NOZOMI NETWORKS

CPS セキュリティー基盤の中心であり続けるものとは？

その考え方とユーザー事例のご紹介

nozominetworks.com

CPS セキュリティー 3 つの観点

CPS 資産との共存と保護 ー 長期間でも陳腐化しない、継続的に価値を高める

ゼロ トラストで脅威モデリング

- 侵入から被害発生後まで
- 防御ラインは破られる
- 認証認可で防げる範囲
- **最終防御ライン – 攻撃現場**
- 有事の際の説明責任
- ビジネス継続計画

防御資産の網羅性を上げていく

- 可視範囲＋データ精細度
- 循環的な改善プロセス
- スモール スタート
- **拡張性（空間／時間）**
- 方向性の正しさを随時確認
- 数値指標、データ駆動

資産を保護し価値を上昇させる

- 資産の脆弱性リスクを算出
- 顕在リスクの即時対処
- リアルタイム脅威の検知／修復
- 規制準拠、監査適合

- **資産データをビジネス利用**
- 他データ セットと結合
- 業務プロセスで利用
- 金融アナロジー

CPS セキュリティーに関する誤解

閉域（エア ギャップ）環境は安全

「利便性を犠牲にして、安全性を担保している」

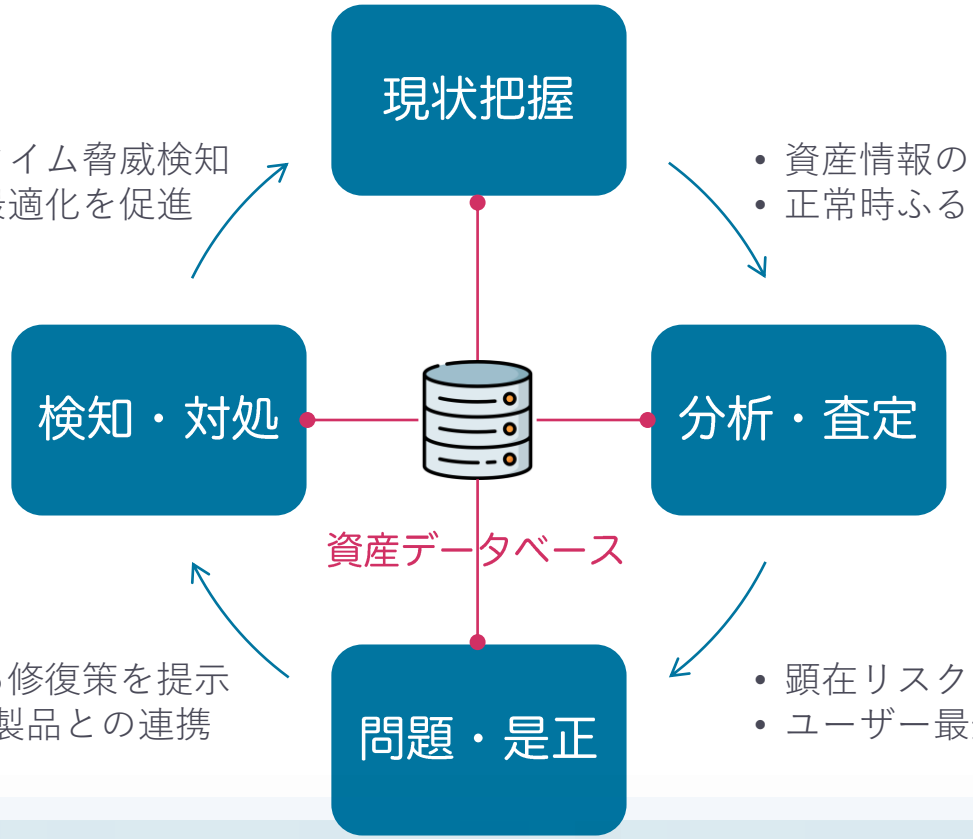
- 隠すこと自体が重要性を示唆
- 侵入後の攻撃容易性を示唆
- 内部の攻撃者を考慮していない
- 無線による侵入は回避していない

