となる場合があります。

ステップ 8　「Cisco ISE 3300 シリーズ アプライアンスを設定する前に」（P.3-1）に記載されている手順を実行します。

ステップ 9　「セットアップ プログラムのパラメータについて」（P.3-3）に記載されている手順を実行します。

ステップ 10　「設定プロセスの確認」（P.3-10）に記載されている手順を実行します。

Cisco NAC アプライアンスの既存の RAID 設定のリセット

Cisco NAC アプライアンスの RAID 設定をリセットするには、次の手順を実行します。

ステップ 1　『*Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)*』DVD がインストール済みの Cisco NAC アプライアンスをリブートします。

ステップ 2　CLI に表示される RAID コントローラのバージョン情報を確認する場合は、Ctrl を押した状態で C を押します。`LSI Corporation MPT SAS BIOS` のようなラベルが表示された、RAID コントローラのバージョン情報が表示され、LSI Corp Config Utility がアクティブになります。

ステップ 3　Enter を押して、デフォルトのコントローラを指定します。（`SR-BR10i` のような強調表示されたコントローラ名が確認できます）。Cisco NAC アプライアンスのアダプタ情報を含む画面が表示されます。

ステップ 4　下矢印で [RAID プロパティ（RAID properties）] に移動して、Enter を押します。

ステップ 5　[アレイの管理（Manage Array）] で、再度 Enter を押します。

ステップ 6　下矢印で [アレイの削除（Delete Array）] オプションに移動して、Enter を押します。

ステップ 7　「Y」を入力して、既存の RAID アレイを削除することを確認します。

ステップ 8　Esc を 2 回押して、RAID 設定ユーティリティを終了します。「`Exit the Configuration Utility and Reboot?`」プロンプトで確認を求められます。

ステップ 9　Enter を押します。Cisco NAC アプライアンスがリブートされます。『*Cisco Identity Services Engine ISE VM Appliance (ISE Software Version 1.1.0.xxx)*』DVD がインストールされている限り、アプライアンスは自動でインストール メニューを起動します。

ステップ 10　1 を押して、Cisco ISE のインストールを開始します。

INDEX

数字

C

E

I

L

M

N

P

R

S

U

V

あ

い

お

か

き

く

け