

セキュリティアプライアンス：ゲートウェイでの攻撃防止

ウイルス、複合型攻撃と悪質なトラフィックを企業インターネットゲートウェイで阻止するための確実なアプローチ



セキュリティアプライアンス：ゲートウェイでの攻撃防止

ウイルス、複合型攻撃と悪質なトラフィックを企業インターネットゲートウェイで阻止するための確実なアプローチ

1. 攻撃ターゲット:企業ネットワークゲートウェイ

「企業が直面するウイルスの問題は、悪化の一途をたどっている。企業のウイルス被害は年々増加しており、これに伴うコストが増大していることは明白である。調査結果によると、企業がコンピュータウイルスやワームの被害にあう可能性は1999年まで毎年倍加しており、その後2年間では毎年約15パーセントずつ増えている。その結果、企業による努力と対策コストの増加にもかかわらず、ウイルス(悪性コード)のリスクは高まり続けている。」

ICSA Labs 7th Annual Computer Virus Prevalence Survey 2001

多くの業界関係者が最大の信頼を寄せているICSAの調査結果は、コンピュータセキュリティの専門家たちを落胆させるものとなりました。さらに、この調査のデータのほとんどは、2001年9月にNimdaウイルスが世界の企業コンピューティングインフラストラクチャを攻撃する前に収集されたものです。この事実は、コンピュータセキュリティの専門家をさらに悩ませる結果となっています。

セキュリティの新たな脅威:複合型攻撃

Nimdaは、Code Red、Goner、KlezやBugBearと同様に、最新型のコンピュータウイルスである複合型ウイルスに分類されます。複合型ウイルスは、電子メールで感染する従来のウイルスと、最新のネットワーク感染機能を組み合わせたものです。また、企業ネットワーク全体のセキュリティ脆弱点をすばやく探し出し、サービス拒否攻撃、ワーム実行によるサーバのクラッシュや、トロイの木馬EXEファイルの実行による脆弱点攻撃などの、破壊的な被害をもたらします。

例えばNimdaには、以下のような多数の感染方法があります。

- ・ ウェブページに感染し、自動ダウンロードによって感染したページを表示し、脆弱点を持つデスクトップ上でREADME.EMLファイルを実行します。
- ・ EXEファイルに付着する方法でファイル感染を起こし、CドライブとDドライブを共有設定に変更します。システムブート時に自動的に感染したファイル自身を起動するように設定します。
- ・ CodeRed C/DやSadmindなどが残したバックドアを利用し、多数のUnicode攻撃によって感染を広げます。

複合型ウイルスは急激に蔓延します。Nimda発生後わずか8時間で全世界のコンピュータネットワークが感染し、総額30億ドルもの被害を被りました。2001年のICSA Labの調査では、回答者の20パーセントが、複合型攻撃の被害にあったことがあると答えています。しかし、この調査は2001年9月のNimdaウイルスの発生以前のもので、実際の数字はさらに大きくなると思われます。この電子メールによる複合型攻撃が、現在最も危険で一般的なセキュリティの脅威であることは間違いなく、SMTP・POP3メールに影響を与え、さらにはHTTP・FTPトラフィックにも影響を与えています。その破壊力による経済的影響は甚大で、Computer Economicsの予測によれば、Code Redによる全世界の経済的被害は26億2,000万ドルにのぼり、Sircamは11億5,000万ドル、Nimdaは6億3,500万ドルの被害をもたらしています(注1)。

今日のウイルスや複合型攻撃と戦うためには、単一のソリューションでは不十分です。2001年のICSAの調査結果にも、「平均的なコンピュータユーザは、100パーセントの効果を発揮する特殊なソリューションを求めている。実際は、『相乗効果』のあるプログラムによる保護戦略をデスクトップとゲートウェイで導入するほうがはるかに容易でコスト効果が高く、道理にかなっている」とあります。デスクトップでの強力なウイルス対策に加えて、インターネットゲートウェイがセキュリティの要点として注目を集めています。インターネットゲートウェイでは、セキュリティソリューションを使ってネットワークを通過するコンテンツを監視することにより、複合型攻撃の被害を低減させることができます。さらに、時間を浪費するスパムメールをブロックするとともに、ユーザによる不適当なウェブサイトの閲覧を防ぐことも可能です。

注1: Computer Security Instituteが実施した2002年CSI/FBI調査の結果。

McAfee WebShield Appliance: 複合型攻撃を確実に防止

ゲートウェイセキュリティソリューションのリーダー企業であるネットワークアソシエイツは、全世界の5億800万ドルのサーバ/ゲートウェイ用ウイルス対策ソフトウェア市場で24パーセントのシェアを獲得しています(注2)。企業ゲートウェイに導入するMcAfee WebShield Applianceは、ウイルス対策およびコンテンツ管理ソフトウェアを高性能なハードウェアと組み合わせたソリューションです。WebShield Applianceは、インターネットと電子メールで感染するウイルスの検出機能に加えて、以下の機能を備えています。

