

# Cisco Security Agent

シスコは Cisco Security Agent エンドポイント セキュリティ ソフトウェアを追加することで、大規模な企業ネットワークをセキュリティの脅威から保護する、最も包括的なポートフォリオをお客様に提供します。

次世代の Cisco® Security Agent ネットワーク セキュリティ ソフトウェアは、サーバおよびデスクトップコンピューティングシステム（「エンドポイント」とも呼びます）をセキュリティの脅威から保護します。Cisco Security Agent には、悪意のある動作を未然に識別し防御するという、これまでのエンドポイントセキュリティソリューションには見られない機能があり、これによって、既知であるか未知であるかを問わず、企業のネットワークおよびアプリケーションの脅威となりうるセキュリティリスクを排除します。Cisco Security Agent はシグニチャに依存するのではなく、動作を解析するため、少ない運用コストで堅牢なセキュリティ保護を実現します。

## 利点

- ホストへの侵入の防御、分散ファイアウォール、悪質なモバイルコードからの保護、オペレーティングシステムの整合性の保証、および監査ログの統合をすべて1つのエージェントで提供することにより、Cisco Security Agent の複数のエンドポイントセキュリティ機能を集約し、拡張します。
- ポート スキャン、バッファ オーバフロー、トロイの木馬、不正パケット、悪意のある HTML 要求、電子メール型ワームなど、あらゆる種類の攻撃から保護します。

- 既知および未知の攻撃を「アップデートせずに」防御します。
- Unix および Windows のサーバやデスクトップ コンピュータに優れた保護を提供します。
- Web サーバやデータベースをアプリケーション別に保護します。
- オープンで拡張可能なアーキテクチャにより、企業のポリシーに従ってセキュリティを定義し、実施できます。
- 企業規模のスケーラビリティによって、Cisco Security Agent では、1つのマネージャにつき、数千のエージェントまで拡張可能なアーキテクチャが提供されます。
- Cisco PIX®、Cisco Secure IDS および Cisco VPN セキュリティ デバイスとの統合管理を実現します。
- 「Are You There」(AYT) 関数により Cisco VPN と統合します。

