

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。



セキュリティインシデントへの取組みと事例 ～事例、Webからの脅威～

トレンドマイクロ 株式会社
サポートサービス本部
コアテクノロジーサポートグループ
Threat Monitoring Center
マネージャー
平原 伸昭

1. 脅威の変化とその背景について
2. スレットモニタリングから見た脅威
3. 実例、Webからの脅威
4. インシデントレスポンスから
インシデントオペレーションへ

安心を、ひとつ上のステージへ。



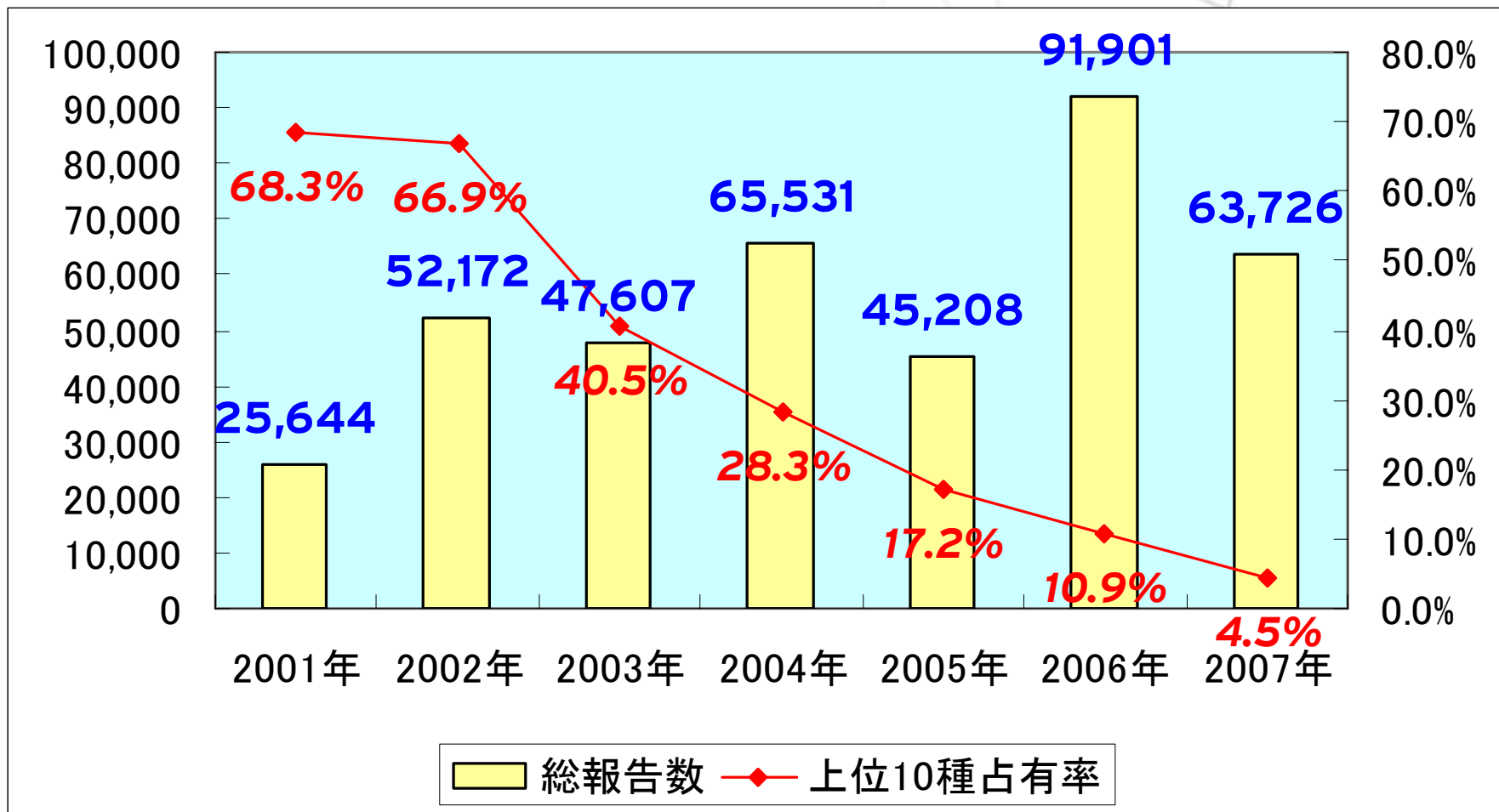
安心を、ひとつ上のステージへ。



脅威の変化とその背景について

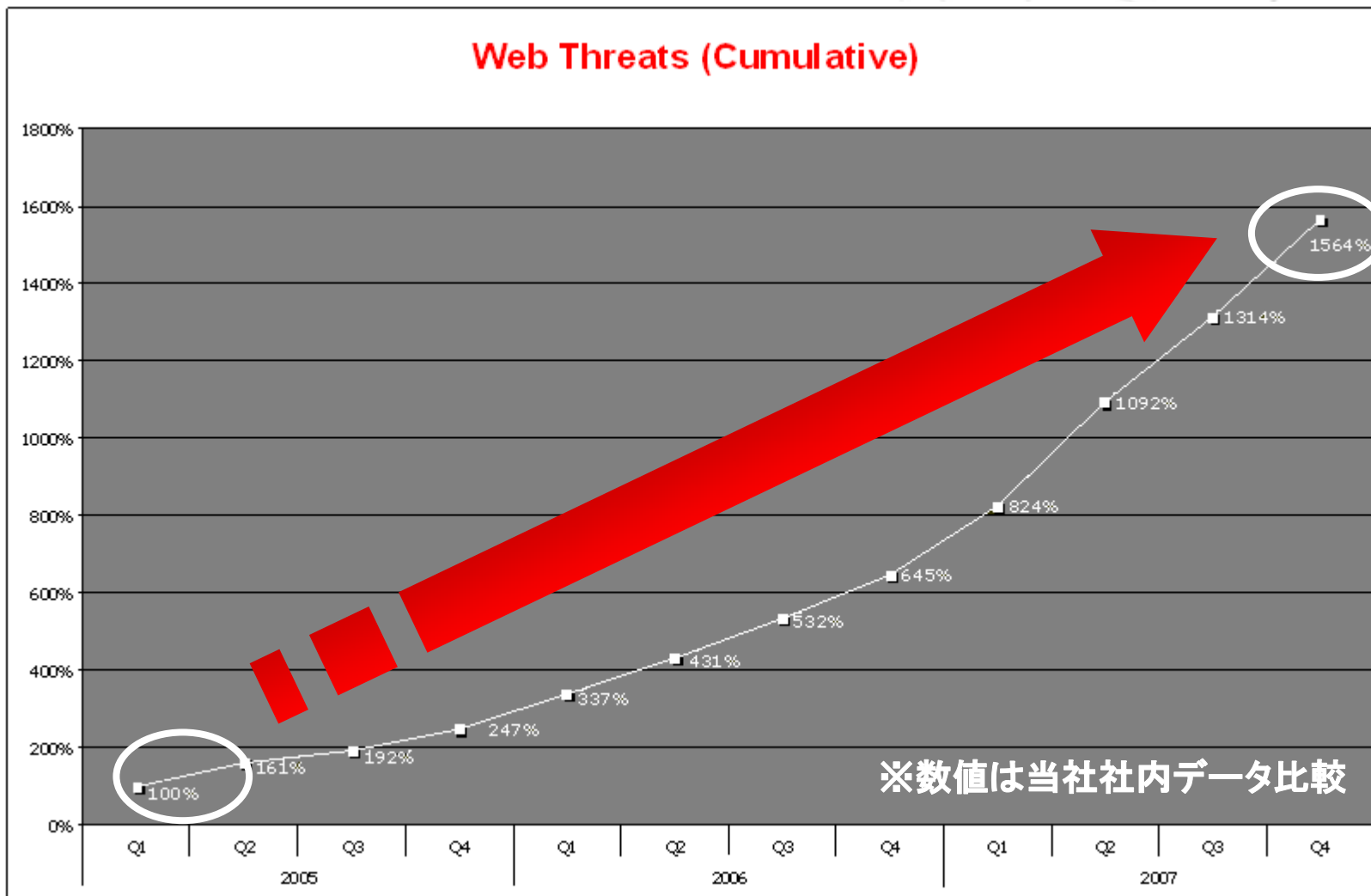
感染被害の分散化

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)

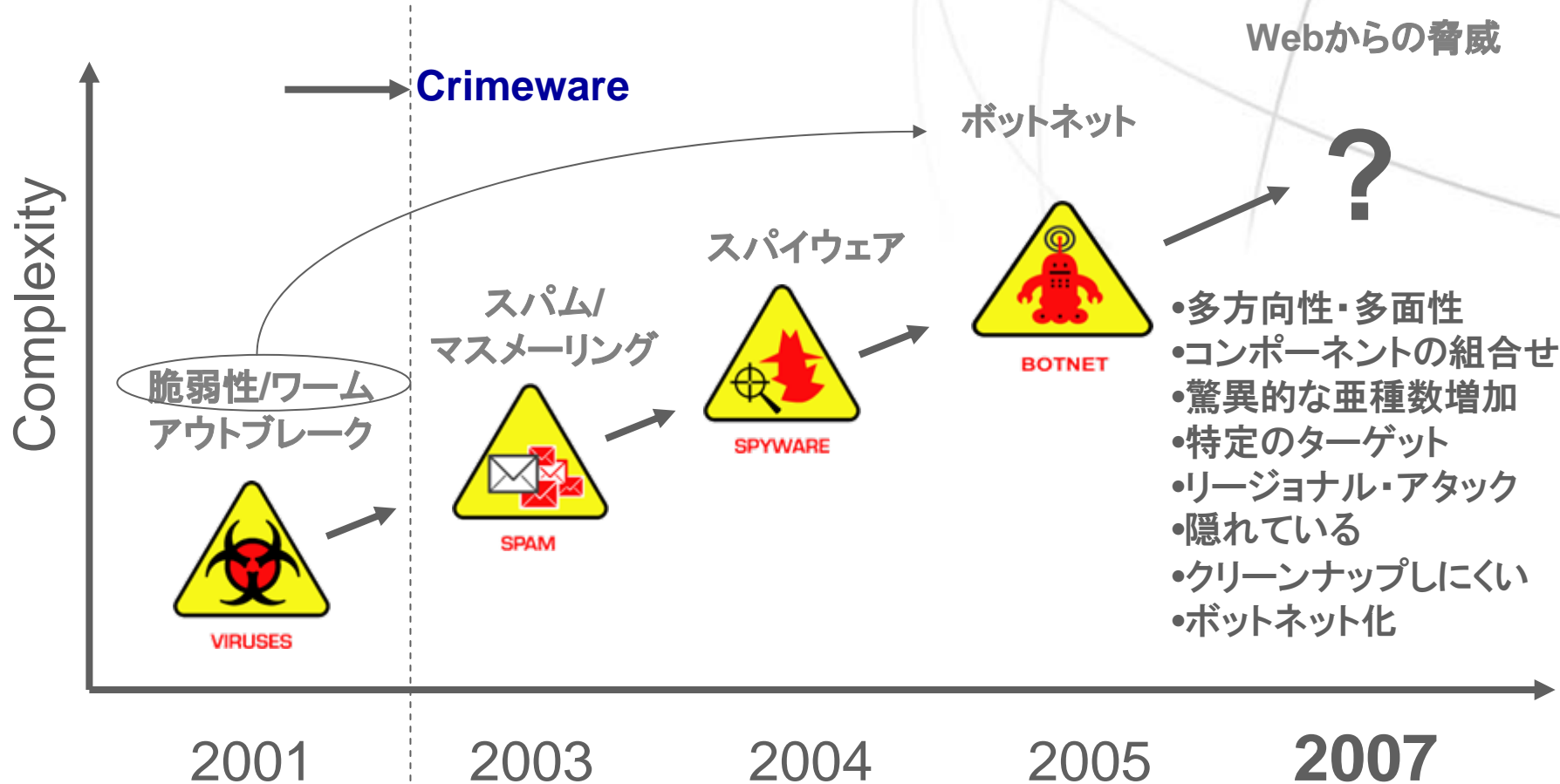


Webからの脅威の増加

「Webからの脅威」に分類される検体数は2005年Q1の15倍に!



