

## Cisco Security Manager 3.2

### Cisco Security Manager の概要

Cisco® Security Manager は、シスコのネットワーク デバイスやセキュリティ デバイス上でファイアウォール、VPN、侵入防御(IPS)といったセキュリティ サービスを設定する目的で設計された、エンタープライズクラスの管理アプリケーションです。ポリシー ベースの管理手法を採用することにより、小規模ネットワークから数千のデバイスで構成される大規模ネットワークにいたるまで、あらゆる規模のネットワークで利用できます。Cisco Security Manager は Cisco Security Monitoring, Analysis, and Response System (CS-MARS)と連携して機能します。両者を同時に利用すれば、設定管理、セキュリティ モニタリング、分析、および脅威の軽減に対応する幅広いセキュリティ 管理ソリューションを実現できます。

### シスコの自己防衛型ネットワーク

シスコの自己防衛型ネットワークは、進化するセキュリティ環境に対応するために設計されたアーキテクチャ ソリューションです。セキュリティをあらゆる場所に統合し、ライフサイクル サービスの手法を併用することにより、企業の重要な業務プロセスを攻撃や中断から守り、機密情報を保護し、ポリシー管理やコンプライアンス管理を支えることが可能なネットワーク プラットフォームを設計、導入、運用、および最適化できるようになります。このようなネットワークをプラットフォームとして利用すれば、人材と IT 資産の安全確保につながるとともに、業務組織の復元力と信頼性を向上させ、IT 投資から最大限の事業効果を得られます。Cisco Security Manager はシスコの自己防衛型ネットワークに不可欠な要素であり、事業責任者がアクティブかつ協調的に既知および未知の脅威を抑制すると同時に、管理下にあるすべてのシスコ セキュリティ デバイスに対して、クローズドループのセキュリティ ポリシーを実施できるようにします。

### コラボレーションによる脅威の識別と軽減

Cisco Security Manager は CS-MARS と連携してネットワークへの脅威を軽減します。Cisco Security Manager と CS-MARS をともに利用すると、ネットワークおよびセキュリティの状況を把握できるほか、設定済みのファイアウォール、VPN、IPS ポリシーの可視性を確保できます。

### 一元化されたセキュリティ ソリューション

Cisco Security Manager は、シスコのセキュリティ アプライアンス、ルータ、スイッチを対象として、横断的なセキュリティ管理を行う統合アプリケーションです。Cisco Security Manager は Role-Based Access Control (RBAC; ロール ベース アクセス コントロール)メカニズムを備えているため、個々のユーザに応じて幅広い機能を適切に管理できます。Cisco Security Manager のオプションであるワークフロー機能をRBAC とともに利用すると、従来からのセキュリティ管理チームとネットワーク運用チームの両方が、それぞれの役割に応じて Cisco Security Manager を使用できます。

### セキュリティの効率と柔軟性の向上

Cisco Security Manager を利用すると、少数のデバイスで構成されるネットワークから数千台のデバイスで構成されるネットワークまでを効率的に管理できます。ポリシーベースの強力な管理手段で柔軟性を実現し、「一度の設定で多数の導入」という効率の高い手法を可能にします。設定を変更した場合、Cisco Security Manager は、関連するすべてのネットワーク デバイスに自動的に

変更を適用します。ファイアウォール、VPN、IPS に関する各ポリシーはプラットフォームに依存しません。したがって、シスコのルータ、セキュリティ アプライアンス、サービス モジュールなどの異なるデバイス プラットフォームにわたってそれらを適用することができます。Cisco Security Manager はデバイスレベルの柔軟な上書き機能も備えており、ポリシーの再利用と共有を行う一方で、必要に応じてデバイス固有の設定をカスタマイズすることもできます。

### 優れた管理機能と可視性

Cisco Security Manager は日常のセキュリティ管理制御に優れ、ファイアウォール ルールの分析と最適化、VPN 設定、および IPS シグニチャ管理の可視性を高めます。Cisco Security Manager と CS-MARS を利用すれば、セキュリティ ポリシー イベントをリアルタイムに把握し、ポリシーの設定内容を即座に分析して制御できます。このような管理体制によって、ネットワーク運用グループとセキュリティ管理グループの緊密なコラボレーションを促進すると同時に、新たな更新ポリシーのイベント検証を即座に可能にします。Cisco Security Manager と CS-MARS 間でのポリシー イベント相関処理によって、インシデント調査における可視性が高まり、脅威軽減に関する問題解決に必要な時間が大幅に短縮されます。

