

# 標的型サイバー攻撃対策

## 出口対策製品連携

FUJITSU Network IPCOM EX2シリーズ  
FireEye NXシリーズ

### お客様のメリット

- 標的型サイバー攻撃対策のサンドボックス製品 (FireEye NXシリーズ) で検知したマルウェアのC&Cサーバへの通信先を出口対策製品のIPCOM EX2シリーズで遮断
- サンドボックス製品と出口対策製品の連携機能で使うことで、遮断の設定が自動化され、運用が簡単
- 自動設定されることで、C&Cへ通信可能な時間が短く、高い精度の情報漏えい対策を実現

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出入口対策が重要ですが、入口対策で見つけたマルウェアに対して、一刻も早く対応することが大切です。

サンドボックス製品と出口対策製品が連携し、検知したマルウェアのC&Cサーバとの通信を出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機能などもありますので、高度なセキュリティ対策が可能になります。



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/>