

広帯域のインターネット接続と ファイアーウォールをサービス型で提供

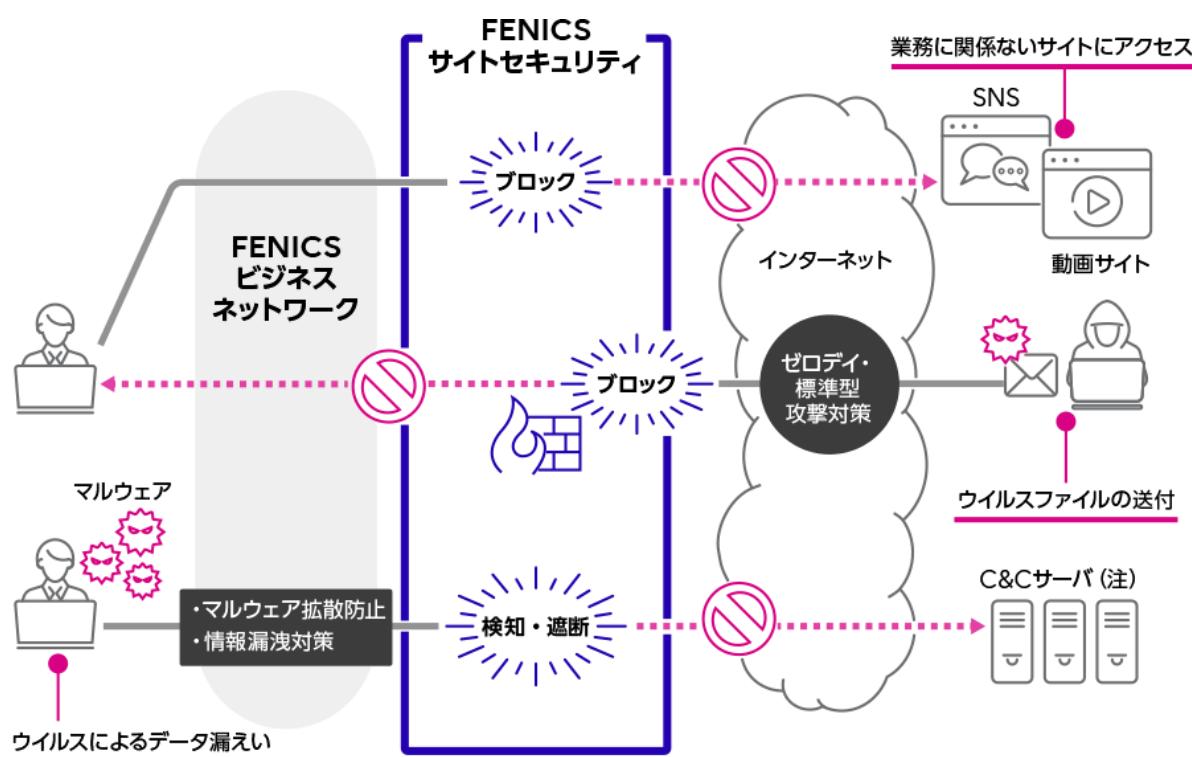
近年のサイバー攻撃は、未知のマルウェアによる標的型攻撃が増加しており、既存のセキュリティ対策をすり抜け、インターネットにまでマルウェアが侵入する（既に侵入している）ケースが増えています。そのため、侵入された後の対処を前提とした新たなセキュリティ対策が重要になっていきます。しかし、日々発生する未知のマルウェアへの対策には専用のアプライアンス装置やクライアントソフトウェアなどが必要となり、導入時のコストや、導入後の維持・運用に膨大な費用やリソースが必要になってしまいます。

FENICSサイトセキュリティは、未知のマルウェアを含む標的型攻撃への対策機能をサービス型にてご提供しますので、迅速な導入と、お客様の設備投資コストや運用負荷の軽減が可能となります。

