Cisco Security Manager 4.5 インストレーション ガイド

2013 年 11 月 15 日

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。
各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices）をご覧ください。

Text Part Number: OL-30012-01-J

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

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

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

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

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

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

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

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

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

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

Cisco Security Manager 4.5 インストレーション ガイド

© 2005-2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

はじめに ix

対象読者 ix

表記法 x

製品マニュアル xi

マニュアルの入手方法およびテクニカル サポート xi

CHAPTER 1 概要 1-1

コンポーネント アプリケーションの概要 1-1

Common Services 1-1

Security Manager 1-2

Auto Update Server 1-2

Performance Monitor 1-3

Resource Manager Essentials 1-3

関連アプリケーションの概要 1-3

イベント管理のイネーブル化の影響 1-4

CHAPTER 2 ライセンス 2-1

Security Manager 4.5 をインストールおよび使用するために必要なライセンスの決定 2-1

Security Manager 4.5 の新規インストール 2-1

Security Manager 4.0、4.0.1、4.1、4.2、4.3 または 4.4 からのアップグレード 2-2

Security Manager 3.3 または 3.3.1 からのアップグレード 2-2

Security Manager 3.2、3.2.1、または 3.2.2 からのアップグレード 2-2

Security Manager のライセンスの説明 2-2

Standard および Professional 2-2

90 日間の評価ライセンス 2-3

Standard から Professional へのアップグレード ライセンス 2-4

バージョン アップグレード ライセンス 2-4

差分（「追加」）ライセンス 2-4

アクティブ サーバとスタンバイ サーバ 2-4

コンポーネント アプリケーションに対するライセンス 2-4

デバイス数 2-5

マルチ コンテキスト モードのスタンドアロン ファイアウォール ブレードの例 2-7

ASA ロード バランシング クラスタに関連するライセンスの例 2-8
Security Manager またはコンポーネント アプリケーションに対するライセンスのインストール 2-8
Security Manager またはコンポーネント アプリケーションに対するライセンスの更新 2-8
ライセンスに関するその他のマニュアル 2-8
API ライセンス 2-8
ライセンスに関する支援 2-9

CHAPTER 3 **要件と依存関係 3-1**
必要なサービスとポート 3-1
Windows ファイアウォール設定スクリプト 3-3
サーバの要件および推奨事項 3-4
地域と言語のオプションと関連設定について 3-8
SAN ストレージの使用 3-9
iSCSI ボリュームの要件 3-9
クライアントの要件 3-10

CHAPTER 4 **サーバのインストール準備 4-1**
サーバのパフォーマンスとセキュリティを向上させるためのベスト プラクティス 4-1
インストール準備状況チェックリスト 4-3

CHAPTER 5 **サーバ アプリケーションのインストールとアップグレード 5-1**
必要なサーバ ユーザ アカウントについて 5-1
Remote Desktop Connection または VNC を使用したサーバ アプリケーションのインストール 5-2
Security Manager サーバ、Common Services、および AUS のインストール 5-2
サーバ アプリケーションのアップグレード 5-5
Security Manager の保留データが送信および承認されることの確認 5-8
プロパティ ファイルに対する変更の復元 5-9
リモート アップグレード時のデータベースのバックアップ 5-10
CLI を使用したサーバ データベースのバックアップ 5-11
サーバ データベースの復元 5-12
アップグレード後の必要な変更の実施 5-13
新しいコンピュータまたはオペレーティング システムへの Security Manager の移行 5-14
Security Manager の更新 5-15
サービス パックとポイント パッチの入手 5-16
サーバ アプリケーションのアンインストール 5-17
サーバ アプリケーションのダウングレード 5-18

CHAPTER 6 クライアントのインストールと設定 6-1
Web ブラウザ クライアントの設定 6-1
HTTP/HTTPS プロキシ例外 6-2
ブラウザ クッキーの設定 6-2
Internet Explorer の設定 6-2
Firefox の設定 6-4
プリファレンス ファイルの編集 6-4
ディスク キャッシュのサイズの編集 6-4
ポップアップ ブロックのディセーブル化またはホワイト リストの作成 6-4
JavaScript のイネーブル化 6-5
最新ウィンドウ内の新しいタブ上でのオンライン ヘルプの表示と以降の要求に対する既存のウィンドウの再利用 6-5
サードパーティ製ツールでの例外のイネーブル化と設定 6-6
Security Manager クライアントのインストールに関するヒント 6-6
Security Manager クライアントのインストール 6-7
インストールを阻止するセキュリティ設定の処理 6-10
非デフォルト HTTP または HTTPS ポートの設定 6-10
以前のバージョンのクライアントからアップグレードできない 6-11
クライアントのパッチング 6-11
アプリケーションへのログイン 6-12
Security Manager クライアントを使用した Security Manager へのログイン 6-12
Web ブラウザを使用したサーバ アプリケーションへのログイン 6-13
Security Manager クライアントのアンインストール 6-14

CHAPTER 7 インストール後のサーバ タスク 7-1
すぐに実行すべきサーバ タスク 7-1
必要なプロセスが動作しているかどうかの確認 7-2
MRF を使用した Security Manager プロセスのヒープ サイズの設定 7-2
デフォルト コンフィギュレーション 7-3
コンフィギュレーション コマンド 7-4
プロセスに対するヒープ サイズの設定 7-4
1. 既存の設定の保存 7-4
2. 既存の設定の読み取り 7-5
3. 設定の変更 7-5
プロセスに対するヒープ サイズの設定の要約 7-6
ユーザがヒープ サイズの再設定を必要とする一般的なシナリオ 7-6
シナリオ 1 7-6
シナリオ 2 7-6
シナリオ 3 7-7

シナリオ 4 7-7
現行のサーバ セキュリティに関するベスト プラクティス 7-7
インストールまたはアップグレードの確認 7-7
関連情報 7-8

CHAPTER 8 ユーザ アカウントの管理 8-1
アカウントの作成 8-1
ローカル アカウント 8-1
ACS アカウント 8-2
非 ACS アカウント 8-2
ユーザの権限 8-3
Security Manager ACS 権限 8-4
CiscoWorks ロールについて 8-6
CiscoWorks Common Services デフォルト ロール 8-6
認可タイプの選択および Common Services 内のユーザへのロールの割り当て 8-7
Cisco Secure ACS ロールについて 8-9
Cisco Secure ACS デフォルト ロール 8-10
Cisco Secure ACS ロールのカスタマイズ 8-11
Security Manager 内の権限とロールのデフォルトの関連付け 8-11
Security Manager と Cisco Secure ACS の統合 8-12
ACS 統合要件 8-13
初期 Cisco Secure ACS セットアップ手順の概要 8-14
Cisco Secure ACS で実行する統合手順 8-15
Cisco Secure ACS でのユーザとユーザ グループの定義 8-15
Cisco Secure ACS での管理対象デバイスの AAA クライアントとしての追加 8-17
Cisco Secure ACS での管理制御ユーザの作成 8-21
CiscoWorks で実行する統合手順 8-21
CiscoWorks でのローカル ユーザの作成 8-22
システム識別ユーザの定義 8-22
CiscoWorks での AAA セットアップ モードの設定 8-23
ACS ステータス通知用の SMTP サーバとシステム管理者の電子メール アドレスの設定 8-25
Daemon Manager の再起動 8-25
Cisco Secure ACS でのユーザ グループへのロール割り当て 8-26
NDG を使用しないユーザ グループへのロールの割り当て 8-26
NDG とロールのユーザ グループへの関連付け 8-27
Security Manager と ACS の相互作用のトラブルシューティング 8-29
複数のバージョンの Security Manager と 1 つの ACS の使用 8-29
ACS モードで認証に失敗する 8-29

読み取り専用アクセスが付与されたシステム管理者 8-30
ACS の変更が Security Manager に表示されない 8-30
ACS で設定されたデバイスが Security Manager に表示されない 8-31
Cisco Secure ACS が到達不能になった後の Security Manager での作業 8-31
Cisco Secure ACS へのアクセスの復元 8-31
マルチホーム デバイスに伴う認証の問題 8-32
NAT 境界の背後に設置されたデバイスに伴う認証の問題 8-32
Common Services 4.2.2 を使用するローカル RBAC 8-32
認証モードの設定 8-33
ユーザ管理 8-33
グループ管理 8-34
ロール管理 8-34

APPENDIX A トラブルシューティング A-1
Cisco Security Manager サービスの起動要件 A-1
必要な TCP ポートと UDP ポートの包括的リスト A-2
Security Manager サーバのトラブルシューティング A-4
インストール中のサーバ障害 A-4
インストール後のサーバ障害 A-5
アンインストール中のサーバ障害 A-8
Security Manager クライアントのトラブルシューティング A-10
インストール中のクライアント障害 A-10
インストール後のクライアント障害 A-13
サーバ セルフテストの実行 A-16
サーバ トラブルシューティング情報の収集 A-17
サーバ プロセス ステータスの表示と変更 A-18
サーバ上の全プロセスの再起動 A-18
サーバ インストール ログ ファイルの確認 A-18
Symantec の共存問題 A-19
Windows アップデートのインストール後の問題 A-19
高度な暗号化による ASA デバイスへの接続の問題 A-20
インストール時に使用する Activation.jar のポップアップ表示 A-20
Windows のデフォルト ユーザ テンプレートのロケールを米国英語に設定する方法 A-21

APPENDIX B Image Manager の権限マトリクス B-1

INDEX

はじめに

Cisco Security Manager（Security Manager）を使用すれば、大規模から小規模までのネットワークに配置されたシスコ デバイス上でセキュリティ ポリシーを管理できます。また、Security Manager 上で共有可能なオブジェクトとポリシーを使用して、数台のデバイスから何千台ものデバイスまでを管理できます。さらに、Security Manager は、ユースケースに合わせて最適化された複数の設定ビューをサポートしたり、複数のプラットフォーム固有設定のプロビジョニングをサポートしたり、デバイス分類機能を提供したりします。

（注） *Cisco Security Management Suite* には、Security Manager の他に、ネットワーク上のセキュリティ脅威のモニタリング、識別、分離、および無効化を可能にするアプライアンス製品の *Cisco Security Monitoring, Analysis, and Response System* が付属しています。http://www.cisco.com/en/US/products/ps6241/index.html を参照してください。

このマニュアルの目的は次のとおりです。

- Security Manager と関連アプリケーションのインストールに関するハードウェア要件とソフトウェア要件を列挙します。
- インストール対象のソフトウェア アプリケーションとそれらのインストール環境に関する重要な概念について説明します。
- Security Manager サーバおよび Auto Update Server のインストール手順と Security Manager の専用クライアント ソフトウェアのインストール手順を示します。
- インストール後に、新しくインストールされたアプリケーションを正しく使用するために必要な作業について説明します。
- インストール中またはインストール後に発生する可能性のある問題の理解とトラブルシューティングを支援します。

（注） アプリケーションをインストールする前に、Cisco.com 上で、インストールする実際のソフトウェア コンポーネントに最適なリリース ノート（最新情報として）を読むことを推奨します。リリース ノートには、このマニュアルに対する修正や追加、または、計画、準備、インストール、または展開に影響を与えるその他の情報が含まれている場合があります。「製品マニュアル」（P.xi）を参照してください。

対象読者

このマニュアルは、セキュリティ インフラストラクチャをインストール、設定、展開、および管理するネットワーク担当者およびセキュリティ担当者を対象とします。

表記法

このマニュアルでは、次の表記法を使用しています。

項目	表記法
コマンドおよびキーワード	**太字**
ユーザが値を指定する変数	*イタリック体*
表示されるセッションおよびシステムの情報	`screen` フォント
ユーザが入力する情報	**太字の screen** フォント
ユーザが入力する変数	*イタリック体の screen* フォント
メニュー項目およびボタン名	**太字**
本文中でのメニュー項目を選択する操作の記述	[Option] > [Network Preferences]
表中でのメニュー項目を選択する操作の記述	[Option] > [Network Preferences]

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

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。

製品マニュアル

シスコのマニュアルおよびその他の資料は、Cisco.com 上で入手できます。表 1 に、Cisco Security Manager および Auto Update Server に関する入手可能なマニュアルを、読む順番に示します。

表 1　　Security Manager のマニュアル

マニュアル タイトル	利用形式
『Release Notes for Cisco Security Manager』 Auto Update Server に関する情報も記載されています。	http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html
『Supported Devices and Software Versions for Cisco Security Manager』 Auto Update Server に関するサポート情報が記載されています。	http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html
『Cisco Security Manager インストレーション ガイド』 （このマニュアル）	http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html
『User Guide for Cisco Security Manager』	http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html
『User Guide for Auto Update Server』	http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html
文脈依存オンライン ヘルプ	GUI でオプションを選択して、[Help] をクリックします。

マニュアルの入手方法およびテクニカル サポート

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

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

概要

この章は、次の内容で構成されています。

- 「コンポーネント アプリケーションの概要」（P.1-1）
- 「関連アプリケーションの概要」（P.1-3）

コンポーネント アプリケーションの概要

Security Manager インストーラを使用すれば、特定のアプリケーションをインストールできます。その場合は、他のアプリケーションのインストールが要求されます。この項では、次のアプリケーションとその相互依存性について説明します。

- 「Common Services」（P.1-1）
- 「Security Manager」（P.1-2）
- 「Auto Update Server」（P.1-2）

Common Services

Common Services 4.2.2 は、Security Manager 4.5 とデフォルトでバンドルされます。

Common Services は、データ保存、ログイン、ユーザ ロール定義、アクセス特権、セキュリティ プロトコル、およびナビゲーション用のフレームワークを提供します。また、インストール、データ管理、イベントおよびメッセージ処理、およびジョブおよびプロセス管理用のフレームワークも提供します。Common Services が Security Manager に供給する必須サーバ側コンポーネントは次のとおりです。

- SSL ライブラリ
- 組み込み型 SQL データベース
- Apache Web サーバ
- Tomcat サーブレット エンジン
- CiscoWorks ホームページ
- バックアップ/復元機能

（注） Common Services 内の Device and Credential Repository（DCR）機能は、Security Manager 4.5 ではサポートされていません。[Groups] タブも、Security Manager 4.5 の [Common Services] ページから削除されます。

Security Manager

Cisco Security Manager は、シスコのネットワーク デバイスとセキュリティ デバイス上でファイアウォール、VPN、および Intrusion Prevention System（IPS; 侵入防御システム）セキュリティ サービスを設定するために設計されたエンタープライズクラスの管理アプリケーションです。また、Cisco Security Manager は、ポリシーベースの管理テクニックを使用することによって、すべての規模のネットワーク（小規模ネットワークから何千ものデバイスで構成された大規模ネットワークまで）で使用できます。さらに、Cisco Security Manager は、Cisco Security Monitoring, Analysis, and Response System（MARS）と連動します。この 2 つの製品を組み合わせて使用することによって、設定管理、セキュリティ モニタリング、分析、および移行を処理する包括的なセキュリティ管理ソリューションが実現します。

（注）　Security Manager の詳細については、http://www.cisco.com/go/csmanager にアクセスしてください。Cisco Security MARS の詳細については、http://www.cisco.com/go/mars にアクセスしてください。

Security Manager を使用するには、サーバ ソフトウェアとクライアント ソフトウェアをインストールする必要があります。

Security Manager が提供する機能は次のとおりです。

- 1 つのデスクトップからの VPN、ファイアウォール、および侵入防御システムのサービスレベルおよびデバイスレベルのプロビジョニング
- デバイス設定のロールバック
- トポロジ マップ形式でのネットワークの可視化
- ワークフロー モード
- 事前定義およびユーザ定義の FlexConfig サービス テンプレート
- 統合インベントリ、資格情報、分類、および共有ポリシー オブジェクト
- 関連アプリケーションに対する便利な相互起動アクセス
  - サーバ ソフトウェアをインストールすると、Adaptive Security Device Manager（ASDM）、PIX Device Manager（PDM）、Security Device Manager（SDM）、および IPS Device Manager（IDM）の各デバイス マネージャの読み取り専用バージョンもインストールされます。
  - ASA デバイスと PIX デバイスを Security Manager から Auto Update Server（AUS）に追加できます。
- ASA デバイスと IPS デバイスによって生成されたイベントの統合モニタリング。Event Viewer 機能を使用することによって、ASA デバイスと IPS デバイスからのイベントを選択的にモニタ、表示、および検査できます。

Auto Update Server

AUS のインストールを選択した場合は、それを Security Manager がインストールされたサーバまたは別のサーバ（DMZ 内のサーバなど）にインストールできます。AUS と Security Manager は、デバイス インベントリ情報とその他のデータを共有できます。AUS は、ブラウザベースのユーザ インターフェイスを使用するため、Common Services が必要です。

AUS を使用すれば、自動アップデート機能を使用する PIX Security Appliance（PIX）デバイスと Adaptive Security Appliance（ASA）デバイス上のデバイス コンフィギュレーション ファイルとソフトウェア イメージをアップグレードできます。AUS は、デバイス設定、設定アップデート、デバイス OS アップデート、および定期設定確認に使用可能な設定のプル モデルをサポートします。加えて、自

動アップデート機能と組み合わせて動的 IP アドレスを使用するサポート対象デバイスは、AUS を使用してコンフィギュレーション ファイルをアップグレードしたり、デバイス情報とステータス情報を渡したりできます。

AUS は、リモート セキュリティ ネットワークのスケーラビリティを向上させ、リモート セキュリティ ネットワークの維持コストを削減し、アドレス指定されたリモート ファイアウォールを動的に管理できるようにします。

AUS の詳細については、Security Manager サイトの http://www.cisco.com/go/csmanager にある AUS のマニュアルを参照してください。

Performance Monitor

バージョン 4.3 から、Cisco Security Manager には、コンパニオン アプリケーションの Performance Monitor は付属していません。

Resource Manager Essentials

バージョン 4.3 から、Cisco Security Manager には、コンパニオン アプリケーションの CiscoWorks Resource Manager Essentials（RME）は付属していません。

関連アプリケーションの概要

Security Manager に統合して追加の機能とメリットを提供するその他のアプリケーションがシスコから提供されています。

- **Cisco Security Monitoring Analysis and Response System（MARS）**：Security Manager は、MARS を使用してファイアウォールと IPS に関するポリシーとイベント間の相互リンクをサポートします。Security Manager クライアントを使用して、特定のファイアウォール ルールまたは IPS 署名を強調表示し、それらのルールまたは署名に関するイベントの表示を要求します。MARS を使用すれば、Security Manager で、ファイアウォール イベントまたは IPS イベントを選択して、一致するルールまたは署名の表示を要求できます。このようなポリシー / イベント相互リンクは、特に、ネットワーク接続のトラブルシューティング、未使用ルールの特定、および署名調整活動に役立ちます。ポリシー / イベント相互リンク機能の詳細が、『*User Guide for Cisco Security Manager*』に記載されています。MARS の詳細については、http://www.cisco.com/go/mars にアクセスしてください。
- **Cisco Secure Access Control System（ACS）**：オプションで、Security Manager ユーザの認証と認可に ACS を使用するように Security Manager を設定できます。ACS は、きめ細かなロールベースの認可制御に関するカスタム ユーザ プロファイルの定義と、特定のデバイス セットにユーザを制限する機能をサポートします。Security Manager と ACS の統合の設定方法については、「Security Manager と Cisco Secure ACS の統合」（P.8-12）を参照してください。ACS の詳細については、http://www.cisco.com/go/acs にアクセスしてください。
- **Cisco Configuration Engine**：Security Manager は、デバイス設定の展開メカニズムとしての Cisco Configuration Engine の使用をサポートします。Security Manager は、差分コンフィギュレーション ファイルを Cisco Configuration Engine に渡して、保存を依頼し、デバイスから読み取れるようにします。Cisco IOS ルータ、PIX ファイアウォール、ASA デバイスなどの Dynamic Host Configuration Protocol（DHCP）サーバを使用するデバイスは、Cisco Configuration Engine に設定（およびイメージ）のアップデートを依頼します。Security Manager と Configuration Engine を使用すれば、静的 IP アドレスを持つデバイスを管理することもできます。静的 IP アドレスを使用している場合は、ネットワーク上でデバイスを特定して、Configuration Engine 経由で

設定を展開できます。Security Manager と一緒に使用可能な Configuration Engine リリースについては、http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html でこの製品バージョンに関するリリース ノートを参照してください。Configuration Engine の詳細については、http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/index.html にアクセスしてください。

イベント管理のイネーブル化の影響

Security Manager サーバ上でイベント管理をイネーブルにした場合は、そのサーバを次のサービスに使用できません。

- CiscoWorks Common Services 上の Syslog

Security Manager のインストールまたはアップグレード時に、Common Services syslog サービス ポートが 514 から 49514 に変更されます。あとで Security Manager がアンインストールされた場合、ポートは 514 に戻されません。ポートに関する追加情報は、表 3-1（P.3-2）と表 A-1（P.A-2）で入手できます。

オペレーティング システムで使用できる RAM の容量が不足している場合は、Event Viewer がディセーブルにされます（表 3-3（P.3-4）で詳細を参照）。ただし、Common Services syslog サービス ポートは変更されます。

ライセンス

この章の情報を使用して、Cisco Security Manager 4.5 をインストールおよび使用するために必要なライセンスを決定できます。さらにこの章では、スタンダード版、プロフェッショナル版、評価版など、入手可能な各種ライセンスについても説明しています。

いくつかの注釈を除き、この章ではライセンス インストールについて説明しません。第 5 章「サーバ アプリケーションのインストールとアップグレード」を参照してください。

この章では、どの Security Manager サーバ ライセンスが必要かを判断する手引きとして、デバイス数について説明します。

この章の最後には、Cisco Security Manager API を使用するシスコ パートナーの API ライセンスに関する情報を示します。

Security Manager 4.5 をインストールおよび使用するために必要なライセンスの決定

必要なライセンスは、新規にインストールするのか、前のバージョンからアップグレードするのかによって異なります。

- 「Security Manager 4.5 の新規インストール」（P.2-1）
- 「Security Manager 4.0、4.0.1、4.1、4.2、4.3 または 4.4 からのアップグレード」（P.2-2）
- 「Security Manager 3.3 または 3.3.1 からのアップグレード」（P.2-2）
- 「Security Manager 3.2、3.2.1、または 3.2.2 からのアップグレード」（P.2-2）

Security Manager 4.5 の新規インストール

Cisco Security Manager 4.5 を新規でインストールするには、該当する Cisco Security Manager 4.5 ライセンスを購入する必要があります。Cisco Security Manager ライセンスの詳細については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html にある製品速報を参照してください。

Security Manager 4.0、4.0.1、4.1、4.2、4.3 または 4.4 からのアップグレード

Security Manager 4.0、4.0.1、4.1、4.2、4.3 または 4.4 からアップグレードするためにライセンスを適用する必要はありません。既存のライセンスが有効です。

Security Manager 3.3 または 3.3.1 からのアップグレード

Cisco Security Manager 3.3 または 3.3.1 からアップグレードするお客様は、該当する Cisco Security Manager 4.5 ライセンスまたはバージョン アップグレード ライセンスを購入する必要があります。Cisco Security Manager ライセンスの詳細については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html にある製品速報を参照してください。

Security Manager 3.2、3.2.1、または 3.2.2 からのアップグレード

Cisco Security Manager 3.2、3.2.1、または 3.2.2 からアップグレードするお客様は、該当する Cisco Security Manager 4.5 ライセンスまたはバージョン アップグレード ライセンスを購入する必要があります。Cisco Security Manager ライセンスの詳細については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html にある製品速報を参照してください。

Security Manager のライセンスの説明

基本ライセンスとして Standard と Professional の 2 種類が提供されており、無料の 90 日間評価ライセンスもあります。

Standard および Professional

Cisco Security Manager 4.5 に対して使用可能な基本ライセンスのリストについては、表 2-1 を参照してください。

表 2-1　使用可能な基本ライセンスのリスト

ライセンス名	ライセンスの略称	管理可能なデバイスの台数（「デバイス数」（P.2-5）を参照）
Standard-5	ST5	5
Standard-10	ST10	10
Standard-25	ST25	25
Professional-50	PRO50	50
Professional-100	PRO100	100
Professional-250	PRO250	250

Professional 基本バージョンと Standard 基本バージョンの比較については、表 2-2 を参照してください。

表 2-2　Professional 基本バージョンと Standard 基本バージョンの比較

機能	Professional でサポートされるか	Standard でサポートされるか
50、100、および 250 台単位でデバイス数を追加する差分（「追加」）デバイス ライセンス パッケージのサポート	Yes	No
Cisco Catalyst 6500 および 7600 シリーズ スイッチと関連サービス モジュールの管理に対するサポート	Yes	No
ファイアウォール サービス モジュールの管理に対するサポート	Yes	No
一時ライセンス（有効期限付きのライセンス）に対するサポート	Yes	No（永久ライセンスのみサポート）

基本ライセンスを取得するには、Cisco.com のユーザ ID を保有（または取得）している必要があり、Cisco.com 上でソフトウェアのコピーを登録する必要があります。登録時に、購入したソフトウェア パッケージ内部の *Software License Claim Certificate* に貼られている Product Authorization Key（PAK; 製品認証キー）を入力する必要があります。

- Cisco.com の登録ユーザの場合は、http://www.cisco.com/go/license から始めてください。
- Cisco.com の登録ユーザでない場合は、http://tools.cisco.com/RPF/register/register.do から始めてください。

使用開始から 90 日以内のできるだけ早い時期に、製品の連続使用を保証するために必要なデバイスの台数分の Security Manager を登録する必要があります。アプリケーションを起動するたびに、評価ライセンスの残りの日数が表示され、評価期間中のアップグレードが促されます。評価期間が終了すると、ライセンスをアップグレードするまでログインできなくなります。

登録後に、基本ソフトウェア ライセンスが、指定した電子メール アドレスに送られてきます。ライセンスは安全な場所に保管してください。

90 日間の評価ライセンス

インストール時にライセンスを入力しないと、そのインストールは評価版になります。また、インストール時に [Evaluation Only] を選択することもできます。「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2）を参照してください。

評価ライセンスでは、使用可能なデバイスが 50 台までに制限されます。

評価ライセンスでは、Professional 版ライセンスと同じ権限が与えられます。ただし、差分ライセンスを評価版に適用することはできません。

Standard から Professional へのアップグレード ライセンス

Standard から Professional へのアップグレード ライセンスを使用できます。基本ライセンスが Standard-25（「ST25」）ライセンスの場合にのみ適用できます。

バージョン アップグレード ライセンス

3.3 などの以前のメジャー バージョンから Security Manager 4.5 にアップグレードする必要がある場合は、バージョン アップグレード ライセンスを購入できます。

バージョン アップグレード ライセンスは複数種類あります。各ライセンスは、以前のバージョンの特定の基本ライセンスと対応します。特定のアップグレード ライセンス（たとえば PRO50U）は、それに対応する基本ライセンス（たとえば PRO50）を以前のバージョンの Security Manager に適用していた場合にのみ使用できます。それ以外のアップグレード ライセンスは受け入れられません。

差分（「追加」）ライセンス

ご使用の基本ライセンスが（Standard 版や評価版ではなく）Professional 版の場合、差分（「追加」）ライセンスを購入して、管理可能なデバイスの台数を増やすことができます。差分ライセンスは、必要な数だけ購入できます。

以前のバージョンに対する差分（「追加」）ライセンスは、現在のバージョンに対しても有効です。たとえば、Security Manager 4.4 に対する Professional-50 ライセンスを保有している場合、4.3 の差分デバイス ライセンスを使用できます。

差分ライセンスは、50、100、および 250 台単位でデバイス数を追加できます。

アクティブ サーバとスタンバイ サーバ

Cisco Security Manager ライセンスでは、Cisco Security Manager の使用は 1 台のサーバ上でのみ許可されます。常に 1 台のサーバのみがアクティブになる場合は、スタンバイの Cisco Security Manager サーバ（ハイ アベイラビリティ設定やディザスタ リカバリ設定などで使用される）に別個のライセンスを用意する必要はありません。これは、ハイ アベイラビリティ（HA）が使用されている場合にも当てはまります。

（注） スタンバイ サーバを使用するユーザは、定期的にアクティブ サーバからデータベースを手動で復元する必要があります。

コンポーネント アプリケーションに対するライセンス

一部のコンポーネント アプリケーションには、ライセンス ファイルは必要ありません。

- Common Services にはライセンス ファイルが必要ありません。
- Auto Update Server にライセンス ファイルは必要ありません。

デバイス数

Security Manager では、次のいずれかをデバイス インベントリに追加すると、（ライセンスで許可される台数から）デバイス数が 1 つ消費されます。

- 物理デバイス
- セキュリティ コンテキスト
- 仮想センサー

Advanced Inspection and Prevention Security Services Module（AIP-SSM）、IDS Network Module、IPS Advanced Integration Module（IPS AIM）、およびホスト デバイスにインストールされた AIP-SSC 5 および Catalyst 6500 または 7600 以外のデバイスに対してサポートされるその他のモジュールは、デバイス数を消費しません。ただし、追加の仮想センサー（最初のセンサーの後に追加されたセンサー）はデバイス数を消費します。

Firewall Services Module（FWSM）または ASA デバイスの場合は、モジュール自体がデバイス数を消費し、セキュリティ コンテキストが追加されるたびに追加のデバイス数を消費します。たとえば、2 つのセキュリティ コンテキストを含む FWSM は、モジュール用、管理コンテキスト用、2 つめのセキュリティ コンテキスト用の 3 つのデバイス数を消費します。

特殊なケースとして、管理対象外デバイスがあります。Security Manager では、管理対象外デバイスをデバイス インベントリに追加することができます。管理対象外デバイスとは、デバイス プロパティ内で [Manage in Cisco Security Manager] を選択解除したデバイスのことです。管理対象外デバイスはデバイス数を消費しません。

別のクラスの管理対象外デバイスは、トポロジ マップに追加されたオブジェクトです。[Map] > [Add Map Object] コマンドを使用して、ネットワーク クラウド、ファイアウォール、ホスト、ネットワーク、ルータなどのさまざまなタイプのオブジェクトをマップに追加できます。このようなオブジェクトは、デバイス インベントリに含まれないため、デバイス数を消費しません。

どの Security Manager サーバ ライセンスを必要とするかを決定するため判断すべき、デバイス数を決定するには、表 2-3 を参照してください。

ヒント　必要な Security Manager サーバ ライセンスを決定することを目的として、デバイスは、Security Manager 4.5 に対して Security Manager 4.3 と 4.4 の場合と同様にカウントされます。

表 2-3　デバイス数の決定

デバイス	モード（コンテキストとも呼ばれる）	デバイス数（またはライセンス数、単にライセンスとも呼ばれる）	コメント
除外デバイス			
Advanced Inspection and Prevention Security Services Module（AIP-SSM）		0	追加の仮想センサー（最初のセンサーの後に追加された）が 1 ライセンスを個別に消費します。
IDS ネットワーク モジュール		0（ただし、次の列のコメントを参照）	追加の仮想センサー（最初のセンサーの後に追加された）が 1 ライセンスを個別に消費します。

表 2-3　デバイス数の決定

デバイス	モード（コンテキストとも呼ばれる）	デバイス数（またはライセンス数、単にライセンスとも呼ばれる）	コメント
IPS Advanced Integration Module（IPS AIM）		0	
ホスト デバイスにインストールされた AIP-SSC 5 および Catalyst 6500 または 7600 以外のデバイスに対してサポートされるその他のモジュール		0	
スタンドアロン ファイアウォール デバイス			
任意のスタンドアロン ファイアウォール デバイス	シングル コンテキスト モード	1	
任意のスタンドアロン ファイアウォール デバイス	マルチ コンテキスト モード	*c*、ここで *c* はシステム コンテキスト以外のコンテキスト数です	
スタンドアロン IPS デバイス			
任意のスタンドアロン IPS デバイス		*n*、ここで *n* は仮想センサーの数で、仮想センサー vs0 が含まれます	追加の仮想センサー（最初のセンサーの後に追加された）が 1 ライセンスを個別に消費します。
非スタンドアロン IPS デバイス			
IPS モジュール、IPS ブレードおよび IPS 仮想マシン		*n*、ここで *n* は仮想センサーの数で、仮想センサー vs0 が含まれます	IPS モジュール、IPS ブレードおよび IPS 仮想マシンは Security Manager で個別に検出されます。 IPS 仮想マシンは 5512-X、5515-X、5525-X、5545-X および 5555-X である Cisco ASA 5500 シリーズの適応型セキュリティ アプライアンスで使用されます。
ファイアウォール ブレード			
任意のスタンドアロン ファイアウォール ブレード	シングル コンテキスト モード	1	
任意のスタンドアロン ファイアウォール ブレード	マルチ コンテキスト モード	*c*、ここで *c* はシステム コンテキスト以外のコンテキスト数です	**例：** この表の後のマルチ コンテキスト モードのスタンドアロン ファイアウォール ブレードの例を参照してください。

表 2-3　デバイス数の決定

デバイス	モード（コンテキストとも呼ばれる）	デバイス数（またはライセンス数、単にライセンスとも呼ばれる）	コメント
フェールオーバー構成のファイアウォール			
フェール オーバー構成の任意のファイアウォール	シングル コンテキスト モード	1	
フェール オーバー構成の任意のファイアウォール	マルチ コンテキスト モード	*c*、ここで *c* はシステム コンテキスト以外のコンテキスト数です	
ASA フェールオーバー構成に含まれる IPS モジュールまたは仮想マシン			
各 IPS デバイス		*n*、ここで *n* は仮想センサーの数で、仮想センサー vs0 が含まれます	追加の仮想センサー（最初のセンサーの後に追加された）が 1 ライセンスを個別に消費します。
ASA ロード バランシング クラスタに関連するライセンス			
各 ASA ロード バランス クラスタ	シングル コンテキスト モード	*N*、ここで *N* はシングル コンテキスト ASA クラスタ内のノード数です	システムと管理コンテキストで、1 個のコンテキストを表します
各 ASA ロード バランス クラスタ	マルチ コンテキスト モード	*N* * *c*、ここで *N* はマルチ コンテキスト ASA クラスタ内のノード数を、*c* はコンテキストの数です	システムと管理コンテキストで、1 個のコンテキストを表します。 「ASA ロード バランシング クラスタに関連するライセンスの例」も参照してください。

マルチ コンテキスト モードのスタンドアロン ファイアウォール ブレードの例

ここでは、デバイス数を理解するうえで役立つコンテキストの例を示します。

次のコマンドが 2 つのセキュリティ コンテキスト（admin および ctx1）とともに、ファイアウォール システム上のシステム コンテキストで実行されました。

```
r41-appinfra-arsenal# sh context
Context Name Class Interfaces Mode URL
*admin default GigabitEthernet3/2, Routed disk0:/admin.cfg
Management0/0
ctx1 default Routed disk0:/ctx1.cfg

Total active Security Contexts: 2
r41-appinfra-arsenal# sh context count

Total active Security Contexts: 2
```

ASA ロード バランシング クラスタに関連するライセンスの例

ここでは、マルチ コンテキスト モードの ASA ロード バランシング クラスタのデバイス数の例を示しています。

```
3 Nodes with 4 security contexts each: License  Count = 3 * 5 = 15.
```

Security Manager またはコンポーネント アプリケーションに対するライセンスのインストール

Security Manager のインストール中に、ライセンス情報の入力を求められます。「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2）を参照してください。

Common Services および AUS のインストール中に、ライセンス情報の入力を求められることはありません。Common Services にはライセンス ファイルが必要ありません。Auto Update Server にライセンス ファイルは必要ありません。

Security Manager またはコンポーネント アプリケーションに対するライセンスの更新

Security Manager またはコンポーネント アプリケーションに対するライセンス ファイルの更新方法については、「Security Manager の更新」（P.5-15）を参照してください。

ライセンスに関するその他のマニュアル

使用可能なライセンスの種類やサポートされているアップグレード パスに関する詳細の他、購入可能な Cisco Software Application Support サービス契約については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html で Security Manager の最新メジャー リリースの製品速報を参照してください。

API ライセンス

API を使用するシスコ パートナーは、API ライセンスを保有している必要があります。API ライセンスには、次の 2 種類があります。

- 開発者ライセンス。これは、開発者がそれぞれの製品を Security Manager と統合するために使用できる 90 日間のライセンスです。
- 製品ライセンス。これは、特定のサードパーティ製品を使用するエンド カスタマーに必要なライセンスです。

（注）　API の評価ライセンスはありません。開発者ライセンスと製品ライセンスはいずれも、API を使用するシスコ パートナーが明示的に注文する必要があります。

Northbound API ライセンスの注文可能部品 ID（PID）は L-CSMPR-API です。

ライセンスに関する支援

Security Manager のライセンスに関する問題については、Cisco Technical Assistance Center（TAC）の Licensing Department にお問い合わせください。

- 電話：+1（800）553-2447
- 電子メール：licensing@cisco.com
- http://www.cisco.com/tac

要件と依存関係

Security Manager は、スタンドアロン製品として、あるいは、Security Manager インストーラで選択可能な、または Cisco.com からダウンロード可能なオプション アプリケーションを含む、他のいくつかの Cisco Security Management Suite アプリケーションと組み合わせてインストールして使用できます。インストールと動作に関する要件は、サーバ上に存在する他のソフトウェアと Security Manager の使用方法によって異なります。

ヒント ネットワーク内のすべての管理サーバとすべての管理対象デバイス上の日付と時刻の設定を同期させることを推奨します。NTP サーバを使用する方法があります。同期化は、ネットワーク上のログ ファイル情報を相互に関連付けたり、分析したりする場合に重要になります。

この章の項では、Security Manager、Auto Update Server などのサーバ アプリケーションと Security Manager クライアント ソフトウェアのインストールに関する要件と依存関係について説明します。

- 「必要なサービスとポート」（P.3-1）
- 「Windows ファイアウォール設定スクリプト」（P.3-3）
- 「サーバの要件および推奨事項」（P.3-4）
- 「クライアントの要件」（P.3-10）

必要なサービスとポート

サーバが関連アプリケーションを実行しているクライアントやサーバと通信できるようにするには、必要なポートがイネーブルで、サーバ上の Security Manager とその関連アプリケーションから使用できることを保証する必要があります。

開く必要のあるポートは、CiscoWorks for AAA と外部サーバ（ACS など）のどちらを使用しているかと、Security Manager を特定の他のアプリケーションと相互作用するように設定しているかどうかによって異なります。

- **必要な基本ポート**：表 3-1 に、非デフォルト ポートを使用するための設定がカスタマイズされていないという前提で、開く必要のある基本ポートを示します。CiscoWorks for AAA（ユーザ認可）サービスを使用しているが、オプション アプリケーションは使用していない場合は、これらのポートだけを、開く必要のあるポートにする必要があります。

表 3-1　Security Manager サーバ上で開く必要のある基本ポート

通信	サービス	プロトコル	ポート	入力	出力
Security Manager クライアントと Security Manager サーバ間	HTTP、HTTPS	TCP	1741/443	X	—
Security Manager クライアントと製品に同梱されたデバイス マネージャ（ASDM など）間	HTTPS	TCP	443	X	—
IPS 署名とエンジンのアップデートをダウンロードするための Security Manager と Cisco.com 間	HTTP	TCP	80	—	X
	HTTPS	TCP	443	—	X
Security Manager サーバとデバイス間 **ヒント** HTTPS ポートと SSH ポートは必要ですが、1 つ以上のデバイス用のトランスポート プロトコルとして Telnet を使用する場合にのみ Telnet ポートを開きます。Telnet ではパスワードがクリアテキストで転送されるため、Telnet の使用は推奨できません。Telnet ポートは開かないようにしてください。	HTTPS	TCP	443	—	X
	SSH	TCP	22	—	X
	Telnet	TCP	23	—	X
IOS デバイス上での設定ロールバック動作用の Security Manager サーバとデバイス間	TFTP	UDP	69	X	X
Security Manager と電子メール サーバ間 このポートは、電子メール通知を提供可能な機能のいずれかに関する電子メール通知を設定する場合にのみ必要です。	SMTP	TCP	25	—	X
Security Manager Event Viewer で使用される Syslog サービス	syslog	UDP	514	X	—
Health and Performance Monitor	HTTP、HTTPS	TCP	2012 および 4444	X	X

- **オプション アプリケーションに必要なポート**：Security Manager を他のアプリケーションと一緒に使用している場合は、表 3-2 に示すように、他のポートも開く必要があります。実際に使用するアプリケーションに必要なポートのみを開きます。

表 3-2　オプション サーバ アプリケーションに必要なポート

通信	サービス	プロトコル	ポート	入力	出力
Security Manager Server と CS-MARS 間	HTTPS	TCP	443	X	X
Security Manager サーバと Cisco Secure Access Control Server（ACS）間	HTTP、HTTPS	TCP	• 2002 • ACS サーバ上でポート制限がイネーブルになっている場合は、HTTP/HTTPS 通信の範囲内ですべてのポートを許可します。 • ポート制限がディセーブルになっている場合は、Security Manager サーバと ACS 間のすべての HTTP/HTTPS トラフィックを許可します。	—	X