図 1 ～ 4 に、Cisco Security Manager と CS-MARS の間で行われるコラボレーション メカニズムの一部を示します。

図 1 Cisco Security Manager IPS ポリシーから CS-MARS イベントへのコラボレーション

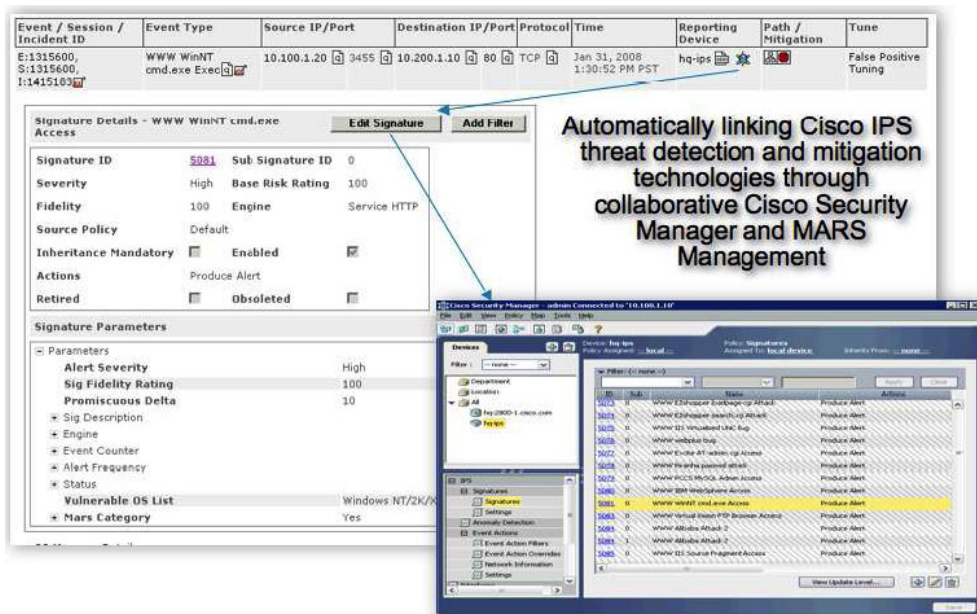


図 2 Cisco Security Manager ACL ポリシーから CS-MARS ログへのコラボレーション

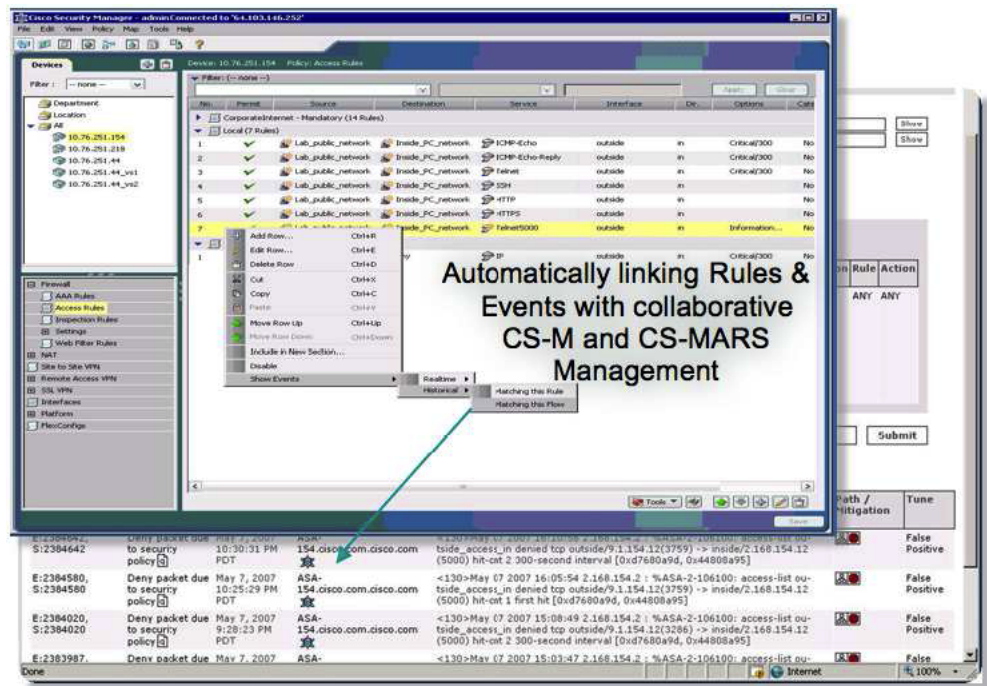


図 3 CS-MARS IPS イベントから Cisco Security Manager ポリシーへのコラボレーション

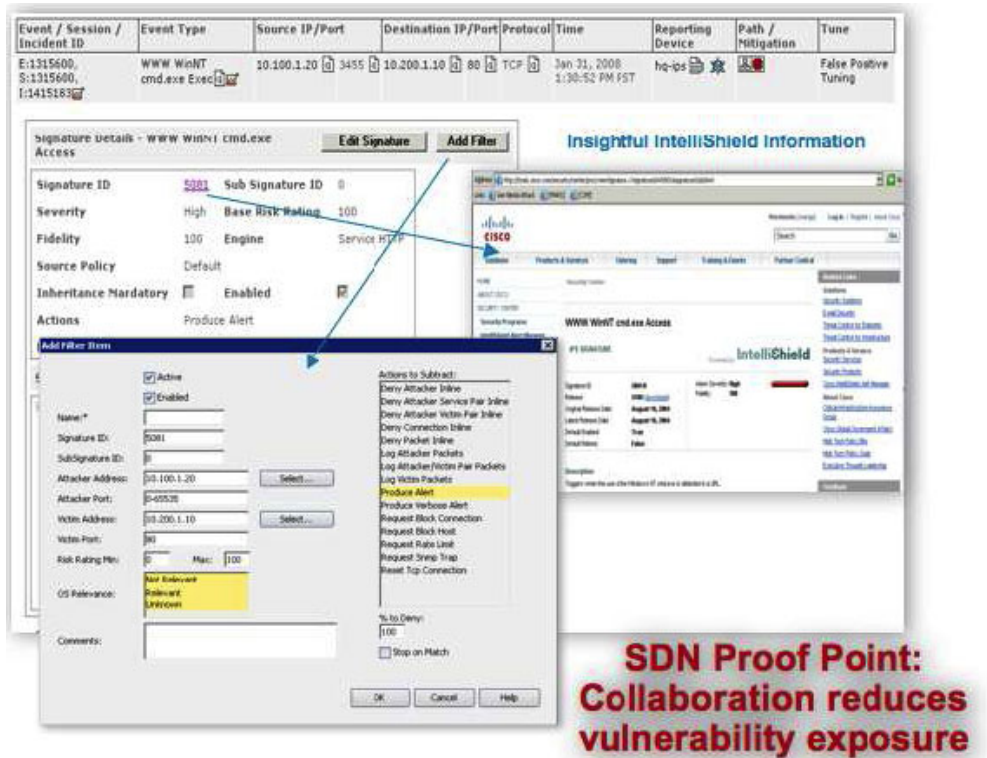


図 4 CS-MARS ファイアウォール ログから Cisco Security Manager ポリシーへのコラボレーション

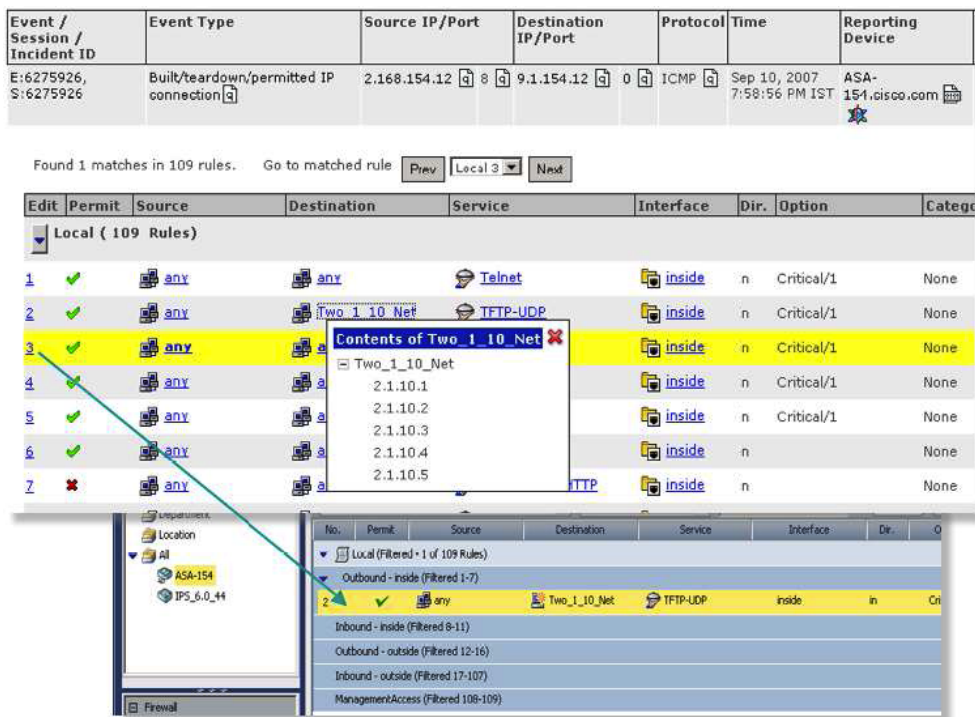


表 1 に、Cisco Security Manager 3.2 の機能と利点を示します。

表 1 Cisco Security Manager 3.2 の機能と利点

| 機能         | 利点   |
|------------|--|
