リスクアセスメント(可視化)の次は防御対策
～トレンドマイクロ OTセキュリティ製品のご紹介～

東京エレクトロン デバイス株式会社

2022年9月14日

EC BUクラウドIoTカンパニー
IIoTソリューション部

1. TEDのOTソリューション（対策編）
2. トレンドマイクロEdgeシリーズ紹介
3. D4IOT/Edgeの連携検証項目

工場セキュリティ対策の第一歩

まず何から手を付けるべきか！

- 工場内にどのような機器があるかわからない
- 生産活動への影響有無が不明なため判断がつかない
- 対策が多数あり、どこから手を付けていいかわからない

工場内部の把握

- 生産設備の確認
- ネットワーク構成の確認

工場の状態把握

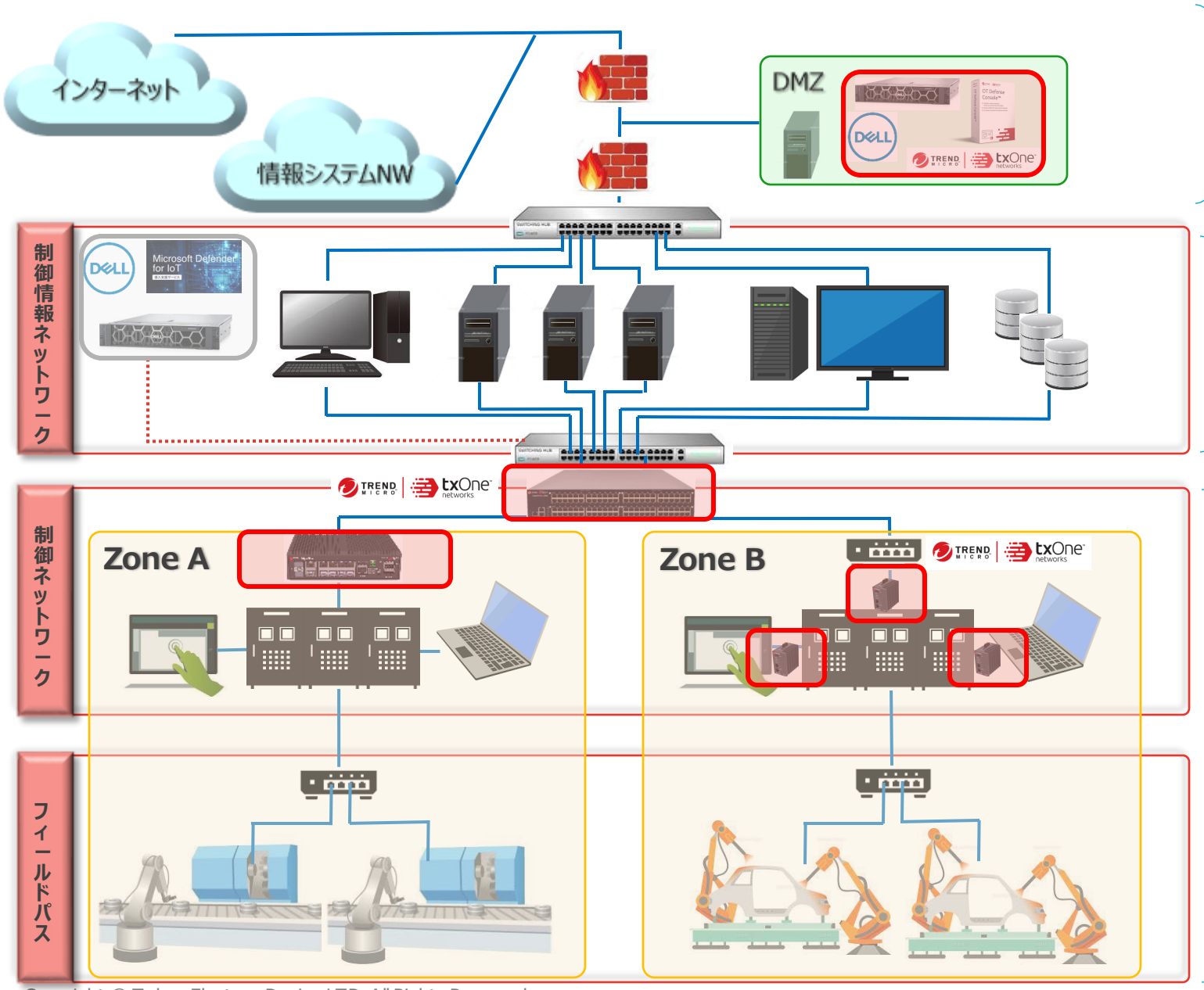
- 通信（脅威）の可視化
- 資産（設備）の可視化

該当設備の保護

- 脆弱な設備への対策
- 脅威の検知・防御

工場内設備の状況把握が重要！

TEDが提供するOTセキュリティ



IT/OTの境界防御

- **ファイアウォール/IPSベンダー**
  外部NWや情報システムからの脅威侵入防止

IT/OT混在領域

- **ネットワーク可視化ベンダー**
  生産現場と制御情報ネットワーク間のトラフィック監視
  資産（機器・設備）の可視化
  ネットワーク脅威の可視化

OT（生産現場）領域

- **OTセキュリティベンダー**
  生産に影響を与える通信や攻撃を防御
  ネットワークセグメンテーションにより内部感染の防止
  内部感染（USB・持込PC）による感染拡大防止
  重要端末（レガシーOSや対策ソフトのインストール不可）を保護

StellarProtect™
StellarEnforce™

Edgeシリーズ製品概要

EdgeIPS(次世代産業向けIPS)

簡単な導入・運用
- ✓ 透過型のため**既存設備のNW構成を変えることなく**導入可能
- ✓ **「監視モード」と「保護モード」**により段階を踏んだセキュリティの導入が可能
- ✓ **「小型サイズ」**で工場内の制御盤などへの設置が容易

幅広い産業プロトコル対応
- ✓ Modbus、SLMP、Ethernet I/Pなどのプロトコルに対応

重要資産の保護・可視化
- ✓ **FW/IPS/Protocol Filter/DoS Prevention**
  などにより重要資産を保護
- ✓ ZDIの脆弱性リサーチを活用した**仮想パッチを提供**
- ✓ 資産情報、利用されている**プロトコル情報の可視化**

産業用途のハードウェア設計
- ✓ 入力電源2重化対応
- ✓ 動作温度範囲：-40 to +75°C
- ✓ ハードウェアバイパスによるフェールセーフ

1:1接続

EdgeFire（次世代産業向けFire Wall ）

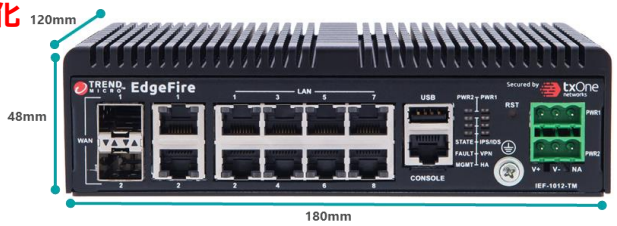
柔軟なネットワーク分離
- ✓ 生産ラインやセル単位でネットワークを分離し、 セキュリティ被害を局所化
- ✓ L3スイッチ（Gatewayモード）とL2スイッチ（**EdgeFire Bridgeモード**）搭載

幅広い産業プロトコル対応
- ✓ Modbus、SLMP、Ethernet I/Pなどのプロトコルに対応

重要資産の保護・可視化
- ✓ **FW/IPS/Protocol Filterなどにより重要資産を保護**
- ✓ ZDIの脆弱性リサーチを活用した**仮想パッチを提供**
- ✓ 資産情報、利用されている**プロトコル情報の可視化**

産業用途のハードウェア設計
- ✓ 入力電源2重化対応
- ✓ 動作温度範囲：-40 to +75°

1:8接続



EdgeIPS Pro
(大規模工場ネットワーク向け 次世代産業用IPS)

EdgeIPS Pro-1048（最大24ペア※）

EdgeIPS Pro-2096（最大48ペア※）

多ポートスイッチ対応の高性能・高可用性産業用IPS
- ✓ IT標準ラックマウント対応
- ✓ **IPSスループット**1048: **10Gbps** / 2096: **20Gbps**
- ✓ 同時接続数 1048: 2,000,000 / 2096: 4,000,000
- ✓ ハードウェアバイパスによるフェールセーフ
- ✓ 入力電源2重化対応

かんたん導入・運用
- ✓ 透過型IPSにより**既存NW設定を変えることなく導入可能**
- ✓ OT Defense Console(ODC)を利用した**統合管理・監視**

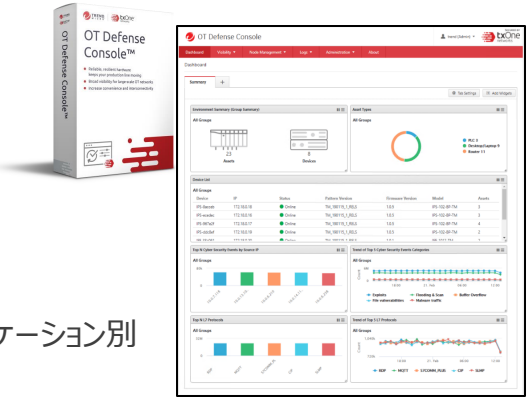
OT資産の保護・可視化
- ✓ **FW/IPS/Protocol FilterDoS Prevention**
  により重要資産を保護
- ✓ **世界トップの脆弱性発見コミュニティ(ZDI)の知見を活用**した
- ✓ 産業向けIPSフィルタの提供
- ✓ OT資産情報、利用OTプロトコル情報の可視化

OT Defense Console(ODC)
～集中管理コンソール～

集中管理による運用の効率化
- ✓ 工場毎に設置し、**EdgeFire、EdgeIPSなどのデバイスを一元管理**
- ✓ グループ設定による複数ポリシーを管理、適用
- ✓ IPSフィルタ（シグネチャファイル)を各デバイスへ配信

セキュリティイベントなどを見える化
- ✓ **検知/ブロックしたセキュリティイベントを集約**
- ✓ 管理下のデバイスが収集した資産の情報を可視化
- ✓ IT/OTプロトコル別総トラフィック量、各資産のアプリケーション別のトラフィック量をリアルタイム表示

