

Web サイトを利用する攻撃が急増しています！

～最近の攻撃の主流である「Web からの脅威」(Web Threats)を解説します～

作成 : 2007/11/1

※ この資料はトレンドマイクロホームページを参考に作成されています。
最新情報は下記ページをご参照ください。
<http://www.trendmicro.co.jp/web-threats>

～はじめに～

愉快犯から金銭目的へ。

コンピュータをめぐる脅威は確実に変化しています。

これらの脅威から守るには、従来のウイルス対策だけでは不十分になってきました。

トレンドマイクロでは、最近の脅威を「Web からの脅威 (Web Threats)」とし、警戒しています。

～目次～

1 章: 脅威の変化	P.3
現在、ウイルス等の不正プログラムの作成目的は自己顕示から金銭搾取へと変化しています。	
2 章: どのような攻撃なのか	P.5
不正プログラムが、侵入や感染などの目的で Web サイト(HTTP 通信)を利用する攻撃手法が「Web からの脅威」です。	
3 章: 攻撃例の紹介	P.7
2007 年 6 月、イタリアで多くの正規な Web サイトを改ざんしてウイルス攻撃を仕掛ける事件が発生しました。これは典型的な「Web からの脅威」です。	
4 章: 何が危険なのか	P.8
「Web からの脅威」には、今までのウイルスになかった新たな危険性をはらんでいます。	
5 章: 今までの対策の限界	P.10
従来のウイルス対策だけでは「Web からの脅威」を防ぐことができません。	
6 章: Total Web Threat Protection	P.11
トレンドマイクロでは、複数階層 (レイヤ) や複数製品を連携させることで、「Web からの脅威」に効率的に対抗できると考えます。	
7 章: 対策に必要な機能	P.12
「Web からの脅威」を対策するためには、さまざまな機能が必要になります。	
8 章: 脅威情報の収集、解析への取り組み	P.15
「Web からの脅威」には、発生したばかりの脅威に関する情報をいち早く収集し、適切なソリューションを迅速に提供することが求められます。	

1章:脅威の変化

最近、ウイルス等の作成目的が大きく変化してきました。この目的の変化によって、まったく新しい攻撃が発生しています。それが「Webからの脅威」です。

かつての攻撃目的

以前、ウイルス等の不正プログラムは、自分の能力を誇示する目的で開発されていました。そのような目的で作られた不正プログラムは、主にメールに添付されてインターネットへと放たれます。ほとんどは広まることのないまま消えていきますが、ごく少数の不正プログラムは、全世界規模で蔓延してしまいます。

このようにして不正プログラムが蔓延すると、セキュリティベンダーからアラートが発令され、新聞やニュースに取り上げられ、世間を騒がすこととなります。



最近の攻撃目的

ところが現在、不正プログラムの作成目的は自己顕示から金銭搾取へと変化してきました。具体的には以下のような目的に不正プログラムが利用されます。

- ✓ ユーザ名、パスワードの取得によるオンラインバンクへの不正アクセス
- ✓ 不正プログラムがコンピュータに裏口を開けること(バックドア活動)による不正侵入、情報搾取
- ✓ 不正プログラムに感染した全世界のコンピュータを利用してスパムメールの大量送信
- ✓ 不正プログラムによる攻撃をちらつかせた脅迫

また、不正プログラムによる悪意ある活動を第三者に代わって実行し、見返りとして報酬を得る業者も現れています。



奥に潜む不正プログラム

かつて不正プログラムは、短期間の感染活動や、感染後の破壊活動を主な目的にしていました。そのため、不正プログラムに感染すると、コンピュータの動作が遅くなり、やがてコンピュータが活動しなくなってしまう。そして、ユーザは不正なプログラムに感染してしまったことに気づきます。

最近の不正プログラムは、金銭を少しでも多く得るために、活動し続ける必要があります。そのため、コンピュータに負荷を与えず、ユーザに何も感じさせないようにひっそりと活動します。画面上にメッセージを出すような不正プログラムは少なくなりました。全世界には、不正プログラムに感染していることに気づかないまま使用されているコンピュータは数十万台とも数百万台ともいわれています。



