# ONIC実行委員より，明日の予習としての座学

Ken Hashimoto, Senior Sales Engineer,
Nozomi Networks, Inc.

# 皆さまに質問

今まで, “OT”のネットワークやインフラを作ったことある？ない？

# myself

橋本 賢一郎（はしもと けんいちろう）
X （旧twitter）：@hashiken_com

趣味　：温泉とバイクと車

所属　：NOZOMI NETWORKS　2024年～

Nozomi Networks, Inc.
Regional Sales Engineering

社外活動　：IPA

情報処理安全確保支援士 試験委員

ONIC Japan

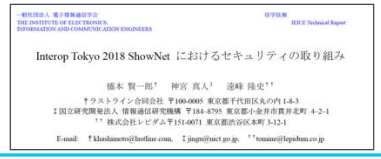
Open Networking Conference Japan 実行委員

経歴　：
- Network Engineer 20+ years
  - ✓ Sumitomo Electric Industry (SUMINET)
  - ✓ Foundry Networks (→ Brocade → Broadcom)
- Security Engineer 10+ years
  - ✓ FireEye (→ Mandiant (Google) / Trellix)
  - ✓ BlueCoat (→ Symantec → Broadcom)
  - ✓ Lastline (→ VMware → Broadcom)
  - ✓ ULTRA RED
- Interop ShowNet NOC Team Member for 15 years
  - ✓ 2010年 ～ 2024年

Interop Tokyo　SHOWNET Inter*Network

執筆　：
- ✓ 電子情報通信学会　インターネットアーキテクチャ研究会
- ✓ ソフトウェアデザイン　ネットワークセキュリティ関連


昨今のサイバー攻撃の手法とその対策について
－Interop Tokyo 2014 ShowNet における結果からの考察－


Interop Tokyo 2018 ShowNet における セキュリティの取り組み




# クイズ (1/3)

Q1：“OT” ってなんの略？

(1) Operational Technology

(2) Operation Technology

(3) OpenNetworking Technology

# クイズ (2/3)

Q2：情報セキュリティ対策の重要度を表す三大要素であるCIA. これは何の略？

(1) Commitment / Interfaces / Alerts

(2) Command Line Interface / Interoperability / Accessibility

(3) Confidentiality / Integrity / Availability
（機密性 / 完全性 / 可用性）

# クイズ (3/3)

## Q3：OTセキュリティ対策の重要度を表す三大要素は？

- ✓ 機密性 … Confidentiality
- ✓ 完全性 … Integrity
- ✓ 可用性 … Availability

(1) Confidentiality / Integrity / Availability

(2) Integrity / Availability / Confidentiality

(3) Availability / Integrity / Confidentiality

# OTって, 考えた時に…

Nozomiに入社するまでは…

**Webカメラとか, 家電のリモコンとかで使うIoTの延長でしょ**

**通信する産業機器繋がってるだけでしょ**

**OTといっても, tcp/ip使ってるから, ITと変わらんでしょ**

**textベースのトラフィックだけだから, 今のIT技術なら繋がればいいんだよね**

**ITの延長だから, セキュリティ的にITと同じで大丈夫っしょ**

# OTって, 考えた時に…

Nozomiに入社するまでは…

Webカメラとか, 家電のリモコンとかで使うIoTの延長でしょ

通信する産業機器繋がってるだけでしょ

## 実はもっと深い沼だった…

OTといっても, tcp/ip使ってるから, ITと変わらんでしょ

textベースのトラフィックだけだから, 今のIT技術なら繋がればいいんだよね

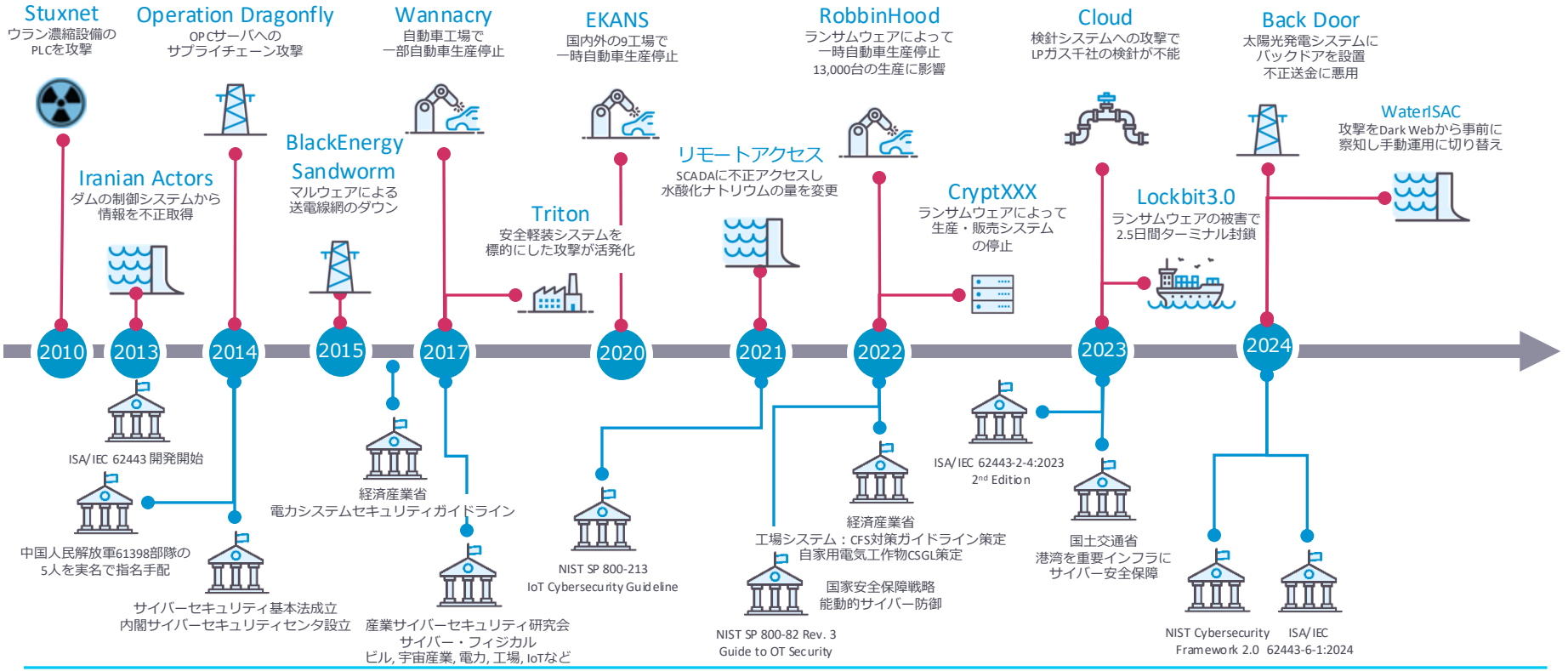
ITの延長だから, セキュリティ的にITと同じで大丈夫でしょ

入社時　一ヶ月後　イマココ

# Bird’s Eyes View

Operational Technology

# OTインシデントと関連組織の動き




OPC: OLE for Process Control
CFS: Cyber Physical Security

# OTのインシデントにかかる高いコスト

**$4.82M USD**

**重要インフラデータ漏洩の平均推定コスト**

“重要インフラへのサイバー攻撃は新しい常態となり，世界のトップ5リスクの1つとなっています.”

