Cisco Identity Services Engine
ハードウェア インストレーション ガイド リリース 1.2

2014 年 6 月

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number: OL-27044-01-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、米国シスコシステムズ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、製品に添付された情報パケット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 ハードウェア インストレーション ガイド リリース 1.2

はじめに

改訂日：2014 年 12 月 18 日

ここでは、次の項について説明します。

目的

このインストール ガイドには、Cisco ISE リリース 1.2 に関する次のような情報が記載されています。

- 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 Cisco Network Admission Control（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 1.2 には 2 つのアプライアンス プラットフォームの選択肢があります。選択は展開の規模に応じて行います。

- 小規模ネットワーク：SNS 3415
- 大規模ネットワーク：SNS 3495

既存の Cisco ISE 3300 シリーズ アプライアンスをリリース 1.2 にアップグレードすることができます。

VMware ベースのインストールの場合は、最小システム要件を満たす VMware 環境を設定して、Cisco ISE リリース 1.2 をインストールする必要があります。詳細については、第 4 章「VMware 仮想マシンでのリリース 1.2 ソフトウェアのインストール」を参照してください。

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.*x* および 5*x*
- VMware vSphere Client 4.*x* および 5*x*

対象読者

このガイドは、Cisco SNS ソフトウェアを Cisco SNS-3400 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および設定するネットワーク管理者、システム インテグレータ、またはネットワーク配置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 ガイドを使用する前提条件として、読者がネットワーキング機器やケーブル配線に精通しており、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　　Cisco ISE ハードウェア インストレーション ガイドの構成

章/付録およびタイトル	説明
第 1 章「Cisco ISE でのネットワーク配置」	Cisco SNS-3400 シリーズ アプライアンスの導入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 の導入を計画する前にこの章を参照してください。
第 2 章「Cisco SNS-3400 シリーズ アプライアンス」	Cisco SNS-3400 シリーズ ハードウェアの概要を紹介します。
第 3 章「Cisco SNS-3400 シリーズ アプライアンスのインストールおよび設定」	Cisco SNS-3400 シリーズ ハードウェアへ 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 仮想マシンでのリリース 1.2 ソフトウェアのインストール」	VMware ESX または ESXi および vSphere 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 3300 シリーズ、Cisco NAC、および Cisco Secure ACS のアプライアンスへのリリース 1.2 ソフトウェアのインストール」	Cisco ISE リリース 1.2 ソフトウェアを既存の ISE 3300 シリーズまたは従来の NAC アプライアンスおよび ACS にインストールする方法について説明します。
第 6 章「管理者アカウントの管理」	Cisco ISE の 2 種類の管理者アカウント、それらのアカウントの権限、およびこれらのアカウントを作成する方法について説明します。
第 7 章「インストール後のタスクの実行」	Cisco ISE 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。

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/付録およびタイトル	説明
付録 A「ラックへの Cisco SNS-3400 シリーズ アプライアンスの設置」	必要な安全手順、設置場所の要件、および Cisco SNS-3400 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。Cisco SNS-3400 シリーズ アプライアンスのラック取り付け、すべてのケーブルの接続、アプライアンスの電源の投入、サーバ コンポーネントの置き換えの方法についても説明します。
付録 B「Cisco SNS-3400 シリーズ サーバの仕様」	インストール後に Cisco SNS-3400 シリーズ アプライアンスを維持するための、物理、環境および電源面の仕様について説明します。
付録 C「Cisco SNS-3400 シリーズ アプライアンスのポート リファレンス」	Cisco SNS-3400 シリーズ アプライアンスのサービス、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 D「Cisco ISE ライセンス」	Cisco ISE で使用できる各種タイプのライセンス、およびそれらのインストール方法について説明します。
付録 E「Cisco ISE での証明書の管理」	ローカル（ワイルドカード証明書を含む）および CA 証明書とそれらをインストールする方法について説明します。

インストールの参考

表 2　　Cisco ISE 1.2 のインストール シナリオ

インストール プロセス	参照先
Cisco ISE アプライアンスおよび事前展開の要件について	第 2 章「Cisco SNS-3400 シリーズ アプライアンス」 付録 A「ラックへの Cisco SNS-3400 シリーズ アプライアンスの設置」
Cisco ISE ソフトウェアの設定	第 3 章「Cisco SNS-3400 シリーズ アプライアンスのインストールおよび設定」
VMware サーバへの Cisco ISE ソフトウェアの初期インストール	第 4 章「VMware 仮想マシンでのリリース 1.2 ソフトウェアのインストール」
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	第 5 章「Cisco ISE 3300 シリーズ、Cisco NAC、および Cisco Secure ACS のアプライアンスへのリリース 1.2 ソフトウェアのインストール」
インストール後に実行 Cisco ISE Web インターフェイスにログインしたら、インストール後のタスクを実行します。	第 7 章「インストール後のタスクの実行」

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。

表記法	項目
bold	手順テキストのタブおよびボタン名のほか、コマンド、キーワード、およびユーザが入力するテキストは**太字**で示しています。
italic	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
courier	システムが表示する端末セッションおよび情報は、ｸｰﾘｴ（モノスペース、固定幅）フォントで示しています。
<>	ASCII 出力など、イタリック体が許可されない例では、値を指定する必要がある引数は山かっこを使用した <angle> の形式で表示されます。

（注） 「*注釈*」です。このマニュアルで取り上げない役立つ情報や参照資料などを紹介します。

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。

警告 **安全上の重要事項**

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。警告の各国語版については、各警告文の末尾に提示されているステートメント番号を使用して、この機器に付属している各国語で記述された安全上の警告を参照してください。

これらの注意事項を保管しておいてください。

ヒント 「*問題解決に役立つ情報*」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

関連資料

リリース固有のドキュメント

（注） Cisco ISE の全般的な製品情報は http://www.cisco.com/go/ise で確認できます。エンドユーザ マニュアルは、Cisco.com の http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html から入手できます。

表 3　Cisco Identity Services Engine の製品マニュアル

マニュアル タイトル	場所
『Release Notes for the Cisco Identity Services Engine, Release 1.2 (Cisco Identity Services Engine のリリース ノート リリース 1.2)』	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
『Cisco Identity Services Engine Network Component Compatibility, Release 1.2 (Cisco Identity Services Engine ネットワーク コンポーネントの互換性リリース 1.2)』	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
『Cisco Identity Services Engine User Guide, Release 1.2 (Cisco Identity Services Engine ユーザ ガイド リリース 1.2)』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
『Cisco Identity Services Engine ハードウェア インストレーション ガイド リリース 1.2』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Upgrade Guide, Release 1.2 (Cisco Identity Services Engine アップグレード ガイド リリース 1.2)』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine, Release 1.2 Migration Tool Guide (Cisco Identity Services Engine リリース 1.2 移行ツール ガイド)』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.2 (Cisco Identity Services Engine スポンサー ポータル ユーザ ガイド リリース 1.2)』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
『Cisco Identity Services Engine CLI Reference Guide, Release 1.2 (Cisco Identity Services Engine CLI リファレンス ガイド リリース 1.2)』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html

表 3　　Cisco Identity Services Engine の製品マニュアル （続き）

マニュアル タイトル	場所
『Cisco Identity Services Engine API Reference Guide, Release 1.2 （Cisco Identity Services Engine API リファレンス ガイド リリース 1.2）』	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
『Cisco Identity Services Engine Troubleshooting Guide, Release 1.2 （Cisco Identity Services Engine トラブルシューティング ガイド リリース 1.2）』	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
『Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler』	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
『Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card （Cisco Identity Services Engine インボックス資料および中国 RoHS ポインタ カード）』	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html
『My Devices Portal FAQs, Release 1.2 （デバイス ポータル FAQ リリース 1.2）』	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

プラットフォーム固有のマニュアル

- Cisco ISE
  http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.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 ゲスト サーバ
  http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html
- Cisco NAC Profiler
  http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- Cisco Secure ACS
  http://www.cisco.com/en/US/products/ps9911/ tsd_products_support_series_home.html
- Cisco UCS C シリーズ
  http://www.cisco.com/en/US/docs/unified_computing/ucs/overview/guide/UCS_rack_roadmap.html

マニュアルの入手方法およびテクニカル サポート

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

『*What's New in Cisco Product Documentation*（*Cisco 製品資料の更新情報*）』は、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し、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をデスクトップに配信することもできます。RSS フィードは無料のサービスです。

Cisco ISE でのネットワーク配置

この章では、いくつかのネットワーク配置のシナリオを説明し、さらに Cisco Identity Services Engine（ISE）SNS 3400 シリーズ アプライアンスおよびその関連コンポーネントを導入する方法、および Cisco ISE をサポートするのに必要なスイッチおよびイヤレス LAN コントローラ設定についての指針について説明します。この章の内容は、次のとおりです。

アーキテクチャの概要

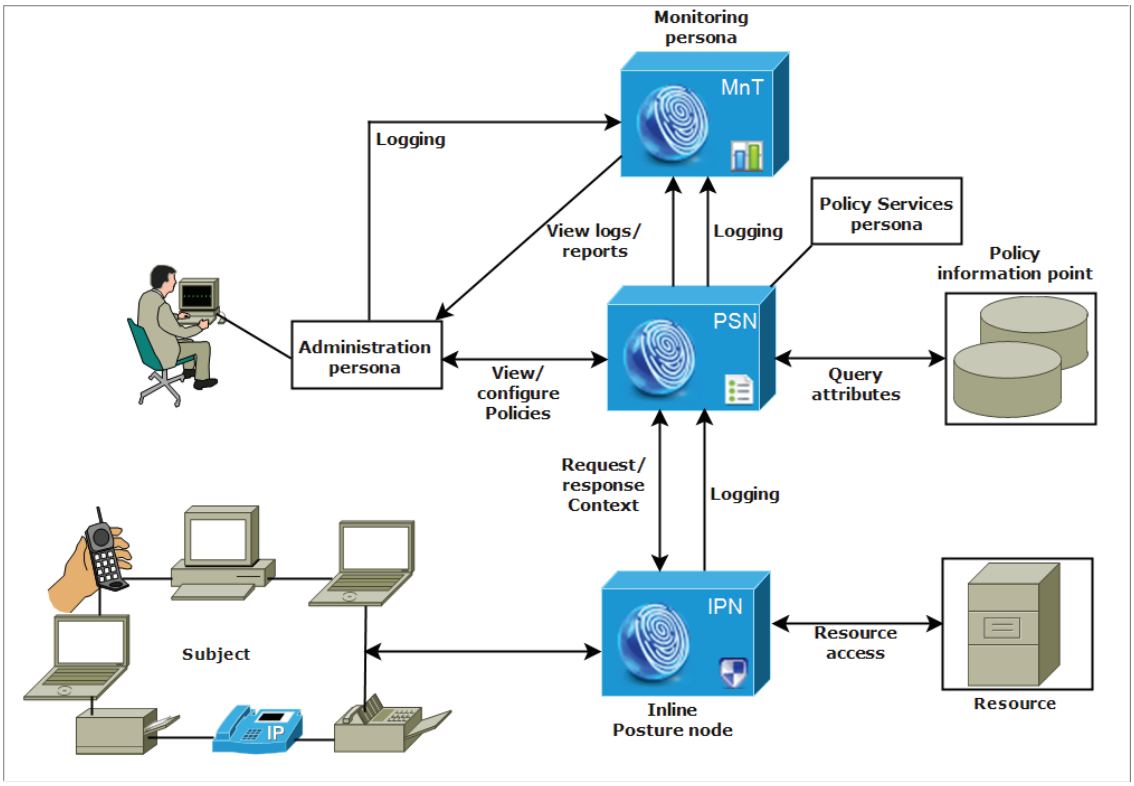
Cisco ISE アーキテクチャには、次のコンポーネントが含まれます。

- ノードおよびペルソナの種類
  - Cisco ISE ノード：Cisco ISE ノードは管理、ポリシー サービスまたはモニタリング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。
  - インライン ポスチャ ノード：アクセス ポリシーの適用を処理するゲートキーピング ノード
- ネットワーク リソース
- エンドポイント

（注） 図 1-1 に Cisco ISE ノードおよびペルソナ（管理、ポリシー サービスおよびモニタリング）、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。外部情報は、たとえば Lightweight Directory Access Protocol（LDAP）属性です。

図 1-1　　Cisco ISE のアーキテクチャ



ネットワーク配置の用語

次の用語は Cisco ISE 導入シナリオの説明に一般に使用されるものです。

- サービス：サービスは、ネットワーク アクセス、プロファイリング、セキュリティ グループ アクセス、モニタリング、およびトラブルシューティングなど、ペルソナが提供する特定の機能です。
- 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、VMware で実行できるアプライアンスおよびソフトウェアとして使用できます。
- ノード タイプ：ノードは、Cisco ISE ノードまたはインライン ポスチャ ノードのいずれかになります。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、そのノードが提供するサービスが決まります。Cisco ISE ノードは、管理、サービス ポリシー、およびモニタリングの各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。管理ユーザ インターフェイスで使用できるメニュー オプションは、ノードが担当するロールおよびペルソナによって異なります。
- ロール：ノードの役割は、ノードがスタンドアロン、プライマリ、セカンダリ ノードかどうかを決定し、管理ノードおよびモニタリング ノードのみに適用されます。

分散導入環境のノード タイプおよびペルソナ

Cisco ISE分散導入環境には、2 種類のノードがあります。

- Cisco ISE ノード：管理、ポリシー サービス、モニタリング
- インライン ポスチャ ノード

Cisco ISE ノードは担当するペルソナに基づき、各種のサービスを提供できます。導入環境内の各ノードは、インライン ポスチャ ノードを除き、管理、ポリシー サービス、およびモニタリングのペルソナのいずれかを担当することができます。分散導入環境では、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。

- ハイ アベイラビリティ用のプライマリ管理ノードとセカンダリ管理 ISE ノード
- 自動フェールオーバー用の 1 組のモニタリング ノード
- セッション フェールオーバー用の 1 つ以上のポリシー サービス ノード
- ハイ アベイラビリティを実現する 1 組のインライン ポスチャ ノード

関連項目

- 「管理ノード」（P.1-3）
- 「ポリシー サービス ノード」（P.1-3）
- 「モニタリング ノード」（P.1-4）
- 「インライン ポスチャ ノード」（P.1-4）

管理ノード

管理ペルソナの Cisco ISE ノードは、Cisco ISE のすべての管理操作を実行することができます。このノードは、認証、承認、およびアカウンティングなどの機能に関するすべてのシステム関連の設定を扱います。分散導入環境では、1 つまたは最大 2 つの管理ペルソナを実行するノードを実行できます。管理ペルソナは、スタンドアロン、プライマリ、セカンダリのロールを担当できます。

ポリシー サービス ノード

ポリシー サービス ペルソナの Cisco ISE ノードは、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、ポリシー評価の結果に基づいてエンドポイントにネットワーク アクセスを提供します。複数のノードがこのペルソナを担当できます。通常、1 つの分散導入環境に複数のポリシー サービス ノードが存在します。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 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がダウンすると、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。

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。

モニタリング ノード

モニタリング ペルソナの機能を持つ Cisco ISE ノードがログ コレクタとして動作し、ネットワーク内のすべての管理およびポリシー サービス ノードからのログを保存します。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モニタリング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したデータを集約して関連付けを行い、有意義なデータを提供します。Cisco ISE では、このペルソナを持つノードを最大 2 つ使用することができます。これらのノードは、ハイ アベイラビリティ用のプライマリ ロールまたはセカンダリ ロールを担うことができます。プライマリ モニタリング ノードおよびセカンダリ モニタリング ノードの両方が、ログ メッセージを収集します。プライマリ モニタリング ノードがダウンした場合は、セカンダリ モニタリング ノードが自動的にプライマリ モニタリング ノードになります。

分散セットアップでは、少なくとも 1 つのノードがモニタリング ペルソナを担当する必要があります。同じ Cisco ISE ノードで、モニタリング ペルソナとポリシー サービス ペルソナを有効にしないことを推奨します。最適なパフォーマンスを実現するために、モニタリング ノードはモニタリング専用とすることを推奨します。

インライン ポスチャ ノード

インライン ポスチャ ノードは、ネットワーク上のワイヤレス LAN コントローラ（WLC）および 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、ゲートキーピング ノードです。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 が処理できない許可変更（CoA）要求が処理されます。Cisco ISE では、インライン ポスチャ ノードを 2 つ使用できます。これらのノードは、ハイ アベイラビリティ用のプライマリ ロールまたはセカンダリ ロールを担うことができます。

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。このノードはインライン ポスチャ サービス専用である必要があり、他の Cisco ISE サービスと同時に実行することはできません。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。たとえば、管理ノード（管理サービスを提供）、またはポリシー サービス ノード（ネットワーク アクセス、ポスチャ、プロファイル、ゲスト サービスを提供）、またはモニタリング ノード（モニタリングおよびトラブルシューティング サービスを提供）として機能することはできません。

インライン ポスチャは Cisco SNS 3495 プラットフォームではサポートされません。インライン ポスチャは、サポートされるプラットフォームである Cisco ISE 3315、Cisco ISE 3355、Cisco ISE 3395、または Cisco SNS 3415 のいずれにインストールしてください。

インライン ポスチャ ノードのインストール

Cisco.com からインライン ポスチャ の ISO イメージをダウンロードし、それをサポートされる任意のプラットフォームにインストールし、CLI を使用して証明書を設定し、プライマリ管理ノードのユーザ インターフェイスから、このノードを登録します。

（注）　インライン ポスチャ ノードの Web ベースのユーザ インターフェイスからアクセスすることはできません。これは、プライマリ管理ノードからのみ設定できます。

導入環境にインライン ポスチャ ノードを追加する前に、このノードに対して証明書を設定し、プライマリ管理ノードに登録します。詳細については、「インライン ポスチャ ノードの証明書の設定」（P.E-37）を参照してください。

インライン ポスチャ ノードの再利用

インライン、ポスチャ ノードを利用しないことを決定した場合は、そのノードにいずれのサービスまたはロールも追加できませんが、該当のノードを Cisco ISE ノードへ変更し、任意のペルソナを割り当てることができます。インライン ポスチャ ノードを再利用する場合は、まず、そのノードを登録解除し、アプライアンスにイメージを再適用して Cisco ISE リリース 1.2 をインストールします。

スタンドアロン導入環境と分散導入環境

単一の Cisco ISE ノードがある導入環境は、スタンドアロン導入環境と呼ばれます。このノードは、管理、ポリシー サービス、およびモニタリングのペルソナを実行します。

複数の Cisco ISE ノードがある導入環境は、分散導入環境と呼ばれます。フェールオーバーをサポートし、パフォーマンスを改善するために、複数の Cisco ISE ノードを分散方式でセットアップできます。Cisco ISE の分散導入環境では、管理およびモニタリング アクティビティは一元化され、処理はポリシー サービス ノード間で分配されます。パフォーマンスのニーズに応じて、導入の規模を変更できます。Cisco ISE ノードは、管理、ポリシー サービス、およびモニタリング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。インライン ポスチャ ノードは、特殊な性質上、この他のペルソナを担当することはできず、専用ノードである必要があります。

分散導入環境のシナリオ

小規模なネットワーク配置

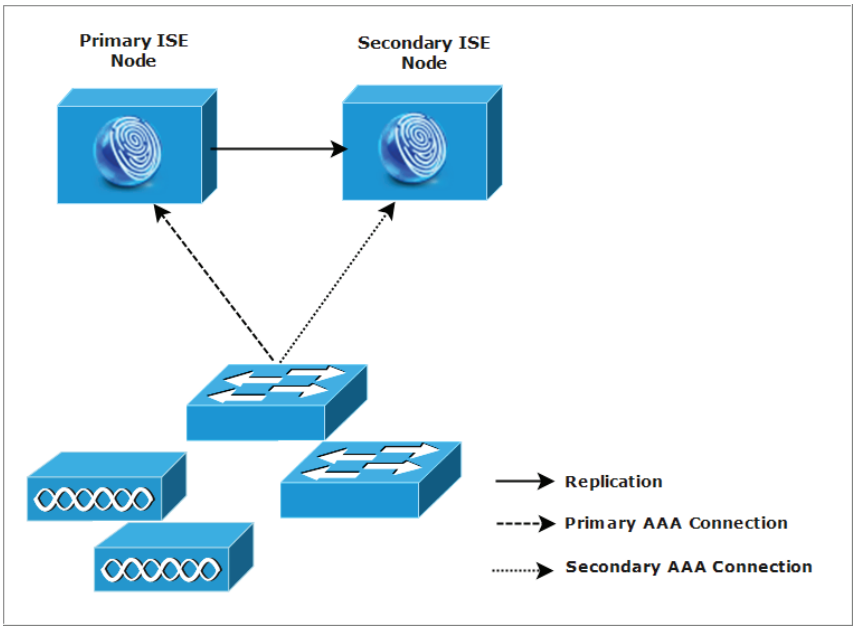
最も小規模な Cisco ISE 導入環境は、図 1-2 で示されているように 2 つの Cisco ISE ノードから構成されます（小規模なネットワークでは 1 つの Cisco ISE ノードがプライマリ アプライアンスとして動作します）。

（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。同時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 デバイスを任意に組み合わせることができます。

プライマリ ノードは、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し、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、プライマリ ノードとネットワーク アプライアンス、ネットワーク リソース、または RADIUS と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。

クライアントとプライマリ Cisco ISE ノード間の一元化された認証、承認、アカウンティング（AAA）操作は RADIUS プロトコルを使用して行われます。Cisco ISE は、プライマリ Cisco ISE ノードに存在するすべてのコンテンツをセカンダリ Cisco ISE ノードに同期（複製）します。したがって、セカンダリ ノードは、プライマリ ノードの状態と同じになります。小規模なネットワーク配置では、このような設定モデルにより、このタイプの導入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することが可能です。

図 1-2　　小規模なネットワーク配置



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、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導入の設定を変更し、分割または分散された導入モデルを使用する必要があります。

図 1-2 に、AAA 機能を実行するポリシー サービスのペルソナとして機能するセカンダリ Cisco ISE ノードを示します。セカンダリ Cisco ISE ノードは、モニタリングまたは管理ペルソナとして動作することもできます。

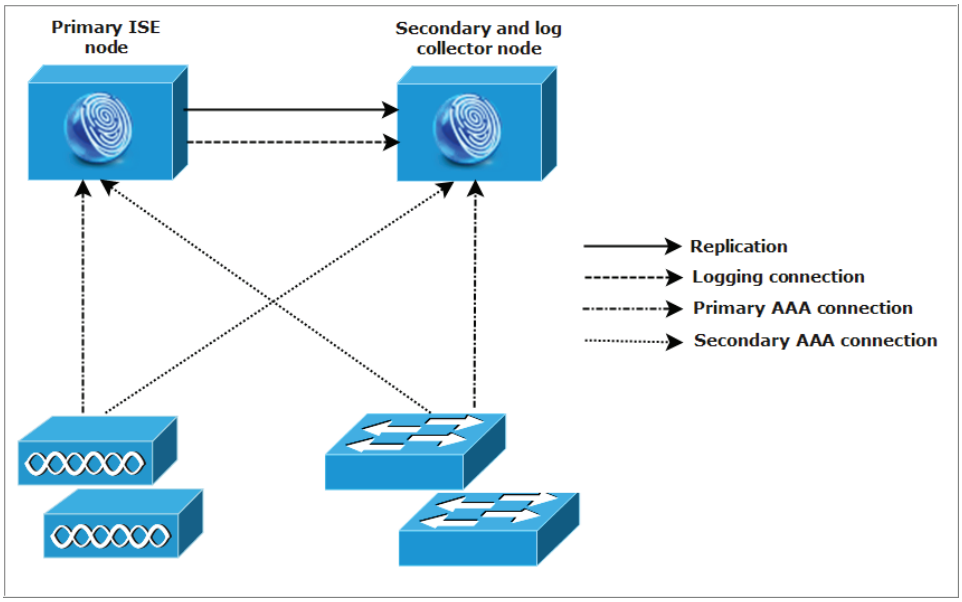
分割された導入

分割 Cisco ISE 導入環境でも、小規模な Cisco ISE 導入環境で説明したように、プライマリ ノードとセカンダリ ノードを維持することができます。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は、プライマリ ノードとセカンダリ ノードのどちらもすべての AAA 要求を処理することはできません。これは、このワークロードがこの 2 つのノード間で分散されているためです。

このように負荷を分割することにより、システムの各 Cisco ISE ノードに対する負荷はただちに減少します。また、負荷の分割により優れた負荷の制御が実現する一方で、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されます。

分割された Cisco ISE の導入環境では、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 機能を引き続き実行することができます。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　　分割されたネットワーク配置



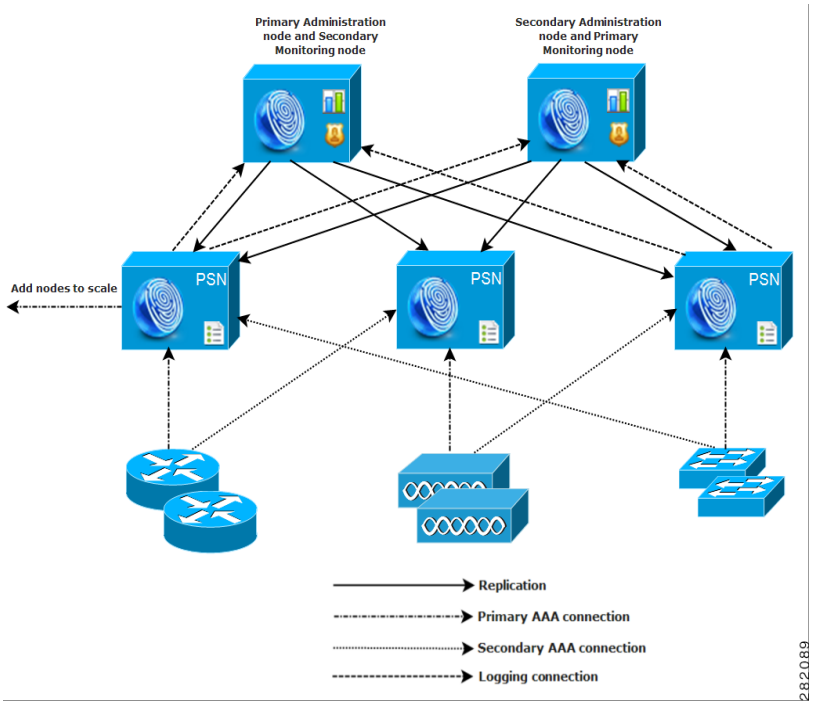
また、分割 Cisco ISE ノード展開の設計により、拡大が可能になる利点も提供されます（図 1-4 を参照）。

中規模サイズのネットワーク配置

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することで、素早くネットワークの拡大に対応できます。中規模のネットワーク配置では、新規ノードをすべての AAA 機能専用とし、元のノードを設定およびロギング機能のために使用します。

ネットワークでログ トラフィックの量が増加した場合は、セカンダリ Cisco ISE ノードの 1 つまたは 2 つを、ネットワークでのログ収集に使用することを選択できます。

図 1-4　　中規模ネットワーク配置



大規模なネットワーク配置

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な syslog トラフィックを処理するモニタリング ペルソナ（モニタリングおよびロギング用）として動作する、専用ロギング サーバを最初に設定する必要があります。

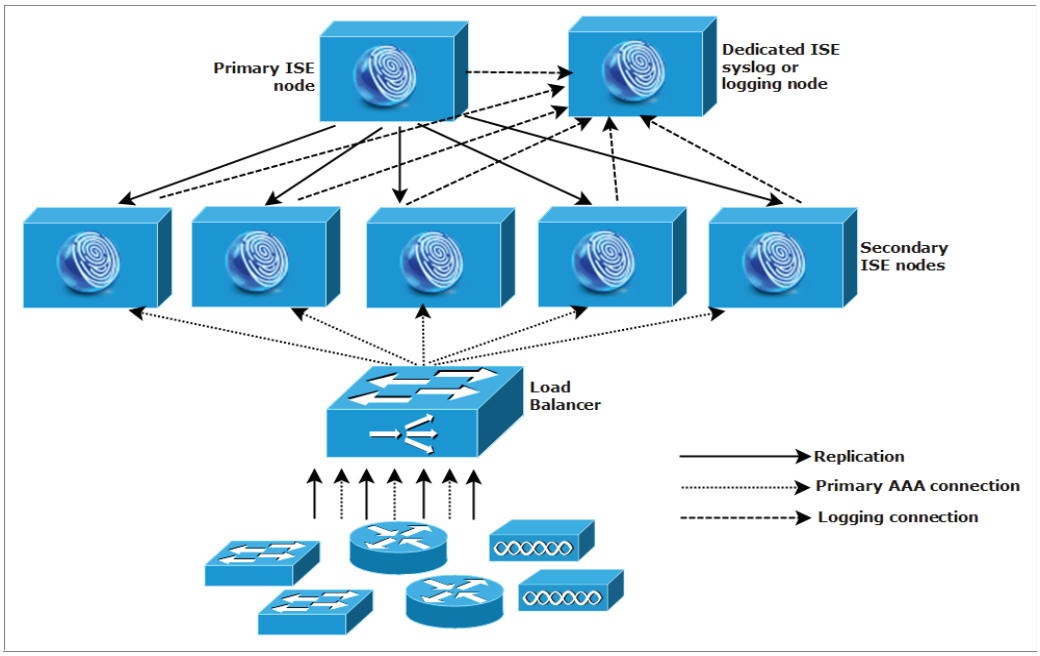
syslog メッセージは発信ログ トラフィックに対して生成されるため、どの RFC 3164 準拠の syslog アプライアンスでも、発信ロギング トラフィックのコレクタとして動作できます。専用ロギング サーバでは、すべての Cisco ISE ノードをサポートするために Cisco ISE で使用できるレポート機能およびアラート機能を使用できます。Cisco ISE ソフトウェアが専用ロギング サーバをサポートするように設定する場合は、「Cisco ISE セットアップ プログラム パラメータ」（P.3-8）を参照してください。

また、アプライアンスが Cisco ISE ノードのモニタリング 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 ノード上のモニタリング ペルソナがダウンした場合の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 クライアントの導入が簡素化されます。ロード バランサを使用に必要な AAA サーバのエントリは 1 つだけです。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 バランサを導入し、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　　大規模なネットワーク配置

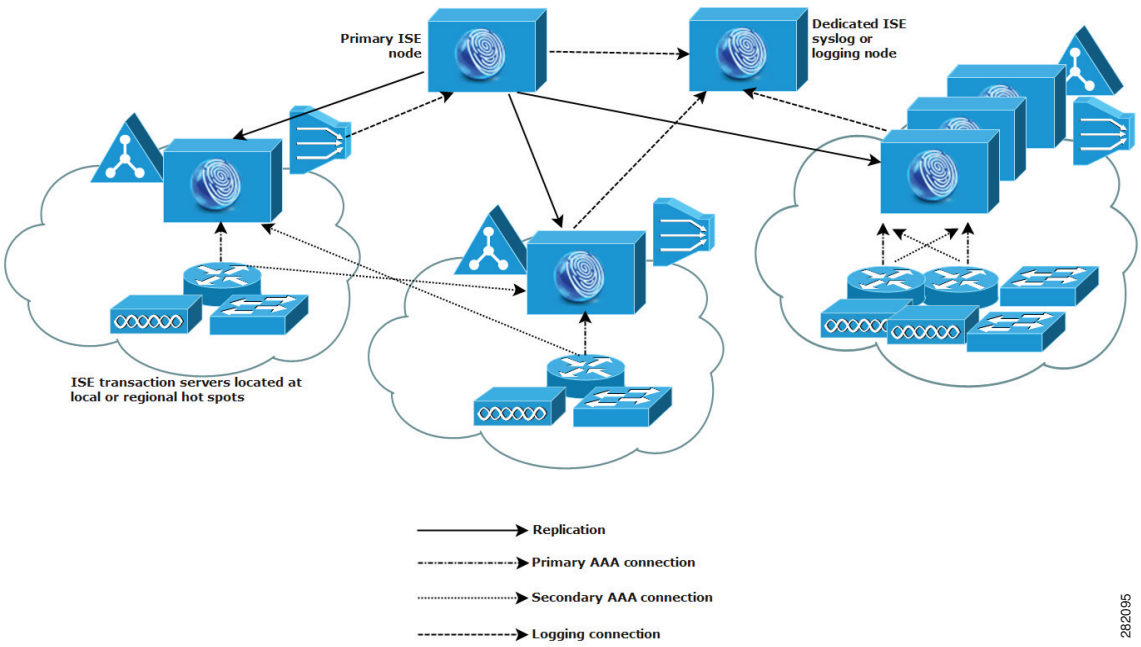


分散されたネットワーク配置

分散 Cisco ISE ネットワーク配置は、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適です。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～大規模な場所であり、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。

大規模なリモート サイトは、AAA パフォーマンスを最適化するために、独自の AAA インフラストラクチャ（図 1-6 に記載）を持つことができます。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 ノードで個別のモニタリング 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、固有のネットワーク要件を満たす必要があります。

図 1-6　　分散された配置



複数のリモート サイトがあるネットワークを計画する前に

- Microsoft Active Directory や Lightweight Directory Access Protocol（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。AAA のパフォーマン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 クライアントの場所は重要です。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、Cisco ISE ノードを AAA クライアントのできるだけ近くに配置する必要があります。
- 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 接続を行うことができます。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確実にアクセスできるようにするために、すべての Cisco ISE ノードでドメイン ネーム システム（DNS）を適切に設定する必要があります。

配置の規模およびスケーリングについての推奨事項

この項では、ネットワークに接続するエンドポイントの数に基づき必要な、物理および仮想マシン アプライアンスのサイズについてのガイダンスを提供します。表 1-1は、ネットワークに接続するエンドポイントの数に基づき必要な、配置の種類、Cisco ISE ノードの数、アプライアンスの種類（小型、中型、および大型）についてのガイダンスを提供します。

表 1-1　Cisco ISE の導入：サイズおよびスケーリングについての推奨事項

展開タイプ	ノード数/ペルソナ	アプライアンス プラットフォーム	専用ポリシー サービス ノードの最大数	アクティブ エンドポイントの数
小	管理、ポリシー サービス、およびモニタリング ペルソナが有効になったスタンドアロンまたは冗長（2 つの）ノード。	Cisco ISE 3300 シリーズ（3315、3355、3395）	0	最大 2,000 エンドポイント
		Cisco ISE 3415	0	最大 5,000 エンドポイント
		Cisco ISE 3495	0	最大 10,000 エンドポイント
中	単一または冗長ノードの管理およびモニタリング ペルソナ。最大 2 つの管理およびモニタリング ノード。	管理およびモニタリング ペルソナ用の Cisco ISE-3355 または Cisco SNS 3415 アプライアンス	5	最大 5,000 エンドポイント
		管理およびモニタリング ペルソナ用の Cisco ISE 3395 または Cisco SNS 3495 アプライアンス	5	最大 10,000 エンドポイント
大	専用の管理ノード（1 つ/複数）。最大 2 つの管理ノード。 専用のモニタリング ノード（1 つ/複数）。最大 2 台のモニタリング ノード。	管理およびモニタリング ペルソナ用の Cisco ISE 3395 アプライアンス	40	最大 100,000 エンドポイント
		管理およびモニタリング ペルソナ用の Cisco SNS 3495 アプライアンス	40	最大 250,000 エンドポイント

表 1-2 に、アクティブなエンドポイントの数およびノード サービスに基づき専用のポリシー サービス ノードに必要なアプライアンスの種類についてのガイダンスを提供します。

表 1-2　ポリシー サービス ノードのサイズについての推奨

フォーム ファクタ	プラットフォームのサイズ	アプライアンス	最大エンドポイント
物理	小	Cisco ISE-3315	3,000
		Cisco SNS-3415	5,000
	中	Cisco ISE-3355	6,000
	大	Cisco ISE-3395	10,000
		Cisco SNS-3495	20,000
仮想マシン	小規模/中規模/大規模	物理アプライアンスに相当	3,000 ～ 20,000

表 1-3 に、単一のインライン ポスチャ ノードがサポートすることができる最大スループットおよびエンドポイントの最大数を記載します。

表 1-3　インライン ポスチャのノードのサイズに関する推奨事項

属性	パフォーマンス
物理アプライアンスごとのエンドポイントの最大数	5,000 ～ 20,000 （ポリシーのサービス ノードによってゲート制御）
任意の物理アプライアンスごとの最大スループット	936 Mbps

インライン ポスチャ計画の考慮事項

ネットワークまたはシステムのアーキテクトは、インライン ポスチャの導入に関する問題を調査する責任を負い、ネットワークの要件に何が最適かを判断します。

ネットワークまたはシステムのアーキテクトは、インライン ポスチャのノードの導入を計画する場合、次の基本的な質問事項に対応する必要があります。

- 導入計画にインライン 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。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。
- どの種類のインライン ポスチャの動作モードを選択しますか。

注意　インライン ポスチャ ノードの信頼されないインターフェイスは、インライン ポスチャのノードの設定時に切断する必要があります。初期設定時に信頼されるインターフェイスと信頼されないインターフェイスが同じ VLAN に接続され、ペルソナの変更後にインライン ポスチャ ノードがブートされると、マルチキャスト パケット トラフィックが信頼できないインターフェイスでいっぱいになります。このマルチキャスト イベントにより、同じサブネットまたは VLAN に接続されたデバイスがダウンする可能性があります。この時点で、インライン ポスチャ ノードはメンテナンス モードになります。

注意　インライン ポスチャ ノードが導入環境に追加されている場合、このノードの CLI パスワードを変更しないでください。パスワードが変更されると、管理ノードを通じてインライン ポスチャ ノードにアクセスした場合に Java 例外エラーが表示され、CLI がロックされます。インストール DVD を使用し、インライン ポスチャ ノードをリブートして、パスワードを回復する必要があります。または、元のパスワードを設定することもできます。

パスワードを変更する必要がある場合は、導入環境から該当のインライン ポスチャ ノードを登録解除し、パスワードを変更して、このノードを新しいクレデンシャルとともに導入環境に追加します。

関連項目

Cisco Identity Services Engine User Guide, Release 1.2（Cisco Identity Services Engine ユーザ ガイド リリース 1.2）

Cisco ISE のサポートに必要なスイッチおよびワイヤレス LAN コントローラの設定

Cisco ISE がネットワーク スイッチと相互運用することができ、Cisco ISE の機能がネットワーク セグメント全体で正常に使用できるよう保証するためには、ご使用のネットワーク スイッチを、必要とされる特定のネットワーク タイム プロトコル（NTP）、RADIUS/AAA、IEEE 802.1X、MAC 認証バイパス（MAB）などの設定を使用して設定する必要があります。

関連項目

スイッチおよびワイヤレス LAN コントローラ設定の要件の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.2（Cisco Identity Services Engine ユーザ ガイド リリース 1.2）*』の付録 C、「Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions（Cisco ISE のサポートに必要なスイッチおよびワイヤレス LAN コントローラの設定）」を参照してください。

Cisco SNS-3400 シリーズ アプライアンス

この章では、Cisco Secure Server（SNS）3415 および 3495 のアプライアンスおよびハードウェアの仕様について説明します。

Cisco SNS-3400 シリーズ アプライアンス ハードウェアの仕様

Cisco SNS-3400 シリーズ アプライアンス ハードウェアは、Cisco SNS 3415 および 3495 のアプライアンスから構成されます。

表 2-1 の「図」列には、電源供給ソケット、LED、および対応するパネルの重要なコントロールおよびボタンを示す図へのハイパーリンクが記載されています。

表 2-1　Cisco ISE SNS 3415/3495 アプライアンス ハードウェアの概要

Cisco ISE アプライアンス	ハードウェア仕様	図
Cisco SNS- 3415-K9	• Cisco UCS C220 M3 • シングル ソケット Intel E5-2609 2.4GHz CPU 合計 4 コア、合計 4 スレッド • 16 GB メモリ • 600 GB ディスク x 1 • 組み込みソフトウェア RAID 0 • 4 GE ネットワーク インターフェイス • 物理的仕様、環境仕様、および電源仕様については、「Cisco SNS-3400 シリーズ サーバの仕様」を参照してください。	• 「Cisco SNS 3415/3495 の前面パネル」 • 「SNS 3415/3495 の背面パネル」

表 2-1　Cisco ISE SNS 3415/3495 アプライアンス ハードウェアの概要 （続き）

Cisco ISE アプライアンス	ハードウェア仕様	図
Cisco SNS- 3495-K9	• Cisco UCS C220 M3 • デュアル ソケット Intel E5-2609 2.4GHz CPU 合計 8 コア、合計 8 スレッド • 32 GB RAM • 600 GB ディスク x 2 • RAID 0+1 • 4 GE ネットワーク インターフェイス • 物理的仕様、環境仕様、および電源仕様については、「Cisco SNS-3400 シリーズ サーバの仕様」を参照してください。	• 「Cisco SNS 3415/3495 の前面パネル」 • 「SNS 3415/3495 の背面パネル」

