TiFRONT-SecuritySwitch 製品紹介

アクセスネットワークのセキュリティ対策

株式会社 パイオリンク

2012年5月

目次

1. はじめに

公共機関、学校、企業などの組織は業務継続性をもって独自の業務を遂行するために多くのITリソースに投資してきた。そして、このようなITリソースがネットワークを介して活用されることによって発生する様々なセキュリティ上問題を解決するための方策を講じてきた。

従来の伝統的なセキュリティシステムを見ると、インターネットなどの外部ネットワークと組織の内部ネットワークを結ぶコアネットワーク区間にインライン上に設置され、主要なサーバー機器やサービス、そしてネットワークリソースに対する各種セキュリティ機能を実行している。このようなセキュリティ機能としてはファイアウォール、IPS、Webアプリケーションファイアウォールなどがある。外部からの攻撃に対して防御を主な目的としたネットワーク環境では入口対策と称される、コアネットワークと主要なサーバーのためのセキュリティシステムの構築だけでセキュリティ対策としてはある程度の効果が期待できたが、徐々にサイバー攻撃が巧妙化、知能化、高度化して攻撃手法が進歩することによってもはや入口対策をメインに実施してきたセキュリティ対策をコアネットワークに集中するだけでなく、アクセスネットワーク及びエンドポイント対策までに拡大せざるを得ない状況になってきたといえる。

昨今のセキュリティ脅威として注目を集めているのが、標的型攻撃（APT：Advanced Persistent Threat）があるが、この場合も同様である。単純にコアネットワークのためのセキュリティ対策だけでは、標的型攻撃の防御ができないだけでなく、攻撃を受けたことすら把握していない場合が発生できる。特定目的を持ってターゲット組織に対して継続的に脆弱性を見つけて攻撃を仕掛ける標的型サイバー攻撃を防御するためには、エンドポイントのセキュリティソリューションやアクセスネットワークのセキュリティソリューションを構築して対応しなければならない。エンドポイントのセキュリティソリューションはウイルス、悪性コードなどを検知し駆除するアンチウィルスが主流であり、アクセスネットワークのセキュリティソリューションは有害トラフィックの遮断、DoS/DDoS 攻撃の発生防止、ARP 攻撃の遮断、アクセス制御やユーザー認証を行うセキュリティスイッチが有効である。

2. TiFRONT-セキュリティスイッチの概要

■ 製品の定義

TiFRONT（ティーフロント）-セキュリティスイッチは、「Traffic Inspection + FRONT」という意味で、日々増加するサイバー攻撃の脅威に対する対策として提案するアクセスネットワークのセキュリティスイッチ製品である。公共機関、学校、企業などの各組織が信頼できる安全なネットワークを作るためには外部ネットワークと接続されるコアネットワークのセキュリティ対策だけでなく、内部ネットワークの出発点となるアクセスネットワークのセキュリティ対策が同時に確立されなければならない。

そのためにTiFRONT-セキュリティスイッチは、ネットワーク構成の基本要素である L2 スイッチの役割とユーザー端末に対するセキュリティ対策を同時に実行することを目的として開発されたセキュリティスイッチである。TiFRONT-セキュリティスイッチは、一般的な L2 スイッチと同等レベルの機能と性能を提供するだけでなく、ユーザー端末からの不正なトラフィック、不正なアクセス、ARP 攻撃などの防御及びユーザー認証などの機能を同時に提供することが特徴である。

従って、公共機関、学校、企業などの各組織は、悪性コードと DoS/DDoS、そして有害トラフィック発生などのユーザー端末によって発生する可能性のある様々なサイバー攻撃に対してTiFRONT-セキュリティスイッチを活用して、各種サイバー攻撃を事前に遮断するアクセスネットワークのセキュリティソリューションを構築することができる。

■ 主な機能

TiFRONT-セキュリティスイッチは VLAN、Spanning Tree、MAC Learning、LACP、IGMP、QoS、Jumbo Frame などのデータトラフィックを転送する L2 スイッチ機能と DoS/DDoS 発生防止、有害トラフィックの自動検知及び遮断、Protocol Anomaly、認証、ARP 攻撃の防御、IP 管理などのアクセスネットワークのセキュリティ機能を組み合わせたものである。

L2 スイッチ機能に関連する主な機能は次の通りである。

VLAN 機能は、TiFRONT-セキュリティスイッチの全モデルで同時に最大 4K を作成して Hybrid VLAN 方式を採用し、顧客のニーズに合わせて Port-based/Protocol/MAC/Voice/Guest VLAN などを生成して使用することができる。

Spanning Tree 機能は、基本的な 802.1D（STP）だけでなく、より様々なネットワーク環境に対応できて迅速な収束時間のために 802.1w（RSTP）、802.1s（MSTP）、PvSTP、PVRSTP+などをサポートしている。

MAC ラーニング機能は、TiFRONT-セキュリティスイッチ 1 台毎、最大 16K の MAC をラーニングすることができ、さらに MAC エージング/フィルタリング機能と重複 MAC ラーニング及びリバース MAC ラーニングを防止する機能をサポートする。

