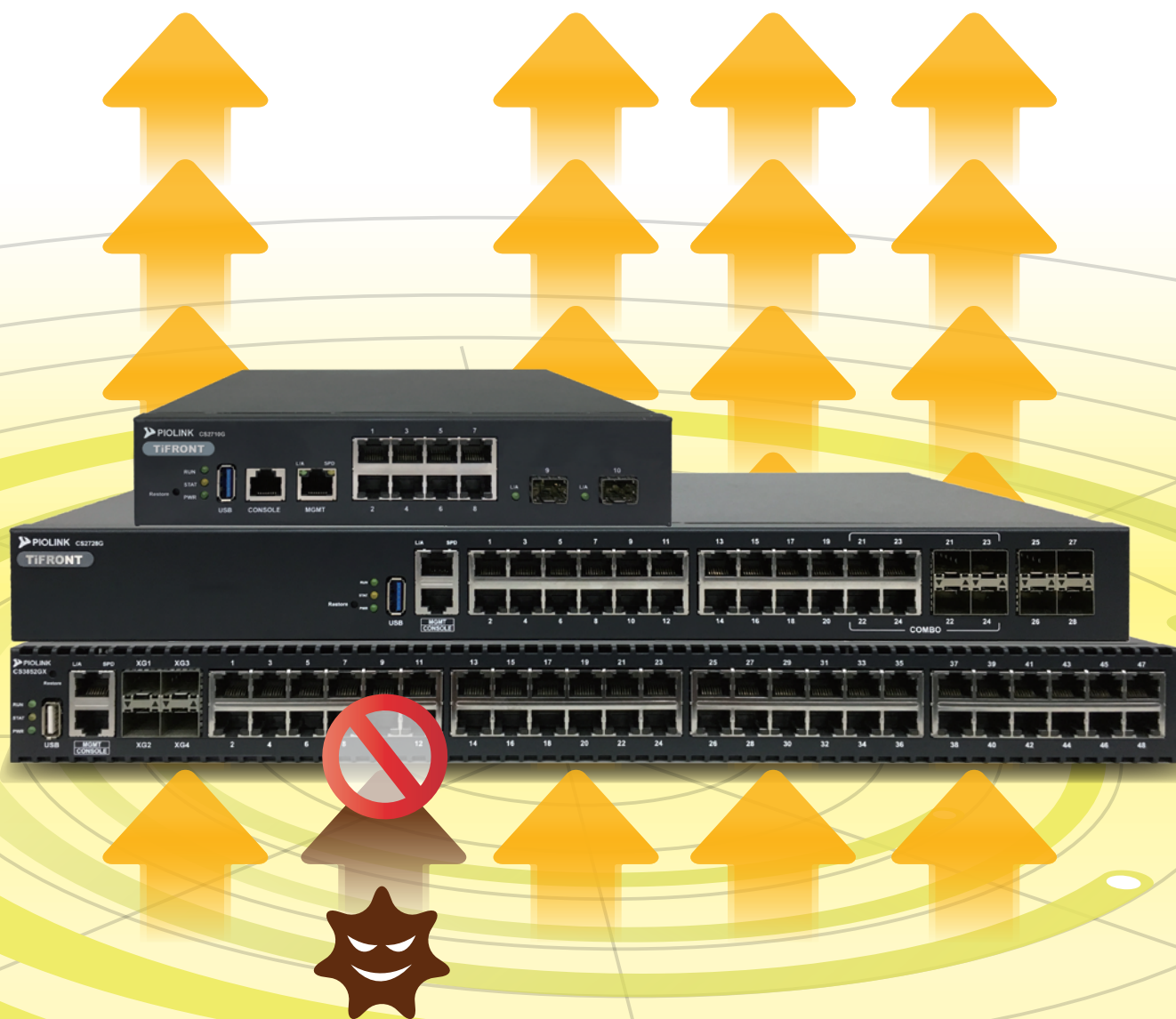


セキュリティスイッチ
TiFRONT
クラウド管理型



不正通信のみを自動ブロック!



対象ポートを
自動遮断
ループ防止!

