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、サーバー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 などのサーバー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

（注）　Security Manager はその内部操作に事前定義されたダイナミックポートを使用します。これらのポートはポートスキャナによってブロックされる可能性があり、Security Manager はこれらのプロセスを実行できません。このため、Qualys などのポートスキャナは有効にしないでください。有効にすると、Security Manager プロセスがクラッシュし、Security Manager の完全な再インストールが必要になる場合があります。

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（Basic Required Ports）]：表 1 : Security Manager サーバ上で開く必要のある基本ポート 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 *1 : Security Manager* サーバ上で開く必要のある基本ポート

コミュニケーション（Communication）	サービス	プロトコル	ポート	入力	発信
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	—
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
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
Report Manager	HTTP、HTTPS	TCP	4334	X	X
Event Manager	HTTP、HTTPS	TCP	11999	X	X

- [オプションアプリケーションに必要なポート（Ports Required By Optional Applications）]：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 2 : オプション

サーバ アプリケーションに必要なポート 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 *2:* オプション サーバ アプリケーションに必要なポート

コミュニケーション（**Communication**）	サービス	プロトコル	ポート	入力	発信
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 サーバーと ACS 間のすべての HTTP/HTTPS トラフィックを許可します。	—	X
Security Manager サーバと外部 AAA サーバ（非 ACS モードで設定可能）間	RADIUSLDAPKerberos	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 TMS サーバ間	FTP	TCP	21	—	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 (x86)\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 （オプション）高度なセキュリティライセンスを持つ Windows ファイアウォールを使用して、追加されたファイアウォールルールを確認します。

サーバの要件および推奨事項

（注） Cisco Security Manager 4.9 以降への移行中にオペレーティングシステムをアップグレードする場合は、適切な Windows ライセンスを購入する必要があります。

（注） CSM 4.28 以降、Microsoft Windows Server 2012 および 2012 R2 はサポートされません。

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）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ー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、「サーバーのインストール準備」を参照してください。

推奨サーバ

Cisco UCS C220 M3 サーバーと同等のサーバーに Security Manager をインストールすることを推奨します。

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*: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	次のいずれかが必要です。 • Microsoft Windows Server 2019 Standard（64 ビット） • Microsoft Windows Server 2019 Datacenter（64 ビット） • Microsoft Windows Server 2016 Standard（64 ビット） • Microsoft Windows Server 2016 Datacenter（64 ビット） • Microsoft Windows Server 2012 R2 Standard（64 ビット） • Microsoft Windows Server 2012 Standard（64 ビット） • Microsoft Windows Server 2012 R2 Datacenter（64 ビット） • Microsoft Windows Server 2012 Datacenter（64 ビット） 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を参照してください。 サーバーが Maria データベースと連携できるようにするには、Maria DB Drive Manager が必要です。

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 5600 シリーズ以上 • 最高の UI エクスペリエンスを提供するために、解像度が 1280 x 1024 のカラーモニターと 16 ビット色に対応したビデオカードが必要になる場合があります。 • 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。 （注） 導入モデルによって RAM は異なります。詳細については、『CSM Deployment guide』[英語] を参照してください。 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。 推奨はされませんが、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および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）。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。
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。

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 8 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（https://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html）[英語] と Veritas マニュアル [英語] 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** Security Manager は複数のネットワーク インターフェイスカードを持つことができますが、ロードバランシングのために複数の NIC をチーミングすることは推奨されません。

