



Check Point®

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

ワームの脅威に打ち勝つ

プロアクティブなセキュリティによるワームの阻止



Intelligent Security

チェック・ポイントはネットワークのあらゆる環境——境界、内部、Web——に対する確実なセキュリティ保護と、情報リソースの安全性、接続性、管理性を兼ね備えたソリューションを提供します。

Contents

本書の内容

はじめに:セキュリティに求められる性質の変化	3
IT管理者が対処を求められるセキュリティの脅威の急増	4
リアクティブ(事後対処型)なセキュリティ技術の限界	4
ネットワーク境界の拡大がもたらす新しい課題	5
問題を打破する新たなアプローチ:プロアクティブなセキュリティとエンドポイント・セキュリティ	6
ポートの脆弱性	7
アプリケーションのスプーフとハイジャック	7
電子メールによる感染	8
複合型脅威	8
ネットワーク内部からの感染拡大	9
セキュリティ・アプリケーションに対する攻撃	10
エンドポイントPCにセキュリティ・ポリシーを適用するIntegrity危機管理からポリシー管理へ	11

はじめに：セキュリティに求められる性質の変化

2004年、IT管理者はBagle、MyDoom、Netskyなどの悪名高い数々のワームやウイルスに加えて、日々出現する無数の新しい亜種による執拗な攻撃に直面しました。これら無数のワームやウイルスの猛攻に対して、ネットワークが攻撃を受けてから対策を施すという従来の受け身の対策では、まったく役に立たないことが明らかになりました。以前は、ハッカーがセキュリティ・ホールを悪用する手段を見つけ出すまで数か月を要していたため、IT管理者はソフトウェア企業・ベンダーが公開する修正ファイルパッチを確実に適用することで、ハッカーの攻撃からネットワークを保護できていました。また、危険性が高いウイルスやワームの出現頻度が数週間から数か月単位だった頃は、ウイルス対策ソフトウェアを頻繁に更新し、定期的にシステムのスキャンを実行することで、セキュリティの脅威に充分に対処できていました。

しかし現在では、セキュリティ・ホールが発見されてから、ほんの数日でそれを悪用するコードが出現するため、発見された脅威に対して事後に対処するという従来のリアクティブ（事後対処型）なセキュリティ対策はまったく無意味となりました。2004年には、有名な大企業や空港のみならず、国防関連機関のネットワークまでもが、感染したワームの急速な拡散により、1週間近くもダウンするというニュースがたびたび報じられました。こうしたネットワークのダウンにより、企業は巨額の損失を被り、政府機関は重要な業務を遂行できなくなりました。ここで重要となるのは、これらの企業や政府機関は、ほぼすべてのPC（ネットワーク・エンドポイント）にウイルス対策ソフトウェアを導入していたにもかかわらず、ネットワークがダウンしてしまったという事実です。

ウイルス対策ソフトウェアに代表されるリアクティブな技術が企業のセキュリティに果たす役割の重要性は、現在も変わっていません。しかし今日の脅威に対処するには、攻撃手法を事前に予測し、攻撃が実際に仕掛けられる前に阻止するプロアクティブ（事前防御型）な技術セキュリティ対策も導入する必要があります。ウイルスやワームの出現頻度が従来と比較にならないくらい高まり、それらを作成するハッカーの動機も変化した現在、プロアクティブなセキュリティ戦略は不可欠です。以前は、ハッカーがウイルスやワームを作成する動機は、自分が作成したコードをインターネット上にできるだけ広めて、ハッカーのコミュニティで名を挙げることでした。こうした動機で作成されたウイルスやワームの大半は、インターネット上に拡散する過程でトラフィックを占有してネットワークをダウンさせる程度で、PCやサーバからデータを窃取したり、それらの動作を停止させるなどの破壊活動を行うものはまれでした。

しかし過去2年の間に、ウイルスやワームは犯罪を犯すためのツールへと変貌しました。例えばBadtransやOrpheusなどのワームは、パスワードなどの重要な個人情報や企業情報を窃取するためのキー・ロガーを内蔵していました。一方、MyDoomは感染したシステムにバックドアを設置するなど、ハッカーによる不正アクセスを補助する機能を備えていました。バックドアからシステムに不正アクセスしたハッカーは、迷惑メールの送信、サービス不能（DoS）攻撃、猥褻なコンテンツの発信など、さまざまな攻撃の踏み台としてそのシステムを悪用しました。

IT管理者にとって、社内のすべてのPCに適切なパッチを確実に適用し、ウイルスやワームに感染したPCを復旧するだけでも、悪夢のように複雑かつ煩雑な作業です。しかし今日、IT管理者はこの悪夢のような作業に加えて、社内のPCをハッカーによる不正アクセスから確実に防御することで、PCからデータが窃取されたり、PCが乗っ取られて（ハイジャックされて）犯罪行為に悪用された場合の法的責任から企業を守る必要もあります。しかし、IT管理者は日々出現する新しい脅威に対応するだけで精一杯で、使用しているソフトウェアが必要とする修正ファイルパッチを検証したり、ネットワークのアーキテクチャや設定を見直してセキュリティを強化するなど、長期的な計画立案に時間を割くのが難しい状況になっています。加えて、IT管理に充てられる人的リソースの慢性的な不足が状況の悪化に拍車をかけており、日々出現する脅威に対処しなければならないIT管理者の負担は倍増しています。IT管理者の多くが、長時間労働や休日出勤を強いられているにもかかわらず、すべての脅威に対処できていないのが実情です。

