

Cisco Security Agent の侵入防御機能による 企業リモート ユーザの保護

以前にも増して、従業員は企業のオフィスから離れた場所で仕事をしています。こうしたユーザの一部は、ホテルの部屋、空港、または顧客のオフィスから、電子メールなどの企業内のアプリケーションにアクセスして、移動中に作業を行います。他には、テレワーカーと呼ばれる、自宅から作業を行うユーザもいます。多くの場合、こうしたユーザは、ダイヤルアップモデムを使用せず、インターネット経由で企業のネットワークにアクセスします。このようなユーザはすべて、インターネットからの攻撃にさらされており、企業の中央に位置するファイアウォールからは全く守られていません。防御措置を取っていないリモートユーザのコンピュータは、企業ネットワークへの侵入経路を攻撃者に与えることになります。

中央集中管理型のパーソナルファイアウォール（分散ファイアウォールとも呼ばれる）市場の誕生と成長は、こうしたリスクの削減を求める IT 担当部署の要望を反映しています。顧客のニーズに応えるために、今日提供されているパーソナルファイアウォールのいくつかは、通常、次のような重要な機能を搭載しています。

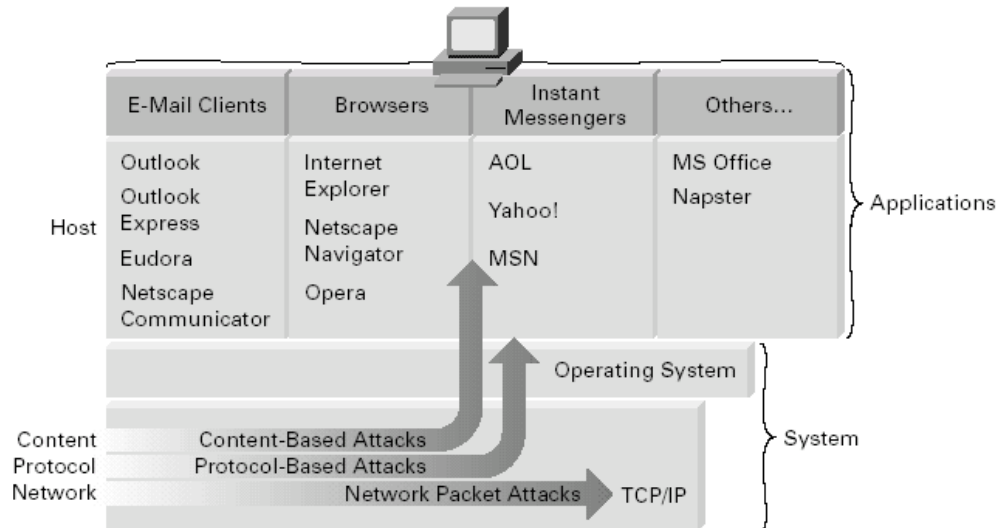
- ポートブロッキング
- 中央集中型のネットワークセキュリティポリシー管理

- 中央集中型レポーティング
- 侵入検知（一部の製品で提供される）
- ネットワーク内で実行可能なアプリケーションの制御（一部の製品で提供される）

こうした機能はリモートユーザが直面するリスクの一部だけに対処します。分散ファイアウォールの大半の機能は、コンピュータ上のアプリケーションに接続を試みるようなネットワーク攻撃だけを対象にしています。しかし、この他にも、電子メールの添付ファイルや JavaScript など悪質なコンテンツのペイロードを利用した攻撃、さらにはネットワークアプリケーションに対するバッファオーバーフローといったプロトコル攻撃によるリスクも多く存在します。



