PIOLINK

サイバー攻撃の対策に**セキュリティスイッチ**と**アンチボット**が結合した

TiFRONT

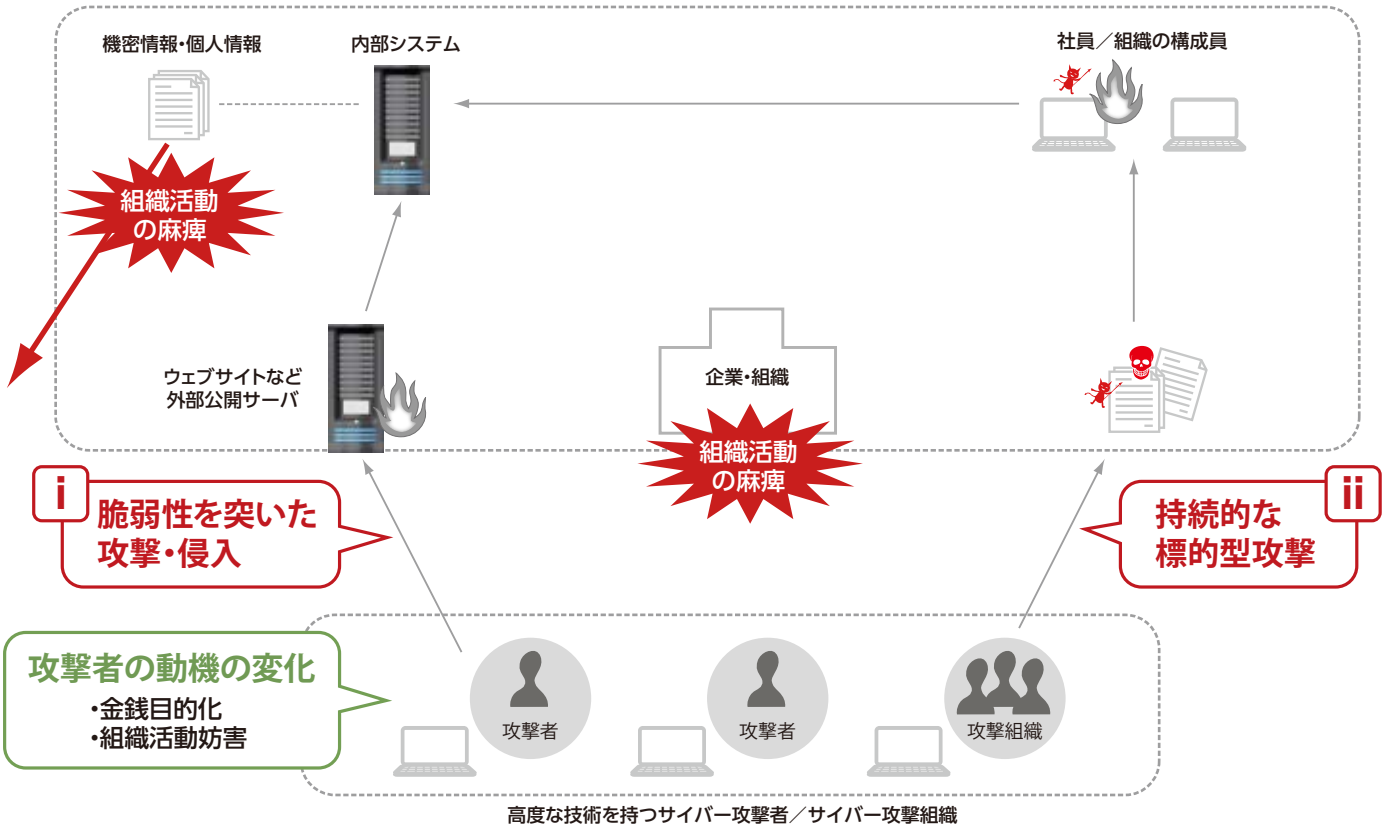
アクセスネットワークのセキュリティソリューション

www.piolink.co.jp

多発するサイバー攻撃の特徴

最近、ソニー、任天堂、Googleなどの大企業、IMF（国際通貨基金）やCIA（米中央情報局）といった公的機関や各国の政府関連機関など、様々な組織がサイバー攻撃の被害に遭っています。経済産業省が実施したアンケート調査※1によると、サイバー攻撃の一種である「標的型攻撃」を受けた経験のある企業は、2007年には5.4%でしたが、2011年には33%と急増しました。被害が表面化していないものも含めると、インターネットを利用している多数の組織がサイバー攻撃の標的になっていると考えられます。

※1　前述「最近の動向を踏まえた情報セキュリティ対策の提示と徹底」（経済産業省）より
企業・組織をとりまく近年のサイバー攻撃では、攻撃者の動機の変化と、攻撃に使われる手口の巧妙化が特徴的です。



TiFRONTで解決できます。

アクセス ネットワーク セキュリティ ソリューション

TiFRONT ソリューションは、悪性コードの検知から遮断まで、
全てをネットワーク上で処理し、簡単な構成で企業機密及び個人情報の漏洩及び
DDoS 発生の被害を防ぐことができます。
パソコン毎に別途のエージェントを設置する面倒な設定もありません。