IT管理者が対処を求められるセキュリティの脅威の急増

IT管理者が対処しなければならないセキュリティの脅威がいかに急増しているかを端的に表す事例を、幾つか紹介します。

- 電子メールのセキュリティ・サービスを提供するMessageLabs社によると、史上第2位の感染数を記録したワームSobig.Fが同社のセキュリティ機能によってブロックされた回数は、このワームの存在が確認された2003年8月から2004年6月までの間で、3千3百万回以上にも達していることが判明しました。これ自体、驚異的な数字ではありますが、史上最悪のワームとして知られるMyDoom.Aの感染数には遠く及びません。MessageLabs社によってMyDoom.Aがブロックされた回数は、同ワームが出現した2004年の1月から6月までの間で、5千4百万回以上に達しました。
- MessageLabs社が2003年12月から2004年1月までの1か月間にワームやウイルスをブロックした回数は、2千5百万回に達しました。以前は、1か月当たりの回数が5百万回前後だったので、単純計算で5倍以上に増えたことになります。さらに2004年2月には、この回数が1か月当たり50万件とさらに倍増しました。
- 2004年の2月15日から3月31日までほぼ毎日、既存ワームの新しい亜種が出現しました。
- 現在、ワームは出現頻度が急上昇しているだけでなく、脆弱性が発見されてから、その脆弱性を悪用するワームが出現するまでの期間も大幅に短縮されています。例えば、ワームSlammerが出現したのは脆弱性が発見されてから101日後でしたが、ワームSasserが出現したのは脆弱性が発見されてからわずか19日後でした。

リアクティブ(事後対処型)なセキュリティ技術の限界

ウイルス対策ソフトウェア、ソフトウェア修正ファイル、不正アクセス防止システムなど、従来のリアクティブなセキュリティ技術は、急速に進化し続ける攻撃手法に追い付くことが事実上不可能になりました。

ウイルス対策ソフトウェアの多くは、効率的な更新メカニズムを備えています。新しい定義ファイルが公開されるまでタイムラグが生じるため、最新のウイルスやワームに対して常に後手に回っています。この事実は、ドイツの調査会社AV-Test社 (www.av-test.org) がVirus Bulletin 2004 Conferenceで発表した調査結果によっても裏付けられています。

AV-Test社によるこの調査では、ウイルス対策の市場をリードする5社を含む、24社の世界的なベンダーの参加の下、悪名高いBagle、MyDoom、Netsky、Sasserを始めとする、2004年に発生した45件のアウトブレイク(ワームの大規模な感染拡散)について、対応する定義ファイルの公開に要した時間が追跡調査されました。この調査により、同じ脅威であっても、ウイルス・ベンダーによって対応に要する時間に大きな差があることが判明しました。Bagle.Aの場合、あるベンダーは出現から1.5時間で定義ファイルを公開していた一方、別のベンダーは定義ファイルの公開に20時間強を要していました。さらに、すべての脅威に対し一貫して短時間で対応できたベンダーは、ただの一社もなかったことも判明しました。これは、ある脅威に対して迅速に対応できたベンダーであっても、別の脅威に対しては対応に長い時間を要していたということです。

リアクティブなセキュリティ技術の欠点は、こうした機能更新までのタイムラグだけに留まりません。例えば、ウイルス対策ソフトウェアのベンダーがどれだけ迅速に定義ファイルを公開したとしても、エンドポイントPCの定義ファイルの更新が遅れば、それらのエンドポイントから社内ネットワーク全体にウイルスやワームが蔓延してしまう可能性があります。例えば、ある社員が週末にラップトップPCノートPCを自宅に持ち帰り、インターネットの閲覧中に新種のワームに感染したとします。そのラップトップPCノートPCにインストールされているウイルス対策ソフトウェアのベンダーが、週明けまでに新しい定義ファイルを公開していたとしても、その社員が定義ファイルを更新していなければ、月曜日に出社してラップトップPCノートPCを社内ネットワークに接続した途端、脆弱性があるすべての社内PCにワームが拡散する結果となります。通常、ワームの感染スピードは非常に速いため、ウイルス対策ソフトウェアの自動更新機能が定義ファイルを更新する前に、ワームは拡散してしまいます。

前述のAV-Test社による調査では、ベンダー各社のウイルス対策ソフトウェアが提供するヒューリスティック・スキャン機能(特定のアルゴリズムに従って、まだ定義ファイルが公開されていない未知のウイルスやワームを検出する機能)の性能もテストされましたが、惨憺たる結果に終わりました。ヒューリスティック・スキャン機能によって新種のウイルスを検出できた製品はたったの1つで、それ以外の製品はいずれも、対応する定義ファイルがなければ未知のウイルスやワームを検出できないばかりでなく、既知のウイルスやワームの亜種すら検出できませんでした。

