あなたのメール、本当に安全ですか？

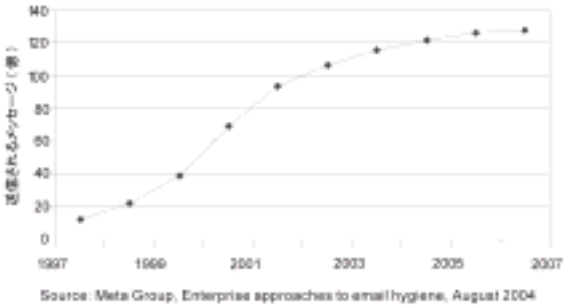
Sophos Positioning Paper
September, 2005

昨今、組織が情報やメールの流れを管理して重要なビジネス情報の機密性を保持するためには、複雑な IT 環境に対応した様々な対策が必要です。セキュリティを確保するためには、単にエンドポイントとゲートウェイにウイルス対策ソフトを配備したり、ファイアウォールを設置するだけでは十分ではありません。

このポジショニングペーパーでは、メールがビジネスにもたらすセキュリティ脅威の性質と問題点を挙げ、対策技術やテクニックを説明します。また、ソフォスのメールセキュリティソリューションである PureMessage と、エンドポイントのセキュリティソリューションである Sophos Anti-Virus について説明します。

メールのビジネス使用

電子メールはいまや必要不可欠なビジネスツールであり、今後もその使用は拡大すると予測されます（図 1 参照）。



Source: Meta Group, Enterprise approaches to email hygiene, August 2004

図1: 1日に個人間でやりとりされるメッセージの数

多くの組織がメールインフラストラクチャの急激な強化を経験していますが、メールのセキュリティ対策は必ずしもそれと同期して強化されているとは限りません。組織にとってメールが最も大きなセキュリティ脅威になり得ることが判明しているにもかかわらず、その状況はかわっていません。実際、ウイルスの 90%がメールを介して感染を広げ、スパムがメールの全体量の 60～80%を占めるといわれています。

> *「...メールの重要性が増すにつれ、システムの安定性に対する脅威も加速的に増えています。」*
> *Meta Group: Enterprise approaches to email hygiene, 2004 年 8 月*

攻撃）などへのメール型セキュリティ脅威への対策が必須

メール型脅威の環境

一般に、メールセキュリティ対策は主にゲートウェイに集中する傾向がありますが、実際にはメールシステムの様々なポイントに脆弱性が存在し得ます（図 2 参照）。そのため、ゲートウェイのみにセキュリティ対策を行っているだけでは、ゲートウェイを回避したり、対策の裏をついたりしてメール型セキュリティ脅威が侵入し、ネットワークが危険にさらされてしまう危険性があります。特に、スパム対策、ウイルス対策、ポリシー施行などがそれぞれ異なるベンダーのソフトウェアを採用してつなぎあわせて導入されている場合、ゲートウェイ自体に脆弱性をはらんでしまい、脅威の侵入を許してしまう危険性が高くなります。

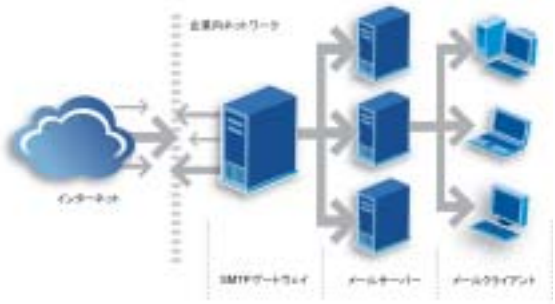


図2: メールシステム中で脆弱性を含む可能性のあるポイント

ゲートウェイのセキュリティ対策

ネットワーク通信量が増え、メールの使用も複雑化する中で、システムに脆弱性が発生する危険性も高まっています。ゲートウェイでは、スパムや、フィッシング詐欺、ウイルス、DoS 攻撃、DHA（ハーベスティング
です。また、攻撃的な内容や業務上不適切なメールもゲ

ートウェイで検出し、社内のメールサーバーに引き渡される前に阻止されなければなりません。

ビジネス上でのメール使用の増加は、組織の機密情報が漏えいする危険性も引き起こしています。たとえば、知的財産、コンプライアンスの遵守、競合他社との競争力などが脅かされたり、企業の信頼性が損なわれたりします。組織内から外部に発信する情報のコンテンツスキャンの実施、情報送信にかかわるポリシーの策定、導入、管理などの対策は、受信する情報のコンテンツスキャンなどの対策に比べると、導入が遅れる傾向がありますが、送信情報の管理も、ネットワーク管理者にとって重大な課題です。

ゲートウェイの内部

ゲートウェイでのセキュリティ脅威だけでなく、組織内部から発生するメールによるセキュリティ脅威も多く存在します。

内部ウイルス拡大

マルウェア（悪意のあるソフトウェア）は、インスタントメッセージや USB ドライブなどのエンドポイントから感染し、ネットワークに重大な被害を与えます。感染したマシンから送信されるウイルスの、他のマシンへの感染を阻止することで、内部感染の被害を防ぐことができます。メールフローの中でも、エンドポイントはセキュリティ脅威の防御の最終ラインであるといえます。

