The Guaranteed Network
いちばん近くで、もっと先へ。

ネットワーク可視化技術とその応用

THE
GUARANTEED
NETWORK

AlaxalA
A FORTINET Company

2025年2月28日

アラクサラネットワークス株式会社

© ALAXALA Networks Corporation 2025 All rights reserved.

会社概要

アラクサラネットワークスは、2004年にNECと日立製作所との合弁会社として発足
2021年からFortinetグループとなり、ネットワークとセキュリティの融合をめざしています

◆ 会社名	アラクサラネットワークス株式会社（ALAXALA Networks Corporation）	
◆ 設立	2004年10月1日	2024年10月に20周年を迎えました
◆ 資本金	20億円	
◆ 株主	米国Fortinet, Inc.　(NASDAQ)	
◆ 本社	神奈川県川崎市　新川崎ツインタワー西棟	
◆ 西日本	大阪市淀川区　新大阪フロントビル	
◆ 名古屋	名古屋市中村区　広小路ガーデンアベニュー	
◆ 事業内容	ルータ・スイッチ等ネットワーク機器の 開発・製造・販売・保守	
◆ 社員数	219名	（2024年12月 現在）
◆ 売上高	142億円	（2024年１月～12月）

営業
SE
マーケティング
設計/開発
品質保証
TAC

営業
SE

営業
SE


新川崎(本社)


大阪オフィス


名古屋オフィス

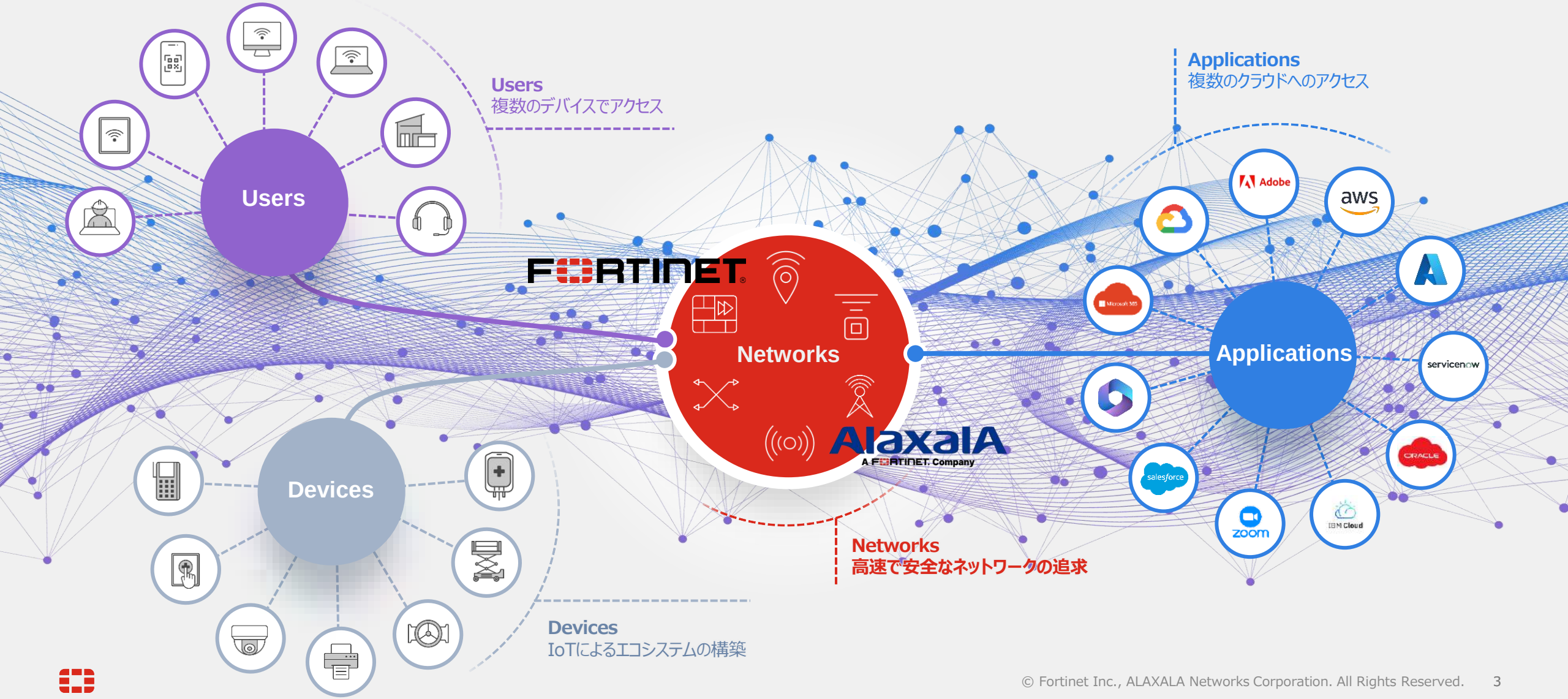
アラクサラネットワークス、
その「ふたつの翼」について

「アラクサラ」の「ALA」はラテン語で「翼」を意味します。
ふたつの「翼」を「X（eXchange）」で結んだ社名には、「ネットワーク」の基幹を支える製品の提供を通じて、お客さまとともに、未来へ飛翔するという思いが込められています。
世界をつなぐライフラインである「ネットワーク」を、より快適で安心して使えるものにするために、アラクサラは今日も、新たな製品の開発と技術への挑戦を続けています。

© Fortinet Inc., ALAXALA Networks Corporation. All Rights Reserved.

ライフラインとしてのネットワーク

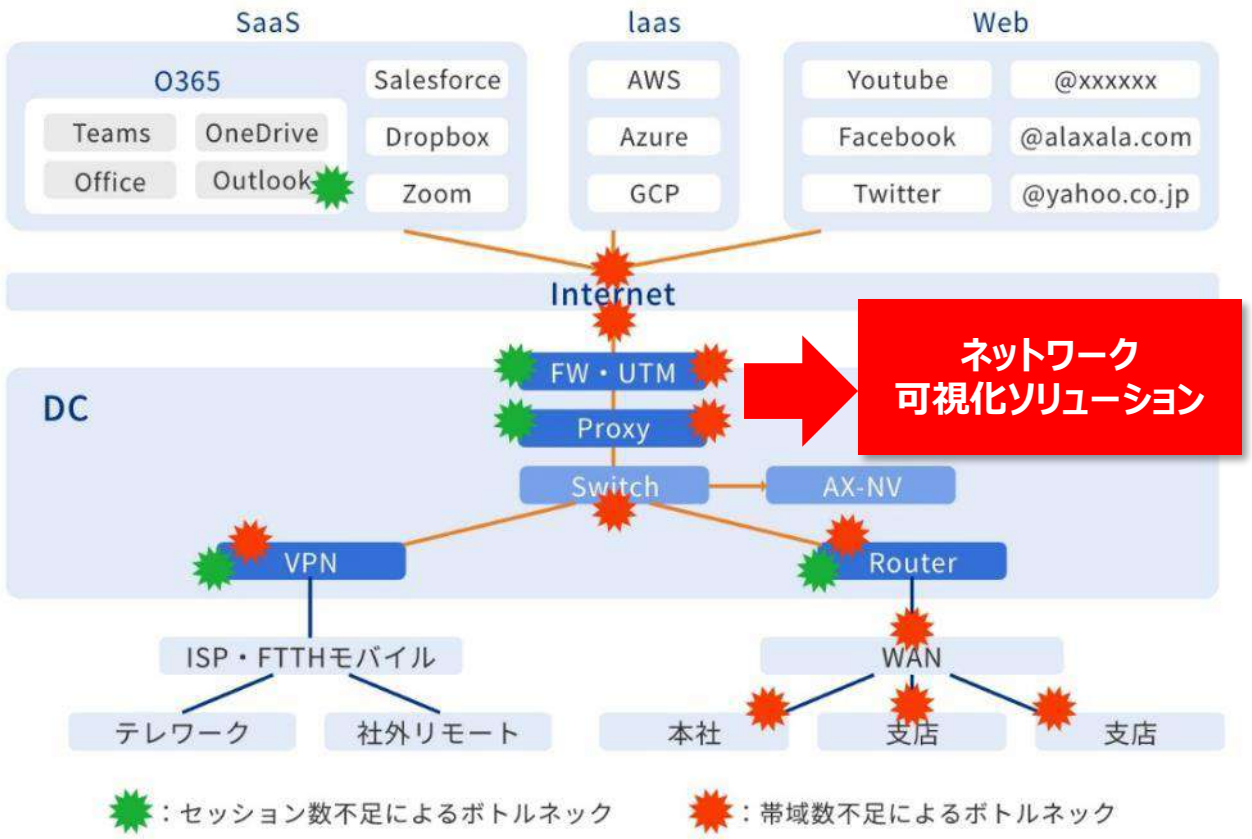
ネットワークは、今後、より重要なポジションとなり、安定と進化の追求が必要



© Fortinet Inc., ALAXALA Networks Corporation. All Rights Reserved.