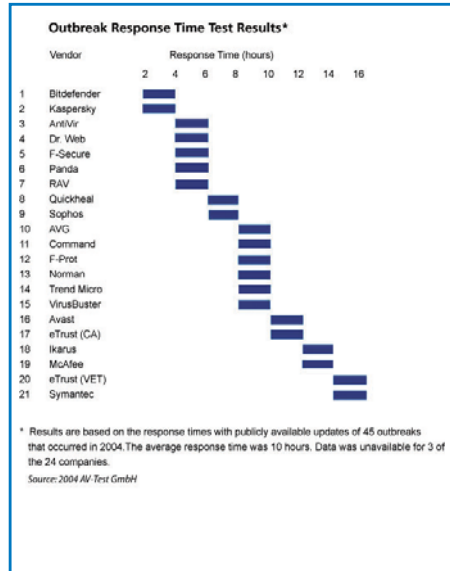
脅威に対処するまでのタイムラグが問題となるのは、ウイルス対策ソフトウェアだけではありません。この問題は、オペレーティング・システムやアプリケーションにも当てはまります。Microsoft社は、過去に脆弱性が発見されてから修正ファイルを公開するまで9か月も要した例があります。

さらに、このタイムラグは別の避けがたい要因によって引き延ばされる場合があります。ある脆弱性に対処する修正ファイルが公開されたとしても、その修正ファイル自体が別の問題を引き起こす可能性があるため、IT管理者は修正ファイルを事前に検証する必要に迫られます。ベンダーはできるだけ迅速に修正ファイルを提供するために、十分なテストを実施しないまま修正ファイルを公開してしまう恐れがあります。Microsoft社は、オペレーティング・システムの開発時には数か月から数年に及ぶ品質管理工程を設けますが、修正ファイルの作成とテストには数日しか割かない場合があります。こうした理由から、企業は修正ファイルの安全性を独自に検証する必要があります。大企業では、修正ファイルを検証してから全社のPCに導入を完了するまで、さらに数週間を要するケースが少なくありません。

ネットワーク境界の拡大がもたらす新しい課題

これまでに述べたさまざまな要因により、IT管理者は社内ネットワークの脆弱性を無防備なまま放置せざるを得ないのが現状です。境界を保護するファイアウォールは、既知のワームが悪用するポートを塞ぐことはできます。しかし、IT管理者はすべてのポートを塞ぐわけにはいかず、あまつさえ続々と登場する新しい通信プログラムによって、解放する必要があるポートの数は増える一方です。例えば、ポート80番を使用するWebアプリケーションは、生産性を向上させるために不可欠のツールですが、攻撃者にとっては鍵のかかっていないドアも同然の存在です。Webサイトは重要な情報源であると同時に、ワーム、バックドア、トロイの木馬など、悪質なプログラムの感染源でもあります。社員が業務に使用するピアツーピア・アプリケーションやインスタント・メッセージャーは、ワームにとって格好の感染経路となります。

企業ネットワークを脅かすのは、増え続ける侵入経路だけではありません。モバイル・アクセスやリモート・アクセスの普及により拡大するネットワーク境界もまた、企業ネットワークを脅かしています。営業先や出張先など、ファイアウォールや電子メール・スキャナなど企業の境界セキュリティの外部でPCを使用する社員が増えるにつれ、それらの社員が外出先でウイルスやワームに感染し、そのPCを社内に持ち帰ってネットワークに接続して、内部から感染を拡大させる危険性が増加します。来客にワイヤレス・アクセスを提供している場合は、これもウイルスやワームの感染経路になりえます。



問題を打破する新たなアプローチ：

プロアクティブなセキュリティとエンドポイント・セキュリティ

このように、リアクティブ（事後対処型）なセキュリティ技術を使用したアプローチだけでは、企業ネットワークを今日の脅威から守ることは到底不可能です。日々進化する多種多様な脅威に対して、リアクティブなアプローチだけで対処しようとするのは、実弾を込めた銃でロシア人ルーレットに挑戦するのと同じくらい無謀な行為です。運が良ければ、新種のウイルスやワームが社内ネットワークに蔓延する前に、全社員のエンドポイントPCに修正ファイルパッチを適用して定義ファイルを更新できるかもしれません。しかし運が悪ければ、IT管理者にできることは被害を最小限に留めるべく奔走するだけとなり、企業は甚大な損害を被ることになります。

危険かつ非効率であるリアクティブな技術と比較して、プロアクティブ（事前防御型）な技術は別次元の安全性と効率性を実現します。次に出現するウイルスやワームの形態や攻撃手法を正確に予測するのが不可能である点に変わりはありませんが、ウイルスやワームが攻撃に悪用する脆弱性を識別して、事前に保護しておくことは十分に可能です。

例えば、電子メールの添付ファイル経由で感染するワームの新種が出現した場合、そのワームの詳細が分からなくても、社内のネットワークやPCへの配信を許可する添付ファイルの種類をあらかじめコントロールしておけば、そのワームの感染や拡散を未然にブロックできます。また、特定のポートを経由して感染するワームの新種が出現したとしても、既知の信頼できるアプリケーションが使用するポートだけを開放するようにしておけば、そのワームの感染や拡散を未然にブロックできるのです。さらに、社内ネットワークの外部から内部に流入するトラフィックをスクリーニングし、悪質なコードやスクリプトを自動的に削除することで、エンドポイントPCのオペレーティング・システムやアプリケーションを狙ったバッファ・オーバーフローなどの攻撃を未然に阻止できます。

