

シグニチャを使用しないネットワーク エンドポイントのセキュリティホストへの侵入防止に対するポリシーベースのアプローチ

要約

今日の分散型オープン ネットワークでは、ネットワーク エッジやネットワーク境界を保護するだけでは不十分です。エンドポイント（ホスト）にあるデータも保護する必要があります。従来のエンドポイントセキュリティテクノロジーは、攻撃の分析後に開発されたシグニチャに依存する対処的なものでした。また、これらのテクノロジー（パーソナルファイアウォール、アンチウイルススキャナ、監査製品、整合性検証製品など）は、分野ごとに細分化されており、それぞれが問題の一部分だけを取り扱っているため、何種類ものエージェントを展開して管理する必要がありました。管理者の負担を重くしていた原因はここにあります。

Slammer や NIMDA などの最近の攻撃は、シグニチャによる識別を巧妙にすり抜け、アップデートが提供される前にサーバやデスクトップへ急速に広まりました。これらの攻撃に利用された脆弱性を修復するパッチは、6 か月以上も前に提供されていました。大企業におけるセキュリティメンテナンスでは、何万に及ぶエンドポイントに対処する必要があります。また、脆弱性の数は年々増え続けているため、パッチの適用作業は際限のないアップデート競争へと発展しつつあります。

この資料では、シグニチャベースのエンドポイントセキュリティテクノロジーの現状を調査し、その重大な欠点を分析した上で、ポリシーベースの新しいテクノロジーを採用した Cisco® Security Agent 侵入保護セキュリティソフトウェアの概要を説明します。このソフトウェアは、今日のオープン ネットワークを標的とした攻撃に対する予防的な対策を必要としている処理環境に、ホストベースの現実的な戦略を導入します。

侵入検知テクノロジー

侵入検知テクノロジーには、ホストベースのものと、ネットワークベースのものがあります。侵入検知製品とは、デバイスまたはネットワークを監視して、悪意のあるアクティビティを検出するソフトウェア製品およびハードウェア製品の総称です。侵入検知ソフトウェアは、ネットワークやリソースのアクティビティと、すでに確認されている悪質なアクティビティのシグニチャとを比較します。この機能は、全体的なセキュリティ戦略の中でどのような役割を果たすのでしょうか。業務の遂行におけるインターネット接続への依存度が高まるにつれて、従来型のネットワークセキュリティテクノロジーに課せられる負担はますます重くなっているため、これに関連する重要なポイントが明確になり始めています。



ネットワーク侵入検知システム

Network Intrusion Detection System (NIDS; ネットワーク侵入検知システム) は、ネットワーク回線上に常駐してネットワークのパケットを分析する専用のソフトウェアシステムです。パケット内にカプセル化されたデータは、既知のネットワーク攻撃シグニチャのデータベースと比較されます。ネットワークを通過中のデータが、データベース内にリストされている既知の攻撃と一致しない場合は、疑われることなくトラフィックが通行されますが、パケットデータが既知の攻撃と一致した場合は、何らかの応答が生成されます。このような応答は、アラートの形式でログファイルまたはネットワーク管理者向けのページに送信されます。

ホストベースの侵入検知システム

本来、Host-based Intrusion Detection System (HIDS; ホストベース侵入検知システム) は、監査ログファイルを監視するための製品として開発されました。従来のシステムを使用する場合、管理者は1日の終わりにログファイルを調べて、特定の時間帯に発生した疑わしいアクティビティを発見する必要があります。この作業は、単調だけでなく、問題を事後的にしか発見できません。最近の HIDS では、同様のスキャン作業をリアルタイムで実行するローカルエージェントが使用されます。ログファイルにイベントが記録されると、リソース上にインストールされているローカルのソフトウェアエージェントによって、そのイベントが攻撃のデータベースにリストされているイベントと一致するかどうかを確認されます。一部の HIDS には、アプリケーションのログファイルを監視して、新たな攻撃の形跡がないかどうかを調査する機能もあります。また、HIDS には、ローカルファイルに変更や改ざんが加えられていないかどうかを監視する機能もあります。イベントが攻撃のプロファイルと一致した場合は、HIDS からアラートが送信され、悪意のあるアクティビティによって生じる被害を阻止するために、可能な対策の中からいずれか1つが実行されます。

対処的な IDS テクノロジーの限界

すべての IDS テクノロジーには、受動的で対処的な他の従来型情報セキュリティテクノロジーと共通する重大な欠点があります。これらのソリューションは、シグニチャによる検出を前提としているため、製品を効果的にインストールして管理している場合でも、ネットワークリソースや個々のマシン上にあるファイルが攻撃の被害を受ける可能性があります。ネットワークベースの IDS も、ホストベースの IDS も、それぞれ固有の弱点を持っています。