リンクアグリゲーション機能は、Link Aggregation Control Protocol（LACP）として最大 8 つのトランクグループを作ることができ、複雑なネットワークでも信頼性の高いネットワーク構成が可能であり、リンク間のロードバランシングも可能である。

IGMP Snooping 機能は、マルチキャストプロトコルのためにサポートしており、最大 1K のマルチキャストグループを作成して一度に多くの端末に情報を送信することができる。また、IGMP v1/v2/v3 をサポートして顧客の様々な選択に対応することができる。

QoS 機能は、レイヤー2/3/4 のヘッダー情報に基づいて分類する機能とポート毎 8 CoS Queue をサポートする。また、Diffserv と Min/Max 帯域幅の保証を行うことができる。

ジャンボフレーム対応については、TiFRONT-F26/G24 モデルの場合には 13K サイズをサポートし、TiFRONT-G48 の場合は 12K サイズをサポートして大容量のパケットサイズを処理するファイルサーバーやストレージなどの使用においても十分な性能を提供する。

アクセスネットワークのセキュリティ機能に関連する主な機能は次の通りである。

DoS/DDoS 攻撃の遮断機能は、有害トラフィックの自動検知及び自動遮断機能として、主に TCP SYN Flooding、UDP Flooding、ARP Flooding などの様々な DoS/DDoS 攻撃の発生を発生元となるユーザー端末を遮断することで実現する。多くの組織は、外部ネットワークからの DoS/DDoS 攻撃を防御する入口対策は講じていても、内部ネットワークから発生する DoS/DDoS 攻撃に対しては十分な対策が取られていないのが現状であり、アクセスネットワークにおける DoS/DDoS 攻撃の遮断機能は有効である。

ARP Spoofing の防御機能は、アクセスネットワークで実行可能な個人情報や企業の重要な情報の窃取、IP 電話、WEB カメラ等の盗聴などを防御できる重要な手段である。特に、IPT（IP Telephony）と WEB カメラ（Web camera）を活用する UC（Unified Communication）環境における個人情報（アカウント、パスワード情報）の窃取、盗聴対策としてプライバシー侵害を防止する重要な防御機能である。

IP/MAC アドレス基盤のアクセス制御及び 802.1x 基盤の認証機能は、認証サーバーと連携して非許可された端末のネットワーク接続を制御することができる。特に IP/MAC アドレスだけでなく、サービスポートと使用時間帯別のアクセス制御も可能なので、様々なユーザーにアクセス制御ポリシーを適用することができる。

標的型サイバー攻撃（APT 攻撃）に対応するために、標的型サイバー攻撃を検知するソリューションと組み合わせることにより、「検知したら即遮断」ができる外部ソリューションとの連動機能を提供している。つまり、標的型サイバー攻撃を検知/分析するソリューションが感染されたユーザー端末情報に基づいて、TiFRONT-セキュリティスイッチがユーザー端末のネットワークアクセスを遮断することができる。結果的に標的型サイバー攻撃を検知して遮断することにより、各種のハッキング事故の防止、ゾンビ PC の拡散防止、重要情報の流出防止等が可能となり、標的型サイバー攻撃（APT 攻撃）対策ソリューションとして活用することができる。

■ 製品の種類

TiFRONT-セキュリティスイッチの製品モデルは、H/W の要素に基づいてサポートする容量とポート数及び PoE/PoE+のサポート可否によって複数の製品モデルを提供する。そして S/W の要素である L2 スイッチ機能とセキュリティ機能は、全モデルで同じである。

TiFRONT-セキュリティスイッチの製品モデルは PoE/PoE+の有無によって 6 種類に分けられる。

Model	Ethernet Port	PoE/PoE+	Dual power
TiFRONT-F26	24 x 10/100 Base-TX port 2 x 1G Dual media combo port (Copper: 2x10/100/1000 BASE-T, Fiber: 2x1000BASE-X SFP type)	N/A	N/A
TiFRONT-F26P		IEEE802.3af/at	○
TiFRONT-G24	24 ports 10/100/1000 Base-TX (4 x combo port included, 1000BASE-X SFP)	N/A	N/A
TiFRONT-G24P		IEEE802.3af/at	○
TiFRONT-G48	48 x 10/100/1000Base-TX (4 combo included, 1000Base-X SFP)	N/A	N/A
TiFRONT-G48P		IEEE802.3af/at	○

3. 一般的なL2スイッチとTiFRONT-セキュリティスイッチの比較

■ 一般的なL2スイッチの限界

一般的な L2 スイッチは、ネットワーク上の通信パケットを転送することを基本機能とし、通信パケットが持つ様々な情報の種類に関係なく、単純に H/W 的な CRC エラーなどのみを検出してパケットを転送する機器である。従って、パケットを転送するときに発生する幾つかのセキュリティ脅威に対しては処理上、非常に脆弱であるといえる。特に、ユーザー端末が作る大量のトラフィックや大量のセッションに起因するネットワークの過負荷が発生する場合などに関して制御することができないので、不正な攻撃が組織内部で発生した場合などには、その組織全体のネットワークが麻痺することもできる。また、内部ネットワークから攻撃者が IP を偽/変造してハッキングを試みても検知及び遮断することが難しく、セキュリティ事故が発生してもその詳細を把握するのが難しい場合もある。このようなアクセスネットワークにおけるサイバー攻撃の問題を解決するために、これまで様々なセキュリティシステムを導入して解決しようとしているがアクセスネットワークまでのセキュリティシステムを導入して監視及び管理するためにはあまりにも膨大な投資が必要なことから対策が後手にまわっているのが実情である。

