サイバー攻撃対策は『企業内通信の可視化』がポイント！
～海外拠点をも可視化する Deep Discovery Inspectorの先進的手法～

トレンドマイクロ株式会社
エンタープライズSE部　パートナーSE課
担当課長代理　栃沢　直樹

2013年10月22日

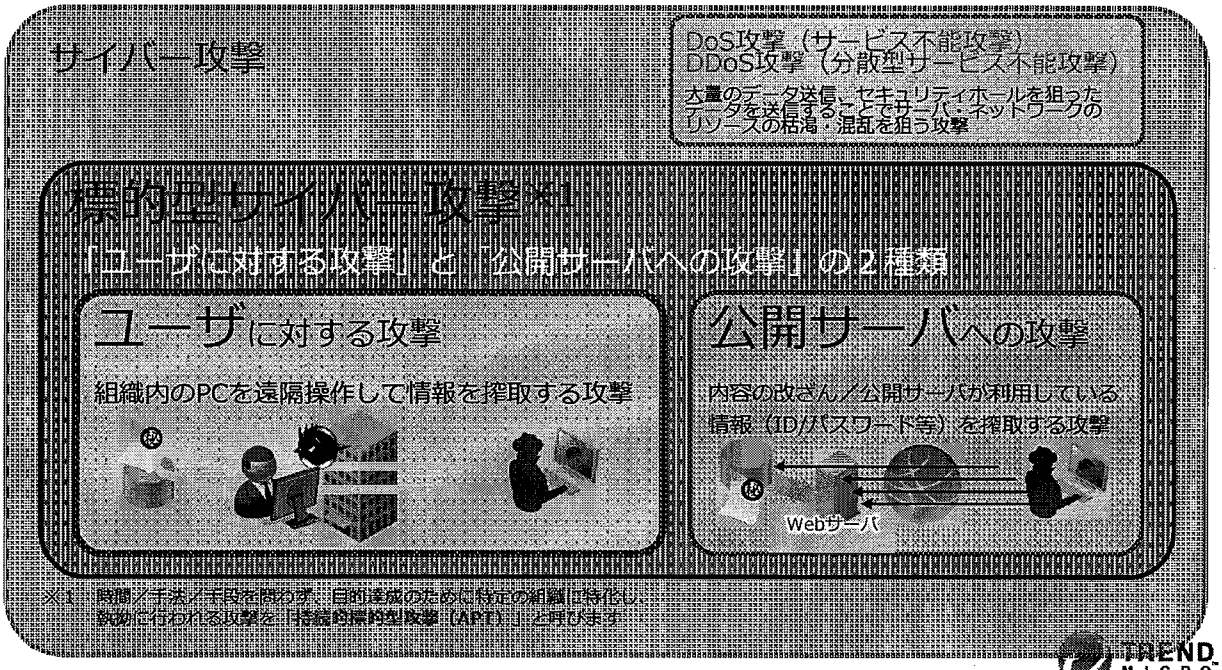
今日のセッションでお伝えしたいこと

- 標的型サイバー攻撃とは（おさらい）
- 標的型サイバー攻撃の最近の動向
- 昨今の脅威事例から見えてくること
- 標的型サイバー攻撃への対策のポイント
  ～ Deep Security Inspector 3.5
- 標的型サイバー攻撃対策を考える上で

標的型サイバー攻撃とは？（おさらい）

攻撃の手法を大別してみると

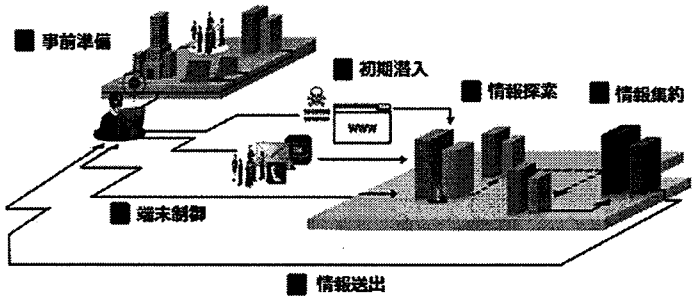
- **特定の組織や個人**に対して行われる
- **個人情報や技術情報**などの知的財産、金銭的利益や破壊行為が目的



持続的標的型攻撃とは？

特定組織に対し、**時間、手段、手法を問わず**、目的達成に向け、その標的に特化して行われる一連の攻撃

持続的標的型攻撃の攻撃段階

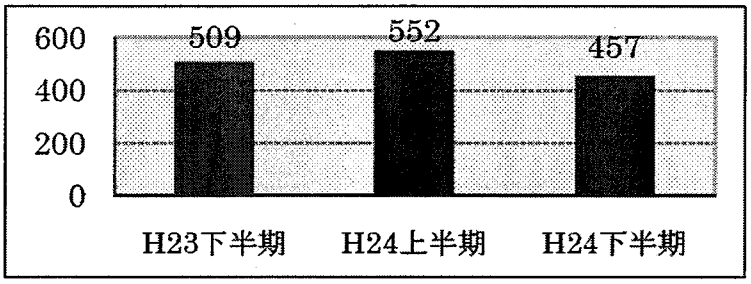


1	事前準備	攻撃先決定、偵察、初期潜入用不正プログラム準備、C&Cサーバ準備
2	初期潜入	メール送信、受信者による添付不正プログラム実行
3	端末制御	感染環境確認
4	情報探索	内部活動ツール送出、LAN内情報探索
5	情報集約	有益情報の収集
6	情報送出	収集情報の入手