図 1
アプリケーション攻撃



従来のパーソナルファイアウォールによってリソースが保護されている場合、その保護は通常ネットワーク内に限定されています。攻撃によってアプリケーションが侵害されると、ホストは完全に脆弱になります。パーソナルファイアウォールによってサービスの実行が許可される場合、そのサービスを実行するソフトウェアは最新の状態であり、正しく設定されている必要があります。アプリケーションがネットワーク経由でアクセスされている場合、パーソナルファイアウォールはそのアプリケーションを保護できません。また、パーソナルファイアウォールはポートやIPアドレスによる単純な制御以外、アプリケーションのネットワーク使用を制御することはできません。標準的なパーソナルファイアウォールには、この他にも次のような不利な点があります。

- 許可されたアプリケーションを装った侵入は、パーソナルファイアウォールセキュリティをすり抜けるおそれがある。一例として、FoundstoneのFirehole attackは、Internet Explorerに似せた動作を他のアプリケーションにさせて、許可される接続を試みます。¹
- パーソナルファイアウォールで作成されるセキュリティイベントの大半は、それほど脅威ではなく、悪意のある攻撃ではない。このため、ファイアウォールを導入した企業は、その効果を判断することが困難になります。²
- パーソナルファイアウォールは、ネットワークを利用したクライアントアプリケーションを全く保護しない。たとえば、最近確認されたInternet Explorerのセキュリティホールは、オペレーティングシステムの安全性を脅かす基本的なHTML攻撃を許可してしまいます。³ その他の例として、ユーザがインスタントメッセージ経由で感染の可能性があるファイルをダウンロードすることができたり、メッセージ本文の埋め込みHTMLを利用した電子メールスヌーピングが許可されたりします。⁴

1. Fireholeは次のURLにあります。
<http://keir.net/firehole.html>
TooLeakyは次のURLにあります。
<http://tooleaky.zensoft.com>

2. 『Study: Constant security fixes overwhelming IT managers』、Computerworld、2001年11月30日
http://www.computerworld.com/itresources/rcstory/0,4167,STO66215_KEY73,00.html

3. CERT Advisory CA-2001-36、『Microsoft Internet Explorer Does Not Respect Content-Disposition and Content-Type MIME Headers』、2001年12月16日
<http://www.cert.org/advisories/CA-2001-36.html>

4. 『Privacy group warns of e-mail wiretap』、CNN.com、2001年2月5日
<http://www.cnn.com/2001/TECH/internet/02/05/email.wiretap.idg/>



NIMDA は複合型のセキュリティ脅威の 1 つです。NIMDA ワームによる攻撃は、HTTP、電子メール、および共有フォルダなど複数の経路を利用した複合型の攻撃でした。ネットワークレベルで HTTP 攻撃から防御されていたシステムは、多くの場合、電子メールや Web ブラウザを利用した攻撃に対しては脆弱でした。Cisco® Security Agent は、侵入を防御する機能があるため、攻撃伝搬や攻撃による損傷を、システムに侵入された後でも制御することが可能です。NIMDA の攻撃によって通常ありえない悪意ある動作が行われたとしても、Cisco Security Agent は NIMDA の攻撃を、システムへの侵入後でも阻止しました。この攻撃は、アプリケーションのバッファオーバーフローを引き起こし、自身を電子メール経由で他の標的に送信しようとしていました。Cisco Security Agent は攻撃シグニチャを含んでおらず、NIMDA も既知の攻撃ではありませんでしたが、Cisco Security Agent は、その悪意のある攻撃の試みを阻止しました。

すべてのクラスの攻撃を御する Cisco Security Agent

Cisco Security Agent は、リモート ユーザに対するネットワーク ベースの攻撃を阻止するなど、パーソナル（分散）ファイアウォールの基本的な要件を満たします。また、こうした従来の機能とともに、プロトコル攻撃や悪意のあるコンテンツによる攻撃からの被害を防止します。Cisco Security Agent はさらに、他のベンダーのパーソナルファイアウォール製品と比較して、次のような利点を提供します。