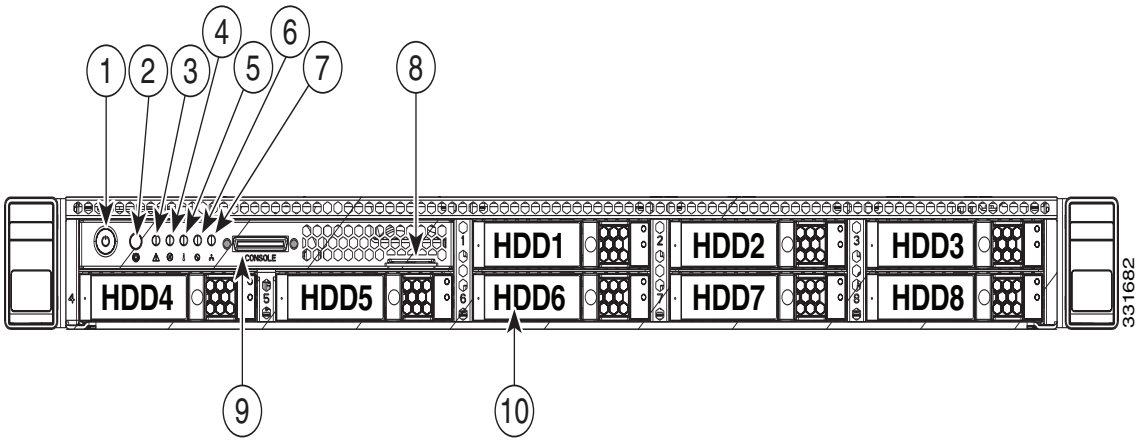
（注）　Cisco ISE 1.2 は、Cisco SNS-3415-K9 のオプションの冗長電源装置をサポートします。追加の電源装置を注文するための製品番号は UCSC-PSU-650W= です。

Cisco SNS-3400 シリーズの前面および背面パネル

前面パネル

図 2-1 に SNS 3415/3495 の前面パネルを示します。

図 2-1　Cisco SNS 3415/3495 の前面パネル

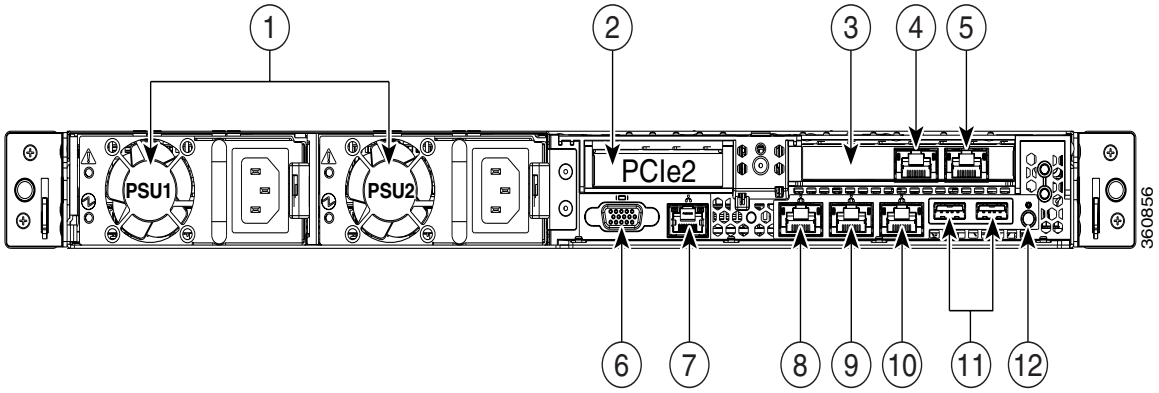


1	電源ボタン/電源ステータス LED	6	電源装置ステータス LED
2	識別ボタン LED	7	ネットワーク リンク アクティビティ LED
3	システム ステータス LED	8	資産タグ（シリアル番号）
4	ファン ステータス LED	9	キーボード、ビデオ、マウス（KVM）コネクタ（2 つの USB（1 つはビデオ グラフィック アダプタ（VGA）、もう 1 つはシリアル コネクタ）を備えた KVM ケーブルと使用）
5	温度ステータス LED	10	ドライブ（最大 8 台のホットスワップ可能な 2 ～ 5 インチのドライブ）

背面パネル

図 2-2 に SNS 3415/3495 の背面パネルを示します。

図 2-2　SNS 3415/3495 の背面パネル



1	電源（最大 2 台）	7	シリアル ポート（RJ-45 コネクタ）
2	スロット 2：ライザーのロープロファイル PCIe（Peripheral Component Interconnect Express）スロット（ハーフハイト、ハーフレングス、x16 コネクタ、x16 レーン幅）	8	CIMC へのアクセスに使用する 1 GB イーサネット専用管理ポート（M というラベル付き）
3	スロット 1：1 GB イーサネット ポートを含む PCIe1 カード（GigE2 および GigE3）	9	Cisco ISE 管理通信用の 1 GB イーサネット ポート 1（GigE0）
4	1 GB イーサネット ポート 3（GigE2）	10	1 GB イーサネット ポート 2（GigE1）
5	1 GB イーサネット ポート 4（GigE3）	11	USB ポート
6	VGA ビデオ コネクタ	12	背面の識別ボタン

シリアル番号の場所

サーバのシリアル番号はサーバ上部、前面近くのラベルに印刷されています。

Cisco ISE に対する Cisco SNS のサポート

Cisco ISE ソフトウェアは、専用の Cisco SNS-3400 シリーズ アプライアンスまたは VMware サーバのいずれかで稼動します。Cisco ISE リリース 1.2 ソフトウェアは、この専用プラットフォームでの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 1.2（Cisco Identity Service Engine のリリース ノート リリース 1.2）*』を参照してください。

リリース 1.2 は、Cisco ISE 3300 シリーズ、Cisco NAC 3300 シリーズ、および Cisco Secure ACS 1121 アプライアンスでもサポートされています。既存の Cisco ISE 3300 シリーズ アプライアンスをリリース 1.2 にアップグレードすることができます。Cisco ISE 3300 シリーズ アプライアンスの詳細については、次を参照してください。第 5 章「Cisco ISE 3300 シリーズ、Cisco NAC、および Cisco Secure ACS のアプライアンスへのリリース 1.2 ソフトウェアのインストール」

Cisco SNS-3400 シリーズ アプライアンスのインストールおよび設定

この章では、Cisco Identity Services Engine（ISE）3400 シリーズ アプライアンスのインストールおよび設定方法について説明します。また、この章には以下のトピックが含まれています。

（注） Cisco SNS-3400 シリーズ アプライアンスで Cisco ISE ソフトウェアを設定する前に、この章に記載されている設定の前提条件を確認してください。詳細については、「Cisco SNS-3400 シリーズ アプライアンスの設定の前提条件」（P.3-7）を参照してください。

ラックへの SNS-3400 シリーズ アプライアンスの設置

安全に関する注意事項、設置場所の要件、および Cisco SNS-3400 シリーズ アプライアンスを設置する前に確認する必要があるガイドラインについては、付録 A「ラックへの Cisco SNS-3400 シリーズ アプライアンスの設置」を参照してください。

Cisco ISE リリース 1.2 の ISO イメージのダウンロード

Cisco ISE リリース 1.2 の ISO イメージは Cisco.com からダウンロードすることができます。

（注）　インライン ポスチャ ノードの場合は、インライン ポスチャ ノード リリース 1.2 の ISO をダウンロードし、インストール プロセスを続行してください。詳細については、「インライン ポスチャ ノードのインストール」（P.1-4）を参照してください。

ステップ 1　http://www.cisco.com/go/ise にアクセスします。このリンクにアクセスするには、有効な Cisco.com ログイン クレデンシャルが必要です。

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

Cisco ISE リリース 1.2 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、インストール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。

SNS-3400 シリーズ アプライアンスへのリリース 1.2 ソフトウェアのインストール

SNS-3400 シリーズ アプライアンスが Cisco ISE リリース 1.1.x を実行している場合は、アプリケーションの更新コマンドを使用して、リリース 1.2 にアップグレードすることを選択できます。『*Cisco Identity Services Engine Upgrade Guide, Release 1.2*（*Cisco Identity Services Engine アップグレード ガイド リリース 1.2*）』を参照してください。また、既存の SNS-3400 シリーズ アプライアンスのイメージを再適用し、リリース 1.2 の新規インストールを実行して、このリリースを既存環境に登録することもできます。

ISO イメージをダウンロードしたら、次の方法のいずれかで、イメージを SNS-3400 シリーズ アプライアンスにインストールできます。

- CIMC リモート管理ユーティリティを使用して ISO イメージをインストールします。このリモート インストールを行うには、CIMC を設定する必要があります。
  1. CIMC を設定します。
  2. Cisco ISE リリース 1.2 をリモートでインストールします。
- USB フラッシュ ドライブを使用して ISO イメージをインストールします。
  1. iso-to-usb.sh スクリプトを使用して、ブート可能な USB フラッシュ ドライブを作成します。
  2. SNS-3400 シリーズ アプライアンスに USB フラッシュ デバイスを接続します。
  3. ローカルの KVM を使用するか、またはリモートで CIMC KVM を使用して、Cisco ISE リリース 1.2 をインストールします。
- USB ポートと外付けの DVD ドライブを使用して ISO をインストールします。
  1. DVD に ISO イメージを書き込みます。
  2. SNS-3400 シリーズ アプライアンスに外付けの USB DVD を接続します。
  3. ローカルの KVM を使用するか、またはリモートで CIMC KVM を使用して、Cisco ISE リリース 1.2 をインストールします。

（注）　USB フラッシュ デバイスを使用するか、USB ポートで外付けの DVD を使用してリリース 1.2 をインストールする場合、CIMC の設定は任意です。リモート インストールを行わない場合は、これらのオプションのいずれかを選択します。

関連項目

- 「CIMC の設定」（P.3-3）
- 「ブート可能な USB ドライブの作成」（P.3-6）
- 「Cisco ISE セットアップ プログラム パラメータ」（P.3-8）
- 「CIMC を使用した Cisco SNS-3400 シリーズ アプライアンスでの リリース 1.2 の設定」（P.3-9）

Cisco Integrated Management Controller

組み込みの Cisco Integrated Management Controller（CIMC）GUI または CLI インターフェイスを使用して、サーバおよびシステムのイベント ログをモニタできます。次の URL で、使用しているリリースのユーザ マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html

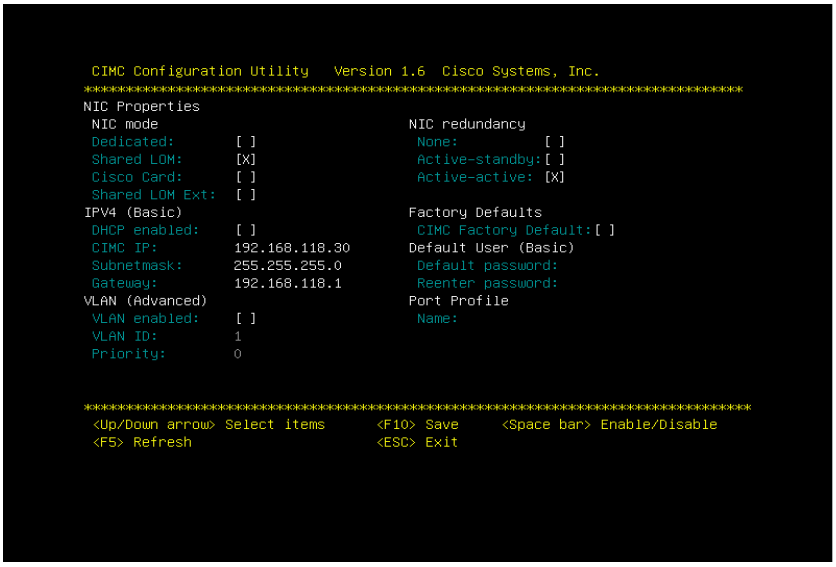
CIMC の設定

CIMC を使用して、Cisco SNS-3400 シリーズのアプライアンスに対するすべての操作を実行できます。これを行うには、最初に Web ベースのブラウザから CIMC にアクセスするための IP アドレスと IP ゲートウェイを設定する必要があります。

ステップ 1　電源コードを差し込みます。

ステップ 2　**電源**ボタンを押して、サーバをブートします。F8 を押して、以下の図のプロンプトが表示されるのを確認します。

ステップ 3　ブートアップ時に、**F8** を押して BIOS CIMC 構成ユーティリティを開きます。次の画面が表示されます。



ステップ 4　NIC モードを設定して、どのポートがサーバ管理用の CIMC にアクセスするかを指定します（ポートの識別については、図 2-2（P.2-3）を参照してください）。Cisco ISE では最高で 4 個のギガビット イーサネット ポートを使用できます。[**Dedicated NIC**（専用 NIC）] モードを選択し、[NIC redundancy（NIC 冗長化）] を [**None**（なし）] に設定して（ステップ 5 を参照）、IP 設定を選択します。

- Dedicated：CIMC へのアクセスに 1 Gb イーサネット管理ポートを使用します。[NIC redundancy（NIC 冗長化）] の [*None*（なし）] を選択し、各種 IP 設定を選択する必要があります。
- Shared LOM（デフォルト）：CIMC へのアクセスに 2 つの 1 Gb イーサネット ポートを使用します。これは工場出荷時設定で、[NIC redundancy（NIC 冗長化）] は active-active、DHCP が有効に設定されています。

– Cisco Card : CIMC へのアクセスに設置されている Cisco UCS P81E VIC のポートを使用します。NIC 冗長化と IP 設定を選択する必要があります。

（注） Cisco Card NIC モードは現在、PCIe スロット 1 に取り付けられている Cisco UCS P81E VIC（N2XX-ACPCI01）だけでサポートされています。「Cisco UCS 仮想インターフェイス カードの特記事項」を参照してください

ステップ 5　以下の [NIC redundancy（NIC 冗長化）] 設定を指定します。

– [None（なし）] : イーサネット ポートは個別に動作し、問題が発生した場合にフェールオーバーを行いません。

– [Active-standby（アクティブ-スタンバイ）] : アクティブなイーサネット ポートに障害が発生した場合、スタンバイ ポートにトラフィックがフェールオーバーします。

– [Active-active（アクティブ-アクティブ）] : すべてのイーサネット ポートが同時に使用されます。

ステップ 6　ダイナミック ネットワーク設定に対して DHCP を有効にするか、スタティック ネットワーク設定を入力するかを選択します。

（注） DHCP を有効にするには、DHCP サーバにこのサーバの MAC アドレス範囲をあらかじめ設定しておく必要があります。MAC アドレスはサーバ背面のラベルに印字されています。このサーバでは、CIMC に 6 つの MAC アドレスが割り当てられています。ラベルに印字されている MAC アドレスは、6 つの連続 MAC アドレスのうち最初のものです。

ステップ 7　（オプション）VLAN の設定を指定し、デフォルトの CIMC ユーザ パスワードを設定します。

（注） 設定の変更は約 45 秒後に有効になります。次の手順のサーバの再起動は、**F5** を押して更新し、新しい設定が表示されてから行います。

ステップ 8　**F10** を押して設定を保存し、サーバを再起動します。

（注） DHCP のイネーブル化を選択した場合、動的に割り当てられた IP アドレスと MAC アドレスがブートアップ時にコンソール画面に表示されます。

次の作業

「CIMC を使用した Cisco SNS-3400 シリーズ アプライアンスでの リリース 1.2 の設定」（P.3-9）

ブート可能な USB ドライブの作成

Cisco ISE リリース 1.2 の ISO イメージには、Readme ファイルおよび Cisco ISE リリース 1.2 をインストールするためのブート可能な USB ドライブを作成するためのスクリプトがある images ディレクトリが含まれています。

はじめる前に

- images ディレクトリにある Readme ファイルを必ず読みます。
- 次の内容が必要になります。
  - RHEL-5.x、RHEL-6.x、CentOS-5.x、または CentOS-6.x の Linux マシン。

    PC または MAC を使用する場合は、RHEL-5.x、RHEL-6.x、CentOS-5.x、または CentOS-6.x を実行する Linux 仮想マシン（VM）がインストールされていることを確認します。
  - 8 GB の USB ドライブ
  - iso-to-usb.sh スクリプト

ステップ 1　USB ポートに USB ドライブを接続します。

ステップ 2　USB デバイスを取り外さずに、Linux CLI または GUI から USB ドライブをアンマウントします。CLI から、コマンド **umount** */dev/sdb* を入力します。ここで、*/dev/sdb* は USB デバイスです。

（注）　GUI から [Safely Remove Drive（安全なドライブの取り外し）] オプションまたは [Eject（取り出し）] オプションを選択しないでください。

ステップ 3　Linux マシンのディレクトリに iso-to-usb.sh スクリプトと Cisco ISE 1.2 の ISO イメージをコピーします。

ステップ 4　**chmod** コマンドを使用してスクリプトの権限を変更します。

たとえば、**# chmod u+x iso-to-usb.sh** のようになります。

ステップ 5　root ユーザとして、次のコマンドを入力します。

iso-to-usb.sh *source_iso usb_device*

たとえば、**# ./iso-to-usb.sh** *ise-1.2.0.434-x86_64.iso /dev/sdb* のようになります。ここで、**iso-to-usb.sh** はスクリプト名、*ise-1.2.0.434-x86_64.iso* は ISO イメージの名前、*/dev/sdb* はご使用の USB デバイスです。

root ユーザ アカウントに切替えるための **su** コマンドを使用しなければならない場合があります。また、**sudo** コマンドを使用することにより、root 権限を使用してスクリプトを実行することもできます。

ステップ 6　イメージをインストールするアプライアンスの値を入力します。

ステップ 7　**Y** と入力して続行します。

ステップ 8　処理が正常に完了したことを知らせるメッセージが表示されます。

ステップ 9　USB ドライブを取り外します。

次の作業

「CIMC を使用した Cisco SNS-3400 シリーズ アプライアンスでの リリース 1.2 の設定」（P.3-9）

Cisco SNS-3400 シリーズ アプライアンスの設定の前提条件

Cisco SNS-3400 シリーズ アプライアンスには、Cisco Application Deployment Engine リリース 2.0.5 オペレーティング システム（ADE-OS）および Cisco ISE リリース 1.2 ソフトウェアがあらかじめインストールされています。

手順を進める前に、導入環境内の各ノードの以下のすべての構成設定が分かっ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
- ドメイン ネーム システム（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 タイム ゾーン
- 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）

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 管理および Web ベース管理のユーザー権限の違い」（P.6-1）を参照してください。

SNS-3400 シリーズ アプライアンスに Cisco ISE をインストールしている場合は、Cisco ISE リリース 1.2 の ISO イメージをダウンロードし、次のオプションのいずれかを使用して、アプライアンスで Cisco ISE リリース 1.2 ソフトウェアを設定します。

- Cisco Integrated Management Interface（CIMC）を設定し、これを使用して Cisco ISE リリース 1.2 をインストールします。「CIMC の設定」（P.3-3）を参照してください。
- ブート可能な USB ドライブを作成し、この USB ドライブを使用して、Cisco ISE 1.2 をインストールします。「ブート可能な USB ドライブの作成」（P.3-6）を参照してください。

（注）　意図的にシスコの SNS-3400 シリーズ アプライアンスの RAID 設定が削除されている場合は、CIMC またはブート可能な USB ドライブを使用して Cisco ISE リリース 1.2 を再インストールする必要があります。ブート可能な USB ドライブを使用して Cisco ISE を再インストールすると同時に、webBIOS を使用して手動で RAID を設定する必要があります。CIMC を使用した Cisco ISE のインストールの詳細については、「CIMC を使用した Cisco SNS-3400 シリーズ アプライアンスでの リリース 1.2 の設定」（P.3-9）を参照してください。ブート可能な USB ドライブを使用した Cisco ISE のインストールの詳細については、「ブート可能な USB ドライブの作成」（P.3-6）を参照してください。

Cisco ISE-3300 シリーズ、Cisco Secure ACS、または Cisco NAC アプライアンスに Cisco ISE をインストールする場合は、Cisco ISE リリース 1.2 の ISO イメージをダウンロードし、DVD に ISO イメージを書き込み、このイメージを使用して Cisco ISE リリース 1.2 をインストールします。サポートされている Cisco Secure ACS と Cisco NAC のプラットフォームについては、付録 5「Cisco ISE 3300 シリーズ、Cisco NAC、および Cisco Secure ACS のアプライアンスへのリリース 1.2 ソフトウェアのインストール」を参照してください。

Cisco ISE セットアップ プログラム パラメータ

Cisco ISE ソフトウェアの設定が開始されると、インタラクティブな CLI により、システムの設定に必要なパラメータを入力するよう要求されます。（表 3-1 を参照）。

セットアップの実行後や導入環境で Cisco ISE がリブートされた場合は毎回、DNS および NTP サーバが到達可能であることを確認します。

（注）　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、Cisco ISE は初期設定中に VMware ツール バージョン 8.3.2 もインストールおよび設定します。インストールを確認するには、「VMware ツールのインストールの確認」（P.7-6）を参照してください。

表 3-1　Cisco ISE セットアップ プログラム パラメータ

プロンプト	説明	例
ホスト名	15 文字以下にする必要があります。有効な文字には、英数字（A–Z、a–z、0–9）、およびハイフン（-）などがあります。最初の文字は文字である必要があります。 （注）　Cisco ISE の証明書認証が、証明書による検証のわずかな違いの影響を受けないようにするために小文字を使用することを推奨します。ノードのホスト名として「localhost」を使用することはできません。	isebeta1
（eth0）イーサネット インターフェイス アドレス	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	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	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	IP アドレスは入力できません。有効な文字には、ASCII 文字、任意の数字、ハイフン（-）、およびピリオド（.）が含まれます。	example.com
プライマリ ネーム サーバ	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	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	ネットワーク タイム プロトコル（NTP）サーバの有効な IPv4 アドレスまたはホスト名である必要があります。	clock.nist.gov
別の NTP サーバの追加/編集	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。

表 3-1　Cisco ISE セットアップ プログラム パラメータ （続き）

プロンプト	説明	例
システム タイム ゾーン	有効なタイム ゾーン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 1.1.x (Cisco Identity Services Engine CLI リファレンス ガイド リリース 1.1.x)*』に記載されている Cisco ISE がサポートするタイム ゾーンのリストを参照してください。たとえば、太平洋標準時（PST）では、システム タイム ゾーンは PST8PDT です（つまり、協定世界時（UTC）から 8 時間を差し引いた時間）。 『CLI Reference Guide（CLI リファレンス ガイド）』に記載されたタイム ゾーンは、最も頻繁に使用されるタイム ゾーンです。サポートされているタイム ゾーンの完全なリストについては、Cisco ISE CLI から **show timezones** コマンドを実行できます。 **（注）** すべての Cisco ISE ノードを UTC タイム ゾーンに設定することを推奨します。このタイム ゾーンの設定により、展開におけるさまざまなノードからのレポート、ログ、およびポスチャ エージェントのログ ファイルが、タイムスタンプで常に同期されるようになります。	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 から 8 文字の長さであり、有効な英数字（A–Z、a–z、または 0–9）で構成される必要があります。	admin（デフォルト）
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。このパスワードにはデフォルトがないため、作成する必要があります。パスワードの長さは 6 文字以上で、少なくとも 1 つの小文字（a–z）、1 つの大文字（A-Z）、および 1 つの数字（0–9）を含める必要があります。	MyIseYPass2

（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.7-4）を参照してください。

CIMC を使用した Cisco SNS-3400 シリーズ アプライアンスでの リリース 1.2 の設定

アプライアンスの CIMC を設定したら、CIMC を使用して、Cisco SNS-3400 シリーズ アプライアンスを管理できます。CIMC を使用して、BIOS の設定を含むすべての操作を実行できます。

（注） VMware サーバを設定するには、「VMware システムを Cisco ISE ソフトウェア DVD から起動するための設定」（P.4-18）を参照してください。

はじめる前に

- アプライアンスで CIMC を設定したことを確認します。詳細については、「CIMC の設定」（P.3-3）を参照してください。
- 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確認します。「サーバの接続と電源投入」（P.A-8）および「LED の確認」（P.A-9）を参照してください。
- CIMC にアクセスするクライアント マシンに Cisco ISE Release 1.2 の ISO イメージがあること、または、インストールのイメージがあるブート可能な USB があることを確認します。「ブート可能な USB ドライブの作成」（P.3-6）を参照してください。
- Cisco ISE アプライアンスは、UTC タイム ゾーンを使用して内部的に時間を追跡します。特定のタイム ゾーンが不明の場合は、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。タイム ゾーンの例については、表 3-2、表 3-3、および表 3-4 を参照してください。インストール中にセットアップ プログラムで該当の設定を行うように要求されたときに、優先されるタイム ゾーン（デフォルトは UTC）を設定することを推奨します。

ステップ 1　サーバ管理用の CIMC に接続します。ネットワーク インターフェイス カードの（NIC）モードの設定で選択されたポートを使用して LAN からサーバにイーサネット ケーブルを接続します。active-active および active-passive の [NIC redundancy（NIC 冗長化）] 設定では、2 つのポートに接続する必要があります。

ステップ 2　ブラウザと CIMC の IP アドレスを使用して CIMC セットアップ ユーティリティにログインします。この IP アドレスは、自分が作成した CIMC 設定に基づいています（スタティック アドレスまたはダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバによって割り当てられたアドレス）。

（注）　サーバのデフォルトのユーザ名は *admin* です。デフォルト パスワードは *password* です。

ステップ 3　[**Launch KVM Console（KVMコンソールの起動）**] をクリックします。

ステップ 4　ログインに CIMC クレデンシャルを使用します。

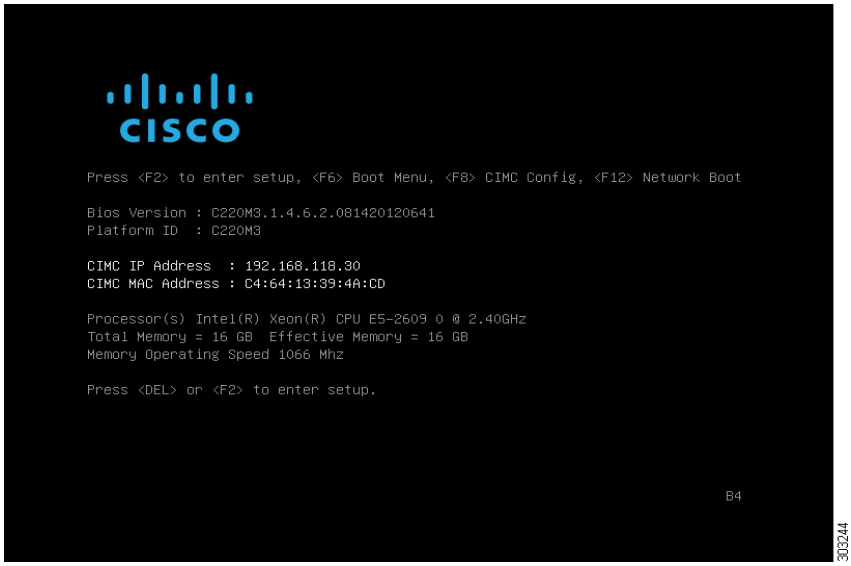
ステップ 5　[**Virtual Media（仮想メディア）**] タブをクリックします。

ステップ 6　クライアント ブラウザを実行しているシステムから Cisco ISE リリース 1.2 の ISO イメージを選択するには、[**Add Image（イメージの追加）**] をクリックします。

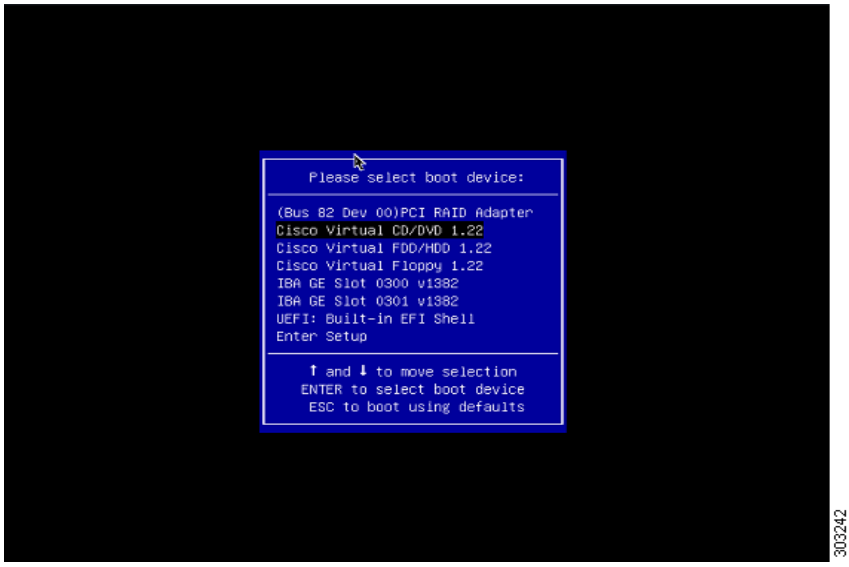
ステップ 7　作成した仮想 CD/DVD ドライブに対して [**Mapped（マップ済み）**] チェックボックスをオンにします。

ステップ 8　[**KVM**] タブをクリックします。

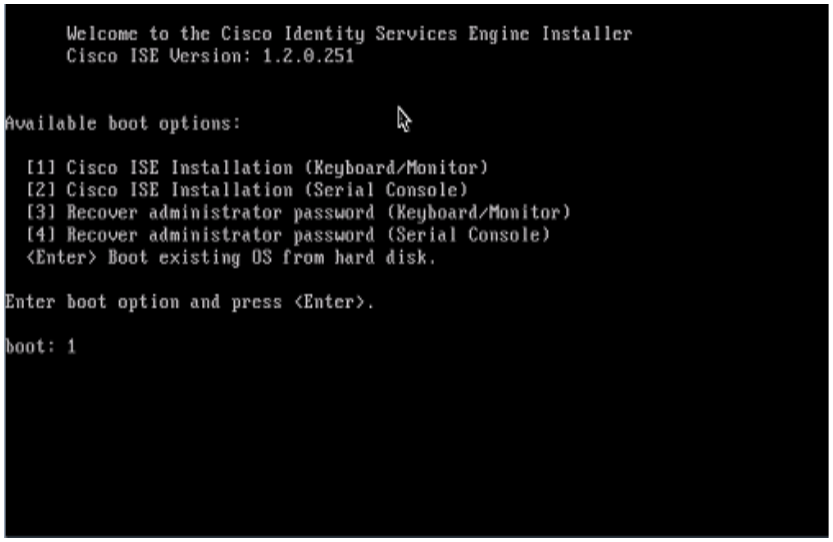
ステップ 9　[**Macros（マクロ）**] > **Ctrl-Alt-Del** を選択して、SNS-3400 シリーズ アプライアンスを ISO イメージを使用して起動します。次の図に示すような画面が表示されます。



ステップ 10　**F6** を押して、[Boot（ブート）] メニューを起動します。次のような画面が表示されます。



ステップ 11　マッピングした CD/DVD を選択して、**Enter** を押します。次のような画面が表示されます。



ステップ 12　ログイン プロンプトで、**1** を入力して、**Enter** キーを押します。

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

ステップ 13　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、サンプルのセットアップ プログラムとデフォルト プロンプトを示します。

```
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
Enable SSH?: Y/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 is non-interactive, and will take roughly 15
minutes to complete.

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

...
```

（注）　インライン ポスチャ ノード リリース 1.2 の ISO イメージをインストールすると「Installing ISE-IPEP」メッセージが表示され、さらに「Application bundle (ISE-IPEP) installed successfully」メッセージが表示されます。

（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にのみ表示されます。

Cisco ISE またはインライン ポスチャ ノード ソフトウェアが設定されると、Cisco ISE システムが自動的にリブートします。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 14　インライン ポスチャ ノード の ISO イメージをインストールしている場合は、「インライン ポスチャ ノードの証明書の設定」（P.E-37）に進みます。

ステップ 15　Cisco ISE リリース 1.2 の ISO イメージをインストールしている場合は、Cisco ISE CLI シェルにログインし、次の CLI コマンドを実行して Cisco ISE アプリケーション プロセスの状態を確認します。

```
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 16　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ら、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.7-1）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 **https://<your-ise-hostname or IP address>/admin/** と入力します。

ここで、「your-ise-hostname or IP address」はセットアップ時に Cisco SNS-3400 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 17　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 ベースの管理ログイン資格情報（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。Cisco ISE Web インターフェイスへの最初のアクセスは、セットアップ プロセスで定義した CLI 管理ユーザのユーザ名、およびパスワードを使用して行うことができます。

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 による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の設定時に作成した 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 管理および Web ベース管理のユーザー権限の違い」（P.6-1）を参照してください。

注意　インストール後に Cisco ISE アプライアンスでタイム ゾーンを変更すると、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。タイム ゾーンの変更による影響の詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.1.2 （Cisco Identity Services Engine CLI リファレンス ガイド 1.1.2）*』の付録 A の「clock time zone（クロック タイム ゾーン）」を参照してください。

サポートされるタイム ゾーン

この項では、欧州と米国とカナダ、オーストラリア、およびアジアの共通の協定世界時（UTC）タイム ゾーンの詳細を 3 つの表で示しています。

（注）　すべての Cisco ISE ノードを UTC タイム ゾーンに設定することを推奨します。このタイム ゾーンの設定により、展開におけるさまざまなノードからのレポート、ログ、およびポスチャ エージェントのログ ファイルが、タイムスタンプで常に同期されるようになります。

タイム ゾーンの形式は、POSIX または System V です。POSIX タイム ゾーン形式の構文は America/Los_Angeles のようになり、System V タイム ゾーンのシンタックスは PST8PDT のようになります。

- 欧州、米国、およびカナダのタイム ゾーンについては、表 3-2 を参照してください。
- オーストラリアのタイム ゾーンについては、表 3-3 を参照してください。
- アジアのタイム ゾーンについては、表 3-4 を参照してください。

表 3-2　欧州、米国、およびカナダのタイム ゾーン

頭字語または名前	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

表 3-2　欧州、米国、およびカナダのタイム ゾーン （続き）

頭字語または名前	時間帯名
WET	西ヨーロッパ時間（UTC）
CET	中央ヨーロッパ時間、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	中部標準時、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
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

表 3-4　アジアの時間帯 （続き）

アジア[1]			
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 の **show timezones** コマンドは、使用可能なすべてのタイム ゾーンのリストを表示します。ネットワークの場所に最適なタイム ゾーンを選択します。

セットアップ プロセスの確認

最初のセットアップ 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で Cisco ISE ISE アプライアンスにログインします。

- Web ブラウザ
- Cisco ISE CLI

Cisco ISE ユーザ インターフェイスにログインした後、次のタスクを実行する必要があります。

- 「ライセンスのインストール」（P.7-4）
- 「Cisco ISE システムの設定」（P.7-10）

VMware 仮想マシンでのリリース 1.2 ソフトウェアのインストール

この章では、Cisco Identity Services Engine（ISE）リリース 1.2 のソフトウェアを VMware 仮想マシン（VM）にインストールするため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 SNS-3415 および 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。Cisco SNS-3495 シリーズまたは VMware サーバ システムではサポートされていません。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。

サポートされる VMWare のバージョン

Cisco ISE は次の VMware サーバとクライアントをサポートしています。

- 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.*x* および 5*x*
- VMware vSphere Client 4.*x* および 5*x*

（注） Cisco ISE リリース 1.2 は、VMware vMotion 機能（あるサーバから別のサーバへの仮想マシンのライブ マイグレーション）をサポートします。

リリース 1.2 における VMware vMotion に対する サポート

Cisco ISE リリース 1.2 では、ライブ仮想マシン（VM）インスタンス（任意のペルソナを実行）のホスト間での移行を可能にする、VMware vMotion 機能がサポートされます。該当の VMware vMotion 機能が機能するには、次の条件を満たす必要があります。

- 共有ストレージ：VM のストレージがストレージ エリア ネットワーク（SAN）に存在している必要があり、この SAN は、移動された VM をホストする可能性があるすべての VMware ホストからアクセスできる必要があります。
- VMFS ボリュームの共有：この VMware ホストは、共有 Virtual Machine File System（VMFS）ボリュームを使用する必要があります。
- ギガビット イーサネットの相互接続：SAN および VMware ホストは、ギガビット イーサネット リンクを使用して相互接続する必要があります。
- プロセッサの互換性：互換性のある一連のプロセッサを使用する必要があります。プロセッサは、vMotion の互換性のために、同じベンダーとプロセッサ ファミリのものである必要があります。

仮想マシンの要件

表 4-1 に、VMware 仮想マシンに Cisco ISE リリース 1.2 ソフトウェアをインストールし、100 のエンドポイントをサポートするための最小システム要件を示します。

Cisco ISE ハードウェア アプライアンスと同等のパフォーマンスと拡張性を実現するには、VMware 仮想マシンに Cisco SNS 3415 および 3495 アプライアンスと同等のシステム リソースが割り当てられている必要があります。詳細については、「配置の規模およびスケーリングについての推奨事項」（P.1-11）および「VMWare アプライアンスの推奨サイズ」（P.4-3）を参照してください。

表 4-1　　最小 VMware システム要件

要件のタイプ	最小要件
CPU	単一のクアッドコア、2.0 GHz 以上の速度
メモリ	4 ～ 32 GB の RAM
ハードディスク	200 GB ～ 2 TB のディスク ストレージ（サイズは展開とタスクによって異なります）。詳細については、表 4-3を参照してください。 VM ホスト サーバでは、最小速度が 10,000 RPM のハード ディスクを使用することを推奨します。Cisco ISE VM では、最低 50 MB/秒の書き込み帯域幅が必要です。ホスティング環境が 10,000 RPM のディスクを使用していれば、この帯域幅は簡単に実現可能です。 **（注）** Cisco ISE に対して仮想マシンを作成する場合は、ストレージ要件を満たす単一の仮想ディスクを使用します。ディスク領域要件を満たしている複数のディスクを使用する場合、インストーラがすべてのディスク領域を認識しない可能性があります。

表 4-1　最小 VMware システム要件 （続き）

要件のタイプ	最小要件
ストレージ	• ファイル システム：VMFS ストレージに VMFS を使用することを推奨します。他のストレージ プロトコルはテストされておらず、何らかのファイルシステム エラーの原因となる可能性があります。 • 内部ストレージ：SCSI/SAS • 外部ストレージ：iSCSI/SAN NFS ストレージの使用は推奨されません。
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（複数の NIC が推奨されます） **（注）** ユーザが設定した任意の NIC のネットワーク接続を作成する場合は、[Adapter（アダプタ）] ドロップダウン リストから [E1000] を選択することを推奨します。Cisco ISE リリース 1.2 は、すべての NIC 用の E1000 および VMXNET3 アダプタをサポートします。その他の仮想 NIC ドライバはサポートされません。「VMware サーバの設定」（P.4-10）の ステップ 10 を参照してください。
ハイパーバイザ	「サポートされる VMWare のバージョン」（P.4-1）を参照してください。

VMWare アプライアンスの推奨サイズ

VMWare アプライアンスの仕様は、物理アプライアンスと同等にする必要があります。表 4-2 に、実稼働環境の物理アプライアンスに対して推奨される VMware 仕様を示します。

表 4-2　実稼働環境向けの VMware アプライアンスの仕様

プラットフォーム	SNS-3415	SNS-3495
プロセッサ[1]	単一ソケットの Intel E5-2609 2.4 Ghz CPU 合計 4 のコア	デュアル ソケットの Intel E5-2609 2.4 Ghz CPU 合計 8 のコア
メモリ	16 GB	32 GB
合計ディスク[2] 領域	600 GB	600 GB
イーサネット NIC[3]	内蔵ギガビット NIC X 4	内蔵ギガビット NIC X 4

1. 仮想マシンのリソースは専用にする必要があります。VM リソースは複数の仮想マシン間で共有またはオーバーサブスクライブすることはできません。
2. 仮想マシンのポリシー サービス ノードは管理またはモニタリング ノードよりも少ないディスク領域で導入できます。ポリシー サービス ノードのディスク領域として 150 から 200 GB を用意することを推奨します。さまざまなペルソナに必要なディスク領域の詳細については、「推奨される VMware ディスク領域」を参照してください。
3. 仮想マシンは 1 ～ 4 つの NIC を使用して設定できます。2 つ以上の NIC を使用できるようにすることを推奨します。追加のインターフェイスは、プロファイリングや RADIUS などのさまざまなサービスをサポートするために使用できます。各ポートでサポートされるサービスに関する詳細については、付録 C「Cisco SNS-3400 シリーズ アプライアンスのポート リファレンス」を参照してください。

Cisco ISE リリース 1.2 は、従来のアプライアンスの仕様に基づいて仮想マシンにインストールできますが、パフォーマンスを改善するために、SNS-3400 シリーズのアプライアンスの仕様に基づいて新しい仮想マシンを導入することを推奨します。

ディスク スペースに関する要件

表 4-3 に、実動環境で VMware サーバを実行するために推奨される、Cisco ISE ディスク領域の割り当てを示します。Cisco ISE ソフトウェアの実行には、表 4-1 に記載された、サポートされている VMware ESX および ESXi のサーバ バージョン使用してください。

表 4-3　　推奨される VMware ディスク領域

ISE ペルソナ	最小ディスク領域	最大ディスク領域	本番環境用に推奨されるディスク領域
スタンドアロン ISE	200 GB	2 TB	600 GB ～2 TB[1]
分散 ISE：管理専用[2]	200 GB	2 TB	250 ～ 300 GB
分散 ISE：モニタリング専用	200 GB	2 TB	600 GB ～ 2 TB[1]
分散 ISE：ポリシー サービス専用[2]	100 GB	2 TB	150 ～ 200 GB
分散 ISE：管理とモニタリング用	200 GB	2 TB	600 GB ～ 2 TB[1]
分散 ISE：管理、モニタリング、およびポリシー サービス	200 GB	2 TB	600 GB ～2 TB

1. ディスク割り当ては、ロギングの保持要件によって異なります。詳細については、表 4-4を参照してください。
2. 追加のディスク領域は、ローカル ロギングのサポートや、ローカル ディスク上のバックアップおよびアップグレード ファイルの保存に割り当てられる可能性があります。

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。

（注）　Cisco ISE リリース 1.2 仮想マシン（VM）に割り当てることができるディスク領域は最高で 2 TB のみです。

モニタリング ペルソナが有効になっている任意のノードでは、VM ディスク領域の 30 パーセントがログ ストレージ用に割り当てられます。25,000 のエンドポイントがある展開では、1 日あたり約 1 GB のログが生成されます。

たとえば、600 GB の VM ディスク領域があるモニタリング ノードがある場合、180 GB がログ ストレージ用に割り当てられます。100,000 のエンドポイントが毎日このネットワークに接続する場合、1 日あたり約 4 GB のログが生成されます。この場合、リポジトリに古いデータを転送し、モニタリング データベースからそのデータをパージすれば、モニタリング ノードのログを 38 日を保存することができます。

追加のログ ストレージ用に、VM ディスク領域を増やすことができます。追加するディスク スペースの100 GB ごとに、ログ ストレージ用に 30 GB が追加されます。要件に応じて、最大 2 TB または 614 GB のログ ストレージ分 VM ディスク サイズを増やすことができます。

仮想マシンのディスク サイズを増やす場合、Cisco ISE 1.2 にアップグレードする必要はありませんが、仮想マシン上で Cisco ISE 1.2 の新規インストールを実行してください。

表 4-4 に、モニタリング ノードに割り当てられたディスク領域とネットワークに接続するエンドポイントの数に基づいて、モニタリング ノードで保持できる日数を示します。

表 4-4　モニタリング ノードにログが保存される日数[1]

エンドポイントの 数	200 GB	400 GB	600 GB	1024 GB	2048 GB
10,000	126	252	378	645	1,289
20,000	63	126	189	323	645
30,000	42	84	126	215	430
40,000	32	63	95	162	323
50,000	26	51	76	129	258
100,000	13	26	38	65	129
150,000	9	17	26	43	86
200,000	7	13	19	33	65
250,000	6	11	16	26	52

1. 数値はログの抑制と異常クライアント検出が有効になっていることに基づいています。

リリース 1.2 の評価

評価のために、Cisco ISE リリース 1.2 を、表 4-1 に記載された要件に準拠した、サポートされる任意の VMware 仮想マシン（VM）にインストールすることができます。リリース 1.2 を評価する場合は、VM のディスク領域を少なく設定できますが、最低 100 GB のディスク領域を割り当てることは必要です。

（注）　200 GB 未満のディスク領域を使用して作成された VM から実稼働 VM にデータを移行することはできません。200 GB 以上のディスク領域を使用して作成された VM のデータのみを実稼働環境に移行できます。

Cisco ISE リリース 1.2 評価版ソフトウェア（R-ISE-EVAL-K9=）を入手するには、シスコのアカウント チームまたは認定されたシスコ チャネル パートナーにお問い合わせください。

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 VM に必要なディスク領域があることを確認する。詳細については、「配置の規模およびスケーリングについての推奨事項」（P.1-11）を参照してください。
- 実稼働の導入ライセンスをインストールする。
- 実稼働システムに設定を復元する。

（注）　評価の場合、100 人のユーザをサポートする VMware サーバに対するハードディスクの最小の割り当て要件は 100 GB です。より多くのユーザをサポートする実稼働環境に VMware サーバを移動する場合は、Cisco ISE インストールを必ず表 4-3 に記載された推奨される最小ディスク サイズ以上（最大許容サイズは 2 TB）に再設定してください。

VMware ESX または ESXi サーバの設定

この項では、VMware 仮想マシンで VMware ESX または ESXi サーバを設定する方法について説明します。

次の手順を実行するには、管理者権限を持つユーザ（root ユーザ）として ESXi サーバにログインする必要があります。次の手順の値や図は一例です。実際の値は導入の要件によって異なります。

はじめる前に

VMware ESX または ESXi サーバを設定する前に、次をお読みください。

- Cisco ISE リリース 1.2 は、64 ビット システムです。64 ビット システムをインストールする前に、仮想化テクノロジー（VT）が ESX/ESXi サーバで有効になっていることを確認してください。また、仮想マシンのゲスト オペレーティング システムが 64 ビットに設定されていることも確認してください。詳細については、「ESX または ESXi サーバの仮想化テクノロジーの有効化」（P.4-7）を参照してください。64 ビットのゲスト オペレーティング システムをサポートするハードウェアおよびファームウェアの要件については、次の VMware ナレッジ ベースを参照してください。

  http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1011712

- ゲスト オペレーティング システムのタイプが Red Hat Enterprise Linux 5（64 ビット）に設定されていることも確認する必要があります。ゲスト オペレーティング システムの設定方法については、http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005870 を参照してください。

- Red Hat Enterprise Linux 5 の場合、デフォルトの NIC タイプは、E1000 です。E1000 アダプタを選択することを推奨します。Cisco ISE は VMXNET3 アダプタもサポートします。Cisco ISE 仮想マシン用に最大 4 つの NIC を追加できますが、すべての NIC に対して必ず同じアダプタを選択するようにしてください。Cisco ISE リリース 1.2 は VMXNET2 アダプタをサポートしません。

- VMware 仮想マシンディスク領域の推奨量を割り当てていることを確認してください。詳細については、表 4-3（P.4-4）を参照してください。

- VMware Virtual Machine File System（VMFS）を作成していない場合は、Cisco ISE 仮想アプライアンスをサポートするために作成する必要があります。VMFS は、VMware ホスト上に設定されたストレージ ボリュームごとに設定されます。
  - VMFS5 を使用する場合、1 MB のブロック サイズは最大で 2 TB の仮想ディスク サイズをサポートします。
  - VMFS3 を使用する場合は、VMware ホストでホストされる仮想ディスクの最大サイズに基づいて VMFS のブロック サイズを選択する必要があります。VMFS のブロック サイズを設定した後にこのサイズを変更するには、VMFS パーティションを再フォーマットする必要があります。VMFS-3 の場合、VMFS のブロック サイズは次の最大仮想ディスク サイズに基づいている必要があります。

表 4-5　VMFS のブロック サイズ

ブロック サイズ	仮想ディスク サイズ
1 MB	256 GB
2 MB	512 GB
4 MB	1 TB
8 MB	2 TB

- 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 ソフトウェアのこのリリースでは、サポートされるいずれの VMware サーバでも、ストレージ タイプとして VMware シン プロビジョニングを使用することはサポートされません。シン プロビジョニングは、デフォルト設定ではなく、ステップ 13 で選択することは推奨されません（図 4-13 を参照）。
- プロファイラ サービスを有効にしている場合は、「Cisco ISE プロファイラ サービスに対する VMware サーバ インターフェイスの設定」（P.4-9）で説明されているタスクを読み、実行したことを確認します。

ESX または ESXi サーバの仮想化テクノロジーの有効化

Cisco ISE リリース 1.2 は 64 ビット システムで、バージョン 4.0、4.0.1、4.1 および ESXi バージョンの VMware ESX 4.*x* および 5.*x* をサポートします。これらの ESX および ESXi のバージョンは 64 ビットのハードウェアにのみインストールできます。したがって、ユーザは Cisco ISE リリース 1.1.x 仮想マシンをホストするのに使用していたのと同じハードウェアをリリース 1.2 で再利用できます。ただし、リリース 1.2 をインストールする前に、ESX または ESXi サーバで仮想化テクノロジー（VT）を有効にする必要があります。

すでに ESX または ESXi サーバをインストールしている場合は、マシンを再起動せずに、VT が有効かどうかを確認できます。これを行うには、**esxcfg-info** コマンドを使用します。次に例を示します。