TiFRONT−アンチボット

サイバー攻撃の検知

＋

TiFRONT−セキュリティスイッチ

サイバー攻撃の遮断

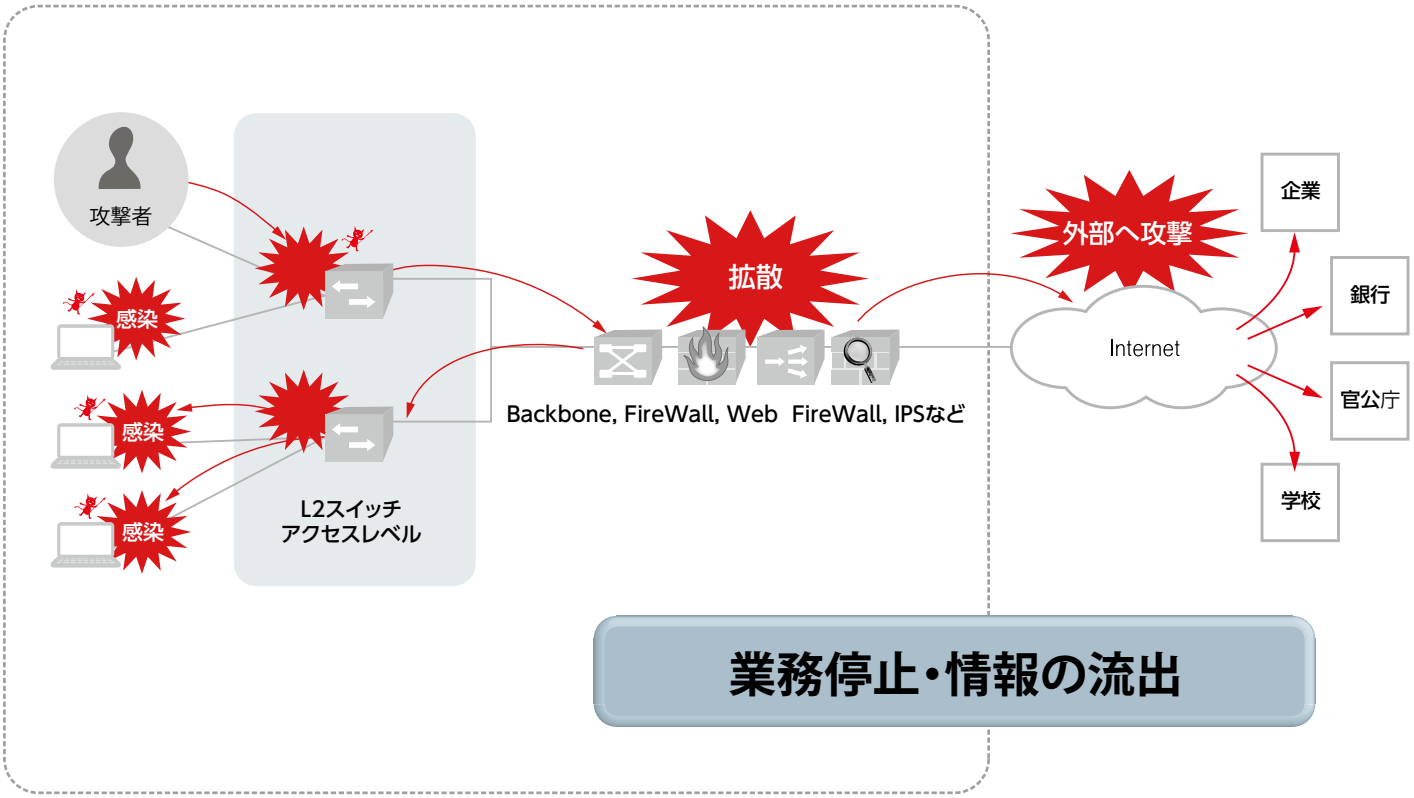
＝

サイバー攻撃対策ソリューション
安全なネットワーク構築

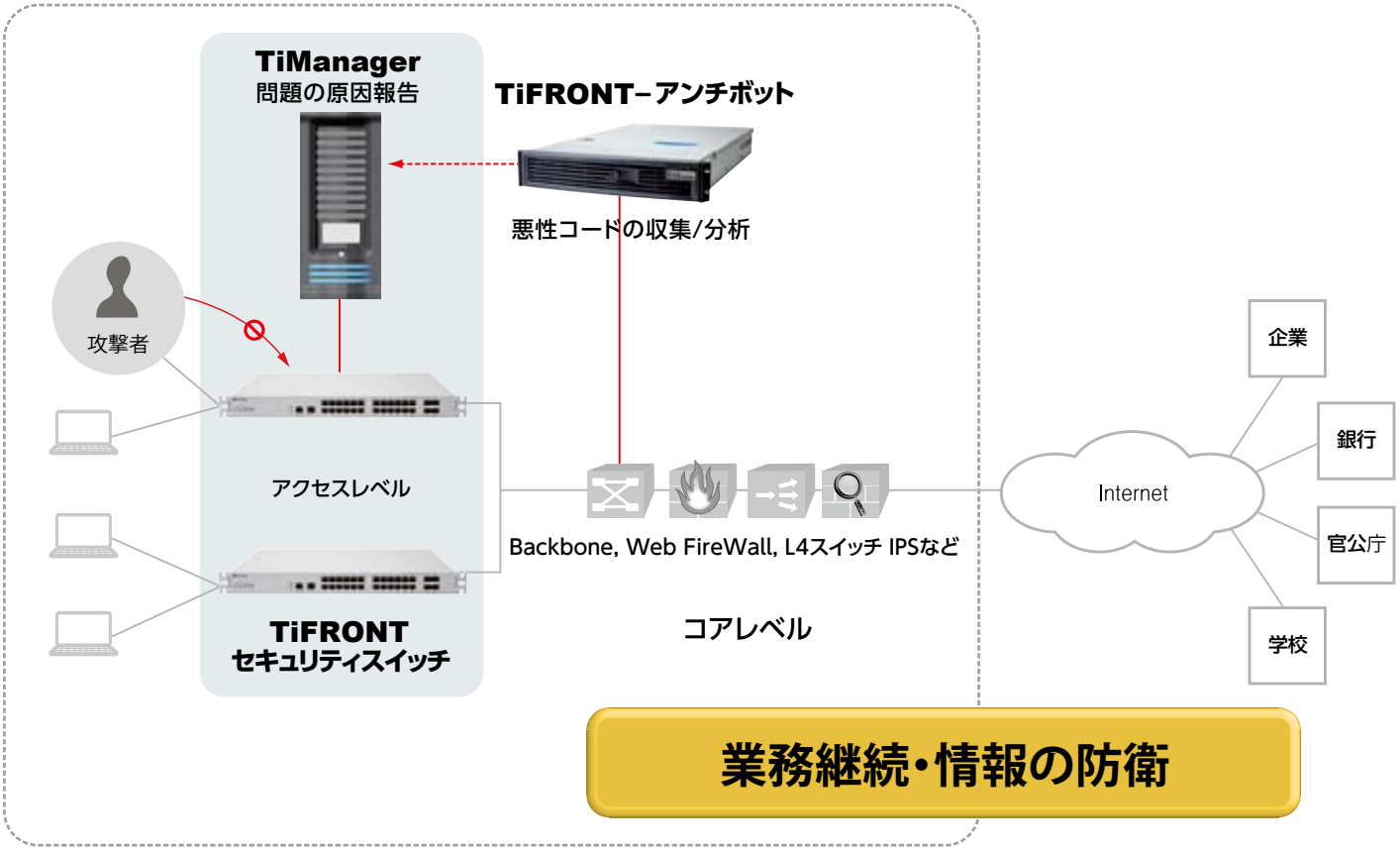
多発性サイバー攻撃

ワーム・ボットによるDoS/DDoS攻撃の封鎖

■一般的なネットワークの構成:アクセスレベルのセキュリティが脆弱



■TiFRONT導入した構成:アクセスレベルのセキュリティを確保



サイバー攻撃を検知する
TiFRONT−アンチボット

