

実践OTセキュリティ対策 OTシステムの可視化と異常検知

株式会社 ソリトンシステムズ
サイバーセキュリティ事業部 鶴田亮

2022/09/14 v.001

- I. OT セキュリティ対策に重要な三要素
- II. Microsoft Defender for IoT
- III. SOC / CSIRT サービス「セキュリティ監視サービス for IoT/OT」

- 可視化
- 異常検知
- 防御



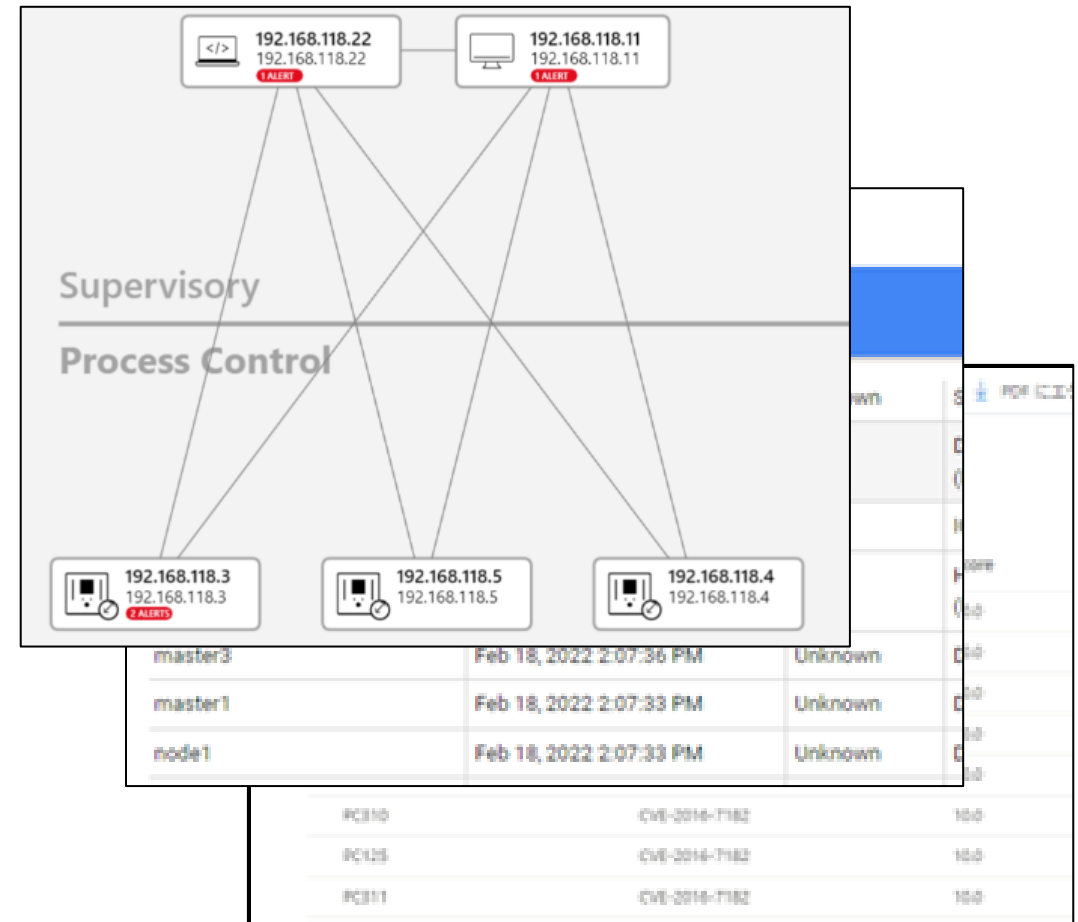
OT システムの例：
ロボットアームの作業セル

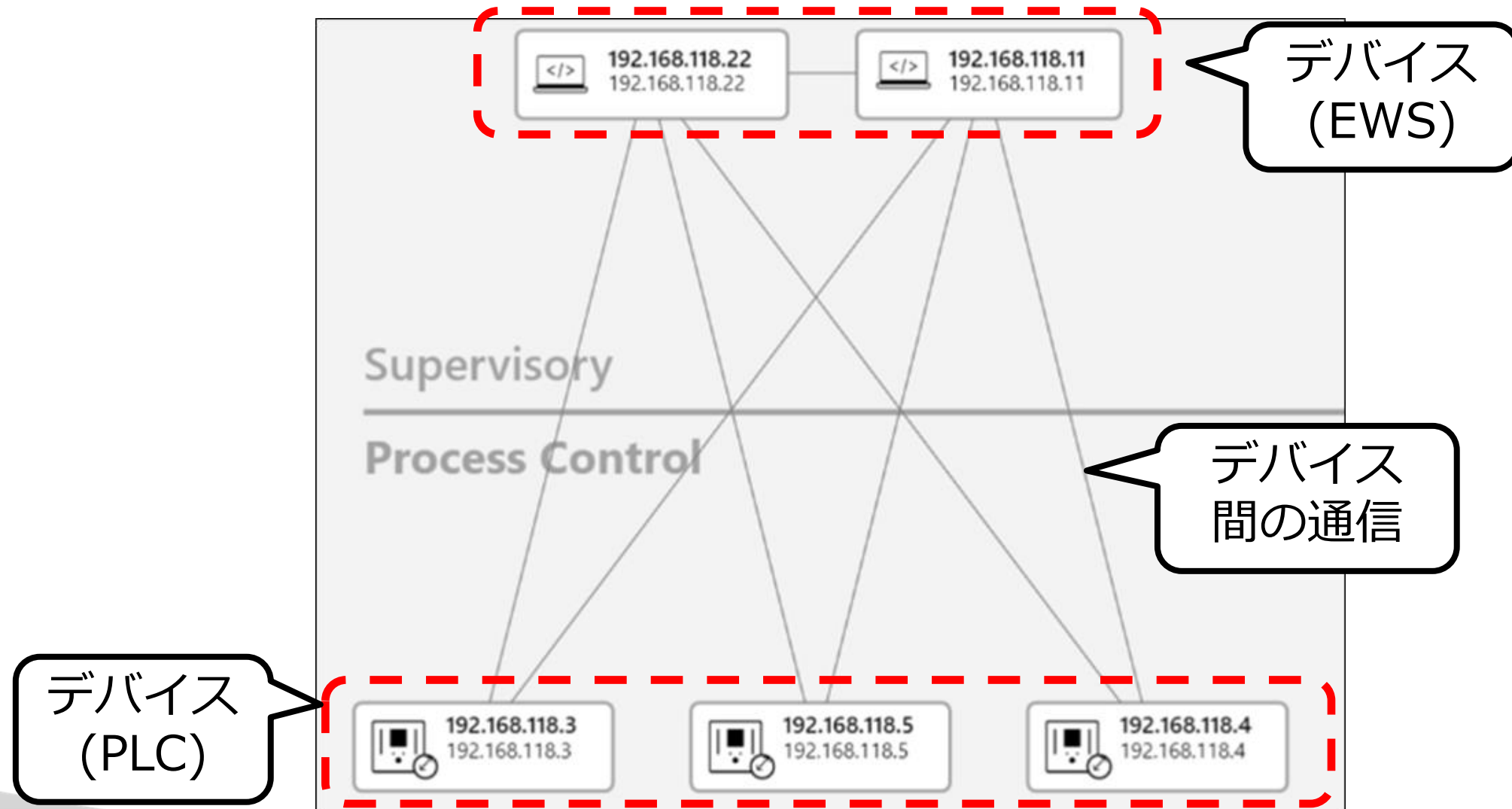
出典：NIST SP1800-10B
産業用制御システム環境における情報とシステムインテグリティの保護
製造業のためのサイバーセキュリティ