こうしたセキュリティ・ポリシーを、社内ネットワークに接続された各エンドポイントPCだけでなく、社外に持ち出されるラップトップPCノートPCにも適用しておけば、社内ネットワーク境界の外部にまでプロアクティブなセキュリティ戦略が拡大され、外部から持ち帰ったPCからの感染を未然に防止できます。また、万が一いずれかのエンドポイントPCがウイルスやワームに感染した場合でも、適切に配置された内部セキュリティ・ゲートウェイと、各エンドポイントPCにインストールされた保護機能が、感染の拡大を最小限に抑えます。

チェック・ポイントのIntegrity™ は、ウイルスやワーム、およびエンドポイントPCを標的にした各種の攻撃に対するプロアクティブなセキュリティを、企業のネットワーク全体に提供します。Integrityは、各方面で絶賛されたチェック・ポイントのステートフル・インスペクション型ファイアウォール機能と、強力な中央集中管理機能を備えています。IT管理者はIntegrityを導入することで、セキュリティ・ポリシーを定義して各エンドポイントPCに適用し、企業のセキュリティ要件を満たしていないPCの社内ネットワークへの接続を禁止できます。

またIntegrityは、史上初の内部セキュリティ・ゲートウェイ製品であるチェック・ポイントInterSpect™ とシームレスに統合し、完全な内部セキュリティを構築できるようにデザインされています。InterSpectは、企業ネットワークを複数の組織的なセキュリティ・ゾーンに分割して管理します。InterSpectとIntegrityを統合することで、最新のワームやウイルスの拡散をセキュリティ・ゾーン内に封じ込めつつ、感染したエンドポイントPCを隔離し、感染の拡大をブロックした状態でウイルスやワームを駆除できます。さらに、社内ネットワークに接続しようとするすべてのエンドポイントPCを事前にスキャンし、企業のセキュリティ要件を満たしているPCにのみアクセスを許可できます。

プロアクティブな内部セキュリティとエンドポイント・セキュリティが、さまざまな脅威に対してどのように機能するのか、幾つかの例を挙げて紹介します。以下の例は、いずれもウイルスやワームによって最も頻繁に悪用される攻撃手法と、それに対するプロアクティブな防御を紹介しています。

ポートの脆弱性

インターネット上で最初に蔓延したワームは、1988年のMorrisです。このワームは、解放されたポートで受信待機している脆弱なアプリケーションに向けて不正なコマンドを送信することで感染を広げました。この攻撃手法は数多くのワームによって「有効性」が実証されており、いまだに悪用される場合があります。例えば、2003年8月に猛威を振るったワームBlasterは、ポート135番経由でネットワーク内部に侵入し、Windowsのリモート・プロシージャ・コール (RPC) の脆弱性を悪用して、感染したシステム上で悪質なコードを実行しました。電子メールの添付ファイルとして拡散するワームと異なり、ポートの脆弱性を悪用するワームは拡散する過程でエンド・ユーザの介入を必要としません。Microsoft社は、Blasterが出現する1か月前にRPCの脆弱性に関する情報と修正ファイルを公開していましたが、Blasterが出現した時点で修正ファイルを適用していたユーザは、全Windowsユーザの半数にも満たない状態でした。Blasterのアウトブレイクが発生して間もなく、インターネット関連ニュース・サイトのCNETは以下のような記事を掲載しました。

「ワームMSBlastの強力な感染力は、脆弱性が発見されてから修正ファイルを適用するという現在のセキュリティ対策が抱える問題点を浮き彫りにした。こうした従来の対策では、全PCに修正ファイルを適用するまでネットワークを正常に使用できない状態が続くと同時に、作業に長時間を要するため、重大な脆弱性への対処が遅れてしまう。例えば米国のフロリダ大学では、MSBlastに感染した1台のPCがダイヤルアップで大学のネットワークに接続したがために、数百台ものPCに感染が拡大する結果となった。」

上記の事例の場合、もしもダイヤルアップ接続したPCにIntegrityがインストールされていれば、たとえオペレーティング・システムの修正ファイルがインストールされていなかったり、ウイルス定義ファイルが更新されていなかったりしたとしても、そのPCは自動的に保護され、あまつさえ感染を拡大させるような事態は未然に防止することができていました。Integrityは、信頼されていないネットワークからの接続試行をデフォルトで自動的にブロックすると同時に、解放されたポートがある場合は、特定の承認されたアプリケーション以外によるそのポートの使用を禁止します。また、Integrityで識別できない実行可能コードを含む外向きの通信をブロックするように設定することもできます。Integrityは、ポートの使用可否をアプリケーション単位で制御できない従来のファイアウォールでは実現できない、ハイレベルな保護機能を提供します。解放されたポートの使用可否をアプリケーション単位で制御する機能は、業務に使用するアプリケーションが使用するポートと、特定のワームが悪用するポートが同じ場合に、非常に重要となります。またWindowsでは、デフォルトで実行されているサービスの中に、ほとんど使用されないものが多く含まれており、それらがワームによって悪用される場合があります。Integrityは、そうしたサービスへのアクセスを自動的にブロックする機能も備えています。