TiFRONT-アンチボットは大容量のネットワークにおいても多量の悪性コードを素早く正確に検知･分析します。
多数の仮想マシンを活用する高性能なカーネルベースの振舞い分析によりまだ発見されていない新種のボットに対する検知及び対応を可能にします。システム仮想化により導入及び運用コストを抑えることができます。
なお、TiFRONTとの連動によりエージェント無しで感染したPCをネットワークから遮断することができます。

スマートな分析

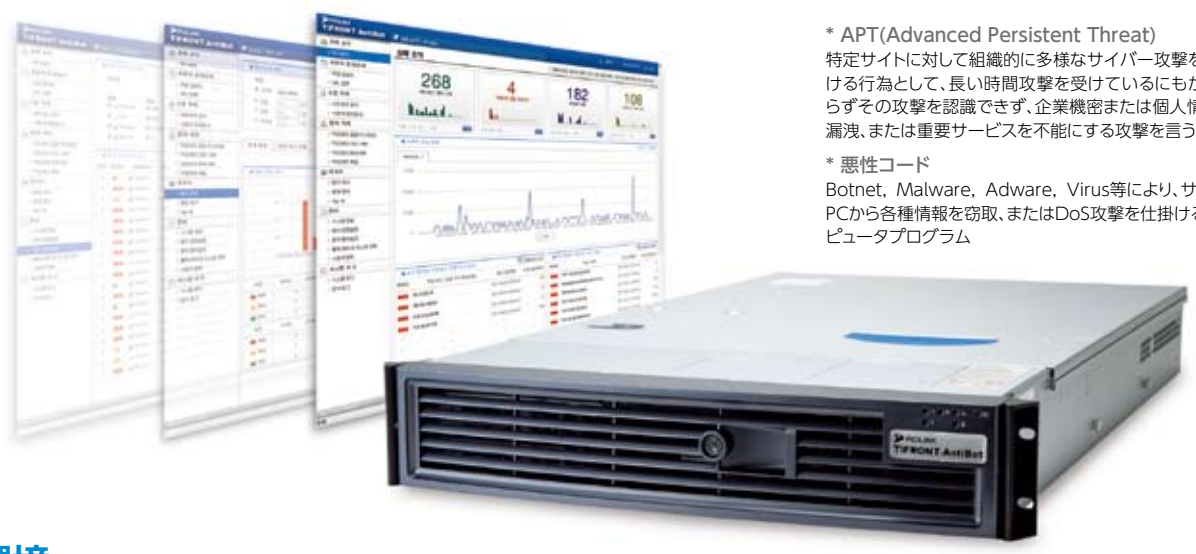
- 悪性コードの振舞い基盤の脅威分析
- 高性能なカーネルベースの正確な分析
- 隠匿化及び仮想環境回避攻撃の対応
- 標的型攻撃(APT)の対応

