

安心を、ひとつ上のステージへ。



Webからの脅威 課題と解決策

課題と解決策 

Webからの脅威

トレンドマイクロホワイトペーパー | 2007年2月



目次

要旨	3
はじめに	3
望ましくないシナリオ	3
背景	4
Webからの脅威の定義	4
Webからの脅威の形態	5
高度な手法	5
Webからの脅威の程度と影響	5
従来の対策ではWebからの脅威への防御は不可能	8
必要とされる新たなアプローチ: マルチレイヤーの統合的な防御	8
インターネット	9
インターネットゲートウェイ	10
エンドポイント	11
フィードスルーとループバック	11
メールセキュリティへのアプローチの拡大	12
トレンドマイクロの戦略	13
まとめ	14
参考資料	14

要旨

昨今、インターネット上の犯罪は、盗んだ機密情報を横流しして儲けるための、悪質な活動の媒体としてWebを利用するようになってきています。こうしたことから増えているWebからの脅威は、複数の技法を併用していること、数多くの亜種を生み出していること、および攻撃対象を特定し地域に特化していることを特徴とし、個人情報の流出、業務上の機密情報の漏えい、ブランド名の失墜、Webによる商取引に対する消費者への信頼の低下といったさまざまな負のリスクをはらんでいます。さらにWeb利用が進む中、Webからの脅威が複雑になってくると、個人情報や業務上の機密情報の保護は、この10年間でおそらくこれまで以上に大きな課題となるでしょう。従来対策では、これらの脅威に対する十分な防御は望めません。また単独の手法や技術ではこの状況を改善することはできません。むしろ、複数の技法を組み合わせ、マルチレイヤーの包括的な方法で対処する必要があります。本ホワイトペーパーでは、Webからの脅威の仕組みと影響について説明し、従来対策でこれらの脅威を撃退できない理由を明らかにするとともに、必要となる新しいアプローチの特徴について解説します。

はじめに

㊦ 望ましくないシナリオ

大手医薬品会社に勤める弁護士、ロバートは、月曜の朝オフィスに到着すると、コンピュータにログオンし、いつものようにまず新着メールをチェックします。ロバートはバスケットボールのファンで、前の晩、テレビで試合を見ていました。昨夜の試合のことをなんとなく思い出しながら、ロバートは友人からの短いメールに目を留めます。メールには、彼のお気に入り選手の1人に関する情報を掲載した新しいWebサイトへのリンクが含まれています。ロバートはさっそくリンクをクリックし、お気に入り選手の画像や動画などの情報が含まれている魅力的なサイトにアクセスします。この作業の裏でロバートが気づかないうちに、画像の1つがブラウザで表示される際、jpgファイルに含まれた不正コードによって、実行可能ファイルをダウンロードするコマンドが発行され、コンピュータ上でそのファイルが自動的に実行されているのです。その後、この不正プログラムはロバートのハードディスクに保管されている事前に定義されたファイルを取り込んで、圧縮および暗号化し、第三者のメールアドレスに送信します。第三者とは、つまりインターネット上の犯罪者です。これらのファイルのいくつかには、ロバートが担当している何件かの特許訴訟に関する、非常に機密性の高い情報が含まれています。インターネット上の犯罪者は、医薬品業界を標的にし、さまざまな医薬品企業の従業員に同様のメールを配信することによって、こうした情報を手に入れ、その後売りさばいて利益を得ようとしているのです。このように、一見害のなさそうなWebサイトへのリンクをクリックすることによって、ロバートは知らぬ間に、自社の機密情報を犯罪者に流すプロセスを自ら実行してしまいました。これが原因で、彼の会社は競争性の高い特許権の喪失や法的トラブルの発生などの損失をこうむる恐れがあります。

同じ日の朝、同じ医薬品会社のIT管理者の1人がネットワークトラフィックを監視しています。同社では、最近、リストを使用したURLフィルタリングを使用して、クライアントベースのウイルス対策を補完したため、管理者は安心して画面を見ています。異常な活動は何も起こっていないようです。ロバートのコンピュータで実行された不正プログラムのダウンロードと機密ファイルの流出が検出されなかったことには、いくつかの理由があり、これには今日のインターネット上の犯罪で行われている一般的な手口が関係しています。第1に、不正プログラムの作成者が用意した不正コンテンツ入りのWebサイトは、当日の朝構築されたばかりの新しいサイトだったため、URLフィルタリングソフトウェアのサイトリストには含まれていません。第2に、ネットワークトラフィックが急増して管理者に気づかれることがないよう、ファイルのエクスポートを時間をかけて実行する命令が不正プログラムに組み込まれていました。この医薬品会社では、ゲートウェイに動作分析を行うソフトウェアをインストールしていなかったため、ロバートのコンピュータから流出した添付ファイル付きのメールは通常のメールと同様に処理されてしまいました。

不幸にも、世界中の大企業、中小企業でこのようなシナリオが展開されています。いわゆる「Webからの脅威」の数が増加するにつれ、上記のような展開となり、さらに無数の亜種が生まれると、大混乱を引き起こす可能性があります。インターネット上の犯罪により、健康保険管理会社からは社会保険番号のリスト、金融機関からはクレジットカード番号、技術を取り扱う企業から機密情報が流出しています。こうした犯罪は、個人情報の流出だけでなく、プライバシー保護能力に対する消費者の信頼を失わせ、さらにはオンラインバンキング、オンライン取引、およびeコマースの基盤を揺るがします。

背景

過去15年間、情報セキュリティ上の脅威は進化を繰り返し、その姿を変化させています。当初、ダウンロードされた実行可能ファイルに埋め込まれていたウイルスは、文書ファイルに含まれるマクロウイルスという形態になり、さらにその数年後には、メールによって配信される脅威（「I Love You」ウイルスや「Melissa」ウイルスなど）という形態をとるようになりました。いずれの場合においても、不正プログラムの作成者は、最も広く使用され、最も防御機能の弱い媒体を探し出しました。不正プログラムでは、ユーザに幅広く利用されているメールが媒体として悪用されていますが、この種の攻撃への防御の必要性が広く認識されるようになるにつれて、防御機能が強化され、最近では、新しい配信手段としてWebを使用する脅威が台頭しています。

これまでの脅威の進化と同じように、Webからの脅威は、その媒体であるWebの利用がこれまでになく活発になり、Webが商取引の主要な牽引力となって成長し続けると同時に、その勢いを増しています。大半の会社員はデスクトップでまずブラウザを開いてから仕事を始めます。MyspaceやYouTubeなどのサイト利用が社会現象化していること、インターネットユーザ行動の地域化は、Web利用を広げる重要な要因となっています。

