ニューノーマル時代のワークスタイルの変化にも対応

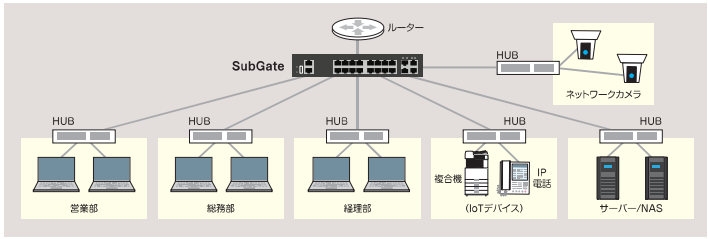
テレワーク環境におけるセキュリティ強化を後押し

テレワークにより、業務端末が社外で利用されるシーンが加速的に増えることにより、これまでのオフィスのネットワークからの侵入だけでなく、持ち込み端末からの二次感染などのリスクを検討する必要があります。SubGate製品はこういったシーンでも大きな力を発揮します。

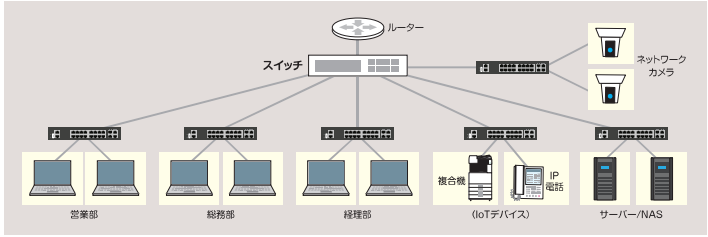
SubGate 構成例

SubGateの設置場所は大きく分けて2パターンあります。
メインスイッチをSubGateに置き換えると島ごとの拡散を防止対策となり、HUB代わりにSubGateを設定すると、デバイスごとに拡散防止が可能となります。

■メインスイッチをSubGateへ　［拡散防止はHUB単位］



■各島ごとにSubGateを設置　［拡散防止は端末（デバイス）単位］※1ポートに1台接続の場合



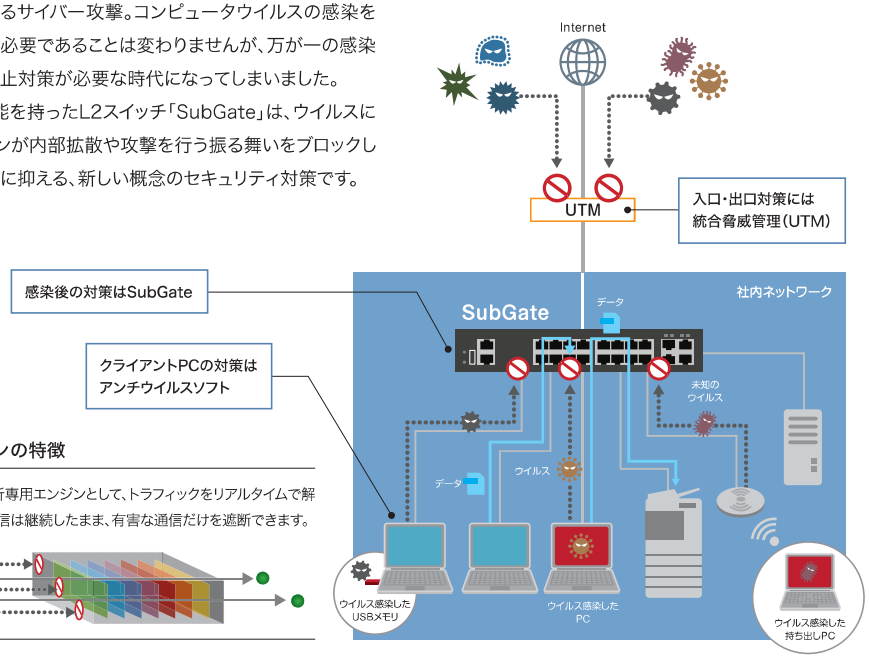
お問い合わせ

SubGate

ネットワーク内での拡散を防ぎ、感染後の被害を最小限にとどめて業務の円滑な遂行を維持する。

ウイルスソフトやUTMによる感染予防に加え、これからは「感染後の対策」も必須に。

身代金ウイルスと呼ばれるランサムウェアを筆頭に、高度化・巧妙化の一途をたどるサイバー攻撃。コンピュータウイルスの感染を予防する対策が必要であることは変わりませんが、万が一の感染に備えた拡散防止対策が必要な時代になってしまいました。
セキュリティ機能を持ったL2スイッチ「SubGate」は、ウイルスに感染したパソコンが内部拡散や攻撃を行う振る舞いをブロックして被害を最小限に抑える、新しい概念のセキュリティ対策です。