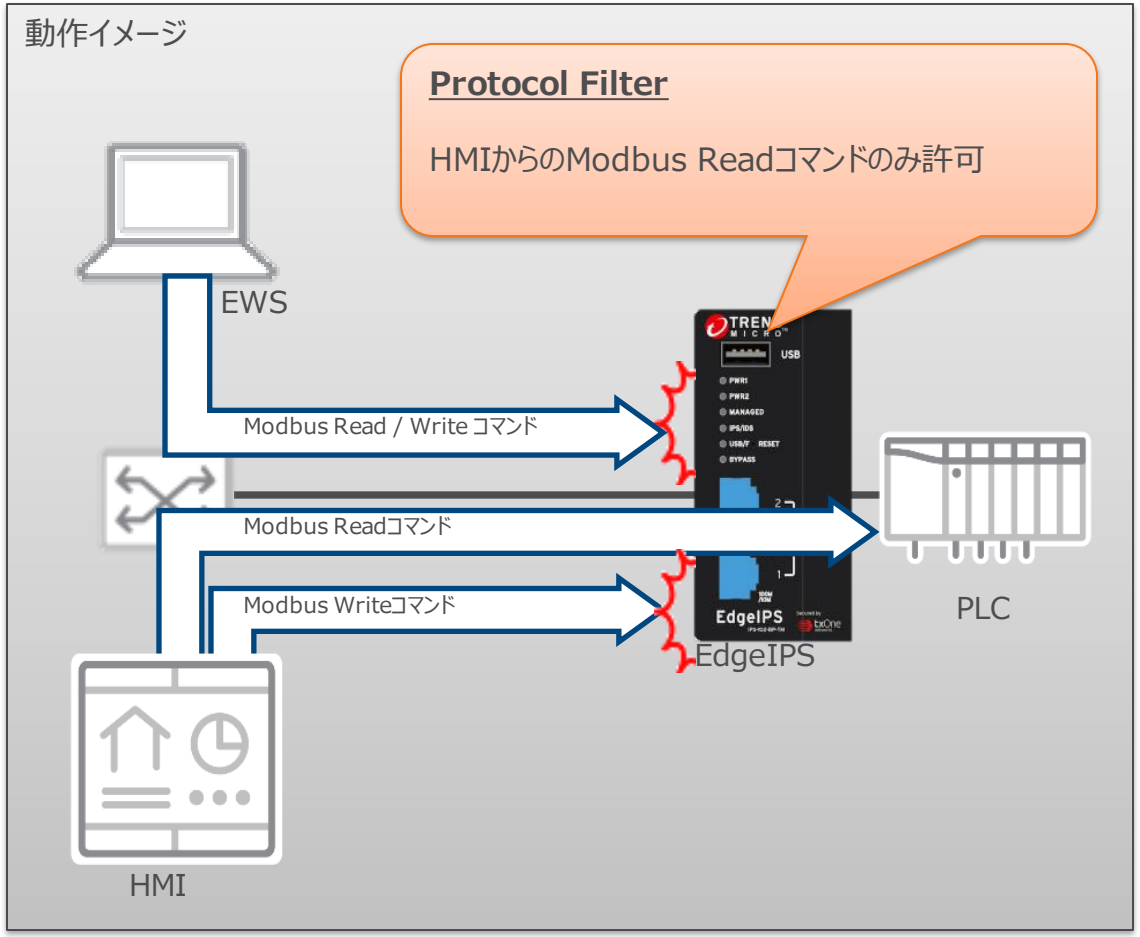
外部サーバ連携
- ✓ 設置済みの**SyslogサーバへSyslogを自動送信**

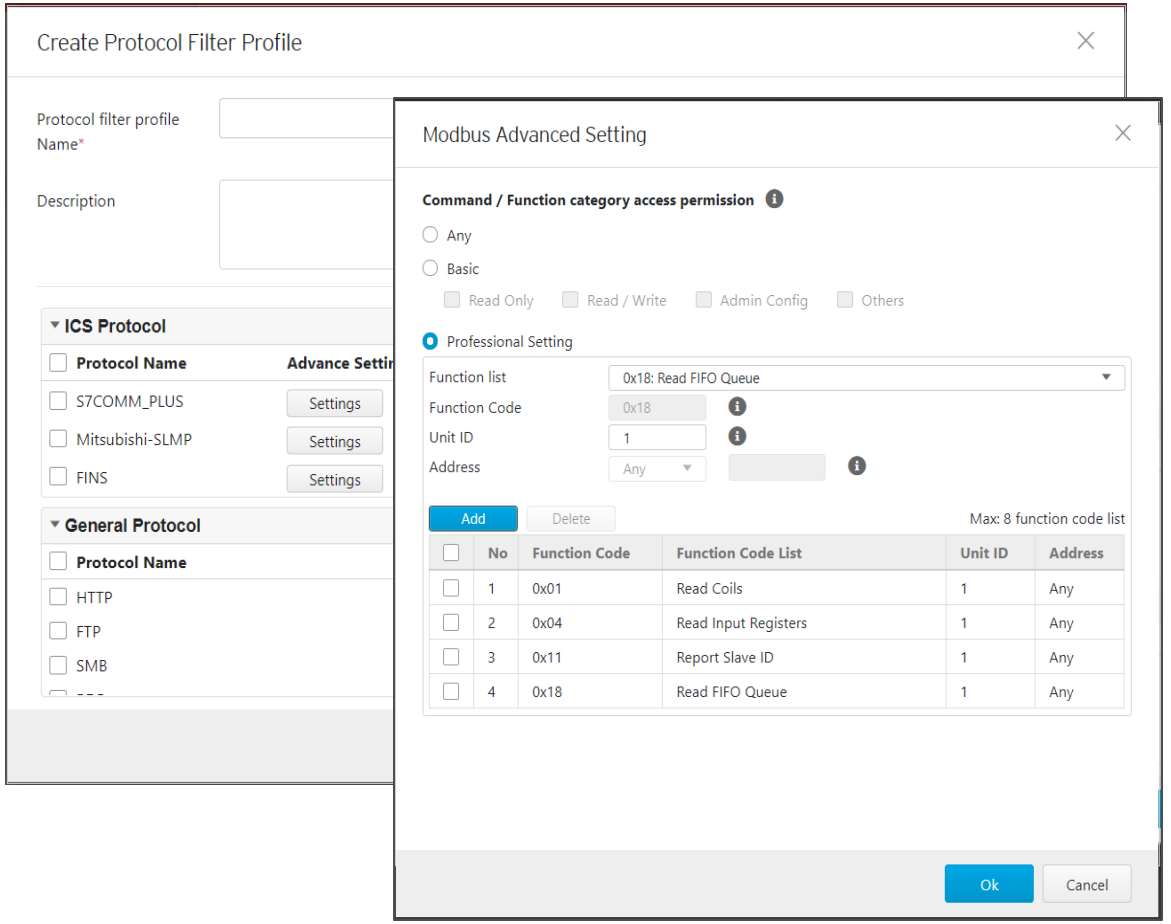


東京エレクトロン デバイス

Protocol Filter

EdgeIPS / EdgeFire / EdgeIPS Proを通過するOTプロトコル、実行コマンドの中身を解析し通信を制御することで、
誤 / 不正操作による誤動作や重要設備への不正なアクセスを防止し生産活動への影響を防止します。





東京エレクトロン デバイス

産業機器ベンダーとの協業（PLC/HMI/controller）

- 国内主要メーカと、EdgeIPSの評価を実施し、セキュリティ推奨品として展開
- EU様の工場に同メーカ製品が設置されていれば、基本評価不要！
- 随時、拡大中

https://www.trendmicro.com/ja_jp/business/products/iot/industrial-network-security.html

東京エレクトロン デバイス

EdgeIPS　導入イメージ

透過型のため、既存設備のネットワーク設定を変更することなく、セキュリティを強化

導入例:

