

Cisco Security Agent バージョン 5.0

Cisco® Security Agent エンドポイント セキュリティ ソフトウェアは、新種および未知の攻撃からシステムを保護するための重要な防御線を提供します。シスコシステムズは、市場をリードするエンドポイントおよびネットワークの統合を通して、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ソリューションを提供します。

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、次のようなさまざまな利点を備えています。

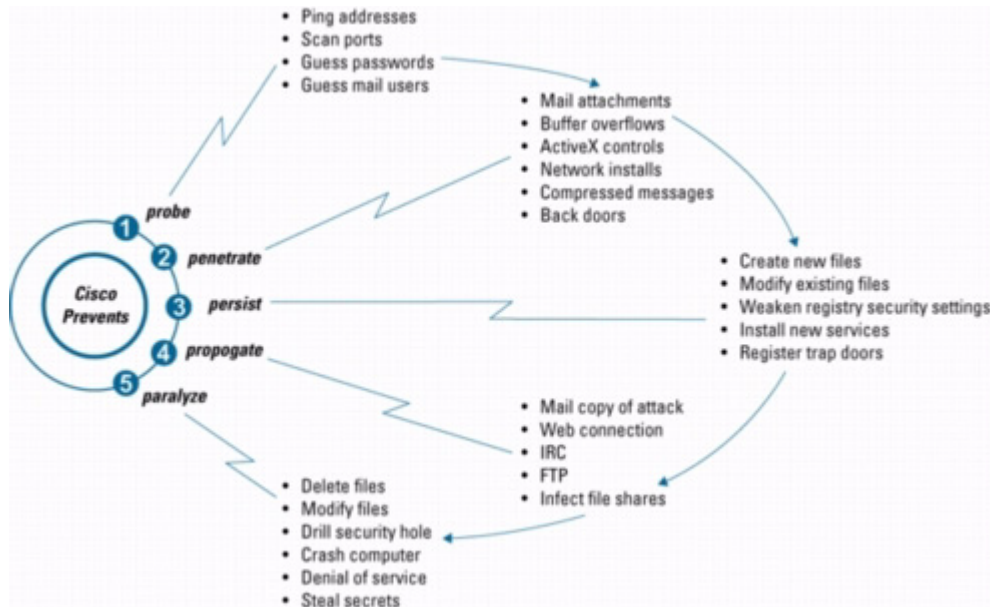
- Cisco Security Agent は、ホストへの侵入防止、分散型ファイアウォール、悪意のモバイル コードからの保護、オペレーティング システムの整合性の保証、および監査ログの連結といった機能のすべてを 1 つのエージェントで提供し、エンドポイント セキュリティのためのさまざまな機能を集約して強化します。
- ポート スキャン、バッファ オーバーフロー、トロイの木馬、不正パケット、悪意のある HTML 要求、E メール型ワームなど、さまざまな種類の攻撃に対応します。
- 既知および未知の攻撃に対する、アップデート作業が不要な防御能力を提供します。
- Unix/Windows のサー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機能を提供します。
- 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。
- 企業全体に拡張可能なアーキテクチャを持つ Cisco Security Agent は、1 つのマネージャにつき 100,000 エージェントまで拡張できます。
- NAC (Cisco Network Admission Control) を搭載した統合型のソリューション アーキテクチャを提供します。
- シスコの VPN 製品が提供する AYT (Are You There) 機能をサポートします。

新種（未知）の攻撃への対処

猛威を振るった Zotob や Windows WMF の脆弱性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。そのため、境界上で、サーバで、あるいは個々のファイル レベルで起こりうるこれらの攻撃に効果的に対処できるのは、階層型のアプローチだけです。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も対処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、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ます。ホストベースのエージェントは、CSA-MC (Management Center for Cisco Security Agents) に管理用データを送信します。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 ビットの Secure Sockets Layer (SSL) が使用されます。Cisco Security Agent の警告は 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。エージェント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、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、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時、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

CSA-MC 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、管理者は数千のエージェントを簡単に全社で展開できます。Management Center 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完全に新規のルールの作成も、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」機能があります。これは、指定したルールまたはポリシーが何を意図したものであるかの説明を、人間が読める言語形式で管理者が出力できる機能です。

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 Virtual Private Network [VPN; 仮想私設網] 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。

