Cisco Security Agent

Cisco® Security Agent エンドポイント セキュリティ ソフトウェアは、大規模な企業ネットワークをセキュリティ上の脅威から保護するための包括的なポートフォリオです。

Cisco Security Agent 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（いわゆるエンドポイント）をセキュリティ上の脅威から保護します。Cisco Security Agent は、従来のエンドポイント セキュリティ ソリューションにない高度な機能として、不審な動作を識別して未然に防御する機能を備えています。 これによって、企業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、既知のものであるか未知のものであるかを問わず排除します。シグニチャ マッチングに依存するのではなく、動作を解析することにより、堅牢なセキュリティ保護を少ない運用コストで実現します。

利点

Cisco Security Agent は、次のような多くの利点を備えています。

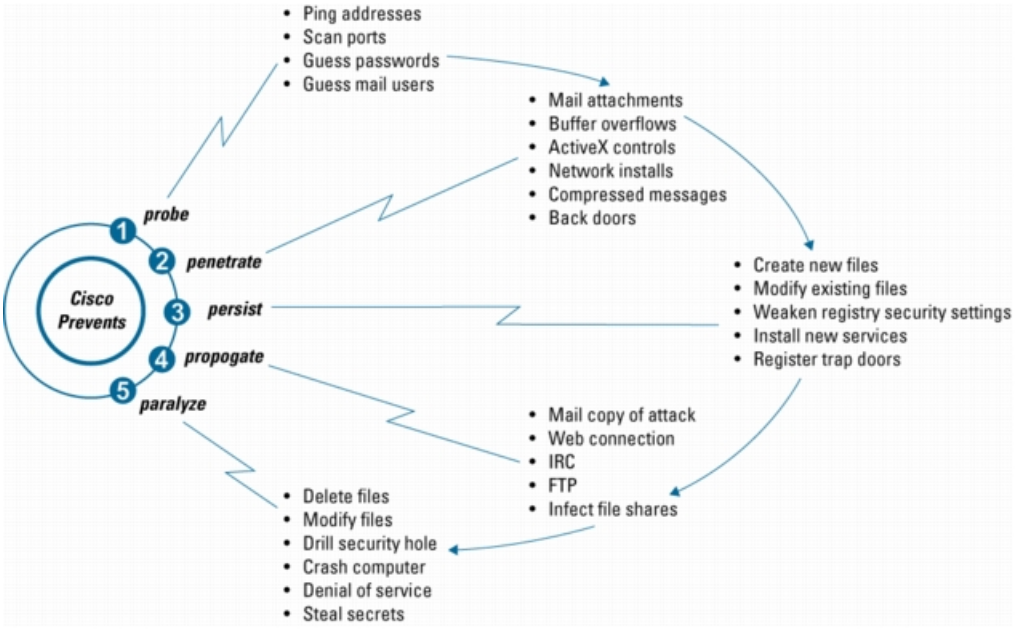
- ホストへの侵入防止、分散型ファイアウォール、悪意のモバイル コードからの保護、オペレーティング システムの整合性の保証、および監査ログの連結といった機能のすべてを 1 つのエージェントで提供し、エンドポイント セキュリティのためのさまざまな機能を集約して強化します。
- ポート スキャン、バッファ オーバーフロー、トロイの木馬、不正パケット、悪意の HTML 要求、E メール型ワームなど、あらゆる種類の攻撃に対応します。
- 既知および未知の攻撃に対する、アップデート作業が不要な防御能力を提供します。
- Unix/Windows サーバおよびデスクトップのための業界随一の保護機能を提供します。
- Web サーバおよびデータベースにアプリケーション固有の保護を提供します。
- 拡張性に優れたオープンなアーキテクチャにより、企業のポリシーに応じたセキュリティの定義および実施が可能です。
- スケーラブルなエンタープライズ アーキテクチャにより、マネージャ 1 つにつき 100,000 エージェントまで拡張できます。
- Cisco Secure IDS、Cisco VPN、および Cisco PIX® セキュリティ デバイスとの統合管理機能を備えています。
- Are You There（AYT）機能を使用して Cisco VPN と統合できます。