**World Economic Forum, *Global Risk Report, 2020***

| | 組織名 | 問題/攻撃 | コスト (USD) |
|---|---|---|---|
| **2023** | ABB | Black Basta Ransomware | Unknown |
| **2022** | Colonial Pipeline | DarkSide Ransomware | 5m ransom |
| | CommonSpirit Health | Ransomware | 150m |
| | JBS | REvil Ransomware | 10m ransom |
| **2021** | SolarWinds | Supply Chain Breach | 40m |
| **2020** | Cognizant | Maze Ransomware | 70m |
| **2019** | Norsk Hydro | LockerGoga Ransomware | 70m |
| | Duke Energy | Compliance Violation | 10m |
| **2018** | Saudi Petrochem | Triton | Unknown |
| | UK NHS | WannaCry | 100m |
| **2017** | Merck | NotPetya | 870m |
| | FedEx (TNT Express) | NotPetya | 400m |
| | Maersk | NotPetya | 300m |

Sources: IBM Security, Wired, Wall Street Journal, UK Telegraph, Threatpost, Forbes

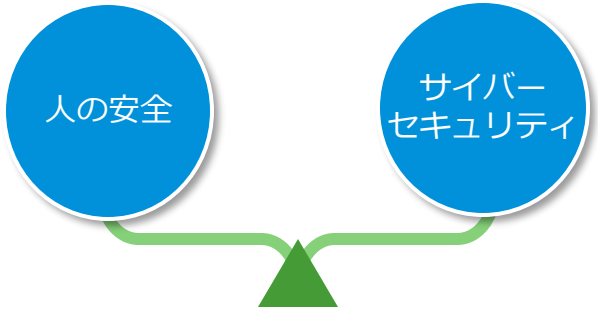
# 昨今の関連するセキュリティインシデント

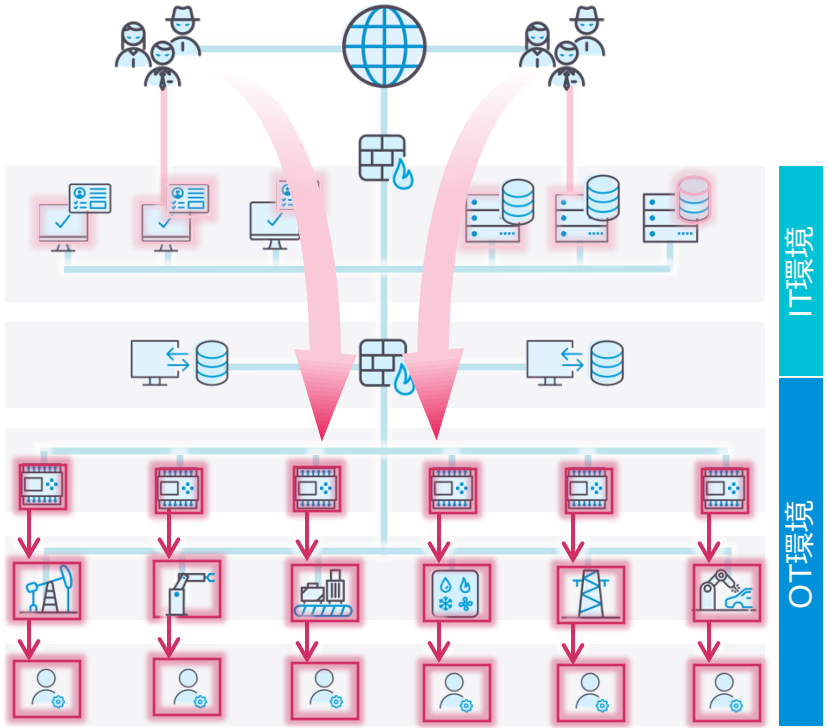
| 被害組織 | 時期 | 被害内容 | 原因 |
|---|---|---|---|
| 米国水処理施設<br>CASA Alert (AA21-042A) | 2021.02. | 不正侵入後, SCADAシステムを操作, 水酸化ナトリウムの量を増やしたが, 担当者が気づいて問題を修正した | 古いOSと脆弱なパスワード<br>デスクトップ共有ソフト |
| 米国石油パイプライン | 2021.05. | 被害は一部のITシステムだったが, 攻撃者によるパイプラインへの攻撃を示唆され, 予防的処置でパイプライン全体を停止. | 未把握のレガシーなVPN装置が侵入口 |
| 自動車部品メーカー | 2022.3. | リモート接続機器の脆弱性を悪用されてランサムウェアの被害. 納品先自動車メーカーでは, 国内14工場, 28ラインの生産を停止し13,000台の生産に影響 | リモート接続機器の脆弱性悪用 |
| 受配電設備, 器具メーカー | 2022.04. | リモート接続機器の脆弱性を悪用されてランサムウェアの被害<br>約1.5ヶ月間, 製造及び販売システムを停止し, 窃取された個人情報の復元は断念 | リモート接続機器の脆弱性悪用 |
| 台湾電子機器メーカー | 2022.06. | ランサムウェアグループLockBit 2.0の被害に遭い, 工場の操業停止に追い込まれる | 未公表. 2度目 |
| 多国籍ハイテク企業 | 2023.05. | Active Directoryがランサムウェアの攻撃を受けて数百台が影響を受ける.<br>OTネットワークへの拡散を防ぐため顧客とのVPNを停止し, プロジェクトの遅延や工場にも影響が拡大 | 未公表 |
| 住宅設備関連機器メーカー | 2023.05. | クラウドが不正アクセスを受け, クラウドサービスが停止したため, 全国約1,000のLPガス会社で検針業務が行えなくなった | 不正アクセスからラテラルムーブメント |
| 国内港湾運営組織 | 2023.07. | リモート接続機器の脆弱性を悪用されて不正侵入後にランサムウェアに感染<br>5つのターミナルの集中管理ゲート, コンテナのほぼ全ての制御を2.5日間喪失<br>某自動車メーカーも部品入荷に影響を受け, 一部のラインを停止する | リモート接続機器の脆弱性悪用 |
| レンズメーカー | 2024.04. | 海外の事業所で不審なシステム挙動を調査していたが, 国内外の事業所でシステム障害を確認. 生産工場内のシステム, 受注システムが停止し, 出荷生産が停止. | 未公表. 3度目 |
| 太陽光発電施設 | 2024.05. | 既知の脆弱性を悪用されてバックドアが設置され, インターネットバンキングの不正送金に悪用されていた. 中国の攻撃者集団の可能性. 処理水の海洋放出が原因か | アタックサーフェスの脆弱性を悪用してバックドア設置 |

# Operational Technology (OT) と産業用制御システム（ICS）

# OTセキュリティとは何を守るものか

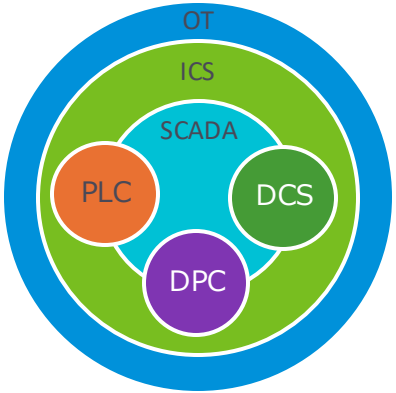
- IT環境
  - ✓ 何から, 何を守るか
    - 悪意ある人や集団から, ZTAで定義されているリソースを守る
- OT環境
  - ✓ 何から, 何を守るか
    - 過去：PLC, DCS, RTUが制御するマシンから人を守る
    - 現在：
      - 悪意ある集団から, 制御装置の正常運用
      - 制御するマシンから, 人を守る



