

Cisco Security Agent Profiler

次世代の Cisco® Security Agent ネットワーク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（「エンドポイント」とも呼びます）をセキュリティの脅威から保護します。Cisco Security Agent には、悪意のある動作を未然に識別し防御するという、これまでのエンドポイントセキュリティソリューションには見られない機能があり、これによって、既知であるか未知であるかを問わず、企業の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排除します。Cisco Security Agent はシグニチャに依存するのではなく、動作を解析するため、少ない運用コストで堅牢なセキュリティ保護を実現します。

Cisco Security Agent Profiler では、特定のアプリケーションの動作を自動分析し、個々のアプリケーション固有の保護ポリシーを構築することによって、セキュリティ機能を強化します。

利点

- すべてのファイル、ネットワーク、レジストリ、アプリケーションからの COM アクセス要求を自動で監視することで、不明アプリケーションによる攻撃の調査が簡素化される。
- アプリケーションの動作を観察に基づいた保護ポリシーが構築される。
- 新旧の社内アプリケーションすべてが保護される。

- Management Center for Cisco Security Agent との統合：アラートからホットリンクされているため、ただちに Cisco Security Agent によって保護されているシステム上のアプリケーションの監視を開始できる。
- セキュリティに関連する動作の分析を 1 か所で自動的に行うため、セキュリティの管理コストを低減する。
- 企業規模のスケーラビリティによって、1 プロファイラにつき数千のエージェントに拡張可能なアーキテクチャが提供される。

セキュリティ調査の自動化

セキュリティを管理する上で最も困難なことの 1 つに、アラートを受信した後の対処方法の判断があります。アラートには、多くの場合、セキュリティオペレータが対応を決める際に必要な情報のうち一部しか含まれていません。現在のセキュリティポリシーを修正する必要があるか、システム管理者に報告する必要があるか、ポリシー違反であるか、それともこのイベントは正常な予想範囲内のことか。アラートに含まれている情報の一部からこれらを判断するのは、困難または不可能です。

Cisco Security Agent Profiler では、Cisco Security Agent から受信したアラートの調査を集中管理します。特定のアプリケーションを監視したり、アプリケーションによるすべての動作要求を観察するエー



ジェントを中央に構築できます。ファイル システム、ネットワーク、レジストリ、COM オブジェクトへの各アクセス要求は、ログに記録され、エージェントから Management Center にアップロードされます。Management Center では、データが分析され、オペレータへのレポートが作成されます。

このようにアプリケーションの動作を自動的に集中監視することで、セキュリティ ポリシーを侵害する動作だけでなく、アプリケーションのすべての動作についての詳しい情報を得られます。このような詳細な情報を得られれば、悪意のある攻撃を容易に特定でき、疑わしいと判断された良性の動作の確認にも役立ちます。Cisco Security Agent Profiler を使用すると、オペレータは、事例データを基に判断するのではなく、疑わしいアプリケーションそのものを確認して判断することができます。判断要素には次のようなものがあります。

- そのアプリケーションによるネットワーク接続はどれか。そのアプリケーションと通信しているリモートシステムはどれか。アプリケーションはネットワーク クライアントとして機能しているか。サーバとして機能しているか。その両方か。Secure Sockets Layer (SSL) 暗号化接続を使用して動作を隠すアプリケーションが多くなっています。Cisco Security Agent Profiler では、このようなアプリケーションの動作を見ることができます。
- そのアプリケーションがアクセスしているファイルはどれか。その中に機密事項を扱っているデータファイルや、禁止されているファイル (リモート システムに MP3 ファイルを送信しているネットワーク アプリケーションなど) があるか。ファイルは読み取られているか、または書き込まれているか。
- どのレジストリ キーが読み取られたり書き込まれたりしているか。多くの場合、これによって、アプリケーションやベンダーの名前を特定できます。
- COM オブジェクトがロードされているか。多くのアプリケーションでは、関数をロード可能なオブジェクトとして提供しています (Microsoft Office や電子メールプログラムなど)。これらのオブジェクトを使用すると、不明アプリケーションの動作目的を判断できます。

この動作を監視し、集約したレポートをセキュリティ オペレータに提示することで、より迅速に確かなセキュリティ上の意思決定を可能にします。

Management Center for Cisco Security Agent との統合

Cisco Security Agent Profiler は Management Center for Cisco Security Agent にインストールされ、Cisco Security Agent で保護されているシステム上のアプリケーションの動作を監視するために使用されます。Management Center では、イベント ログに表示されるアラートからのホットリンクがあり、それによって、プロファイラは、アラートを発したエージェント上の特定のアプリケーションを調査します。アラートを発していないアプリケーションに対しての分析もできます。たとえば、Cisco Secure IDS センサーがアラートを確認した場合に、プロファイラからも調査を支援できます。

専用の保護ポリシーの構築

多くの組織では、ビジネスにおいて重要な機能を果たすカスタム アプリケーションを使用しています。組織が、これらのアプリケーションに対するセキュリティ保護を強化したいと考えていても、アプリケーションのソースコードを変更する以外に方法はありませんでした。アプリケーションに多くのセキュリティ層を設けても、このセキュリティ方法で必要な機能をブロックできているかどうかは確信が持てないままでした。セキュリティ保護の手段そのものが、アプリケーションに障害をもたらす可能性のある、非常に大きなリスクとなっているとも言えます。



Cisco Security Agent Profiler には、すべてのアプリケーションの動作を監視する機能があり、これによって、セキュリティの要件に合わせてアプリケーションの動作を制限するのではなく、アプリケーションの要件に合わせてセキュリティをカスタマイズするという独自の機能が提供されます。アプリケーションによる通常どおりのリソースアクセスを、不明アプリケーションの動作を調査するプロセスと同じプロセスで監視できます。このデータは、エージェントによって収集され、プロファイラによって、そのアプリケーションに対する Cisco Security Agent の保護ポリシーが自動構築されます。ポリシーには、実際に観察されたアプリケーションの動作が反映されているので、そのアプリケーションに必要なセキュリティ保護が自動的に構築されます。

Cisco Security Agent Profiler では、どんなアプリケーションに対しても保護ポリシーを構築できます。アプリケーションの動作についての情報やアプリケーションのソースコードを入手する必要はありません。プロファイラで構築された保護ポリシーは、Management Center で管理されている他のエージェントで使用したり、別の Management Center にエクスポートして使用することもできます。

技術仕様

使用できる言語：すべてのエージェントについて、英語（アメリカ英語）のみです。（日本語は近日対応予定）

インストール要件

プロファイラを機能させるには、Management Center にライセンス キーをインストールする必要があります。

発注情報

Cisco Security Agent Profiler は、Management Center for Cisco Security Agent にライセンス キーをインストールすると有効になります。表 1 に、Cisco Security Agent Profiler の部品番号を示します。

表 1 Cisco Security Agent の部品番号

部品番号	製品説明
CSA-PROILER-K9	Cisco Security Agent Profiler

©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