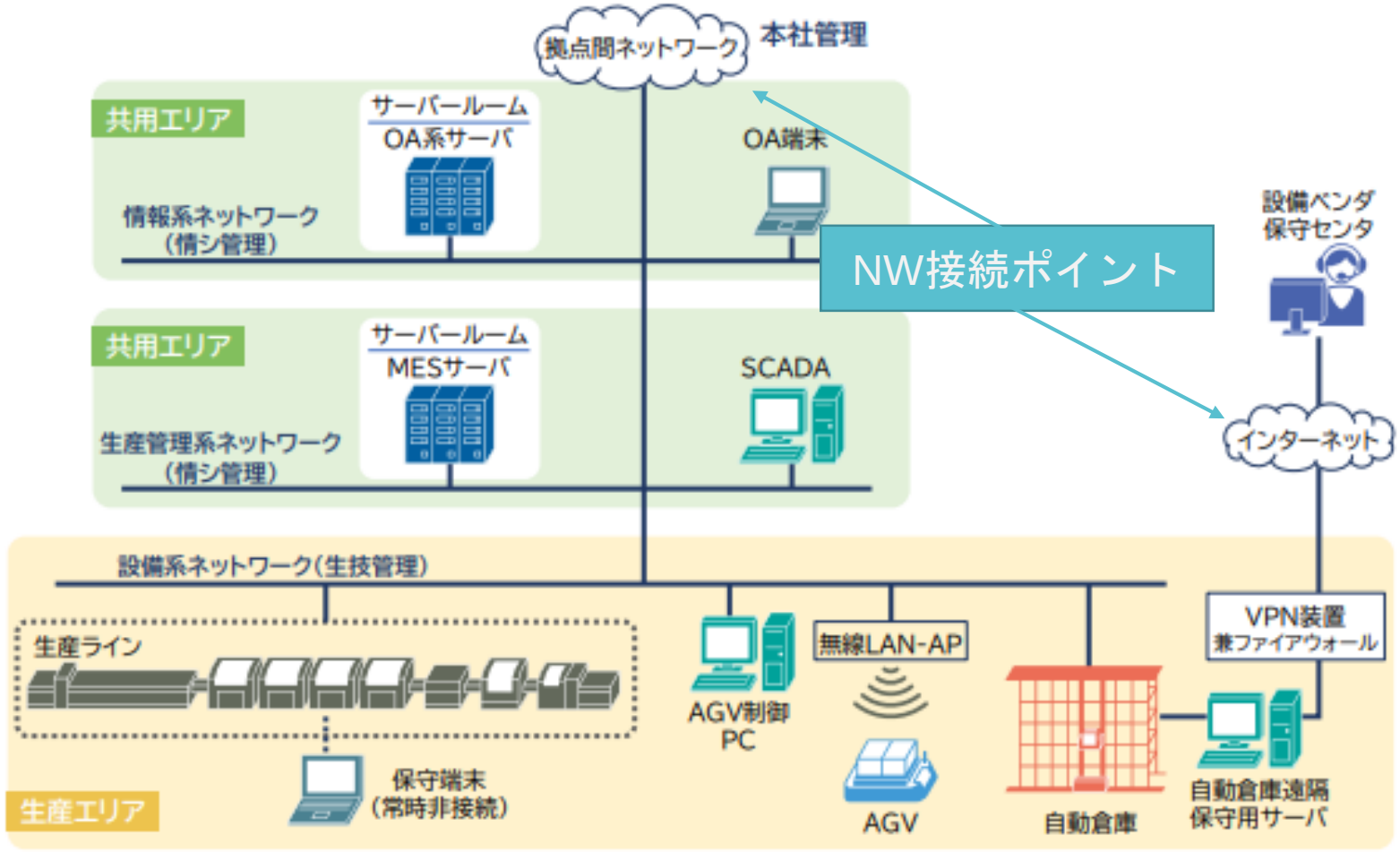
「Flowmon」でネットワークの可視化を始めよう！
～サイバー・フィジカルセキュリティ対策～