■ TiFRONT-セキュリティスイッチの可能性

特定の目標を対象に標的型サイバー攻撃（APT 攻撃）を実行する方法は、様々な悪性コードをユーザー端末に感染させ、ネットワークのリソースを枯渇させる。または、ユーザーの同意なしに重要な情報を盗み取る形で現れている。また、悪性コードに感染したゾンビ PC に対して、遠隔の攻撃者がいつでもリモートからゾンビ PC 化したユーザー端末を制御し、内部情報にアクセスする、またはこれを利用して大規模の DoS/DDoS 攻撃を仕掛けることができるようになった。このようにユーザーの意志と関係なく、アクセスネットワーク段で多くのセキュリティ脅威が存在するが、今までは適切な対応ソリューションがなかったのが実情である。ユーザー端末に対するエンドポイントのセキュリティ対策として、アンチウィルスやパーソナルファイアウォールなどを使用してきたが、これも悪性コードに感染され、サイバー攻撃に利用される場合も発生している。

このようなネットワーク環境で最適な対応セキュリティソリューションとしてTiFRONT-セキュリティスイッチがある。TiFRONT-セキュリティスイッチは、ネットワークにおけるデータ転送のための L2 スイッチ機能をフルに提供するとともに、有害トラフィックの遮断とユーザー認証機能、IP 管理機能などを活用してアクセスネットワークに必要な最適なセキュリティソリューション機能を提供する。なお、TiFRONT-セキュリティスイッチはアクセスネットワークにおける基本的なセキュリティ機能だけではなく、様々なセキュリティインフラストラクチャのセキュリティ機器（ファイアウォール/IPS/ウェブファイアウォール/悪性コードの検知システムなど）との連動により全体的なネットワークのセキュリティ確保を実行する上でも重要な役割を遂行することができる。

■ TiFRONT-セキュリティスイッチの導入メリット

多くの組織は、ファイアウォール、IPS/IDS、WEB ファイアウォール、UTM、DDoS 専用機器などのセキュリティ機器を従来からのセキュリティ対策として実施してきている。しかし、このようなセキュリティ機器はネットワーク上の業務用サーバーなどの重要なインフラストラクチャを保護するために使用されるコアレベルのセキュリティ機器である。反面、膨大なコストなどの理由にエンドポイント対策しか取られていないアクセスネットワークにおける対策としてTiFRONT-セキュリティスイッチを活用できる。

一般的に、アクセスネットワーク構築のためには L2 スイッチは必ず必要な機器である。従って、必要な L2 スイッチ機能として TiFORNT-セキュリティスイッチを導入してネットワークを構築する、同時に TiFORNT-セキュリティスイッチのセキュリティ機能を活用することにより、内部ネットワークから発生し得る様々な DoS/DdoS 攻撃及びセキュリティ脅威を検知して遮断する。これにより、ユーザーは、非常に安定的且つ信頼性の高いネットワークを構築することができて、最終的には組織の長期的な TCO 削減に貢献することができる。また、TiFRONT 統合管理システムである TiManager の活用により、アクセスネットワークにおけるネットワークの動作状況及びセキュリティ状況を一括して監視することができる。このような TiManager は、ネットワーク及びセキュリティ管理におけるリアルタイムの通知機能、及び遮断機能により運用コストの削減にも貢献できる。

TiFRONT-セキュリティスイッチの導入は、アクセスネットワーク段で発生する不正なトラフィック、TCP Syn Flooding、UDP Flooding、ICMP Flooding と ARP Spoofing、IP Spoofing などのサイバー攻撃による組織内の被害を事前に防ぐことができる。特に有害トラフィックを検知してTiFRONT-セキュリティスイッチで遮断する場合は、物理的なポート単位で遮断するのではなく、その有害トラフィックを発生させる IP のみを検知して遮断するため、他のユーザーのネットワーク利用には影響を及ぼすことなく、継続的な業務遂行が可能である。

もう一つのTiFRONT-セキュリティスイッチの導入メリットは、標的型サイバー攻撃を検知するソリューションと組み合わせることにより、「検知したら即遮断」ができることである。標的型サイバー攻撃は、巧妙化且つ高度化してきているので、攻撃を受けていることすら分からないことが特徴であり、怪しい動きがあれば直ちにその攻撃と疑われるゾンビ PC をネットワークから隔離することが重要であり、リアルタイムで隔離するためにTiFRONT-セキュリティスイッチが必要である。

4. TiFRONT-セキュリティスイッチの動作構造

■ 基本動作構造

TiFRONT-セキュリティスイッチは、安定性と品質の高い Broadcom 社のスイッチングチップセットを採用し、一般的な L2 スイッチが持つ様々な L2 スイッチ機能とプロトコルをサポートしている。また、様々な有害トラフィックの検知/遮断及び各種スプーフィングの検知/遮断などの機能を実行するためにエンジンとしては、Cavium 社の高性能のマルチコアの CPU を採用している。

