セキュリティギャップにご注意：
マルチレベルの統合ソリューションで悪質コンテンツを阻止

Sophos White Paper
July, 2005

一般に、組織にとって最も効率よくネットワークを保護する方法は、複数のベンダーのセキュリティ対策を組み合わせて導入することである、と考えられています。しかし、今日のセキュリティ脅威はより迅速に蔓延しすると同時に複雑さを増しているため、保護対策基準もセキュリティ脅威の変遷に対応した迅速で柔軟な変更に迫られています。組織には、マルチレベルにおける統合脅威管理が必要です。

このホワイトペーパーでは、ソフォスが提供する統合脅威管理ソリューションについてご紹介します。ソフォスのセキュリティ解析センターソフォスラボ（SophosLabs™）は、多様なセキュリティ脅威に関する豊富な知識を備えており、新種のマルウェア（悪意のあるソフトウェア）やスパムキャンペーン（同一のメッセージを通知するために多様な形式で配信される一連のスパムのこと）の出所や蔓延方法にかかわらず、柔軟かつ迅速に対応します。

高速化するセキュリティ脅威

PC のブートセクタに感染する最初の PC ウイルス「Brain」が 1986 年に登場して以来、セキュリティ脅威の状況は大幅に変化し、そのスピードも日々高速化しています。ブートセクタ感染型ウイルスの後には、実行ファイルに感染するウイルスや、自身の姿を変えるポリモーフィック型ウイルスなど、多様なウイルスが登場しました。その後出現したマクロウイルスは、Microsoft Office ファイルに感染し、感染数と蔓延速度においてセキュリティ脅威新時代の到来を告げました。そして、最初のメール送信型ウイルス、Melissa（1999 年）および Lovebug（ラブレターウイルス：2000 年）の登場によって状況はさらに悪化し、過剰トラフィックが原因でメールシステムが崩壊し、保護されていないネットワークは麻痺しました。その後、スパムが登場し、セキュリティ脅威の深刻さが深まっています。

新種のセキュリティ脅威は、当初の予測をはるかに超える速度で増加を続けました。実際、新種のセキュリティ脅威が出現する頻度は増加しており、現在、Sophos Anti-Virus は 10 万種類以上のウイルスを認識しています（図 1 参照）。

コーポレートネットワーク保護の責任者にとって最大の課題は、保護するネットワークとセキュリティ脅威の両方が、ますます急速な変化を続けていることです。これまでは、

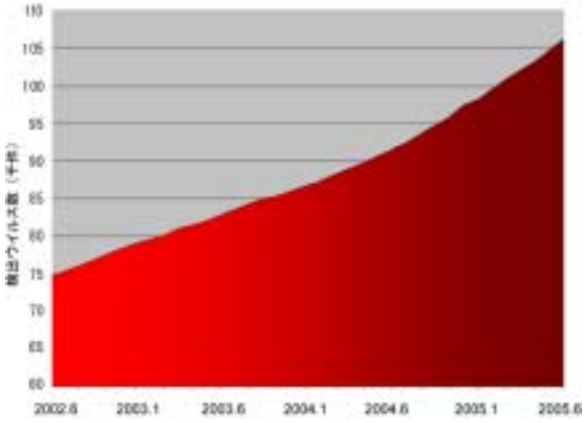

図 1：検出ウイルス数の増加（2002 年 7 月～2005 年 7 月）

ネットワークの各ポイントでの問題に対応するため、異なるベンダーの製品を個別に導入して、問題に対処することが一般的でした。しかし、この取り組みでは不十分になってきており、防御対策にギャップが生じてきています。

「各種製品を組み合わせてセキュリティ戦略を構築した組織は、しばしば、環境が統一されていないため問題が発生することを経験しています。複数のベンダーの製品の管理に追われ、お手上げになっている組織もあります。」

Chris Christiansen, IDC VP of Security Products, 2005 年 6 月

新規に発生し、急激に変遷するセキュリティ脅威

今日、「ウイルス」という用語は元来の意味から発展して、ワームやトロイの木馬などを含むセキュリティ脅威全般を指すようになってきています。また、「スパイウェア」、「ダイヤラー」、「キーロガー」などの新しい用語も登場しており、その多くは、従来なら「トロイの木馬」という包括的な用語で説明されていたものです。