ネットワークの問題を解消するためには

ネットワーク可視化ソリューションにより問題箇所を明確化



ネットワーク
可視化ソリューション

可視化

・本社/支店/テレワークからWebサービスへの通信を可視化
・通信帯域に加え、通信遅延やTCPの通信品質も可視化
・各種通信におけるヘビートラフィックや通信ランキングを可視化
・TCPのコネクションの成功や失敗の状況を可視化
・SaaSやWebサービスの利用ユーザ状況を可視化

異常検知

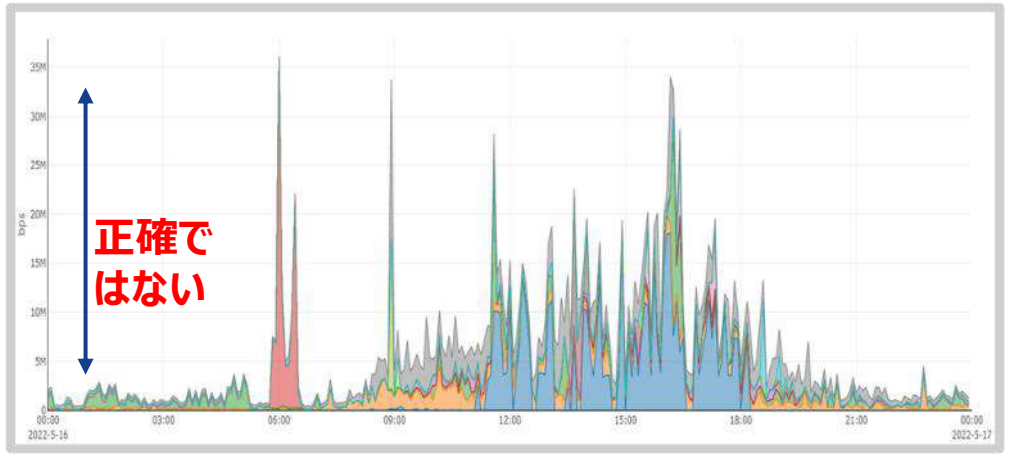
SaaSやWebサービス通信において、拠点毎,部門毎,テレワーク毎,端末毎に通信量・遅延などを監視して異常検知

© ALAXALA Networks Corporation 2025 All rights reserved.

正確なデータ取得ができるか？

データ精度が高くなければ、トラブル時の通信解析には使えない

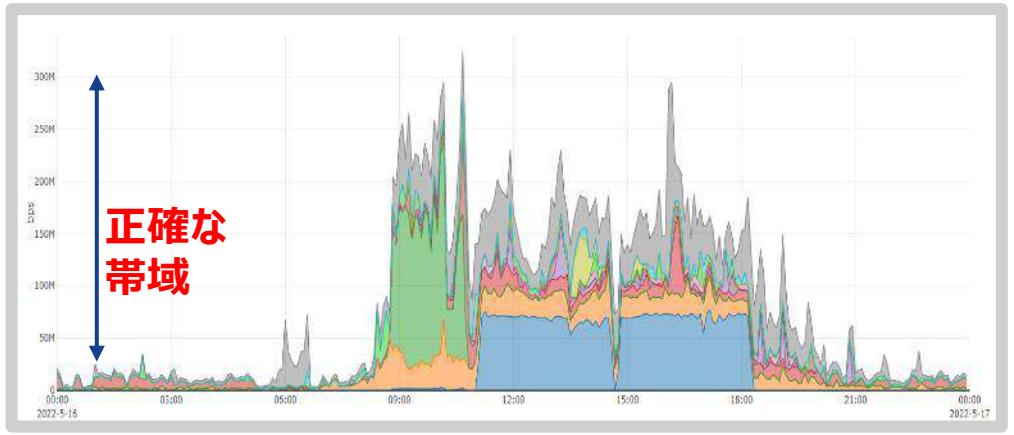
サンプリング方式によるトラフィック可視化



**ざっくりとしたトラフィック傾向を知るために活用、
通信障害の影響や通信ログ解析には使えない**

- 帯域やユーザ数は正確ではない
- 各種ランキングの順位が正確でない

ノンサンプリング方式によるトラフィック可視化



**精度が良いので活用範囲が広く、
通信障害の原因究明やログ解析に活用可能**

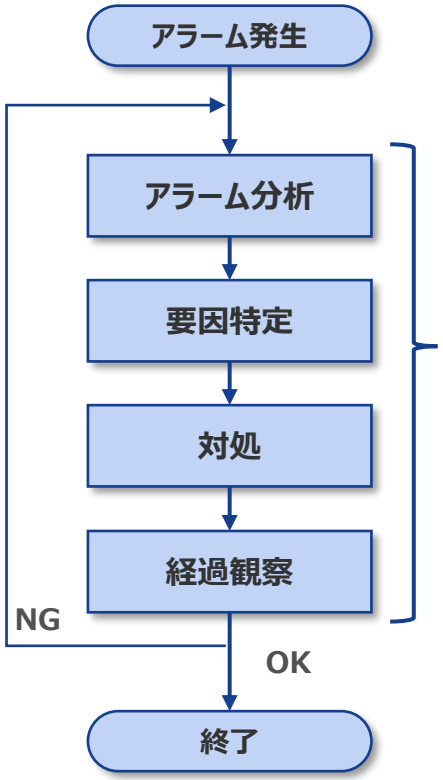
- 正確なトラフィックの傾向を知ることができる
- 帯域やユーザ数,ランキングの順位が正確

© ALAXALA Networks Corporation 2025 All rights reserved.

俯瞰的かつ直感的なデータの表示方法になっているか

障害部位などが一目でわかれば、より迅速・適切・簡単に対応可能

従来の通信障害対応



アラームリスト・ログリスト

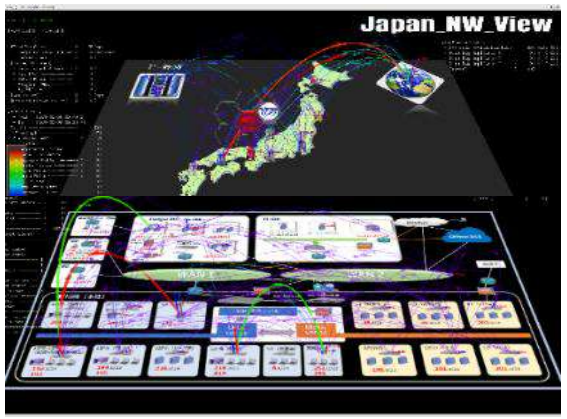
高スキル
運用者

この障害は過去の事例に似ているから、ここが要因だろう。

- 各種ログリストから、経験と勘にもとづいて要因特定・対処・経過観察
- 要因特定に時間がかかったり、影響範囲の把握が難しかったりしていた

俯瞰的・直観的な通信障害対応

3D可視化



俯瞰画面※

	WAN回線	Proxy サーバ	DNS サーバ	File サーバ
東京本社	✓	✓	✓	✓
大阪支店	✓	✓	✓	✓
名古屋支店	✓	✓	✓	✓
テレワーク	✓	✓	✓	✓

	OneDrive	Office Online	Exchange Online	Microsoft Teams
東京本社	✓	✓	✓	↓
大阪支店	✓	✓	✓	↓
名古屋支店	✓	✓	✓	↓
テレワーク	✓	✓	✓	↓