TiFRONT-セキュリティスイッチの構造は、大きく L2 スイッチ部分と TiMatrix（ティーマトリックス）というセキュリティエンジン部分に区分される。一般的な L2 スイッチ機能である VLAN、STP、MAC Learning などのネットワーク設定とユーザー端末との接続などに関連した機能は L2 スイッチ部分で処理する。TiMatrix セキュリティエンジンは、様々な有害トラフィックの検知及び遮断機能を提供する。また、IP 管理機能を実装していて、1 台のTiFRONT-セキュリティスイッチで最大 256 個の IP へのアクセス制御を管理することができる。IP へのアクセスを許可・遮断するためのフィルタリング方法は IP のみをもって行うことも可能であるが、IP と MAC アドレスを組み合わせる方法、そして IP/MAC/ポートを組み合わせてユーザー端末のアクセスを許可、または遮断するかを決定できるようになっている。

TiFRONT-セキュリティスイッチは、スイッチング処理性能を基準に 100M と 1G のインタフェースに分かれている。基本的な動作構造は、L2 スイッチグ処理としてパケット転送を処理し、この過程で TiMatrix セキュリティエンジンを利用して様々なセキュリティ機能を実行することになる。具体的に処理の仕組みを理解するためにTiFRONT-セキュリティスイッチの内部のパケットの処理過程を調べてみると、ユーザー端末から送信されたパケットはTiFRONT-セキュリティスイッチに流入され、この時に L2 スイッチ機能を担当するスイッチング処理部分でパケットの転送に関連した一連の処理（ソース MAC、宛先 MAC、フォーワード処理など）が行われて、同時に TiMatrix セキュリティエンジンにもパケットが転送され、Protocol Anomaly => TCP/UDP/ICMP Flooding => ARP/IP Spoofing => Port Scanning などの順番でトラフィックの整合性等を検査し、サイバー攻撃を検知して遮断する措置を実行する。

前述のように L2 スイッチの部分と TiMatrix セキュリティエンジンの部分は別々に区分されているため、トラフィックの検査及びセキュリティ管理のための処理を行う TiMatrix セキュリティエンジンによって L2 スイッチング処理は影響を受けない。つまり、パケットの転送処理と同時に、セキュリティ機能が並列に処理されるため、セキュリティ機能を実行しながらも L2 スイッチとしてのワイヤスピードの処理性能を保証している。

TiMatrixセキュリティエンジンは、PLOS（Piolink OS）おいう専用エンジンで処理するために、新しいサイバー攻撃に対してアクセスネットワークで防御すべきの処理はソフトウェア開発により対応可能であるという特長をもっている。

■ セキュリティ機能の動作

TiFRONT-セキュリティスイッチは、L2 スイッチとしての L2 機能を処理しながら有害トラフィックを検知/遮断するセキュリティ機能を処理する「L2 スイッチ ＋ セキュリティ機能」を提供する。従って、L2 機能を利用するスイッチング処理においては、一般的な L2 スイッチと同レベルの機能と性能を提供する。しかし、セキュリティ機能及び性能については、アクセスネットワークで動作するスイッチであるために、コアネットワークで設置する通常のセキュリティ機器とは異なるので注意が必要である。つまり、TiFRONT-セキュリティスイッチは、アクセスネットワークにおいて L2 スイッチン

グ処理とセキュリティ処理を同時に行うため、スイッチ処理における処理性能と同じくアクセスネットワークで接続する適切なユーザー数に基づいて動作する。

TiFRONT-セキュリティスイッチは、標的型サイバー攻撃（APT 攻撃）自体を検知する機能は持っていないが、標的型サイバー攻撃の初期潜入段階、またはシステム調査段階においてアクセスネットワークから防御することができる。例えば、潜入した悪性コードによりシステムのスキャン、ARP スプーフィングを仕掛けてシステム管理者の ID・パスワードを奪取する段階などにおいてアクセスネットワークでその攻撃を検知して遮断することができる。なお、他の標的型サイバー攻撃を検知するソリューションと組み合わせることにより、「検知したら即遮断」ができるので多階層的な標的型サイバー攻撃の対策ができる。

最後に、TiFRONT-セキュリティスイッチが使用する TiMatrix セキュリティエンジンは、ネットワーク上で発生する様々な異常現象を数学的統計技法に適用して開発されたパイオリンク独自のセキュリティエンジンとして、シグネチャの必要がない。しかし、正常なネットワークトラフィックの動作であるのに、有害なトラフィックとして誤って検知する場合が発生する可能性がある。しかし、このような場合は、TiFRONT-セキュリティスイッチのセキュリティポリシー設定で例外設定として処理できるホワイトリスト（White List）機能を提供している。その他、フローディングなどの有害トラフィックに対して遮断できず通過させてしまう可能性があるが、これは主に大量のトラフィックが発生する初期に非常に短い時間で発生する可能性があるため、攻撃が続いた場合には確実に検知できるので実際のネットワークに障害までには至らないことである。

製品分類の理解のために、下記の表にアクセスネットワークにおけるセキュリティ製品とTiFRONT-セキュリティスイッチを比較し、主な特徴をまとめる。

[表 ： TiFRONT-セキュリティスイッチと主要なアクセスネットワークセキュリティ機器の比較]