Progress Flowmon

Flowmonって何モン？

工場NWサンプル構成例



※出典：経済産業省「サイバー・フィジカルセキュリティ対策ガイドライン」

管理者様が抱えるお悩み

クローズ環境でなくなったということは・・・
外部へのアクセスができるようになり便利になった反面・・・
外部からもアクセスできるということ・・・

対策を取る上での懸念点

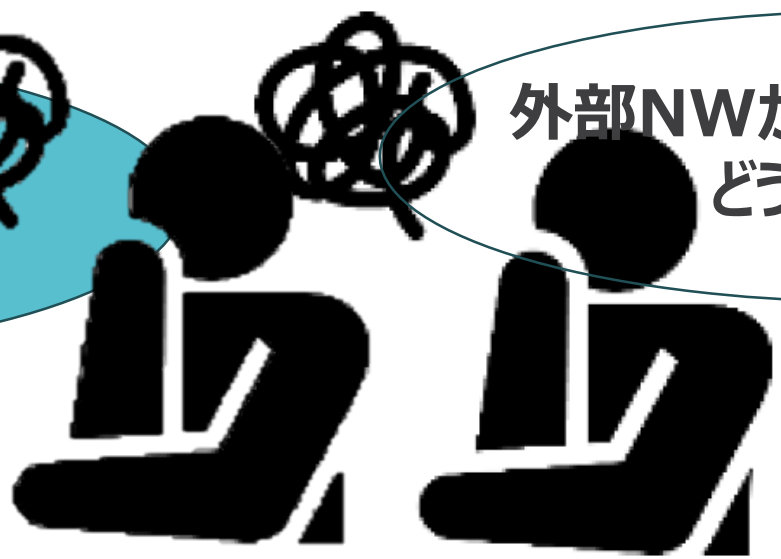
複数のNW

多数の
管理ノード

セキュリティ対策

最適な投資にするために
複数NWはどうすればいい?
NWを包括的に見れるのか？

サーバ、端末個別に監視？



外部NWからの攻撃対策を
どうするか？

問題点を明らかにするために必要な情報とは

いつ、誰が、何を した？

怪しいふるまいをしている端末は ないか？

可視化情報からできることとは

問題点が明らかになり、**適切な対策**がわかる

怪しいふるまいをしている端末がある
管理者が把握できていない 通信が転送されている

Flowmonとは？

ネットワークフローを使って
「**トラフィック可視化　怪しいふるまいを検知**」する解析ツール

NetFlowとは？

■フロー分析のメリット

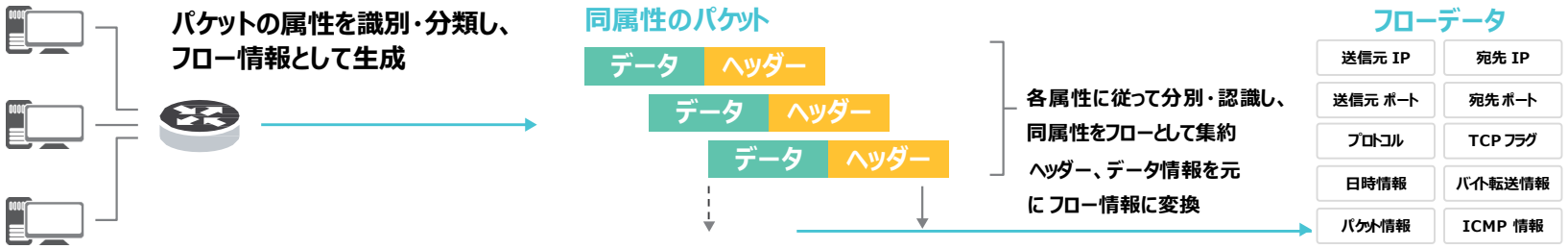
＊パケットのヘッダー情報から**詳細な分析が可能**

＊データが軽い（パケットのおよそ**1/500程度**）

・長期的なログ収集が可能

・WAN越しにデータ転送が可能、かつ既存ネットワークへ**負荷がかからない**