表 3-2　オプション サーバ アプリケーションに必要なポート （続き）

通信	サービス	プロトコル	ポート	入力	出力
Security Manager サーバと外部 AAA サーバ（非 ACS モードで設定可能）間	RADIUS LDAP Kerberos	TCP	1645、1646、1812（新規）、389、636（SSL）、88	—	X
Security Manager サーバと Configuration Engine 間	HTTPS	TCP	443	—	X
Security Manager サーバと AUS 間	HTTPS	TCP	443	—	X
デバイスと AUS 間。イメージと設定の読み取りに使用されます。	HTTP	TCP	1751	X	—
Security Manager サーバと TMS サーバ間	FTP	TCP	21	—	X
クライアント システム上で動作しているインターネットブラウザと Security Manager または AUS サーバ上のブラウザ インターフェイス間。	HTTP、 HTTPS	TCP	1741/443	X	—

Windows ファイアウォール設定スクリプト

バージョン 4.4 以降から、Security Manager にはサーバのインストーラに Windows ファイアウォール設定スクリプトが含まれます。このスクリプトは、Windows ファイアウォールが正しく安全に機能するために必要なポートを開閉するプロセスを自動化します。これは、Security Manager サーバを強化する目的で行われます。

インストール時にこのスクリプトは *NMSROOT* にコピーされますが、実行されません。このスクリプトを手動で実行して、Security Manager サーバで Windows ファイアウォールを設定できます。これにより不要なポートをブロックし、サーバを保護します。*NMSROOT* は Security Manager インストール ディレクトリへのパスです。デフォルトは **C:\Program Files\CSCOpx** です。

このスクリプトは、Security Manager がタスクを実行するために必要な「IN」ポートのみ開きます。したがって、「Firewall.txt」ファイルには Security Manager に必要最小限のポートが含まれます。後で他のポートを開く必要あることが判明した場合には、それを実行できます。

Windows ファイアウォールのスクリプトを実行するには、次の手順に従います。

ステップ 1　Powershell スクリプトが制限なしで実行できることを確認してください。

a. Powershell コマンドライン ツールを開きます。

b. コマンド「Set-ExecutionPolicy Unrestricted」を実行します。

ステップ 2　NMSROOT でコマンド プロンプトを開き、firewall.bat を実行します。

a. 出力はフォルダ NMSROOT/log に表示されます。

b. Windows.FW_Config.wfw はスクリプトを実行する前の Windows ファイアウォール設定のバックアップです。

c. initialfirewallsettings.txt は、スクリプトを実行する前に開いていたポートを示します。

d. finalfirewallsettings.txt は、スクリプトの実行後に開いているポートを示します。

ステップ 3　Windows ファイアウォールを有効にし、プライベート ネットワーク設定を使用するには、[Control Panel] > [Windows Firewall] > > [Turn Windows Firewall on or off] > [General tab] を選択します。

ステップ 4　セキュリティの Powershell スクリプトの無効化：

a.　Powershell コマンドライン ツールを開きます。

b.　コマンド「Set-ExecutionPolicy Restricted」を実行します。

ステップ 5　（任意）Advanced Security による Windows ファイアウォールを使用して、追加したファイアウォールを検証します（Windows 2008 R2 Enterprise Server SP1（64 ビット）では入手できますが、Windows 2008 Enterprise Server（Service Pack 2）（64 ビット）では入手できません）

サーバの要件および推奨事項

特に明記されている場合を除き、この項はすべてのアプリケーション（Security Manager および Auto Update Server）に適用されます。

Security Manager をインストールするには、管理者またはローカル管理権限を持つユーザになる必要があります。このことは、クライアントだけをインストールする場合にも当てはまります。

Security Manager は制御環境下の専用サーバにインストールすることを推奨します。ベスト プラクティスと関連ガイダンスについては、第 4 章「サーバのインストール準備」を参照してください。

推奨サーバ

Security Manager は、表 3-3 に示すコンポーネントを搭載した Cisco UCS C210 M2 サーバ上にインストールすることを推奨します。Cisco Unified Computing System（UCS）の詳細については、http://www.cisco.com/go/ucs を参照してください。

インストール時の回避事項

- プライマリやバックアップのドメイン コントローラにアプリケーションをインストールしないこと。Windows ドメイン コントローラ上での Common Services の使用はサポートされていません。
- 暗号化されたディレクトリにアプリケーションをインストールしないこと。Common Services はディレクトリの暗号化をサポートしていません。
- Terminal Services がアプリケーション モードでイネーブルになっている場合、アプリケーションをインストールしないこと。このような場合は、Terminal Services をディセーブルにしてから、サーバを再起動して、インストールする必要があります。Common Services は、Terminal Services のリモート管理者モードしかサポートしていません。

表 3-3　サーバのハードウェア要件と推奨事項

コンポーネント	説明
オペレーティング システム	強く推奨：Windows 2008 R2 Enterprise Server SP1（64 ビット）。 その他のサポートされるオペレーティング システム： • Windows 2008 Enterprise Server（Service Pack 2）（64 ビットのみ）。 サポートされている言語は英語と日本語のみです。詳細については、「地域と言語のオプションと関連設定について」（P.3-8）を参照してください。 サーバと Sybase データベース ファイルを連動させるためには、Microsoft ODBC Driver Manager 3.510 以降も必要です。インストールされた ODBC バージョンを確認するには、ODBC32.DLL を探して右クリックしてから、ショートカット メニューで [Properties] を選択します。ファイルのバージョンが [Version] タブに一覧表示されます。

表 3-3　サーバのハードウェア要件と推奨事項 （続き）

コンポーネント	説明
システム ハードウェア	• プロセッサ：Intel Quadcore Xeon 5500 シリーズ以上 • 1280 x 1024 以上の解像度を持つカラー モニタと 16 ビット色に対応したビデオ カード AUS-only サーバの場合は、1024 x 768 の解像度で十分です。 • DVD-ROM ドライブ • 1 Gbps ネットワーク アダプタ • キーボード • マウス
メモリ（RAM）	Security Manager のすべての機能を使用するには、少なくとも 16 GB が必要です。これよりもメモリ容量が少ないと、イベント管理やレポート管理などの機能に影響が出ます。 特に、オペレーティング システムで使用可能な RAM の容量が 8 GB 未満の場合は、イベント管理と Report Manager がインストール時にディセーブルになります。 OS で使用可能なメモリが 8 ～ 12 GB の場合は、イベント管理とレポート管理を使用しないことを前提として、それらを無効にすることができます。そのようなシステムでは、コンフィギュレーション管理を使用することができます。 **ヒント** イベント管理をオフにするには、次のパスに従います。[Configuration Manager] > [Tools] > [Security Manager Administration] > [Event Management] > [Enable Event Management] >（チェックボックスをオフにする）。 **ヒント** レポート管理をオフにするには、レポート管理アプリケーションを終了します。 推奨はできませんが、インストールの完了後に Security Manager クライアントからロー メモリ システムに対してイベント管理とレポート管理をイネーブルにできます（[Tools] > [Security Manager Administration] > [Event Management] を選択します）。ロー メモリ システム上でイベント管理とレポート管理をイネーブルにすると、アプリケーション全体のパフォーマンスに深刻な影響が及ぶ可能性があることに注意してください。 AUS を別のサーバにインストールする場合は、次の最小用件が適用されます。 • AUS-only サーバ：4 GB。4 GB より大きくすることを推奨します。
ファイル システム	NTFS
ディスク最適化	Diskeeper 2010 サーバ これは推奨事項であり、必要条件ではありません。パフォーマンス低下の原因がディスクのフラグメンテーションにある場合は、ディスク最適化によりパフォーマンスが向上します。

表 3-3　サーバのハードウェア要件と推奨事項 （続き）

コンポーネント	説明
ハード ドライブ スペース	RAID 構成で適切な組み合わせの HDD を使用して、必要なディスク領域を確保します。必要なディスク領域は次のとおりです。 • OS パーティション用に 100 GB を推奨します。 • アプリケーション（Security Manager）パーティション用に 150 GB を推奨します。Security Manager のインストールのみに必要な*最小*空きディスク領域は 7 GB です。この要件を満たしていないと、インストールは中断されます。 **（注）** OS とアプリケーションは別々のパーティションにインストールすることを強く推奨します。 **（注）** ハイ アベイラビリティ（HA）モードで Veritas を使用する場合、上記のアプリケーション パーティション、およびその他のイベント ストア パーティションは関係しない場合があります。詳細については、該当する Security Manager ハイ アベイラビリティ マニュアル（http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html）と Veritas マニュアルを参照してください。 • 独立したパーティション上に Event Viewer 用のログ ストレージとして 1.0 TB の追加領域: Event Viewer を使用する場合にのみ必要な条件です。この独立したパーティションは、直接接続ストレージ デバイス上に作成することを推奨します。 • 1.0 TB 以上の追加領域：イベント記録をイネーブルにする場合にのみ必要な条件です。イベント記録機能では、（長期間の保存などにより）プライマリ ストレージの容量を超えるログ ストレージが必要になると、セカンダリのイベント ストレージが作成されます。このセカンダリ イベント ストアには、プライマリ ストレージに設定されたサイズよりも大きいサイズが要求されます。そのため、イベント記録を使用するには、1.0 TB 以上の追加のディスク領域が必要です。プライマリとセカンダリのイベント ストアは両方とも SAN 上に配置できますが、最適なパフォーマンスを実現するために、プライマリ ストア パーティションは直接接続ストレージ（DAS）上に作成することを推奨します。SAN ストレージの詳細については、「SAN ストレージの使用」（P.3-9）を参照してください。 パフォーマンス向上のために、RAID 10 の使用を推奨します。必要ならば、RAID 5 も使用できます。 **ヒント** • 連続 10,000 イベント / 秒（EPS）の場合は、1 日に約 86 GB の圧縮ディスク スペースが消費されます。イベント ストア（プライマリ / セカンダリ）に割り当てられたディスク領域の 90 % がいっぱいになった段階でログ ロールオーバーが発生します。ディスクのサイズが小さいほど、ロールオーバーの発生が早くなります。予想 EPS レートとロールオーバー要件に基づいて、イベント管理の使用時に最小ディスク サイズを増減できます。
IP アドレス	1 つの静的 IP アドレス。動的アドレスはサポートされません。 **ヒント** サーバに複数の IP アドレスが設定されている場合は、インストール前に複数のネットワーク インターフェイス カードのいずれかをディセーブルにする必要がありません。

表 3-3　サーバのハードウェア要件と推奨事項 （続き）

コンポーネント	説明
仮想メモリ（ページング ファイル）	1.5 x インストールされているメモリ。これは、Windows プラットフォームに関する Microsoft の推奨事項です。シスコの要件ではありません。メモリ ページングは、システムに搭載されたメモリが負荷を処理するのに足りない場合にのみ発生します。 **注意** Windows Server 2008 では [Automatically manage paging file size for all drives] チェックボックスをオフにする必要があります。このチェックボックスは、[Computer] > [Properties] > [Advanced System Settings] > [Performance] > [Settings] > [Advanced] > [Virtual Memory] > [Change] にあります。
ウイルス対策	リアルタイム保護がディセーブルになっていること。これは推奨事項であり、必要条件ではありません。システムにはアンチウイルス アプリケーションをインストールできますが、パフォーマンス低下の原因となるため、リアルタイム保護をディセーブルにすることを推奨します。サーバの負荷が小さい時間帯にクイック スキャンを実行するようにスケジューリングすることもできます。
ブラウザ	次のいずれかが必要です。 • Internet Explorer 7.0（この表の始めに示したオペレーティング システムを使用する場合）。 • Internet Explorer 8.0（この表の始めに示したオペレーティング システムを使用し、互換表示のみで使用する場合）。 • Internet Explorer 9.0（この表の始めに示したオペレーティング システムを使用し、互換表示のみで使用する場合）。 **ヒント** Internet Explorer 8 または 9 で互換表示を使用するには、[Tools] > [Compatibility View Settings] に移動し、[website to be displayed in Compatibility View] として Security Manager サーバを追加します。 **（注）** クライアントをダウンロードするために Internet Explorer（任意のバージョン）を使用する場合は、次の設定が正しいかどうかを確認します。Internet Explorer > [Tools] > [Internet Options] > [Advanced] > [Security] で、[Do not save encrypted pages to disk] チェックボックスをオフにします。この設定が正しくない（つまり、チェックボックスがオン）場合、クライアントをダウンロードしようとすると失敗します。 • Firefox 13.0.x 以降（この表の始めに示したオペレーティング システムを使用する場合）。
Java プラグイン	JRE をインストールするための要件はありません。Java スクリプトが Web ブラウザでイネーブルになっている必要があります。
オプションの仮想化ソフトウェア	オプションとして、VMware ESX 4.1、VMware ESXi 4.1、VMware ESXi 5.0、ESXi 5.1、または ESXi 5.1 Update 1 を実行しているシステム上にアプリケーションをインストールできます。 Security Manager と一緒に使用する仮想マシンには、非仮想化サーバを使用する場合の容量以上のメモリを割り当てる必要があります。仮想化パフォーマンスを向上させるように設計されたテクノロジーを使用した新世代 CPU（Intel-VT や AMD-V CPU など）の使用が推奨されています。 **ヒント** 複数の CPU を VM イメージに割り当てます。1 つの CPU しか使用していない場合は、システム バックアップなどの一部のプロセスに異常に長い時間がかかる可能性があります。

地域と言語のオプションと関連設定について

Security Manager は、米国だけをサポートします。Windows の英語および日本語版。[Start] メニューから、Windows のコントロール パネルを開いて、地域と言語を設定するパネルを開き、デフォルト ロケールを設定します （日本語バージョンの Windows では言語として英語がサポートされません）。

ヒント　詳細な手順については、「Windows のデフォルト ユーザ テンプレートのロケールを米国英語に設定する方法」（P.A-21）を参照してください。

（注）　Security Manager をインストールする前に、デフォルトのシステム ロケールを米国英語に変更する必要があります。デフォルト システム ロケールを変更し、サーバをリブートしても、デフォルト プロファイルは変更されません。現在のユーザは、適切な設定をするだけでは十分ではありません。これは、Security Manager はすべての Security Manager サーバ プロセスを実行する新しいアカウント（「casuser」）を作成するためです。

加えて、サーバのオペレーティング システム（Windows Server 2008）内の地域と言語のオプションを正しく設定する必要があります。また、他の言語を使用するキーボードなどの周辺デバイスは、Security Manager の動作に影響する可能性があります。

次のリストに、Security Manager のインストールを成功させるために従う必要のある地域と言語のオプションと関連設定を示します。

- サーバ ロケールは米国である必要があります。英語または日本語。
- 他の言語を使用するキーボードなどの周辺デバイスの使用は避ける必要があります。このようなデバイスはサーバにも接続しないでください。
- サーバへの非コンソール RDP セッションを使用している場合はサーバ設定を妨げないように注意する必要があります。非コンソール RDP を使用してサーバに接続している場合は、RDP クライアント マシンのロケールがサーバに適用される可能性があります。
- 地域と言語のオプションをチェックして、非 Unicode プログラム用に選択された言語が英語（米国）になっていることを確認する必要があります。その選択パスは、[Control Panel] > [Regional and Language Options] > [Advanced] > [Language for non-Unicode Programs] です。
- Windows レジストリのシステム ロケールがサポートされている言語であることを確認する必要があります。これを変更するには、次の手順に従ってください。

a. コマンド ウィンドウで、**regedit.exe** または **regedt32.exe** のいずれかのコマンドを実行します。

b. localname がサポートされていることを確認します。次の例は米国の場合です。English:

\HKEY_USERS\.DEFAULT\Control Panel\International

LocaleName を en-US に変更します

（注）　パスとファイル名に使用可能な文字は、英語のアルファベットに制限されています。パスとファイル名に対して日本語はサポートされていません。Windows 日本語 OS システムでファイルを選択する場合は、通常のファイル区切り文字 \ がサポートされますが、これは円記号（U+00A5）として表示されることがあることに注意する必要があります。

SAN ストレージの使用

十分な I/O 速度と容量を備えている SAN ストレージであれば、Security Manager で使用することができます。次に、Security Manager 内でストレージを必要とする主な項目とともに、サーバに直接搭載されたディスク ストレージを使用する以外に選択可能なストレージ オプションを示します。

- Security Manager インストール フォルダ（CSCOpx およびサブフォルダ）：アプリケーションの最適なインストール先はローカル ドライブです。ただし、インストール フォルダは、直接接続ストレージ（DAS）にすることも、ブロックベースの SAN ストレージ（FC、FCoE、iSCSI）にすることもできます。Security Manager のハイ アベイラビリティ設定（『*High Availability Installation Guide for Cisco Security Manager*』を参照）には、共有クラスタ ボリュームが必要です。
- Event Manager サービス用のプライマリ ストレージ：Event Viewer を使用してイベントを監視する場合、プライマリ ストレージの場所を指定する必要があります。プライマリ ストレージは、直接接続ストレージ（DAS）にすることも、ローカル ドライブとしてマップされたブロック ストレージ（SAN プロトコル：FC、FCoE、iSCSI）にすることもできます。
- Event Manager サービス用の拡張ストレージ：拡張ストレージの場所は、SAN ストレージ上に存在すると想定されます。拡張ストレージは、直接接続ストレージ（DAS）にするか、ローカル ドライブとしてマップされたブロック ストレージ（SAN プロトコル：FC、FCoE、iSCSI）にする必要があります。

ヒント

- CIFS と NFS はサポートされていません。
- サポートされているネットワーク ストレージ タイプは、VMware 設定でもサポートされます。

iSCSI ボリュームの要件

システム リブート後に Security Manager サービスが開始しようとしているときは、ソフトウェア イニシエータを使用する iSCSI ボリュームを使用できないことがあります。これらが適切に初期化されるまでは少し時間がかかる場合があります。

Security Manager サービスが開始していない場合は、Security Manager サービスの依存関係とサービス スタートアップを設定する必要があります。

依存関係とスタートアップを設定するには、次の手順に従います。

ステップ 1　Windows コマンド プロンプトで次のコマンドを実行して、Cisco Security Manager Daemon Manager、syslog、および tftp サービスの起動タイプを「Delayed auto start」に変更します。

```
sc config CRMDmgtd start= delayed-auto
sc config crmlog start= delayed-auto
sc config crmtftp start= delayed-auto
```

ステップ 2　次のコマンドを実行して、Microsoft iSCSI の依存関係を Cisco Security Manager Daemon Manager サービスに設定します。

```
sc config CRMDmgtd depend= MSiSCSI
```

ヒント　これらのコマンドでは、オプション名に等号が含まれます。等号と値の間にはスペースが必要です。

ステップ 3　次のコマンドを実行して、Cisco Security Manager Daemon Manager サービスの依存関係の設定を確認します。iSCSI イニシエータの依存関係の設定は「DEPENDENCIES　　: MSiSCSI」と表示されます。

```
sc qc CRMDmgtd
```

クライアントの要件

表 3-4 に、Security Manager クライアントの要件と制約事項を示します。

（注） クライアントに選択する日時の形式はサーバ マシンで使用されているものと同じである必要があります。そうでない場合、Security Manager のデバイス ビューが適切にロードしない場合があります。

表 3-4　クライアントの要件と制約事項

コンポーネント	要件
システム ハードウェア	• 2 GHz 以上の速度の CPU x 1 • 1280 x 1024 以上の解像度を持つカラー モニタと 16 ビット色に対応したビデオ カード • キーボード • マウス
システム ソフトウェア	次のいずれかが必要です。 • Windows 7 SP1 Enterprise Edition（64 ビットおよび 32 ビット）。 • Windows 2008 Enterprise Server（Service Pack 2）（64 ビットのみ）。 • Windows 2008 R2 Enterprise Server SP1（64 ビット）。 **（注）** Security Manager は、米国だけをサポートします。Windows の英語および日本語版。[Start] メニューから、Windows のコントロール パネルを開いて、地域と言語を設定するパネルを開き、デフォルト ロケールを設定します （日本語バージョンの Windows では言語として英語がサポートされません）。
メモリ（RAM）	32 ビット システムの場合。 • 最小：2 GB • 推奨：2 GB 以上 64 ビット システムの場合。 • 最小：4 GB • 推奨：4 GB 以上
仮想メモリ（ページング ファイル）	512 MB **注意** Windows Server 2008 では [Automatically manage paging file size for all drives] チェックボックスをオフにする必要があります。このチェックボックスは、[Computer] > [Properties] > [Advanced System Settings] > [Performance] > [Settings] > [Advanced] > [Virtual Memory] > [Change] にあります。
ハード ドライブ スペース	10 GB の空きディスク スペース

表 3-4　クライアントの要件と制約事項 （続き）

コンポーネント	要件
ブラウザ	次のいずれかが必要です。 • Internet Explorer 7.0（この表の始めに示したオペレーティング システムを使用する場合）。 • Internet Explorer 8.0（この表の始めに示したオペレーティング システムを使用し、互換表示のみで使用する場合）。 • Internet Explorer 9.0（この表の始めに示したオペレーティング システムを使用し、互換表示のみで使用する場合）。 **ヒント** Internet Explorer 8 または 9 で互換表示を使用するには、[Tools] > [Compatibility View Settings] に移動し、[website to be displayed in Compatibility View] として Security Manager サーバを追加します。 **（注）** クライアントをダウンロードするために Internet Explorer（任意のバージョン）を使用する場合は、次の設定が正しいかどうかを確認します。Internet Explorer > [Tools] > [Internet Options] > [Advanced] > [Security] で、[Do not save encrypted pages to disk] チェックボックスをオフにします。この設定が正しくない（つまり、チェックボックスがオン）場合、クライアントをダウンロードしようとすると失敗します。 • Firefox 13.0.x、14.0.x、または 15.0.x（この表の始めに示したオペレーティング システムを使用する場合）。
Java プラグイン	JRE をインストールするための要件はありません。Java スクリプトが Web ブラウザでイネーブルになっている必要があります。 Security Manager クライアントには、組み込みバージョンと完全分離バージョンの Java（JRE 1.7.x）が含まれます。この Java バージョンが、ブラウザの設定または他の Java ベースのアプリケーションを妨害することはありません。
Windows ユーザ アカウント	Security Manager クライアントを使用するには、管理者特権を持つ Windows ユーザ アカウントでワークステーションにログインする必要があります。 より低い特権ではクライアントの一部の機能しか使用できませんが、管理者ユーザはすべての機能を使用できます。

CHAPTER 4

サーバのインストール準備

ターゲット サーバが第 3 章「要件と依存関係」に記載されている要件を満たしていることを確認したら、このチェックリストを使用してサーバをインストール用に準備し、最適化できます。

- 「サーバのパフォーマンスとセキュリティを向上させるためのベスト プラクティス」（P.4-1）
- 「インストール準備状況チェックリスト」（P.4-3）

サーバのパフォーマンスとセキュリティを向上させるためのベスト プラクティス

ベスト プラクティスのフレームワーク、推奨事項、およびその他の準備タスクを使用すると、Security Manager サーバの速度と信頼性を高めることができます。

注意 このチェックリスト内のタスクを完了することによって、すべてのサーバのパフォーマンスが向上するわけではありません。それでも、これらのタスクを完了しなかった場合は、Security Manager が設計どおりに動作しないことがあります。

このチェックリストは、推奨タスクの進捗を追跡するために使用できます。

✓	タスク
❑	**1. サーバへのインストールが推奨されているすべてのアップデート、パッチ、サービス パック、ホット フィックス、およびセキュリティ ソフトウェアを探して、インストーラ アプリケーションを編成します。**
❑	**2. アップグレードが入手可能な場合は、サーバ BIOS をアップグレードします。**
❑	**3. 他の目的に使用しているサーバ上に Security Manager をインストールする場合は、すべての重要なサーバ データをバックアップしてから、ブート CD または DVD を使用してサーバからすべてのデータをワイプします。** Security Manager 4.5 と 4.2.2 以前のリリースの Common Services を 1 台のサーバ上にインストールまたは共存させることは *できません*。また、このマニュアルまたは http://www.cisco.com/go/csmanager に明記されていない場合は、サードパーティ ソフトウェアまたはその他のシスコ ソフトウェアと共存させることもできません。
❑	**4. サーバ管理用のメーカー カスタマイズが施されていないベースライン サーバ OS のみのクリーン インストールを実行します。**

✓	タスク
❑	**5. ターゲット サーバ上に必要なすべての OS サービス パックと OS パッチをインストールします。**使用している Windows に関してどのサービス パックまたはアップデートが必要なのかをチェックするには、[Start] > [Run] を選択してから、**wupdmgr** と入力します。
❑	**6. ドライバとファームウェアに関して推奨されているすべてのアップデートをターゲット サーバにインストールします。**
❑	**7. システム上でマルウェアをスキャンします。**ターゲット サーバとその OS をセキュリティで保護するには、システム上でウイルス、トロイの木馬、スパイウェア、キーロガー、およびその他のマルウェアをスキャンしてから、見つかったすべての関連問題に対処します。
❑	**8. セキュリティ製品の競合を解消します。**ポップアップ ブロック、アンチウイルス スキャナ、他社の同等製品などのセキュリティ ツールに関する既知の非互換性または制約事項を理解して解決します。このような製品の競合や相互作用を理解するに当たって、インストール、アンインストール、または一時的にディセーブルにするものを決定し、従うべき順序を考慮します。
❑	**9. ユーザ アカウントを「強化」します。**ターゲット サーバを総当たり攻撃から保護するには、ゲスト ユーザ アカウントをディセーブルにして、管理者ユーザ アカウントの名前を変更し、管理環境内の悪用される可能性のあるその他のユーザ アカウントを削除します。
❑	**10. 管理者ユーザ アカウントと残りのユーザ アカウントに対して強力なパスワードを使用します。**強力なパスワードは、8 文字以上で構成され、数字、文字（大文字と小文字の両方）、および記号が含まれています。 **ヒント** Local Security Settings ツールを使用して、強力なパスワードを要求します。[Start] > [Administrative Tools] > [Local Security Policy] を選択します。
❑	**11. 未使用のアプリケーション、不必要なアプリケーション、および互換性のないアプリケーションを削除します。** 例： • Microsoft Internet Information Server（IIS）は Security Manager と互換性がありません。IIS がインストールされている場合は、それをアンインストールしてから Security Manager をインストールする必要があります。 • このマニュアルまたは http://www.cisco.com/go/csmanager に明記されていなければ、Security Manager とサードパーティ ソフトウェアまたはその他のシスコ ソフトウェア（LAN Management Solution（LMS）などの CiscoWorks ブランドの「ソリューション」または「バンドル」を含む）の共存がサポートされません。Security Manager と AUS の同じサーバ上へのインストールはサポートされますが、非常に低速なネットワークにのみ推奨されている設定です。また、いずれかの製品をインストールする前に、CiscoWorks Common Services をインストールする必要があります。 • 1 台のサーバ上で、このバージョンの Security Manager と 4.2.2 以前のリリースの Common Services をインストールまたは共存させることはできません。 • 1 台のサーバ上で、Security Manager と Security Manager の購入時に受領したものではない CD-ONE コンポーネント（CiscoView Device Manager を含む）を共存させることはできません。 • 1 台のサーバ上で、Security Manager と Cisco Secure ACS for Windows を共存させることはできません。 • 1 台のサーバ上で、Security Manager とフル バージョンの Cisco IPS Event Viewer を共存させることはできません。
❑	**12. 未使用のサービスと不必要なサービスをディセーブルにします。**Windows では、少なくとも、DNS クライアント、イベント ログ、プラグ アンド プレイ、保護された記憶域、およびセキュリティ アカウント マネージャを実行する必要があります。 ソフトウェアとハードウェアのマニュアルをチェックして、特定のサーバでその他のサービスが必要ないかどうかを確認します。
❑	**13. TCP と UDP を除くすべてのネットワーク プロトコルをディセーブルにします。**どのプロトコルもサーバへのアクセス権の取得に使用される可能性があります。ネットワーク プロトコルを制限することによって、サーバへのアクセス ポイントが制限されます。

✓	タスク
❑	**14. IPv6 をディセーブルにします。**Cisco Security Manager は IPv6 をサポートしていません。IPv6 は Windows Server 2008 で使用されるデフォルトのプロトコルです。
❑	**15. ネットワーク共有は作成しないでください。**ネットワーク共有を作成しなければならない場合は、共有リソースを強力なパスワードで保護してください。 **（注）**　ネットワーク共有はあまり推奨できません。NETBIOS を完全にディセーブルにすることを推奨します。
❑	**16. サーバ ブート設定を構成します。**起動時間を 0 秒に設定して、Windows をデフォルトでロードするように設定し、システム障害発生時の自動リブートをイネーブルにします。

インストール準備状況チェックリスト

Security Manager をインストールする前に、次のタスクを完了する必要があります。

✓	準備状況要因
❑	⚠ **注意**　セキュリティ アプリケーションをアンインストールまたはディセーブルにした場合は、サーバが攻撃に対して脆弱になる可能性があります。 **1. 一時的にセキュリティ アプリケーションをディセーブルにします。**たとえば、Security Manager をインストールする前に、ターゲット サーバ上のアンチウイルス ソフトウェアを一時的にディセーブルにする必要があります。これらのプログラムがアクティブの間はインストールを実行できません。
❑	**ヒント**　サーバに SSL 証明書の有効期間以外の日付と時刻を設定した場合は、サーバ上の SSL 証明書が無効になります。サーバの SSL 証明書が無効になっている場合は、DCRServer プロセスが起動できません。 **2. サーバに適用する日付と時刻の設定は慎重に検討してください。**NTP サーバを使用して、サーバの日付と時刻の設定と管理対象デバイスの日付と時刻の設定を同期させる方法が理想的です。また、Security Manager を Cisco Security Monitoring, Analysis, and Response System（Cisco Security MARS）アプライアンスと組み合わせて使用する場合は、使用する NTP サーバを Cisco Security MARS アプライアンスが使用するサーバと同じにする必要があります。ネットワーク上で発生したものを正確に再構成するためにはタイムスタンプ情報が不可欠なため、特に、Cisco Security MARS で同期化された時間が重要です。 **ヒント**　サーバ上の日付と時刻の設定を変更して SSL 証明書が無効になった場合は、「java.security.cert.CertificateNotYetValidException」エラーが *NMSROOT*\log\DCRServer.log ファイルに記録されます。ここで、*NMSROOT* は Security Manager インストール ディレクトリへのパスです。デフォルトは **C:\Program Files\CSCOpx** です。
❑	**3. 必要なサービスとポートがイネーブルになっており、Security Manager から使用可能なことを確認します。**「必要なサービスとポート」（P.3-1）を参照してください。
❑	**4. Terminal Services がアプリケーション モードでイネーブルになっている場合は、Terminal Services をディセーブルにして、サーバをリブートします。**Terminal Services がアプリケーション モードでイネーブルになっているサーバ上に Security Manager をインストールできません。リモート管理モードでイネーブルにされた Terminal Services はサポートされます。 Terminal Services がアプリケーション モードでイネーブルになっているターゲット サーバに Security Manager をインストールしようとすると、エラーでインストールが終了します。
❑	**5. 実行中のドメイン コントローラ サービス（プライマリまたはバックアップ）をディセーブルにします。**

✓	準備状況要因
❑	**6. インストールのターゲット ディレクトリが暗号化されていないことを確認します。**暗号化されたディレクトリに Security Manager をインストールしようとすると失敗します。
❑	**7. フレッシュ インストールを実行している場合は、インストールの前にライセンス ファイルをターゲット サーバに配置する必要があります。**インストール中にこのファイルの選択が要求されます。 **（注）**　ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。
❑	**8. インストールされている IIS をアンインストールします。**IIS は Security Manager と互換性がありません。
❑	**9. 存在する場合の Cisco Secure ACS for Windows を含めて、サーバ上のすべてのアクティブな Sybase インスタンスをディセーブルにします。**Security Manager のインストール後に Sybase を再イネーブルするか、再起動するかを選択できますが、同じサーバ上での Security Manager と Cisco Secure ACS for Windows の共存がサポートされていないことに注意してください。
❑	**10. Cisco Security Manager クライアントがすでにサーバ上にインストールされている場合は、そのクライアントを停止する必要があります。**この状態はインストール中にチェックされます。
❑	**11. FIPS 準拠の暗号化をディセーブルにします。**Windows Server 2008 のグループ セキュリティ ポリシーで、Federal Information Processing Standard（FIPS; 連邦情報処理標準）準拠の暗号化アルゴリズムがイネーブルになっていることがあります。FIPS 準拠がオンになっている場合は、CiscoWorks サーバ上の SSL 認証が失敗する可能性があります。CiscoWorks を正しく機能させるためには、FIPS 準拠をディセーブルにする必要があります。 **手順** Windows Server 2008 上で FIPS をイネーブルまたはディセーブルにするには、次の手順を実行します。 **a.** [Start] > [Administrative Tools] > [Local Security Policy] に移動します。[Local Security Policy] ウィンドウが表示されます。 **b.** [Local Polices] > [Security Options] をクリックします。 **c.** [System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing] を選択します。 **d.** 選択したポリシーを右クリックして、[Properties] をクリックします。 **e.** [Enabled] または [Disabled] を選択して、FIPS 順序アルゴリズムをイネーブルまたはディセーブルにします。 **f.** [Apply] をクリックします。 サーバをリブートして変更を有効にする必要があります。
❑	**12. Internet Explorer Enhanced Security Configuration（IE ESC）をディセーブルにします。**クライアントのダウンロードが IE ESC によって禁止されるため、この作業を行う必要があります。 **手順** Security Manager のインストール準備をしているサーバ上で IE ESC をディセーブルにするには、次の手順を実行します。 **a.** Windows で、Server Manager を開きます。これを行うには、[Computer] を右クリックしてから、[Manage] をクリックします。 **b.** [Security Information] の下で、[Configure IE ESC] をクリックし、IE ESC を無効にします。

CHAPTER 5

サーバ アプリケーションのインストールとアップグレード

次のトピックでは、Security Manager サーバ ソフトウェアとその他のサーバ アプリケーション（Common Services、AUS など）のインストール方法について説明します。

- 「必要なサーバ ユーザ アカウントについて」（P.5-1）
- 「Remote Desktop Connection または VNC を使用したサーバ アプリケーションのインストール」（P.5-2）
- 「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2）
- 「サーバ アプリケーションのアップグレード」（P.5-5）
- 「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.5-14）
- 「Security Manager の更新」（P.5-15）
- 「サービス パックとポイント パッチの入手」（P.5-16）
- 「サーバ アプリケーションのアンインストール」（P.5-17）
- 「サーバ アプリケーションのダウングレード」（P.5-18）

必要なサーバ ユーザ アカウントについて

CiscoWorks Common Services と Security Manager は、必要な認可を受けているユーザにのみ特定の機能へのアクセスを許可する多層セキュリティ システムを採用しています。そのため、Common Services 上で動作するアプリケーションがインストールされたシステム上では、事前に定義された次の 3 つのユーザ アカウントが作成されます。

- **admin**：admin ユーザ アカウントは、Windows 管理者と等価で、Common Services、Security Manager、およびその他のアプリケーション タスクのすべてにアクセスできるようにします。インストール中にパスワードを入力する必要があります。このアカウントは、初めてサーバにログインするときに使用して、アプリケーションを日常的に使用するための他のユーザ アカウントを作成できます。
- **casuser**：casuser ユーザ アカウントは、Windows 管理者と等価で、Common Services タスクと Security Manager タスクのすべてにアクセスできるようにします。このアカウントを直接使用することはあまりありません。

  製品のインストール中に設定された casuser（デフォルト サービス アカウント）権限またはディレクトリ権限を変更しないでください。変更した場合は、次の操作ができなくなる可能性があります。

  - Web サーバへのログイン

  - クライアントへのログイン
  - データベースの正常なバックアップ

- *システム識別*: システム識別ユーザ アカウントは、Windows 管理者と等価で、Common Services タスクと Security Manager タスクのすべてにアクセスできるようにします。このアカウントには固定の名前がありません。ニーズに合った名前を使用してアカウントを作成できます。Common Services でアカウントを作成した場合は、そのアカウントにシステム管理者特権を付与する必要があります。ユーザ認証に Cisco Secure Access Control Server（ACS）を使用している場合は、ACS にすべての特権を付与する必要があります。

  Cisco Security Management Suite アプリケーションを別のサーバにインストールする場合（推奨アプローチ）は、マルチサーバ セットアップ内のすべてのサーバ上で同じシステム識別ユーザ アカウントを作成する必要があります。サーバ間の通信は、証明書と共有秘密キーを使用する信頼モデルに依存します。システム識別ユーザは、マルチサーバ セットアップ内の他のサーバから信頼できるアカウントと見なされるため、ドメイン内のサーバ間通信が容易になります。

必要な数のユーザ アカウントを追加できます。アカウントはユーザごとに一意にする必要があります。このような追加のアカウントを作成するには、システム管理者権限（admin アカウントの使用など）を持っている必要があります。ユーザ アカウントを作成したら、それにロールを割り当てる必要があります。このロールによって、表示も含めて、ユーザがアプリケーション内で可能な操作が定義されます。使用可能な権限の種類と ACS を使用してアプリケーションへのアクセスを制御する方法については、第 8 章「ユーザ アカウントの管理」を参照してください。

Remote Desktop Connection または VNC を使用したサーバ アプリケーションのインストール

サーバ アプリケーションは、サーバに直接ログインしてインストールすることを推奨します。

ただし、リモート インストール（別のワークステーション経由のログイン）を行わなければならない場合は、次のヒントを考慮してください。

- リモート ディスクからソフトウェアをインストールしようとしないでください。ソフトウェア インストーラは、サーバ内の DVD ドライブ上で動作している製品 DVD 上に存在するか、直接接続されたディスク ドライブ上に存在する必要があります。リモート ディスクからのインストールが成功したように見える場合がありますが、実際には成功していません。
- ソフトウェアのインストールに Virtual Network Computing（VNC）を使用できます。
- ソフトウェアのインストールに Remote Desktop Connection を使用できます。Remote Desktop Connection を使用する場合は、Remote Desktop Protocol 非コンソール セッションではなく、コンソール セッションを使用することを推奨します。

Security Manager サーバ、Common Services、および AUS のインストール

メインの Security Manager インストール プログラムで次のようなアプリケーションをインストールできます。

- CiscoWorks Common Services 4.2.2：サーバ アプリケーションに必要な基盤ソフトウェアです。Security Manager 4.4 から、[CiscoWorks Common Services] チェックボックスはコンポーネントの選択ページに表示されなくなりました。Common Services のインストールは、デフォルトで選択されます。

- Cisco Security Manager 4.5：Security Manager のメイン サーバ ソフトウェアです。
- Auto Update Server 4.5。
- Cisco Security Manager Client 4.5：Security Manager サーバとデータをやり取りするためのクライアント ソフトウェアです。サーバと同じコンピュータ上にインストールできますが、このセットアップを Security Manager を使用する通常の方法として使用しないでください。推奨されているクライアントのインストールとセットアップの詳細については、第 6 章「クライアントのインストールと設定」を参照してください。

ヒント Security Manager 4.4 から、インストール時間を短縮するために、AUS および Security Manager クライアントが同時にインストールされます。

次の手順を使用して、これらのアプリケーションをインストールまたは再インストールします。以前のバージョンのアプリケーションからアップグレードしている場合は、先に進む前に、「サーバ アプリケーションのアップグレード」（P.5-5）を参照してください。

はじめる前に

- このインストレーション ガイドの「ライセンス」の章を参照してください。
- すでにサーバ上にインストールされている既存のバージョンのアプリケーションに対するアップグレードとして製品をインストールしている場合は、「リモート アップグレード時のデータベースのバックアップ」（P.5-10）に記載されているようにバックアップを実行してください。アップグレードをインストールする前に、バックアップが正常に終了し、既存のアプリケーションが正しく機能していることを確認してください。
- Security Manager の永久ライセンスのインストール時は、Security Manager サーバにとってローカルなディスク上にライセンス ファイルを配置する必要があります。Security Manager を使用してサーバ上のディレクトリを参照する場合、マップされたドライブは表示されません。そのため、インストール時にライセンス ファイルを選択するには、そのライセンス ファイルがサーバ上に存在している必要があります。（Windows ではこの制限が課されますが、これにより Security Manager のパフォーマンスとセキュリティが向上します）。このファイルは製品をインストールするフォルダに配置しないでください。

