

Cisco Security Agent — スパイウェアおよびアドウェア 対策エンタープライズ ソリューション

はじめに

ユーザが気付かないうちにユーザのコンピュータにインストールされるスパイウェアプログラムが広がりを見せ、大きな問題となっています。2004 年の Harris Poll の調査によると、IT マネージャの 92%が、スパイウェアが組織に感染し、平均 29%のワークステーションが影響を受けたと報告しています。また、全体の 40%が感染の増加を指摘しています。

ハッカーはスパイウェアを利用して、ユーザ名、パスワード、クレジットカード番号などの機密情報を記録したり、企業の機密情報を盗んだりします。情報の盗難は企業にとって最大のセキュリティ問題の 1 つであり、経済的にも最も大きな損害を受けます。しかし、大部分のスパイウェアは通常、「スパイ」機能が付属したフリーウェアまたはシェアウェアにバンドルされたアドウェアプログラムにすぎません。「スパイ」機能は、Cookie や URL のアクセス履歴に基づいて、購買やネット サーフィン
の傾向に関するマーケティング用の情報を収集します。

スパイウェアとアドウェアはキーボード操作を記録し、ときには Web サーバにデータを送信できる点で共通しており、セキュリティとプライバシーに対する深刻な脅威となります。現在市販されているスパイウェア対策ソリューションは、受動的で対処的な検出機能に基づいており、このようなますます大きくなる問題には対処できません。Cisco[®] Security Agent はプロアクティブなアプローチを提供し、スパイウェアとアドウェアの両方の感染から保護し、システムの整合性を維持し、エンドポイントに階層的な防御を提供するのに役立ちます。Cisco Security Agent は 2 つの方法で感染に対抗します。まず、スパイウェアプログラムが最初にインストールされることを防止します。さらに、すでにインストールされている場合は、スパイウェアが実行され、悪意のある動作（機密データの読み取りや中継など）を行うことを阻止します。

スパイウェアとアドウェアの比較

スパイウェアとアドウェアの相違を理解することは重要です。スパイウェアの目的は、ユーザの情報またはお金をユーザに気付かれないように盗むことです。それに対してアドウェアの目的は、お金を使うようにユーザを説得することにあります。一般的にアドウェアはきわめて目立った動作を伴います。使用中のコンピュータが突然、ポップアップを表示し始めたり、検索エンジンをリダイレクトしたりします。それに対して、スパイウェアは検出されずにバックグラウンドでひそかに動作するように設計されています。スパイウェアもアドウェアも、類似の方法を利用してインストールされ、コンピュータを制御します。

スパイウェア

スパイウェアはもともと合法的なプログラムで、1990 年代に親が子供のオンライン アクティビティを監視したり、雇用者が従業員のコンピュータの使用を監視したりするために販売されていました。これらのプログラムの多くは、機能の 1 つとして「リモート インストール」（監視対象のコンピュータに物理的にアクセスすることなくインストールできる機能）を売り物にしていました。現在、ハッカーは、次のような機密データを記録できるスパイウェアプログラムを開発し、悪用するようになっています。

- ユーザ名
- パスワード
- クレジット カード番号
- 社会保障番号
- 企業機密
- 自宅の住所
- 個人電話番号
- 閲覧された URL
- 表示画面の画像
- 「スパイ サーバ」に中継される情報

スパイウェアは、ユーザに気付かれずにリモート インストールできるように設計されています。実際にスパイウェアがコンピュータにインストールされていると、スパイはユーザの行う動作（閲覧先の Web サイト、ユーザのタイプ入力、ユーザの画面に表示されている文書の内容など）をすべて見ることができます。スパイウェアには、スパイがユーザのコンピュータを完全に制御することを可能にするトロイの木馬プログラムが含まれている場合もあります。

アドウェア

アドウェアはスパイウェアよりも一般的であり、フリーウェアにバンドルされたマーケティング プログラムで構成されます。このプログラムは、ポップアップ広告をユーザのコンピュータに配信するように設計されており、ユーザを特定の検索エンジンにリダイレクトすることで開発元が手数料を得られるようになっている場合もあります。ユーザは、株価情報、天気予報、または交通情報を無料で受け取るなど、特定のプログラムを使用するための代償として、自発的に、承知のうえでアドウェアを自分のコンピュータにインストールし、広告を表示させる場合もあります。