- アクティブ コンテンツ停止は、Java、JavaScript、および ActiveX などのモバイル コードを利用した破壊活動から Web ブラウザを防御します。
- 電子メール ワーム防御は、NIMDA や GONER のような電子メール ワーム攻撃を阻止します。
- アプリケーションなりすましの防御は、Firehole 攻撃や Tooleaky 攻撃のようにダイナミック リンク ライブラリ（DLL）を利用した「アプリケーションハイジャック」と呼ばれる攻撃から防御します。
- アプリケーション ポリシー制御は、インスタント メッセージアプリケーションによるファイルのダウンロードなど、アプリケーションを使用した際のユーザによる危険な操作を防止します。
- バッファ オーバーフロー制御は、既知または未知のバッファオーバーフロー攻撃からの防御を行います。
- アプリケーション実行制御は中央集中型管理により、実行、ネットワーク使用、またはネットワーク使用の禁止をアプリケーション単位で指定できます。
- ロケーションを識別した制御は、オフィス内でのファイル共有などの通常のネットワーク使用を許可し、リモートロケーションからは危険なネットワーク使用を許可しません。
- アップデート不要な侵入検知は、シグニチャを使用せずに攻撃を検知し阻止します。侵入を阻止する際、他の侵入検知製品と異なりシグニチャは必要ないため、ネットワークを徘徊している攻撃に対するシグニチャをベンダーがまだ作成していなくても、攻撃にさらされる期間がありません。また、シグニチャのインストールや更新に伴う管理負荷もありません。

Cisco Security Agent の機能

次に示す機能、パフォーマンス ベンチマーク、および製品特性を、他のパーソナル ファイアウォール製品と比較して、お客様のネットワーク セキュリティ要件に適合するかを確認してください。



ネットワーク セキュリティの基本機能

着信 / 発信ポート ブロッキング : Cisco Security Agent の分散ファイアウォール ポリシーは、着信および発信接続を含めた、すべてのネットワークトラフィックを制御します。Cisco Security Agent は、さらに、プロトコル、ポート、および通信を行っているホストアドレスをもとに、トラフィックの制御を行います。他のパーソナルファイアウォール製品と異なり、どのアプリケーションが活動を実行しようとしているかをもとに、制御を行います。たとえば管理者は、Web ブラウザからリモート Web サーバへの接続は許可し、電子メールクライアントからリモート Web サーバへの接続を拒否する、という設定が可能になります。

断片化したパケット攻撃からの防御 : Cisco Security Agent は、断片化したパケットを含む、さまざまな Layer 3 攻撃からの防御を行います。これは WinNuke や SMBDie のような Denial-of-Service (DoS) 攻撃だけではなく、ポート スキャンやオペレーティング システムフィンガープリント (nmap) 攻撃の阻止も可能です。

回避テクニックを使用した攻撃からの防御 : Cisco Security Agent は、Intrusion Detection System (IDS; 侵入検知システム)⁵ の監視を回避する攻撃の手法にも対応しています。

侵入検知と阻止 : 既知または未知の攻撃はエージェントによって検知され、自動的に阻止されます。Cisco Security Agent には、適切なシステム動作を実行させる動作ポリシーを使用した侵入阻止システムがあるため、侵入検知シグニチャは不要です。他の侵入検知製品は、新しいシグニチャのリリースによって、新しい攻撃を検知および阻止します。しかし、こうしたシグニチャの更新のリリース頻度は新しい攻撃の出現頻度より低く、対応シグニチャのない期間はコンピュータが脆弱になります。

Cisco Security Agent の侵入検知および防御機能はシグニチャを使用しないため、提供する防御機能は、新しいシグニチャの作成頻度やリリース頻度に依存しません。頻繁に、相当量のシグニチャアップデートを数多くのクライアント デスクトップやラップトップ コンピュータに展開することは、管理が難しいだけでなく、ネットワーク帯域幅も著しく消費します。Cisco Security Agent は高レベルの防御機能とアップデート不要なアーキテクチャを提供でき、しかもシグニチャ アップデートの管理が全く必要ないのです。