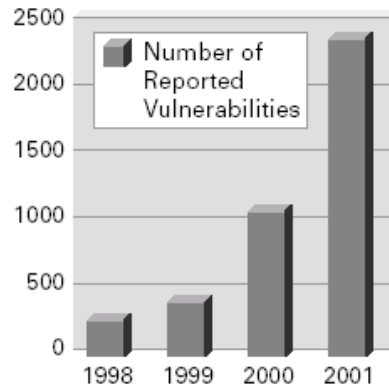
増え続ける脆弱性

シグニチャベースのセキュリティテクノロジーは、脆弱性があまり報告されていなかった 1990 年代の半ばに考案されました。CERT によると、1995 年に発表された脆弱性はわずか 171 件でした。つまり、毎月 12 種類程度のシグニチャを追加してシステムを更新していれば、シグニチャベースの製品でも、比較的良好なネットワークセキュリティを維持することができました。

それ以来、脆弱性の報告件数は増加の一途をたどり、状況は大きく変わりました。毎年報告される脆弱性の件数は急激に増え続けており、衰える気配はありません。亜種の数も増えています。図 1 は、1990 年台の後半から 2000 年台の前半かけて報告された脆弱性の数の増加を示しています (出典: CERT)。



図 1
増え続ける脆弱性の数



シグニチャベースのセキュリティ製品を使用して攻撃を阻止するには、シグニチャが必要になります。2001年には、毎日6件の新しいシグニチャが必要でした。現在、この数字は、1日あたり12件に近づきつつあると推測されます。シグニチャベースのセキュリティがこの状況に追い付くことができないのは明白です。脆弱性の報告件数が急激に増加しているため、攻撃に対するシグニチャの提供が間に合わない可能性が高いからです。

アラートと False Positive の管理

パターンやシグニチャを照合するテクノロジーでは、ホストやネットワークで実行された正常な振る舞いが、悪意のあるアクティビティと誤認され、誤ったアラームが生成される場合があります。多数の False Positive および False Negative が発生する傾向があります。大量の False Positive が管理コンソールに送信されるため、製品と管理者の効率が低下し、管理者は不確実なセキュリティアラートへの対応を余儀なくされます。

別のアプローチ

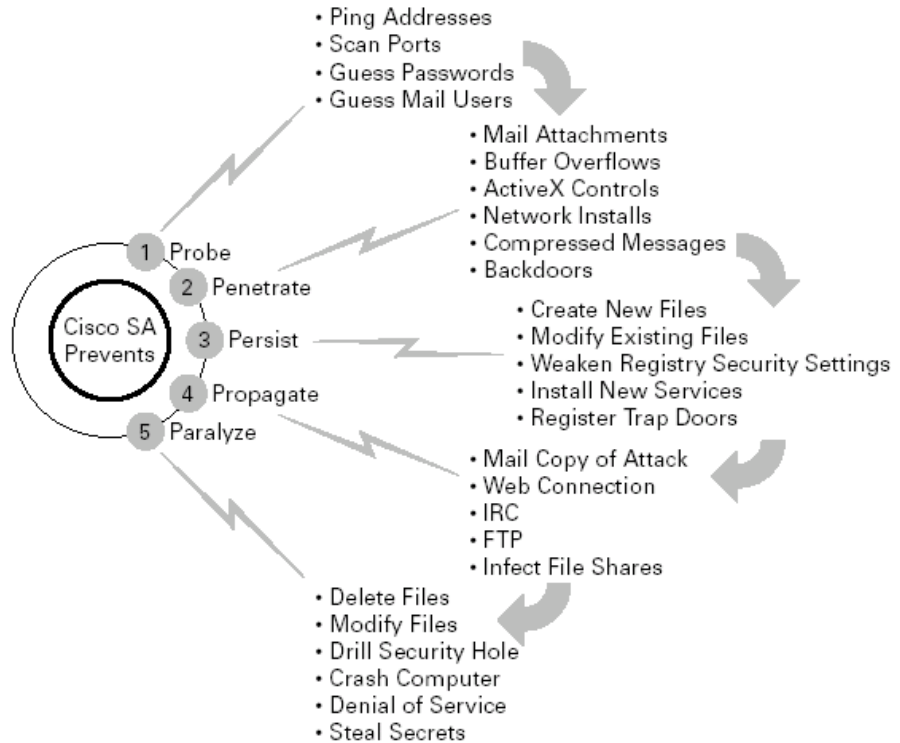
現在では、未発表あるいは未発見の脆弱性に対する攻撃を検出できる別のアプローチが求められています。興味深いことに、すべての攻撃には共通性があるため、このような検出も正確に行うことができます。

システム攻撃のライフ サイクル

図2に示すように、すべての攻撃は同一の論理的過程をたどります。



図2
システム攻撃のライフ サイクル



1. 探索フェーズでは、脆弱なターゲットが特定されます。このフェーズの目的は、攻撃可能なコンピュータを探すことです。
2. 侵入フェーズでは、脆弱なターゲットにエクスプロイトコードが送信されます。このフェーズの目的は、バッファオーバーフローなどの攻撃を利用して、ターゲットにエクスプロイトコードを実行させることです。
3. これが成功すると、エクスプロイトコードはターゲット上への常駐を試みます。常駐フェーズの目的は、ターゲットのシステムが再起動された場合でも攻撃者のコードが実行されて、攻撃者がアクセスできる状態を確保することです。
4. 攻撃者が組織のネットワークにアクセスできるようになると、他のターゲットにも攻撃が拡大します。増殖フェーズでは、エクスプロイトコードを拡散できる近隣の脆弱なデバイスが検索されます。
5. 実際の被害は、機能麻痺フェーズにおいて初めて発生し、ファイルが消去されたり、システムに障害が発生したり、Distributed Denial-of-Service (DDoS; 分散型サービス拒否) 攻撃が開始されます。

