概要

この章は、次の項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 （1 ページ）
- セキュリティ マネージャ （2 ページ）

バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および次のデバイスを含む Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

- Cisco Catalyst 6500 および 7600 シリーズファイアウォール サービスモジュール（EOL8184）
- Cisco Catalyst 6500 シリーズ Intrusion Detection System サービスモジュール 2（EOL8843）
- Cisco Intrusion Prevention System：IPS 4200、4300、および 4500 シリーズセンサー（EOL9916）
- Cisco SR 500 シリーズセキュアルータ（EOL7687、EOL7657）
- PIX ファイアウォール（EOL）

Common Services

Common Services 4.2.2 は、Security Manager 4.27 とデフォルトでバンドルされます。

Common Services は、データ ストレージ、ログイン、ユーザ ロールの定義、アクセス権限、セキュリティプロトコル、およびナビゲーションに対する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ー側コンポーネントは次のとおりです。

- SSL[1] ライブラリ
- MariaDB 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 4.27 ではサポートされていません。

（注） このバージョン 4.27 では、CiscoSSL バージョン 1.1.1N および Apache バージョン 2.4.51 が使用されています。

セキュリティ マネージャ

Cisco Security Manager は、Cisco 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 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 [英語] 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 [英語] にアクセスしてください。

[1] Cisco Security Manager は、Transport Layer Security（TLS）およびセキュアソケットレイヤ（SSL）プロトコルに OpenSSL を使用していました。バージョン 4.13 以降、Cisco Security Manager は OpenSSL を CiscoSSL に置き換えました。

Security Manager を使用するには、サーバー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
    - サーバーソフトウェアをインストールすると、Adaptive Security Device Manager（ASDM）と Security Device Manager（SDM）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。
    - サーバーソフトウェアをインストールするときに、Cisco Prime Security Manager への相互起動ポイントもインストールします（ただし、実際のインストールではありません）。
- ASA 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。イベントビューア機能を使用することによって、ASA デバイスからのイベントを選択的にモニタリング、表示、および検査できます。

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*』[英語] に記載されています。MARS の詳細については、http://www.cisco.com/go/mars [英語] 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 ユーザーの認証と認可に 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 の統合を参照してください。ACS の詳細については、http://www.cisco.com/go/acs [英語] にアクセスしてください。

（注） Cisco Security Manager 4.21 以降では、以前の ACS サーバーの代わりに Cisco Identity Services Engine（ISE）を認証に使用できます。

- **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。Dynamic Host Configuration Protocol（DHCP）サーバーを使用する ASA デバイスは、設定（およびイメージ）のアップデートについて、Cisco Configuration Engine に通知します。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/c/en/us/support/security/security-manager/products-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 [英語] を参照してください。Configuration Engine の詳細については、http://www.cisco.com/c/en/us/products/cloud-systems-management/configuration-engine/index.html [英語] 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については、表 3-1 および表 A-1 を参照してください。

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、イベントビューアがディセーブルにされます（表 3-3 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。

翻訳について

このドキュメントは、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。