一般的な
運用者

なるほど、全拠点のTeamsのみが停止しているな。

- ３D可視化によりトラフィックや障害発生位置を一目で把握
- 俯瞰画面により障害部位と影響範囲を一目で把握
- 要因特定時間の短縮・影響範囲の容易な把握

※俯瞰画面：ロケーションやサービスなどの状態をマトリクス表示したもの

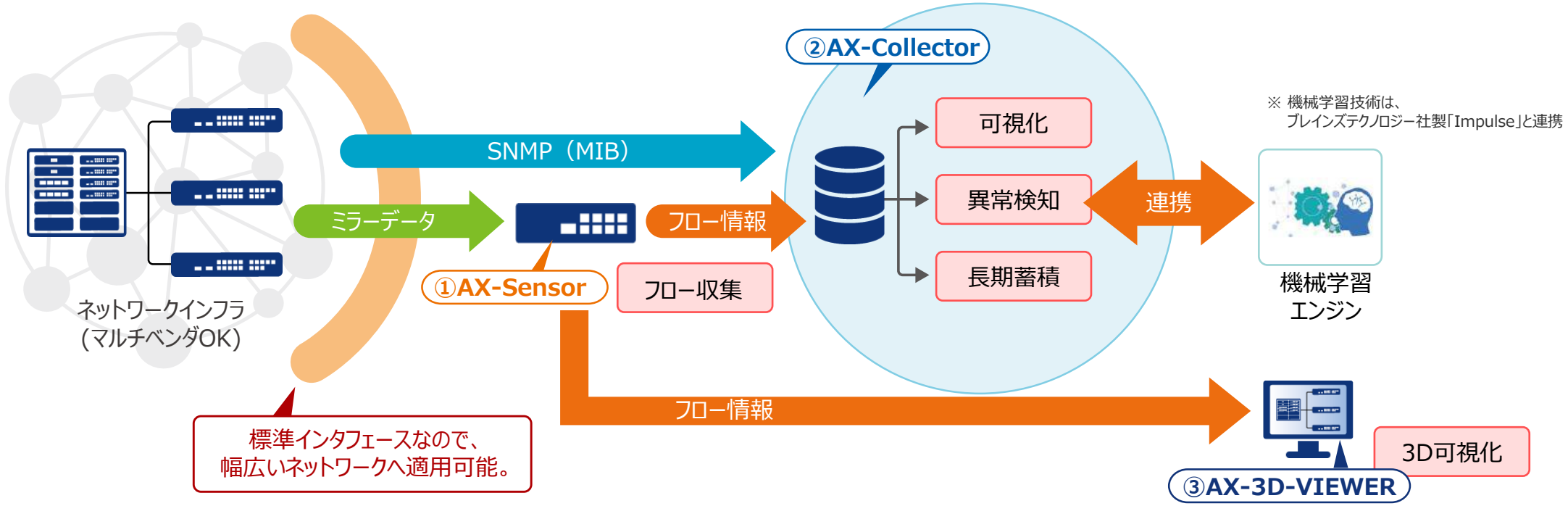
© ALAXALA Networks Corporation 2025 All rights reserved.

AX-Network-Visualization(AX-NV) 概要

通信状況を高い精度で可視化し、障害発生時の原因究明と対処を迅速化

◆ネットワークのミラーデータをセンサで取得し、フロー情報としてコレクタに蓄積 & 分析 ①AX-Sensor ②AX-Collector

- インフラから独立したセンサでデータを収集するため、自由度と安定性に優れる
  (どこでも好きなところのデータが取得できる、インフラ機器の入れ替え不要、インフラ機器に余計な負荷をかけない)
- ノンサンプルの完全なデータを取得できるため、トラフィックの時系列可視化ときめ細かな分析が可能
- 3D描画による直感的な可視化や、機械学習エンジンと連携してのサイレント故障・予兆検知にも対応



© ALAXALA Networks Corporation 2025 All rights reserved.

①AX-Sensor ～フロー収集～

ミラーデータからフロー情報を生成し、
リアルタイムかつノンサンプリングでのパケット統計/通知を可能に

低 ← 価格・性能 → 高

UTP 8port
AX-Sensor-08TL 200Mセンサ

- ✓ 1G(UTP)×8ポート (2ポートがモニター)
- ✓ **性能上限200Mbps**

UTP 8port
AX-Sensor-08T 1Gセンサ

- ✓ 1G(UTP)×8ポート (4ポートがモニター)

UTP 8port + SFP+ 2port
AX-Sensor-08T2X 10Gセンサ

- ✓ 1G(UTP)×8ポート (2ポートがモニター)
- ✓ 10G(SFP+)×2ポート (1ポートがモニター)

受信したミラーデータからフロー情報を生成し、AX-Collector や他社の NetFlow Collector へ転送

簡単	既設のネットワークに手を加えず、見たいデータをミラーするだけで導入できる
安心	外付け設置なので、インフラを構成するネットワーク装置に負荷をかけない
カスタマイズ	標準のNetFlow v9に加え、アラクサラ独自のフロー識別(AX-Flow)をサポート

NetFlow v9対応の標準的なコレクタと接続可能

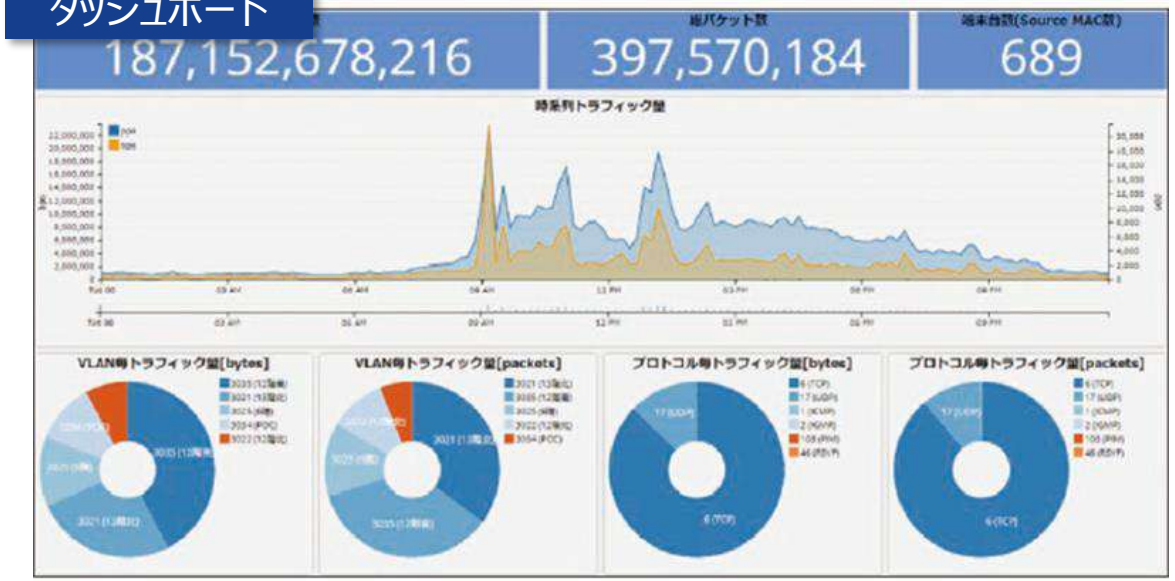
© ALAXALA Networks Corporation 2025 All rights reserved.

②AX-Collector ～可視化～

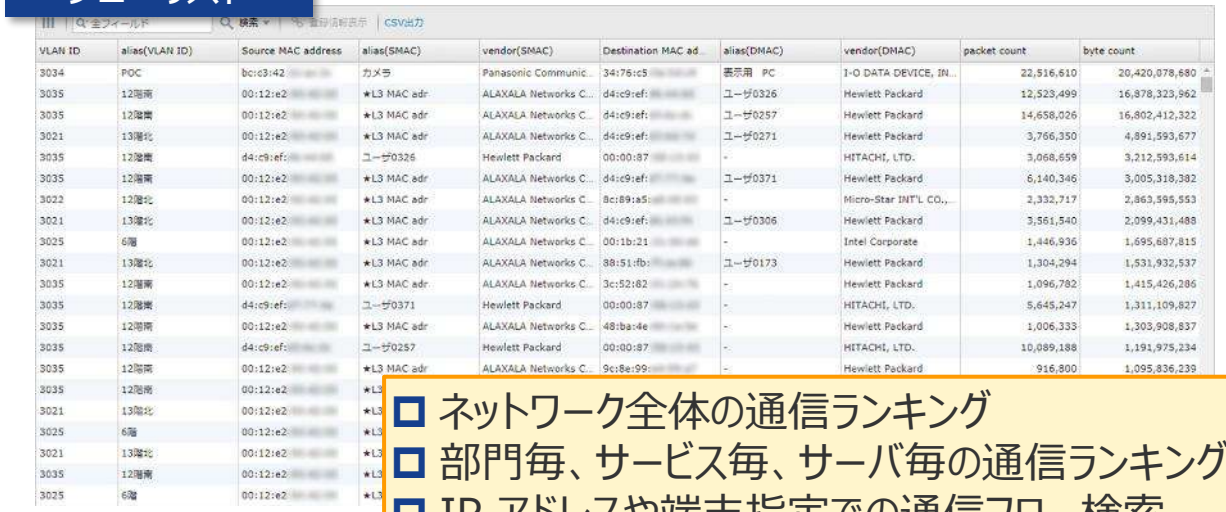
AX-Sensor やネットワーク機器からフロー情報/MIBデータを収集・蓄積・分析し、Webブラウザを介してネットワークを可視化

- ◆トラフィック情報、端末通信フロー、各種ランキングをダッシュボードにリアルタイムで可視化
- ◆ユーザごと、部門ごと、サーバごとなど目的に応じて可視化の内容を柔軟にカスタマイズ可能
- ◆収集した通信フローリストにエイリアスを付加し、可読性をアップして柔軟に検索可能

