PIOLINK

ネットワークにもカイゼンを

攻撃にも強い組織のための
合理的なスイッチを選択せよ

ネットワークにも“カイゼン”を

攻撃に強い組織のための合理的なスイッチを選択せよ!!

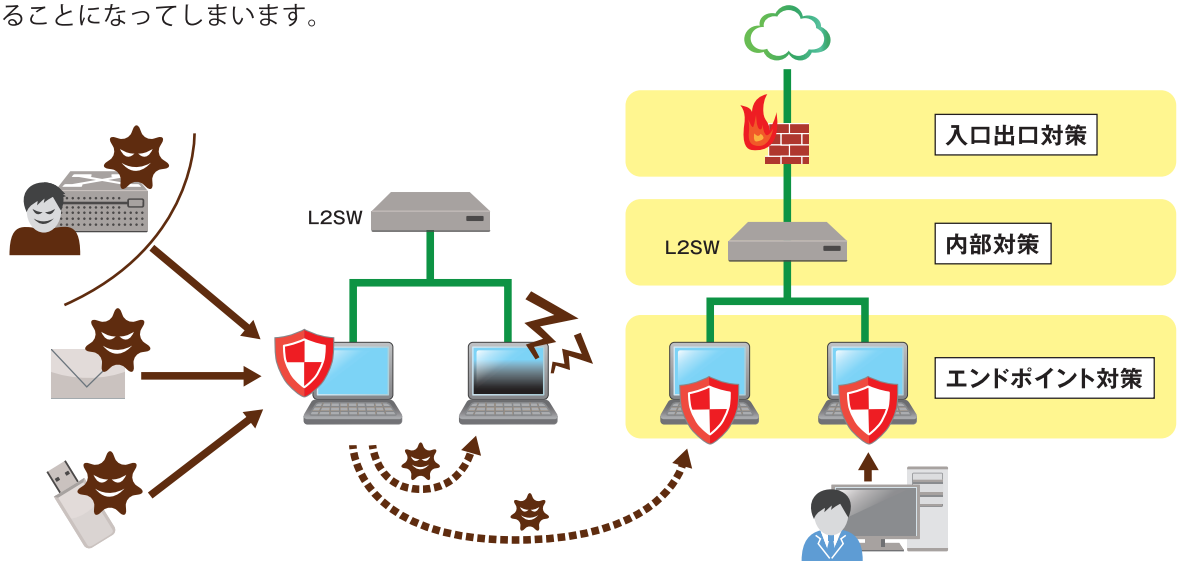
ネットワークにも「清潔さ」や「しつけ」を

製造業の世界では、職場を改善するスローガンとして“5S活動”という、誇るべき指針があります。いらないものを捨てる「整理 Sort」、決められた場所に決められたものを置く「整頓 Set」、常にクリーンな状態を保つ「清掃 Shine」、その上で衛生状態を保つ「清潔 Standardize」そして決められたルールを守り、手順に従う「しつけ Sustain」―これらはみな、ネットワークの世界でも同じことが言えるのです。

5S活動

情報をつなぐネットワークでは、いま未曾有の危機が差し迫っています。WannaCryやMirai、Emotetといった破壊的なマルウェアや、ランサムウェアなど大きな被害をもたらす攻撃、未知の脆弱性を利用したゼロデイ攻撃など、いわゆる「標的型攻撃」への対策が必要とされています。これらへの攻撃の個別の対策をしていては、次から次へとやってくる新しい攻撃のたびに、私たちは頭を悩ませることになってしまいます。

製造業に習い、ネットワークの世界でも整理、整頓し、きれいに清掃して清潔になるよう心がけ、その中の通信をしつけることができれば、外部からやってくる攻撃も、内部の感染拡大もすぐに気がつくことができ多くのトラブルは未然に防ぐことができるはず。そのコンセプトが、パイオリンクの「TiFRONT」シリーズに根付いています。

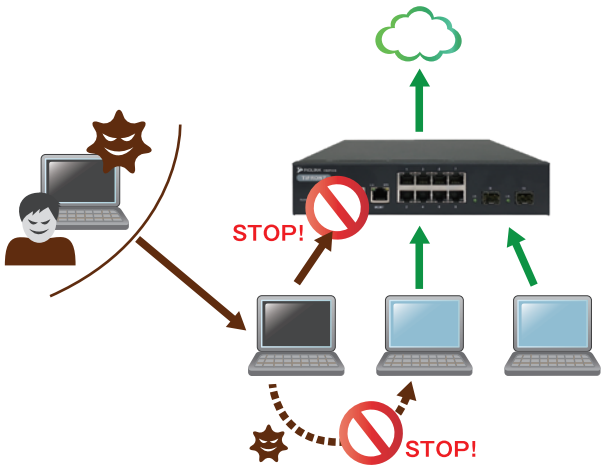


TiFRONTの機能は「攻撃者の心理」に合わせて作られている

サイバー攻撃を行うものが最も嫌うのは、きっと「きれいでよく見えるネットワーク」でしょう。悪いことをしたらそれがすぐ見えるようになっていれば、対策が打てるとともに「この組織は手強い」という印象を与えることができます。では、そういった状態にするためにはどのような機能が必要でしょうか。