＊Cisco以外でもフロー対応機種が増えており、かつフロー設定時の負荷も軽減



NetFlowはSNMPとパケットキャプチャの良いとこどり！

Flowmonで何ができるのか？

Flowmonの活躍その１：トラブルシューティングツール

- 帯域を占有しているユーザ（端末）を特定

Flowmonの活躍その２：通信ログ管理、キャパシティプランニング

- ネットワーク上で、いつ・誰が・何をしたかの証跡管理
- 回線速度の最適化、現状把握及び報告（自動レポート機能）

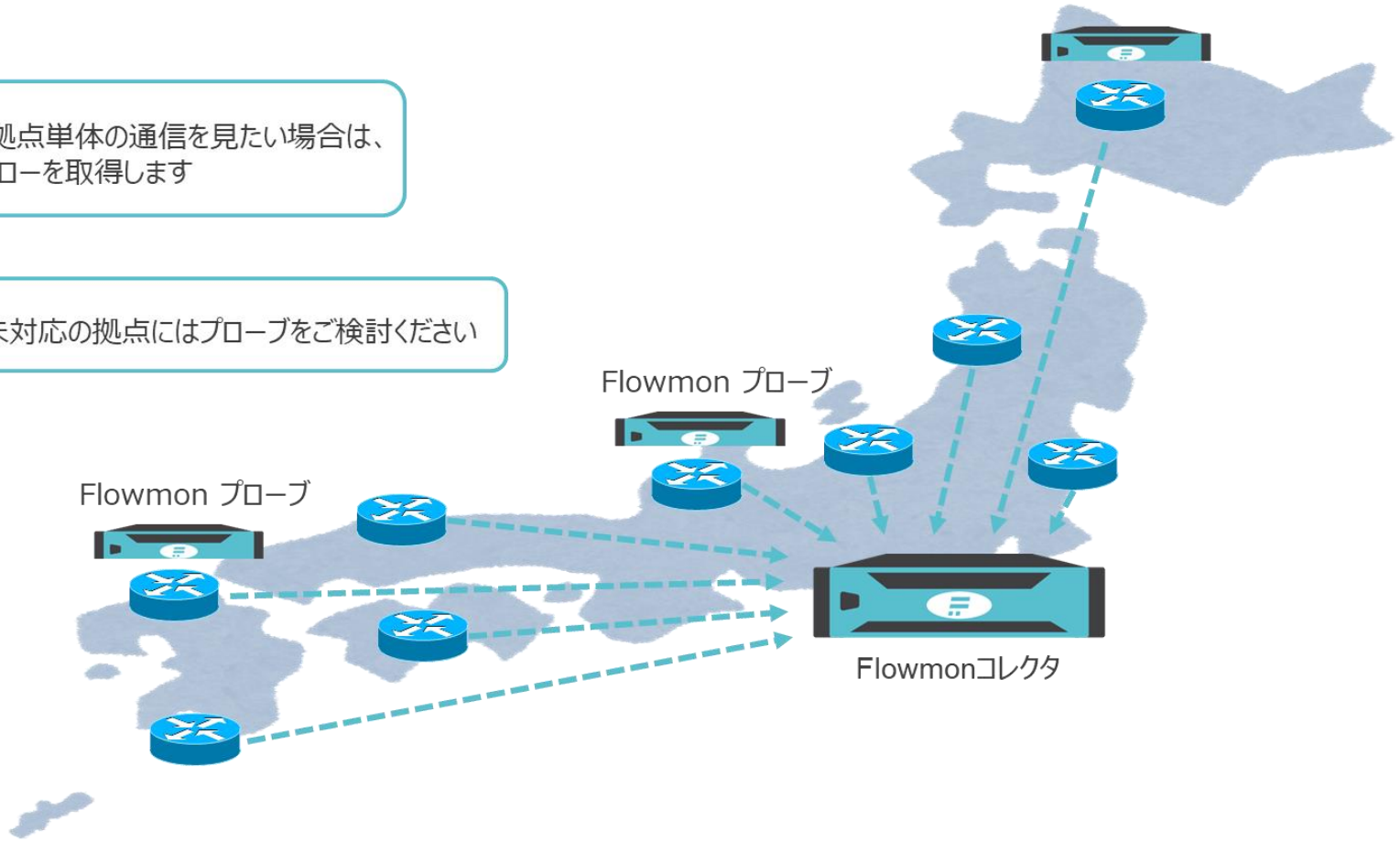
Flowmonの活躍その３：セキュリティ対策（振る舞い検知プラグイン）

- ゲートウェイをすり抜けてきた攻撃の検知
- ウィルス感染端末やユーザのポリシー違反の発見

Flowmonご検討の背景１ 全国に多数の拠点がある

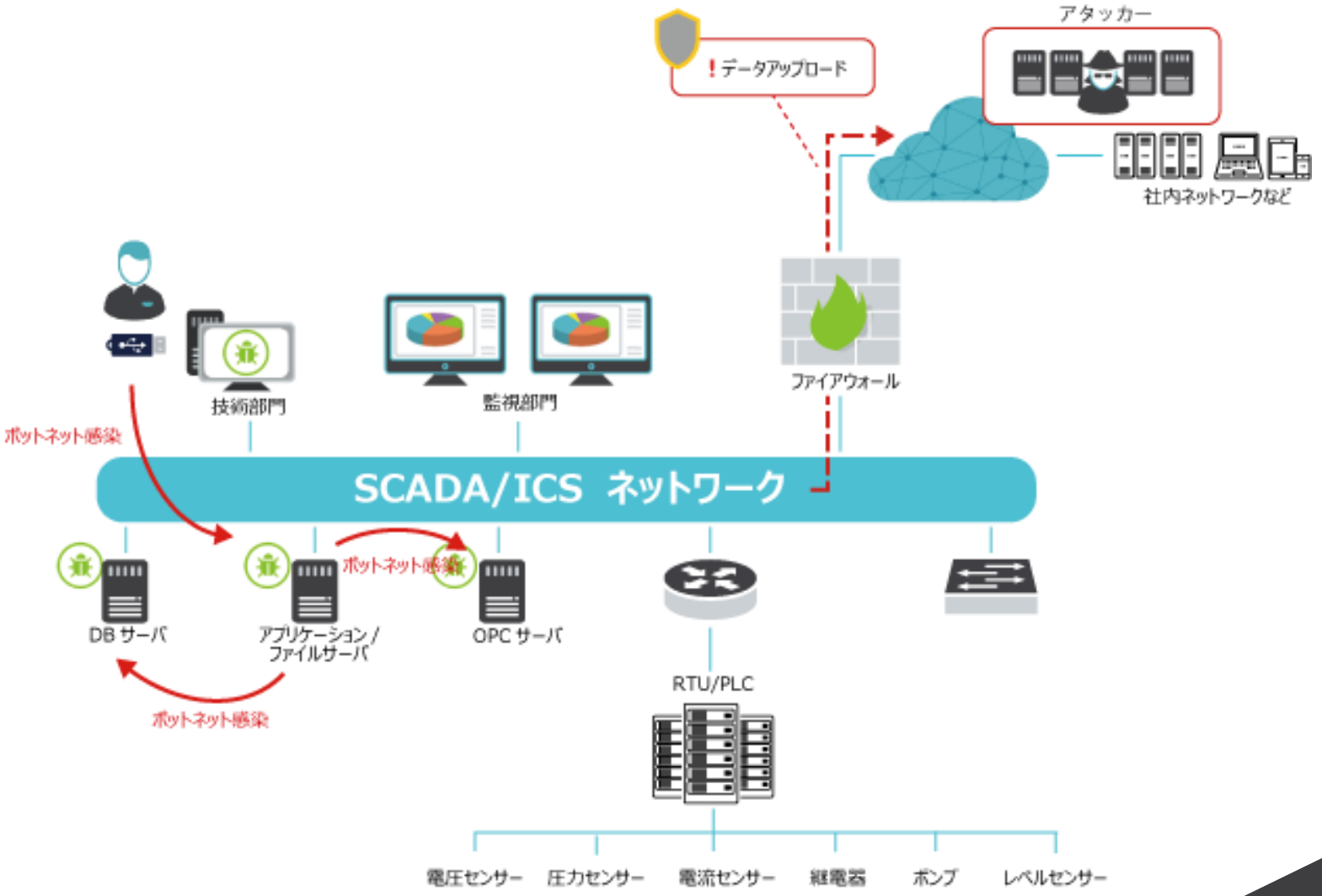
拠点間通信や拠点単体の通信を見たい場合は、
各拠点側からフローを取得します

フロー未対応の拠点にはプローブをご検討ください



ORIZON

Flowmonご検討の背景２ IoTの推進



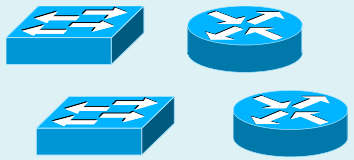
Progress Flowmon

ORIZON

構成イメージ

<データセンター>

ネットワーク機器



プローブはNW機器に専用線で接続、
コレクタへは常用のLANやWAN経由で
フローデータを送出します

①直接フローデータを送出できる
機器の場合は直接コレクタへ

NetFlow
sFlow, etc.