設定可能な IDS 規則 : Cisco Security Agent は、侵入の検知よりも侵入の防御に重点をおいた製品です。システムを構成する動作ポリシーは、管理者によって詳細なカスタマイズが可能です。

アプリケーション実行防御 : Cisco Security Agent は、どのアプリケーションの実行を許可するかを制御できます。この規則によって、実行を許可するアプリケーションだけでなく、そのバージョンの指定ができる、非常に詳細な制御が可能になります。さらに、どのバージョンの DLL の実行を許可するかという制御も行えます。

ロケーションを識別した防御 : Cisco Security Agent は、オフィス内の、コンピュータ間のファイル共有など、通常のネットワーク利用を許可しますが、リモート ロケーションから行われる危険度の高い活動を防止します。

5. 『IDS Evasion with Unicode』、Eric Hacker、Bugtraq security mailing list、2001 年 1 月 3 日
<http://www.securityfocus.com/infocus/1232>



拡張セキュリティ機能

Web ブラウザおよび電子メール クライアントの停止保護：Cisco Security Agent は Web ブラウザや他のエンド ユーザ ネットワーク アプリケーションに対する、Java、JavaScript、および ActiveX などのモバイル コードを利用したコンテンツベースの攻撃を防御します。ユーザがオンラインで参照したり、電子メールを読んだり、チャットを行う際、悪意のあるコンテンツから防御します。

電子メール ワーム防御：Cisco Security Agent は悪質と見られるファイルを添付した大量の電子メールの送信を検知して阻止します。こうした試みを Microsoft Outlook のアドレス帳へのアクセスを厳しく制御することで阻止するだけでなく、悪質なファイルが添付された電子メールの存在は中央管理へレポートされ、システム全体をカバーする検疫リスト（Global Quarantine List）がアップデートされます。この検疫リストはすべてのエージェントに配布され、以前にそのワームに攻撃されたことがなくても、予防接種としての役割を果たします。

既知または未知のバッファ オーバーフロー攻撃の防御：Cisco Security Agent は保護されたコンピュータ上で実行されるすべてのアプリケーションに対するバッファ オーバーフロー攻撃を検知し、阻止します。検知はアプリケーションのコード実行方法に基づいて行われ、パケットのコンテンツの解析をするものではないため、既知/未知にかかわらず、バッファオーバーフロー攻撃を阻止します。また、IDS 回避テクニックを利用した攻撃も阻止します。Cisco Security Agent の高度バッファ オーバーフロー防御は、既知のスタックオーバーフローだけでなく、検知がより難しいヒープ オーバーフローも阻止します。

アプリケーションなりすましの防御：パーソナルファイアウォールに対する最新の攻撃テクニックの1つに、DLL Injection⁶などのメカニズムを利用して、悪意のあるアプリケーションが許可されたアプリケーションを装う方法があります。このテクニックでは、悪意のあるプログラムコードが、許可されたアプリケーション内で実行されているように装うため、ファイアウォールはこの悪意のあるプログラムコードを、許可されたアプリケーションの一部として誤認します。したがって、悪意のあるアプリケーションが、たとえばネットワークにアクセスするために、ファイアウォール制御をすり抜けることができます。Cisco Security Agent は、すべての DLL Injection 攻撃を阻止し、許可されていないネットワークアクセスだけでなく、ローカルパスワードの盗用による攻撃も阻止します。

設定可能なインスタント メッセージング制御：Cisco Security Agent はアプリケーション ポリシー制御により、企業内で使用されるインスタント メッセンジャ アプリケーションに対して、詳細に指定ができる制御方法を提供します。Cisco Security Agent はたとえば、インスタント メッセンジャ システムにおいて、テキストによるメッセージを許可してファイル転送だけを禁止し、同時にブラウザや FTP を使用したファイル転送を許可できます。インスタント メッセンジャ クライアントの接続は、許可された企業のインスタント メッセンジャ サーバだけを利用したり、内部のインスタントメッセンジャ サーバの使用に限定して文書の転送を許可したりできます。

