

安心を、ひとつ上のステージへ。



安心を、ひとつ上のステージへ。



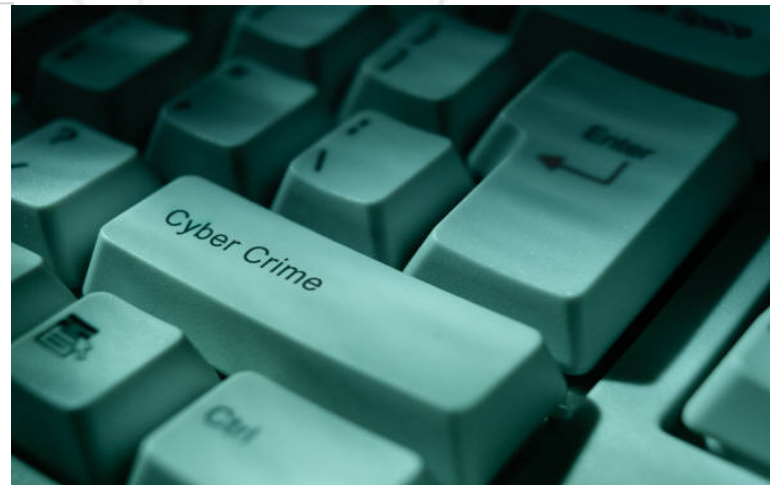
Webからの脅威再確認：2007年の実態

グローバル・国内の状況と、今後の動向

トレンドマイクロ株式会社
上級 セキュリティエキスパート
黒木 直樹

これが現実です

サイバー犯罪は
すでに本格化しています。



なぜか？

なぜならそこに
お金があるからです。



安心を、ひとつ上のステージへ。



安心を、ひとつ上のステージへ。



グローバルの視点から

第5回 情報セキュリティEXPO

サイバー犯罪を助長するアンダーグラウンドのマーケット

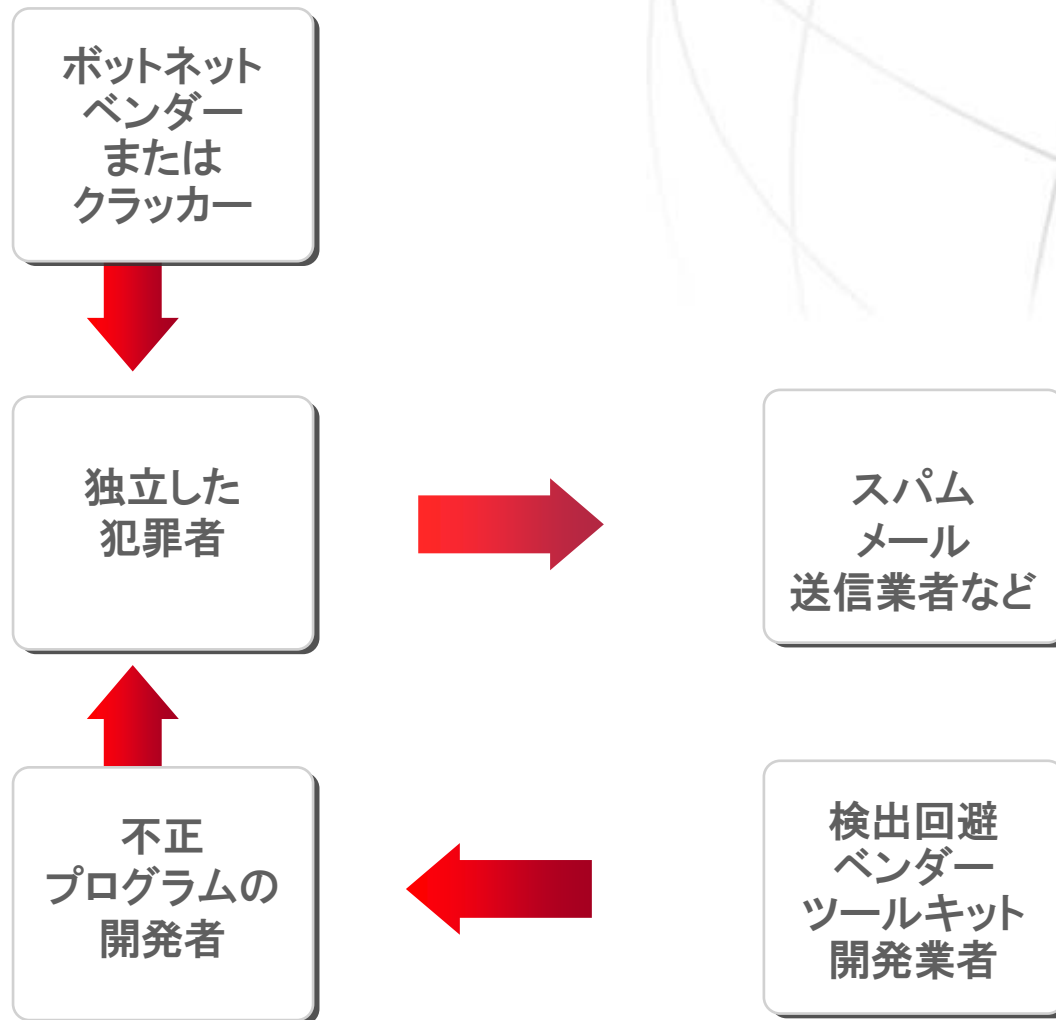
安心を、ひとつ上のステージへ。

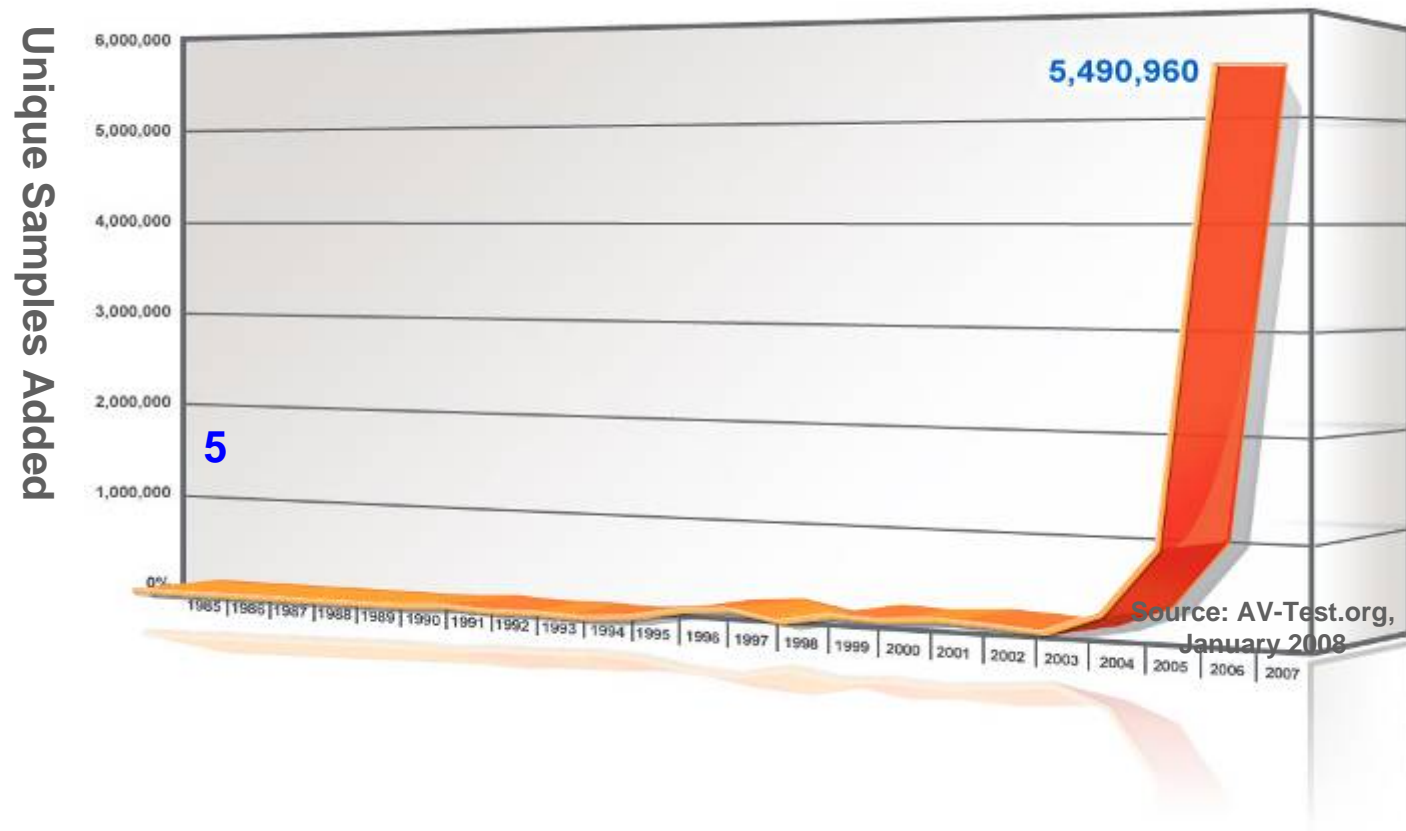


対象	単価
個別に管理可能なアドウェアのインストール 1件あたりに対する対価	米国では30セント、カナダは20セント、英国は10 セント。その他の地域であれば2セント
