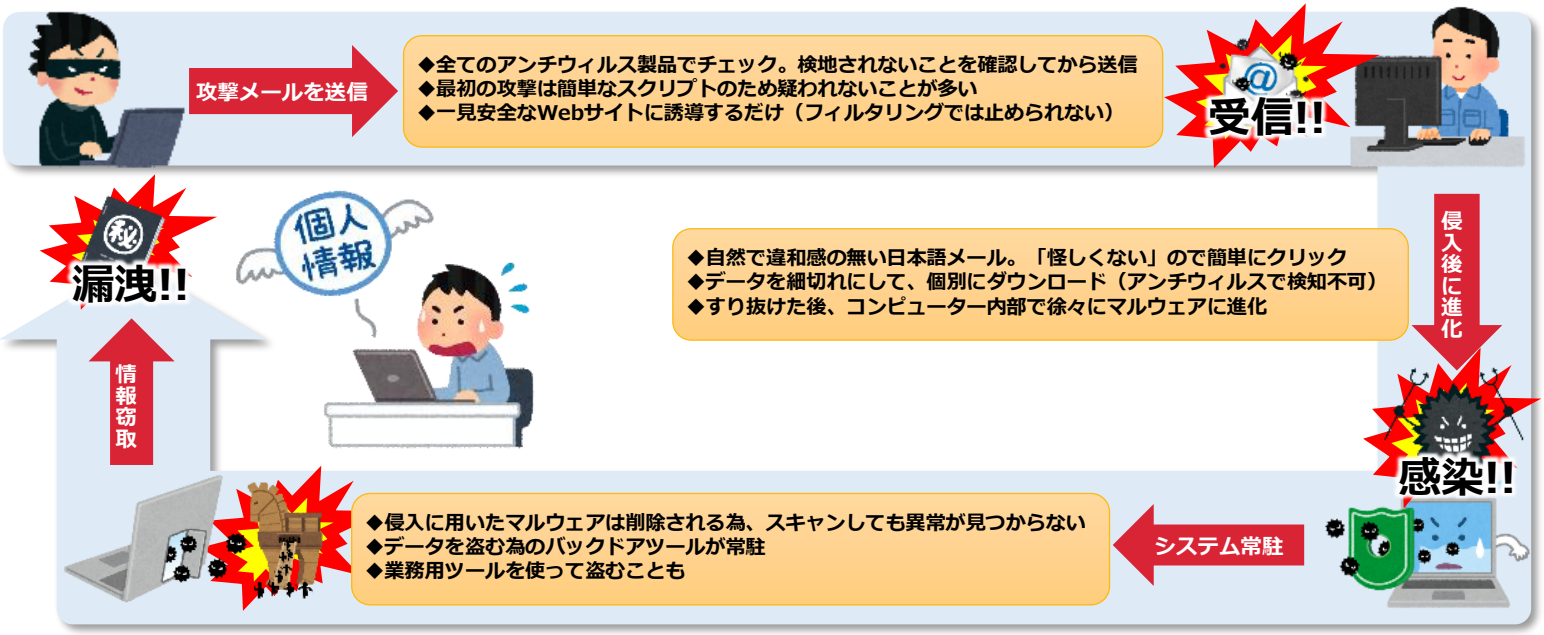
ICT環境整備はお済みですか？
情報セキュリティ対策もお忘れなく！

FireEye

教育ネットワークにおける情報セキュリティ強化の必要性が叫ばれています。
公立学校でも被害の増えている**標的型攻撃**や**ランサムウェア**は、アンチウィルスやファイア･ウォールだけでは防ぐことが出来ません。

なぜ防げない？標的型攻撃の例



仮想環境で攻撃のプロセスを全て再現・分析！

ファイア・アイでは、既存のセキュリティ技術では検知できない高度な攻撃を検知するために、実際にファイルを解析し、その振る舞いにより検知する仮想実行環境技術を採用しています。ファイア・アイはこの仮想実行環境をマルウェアの検知のために業界で初めて採用した企業であり、独自の仮想実行環境である、「FireEye Multi Vector Virtual eXecution™ （MVX）」エンジンを自社開発しています。

