



Securing Your Journey  
to the Cloud



# “これから”のサイバー攻撃に対応する

**大三川彰彦**

トレンドマイクロ株式会社

取締役 エグゼクティブバイスプレジデント 日本地域担当 兼

エグゼクティブバイスプレジデント アジア・ラテンアメリカ地域営業推進担当

# 標的型攻撃、APTの特徴

	標的型攻撃	持続的標的型攻撃 (新しいタイプの攻撃、APT)
標的	個人、組織	企業・団体など特定の組織
攻撃者	比較的技能レベルの低い個人	組織、または比較的技能レベルの高い個人
目的	金銭につながる情報の窃取、機密情報の窃取	知的財産などの機密情報の窃取、組織的スパイ活動
タイミング	攻撃者が攻撃したいとき	事前に綿密な計画を立てた後
期間	一回きりの攻撃を行い、失敗すると別の攻撃を行う、比較的短期間	目的達成まで執拗に攻撃を繰り返すため、比較的長期間
手法	不正プログラム添付のメール、不特定多数、特定のグループに対するソーシャルエンジニアリング、偽装のレベルは比較的低い	不正プログラム添付のメール、特定の組織に対するソーシャルエンジニアリング、偽装のレベルはかなり高い
感染後	感染端末内の情報を窃取	感染端末から他のシステムを調査、侵入

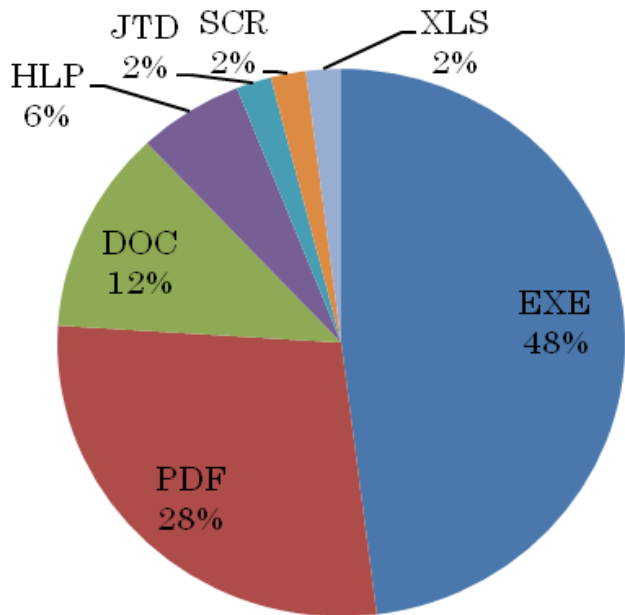
# 日本で発生している標的型攻撃 攻撃手法の特徴

- 実在する関係者、部内者になりすます
- トピック、内容も実在するトピック、受信者に関連するトピックを悪用する
- 広く使われているアプリケーションの脆弱性、あるいは人間の脆弱性を悪用する
- 外部のサーバとの通信には独自プロトコル、あるいはHTTP/HTTPSを利用する
- 新しい不正プログラムのダウンロードや情報の送受信を行う
- 目的達成のために長期間かけて、執拗に攻撃を実行する
- 個人のパソコンが踏み台として使われている

2011年10月トレンドマイクロリージョナルトレンドラボ調べ  
2011年4月から10月にかけて日本国内で収集したAPTサンプルのうち50種類について調査

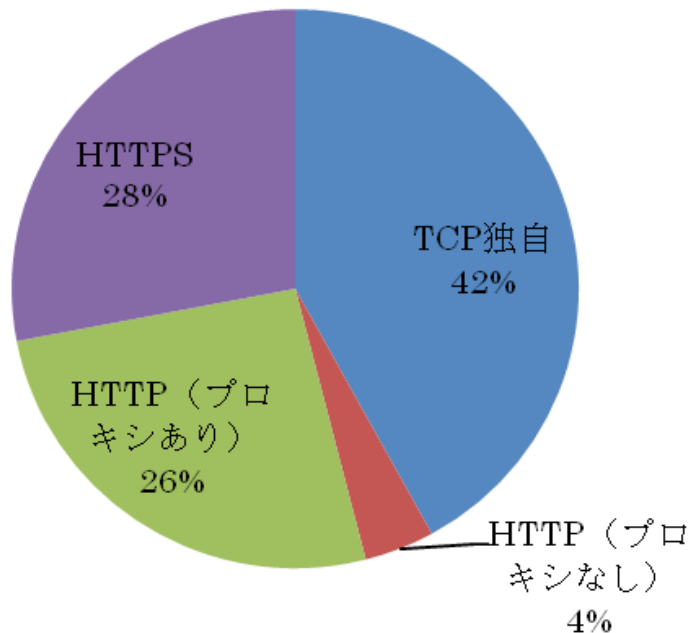
# 日本国内で発生している 持続的標的型攻撃の特徴

特徴①: 攻撃で利用される  
不正プログラムのファイル形式



- セキュリティパッチの適用
- IPS機能搭載製品の導入
- 実行ファイルのメール送受信拒否
- 外部からのなりすましメール受信拒否
- E-mailレピュテーションの導入

特徴②: 不正プログラムが  
通信に利用するプロトコル



- 直接的な外部通信を許可しない  
ファイアウォール設定
- プロキシ経由での外部通信設定
- Webレピュテーションの利用
- 通信監視、検知サービスの導入

2011年10月トレンドマイクロ リージョナルトレンドラボ調べ  
2011年4月から9月にかけて日本国内で収集した持続的標的型攻撃のサンプル100種類について調査



# サイバー攻撃に必要なセキュリティ

## 防御

## 可視化

## 対処

技術

暗号化

認証

ファイアウォール

侵入防御 (IPS)

挙動監視

Webアプリケーション

E-mailアプリケーション

URLフィルタリング

迷惑メール対策

ウイルス対策

アプリケーションコントロール

デバイスコントロール

モニタリング

改ざん検知

脆弱性管理

侵入検知 (IDS)

情報漏えい対策 (DLP)

フォレンジック

ログ管理

統制

セキュリティ運用・管理

セキュリティライフサイクル管理

セキュリティポリシー策定・徹底

情報

ナレッジ共有（外部連携・組織/体制づくり）

リスクアセスメント

セキュリティインテリジェンス

# Security That Fits: お客様の環境

トレンドマイクロのユビキタス環境に適したソリューションが  
あなたの情報資産を守ります





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