

媒体名	発行部数	掲載日	掲載面
NETWORK MAGAZINE	24,208	2006年5月号	

電子メール セキュリティ 最前線

特集 1

日本版SOX法 「対応」製品が 続々登場!

電子メールのセキュリティ対策といえば、古くはウイルスの除去やメッセージの暗号化、最近ではスパムメールやフィッシング詐欺メールの分別が定番である。しかし、早ければ2008年施行ともいわれる「日本版SOX法」への対応製品として、最近ではメッセージの監視やアーカイブといった分野にも注目が集まっている。特に上場企業を中心に必須となる内部統制、内部監査の切り札として電子メールのセキュリティを見直そうというのだ。

文●編集部
写真●三浦健司
撮影協力●通信総合博物館



製品による得意・不得意を知ろう！

ウイルスとフィッシングの被害を防ぐ

企業のメールサーバでやりとりする電子メールを監視し、ウイルスやフィッシング詐欺メールなど、問題のあるメッセージを削除する技術に、ウイルス対策用のゲートウェイがある。最近では管理の手間がかからないアプライアンス型や、メールサーバ一体型の製品も増えてきた。このような製品やサービスは、どのような観点で選べばよいのだろうか？

ウイルス対策ソフトに違いはあるのか？

国内ではシマンテック、トレンドマイクロ、マカフィーの3社が「3大ウイルス対策ソフトメーカー」とわれている。このほかに、韓国やロシア、中国製などのウイルス検出エンジンを採用したパッケージソフトが販売されている状況だ。

では、こうしたメーカーはどのように異なるのだろうか？ さらにいえば、ウイルス対策の精度には違いはあるのだろうか？

結論からいうと、ウイルス対策の精度には偏りがある。

パターンファイルの偏りは、ウイルスの検体をいかに早く入手できるかで決まる。平均的には観測地点が多いメーカーほど有利だ。たとえば日本発のウイルスの検体を素早く入手するには、日本に研究開発拠点のあるメーカーが有利になる。

また、Winnyのようにほぼ日本でしか使われていないソフトウェアの場合、日本に研究開発拠点がないと検体そのものを入手できない可能性がある。ウイルス対策の精度に偏りが生じるのは、検体採取の母数や地域がメーカーによって異なるのが原因だ。

なぜ偏るのか、パターンファイルの作り方を見ることで説明しよう。

■検体の入手

ウイルス対策ソフトのメーカーは、ウイルスの発生源となるWebサイトやスパムメール、ファイル共有ソフトのネットワークを常時監視している。また、契約企業のネットワークを監視し、疑わしいファイルの検査を依頼されることもある。一般ユーザー向けのパッケージソフトを販売しているメーカーの場合は、一般ユーザーから疑わしいファイルを提供されることもある。こうした検体を分析し、ウイ

ルスが既存のウイルスの亜種なのか、まったく新しいウイルスなのかを判断する。

■パターンファイルの作成

検体からウイルスの特徴を抽出する。「パターンファイル」といっても、実際に個々のウイルスごとのパターンを記述したファイルがあるわけではない。ウイルスやスパイウェア、フィッシングは膨大な種類があり、いちいちパターンファイルを作っていたのでは迅速に検査できなくなるからだ。そのため、多くのウイルス検出エンジンではディスクのアクセス、電子メールのヘッダ部分など、検査対象ごとにプログラムが分かれている。

■パターンファイルの検査

作成したパターンファイルはすぐには配布できない。パターンファイルには、ウイルスの特徴が書き込まれているだけであり、無害なファイルの特徴と一致して

会社名	種別	ウイルス検出エンジン
IIJ	サービス	トレンドマイクロ InterScan VirusWall
アイアンポートシステムズ	アプライアンス	ソフォス Anti-Virus
クリアスウィフト	アプライアンス/ソフトウェア	ソフォス Anti-Virus/シマンテック AntiVirus
サーフコントロールジャパン	アプライアンス	マカフィー Anti-Virus Agent
サイファートラスト	アプライアンス	サイファートラスト Zero Day Virus Protection
シマンテック	アプライアンス/ソフトウェア	シマンテック AntiVirus
フォーティネット	アプライアンス	フォーティネット FortiGate
ホライズン・デジタル・エンタープライズ	ソフトウェア	Fセキユア Anti-Virus
ミラポイント	アプライアンス	ソフォス Anti-Virus