さらに上記の事例で、もしもフロリダ大学のネットワークにInterSpectが導入されていれば、被害の拡大をより効果的に防止できていました。InterSpectは、通常予期される使用方法やプロトコル標準に合致しない、不審なネットワーク・トラフィックをブロックします。また、各社が提供するソリューションが、軒並み安全性と利便性のトレードオフを強要するのに対し、InterSpectはネットワークの安全性を確保しつつ、アプリケーションの正常な利用を妨げません。例えば、有名なワームBlasterはWindowsの重要なプロトコルであるRPC (リモート・プロシージャ・コール) を悪用しますが、InterSpectは悪質なRPCトラフィックだけを検出してブロックし、危険性がないRPCトラフィックはそのまま通過させます。InterSpectのゲートウェイはネットワークを通過するトラフィックを常時監視するため、他社製のソリューションが検出できないような、高速で移動し拡散するワームも漏らさず検出してブロックできます。

アプリケーションのスプーフとハイジャック

Integrityのアプリケーション制御機能を使用すると、ユーザが意図的にインストールした安全でないアプリケーション (ファイル交換ソフトウェアなど) と、ユーザの許可なくPCに潜入した危険なプログラム (トロイの木馬やスパイウェアなど) によるネットワークへのアクセスを、識別してブロックすることができます。Integrityは、アプリケーションが信頼できるかどうかを判断する際に、アプリケーションの名前だけでなく、有効性が実証されているMD5ハッシュ関数のフィンガー・プリントを利用します。これにより、たとえワームやトロイの木馬が信頼できるアプリケーションをスプーフまたはハイジャックした場合でも、危険な通信を確実に検出してブロックできます。さらに、この機能を応用して、特定のアプリケーションの特定のバージョンにのみネットワークへのアクセスを許可することもできます。例えば、信頼されているアプリケーションであっても、既知の脆弱性がある古いバージョンや、安全性が検証されていない新しいバージョンのネットワークへのアクセスを禁止する、といった使い方が可能です。

高機能なワームの中には、信頼されているアプリケーションのプロセス内に自らを「挿入（インジェクション）」することで、従来のファイアウォールによる検出を回避するものが存在しますが、Integrityはこうしたワームからもシステムを保護します。例えば有名なワームBagleは、WindowsのOpenProcessというAPIを悪用します。OpenProcessは、あるアプリケーションが別のアプリケーションを制御できるようにするためのAPIですが、Bagleはこの機能を悪用してWindowsエクスプローラをハイジャックします。WindowsエクスプローラをハイジャックしたBagleがポートを開放しようとした場合、他社製ファイアウォールの多くは、それをWindowsエクスプローラの通常の動作と区別できません。しかしIntegrityはOpenProcess APIの動作を監視し、Bagleによるアプリケーションのハイジャック自体を未然に阻止します。

電子メールによる感染

ウイルスの最大の感染源は、いまだに電子メールです。ウイルスを添付した電子メールは、感染を拡大させる最も効果的な手段として、現在も頻繁に悪用されています。見知らぬ差出人から届いた電子メールを開いたり添付ファイルをクリックしてはいけないと、どれだけ警告し続けても、不用意な操作によって電子メールからウイルスに感染するユーザは後を絶ちません。原因の一つは、電子メールの詐称技術（不審でないメールに偽装する技術）が巧妙化した点にあります。例えばBagle、MyDoom、Netskyなどのワームは、感染したシステムから収集した電子メール・アドレスを使用してメッセージを送信します。また、以前はウイルスを添付した電子メールの多くが、件名や本文が明らかに怪しい内容だったり、内容が支離滅裂だったりして、比較的簡単に見分けることができましたが、近年はユーザに不信感を抱かせないような洗練された内容に進化しています。例えばMyDoom.AやNetsky.Pは、差出人を電子メール・サーバに偽装し、本文に「エラーが発生したので、添付ファイルを参照して詳細を確認せよ」と記載した電子メールをユーザに送信します。一方、Netsky.Aは、差出人をインターネットのオークション・サイトに偽装し、やはり添付ファイルを開くように誘導するような本文を記載した電子メールを送信します。

前述したIntegrityのアプリケーション制御機能を使用すれば、ウイルスの実行可能ファイルが添付された電子メールの、ネットワーク上での拡散を防止できます。また、従業員が自分でインストールした個人用の電子メール・ソフトウェアでPOPサーバやIMAPサーバからダウンロードする添付ファイルは、企業の電子メール・セキュリティ上の盲点となる場合がありますが、Integrityを導入すれば、事前定義された危険な拡張子（45種類以上）を持つ添付ファイルをブロックできます。なお、受信メールに適用するセキュリティ・ポリシーは、Integrityの他の機能と同様に、グループ単位またはユーザ単位で柔軟にカスタマイズ可能です。

Integrityは大量メール送信型ワームの拡散もブロックします。PCにインストールされている電子メール・ソフトウェアが、同一内容の電子メールを、事前定義した数を超える宛先に対して送信しようとした場合は、IntegrityのMailSafe機能によってブロックされます。また、独自のSMTPエンジンを内蔵するワームが電子メールを送信しようとした場合は、Integrityのアプリケーション制御機能によってブロックされます。