不正プログラムのパッケージ:基本版	\$1,000 – \$2,000
不正プログラムのパッケージ:アドオンサービス	\$20～
エクスプロイト キットのレンタル:1時間	\$0.99 ～ \$1
エクスプロイト キットのレンタル:2.5時間	\$1.60 ～ \$2
エクスプロイト キットのレンタル:5時間	\$4 ただし条件によって異なる
情報搾取を目的とした検知不可能なトロイの木馬の コピー	\$80 ただし条件によって異なる
DDos攻撃	1日あたり\$100
10,000台の感染PC	\$1,000
不正に取得した銀行口座情報	\$50 ～
未検証の新しいe-mailアドレス100万件	\$8～ 品質に依存する

2007年のアンダーグラウンドマーケット調査からのサンプルデータ

アンダーグラウンドでの協業





出典:トレンドマイクロ株式会社

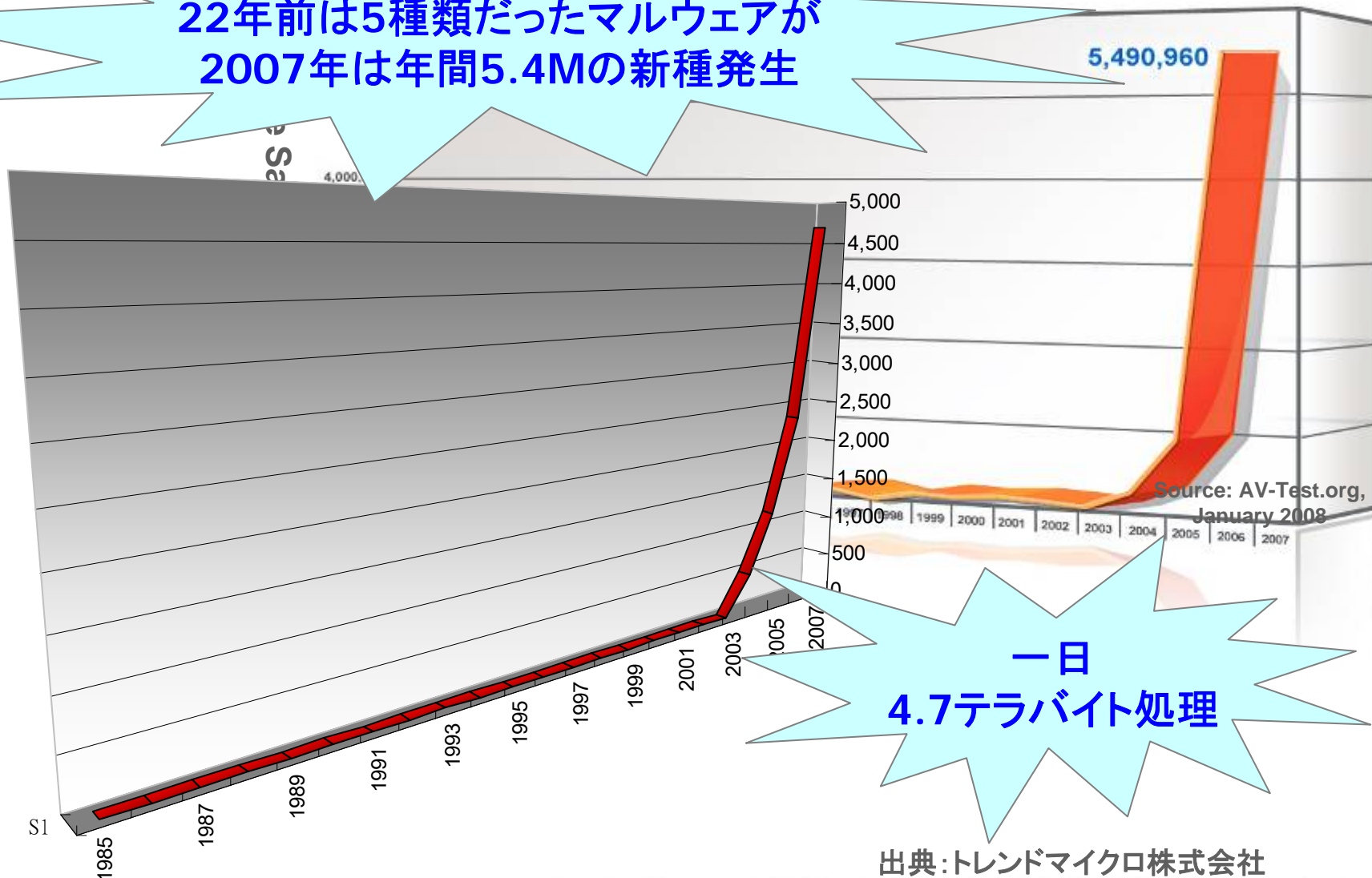
市場環境の変化

安心を、ひとつ上のステージへ。



22年前は5種類だったマルウェアが
2007年は年間5.4Mの新種発生

Data Processed (1000MB)