また、不正プログラムの配信手段として、Webはメッセージングなどと比べると、防御がそれほど強固ではありません。IDCの調査では、スタッフ500人以上の企業のうち、ネットサーフィンによってウイルスに感染したことがある企業は30%を上回るのに対し、これらの企業のうちメールを介してウイルスやワームに感染したことがある企業は20%~25%に過ぎないことが判明しています。[1]

Webからの保護が難しいのは、データストリームの検索やフィルタに必要な帯域幅がメールよりはるかに広いからです。メールに含まれるデータはWebのデータの1/1000以下に過ぎません。たとえばクライアントコンピュータにインストールされている従来のウイルス対策ソフトウェアは、さまざまな脅威からクライアントコンピュータを防御するためにはきわめて重要ですが、進化するWebからの脅威群に対しては十分な防御とはなりません。こうした状況は、Webからの脅威にとって「絶好の攻撃対象」となります。それは、業務上不可欠な媒体を、比較的防御が弱いにもかかわらず、広範かつ継続的に使用しているからです。いうなれば、今日の情報セキュリティは、きわめて重大なターニングポイントに立たされているのです。最新クラスの脅威に対処する新たなアプローチが必要となります。

Webからの脅威の定義

Webからの脅威にはインターネットで発生するあらゆる脅威が含まれます。Webからの脅威では、単独のファイルやアプローチではなく、さまざまなファイルや技法を組み合わせることにより、きわめて高度な技術が使用されます。たとえば、Webからの脅威の作成者は、使用するプログラムのバージョンや亜種を絶えず変更します。Webからの脅威は、感染したユーザのコンピュータ上ではなく、Webサイトの一定の場所に保存されているため、検出されないようにプログラムのコードが頻繁に変更されます。

かつてハッカー、ウイルス作成者、スパムメール送信者、スパイウェア作成者などと称された不正ユーザは、近年ではまとめてインターネット犯罪者と呼ばれています。こうした犯罪では、主に金銭目的でWebからの脅威を広げます。その方法は、ユーザを対象のWebページに誘い込んだ後、さまざまなステルス技術を駆使してコンピュータやWeb上に潜伏することによって感染を広げる、というものです。不正コードがひとたびユーザのコンピュータに侵入すると、気づかれないようゆっくりとユーザのファイルを盗み、CPUの処理能力を低下させます。

従来の対策のままでは、Webからの脅威にとって「絶好の攻撃対象」となります。それは、業務上不可欠な媒体を、比較的防御が弱いにもかかわらず、広範かつ継続的に使用しているからです。

② Webからの脅威の形態

次に、脅威のグループ例を、脅威のライフサイクルのさまざまな段階に分けて示します。

- Webリンクが配信される手段
 - スпамメール、フィッシング攻撃メール、「手っ取り早く儲かる」を歌い文句にした悪徳商法メールなど、URLリンクによってユーザを悪質なサイトに誘い込むよう対象を特定したメール。
 - ファーミングによって感染したドメインネームサーバ (DNS) や欠陥のあるWebサイト。情報を盗み取ったり、ユーザのシステムを感染させたりする目的で不正なWebサイト (正規のサイトではなく) やプロキシサーバにリダイレクトします。
 - ユーザのシステムをウイルスに感染させようとするソーシャルネットワーキングサイトなど。
- Webサイトで実行される処理
 - ブラウザでメディアファイル (イメージ、アニメーション、ビデオ、オーディオなどのファイル) が表示される際に、そのファイルに組み込まれた不正コードによって不正ファイルがダウンロードされたりします。
 - ActiveXコントロールや自動的なダウンロードによって、ユーザが表示を続行しようとするときにダウンロードが強制されたり、パッチ未適用のブラウザを使用している場合に不正ファイルが自動的に送込まれたりします。
- 感染ルーチン
 - システムに不正ファイルを取り込むアプリケーションによって感染します。
 - 従来の検索機能によって検出されないよう、潜伏する不正プログラムが、Web上で複数のコードセットのアップデートをダウンロードすることによって、頻繁に自己アップデートを繰り返します。
- 感染後のペイロード
 - スパイウェアまたはアプリケーションによってシステムからデータや情報が流出し、第三者に送信されます。
 - アドウェア、データマイナ、またはポップアップによって、営利活動サイトに誘導します。
 - ブラウザヘルパーオブジェクトによって、検索エンジンの結果を悪用したり、ユーザの関心事 (商品またはサービスなど) に関する情報を収集してマーケティング広告を送りつける目的でユーザのWeb閲覧傾向を監視したりします。
 - ボット (リモート制御によって不正な処理を実行できるコード) やゾンビ (ウイルスに感染したコンピュータ) がWebからコマンドを受信します。

③ 高度な手法

Webからの脅威は、通常、http80番ポートを悪用します。このポートは、従業員がWebを通じて、情報へのアクセス、通信、および業務活動ができるように、ほとんど開かれたままの状態になっているポートです。(前述の例は、このアプローチを示しています)。

Webからの脅威の亜種は、これまでの数多くの不正プログラムで用いられたアプローチとは異なり、地域または局所レベルでの攻撃に対象を特定します (たとえば、特定のレイヤーを攻撃対象とするために現地語サイトを使用するなど)。また、不正プログラムの作成者は、レジャー、人気タレント、スポーツ、ポルノ、世界の出来事などの話題に関連する魅力的な件名をメールに付けるなどのテクニックを使用します (メールにはたいてい、不正コードがダウンロードされるサイトのURLが含まれています)。

Webからの脅威の程度と影響

次の2つのどちらかの目的で、Webからの脅威がインターネット上の犯罪で活用されています。1つは、情報を盗み、転売することです。この脅威がもたらすリスクは、主に、個人情報の流出という形での機密情報の漏えい、または感染システムを媒介として使用したフィッシングなどの、情報収集プログラムの配信などです。その結果、Web上での商取引の信頼性を損い、インターネット取引に欠かせない信用を低下させる可能性があります。もう1つの目的は、感染したユーザのCPUの処理を占有し、金銭目的の活動 (スパムメールの送信、サービス妨害攻撃やクリック課金操作による不正行為など) を実行するためのツールとして使用することです。

課題と解決策: Webからの脅威

さまざまなWebからの脅威によって得られる利益は莫大なものになります。たとえば、Jeanson James Anchetalaは、400,000台のPCのボットネットを管理することによって60,000USドルを稼ぎました [2]。Ivan Maksakov、Alexander Petrov、およびDenis Stepanovは、英国のスポーツブックメーカーにサービス妨害攻撃を仕掛けて、400万USドルを脅し取りました [3]。このような不正プログラムの闇市場では、たとえば、オンラインアカウント情報を盗むことができるトロイの木馬が通常1,000~5,000USドルで取引されています [4]。しかし、こうした地下組織の活動でどれほどの利益があるのかは、闇取引というその性質上、ほとんど分かっていません。