オペレーティング システムのロックダウン：Cisco Security Agent は、重要なオペレーティング システムのバイナリ ファイルやシステム設定の修正を試みる攻撃を防御することで、Windows オペレーティングシステムを強固にします。この機能はファイルシステムのコンテンツを暗号化分析する必要がないため、実質的にはシステムパフォーマンスに影響を与えません。

監査ログの統合：Cisco Security Agent は攻撃の詳細なログを記録します。また、不正なログオンなどが記録された Security Log エントリや Windows Event Log エントリを収集できます。

6. Bindview Razor セキュリティ チームによる PWDUMP2 は、Windows NT および Windows 2000 のコンピュータからパスワードを取得します。
(http://razor.bindview.com/tools/desc/pwdump2_readme.html)
パーソナル ファイアウォールをすり抜ける DLL Injection 攻撃に関する詳細については、次の URL を参照してください。
<http://keir.net/firehole.html>



オープンでカスタマイズ可能：アプリケーションのセキュリティ対策基準はポリシーによって制御されます。ポリシーは、ネットワーク、ファイルシステム、レジストリ、または COM システム コンポーネントに対するアプリケーションのアクセス方法を特定した規則セットで構成されています。Cisco Security Agent では、分散ファイアウォールとデスクトップアプリケーションを保護するデフォルト ポリシーが設定されていますが、すべてのポリシーをカスタマイズすることができ、管理者は、ブラウザベースの GUI を利用して新しくポリシーを簡単に定義することができます。

管理機能

エージェントの中央集中管理：Cisco Security Agent のポリシーは中央で定義され、防御が必要なデスクトップやサーバ上のエージェントに自動的に配布されます。

場所に依存しない管理ソリューション：Cisco Security Agent 管理は HTTP および HTTP 経由で実施されます。つまり、標準の Web ブラウザを使用できる場所であれば、場所を問わず管理が行えます。

Dynamic Host Configuration Protocol (DHCP) 環境で実行可能：エージェントの識別は IP アドレスによるものではないため、頻繁に IP アドレスが変更される DHCP 環境での使用が可能です。代わりに、各エージェントには IP アドレスに依存しない、Globally Unique Identifier (GUID) が割り振られます。したがって、グループ化、ポリシーの適用または修正、あるいはエージェントのアップデートといったすべての中央管理機能は、指定されたエージェントのアドレスが変更されても適用されます。

中央アラート：すべてのエージェント イベントは管理コンソールに送信され、中央でアラートが生成されます。

設定可能なアラート：アラートは中央コンソールにレポートされます。すべてのクライアントイベントは Cisco Security Agent 管理コンソールにレポートされ、中央カスタマー コンソールのためのアラートを生成します。クライアント エージェントによるイベントは、すべて、電子メール、ポケットベル、Simple Network Management Protocol (SNMP) トラップ、フラット ログ ファイル、またはカスタム プログラムによるインターフェイス経由でアラートするように設定できます。

エージェントと管理コンソール間のセキュアな通信：管理コンソールとエージェント間の通信はすべて、設定可能なポートを経由した Secure Sockets Layer (SSL) で行われます。

中央によるポリシー定義とローカルでのポリシー実行：エージェントが一定時間接続されていない場合、ローカルではすべてのポリシーの実行は継続されます。エージェントが再度接続すると、新しいポリシーやアップデートが自動的にインストールされます。エージェントに対するアップデートは、設定した期間ごとに管理コンソールから自動的に取り込まれます。

リモート インストールと自動設定：初期導入の際、エージェント ソフトウェアは、HTTP、Short Message Service (SMS)、または他のソフトウェア社内配布メカニズムを利用して展開できます。その後、すべてのポリシーやソフトウェア アップデートは、エージェント ポーリング メカニズムを利用して自動的に行われます。