舞台はメールから Web サイトへ

かつての不正プログラムは、メールの添付ファイルとして侵入してくる方法が侵入方法全体の 9 割以上を占めていました。しかし、人々の意識の高まりや、メールのセキュリティ製品の普及に伴って、メールに不正プログラムが添付される機会は少なくなりました。

現在、不正プログラムは Web サイトにおかれることが多くなりました。一般ユーザがインターネットを使用する場合、情報収集、ブログ、ショッピングなど、目的の違いはあっても、Web サイトにアクセスしています。企業においても、Web サイトを通じて他企業や一般ユーザとコミュニケーションを取ることがビジネスにおいて不可欠になっています。そのため、悪意のあるユーザは不正プログラムを Web サイトに仕掛けます。利用者の多い地点に仕掛けた方が、効率的に不正プログラムを実行させることができます。不正プログラムが仕掛けられる Web サイトは、不正目的で運営されている Web サイトだけではなく、一般ユーザが利用する Web サイトにも密かに仕掛けられます。仕掛けを施された Web サイトにアクセスしただけで感染活動を実行できる不正プログラムも存在しています。



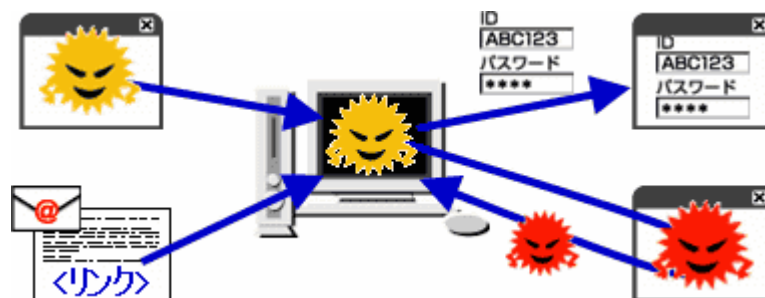
ユーザがどんなに注意を払っていても、不正プログラムが仕掛けられた Web サイトにアクセスしてしまう可能性があり、Web サイトに潜む不正プログラムを実行してしまう可能性があります。

2章:どのような攻撃なのか

ウイルスやスパイウェアなどの不正プログラムが、侵入や感染などの目的で Web サイト(HTTP 通信)を利用する攻撃手法を、トレンドマイクロでは「Web からの脅威」と呼んでいます。

攻撃手法の例

- ✓ Web サイトに不正なコードを仕掛けておき、Web サイトを閲覧したユーザに不正プログラムを感染させる
- ✓ 不正プログラムが、自分自身の機能をアップデートさせるために Web サイトからアップデートモジュールをダウンロードする
- ✓ 活動を開始した不正プログラムが、Web サイトから別の不正プログラムをダウンロードして実行させる
- ✓ 不正プログラムが収集した個人情報を、Web サイトへアップロードさせる
- ✓ 不正プログラムが URL 付きのメールをばらまき、その URL にアクセスしたユーザに不正プログラムを感染させる



データから見る Web からの脅威

2007 年上半期のウイルス感染被害レポートをみると、上位にランキングされているウイルスのすべてが、活動のひとつとして Web サイトを利用した攻撃を行っていることがわかります。

順位	ウイルス名	活動	ウイルス種類	発見時期
1位	BKDR_AGENT	Webからダウンロード	バックドア	2003年 8月
2位	TROJ_VUNDO	Webに情報送信	トロイの木馬型	2004年 11月
3位	JAVA_BYTEVER	Webに埋め込み	その他	2003年 5月
4位	TROJ_ZLOB	Webからダウンロード	トロイの木馬型	2005年 11月
5位	TROJ_DLOADER	Webからダウンロード	トロイの木馬型	2004年 7月
6位	WORM_SDBOT	Webでアップデート	ワーム型	2003年 10月
7位	WORM_STRATION	Webでアップデート	ワーム型	2006年 8月
8位	WORM_RBOT	Webでアップデート	ワーム型	2004年 3月
9位	BKDR_HUPIGON	Webからダウンロード	バックドア	2005年 2月
10位	TROJ_VB	Webからダウンロード	トロイの木馬型	2003年 1月

