Cisco Security Manager 4.0

Cisco Security Manager の概要

Cisco® Security Manager は、シスコのセキュリティ デバイスおよびネットワーク デバイスを把握し制御するための、エンタープライズクラスのセキュリティ管理アプリケーションです。Cisco Security Manager は、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、Cisco IPS 4200 シリーズ センサー アプライアンス、Cisco サービス統合型ルータ(ISR)、Cisco 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 スイッチなどの幅広いシスコ セキュリティ アプライアンスの包括的なセキュリティ管理(設定とイベント管理)を提供します。Cisco Security Manager によって、小規模ネットワークから数百のデバイスで構成されるような大規模ネットワークまで、あらゆる規模のネットワークを効率的に管理できます。

Cisco Threat Defense

Cisco Threat Defense は、ボーダレスなネットワーク環境を保護および管理するのに役立ちます。Cisco Security Intelligence Operations(SIO)、市場をリードするネットワーク セキュリティ機器、および単一の統合セキュリティ管理プラットフォームのプロアクティブなインテリジェンスを使用することで、現在の複雑で動的な脅威環境から保護することができます。

簡素化されたセキュリティ管理

- 次世代の Cisco Security Manager では、単一の統合されたユーザ インターフェイス(図 1)を使用して、セキュリティトポロジ全体を把握し制御できます。これには次のものがあります。
  - Cisco ASA および IPS アプライアンスのグローバル ポリシー
  - 設定およびイベント管理の単一コンソール
- 次世代の Cisco Security Manager では、セキュリティ環境の可視性が向上しているため、脅威パターンとリスクをより適切に理解して、これらに対応できます。次のような機能が含まれます。
  - Global Threat Correlation エンジン搭載の Cisco IPS と Cisco ASA アプライアンスで阻止されたイベントの単一ビュー
  - 履歴トラフィック パターン情報
  - 強力なフィルタリングおよびドリル ダウン機能
  - レピュテーション データの IPS イベントへの統合
  - アクション可能なイベントをベースにしたダイナミック ポリシー調整
- Cisco Global Threat Correlation エンジン搭載の Cisco IPS は、より正確な検出と自動化されたルール セットによって、IPS 管理に必要な時間を削減
- イベントとポリシーのリンク付けと相互ローンチのサポート(図 2)
- Cisco Packet Tracer や traceroute コマンドなどの、統合されたトラブルシューティング ツール
- 異機種を運用する IT 環境に対応した、Out-of-Band(OOB; アウトオブバンド)変更の検出と選択的な ASA ポリシー管理
- ASA アプライアンス向けに簡素化されたポリシー定義パラダイム(Network Address Translation [NAT; ネットワーク アドレス変換] サービスを提供)(図 3)およびグローバル アクセス ルールで管理効率を向上
- Botnet Traffic Filter や Global Threat Correlation エンジンなどのシスコの最新 IPS およびファイアウォール機能の拡張サポートによって、脅威への対応エクスペリエンスを向上

All contents are Copyright © 1992–2010 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