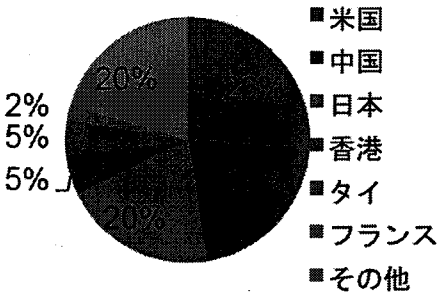
TREND MICRO

標的型サイバー攻撃の最近の動向

標的型メールによるユーザに対する攻撃の動向



【サイバーインテリジェンス情報共有ネットワーク
等を通じて警察が把握した標的型メール攻撃の件数】



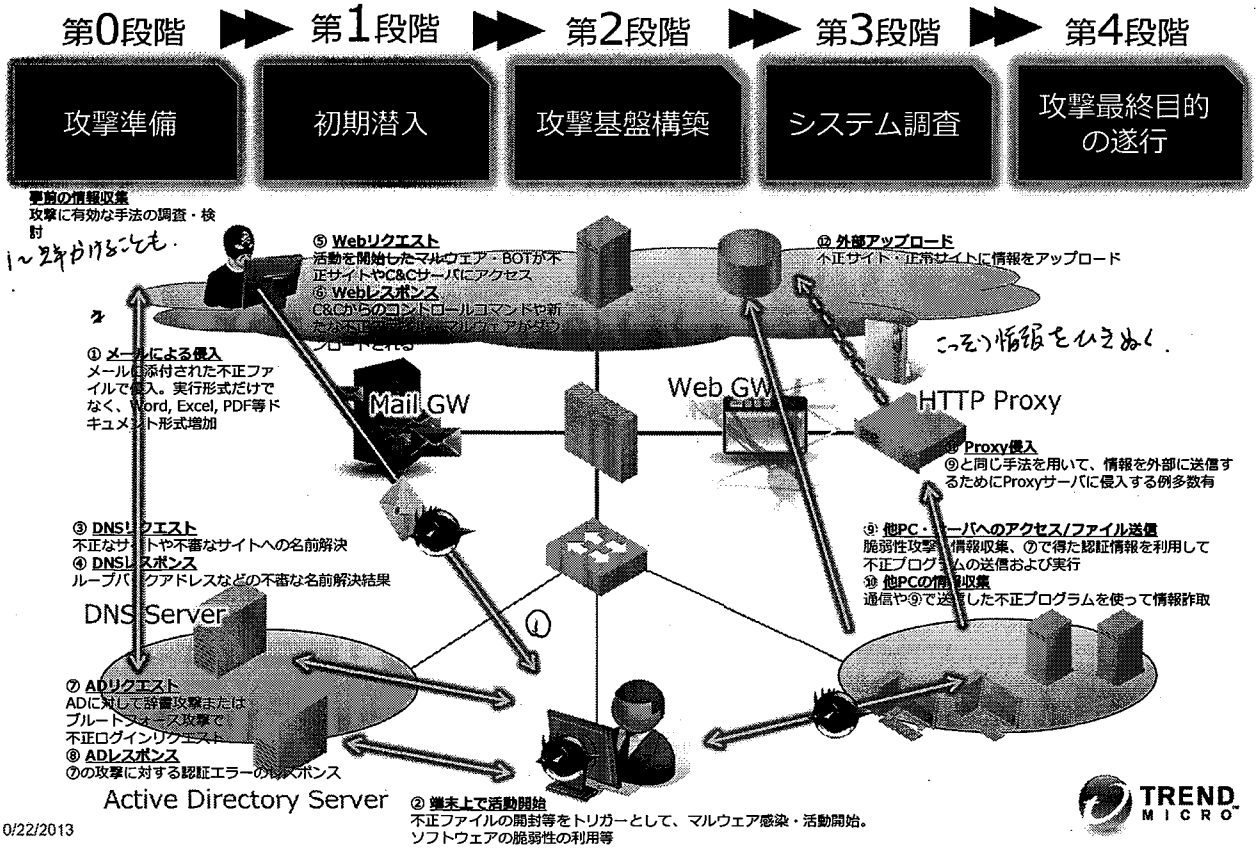
【H24 中の標的型メール攻撃に使用
された不正プログラム等の接続先】

警察庁「平成24年中のサイバー攻撃情勢について」

- 平成24年中に1009件の標的型メールが民間事業者等に送付されていることを把握
  【政府機関だけでなく、民間企業・地方企業でも判明】
- 最初から標的型メールを送付するのではなく、業務との関連を装った通常のメールのやりとりを何通か行った後に標的型メールを送付する「やり取り型」を確認
  【より巧妙な手口に】

TREND MICRO

ユーザに対する標的型サイバー攻撃の流れ

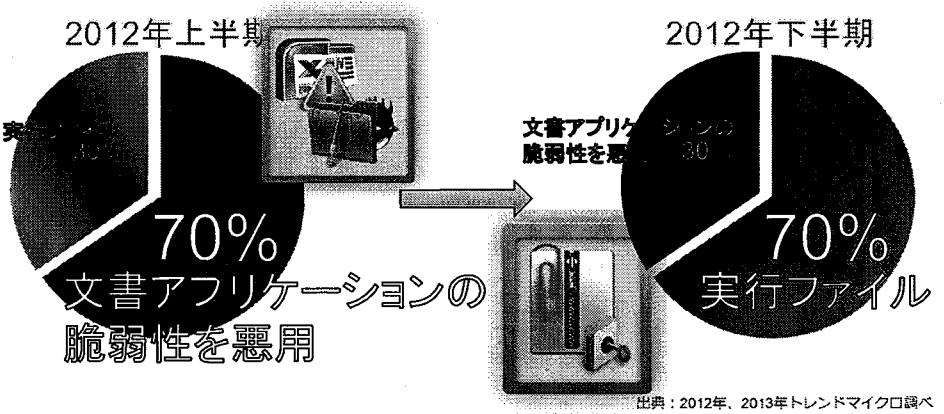


TREND MICRO

ユーザをターゲットにした場合の侵入方法

第1段階

初期潜入



出典：2012年、2013年トレンドマイクロ調べ
https://inet.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=81

- パスワード圧縮によりセキュリティ製品からの検出を逃れる
- 不正プログラムを含む複数の関連ファイルを一度に送付するために添付ファイルを圧縮
- ショートカットを表示させ、実体の不正プログラムは隠しファイルに
- 不正プログラムを画像や文書ファイルの拡張子やアイコンで偽装

侵入後に攻撃に利用される通信経路

第2段階

攻撃基盤構築

2012年上半期

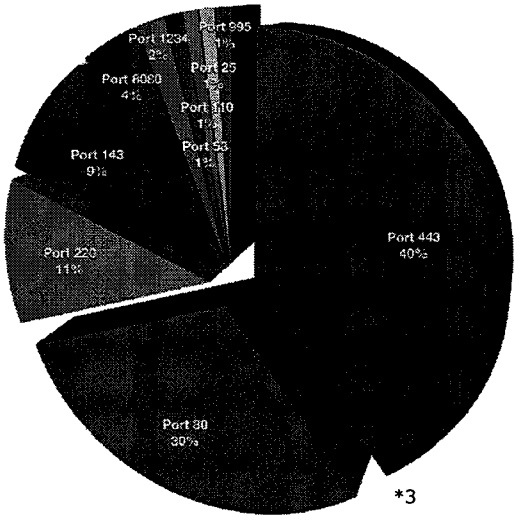
ポート	プロトコル	割合	割合
80	独自プロトコル	4.00%	60.00%
	HTTP	56.00%	
443	独自プロトコル	16.00%	32.00%
	HTTPS	16.00%	
8080	独自プロトコル	2.00%	4.00%
	HTTP	2.00%	
1080	独自プロトコル	2.00%	2.00%
8050	独自プロトコル	2.00%	2.00%

*1

2012年下半期

ポート	プロトコル	割合	割合
80	独自プロトコル	9.00%	38.50%
	HTTP	29.50%	
443	独自プロトコル	37.50%	51.00%
	HTTPS	13.50%	
8080	独自プロトコル	3.00%	6.50%
	HTTP	3.50%	
53	独自プロトコル	1.50%	1.50%
2002	独自プロトコル	0.50%	0.50%
8050	独自プロトコル	1.50%	1.50%
54124	独自プロトコル	0.50%	0.50%

