Cisco Security Manager 4.27 展開計画ガイド

初版：2023 年 9 月 7 日

はじめに

本書では、Cisco Security Manager 4.27 の展開計画に関するガイドラインについて説明します。このマニュアルには、推奨されるサーバーハードウェア、クライアントハードウェア、リファレンスネットワークに基づいたサイジングおよびソフトウェア、Cisco Security Manager、Cisco Security Manager サーバーの高度なチューニングオプションに含まれているアプリケーションセットの展開オプションとライセンシングに関する内容が含まれています。Cisco Security Manager のソフトウェア機能の詳細については、http://www.cisco.com/go/csmanager の製品マニュアル [英語] を参照してください。

このマニュアルは、『*User Guide for Cisco Security Manager 4.27*』[英語] や『*Installation Guide for Cisco Security Manager 4.27*』[英語] など、Cisco Security Manager の他のユーザーマニュアルを補足するものです。

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

Cisco Security Manager 4.27 アプリケーション

各 Cisco Security Manager 4.27 インストールには、6 つの主要アプリケーションとモバイルデバイス用に設計された 1 つのアプリケーションがあります。

- Configuration Manager
- イベントビューア
- Report Manager

- Health and Performance Monitor
- Image Manager
- ダッシュボード
- CSM Mobile

Configuration Manager

Configuration Manager を使用すると、250 以上のさまざまなタイプおよびモデルの Cisco セキュリティデバイス上でセキュリティポリシーを集中管理できます。Cisco Security Manager は、ASA デバイス全体で、ファイアウォールおよび VPN（サイト間、リモートアクセス、および SSL）サービスの統合プロビジョニングをサポートします。

Cisco Security Manager でサポートされるデバイスおよび OS バージョンの一覧については、Cisco.com で『Supported Devices and Software Versions for Cisco Security Manager』[英語] を参照してください。

イベントビューア

高パフォーマンスで、使い勝手の良い統合イベントビューアを使用すると、ASA デバイスからイベントを集中監視し、関連する設定ポリシーに相互に関連付けることができます。このことは、問題の特定や、設定のトラブルシューティングに役立ちます。さらに、Configuration Manager を使用して、設定を調整し、展開することができます。イベントビューアは、Cisco ASA デバイスのイベント管理をサポートします。

プライマリ イベント データ ストアだけではなく、拡張イベントデータストアにイベントをコピーして格納できます。拡張イベントデータストアは、大量のイベントのバックアップおよびアーカイブに使用できます。これは、Event Viewer がプライマリ イベント データ ストアと拡張イベントデータストアの両方からイベントデータを収集できる場合、イベントの履歴のレビューおよび分析に役立ちます。拡張イベントデータストアは、Cisco Security Manager の管理設定内のイベント管理でイネーブルにできます。

（注） 4.17 以降、Cisco Security Manager イベントビューアは非管理インターフェイスから生成された syslog の表示もサポートしています。

サポートされているプラットフォームと詳細については、Cisco.com で『*User Guide for Cisco Security Manager 4.27*』の「Monitoring, Reporting, and Diagnostics」[英語] および「*Supported Devices and Software Versions for Cisco Security Manager 4.27*」[英語] を参照してください。

Report Manager

この統合型の Report Manager アプリケーションでは、ASA および Remote Access VPN レポートの生成とスケジュール作成を実行できます。ASA のレポートは、イベントビューアで収集されたイベントを集約することによって作成されます。Security レポートは、管理対象デバイスによって報告されたネットワークの使用状況やセキュリティの問題を効率的に監視、追跡、およ

び監査できます。ユーザーは、Report Manager を使用して、Cisco ASA デバイスのレポートを作成およびカスタマイズできます。

サポートされているプラットフォームと詳細については、Cisco.com で『*User Guide for Cisco Security Manager 4.27*』の「Monitoring, Reporting, and Diagnostics」[英語] および「*Supported Devices and Software Versions for Cisco Security Manager 4.27*」[英語] を参照してください。

Health and Performance Monitor

Health and Performance Monitor には、次の機能があります。

- ASA IPS デバイスの監視機能の提供
- 重要なメトリックのトレンドグラフの提供
- 1 つのビュー内での、統合された稼働状態、アラート、およびメトリック値情報のサマリーパネルの提供
- さまざまなモニタリングパラメータのアラートメカニズムの提供
- 事前定義された一連のモニタリングビューの提供
- ユーザへのカスタムモニタリングビューの作成、編集、および削除の許可

Image Manager

Image Manager は、ASA デバイス用の完全なイメージ管理を提供します。特に、次の手順を実行することで、ASA イメージ アップグレード プロセスのさまざまな段階でユーザーを支援します。

- さまざまなタイプおよびバージョンのイメージのリポジトリのダウンロードおよび維持
- イメージの評価
- これらのイメージをデバイスに対してアップグレードする場合の影響の分析（分析にはデバイス構成へのアップグレードの影響が含まれます）
- アップグレードの準備と計画
- ダウンタイムを最小限にする、組み込みの十分なフォールバックとリカバリメカニズムによる、信頼性があり安定したデバイスのアップグレード方法の提供

ダッシュボード

ダッシュボードは、FW タスクをより便利にする Cisco Security Manager で設定可能な起動点です。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成したり、すべてのダッシュボードをカスタマイズしたりすることができます。ダッシュボードを使用することによって、Cisco Security Manager の他のいくつかの領域にある、Report Manager、Health and Performance Monitor および IP Intelligence 設定などの多くのタクスを 1 箇所で実行できます。

CSM Mobile

CSM Mobile では、モバイルデバイスからのデバイスのヘルスに関するサマリー情報にアクセスできます。この方法で入手できる情報は、Device Health Summary ウィジェットで入手可能な情報と同じ、HPM によって生成される現在の重大度が低いまたは中程度のアクティブなアラートになります。アラートは、Alert-Description、Predefined-Category、Device または Alert Technology 別にグループ化できます。

CSM Mobile のプリンシパルユーザは、Apple iPad、Apple iPhone、Google Chrome ブラウザ、Apple Safari ブラウザを使用するユーザであることが想定されています。

Syslog リレー

Cisco Security Manager サーバーで受信したイベントに加えて、最大 2 台の外部/リモートコントローラ（syslog ホスト）にイベントを転送できます。この syslog リレー機能は、UDP syslog プロトコルを使用して受信したメッセージを別の Syslog ホストに転送します。

Retain the original source address of the message

この機能は、メッセージの元の送信元 IP アドレスを維持するオプションを提供します。これは、ユーザがリモートコントローラの送信元 IP アドレスで受信したイベントを表示する場合です。これはデフォルトの設定です。

Use CSM server IP address as source IP address

このオプションがコンフィギュレーション ファイルでイネーブルの場合、Cisco Security Manager サーバーから転送されたすべての syslog メッセージには、syslog メッセージの送信元 IP アドレスとして Cisco Security Manager サーバーの IP アドレスが含まれます。

（注） 4.13 以降、Cisco Security Manager はイベントビューアで IPv6 を介した syslog をサポートします。ただし、syslog リレーは IPv6 を介した syslog ではサポートされていません。

構成および設定の詳細については、Cisco.com で『*User Guide for Cisco Security Manager 4.27*』[英語] を参照してください。

注意 IP アドレスのスプーフィングはネットワークポリシーで許可されている場合にのみ実現できます。

（注） 4.17 以降、CSM イベントビューアは非管理インターフェイスから生成された syslog の表示もサポートしています。ただし、syslog リレー機能は非管理インターフェイスの syslog ではサポートされません。

Common Services 4.2.2

CiscoWorks Common Services 4.2.2（Common Services）は、Security Manager 4.27 が動作するために必要です。Common Services は、Cisco Security Manager 4.27 のインストールを選択するとデフォルトでインストールされます。

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 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、Cisco Security Manager のインストールに付属している Common Services のマニュアルを参照してください。これを行うには、Cisco Security Manager をインストールしたサーバーにログオンし、[Cisco Security Manager（Cisco Security Manager）] アイコンをダブルクリックしてログオンします。次に、[サーバー管理（Server Administration）] をクリックして、[ヘルプ（Help）] をクリックします。

共通サービスを使用するローカル RBAC

Cisco Security Manager 4.3 よりも前は、Cisco Secure ACS を使用する重要なメリットは、（1）特殊な権限セット（特定のポリシータイプの設定だけをユーザーに許可する場合など）を使用して非常に粒度の高いユーザーロールを作成できることと、（2）ネットワーク デバイス グループ（NDG）を設定することによって特定のデバイスにユーザーを制限できることでした。このような粒度の高い特権（効率的な「ロールベース アクセス コントロール」（RBAC））は、Cisco Secure ACS を使用していない限り、Cisco Security Manager 4.2 以前のバージョンでは利用できませんでした。このような粒度の高い特権（RBAC）は、ACS を使用せずにローカル RBAC を利用できる Common Services 4.0 以降を使用するため、Cisco Security Manager 4.3 ～ 4.19 バージョンで利用可能です。詳細については、『Installation Guide for Cisco Security Manager 4.20』[英語] を参照してください。