可視化



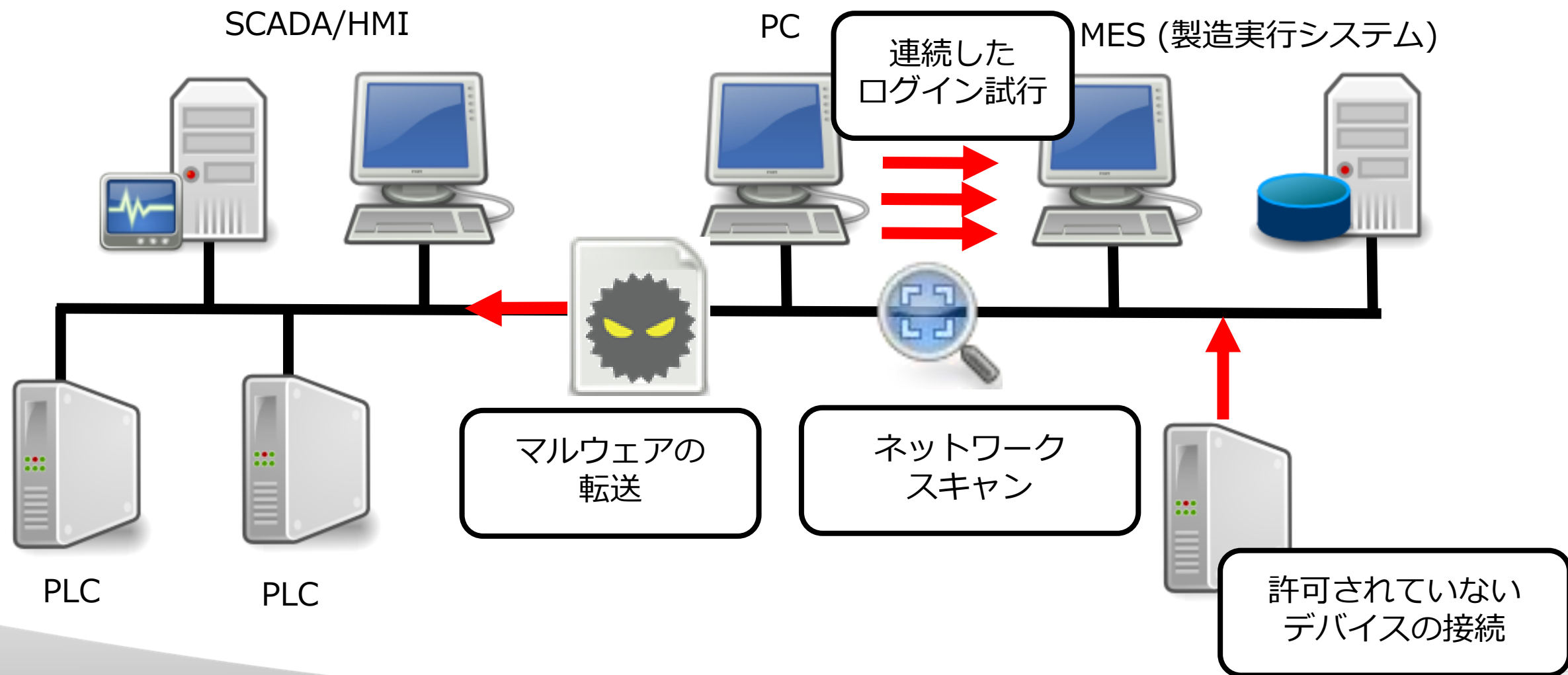
ネットワーク構成図



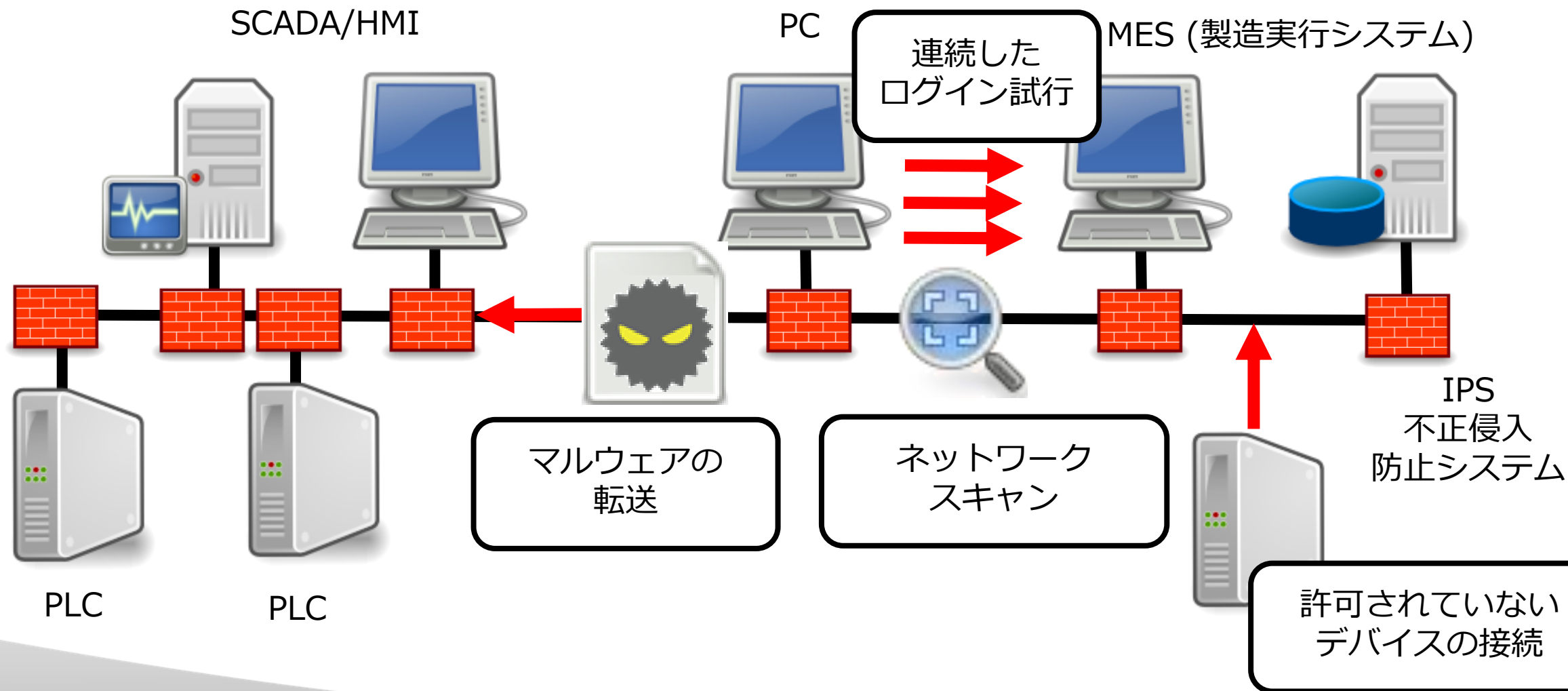


Device Inventory						
IPアドレス	最後に通信した時間	デバイスタイプ	通信プロトコル	デバイスベンダー		
IP Address	Last Activity	Type	Protocols	Vendor		
192.168.17.8	Aug 4, 2022 6:29:51 PM	PLC	ICMP, Netbios Datagram Service, SMB, Siemens SICAM	SAT GMBH & CO.		
192.168.18.22	Aug 4, 2022 6:29:50 PM	Engineering Station	Netbios Datagram Service, SMB, Siemens S7			
192.168.18.5	Aug 4, 2022 6:29:50 PM	PLC	Netbios Datagram Service, SMB, Siemens S7	SIEMENS AG		
192.168.18.4	Aug 4, 2022 6:29:50 PM	PLC	Netbios Datagram Service, Netbios Name Service, SMB, Siemens S7	SIEMENS AG		
192.168.23.10	Aug 4, 2022 6:29:49 PM	Engineering Station	Netbios Datagram Service, SMB, Siemens S7 Plus	VMWARE INC.		