- ・ ネットワークを通過しようとする不適切なコンテンツの検出
- ・ ウイルス対策アプリケーションを最新の状態に保持
- ・ 企業リソースを濫用してウェブサイトを見たりスパムメールを読むユーザの検出
- ・ 仕事と無関係なトラフィックによるネットワーク帯域幅消費量の検出

デスクトップ上のセキュリティを再構成してHTTPやFTPのスキャンを可能にするには、多大な時間と労力が必要です。WebShieldは、企業インターネットゲートウェイでウイルス対策を実行することにより、容易でコスト削減効果の高いソリューションを提供します。高いスケーラビリティを備えたWebShieldソリューションは、デバイス1台で1時間に最大16万件の電子メール、または1秒間に2MBのHTTPトラフィックをスキャンすることができます。さらに、必要に応じて複数のWebShield Applianceで負荷を共有し、さらに高度なスケーラビリティとパフォーマンスを実現することも可能です。

WebShieldは、McAfee ePolicy Orchestratorとの統合により、ゲートウェイでのウイルスアクティビティの詳細なグラフィカルレポートを提供します。包括的なレポートをもとに、コンテンツフィルタリングルールで設定されたポイントやアクセス禁止URLへのアクセスを調べることができます。さらに、完全なウイルス傾向分析とレポート機能を利用して、ウイルス感染を総合的に把握することもできます。

II. WebShield Appliance: ゲートウェイセキュリティのための確実なアプローチ

McAfee WebShield Applianceは、インターネット電子メールとウェブトラフィックに含まれるウイルスと悪性コードをスキャンするために設計された、一体型のゲートウェイスキャンソリューションです。WebShield Applianceは、以下の機能を備えています。

- ・ アンチスパム・アンチリレー機能
- ・ ルールベースのコンテンツフィルタリング機能
- ・ グラフィカルなレポートの作成と傾向分析
- ・ ウェブサイトのブロック
- ・ ウイルス定義ファイルとスキャンエンジンの自動アップデート
- ・ SNMPを含む柔軟なアラート機能

WebShieldの設計思想: ゲートウェイスキャン専用に設計

WebShieldは、デスクトップ、サーバや電子メールアプリケーションに展開する従来のウイルス対策製品に代わって、企業のセキュリティ戦略の中心的役割を果たします。また、ターゲットに到達して被害をもたらす前にウイルスと悪性コードを阻止する、非常に効果的な機能を備えています。WebShield Applianceは、特定プロトコルのトラフィック(SMTP、FTP、HTTPおよびPOP3)をスキャンして感染を検出し、ウイルスが企業ネットワークに侵入する前に駆除します。さらに、コンテンツフィルタリング機能により、管理者が「不適切」と定義したコンテンツの送受信を防止します。

WebShield Applianceは、ハードウェア、オペレーティングシステムおよびアプリケーションが統合された一体型ソリューションで、全てのコンポーネントがあらかじめインストールされています。この製品には、以下のコンポーネントが含まれています。

- ・ 最適化されたIntelベースのサーバ
- ・ 高速で安全性とアベイラビリティの高い、最適化されたネットワークオペレーティングシステム(Linux)
- ・ 以上のコンポーネントに合わせて最適化されたアプリケーション

注2: 2001年の市場シェアは'Antivirus Software 2002: A Segmentation of the Market' (Brian Burke他、2002年IDC発行)によるもの。

WebShield Applianceの特長

WebShieldは、企業ゲートウェイでウイルスと複合型攻撃を防止する、高性能でコスト効果の高いソリューションです。業界標準のハードウェアとオペレーティングプラットフォームにMcAfeeの実績あるウイルス対策・フィルタリングソフトウェアを搭載したWebShield Applianceには、以下をはじめとする多数の特長があります。