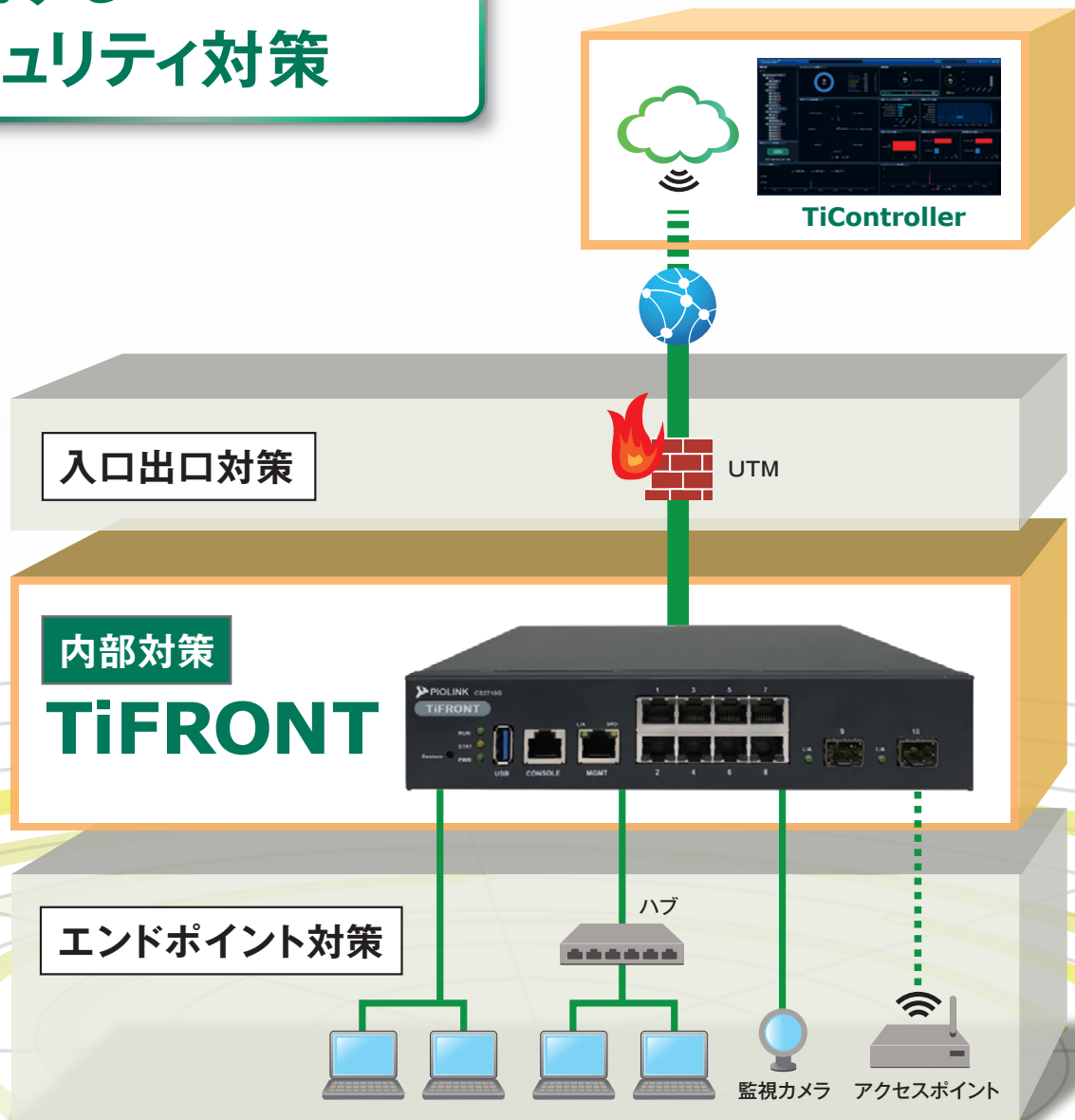
管理・工数不要の
クラウド管理!

L2スイッチベースの
ネットワーク
セキュリティ!