OTネットワーク



OTネットワーク



可視化

システム構成や稼働状況を機械や人間が分析できる形にして明らかに

異常検知

システムを継続的に監視して、普段とは異なる動作を捉える

防御

不正な通信を遮断してサイバー攻撃からシステムやデータを保護する

三要素の実現で効果的な OT セキュリティ対策

- 概要
- システム構成
- 機能
 - 操作方法
 - 可視化
 - 異常検知
 - 他のセキュリティ製品との連携



製造業や重要インフラなど OT システム向けに作られた資産管理、脅威監視を行うセキュリティソリューション

システムの可視化、リスク分析

デバイス一覧やネットワークマップを自動作成。自動リスク分析機能により脆弱性やリスク緩和策を提示

異常検知

OT 対応の行動分析と脅威インテリジェンスにより異常を検知

他のセキュリティ製品との連携

SIEM、SOAR、ファイアウォール、IDS/IPS など様々なベンダーのセキュリティ製品と連携

Defender for IoT

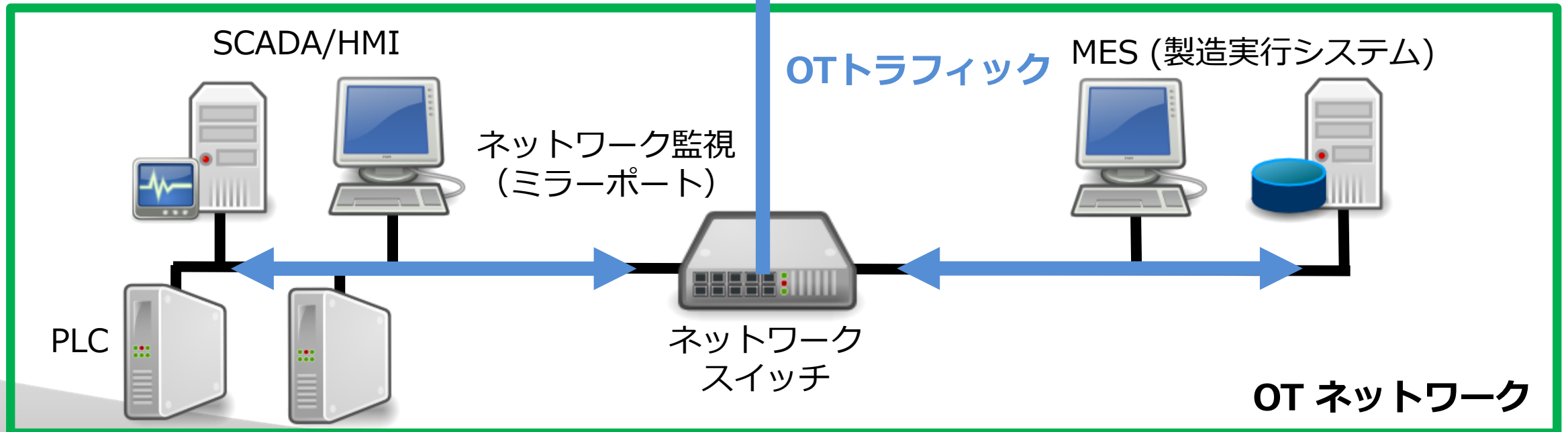
センサー

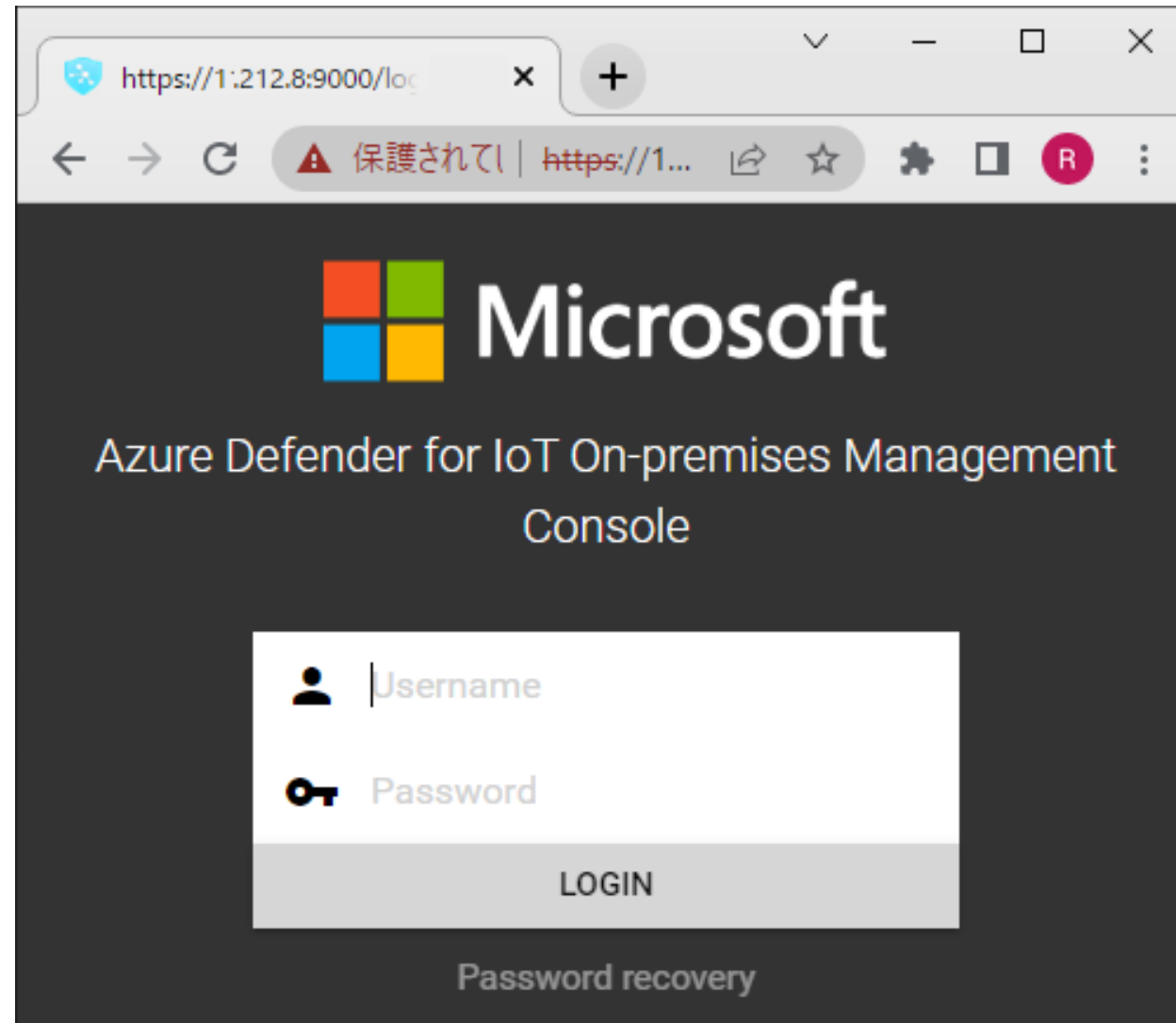


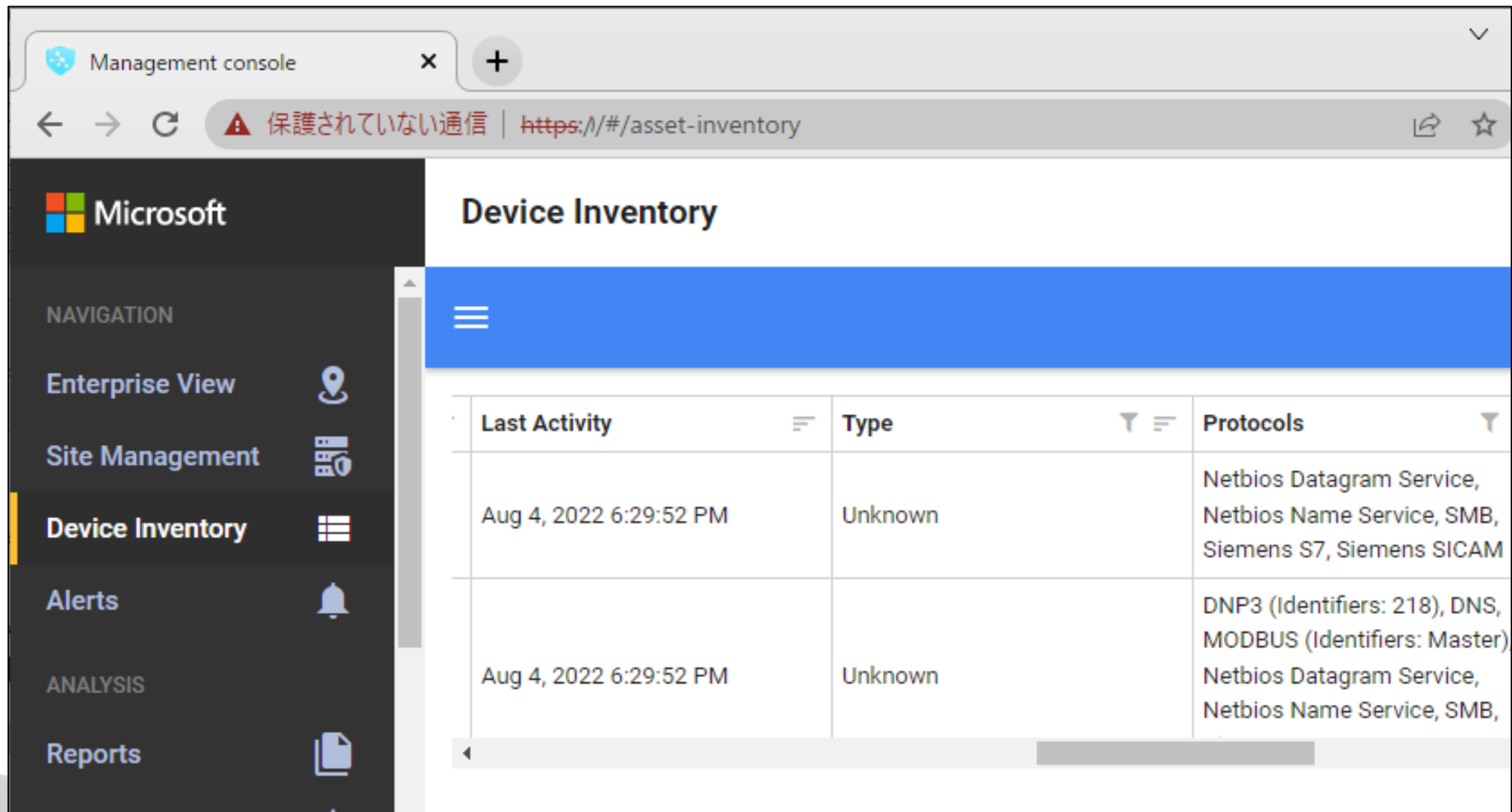
管理コンソール



- デバイス情報
- リスク分析結果
- アラート

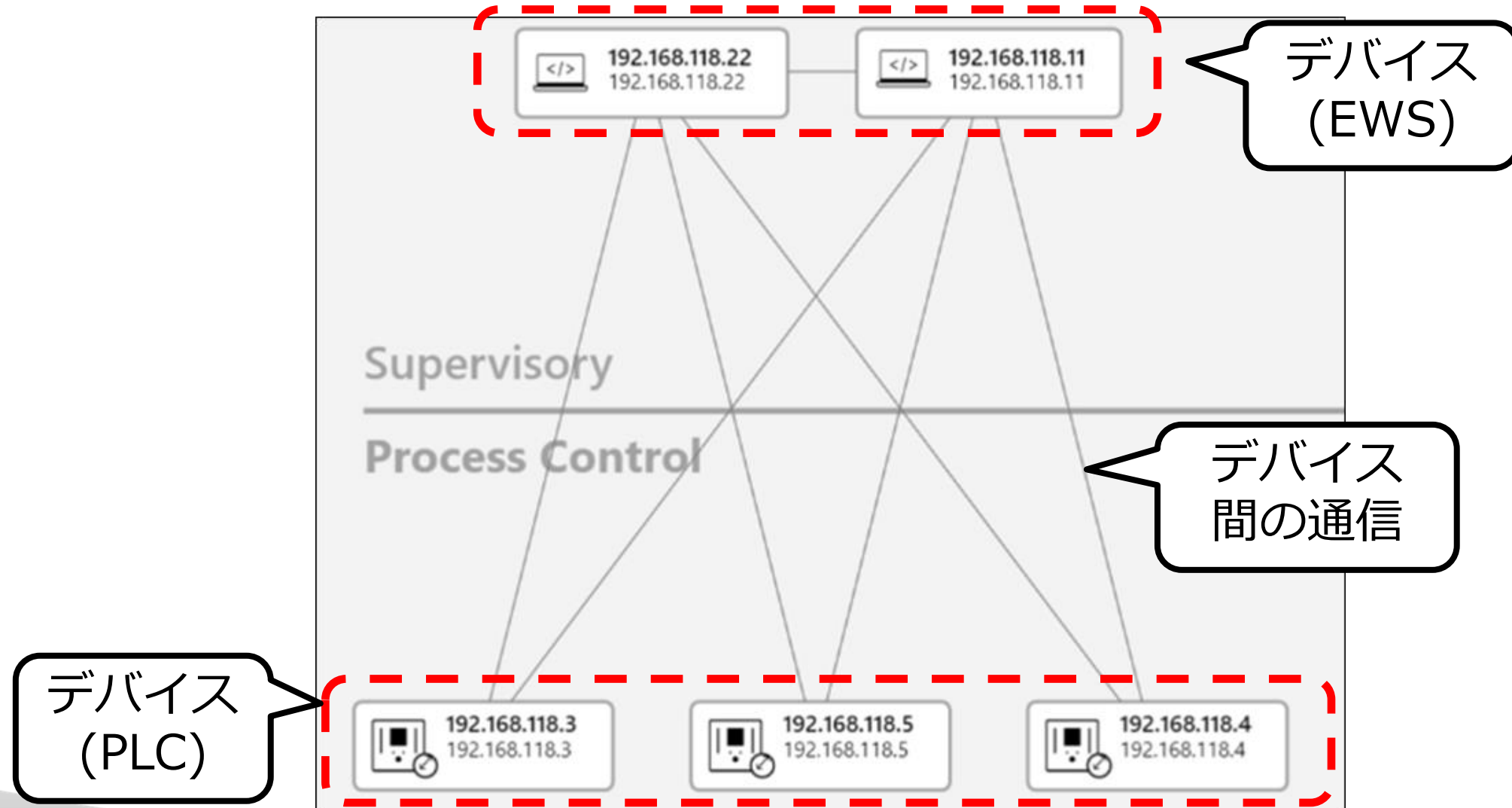






The screenshot shows a web browser window with the title "Management console". The address bar displays a warning icon and the text "保護されていない通信" (Communication not protected) followed by the URL "https:///#/asset-inventory". The interface features a dark sidebar on the left with the Microsoft logo at the top. Below the logo, the "NAVIGATION" section includes links for "Enterprise View", "Site Management", "Device Inventory" (which is highlighted with a yellow bar), "Alerts", and "Reports". The main content area is titled "Device Inventory" and contains a table with two columns: "Last Activity" and "Type". The table has two rows of data, both showing "Aug 4, 2022 6:29:52 PM" and "Unknown". A third column, "Protocols", is partially visible on the right side of the table.