セキュリティ ポリシーから隔離されたエンドユーザ：エンド ユーザは Cisco Security Agent に直接アクセスすることができないため、ローカルでポリシーの変更は行えません。Cisco Security Agent は、中央で定義されたポリシーをローカルにキャッシュして実行します。このポリシーはクライアント ユーザが参照または修正することはできません。



エンド ユーザが攻撃された場合の通知オプション：すべてのセキュリティ イベントはクライアントにローカルに保存され、さらに中央管理コンソールへ通知されます。ポリシー違反が発生した場合、クライアントの Windows タスクバーに違反を通知する旗を表示させるオプション設定が可能です。必要に応じて、Cisco Security Agent がエンド ユーザから不可視になるようにも設定できます。

ログの縮小と False Positive の解消：Cisco Security Agent はカスタマイズ可能な、動作ベースのポリシー システムであるため、False Positive は発生しません。ポリシーは特定のコンピュータ環境に簡単に適応させることができます。

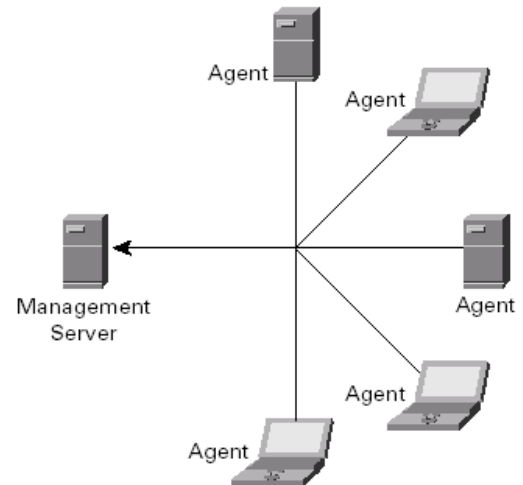
リモート コンピュータの調査と安全なシステム

図 2
Cisco Security Agent アーキテクチャ

- 攻撃の阻止
- ポリシーの実行
- 必要に応じたアクティビティ情報の取得

- アプリケーション動作の調査
- 新しいアプリケーションを保護または制御するための新しいポリシーの確立

- システム上にインストールまたは実行されているすべてのアプリケーションの特定
- A/V Scanner など、見つからない、または未使用の Security Agent の特定
- StormWatch Agent に保護されていないシステムの特特定



従来のパーソナル ファイアウォールでは安全であることが確認済みのアプリケーションはアプリケーション制御によって識別できるが、ユーザがインストールする可能性のあるアプリケーションの種類はそれよりも多いという点が指摘されています。アプリケーションごとに多く存在するバージョンやパッチレベルも考慮する必要があるため、問題は表面的な検査で得られる指摘よりも深刻です。悪質ではないアプリケーションがファイアウォールによって阻止されると不便なため、管理者も実行するアプリケーションを許容しすぎています。

管理者にとっての問題は、今までにインストールおよび使用されているアプリケーションを特定したり、アプリケーションの動作を調査する簡単な方法がなかったことです。このため、動作が不明なアプリケーションが存在する中で、安全なアプリケーションのリストを作成することは難しくなります。

アンチウイルス スキャナが実行されておりシグニチャが定期的にアップデートされているかなど、許可されたアプリケーションを正しく機能させているかどうか監視できませんでした。多くのシステムが物理的にリモートの場所にある場合は、さらに難しくなります。

Cisco Security Agent フレームワークによって Cisco Security Agent は、Cisco Security Agent 中央管理サーバ上で稼動する、他のシスコ製品と連動します。これにより、管理が簡単になります。



Cisco Security Agent Profiler は配置された Cisco Security Agent を使用して、すべてのリモート システム内のすべてのアプリケーションの次のような状態を確認します。