（注） ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。

- 「インストール準備状況チェックリスト」（P.4-3）を完了したことを確認してください。
- サーバが「サーバの要件および推奨事項」（P.3-4）に記載された要件を満たしていることを確認してください。
- Security Manager は制御環境下の専用サーバにインストールすることを推奨します。他のソフトウェア アプリケーションをインストールした場合は、Security Manager の通常動作と競合したり、サポートされていなかったりする可能性があります。
- Common Services のインストール後にシステム時間を変更しないでください。このような変更が一部の時間依存機能の動作に影響する可能性があります。
- Cisco Secure Access Control Server（ACS）を使用して、Security Manager または AUS へのユーザ アクセスに AAA サービスを提供する場合は、アプリケーションをインストールしてから、ACS を使用するように Common Services を設定します。ACS 制御の設定方法については、「Security Manager と Cisco Secure ACS の統合」（P.8-12）を参照してください。

ACS を使用するように Common Services を設定してから Security Manager または AUS をインストールした場合は、インストール中に、インストールしたアプリケーションを ACS に登録する必要があることが通知されます。まだアプリケーション（このサーバ上または別のサーバ上）を ACS に登録していない場合は、[Yes] を選択します。すでにアプリケーションを登録している場合は、[Yes] を選択すると、アプリケーションの ACS 内で設定されたユーザ ロールのカスタマイズが失われるため、[No] を選択する必要があります。同じ ACS サーバを使用するすべての Security Manager サーバと AUS サーバがユーザ ロールを共有します。

手順

Security Manager サーバ、Common Services、AUS、またはメインの Security Manager インストール プログラムを使用する複数のアプリケーションをインストールするには、次の手順を実行します。

ステップ 1　インストール プログラムを入手または検索します。次のいずれかの操作を実行できます。

- サーバの DVD ドライブに Security Manager インストール DVD を挿入します。インストール アプリケーションが自動的に起動しなかった場合は、**csm**<*version*>**_win_server** フォルダ内の **Setup.exe** ファイルを実行します。
- Cisco.com アカウントにログインして、http://www.cisco.com/go/csmanager にある Security Manager ホームページにアクセスします。[Download Software] をクリックして、圧縮された Security Manager のインストール ファイルをダウンロードします。
  - WinZip や圧縮フォルダの展開ウィザードなどの Windows Server 2008 に付属しているファイル圧縮ユーティリティのいずれかを使用して、圧縮されたソフトウェア インストール ファイル内のすべてのファイルを一時ディレクトリで解凍します。パス名があまり長くないディレクトリを使用してください。たとえば、C:\Documents and Settings\Administrator\Desktop よりは C: を選択してください。通常は、圧縮ファイルと同じディレクトリに解凍される、インストール プログラムの **Setup.exe** を開始します。
  - ファイルの内容を解凍できないというエラー メッセージが表示された場合は、Temp ディレクトリを空にして、ウイルスをスキャンし、C:\Program Files\Common Files\InstallShield ディレクトリを削除してから、リブートしてもう一度試してみてください。

ステップ 2　インストール ウィザードの指示に従います。インストール中に、次の情報の入力が要求されます。

- [Backup location]：特定のバージョンの Common Services、Security Manager、または AUS がすでにインストールされている場合は、インストール プログラムによってインストール中のデータベース バックアップが許可されます。バックアップを実施する場合は、バックアップに使用する場所を選択します。ただし、バックアップは、インストールを開始する前に実施することを推奨します。

（注）　バックアップに使用するために選択する場所は、*NMSROOT* の外にする必要があります。場所 *NMSROOT* は Security Manager インストール ディレクトリへのパスです。デフォルトは **C:\Program Files (x86)\CSCOpx** です。特に、*NMSROOT*\backup をバックアップに使用しないように注意してください。

- [Destination folder]：アプリケーションをインストールするフォルダ。他の場所にインストールする特別な理由がなければ、デフォルトを受け入れます。デフォルト フォルダ以外のフォルダを指定した場合は、その下にファイルが存在しないことと、パス名が 256 文字未満であることを確認してください。また、デフォルト フォルダ以外のフォルダを指定すると、パスに特殊文字を含めることはできません。
- [Applications]：インストールするアプリケーション：Security Manager、AUS、または両方。CiscoWorks Common Services 4.2.2 が Security Manager または AUS のインストール時に自動的にインストールされます。

- [License information]：次のいずれかを選択します。
  - [License File Location]：ライセンス ファイルのフル パス名を入力するか、[Browse] をクリックして検索します。永久ライセンス ファイルを事前にサーバ上に配置してあった場合は、そのファイルを指定できます。

（注）　ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。

  - [Evaluation Only]：無料の 90 日の評価期間をイネーブルにします。
- [Admin password]：5 文字以上の **admin** ユーザ アカウント用パスワード。このアカウント、システム識別アカウント、および casuser アカウントの詳細については、「必要なサーバ ユーザ アカウントについて」（P.5-1）を参照してください。
- [System Identity user]：システム識別ユーザとして使用するアカウントのユーザ名とパスワード。Cisco Security Management Suite アプリケーションを複数のサーバ上にインストールする場合は、すべてのサーバ上で同じシステム識別ユーザ アカウントを使用してください。
- [Create casuser]：新しいインストールで casuser アカウントを作成するかどうか。このユーザ アカウントは作成する必要があります。

（注）　パスワードの複雑度の制限に対するセキュリティ ポリシーがある場合、このアカウント作成は失敗することがあります。そのような場合は、アカウントを手動で作成して、**resetcasuser.exe** コマンドを実行する必要があります。詳細については、表 A-3、「LiaisonServlet エラーの原因と対処法」の casuser パスワードを参照してください。

ステップ 3　インストールの完了後に、サーバが自動的に再起動しない場合は、サーバを再起動します。

サーバ アプリケーションのアップグレード

アプリケーションのアップグレードとは、古いバージョンからのデータを維持しながら、新しいバージョンのアプリケーションをインストールするプロセスです。3 種類のアップグレード パスがあります。

- ローカル：古いバージョンをアンインストールせずに、古いバージョンを実行中のサーバ上に新しいバージョンをインストールします。既存のデータが保存され、新しくインストールされたバージョンで使用できます。ローカル アップグレードを実施する場合は次の点に注意してください。
  - この方式を使用する前に、アップグレードするすべてのアプリケーションが正しく機能していることを確認してください。また、アップグレード対象のアプリケーションをインストールする前に、データベースのバックアップを実施して、正常に終了したことを確認してください。
  - サーバ上のオペレーティング システムもアップグレードしている場合、たとえば、Windows 2003 から Windows 2008 にアップグレードしている場合は、この方式が使用できません。オペレーティング システムのアップグレードも行いながら Security Manager をアップグレードしている場合は、代わりに、リモート バックアップ/復元アップグレード方式を使用します。同じ Security Manager リリースを維持しながらオペレーティング システムをアップグレードしている場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.5-14）に記載された手順を実行します。
  - データベースの移行エラーが発生した場合はエラー メッセージが表示されます。これが表示されるのは、停止しなくてもインストールを先に進めることが可能な時点です。

（注）　ローカル アップグレード時に、インストーラによって、Performance Monitor または Resource Manager Essentials がインストールされているかどうかがチェックされます。いずれか 1 つ、または両方が検出された場合、「Performance Monitor or Resource Manager Essentials (or both) needs to be uninstalled」というエラー メッセージを表示してインストーラが終了します。

- リモート（バックアップ/復元）：新しいバージョンをクリーン サーバ（古いアプリケーションがインストールされていないサーバ）にインストールしてから、古いバージョンから作成したバックアップからデータベースを復元します。新しいサーバ上にインストールする場合、または、インストールを実施する前にサーバをクリーンオフする（アプリケーションをアンインストールする前にバックアップを作成する）場合に、この手順を使用します。

  （注）　Security Manager サーバ アプリケーションを実行しているサーバのバックアップを作成する前に、すべての保留データがコミットされていることを確認する必要があります。「Security Manager の保留データが送信および承認されることの確認」（P.5-8）を参照してください。

- 間接：ローカルまたはリモート アップグレードでサポートされていない古いバージョンのアプリケーションを使用している場合は、2 段階プロセスを実行する必要があります。ローカルまたはリモート アップグレードでサポートされているバージョンにアップグレードしてから、ローカルまたはリモート アップグレードを実施します。中間のバージョンを Cisco.com からダウンロードします。

  使用中のバージョンが下の表に間接アップグレード用として掲載されておらず、古いデータを保存する必要がある場合は、3 つ以上の中間アップグレード手順を実施する必要があります。たとえば、Security Manager 3.0.x からアップグレードする場合は、3.2.2 にアップグレードしてから、4.1 にアップグレードし、その後で 4.4 にアップグレードする必要があります。

表 5-1 に、アップグレード パスごとにサポートされているソフトウェアのバージョンに関する説明を示します。

次のアップグレード パスがサポートされています。

- 4.3（サービス パックを含む）> 4.5
- 4.4（サービス パックを含む）> 4.5

表 5-1　アプリケーション アップグレード パス

アップグレード パス	アプリケーション	サポートされている古いバージョン	アップグレード手順
ローカル	Security Manager 4.5 Auto Update Server 4.5	4.3 および 4.4	1. すべての保留データをコミットします。「Security Manager の保留データが送信および承認されることの確認」（P.5-8）を参照してください。 2. その後で、ソフトウェアをインストールします。「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2）を参照してください。 3. 最後に、アップグレード後の必要な変更を加えます。「アップグレード後の必要な変更の実施」（P.5-13）を参照してください。

表 5-1　アプリケーション アップグレード パス （続き）

アップグレード パス	アプリケーション	サポートされている古いバージョン	アップグレード手順
リモート	Security Manager 4.5 Auto Update Server 4.5	4.3 および 4.4	1. すべての保留データをコミットします。「Security Manager の保留データが送信および承認されることの確認」（P.5-8）を参照してください。 2. データベースをバックアップします。「リモート アップグレード時のデータベースのバックアップ」（P.5-10）を参照してください。 3. アプリケーションをインストールします。次の項を参照してください。 「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2） 4. 必要に応じて、データベースのバックアップをサーバに転送します。 5. データベースを回復します。「サーバ データベースの復元」（P.5-12）を参照してください。 6. 最後に、アップグレード後の必要な変更を加えます。「アップグレード後の必要な変更の実施」（P.5-13）を参照してください。

表 5-1　アプリケーション アップグレード パス （続き）

アップグレード パス	アプリケーション	サポートされている古いバージョン	アップグレード手順
間接	Security Manager 4.5	3.3.x	1. すべての保留データをコミットします。「Security Manager の保留データが送信および承認されることの確認」（P.5-8）を参照してください。 2. 次に、4.2 にリモート アップグレードしてから、4.2 のインストレーション ガイドのアップグレードに関する章内のデータ移行手順を忠実に実行します。 3. 次に、4.3 にアップグレードしてから、4.3 のインストレーション ガイドのアップグレードに関する章内のデータ移行手順を忠実に実行します。 4. 最後に、4.5 にアップグレードして 4.5 用のインストレーション ガイドのアップグレードに関する章内のデータ移行手順を忠実に実行します。
間接	Security Manager 4.5	3.2.x（3.2.2 のみ）	1. すべての保留データをコミットします。「Security Manager の保留データが送信および承認されることの確認」（P.5-8）を参照してください。 2. 次に、4.0 にアップグレードしてから、4.0 のインストレーション ガイドのアップグレードに関する章内のデータ移行手順を忠実に実行します。 3. 次に、4.3 にアップグレードしてから、4.3 のインストレーション ガイドのアップグレードに関する章内のデータ移行手順を忠実に実行します。 4. 最後に、4.5 にアップグレードして 4.5 用のインストレーション ガイドのアップグレードに関する章内のデータ移行手順を忠実に実行します。
間接	Security Manager 4.5	4.0、4.1、4.2	1. すべての保留データをコミットします。「Security Manager の保留データが送信および承認されることの確認」（P.5-8）を参照してください。 2. 次に、4.3 にアップグレードしてから、4.3 のインストレーション ガイドのアップグレードに関する章内のデータ移行手順を忠実に実行します。 3. 次に、4.5 にアップグレードしてから、4.5 のインストレーション ガイドのアップグレードに関する章内のデータ移行手順を忠実に実行します。

Security Manager の保留データが送信および承認されることの確認

Security Manager のアップグレードを成功させるためには、既存の Security Manager データベースに保留データが含まれていないことを確認する必要があります。保留データとは、データベースに対してコミットされていないデータのことです。保留データが残っている以前のバージョンの Security Manager からのデータベースは復元できません。復元できるのは、バックアップと同じバージョンを実行しているシステム上に保留データが残っているデータベースだけです。

ユーザごとに変更を送信または破棄する必要があります。Approver でワークフロー モードを使用している場合は、このような送信も承認する必要があります。すべてのデバイス設定と Security Manager データベースを同期させるためには、すべてのデータのコミット後に展開を実施する必要もあります。

- ワークフロー以外のモードで、次の手順を実行します。
  - 変更をコミットするには、[File] > [Submit] を選択します。
  - コミットされていない変更を廃棄するには、[File] > [Discard] を選択します。
  - 別のユーザの変更をコミットまたは廃棄する必要がある場合は、そのユーザのセッションを引き継ぐことができます。セッションを引き継ぐには、[Tools] > [Security Manager Administration] > [Take Over User Session] を選択してから、[Take Over Session] をクリックします。
- ワークフロー モードで、次の手順を実行します。
  - 変更をコミットして承認するには、[Tools] > [Activity Manager] を選択します。[Activity Manager] ウィンドウからアクティビティを選択し、[Approve] をクリックします。Activity Approver を使用している場合は、[Submit] をクリックして、Approver にアクティビティを承認してもらいます。
  - コミットされていない変更を破棄するには、[Tools] > [Activity Manager] を選択します。[Activity Manager] ウィンドウで、アクティビティを選択してから、[Discard] を選択します。廃棄できるのは、Edit または Edit Open の状態にあるアクティビティだけです。

プロパティ ファイルに対する変更の復元

すべての Security Manager インストールにいくつかのプロパティ ファイルが含まれています。このファイルには、使用中に変更されたデータが保存されます。

- *$NMSROOT*\MDC\athena\config\csm.properties
- *$NMSROOT*\MDC\athena\config\DCS.properties
- *$NMSROOT*\MDC\athena\config\taskmgr.prop

ヒント　*$NMSROOT* は、Common Services インストール ディレクトリ（デフォルトは C:\Program Files\CSCOpx）のフル パス名です。

現在のインストールに対してサービス パックのアップグレードまたはインストールを実施した場合の Security Manager の動作は次のとおりです。

- アップグレードまたはサービス パックに関連する新しいファイルをインストールします。
- 新しいファイルと使用中に変更されたファイルを比較します。
- 新しいファイルと使用中に変更されたファイルが異なる場合は警告を発します。その場合は、Security Manager が次のように処理します。
  - 使用中に変更されたファイルを *<filename>.org* という名前で保存します。
  - 参考用として、差分ファイルを *<filename>.diff* という名前で保存します。

新しいファイルと使用中に変更されたファイルが異なるという内容の警告を受け取った場合は、*<filename>.org* と *<filename>.diff* 内の情報を使用して、アップグレードまたはサービス パックのインストール前に、加えた変更をプロパティ ファイルに復元します。

リモート アップグレード時のデータベースのバックアップ

CiscoWorks Common Services は、データベースのバックアップと復元に使用される Common Services バックアップ/復元ユーティリティで、すべてのサーバ アプリケーションのデータベースを管理します。そのため、バックアップを作成すると、サーバ上にインストールされたすべての CiscoWorks アプリケーションのバックアップが作成されます。

（注） Security Manager 4.4 から、新しい属性の PURGE_DBBACKUP_LOG が backup.properties ファイルに追加されました。デフォルト値は 20 で、20 日経過した後にバックアップを削除するという意味です。この新しい属性が NIL に設定されている場合、バックアップは削除されません。dbbackup.log は dbbackup_[YYYY-MM-DD_HH-mm-ss].log のタイムスタンプ形式で作成されます。削除設定に関係なく、常時、dbbackup.log ファイルは少なくとも 5 個維持されます。

（注） データベースをバック アップするには、Short Date フォーマットは M/d/YYYY または M/d/yy にする必要があります。Short Date フォーマットを M/d/YYYY または M/d/yy に変更するには、[Start] > [Control Panel] > [Region and Language] > [Formats] > [Short Date] を選択し、次に Short Date フォーマットを M/d/YYYY または M/d/yy に変更します。

ヒント このバックアップ手順はデータベースのみをバックアップします。イベント データ ストアをバックアップする必要がある場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.5-14）に記載されているデータ ストア コピー手順を使用します。

ステップ 1 Security Manager を実行しているサーバをバックアップしている場合は、Security Manager クライアントの [Tools] > [Backup] というショートカットを使用してバックアップ ページを表示できます。また、保留データがコミットされていることを確認します（「Security Manager の保留データが送信および承認されることの確認」（P.5-8）を参照）。

Security Manager を実行していないサーバの場合は、次の手順でバックアップ ページを表示します。

a. サーバ上の Cisco Security Management Server デスクトップにログインします（「Web ブラウザを使用したサーバ アプリケーションへのログイン」（P.6-13）を参照）。

b. [Server Administration] パネルをクリックします。次に、[Server] > [Admin] > [Backup] を選択します。

ステップ 2 [Immediate for Frequency] を選択して、必要に応じて他のフィールドを設定し、[Apply] をクリックしてデータをバックアップします。

CLI を使用したサーバ データベースのバックアップ

この項の手順では、サーバ上の Windows コマンドラインからスクリプトを実行することによって、サーバ データベースをバックアップする方法について説明します。

データベースのバックアップ中に、Common Services と Security Manager の両方のプロセスがシャットダウンされ、再起動されます。Security Manager の再起動が完了するまでには数分かかる可能性があるため、再起動の完了前にユーザがクライアントを起動してしまうことがあります。この場合、デバイス ポリシーのウィンドウに「error loading page」というメッセージが表示されることがあります。

CiscoWorks サーバ上にインストールされたすべてのアプリケーションをバックアップするのに 1 つのバックアップ スクリプトしか使用されません。個別のアプリケーションをバックアップできません。

ヒント　このバックアップ コマンドはデータベースのみをバックアップします。イベント データ ストアをバックアップする必要がある場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.5-14）に記載されているデータ ストア コピー手順を使用します。

ステップ 1　保留データがコミットされていることを確認します（「Security Manager の保留データが送信および承認されることの確認」（P.5-8）を参照）。

ステップ 2　コマンド プロンプトで、**net stop crmdmgtd** と入力してすべてのプロセスを停止します。

ステップ 3　次のコマンドを入力することによって、データベースをバックアップします。

*$NMSROOT***bin\perl** *$NMSROOT***bin\backup.pl** *backup_directory* [*log_filename* [**email=***email_address* [*number_of_generations* [**compress**]]]]

引数の説明

- *$NMSROOT* : Common Services インストール ディレクトリのフル パス名（デフォルトは C:\Program Files\CSCOpx）。
- *backup_directory* : バックアップを作成するディレクトリ。C:\Backups などです。

（注）　バックアップに使用するために選択する場所は、*NMSROOT* の外にする必要があります。場所 *NMSROOT* は Security Manager インストール ディレクトリへのパスです。デフォルトは **C:\Program Files\CSCOpx** です。特に、*NMSROOT*\backup をバックアップに使用しないように注意してください。

- *log_filename* :（任意）バックアップ中に生成されるメッセージ用のログ ファイル。現在のディレクトリ以外の場所にバックアップを作成する場合は、そのパスを追加します。C:\BackupLogs などです。名前を指定しなかった場合は、*$NMSROOT*\log\dbbackup.log になります。
- **email=***email_address* :（任意）通知を送信する電子メール アドレス。電子メール アドレスは指定しないが、後続のパラメータは指定する必要がある場合は、サイズまたはアドレスが一致しない **email** を入力します。CiscoWorks Common Services で SMTP を設定して、通知をイネーブルにする必要があります。
- *number_of_generations* :（任意）バックアップ ディレクトリに保存しておくバックアップの最大世代数。最大数に達すると、古いバックアップが削除されます。デフォルトは 0 で、保存される世代数に制限はありません。
- **compress** :（任意）バックアップ ファイルを圧縮するかどうか。このキーワードを入力しないと、backup.properties ファイル内に VMS_FILEBACKUP_COMPRESS=NO が指定されている場合、バックアップは圧縮されません。指定されていない場合は、このキーワードを入力しなくてもバックアップは圧縮されます。バックアップは圧縮することを推奨します。

たとえば、次に示されているコマンドは、perl コマンドと backup.pl コマンドが存在するディレクトリで発行することを想定しています。（ただし、該当ディレクトリの場合でも、DOS 8.1 形式（スペースなし）の完全修飾された、perl と backup.pl の完全なパスを指定する必要があります）。

次に示されているコマンドでは、バックアップ ディレクトリ内に圧縮されたバックアップおよびログ ファイルが作成され、admin@domain.com に通知が送信されます。

backup.pl コマンドを使用する場合、圧縮パラメータを含めるにはバックアップ世代を指定する必要があります。

ログ ファイル パラメータの後ろにパラメータを指定する場合は、先行するすべてのパラメータの値を含める必要があります。

次の例では、*$NMSROOT* は D:\CSM であり、デフォルト値の C:\Program Files\CSCOpx ではありません。

D:\CSM\bin\perl D:\CSM\bin\backup.pl C:\backups C:\backups\backup.log email=admin@domain.com 0 compress

ステップ 4　ログ ファイルを調査して、データベースがバックアップされていることを確認します。

ステップ 5　コマンド プロンプトで、**net start crmdmgtd** と入力して、すべてのプロセスを再起動します。

サーバ データベースの復元

コマンドラインからスクリプトを実行することにより、データベースを復元できます。データの復元中に、CiscoWorks をシャットダウンしてから再起動する必要があります。ここでは、サーバ上のバックアップ データベースを復元する方法について説明します。バックアップおよび復元のための機能は 1 つだけであり、CiscoWorks サーバにインストールされているすべてのアプリケーションをバックアップおよび復元できます。個々のアプリケーションをバックアップまたは復元することはできません。

複数のサーバにアプリケーションをインストールした場合は、インストールされているアプリケーションに適したデータが含まれるデータベース バックアップを復元する必要があります。

ヒント

- 以前のリリースのアプリケーションから作成したバックアップは、このバージョンのアプリケーションへのダイレクト ローカル インライン アップグレードがサポートされているバージョンからのバックアップであれば、復元できます。アップグレードに対応したバージョンの詳細については、「サーバ アプリケーションのアップグレード」（P.5-5）を参照してください。
- restore コマンドは、データベースのみを復元します。イベント データ ストアを復元する必要がある場合は、「新しいコンピュータまたはオペレーティング システムへの Security Manager の移行」（P.5-14）に記載されているデータ ストア コピー手順を使用します。

手順

ステップ 1　コマンドラインで次のように入力して、すべてのプロセスを停止します。

net stop crmdmgtd

ステップ 2　次のコマンドを入力することによって、データベースを復元します。

*$NMSROOT***bin\perl** *$NMSROOT***bin\restorebackup.pl** [**-t** *temporary_directory*] [**-gen** *generationNumber*] **-d** *backup_directory* [**-h**]

引数の説明

- *$NMSROOT* : Common Services インストール ディレクトリのフル パス名（デフォルトは C:\Program Files\CSCOpx）。
- **-t** *temporary_directory* :（任意）復元プログラムで一時ファイルを保存するために使用されるディレクトリまたはフォルダ。デフォルトでは、このディレクトリは *$NMSROOT*\tempBackupData です。
- **-gen** *generationNumber* :（任意）復元するバックアップ世代番号。デフォルトでは、最新の世代です。第 1 ～ 5 世代が存在する場合は、第 5 世代が最新です。
- **-d** *backup_directory* : 復元するバックアップが保存されたバックアップ ディレクトリ。
- **-h** :（任意）ヘルプを表示します。**-d** *BackupDirectory* を使用した場合は、ヘルプに正しい構文と使用可能なスイートおよび世代が表示されます。

たとえば、c:\var\backup ディレクトリから最新のバージョンを復元する場合は、次のコマンドを入力します（これは 64 ビット OS の場合です）。

C:\Progra~2\CSCOpx\bin\perl C:\Progra~2\CSCOpx\bin\restorebackup.pl -d C:\var\backup

ステップ 3　ログ ファイル *NMSROOT***log\restorebackup.log** を調べて、データベースが復元されたことを確認します。

ステップ 4　次のように入力して、システムを再起動します。

net start crmdmgtd

ステップ 5　Security Manager サービス パックのインストール前にバックアップされたデータベースを復元する場合は、データベースの復元後にサービス パックを再適用する必要があります。

アップグレード後の必要な変更の実施

アプリケーションをアップグレードすると、特定の情報の処理方法が変わって、手動で変更しなければならなくなる場合があります。このバージョンの製品にアップグレードしたら、下の必要な変更リストを参照して、状況に合わせて変更を適用する必要があります。

- 3.3.1 より以前のバージョンからアップグレードする場合は、4 ポート Gigabit Ethernet Fiber インターフェイス カード（ハードウェア タイプ : i82571EB 4F）が実装された ASA 5580 デバイス上でインベントリを再検出する必要があります。インベントリの再検出によって、デバイス上での速度非ネゴシエート設定を変更できない以前のリリースからのバグが解決されます。インベントリを再検出するには、Security Manager クライアントのデバイス ビューでデバイスを右クリックして、[Discover Policies on Device] を選択してから、[Policies to Discover] グループ内の [Live Device discovery and only the Inventory] チェックボックスをオンにします。再検出によって、デバイスに関するインターフェイス ポリシーが置き換えられます。
- 3.3.1 以前のバージョンからアップグレードしており、未サポートの共有ポート アダプタ（SPA）を使用する Cisco ASR 1000 シリーズ アグリゲーション サービス ルータを管理している場合は、Security Manager で、サポートされているバージョン 4.0 以降の SPA が検出できるように、デバイスに関するポリシーを再検出する必要があります。新しくサポートされる SPA には、すべてのイーサネット（すべての速度）、シリアル、ATM、および Packet over Sonet（POS）SPA が含まれますが、サービス SPA は含まれません。デバイス CLI で ATM、PVC、またはダイヤラ関連ポリシーを設定した場合は、再検出が必要です。

新しいコンピュータまたはオペレーティング システムへの Security Manager の移行

Security Manager を新しいサーバに移行しなければならない場合があります。この移行を新しい物理コンピュータに対して行う場合と、サーバ上のオペレーティング システムにメジャー アップグレードを施す場合（Windows 2003 から Windows 2008 に移行する場合など）があります。

Security Manager のバージョンは変更しないが、物理ハードウェアまたはオペレーティング システムを変更する場合は、移行プロセスを通過する必要があります。この移行プロセスは、基本的に、「サーバ アプリケーションのアップグレード」（P.5-5）に記載されているリモート バックアップ/復元アップグレード プロセスと同じものですが、Event Manager データ ストアに保存されたデータを移行する場合は追加のステップが必要です。Security Manager サーバの移行を実施する場合は、この手順を使用します。

（注）　オペレーティング システムに対するマイナー サービス パック アップデートは、それが Security Manager サーバ移行要件になるまで、アップグレードとは見なされません。サーバ移行は、オペレーティング システムの正式名称が変更される場合のように、異なるメジャー バージョンのオペレーティング システム同士を移行する場合に必要になります。

はじめる前に

この手順では、ターゲット サーバ（Security Manager を移行するサーバ）にソース コンピュータと同じデータベースとイベント データ ストアの内容を保存するものとします。ターゲット サーバ上で Security Manager の使用を開始している場合は、ソース システムとターゲット システムのデータベースまたはイベント データ ストアをマージできません。ターゲット データをソース データで置き換える必要があります。移行前にターゲット システム上に存在していたすべてのデータが、移行完了後に使用できなくなります。古いターゲット システム データを新しく移行するフォルダにコピーしないでください。

また、イベント データ ストアのコピーおよび復元ステップは、そのデータを保存する場合にのみ必要なことに注意してください。新しい空のイベント データ ストアから始める場合は、このステップを省略できます。

ステップ 1　ソース Security Manager サーバ（移行元のサーバ）上で次の手順を実行します。

a. イベント データ ストア フォルダの名前を特定します。Security Manager クライアントで、[Tools] > [Security Manager Administration] を選択し、コンテンツ テーブルから [Event Management] を選択します。フォルダは、[Event Data Store Location] フィールドに表示されています。デフォルトは *NMSROOT***MDC\eventing\database** で、NMSROOT はインストール ディレクトリ（通常は C:\Program Files\CSCOpx）です。

b. コマンドラインで次のように入力して、すべてのプロセスを停止します。

net stop crmdmgtd

c. *NMSROOT***MDC\eventing\config\collector.properties** ファイルのコピーとイベント データ ストア フォルダを作成します。そのコピーをターゲット コンピュータからアクセス可能なディスクに配置します。

d. 「CLI を使用したサーバ データベースのバックアップ」（P.5-11）に記載されているコマンドライン方式を使用して、Security Manager データベースをバックアップします。

ステップ 2　新しいターゲット コンピュータを準備します。例：

- オペレーティング システムをアップグレードするだけで、新しいハードウェアに移行しない場合は、オペレーティング システム アップグレードを実施して、オペレーティング システムが正しく機能していることを確認します。その後で、Security Manager をインストールします。
- 新しいコンピュータに移行する場合は、そのコンピュータが正しく機能していることを確認して、Security Manager をインストールします。

ステップ 3　ターゲット Security Manager サーバ上で次の手順を実行します。

a. コマンドラインで次のように入力して、すべてのプロセスを停止します。

net stop crmdmgtd

b. 「サーバ データベースの復元」（P.5-12）に記載されている手順を使用して、データベースを復元します。

c. データベース復元の完了後にプロセスを再起動しなかった場合は、ここで再起動します。

net start crmdmgtd

d. Security Manager クライアントを使用して新しいサーバにログインしてから、[Tools] > [Security Manager Administration] を選択して、目次から [Event Management] を選択します。

e. イベント データ ストア フォルダが存在し、それが空であることを確認します（必要に応じてファイルを削除します）。このフォルダには、ソース サーバ上のイベント データ ストアと同じ名前と場所を設定する必要があります。

f. 正しい [Event Data Store Location]（デフォルトが正しいフォルダでない場合）を選択して、[Enable Event Management] チェックボックスをオフにし、Event Manager サービスを停止します。[Save] をクリックして変更を保存します。サービスを停止するかどうかの確認が要求されます。[Yes] をクリックしてサービスの停止が通知されるまで待ちます。

g. バックアップされたイベント データ ストアをソース コンピュータからターゲット サーバ上の新しい場所にコピーします。

h. バックアップされた *NMSROOT***MDC\eventing\config\collector.properties** ファイルをソース コンピュータからターゲット コンピュータにコピーして、ターゲット サーバ上のファイルを上書きします。

i. Security Manager クライアントで、[Tools] > [Security Manager Administration] を選択し、コンテンツ テーブルから [Event Management] を選択します。[Enable Event Management] チェックボックスをオンにして、[Save] をクリックします。サービスを開始するかどうかの確認が要求されます。[Yes] をクリックしてサービスの開始が通知されるまで待ちます。

Security Manager の更新

インストール時に永久ライセンス ファイルを指定できますが、Security Manager のインストール後にもライセンスを追加できます。AUS にはライセンスは不要です。

はじめる前に

ライセンス ファイルをサーバ マシンまたはクライアント マシンにコピーしてから、ライセンスをアプリケーションに追加します。クライアント マシンを使用する場合は、クライアント側のブラウザをイネーブルにする必要があります。

（注）　ライセンス ファイルのパスには、アンパサンド（&）などの特殊文字が含まれていてはなりません。

ヒント　Security Manager にログイン中にライセンスを適用することもできます。Security Manager に、「Upgrade license」または「Continue Evaluation」のいずれかのメッセージが表示されます。「Upgrade License」をクリックすると、ライセンスを適用できます。

手順

Security Manager のライセンスをインストールするには、次の手順を実行します。

ステップ 1　Security Manager クライアント アプリケーションを使用してサーバにログインします（「Security Manager クライアントを使用した Security Manager へのログイン」（P.6-12）を参照）。

ステップ 2　[Tools] > [Security Manager Administration] を選択し、コンテンツ テーブルから [Licensing] を選択します。

ステップ 3　タブがアクティブになっていない場合は、[CSM] をクリックします。

ステップ 4　[Install a License] をクリックして、[Install a License] ダイアログボックスを開きます。このダイアログボックスを使用して、ライセンス ファイルを選択し、[OK] をクリックします。このプロセスを繰り返して他のライセンスを追加します。

（注）　パスとファイル名は、英語のアルファベット文字に制限されます。日本語文字はサポートされません。Windows 日本語 OS システムでファイルを選択する場合は、通常のファイル区切り文字 \ がサポートされますが、これは円記号（U+00A5）として表示されることがあることに注意する必要があります。

サービス パックとポイント パッチの入手

注意　Security Manager のサービス パックまたはポイント パッチは、シスコから入手してください。それ以外のファイルをダウンロードしたり、開いたりしないでください。サードパーティ製のサービス パックとポイント パッチはサポートされていません。

Security Manager またはその他のアプリケーションをインストールしたら、シスコから入手したサービス パックまたはポイント パッチをインストールして、バグを修復したり、新しいデバイス タイプをサポートしたり、アプリケーションを強化したりできます。

- 新しいサービス パックの入手可能な時期を知って、必要なサービス パックをダウンロードするには、Security Manager を開いて、[Help] > [Security Manager Online] を選択します。または、http://www.cisco.com/go/csmanager にアクセスします。
- 企業から Cisco TAC サービス リクエストが提出されると、TAC が、その問題の解決に役立つ未公開のポイント パッチがあるかどうかを通知します。これ以外の方法で Security Manager ポイント パッチが配布されることはありません。

サービス パックとポイント パッチは、クライアント ソフトウェア アップデートにサーバ サポートを提供し、クライアントとサーバ間のバージョン レベルのミスマッチを検出します。

サーバ アプリケーションのアンインストール

サーバ アプリケーションをアンインストールするには、この手順を使用します。アプリケーションをアンインストールする前に、アプリケーションの再インストールが必要な場合にデータを復元できるようにバックアップの実施を検討してください。バックアップの実施方法については、「リモート アップグレード時のデータベースのバックアップ」（P.5-10）を参照してください。

はじめる前に

任意のバージョンの Windows Defender がインストールされている場合は、それをディセーブルにしてからサーバ アプリケーションをアンインストールします。そうしなければ、アンインストール アプリケーションを起動できません。

手順

サーバ アプリケーションをアンインストールするには、次の手順を実行します。

ステップ 1　[Start] > [Programs] > [Cisco Security Manager] > [Uninstall Cisco Security Manager] を選択します。

デフォルトでは、すべてのアプリケーションがアンインストールされます。

ステップ 2　アンインストーラによって、すべてのアプリケーションが削除されます。

（注）　アンインストール中にエラーが発生した場合は、「アンインストール中のサーバ障害」（P.A-8）、および次の URL にある『*Installing and Getting Started With CiscoWorks LAN Management Solution 3.1*』の「Troubleshooting and FAQs」の章を参照してください。
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html

ステップ 3　リブートは必須ではありませんが、アンインストール後はサーバをリブートして、サーバ上のレジストリ エントリと実行中のプロセスが将来の再インストールに適切な状態になるようにすることを推奨します。

ステップ 4　Common Services を含むすべての Cisco Security Management Suite アプリケーションをアンインストールする場合のみ：

a. *NMSROOT* が残っている場合は、それを削除、移動、または名前を変更します。*NMSROOT* は Security Manager インストール ディレクトリへのパスです。*NMSROOT* のデフォルト値は **C:\Program Files\CSCOpx** です。**E:\Program Files\CSCOpx** などのその他の値も使用できます。

b. C:\CMFLOCK.TXT ファイルが存在する場合は、それを削除します。

c. アプリケーションを再インストールする前に、レジストリ エディタを使用して、次のレジストリ エントリを削除します。

- My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Resource Manager
- My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\MDC

ステップ 5　アプリケーションをアンインストールする前に Windows Defender をディセーブルにした場合は、ここで、もう一度イネーブルにします。

サーバ アプリケーションのダウングレード

Security Manager アプリケーションを以前のリリースにダウングレードして、この製品リリースで作成した設定を保持することはできません。このリリースの Security Manager を使用しない場合は、これをアンインストールし、必要な古いバージョンの製品を再インストールします（これは、必要なライセンスと古いバージョンのインストール メディアがそろっていることが前提です）。その後で、「サーバ データベースの復元」（P.5-12）に記載されているように、ダウングレードされたバージョンの以前のインストールで保存した必要なデータベースのバックアップを復元できます。

Security Manager をダウングレードする場合は、Auto Update Server も、再インストールする Security Manager のバージョンでサポートされるバージョンにダウングレードする必要があります。

古いデータベースを復元した場合、管理対象デバイスの現在の状態と同期しなくなったデバイスのプロパティやポリシーが含まれる可能性があることに注意してください。たとえば、デバイス上のオペレーティング システムを、古いバージョンの Security Manager では直接サポートされないものにアップグレードしたり、古いバージョンには存在しないポリシーを設定し、展開したりした可能性があります。データベースとデバイスを正しく同期させるために、すべての管理対象デバイスのデバイス ポリシーを再検出することを検討してください。大幅な変更（オペレーティング システムのメジャー リリースのアップグレードなど）では、デバイスをインベントリから削除し、再度追加しなければならない場合があることに注意してください。一部の例では、オペレーティング システムのアップグレードを元に戻す必要がある場合もあります（たとえば、ASA ソフトウェア リリース 8.3 は特別な処理が必要で、下位互換モードではサポートできないため、使用する Security Manager のバージョンで直接サポートされている必要があります）。詳細については、『User Guide for Cisco Security Manager』の「Managing the Device Inventory」の章を参照してください。

ヒント　古いバージョンの Security Manager では管理できないデバイスとオペレーティング システム リリースの組み合わせを管理しようとした場合、展開エラーが発生します。

CHAPTER 6

クライアントのインストールと設定

Security Manager アプリケーションと一緒に使用する重要なクライアント アプリケーションが 2 つあります。

- Security Manager クライアント。これは、ワークステーション上にインストールされ、通常は別のサーバ上にインストールされている Security Manager サーバ上で動作しているデータベースと相互作用するクライアント/サーバ アプリケーションです。このクライアントは一部の機能で Web ブラウザも使用します。
- Web ブラウザ。AUS を使用したり、Security Manager サーバや Common Services を使用する他のサーバを設定したりするために Web ブラウザを使用します。

次のトピックで、クライアントを実行するブラウザの設定方法と、Security Manager クライアントのインストール方法について説明します。

- 「Web ブラウザ クライアントの設定」（P.6-1）
- 「Security Manager クライアントのインストールに関するヒント」（P.6-6）
- 「Security Manager クライアントのインストール」（P.6-7）
- 「アプリケーションへのログイン」（P.6-12）
- 「Security Manager クライアントのアンインストール」（P.6-14）

Web ブラウザ クライアントの設定

Web ブラウザが、特定の種類のコンテンツを許可し、アプリケーションを実行しているサーバからのポップアップ ウィンドウをブロックしないように設定されていることを確認する必要があります。Web ブラウザは、オンライン ヘルプだけでなく、機能的なアプリケーション ウィンドウを表示するために使用されます。次の項で、ブラウザをアプリケーション クライアントとして効率的に使用するために必要な設定方法について説明します。

- 「HTTP/HTTPS プロキシ例外」（P.6-2）
- 「ブラウザ クッキーの設定」（P.6-2）
- 「Internet Explorer の設定」（P.6-2）
- 「Firefox の設定」（P.6-4）
- 「サードパーティ製ツールでの例外のイネーブル化と設定」（P.6-6）

HTTP/HTTPS プロキシ例外

HTTP/HTTPS プロキシを使用する場合は、Security Manager サーバ用のプロキシ例外を設定する必要があります。

この要件は、Internet Explorer と Firefox に適用されます。それぞれに対する追加設定の詳細を以降に説明します。

ブラウザ クッキーの設定

複数のブラウザがインストールされている場合、デフォルト ブラウザのクッキーを有効にする必要があります。具体的には、Internet Explorer のプライバシー設定は、中レベル以下（IE > [Tools] > [Internet Options] > [Privacy Settings] <= [Medium]）に設定する必要があります。

クッキーをブロックすることにより、Security Manager のユーザ ログインは Security Manager のクリーン インストール後も失敗する場合があります。ユーザ ログインが Security Manager のクリーン インストール後に失敗した場合は、次のエラー メッセージが表示される場合があります。「CMF session id cannot be assigned.」

Internet Explorer の設定

Security Manager とそのアプリケーションを正しく機能させるために必要な Internet Explorer の設定がいくつかあります。Internet Explorer は、オンライン ヘルプ、アクティビティ レポート、CS-MARS ルックアップ情報などの表示に使用されます。この手順では、Internet Explorer に必要な設定について説明します。