侵入フェーズと常駐フェーズの間には、大きな分岐点があります。最初の2つの段階は、非常に亜種の多いフェーズです（攻撃の形跡が常に変化しています）。また、防御システムによる検出を回避するために、Web文字列のUnicode符号化やパケット断片のオーバーラップといった技術がしばしば利用されます。侵入段階における攻撃の特定では、一定量の解釈（ターゲットコンピュータがそのネットワークパケットをどのように処理するかに関する推測）が伴う場合があるため、誤ったアラームが大量に生成される傾向があります。



これとは対照的に、最後の3つの段階は、長期にわたって非常に似通っており、攻撃者が実行できる悪質なアクティビティの種類は限られています（オペレーティングシステムの改ざん、新規ユーザアカウントの追加、発信ネットワーク接続の確立、ファイルの削除など）。これらのアクティビティは、以前からほとんど変わっておらず、1988年のMorrisワームと2001年のNIMDAワームでは、同じタイプの被害が報告されています。また、オペレーティングシステムのバイナリ変更といったアクティビティは、きわめて例外的で特殊なイベントであるため、これらの段階で攻撃を正確に特定することは比較的容易です。

つまり、ライフサイクルの初期の段階で攻撃を特定しようとする、各攻撃の特徴が変化するため、シグニチャのアップデート競争が生じることとなります。システムセキュリティは、攻撃のすべての段階で確保する必要がありますが、実際に被害が生じる最後の3段階が特に重要になります。このような重層的防御ソリューションを提供することが、シスコの振る舞いベーステクノロジーの最大の目標です。

脆弱性の状況に対処することは、明らかに困難です。シグニチャベースのホストセキュリティでは、脅威のペースに追い付くことができず、その遅れはますます大きくなり始めています。シスコのテクノロジーは、コンピュータシステムへの攻撃と破壊に使用される振る舞いを分析することで、多くの欠点を持つ従来型テクノロジーからの根本的な脱却を可能にします。

振る舞いの種類

振る舞いベースのセキュリティでは、攻撃に重点を置くのではなく、ホスト上で行われる悪質なアクティビティを阻止することに重点を置いています。振る舞いに的を絞ることで、攻撃の種類に関係なく、有害なアクティビティを検出して阻止できます。たとえば、セキュリティ関連の振る舞いの1つとして、Webサーバによるシステムへの新規ユーザアカウントの追加があります。（侵入段階から見ると）これを実行する可能性がある攻撃は数多く存在します。シグニチャベースのセキュリティシステムでは、これらのすべてに対応するシグニチャが必要ですが、振る舞いベースのシステムではその必要がありません。

セキュリティ関連の振る舞いは、次の3つのクラスに分類されます。

- **悪意のあるアクティビティ**：この種の振る舞いは、一般的に攻撃ライフサイクルの最後の3段階で発見されます。例としては、オペレーティングシステムに対する不正な改ざんやファイルの削除などがあります。悪意のあるアクティビティは常に排除する必要があるため、このレベルでのシステムセキュリティは非常に低コストで展開できます。悪意のあるアクティビティを阻止するための環境調整はほとんど、あるいはまったく必要ありません。
- **ポリシー関連のアクティビティ**：この種のアクティビティには、必ずしも悪意はありませんが、望ましくありません。たとえば、ネットワーク管理者は、ユーザがインスタントメッセージングのプログラムを使用してファイルをダウンロードできないようにする場合があります。このようなファイルは、企業のウィルススキャナによってスキャンされないからです。この明示的に禁止されていない限りすべてが許可される手法を使用すれば、経営陣からのポリシーに関する指示をすばやく実装できます。
- **アプリケーション ラッピング**：最高レベルのシステムセキュリティでは、アプリケーションを完全にロックすることも可能です。これらのアプリケーションには、既知の安全な振る舞いだけが許可されます。適切な振る舞いを強制することにより、新種の攻撃か単なるエラーかを問わず、適切な振る舞いの範囲から外れるすべての振る舞いをきわめて効果的に処理できます。基本的に、明示的に許可されていない限りすべてが禁止される手法を使用すると、最大レベルのシステムセキュリティが提供されますが、調整作業が複雑になります。ただし、ほとんどのシステムでは、ここまで厳格なレベルの制御は必要ありません。



大半の組織は、悪質なアクティビティを阻止するだけで満足しているため、ポリシー関連のアクティビティやアプリケーション ラッピングを含めた振る舞いベースの制御は実施されていません。