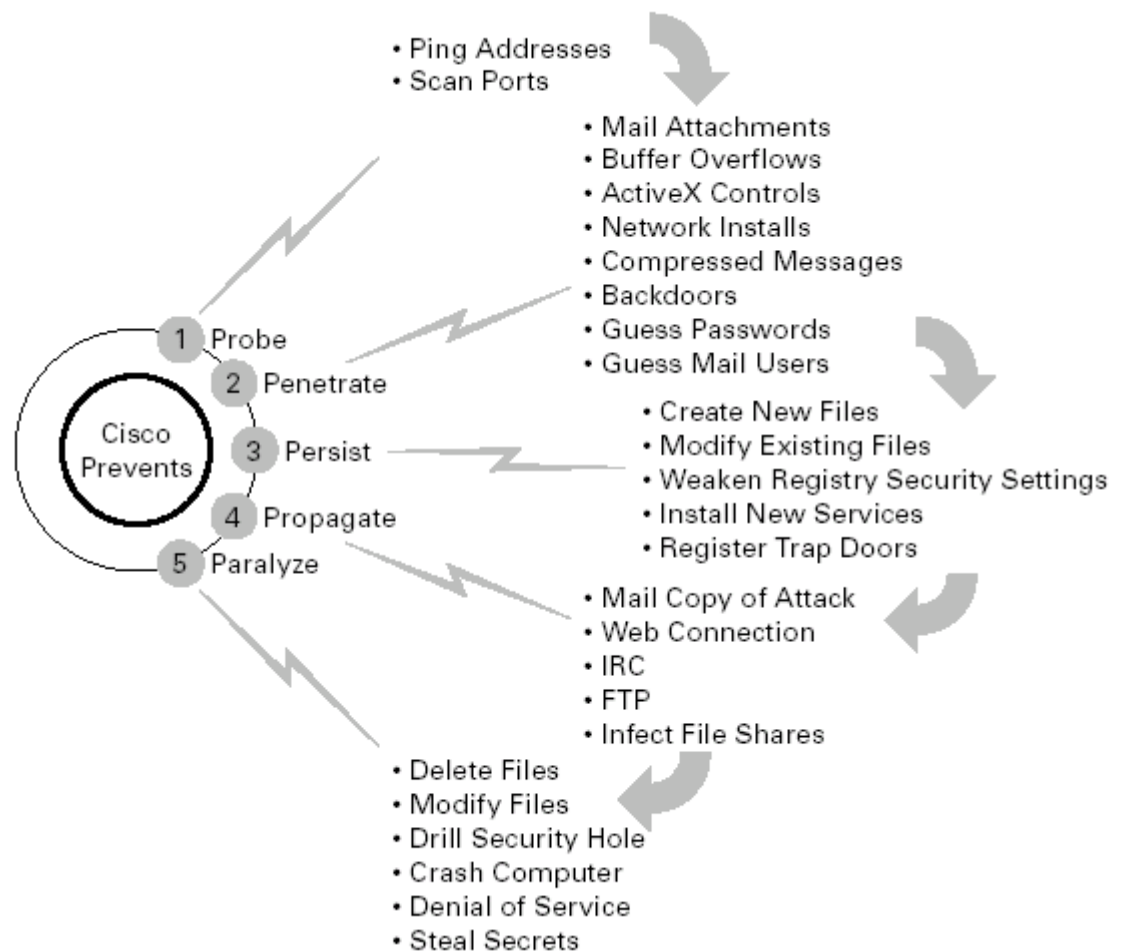
## 新しい未知の攻撃への対応

最近注目を浴びた Code Red や SQL Slammer ワームなどの攻撃からもわかるように、進化し続ける新たな攻撃に対して従来のテクノロジーの対応能力には限界があります。お客様が求めているのは、攻撃のすべての段階を通じて新しい未知の脅威から保護するホストセキュリティです。



ネットワークシステムへの攻撃には通常いくつかの段階があります。シスコでは、境界からサーバまで、あるいはファイルレベルの段階といった、あらゆる段階で起こりうるセキュリティ侵犯に有効であるのは、階層型のアプローチしかないと認識しています。Cisco Security Agent は攻撃のすべての段階を通じてホストへの被害を予防的に防御します。それに対して他のテクノロジーは初期段階での保護を提供するだけであり、それもシグニチャがあらかじめわかっている場合に限られます。Cisco Security Agent (図 1) は、特にシグニチャが不明な新しい攻撃から保護するように設計されています。

図 1  
攻撃のライフ サイクル



### Cisco Security Agent ソリューション

Cisco Security Agent はホストをベースとしたエージェントによって構成されています。これらのエージェントは重要なデスクトップ コンピュータやサーバに展開され、CiscoWorks VPN/Security Management Solution (VMS) 上で稼動している Management Center にレポートを送信します。エージェントは、管理インターフェイス、およびエージェントと管理センター間の通信に HTTP プロトコルと Secure Sockets Layer (SSL) プロトコル (128 ビット SSL) を使用します。すべての設定は CiscoWorks VMS を介して構成され、アラートは、CiscoWorks Security Monitor (SecMon) を介して、シスコの他のセキュリティ製品からのアラートと統合されます。



## エージェントのアーキテクチャ

Cisco Security Agent はアプリケーションとカーネルの間に位置し、基盤となるオペレーティング システムの安定性とパフォーマンスにほとんど影響を与えることなく、アプリケーションの動作を最大限に捕捉します。エージェントの持つ独自のアーキテクチャは、ファイル、ネットワーク、およびレジストリソースへのシステムコールと、メモリ ページ、共有ライブラリ モジュール、COM オブジェクトなどの動的なランタイム リソースへのオペレーティング システム コールをすべて代行受信します。エージェントは独自のインテリジェンスを利用し、特定のアプリケーションまたはすべてのアプリケーションにとって適切ではない動作または許容されない動作を定義するルールに基づいて、これらのシステムコールの動作を関連付けます。この関連付けと、その後のアプリケーションの動作を理解することにより、セキュリティ担当者の指示に従って、未知の方法によるシステムへの侵入を阻止することが可能になります。