- ・ TCOの削減: WebShieldは統合型ソリューションであるため、単一の契約で全てのメンテナンスをカバーすることができます。ハードウェア、オペレーティングシステムとスキャンアプリケーションのそれぞれに個別のメンテナンス契約は必要ありません。
- ・ 容易な導入: WebShield Applianceの全てのコンポーネントはあらかじめ統合されているため、購入後すぐに導入することができます。ソフトウェアおよびハードウェアのライセンスとサポートも、単一ベンダーがまとめて提供します。
- ・ 高度なパフォーマンスとセキュリティ: WebShieldの堅牢なオペレーティングシステムが、高度なパフォーマンスとセキュリティを提供します。WebShield ApplianceにはLinuxオペレーティングシステムの主要コンポーネントとユーティリティのみが組み込まれているため、デバイスのセキュリティホールを産み出しにくいように設計されています。さらに、チューニング済のオペレーティングシステムが高度なスループットを実現し、WebShieldデバイス1台で1時間に最大16万件の電子メール、または1秒間に2MBのHTTPトラフィックをスキャンすることができます。
- ・ 継続的なオペレーション: 重大な障害が発生した場合でも、それぞれのWebShield Applianceに同梱されているリカバリCDを利用して、アプリケーションを再構築することができます。リカバリCDを使って既存ディスクをフォーマットし、アプライアンスを出荷時設定に戻すことができます。また、メッセージログ、設定ファイルや処理延期・隔離メッセージなどの重要データを保存しながら、アプライアンスを再インストールすることもできます。さらに、ソフトウェアのアップグレードと紛失したパスワードの回復も可能です。
- ・ グローバルなソリューション: WebShieldは、ドイツ語、フランス語、スペイン語、日本語、韓国語、繁体中国語と簡体中国語で完全にローカライズされているため、これらの言語を使った管理が可能です。

高速導入と容易で安全なメンテナンスを考慮した設計

従来のソフトウェア製品をインストールする場合、ハードウェアとオペレーティングシステムが特定のタスクに合わせて最適化されているとは限りません。一方、WebShieldは、電子メールとトラフィックのスキャンのために特別に設計されています。一体型ソリューションの特長である高いパフォーマンスと信頼性に加え、ハードウェアとオペレーティングシステムを一体化するアプローチにより、トラブルシューティングと管理作業の負担が軽減されます。

WebShieldの設定とメンテナンスには、ウェブベースのユーザインターフェースを利用します。クライアントのインストールは必要なく、ブラウザがインストールされた、TCP/IP通信が可能な全てのクライアントPCを使った管理が可能です。クライアントPCとアプライアンスの間には、SSL (Secure Socket Layer) を使った暗号化トンネルが作成されます。管理者は、安全な接続の確立後に認証を行い、ウェブベースのインターフェースを使ってアプライアンスを管理することができます。

Linuxのパワーを活用

WebShield Applianceは、(Red Hat) Linuxオペレーティングシステム上で動作し、2.4 Linuxカーネルによりパフォーマンス、安定性とスケーラビリティが最適化されています。WebShieldは、Linuxコンソールへの直接接続を必要としない、「ブラックボックス」ソリューションです。

McAfeeは、オペレーティングシステムの安全化を図るため、アプライアンスの操作に必要なLinuxの機能とユーティリティのみを組み込み、Bastille Linuxユーティリティを使って安全性を強化しています。

III. 企業を全面的に保護

不安定な経済状況のもとでIT予算が削減されている現在、予防的なセキュリティ戦略が非常に重要になっています。大企業が複合型攻撃などの被害を受けた場合、復旧には莫大なコストがかかります。2001年のICSA調査によれば、ウイルス感染後の復旧には以下のコストが必要です。

「一般的な回答では、復旧作業には4人日が必要という事だった。平均では、推察される直接費用は概ね5,500ドル(一般値)から6万9,000ドル(平均値)である。前年の調査から詳細分析を検討した結果、ウイルス対策担当者は復旧コストを少なく見積もる傾向がある。平均的な企業でのウイルス感染の副次的影響(ソフトウェアとハードウェアを含む)による年間コスト合計は、5万ドルから50万ドルと予測されている(注3)。」

WebShield Applianceは、複合型攻撃、電子メール攻撃とダウンロードしたファイルを使った攻撃から企業を保護するための、非常に効果的でコスト効果の高い手段を提供します。

HTTPスキャンが複合型攻撃を企業ゲートウェイで阻止

WebShieldの主な複合型攻撃防止策として、HTTPトラフィックのスキャンが挙げられます。現在、HTTPトラフィックがセキュリティの脅威となるケースが急増しています。以下は、2001年ICSA調査結果からの抜粋です。

「FD等の媒体を介してデスクトップから発生する感染被害の伸びは鈍っていると見られるが、インターネットから侵入するウイルス感染とその被害の発生率は、現在の年間発生率の15パーセントを大幅に上回る見込みである。インターネット経由でのウイルス感染の増加に伴い、保護と復旧のコストも増大する。新型ウイルスの登場、接続方法の多様化、VPNおよびパートナーシップ接続の拡大、一般ユーザによる電子メールの利用方法の多様化と、新たな複製方法の普及が、我々が予測する悪性コードの問題発生率増加を助長するものと思われる(注4)。」

WebShieldは、1秒間に2MBのHTTPトラフィックをスキャンし(注5)、ウェブページのダウンロードと同時にウイルスを検出します。WebShieldは、ファイルのダウンロード実行中にポップアップステータス画面を表示し、ダウンロードが完了したファイルのパーセンテージまたはバイト数をユーザに通知するか(アプライアンスによる確定が可能な場合)、ダウンロード実行中であることを知らせます。ダウンロードが即時に開始されない場合、「再実行」ボタンを連続クリックするユーザが多いものですが、ダウンロード実行中の表示によってこの操作を防ぐことができます。その結果、ヘルプデスクへの問い合わせも少なくなります。