図 1　統合されたイベント コンソール

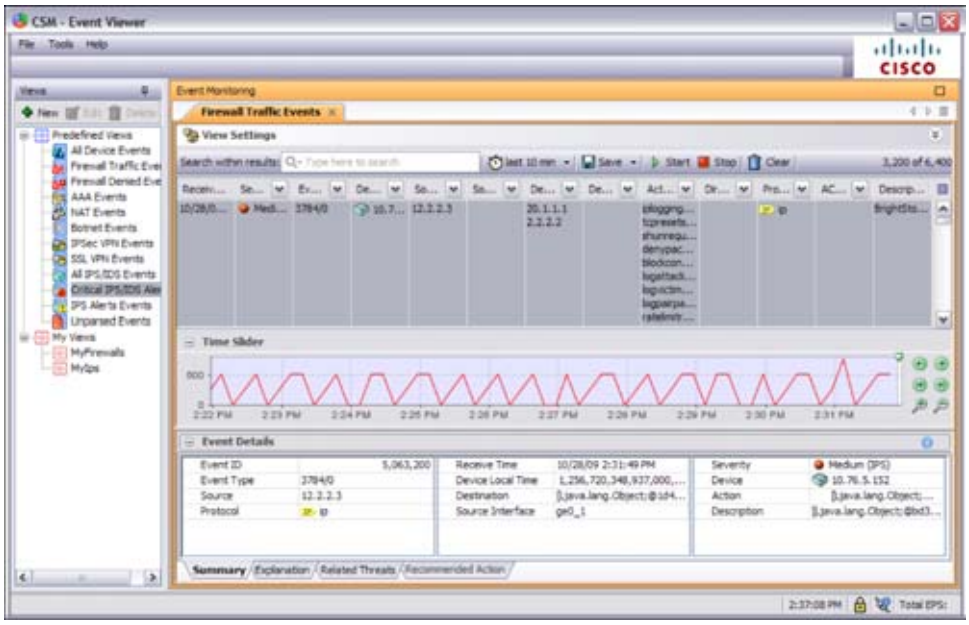
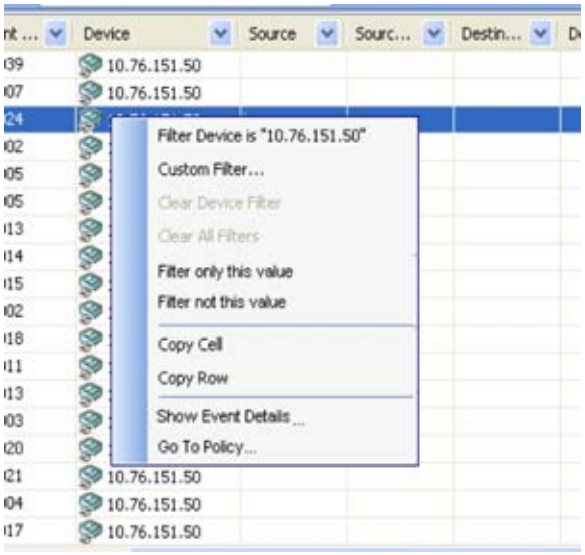
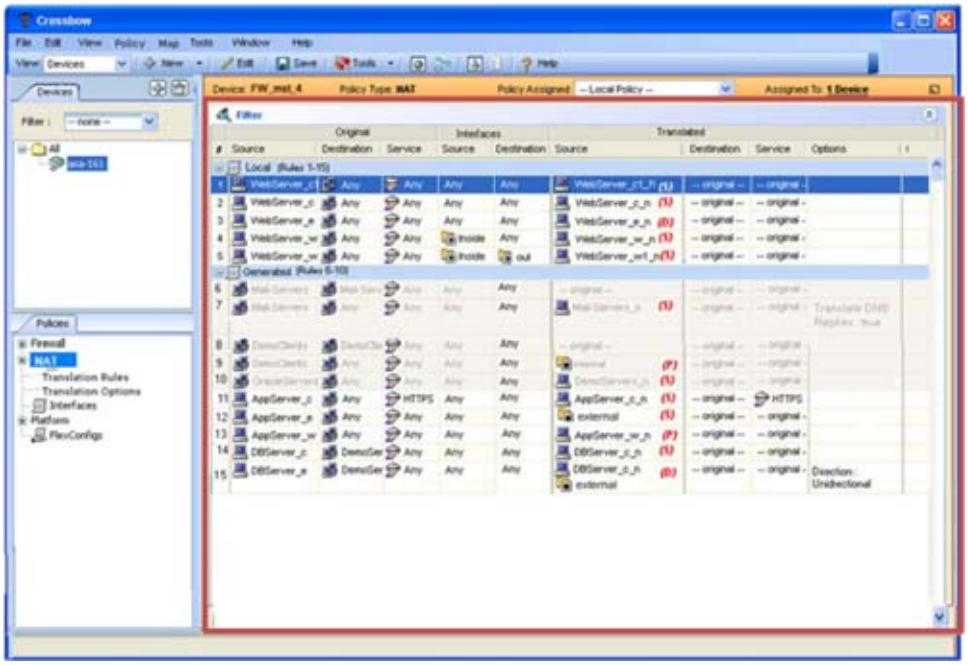