```
~ # esxcfg-info |grep "HV Support"
    |----HV Support.......................................3
        |----World Command Line.............................grep HV Support
```

HV サポートの値が 3 の場合、VT は ESX または ESXi サーバで有効であるため、インストールに進むことができます。HV サポートの値が 2 の場合、VT はサポートされていますが、ESX または ESXi サーバで有効になっていません。BIOS 設定を編集し、ESX または ESXi サーバで VT を有効にする必要があります。**esxcfg-info** コマンドの詳細については、次の VMware ナレッジ ベースを参照してください。

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1011712

この項では、BIOS 設定を編集し、SNS-3400 シリーズ アプライアンスで VT を有効にする方法について説明します。この項の手順および図は、単なる例です。ご使用のハードウェアの BIOS メニューはこの例とは異なる場合があります。ESX または ESXi サーバで VT を有効にする前に、次の VMware ナレッジ ベースを参照してください。

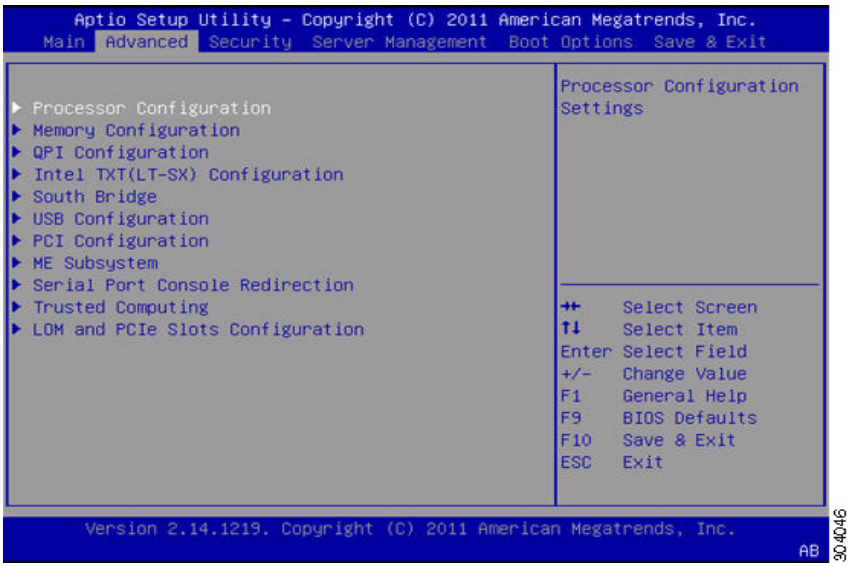
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003944

ステップ 1　SNS-3400 シリーズ アプライアンスをリブートします。

ステップ 2　**F2** を押して、セットアップを開始します。

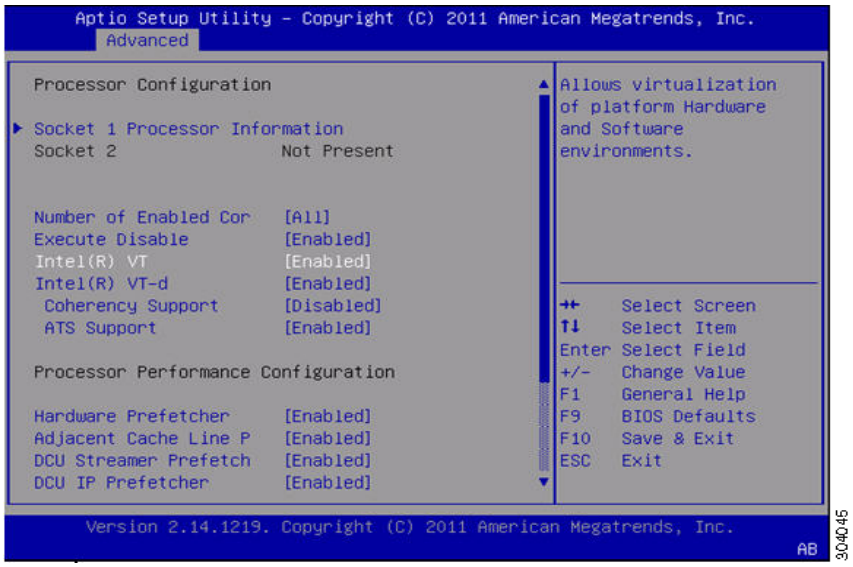
ステップ 3　[**Advanced**（拡張）] > [**Processor Configuration**（プロセッサの設定）] を選択します。

図 4-1　SNS-3400 シリーズ アプライアンスの BIOS 設定の編集



ステップ 4　[**Intel(R) VT**] を選択して、有効にします。

図 4-2　SNS-3400 シリーズ アプライアンスでの VT の有効化



ステップ 5　変更を保存し、終了するには、**F10** を押します。

Cisco ISE プロファイラ サービスに対する VMware サーバ インターフェイスの設定

VMware サーバ インターフェイスを、スイッチ ポート アナライザ（SPAN）またはミラー化されたトラフィックの Cisco ISE プロファイラ サービスの専用プローブ インターフェイスへの収集をサポートするように設定するには、次の手順に従います。

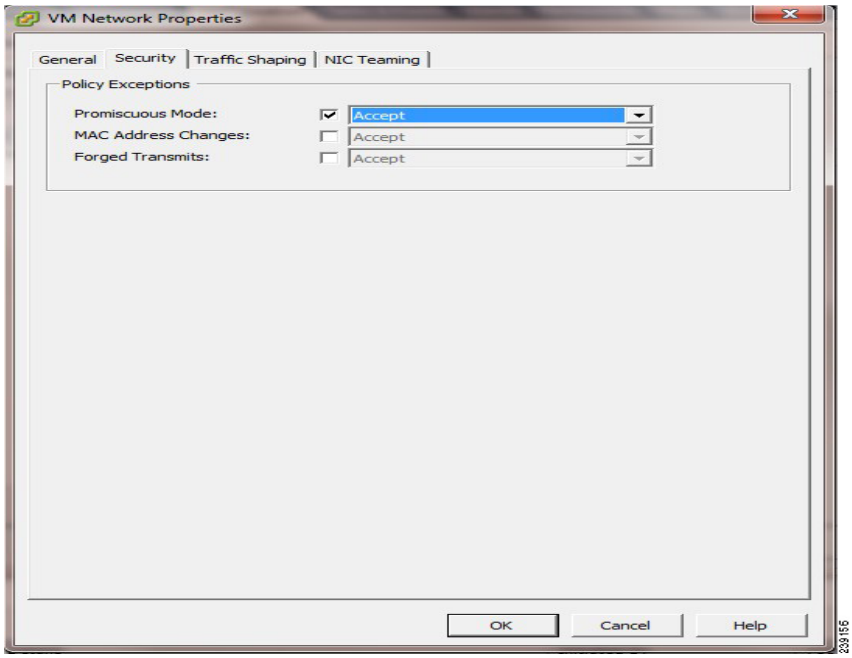
ステップ 1　以下のように選択します。**[Configuration（設定）]** > **[Networking（ネットワーク）]** > **[Properties（プロパティ）]** > *[VMNetwork （ご使用の VMware サーバ インスタンスの名前）]* > *[VMswitch0 （ご使用の VMware ESXi サーバ インターフェイスの 1 つ）]* > **[Properties（プロパティ）]** > **[Security（セキュリティ）]**

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

ステップ 3　[Promiscuous Mode（無差別モード）] ドロップダウン リストで、**[Accept（許可）]** を選択し、**[OK]** をクリックします。

SPAN またはミラー化されたトラフィックのプロファイラ データ収集に使用する他の VMware ESX サーバ インターフェイスで同じ手順を繰り返して行ってください。

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



VMware サーバの設定

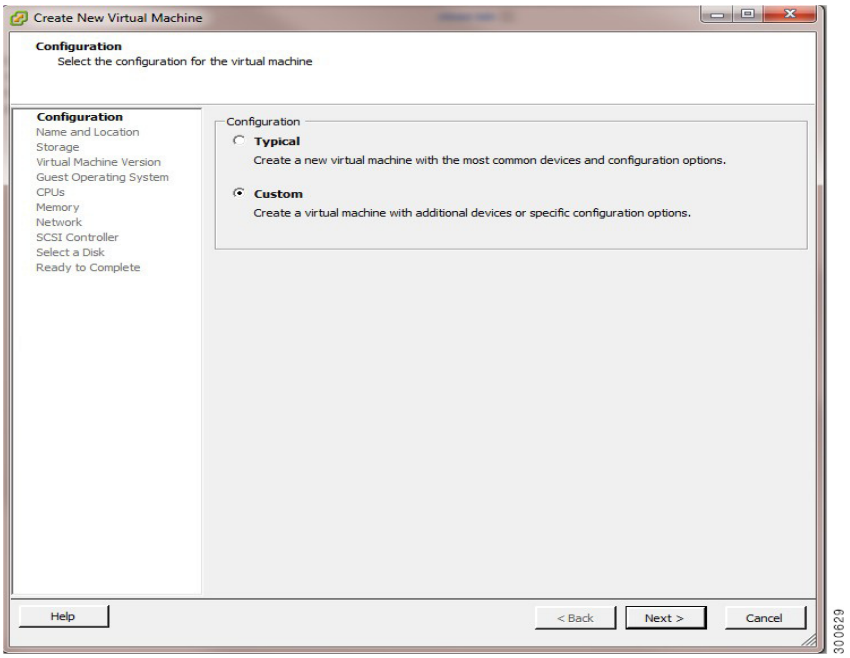
この項では、VMware vSphere Client を使用して VMware サーバを設定する方法について説明します。

ステップ 1　ESXi サーバにログインします。

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

ステップ 3　[Configuration Type（設定タイプ）] ダイアログボックスで、VMware 設定として **[Custom（カスタム）]** を選択し（図 4-4 を参照）、**[Next（次へ）]** をクリックします。

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

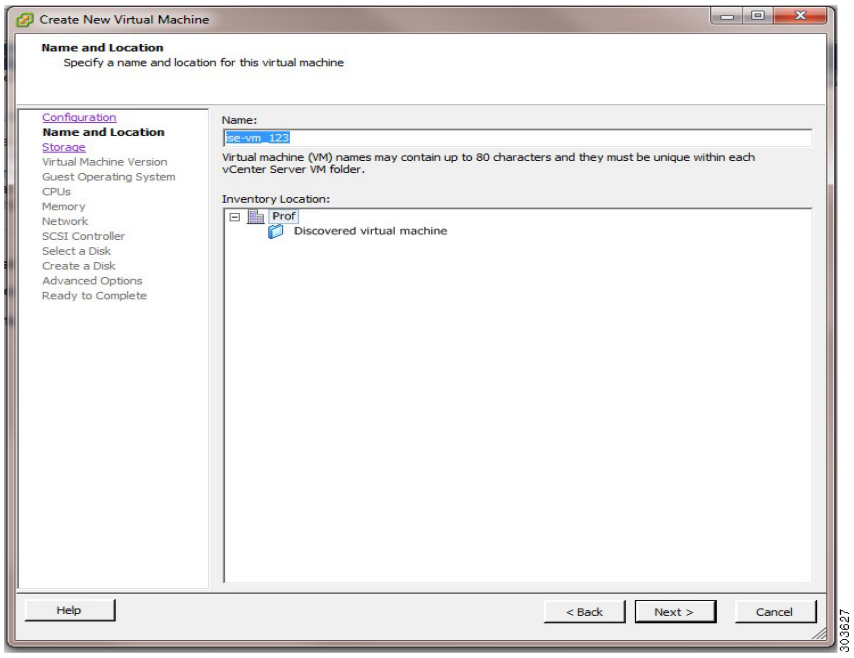


[Name and Location（名前とロケーション）] ダイアログボックスが表示されます（図 4-5 を参照）。

ステップ 4　VMware システムの名前を入力し、**[Next（次へ）]** をクリックします。

ヒント　VMware ホストに使用するホスト名を使用します。

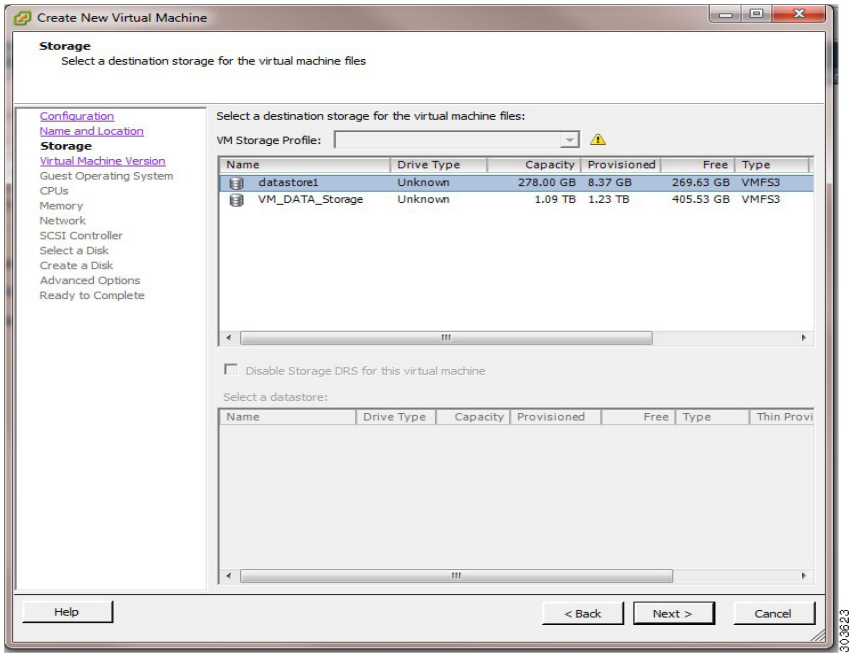
図 4-5　　[Name and Location（名前とロケーション）] ダイアログボックス



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

ステップ 5　推奨される使用可能な領域があるデータストアを選択し **[Next（次へ）]** をクリックします。詳細については、表 4-3を参照してください。

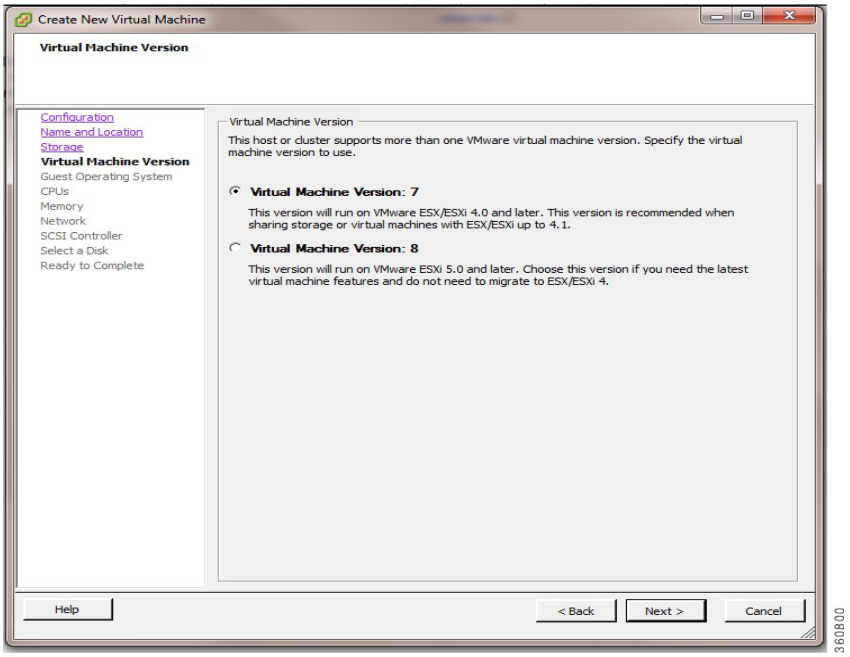
図 4-6　　[Datastore（データストア）] ダイアログボックス



[Virtual Machine Version（仮想マシンのバージョン）] ダイアログボックスが表示されます。

ステップ 6　（オプション）VM ホストまたはクラスタが複数の VMware 仮想マシン バージョンをサポートする場合は、[Virtual Machine Version 7（仮想マシン バージョン 7）] などの仮想マシン バージョンを選択して、[**Next（次へ）**] をクリックします（図 4-7 を参照）。

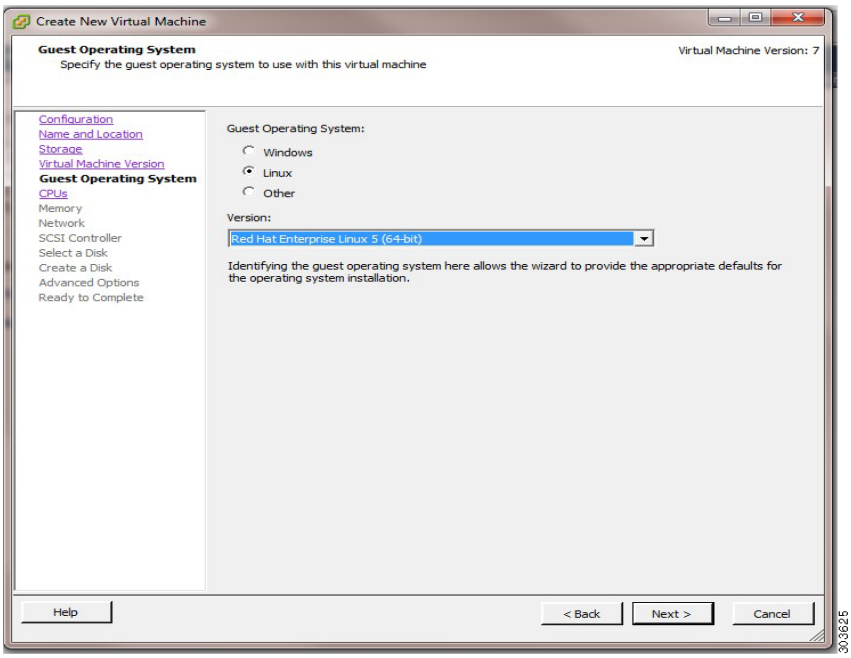
図 4-7　　仮想マシンのバージョン



[Guest Operating System（ゲスト オペレーティング システム）] ダイアログボックスが表示されます（図 4-8 を参照）。

ステップ 7　[Version（バージョン）] ドロップダウン リストから、[**Linux**] および [**Red Hat Enterprise Linux 5 (64-bit)**] を選択します。

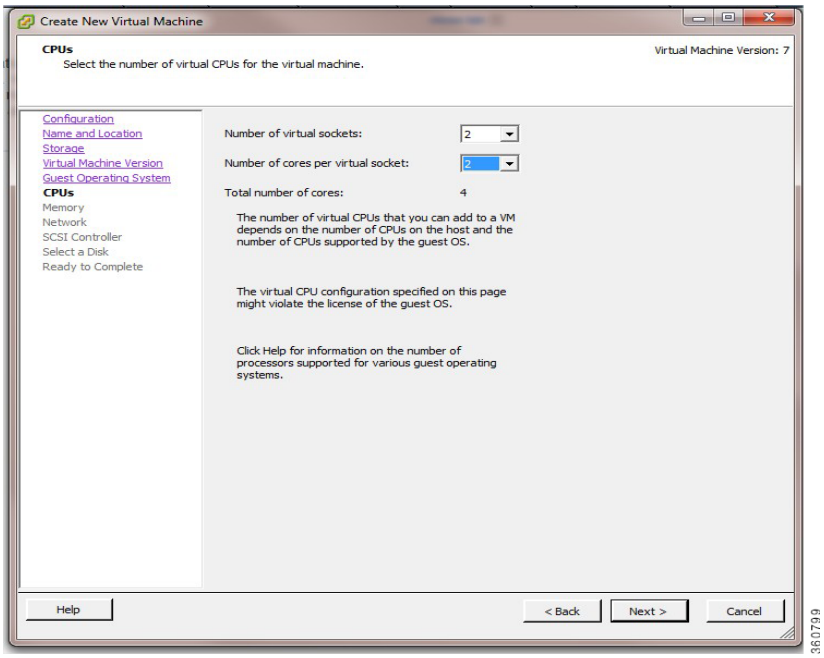
図 4-8　　[Guest Operating System（ゲスト オペレーティング システム）] ダイアログボックス



[Number of Virtual Processors（仮想プロセッサの数）] ダイアログボックスが表示されます（図 4-9 を参照）。

ステップ 8　[Number of virtual sockets（仮想ソケットの数）] および [Number of cores per virtual socket（仮想ソケットあたりのコア数）] ドロップダウン リストで、[2] を選択します。コアの総数は 4 にする必要があります。詳細については、「実稼働環境向けの VMware アプライアンスの仕様」を参照してください。[**Next（次へ）**] をクリックします。

図 4-9　　[Number of Virtual Processors（仮想プロセッサの数）] ダイアログボックス

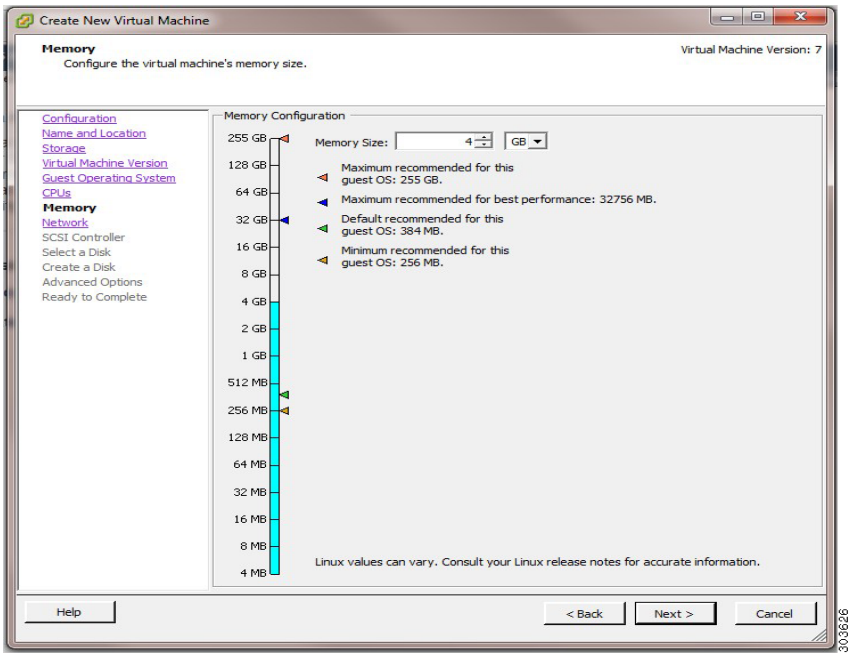


（オプション、一部の ESX サーバのバージョンに表示されます。[Number of virtual processors（仮想プロセッサの数）] のみが表示される場合は、[4] を選択します。

[Memory Configuration（メモリ設定）] ダイアログボックスが表示されます（図 4-10 を参照）。

ステップ 9　表 4-2 に記載されている推奨に基づいた値を入力し、[**Next（次へ）**] をクリックします。

図 4-10　[Memory Configuration（メモリ設定）] ダイアログボックス

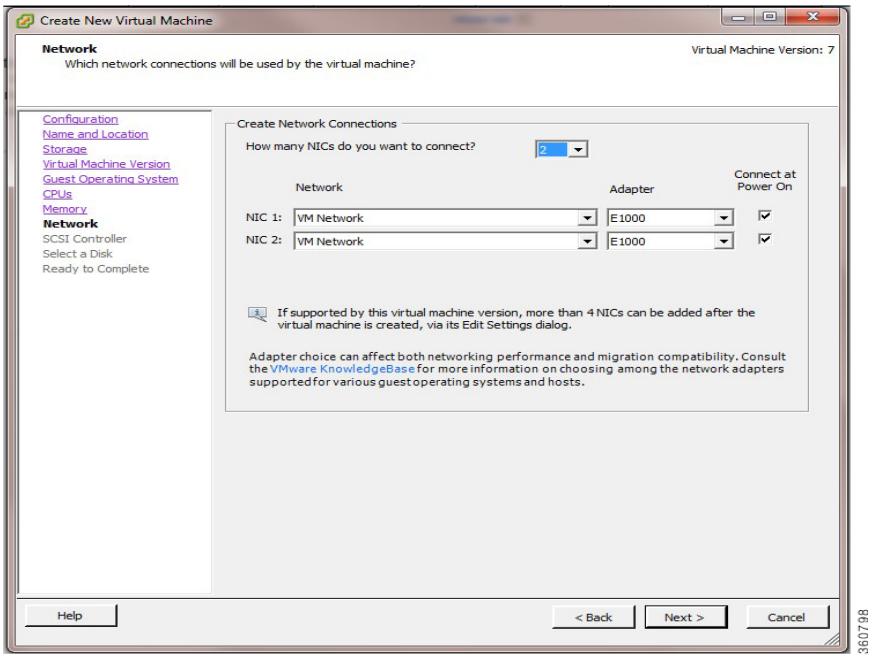


[Network Interface Card (NIC) Configuration（ネットワーク インターフェイス カード（NIC）設定）] ダイアログボックスが表示されます（図 4-11 を参照）。

ステップ 10　NIC およびアダプタを選択し、[**Next（次へ）**] をクリックします。

（注）　E1000 アダプタを選択することを推奨します。Cisco ISE リリース 1.2 は、E1000 および VMXNET3 アダプタのみをサポートします。その他の仮想 NIC ドライバはサポートされません。

図 4-11　[NIC Configuration（NIC 設定）] ダイアログボックス



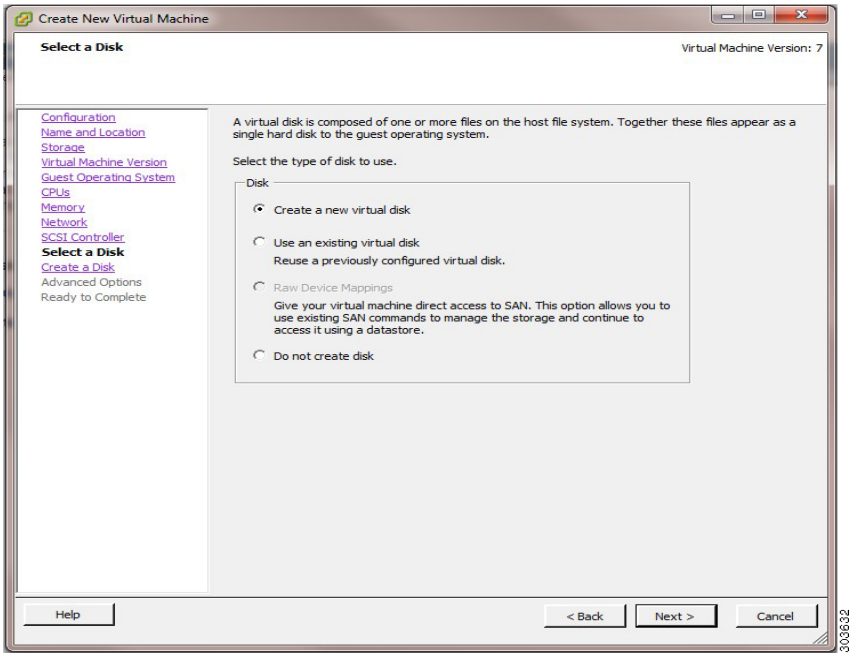
[SCSI Controller（SCSI コントローラ）] ダイアログ ボックスが表示されます。

ステップ 11　SCSI コントローラとして **[LSI Logic Parallel（LSI 論理並列）]** を選択し、[Next（次へ）] をクリックします。

[Select a Disk（ディスクの選択）] ダイアログ ボックスが表示されます（図 4-12 を参照）。

ステップ 12　**[Create a new virtual disk（新しい仮想ディスクの作成）]** を選択し、**[Next（次へ）]** をクリックします。

図 4-12　　ディスクの選択



[Virtual Disk Size and Provisioning Policy（仮想ディスク サイズとプロビジョニング ポリシー）] ダイアログ ボックスが表示されます。

ステップ 13　[Disk Provisioning（ディスク プロビジョニング）] ダイアログ ボックスで、[Thick Provisioning Lazy Zeroed（Lazy Zeroed のシック プロビジョニング）] オプション ボタンをクリックします。**[Next（次へ）]** をクリックして続行します。（図 4-13 を参照）。

VMware クライアントの以前のバージョンを使用する場合、チェックボックスの選択を解除します。

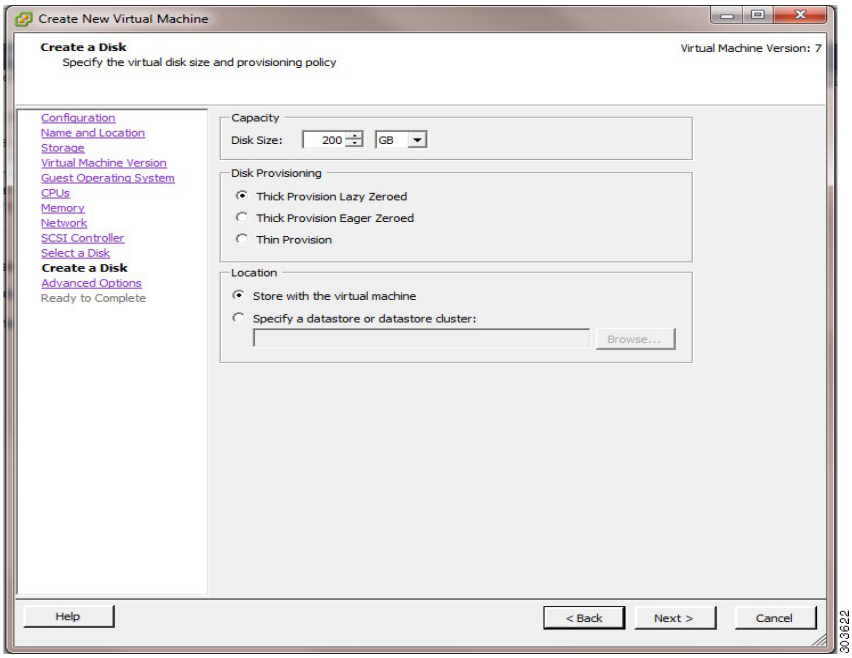
a. **[Allocate and commit space on demand （Thin Provisioning）（オンデマンドでスペースを割り当ててコミットする（シン プロビジョニング））]** チェックボックスの選択を解除します。

b. **[Support clustering features such as Fault Tolerance（フォルト トレランスのようなクラスタリング機能をサポートする）]** チェックボックスの選択を解除します。

（注）　[Thick Provisioned Lazy Zeroed（シックプロビジョニングされた Lazy Zeroed）] オプションが選択されていると、仮想ディスクはすべてのプロビジョニングされた領域に割り当てられ、ただちに仮想マシンからアクセスできるようになります。Lazy Zeroed ディスクはそれまでゼロ化されてないため、これにより、プロビジョニングが非常に高速になります。ただし、各ブロックは最初の書き込みが行われる前にゼロでクリアされるため、最初の書き込み時にはその分の遅延が発生します。

VMFS に I/O 集中型のアプリケーションを導入する場合は、[Thick Provisioned Eager Zeroed（Recommended for I/O intensive workloads）（シックプロビジョニングされた Eager Zeroed（I/O 集中型のワークロードに推奨））] オプションを推奨します。仮想ディスクはすべてのプロビジョニングされた領域に割り当てられ、VMDK ファイル全体がゼロでクリアされてから、仮想マシンがアクセスできるようになります。これは、仮想マシンが VMDK ファイルにアクセスできるようになるまでの時間が長くなるが、最初の書き込み時のゼロ化による追加の遅延は発生しないことを意味します。

図 4-13　[Disk Provisioning（ディスク プロビジョニング）] ダイアログ ボックス



[Advanced Options（拡張オプション）] ダイアログボックスが表示されます。

ステップ 14　詳細オプションを選択し、[**Next（次へ）**] をクリックします。

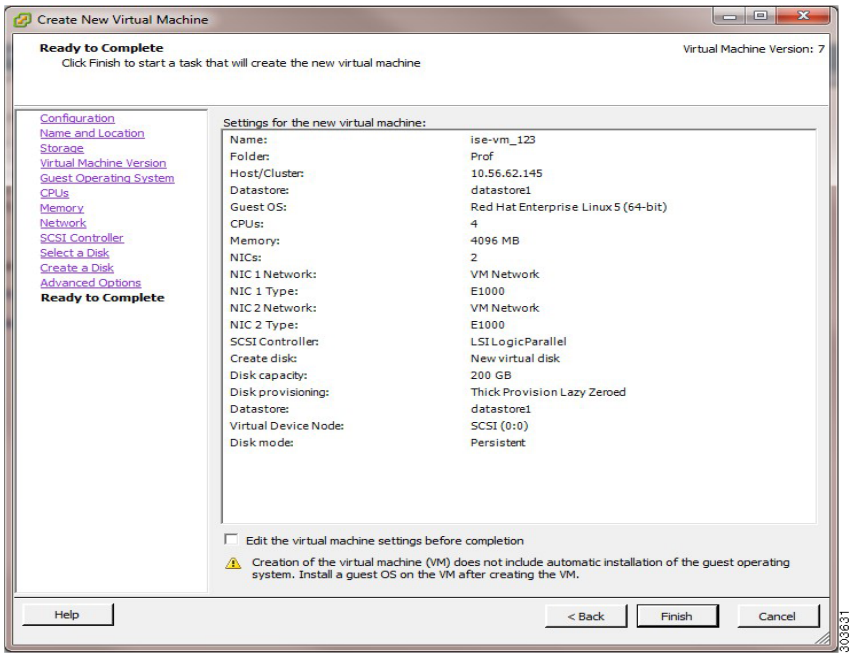
[Ready to Complete New Virtual Machine（新規仮想マシンを完了する準備ができました）] ダイアログボックスが表示されます（図 4-14 を参照）。

ステップ 15　新しく作成された VMware システムの名前、ゲスト OS、CPU、メモリ、およびディスク サイズなどの設定の詳細を確認します。次の値が確認されるはずです。

- ゲスト OS：Red Hat Enterprise Linux 5（64 ビット）
- CPU：4
- メモリ：4 GB または 4096 MB
- ディスク サイズ：VMware ディスク領域の推奨事項に基づいて、200 GB ～ 2 TB

仮想マシンでの Cisco ISE のインストールを正常に行うには、このマニュアルに記載されている推奨事項に必ず従ってください。

図 4-14　[Ready to Complete（完了する準備ができました）] ダイアログボックス



ステップ 16　[**Finish（完了）**] 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。

新しく作成された VMware システムをアクティブにするには、VMware クライアントのユーザ インターフェイスの左側のペインで [**VM**] を右クリックして、[**Power（電源）**] > [**Power On（電源の投入）**] 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。DVD から Cisco ISE ソフトウェアをインストールするには、DVD からブートするように VMware システムを設定する必要があります。このためには、仮想 DVD ドライブを使用して VMware システムを設定する必要があります。

このインストールは、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、「VMware システムを Cisco ISE ソフトウェア DVD から起動するための設定」を参照してください。

（注）　Cisco ISE 1.2 ISO をダウンロードし、その ISO イメージを DVD に書き込み、Cisco ISE 1.2 を仮想マシンにインストールするために使用します。

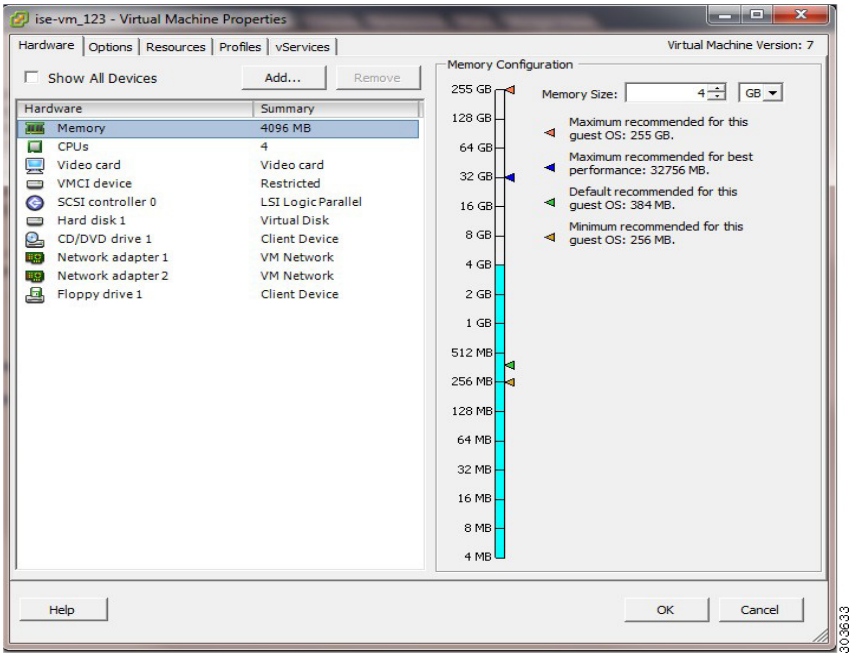
VMware システムを Cisco ISE ソフトウェア DVD から起動するための設定

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 ISE ソフトウェア 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。

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

[Virtual Machine Properties（仮想マシンのプロパティ）] ウィンドウが表示されます。図 4-15 に作成された VMware システムのプロパティを表示します。

図 4-15　[Virtual Machine Properties（仮想マシンのプロパティ）] ダイアログボックス

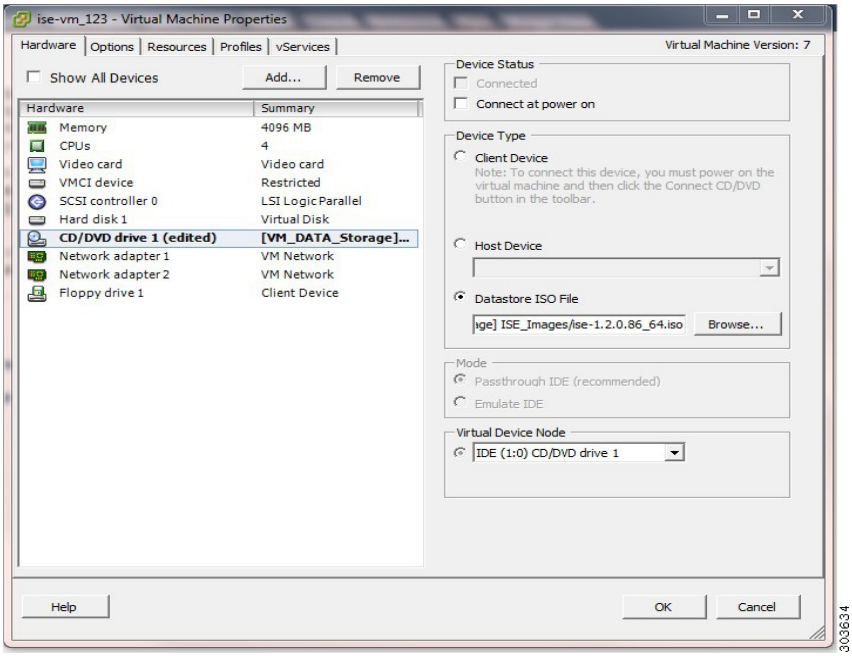


ステップ 2　[Virtual Machine Properties（仮想マシンのプロパティ）] ダイアログボックスで、**[CD/DVD Drive 1（CD/DVD ドライブ 1）]** を選択します。

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

ステップ 3　**[Host Device（ホスト デバイス）]** オプション ボタンをクリックし、ドロップダウン リストから DVD ホスト デバイスを選択します。

図 4-16　　仮想マシンのプロパティ：[Host Device（ホスト デバイス）] オプション



ステップ 4　[**Connect at Power On（電源投入時に接続）**] オプションを選択し、[**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。

このタスクを完了すると、VMware クライアント ユーザ インターフェイスで [**Console（コンソール）**] タブをクリックし、左側のペインで、[**VM**] を右クリックし、[**Power（電源）**] を選択して、[**Reset（リセット）**] を選択します。

VMware システムへの Cisco ISE ソフトウェアのインストール

ステップ 1　VMware クライアントにログインします。

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 システムが起動している場合は、システムをオフにします。

b.　VMware システムを起動します。

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 [Date and Time（日付と時刻）] フィールドに移動し、**Enter** を押します。

e.　UTC/グリニッジ標準時（GMT）タイム ゾーンを入力します。

（注）　すべての Cisco ISE ノードを UTC タイム ゾーンに設定することを推奨します。このタイム ゾーンの設定により、展開におけるさまざまなノードからのレポート、ログ、およびポスチャ エージェントのログ ファイルが、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がインストールされない場合、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　Cisco ISE ソフトウェア DVD を VMware ESX ホストの CD/DVD ドライブに挿入して、仮想マシンをオンにします。

（注）　Cisco ISE リリース 1.2 ソフトウェアを Cisco ソフトウェアのダウンロード サイト（http://www.cisco.com/en/US/products/ps11640/index.html ）からダウンロードし、DVD に書き込みます。Cisco.com クレデンシャルの提供が求められます。

DVD の起動時、コンソールには以下のように表示されます。