Last Activity	Type	Protocols
Aug 4, 2022 6:29:52 PM	Unknown	Netbios Datagram Service, Netbios Name Service, SMB, Siemens S7, Siemens SICAM
Aug 4, 2022 6:29:52 PM	Unknown	DNP3 (Identifiers: 218), DNS, MODBUS (Identifiers: Master) Netbios Datagram Service, Netbios Name Service, SMB,



Device Inventory

IPアドレス

稼働状況

デバイス
タイプ

通信
プロトコル

デバイス
ベンダー

IP Address	Last Activity	Type	Protocols	Vendor
192.168.123.10	Aug 4, 2022 6:29:49 PM	Engineering Station	Netbios Datagram Service, SMB, Siemens S7 Plus	VMWARE INC.
192.168.118.22	Aug 4, 2022 6:29:50 PM	Engineering Station	Netbios Datagram Service, SMB, Siemens S7	
172.30.35.255	Aug 4, 2022 4:49:03 PM	Multicast/Broadcast	Netbios Datagram Service, Netbios Name Service, SMB	
192.168.117.7	Aug 4, 2022 6:29:52 PM	PLC	Netbios Name Service, SMB, Siemens S7, Siemens SICAM	SAT GMBH & CO.
192.168.117.8	Aug 4, 2022 6:29:51 PM	PLC	ICMP, Netbios Datagram Service, SMB, Siemens SICAM	SAT GMBH & CO.

0

Critical

1

Major

0

Minor

1

Warning

☐ Show Acknowledged

test-sensor-1

Unauthorized PLC Configuration Write

Aug 4, 2022 4:42:47 PM | Device 192.168.117.239 sent a command to write configuration to PLC 192.168.117.7

Message: Device 192.168.117.239 sent a command to write configuration to PLC 192.168.117.7

Severity: Major

Sensor: test-sensor-1