# ICSのコンポーネント

- **OT** (Operation Technology)
  - ✓ IT業務ではなく, 産業業務を管理するために使用されるコンピュータシステム
- **ICS** (Industrial Control System)
  - ✓ OTにおける主要分野であり, 産業プロセスをモニタ, 制御するために使用されるシステム
- **SCADA** (Supervisory Control And Data Acquisition)
  - ✓ オペレータがシステムの状態をモニタ, 正常外操作を示すアラームの受信, 制御下プロセスの管理を実現し, システム調整を行うためのグラフィカルユーザインタフェースを提供
- **PLC** (Programmable Logic Controller)
  - ✓ センサーやアクチュエーターを制御
- **DPC** (Discrete Process Control system)
  - ✓ 個別プロセス制御システム
- **DCS** (Distributed Control System)
  - ✓ システムを構成する各機器ごとに制御装置を設ける分散制御システム
- **センサー, アクチュエーター**
  - ✓ 物理的世界との相互作用を実現（圧力センサー, バルブなど）
- **HMI (Human-Machine Interface):**
  - ✓ サブプロセスの監視と制御
- **監視画面**
  - ✓ 産業プロセスの遠隔監視
- **データヒストリアン:**
  - ✓ プロダクションネットワークとSCADAネットワークからのすべてのデータを記録し, 企業のIS（たとえばERP）にエクスポートする

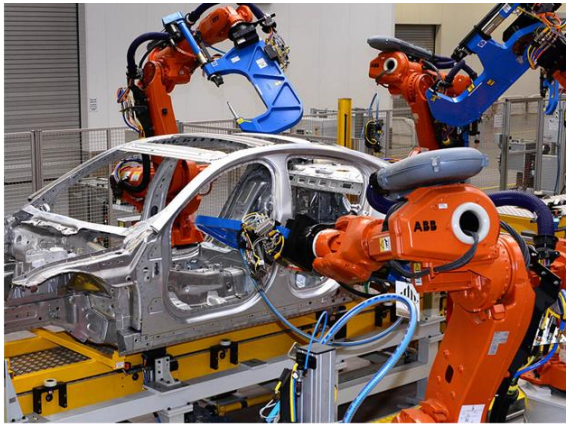



Source: https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference

# 産業用制御システム（ICS=Industrial Control Systems）

https://vecer.mk/files/article/2017/05/02/485749-saudiska-arabija-ja-kupi-najgolemata-naftena-rafinerija-vo-sad.jpg

http://www.jfwhite.com/Collateral/Images/English-US/Galleries/middleboro9115kvbreakers.jpg




https://www.roboticsbusinessreview.com/wp-content/uploads/2016/05/jaguar-factory.jpg

https://www.oilandgasproductnews.com/files/slides/locale_image/medium/0089/22183_en_16f9d_8738_honeywell-process-solutions-rtu2020-process-controller.jpg

https://selinc.com/uploadedImages/Web/Videos/Playlists/Playlist_RTAC_1280x720.png?n=63584758126000


http://www02.abb.com/global/seitp/seitp202.nsf/0/0601d25ed243cfb0c1257d7e0043e50e/$file/7184_lvl2.jpg





http://fukushimawatch.com/wp-content/uploads/sites/12/2016/05/Fukushima_fire_explosion_radiation.jpg

# “産業用ネットワーク” はどこにあるか？

- 電力
- 石油 & ガス
- 製造業
- 化学
- 製薬
- 交通機関
- 鉱業
- 水道

しかし, ここにも …..