図:2007 年上半期ウイルス感染被害レポート

※このランキングは、2007 年 1 月 1 日から 6 月 30 日までの間に、日本のトレンドマイクロのサポートセンターに寄せられた問い合わせをもとに順位付けを行ったものです。本数値は、2007 年 7 月 5 日現在の情報に基づき作成されたものです。以前に集計されたものと数字が異なっている可能性や、今後のサポート調査により、件数に変更が生じる可能性があります。

※亜種をひとつのウイルス名にまとめてカウントしたランキングです。

3章:攻撃例の紹介

イタリアで発生した大規模攻撃

2007年6月にイタリアで多くの正規なWebサイトを改ざんしてウイルス攻撃を仕掛ける大規模な攻撃が発生しました。

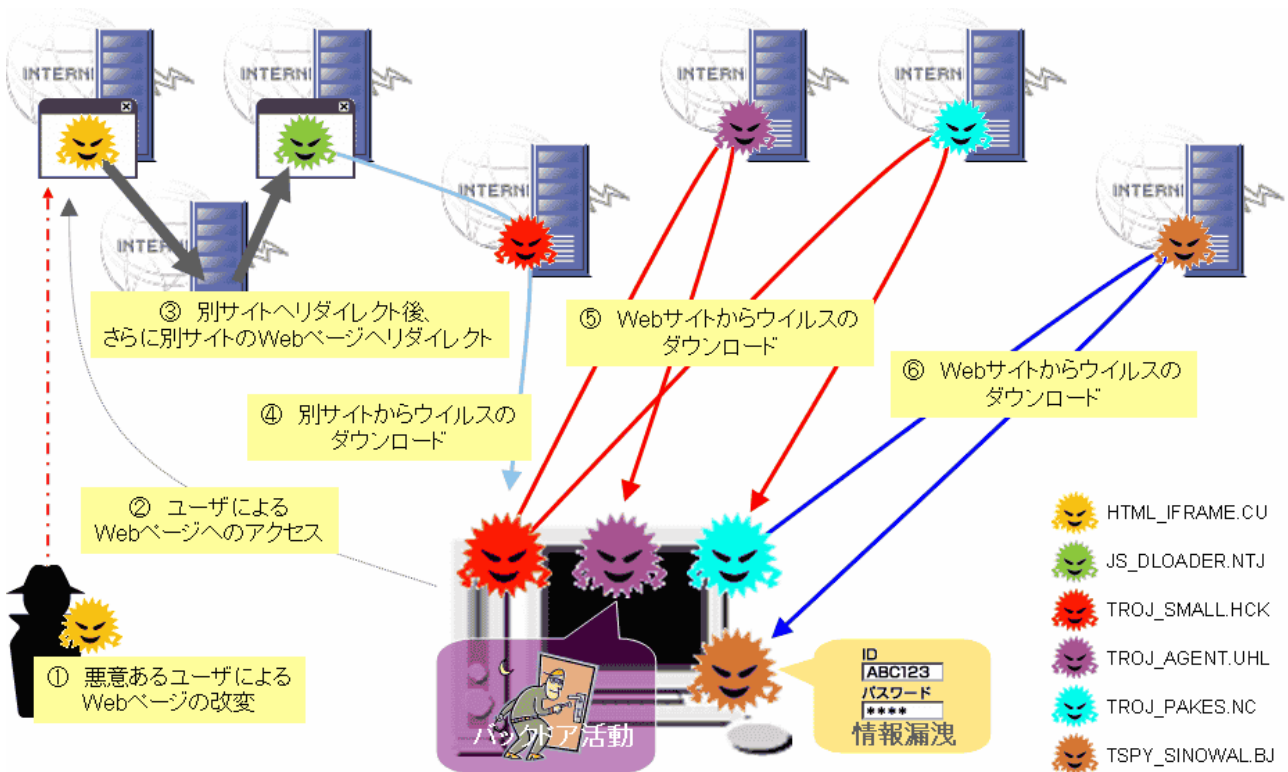


図:イタリアで発生した大規模攻撃イメージ

ユーザが日頃利用している正規なサイトにアクセスしただけでウイルスの攻撃を受けてしまいます。いったん攻撃が始まると、次々に違うウイルスの攻撃を受けてしまいます。最終的には個人情報盗まれてしまったり、コンピュータを外部から操作されてしまったりします。最初のWebサイトへのアクセス以外は自動で実行されてしまいますので、ユーザが高いセキュリティ意識を持っていても、開始されてしまった一連のウイルス攻撃を止めることができません。

