CHAPTER 3

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

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	In	Out
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	—

- **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	In	Out
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	In	Out
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	—

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.3-6）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。
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

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
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。
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.3-7）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）。 **ヒント** 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。 • Firefox 3.6.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。
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、または VMware ESXi 5.0 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することもできます。 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、米国英語と日本語のバージョンの Windows のみサポートしています。[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）。

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 ロケールは米国英語または日本語にする必要があります。
- 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。

（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、tftp、および rsh 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
esc config crmrsh 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。

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 XP（Service Pack 3） • Windows 7 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、米国英語と日本語のバージョンの Windows のみサポートしています。[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）。

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
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
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システム ソフトウェア（OS）を使用する場合）。 • Internet Explorer 8.0（この表の始めに示したシステム ソフトウェア（OS）を使用し、互換表示のみで使用する場合）。 **ヒント** 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。 • Firefox 3.6.x（この表の始めに示したシステム ソフトウェア（OS）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 1.6.0_30）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。