2008年～2012年の間に日本で確認された PoisonIvy の検体が利用していた各ポート



*3

URL：
https://inet.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=81

 *2

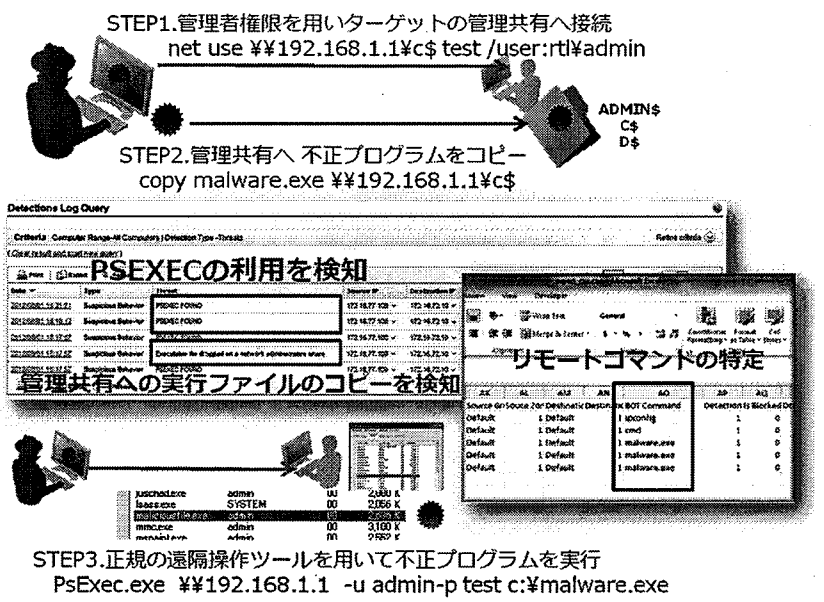
正規ツールを悪用した攻撃の検知例

第3段階

システム調査

第4段階

攻撃最終目的の遂行



- 正常と思われる通信にまぎれて、不正と言えない『不審』な通信が内部ネットワークを介して、システム調査を行う
- 特権アカウントを奪取されてしまえば、情報の搾取は容易なものに。

TREND MICRO

より詳細な情報・現在の脅威動向については

2013/8/21（水）リリースレポート

2013年上半期
国内における持続的標的型攻撃の分析

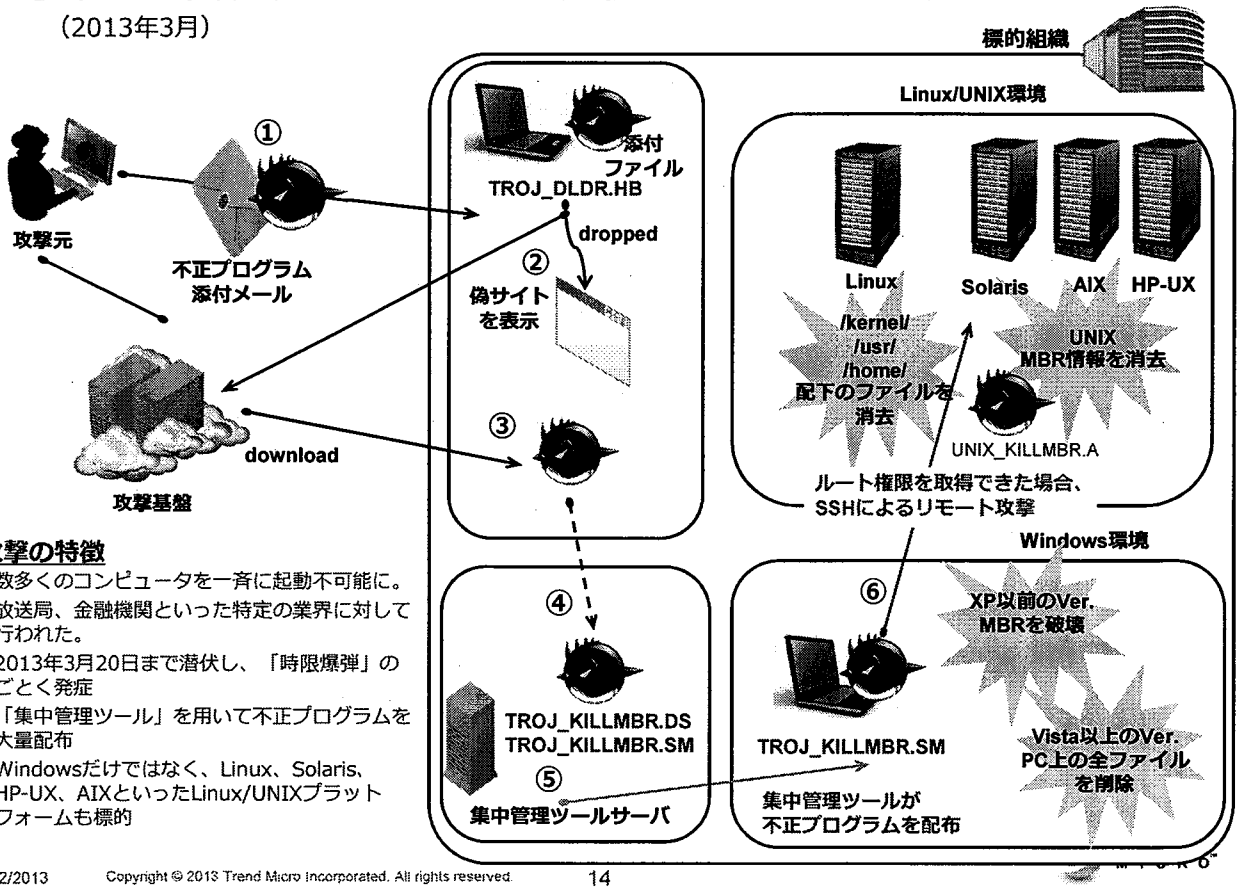
DLページ： https://inet.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=81
ブログ　： http://blog.trendmicro.co.jp/archives/7726

TREND MICRO

昨今の脅威事例から見えてくること

事例：韓国における大規模サイバー攻撃

（2013年3月）



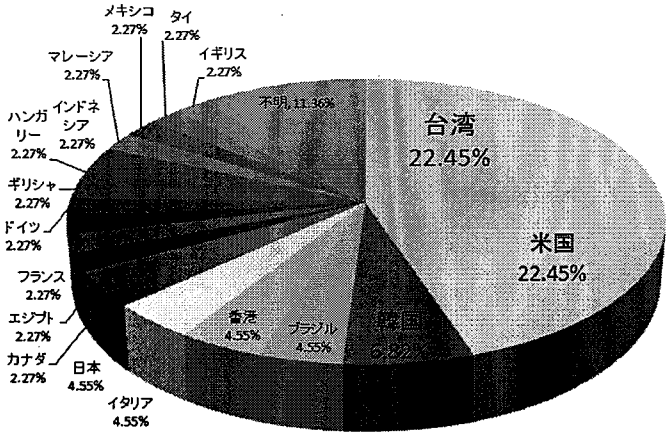
攻撃の特徴

- 数多くのコンピュータを一斉に起動不可能に。
- 放送局、金融機関といった特定の業界に対して行われた。
- 2013年3月20日まで潜伏し、「時限爆弾」のごとく発症
- 「集中管理ツール」を用いて不正プログラムを大量配布
- Windowsだけではなく、Linux、Solaris、HP-UX、AIXといったLinux/UNIXプラットフォームも標的