アプリケーションがなんらかの操作を実行しようとする時、エージェントはその操作をアプリケーションのセキュリティポリシーと照合して操作を継続するか拒否するかをリアルタイムで判断し、要求のロギングが適切かどうかを決定します。セキュリティポリシーは、IT 管理者とセキュリティ管理者が割り当てるルールが集約されたものです。これは保護対象であるサーバやデスクトップにおいて、全社的、または個人レベルで割り当てられます。これらのルールにより、要求されたリソースにアプリケーションが安全にアクセスできるようになります。また、分散ファイアウォール、オペレーティングシステムのロックダウン、整合性の保証、悪質なモバイルコードからの保護、および監査イベントの収集機能をサーバおよびデスクトップのデフォルトポリシーに実装するセキュリティポリシーを組み合わせることで、Cisco Security Agent は公開された企業システムにおいて重層的な防御を提供します。

悪質な動作を阻止することが保護の基本となっているため、デフォルトのポリシーを更新しなくても、既知の攻撃と未知の攻撃の両方に対処できます。関連付けはエージェントと Management Center コンソールの双方で実行されます。エージェントで関連付けを行うことにより、実際の攻撃と単なる誤用を、正当なアクティビティを阻止することなく識別できるため、精度が大幅に向上します。また、Management Center での関連付けでは、ネットワーク ワームや分散スキャンなどのグローバルな攻撃が識別されます。

## 集中管理

Management Center for Cisco Security Agent には、CiscoWorks VMS プラットフォームによってすべてのエージェントを中央から管理するための、さまざまな管理機能があります。ロールベースで、Web ブラウザを使用してどこからでもアクセスできるため、管理者はエージェント 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と修正、アラートの監視、レポートの生成などを簡単に行うことができます。また、完全に設定されたデフォルトポリシーが最初から 20 以上定義されているため、数千単位のエージェントを社内全体に簡単に展開できます。エージェントは「IDS モード」で展開することも可能です。IDS モードでは、アクティビティに対してアラートが発生しますが、アクティビティ自体は阻止されません。

Management Center for Cisco Security Agent には、ウィザードの調整など、シンプルではあるものの強力なカスタマイズ機能があり、管理者はデフォルト ポリシーをそれぞれの環境に迅速に適応させることができます。独自のニーズや要件に合わせたルールの修正や新規作成も簡単です。また、監査適合要件のヘルプとして「ルール説明」機能があり、指定したルールまたはポリシーについての説明が出力されます。



エージェントは Management Center for Cisco Security Agent から直接サーバとデスクトップに配布され、このマネージャから制御および更新されます。マネージャと通信できない場合（たとえば、リモートラップトップユーザが VPN 経由でまだ接続していない場合など）、エージェントはセキュリティポリシーを実行し続けるなど、各エージェントは自律的に動作します。発生したセキュリティアラートはエージェントによってすべてキャッシュされ、通信が回復したときにマネージャにアップロードされます。

シスコ製品には、他にも Management Center for Cisco Security Agent 用のスナップインアプリケーションである、Cisco Security Agent Profiler があります。これは、総合的にデータを解析したり、カスタムのアプリケーションや環境に応じてポリシーを構築するツールとして使用されます。プロファイラは実際のアプリケーションの動作を解析し、任意のアプリケーションを保護するカスタムポリシーを作成します。これは、お客様独自の環境に合わせて高度にカスタマイズされた複雑なアプリケーションにも対応しています。

## 技術仕様

Server Agent のサポートするオペレーティング システムは次のとおりです。

- Windows 2000 Server および Advanced Server
- Windows NT 4.0 Server および Enterprise Server (Service Pack 5 以降)
- Solaris 8 SPARC アーキテクチャ (64 ビット カーネル)

Desktop Agent のサポートするオペレーティング システムは次のとおりです。

- Windows NT Workstation (Service Pack 5 以降)
- Windows 2000 Professional
- Windows XP Professional

CiscoWorks Management Center for Cisco Security Agent を使用できるオペレーティング システムは次のとおりです。

- Windows 2000 Server および Advanced Server (Service Pack 3)