```
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。

インストーラが、VMware システムへの Cisco ISE ソフトウェアのインストールを開始します。

（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、「Cisco ISE セットアップ プログラム パラメータ」（P.3-8）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、次の手順に従います。

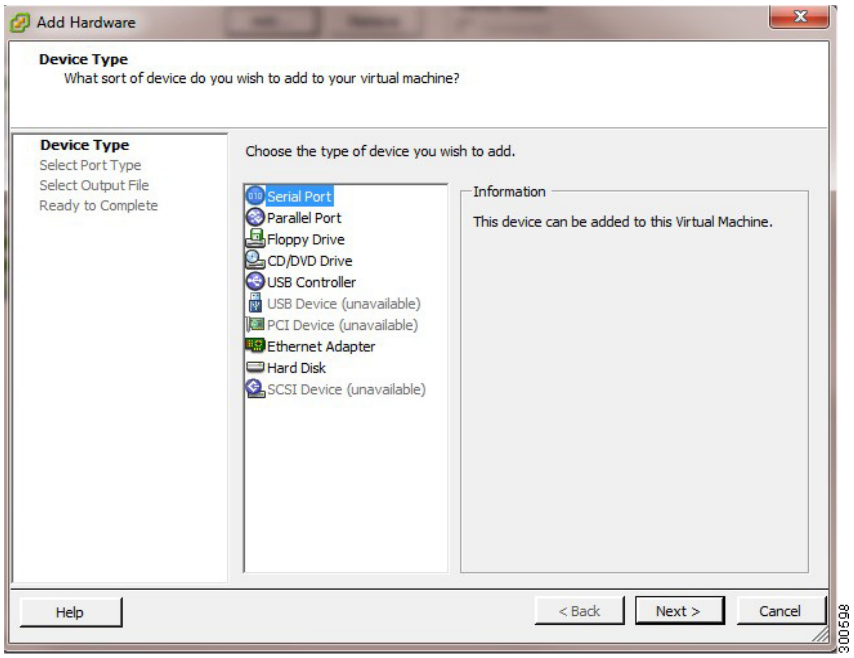
ステップ 1　特定の VMware サーバ（たとえば ISE-120）の電源をオフにします。

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

ステップ 3　[Hardware（ハードウェア）] タブで [**Add（追加）**] をクリックします（図 4-15 を参照）。

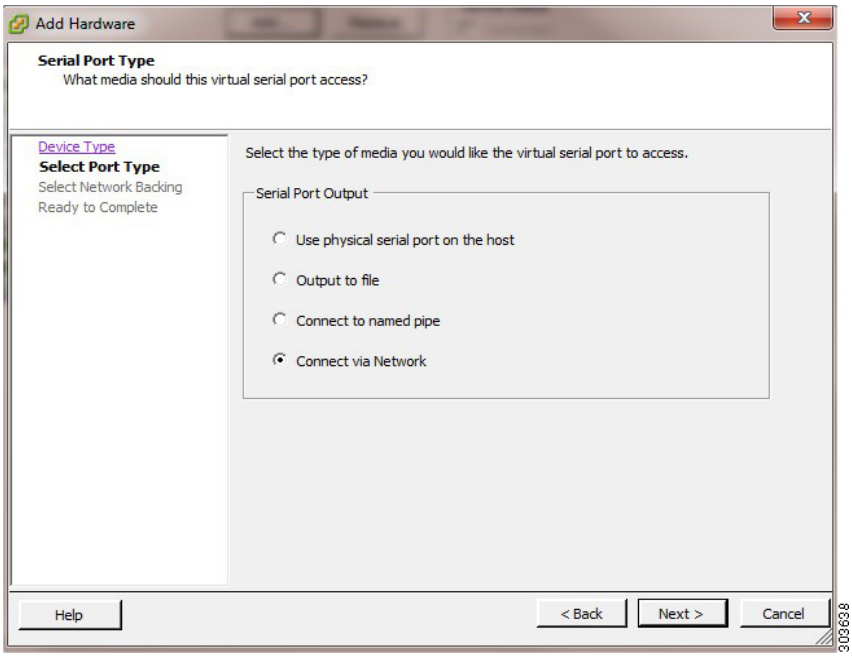
ステップ 4　[**Serial Port（シリアル ポート）**] を選択し、[**Next（次へ）**] をクリックします（図 4-17 を参照）。

図 4-17　ハードウェアの追加：デバイス タイプ



ステップ 5　[Serial Port Output（シリアル ポートの出力）] 領域で、[**Use physical serial port on the host（ホスト上の物理シリアル ポートを使用する）**] または [**Connect via Network（ネットワーク経由で接続）**] オプション ボタンを使用して、[**Next（次へ）**] をクリックします（図 4-18 を参照）。

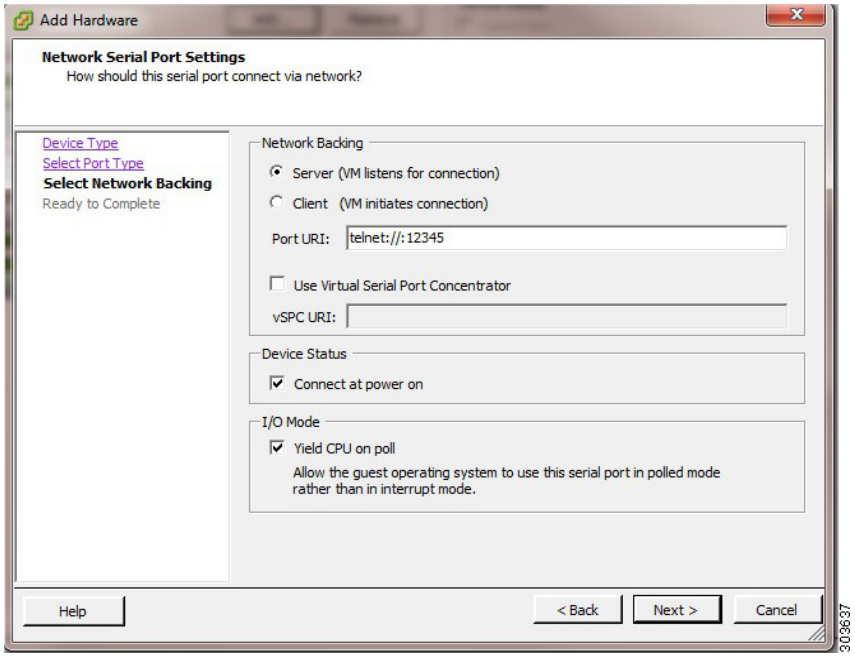
図 4-18　　ハードウェアの追加：シリアル ポート タイプ



a. [Connect via Network（ネットワーク経由で接続）] オプションを選択した場合は、ESX サーバ上のファイアウォール ポートを開く必要があります。

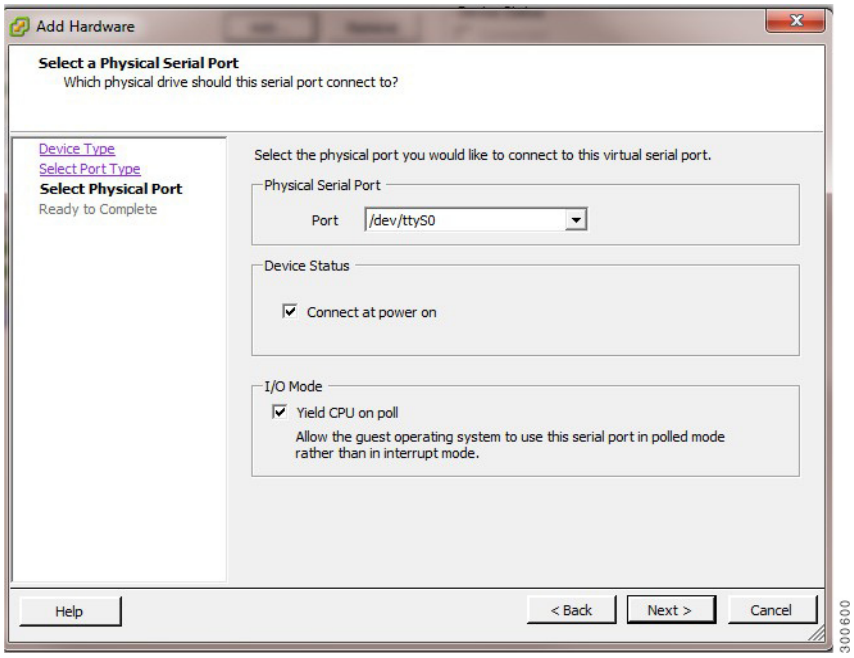
b. ホスト上の物理シリアル ポートを選択する場合は、そのポートを選択します。次の 2 つのいずれかのオプションを選択できます。

- **/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）。



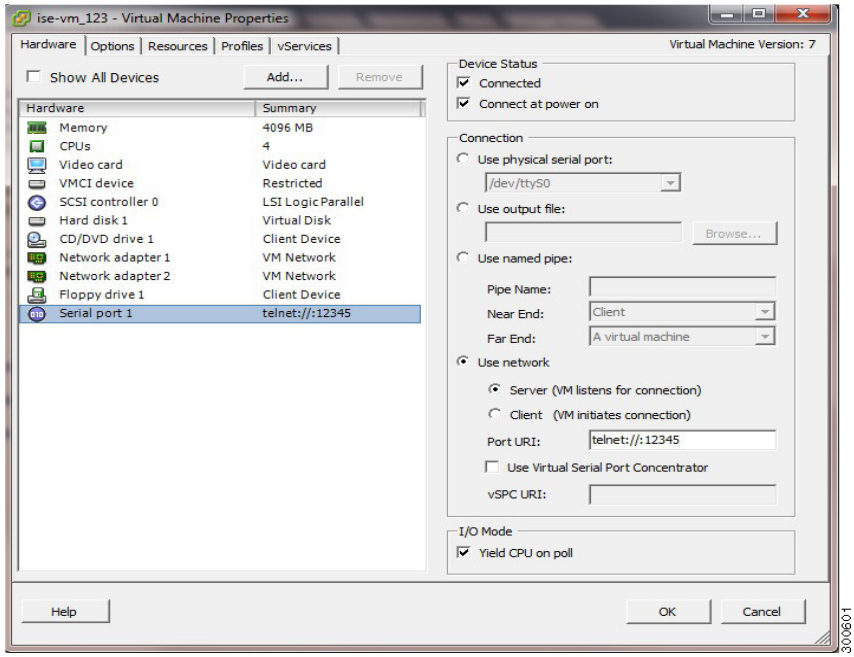
ステップ 6　[**Next**（次へ）] をクリックします（図 4-19 を参照）。

図 4-19　　物理シリアル ポートの選択



ステップ 7　[Device Status（デバイスのステータス）] 領域で、適切なチェックボックスをオンにします。デフォルトは [Connected（接続済み）] です（図 4-20 を参照）。

図 4-20　　ハードウェア：デバイスの状態



ステップ 8　Cisco ISE VMware サーバに接続するには、**[OK]** をクリックします。

Cisco ISE 仮想マシンの複製

Cisco ISE ノードの厳密なレプリカを作成することで、Cisco ISE VMware 仮想マシン（VM）を複製できます。たとえば、複数のポリシー サービス ノード（PSN）を使用した分散導入環境で、VM の複製は PSN を迅速かつ効率的に導入するのに役立ちます。PSN をそれぞれ別個にインストールして設定する必要はありません。

テンプレートを使用して Cisco ISE VM を複製することもできます。詳細については、「テンプレートを使用した Cisco ISE 仮想マシンの複製」（P.4-26）を参照してください。

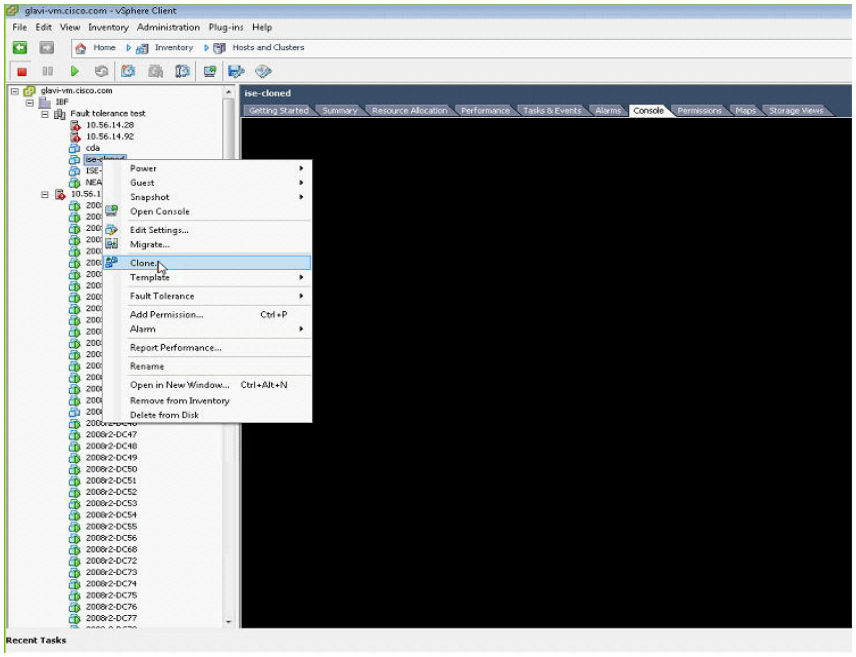
はじめる前に

- 複製する Cisco ISE VM がシャット ダウンされていることを確認します。vSphere クライアントで、複製する Cisco ISE VM を右クリックし、**[Power（電源）] > [Shut Down Guest（ゲストをシャットダウン）]** を選択します。
- 複製されたマシンの IP アドレスとホスト名を変更したことを確認してから、そのマシンの電源をオンにして、ネットワークに接続します。

ステップ 1　管理者権限を持つユーザ（root ユーザ）として ESXi サーバにログインします。

ステップ 2　複製する Cisco ISE VM を右クリックし、**[Clone（複製）]** をクリックします（図 4-21 を参照）。

図 4-21　Cisco ISE 仮想マシンの複製



ステップ 3　[Name and Location（名前とロケーション）] ダイアログ ボックスに作成する新しいマシンの名前を入力し、[**Next（次へ）**] をクリックします。

これは、新しく作成する Cisco ISE VM のホスト名ではなく、参照のための説明となる名前です。

ステップ 4　新しい Cisco ISE VM を実行するホストまたはクラスタを選択し、[**Next（次へ）**] をクリックします。

ステップ 5　新しい Cisco ISE VM 用のデータストアを選択して、[**Next（次へ）**] をクリックします。

このデータストアは、ESX または ESXi サーバ上のローカル データストアまたはリモート ストレージの場合があります。サポートされるストレージ タイプについては、表 4-1（P.4-2）を参照してください。データストアに表 4-3（P.4-4）に記載されている十分なディスク領域があることを確認します。

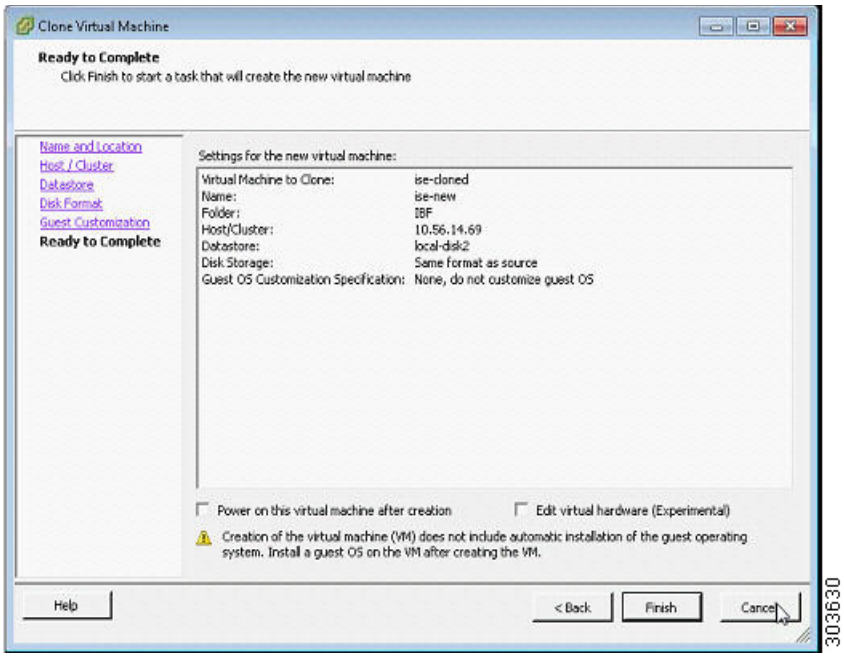
ステップ 6　[Disk Format（ディスクのフォーマット）] ダイアログ ボックスで [**Same format as source（ソースと同じフォーマット）**] オプション ボタンをクリックし、[**Next（次へ）**] をクリックします。

このオプションは、この新しいマシン複製元である Cisco ISE VM で使用されているのと同じフォーマットをコピーします。

ステップ 7　[Guest Customization（ゲスト カスタマイズ）] ダイアログ ボックスで [**Do not customize（カスタマイズしない）**] オプション ボタンをクリックし、[**Next（次へ）**] をクリックします。

[Ready to Complete（完了する準備ができました）] ダイアログ ボックスが表示されます（図 4-22 を参照）。

図 4-22　　ダイアログの複製の準備



ステップ 8　[**Finish**（完了）] をクリックします。

次の作業

- 「複製された仮想マシンの IP アドレスおよびホスト名の変更」（P.4-28）
- 「複製された Cisco 仮想マシンのネットワークへの接続」（P.4-30）

関連項目

- 「テンプレートを使用した Cisco ISE 仮想マシンの複製」（P.4-26）

テンプレートを使用した Cisco ISE 仮想マシンの複製

vCenter を使用している場合は、VMware テンプレートを使用して、Cisco ISE 仮想マシン（VM）を複製できます。テンプレートに Cisco ISE ノードを複製し、そのテンプレートを使用して、複数の新しい Cisco ISE ノードを作成できます。テンプレートを使用した仮想マシンの複製は、次の 2 つのステップで構成される手順です。

1. 「仮想マシン テンプレートの作成」（P.4-27）
2. 「仮想マシン テンプレートの導入」（P.4-27）

仮想マシン テンプレートの作成

はじめる前に

- 複製する Cisco ISE VM がシャット ダウンされていることを確認します。vSphere クライアントで、複製する Cisco ISE VM を右クリックし、[**Power（電源）**] > [**Shut Down Guest（ゲストをシャットダウン）**] を選択します。
- テンプレートは、インストールしたばかりでセットアップ プログラムを実行していない Cisco ISE リリース 1.2 VM から作成することを推奨します。次に、IP アドレスおよびホスト名を個別に作成し、設定した Cisco ISE の各ノードでセットアップ プログラムをそれぞれ実行します。

ステップ 1　管理者権限を持つユーザ（root ユーザ）として ESXi サーバにログインします。

ステップ 2　複製する Cisco ISE VM を右クリックし、[**Clone（複製）**] > [**Clone to Template（テンプレートに複製）**] を選択します。

ステップ 3　テンプレートの名前を入力し、[Name and Location（名前とロケーション）] ダイアログ ボックスでテンプレートを保存する場所を選択して、[**Next（次へ）**] をクリックします。

ステップ 4　テンプレートを保存する ESX ホストを選択して、[**Next（次へ）**] をクリックします。

ステップ 5　テンプレートを保存するデータストアを選択して、[**Next（次へ）**] をクリックします。

このデータストアに必要なディスク領域があることを確認します。詳細については、表 4-3（P.4-4）を参照してください。

ステップ 6　[Disk Format（ディスクのフォーマット）] ダイアログ ボックスで [**Same format as source（ソースと同じフォーマット）**] オプション ボタンをクリックし、[**Next（次へ）**] をクリックします。

[Ready to Complete（完了する準備ができました）] ダイアログボックスが表示されます。

ステップ 7　[**Finish（完了）**] をクリックします。

仮想マシン テンプレートの導入

仮想マシン テンプレートを作成したら、他の仮想マシン（VM）に導入できます。

ステップ 1　作成した Cisco ISE VM テンプレートを右クリックして、[**Deploy Virtual Machine from this template（このテンプレートから仮想マシンを導入）**] を選択します。

ステップ 2　新しい Cisco ISE ノードの名前を入力し、[Name and Location（名前とロケーション）] ダイアログ ボックスでノードの場所を選択して、[**Next（次へ）**] をクリックします。

ステップ 3　新しい Cisco ISE ノードを保存する ESX ホストを選択して、[**Next（次へ）**] をクリックします。

ステップ 4　新しい Cisco ISE に使用するデータストアを選択して、[**Next（次へ）**] をクリックします。

このデータストアに必要なディスク領域があることを確認します。詳細については、表 4-3（P.4-4）を参照してください。

ステップ 5　[Disk Format（ディスクのフォーマット）] ダイアログ ボックスで [**Same format as source（ソースと同じフォーマット）**] オプション ボタンをクリックし、[**Next（次へ）**] をクリックします。

ステップ 6　[Guest Customization（ゲスト カスタマイズ）] ダイアログ ボックスの [Guest Customization（ゲスト カスタマイズ）] オプション ボタンをクリックします。

[Ready to Complete（完了する準備ができました）] ダイアログボックスが表示されます。

ステップ 7　[**Edit Virtual Hardware（仮想ハードウェアの編集）**] チェックボックスをオンにして、[**Continue（続行）**] をクリックします。

[Virtual Machine Properties（仮想マシンのプロパティ）] ページが表示されます。

ステップ 8　[**Network Adapter（ネットワーク アダプタ）**] を選択し、チェックボックスおよび [**Connect at power on（電源投入時に接続）**] チェックボックスをオフにして、[**OK**] をクリックします。

ステップ 9　[**Finish（完了）**] をクリックします。

この Cisco ISE ノードの電源を投入し、IP アドレスとホスト名を設定し、ネットワークに接続できるようになりました。

次の作業

- 「複製された仮想マシンの IP アドレスおよびホスト名の変更」（P.4-28）
- 「複製された Cisco 仮想マシンのネットワークへの接続」（P.4-30）

関連項目

- 「テンプレートを使用した Cisco ISE 仮想マシンの複製」（P.4-26）

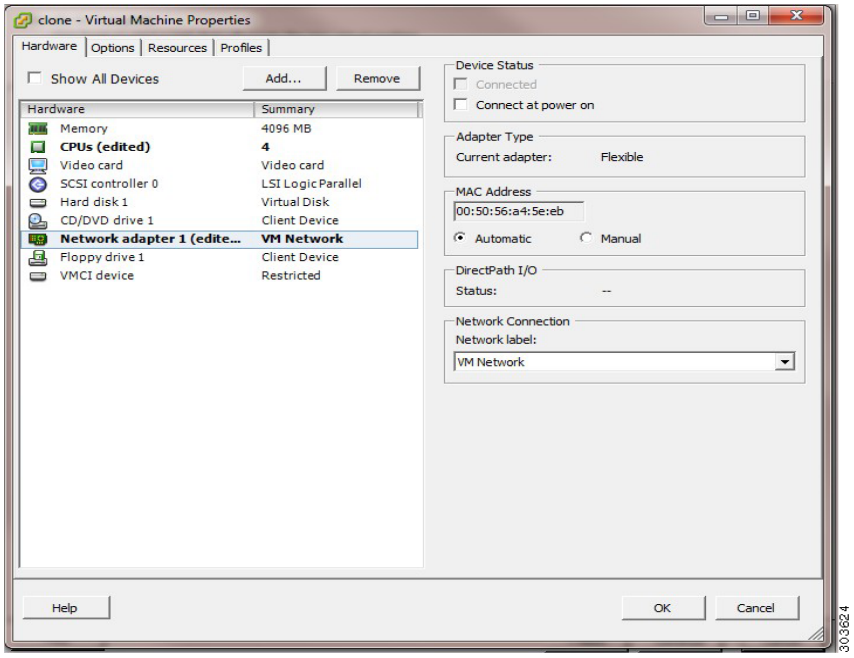
複製された仮想マシンの IP アドレスおよびホスト名の変更

Cisco ISE 仮想マシン（VM）を複製したら、そのマシンの電源を入れて、IP アドレスとホスト名を変更する必要があります。ノードのホスト名として「localhost」を使用することはできません。

はじめる前に

- Cisco ISE ノードがスタンドアロン状態であることを確認します。
- 新しく複製された Cisco ISE VM に電源を入れるときに、このマシンにネットワーク アダプタが接続されていないことを確認します。[Connected（接続済み）] および [**Connect at power on（電源投入時に接続）**] チェック ボックスをオフにします。図 4-23を参照してください。そうでない場合は、このノードが起動すると、複製元のマシンと同じ IP アドレスが使用されます。

図 4-23　　ネットワーク アダプタの接続解除



- 新しく複製された VM マシンの電源が投入されたらすぐに、このマシン用に設定するホスト名と IP アドレスがあることを確認します。この IP アドレスおよびホスト名のエントリは DNS サーバにある必要があります。
- 新しい IP アドレスまたはホスト名に基づく Cisco ISE ノードの証明書があることを確認します。

ステップ 1　新しく複製された Cisco ISE VM を右クリックして、[**Power（電源）**] > [**Power On（電源の投入）**] を選択します。

ステップ 2　新しく複製された Cisco ISE VM を選択して、[**Console（コンソール）**] タブをクリックします。

ステップ 3　Cisco ISE CLI で、次のコマンドを入力します。

configure terminal

hostname *hostname*

hostname は、設定する新しいホスト名です。Cisco ISE サービスが再起動されます。

ステップ 4　次のコマンドを入力します。

interface gigabit 0

ip address *ip_address netmask*

ip_address は、ステップ 3 で入力したホスト名に対応するアドレスであり、*netmask* はその *ip_address* のサブネット マスクです。システムにより、Cisco ISE サービスを再起動するように求められます。

ステップ 5　**Y** を入力して、Cisco ISE サービスを再起動します。

関連項目

『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2 (Cisco Identity Services Engine CLI リリース 1.2)*』を参照して、**ip address** コマンドおよび **hostname** コマンドについて確認してください。

複製された Cisco 仮想マシンのネットワークへの接続

電源を入れ、IP アドレスおよびホスト名を変更したら、ネットワークに Cisco ISE ノードを接続する必要があります。

ステップ 1　新しく複製された Cisco ISE 仮想マシン（VM）を右クリックして、[**Edit Settings（設定の編集）**] をクリックします。

ステップ 2　[Virtual Machine Properties（仮想マシンのプロパティ）] ダイアログ ボックスで [**Network Adapter（ネットワーク アダプタ）**] をクリックします。

ステップ 3　[Device Status（デバイスのステータス）] 領域で、[**Connected（接続済み）**] チェックボックスおよび [**Connect at power on（電源投入時に接続）**] チェックボックスをオンにします。

ステップ 4　[**OK**] をクリックします。

Cisco ISE 3300 シリーズ、Cisco NAC、および Cisco Secure ACS のアプライアンスへのリリース 1.2 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 ISE-3300、Cisco Secure ACS、および Cisco NAC のアプライアンス プラットフォームに、Cisco ISE リリース 1.2 ソフトウェアを DVD から最初にインストール（フレッシュ インストール）する手順について説明します。

- Cisco ISE-3315
- Cisco ISE-3355
- Cisco ISE-3395
- Cisco Secure ACS-1121
- Cisco NAC-3315
- Cisco NAC-3355
- Cisco NAC-3395

（注） Cisco ISE リリース 1.2 ISO イメージをダウンロードし、ISO イメージをDVD に書き込んで、Cisco ISE-3300 シリーズ、および従来の Cisco NAC および Cisco Secure ACS のアプライアンスへのリリース1.2 のインストールに使用します。

Cisco Secure ACS または Cisco NAC アプライアンスへのこのソフトウェアのインストールは、Cisco ISE ソフトウェアがインストールされる基盤ハードウェアが同じ物理デバイス タイプであるため、シンプルなプロセスです。

- 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（それぞれ、Cisco ISE 3355 と Cisco ISE 3395 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。

（注） Cisco ISE 3300 シリーズ ハードウェア プラットフォームについての具体的な詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.x （Cisco Identity Services Engine ハードウェア インストール ガイド リリース 1.1.x）*』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。

- 「Cisco ISE リリース 1.2 ソフトウェアの DVD からのインストール」（P.5-2）：Cisco ISE リリース 1.2 ソフトウェアを DVD を使用してインストールする手順について説明します。
- 「イメージを再適用した Cisco ISE-3300 シリーズ 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.5-3）：Cisco ISE ソフトウェアを DVD を使用してインストールし、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、設定を確認する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.5-4）：Cisco ISE ソフトウェアを DVD を使用してインストールし、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、設定を確認する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.5-5）：イメージの再適用を完了する前に Cisco NAC アプライアンスで RAID の設定をリセットする方法など、Cisco ISE ソフトウェアを DVD を使用してインストールする手順について説明します。

（注）　Cisco ISE リリース 1.2 アプライアンスとして Cisco Secure ACS または Cisco NAC 再利用するには、Cisco Secure ACS または Cisco NAC アプライアンスのイメージを最適用し、Cisco ISE ソフトウェアをインストールして、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。

Cisco ISE リリース 1.2 ソフトウェアの DVD からのインストール

はじめる前に

- Cisco ISE リリース 1.2 またはインライン ポスチャ ノードの ISO イメージをダウンロードし、その ISO イメージを DVD に書き込んで、Cisco ISE-3300 シリーズ、および従来の Cisco NAC および Cisco Secure ACS アプライアンスへのリリース 1.2 のインストールに使用します。
- セットアップ プログラムを実行する前に、「Cisco ISE セットアップ プログラム パラメータ」（P.3-8）を確認してこの情報を準備します。

ステップ 1　アプライアンスにキーボードおよび VGA モニタを接続します。

ステップ 2　電源コードがアプライアンスに接続されており、DVD がアプライアンス CD/DVD ドライブに挿入されており、アプライアンスの電源が入っていることを確認します。

コンソールにブート オプションが表示されます。

ステップ 3　ログイン プロンプトで、**1** を入力して、**Enter** キーを押します。

ステップ 4　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。

ステップ 5　セットアップ プログラム パラメータの値を入力します。

Cisco ISE または IPN ソフトウェアが設定されると、システムが自動的にリブートします。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。

次の作業

- IPN ISO がインストールされている場合は、「インライン ポスチャ ノードの証明書の設定」（P.E-37）に進みます。
- Cisco ISE リリース 1.2 ISO イメージがインストールされている場合は、Cisco ISE CLI シェルにログインし、**show application status ise** の CLI コマンドを実行して、Cisco ISE アプリケーション プロセスの状態を検査できます。

イメージを再適用した Cisco ISE-3300 シリーズ 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、既存のシスコ ISE-3300 シリーズ アプライアンスに Cisco ISE 1.2 アプライアンスとしてイメージを最適用する手順を説明します。

はじめる前に

- Cisco ISE リリース 1.2 またはインライン ポスチャ ノードの ISO イメージをダウンロードし、その ISO イメージを DVD に書き込んで、Cisco ISE-3300 シリーズ、および従来の Cisco NAC および Cisco Secure ACS アプライアンスへのリリース 1.2 のインストールに使用します。
- 「Cisco SNS-3400 シリーズ アプライアンスの設定の前提条件」（P.3-7）の情報を確認してください。
- セットアップ プログラムを実行する前に、「Cisco ISE セットアップ プログラム パラメータ」（P.3-8）を確認してこの情報を準備します。

ステップ 1　Cisco ISE アプライアンスの電源が入っている場合は、オフにします。

ステップ 2　Cisco ISE 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 [Date and Time（日付と時刻）] フィールドに移動し、**Enter** を押します。

ステップ 5　UTC/GMT のタイム ゾーンに時間を設定します。

（注）　すべての Cisco ISE ノードを UTC タイム ゾーンに設定することを推奨します。このタイム ゾーンの設定により、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 リリース 1.2 ソフトウェアの DVD からのインストール」（P.5-2）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 プロセスの確認」（P.3-16）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 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、既存の Cisco Secure ACS アプライアンスに Cisco ISE 3300 シリーズ リリース 1.2 アプライアンスとしてイメージの再適用を行う手順を説明します。

はじめる前に

- Cisco ISE リリース 1.2 またはインライン ポスチャ ノードの ISO イメージをダウンロードし、その ISO イメージを DVD に書き込んで、Cisco ISE-3300 シリーズ、および従来の Cisco NAC および Cisco Secure ACS アプライアンスへのリリース 1.2 のインストールに使用します。
- 「Cisco SNS-3400 シリーズ アプライアンスの設定の前提条件」（P.3-7）の情報を確認してください。
- セットアップ プログラムを実行する前に、「Cisco ISE セットアップ プログラム パラメータ」（P.3-8）を確認してこの情報を準備します。

ステップ 1　Cisco ACS アプライアンスの電源が入っている場合は、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 [Date and Time（日付と時刻）] フィールドに移動し、**Enter** を押します。

ステップ 5　アプライアンスの時刻を UTC/GMT タイム ゾーンに設定します。

（注）　すべての Cisco ISE ノードを UTC タイム ゾーンに設定することを推奨します。このタイム ゾーンの設定により、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 リリース 1.2 ソフトウェアの DVD からのインストール」（P.5-2）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 プロセスの確認」（P.3-16）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、既存の Cisco NAC アプライアンスに Cisco ISE 1.2 アプライアンスとしてイメージを最適用する手順を説明します。

はじめる前に

- Cisco ISE リリース 1.2 またはインライン ポスチャ ノードの ISO イメージをダウンロードし、その ISO イメージを DVD に書き込んで、Cisco ISE-3300 シリーズ、および従来の Cisco NAC および Cisco Secure ACS アプライアンスへのリリース 1.2 のインストールに使用します。
- 「Cisco SNS-3400 シリーズ アプライアンスの設定の前提条件」（P.3-7）の情報を確認してください。
- セットアップ プログラムを実行する前に、「Cisco ISE セットアップ プログラム パラメータ」（P.3-8）を確認してこの情報を準備します。

ステップ 1　Cisco NAC アプライアンスの電源が入っている場合は、オフにします。

ステップ 2　Cisco NAC 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 [Date and Time（日付と時刻）] フィールドに移動し、**Enter** を押します。

