Cisco Security Agent バージョン 5.1

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。Cisco Security Agent は、エンドポイントの再設定やアップデートを行わずに巧妙化する新種の脅威を軽減し、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。

ネットワーク統合機能

表 1 に、Cisco Security Agent のネットワーク統合機能を示します。

表 1　ネットワーク統合機能

機能	説明
IPS との統合	Cisco Security Agent をシスコのネットワーク IPS（Intrusion Prevention System; 侵入防御システム）デバイスと統合すると、ネットワーク内での攻撃を効果的に識別できる。Cisco Security Agent から Cisco IPS 4200 シリーズ アプライアンスや Cisco ASA 5500 および Cisco Catalyst 6500/7600 シリーズの IPS モジュール（IDSM-2）に対して重要なエンドポイント セキュリティ情報が提供されるため、完全なエンドツーエンドのセキュリティ ソリューションを実現できる
Trusted QoS	Cisco Security Agent を使用すると、エンドポイントで Cisco Security Agent のポリシー ルールに従ってアプリケーション ネットワーク トラフィックに QoS（Quality of Service）マーキングを適用できる。企業ネットワークのアップストリームにある Cisco IOS デバイスは、これらのマーキングを使用してパケットを分類し、ポリシングやキューイングといった QoS サービス ポリシーを適用できる。また、Cisco NAC（Network Admission Control）フレームワークおよび NAC アプライアンス（Cisco Clean Access）を使用すると、Cisco Security Agent が稼働するホストによる QoS マーキングの有効性を保証できる。Trusted QoS によって、ネットワークが過負荷の状態でもミッションクリティカルなトラフィックの適切な配信が可能
NAC との統合	NAC フレームワークでは、Cisco Security Agent と NAC の統合によって双方向の情報交換が行われ、エンドポイントのポスチャが変更される。Cisco Security Agent はエンドポイントのポリシーのアップデートをダイナミックに実行して、NAC ポスチャを変更できる。また、Cisco Security Agent が稼働するホストを識別および信頼して、フル ネットワーク アクセスを許可できる。条件を満たさないホストは、修復されて条件を満たすようになるまで隔離することが可能。これにより、DoS 攻撃（サービス拒絶攻撃）やマルウェアによる攻撃を緩和して、企業ネットワークの自己防衛力を高めることが可能
CS-MARS イベントとの統合	Cisco Security Agent から CS-MARS（Cisco Security Monitoring, Analysis and Response System）に重要なエンドポイント情報を提供することで、CS-MARS はネットワーク内の脅威の発見や調査をより効果的に実施できる