必要ないのに勝手に送られてくる商用メールであるスパムは、一時、単に厄介なものとして扱われていましたが、現在はより高度なセキュリティ脅威となっています。フィッシング攻撃は元来、スパムの一種で、ユーザーを不安がらせることで機密情報をだまし取るものでした。しかし現在では、そのような心理的手法だけでなく、トロイの木馬、ワーム、またはウイルスを使用して、キーロガーその他のスパイウェアをインストールし、ユーザーのアクセスコードやパスワードを密かに収集し、ハードドライブやネットワークにて機密情報を探し出す手法にまで発展しています。搾取したデータはインターネットを介して第三者に送信され、何も知らないユーザーの個人機密情報や金融情報に容易にアクセスすることを可能にします。また、高額料金の電話番号に密かに接続し、感染ユーザーに多額の電話料金を払わせる「ダイヤラー」は、通常、ユーザーのシステムで実行されるよう、クリックしたくなるようなリンクや画像などを伴うトロイの木馬として配信されます。

このような金銭搾取目的の攻撃の登場は、コンピュータセキュリティの問題をより深刻なものにし、サイバー破壊者はサイバー犯罪者に変わりつつあります。これまでのウイルスは、たいてい愉快犯的な目的で作成されていましたが、金銭の魅惑に引きつけられて犯罪組織がウイルス作成に加わり、より狡猾な方法で他人のコンピュータやネットネットワークに侵入するようになりました。このように、ウイルス脅威とスパム脅威の境界線が薄れるなか、ウイルスやスパムに統合的に対応する防御ソリューションが不可欠となってきています。

ウイルス脅威とスパム脅威の境界線が薄れるなか、統合防御ソリューションが不可欠となっています。

数秒で世界中に蔓延

セキュリティ脅威は、多様化、大量化が進むだけでなく、新種のセキュリティ脅威が蔓延する速度も大幅に増加しています。ソフトウェアの脆弱性を悪用した脅威は、ユーザーの介在なしに蔓延します。たとえば、Windows OS や Windows アプリケーションにある脆弱性を悪性した Blaster や Slammer などのインターネット送信型ワームは、世界中の何 10 万台というコンピュータに 1 時間以内で感染できます。

十分に保護されていないコンピュータは、これまでになく短時間で攻撃を受けています。ソフォスの研究によると、パッチを適用しておらず、セキュリティ脅威から保護されていないマシンをインターネットに接続した場合、約 10 分以内に感染する確率は 50%で、45 分後に感染している確率は 90%に至ります（図 2 参照）。パッチやファイアウォールをダウンロードし、インストールしている余裕がないのが実情です。

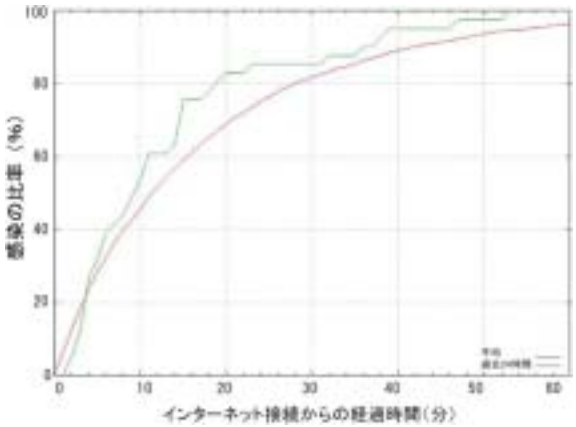

図 2：感染時間の分布

ネットワークファイアウォールがインストールされている環境では、瞬時に感染が広がってもすぐに直接的な被害につながることはありません。しかし、インターネットは、感染の対象とする脆弱なシステムを探すスキャナで溢れており、ブロードバンド接続している個人のコンピュータは格好の標的となります。このようなコンピュータはユーザーの知らないうちにハイジャックされる危険性が高く、法人ユーザーにさまざまな攻撃を仕掛けるステップに使用されます。ハイジャックされたコンピュータのグループは、「ゾンビネットワーク」と呼ばれ、疑わしい送信元アドレスや大量同報メールなどを検出するスパムフィルタを回避するために使用・売買されています。