ステップ 5　アプライアンスの時刻を UTC/GMT タイム ゾーンに設定します。

（注）　すべての Cisco ISE ノードを UTC タイム ゾーンに設定することを推奨します。このタイム ゾーンの設定により、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 600 GB disk space for this appliance type」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」で説明されているように、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 リリース 1.2 ソフトウェアの DVD からのインストール」（P.5-2）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 プロセスの確認」（P.3-16）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 ISE 1.2 のインストールを進めるために、NAC アプライアンスの RAID 設定のリセットが必要な場合があります。

ステップ 1　Cisco ISE ソフトウェア DVD を使用して 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るはずです）。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　矢印キーを使用して [RAID Properties（RAID のプロパティ）] に移動し、**Enter** を押します。

ステップ 5　矢印キーを使用して [Manage Array（アレイの管理）] に移動し、**Enter** を押します。

ステップ 6　矢印キーを使用して [Delete Array（アレイの削除）] に移動し、**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。

システムにより、[Exit the Configuration Utility and Reboot?（設定ユーティリティを終了して再起動しますか?）] プロンプトが表示されます。

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 ISE ソフトウェア DVD がまだ挿入されているのであれば、アプライアンスによってインストール メニューが自動的に起動されます。

ステップ 10　Cisco ISE リリース 1.2 のインストールを開始するには **1** を押します。

管理者アカウントの管理

この章では、Cisco ISE の 2 種類の管理者アカウント、これらのアカウントの権限、およびこれらのアカウントを作成する方法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。

CLI 管理および Web ベース管理のユーザー権限の違い

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使用するためのものです。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。

Cisco ISE Web インターフェイスへの最初のアクセスは、セットアップ プロセスで定義した CLI 管理ユーザのユーザ名、およびパスワードを使用して行うことができます。Web ベースの管理の場合、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。

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、他の管理タスクを実行できます。

CLI 管理ユーザおよび Web ベースの管理ユーザによって実行されるタスク

- Cisco ISE アプリケーション データをバックアップする。
- Cisco ISE アプライアンス上に任意のシステム、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 サーバの設定を行う。

CLI 管理ユーザによってのみ実行されるタスク

- 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に、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リセット」（P.7-9）を参照してください。

（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 ベースの管理ユーザは、Cisco ISE CLI に自動的にログインできません。CLI 管理ユーザだけが Cisco ISE CLI にアクセスできます。

サポートされているブラウザについては、「Web ブラウザを使用した Cisco ISE へのアクセス」（P.7-1）を参照してください。

CLI 管理ユーザの作成

Cisco ISE では、セットアップ プロセスで作成した CLI 管理ユーザ アカウントに加え、追加の CLI 管理ユーザ アカウントを作成することができます。CLI 管理ユーザのクレデンシャルを保護するために、Cisco ISE CLI アクセスに必要な CLI 管理ユーザの作成数は最低限にします。

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　**設定**モードを開始します。

ステップ 3　**username** コマンドを入力します。

（注） **username** コマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2（Cisco Identity Services Engine CLI リファレンス ガイド リリース 1.2）*』を参照してください。

Web ベース管理ユーザの作成

Cisco ISE システムに初めて Web によるアクセスを行う場合、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。

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。詳細については、『*Cisco Identity Services Engine User Guide, Release 1.2（Cisco Identity Services Engine ユーザ ガイド リリース 1.2）*』の「Creating a New Cisco ISE Administrator（新規 Cisco ISE 管理者の作成）」セクションを参照してください。

インストール後のタスクの実行

この章では、Cisco Identity Services Engine（ISE）リリース 1.2 ソフトウェア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。

Web ブラウザを使用した Cisco ISE へのアクセス

Cisco SNS-3400 シリーズ アプライアンスは次の HTTPS 対応ブラウザを使用して Web インターフェイスをサポートします。

- Mozilla Firefox バージョン 3.6.x 以降
- Microsoft Internet Explorer 8.x 以降

（注） Cisco ISE ユーザ インターフェイスは Microsoft IE8 のブラウザの IE7 互換モードでの使用をサポートしません（Microsoft IE8 は IE8 モードのみでサポートされます）。

- Apple Safari 4.x 以降

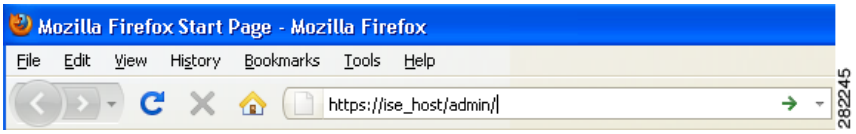
クライアント ブラウザを実行しているシステムに、Adobe Flash Player 11.2.0.0 以降がインストールされている必要があります。

この項では、次の内容について説明します。

Cisco ISE の Web ベースのインターフェイスへのログイン

初めて Cisco ISE の Web ベースの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 対応の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 ベースのインターフェイスにログインできます。

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　[Address（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。

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

たとえば、`https://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　設定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　**[Login（ログイン）]** をクリックします。

（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.7-8）を参照してください。

ヒント　Cisco ISE の GUI を表示するのに最低限必要な画面解像度は 1280 x 800 ピクセルです。

CLI 管理および Web ベースの管理のユーザ名とパスワードは同じではありません。Cisco ISE へのログイン時。これらの違いの詳細については、「CLI 管理および Web ベース管理のユーザー権限の違い」（P.6-1）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 ユーザ インターフェイスを使用して、定期的に管理者ログイン パスワードをリセットすることを推奨します。詳細については、『*Cisco Identity Services Engine User Guide, Release 1.2 (Cisco Identity Services Engine ユーザ ガイド リリース 1.2)*』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

指定された管理者のユーザ ID に対して誤ったパスワードを一定の回数入力すると、Cisco ISE ユーザ インターフェイスはシステムから「そのユーザをロックアウト」します。「管理者のロックアウトによるパスワードのリセット」（P.7-9）で説明されているように、Cisco ISE は、その管理者 ID に関連付けられたパスワードがリセットされるまで、[Monitor（モニタ）] > [Reports（レポート）] > [Catalog（カタログ）] > [Server Instance（サーバ インスタンス）] > [Server Administrator Logins report（サーバ管理者のログイン レポート）] にログ エントリを追加し、その管理者 ID のクレデンシャルを一時停止します。その管理者アカウントが無効になるまでの失敗回数は、『*Cisco Identity Services Engine User Guide, Release 1.2 (Cisco Identity Services Engine ユーザ ガイド リリース 1.2)*』の「Managing Administrators and Admin Access Policies（管理者および管理アクセスのポリシーの管理）」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。

Cisco ISE の Web ベースのインターフェイスからのログアウト

Cisco ISE の Web ベースのインターフェイスから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 [Log Out（ログアウト）] 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、管理セッションの完了時には、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 ベースのインターフェイスからログアウトされ、サブミットされていない構成データは保存されません。

Cisco ISE の 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 1.2 (Cisco Identity Services Engine ユーザ ガイド リリース 1.2)*』を参照してください。

ライセンスのインストール

ライセンスの詳細については、付録 D「Cisco ISE ライセンス」を参照してください。

証明書のインストール

証明書の詳細については、付録 E「Cisco ISE での証明書の管理」を参照してください。

Cisco ISE の設定の確認

この項では、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 つの方法について説明します。

- 「Web ブラウザを使用した設定の確認」（P.7-4）
- 「CLI を使用した設定の確認」（P.7-5）

（注）　Cisco ISE システムに初めて Web によるアクセスを行う場合、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 システムへの CLI ベースのアクセスの場合、デフォルトの管理者ユーザ名は admin であり、管理者パスワードにはデフォルトがないためユーザ定義です。

CLI 管理ユーザと Web ベースの管理ユーザの違いをさらに詳細に理解するには、「CLI 管理および Web ベース管理のユーザー権限の違い」（P.6-1）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 SNS-3400 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　[**Address（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。

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

たとえば、`https://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、[**Login（ログイン）**] 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 ユーザ インターフェイスを使用して、定期的に管理者パスワードをリセットすることを推奨します。管理者パスワードをリセットの詳細については、『*Cisco Identity Services Engine User Guide, Release 1.2（Cisco Identity Services Engine ユーザ ガイド リリース 1.2）*』を参照してください。

CLI を使用した設定の確認

Cisco ISE 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、PuTTY などのサポートされる製品を起動して、Cisco ISE アプライアンスへの Secure Shell（SSH）接続を確立します。

ステップ 2　[Host Name（ホスト名）]（または [IP Address（IP アドレス）]）フィールドにホスト名（または Cisco ISE アプライアンスのドット付き 10 進表記の IP アドレス）を入力し、[**Open（開く）**] をクリックします。

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あり、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　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。

```
Positron/admin# show application version ise

Cisco Identity Services Engine
------------------------------------------
Version      : 1.2.0.469
Build Date   : Mon Oct  8 23:06:25 2012
Install Date : Tue Oct  9 01:54:07 2012

Positron/admin#
```

303247

（注）　[Version（バージョン）] フィールドに、Cisco ISE ソフトウェアに現在インストールされているバージョンが表示されます。

ステップ 6　Cisco ISE プロセスの状態を調べるには、**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。

```
Install Date : Tue Oct  9 01:54:07 2012


Positron/admin# show application status ise

ISE Database listener is running, PID: 15502
ISE Database is running, number of processes: 29
ISE Application Server is running, PID: 18276
ISE Profiler DB is running, PID: 17524
ISE M&T Session Database is running, PID: 17409
ISE M&T Log Collector is running, PID: 18415
ISE M&T Log Processor is running, PID: 18521

Positron/admin#
```

303246

（注）　最新の Cisco ISE パッチを入手し Cisco ISE を最新に保つには、Web サイト 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 リリース 2.0.5 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、**show version** と入力し、**Enter** を押します。

コンソールに次のような出力が表示されます。

```
Cisco Application Deployment Engine OS Release: 2.0
ADE-OS Build Version: 2.0.5.083
ADE-OS System Architecture: i386
```

VMware ツールのインストールの確認

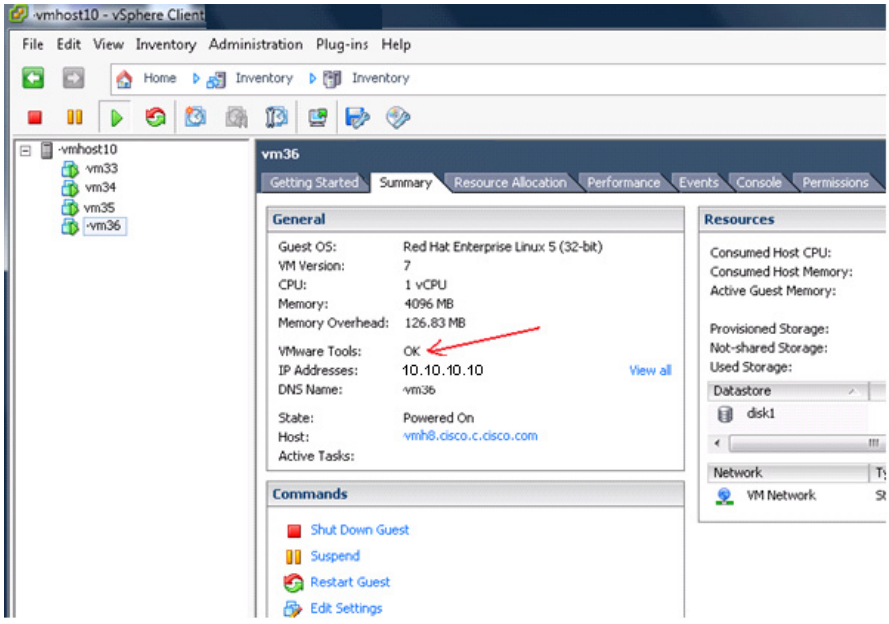
VMware ツールのインストールは次の 2 つの方法で確認できます。

- vSphere クライアントの [Summary（概要）] タブを使用する
- CLI の使用

vSphere クライアントの [Summary（概要）] タブを使用する

vShpere クライアントで指定された VMware ホストの [Summary（概要）] タブに移動します。[VMware Tools（VMware ツール）] フィールドの値が OK である必要があります。（図 7-1 を参照）。

図 7-1　　vSphere Client での VMware ツールの確認



CLI の使用

show inventory 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ている仮想マシンの [Driver Descr（ドライバの説明）] フィールドに、VMware Virtual Ethernet ドライバが表示されます。

```
vm36/admin# show inventory

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#
```

VMware ツールのアップグレード

Cisco ISE ISO イメージ（通常、アップグレード、またはパッチ）には、サポートされる VMware ツールが含まれています。VMware クライアント ユーザ インターフェイスを使用した VMware ツールのアップグレードは、Cisco ISE ではサポートされていません。VMware ツールを新しいバージョンにアップグレードする場合、サポートは Cisco ISE の新しいバージョンで提供されます（通常、アップグレード、またはパッチ リリース）。

管理者パスワードのリセット

Cisco ISE 管理者パスワードをリセットする方法には次の 2 通りがあります。

- 「紛失、失念、侵害されたパスワードのリセット」（P.7-8）：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 システム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リセット」（P.7-9）：ログイン試行の失敗回数が多すぎたことが原因で管理者アカウントがロックされた場合は、この手順を使用します。

紛失、失念、侵害されたパスワードのリセット

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 システムにログインできない場合は、Cisco ISE ソフトウェア DVD を使用して、管理者パスワードをリセットすることができます。

はじめる前に

次の接続関連の状態が原因で、Cisco ISE ソフトウェア DVD を使用して Cisco ISE アプライアンスを起動しようとしたときに問題が発生する場合があることを理解しておいてください。

- ターミナル サーバにシリアル コンソールから Cisco ISE アプライアンスへの *exec* に設定された接続が関連付けられている。これを *no exec* に設定すると、KVM 接続およびシリアル コンソール接続を使用できるようになります。
- 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 Client コンソール接続のいずれかの場合があります）。
- 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。

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　Cisco ISE ソフトウェア DVD を挿入します。

ステップ 3　DVD から起動するように Cisco ISE アプライアンスをリブートします。

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 4　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** を入力し、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 5　表 7-1 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 7-1　　パスワード リセット パラメータ

パラメータ	説明
Admin username	パスワードをリセットする管理者の番号を入力します。
Password	新しいパスワードを入力します。
Verify password	再度パスワードを入力します。
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]:
```

詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2*（*Cisco Identity Services Engine CLI リファレンス ガイド リリース 1.2*）』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リセット

管理者が、誤ったパスワードをアカウントが無効になる所定の回数入力する場合があります。デフォルトの最小試行回数は 5 です。

（注）　管理者ユーザ インターフェイス パスワードをリセットするには、次のコマンドを使用します。このコマンドは、管理者の CLI のパスワードには影響を与えません。

ステップ 1　ダイレクト コンソール CLI にアクセスして、次を入力します。

application reset-passwd ise *administrator_ID*

ステップ 2　この管理者 ID に使用されていた前の 2 つのパスワードと異なる新しいパスワードを指定して、確認します。

```
Enter new password:
Confirm new password:

