

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

世の中の現実、今後の動向

第5回 情報セキュリティEXPO

# Cyber Crime:サイバー犯罪

## これが現実

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



## 【世の中の現状】

# サイバー犯罪を助長するアンダーグラウンドマーケット

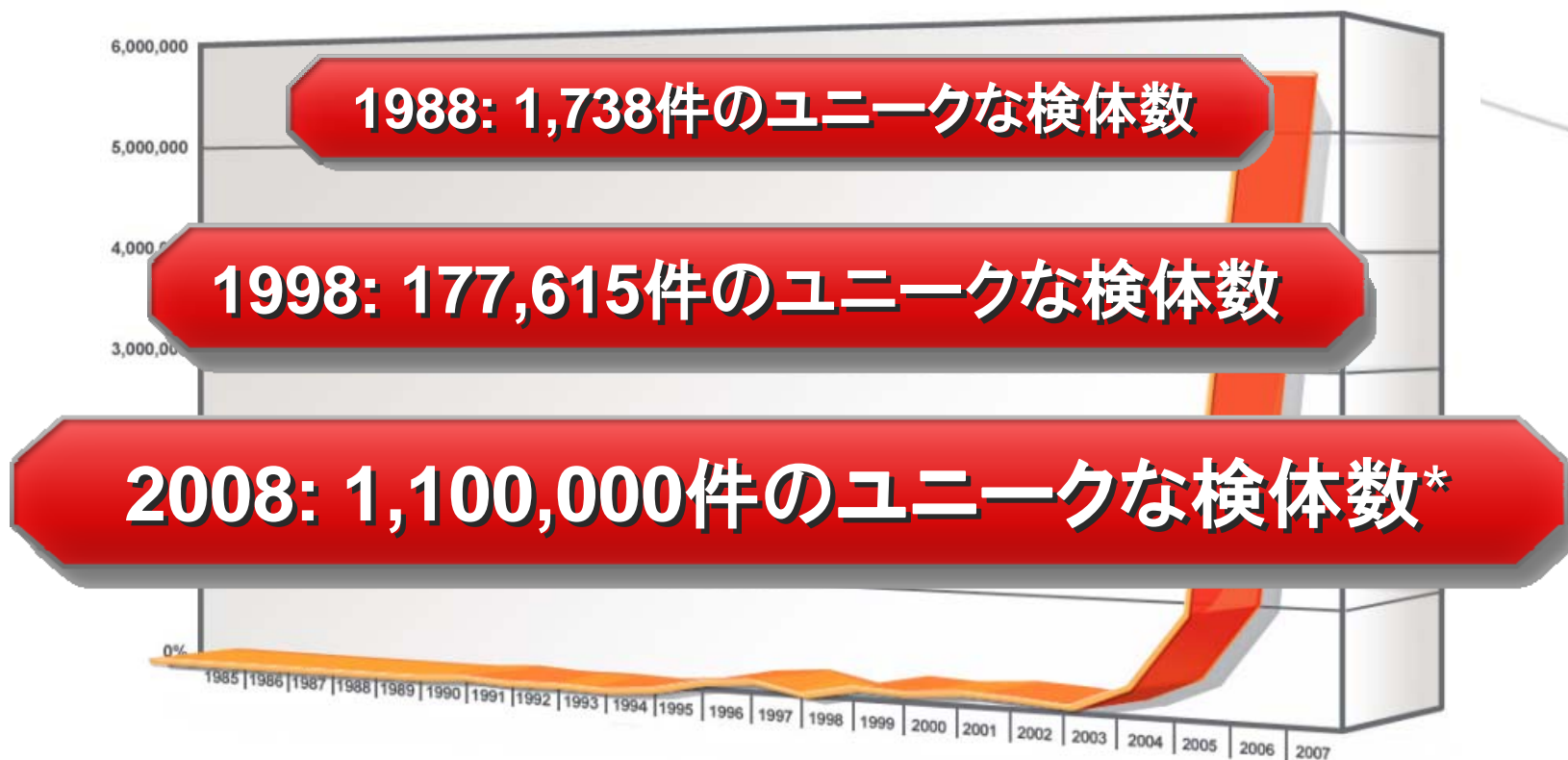
安心も、ひとつ上のステージへ。



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

# 急激な伸びを示す不正プログラムの検体数



Data source: AV-Test.Org, March 2008

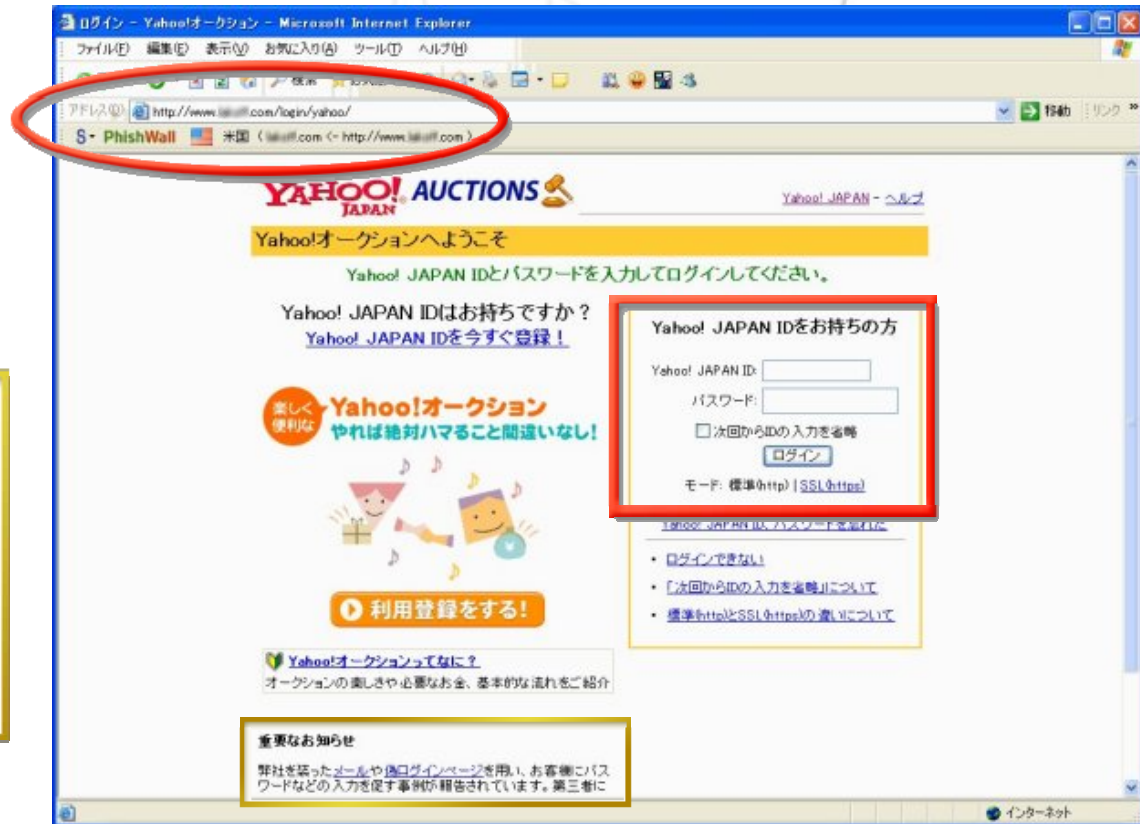
\* = January and February 2008

# 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。...

# 【日本の現状】 感染報告数上位10種



## 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	Webからダウンロード	バックドア	832件	2003年8月
【2位】	TROJ_VUNDO ※①	Webからダウンロード	トロイの木馬	342件	2004年11月
【3位】	JAVA_BYTEVER ※②	Webに埋め込み	その他	277件	2003年5月
【4位】	TROJ_DLOADER ※①	Webからダウンロード	トロイの木馬	245件	2004年7月
【5位】	TROJ_ZLOB ※①	Webからダウンロード	トロイの木馬	230件	2005年11月
【6位】	BKDR_HUPIGON ※①	Webでアップデート	バックドア	214件	2005年2月
【7位】	WORM_RBOT ※①	Webでアップデート	ワーム型	206件	2004年3月
【8位】	WORM_SDBOT ※①	Webでアップデート	ワーム型	204件	2003年10月
【9位】	ADWARE_BESTOFFERS ※①	Webからダウンロード	アドウェア	166件	2006年7月
【10位】	EXPL_ANICMOO ※①	Webからダウンロード	その他	146件	2007年3月