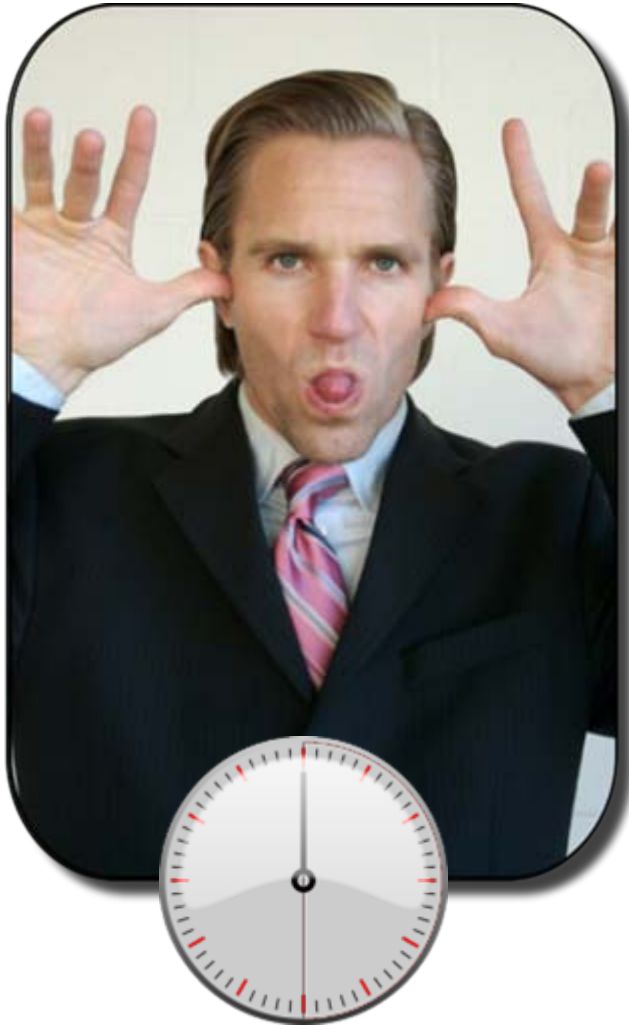
一日
4.7テラバイト処理

出典:トレンドマイクロ株式会社

作る側と守る側

安心を、ひとつ上のステージへ。





ウイルスはどう変遷してきたのか？

安心を、ひとつ上のステージへ。



ウイルス

不正プログラム

Webからの脅威

不正プログラムはさらに細分化できる

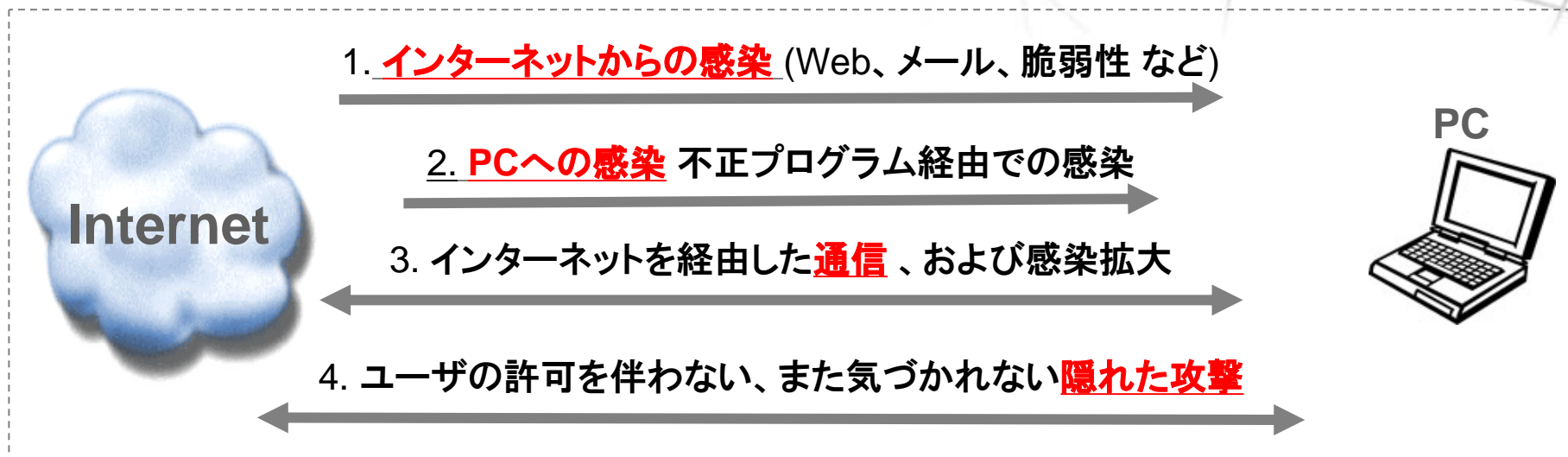
安心を、ひとつ上のステージへ。



金銭を目的とした
不正プログラム

クライムウェア

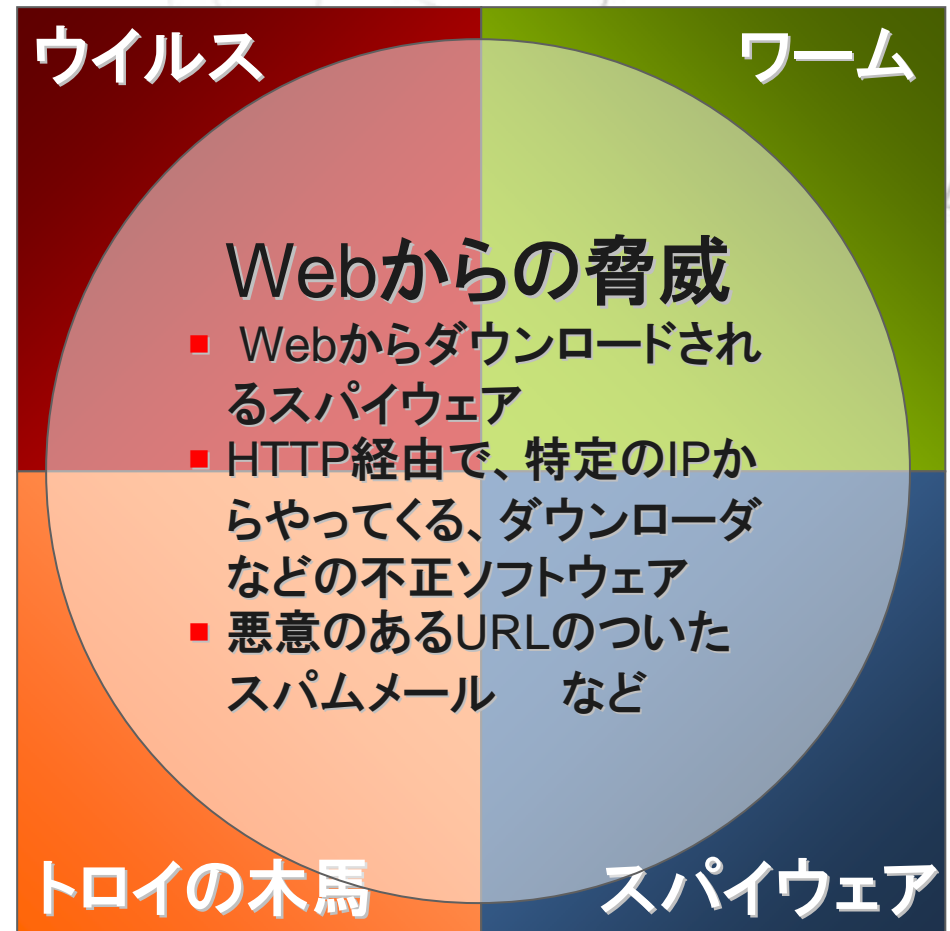
「サイバー犯罪を促進するためのインターネットの利用」



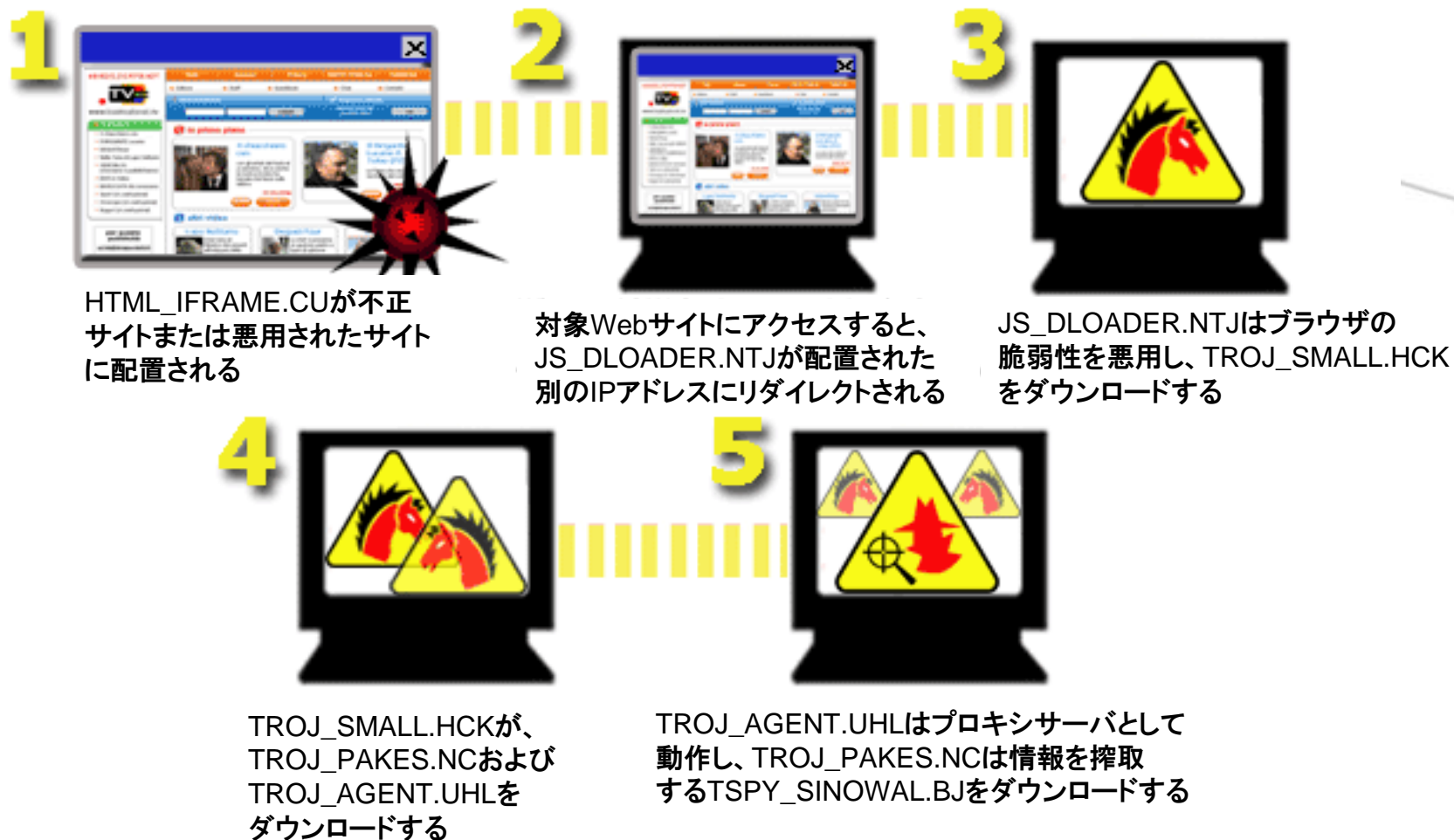
注意:3番目の行動を伴うものが、「Webからの脅威に当てはまる」

Webを媒介とした予期できない脅威

- 主に、悪意ある行動を実行するために、HTTP経由で送られる不正プログラムを指す
 - ▶ 例：身元詐称、個人情報/機密情報盗用など
 - ▶ インターネット経由で流入、増殖、配信し、身を隠す
- 不正プログラムや不正技術の複合的な脅威、または連続する(シーケンシャルな)攻撃が特徴
- ブラウザ経由だけでなく、ユーザの許可なくインストールされ密かに自分の目的を達成するような不正プログラムを含む



Webからの脅威の例：“The Italian Job”



Webからの脅威の例

安心を、ひとつ上のステージへ。



OfficeScan Notification Message

TREND MICRO™ OfficeScan™

Number of instances: 1

Date/Time	URL
12/7/2007 07:29:20	http://77.221.133.188/#/go.html?338228cddf1e1e

OK

最初の感染は、アクセスしたブラウザの脆弱性を突くだけでなく、脆弱性のないシステムについては、レジストリが感染しているためクリーンアップが必要だとし、ユーザ自身に自身の手で感染プログラムをインストールさせる、ソーシャルエンジニアリングの手法を取っている。

Welcome To MonaRonaDona

Hi, My name is MonaRonaDona. I am a Virus & I am here to Wreck Your PC. If you observe strange behavior with your PC, like program windows disappearing etc, it's me who is doing all this. I was created as a protest against the Human Rights Violation being observed throughout the world & the very purpose of my existence is to remind & stress the world to respect humanity.