手順

ステップ 1　Internet Explorer 8 を使用している場合は、互換表示を使用します。Internet Explorer 8 は、互換表示の場合にのみサポートされています。互換表示を使用するには、Internet Explorer 8 を開いて、[Tools] > [Compatibility View Settings] に移動し、[website to be displayed in Compatibility View] として Security Manager サーバを追加します。

ステップ 2　次の手順を実行して、Security Manager のポップアップ ブロックをオフにします。

a. Internet Explorer を開きます。

b. [Tools] > [Pop-up Blocker] > [Pop-up Blocker Settings] に移動します。

c. [Address of website to allow] フィールドに、Security Manager サーバの IP アドレスを入力して、[Add] をクリックします。
http://windows.microsoft.com/en-US/windows-vista/Internet-Explorer-Pop-up-Blocker-frequently-asked-questions を参照してください。

注意　ポップアップ ブロックをオフにしなかった場合は、Security Manager でデバイスを検出できない可能性があります。

ヒント　「ポップアップ ブロックは、ポップアップの大半を制限またはブロックする Internet Explorer の機能です。」 http://windows.microsoft.com/en-US/windows-vista/Internet-Explorer-Pop-up-Blocker-frequently-asked-questions を参照してください。

ステップ 3　Internet Explorer で、[Tools] > [Internet Options] を選択します。この手順内の以降のステップは、[Internet Options] ダイアログボックス上で実行します。

ステップ 4　アクティブ コンテンツを許可するには、次の手順を実行します。

a. [Advanced] タブをクリックして、[Security] セクションにスクロールし、[Allow active content to run in files on My Computer] を選択します。

b. [Apply] をクリックして変更内容を保存します。

ステップ 5　ブラウザのセキュリティ設定が、暗号化されたページをディスクに保存できるようになっていることを確認します。暗号化されたページを保存できない場合は、クライアント ソフトウェア インストーラをダウンロードできません。

[Advanced] タブの [Security] エリアで、[Do not save encrypted Pages to Disk] を選択解除します。設定を変更する必要がある場合は、[Apply] をクリックして変更を保存します。

ステップ 6　一時ファイル用のディスク キャッシュのサイズが、ダウンロードを予定しているクライアント ソフトウェア インストーラのサイズを上回っていることを確認します。キャッシュ割り当てが少なすぎる場合は、インストーラをダウンロードできません。キャッシュ サイズを変更するには、次の手順を実行します。

a. [General] タブをクリックします。

b. [Temporary Internet Files] グループで [Settings] をクリックします。

c. 必要に応じて、インターネット一時ファイルに使用されるディスク スペースの容量を増やして [OK] をクリックします。

d. [Apply] をクリックして変更内容を保存します。

ステップ 7　（任意）CS-MARS と Security Manager 間でデータをやり取りするときに、セキュア コンテンツとノンセキュア コンテンツの両方が含まれたページを開かなければならないことがあります。デフォルトで、Internet Explorer からノンセキュア項目を表示するかどうかが尋ねられます。このプロンプトで [Yes] をクリックすると、ソフトウェアを正常に機能させることができます。

必要な場合は、プロンプトが表示されず、混合コンテンツ、つまり、セキュア コンテンツとノンセキュア コンテンツの両方が含まれるページが自動的に表示されるように Internet Explorer の設定を変更できます。混合コンテンツ ページを表示するように Internet Explorer を設定するには、次の手順を実行します。

a. [Security] タブをクリックします。

b. ダイアログボックス下部の [Custom Level] をクリックします。

c. [Miscellaneous] 見出しの下で、[Display mixed content] 設定に対応する [Enable] オプション ボタンを選択します。（[Disable] が選択されていないことを確認してください）。

d. [Apply] をクリックして変更内容を保存します。

ステップ 8　[OK] をクリックして [Internet Options] ダイアログボックスを閉じます。

Firefox の設定

Security Manager とそのアプリケーションを正しく機能させるために必要な Firefox の設定がいくつかあります。Firefox は、オンライン ヘルプ、アクティビティ レポート、CS-MARS ルックアップ情報などの機能の表示に使用します。この手順では、Firefox の設定に必要なオプションについて説明します。

- 「プリファレンス ファイルの編集」（P.6-4）
- 「ディスク キャッシュのサイズの編集」（P.6-4）
- 「ポップアップ ブロックのディセーブル化またはホワイト リストの作成」（P.6-4）
- 「JavaScript のイネーブル化」（P.6-5）
- 「最新ウィンドウ内の新しいタブ上でのオンライン ヘルプの表示と以降の要求に対する既存のウィンドウの再利用」（P.6-5）

プリファレンス ファイルの編集

手順

プリファレンス ファイルを編集するには、次の手順を実行します。

ステップ 1　メモ帳などのテキスト エディタで、\Mozilla Firefox\defaults\pref サブディレクトリにある **firefox.js** を開きます。

ステップ 2　次の式を追加します。

```
pref("dom.allow_scripts_to_close_windows", true);
```

ステップ 3　編集したファイルを保存して閉じます。

ディスク キャッシュのサイズの編集

一時ファイル用のディスク キャッシュのサイズが、ダウンロードを予定しているクライアント ソフトウェア インストーラのサイズを上回っていることを確認します。キャッシュ割り当てが少なすぎる場合は、インストーラをダウンロードできません。

手順

キャッシュ サイズを変更するには、次の手順を実行します。

ステップ 1　[Tools] > [Options] を選択してから、[Advanced] をクリックします。

ステップ 2　設定が少なすぎる場合は、より多くのキャッシュ スペースを確保して、[OK] をクリックします。

ポップアップ ブロックのディセーブル化またはホワイト リストの作成

手順

ポップアップ ブロックをディセーブルにするには、次の手順を実行します。

ステップ 1　[Tools] > [Options] を選択してから、[Contents] アイコンをクリックします。

ステップ 2　[Block pop-up windows] チェックボックスをオフにします。

または、ポップアップを受け入れる信頼できるソースのホワイト リストを作成するには、[Block pop-up windows] チェックボックスをオンにしてから、[Exceptions] をクリックして [Allowed Sites - Popups] ダイアログボックスで次の手順を実行します。

a. [Address of web site] フィールドに **http://**<*SERVER_NAME*>（ここで、*SERVER_NAME* は Security Manager サーバの IP アドレスまたは DNS ルーティング可能名）と入力してから、[Allow] をクリックします。

b. **file:///***C:*/**Documents%20and%20Settings/**<*USER_NAME*>**/Local%20Settings/Temp/**（ここで、*C:* は Windows がインストールされているクライアント システムのディスク ドライブで、*USER_NAME* はクライアント システム上の Windows ユーザ名）と入力してから、[Allow] をクリックします。

c. [Close] をクリックします。

ステップ 3　[OK] をクリックします。

JavaScript のイネーブル化

手順

JavaScript をイネーブルにするには、次の手順を実行します。

ステップ 1　[Tools] > [Options] を選択してから、[Contents] アイコンをクリックします。

ステップ 2　[Enable JavaScript] チェックボックスをオンにします。

ステップ 3　[Advanced] をクリックし、[Advanced JavaScript Settings] ダイアログボックスで、[Allow scripts to] エリア内のすべての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。

最新ウィンドウ内の新しいタブ上でのオンライン ヘルプの表示と以降の要求に対する既存のウィンドウの再利用

初めてオンライン ヘルプにアクセスしたときに、2 つの新しいブラウザ ウィンドウ（空のページとヘルプ コンテンツが含まれるページ）が開くことがあります。その後、オンライン ヘルプにアクセスしようとしたときに、既存のブラウザ ウィンドウが再利用されないこともあります。

手順

最近開かれたブラウザ ウィンドウの新しいタブ上にオンライン ヘルプを表示し、それ以降は既存のブラウザ ウィンドウを再利用するように Firefox を設定するには、次の手順を実行します。

ステップ 1　アドレス バーに、**about:config** と入力して、Enter を押します。ユーザ プリファレンスのリストが表示されます。

ステップ 2　[browser.link.open_external] をダブルクリックして、表示されたダイアログボックスに **3** と入力します。この値は、外部アプリケーションからのリンクが、最後に開かれたブラウザ ウィンドウ内の新しいタブで開かれることを意味します。

ステップ 3　[browser.link.open_newwindow] をダブルクリックして、それを **1** に設定します。この値は、リンクがアクティブなタブまたはウィンドウで開かれることを意味します。

ステップ 4　[browser.link.open_newwindow.restriction] をダブルクリックして、それを **0** に設定します。この値は、新しいウィンドウのすべてがタブとして開かれることを意味します。

ステップ 5　[about:config] ページを閉じます。

（注）　ブラウザのステータス バーに Done というステータスが表示された後でも、状況依存のヘルプを開いたときに空白のページが開く場合があります。この問題が発生した場合は、数分待てば、コンテンツがダウンロード可能になり、表示されます。

サードパーティ製ツールでの例外のイネーブル化と設定

一部のサードパーティ製ポップアップ ブロックを使用すれば、通常はポップアップを拒否しながら、特定のサイトまたはサーバからのポップアップだけを許可できます。ポップアップ ブロックでホワイト リストに例外を含めることができない場合、または、そのオプションでは要件が満たせない場合は、すべてのポップアップを許可するようにユーティリティを設定する必要があります。信用されたサイトからのポップアップを許可する方式は、使用されているユーティリティによって異なります。詳細については、サードパーティ製品のマニュアルを参照してください。

Security Manager クライアントのインストールに関するヒント

Security Manager クライアントを使用してデバイスを設定します。クライアントで変更を保存すると、それらはワークステーションに保存されます。続いて、変更をデータベースに送信して、サーバ上のデータベースを更新する必要があります。

クライアントを使用している間は、クライアントとサーバ間で継続的に相互通信が行われます。この点を踏まえて、クライアントをインストールしてそのパフォーマンスを向上させるためのヒントを考慮してください。

- サーバと同じコンピュータ上でクライアントを日常業務として実行しないでください。クライアントをサーバ上にインストールした場合は、トラブルシューティングの目的にのみ使用してください。
- ネットワーク遅延の問題を避けるために、クライアントはサーバからあまり離れていないワークステーション上にインストールします。たとえば、米国にサーバを設置しながら、インド国内のネットワークからクライアントを実行した場合は、遅延が生じて応答性能が低下する可能性があります。この問題を軽減するには、クライアントがサーバと同じデータセンター内に設置される、リモート デスクトップまたはターミナル サーバ配置を採用する必要があります。
- 1 台のコンピュータ上には 1 つのクライアントのコピーしかインストールできません。クライアントとサーバのバージョンは完全に一致する必要があります。したがって、2 つの異なるバージョンの Security Manager 製品を実行する場合は、それぞれのクライアントを実行する 2 台のワークステーションを用意する必要があります。

  一方で、クライアントを複数回起動して、同じバージョンを実行している複数の Security Manager サーバに接続できます。

Security Manager クライアントのインストール

Security Manager クライアントは、ワークステーション上にインストールする個別のプログラムです。このクライアントを使用して、Security Manager サーバにログインして、デバイスに関するセキュリティ ポリシーを設定します。Security Manager クライアントは、製品と一緒に使用するメイン アプリケーションです。

サーバ ソフトウェアがインストールされていれば、Security Manager サーバ上にクライアントがインストールされている可能性があります。ただし、サーバと同じシステム上でクライアントを使用する場合は、製品の日常的な使用を避けることを推奨します。代わりに、次の手順を使用して、クライアントを別のワークステーションにインストールしてください。ワークステーション システムの要件とサポートされているブラウザのバージョンについては、「クライアントの要件」（P.3-10）を参照してください。

インストール中に問題が発生した場合は、次のトピックを参照してください。

- 「インストールを阻止するセキュリティ設定の処理」（P.6-10）
- 「以前のバージョンのクライアントからアップグレードできない」（P.6-11）
- 「インストール中のクライアント障害」（P.A-10）

はじめる前に

- ブラウザが正しく設定されていることを確認します。「Web ブラウザ クライアントの設定」（P.6-1）を参照してください。
- Windows ファイアウォールが正しく設定されていることを確認します。Security Manager でサポートされるオペレーティング システムでは、Windows ファイアウォールはデフォルトでイネーブルになっています。その結果、HTTP、HTTPS、および syslog の着信接続がブロックされます。たとえば、管理者はサーバの Security Manager クライアントのインストール URL にローカルでアクセスできますが、リモート ワークステーションからはアクセスできません。また、syslog データは Event Viewer に表示されません。Windows ファイアウォールをディセーブルにするか、問題になっている管理トラフィックを許可する着信ルールを設定する必要があります。

注意　ワークステーションの Windows ファイアウォールをディセーブルにすると、Windows ファイアウォールのイネーブル時に防御されていた悪意のあるアクティビティに対して無防備になります。

- クライアント ソフトウェア インストーラをダウンロードする前に、クライアント システム上の Temp ファイルを手動で削除することを推奨します。このようなファイルを削除することによって、使用可能な十分なスペースを確保できる可能性があります。
- ワークステーションに Cisco Security Agent がインストールされている場合は、クライアントのインストール プロセスの前または中に、それをディセーブルにする必要があります。インストール プロセス中にクライアント インストーラが Cisco Security Agent をディセーブルできなかった場合は、プロセスが中断して、クライアントのインストールを再開する前に、Cisco Security Agent を手動でディセーブルにするように要求されます。

ヒント ワークステーション上の Cisco Security Agent をディセーブルにするには、次の 2 つの方法のいずれかを使用します：(1) システム トレイ内の Cisco Security Agent アイコンを右クリックし、[Security Level] > [Off] を選択するか、(2) [Services] を開き（[Control Panel] > [Administrative Tools] > [Services]）、[Cisco Security Agent] を右クリックし、[Stop] をクリックします。2 つのどちらの方法の場合でも、Windows のバージョンによっては、次の手順を実行する必要があります。[Services] を開き、[Cisco Security Agent Monitor] をクリックして [Stop] をクリックします。クライアントのインストール終了後、Cisco Security Agent を再起動します。

注意 ワークステーション上で Cisco Security Agent がディセーブルになっている間は、Cisco Security Agent のイネーブル時に防御されていた悪意のあるアクティビティに対して無防備になります。

- すでに Security Manager クライアントがワークステーション上にインストールされている場合は、インストール プログラムが最新のクライアントをインストールする前に Security Manager クライアントをアンインストールする必要があります。ウィザードからこの必要があるかどうかが尋ねられます。

手順

ステップ 1　Windows 管理者特権を持つユーザ アカウントを使用してクライアント ワークステーションにログインします。

ステップ 2　Web ブラウザで、次の URL のいずれかを開きます。ここで、*SecManServer* は、Security Manager がインストールされているコンピュータの名前です。いずれかのセキュリティ アラート ウィンドウで [Yes] をクリックします。

- SSL を使用していない場合は、**http://***SecManServer***:1741** を開きます。
- SSL を使用している場合は、**http://***SecManServer***:443** を開きます。

Cisco Security Management Suite のログイン画面が表示されます。ページ上で、JavaScript と cookie がイネーブルになっていることと、サポートされているバージョンの Web ブラウザを実行していることを確認します。

ステップ 3　ユーザ名とパスワードを使用して、Cisco Security Management Suite サーバにログインします。初めてサーバをインストールする場合は、ユーザ名の **admin** と製品のインストール中に定義されたパスワードを使用してログインできます。

ステップ 4　Cisco Security Management Suite のホームページで、[Cisco Security Manager Client Installer] をクリックします。

ファイルを開くまたは実行するのか、ディスクに保存するのかが尋ねられます。いずれかのオプションを選択できます。ファイルのディスクへの保存を選択した場合は、ファイルのダウンロード後にプログラムを実行します（ファイルをダブルクリックするか、ブラウザから尋ねられたときに [Run] オプションを選択します）。

ヒント「a problem was detected」や「the publisher cannot be verified」などのアプリケーションに関するセキュリティ警告、または、未確認のアプリケーションがコンピュータにアクセスしようとしているという内容のセキュリティ警告が表示された場合は、アクセスが許可されていることを確認します。複数のボタンをクリックしなければならない場合があります。ボタン名はアプリケーションのプロンプトによって異なります（[Allow]、[Yes]、[Apply] など）。

ステップ 5　インストール ウィザードの [Welcome] 画面が開き、次の文が表示されます。「Install these Cisco Security Manager 4.5 client applications:」

- Configuration Manager
- Event Viewer
- Report Manager
- Health and Performance Manager
- Image Manager
- ダッシュボード

Security Manager クライアントは、6 台のアプリケーション スイートとしてインストールされます。Configuration Manager、Event Viewer、Report Manager、Health and Performance Manager、Image Manager およびダッシュボード。各アプリケーションは、次の 3 つの方法のいずれかで別々に起動できます（各アプリケーションの起動方法の詳細については、「Security Manager クライアントを使用した Security Manager へのログイン」（P.6-12）を参照してください）。

- [Start] > [All Programs] > [Cisco Security Manager Client]（フォルダ）> [Cisco Security Manager Client]
- （ログイン画面）
- （いずれかのアプリケーションを起動した後）[Launch] >（Security Manager クライアント アプリケーション スイート内の他のアプリケーションを選択する）

（注）　Cisco Security Manager のデスクトップ アイコンも作成されます。このアイコンで Cisco Security Management Suite のホーム ページを開きます。

ステップ 6　インストール ウィザードの指示に従います。インストール中に、次の情報の入力が要求されます。

- [Server name]：Security Manager サーバ ソフトウェアがインストールされているサーバの DNS 名または IP アドレス。通常は、クライアント インストーラをダウンロードしたサーバです。
- [Protocol]：HTTPS または HTTP。Security Manager サーバで使用されるプロトコルを選択します。ほとんどのサーバは HTTPS を使用するように設定されます。どれを選択していいかがわからない場合は、システム管理者にお問い合わせください。また、サーバが非デフォルト ポートを使用するように設定されていることがわかっている場合は、「非デフォルト HTTP または HTTPS ポートの設定」（P.6-10）内の情報を使用してインストール後にポートを設定します。
- [Shortcuts]：自分専用のショートカットだけを作成するのか、このワークステーションにログインしているすべてのユーザ アカウント用のショートカットを作成するのか、またはどのユーザ用のショートカットも作成しないのか。これによって、誰の [Start] メニューに Cisco Security Manager Client が表示されるかが決定されます。クライアントは、[Start] > [Programs] > [Cisco Security Manager Client]（フォルダ）> [Cisco Security Manager Client] またはデスクトップ上のアイコンから起動できます。
- [Installation location]：クライアントをインストールするフォルダ。他の場所にインストールする特別な理由がなければ、デフォルトを受け入れます。デフォルトの場所は、C:\Program Files\Cisco Systems です。

ステップ 7　インストール ウィザードの指示に従って続行します。

ステップ 8　[Done] をクリックしてインストールを完了したら、アンチウイルス アプリケーションを一時的にディセーブルにしていた場合はイネーブルに戻します。

クライアント インストーラによってワークステーション上の Cisco Security Agent が停止されていた場合は、インストールの完了時に再起動されます。ただし、システム上で Cisco Security Agent を手動でディセーブルにしていた場合は、クライアントのインストールが完了してからそれをイネーブルにする必要があります。

インストールを阻止するセキュリティ設定の処理

ワークステーション上のセキュリティ設定を構成可能な複数の方法と、Security Manager クライアントのインストールを阻止するためにインストール可能な複数の製品が存在します。インストール中に問題が発生した場合は、Windows ユーザ アカウントにソフトウェアのインストールに必要な管理特権が付与されていることを確認してから、次のヒントを考慮してください。

- （Windows XP）Internet Explorer セキュリティ強化のデフォルト設定では、サーバからのインストール ユーティリティのダウンロードが阻止される可能性があります。この場合は、次のメッセージが表示されます。

  ```
  Internet Explorer cannot download CSMClientSetup.exe from <server>.Internet Explorer
  was not able to open this Internet site.The requested site is either unavailable or
  cannot be found.Please try again later.
  ```

  この問題を解決するには、[Start] > [Settings] > [Control Panel] > [Add or Remove Programs] を選択してから、[Add/Remove Windows Components] をクリックします。Windows コンポーネント ウィザード ウィンドウで、[Internet Explorer Enhanced Security Configuration] チェックボックスをオフにして、[Next] をクリックし、[Finish] をクリックします。
- （Windows XP SP2）向上したセキュリティ機能によって、次のメッセージが表示される可能性があります。

  ```
  Security Warning Message.The publisher could not be verified.Are you sure you want to
  run this software?
  ```

  このメッセージが表示されたら、[Yes] をクリックして継続します。

非デフォルト HTTP または HTTPS ポートの設定

Security Manager サーバは、443 の HTTPS と 1741 の HTTP のデフォルト ポートを使用します。組織で別のポートを使用するように Security Manager サーバをインストールしていた場合は、非標準ポートを使用するようにクライアントを設定する必要があります。そうしなければ、クライアントとサーバを接続できません。

クライアントの別のポートを設定するには、メモ帳などのテキスト エディタを使用して **C:\Program Files\Cisco Systems\Cisco Security Manager Client\jars\client.info** ファイルを編集します。次の設定を追加して、<*port number*> の場所にカスタム ポート番号を指定します。

- HTTPS_PORT=<*port number*>
- HTTP_PORT=<*port number*>

これらの設定は、次のクライアントを起動したときに使用されます。

以前のバージョンのクライアントからアップグレードできない

古いバージョンのクライアントがインストールされている、または、クライアントがインストールされていたことがあるワークステーション上に Security Manager クライアントをインストールしようとした場合は、クライアント インストーラによって新しいバージョンがインストールされる前に古いバージョンがアンインストールされます。「Could not find main class.Program will exit」というエラー メッセージが表示された場合は、インストーラでクライアントをインストールできません。

手順

この問題は、システム内に古いレジストリ エントリが残っている場合に発生します。この問題を解決するには、次の手順を実行します。

ステップ 1　[Start] > [Run] を選択して、**regedit** と入力することによって、レジストリ エディタを起動します。

ステップ 2　次のレジストリ キーを削除します。

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\f427e21299b0dd254754c0d2778feec4-837992615

ステップ 3　以前のインストール ディレクトリ（通常は、C:\Program Files\Cisco Systems\Cisco Security Manager Client）を削除します。

ステップ 4　次のフォルダの名前を変更します。

C:\Program Files\Common Files\InstallShield\Universal\common\Gen1

ステップ 5　[Start] > [Control Panel] > [Add or Remove Programs] を選択します。Cisco Security Manager Client がまだ表示されている場合は、[Remove] をクリックします。「Program already removed; do you want to remove it from the list?」というメッセージが表示されたら、[Yes] をクリックします。

まだ Security Manager クライアントを再インストールできない場合は、C:\Program Files\Common Files\InstallShield ディレクトリの名前を変更して、もう一度試してみてください。「インストール中のクライアント障害」（P.A-10）も参照してください。

クライアントのパッチング

サービス パックまたはポイント パッチを Security Manager サーバに適用したら、サーバにログインしたときに Security Manager クライアントからアップデートを適用するかどうかが尋ねられます。クライアント ソフトウェアのバージョン番号は、サーバ ソフトウェアのバージョン番号と同じにする必要があります。

必要なソフトウェア アップデートをダウンロードして適用するかどうかが尋ねられた場合は、Web ブラウザがアップデートのダウンロードに使用されます。ファイルを開くまたは実行するのか、ディスクに保存するのかが尋ねられます。いずれかのオプションを選択できます。ファイルのディスクへの保存を選択した場合は、ファイルのダウンロード後にプログラムを実行します（ファイルをダブルクリックするか、ブラウザから尋ねられたときに [Run] オプションを選択します）。

パッチのインストールは、クライアントのインストールに似ているため、Cisco Security Agent またはインストーラの起動を可能にするためにインストールしたその他のセキュリティ ソフトウェアからの任意のセキュリティ アラートを許可（または [Yes] をクリック）する必要があります。

インストールの場所が尋ねられたら、クライアントがインストールされているフォルダが選択されていることを確認して、ファイルを上書きするかどうかが尋ねられたら [Yes to All] を選択します。

ヒント　URL が取得できない、または、接続がタイムアウトしたことを伝えるエラー メッセージが表示された場合は、Security Manager クライアントをアンインストールしてから、フレッシュ コピー（すでにパッチが適用されている）をインストールする必要があります。詳細については、「Security Manager クライアントのアンインストール」（P.6-14）および「Security Manager クライアントのインストール」（P.6-7）を参照してください。

アプリケーションへのログイン

サーバ アプリケーションをインストールし、Web ブラウザを設定し、Security Manager クライアントをインストールしたら、アプリケーションにログインできます。

- 「Security Manager クライアントを使用した Security Manager へのログイン」（P.6-12）
- 「Web ブラウザを使用したサーバ アプリケーションへのログイン」（P.6-13）

Security Manager クライアントを使用した Security Manager へのログイン

Security Manager クライアントは、6 台のアプリケーション スイートとしてインストールされます。Configuration Manager、Event Viewer、Report Manager、Health and Performance Manager、Image Manager およびダッシュボード。各アプリケーションは、後述の手順内で示される 3 つの方法のいずれかで別々に起動できます。

ほとんどの Security Manager タスクは、Configuration Manager アプリケーション（Security Manager クライアント アプリケーション スイートの一部）を使用して実行します。

ヒント　Security Manager クライアントを十分に活用できる管理者特権が付与された Windows ユーザ アカウントを使用してクライアント ワークステーションにログインする必要があります。より低い特権を使用してクライアントを操作しようとした場合は、一部の機能が正しく機能しない場合があります。

手順

ステップ 1　Configuration Manager、Event Viewer、Report Manager、Health and Performance Monitor、Image Manager またはダッシュボードのいずれかを起動します。各アプリケーションは、次の 3 つの方法のいずれかで別々に起動できます。

- [Start] > [All Programs] > [Cisco Security Manager Client]（フォルダ）> [Cisco Security Manager Client]
- （ログイン画面）
- （いずれかのアプリケーションを起動した後）[Launch] >（Security Manager クライアント アプリケーション スイート内の他のアプリケーションを選択する）。ログイン ダイアログ ウィンドウは表示されません。

ステップ 2　Security Manager のログイン ダイアログ ウィンドウで、ログインするサーバの DNS 名を入力または選択します。

（注）　DNS 名ではなく IP アドレスを入力または選択すると、Internet Explorer 7 環境において一部の機能が意図したとおりに動作しない可能性があります。すべての Security Manager 機能を正しく動作させるには、ログインするサーバの DNS 名を入力します。

ステップ 3　Security Manager のユーザ名とパスワードを入力します。

ステップ 4　サーバが接続に HTTPS を使用する場合は、[HTTPS] チェックボックスがオンになっていることを確認します。HTTPS を使用しない場合は、そのチェックボックスをオフにします。[Login] をクリックします。

ステップ 5　サーバからクライアント ソフトウェア アップデートのダウンロードとインストールが要求された場合は、「クライアントのパッチング」（P.6-11）を参照してください。

ステップ 6　ご使用のクライアントよりも新しいバージョンを実行している Security Manager サーバにログインすると、通知が表示され、一致するクライアント バージョンをダウンロードするオプションが提供されます。

ステップ 7　入力したユーザ名とパスワードで実行中のセッションがない場合は、クライアント アプリケーション（Configuration Manager、Event Viewer、Report Manager、Health and Performance Monitor、Image Manager、またはダッシュボード）がサーバにログインして、クライアント インターフェイスを開きます。

ステップ 8　入力したユーザ名とパスワードで実行中のセッションがすでに存在する場合は、既存のアプリケーションから同一セッションで新しいアプリケーションを簡単に起動できる方法があることを知らせる情報メッセージが表示されます。その方法とは、次のとおりです。

（いずれかのアプリケーションを起動した後）[Launch] >（Security Manager クライアント アプリケーション スイート内の他のアプリケーションを選択する）。

ステップ 9　新しいアプリケーションが既存のセッションから起動されるか、すでに実行中ならばそのアプリケーションがフォーカス状態になります。

ヒント　クライアントは 120 分間アイドル状態が続くと自動的に閉じます。アイドル タイムアウトを変更するには、[Tools] > [Security Manager Administration] を選択して、目次から [Customize Desktop] を選択し、必要なタイムアウト期間を入力します。この機能をディセーブルにして、クライアントが自動的に閉じないようにすることもできます。

ステップ 10　Security Manager を終了する場合は、[File] > [Exit] を選択します。

Web ブラウザを使用したサーバ アプリケーションへのログイン

正規の Windows アプリケーションを使用してクライアント アプリケーションをホストするのは、Security Manager サーバだけです。Security Manager（Common Services アプリケーション経由）、CiscoWorks、および Auto Update Server のサーバ管理機能を含め、その他すべてのアプリケーションは Web ブラウザ内でホストされます。

これらのアプリケーションへのログイン方法は同じです。1 台のサーバ上に複数のアプリケーションをインストールした場合は、インストールしたすべてのアプリケーションに同時にログインします。これは、ログインが CiscoWorks によって制御され、これらのアプリケーションはすべて CiscoWorks の制御下でホストされるためです。

手順

ステップ 1　Web ブラウザで、次のいずれかの URL を開きます。*server* は、サーバ アプリケーションがインストールされているコンピュータの名前です。いずれかのセキュリティ アラート ウィンドウで [Yes] をクリックします。

- SSL を使用していない場合は、http://*server*:1741 を開きます。
- SSL を使用している場合は、http://*server*:443 を開きます。

Cisco Security Management Suite のログイン画面が表示されます。ページ上で、JavaScript と cookie がイネーブルになっていることと、サポートされているバージョンの Web ブラウザを実行していることを確認します。アプリケーションを実行するようにブラウザを設定する方法については、「Web ブラウザ クライアントの設定」（P.6-1）を参照してください。

ステップ 2　ユーザ名とパスワードを使用して、Cisco Security Management Suite サーバにログインします。初めてサーバをインストールする場合は、ユーザ名の **admin** と製品のインストール中に定義されたパスワードを使用してログインできます。

ステップ 3　Cisco Security Management Suite のホームページで、サーバ上にインストールされた機能にアクセスできます。このホームページには、インストールされているものによって異なる項目を含めることができます。

- 実行するアプリケーション（**Auto Update Server** など）に対応するパネルをクリックします。
- [Server Administration] パネルをクリックして、CiscoWorks Common Services サーバ メニューを開きます。このリンクをクリックすれば、Common Services 内の任意の場所に移動できます。CiscoWorks Common Services は、サーバを管理する基盤ソフトウェアです。このソフトウェアを使用して、サーバの保守とトラブルシューティングやローカル ユーザ定義などのバックエンド サーバ機能を設定して管理します。
- [CiscoWorks] リンク（ページの右上）をクリックして、サーバ上で CiscoWorks ホームページを開きます。
- [Cisco Security Manager Client Installer] をクリックして、Security Manager クライアントをインストールします。このクライアントは、Security Manager サーバを使用するためのメイン インターフェイスです。

ステップ 4　アプリケーションを終了するには、画面右上にある [Logout] をクリックします。ホームページと Security Manager クライアントの両方を同時に開いている場合は、ブラウザ接続を終了しても Security Manager クライアントが終了しません。

Security Manager クライアントのアンインストール

Security Manager クライアントをアンインストールする場合は、[Start] > [Programs] > [Cisco Security Manager Client] > [Uninstall Cisco Security Manager Client] を選択して、アンインストール ウィザードの指示に従います。

インストール後のサーバ タスク

次のトピックは、Security Manager またはその関連アプリケーションをサーバ上にインストールしてから実行すべきタスクです。

- 「すぐに実行すべきサーバ タスク」（P.7-1）
- 「必要なプロセスが動作しているかどうかの確認」（P.7-2）
- 「MRF を使用した Security Manager プロセスのヒープ サイズの設定」（P.7-2）
- 「現行のサーバ セキュリティに関するベスト プラクティス」（P.7-7）
- 「インストールまたはアップグレードの確認」（P.7-7）
- 「関連情報」（P.7-8）

すぐに実行すべきサーバ タスク

インストール直後に次のタスクを実行してください。

✓	タスク
❑	**1. アンチウイルス スキャナと同等の製品を再イネーブルまたは再インストールします。**アンチウイルス ツールなどのサーバ セキュリティ ソフトウェアをアンインストールまたは一時的にディセーブルにした場合は、今すぐ、そのソフトウェアを再インストールまたは再起動して、必要に応じてサーバを再起動します。 **（注）** アンチウイルス ソフトウェアが原因で Security Manager サーバの効率性や応答性が損なわれていることが判明した場合は、アンチウイルス ソフトウェアのマニュアルで推奨設定を確認してください。
❑	**2. インストール中にディセーブルにしたサービスとサーバ プロセスを再イネーブルします。**IIS は再イネーブルしないでください。
❑	**3. Sybase テクノロジーやソフトウェア コードを使用しているアプリケーションも含めて、インストール中にディセーブルにした基幹業務アプリケーションを再イネーブルします。**
❑	**4. サーバ上で、自己署名証明書を信頼できる証明書のリストに追加します。**手順については、ブラウザのマニュアルを参照してください。
❑	**5. Cisco.com 上で Security Manager とその関連アプリケーションのアップデートをチェックします。**アップデートが入手可能なことがわかった場合は、組織やネットワークに関連するアップデートをインストールします。

必要なプロセスが動作しているかどうかの確認

Windows のコマンド プロンプト ウィンドウから **pdshow** コマンドを実行して、インストールする Cisco サーバ アプリケーションに必要なプロセスのすべてが正しく動作していることを確認できます。プロセス要件はアプリケーションによって異なります。

ヒント　**pdshow** の詳細については、Common Services のマニュアルを参照してください。

表 7-1 を使用して、どのアプリケーションにどのプロセスが必要かを確認してください。

表 7-1　アプリケーション プロセス要件

アプリケーション	必要な Daemon Manager プロセス
Common Services	Apache CmfDbEngine CmfDbMonitor CMFOGSServer CSRegistryServer DCRServer diskWatcher EDS EDS-GCF ESS EssMonitor jrm LicenseServer Proxy Tomcat TomcatMonitor NameServer NameServiceMonitor EventFramework
Cisco Security Manager	AthenaOGSServer ccrWrapper CsmReportServer rptDbEngine rptDbMonitor VmsBackendServer vmsDbEngine vmsDbMonitor VmsEventServer CsmHPMServer
Auto Update Server	AusDbEngine AusDbMonitor

MRF を使用した Security Manager プロセスのヒープ サイズの設定

Security Manager 4.1 で導入された機能である Memory Reservation Framework（MRF）は、Cisco Security Manager 管理者に、主要プロセスのヒープ サイズを変更する機能を提供します。それにより、サーバのパフォーマンスを向上させることができます。MRF を使用すると、プロセスは、サーバに搭載された RAM の容量に基づいてヒープ サイズを調整できるようになります。

MRF を使用して設定可能な Security Manager プロセスを表 7-2 に示します。

表 7-2　MRF を使用して設定可能な Security Manager プロセス [1]

プロセス	pdshow で表示される名前[2]	説明
バックエンド プロセス	VmsBackendServer	デバイス検出操作と展開操作を実行します。
Tomcat	Tomcat	ポリシーなどの編集および検証を行うためのアプリケーションをホストします。
レポート サーバ	CsmReportServer	レポート データを生成します。
イベント サーバ	VmsEventServer	デバイスから送信されているイベントを収集します。

1. HPM（Health and Performance Monitor）サーバの MRF 設定はありません。
2. pdshow コマンドの詳細については、前述の必要なプロセスが動作しているかどうかの確認および Common Services のマニュアルを参照してください。

デフォルト コンフィギュレーション

表 7-3 に示されているプロセス（MRF を使用して設定可能な Security Manager プロセス）は、ヒープ サイズに対してデフォルト値が事前に設定されています。表 7-3 には、MRF を使用して設定可能な Security Manager プロセスごとに、サーバで使用可能なさまざまな RAM 容量に応じたデフォルトの最小および最大ヒープ サイズが MB 単位で示されています。

表 7-3　Security Manager プロセスに対して事前に設定されるデフォルトのヒープ サイズ

サーバ上の物理 RAM（GB）	VmsBackendServer	Tomcat	CsmReportServer	VmsEventServer	CsmHPMServer
< 8	1024、2048	512、1024	512、1024	1024、2048	512、1024
8	1024、3072	1024、2048	1024、1024	1024、3072	512、1024
12	2048、4096	2048、3072	1024、1024	2048、4096	512、1024
16	2048、4096	2048、4096	1024、1024	4096、4096	512、1024
24	4096、8192	4096、4096	1024、1024	4096、8192	512、1024
>= 28	8192、8192	4096、4096	1024、1024	4096、8192	512、1024

レポート サーバ（CsmReportServer）に対する最大ヒープ サイズは、必要に応じて 1408 MB まで増やすことができます。

一定量の RAM がオペレーティング システム用とその他のプロセス用に予約されていますが、この表には示されていません。たとえば、表 7-3 の RAM が 16 GB の場合について考えてみます。4 つすべてのプロセスに対する最大ヒープ サイズの合計は、(4096 + 4096 + 1024 + 4096) = 13312 MB、つまり 13 GB です。残りの 3 GB の RAM がオペレーティング システム用とその他のプロセス用に使用できます。

コンフィギュレーション コマンド

MRF では、1 つのコマンドと一連のサブコマンドが提供され、Security Manager サーバ プロセスのヒープ サイズの読み取りや変更に使用されます。各プロセスの最小および最大ヒープ サイズは、mrf コマンドを使用して設定できます。次のようにこのコマンドを実行すると、このコマンドの使用方法に関する情報が表示されます。

```
> mrf
mrf help
           Prints this message.
mrf backup
           Backup existing configuration
mrf revert
           Restores backed up configuration
mrf set_heap_params process X-Y [min],[max]
           Sets minimum and maximum heap sizes
           process -> process name
           X-Y -> Memory Range in MB to which heap sizes apply
           [min],[max] -> minimum and maximum heap sizes in MB. These are optional but
atleast one should be specified.
mrf get_heap_params process [memory]
           Prints minimum and maximum heap sizes in MB
           process -> process name
           [memory] -> memory size in MB for which heap sizes are to be printed. If not
specified heap sizes are to be printed for current system memory.
```

mrf コマンドを実行する際は、有効なプロセス名のみを使用してください。無効なプロセス名を指定しても、エラーは発生しません。有効なプロセス名は、表 7-2 に示されています。プロセス名は大文字と小文字が区別されます。

プロセスに対するヒープ サイズの設定

Security Manager プロセスに対するヒープ サイズの設定は、次の主要な 3 つの手順で構成されます。

1. 既存の設定の保存
2. 既存の設定の読み取り
3. 設定の変更

1. 既存の設定の保存

プロセスのヒープ サイズの設定は、Security Manager のパフォーマンスに影響する可能性のある重要な手順であるため、アプリケーションの専門家の指示の下でのみ実施することを推奨します。

また、予防措置として、プロセスの既存のメモリ設定を変更する前に、それらを保存しておくことも推奨します。MRF では、2 種類の保存方法が用意されています。

1. 1 つ目の方法は、設定変更をテストする場合に使用できます。この場合、次に示す 2 つのコマンドを使用して、それぞれ、古い設定を保存すること、および新しい変更を古い設定に戻すことができます。

```
mrf backup
mrf revert
```

2. 2 つ目の方法は、新しい設定をしばらく使用した後に、古い値に戻す場合に役立ちます。これには 2 つの方法があり、次のうちのいずれか一方を使用できます。

a. 設定変更を行った後に mrf backup を実行していなければ、mrf revert を実行できます。

b. Cisco Security Manager サーバのバックアップを取ってから、設定変更を行います。変更を元に戻すときは、バックアップを復元します。この場合、バックアップ後に行われたデータの変更は失われます。

2. 既存の設定の読み取り

データの保存が完了しましたので、次のコマンドを使用して、プロセスの既存の値を問い合わせることができます。

mrf get_heap_params *[process name] [memory]*

このコマンドで memory 値を指定しなければ、現在の RAM サイズが使用されます。一般に関心があるのは、現在の RAM サイズに対する情報です。パラメータ *[process name]* は、表 7-2 に示されている値のいずれかになります。プロセス名は大文字と小文字が区別されます。

このコマンドの出力は、次のように表示されます。値の単位は MB です。

```
Minimum Heap Size = 1024
Maximum Heap Size = 2048
```

3. 設定の変更

現在の設定を確認した後、この項に記載された説明に従って設定を変更することができます。

ヒープ サイズを設定するには、次のコマンドを使用します。

mrf set_heap_params *[process name] [X-Y] [min],[max]*

パラメータ *[process name]* は、表 7-2 に示されているプロセスのいずれかにすることができます。プロセス名は大文字と小文字が区別されます。

このコマンドを実行した後、Security Manager サーバを再起動して変更を反映させる必要があります。

（注）　**mrf set_heap_params** を使用して行われた変更は、ヒープ パラメータの変更前に取られたバックアップが復元されると、失われる可能性があります。この場合、新しい値を保持する必要があるときは、次の手順を実行できます。