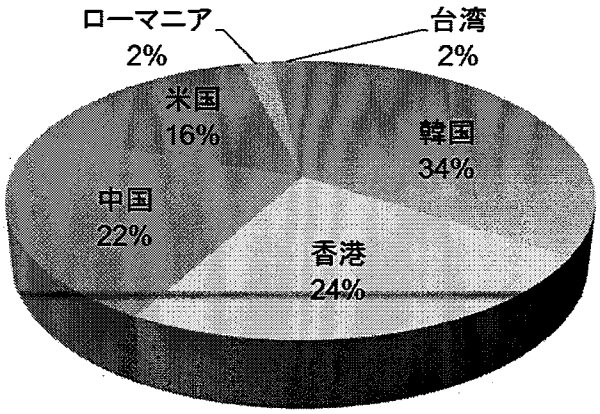
持続型標的型攻撃におけるC&Cサーバの設置国

Command and Control

キャンペーン「IXESHE」のC&Cサーバ設置国*1



キャンペーン「Safe」のC&Cサーバ設置国*2



日本は少ない

*1： https://inet.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=81
*2： http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-safe-a-targeted-threat.pdf

TREND MICRO

海外から日本への脅威の流入

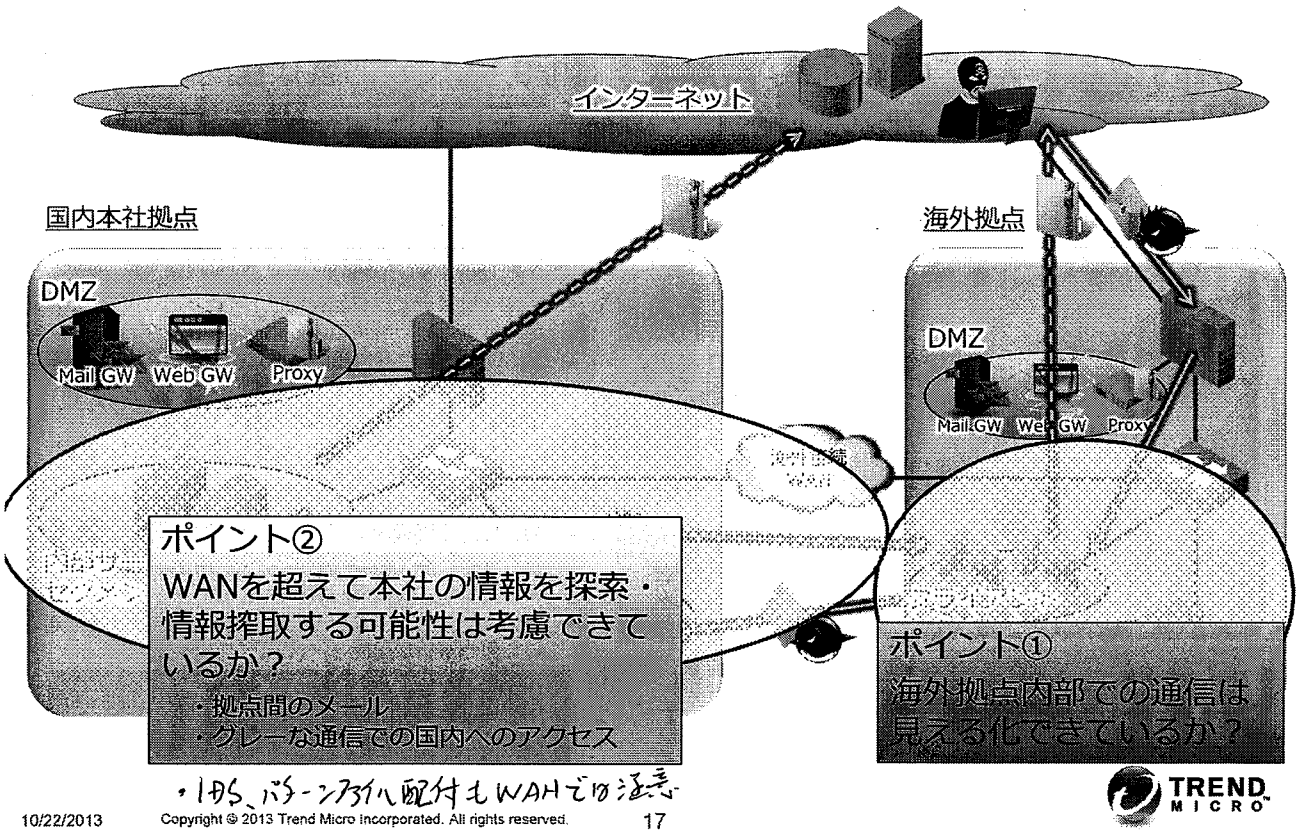
半年～1年後

脅威	海外	日本	差
オンライン銀行詐欺ツール	2010年前後	2012年11月以降（2013年1月以降の調査で確認）	2年前後（今後、ATS、モバイルフィッシングの流入を予想）
SSHD Rootkit	2013年2月頭	2013年2月中旬	半月前後
Darkleech Apache Module	2012年9月前後	2013年3月頭（報道は3月中旬）	約半年間
Blackhole Exploit Kit（BHEK）	2012年前半	2013年3月頭（それ以前もSPAMメールでの拡散が確認されていた）	約1年間

海外脅威動向から得られた知見を今後の対策に生かすべき

TREND MICRO

海外企業ネットワークの中で考えてみると



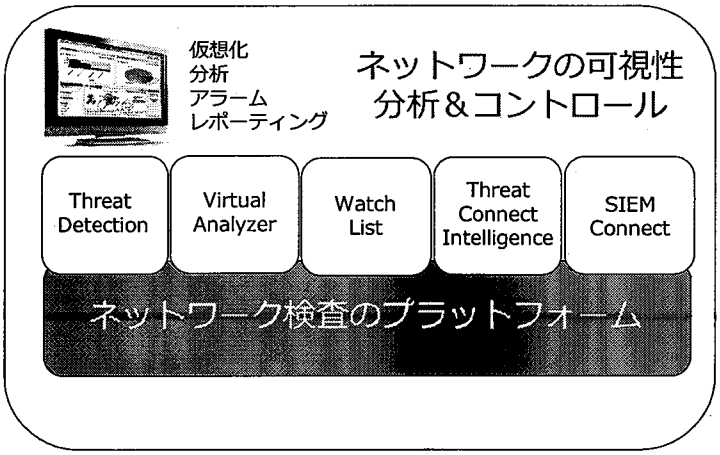
・IDS、パターンファイル配付もWANでの注意

TREND MICRO

標的型サイバー攻撃への対策のポイント
～Deep Discovery Inspector 3.5

Deep Discovery Inspector(DDI)とは？

標的型攻撃などの新たな脅威に対抗すべく、お客様社内のネットワークにおける脅威の可視化と分析、コントロールを実現する製品。



What's New?