Cisco Security Agent によるサーバおよびデスクトップの侵入防御

Cisco Security Agent は、ネットワーク全体への攻撃の拡散を防ぐインテリジェントなエージェントをデスクトップおよびサーバに展開することで、妥協のない侵入防御セキュリティを実現する企業向けソリューションです。

Cisco Security Agent は、ユニークかつ徹底的な予防的アプローチを利用して、侵入を阻止します。既存のホストベースのセキュリティソリューションには、既知の攻撃シグニチャのデータベースに依存する攻撃中心のソリューションや、ユーザアクセスの制御を行うユーザ中心のソリューションしかありませんでしたが、Cisco Security Agent は振る舞い中心のソリューションです。Cisco Security Agent は、ミッションクリティカルアプリケーションの振る舞いに的を絞ることで、既知のホストベースのセキュリティリスクだけでなく、未知のリスクからも企業を保護します。

Cisco Security Agent には、5 つの重要な利点があります。

1. **デスクトップおよびサーバの侵入保護**：セキュリティのアップデート競争を克服するために必要なことは、検出ではなく防御です。
2. **大幅な精度の向上によって実現される防御**：セキュリティ製品が正常な振る舞いと悪質な振る舞いを区別できなければ、攻撃を阻止できません。ほとんどのセキュリティ製品では、生成される False Positive（誤ったアラーム）の数が多すぎるため、正当なアクティビティが数多く阻止されます。Cisco Security Agent の自動関連付け機能と、重層的防御のアプローチを組み合わせれば、False Positive はほとんど生成されなくなります。
3. **シグニチャベースではなく振る舞いベース**：同一の悪質なアクティビティを試みる攻撃を阻止します。
4. **ゼロ アップデート**：シスコのデフォルトのセキュリティ ポリシーを使用すれば、単調な HIDS シグニチャのアップデート作業が不要になります。
5. **重層的防御によるネットワーク セキュリティ**：ネットワーク上のシグニチャと、エンドポイント上の振る舞いベース保護の組み合わせは、絶えず進化し続ける企業の安全保護に最適です。重層的防御では、最適なセキュリティを実現するために、さまざまなテクノロジーが各層で提供されます。

Cisco Security Agent は、攻撃を検出するだけでなく、攻撃を阻止します。IT 部門は、少ない労力で多くの成果を得ようと努力しており、攻撃の自動防御はもはや任意のオプションではなく、必須条件となっています。シスコのテクノロジーは、悪意のあるすべてのアクティビティを阻止するように設計されています。Cisco Security Agent は、過剰な負担を抱えた管理者に対して、「現在、攻撃が行われている可能性があります」といったアラートや、「ホストに被害が生じていないことを確認してください」といったアラートを提示するのではなく、実際の攻撃を警告し、検出し、阻止します。

Cisco Security Agent は、攻撃ライフ サイクルの全段階で攻撃に対処します。すべての段階で情報を分析して相互に関連付けることで、真に悪意があるものと、表面上疑わしいが実際は正当なトラフィックとを区別します。また、データパケットが暗号化されている場合でも、攻撃を検出できます（Secure Sockets Layer (SSL) で暗号化されている場合も検出可能）。これにより、False Positive アラートの数が大幅に減少します（通常、1/40 以下になります）。



大半の HIDS は、誤ったアラームに苦慮しています。ある HIDS ベンダーは、1つの管理コンソールにレポートを送信するセンサーの数を 20 から 30 未満にすることを推奨しています。その理由は、コンソールがその数のセンサーにしか対処できないからではなく、人間のオペレータがアラートを処理しきれないからです。システムはそれほど多くの攻撃にさらされているのでしょうか。決してそのようなことはなく、シグニチャによる対応がそのような結果をもたらすのです。センサーでトラフィックを阻止するように設定できたとしても、膨大な数の False Positive アラートが生成されます。

Cisco Security Agent はシグニチャに依存しておらず、シグニチャ自体が存在しません。エンドポイントセキュリティは、ポリシールールによって実装されます。ポリシールールは、管理コンソールで定義され、セキュリティが必要とされる重要なサーバおよびデスクトップに常駐するインテリジェントなエージェントに配布されます。ポリシールールは、振る舞いを中心として定義されます。攻撃ライフサイクルの図 (図 2) が示すように、悪意のある振る舞いはそれほど多くありません。オペレーティングシステムの上書きを禁止するルールを 1 つだけ定義すれば、オペレーティングシステムの上書きを必要とする新種または既知の攻撃を数多く阻止できます。

また、セキュリティが振る舞いとポリシーに基づいているため、シグニチャのアップデートをエージェントに配信する必要がありません。このゼロアップデートアーキテクチャにより、製品のライフタイム全体での大幅なコスト削減が実現します。HIDS によって保護された重要なサーバ上のシグニチャをアップデートするには、ベンダーからシグニチャを入手する必要があります。次に、シグニチャをラボでテストし、ホスト上で振る舞いしているアプリケーションが停止しないことを確認する必要があります。さらに、シグニチャをサーバに展開する必要があります。また、テスト時に発見されなかった弊害が生じた場合は、削除する必要があります。管理者は、アップデートの入手、検証、展開といったこれらの作業のために多くの時間を費やす必要があります。アップデートの数が増えるほど、そのコストは高くなります。アップデートを頻繁に行わなければ、このコストを低く抑えることもできますが、長期間にわたってホストが危険にさらされます。