機能および利点

Cisco Security Agent は、次のようなさまざまな利点を備えています。

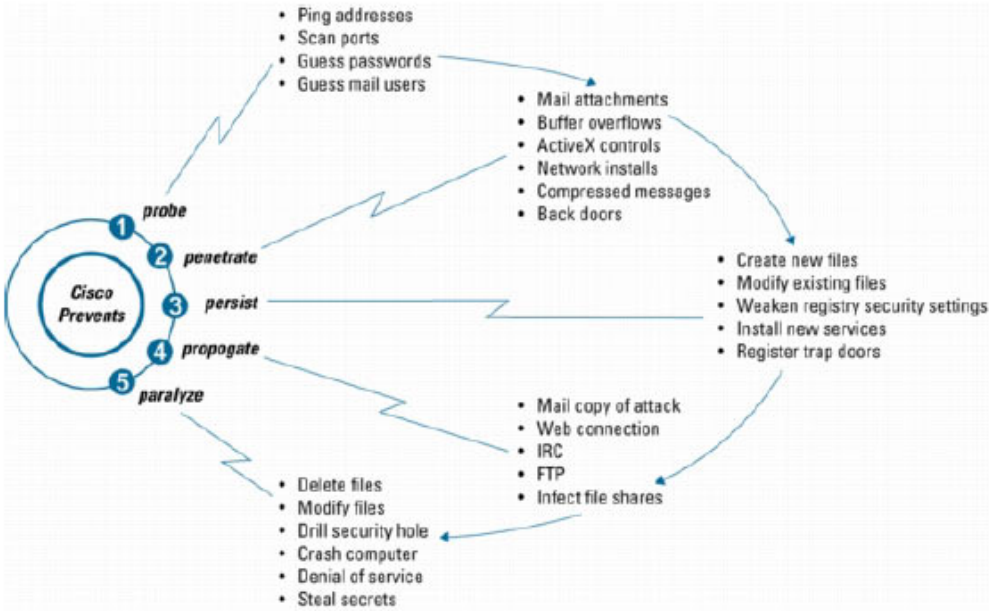
- 侵入防止、分散型ファイアウォール、悪意のモバイル コードからの保護、オペレーティング システムの整合性の保証、および監査ログの連結といった機能のすべてを 1 つのエージェントで提供し、エンドポイント セキュリティのためのさまざまな機能を集約して強化します。
- ポート スキャン、バッファ オーバーフロー、トロイの木馬、不正パケット、悪意のある HTML 要求、E メール型ワームなど、さまざまな種類の攻撃に対応します。
- 既知および未知の攻撃に対する、アップデート作業が不要な防御能力を提供します（緊急のパッチ適用作業が不要）。
- サーバおよびデスクトップのための業界随一の保護機能を提供します。
- 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で、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。
- Cisco NAC フレームワークおよび NAC アプライアンス（Cisco Clean Access）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。
- Cisco VPN デバイスとの統合により、IP Security（IPSec）および Secure Sockets Layer（SSL）VPN でのエンドポイント セキュリティを提供します。

新種（未知）の攻撃への対処

図 1 に、ネットワーク攻撃のライフサイクルを示します。

図 1　ネットワーク攻撃のライフサイクル



製品のアーキテクチャ

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。Management Center は Cisco Security Agent の設定を行うスタンドアロンのアプリケーションです。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 SSL が使用されます。Cisco Security Agent のアラートは、CS-MARS を使用して他のシスコ製セキュリティ製品から発生するアラートと統合できます。

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、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

CSA-MC 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。Web ブラウザを使用して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 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。

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。

まとめ

Cisco Security Agent は、シスコ自己防衛型ネットワーク ソリューションの中心となる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、ネットワークが過負荷の状態でも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、ミッションクリティカルなアプリケーション フローを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。

製品仕様

表 2 に、Cisco Security Agent バージョン 5.1 の製品仕様を示します。

表 2 製品仕様

説明	仕様
Cisco Security Server Agent のソフトウェア互換性	• Windows 2003（Standard Edition、Enterprise Edition、Web Edition、または Small Business Edition） • Windows 2000 Server および Advanced Server • Windows NT 4.0 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 のソフトウェア互換性	• Windows XP Professional • Windows XP Tablet Edition • Windows 2000 Professional • Windows NT 4.0 Workstation（Service Pack 6a） • Red Hat Enterprise Linux 3.0 WS
Cisco Security Agent のハードウェア互換性（Windows OS の最小要件）	• 200 MHz x86 プロセッサ • 25 MB のハード ドライブの空き領域 • 128 MB RAM • イーサネットまたはダイヤルアップ ネットワーク接続
Cisco Security Agent のハードウェア互換性（Solaris OS の最小要件）	• UltraSPARC 400 MHz プロセッサ • 25 MB のハード ドライブの空き領域 • 256 MB RAM • イーサネット ネットワーク接続
Cisco Security Agent のハードウェア互換性（Linux OS の最小要件）	• 500 MHz x86 プロセッサ • 25 MB のハード ドライブの空き領域 • 256 MB RAM • イーサネット ネットワーク接続
CSA-MC のソフトウェア互換性	• Windows 2003 R2 Server
CSA-MC のハードウェア互換性（最小要件）	• 1 GHz x86 プロセッサ • 1 GB RAM • 2 GB 仮想メモリ
各国語対応	• 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）、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