サイトセキュリティ導入の価値

解決策

- ◆ 業務に関係ないサイトへのアクセスを制限しガバナンス強化
- ◆ サンドボックス分析によるゼロディ・標的型攻撃への対策強化
- ◆ C&Cサーバとの通信遮断による情報漏えい対策強化



(注) 「command & control server」の略で、マルウェアに感染したPCに指令（command）を送り、遠隔制御（control）するサーバ。

サービスの特長

①高度な脅威識別機能を提供

従来のファイアーウォール機能に加え、ソーシャルメディア等の外部アクセスをアプリケーション単位で識別・制限します。これにより、内部からの情報流出を防ぎます。

②社外から社内へ、社内から社外へ、インターネットの入口・出口で、新たな脅威を遮断し、迅速に通知

・本サービスを通過したファイルデータ（PDF等）に対して、サンドボックス分析（注1）を行い、ゼロデイ攻撃、標的型攻撃をお客様へ通報します。これにより、ウイルスなどの脅威を早期発見し、拡散を防止できます。

・社内から社外に向けたウイルスやスパイウェアの通信を検知/遮断し、お客様へ通報します。これにより、感染後の影響を小さくします。

（注1） 外部との通信で受け取ったプログラムを、保護された領域で動作させることにより、一般的なウイルス対策ソフトで検知できないマルウェアを見つけ出す分析方法

③クラウド利用に適した1Gbpsインターネットアクセス

1Gbpsベストエフォートのインターネットアクセス環境により、クラウド利用等により増大するトラフィックに対応しています。

④お客様の運用負荷の軽減

サイトセキュリティでは運用のための技術者の確保や運用負荷（人件費等）の軽減が可能となります。24時間365日の監視を行い、毎週1回、稼働状況のレポート作成やサイトセキュリティで遮断された脅威のログを専用Webポータルに掲載します。これにより、脅威の検出状況をわかりやすく確認することができます。

サービス構成

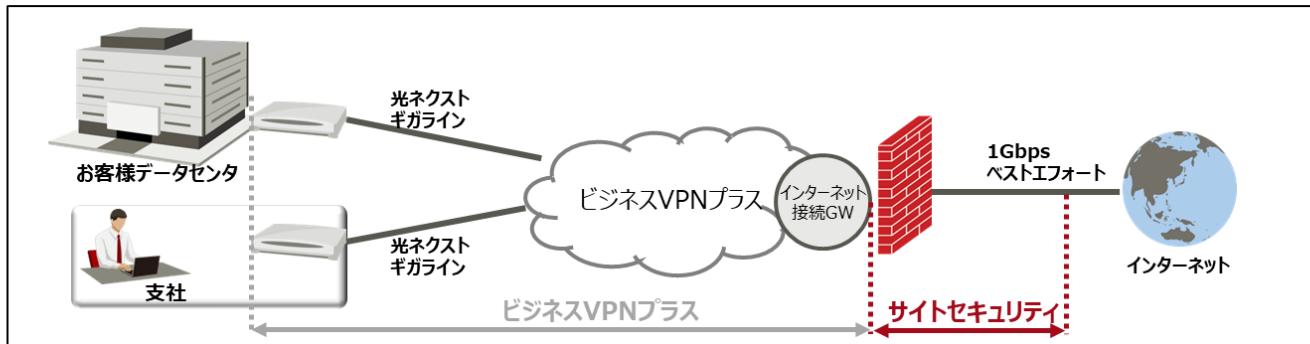
●ビジネスVPNプラスとサイトセキュリティご利用の場合

●ビジネスVPNプラス

- 拠点数 : 5拠点
- オプション : インターネット接続GW

●サイトセキュリティ

- 基本サービス : URLフィルタリング、アプリケーション制御等
- アナライズオプション : ゼロデイ攻撃、標的型攻撃対策



お問い合わせ先

製品・サービスについてのお問い合わせは[コチラ](#)

富士通株式会社 〒211-8588 神奈川県川崎市中原区上小田中4-1-1