図 2　イベントからポリシーへのナビゲーション



All contents are Copyright © 1992–2010 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

図 3　簡素化された NAT ポリシー



機能概要

表 1 に、Cisco Security Manager 4.0 の機能と利点を示します。

表 1　Cisco Security Manager 4.0 の機能と利点

機能	利点
ファイアウォール設定	• 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 FWSM、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 Cisco ISR プラットフォーム向けのポリシーを一元的に設定できます。 • 管理者は Zone-Based Firewall（ZBF; ゾーンベース ファイアウォール）ポリシー設定を、サポート対象のデバイス プラットフォームで導入できるようになりました。 • Cisco ASA プラットフォームでの Botnet Traffic Filter サポートによって、アプリケーション層のインスペクションと、ボットネットによる「コール ホーム」アクティビティのブロックが可能です。 • Cisco IOS ソフトウェアベース デバイス プラットフォーム対応のコンテンツ フィルタリング サポートによって、詳細なコンテンツ インスペクションに基づいたトラフィック フィルタリングが可能です。 • Cisco Security Manager ソフトウェアは、すべてのプラットフォームに対して単一のルール テーブルを提供します。お客様は、1 つの管理ツールを使用して異なるデバイス プラットフォームを管理できます。 • ポリシー クエリー機能によって、ワイルドカードを含め、特定の発信元、宛先、およびサービス フローに一致するルールが表示されます。この機能を使用すると、管理者はより効率的にポリシーを定義できます。 • 設定を簡単にするために、デバイス情報をデバイス リポジトリまたは設定ファイルからインポートしたり、ソフトウェアで追加したりできます。さらに、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。この機能によって、最初のセキュリティ管理セットアップが簡単になります。 • インターフェイス ロールを使用すると、スケーラブルな方法でルール ポリシーをインターフェイスのグループに適用できます。この機能によって、Cisco Security Manager を使用して一元的に、デバイスのグループを柔軟に管理できます。
IPS 設定	• 管理者は Cisco Security Manager を使用して、Cisco IPS 4200 シリーズ センサー、Cisco ASA Advanced Inspection and Prevention Security Services Module（AIP-SSM）、Cisco ASA Advanced Inspection and Prevention Security Services Card（AIP-SSC）、Cisco Catalyst 6500 Series Intrusion Detection System Services Module 2（IDSM-2）、Cisco IDS ネットワーク モジュール、Cisco IPS Advanced Integration Module（AIM）、および Cisco IOS IPS 用の IPS ベースの設定およびアップデート ポリシーを簡単かつ効果的に管理できます。 • Cisco IPS センサー ソフトウェア バージョン 7.0 および 6.2 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革新的なテクノロジーを組み合わ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、アプリケーション不正使用などの悪意のあるトラフィックを、ビジネスの継続性に影響を及ぼす前に正確に識別、分類、および阻止します。 • Cisco IPS センサー ソフトウェア バージョン 7.0 の新機能には、グローバル相関やレピュテーションスコアベースのポリシー設定などがあります。これらの機能によって、セキュリティの脅威の相関付けが可能になり、ネットワーク セキュリティが強化されます。

All contents are Copyright © 1992–2010 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