シスコでは、Management Center から分析レポートを作成する一連のツールも提供しています。配置分析機能は、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に関する情報を提供します。動作分析機能は、特殊な、または未知のアプリケーションや環境に対する包括的なデータ分析ツールを提供します。この機能はアプリケーションの動作に関する詳細なレポートを提供するため、お客様は、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非常に複雑なアプリケーションも含め、すべてのアプリケーションを理解できるようになります。

エンドツーエンドのセキュリティ ソリューション

Cisco Security Agent は、自己防衛型ネットワーク ソリューションを構築するお客様にとって不可欠なコンポーネントです。お客様は、相互に連携するエンドポイントおよびネットワーク コンポーネントに投資することにより、異種システム間では実現できない新しい重要なセキュリティ サービスを実現できます。

Trusted QoS は、新しいセキュリティ サービスで、ミッションクリティカルなアプリケーションのデータフローを保護します。Trusted QoS を使用すると、Cisco Security Agent は、重要なトラフィックがネットワークに到達する前にエンドポイントで識別および分類できるようになります。また、ネットワーク インフラストラクチャと連携することにより、ミッションクリティカルなデータがネットワークを通過する際に、これらのデータに高レベルのサービスが付加されます。このエンドツーエンド アプリケーションの認識と保護が実現されるのは、適応性と連携性を備え、ネットワークとエンドポイントを組み込んだ統合型ソリューションを使用する場合のみです。

システム要件

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 (Service Pack 6a)

- Solaris 8 SPARC アーキテクチャ (64 ビット カーネル)
- Solaris 9 SPARC アーキテクチャ (64 ビット カーネル)
- Red Hat Enterprise Linux 3.0 ES および AS

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

- Windows NT 4 Workstation (Service Pack 6a)
- Windows 2000 Professional
- Windows XP Professional
- Windows XP Tablet Edition
- Red Hat Enterprise Linux 3.0 WS

CiscoWorks VMS 上の CSA-MC をサポートする OS :

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

各国語対応 (Cisco Security Desktop Agent および Server Agent) :

- 英語 (アメリカ英語) および国際的な (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)、中国語 (簡体字)、フランス語、ドイツ語、イタリア語、日本語、韓国語、およびスペイン語でのユーザ インターフェイスの提供
- 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

Cisco Security Agent のシステム要件の詳細については、次の URL にある製品リリース ノートを参照してください。

http://www.cisco.com/en/US/products/sw/secursw/ps5057/prod_release_notes_list.html

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 Agents [デスクトップ エージェントとサーバー エージェント] 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。CSA-MC は、CiscoWorks VMS 制限版および無制限版、もしくは Cisco Security Agent スターターバンドル (CSA-STARTER-K9) に無償で同梱されます。

表 1 に Cisco Security Agent の製品番号、表 2 にメンテナンス製品番号を示します。

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-B1000-SRVR-K9	Cisco Security Server Agent (Windows、Linux、および Solaris)、1000 エージェント バンドル
CSA-B2500-SRVR-K9	Cisco Security Server Agent (Windows、Linux、および Solaris)、2500 エージェント バンドル
CSA-B5000-SRVR-K9	Cisco Security Server Agent (Windows、Linux、および Solaris)、5000 エージェント バンドル
CSA-B10000-SRVR-K9	Cisco Security Server Agent (Windows、Linux、および Solaris)、10,000 エージェント バンドル

製品番号	製品の説明
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-B50000-DTOP-K9	Cisco Security Desktop Agent (Windows および Linux)、50,000 エージェント バンドル
CSA-B75000-DTOP-K9	Cisco Security Desktop Agent (Windows および Linux)、75,000 エージェント バンドル
CSA-B100K-DTOP-K9	Cisco Security Desktop Agent (Windows および Linux)、100,000 エージェント バンドル
CSA-B200K-DTOP-K9	Cisco Security Desktop Agent (Windows および Linux)、200,000 エージェント バンドル
CSA-B300K-DTOP-K9	Cisco Security Desktop Agent (Windows および Linux)、300,000 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 (1 Server Agent および 10 Desktop Agent 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
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

関連情報

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

©2006 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
〒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/service/contactcenter>
0120-933-122 (通話料無料)、03-6670-2992 (携帯電話、PHS)
電話受付時間：平日 10:00～12:00、13:00～17:00