②NetFlow未対応の場合は、
ミラーポートもしくはTAP経由で
一旦プローブへトラフィックを送る

パケット

Flowmon プローブ

NetFlow

Flowmon コレクタ

Progress Flowmon

ORIZON

Flowmonシリーズについて

Flowmon Collector　（コレクタ：フロー分析機）

- Flowmon　Probeもしくは、スイッチやルータなどの他ネットワーク機器から、フロー統計情報(NetFlow/IPFIX、sFlow)を取得・保管し監視・分析します。
- 仮想アプライアンスあり（VMware、Windows Hyper-V）

Flowmon Probe　（プローブ：フロー生成機）

- ネットワークトラフィックからフロー統計情報（NetFlow/IPFIX）を生成します。
- NetFlow/IPFIXを外部コレクタに転送します。コレクタ機能付き（一部制限あり）

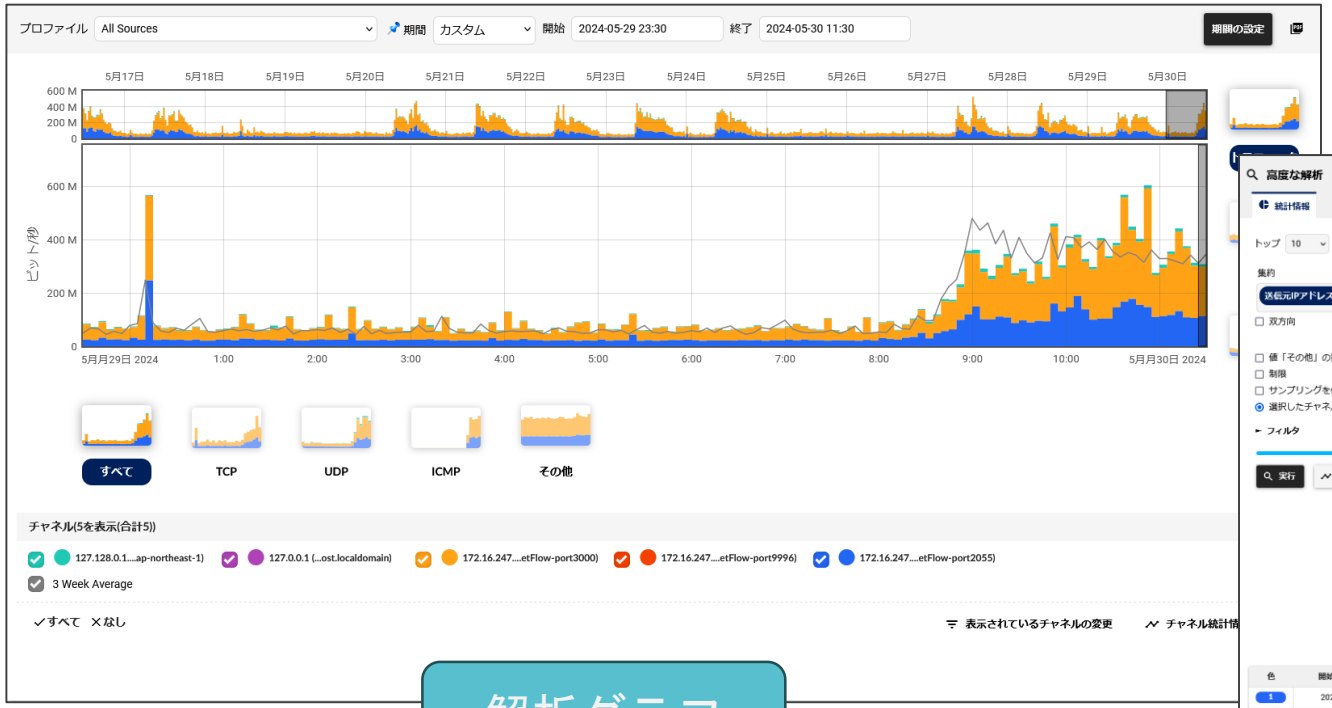