テーマパーク（複雑な運行管理）

倉庫（例えばアマゾンの自動倉庫）

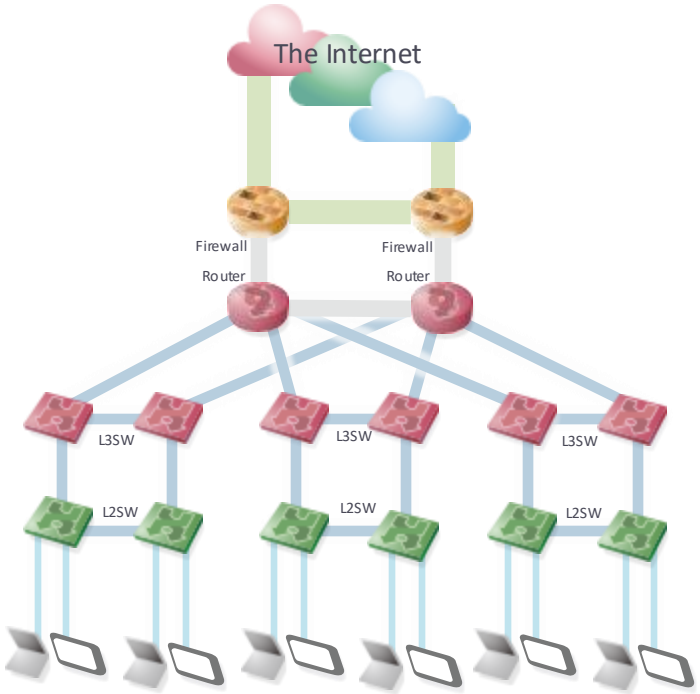
空港（手荷物システム）

船舶（クルーズ船）

ビルオートメーション
（エレベーター, エアコン, 発電所, , ）

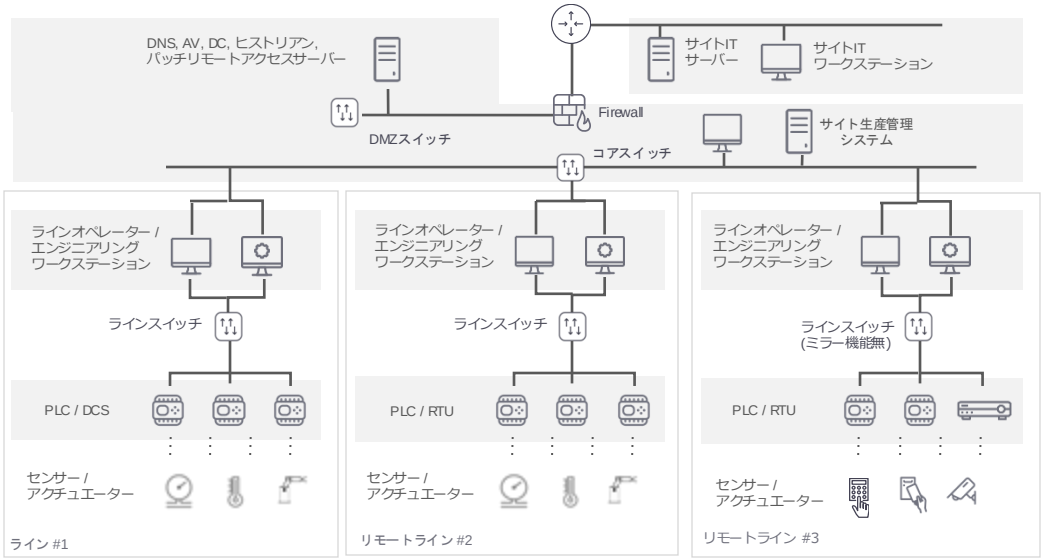
**基本的にはどこにでも …….**

# Prev-DXでのITとOT



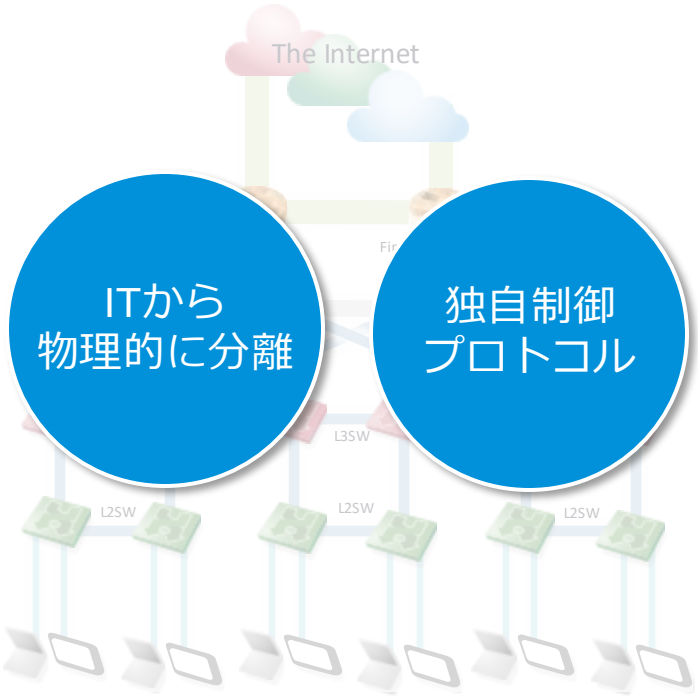

IT環境

ITとOTの物理的な隔離で安全を担保




OT環境

# Prev-DXでのOTの特徴

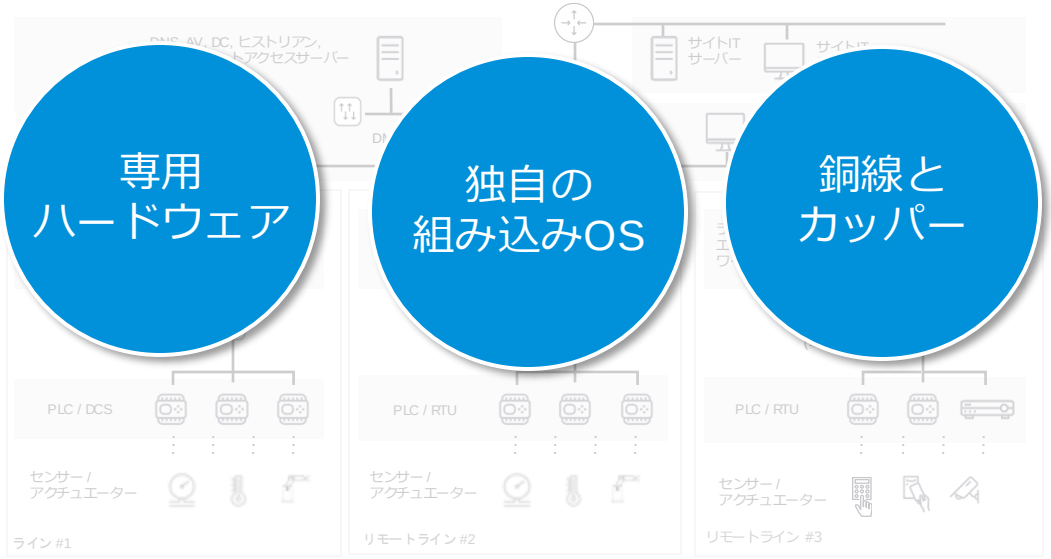



ITから
物理的に分離

独自制御
プロトコル

IT環境

ITとOTの物理的な隔離で安全を担保




専用
ハードウェア

独自の
組み込みOS

銅線と
カッパー

OT環境

# Prev-DXでのOTの特徴

ITから
物理的に分離

独自制御
プロトコル

独自の
組み込みOS

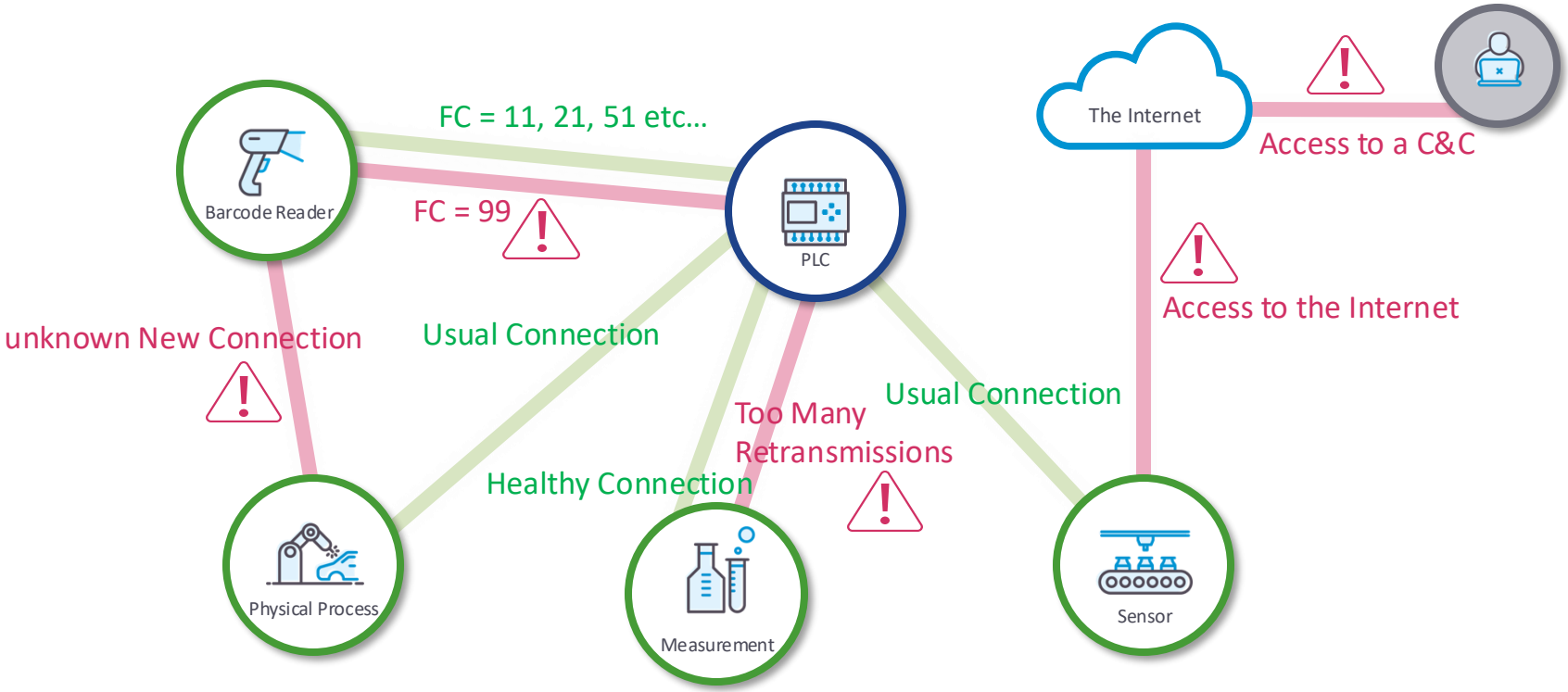
銅線と
カッパー

**可用性**
**継続した安定運用**

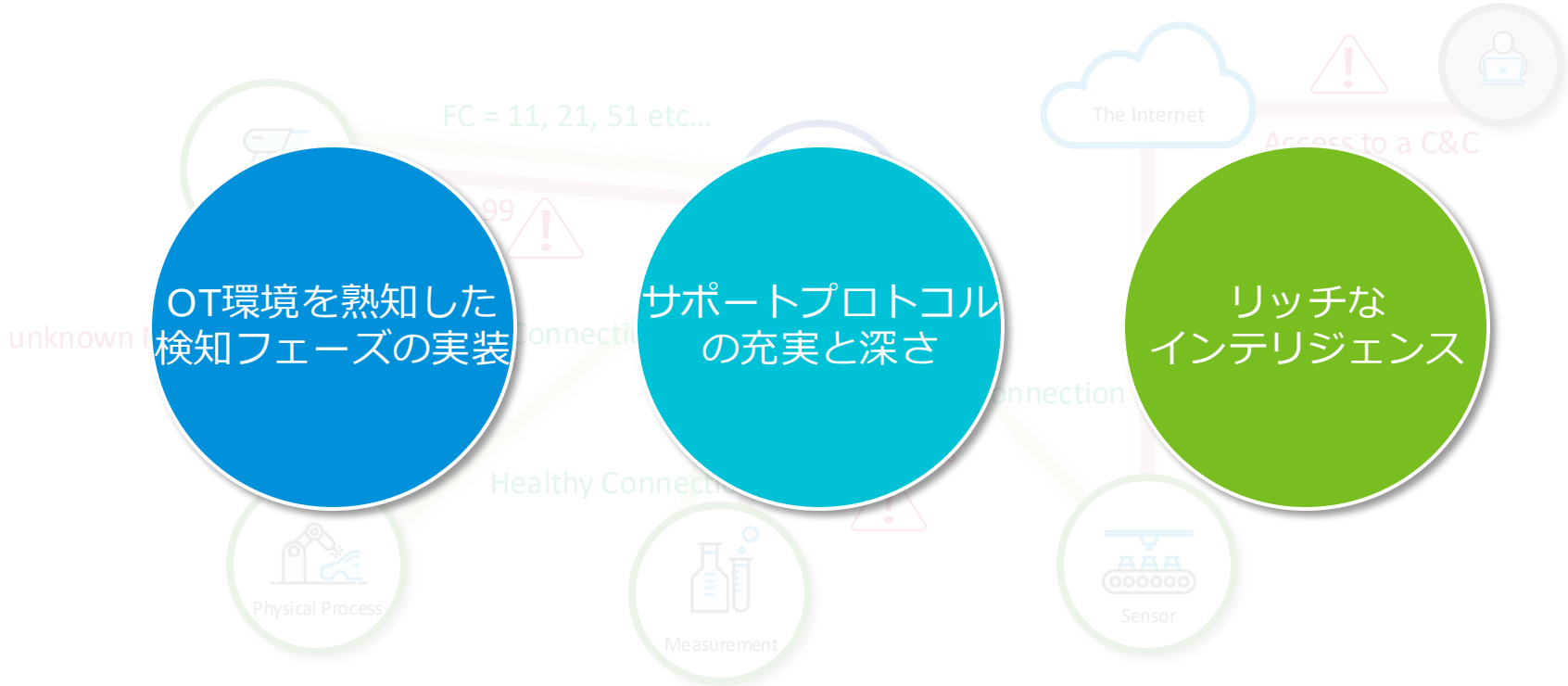