多様化するセキュリティ脅威侵入ルート

セキュリティ脅威がますます多様化・高度化するなか、その感染ルートの種類も爆発的に増加しています（図3参照）。異なるハードウェア/ソフトウェア間の可動性・柔軟性・相互運用性など、より複雑な環境が IT システムに求められていることに起因します。

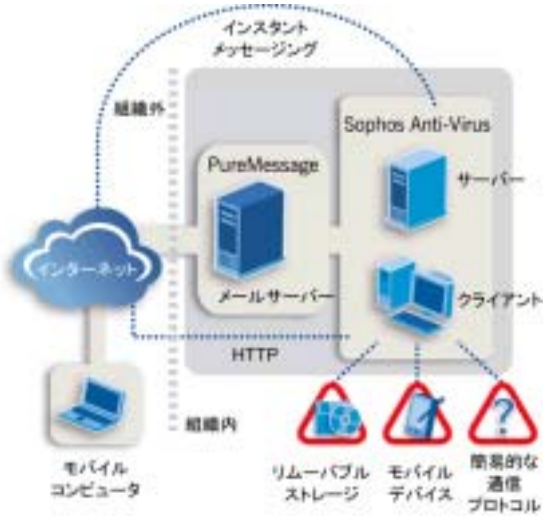

図 3：セキュリティ脅威侵ルートの多様化

従来、感染対象のシステムに悪質なコンテンツを侵入させるための主な手段としてメールが使用されていました。そのためセキュリティ担当者は、メールゲートウェイにおける保護の提供に重点を置いてきました。メールゲートウェイの保護は現在でもセキュリティ対策の要となっていますが、それだけでは他の感染ルートに対しては無防備です。

また、今日、悪質なコンテンツは、Web サイトからのダウンロードや、AIM や Skype などのインスタントメッセージング（IM）アプリケーション経由で（これらのアプリケーションの使用が認証されているかどうかにかかわらず）、組織に侵入する危険性が十分にあります。事実 IM アプリケーションは、しばしば企業のセキュリティシステムを回避することを目的として開発されており、その監視や規制は非常に難しくなっています。ネットワーク内で IM が使用されていないと思っている組織の多くは、単に管理者がその存在を確認していないに過ぎません。現行の IM アプリケーションでは組織内外へのファイル転送が許可されているため、メールシステムに厳重なセキュリティ規制が設けられている組織では、幹部役員が便宜上、IM を使用していることが多く見受けられます。

コミュニケーションネットワークの変化だけでなく、多様なプロトコルを介して、クライアントソフトや物理的接続なしにファイルを転送できるデバイスが増えています。企業コンピュータにアクセスしようとするすべての CD、USB ストレージデバイス、メモリカード、スマートフォン、および MP3 プレーヤーを管理するのは不可能に近いですが、これらのデバイスはすべて、悪質なコンテンツの侵入口となる可能性があります。同様に、ネットワーク周辺のすべてのルートでトラフィックをフィルタリングすることも困難です。クライアントマシンを含むエンドポイント保護は、これまで以上に重要となっています。有効な保護を実現するためには、エンドポイントとゲートウェイを統合的に保護することが必要です。

新種のハイブリッド型セキュリティ脅威は、保護責任の分担やネットワーク構成の複雑化によって発生するギャップを悪用します。

マルチレベルにおける脅威

悪質なコンテンツからネットワークを防御するために、すべてのレベルで保護を提供する必要があることは広く認識されています。しかし、各セキュリティ製品の機能の限界の問題ではなく、セキュリティ対策を講じる際に悪質なコンテンツをそれぞれ個別の問題として扱うという取り組みが原因で、防御体制にギャップが生じる危険があります。攻撃者は、各種の攻撃を整理、分類して行うわけではないので、防御側が分類して個別に対処していても無意味です。