Flowmon ADS（コレクタ+拡張プラグイン）

- ADS（振る舞い検知機能/アノマリー・ディテクション・システム）によりトラフィックを監視し、セキュリティ面での監視・分析を強化します。

Progress Flowmon

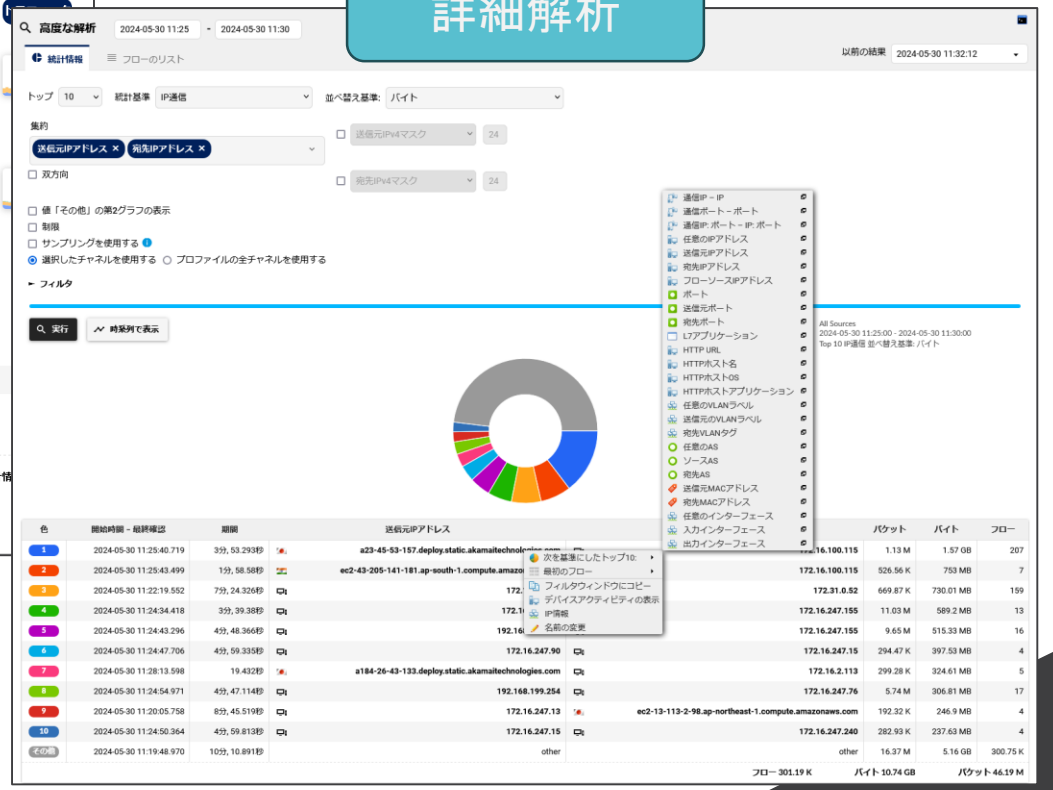
ORIZON

Flowmon画面イメージ①



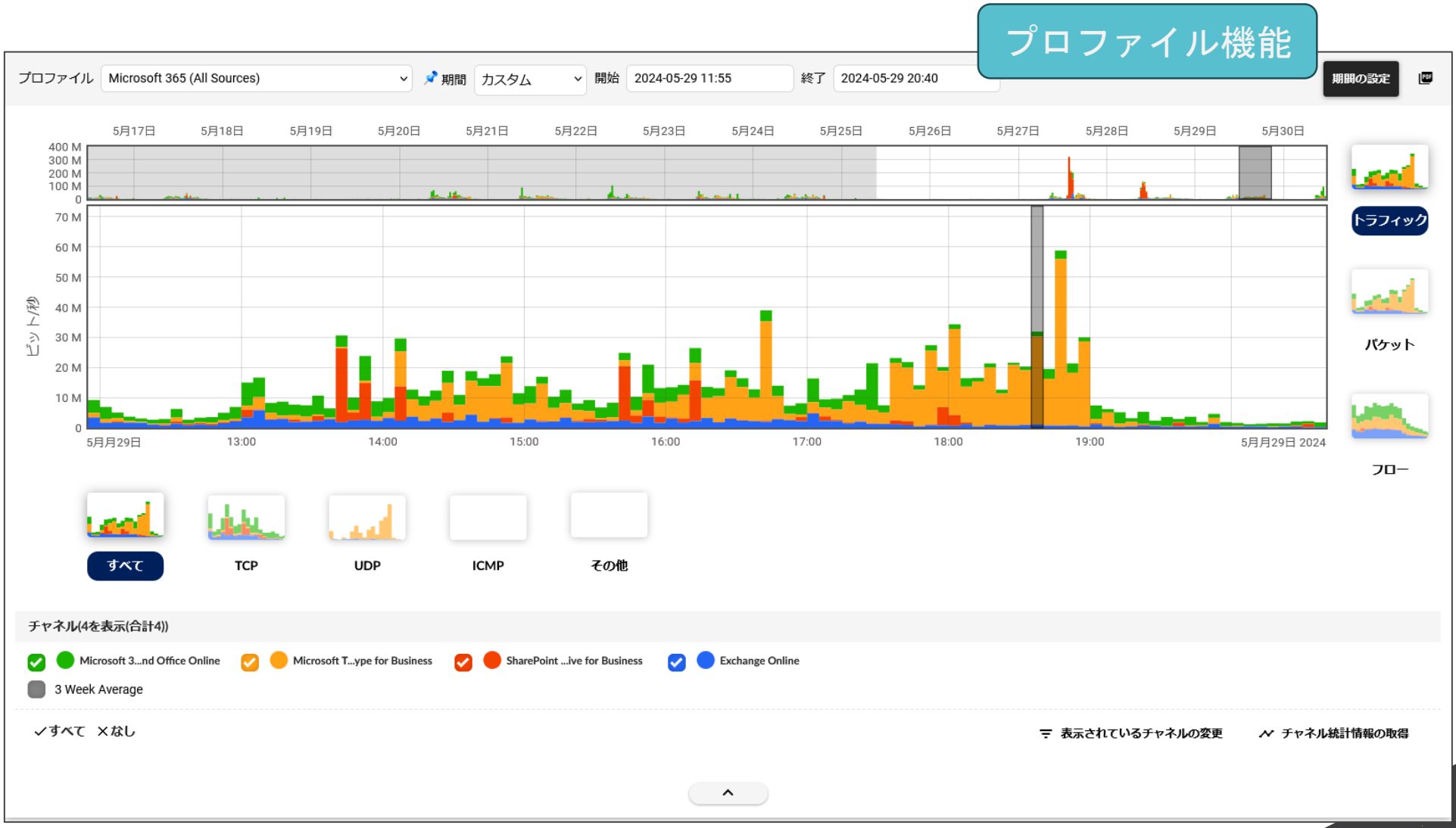
解析グラフ

詳細解析



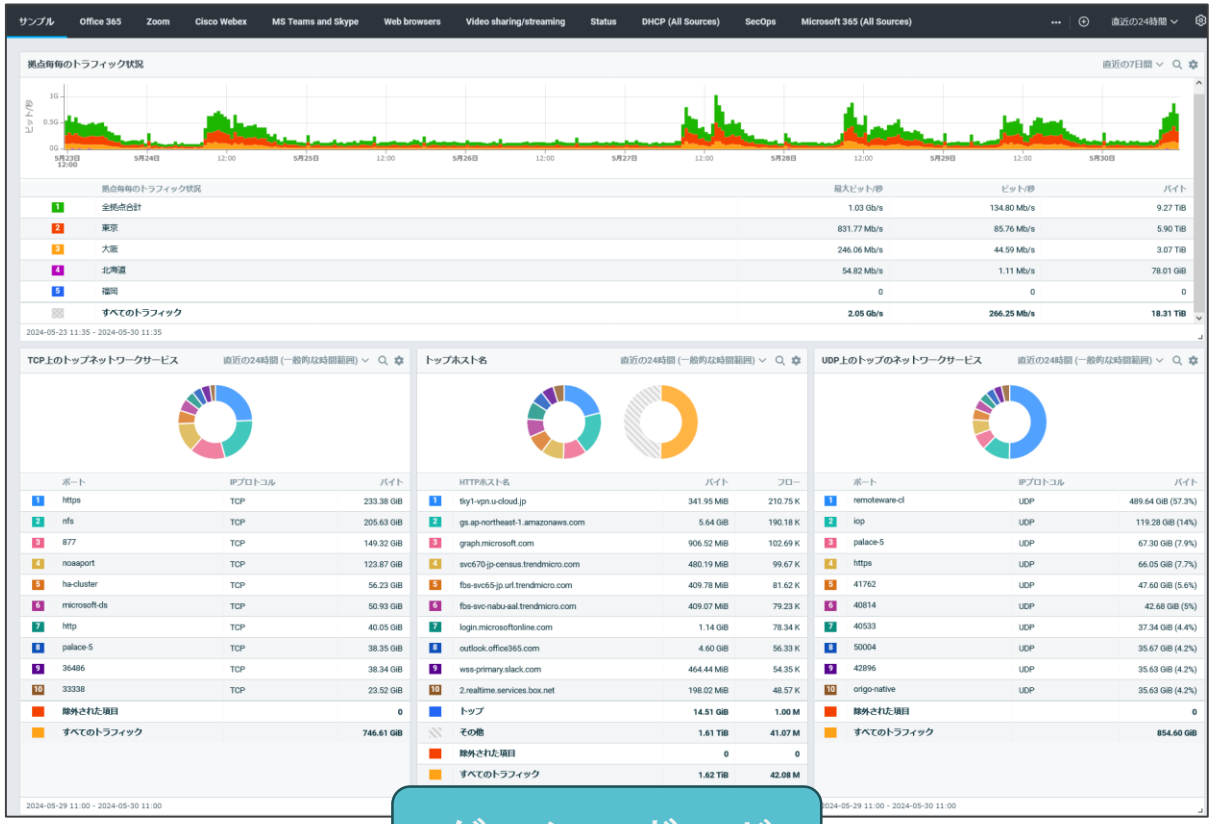
Progress Flowmon

Flowmon画面イメージ②

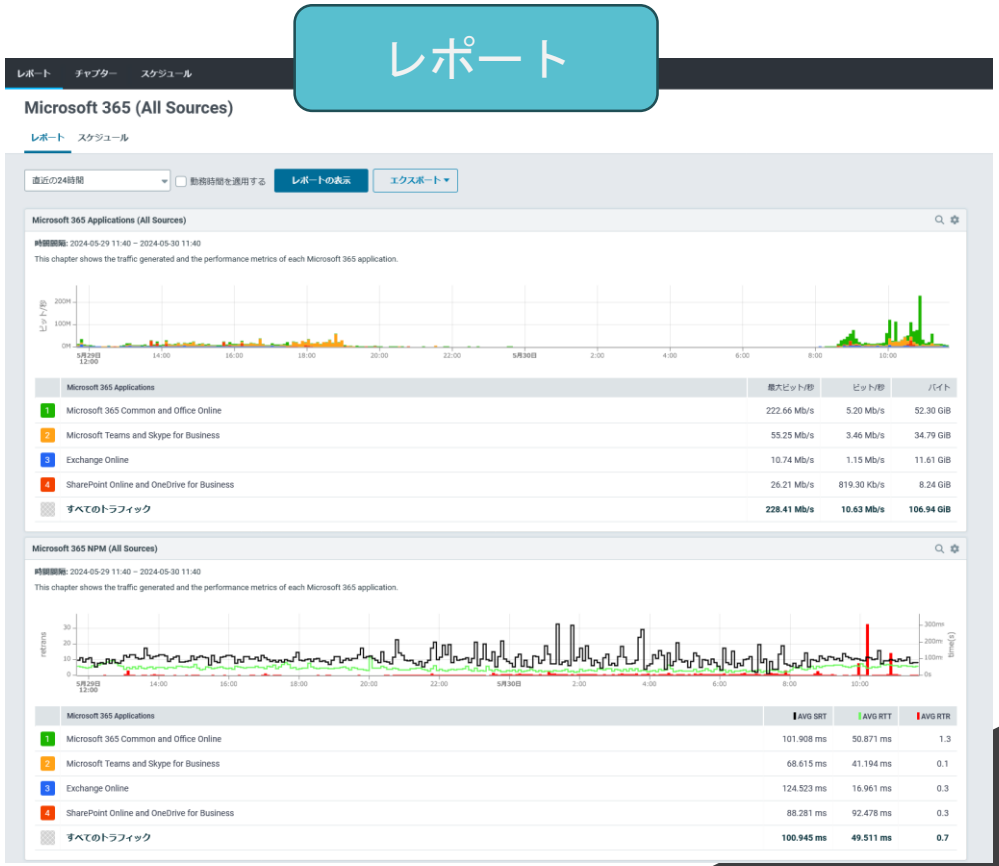


ORIZON

Flowmon画面イメージ③



ダッシュボード

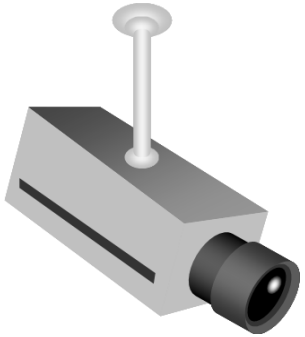