IT環境

OT環境

# 可用性の向上 - 継続した安定運用のために



# 可用性の向上 - 継続した安定運用のために



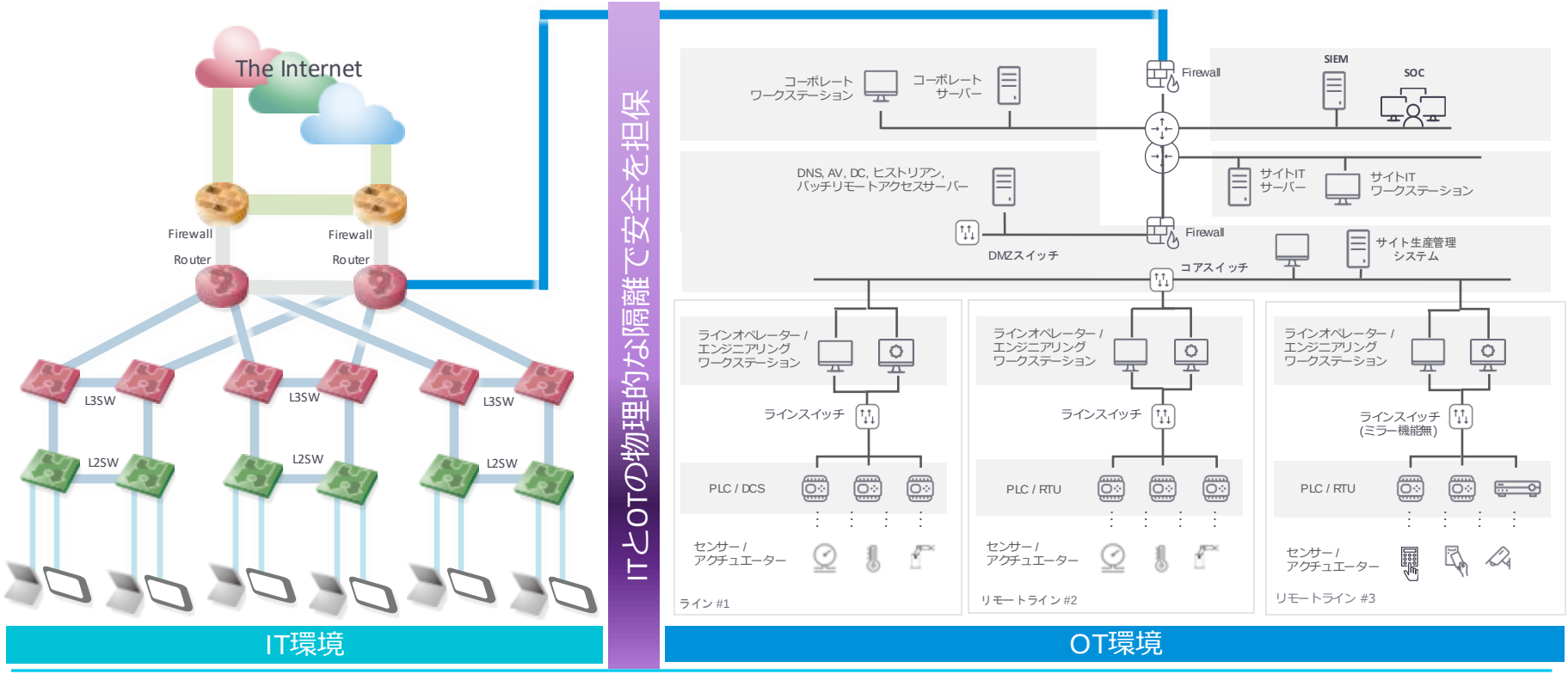
# ゼロトラストの時代になぜネットワークなのか？

エンドポイントの
リソース不足

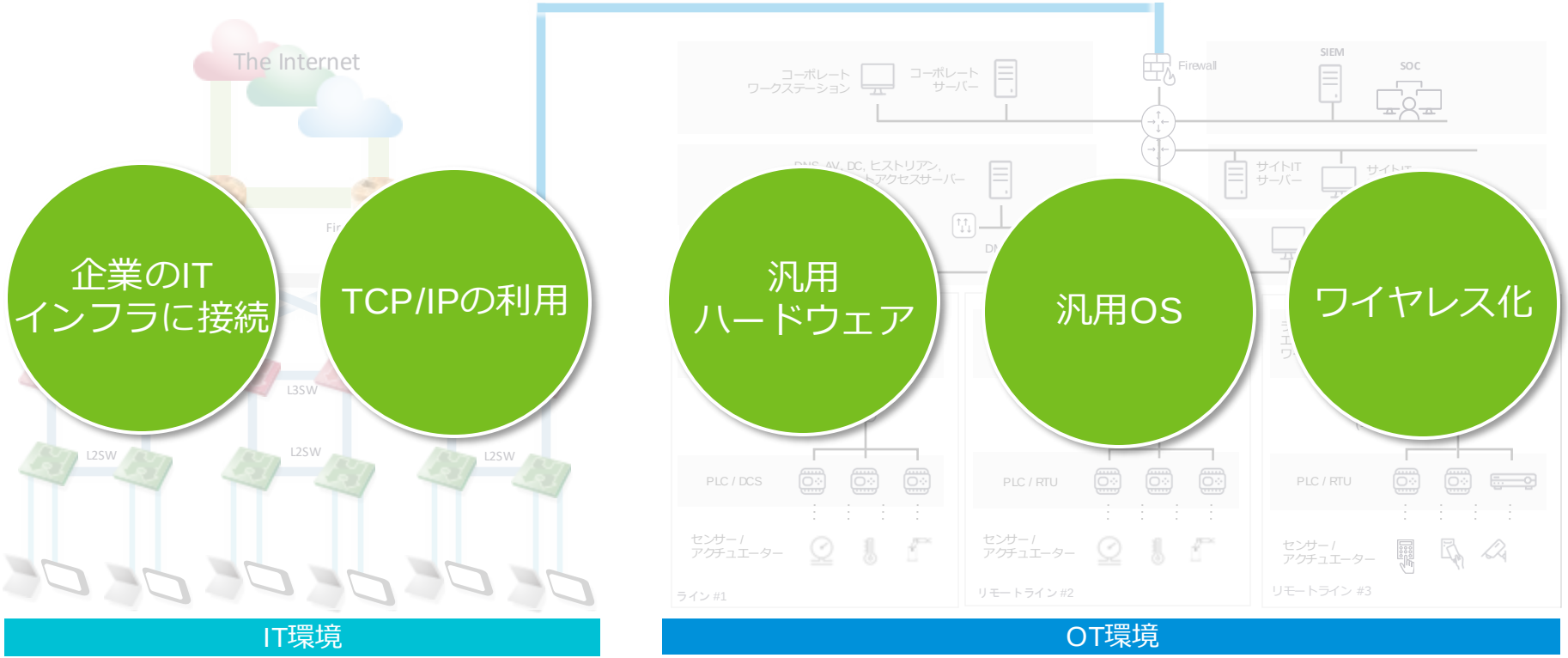
既存構成に影響なく
モニターできる

未把握の資産も
その存在を検出可能

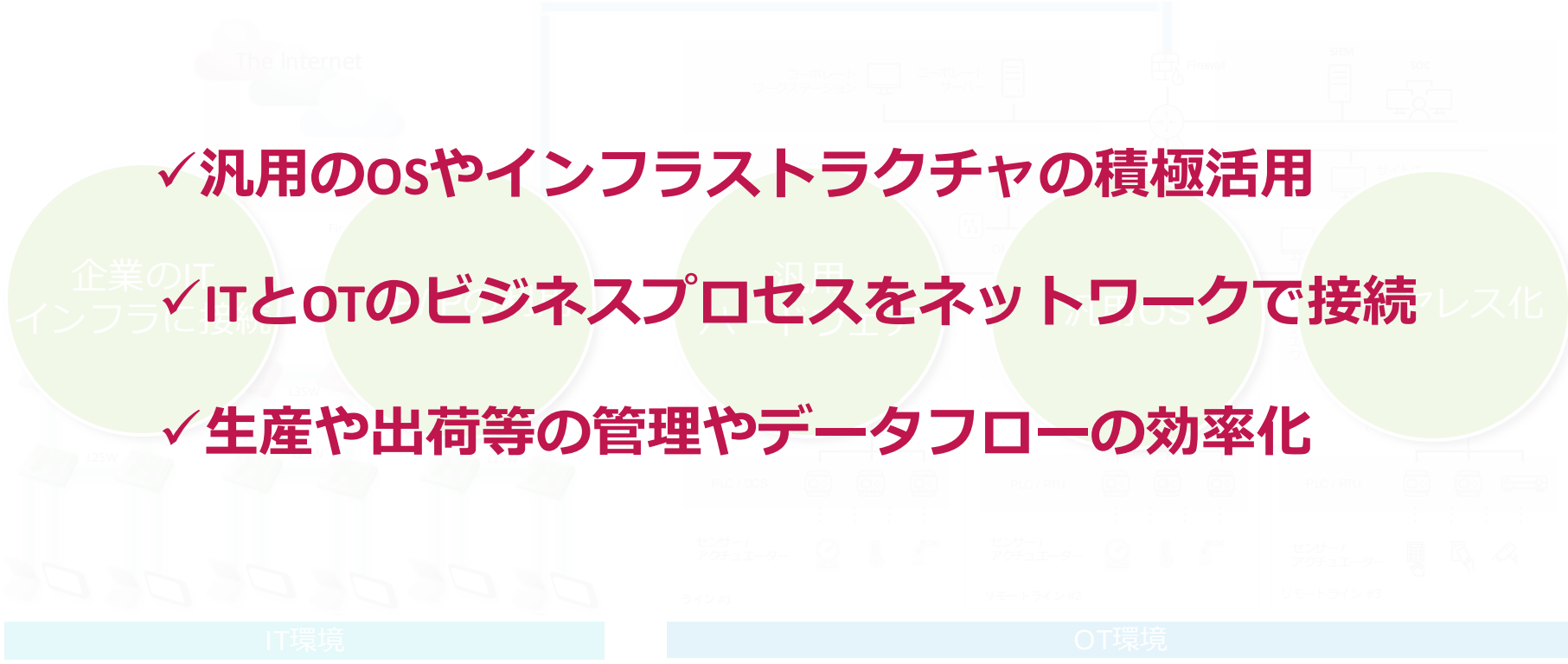
# Post-DXによるビジネスプロセスとの相互接続と運用



# Post-DXによる変化の特徴

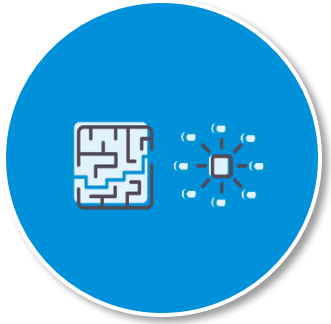


# Post-DXによる変化の特徴




- ✓汎用のOSやインフラストラクチャの積極活用
- ✓ITとOTのビジネスプロセスをネットワークで接続
- ✓生産や出荷等の管理やデータフローの効率化

# OT環境におけるPost-DXのリスク



ITネットワークの侵害による
OTネットワークの停止

ITネットワークを経由した
OTネットワークへの侵害や停止

OTネットワークの侵害による