ウイルスが検出されると、WebShieldが感染したページへのアクセスをブロックして、企業ネットワークにおける問題発生を防止します。感染が発生した場合は、管理者はゲートウェイの定義ファイルを最新版にアップデートすることで、ネットワーク全体を保護し、感染源を遮断して、電子メールサーバとデスクトップの感染を防止することができます。さらに、WebShieldがウイルス感染を未然に防ぐ事で、複数サーバに対するウイルス駆除作業の必要性をなくし、ヘルプデスクにエンドユーザからの問い合わせが殺到することを防ぎます。

大企業では、大量のHTTPトラフィックに対応するために、複数のWebShield Applianceが必要になる場合もあります。キャパシティを追加する場合は、複数のWebShield Appliance間で負荷を自動的に分散させることができます。

注3: ICSA Labs 7th Annual Computer Virus Prevalence Survey 2001 より

注4: 同調査結果の内容を強調したもの

注5: 1秒間の最大スキャン速度は、WebShield e1000モデルで2MB、WebShield e500で1MB、e250の場合は毎秒250KB。

企業のSMTP電子メールリソースの保護

ウイルス感染源のトップは、依然として電子メールです。1台のWebShield Applianceで、1時間に最大16万件のSMTPメールをスキャンすることができます。このデバイスは、受信メールと送信メールを即時にスキャンして、ウイルスを検出します。ウイルスに感染した全ての電子メールは、自動的に隔離、修復または削除することができます。

WebShieldは、コンテンツフィルタリング機能を利用して、送受信時に、それぞれのSMTP電子メールの件名とメッセージ本体のほか、添付ファイルの名前、種類とサイズをスキャンします。さらに、テキスト形式の添付ファイルのコンテンツをスキャンすることもできます。これらの機能を利用して、実行可能ファイルやVisual Basicスクリプトをブロックすることができます。つまり、このタイプのファイルやスクリプトのように、ウイルスが含まれる可能性が高いものの、一般のユーザの場合には電子メールで送受信する必要性はほとんどないと思われるものを効果的にブロックします。さらに、新型のマスメール型電子メールウイルスや、時間を浪費するデマ電子メールもブロックします。

WebShieldは、ネットワークコストの削減という付加的な利益も提供します。また、受信電子メールのサイズを制限(メッセージの上限バイト数を設定)することにより、ネットワーク帯域幅の有効利用を可能にします。

POP3電子メールの攻撃とスパムメールを防止

多くの企業ユーザは、個人(POP3)電子メールアカウントの確認に企業リソースを利用しています。POP3トラフィックは、デスクトップからインターネットに直接送信されます。そのため、企業のSMTPサーバにインストールされたウイルス対策製品は、一般的に受信・送信POP3メッセージをスキャンしません。WebShieldをインターネットゲートウェイに導入することにより、POP3トラフィックを確実にスキャンし、企業内外でのウイルス感染の拡大を防ぐことができます。

さらにWebShieldは、3段階のアプローチによってスパムメールを防止し、ネットワークトラフィックとネットワークストレージに対する処理を低減させることにより、企業の生産性を維持します。

- ・ まず、WebShieldのスパム検出機能が、既知のスパムソースからの電子メールを確実にブロックします。ここでは、MAPS(有料サービス)やORDB(無料サービス)などのサードパーティプロバイダが提供する、リアルタイムの「ブラックホール」リストを利用します。
- ・ ブラックホールリストを利用しない企業では、スパムメールに使われる語句を含むコンテンツルールを管理者が作成します。
- ・ 最後に、WebShieldが、ブラックリスト電子メールドメインの代わりに、許可済み電子メールドメインの「ホワイトリスト」を有効にします。

WebShieldのアンチリレー機能が、企業による不本意または無意識のスパムメール転送を防止します。さらに、WebShieldの免責サポート機能を利用して、全ての送信メールのフッターに標準的な免責事項を追加し、企業の法的ポリシーとセキュリティポリシーを徹底することができます。

プロテクションの強化:FTPダウンロード

WebShieldを利用して、FTPプロトコルを使ってダウンロードしたファイルのスキャンを実行することができます。ウイルスを含むファイルは、自動的に隔離、修復または削除されます。WebShieldは、ASCIIモードの8ビットFTPデータ転送をブロックするオプションを備えています。このタイプのデータ転送では、ウイルスを隠蔽し、スキャンデバイスによる検出回避を可能にしています。WebShieldは、ASCIIモードでの転送を禁止し、ASCIIファイルを含む全てのFTPファイルのバイナリモードによる転送を許可することにより、このセキュリティホールを解消しています。