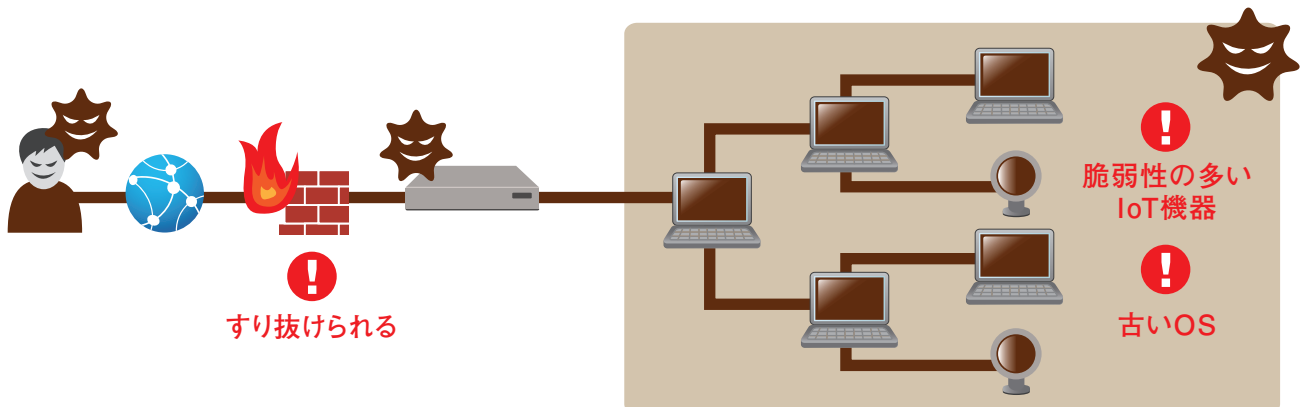
サイバー攻撃を拡散させない 新感覚

ネットワークレベルで 実施する セキュリティ対策

多層防御の構築



シグネチャーベースの限界



侵入を検知して通信を遮断する感染を前提とした対策が必要!!