物理プロセスの不正操作

ウラン濃縮の
不正操作

ITへの侵害で
パイプライン
停止

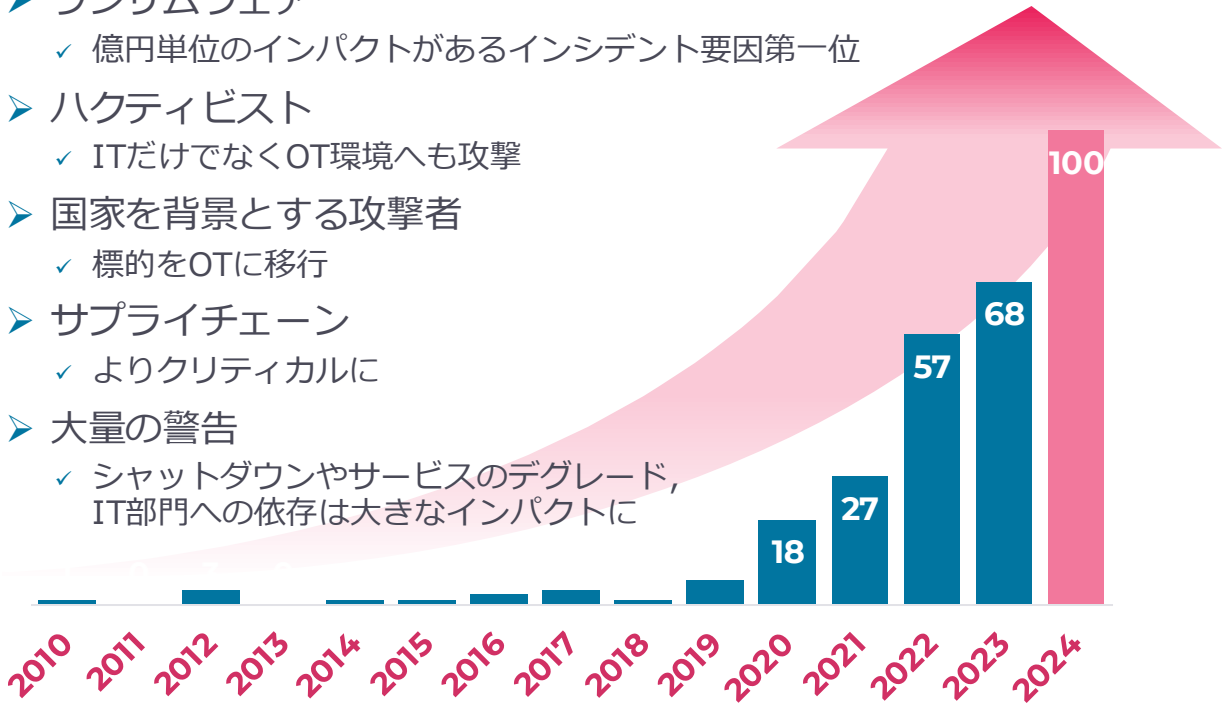
ランサム
ウェア攻撃で
工場停止

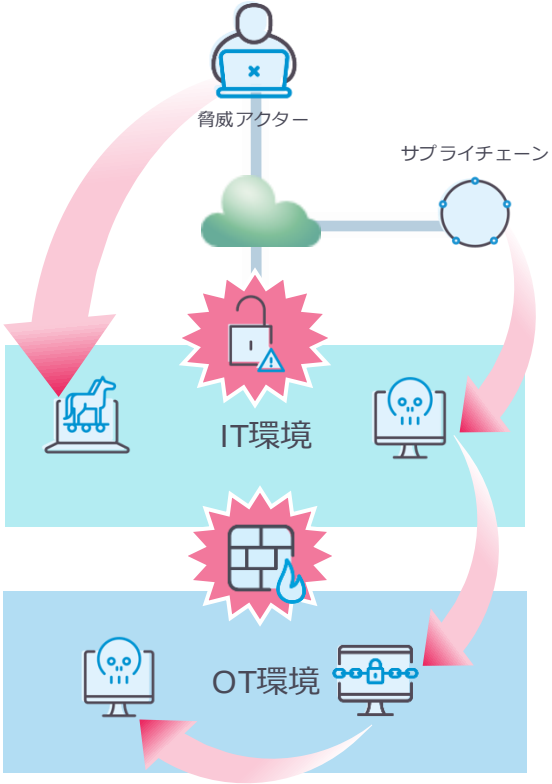
水道施設の
薬品濃度
不正引き上げ

クラウド侵害で
ガス検針停止

# サイバー フィジカル セキュリティインシデント

- ランサムウェア
  - ✓ 億円単位のインパクトがあるインシデント要因第一位
- ハクティビスト
  - ✓ ITだけでなくOT環境へも攻撃
- 国家を背景とする攻撃者
  - ✓ 標的をOTに移行
- サプライチェーン
  - ✓ よりクリティカルに
- 大量の警告
  - ✓ シャットダウンやサービスのデグレード，IT部門への依存は大きなインパクトに




Source: https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2024-threat-report-ot-cyberattacks-with-physical-consequences/

# 数字から見るOTセキュリティインシデントの状況

**76%**

OT環境へのサイバー攻撃を経験
