



# 脅威のランサムウェア

パソコンの画面が  
ロックされ使えない

ファイルが破壊され  
開かない



出典：IPA 2015年6月の呼びかけ

## 対策できていますか？

ランサムウェアによる被害は復元が困難  
予防策が極めて重要！

脆弱性が狙われ、Webをみただけでランサムウェアに感染し、  
**パソコンが使えなくなる事件が急増中！**

古いバージョンのソフトウェアが入っている（＝脆弱性が残っている）PCで、改ざんサイトを閲覧すると、ランサムウェアに感染！



➡ ランサムウェアには、**多層防御**で対抗することが必要です！

# 入口・出口の対策で多層防御！

ウイルスの脅威を  
ネットワーク経路で遮断！

## ①ファイアウォールで不正なアクセスを制限！～Forti Gate～

入口対策

### ASIC内蔵 Forti Gate (単体モデル)

インターネットの入口で業務に関係ないWebサイトへのアクセスをブロック！

UTM製品のベストセラー。  
国内市場トップシェアの実績！



★主な機能★  
ファイアウォール機能

## ②標的型攻撃に有効な対策でセキュリティを強化！～Cloud Edge～

入口・  
出口対策

### トレンドマイクロ Cloud Edge

サイバー攻撃に強いセキュリティBOX

標的型攻撃対策に有効な3つの機能で更に安全なセキュリティ対策を実現します！



★主な機能★

- ① 標的型メールの対策
- ② 不正Webサイトのアクセスをブロック
- ③ 遠隔操作 (C&Cサーバー) の通信をブロック



内部対策

## ③サーバー・クライアントの脆弱性を埋める！～脆弱性対策～

クライアントの脆弱性には

### 脆弱性対策オプション (Corpオプション)

※Client/Server Suite Premiumにも同梱。

サーバーの脆弱性には

### サーバプロテクションサービス 仮想パッチモデル



●ここがポイント！●

脆弱性対策が必要なには大きく2つの理由があります。1つは、脆弱性に用いられるウイルスや攻撃者サーバは、日々変化していること。もう1つは、未知のウイルス（検体がないウイルス）は検知ができないということです。脆弱性対策製品では、下記が可能なのが特徴です！

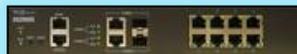
★主な機能★

- ① フクチンファイルに含まれていないウイルスによる脆弱性への攻撃に対して検知が可能！
- ② 攻撃者によるWebサイトの改ざんなどを防ぐことができる！

## ④社内ネットワーク内部での攻撃拡散を阻止！～SubGate～

出口対策

### ASIC内蔵 SubGate



L2セキュリティスイッチ  
世界シェアNo.1の実績を誇ります。

クライアントが感染しても拡散させない、L2スイッチで実現する出口対策！

★主な機能★

- ① ウイルス・ワーム拡散防止
- ② E-mailの盗聴を防止
- ③ IP電話の盗聴攻撃遮断
- ④ 機密情報漏洩の防止



## 万が一に備えたデータ復旧対策も！

直近データのバックアップだけでは、既に感染しているリスクが。  
バックアップの世代管理が、リスクを下げるポイントです。



手間なく、効率よく世代管理バックアップするなら

### 重複排除バックアップソリューション

★主な機能★

- ① バックアップデータの容量を削減し効率よく世代管理！
- ② ディスク装置へのバックアップでメディア交換・管理不要！
- ③ 重複排除で小さくなったデータを遠隔地へ転送可能！



■ 重複排除バックアップソフト

イメージバックアップソフト  
Arcserve UDP

※別途専用サーバーが必要

■ 重複排除バックアップデバイス

HP StoreOnce  
NEC iStorageHS

※別途バックアップソフトが必要