① 重要設備前

- EdgeIPSにより重要設備への攻撃を防止

② L2SWのミラーポート

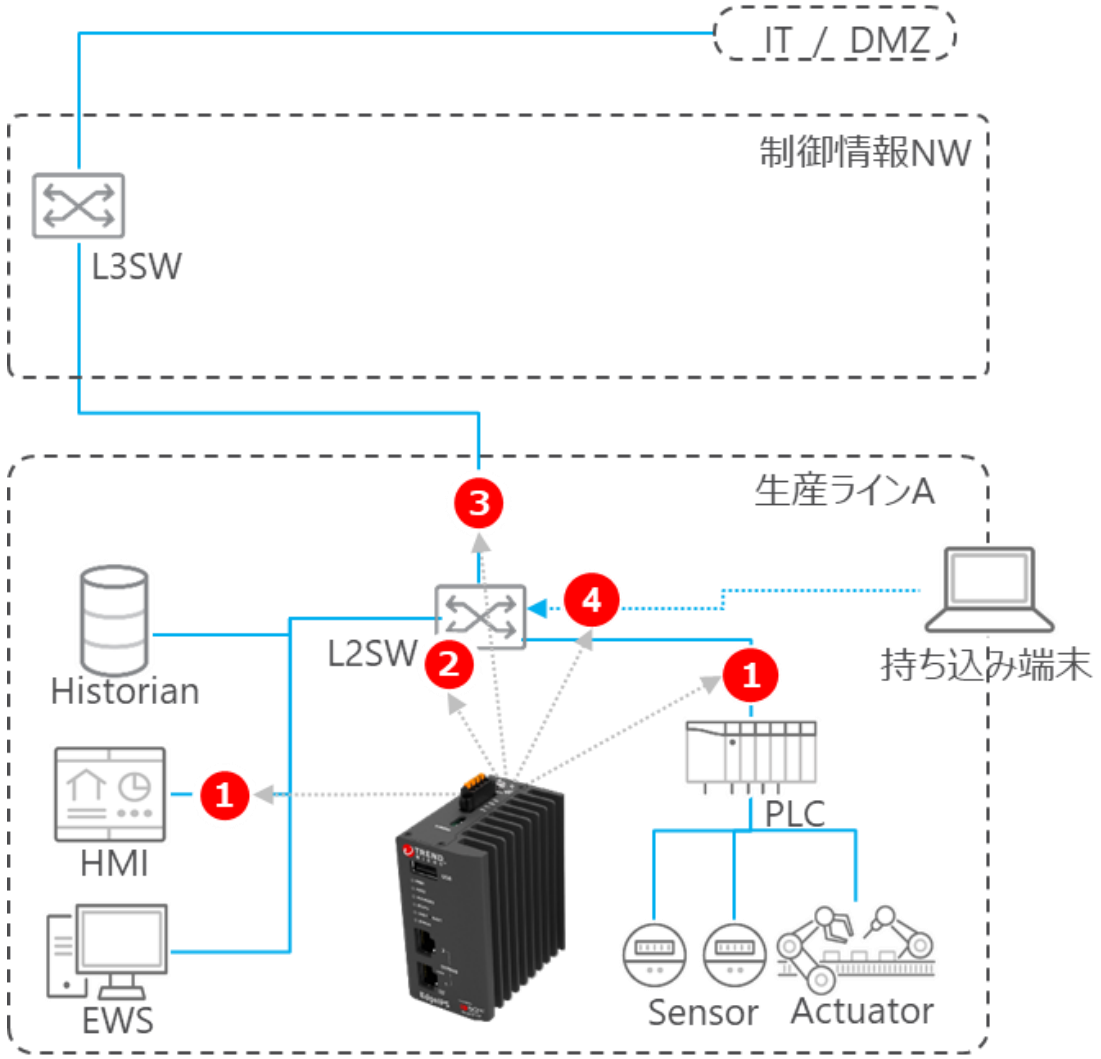
- L2SWを通過するパケットを検査

③ 生産ラインA-制御情報NW間

- 生産ラインA内外への攻撃を防止

④ 持ち持ち込み端末の接続先

- 持ち込み端末をEdgeIPSに接続し、持ち込み端末からの攻撃を防止



東京エレクトロン デバイス

EdgeFire 導入イメージ

生産ラインのゾーン化やL2スイッチとの置き換えによりセキュリティを強化が可能

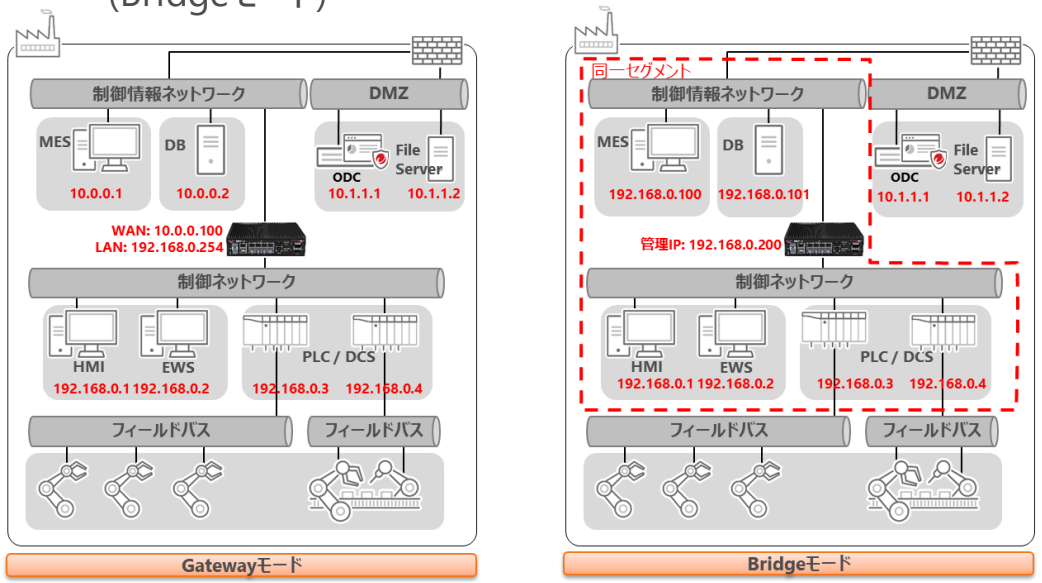
導入例:

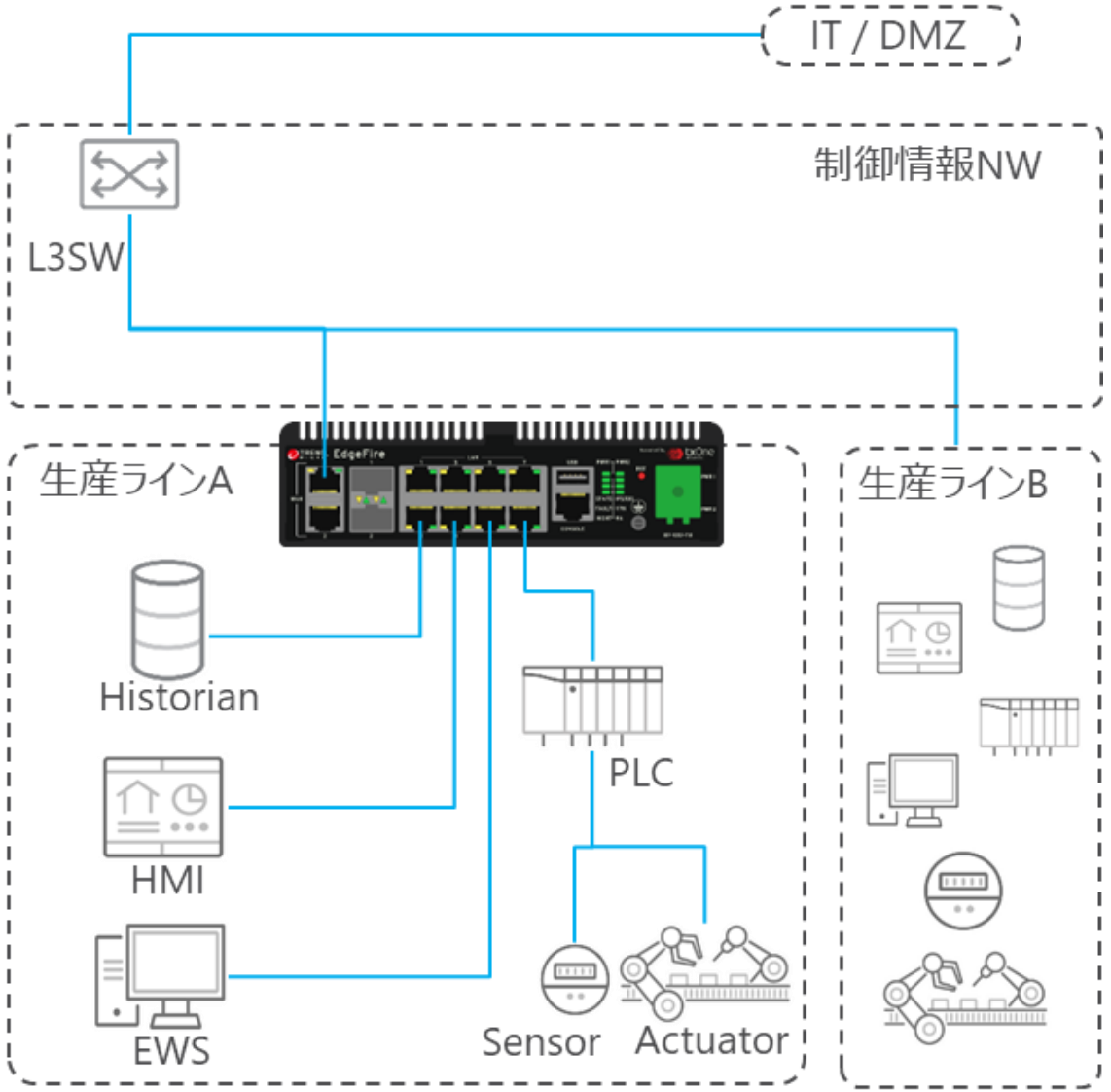
① **生産ラインA-制御情報NW間**

- EdgeFireにより生産ラインAを分離しセキュリティを強化 (Gatewayモード)

② **既設L2スイッチの置き換え**

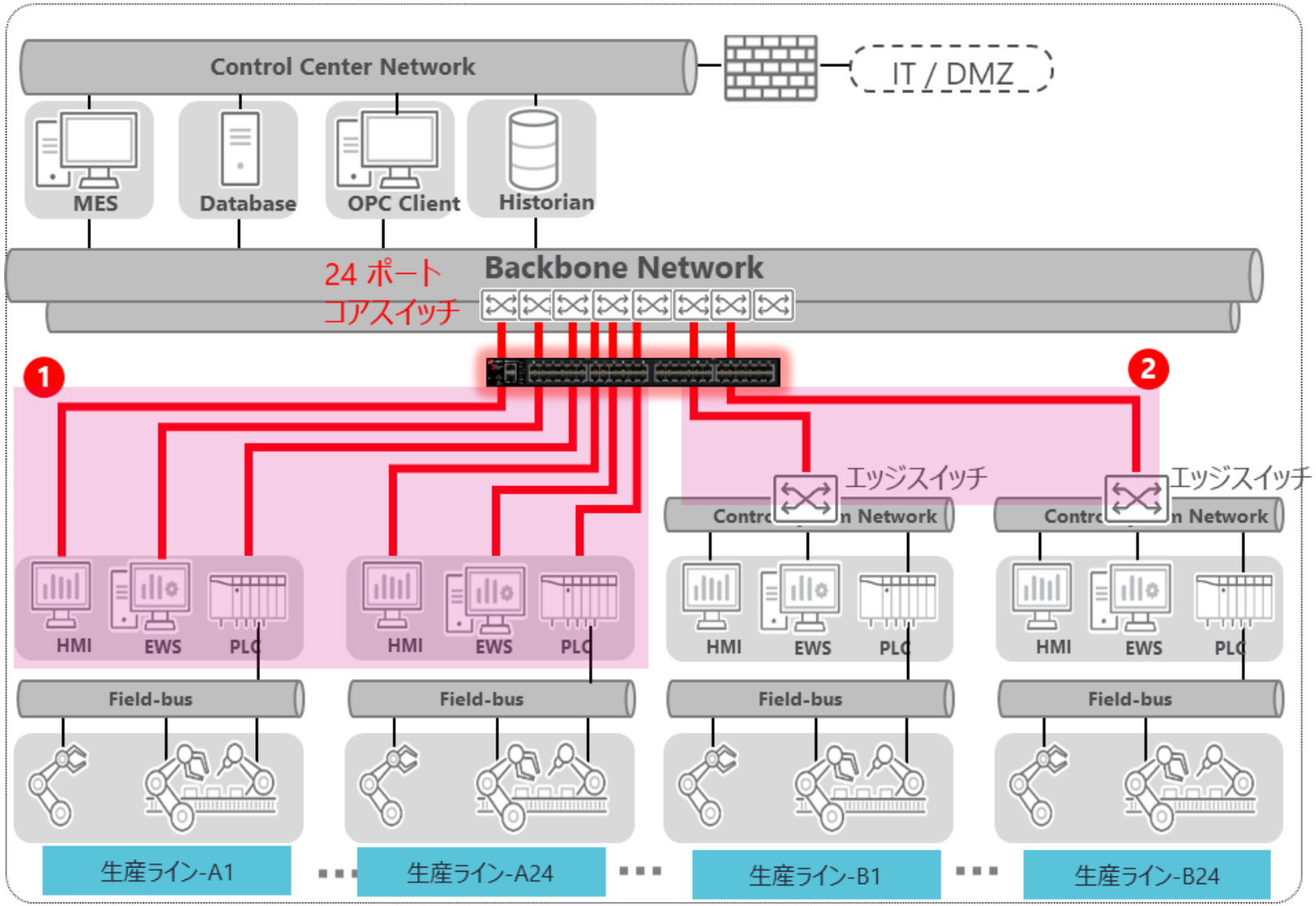
- 同一ネットワーク内にEdgeFireを導入しセキュリティを強化 (Bridgeモード)