脅威の変遷-犯罪化は2003年頃から



Webからの脅威とは？

- インターネットには「人々の興味」が溢れている。
 - クリックせずにはいられない。
- 安全なはずのサイトが「改ざん」により危険なサイト化してしまう。
 - サイトの”信用度”だけで安心できない。
- 攻撃の手口は巧妙かつ複雑。
 - 専門家でもそれが「脅威」であることがわかりにくい。
- 何か一つに注意していれば安全ということは通用しなくなった。
 - インターネットに関わる全てが脅威に晒されている。
- 必ずしも狙われた人が最終目的とは限らない。
 - 犯罪の全貌が把握しにくい。

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。



スレットモニタリングから見た脅威

•24時間365日体制のウイルス解析・サポートセンター

- ウイルス解析&パターンファイル作成
- トレンドマイクロ エキスパートサービス 運用監視センター
- カスタマーサポート

•フィリピンを中心に世界7拠点、1,000名以上のスタッフで構成



“地域密着型”トレンドラボの設立

地域に特化した脅威情報を積極的に収集し、
国内独自のソリューションを提供することにより
ターゲット攻撃へ迅速な対応を実現
※日本では2007年5月から本格稼働



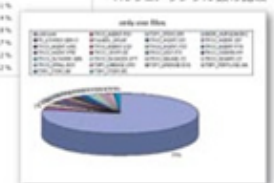
主な活動内容

- トレンドマイクロ セキュリティブログによる情報提供
- トレンドマイクロ エキスパートサービス 運用監視センター
- 不正プログラムのサンプル(検体)収集
- 不正プログラムの解析

ハニーポットによるモニタリングシステム



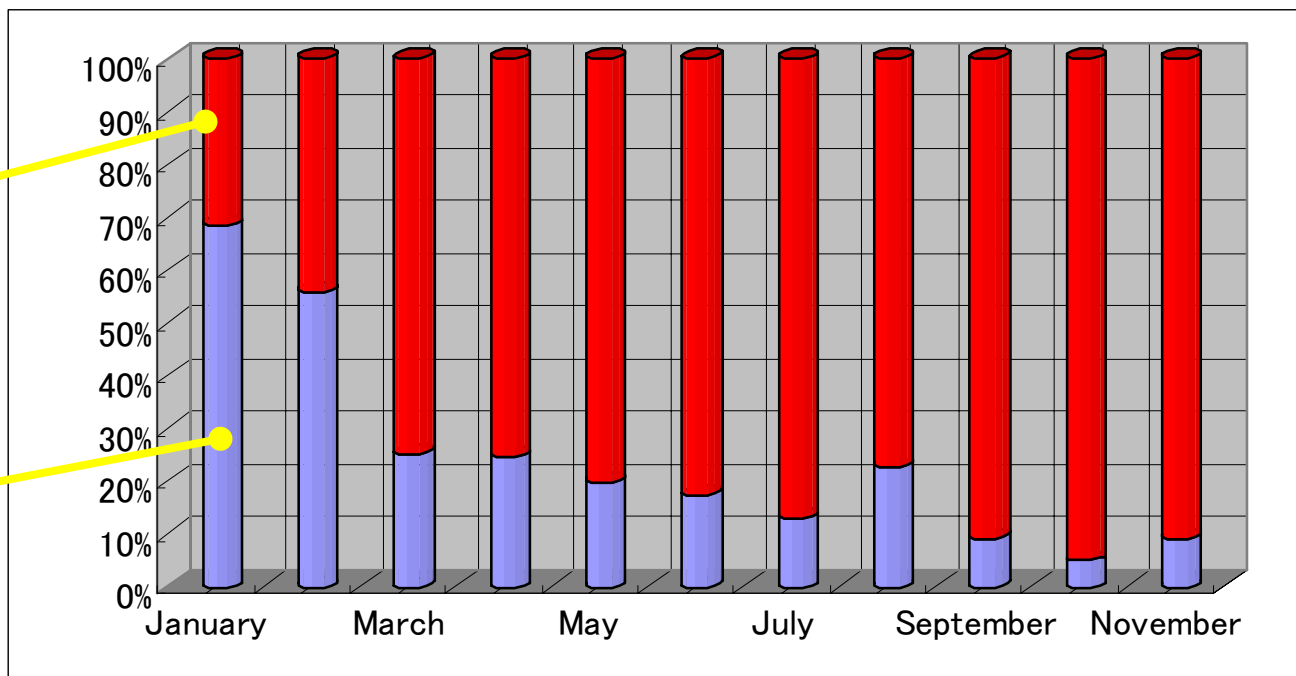
マルウェアサンプル数の比較



不正プログラムのサンプル(検体)収集

- 日本国内におけるお客様からの検体提供と、検体収集システム(おとり調査)を利用したプロアクティブな検体収集の比率が逆転
- 90%以上がプロアクティブな検体収集による(2007年11月現在)
- 新しい不正プログラムは1日平均450種(2007年9月~11月平均値)

検体数の入手経路別の比較(2007年1月~11月)