パワフルなラインアップ

- 1-10Gbps処理性能のラインアップ
- 最大12,000/日個の悪性コード分析
- 最大20個の仮想マシンを同時分析

エージェント設置不要な簡単制御

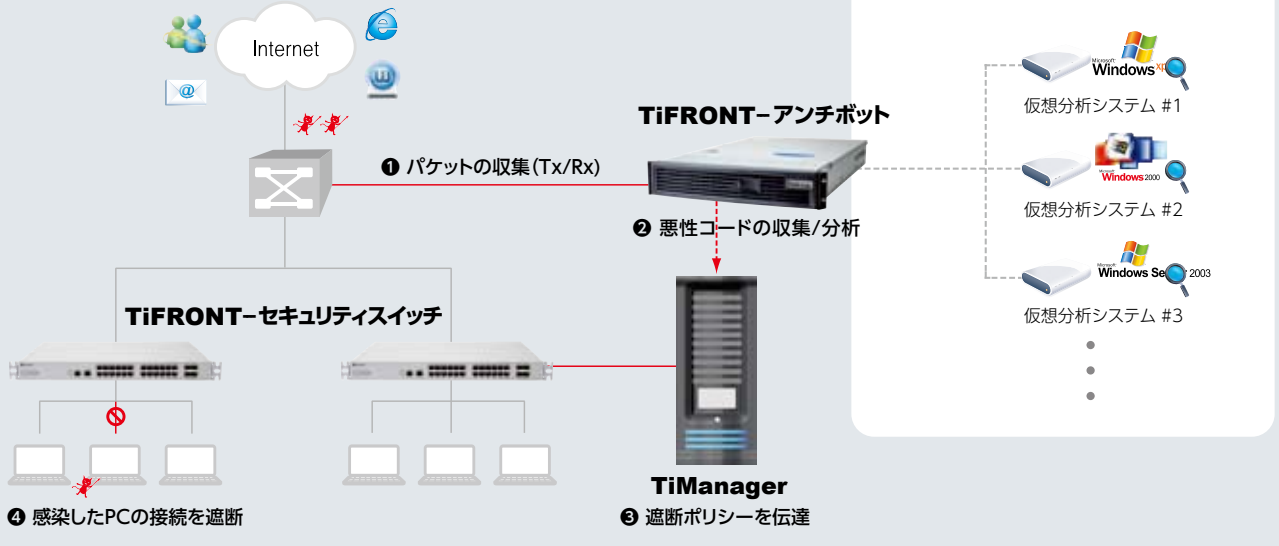
- TiFRONT-セキュリティスイッチと連動してPCにエージェント無しで悪性コード及び有害トラフィックを遮断
- 多数のTiFRONT-セキュリティスイッチを同時に遮断制御



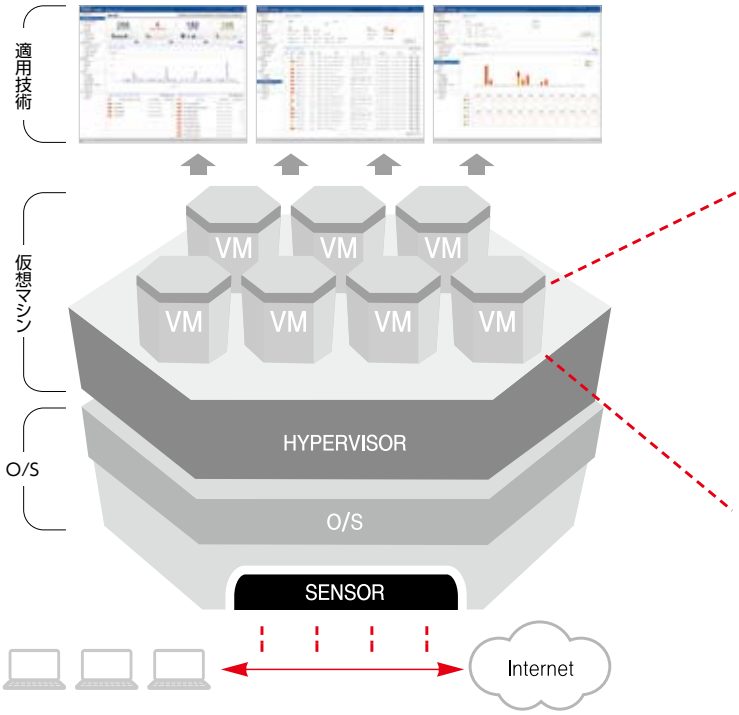
* APT(Advanced Persistent Threat)
特定サイトに対して組織的に多様なサイバー攻撃を仕掛ける行為として、長い時間攻撃を受けているにもかかわらずその攻撃を認識できず、企業機密または個人情報の漏洩、または重要サービスを不能にする攻撃を言う。

* 悪性コード
Botnet, Malware, Adware, Virus等により、サーバ･PCから各種情報を窃取、またはDoS攻撃を仕掛けるコンピュータプログラム

運用環境



適用技術



分析対象	悪性振舞いの分析基準
Process	プロセスの生成/終了、子プロセスの追跡、悪性コード感染の検知
File	システムファイルの生成・削除・変造行為の検知
Registry	システムセキュリティ設定の変更、悪性コード実行の検知、レジストリ変造の検知
Network	C&Cサーバへの接続、ブラックリストのIP/URLへの接続、配布サーバへの接続、悪性コードのダウンロード検知

TiFRONT-アンチボット製品スペック

モデル	TiFRONT-AntiBot2000	TiFRONT-AntiBot4000	TiFRONT-AntiBot8000
CPU	Intel Xeon 2.4 Quad x 1	Intel Xeon 2.4 Quad x 2	Intel Xeon 2.4 Quad x 2
RAM	16G	32G	64G
HDD	1TB	1TB	1TB
SSD	80G	240G	500G
InterFace	1G x 2port	10G x 1port, 1G x 1port	10G x 1port, 1G x 1port
OS	Windows 2008 server R2 Std 64bit		Windows 2008 server R2 Ent 64bit
DB	MS SQL server 2008 R2		
AntiBot S/W	TiFRONT-AntiBot 2.0		