標的型攻撃を想定すると、閉域環境はシンプルに危険

CPS セキュリティー基礎 – 資産のライフ サイクル

課題の理解

- 資産を保護してデータ活用
- OT ↔ IT の相互活用は不可避
- 施設／設備の停止は不可

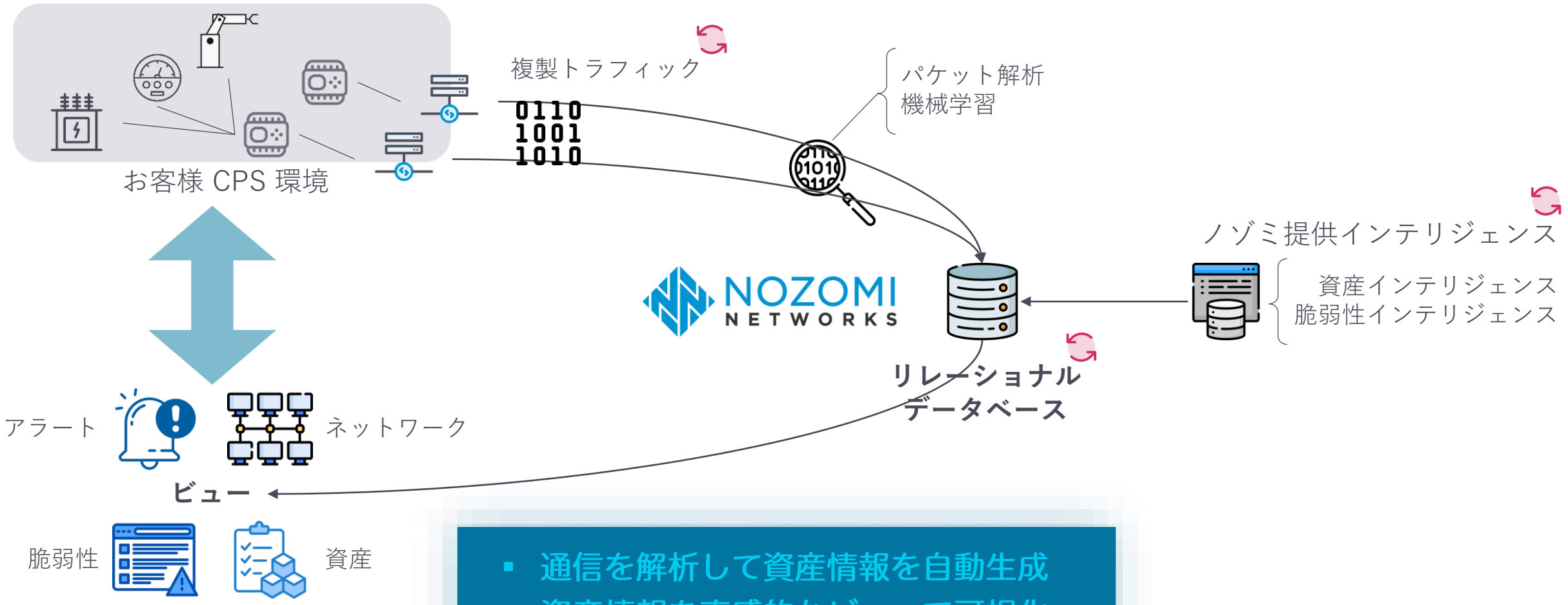


ソリューションの価値

- 資産情報を自動構築リスク算定
- 既存 OT 設備に影響なし
- 資産データをビジネス活用

資産情報は CPS セキュリティーの必須要素 かつ OT⇔IT 間の共通語彙

現状把握 – 資産状況と推移の可視化



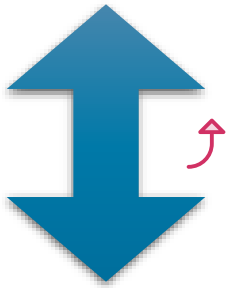
- 通信を解析して資産情報を自動生成
- 資産情報を直感的なビューで可視化

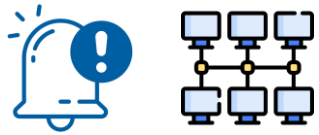
査定と是正 – 既知の問題への対処

- 製品が自動的に識別した顕在リスクに対処
- 監視基準となるベース ラインの妥当性チェック

査定と是正 – ユーザー最適化

お客様 CPS 環境