※(※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になります。

※(※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。



# これからのセキュリティ対策のありかたは？



これまでにないスピードで増加する不正プログラム

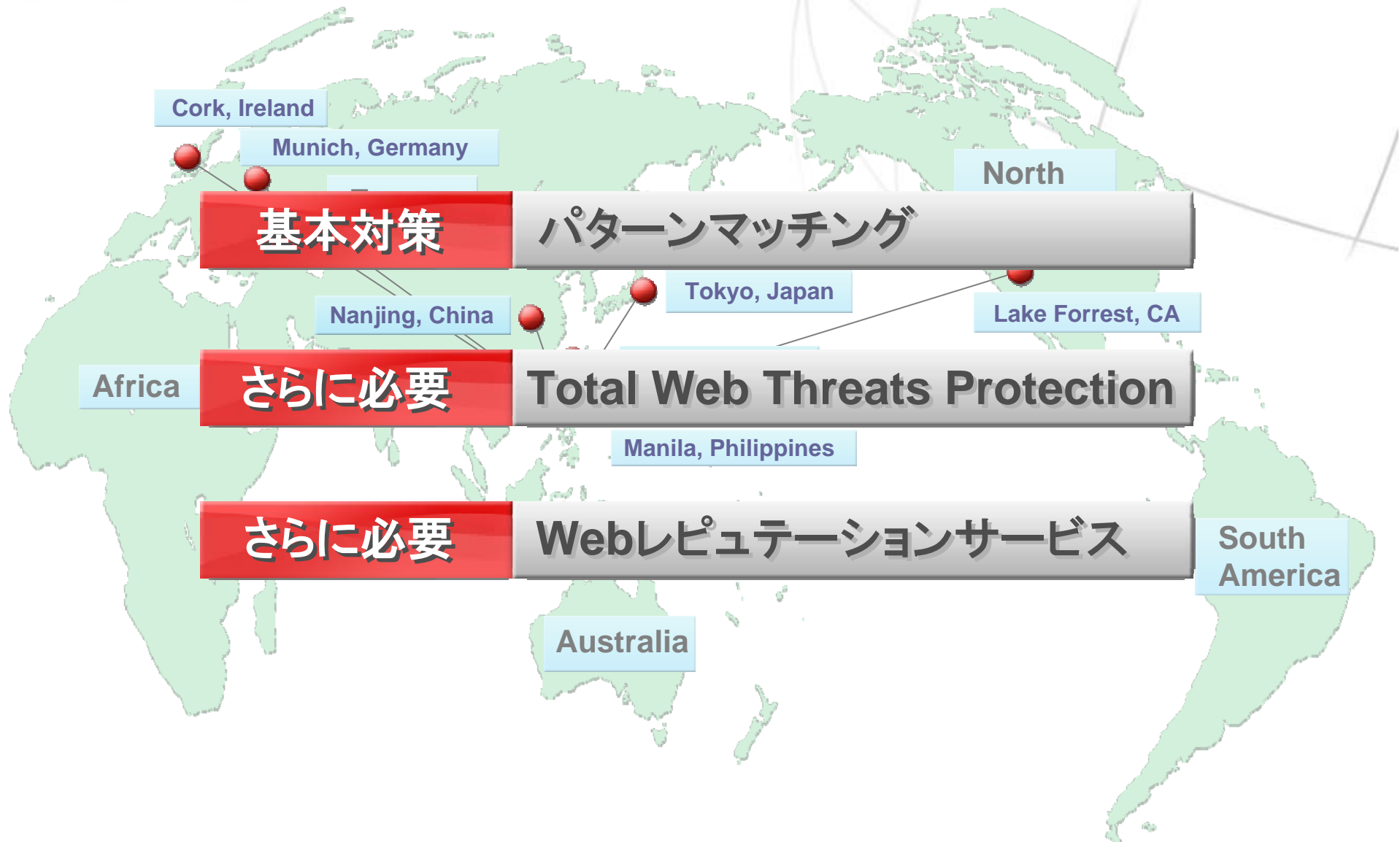