* VM用のクライアントライセンス含む

TiFRONT-アンチボット主要機能

悪性コード検査	仮想マシンの振舞い分析基盤の悪性コードの収集及び自動検査
統合ダッシュボード	検査対象ファイルの収集現況、悪性コード数、感染PC,C&Cサーバ等のリアルタイムの情報提供 トラフィック流入現況及び分析結果の一覧照会
ユーザ定義検査	ユーザファイルのアップロード検査、URL入力検査
多様な統計及びレポート	検知推移の分析及び統計(期間別・発生回数別・危険度別の分析) 悪性コード配布国家別、ポート、C&Cサーバ、拡張子別の統計分析(年・月・日基準の分析) 分析結果の詳細情報提供及び悪性コードのダウンロード状況
システム管理	システムログ、システム監査 分析の振舞い・範囲・種類・対象に対するユーザ設定機能 ブラック・ホワイトリスト管理、詳細分析の照会、検索及びファイル保存

サイバー攻撃を遮断する
TiFRONT-セキュリティスイッチ

日々増加し続けるセキュリティの脅威に安全に対応するためには、外部からの攻撃のみならず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を同時に講ずる必要があります。このために一番効率的なソリューションとして、L2スイッチング機能とセキュリティ機能を同時に対策する必要があります。TiFRONT-セキュリティスイッチはアクセスネットワークのセキュリティ課題に有効な手段で適切に対応できます。

ARP spoofing 防止

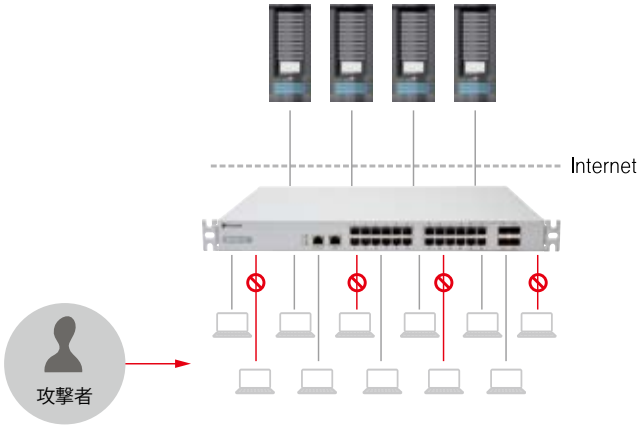
アカウント情報の窃取、通話盗聴から守る安全なネットワーク

ポート単位で細密に判断するために攻撃者と変造されたMAC被害者を区別して、攻撃者の通信のみ遮断します。
TiFRONT-セキュリティスイッチでUC環境における通話盗聴、私生活情報の漏洩及び情報窃取などの脅威から安全なネットワークを構成することができます。

DoS/DDoS 攻撃を発生元で遮断

トラフィック過負荷による速度低下、サービス不能を防御

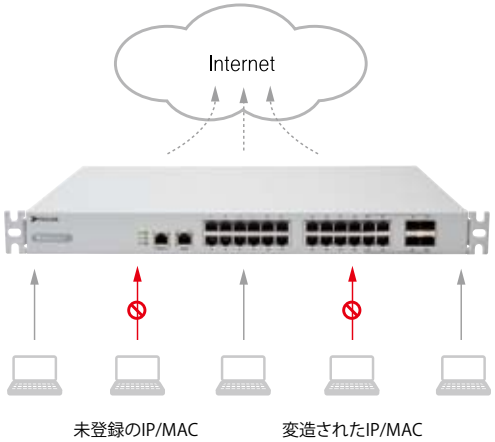
TCP SYN flooding、UDP floooding、ARP floodingなどアクセスネットワークを通過する各種DoSトラフィックからネットワークリソースを安全に保護します。DoSトラフィックをセキュリティスイッチが検知すると自動で攻撃トラフィックのみを遮断するので常に安定したサービス状態を維持することができます。



ユーザ/IP基盤の強力なアクセス制御

非許可の端末からの悪性コード及びウィルス流入の遮断

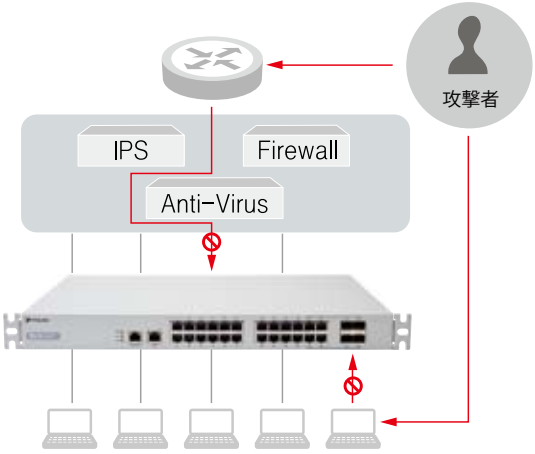
TiFRONT-セキュリティスイッチは、IP/MACアドレス基盤の強力なアクセス制御及びIPリソース管理、端末の接続状態及び履歴を確認することができます。
また、802.1x基盤のユーザ認証、TACACS+、RADIUS等の認証サーバと連動が可能であり、非許可端末のネットワーク接続を制御することができます。