ダッシュボード



フローリスト



VLAN ID	alias(VLAN ID)	Source MAC address	alias(SMAC)	vendor(SMAC)	Desbination MAC ad...	alias(DMAC)	vendor(DMAC)	packet count	byte count
3034	POC	bc:c3:42	カメラ	Panasonic Communic...	34:76:c5	表示用 PC	I-O DATA DEVICE, IN...	22,516,610	20,420,078,680
3035	12階南	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	d4:c9:ef:	ユーザ0326	Hewlett Packard	12,523,499	16,878,323,962
3035	12階南	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	d4:c9:ef:	ユーザ0257	Hewlett Packard	14,658,026	16,802,412,322
3021	13階北	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	d4:c9:ef:	ユーザ0271	Hewlett Packard	3,766,350	4,891,593,677
3035	12階南	d4:c9:ef:	ユーザ0326	Hewlett Packard	00:00:87	-	HITACHI, LTD.	3,068,659	3,212,593,614
3035	12階南	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	d4:c9:ef:	ユーザ0371	Hewlett Packard	6,140,346	3,005,318,382
3022	12階北	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	8c:89:a5	-	Micro-Star INT'L CO,...	2,332,717	2,863,595,553
3021	13階北	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	d4:c9:ef:	ユーザ0306	Hewlett Packard	3,561,540	2,099,431,488
3025	6階	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	00:1b:21	-	Intel Corporate	1,446,936	1,695,687,815
3021	13階北	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	88:51:fb:	ユーザ0173	Hewlett Packard	1,304,294	1,531,932,537
3035	12階南	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	3c:52:82	-	Hewlett Packard	1,096,782	1,415,426,286
3035	12階南	d4:c9:ef:	ユーザ0371	Hewlett Packard	00:00:87	-	HITACHI, LTD.	5,645,247	1,311,109,827
3035	12階南	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	48:ba:4e	-	Hewlett Packard	1,006,333	1,303,908,837
3035	12階南	d4:c9:ef:	ユーザ0257	Hewlett Packard	00:00:87	-	HITACHI, LTD.	10,089,188	1,191,975,234
3035	12階南	00:12:e2	★L3 MAC adr	ALAXALA Networks C...	9c:8e:99:	-	Hewlett Packard	916,800	1,095,836,239
3035	12階南	00:12:e2	★L3						
3021	13階北	00:12:e2	★L3						
3025	6階	00:12:e2	★L3						
3021	13階北	00:12:e2	★L3						
3035	12階南	00:12:e2	★L3						
3025	6階	00:12:e2	★L3						

- ネットワーク全体の通信ランキング
- 部門毎、サービス毎、サーバ毎の通信ランキング
- IP アドレスや端末指定での通信フロー検索
- その他

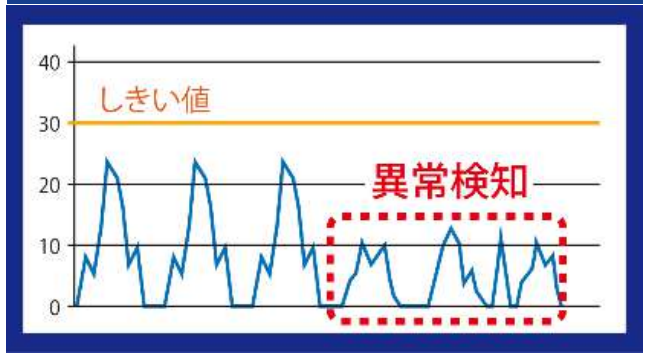
© ALAXALA Networks Corporation 2025 All rights reserved.

②AX-Collector ～異常検知・長期蓄積～

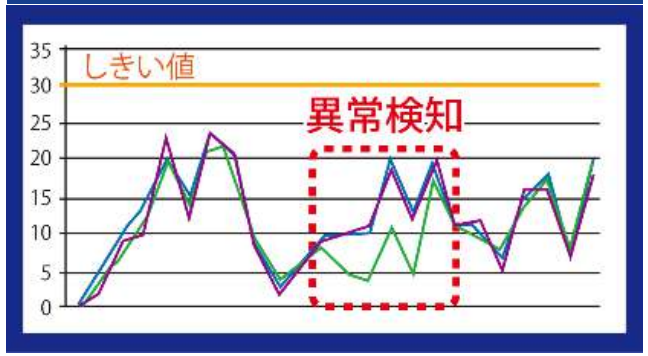
収集した情報を基に、しきい値や機械学習エンジンとの連携による異常検知を実施

◆機械学習技術により、従来のしきい値監視では検知できなかったサイレント故障や障害の予兆を的確に検知

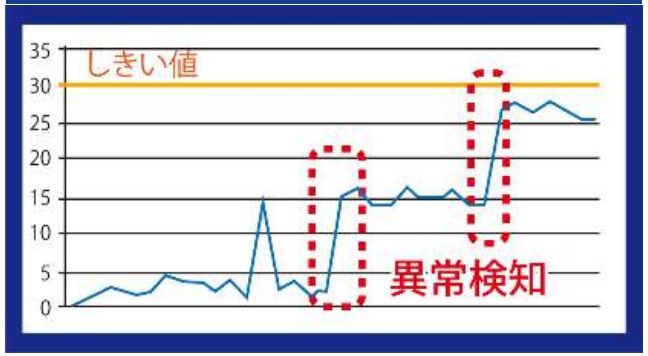
周期性の異常（周期ずれ）



相関性の異常（相関ずれ）



状態変化の異常（変化点検知）

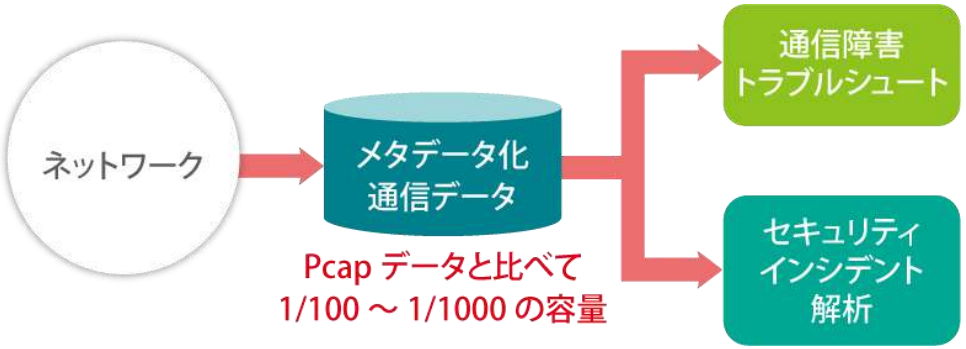


※ 機械学習技術は、ブレインズテクノロジー社製「Impulse」と連携

メタデータ化された通信履歴データにより容量を削減し、長期保存と高速検索を可能に

◆収集した通信フロー情報は、
ネットワークフォレンジックとして長期間蓄積可能

◆少ないデータ量と高速検索を活かして、
障害のトラブルシュートや
セキュリティインシデントの解析を支援



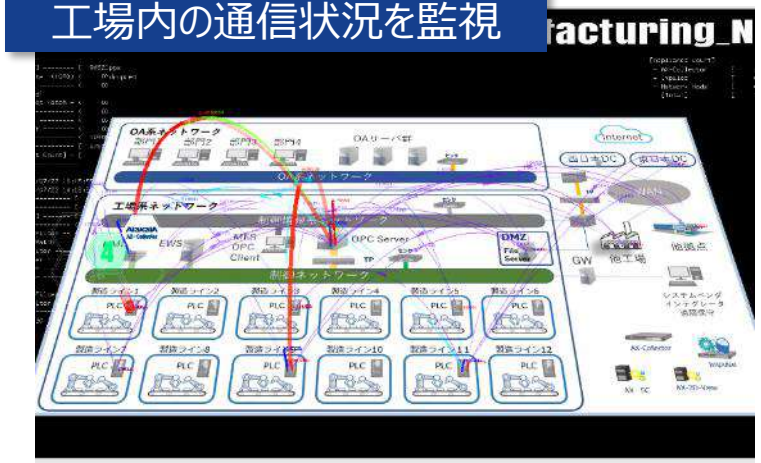
© ALAXALA Networks Corporation 2025 All rights reserved.

③AX-3D-Viewer ～3D可視化～

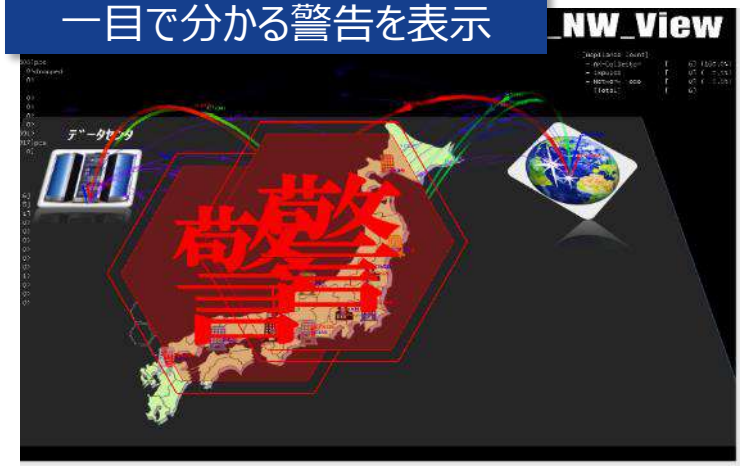
**AX-Sensorから送られるフロー情報を受信し、ネットワークマップ(地図や構成図)上に
リアルタイムなトラフィックや障害の発生状況を直観的で分かりやすく3D表示**