一部のアドウェアは、市場調査の目的でユーザのネット サーフィンの傾向を追跡するように設計されています。しかし、現在の合法的なアドウェアの開発元のほとんどは、注記を付けて、ユーザのアクティビティの監視と記録は行っておらず、したがってセキュリティまたはプライバシー上の脅威にはならないと正当性を主張しています。

一部のアドウェアは、評判の悪い機能が組み込まれているため、スカムウェアと呼ばれています。これは、ユーザのコンピュータを使って高価な国際通話や市外通話を行うダイヤラ プログラムをインストールしたり、その目障りなプログラムを削除する際にユーザに対して強制的に課金したりします。

ほとんどは無害とはいえ、アドウェアが組織に与える潜在的影響には注意すべきです。Dell の最近の報告によると、Dell に対するテクニカル サポート コール最大の 12% がスパイウェアまたはアドウェアの問題に関連しています。ポップアップ広告が繰り返し表示されたり、ブラウザが乗っ取られたり、アドウェアの検索エンジンにリダイレクトされたりすることに、ビジネスユーザは腹立たしい思いをさせられています。設計の悪いアドウェアは CPU リソースを大量に消費したり、脆弱性をもたらしたり、システムのパフォーマンスに影響を与えたりし、さらにはエラー メッセージ、システムのフリーズ、およびクラッシュの原因になることもあります。アドウェアがいったんインストールされると、削除することは困難です。その目障りなプログラムがさらにアドウェアを導いてインストールするため、削除が不可能な場合もあります。

理想的なソリューションは、管理者がインストールを防止できるか、またはバンドルされたアドウェアが実行されてシステムの安定性と整合性が大規模に破壊されることを防止しながら、社員がフリーウェアやシェアウェアを安全に使用し続けられるようなソリューションです。

スパイウェアまたはアドウェアで考えられる動作

スパイウェアまたはアドウェアでは、ほかにも以下のような動作が考えられます。

- キーボード操作の監視
- ハードドライブ内のファイルのスキャン
- 他のアプリケーション（チャット プログラムやワード プロセッサなど）のスヌーピング
- 他のスパイウェアプログラムのインストール
- Cookie の読み取り
- デフォルト ホーム ページの変更
- スタートアップ時の起動とメモリへの常駐
- インターネットへの接続
- 特定の電話番号へのダイヤル
- 閲覧された URL の転送
- ネットワーク トラフィックの盗聴
- リモート管理ツールのインストール
- コンピュータの制御を奪うトロイの木馬のインストール
- ファイル、フォルダ、Cookie、Dynamic Link Library (DLL)、およびレジストリ エントリの追加

スパイウェアとアドウェアのインストール方法

ほとんどのアドウェアは偶然に、または故意に、スクリーンセーバー、ゲーム、天気および株価表示器、またはファイル共有ソフトウェアといったフリーウェアとともにダウンロードされます。フリーウェアはアドウェアからの収入に支えられています。ユーザはプログラムのダウンロードを承諾する前に法的なライセンス契約に関するただし書きを読んでアドウェアを拒否できますが、多くのプログラムでは「社会工学」が駆使されています。ユーザは繰り返し表示されるダウンロード画面にうんざりさせられ、最終的に「yes」をクリックしてアドウェアを受け入れることとなります。

スパイウェアは、ユーザが「no」をクリックした場合でさえ、不正にインストールされるように設計されている場合があります。さらに、アドウェアのベンダーやハッカーは、Web ページや E メール メッセージが閲覧されたときに侵入プログラムをインストールするアクティブ コンテンツ コードを使って、「ドライブバイダウンロード」を悪用します。疑わしいサイトをブロックするだけでは効果はありません。Web の自由さ、匿名性、および拡大によって、何百もの新しいスパイウェア サイトが増殖しています。