プロアクティブな
検体収集

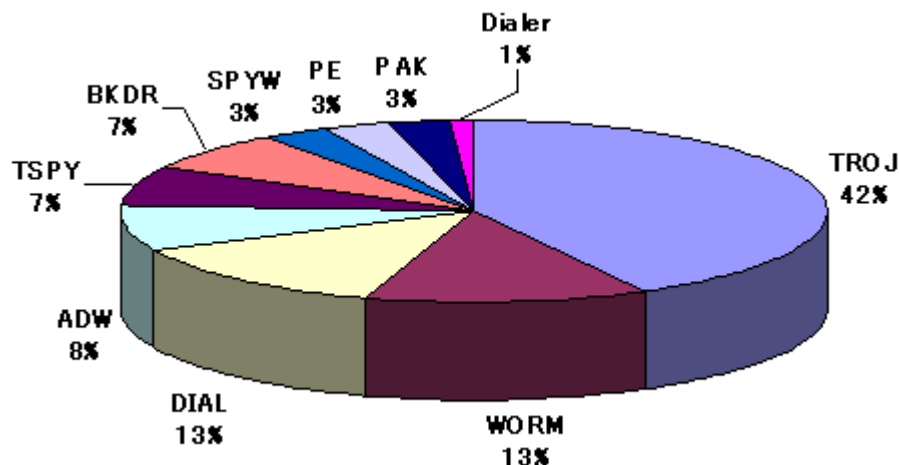
お客様からの
検体提供

収集したサンプル(検体)の内訳

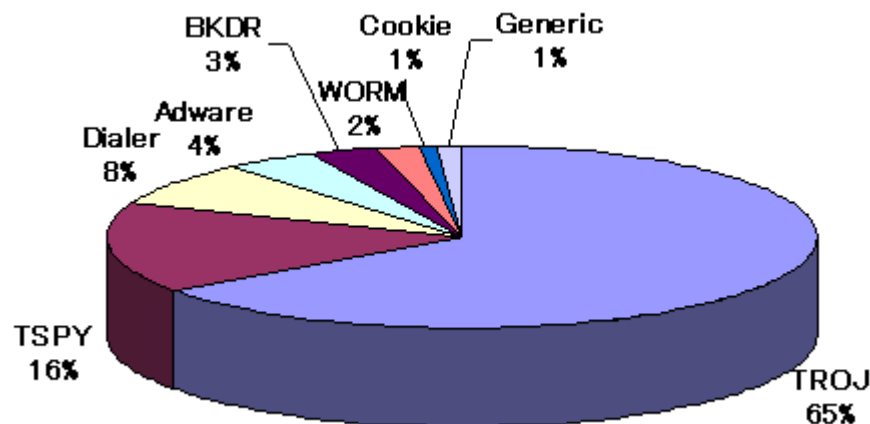
ネットワーク上で流通している不正プログラムは
TROJ(42%)に続き、**WORM(13%)**が占める

しかし、新種に限った場合、
TROJ、TSPY、Dialer、Adware、BKDRの**トップ5種で96%**
 にのぼり、これらの大半がHTTP経由での感染経路を持つ。

収集検体の接頭語別比較【全体】
 (2007年7月)



収集検体の接頭語別比較【新種のみ】
 (2007年7月)



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。



実例、Webからの脅威

実例、Webからの脅威

この事例は、2月4日から2月8日にかけてITproに連載された「Webからの脅威と戦った24時間—インシデント対応の現場から—」で紹介したものをベースに説明します。

Webからの脅威と戦った24時間— インシデント対応の現場から —

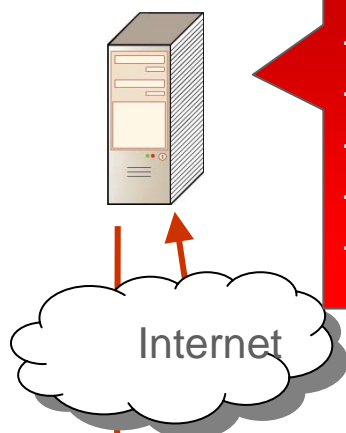
http://itpro.nikkeibp.co.jp/article/COLUMN/20080128/292230/?ST=web_threat

A社が被害にあった不正プログラム

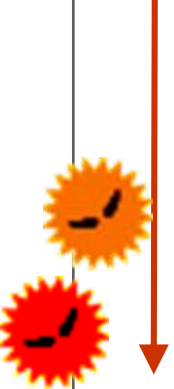
BKDR_AGENT
 TROJ_AGENT
 TSPY_AGENT
 TROJ_LEG MIR
 TSPY_LINEAGE
 TSPY_ONLINEGA など

ワーム活動

同一ネットワーク上の他のPCに対し、共有フォルダ (admin\$, ipc\$) をターゲットにし感染活動を行う。



ダウンロード活動



Svhost32.exe
 dxdiag.com



ドロップ

vDll.dll (TROJ_LOOKED.AB)

ファイル感染

C:~Z: ドライブ内の
 すべての .exe ファイルに感染

PE_LOOKED

PE_LOOKED



まず始めに管理者がすべき4つのポイント

1. 悪意のあるファイルの発見
2. 感染コンピュータ環境の把握
3. 発生している被害の把握
4. 感染原因、経路の特定

The screenshot displays a network analysis environment. On the left, a command prompt shows the execution of `netstat -nb`, listing established HTTP connections from Lab01:1146 to Lab01:1150. In the center, Wireshark captures network traffic, with a filter set to `tcp`. The packet list shows several TCP segments and one HTTP GET request. On the right, the Trend Micro SIC (System Information Collector) v3.1 interface is visible, showing a progress bar and a list of tasks being performed, such as 'Retrieving User Information' and 'Retrieving System Information'. A console window in the foreground shows the output of `SICWin.exe /console`, listing various system details being collected.