（注） バージョン 4.21 以降、Cisco Security Manager は Cisco Identity Services Engine（ISE）を介した TACACS+ 認証のみをサポートします。これは、ACS のサポートが終了しているためです。

関連アプリケーション

Cisco 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。

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

ハードウェアおよびソフトウェアの最小要件

各 Cisco Security Manager サーバーのインストールには、Configuration Manager、イベントビューア、Report Manager、Health and Performance Monitor、Image Manager とダッシュボード用の専用の物理サーバーまたは仮想マシンが 1 台必要です。

表 1 : サーバの最小ハードウェアとソフトウェア は、Cisco Security Manager サーバーソフトウェア、および他のオプションのモジュールをインストールする場合のハードウェアとソフトウェアの最小仕様を示しています。Cisco Security Manager ソフトウェアは、最小仕様を備えたシステムにインストールできますが、この場合のパフォーマンスと容量は、より小規模な展開（最大25のデバイスを管理）に制限されます。より大規模な展開については、推奨されるハードウェアおよびソフトウェア仕様 （12 ページ）の項で推奨されている仕様で物理サーバを使用する必要があります。

表 *1:* サーバの最小ハードウェアとソフトウェア

サーバの最小ハードウェア	
推奨サーバ	Cisco UCS C220 M3 の同等品
CPU	1 x Intel Xeon Four-core 5600 シリーズこの Four-core（qu 最小です。コア数が多くなると、パフォーマンスがさら

サーバの最小ハードウェア	
メモリ（RAM）	Cisco Security Manager のすべての機能を使用するに GB が必要です。これよりもメモリ容量が少ないと 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が使用できる RA 満であると、Event Viewer および Report Manager が 効化されます。 OS が使用できるメモリが 8 ～ 12 GB の場合は、Ev Report Manager を使用しないと判断し、オフにする のようなシステムでは、コンフィギュレーション管 できます。 推奨はできませんが、インストールの完了後に Cis クライアントからローメモリシステムに対してイベ Report Manager をイネーブルにできます（[ツール Managerの管理（Security Manager Administration）]>[Management）] を選択します）。ローメモリシステ および Report Manager をイネーブルにすると、アプ パフォーマンスに深刻な影響が及ぶ可能性があるこ い。 （注） Windows タスクマネージャによって表示 モリ使用率は、設定操作中に 99 % になる これは問題を示しているわけではなく、 Manager のすべてのプロセスと機能がそ られたメモリを使用または割り当てるた

サーバの最小ハードウェア	
ハードドライブスペース	

サーバの最小ハードウェア	
	必要なディスク領域の確保に適した HDD の組み合 を使用します。 • 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（Cisco Security Manager）パ 150 GB を推奨します。Cisco Security Manager の に必要な最小空きディスク領域は 7 GB です。 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 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 場合、上記のアプリケーション パーテ の他のイベント ストア パーティションに あります。詳細については、該当する C ハイ アベイラビリティ マニュアル（http c/en/us/support/security/security-manager/ products-installation-guides-list.html）[英語 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 て 1.0 TB の追加領域：Event Viewer を使用する 件です。この独立したパーティションは、直接 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 み必要な条件です。イベント記録機能では、（ より）プライマリストレージの容量を超えるロ になると、セカンダリのイベントストレージが セカンダリイベントストアには、プライマリス たサイズよりも大きいサイズが要求されます。 記録を使用するには、1.0 TB 以上の追加のディ す。プライマリとセカンダリのイベントストア に配置できますが、最適なパフォーマンスを実 イマリ ストア パーティションは直接接続スト 作成することを推奨します。 パフォーマンス向上のために、RAID 10 の使用を推 ば、RAID 5 も使用できます。シーケンシャルな動 とんどのケースではそうなりません）、書き込みポ クに設定します。そうでない場合は、書き込みポリ ルーに設定します。書き込みポリシーをライトスル フォーマンスも向上します。 ヒント

サーバの最小ハードウェア	
	連続 10,000 イベント/秒（EPS）の場合は、1 日に約 86 スク スペースが消費されます。イベントストア（プラ リ）に割り当てられたディスク領域の 90 % がいっぱい ログロールオーバーが発生します。ディスクのサイズ ロールオーバーの発生が早くなります。予想 EPS レー バー要件に基づいて、イベント管理の使用時に最小デ 増減できます。
サポートされるデバイス	最大 25
ネットワークアダプタ	1 Gbps
サーバの最小ソフトウェア	
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 • Microsoft Windows Server 2016 Standard（64 ビット • Microsoft Windows Server 2016 Datacenter（64 ビッ • Microsoft Windows Server 2012 R2 Standard（64 ビッ • Microsoft Windows Server 2012 Standard（64 ビット • Microsoft Windows Server 2012 R2 Datacenter（64 ビ • Microsoft Windows Server 2012 Datacenter（64 ビッ サポートされている言語は英語と日本語のみです。

表 2 : クライアントの最小ハードウェアとソフトウェア は、Cisco Security Manager クライアントソフトウェアのインストールのためのハードウェアとソフトウェアの最小仕様を示しています。Cisco Security Manager クライアントソフトウェアは専用のマシンにインストールすることを推奨します。

表 *2:* クライアントの最小ハードウェアとソフトウェア

クライアントの最小ハードウェア	
[CPU（CPU）]	デュアルコア 2.0 GHz 以上

クライアントの最小ハードウェア	
[メモリ（Memory）]	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
[HDD（HDD）]	10 GB の空き容量
[ディスプレイ（ディスプレイ）]	1280 X 1024
[ネットワークアダプタ（Network adapter）]	1 Gbps
クライアントの最小ソフトウェア	
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 • Microsoft Windows Server 2019 Datacenter（64 • Microsoft Windows Server 2016 Standard（64 ビ • Microsoft Windows Server 2016 Datacenter（64 • Microsoft Windows 7 • Microsoft Windows 8.1 Enterprise Edition（64 ビット） • Microsoft Windows 10（64 ビットおよび 32 ビ • Microsoft Windows Server 2012 R2 Standard（6 • Microsoft Windows Server 2012 Standard（64 ビ • Microsoft Windows Server 2012 R2 Datacenter（ • Microsoft Windows Server 2012 Datacenter（64 • Windows 2008 R2 Enterprise Server SP1（64 ビ Security Manager は、米国英語と日本語のバージョ ポートしています。[Start] メニューから、Window ルを開いて、地域と言語を設定するパネルを開き を設定します（日本語バージョンの Windows では ポートされません）。

クライアントの最小ハードウェア	
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（たた （注） クライアントをダウンロードするために I 意のバージョン）を使用する場合は、次の どうかを確認します。Internet Explorer > [> [インターネットオプション（Internet op 定（Advanced）] > [セキュリティ（Securi されたページをディスクに保存しない（D pages to disk）] チェックボックスをオフに 定が正しくない（つまり、チェックボック クライアントをダウンロードしようとす • Firefox 15.0.1 以降（サポートおよび推奨）

仮想マシンのハードウェアおよびソフトウェア要件

仮想マシンのハードウェア要件およびソフトウェア要件については、表 3 : 推奨される VMware ESXi バージョン別 OS のサポート：推奨される VMware ESXi バージョン別 OS のサポートを参照してください。

推奨されるハードウェアおよびソフトウェア仕様

単一プロセッサ（コア）サーバーから複数プロセッサ（コア）サーバーへ移行する場合には、Cisco Security Manager を使用するとパフォーマンスの改善が見られます。最適なパフォーマンスを得るために、適切なハードウェアとソフトウェアの仕様を使用することを推奨します。また、将来の拡張用にサーバのサイジングもお勧めします。

最良のパフォーマンスを得るためには、最小要件として、2.66 MHz インテル Xeon クワッドコアプロセッサ（ハイパースレッディング機能あり）以上を備えた Cisco Security Manager サーバーが推奨されます。イベント管理を使用する場合には、Cisco Security Manager アプリケーションに対して専用のハードディスクまたはストレージボリュームを用意すること、およびイベントストレージに対して専用のディスクまたはボリュームを用意することを強くお勧めします。Cisco Security Manager クライアントシステムでは、ハードウェアおよびソフトウェアの最小要件 （6 ページ）の項に記載されている最小のハードウェア仕様を使用できます。