The only solution would be to install a good Antivirus software package which can detect and kill the virus. There are a lot of free Antivirus softwares available online. However the normal antivirus such as Norton or McAfee may not work for this Virus.

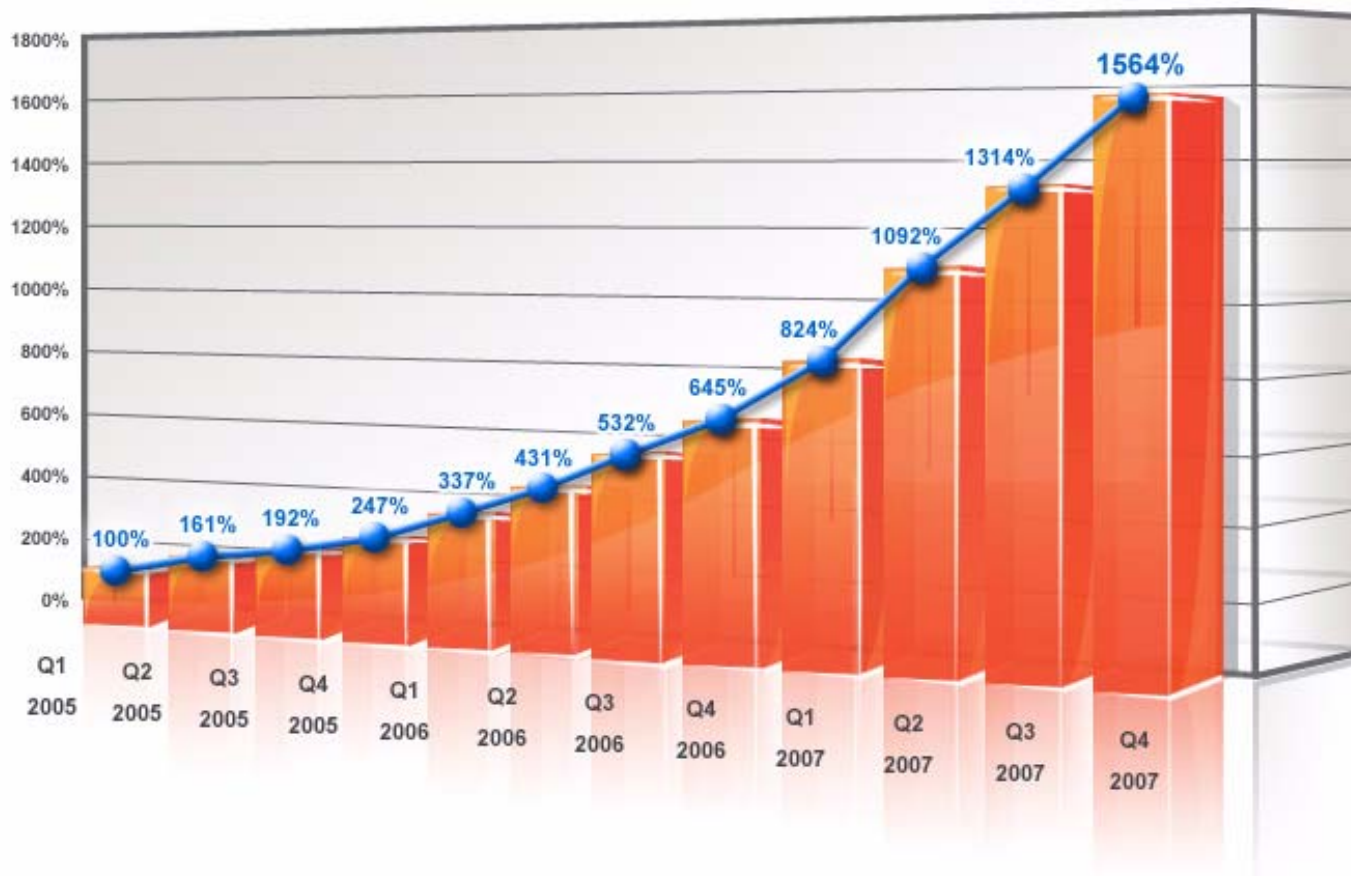
You can try downloading the **Unigray Antivirus** which is considered the best for removing the monaronadona virus compared to the other spyware / antivirus programs.

How to use Unigray Antivirus and how it works



これがWebからの脅威の現状です

安心を、ひとつ上のステージへ。



安心を、ひとつ上のステージへ。



安心を、ひとつ上のステージへ。



では日本では？

第5回 情報セキュリティEXPO

2007年 感染報告数上位10種

安心を、ひとつ上のステージへ。



ウイルス感染被害報告件数上位10種 (2007年1月1日~12月31日)

順位	ウイルス名	通称	ウイルス種類	被害件数	発見時期
【1位】	BKDR_AGENT ※①	エージェント	バックドア	832件	2003年8月
【2位】	TROJ_VUNDO ※①	ヴァンドー	トロイの木馬型	342件	2004年11月
【3位】	JAVA_BYTEVER ※②	バイトバー	その他	277件	2003年5月
【4位】	TROJ_DLOADER ※①	ディーローダー	トロイの木馬型	245件	2004年7月
【5位】	TROJ_ZLOB ※①	ゼットロブ	トロイの木馬型	230件	2005年11月
【6位】	BKDR_HUPIGON ※①	フピゴン	バックドア	214件	2005年2月
【7位】	WORM_RBOT ※①	アールボット	ワーム型	206件	2004年3月
【8位】	WORM_SDBOT ※①	エスディーボット	ワーム型	204件	2003年10月
【9位】	ADWARE_BESTOFFERS ※ ①	ベストオファーズ	アドウェア	166件	2006年7月
【10位】	EXPL_ANICMOO ※①	アニクモー	その他	146件	2007年3月