それでも、これまでに特定のタイプのWebベースの脅威がもたらす被害を金銭的に示すデータがいくつか収集されています。たとえば、Consumer Reports USAは、フィッシング被害に遭ったアメリカ国民の被害額は2005年には6億3,000万USドルに上ったと報告しています [5]。ユーザ名とパスワードの他に取引認証番号 (Transaction Authentication Number: TAN) を使用しているにもかかわらず、ドイツのさまざまな銀行の顧客がフィッシングの被害に遭っています。ミュンヘン警察の概算では、2006年の1月~6月のオンライン詐欺による被害がミュンヘンだけで100万ユーロを超えています [6]。Asia.Internetの記事によれば、Gartner Groupは2006年のフィッシング攻撃の被害合計額は、280億ドルに上ったと報告しています [7]。

図1および図2は、あらゆるタイプのWebからの脅威の被害推定を示したものです。また、Webからの脅威は、全体的に増加傾向にあることもわかっています (図3参照)。Standard Bankは、過去18ヶ月でスパイウェアは50%増加し、過去3年間でウィルスの作成件数は16倍になったと推定しています [8]。ある調査では、フィッシング犯罪で使用される偽のメールの14%が、たった24時間で目的を遂行する可能性があることが報告されています。この比率は、ネットワークセキュリティ専門家による以前の推定値よりはるかに高くなっています [9]。

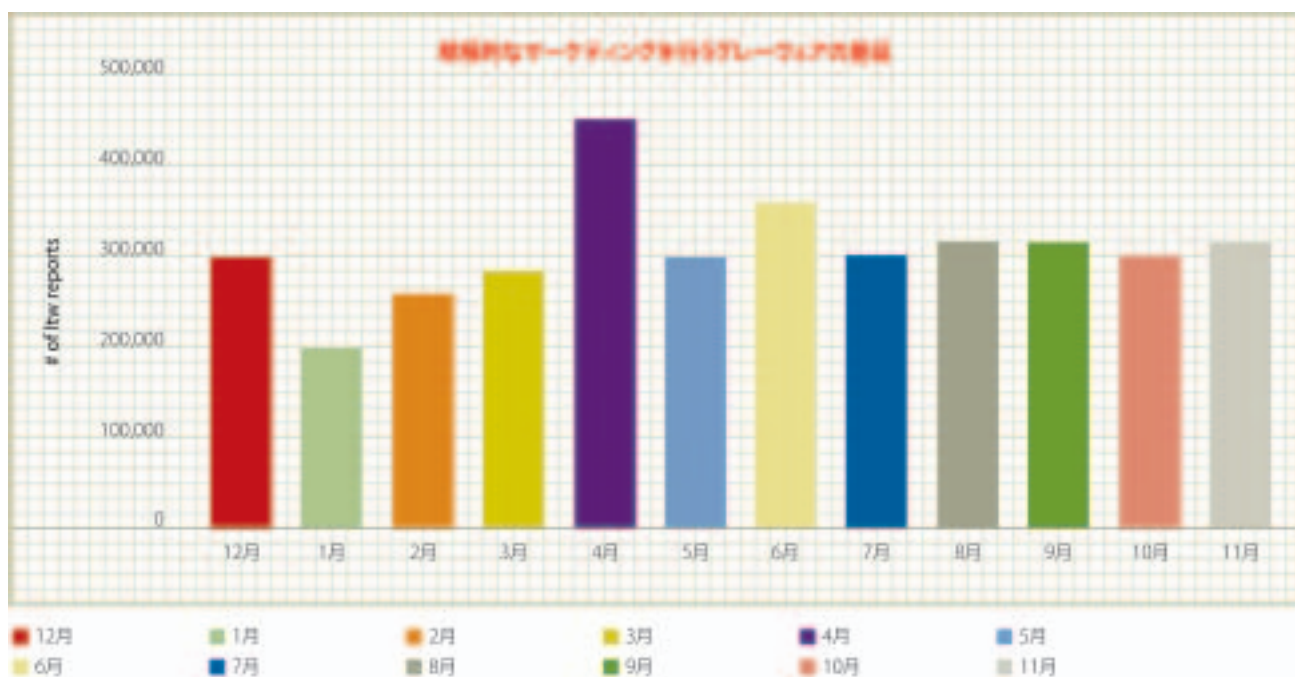


図1. グレーウェアは2006年に著しく増加しました。グレーウェアは悪質なものとはみなされていませんが、トレンドマイクロでは、クリック操作による収益創出の手段として不正プログラムを使用する動向を踏まえ、この増加を問題視しています。

