

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
iNetSec MPシリーズ

お客様のメリット

- サイバー攻撃検知製品（iNetSec MPシリーズ）が攻撃者の攻撃活動（感染進行、感染拡大）を早期に検知し、出口対策製品のIPCOM EX2シリーズにて自動遮断することで運用負担を軽減しつつ情報漏えい対策が可能
- 業務に応じ怪しい外部通信に対して、お客様の運用方針にあわせた対応（「とにかく止める」「様子を見る」）が可能
- 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検出するためのサンドボックス製品をもすり抜けてくる攻撃が出て来ており、すり抜けてきたものに対する対策が重要になっています。

攻撃プロセスを時系列で見える化し、攻撃の全容把握が可能なサイバー攻撃検知製品のiNetSec MPシリーズを導入し、対処の際に必要な情報を的確に把握し、出入口対策製品であるIPCOM EX2シリーズと連携することで、検知したマルウェアのC&Cサーバとの通信を遮断する出口対策として情報漏えい対策が可能となります。

また、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/>