Bofra、セキュリティホールを悪用

今日のハイブリッド型セキュリティ脅威を、「ウイルス」や「スパム」などに分類するのは容易ではありません。たとえば、2004 年 11 月に登場した Bofra は、セキュリティ脅威の分類方法に基づいた防御が困難かつ危険であることを示しました。Bofra は、一風変わった同報メール送信型ワームです。収集したメールアドレスに単に自身のコピーを送信するのでなく、送信者のコンピュータで稼動し、悪質コードを含む Web サーバーへのリンクのあるメールを送信します。以下は Bofra の感染プロセスをまとめたものです。

1. 感染したコンピュータに Web サーバーを作成する
2. 感染したコンピュータからメールアドレスを収集する
3. 収集した各メールアドレスに、この Web サーバーへのリンクを含むメールを送信する
4. 未感染コンピュータで受信者がそのメールを開き、リ

ンク(アダルト系コンテンツを含む)にクリックする

5. リンクは Internet Explorer IFrame の脆弱性を悪用して、コンピュータに感染し、Web サーバーを作成する

以上の手順を繰り返して感染を拡大させます。

技術的には Bofra はワームに分類されますが、重要なのは分類することではなく、感染を阻止することです。Bofra はメール内に存在しないので、メールゲートウェイでのウイルス対策ソリューションは無効です。メールにはリンクが存在するのみです。しかし、Bofra が送信するメールにはスパムの特徴がいくつか含まれています。実際、ソフォスは、当初より Sophos PureMessage のスパムフィルタを使用して Bofra に対する保護を提供していました。

結局、Bofra のような複合的なセキュリティ脅威から組織を守るのは誰の責任になるでしょう?ウイルス対策部門、メール部門、Web 部門、パッチ管理部門などが候補にあがりますが、このような脅威に対しては責任をいずれかの部門に割り当てることは困難です。

時代遅れのセキュリティ対策を見直す

多くの組織は、このような主観的な境界に沿って防御体制をとっていますが、これは責任の所在を不明瞭にし、セキュリティ対策のギャップを悪用する脅威につけこまれる要因となりかねません。複数のベンダーの製品を使用して、ギャップを埋めるのが一番効果的であるという考え方は時代遅れです。マルチベンダー・アプローチでは、経済的・管理負荷にコストがかさむだけでなく、深刻なのは、セキュリティレベルの低下を招いてしまうことです。

より確実な保護は、セキュリティ問題を全体的にとらえることで提供できます。多様な新種セキュリティ脅威にも対処できる、ソフォスの包括的なウイルス/スパム検出機能を採用することで、組織は保護体制を大幅に強化することができます。問題の一部分のみに対処するアプリケーションは、このような高レベルの保護を提供することはできません。

「ソフォスラボの経験豊富なアナリストは、豊富な知識と多様なテクノロジーの統合をベースに、多種手法が組み合わされている新種のセキュリティ脅威にも、迅速かつ効果的に対応します。

悪質コンテンツの問題が、複数の次元で同時進行するなか、統合された多次元アプローチでの保護が重要です。図 4a のような場当たり的な保護体制から、図 4b のような統合脅威管理体制への速やかな移行により、スパムとウイルスを区別して防御することによるセキュリティギャップが解消されます。組み合わされた複雑な性質を持ちます。