Password reset successfully
```

正常に管理者パスワードをリセットすると、クレデンシャルはただちにアクティブになり、システムをリブートせずにログインできます。

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 1.2*（*Cisco Identity Services Engine CLI リファレンス ガイド リリース 1.2*）』を参照してください。

Cisco ISE アプライアンスの IP アドレスの変更

Cisco SNS-3400 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。

はじめる前に

IP アドレスを変更する前に、Cisco ISE ノードがスタンドアロン状態であることを確認します。ノードが分散導入環境の一部である場合は、その環境からノードを登録解除して、スタンドアロン ノードにします。

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。

configure 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際に **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 システムの設定

Cisco ISE の Web ベースのユーザ インターフェイスのメニューおよびオプションを使用して、Cisco ISE システムをニーズに合わせて設定できます。認証および認証ポリシーの設定、および他の機能、メニュー、およびオプションの詳細については、『*Cisco Identity Services Engine User Guide, Release 1.2*（*Cisco Identity Services Engine ユーザ ガイド リリース 1.2*）』を参照してください。

Cisco ISE の操作およびモニタリング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 1.2（Cisco Identity Services Engine ユーザ ガイド リリース 1.2）*』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 1.2（Cisco Identity Service Engine のリリース ノート リリース 1.2）*』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 をインストールした後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有効にすることができます（システム診断についてのレポートを行うロギング機能は、デフォルトでは Cisco ISE で有効になっていません）。

システム診断レポートを有効にするには、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。

a. **configure terminal**

b. **logging 127.0.0.1:20514**

c. **end**

d. **write memory**

Cisco ISEユーザ インターフェイス（**[Administration（管理）] > [System（システム）] > [Logging（ロギング）] > [Logging Categories（ロギングのカテゴリ）] > [System Diagnostics（システム診断）]**）からシステム診断設定を指定できます。

ラックへの Cisco SNS-3400 シリーズ アプライアンスの設置

この付録では、Cisco SNS-3400 シリーズ アプライアンスを設置する前に確認する必要がある、安全に関する注意事項、設置場所の要件、およびガイドラインについて説明します。また、Cisco SNS-3400 シリーズ アプライアンスをラック マウントする方法、すべてのケーブルを接続する方法、アプライアンスの電源投入方法、およびサーバ コンポーネントを削除または交換する方法についても説明します。

この付録の内容は、次のとおりです。

サーバの開梱と点検

この項では、Cisco SNS-3400 シリーズ アプライアンスを安全に設置するために場所を準備する方法について説明します。

注意 内部サーバのコンポーネントを取り扱うときは、静電気防止用ストラップを着用し、常にモジュールのフレームの端を持つようにしてください。

ヒント サーバの輸送が必要となる場合に備えて、輸送用の箱は保管しておいてください。

（注） シャーシは厳密に検査したうえで出荷されています。輸送中の破損や内容品の不足がある場合には、ただちにカスタマー サービス担当者に連絡してください。

梱包内容を確認する手順は、次のとおりです。

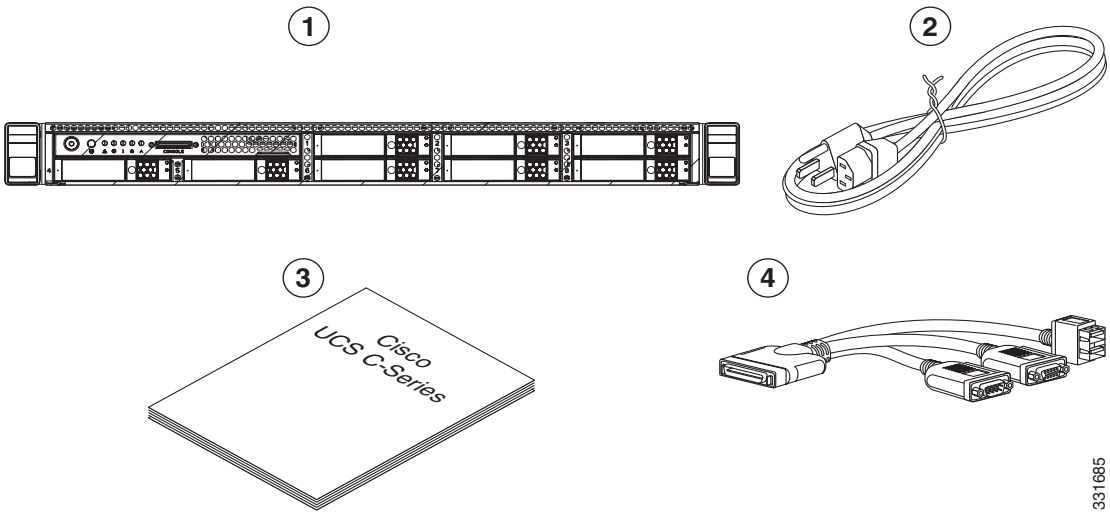
ステップ 1　段ボール箱からサーバを取り出します。梱包材はすべて保管しておいてください。

ステップ 2　カスタマー サービス担当者から提供された機器リストおよび図 A-1 と、梱包品の内容を照合します。すべての品目が揃っていることを確認してください。

ステップ 3　破損の有無を調べ、内容品の間違いや破損がある場合には、カスタマー サービス担当者に連絡してください。次の情報を用意しておきます。

- 発送元の請求書番号（梱包明細を参照）
- 破損している装置のモデルとシリアル番号
- 破損状態の説明
- 破損による設置への影響

図 A-1　　梱包内容



1	サーバ	3	マニュアル
2	電源コード（オプション、最大 2 本）	4	KVM ケーブル

安全に関する注意事項

（注）　Cisco SNS-3400 シリーズ アプライアンスの設置、操作、手入れを行う前に、安全上の重要事項について、*Cisco SNS 3400 シリーズ アプライアンスに関する法規制の遵守と安全についての情報*を確認してください。

警告　**安全上の重要事項**

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。警告の各国語版については、各警告文の末尾に提示されているステートメント番号を使用して、この機器に付属している各国語で記述された安全上の警告を参照してください。
ステートメント 1071

警告　**システムの過熱を防ぐため、最大推奨周囲温度の 40° C （104° F）を超えるエリアで操作しないでください。**
ステートメント 1047

警告　**いつでも装置の電源を切断できるように、プラグおよびソケットにすぐ手が届く状態にしておいてください。**
ステートメント 1019

警告　**この製品は、設置する建物にショート（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。この保護装置の定格が 250 V、15 A 以下であることを確認します。**
ステートメント　1005

警告　**装置は地域および国の電気規則に従って設置する必要があります。**
ステートメント　1074

サーバを設置する際には、次のガイドラインに従ってください。

- サーバを設置する前に、設置場所の構成を計画し、設置環境を整えます。設置場所を計画する際に推奨される作業については、『*Cisco UCS Site Preparation Guide*』を参照してください。
- サーバの周囲に、保守作業および適切な通気のための十分なスペースがあることを確認します。サーバ内では前面から背面へ空気が流れます。
- 空調が、付録 B「Cisco SNS-3400 シリーズ サーバの仕様」に記載された温度要件に適合していることを確認します。
- キャビネットまたはラックが、「ラックに関する要件」（P.A-4）に記載された要件に適合していることを確認します。
- 設置場所の電力が付録 B「Cisco SNS-3400 シリーズ サーバの仕様」に記載されている電力要件を満たしていることを確認します。可能な場合は、電力障害から保護するために、無停電電源装置（UPS）を使用できます。

注意　鉄共振テクノロジーを使用する UPS タイプは使用しないでください。このタイプの UPS は、データ トラフィック パターンの変化によって入力電流が大きく変動する可能性がある Cisco SNS 3400 シリーズ アプライアンスなどのシステムに使用すると、動作が不安定になる可能性があります。

ラックへの Cisco SNS-3400 シリーズのアプライアンスの設置

この項では、ラックに ISE 3400 シリーズ アプライアンスを設置する方法について説明します。また、次のトピックが含まれています。

ラックに関する要件

次は、標準的なオープン ラックに関する要件です。

- 標準 19 インチ （48.3 cm）幅 4 支柱 EIA ラック、ANSI/EIA-310-D-1992 のセクション 1 に準拠した英国ユニバーサル ピッチに適合するマウント支柱付き。
- 付属のスライド レールを使用する場合、ラック支柱の穴は、0.38 インチ（9.6 mm）の正方形、0.28 インチ（7.1 mm）の丸形、#12-24 UNC、または #10-32 UNC になります。
- サーバあたりの縦方向の最小ラック スペースは、1 RU、つまり 1.75 インチ （44.45 mm）である必要があります。

機器の要件

このサーバ用にシスコから提供されるスライド レールの場合、設置に必要な工具はありません。内側のレール（取り付けブラケット）が、サーバの側面にあらかじめ取り付けられています。

スライド レールの調整範囲

このサーバのスライド レールの調整範囲は 24 ～ 36 インチ（610 ～ 914 mm）です。

ラックへのサーバの設置

ここでは、ラックにサーバを設置する方法について説明します。

警告　**ラックへのユニットの設置や、ラック内のユニットの保守作業を行う場合は、負傷事故を防ぐため、システムが安定した状態で置かれていることを十分に確認してください。安全を確保するために、次のガイドラインを守ってください。**
ラックに設置する装置が 1 台だけの場合は、ラックの一番下に取り付けます。
ラックに複数の装置を設置する場合は、最も重い装置を一番下に設置して、下から順番に取り付けます。
ラックにスタビライザが付いている場合は、スタビライザを取り付けてから、ラックに装置を設置したり、ラック内の装置を保守したりしてください。ステートメント 1006

スライド レールとサーバをラックに取り付けるには、次の手順に従います。

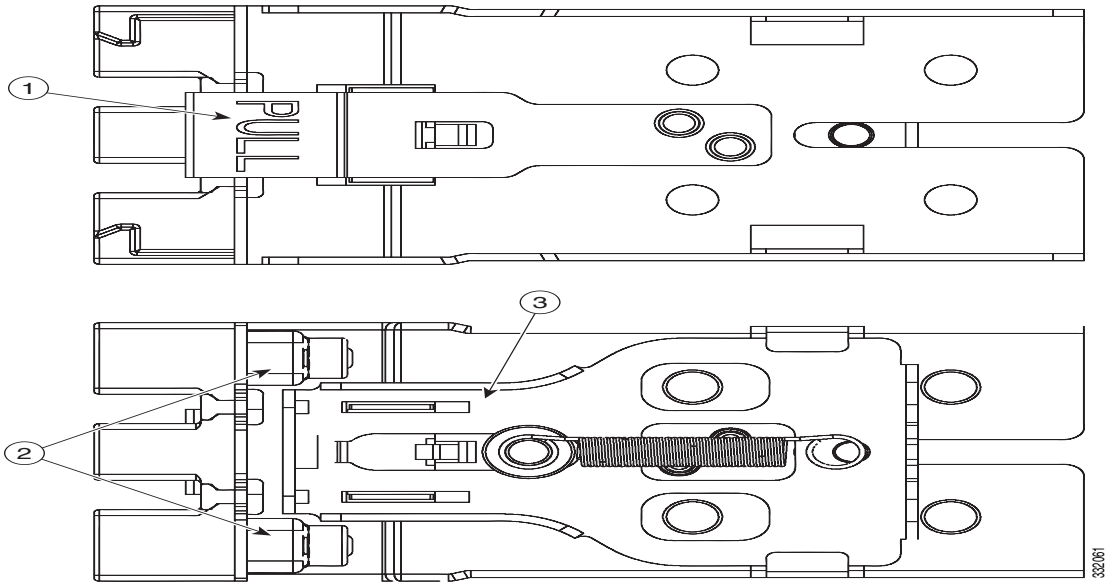
ステップ 1　前面側の固定ラッチを開きます（図 A-2 を参照）。スライド レール部品の「FRONT」のマークの付いた端部に、バネ仕掛けの固定ラッチがあります。取り付けペグをラック支柱の穴に挿入する前に、この固定ラッチが開いている必要があります。

a. 固定ラッチ部品の背面側で、「PULL」のマークの付いたクリップを開いた状態に維持します。

b. バネ仕掛けの固定ラッチを取り付けペグから離れる方向にスライドさせます。

c. 開位置で「PULL」クリップを解放して固定ラッチをロックします。

図 A-2　　前面側の固定ラッチ



1	部品の背面にある「PULL」のマークの付いたクリップ	**3**	部品の前面にあるバネ仕掛けの固定ラッチ
2	前面側の取り付けペグ		

ステップ 2　次のようにして、スライド レールをラックに取り付けます。

a. 左側の 2 本のラック支柱の内側でスライド レール部品の位置を合わせます（図 A-3 を参照）。

スライド レール部品上の「FRONT」および「REAR」のマークを使用して、ラックの前後の支柱の向きに部品を正しく合わせます。

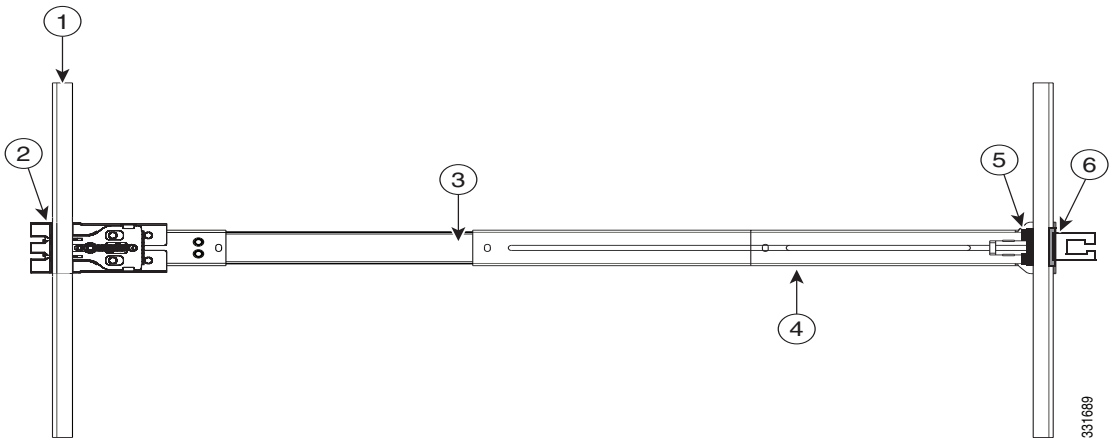
b. 前面側のラック支柱の目的の穴に前面から入るように、前面側の取り付けペグの位置を合わせます。

（注）　ラック支柱の穴を通る取り付けペグは、丸形または正方形の穴か、より小さい #10-32 の丸形の穴（取り付けペグの圧縮時）に適合するように設計されています。ラックに #10-32 のラック支柱の穴がある場合は、取り付けペグをそれらの穴の位置に合わせてから、バネ仕掛けのペグを圧縮して内側の #10-32 ペグを露出させます。

c. 取り付けペグがラックの後側の支柱の目的の穴にはまるまで、長さ調整ブラケットを伸ばします。

穴に背面側の取り付けペグを挿入する際、背面の固定ラッチを指で開いたままにします。ラッチを放すと、ラックの支柱が巻き込まれ、スライド レール部品が固定されます。

図 A-3　　スライド レール部品の取り付け



1	左前側ラック支柱	**4**	長さ調整ブラケット
2	前面側の取り付けペグ	**5**	背面側の取り付けペグ
3	スライド レール部品	**6**	背面側の固定ラッチ

d. 2 つ目のスライド レール部品を、ラックの反対側に取り付けます。2 つのスライド レール部品が水平で同じ高さになっていることを確かめます。

e. 所定の位置に収まって留まるまで、各部品の内側のスライド レールをラック前方へ引き出します。

ステップ 3　サーバを次のようにスライド レールに装着します。

（注）　内側のレールは、工場出荷時にあらかじめサーバの側面に取り付けられています。内側のレールが損傷したり、失われたりした場合は、交換用の内側レールを発注できます（Cisco PID UCSC-RAIL1-I）。

a. サーバ側面に事前に取り付けられた内側のレールを、空のスライド レールの前側に合わせます。

b. 内部の停止位置に収まるまで、サーバをスライド レールに押し込みます。

c. プラスチック製の解除クリップ（「PUSH」のラベルのついた）を内側の各レールに押し込み、次に、全面側のラッチがラック支柱に差し込まれるまでサーバをラックに押し込みます。

ステップ 4　（オプションの）ケーブル マネジメント アーム（CMA）をスライド レールの後ろ側に取り付けます。

（注）　CMA は、右側と左側のどちらのスライド レールにも取り付けられます。次の手順では、サーバの背面から見て、右側のスライド レールの後部に取り付ける方法について説明します。

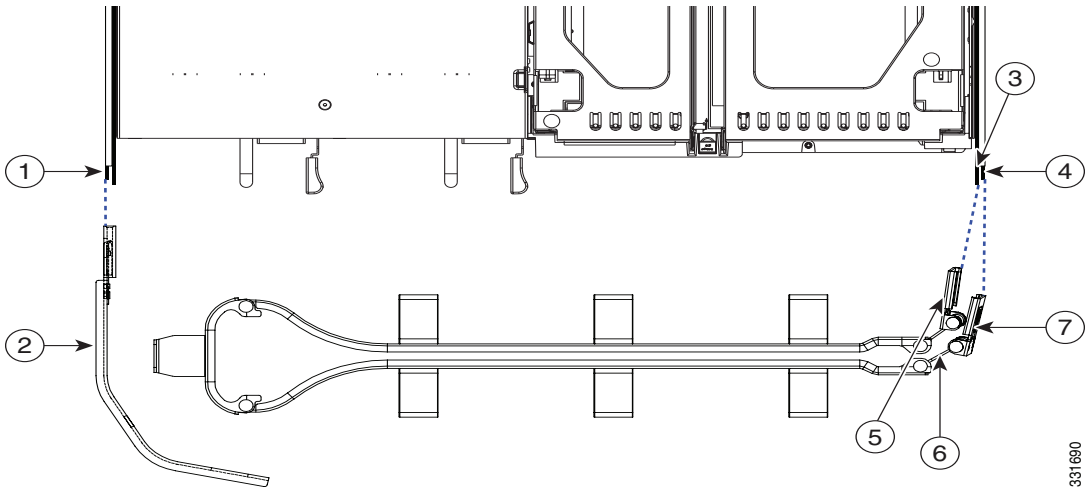
a. 内側の CMA アーム上のプラスチック製クリップを、サーバの側面にある取り付けブラケットのフランジ上でスライドさせます。図 A-4を参照してください。

（注）　CMA を取り付けるスライド レールが左側と右側のどちらにあるかに関係なく、必ず「UP」のマークが CMA の上側になるように注意してください。図 A-4を参照してください。

b. 外側の CMA アーム上のプラスチック製クリップを、スライド レールのフランジ上でスライドさせます。図 A-4を参照してください。

c. CMA 固定ブラケットを左側のスライド レールに取り付けます。ブラケット上のプラスチック製クリップを、左側のスライド レールの端部にあるフランジ上でスライドさせます。図 A-4を参照してください。

図 A-4　　ケーブル マネジメント アームの取り付け（サーバの後部）



1	外側の左側スライド レールの後部にあるフランジ	5	内側 CMA アームの取り付けクリップ
2	CMA 固定ブラケット	6	「UP」の方向マーク
3	右側の取り付けブラケットの後部にあるフランジ	7	外側 CMA アームの取り付けクリップ
4	外側の右側スライド レールの後部にあるフランジ		

ステップ 5　「CIMC を使用した Cisco SNS-3400 シリーズ アプライアンスでの リリース 1.2 の設定」（P.3-9）に進みます。

サーバの接続と電源投入

この項では、サーバの電源をオンにして、サーバに接続するための IP アドレスを割り当てる方法について説明します。このサーバにはあらかじめ *Shared LOM* というデフォルトの NIC モードが設定されています。デフォルトの NIC 冗長化は active-active で、DHCP はイネーブルです。Shared LOM モードでは、2 つの 1 Gb イーサネット ポートが Cisco Integrated Management Interface（CIMC）にアクセスできます。1 Gb イーサネット専用管理ポート、または Cisco UCS P81E 仮想インターフェイス カード（VIC）のポートを使用して CIMC にアクセスする場合は、次の手順のステップ 3 の説明に従って、まずサーバに接続して NIC モードを変更する必要があります。このステップでは、NIC 冗長化を変更し、スタティック IP 設定を設定することもできます。

サーバの初期設定を実行する手順は、次のとおりです。

ステップ 1　付属の電源コードをサーバの各電源装置に接続し、次に、接地された AC 電源出力に接続します。電源の仕様については、「電力仕様」（P.B-2）を参照してください。

最初のブート中、サーバがスタンバイ電源でブートするまでに約 2 分かかります。

電源ステータスは、次のように電源ステータス LED で確認できます。

- 消灯：サーバには AC 電力が供給されていません。
- オレンジ：サーバはスタンバイ電源モードです。CIMC と一部のマザーボード機能にだけ電力が供給されています。
- 緑：サーバは主電源モードです。すべてのサーバ コンポーネントに電力が供給されています。

（注）　サーバはブートアップ時に、サーバに取り付けられている各 USB デバイスに対して 1 度ビープ音を鳴らします。外部の USB デバイスが取り付けられていない場合でも、仮想フロッピーディスク、CD/DVD ドライブ、キーボード、またはマウスなどの各仮想 USB デバイスに対して短いビープ音が鳴ります。BIOS 電源投入時自己診断テスト（POST）時に USB デバイスをホットプラグまたはホットアンプラグした場合、または、BIOS セットアップ ユーティリティや EFI シェルにアクセスしている間にもビープ音が鳴ります。

ステップ 2　前面パネルの KVM コネクタに接続されている付属の KVM ケーブルを使用して USB キーボードと VGA モニタを接続します。

（注）　または、背面パネルの VGA および USB ポートを使用することもできます。ただし、前面パネルの VGA と背面パネルの VGA は同時に使用できません。1 つの VGA コネクタに接続している場合に、反対側のコネクタにビデオ デバイスを接続すると、最初の VGA コネクタがディセーブルになります。

LED の確認

Cisco SNS-3400 シリーズ アプライアンスが起動して動作中のときに、前面パネルおよび背面パネルの LED の状態を確認します。次のトピックでは、LED の色、電源状態、アクティビティ、および Cisco SNS 3400 シリーズ アプライアンスについて表示される重要なステータス インジケータについて説明します。

前面パネルの LED およびボタン

表 A-1　　前面パネルの LED の状態

LED 名	状態
電源ボタン/電源ステータス LED	• 消灯：サーバに AC 電力が供給されていません。 • オレンジ：サーバはスタンバイ電源モードです。CIMC と一部のマザーボード機能にだけ電力が供給されています。 • 緑：サーバは主電源モードです。すべてのサーバ コンポーネントに電力が供給されています。
ID	• 消灯：ID LED は使用されていません。 • 青：ID LED がアクティブです。
システム ステータス	• 緑：サーバは正常動作状態で稼働しています。 • 緑の点滅：サーバはシステムの初期化とメモリ チェックを行っています。 • オレンジの点灯：サーバは、運用サービス低下状態になっており、次のいずれかが原因の可能性があります。 – 電源装置の冗長性が失われている。 – CPU が一致しない。 – 少なくとも 1 つの CPU に障害が発生している。 – 少なくとも 1 つの DIMM に障害が発生している。 – RAID 構成内の少なくとも 1 台のドライブに障害が発生している。 • オレンジの点滅：サーバは重大な障害が発生している状態であり、次のいずれかが原因の可能性があります。 – ブートに失敗した。 – 修復不能な CPU またはバス エラーが検出された。 – サーバが過熱状態にある。
ファン ステータス	• 緑：すべてのファン モジュールが正常に動作中です。 • オレンジの点灯：1 つのファン モジュールに障害が発生しています。 • オレンジの点滅：重大な障害。2 つ以上のファン モジュールに障害が発生しています。

表 A-1　前面パネルの LED の状態 （続き）

LED 名	状態
温度ステータス	• 緑：サーバは正常温度で稼働中です。 • オレンジの点灯：1 つ以上の温度センサーが警告しきい値を超過しています。 • オレンジの点滅：1 つ以上の温度センサーが重大しきい値を超過しています。
電源装置ステータス	• 緑：すべての電源装置が正常に動作中です。 • オレンジの点灯：1 台以上の電源装置が縮退運転状態にあります。 • オレンジの点滅：1 台以上の電源装置が重大な障害発生状態にあります。
ネットワーク リンク アクティビティ	• 消灯：イーサネット リンクがアイドル状態です。 • 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 • 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。
ハード ドライブ障害	• 消灯：ハード ドライブは正常に動作中です。 • オレンジ：ハード ドライブで障害が発生しています。 • オレンジの点滅：デバイスの再構成中です。
ハード ドライブ アクティビティ	• 消灯：ハード ドライブ スレッドにハード ドライブが存在しません（アクセスなし、障害なし）。 • 緑：ハード ドライブの準備が完了しています。 • 緑の点滅：ハード ドライブはデータの読み取り中または書き込み中です。

背面パネルの LED およびボタン

表 A-2　背面パネルの LED の状態

LED 名	状態
電源装置障害	• 消灯：電源装置は正常に動作中です。 • オレンジの点滅：イベント警告しきい値に達しましたが、電源装置は動作し続けています。 • オレンジの点灯：重大障害しきい値に達し、電源装置がシャットダウンしています（たとえば、ファンの障害や過熱状態など）。
電源装置 AC OK	• 消灯：電源装置に AC 電力が供給されていません。 • 緑の点滅：AC 電力の供給は OK、DC 出力は使用不可。 • 緑の点灯：AC 電力供給も、DC 出力も OK。
1 Gb イーサネット専用管理リンク速度	• 消灯：リンク速度は 10 Mbps です。 • オレンジ：リンク速度は 100 Mbps です。 • 緑：リンク速度は 1 Gbps です。

表 A-2　背面パネルの LED の状態 （続き）

LED 名	状態
1 Gb イーサネット専用管理リンク ステータス	• 消灯：リンクが確立されていません。 • 緑：リンクはアクティブです。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。
1 GB イーサネット リンク速度	• 消灯：リンク速度は 10 Mbps です。 • オレンジ：リンク速度は 100 Mbps です。 • 緑：リンク速度は 1 Gbps です。
1 GB イーサネット リンク ステータス	• 消灯：リンクが確立されていません。 • 緑：リンクはアクティブです。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。
ID	• 消灯：ID LED は使用されていません。 • 青：ID LED がアクティブです。

サーバ コンポーネントの取り付けまたは交換

Cisco SNS 3415 または 3495 アプライアンス コンポーネントの取り付けおよび交換の方法については、『*Cisco UCS C220 Server Installation and Service Guide（Cisco UCS C220 サーバ インストールおよびサービス ガイド）*』を参照してください。

Cisco SNS-3400 シリーズ サーバの仕様

この付録では、サーバの技術仕様について説明します。内容は次のとおりです。

物理的仕様

表 B-1 に、サーバの物理的仕様を示します。

表 B-1　Cisco SNS-3400 シリーズ サーバの物理仕様

説明	仕様
高さ	1.7 インチ （4.3 cm）
幅	16.9 インチ （42.9 cm）
奥行	28.5 インチ （72.4 cm）
重量（フル装備シャーシ）	35.6 ポンド （16.1 kg）

環境仕様

表 B-2 に、サーバの環境仕様を示します。

表 B-2　Cisco SNS-3400 シリーズ サーバの環境仕様

説明	仕様
動作時温度	41～104 °F（5 ～ 40 °C） 海抜 305 m ごとに最高温度が 1 ℃ 低下。
非動作時温度	–40 ～ 149°F（–40 ～ 65°C）
湿度（RH）、結露なし	10 ～ 90 %
動作時高度	0 ～ 10,000 フィート
非動作時高度	0 ～ 40,000 フィート

表 B-2　Cisco SNS-3400 シリーズ サーバの環境仕様 （続き）

説明	仕様
音響出力レベル ISO7779 に基づく A 特性音響出力レベル LwAd（Bels）を測定 73°F （23°C）で動作	5.4
騒音レベル ISO7779 に基づく A 特性音圧レベル LpAm（dBA）を測定 73°F （23°C）で動作	37

電力仕様

2 つの電源オプションの電源仕様を次に示します。

- 「450 ワットの電源」（P.B-2）
- 「650 ワットの電源」（P.B-3）

Cisco UCS Power Calculator を使用すると、ご使用のサーバ設定の電源に関する詳細情報を取得できます。

（注）　サーバ内で異なるタイプの電源装置を組み合わせて使用しないでください。電源装置は、両方とも 450 W、あるいは 650 W にする必要があります。

450 ワットの電源

表 B-3 に、各 450W 電源装置の仕様を示します（Cisco 部品番号 UCSC-PSU-450W）。

表 B-3　Cisco SNS-3400 シリーズ サーバの 450 ワットの電源仕様

説明	仕様
AC 入力電圧範囲	低範囲：100 VAC ～ 120 VAC 高範囲：200 VAC ～ 240 VAC
AC 入力周波数	範囲：47 ～ 63 Hz（単相、公称 50 ～ 60Hz）
AC 回線入力電流（定常ステート）	6.0 A（100 VAC で最大） 3.0 A（208 VAC で最大）
各電源装置の最大出力電力	450 ワット
電源装置の出力電圧	主電源：12 VDC スタンバイ電源：12 VDC

650 ワットの電源

表 B-4 に、各 650 W 電源装置の仕様を示します（Cisco 部品番号 UCSC-PSU-650W）。

表 B-4　Cisco SNS-3400 シリーズ サーバの 650 ワットの電源仕様

説明	仕様
AC 入力電圧範囲	90 ～ 264 VAC（自己調整、公称 180 ～ 264 VAC）
AC 入力周波数	範囲：47 ～ 63 Hz（単相、公称 50 ～ 60Hz）
AC 回線入力電流（定常ステート）	7.6 A（100 VAC で最大） 3.65 A（208 VAC で最大）
各電源装置の最大出力電力	650 ワット
電源装置の出力電圧	主電源：12 VDC スタンバイ電源：12 VDC

Cisco SNS-3400 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、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 C-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、特定のポートに関連する情報（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）を説明します。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。このポートのリストは、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。

- Cisco ISE 管理は、ギガビット イーサネット 0 に制限されます。
- RADIUS はすべてのネットワーク インターフェイス カード（NIC）でリッスンします。
- すべての NIC が IP アドレスを使用して設定できます。

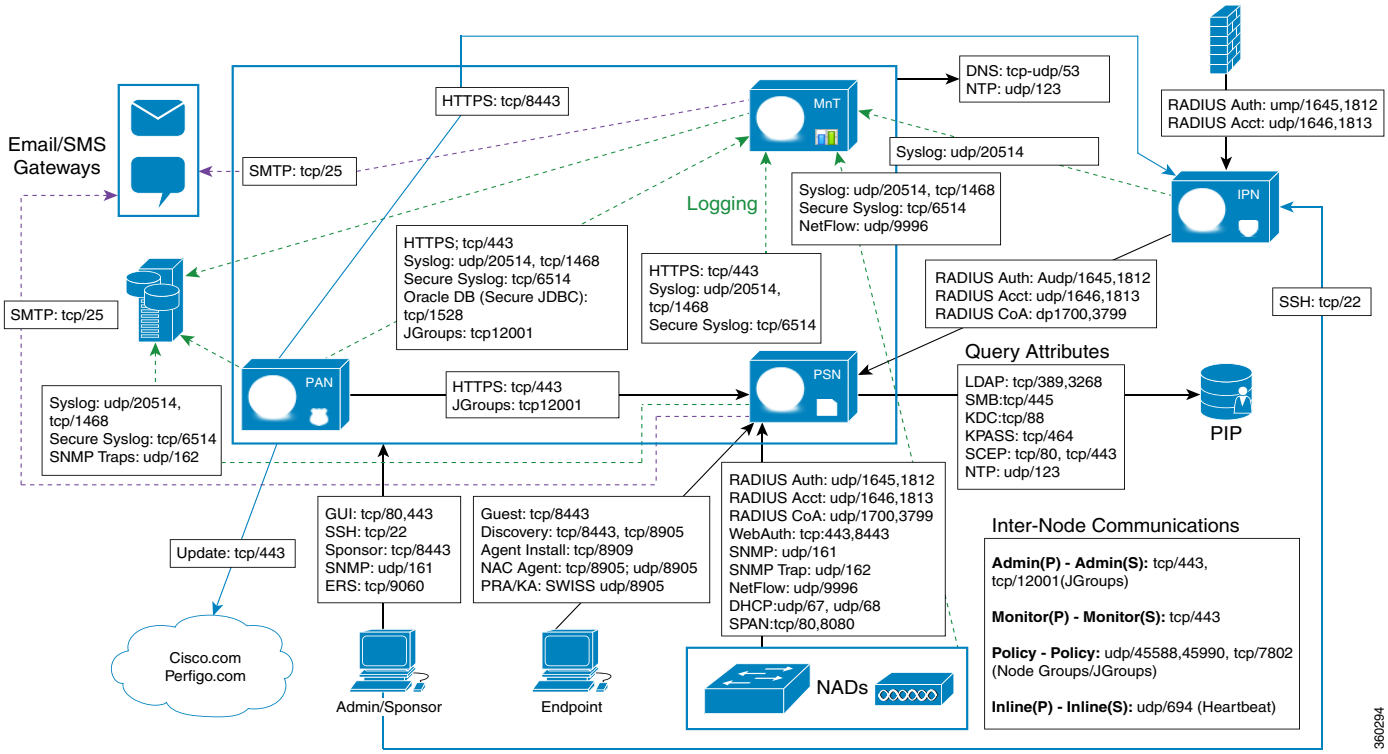


表 C-1　Cisco ISE のサービスとポート

Cisco ISE ノード	Cisco 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
管理ノード	管理機能	• TCP：22（セキュア シェル [SSH] サーバ） • TCP：80[1]（HTTP） • TCP：443[1]（HTTPS） • TCP：9060（外部 RESTful サービス（ERS）REST API） **（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、デフォルトで有効になっています。	Cisco ISE 管理は、ギガビット イーサネット 0 に制限されます。	Cisco ISE 管理は、ギガビット イーサネット 0 に制限されます。	Cisco ISE 管理は、ギガビット イーサネット 0 に制限されます。
	複製および同期	• TCP：443（HTTPS SOAP） • TCP：12001 グローバル（JGroups：データ同期/データレプリケーション）	—	—	—
	モニタリング	• 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。	—	—	—

表 C-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	Cisco 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
	ロギング（アウトバウンド）	• UDP：20514、TCP：1468（Syslog） • TCP：6514（セキュア Syslog） **（注）** デフォルト ポートは外部ロギング用に設定できます。 • UDP：162（SNMP トラップ）：			
	外部 ID ストアおよびリソース	• TCP：389、3268、UDP：389（LDAP） • TCP：445（SMB） • TCP：88、UDP：88（KDC） • TCP：464（KPASS） • UDP：123（NTP） • TCP：53、UDP：53（DNS） （管理ユーザ インターフェイス認証）	—	—	—

表 C-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	Cisco 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 ノード	管理機能	• TCP：22（SSH サーバ） • TCP：80[1]（HTTP） • TCP：443[1]（HTTPS）	—	—	—
	複製および同期	• TCP：443（HTTPS SOAP） • TCP：1528（セキュア JDBC：Oracle DB リスナー） • TCP：12001 グローバル（JGroups：データ同期/データ レプリケーション）	• TCP：1528（セキュア JDBC：Oracle DB リスナー）	• TCP：1528（セキュア JDBC：Oracle DB リスナー）	• TCP：1528（セキュア JDBC：Oracle DB リスナー）
	モニタリング	• UDP：161（SNMP） **（注）** このポートは、ルート テーブルによって異なります。			
	ロギング	• UDP：20514、TCP：1468（Syslog） • TCP：6514（セキュア Syslog） **（注）** デフォルト ポートは外部ロギング用に設定できます。 • TCP：25（SMTP） • UDP：162（SNMPトラップ）			
	外部リソース	• TCP：389、3268、UDP：389（LDAP） • TCP：445（SMB） • TCP：88、UDP：88（KDC） • TCP：464（KPASS） • UDP：123（NTP） • TCP：53、UDP：53（DNS） (管理ユーザ インターフェイス認証)	—	—	—

表 C-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	Cisco 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 ノード	管理機能	• TCP：22（SSH サーバ） • TCP：80[1]（HTTP） • TCP：443[1]（HTTPS）	—	—	—
	複製および同期	• TCP：443（HTTPS SOAP） • TCP：12001 グローバル（JGroups：データ同期/データ レプリケーション）	—	—	—
	クラスタリング（ノード グループ）	• UDP：45588、45590（ローカル JGroup） • TCP：7802（JGroup のローカル障害検出）	—	—	—
	モニタリング	• UDP：161（SNMP） **（注）** このポートは、ルート テーブルによって異なります。	—	—	—
	ロギング（アウトバウンド）	• UDP：20514、TCP：1468（Syslog） • TCP：6514（セキュア Syslog） **（注）** デフォルト ポートは外部ロギング用に設定できます。 • UDP：162（SNMPトラップ）			
	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 （RADIUS 認可変更の送信） • UDP：1700、3799（RADIUS 認可変更のリッスン/リレー） **（注）** UDP ポート 3799 は設定できません。			

表 C-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	Cisco 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 ノード（続き）	外部 ID ストアおよびリソース	• TCP：389、3268（LDAP） • TCP：445（SMB） • TCP 88（KDC） • TCP：464（KPASS） • UDP：123（NTP） • UDP: 53（DNS） (管理ユーザ インターフェイス認証およびエンドポイント認証)	—	—	—
	Web ポータル サービス： - ゲスト/Web 認証 - ゲスト スポンサー ポータル - デバイス ポータル - クライアントのプロビジョニング - ポータルのブラックリスト化	• HTTPS（インターフェイスは Cisco ISE のサービスに対して有効にする必要があります)。 • TCP: 8000-8999（ゲスト ポータルおよびクライアントのプロビジョニング。デフォルト ポートは TCP：8443 です)。 • TCP：8000-8999 （スポンサー ポータル。デフォルト ポートは TCP：8443 です)。 • TCP：8000-8999 （デバイス ポータル。デフォルト ポートは TCP：8443 です)。 • TCP: 8000-8999 （ブラックリスト ポータル。デフォルト ポートは TCP：8444です)。 • TCP：25（SMTP 通知）			

表 C-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	Cisco 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 ノード（続き）	ポスチャ - 検出 - プロビジョニング - アセスメント/ハートビート	• TCP：80（HTTP）検出：クライアント側 • TCP：8905（HTTPS）検出：クライアント側 **（注）** デフォルトでは、TCP：80 は TCP：8443 にリダイレクトされます。「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」を参照してください。 • TCP：8443、8905（HTTPS）検出：ポリシー サービス ノード側 • URL リダイレクト：プロビジョニング。「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」を参照してください。 • ActiveX と Java アプレットのインストール（IP 更新を含む）、Web エージェント、および NAC エージェントのインストールの開始：プロビジョニング。次を参照してください。「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」 • TCP：8443 プロビジョニング：NAC Agent のインストール • UDP：8905（SWISS）プロビジョニング：NAC エージェントの更新通知 • TCP：8905（HTTPS）プロビジョニング: NAC エージェントおよびその他のパッケージ/モジュールの更新 • TCP：8905（HTTPS）アセスメント：ポスチャのネゴシエーションとエージェントのレポート • UDP：8905（SWISS）評価：PRA/キープアライブ			
	個人所有デバイスの持ち込み（BYOD）/ネットワーク サービス プロトコル - リダイレクト - プロビジョニング - SCEP	• URL リダイレクト：プロビジョニング。次を参照してください。「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」 • Active-X および Java アプレットのインストール（ウィザードのインストールの開始を含む）：プロビジョニング。次を参照してください。「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」 • TCP：8443 プロビジョニング：Cisco ISE からのウィザード インストール（Windows および Mac OS） • TCP：443 プロビジョニング：Google Play からのウィザード インストール（Android） • TCP：8905 プロビジョニング：サプリカントのプロビジョニング プロセス • TCP：80 または TCP：443 SCEP プロキシから CA（SCEP URL の設定に基づく）			
	モバイル デバイス管理（MDM）API の統合	• URL リダイレクト：次を参照してください。「Web ポータル サービス：ゲスト ポータルおよびクライアント プロビジョニング」 • API：ベンダー固有 • エージェントのインストールおよびデバイスの登録：ベンダー固有			

表 C-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	Cisco 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 ノード（続き）	プロファイル	• UDP：9996（NetFlow） **（注）** このポートは、設定可能です。 • UDP 67（DHCP） **（注）** このポートは、設定可能です。 • UDP：68（DHCP SPAN） • TCP：80、8080（HTTP） • NMAP は、ポート 0 ～ 65535[2] 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 C-1　Cisco ISE のサービスとポート （続き）

Cisco ISE ノード	Cisco 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
インライン ポスチャ ノード	管理機能	• TCP：22（SSH サーバ） • TCP：8443（HTTPS） **（注）** TCP：8443 は管理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） **（注）** UDP ポート 3799 は設定できません。 • TCP：9090（リダイレクト）	• 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） • RADIUS CoA：該当なし • TCP：9090（リダイレクト）	—	—
	ロギング	• UDP：20154（Syslog） **（注）** このポートは、設定可能です。	• UDP：20154（Syslog） **（注）** このポートは、設定可能です。	—	—
（注） インライン ポスチャのノードのハイ アベイラビリティは、他の Cisco ISE にノード タイプには適用されません。					
インライン ポスチャ ノード（続き）	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）

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ないため、このポートへのアクセスはありません。
2. 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。

OCSP および CRL に使用されるポート

上記の Cisco ISE サービスとポートの表には、Cisco ISE で使用される基本的なポートが記載されていますが、Online Certificate Status Protocol（OCSP）サービスおよび証明書失効リスト（CRL）の場合、ポートは CA サーバまたはサービスをホストしている OCSP/CRL によって異なります。

OCSP の場合、使用可能なデフォルト ポートは TCP 80/TCP 443 です。Cisco ISE 管理ポータルでは、OCSP サービス用の HTTP ベースの URL が予期されるため、TCP 80 がデフォルトです。デフォルト以外のポートも使用できます。

CRL の場合、デフォルトのプロトコルには、HTTP、HTTPS、および LDAP が含まれており、それぞれのデフォルト ポートは通常 80、443、および 389 になります。実際のポートは CRL サーバで設定されます。

詳細については、次の情報を参照してください。*OCSP サービス*および*証明書ストアの設定の編集*

Cisco ISE ライセンス

この章では、Cisco ISE で使用できるライセンスのメカニズムとスキーム、およびライセンスの追加やアップグレードを行う方法について説明します。

Cisco ISE のライセンス設定

Cisco ISE 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やアクセスを管理する機能を提供します。

ユーザが必要な機能を選択できるようにするために、Cisco ISE でのライセンス設定はきめ細かく行われます。シスコは、Base、Plus、おおび Advanced など、複数のライセンス パッケージを用意しています。

表 D-1　　Cisco ISE ライセンス パッケージ

ライセンス パッケージ	永久かサブスクリプションか	カバーされる ISE 機能	注意
Base	永久	• 基本的なネットワーク アクセス：AAA、IEEE-802.1X • ゲスト管理 • リンク暗号化（MACSec）	
Plus	サブスクリプション（1、3、または 5 年）	• 個人所有デバイスの持ち込み（BYOD） • プロファイル • エンドポイント保護サービス（EPS） • TrustSec SGT	Base サービスは含まれません。各 Plus ライセンスには、Base ライセンスがそれぞれ必要です。

表 D-1　Cisco ISE ライセンス パッケージ

ライセンス パッケージ	永久かサブスクリプションか	カバーされる ISE 機能	注意
Advanced	サブスクリプション（1、3、または 5 年）	• 個人所有デバイスの持ち込み（BYOD） • プロファイル • エンドポイント保護サービス（EPS） • TrustSec SGT • Mobile Device Manager（MDM） • ヘルス コンプライアンスと修復 • ポスチャ	Base サービスは含まれません。各 Advanced ライセンスには、Base ライセンスがそれぞれ必要です。Advanced ライセンスには、Plus ライセンスのすべての機能が含まれます。
Wireless	サブスクリプション（1、3、または 5 年）	Wireless ライセンスにより、ワイヤレス LAN 展開の Base および Advanced ライセンスの機能が有効になります。	Cisco 管理ノードで Base、Plus、Advanced のライセンスを共存させることはできません。
Wireless アップグレード	サブスクリプション（1、3、または 5 年）	Wireless アップグレード ライセンスにより、すべてのワイヤレスおよび非ワイヤレスのクライアント アクセス方式（有線および VPN コンセントレータ アクセスを含む）に対する Base および Advanced ライセンスの機能が有効になります。	Wireless アップグレード ライセンスは既存の Wireless ライセンスが存在する場合にのみインストールすることができます。
評価	一時（90 日）	完全な Cisco ISE 機能が、100 台のエンドポイントに対して提供されます。	プリセールスの顧客評価のための Cisco ISE 製品の限定的な使用。すべての Cisco ISE アプライアンスには、評価ライセンスが付属しています。

すべての Cisco ISE アプライアンスには 90 日間有効な評価ライセンスが付属しています。90 日間の評価期間の終了後に Cisco ISE サービスの使用を継続し、ネットワークで 100 を超える数の同時エンドポイントをサポートするには、システム上の現在のユーザの数の Base ライセンスを取得して登録する必要があります。追加機能が必要な場合は、該当の機能を有効にする Plus または Advanced のライセンスが必要です。

Cisco ISE ソフトウェアをインストールし、最初にアプライアンスをプライマリ管理ノードとして設定したら、Cisco ISE のライセンスを取得して、そのライセンスを登録する必要があります。

Cisco ISE では、2 つのハードウェア ID を使用するライセンスがサポートされます。プライマリおよびセカンダリ管理ノードのハードウェア ID に基づいてライセンスを取得できます。プライマリおよびセカンダリ管理ノードのハードウェア ID を使用して、Cisco ISE プライマリ管理ノードにすべてのライセンスを登録します。その後、プライマリ管理ノードは、導入環境に登録されているすべてのライセンスを集中管理します。

（注） Base ライセンスは常に必要です。ただし、Advanced ライセンスの取得に Plus ライセンスは必要ではなく、Plus ライセンスの取得にも Advanced ライセンスは必要ありません。

Base、Plus、Advanced ライセンスは同時にインストールすることを推奨します。

- デフォルトの評価ライセンスの上に Base ライセンスをインストールすると、Base ライセンスにより評価ライセンスの Base ライセンスに関連する部分のみがオーバーライドされ、デフォルトの残りの評価ライセンス期間中に使用できる Plus および Advanced ライセンスの機能が維持されます。
- 最初に Base ライセンスをインストールしないと、評価ライセンスを Plus または Advanced ライセンスにアップグレードすることができません。
- デフォルトの評価ライセンスの上に Wireless ライセンスをインストールすると、Wireless ライセンスにより、評価ライセンスのパラメータが Wireless ライセンスに関連付けられている特定の期間とユーザ カウントが上書きされます。

ライセンス カウント

Cisco ISE ユーザはアクティブ セッション中にライセンスを使用します。セッションが終了すると、ISE は、他のユーザが再利用できるようにライセンスを解放します。

Cisco ISE ライセンスは次のようにカウントされます。

- Base、Plus、または Advanced ライセンスは、使用している機能に基づいて使用されます。
- 複数のネットワーク接続があるエンドポイントは、MAC アドレスごとに複数のライセンスを使用する可能性があります。たとえば、有線で接続されたラップトップが、同時に無線でも接続している場合です。VPN 接続のライセンスは IP アドレスに基づきます。
- ライセンスは、同時のアクティブなセッションに対してカウントされます。アクティブなセッションとは、RADIUS アカウンティングの開始が受信されるが、RADIUS アカウンティングの停止が受信されていないセッションのことです。

（注） RADIUS のアクティビティのないセッションは、該当のエンドポイントがシステムから削除されていない場合、5 日ごとにアクティブ セッションのリストから自動的に削除されます。

サービスの中断を回避するために、Cisco ISE はライセンスの権限付与を超えたエンドポイントにサービスを提供し続けます。ただし、Cisco ISE は RADIUS アカウンティング機能を使用して、ネットワーク上の現在のエンドポイントを追跡し、エンドポイントの数がライセンスの数を超過すると、次のようにアラームを生成します。

- 80% Info
- 90% Warning
- 100% Critical

Cisco.com からの Cisco ISE ライセンスの取得

90 日間の評価期間の終了後に Cisco ISE サービスの使用を継続し、ネットワークで 100 を超える数の同時エンドポイントをサポートするには、Cisco ISE の Base、Plus、Advanced、または Wireless のライセンスを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 を購入したら、90 日間のライセンスの期限が切れる前に、Cisco.com のライセンス オプションを調べて、使用する Cisco ISE の導入に適したパッケージを発注できます。

ハイ アベイラビリティ ペアに 2 つの管理ノードを導入している場合、これらのノードがスタンドアロンまたはプライマリ ステートの間に、それぞれのノードに同じライセンスの機能があることを確認し、ライセンスを追加する必要があります。

Cisco.com からライセンス ファイルを注文して 1 時間以内に、シスコ補足エンド ユーザ ライセンス契約書および発注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 Web 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、次の具体的な情報を指定する必要があります。

- プライマリおよびセカンダリ管理ノードの両方の製品 ID（PID）
- バージョン ID（VID）
- シリアル番号（SN）
- PAK

詳細については、*Cisco Identity Services Engine のライセンスに関する注意*を参照してください。

シスコ製品ライセンス登録 Web 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が送信されます。このライセンス ファイルをローカル マシンの既知の場所に保存し、「ライセンスの追加またはアップブレード」（P.D-5）の指示に従って、Cisco ISE に任意の製品ライセンスを追加したり、更新したりします。

詳細情報および Cisco ISE で使用できるライセンス部品番号については（新規インストールのライセンス設定オプションや、Cisco Secure Access Control Server など、既存のシスコのセキュリティ製品からの移行についての情報を含む）、以下の URL にある Cisco Identity Services Engine の発注ガイドラインを参照してください。http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/guide_c07-656177.html。

関連項目

- 「CLI を使用したハードウェア ID の確認」（P.D-4）
- 「管理ポータルを使用したハードウェア ID の確認」（P.D-5）

CLI を使用したハードウェア ID の確認

Cisco ISE ライセンスは、MAC アドレスではなく、管理ノードのハードウェア ID に基づいて生成されます。

ハードウェア ID を確認するには、Cisco ISE のダイレクト コンソール CLI にアクセスし、**show inventory** コマンドを入力します。出力には次のように、PID、VID、および SN を示す行が含まれています。

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

管理ポータルを使用したハードウェア ID の確認

Cisco ISE ライセンスは、MAC アドレスではなく、管理ノードのハードウェア ID に基づいて生成されます。

現在のライセンスが期限切れになっていない場合は、次の手順に従って管理ノードのハードウェア ID を表示できます。

ステップ 1　Cisco ISE 管理インターフェイスから、**[Administration（管理）] > [System（システム）] > [Licensing（ライセンス）]** を選択します。

ステップ 2　[ライセンスの操作（ライセンスのオプション）] ナビゲーション ペインで **[Current Licenses（現在のライセンス）]** をクリックします。

ステップ 3　管理ノードのハードウェア ID を確認する Cisco ISE ノードに対応するボタンを選択し、**[Administration Node（管理ノード）]** をクリックして、PID、VID、および SN を表示します。

ライセンスの追加またはアップブレード

ライセンスを追加できるのは、スタンドアロンまたはプライマリの管理ノードのみです。既存の評価ライセンスは、90 日の評価期間の期限が切れたとき、またはその前にアップグレードできます。評価ライセンスをアップグレードするか、または置き換えるには、2 つの方法があります。

- Base ライセンスをインストールしてから、Plus または Advanced ライセンスもインストールするかどうかを選択する
- Wireless ライセンスをインストールする

複数のネットワーク接続を使用する単一のエンドポイントは、複数の Base、Plus、または Advanced ライセンスを使用する可能性があります。この状況は、エンドポイントが有線および無線の両方のネットワーク接続を使用する場合に発生する可能性があります。固有の認証された接続には、それぞれ独自のライセンスが必要です。

はじめる前に

適切なライセンスを取得し、そのライセンスを Cisco ISE ノードにインストールしたことを確認します。詳細については、「Cisco.com からの Cisco ISE ライセンスの取得」（P.D-4）を参照してください。

ステップ 1　Cisco ISE 管理インターフェイスから、**[Administration（管理）] > [System（システム）] > [Licensing（ライセンス）] > [Current Licenses（現在のライセンス）]** を選択します。

ステップ 2　アップグレードするライセンス名の隣のオプション ボタンをクリックし、**[Edit（編集）]** をクリックします。

ステップ 3　**[Add Services（サービスの追加）]** をクリックします。

ステップ 4　**[Browse（参照）]** をクリックして、該当のライセンス ファイルを選択します。

ステップ 5　**[Import（インポート）]** をクリックして、追加したサービスをサポートする新しいライセンス ファイルをインポートします。

ステップ 6 [Current Licenses（現在のライセンス）] ページに戻り、アップグレードされたライセンスが追加されていることを確認します。さらに確認するには、ライセンスがアップグレードされた各サービスの機能を確認します。

（注） [Current Licenses（現在のライセンス）] ページに、インストールされている Plus および Advanced ライセンスの数が、Advance/Plus の合算として表示されます。たとえば、500 の Plus ライセンスと 1000 の Advanced ライセンスをがある場合、Advance/Plus の数は 1500 となります。

関連項目

- 「ライセンスの削除」（P.D-6）

ライセンスの削除

Base、Plus、Advanced、および Wireless ライセンスは個別に削除できますが、次の条件に注意する必要があります。

- Plus または Advanced ライセンスの数が Base ライセンスの数を超えている場合、Base ライセンスは削除できません。
- 組み合わされたライセンスをインストールした場合は、Base および Advanced パッケージの関連インストールがすべて削除されます。
- 標準の 90 日間の評価期間内に実稼働レベルのライセンスを削除した場合、実稼働ライセンスが削除されると、評価ライセンスが自動的に復元されます。
- 評価ライセンスは削除できません。

はじめる前に

Wireless ライセンスの後に Wireless アップグレード ライセンスをインストールした場合は、Wireless アップグレード ライセンスを削除してから基盤となる Wireless ライセンスを削除する必要があります。

ステップ 1 **[Administration（管理）] > [System（システム）] > [Licensing（ライセンス）] > [Current Licenses（現在のライセンス）]** を選択します。

ステップ 2 ノード名の隣にあるオプション ボタンをクリックして **[Edit（編集）]** をクリックします。

ステップ 3 削除するライセンス名の隣のオプション ボタンをクリックし、**[Remove（削除）]** をクリックします。

ステップ 4 **[OK]** をクリックします。

Cisco ISE での証明書の管理

証明書は、ネットワークに対するセキュアなアクセスを提供するために使用されます。また、証明書はエンドポイントに対して Cisco ISE を識別するため、そして、そのエンドポイントと Cisco ISE ノード間の通信のを保護するために使用されます。証明書は、すべての HTTPS 通信および拡張認証プロトコル（EAP）の通信に使用されます。

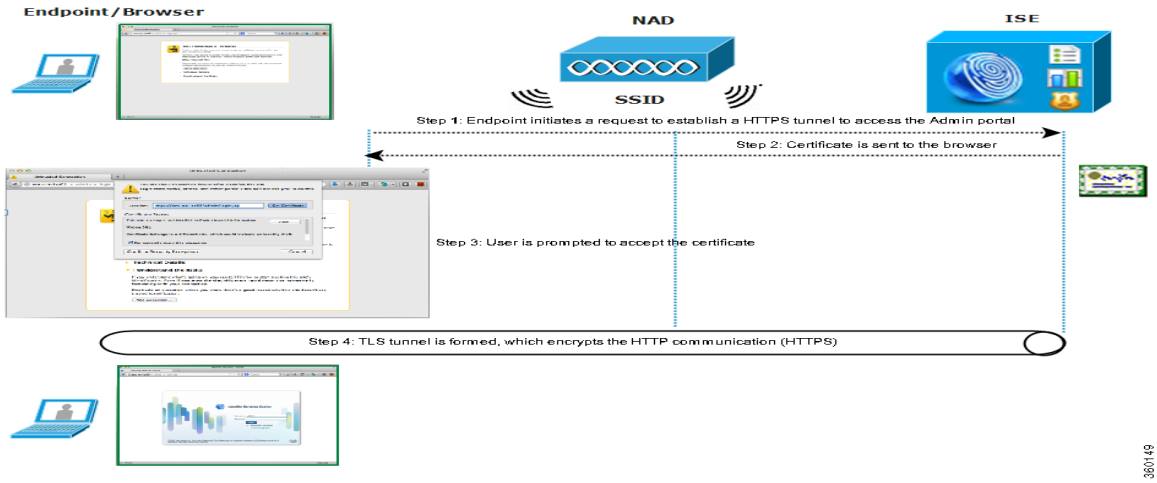
Cisco ISE 証明書を使用した HTTPS 通信

リリース 1.1.0 以降では、次のすべての Cisco ISE Web ポータルは HTTPS（TLS 暗号化された HTTP 通信）プロトコルを使用して、保護されています。

- 管理ポータル
- 一元化された Web 認証ポータル
- スポンサー ポータル
- クライアント プロビジョニング ポータル
- デバイス ポータル

図 E-1 に、管理ポータルと通信する際の TLS 暗号化プロセスを示します。

図 E-1　　HTTPS（TLS 暗号化された HTTP 通信）



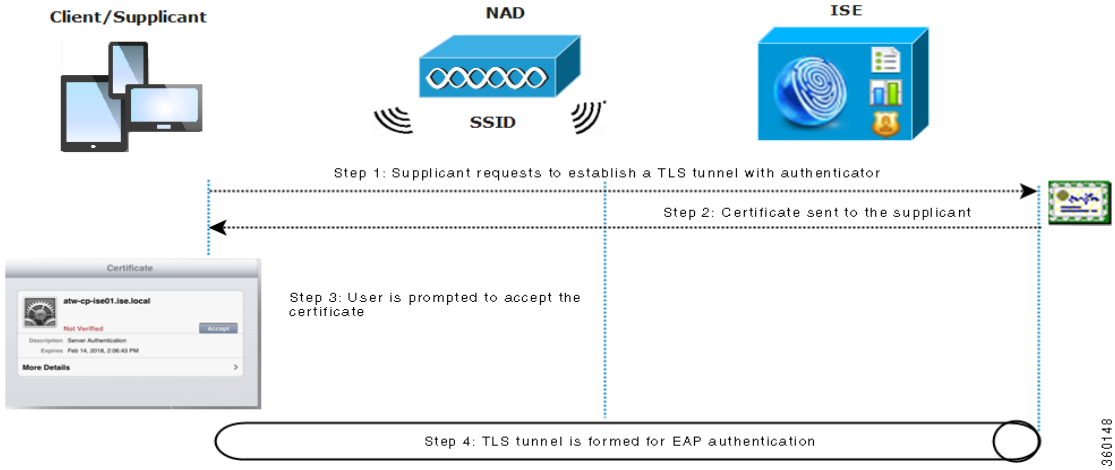
Cisco ISE 証明書を使用する EAP 通信

証明書はほとんどすべての EAP 方式で使用されます。一般に使用されるのは、次の EAP 方式です。

- EAP-TLS
- PEAP
- EAP-FAST

PEAP や FAST など、トンネル型の EAP 方式の場合は、クレデンシャルの交換を保護するために、Transport Layer Security（TLS）が使用されます。HTTPS Web サイトへの要求と同様に、クライアントがサーバとの接続を確立します。サーバがクライアントへ証明書を提示します。クライアントが証明書を信頼する場合は、TLS トンネルが形成されます。クライアントのクレデンシャルはトンネルが確立されるまでサーバに送信されないため、安全な交換が保障されます。セキュアなアクセスの導入では、クライアントはサプリカントであり、サーバは ISE ポリシー サービス ノードです。図 E-2 に PEAP を使用する例を示します。

図 E-2　　EAP 通信



Cisco ISE によるセキュアなアクセスの提供を可能にする証明書

Cisco Identity Services Engine（ISE）は、公開キー インフラストラクチャ（PKI）に依存して、エンドポイントおよび管理者の両方とのセキュアな通信、そしてマルチノード導入環境内の複数の Cisco ISE ノード間のセキュアな通信を実現しています。PKI は X.509 デジタル証明書に依存して、メッセージの暗号化と復号化のための公開キーの転送、およびユーザとデバイスを表す他の証明書の信頼性の検証を行います。Cisco ISE には、次の 2 つの X.509 証明書のカテゴリを管理する、管理ポータルが用意されています。

- ローカル証明書：これらはクライアント アプリケーションに対して Cisco ISE ノードを識別するサーバ証明書です。各 Cisco ISE ノードには独自のローカル証明書があり、それぞれの証明書は対応する秘密キーとともにノードに格納されています。

- 証明書ストア証明書：この証明書は、ユーザおよびデバイスから受信した公開キーの信頼を確立するために使用される認証局（CA）証明書です。証明書ストアには、Simple Certificate Enrollment Protocol（SCEP）から配信された証明書も含まれます。これにより、モバイル デバイスのエンタープライズ ネットワークへの登録が可能になります。証明書ストア内の証明書はプライマリ管理ノードで管理され、Cisco ISE の導入環境内の他のすべてのノードに自動的に複製されます。

分散導入環境では、証明書をプライマリ管理ノードの証明書信頼リスト（CTL）のみにインポートする必要があります。この証明書はセカンダリ ノードに複製されます。

一般に、Cisco ISE での証明書認証が、証明書による認証機能のわずかな違いの影響を受けないようにするために、ネットワークに導入されているすべての Cisco ISE ノードには小文字のホスト名を使用してください。

Cisco ISE での PKI の有効化

次のようにして、Cisco ISE で PKI を有効にする必要があります。

ステップ 1　ブラウザおよび REST クライアントが Cisco ISE Web ポータルへのアクセスするのに使用する、TLS 対応の認証プロトコル（たとえば、EAP-TLS プロトコル）および HTTPS を対象として、各導入ノードでローカル証明書を確立します。

デフォルトでは、Cisco ISE ノードには両方の目的に使用される自己署名証明書があらかじめインストールされています。一般的な企業環境では、この証明書は、信頼された CA によって署名された 1 つおよび 2 つののサーバ証明書に置き換えられます。

ステップ 2　証明書ストアに、ユーザとの信頼を確立するために必要な CA 証明書と、Cisco ISE に提示されるデバイス証明書を配置します。

ユーザまたはデバイスの証明書の信頼性を検証するために、ルート CA 証明書と 1 つ以上の中間 CA 証明書で構成される証明書チェーンが必要な場合は、証明書ストアにそのチェーン全体をインポートする必要があります。

関連項目

- 証明書署名要求を生成し、CA 署名付きの証明書をインポートする方法の詳細については、「ローカル証明書」（P.E-4）を参照してください。
- これらの証明書チェーンをインポートする方法の詳細については、「証明書ストア」（P.E-25）を参照してください。

Cisco ISE ノードはノード間の通信に HTTPS を使用するため、管理者は、Cisco ISE 導入環境内の各ノードに属する HTTPS ローカル証明書を検証するために必要な信頼証明書を、証明書ストアに配置する必要があります。デフォルトの自己署名証明書を HTTPS に使用する場合は、各 Cisco ISE ノードからこの証明書をエクスポートし、証明書ストアにインポートする必要があります。自己署名証明書を CA 署名証明書で置き換える場合に必要なのは、適切なルート CA 証明書および中間 CA 証明書を証明書ストアに配置することだけです。この手順を完了するまでは、ノードを Cisco ISE 導入環境に登録できないことに注意してください。

導入した Cisco ISE が FIPS モードで動作するようにする場合、すべてのローカル証明書および証明書ストアの証明書が FIPS 準拠であることを確認する必要があります。つまり、各証明書のキー サイズが 2048 バイト以上であり、SHA-1 または SHA-256 暗号化を使用する必要があります。

（注） スタンドアロンの Cisco ISE またはプライマリ管理ノードからバックアップを取得した後に導入環境内の 1 つ以上のノードの証明書設定を変更する場合は、データを復元するために、もう一度バックアップを取得する必要があります。そうしないで古いバックアップを使用してデータを復元すると、ノード間の通信が失敗する可能性があります。

この章の内容は、次のとおりです。

ローカル証明書

Cisco ISE ローカル証明書は、クライアント アプリケーションに対して Cisco ISE ノードを識別するサーバ証明書です。ローカル証明書は、

- Cisco ISE Web ポータルにブラウザおよび REST クライアントで使用されます。これらの接続には HTTPS プロトコルを使用する必要があります。
- PEAP および EAP-FAST を使用する外部 TLS トンネルを形成するために使用される。これらの証明書は、EAP-TLS、PEAP、および EAP-FAST を使用した相互認証に使用できます。

Cisco ISE 導入環境内の各ノードに HTTPS および EAP-TLS 用の有効なローカル証明書をインストールする必要があります。デフォルトでは、自己署名証明書はインストール時に Cisco ISE ノードに作成されます。また、この証明書は、HTTPS、および EAP-TLS を使用するために設計されています（キーの長さは 1024 で、1 年間有効です）。セキュリティを強化するために、自己署名証明書を CA 署名証明書で置き換えることが推奨されます。

ワイルドカード証明書

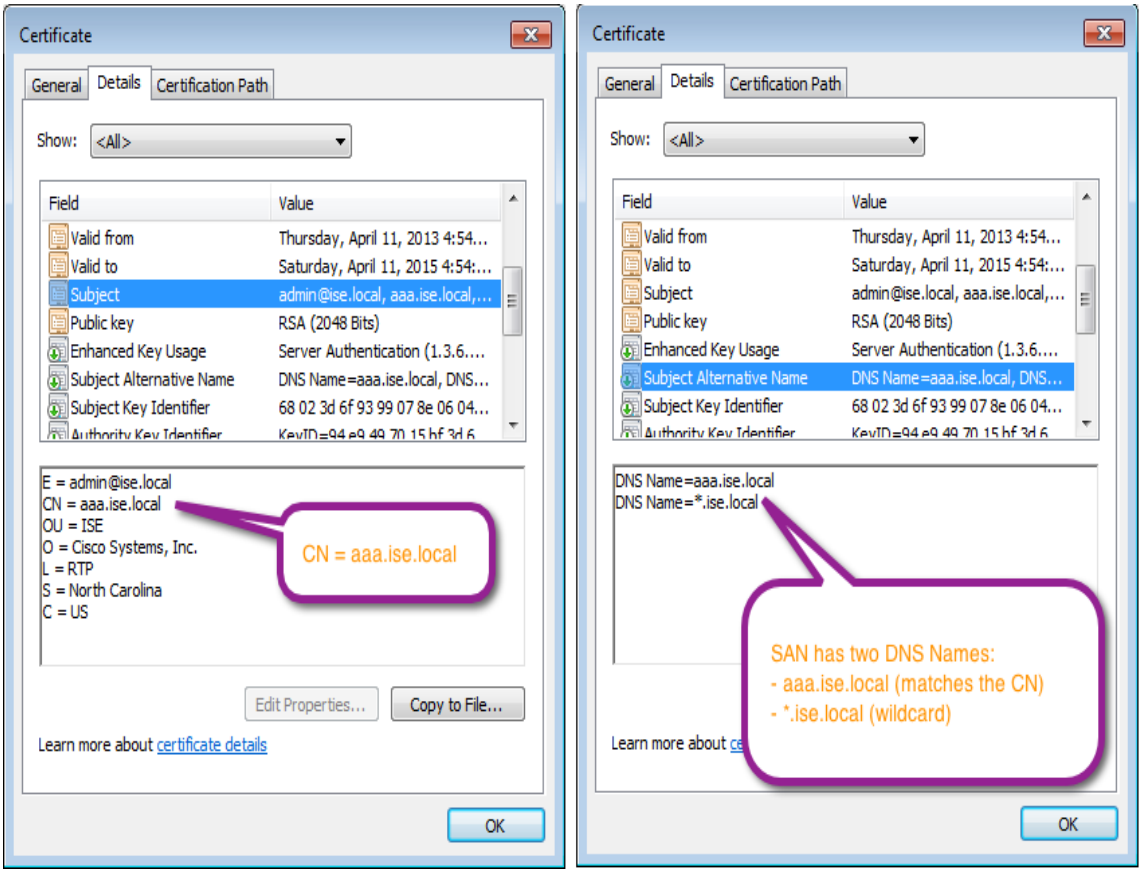
ワイルドカード証明書はワイルドカード表記（ドメイン名の前にアスタリスクとピリオドの形式）を使用し、組織の複数のホスト間で証明書を共有できるようにします。たとえば、証明書サブジェクトの CN 値は aaa.ise.local などの汎用ホスト名であり、SAN フィールドには、同じ汎用ホスト名と DNS.1=aaa.ise.local および DNS.2=*.ise.local などのワイルドカード表記が含まれます。

*.ise.local を使用してワイルドカードの証明書を設定している場合は、同じ証明書を使用して、次のような、DNS 名が「.ise.local」で終了する他の任意のホストを保護することができます。

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

図 E-3 に、Web サイトを保護するために使用されるワイルドカードの証明書の例を示します。

図 E-3　　ワイルドカードの証明書の例



ワイルドカード証明書は通常の証明書と同じ方法で通信を保護し、要求は同じ検証方式を使用して処理されます。

関連項目

- 「HTTPS および EAP 通信用のワイルドカード証明書」（P.E-5）
- 「Cisco ISE リリース 1.2 におけるワイルドカード証明書のサポート」（P.E-6）
- 「URL リダイレクトの完全修飾ドメイン名」（P.E-6）
- 「ワイルドカード証明書の互換性」（P.E-8）
- 「ワイルドカードの証明書の作成」（P.E-9）
- 「Cisco ISE へのワイルドカード証明書のインストール」（P.E-10）

HTTPS および EAP 通信用のワイルドカード証明書

SSL/TLS トンネリングを使用する HTTPS（Web ベースのサービス）および EAP プロトコルに対して、Cisco ISE でワイルドカード サーバ証明書を使用できます。ワイルドカードの証明書を使用することにより、各 Cisco ISE ノード用の固有の証明書を生成する必要がなくなります。また、証明書の警告を防ぐために、SAN フィールドに複数の FQDN 値のを入力する必要もありません。SAN フィールドでアスタリスク（*）を使用すると、導入環境内の複数のノードで単一の証明書を共有できるようになり、証明書名の不一致による警告を防止することができます。ただし、ワイルドカード証明書は、各 Cisco ISE ノードに固有のサーバ証明書を割り当てる場合より、安全性が低いと見なされます。

（注） ワイルドカード証明書を使用する場合は、セキュリティを強化するためにドメイン領域を分割することを推奨します。たとえば、*.example.com の代わりに *.amer.example.com を使用して領域を分割することができます。ドメインを分割しないと、重大なセキュリティ問題が発生する可能性があります。

ワイルドカード証明書では、ドメイン名の前にアスタリスク（*）およびピリオドが使用されます。たとえば、証明書のサブジェクト名の CN 値は aaa.ise.local などの汎用ホスト名になり、SAN フィールドには *.ise.local のようなワイルドカード文字が入力されます。Cisco ISE は、ワイルドカード証明書（表示される ID の一番左の文字がワイルドカード文字（*））をサポートします。たとえば、*.example.com または *.ind.example.com です。表示される ID にワイルドカード文字とともに追加の文字が含まれた証明書はサポートされません。たとえば、abc*.example.com、a*b.example.com、または *abc.example.com です。

Cisco ISE リリース 1.2 におけるワイルドカード証明書のサポート

Cisco ISE リリース 1.2 は、ワイルドカード証明書をサポートしています。リリース 1.2 よりも前の Cisco ISE では、HTTPS に対して有効になったすべての証明書を検証し、CN フィールドがホストの完全修飾（FQDN）が正確に一致することが確認されます。フィールドが一致しない場合、その証明書は HTTPS 通信に使用できませんでした。

1.2 より前のリリースでは、Cisco ISE はその CN 値 を使用して、URL リダイレクト A-V ペア文字列内の変数を置き換えます。この CN 値は、すべての Centralized Web Authentication（CWA）、オンボーディング、ポスチャのリダイレクトなどに使用されます。

Cisco ISE 1.2 は CN フィールドを使用する代わりに CN として このホスト名を使用します。

URL リダイレクトの完全修飾ドメイン名

Cisco ISE が承認プロファイル リダイレクトを構築（中央集中型 Web認証、デバイス登録 Web 認証、ネイティブ サプリカントのプロビジョニング、モバイル デバイス管理、およびクライアントのプロビジョニングとポスチャ サービスに対して）する場合、結果の cisco-av-pair ペアには、次のような文字列が含まれます。

url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

この要求を処理するときに、Cisco ISE は文字列の一部のキーワードを実際の値で置き換えます。たとえば、SessionIdValue は、要求の実際のセッション ID に置き換えられます。eth0 インターフェイスの場合、Cisco ISE は URL 内の IP を Cisco ISE ノードの FQDN で置き換えます。eth0 以外のインターフェイスの場合、Cisco ISE は URL 内の IP アドレスを使用します。インターフェイス eth1 から eth3 にはホストのエイリアス（名前）を割り当てることができます。このエイリアスは Cisco ISE が URL リダイレクト時に IP アドレスの代わりに置き換えることができます。これを行うには、次のように、Cisco ISE CLI から設定モードで **ip host** コマンドを使用できます。

ISE /admin(config)# **ip host** *IP_address host-alias FQDN-string*

ここで、*IP_address* はネットワーク インターフェイス（eth1、eth2、または eth3）の IP アドレスです。

host-alias はネットワーク インターフェイスに割り当てる名前です。

FQDN-string は、ネットワーク インターフェイスの完全修飾ドメイン名です。

このコマンドを使用して、ネットワーク インターフェイスに *host-alias* または *FQDN-string* あるいはその両方を割り当てることができます。

次に例を示します。

