未知脅威を高精度で検出

FireEye NXシリーズ(Webトラフィック用脅威対策プラットフォーム)

FireEye NXシリーズは、従来のWebベース脅威への対策（ファイアーウォール、IPSやアンチウイルスなど、既知脅威への対策）では検知できず、すり抜けてしまうWebベースの未知脅威の攻撃を検知する、脅威対策プラットフォームです。
Web経由による未知の攻撃による侵入と外部C&Cサーバ※1とのアクセスを検知し、機密データやシステムを保護します。

※1　C&Cサーバ：外部から侵入して乗っ取ったコンピュータを制御したり命令を出したりする役割を担うサーバ

標的型サイバー攻撃の傾向

- 特定のターゲットに対して持続的に攻撃・潜伏を行い、様々な手法を駆使して執拗なスパイ行為や妨害行為などを行うAPT攻撃(Advanced Persistent Threat：持続的標的型攻撃)が増加している。
- APT攻撃は、未知のマルウェアや脆弱性が使われるため、定義ファイル(シグネチャ)によるブロックを主とする従来型のセキュリティ対策では、攻撃自体を検出できず、防御はおろか、攻撃があったことを把握することもできない。

①マルチフロー解析による、APT攻撃の検知

高性能なサンドボックスにより複雑化する未知脅威を高精度で検出可能

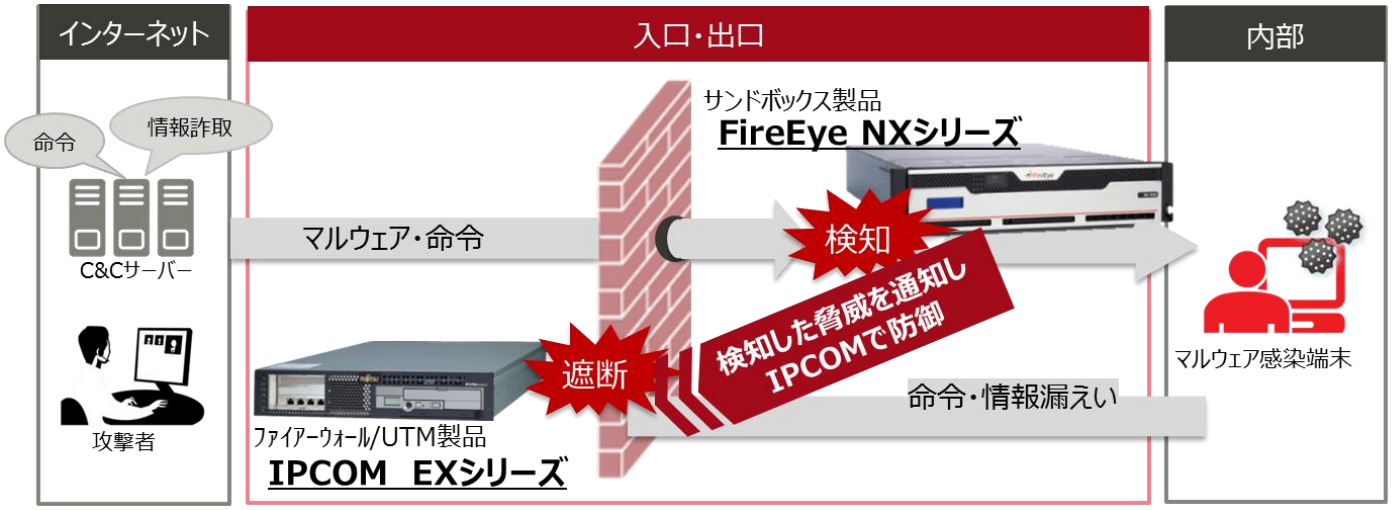
①定義ファイル（シグネチャ）が効かずサンドボックスも回避するマルウェアに対抗できる
- 独自開発の仮想環境、OSやアプリのAPIをフック、通信行為の補完 等の独自技術により、マルウェアの高度な回避行為を検知し、回避阻止が可能

②多段階な通信による攻撃テクニックに対抗できる
- 通信過程でマルウェアに進化する攻撃手法や、ブラウザのプロセス内で実行する攻撃(ファイル形成しない攻撃)をも検出可能

③ゼロデイを含む複数の脆弱性をついた攻撃に対抗できる
- 独自の仮想環境内には約2,000パターンの解析環境が予め導入されており、これらの環境を使い、複数の環境下で解析を行うことで、特定の環境下で実行される攻撃も検知可能

②IPCOM連携による入口出口対策

入口(FireEye)で検知した脅威情報を元に出口(IPCOM)で迅速に対処



検知実績No.1のFireEyeで検知した脅威情報を元に、出口のIPCOMで該当通信を遮断し、情報漏えいを防止

【効果】FireEyeとIPCOMが脅威情報を自動連携することで、迅速な対応と運用負荷 軽減を実現

※１：本連携機能をもたないIPCOM EXシリーズ以外のファイアーウォール/UTM製品の場合FireEye NXシリーズで検知した脅威情報に基づいた、ファイアーウォール/UTM製品での遮断を実現するためには ファイアーウォール/UTM製品の「設定変更作業」が必要となります。

中堅市場向けのラインナップ強化

- 中小企業は、セキュリティ対策をしたいが予算的に導入できず、セキュリティ対策で後れを取っている企業が多い。
- 従来と同等性能のまま、中堅市場向けに必要な機能に絞り、低価格化(従来比約60%オフ)を実現したNX Essentialsシリーズを中堅市場向けに新規ラインナップ追加。

■ 従来品（NX2400 Essentials）

製品名	型名	数量	標準価格(税別)	小計(税別)
NX2400 Essentials 1Y BDL	FSPQN240E1	1	¥5,658,660	¥5,658,660
			合計	**¥5,658,660**

DTI 1年間利用費用込み

■ 新製品（NX2500 Essentials）

製品名	型名	数量	標準価格(税別)	小計(税別)
NX2500 50Mbps Essentials	FSPQN25LE	1	¥1,887,840	¥1,887,840
DTI 2500 Essentials 50Mbps NX2-way 1year	FSPQE25L1E	1	¥377,460	¥377,460
			合計	**¥2,265,300**

性能そのままに60%オフ

お問い合わせ先

富士通コンタクトライン　0120-933-200

受付時間 9:00～17:30（土・日・祝日・当社指定の休業日を除く）