- ヒューリスティック型脆弱性ドキュメント検索エンジンによる静的解析力の強化
- 100以上のプロトコルに対応した、ネットワーク振る舞い検知
- 相関解析エンジンの実装と各種レポート生成
- カスタマイザブルDashboard 、ジオグラフィックマップなど自社にあった情報を容易にリアルタイムで確認可能
- 解析詳細情報確認
- サンドボックス技術を利用した、Virtual Analysisテクノロジによる動的な詳細分析
- カスタマイズ可能なSandboxにより、自社環境に適した仮想解析が可能

•ネットワークへの接続は、ミラーポートを利用するため、既存環境への影響を最小限に抑えて利用できます。
•サンドボックス 用の各種OSやアプリケーションラインセンスはお客様にて用意する必要があります。

TREND MICRO

Deep Discovery Inspector(DDI)での対策

1. 入口対策

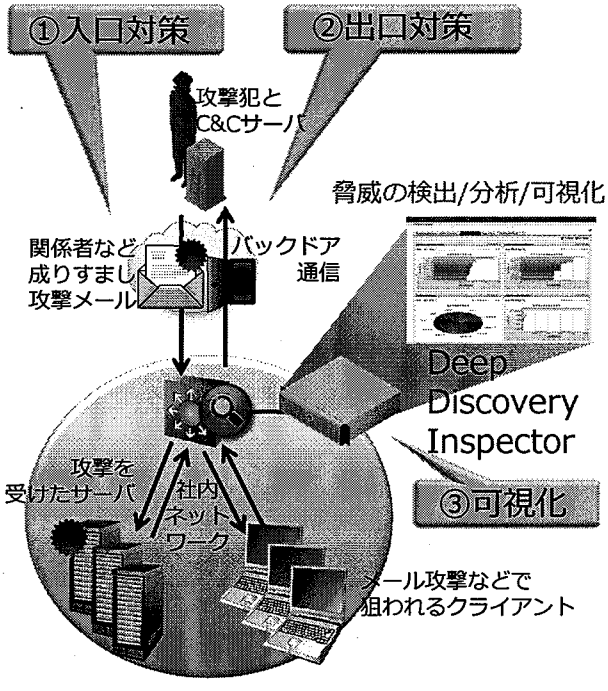
- ルールベースでのNetwork検出とヒューリスティックルールによる検出、仮想環境を用いた動的解析の「多段解析」により、効率よく脅威を分析
- プロトコルを幅広くカバレッジすることで、多様な攻撃に対応

2. 出口対策

- 入り込んだ脅威が、バックドアを通じて外部サーバと通信し、攻撃を悪化させる様子をネットワークモニタリングで検出

3. 内部ネットワーク脅威の可視化

- 今起こっている脅威状況を、グラフィカルなウィジェットを用いて把握
- 長期にわたるログを分析したレポートを待つことなく、脅威に気付き、対応を行うことが可能

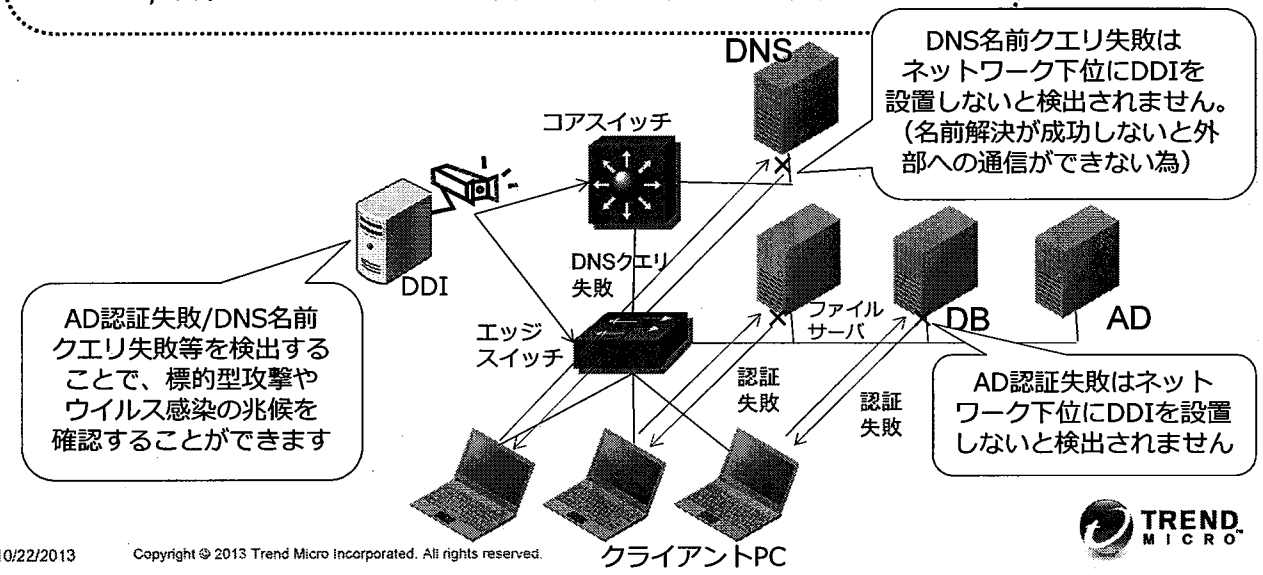


TREND MICRO

内部間通信を可視化することによるメリット

標的型攻撃の検出のポイント

- クライアント端末が特定できるネットワークの下位を監視
- クライアント端末から各種内部サーバへの通信が監視可能なポイントに設置
- クライアント間の探索・感染の通知も確認する
- SMB, 各種DB-クライアント間の通信を中心に監視