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 [デスクトップ エージェントとサーバ 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、Cisco Security Agent スターター バンドル（CSA-START-5.1-K9）に同梱されます。

表 3 に Cisco Security Agent の製品番号、表 4 にメンテナンス製品番号を示します。

シスコ製品の購入方法の詳細は、「発注方法」を参照してください。

表 3　Cisco Security Agent の発注情報

製品番号	製品名
CSA-START-5.1-K9	Cisco Security Agent バージョン 5.1 用スターター バンドル（CSA-MC、サーバ エージェント× 1、およびデスクトップ エージェント× 10 を含む）
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）、1,000 エージェント バンドル
CSA-B2500-SRVR-K9	Cisco Security Server Agent（Windows、Linux、および Solaris）、2,500 エージェント バンドル
CSA-B5000-SRVR-K9	Cisco Security Server Agent（Windows、Linux、および Solaris）、5,000 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
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）、1,000 エージェント バンドル
CSA-B2500-DTOP-K9	Cisco Security Desktop Agent（Windows および Linux）、2,500 エージェント バンドル
CSA-B5000-DTOP-K9	Cisco Security Desktop Agent（Windows および Linux）、5,000 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-B25000-DTOP-K9	Cisco Security Desktop Agent（Windows および Linux）、25,000 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-B100000-DTOP-K9	Cisco Security Desktop Agent（Windows および Linux）、100,000 エージェント バンドル
CSA-B200000-DTOP-K9	Cisco Security Desktop Agent（Windows および Linux）、200,000 エージェント バンドル
CSA-B300000-DTOP-K9	Cisco Security Desktop Agent（Windows および Linux）、300,000 エージェント バンドル

サービスおよびサポート

シスコは、お客様がそのネットワーク サービスを最大限に活用するため、各種サービス プログラムを用意しています。これらのサービスは、スタッフ、プロセス、ツールをそれぞれに組み合わせて提供され、お客様から高い評価を受けています。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。サービスについての詳細は、以下の URL を参照してください。

テクニカル サポート サービス
http://www.cisco.com/jp/go/tac/

サービス プログラム
http://www.cisco.com/jp/services/

表 4　Cisco Security Agent のメンテナンスに関する発注情報

製品番号	製品名
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（Windows、Linux、および Solaris）の SASU
CON-SAU-CSA-B25S	25 Server Agent（Windows、Linux、および Solaris）の SASU
CON-SAU-CSA-B50S	50 Server Agent（Windows、Linux、および Solaris）の SASU
CON-SAU-CSA-B100S	100 Server Agent（Windows、Linux、および Solaris）の SASU

製品番号	製品名
CON-SAU-CSA-B250S	250 Server Agent（Windows、Linux、および Solaris）の SASU
CON-SAU-CSA-B500S	500 Server Agent（Windows、Linux、および Solaris）の SASU
CON-SAU-CSA-B1000S	1,000 Server Agent（Windows、Linux、および Solaris）の SASU
CON-SAU-CSA-B2500S	2,500 Server Agent（Windows、Linux、および Solaris）の SASU
CON-SAU-CSA-B5000S	5,000 Server Agent（Windows、Linux、および Solaris）の SASU
CON-SAU-CSA-B10000S	10,000 Server Agent（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-B1000D	1,000 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B2500D	2,500 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B5000D	5,000 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B10KD	10,000 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B25KD	25,000 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B50KD	50,000 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B75KD	75,000 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B100KD	100,000 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B200KD	200,000 Desktop Agent バンドル（Windows および Linux）の SASU
CON-SAU-CSA-B300KD	300,000 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

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
0120-092-255 (通話料無料)
電話受付時間 : 平日10:00～12:00、13:00～17:00

07.02