1. mrf backup を実行します。
2. アプリケーションの復元を行います。
3. mrf revert を実行します。

このコマンドでは、次の構文が使用されます。

mrf set_heap_params *[process name] [X-Y] [min],[max]*

最小および最大ヒープ サイズを設定します。

[X-Y]：ヒープ サイズを適用するメモリ範囲（単位は MB）

[min],[max]：最小および最大ヒープ サイズ（単位は MB）。これらはオプションですが、少なくとも 1 つは指定する必要があります。

パラメータ *[process name]* は、表 7-2 に示されている値のいずれかになります。プロセス名は大文字と小文字が区別されます。

設定変更の例

次に、ヒープ サイズの設定変更の例を示します。

- mrf set_heap_params Tomcat 7372-8192 2048,4096

  RAM サイズが 7372 ～ 8192 MB の範囲内のときの Tomcat プロセスに対して最小および最大ヒープ サイズをそれぞれ 2048 MB と 4096 MB に設定します。

- mrf set_heap_params Tomcat 7372-8192 2048

  RAM サイズが 7372 ～ 8192 MB の範囲内のときの Tomcat プロセスに対して最小ヒープ サイズを 2048 MB に設定します。

- mrf set_heap_params Tomcat 7372-8192,4096

  RAM サイズが 7372 ～ 8192 MB の範囲内のときの Tomcat プロセスに対して最大ヒープ サイズを 4096 MB に設定します。

- mrf set_heap_params Tomcat 8080-8080 2048,4096

  RAM サイズが 8080 MB ときの Tomcat プロセスに対して最小および最大ヒープ サイズをそれぞれ 2048 MB と 4096 MB に設定します。**getramsize** コマンドを実行すると、既存の RAM サイズを MB 単位で取得できます。

設定変更の確認

ヒープ パラメータを設定した後、**mrf get_heap_params** コマンドを実行して変更を確認できます。

プロセスに対するヒープ サイズの設定の要約

ここで説明した、Security Manager プロセスに対するヒープ サイズの設定のための 3 つの主要手順は、次のように要約されます。これらのコマンドは、実行順で示されています。

```
mrf backup
mrf get_heap_params process
mrf set_heap_params Tomcat 7372-8192 2048,4096
mrf revert #if required to revert changes
```

ユーザがヒープ サイズの再設定を必要とする一般的なシナリオ

シナリオ 1

ある Security Manager 4.0 ユーザが、バックエンド プロセス（VmsBackendServer）に対して 4 GB の最大ヒープ サイズを使用しています。これは、8 GB RAM に対して Security Manager 4.1 で割り当てられるデフォルトの最大ヒープ サイズである 3 GB を超えています。このシナリオのユーザは、バックエンド プロセスのヒープ サイズを 4 GB に再設定する必要があります。イベント管理（Event Server プロセス（VmsEventServer）を使用）がイネーブルになっていなければ、そうすることができます。

シナリオ 2

Security Manager が設定専用モードで使用されています（イベント管理とレポートがディセーブルになっている）。このシナリオでは、バックエンド プロセスと Tomcat のヒープ サイズを増やすことができます。

シナリオ 3

Security Manager が設定専用モードで使用されており（イベント管理とレポートがディセーブルになっている）、イベント管理をイネーブルにする必要があります。このシナリオでは、すべての Security Manager プロセスのヒープ サイズの合計がサーバで使用可能な RAM サイズを超えないように、バックエンド プロセスと Tomcat のヒープ サイズを減らしてから、イベント管理をイネーブルにする必要があります。

シナリオ 4

イベント管理とバックエンド プロセスは、メモリを大量に消費するため、より多くの RAM 割り当てを必要とします。（イベント管理が使用されない場合は、その分の RAM がバックエンド プロセスに割り当てられるように、バックエンド プロセスの最大ヒープ サイズを増やすことができます）。

現行のサーバ セキュリティに関するベスト プラクティス

システムの最小限のセキュア コンポーネントによってシステムの安全性が定義されます。下のチェックリスト内のステップは、Security Manager のインストール後のサーバとその OS のセキュリティ保護に役立ちます。

✓	タスク
❑	**1. サーバ セキュリティを定期的にモニタします。**システム アクティビティを記録して確認します。Microsoft Security Configuration Tool Set（MSCTS）や Fport などのセキュリティ ツールを使用して、サーバのセキュリティ設定を定期的に確認します。Security Manager サーバ上にインストールされたスタンドアロン バージョンの Cisco Security Agent に関するログ ファイルを確認します。 **ヒント** MSCTS は Microsoft の Web サイトから、Fport は Foundstone/McAfee の Web サイトから入手できます。
❑	**2. サーバへの物理アクセスを制限します。**サーバに取り外し可能なメディア ドライブが接続されている場合は、ハード ドライブから起動するようにサーバを設定します。誰かが取り外し可能なメディア ドライブからサーバを起動した場合に、データが侵害されるおそれがあります。通常は、システム BIOS 内で起動順序を設定できます。BIOS が強力なパスワードで保護されていることを確認します。
❑	**3. リモート アクセス ツールやリモート管理ツールをサーバ上にインストールしないでください。**このようなツールは、サーバへのエントリ ポイントを提供するセキュリティ リスクになります。
❑	**4. サーバ上で自動的かつ継続的に動作するようにウイルス スキャン アプリケーションを設定します。**ウイルス スキャン アプリケーションは、トロイの木馬アプリケーションのサーバへの侵入を阻止できます。ウイルス署名を定期的に更新します。
❑	**5. サーバ データベースを頻繁にバックアップします。**すべてのバックアップをアクセスが制限されたセキュアな場所に保管します。

インストールまたはアップグレードの確認

Common Services を使用して、Security Manager のインストールまたはアップグレードが成功したかどうかを確認できます。Security Manager インターフェイスが表示されない、または、正しく表示されないことが原因でインストールを確認する場合は、「インストール後のサーバ障害」（P.A-5）を参照してください。

ステップ 1　クライアント システム上のブラウザを使用して、次のいずれかを使用している Security Manager サーバにログインします。

- HTTP サービスの場合：**http://**<*server_name*>**:1741**
- SSL サービスの場合：**https://**<*server_name*>**:443**

サポートされているブラウザとブラウザのバージョンを確認するには、「クライアントの要件」（P.3-10）を参照してください。

ステップ 2　[Cisco Security Management Suite] ページで、[Server Administration] パネルをクリックして、Common Services の [Server] > [Admin] ページを開きます。

ステップ 3　[Process Management] ページを表示するには、[Processes] をクリックします。

結果のリストには、すべてのサーバ プロセスの名前とプロセスごとの動作ステータスの説明が表示されます。次のプロセスが正常に動作している必要があります。

- vmsDbEngine
- vmsDbMonitor
- EDS

関連情報

項目	対応
基本の理解	Security Manager を起動すると表示される対話形式の *JumpStart* ガイドを参照してください。
製品の迅速な稼働	オンライン ヘルプの「Getting Started with Security Manager」トピックを参照するか、『*User Guide for Cisco Security Manager*』の第 1 章を参照してください。
製品設定の実施	オンライン ヘルプの「Completing the Initial Security Manager Configuration」トピックを参照するか、『*User Guide for Cisco Security Manager*』の第 1 章を参照してください。
ユーザの認証と認可の管理	次の項を参照してください。 • 「ユーザの権限」（P.8-3） • 「Security Manager と Cisco Secure ACS の統合」（P.8-12）
デバイスのブート	オンライン ヘルプの「Preparing Devices for Management」トピックを参照するか、http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html から入手可能な『*User Guide for Cisco Security Manager 4.4*』の第 2 章を参照してください。

CHAPTER 8

ユーザ アカウントの管理

ユーザ アカウントの管理には、アカウントの作成とユーザの権限が含まれます。

- 「アカウントの作成」（P.8-1）アカウントには、Security Manager Server のローカル アカウント、CiscoWorks Common Services サーバの ACS アカウント、または Common Services サーバの非 ACS アカウントがあります。
- 「ユーザの権限」（P.8-3）権限（または特権）は、実行を許可されるタスクです。権限は、Security Manager 内のユーザ ロールによって定義されます。Security Manager 内のロールは、ユーザ名とパスワードの認証後に設定されます。認証は、ログイン中に Security Manager によって行われます。

アカウントの作成

Cisco Security Manager を使用するには、インストール中に作成した **admin** アカウントを使用してログインして、各ユーザのアカウントを作成する必要があります。次のタイプのアカウントを作成できます。

- 「ローカル アカウント」（P.8-1）
- 「ACS アカウント」（P.8-2）
- 「非 ACS アカウント」（P.8-2）

ローカル アカウント

ローカル アカウントは、CiscoWorks Common Services サーバではなく、Security Manager サーバで定義されます。これは Security Manager サーバに固有です。次のパスに従います。

Security Manager がインストールされているサーバ >

Configuration Manager アプリケーションのデスクトップ アイコン >

admin アカウント ログイン >

[Tools] >

[Security Manager Administration] >

[Server Security] >

[Local User Setup] >

[Add]

ヒント　ローカル アカウントは、CiscoWorks ローカル ログイン モジュールを使用します。ただし、CiscoWorks インターフェイスではなく、Security Manager ユーザ インターフェイスを使用して操作します。

ACS アカウント

ACS アカウントは、Security Manager サーバではなく、CiscoWorks Common Services サーバで定義されます。（最初は明らかではないこともありますが、Security Manager には、Common Services 内の Server Security Tools を相互起動するためのボタンがあります）。次のパスに従います。

Security Manager がインストールされているサーバ >

Configuration Manager アプリケーションのデスクトップ アイコン >

ユーザ アカウント ログイン >

[Tools] >

[Security Manager Administration] >

[Server Security] >

[AAA Setup]（このボタンは Common Services 内の Server Security Tools を相互起動します）>

[ACS]

ヒント　ACS アカウントは、（1）ACS タイプの AAA Mode Setup（これは [Authentication Mode Setup] ページにあります）、および（2）CiscoWorks Common Services の ACS ログイン モジュールを使用します。ただし、ACS ログイン モジュールを選択する必要はありません。これは、ACS タイプの [AAA Mode Setup] を選択すると自動的に選択されます。

非 ACS アカウント

非 ACS アカウントは、Security Manager サーバではなく、CiscoWorks Common Services サーバで定義されます。次のパスに従います。

Security Manager がインストールされているサーバ >

Configuration Manager アプリケーションのデスクトップ アイコン >

ユーザ アカウント ログイン >

[Tools] >

[Security Manager Administration] >

[Server Security] >

[AAA Setup] >

[Local RBAC] >

ヒント　非 ACS アカウントは、(1) Local RBAC タイプの AAA Mode Setup（これは [Authentication Mode Setup] ページにあります）、および (2) CiscoWorks Common Services の次のログイン モジュールのいずれかを使用します。CiscoWorks Local（デフォルトのログイン モジュール）、IBM SecureWay Directory、KerberosLogin、Local NT System、MS Active Directory、Netscape Directory、RADIUS、または TACACS+。

ユーザの権限

Cisco Security Manager が、ログイン前にユーザ名とパスワードを認証します。これらが認証されると、Security Manager がアプリケーション内のユーザ ロールを設定します。このロールによって、実行が認可されるタスクまたは操作のセットである権限（特権とも呼ばれる）が定義されます。特定のタスクまたはデバイスに対して認可されなかった場合は、関連するメニュー項目、目次内の項目、およびボタンが非表示またはディセーブルになります。加えて、選択した情報を表示したり、選択した操作を実行したりするための権限がないことを伝えるメッセージが表示されます。

Security Manager の認証と認可は、CiscoWorks サーバと Cisco Secure Access Control Server（ACS）のどちらかによって管理されます。デフォルトで、CiscoWorks は、認証と認可を管理しますが、CiscoWorks Common Services の [AAA Mode Setup] ページを使用して Cisco Secure ACS を変更できます。ACS 統合の詳細については、この章の次の項を参照してください。

- 「Security Manager と Cisco Secure ACS の統合」（P.8-12）
- 「Security Manager と ACS の相互作用のトラブルシューティング」（P.8-29）

Security Manager 4.3、4.4 および 4.5 以前は、Cisco Secure ACS を使用する重要なメリットは、(1) 特殊な権限セット（特定のポリシー タイプの設定だけをユーザに許可する場合など）を使用して非常に粒度の高いユーザ ロールを作成できることと、(2) ネットワーク デバイス グループ（NDG）を設定することによって特定のデバイスにユーザを制限できることでした。このような粒度の高い特権（効率的な「ロールベース アクセス コントロール」（RBAC））は、Cisco Secure ACS を使用していない限り、Security Manager 4.2 以前のバージョンでは利用できませんでした。このような粒度の高い特権（RBAC）は、ACS を使用せずにローカル RBAC を利用できる Common Services 4.0、4.0 および 4.2.2 をそれぞれ使用するため、Security Manager 4.3、4.4 および 4.5 で利用できます。

Security Manager 4.3、4.4 および 4.5 は ACS 4.2 との互換性を維持します。「Security Manager と Cisco Secure ACS の統合」（P.8-12）を参照してください。

（注）　RBAC 機能を ACS から Common Services に移行したいユーザは、手動で行う必要があります。移行スクリプトも、他の移行サポートもありません。

ヒント　Security Manager 権限ツリーの全体を表示するには、Cisco Secure ACS にログインしてから、ナビゲーション バーの [Shared Profile Components] をクリックします。詳細については、「Cisco Secure ACS ロールのカスタマイズ」（P.8-11）を参照してください。

次のトピックで、ユーザ権限について説明します。

- 「Security Manager ACS 権限」（P.8-4）
- 「CiscoWorks ロールについて」（P.8-6）
- 「Cisco Secure ACS ロールについて」（P.8-9）
- 「Security Manager 内の権限とロールのデフォルトの関連付け」（P.8-11）

Security Manager ACS 権限

Cisco Security Manager はデフォルトの ACS ロールと権限を提供します。デフォルト ロールをカスタマイズすることも、ニーズに合わせて追加のロールを作成することもできます。ただし、新しいロールを定義する場合、または、デフォルト ロールをカスタマイズする場合は、選択した権限が Security Manager アプリケーションの観点から適切であることを確認してください。たとえば、表示権限を伴わない変更権限を付与した場合、そのユーザはアプリケーションを使用できなくなります。

Security Manager 権限は次のカテゴリに分類されます。個々の権限に関する説明については、Cisco Secure ACS に統合されているオンライン ヘルプを参照してください（権限の表示方法については、「Cisco Secure ACS ロールのカスタマイズ」（P.8-11）を参照してください）。

- [View]：現在の設定の表示を可能にします。主な表示権限を次に示します。
  - [View] > [Policies]：さまざまなタイプのポリシーの表示を可能にします。このフォルダには、ファイアウォールや NAT などのさまざまなポリシー クラスの権限が含まれています。
  - [View] > [Objects]：さまざまなタイプのポリシー オブジェクトの表示を可能にします。このフォルダには、ポリシー オブジェクト タイプごとの権限が含まれています。
  - [View] > [Admin]：Security Manager 管理設定の表示を可能にします。
  - [View] > [CLI]：デバイス上で設定された CLI コマンドの表示と、展開しようとしているコマンドのプレビューを可能にします。
  - [View] > [Config Archive]: 設定アーカイブに保存されている設定の一覧表示を可能にします。デバイス設定や CLI コマンドは表示できません。
  - [View] > [Devices]：[Device] ビュー内のデバイスと関連情報（デバイス設定、プロパティ、割り当てなど）の表示を可能にします。NDG を設定することによって、デバイス権限を特定のデバイスのセットに制限できます。
  - [View] > [Device Managers]：Cisco IOS ルータ用の Cisco Router and Security Device Manager（SDM）など、あるデバイス専用のデバイス マネージャ（読み取り専用バージョン）の起動を可能にします。
  - [View] > [Topology]：[Map] ビューで設定されたマップの表示を可能にします。
  - [View] > [Event Viewer]: Real Time Viewer と Historical Viewer の両方で Event Viewer のイベントの表示を可能にします。
  - [View] > [Report Manager]：Report Manager のレポートの表示を可能にします。
  - [View] > [Schedule Reports]：Report Manager のレポートのスケジューリングを可能にします。
- [Modify]：現在の設定の変更を可能にします。
  - [Modify] > [Policies]：さまざまなタイプのポリシーの変更を可能にします。このフォルダには、さまざまなポリシー クラスの権限が含まれています。
  - [Modify] > [Objects]：さまざまなタイプのポリシー オブジェクトの変更を可能にします。このフォルダには、ポリシー オブジェクト タイプごとの権限が含まれています。
  - [Modify] > [Admin]：Security Manager 管理設定の変更を可能にします。
  - [Modify] > [Config Archive]：設定アーカイブ内のデバイス設定の変更を可能にします。加えて、アーカイブへの設定の追加と設定アーカイブ ツールのカスタマイズを可能にします。
  - [Modify] > [Devices]：デバイスの追加と削除だけでなく、デバイスのプロパティと属性の変更を可能にします。追加するデバイスに関するポリシーを検出するには、[Import] 権限もイネーブルにする必要があります。加えて、[Modify] > [Devices] 権限をイネーブルにした場合は、[Assign] > [Policies] > [Interfaces] 権限もイネーブルになっていることを確認してください。NDG を設定することによって、デバイス権限を特定のデバイスのセットに制限できます。

  - [Modify] > [Hierarchy]：デバイス グループの変更を可能にします。
  - [Modify] > [Topology]：[Map] ビュー内のマップの変更を可能にします。
  - [Modify] > [Manage Event Monitoring]：任意のデバイスに対して Security Manager のモニタリングをイネーブルおよびディセーブルにすることを可能にします。それにより、Security Manager は、デバイスからのイベントの受信および処理を開始または停止します。
- [Assign]：デバイスと VPN へのさまざまなポリシー タイプの割り当てを可能にします。このフォルダには、さまざまなポリシー クラスの権限が含まれています。
- [Approve]：ポリシー変更と展開ジョブの承認を可能にします。
- [Control]：ping などのデバイスに対するコマンドの発行を可能にします。この権限は、接続診断に使用されます。
- [Deploy]：ネットワーク内のデバイスに対する設定変更の展開と、以前の展開設定に戻すためのロールバックの実施を可能にします。
- [Import]：すでにデバイス上に展開された設定の Security Manager へのインポートを可能にします。デバイスの表示特権とデバイスの変更特権も持っている必要があります。
- [Submit]：設定変更の送信と承認を可能にします。

ヒント

- 変更、割り当て、承認、インポート、制御、または展開権限を選択した場合は、対応する表示権限も選択する必要があります。そうしなかった場合は、Security Manager が正しく機能しません。
- ポリシーの変更権限を選択した場合は、対応するポリシーの割り当て権限と表示権限も選択する必要があります。
- その定義の一部としてポリシー オブジェクトを使用するポリシーを許可した場合は、これらのオブジェクト タイプに表示権限も付与する必要があります。たとえば、ルーティング ポリシーを変更するための権限を選択した場合は、ルーティング ポリシーに必要なオブジェクト タイプのネットワーク オブジェクトとインターフェイス ロールを表示するための権限も選択する必要があります。
- その定義の一部として他のオブジェクトを使用するオブジェクトを許可する場合も同様です。たとえば、ユーザ グループを変更するための権限を選択した場合は、ネットワーク オブジェクト、ACL オブジェクト、および AAA サーバ グループを表示するための権限も選択する必要があります。
- NDG を設定することによって、デバイス権限を特定のデバイスのセットに制限できます。NDG はポリシー権限に対して次のような影響を与えます。
  - ポリシーを表示するには、そのポリシーが割り当てられた少なくとも 1 つのデバイスに対する権限を持っている必要があります。
  - ポリシーを変更するには、そのポリシーが割り当てられたすべてのデバイスに対する権限を持っている必要があります。
  - VPN ポリシーを表示、変更、または割り当てるには、VPN トポロジ内のすべてのデバイスに対する権限を持っている必要があります。
  - デバイスにポリシーを割り当てるには、ポリシーが割り当てられた他のデバイスに対する権限を持っているかどうかに関係なく、そのデバイスの権限のみが必要です （上述したように、VPN ポリシーは例外です）。ただし、権限を持っていないデバイスに割り当てられているポリシーを変更することはできません。

CiscoWorks ロールについて

CiscoWorks Common Services 内で作成されたユーザには、1 つ以上のロールが割り当てられます。各ロールに割り当てられた権限によって、各ユーザが Security Manager 内で実行を認可される操作が決定されます。

次のトピックで、CiscoWorks ロールについて説明します。

- 「CiscoWorks Common Services デフォルト ロール」（P.8-6）
- 「認可タイプの選択および Common Services 内のユーザへのロールの割り当て」（P.8-7）

CiscoWorks Common Services デフォルト ロール

CiscoWorks Common Services には、Security Manager 用の次のデフォルト ロールが用意されています。

- **Help Desk**：Help Desk ユーザは、デバイス、ポリシー、オブジェクト、およびトポロジ マップを表示できます（ただし、変更はできません）。
- **Approver**：変更および CLI 変更の修正を承認できます。
- **Network Operator**：表示権限に加えて、Network Operator は、CLI コマンドと Security Manager 管理設定を表示できます。Network Operator は、設定アーカイブを変更したり、デバイスにコマンド（ping など）を発行したりすることもできます。
- **Network Administrator**：変更のみ展開できます。

（注） Cisco Secure ACS は、さまざまな権限セットを含む Network Administrator という名前のデフォルト ロールを特徴とします。詳細については、「Cisco Secure ACS ロールについて」（P.8-9）を参照してください。

- **System Administrator**：System Administrator は、変更、ポリシー割り当て、アクティビティとジョブの承認、検出、展開、およびデバイスに対するコマンドの発行を含む、すべての Security Manager 権限にアクセスできます。

ヒント Security Manager では、System Administrator ロールは最高レベルの権限を持っています。

- **Super Admin**：管理および承認タスクを含む、CiscoWorks のすべての操作を実行できます。デフォルトでは、このロールは完全な特権を持っています。

ヒント Security Manager では、Super Admin ロールは最高レベルの権限を持っていません。また、Super Admin ロールは ACS ではなく、Common Services に固有のものです。

- **Security Administrator**：変更の修正、割り当て、および送信のみできます。
- **Security Approver**：変更の修正のみ承認できます。

Image Manager

各デフォルト ロールの追加タスクは、Security Manager 4.3 に最初に表示される機能である Image Manager 用に定義されています。Security Manager 4.4 でもこれを引き続き使用できます。

- Image Manager の起動

- Security Manager のリポジトリへのイメージの追加
- イメージ アップグレード ジョブの作成

ローカル アカウント（Security Manager サーバに定義されている Security Manager に固有）を使用する場合、これらの追加タスクが表 8-1 に示されているさまざまなロールに割り当てられます。

表 8-1　デフォルト ロールの Image Manager タスク

ロール	タスク		
	起動と表示	リポジトリへのイメージの追加	イメージ アップグレード ジョブの作成
Help Desk	Yes	No	No
Approver	Yes	No	No
Network Operator	Yes	No	No
Network Administrator	Yes	Yes	Yes
System Administrator	Yes	Yes	Yes
Security Administrator	Yes	No	No

Security Manager 権限と CiscoWorks ロールの関連付けについては、「Security Manager 内の権限とロールのデフォルトの関連付け」（P.8-11）を参照してください。

Image Manager の RBAC 権限マトリクスを示す一連の表の詳細については、付録 B「Image Manager の権限マトリクス」を参照してください。

ヒント

- 追加のアプリケーションがサーバ上にインストールされた場合に、追加のロール（データのエクスポートなど）が Common Services に表示される場合があります。データのエクスポート ロールは、サードパーティ開発者用であり、Security Manager では使用されません。
- CiscoWorks ロールの定義は変更できませんが、各ユーザに割り当てるロールを定義できます。詳細については、「認可タイプの選択および Common Services 内のユーザへのロールの割り当て」（P.8-7）を参照してください。
- CiscoWorks で権限テーブルを生成するには、[Server] > [Reports] > [Permission] を選択して、[Generate Report] をクリックします。

認可タイプの選択および Common Services 内のユーザへのロールの割り当て

CiscoWorks Common Services 4.2.2 では、[Local User Setup] > [Add] ページを使用して、(1) ローカル ユーザに選択可能な 3 つの認可タイプのいずれかを選択し、(2) ロールをユーザに割り当てます。3 つの認可タイプは次のとおりです。

- Full Authorization
- Enable Task Authorization
- Enable Device Authorization

Common Services にローカル ユーザを追加する場合、この 3 つの認可タイプ（Full Authorization、Enable Task Authorization、または Enable Device Authorization）のいずれかを選択する必要があります。

3 つの認可タイプのいずれかを選択することで、ローカル ユーザに必要なロールを選択できます。ローカル ユーザに必要なロールを選択することは、ユーザが実行を許可される操作を定義することになるので重要です。

たとえば、Help Desk ロールを選択した場合、ユーザは表示操作に制限され、データを変更できません。また、Network Operator ロールを割り当てた場合、ユーザは設定アーカイブを変更することもできます。特定のユーザに複数のロールを割り当てることができます。

デフォルトでは、Help Desk ロールがイネーブルになっています。デフォルト ロールをクリアして、任意のロールをデフォルト ロールに設定することもできます。

ヒント　ユーザ権限を変更したら、Security Manager クライアントを再起動する必要があります。

関連トピック

- 「Security Manager ACS 権限」（P.8-4）
- 「Security Manager 内の権限とロールのデフォルトの関連付け」（P.8-11）
- 「CiscoWorks ロールについて」（P.8-6）

ステップ 1　次のパスに従い、Common Services の [Local User Setup] ページに移動します。

Security Manager がインストールされているサーバ >

Cisco Security Manager アプリケーションのデスクトップ アイコン >

admin アカウント ログイン（または十分な権限があるユーザ アカウント）>

[Server Administration] >

[Server] >（メニュー セレクタ記号）>

[Security] >

[Single-Server Management] >

[Local User Setup]

ステップ 2　次のいずれかを実行します。

- ユーザを作成するには、[Add] をクリックして、[Username]、[Password]、[Verify Password]、および [Email] の各フィールドに適切な情報を入力します。
- 既存のユーザの認可を変更するには、ユーザ名の横にあるチェックボックスをオンにして、[Edit] をクリックします。

ステップ 3　ユーザに Security Manager で利用可能なすべてのロール（Help Desk、Approver、Network Operator、Network Administrator、System Administrator、Super Admin、Security Administrator、および Security Approver）を持たせる場合は、[Full Authorization] を選択します。

ヒント　[Full Authorization] を選択する場合、[Enable Task Authorization] は選択できません（オプション ボタン形式のため）。

ヒント　[Full Authorization] を選択する場合、[Enable Device Authorization] は選択できません（オプション ボタン形式のため）。

a.　この手順のステップ 6 に進みます。

ステップ 4　新しいユーザに、選択したロールのみ（たとえば、Network Operator のみ）を持たせる場合は、[Enable Task Authorization] を選択します。

ヒント [Enable Task Authorization] を選択する場合、[Full Authorization] は選択できません（オプション ボタン形式のため）。

ヒント [Enable Task Authorization] を選択する場合、[Enable Device Authorization] は選択できません（オプション ボタン形式のため）。

a. 次のロールを 1 つ以上選択します。Help Desk、Approver、Network Operator、Network Administrator、System Administrator、Super Admin、Security Administrator、および Security Approver。各ロールの詳細については、「CiscoWorks Common Services デフォルト ロール」（P.8-6）を参照してください。

b. この手順のステップ 8 に進みます。

ステップ 5　新しいユーザを、Security Manager インストールに存在するすべてのデバイス グループではなく、選択するデバイス グループに対してのみ認可させる場合は、[Enable Device Authorization] を選択します。(デバイス グループは [Device Groups] ページ（[Security Manager] > [Tools] > [Security Manager Administration] > [Device Groups]）で定義できます)。

ヒント [Enable Device Authorization] を選択する場合、[Full Authorization] は選択できません（オプション ボタン形式のため）。

ヒント [Enable Device Authorization] を選択する場合、[Enable Task Authorization] は選択できません（オプション ボタン形式のため）。ただし、特定のデバイス グループに対して個別のロールを選択できます。

a. 新しいユーザが認可されるデバイス グループを選択します。

b. 次のロールを 1 つ以上選択します。Help Desk、Approver、Network Operator、Network Administrator、System Administrator、Super Admin、Security Administrator、および Security Approver。各ロールの詳細については、「CiscoWorks Common Services デフォルト ロール」（P.8-6）を参照してください。

ステップ 6　[OK] をクリックして変更を保存します。

ステップ 7　Security Manager クライアントを再起動します。

Cisco Secure ACS ロールについて

Common Services 4.0（Security Manager 4.3 と 4.4 で使用）と Common Services 4.2.2（Security Manager 4.5 で使用）以前は、Cisco Secure ACS ではアプリケーション固有のロール（効率的な「ロールベース アクセス コントロール」（RBAC））をサポートしていたため、Common Services よりも柔軟性の高い Security Manager 権限の管理が可能でした。

このような粒度の高い特権（RBAC）は、ACS を使用せずにローカル RBAC を利用できる Common Services 4.0 および 4.2.2 で利用できます。各ロールは、Security Manager タスクに対する認可レベルを決定する権限セットで構成されます。Cisco Secure ACS で、各ユーザ グループに（およびオプションで個別のユーザにも）ロールを割り当てます。これによって、グループ内の各ユーザは、そのロールに対して定義された権限によって認可される操作を実行できます。

加えて、これらのロールを Cisco Secure ACS デバイス グループに割り当てて、デバイスのセットごとに権限を区別できるようにできます。

（注）　Cisco Secure ACS デバイス グループは、Security Manager デバイス グループとは無関係です。

次のトピックで、Cisco Secure ACS ロールについて説明します。

- 「Cisco Secure ACS デフォルト ロール」（P.8-10）
- 「Cisco Secure ACS ロールのカスタマイズ」（P.8-11）

Cisco Secure ACS デフォルト ロール

Cisco Secure ACS には、CiscoWorks と同じロール（「CiscoWorks ロールについて」（P.8-6）を参照）に加えて、次のロールが含まれています。

- **Security Approver**：Security Approver は、デバイス、ポリシー、オブジェクト、マップ、CLI コマンド、および管理設定を表示できます（ただし、変更はできません）。加えて、Security Approver は、アクティビティに含まれる設定変更を承認または拒否できます。
- **Security Administrator**：表示権限が付与されていることに加えて、Security Administrator は、デバイス、デバイス グループ、ポリシー、オブジェクト、およびトポロジ マップを変更できます。彼らは、デバイスと VPN トポロジにポリシーを割り当てたり、システムに新しいデバイスをインポートするための検出を実行したりすることもできます。
- **Network Administrator**：表示権限に加えて、Network Administrator は、設定アーカイブを変更したり、展開を実行したり、デバイスにコマンドを発行したりできます。

（注）　Cisco Secure ACS Network Administrator ロール内に含まれる権限は、CiscoWorks Network Administrator ロール内に含まれる権限と同じではありません。詳細については、「CiscoWorks ロールについて」（P.8-6）を参照してください。

CiscoWorks と違って、Cisco Secure ACS を使用すれば、各 Security Manager ロールに関連付けられた権限をカスタマイズできます。デフォルト ロールの変更方法については、「Cisco Secure ACS ロールのカスタマイズ」（P.8-11）を参照してください。

Security Manager 権限と Cisco Secure ACS ロールの関連付けについては、「Security Manager 内の権限とロールのデフォルトの関連付け」（P.8-11）を参照してください。

関連トピック

- 「Security Manager と Cisco Secure ACS の統合」（P.8-12）
- 「ユーザの権限」（P.8-3）

Cisco Secure ACS ロールのカスタマイズ

Cisco Secure ACS を使用すれば、各 Security Manager ロールに関連付けられた権限を変更できます。特定の Security Manager タスクを対象とする権限が付与された特殊なユーザ ロールを作成することによって、Cisco Secure ACS をカスタマイズすることもできます。

（注） ユーザ権限を変更したら、Security Manager を再起動する必要があります。

関連トピック

- 「Security Manager ACS 権限」（P.8-4）
- 「Security Manager 内の権限とロールのデフォルトの関連付け」（P.8-11）

ステップ 1　Cisco Secure ACS のナビゲーション バーで、[Shared Profile Components] をクリックします。

ステップ 2　[Shared Components] ページで [Cisco Security Manager] をクリックします。Security Manager 用に設定されたロールが表示されます。

ステップ 3　次のいずれかを実行します。

- ロールを作成するには、[Add] をクリックします。ロールの名前を入力して、オプションで、説明を入力します。
- 既存のロールを変更するには、そのロールをクリックします。

ステップ 4　権限ツリー内のチェックボックスをオン/オフして、そのロールに対する権限を定義します。

ツリーのブランチに対応するチェックボックスをオンにすると、そのブランチ内のすべての権限が選択されます。たとえば、[Assign] チェックボックスをオンにすると、すべての割り当て権限が選択されます。

個々の権限に関する説明がウィンドウに表示されます。詳細については、「Security Manager ACS 権限」（P.8-4）を参照してください。

ヒント 変更、承認、割り当て、インポート、制御、または展開権限を選択した場合は、対応する表示権限も選択する必要があります。そうしなかった場合は、Security Manager が正しく機能しません。

ステップ 5　[Submit] をクリックして、変更を保存します。

ステップ 6　Security Manager を再起動します。

Security Manager 内の権限とロールのデフォルトの関連付け

表 8-2 に、Security Manager 権限、CiscoWorks Common Services ロール、および Cisco Secure ACS 内のデフォルト ロールの関連付けを示します。一部のロール（Super Admin、Security Administrator、および Security Approver）は、Cisco Secure ACS のデフォルト ロールと特に関連付けられていないので含まれていません。特定の権限に関する詳細については、「Security Manager ACS 権限」（P.8-4）を参照してください。

表 8-2　Security Manager と CiscoWorks Common Services のロール関連付けに対するデフォルトの権限

権限	ロール						
	System Admin.	Security Admin.	Security Approver	Network Admin.	Approver	Network Operator	Help Desk
表示権限							
デバイスの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ポリシーの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes
オブジェクトの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes
トポロジの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CLI の表示	Yes	Yes	Yes	Yes	Yes	Yes	No
管理設定の表示	Yes	Yes	Yes	Yes	Yes	Yes	No
設定アーカイブの表示	Yes	Yes	Yes	Yes	Yes	Yes	Yes
デバイス マネージャの表示	Yes	Yes	Yes	Yes	Yes	Yes	No
変更権限							
デバイスの変更	Yes	Yes	No	No	No	No	No
階層の変更	Yes	Yes	No	No	No	No	No
ポリシーの変更	Yes	Yes	No	No	No	No	No
イメージの変更	Yes	Yes	No	No	No	No	No
オブジェクトの変更	Yes	Yes	No	No	No	No	No
トポロジの変更	Yes	Yes	No	No	No	No	No
管理設定の変更	Yes	No	No	No	No	No	No
設定アーカイブの変更	Yes	Yes	No	Yes	No	Yes	No
その他の権限							
ポリシーの割り当て	Yes	Yes	No	No	No	No	No
ポリシーの承認	Yes	No	Yes	No	No	No	No
CLI の承認	Yes	No	No	No	Yes	No	No
検出（インポート）	Yes	Yes	No	No	No	No	No
展開	Yes	No	No	Yes	No	No	No
制御	Yes	No	No	Yes	No	Yes	No
送信	Yes	Yes	No	No	No	No	No

Security Manager と Cisco Secure ACS の統合

この項では、Cisco Secure ACS と Cisco Security Manager の統合方法について説明します。

Cisco Secure ACS は、Security Manager などの管理アプリケーションを使用しているユーザに管理対象ネットワーク デバイスを設定するためのコマンド認可を提供します。コマンド認可に対するサポートは、一連の権限が含まれる一意のコマンド認可セット タイプ（Security Manager ではロールと呼ばれている）によって提供されます。これらの権限（特権とも呼ばれる）によって、特定のロールを持つユーザが Security Manager 内で実行できるアクションが決定されます。

Cisco Secure ACS は、TACACS+ を使用して管理アプリケーションと通信します。Security Manager と Cisco Secure ACS が通信するためには､Cisco Secure ACS 内の CiscoWorks サーバを TACACS+ を使用する AAA クライアントとして設定する必要があります。加えて、CiscoWorks サーバに Cisco Secure ACS へのログインに使用する管理者名とパスワードを提供する必要があります。これらの要件を満たすことによって、Security Manager と Cisco Secure ACS 間の通信の有効性が保証されます。

（注）　TACACS+ のセキュリティ メリットを理解するには、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

Security Manager が初めて Cisco Secure ACS と通信するときに、デフォルト ロールの作成を Cisco ACS に指示します。このロールは、Cisco Secure ACS HTML インターフェイスの [Shared Profile Components] セクションに表示されます。また、TACACS+ による認可をカスタム サービスに指示します。このカスタム サービスは、HTML インターフェイスの [Interface Configuration] セクション内の [TACACS+ (Cisco IOS)] ページに表示されます。その後で、各 Security Manager ロールに含まれる権限を変更したり、これらのロールをユーザとユーザ グループに適用したりできます。

次のトピックで、Cisco Secure ACS と Security Manager の使用方法について説明します。

- 「ACS 統合要件」（P.8-13）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.8-14）
- 「Cisco Secure ACS で実行する統合手順」（P.8-15）
- 「CiscoWorks で実行する統合手順」（P.8-21）
- 「Daemon Manager の再起動」（P.8-25）
- 「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.8-26）

ACS 統合要件

Cisco Secure ACS を使用するには、次の手順を完了する必要があります。

- Security Manager 内で必要な機能を実行するために必要な権限を含むロールを定義しました。
- Network Access Restriction（NAR）には、NAR をプロファイルに適用する場合に管理するデバイス グループ（またはデバイス）が含まれています。
- 管理対象デバイス名は、Cisco Secure ACS と Security Manager で綴りと大文字/小文字を合わせる必要があります。この制限は、表示名に適用され、デバイス上で定義されるホスト名には適用されません。ACS の命名制限は Security Manager の命名制限よりも厳密なため、先に、ACS 内でデバイスを定義する必要があります。
- PIX/ASA セキュリティ コンテキスト、FWSM、および IPS デバイスに関して満たさなければならないその他のデバイス表示名要件があります。これらについては、「NDG を使用しないデバイスの AAA クライアントとしての追加」（P.8-17）に記載されています。
- ネットワーク デバイス グループをイネーブルにする必要があります。

ヒント

- ACS 統合の前にデバイスが Security Manager にすでにインポートされている場合は、それらのデバイスを AAA クライアントとして ACS に追加してから統合することを推奨します。AAA クライアントの名前は、CSM 内でのデバイスの表示名と一致する必要があります。一致していないと、それらのデバイスは、ACS 統合後に Security Manager のデバイス リストに表示されなくなります。

- 複数の Cisco Secure ACS サーバを使用するフォールトトレラントなインフラストラクチャの構築を強く推奨します。複数のサーバを使用することによって、いずれかの ACS サーバの通信機能が失われても、Security Manager 内の作業を継続できます。
- Cisco Secure ACS と統合できるのは 1 つのバージョンの Security Manager だけです。そのため、組織で 2 つの異なるバージョンの Security Manager が同時に使用されている場合は、2 つの異なる Cisco Secure ACS サーバとの統合を実施する必要があります。ただし、別の ACS を使用しなくても、新しいバージョンの Security Manager にアップグレードできます。
- Cisco Secure ACS 認証が使用されている場合でも、CiscoWorks Common Services ソフトウェアは Compact Database や Database Checkpoint などの CiscoWorks Common Services 固有のユーティリティのローカル認可を使用します。これらのユーティリティを使用するには、ユーザをローカルに定義して、適切な権限を付与する必要があります。

関連トピック

- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.8-14）
- 「Security Manager と Cisco Secure ACS の統合」（P.8-12）

初期 Cisco Secure ACS セットアップ手順の概要

次の手順では、Cisco Secure ACS と Security Manager を使用して実行する必要のあるすべてのタスクの概要を示します。この手順には、各ステップの実行に使用されるより詳しい手順への参照が含まれています。

関連トピック

- 「ACS 統合要件」（P.8-13）
- 「Security Manager と Cisco Secure ACS の統合」（P.8-12）

ステップ 1　**管理認証および認可モデルを計画します。**

Security Manager を使用する前に、管理モデルを決定する必要があります。これには、使用する予定の管理ロールとアカウントの定義も含まれます。

ヒント　潜在的管理者のロールと権限を定義するときに、イネーブルにするワークフローも考慮する必要があります。この選択は、アクセスの制限方法に影響します。

詳細については、次を参照してください。

- 「Cisco Secure ACS ロールについて」（P.8-9）
- *『User Guide for Cisco Security Manager』*
- *『User Guide for Cisco Secure Access Control Server』*