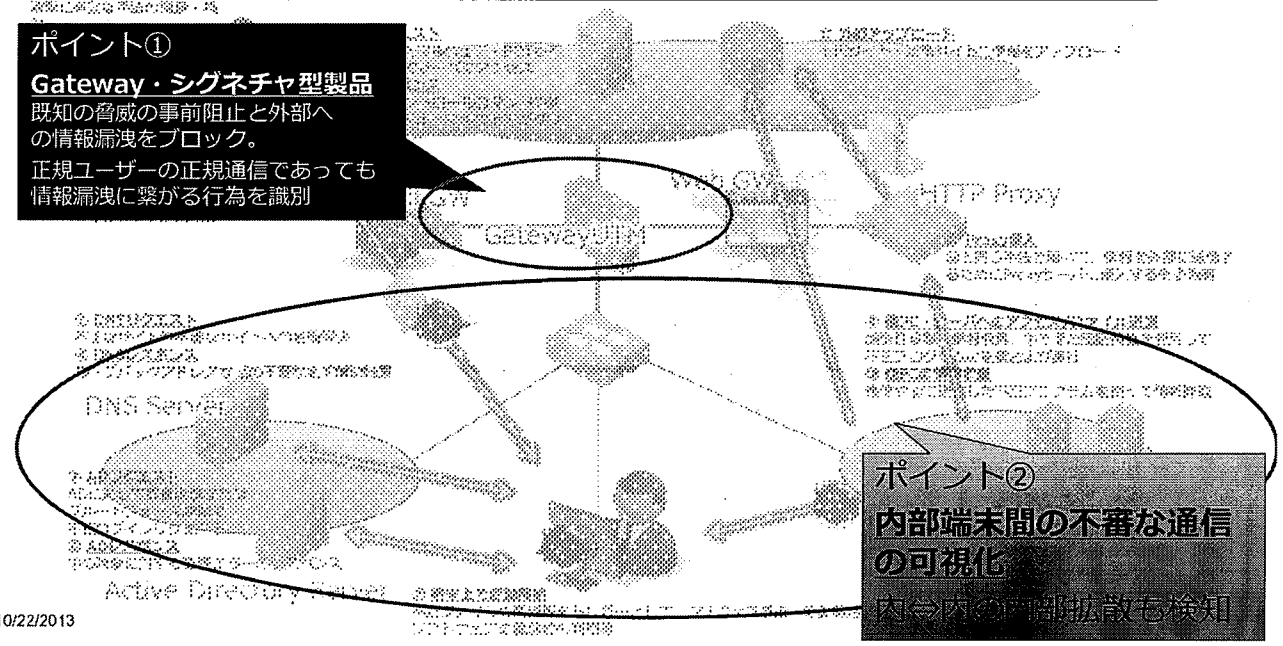


Deep Discovery Inspector の強み

- **トレンドマイクロ独自の挙動分析ルールエンジンを搭載**
  - ブラックリスト・ホワイトリスト方式では判別できない **"グレーな（=ネットワークに潜在する脅威）通信"をアグレッシブ**に検知することで、**内部での不審な振る舞い**を検知可能。
  - 従来のネットワーク型IPS/UTMのシグネチャでは、ブラックな通信は検知できるが、グレーな通信は検知が難しい。
- **ファイルベースでのパターンマッチング・ルールエンジンを搭載**
  - 従来のウィルスパターンファイルのほか、昨今急増する**パッカーによる難読化された不正プログラムもルールベースで検出**も可能
  - UTM製品でもウィルス対策機能はあるが、フローベースがほとんど。また、パッカーを組み合わせた亜種の急増への対応が難しい
- **プロセス動作・システム変更を検知するSandboxの搭載**
  - 静的解析では判定が難しい攻撃手法を仮想空間にて実際し、相関分析、検体取得を行うことが可能。

標的型サイバー攻撃におけるDDIの強み

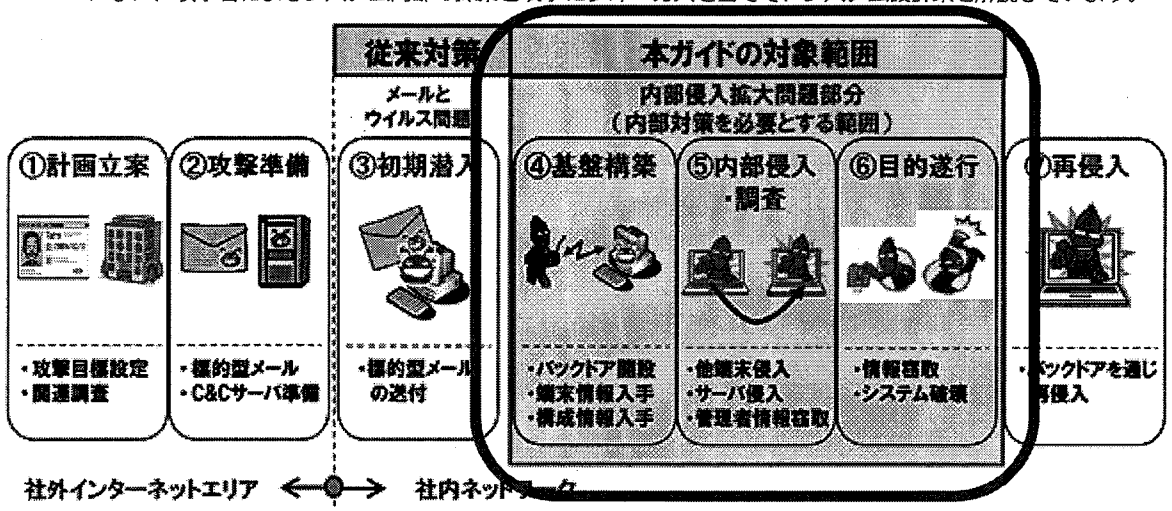
標的型サイバー攻撃では、**DNS・ADへの不正アクセス**に加えて、正規ツールを悪用した攻撃により、**単一の通信としては、不正と言えない不審な通信**が内部ネットワークでのシステム調査に利用されています。
*DDI*では、従来のブラックリスト型の検知手法では検知できないこのような通信を可視化し、早期に対応をすることが可能です。



10/22/2013

情報処理推進機構（IPA）による対策ガイド

- IPAより「**『標的型メール攻撃』対策に向けたシステム設計ガイド**」が2013/08/29に公開されて、まさに**DDIのフォーカスするポイント**と合致しています。
  - 以下、引用
  - ～ IPAでは、標的型メール攻撃を7段階に分類し、各段階における攻撃者の狙い、特徴・パターンを踏まえて、10種のシステム設計対策を紹介しています。また攻撃7段階の内、従来のセキュリティ対策ではカバーしきれていない、攻撃者によるシステム内部の探索と攻撃にフォーカスを当てて、システム設計策を解説しています。～



引用：「『標的型メール攻撃』対策に向けたシステム設計ガイド」の公開
<http://www.ipa.go.jp/security/vuln/newattack.html>