Cisco Security Agent

Cisco Security Agent のようなポリシーベースのシステムを使用すれば、ポリシーの設定方法に応じて、エンドポイントセキュリティに関する複数の問題を解決できます。Cisco Security Agent は、エンドポイントセキュリティに関する次の領域に対処します。

- サーバおよびデスクトップの堅牢化 (ファイルシステムおよびオペレーティングシステムのロックダウンおよび整合性のベースラインなど)
- バッファオーバーフローおよびネットワーク攻撃からの保護
- Web サーバの保護
- デスクトップ用の分散型ファイアウォール
- 悪意のあるコードのサンドボックス (Java、JavaScript、ActiveX、または他のモバイルコードによる攻撃を阻止)

エージェントの統合により、お客様は高い投資利益を得ることができます。



Cisco Security Agent のアーキテクチャ

Cisco Security Agent は、カーネルに隣接しているため、アプリケーションの振る舞いを監視することができます。Cisco Security Agent Intercept Correlate Rules Engine (INCORE) テクノロジーを使用することで、ファイル、ネットワーク、および設定リソースに対するすべてのシステムコールを代行受信できます。ただし、コールの代行受信よりも重要なことは、その後にセキュリティ エージェントで実行される関連付けの機能です。関連付けを行い、アプリケーションの振る舞いを理解することによって、未知の方法によるシステムへの侵入を確実に阻止することが可能になります。

アプリケーションは、システム リソースにアクセスする必要がある場合、カーネルに対してオペレーティングシステム コールを発行します。INCORE は、これらのオペレーティングシステム コールを代行受信し、マネージャで一元的に定義された（マネージャのポーリング時にエージェントへダウンロードされる）キャッシュ ポリシーと、これらのコールとを比較します。INCORE は、そのオペレーティングシステム コールと、同じアプリケーションまたはプロセスによって作成された他のコールとを関連付けることにより、これらのイベントを関連付けて、悪意のあるアクティビティを検出します。ポリシーに違反していない要求は、カーネルに渡されて実行されます。ポリシーに違反している要求は阻止されて（カーネルに渡されず）、エラーメッセージがアプリケーションに戻され、アラートが生成されてエージェントからマネージャに送信されます。

たとえば、Web サーバで HTML Web ページが配信されているとします。その Web サーバは、着信方向の Web 要求を受信すると、ファイルシステム I/O 要求およびネットワーク パケット I/O 要求を生成します。これらがポリシーに違反していない場合（たとえば、Web サーバアプリケーションによる Web ページへの読み取りアクセスなど）、セキュリティ イベントは生成されません。既知の攻撃（たとえば、SSL 暗号化によって隠匿された Unicode ディレクトリ トラバーサル攻撃）によって、このポリシーに違反したアプリケーション振る舞い（たとえば、CMD.EXE などのコマンド シェルを開く振る舞い）が試みられた場合、その要求はポリシーに違反するため、阻止されます。リモートユーザに対しては、「404: Not Found」のようなエラー メッセージが生成されます。

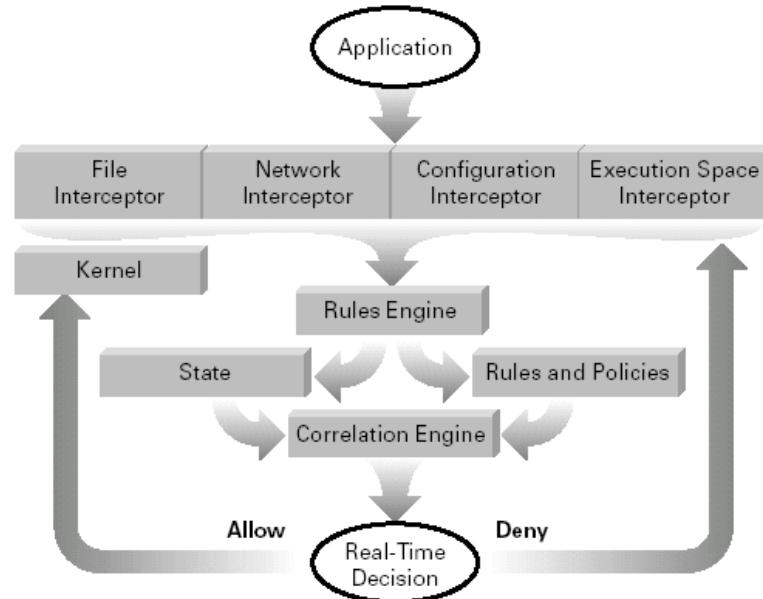
攻撃者が、バッファ オーバーフロー攻撃に似た新種の攻撃を試行したとします。繰り返しになりますが、このような攻撃は SSL 暗号化や他の回避手法を利用して隠匿されている場合があります。実行スペース代行受信機能は、固有の、または別のアプリケーションの実行スペースや実行環境を侵害しているアプリケーションを検出します。このケースでは、データスペースから実行されるコードが検出され、実行が阻止されます。この振る舞いはポリシーに違反しているため、新種の攻撃を阻止するためのアップデートは必要ありません。これが、「ゼロアップデート」という名前の由来です。