東京エレクトロン デバイス

EdgeIPS Pro 導入イメージ



透過型のため、既存設備のネットワーク設定を変更することなく、セキュリティを強化

適用例:

① **コアスイッチ-エッジデバイス間**
- **生産ライン内の各デバイス間**での横感染防止

② **コアスイッチ-エッジスイッチ間**
- **生産ライン間**での横感染防止

* エッジスイッチ配下の横感染は防止できません。

OT Defense Console ～集中管理コンソール～

集中管理による運用の効率化

- 工場毎に設置し、**EdgeFire、EdgeIPSなどのデバイスを一元管理**
- **グループ設定**による複数ポリシーを管理、適用
- **IPSフィルタ（シグネチャファイル)を各デバイスへ配信**

セキュリティイベントなどを見える化

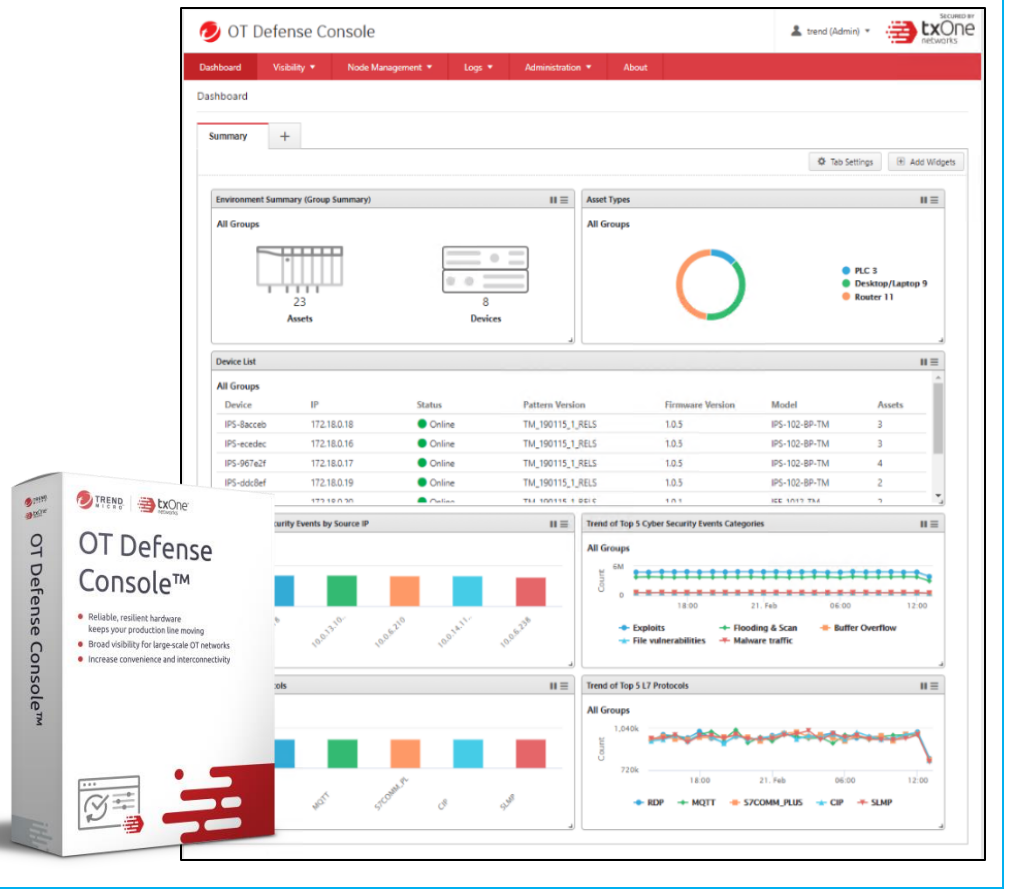
- 検知/ブロックした**セキュリティイベントを集約**
- 管理下のデバイスが収集した**資産の情報を可視化**
- **プロトコル別総トラフィック量、各資産のアプリケーション別のトラフィック量をリアルタイム表示**

外部サーバ連携

- **設置済みのSyslogサーバへSyslogを自動送信**
- 高負荷状態発生時など**SNMPサーバへTrapを送信**
- **TACACS+サポート**