次の仕様は、さまざまな規模の展開に対して、Cisco Security Manager サーバーで推奨される仕様を示しています。

- オペレーティングシステム別 VM サポート （13 ページ）
- VMware ESXi 5.1U2 および ESXi 7.0 までの VMware ESXi バージョンを使用した小規模な展開 （13 ページ）

- Hyper-V を使用した小規模な展開 （21 ページ）
- VMware ESXi 5.1U2 および ESXi 7.0 までの VMware ESXi バージョンを使用した中規模な企業での展開 （25 ページ）
- 中規模な企業での展開 （30 ページ）
- 大規模な企業での展開 （33 ページ）
- 大規模な小売店舗での展開 （38 ページ）

これらの仕様は、デバイス数に基づいてこのような展開をサポートするための、適切なハードウェアおよびソフトウェアの一般的なガイドラインです。このマニュアルの導入シナリオ （42 ページ） で説明している他の要因によっては、パフォーマンスの結果が異なる場合があります。Cisco Security Manager に対するこれらのハードウェアおよびソフトウェア要件は、Cisco Security Manager を新しくインストールする場合も、Cisco Security Manager の以前のバージョンからバージョン 4.27 にアップグレードする場合も同じです。

オペレーティングシステム別 VM サポート

表 3 : 推奨される VMware ESXi バージョン別 OS のサポート に、推奨される VMware ESXi バージョン別 OS のサポートを示します。

表 *3* : 推奨される *VMware ESXi* バージョン別 *OS* のサポート

	ESXi バージョン					
ゲスト OS	**4**	**4.1**	**5**	**5.1**	**5 アップデート 2**	**5.1 アップデート 2**
Windows Server 2019	×	×	×	×	×	×
Windows Server 2016	×	×	×	×	×	×
Windows Server 2012 R2	×	×	×	×	対応	対応
Windows Server 2012	×	×	×	×	対応	対応

VMware ESXi 5.1U2 および ESXi 7.0 までの VMware ESXi バージョンを使用した小規模な展開

VMware ESX 5.1U2 および ESXi 7.0 までの VMware ESXi バージョンを使用した小規模な展開で推奨される Cisco Security Manager の仕様は、表 4 : VMware ESXi 5.1U2 および ESXi 7.0 までの VMware ESXi バージョンを使用した小規模な展開 に示してあります。

表 *4 : VMware ESXi 5.1U2* および *ESXi 7.0* までの *VMware ESXi* バージョンを使用した小規模な展開

（注）	**VMware** のパフォーマンスは、同じホスト システム上の他の **VM** によって生成される負荷によ そのため、これらの**VM**のサイジングの数字は、他の**VM**による大きな負荷が掛かっていない になります。
推奨されるホストサーバ	**Cisco UCS C220 M3** の同等品
仮想 CPU	6 vCPU vCPU を増やすと、パフォーマンスが向
メモリ（RAM）	Cisco Security Manager のすべての機能を使用す GB が必要です。これよりもメモリ容量が少な 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が使用できる 満であると、Event Viewer および Report Manag 効化されます。 OS が使用できるメモリが 8 ～ 12 GB の場合は Report Manager を使用しないと判断し、オフに のようなシステムでは、コンフィギュレーショ できます。 推奨はできませんが、インストールの完了後に クライアントからローメモリシステムに対して Report Manager をイネーブルにできます（[ツー Managerの管理（Security Manager Administration） Management）] を選択します）。ローメモリシ および Report Manager をイネーブルにすると、 パフォーマンスに深刻な影響が及ぶ可能性があ い。 （注） Windows タスクマネージャによって モリ使用率は、設定操作中に 99 % に これは問題を示しているわけではな Manager のすべてのプロセスと機能 られたメモリを使用または割り当て

（注）	**VMware** のパフォーマンスは、同じホスト システム上の他の **VM** によって生成される負荷に そのため、これらの**VM**のサイジングの数字は、他の**VM**による大きな負荷が掛かっていな になります。
推奨されるホストサーバ	**Cisco UCS C220 M3** の同等品
ハードドライブスペース	

（注）	**VMware** のパフォーマンスは、同じホスト システム上の他の **VM** によって生成される負荷によ そのため、これらの**VM**のサイジングの数字は、他の**VM**による大きな負荷が掛かっていない になります。
推奨されるホストサーバ	**Cisco UCS C220 M3** の同等品
	必要なディスク領域の確保に適した HDD の組 を使用します。 • OS パーティション用に 100 GB を推奨し • アプリケーション（Cisco Security Manager 150 GB を推奨します。Cisco Security Mana に必要な最小空きディスク領域は 7GB で 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 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 場合、上記のアプリケーション パ の他のイベント ストア パーティシ あります。詳細については、該当す ハイアベイラビリティ マニュアル en/us/support/security/security-manage products-installation-guides-list.html） 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 て 1.0 TB の追加領域：Event Viewer を使用 件です。この独立したパーティションは、 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 み必要な条件です。イベント記録機能では より）プライマリストレージの容量を超え になると、セカンダリのイベントストレー セカンダリイベントストアには、プライマ たサイズよりも大きいサイズが要求されま 記録を使用するには、1.0 TB 以上の追加の す。プライマリとセカンダリのイベントス に配置できますが、最適なパフォーマンス イマリ ストア パーティションは直接接続 作成することを推奨します。 パフォーマンス向上のために、RAID 10 の使用 ば、RAID 5 も使用できます。シーケンシャル とんどのケースではそうなりません）、書き込 クに設定します。そうでない場合は、書き込み

（注）	**VMware** のパフォーマンスは、同じホスト システム上の他の **VM** によって生成される負荷に そのため、これらの**VM**のサイジングの数字は、他の**VM**による大きな負荷が掛かっていな になります。
推奨されるホストサーバ	**Cisco UCS C220 M3** の同等品
	スルーに設定します。書き込みポリシーを パフォーマンスも向上します。 **ヒント** 連続 10,000 イベント/秒（EPS）の場合は、 スク スペースが消費されます。イベントス リ）に割り当てられたディスク領域の 90 % ログ ロールオーバーが発生します。ディス ロールオーバーの発生が早くなります。予 バー要件に基づいて、イベント管理の使用時 減できます。
ホストサーバの HDD RAID	VM 内の RAID は、基礎となるホストシス 仮想化されたファイルシステムが使用され また、ソフトウェアベースの RAID は、VM ません。詳細については、VMware, Inc. 発行 ださい。
ネットワークアダプタ	1 Gbps
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 • Microsoft Windows Server 2019 Datacente • Microsoft Windows Server 2016 Standard • Microsoft Windows Server 2016 Datacente • Microsoft Windows Server 2012 R2 Stand • Microsoft Windows Server 2012 Standard • Microsoft Windows Server 2012 R2 Datac • Microsoft Windows Server 2012 Datacente
推奨されるサイジング	
デバイスの最大数	最大 100 台
サポートされる最大累積 EPS	ASA syslog の 1 秒あたり 5,000 件のイベン

（注）	**VMware** のパフォーマンスは、同じホスト システム上の他の **VM** によって生成される負荷によ そのため、これらの**VM**のサイジングの数字は、他の**VM**による大きな負荷が掛かっていない になります。
推奨されるホストサーバ	**Cisco UCS C220 M3** の同等品
最大同時利用者数	同時利用者は多くても 2 人（コンフィギュレー 人と、イベント画面およびレポーティング画面 人）

小規模な企業での展開

表 5 : 小規模な企業での展開 に、小規模な企業での展開用に推奨される Cisco Security Manager サーバーの仕様を示します。

表 *5:* 小規模な企業での展開

推奨サーバ	**Cisco UCS C220 M3** の同等品
[CPU（CPU）]	1 x Hex Core（X5670 または同等シリーズを推奨）
メモリ（RAM）	Cisco Security Manager のすべての機能を使用するに GB が必要です。これよりもメモリ容量が少ないと、 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 満の場合は、イベント管理と Report Manager がイン 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 ト管理を使用しないことを前提として、それらを無効 ます。そのようなシステムでは、コンフィギュレーシ ることができます。 推奨はできませんが、インストールの完了後に Cisc クライアントからローメモリシステムに対してイベン 管理をイネーブルにできます（[ツール（Tools）] > [管理（Security Manager Administration）] > [イベント Management）] を選択します）。ローメモリシステム とレポート管理をイネーブルにすると、アプリケーシ マンスに深刻な影響が及ぶ可能性があることに注意 （注） Windows タスク マネージャによって表示 モリ使用率は、設定操作中に 99 % になる これは問題を示しているわけではなく、 Manager のすべてのプロセスと機能がそ られたメモリを使用または割り当てるた