TiFRONTシリーズには、サイバー犯罪者がネットワーク侵入後に利用する“攻撃性トラフィック”を検知し、それに対処できる機能があります。攻撃性トラフィックとは、例えばPCにバックドア型不正プログラムを仕掛けるだけでなく、情報収集をするさまざまな攻撃を実行するのに利用できる「ARPスプーフィング」や、組織にどのような端末が存在しているのかをチェックする「スキャン」、サービス停止を狙う「Dos/DDoS攻撃」などがあります。これらの偵察行動を止めることができさえすれば、サイバー犯罪者の最終目的である情報の詐取やシステムの破壊に至ることなく、あなたの組織を守れます。

これはまるで、ネットワーク内に悪意ある犯罪者が入り込んだとしても、“手足を縛られ真っ暗闇の状態に放り込まれた” ようなもの。おそらく、その状態の犯罪者は早々に諦め、次の簡単に攻略できる組織に目標を変えることでしょう。彼らはきっと思うはずです――「この組織、俺たちの行動が先回りされている！」
マルウェアが使う“道具”を封じ込めれば、新種のマルウェアが出るたびに対策に追われる必要はありません。攻撃者の視界を奪い、手強さを体感させる。TiFRONTはそのように設計されています。



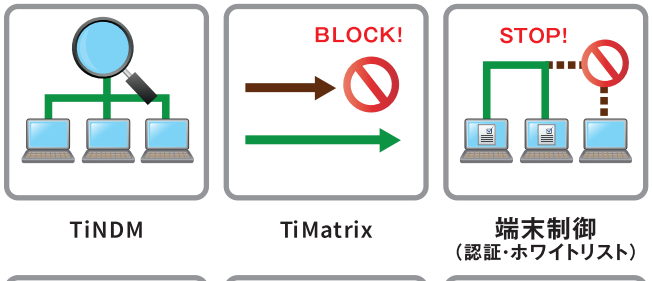
気付けるからこそ、行動ができる

TiFRONTシリーズは“L2スイッチ”でこれら不正なトラフィックを素早く検知し、セキュリティスイッチとして通信を外部に伝搬させないということが実現できます。既存のセキュリティ対策に加え、この仕組みを追加することで、トラフィックを整理整頓でき、清潔な状態がキープできるはずです。

これ以外にも、TiFRONTシリーズではセキュリティアセスメント、脆弱性診断を行える「TiNDM」でネットワークの“整理”が可能。策定されたセキュリティポリシーをTiFRONTに適用し、ネットワーク内に存在するデバイス資産管理を行うことで、不要、不正なデバイスが検知でき、整頓が行えます。また、「TiController」を活用することで、ネットワークのクリーンな状態を管理し、モニタリングを行うことで清潔な状態を維持。もちろん、監査も行えますので、しつけも完璧です。

「管理者不足」の現場でも大丈夫。TiFRONTシリーズは不審な行動を検知したタイミングで、的確なアラートを発行できますので、システム管理者が常にコンソールに張り付くことなく、アラートをきっかけとしたチェック体制をとることができます。これならば、セキュリティ担当を兼任せざるを得ない環境でも運用が可能です。

TiFRONTクラウド管理型モデルであれば、箱を開けてネットワークに繋ぐだけで、クラウドから設定が降ってきて自動設定も可能。離れた拠点に設置するのも簡単です。



TiNDM　TiMatrix　端末制御（認証・ホワイトリスト）

レポート　ダッシュボード　アラート

“サプライチェーン対策”としても有効、目指すは取引先も安心できるネットワーク作り

情報処理推進機構（IPA）が2020年2月に発表した「セキュリティ10大脅威2020」には昨年に続き、4位に「サプライチェーンの弱点を悪用した攻撃の高まり」がランクインしました。サプライチェーンとは、原材料や部品の調達、製造、在庫管理、物流、販売までの一連の商流、およびこの商流に関わる複数の組織群のこと。例えば業務委託先組織がセキュリティ対策を適切に実施していないと、業務委託元組織への攻撃の足がかりとして狙われることになります。

サプライチェーンのリスクを適切に下げることは非常に難しく、多くの場合は取引先からの「信頼」を信用するしかありません。おそらく多くの企業は取引先から「適切なセキュリティ対策が行われているか？」という問いを突きつけられていることでしょう。

これに回答するためにも、これまで投資してきたマルウェア対策や境界対策だけでなく、その上で「内部対策」「見える化」そして「検知したら、即対応」が可能な状態を、取引先にもアピールする必要があります。TiFRONTシリーズを組織内に配置することで、悪意ある通信をしっかり検知し、それを通過させない環境が作れることこそが回答になるはずです。

もっとも必要なのは「安心」「信頼」だから、スイッチも合理的な選択を

サプライチェーンに対する攻撃対策は、セキュリュティにおけるトライアスロンのようなもの。内部から、外部からの攻撃の全てに対策を行ってはじめて、安心や信頼を得ることができます。これまで、L2スイッチの機能といえば「通信できること」でしかありませんでした。そのL2スイッチをセキュリティスイッチに進化させ、正しい通行手形を持つものだけが通れる「ネットワークの関所」として動作させること、この礎になるものが、パイオリンクのTiFRONTシリーズなのです。
マルウェアの進歩、そして内部不正が当たり前になったこの時代、組織の内側だからといって、全てを信頼すべきではありません。より小さな単位でインテリジェントなスイッチを導入し、ネットワークをきれいに可視化することが、安全、安心を作り出す秘訣なのです。そのためにも、あなたの組織のネットワークに新たな機能を追加し、「Security switch is everywhere」の世界を作ることで、自社だけでなく取引先を含めた大きな流れ全体に、安心と信頼を手に入れましょう。

TF9130_202002