Harris の調査では、スパイウェアを含むとみられるサイトにアクセスしたと報告したユーザは全体の 6%にすぎませんが、IT マネージャの 92%は、自社が感染したことがあると指摘しています。スパイウェアは、ユーザに気付かれずに、または承諾なしにインストールされるように設計されており、スパイウェアのプログラマはスパイウェアの配信システムについてますます巧妙になっています。ネット サーフィンを安全な方法で行い、ライセンス契約を注意深く読むようにユーザを教育することは重要ですが、こうしたやり方だけで問題を解決することはできません。

スパイウェアの検出および削除ツールの限界

ほとんどのスパイウェアは E メールで配信されることはないため、ウィルス対策ソフトウェア製品は検出には効果がありません。スパイウェア検出ツールは、基本的にウィルス対策ソフトウェア テクノロジーと同じ原理で機能します。スパイソフトウェア検出ツールはシグニチャ、パターン マッチング、および既知のファイル名を使用して、コンピュータ上にスパイウェアがないか検出します。スパイウェア検出テクノロジーには、他の従来の情報セキュリティ テクノロジーと同じ重大な欠陥があります。つまり、スパイウェア検出テクノロジーは受動的で対処的です。これらのソリューションはシグニチャ検出に基づいているため、効率的にインストールされ管理される場合でも、個々のマシンでは新しい変化するスパイウェア攻撃によってネットワーク リソースとファイルに損害が発生します。

あらゆるスパイウェアを検出できる単一の検出ツールは存在しないように思われます。製品アナリストは多くの場合、複数の検出ツールを使用することを勧めています。1 つの製品が特定のスパイウェア プログラムを見落としとしても、他の製品で検出できるようにするためです。

ウィルス対策ソフトウェアの場合と同様、スパイウェア対策ソフトウェアの開発元には、次のような継続的なサポートの問題が付きまといまいます。

- 継続的なシグニチャ アップデートを行い、スパイウェア開発者に遅れをとらないようにする
- シグニチャを最新の状態に保つ
- 高レベルのフォールス ポジティブが発生する
- 新しい (Day Zero)、進化するスパイウェア プログラムは捕捉できない

スパイウェアおよびアドウェア除去ツールは、プログラムに感染したものを特定するには役立ちますが、感染そのものは防止できません。予防は非常に望ましい方法です。クリーンアップは長く複雑な処理となる場合があるからです。多くのスパイウェア プログラムは永続的であり、削除されるとそれ自体を再インストールし、複数のスパイウェア プログラムを同時に維持し、さらにはスパイウェア対策製品による検出を阻止するように設計されています。スパイウェアを削除することは不可能に近い場合もあります。たとえば、一部のプログラムは、Windows レジストリに数千ものエントリを作成するように設計されているため、レジストリ情報をチェックして修正するには、ほぼ実現不可能な量の高度な IT サポートが必要となります。

Cisco Security Agent — もう 1 つのアプローチ

Cisco Security Agent は予防的アプローチを採用し、動作ベースのセキュリティを利用してホスト上での悪意あるアクティビティを防止することに重点を置いています。有害なアクティビティは、スパイウェアまたはアドウェアのタイプに関係なく検出されブロックされます。Cisco Security Agent は、Cisco Theft of Information Prevention（情報漏洩/データ盗難対策）ソリューションの重要なコンポーネントです。

他のテクノロジーが単一ポイントの保護機能を（シグニチャが既知の場合のみ）提供するのに対して、Cisco Security Agent は、侵入のあらゆる段階でホストへの攻撃をプロアクティブに阻止し、複数階層の防御を実現します。さらに、Cisco Security Agent は、既知のシグニチャが存在しない新しい攻撃からも保護できる設計となっています。

アプリケーションが動作するときに、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、動作の継続についてリアルタイムで「許可」または「拒否」の決定を行い、さらにその動作要求のログギングが適切かどうかを判定します。セキュリティ ポリシーとは、IT またはセキュリティ管理者がサーバとデスクトップの保護のために、個別または企業全体に割り当てるルールの集合です。これらのルールは、ユーザが Web サイトの閲覧を行うための安全な環境を提供します。Cisco Security Agent は、分散ファイアウォールを実装するセキュリティ ポリシー、OS（オペレーティング システム）のロックダウンと整合性の保証、悪意のあるモバイル コードからの保護、および監査イベント収集の機能を、サーバおよびデスクトップ用のデフォルト ポリシーに結合することによって、スパイウェアとアドウェアに対する階層的な防御の保護を提供します。