製品

TREND MICRO



東京エレクトロン デバイス

D4IoT + EdgeIPS 簡易アセスメント検証

- マイクロソフト　D4IoT　可視化ソリューション
- トレンドマイクロ　EdgeIPS　IPS（検知･防御）

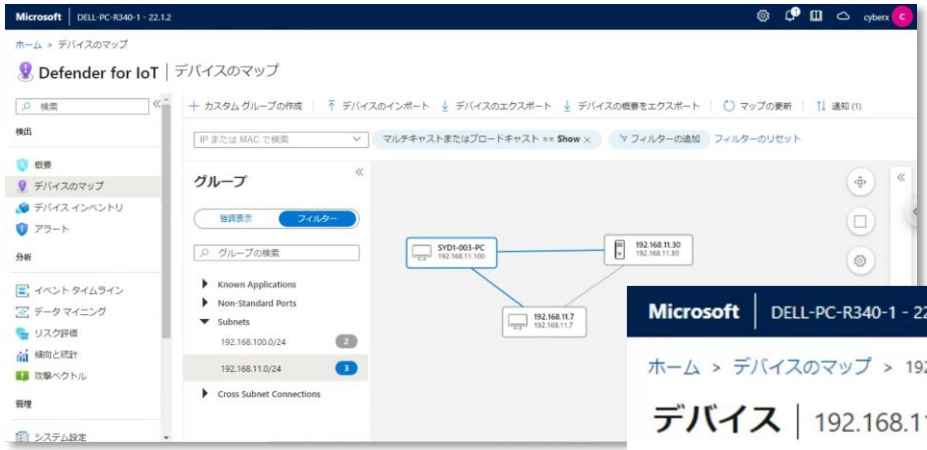
D4IoT + EdgeIPS 連携シナリオ

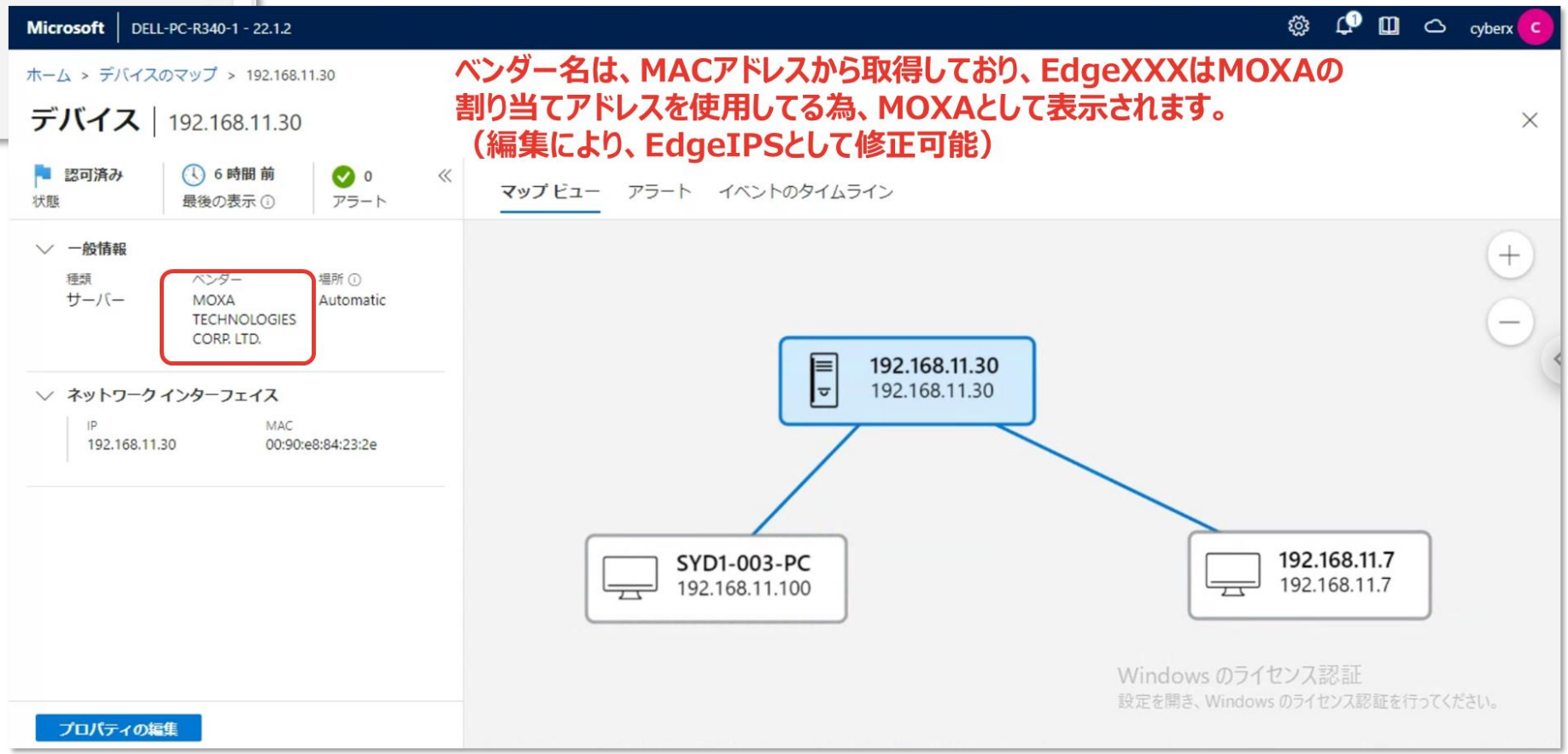
D4IoTで疑似攻撃（ICMP）の通信を検知

D4IoT検知結果を、EdgeIPSにルール追加し通信を遮断

通常通信(HTTP)は通信遮断せず、D4IoTで通信を可視化

D4IoT 192.168.11.0/24セグメントデバイスマップ



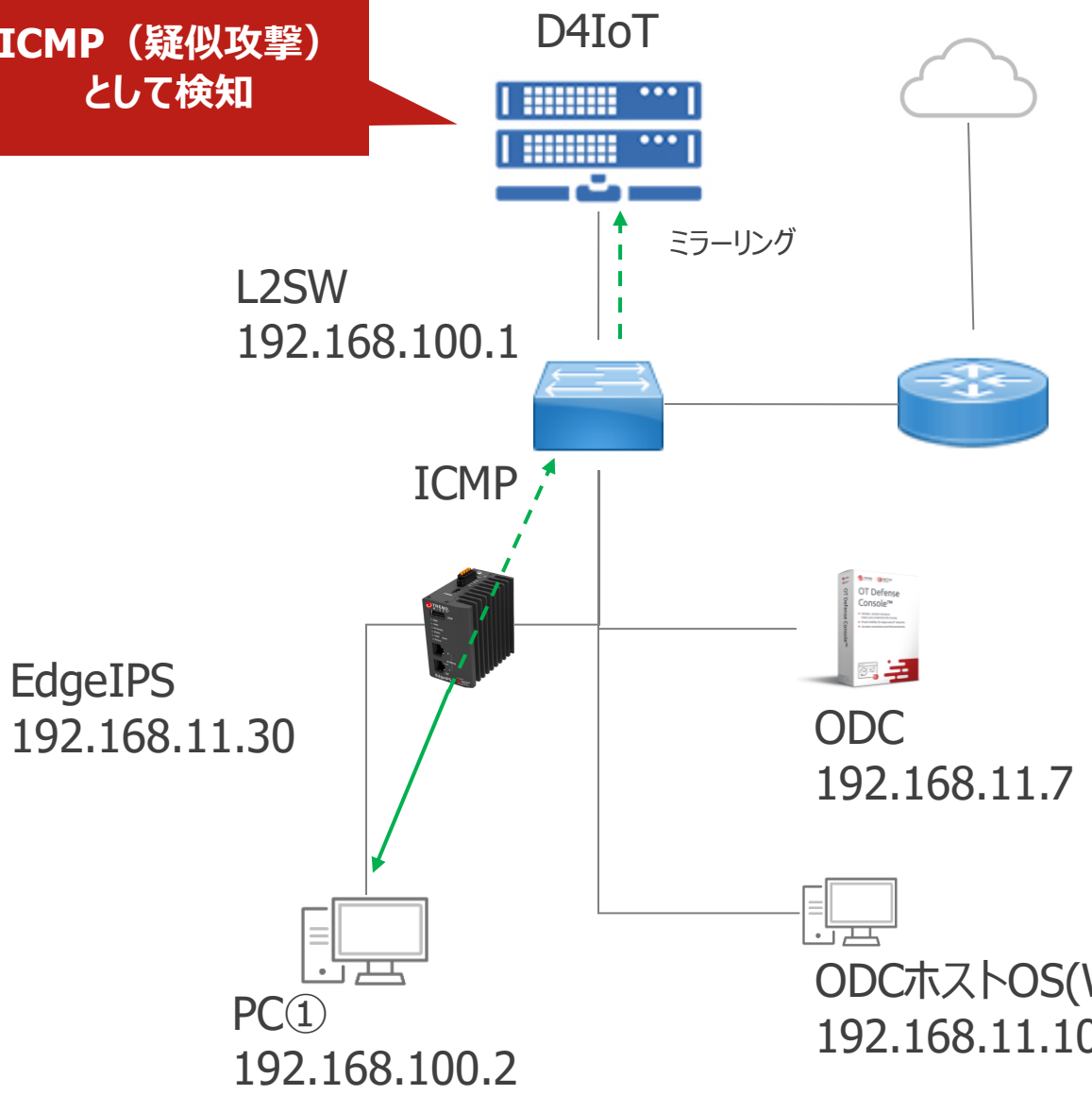


ベンダー名は、MACアドレスから取得しており、EdgeXXXはMOXAの割り当てアドレスを使用してる為、MOXAとして表示されます。（編集により、EdgeIPSとして修正可能）