| VPN 設定     | <p>VPN ウィザードを使用すると、サイト間、ハブ アンド スポーク、フルメッシュ、およびエクストラ ネット VPN を簡単に設定できます。</p> <ul style="list-style-type: none"> <li>• Cisco Security Manager は、ダイナミック IP と階層型認証を使用する、Dynamic Multipoint VPN(DMVPN)と Generic Routing Encapsulation(GRE; 総称ルーティング カプセル化) IP Security(IPSec)をサポートしています。</li> <li>• VPN と Easy VPN サービスはリモートで設定できます。</li> <li>• 安全なデバイス プロビジョニングのサポートにより、自動で展開が可能です。</li> <li>• ヘッドエンド用の自動フェールオーバーとロードバランシングの設定がサポートされています。</li> </ul>  |
| ファイアウォール設定 | <p>Cisco Security Manager を使用すると、管理者は、Cisco ASA 5500 シリーズ アプライアンス、Cisco PIX アプライアンス、Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール、および Cisco IOS ソフトウェア セキュリティ イメージを実行するシスコ サービス統合型ルータ プラットフォームのポリシーを設定できます。</p> <ul style="list-style-type: none"> <li>• ソフトウェアにより、すべてのプラットフォームに 1 つのルール テーブルが提供されます。ユーザは、1 つのソリューションでこれらのデバイスを管理できます。</li> <li>• ルール分析機能により、他のルールと重複または競合するファイアウォール ルールがレポートされます。</li> <li>• オブジェクト グループ化機能により、特定のセキュリティ ポリシーの実装に必要なアクセス ルールの数が大幅に削減されます。オブジェクト グループ化では、類似したオブジェクトをグループ化するアルゴリズムを使用することで、1 つのアクセス ルールをグループ内のすべてのオブジェクトに適用できます。</li> <li>• ソフトウェアにより、ネットワークに影響しないルールの識別と削除が可能です。</li> <li>• ACL ヒット カウント機能により、トラフィックが正常に送信されていることが確認されます。</li> <li>• ポリシー クエリー機能により、ワイルドカードを含む、特定の送信元、宛先、およびサービス フローと一致するルールが表示されます。</li> <li>• 設定を容易にするために、デバイス情報をデバイス リポジトリまたはコンフィギュレーション ファイルからインポートしたり、ソフトウェアに追加したりできます。また、デバイス自体からファイアウォール ポリシーを検出することもできます。</li> <li>• インターフェイス ロールを使用すると、ユーザはインターフェイスのグループにスケーラブルな方法でルール ポリシーを適用できます。</li> </ul> |