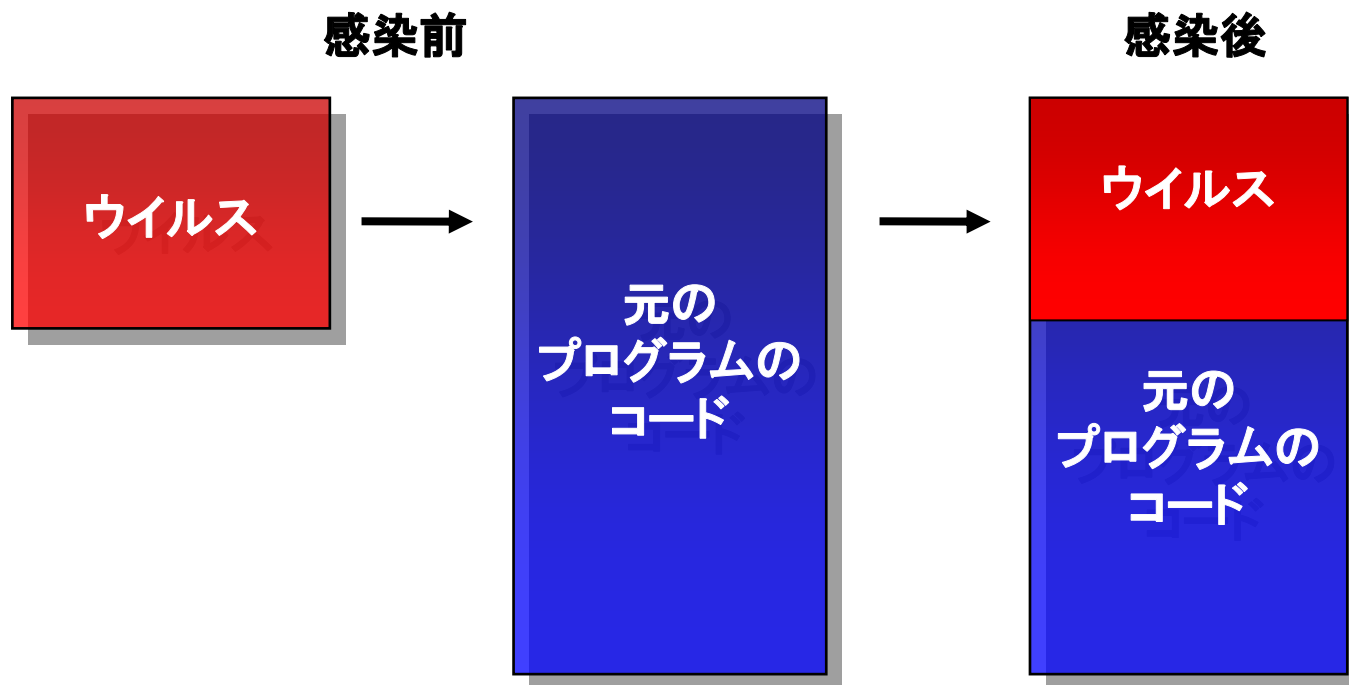
トリアージによる修復端末の優先度

•不正プログラムが**感染**したコンピュータシステムをセキュリティ対策製品により完全に復旧できるとは限らない。

カテゴリー	災害医療等における判定	セキュリティインシデントにおける判定
黒 (Black Tag) カテゴリー0	死亡、もしくは救命に現況以上の救命資 機材・人員を必要とし救命不可能なもの。	上書き感染型に感染し駆除作業が不可能な 状態になったファイルを含むコンピュータシ ステム
赤 (Red Tag) カテゴリーI	生命に関わる重篤な状態で一刻も早い処 置が必要で救命の可能性のあるもの。	上書き感染型以外のファイル感染型に感染 し駆除作業に時間がかかる状態になったフ ァイルを含むコンピュータシステム
黄 (Yellow Tag) カテゴリーII	今すぐに生命に関わる重篤な状態ではな いが、早期に処置が必要なもの。	トロイの木馬、ワームなど1個の不正プログラ ムに感染した状態のコンピュータシステム
緑 (Green Tag) カテゴリーIII	救急での搬送の必要がない軽症なもの。	現時点で感染の疑いはないが近接ネット ワークに不正プログラムの感染が確認されて いるコンピュータシステム