（調査対象はOT環境がある組織のみ）

**72%**

IT環境からOT環境へ
サイバー攻撃が拡散

**20,405件**

2024年上半期に 新規登録された脆弱性
（28,902件 / 2023年）

**1/4社**

サイバー攻撃によって
業務停止に

**62分**

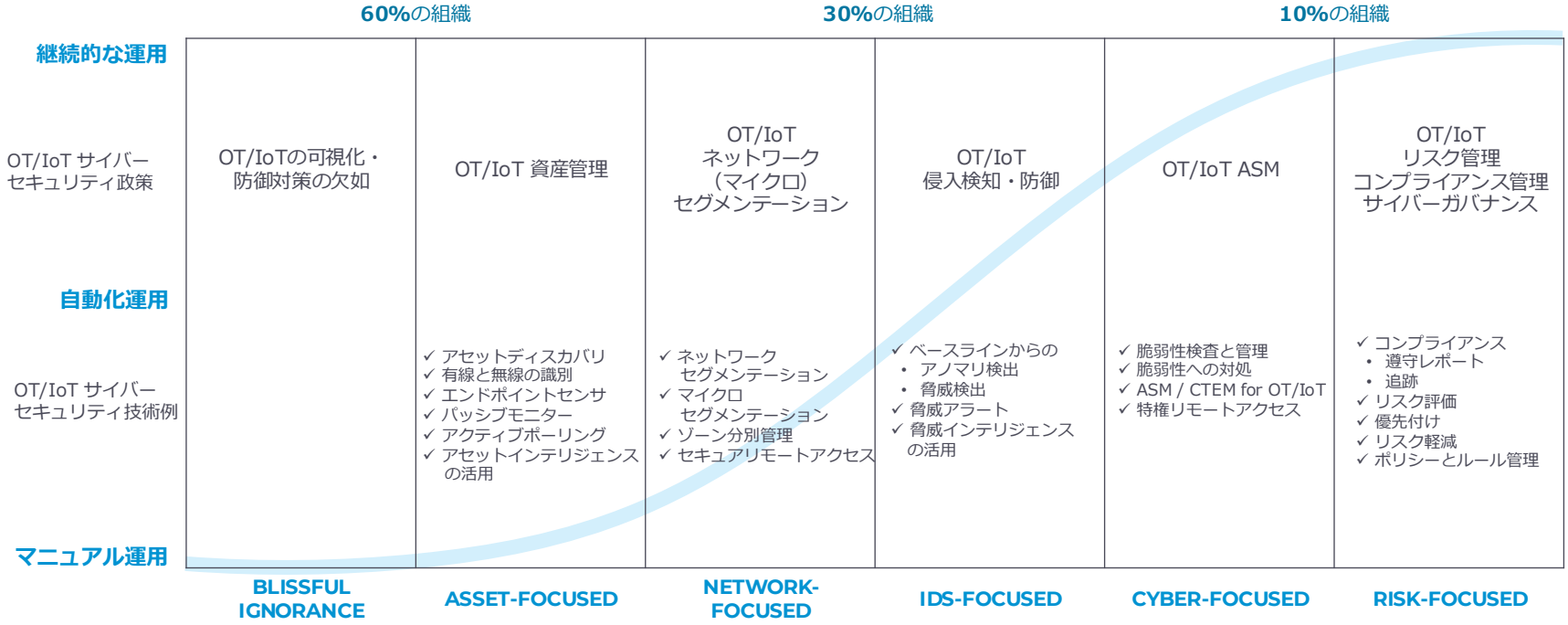
ラテラルムーブメント
開始まで

**73 vs 390件**

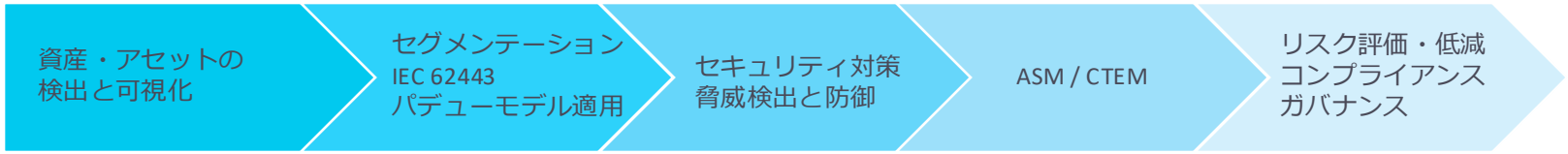
CISA KEV vs VulnCheck KEV
（米国政府機関のみ vs エンタープライズ追加）

CrowdStrike Global Threat Report: https://www.crowdstrike.jp/resources/infographics/global-threat-report-2024/
CISA NVD Search: https://nvd.nist.gov/vuln/search
Palo Alto Networks OT Security Report 2024: https://www.paloaltonetworks.jp/resources/research/state-of-ot-security-report