- 輻輳の発生箇所や通信の途切れなどの異常な状態を視覚で直観的に把握可能
- 【警告表示】 障害の発生箇所を3D画面上にリアルタイム表示
  直観的で分かりやすく警告を表示、専門知識がなくてもインシデント発生の確認が可能
- 【利便性】 Webベースのマルチ画面表示と録画機能で、ブラウザ上に複数の画面を同時に表示

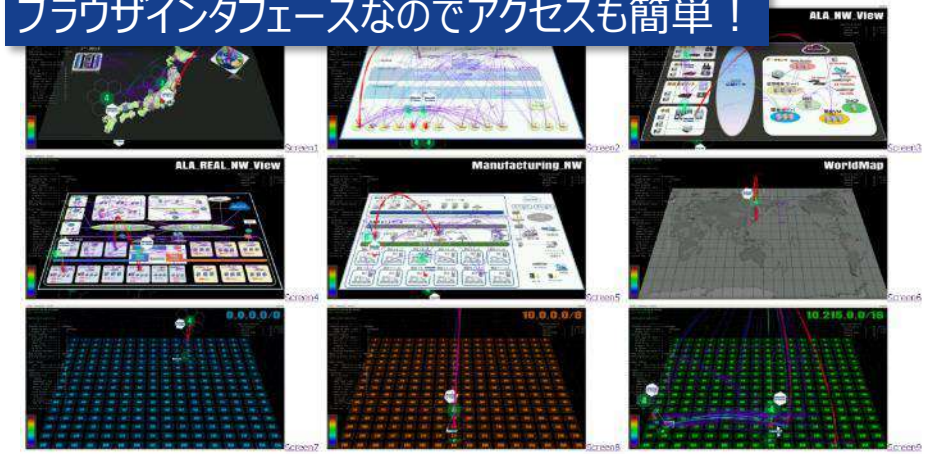
構成図を背景にして
工場内の通信状況を監視



障害発生時には
一目で分かる警告を表示



複数画面を同時に監視、
ブラウザインタフェースなのでアクセスも簡単！



© ALAXALA Networks Corporation 2025 All rights reserved.

品質可視化

従来のTCP品質測定に加え、UDPトラフィックの品質測定にも対応、Web会議アプリケーションがTCP/UDPのどちらを利用していても可視化可能

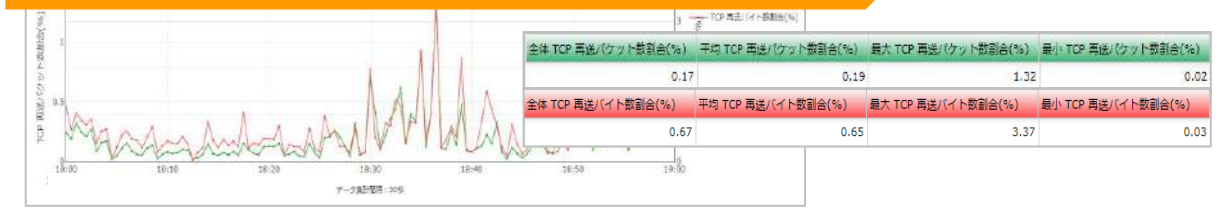
TCP品質測定

TCPを可視化し「なぜか遅い」の原因特定を容易に

- ✓ 往復遅延時間(RTT)、応答時間(SRT)、遅延時間(Delay)を可視化
- ✓ TCPフラグごとの可視化も可能
  (SYN攻撃を受けている、接続・切断の状況がわかる、など)
- ✓ 再送パケットの情報も収集し、TCP再送パケット数割合と
  バイト数割合を表示(閾値監視も可能)

特定アドレス宛のRTT

特定アドレス宛のTCP再送パケット数割合/バイト数割合



UDP品質測定

UDPを使用するWeb会議等の通信品質分析が可能

- ✓ 遅延時間(Delay)、揺らぎ(Jitter)を可視化
- ✓ RTP(Real-time Transport Protocol)を使用している場合は、
  RTPヘッダから詳細情報(RTT、パケットロス数など)も可視化可能
- ✓ Zoom(※)、Microsoft Teams、Cisco WebEx、Google Meet は
  RTPを使用している

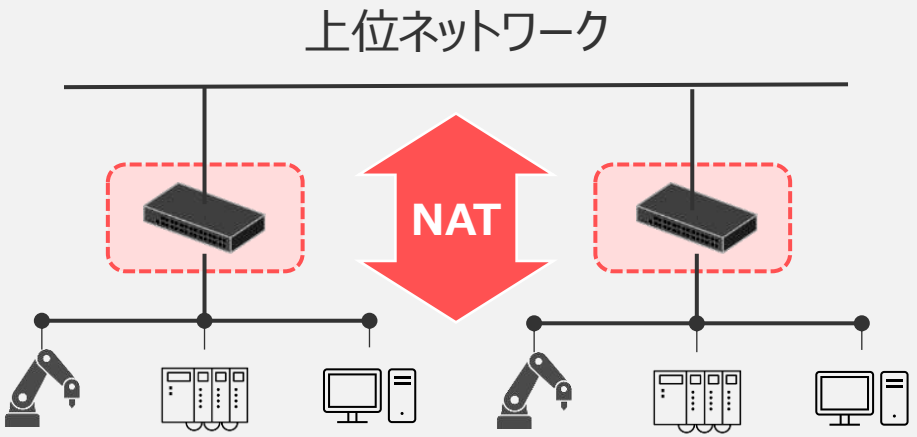
UDP品質測定項目		説明
一版のUDP	Delay	連続するUDPストリームの到着間隔
	Jitter	連続するUDPストリームの到着間隔の揺らぎ
RTP時の追加項目	RTT	STUN bindingパケットの送受信時刻差分 (※)
	パケットロス数	RTPヘッダの抜けたシーケンス番号の合計
	順序外到着回数	RTPヘッダのシーケンス番号が連続していなかった回数

※ ZoomはSTUN未使用のため、RTTは測定不可

© ALAXALA Networks Corporation 2025 All rights reserved.

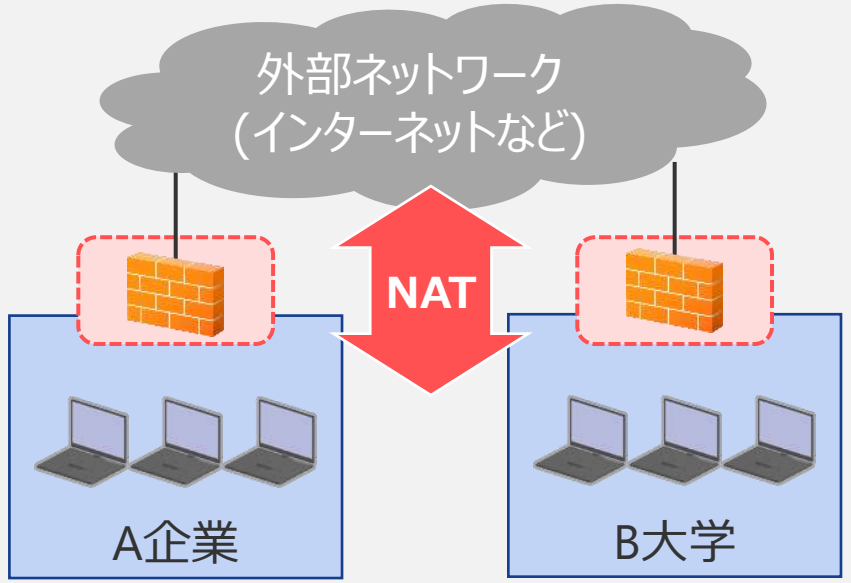
NAT機能(IPアドレス変換)

生産工場のラインネットワークと、上位ネットワークとの境界



端末(PC、サーバ、PLCなど)を収容

組織(企業/事業所/大学など)と、外部ネットワークとの境界



© ALAXALA Networks Corporation 2025 All rights reserved.