IV. インストールとレポート作成:柔軟性とオプション

WebShieldを利用する上で、最大限の柔軟性を提供するために、透過型ブリッジ、透過型ルーティングとプロキシモードの3つのインストールモードが用意されています。

透過型ブリッジ:理想的なソリューション

トランスペアレントブリッジは、ネットワークアソシエイツが提供する最新のインストールモードです。このモードは、ファイアウォールでIPアドレス認証製品を利用する場合に最適です。

トランスペアレントブリッジモードでは、ネットワークブリッジ環境と同様に、トラフィックが1枚目のNICカードから入り、2枚目から通過していきます。WebShield自身がソースIPやMACアドレスなどの情報を保持するため、ファイアウォールを含む全ての隣接デバイスは、もとのクライアントマシンからのトラフィックとして要求を認識することができます。その結果、企業のネットワークルータやファイアウォールを一切変更せずに、WebShield Applianceは、デバイスを通るHTTP、FTP、POP3およびSMTPトラフィックをスキャンすることができます。これらのプロトコルのスキャンを実行するために、クライアント設定を変更する必要はありません。透過型ブリッジの利用により、ソリューション導入が簡略化されるだけでなく、複数の内部サーバを外部ユーザから保護することができます。アプライアンスの管理とウイルス定義ファイル(DAT)の更新には、1つのIPアドレスを割り当てます。

透過型ルーティング:スキャン実行を容易に

透過型ルーティングは、拡張が容易で、ネットワークオーバーヘッドの低減を可能にする、強力なソリューションです。このモードでは、保護するそれぞれのPCを設定する必要がないため、導入が大幅に簡略化されます。WebShieldは、保護するPCが他のネットワークとの通信に利用する(デフォルト)ルータの1台として設置されます。WebShield Applianceが保護されたPCからの要求を受信すると、パケット検査を実行します。ただし、WebShieldが要求をスキャン対象プロトコルとして認識しない場合は、他のルータと同様に要求をそのまま送信します。要求をスキャン対象プロトコルとして認識した場合は、内部スキャナのいずれかに要求を転送します。続いてWebShieldは、保護されたPCに代わって同一の要求をターゲットサーバに送信し、応答をスキャンして感染を調べ、その結果に応じてウイルスの駆除、応答のブロックまたは送信を実行します。

透過型の実装は、スキャンアプリケーションソリューションの導入とメンテナンスを大幅に簡素化します。WebShieldは、ブリッジングモードとルータモードで透過型SMTPに対応するため、電子メールトラフィックをアプライアンスに送信するためにメールサーバを変更する必要はありません。さらに、MXレコードを変更することなく、ネットワークの着信メールをWebShield Applianceに送信することができます。この機能により、多数のメールサーバを利用する環境やウイルス対策管理者の管轄外の環境であっても、WebShield導入が容易になり、SMTPトラフィックをスキャンできるようになります。

プロキシモード:従来のアプローチ

プロキシモードは、スキャンデバイスが持つ従来の実装方法です。プロキシオペレーションでは、保護するそれぞれのPCを設定して、特定プロトコル(POP3、HTTP、FTP)のトラフィックをWebShield Applianceに送信します。WebShieldは、要求を受信するたびに、パケットの検査を実行します。WebShieldがこの要求をスキャン対象プロトコルとして認識しない場合は、要求を無視します。要求をスキャン対象プロトコルとして認識した場合は、保護されたPCに代わって同一の要求をターゲットサーバに送信します。WebShieldが応答を受信すると、これをスキャンして感染を調べます。感染が検出された場合は、WebShieldがウイルスを駆除するか、応答をブロックします。感染していない場合は、応答をユーザに送信します。

プロキシモードの長所は、スキャンを実行するアプライアンスにスキャン対象トラフィックのみが送信されることです。その他のトラフィックは、デバイスを通り送らずに送信されます。プロキシモードでは、既存のキャッシングソリューションと負荷共有ソリューションとの併用によって機能を強化し、容易に拡張することができます。

プロキシモードの短所は、HTTPキャッシングが可能な場合を除き、WebShield Applianceで保護する全てのデバイス(クライアントマシンと電子メールサーバ)を明示的に設定し、WebShieldにトラフィックを送信するようにしなければならないことです。クライアントのウェブブラウザでアプライアンスをプロキシサーバーとして設定し、ログインスクリプトかSMSを使ってルーティングを変更します。さらに、電子メールサーバのMXレコードを手動操作で変更する必要があります。大企業では、このような設定変更に多大な労力が必要になる可能性があります。

いずれの導入オプションでも、WebShieldをファイアウォールの裏側に配置します。WebShieldは、あらゆるファイアウォールと電子メールサーバに対応しています。