保護機能は悪意のある動作をブロックすることに基づいているため、このデフォルト ポリシーによって既知と未知の両方の攻撃を阻止でき、アップデートの必要はありません。関連付けは、Cisco Security Agent と Management Center コンソールの両方で実行されます。エージェント ベースの関連付けによって精度が大幅に向上しているため、合法的なアクティビティをブロックすることなく実際の攻撃または誤使用を識別できます。

Cisco Security Agent は Windows OS を強化し、スパイウェアによって OS の重要なバイナリ ファイルやコンフィギュレーション設定値が変更されることを防止します。この機能ではファイル システムの内容に対する暗号分析を利用する必要がないため、システムのパフォーマンスへの影響は事実上ありません。

Cisco Security Agent :

- キーボードのログギングを検出し、防止する
- システムの実行可能ファイルへの未認証の書き込みを防止し、OS の整合性を保持する
- シェルを経由したシステム上での任意のコマンド呼び出しによる攻撃を防止する
- 障害が起きた可能性のあるアプリケーションが既存のアプリケーションを損傷したり、新しいアプリケーションをダウンロードしたりすることを防止する
- デスクトップで実行できるアプリケーションを監視し、実行する
- トロイの木馬を検出し、阻止する
- モバイル コード（Java、JavaScript、ActiveX など）を使用したドライブバイダウンロードから Web ブラウザを保護する
- DLL の制御フックを利用した「アプリケーションの乗っ取り」から保護する
- アプリケーション内での危険なユーザ動作を防止する（インスタント メッセージング アプリケーションを使用したファイルのダウンロードなど）
- 既知および未知のバッファ オーバーフロー攻撃（ユーザのコンピュータへスパイウェアをインストールするために悪用されることがある）から保護する
- 実行できるアプリケーションを中央で指定でき、管理者が疑わしいスパイウェアの実行を防止できる
- 機密データ ファイルを読み取ることのできるアプリケーションを監視または阻止する機能を提供する
- メディア デバイスを監視し、スパイウェアが Web フォンや Webcam を起動するとユーザに警告する

コンピュータで実行されているアプリケーションの追跡

Cisco Security Agent は、どのようなアプリケーションが単一のコンピュータまたはワークグループ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際に呼び出されているか、どのアプリケーションがネットワークを使用しているか、そのアプリケーションはネットワーク クライアントかネットワーク サーバか、およびそのアプリケーションが通信するすべてのリモート IP アドレスの ID を追跡できます。また、Cisco Security Agent は、ユーザ別のインストール情報や望ましくないアプリケーションが実行されようとしているかどうかなど、すべてのリモート システム上のあらゆるアプリケーションの状態を確認できます。

Cisco Security Agent によって、管理者は任意のコンピュータの任意のアプリケーションについて、詳細な科学的検査を実行できます。Cisco Security Agent は、アプリケーションの動作をリアルタイムで観察します。これには、アクセスするすべてのファイルと読み取りまたは書き込みの区別、すべてのネットワーク接続と着信（サーバ）または発信（クライアント）の区別、リモート コンピュータのアドレス、すべてのレジストリ アクセスと読み取りまたは書き込みの区別、および COM オブジェクトのすべてのロードが含まれます。Cisco Security Agent は、アプリケーションの動作に関する情報を収集し、それを管理者向けのレポートにまとめ、さらにアプリケーションの通常の動作に基づいて制御ポリシーを作成します。

Cisco Security Agent のフレームワークを使用すると、管理者は以下のことを中央で集中的に行うことができます。

- リモート コンピュータでインストールまたは実行されている未認証または未知のアプリケーションを識別する
- 未知のアプリケーションが実行されているときはそのアプリケーションが実行する動作を識別し、未知のアプリケーションのうち悪意のあるものと良性のものを区別する
- アプリケーションが実行を許可されている動作、またはアプリケーションが実行できる機能を、動作の分析に基づいて制御する