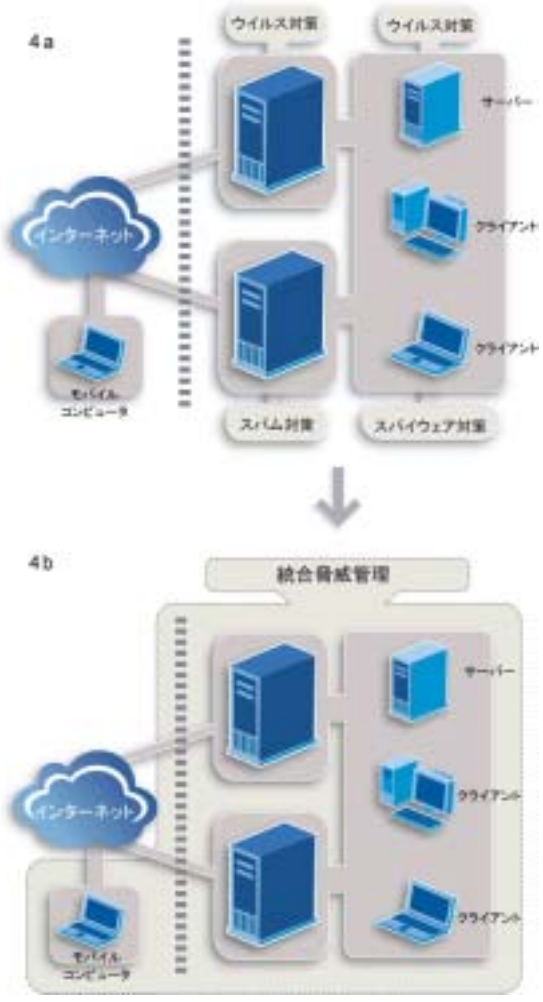

図 4: 統合脅威管理によるトータル保護

ソフォスの統合脅威管理

ソフォスは、セキュリティ分野で 20 年の経験と実績を持ち、あらゆる種類の悪質コンテンツから組織を保護する豊富な知識と技術を備えています。ソフォス製品は、あらゆるポイントで統合保護を提供できるよう、設計・開発されています。たとえば Bofra は、ゲートウェイでスパムフィルタによって阻止され、Web ダウンロードファイルが実行される前に、クライアントマシン/モバイル PC でウイルス検出が行われます。

SophosLabs（ソフォスラボ）

世界各地に展開する脅威解析センター、ソフォスラボでは、長年の知識と経験に基づいてマルウェアとメールを統合的に解析し、あらゆるタイプの新種脅威に多様な検出機能を提供します。ソフォスは早期検出および高レベルの保護機能を提供するため、常時、最新の手法を開発し、提供しています。ソフォスウイルス検出エンジンとスパム検出エンジンには Genotype™（ジェノタイプ: 遺伝子型）テクノロジーが含まれており、新種脅威へのプロアクティブな保護を実現し、新種脅威が出現してから特定のウイルス定義ファイルやスパムルールがリリースされるまでの期間も、組織のネットワークを保護します。

ソフォスラボは世界各地に拠点を置き、多種のセキュリティ脅威に関する知識と強力な統合テクノロジーをユニークに統合して提供します。正確な解析と迅速な対応を 24 時間/365 日提供し、複雑化を増す脅威から組織を保護しています。詳細は、ソフォスの技術資料『ソフォスラボ: セキュリティ脅威が迅速に変遷するなか、「デイ・ゼロ」攻撃に対する保護を提供』をご参照ください（www.sophos.co.jp/virusinfo/whitepapers）。

> *「ソフォスはあらゆる拠点を強固に保護する統合ソリューションを提供しているため、ユーザーは、異なるベンダーから複数のソリューションを使用することに伴うコストや不確実さを排除できます。」*
>
> *Chris Christiansen, IDC VP of Security Products, 2005 年 6 月*

ゲートウェイ/メール保護 – Sophos PureMessage

Sophos PureMessage™は、ゲートウェイで包括的かつ柔軟なメール管理機能を提供します。多言語環境で 98%までのスパムを阻止し、すべてのメールトラフィックでウイルス、トロイの木馬、ワームおよびスパイウェアを検出・駆除します。Genotype 検出テクノロジーを提供するほか、「脅威の削減」テクノロジーにより、多様な条件にあてはまる既知または新規のウイルスやスパムを阻止し、特定のウイルス定義ファイルがリリースされる前でも、メール送信型ワームなどの新種セキュリティ脅威を阻止します。PureMessage は、悪質コンテンツの検出・削除のほか、あらゆる要件に対応できる高度なメール転送ポリシーを施行でき、複雑化する法規制の遵守を支援します。インターネットを介して最新のウイルス定義ファイルとスパムルールを自動アップデートすることができます。