4章:何が危険なのか

Web サイト(HTTP 通信)をベースに攻撃を仕掛けるのが「Web からの脅威」です。この攻撃手法の変化はどのような危険性をはらんでいるのでしょうか。

どの Web サイトにアクセスしても攻撃が開始される可能性がある

今までは、ほとんどの場合、個人の Web サイトや、ウイルスを広めることを目的とした Web サイトにアクセスして、ウイルスに感染していました。

最近では、正規の Web サイトにアクセスしてもウイルスに感染してしまうことがあります。悪意のあるユーザは、正規の Web サイトを改変します。その改変は、アクセスするとウイルスに感染するような設定をした Web サーバへ自動的に転送するための記述を追加するだけです。この些細な変更で、正規な Web サイトが、ウイルス感染の入り口になってしまいます。

つまり、昨日まで利用していた Web サイトが、今日はウイルス感染の入り口になってしまいます。



メールにウイルスが添付されていなくても URL をクリックするとウイルスに感染してしまう

ウイルスの侵入経路として一番利用されていたのは、メールの添付ファイルとして侵入する方法でした。そのため、知らない人から届くメールに添付されたファイルは危険である、という認識は広まっています。

最近では、メールにウイルスそのものは添付せずに、ウイルスが潜む Web サイトへの URL だけを記述して送られます。この URL は、メール表記上の Web サイトと実際アクセスする Web サイトが異なるという偽装がされていることがあります。また、画像に URL がつけられていて、クリックしてみないとどの Web サイトにアクセスするのかわからないものもあります。

つまり、ウイルスが仕掛けられた Web サイトへの入り口が、メール内の URL という形で手元に届いてしまいます。



Web サイトにおかれたウイルスが変更されると攻撃の流れが変わってしまう

2007年6月に発生したイタリアでの攻撃事例のように、あるウイルスに感染すると次から次に違うウイルスに感染してしまいます。ウイルスがWebサイトから違うウイルスをダウンロードしてしまうためです。一度攻撃の全容がわかっただけで、ダウンロードされるウイルスをウイルス対策製品で次々に止めてしまうことが可能です。しかし、Webサイトからダウンロードされるウイルスが前回と異なるウイルスだった場合はどうでしょうか。そのウイルスを止めることができないだけでなく、今までと異なるWebサイトから新たなウイルスをダウンロードしてきてしまいます。悪意のあるユーザは、不正なサーバにおかれたウイルスファイルを置き換えるだけの簡単な作業で、今までとは違う攻撃を仕掛けることができます。



つまり、一度対策ができあがっても、サーバに置かれたウイルスを変更されてしまうと、その対策は使えなくなってしまう。

Web サイトにアクセスできる＝ウイルスに感染する可能性がある

通常、ユーザがウイルスファイルを実行してしまい、はじめてウイルスに感染してしまいます。

最近はWebサイトにアクセスしただけでウイルスが活動を開始してしまうことがあります。これはインターネット家電やゲーム機、携帯電話などもウイルスに感染してしまう可能性を意味しています。悪意のあるユーザは、どのようにウイルスファイルをユーザに届けるかを考える必要がなくなりました。ユーザがアクセスしそうなWebサイトにウイルスファイルを仕掛けておくだけで、あらゆるユーザにウイルスを感染させることができるようになります。



つまり、ウイルスに感染する可能性があるのはコンピュータに限ったことではなくなっているのです。

5章: 今までの対策の限界

現在、すでにさまざまなセキュリティ製品が発売されており、コンピュータ環境を守っています。しかし、単体の既存製品のみでは「Web からの脅威」に対抗することが困難です。

ファイアウォールのみでは防げません

ファイアウォールは、インターネットと内部ネットワークの間に配置し、インターネットからの攻撃を防ぐためのものです。内部ネットワークから不正プログラムが仕掛けられている Web サイトへのアクセスのみを、ファイアウォールでは防げません。Web サイトへのアクセスをブロックすると、すべての Web サイトへのアクセスをブロックすることになります。「Web からの脅威」では、ウイルスの仕掛けられた Web サイトにアクセスしてしまうことが問題になります。



