サイバー攻撃検知と遮断連携による自動防御

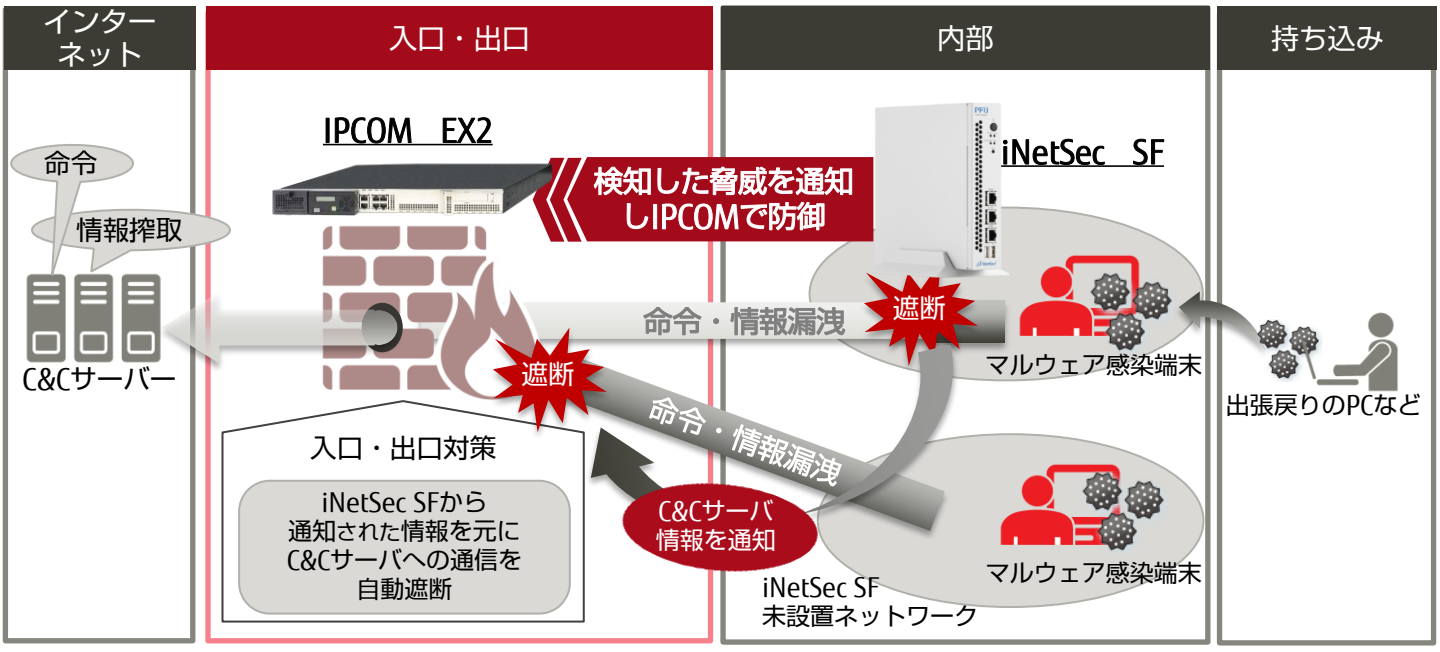
FUJITSU Network IPCOM EX2シリーズ，iNetSec SF

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サーバへ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における入口対策や、持ち込み・すり抜けを前提としたマルウェアの内部対策や、情報漏えい対策における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 EX2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、高度なセキュリティ対策が可能になります。



※iNetSec SF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 EX2シリーズの以下で連携機能の利用が可能です。
EX2-1000 SC/NWソフトウェア、EX2-3000 SC/NW/IN ソフトウェアで、連携には標的型攻撃対策連携ライセンスが必要です。