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

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。