推奨サーバ	Cisco UCS C220 M3 の同等品
ハードドライブスペース	

推奨サーバ	Cisco UCS C220 M3 の同等品
	必要なディスク領域の確保に適した HDD の組み合わ を使用します。 • 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（Cisco Security Manager）パー 150 GB を推奨します。Cisco Security Manager の に必要な最小空きディスク領域は 7 GB です。こ 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 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 場合、上記のアプリケーション パーティ の他のイベント ストア パーティションは あります。詳細については、該当する Cis ハイアベイラビリティ マニュアル（https en/us/support/security/security-manager/ products-installation-guides-list.html）[英語 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 て 1.0 TB の追加領域：Event Viewer を使用する場 件です。この独立したパーティションは、直接接 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 み必要な条件です。イベント記録機能では、（長 より）プライマリストレージの容量を超えるロ 要になると、セカンダリのイベント ストレージ このセカンダリイベントストアには、プライマリ されたサイズよりも大きいサイズが要求されます ント記録を使用するには、1.0 TB 以上の追加のデ です。プライマリとセカンダリのイベント スト 上に配置できますが、最適なパフォーマンスを実 ライマリ ストア パーティションは直接接続スト に作成することを推奨します。 パフォーマンス向上のために、RAID 10 の使用を推奨 ば、RAID 5 も使用できます。シーケンシャルな動作 とんどのケースではそうなりません）、書き込みポリ クに設定します。そうでない場合は、書き込みポリシ ルーに設定します。書き込みポリシーをライトスルー フォーマンスも向上します。 ヒント

推奨サーバ	Cisco UCS C220 M3 の同等品
	連続 10,000 イベント/秒（EPS）の場合は、1 日に スク スペースが消費されます。イベントストア リ）に割り当てられたディスク領域の 90 % がい ログロールオーバーが発生します。ディスクのサ ロールオーバーの発生が早くなります。予想 EPS バー要件に基づいて、イベント管理の使用時に最 減できます。
[ネットワークアダプタ（Network adapter）]	1 Gbps
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 • Microsoft Windows Server 2019 Datacenter（64 • Microsoft Windows Server 2016 Standard（64 ビ • Microsoft Windows Server 2016 Datacenter（64 • Microsoft Windows Server 2012 R2 Standard（6 • Microsoft Windows Server 2012 Standard（64 ビ • Microsoft Windows Server 2012 R2 Datacenter • Microsoft Windows Server 2012 Datacenter（64
推奨されるサイジング	
デバイスの最大数	最大 100 台
サポートされる最大累積 EPS	ASA syslog の 1 秒あたり 5,000 件のイベント
最大同時利用者数	同時利用者は多くても 4 人（コンフィギュレーシ 人と、イベント画面およびレポーティング画面を 人）

Hyper-V を使用した小規模な展開

推奨サーバ	Cisco UCS C220 M3 の同等品
Hyper-V Server Core	Hyper-V Server 2016 または Hyper-V Server 2012 R2
[仮想 CPU（Virtual CPU）]	6 vCPU vCPU を増やすと、パフォーマンスが向上し

推奨サーバ	Cisco UCS C220 M3 の同等品
メモリ（RAM）	Cisco Security Manager のすべての機能を使用するには、 GB が必要です。これよりもメモリ容量が少ないと、イ 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 満の場合は、イベント管理と Report Manager がインス 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 ト管理を使用しないことを前提として、それらを無効に ます。そのようなシステムでは、コンフィギュレーショ ることができます。 推奨はできませんが、インストールの完了後に Cisco S 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 管理をイネーブルにできます（[ツール（Tools）] > [Se 管理（Security Manager Administration）] > [イベント管 Management）] を選択します）。ロー メモリ システム 理とレポート管理をイネーブルにすると、アプリケー フォーマンスに深刻な影響が及ぶ可能性があることに い。 （注） Windows タスクマネージャによって表示さ モリ使用率は、設定操作中に 99 % になる場 これは問題を示しているわけではなく、Cis Manager のすべてのプロセスと機能がそれ られたメモリを使用または割り当てるため

推奨サーバ	Cisco UCS C220 M3 の同等品
ハードドライブスペース	

推奨サーバ	Cisco UCS C220 M3 の同等品
	必要なディスク領域の確保に適した HDD の組み合わせ を使用します。 • 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（Cisco Security Manager）パーテ 150 GB を推奨します。Cisco Security Manager のイ に必要な最小空きディスク領域は 7 GB です。この 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 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 Ver 場合、上記のアプリケーション パーティシ の他のイベント ストア パーティションは関 あります。詳細については、該当する Cisco ハイ アベイラビリティ マニュアル（https:// c/en/us/support/security/security-manager/ products-installation-guides-list.html）[英語] と 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 て 1.0 TB の追加領域：Event Viewer を使用する場合 件です。この独立したパーティションは、直接接続 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 み必要な条件です。イベント記録機能では、（長期 より）プライマリストレージの容量を超えるログス になると、セカンダリのイベントストレージが作成 セカンダリイベントストアには、プライマリストレ たサイズよりも大きいサイズが要求されます。その 記録を使用するには、1.0 TB 以上の追加のディス す。プライマリとセカンダリのイベントストアは同 に配置できますが、最適なパフォーマンスを実現す イマリ ストア パーティションは直接接続ストレー 作成することを推奨します。 パフォーマンス向上のために、RAID 10 の使用を推奨し ば、RAID 5 も使用できます。シーケンシャルな動作を とんどのケースではそうなりません）、書き込みポリシ クに設定します。そうでない場合は、書き込みポリシー ルーに設定します。書き込みポリシーをライトスルーに フォーマンスも向上します。 ヒント

推奨サーバ	Cisco UCS C220 M3 の同等品
	連続 10,000 イベント/秒（EPS）の場合は、1 日に約 スクスペースが消費されます。イベントストア（フ リ）に割り当てられたディスク領域の 90 % がいっ ログロールオーバーが発生します。ディスクのサイ ロールオーバーの発生が早くなります。予想 EPS レ バー要件に基づいて、イベント管理の使用時に最小 増減できます。
[ネットワークアダプタ（Network adapter）]	1 Gbps
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 • Microsoft Windows Server 2019 Datacenter（64 ビ • Microsoft Windows Server 2016 Standard（64 ビッ • Microsoft Windows Server 2016 Datacenter（64 ビ • Microsoft Windows Server 2012 R2 Standard（64 • Microsoft Windows Server 2012 Standard（64 ビッ • Microsoft Windows Server 2012 R2 Datacenter（64 • Microsoft Windows Server 2012 Datacenter（64 ビ
推奨されるサイジング	
デバイスの最大数	最大 100 台
サポートされる最大累積 EPS	ASA syslog の 1 秒あたり 5,000 件のイベント
最大同時利用者数	同時利用者は多くても 4 人（コンフィギュレーショ 人と、イベント画面およびレポーティング画面を使 人）

VMware ESXi 5.1U2 および ESXi 7.0 までの VMware ESXi バージョンを使用した中規模な企業での展開

VMware ESX 5.1U2 および ESXi 7.0 までの VMware ESXi バージョンを使用した中規模な展開で推奨される Cisco Security Manager の仕様は、表 6 : VMware ESXi 5.1U2 および ESXi 7.0 までの VMware ESXi バージョンを使用した中規模な展開 に示してあります。

表 *6 : VMware ESXi 5.1U2* および *ESXi 7.0* までの *VMware ESXi* バージョンを使用した中規模な展開

（注） **VMware** のパフォーマンスは、同じホスト システム上の他の **VM** によって生成される負荷によ す。そのため、これらの **VM** のサイジングの数字は、他の **VM** による大きな負荷が掛かってい づいた数字になります。	
推奨されるホスト サーバ	**Cisco UCS C220 M3** の同等品
仮想 CPU	12 vCPU。vCPU を増やすと、パフォーマンスが向上
メモリ（RAM）	• Configuration Manager のみを使用する場合は 16 • すべての機能を使用する場合は 24 GB （注） Windows タスクマネージャによって表示 モリ使用率は、設定操作中に 99 % になる これは問題を示しているわけではなく、 Manager のすべてのプロセスと機能がそ られたメモリを使用または割り当てるた

（注） **VMware** のパフォーマンスは、同じホスト システム上の他の **VM** によって生成される負荷に す。そのため、これらの **VM** のサイジングの数字は、他の **VM** による大きな負荷が掛かって づいた数字になります。	
推奨されるホスト サーバ	**Cisco UCS C220 M3** の同等品
ハードドライブスペース	

（注） **VMware のパフォーマンスは、同じホスト システム上の他の VM によって生成される負荷によ**
す。そのため、これらの VM のサイジングの数字は、他の VM による大きな負荷が掛かってい
づいた数字になります。