「ウイルス感染したノート PC は、企業のネットワークに対し、ハッカー攻撃よりも甚大な被害を与えます。北米の年間ウイルス被害 450 億ドルのうち、40～60%が、ウイルスやトロイの木馬による内部からの攻撃に起因しています。」
バンクーバー Sun 紙、2004 年 5 月 25 日

今日のセキュリティ脅威は、ワーム、スパム、ウイルスが組み合わされた複雑な性質を持ちます。たとえば、マスメール型ワームである Bofra は、当初スパムとして出現しましたが、実際には悪質なペイロードを含むウイルスでした。しかし、ウイルスはメールで配信されなかったため（Web リンクから感染コンピュータに攻撃を加えました）、メールゲートウェイのウイルス対策ソリューションは、このワームには無効でした。このワームはスパムフィルタによって防御されるべきですが（実際、ソフォスの PureMessage では防御することができました）、このようなタイプのセキュリティ脅威には、ゲートウェイよりもエンドポイントでの防御が有効です。

メールボックス中の感染メール

マルウェアはメールの添付ファイルとしてシステムの中に保存され、長い時間がたってから起動され組織内に感染を広げることがあります。そのため、システムに保存されているメールを定期的にスキャンし、パブリックフォルダや未配信メッセージにウイルスが含まれていないかをチェックすることは重要です。

情報漏えい

フィッシングは、偽のサイトにユーザーの機密情報を入力させる詐欺行為ですが、それよりも情報漏えいが発生する危険性が高いのは、組織内のユーザーによる機密情報の送信です。フィッシング詐欺はスパムフィルタで防御することができますが、情報漏えい対策にはポリシー施行が有効です。

ハイジャックされたコンピュータ

デスクトップマシンやノート PC などのメールクライアントがメールで配信されるトロイの木馬やワームなどによって「ゾンビ」化されると、スパムやウイルスの配信や DoS 攻撃に利用されてしまいます。ソフォスの調査によると、スパムの約 50%が、このようなハイジャックされたコンピュータから送信されています。多くのマシンは、正規の組織の正規のネットワークに属しており、発信するメッセージも正当なものであるかのように偽装されます。マシンのゾンビ化を防ぐためには、デスクトップ用のウイルス対策ソフトが効果的です。もし、組織がスパム送信者リスト（DNSBLs）に掲載されてしまうと、メール送受信の機能は制限され、組織の信頼も大きく損なわれます。

セキュリティ業界のポジショニング

メールによるセキュリティ脅威が多様化する中で、組織を完璧に保護するメール防御モデルの構築も難しくなっています。SMTP 以外の IMAP や POP3 などのプロトコルを採用した場合でも問題は解決されませんし、送信メールのセキュリティも、暗号化ソフトによる対策だけでは十分とはいえません。

ゲートウェイを中心としたソリューションは、ネットワーク全体の脆弱性をカバーすることにはつながらず、システム

管理全体の課題への解決策とはなり得ません。継続のあるシステム管理モデルの構築や統合的なソリューションの導入を行わずに、各セキュリティベンダーが提供する新しいテクノロジーを場当たり的に導入して組み合わせていると、結果的に安全性に欠けたシステムが構築されてしまう可能性があります。

メールに関するセキュリティ対策をゲートウェイのみに集中させているベンダーに依存してしまうと、Bofra のようなマルウェアに対抗できない危険性があります。

また、テクノロジーは常に変動しているため、永続的に安全であり続けるシステムは存在しません。現在、スパム対策の主流は、まずスパムやウイルスを阻止した後、送信者認証フィルタリング（受信したメールの送信者が DNSBL に含まれていないかを確認する）を行う「トラフィックプロファイリング」の手法を採用しています。加えて、トラフィック量をモニタリングし、ウイルスの大規模感染発生や新規スパムキャンペーン（同一のメッセージを異な形式や形態で送信する一連のスパム）の情報などを収集するなどの対策手法が平行して採用されます。

トラフィックプロファイリングは、メール型ウイルス亜種やスパムキャンペーンの大規模発生に有効ですが、以下の理由によりその効果は低下し始めています。

1. スパマーやウイルス作成者がゾンビネットワークを使用している場合、送信者認証フィルタリングは有効ではない。
2. トラフィック量監視による防御は、検知を回避するためにメール送信量を制御して配信するような攻撃に対しては有効ではない。

セキュリティソリューションを回避しようとする攻撃が増えている中で、トラフィックプロファイリングの効果は低くなりつつあります。

3. 最新のウイルス/スパム対策エンジンでは、ウイルスファミリーやスパムキャンペーンへのより効果的な防御方法を提供し、効率的に保護する。

IT システムの課題

現在、組織は大量化する脅威にさらされており、IT 部門は、ビジネスネットワークと組織内の機密情報を守り、組織の対外的な信頼性を保たなければならないという課題がつきつけられています。

