

ちょっと待ったー!

テレワーク明けの **[帰還PC]** にご用心!!
普通につないでませんか?

**テレワークで使用したPCは、帰還後に
社内にウイルスをばらまくリスク大!**

やっちゃダメ接続1 -自宅のネット-
攻撃者やりたい放題!

やっちゃダメ接続2 -フリーWiFi-
無防備・感染し放題!

守るべきは、企業の3密

- ① 秘密 (社外に知られたくない情報) 悪評・噂・風説の流布
- ② 機密 (社外に出せない重要な情報) 不利益・技術情報流出
- ③ 厳密 (改ざんをされては困る情報) 判断ミス・トラブル等

しかし、現実には・・・。

自宅のネット環境へ接続

会社からポケットWiFiを支給してもらっていないし、
スマホのテザリングは繋がりにくい!!
結果、家族と同じネットワーク内で仕事している状況に!

貸し会議室やフリーのネット接続

感染・乗っ取り等のセキュリティ事故に対する

保証は一切ありません!

対策は裏面をご覧ください。



感染拡大によるネットワーク崩壊

テレワーク明けの帰還PCからのウイルス・脅威の拡散を防ぐ

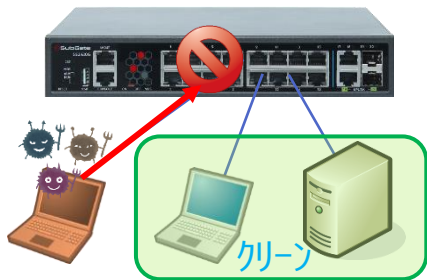
究極のセキュリティスイッチ

SubGate

サイバーウイルスのクラスターにならないために！

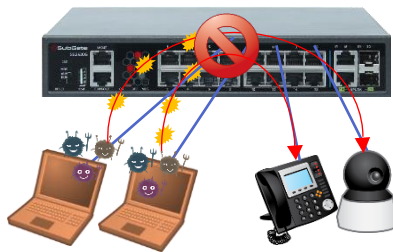
ウイルスの拡散を防止！ DoS攻撃を即時に遮断！ 盗聴御行為を防止！

ウイルス拡散防止



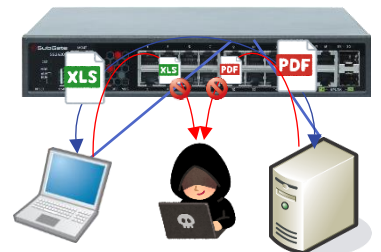
ウイルス拡散時の前兆動作を検知・遮断し、脅威の蔓延を阻止します。

DoS/DDoS攻撃ブロック



大量の packets を送り、機能を停止させるDoS攻撃など、有害な packets を検知し遮断します。

データ盗み取り防止



通信の間に割って入り、不正に情報を盗み取る行為「ARP-Spoofing」を遮断できます。

入れて良かった！ SubGate Story

Story1

会社内



部長
「みんな、明日からテレワークだ！」
部長
「緊急事態のため、社用PCを使用し
ての自宅での業務を許可します。」
営業一同
「かしこまりました。」

Story2

自宅



営業A
「さあ！自宅を使っているWifiに接続
して仕事にとりかかろう！」
営業A
「よし、今日の業務、終わったぞ。」
営業A
「なんか、変な通知が来るけど、大丈夫
でしょ！」

Story3

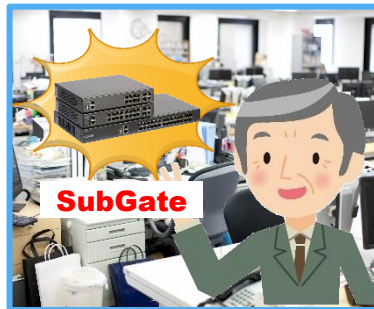
会社内(テレワーク終了後)



営業A
「今日のは社日！
社内LANにPCを接続完了！」
営業A
「あれ、なんかPCが変だぞ！。も、
もしや。。。ウイルス？」
営業A
「部長！、た、大変です。」

Story4

会社内



営業A
「私のPCがウイルス感染したみたい
です〜〜泣。
他のパソコンやサーバにも拡散したか
もしれません」
部長
「状況はわかった。SubGateを導入
しているから拡散は防いでいるぞ。
導入しておいてホントよかった！」

お問い合わせ