表1●ウイルス検出エンジンの採用例



しまうこともあるからだ。そこで、実際のシステムに試験的にパターンファイルを組み込むなどして事故が起きないかどうかを検査する。

■パターンファイルの配布

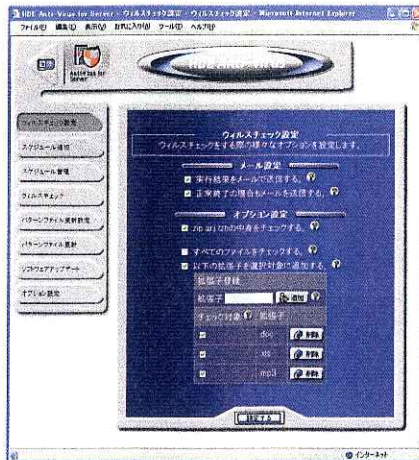
無害なファイルをウイルスなどと誤認しないかどうかの検査をパスしたパターンファイルは、一般に公開される。最近のウイルス対策ソフトでは、定期的に自動更新されることが多い。

メーカーによって異なるが、パターンファイルの作成手順はおおよそ以上のような形である。検体の入手からパターンファイルの配布まで、早くても数時間かかるといわれている。そのため、最近ではパターンファイルの配布がウイルスの感染スピードに追いつかない問題が指摘されている。また、パターンファイルの更新を怠ったり、自動更新時にインターネットに接続できなければ、最新のウイルスに対応できないことになる。

もちろん、日本に研究開発拠点が無いからといって、ウイルスの検体をまったく入手できない、ということはない。ただ、検体入手のタイミングが遅れば、その分パターンファイルの配布も遅れる。国内のみで活動する企業であれば、営業拠点だけではなく、国内に研究開発拠点があるウイルス対策メーカーや、そこからウイルス検出エンジンの供給を受けているメーカーの製品やサービスを選ぶとよいだろう。

ウイルス対策製品の種類

ウイルス対策用の製品やサービスは、メールサービス統合型やメールサーバー一体型、独立アプライアンス型など、いくつかの種類がある。どの場合でも、メーカー側がウイルスの特徴を記述したパターンファイルを配布しているのは同じで



画面1●HDE Anti-Virus
エフ・セキュアのウイルス検出エンジンを採用している

ある。どの製品でもこのパターンファイルとメッセージやファイルと照合、特徴が一致すればウイルスとみなす、というのが基本的な仕組みだ。ただ、仕組みが同じだからといっても、製品やサービスの形態によって管理者の手間は変わってくる。ウイルスやフィッシング対策製品、サービスを分類し、管理者の手間という観点で見たいこう。

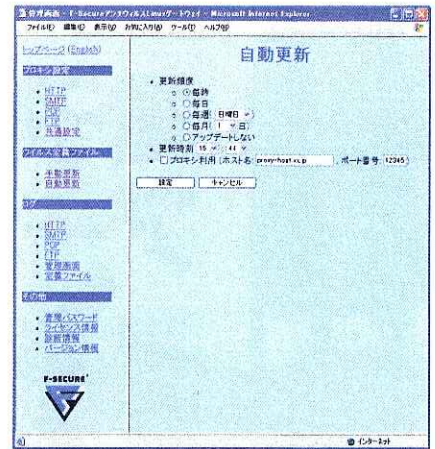
■メールサービス統合型

電子メールのASP型サービスを利用する方法。ウイルスやフィッシングメールの駆除機能は、メールサービスのオプションとして提供される。

この方式は管理者の手間がもっともかからないため、特に中小企業にはオススメだ。パターンファイルの更新などもサービス提供者の責任になるため、管理者はユーザーの追加や削除だけすればよい。ただし、1メールボックスあたり数百円の月額利用料がかかるため、ユーザー数が多くなると自社運用に比べてかなり割高になる。

■メールサーバー一体型

メールサーバーアプライアンスにウイルス対策機能が付加されているタイプ。パ



画面2●エフ・セキュアのウイルス検出サーバの設定画面
HDEと同種のサーバソフトだが、HDEの方がカスタマイズされていることがわかる

ターンファイルはアプライアンスが自動的に更新してくれる。また、メールサーバーの基本機能とウイルス対策機能が統一されたインターフェイスで操作できるため、管理者の手間は小さい。