ビュー

NOZOMI NETWORKS

- 組織の知識ベース（命名規則、優先度、等）
- 組織内ポリシー（関連組織／職位、連絡先、等）

資産データベース

インテリジェンス情報

ユーザー ロジック

ワーク ブック

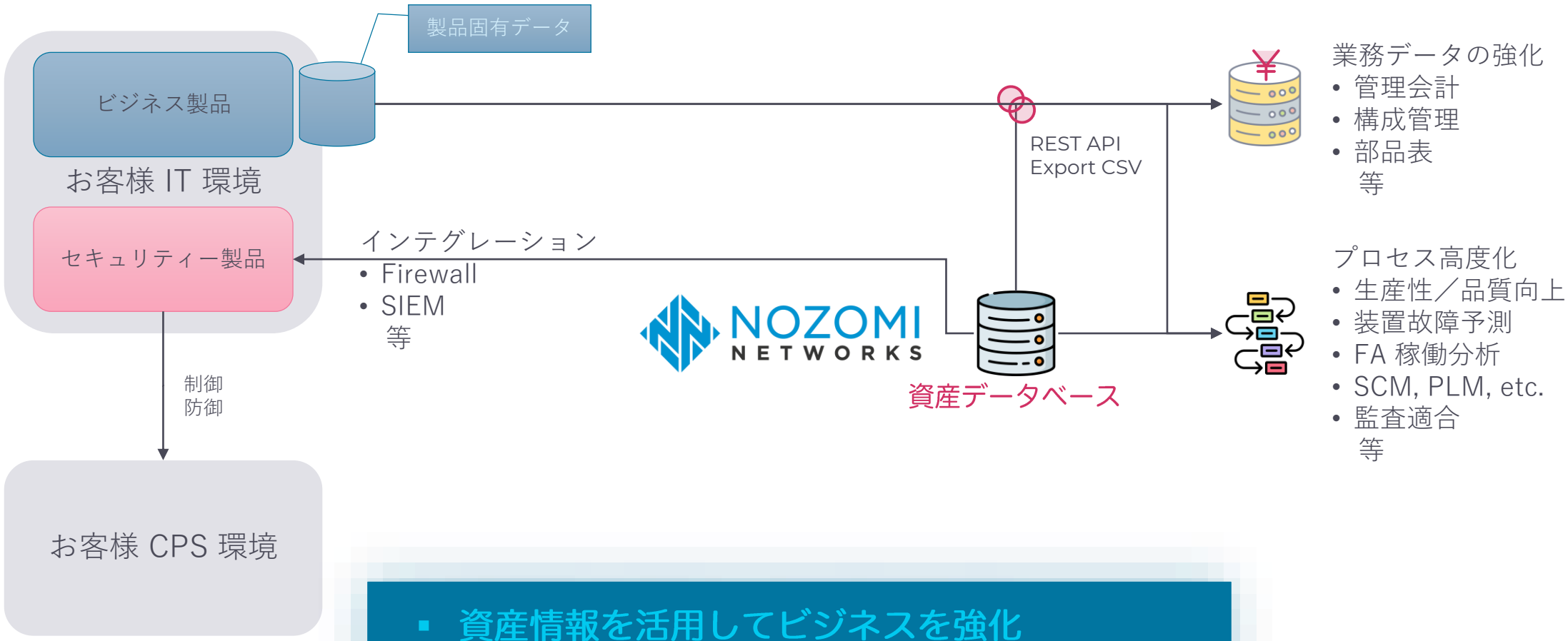
- 組織の知識ベースと調和した可視化
- 組織の対応ポリシー／フローに準拠

検知と対処 – 変化への対応、運用の最適化

- アノマリー検知（インシデント、新設／廃棄、等）
- 定常運用フロー（月次報告、年次監査、等）

- 検知イベントに想定フローで対応
- 潜在的リスクを予防的に検知

CPS セキュリティー拡張 – 資産データの発展的活用



- 資産情報を活用してビジネスを強化
- インシデントの回復は他製品と連携して対処

リファレンス アーキテクチャー

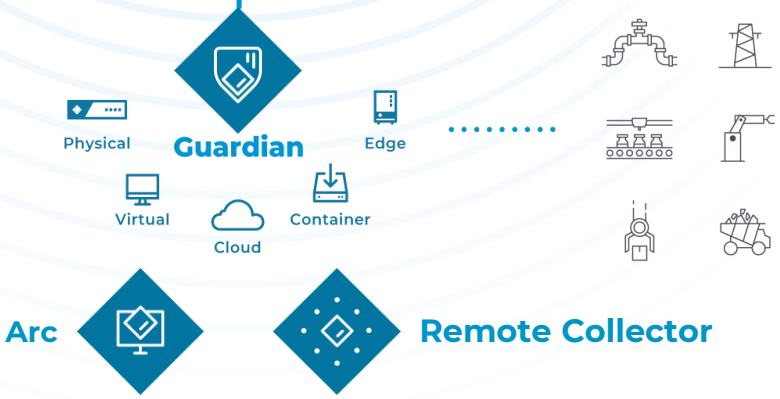
管理コンソール
SaaS

- グループ／リージョン一元管理
- AI アナリティクス
- 脆弱性スコアリング
- ライセンス／更新データ配布