Cisco Security Agent によって、管理者は企業全体で実行されている疑わしいスパイウェア アプリケーションの一覧を作成し、分析に利用できます。この分析から、管理者はスパイウェアが行うことのできる動作に関するポリシーを開発できます。たとえば、管理者は、プログラムが別のコンピュータにインストールされることを自動的に禁止したり、すでにインストールされている場所でその動作を厳しく制限したり、それをまったく実行できないようにしたりするポリシーを作成できます。

アドウェアの利点を考慮して、企業はユーザがアドウェアを安全に実行することを許可する場合があります。たとえば、システム管理者は、「このアプリケーションはユーザに広告を提供するが、ユーザのキーボード操作を記録したり、ポートを開いてデータをアドウェア サーバに中継したりすることはできない」と規定したポリシーを設定できます。

図 1 Cisco Security Agent のカスタム レポート

Product	Number of hosts installed
Fun Web Products Easy Installer	1
Kazaa Media Desktop 2.5	1
My Web Search (Outlook, Outlook Express, and IncrediMail)	1
My Web Search (Smiley Central)	1
Search Assistant - My Web Search	1
Spin4Dough	1

Cisco Security Agent は、カスタム レポートを作成する機能を備えています。カスタム レポートでは、企業の承認済みのリストに記載されていない外部の IP アドレスに接続しようとするすべてのアプリケーションが示されます。

疑わしいスパイウェアの種類を設定するため、管理者は Cisco Security Agent を使用して、たとえば、企業の承認済みのリストに記載されていない外部の IP アドレスに接続しようとするすべてのアプリケーションを示すレポートを作成できます（図 1）。環境とセキュリティ ポリシーに応じて、管理者はブラウザ、E メール クライアント、または IM クライアントを除外したり含めたりできます。

Cisco Security Agent の動作

Cisco Security Agent は、インストールの防止、および侵入のあらゆる段階で防御を提供するという 2 つの方法で、効果的にスパイウェアから保護します。

インストールの防止

アドウェアはいったんインストールされると、コンピュータから削除することが困難な場合があります。Cisco Security Agent は、プログラムがドライブバイダウンロード方式を使用する場合でも、インストールを防止するのに役立ちます (図 2 および図 3)。

図 2 一部のアドウェアは「キャンセル」要求を無視してダウンロードされる



図 3 Cisco Security Agent はアドウェアを検出して複数の対処方法を提供する

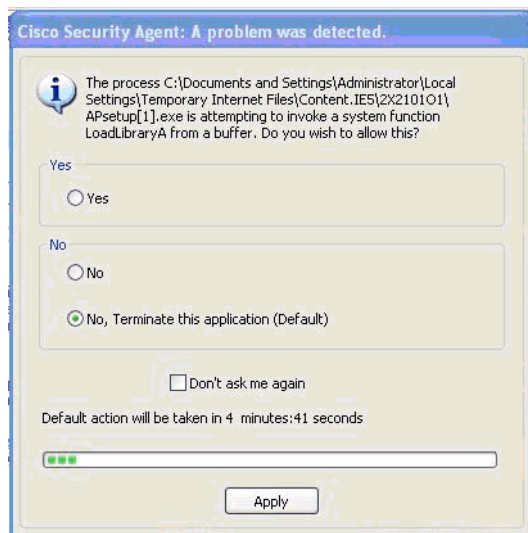


ひそかにダウンロードされたアドウェアが実行されようとした場合、対応として Cisco Security Agent は、ユーザが「Yes」をクリックしないかぎり、デフォルトでそのアプリケーションを終了させます (図 3)。管理者は、アプリケーションがユーザの操作を介さずに行われることを自動的に阻止するように、Cisco Security Agent を設定できます。「Don't ask me again」オプションに注意してください。スパイウェアがユーザに対して繰り返しダウンロード要求を表示する場合 (「Yes」をクリックするようにユーザをだましたり腹立たしい思いをさせたりする社会工学の手法の 1 つ)、ユーザは「Don't ask me again」をクリックするだけでこの要求を停止させることができます。