ロードシェアリング機能:インストールと操作をさらに合理化

WebShieldは、導入をさらに容易にするために、ロードシェアリング機能による自動負荷共有を提供しています。アプライアンスをマスターまたはロードシェアリングサーバとして設定すると、1台のマスターがロードシェアリングサーバ群にスキャンするトラフィックを受け渡すようになります。その後、ロードシェアリングサーバがスキャンを実行します。負荷共有は、全てのプロトコルと、プロキシ、透過型ルーティング、透過型ブリッジングの全ての構成モードで利用することができ、特にHTTPトラフィックのスキャンで役立ちます。大量のHTTPトラフィックを処理する場合は、複数台のアプライアンス導入が必要になります。WebShieldのロードシェアリング共有を利用すれば、サードパーティ製のロードバランシングハードウェアに依存せずにHTTPトラフィックをスキャンすることができます。

ePolicy Orchestratorのレポート:インターネットゲートウェイの把握が容易に

WebShieldは、スキャンアクティビティの結果を2つの方法で通知します。「ログと警告のレポート」のページでは、グラフィカルなレポートを作成することができます。また、ePolicy Orchestratorとの統合管理により、ePOサーバを使ったレポートの作成も可能です。WebShieldは、ウイルス、ブロックしたURL、スパムや電子メールなど、さまざまな種類のレポートを生成する機能を備えています。さらに、日付の範囲、ログ、図表や「トップ10」レポートなどの出力フォーマットを選択することもできます。

WebShield Applianceは、ePolicy Orchestratorとの統合により、ゲートウェイでの主要なウイルスアクティビティのグラフィカルなレポートを提供します。28種類の詳細なレポートを利用して、コンテンツフィルタリングルールに設定されているポイントやアクセス禁止URLへのアクセスを調べ、ネットワークのゲートウェイ保護を総合的に把握することができます。つぎに、ePolicy Orchestratorを使って表示したレポートの例を紹介します。

