Solution

セキュリティ

なんの数字だかわかりますか？

25% ▶ **2016年 ランサムウェアに 感染した企業の割合**

不注意な“クリック”がビジネスを止めてしまい被害も深刻化！

ランサムウェアとは

ランサムウェアとは、感染したPCをロックしたり、ファイルを暗号化したりすることによって
使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムです。

ランサムウェア感染した企業の被害事例

case1 **経理サーバーが全滅。**バックアップするも数日前のデータなので
復元して元にもどすのに1日以上かかった［製造業］

Case2 10名程度のファイルが暗号化され、また**社内基幹システムが修復不能**
となり、業者が復旧するまでに2～3日要した［出版・放送・印刷業］

case3 得意先の顧客情報や入出金情報等の重要データへのアクセスが止まり、
3日間で**約2,000万円の損失**となた［情報サービス・通信プロバイダ］

2016年7月～9月
ランサムウェア検出台数は
過去最大
（トレンドマイクロランサム被害実態調査により）

企業規模の大小に関係なく
ランサムによる攻撃が激化しています。
もはや、対岸の火事ではありません。

外部からの攻撃
不注意によるリスク
への対策を
ご提案いたします

▼

裏面へ

用途にあわせて2つのセキュリティパックをご用意

ネットワーク環境 導入構築・保守
ネットワークセキュリティパック

UTM機器の導入設置・フルタイム保守
ゲートウェイセキュリティパック

新世代のセキュリティ・UTM

RICOH

ゲートウェイセキュリティパック［GSP］

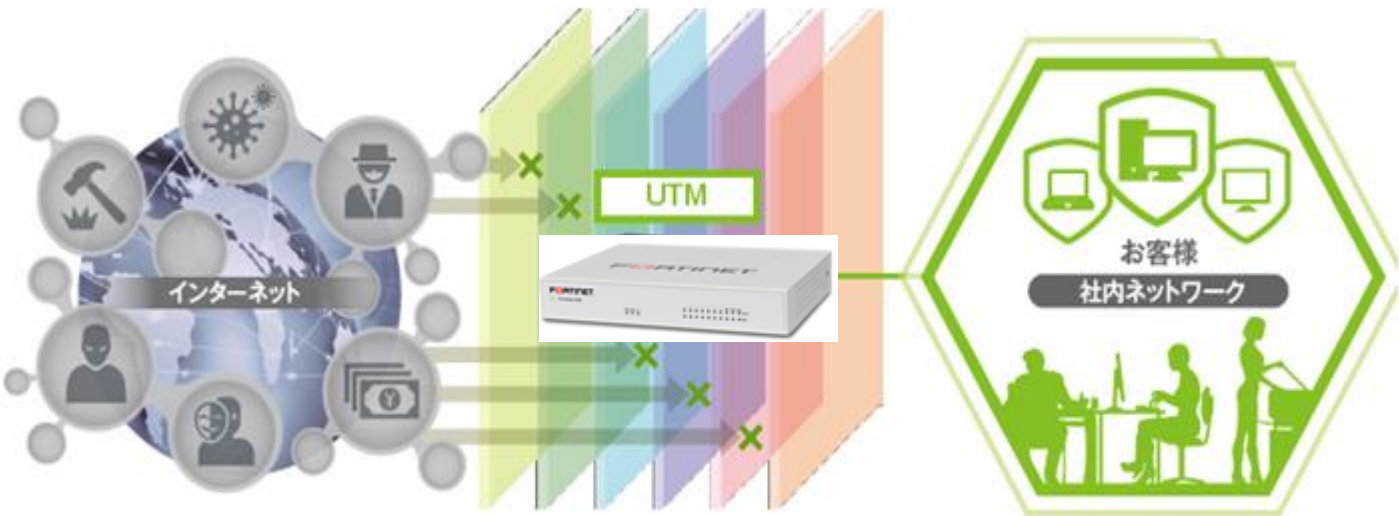
※UTM（Unified Threat Management）統合型脅威管理
※写真はネットワークセキュリティパックUTM

万一**クリック**してしまったとしても、豊富なセキュリティ機能で
ランサムウェアが悪さをする前に動きを止める！

①スパムメール対策　②不正サイトへアクセス制御　③攻撃者から通信遮
④不正ウイルス対策⑤URLフィルタリング

ゲートウェイセキュリティパック

ランサムウェアの特徴的な攻撃パターンをブロック



ネットワークセキュリティパック

ネットワーク活用もワンパッケージでご提供

- ■ネットワーク環境の導入
- ■周辺機器のNW設定
- ■設定変更等のリモート対応
- ■UTM機器状況の監視
- ■万一の際はオンサイト対応
- ■セキュリティ対策効果の確認

NSPとGSPの各サービス内容詳細をご紹介します。

お問合せは
株式会社　マルエイ六峰社
TEL(0154)25-0770