新種（未知）の攻撃への対処

猛威を振るった Code Red や SQL Slammer ワームなどの事例からもわかるように、進化する新種の攻撃に対しては、従来からのテクノロジーでは対応に限界があります。必要なのは、未知の脅威にも、攻撃のあらゆる段階で万全に対処できるホスト セキュリティです。

通常、ネットワーク システムへの攻撃にはいくつかの段階があります。境界を突破し、サーバやファイル レベルで発生する攻撃に対して効果的な対処ができるのは、階層型アプローチだけであるとシスコは認識しています。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既知である場合に限られます。 これに対して Cisco Security Agent は、攻撃のあらゆる段階を通じてホストへの被害を未然に防ぎます。Cisco Security Agent は、既知のシグニチャが存在しない、新種の攻撃に対する防御策として設計されています。

図 1　攻撃のサイクル



Cisco Security Agent ソリューション

Cisco Security Agent は、ミッションクリティカルなデスクトップおよびサーバにインストールするホストベースのエージェントで構成され、これらのエージェントから、Management Center for Cisco Security Agent にレポートが送信されます。この Management Center は、CiscoWorks VPN and Security Management System（VMS）上で稼働します。エージェントの管理インターフェイスおよびエージェントと Management Center 間の通信には、HTTP および 128 ビット Secure Sockets Layer（SSL）が使用されます。設定は CiscoWorks VMS を通して実行されます。また、警告は、Cisco Security Monitoring, Analysis, and Response System によって他のセキュリティ製品から発生する警告に統合されます。

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把握します。ソフトウェアは独自のアーキテクチャにより、ファイル、ネットワーク、およびレジストリ リソースに対するオペレーティング システム コールのほかに、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実行時リソースへのシステム 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、個々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不適切または許容不可とされる動作を定義したルールに基づいて、これらのシステム コール動作の関連付けを行います。この関連付けと、その後のアプリケーション動作を認識することにより、未知の方法による侵入をセキュリティ担当者の指示に従って阻止することが可能になります。

アプリケーションが何らかの動作を実行しようとすると、Cisco Security Agent はその動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、動作を続行するか拒否するかをリアルタイムで判断するとともに、要求をログに記録するのが妥当かどうかを決定します。セキュリティ ポリシーとは、保護対象のサーバおよびデスクトップに対し、個別または全社的に IT 管理者またはセキュリティ管理者が割り当てるルールの集合です。これらのルールによって、必要なリソースへの安全なアプリケーション アクセスを確保できます。Cisco Security Agent は、分散型ファイアウォール、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、悪意のモバイル コードからの保護、監査イベントの収集といった各機能を実装するセキュリティ ポリシーを、サーバおよびデスクトップのデフォルト ポリシーに組み合わせることで、外部に開かれた企業システムを階層的に保護します。

不審な動作を阻止することが保護機能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。エージェントと Management Center コンソールの両方で関連付けが実行されます。エージェントでの関連付けにより、精度が大幅に向上し、正当なアクティビティを妨害せずに攻撃と誤用を区別できます。 また、Management Center での関連付けにより、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を認識できます。

集中管理

Management Center for Cisco Security Agent は、CiscoWorks VMS プラットフォームから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。Web ブラウザを使用してどこからでもロールベースでアクセスできるので、管理者によるエージェント 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簡単に行うことができます。Management Center は、あらかじめ設定済みのデフォルト ポリシーを 20 以上組み込んだ状態で出荷されるので、数千のエージェントを簡単に全社で展開できます。エージェントを「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するアラートが生成されますが、アクティビティ自体は阻止されません。

Management Center には、シンプルでありながら強力なカスタマイズ機能（調整ウィザードなど）が備わっているので、管理者はデフォルト ポリシーを環境にすばやく適合させることができます。特別なニーズや要件に合わせたルールの修正や、まったく新規のルール作成が簡単に行えます。規制準拠の監査に役立つ機能として「ルール説明」機能があり、管理者は指定したルールまたはポリシーの機能を、人間が読める言語形式で出力できます。