区分	TiFRONT	Anti-Bot	Anti-DDoS	NAC
設置場所	エンドポイントの前段	G/W	G/W	G/W または 各ネットワーク
設置方法	アクセスネットワーク	Mirroring	In-Line or Out of path	Mirroring or Out of Path
L2スイッチ機能	○	X	X	X
検知対象の トラフィック	Incoming Outgoing	Incoming Outgoing	Incoming	Incoming Outgoing
検知対象	有害トラフィック DoS/DDoS IP/MAC/Port	悪性コード	外部のDoS/DDoS	不正ユーザー
トラフィック量	少ない (内部ユーザー)	普通 (外部の伝播者)	多い (外部攻撃者)	普通 (ユーザー認証)
セキュリティの 処理手法	統計的技法	行為分析 シグネチャ	行為分析 シグネチャ	IP/MAC ID/PW
要求スペック	低い	高い	高い	高い
処理性能 （ワイヤスピード）	○	X	△	X
管理しやすさ	良い	複雑	複雑	複雑
導入目的	L2スイッチ機能と セキュリティ機能	アンチボット専用	DDoS専用	ユーザー管理
製品価格	L2スイッチ価格より やや高い	非常に高い	非常に高い	非常に高い

5. TiFRONT-セキュリティスイッチの構成要素

■ TiFRONT-セキュリティスイッチ

今まで説明してきた L2 スイッチ機能とセキュリティ機能を提供するTiFRONT-セキュリティスイッチ本体である。TiFRONT-セキュリティスイッチは、実際にアクセスネットワークに位置してユーザー端末にネットワーク接続機能を提供すると共に、有害トラフィックの遮断、DoS/DDoS、Spoofing、ユーザー認証などのセキュリティ機能を提供する。

■ TiManager（ティーマネージャー）

TiManager は、TiFRONT-セキュリティスイッチの統合管理システムとして、アクセスネットワークに設置される多くのTiFRONT-セキュリティスイッチを統合管理するために開発したサーバー・クライアント型の専用システムである。サーバー及びクライアントモジュールは、Microsoft Windows 環境で動作し、DBMS は PostgreSQL と Microsoft の MS-SQL サーバーの中で選択して使用することができる。

主な特徴としては、小規模ネットワーク環境ではオフィス用の PC に設置して非常に手軽く使用できることと、複雑で膨大なネットワーク環境でも使用することが可能である。実際に 1000 台以上のTiFRONT-セキュリティスイッチを登録して運用管理した実績もある。

TiManager はTiFRONT-セキュリティスイッチを管理するために下記の連動プロトコルを使用している。

1. セキュリティ設定及び各種制御のためのプロトコル ： SNMP
2. TiFRONT-セキュリティスイッチのイベント収集プロトコル ： SysLog
3. IP管理のためのTiFRONT-セキュリティスイッチのIP収集及び制御プロトコル ： SSH
4. 検知ソリューションと連動のためのプロトコル ： SysLog、SysLog-NG、Customize

TiManager の基本機能は、統合されてダッシュボード、セキュリティ動作状況、ネットワークトラフィックの状況、ユーザーIP の使用現状、トポロジーなどを管理者が一目で見ることができる監視機能と TiFRONT の機器別/グループ別セキュリティ管理及びセキュリティポリシーの適用などのセキュリティ設定の管理機能、そして様々な攻撃の種類別、期間別のレポートを作成する機能がある。これらの全ての機能は、日本語により提供している。

[主な機能]

- セキュリティログ、またはTiFRONT機器の動作ログ発生時に迅速な対応ができるようにリアルタイムのセキュリティイベントの状況とネットワーク動作状況を表示する統合ダッシュボード
- 現在ネットワークを使用しているユーザーIPの現況を通じてどのユーザーが有害トラフィックを発生しているかを確認できるセキュリティログ
- TiFRONT-セキュリティスイッチの機器別/ポート別のトラフィック使用量の情報及びランキングなどのトラフィック現況の表示機能
- TiFRONT-セキュリティスイッチのセキュリティイベントの発生状況を知らせるセキュリティログ
- 機器の障害状況などの詳細情報を表示する障害ログ表示機能
- TiFRONT-セキュリティスイッチを経由してネットワークに接続しているユーザーのIP管理機能
- TiFRONT-セキュリティスイッチの接続状態及び構成図を管理するトポロジー管理機能

TiManagerサーバーの最小構成の推奨スペックは下記の通りである。

- CPU ： Intel Core i5 2.x以上
- Memory ： 3GB以上
- HDD ： 200G以上
- O/S ： Windows XP, Windows 7, Windows Server 2003/2008 (現在32Bitのみサポート)
- DBMS ： PostgreSQL 9.0.2以上, MS-SQL 2008以上