次のデフォルト セキュリティ ポリシーが用意されています（必要に応じてこれらを組み合わせることができません）。

- 汎用サーバ
- 汎用デスクトップ
- Microsoft IIS v4.0 および v5.0
- Apache v1.3
- Microsoft SQL Server
- Microsoft Exchange
- Sendmail
- Domain Name System (DNS; ドメイン ネーム システム)
- Dynamic Host Control Protocol (DHCP; 動的ホスト制御プロトコル) サーバ
- ネットワーク タイム サーバ
- ドメイン コントローラ
- 分散ファイアウォール
- ブラウザの保護



- インスタント メッセージのコントロール
- Microsoft Office の保護
- データ盗難の阻止
- Cisco Security Agent Manager の保護
- CiscoWorks VMS
- Cisco CallManager の保護

**使用できる言語：**

- サポートされているすべてのオペレーティング システムについて、英語（アメリカ英語）のみです。  
（日本語近日対応予定）

**インストール要件の注意：**

サポートされているのは、英語（アメリカ英語）版のオペレーティング システムのみです。  
（日本語近日対応予定）

**Server Agent: Windows**

- Windows NT 4.0 Server（Service Pack 5 以降）
- Windows NT 4.0 Enterprise Server（Service Pack 5 以降）
- Windows 2000 Server（Service Pack 3 まで）
- Windows 2000 Advanced Server（Service Pack 3 まで）
- 1 つまたは複数の Pentium プロセッサ、200 MHz 以上
- 128 MB 以上の RAM

**Server Agent: Solaris**

- Solaris 8 SPARC アーキテクチャ（64 ビット カーネル）
- 500 MHz 以上の Ultra SPARC プロセッサ
- 256 MB 以上の RAM

**Desktop Agent**

- Windows NT 4.0 Workstation（Service Pack 5 以降）
- Windows 2000 Professional（Service Pack 3 まで）
- Windows XP Professional（Service Pack 0 または 1 まで）
- 1 つまたは複数の Pentium プロセッサ、200 MHz 以上
- 128 MB 以上の RAM



## CiscoWorks VMS with Management Center for Cisco Security Agent

- Windows 2000 Server または Advanced Server (Service Pack 1 または Service Pack 2)
- 500 MHz 以上の Pentium プロセッサ
- 384 MB 以上の RAM
- 2 GB ディスク

### 発注情報

Cisco Security Agent を構成する主要コンポーネントは、エージェントと Management Center for Cisco Security Agent です。エージェントを実行するためには Management Center for Cisco Security Agent が必要です。ライセンスを受けていないコンソールにエージェントをライセンスすることはできません。Management Center for Cisco Security Agent は、別途ライセンスされる CiscoWorks VMS (restricted、unrestricted 共) に、同梱されています。表 1 に、Cisco Security Agent の部品番号を示します。

表 1 Cisco Security Agent の部品番号

部品番号	製品説明
CSA-SRVR-K9	Cisco Security Server Agent (Windows および Solaris)、1 エージェント
CSA-B10-SRVR-K9	10 エージェントをバンドルした Cisco Security Server Agent (Windows および Solaris)
CSA-B25-SRVR-K9	25 エージェントをバンドルした Cisco Security Server Agent (Windows および Solaris)
CSA-B50-SRVR-K9	50 エージェントをバンドルした Cisco Security Server Agent (Windows および Solaris)
CSA-B100-SRVR-K9	100 エージェントをバンドルした Cisco Security Server Agent (Windows および Solaris)
CSA-B500-SRVR-K9	500 エージェントをバンドルした Cisco Security Server Agent (Windows および Solaris)
CSA-B25-DTOP-K9	25 エージェントをバンドルした Cisco Security Server Agent
CSA-B100-DTOP-K9	100 エージェントをバンドルした Cisco Security Server Agent
CSA-B250-DTOP-K9	250 エージェントをバンドルした Cisco Security Server Agent
CSA-B500-DTOP-K9	500 エージェントをバンドルした Cisco Security Server Agent
CSA-B1000-DTOP-K9	1000 エージェントをバンドルした Cisco Security Server Agent
CSA-B5000-DTOP-K9	5000 エージェントをバンドルした Cisco Security Server Agent

©2003 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。  
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。  
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。



シスコシステムズ株式会社

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

問合せ URL: <http://www.cisco.com/jp/service/contactcenter/>

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL.03-6670-2992

電話でのお問合せは、以下の時間帯で受け付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問い合わせ先