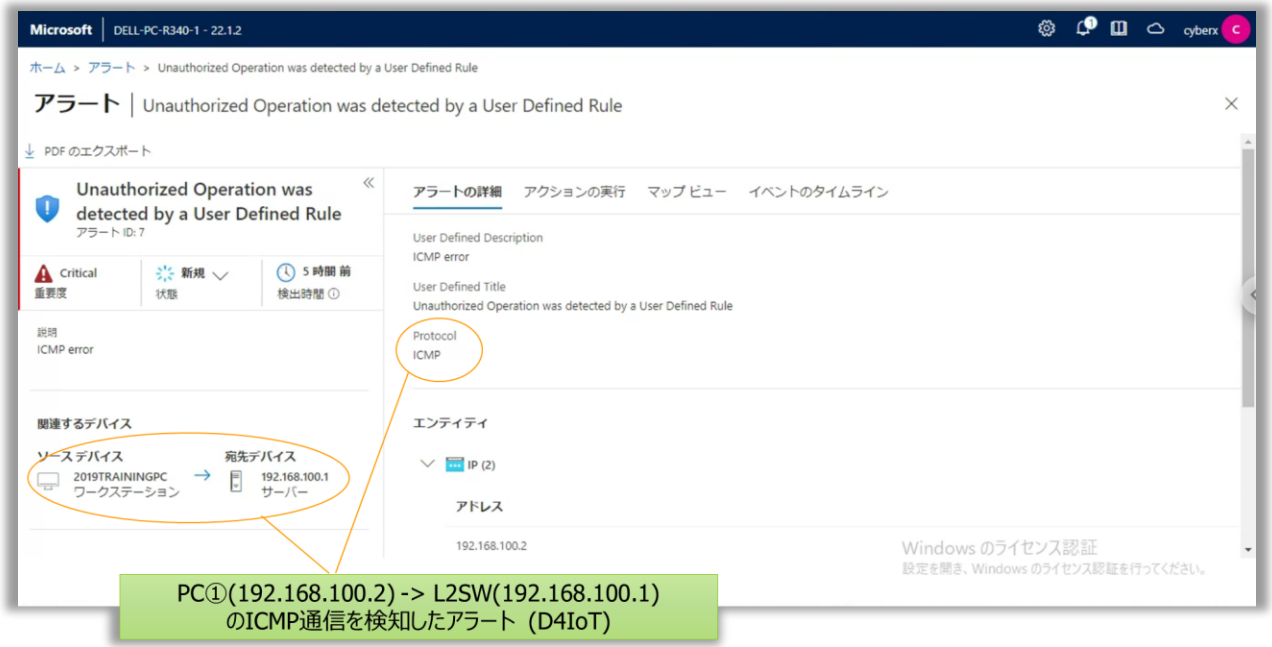
東京エレクトロン デバイス

検証内容：ICPM通信の検知

ICMP（疑似攻撃）として検知

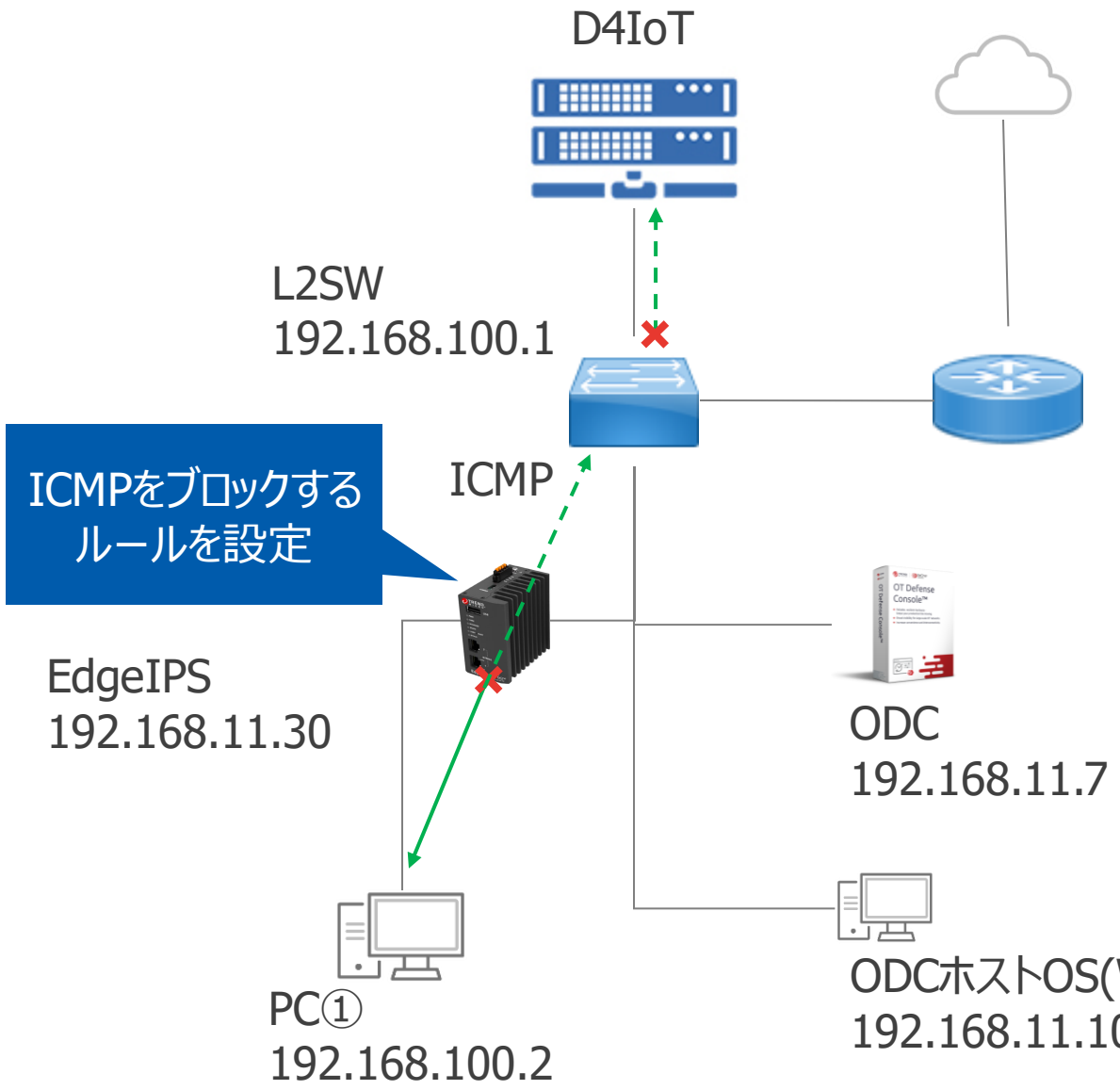


- PC①からL2SWへのICMP通信を実行
- D4IoTがPC①からのICMP通信（攻撃）を検知

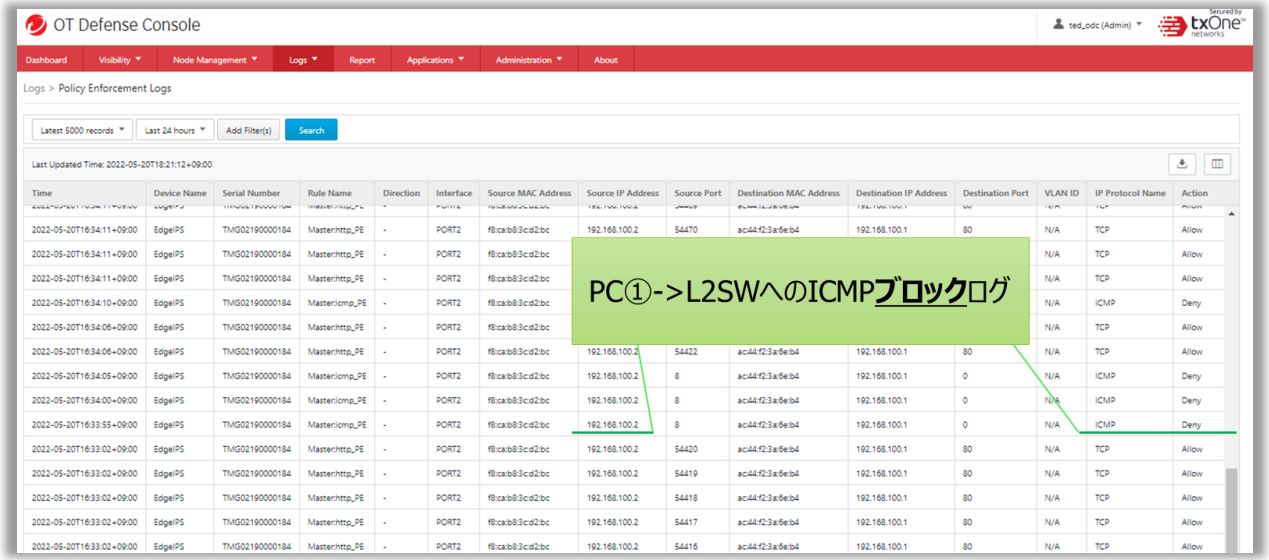


PC①(192.168.100.2) -> L2SW(192.168.100.1)
のICMP通信を検知したアラート（D4IoT）

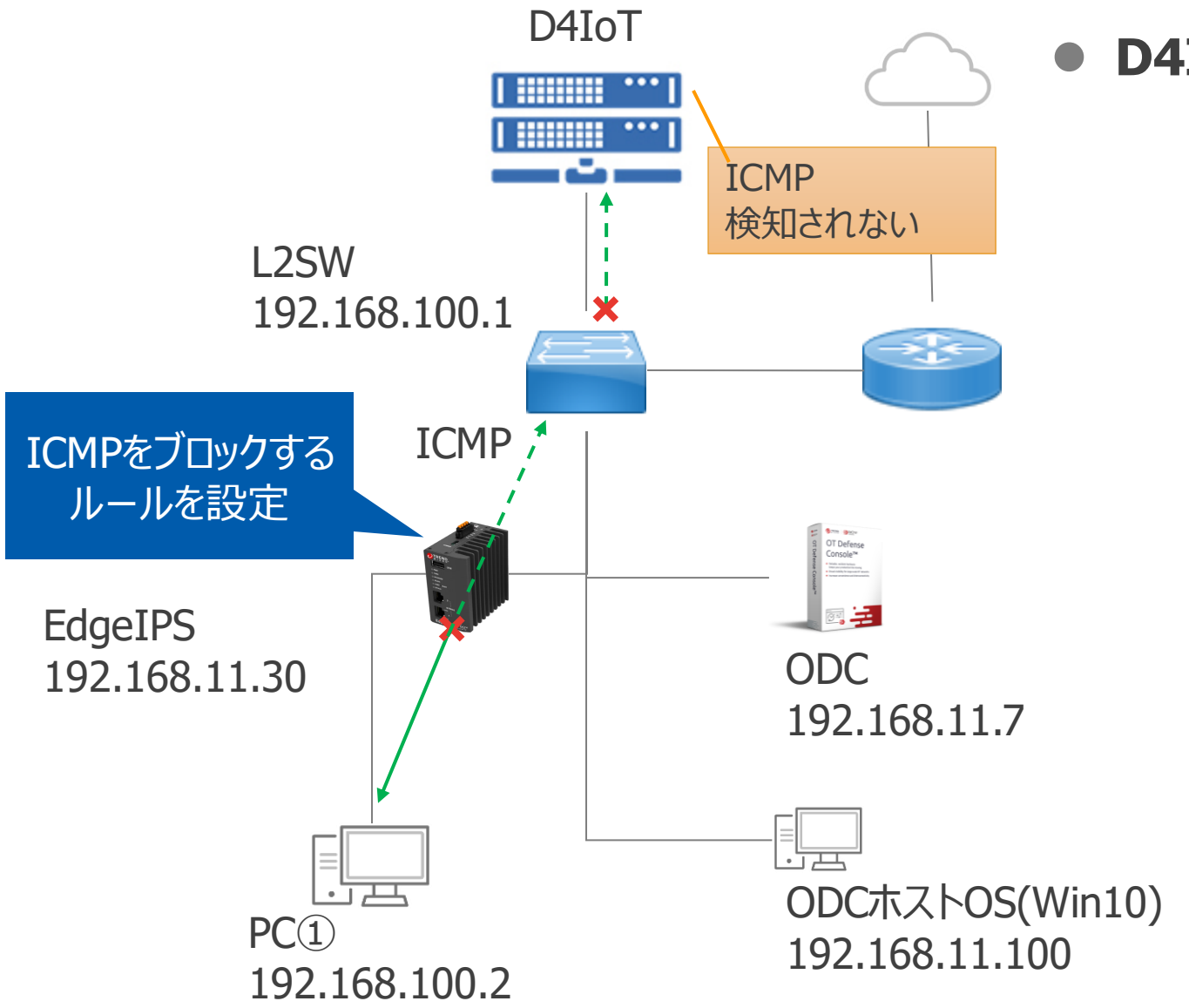
検証内容：ICPM通信の遮断



- EdgeIPSでICMP通信を遮断するルール設定
- EdgeIPSでICMP通信を遮断

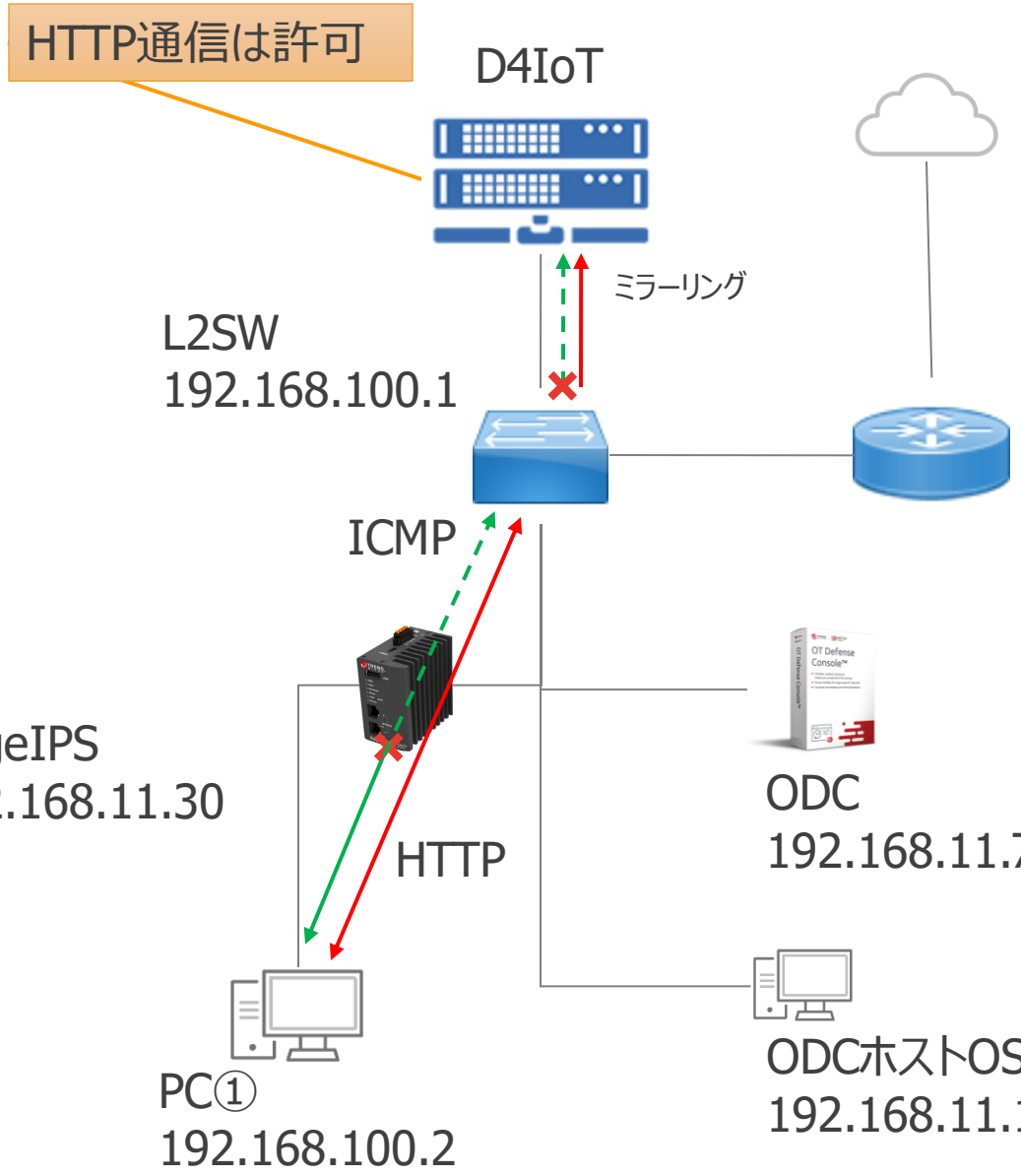


検証内容：ICPM通信の遮断

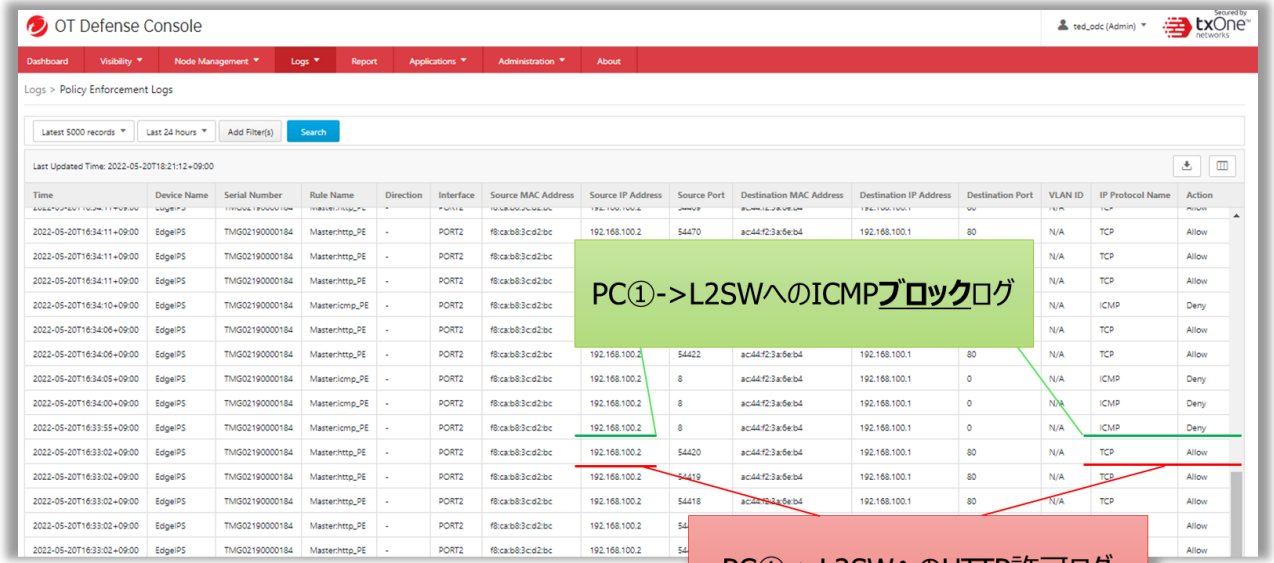


- **D4IoTでPC①からのICMP通信(攻撃)を非検知**

検証内容：ICPM通信の可視化



- 通常通信(HTTP)は、EdegIPSを通過
- D4IoTでも通常通信として通信の可視化を確認



ICMP通信をブロック
HTTP通信は許可

東京エレクトロン デバイス

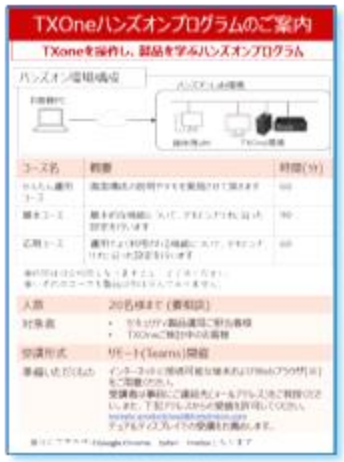
Edgeシリーズ　導入支援フロー

導入検討
お問合せ
→ 工場ネットワーク開示
（NDA締結可）
→ 工場セキュリティ提案
（松・竹・梅）
→ ハンズオントレーニング
PoC支援
→ 導入・運用
支援

お客様　　東京エレクトロンデバイス

● ハンズオントレーニング

PoC導入前(実環境でのPoCが難しい方)に、
操作方法などWeb会議形式で体験頂けます。



● PoC支援

1カ月の評価環境一式ご提供
技術サポート、フォロアップMTG（1回/2週間）

評価期間	：1か月
貸出機材	：EdgeIPS/Fire_1台分一式
貸出機材	：ODC用PC（※要相談）
ドキュメント	：PoC導入マニュアル提供
技術支援	：随時Q&A
進捗確認	：1回/2週間 フォロアップ会議
PoC構築	：設置支援（※要相談）

● 導入・運用

EdgeIPS/ODCの設置支援致します。
SoCご所望の場合は、パートナー様ご紹介可能