出典:トレンドマイクロ

課題と解決策: Webからの脅威



図2. 2006年には、クライムウェア（金融犯罪を自動化することを目的とした不正ソフトウェア）が著しく増加しました。
出典: トレンドマイクロ

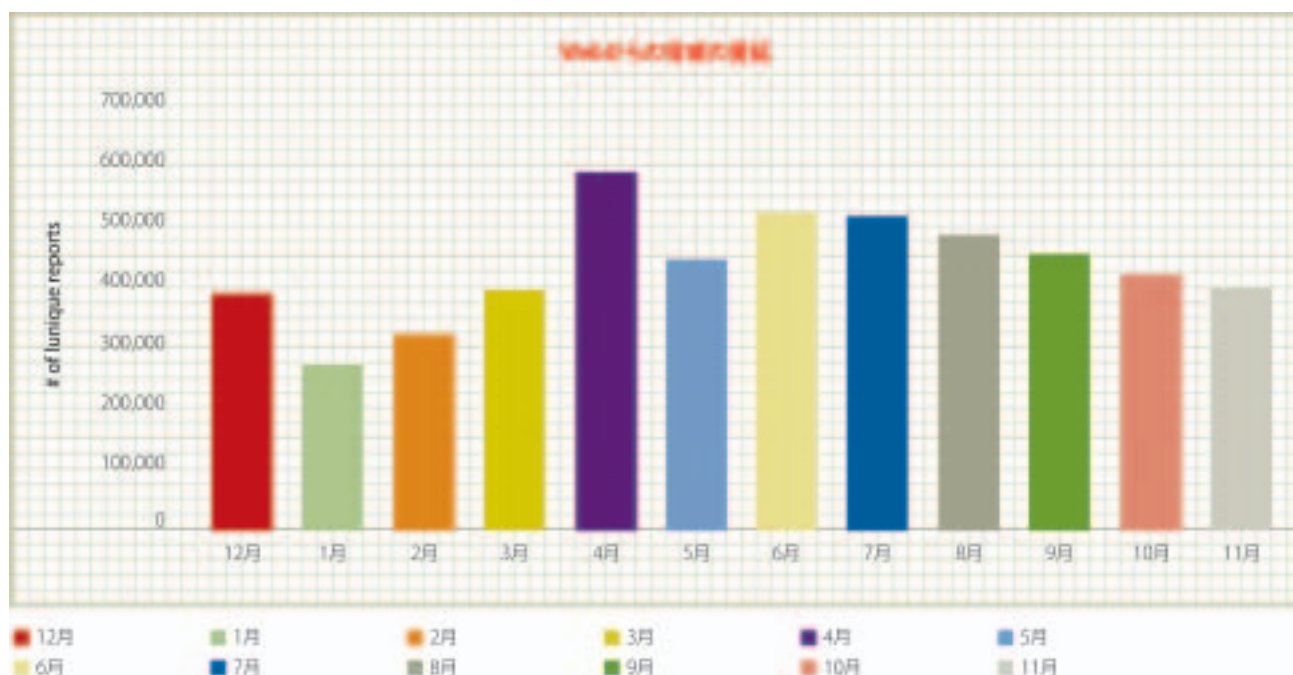


図3. 不正プログラムの配信手段として、メールの次に広く使用されているのはWebです。
出典: トレンドマイクロ

従来の対策ではWebからの脅威への防御は不可能

従来のウイルス防御策は、ウイルスのサンプルを収集してパターンファイルを開発し、そのパターンファイルをユーザにいち早く配信するというものです。しかし、さまざまな理由から、Webからの脅威に対処するにはこの方法では不十分であると考えられます。

たとえば、Webからの脅威の多くは攻撃対象を特定しており、多くの亜種が存在するため、サンプルの収集はほとんど不可能です。数多くの亜種で、スパムメール、インスタントメッセージング、Webサイトなどの複数の配信手段が使用されており、従来のサンプル収集およびパターンファイル作成プロセスでは対処できません。Webからの脅威は、攻撃対象を特定した局所的/地域的な攻撃や、局所的/地域的な言語のスパムメール、Webサイトなどのさまざまな戦術を使用するため、1つのソリューションですべての脅威に対応することはできません。たとえば、攻撃対象が特定された局所的な攻撃用に収集したサンプルは別の局所的攻撃には有効ではありません。

基本的に、Webからの脅威の目的は、拡散することではなく潜伏することなので、従来のウイルス対策の技法では検出が困難です。場合によっては、Webからの脅威が、システムファイルを置換するルートキットを使用する事で非常に広範なシステム感染を引き起こし、従来のアンインストールやシステムクリーンアップアプローチでは役に立たないことがあります。大抵このような場合には、ハードディスクをクリーンにして、OS、アプリケーション、およびユーザデータを再インストールする全面的な復旧処理が必要になります。また、インターネットの犯罪では、正規のトラフィック用に開いた状態にする必要があるポート80を悪用して、既存のクライアントファイアウォールを迂回します。さらに、本格的なインターネットの犯罪では、脆弱点の公開前の脆弱性につけこみます。この場合、リリースされたセキュリティパッチをすぐに適用しても脅威の影響を防御できません。

さらに、金銭目的のインターネットの犯罪では、(ダウンロードソースを配信するなどの目的で) WindowsのWebサーバプラットフォームだけでなく、他のプラットフォームも攻撃対象にします。事実、Webからの脅威はOSには依存せず、あらゆる種類のWebサーバを攻撃対象にします。つまり、LinuxベースのWebサーバも、セキュリティの脅威に脆弱なことが分かれば、攻撃を仕かけられることになります。いったん不正プログラムがインストールされると、引き続きそのプログラムによってホストベースの侵入予防システム (Host Intrusion Prevention System: HIPS) のルールに違反する別のプログラムが起動されます。そして、おびただしい数の偽のアラームが生成されるため、ユーザは煩わしさからついに保護機能を無効にし、不正プログラムを実行可能にしてしまいます。こうして、不正プログラムは従来のHIPS技法をかわします。

Webからの脅威の一部として広く使用されている個々のダウンロードプログラムは、単独では「無害」に見えます。しかし、脅威の他の部分と合わせると悪質なものとなり、ファイルベースのヒューリスティック検索で誤検出になったり、検索機能が役に立たなくなったりします。Webからの脅威はしばしばこの技法を拡張して、複数のプロトコルを組み合わせたマルチレイヤーの攻撃を実行し、従来の方法による検出の網をすり抜けます。たとえば、インターネット上の犯罪では、WebメールやインスタントメッセージにURLが組み込まれています。ユーザはこのURLのリンクをクリックします。このURLは正規のWebサイトですが、数日間ないし数時間、インターネット上の犯罪者によってハイジャックされたものでした。そして、ActiveXコントロールによって、ユーザのブラウザの脆弱性がテストされます。脆弱性が検出されると、不正プログラムが攻撃を行います。脆弱性が検出されなければ、不正プログラムによってファイルがダウンロードされ、脆弱性がテストされ、さらに別のファイルがダウンロードされる、というように処理が続行されます。トラフィックの個々のセッションは悪質なものには見えませんが、個々の活動を組み合わせると、連携した攻撃になります。

必要とされる新たなアプローチ: マルチレイヤーの統合的な防御

Webからの脅威に対処するためには、既存の技法を補うような新たなアプローチが必要なのは明らかです。最も有効なアプローチは、複数の防御レイヤーを導入して、一連の防御策を適用することです。また、脅威の進化性という性質をふまえ、なんらかのフィードバックを行うことにより、防御システムの中で収集した情報に基づいて他のレイヤーで情報をアップデートする必要があります。さらに、Webからの脅威は関連するすべてのプロトコルを活用できるため、有効なアプローチのどれについても、これらすべてのプロトコルに対応しなければなりません。こうした対策を組み合わせるには、なんらかの効率的な一元管理を行う必要があります。

課題と解決策: Webからの脅威

Webからの脅威に有効に対処するために重要なのは、マルチレイヤーのアプローチを導入することです。このアプローチでは、異なる3つのレイヤー、つまり1) インターネット (トラフィックがインターネットゲートウェイに到達する前)、2) インターネットゲートウェイ、3) エンドポイント (クライアント) の各レイヤーで対策を講じます (図4を参照)。Webからの脅威は、たいてい、開始点となるWebリンクの配信手段としてメールを使用します。そのため、Web上のリンクをインターネット上で遮断することで、ゲートウェイに到達するメールトラフィックを削減し、帯域幅を解放し、処理容量を節約し、法令基準を順守するために必要なメールや他の情報の保管とアーカイブを削減し、その結果、費用対効果が向上します。