Protocol Data: Protocol: SIEMENS SICAM, Details: Command WriteBlock

OPEN SENSOR

SHOW DEVICES

LEARN

ACKNOWLEDGE

test-sensor-1

An S7 Stop PLC Command was Sent

Aug 2, 2022 4:31:46 PM | A device 192.168.118.1 sent a Siemens S7 Stop PLC Command via Siemens S7 to device 192.168.118.1

Message: A device 192.168.118.1 sent a Siemens S7 Stop PLC Command via Siemens S7 to device 192.168.118.1

未承認の
PLC 書込み

学習ボタン

アラート
確認ボタン

PLC 停止
コマンドの送信

17

連携可能製品

- Aruba ClearPass
- Axonics
- CyberArk PSM
- Forescout
- Fortinet
- IBM QRadar
- LogRhythm
- Micro Focus ArcSight
- Microsoft Defender for EndPoint
- Micosorft Sentinel
- Palo ALto
- RSA NetWitness
- ServiceNow
- Skybox
- Splunk

アラート転送方式

- Syslog (TEXT/CEF/LEEF)
- 電子メール
- Webhook

外部制御

- WEB API
- SSH

test-sensor-1 - 22.2.4

保護されていない通信 | https://device-inventory

Microsoft | test-sensor-1 - 22.2.4

ホーム > デバイスインベントリ

Defender for IoT | デバイス インベントリ

検索

検出

- 概要
- デバイスのマップ
- デバイスインベントリ
- アラート

分析

- イベントタイムライン
- データマイニング

+ フィルターの保存 | 最新の情報に更新 | 列の編集 | エクスポート | Delete | Merge

>> フィルターの追加

132 個中 100 個の項目を表示しています

☐	IP アド...	名前	最後のアクティビティ	種類	プロト...	MAC ア...	ベンダー
☐	192.168....	192.168.11...	2 週 前	PLC	Siemens...	00:01:e3...	SIEMEN..
☐	192.168....	192.168.11...	2 週 前	PLC	Siemens...	00:01:e3...	SIEMEN..
☐	192.168....	192.168.11...	2 週 前	PLC	Siemens...	00:01:e3...	SIEMEN..
☐	192.168....	192.168.11...	2 週 前	PLC	Siemens...	00:01:e3...	SIEMEN..