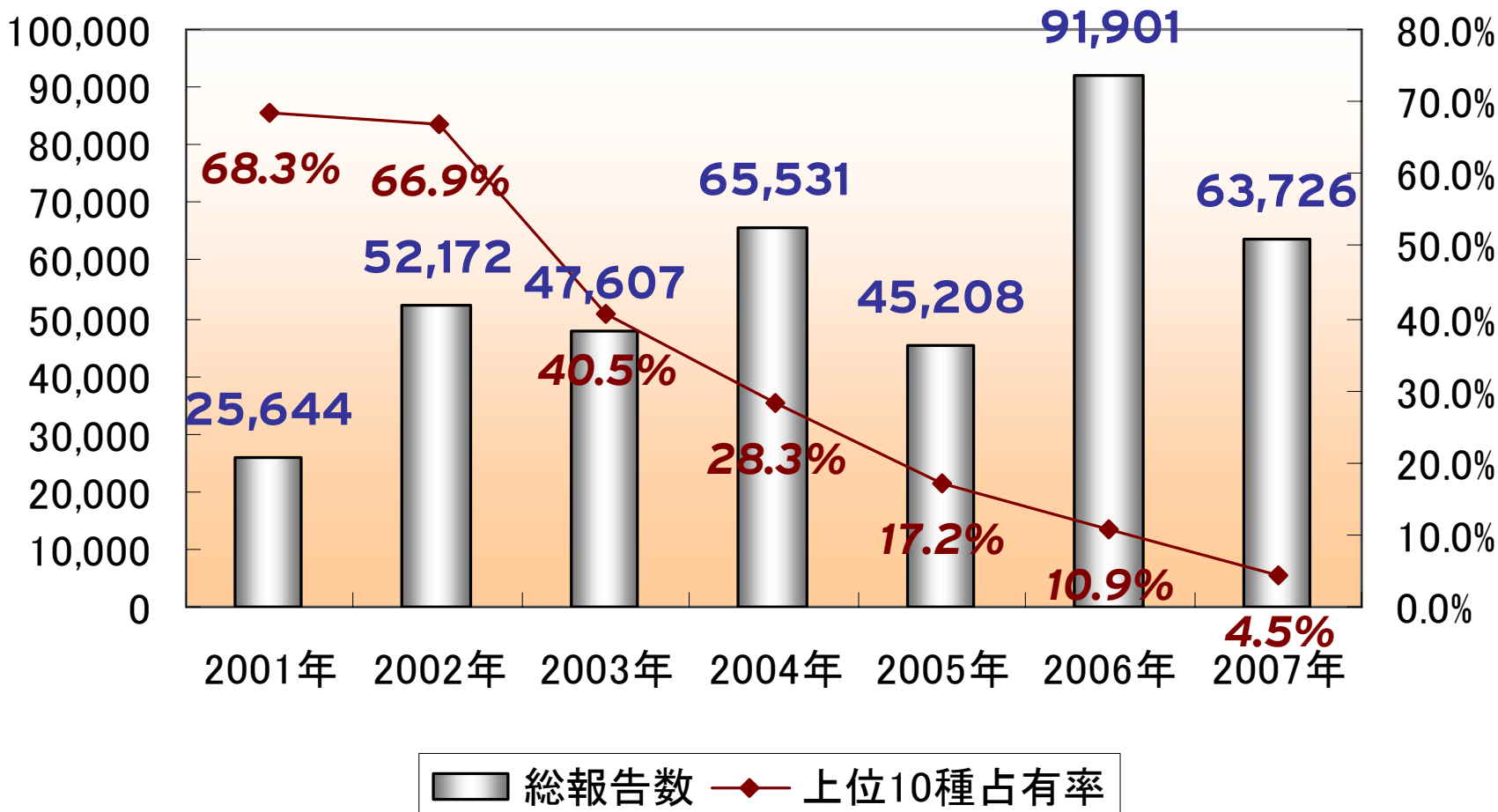
出展:トレンドマイクロ2007年度ウイルス感染被害年間レポート

※(※①)のウイルスに関しては、亜種をまとめてカウントした件数となります。

※(※②)「JAVA_BYTEVER.A」に関しては、パターンファイル番号1.546.00から「JAVA_BYTVERIFY.A」の検出名で対応いたしておりましたが、パターンファイル番号1.731.00から「JAVA_BYTEVER.A」に改称いたしましたので、双方の数を集計したものになります。

感染被害の分散化 - 上位10種の占有率の推移

ウイルス感染被害報告件数年間総計と上位10種の占有率の推移 (2001年~2007年)



※1 本データは、トレンドマイクロの日本サポートセンターへの問い合わせを元に集計しています。各年の数値は、「ウイルス感染被害年間レポート」でトップ10のウイルスを種別の件数でまとめたものです。<参考>ウイルス感染被害レポート: http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/index.html

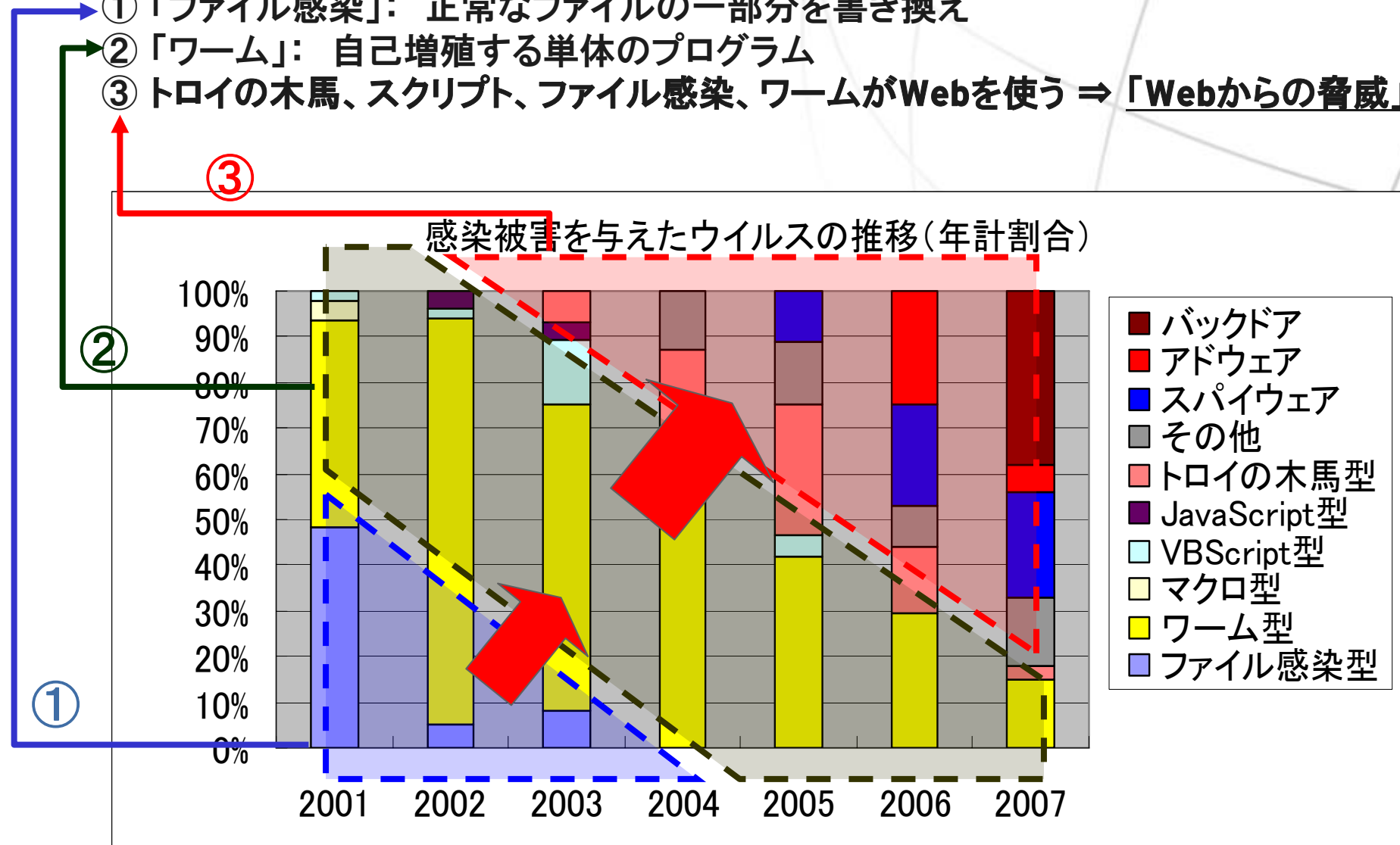


ファイル感染→ワーム→Web経由へ

※1 本データは、トレンドマイクロの日本サポートセンターへの問い合わせを元に集計しています。
各年の数値は、「ウイルス感染被害年間レポート」でトップ10のウイルスを種別の件数でまとめたものです。
<参考>ウイルス感染被害レポート: http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/index.html