| 機能   | 利点   |
|--|--|
| <b>IPS 設定</b>  | <p>Cisco Security Manager を使用すると、管理者は、Cisco IPS センサー ソフトウェア バージョン 5.1 および 6.0 をサポートする Cisco IPS 4200 シリーズ センサー、Cisco ASA 5500 シリーズ AIP-SSM (Advanced Inspection and Prevention Security Services Module)、Cisco Catalyst 6500 シリーズ Intrusion Detection System Module 2 (IDSM-2)、Cisco IDS ネットワーク モジュール、Cisco AIM-IPS、および Cisco IOS IPS の IPS ソリューションベースの設定やアップデート ポリシーを容易かつ効果的に管理できます。</p> <ul style="list-style-type: none"> <li>• Cisco IPS センサー ソフトウェア バージョン 5.1 および 6.0 - この Cisco IPS ソリューションは、インライン型侵入防御サービスと画期的なテクノロジーを組み合わせることで精度の向上を実現しています。Cisco IPS センサー ソフトウェアは、ワーム、スパイウェアとアドウェア、ネットワーク ウイルス、およびアプリケーションの不正利用を含む不正なトラフィックを、業務の継続に影響する前に、正確に識別、分類、抑止できます。</li> <li>• Cisco IOS IPS は、インライン型のディープ パケット インスペクションベースの機能で、Cisco IOS ソフトウェアでさまざまなネットワーク攻撃を効率的に軽減できるようになります。また、シスコの自己防衛型ネットワークの中心となる Cisco IOS IPS を使用すると、ネットワークで不正なトラフィックや攻撃的なトラフィックをリアルタイムで正確に識別、分類、および抑止できるようになります。</li> <li>• Cisco IPS シグニチャの更新を把握できるため、新しいシグニチャや更新したシグニチャの差分プロビジョニングが可能になります。また、社内に導入する前に IntelliShield で詳細を把握することができます。これにより、Cisco IPS セキュリティ リサーチ チームが推奨するデフォルト設定をすみやかに確認し、シグニチャの更新を配布する前にユーザの環境に合わせて調整することが可能になります。</li> <li>• Cisco IPS 更新ウィザードを利用すると、ステータスや詳細情報を通知して、自動 IPS 更新、スケジューリング、およびポリシーの配布を効率的に行うことができます。</li> <li>• CS-MARS と相互コラボレーションを行うことにより、ポリシー展開に関する変更をただちに発見して、イベントや異常の検査を行うことができます。このコラボレーションにより、過去および現在進行中のイベントに対するポリシーの起動が可能になります。ネットワーク運用チームとセキュリティ管理チームのより緊密なコラボレーションを促すと同時に、Cisco Security Manager のさまざまなポリシーをひとつにまとめる効果も果たします。状況のすみやかな把握と相互コラボレーションにより、イベント検査とトラブルシューティングを減らし、解決時間を短縮します。Cisco Security Manager と CS-MARS のコラボレーションにより、インタラクティブな IPS イベント アクション フィルタの作成が可能になります。その結果、ネットワークの脆弱性が外部に曝される可能性が低くなります。</li> <li>• IPS シグニチャ ポリシーおよびイベント アクション フィルタは、あらゆるデバイスに継承および割り当てることができます。その他の IPS ポリシーもすべて割り当て可能で、他の IPS デバイスと共有できます。IPS の管理には、ポリシーのロールバック、設定のアーカイブ、およびシグニチャのコピーまたは作成も含まれます。デバイス間でポリシーをコピーすることにより、導入の手間を省いて効果的な管理と TCO の削減を行うことができます。</li> <li>• IPS の更新管理および IPS サブスクリプション ライセンスの更新によって配布が簡素化され、ユーザはローカル ポリシーおよび共有ポリシーに基づいて IPS ソフトウェア、シグニチャの更新、およびライセンスの管理を行うことができます。</li> </ul> |
| <b>統合セキュリティ サービスの管理</b>  | Cisco Security Manager により、VPN の QoS (Quality of Service)、ルーティング、Network Admission Control (NAC) などを含む、統合セキュリティ サービスを管理できます。   |
| <b>柔軟なデバイス グループ化オプション</b>  | ユーザは、業務上の機能または配置に基づいてデバイス グループを作成および定義し、組織的な構造を正確に表すことができます。グループ内のすべてのデバイスを 1 つのデバイスを扱うように簡単に管理できます。   |
| <b>複数のアプリケーションビュー</b>  | Cisco Security Manager は、さまざまな使用事例とエクスペリエンス レベルをサポートするために、アプリケーションに関する複数のビューを提供します。デバイス視点のビューは、初心者ユーザ、または単一のデバイス マネージャの使用に慣れているユーザに便利です。マップ視点のビューは、VPN のトポロジ、または Cisco Catalyst 6500 シリーズ サービス モジュールとセキュリティ コンテキスト間の抑制関係を視覚化します。ポリシー視点のビューは、非常に効率的でスケーラブルな複数デバイスの管理を可能にします。  |
| <b>Policy Object Manager</b>   | 再利用可能なオブジェクトを作成して、ネットワーク アドレス、サービス、デバイス設定、時間範囲、または VPN パラメータなどを表すことができます。オブジェクトは、1 回定義すると何回でも使用できるため、手動で値を入力する必要がありません。  |
| <b>Deployment Manager による柔軟な展開オプション</b>  | Cisco Security Manager は、デバイスまたはファイルへのオンデマンドの展開と計画的な展開の両方をサポートしています。   |
| <b>ロールバック</b>  | Cisco Security Manager は、必要に応じて、以前の設定へのロールバックを実行できます。  |
| <b>ロールベースのアクセスコントロール</b>   | Cisco Security Manager を使用すると、複数の管理者に対して適切な制御を使用してアクセス権を定義できます。Cisco Security Manager には 5 つのユーザ ロールがあり、オプションの Cisco Secure ACS (Access Control Server) で追加のロールを使用することもできます。   |
| <b>ワークフロー</b>  | Cisco Security Manager では、ポリシーの導入時に特定のタスクを各管理者に割り当てることができ、変更管理と追跡機能も提供します。ワークフローを使用すると、スタッフの共同作業 (ネットワークとセキュリティ運用間など) が改善されます。   |
| <b>分散型の展開方法 (Auto Update Server、Cisco Network Services Configuration Engine)</b> | Cisco Security Manager により、ダイナミック アドレスまたは NAT (Network Address Translation; ネットワーク アドレス変換) アドレスを持つ多数のリモート ファイアウォールの更新が簡易化されます。この機能は、リモート サイトに断続的なネットワーク リンクがあり、最小限の技術スタッフしかいないユーザに役立ちます。   |