エージェントは Management Center からサーバとデスクトップに直接配布され、このマネージャによって制御および更新されます。各エージェントは自律的に動作します。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、エージェントは継続的にセキュリティ ポリシーに基づく検査を実施します。その間に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。

Management Center から使用できる一連の分析レポート ツールも用意されています。展開分析機能では、すべてのエージェントにインストールされているアプリケーションの詳細、およびそのアプリケーションの使用状況に関する情報が提供されます。動作分析機能は、カスタムまたは不明なアプリケーションおよび環境に対応する包括的なデータ分析ツールです。この機能では、アプリケーションの動作に関する詳細なレポートを作成して、すべてのアプリケーションを把握できるようにします。お客様固有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ます。

技術仕様

Cisco Security Server Agent がサポートする OS:

- Windows 2003
- Windows 2000 Server および Advanced Server
- Windows NT v4.0 Server および Enterprise Server（SP 6a 以降）
- Solaris 8 SPARC アーキテクチャ（64 ビット カーネル）
- Red Hat Enterprise 3.0 ES および AS

Cisco Security Desktop Agent がサポートする OS:

- Windows NT 4 Workstation（SP 6a 以降）
- Windows 2000 Professional
- Windows XP Professional
- Red Hat Enterprise 3.0 WS

CiscoWorks VMS 上の Management Center for Cisco Security Agent をサポートする OS:

- Windows 2000 Server および Advanced Server(SP 4)(英語 [アメリカ英語] 環境のみ)

各国語対応(エージェント):

- 英語(アメリカ英語)およびインターナショナル(アラビア語、ヘブライ語を除く)の Windows オペレーティング システム
- Windows オペレーティング システムにおける、英語(アメリカ英語)、フランス語、ドイツ語、日本語でのユーザ インターフェイス オプション
- Linux および Solaris オペレーティング システムについては、英語(アメリカ英語)のみに対応

インストールの要件

注: 英語(アメリカ英語)および各国語バージョン(アラビア語、ヘブライ語を除く)の Windows オペレーティング システムがサポートされます。

Cisco Security Server Agent — Windows の場合:

- Windows NT v4.0 Server または Enterprise Server(SP 6a 以降)
- Windows 2000 Server または Advanced Server
- Windows 2003
- 1 つまたは複数の Pentiumプロセッサ(200 MHz 以上)
- 128 MB 以上の RAM
- 15 MB 以上のディスク スペース
- イーサネットまたはダイヤルアップ ネットワーク
- Citrix メタフレームはサポートされます。Windows 2000 の Windows ターミナル サービス(WTS)もサポートされます。

Cisco Security Server Agent — Solaris の場合:

- Solaris 8 SPARC アーキテクチャ(64 ビット カーネル)(12/02 版以降)
- 1 プロセッサ、2 プロセッサ、4 プロセッサの Ultra SPARC(400 MHz 以上)
- 256 MB 以上の RAM
- 15 MB 以上のディスク スペース

Cisco Security Server Agent — Linux の場合:

- Red Hat Enterprise Linux 3.0 ES または AS
- 1 プロセッサ、2 プロセッサ、4 プロセッサの x86 プラットフォーム(500 MHz 以上)
- 256 MB 以上の RAM
- 15 MB 以上のディスク スペース

Cisco Security Desktop Agent — Windows の場合:

- Windows NT v4.0 Workstation(SP 6a 以降)
- Windows 2000 Professional
- Windows XP Professional
- Windows XP Home Edition
- 1 つまたは複数の Pentiumプロセッサ(200 MHz 以上)
- 128 MB 以上の RAM
- 15 MB 以上のディスク スペース

- イーサネットまたはダイヤルアップ ネットワーク
- Citrix XP はサポートされます。Windows XP の WTS もサポートされます。

Cisco Security Desktop Agent — Linux の場合:

- Red Hat Enterprise Linux 3.0 WS
- 1 プロセッサ、2 プロセッサ、4 プロセッサの x86 プラットフォーム(500 MHz 以上)
- 256 MB 以上の RAM
- 15 MB 以上のディスク スペース