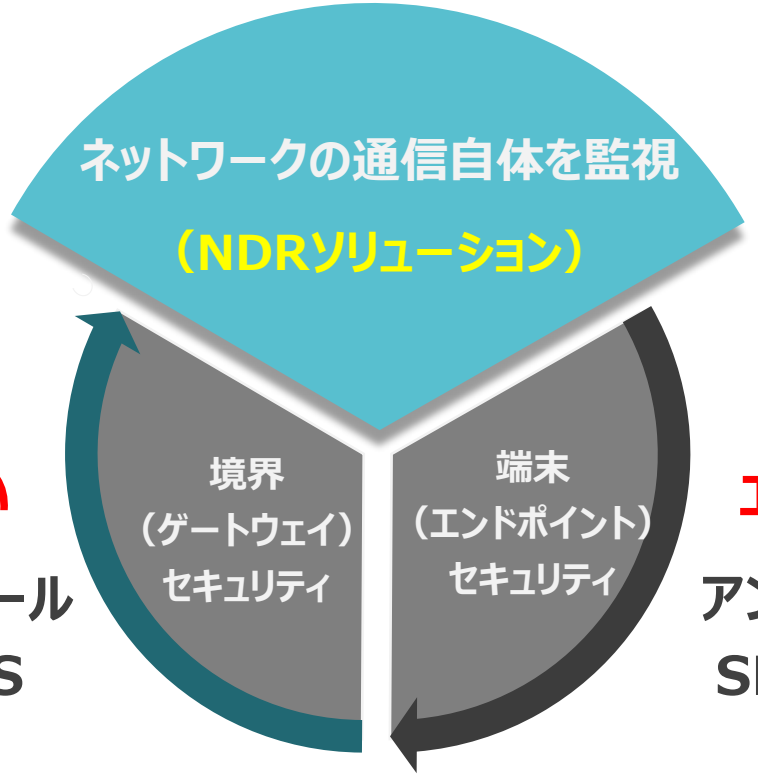
レポート

Progress Flowmon

FlowmonADSでセキュリティ強化

Flowmon ADSは「ネットワークの監視カメラ」がコンセプト





ゲートウェイで全て防ぐのは難しい

ファイアウォール
IDS/IPS

エンドポイント製品は管理が大変

アンチウイルス
SNMP監視

ADSはNDRソリューションとして、
ゲートウェイをすり抜けた脅威（標的型攻撃・マルウェア）への対策
ポリシー違反通信の監視・抑止・証跡管理が可能です

Flowmonでセキュリティ対策

多方面でのセキュリティの相互補完

- セキュリティ対策において完璧を望むことは厳しくなってきている
- 多方面から対策をし、 お互いに補完し合うことが非常に重要

振る舞い検知によるセキュリティ強化

- 悪意のあるマルウェアのほとんどは、パターンマッチングをすり抜けてしまう
- 振る舞い検知によるマルウェア検知強化が必要となっている