| 機能                | 利点   |
|-------------------|--|
| 運用管理              | Cisco Security Manager は、ソフトウェアの配布やデバイス インベントリ レポートなどの運用機能に役立ちます。また、Device and Credentials Repository (DCR) と CiscoWorks Resource Manager Essentials (RME) と統合できます。                                      |
| 状態とパフォーマンスのモニタリング | Cisco Security Manager サービス契約を結んでいるユーザは、Cisco.com から CiscoWorks Monitoring Center for Performance アプリケーションをダウンロードできます。このアプリケーションは、シスコの VPN ネットワーク デバイスおよび特定のセキュリティ サービスのための、状態とパフォーマンスのモニタリング データを提供します。 |

表 2 に Cisco Security Manager の最小サーバ要件、表 3 に最小クライアント要件を示します。

表 2 サーバの要件と技術仕様

| コンポーネント      | 最小要件   |
|--------------|--|
| システム ハードウェア  | <ul style="list-style-type: none"> <li>IBM PC 互換機、2 GHz 以上のプロセッサ搭載</li> <li>1024 × 768 以上の解像度のカラー モニタと 16 ビット カラーに対応したビデオ カード</li> <li>DVD-ROM ドライブ</li> <li>100BASE-T (100 Mbps) 以上のネットワーク接続、単一インターフェイスのみ</li> <li>キーボード</li> <li>マウス</li> </ul>  |
| ファイル システム    | NTFS   |
| メモリ (RAM)    | 2 GB   |
| システム ソフトウェア  | <p>次のいずれかを使用できます。</p> <ul style="list-style-type: none"> <li>Microsoft Windows 2003 Server の以下のエディション: <ul style="list-style-type: none"> <li>Enterprise Edition (SP1 または SP2)</li> <li>Standard Edition (SP1 または SP2)</li> <li>R2 Enterprise Edition (SP1 または SP2)</li> <li>R2 Standard Edition (SP1 または SP2)</li> </ul> </li> </ul> <p>注: Cisco Security Manager は、Windows のアメリカ英語版と日本語版のみをサポートしています。</p> <p>サーバで Sybase データベース ファイルを使用するためには、Microsoft ODBC Driver Manager 3.510 以降も必要です。</p> |
| ブラウザ         | <p>次のいずれかを使用できます。</p> <ul style="list-style-type: none"> <li>Microsoft Internet Explorer 6.0 (SP2)</li> <li>Microsoft Internet Explorer 7.0</li> <li>Firefox 2.0</li> </ul>  |
| 圧縮ソフトウェア     | WinZip 9.0 または同等のソフトウェア  |
| ハードドライブの空き容量 | 20 GB  |
| IP アドレス      | <p>最低 1 つのスタティック IP アドレス</p> <p>サーバに複数の IP アドレスが設定されている場合は、1 つのアドレスを除いてすべてを無効にします。ターゲット サーバでダイナミック IP アドレスが検出された場合、Cisco Security Manager インストーラに警告が表示されます。ダイナミック アドレスはサポートされていません。</p>  |