～不正プログラムの形態～

- ① 「ファイル感染」: 正常なファイルの一部を書き換え
- ② 「ワーム」: 自己増殖する単体のプログラム
- ③ トロイの木馬、スクリプト、ファイル感染、ワームがWebを使う ⇒ 「Webからの脅威」



一太郎へのゼロデイ攻撃

対象となる製品

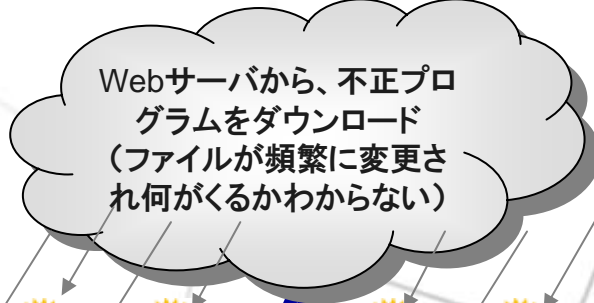
- 一太郎2007
- 一太郎ガバメント2007
- 一太郎2007体験版
- 一太郎2006
- 一太郎ガバメント2006
- 一太郎2005
- 一太郎 文藝
- 一太郎2004
- 一太郎13
- 一太郎12
- 一太郎11
- 一太郎ビューア
- 一太郎 for Linux



ROJ_TARODROP.Q



Windows Temporaryフォルダに
SVHOST.EXEを作成



Windowsシステムフォルダに
DG.EXEを作成
IEXPLORER.EXEのメモリに常駐

TROJ_SMALL.QQM



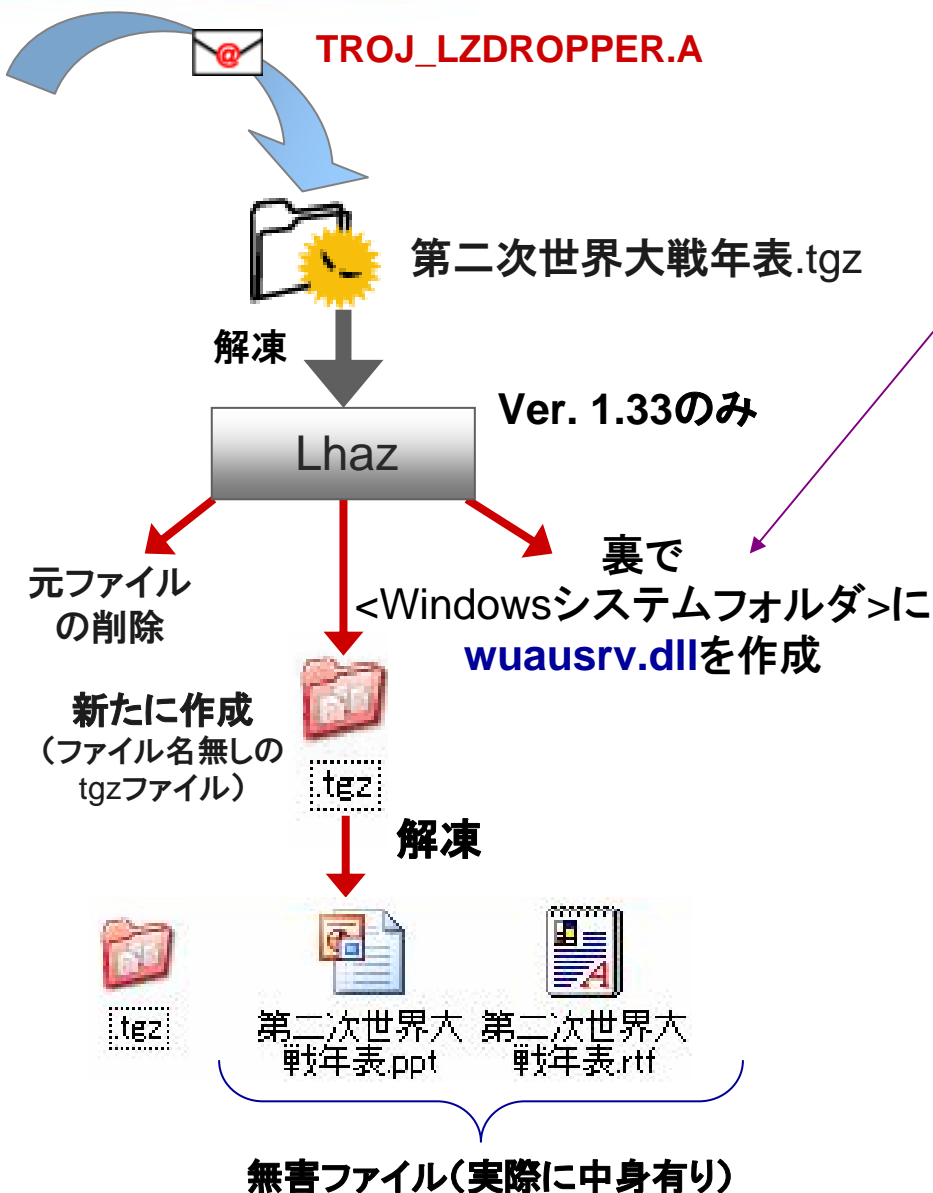
Windowsレジストリに登録
自動起動設定

JUSTSYSTEM社からの案内
<http://www.justsystem.co.jp/info/pd7003.html>

Webサーバは北京に置かれていた



Lhaz 1.33へのゼロデイ攻撃



これが **BKDR_PROTUX.AU**

レジストリを変更し自身の自動起動を登録

ランダムなTCPポートを開き不正アクセスに備える

- レジストリ値の追加、削除
- ファイルの削除、検索、アップロード
- シェルコマンドの実行
- プロセスの実行、終了
- 不正プログラムのアンインストール

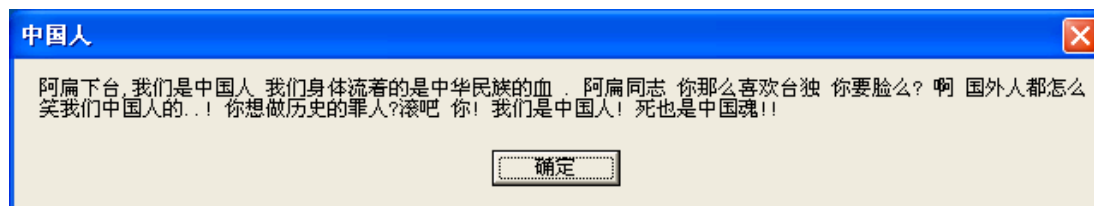
2007/8/23 修正版 1.34 公開
<http://www.chitora.jp/lhaz.html>

OSの言語設定を見分けるウイルス

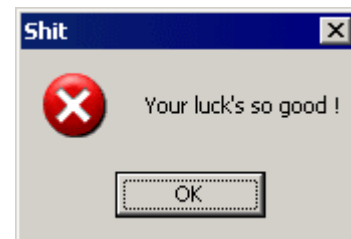
- 10月中旬にOSの言語設定を見分けるトロイの木馬型不正プログラムが確認された。

一言語設定詳細

- ✓ 言語設定が中国：何も行わずに終了し無害
- ✓ 言語設定が日本、もしくはインドネシア：
ハードディスクをゴミデータで上書きしてコンピュータを起動不能にする
- ✓ 言語設定が台湾：以下のメッセージを表示して終了



- ✓ 言語設定がその他：以下のメッセージを表示して終了



Iframeを利用したウイルスの急増

- Iframeとは「インラインフレーム」のことで、HTMLテキストの中にフレームを埋め込むタグのこと。
- 最近、Iframeの機能を悪用して、外部から任意のコードを実行させるといった手法でよく使用されるため、現在では「Iframe=Malware」というような認識が増えている。
- IframeはWebサイトの脆弱性について、サイト内に埋め込まれる。
- 最近では、「目では見えないIframeを追加し、自動的に他のサイトへ接続し、悪意のあるファイル(Malware)などをダウンロードさせる」等の使われ方が増加している。