リアルタイムのモニタリング

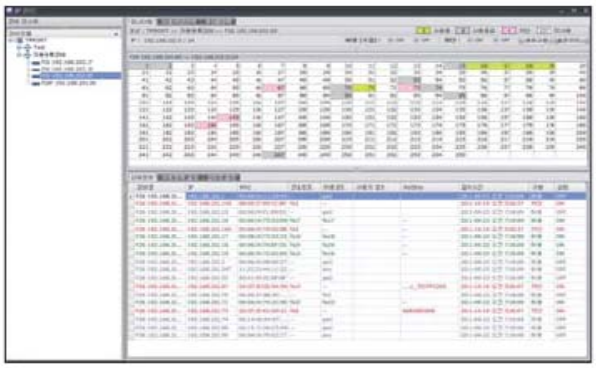
リアルタイムのトラフィック、セキュリティ侵害の状態のみならず、セキュリティスイッチ、ユーザーIP使用現況等を一目で把握できる。セキュリティログ、機器の動作状態ログ及びネットワーク構成状態等をリアルタイムで確認できる。

細密なセキュリティ設定

TiFRONT-セキュリティスイッチに個別/グループ別のセキュリティポリシーを設定することができる。
ポート別セキュリティポリシー設定で使用するIP/MAC/ポートを指定して使用時間を制限したり接続を許可/遮断できる。

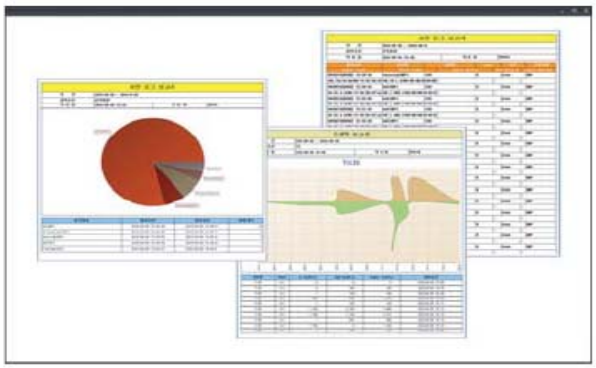
ユーザーIP管理

どのセキュリティスイッチの何番ポートにどんなIPで誰がいつ使用したのかなどをリアルタイムで把握できる。IP/MAC基盤のユーザー認証でIPリソース管理及び端末の接続制御及び履歴照会ができる。



多様なレポート

セキュリティスイッチと登録されたIP情報に対する報告書を出力する。数十～数百台に至るスイッチと各ポートに接続したIP情報をトラフィック状態、セキュリティ状態、機器状態などのレポートを出力することができる。



■ TiMatrix（ティーマトリックス）セキュリティエンジン

TiMatrix セキュリティエンジンは、TiFRONT-セキュリティスイッチで使用する専用のセキュリティエンジンとして、パケットの送信元 IP、宛先 IP、送信元 MAC、宛先 MAC、流入ポート、パケット数、タイムスタンプなどの要素を活用して、それぞれの送信元/宛先別の使用頻度、パケットの間隔、隣接タイムのパケット情報などをリアルタイムに分析し、自動的にサイバー攻撃を検知して遮断ポリシーに反映するパイオリンク独自のセキュリティエンジンである。

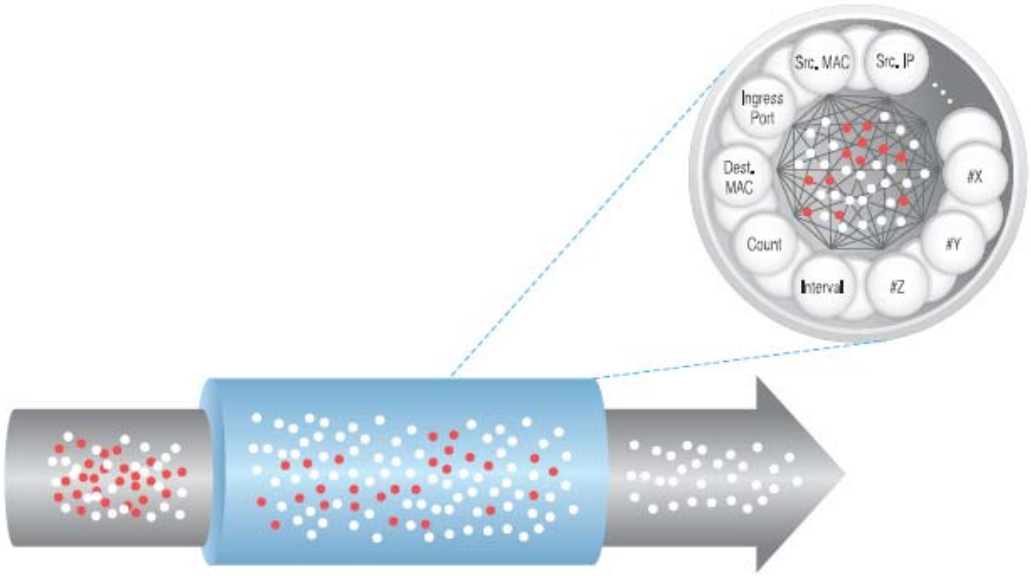
TiMatrixセキュリティエンジンの基本的な動作方式は次の通りである。

1. L2スイッチレイヤでリアルタイムのパケット収集及び分類機能 (Gathering & Classification)
2. 収集したパケットの相関関係の分析によるサイバー攻撃の分析機能 (Security Threat Analyzing)
3. 分析された結果によりサイバー攻撃と判断した場合はセキュリティポリシーを生成 (Security Policing)
4. L2スイッチレイヤに反映して自動的にサイバー攻撃を遮断又は解除 (Protection or Release)