推奨されるホスト サーバ	**Cisco UCS C220 M3 の同等品**
	必要なディスク領域の確保に適した HDD の組み合わ を使用します。 • 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（Cisco Security Manager）パ 150 GB を推奨します。Cisco Security Manager の に必要な最小空きディスク領域は 7 GB です。 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 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 場合、上記のアプリケーション パーテ の他のイベント ストア パーティションに あります。詳細については、該当する Cis ハイ アベイラビリティ マニュアル（http c/en/us/support/security/security-manager/ products-installation-guides-list.html）[英語 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 て 1.0 TB の追加領域：Event Viewer を使用する場 件です。この独立したパーティションは、直接 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 み必要な条件です。イベント記録機能では、（ より）プライマリストレージの容量を超えるロ 要になると、セカンダリのイベントストレージ のセカンダリイベントストアには、プライマリ れたサイズよりも大きいサイズが要求されます ト記録を使用するには、1.0 TB 以上の追加のデ す。プライマリとセカンダリのイベントストア に配置できますが、最適なパフォーマンスを実 イマリ ストア パーティションは直接接続スト 作成することを推奨します。 パフォーマンス向上のために、RAID 10 の使用を推 ば、RAID 5 も使用できます。シーケンシャルな動作 とんどのケースではそうなりません）、書き込みポ クに設定します。そうでない場合は、書き込みポリ

（注）	**VMware** のパフォーマンスは、同じホスト システム上の他の **VM** によって生成される負荷に す。そのため、これらの **VM** のサイジングの数字は、他の **VM** による大きな負荷が掛かって づいた数字になります。
推奨されるホスト サーバ	**Cisco UCS C220 M3** の同等品
	ルーに設定します。書き込みポリシーをライトス フォーマンスも向上します。 ヒント 連続 10,000 イベント/秒（EPS）の場合は、1 日に スク スペースが消費されます。イベントストア リ）に割り当てられたディスク領域の 90 % がい ログロールオーバーが発生します。ディスクの ロールオーバーの発生が早くなります。予想 EP バー要件に基づいて、イベント管理の使用時に最 増減できます。
ホストサーバの HDD RAID	Hyper-V 内の RAID は、基礎となるホストシステ て、仮想化されたファイルシステムが使用される ん。また、ソフトウェアベースの RAID は、VM できません。詳細については、VMware, Inc. 発行 てください。
ネットワークアダプタ（Network adapter）	1 Gbps
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 • Microsoft Windows Server 2019 Datacenter（64 • Microsoft Windows Server 2016 Standard（64 • Microsoft Windows Server 2016 Datacenter（64 • Microsoft Windows Server 2012 R2 Standard（ • Microsoft Windows Server 2012 Standard（64 • Microsoft Windows Server 2012 R2 Datacenter • Microsoft Windows Server 2012 Datacenter（64
推奨されるサイジング	
デバイスの最大数	最大 200 台
サポートされる最大累積 EPS	ASA syslog の 1 秒あたり 10,000 件のイベント

（注）	**VMware** のパフォーマンスは、同じホスト システム上の他の **VM** によって生成される負荷によ す。そのため、これらの **VM** のサイジングの数字は、他の **VM** による大きな負荷が掛かってい づいた数字になります。
推奨されるホスト サーバ	**Cisco UCS C220 M3** の同等品
最大同時利用者数	同時利用者は多くても 2 人（コンフィギュレーショ 人と、イベント画面およびレポーティング画面を使 人）

中規模な企業での展開

表 7 : 中規模な企業での展開 に、中規模な企業での展開用に推奨される Cisco Security Manager サーバーの仕様を示します。

表 *7:* 中規模な企業での展開

推奨サーバ	**Cisco UCS C220 M3** の同等品
[CPU（CPU）]	1 x Hex Core（X5670 または同等シリーズを推奨）
メモリ（RAM）	• Configuration Manager のみを使用する場合は • すべての機能を使用する場合は 24 GB （注） Windows タスクマネージャによって表 モリ使用率は、設定操作中に 99 % にな これは問題を示しているわけではなく Manager のすべてのプロセスと機能が られたメモリを使用または割り当てる

推奨サーバ	Cisco UCS C220 M3 の同等品
ハードドライブスペース	

推奨サーバ	Cisco UCS C220 M3 の同等品
	必要なディスク領域の確保に適した HDD の組み を使用します。 • OS パーティション用に 100 GB を推奨しま • アプリケーション（Cisco Security Manager） 150 GB を推奨します。Cisco Security Manage に必要な最小空きディスク領域は 7 GB です 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 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 場合、上記のアプリケーション パー の他のイベント ストア パーティショ あります。詳細については、該当する ハイ アベイラビリティ マニュアル（ c/en/us/support/security/security-manager products-installation-guides-list.html）[英 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 て 1.0 TB の追加領域：Event Viewer を使用す 件です。この独立したパーティションは、直 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 み必要な条件です。イベント記録機能では、 より）プライマリストレージの容量を超える になると、セカンダリのイベントストレージ セカンダリイベントストアには、プライマリ たサイズよりも大きいサイズが要求されます 記録を使用するには、1.0 TB 以上の追加のテ す。プライマリとセカンダリのイベントスト に配置できますが、最適なパフォーマンスを イマリ ストア パーティションは直接接続ス 作成することを推奨します。 パフォーマンス向上のために、RAID 10 の使用を ば、RAID 5 も使用できます。シーケンシャルな とんどのケースではそうなりません）、書き込み クに設定します。そうでない場合は、書き込みポ ルーに設定します。書き込みポリシーをライトス フォーマンスも向上します。 ヒント

推奨サーバ	Cisco UCS C220 M3 の同等品
	連続 10,000 イベント/秒（EPS）の場合は、1 スク スペースが消費されます。イベントストリ）に割り当てられたディスク領域の 90 % がログ ロールオーバーが発生します。ディスクロールオーバーの発生が早くなります。予想バー要件に基づいて、イベント管理の使用時に増減できます。
[ネットワークアダプタ（Network adapter）]	1 Gbps
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（6 • Microsoft Windows Server 2019 Datacenter • Microsoft Windows Server 2016 Standard（6 • Microsoft Windows Server 2016 Datacenter • Microsoft Windows Server 2012 R2 Standard • Microsoft Windows Server 2012 Standard（6 • Microsoft Windows Server 2012 R2 Datacent • Microsoft Windows Server 2012 Datacenter
推奨されるサイジング	
デバイスの最大数	最大 200 台
サポートされる最大累積 EPS	ASA syslog の 1 秒あたり 10,000 件のイベント
最大同時利用者数	同時利用者は多くても 7 人（コンフィギュレ 人と、イベント画面およびレポーティング画面 人）

大規模な企業での展開

表 8 : 大規模な企業での展開 に、大規模な企業での展開用に推奨される Cisco Security Manager サーバーの仕様を示します。

表 *8 :* 大規模な企業での展開

推奨サーバ	Cisco UCS C220 M3 の同等品
[CPU（CPU）]	2 x Hex Core（X5670 または同等シリーズを推

推奨サーバ	Cisco UCS C220 M3 の同等品
メモリ（RAM）	• Configuration Manager のみを使用する場合は • すべての機能を使用する場合は 32 GB （注） Windows タスク マネージャによって モリ使用率は、設定操作中に 99% に これは問題を示しているわけではな Manager のすべてのプロセスと機能が られたメモリを使用または割り当て

推奨サーバ	**Cisco UCS C220 M3** の同等品
ハードドライブスペース	

推奨サーバ	Cisco UCS C220 M3 の同等品
	必要なディスク領域の確保に適した HDD の組み を使用します。 • OS パーティション用に 100 GB を推奨しま • アプリケーション（Cisco Security Manager） 150 GB を推奨します。Cisco Security Manag に必要な最小空きディスク領域は 7 GB です 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 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 場合、上記のアプリケーション パー の他のイベント ストア パーティショ あります。詳細については、該当する ハイ アベイラビリティ マニュアル（ c/en/us/support/security/security-manage products-installation-guides-list.html）[英 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 て 1.0 TB の追加領域：Event Viewer を使用す 件です。この独立したパーティションは、直 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 み必要な条件です。イベント記録機能では、 より）プライマリ ストレージの容量を超える になると、セカンダリのイベント ストレージ セカンダリ イベント ストアには、プライマリ たサイズよりも大きいサイズが要求されます 記録を使用するには、1.0 TB 以上の追加のデ す。プライマリとセカンダリのイベント ス に配置できますが、最適なパフォーマンスを イマリ ストア パーティションは直接接続ス 作成することを推奨します。 パフォーマンス向上のために、RAID 10 の使用を ば、RAID 5 も使用できます。シーケンシャルな とんどのケースではそうなりません）、書き込み クに設定します。そうでない場合は、書き込みポ ルーに設定します。書き込みポリシーをライト ス フォーマンスも向上します。 **ヒント**