# OT/IoTサイバーセキュリティの進捗度



# OT/IoTのセキュリティ強化ステップ



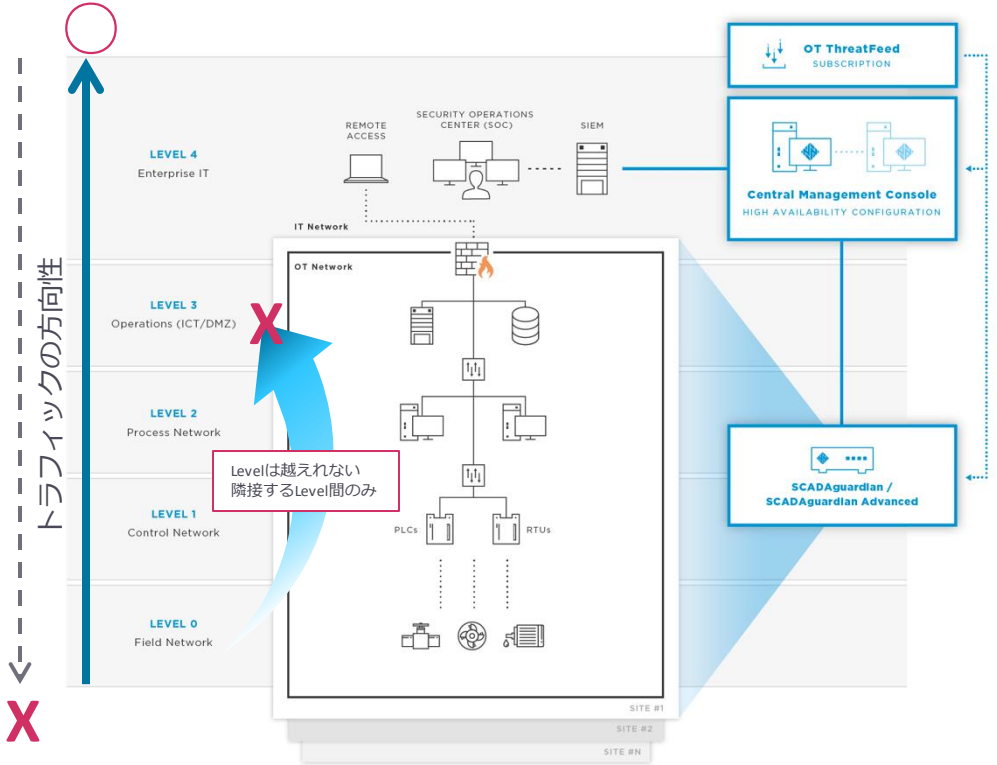

| 対象 | 資産・アセット | ネットワーク | 検出・防御装置 | アタックサーフェス | リスク管理 |
|---|---|---|---|---|---|
| 強化内容 | 資産・アセットの検出と可視化 | (マイクロ)セグメンテーション | ITとの境界（多層）防御 | インターナルのみ | リスク評価と優先度 |
| | 検出資産の管理, 可視化 | パデューモデル適用 | アセットごとのIPS | 脆弱性悪用の可否検査 | コンプラ遵守レポート |
| | 脆弱性管理 | 正常性確認と異常の検出 | トラフィックを解析 | 脆弱性悪用の容易性 | ポリシー・ルール管理 |
| 課題 | 管理対象外の資産の検出方法 | 生産停止を伴うので停止不可 | エンドポイントのリソース | スキャンしても大丈夫か | ITと異なる優先度 |
| 実現方法 | ネットワークからトラフィックを取得・解析して検出 | ✓ セグメンテーション<br>✓ ネットワークからトラフィック取得して解析 | ✓ マイセグと分散IPS<br>✓ ネットワークからトラフィックを取得・解析して検出<br>✓ FirewallやIPSと連携して防御 | アセットへの影響度から要検討 | OTの運用に合わせたルール作り |

**守るべき対象の検出と管理が, セキュリティ強化の第一歩**

# OT環境での特徴の差分

| 差分項目（抜粋） | IT | OT |
|---|---|---|
| **セキュリティに対する要求の優先度** | • 機密性 … Confidentiality<br>• 完全性 … Integrity<br>• 可用性 … Availability | • 安全性 …… Safety<br>• 制御 …… Control<br>• **可用性／回復性** (物理・サイバー両方) …… A<br>• 完全性 …… I<br>• 機密性 …… C |
| **コンポーネントの寿命** | • 3-5 年 | • **15-20 年** |
| **インシデント管理とメンテナンス** | • IT標準手順<br>• 対策としてシャットダウンを許可 | • 緊急対応手順<br>• **対策としてシャットダウンは許可されない** |
| **入力処理** | • バッチ（例: メールサービス） | • バッチ（例: 食品製造）<br>• 連続的（例: 電力システムコントロール） |
| **稼働ソフトウェア** | • ダイナミック, 実験的 | • **固定的**, 保守的 |
| **アプリケーションとプロトコル** | • 標準, 非常に多い | • **カスタマイズ化, 少ない** |
| **メンテナンスプロファイル** | • ITエンジニア | • 制御エンジニア, プロセスエンジニア |
| **攻撃ベクトル** | • 一般的 | • カスタマイズ化（例: Petya, WannaCry, Stuxnet） |
| **性能** | • 高帯域<br>• ベストエフォート<br>• 遅延を許容 | • **低帯域**<br>• 仮想サーキットが使用される（より決定論的）<br>• 遅延とジッターを許容しない |

# リファレンスアーキテクチャ: IEC 62443 PURDUE（パデュー）モデル




- Level 4-5: サイトビジネスプランニングとロジスティクス, 企業ネットワーク
  - ✓ メール, イントラネット, プリンターなど
- Level 3.5: 上流DMZ
- Level 3: オペレーション（ICT / DMZ）ネットワーク
  - ✓ ITシステムと対話するシステム（例: ネットワーク管理, ヒストリアン, アンチウイルス, DNS, パッチ管理, DHCP）
- Level 2.5: 下流DMZ
- Level 2: エリア監視制御/プロセス*
  - ✓ ITシステムと対話し, 制御ネットワークからデータを制御および取得するシステム（HMI, SCADAマスター, MTU, エンジニアリングワークステーションなど）
- Level 1: コントロール
  - ✓ フィールドデバイス（アクチュエーターやセンサー）とプロセスネットワーク（RTU, PLC）の間でデータを収集および送信するシステム
- Level 0: フィールド/プロセス**
  - ✓ 閉じたネットワーク（つまり, 有線, シリアルケーブル, ファイバーリング, 独自のプロトコル）によってRTUやPLCに直接接続されたアクチュエーターとセンサー

* プロセスビューとは異なるプロセスの概念
** プロセスビューと同じ概念

# ONIC 2024 本会議- OT関連セッション

- 13:30
  - 工場に求められるセキュリティ「セキュア生産」の取組み
  - 日本電気株式会社　淵上 真一 様
- 14:30
  - スマートビルに見るオープン化の取り組み
    ～BIM・ビルOS・デジタルツイン～
  - 株式会社竹中工務店　政井 竜太 様
- 17:30
  - NTTコミュニケーションズにおける制御システムセキュリティの取組み
  - NTTコミュニケーションズ株式会社　加島 伸悟様


# Thank You

Nozomi Networksは, 世界の重要なインフラ, 産業, 政府機関をサイバー脅威から保護することで, デジタル変革を加速させます. 当社のソリューションは, OTおよびIoT環境において, 優れたネットワークと資産の可視性, 脅威の検出, 洞察を提供します. お客様は, 運用の回復力を最大限に高めながら, リスクと複雑さを最小限に抑えることができると, 私たちを信頼しています.

**nozominetworks.com**