標的型攻撃（APT攻撃）、悪性コードの遮断

各種ハッキング、サイバー攻撃による重要情報窃取を保護

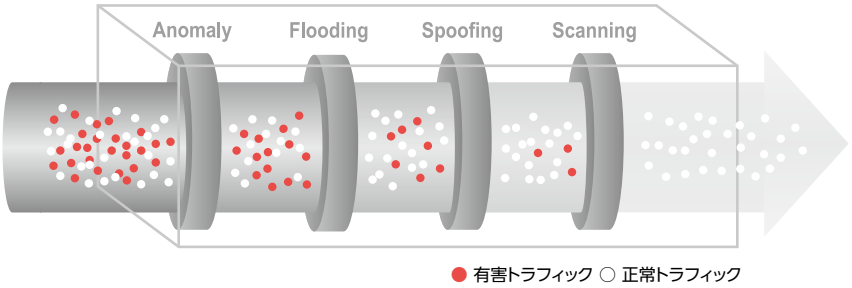
知能型持続攻撃と言われているAPT（Advanced　Persistent Threat）攻撃は特定サイトにサイバー攻撃を持続的に行う行為として、政府機関、銀行、企業を問わずに長時間にわたり攻撃を加えて有効な機密情報を窃取します。TiFRONT-アンチボットと連動する場合、高性能のカーネルベースの振舞い分析手法により、未知の悪性コードの検知率を高めることができます。



スマートセキュリティエンジン：TiMatrix

パケットの正確な危険度予測のために Frequency Matrix モデルを適用したセキュリティエンジン

- スマートエンジンとして有害トラフィックのみ選別し遮断
- 自動セキュリティポリシー On/Off で管理者の手間を最小限に
- Wire Speedのセキュリティ性能を維持
- DoS/DDoS 攻撃発生の検知及び自動対応



● 有害トラフィック ○ 正常トラフィック

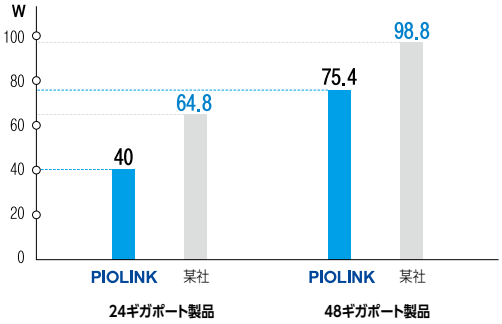
次世代 IEEE 802.3at PoE 標準をサポート

既存のIEEE 802.3af PoEでは動作できないパン/チルト/ズーム機能が可能な高解像度WEBカメラ(CCTV)、高性能無線APなどの最新PoE端末もTiFRONTでは IEEE 802.3at PoE サポートにより動作します。

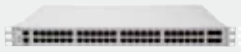
区分	802.3af	802.3at
PoEスイッチの最大出力電力	15.4W	34.2W
PoEスイッチの最大入力電力	12.95W	25.5W
主要接続機器	小型無線AP、小型WEBカメラ IP電話機	大型高性能の有・無線AP、パン/チルト/ズーム機能が可能な高解像度WEBカメラ(CCTV)、IP電話機、小型AP

RoHS指令準拠及び低消費電力

TiFRONT-セキュリティスイッチはRoHS指令を準拠した部品のみを採用して製造しております。
なお、TiFRONT-セキュリティスイッチは他社の同レベルモデルの製品に比べて使用電力を低く押さえた省エネ製品を目指しております。



TiFRONT-セキュリティスイッチ 製品スペック

区分	TiFRONT-F26	TiFRONT-F26P(D)	TiFRONT-G24	TiFRONT-G24P(D)	TiFRONT-G48
					
Performance	•16K MAC address •28.8Gbps Switch capacity •13.09Mpps Forwarding rate		•16K MAC address •72Gbps Switch capacity •71.43Mpps Forwarding rate		•32K MAC address •200Gbps Switch capacity •142.85Mpps Forwarding rate
Memory	• Flash : 160MB (OS 32MB, Log Buffer 128MB) • Main memory : 512MB SDRAM				•Flash : 160MB (OS 32MB, Log Buffer 128MB) •Main memory : 1GB SDRAM
Ethernet port	• 24 x 10/100Base-TX ports • 2 x 1GbE Dual media combo ports (Copper ports : 10/100/1000 BASE-T 2 ports, Fiber ports : 1000BASE-X SFP type 2 ports)		• 24 x 10/100/1000Base-TX ports (4 combo ports included, 1000BASE-X SFP 4ports)		•48 x 10/100/1000Base-TX ports (4 combo ports included, 1000BASE-X SFP 4ports)
AC input	100~240VAC, 50/60Hz (Free Voltage)				
Power over Ethernet	N/A	• IEE802.3at (PoE+)	N/A	• IEE802.3at (PoE+)	N/A
Dual Power	×	○	×	○	×
Power consumption	24.3W	41.1W	40W	42W	75.4W
Dimension	440x350x44 (WxDxH, mm, 19" 1U rack size)				
Weight	4.1Kg	5Kg	4.1Kg	5.25Kg	4.3Kg
EMC Certification	KCC / VCCI (Class A)				