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 2012 または 2012 R2（Standard または Datacenter）（64 ビット）を使用している場合は、特別な考慮事項が適用されます。 ページングファイルサイズを自動的に管理することを選択した場合、Security Manager のインストールが失敗し、インストールプログラムを実行する前に仮想メモリを設定することを推奨するエラーメッセージが表示されることがあります。 Security Manager を正常にインストールするには、次の手順に従います。 **1.** [すべてのドライブのページングファイルのサイズを自動的に管理する（Automatically manage paging file size for all drives）] チェックボックスを選択解除（クリア）します。（このチェックボックスは、[コントロールパネル（Control Panel）] > [システム（System ）] > [システムの詳細設定（Advanced System Settings）] > [パフォーマンス（Performance）] > [設定（Settings）] > [詳細設定（Advanced）] タブ > [仮想メモリ（Virtual Memory）] > [変更（Change）] にあります）。 **2.** 最小サイズが 4 GB のページングファイルを作成します。ページングファイルの値は、スワップサイズに基づいて設定されます。ページング設定のデフォルト値は、それぞれ 10240 と 16384 です。 **3.** Security Manager のインストールを開始します。
Antivirus	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。 （注） NMSROOT ディレクトリとイベントフォルダをスキャンから除外する必要があります。

コンポーネント	説明
ブラウザ	次のいずれかが必要です。 • Internet Explorer 8.x、9.x、10.x、または 11.x（ただし互換表示のみ） （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 > [ツール（Tools）] > [インターネットオプション（Internet options）] > [詳細設定（Advanced）] > [セキュリティ（Security）] で、[暗号化されたページをディスクに保存しない（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。 ヒント 互換表示を Internet Explorer で使用するには、[ツール（Tools）] > [互換表示設定（Compatibility View Settings）] に移動し、[すべてのWebサイトを互換表示で表示する（Display all websites in Compatibility View）] として Security Manager サーバーを追加します。 • Firefox 15.0.1 以降（サポートおよび推奨）
Java Plug-in	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。サポートされているバージョンは、Azul JRE 1.8.0 update 322 です。
Maria DB	バージョン 4.26 以降、Security Manager は Maria DB 10.5.15 バージョンを使用します。
オプションの仮想化ソフトウェア	必要に応じて、VMware のバージョン 5 update 2 から ESXi 6.5 までの ESXi バージョンを実行しているシステム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。

コンポーネント	説明
ハイアベイラビリティ サポート（HA サポート）	次のいずれかが必要です。 • Veritas Storage Foundation 6.0.1 • Veritas Storage Foundation 6.0.2 • Veritas Storage Foundation 6.1 • Veritas Storage Foundation 7.0 • Veritas Storage Foundation 7.2 • Veritas Storage Foundation 7.4 • Veritas InfoScale 7.4.2 以降は Windows Server 2019 をサポートしています。 • Windows 2019： Veritas Storage Foundation for Windows Version：7.4.2 • Windows 2016： Veritas Storage Foundation for Windows Version：7.4

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）。

ヒント 詳細な手順については、「Windows の既定のユーザーテンプレートのロケールを米国英語に設定する方法」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。現在のユーザーは、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 サーバー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、サーバーのオペレーティングシステム内の [地域と言語のオプション（Regional and Language Options）] 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。

Security Manager を正常にインストールするには、次の [地域と言語のオプション（Regional and Language Options）] と関連設定に従う必要があります。

- 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。
- 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。
- 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。
- localname がサポートされていることを確認します。次に、英語 (米国) の例を示します。

\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』[英語] 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 4 : クライアントの要件と制約事項 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。

注意 競合検出では、CSM クライアントで大量のメモリサイズが使用されます。メモリ使用量は、ポリシー内のルールの数または使用されるデバイスによって異なります。必要な場合にのみ、クライアント UI で競合検出機能を有効にします。システム RAM サイズに基づいて、CSM クライアントの LAX ファイルに十分なメモリが設定されていることを確認します。デフォルトでは 2 GB です。たとえば、マシンの RAM サイズが 8 GB の場合は 4 GB、マシンの RAM が 16 GB の場合は 8 GB で LAX ファイルを構成してみてください。ただし、環境の要件に合わせてクライアント LAX ファイルを設定することを強くお勧めします。