標的型サイバー攻撃対策を考える上で

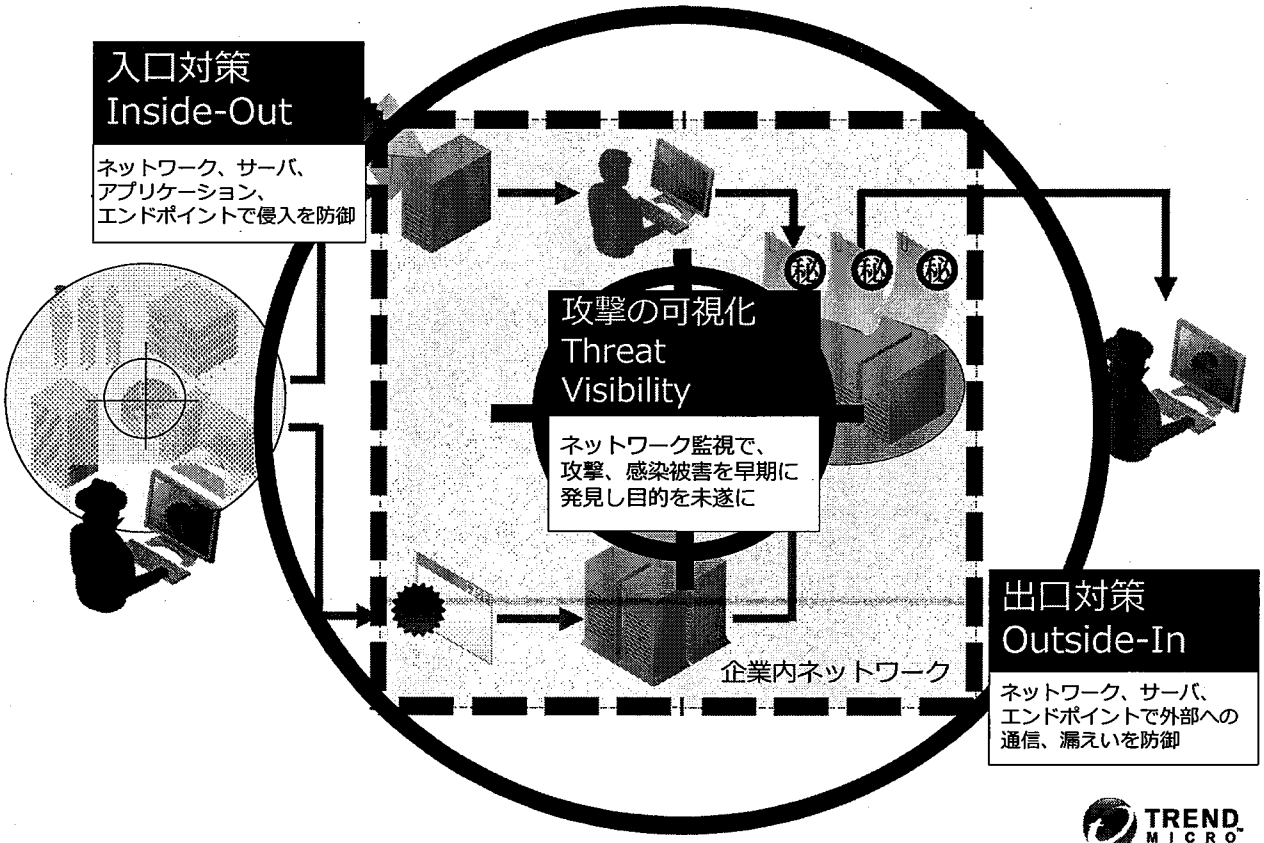
対策を考える上での留意点

- 従来からの対策・課題 (防災)
  堤防を際限なく高くするのは非現実的
  - なるべく侵入をさせない仕組みは必要だが限界があることを認識する
    (システム担当者のみならず、上層部にも認識させる)
  - 現在の状況を知り、何が不足しているかを可視化し、対策を講じる

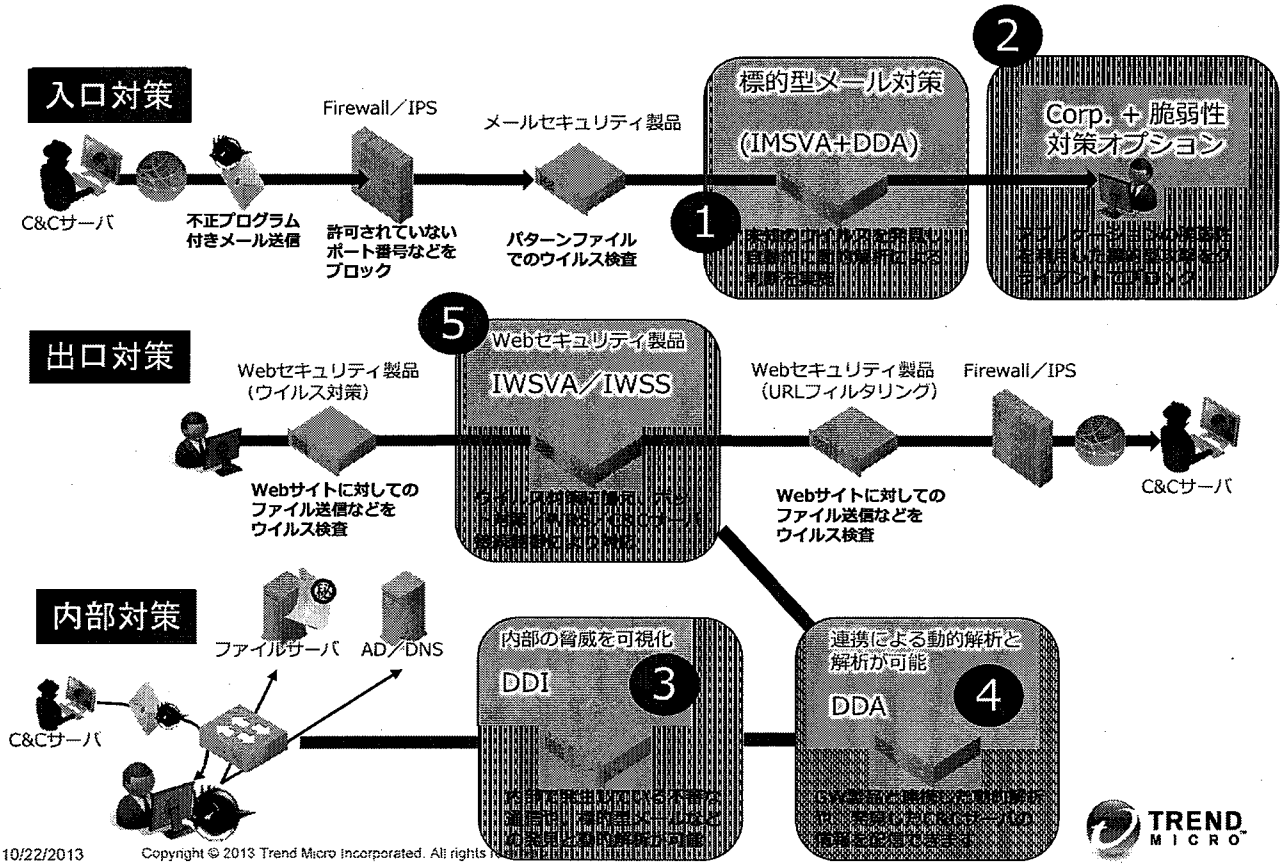
- 新しい対策・課題 (減災)
  仮に津波が堤防を越えても被害を最小限にする
  - 侵入は許しても、悪事を完遂できない仕組み
    泥棒が入ってきても、金品(情報)を持っていけない仕組み
  - 不審な傾向があったときにすぐ分かる仕組み
  - 脆弱性（セキュリティホール）対策
    一般的に脆弱性対策は後手に回っているため、攻撃者が利用