セキュリティ対策製品では復旧できない例

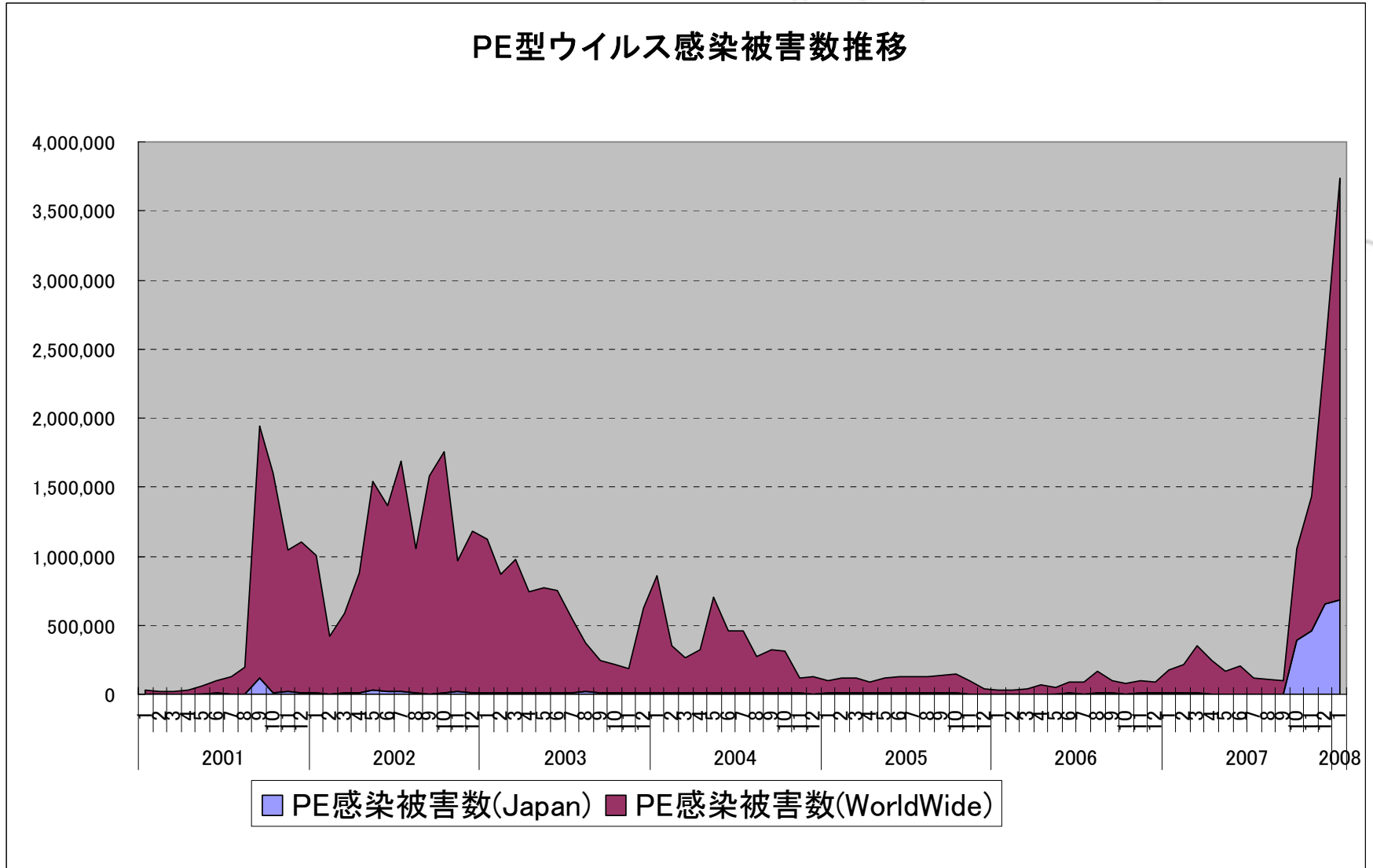
- 元のプログラムのコードの一部またはすべてを上書きし、元のプログラムを破壊し感染を行う**上書き感染型 (Overwrite)**のファイル感染型不正プログラム



ファイル感染型ウイルスの復権



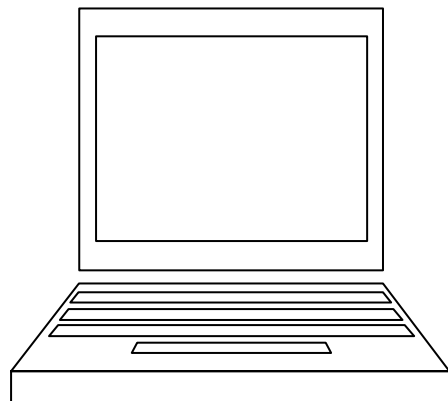
PE型ウイルス感染被害数推移



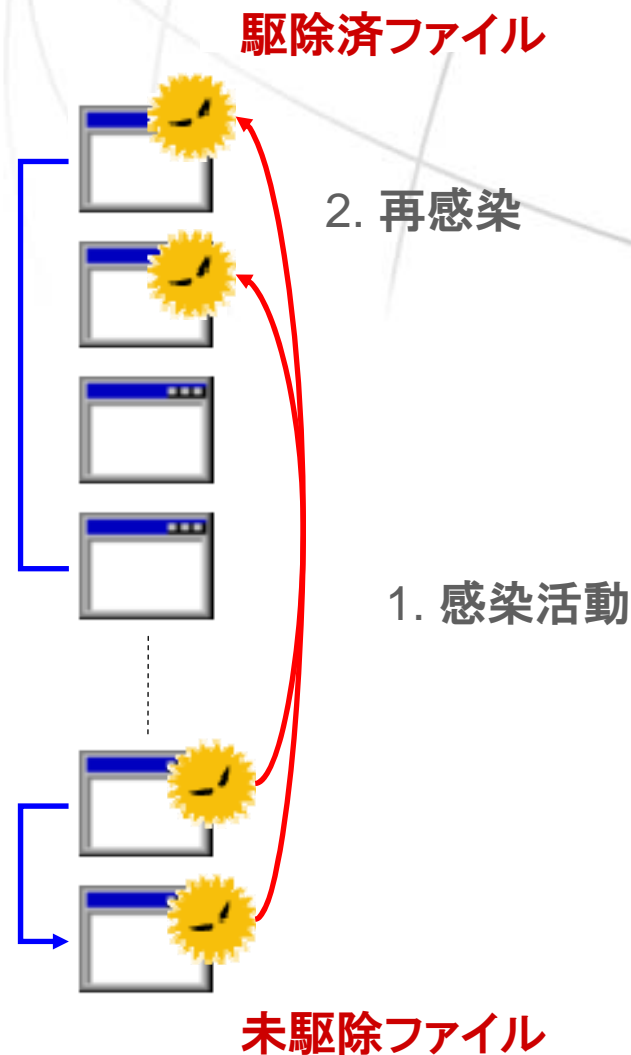
対応の現場で起こりうる落とし穴

1. 許可されていないインターネット回線
2. ウイルス対策製品が入っていない
3. 最新のパターンファイルが適用されていない
4. 何度修復しても検出、駆除を繰り返す