ネットワーク・メモリ環境も再現

C&Cサーバーへの通信やメモリへ直接ロードするモジュールなど、複雑なマルウェアのプロセスを徹底的に再現します

2000パターンにも及ぶ仮想実行環境

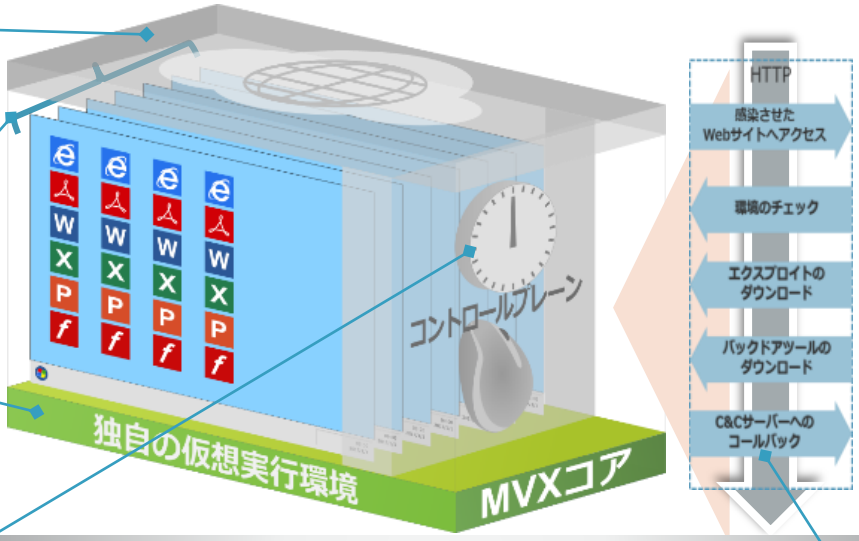
特定のOS、アプリのバージョンを狙うマルウェアの意図を確実に把握する多彩な実行環境をライセンス含めてご提供します

マルウェアに見抜かれない仮想技術

一般的なハイパーバイザーと違い、マルウェアに”SandBox内にいる”ということを気づかせません。

時間経過を再現

発症遅延型マルウェアの潜伏・侵入を許しません。

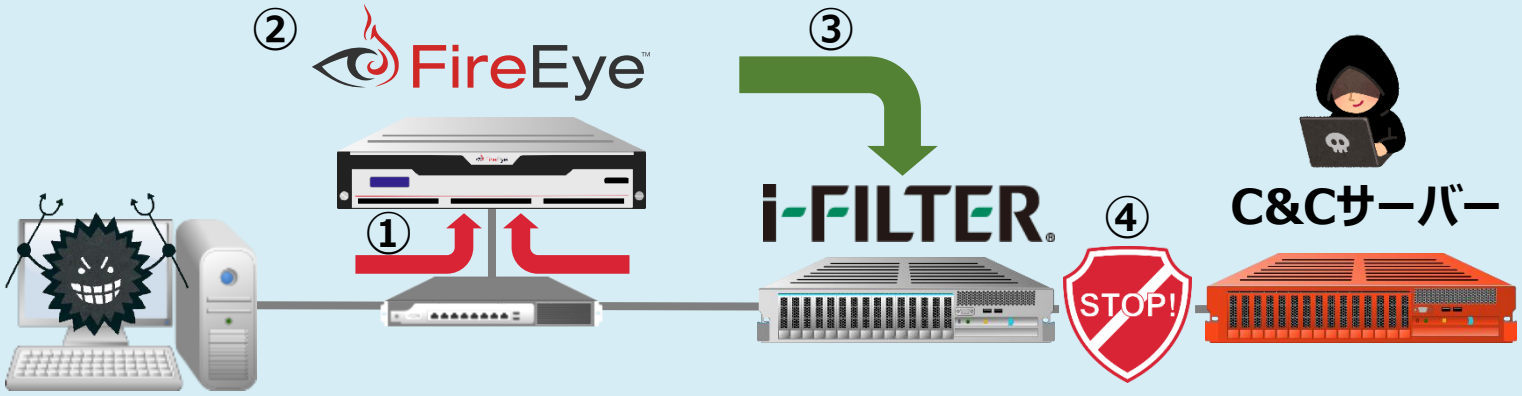


マルチフロー解析により多段階攻撃にも対抗

ファイルだけでなく攻撃者との通信そのものを解析するため、巧みな攻撃にも対抗可能です

「i-FILTER」との連携で危険な通信を即時遮断

より安心、手間なく即時的な標的型攻撃対策が可能に!!



① マルウェア感染による通信、Webからの攻撃による通信を検知
② FireEye NXがアラートを出力
③ 連携モジュールがアラート内のIP、URLを取得し、Webフィルタリングに登録
④ 危険なWeb通信を即時ブロック！

NEW Web通信の脅威対策製品　NX2500シリーズ

- **従来のセキュリティ製品では検知できない標的型攻撃の検知・防御**
- **パターンマッチに頼らず、独自の仮想実行環境で実行させ脅威判断**
- **Windows・Mac両環境に対応。**
- **Microsoft社”Office”に加え、ジャストシステム社“一太郎”にも対応**

モデル名	ユーザー規模	契約期間	アカデミック価格※
NX2500 [50Mbps]	約500人	5年	¥5,069,898
NX2500 [100Mbps]	約1,000人	5年	¥9,330,323

※ 教育委員会および学校法人等、教育機関のみを対象とした特別価格です。適用条件について詳しくはお問い合わせください。
※ 上記価格にはハードウェア本体価格および5年間のライセンス費用・オンサイトサポート(平日9時～17時)費用が含まれます
※ 構築費用は含まれておりません。

✉お問合せ：japan@fireeye.com

ファイア・アイ株式会社
http://www.fireeye.jp/
〒101-0054
東京都千代田区神田錦町3-22 テラススクエア8F
Tel: 03-4577-4401
Fax: 03-4577-4410