エンドポイントセキュリティの管理 – Sophos Anti-Virus

Sophos Anti-Virus™は、マルチプラットフォームに対応し、ウイルス、トロイの木馬、ワーム、およびスパイウェアを、サーバー/クライアントマシンやモバイル PC で検出・駆除します。ソフォスウイルス検索エンジンには、ソフォス独自の Decision Caching 機能が含まれており、高速スキャンを実現します。その他、Genotype テクノロジーをはじめとする多彩な機能のほか、EM Library™ や Enterprise Console™ などの高度な管理ツールを統合しています。EM Library は、ネットワークを介して Sophos Anti-Virus を自動的にインストール/アップデートします。

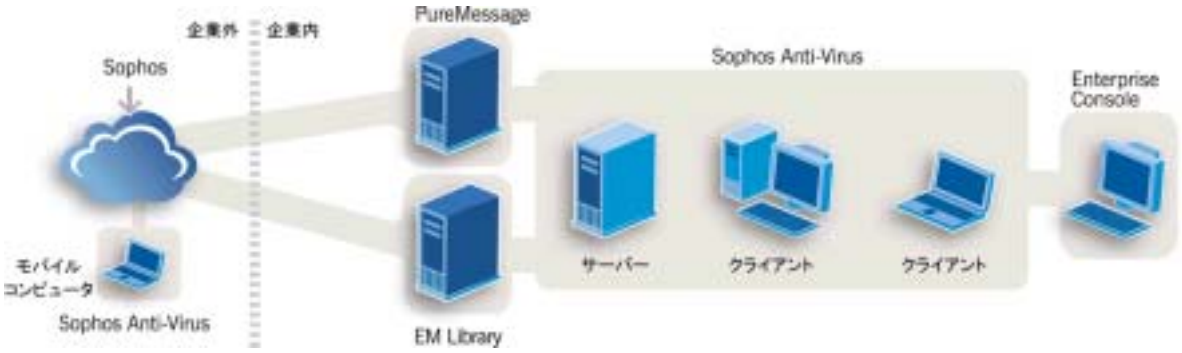

図 5: ソフォスの統合脅威管理

Enterprise Console は、(リモートコンピュータを含む) ネットワーク全体で Sophos Anti-Virus の環境設定とアップデートポリシーを一括設定できます。すべてのコンピュータにおける製品のステータスを表示し、ウイルス活動すべてに対するレポートを作成するなど、管理者の負荷が大幅に軽減し、TCO が削減されます。

サポート体制

すべてのソフォスライセンスは自動アップデート機能を提供しており、アップデート版がクライアントマシンやゲートウェイに迅速に配信されます。

まとめ

今日、ウイルスやスパムなど、各種セキュリティ脅威の境目は必ずしも明確ではなくなってきています。セキュリティ脅威とその侵入口を個別の問題として対策することによって、ネットワークセキュリティにギャップができてしまいます。また、ゲートウェイおよびエンドポイントで異なったベンダーの製品を導入することによるコストや管理負荷の増大も軽視できません。

多様なセキュリティ脅威に関する知識・経験に基づいたソフォス製品を使用すれば、そのような問題に遭遇することはありません。ソフォスは、20 年を超える経験、研究・解析ノウハウ、および強力なテクノロジーを活用して、セキュリティ脅威に迅速かつ確実に対応し、悪質コンテンツに対する優れた統合ソリューションを提供しています。

ソフォスやソフォス製品を使って組織を保護する方法の詳細は、www.sophos.co.jp をご覧ください。

ソフォスとは

ソフォスは法人向けセキュリティ対策ソリューションの世界的なリーディング プロバイダです。グローバル企業、SMB市場、製造業、金融業、政府機関、教育機関など、あらゆる分野、規模の法人・組織をセキュリティ脅威から保護します。全世界150カ国以上で3,500万以上のお客様にご導入いただき、その高品質な技術力とサービスは高い評価をいただいております。

ソフォス株式会社
〒231-0062　神奈川県横浜市中区桜木町1-1-8 日石横浜ビル15F
Tel. 045-227-1800　　E-mail. sales@sophos.co.jp

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

SOPHOS
WWW.SOPHOS.CO.JP