IDS(不正侵入検知)のみでは防げません

ネットワーク内の通信を監視して、挙動の怪しい通信が発生した際に管理者に知らせる機能を持つのが IDS(不正侵入検知)です。不正プログラムが仕掛けられた Web サイトにアクセスしダウンロードしてしまっても、ダウンロード自体は通常の HTTP 通信になりますので怪しい通信とは検出されません。不正プログラムが活動を開始しても、ネットワーク内のコンピュータにウイルスをばらまくような活動はしないため、一気にネットワーク使用量が増えることもありません。



メールのウイルス対策製品のみでは防げません

メールのウイルス対策製品は、メールの添付ファイルが不正プログラムかどうかを監視します。しかし、Web からの脅威で使用されるメールには不正プログラムそのものは添付されていません。不正プログラムが潜む Web サイトへの URL が記述されているだけです。そのため、メールのウイルス対策製品では問題ないと判定されたメールでも、その中の URL をクリックしてしまうことで不正プログラムに感染してしまいます。



クライアントのウイルス対策製品のみでは防げません

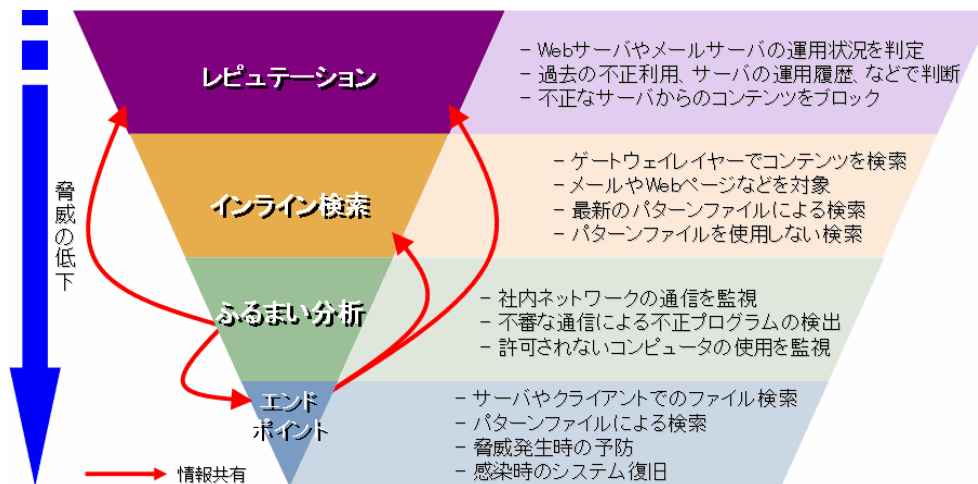
日常的に使用しているコンピュータにやってきたファイルが不正プログラムかどうかを監視するのがクライアントのウイルス対策製品です。次々と新しい不正プログラムが大量に使用される「Web からの脅威」に対抗するためには、パターンファイルのアップデートによる検出だけでは対応が遅れてしまうことになります。パターンファイルを使用せずにウイルスを検出する機能もありますが、完璧にはすべての新しいウイルスを検出できません。