肥大化するパターンファイル、増えるパターンファイル配信回数

お客様のネットワークへの負荷の増大

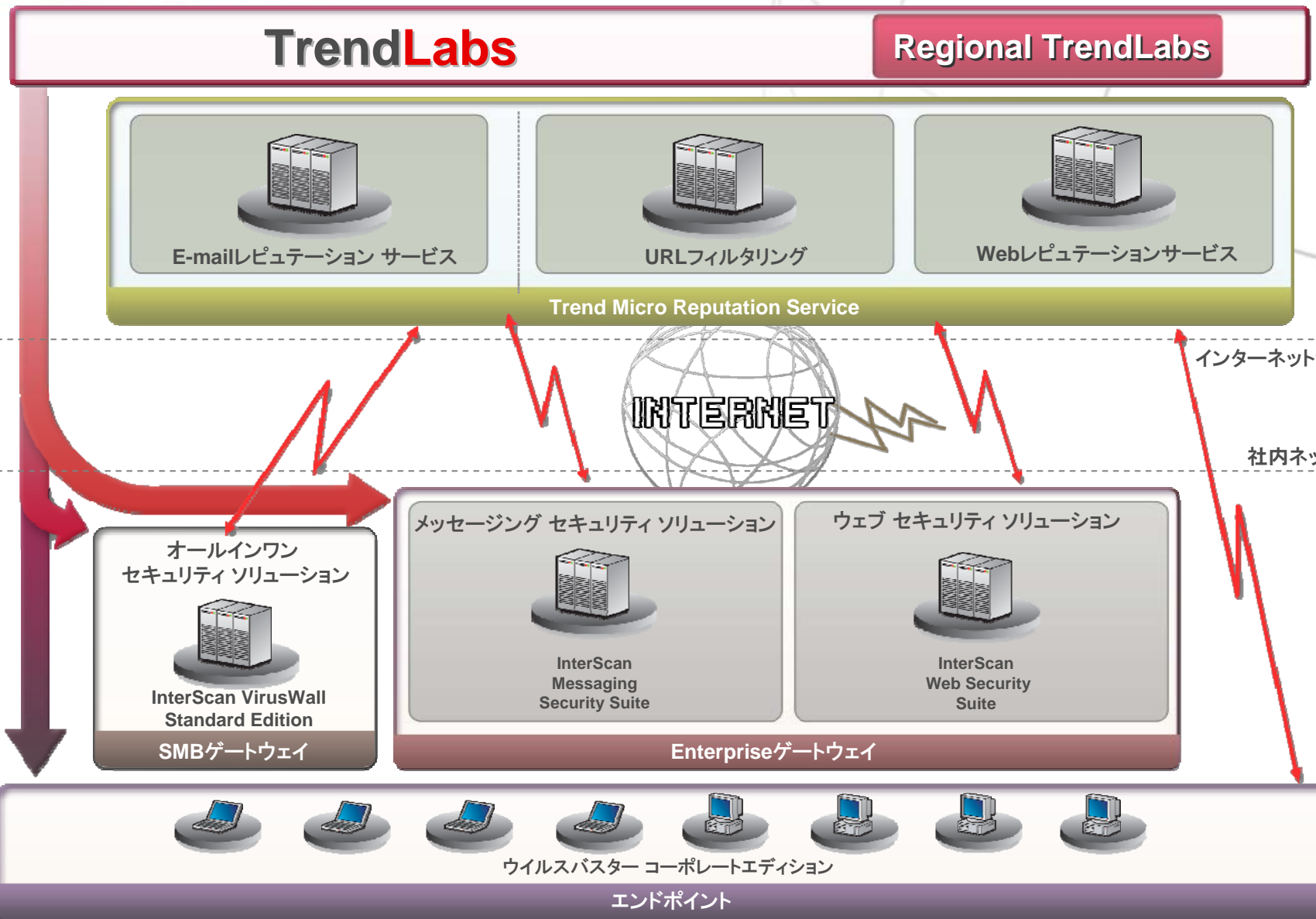


現行のパターンファイルに依存したソリューションを補完する、  
新たなアプローチが必要に。

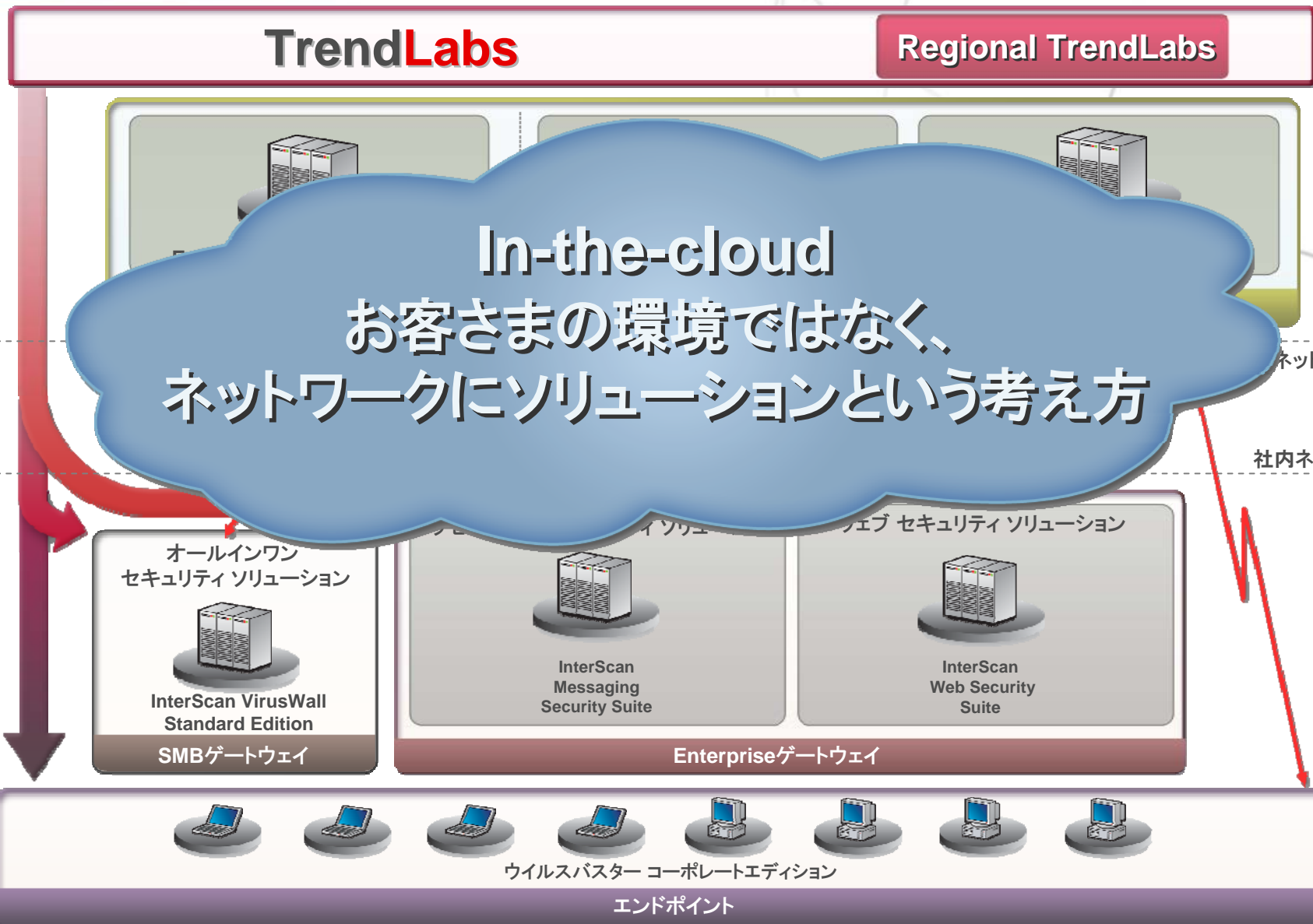