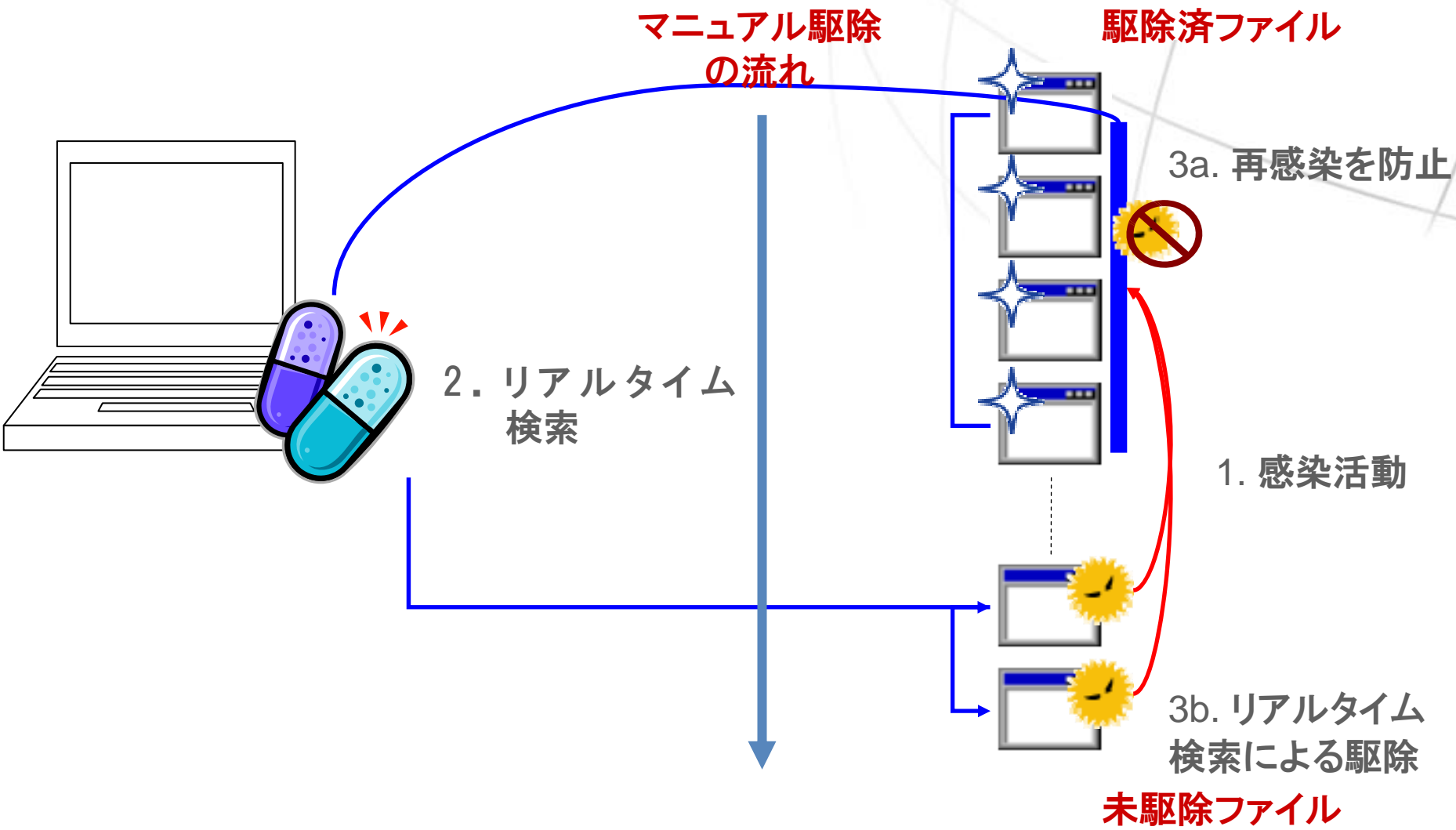
何度修復しても検出、駆除を繰り返す



マニュアル駆除
の流れ



何度修復しても検出、駆除を繰り返す



本インシデントを振り返って

良かった事

- ・有事におけるサポート体制の構築(プレミアムサポート契約)
- ・インシデント発生時における社内の雰囲気
- ・修復端末の優先度決定における柔軟性

悪かった事

- ・従来のセキュリティ対策製品のみを導入で安心
- ・情報システム部門の横連携
- ・セキュリティポリシー, ガイドラインの周知徹底

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。



インシデントレスポンスから インシデントオペレーションへ

営業機会損出暫定被害額

暫定被害額 = 1時間当たりの売上 × ダウン時間 × 影響度

1時間当たりの売上 = 年間売上 ÷ 営業時間(営業日 × 8)

影響度 = 被害クライアント数 ÷ 全クライアント数

年間売上 300億円、240営業日の企業において、
全クライアント数1,000台のうち20%がWebからの脅威に
感染したインシデントが年に1度発生した例：
1時間当たりの売上 = 1,562万

仮に上記例でダウン時間 72時間で計算した
場合の暫定被害額 = 2億2,492万円

レスポンスとオペレーションの違い

インシデントレスポンス

- インシデントが発生した際の事後対応
- リアクティブ(受動的)な対応

インシデントオペレーション

- インシデントが発生しないための対応
- プロアクティブ(能動的)な対応

1. 問題に関する患者および家族が直接提供する訴えなどの主観的情報(Subjective data; S)
2. 観察や検査などにより医師や看護師などの専門職が取り出す客観的情報(Objective data; O)
3. ①と②を分析してその問題が解決に近づいているか否かを判断する(Assessment; A)
4. ④ ③に基づいて行った計画の実施、計画の続行、修正の有無(Plan; P)の順に記載される。

SOAP方式 – インシデントオペレーション

- 1. 主観的情報**「いくつかの業務アプリケーションにおいて起動不可になるアプリケーションや、起動はするが途中でエラー・メッセージが表示されて終了してしまうアプリケーションがある」
- 2. 客観的情報の収集**は、SIC(シック)ツールやその他ネットワーク・プロトコル・アナライザなど情報採取ツールを使用しての情報収集活動
- 3. 情報の分析**(Assessment; A)とは、①と②で収集した情報の分析。動的解析手法や静的解析手法
- 4. 問題解決のための計画立案と実行**は、③で得た情報を基に感染被害の最小化または局所化や修復作業の展開