Microsoft Defender for IoT とは、

- OT 対応の行動分析と脅威インテリジェンス、多数の制御機器ベンダーのプロトコル対応により「可視化」と「異常検知」を実現
- 稼働中のシステムの可用性やパフォーマンスを損なうことなく、導入・運用が可能。
- 他のセキュリティ製品と連携して「防御」も可能。OT システムのセキュリティ対策に重要な三要素を全てカバー

OT システムのセキュリティ対策に最適なソリューション

ソリトンのサービス

- サービス概要
- システム導入例
- 運用体制
- 平時のタスク
- インシデント対応
- Soliton コールセンターのご紹介
- 無償 PoC のご案内

「OT セキュリティの専門家がない！」 「24時間監視体制の構築は難しい！」 といった課題を解決

Microsoft Defender for IoT を使った OT SOC & CSIRT サービス

- 稼働中の OT システムへの影響を極力抑えたサービス導入
- OT セキュリティの専門家による SOC / CSIRT チーム
- 24時間365日 受付・対応可能なサービス運用体制
- インシデント発生時の現場急行サービスをオプションで用意

Soliton®

SOC



Defender for IoT 管理コンソール

インターネット



VPN
ルータ



MES (製造実行システム)



L3SW



SCADA/HMI
製造設備
LAN1



L2SW



Defender for IoT
センサー



PLC



製造設備 1

SCADA/HMI
製造設備
LAN2



L2SW



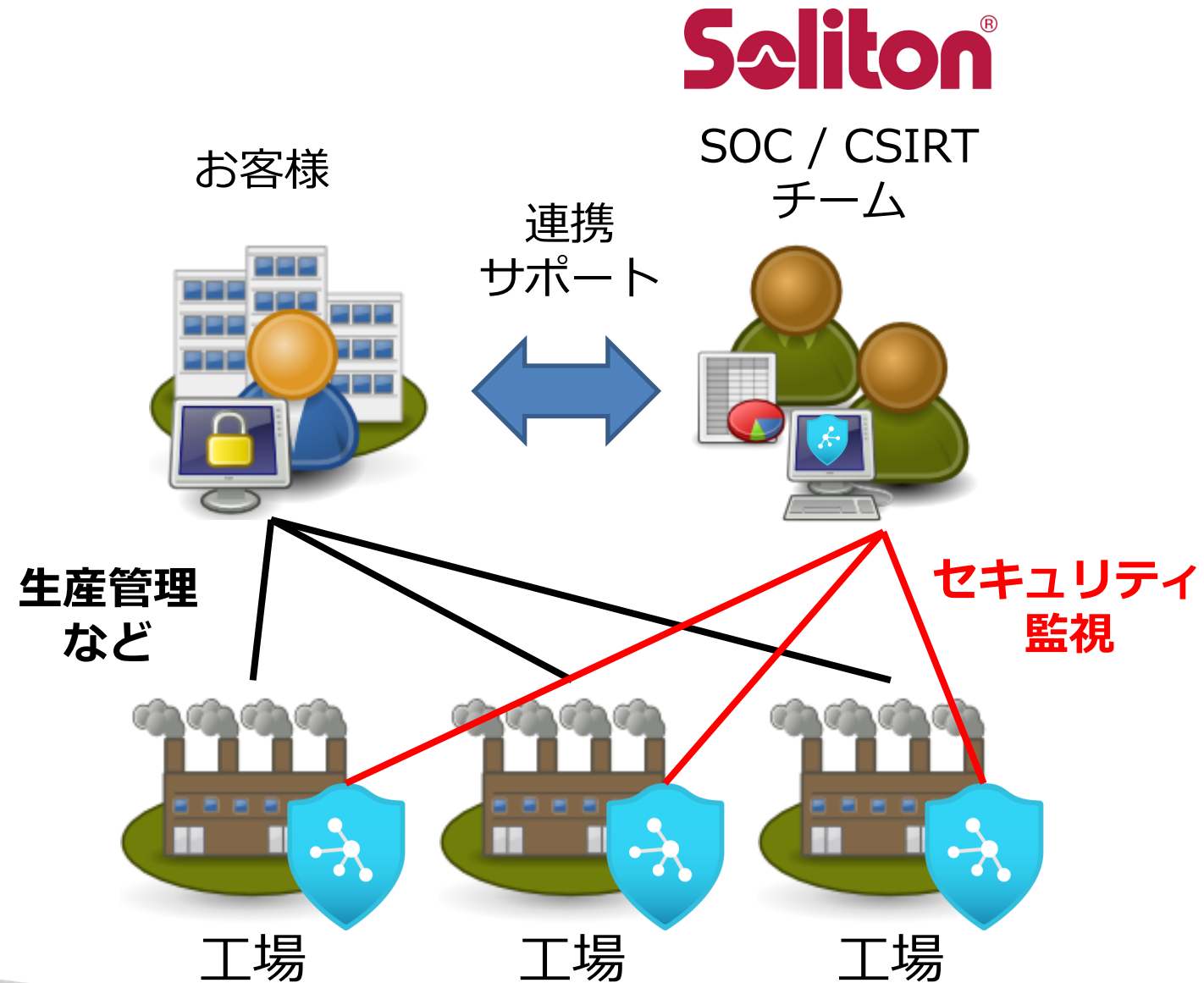
Defender for IoT
センサー



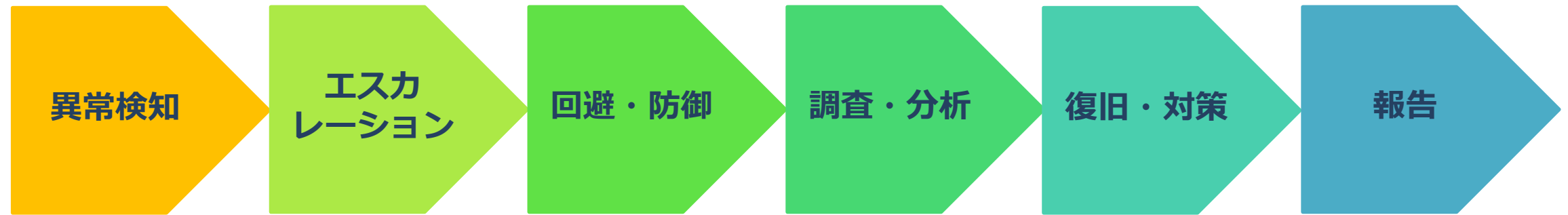
PLC



製造設備 2



- アラート監視
- お客様からのお問い合わせ対応
- 脆弱性情報をはじめとするサイバーセキュリティ関連情報の収集と注意喚起
- サービス運用レポートの作成
 - 定期リスクアセスメント結果（脆弱性情報、対応状況など）
 - お問い合わせ内容分析（問い合わせ件数、対応状況など）
 - インシデント対応分析（発生件数、発生傾向、対応状況など）
- 監視システムメンテナンス

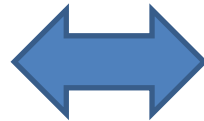