主な特徴は、ユーザー端末からリアルタイムで有害トラフィックが流入した場合、「パケット収集＆分類 => サイバー攻撃の分析 =>セキュリティポリシーの生成 => サイバー攻撃の遮断、または解除」の一連の過程をワイヤスピードの性能で処理し、管理者またはユーザーの介入無しに自動的に有害トラフィックのみ検知して遮断することである。特に、有害トラフィックの遮断により、ユーザーがネットワークに接続できない場合には、WEBアラート機能を通してユーザーにネットワークから遮断された理由を通知することができる。また、新たなサイバー攻撃の手法が現れた場合でも、新たな攻撃手法に対する TiMatrix セキュリティエンジンを開発して直ちに適用することができ、今後の進化した攻撃に対しても素早い対応ができる強みを持つ。

[TiMatrixセキュリティエンジンの主な機能]

- TCP Syn Flooding、UDP Flooding、ICMP Floodingなどの各種有害トラフィックの自動検知及び遮断、解除
- ARP Spoofingによる情報窃取及びIP電話などでの盗聴の防止
- ゾンビPC又は悪意を持った攻撃者からリモート制御により外部攻撃DoS/DDoS発生元の遮断
- 不正なプロトコルの検知/遮断でネットワークの信頼性を維持



●有害トラフィック　○正常トラフィック

6. TiFRONT-セキュリティスイッチ導入時の検討事項

■ 導入時の検討事項

新規のネットワークを構築する場合、または既存のネットワークを高度化してセキュリティを強化する場合、または標的型サイバー攻撃対策のために多階層セキュリティソリューションを構築する場合などにおいて、アクセスネットワークにおけるセキュリティ対策を検討するならば、TiFRONT-セキュリティスイッチが適切であるだろう。一般的な L2 スイッチ製品と同等の L2 機能と性能を提供しながらも L2/L3/L4 レベルのセキュリティ機能を提供していて、より安全で安定的なネットワークを構築できるだけでなく、様々な監視および統合管理を提供して管理者の負担を軽減することができるからである。

次はTiFRONT-セキュリティスイッチだけでなく、一般的な L2 スイッチ製品を導入する場合でも検討すべき項目を記載したものである。

区分	詳細項目
安定性	電源に対する二重化及び電源の負荷分散による耐久性の向上
	大容量のフラッシュメモリの実装による機器の動作及びセキュリティログの保存
	大容量のスイッチ容量の採用による余裕のあるスイッチ処理の性能
	最新の高性能スイッチングチップセットの採用による様々な機能の拡張可能性
セキュリティ性	セキュリティ機能に対する外部機関の公認検証のための CC 認証
	効果的な有害トラフィック(DoS/DDoS など)の自動検知及び自動遮断
	ハッキング行為(ARP/IP Spoofing など)に対する自動検知及び自動遮断
拡張性	数の多いスイッチの統合管理のためのモニタリング機能
	検知ソリューションとの連動を通して全体のネットワークのセキュリティ性の向上
	ワイヤスピードのセキュリティ処理性能でネットワークの応答性能を保障
	Cisco, 3Com, Alcatel などの他社スイッチと標準的な相互互換性を保障
利便性	管理者のための運用管理の便宜性(フォームウェアのアップグレード、セキュリティポリシーの適用など)
	ユーザーに遮断理由を知らせるWEBアラート機能
	大規模のネットワークにおける運用管理のための統合管理システムの提供
	有害トラフィック発生時、管理者、またはユーザーの介入なしに自動で検知及び遮断、解除
技術サポート	365 日 24 時間のオンサイト保守サービス
	導入・運用管理のための技術サポート

7. 検知ソリューションとの連動機能

■ サイバー攻撃を検知する様々なセキュリティシステムとの連動

TiFRONT-セキュリティスイッチは、独自に遂行できるセキュリティ機能に加えてサイバー攻撃を検知する様々なインフラセキュリティシステムとの連動により多階層のセキュリティソリューションにおけるアクセスネットワークのセキュリティ対策の役割も果たしている。

例えば、McAfee の IPS、または FireEye のMPSなどの悪性コードを検知または分析するシステムは、外部ネットワークと内部ネットワークの境界に設置され、通過する全てのパケットをキャップチャし悪性コードかどうかを分析している。ところが、分析が行われる時間が数秒～数分掛かるが、検知してからリアルタイムでセキュリティポリシーに反映して適用することができないのが現状である。現状としては、検知または分析された結果を持って管理者がそのユーザー端末を探してネットワークから遮断することは非常に工数が掛かることである。

このような状況でTiFRONT-セキュリティスイッチは非常に効果的な対応ができるセキュリティ機能を提供する。
McAfee の IPS は悪性コードに感染したユーザー端末を検知した場合、直ちにユーザー端末の IP アドレス、ポート番号、危険度レベル、検知理由等の情報を TiManager へ転送し、TiManager は予め登録してある遮断ポリシーをTiFRONT-セキュリティスイッチに転送する。TiFRONT-セキュリティスイッチはその遮断ポリシーに従ってユーザー端末をネットワークから隔離することになる。結果的に、悪性コードに感染されたユーザー端末はネットワークを使用することはできず、WEB アクセス時にTiFRONT-セキュリティスイッチより WEB アラートを受け取ることによって、遮断された理由を知ることになるので、管理者の負荷を軽減することができる。