# トレンドマイクロの取り組み



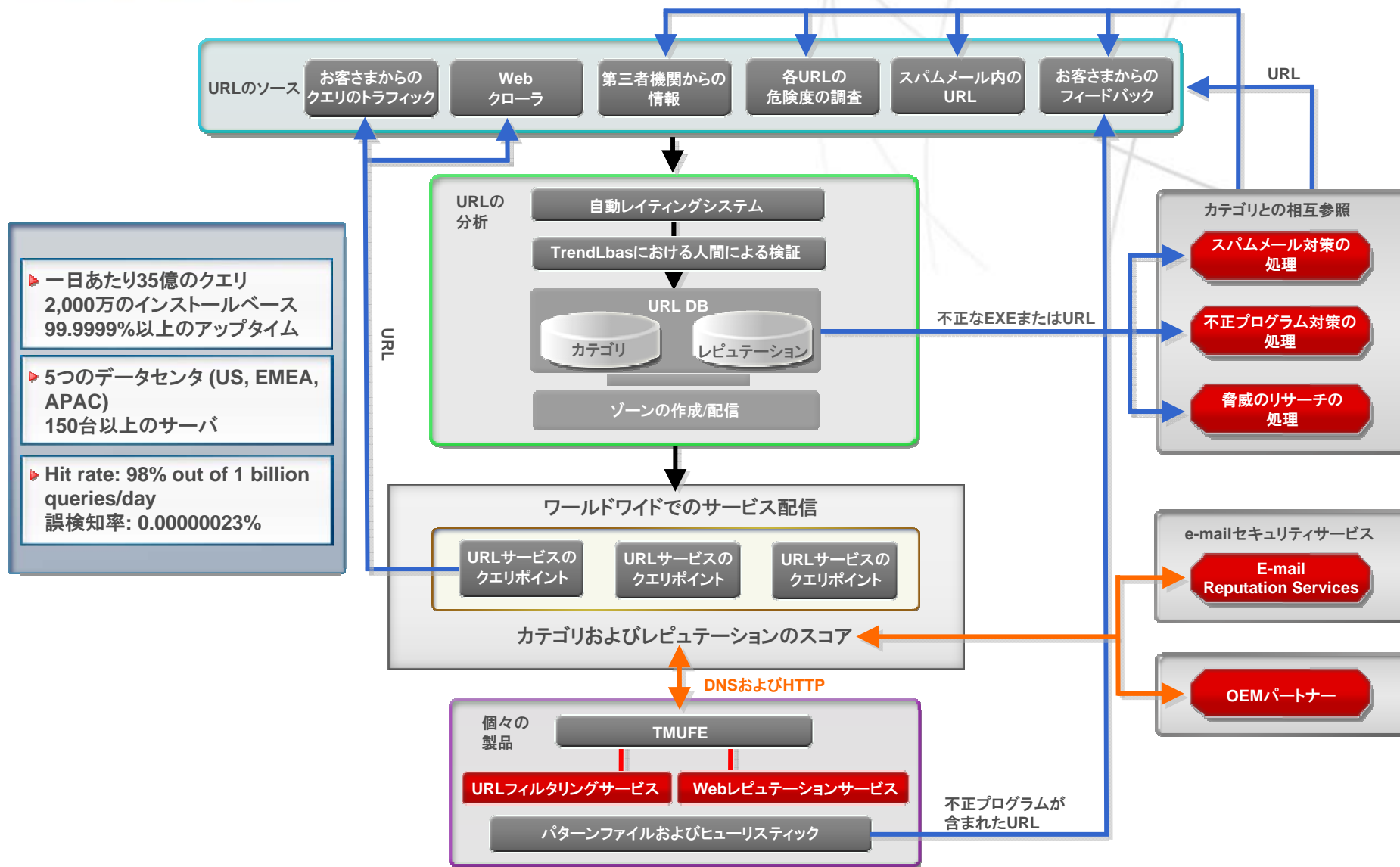
# Total Web Threats Protection



# Total Web Threats Protection

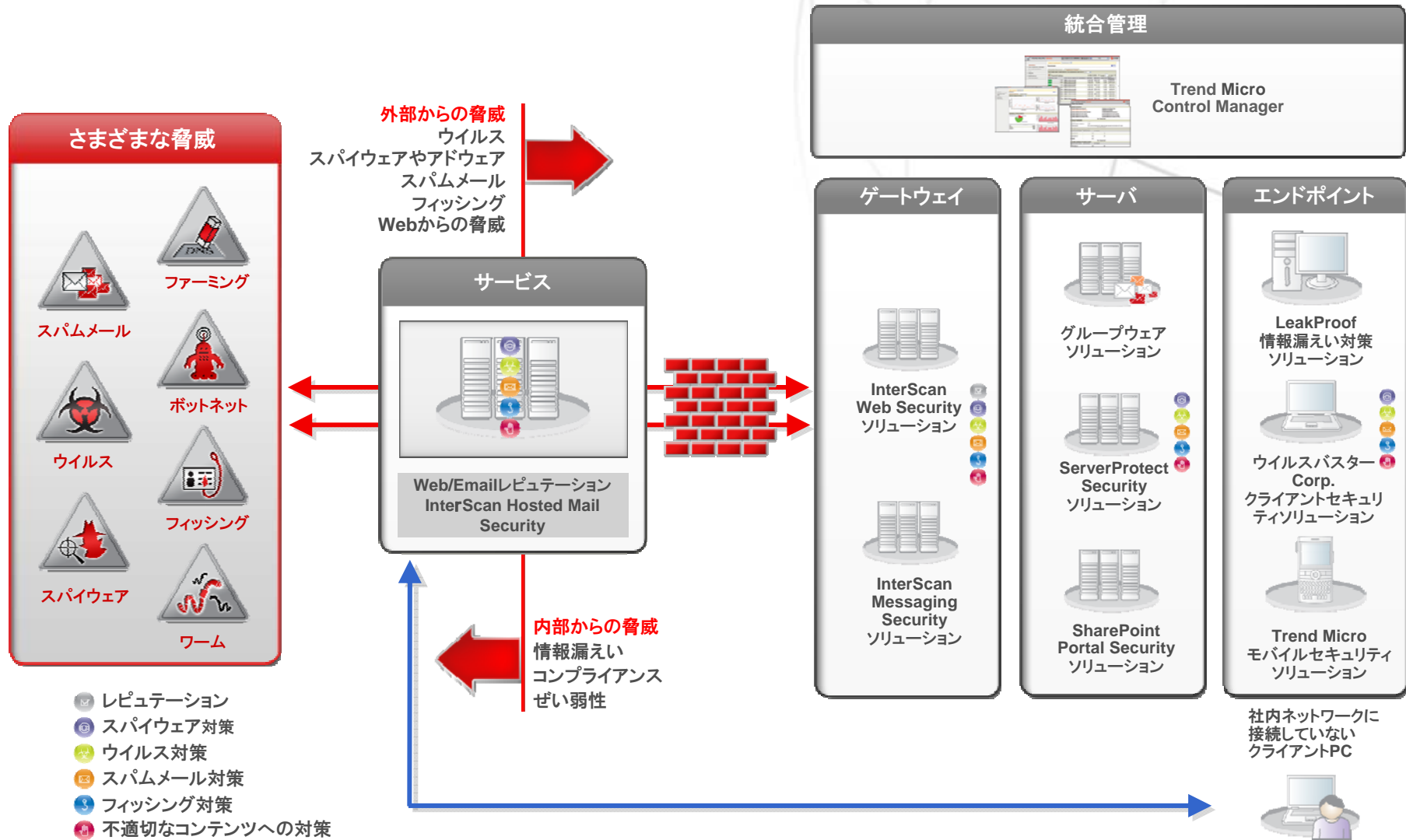


# Webレピュテーションサービスの概要



※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。

ウイルスバスター Corp.  
クライアントセキュリティ  
ソリューション

# SaaS型メールセキュリティ

トレンドマイクロのSaaS型メールセキュリティを利用するに  
当たって、追加でハードウェアやソフトウェアは必要ありません。



example.comへの  
メール

メールはまずIMHSを  
通過します

メールは検索後、スパムメール  
は隔離、感染メールは削除され、  
実際のexample.comに必要な  
メールが届きます

メールのリダイレクトだけで、不正プログラム対策、スパムメール対策を提供



**TREND**  
**M I C R O**<sup>TM</sup>

1988-2008

**20**

ANNIVERSARY