標的型サイバー攻撃対策
内部対策と出入口対策製品連携

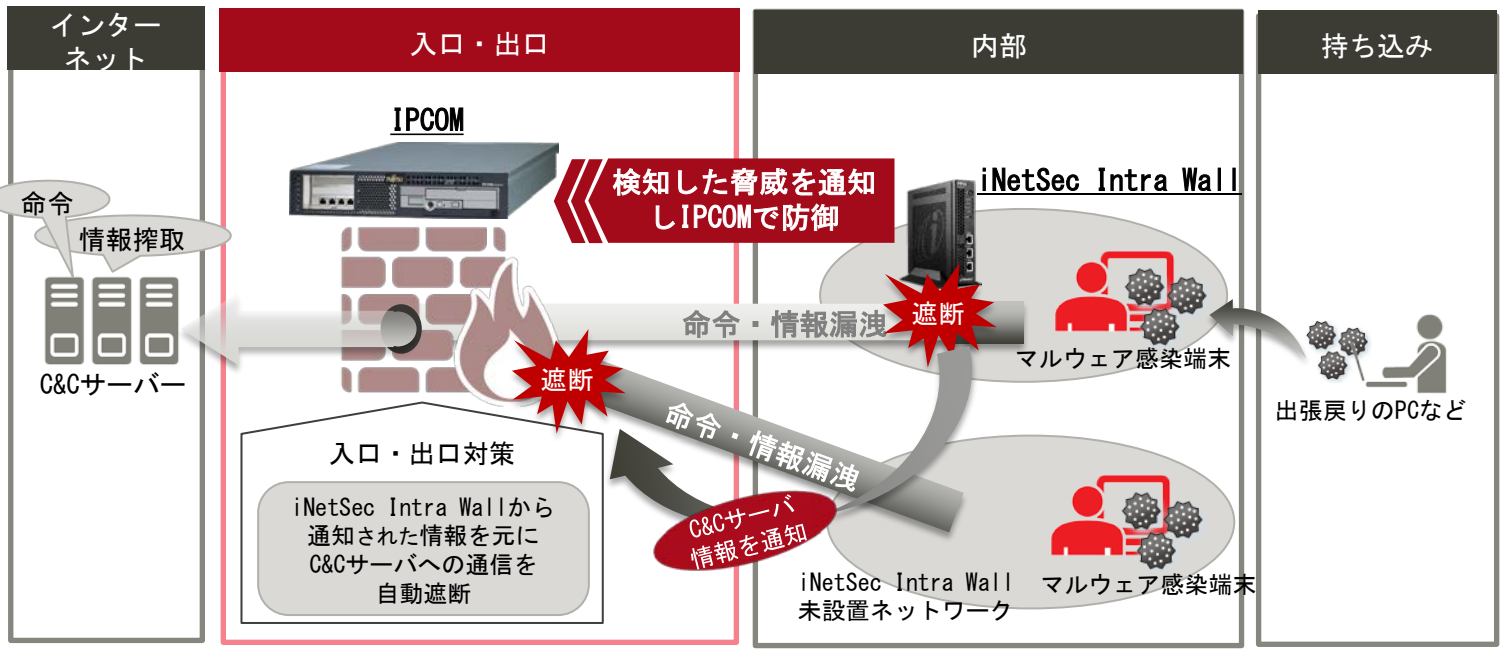
FUJITSU Network IPCOM EXシリーズ
セキュリティアプライアンス製品 iNetSec Intra Wall

お客様のメリット

- 標的型サイバー攻撃の内部対策で検知したC&Cサーバの通信を出入口対策製品で自動遮断
- 内部対策製品を導入していないネットワークからのC&Cサーバへの通信も出入口対策製品で遮断が可能
- 連携機能があることで、少ない内部対策製品の導入でも、標的型サイバー攻撃対策に対して、高い効果

近年のサイバー攻撃では、未知のマルウェアを使用した標的型サイバー攻撃が増加しており、対策が重要になっています。マルウェアの侵入対策で入口対策や、持ち込み・すり抜けを前提にマルウェアの内部対策や、情報漏えい対策で出口対策が重要になっています。

内部対策製品と出入口対策製品が連携し、内部対策製品が検知したマルウェアのC&Cサーバとの通信を出入口対策製品で遮断することで、マルウェアによる情報漏えいを防ぐことが可能になります。また、出入口対策製品のIPCOM EXシリーズはさまざまなセキュリティ機能を持っており、入口対策としても、アンチウイルス機能やシグネチャー型IPS機能などもありますので、高度なセキュリティ対策が可能になります。



※iNetSec Intra Wallは、総務省委託研究「サイバー攻撃・検知に関する研究開発」の成果を使用しています。
※IPCOM EXシリーズはIPCOM EX IN/SC/NWシリーズのE20L32以降でオプションが必要
※iNetSec Intra WallはIPCOM連携モジュール(無償)が必要

商品・サービスについてのお問い合わせは
富士通コンタクトライン（総合窓口） 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）
富士通公開サイト http://jp.fujitsu.com/ 詳細はこちら http://fenics.fujitsu.com/products/inetsec/

2016.1