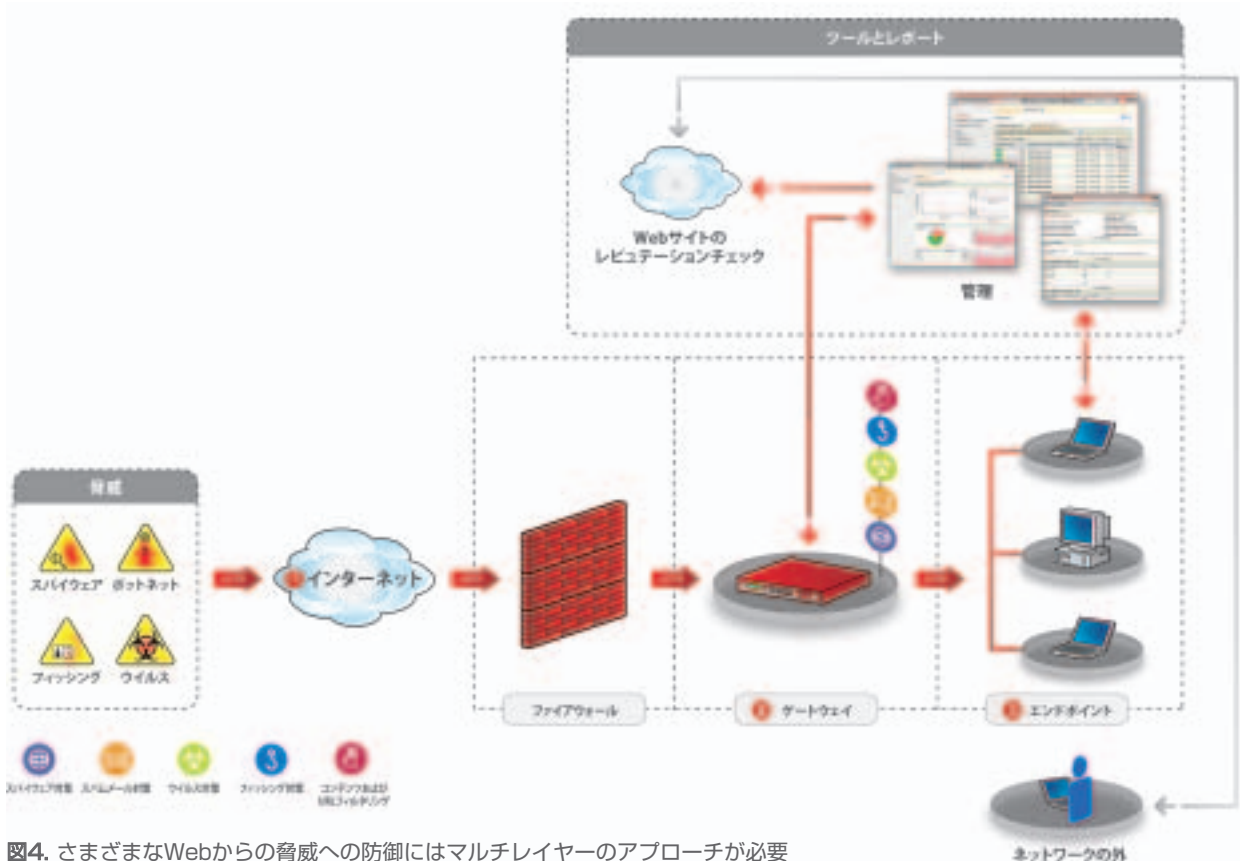


図4. さまざまなWebからの脅威への防御にはマルチレイヤーのアプローチが必要

④ インターネット

このレベルでの主な機能は、ユーザが各Webサイトにアクセスする前にそのサイトの「レピュテーション」をチェックすることです。これは、金融取引を始める前に「信用調査」をするのに似ています。Webレピュテーションのチェックでは、URLフィルタリングデータベースが使用されますが、毎日およそ5,000の新しいドメインが追加されるため、これらのサイトの信用情報を補完するような対策がさらに必要になります。こうした対策には、Webサイトのデータの定期的な検索に基づいて作成された「セキュリティ評価」のデータベースと、フィッシングとファームングに関連する既存のURLのデータベースのチェックが含まれます。インターネット上の犯罪では、しばしばサーバのIPアドレスやドメインを変更することによって検出を回避しようとするため、インターネットレベルでの追加対策では、IPアドレスやドメインの示す場所のチェックを実行し、IPアドレスやドメイン、URLを相互に関連付けます。最大限の効率を得るために、トップレベルのすべてのドメイン (URL内の最後のピリオドの右側にある文字 (国コードも含む)) の分析を実行することもお勧めします (図5を参照)。