INCORE (図 3) は、4 つの代行受信機能をサポートしています。

- ファイル システム（すべてのファイル読み取りまたは書き込み要求を代行受信します）
- ネットワーク（ドライバ (NDIS) またはトランスポート (TDI) レベルでのパケット イベント)
- 設定 (Windows のレジストリまたは Unix の rc ファイルに対する読み取りまたは書き込み要求)
- 実行スペース



図 3
Cisco INCORE アーキテクチャ



実行スペース代行受信機能は、ファイルやネットワークのような特定のリソースを直接参照せず、各アプリケーションの動的なランタイム環境の整合性を維持します。この代行受信機能によって、要求を発行したアプリケーションが所有していないメモリ領域への書き込み要求が検出されると、その要求は阻止されます。同様に、1つのアプリケーションが別のプロセスにコードを挿入（たとえば、Dynamic Link Library (DLL; ダイナミックリンクライブラリ) のような共有ライブラリの挿入) する試みも検出されて阻止されます。たとえば、Windows NT への getadmin 攻撃では、DLL の挿入技術を使用してユーザーの特権レベルが拡張されます。Cisco Security Agent はこの攻撃も阻止します。さらに、この代行受信機能は、バッファオーバーフロー攻撃も検出して、被害を防ぎます。これにより、ファイルシステムや設定などの動的なリソースの整合性だけでなく、メモリやネットワーク I/O などのきわめて動的なリソースの整合性も保護されます。

Cisco Security Agent は、ファイル、ネットワーク、設定、およびランタイムの操作を代行受信してポリシーと比較するので、各アプリケーションの状態を追跡できます。アプリケーションの振る舞いは、ファイル、設定、およびネットワーク操作の組み合わせやシーケンスによって構成されています。アプリケーションが操作を試みると、Cisco Security Agent はその操作をポリシーと照合してチェックするだけでなく、アプリケーションの状態と、その操作に関するポリシーを関連付けます。これにより、エージェントは、一連の振る舞いとの関係において許可または拒否の決定をリアルタイムで下すことができるので、関連付けを行わない従来型の振る舞い阻止スキームよりも False Positive の数が大幅に減少します。

Cisco Security Agent のポリシーは、IT によって各サーバおよびデスクトップに割り当てられるルールの集合です。これらの（ユーザや ID を基準としない）アプリケーション中心のアクセス制御ルールにより、必要なリソースへの安全なアクセスが実現します。シスコから提供されているポリシーをそのまま実装することもでき、それらのポリシーをカスタムポリシー作成用のモデルとして使用することもできます。



Cisco Security Agent は、サーバ用の重要な侵入保護機能と、分散型ファイアウォール機能を迅速に提供します。これらのソリューションを利用すれば、各種の脆弱性を保護できるだけでなく、Microsoft SQL Server、Microsoft Office、インスタント メッセンジャ、IIS Web サーバなどの一般的なアプリケーション向けのポリシーを簡単に展開することができます。重要なサーバおよびデスクトップを保護するこれらのポリシーは、最低限の設定だけで迅速に展開できます。

Cisco Security Agent と複数のセキュリティ テクノロジー

Cisco Security Agent は、独自の INCORE アーキテクチャを採用しているため、侵入検知および防御エージェント、ファイルの整合性を監視するエージェント、およびアプリケーション サンドボックスとして機能します。また、(マネージャで定義されたポリシーをベースとする) 代行受信機能と組み合わせて使用すれば、必要なネットワークセキュリティアプリケーションを作成することも可能になります。一元的に定義されるポリシールールをベースとした代行受信機能を組み合わせることができるので、新たなエンドポイントセキュリティ機能 (表 1) を迅速に実装することができます。

表 1

必要なセキュリティ機能	ネットワーク代行受信機能	ファイル システム代行受信機能	実行スペース代行受信機能	設定代行受信機能
分散型ファイアウォール	X			
侵入検知	X	X		X
アプリケーション サンドボックス		X	X	X
ネットワーク ワームの防御	X	X		X
システムの堅牢化		X	X	

Cisco Security Agent に付属するデフォルトのポリシーでは、これらのネットワーク セキュリティ アプリケーション (分散型ファイアウォール、IDS、アプリケーション サンドボックスなど) のすべてが実装されるため、お客様は独自のポリシーを作成する必要がありません。GUI を使用して簡単にポリシーを作成したり変更することもできますが、デフォルトのポリシーを使用すれば、これらすべての保護機能が同時に提供されます。

