

Cisco Security Agent バージョン 6.0

常時稼働のエンドポイント セキュリティ

Cisco® Security Agent 6.0 は、アップデート不要の攻撃防御機能、ポリシーによるデータ損失防止 (DLP; Data Loss Prevention) 機能、およびシグニチャベースのウイルス検出機能を 1 つのエージェントに搭載した、初のエンドポイント セキュリティ ソリューションです。これらの機能を独自の方法で組み合わせることで、サーバやデスクトップを高度な Day Zero 攻撃から保護し、シンプルな管理インフラストラクチャのなかで利用の許可とコンプライアンス ポリシーの適用を実現します。

アップデート不要の防御機能

Cisco Security Agent は、標的型攻撃、悪意のあるモバイル コード、ルートキット、ワーム、および Day Zero 攻撃に対する先進のエンドポイント防御機能を提供します。アップデート不要 (ゼロ アップデート) の防御機能により、公開済みまたは公開前のシステムやアプリケーションの脆弱性を悪用した、未知の 익스プロイトや亜種 (バリエーション) に対処することができます。Cisco Security Agent を利用すると、オペレーティング システムやアプリケーションへの脆弱性パッチ適用のためのサービス停止が許されない重要なサーバを、常に保護できます。これにより、脆弱性が公開されるたびに急いでパッチを適用する必要がなくなるため、パッチの適用に伴うダウンタイムと IT 運用コストを最小限に抑えることができます。

データ損失防止

Cisco Security Agent を使用すると、すべてのエンドポイントにわたって、機密データを確認および制御し、エンドユーザの操作と標的型マルウェアのどちらについてもデータ損失を防止できます。新たに追加されたコンテンツ スキャン機能は、ローカル ファイル内のクレジットカード番号、社会保障番号、およびカスタム定義した機密データを検出します。これらの機密ファイルへのアクセスは監査およびポリシー制御され、リムーバブル デバイスや安全性の低いネットワーク アプリケーションを通じた悪意のあるデータ移転の防止を実現します。Cisco Security Agent にはカスタマイズが可能なフィードバック クエリー機能があり、エンドユーザの教育および企業のセキュリティ ポリシー強化のために役立てることができます。正当性 (Justification) オプションは、従業員の生産性と重要なデータへのタイムリーなアクセスを損なうことなく、監査証跡 (Audit Trail) 機能を提供します。さらに、エンドユーザ インターフェイスは 11 種類の言語にローカライズされているため、さまざまな国で簡単に導入できます。

シグニチャベースのウイルス対策機能

エンドポイントでマルウェア攻撃を阻止する場合、振る舞いに基づく制御が一般的かつ最も信頼性の高い手段ですが、シグニチャベースのウイルス対策は、既知のマルウェアを検出する際に重要な役割を果たします。シグニチャベースのウイルス対策機能を新たに導入したことで、マルウェアを名前前で特定できるため、エンドポイントからマルウェアを確実に削除できる可能性が高くなります。また、ウイルス対策にシグニチャベースのテクノロジーの使用が義務付けられた規制の遵守にも対応できます。

コンプライアンス ポリシーと利用許可ポリシーの監査と適用

Cisco Security Agent の強固なポリシー エンジンは、コンプライアンスの監査および制御機能を提供します。事前に定義およびカスタマイズされたポリシーを集中的に管理することで、アクティビティの効率的なレポートと監査が可能になります。シスコでは、さまざまな定義済みのコンプライアンスポリシーと利用許可ポリシーを用意しています。次に、いくつかの例を示します。

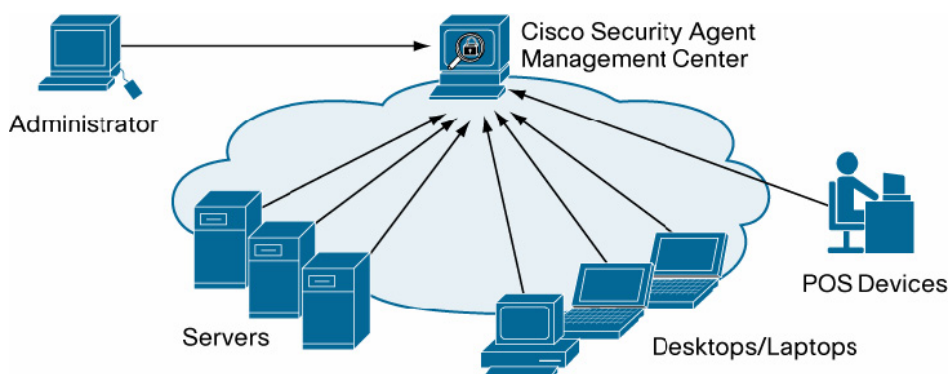
- **Payment Card Industry Data Security Standard (PCI DSS) ポリシー**を適用すると、ベンダーが監査中に見落としがちな要件など、コンプライアンスへの準拠性を制御および監査できます。
- **ロケーションベース ポリシーの適用**によって、オフィス外にいるユーザに、VPN 接続の使用を義務付けることができます。
- **USB ドライブへの読み書きの無効化**
- **ワイヤレス通信**を、エンドポイントが有線ネットワークにも接続されている場合に制限できます。

ネットワーク セキュリティの統合

Cisco Security Agent が提供する、先進のネットワーク セキュリティとエンドポイント セキュリティの統合により、自己防衛型ネットワークの導入効果が向上します。