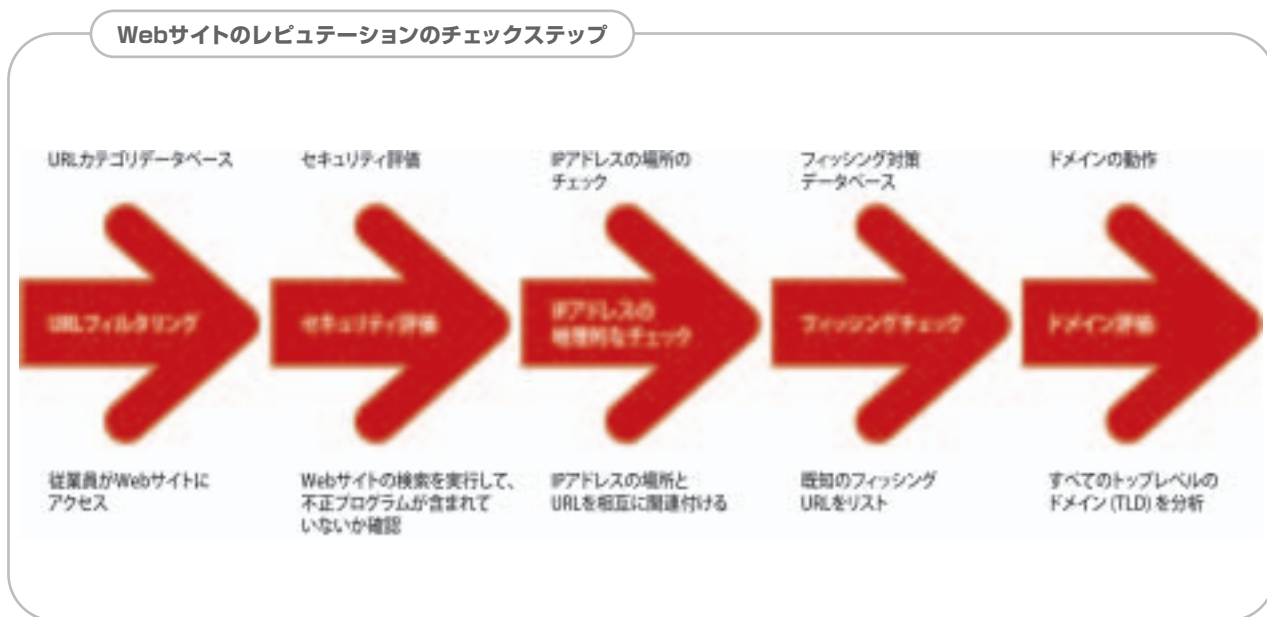


図5. インターネットでは、一連の包括的なステップによって各Webサイトの「レピュテーション」をチェックすることが重要。

③ インターネットゲートウェイ

3つのレベルの2番目であるインターネットゲートウェイでも、重要な機能が必要となります。ソフトウェアまたはハードウェアアプライアンスによって実行されるゲートウェイ機能には、ファイルチェック処理が組み込まれています。このファイルチェック機能では、ユーザによるWebからの各ファイルのダウンロードを許可する前にそのファイルのレピュテーションをチェックします。この処理で、Webサイトの各ファイルデータの検索と、各ファイルの「レピュテーション」の診断が定期的に行われることで、ファイルレピュテーションデータベースの情報が常に新しいものに維持されます。インターネットでのWebレピュテーション機能に加えてこのファイルチェック機能が必要なのは、インターネット上の犯罪では不正コンテンツを含む個々のファイルを1つのWebサイトから別のサイトに簡単に移動できるためです。

ゲートウェイで必要となるWebからの脅威に対する2番目の防御は、何らかの動作分析を実行することで、それによって、活動を組み合わせて関連付けを行い、活動が悪質なものであるかどうか判断する事です。この分析によって、活動の組み合わせごとにスコアを設定し、そのスコアがしきい値を超えた場合はその活動の組み合わせをブロックできます。このアプローチでは、セッションデータやプロトコルプロパティに含まれるトリガを識別し、このトリガを証拠または手がかりにして疑わしい活動を特定できます。さらに、このアプローチでは、定義済みの不正活動の条件に一致するトリガとの相関を示すルールをゲートウェイに実装することができます。

たとえば、このアプローチでは、同じプロトコルでの単一セッションの活動（疑わしい二重拡張子を持つSMTP添付ファイルなど）を相互に関連付けます。また、このアプローチでは、同一プロトコルでの複数のネットワーク接続セッション中に行われる活動（無害に見える個々のファイルであっても、全体的には不正プログラムの一部となるファイルをダウンロードするダウンロードが取り込まれる脅威など）も相互に関連付けます。さらに、複数のセッションと複数の異なるプロトコル（SMTPとHTTPなど）の活動についても相互に関連付け、疑わしい活動の組み合わせ（複数の受信者を宛先とするURLリンク入りのメールと、リンクからダウンロードされたHTTP実行可能ファイルなど）についても相互に関連付けられます。

④ エンドポイント

インターネットとゲートウェイに防御策を導入しても、さらにエンドポイント（クライアント）での第3レベルの防御を忘れてはなりません。近年、アメリカで販売されるコンピュータのおよそ3分の1はノート型コンピュータです [10]。ノート型コンピュータは、ビジターや委託業者によって企業のゲートウェイをまたいで物理的に持ち運ばれ、複数のネットワークに接続されることから、単独での防御強化が必要になります。企業のWebセキュリティポリシーは、ユーザがネットワークの中にいるか外にいるかにかかわらず、常に適用されなければなりません。そのため、クライアントレベルの防御（アクセス制御や検索など）と、感染時の駆除処理および復旧処理を行うソリューションが必要になります。たとえば、ノート型コンピュータがどこかでウイルスに感染し、ボットネットの一部と化している場合、そのコンピュータはボット管理者（ボットネットの構築者）に接続しようとしています。また、それとは別に、「phone-home」機能（感染したホストから取り込んだ情報をスパイウェアの所有者に定期的を送信しようとする機能）を実行するスパイウェアもあります。いずれの場合も、この種の活動を検出してブロックし、必要に応じてクリーンアップ処理を指示することができます。

クリーンアップ機能では、エージェントベースの駆除処理と非エージェントベースの駆除処理の2つが想定されます。エージェントベースの駆除処理では、集中管理されたエージェントがノート型コンピュータに常駐し、活動を調整します。非エージェントベースの駆除処理は、ビジターまたは委託業者のノート型コンピュータにエージェントがインストールされていない状況に適用されます。この場合、駆除処理は、ネットワークへのアクセス制御により、オンデマンドで実行されます（つまり、駆除処理の際はネットワークへのアクセスを許可）。ルートキットの感染などが原因でクリーンアップが実行不可能な場合は、全体的な復旧処理も必要になります。

④ フィードスルーとループバック

図6は、マルチレイヤーアプローチを説明し、この実装で重要な機能の要素を示しています。インターネット、ゲートウェイ、およびエンドポイントにおける防御レイヤーの導入では、「フィードスルー」メカニズムが採用されています。また、レイヤー間の情報のフィードバックでは、「ループバック」メカニズムが採用されています。たとえば、ゲートウェイの動作分析機能で学習した情報をループバックして、Webレピュテーションデータベースとエンドポイント機能をアップデートすることができます。同様に、エンドポイントで学習した情報をゲートウェイのファイル検索機能とインターネットのWebレピュテーション機能にループバックできます。十分な防御を継続的に維持するためには、フィードスルー技法とループバック技法の両方が必要になります。

これらの機能および関連ポリシーのすべてを集中コンソールから監視し、管理する必要があります。同時に、世界の特定の地域を専門とする各チームが、それぞれの地域に対象を特定した対策を講じる必要があります。これらのチームは、Webからの脅威に対抗するため、情報収集、サンプル収集、脅威の削減および予防策、地元のセキュリティグループや司法当局との連携など、最前線で活躍しなければなりません。このアプローチにより、脅威への迅速な対応、カスタマイズされたソリューション提供の実現が可能になるでしょう。