複合型脅威

企業ネットワークのセキュリティに対する脅威は、攻撃に要する時間が短縮されているだけでなく、手段が非常に巧妙化しています。近年、単一の脆弱性だけを攻撃する脅威よりも、複数の攻撃手法を組み合わせる「複合型脅威」と呼ばれる脅威が増加しています。初期の複合型脅威で有名なのは、2001年に猛威を振るったNimdaです。Nimdaは、ファイルやWebページに感染し、自身を添付した電子メールを大量に送信し、ローカル・ネットワークのファイル共有を悪用し、さらにファイル・サーバをスプーフすることで、急速に感染を拡大しました。

複合型脅威は、ウイルス対策ソフトウェアにとって大きな脅威となっています。通常、これらのソフトウェアは、定義ファイルの公開に時間を要するだけでなく、多くの場合、感染源となったワームまたはウイルスの本体しか駆除できず、複合型脅威が各所に仕掛けた攻撃手段を見落としてしまいます。ワームやウイルスの本体が駆除されても、それらが仕掛けたキー・ロガーが削除されなかったり、バックドア設置を目的として改竄されたDLLやレジストリ値が修復されなければ、さらなる攻撃の足がかりとして悪用される恐れがあります。例えばワームDoomjuiceは、システムに侵入する手段として、MyDoomが仕掛けたバックドアを悪用します。

ウイルス対策ソフトウェアにとってさらに大きな脅威となるのが、新たに登場した「スパイウェア」と呼ばれるプログラムです。スパイウェアは、インターネットからダウンロードしたファイルや、インターネットCookieなどに紛れてシステムに侵入します。スパイウェアの多くは、宣伝目的やマーケティング目的で、侵入したシステムからさまざまな情報を収集し、ユーザーに無断でスパイウェアの作成者に送信します。その過程で、企業ネットワークのトラフィックが占有されたり、システムのパフォーマンスが低下するなどの弊害が起こり、結果としてそれに対処するIT管理者の作業負荷が増大します。ウイルス対策ソフトウェアによっては、ある程度のスパイウェア検出機能を備えたものもありますが、オペレーティング・システム内に巧妙に紛れ込むスパイウェアが増加する中、それらを完璧に検出して駆除するのは困難なのが現状です。

Integrityのステートフル・インスペクション・ファイアウォール機能とアプリケーション制御機能は、ワームをブロックするのと同様の方法で、複合型脅威やスパイウェアを効果的にブロックします。Integrityは、エンドポイントが送受信するトラフィックを監視し、許可されていないトラフィックを完全にブロックします。そのため、キー・ロガー、トロイの木馬、スパイウェアなどは、システムから収集した情報をインターネットに送信することができません。また、万が一システムにバックドアが設置された場合も、Integrityによってネットワーク外部からバックドアへのアクセスがブロックされます。さらに、Integrityは外部からのアクセス要求が妥当かどうかを、全アプリケーション・レイヤ、各種ネットワーク設定、セキュリティ・ポリシー、通信状態、およびアプリケーション状態から総合的に判断します。

ネットワーク内部からの感染拡大

有名なワームBlasterとSasserがあれほどの猛威を振るったのは、これらがローカルのファイルおよびプリンタ共有に必要なポートを悪用して企業ネットワーク全体に拡散したのが原因です。このとき、もしもその企業がIntegrityとInterSpectを導入していれば、ワームが拡散する際のトラフィックをサブネット内やセキュリティ・ゾーン内に封じ込めて、ネットワーク全体への感染拡大を防ぐことができました。例えばIntegrityを使用すると、ファイルおよびプリンタ共有を、ネットワーク上の限定された「信頼済み」ゾーン内だけで有効にして、ファイルおよびプリンタ共有のポートから、そのゾーン以外のネットワーク・リソースにアクセスできないように設定できます。ネットワークを複数のセキュリティ・ゾーンに分割するアプローチにより、境界の突破を目的とするすべての攻撃手段を効果的にブロックし、企業ネットワーク全体にワームが蔓延して日常業務が停止するような最悪の事態を未然に防ぐことができます。

数千台ものエンドポイントPCが接続されている大規模な企業ネットワークの場合は、インフラストラクチャの要所にInterSpectを配置して、ネットワークを複数のセキュリティ・ゾーンに分割すると効果的です。InterSpectは、セキュリティ・ゾーン間で交わされるトラフィックを監視して、業務に必要なトラフィックは通過させ、許可されていないトラフィックはブロックします。これらのセキュリティ・ゾーンは、物理的なネットワーク構造で分割できるのはもちろん、仮想的なネットワーク構造で分割することも可能なので、企業ネットワークを実際の部門構成に合わせて柔軟に分割し、部門ごとに最適なセキュリティ・ポリシーを運用できます。セキュリティ・ゾーンは、地理的または物理的な制約に左右される必要はありません。IT管理者は、部門構成や従業員のニーズに合わせて柔軟にゾーンを定義したり、定義済みのゾーンを簡単に変更することができます。