[検知するセキュリティシステムとTiFRONT-セキュリティスイッチ連動機能の概要]

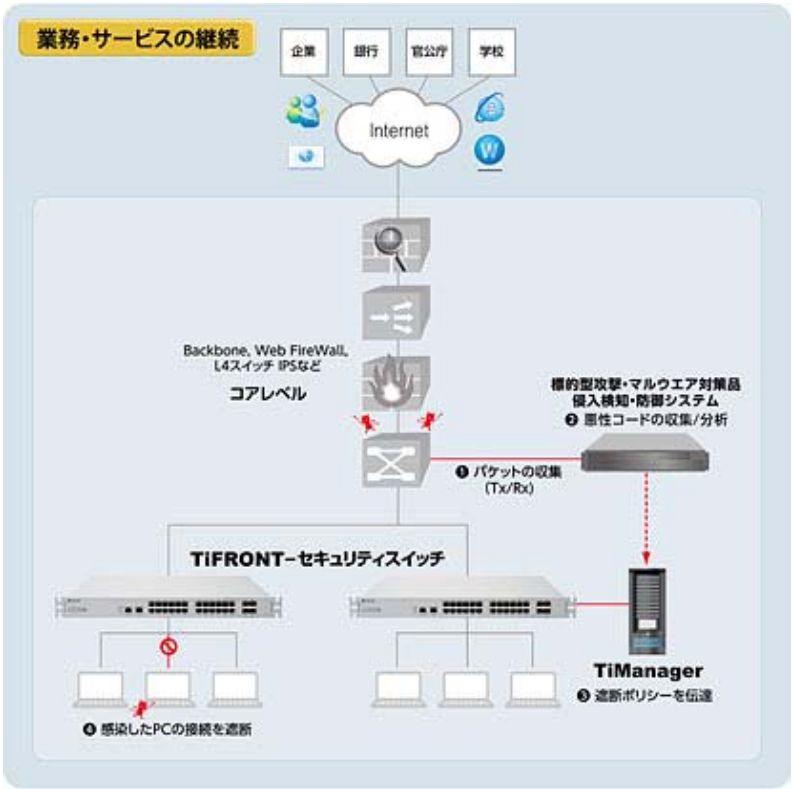
[連動機能による処理フロー]

① コアネットワークよりパケットの収集

② 悪性コードの収集/分析

③ TiManagerにより遮断ポリシーの伝達

④ TiFRONTーセキュリティスイッチにより遮断



TiFRONT-セキュリティスイッチと連動が可能な外部セキュリティソリューションは悪性コートの検知ソリューション、ネットワークアクセス制御（NAC）システムなどがあり、連動可能なセキュリティソリューションの種類と範囲は引き続き増やしていく計画である。

動作確認を実施した連動可能なセキュリティシステムとしては、TiFRONT-AntiBot、McAfee の IPS、FireEye の MPS、Fortigate 等がある。

8. 終わりに

■ 企業の業務継続性及び内部ネットワーク信頼性の確保

公共機関、大学、企業等の各組織は、サイバー攻撃の対策として主にコアネットワークにおいて様々なインフラセキュリティシステムの構築に多額の投資をしている。勿論、企業の業務継続性や対外サービスの信頼性を確保するためには、コアネットワークにおけるセキュリティシステムの整備は必須である。ところが、昨今のサイバー攻撃の巧妙化、高度化により、今はコアネットワークだけでなく、アクセスネットワークにおいても、セキュリティソリューションを備えなければならない必要が徐々に増大している。何回も前述した標的型サイバー攻撃（APT 攻撃）は、コアネットワークのセキュリティシステムを迂回する、または無力化させるために、アクセスネットワーク段に悪性コードを流布する形で進化しているからである。

特に最近のサイバー攻撃は、単に組織の主なサービスを麻痺させるレベルを超えて、重要情報の窃取や削除、そして業務の混乱を加重させるなど組織の存続そのものを脅かすような状況に至っている。

TiFRONT-セキュリティスイッチは、アクセスネットワークにおいて様々な有害トラフィックとスプーフィングのタイプのハッキング行為を自動検知して遮断する。そして、強固なユーザー認証機能により不正なユーザーのネットワークアクセスを根本的に遮断し、より安全なアクセスネットワーク環境を保持する。さらにコアネットワークで運用されている様々なセキュリティシステムと連動してユーザー端末のネットワーク接続を直接コントロールすることができ、非常に効果的且つ強力な多階層セキュリティソリューションとして役割を果たしている。

本文書の結論としては、企業の業務継続性と内部ネットワークの信頼性確保のためには、コアネットワークセキュリティソリューションの効果的な運用だけでなく、アクセスネットワークセキュリティソリューションと連携し、様々なセキュリティポリシーを適用することにより、標的型サイバー攻撃の攻撃者が組織の重要情報を窃取したり、ユーザーPC をゾンビ PC 化して悪用することなどを防ぐことができることである。