設置支援　：有償（要お見積り）
①標準プラン
　EdgeIPS/ODC初期設定、物理的な設置業務
②オプション
　セキュリティ設定（要各種パラメータシート提供）

運用支援　：SoCサービス
（パートナー様ご紹介）
Secureworks

Edgeシリーズ　導入支援フロー

導入検討
お問合せ

工場ネットワーク開示
（NDA締結可）

工場セキュリティ提案
（松・竹・梅）

ハンズオントレーニング
PoC支援

導入・運用
支援

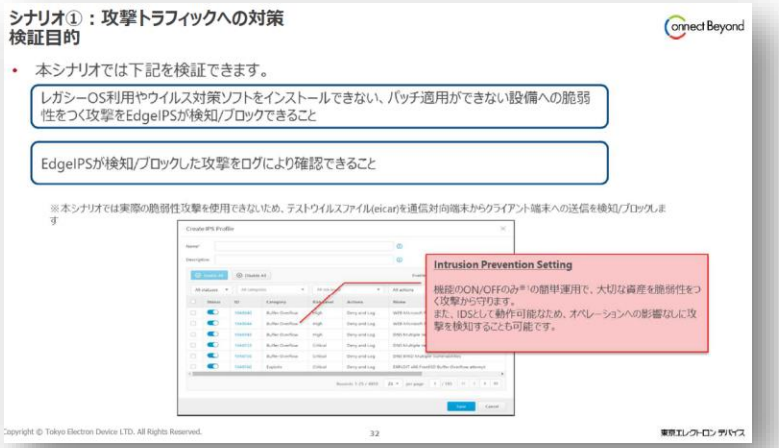
お客様

東京エレクトロンデバイス

- **PoC支援**

評価ガイド目次

1. EdgeIPS・ODCの検証準備
2. EdgeIPS・ODCの初期設定
3. 機能検証
   - シナリオ①：攻撃トラフィックへの対策
   - シナリオ②：DoS攻撃への対策
   - シナリオ③：ネットワークアクセス制御(Policy Enforcement)
   - シナリオ④：プロトコル制御（Protocol Filter）
   - シナリオ⑤：資産可視化
4. 運用検証
   - シナリオ⑥：自動ルール生成
   - シナリオ⑦：シグネチャファイル・ファームウェアの更新
   - シナリオ⑧：バックアップ/リストア



PoC期間中に、各種攻撃を検知するケースは稀となりますので、PoCの主目的は以下となります。
・インライン設置時の通信速度・レイテンシの確認
・セキュリティ機能の確認
・ODCを用いた運用確認

Edgeシリーズ/ODC ハードウェア設置・設定サービス

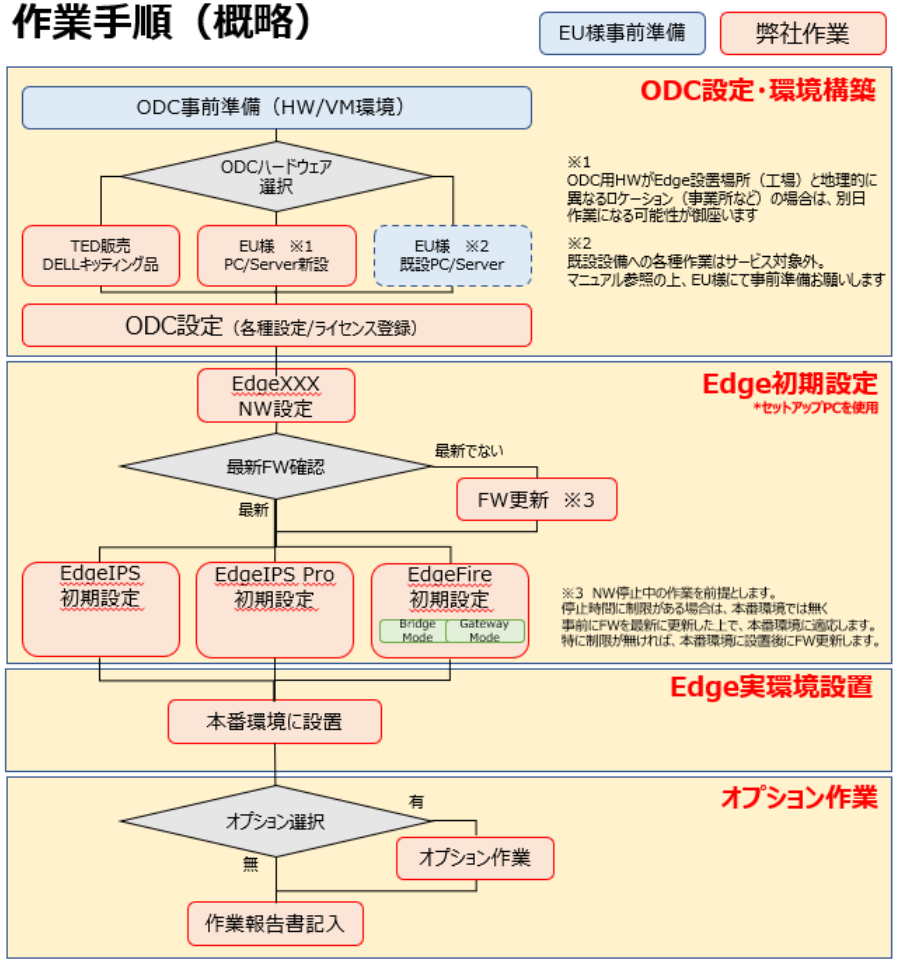
Connect Beyond

TREND MICRO | txOne networks

➢ 当社サービスエンジニアを派遣し、ご指定の導入場所で設置・接続及び起動を確認し
ラッキングや機器の設定を提供致します。
（※ネットワーク設計は含まず、事前に指定頂いた場所に機器を設置し、初期設定を行います。）

項	サービス名	プラン名称	サービス概要
1	機器設置サービス	スタンダード	・ODC構築準備/構築(※) ・Edge機器初期設定 ・Edge機器の設置及び動作確認 ・Edge機器のファームウェア更新
2	セキュリティ設定入力 （※要 パラメータシート記入・提供）	オプション	・グループ設定 ・アクセス権限設定 ・IPS機能設定 ・プロトコルフィルタ設定 ・Syslog転送設定 ・Email送信設定連携サーバ設定