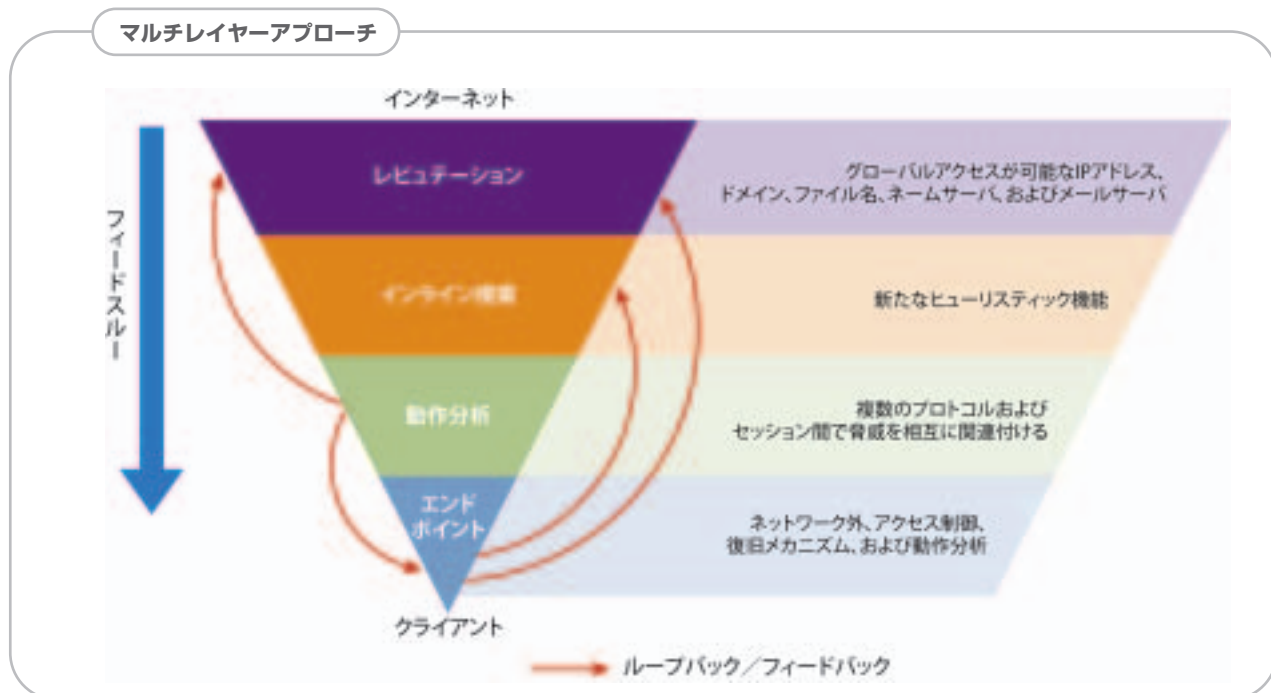


図6. フィードスルー機能（上から下へ）とフィードバック機能（矢印）によって、インターネットで始まり、ゲートウェイ、ネットワーク、エンドポイントで受け継がれるマルチレイヤーアプローチが完成します。

メールセキュリティへのアプローチの拡大

このマルチレイヤーアプローチは、メールセキュリティにまで拡大することができます。現状では、法令基準によって10年間メールの保護が義務付けられることから、メッセージング領域でのインターネットからの積極的な防御が重要になります。インターネットでメールを事前にフィルタ処理することで、帯域幅の使用を節約し、保管や保守にかかる経費も削減され、防御を後押しします。このレイヤーでの防御は、メール送信元IPアドレスのレピュテーションチェック、ドメイン (IPアドレス) のレピュテーションチェック、メールのファイアウォール、およびスパムメール/ウイルス対策用のフィルタリングを含みます。メールファイアウォールのホストは、メールサーバの外部に配置し、サービス妨害攻撃やディレクトリハーベスト攻撃 (有効なメールアドレスをランダムに検索する攻撃) の配信をブロックするようにします。

インターネットゲートウェイでは、スパムメール対策およびウイルス対策ソフトウェアに添付ファイル検索機能を組み込むことによって、識別が困難な、ポットが生成する比較的新しい形式のスパムメールである添付ファイル付きスパムメールを検出するようにします。この種のスパムメールは、画像を使用してスパムメッセージを隠し、保存領域を消費したり、通常不正プログラムを含んでいます。このレベルでは、またメールサーバからLDAPなどのディレクトリに接続するポリシーエンジンも必要でしょう。ここでは、例えば動作分析テクノロジーを使用して、繰り返し送信されるメールにユーザがまったく返信しないことを検出し、そのメールをスパムメールとして分類して送り返すことができるようにします。メールコンテンツの検索を実行して、従業員やその他の関係者が不正な第三者にメールや添付ファイルによって自社の機密情報を漏らしていないか確認することもできます。そのためには、送信メールの暗号化と、法令基準を順守するためのメールのアーカイブ化が求められるでしょう。

課題と解決策: Webからの脅威

メッセージング環境の場合、メールボックスがメールサーバ上に存在するため、第3レベル（エンドポイントレベル）はメールサーバ自体になります。そのためメールサーバでセキュリティソフトウェアを実行する必要があります。またスパムメールが送られる隔離メールボックスなどのユーティリティをエンドユーザが管理できる必要があるでしょう。こうしたことは、内部メッセージングにおける脅威に対処するためには重要です。

メールとWebからの脅威は結びついており、これら2つの間でフィードバックを行い、これらすべての脅威に対してネットワークを集中管理できるソリューションが必要でしょう（図7を参照）。IT管理者は不正プログラムのネットワークへの侵入方法を認識する必要があります。防御を必要とするその他の媒体として、インスタンスメッセージングツールやコラボレーションツールがあります。

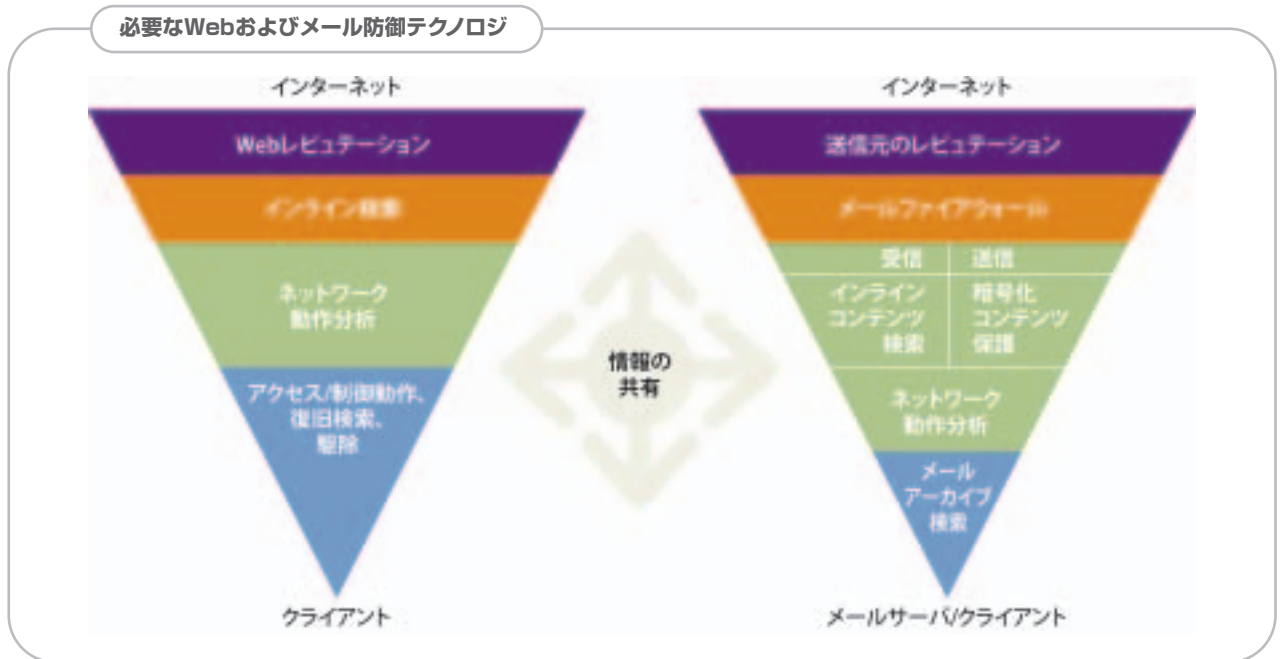


図7.トレンドマイクロでは、Webおよびメール防御技術間でフィードバックをお互いに供給し、これらすべての脅威に対してネットワークを集中管理できるソリューションをお勧めします。