6章: Total Web Threat Protection

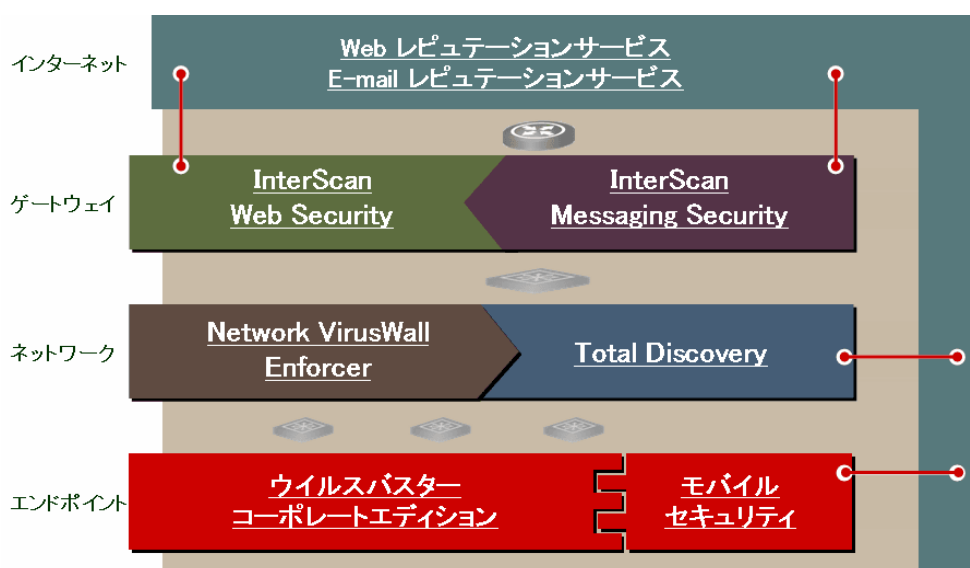
ひとつの製品の機能を強化していくだけでは、「Web からの脅威」への対策には限界があります。トレンドマイクロでは、複数階層(レイヤ)や複数製品を連携させることで、「Web からの脅威」に効率的に対抗できると考えます。

インターネットからのコンテンツを4段階のふるいにかけて、コンテンツに潜む脅威を効率的に減少させます。



この4段階のふるい、つまり、4つのレイヤで「Web からの脅威」に対抗するのが、「Total Web Threat Protection」です。4レイヤによる防御は、各レイヤで脅威を効率的に減少させるだけでなく、各レイヤで検出した脅威情報を共有し、次々と発生する新しい脅威への迅速な対応を可能にします。

「Total Web Threat Protection」の考えを、トレンドマイクロの製品に当てはめたのが、以下の概念図になります。



※「Total Discovery (仮称)」は今後発売予定の製品です。

7章:対策に必要な機能

「Webからの脅威」を対策するためには、さまざまな機能が必要になります。トレンドマイクロの製品は、「Webからの脅威」を対策するための最新の機能が搭載されています。

信頼性の低いWebサーバへのアクセスをブロックする

Webサイトにアクセスすると不正プログラムに感染してしまう「Webからの脅威」。不正プログラム自身がWebサイトにアクセスして不正な活動を続ける「Webからの脅威」。これらに効率よく対応するためには、不正な目的に利用されるWebサイトにアクセスしないようにする必要があります。リアルタイムに更新される全世界のWebサイト情報を利用して、信頼性の低いWebサイトへのアクセスをブロックできます。



トレンドマイクロ製品・サービスによる対策

- ✓ Webセキュリティサービス

信頼性の低いメールサーバからのメール受信をブロックする

スパムメール内のURLで、不正プログラムが仕掛けられたWebサイトへと導かれてしまうことがあるのも、「Webからの脅威」の特徴のひとつです。日々増え続けるスパムメールを効率よくブロックするためには、メールを受信する前に、必要なメールかどうかを判断する必要があります。数種類のデータベースを使用して、スパムメール配信に関与するメールサーバの接続そのものをブロックすると、スパムメール受信を大幅に減らすことが可能です。



トレンドマイクロ製品・サービスによる対策

- ✓ Email Reputation Services Advanced

ゲートウェイレイヤで Web サイトからの不正ファイルのダウンロードをブロックする

「Web からの脅威」では、Web サイトに仕掛けた不正プログラムを、ユーザにダウンロードさせて実行させます。ダウンロードされる不正プログラムは、ゲートウェイでチェックしブロックするのが最も効率的です。トレンドマイクロのゲートウェイ対策製品は、ウイルスだけでなくスパイウェアのダウンロードもチェックします。設定が柔軟なソフトウェア製品に加え、導入が簡単なハードウェア製品も提供しています。



トレンドマイクロ製品・サービスによる対策

- ✓ InterScan Web Security Suite
- ✓ InterScan Web Security Appliance
- ✓ InterScan Gateway Security Appliance
- ✓ InterScan VirusWall スタンダードエディション
- ✓ ASA 5500 Content Security Edition