インストール済みの場合は悪意のある動作を阻止

Cisco Security Agent は、侵入のあらゆる段階で階層的な防御を提供します。ユーザが度重なるセキュリティ警告にもかかわらずダウンロードとインストールを承認した場合でも、Cisco Security Agent は、危険なまたは破壊的な動作を実行するスパイウェアからの保護を継続します（図 4～7）。

図 4 Cisco Security Agent は疑わしいアクティビティの追跡を継続



Cisco Security Agent が問題を検出しているにもかかわらずユーザが「Yes」をクリックし、プログラムがインストールされた場合、Cisco Security Agent は疑わしいアクティビティの監視を継続し、ユーザに警告します（図 4）。この場合、Cisco Security Agent は、プログラムが自己書き換えコードを使用しているか、またはバッファオーバーフロー攻撃で破壊されている場合によく見られる動作を、スパイウェアが実行できないようにします。

図 5 キーボード スニффィングに関するユーザへの問い合わせ



図 5 では、Cisco Security Agent は Silentlog というプログラムを検出しています。Silentlog は「キーストローク ロガー」プログラムで、すべてのキーボード入力をひそかにキャプチャし、ファイルにロギングします。スパイウェアは多くの場合、このようなキーストローク ロガーをインストールしてユーザが入力するパスワードをキャプチャします。

図 6



図 6 は、Cisco Security Agent が一般的な商用スパイウェアプログラムである WinSpy によるキーボード操作のロギングをブロックする様子を示しています。WinSpy は、「スパイ対策ソフトウェアに影響を受けない」ことを売り文句にしています。Cisco Security Agent はこうしたキーストローク ロガーを、ファイル名によってではなく、アプリケーションが行う動作を監視することによって検出することに注意してください。

図 7 ブロックされたスパイウェアのアクティビティを示す Cisco Security Agent のログ

```
12/16/2004 2:53:02 PM: The process 'C:\WINNT\ntsv32.exe' (as user W2KSP0-DESKTOP\win2k) attempted to call the function OpenProcess("<pid:66130>") from a buffer (the return address was 0x40f3cd). The code at this address is '008b5508 52536800 060000e8 c3a5ffff 8bf0ffd7 3bf3740c 8b451050 56e89da6'. This either happens when a process uses self-modifying code or when a process has been subverted by a buffer overflow attack. The user was queried and a 'Terminate' response was received. The response was the default taken after a timeout.

12/16/2004 2:53:14 PM: The process 'C:\WINNT\ntsv32.exe' (as user W2KSP0-DESKTOP\win2k) attempted to call the function CreateProcessA("ipconfig") from a buffer (the return address was 0x404bcf). The code at this address is
```

図 7 は、WinSpy に感染したコンピュータに関する管理者ログを示しています。スパイウェアの動作はシステムの起動中に実行されたため、ユーザはセキュリティ メッセージを受け取りませんでした。Cisco Security Agent は、ユーザの操作を介さず、自動的に悪意のあるアクティビティを終了させました。

特定の動作パターンへの対応

表 1 は、スパイウェアが行うと考えられる動作の各種カテゴリ、およびエンドポイントを保護するために機能する Cisco Security Agent のルールの一覧です。