遠隔操作する悪者



フィッシング詐欺犯

HTML_IFRAME 検出数の推移

安心を、ひとつ上のステージへ。



*トレンドマイクロWTCデータ調べ。2007年1月の数を「1」としたときの比較

	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月
全世界	1	1.53	2.79	1.87	1.27	22.37	4.22	2.56	6.64	18.41	183.14
日本国内	1	1.05	1.63	0.95	0.47	0.83	1.46	0.53	0.79	7.22	143.18

Windowsの
アニメーションカーソルへの
ゼロデイ攻撃
TROJ_ANICMOO.AX

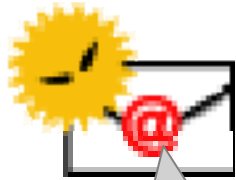
Italian Job による被害発生
Web Threatsの現実化

急激な増加
何かの前触れか？

正規Webページ改ざんや、HTMLメールを使った手法、OSの脆弱性を狙った攻撃などの裏には、Iframeの手法を使ったものが多く存在している。

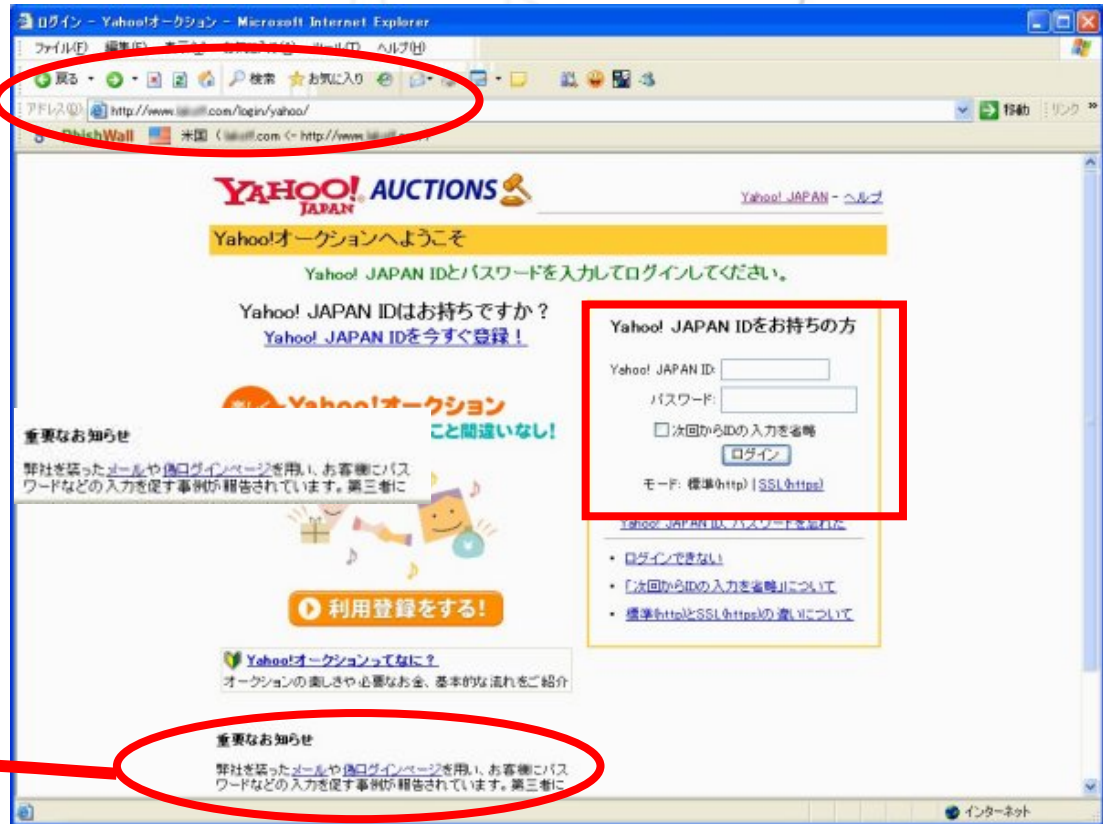
最新のセキュリティパッチの適用は当然として、怪しいメールは開かない、不審なサイトへは行かないなど、それだけでは危険を回避出来なくなって来ているのが現状である。

Yahoo!オークション評価メールを装うフィッシング



Yahoo!オークションの評価メールを偽装。

<http://www.yahoo...>と記載されたURLも、実際はフィッシングサイトへのURL



重要なお知らせ

弊社を装ったメールや偽ログインページを用い、お客様にパスワードなどの入力を促す事例が報告されています。第三者に

安心を、ひとつ上のステージへ。



安心を、ひとつ上のステージへ。



もう脅威には追いつけないのか？

第5回 情報セキュリティEXPO

さらにもう一歩対策を進める必要があります

安心を、ひとつ上のステージへ。



基本対策

パターンマッチング

さらに必要

Webからの脅威への対策

さらに必要

複数レイヤでの対策

さらに必要

振る舞い検知(HIPS)