作業手順（概略）



➢ サービス提供条件・事前準備

事前チェックシートにてご確認の上、事前情報及びユーザ様での準備をお願い致します。
パラメータシートに、必要事項をご記入の上、作業1週間前迄にご提供下さい。

Edge設置業務_事前チェックシート

EdgeFireパラメータシート

EdgeIPSパラメータシート

ODCパラメータシート

EdgeIPS Proパラメータシート

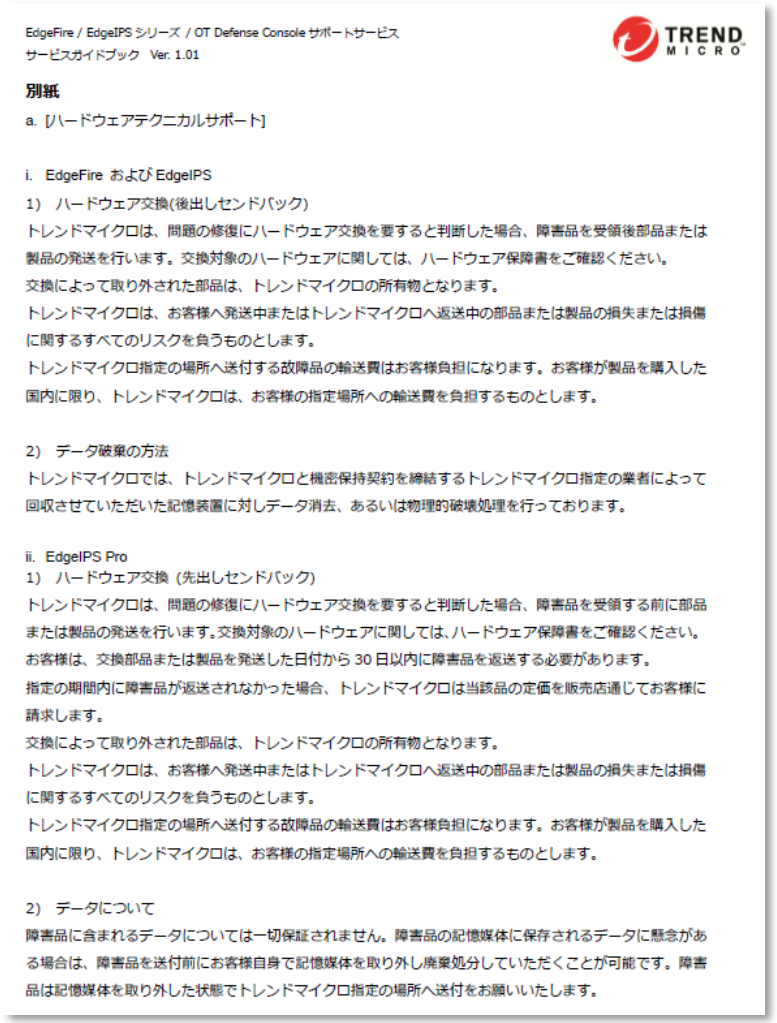
東京エレクトロン デバイス

ハードウェアサポート（障害調査・交換）


Trend Micro
EdgeFire
EdgeIPS シリーズ
OT Defense Console
サポートサービス

サービスガイドブック

トレンドマイクロ株式会社


EdgeFire / EdgeIPS シリーズ / OT Defense Console サポートサービス
サービスガイドブック Ver. 1.01

別紙

a. [ハードウェアテクニカルサポート]

i. EdgeFire および EdgeIPS

1） ハードウェア交換(後出しセンドバック)

トレンドマイクロは、問題の修復にハードウェア交換を要すると判断した場合、障害品を受領後部品または製品の発送を行います。交換対象のハードウェアに関しては、ハードウェア保障書をご確認ください。

交換によって取り外された部品は、トレンドマイクロの所有物となります。

トレンドマイクロは、お客様へ発送中またはトレンドマイクロへ返送中の部品または製品の損失または損傷に関するすべてのリスクを負うものとします。

トレンドマイクロ指定の場所へ送付する故障品の輸送費はお客様負担になります。お客様が製品を購入した国内に限り、トレンドマイクロは、お客様の指定場所への輸送費を負担するものとします。

2） データ破棄の方法

トレンドマイクロでは、トレンドマイクロと機密保持契約を締結するトレンドマイクロ指定の業者によって回収させていただいた記憶装置に対しデータ消去、あるいは物理的破壊処理を行っております。

ii. EdgeIPS Pro

1） ハードウェア交換（先出しセンドバック）

トレンドマイクロは、問題の修復にハードウェア交換を要すると判断した場合、障害品を受領する前に部品または製品の発送を行います。交換対象のハードウェアに関しては、ハードウェア保障書をご確認ください。

お客様は、交換部品または製品を発送した日付から 30 日以内に障害品を返送する必要があります。

指定の期間内に障害品が返送されなかった場合、トレンドマイクロは当該品の定価を販売店通じてお客様に請求します。

交換によって取り外された部品は、トレンドマイクロの所有物となります。

トレンドマイクロは、お客様へ発送中またはトレンドマイクロへ返送中の部品または製品の損失または損傷に関するすべてのリスクを負うものとします。

トレンドマイクロ指定の場所へ送付する故障品の輸送費はお客様負担になります。お客様が製品を購入した国内に限り、トレンドマイクロは、お客様の指定場所への輸送費を負担するものとします。

2） データについて

障害品に含まれるデータについては一切保証されません。障害品の記憶媒体に保存されるデータに懸念がある場合は、障害品を送付前にお客様自身で記憶媒体を取り外し廃棄処分していただくことが可能です。障害品は記憶媒体を取り外した状態でトレンドマイクロ指定の場所へ送付をお願いいたします。

- ➢ 後出しセンドバック
  - EdgeIPS
  - EdgeFire

- ➢ 先出しセンドバック
  - EdgeIPS Pro

※故障診断・切り分け

- お客様にて障害切り分け実施の上、指定の報告書にご記入下さい。
- トラブルシューティングガイドを参考に障害切り分けお願い致します。

RMA報告書_Ver3.1_TXOne

TXOneトラブルシューティングガイド_1.00

ご清聴ありがとうございました

Edgeシリーズ：セキュリティ/可視化機能一覧

機能	概要	備考
IPS	✓ EdgeXXXを通過するパケットの内容をチェックし脆弱性をつく攻撃を検知、ブロック。	脆弱性攻撃の検知/ ブロックはトレンドマイクロから配信されるシグネチャファイルに登録されているルールとマッチした攻撃を検知/ ブロックします。すべての攻撃をブロックできるわけではありません。
DoS Prevention	✓ EdgeXXXを通過するパケットの内容をチェックし、5秒間の間に指定した各挙動のしきい値超えた場合検知/ブロック。	IPSでは防げないTCP SYNflood攻撃などを検知/ ブロック 検知時間(5秒間) は変更不可
Protocol Filter	✓ EdgeXXXを通過するパケットの中身をチェックし指定されたOTプロトコル/ ITプロトコルへルールを設定。	設定したProtocolFilterはPolicyEnforcementを利用しEdgeデバイスに適用します。 誤操作など意図しない設定変更コマンドの送信を検知、ブロック
File Filter	✓ HTTP / FTP /SMBを利用しダウンロード/ アップロードされる実行ファイルやActiveDirectlyのGPOを利用し配布される実行ファイルを制御。	EdgeIPSPro v1.1のみ。
Policy Enforcement	✓ IPアドレス、ポートに基づいた通信の制御を。 ✓ ProtocolFilter / File Filterにて指定したルールを適用。 ✓ 設備ごとに異なるIPS Profileを適用。	PolicyEnforcementによる全トラフィックログとIPSログを同時に記録することはできません。
Suspicious Object	✓ DDIなどが検知した不正なデバイスや通信をブロック。	EdgeIPS v1.2のみ。
Asset Management	✓ EdgeXXXを通過するパケットを送信する資産の情報、通信アプリケーション一覧を表示。	

EdgeIPS/EdgeFire/EdgeIPS Pro比較

機能		EdgeIPS	EdgeFire	EdgeIPS Pro	機能概要
セキュリティ機能	IPS/IDS	○	○	○	OSや産業用アプリケーションなどの脆弱性攻撃を検知/ブロックします。
	DoS Prevention	○	○	○	TCP SYN FloodやICMP FloodなどDoS攻撃を検知/ブロックします。
	Policy Enforcement	○	○	○	IPアドレス, ポート番号ベースで通信制御を行います。
	Protocol Filter	○	○	○	産業用プロトコルのコマンドベースで通信制御を行うことで、不正アクセスや誤操作を検知/ブロックします。
	Asset Visibility	○	○	○	通過するパケットを検査することで、配下に存在する資産や利用されているプロトコルの情報などを可視化し、資産状況の把握を容易に行うことが可能です。
	検知/ブロックモードの切り替え	○	○	○	各種セキュリティ機能は動作モードを柔軟に切り替えることが可能なため、初期導入時の検証作業を容易にします。
マネジメント	Web Console	○	○	○	コマンドラインやWebコンソールを介して設定を行うことが可能です。
	集中管理	○	○	○	別製品であるOT Defense Console(ODC)を利用することで、管理下にあるEdgeFireを統合的に管理・監視し、運用性をさらに向上することが可能です。

EdgeIPS/EdgeFire/EdgeIPS Pro比較

機能		EdgeIPS	EdgeFire	EdgeIPS Pro	機能概要
NW機能	動作レイヤ	L2	L3	L2	EdgeFireはL3で動作し、ネットワーク分離とセキュリティを提供します。EdgeIPS/EdgeIPS ProはL2で動作しネットワーク変更無くセキュリティを提供します。
	ミラーポート接続 (TAP接続)	○	-	-	Switchなどのミラーポートに接続し、コピーされたパケットを検査することで、通信への影響を与えることなくセキュリティを提供します。
	NAT	-	○	-	静的/動的NAT、静的NAPTによるアドレス変換を行います。
	Portフォワーディング	-	○	-	指定したPortへのパケットをLAN側端末へ転送します。
	スループット	200Mbps	200Mbps	10Gbps/ 20Gbps	パケット処理可能なスループット。EdgeIPS Pro 1024は10Gbps、EdgeIPS Pro 2096は20Gbpsとなります。
HW	HWバイパス	○	-	○	機器故障時にバイパスが有効となり通信を確保します。
	Port数	2 (RJ-45)	WAN • 2 (SFP) • 2 (RJ-45) LAN • 8 (RJ-45)	1048 (RJ-45) • 1 管理ポート • 48 データポート 2096 (RJ-45) • 1 管理ポート • 96 データポート	
	動作温度	-40 ~ 75˚C	-40 ~ 75˚C	0 ～ 40 ˚C	