推奨サーバ	Cisco UCS C220 M3 の同等品
	連続 10,000 イベント/秒（EPS）の場合は、1 スクスペースが消費されます。イベントスト リ）に割り当てられたディスク領域の 90 % が ログロールオーバーが発生します。ディスク ロールオーバーの発生が早くなります。予想 バー要件に基づいて、イベント管理の使用時に 減できます。
[ネットワークアダプタ（Network adapter）]	1 Gbps
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（ • Microsoft Windows Server 2019 Datacenter • Microsoft Windows Server 2016 Standard（ • Microsoft Windows Server 2016 Datacenter • Microsoft Windows Server 2012 R2 Standard • Microsoft Windows Server 2012 Standard（ • Microsoft Windows Server 2012 R2 Datacen • Microsoft Windows Server 2012 Datacenter
推奨されるサイジング	
デバイスの最大数	最大 500 台
サポートされる最大累積 EPS	ASA syslog の 1 秒あたり 10,000 件のイベント
最大同時利用者数	同時利用者は多くても 10 人（コンフィギュレ 5 人と、イベント画面およびレポーティング画 人）

（注） イベント記録を有効にする場合は、プライマリストアと同サイズまたはそれ以上の追加のストレージ容量が必要です。

（注） 上記のサイジングのガイドラインは、平均 3000 ～ 5000 のルールを持つファイアウォールデバイスに基づいています。ルール数がこれよりも大幅に多い場合は、展開でサポートされるデバイスの数を減らすか、すぐ上のハードウェアを考慮する必要があります。

大規模な小売店舗での展開

表 9 : 大規模な小売店舗での展開 に、大規模な小売店舗での展開用に推奨される Cisco Security Manager サーバーの仕様を示します。

表 *9 :* 大規模な小売店舗での展開

推奨サーバ	Cisco UCS C460 M2 の同等品
[CPU（CPU）]	4 x 8 コア
メモリ（RAM）	64 GB（すべての場合の最小）。

推奨サーバ	Cisco UCS C460 M2 の同等品
ハードドライブスペース	

推奨サーバ	Cisco UCS C460 M2 の同等品
	必要なディスク領域の確保に適した HDD の組み を使用します。 • OS パーティション用に 100 GB を推奨しま • アプリケーション（Cisco Security Manager） 150 GB を推奨します。Cisco Security Manag に必要な最小空きディスク領域は 7 GB で 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 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 場合、上記のアプリケーション パー の他のイベント ストア パーティショ あります。詳細については、該当す ハイ アベイラビリティ マニュアル c/en/us/support/security/security-manag products-installation-guides-list.html）[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 て 1.0 TB の追加領域：Event Viewer を使用す 件です。この独立したパーティションは、直 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 み必要な条件です。イベント記録機能では、 より）プライマリ ストレージの容量を超え 要になると、セカンダリのイベント ストレー のセカンダリ イベント ストアには、プライ れたサイズよりも大きいサイズが要求され ト記録を使用するには、1.0 TB 以上の追加の す。プライマリとセカンダリのイベント ス に配置できますが、最適なパフォーマンスを イマリ ストア パーティションは直接接続ス 作成することを推奨します。 パフォーマンス向上のために、RAID 10 の使用を ば、RAID 5 も使用できます。シーケンシャルな とんどのケースではそうなりません）、書き込み クに設定します。そうでない場合は、書き込みポ ルーに設定します。書き込みポリシーをライト フォーマンスも向上します。 アプリケーション パーティションには、RAID

推奨サーバ	Cisco UCS C460 M2 の同等品
	ヒント 連続 10,000 イベント/秒（EPS）の場合は、1 スク スペースが消費されます。イベントス リ）に割り当てられたディスク領域の 90 % ログ ロールオーバーが発生します。ディス ロールオーバーの発生が早くなります。予想 バー要件に基づいて、イベント管理の使用時 増減できます。
[ネットワークアダプタ（Network adapter）]	1 Gbps
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 • Microsoft Windows Server 2019 Datacenter • Microsoft Windows Server 2016 Standard • Microsoft Windows Server 2016 Datacenter • Microsoft Windows Server 2012 R2 Standar • Microsoft Windows Server 2012 Standard • Microsoft Windows Server 2012 R2 Datace • Microsoft Windows Server 2012 Datacenter
推奨されるサイジング	
デバイスの最大数	最大 2,500 のリテール ブランチ ファイアウ
サポートされる最大累積 EPS	ASA syslog の 1 秒あたり 15,000 件のイベン
最大同時利用者数	同時利用者は多くても 5 人（コンフィギュレ イベント画面およびレポーティング画面を使

（注） イベント記録を有効にする場合は、プライマリストアと同サイズまたはそれ以上の追加のストレージ容量が必要です。

（注） **1**）上記のサイジングのガイドラインは、平均 600 個のルールを持ち、合計で約 20,000 個のオブジェクトが関連付けられたファイアウォールデバイスに基づいています。ルール数がこれよりも大幅に多い場合は、展開でサポートされるデバイスの数を減らすか、デバイス管理を複数のサーバに分割することを検討します。

2）設定変更の展開を 1 つのジョブで多数のデバイスに対して実行した場合、展開の合計時間は実際のデバイスの応答（つまり、Cisco Security Manager がデバイスに接続し、最新の設定を取得するためなどに要する時間）に依存することに注意してください。したがって、展開ジョブのジョブあたりのデバイスの数が 100 未満になるよう検討することをお勧めします。

3）展開の更新を並行して実行できるデバイスの総数を増やすために Cisco Security Manager サーバーを調整することもできます。これは、インベントリ内のデバイスの設定サイズ、デバイスの応答時間や場所などによって異なります。大規模な小売環境向けにそれらのパラメータを調整するには、Cisco Technical Assistance Center（TAC）にお問い合わせください。

導入シナリオ

Cisco Security Manager アプリケーションについては、さまざまな展開が考えられます。展開のシナリオを決定する場合には、システムのパフォーマンスに影響を与える可能性のある、次の重要な要因について考慮する必要があります。

Cisco Security Manager で管理するデバイスの数はいくつありますか。

各 Cisco Security Manager のインストールには、管理するデバイスの数にハードリミットはありませんが、Cisco Security Manager サーバーごとに 500 エンタープライズクラス ファイアウォールまたは 2,500 リテールブランチ ファイアウォール未満にすることを推奨します（推奨されるハードウェアとソフトウェアを使用している場合）。1 台のサーバ当たりの適切なデバイス数を管理するには、前の項に記載されている推奨仕様に従う必要があります。管理対象デバイスが非常に大きな構成になっている場合には、デバイスの数は少なくなることがあります。たとえば、多数のファイアウォールデバイスが 20,000 ～ 50,000 のルールを持つ場合、または数千の支店で大規模かつ複雑な VPN ポリシーを持つ場合には、Cisco Security Manager の実行で実現できるパフォーマンスが準最適を下回ることがあります。多数のデバイスおよびネットワークを管理するには、必要に応じて複数の Cisco Security Manager サーバーを展開する必要があります。

複数の Cisco Security Manager サーバーにわたって、ポリシー、オブジェクト、およびデバイスをどのように管理できますか。

共有されているポリシー、オブジェクト、およびデバイスは、Policy Export/Import 機能を使用して、ある Security Manager サーバーから別の Cisco Security Manager サーバーにエクスポート/インポートできます。この機能を使用すると、共有されているポリシーやオブジェクトを複数のサーバにわたって簡単に同期できます。また、必要に応じて、管理対象デバイスをあるサーバから別のサーバに移行（移動）するのにも使用できます。

Cisco Security Managerでは、どのようなタイプのデバイスが管理されますか。デバイスのタイプによってパフォーマンスも変わりますか。

多くのタイプのデバイスを Cisco Security Manager で管理できますが、最も多く見られるのはファイアウォールと VPN デバイスで、この種のデバイスは、さまざまなタイプのデバイスでパフォーマンスがどのように異なるかを示す良い例となります。

他のタイプのデバイスよりもポリシー変更が頻繁に必要なタイプのデバイスもあります。たとえば、ファイアウォールなどのデバイスでは、VPNデバイスよりもポリシー変更が頻繁に必要です。したがって、ファイアウォールには VPN デバイスよりもはるかに多くのリソースが必要です。そのため、通常、Cisco Security Manager はファイアウォール環境よりも VPN 環境でより多くのデバイスを管理できます。

構成の一般的なサイズはどのくらいですか。

小規模な環境では、一般的なサイズは100～数千行です。中規模な環境では、一般的なサイズは 1000 ～ 5000 の ACL ですが、大規模な環境では、5000 ～ 50,000 以上の ACL になることがあります。より規模の大きい環境では、将来的な成長に対して十分な余裕を確保しておくために、1 台の Cisco Security Manager サーバー当たりのデバイス数を減らすことを考慮する必要があります。