TiFRONT−セキュリティスイッチ 主要機能

L2	
Port Management	Autonego/Speed/duplex
	Flow control
VLAN	Broadcasting Domain
	Port-based VLAN
	Tagging/untagging
	Multiple VLAN
	Hybrid VLAN
	Max. VLAN (4K)
	Ingress/Egress tagging
Spanning Tree	STP, RSTP, MSTP, PvSTP
MAC learning	MAC address aging
	MAC filtering
	Duplicate MAC address learning
	Reserve MAC learning 防止
	Static entry support
	Independent VLAN learing
	Max MAC entry (16K)
Port Mirroring	Port Mirroring
Link Aggregation	LACP
	Link trunking
	LACP load balancing
	Trunk Groups(8)
	Members per group (8)
	Static Trunk load balancing
	障害リンクに対するトラフィック切り離し
IGMP snooping	Join/Leave, Multicast group (1K), v1/v2/v3
QoS	L2, L3, L4 header based classification
	QoS marking & Remaring
	QoS queuing & scheduling - Cos Queue mapping - 8 CoS queues per port - Scheduling by SPQ/WRR/DRR - Drop precedence - Congestion Avoidance
	Ingress rate-limiting (per port/per flow)
	Egress rate-limiting(per port)
	Diffserv
	Shaping & packet drop policy
	MIN/Max BW guarantee
	最大ルール数 (G48:128個 , F26/G24:256個)
ACL	L2/L3/L4 基盤のフィルタリング
	VLAN ACL
	ACL filter naming
	最大ルール数 (G48:256個 , F26/G24:512個)
PoE	PoE+ 標準サポート (802.3at)
	ポート別　イネーブル / ディセーブル
	ポート別の供給電力の優先順位設定
	PoE 動作状況のモニタリング
Jumbo Frame	G48 : 12K, F26/G24 : 13K

その他	
IPv6 対応	Phase Ⅱ 対応
連動	TiFRONT−AntiBot と連動

セキュリティ	
Performance	One-to-One flooding, Random flooding, IP scanning, Port scanning, IP spoofing, ARP spoofing, MAC flooding, counting & logging
	自動検知遮断及び解除
	Source MAC/IP 別遮断
	検知の例外設定
Protocol Anomaly	Land attack, Teardrop attack, L4 source port range 異常 , same port(sPort/dPort), TCP flag 異常 , TCP fragments, ICMP fragments, Smurf, counting
Authentication	802.1x, RADIUS, TACACS+
	IP/MAC 基盤の認証及び遮断
Port Protection	Storm control
	Max. MAC 指定
Accounting	Login/Logout ログ
	コマンド実行ログ
その他	DHCP filtering
	NetBIOS filtering
	Self loop detect
	System Access security

管　理	
SNMP	SNMP v1/v2c/v3
	Public MIB (System, Interface, IP address, UCD, Router(RFC-1213), Protocol(TCP, UDP, SNMP, ICMP), RFC1573 Private Interface MIB),
	Private MIB (Learning MAC table, セキュリティ設定)
	SNMP Trap (Authentication, Port Link up/down)
Shell Interface	Telnet, SSH, Console
EMS Interface	SNMP, Syslog, SSH
Authentication	RADIUS, TACACS+
ユーザ管理	Password Based user login, Login timeout 設定 , Multi user, User 別権限 , Multi-configure, Email アラム
設定及び OS 管理	OS update via TFTP
	設定保存
ログ管理	Syslog server, モニタリング, ログ閾値管理 , ログバックアップ, System/Security/Panic ログ
モニタリング	Port statistics, CPU/Memory usage, Fan, Watchdog, Temperature sensor
システム管理	温度によるファン On/Off

TiManager：統合管理システム

スイッチ＋
ユーザIP
の統合管理

グループ及び個別の
セキュリティポリシー
設定

1,000台以上の
スイッチを
同時に管理

AntiBotとの
連動により
ゾンビPCを遮断

リアルタイムのモニタリング

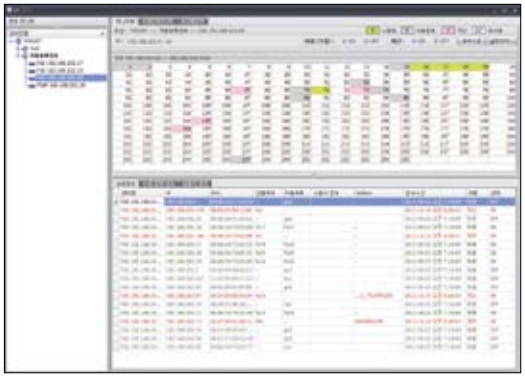
リアルタイムのトラフィック、セキュリティ侵入状態のみならずセキュリティスイッチ、ユーザIP使用現況等を一目で把握できます。セキュリティログ、機器の動作状態ログ、ネットワーク構成状況等をリアルタイムで確認できます。

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ます。ポート別の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、または接続を許可・遮断することができます。

ユーザ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で誰が何時使用したのかリアルタイムで把握することができます。
IP/MACアドレス基盤のユーザ認証により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ます。



多様なリポート

セキュリティスイッチと登録したIPに対するレポートを出力します。数十から数百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、機器状態等のレポートとして出力することができます。

TiManager 推奨サーバスペック

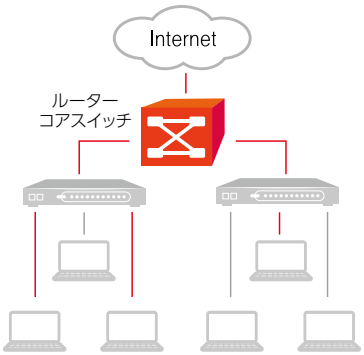
CPU	Intel® Core™ i5 2.X 以上	OS	Windows XP 以上, Windows Sever 2003/2008
RAM	3GB 以上	DBMS	PostgreSQL 9.0.2 以上
HDD	200MB 以上		