```
ISE/admin(config)# ip host a.b.c.d sales sales.amer.xyz.com
```

eth0 以外のインターフェイスにホストのエイリアスを割り当てたら、**application start ise** コマンドを使用して Cisco ISE でアプリケーション サービスを再起動する必要があります。

このホスト エイリアスのネットワーク インターフェイスとの関連付けを削除するには、次のようにこのコマンドの no 形式を使用します。

ISE/admin(config)# **no ip-host** *IP_address host-alias FQDN-string*

ホストのエイリアスの定義を表示するには、**show running-config** コマンドを使用します。

FQDN 文字列を指定している場合は、その FQDN で URL 内の IP アドレスが置き換えられます。ホストのエイリアスのみを指定した場合は、そのホスト エイリアスと設定された IP ドメイン名を結合して完全な FQDN が結合され、URL 内の IP アドレスがその FQDN で置き換えられます。ネットワーク インターフェイスをホストのエイリアスにマッピングしない場合は、URL 内のネットワーク インターフェイスの IP アドレスが使用されます。

クライアントのプロビジョニング、ネイティブ サプリカント、またはゲスト フローに対して eth0 以外のインターフェイスを使用する場合は、eth0 以外のインターフェイスの IP アドレスまたはホスト エイリアスがポリシー サービス ノードの証明書の SAN フィールドに適切に設定されていることを確認する必要があります。

ワイルドカード証明書を使用する利点

- コスト削減。サードパーティの認証局によって署名された証明書には高額な費用がかかります（特にサーバ数が多い場合）。ワイルドカード証明書は、Cisco ISE 導入環境内の複数ノードで使用できます。
- 運用の効率化。ワイルドカード証明書は、すべてのポリシー サービス ノード（PSN）EAP および Web サービスが同じ証明書を共有することを可能にします。証明書を 1 回作成して、すべての PSN に適用することにより、コストを大幅に削減できるだけでなく、証明書の管理も簡素化されます。
- 認証エラーの低減。ワイルドカード証明書は、クライアントがプロファイル内に信頼された証明書を保存しており、そのクライアントが iOS のキーチェーン（署名ルートが信頼されている）に従っていない Apple iOS デバイスで発生する問題に対処します。iOS クライアントが最初に PSN と通信する際、このクライアントはその PSN の証明書を（信頼された認証局が署名している場合でも）明示的に信頼しません。ワイルドカード証明書を使用すると、この証明書がすべての PSN で同一になるため、ユーザは証明書の受け入れを 1 回行えばよく、その後の異なる PSN に対する認証はエラーやプロンプトが表示されることなく進行します。
- 簡素化されたサプリカントの設定。たとえば、PEAP-MSCHAPv2 およびサーバ証明書の信頼が有効化された Microsoft Windows サプリカントで、各サーバ証明書を信頼するように指定することが必要とされており、そのように指定されていない場合、そのクライアントが別の PSN を使用して接続を行うと、各 PSN 証明書を信用するように、ユーザにプロンプトが出される可能性があります。ワイルドカード証明書を使用すると、各 PSN の個別の証明書ではなく、単一のサーバ証明書を信頼するだけで済みます。
- ワイルドカード証明書を使用すると、プロンプトの提示が減り、よりシームレスな接続が実現されることにより、ユーザ エクスペリエンスが改善されます。

ワイルドカード証明書を使用することの欠点

次に、ワイルドカード証明書に関連するセキュリティ上の考慮事項の一部を説明します。

- 監査性と否認防止性の低下
- 秘密キーの露出の増加
- 一般的ではなく、管理者により理解されていない

ワイルドカード証明書は ISE ノードごとの固有のサーバ証明書より安全性が低いと見なされています。ただし、コスト、およびその他の運用関連の要因がセキュリティ リスクに勝っています。

ASA などのセキュリティ デバイスも、ワイルドカード証明書をサポートしています。

ワイルドカード証明書を導入する場合には注意が必要です。たとえば、*.company.local を使用して証明書を作成したとします。該当の秘密キーを攻撃者が回復できた場合、攻撃者は company.local ドメイン内のすべてのサーバをスプーフィングすることができます。したがって、このタイプの危険を回避するために、ドメイン領域を分割することがベスト プラクティスと見なされています。

この想定される問題に対処し、利用範囲を制限するために、ワイルドカード証明書を使用して組織の特定のサブドメインを保護することもできます。ワイルドカードを指定する一般名のサブドメイン領域に、アスタリスク（*）を追加します。

たとえば、*.ise.company.local に対してワイルドカード証明書を設定すると、その証明書は次のような、DNS 名が「.ise.company.local」で終わるすべてのホストを保護するために使用できます。

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

ワイルドカード証明書の互換性

ワイルドカード証明書は、通常図 E-3 の例にあるような、一般名（CN）としてリストされているワイルドカードを使用して作成されます。Cisco ISE リリース 1.2 は、このタイプの作成をサポートします。ただし、すべてのエンドポイント サプリカントが証明書サブジェクトのワイルドカード文字をサポートするわけではありません。

テスト済みのすべての Microsoft ネイティブ サプリカント（Windows Mobile を含む）の一部は、証明書のサブジェクトのワイルドカード文字をサポートしていません。

Cisco AnyConnect Network Access Manager（NAM）など、[Subject（サブジェクト）] フィールドでのワイルドカード文字の使用をサポートできる他のサプリカントを使用することができます。

また、DigiCert の Wildcard Plus など、証明書のサブジェクト代替名に特定のサブドメインを含めることで、互換性のないデバイスを使用するように設計された、特別なワイルドカード証明書を使用することもできます。

Microsoft サプリカントの制限はワイルドカード証明書の使用にとって妨げになるように見えますが、Microsoft のネイティブ サプリカントを含む、セキュアなアクセスについてテスト済みのすべてのデバイスを使用できるようにする代替の方法があります。

このためには、サブジェクトにワイルドカードを使用する代わりに、[Subject Alterative Name (SAN)（サブジェクト代替名（SAN））] フィールドでワイルドカード文字を使用します。SAN フィールドはドメイン名（DNS 名）を検査するように設計された拡張を保持します。詳細については、RFC 6125 および 2128 を参照してください。

ワイルドカード証明書の Microsoft サポートの詳細については、次を参照してください。
http://technet.microsoft.com/en-US/cc730460

ワイルドカードの証明書の作成

この項では、ワイルドカード証明書を作成する方法について説明します。この手順は、ほとんどの SSL 証明書のプロバイダーに適用されます。

ただし SSL 証明書プロバイダーが証明書の SAN フィールドにおけるワイルドカード値をサポートしていない場合は、証明書の SAN に各 ISE ノードのおよびインターフェイスの FQDN を設定します（ip host コマンドを使用して指定されたエイリアスごと）。この証明書は複数ドメイン証明書と呼ばれます。デバイス ポータルおよびスポンサー ポータルで使用されるような特定のサービス エイリアスの FQDN も、証明書の SAN に含める必要があります。ISE 管理ポータル、スポンサー ポータル、およびデバイス ポータルに対するローカル Web 認証ネットワーク認証など、一部のサービスではロード バランサを使用できます。このような場合は、証明書の SAN フィールドに、ロード バランス対象のサービスの仮想 IP アドレスに割り当てられた FQDN を含める必要があります。

（注） HTTPS および EAP 認証に別々の証明書を使用することもできます。HTTPS に対して指定された証明書はノード間の通信およびすべての Web ポータル サービス（中央集中型 Web 認証、DRW、ポスチャの検出と評価、モバイル デバイス管理、ネイティブ サプリカントのプロビジョニング、スポンサー、および自分のデバイスのポータルなど）を保護するために使用されます。EAP に指定された証明書は、PEAP、EAP-TLS、EAP-FAST など、EAP プロトコルを使用するすべてのクライアント認証を保護するために使用されます。

たとえば 2 つの PSN ノードがある ISE の導入環境（eth0、eth1、および eth2 インターフェイスが有効になった psn1 および psn2）を使用しており、ワイルドカードを使用せずに複数ドメインの証明書を作成する場合、値は次のようになります。

CN=aaa.company.local（導入環境内の ISE ノードの FQDN）

SAN=DNS.1=aaa.company.local、DNS.2=psn1.company.local、DNS.3=psn2.company.local、DNS.4=psn1-e1.company.local、DNS.5=psn2-e1.company.local、DNS.6=psn1-e2.company.local、DNS.7=psn2-e2.company.local。

ヒント 追加のポリシー サービス ノードを今後導入することを計画している場合は、SAN フィールドに追加の DNS 名のエントリを追加して、新しいノードの導入時に同じ証明書を再利用できるようにします。

証明書の SAN フィールドに IP アドレスを指定する必要がある場合は（たとえば、URL リダイレクションのための固定 IP アドレスを使用する DMZ）証明書の SAN フィールドの DNS 名および IP アドレスとして、該当のポリシー サービス ノードの IP アドレスを指定していることを確認します。たとえば、CN=psn.ise.local および SAN=DNS.1=psn.ise.local、DNS.2=*.ise.local、DNS.3= 10.1.1.20、IP.1=10.1.1.20 のようになります。

はじめる前に

Microsoft のネイティブ サプリカントの場合は、証明書の SAN フィールドでワイルドカードを使用します。

ステップ 1 サブジェクトの CN フィールドに汎用のホスト名を入力します。たとえば、CN=aaa.ise.local のようになります。

ステップ 2 証明書の SAN フィールドに同じ汎用のホスト名とワイルドカード表記を入力します。たとえば、DNS Name=aaa.ise.local、DNS Name=*.ise.local のようになります。図 E-3を参照してください。

この方法は、Comodo.com や SSL.com など、大部分のテスト済みのパブリック認証局で成功します。これらの パブリック CA を使用する場合は、「Unified Communications Certificates (UCC)」を要求する必要があります。

次の作業

ポリシー サービス ノードにワイルドカード証明書をインポートします。

関連項目

「Cisco ISE へのワイルドカード証明書のインストール」（P.E-10）

Cisco ISE へのワイルドカード証明書のインストール

はじめる前に

eth0 以外のインターフェイスを有効にしている場合は、CLI で **ip host** コマンドを使用して、必ずそのインターフェイスにホストのエイリアスをマッピングします。詳細については、「URL リダイレクトの完全修飾ドメイン名」を参照してください。

ワイルドカード証明書をインストールするには、次のタスクを実行する必要があります。

ステップ 1　ワイルドカード証明書の証明書署名要求を作成します。「ワイルドカード証明書に対する証明書署名要求の作成」（P.E-10）を参照してください。

ステップ 2　証明書署名要求をエクスポートします。「証明書署名要求のエクスポート」（P.E-11）を参照してください。

ステップ 3　証明書署名要求を認証局へ送信します。「認証局への CSR の送信」（P.E-12）を参照してください。

ステップ 4　証明書ストアにルート証明書をインポートします。「証明書ストアへのルート証明書のインポート」（P.E-13）を参照してください。

ステップ 5　証明書署名要求を新しいパブリック証明書にバインドします。「新しいパブリック証明書と CSR のバインド」（P.E-13）を参照してください。

ステップ 6　CA 署名付き証明書と秘密キーをエクスポートします。「CA 署名付き証明書と秘密キーのエクスポート」（P.E-13）を参照してください。

ステップ 7　すべてのポリシー サービス ノードに CA 署名付き証明書と秘密キーをインポートします。「ポリシーのサービス ノードへの CA 署名付き証明書のインポート」（P.E-13）を参照してください。

ワイルドカード証明書に対する証明書署名要求の作成

ステップ 1　[**Administration**（管理）] > [**Certificates**（証明書）] > [**Local Certificates**（ローカル証明書）] を選択します。

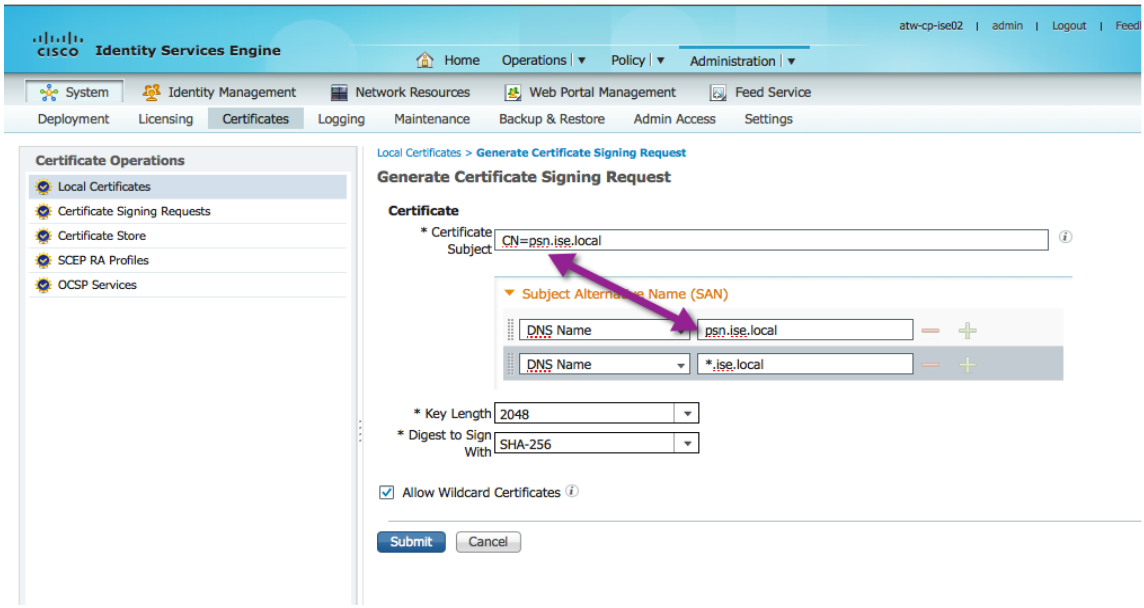
ステップ 2　[**Add**（追加）] > [**Generate Certificate Signing Request**（証明書署名要求の作成）] をクリックします。

ステップ 3　証明書のサブジェクトに、ポリシーのサービス ノードのいずれかの汎用 FQDN を入力します。たとえば、CN=psn.ise.local です。

ステップ 4　SAN に 2 つの値を入力します。値の 1 つは、証明書のサブジェクトに入力した CN と同じである必要があります。もう 1 つの値はワイルドカード表記です。たとえば、DNS name=psn.ise.local、DNS name=*.ise.local のようになります。

ステップ 5　[**Allow Wildcard Certificates（ワイルドカード証明書の許可）**] チェックボックスをオンにします。

図 E-4　　ワイルドカード表記を使用した証明書署名要求



ステップ 6　[**Submit（送信）**] をクリックします。

証明書署名要求のエクスポート

ステップ 1　[**Administration（管理）**] > [**Certificates（証明書）**] > [**Certificate Signing Requests（証明書署名要求）**] を選択します。

ステップ 2　作成した CSR の横にあるチェックボックスをオンにします。たとえば、psn.ise.local です。

ステップ 3　[**Export（エクスポート）**] をクリックします。

ステップ 4　ローカル システムに CSR を保存します。

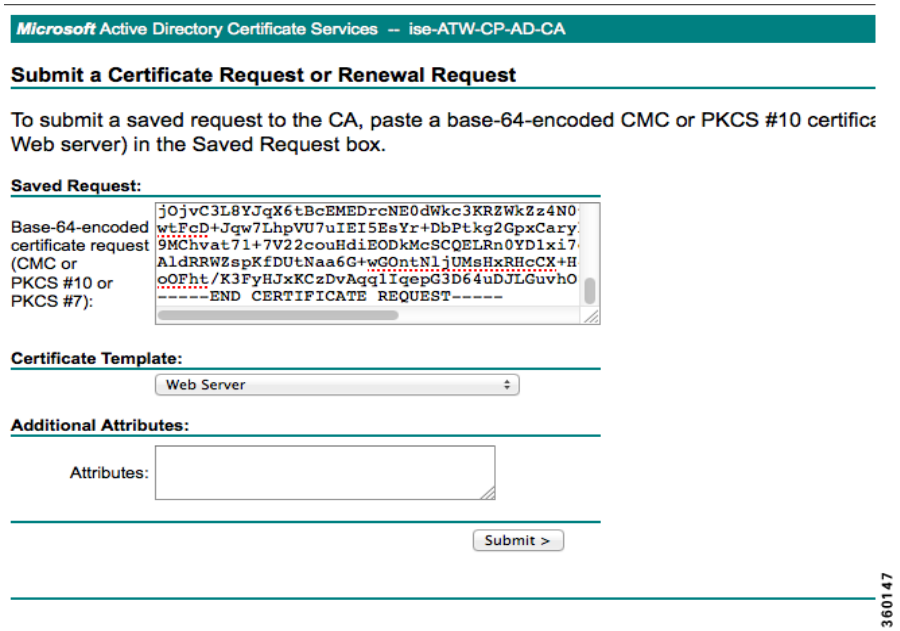
認証局への CSR の送信

ステップ 1　CSR をメモ帳などのテキスト エディタで開きます。

ステップ 2　「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」までのテキストをコピーします。

ステップ 3　選択した CA の証明書要求に、この CSR の内容を貼ってください。図 E-5を参照してください。

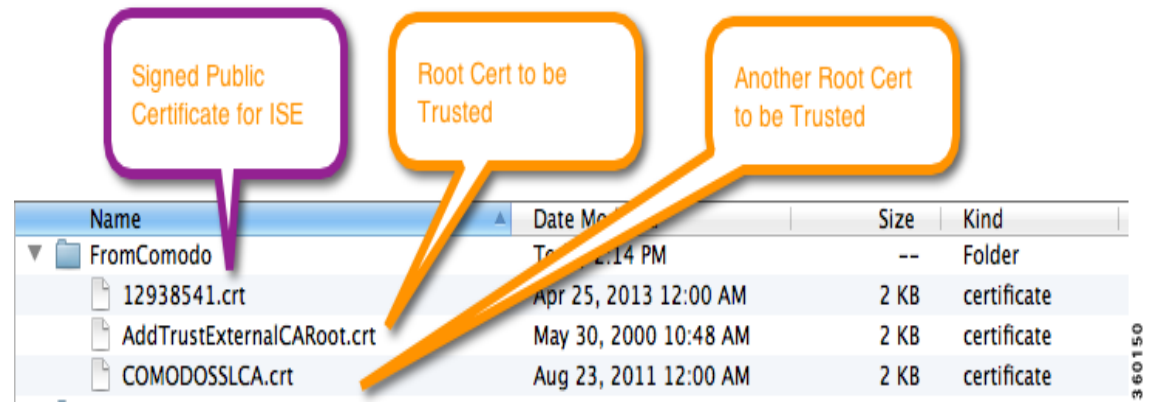
図 E-5　証明書署名要求フォームの CSR のコンテンツ：Active Directory CA



ステップ 4　署名済みの証明書をダウンロードします。

CA によっては、署名付き証明書が電子メールで送信される場合があります。署名付き証明書は、zip ファイルの形式で、Cisco ISE の信頼された証明書ストアに追加する必要がある、新規発行の証明書と CA のパブリック署名証明書が含まれています。図 E-6を参照してください。

図 E-6　CA によって返される証明書



証明書ストアへのルート証明書のインポート

はじめる前に

Cisco ISE の CSR に新規の署名付き証明書をバインドする前に、署名ルート証明書が Cisco ISE 証明書ストアにあることを確認します。

ステップ 1　[**Administration（管理）**] > [**Certificates（証明書）**] > [**Certificate Store（証明書ストア）**] を選択します。

ステップ 2　[**Import（インポート）**] をクリックします。

ステップ 3　CA によって返されたルート証明書を選択します。

新しいパブリック証明書と CSR のバインド

ステップ 1　[**Administration（管理）**] > [**Certificates（証明書）**] > [**Local Certificates（ローカル証明書）**] を選択します。

ステップ 2　[**Add（追加）**] > [**Bind CA signed Certificate（CA 署名付き証明書のバインド）**] をクリックします。

ステップ 3　CA 署名付き証明書を選択します。

ステップ 4　[**Allow Wildcard Certificates（ワイルドカード証明書の許可）**] チェックボックスをオンにします。

ステップ 5　プロトコルを選択します。

ステップ 6　[**Submit（送信）**] をクリックします。

CA 署名付き証明書と秘密キーのエクスポート

ステップ 1　[**Administration（管理）**] > [**Certificates（証明書）**] > [**Local Certificates（ローカル証明書）**] を選択します。

ステップ 2　エクスポートする CA 署名付き証明書の横にあるチェックボックスをオンにし、[**Export（エクスポート）**] をクリックします。

ステップ 3　ファイルをローカル システムに保存します。

ポリシーのサービス ノードへの CA 署名付き証明書のインポート

ステップ 1　[**Administration（管理）**] > [**Certificates（証明書）**] > [**Certificate Store（証明書ストア）**] を選択します。

ステップ 2　エクスポートした CA 署名付き証明書を選択します。

ステップ 3　[**Submit（送信）**] をクリックします。

Cisco ISE での CA 署名付き証明書のインストール

CA 署名付き証明書をインストールするための手順は次のとおりです。

ステップ 1　CA 署名付き証明書を必要とするノードの Cisco ISE 管理インターフェイスで、証明書署名要求（CSR）を生成します。

ステップ 2　CSR をファイルにエクスポートします。

ステップ 3　CSR ファイルを認証局に提供し、その CA に、CSR に指定された属性を使用して証明書を作成し、署名するよう要求します。CA が、証明書をファイルで返します。

ステップ 4　同じノードの Cisco ISE 管理インターフェイスで、ノードに CSR とともに保持されている秘密キーに CA 署名付き証明書を バインドします。HTTPS または EAP-TLS 用に使用する証明書を指定します。

（注）　HTTPS に CA 署名付き証明書を使用する場合、CSR に対して指定されるサブジェクトの一般名の値が Cisco ISE ノードの完全修飾ドメイン名（FQDN）に一致するか、証明書の SAN/CN フィールドで指定されているワイルドカード ドメイン名に一致する必要があります。

Cisco ISE は、サブジェクト名の一致を次のようにして確認します。

1. 証明書のサブジェクト代替名（SAN）の拡張が確認されます。SAN に 1 つ以上の DNS 名が含まれている場合は、それらの DNS 名の 1 つが Cisco ISE ノードの FQDN に一致している必要があります。ワイルドカード証明書が使用されている場合、ワイルドカード ドメイン名は Cisco ISE ノードの FQDN ドメインに一致している必要があります。
2. SAN に DNS 名が存在しない場合、または SAN 全体が欠落している場合は、証明書の Subject フィールドの一般名（CN）または証明書の Subject フィールドのワイルドカード ドメインが、ノードの FQDN に一致している必要があります。
3. 一致しない場合、証明書は拒否されます。

（注）　Cisco ISE にインポートされる X.509 証明書は、Privacy Enhanced Mail（PEM）または Distinguished Encoding Rules（DER）形式である必要があります。 証明書チェーン（ローカル証明書、およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。詳細については、「証明書チェーンのインポート」（P.E-29）を参照してください。

X.509 証明書が有効なのは、指定された特定の日付までのみです。ローカル証明書が期限切れになった場合、その証明書に依存する Cisco ISE 機能が影響を受けます。Cisco ISE は、有効期限が 90 日以内になると、ローカル証明書の有効期限の保留について通知します。この通知は、いくつかの方法で表示されます。

- 配色された有効期限の状態アイコンが、[Local Certificates（ローカル証明書）] ページに表示されます。
- 期限切れメッセージが Cisco ISE システム診断レポートに表示されます。
- 有効期限のアラームは、有効期限の 90 日前、60 日前に生成され、有効期限前の最後の 30 日間には毎日生成されます。

失効した証明書が自己署名証明書の場合は、この証明書を編集して有効期限を延長できます。CA 署名付き証明書の場合は、CA から新しい証明書を取得するのに十分な期間を取ってください。

Cisco ISE 管理インターフェイスから次のタスクを実行して、ローカル証明書を管理できます。

- Cisco ISE ノードに保存されたローカル証明書のリストを表示する。リストには、有効期限の状態とともに、各証明書プロトコルの割り当て（HTTPS、EAP-TLS）が表示されます。
- CSR を作成する
- CSR をエクスポートする
- CA 署名付き証明書をその秘密キーにバインドする
- ローカル証明書と、オプションで秘密キーをエクスポートする
- ローカル証明書と秘密キーをインポートする
- 自己署名したローカル証明書を生成する
- ローカル証明書を編集する（証明書が自己署名の場合は有効期限の延長を含む）
- ローカル証明書を削除する
- CSR を削除する

ここでは、次の内容について説明します。

- 「ローカル証明書の表示」（P.E-15）
- 「ローカル証明書の追加」（P.E-16）
- 「ローカル証明書の編集」（P.E-22）
- 「ローカル証明書のエクスポート」（P.E-23）

関連項目

- 「ワイルドカード証明書」（P.E-4）
- 「URL リダイレクトの完全修飾ドメイン名」（P.E-6）
- 「ローカル証明書のインポート」（P.E-16）
- 「証明書署名要求の生成」（P.E-20）
- 「CA 署名付き証明書のバインディング」（P.E-21）

ローカル証明書の表示

[Local Certificate（ローカル証明書）] ページに、Cisco ISE に追加されたすべてのローカル証明書が一覧表示されます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　**[Administration（管理）] > [System（システム）] > [Certificates（証明書）] > [Local Certificates（ローカル証明書）]** を選択します。

[Local Certificate（ローカル証明書）] ページが表示されます。このページには、ローカル証明書に関する次の情報が表示されています。

- [Friendly Name（わかりやすい名前）]：証明書の名前。
- [Protocol（プロトコル）]：証明書を使用するプロトコル。

- [Issued To（発行先）]：証明書のサブジェクトの一般名。
- [Issued By（発行者）]：証明書の発行者の一般名。
- [Valid From（有効期限の開始）]：証明書の作成日付（[Not Before（作成日付後）] 証明書属性）。
- [Expiration Date（有効期限）]：証明書の有効期限（[Not After（有効期限前）] 証明書属性）。
- [Expiration Status（有効期限のステータス）]：証明書の有効期限がいつ切れるかを示します。ここには、アイコンが関連付けられた 5 つのカテゴリがあります。
  1. [Expiring in more than 90 days（有効期限が 90 日以上先）]（緑のアイコン）
  2. [Expiring in 90 days or less（有効期限が 90 日以内）]（青のアイコン）
  3. [Expiring in 60 days or less（有効期限が 60 日以内）]（青のアイコン）
  4. [Expiring in 30 days or less（有効期限が 30 日以内）]（青のアイコン）
  5. [Expired（期限切れ）]（赤のアイコン）

関連項目

- 「ワイルドカード証明書」（P.E-4）

ローカル証明書の追加

次のいずれかの方法で、ローカル証明書を Cisco ISE に追加できます。

- 「ローカル証明書のインポート」（P.E-16）
- 「自己署名証明書の生成」（P.E-18）
- 「証明書署名要求の生成」（P.E-20）および「CA 署名付き証明書のバインディング」（P.E-21）

ワイルドカード証明書のインポートを計画している場合は、必ず次の項をお読みください。

- 「ワイルドカード証明書」（P.E-4）
- 「ワイルドカードの証明書の作成」（P.E-9）
- 「Cisco ISE へのワイルドカード証明書のインストール」（P.E-10）

（注） Firefox および Internet Explorer 8 ブラウザを使用している場合、あるノードにある HTTPS ローカル証明書を変更すると、そのノードに接続された既存のブラウザ セッションでは新しい証明書への自動的な切り替えは行われません。新しい証明書を表示するには、ブラウザを再起動する必要があります。

ローカル証明書のインポート

ローカル証明書をインポートすることにより、新しいローカル証明書を追加できます。

はじめる前に

クライアント ブラウザを実行しているシステムに、ローカル証明書と秘密キー ファイルがあることを確認します。

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

インポートするローカル証明書に基本制約拡張が含まれていて CA フラグが true に設定されている場合は、キー使用拡張が存在することと、keyEncipherment ビットと keyAgreement ビットの一方または両方が設定されていることを確認してください。

ステップ 1　[**Administration（管理）**] > [**System（システム）**] > [**Certificates（証明書）**] > [**Local Certificates（ローカル証明書）**] を選択します。

ローカル証明書をセカンダリ ノードにインポートするには、[**Administration（管理）**] > [**System（システム）**] > [**Server Certificate（サーバ証明書）**] を選択します。

ステップ 2　[**Add（追加）**] > [**Import Local Server Certificate（ローカル サーバ証明書のインポート）**] を選択します。

ステップ 3　[**Browse（参照）**] をクリックして、クライアント ブラウザを実行しているシステムから証明書ファイルと秘密キーを選択します。

秘密キーが暗号化されている場合は、パスワードを入力して復号化します。

ステップ 4　証明書のフレンドリ名を入力します。名前を入力しない場合は、*<common name>#<issuer>#<nnnnn>* の形式で自動的に名前が作成されます。ここで、*<nnnnn>* は固有の 5 桁の数値です。

ステップ 5　Cisco ISE に証明書の拡張の検証を許可する場合は、[**Enable Validation of Certificate Extensions（証明書の拡張の検証を許可）**] チェックボックスをオンにします。

[**Enable Validation of Certificate Extensions（証明書の拡張の検証を許可）**] チェックボックスがオンになっており、インポートする証明書に CA フラグ が true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在しており、keyEncipherment ビットまたは keyAgreement ビット、あるいはその両方が設定されていることを確認します。

ステップ 6　ワイルドカード証明書（サブジェクトまたはサブジェクト代替名の DNS 名、またはその両方にアスタリスク（*）が含まれている証明書）をインポートする場合は、[**Allow Wildcard Certificates（ワイルドカード証明書の許可）**] チェックボックスをオンにします。

ステップ 7　[Protocol group（プロトコル グループ）] ボックスで、次のようにします。

- Cisco ISE ノードを識別する EAP プロトコルでこの証明書を使用するには、[**EAP**] チェックボックスをオンにします。
- この証明書を Web サーバの認証に使用するには、[**HTTPS**] チェックボックスをオンにします。

  [Management Interface（管理インタフェース）] チェックボックスをオンにする場合は、証明書サブジェクトの一般名の値がノード完全修飾ドメイン名（FQDN）またはワイルドカード表記（ワイルドカード証明書が使用されている場合）に一致していることを確認してください。そうしない場合、インポート プロセスは失敗します。

ステップ 8　既存の証明書を複製した証明書で置き換えるには、[**Replace Certificate（証明書を置き換える）**] チェックボックスをオンにします。証明書のサブジェクトまたは発行者、およびシリアル番号が既存の証明書と同じ場合、その証明書は複製と見なされます。このオプションでは証明書の内容が更新されますが、証明書の既存のプロトコルの選択は保持されます。

（注）　Cisco ISE を FIPS モードで動作するように設定する場合、証明書の RSA キー サイズは 2048 ビット以上であり、SHA-1 または SHA-256 ハッシュ アルゴリズムを使用する必要があります。

ステップ 9　ローカル証明書をインポートするには、[**Submit（送信）**] をクリックします。

プライマリ Cisco ISE ノードにローカル証明書をインポートし、管理インターフェイス オプションが導入環境内のノードで有効になっている場合は、ノードのアプリケーション サーバが自動的に再起動されます。それ以外の場合は、プライマリ Cisco ISE ノードに接続されているセカンダリ ノードを再起動します。

CLI からセカンダリ ノードを再起動するには、指定された順序で次のコマンドを入力してください。

a. **application stop ise**

b. **application start ise**

これらのコマンドの詳細については、『*Cisco Identity Services Engine CLI Reference Guide, Release 1.2（Cisco Identity Services Engine CLI リファレンス ガイド リリース 1.2）*』を参照してください。

関連項目

- 「ワイルドカード証明書」（P.E-4）
- 「ワイルドカードの証明書の作成」（P.E-9）
- 「Cisco ISE へのワイルドカード証明書のインストール」（P.E-10）

自己署名証明書の生成

自己署名証明書を生成することにより、新しいローカル証明書を追加できます。自己署名証明書は、内部テストと評価のニーズに対してのみ使用することを推奨します。実稼働環境に Cisco ISE を導入することを計画している場合、可能な場合は CA 署名付き証明書を使用して、実稼働ネットワーク全体でより均一な受け入れが行われるようにします。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[**Administration（管理）**] > [**System（システム）**] > [**Certificates（証明書）**] > [**Local Certificates（ローカル証明書）**] を選択します。

セカンダリ ノードから自己署名証明書を生成するには、[**Administration（管理）**] > [**System（システム）**] > [**Server Certificate（サーバ証明書）**] を選択します。

ステップ 2　[**Add（追加）**] > [**Generate Self Signed Certificate（自己署名証明書の生成）**] を選択します。

ステップ 3　[Generate Self Signed Certificate（自己署名証明書の生成）] ページで、次の情報を入力してください。

- **証明書サブジェクト**：証明書に関連付けられているエンティティを識別する識別名（DN）。DN には一般名（CN）値が含まれている必要があります。
- **サブジェクト代替名**：証明書に関連付けられた DNS 名または IP アドレス。
- 必要な**キーの長さ**：有効な値は 512、1024、2048、および 4096 です。Cisco ISE を FIPS 準拠のポリシー管理エンジンとして導入する場合は、2048 ビット以上のキーの長さを指定する必要があります。
- **署名するダイジェスト**：SHA-1 または SHA-256 を使用して証明書を暗号化および復号化できます。

- 証明書の**期限切れ TTL**：有効期限の期間を日、週、月、または年単位で指定できます。
- 証明書の**フレンドリ名**を指定する場合は、フレンドリ名を秘密キー パスワードの下のフィールドに入力します。名前を入力しない場合は、*<common name>#<issuer>#<nnnnn>* の形式で自動的に名前が作成されます。ここで、*<nnnnn>* は固有の 5 桁の数値です。

ステップ 4　自己署名したワイルドカード証明書（サブジェクトまたはサブジェクト代替名の DNS 名、またはその両方にアスタリスク（*）が含まれている証明書）を作成する場合は、**[Allow Wildcard Certificates（ワイルドカード証明書の許可）]** チェックボックスをオンにします。たとえば、SAN に割り当てられている DNS 名が *.amer.cisco.com の場合です。

ステップ 5　[Protocol group（プロトコル グループ）] ボックスで、次のようにします。

- SSL/TLS トンネルを使用する EAP プロトコルでこの証明書を使用するには、**[EAP]** チェックボックスをオンにします。
- この証明書を Cisco ISE ポータルの認証に使用するには、**[HTTPS]** チェックボックスをオンにします。

  [Management Interface（管理インターフェイス）] チェックボックスをオンにする場合は、証明書のサブジェクトの一般名値がノードの完全修飾ドメイン名 （FQDN）に一致していることを確認します。そうでない場合、自己署名証明書は生成されません。

  [HTTPS] チェックボックスがオンになっている場合は、導入環境内のプライマリ管理ノードが再起動されます。

ステップ 6　[Override Policy（上書きポリシー）] 領域で、既存の証明書を複製された証明書で置き換えるには、**[Replace Certificate（証明書を置き換える）]** チェックボックスをオンにします。証明書のサブジェクトまたは発行者、およびシリアル番号が既存の証明書と同じ場合、その証明書は複製と見なされます。このオプションでは証明書の内容が更新されますが、証明書の既存のプロトコルの選択は保持されます。

ステップ 7　証明書を生成するには、**[Submit（送信）]** をクリックします。

（注）　自己署名証明書を使用しており、Cisco ISE ノードのホスト名を変更する必要がある場合は、Cisco ISE ノードの [Admin（管理）] ポータルにログインし、古いホスト名が使用された自己署名証明書を削除し、新しい自己署名証明書を生成します。そうしないと、Cisco ISE は古いホスト名が使用された自己署名証明書を引き続き使用します。

関連項目

- 「ワイルドカード証明書」（P.E-4）
- 「Cisco ISE へのワイルドカード証明書のインストール」（P.E-10）

証明書署名要求の生成

証明書署名要求を生成し、CA 署名付き証明書をバインドすることにより、新しいローカル証明書を追加できます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[**Administration（管理）**] > [**System（システム）**] > [**Certificates（証明書）**] > [**Local Certificates（ローカル証明書）**] を選択します。

セカンダリ ノードから CSR を生成するには、[**Administration（管理）**] > [**System（システム）**] > [**Server Certificate（サーバ証明書）**] を選択します。

ステップ 2　[Add（追加）] > [Generate Certificate Signing Request（証明書署名要求の作成）] を選択します。

ステップ 3　証明書サブジェクトおよび必要なキーの長さを入力します。証明書サブジェクトは、証明書に関連付けられているエンティティを識別する識別名（DN）です。DN には一般名の値が含まれている必要があります。識別名の要素は次のとおりです。

- C = 国
- ST = テスト州または都道府県
- L = テスト地名（都市）
- O = 組織名
- OU = 組織ユニット名
- CN = 一般名
- E = 電子メール アドレス

たとえば、ある CSR の証明書サブジェクトの値は次のような値になる可能性があります。「CN=Host-ISE.cisco.com、OU=Cisco、O=security、C=US、ST=NC、L=RTP、e= test@test.com」または「CN=aaa.amer.cisco.com、SAN 内の DNS 名=*.amer.cisco.com、OU=Cisco、O=security、C=US、ST=NC、L=RTP、e=abc@xyz.com」。

（注）　[Certificate Subject（証明書件名）] フィールドに入力するときは、文字列を引用符でカプセル化しないでください。

この CSR から生成された証明書を HTTPS 通信に使用する場合は、証明書サブジェクトの一般名の値がノードの FQDN であることを確認してください。そうでない場合は、生成された証明書をバインドするときに [**Management Interface（管理インターフェイス）**] を選択できません。

ステップ 4　**サブジェクト代替名**：証明書に関連付けられた DNS 名または IP アドレス。

ステップ 5　SHA-1 または SHA-256 を使用して証明書を暗号化および復号化することを選択します。

（注）　Cisco ISE を FIPS モードで動作するように設定する場合、証明書の RSA キー サイズは 2048 ビット以上であり、SHA-1 または SHA-256 ハッシュ アルゴリズムを使用する必要があります。

ステップ 6　証明書サブジェクトにCN または SAN とともにワイルドカードの FQDN を含める場合は、[**Allow Wildcard Certificates（ワイルドカード証明書の許可）**] チェックボックスオンにします。

ステップ 7　[**Submit（送信）**] をクリックして CSR を生成します。

CSR とその秘密キーが生成され、Cisco ISE に保存されます。この CSR は、[Certificate Signing Requests（証明書署名要求）] ページで表示できます。この CSR をエクスポートし、CA に送信して署名を取得できます。

関連項目

- 「ワイルドカード証明書」（P.E-4）
- 「ワイルドカード証明書に対する証明書署名要求の作成」（P.E-10）

CA 署名付き証明書のバインディング

証明書署名要求が認証局によって署名され、返されたら、CA 署名付き証明書とその秘密キーとをバインドして、Cisco ISE へのローカル証明書の追加プロセスを完了します。

はじめる前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[**Administration（管理）**] > [**System（システム）**] > [**Certificates（証明書）**] > [**Local Certificates（ローカル証明書）**] を選択します。

CA 署名付き証明書をセカンダリ ノードにバインドするには、[**Administration（管理）**] > [**System（システム）**] > [**Server Certificate（サーバ証明書）**] を選択します。

ステップ 2　[**Add（追加）**] > [**Bind CA Certificate（CA 証明書のバインド）**] を選択します。

ステップ 3　[**Browse（参照）**] をクリックして CA 署名付き証明書を選択します（該当する CA 署名付き証明書を選択します）。

ステップ 4　証明書の**フレンドリ名**を指定します。名前を入力しない場合は、*<common name>#<issuer>#<nnnnn>* の形式で自動的に名前が作成されます。ここで、*<nnnnn>* は固有の 5 桁の数値です。

ステップ 5　Cisco ISE に証明書の拡張の検証を許可する場合は、[**Enable Validation of Certificate Extensions（証明書の拡張の検証を許可）**] チェックボックスをオンにします。

（注）　[**Enable Validation of Certificate Extensions（証明書の拡張の検証を許可）**] オプションが有効になっており、インポートする証明書に CA フラグ が true に設定された基本制約拡張が含まれている場合は、キー使用拡張が存在しており、keyEncipherment ビットまたは keyAgreement ビット、あるいはその両方が設定されていることを確認します。

ステップ 6　サブジェクトのいずれかの CN またはサブジェクト代替名の DNS にワイルドカード文字であるアスタリスク（*）が含まれている証明書をバインドするには、[**Allow Wildcard Certificates（ワイルドカード証明書の許可）**] チェックボックスをオンにします。

ステップ 7　[Protocol group（プロトコル グループ）] ボックスで、次のようにします。

- SSL/TLS トンネルを使用する EAP プロトコルでこの証明書を使用するには、[**EAP**] チェックボックスをオンにします。
- この証明書を Cisco ISE Web ポータルの認証に使用するには、[**HTTPS**] チェックボックスをオンにします。

[Management Interface（管理インタフェース）] チェックボックスをオンにする場合は、証明書サブジェクトの一般名の値がノード完全修飾ドメイン名（FQDN）またはワイルドカード表記（ワイルドカード証明書が使用されている場合）に一致していることを確認してください。そうではない場合、バインド操作は失敗します。

[HTTPS] チェックボックスがオンになっている場合は、導入環境内のプライマリ管理ノードが再起動されます。

ステップ 8　既存の証明書を複製した証明書で置き換えるには、[**Replace Certificate（証明書を置き換える）**] チェックボックスをオンにします。証明書のサブジェクトまたは発行者、およびシリアル番号が既存の証明書と同じ場合、その証明書は複製と見なされます。このオプションでは証明書の内容が更新されますが、証明書の既存のプロトコルの選択は保持されます。

ステップ 9　[**Submit（送信）**] をクリックして、CA 署名付き証明書をバインドします。

関連項目

- 「ワイルドカード証明書」（P.E-4）
- 「Cisco ISE へのワイルドカード証明書のインストール」（P.E-10）

ローカル証明書の編集

このページを使用して、ローカル証明書を編集できます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[**Administration（管理）**] > [**System（システム）**] > [**Certificates（証明書）**] > [**Local Certificates（ローカル証明書）**] を選択します。

ローカル証明書をセカンダリ ノードで編集するには、[**Administration（管理）**] > [**System（システム）**] > [**Server Certificate（サーバ証明書）**] を選択します。

ステップ 2　編集する証明書の横にあるチェックボックスをオンにして、[**Edit（編集）**] をクリックします。

ステップ 3　次の項目を編集できます。

- フレンドリ名
- 説明
- プロトコル
- 有効期限 TTL（証明書が自己署名の場合）

ステップ 4　オプションで、この証明書を識別するためのフレンドリ名と説明を入力します。

ステップ 5　[Protocol group（プロトコル グループ）] ボックスで、次のようにします。

- SSL/TLS トンネルを使用する EAP プロトコルでこの証明書を使用するには、[**EAP**] チェックボックスをオンにします。
- この証明書を Cisco ISE Web ポータルの認証に使用するには、[**HTTPS**] チェックボックスをオンにします。

  [HTTPS] チェックボックスがオンになっている場合は、導入環境内のプライマリ管理ノードが再起動されます。

（注）　[Management Interface（管理インタフェース）] チェックボックスをオンにする場合は、証明書サブジェクトの一般名の値がノード完全修飾ドメイン名（FQDN）またはワイルドカード表記（ワイルドカード証明書が使用されている場合）に一致していることを確認してください。一般名の値がブランクの場合、編集操作は失敗します。
たとえば、現在 local_certificate_1 が EAP に対して指定されており、local_certificate_2 の編集時に [EAP] チェックボックスをオンにした場合、local_certificate_2 への変更を保存すると、local_certificate_1 の EAP への関連付けが解除されます。

ステップ 6　自己署名証明書を編集しており、有効期限を延長する必要がある場合は、**[Renew Self Signed Certificate（自己署名証明書の更新）]** チェックボックスをオンにします。

ステップ 7　日、週、月、年単位で、証明書の有効期限の TTL（存続可能時間）を入力します。

ステップ 8　**[Save（保存）]** をクリックして変更を保存します。

関連項目

- 「ワイルドカード証明書」（P.E-4）
- 「ワイルドカードの証明書の作成」（P.E-9）
- 「Cisco ISE へのワイルドカード証明書のインストール」（P.E-10）

ローカル証明書のエクスポート

選択したローカル証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　**[Administration（管理）] > [System（システム）] > [Certificates（証明書）] > [Local Certificates（ローカル証明書）]** を選択します。

ローカル証明書をセカンダリ ノードからエクスポートするには、**[Administration（管理）] > [System（システム）] > [Server Certificate（サーバ証明書）]** を選択します。

ステップ 2　エクスポートする証明書の横にあるチェックボックスをオンにし、**[Edit（編集）]** をクリックします。

ステップ 3　証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント　値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合は、秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE サーバにインポートするときに指定して、秘密キーを復号化する必要があります。

ステップ 4　エクスポートする証明書コンポーネントを選択します。

ステップ 5　秘密キーをエクスポートすることを選択した場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 6　**[OK]** をクリックして、クライアント ブラウザを実行しているファイル システムに証明書を保存します。

証明書のみをエクスポートする場合、証明書は Privacy Enhanced Mail 形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書は Privacy Enhanced Mail 形式の証明書と暗号化された秘密キー ファイルを含む .zip ファイルとしてエクスポートされます。

関連項目

- 「ローカル証明書のインポート」（P.E-16）

証明書署名要求

自分が作成した証明書署名要求（CSR）のリストは、[Certificate Signing Requests（証明書署名要求）] ページで使用できます。CA から署名を取得するには、クライアント ブラウザを実行しているローカル ファイル システムに CSR をエクスポートする必要があります。次に、CA に証明書を送信します。証明書は CA によって署名され、返されます。

（注）　Cisco ISE 導入環境の分散セットアップに複数のノードがある場合は、導入環境内の各ノードから CSR を個別にエクスポートする必要があります。

関連項目

「証明書署名要求のエクスポート」（P.E-24）

証明書署名要求のエクスポート

[Exporting Certificate Signing Requests（証明書署名要求のエクスポート）] ページを使用して、証明書署名要求をエクスポートすることができます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　**[Administration（管理）] > [System（システム）] > [Certificates（証明書）] > [Certificate Signing Requests（証明書署名要求）]** を選択します。

セカンダリ ノードから CSR をエクスポートするには、**[Administration（管理）] > [System（システム）] > [Certificate Signing Requests（証明書署名要求）]** を選択します。

ステップ 2　エクスポートする証明書の横にあるチェックボックスをオンにし、**[Edit（エクスポート）]** をクリックします。

ステップ 3　**[OK]** をクリックして、クライアント ブラウザを実行しているファイル システムにファイルを保存します。

関連項目

- 「ワイルド カード証明書」（P.E-4）

証明書ストア

Cisco ISE 証明書ストアには、信頼に使用される、Simple Certificate Enrollment Protocol（SCEP）用の X.509 証明書が含まれています。証明書ストア内の証明書はプライマリ管理ノードで管理され、Cisco ISE の導入環境内の他のすべてのノードに複製されます。

Cisco ISE はワイルドカード証明書をサポートしています。

Cisco ISE は、次の目的で証明書ストアの証明書を使用します。

- 証明書ベースの管理認証を使用して管理ポータルにアクセスする Cisco ISE 管理者、およびエンドポイントによる認証に使用されるクライアント証明書の検証。
- 導入環境内の Cisco ISE ノード間のセキュアな通信を可能にする。証明書ストアには、導入環境内の各ノードのローカル HTTPS サーバ証明書との信頼を確立するために必要な CA 証明書のチェーンが含まれている必要があります。
  - 自己署名証明書をサーバ証明書に使用する場合は、各ノードの自己署名証明書をプライマリ管理ノードの証明書ストアに配置する必要があります。
  - CA 署名付き証明書をサーバ証明書に使用する場合は、CA ルート証明書だけでなく、信頼チェーン内のすべての中間証明書もプライマリ管理ノードの証明書ストアに配置する必要があります。
- 安全な LDAP 認証を有効にする。SSL を経由してアクセスされる LDAP ID ソースを定義するときに、証明書ストアから証明書を選択する必要があります。
- デバイス ポータルを使用してネットワークでの登録を準備するモバイル デバイスへの配布のため。Cisco ISE は、モバイル デバイス登録をサポートするために、ポリシー サービス ノード（PSN）での SCEP を実装しています。登録するデバイスは、SCEP プロトコルを使用して、PSN にクライアント証明書を要求します。PSN には仲介として動作する登録局（RA）が含まれています。RA は登録からの要求を受信し、検証して、その要求を CA（実際にクライアント証明書を発行する）に転送します。CA は RA に証明書を返し、RA が証明書をデバイスに返します。

  Cisco ISE によって使用される各 SCEP CA は、SCEP RA プロファイルによって定義されます。SCEP RA のプロファイルが作成されると、次の 2 つの証明書が証明書ストアに自動的に追加されます。

  a. CA 証明書（自己署名証明書）

  b. CA によって署名された RA 証明書（証明書要求のエージェントの証明書）。

  SCEP プロトコルでは、これらの 2 つの証明書が RA によって登録デバイスに提供されている必要があります。証明書ストアにこの 2 つの証明書を配置すると、これらのノードの RA が使用するために、証明書がすべての PSN ノードに複製されます。

（注） Cisco ISE にインポートされる X.509 証明書は、Privacy Enhanced Mail（PEM）または Distinguished Encoding Rules（DER）形式である必要があります。 証明書チェーン（つまり、ローカル証明書、およびその証明書に署名する一連の信頼された証明書）が含まれたファイルはインポートすることができますが、特定の制限の対象となります。

関連項目

- 「Simple Certificate Enrollment Protocol プロファイル」（P.E-31）
- 「証明書チェーンのインポート」（P.E-29）
- 「X.509 証明書の有効期限」（P.E-26）
- 「証明書の名前の制約」（P.E-26）

- 「証明書ストアの証明書の表示」（P.E-27）
- 「証明書ストア内の証明書の変更」（P.E-28）
- 「証明書ストアへの証明の追加」（P.E-28）
- 「証明書ストアの証明書の編集」（P.E-28）
- 「証明書ストアからの証明書のエクスポート」（P.E-29）

X.509 証明書の有効期限

X.509 証明書が有効なのは、指定された特定の日付までのみです。証明書ストアの証明書が期限切れになると、その証明書に依存する Cisco ISE 機能が影響を受けます。Cisco ISE は、有効期限が 90 日以内になると、証明書の有効期間の残りについて通知します。この通知は、いくつかの方法で表示されます。

- 配色された有効期限の状態アイコンが、[Certificate Store（証明書ストア）] ページに表示されます。
- 期限切れメッセージが Cisco ISE システム診断レポートに表示されます。
- 有効期限のアラームは、有効期限の 90 日前、60 日前に生成され、有効期限前の最後の 30 日間には毎日生成されます。

証明書ストアには、製造証明書とルート証明書の 2 つのシスコ CA 証明書があります。ルート証明書は製造証明書に署名します。これらの証明書は、デフォルトでは無効になっています。導入環境でエンドポイントとして Cisco IP Phone を使用している場合は、これら 2 つの証明書を有効にして、この電話用にシスコが署名した証明書の認証ができるようにします。

ここでは、次の内容について説明します。

- 「証明書ストアの証明書の表示」（P.E-27）
- 「証明書ストアへの証明の追加」（P.E-28）
- 「証明書ストアの証明書の編集」（P.E-28）
- 「証明書ストアからの証明書のエクスポート」（P.E-29）
- 「証明書チェーンのインポート」（P.E-29）
- 「Cisco ISE のノード間通信のための CA 証明書のインストール」（P.E-30）

証明書の名前の制約

CTL の CA 証明書には名前の制約の拡張が含まれている場合があります。この拡張は、証明書チェーンの後続のすべての証明書のサブジェクト名とサブジェクト代替名フィールドの値の名前空間を定義します。Cisco ISE は、ルート証明書で指定された制約を検査しません。

次の名前の制約がサポートされています。

- ディレクトリ名

  ディレクトリ名の制限は、サブジェクト /SAN のディレクトリ名のプレフィクスです。次に例を示します。

  – 正しいサブジェクト プレフィクス：

    CA 証明書の名前の制約：Permitted: O=Cisco

    クライアント証明書のサブジェクト：O=Cisco,CN=Salomon

– 不正なサブジェクト プレフィクス：

CA 証明書の名前の制約：Permitted: O=Cisco

クライアント証明書のサブジェクト：CN=Salomon,O=Cisco

- DNS
- 電子メール
- URI（URI の制約は、http://、https://、ftp:// または ldap:// のような URI プレフィクスで開始する必要があります）。

次の名前の制約はサポートされていません。

- IP アドレス
- Othername

CA 証明書にサポートされていない制約が含まれており、検証中の証明書に該当のフィールドが含まれていない場合は、Cisco ISE がサポートされない制約を検証できないため、その証明書は拒否されます。

CA 証明書内の名前の制約の定義例を次に示します。