Cisco Security Managerはいくつのイベントを管理できますか。ファイアウォールの正しい設定はどのようなものですか。

イベント管理は、多数のユーザおよびデバイスを持つ大規模な環境において、特に大量のシステムリソースを消費することがあります。適切なハードウェアおよびソフトウェアの仕様を備えた 1 つの Cisco Security Manager サーバーでは、1 秒間に最大 10,000 のイベントを管理できますが、運用に必要な重要ログだけを送信するようにデバイスを設定することをお勧めします。ファイアウォールデバイスで推奨されるロギングレベルは 0（緊急）～5（通知）です。0 では、Cisco Security Manager に送信されるログの量が最小になります。追加のロギングについては、トラブルシューティングおよびデバッグの目的で必要なときのために、1 つのデバイスに対して常に有効にしておくことができます。ロギングのレベルで 7（デバッグ）または 6（情報）を使用する場合は注意してください。これらは、必要に応じてデバイスのコンソールまたは Device Manager のみでオンにして、使用後はオフにする必要があります。

何人のユーザがこれらのアプリケーションを使用しますか。

アクティブなユーザセッションはサーバに負荷をかけるため、展開のサイズを決定する場合には、要因として考慮する必要があります。たとえば、あるアプリケーションではデバイス数が上限に達することはありませんが、同時ユーザセッション数のために最大負荷近くなることがある場合は、1 台のサーバをそのアプリケーション専用にすることが妥当です。Cisco Security Manager は 5 人を超える同時ユーザーをサポートしますが、ユーザーはイベントビューア内の最大 5 つのリアルタイムイベントビューをいつでも開くことができます。Event Server は、自身に接続している Event Viewer のインスタンスの数を制限しませんが、アクティブなすべての Event Viewer にわたる同時リアルタイムイベントビューの数に 5 というハードリミットを設定します。

Cisco Security Manager は IPv6 デバイスをサポートしていますか。

Cisco Security Manager 4.12 より前は、Cisco Security Manager サーバーは IPv4 アドレスを介してのみ管理対象デバイスと通信していました。バージョン 4.12 以降、Cisco Security Manager は、IPv6 アドレスまたは IPv4 アドレスを介した Cisco Security Manager サーバーと管理対象デバイス間の通信をサポートします。この機能は、ASA または FWSM ファイアウォールデバイスでのみ使用できます。IPv6 アドレスを介した通信を有効にするには、最初に Cisco Security Manager サーバーで IPv6 アドレスを有効にする必要があります。詳細については、『User Guide for Cisco Security Manager 4.27』の「Getting Started with Cisco Security Manager」の章 [英語] を参照してください。

Cisco Security Manager は IPv6 デバイスをサポートするようになりましたが、ASA デバイスは IPv6 Syslog サーバーをサポートしません。このシナリオでイベントマネージャはどのように機能しますか。

Cisco Security Manager 4.12 以降では、IPv6 アドレスを使用して追加されたデバイスには、デバイスインベントリに IPv6 アドレスのみがあります。デバイスがデュアルスタックで設定されている場合、Security Manger は IPv6 アドレスでデバイスと通信しますが、デバイスは引き続き管理 IPv4 アドレスを使用して syslog パケットを転送します。

イベントマネージャは、デバイスの管理 IPv4 アドレスをその [検出の詳細（Discovery Details）] から内部で取得します。デバイスから（[IPv4アドレス（IPv4 Address）] で）syslog を受信するたびに、対応する IPv6 デバイスの表示名と自動的に照合し、イベントマネージャの UI に表示します。

（注） Cisco Security Manager から IPv6 アドレスを介してのみ到達可能なファイアウォールデバイスがある場合、これらのデバイスは Cisco Security Manager で管理できますが、IPv6 アドレスを介して syslog を送信できないため、これらのデバイスでイベントマネージャは使用できません。

アプリケーション パフォーマンスに影響を与える要因

アプリケーションのパフォーマンスに影響を与える要因には、多くのものがあります。具体的には次のものがありますが、これ以外にも考えられます。

- サーバおよびクライアントのハードウェア（プロセッサ、メモリ、ストレージのテクノロジーなど）。
- 管理対象デバイスの数、およびデバイスのタイプ、デバイスの複雑さ、構成のサイズ（多数の ACL など）。
- イベント管理エンジン、管理デバイスによって報告されるイベントボリューム、およびログレベル。
- ポリシーオブジェクトの数と複雑さ。

- 同時ユーザの数と、それらのユーザが実行している特定のアクティビティ。
- デバイスの数が多い場合の、コンフィギュレーションの展開頻度、またはIPSシグニチャのアップデート頻度。
- 展開ジョブ内のデバイスの数。
- ネットワークの帯域幅と遅延（Cisco Security Managerクライアントとサーバー間、サーバーと管理対象デバイス間など）。
- VMware ESXなどの仮想テクノロジーの使用。
- AAAサービスでのISEサーバーの使用
- スケジュール済みレポートの数。
- レポーティングエンジン、管理対象デバイスによって報告されるイベントボリューム、およびイベント集約。

Cisco Security Managerクライアントとサーバーが地理的にかなり離れていると、遅延が生じて、クライアントの応答性が低下することがあります。たとえば、カリフォルニアにあるサーバで、インドにあるクライアントを使用することは、大きな遅延が生じるため推奨されません。このような場合には、クライアントがサーバと同じデータセンター内（または、少なくとも近隣）に設置される、リモートデスクトップまたはターミナルサーバ配置を採用することをお勧めします。

単一サーバのインストール

単一サーバーは、最も簡単な展開シナリオで、Cisco Security Managerの対象のアプリケーションをすべて同じサーバーにインストールします。ネットワークのセキュリティ管理者が1人、または2人の小規模なセキュリティ環境では、通常は単一サーバの展開で十分です。

複数サーバのインストール

デバイスが数百台または数千台あるような大規模な環境では、単一サーバですべてのデバイスを効率よく管理できないことがあります。パフォーマンス上の理由から、Cisco Security Managerの対象のアプリケーションを複数のサーバー間に展開することを選択できます。アプリケーション配布の例としては、たとえば次のようになります。

サーバA：ファイアウォールポリシーおよびデバイス管理

- Common Services
- セキュリティマネージャ
- Event/Log Monitoring
- Report Manager
- Image Manager

サーバー B：VPN ポリシーおよびデバイス管理

- Common Services
- セキュリティマネージャ
- Event/Log Monitoring
- Report Manager
- Health and Performance Monitor

サーバー A は、すべての ASA ファイアウォールデバイスのコンフィグレーションおよびイベント管理専用です。サーバー B は、ASA VPN デバイスの VPN ポリシー管理専用です。ファイアウォールデバイスは VPN トポロジの一部であるため、サーバー C はファイアウォールデバイスの管理も行います。この展開方法では、各サーバはそれ自身の中ではほとんど同じポリシー データしか使用しないため、サーバ間でポリシー データを共有する必要性はほとんどありません。ただし、Cisco Security Manager サーバーと管理デバイスが非常に離れた場所に展開されているようなネットワークでは、この展開は適していません。このようにすると、モニタリング、設定の検出、および展開に影響を与えることがあります。

もうひとつの方法として、地域ごとにデバイスを分けて、各 Cisco Security Manager は、地域内（米国西部、米国中部、米国東部、ヨーロッパ、アジアなど）の少数のデバイスのみを管理する、というものがあります。この方法では、管理コンソール、イベントモニタリング、および管理デバイスの設定展開について、ローカルな Security Manager サーバから最適なパフォーマンスを提供できます。

複数のサーバ展開では、ポリシーのインポート/エクスポート機能を使用して、共有ポリシーおよびオブジェクトを異なるサーバ間でエクスポートおよびインポートできます。ポリシーのインポート/エクスポートを使用して、デバイスを別のサーバに移行（移動）することもできます。これは、さまざまなサーバの多数のデバイスにわたってポリシーとオブジェクトの同期を保持しながら、管理をスケールアップするのに役立ちます。

VMware の仮想マシン環境でのインストール

Cisco Security Manager は、VMware ESXi 5.1U2 および ESXi 7.0 までの VMware ESXi バージョンでの実行をサポートしています。VMware Server や VMware Workstation などの VMware の他の環境はサポートしていません。

VMware のゲスト オペレーティング システムとして、Cisco Security Manager でサポートされている任意のサーバー オペレーティング システムを使用できます。VMware の認定作業では、通常の仮想化されていないサーバー上で稼働している Cisco Security Manager で実行されたものと同じパフォーマンステストおよび耐久性テストを行う必要がありました。テスト結果として、VMware ESX Server 4.0 で Cisco Security Manager を実行すると、イベント管理機能をオンにしない場合、アプリケーション パフォーマンスが少し低下することがわかりました。これは、関連するリファレンスネットワークのサイズや、特定のテストケースによって異なります。VMware 環境で Cisco Security Manager を展開することは、小さいサイズのネットワークにのみ適しています。