ただし、メールサーバーアプライアンスはメールサーバーの自社運用に比べると高価である。管理の手間が減るのは確かだが、ユーザー数によってはユーザー単価が自社運用に比べて数倍から数十倍になることもある。また、メールサーバーのストレージ容量が大きい製品もあるため、1ユーザーあたりの容量がどのくらいになるのか計算するとよい。(1ユーザーあたりの推奨容量は業種によって異なるのでここでは明記しない)。

■独立アプライアンス型

ウイルスとフィッシングメールの駆除機能がアプライアンス製品として提供されているタイプ。スパムメールの分別やメールアーカイブなど、メールサーバ以外の電子メールセキュリティ機能と一体化している場合もある。

既存のメール環境に付加する形で導入するため、管理者の手間は少なく済む。ウイルス対策機能としてどのウイルス検出エンジンが搭載されているかなど、機能や価格で製品を選ぶとよいだろう。



企業内犯罪を防ぐには？

電子メールの監査とアーカイブ

「日本版SOX法」に対応するには、業務プロセスを記録として残す必要がある。これに対応し、電子メールのやりとりをすべて保存するアプライアンスや、メッセージ内に特定の語句がある場合には上長の許可がなければ送信できないメール監査のソフトウェアが登場している。どのような製品がサービスがあり、特徴があるのか見ていこう。



メール監査の必要性

電子メールのセキュリティではウイルスやスパムメールへの対策が話題になることが多い。しかし最近では、情報漏えい対策や企業の内部統制を強化する目的での製品やサービスも増えてきた。

情報漏えいというと、最近ではWinnyユーザーがウイルスに感染して漏えいするケースが取り上げられているが、電子メールで意図的に漏えいするケースもある。そこで、電子メールのやりとりを監視し、あらかじめ設定したキーワードが含まれていたら管理者が一時的に送受信を差し止めるのが「メール監査」機能である。

メール監査には、メールサーバと同じ

コンピュータにソフトウェアをインストールしたり、メールサーバとインターネットとの接続点の間にゲートウェイとして設置するタイプがある。いずれの場合でも、SMTPのゲートウェイとしてメッセージの内容を検査し、特定のキーワードが含まれている場合は差出人ではなく監査担当者に送信される。そして監査対象のメッセージは、担当者によって送受信を許可するか破棄するかが判断される。

一方、メールアドレスの情報漏えいのみを防止する技術もある。サポート部門など、顧客のメールアドレスを大量に扱う部門の場合、いちどの情報流出で膨大な数のメールアドレスが流出しかねない。であれば、インプルーブシステムの「PMX」のように、始めから顧客のメールアドレスを担当者の目に触れさせなければよい、という考え方もある。このPMXは、SMTPゲートウェイとしてメッセージを監視し、顧客のメールアドレスを無意味なアドレスに変換することで、メールアドレスの価値をなくしてしまう。

たとえば顧客である山田さんがyamada@example.comというメールアドレスからNMAG商事のサポート担当者にメッセージを送信したとしよう。このとき、顧客のメールアドレスはPMXを経由する際にf0e1d2c3b4a5@pmx.nmag.jpのようなメールアドレスに変換され、担当者に届く。担当者がf0e1d2c3b4a5@pmx.

nmag.jp宛てに返信すると、PMXが元のメールアドレスに変換、山田さんにメッセージが届く仕組みである。

監査を発展させたアーカイブ機能

どんなに監査をしても情報が漏えいしてしまうことはあり得る。実際に情報が漏えいしたとき、漏えいしたと思われる時期にどのようなメッセージがやりとりされていたかを知るには、すべてのメッセージを保存しておくしかない。こうした機能を「メールアーカイブ」と呼ぶ。

メールアーカイブには企業でやりとりされるメッセージをすべて保存できるような膨大なハードディスク容量が必要だ。そのため、数年前まで、一般企業ではそこまで巨大な容量を持つハードディスクをメールアーカイブ用に持つことは現実的ではなかった。しかし最近では大容量ハードディスクの価格も安くなり、電子メールのすべてのやりとりを数カ月分、数年分記録できるようになった。

メールアーカイブには、特定のメッセージを必要ときに瞬時に取り出せるような検索機能が必須である。ただ、こうした点はどのメールアーカイブ（製品、サービス）でもほとんど違いはない。高速な検索を売りにする製品もあるが、メール監査はしばしば必要になる機能ではないから、製品選びの基準にはならないだろう。



画面1 ●PMXのアドレス変換設定
「プライバシーメールアドレス」と呼ばれる社内参照用のアドレスと実メールアドレスの対応を管理しているところ