機能	利点
	• 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 ソフトウェアでき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 シスコの自己防衛型ネットワークの中核として、Cisco IOS IPS は、悪意のあるトラフィックまたは打撃を与えるトラフィックをリアルタイムで正確に識別、分類、阻止またはブロックするインテリジェンスによって、ネットワークの自己防御を可能にします。 • Cisco IPS シグニチャ アップデートを把握することで、企業にシグニチャを展開する前に Cisco IntelliShield Alert Manager Service で把握できるとともに、新規および更新され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。Cisco IPS セキュリティ リサーチ チームの推奨デフォルトを即時に把握することで、お客様はシグニチャ アップデートを配布する前に自身の環境に合わせて調整できるようになります。 • Cisco IPS 更新ウィザードを使用すると、ステータスや詳細情報を通知して、自動 IPS アップデート、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。 • Cisco Security Monitoring, Analysis, and Response System（Cisco Security MARS）との相互コラボレーションによって、ポリシー展開の変更を即時に把握してイベントや異常の検出を行うことができます。これによって、履歴およびリアルタイム イベントのポリシーの起動が可能になり、Cisco Security Manager ポリシーをインバンドに保ちつつ、ネットワーク運用チームとセキュリティ運用チームのコラボレーションをより強固にします。把握と相互コラボレーションによって、イベント検査やトラブルシューティングが減り、解決時間が短縮されます。Cisco Security Manager と Cisco Security MARS のコラボレーションによって、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、ネットワークが脆弱性にさらされる機会が減少します。 • IPS シグニチャ ポリシーとイベント アクション フィルタは、どのデバイスにも継承および割り当てが可能です。その他のすべての IPS ポリシーは、ほかの IPS デバイスに割り当て可能であり、共有できます。IPS 管理には、ポリシー ロールバック、構成アーカイブ、シグニチャのクローニングまたは作成も含まれます。デバイス間でのポリシーのコピーによって展開の労力を減らすことで、効率的な管理が可能になり、Total Cost of Ownership（TCO; 総所有コスト）が削減されます。 • IPS アップデート管理および IPS サブスクリプション ライセンス アップデートによって配布が合理化されます。これによってユーザは、IPS ソフトウェア、シグニチャ アップデート、ライセンスをローカル ポリシーおよび共有ポリシーに基づいて管理できます。 • IPS ライセンスおよびシグニチャ アップデート用の Cisco NT LAN Manager Version 2（NTLMv2）プロキシ認証によって、Microsoft Windows ベースのクライアント認証がサポートされます。 • シグニチャ、イベント アクション フィルタ、シグニチャ デルタ設定などの一部の IPS 機能の CSV（Comma-Separated Values）エクスポートによって、このデータを異なる Cisco Security Manager サーバ インスタンス間で容易に保存したり交換したりできます。
VPN 設定	• VPN ウィザードを使用すると、サイトツーサイト、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。 • ダイナミック IP と階層型証明書の両方を使用する、Group Encrypted Transport VPN（GET VPN）、Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）、および Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）IP Security（IPSec; IP セキュリティ）のサポートによって、顧客共通の VPN 展開シナリオが可能です。 • VPN および Easy VPN サービスはリモートで設定できるため、一元管理が可能です。 • セキュア デバイス プロビジョニングでのゼロタッチ展開がサポートされています。 • ヘッドエンド用の自動フェールオーバーおよびロード バランシングの設定がサポートされており、より堅牢な展開が可能です。 • Cisco ASA 5500 シリーズでの Secure Sockets Layer（SSL）VPN のサポートによって、VPN 展開に高い柔軟性がもたらされます。
イベント管理	統合されたイベント管理機能によって、管理者はステータスの監視やセキュリティ問題のトラブルシューティングが可能です。サポートされる機能には次のものがあります。 • Cisco ASA アプライアンスからの syslog メッセージおよび Cisco IPS センサーからの Security Device Event Exchange（SDEE）メッセージの受け取り • リアルタイムおよび履歴イベントの表示 • ソース ポリシーへの迅速なナビゲーションのための、ファイアウォール アクセス ルールおよび IPS シグニチャの相互関連付け • ファイアウォール、IPS、および VPN モニタリング用の事前にバンドルされたビュー セット • 選択されたデバイスまたは選択された時間範囲のモニタリング用のカスタマイズ可能なビュー • 直観的な GUI による、イベントの検索、ソート、およびフィルタリングの制御 • 一部のセキュリティ デバイスのイベント コレクションのオンとオフを切り替える管理オプション
バルク操作機能	新しいバルク操作機能によって、多くのデバイスが存在するネットワークでの管理オーバーヘッドが削減されます。機能には次のものがあります。 • ポリシー オブジェクトのバルク インポートおよびバルク エクスポート • オフライン デバイスのバルク追加 • デバイスレベルのオーバーライドのバルク インポート
統合セキュリティ サービスの管理	Cisco Security Manager では、VPN の Quality of Service（QoS）、ルーティング、Network Admission Control（NAC; ネットワーク アドミッション コントロール）などの統合セキュリティ サービスの管理が可能です。
柔軟なデバイス グループ化オプション	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反映することができます。グループ内のすべてのデバイスを 1 つのデバイスのように簡単に管理できます。