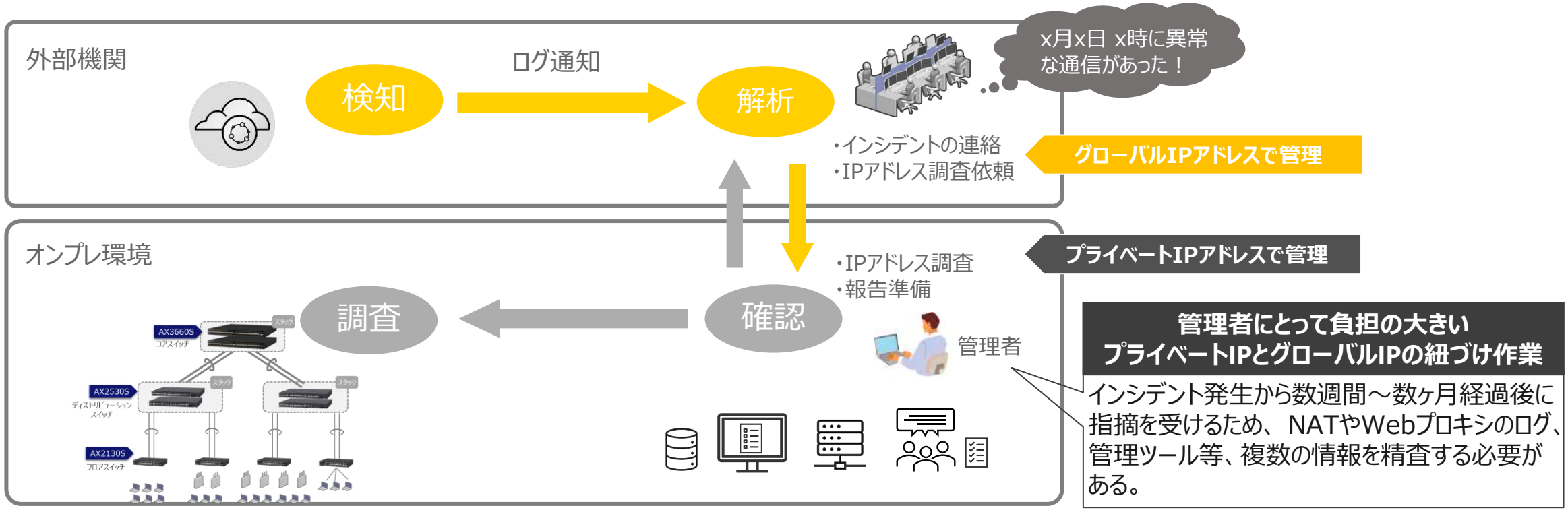
NAT可視化（1/3）

AX-Collector(Ver 1.12)
2024年1月リリース済

インシデント発生時、NAT環境の送信元IPアドレス調査に時間を要する

◆NAT環境下における調査依頼の現状と課題

- プライベートIPアドレスの位置情報は、管理ツール(AX-NM)により可視化可能
- ただし、調査依頼はグローバルIPアドレスでの指摘となるため、指摘のあった特定時間帯における
  グローバルIPアドレス（または企業内のローカルIP）とプライベートIPアドレスの関係を同時に把握する必要がある

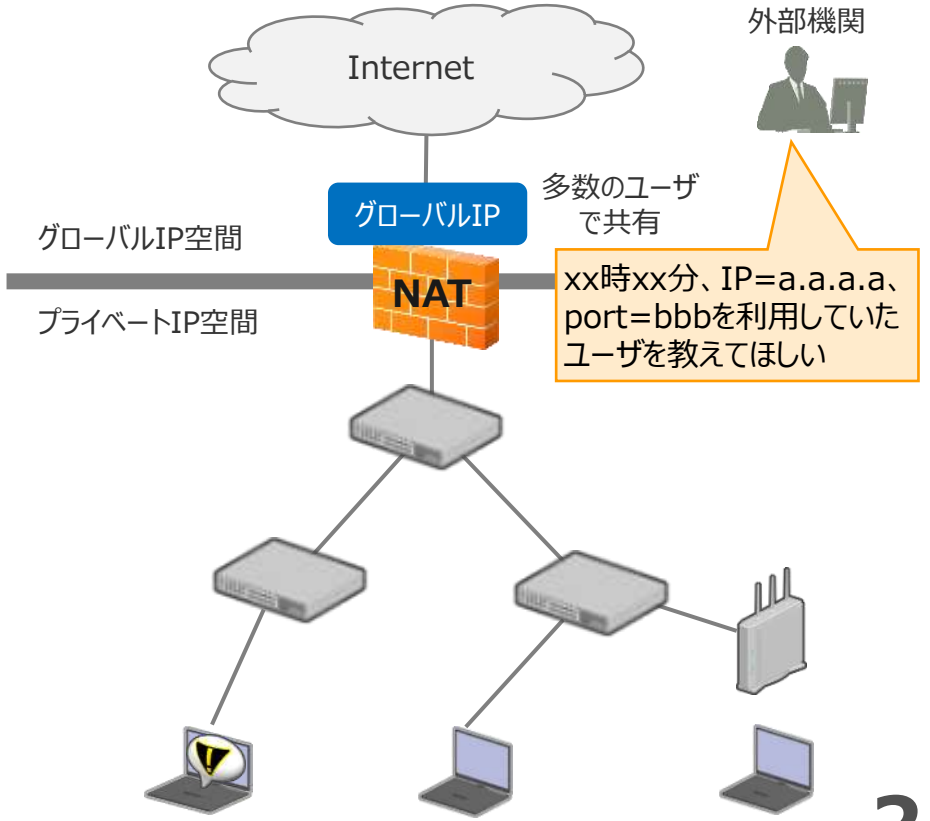


© ALAXALA Networks Corporation 2025 All rights reserved.

NAT可視化（2/3）

AX-Collector(Ver 1.12)
2024年1月リリース済

NAT環境のIPアドレス調査工数を、FortiGateとAX-NVの連携で最適化

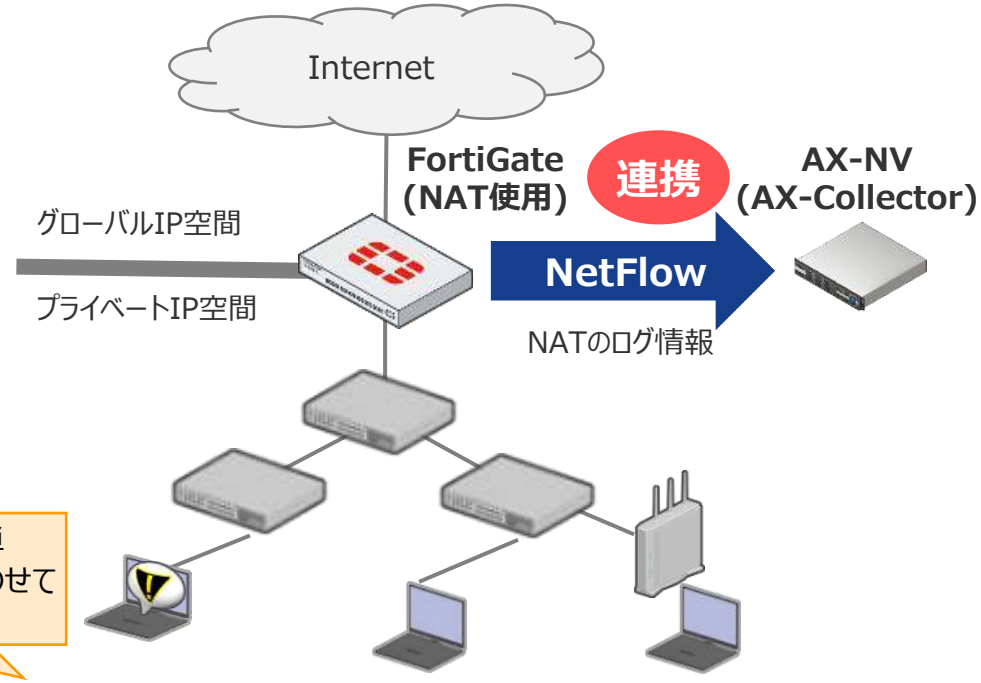


外部機関(警察やSINET)からのIPアドレス開示請求はグローバルIPで調査依頼が来るため、対応するプライベートIPを利用していたユーザの特定には大きな手間がかかる

FORTINET

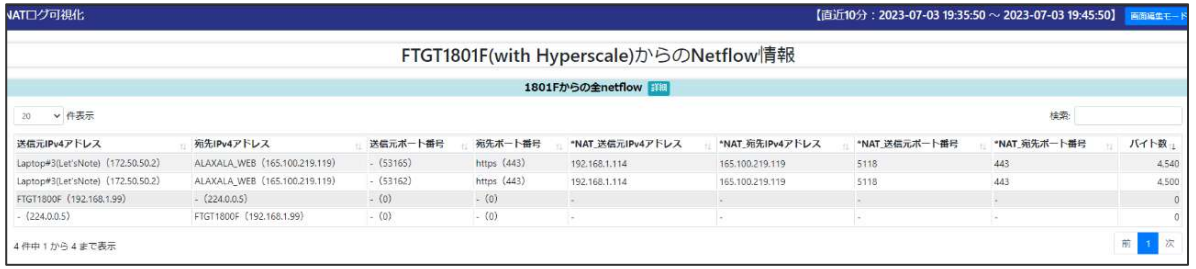
連携で解決!

AlaxalA



WebUIなので調査も簡単
(多数のテキストログを突き合わせて調査する必要が無い)

NAT前後のIPアドレスの関係をGUIで確認



© ALAXALA Networks Corporation 2025 All rights reserved.