- どのアプリケーションがどのコンピュータにインストールされているか
- どのアプリケーションが実行されているか
- どのアプリケーションがクライアントとして、またはサーバとしてネットワークを使用するか
- アンチウイルス スキャナなど必要なアプリケーションがインストールされているか、または実行されているか
- ピアツーピア ファイル共有などの不要なアプリケーションが実行されているか
- Cisco Security Agent によって保護されていないリモート システムがあるか。これには、Cisco Security Agent を電子メール、Domain Name System (DNS)、または DHCP などの主要な内部サーバにインストールする必要があります。Cisco Security Agent Profiler は、これらのサーバと通信している Cisco Security Agent がないシステムを特定します。

Cisco Security Agent Profiler は、すべてのコンピュータ上のすべてのアプリケーションの詳細な調査を行います。ここでは、アプリケーションのライブ動作、すなわち、読み取り / 書き込みの目的にかかわらずアクセスしたファイル、受信 (サーバ) または発信 (クライアント) とリモート コンピュータのアドレスを含めたすべてのネットワーク接続、読み取り / 書き込みの目的にかかわらずアクセスしたレジストリ、およびすべての COM オブジェクトのロードが監視されます。Cisco Security Agent Profiler はアプリケーション動作に関する情報を取得し、管理者用にレポートにまとめ、制御するためのポリシーを生成します。

Cisco Security Agent フレームワークを使用すれば、管理者は次の作業を中央から行うことができます。

- Cisco Security Agent によって防御されていないリモート コンピュータの特定
- アンチウイルス スキャナなどのシステム セキュリティ製品を実行していないリモート コンピュータの特定
- Symantec の LiveUpdate などのアンチウイルス シグニチャ アップデータを実行していないリモートコンピュータの特定
- サービス パックやホット フィックスなどのシステムの重要なセキュリティ アップデートが適用されていないリモート コンピュータの特定
- 企業ポリシーで義務付けられたアプリケーションを実行していないリモートコンピュータの特定
- リモート コンピュータ上にインストールまたは実行された、許可されない、または不明なアプリケーションの特定
- 不明なアプリケーションが実行された際の動作の分析。悪意のある不明なアプリケーションと、悪意のない不明なアプリケーションを識別します。
- 動作分析に基づいた、アプリケーションに許可される動作および関数の制御

Cisco Security Agent と Cisco Security Agent Profiler の双方は、Cisco Security Agent 管理サーバにインストールされ、既存のファイアウォール エージェントを使用します。リモート システムに追加でインストールするものではありません。



優れた機能とネットワーク セキュリティ

Cisco Security Agent では、ファイアウォールの基本機能だけでなく拡張機能よりも優れた、リモートの調査機能と制御機能が追加されます。従来のパーソナルファイアウォール製品の制約を解消する優れた防御機能を備えています。幅広いネットワークセキュリティ カバレッジと詳細なシステム分析で、Cisco Security Agent はリモート コンピュータのための強固なネットワーク セキュリティを管理者に提供します。Cisco Security Agent は、企業環境における徹底的な侵入防御を実現します。侵入を防御するとともに、シグニチャに依存しないセキュリティを可能にします。

Cisco Security Agent は、重要なサーバやデスクトップに常駐して、標準的なパーソナルファイアウォール製品では実現できない、求められるリソースへの安全なアクセスを独自の Intercept Correlate Rules Engine (INCORE) アーキテクチャを使用して提供します。INCORE はオペレーティング システムに対するアプリケーションのリソース要求を阻止し、その動作と規則エンジンとを照らし合わせて、設定されたアプリケーション セキュリティ ポリシーに応じたリアルタイムの許可 / 拒否決定を行います。エージェントはサーバやデスクトップへの攻撃に対して自動的に防御を行う機能を持つことで、顧客のセキュリティポリシーの中央コンポーネントとしての役割を果たします。Cisco Security Agent は防御の全く新しいスタンドアロンレイヤとなり、シグニチャアップデートの継続的な管理という、IT・担当部署の負担を軽減します。

©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