ステップ 2　**Cisco Secure ACS、Cisco Security Manager、および CiscoWorks Common Services をインストールします。**

Cisco Secure ACS をインストールします。別のサーバ上に CiscoWorks Common Services と Cisco Security Manager をインストールします。Cisco Secure ACS と Security Manager を同じサーバ上で実行しないでください。

詳細については、次を参照してください。

- 『*Release Notes for Cisco Security Manager*』（サポートされている Cisco Secure ACS のバージョンの詳細）

- 「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2）
- *『Installation Guide for Cisco Secure ACS for Windows Server』*

ステップ 3　**Cisco Secure ACS で統合手順を実行します。**

Security Manager ユーザを ACS ユーザとして定義し、それらを計画されたロールに基づいてユーザ グループに割り当て、すべての管理対象デバイス（および CiscoWorks/Security Manager サーバ）を AAA クライアントとして追加し、管理制御ユーザを作成します。

詳細については、「Cisco Secure ACS で実行する統合手順」（P.8-15）を参照してください。

ステップ 4　**CiscoWorks Common Services で統合手順を実行します。**

Cisco Secure ACS で定義されたシステム識別ユーザと一致するローカル ユーザを設定し、同じユーザをシステム識別セットアップ用に定義し、ACS を AAA セットアップ モードとして設定し、SMTP サーバとシステム管理者の電子メール アドレスを設定します。

詳細については、「CiscoWorks で実行する統合手順」（P.8-21）を参照してください。

ステップ 5　**Daemon Manager を再起動します。**

Security Manager サーバの Daemon Manager を再起動して、構成した AAA 設定を有効にします。

詳細については、「Daemon Manager の再起動」（P.8-25）を参照してください。

ステップ 6　**Cisco Secure ACS でユーザ グループにロールを割り当てます。**

Cisco Secure ACS で設定されたユーザ グループごとにロールを割り当てます。使用すべき手順は、Network Device Group（NDG; ネットワーク デバイス グループ）を設定したかどうかによって異なります。

詳細については、「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.8-26）を参照してください。

Cisco Secure ACS で実行する統合手順

次のトピックで、Cisco Security Manager と統合する場合に Cisco Secure ACS で実行すべき手順について説明します。列挙された順にタスクを実行します。これらの項で説明する手順の詳細については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

1. 「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.8-15）
2. 「Cisco Secure ACS での管理対象デバイスの AAA クライアントとしての追加」（P.8-17）
3. 「Cisco Secure ACS での管理制御ユーザの作成」（P.8-21）

Cisco Secure ACS でのユーザとユーザ グループの定義

Security Manager のすべてのユーザを Cisco Secure ACS で定義し、彼らの職務権限に応じたロールを割り当てる必要があります。この最も簡単な方法は、ACS で使用可能なデフォルト ロールに従ってユーザを複数のグループに分ける方法です。たとえば、すべてのシステム管理者をあるグループに割り当て、すべてのネットワーク オペレータを別のグループに割り当てるといった具合です。ACS 内のデフォルト ロールの詳細については、「Cisco Secure ACS デフォルト ロール」（P.8-10）を参照してください。

デバイスに対するフル権限を持つ System Administrator ロールを割り当てる新しいユーザを作成する必要があります。このユーザに対して設定された資格情報が、後で、CiscoWorks の [System Identity Setup] ページで使用されます。「システム識別ユーザの定義」（P.8-22）を参照してください。

この段階で、ユーザを複数のグループに割り当てることはまれであることに注意してください。これらのグループに対する実際のロールの割り当ては、CiscoWorks、Security Manager、およびその他のアプリケーションが Cisco Secure ACS に登録された後で実行されます。

ヒント　この手順では、初期 Cisco Secure ACS 統合中のユーザ アカウントの作成方法について説明します。統合を完了したら、ユーザ アカウントを作成して、適切なグループに割り当てることができます。

関連トピック

- 「ACS 統合要件」（P.8-13）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.8-14）
- 「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.8-26）

ステップ 1　Cisco Secure ACS にログインします。

ステップ 2　次の手順を使用して、フル権限を持つユーザを設定します。ユーザとユーザ グループの設定時に使用可能なオプションの詳細については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

a. ナビゲーション バーの [User Setup] をクリックします。

b. [User Setup] ページで、新しいユーザの名前を入力して [Add/Edit] をクリックします。

ヒント　**admin** という名前のユーザは作成しないでください。admin ユーザは Security Manager のフォールバック ユーザです。ACS システムが何らかの理由で停止した場合は、admin アカウントを使用して Security Manager サーバ上の CiscoWorks Common Services にログインし、AAA モードを CiscoWorks ローカル認証に変更して、製品の使用を続けることができます。

c. [User Setup] の下の [Password Authentication] リストから認証方式を選択します。

d. 新しいユーザのパスワードを入力して確認します。

e. ユーザに割り当てるべきグループとして [Group 1] を選択します。

f. [Submit] をクリックしてユーザ アカウントを作成します。

ステップ 3　Security Manager ユーザごとにこのプロセスを繰り返します。ユーザは割り当てられたロールに基づいてグループに分けることを推奨します。

- グループ 1：System Administrator
- グループ 2：Security Administrator
- グループ 3：Security Approver
- グループ 4：Network Administrator
- グループ 5：Approver
- グループ 6：Network Operator
- グループ 7：Help Desk

各ロールに関連付けられたデフォルト権限の詳細については、「Security Manager 内の権限とロールのデフォルトの関連付け」（P.8-11）を参照してください。ユーザ ロールのカスタマイズ方法については、「Cisco Secure ACS ロールのカスタマイズ」（P.8-11）を参照してください。

（注）　この段階で、グループはどのロールも定義されていないユーザの集合でしかありません。統合プロセスが完了してから、各ユーザにロールを割り当てます。「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.8-26）を参照してください。

ステップ 4　CiscoWorks Common Services でシステム識別ユーザとして使用する新しいユーザを作成します。このユーザをシステム管理者グループに割り当て、デバイスに対するすべての特権を付与します。このユーザに対して設定された資格情報が、後で、CiscoWorks の [System Identity Setup] ページで使用されます。「システム識別ユーザの定義」（P.8-22）を参照してください。

ステップ 5　「Cisco Secure ACS での管理対象デバイスの AAA クライアントとしての追加」（P.8-17）に進みます。

Cisco Secure ACS での管理対象デバイスの AAA クライアントとしての追加

Security Manager にデバイスをインポートするには、Cisco Secure ACS で各デバイスを AAA クライアントとして設定する必要があります。加えて、CiscoWorks/Security Manager サーバを AAA クライアントとして設定する必要があります。

Security Manager が、Catalyst 6500/7600 デバイス用の FWSM を含むファイアウォール デバイス上で設定されたセキュリティ コンテキストを管理している場合は、それぞれのコンテキストを個別に Cisco Secure ACS に追加する必要があります。同様に、IPS デバイス上で定義されたすべての仮想センサーを追加する必要もあります。

管理対象デバイスを追加する方式は、NDG を作成して特定のデバイス セットの管理にユーザを制限するかどうかによって異なります。次のように進めます。

- 特定の NDG へのアクセスだけをユーザに許可する場合は、「Security Manager で使用するネットワーク デバイス グループの設定」（P.8-18）に記載されているようにデバイスを追加します。

（注）　デバイスがネットワーク デバイス グループに分類される必要はありませんが、Security Manager は NDG にある Security Manager ネットワーク デバイスを要求します。「Not Assigned」は NDG ではありません。複数の NDG が必要でない場合は、すべてのデバイスを Not Assigned からデフォルトの NDG に移動することを推奨します。

NDG を使用しないデバイスの AAA クライアントとしての追加

この手順では、デバイスを Cisco Secure ACS の AAA クライアントとして追加する方法について説明します。使用可能なオプションの詳細については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

ヒント　CiscoWorks/Security Manager サーバを AAA クライアントとして追加することを忘れないでください。

関連トピック

- 「ACS 統合要件」（P.8-13）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.8-14）

ステップ 1　Cisco Secure ACS のナビゲーション バーで、[Network Configuration] をクリックします。

ステップ 2　[AAA Clients] テーブルの下で [Add Entry] をクリックします。

ステップ 3　[Add AAA Client] ページで AAA クライアントのホスト名（32 文字以下）を入力します。AAA クライアントのホスト名は、Security Manager 内でデバイスとして使用する予定の表示名と一致させる*必要があります*。

たとえば、Security Manager でドメイン名をデバイス名に付加する場合は、ACS 内の AAA クライアントのホスト名を **<device_name>.<domain_name>** にする必要があります。

CiscoWorks サーバに名前を付ける場合は、完全修飾ホスト名を使用することを推奨します。ホスト名の綴りが正しいことを確認してください （ホスト名は大文字と小文字が区別されません）。

その他の命名規則を次に示します。

- PIX または ASA セキュリティ コンテキスト、あるいは、FWSM 経由で検出された FWSM セキュリティ コンテキスト：**<parent_display_name>_<context_name>**
- FWSM ブレード：**<chassis_name>_FW_<slot_number>**
- シャーシ経由で検出された FWSM セキュリティ コンテキスト：**<chassis_name>_FW_<slot_number>_<context_name>**
- IPS センサー：**<IPSParentName>_<virtualSensorName>**

ステップ 4　[AAA Client IP Address] フィールドにネットワーク デバイスの IP アドレスを入力します。デバイスに IP アドレスが設定されていない場合（仮想センサーや仮想コンテキストなど）は、アドレスの代わりに単語の **dynamic** を入力します。

（注）　マルチホーム デバイス（複数の NIC が実装されたデバイス）を追加している場合は、各 NIC の IP アドレスを入力します。各アドレスの間で Enter を押します。加えて、Security Manager サーバ上の gatekeeper.cfg ファイルを変更する必要があります。

ステップ 5　[Key] フィールドに共有秘密キーを入力します。

ステップ 6　[Authenticate Using] リストから [TACACS+ (Cisco IOS)] を選択します。

ステップ 7　[Submit] をクリックして、変更を保存します。追加したデバイスが [AAA Clients] テーブル内に表示されます。

ステップ 8　このプロセスを繰り返して、新しいデバイスを追加します。

ステップ 9　追加したデバイスを保存するには、[Submit + Restart] をクリックします。

ステップ 10　「Cisco Secure ACS での管理制御ユーザの作成」（P.8-21）に進みます。

Security Manager で使用するネットワーク デバイス グループの設定

Cisco Secure ACS を使用すれば、特定の管理対象デバイスを含む NDG を設定できます。たとえば、地理的地域別の NDG や組織構造と一致する NDG を作成できます。NDG を Security Manager と一緒に使用すれば、管理対象デバイスに応じて、さまざまなレベルの権限をユーザに付与できます。たとえば、NDG を使用することによって、ユーザ A に、ヨーロッパに設置されたデバイスに対するシステム管理者権限とアジアに設置されたデバイスに対するヘルプ デスク権限を割り当てることができます。その後で、正反対の権限をユーザ B に割り当てることができます。

NDG は直接はユーザに割り当てません。その代わりに、ユーザ グループごとに定義したロールに NDG を割り当てます。各 NDG は 1 つのロールにしか割り当てることができませんが、各ロールに複数の NDG を含めることができます。これらの定義は、選択されたユーザ グループの定義の一部として保存されます。

ヒント

- 各デバイスは 1 つの NDG のメンバーにしかなれません。
- NDG は、Security Manager で設定可能なデバイス グループに*関連付けられません*。
- NDG の管理方法については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

次のトピックで、NDG の設定に関する基本的な情報とステップについて説明します。

- 「NDG とユーザ権限」（P.8-19）
- 「NDG 機能のアクティブ化」（P.8-19）
- 「NDG の作成」（P.8-20）
- 「NDG とロールのユーザ グループへの関連付け」（P.8-27）

NDG とユーザ権限

NDG はユーザを特定のデバイス セットに制限するため、次のように、ポリシー権限に影響します。

- ポリシーを表示するには、そのポリシーが割り当てられた少なくとも *1* つのデバイスに対する権限を持っている必要があります。
- ポリシーを変更するには、そのポリシーが割り当てられた*すべて*のデバイスに対する権限を持っている必要があります。
- VPN ポリシーを表示、変更、または割り当てるには、VPN トポロジ内の*すべて*のデバイスに対する権限を持っている必要があります。
- デバイスにポリシーを割り当てるには、ポリシーが割り当てられた他のデバイスに対する権限を持っているかどうかに関係なく、そのデバイスの権限のみが必要です （上述したように、VPN ポリシーは例外です）。ただし、権限を持っていないデバイスに割り当てられているポリシーを変更することはできません。

（注） オブジェクトを変更するには、そのオブジェクトを使用しているすべてのデバイスに対する変更権限を持っている必要は*ありません*。ただし、そのデバイス上で定義されたデバイスレベルのオブジェクトの上書きを変更するには、特定のデバイスに対する変更権限を持っている必要があります。

関連トピック

- 「Security Manager で使用するネットワーク デバイス グループの設定」（P.8-18）
- 「ユーザの権限」（P.8-3）

NDG 機能のアクティブ化

NDG を作成して、デバイスを追加するには、NDG 機能をアクティブにする必要があります。

関連トピック

- 「NDG の作成」（P.8-20）
- 「NDG とロールのユーザ グループへの関連付け」（P.8-27）
- 「NDG とユーザ権限」（P.8-19）
- 「Security Manager で使用するネットワーク デバイス グループの設定」（P.8-18）

ステップ 1　Cisco Secure ACS のナビゲーション バーで、[Interface Configuration] をクリックします。

ステップ 2　[Advanced Options] をクリックします。

ステップ 3　スクロール ダウンしてから、[Network Device Groups] チェックボックスをオンにします。

ステップ 4　[Submit] をクリックします。

ステップ 5　「NDG の作成」（P.8-20）に進みます。

NDG の作成

この手順では、NDG を作成して、デバイスを追加する方法について説明します。各デバイスは 1 つの NDG にしか属することができません。

ヒント　CiscoWorks/Security Manager サーバを含む特別な NDG を作成することを強く推奨します。

はじめる前に

「NDG 機能のアクティブ化」（P.8-19）に記載されているように、NDG 機能をアクティブにします。

関連トピック

- 「NDG とロールのユーザ グループへの関連付け」（P.8-27）
- 「NDG とユーザ権限」（P.8-19）
- 「Security Manager で使用するネットワーク デバイス グループの設定」（P.8-18）

ステップ 1　ナビゲーション バーで、[Network Configuration] をクリックします。

最初は、すべてのデバイスが Not Assigned に配置されます。この場所には、NDG 内に存在しなかったすべてのデバイスが保存されます。Not Assigned は NDG でないことに注意してください。

ステップ 2　NDG を作成します。

a.　[Add Entry] をクリックします。

b.　[New Network Device Group] ページで、NDG の名前を入力します。最大長は 24 文字です。スペースを使用できます。

c.　（任意）NDG 内のすべてのデバイスで使用されるキーを入力します。NDG 用のキーを定義すると、NDG 内の個別のデバイスに対して定義されたすべてのキーが上書きされます。

d.　[Submit] をクリックして NDG を保存します。

e.　このプロセスを繰り返して、新しい NDG を作成します。

ステップ 3　NDG にデバイスを追加します。各デバイスは 1 つの NDG のメンバーにしかなれないことに注意してください。

a.　[Network Device Groups] エリアで、NDG の名前をクリックします。

b.　[AAA Clients] エリアで、[Add Entry] をクリックします。

c.　NDG に追加するデバイスの詳細を定義してから、[Submit] をクリックします。詳細については、「NDG を使用しないデバイスの AAA クライアントとしての追加」（P.8-17）を参照してください。

d.　このプロセスを繰り返して、残りのデバイスを NDG に追加します。Not Assigned カテゴリに残すことを検討すべき唯一のデバイスが、デフォルト AAA サーバです。

e.　最後のデバイスを設定したら、[Submit + Restart] をクリックします。

ステップ 4　「Cisco Secure ACS での管理制御ユーザの作成」（P.8-21）に進みます。

ヒント Cisco Secure ACS と CiscoWorks Common Services の統合プロセスが完了しなければ、ロールを各 NDG に関連付けることができません。「NDG とロールのユーザ グループへの関連付け」（P.8-27）を参照してください。

Cisco Secure ACS での管理制御ユーザの作成

Cisco Secure ACS の [Administration Control] ページを使用して、CiscoWorks Common Services の AAA セットアップ モードの定義に使用される管理者アカウントを定義します。Security Manager は、このアカウントを使用して、ACS サーバにアクセスしてアプリケーションを登録したり、デバイス グループ メンバーシップとグループ セットアップを問い合わせたり、その他の基本的な ACS とのデータのやり取りを行ったりします。詳細については、「CiscoWorks での AAA セットアップ モードの設定」（P.8-23）を参照してください。

関連トピック

- 「ACS 統合要件」（P.8-13）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.8-14）

ステップ 1　Cisco Secure ACS のナビゲーション バーで、[Administration Control] をクリックします。

ステップ 2　[Add Administrator] をクリックします。

ステップ 3　[Add Administrator] ページで、管理者の名前とパスワードを入力します。

ステップ 4　次の管理者特権を選択します。

- Under Users and Group Setup
  - グループ内のユーザに対する読み取りアクセス
  - これらのグループの読み取りアクセス
- Under Shared Profile Components
  - デバイス コマンド セット タイプの作成
- ネットワーク設定

ステップ 5　[Submit] をクリックして管理者を作成します。管理者の設定時に使用可能なオプションの詳細については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

CiscoWorks で実行する統合手順

Cisco Secure ACS での統合タスク（「Cisco Secure ACS で実行する統合手順」（P.8-15）を参照）が完了したら、CiscoWorks Common Services でいくつかのタスクを完了する必要があります。Common Services は、Cisco Security Manager や Auto Update Server などのインストール対象アプリケーションの Cisco Secure ACS への登録を実行します。

次のトピックで、Cisco Security Manager と統合する場合に CiscoWorks Common Services で実行する手順について説明します。

- 「CiscoWorks でのローカル ユーザの作成」（P.8-22）

- 「システム識別ユーザの定義」（P.8-22）
- 「CiscoWorks での AAA セットアップ モードの設定」（P.8-23）
- 「ACS ステータス通知用の SMTP サーバとシステム管理者の電子メール アドレスの設定」（P.8-25）

CiscoWorks でのローカル ユーザの作成

CiscoWorks Common Services の [Local User Setup] ページを使用して、Cisco Secure ACS で作成されたシステム識別ユーザ（「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.8-15）を参照）とまったく同じローカル ユーザ アカウントを作成します。このローカル ユーザ アカウントは、後で、システム識別セットアップに使用されます。詳細については、「システム識別ユーザの定義」（P.8-22）を参照してください。

関連トピック

- 「ACS 統合要件」（P.8-13）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.8-14）

ステップ 1　次のパスに従い、Common Services の [Local User Setup] ページに移動します。

Security Manager がインストールされているサーバ >

Cisco Security Manager アプリケーションのデスクトップ アイコン >

admin アカウント ログイン >

[Server Administration] >

[Server] >（メニュー セレクタ記号）>

[Security] >

[Single-Server Management] >

[Local User Setup]

ステップ 2　[Add] をクリックします。

ステップ 3　Cisco Secure ACS でシステム識別ユーザを作成したときに入力したものと同じ名前とパスワードを入力します。「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.8-15）を参照してください。

ステップ 4　[Roles] の下のチェックボックスをすべてオンにします。

ステップ 5　[OK] をクリックしてユーザを作成します。

システム識別ユーザの定義

CiscoWorks Common Services の [System Identity Setup] ページを使用して、同じサーバ上に配置された同じドメインおよびアプリケーション プロセスに属しているサーバ間通信をイネーブルにする信頼ユーザ（システム識別ユーザと呼ばれる）を作成します。アプリケーションは、システム識別ユーザを使用して、リモート CiscoWorks サーバ上のプロセスを認証します。これは、特に、ユーザのログイン前に、アプリケーションの同期化が必要な場合に役立ちます。

加えて、システム識別ユーザは、プライマリ タスクがすでにログイン ユーザに対して認可されている場合にサブタスクを実行するためによく使用されます。

ここで設定したシステム識別ユーザは、CiscoWorks ではローカル ユーザとして（すべてのロールが割り当てられる）、ACS ではデバイスに対するすべての特権を持つユーザとして定義する必要もあります。必要な特権を持つユーザを選択しなかった場合は、Security Manager で設定されたすべてのデバイスとポリシーを表示できない可能性があります。先に進む前に次の手順を実行したことを確認してください。

- 「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.8-15）
- 「CiscoWorks でのローカル ユーザの作成」（P.8-22）

関連トピック

- 「ACS 統合要件」（P.8-13）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.8-14）

ステップ 1　次のパスに従い、Common Services の [System Identify Setup] ページに移動します。

Security Manager がインストールされているサーバ >

Cisco Security Manager アプリケーションのデスクトップ アイコン >

admin アカウント ログイン >

[Server Administration] >

[Server] >（メニュー セレクタ記号）>

[Security] >

[Multi-Server Trust Management] >

[System Identity Setup]

ステップ 2　Cisco Secure ACS で作成したシステム識別ユーザの名前を入力します。「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.8-15）を参照してください。

ステップ 3　このユーザのパスワードを入力して確認します。

ステップ 4　[Apply] をクリックします。

CiscoWorks での AAA セットアップ モードの設定

CiscoWorks Common Services の [AAA Setup Mode] ページを使用して、Cisco Secure ACS を必要なポートと共有秘密キーを含む AAA サーバとして定義します。加えて、最大 2 台のバックアップ サーバを定義できます。

この手順は、CiscoWorks と Security Manager（およびオプションの Auto Update Server）の Cisco Secure ACS への登録を実行します。

ヒント　CiscoWorks Common Services または Cisco Security Manager をアンインストールした場合は、ここで設定した AAA セットアップが保存されません。加えて、この設定はバックアップして再インストール後に復元できません。そのため、いずれかのアプリケーションの新しいバージョンにアップグレードする場合は、AAA セットアップ モードを再設定して、Security Manager を ACS に再登録する必要があります。差分アップデートの場合は、このプロセスが必要ありません。AUS などの新しいアプリケーションを CiscoWorks 上にインストールする場合は、そのアプリケーションと Cisco Security Manager を再登録する必要があります。ACS への Security Manager の再登録以外に、既存のシステム識別ユーザを設定し、新しく導入された権限を付与する必要があります。そうしないと、RBAC が正常に機能しません。「システム識別ユーザの定義」（P.8-22）を参照してください。

関連トピック

- 「ACS 統合要件」（P.8-13）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.8-14）

ステップ 1　次のパスに従い、Common Services の [AAA Mode Setup] ページに移動します。

Security Manager がインストールされているサーバ >

Cisco Security Manager アプリケーションのデスクトップ アイコン >

admin アカウント ログイン >

[Server Administration] >

[Server] >（メニュー セレクタ記号）>

[Security] >

[AAA Mode Setup]

ステップ 2　[Available Login Modules] の下で [TACACS+] を選択します。

ステップ 3　AAA タイプとして [ACS] を選択します。

ステップ 4　最大 3 つの Cisco Secure ACS サーバの IP アドレスを [Server Details] エリアに入力します。セカンダリ サーバとターシャリ サーバは、プライマリ サーバで障害が発生した場合のバックアップとして機能します。すべてのサーバで同じバージョンの Cisco Secure ACS が実行している必要があります。

（注）　設定されたすべての TACACS+ サーバが応答しなかった場合は、*admin* CiscoWorks ローカル アカウントを使用してログインしてから、AAA モードを Non-ACS/CiscoWorks Local に変更する必要があります。TACACS+ サーバのサービスが回復されたら、AAA モードを ACS に変更する必要があります。

ステップ 5　[Login] エリアで、Cisco Secure ACS の [Administration Control] ページで定義した管理者の名前を入力します。詳細については、「Cisco Secure ACS での管理制御ユーザの作成」（P.8-21）を参照してください。

ステップ 6　この管理者のパスワードを入力して確認します。

ステップ 7　Security Manager サーバを Cisco Secure ACS の AAA クライアントとして追加したときに入力した共有秘密キーを入力して確認します。「NDG を使用しないデバイスの AAA クライアントとしての追加」（P.8-17）を参照してください。

ステップ 8　[Register all installed applications with ACS] チェックボックスをオンにして、Security Manager とその他のインストール済みアプリケーションを Cisco Secure ACS に登録します。

ステップ 9　[Apply] をクリックして設定値を保存します。経過表示バーに登録の進捗が表示されます。登録が完了するとメッセージが表示されます。

ステップ 10　Cisco Security Manager の Daemon Manager サービスを再起動します。「Daemon Manager の再起動」（P.8-25）を参照してください。

ステップ 11　Cisco Secure ACS に再ログインしてロールを各ユーザ グループに割り当てます。「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.8-26）を参照してください。

ACS ステータス通知用の SMTP サーバとシステム管理者の電子メール アドレスの設定

すべての ACS サーバが使用不能になった場合は、Security Manager でタスクを実行できません。ログイン ユーザは、ACS 認可が必要なタスクを実行しようとすると、強制的に（変更を保存する機会を与えられずに）アプリケーションからログアウトされます。

SMTP サーバとシステム管理者を識別するように Common Services を設定した場合は、すべての ACS サーバが使用不能になったときに、Security Manager から管理者に電子メール メッセージが送信されます。このメッセージにより、早急な対応を必要とする問題に対して警告を出すことができます。管理者は、Common Services から非 ACS 関連イベントに関する電子メール メッセージを受け取ることもあります。

ヒント　Security Manager は、展開ジョブの完了、アクティビティの承認、ACL ルールの期限切れなどのイベント タイプに関する電子メール通知を送信できます。ここで設定する SMTP サーバはこれらの通知にも使用されますが、送信者の電子メール アドレスは Security Manager で設定されます。このような電子メール アドレスの設定方法については、このバージョンの製品の『*User Guide for Cisco Security Manager*』か、クライアントのオンライン ヘルプを参照してください。

ステップ 1　次のパスに従い、Common Services の [System Preferences] ページに移動します。

Security Manager がインストールされているサーバ >

Cisco Security Manager アプリケーションのデスクトップ アイコン >

admin アカウント ログイン >

[Server Administration] >

[Server] >（メニュー セレクタ記号）>

[Admin] >

[System Preferences]

ステップ 2　[System Preferences] ページで、Security Manager が使用可能な SMTP サーバのホスト名または IP アドレスを入力します。SMTP サーバは、電子メール メッセージの送信に対してユーザ認証を要求できません。

ステップ 3　CiscoWorks が電子メールの送信に使用可能な電子メール アドレスを入力します。これは、Security Manager の通知の送信に使用される電子メール アドレスと同じにする必要はありません。

ACS サーバが使用不能になると、このアカウントに（およびこのアカウントから）メッセージが送信されます。

ステップ 4　[Apply] をクリックして変更内容を保存します。

Daemon Manager の再起動

この手順では、Security Manager サーバの Daemon Manager の再起動方法について説明します。この操作は、構成した AAA 設定値を有効にするために行う必要があります。そうすれば、Cisco Secure ACS で定義された資格情報を使用して CiscoWorks に再ログインできます。

関連トピック

- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.8-14）
- 「ACS 統合要件」（P.8-13）

ステップ 1　Security Manager サーバがインストールされたマシンにログインします。

ステップ 2　[Start] > [Programs] > [Administrative Tools] > [Services] を選択して [Services] ウィンドウを開きます。

ステップ 3　右ペインに表示されたサービスのリストから、[Cisco Security Manager Daemon Manager] を選択します。

ステップ 4　ツールバーで [Restart Service] ボタンをクリックします。

ステップ 5　「Cisco Secure ACS でのユーザ グループへのロール割り当て」（P.8-26）に進みます。

Cisco Secure ACS でのユーザ グループへのロール割り当て

CiscoWorks、Security Manager、およびその他のインストール済みアプリケーションを Cisco Secure ACS に登録したら、Cisco Secure ACS で設定したユーザ グループのそれぞれにロールを割り当てることができます。これらのロールによって、各グループ内のユーザが Security Manager で実行を許可されるアクションが決定されます。

ユーザ グループにロールを割り当てる手順は、NDG が使用されるかどうかによって異なります。

- 「NDG を使用しないユーザ グループへのロールの割り当て」（P.8-26）
- 「NDG とロールのユーザ グループへの関連付け」（P.8-27）

（注）　CiscoWorks/Security Manager サーバを含む特別な NDG を作成することによって、CSM と ACS の統合はより有効に機能します。

NDG を使用しないユーザ グループへのロールの割り当て

この手順では、NDG が定義されていない場合のユーザ グループへのデフォルト ロールの割り当て方法について説明します。詳細については、「Cisco Secure ACS デフォルト ロール」（P.8-10）を参照してください。

はじめる前に

- デフォルト ロールごとにユーザ グループを作成します。「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.8-15）を参照してください。
- 次のトピックに記載された手順を実行します。
  - 「Cisco Secure ACS で実行する統合手順」（P.8-15）
  - 「CiscoWorks で実行する統合手順」（P.8-21）

関連トピック

- 「CiscoWorks ロールについて」（P.8-6）
- 「Cisco Secure ACS ロールについて」（P.8-9）

ステップ 1　Cisco Secure ACS にログインします。

ステップ 2　ナビゲーション バーの [Group Setup] をクリックします。

ステップ 3　リストからシステム管理者用のユーザ グループを選択（「Cisco Secure ACS でのユーザとユーザ グループの定義」（P.8-15）を参照）してから、[Edit Settings] をクリックします。

ヒント　グループ名を意味のある名前に変更して、正しいグループを特定しやすいようにすることができます。グループを選択して、[Rename Group] をクリックし、名前を変更します。

ステップ 4　このグループに System Administrator ロールを割り当てます。

a.　[TACACS+ Settings] の下の [CiscoWorks] エリアまでスクロール ダウンします。

b.　最初の [Assign] オプションを選択して、CiscoWorks ロールのリストから [System Administrator] を選択します。

c.　[Cisco Security Manager Shared Services] エリアまでスクロール ダウンします。

d.　最初の [Assign] オプションを選択して、Cisco Secure ACS ロールのリストから [System Administrator] を選択します。

e.　[Submit] をクリックして、グループ設定を保存します。

ステップ 5　残りのロールに対してこのプロセスを繰り返して、各ロールを適切なユーザ グループに割り当てます。

Cisco Secure ACS で [Security Approver] ロールまたは [Security Administrator] ロールを選択するときは、最も近い CiscoWorks ロールとして [Network Administrator] を選択することを推奨します。

ACS 内のデフォルト ロールのカスタマイズ方法については、「Cisco Secure ACS ロールのカスタマイズ」（P.8-11）を参照してください。

NDG とロールのユーザ グループへの関連付け

NDG とロールを関連付けて Security Manager で使用する場合は、[Group Setup] ページの次の 2 か所で定義を作成する必要があります。

- [CiscoWorks] エリア
- [Cisco Security Manager] エリア

各エリア内の定義は、できるだけ細部まで一致する必要があります。CiscoWorks Common Services 内に存在しないカスタム ロールまたは ACS ロールを関連付ける場合は、そのロールに割り当てられた権限に基づいて、できるだけ近い定義を作成するようにします。

Security Manager で使用されるユーザ グループごとの関連付けを作成する必要があります。たとえば、西部地域のサポート担当者を含むユーザ グループがある場合は、そのユーザ グループを選択して、西部地域内のデバイスを含む NDG と Help Desk ロールを関連付けることができます。

はじめる前に

NDG 機能をアクティブにして、NDG を作成します。「Security Manager で使用するネットワーク デバイス グループの設定」（P.8-18）を参照してください。

関連トピック

- 「ACS 統合要件」（P.8-13）
- 「初期 Cisco Secure ACS セットアップ手順の概要」（P.8-14）

ステップ 1　ナビゲーション バーの [Group Setup] をクリックします。

ステップ 2　[Group] リストからユーザ グループを選択してから、[Edit Settings] をクリックします。

ヒント　グループ名を意味のある名前に変更して、正しいグループを特定しやすいようにすることができます。グループを選択して、[Rename Group] をクリックし、名前を変更します。

ステップ 3　CiscoWorks 内で使用する NDG とロールをマップします。

a. [Group Setup] ページで、[TACACS+ Settings] の下の [CiscoWorks] エリアまでスクロール ダウンします。

b. [Assign a Ciscoworks on a per Network Device Group Basis] を選択します。

c. [Device Group] リストから NDG を選択します。

d. この NDG を関連付けるべきロールを 2 つめのリストから選択します。

e. [Add Association] をクリックします。関連付けが [Device Group] ボックスに表示されます。

f. このプロセスを繰り返して、新しい関連付けを作成します。

g. 関連付けを削除するには、[Device Group] からそれを選択して、[Remove Association] をクリックします。

ステップ 4　Cisco Security Manager 内で使用する NDG とロールをマップします。以前のステップで定義した関連付けにできるだけ近い関連付けを作成する必要があります。

a. [Group Setup] ページで、[TACACS+ Settings] の下の [Cisco Security Manager] エリアまでスクロール ダウンします。

b. [Assign a Cisco Security Manager on a per Network Device Group Basis] を選択します。

c. [Device Group] リストから NDG を選択します。

d. この NDG を関連付けるべきロールを 2 つめのリストから選択します。

e. [Add Association] をクリックします。関連付けが [Device Group] ボックスに表示されます。

f. このプロセスを繰り返して、新しい関連付けを作成します。

（注）　Cisco Secure ACS で [Security Approver] ロールまたは [Security Administrator] ロールを選択するときは、最も近い CiscoWorks ロールとして [Network Administrator] を選択することを推奨します。

（注）　CiscoWorks Common Services には「Network Administrator」というデフォルトのロールがあります。Cisco Secure ACS には「Network Admin」というデフォルトのロールがあります。これらのロールは同一ではありません。Cisco Security Manager 内での権限のいくつかについて、ロールが異なっています。

ステップ 5　[Submit] をクリックして設定値を保存します。

ステップ 6　このプロセスを繰り返して、残りのユーザ グループ用の NDG を定義します。

ステップ 7　作成した関連付けを保存するには、[Submit + Restart] をクリックします。

ACS 内のデフォルト ロールのカスタマイズ方法については、「Cisco Secure ACS ロールのカスタマイズ」（P.8-11）を参照してください。

Security Manager と ACS の相互作用のトラブルシューティング

次のトピックで、Security Manager と Cisco Secure ACS の相互作用のやり方が原因で発生する可能性のある一般的な問題の解決方法について説明します。

- 「複数のバージョンの Security Manager と 1 つの ACS の使用」（P.8-29）
- 「ACS モードで認証に失敗する」（P.8-29）
- 「読み取り専用アクセスが付与されたシステム管理者」（P.8-30）
- 「ACS の変更が Security Manager に表示されない」（P.8-30）
- 「ACS で設定されたデバイスが Security Manager に表示されない」（P.8-31）
- 「Cisco Secure ACS が到達不能になった後の Security Manager での作業」（P.8-31）
- 「Cisco Secure ACS へのアクセスの復元」（P.8-31）
- 「マルチホーム デバイスに伴う認証の問題」（P.8-32）
- 「NAT 境界の背後に設置されたデバイスに伴う認証の問題」（P.8-32）

複数のバージョンの Security Manager と 1 つの ACS の使用

1 つの Cisco Secure ACS と 2 つの異なるバージョンの Security Manager を一緒には使用できません。たとえば、Security Manager 3.3.1 と Cisco Secure ACS を統合してから、別の部署で既存のインストールをアップグレード*せずに* Security Manager 4.0.1 の使用を計画している場合は、Security Manager 4.0.1 と、Security Manager 3.3.1 用に使用されているものとは別の ACS を統合する必要があります。

既存の Security Manager インストールをアップグレードすれば、同じ Cisco Secure ACS を使用し続けることができます。必要に応じて、権限設定が更新されます。

ACS モードで認証に失敗する

Security Manager または CiscoWorks Common Services にログインしようとして続けて認証が失敗する場合は、Common Services を使用して Cisco Secure ACS を認証用の AAA サーバとして設定していたとしても、次の手順を実行します。

- ACS サーバと、Common Services と Security Manager を実行しているサーバ間の接続が確立されていることを確認します。
- 使用しているユーザ資格情報（ユーザ名とパスワード）が ACS 内で定義されており、適切なユーザ グループに割り当てられていることを確認します。
- ACS の [Network Configuration] ページで、Common Services サーバが AAA クライアントとして定義されていることを確認します。Common Services（[AAA Mode Setup] ページ）と ACS（[Network Configuration]）で定義された共有秘密キーが一致することを確認します。
- Common Services の [AAA Mode Setup] ページで、各 ACS サーバの IP アドレスが正しく定義されていることを確認します。
- ACS の [Administration Control] ページで、正しいアカウントが定義されていることを確認します。

- Common Services の [AAA Mode Setup] ページにアクセスして、Common Services と Security Manager（および AUS などの他のインストール済みアプリケーション）が Cisco Secure ACS に登録されていることを確認します。
- ACS で [Administration Control] > [Access Setup] に移動して、ACS が HTTPS 通信用に設定されていることを確認します。
- ACS ログに「key mismatch」エラーが書き込まれている場合は、Security Manager サーバがネットワーク デバイス グループ（NDG）のメンバーとして定義されているかどうかを確認します。その場合は、NDG 用のキーが事前に定義されていれば、そのキーが Security Manager サーバを含む NDG 内の個々のデバイスに対して定義されたキーよりも優先されることに注意してください。NDG 用に定義されたキーが、Security Manager サーバの秘密キーと一致することを確認します。

読み取り専用アクセスが付与されたシステム管理者

フル権限を持つ System Administrator としてログインしたにもかかわらず、Security Manager のすべてのポリシー ページに読み取り専用アクセスしかできない場合は、Cisco Secure ACS で次の手順を実行します。

- （NDG を使用している場合）Cisco Secure ACS のナビゲーション バーの [Group Setup] をクリックしてから、System Administrator ユーザ ロールが CiscoWorks と Cisco Security Manager の*両方*の必要なすべての NDG（特に、Common Services/Security Manager サーバを含む NDG）に関連付けられていることを確認します。
- ナビゲーション バーの [Network Configuration] をクリックしてから、次の手順を実行します。
  - Common Services/Security Manager サーバが Not Assigned（デフォルト）グループに割り当てられていないことを確認します。
  - Common Services/Security Manager サーバが RADIUS ではなく TACACS+ を使用するように設定されていることを確認します。TACACS+ は、2 台のサーバ間でサポートされている唯一のセキュリティ プロトコルです。

（注）　TACACS+ または RADIUS 用に Security Manager で管理するネットワーク デバイス（ルータ、スイッチ、ファイアウォールなど）を設定できます。

ACS の変更が Security Manager に表示されない

Security Manager と Cisco Secure ACS 4.x を使用している場合は、Security Manager サーバ上の Security Manager または CiscoWorks Common Services にログインしたときに ACS からの情報がキャッシュされます。Security Manager にログイン中に Cisco Secure ACS の [Network Configuration] と [Group Setup] で変更を加えた場合は、Security Manager で、その変更が、すぐに表示されない、または、すぐに有効にならない可能性があります。Security Manager と Common Services をログアウトしてそれらのウィンドウを閉じてから、再度ログインして、ACS からの情報をリフレッシュする必要があります。

ACS で変更を加える必要がある場合は、ログアウトして Security Manager ウィンドウを閉じてから、製品に再ログインする方法がベスト プラクティスです。

（注）　Cisco Secure ACS 3.3 はサポートされていませんが、このバージョンの ACS を使用している場合は、Windows サービスを開いて Cisco Security Manager Daemon Manager サービスを再起動し、ACS の変更を Security Manager に表示させる必要があります。

ACS で設定されたデバイスが Security Manager に表示されない

Cisco Secure ACS 上で設定したデバイスが Security Manager に表示されない場合は、デバイスの表示名に伴う問題だと思われます。

Security Manager で定義するデバイスの表示名は、そのデバイスを AAA クライアントとして追加したときに ACS で設定した名前と一致する*必要があります*。このことは、特に、ドメイン名を使用する場合に重要です。Security Manager でドメイン名をデバイス名に付加する場合は、ACS 内の AAA クライアントのホスト名を **<device_name>.<domain_name>** にする必要があります（例：pixfirewall.cisco.com）。

Cisco Secure ACS が到達不能になった後の Security Manager での作業

Cisco Secure ACS が到達不能な場合は、Security Manager セッションが影響を受けます。そのため、複数の Cisco Secure ACS サーバを使用するフォールトトレラントなインフラストラクチャの構築を検討する必要があります。複数のサーバを使用することによって、いずれかの ACS サーバの通信機能が失われても、Security Manager 内の作業を継続できます。