表 3 クライアントの要件と技術仕様

| コンポーネント      | 最小要件  |
|--------------|---|
| システム ハードウェア  | <ul style="list-style-type: none"> <li>IBM PC 互換機、1 GHz 以上のプロセッサ搭載</li> <li>カラー モニタと 24 ビット カラーに設定されたビデオ カード</li> <li>キーボード</li> <li>マウス</li> </ul> |
| メモリ (RAM)    | 1 GB  |
| 仮想メモリスワップ領域  | 512 MB  |
| ハードドライブの空き容量 | 10 GB   |

| コンポーネント       | 最小要件  |
|---------------|---|
| オペレーティング システム | 次のいずれかを使用できます。 <ul style="list-style-type: none"> <li>• Microsoft Windows Vista Business Edition または Enterprise Edition</li> <li>• Microsoft Windows XP Professional (SP1 または SP2)</li> <li>• Microsoft Windows 2003 Server の以下のエディション: <ul style="list-style-type: none"> <li>◦ Enterprise Edition (SP1 または SP2)</li> <li>◦ Standard Edition (SP1 または SP2)</li> <li>◦ R2 Enterprise Edition (SP1 または SP2)</li> <li>◦ R2 Standard Edition (SP1 または SP2)</li> </ul> </li> </ul> <p>注: Cisco Security Manager クライアントは、Windows のアメリカ英語版と日本語版のみをサポートします。他の言語バージョンはサポートしていません。</p> |
| ブラウザ          | 次のいずれかを使用できます。 <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 6.0 (SP2)</li> <li>• Microsoft Internet Explorer 7.0</li> <li>• Firefox 2.0</li> </ul>  |
| Java          | Cisco Security Manager クライアントには、完全に独立して機能する Java が組み込まれます。このバージョンの Java は、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には影響しません。<br>Cisco Security Manager の起動時に必要なバージョンの Java が存在しない場合、Cisco Security Manager サーバに、必要なバージョンの Java をダウンロードおよびインストールする方法を示すメッセージが表示されます。  |

Cisco Security Manager のハードウェアおよびソフトウェアの要件の詳細については、[http://www.cisco.com/en/US/products/ps6498/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html) にある『Cisco Security Manager Installation Guide』(英語)を参照してください。

表 4 に、Cisco Security Manager でサポートされるデバイス製品ファミリをまとめます。サポートされるデバイス ソフトウェア バージョンを含む詳細な一覧については、[http://www.cisco.com/en/US/products/ps6498/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html) にある『Supported Devices and OS Versions for Cisco Security Manager 3.2』(英語)を参照してください。

表 4 Cisco Security Manager でサポートされるシスコ デバイスの概要

| サポート対象デバイス   |
|--|
| Cisco PIX セキュリティ アプライアンス   |
| Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンス                            |
| Cisco サービス統合型ルータ   |
| Cisco 7600 シリーズ ルータ  |
| Cisco 7500 シリーズ ルータ  |
| Cisco 7300 シリーズ ルータ  |
| Cisco 7200 シリーズ ルータ  |
| Cisco 7100 シリーズ ルータ  |
| Cisco 3200 シリーズ ルータ  |
| Cisco 2600 シリーズ ルータ  |
| Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール (FWSM)              |
| Cisco Catalyst 6500 シリーズ VPN サービス モジュール (VPNSM)                  |
| Cisco 7600 シリーズ/Catalyst 6500 シリーズ IPsec VPN 共有ポート アダプタ (VPNSPA) |
| Cisco Catalyst 6500 シリーズ IDSM-2                                  |
| Cisco IPS 4200 シリーズ センサー   |
| 適応型セキュリティ アプライアンス用 Cisco AIP-SSM                                 |
| サービス統合型ルータ用 Cisco AIM-IPS  |

| サポート対象デバイス  |
|---|
| アクセス ルータ用 Cisco IPS モジュール (NM-CIDS)   |
| Cisco Catalyst 3550、3560、3560E、3750、3750 Metro、4500、4948、および 4948 10GE スイッチ |