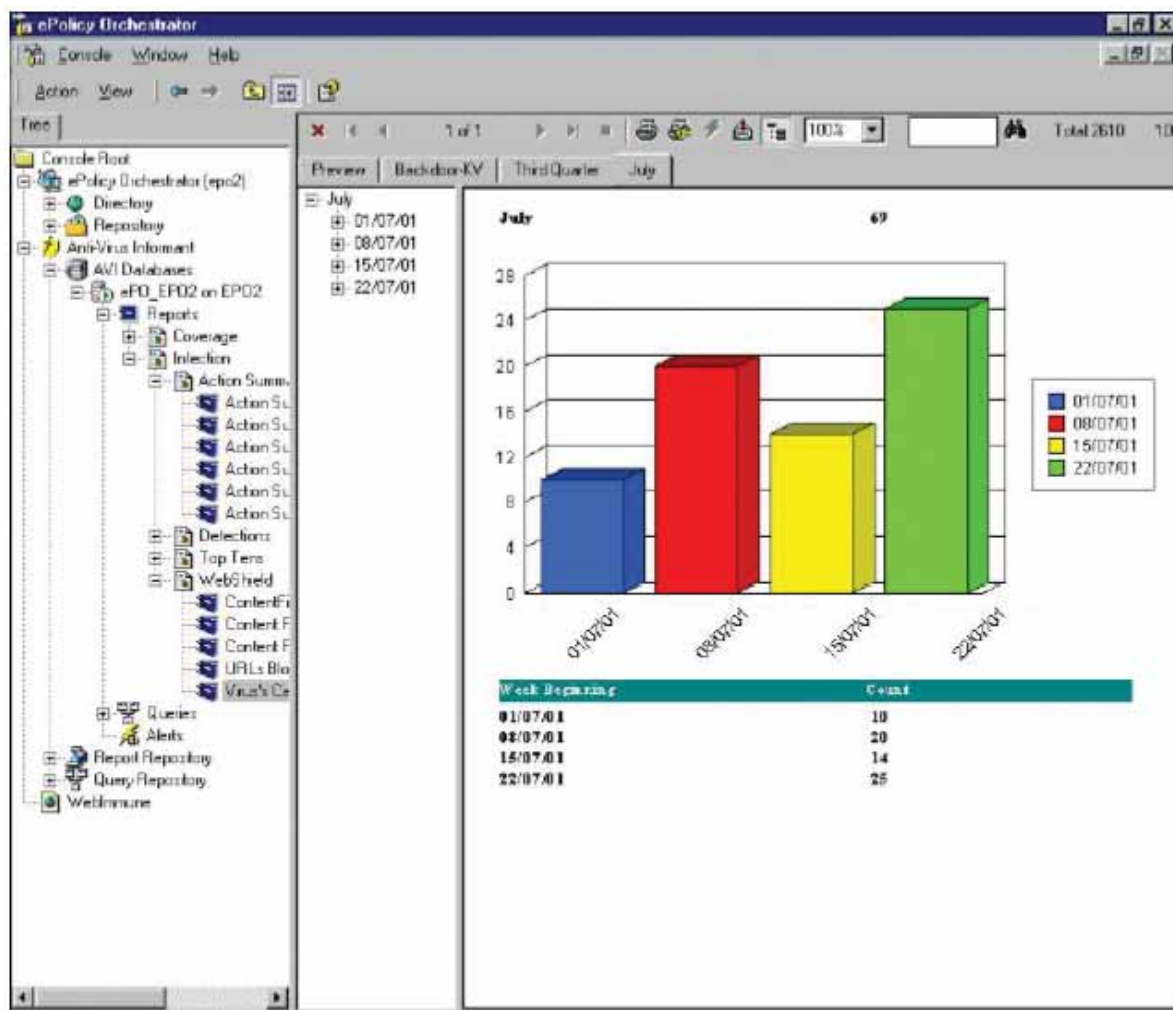


図 1

ウイルスイベントレポート：図1は、7日間で検出された、最も感染率の高いウイルスを示しています。グラフの該当部分をクリックすると、それぞれのウイルスの詳しい情報が表示されます。この情報は、アプライアンスログのフォーマットに似ており、日時、送信者、名前、対処方法と使用したスキャナなどが含まれています。

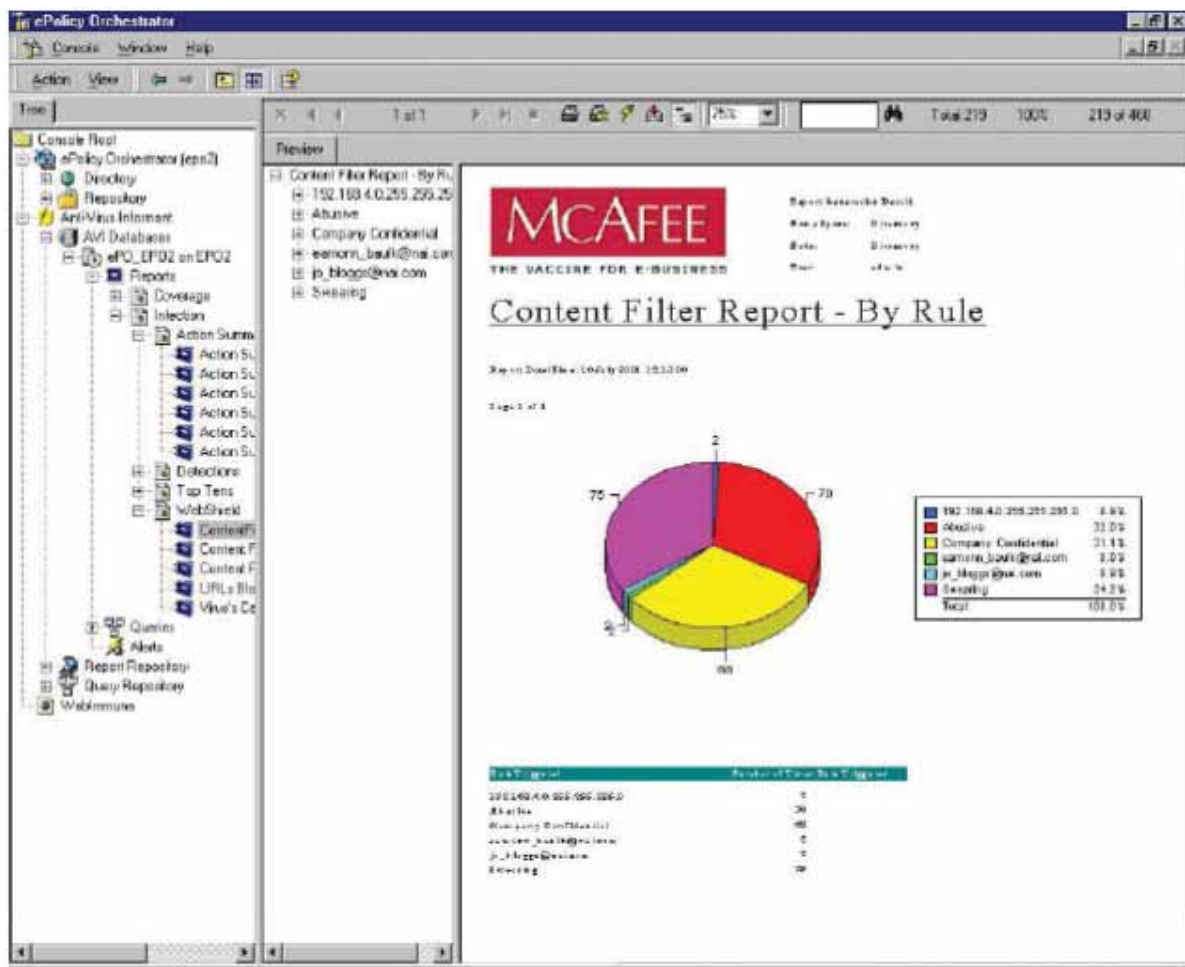


図 2

電子メールのコンテンツスキャンレポート: 図2のレポートでは、電子メールコンテンツスキャンのルールが表示されています。これらのルールは、企業メールシステムを使った、禁止されたテキストと語句を含む電子メールの送受信を防ぐために設定されたものです。