NAT可視化（3/3）

AX-Collector(Ver 1.12)
2024年1月リリース済

IPアドレス開示請求書などに記載の「日時」「グローバルIP」「L4ポート番号」で検索可能

AX-Collectorの画面

【直近10分：2023-07-03 19:35:50 ～ 2023-07-03 19:45:50】 画面編集モード

プライベートIPアドレスとL4ポート、グローバルIPアドレスとL4ポートを見やすく併記することで、
指定された時刻のプライベート/グローバルの紐づけ作業を簡単化

20 件表示　　検索:

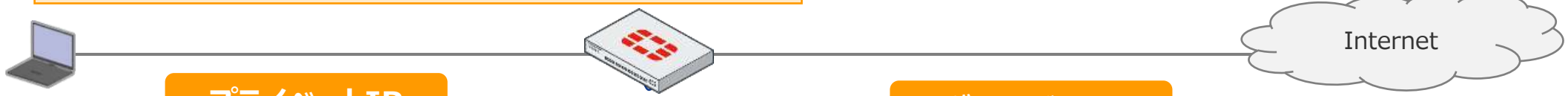
送信元IPv4アドレス	宛先IPv4アドレス	送信元ポート番号	宛先ポート番号	*NAT_送信元IPv4アドレス	*NAT_宛先IPv4アドレス	*NAT_送信元ポート番号	*NAT_宛先ポート番号	バイト数
Laptop#3(Let'sNote)（172.50.50.2）	ALAXALA_WEB（165.100.219.119）	-（53165）	https（443）	192.168.1.114	165.100.219.119	5118	443	4,540
Laptop#3(Let'sNote)（172.50.50.2）	ALAXALA_WEB（165.100.219.119）	-（53162）	https（443）	192.168.1.114	165.100.219.119	5118	443	4,500
FTGT1800F（192.168.1.99）	-（224.0.0.5）	-（0）	-（0）	-	-	-	-	0
-（224.0.0.5）	FTGT1800F（192.168.1.99）	-（0）	-（0）	-	-	-	-	0

4 件中 1 から 4 まで表示　　前 1 次

プライベート側 IPアドレス　　プライベート側 L4ポート番号　　グローバル側 IPアドレス　　グローバル側 L4ポート番号

グローバルIP(192.168.1.114/5118)で指摘されたのは、
172.50.50.2のプライベートIPを付与していた
ユーザだと簡単に特定できた！

※ テスト環境でグローバルIPを「192.168.1.114」とした場合の例



プライベートIP

送信元IP/L4ポート：172.50.50.2/53165, 53162
宛先IP/L4ポート　：165.100.219.119/443

NAT

グローバルIP

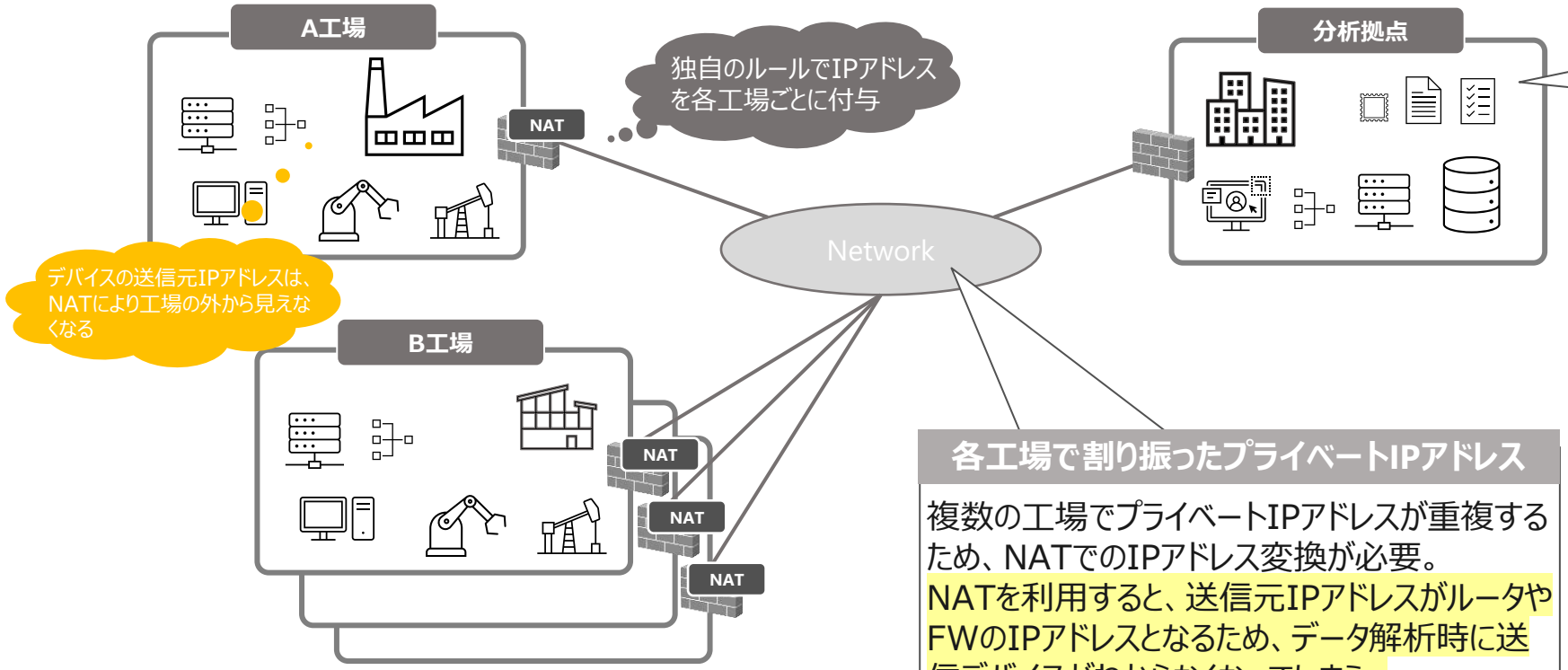
送信元IP/L4ポート：192.168.1.114/5118
宛先IP/L4ポート　：165.100.219.119/443

© ALAXALA Networks Corporation 2025 All rights reserved.

製造業向け利用シーン（1/2）

複数の工場にてプライベートIPアドレスが重複した際、変換前の情報がNATにより不明

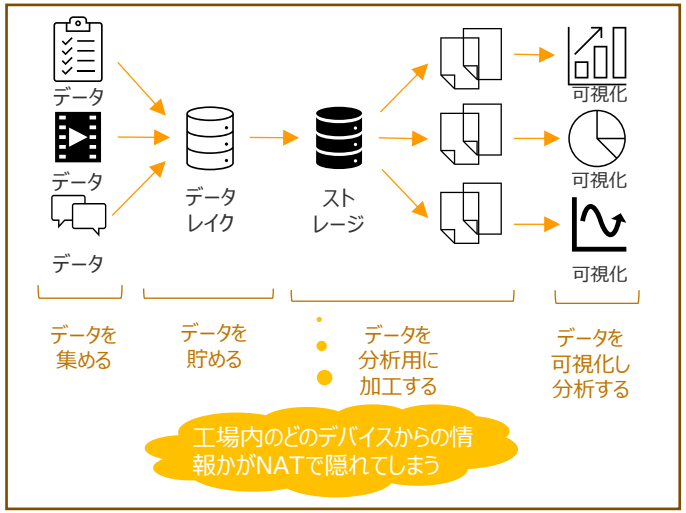
- 各工場からのデータ集積（DXに向けた準備）に関しての課題
- 各工場がローカルにプライベートIPアドレスをOT環境向けに割り振り
- いくつかの工場でIPアドレスが重複し、データ集積時にNATでのIPアドレス変換が必要
- 送信元IPアドレスをNAT変換するため、どのデバイスからのデータが特定できず、データ集積に支障が出る



各工場で割り振ったプライベートIPアドレス

複数の工場でプライベートIPアドレスが重複するため、NATでのIPアドレス変換が必要。
NATを利用すると、送信元IPアドレスがルータやFWのIPアドレスとなるため、データ解析時に送信デバイスがわからなくなってしまう。