セットアップに Cisco Secure ACS が 1 つしか含まれておらず、ACS が到達不能になった場合でも Security Manager での作業を継続する場合は、Security Manager サーバ上でのローカル AAA 認証に切り替えることができます。

手順

AAA モードに変更するには、次の手順を実行します。

ステップ 1　**admin** CiscoWorks ローカル アカウントを使用して Common Services にログインします。

ステップ 2　[Server] > [Security] > [AAA Mode Setup] を選択してから、AAA モードを Non-ACS/CiscoWorks Local に変更します。これによって、ローカル Common Services データベースとその組み込みロールを使用して認証と認可を実行できます。ローカル認証を利用するには、AAA データベース内にローカル ユーザを作成する必要があります。

ステップ 3　[Change] をクリックします。

Cisco Secure ACS へのアクセスの復元

Cisco Secure ACS がダウンしたために Security Manager にアクセスできなくなった場合は、次の手順を実行します。

- ACS サーバ上で Windows サービスを起動して、CSTacacs サービスと CSRadius サービスが稼働しているかどうかを確認します。必要に応じて、これらのサービスを再起動します。
- CiscoWorks Common Services で次の手順を実行します。

ステップ 1　**admin** ユーザとして Common Services にログインします。

ステップ 2　DOS ウィンドウを開いて、*NMSROOT***bin****perl ResetLoginModule.pl** を実行します。

ステップ 3　Common Services を終了してから、**admin** ユーザとして再度ログインします。

ステップ 4　[Server] > [Security] > [AAA Mode Setup] に移動してから、AAA モードを [Non-ACS] > [CW Local] モードに変更します。

ステップ 5　Windows サービスを開いて、Cisco Security Manager Daemon Manager サービスを再起動します。

マルチホーム デバイスに伴う認証の問題

Cisco Secure ACS に追加されたマルチホーム デバイス（複数の Network Interface Card（NIC; ネットワーク インターフェイス カード）が実装されたデバイス）が設定できない場合は、ユーザ ロールにデバイスの変更権限が含まれていたとしても、そのデバイスの IP アドレスの入力方法に伴う問題が発生する可能性があります。

マルチホーム デバイスを Cisco Secure ACS の AAA クライアントとして定義する場合は、NIC ごとの IP アドレスを定義してください。入力するたびに Enter を押します。詳細については、「NDG を使用しないデバイスの AAA クライアントとしての追加」（P.8-17）を参照してください。

NAT 境界の背後に設置されたデバイスに伴う認証の問題

Cisco Secure ACS に追加された NAT 前または NAT 後の IP アドレスを持つデバイスを設定できない場合は、ユーザ ロールにデバイスの変更権限が含まれていたとしても、設定した IP アドレスに伴う問題が発生する可能性があります。

デバイスが NAT 境界の背後に設置されている場合は、Cisco Secure ACS の AAA クライアント設定でデバイスのすべての IP アドレス（NAT 前と NAT 後を含む）を定義してください。ACS への AAA クライアント設定の追加方法については、『*User Guide for Cisco Secure Access Control Server*』を参照してください。

Common Services 4.2.2 を使用するローカル RBAC

Security Manager 4.3、4.4 および 4.5 以前は、Cisco Secure ACS を使用する重要なメリットは、(1) 特殊な権限セット（特定のポリシー タイプの設定だけをユーザに許可する場合など）を使用して非常に粒度の高いユーザ ロールを作成できることと、(2) ネットワーク デバイス グループ（NDG）を設定することによって特定のデバイスにユーザを制限できることでした。このような粒度の高い特権（効率的な「ロールベース アクセス コントロール」（RBAC））は、Cisco Secure ACS を使用していない限り、Security Manager 4.2 以前のバージョンでは利用できませんでした。このような粒度の高い特権（RBAC）は、ACS を使用せずにローカル RBAC を利用できる Common Services 4.0、4.0 および 4.2.2 をそれぞれ使用するため、Security Manager 4.3、4.4 および 4.5 で利用できます。

Security Manager 4.3、4.4 および 4.5 は ACS 4.2 との互換性を維持します。「Security Manager と Cisco Secure ACS の統合」（P.8-12）を参照してください。

（注）　RBAC 機能を ACS から Common Services に移行したいユーザは、手動で行う必要があります。移行スクリプトも、他の移行サポートもありません。

Common Services 4.2.2 には、ユーザのカスタム ロールを定義し、ユーザの既存のロールをカスタマイズするためのデバイス レベルの RBAC があります。次の機能を使用できます。

- ユーザの管理（追加、削除、編集）
- デバイス レベルの RBAC を提供するためのネットワーク デバイス グループ（NDG）の管理
- カスタム ロールの管理

- デバイス グループへのロールのマッピング
- 「ネットワーク オブジェクトの表示」、「サービス オブジェクトの変更」、および「アクセス ルールの変更」などのポリシー オブジェクト タイプとポリシー タイプに対する粒度の高い特権。

次のエリアのタスクを完了することで、Common Services 4.2.2 を使用してローカル RBAC を実装できます。

- 「認証モードの設定」（P.8-33）
- 「ユーザ管理」（P.8-33）
- 「グループ管理」（P.8-34）
- 「ロール管理」（P.8-34）

認証モードの設定

次の手順を実行して、非 ACS アカウントを設定します。「非 ACS アカウント」（P.8-2）を参照してください。

次に、[CiscoWorks Local] ログイン モジュールを選択します。

ヒント　[CiscoWorks Local] は Security Manager のクリーン インストールのデフォルト値です。

ユーザ管理

Common Services の [Local User Setup] ページに移動します。

Security Manager がインストールされているサーバ >

Cisco Security Manager アプリケーションのデスクトップ アイコン >

ユーザ アカウント ログイン >

[Server Administration] >

[Home] >

[System Tasks] >

[Local User Setup]

[Local User Setup] ページで、ユーザを選択し、次のアクションのいずれかを選択できます。

- Import Users
- Export Users
- Edit
- Delete
- Add
- Modify My Profile

複数のユーザを選択する場合、[Edit] は選択できません。

ユーザを選択しない場合は、次のアクションのいずれかを選択できます。

- Import Users
- Add

- Modify My Profile

[Edit] または [Add] を選択する場合は、次の 3 つの認可タイプのいずれかを選択できます。

- Full Authorization
- Enable Task Authorization
- Enable Device Authorization

グループ管理

Security Manager の [Device Groups] ページに移動します。

Security Manager がインストールされているサーバ >

Configuration Manager アプリケーションのデスクトップ アイコン >

ユーザ アカウント ログイン >

[Tools] >

[Security Manager Administration] >

[Device Groups]

Common Services インターフェイス（Security Manager がインストールされているサーバ > Cisco Security Manager アプリケーションのデスクトップ アイコン）を使用してデバイス グループを管理することはできません。

ロール管理

[Role Management Setup] ページに移動します。

Security Manager がインストールされているサーバ >

Cisco Security Manager アプリケーションのデスクトップ アイコン >

ユーザ アカウント ログイン >

[Server Administration] >

[Server] >（メニュー セレクタ記号）>

[Security] >

[Single-Server Management] >

[Role Management Setup]

[Role Management Setup] ページにはデフォルトのロール（Approver、Help Desk、Network Administrator、Network Operator、Security Administrator、Security Approver、Super Admin、および System Administrator）が表示されます。[Role Management Setup] ページには、追加したカスタム ロール（ある場合）も表示されます。

[Role Management] ページでは、Add、Edit、Delete、Copy、Export、Import、Set as default、および Clear default の各操作を実行できます。

トラブルシューティング

CiscoWorks Common Services は、Security Manager に、サーバ上でのインストール、アンインストール、および再インストール用のフレームワークを提供します。Security Manager サーバ ソフトウェアのインストールまたはアンインストールでエラーが発生した場合は、Common Services のオンライン ヘルプの「Troubleshooting and FAQs」を参照してください。

次のトピックは、スタンドアロン バージョンの Cisco Security Agent を含む、クライアント システムまたはサーバ上に Security Manager 関連ソフトウェア アプリケーションをインストール、アンインストール、または再インストールしたときに発生する可能性のある問題の解決に役立ちます。

- 「Cisco Security Manager サービスの起動要件」（P.A-1）
- 「必要な TCP ポートと UDP ポートの包括的リスト」（P.A-2）
- 「Security Manager サーバのトラブルシューティング」（P.A-4）
- 「Security Manager クライアントのトラブルシューティング」（P.A-10）
- 「サーバ セルフテストの実行」（P.A-16）
- 「サーバ トラブルシューティング情報の収集」（P.A-17）
- 「サーバ プロセス ステータスの表示と変更」（P.A-18）
- 「サーバ インストール ログ ファイルの確認」（P.A-18）
- 「Symantec の共存問題」（P.A-19）
- 「Windows アップデートのインストール後の問題」（P.A-19）
- 「高度な暗号化による ASA デバイスへの接続の問題」（P.A-20）
- 「インストール時に使用する Activation.jar のポップアップ表示」（P.A-20）
- 「Windows のデフォルト ユーザ テンプレートのロケールを米国英語に設定する方法」（P.A-21）

Cisco Security Manager サービスの起動要件

Cisco Security Manager サービスは、特定の順序で起動しなければ、Security Manager が正しく機能しません。これらのサービスの初期化は、Cisco Security Manager Daemon Manager サービスによって制御されます。Cisco Security Manager サービスの起動タイプは変更しないでください。また、Cisco Security Manager サービスは手動で停止または開始しないでください。特定のサービスを再起動しなければならない場合は、Cisco Security Manager Daemon Manager を再起動して、すべての関連サービスが正しい順序で停止および開始する必要があります。

必要な TCP ポートと UDP ポートの包括的リスト

Cisco Security Management Suite アプリケーションは、クライアントや他のアプリケーションと通信する必要があります。その他のサーバ アプリケーションは別のコンピュータ上にインストールできます。通信を成功させるためには、特定の TCP ポートと UDP ポートを開いて、トラフィック送信に使用できるようにする必要があります。通常は、「必要なサービスとポート」（P.3-1）に記載されているポートを開くだけで十分です。ただし、アプリケーションが通信不能なことを検出した場合は、次の表内のポートも開く必要もあります。リストはポート番号順に並んでいます。

表 A-1　必要なサービスとポート

サービス	対象または使用アプリケーション	ポート番号/ポートの範囲	プロトコル	着信	発信
FTP	Security Manager と TMS サーバ間の通信	21	TCP	—	X
SSH	Common Services	22	TCP	—	X
	Security Manager	22	TCP	—	X
Telnet	Security Manager	23	TCP	—	X
SMTP	Common Services	25	TCP	—	X
TACACS+（ACS の場合）	Common Services	49	TCP	—	X
TFTP	Common Services	69	UDP	X	X
HTTP	Common Services	80	TCP	—	X
	Security Manager		TCP	—	X
SNMP（ポーリング）	Common Services	161	UDP	—	X
	Performance Monitor	161	UDP	—	X
SNMP（トラップ）	Common Services	162	UDP	—	X
	Performance Monitor	162	UDP	X	—
HTTPS（SSL）	Common Services	443[1]	TCP	X	—
	Security Manager		TCP	X	X
	AUS		TCP	X	—
	Performance Monitor		TCP	X	—
syslog[2]	Security Manager	514	UDP	X	—
	Common Services（Security Manager がインストールされていない場合）	514 または 49514（この行の脚注を参照）	UDP	X	—
	Performance Monitor（Security Manager がインストールされていない場合）	514	UDP	X	—
リモート コピー プロトコル	Common Services	514	TCP	X	X

表 A-1　必要なサービスとポート （続き）

サービス	対象または使用アプリケーション	ポート番号/ポートの範囲	プロトコル	着信	発信
HTTP	Common Services	1741	TCP	X	—
	Security Manager		TCP	X	—
	AUS		TCP	X	—
	Performance Monitor		TCP	X	—
RADIUS LDAP Kerberos	Security Manager（外部 AAA サーバへ）	1645、1646、1812（新規）、389、636（SSL）、88	TCP	—	X
Access Control Server HTTP/HTTPS	Security Manager	2002	TCP	—	X
CiscoWorks ゲートキーパー用の HIPO ポート	Common Services	8088	TCP	X	X
Tomcat シャットダウン	Common Services	9007	TCP	X	—
Tomcat Ajp13 コネクタ	Common Services	9009	TCP	X	—
データベース	Security Manager	10033	TCP	X	—
License Server	Common Services	40401	TCP	X	—
Daemon Manager	Common Services	42340	TCP	X	X
Osagent	Common Services	42342	UDP	X	X
データベース	Common Services	43441	TCP	X	—
Sybase	Auto Update Server	43451	TCP	X	X
	Performance Monitor	43453	TCP	X	X
DCR と OGS	Common Services	40050 ～ 40070	TCP	X	—
Event Services	Software Service	42350/ 44350	UDP	X	X
	Software Listening	42351/ 44351	TCP	X	X
	Software HTTP	42352/ 44352	TCP	X	X
	Software Routing	42353/ 44353	TCP	X	X
転送メカニズム（CSTM）	Common Services	50000 ～ 50020	TCP	X	—

1. Cisco Security Monitoring, Analysis, and Response System（Cisco Security MARS）アプライアンスと情報を共有または交換するために、Security Manager はデフォルトでポート 443 上の HTTPS を使用します。この目的で別のポートを使用するかどうかを選択できます。
2. Security Manager のインストールまたはアップグレード時に、Common Services syslog サービス ポートが 514 から 49514 に変更されます。あとで Security Manager がアンインストールされた場合、ポートは 514 に戻されません。

Security Manager サーバのトラブルシューティング

この項では、次の疑問にお答えします。

- 「インストール中のサーバ障害」（P.A-4）
- 「インストール後のサーバ障害」（P.A-5）
- 「アンインストール中のサーバ障害」（P.A-8）

インストール中のサーバ障害

Q. サーバ ソフトウェアのインストール時に表示されたこのインストール エラー メッセージはどういう意味ですか。

A. サーバ ソフトウェアのインストール エラー メッセージと説明を表 A-2（P.A-4）に示します。この表は先頭の文字のアルファベット順に並べられています。

表 A-2　インストール エラー メッセージ（サーバ）

メッセージ	メッセージの理由	ユーザ アクション
`License file failed.ERROR: The file with the name c:\progra~1\CSCOpx\setup does not exist`	先に Common Services 依存アプリケーションをアンインストールしようとして失敗しました。	1. サーバをシャットダウンしてから、再起動します。 2. レジストリ エディタを使用して次のエントリを削除します。 `$HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Resource Manager\CurrentVersion` 3. Security Manager をインストールしたディレクトリで、*setup* という名前のサブディレクトリを作成します。 4. CMFLOCK.TXT を削除します（存在する場合）。 5. Security Manager を再インストールします。
`Corrupt License file. Please enter a valid License file.`	ライセンス ファイルが破損しているか、ライセンス ファイルの内容が無効です。	「ライセンスに関する支援」（P.2-9）を参照してください。
`Corrupt License file entered for 5 tries. Install will proceed in EVAL mode. Press OK to proceed.`	5 回連続で無効なライセンス ファイルへのパス名を入力した可能性があります。試行が 5 回失敗したら、インストールが評価モードに変わります。	[OK] をクリックして、ライセンス エラー ダイアログ ボックスを閉じて、ウィザードの次の画面に進みます。
`One instance of CiscoWorks Installation is already running.If you are sure that no other instances are running, remove the file C:\CMFLOCK.TXT.This installation will now abort.`	先に Common Services 依存アプリケーションをインストールしようとして失敗した可能性があります。	C:\CMFLOCK.TXT ファイルを削除してから、もう一度試してみてください。

`Severe`
 	
`Failed on call to FileInsertLine.`
	サーバがハード ドライブ スペースに関する要件を満たしていません。	「サーバの要件および推奨事項」（P.3-4）を参照してください。

表 A-2　インストール エラー メッセージ（サーバ）（続き）

メッセージ	メッセージの理由	ユーザ アクション
Temporary directory used by installation has reached _istmp9x. If _istmp99 is reached, no more setups can be run on this computer, they fail with error -112.	サーバ上で、ソフトウェア インストール中に自動的に削除される予定の一時ファイルが残っています。	サーバ上の一時ディレクトリで名前に「_istmp」文字列が含まれるサブディレクトリを探します。このようなサブディレクトリをすべて削除します。
Windows cannot find 'C:\Documents and Settings\Administrator\WINDOWS\System32\cmd.exe'. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search.	サポートされていないにもかかわらず、Terminal Services をインストール中にイネーブルにした可能性があります。「インストール準備状況チェックリスト」（P.4-3）を参照してください。	1. Terminal Services をディセーブルにします。 この手順については、次の URL にある『*Installing and Getting Started With CiscoWorks LAN Management Solution 3.1*』の「Terminal Server Support for Windows 2000 and Windows 2003 Server」トピックを参照してください。 http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.1/install/guide/IGSG31.html 2. Security Manager をもう一度インストールしてみてください。
Setup has detected that unInstallShield is in use. Close unInstallShield and restart setup. Error 432.	インストール中に Windows アカウント権限がチェックされます。CiscoWorks Common Services をインストールしている Windows アカウントがローカル管理者特権を持っていない場合は、InstallShield にこのエラー メッセージが表示されます。	1. %WINDIR% に書き込むための適切な権限が付与されていることを確認します。インストールまたはアンインストールは、ローカル管理者グループのメンバーが実施する必要があります。 2. [OK] をクリックしてエラー メッセージを閉じ、Windows からログアウトして、ローカル管理者特権を持つアカウントを使用して Windows に再ログインします。

Q. サーバ インストーラが処理を中断（ハングアップ）した場合はどうしたらいいですか。

A. リブートしてもう一度試してみてください。

Q. Cisco Security Manager と Cisco Secure Access Control Server の両方を 1 つのシステム上にインストールできますか。

A. インストールしないことを推奨します。同じサーバ上での Security Manager と Cisco Secure ACS for Windows の共存はサポートされていません。

Q. Security Manager データベースのバックアップが失敗するのはなぜですか。

A. Tivoli などのネットワーク管理アプリケーションを使用して、Security Manager がインストールされたシステム上に Cygwin をインストールした場合は、Security Manager データベースのバックアップに失敗します。Cygwin をアンインストールしてください。

インストール後のサーバ障害

Q. Security Manager インターフェイスが表示されない、または、正しく表示されない、あるいは、特定のインターフェイス要素が欠けています。原因は何でしょうか。

A. いくつかの可能性が考えられます。このリスト内のシナリオを参照して、インターフェイスに影響を与える可能性のある単純な問題を特定し、対処してください。

- 必要なサービスのいくつかがサーバ上で動作していません。サーバのデーモン マネージャを再起動して、すべてのサービスの起動が完了するのを待ってから、Security Manager クライアントを再起動して接続し直してみてください。
- サーバに十分な空きディスク スペースがありません。サーバ上の Security Manager パーティションの空き容量が 500 MB 以上あることを確認してください。
- 基本ライセンス ファイルが破損しています。「ライセンスに関する支援」（P.2-9）を参照してください。
- サーバで使用されている Windows 言語が間違っています。米国英語バージョンの Windows 上の英語と、日本語バージョンの Windows 上の日本語しかサポートされていません（「サーバの要件および推奨事項」（P.3-4）を参照）。他の言語はインストールされたバージョンの Security Manager に悪影響を与える可能性があります。また、GUI 要素の欠落は可能性のある症状の 1 つです。サポートされていない言語を使用している場合は、サポートされている言語を選択してから、Security Manager をアンインストールして再インストールしてください。「サーバ アプリケーションのアンインストール」（P.5-17）を参照してください。
- ネットワーク接続上で Security Manager インストール ユーティリティを実行しましたが、この使用方法はサポートされていません（「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-2）を参照）。サーバ ソフトウェアをアンインストールして再インストールする必要があります。「サーバ アプリケーションのアンインストール」（P.5-17）を参照してください。
- クライアント システムが最小限の要件を満たしていません。「クライアントの要件」（P.3-10）を参照してください。
- HTTP を使用しようとしましたが、必要なプロトコルは HTTPS です。
- ボタンだけが表示されません。Security Manager クライアントを使用している最中に、クライアント システム上で [Display Properties] コントロール パネルを開いて、[Appearance] タブでいくつかの設定を変更した可能性があります。この問題に対処するには、Security Manager クライアントを終了してから、再起動してください。
- 間違ったグラフィックス カードのドライバ ソフトウェアがクライアント システム上にインストールされています。「クライアントの要件」（P.3-10）を参照してください。

問題　Web ブラウザを使用して Security Manager への Web インターフェイスを開こうとしたときに、Security Manager サーバ上の /cwhp/LiaisonServlet にアクセスするための権限がないことを伝えるメッセージが表示されました。これはどういう意味ですか。

ソリューション　下の表に、この問題の一般的原因と提案されている対処法を示します。

表 A-3　LiaisonServlet エラーの原因と対処法

原因	回避策
サーバ上にアンチウイルス アプリケーションがインストールされている	アンチウイルス アプリケーションをアンインストールします。
サーバ上に IIS がインストールされている	IIS は Security Manager と互換性がないため、アンインストールする必要があります。

表 A-3　LiaisonServlet エラーの原因と対処法 （続き）

原因	回避策
Security Manager に必要なサービスが正しい順序で開始されていない	自動に設定する必要があるサービスは Cisco Security Manager Daemon Manager だけです。他の CiscoWorks サービスは手動に設定する必要があります。Daemon Manager が他の Ciscoworks サービスを起動するまでに数分かかる場合があることに注意してください。これらのサービスは、正しい順序で起動する必要があります。手動でサービスを起動した場合はエラーを引き起こす可能性があります。
casuser パスワード	casuser ログインは、Windows 管理者と同じで、すべての Common Services タスクと Security Manager タスクにアクセスできます。次のように casuser パスワードをリセットします。 1. サーバ上でコマンド プロンプトを開きます。 （注） Windows Server 2008 を使用している場合は、コマンド プロンプトを開くときに [Run as administrator] オプションを使用する必要があります。 2. `C:\Program Files\CSCOpx\setup\support\resetCasuser.exe` と入力して、Enter を押します。 3. オプション 1（casuser パスワードのランダム生成）を選択します。

Q. Security Manager を使用してサーバ上のディレクトリを参照したときに、ローカル ボリュームだけが表示され、マップされたドライブは表示されません。どうしてですか。

A. Microsoft はサーバ セキュリティを強化するために Windows の設計にこの機能を組み込みました。Security Manager で選択する必要のあるすべてのファイル（ライセンス ファイルなど）をサーバ上に配置する必要があります。

Q. 日本語バージョンの Windows の [Start] メニューに Security Manager が表示されないのはなぜですか。

A. サーバ上の地域と言語のオプションを、英語を使用するように設定した可能性があります。日本語バージョンの Windows 内の言語として英語はサポートされていません（「サーバの要件および推奨事項」（P.3-4）を参照）。コントロール パネルを使用して、言語を日本語にリセットしてください。

Q. サーバの SSL 証明書が無効になっています。また、DCRServer プロセスが開始しません。原因は何でしょうか。

A. サーバの日付または時刻が SSL 証明書の有効範囲外にリセットされています。「インストール準備状況チェックリスト」（P.4-3）を参照してください。この問題に対処するには、サーバの日付/時刻の設定をリセットしてください。

Q. サーバとクライアント間の通信に使用されるプロトコルの入力が要求されませんでした。デフォルトで使用されるプロトコルは何ですか。他のモードを使用してこの設定を手動で変更する必要がありますか。

A. サーバのインストール中にクライアントをインストールした場合は、デフォルトで、サーバとクライアント間の通信プロトコルとして HTTPS が使用されます。通信はデフォルト プロトコルを使用して保証されているため、この設定を手動で変更する必要はありません。

プロトコルとして HTTP を選択するオプションは、サーバ インストーラとは別に、クライアント インストーラを実行して Security Manager クライアントをインストールした場合にのみ使用できます。ただし、サーバとクライアント間の通信プロトコルとして HTTP を使用しないことを推奨します。クライアントは、サーバが使用するように設定されたプロトコルを使用する必要があります。

Q. VMware セットアップを使用しているとシステムのパフォーマンスが受け入れられないほど低下します。たとえば、システムのバックアップに 2 時間もかかります。

A. Security Manager を実行している VM に複数の CPU が割り当てられていることを確認してください。1 つの CPU しか割り当てられていないシステムでは、一部のシステム アクティビティに対して受け入れられないほどのパフォーマンスを示すことがわかっています。

Q. 検証などのいくつかの操作が、SQL クエリー例外をログに出力して失敗します。原因は何でしょうか。

A. Sybase の一時ディレクトリのディスク領域が足りなくなり、一時ファイルの作成に失敗した可能性があります。デフォルトでは、Windows の一時ディレクトリの下に Sybase の一時ファイルが作成されます。システム変数 SA_TMP が定義されている場合は、SA_TMP に指定されたディレクトリに一時ファイルが作成されます。Sybase の一時ファイルが配置されるディスク領域をクリアしてから、Security Manager を再起動します。

アンインストール中のサーバ障害

Q. このアンインストール エラー メッセージはどういう意味ですか。

A. アンインストール エラー メッセージと説明を表 A-4（P.A-9）に示します。この表は先頭の文字のアルファベット順に並べられています。アンインストール エラー メッセージに関するその他の情報については、Security Manager のインストールの Common Services のマニュアルを参照してください。

表 A-4　アンインストール エラー メッセージ

メッセージ	メッセージの理由	ユーザ アクション
C:*NMSROOT*\MDC\msfc-backend refers to a location that is unavailable. It could be on a hard drive on this computer, or on a network. Check to make sure that the disk is properly inserted, or that you are connected to the Internet or your network, and then try again. If it still cannot be located, the information might have been moved to a different location.	このメッセージは害がない可能性があります。[OK] をクリックしてメッセージを消去する以外は何もする必要がありません。そうしなかった場合は、次の条件の一方または両方が適用されるサーバ上でメッセージが表示される可能性があります。 - 簡易ファイル共有が Windows 上でイネーブルになっている。 - オフライン ファイル同期が Windows 上でイネーブルになっている。	メッセージを消去してアンインストールが失敗した場合は、次の可能性のある対処法の一方または両方を試して、もう一度アンインストールを行ってみてください。 **簡易ファイル共有** 1. [Start] > [Settings] > [Control Panel] > [Folder Options] を選択します。 2. [View] タブをクリックします。 3. [Advanced Settings] ペインの一番下までスクロールします。 4. [Use simple file sharing (Recommended)] チェックボックスをオフにしてから、[OK] をクリックします。 **オフライン ファイル同期** 1. [Start] > [Settings] > [Control Panel] > [Folder Options] を選択します。 2. [Offline Files] タブをクリックします。 3. [Enable Offline Files] チェックボックスをオフにしてから、[OK] をクリックします。
C:\temp\<*subdirectory*>\ setup.exe - Access is denied. The process cannot access the file because it is being used by another process. 0 file(s) copied. 1 file(s) copied.	アンインストールが失敗しました。	サーバをリブートしてから、「サーバ アプリケーションのアンインストール」（P.5-17）に記載されている手順を実行してください。
Windows Management Instrumentation (WMI) is running. The setup program has detected Windows Management Instrumentation (WMI) services running. This will lock some Cisco Security Manager processes and may abort uninstallation abruptly. To avoid this, uninstallation will stop and start the WMI services. Do you want to proceed? Click Yes to proceed with this uninstallation. Click No to exit uninstallation.	組織で WMI が使用されているか、誰かが誤ってサーバ上の WMI サービスをイネーブルにした可能性があります。	[Yes] をクリックします。

Q. アンインストーラがハングアップした場合はどうしたらいいですか。

A. リブートしてからもう一度試してみてください。

Q. アンインストーラに *crmdmgtd* サービスが応答していないという内容のメッセージが表示され、「Do you want to keep waiting?」と尋ねられた場合はどうしたらいいですか。

A. アンインストール スクリプトには、スクリプトがタイムアウトする前に命令に応答しなかった crmdmgtd サービスを停止する命令が含まれています。[Yes] をクリックします。ほとんどの場合、crmdmgtd サービスは、その後、予想どおりに停止します。

Security Manager クライアントのトラブルシューティング

この項では、次の疑問にお答えします。

- 「インストール中のクライアント障害」（P.A-10）
- 「インストール後のクライアント障害」（P.A-13）

インストール中のクライアント障害

Q. クライアント ソフトウェアのインストール時に表示されたこのインストール エラー メッセージはどういう意味ですか。

A. クライアント ソフトウェアのインストール エラー メッセージと説明を表 A-5 に示します。この表は先頭の文字のアルファベット順に並べられています。

表 A-5　インストール エラー メッセージ（クライアント）

メッセージ	メッセージの理由	ユーザ アクション
Could not install engine jar	以前のソフトウェア インストールとアンインストールが原因で InstallShield が正しく動作していません。	1. 次のとおりに移動します。**C:\Program Files\Common Files\InstallShield\Universal\common\Gen1**. 2. Gen1 フォルダの名前を変更してから、もう一度 Security Manager クライアントのインストールを試してみてください。 Gen1 が存在しない場合は、代わりに **common** の名前を変更します。

表 A-5　インストール エラー メッセージ（クライアント）（続き）

メッセージ	メッセージの理由	ユーザ アクション
Error - Cannot Connect to Server The client cannot connect to the server. This can be caused by one of the following reasons: The server name is incorrect. The protocol (http, https) is incorrect. The server is not running. Network access issues. Please confirm that the server name and protocol are correct. The server is running and you are not experiencing network connectivity issues by loading the CS Manager home page in your browser.	サーバが誤って HTTPS トラフィック用に設定されている可能性があります。	1. ブラウザから、**https://**<*server*>**/CSCOnm/servlet/login/login.jsp** にある Cisco Security Management Suite デスクトップにログインします。 2. [Server Administration] をクリックします。 3. [Admin] ウィンドウで、[Server] > [Security] を選択します。 4. TOC で、[Single Server Management] > [Browser-Server Security Mode Setup] を選択してから、[Enable] オプション ボタンが選択されていることを確認します。 オプション ボタンが選択されていなかった場合は、それを選択してから、[Apply] をクリックします。 5. プロンプトが表示されたら、Cisco Security Manager Daemon Manager を再起動します。 6. 5 分待ってから、もう一度 Security Manager クライアントを使用してみてください。 それでも接続できない場合は、エラー メッセージが示している他の可能性のある問題を検討してください。
Error - Cisco Security Agent Running Installation cannot proceed while the Cisco Security Agent is running Do you want to disable the Cisco Security Agent and continue with the installation?	クライアントのインストール中は、Cisco Security Agent を停止する必要があります。	• Cisco Security Agent をディセーブルにする場合は、[Yes] をクリックします。 • 操作をキャンセルして、Cisco Security Agent を手動で停止する場合は、[No] をクリックします。 • Security Manager クライアントのオンライン ヘルプにアクセスする場合は、[Help] をクリックします。
Error - Cisco Security Agent not Stopped The installation will be aborted because the Cisco Security Agent could not be stopped. Please attempt to disable Cisco Security Agent before repeating the installation process.	Security Manager クライアントから Cisco Security Agent を停止できませんでした。	[OK] をクリックして、このエラー メッセージを閉じ、インストールを中断します。もう一度インストールを試す前に、Cisco Security Agent を手動でディセーブルにします。

表 A-5　インストール エラー メッセージ（クライアント）（続き）

メッセージ	メッセージの理由	ユーザ アクション
Error occurred during the installation: null.	以前のソフトウェア インストールとアンインストールが原因で InstallShield が正しく動作していません。	1. C:\Program Files\Common Files\InstallShield\Universal\common\Gen1 に移動します。 2. Gen1 フォルダの名前を変更してから、もう一度 Security Manager クライアントのインストールを試してみてください。 Gen1 が存在しない場合は、代わりに **common** の名前を変更します。
Errors occurred during the installation. • null	ログイン アカウントに管理特権が付与されている Windows ユーザだけが、Security Manager Client をインストールできます。	Windows 管理者としてログインしてから、もう一度 Security Manager クライアントのインストールを試してみてください。
Internet Explorer cannot download CSMClientSetup.exe from <*server*>. Internet Explorer was not able to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later.	クライアント システム上の OS が Windows 2008 の場合は、Internet Explorer セキュリティ強化のデフォルト設定が原因で、サーバからクライアント ソフトウェア インストール ユーティリティをダウンロードできない可能性があります。	1. [Start] > [Control Panel] > [Add or Remove Programs] を選択します。 2. [Add/Remove Windows Components] をクリックします。 3. Windows コンポーネント ウィザード ウィンドウが開いたら、[Internet Explorer Enhanced Security Configuration] チェックボックスをオフにして、[Next] をクリックし、[Finish] をクリックします。
Please read the information below. The following errors were generated: • WARNING: The <*drive*> partition has insufficient space to install the items selected.	空きスペースが不十分なドライブまたはパーティション上に Security Manager クライアントをインストールしようとした可能性があります。	[Back] をクリックしてから、Security Manager クライアントをインストールする別の場所を選択してください。
Unable to Get Data A database failure prevented successful completion of this operation.	サーバ データベースが完全に稼働する前に、クライアントを使用してサーバに接続しようとした可能性があります。	数分待ってから、もう一度ログインしてみてください。問題が解決されない場合は、必要なすべてのサービスが実行していることを確認してください。

Q. クライアント インストーラが処理を中断（ハングアップ）した場合はどうしたらいいですか。

A. 次の手順を試してみてください。いずれかの手順で問題が解決される可能性があります。

- クライアント システム上にアンチウイルス ソフトウェアがインストールされている場合は、それをディセーブルにしてから、もう一度インストーラを実行してみてください。
- クライアント システムをリブートしてから、もう一度インストーラを実行してみてください。
- クライアント システム上でブラウザを使用して、**http://**<*server_name*>**:1741** にある Security Manager サーバにログインします。「Forbidden」または「Internal Server Error」というエラー メッセージが表示された場合は、必要な Tomcat サービスが実行していません。最

近サーバをリブートして、Tomcat の稼働までに十分な時間がなかったことがない場合は、サーバ ログを確認するか、その他のステップを実行して、Tomcat が動作していない理由を調査する必要があります。

Q. インストーラに、以前のバージョンのクライアントがインストールされているためアンインストールされるという内容のメッセージが表示されます。しかし、以前のバージョンのクライアントはインストールされていません。これは障害ですか。

A. クライアントのインストールまたは再インストール中に、インストーラがインストールされていないクライアントを検出して、そのクライアントがアンインストールされるという内容の誤ったメッセージを表示することがあります。このメッセージは、システム内に特定の古いレジストリ エントリが残っていることが原因で表示されます。このメッセージが表示されてもクライアントのインストールは正常に進行しますが、レジストリ エディタを使用して次のキーを削除し、今後のインストールでこのメッセージが表示されないようにします。HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Cisco Security Manager Client （レジストリ エディタを開くには、[Start] > [Run] を選択して **regedit** と入力します）。また、C:\Program Files\Zero G Registry\.com.zerog.registry.xml ファイルの名前を変更します（どんな名前でも可）。

インストール後のクライアント障害

Q. インターフェイスが正しく表示されないのはなぜですか。

A. 古いビデオ（グラフィックス）カードは、ドライバ ソフトウェアをアップグレードしなければ、Security Manager GUI を正しく表示しない可能性があります。この問題がクライアント システムに影響するかどうかをテストするには、[My Computer] を右クリックして、[Properties] を選択し、[Hardware] を選択して、[Device Manager] をクリックしてから、[Display adapters] エントリを展開します。アダプタのエントリをダブルクリックして、使用されているドライバのバージョンを確認します。その後で、次のいずれかを実行できます。

- クライアント システムで ATI MOBILITY FireGL ビデオ カードが使用されている場合は、カードに付属していたビデオ ドライバ以外のドライバを入手しなければならない場合があります。使用するドライバは、手動で Direct 3D が設定できる必要があります。このような機能のないドライバは、Security Manager GUI 内の要素をクライアント システムに表示できない可能性があります。
- ビデオ カードの場合は、PC メーカとカード メーカの Web サイトにアクセスして、最新の Java2 グラフィックス ライブラリの表示との非互換性をチェックしてください。既知の非互換性が残っているほとんどのケースで、半分以上のメーカが互換性のあるドライバを入手してインストールするための手段を提供しています。

Q. 日本語バージョンの Windows の [Start] メニューに Security Manager クライアントが表示されないのはなぜですか。

A. クライアント システム上で英語を使用するように、地域と言語のオプションを設定している可能性があります。日本語バージョンの Windows 内の言語として英語はサポートされていません。コントロール パネルを使用して、言語を日本語にリセットしてください。

Q. Security Manager クライアントがインストールされたワークステーション上で一部または全部のユーザの [Start] メニューに Security Manager クライアントが表示されないのはなぜですか。

A. クライアントをインストールするときに、製品をインストールしているユーザ専用のショートカットを作成するのか、すべてのユーザ用のショートカットを作成するのか、どのユーザ用のショートカットも作成しないのかを選択します。インストール後にこの選択を変更する場合は、Cisco Security Manager Client フォルダを Documents and Settings\<user>\Start Menu\Programs\Cisco

Security Manager から Documents and Settings\All Users\Start Menu\Programs\Cisco Security Manager にコピーすることによって、手動で変更できます。ショートカットを作成しないことにした場合は、指定された All Users フォルダ内にショートカットを手動で作成する必要があります。

Q. クライアント システムとサーバ間の接続が異常に遅いと感じる場合、または、ログイン時に DNS エラーが表示される場合はどうしたらいいですか。

A. クライアント システム上の **hosts** ファイル内に Security Manager サーバ用のエントリを作成しなければならない場合があります。このようなエントリは、ネットワーク用の DNS サーバに登録されていない場合にサーバへの接続の確立に役立つ可能性があります。クライアント システム上でこの有効なエントリを作成するには、メモ帳またはその他のプレーン テキスト エディタを使用して、C:\WINDOWS\system32\drivers\etc\hosts を開きます （ホスト ファイル自体にエントリの追加方法に関する詳細な手順が保存されています）。

Q. Security Manager クライアントを使用してログインしようとしたときにエラー メッセージが表示されることなくログイン資格情報が受け入れられましたが、Security Manager デスクトップが空の状態で使用できません。認証セットアップの何が間違っているのでしょうか （また、Security Manager サーバ上の Common Services でログイン資格情報が受け入れられましたが、Web ブラウザ上で Cisco Security Management Suite デスクトップのロードに失敗します。これも同じ原因でしょうか）。

A. Security Manager と Common Services に対してログイン認証サービスを提供するための Cisco Secure ACS に必要なステップが完了していない可能性があります。ACS でログイン資格情報を入力しましたが、Security Manager サーバを AAA クライアントとして定義していません。この定義を行わなければ、ログインできません。詳しい手順については、ACS のマニュアルを参照してください。

Q. Security Manager クライアントを使用してサーバにログインできず、次のようなメッセージが表示されます。どうしたらいいですか。

... repeatedly that the server is checking its license.	サーバが最小限のハードウェア要件とソフトウェア要件を満たしていることを確認してください。「サーバの要件および推奨事項」（P.3-4）を参照してください。
`Synchronizing with DCR.`	2 通りの可能性が考えられます。 • サーバの再起動直後に Security Manager クライアントを起動した可能性があります。その場合は、サーバが完全に使用可能になるまで数分待ってから、Security Manager クライアントを使用してみてください。 • CiscoWorks 管理パスワードにアンパサンド（&）などの特殊文字が含まれている可能性があります。その結果、Security Manager のインストール時にサーバ上の *NMSROOT*\lib\classpath サブディレクトリで comUser.dat ファイルを作成できませんでした。ここで、*NMSROOT* は Common Services をインストールしたディレクトリです（デフォルトは C:\Program Files\CSCOpx です）。 **a.** Cisco TAC に連絡して、**comUser.dat** の交換または Security Manager の再インストールに関する支援を要請してください。 **b.** または、特殊文字を含まない Common Services パスワードを作成します。

Error - Unable to Check License on Server. An attempt to check the license file on the Security Manager server has failed. Please confirm that the server is running. If the server is running, please contact the Cisco Technical Assistance Center.	次のサービスのいずれかが正しく起動していない可能性があります。サーバ上で、[Start] > [Programs] > [Administrative Tools] > [Services] を選択して、次のような名前のサービスを右クリックし、ショートカット メニューから [Restart] を選択します。 • Cisco Security Manager Daemon Manager • Cisco Security Manager database engine • Cisco Security Manager Tomcat Servlet Engine • Cisco Security Manager VisiBroker Smart Agent • Cisco Security Manager Web Engine 5 分待ってから、もう一度 Security Manager クライアントを起動してみてください。