パフォーマンスが常に大きく低下するようなエリアでは、多数のASAデバイスへの展開を行っていたり、または多数（約 5,000 ～ 50,000）のルールを使用するデバイスへの展開を行っていました。このような場合には、展開にかかる時間が、容認できる範囲を超えてしまいます。VMware のパフォーマンスのベストプラクティスについては、次のマニュアル（http://www.vmware.com/pdf/Perf_Best_Practices_vSphere4.1.pdf [英語]）を参照してください。

ただし、通常、デフォルトの値または設定は最適になっているため、詳細なVMwareパラメータは調整すべきではありません。

また、仮想化の効率を向上させることに特化して設計されたテクノロジーが含まれているプロセッサを使用した、最新世代のサーバを使用することが推奨されます。たとえば、Intel® Virtualization Technology（IVT）が含まれている Intel® Xeon® X5500 シリーズの Quad-core プロセッサ上で、VMware ESX Server 4.0 で実行している Cisco Security Manager をテストした場合には、良好な結果が得られました。AMD は、仮想化の機能拡張に対して 64 ビット x86 アーキテクチャプロセッサを提供しており、これは AMD Virtualization（AMD-V）と呼ばれます。

仮想マシンのハードウェア要件およびソフトウェア要件については、表 3 : 推奨される VMware ESXi バージョン別 OS のサポート：推奨される VMware ESXi バージョン別 OS のサポートを参照してください。

ハイ アベイラビリティ/ディザスタ リカバリ

Cisco Security Manager をハイアベイラビリティまたはディザスタリカバリの構成に展開して、サーバー、ストレージ、ネットワーク、またはサイトの障害時にアプリケーションの可用性および存続可能性を大幅に向上させることができます。これらの展開オプションについては、適用可能な Cisco Security Manager ハイアベイラビリティに関するマニュアル（http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html）[英語] に詳しい説明が記載されています。

（注） VMware HA/DR シナリオで Cisco Security Manager を使用するには、Cisco Security Manager の単一ライセンスで十分です。

設置に関するガイドライン

Cisco Security Manager のインストールの詳細については、『*Installation Guide for Cisco Security Manager 4.27*』[英語] を参照してください。

インストール可能なモジュール

Cisco Security Manager サーバーのインストールは、複数の異なるコンポーネントに適用されます。コンポーネントのいくつかはオプションです。Cisco Security Manager のインストーラは、次のコンポーネントのインストールを行います。

- Common Services 4.2.2（Cisco Security Manager 4.27 のインストールを選択するとデフォルトでインストールされる）

- Security Manager 4.27 Server（必須）
- Security Manager 4.27 Client（クライアントが専用クライアント マシンにインストールされている場合はオプション）

Cisco Security Manager クライアントは、スタンドアロンインストーラを使用してインストールできます。このインストーラにアクセスする最も一般的な方法は、Web ブラウザ（https://server_hostname_or_ip）を使用してサーバにログインし、クライアント インストーラをクリックする方法です。

Cisco Security Manager のインストーラ、および Cisco Security Manager クライアントインストーラの詳細な使用方法については、『*Installation Guide for Cisco Security Manager 4.27*』[英語] を参照してください。

IP アドレス、ホスト名、および DNS 名

Cisco Security Manager では、DHCP アドレスではなく、スタティック IP アドレスが必要です。Cisco Security Manager サーバーの IP アドレスは変更できます。変更後に、システムのリブートが必要です。Cisco Security Manager の TCP/IP 設定で DNS サーバーを設定する場合は、Cisco Security Manager サーバーのホスト名と DNS 名が同じで、設定されている DNS サーバーで解決可能であることを確認してください。Cisco Security Manager をインストールする前に、サーバーに対して永続的な DNS 名とコンピュータホスト名を選択する必要があります。これは、ホスト名と DNS 名はインストールの後に修正できないためです。インストール後に Cisco Security Manager サーバーのホスト名を変更すると、Cisco Security Manager の再インストールが必要になる場合があります。

（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。IPv6 アドレスは 128 ビットの一意のアドレスです。IPv6 アドレスについては、スタティック IP タイプのみがサポートされています。ダイナミック IP タイプは、IPv6 アドレスではサポートされません。詳細については、『**User Guide for Cisco Security Manager 4.27**』の「*Getting Started with Cisco Security Manager*」の章 [英語] を参照してください。

クライアントの展開

推奨される通常の手順では、Cisco Security Manager クライアントを個別のクライアントマシンにインストールし、実行します。Cisco Security Manager では、特定のマシン上にクライアントのシングルバージョンをインストールすることのみサポートしています。そのため、同じマシン上で Cisco Security Manager 4.10 と 4.27 の両方のクライアントを持つことはできません。サーバにクライアントをインストールして使用することはできますが、これは、規模の小さいネットワークにのみ適しており、規模の大きい企業ネットワークにはお勧めできません。

アプリケーション パフォーマンスに影響を与える要因 （44 ページ）の項に記載されているように、エンドユーザーとサーバーの場所がかなり離れていて、相当な遅延が発生している場合

（大陸間の距離がある場合）でも容認できるパフォーマンスを保持するために、サーバーに近い場所にあるターミナルサーバー上に、クライアントを展開することをお勧めします。

Cisco Security Manager サーバーのチューニング

Cisco Security Manager には、いくつかの詳細なパラメータが用意されています。このパラメータを修正して、アプリケーションのパフォーマンスを調整できます。50以上のデバイスを管理する中規模および大規模な展開では、最適なパフォーマンスを得るために、Cisco Security Manager で次のパラメータを変更できます。

- ディスクの最適化 （49 ページ）
- Windows オペレーティングシステムのスワップファイルサイズ （49 ページ）

ディスクの最適化

最適なパフォーマンスのために、ディスクサイズの50GB増加ごとにディスク フラグメンテーションを行うことを推奨します。

注意 頻繁に最適化を行うことによって、最終的にディスク障害を引き起こす、不良セクタを防ぐこともできます。

Windows オペレーティングシステムのスワップファイルサイズ

仮想メモリ（ページングファイル）は、インストールされているメモリの 1.5 倍である必要があります。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 [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オフに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。

Cisco Security Manager のライセンスについて

Cisco 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、Cisco 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。

重要なライセンシング情報については、次のマニュアルを参照してください。

- 『*Installation Guide for Cisco Security Manager 4.27*』
- http://www.cisco.com/c/en/us/products/security/security-manager/bulletin-listing.html [英語] にある、Cisco Security Manager の最新メジャーリリースの製品速報

ライセンスの例

ここでは、Cisco Security Manager のライセンスを理解しやすいように、いくつかの代表的なライセンスの例を示します。

例 1

管理対象ネットワークの説明：フェールオーバーモードで動作する 250 の ASA ペアがある（500 台のデバイス）。

必要なライセンス：**Professional-250 ライセンス。**また、Professional-50 ライセンスまたは Professional-100 ライセンスを、適切な差分（「アドオン」）デバイスライセンスとともに注文することもできます。差分デバイスライセンスは、50、100、および 250 台単位でデバイス数を追加できます。

例 2

管理対象ネットワークの説明：Cisco Security Manager Standard-25 デバイスライセンスがあるが、追加で、シングルモードで稼働している 20 台の ASA デバイスを管理する必要がある。

必要なライセンス：Enterprise Standard-25 to Professional-50 Upgrade ライセンスが必要です。

例 3

管理対象ネットワークの説明：アクティブ/スタンバイ、またはアクティブ/アクティブのペアの組み合わせで展開されており、それぞれ 5 つのセキュリティコンテキストを持つ、10 ペアのフェールオーバー ASA デバイス（20 台のデバイス）。

必要なライセンス：Enterprise Professional-50、および Enterprise Professional Incremental 50 Device

冗長性を得るためフェールオーバーデバイスのペアを展開する場合は、Cisco Security Manager にアクティブデバイスおよびコンテキストを追加するだけで済みます。必要なデバイスのライセンス数は、（10 台のデバイス）×（5 つのコンテキスト）+（10 台のシャーシ）で、合計 60 個のデバイスライセンスになります。

（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/c/en/us/products/security/security-manager/bulletin-listing.html で Cisco Security Manager の最新メジャーリリースの製品速報 [英語] を参照してください。

（注） 上記のすべての例では、Cisco Technical Assistance Center（TAC）およびアプリケーションのマイナー リリース アップデートを無料で使用できるようにするために、対応する Cisco Service Application Support（SAS）の注文を検討する必要があります。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。