侵入されることを前提としたセキュリティ対策が重要

対策の考え方

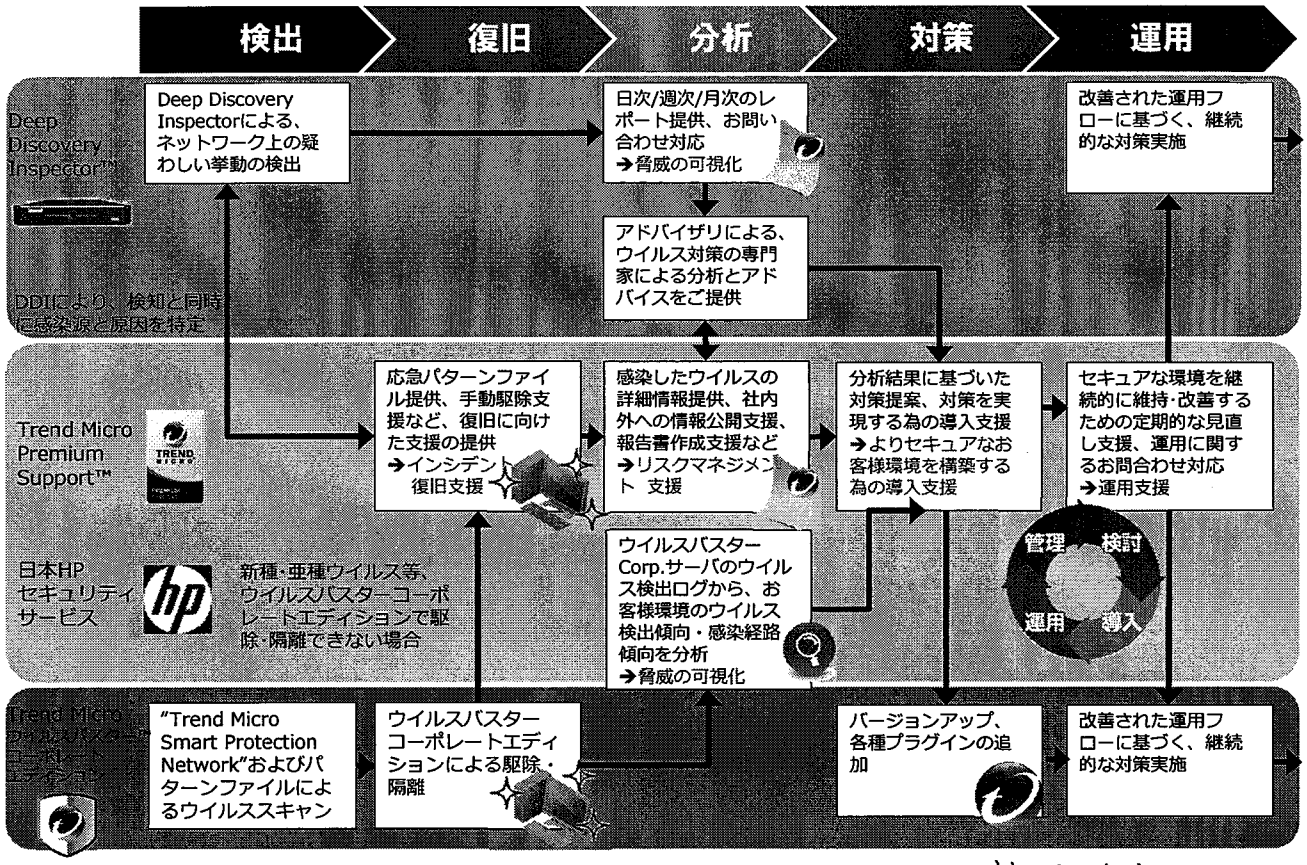


標的型サイバー攻撃に対するソリューション



未知の脅威に備えたウイルス対策フロー

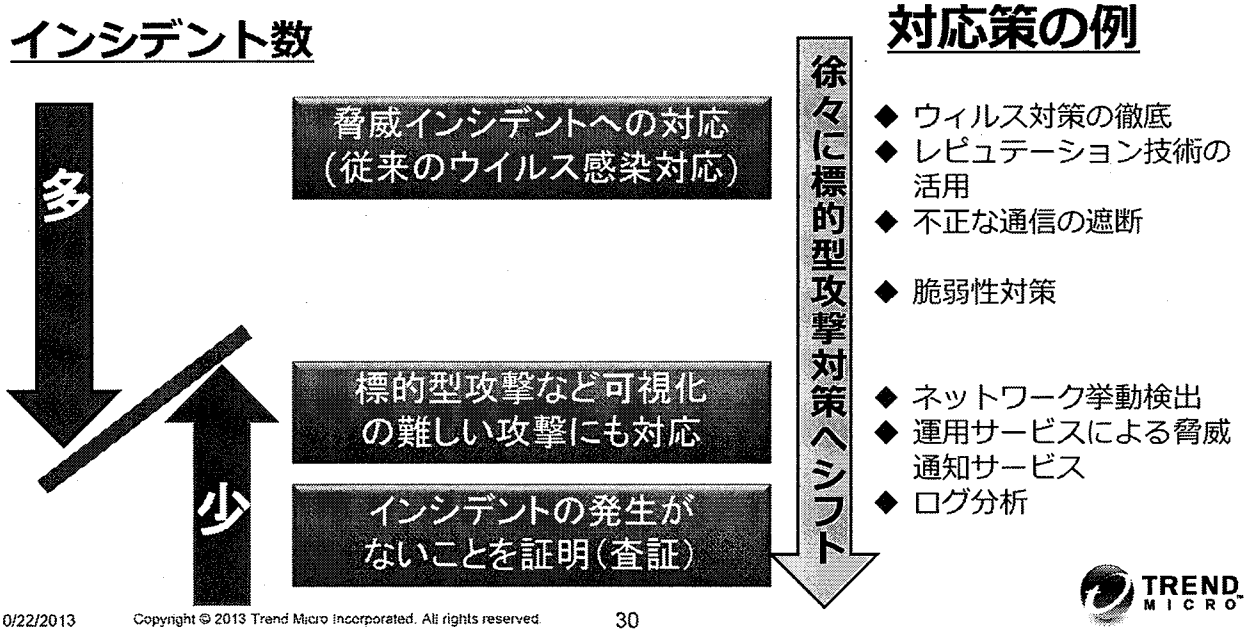
Deep Discovery Inspector x Trend Micro Premium Support x ウイルスバスターコーポレートエディション 連携イメージ



基本的色々組合せること

ネットワークの可視化を行う上でのポイント

Deep Discovery Inspector（DDI）を利用することで社内ネットワークのインシデントの発生状況を可視化することが可能です。
標的型サイバー攻撃に対しては様々な対策が必要となりますが、お客様のセキュリティレベル、規模、業種・業態に応じた対応が必要となります。まずは、実情を知るところからはじめましょう。



基本は積み上げ

まとめ

- ✔ 従来のセキュリティ対策をしっかり実践することは大前提
- ✔ 攻撃基盤(C&Cサーバ)が利用する通信、内部ネットワークで拡散する通信の特徴に応じたアプローチが必要
- ✔ 攻撃手法、ツール、攻撃基盤、通信の特徴から関連性を紐づけて、『点』をつなぎあわせ、『線』で見る観点が必要
  (相関分析・侵入されることを前提とした対策)

TREND MICRO

TREND MICRO™

Securing Your Journey to the Cloud