ePO レポートは、ネットワーク境界部でのアクティビティ情報を、複数の方法で提供することができます。このレポートを使って、ePO の企業全体のウイルスプロテクション表示機能を最大限に活用し、電子メールと HTTP セキュリティの課題を総合的な視点から把握することができます。

IV. まとめ

WebShield は、SMTP、HTTP、FTP および POP3 トラフィックのスキャンにより、複合型攻撃と関連性の高い電子メール感染ウイルス、悪性コードとサービス拒否攻撃から企業を保護するための重要な役割を果たします。WebShield スキャナは、潜在的な攻撃を企業ゲートウェイで確実に阻止し、内部のメッセージサーバやエンドユーザへの影響を未然に防ぎます。

McAfee WebShield は、以下の特長を備えた、最先端のゲートウェイスキャンソリューションです。

- ・ 必要な機能を全て備え、導入とメンテナンスが簡単な、完全統合型ソリューション
- ・ 業界最先端の透過型インラインスキャンにより、ソリューション導入をさらに簡易化
- ・ ロードシェアリング機能の統合により、複数アプライアンスの導入を容易にし、最高のスケーラビリティを実現
- ・ 企業の攻撃に最も頻繁に使われる4種のプロトコル(SMTP、FTP、HTTP、POP3)をサポート
- ・ コンテンツフィルタリングと URL ブロックにより、セキュリティを強化
- ・ アンチスパム機能とアンチリレー機能により、スパムメールの大量受信・転送から企業を保護

WebShield は、ウイルス検知および駆除ソリューションの最有力プロバイダーである McAfee Security のソリューションです。McAfee Security の優位性は、ハンブルグ大学 (<http://agn-www.informatik.uni-hamburg.de/vtc>) とマクデブルグ大学 (<http://www.av-test.org/>) が独自に実施した調査によって実証されています。

McAfee WebShield の詳しい情報については、<http://www.nai.com/japan> をご覧ください。

McAfee Security について

McAfee Security は、ネットワークアソシエイツ社の製品ラインであり、セキュリティ侵害、ウイルス攻撃と複合型攻撃からビジネスを保護しています。また、業界最先端のウイルス対策、暗号化、デスクトップファイアウォール、侵入検知、脆弱点検およびマネージド セキュリティ テクノロジーを通じて、包括的なネットワークプロテクションを提供しています。McAfee Security の全ての製品とサービスは、世界最先端のウイルス対策研究機関である AVERT (Anti-Virus Emergency Response Team: アンチウイルス緊急対策チーム) によってバックアップされています。AVERT チームは、LoveLetter、CodeRed や Nimda などの主要ウイルスの駆除手段を提供しています。McAfee Security の詳細については 03-5428-1104 まで電話でお問い合わせいただくか、ウェブサイト <http://www.nai.com/japan/product/product.asp> をご覧ください。



YOUR NETWORK. OUR BUSINESS.

製品、サービスに関するお問い合わせは下記へ

日本ネットワークアソシエイツ株式会社 www.nai.com/japan/

東京本社	〒150-0043	東京都渋谷区道玄坂 1-12-1 マークシティ ウエスト 20F TEL: 03-5428-1100(代) FAX: 03-5428-1480
西日本営業所	〒530-0003	大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL: 06-6344-1511(代) FAX: 06-6344-1517
名古屋営業所	〒460-0002	名古屋市中区丸の内 2-14-4 EXE 丸の内 4F TEL: 052-203-8421(代) FAX: 06-6344-1517
福岡営業所	〒812-0013	福岡市博多区博多駅東 1-10-27 アステリア博多ビル 8F TEL: 092-452-3511(代) FAX: 092-452-3515

Network Associates, McAfee, WebShield, ePolicy Orchestrator, ePO および PrimeSupport は、米国法人 Network Associates, Inc.またはその関係会社の登録商標です。Sniffer®ブランドの製品は Network Associates, Inc.が製造しています。© 2003 Network Associates Technology, Inc. All Rights Reserved.
製品、サービス、サポート内容の詳細は、最寄りの代理店または弊社事業部までお問い合わせください。製品の仕様、機能は予告なく変更する場合がありますので、ご了承ください。