DX推進に向けたデータ集積（データレイク等）の際、NAT変換前の送信元を特定できない

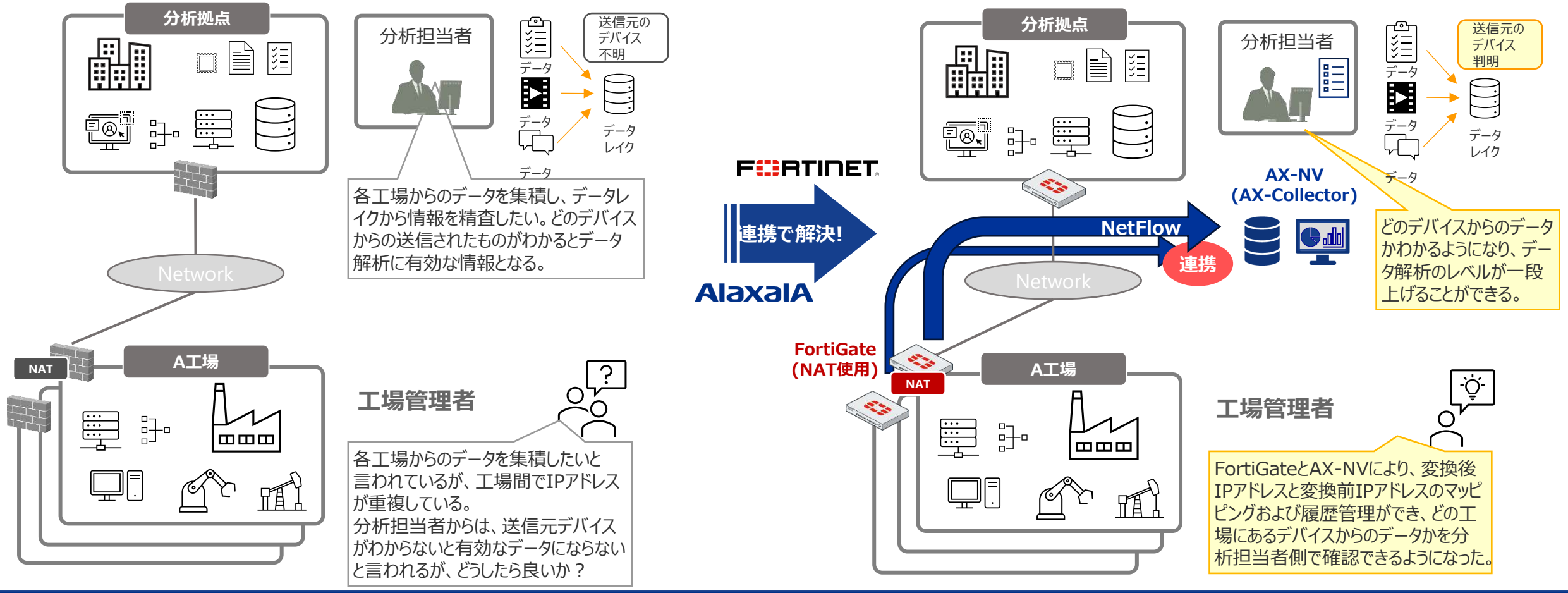


© ALAXALA Networks Corporation 2025 All rights reserved.

製造業向け利用シーン（2/2）

複数の工場でIPアドレスが重複し、NATを利用時もデータの送信元デバイスを特定します

- FortiGate + AXシリーズのソリューション提案（AX-NV/Collector）
- NAT/FW製品をFortiGateへのリプレースし、AX-NV/Collectorとの連携によるNAT変換前後のIPアドレスマッピングの可視化



© ALAXALA Networks Corporation 2025 All rights reserved.

ユースケース：公開サーバのDDoS対応/情報漏洩(1/2)

【文教/エンプラ/官公庁】DDoS などのサイバー攻撃の詳細を分析

課題

サイバー攻撃を受けている状況を可視化したい

- 組織外にも公開しているサービスが、サイバー攻撃の対象になっていないか知りたい
- SNMP(MIB)による監視では、正式なサービスリクエストなのか、不正攻撃なのか判別できない
- トラフィックが増えているかなど、リアルタイムな状況を直観的に分かるようにしたい

適用

外部公開サーバのフロー情報を分析し、トラフィックの状況を3Dで可視化

- AX-Sensorにファイアウォール前後のパケットをミラーでインプットし、フロー情報はAX-Collectorに蓄積
- ファイアウォールのログ(syslog)を、AX-3D-VIEWERで直観的に可視化

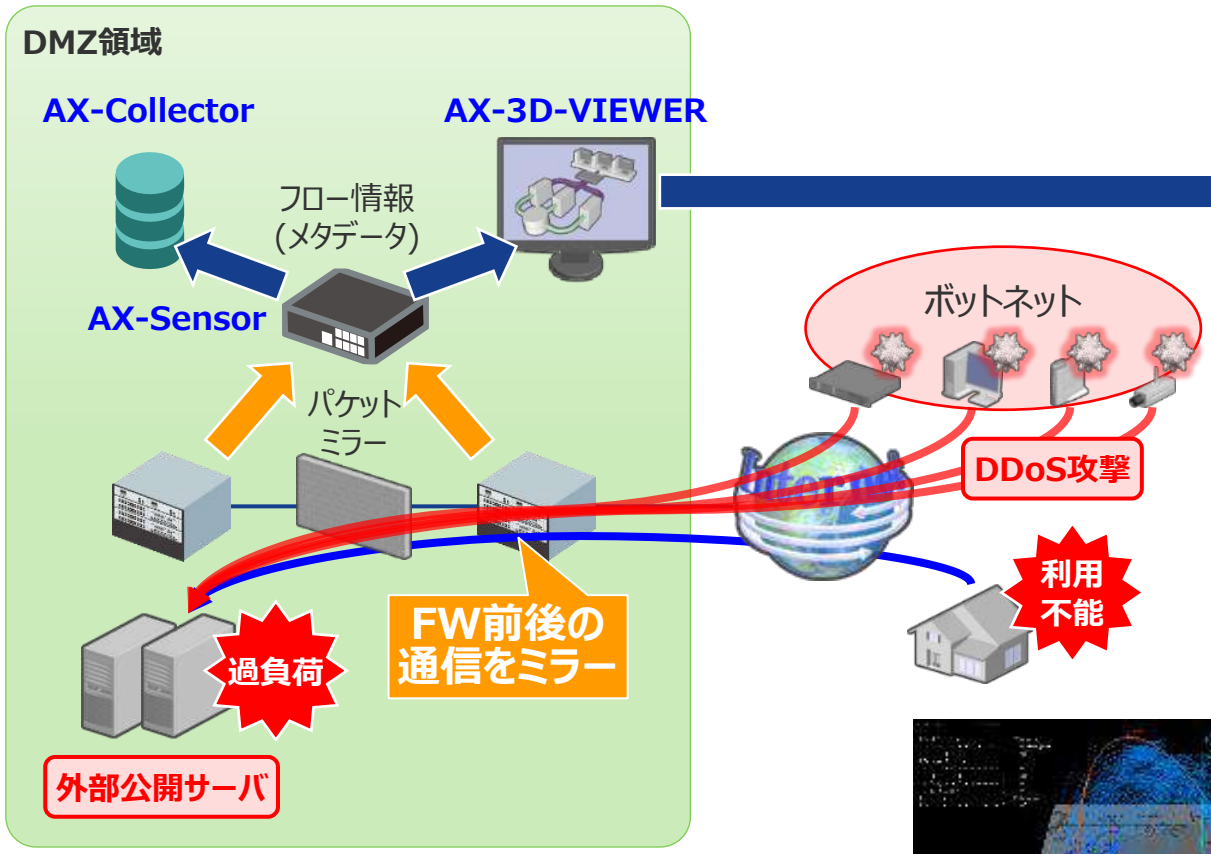
効果

DDoS 攻撃を特定 & ファイアウォールで防御し、インフラの負荷を低減

- DDoS攻撃の詳細を分析し、原因を特定
- 原因となる通信のフィルタリングをファイアウォールに設定し、防御を実施
- サービスへのリクエスト状況を、3次元的なトラフィック表示で直感的に把握

© ALAXALA Networks Corporation 2025 All rights reserved.

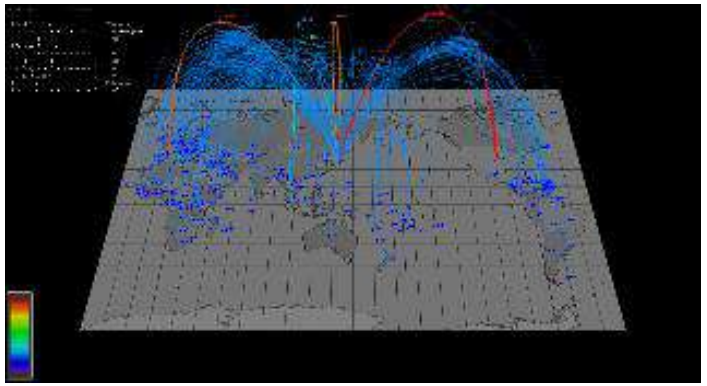
ユースケース：公開サーバのDDoS対応/情報漏洩(2/2)

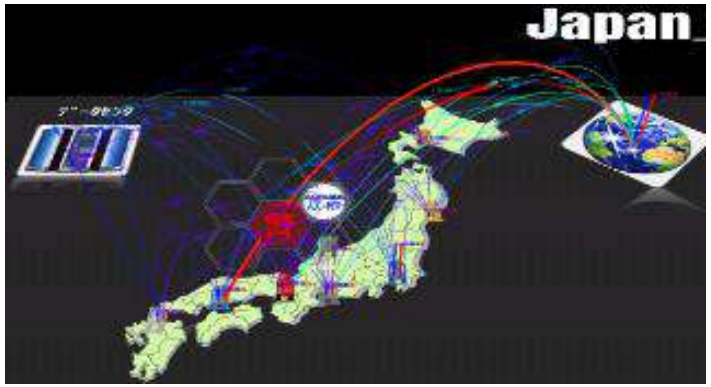


攻撃フローの詳細分析

フローの可視化･長期保存

3D可視化(システムを俯瞰的に監視)





© ALAXALA Networks Corporation 2025 All rights reserved.

The Guaranteed Network

いちばん近くで、もっと先へ。

© ALAXALA Networks Corporation 2025 All rights reserved.