■MDSエンジンの特徴

有害トラフィック分析専用エンジンとして、トラフィックをリアルタイムで解析。正常な業務の通信は継続したまま、有害な通信だけを遮断できます。

SubGate の機能

■拡散防止

ウイルスの動きをいち早く検知し、二次感染を防ぐ

ネットワーク内の端末情報を収集して次なる感染先を探し出し、被害の拡大を狙うウイルスの動きを検知・遮断し、二次感染を防ぎます。

■被害軽減

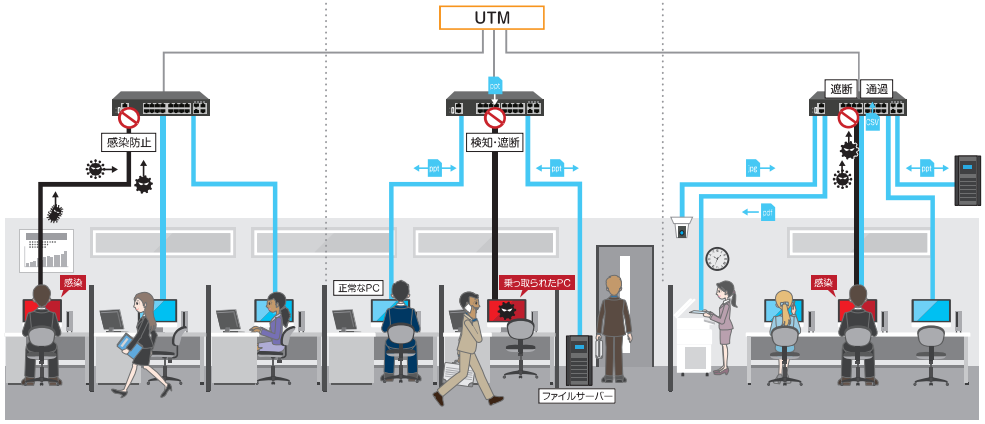
不正な傍受・改ざんによる攻撃を、未然に防止する

通信の不正な傍受・改ざんを行うARPスプーフィング攻撃を検知し、音声や画像、ファイル、パスワードの搾取を未然に防止します。

■業務遂行

攻撃パケットのみ遮断して、ウイルスを封じ込める

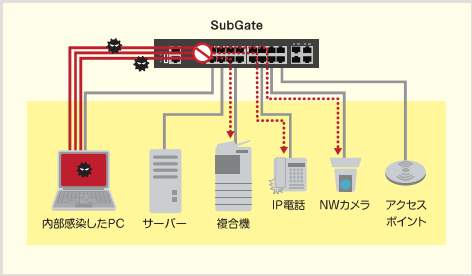
ネットワークの遅延、アクセス不能などにつながる攻撃パケットのみ遮断し、業務の遂行を妨げることなくウイルスの活動を封じ込めます。



SubGate の導入メリット

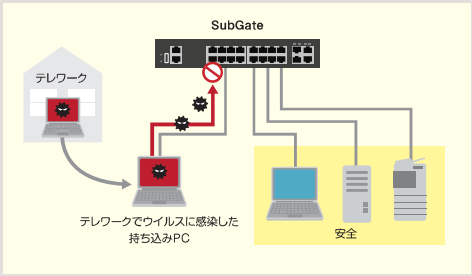
IoT機器のセキュリティにも有効

パソコンやサーバーのみならず、機器自身にセキュリティが適用しにくいIoT機器もLANにつなぐだけで保護OK。万が一感染してしまったデバイスからの二次被害や攻撃をSubGateが検知、ブロックします。



テレワークで使用した機器の持ち込みも安心

万が一感染していても、ウイルスの拡散防止を図ることができ、被害を最小限に抑えることができるので、テレワークで使用したPCやUSBメモリを社内ネットワークにつなぐ際も安心です。



SubGate管理ツール「VNM(Visual Node Manager)」

ネットワークの状況を一目で把握できる

- **通信状況を可視化し、社内ネットワークを管理**
- **複数台のSubGateを同時に管理**
- **検知、ブロック情報をリアルタイムで確認、ログでイベント追跡**

発生したインシデントは雷マークで表示され、攻撃を受けた端末を特定することが可能です。
また、インシデントが発生した際には担当者にアラートメールで通知を行う機能も搭載しています。
その他、インシデントのレポート表示やIP死活監視をリアルタイムで把握することができます。