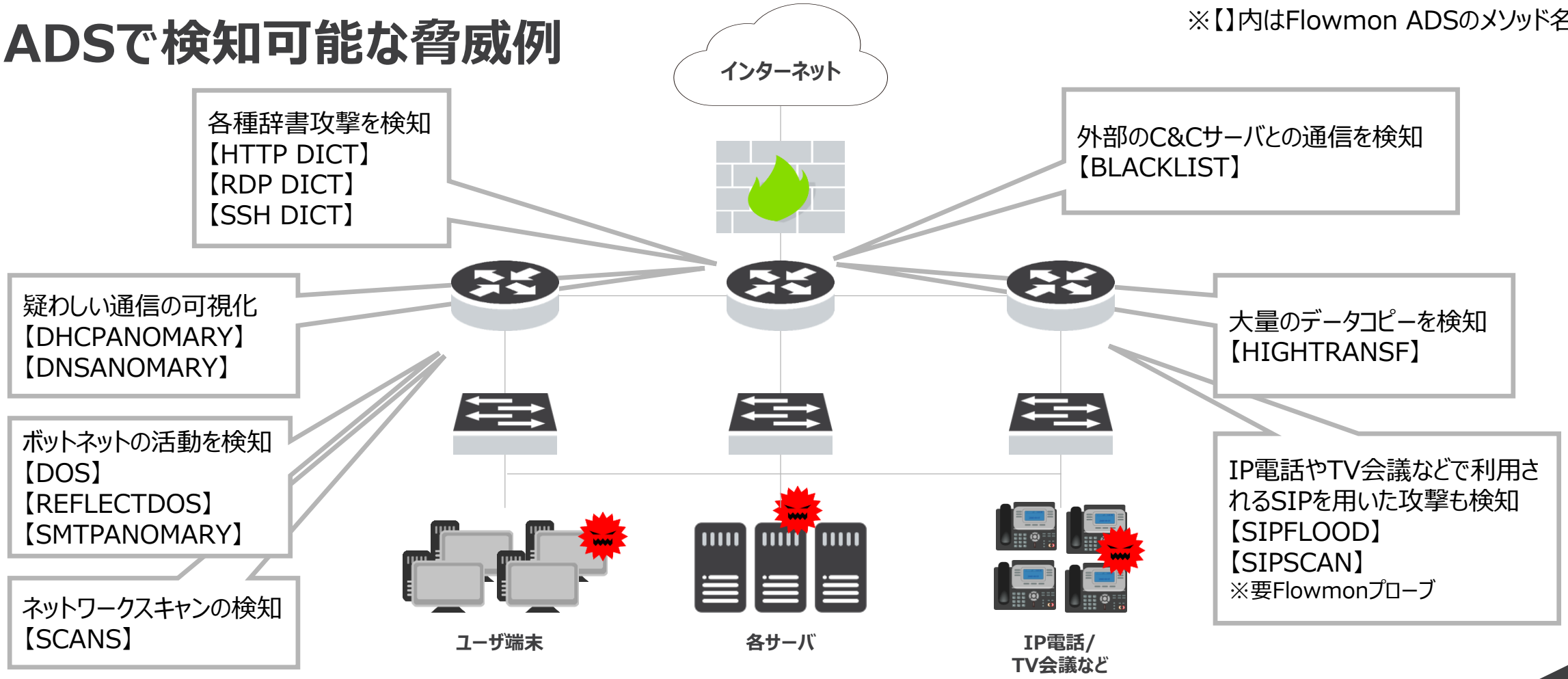
セキュリティ事故発生後の対策として

- Flowmonはネットワークの監視カメラ的役割を担うことができる
- 常に見られていることを意識することで規律を保ち、問題が発生した後の証跡確認としても有効

ORIZON

ADSで検知可能な脅威例

※【】内はFlowmon ADSのメソッド名



入口出口の境界セキュリティを**すり抜けた**脅威や、NW内に**潜む**脅威を
ネットワークフローを用いて監視・分析・検知します。

Progress Flowmon

従来型IPS比較なぜ振る舞い検知が注目されるのか

種別	ADS （Anomaly Detection System）	IPS （Intrusion Prevention System）
検知方法	振る舞いの変化	シグネチャ
既知の攻撃の検知	可	可
未知の攻撃の検知	可	不可
内部脅威の検知	可	不可
自動ブロック・遮断	不可	可
シグネチャの更新	頻繁な更新は不要	必要