IntegrityやInterSpectのセキュリティ・ゾーンは、船舶の浸水防水隔壁に相当します。通常、大型の船舶は浸水を特定の箇所だけに封じ込めるための隔壁を備えています。隔壁に不備があれば、浸水が船全体に及び、その船は沈没します。企業ネットワークを、既存のサブネット単位でセキュリティ・ゾーンに分割したり、部門単位やプロジェクト・チーム単位でセキュリティ・ゾーンに分割すれば、いずれかのセキュリティ・ゾーンがワームやウイルスに感染しても、それらの脅威はゾーン内に自動的に隔離され、企業ネットワーク全体への拡散が防止されます。また、この隔離機能を応用して、脆弱性や攻撃にさらされているネットワークからサーバを隔離しておき、修正ファイルの適用やワームの駆除が完了したら隔離を解除する、という使い方もできます。

セキュリティ・アプリケーションに対する攻撃

LoveGate.Vなどのように、セキュリティ・アプリケーションそのものを攻撃対象にするワームが数多く存在します。これらのワームは、セキュリティ・アプリケーションを強制的に終了させ、システムを無防備な状態に陥れようとします。こうした攻撃への対処が施されていない場合、アプリケーションは実に簡単に終了させられてしまいます。セキュリティ・アプリケーションの中には、Windowsタスク・マネージャから簡単に終了できるものが存在します。

しかし、Integrityは簡単には強制終了できません。たとえハッカーやワームがシステムの管理者権限を奪取したとしても、Integrityを終了させることはできません。Integrityは攻撃への耐性を高めるために、本体がドライバ、サービス、クライアントなどの複数レベルに分散されています。他社製セキュリティ・アプリケーションの多くは、サービスとクライアントを組み合わせてセキュリティ機能を提供しているため、攻撃に弱いクライアントを強制終了させるだけで、サービスも終了させることができます。一方、Integrityのサービスはクライアントと無関係に稼働し、ドライバはサービスと無関係に稼働します。

Integrityは上記のように自身を保護すると同時に、他のセキュリティ・アプリケーションが正しく実行されているかどうかを監視します。特にウイルス対策ソフトウェアについては、IT管理者が指定した製品が正しくインストールされて稼働しているか、また定義ファイルが最新の状態に更新されているかどうかを厳密に監視されます。最新の状態に更新されたウイルス対策ソフトウェアが実行されていないエンドポイントPCは、Integrityによって企業ネットワークへの接続を禁止されます。

エンドポイントPCにセキュリティ・ポリシーを適用するIntegrity

「蟻の一穴」という諺が表すように、最高レベルのセキュリティで保護された企業ネットワークであっても、ワームに感染した1台のエンドポイントPCによって壊滅的な打撃を被る可能性があります。Integrityは、エンドポイントPCにセキュリティ・ポリシーを適用することで、蟻の一穴を確実に塞ぎます。Integrityは、企業ネットワークの最前線に立って攻撃からシステムを守ると同時に、すべてのエンドポイントPCにセキュリティ・ポリシーを迅速かつ柔軟に適用するためのツールとしても機能します。IT管理者はIntegrityを使用して、企業ネットワークに接続するすべてのエンドポイントPCを監視し、所定のセキュリティ要件を満たしていないPCのネットワークへの接続を禁止できます。エンドポイントPCには、以下のようなセキュリティ要件を適用できます。

- ・ Integrityクライアントの最新バージョンがインストールされ、最新のポリシーで稼働しているかどうか。
- ・ 指定されたウイルス対策ソフトウェアがインストールされ、最新の定義ファイルで稼働しているかどうか。
- ・ 指定された修正ファイルやサービス・パックがインストールされているかどうか。
- ・ 指定されたレジストリ設定が存在するかどうか。
- ・ 指定されたプロセスやアプリケーションが稼働しているかどうか。
禁止されたプロセスやアプリケーションが稼働またはインストールされていないかどうか。

チェック・ポイントのセキュリティ製品が提供する保護機能は、TAP (Total Access Protection) と呼ばれます。Total Access Protection (すべてのアクセスを保護) はその名のとおり、ゲスト・アクセス、リモート・アクセス、社内アクセス、ワイヤレス・アクセスなどの種類を問わず、企業ネットワークにアクセスするすべてのPCに、セキュリティ・ポリシーを適用する機能です。さらに、Cooperative Enforcement™技術で数百台ものネットワーク・ゲートウェイ製品と統合可能になったIntegrityは、セキュリティ要件を満たさないPCを隔離してネットワークへのアクセスを禁止し、ユーザが自力でセキュリティ要件を満たせるように、最大限の支援を提供します。

IntegrityはIEEE 802.1x規格を満たしているため、Cisco、Nortel、Avantail、Enterasys、Foundryを始めとする各ベンダーの、スイッチ、ルーター、ワイヤレス・アクセス・ポイントなど、200種類以上のネットワーク・デバイスと統合可能です。Integrityを使用すれば、IntegrityクライアントがインストールされていないPCに対してもセキュリティ・ポリシーを適用できます。その場合、例えば従業員がWebインターフェイスから企業ネットワークに初めてアクセスした際に、Integrity Clientless Securityをダウンロードするように促されます。Integrity Clientless Securityは、Integrityと同等のセキュリティ・チェック機能を提供するActiveXアプレットです。Integrity Clientless Securityは、従業員のPCにワーム、スパイウェア、キー・ロガーなどが潜入していないかどうかをスキャンし、それらが検出された場合は無効にしたうえで、企業ネットワークへのアクセスを許可します。