セキュリティインシデントへの取組み

Trend Micro
Expert Service
Expert on Guard

24時間365日のモニタリング
専門的なレポート

Total
Discovery
Solution

効果的な製品連携
振舞検知ソリューション

Trend Micro Premium
Support Service

柔軟できめ細かい
製品サポートを提供

トレンドマイクロが蓄積してきた
専門性、ナレッジを様々な方法で
お客様に提供する

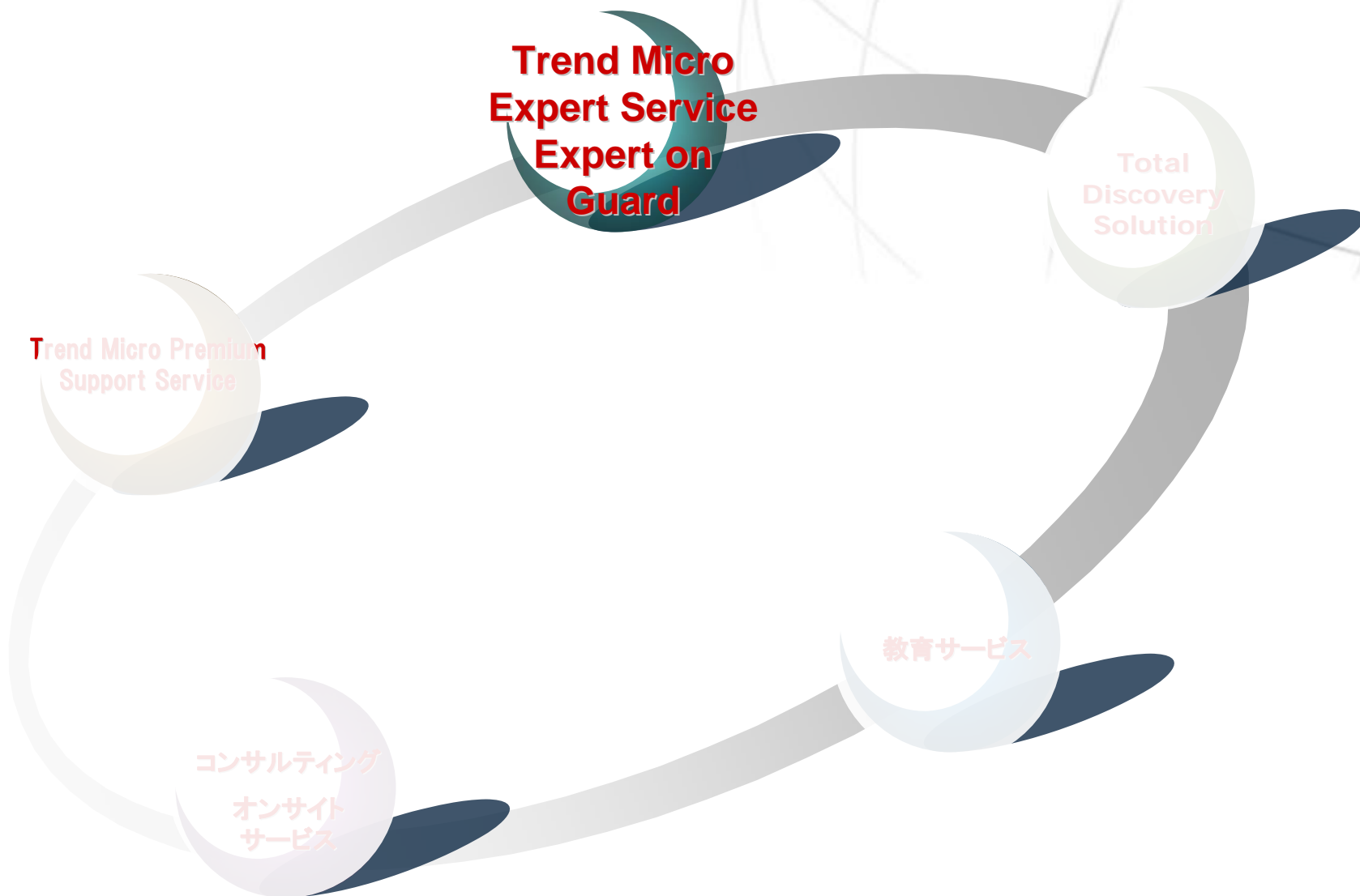
教育サービス

専門知識をわかりやすい
コンテンツで提供
お客様社内のエキスパート育成支援

コンサルティング
サービス

効果的な導入プランの提案と
万が一の場合の迅速かつ柔軟な対応

セキュリティインシデントへの取組み



Trend Micro Expert Service (TMES)は

- ☑ 「診断(Diagnose)」
- ☑ 「企画(Plan)」
- ☑ 「実施(Enable)」
- ☑ 「レビュー(Review)」

のPDCAサイクルを網羅したトレンドマイクロのサービスフレームワークです。



Expert on Guard(EoG)は、TMESの中核をなすサービスで、お客様のウイルス対策状況を24時間365日モニタリングし、ウイルス感染を始めとするさまざまな脅威に迅速に対応します。また専門のアナリストによる分析レポートで、ウイルス対策の有効性、今後強化すべきポイントを明確に把握する事ができます。



モニタリング
サービス

1. モニタリングサービス

- ・ 24時間365日常時モニタリング
- ・ 国内に設立したウイルス研究機関「Regional Trend LAB」と連携した早期ウイルス感染対応ソリューション



事前対策情報

ソリューション提供

2. 事前対策情報・ソリューション提供

- ・ 大規模感染を予防する迅速な情報通知サービス
- ・ 効果的な対策の事前提言
- ・ 柔軟性のあるパターンファイルリリース
- TrendMicro Premium Service(TPS)との連携



レポートینگ
アドバイス

3. レポートینگ&マネージメントアドバイス

- ・ オペレーションマネージメントレポート
- ・ トレンドマイクロの専門家による提言



TREND
M I C R O[™]

1988-2008

20

ANNIVERSARY