メールシステムのセキュリティを確保するために最低限必要な要件として、以下の 3 点が挙げられます。

- **システムの複数の脆弱性を防御する。**
  ゲートウェイとエンドポイントに統合的にセキュリティ対策を導入する。
- **システムの連続性を維持する。**
  ウイルスやスパムの誤検知による混乱を最小限にとどめる。また、メール型ウイルス亜種のネットワーク攻撃を阻止し、亜種による警告数や対策の必要性を最小限に抑える。
- **管理要件を明確化して実施する。**
  機密情報や知的財産を守るため、セキュリティポリシーを徹底して施行し、リソース管理、制御を自動的に行う。

Sophos PureMessage – ソフォスソリューション

ソフォスは、ウイルス、スパイウェア、スパムに対し、マルチレベルでの防御を 24 時間/365 日年中無休で提供すると同時に、メールポリシーの違反を阻止します。

統合脅威管理：すべてのポイントにセキュリティを提供

ソフォスは、エンドポイントからゲートウェイまで、あらゆるポイントでメールシステムの脆弱性をカバーし、セキュリティを確保します。PureMessage はメールゲートウェイ、メールサーバー、部門内の各ワークグループ単位に、ウイルス対策、スパム対策、ポリシー強化機能を提供します。また、Sophos Anti-Virus は、エンドポイントでのウイルス対策を提供します。

信頼性の高い防御機能：システム連続性の維持

ソフォスの PureMessage は、高度なウイルス/スパム対策機能を提供し、システムの連続性をサポートします。Genotype™（ジェノタイプ: 遺伝子型）検出テクノロジーによって、急速に蔓延する新規のウイルスやウイルス亜種、スパムキャンペーンから、ネットワークをプロアクティブ（予防保守）に阻止します。Genotype テクノロジーにより、特定のウイルス定義ファイルやスパムルールが提供されていなくても、ウイルスファミリーやスパムキャンペーンを検知・駆除し、ネットワークを保護します。

ソフォスのグローバルなセキュリティ解析センターであるソフォスラボは、Genotype テクノロジーおよび、その他多様なウイルス/スパム検知技術を駆使してウイルス/スパムを検知し、24 時間 365 日、ソフォスのお客様に最新の対策を迅速にご提供しています。PureMessage for UNIX および PureMessage for Windows は、ゲートウェイでスパムやマルウェアを阻止し、PureMessage for Exchange はメールボックスの中のメールや、メールサーバー上のトラフィックに含まれるウイルスやスパイウェアを阻止し、組織内でウイルス被害が拡大するのを防御します。

管理の容易さ：管理要件の明確化と実施

PureMessage は優れた管理ツールを装備しており、大規模で複雑なネットワークの要件にも柔軟に対応し、容易に管理する機能を提供します。フレキシブルで拡張性が高く、組織内の既存のシステム環境に容易に統合できます。

「Sophos PureMessage は、最も優れたメールポリシー施行を提供している製品だ。その豊富な機能に迫るソリューションは他に存在しない。」
Networkworld 誌 2004 年 12 月号

PureMessage for UNIX は、スタンダードベースのテクノロジーで構築されており、一般的なメール転送エージェント（MTA）や LDAP、Active Directory などをサポートしています。組織内のすべての隔離アイテムをシングルポイントに集中化して管理することができます。

ハイレベルなコンテンツスキャン機能、メッセージルーティング、ホワイトリストやブラックリストの設定など、組織独自の要件にあわせてきめ細かく設定することができ、複雑な要件にも柔軟に対応して、組織の知的財産などの機密情報を堅固に保護します。

ソフォスのサポート体制

ソフォスラボは、全世界で 24 時間 365 日、ウイルス/スパム解析を行い、最新のウイルス定義ファイル、スパムルールを常時お客様にご提供しています。ソフォスはセキュリティ分野で 20 年以上におよぶ経験と実績を持ち、ソフォスラボのエキスパートが、ウイルスやスパムなどのセキュリティ脅威を統合的に解析し、複雑に組み合わされた脅威に対し、最適のソリューションをご提供します。

まとめ

メールセキュリティ対策の最も大きな課題のひとつに、組織がセキュリティ対策を行うにあたって、マルチレベルでの対策が必要であることを意識していない点が挙げられます。現在の大規模化、複雑化したネットワークシステムの中で、すべてのレベルで脆弱性に対策を講じることは、IT 専門家にとっても大変に難しく、特に、個々のレベルでそれぞれ異なるセキュリティソリューションが適用されている場合、統合的な対策をとることは非常に困難です。

ソフォスの PureMessage は、組織のゲートウェイ、部門メールサーバーでメール型ウイルスやスパムを阻止し、Sophos Anti-Virus と連携してすべてのエンドポイントをセキュリティ脅威から防御します。経験豊富なソフォスラボがお客様を強力にサポートし、多様化、大量化、複雑化する脅威に対し、的確なメールセキュリティソリューションをご提供します。

参考

1. 『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』ソフォスホワイトペーパー, 2005 年 7 月,
www.sophos.co.jp/virusinfo/whitepapers

2. 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,
ソフォスポジショニングペーパー, 2005 年 6 月,
www.sophos.co.jp/virusinfo/whitepapers

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