CiscoWorks VMS での Management Center for Cisco Security Agent の実行要件:

- Windows 2000 Server または Advanced Server
- Pentiumプロセッサ(1 GHz 以上)
- 1 GB 以上の RAM
- 9 GB 以上のディスク スペース

発注情報

Cisco Security Agent ソリューションは、2 つの主要コンポーネント(Cisco Security Agent および Management Center)で構成されています。エージェントを使用するには Management Center が必要です。 ライセンスを受けていないコンソールでエージェントを使用することはできません。Management Center for Cisco Security Agent は、CiscoWorks VMS 制限版および無制限版、もしくは CSA スターター バンドル(CSA-STARTER-K9)に無償で同梱されます。

表 1 Cisco Security Agent の製品番号

製品番号	製品の説明
CSA-SRVR-K9	Cisco Security Server Agent(Windows、Linux、および Solaris)、1 エージェント
CSA-B10-SRVR-K9	Cisco Security Server Agent(Windows、Linux、および Solaris)、10 エージェント バンドル
CSA-B25-SRVR-K9	Cisco Security Server Agent(Windows、Linux、および Solaris)、25 エージェント バンドル
CSA-B50-SRVR-K9	Cisco Security Server Agent(Windows、Linux、および Solaris)、50 エージェント バンドル
CSA-B100-SRVR-K9	Cisco Security Server Agent(Windows、Linux、および Solaris)、100 エージェント バンドル
CSA-B500-SRVR-K9	Cisco Security Server Agent(Windows、Linux、および Solaris)、500 エージェント バンドル
CSA-B25-DTOP-K9	Cisco Security Desktop Agent(Windows および Linux)、25 エージェント バンドル
CSA-B100-DTOP-K9	Cisco Security Desktop Agent(Windows および Linux)、100 エージェント バンドル
CSA-B250-DTOP-K9	Cisco Security Desktop Agent(Windows および Linux)、250 エージェント バンドル
CSA-B500-DTOP-K9	Cisco Security Desktop Agent(Windows および Linux)、500 エージェント バンドル
CSA-B1000-DTOP-K9	Cisco Security Desktop Agent(Windows および Linux)、1000 エージェント バンドル
CSA-B5000-DTOP-K9	Cisco Security Desktop Agent(Windows および Linux)、5000 エージェント バンドル
CSA-B10000-DTOP-K9	Cisco Security Desktop Agent(Windows および Linux)、10,000 エージェント バンドル
CSA-STARTER-K9	Cisco Security Agent スターター バンドル(Server Agent × 1 および Desktop Agent × 10 を含む)

表 2 Cisco Security Agent のメンテナンス製品番号

メンテナンス製品番号	メンテナンス製品の説明
CON-SAU-CSA-STRT	Cisco Security Agent スターター バンドルの Software Application Support plus Upgrades (SASU)
CON-SAU-CSA-SRVR	1 Server Agent(Windows、Linux、および Solaris)の SASU
CON-SAU-CSA-B10S	10 Server Agent バンドル(Windows、Linux、および Solaris)の SASU
CON-SAU-CSA-B25S	25 Server Agent バンドル(Windows、Linux、および Solaris)の SASU
CON-SAU-CSA-B50S	50 Server Agent バンドル(Windows、Linux、および Solaris)の SASU
CON-SAU-CSA-B100S	100 Server Agent バンドル(Windows、Linux、および Solaris)の SASU

メンテナンス製品番号	メンテナンス製品の説明
CON-SAU-CSA-B500S	500 Server Agent バンドル（Windows、Linux、および Solaris）の SASU
CON-SAU-CSA-B25D	25 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B100D	100 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B250D	250 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B500D	500 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-1000D	1000 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-5000D	5000 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-10KD	10,000 Desktop Agent バンドル（Windows および Linux）の SASU

お問い合わせ先

シスコシステムズ株式会社
〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館
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
(通話料無料)
電話受付時間 : 平日10:00～12:00、13:00～17:00

07.04