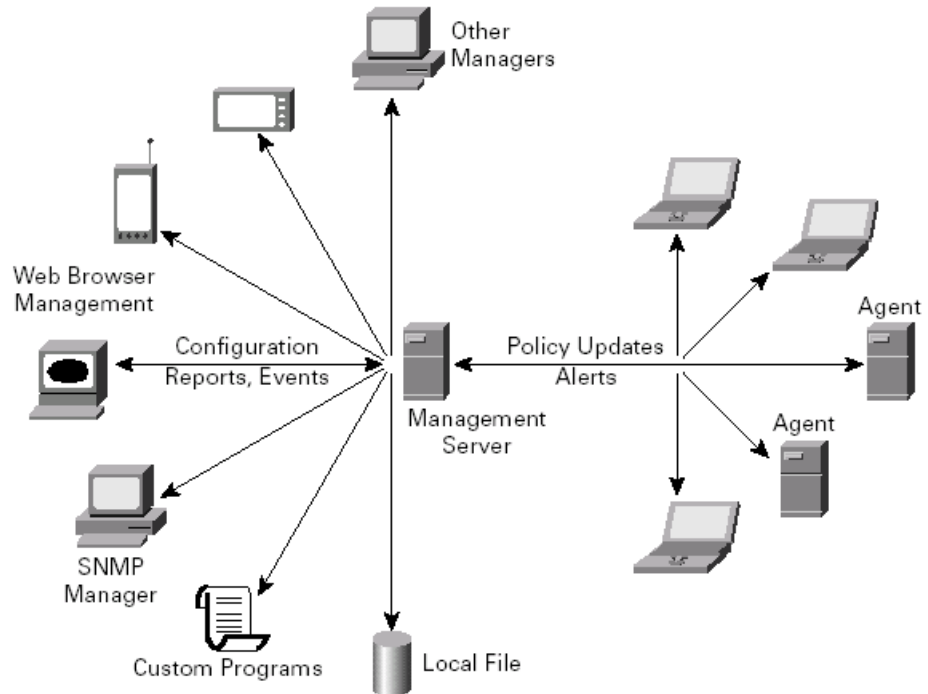
INCORE により、さまざまな代行受信機能が提供されるため、Cisco Security Agent は、さまざまなセキュリティ機能を提供できます。INCORE の代行受信機能を組み合わせれば、従来型のセキュリティ機能を効果的に作成できます。たとえば、ネットワーク代行受信機能では、アドレスとポートのブロッキングを処理する、従来の分散型ファイアウォール製品の機能が提供されます。オペレーティングシステムの堅牢化または整合性の強制では、重要なファイルまたはレジストリ キーへの変更が検出されるため、これら 2 つの代行受信機能を使用すれば、システム堅牢化機能が提供されます。



Cisco Security Agent 管理のアーキテクチャ

Management Center for Cisco Security Agents (VMS 2.2 以降に統合) は、エージェントマネージャ (サーバ) アーキテクチャ (図 4) を採用しています。このアーキテクチャでは、マネージャ上で作成または変更されたポリシーが、すべてのエージェントへ自動的に配布されます。このマネージャでは、管理 GUI への安全な Web インターフェイスが採用されているので、安全が確保されていないリモートアクセス方法を使用せずに、社内のどこからでも管理を行えます。エージェントは、ポリシーの変更または新しいソフトウェアアップデートを確認するために、定期的にマネージャをポーリングし、マネージャにリアルタイムでアラートを送信します。エージェント / マネージャ間のすべての通信は安全であり、標準ベースのプロトコル (セキュア Web、SSL、HTTP over SSL (HTTPS)、TCP ポート 443) が使用されます。

図 4
Cisco Security Agent 管理のアーキテクチャ



バックエンドのアラート システムには柔軟性があります。エージェントによって生成されるイベントは、電子メール、ダイヤルアップ ポケットベル、または SNMP トラップを使用して送信できます。また、ローカル ファイルへの書き込み、Cisco VMS SecMon へのアップロード、カスタムプログラムの起動も可能です。シスコの一部のお客様は、Unicenter や OpenView などの SNMP ベース ネットワーク管理システムと、Cisco Security Agent の統合に成功しています。また、Management Center for Cisco Security Agents は、netForensics などのサードパーティ管理コンソールと統合することができます。



Cisco Security Agent による関連付け

イベントは、エージェントのローカルで関連付けられるだけでなく、マネージャによってグローバルに関連付けられます。これにより、シグニチャベースの HIDS よりも大幅に精度が向上します。