＜Flowmon ADSの特徴＞　※ブラックリストについては約8時間ごとに更新をします

- 入口/出口（ゲートウェイ）だけでなく、内側（LAN内）の脅威も検知可能
- NW機器がNetFlowに対応していれば、1台で広範囲（複数拠点など）を監視可能
- 従来のFWやIDS/IPSで見つけられなかった脅威の検知

Flowmonの主な4つの機能

1

カスタマイズ自在なダッシュボード

拠点別トラフィック推移や、アプリケーション単位のトラフィック状況などお客様のご覧になりたい情報を１画面に表示します。

2

強力な解析機能

数クリックでの詳細な解析や、見慣れた構文でのフィルタ、出力項目も自由にカスタマイズ。

3

定期報告は自動作成レポートで

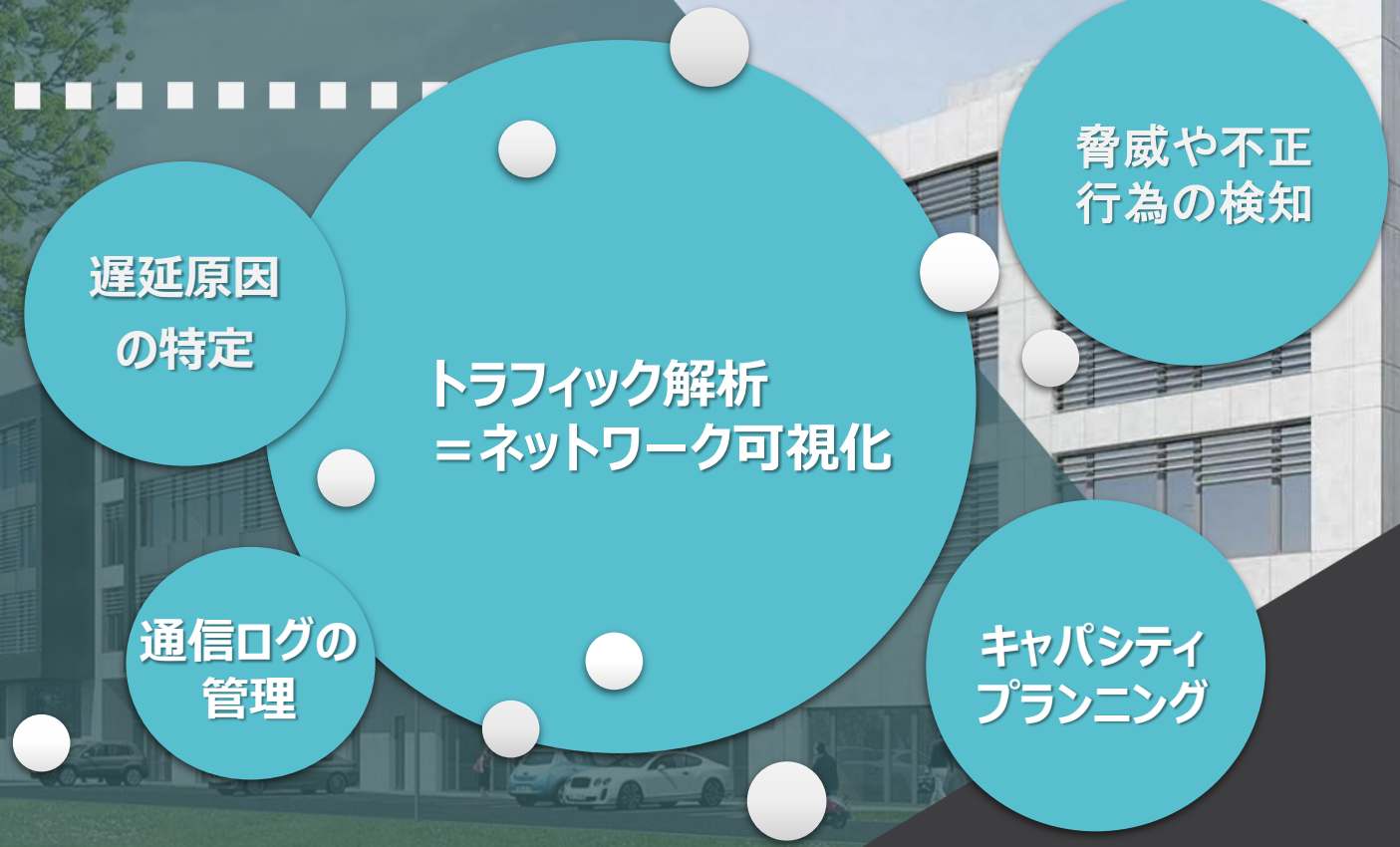
お客様のご覧になりたい情報を1日、1週間、１ヶ月単位のレポートを自動生成。メールやデータ出力も可能。

4

ふるまい検知機能

収集したFlow情報を利用しセキュリティ対策も行うことが可能。一目でLAN内の怪しいふるまいをしている端末を特定できる。

ご清聴ありがとうございました



ORIZON

Progress® Flowmon®