正常な通信のみを通過

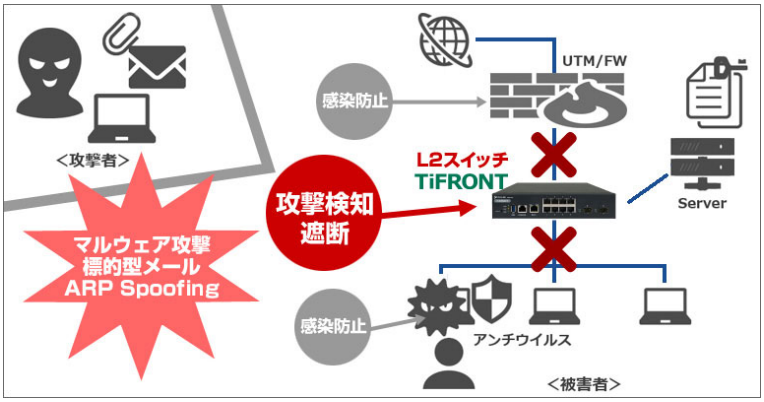
危険な通信のみをブロックするセキュリティスイッチ
ランサムウェア対策や旧OS端末のセキュリティ対策にも

TiFRONT
クラウド管理型

■ TiFrontの概要

TiFRONTは、セキュリティエンジンを搭載したハードウェア製品です。L2スイッチやHUBをTiFRONTに置き換えることで、基本的な通信のスイッチング機能とセキュリティ対策機能の両方を担わせることができます。最小限の構成変更で導入が完了し、その後は自動でネットワークの監視を行い、危険な通信のみをブロックします。これにより、業務を止めないセキュリティ対策が実現します。

- ◆ 危険な通信のみをブロック。
  業務を止めずにオペレーションが可能
- ◆ 既存のL2スイッチと置き換えることで、
  セキュリティ強度を大幅にアップ
- ◆ 攻撃の兆候を検知したら、即遮断を実行
- ◆ 管理システム（TiController）上で
  攻撃情報のモニタリング・レポート作成が可能



■ TiFrontの特徴

① サポート終了端末のセキュリティを確保

TiFRONTは、ファイアウォールやエンドポイント対策製品に付加できる、セキュリティ製品です。L2スイッチやHUBに代えて設置することで、経由する通信の挙動を監視し、異常を察知した場合に自動で通信を遮断します。これにより、配下に属するすべての端末を保護することができます。これは、Windows XPなど、脆弱性を抱えた端末を含むネットワークのセキュリティ対策として有効です。※

※OSのアップデートは推奨されます。

TiControllerの管理画面

② ランサムウェア・ファイルレス攻撃対策に有効

TiFRONTが攻撃を検知すると、それに関わる不正な通信および内部拡散の経路となる通信を遮断します。これにより、感染の拡大や事態の深刻化（ラテラルムーブメント）を防ぎ、被害を最小限に抑えます。マルウェアがUSBメモリなどを媒介として持ち込まれた場合も、同様に機能します。
検知には、ふるまい検知方式を採用しているため、ランサムウェアや標的型攻撃、ファイルレス攻撃など、未知の脅威にも有効です。

③ 内部不正接続を取り締まり

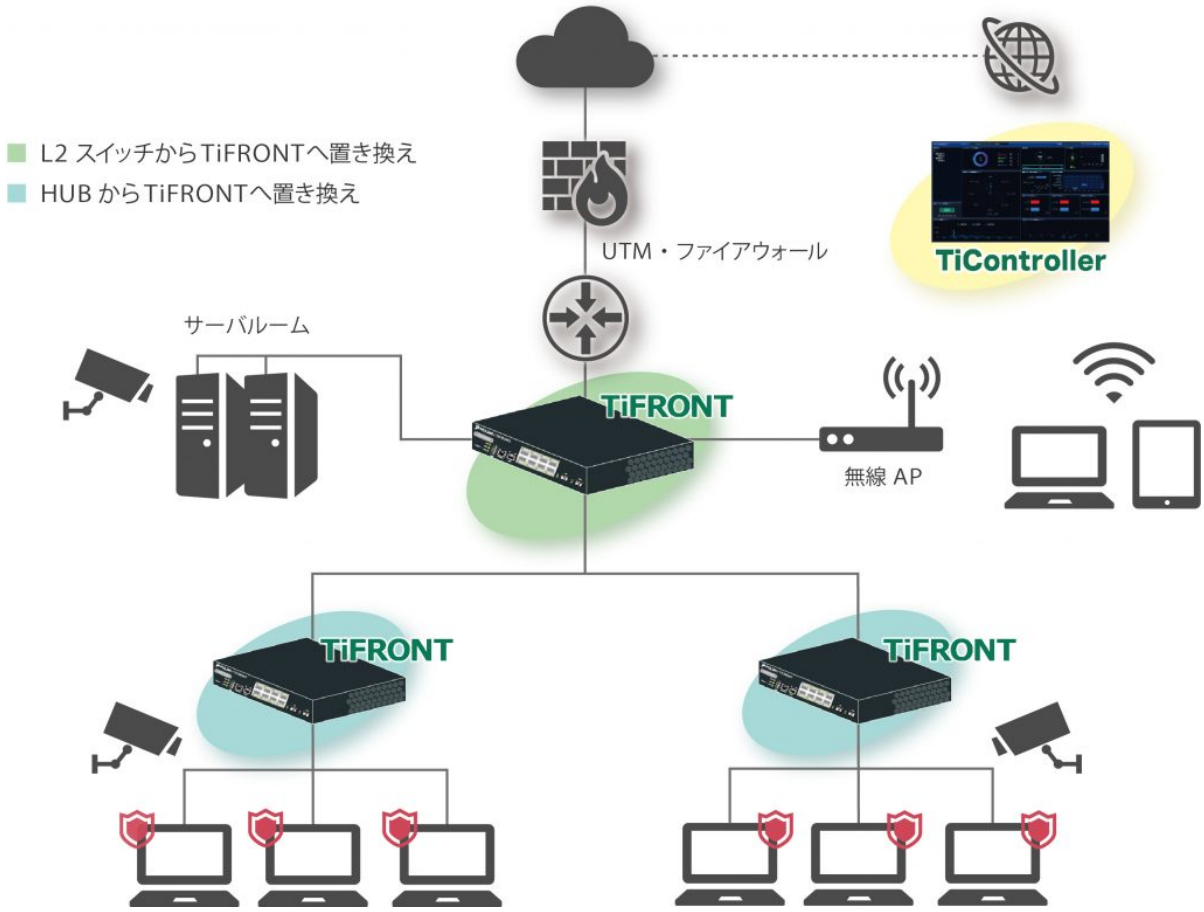
TiFRONTが設置されているネットワークに属する端末の情報を管理することができます。ネットワーク内での不正接続を検知し、必要に応じて遮断します。これにより、内部からの不正接続対策が可能です。

④ エージェントレスな導入形態

導入時に、ネットワークの構成を大きく変更する必要がありません。これによって、スムースな導入が実現します。

■ システム構成（通常構成例）

端末へのエージェントのインストールは不要です。



※内容は予告なく変更することがあります。

情報セキュリティ株式会社
〒650-0012 神戸市中央区北長狭通4丁目9-26　西北神ビル3・8階
TEL：078-381-8980（10:00~17:00　土・日・祝除く）
FAX：078-381-8979
E-mail:　inquiry@isec.ne.jp　URL: https://isec.ne.jp