All contents are Copyright © 1992–2010 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

機能	利点
複数のアプリケーション ビュー	Cisco Security Manager は、アプリケーションの複数のビューを提供して、さまざまな使用例やエクスペリエンス レベルをサポートします。デバイス中心のビューは、不慣れなユーザや 1 つのデバイス マネージャの使用に慣れているユーザに便利です。マップ中心のビューは、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 コンテキスト間の包含関係を視覚化するのに役立ちます。ポリシー中心のビューでは、効率が高くスケーラブルな複数デバイスの管理が可能です。
Policy Object Manager	ネットワーク アドレス、サービス、デバイス設定、時間範囲、VPN パラメータなどを表すオブジェクトを作成して、再利用することができます。オブジェクトは、1 回定義すると何回でも使用できるので、値を手動で入力する必要がありません。
Deployment Manager による柔軟な展開オプション	Cisco Security Manager は、デバイスまたはファイルへのオンデマンド展開とスケジュール展開の両方をサポートします。
ロールバック	Cisco Security Manager では、必要に応じて以前の設定にロールバックできます。
ロールベースのアクセス コントロール	Cisco Security Manager では、適切に制御を行いながら複数の管理者に対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 Access Control Server（ACS）で追加ロールを使用することもできます。
ワークフロー	Cisco Security Manager では、ポリシーの展開中に、正式な変更管理やトラッキングによって各管理者に特定のタスクを割り当てることができるオプションがあります。ワークフローによって、スタッフのコラボレーション（たとえば、ネットワーク運用とセキュリティ運用の間など）が向上します。
分散型の展開方法（Auto Update Server、Cisco Network Services Configuration Engine）	Cisco Security Manager は、多数のリモートのファイアウォールへのアップデートを簡素化します（ダイナミック アドレスまたは NAT アドレスを含んでいる場合もあります）。これは、ネットワーク リンクが断続的にあり、最低限の技術スタッフしかいないようなリモート サイトを持つ顧客にとって価値のある機能です。
運用管理	一緒に含まれているアプリケーションの CiscoWorks Resource Manager Essentials（RME）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。
状態とパフォーマンスのモニタリング	一緒に含まれているアプリケーションの Cisco Performance Monitor は、シスコの VPN デバイスおよび特定のセキュリティ サービス向けの、状態およびパフォーマンスのモニタリング データを提供します。

技術仕様

Cisco Security Manager 4.0 の詳細なハードウェア仕様およびサイズに関するガイドラインは、製品の出荷開始（FCS）前に提供されます。

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/JP/support/public/nav/lll_280033778_4_221.shtml にある「Cisco Security Manager インストレーション ガイド」を参照してください。

デバイス サポート

表 2 は、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たものです。サポートされるデバイス ソフトウェア バージョンなどの詳しい一覧は、http://www.cisco.com/JP/support/public/nav/lll_280033778_3_210.shtml にある「Supported Devices and Software Versions for Cisco Security Manager 4.0」[英語] を参照してください。

表 2　Cisco Security Manager でサポートされるシスコのデバイスの概要

サポートされるデバイス
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（800、1800、2800、および 3800 シリーズ） Cisco 第 2 世代サービス統合型ルータ（1900、2900、および 3900 シリーズ）
Cisco 1000 シリーズ アグリゲーション サービス 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

All contents are Copyright © 1992–2010 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

