CHAPTER 1

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

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

CiscoWorks Common Services 3.3（Common Services）は、Security Manager 4.0.1、Resource Manager Essentials 4.3、Auto Update Server 4.0、および Performance Monitor 4.0.1 が動作するために必要です。Security Manager は、Common Services がすでにシステムにインストールされている場合、または、Security Manager と一緒に Common Services のインストールも選択した場合にのみインストールできます。

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

詳細については、
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/tsd_products_support_series_home.html にある Common Services のマニュアルを参照してください。

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。
  - RME に対する相互起動を設定できます。
  - Performance Monitor からデータを収集して、インベントリ ステータス ウィンドウに表示できます。
  - 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。

Cisco Security Agent

Cisco Security Agent は、ホストベースの侵入防御を提供します。Security Manager に関して、Cisco Security Agent には、外部と同梱の 2 つのバージョンがあります。

- 外部 Cisco Security Agent：Cisco Security Manager インストールの一部としてインストールされない Cisco Security Agent。
- 同梱 Cisco Security Agent：Cisco Security Manager インストールの一部としてインストールされる Cisco Security Agent。同梱 Cisco Security Agent は、「カスタマイズされたスタンドアロン エージェント」と呼ばれることがあります。これは、このエージェントが Security Manager 用にカスタマイズされており、Management Center for Cisco Security Agents がインストールされない、つまり、スタンドアロンであるためです。

Security Manager をインストールしたサーバに外部バージョンの Cisco Security Agent がインストールされていない場合は、Security Manager インストール プログラムが次のように対処します。

- Windows 2003 R2 Enterprise Server（Service Pack 2）（32 ビット）上では、インストール プログラムから Cisco Security Agent をインストールするかどうかが尋ねられます。インストールを選択した場合は、Security Manager インストーラによって同梱バージョンがサーバにインストールされます。このバージョンには、変更不可能な事前定義のポリシーが組み込まれています。この同梱バージョンの詳細については、付録 B「同梱 Cisco Security Agent：概要」を参照してください。
- Windows 2008 Enterprise Server（Service Pack 2）（32 ビット）と Windows 2008 Enterprise Server（Service Pack 2）（64 ビット）上では、インストール プログラムによって Cisco Security Agent がインストールされません。

Security Manager をインストールしたサーバに外部バージョンの Cisco Security Agent がインストールされている場合は、インストール プログラムから Cisco Security Agent をインストールするかどうかが尋ねられません。

Performance Monitor

Cisco Security Manager には、コンパニオン アプリケーションの Performance Monitor 4.0.1 が付属しています。Performance Monitor は、セキュリティ デバイスとセキュリティ サービスに重点を置いたヘルスおよびパフォーマンス モニタ アプリケーションです。また、Performance Monitor は、ネットワーク パフォーマンスの問題が大きくなる前に積極的に検出することを可能にし、過負荷状態で、余分なリソースを必要としているネットワーク部分の特定を支援し、ヘルスとパフォーマンスに関する豊富な履歴情報を事後調査と分析に提供します。さらに、Performance Monitor は、リモートアクセス VPN、サイト間 VPN、ファイアウォール、Web サーバのロードバランシング、および SSL ターミネーションのモニタをサポートします。Performance Monitor では、ブラウザベースのユーザ インターフェイスが使用されます。

Performance Monitor をインストールできるのは、Common Services のインストール後のみです。Performance Monitor は、Common Services のインストールと起動後に使用可能になる別のインストール プログラムを使用してインストールします。

Security Manager メディア キットに、Performance Monitor と RME の共用 Software License Claim Certificate が含まれています。Performance Monitor を入手するには、http://www.cisco.com/go/csmanager にアクセスし、[Download Software] を探してクリックしてください。Performance Monitor のダウンロード可能なバイナリ パッケージには、ソフトウェアのインストールと使用方法に関する詳細なマニュアルが付属しています。

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

Resource Manager Essentials

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）が付属しています。RME は、シスコ製ネットワーク デバイスのライフサイクルを管理します。ライフサイクル管理をサポートするために、RME は、デバイス インベントリを管理し、変更、コンフィギュレーション ファイル、およびソフトウェア イメージだけでなく、syslog 分析も監査できるようにします。RME では、ブラウザベースのユーザ インターフェイスが使用されます。

Security Manager メディア キットに、Performance Monitor と RME の共用 Software License Claim Certificate が含まれています。RME を入手するには、http://www.cisco.com/go/csmanager にアクセスし、[Download Software] を探してクリックしてください。RME のダウンロード可能なバイナリ パッケージには、ソフトウェアのインストールと使用方法に関する詳細なマニュアルが付属しています。

RME には、CiscoWorks LAN Management Solution（LMS）も付属しています。『CiscoWorks LAN Management Solution Deployment Guide 3.0』に RME の展開に役立つ情報が記載されていますが、Security Manager に付属の RME の場合は一部の情報が適用されないことに注意してください。詳細については、http://www.cisco.com/en/US/products/sw/cscowork/ps2073/tsd_products_support_series_home.html を参照してください。