お客様
OT セキュリティ
担当部署



OT 現場との調整・連携

連携
サポート



Soliton®
SOC / CSIRT
チーム



インシデント対応中心の業務

- 24時間365日問い合わせ対応
- 電話、メール、WEB、各種メッセージングサービス（オプション）による受付
- アラート対応
 - 緊急度の高いアラートは即座にエスカレーション
 - オプションで現場駆けつけサービスもご用意
- ISMS 認証、プライバシーマーク取得



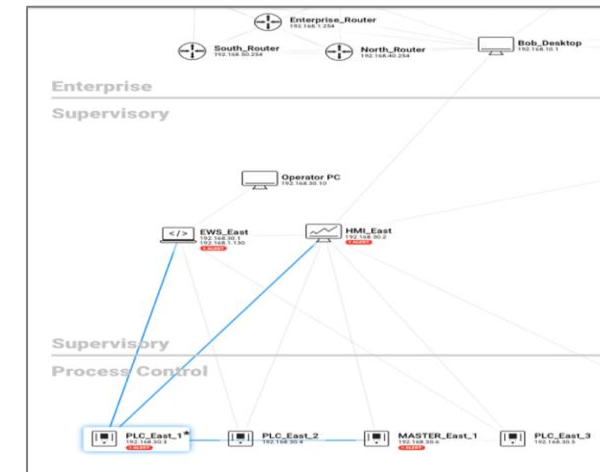
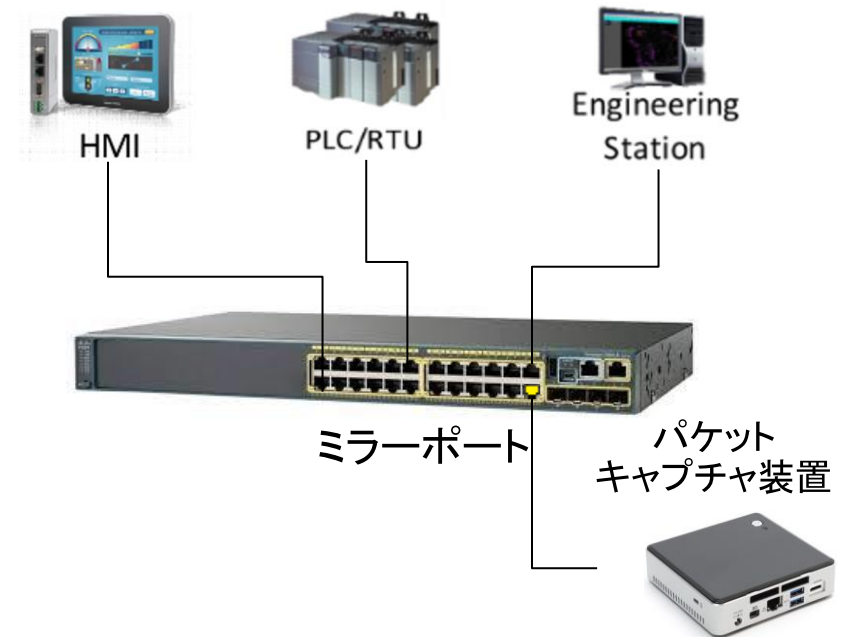
- 簡易アセスメントを実施いたします

1. PLCやHMIが接続されている
スイッチにミラーポートを設定
2. ミラーポートにパケットキャプチャ装置を接続
3. 30分から数時間分のPCAPを保存



- 下記の情報をご確認いただけます

- どのようなデバイスが接続されているか
- それらのデバイスはどのようなプロトコルで通信をしているか
- 脆弱性や潜在的な脅威は存在しないか



リポート

Microsoft Defender for IoT を使った OT SOC & CSIRT サービス

- 稼働中の OT システムへの影響を極力抑えたサービス導入
- OT セキュリティの専門家による SOC / CSIRT チーム
- 24時間365日 受付・対応可能なサービス運用体制
- インシデント発生時の現場急行サービスをオプションで用意

OT セキュリティ対策の導入から運用までフルサポート

ソリトン セキュリティ監視サービス for IoT/OT と
Trend Micro EdgeIPS を組み合わせ
OT セキュリティ対策の三要素を実現



セキュリティ監視サービス for IoT/OT

- OT セキュリティ対策の重要な三要素
「可視化」「異常検知」「防御」

三要素の実現で効果的な OT セキュリティ対策

- 三要素を実現するソリューション Microsoft Defender for IoT

OT システムのセキュリティ対策に最適なソリューション

- Microsoft Defender for IoT を使った OT SOC / CSIRT サービス
「セキュリティ監視サービス for IoT/OT」

OT セキュリティ対策の導入から運用までフルサポート