ゲートウェイレイヤで不審なメールの侵入をブロックする

メールは有益なツールのひとつですが、不正なものが添付されることがあります。「Web からの脅威」では、ウイルスが仕掛けられた Web サイトへの URL がメールに記述されます。メールの内部の不正な記述をチェックするのがメールのコンテンツフィルタリング製品です。この機能では、添付ファイルが不正プログラムだった場合に加え、不正なキーワード、不正な URL が記述されたメールをブロックします。



トレンドマイクロ製品・サービスによる対策

- ✓ InterScan Messaging Security Suite
- ✓ Email Reputation Services
- ✓ InterScan Gateway Security Appliance
- ✓ InterScan VirusWall スタンダードエディション
- ✓ InterScan for Microsoft Exchange
- ✓ InterScan for Domino
- ✓ InterScan Messaging Security Appliance

セキュリティポリシーを満たさないコンピュータのネットワーク使用をブロックする

セキュリティレベルの低いコンピュータが社内ネットワークに接続された場合、そのコンピュータを中心とした攻撃が全社に影響を及ぼすことがあります。「Web からの脅威」で狙われるのは、このようなセキュリティレベルの低いコンピュータです。そのコンピュータを足がかりに、全社へ攻撃の手を広げます。社内ネットワークのセキュリティレベル向上のためには、コンピュータのセキュリティ状況を常に監視し、万が一の場合には規制をかける必要があります。



トレンドマイクロ製品・サービスによる対策

- ✓ Network VirusWall Enforcer 1200/2500

コンピュータ上で不正プログラムが活動を開始するのをブロックする

「Web からの脅威」で使用される不正プログラムは、ユーザのコンピュータ上でさまざまな悪意のある活動をします。サーバやクライアントのセキュリティ対策製品は、コンピュータ上で不正プログラムの活動をチェックし、その活動をブロックします。不正プログラムの検出以外にも、感染してしまったシステムを復旧する機能や、ウイルスや悪意のあるユーザによるネットワークからの攻撃を防ぐファイアウォール機能も搭載し、複合的な脅威に迅速に対応できます。



トレンドマイクロ製品・サービスによる対策

- ✓ Client/Server Suite アドバンス Powered by ウイルスバスター コーポレートエディション 8.0
- ✓ ウイルスバスター ビジネスセキュリティ

ご家庭のお客さま向けの機能

ご家庭におけるインターネット利用目的の中心は、Web サイトやメールの閲覧です。そこには、企業ユーザと同じように「Web からの脅威」が潜んでいます。ご家庭では、使用しているコンピュータですべての脅威に対抗しなくてはなりませんので、要求されるセキュリティ機能は多岐にわたります。つまり、メール使用時、Web サイト閲覧時、ファイル操作時、など、それぞれの場面で遭遇する脅威に対抗するためのさまざまな機能が必要です。



トレンドマイクロ製品・サービスによる対策

- ✓ ウイルスバスター2008

8 章: 脅威情報の収集、解析への取り組み

「Web からの脅威」には、発生したばかりの脅威に関する情報をいち早く収集し、適切なソリューションを迅速に提供することが求められます。トレンドマイクロでは、脅威情報を収集、解析するための専用の組織を設置しています。

TrendLabs (トレンドラボ)

トレンドラボは、フィリピンの首都マニラを中心に、世界各地に拠点を持つ組織です。24 時間 365 日体制で世界中の脅威を監視しています。発見された新種の不正プログラムは、すぐに解析されてパターンファイルにその情報が反映されます。その他にも、新しい脅威に対抗するための新機能もトレンドラボで開発されています。トレンドラボの高い技術力で、トレンドマイクロはみなさまに毎日の安心を提供しています。



トレンドラボ/ビルの外観

リージョナルトレンドラボ

リージョナルトレンドラボは、特定地域で発生している脅威情報を収集し、その地域向けのソリューションを提供するための組織です。トレンドラボの全世界的なソリューション提供に加え、リージョナルトレンドラボによる特定地域に特化したソリューションを、今まで以上に迅速に提供いたします。たとえば、日本のリージョナルトレンドラボでは、日本のある企業が攻撃された場合に、その企業からの情報を基に、その企業向けのソリューションを素早く提供することが可能です。