サポートされるデバイス
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（VPN SM）
Cisco 7600 シリーズ/Catalyst 6500 シリーズ IPsec VPN 共有ポート アダプタ（VPN SPA）
Cisco Catalyst 6500 シリーズ IDSM-2
Cisco IPS 4200 シリーズ センサー
Cisco ASA 5500 シリーズ用 Cisco AIP-SSM
Cisco ASA 5500 シリーズ用 Cisco AIP-SSC
サービス統合型ルータ用 Cisco IPS AIM
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 デスクトップ スイッチ

オプションの CiscoWorks RME 4.3 でサポートされるデバイスの一覧については、http://www.cisco.com/JP/support/public/nav/lll_268439660_3_210.shtml にあるサポート対象デバイス表を参照してください。

発注情報

Cisco Security Manager 製品速報には、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。速報は、http://www.cisco.com/web/JP/product/hs/security/csm/index.html で公開されています。

シスコのサービス

シスコは、サービスに対するライフサイクル アプローチにより、シスコのパートナーとともに幅広い一連のセキュリティ サービスを提供しています。これらサービスを利用すると、重要なビジネス プロセスを攻撃や中断から守り、プライバシーを保護し、ポリシー管理や法令準拠管理をサポートするネットワーク プラットフォームの設計、実装、運用、および最適化が可能になります。

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の拡張を進めていただくために、シスコのサービスを是非お役立てください。シスコのサービスの詳細については、
http://www.cisco.com/web/JP/services/portfolio/as/as_security.html を参照してください。

- **Cisco Security Intelligence Operations（SIO）**サービスは、脅威や脆弱性の情報および分析に関する早期の警告や、Cisco IPS シグニチャ、および緩和手法の集中管理を提供します。http://www.cisco.com/security/ [英語] にアクセスして、Cisco SIO をブックマークに登録してください。
- **Cisco Security IntelliShield Alert Manager Service** は、脅威と脆弱性警告に関する、カスタマイズ可能な Web ベースのサービスを提供します。このサービスを利用すると、使用する環境に存在する潜在的な脆弱性に関する正確で信頼性の高い情報に、簡単かつタイムリーにアクセスできます。
- **Cisco Software Application Support（SAS）Service** は、Cisco Security Manager の常時稼動を支援します。テクニカル サポートとソフトウェア アップデートに 24 時間アクセスが可能です。
- **Cisco Security Optimization Service** は、ピーク ネットワークの健全性維持に役立ちます。ネットワーク インフラストラクチャは、機敏性と適応性に富むビジネスの基盤です。Cisco

All contents are Copyright © 1992–2010 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Security Optimization Service は、変化を続けるセキュリティの脅威に対応するために、計画と評価、設計、パフォーマンス調整、システム変更に対する継続的なサポートを組み合わせて提供することによって、進化し続けるセキュリティ システムをサポートします。

Cisco Security Manager ソフトウェアは、Cisco Software Application Support（SAS）サービス契約によるテクニカル サポート サービスの対象です。これには次のものがあります。

- Cisco Technical Assistance Center（TAC）に無制限にアクセスして、受賞実績のあるサポートを得ることができます。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、シスコのソフトウェア アプリケーションの専門家による技術サポートが提供されます。サポートは年中無休 1 日 24 時間、全世界で利用できます。
- ネットワーク セキュリティ問題の診断に役立つアプリケーション ツールおよびテクニカル ドキュメントの堅牢なリポジトリである Cisco.com に登録してアクセスできます。新しいテクノロジーや先進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、設定ドキュメント、およびケース管理ツールを使用して、社内の技術能力を向上させることができます。
- アプリケーション ソフトウェアのバグ修正およびメンテナンス、マイナー ソフトウェア リリースにアクセスできます。

関連情報

Cisco Security Manager 4.0 の詳細については、http://www.cisco.com/web/JP/product/hs/security/csm/index.html をご覧いただくか、担当のアカウント マネージャまたはシスコの Authorized Technology Provider（ATP; 認定技術プロバイダー）にお問い合わせください。ask-csmanager@cisco.com まで E メールでお問い合わせいただくこともできます。

All contents are Copyright © 1992–2010 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

©2010 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。(0809R)
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。

お問い合わせ先

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
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間:平日10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/

10.08