```
X509v3 Name Constraints: critical
               Permitted:
                 othername:<unsupported>
                 email:.stihl.at
                 email:.stihl.be
                 email:.stihl.bg
                 email:.stihl.by
                 DNS:.dir
                 DirName: DC = dir, DC = emea
                 DirName: C = AT, ST = EMEA, L = AT, O = STIHL Group, OU = Domestic
                 DirName: C = BG, ST = EMEA, L = BG, O = STIHL Group, OU = Domestic
                 DirName: C = BE, ST = EMEA, L = BN, O = STIHL Group, OU = Domestic
                 DirName: C = CH, ST = EMEA, L = CH, O = STIHL Group, OU = Service Z100
                 URI:.dir
                 IP:172.23.0.171/255.255.255.255
               Excluded:
                 DNS:.dir
                 URI:.dir
```

受け入れ可能なクライアント証明書のサブジェクトは、次のように上記の定義に一致します。

```
          Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=flovison
```

証明書ストアの証明書の表示

[Certificate Store（証明書ストア）] ページに、Cisco ISE に追加されたすべての CA 証明書が一覧表示されます。CA 証明書を表示するには、スーパー管理者またはシステム管理者である必要があります。

すべての証明書を表示するには、[Administration（管理）] > [System（システム）] > [Certificates（証明書）] > [Certificate Store（証明書ストア）] を選択します。[Certificate Store（証明書ストア）] ページが表示され、すべての CA 証明書の一覧が一覧表示されています。

証明書ストア内の証明書の変更

証明書のステータスが有効になっている必要があります。これにより、Cisco ISE が信頼の確立にこの証明書を使用できるようになります。証明書が証明書ストアにインポートされると、この証明書は自動的に有効になります。

ステップ 1　[**Administration（管理）**] > [**System（システム）**] > [**Certificates（証明書）**] > [**Certificate Store（証明書ストア）**] を選択します。

ステップ 2　有効または無効にする証明書の横にあるチェックボックスをオンにし、[**Change Status（ステータスの変更）**] をクリックします。

証明書ストアへの証明の追加

[Certificate Store（証明書ストア）] ページを使用して、Cisco ISE に CA 証明書を追加することができます。

はじめる前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- ブラウザを実行しているコンピュータのファイル システムに、証明書ストアの証明書が存在することを確認します。証明書は PEM または DER 形式である必要があります。

ステップ 1　[**Administration（管理）**] > [**System（システム）**] > [**Certificates（証明書）**] > [**Certificate Store（証明書ストア）**] を選択します。

ステップ 2　[**Import（インポート）**] をクリックします。

ステップ 3　必要に応じてフィールドの値を設定します。

クライアント証明書ベースの認証が有効の場合は、導入環境内の各ノードのアプリケーション サーバが再起動されます（最初にプライマリ管理ノードのアプリケーション サーバが再起動され、続いて追加のノードのアプリケーション サーバが 1 つずつ再起動されます）。

証明書ストアの証明書の編集

証明書を証明書ストアに追加したら、編集の設定を使用して、その証明書をさらに編集できます。

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[**Administration（管理）**] > [**System（システム）**] > [**Certificates（証明書）**] > [**Certificate Store（証明書ストア）**] を選択します。

ステップ 2　編集する証明書の横にあるチェックボックスをオンにして、[**Edit（編集）**] をクリックします。

ステップ 3　必要に応じて編集可能なフィールドを変更します。

ステップ 4　[**Save（保存）**] をクリックして、証明書ストアに対して行った変更を保存します。

証明書ストアからの証明書のエクスポート

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　[**Administration（管理）**] > [**System（システム）**] > [**Certificates（証明書）**] > [**Certificate Store（証明書ストア）**] を選択します。

ステップ 2　エクスポートする証明書の横にあるチェックボックスをオンにし、[**Edit（エクスポート）**] をクリックします。一度に 1 つの証明書のみをエクスポートできます。

ステップ 3　クライアント ブラウザを実行しているファイル システムに Privacy Enhanced Mail ファイルを保存します。

証明書チェーンのインポート

証明書ストアから受信した証明書チェーンを含む単一のファイルから、複数の証明書をインポートすることができます。ファイル内のすべての証明書は Privacy-Enhanced Mail (PEM) の形式であり、証明書は次の順序に並べられている必要があります。

- ファイル内の最後の証明書は、CA によって発行されたクライアントまたはサーバ証明書である必要があります。
- 前にあるすべての証明書は、ルート CA 証明書と、発行された証明書の署名のチェーンにあるすべて中間 CA 証明書である必要があります。

証明書チェーンのインポートは、次の 2 つのステップで構成される手順です。

ステップ 1　証明書ストアへの証明の追加に記載された操作によって、証明書ストアに証明書チェーン ファイルをインポートします。この操作により、証明書ストアにある最後の 1 つを除き、すべての証明書がファイルからインポートされます。このステップは、プライマリ管理ノードでのみ実行できます。

ステップ 2　CA 署名付き証明書のバインディングに記載された操作によって、証明書チェーン ファイルをインポートします。この操作により、最後の証明書がローカル証明書としてインポートされます。

Cisco ISE のノード間通信のための CA 証明書のインストール

分散導入環境では、セカンダリ ノードを登録する前に、セカンダリ ノードの HTTPS 証明書を検証するために使用する適切な CA 証明書をプライマリ ノードの CTL に入力する必要があります。プライマリ ノードの CTL に入力する手順は、シナリオに応じて異なります。

- セカンダリ ノードで HTTPS 通信に CA 署名付き証明書が使用されている場合は、セカンダリ ノードの CA 署名付き証明書をプライマリ ノードの CTL にインポートできます。
- セカンダリ ノードで HTTPS 通信に自己署名証明書が使用されている場合は、セカンダリ ノードの自己署名証明書をプライマリ ノードの CTL にインポートできます。

（注） セカンダリ ノードをプライマリ ノードに登録した後に、登録されているセカンダリ ノードの HTTPS 証明書を変更する場合は、セカンダリ ノードの HTTPS 証明書の検証に使用できる適切な CA 証明書を取得する必要があります。

関連項目

- 「セカンダリ ノードからプライマリ ノードの CTL への CA 署名付き証明書のインポート」（P.E-30）
- 「セカンダリ ノードからプライマリ ノードの CTL への自己署名証明書のインポート」（P.E-31）

セカンダリ ノードからプライマリ ノードの CTL への CA 署名付き証明書のインポート

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　セカンダリ ノードとして登録するノードの管理ポータルにログインし、HTTPS 通信に使用される CA 署名付き証明書を、クライアント ブラウザを実行しているファイル システムにエクスポートします。

ステップ 2　[Export（エクスポート）] ダイアログボックスで、**[Export Certificate Only（証明書のみをエクスポート）]** オプション ボタンををクリックします。

ステップ 3　プライマリ ノードの管理ポータルにログインして、プライマリ ノードの CTL にセカンダリ ノードの CA 署名付き証明書をインポートします。

関連項目

- 「証明書ストアからの証明書のエクスポート」（P.E-29）
- 「証明書ストアへの証明の追加」（P.E-28）

セカンダリ ノードからプライマリ ノードの CTL への自己署名証明書のインポート

はじめる前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1　セカンダリ ノードとして登録するノードの管理ポータルにログインし、HTTPS 通信に使用される自己署名証明書を、クライアント ブラウザを実行しているファイル システムにエクスポートします。

ステップ 2　[Export（エクスポート）] ダイアログボックスで、**[Export Certificate Only（証明書のみをエクスポート）]** オプション ボタンををクリックします。

ステップ 3　プライマリ ノードの管理ポータルにログインして、プライマリ ノードの CTL にセカンダリ ノードの自己署名証明書をインポートします。

関連項目

- 「ローカル証明書のエクスポート」（P.E-23）
- 「証明書ストアへの証明の追加」（P.E-28）

Simple Certificate Enrollment Protocol プロファイル

ユーザがネットワークで登録できるさまざまなモバイル デバイスの証明書のプロビジョニング機能を有効にするために、1 つ以上の Simple Certificate Enrollment Protocol（SCEP）認証局（CA）プロファイルを設定して、Cisco ISE に複数の CA の場所を指定できます。複数のプロファイルを使用できる利点は、ハイ アベイラビリティが実現できるようになり、指定した CA の場所の間でロード バランシングを実行できることです。特定の SCEP CA への要求に 3 回連続して応答がなかった場合、Cisco ISE は特定のサーバが使用不能であると宣言し、次に負荷が小さく応答時間が短い既知の CA に自動的に移動して、サーバがオンラインに復帰するまで、定期的なポーリングを開始します。

Microsoft SCEP サーバを Cisco ISE と相互運用するように設定する方法については、次を参照してください。

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf.

関連項目

- 「Simple Certificate Enrollment Protocol（SCEP）プロファイルの追加」（P.E-31）
- 「OCSP サービス」（P.E-32）

Simple Certificate Enrollment Protocol（SCEP）プロファイルの追加

ステップ 1　**[Administration（管理）] > [System（システム）] > [Certificates（証明書）] > [SCEP CA Profile（SCEP CA プロファイル）]** を選択します。

ステップ 2　他の SCEP CS プロファイル名と区別するために、プロファイルの**名前**を指定します。

ステップ 3　オプションで、プロファイルの**説明**を入力します。

ステップ 4　ユーザがモバイル デバイスからネットワークにアクセスしたときに Cisco ISE が SCEP CA 要求を転送できる、該当のSCEP CA サーバの **URL** を指定します。

[Submit（送信）] ボタンをクリックしてセッションを終了する前に、オプションで横にある [**Test Connectivity（接続のテスト）**] ボタンを使用して、指定した URL のサーバに Cisco ISE が到達できることを確認できます。（いずれにしても、Cisco ISE ではプロファイルを保存する前に URL がテストされます）。

ステップ 5　[**Submit（送信）**] をクリックします。

参考：
ユーザのデバイスが検証済みの証明書を受信すると、表 E-1 に示すように、証明書はそのデバイスに置かれます。

表 E-1　　デバイス証明書の場所

デバイス	証明書ストレージの場所	アクセス方法
iPhone/iPad	標準の証明書ストア	[Settings（設定）] > [General（一般）] > [Profile（プロファイル）]
Android	暗号化された証明書ストア	エンド ユーザに不可視です。 **（注）** 証明書は、[Settings（設定）] > [Location & Security（ロケーションおよびセキュリティ）] > [Clear Storage（ストレージのクリア）] を使用して削除できます。
Windows	標準の証明書ストア	**/cmd** プロンプトから mmc.exe を起動するか、または証明書スナップインで表示します。
Mac	標準の証明書ストア	[Application（アプリケーション）] > [Utilities（ユーティリティ）] > [Keychain Access（キーチェーン アクセス）]

OCSP サービス

Online Certificate Status Protocol（OCSP）は、x.509 デジタル証明書のステータスのチェックに使用されるプロトコルです。このプロトコルは証明書失効リスト（CRL）に代わるものであり、CRL の処理が必要となる問題に対処します。

Cisco ISE には HTTP を介して OCSP サーバと通信し、認証で証明書のステータスを検証する機能があります。OCSP の設定は、Cisco ISE で設定される任意の認証局（CA）の証明書から参照できる、再利用可能な設定オブジェクトで設定されます。「証明書ストアの証明書の編集」（P.E-28）を参照してください。

CRL 検証または OCSP 検証、あるいはその両方を CA ごとに設定できます。両方を選択すると、Cisco ISE は最初に OCSP を介した検証を実行します。プライマリ OCSP サーバとセカンダリ OCSP サーバの両方で通信の問題が検出された場合、または特定の証明書に対して不明のステータスが返された場合、Cisco ISE は CRL チェックの実行に切り替えます。

ここでは、次の内容について説明します。

OCSP 証明書のステータスの値

OCSP サービスは、指定された証明書要求に対して次の値を返します。

- [Good（良い）]：ステータスの問い合わせに対する肯定的な応答を示します。証明書が失効していないこと、および状態が次の時間間隔（存続可能時間）値までは良好であることを示します。
- [Revoked（失効）]：証明書は失効しています。
- [Unknown（不明）]：証明書のステータスが不明です。これは、OCSP が特定の証明書 CA を処理するように設定されていない場合に発生することがあります。
- [ERROR（エラー）]：OCSP 要求に対する応答を受信しませんでした。

関連項目

「OCSP 統計情報カウンタ」（P.E-36）

OCSP ハイ アベイラビリティ

Cisco ISE では CA ごとに最大 2 つの OCSP サーバを設定でき、それらのサーバはプライマリおよびセカンダリ OCSP サーバと呼ばれます。各 OCSP サーバ設定には、次のパラメータが含まれます。

- [URL]：OCSP サーバの URL。
- [Nonce（ナンス）]：要求で送信される乱数。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。
- [Validate Response（応答の検証）]：Cisco ISE は OCSP サーバから受信した応答署名を検証します。

Cisco ISE がプライマリ OCSP サーバと通信しているときに、タイムアウト（5 秒）が発生した場合、Cisco ISE はセカンダリ OCSP サーバに切り替えます。

Cisco ISE はプライマリ サーバの再使用を試行する前に、設定可能な期間セカンダリ OCSP サーバを使用します。

OCSP エラー

3 つの一般的な OCSP 障害のシナリオは次のとおりです。

1. 失敗した OCSP キャッシュまたは OCSP クライアント側（Cisco ISE）の障害
2. 失敗した OCSP 応答側のシナリオ。例：
   a. 最初のプライマリ OCSP 応答側が応答せず、セカンダリ OCSP 応答側が Cisco ISE OCSP 要求に応答する。
   b. Cisco ISE OCSP 要求からエラーまたは応答が受信されない。

   OCSP レスポンダが、Cisco ISE OCSP 要求への応答を提供しないか、失敗の OCSP 応答のステータスを返している可能性があります。OCSP 応答のステータス値は次のようになります。
   - tryLater
   - signRequired
   - unauthorized
   - internalError
   - malformedRequest

   OCSP 要求に対する多数の日時チェック、署名の有効性チェックなどがあります。詳細については、「*RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP (RFC 2560 X.509 インターネット パブリック キー インフラストラクチャのオンライン証明書ステータスのプロトコル：OCSP)*」を参照してください。これにはエラー ステータスを含む、可能性があるすべてのステータスが説明されています。
3. 失敗した OCSP レポート

OCSP サービスの追加

[Add OCSP（OCSP の追加）] ページを使用して、Cisco ISE に新しい OCSP サービスを追加することができます。

ステップ 1　[**Administration（管理）**] > [**System（システム）**] > [**Certificates（証明書）**] > [**OCSP Services（OCSP サービス）**] を選択します。

ステップ 2　[**Add（追加）**] をクリックします。

ステップ 3　OCSP サービスの名前と説明を入力します。

ステップ 4　ハイ アベイラビリティを有効にする場合は、[**Enable Secondary Server（セカンダリ サーバの有効化）**] チェックボックスをオンにします。

ステップ 5　ハイ アベイラビリティの次のいずれかのオプションを選択します。

- [Always Access Primary Server First（常にプライマリ サーバに最初にアクセスする）]：このオプションは、セカンダリ サーバへの移動を試行する前にプライマリ サーバをチェックする場合に使用します。プライマリが以前にチェックされ、応答しないことが確認されている場合にも、Cisco ISE はセカンダリ サーバに移動する前にこのプライマリ サーバへの要求の送信を試行します。

- [Fallback to Primary Server After Interval（時間を置いてプライマリ サーバにフォールバックする）]：このオプションは、Cisco ISE がセカンダリ サーバに移動してから、再度プライマリ サーバにフォールバックする場合に使用します。この場合、その他の要求はすべてスキップされ、テキスト ボックスで設定した期間セカンダリ サーバが使用されます。許可される時間の範囲は 1 ～ 999 分です。

ステップ 6　プライマリおよびセカンダリの OCSP サーバの URL または IP アドレスを指定します。

ステップ 7　次のオプションをオンまたはオフにします。

- [Nonce（ナンス）]：ナンスが OCSP 要求の一部として送信されるように設定できます。ナンスには、OCSP 要求の擬似乱数が含まれます。応答で受信される数値が要求に含まれる数値と同じであることが検証されます。このオプションにより、リプレイ アタックで古い通信を再利用できないことが保証されます。
- [**Validate Response Signature**（応答の署名の検証）]：OCSP レスポンダは次のいずれかの署名を使用して応答に署名します。
  - CA 証明書
  - CA 証明書とは別の証明書

  Cisco ISE が応答の署名を検証するためには、OCSP レスポンダが応答を証明書とともに送信する必要があります。そうでない場合、応答の検証は失敗し、証明書のステータスを信頼にすることはできません。RFC に従い、OCSP は異なる証明書を使用して応答に署名できます。このことは、OCSP が検証のために、Cisco ISE の応答に署名した証明書を送信する限り当てはまります。OCSP が Cisco ISE で設定されているものとは異なる証明書を使用して応答に署名した場合、応答の検証は失敗します。

ステップ 8　キャッシュ エントリの存続可能期間を分単位で入力します。

OCSP サーバからの各応答には nextUpdate 値が含まれています。この値は、証明書のステータスがサーバで次にいつ更新されるかを示します。OCSP 応答がキャッシュされるとき、2 つの値（1 つは設定から、もう 1 つは応答から）が比較され、この 2 つの最小値の期間だけ応答がキャッシュされます。nextUpdate 値が 0 の場合、応答はまったくキャッシュされません。

Cisco ISE は設定された期間 OCSP 応答をキャッシュします。キャッシュは複製されず、永続的でもないため、Cisco ISE が再起動するとキャッシュはクリアされます。

次の理由により、OCSP キャッシュは OCSP 応答を保持するために使用されます。

- 既知の証明書に関する OCSP サーバからのネットワーク トラフィックと負荷を低減するため
- 既知の証明書のステータスをキャッシュすることによって Cisco ISE のパフォーマンスを向上させるため

ステップ 9　OCSP サービスに接続されているすべての認証局のエントリをクリアするには、[**Clear Cache（キャッシュを消去）**] をクリックします。

導入環境内で、キャッシュのクリアはすべてのノードと相互作用して、処理を実行します。このメカニズムにより、導入環境内のすべてのノードが更新されます。

OCSP 統計情報カウンタ

OCSP カウンタは、OCSP サーバのデータと健全性のロギングおよびモニタリングに使用されます。ロギングは 5 分ごとに実行されます。syslog メッセージが Cisco ISE モニタリング ノードに送信され、ローカル ストア（前の 5 分間のデータが格納されている）に保存されます。メッセージが送信された後、カウンタは次の間隔について再計算されます。つまり、5 分後に、新しい 5 分間の間隔が再度開始されます。

表 E-2 に OCSP syslog メッセージとその説明を示します。

表 E-2　OCSP Syslog メッセージ

メッセージ	説明
OCSPPrimaryNotResponsiveCount	応答のないプライマリ要求の数
OCSPSecondaryNotResponsiveCount	応答のないセカンダリ要求の数
OCSPPrimaryCertsGoodCount	プライマリ OCSP サーバを使用して返された所定の CA の「良好な」証明書の数
OCSPSecondaryCertsGoodCount	プライマリ OCSP サーバを使用して返された所定の CA の「良好な」ステータスの数
OCSPPrimaryCertsRevokedCount	プライマリ OCSP サーバを使用して返された所定の CA の「失効した」ステータスの数
OCSPSecondaryCertsRevokedCount	セカンダリ OCSP サーバを使用して返された所定の CA の「失効した」ステータスの数
OCSPPrimaryCertsUnknownCount	プライマリ OCSP サーバを使用して返された所定の CA の「不明の」ステータスの数
OCSPSecondaryCertsUnknownCount	セカンダリ OCSP サーバを使用して返された所定の CA の「不明の」ステータスの数
OCSPPrimaryCertsFoundCount	プライマリの送信元からのキャッシュ内に見つかった証明書の数
OCSPSecondaryCertsFoundCount	セカンダリの送信元からのキャッシュ内に見つかった証明書の数
ClearCacheInvokedCount	一定間隔の後にキャッシュのクリアがトリガーされた回数
OCSPCertsCleanedUpCount	一定間隔の後にクリーンアップされたキャッシュ エントリの数
NumOfCertsFoundInCache	キャッシュから実行された要求の数
OCSPCacheCertsCount	OCSP キャッシュ内に見つかった証明書の数

OCSP のモニタリング

OCSP サービス データを OCSP モニタリング レポートの形式で表示することができます。Cisco ISE レポート作成の詳細については、『*Cisco Identity Services Engine User Guide, Release 1.2*（*Cisco Identity Services Engine ユーザ ガイド リリース 1.2*）』を参照してください。

インライン ポスチャ ノードの証明書の設定

サポートされる任意のアプライアンス プラットフォームでインライン ポスチャ ノード リリース 1.2 の ISO イメージをインストールし、セットアップ プログラムを実行したら、インライン ポスチャ ノードを導入環境に追加する前に、それらのノードの証明書を設定する必要があります。インライン ポスチャ ノードの証明書の設定は CLI からのみ行います。

はじめる前に

- インライン ポスチャ ノードは、プライマリ管理ノードを認証したのと同じ認証局（CA）から認証する必要があります。
- インライン ポスチャ ノードのアクティブ/スタンバイ ペアを導入する場合は、アクティブおよびスタンバイの両方のインライン ポスチャ ノードで証明書を設定します。

ステップ 1　CLI を使用してインライン ポスチャ ノードにログインします。

ステップ 2　次のコマンドを入力します。

pep certificate server generatecsr

ステップ 3　証明書署名要求（CSR）とともに既存の秘密キー ファイルを使用するには **n** を入力し、新規の秘密キーファイルを使用するには **y** を入力します。

ステップ 4　必要なキー サイズを入力します。

ステップ 5　証明書に署名するダイジェストのタイプを入力します。

ステップ 6　国番号名（2 文字のコード）を入力します。

ステップ 7　州、都市、組織、組織単位の値を入力します。

ステップ 8　一般名を入力します。一般名はホスト名と同じです。完全修飾ドメイン名（FQDN）を入力します。たとえば、ホスト名が *IPN1*、DNS ドメイン名が *cisco.com* である場合は、一般名として *IPN1.cisco.com* を入力します。

ステップ 9　電子メール アドレスを入力します。

ステップ 10　END CERTIFICATE REQUEST タグの後に、空白行を含むテキスト ブロック全体をコピーします（復帰改行を含みます）。

ステップ 11　プライマリ管理ノードの証明書に署名した CA にこの CSR を送信します。

Microsoft の CA を使用している場合は、署名要求の送信時に証明書のテンプレートとして [Web Server（Web サーバ）] を選択します。

（注）　リリース 1.2 でサポートされるのはサーバ認証のみです。証明書に署名するために他の CA を使用する場合は、キーの拡張用途でサーバ認証のみが指定されていることを確認します。

ステップ 12　DER または Base64 形式の署名付き証明書をダウンロードし、FTP サーバにコピーします。

ステップ 13　インライン ポスチャ ノードの CLI から次のコマンドを入力します。

copy ftp://*a.b.c.d*/*ipn1.cer* **disk:**

ここで、*a.b.c.d* は FTP サーバの IP アドレスであり、*ipn1.cer* はインライン ポスチャ ノードに追加する CA 署名付き証明書です。

ステップ 14　FTP サーバのユーザ名とパスワードを入力します。

ステップ 15　インライン ポスチャ ノードの CLI から次のコマンドを入力します。

pep certificate server add

ステップ 16　再起動するアプリケーションに対して **y** を入力します。

ステップ 17　最後の CSR に証明書をバインドするために **y** を入力します。

ステップ 18　CA 署名付き証明書の名前を入力します。

インライン ポスチャ アプリケーションが再起動します。これで、プライマリ管理ノードにインライン ポスチャのノードを登録できるようになりました。詳細については、『*Cisco Identity Services Engine User Guide, Release 1.2（Cisco Identity Services Engine ユーザ ガイド リリース 1.2）*』を参照してください。

INDEX

す

せ

て

と

は

ひ

ふ

ま

ら