パターンファイルだけの対策には限界が

検体入手



検体分析



新しいパターンを追加



パターンDB

...一ヶ月に、250,000件のユニークな検体？

...一ヶ月に500,000件のユニークな検体？

...一ヶ月に1,000,000件のユニークな検体？

...一ヶ月に1,000,000,000件のユニークな検体？

お客さまに配信



お客さま



パターンファイルの配信だけでは追いつけない現状

安心を、ひとつ上のステージへ。



安心を、ひとつ上のステージへ。



安心を、ひとつ上のステージへ。



Total Web Threat Protectionという考え方

Total Web Threat プロテクション

Trend**Labs**

Regional TrendLabs



Trend Micro Reputation Service



パターンファイル

Internet

オールインワン
セキュリティ ソリューション



InterScan Gateway
Security Appliance

SMBゲートウェイ

メッセージング セキュリティ ソリューション



InterScan
Messaging
Security Suite



InterScan
Messaging
Security Appliance

Enterpriseゲートウェイ

ウェブ セキュリティ ソリューション



InterScan
Web Security
Appliance



InterScan
Web Security
Suite



ウイルスバスター コーポレートエディション

エンドポイント

Total Web Threat プロテクション

TrendLabs

Product TrendLabs

In-the-cloud
お客さまの環境ではなく、
ネットワークにソリューションという考え方

インターネットサービス

パター

社内ネットワーク

オールインワン
セキュリティソリューション



InterScan Gateway
Security Appliance

SMBゲートウェイ

メッセージング セキュリティ ソリューション



InterScan
Messaging
Security Suite



InterScan
Messaging
Security Appliance

ウェブ セキュリティ ソリューション



InterScan
Web Security
Appliance



InterScan
Web Security
Suite

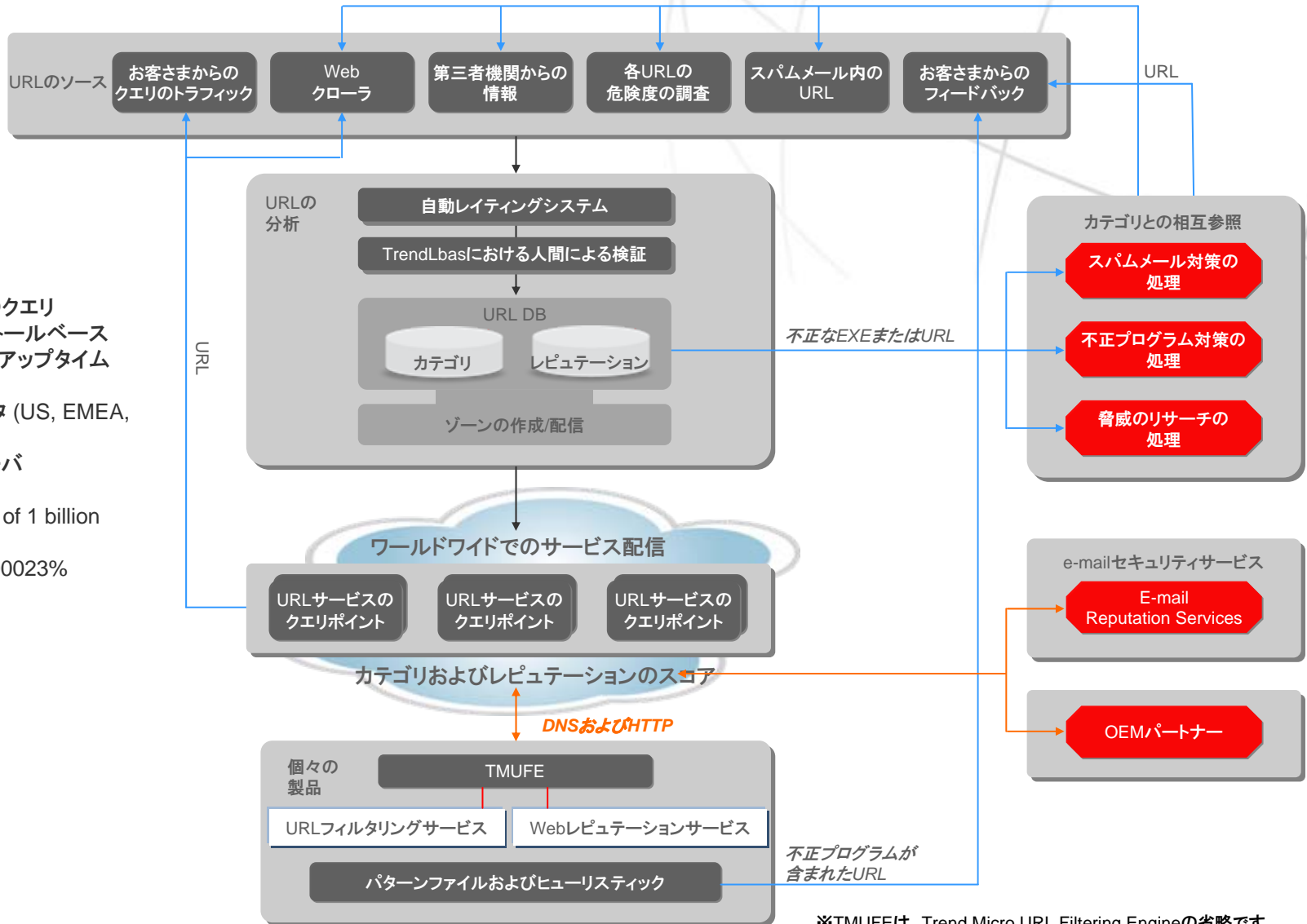
Enterpriseゲートウェイ



ウイルスバスター コーポレートエディション

エンドポイント

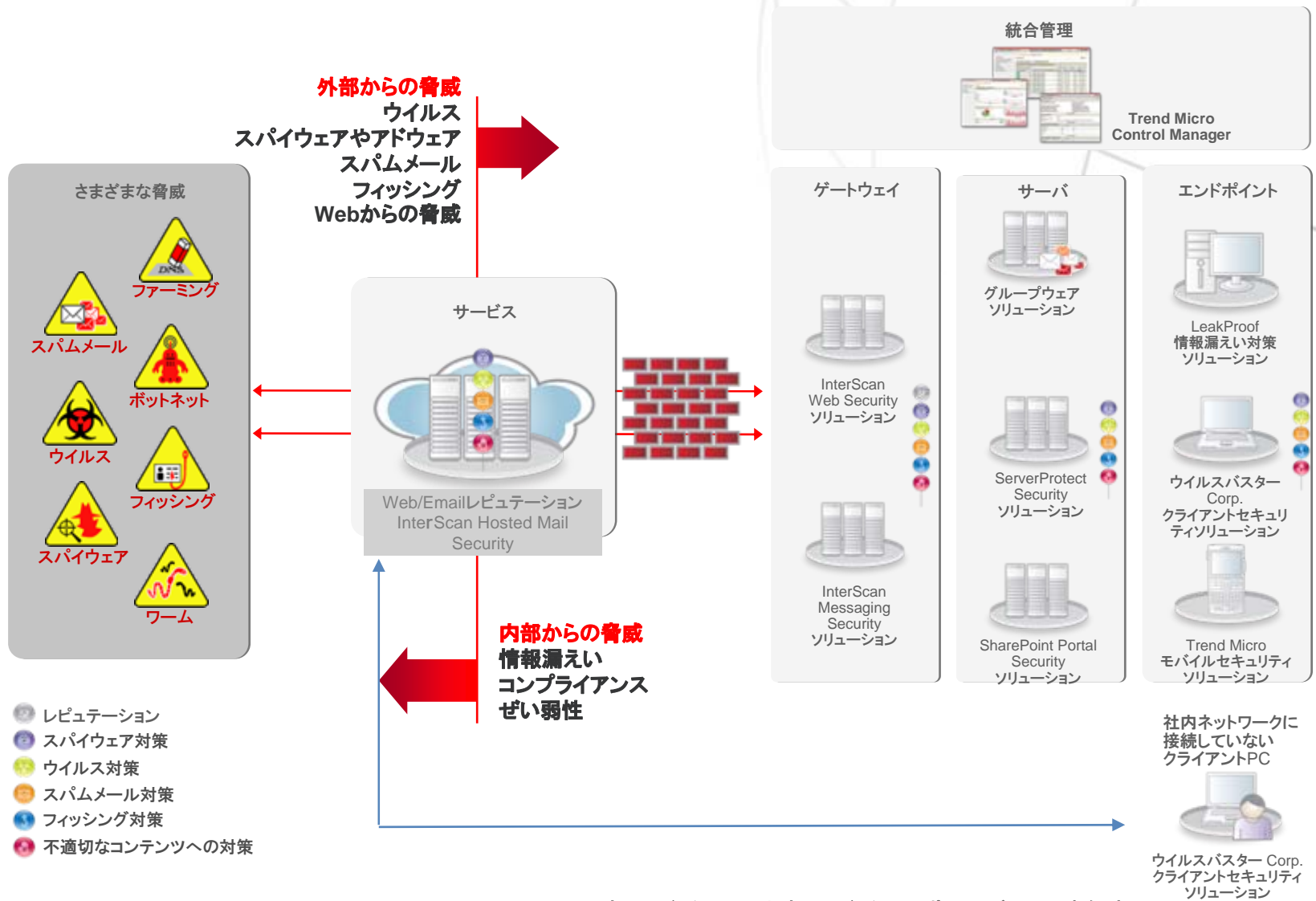
Webセキュリティの概要



- ▶ 一日あたり35億のクエリ
2,000万のインストールベース
99.9999%以上のアップタイム
- ▶ 5つのデータセンタ (US, EMEA, APAC)
150台以上のサーバ
- ▶ Hit rate: 98% out of 1 billion queries/day
誤検知率: 0.00000023%

※TMUFEは、Trend Micro URL Filtering Engineの省略です

複数レイヤーでのセキュリティ対策モデル



※ウイルスバスター Corp.は、ウイルスバスター コーポレートエディションの省略です。

- Webレピュテーションサービス
- Eメールレピュテーションサービス

それを支えているのは:

- ✓ 独自の不正プログラム解析
- ✓ 独自のスパムメール解析
- ✓ 独自のURL解析
- ✓ お客様の環境からのフィードバックのループ
- ✓ ハニーポッドや、Webクローラといったファシリティ



これらの技術がトレンドマイクロ製品に加えて、Sony、Ciscoといったパートナーのソリューションに統合されています。

セキュリティのためのベストプラクティス

安心を、ひとつ上のステージへ。



Webレピュテーション
を利用し、
Webからの脅威の
ネットワークへの侵入
をブロック

ネットワークに接
続されている
ユーザ、接続され
ていないユーザ
の双方を
Webからの脅威
から守る

HTTPのための
不正プログラム、
スパイウェア対
策を利用する

すべてのユーザの
Webアクセスを、
不正プログラム、
スパイウェア対策
ソリューションで検
索し、危険な
コンテンツへの
アクセスを防止す
る

不必要なプロトコル
による
企業ネットワークへ
の侵入を防止する

ボットネットに悪
用される可能性
が非常に高い
P2Pや、IRCと
いったプロトコル
を見直し、
必要であればブ
ロックする

ネットワークに
ぜい弱性診断
のための検索
ソリューション
を導入する

OSおよびその他
アプリケーション
に、最新のパッチ
があたっている
ことを確認する

全ネットワーク
ユーザの権限
を再度見直す

管理者権限は、
本当に必要な
数名に限定する

脅威の動向、
注意すべき点
を利用者に広く
告知するキャン
ペーンを行う

従業員に対して、
空港や自宅、カフェ
でネットワークを
利用する際の危険
性を十分に理解さ
せる



TREND
M I C R O[™]

1988-2008

20

ANNIVERSARY