TiFRONT セキュリティスイッチ 機能

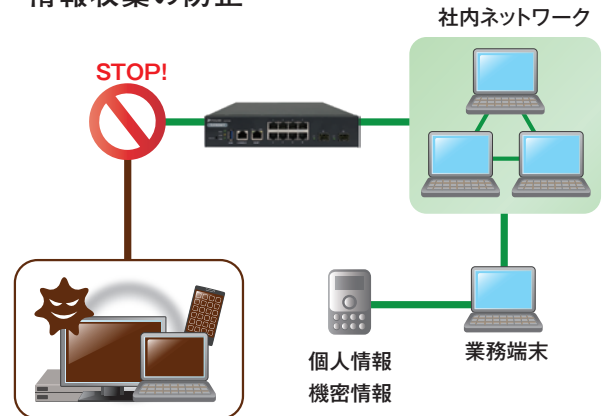
内部拡散防止

ランサムウェアが拡散で使用する
SMB通信を検知・遮断



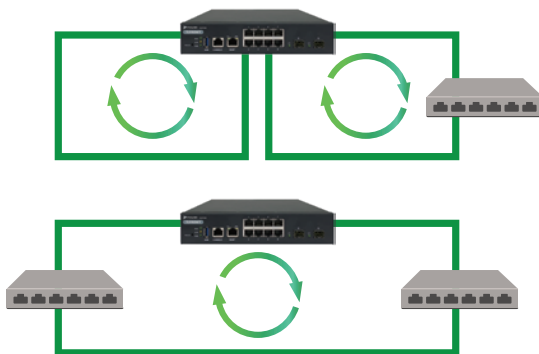
内部不正通信の遮断

情報収集の防止



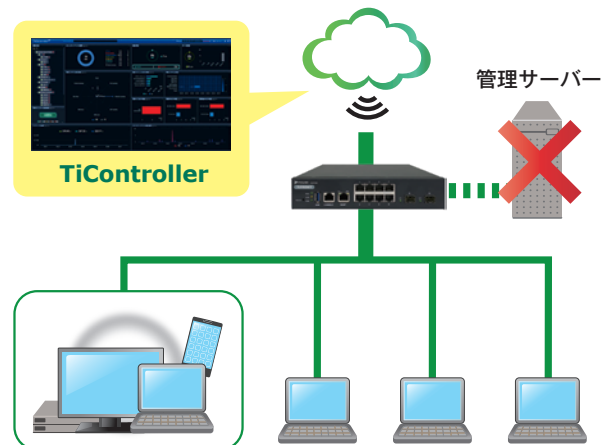
ループの防止

セルフループ防止機能で
ネットワークダウンを防止



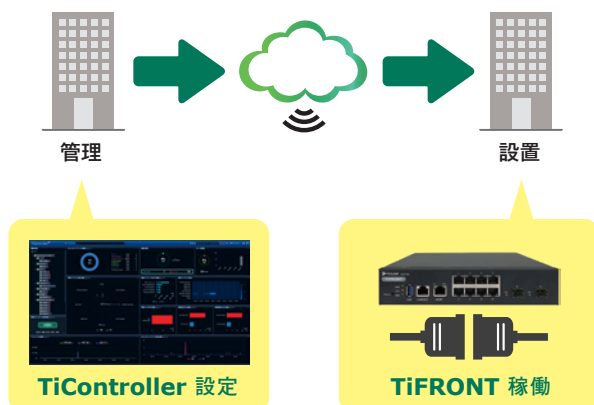
管理サーバー不要

場所を選ばず設置が可能



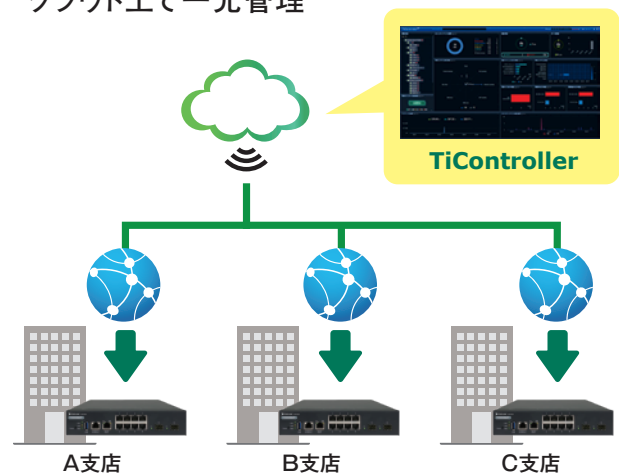
機器設定

ゼロタッチ インストレーション
ケーブル接続で設定完了

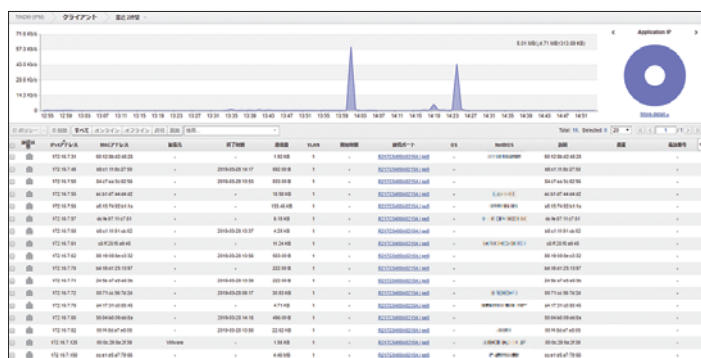


一元管理

インターネット環境があれば
クラウド上で一元管理



自動生成の セキュリティ レポート



レポートスケジュールの管理

レポートタイプ: 統合レポート

作成期間: 1番のみ

レポート表:

日付	時間	単位

検索: 1件

言語: 日本語

実行時期: 2019-03-28 15:03

検索範囲: 2019-03-28 14:03 ~ 2019-03-28 15:03

フィルターの選択: 優先度 [Controller] レポート

メールアドレス: (1列に1つずつ入力)

追加 キャンセル

セキユリティレポート

期間：2018-03-08 00:00 ~ 2018-03-09 00:00 作成対象：piolink_東京

攻撃者の検出状況

検出項目	件数	アイコン	説明	件数
フッディング	10 件	🔍	ポートスキャン	2 件
ネットワークスキャン	3 件	🌐	ARP スプーフィング	3 件
SMB 通信	2 件	💻	MAC フラッシング	3 件
プロトコルアナライザ	8 件	🕒	ランダムウェア探索(SMB-scan)	3 件

攻撃毎の分布

攻撃種別	割合 (%)
フラッシング	23.8%
ネットワークスキャン	23.8%
SMB 通信	16.8%
プロトコルアナライザ	16.8%
ポートスキャン	9.9%
ARP スプーフィング	9.9%
MAC フラッシング	9.9%
ランダムウェア探索	9.9%

発生件数

時間区間	発生件数
0-3	0
3-6	0
6-9	0
9-12	7
12-15	18
15-18	10
18-21	0
21-24	0

攻撃者IP TOP-5

No.	IP	MAC	発生件数	組織	ネットワーク	スイッチ名	ポート名
1	172.20.10.3	d0:0e:a1:5d:06:d9	3	PIOLINK	東京	R217C5400A02154	ge7
2	192.168.1.101		3	PIOLINK	東京	R217C5400A02154	ge7
3		d0:0e:a1:5d:06:d9	2	PIOLINK	東京	R217C5400A02154	ge7
4	172.16.7.130		2	PIOLINK	東京	R217C5400A02154	ge4
5	172.16.7.130		2	PIOLINK	東京	R217C5400A02154	ge5

攻撃対象機器 TOP-5

No.	スイッチ名	発生件数	組織	ネットワーク
1	R217C5400A02154	34	PIOLINK	東京

スイッチの自動アップデート	on ▼
アップデートチェック	日曜日 ▼ / 01:00 ▼
ファームウェアのアップデート実行日時	2018-04-07 02:00 ▼

株式会社バイオリンク

〒160-0022
東京都新宿区新宿5-8-8 カールツァイス新宿別館3F
TEL: 03-5363-9100 FAX: 03-5363-9101
URL: <http://www.piolink.co.jp/>
E-mail: sales@piolink.co.jp

販売パートナー