オプションの CiscoWorks RME 4.1 でサポートされるデバイスの一覧については、次の URL にある LMS 3.0 向けのサポート対象デバイス表を参照してください。

[http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_device_support_tables_list.html)

## 発注情報

Cisco Security Manager の Product Bulletin には、ライセンス オプションと発注の詳細が記載されています。この Product Bulletin は、<http://www.cisco.com/go/jp/csm/> で公開されています。

## シスコのサービス

シスコは、ライフサイクル アプローチによるサービスを提供しており、シスコのパートナーと連携して幅広い一連のセキュリティ サービスを実現しています。このサービスをご利用いただくと、お客様の重要な業務プロセスを攻撃や中断から守り、機密情報を保護し、ポリシー管理やコンプライアンス管理を支えることが可能なネットワーク プラットフォームを設計、導入、運用、および最適化できるようになります。

ネットワークへの投資を無駄にすることなく、ネットワーク運用を最適化し、ネットワーク インテリジェンスの強化や事業拡張を進めていただくために、シスコのサービスをお役立てください。サービスについての詳細は、以下の URL を参照してください。

<http://www.cisco.com/web/JP/services/portfolio/index.html>

- **Cisco Security Optimization Service** は、セキュリティをコア ネットワーク インフラストラクチャに統合するための支援を提供します。ネットワーク インフラストラクチャは即応性と適応力に富むビジネスの基盤です。Cisco Security Optimization Service は、絶えず変化するセキュリティ脅威に対抗するため、プランニングとアセスメントを組み合わせ、設計、パフォーマンスチューニング、あるいはシステム変更に対応する恒常的サポートを提供することにより、進化し続けるセキュリティシステムを実現します。
- **Cisco Security Center** は、早期警告、脅威に対抗するインテリジェンス、脅威と脆弱性の分析、Cisco IPS シグニチャ、および脅威軽減の各種技術のすべてを集約して提供します。Cisco Security Center については、次の URL を参照してください。  
<http://www.cisco.com/security>
- **Cisco Security Intellishield Alert Manager Service** は、カスタマイズ可能な Web ベースの脅威および脆弱性警告サービスを提供します。このサービスをご利用いただくと、お客様の環境に存在する潜在的な脆弱性に関する正確かつ信頼性の高い情報に、適切なタイミングで簡単にアクセスできます。

Cisco Security Manager ソフトウェアは、Cisco Software Application Support (SAS) のテクニカルサポート サービスの適用対象となります。Cisco SAS サービス契約の特長は、次のとおりです。

- 評価の高いサポートを提供する Cisco Technical Assistance Center (TAC) に無制限にアクセスできます。テクニカル サポートは、シスコのセキュリティ ソフトウェア アプリケーションのトレーニングを受けた、ソフトウェア アプリケーションの専門家が担当し、常時世界中から利用できます。

- Cisco.com に登録し、アクセスできます。Cisco.com では、豊富なアプリケーション ツールと技術文書が利用でき、ネットワーク セキュリティの問題の診断、新しいテクノロジーの理解、および革新的なソフトウェア拡張機能の把握に役立ちます。ユーティリティ、ホワイト ペーパー、アプリケーション設計データ シート、コンフィギュレーション ドキュメント、およびケース管理ツールを利用して、社内の技術力の向上を図ることができます。
- アプリケーション ソフトウェアのバグ修正、保守、およびマイナー ソフトウェア リリースが利用できます。

有効な SAS または Software Application Support plus Upgrades(SASU) 契約に含まれる既存の CiscoWorks VMS (VPN/Security Management Solution) から Cisco Security Manager に移行することもできます。

### 関連情報

Cisco Security Manager 3.2 についての詳細は、<http://www.cisco.com/jp/go/csmanager/> を参照してください。

CS-MARS についての詳細は、次の URL を参照してください。

<http://www.cisco.com/jp/go/mars/>

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

お問い合わせ先