トレンドマイクロの戦略

トレンドマイクロが提供するWebからの脅威への防御戦略には、あらゆるWebからの脅威から防御するマルチレイヤーの総合ソリューションです。インターネットでは、Webレピュテーションを提供します。インターネットゲートウェイでは、InterScan Web Security SuiteやInterScan Gateway Security Applianceなど、ソフトウェアおよびハードウェアベースのソリューションでファイルチェックと動作分析を行い、不正な活動を相互に関連付けます。エンドポイントでは、ウイルスバスター コーポレートエディションがアクセス制御と検索を実行します。

さらに、ダメージクリーンナップサービスを提供するとともに、Trend Micro Control Managerを使用した集中管理機能を提供しています。これらの機能は、大企業、中小企業、および個人ユーザのそれぞれに適した形態で提供されます。

また、トレンドラボは、世界7箇所、800人を超える専任エンジニアから構成され、24時間365日体制でWebの脅威からユーザを防御するためのウイルス解析/サポートセンターです。

また、トレンドマイクロでは、ITリソースが限られた中小企業向けに、Webからの脅威やその他の新たな脅威から防御するためのオールインワンの総合防御機能を備える「Worry-Free」セキュリティソリューションを提供しています。

まとめ

今日、Webからの脅威はその数を増し、その影響も拡大しています。複雑で、多数の亜種が存在し、複数の媒体を使用し、さらに今日最も広く使用されているインターネット、Webを利用するというその性質から、Webからの脅威は、企業、および個人ユーザにとって、まれに見る最も困難な脅威となっています。Webからの脅威がもたらす弊害は、機密情報の漏えい、それによるブランド名の失墜、および法令基準への影響に加え、機密情報の競合他社への流出による損失が想定されます。従来のアプローチではWebからの脅威への対策は不十分なことから、現在、情報セキュリティは重大な岐路に立たされています。規模の大小を問わず、あらゆる企業は、マルチレイヤーの総合アプローチによってソリューションを配置し、Webからの脅威に対して十分な防御体制をとる必要に迫られています。

参考資料

1. IDC, press release, July 18, 2006, "Private Internet Use by Staff Threatens IT Security in Danish Companies, Says IDC," http://www.idc.com/getdoc.jsp?containerId=pr2006_07_14_125434.
2. Gregg Keizer, TechWeb Technology News, January 24, 2006, "Botnet Creator Pleads Guilty, Faces 25 Years," <http://www.techweb.com/wire/security/177103378>
3. Marius Oiaga, Softpedia, October 4, 2006, "Hacking Russian Trio Gets 24 Years in Prison," <http://news.softpedia.com/news/Hacking-Russian-Trio-Gets-24-Years-in-Prison-37149.shtml>.
4. Byron Acohido and Jon Swartz, USA TODAY "Cybercrime flourishes in online hacker forums," October 11, 2006, http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hacker-forums_x.htm
5. Consumer Reports, "Don't bite at phishers' e-mail bait," September 2006, http://www.consumerreports.org/cro/personal-finance/news/september-2006/dont-bite-at-phishers-e-mail-bait-9-06/overview/0609_dont-bite-at-phishers-email-bait_ov.htm.
6. Police of the City of Munich, August 25, 2006, <http://www.sueddeutsche.de/tt3m3/muenchen/artikel/612/83529/>
7. "Scammers Hooking Bigger Phish," Asia.Internet, November 9, 2006, <http://asia.internet.com/news/article.php/3642971>.
8. Herman Singh, Standard Bank, "Next Generation Internet Fraud and Techniques to Combat This," BMI-T Annual Banking Forum, October 19, 2006, Johannesburg, <http://www.bmi-t.co.za/presentations/bf/links/presentations/Herman%20Singh.pdf>.
9. Markus Jakobsson, Jacob Ratkiewicz, "Designing Ethical Phishing Experiments: A study of (ROT-13) rOnI query features," International World Wide Web Conference Committee, WWW 2006, May 23-26, 2006, Edinburgh, Scotland, ACM 1-59593-323-9/06/0005, http://www.informatics.indiana.edu/markus/papers/ethical_phishing-jakobsson_ratkiewicz_06.pdf.
10. Tom Krazit, Cnet, "Two in three retail PCs are notebooks," December 20, 2006, http://news.com.com/Two+in+three+retail+PCs+are+notebooks/2100-1044_3-6144921.html.

トレンドマイクロは、コンテンツや脅威のセキュリティ対策管理のバイオニアです。同社は1988年に設立され、個人や企業を問わずあらゆる規模のお客さまに対して、セキュリティソフトウェア、ハードウェア、およびサービスを提供し、高く評価されています。東京本社をはじめ、海外には30ヶ所以上の拠点が置かれ、トレンドマイクロのソリューションは、付加価値の高い販売代理店やサービスプロバイダを通じて世界中で販売されています。トレンドマイクロ製品およびサービスに関する詳細および評価資料については、トレンドマイクロのWebサイト (www.trendmicro.co.jp) へアクセスしてください。

トレンドマイクロ株式会社

東京本社:

〒151-0053 東京都渋谷区代々木
2-1-1 新宿メインタワー
TEL.03-5334-3601 (営業代表)
FAX.03-5334-3639

大阪営業所:

〒541-0059 大阪府大阪市中央区
博労町3-5-1エブソン大阪ビル7F
TEL.06-6258-8091
FAX.06-6258-8092

名古屋営業所:

〒460-0003 愛知県名古屋市中区
錦3-5-27 錦中央ビル10F
TEL.052-955-1221
FAX.052-963-6332

福岡営業所:

〒812-0011 福岡県福岡市博多区
博多駅前2-3-7サンエフビル7F
TEL.092-471-0562
FAX.092-471-0563

掲載されている機能等の製品情報には現在開発中のものも含まれております