Q. デフォルト ブラウザとして Internet Explorer を使用しているときにアクティビティ レポートが表示されないのはなぜですか。

A. この問題は、無効なレジストリ キー値、または Internet Explorer に関連付けられた DLL ファイルの場所に関する間違いが原因で発生します。この問題の対処法については、http://support.microsoft.com/kb/281679/EN-US から入手可能な Microsoft サポート技術情報の記事 281679 を参照してください。

Q. どうすれば、ログイン ウィンドウの [Server Name] フィールドからサーバ リストを消去できますか。

A. csmserver.txt を編集して必要のないエントリを削除します。このファイルは、Security Manager クライアントをインストールしたディレクトリ内にあります。デフォルトの場所は、C:\Program Files\Cisco Systems\Cisco Security Manager Client です。

Q. バージョン ミスマッチが原因で Security Manager クライアントがロードされなかった可能性があります。これはどういう意味ですか。

A. Security Manager サーバのバージョンとクライアントのバージョンが一致していません。これを修正するには、最新のクライアント インストーラをサーバからダウンロードしてインストールします。

Q. クライアント ログ ファイルはどの場所にありますか。

A. クライアント ログ ファイルは、C:\Program Files\Cisco Systems\Cisco Security Manager Client\logs に配置されています。GUI セッションごとに専用のログ ファイルが作成されます。

Q. Security Manager が HTTPS モードで動作中かどうかはどうすれば確認できますか。

A. 次のいずれかを実行します。

- ブラウザを使用してサーバにログインしたら、アドレス フィールド内の URL を調査します。URL が https で始まっていれば、Security Manager が HTTPS モードで動作しています。
- [Common Services] > [Server] > [Security] > [Single Server Management] > [Browser-Server Security Mode Setup] に移動します。[Current Setting] が [Enabled] になっていれば、Security Manager が HTTPS モードで動作しています。この設定が [Disabled] の場合は、HTTP を使用します。

- クライアントを使用してログインするときに、まず、HTTPS モードを試してみてください（[HTTPS] チェックボックスをオンにします）。「Login URL access is forbidden; Please make sure your protocol (HTTP, HTTPS) is correct」というメッセージが表示されたら、サーバは HTTP モードで動作している可能性があります。[HTTPS] チェックボックスをオフにして、もう一度試してみてください。

Q. どうすれば、クライアント デバッグ ログ レベルをイネーブルにできますか。

A. デフォルトで C:\Program Files\Cisco Systems\Cisco Security Manager Client\jars に配置されている client.info ファイル内で、DEBUG_LEVEL パラメータに DEBUG_LEVEL=ALL を追加してから、Security Manager クライアントを再起動します。

Q. 2 画面構成で作業している場合は、Security Manager クライアントが第 2 画面上で動作していても、必ず、特定のウィンドウとポップアップ メッセージが第 1 画面に表示されます。たとえば、クライアントが第 2 画面上で動作しているときに、必ず、Policy Object Manager などのウィンドウが第 1 画面に表示されます。これを修正できますか。

A. これは、特定のオペレーティング システムにおける 2 画面サポートの実装方法に伴う既知の問題です。Security Manager クライアントを第 1 画面上で動作させることを推奨します。クライアントは、2 画面構成の設定後に起動する必要があります。

他の画面でウィンドウが開いた場合は、Alt + スペースバーを押した後に M を押すことによってそのウィンドウを移動できます。その後で、矢印キーを使用してウィンドウを移動します。

Q. クライアント システム上でソフトウェアをインストールまたはアンインストールできません。どうしてですか。

A. クライアント システム上でインストールとアンインストールを*同時に*実行した場合は、それらが別々のアプリケーションに対するものであっても、クライアント システムの InstallShield データベース エンジンに悪影響を与え、ソフトウェアのインストールまたはアンインストールができなくなります。詳細については、Cisco.com アカウントにログインしてから、Bug Toolkit を使用して CSCsd21722 と CSCsc91430 を確認してください。

サーバ セルフテストの実行

Security Manager サーバが正しく動作していることを確認するセルフテストを実行するには、次の手順を実行します。

ステップ 1　Security Manager クライアントが Security Manager サーバに接続されているシステムから、[Tools] > [Security Manager Administration] を選択します。

ステップ 2　[Administration] ウィンドウで、[Server Security] をクリックしてから、任意のボタンをクリックします。新しいブラウザが開いて、クリックしたボタンに対応する Common Services GUI のセキュリティ設定ページが表示されます。

ステップ 3　[Common Services] ページの [Server] タブで、[Admin] を選択します。

ステップ 4　[Admin] ページの TOC で、[Selftest] をクリックします。

ステップ 5　[Create] をクリックします。

ステップ 6　[SelfTest Information at <*MM-DD-YYYY HH:MM:SS*>] リンクをクリックします。ここで、

- *MM-DD-YYYY* は、現在の月、日、年です。
- *HH:MM:SS* は、[Selftest] をクリックした時、分、秒を表すタイムスタンプです。

ステップ 7　[Server Info] ページでエントリを読み取ります。

サーバ トラブルシューティング情報の収集

Security Manager で問題が発生しており、エラー メッセージ内の推奨事項のすべてを試し、このマニュアル内の可能性のある解決策を確認したにもかかわらず、問題が解決されない場合は、Security Manager Diagnostics ユーティリティを使用してサーバ情報を収集します。

Security Manager Diagnostics ユーティリティは、ZIP ファイルの CSMDiagnostics.zip からサーバ診断情報を収集します。このファイル名を変更しなかった場合は、Security Manager Diagnostics を実行するたびに新しい情報でファイルが上書きされます。CSMDiagnostics.zip ファイル内の情報は、サーバ上の Security Manager または関連アプリケーションで発生した問題のシスコ テクニカルサポート エンジニアによる解決を支援します。

ヒント　Security Manager には、アプリケーションによって実施された設定変更に関する情報を収集する高度なデバッギング オプションも用意されています。このオプションをアクティブにするには、[Tools] > [Security Manager Administration] > [Debug Options] を選択してから、[Capture Discovery/Deployment Debugging Snapshots to File] チェックボックスをオンにします。診断ファイルに保存されたその他の情報はトラブルシューティングの試みに役立つ可能性がありますが、ファイルにはパスワードなどの機密情報が書き込まれている場合があることに注意してください。デバッグ レベルは、Cisco Technical Assistance Center（TAC）から変更を指示された場合にだけ変更してください。

Security Manager Diagnostics は次のいずれかの方法で実行できます。

Security Manager クライアント システムから	Security Manager サーバから
1. サーバへの Security Manager クライアント セッションを確立したら、[Tools] > [Security Manager Diagnostics] をクリックして [OK] をクリックします。 CSMDiagnostics.zip ファイルは、サーバ上の *NMSROOT*\MDC\etc\ ディレクトリに保存されます。ここで、*NMSROOT* は、Common Services をインストールしたディレクトリです（C:\Program Files\CSCOpx など）。 **2.** [Close] をクリックします。 **（注）** このユーティリティを実行するたびに上書きされないようにこのファイルの名前を変更することを推奨します。	**1.** Windows のコマンド ウィンドウを開きます。それには、たとえば [Start] > [Run] を選択し、**command** と入力します。 **2.** 次のように入力します。**C:\Program Files\CSCOpx\MDC\bin\CSMDiagnostics**。または、この ZIP ファイルを *NMSROOT*\MDC\etc\ とは別の場所に保存するには、**CSMDiagnostics** *drive:\path* と入力します。たとえば、CSMDiagnostics D:\temp と入力します。

サーバ プロセス ステータスの表示と変更

Security Manager のサーバ プロセスが正しく動作していることを確認するには、次の手順を実行します。

ステップ 1　CiscoWorks のホームページで、[Common Services] > [Server] > [Admin] を選択します。

ステップ 2　[Admin] ページの TOC で、[Processes] をクリックします。

[Process Management] テーブルにすべてのサーバ プロセスが表示されます。[ProcessState] カラム内のエントリが、プロセスが正常に動作しているかどうかを示します。

ステップ 3　必要なプロセスが動作していない場合は、それを再起動します。「サーバ上の全プロセスの再起動」（P.A-18）を参照してください。

（注）　ローカル管理者特権を持つユーザのみがサーバ プロセスを起動または停止できます。

サーバ上の全プロセスの再起動

（注）　すべてのプロセスを停止してから、それらを再起動しなければ、この方法は機能しません。

ステップ 1　コマンド プロンプトで、**net stop crmdmgtd** と入力してすべてのプロセスを停止します。

ステップ 2　**net start crmdmgtd** と入力してすべてのプロセスを再起動します。

ヒント　または、[Start] > [Settings] > [Control Panel] > [Administrative Tools] > [Services] を選択してから、Cisco Security Manager Daemon Manager を再起動できます。

サーバ インストール ログ ファイルの確認

サーバからの応答が期待していたものと違っていた場合は、サーバ インストール ログ ファイルでエラー メッセージと警告メッセージを確認できます。

Cisco_Prime_install_*.log を開くときにはテキスト エディタを使用します。

ほとんどの場合、確認すべきログ ファイルは、ファイル名に最大の番号が付けられたファイルか、作成日が最新のファイルです。

たとえば、ログ ファイルでは、次のようなエラー エントリと警告エントリが確認できます。

```
ERROR: Cannot Open C:\PROGRA~1\CSCOpx/lib/classpath/ssl.properties at
C:\PROGRA~1\CSCOpx\MDC\Apache\ConfigSSL.pl line 259.
INFO: Enabling SSL....
WARNING: Unable to enable SSL. Please try later....
```

（注）　重大な問題が発生した場合は、ログ ファイルを Cisco TAC に送信できます。「マニュアルの入手方法およびテクニカル サポート」（P.xi）を参照してください。

Symantec の共存問題

Symantec Antivirus Corporate Edition 10.1.5.5000 と Security Manager を同じシステムで使用し、Security Manager 起動中に問題が発生した場合は、次の手順に従ってください。

手順

1. Symantec Antivirus を完全にディセーブルにします。
2. Security Manager サービスを再起動します。（「サーバ上の全プロセスの再起動」（P.A-18）を参照）。
3. Symantec Event Manager を最後に起動したような方法で、Symantec サービスのセット（Symantec Antivirus、Symantec Antivirus Definition Watcher、Symantec Settings Manager、および Symantec Event Manager）を再起動します。

Windows アップデートのインストール後の問題

Microsoft Windows アップデートをインストールした後に、Security Manager Daemon Manager に関する問題が発生する可能性があります。原因は、Windows アップデートのインストールにより、*.dll ファイルが更新される場合があり、これに依存する Common Services などのアプリケーションの機能に影響する可能性があることです。

この問題は、次の症状で認識できます。Windows アップデートの後、Security Manager によってすべてのプロセスを開始しますが、Security Manager に HTTPS を介して到達できません。このため、Security Manager クライアントから HTTPS を使用します。

この問題が生じるのは、Common Services が Windows 内のファイルおよび関連付けに依存するためです。これらのファイルは、脆弱性を修正し、不正利用から Windows を保護するために変更できます。ただし、意図しない副作用として再起動した場合はこれらの変更により、Security Manager サーバの異常動作が起きる可能性があります。

この問題は、Windows アップデート、またはその他のアプリケーションが、*.dll ファイル、実行可能ファイル、起動プロセス、Windows コンポーネント、またはパーティション サイズに影響する Windows に変更を加えると、いつでも発生する可能性があります。

Windows で変更が行われ、その再起動で Security Manager が異常動作した場合に、この問題を解決するには、Security Manager を再インストールする必要があります。

シスコは Security Manager サーバを定期的にバック アップすることを推奨します。特に、定期的なバック アップが行われていない場合、または Security Manager インストールに対して多数の変更を行う場合は、Windows アップデートまたはその他のインストーラ パッケージを実行する前に Security Manager サーバをバックアップする必要があります。

高度な暗号化による ASA デバイスへの接続の問題

このトラブルシューティングの項目は、高度な暗号化を使用して ASA デバイスを追加および検出できない場合に役立ちます。特に AES-256 を使用する場合は、Java Cryptography Extension（JCE）Unlimited Strength Jurisdiction Policy File をダウンロードしてインストールする必要があります。Security Manager はこの拡張を含みませんが、これをサポートします。

問題　証明書に含まれるキーが 1024 ビットを超える場合に問題が発生します。Java ランタイム環境（JRE）に含まれているデフォルト ポリシー ファイルによって設定される暗号化強度の制限は、すべての国へのインポートが可能な、最高強度暗号化アルゴリズムとキー長を提供します。

ソリューション　当該国で暗号化のインポートに制限が定められていなければ、無制限強度ポリシー ファイルをダウンロードできます。

ステップ 1　http://java.sun.com/javase/downloads/index.jsp に移動します。

ステップ 2　「Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6」をダウンロードします。

ステップ 3　ダウンロードしたパッケージの README.txt ファイルの説明に従ってください。

インストール時に使用する Activation.jar のポップアップ表示

このトラブルシューティング項目は、インストール中に「Activation.jar being used by some other service.」というメッセージがポップアップ ウィンドウで表示される場合に役立ちます。

ヒント　この問題はきわめてまれにしか起こりません。

はじめる前に

サーバのすべてのアンチウイルスまたはモニタリング エージェント プロセスは、インストール前にシャット ダウンする必要があります。詳細については、「インストール準備状況チェックリスト」（P.4-3）を参照してください。

問題

「Activation.jar being used by some other service.」というメッセージがポップアップ ウィンドウで表示されます。

ソリューション

次の手順を使用してください。

ステップ 1　ポップアップで [OK] をクリックして、インストールを完了します。

ステップ 2　Security Manager をアンインストールし、サーバを再起動します。

ステップ 3　Security Manager を再インストールします。

ステップ 4　インストールを開始した直後に、「services.msc」をコマンド プロンプトに入力し、Enter キーを押します。

ステップ 5　[Services] メニューを開くと、「Cisco Security Manager Daemon Manager」が表示されるまで更新が続きます。

ステップ 6　[CSM Daemon Manager] を右クリックして、[Properties] > [Startup type] > [Disabled] の順にクリックします。

ステップ 7　[CWCS syslog service] を右クリックして、[Properties] > [Startup type] > [Disabled] の順にクリックします。

ステップ 8　インストールの完了後、サーバの再起動時に、「Disabled」から「Automatic」モードに上記のサービスの両方の起動タイプを変更します。

Windows のデフォルト ユーザ テンプレートのロケールを米国英語に設定する方法

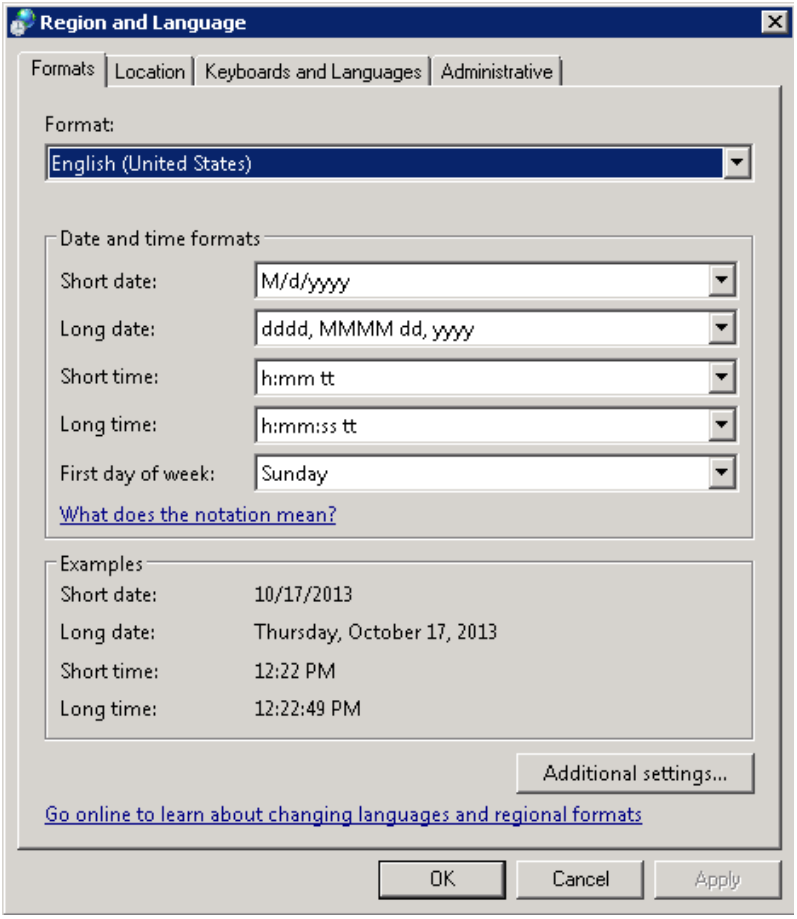
通常、英語（米国）以外の Windows ロケールを使用する場合は、Security Manager をインストールする前にデフォルトのシステム ロケールを米国英語に変更する必要があります。デフォルト システム ロケールを変更し、サーバをリブートしても、デフォルト プロファイルは変更されません。現在のユーザは、適切な設定をするだけでは十分ではありません。これは、Security Manager はすべての Security Manager サーバ プロセスを実行する新しいアカウント（「casuser」）を作成するためです。

ここでは、特に、通常英語（米国）以外の Windows ロケールを使用する場合に、Security Manager サーバの地域と言語設定を設定する方法について説明します。具体的な詳細は、Windows 2008 R2 Enterprise Server SP1（64 ビット）に適用されますが、その他のサポートされているサーバ オペレーティング システムに非常に似ています。

新たに作成されたすべてのユーザに現在のユーザと同じ設定を適用するには、新しいユーザ アカウントに現在のユーザの設定をコピーする必要があります。これは、次に示す手順で実行できます。

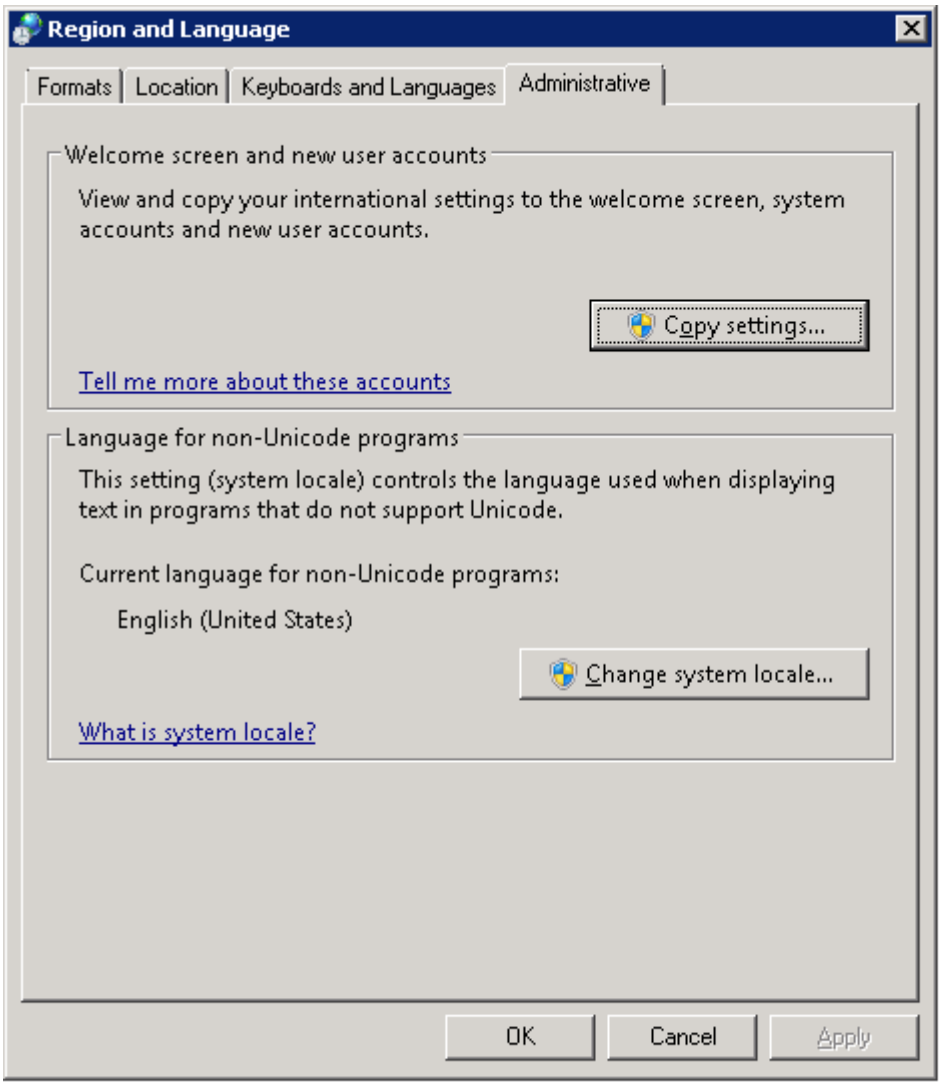
現在のユーザが、[Region and Language] ダイアログボックスで適切な米国英語に設定されていることを確認します。（このダイアログボックスのナビゲーション パスは [Start] > [Control Panel] > [Region and Language] です）。

図 A-1　Windows の [Region and Language] ダイアログボックス



[Administrative] タブをクリックします。[Copy Settings...] ボタンを見つけます。

図 A-2　[Administrative] タブ



[Copy settings...] ボタンをクリックします。[Welcome screen and new user account] 設定ダイアログ ボックスが表示されます。

[Copy your current settings to:] で、[New user accounts] ボックスをオンにします。これによって、新たに作成されたすべてのユーザに現在のユーザと同じ設定を適用します。

最後に、Cisco Security Manager サーバをインストール（または再インストール）します。新しいインストールでは、すべての Security Manager サーバ プロセスを実行する新しいアカウント（「casuser」）には米国英語のデフォルト プロファイルが適用されます。

Image Manager の権限マトリクス

次の一連の表には、Image Manager の RBAC（ロールベース アクセス コントロール）権限マトリクスが示されています。

- 表 B-1、「その他のアクション」
- 表 B-2、「イメージ ビュー」
- 表 B-3、「バンドル ビュー」
- 表 B-4、「デバイス ビュー」
- 表 B-5、「ジョブ ビュー」

これらの表に示されている、Image Manager とビュー、アクション、および権限の詳細については、次の URL にある『*User Guide for Cisco Security Manager 4.4*』を参照してください。

http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html

表 B-1　その他のアクション

	その他のアクション				
	IM の起動	管理設定の表示	管理設定の変更	設定アーカイブの表示	設定アーカイブの変更
Image Manager の表示	YES	NO	NO	NO	NO
管理設定の表示	NO	YES	NO	NO	NO
デバイスの表示	NO	NO	NO	NO	NO
設定アーカイブの表示	NO	NO	NO	YES	NO
デバイスの変更	NO	NO	NO	NO	NO
Image Manager リポジトリの変更	NO	NO	NO	NO	NO
管理設定の変更	NO	NO	YES	NO	NO
展開	NO	NO	NO	NO	NO
送信（WF）	NO	NO	NO	NO	NO
承認（WF）	NO	NO	NO	NO	NO

表 B-2　　イメージ ビュー

	イメージ ビュー								
	リポジトリに移動	イメージのダウンロード							
		ファイル システム	CCO	インストール ウィザードの起動	リリース ノートのチェック	アップデートのチェック	リポジトリからの削除	バンドルへの追加	ダウンロード進行状況の表示
Image Manager の表示	YES	NO	NO	NO	YES	NO	NO	NO	YES
管理設定の表示	NO	NO	NO	NO	NO	NO	NO	NO	NO
デバイスの表示	NO	NO	NO	NO	NO	NO	NO	NO	NO
設定アーカイブの表示	NO	NO	NO	NO	NO	NO	NO	NO	NO
デバイスの変更	NO	NO	NO	YES	NO	NO	NO	NO	NO
Image Manager リポジトリの変更	YES	YES	YES	NO	NO	YES	YES	YES	YES
管理設定の変更	NO	NO	NO	NO	NO	NO	NO	NO	NO
展開	NO	NO	NO	NO	NO	NO	NO	NO	NO
送信（WF）	NO	NO	NO	NO	NO	NO	NO	NO	NO
承認（WF）	NO	NO	NO	NO	NO	NO	NO	NO	NO

表 B-3　バンドル ビュー

	バンドル ビュー			
	バンドル名の表示	バンドル コンテンツのチェック	バンドル コンテンツの変更	バンドルのインストール
Image Manager の表示	YES	YES	NO	NO
管理設定の表示	NO	NO	NO	NO
デバイスの表示	NO	NO	NO	NO
設定アーカイブの表示	NO	NO	NO	NO
デバイスの変更	NO	NO	NO	NO
Image Manager リポジトリの変更	YES	YES	YES	YES
管理設定の変更	NO	NO	NO	NO
展開	NO	NO	NO	NO
送信（WF）	NO	NO	NO	NO
承認（WF）	NO	NO	NO	NO

表 B-4　デバイス ビュー

	デバイス ビュー								
	デバイスとデバイス グループの表示	デバイス インベントリの表示	[Device Detail] タブの表示：全部で 4 つ	フラッシュからのイメージの削除	フラッシュからのイメージのダウンロード	イメージ インストール ウィザードの起動	イメージ アップグレードの実行	バンドルへの追加	ダウンロードの表示
Image Manager の表示	YES	YES	YES	NO	NO	NO	NO	NO	YES
管理設定の表示	NO	NO	NO	NO	NO	NO	NO	NO	NO
デバイスの表示	NO	NO	NO	NO	NO	NO	NO	NO	NO
設定アーカイブの表示	NO	NO	NO	NO	NO	NO	NO	NO	NO
デバイスの変更	NO	NO	NO	YES	YES	YES	YES	NO	NO
Image Manager リポジトリの変更	NO	NO	NO	NO	NO	NO	NO	YES	NO
管理設定の変更	NO	NO	NO	NO	NO	NO	NO	NO	NO
展開	NO	NO	NO	NO	NO	NO	NO	NO	NO
送信（WF）	NO	NO	NO	NO	NO	NO	NO	NO	NO
承認（WF）	NO	NO	NO	NO	NO	NO	NO	NO	NO

表 B-5　ジョブ ビュー

	ジョブ ビュー										
	ジョブ アクション（NWF モード）							追加のジョブ オプション（WF モード）			
	ジョブ テーブルとジョブの詳細の表示（全部で 3 タブ）	更新	編集	再試行	廃棄	ロールバック	中断	承認	拒否	送信	展開
Image Manager の表示	YES	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO
管理設定の表示	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
デバイスの表示	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
設定アーカイブの表示	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
デバイスの変更	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Image Manager リポジトリの変更	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
管理設定の変更	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
展開	NO	NO	YES	YES	YES	YES	YES	NO	NO	NO	YES
送信（WF）	NO	YES	NO	NO	NO	NO	NO	NO	NO	YES	NO
承認（WF）	NO	YES	NO	NO	NO	NO	NO	YES	YES	NO	NO

数字

2 画面構成 A-16

A

Access Control Server（ACS）
- ACS が到達不能になってからの作業 8-31
- CiscoWorks AAA モードの設定 8-23
- CiscoWorks での統合の実行 8-21
- CiscoWorks でのローカル ユーザの作成 8-22
- Daemon Manager の再起動 8-25
- NDG 機能のアクティブ化 8-19
- NDG を使用したユーザ グループへのロールの割り当て 8-27
- NDG を使用しない AAA クライアントとしてのデバイスの追加 8-17
- NDG を使用しないユーザ グループへのロールの割り当て 8-26
- Security Manager との統合 8-12
- Security Manager に表示されないデバイス 8-31
- Security Manager に表示されない変更 8-30
- Security Manager の登録 8-24
- アクセスの復元 8-31
- 管理制御ユーザの作成 8-21
- 管理対象デバイスの追加 8-17
- 管理対象デバイスの追加と NDG の設定 8-27
- サーバ アプリケーションの再インストール 5-3
- システム管理者の読み取り専用アクセス 8-30
- システム識別ユーザの定義 8-15
- 通知用の SMTP と電子メールの設定 8-25
- デフォルト ロール 8-10
- 統合チェックリスト 8-14
- 統合の実行 8-15
- 統合要件 8-13
- トラブルシューティング 8-29
- 認証の失敗 8-29
- ネットワーク デバイス グループの作成 8-20
- ネットワーク デバイス グループの設定 8-18
- 複数のバージョンの Security Manager の使用 8-29
- マルチホーム デバイスの追加 8-32
- ユーザ グループへのロールの割り当て 8-26
- ユーザ権限 8-4
- ユーザ権限について 8-3
- ユーザの追加 8-15
- ユーザ ロールと権限の関連付け 8-11
- ユーザ ロールのカスタマイズ 8-11

Approver ロール 8-6

Auto Update Server（AUS）
- アップグレード 5-5
- アンインストール 5-17
- インストール 5-2
- 概要 1-2
- サーバ要件 3-4
- 必要なユーザ アカウント 5-1
- ライセンス 2-4, 2-8
- ログイン 6-13

C

Cisco Security Agent（CSA）
- アップグレード 5-5
- インストール 5-2

Cisco Security Agent、ディセーブル化 6-8

Cisco Security Agent、ディセーブル中の注意事項 6-8

CiscoWorks Common Services
- AAA モードの設定 8-23

ACS での管理制御ユーザの作成 8-21
Cisco Secure ACS への Security Manager の登録 8-24
Cisco Secure ACS 用の統合の実行 8-21
Cisco Secure ACS 用のローカル ユーザの作成 8-22
アップグレード 5-5
アンインストール 5-17
インストール 5-2
概要 1-1
システム識別ユーザの定義 8-22
使用可能なユーザ ロール 8-6
必要なバージョン 1-1
ユーザ権限について 8-3
ユーザへのロールの割り当て 8-7
ユーザ ロールと権限の関連付け 8-11
ライセンス供与 2-4, 2-8
ログイン 6-13

D

Daemon Manager
Cisco Secure ACS 統合後の再起動 8-25

F

Firefox
Javascript のイネーブル化 6-5
新しいタブでのヘルプの表示 6-5
キャッシュ サイズ要件 6-4
サポートされているバージョン 3-7, 3-11
必要な設定の構成 6-4
プリファレンス ファイルの編集 6-4
ポップアップ ブロックのディセーブル化 6-4

H

Help Desk ユーザ ロール 8-6
HTTPS
非デフォルト ポートの設定 6-10
モードの決定 A-15
HTTP、非デフォルト ポートの設定 6-10

I

IE 8 互換表示 3-7, 3-11, 6-2
Internet Explorer
キャッシュ サイズ要件 6-3
サポートされているバージョン 3-7, 3-11
セキュリティ設定 6-3
必要な設定の構成 6-2
Internet Information Server（IIS）、アンインストールするための要件 4-2

J

Java 要件 3-7, 3-11

L

LAN Management Solution（LMS）、サポートされていない使用 4-2
LiaisonServlet エラー、トラブルシューティング A-6

N

Network Access Restriction（NAR） 8-13
Network Administrator ロール
Cisco Secure ACS 8-10
CiscoWorks 8-6
Network Operator ロール 8-6

P

pdshow コマンド 7-2
Performance Monitor
アップグレード 5-5
アンインストール 5-17
概要 1-3

サーバ要件 3-4
必要なユーザ アカウント 5-1
ライセンスの更新 5-15
ログイン 6-13

R

Resource Manager Essentials（RME）
アップグレード 5-5
アンインストール 5-17
サーバ要件 3-4
必要なユーザ アカウント 5-1
ライセンスの更新 5-15
ログイン 6-13
restorebackup.pl コマンド 5-12

S

Security Administrator ロール 8-10
Security Manager
ACS との相互作用のトラブルシューティング 8-29
Daemon Manager の再起動 8-25
アップグレード後の必要な変更 5-13
アップグレード前の保留データのコミット 5-8
インストール 5-2
概要 1-2
関連アプリケーション 1-3
クライアントを使用したログイン 6-12
コンポーネント アプリケーション 1-1
サーバのアップグレード 5-5
サーバのアンインストール 5-17
サーバのダウングレード 5-18
サーバ要件 3-4
サービス起動要件 A-1
はじめる前に 7-8
必要なユーザ アカウント 5-1
ブラウザを使用したログイン 6-13
ライセンスの更新 5-15
Security Manager クライアント
2 画面モードでの実行 A-16
HTTPS モードの決定 A-15
アップグレードできない 6-11
アンインストール 6-14
インストール 6-7
インストールを阻止するセキュリティ設定の処理 6-10
クライアント ログの配置 A-15
バージョン ミスマッチの解決 A-15
パッチング 6-11
非デフォルト HTTP/HTTPS ポートの設定 6-10
ログイン 6-12
ログイン ウィンドウでのサーバ リストの消去 A-15
SMTP、ACS 通知用の設定 8-25
SSL 証明書の無効化 4-3
Sybase、ディセーブルにするための要件 4-4
System Administrator ロール 8-6

T

TACACS+
ACS の使用 8-12
CiscoWorks AAA モードとしての選択 8-23
TCP
必要なポートの包括的リスト A-2
標準で必要なポートのリスト 3-1
Terminal Services、サポートされていない設定 3-4

U

UDP
必要なポートの包括的リスト A-2
標準で必要なポートのリスト 3-1

V

VMWare のサポートされているバージョン 3-7
VNC、インストールに使用 5-2

W

Web ブラウザ
- アプリケーションへのログイン 6-13
- サポートされている 3-7, 3-11
- 必要な設定の構成 6-1

Windows サービス、必要な 4-2

あ

アカウント、ユーザ
- 管理 8-1
- 必要な 5-1

アップグレード、確認 7-7

アプリケーション
- クライアントのインストールと設定 6-1
- サーバのアップグレード 5-5
- サーバのアップグレード後の必要な変更 5-13
- サーバのアンインストール 5-17
- サーバのインストールとアップグレード 5-1
- サーバのダウングレード 5-18
- ログイン 6-12

アンインストール
- Security Manager クライアント 6-14
- サーバ アプリケーション 5-17
- サーバのトラブルシューティング A-8
- サーバを再起動するための推奨事項 5-17

暗号化されたディレクトリ、制限 3-4

アンチウイルス ユーティリティ、ディセーブルにするための要件 4-3

い

インストール
- Security Manager、AUS、Common Services 5-2
- Security Manager クライアント 6-7
- 確認 7-7
- クライアントのトラブルシューティング A-10
- クライアントを阻止するセキュリティ設定 6-10
- サーバのトラブルシューティング A-4
- リモート デスクトップまたは VNC の使用 5-2

インポート権限 8-5

え

エラー メッセージ
- クライアントのインストール A-10
- サーバのアンインストール A-8
- サーバのインストール A-4

お

オペレーティング システム
- クライアント 3-10

か

概要 1-1, 2-1

間接アップグレード パス、定義 5-6

く

クライアント
- インストール後のトラブルシューティング A-13
- インストールのトラブルシューティング A-10
- オペレーティング システム 3-10
- 要件 3-10
- ログイン ウィンドウでのサーバ リストの消去 A-15
- ログ ファイル A-15

け

権限
- ACS 用のカスタマイズ 8-11
- CiscoWorks でのロールの割り当て 8-7
- NDG の影響 8-19
- 概要 8-3

カテゴリ 8-4
ユーザ ロールとの関連付け 8-11
言語サポート 3-10

こ

互換表示 3-7, 3-11, 6-2
このマニュアル内の表記法 ii-x

さ

サーバ
一般的な要件 3-1
インストール後タスク 7-1
インストール後のトラブルシューティング A-5
サポートされていない設定 3-4
準備状況チェックリスト 4-1, 4-3
セキュリティ、向上させるためのベスト プラクティス 4-1
セキュリティに関するベスト プラクティス 7-7
パフォーマンス、向上させるためのベスト プラクティス 4-1
日付と時刻の設定 3-1, 4-3
プロセスの確認 7-2
要件 3-4
サービス、Windows に必要な最低限の 4-2
サービス起動要件 A-1
サービス パック
クライアントへの適用 6-11
取得 5-16

し

システム識別ユーザ 8-15, 8-22
詳細 7-8
承認権限 8-5
証明書
作成するための要件 7-1
トラブルシューティング 4-3

す

ストレージ、サポートされている SAN 3-9

せ

制御権限 8-5
セキュリティ
サーバのベスト プラクティス 4-1

そ

送信権限 8-5

て

ディレクトリの暗号化、制限 3-4
データベース
アップグレード前の保留データのコミット 5-8
バックアップ 5-10, 5-11
復元 5-12
データベースのバックアップ 5-11
データベースのバックアップ中の Cygwin 障害 A-5
データベースの復元 5-12
デバイス
Security Manager に表示されない ACS 認可に対する変更 8-30
ブートストラップ 7-8
デバイスのブートストラップ 7-8
展開権限 8-5
電子メール アドレス、Security Manager 管理者 8-25

と

ドメイン コントローラ（プライマリまたはバックアップ）、サポートされていない使用 3-4
トラブルシューティング
2 画面構成 A-16
ACS 設定 8-29

Cygwin によるバックアップの阻止 A-5
java.security.cert エラー 4-3
LiaisonServlet エラー A-6
アンインストールが実行できない A-16
アンインストールのハングアップ A-10
アンチウイルス スキャナ 4-2
インストールが実行できない A-16
インストール後のクライアント A-13
インストール後のサーバ障害 A-5
インストールのハングアップ A-5, A-12
インストール ログ ファイルの確認 A-18
インストールを阻止するセキュリティ設定 6-10
エラー メッセージ
クライアントのインストール A-10
サーバのアンインストール A-8
サーバのインストール A-4
概要 A-1, B-1
クライアント インストーラから古いバージョンがインストールされていることが通知される A-13
クライアントのインストール A-10
クライアントをアップグレードできない 6-11
欠落した製品機能 A-5
サーバ セルフテスト A-16
サーバ トラブルシューティング情報の収集 A-17
サーバのアンインストール A-8
サーバのインストール A-4
サーバ プロセス A-18
サーバ プロセスの再起動 A-18
セキュリティ ソフトウェアの競合 4-2
不正なインターフェイスの表示 A-5
ホストベースの侵入防御ソフトウェア 4-2
マップされたドライブ A-7
無効な SSL 証明書 4-3

に

認可、デバイスに対する ACS での変更 8-30

ね

ネットワーク デバイス グループ（NDG）
NDG 機能のアクティブ化 8-19
作成 8-20
設定 8-18
ユーザ権限に対する影響 8-19
ロールとユーザ グループの関連付け 8-27

は

バージョン ミスマッチ、解決 A-15
バックアップ
Cygwin の制限 A-5
実行前の保留データのコミット 5-8
データベース 5-10
バックアップ / 復元アップグレード パス、定義 5-6
パフォーマンス
クライアント要件 3-10
サーバ推奨事項 3-4
サーバのベスト プラクティス 4-1

ひ

日付と時刻の設定 3-1, 4-3
表示権限 8-4

ふ

ブラウザ
Firefox に関する必要な設定の構成 6-4
Internet Explorer に関する必要な設定の構成 6-2
アプリケーションへのログイン 6-13
サポートされている 3-7, 3-11
必要な設定の構成 6-1
ブラウザ クッキー 6-2
ブラウザのクッキー 6-2
プロセス
確認 7-2

サーバの再起動 A-18
トラブルシューティング A-18
プロパティ ファイル 5-9

へ

変更権限 8-4

ほ

ポイント パッチ
クライアントへの適用 6-11
取得 5-16
ポート
必要な TCP/UDP の包括的リスト A-2
非デフォルト HTTP/HTTPS の設定 6-10
標準で必要なリスト 3-1
ポップアップ ブロック
Firefox 用のディセーブル化 6-4
ディセーブル化 6-6
保留データ、コミット 5-8

め

メモリ（RAM）
クライアント要件 3-10

ゆ

ユーザ アカウント
admin 5-1
casuser 5-1
管理 8-1
作成 5-1
システム識別 5-2
ユーザ権限
ACS 用のカスタマイズ 8-11
CiscoWorks でのロールの割り当て 8-7
NDG の影響 8-19
概要 8-3
カテゴリ 8-4
ユーザ ロールとの関連付け 8-11
ユーザ ロール
Cisco Secure ACS 8-9
CiscoWorks 8-6
使用可能な CiscoWorks ユーザ ロール 8-6
デフォルト ACS ロール 8-10
ユーザ権限との関連付け 8-11

よ

要件
一般的なサーバ 3-1
クライアント 3-10
サーバ 3-4
サポートされていないサーバ設定 3-4
日付と時刻の設定 3-1, 4-3

ら

ライセンス
Product Authorization Key（PAK） 2-3
Security Manager キット部品番号 2-8
Software License Claim Certificate 2-3
更新 5-15

り

リモート アップグレード パス、定義 5-6
リモート デスクトップ、インストールに使用 5-2

ろ

ローカル アップグレード パス、定義 5-5
ロール
Cisco Secure ACS ユーザ 8-9

CiscoWorks ユーザ 8-6
ログ ファイル A-18

わ

割り当て権限 8-5

©2008 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/