表 1 Cisco Security Agent のルール

カテゴリ	動作	Cisco Security Agent のルール
Cookie	サイト間を移動するユーザのコンピュータ上の Web サイト情報（登録の詳細情報など）を保存する。	Cisco Security Agent は、Cookie 情報へのアクセスをブラウザ以外のプログラムから保護できる。
アドウェア	ポップアップ広告を配信する。	Cisco Security Agent は、ポップアップ（JavaScript の新しいウィンドウなど）に対してブラウザ固有の制御を提供しない。ブラウザの外部で実行されるアドウェアプログラムによって、Cisco Security Agent のインストールポリシーが起動される（サイレントインストールは不可能）。
ブラウザヘルパーオブジェクト	起動時にブラウザを乗っ取り、多くの場合、ユーザを未知の検索エンジンにリダイレクトする。URL を追跡し、収集し、中継する場合もある。	ブラウザヘルパーオブジェクトへの書き込みは、システムプロセスのみに限定される。
ブラウザプラグイン	新しいツールバーをブラウザ内に作成する。URL を追跡し、収集し、中継する場合もある。	ブラウザプラグインがインストールされると、Cisco Security Agent のインストールポリシーが起動される（サイレントインストールは不可能）。インストールが許可された場合、これらは使用分析レポートに記載される。
キーロガー	キーボードを「スニффイング」してキーボード操作を記録し、パスワード、クレジットカード番号、その他の機密情報を第三者に中継する。	システム API ルールによってキーストロークロガーを検出し、ブロックする。
ネットワーク管理ツール	ネットワークアクティビティをリモート監視し、攻撃者によって悪用されることがある。	ネットワーク管理ツールがインストールされると、Cisco Security Agent のインストールポリシーが起動される。
リモート管理ツール	リモートコンピュータのユーザ権限を与え、攻撃者がファイルの変更、転送、削除やキーボードの制御ができるようにする。	リモート管理ツールがインストールされると、Cisco Security Agent のインストールポリシーが起動される。ネットワークベースのアプリケーションは、特定の権限がなければシステムファイルを変更できない。
トロイの木馬	問題のないアプリケーションに埋め込まれた悪意のあるコード。OS を損傷したり、ファイルを削除したり、ハードドライブを破壊したりする場合がある。	Cisco Security Agent によって、トロイの木馬、ワーム、およびウイルスから強力に保護できる。詳細については、次のリンクを参照。 www.cisco.com/jp/go/csa
ワーム	ネットワークをクラッシュさせることができる自己複製および自己増殖型のプログラム。スパイウェアはワームを利用して拡散する場合がある。	
ウイルス	Eメールで配信され複製される自己複製型プログラム。スパイウェアはウイルスを利用して拡散する場合がある。	

結論

Cisco Security Agent は、スパイウェアとアドウェアの両方に対抗する強固で効果的な保護を提供します。検出を動作ベースで行うことによって、Cisco Security Agent はシグニチャのアップデートを行わなくても新しい未知のスパイウェアをブロックします。この「ゼロアップデート」の予防機能によって、アップデートの実行に関連するセキュリティ管理コストが削減されます。

安定したエンタープライズ管理機能によって、管理者は数十万もの Cisco Security Agent を効率的に展開および管理できます。ポリシーの作成と警告のレポートは、中央集中型となっています。ルールとポリシーはユーザ、グループ、ロケーション、または Network Admission Control (NAC) のステータスに基づいて適用できます。アプリケーション インベントリ機能によって、管理者は組織で実行されている未知のアプリケーションを追跡し、その動作を分析し、疑わしいスパイウェアまたはアドウェアのカテゴリに分類し、さらにその動作を制限または禁止するルールを作成できます。

最後に、スパイウェアからの保護機能はアドオンではなく、追加コストなしで組み込まれます。また、Cisco Security Agent は、ポート スキャン、バッファ オーバーフロー、トロイの木馬、不正な形式のパケット、悪意のある HTML 要求、E メール ワームなど、あらゆる種類の攻撃に対抗するプロアクティブな保護を提供します。複数のセキュリティ機能を集約することによって、Cisco Security Agent は、ホストへの侵入防止、分散ファイアウォール、悪意のあるモバイルコードからの保護、OS の整合性の保証、アプリケーションの使用調査、および監査ログの統合を、すべて単一のエージェント パッケージで提供します。

Cisco Security Agent の詳細については、次の URL にアクセスしてください。

www.cisco.com/jp/go/csa

情報漏洩/データ盗難の防止対策に関するシスコの統合ソリューションの詳細については、次の URL にアクセスしてください。

<http://www.cisco.com/jp/solution/netsol/security/theft/>

©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>

0120-092-255 (通話料無料)

電話受付時間: 平日 10:00 ~ 12:00, 13:00 ~ 17:00