導入事例

アクセス
セキュリティ
及び安定性

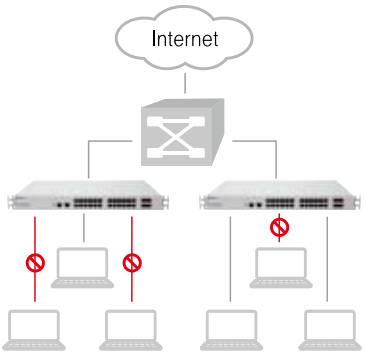
インターネットカフェにおける有害トラフィックの遮断及びネットワークの安定化

不特定多数が使用するインターネットカフェはアクセスネットワークから発生する多様な攻撃に曝されていて障害も頻繁に発生します。TiFRONT-セキュリティスイッチを導入した後は、上位ネットワークへのトラフィックが激減し、上位ルーターのトラフィック過負荷によるCPUロードも下がることにより通信障害も無くなり、DoS/DDoS攻撃、Flooding、Scanning攻撃も遮断されることにより安定したネットワーク環境を維持することができました。



導入前	区　分	導入後
287	DHCP Deny	0
13	Dest MAC Failures	0
540	IP Validation Failures	128
71%	CPU Load	5%

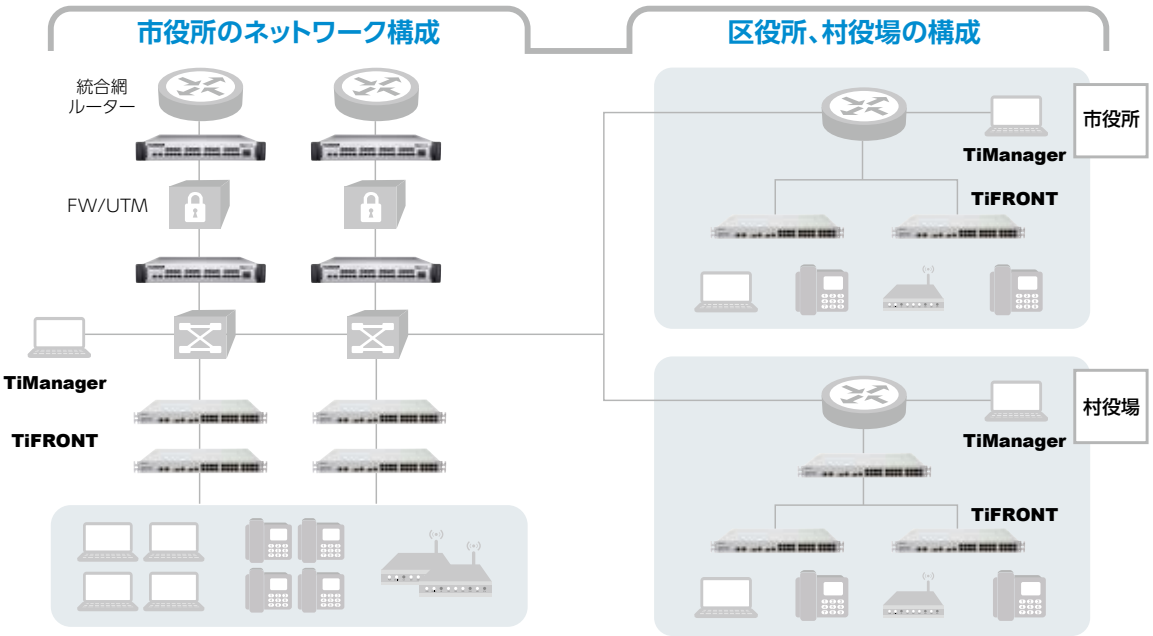
分析期間:2010.10.27 - 11.19



コスト削減及び
管理の容易性

自治体の導入例（市役所、区役所、村役場）

市役所と区役所及び村役場を接続するIPT構築事業でIP電話、有無線APの接続のためにPoE機能搭載のTiFRONT-セキュリティスイッチを導入しました。PoEモデルは別途の電源供装置給無しに電源とデータを同時に伝送可能な機能でありネットワーク配線を簡素化できます。統合セキュリティ管理システムとしてTiManagerを市役所と区役所、村役場へ設置することにより統合管理及び個別のセキュリティ管理が可能になりました。



大規模
ネットワークの
集中管理

各自治体の教育委員会傘下の小中高校及びその他教育機関

小中高校の学生向けのインターネット環境においてセキュリティ対策と各学校におけるセキュリティポリシーの統合管理のためにTiFRONT及びTiManagerを導入しました。1,000台を超えるTiFRONTを管理するTiManagerはセキュリティポリシーの一括適用、または学校毎の個別のセキュリティポリシー設定なども可能になりました。

株式会社 パイオリンク

PIOLINKは、アプリケーションスイッチ、ネットワーキング及び、ウェブセキュリティの専門ベンダーです。
業務継続性、安定性、セキュリティ確保のためにADC（アプリケーション・デリバリ・コントローラ）製品としてPASシリーズ及びPAS-Kシリーズ、WAF（ウェブ・アプリケーション・セキュリティ）製品としてWEBFRONTシリーズ、そしてANS（アクセス・ネットワーク・セキュリティ）製品としてTIFRONT-セキュリティスイッチ及びTiFRONT-アンチボット製品を提供しております。

ADC（アプリケーション・デリバリ・コントローラ）製品
アプリケーション配信の最適化

PAS-K

PAS

WAF（ウェブ・アプリケーション・ファイアーウォール）製品
WEBアプリケーションのセキュリティ確保

WEBFRONT

ANS（アクセス・ネットワーク・セキュリティ）製品
サイバー攻撃の防御

TiFRONT-セキュリティスイッチ

TiFRONT-アンチボット

開発元

株式会社パイオリンク

〒160-0022
東京都新宿区新宿1-34-14 第2貝塚ビル 3F
TEL:03-5367-2547　FAX:03-5367-2546

U R L : http://www.piolink.co.jp
E-mail : sales@piolink.co.jp

販売パートナー