ルールとデバイスの要件の数に基づいて、次のパラメータを使用します。

```
#   LAX.NL.JAVA.OPTION.JAVA.HEAP.SIZE.MAX
#   -------------------------------------
#   2420m
```

lax.nl.java.option.java.heap.size.max=2420m

表 *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

コンポーネント	要件
オペレーティング システム	次のいずれかが必要です。 • Microsoft Windows Server 2019 Standard（64 ビット） • Microsoft Windows Server 2019 Datacenter（64 ビット） • Microsoft Windows Server 2016 Standard（64 ビット） • Microsoft Windows Server 2016 Datacenter（64 ビット） • Microsoft Windows 7 • Microsoft Windows 8（64 ビットおよび 32 ビット） • Microsoft Windows 8.1 Enterprise Edition（64 ビットおよび 32 ビット） • Microsoft Windows 10（64 ビットおよび 32 ビット） • Microsoft Windows Server 2012 R2 Standard（64 ビット） • Microsoft Windows Server 2012 Standard（64 ビット） • Microsoft Windows Server 2012 R2 Datacenter（64 ビット） • Microsoft Windows Server 2012 Datacenter（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）。
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 （注） 競合検出を有効にすると、最小メモリ要件が増加します。この場合、クライアントの lax ファイルでメモリ領域を必要な値に増やします。 （注） 導入モデルに応じてRAMサイズを増やす必要があります。詳細については、『CSM Deployment guide』[英語] を参照してください。

コンポーネント	要件
仮想メモリ（ページング ファイル）	512 MB **注意**： [すべてのドライブのページングファイルのサイズを自動的に管理する（Automatically manage paging file size for all drives）] チェックボックスを選択解除（クリア）する必要があります（このチェックボックスは、[コントロールパネル（Control Panel）] > [システム（System ）] > [システムの詳細設定（Advanced System Settings）] > [パフォーマンス（Performance）] > [設定（Settings）] > [詳細設定（Advanced）] タブ > [仮想メモリ（Virtual Memory）] > [変更（Change）] にあります）。ページングファイルの値は、スワップサイズに基づいて設定されます。ページング設定のデフォルト値は、それぞれ 10240 と 16384 です。 **注意**： Windows Server 2012 または 2012 R2（Standard または Datacenter）（64 ビット）を使用している場合は、特別な考慮事項が適用されます。サーバーに 2 つの独立したパーティション（C: と F: など）がある場合、この考慮事項に注意する必要があります。 次の手順に従うと、**インストールは失敗します**。 **1.** [すべてのドライブのページングファイルのサイズを自動的に管理する（Automatically manage paging file size for all drives）] をオフ（チェックボックスをクリア）にする必要があります。 **2.** 非システムパーティション（F: など）で、ページングファイルを作成します。 **3.** システムパーティション（C: など）で、ページングファイルサイズを自動的に管理するオプションを保持します。 **4.** Security Manager のインストールを開始します。 インストーラは、システム管理のページングファイルサイズを使用しないことを示すエラーメッセージを表示して終了します。
ハード ドライブ スペース	10 GB の空きディスク スペース

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 8.x、9.x、10.x、または 11.x（ただし互換表示のみ） （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 > [ツール（Tools）] > [インターネットオプション（Internet options）] > [詳細設定（Advanced）] > [セキュリティ（Security）] で、[暗号化されたページをディスクに保存しない（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。 ヒント 互換表示を使用するには、Internet Explorer 8 または 9 で、[ツール（Tools）] > [互換表示設定（Compatibility View Settings）] に移動し、[すべてのWebサイトを互換表示で表示する（Display all websites in Compatibility View）] として Security Manager サーバーを追加します。 • Firefox 15.0.1 以降（サポートおよび推奨）
Java Plug-in	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。サポートされているバージョンは、Azul JRE 1.8.0 update 322 です。 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（Azul JRE 1.8.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、管理者ユーザーのみすべての機能を使用できます。

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。