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.7-8）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。

Security Manager のライセンスについて

Security Manager の展開を計画して、管理対象デバイスの数とタイプに応じた基本ライセンスとデバイス ライセンスが揃っていることを保証するためには、Security Manager のライセンスについて理解しておくことが重要です。次のトピックでは、Security Manager のライセンスについて説明し、特定のライセンスの例をいくつか紹介します。

ライセンスの概要

Cisco Security Manager Enterprise Edition には次の 4 つの基本バージョンがあります。

- Standard-5
- Standard-10
- Standard-25
- Professional-50

これらの基本バージョンは、それぞれ、5 台、10 台、25 台、および 50 台のデバイスを管理できます。

Professional バージョンは、50 台、100 台、および 250 台のデバイスの増加に使用可能な増分デバイス ライセンス パッケージをサポートします。また、Professional バージョンには、Cisco Catalyst 6500 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も含まれています。Standard バージョンにはこのサポートが含まれていません。

Security Manager は、デバイス インベントリに次のいずれかが追加されるたびにデバイス ライセンスを消費します。

- 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 Modules（IPS AIM）、およびホスト デバイスにインストールされた Catalyst 6500 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、ライセンスを消費しません。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）はライセンスを消費します。

Firewall Services Module（FWSM）の場合は、モジュール自体がライセンスを消費し、セキュリティ コンテキストが追加されるたびに追加のライセンスを消費します。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 つのライセンスを消費します。

デバイスのライセンスに関して理解しておくべき特別なケースを次に示します。

- **管理対象外デバイス**：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ライセンスを消費しません。

  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 ライセンスを消費しません。

- **アクティブ サーバとスタンバイ サーバ**：このライセンスは、1 台のサーバ上でのソフトウェアの使用を許可します。ハイ アベイラビリティ設定または障害回復設定で使用されるような Cisco Security Manager スタンバイ サーバは、一度に 1 台のサーバしかアクティブにならなければ、別のライセンスを必要としません。

- **RME と Performance Monitor 用のライセンス**：Cisco Security Manager には、RME と Performance Monitor 用の別のライセンス ファイルも付属しています。Cisco Security Manager 用に購入した分のデバイスに対してこれらのアプリケーションを使用する権利が与えられます。Security Manager の基本製品を注文すると、RME と Performance Monitor のライセンス用の Product Authorization Key（PAK）がもう一つ送られてきます。

インストールに対するライセンスの影響とライセンスの取得

（従来の）Security Manager 3.x リリースの有効なライセンスを持っているかどうかに関係なく、3.x 以前のお客様はすべて Security Manager 4.0.1 の新しいライセンスを取得する必要があります。増分ライセンスを除いて、既存の Security Manager 3.x ライセンスは Security Manager 4.0.1 に使用できません。

（注） 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。

50 台までのデバイスに制限されている無料の 90 日間の評価期間に加えて、Standard と Professional の 2 種類のライセンスを取得できます。

- Security Manager には、基本ライセンス ファイルと購入した数だけの追加ライセンスが付属しています。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）する必要があり、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）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。

  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。
- Common Services にはライセンス ファイルが必要ありません。
- Auto Update Server にはライセンス ファイルが必要ありません。
- Security Manager メディア キットに、Performance Monitor と RME の共用 Software License Claim Certificate が含まれています。Security Manager を登録するときに、Performance Monitor と RME の共用ライセンス ファイルも取得する必要があります。製品 DVD からアプリケーションをインストールすることも、http://www.cisco.com/go/csmanager にアクセスして、[Download Software] をクリックし、アプリケーションをダウンロードすることによってソフトウェアを入手することもできます。

割り当てられた期間（評価ライセンスの場合）またはライセンスで許可されたデバイス数を超えた場合は、ライセンスの制限が適用されます。評価ライセンスは、Professional Edition ライセンスと同じ特権を提供します。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。

ライセンス ファイルのインストール方法については、「Security Manager、Performance Monitor、および RME ライセンスの更新」（P.4-18）を参照してください。

（注）　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。サーバ上のディレクトリを参照するためにマップされたドライブを使用している場合は、Security Manager からそのドライブが認識されません。この制限は、Security Manager のパフォーマンスとセキュリティを向上させるために、Windows によって課されているものです。

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

Event Management のイネーブル化の影響

Security Manager サーバ上で Event Management をイネーブルにした場合は、そのサーバを次のいずれかのサービスに使用できなくなります。

- CiscoWorks Common Services 上の Syslog
- CiscoWorks Resource Manager Essentials（RME）上の Syslog
- Performance Monitor 上の Syslog

Security Manager のインストールまたはアップグレード中に、Common Services の syslog サービス ポートが 514 から 49514 に変更されます。Security Manager をアンインストールしても、このポートは 514 に戻りません。ポートに関する追加情報は、表 2-1（P.2-2）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 2-3（P.2-4）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。