このように強力かつ厳格なセキュリティ・ポリシーの適用機能を備えたIntegrityですが、その最大の目的は、強固なセキュリティとユーザの利便性の両立にあります。Integrityは、ユーザを遠ざけるための製品ではありません。セキュリティ要件を満たしていないユーザに、必要なファイルや設定を提供したり、それらを提供するサーバに誘導することによって、ユーザが簡単に自力で要件を満たせるように支援し、セキュリティ・ポリシーの徹底を促進するのが、Integrityの役割です。なぜなら、セキュリティの強化によって従業員の生産性が犠牲になるようなことは、決してあってはならないからです。

ユーザの支援は、Integrityの重要な機能の一つです。ユーザが企業ネットワークにアクセスしようとする、そのユーザのPCが所定のセキュリティ要件を満たしているかどうか自動的にスキャンされます。満たされていない要件が一つでもある場合、ユーザはネットワークへのアクセスを一時的に禁止され、必要な情報やファイルなどを提供するサーバにリダイレクトされます。ユーザが簡単な画面の指示に従ってセキュリティ要件を満たすと、Integrityとネットワーク・ゲートウェイによってユーザに再びアクセス権が与えられます。

危機管理からポリシー管理へ

短期的に見ると、ワームやウイルスの出現頻度には波があります。しかし長期的に見れば、それらの脅威は常に高いレベルへと上昇を続けています。限られた人的リソースですでに限界に達している現在のIT部門が、従来のリアクティブなセキュリティ技術を使い続けていけば、近い将来セキュリティ対策が破綻することは火を見るよりも明らかです。

ソフトウェア修正ファイルパッチやウイルス対策ソフトウェアに代表されるリアクティブな技術が企業のセキュリティに果たす役割の重要性は、今後も変わらないでしょう。しかし、それだけでネットワークのセキュリティを確保できる時代は終わりました。これは、リモート・アクセスやワイヤレス・アクセスの普及によって保護しなければならない境界が拡大し続ける、従来のファイアウォールにも当てはまりません。

チェック・ポイントのInterSpectとIntegrityに代表されるプロアクティブなセキュリティ技術は、上記の問題に対処するために開発されました。両者の機能を組み合わせることで、最新のワームやウイルスをネットワークとエンドポイントの両方でブロックしつつ、セキュリティ要件を満たしたエンドポイントにのみネットワークへのアクセスを許可することで、企業ネットワーク全体にセキュリティ・ポリシーを確実に提供できます。InterSpectとIntegrityを組み合わせた二重の防御は、日々巧妙化するワームやウイルスから確実にネットワークを保護し、ビジネスの継続性を保障します。チェック・ポイントのソリューションは、ネットワークの脆弱性自体を保護することで、それを悪用するすべての攻撃手段を無効化し、ワームやウイルスの新しい亜種からネットワークを事前に保護します。また、すべてのネットワーク・ノードが保護されるため、事実上すべての侵入経路が保護されます。

Check Point Software Technologiesについて

チェック・ポイント・ソフトウェア・テクノロジーズ (www.checkpoint.com) はインターネット・セキュリティにおける世界トップ企業として、特に企業向けファイアウォール、パーソナル・ファイアウォール、およびVPNの市場においてマーケット・リーダーとして広く認められています。

チェック・ポイントはNext Generation製品ラインナップを通じ、インテリジェント性を兼ね備えた境界、内部、およびWeb環境に対するセキュリティ・ソリューションを提供し、エンタープライズ・ネットワークをはじめ、アプリケーション、エンドポイント、支店・支社環境、更にはパートナー各社のエクストラネットなどに対する包括的なセキュリティ保護を実現します。

チェック・ポイントの一部門である Zone Labs (www.zonelabs.com) は、インターネット・セキュリティの分野で高い信頼性を誇るブランドとして数々の賞に輝くエンドポイント・セキュリティ・ソリューションを提供し、世界中で何百万台ものコンピュータをハッカーやスパイウェア、データの盗難などから守っています。

またチェック・ポイントは、350社を超える各分野のトップベンダーが提供する最高のソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security) により、自社ソリューションの能力をさらに拡大します。現在チェック・ポイントは世界88ヶ国、2200社を超えるパートナー・ネットワークを通じてソリューションの販売、導入、サービス提供を行っています。

©2004-2005 Check Point Software Technologies Ltd. All rights reserved.
Check Point, Application Intelligence, Check Point Express, Check Pointのロゴ、AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, Zone Labs のロゴは、Check Point Software Technologies Ltd.およびその関連会社の商標、サービス・マーク又は登録商標です。その他の企業、製品名は各企業が所有する商標または登録商標です。本書に記載された製品は米国の特許 No.5,606,668、5,835,726および6,496,935により保護されています。その他の 米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Winning Against Worms : Combating Worms with Proactive Security

P/N:501692-J 2005.6

※記載された製品仕様は予告無く変更される場合があります。



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成ビル6F
<http://www.checkpoint.co.jp/> E-mail: info_jp@checkpoint.com Tel: 03(5367)2500