ローカルでの関連付けにより、大半の HIDS が直面している **False Positive** の問題が大幅に緩和されます。さまざまな振る舞いが分析されるため、悪意のあるアクティビティを高い精度で特定できます。これを示す 1 つの例は、ネットワークワームの増殖です。ワームによって実行される各アクティビティを個々に分析した場合、ファイルがダウンロードされ、そのファイルが実行され、そのプロセスによって Outlook のアドレスブックが開かれ、電子メールが送信されるといった振る舞いが実行されているにすぎないので、何も問題がないように見えます。これらの各プロセスは、1 日に何度も繰り返される通常の振る舞いです。しかし、これらを一連の流れで見ると、悪意のある破壊的な振る舞いであることが判明します。これらのイベントを関連付けることで、エージェントは、1 日に多数のアラームを発することなく、ワームのアクティビティを阻止できます。イベントの関連付けを行わない HIDS では、「アプリケーション A がアドレス帳を開きました」といったアラートや、「プログラムがダウンロードされ、実行されました」といったアラートが生成される場合があり、攻撃と通常のイベントを区別するには、これらすべてのアラートを人間のオペレータが分析する必要があります。

トロイの木馬の検出も関連付けに関する例の 1 つです。この場合は、キーボードのフッキングや IRC による通信などのアクティビティが、広範なコンテキストにおいて分析され、誤ったアラートを過剰に生成することなく悪意のあるアクティビティが検出されます。同様に、振る舞いに基づきアプリケーションを分類するエージェントの機能も、アプリケーションを制御する重要な機能の 1 つです。たとえば、何らかのプログラムが電子メールクライアントと同様の機能を実行する場合（たとえば、POP、IMAP、または SMTP による発信接続を使用する場合）、Cisco Security Agent は、そのプログラムを電子メールクライアントと見なします。したがって、電子メールクライアントによる送信 HTTP 接続を禁止するルールを作成すれば、企業のポリシーによって「Web バグ」や「通信傍受」の電子メールセッションが禁止されるため、実行可能ファイルの名前（OUTLOOK.EXE）をリスト内にハードコードする必要がなくなります。

同様に、グローバルの関連付けでは、多数のエージェントから受信したイベントが関連付けられます。企業全体でイベントを監視することにより、これまで見逃されていた可能性のある攻撃も検出されます。これは、**False Negative** 状況と呼ばれ、**False Positive** よりもはるかに悪い状況といえます。従来、少数の（場合によっては、1 つの）パケットだけを企業内の各ホストに送信する攻撃者は、検出を巧妙に逃れながら、ネットワーク全体のマップを作成することが可能でした。グローバルな関連付けを使用すれば、これらの分散型スキャンが、エージェントマネージャによって自動的に検出されます。電子メールを介して増殖しようとする共通のプログラムが複数のエージェントによって検出されると、エージェントマネージャはそのプログラムをグローバルの検疫リストに追加します。エージェントは、アップデートされたリストをポーリング時に受け取ります。まだ攻撃を開始していないワームの実行可能ファイルも、検疫に移動されます。



Cisco Security Agent の投資利益

Cisco Security Agent は、真に予防的なアプローチを採用している点で、他のエンドポイントセキュリティソリューションとは大きく異なります。未知の攻撃を阻止することは、日常的に行われる既知の攻撃を阻止することよりもはるかに困難ですが、最も大きな被害を与え、復旧に最も労力を要するのは、未知の攻撃です。

複数の製品（たとえば、分散型ファイアウォールと改ざん防止製品）を使用してシステムを保護しようと考えている組織は、Cisco Security Agent が非常に経済的で（2つではなく1つの製品で済む）、展開が容易であり（2つではなく1つのエージェントで済む）、運用が簡単で（スタッフトレーニングの対象製品が1つだけであり、1つのコンソールだけを監視すれば済む）あることに気付くでしょう。

Cisco Security Agent は、サーバとデスクトップを保護するので、両方を保護する場合は、運用上の経済性も大幅に向上します。また、Cisco Security Agent は、Windows だけでなく UNIX システムも保護するので、さらに大幅な運用コストの削減が実現します。UNIX と Windows のサーバおよびデスクトップを他の製品（分散型ファイアウォール、HIDS、悪意のあるコードのサンドボックス、監査統合ツールなど）で保護するには、何種類もの製品が必要でしたが、Cisco Security Agent を使用すれば1つで済みます。

さらに、テストおよび展開が必要なシグニチャが存在しません。頻繁にアップデートされる HIDS では、常に管理者が新たなアップデートをテスト ラボで展開し、本稼動サーバとの互換性を確認する必要があります。この作業に必要な多大な人件費が、Cisco Security Agent では不要になります。ゼロ アップデート アーキテクチャにより、HIDS シグニチャのアップデート、テスト、およびロールバックに関する管理上の負担はなくなります。

アプリケーション中心の侵入防御は、今日の発展的なネットワークおよび企業環境の保護に関する新たなカテゴリまたは思想的アプローチを形成します。従来型の IDS テクノロジーは、ネットワークやユーザの正当なアクティビティを妨げる場合があるため、パフォーマンスに影響を与えるだけでなく、管理上の負担やフラストレーションを過度に生んできました。侵入防御のコンテキストにおいて振る舞いを強制する戦略では、攻撃の進化に対応した総合的な手法が採用されています。その結果が、アプリケーションの振る舞いに基づいてネットワーク攻撃やファイル攻撃による被害を阻止する、予防的防御ソリューションです。

©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