- **Cisco Network Admission Control** は、ネットワークへの接続を許可する前に実行されるポスチャチェックにおいて、Cisco Security Agent のステータスを利用します。
- **シスコのネットワーク IPS デバイス**は、Cisco Security Agent で収集したホスト情報を受信します。これにより、ネットワーク内で実行する IPS 処理の精度が向上します。
- **CS-MARS (Cisco Security Monitoring, Analysis, and Response System)**は、Cisco Security Agents からセキュリティ情報を収集します。これにより、CS-MARS では、ネットワーク全体の脅威の特定や調査を、より効果的に実施できます。
- **Cisco VPN リモート アクセス クライアント**は、Cisco Security Agent のパーソナル ファイアウォールおよびホスト侵入防御機能によって保護されます。
- **Cisco IronPort®** によるネットワーク検査の対象範囲を、ユーザがローミングを利用して企業ネットワークへアクセスする場合に VPN 接続の確立を義務付ける Cisco Security Agent ポリシーを用いて、拡張することができます。
- **Cisco Security Agent のネットワークトラフィック マーキング ポリシー**は、送信元アプリケーションに基づいて、より詳細かつ管理しやすくネットワークを細分化できます。Cisco ASA 5500 シリーズおよび Cisco PIX® セキュリティ アプライアンスのファイアウォールおよびアプリケーション検査機能と組み合わせて使用すると、特定のアプリケーションからのトラフィックを検査できます。
- **シスコ ユニファイド コミュニケーション サーバ**は、攻撃阻止のために、Cisco Security Agent をインストールして出荷されます。

図 1



集中管理

CSA-MC (Management Center for Cisco Security Agents) は、すべてのエージェントを集中的に管理するためのさまざまな管理機能を提供します。振る舞い検知ポリシー、データ損失防止、およびウイルス対策の各機能はすべて、1 つの設定およびレポート インターフェイスに統合されます。ロールベースの Web ブラウザ アクセスにより、エージェント ソフトウェア配布パッケージの作成、セキュリティ ポリシーの作成または修正、アラートの監視、レポートの生成などの作業を管理者が簡単に行うことができます。各エージェントは、マネージャと通信できない場合 (たとえば、ノート型パソコンを使用するリモート ユーザがまだ VPN 経由で接続していない場合) にも、自律的に動作してセキュリティ ポリシーを適用します。

表 1 に、Cisco Security Agent バージョン 6.0 の仕様を示します。

表 1 エージェントの仕様

仕様	詳細
サーバエージェント	<ul style="list-style-type: none"> • Windows 2003 Server • Windows 2000 Server および Advanced Server • Solaris 9 SPARC アーキテクチャ (64 ビット カーネル) • Solaris 8 SPARC アーキテクチャ (64 ビット カーネル) • Red Hat Enterprise Linux 4.0 ES および AS • Red Hat Enterprise Linux 3.0 ES および AS
デスクトップ エージェント	<ul style="list-style-type: none"> • Windows Vista • Windows Embedded Point of Service (WEPOS) • Windows XP Professional • Windows XP Tablet Edition • Windows 2000 Professional • Red Hat Enterprise Linux 4.0 WS • Red Hat Enterprise Linux 3.0 WS
ローカリゼーション	<ul style="list-style-type: none"> • 中国語 • 英語 • フランス語 • ドイツ語 • イタリア語 • 日本語 • 韓国語 • ポーランド語 • ポルトガル語 • ロシア語 • スペイン語

シスコのサービスおよびサポート

シスコとパートナーは、サービスのライフサイクル アプローチという立場から、幅広いセキュリティ サービス ポートフォリオを提供しています。そのため、企業では、重要なビジネス プロセスを攻撃 やサービス の中断から保護して機密を保持するとともに、ポリシーおよび規制への準拠性管理機能をサポートするネットワーク プラットフォームを、設計、実装、運用、および最適化できます。

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是非お役立てください。シスコが提供するサービスは次のとおりです。

- **Cisco Security Center** は、脅威のインテリジェントな早期アラート、脅威と脆弱性の分析、Cisco IPS シグニチャ、および脅威緩和技術といったあらゆる情報を提供します。Cisco Security Center (www.cisco.com/security) にアクセスしてください。
- **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アラート サービスを提供します。これにより、自社環境の潜在的な脆弱性について、タイムリーかつ正確で信頼できる情報に簡単にアクセスできます。
- **Cisco Security Optimization Service** — 即応性を備えた適応型のビジネス基盤を提供できるネットワーク インフラストラクチャは、ますます重要性を増しています。Cisco Security Optimization Service は、計画と評価、設計、パフォーマンス チューニング、およびシステム変更の継続的サポートを組み合わせることで、絶えず変化する新たなセキュリティ上の脅威に対処するために、常に進化するセキュリティ システムをサポートします。このサービスにより、コアネットワーク インフラストラクチャへのセキュリティ統合が可能になります。
- **Cisco Software Application Support Services, plus Upgrades (SASU)** では、テクニカルサポート、ソフトウェア アップデート、および主要なアップグレードに 24 時間いつでもアクセスできるようにすることで、Cisco Security Agent のアベイラビリティ、機能性、および信頼性を保証します。
- **[Cisco Security Agent Implementation Service](#)** は、企業環境への Cisco Security Agent の統合を支援するため、専門家によるセキュリティ分析、計画、設計、および実装サービスを提供します。

関連情報

[Cisco Security Agent 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。Cisco Security Agent の詳細については、<http://www.cisco.com/jp/go/csa/> を参照してください。

Cisco Security Services の詳細については、http://www.cisco.com/web/JP/services/portfolio/serv_tech/security/ を参照してください。

©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