管理コンソール
オンプレミス

- センサー集約
- センサーへのゲートウェイ
- 更新データ配布

センサー



- 通信トラフィック解析
- 資産データベース構築
- リスク検知と対処

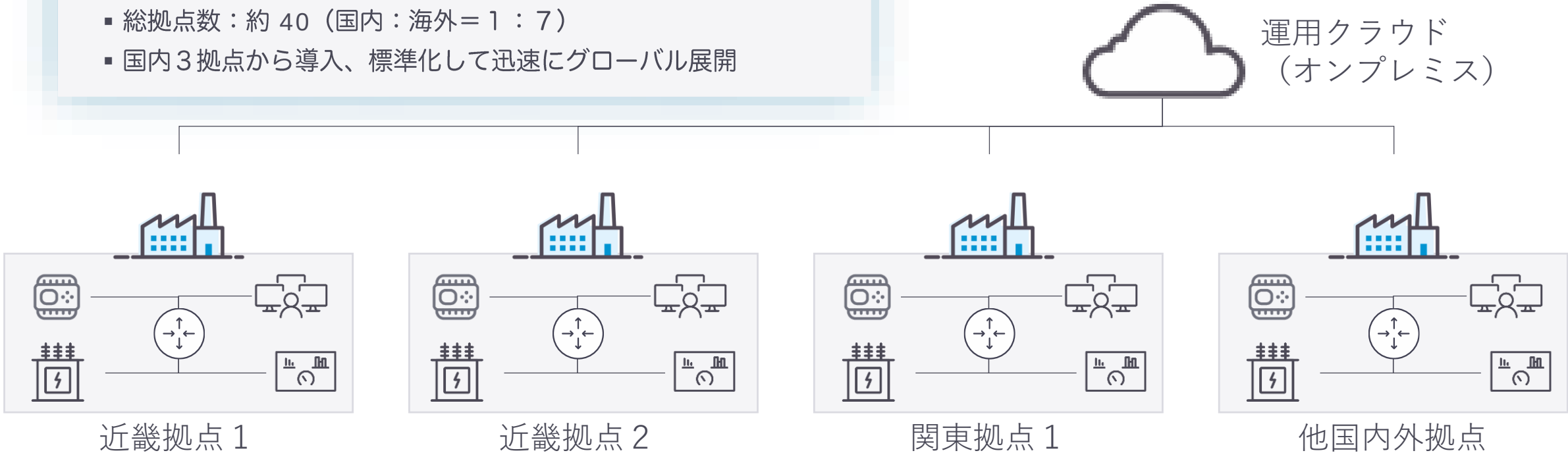
- エンド ポイント
- 小規模サイト

統合プラント防御基盤：導入前の課題

グローバル拠点、シームレス運用、標準展開モデル ― 国内化学系製造業

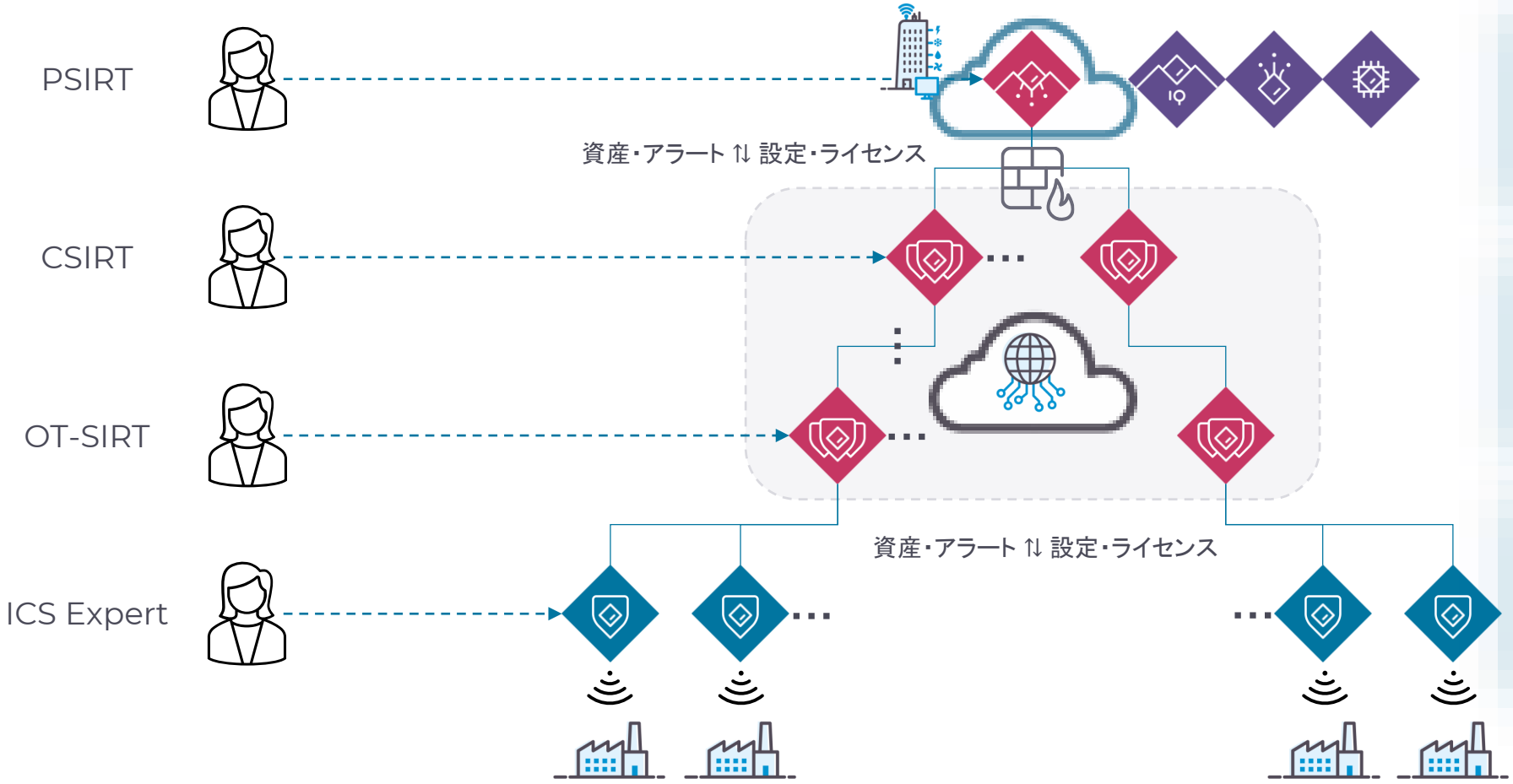
課題：全拠点の統一運用、自社運用クラウドの実装負荷大

- 既存 IT+OT 製品群（侵入検知＋資産管理＋他）の置き換え
- 総拠点数：約 40（国内：海外＝１：７）
- 国内３拠点から導入、標準化して迅速にグローバル展開



統合プラント防御基盤：技術階層アーキテクチャー

一貫性があり、適所適材で協力し合える、自組織に合った拡張ができる実装



グループ横断分析／オペレーション

- ダッシュボード、AI インテリジェンス
- ライセンス／構成情報の共通運用

複数拠点の最適化（運用クラウド）

- 組織／地域で拠点資産を階層化
- SaaS-センサー間ルーティング

拠点インフラ（ICS + 必須 IT）

- 資産データソースを収集して分析
- フォレンジックの実施現場

統合プラント防御基盤：ビジネス階層アーキテクチャー

資産データを利用する CPS 関連シナリオ

CPS ポータル

本社

グループ横断で戦略を共有、資源配分を最適化

CPS MSSP

DX 推進チーム

グループ横断で情報を共有、情報基盤を最適化

プラント

カンパニー工場

プラント資源の最適化、戦略／デジタルハブへのフィードバック

ミッション	平常時タスク	インシデント対応
経営連動 KPI 策定 製品安全性担保プラン策定 業務プロセス指針と窓口 システム費用の承認割付	業務プロセスの遂行指揮 KPI と戦略の相関性向上	有事プロセスの遂行指揮 社外への説明責任
KPI 実装 脅威モデリング／リスク査定 業務プロセスのデジタル化 プロジェクト標準／最適化	必要データ収集生成 改善フィードバック 共通基盤の実装整備 SOC/CSIRT 定常監視	関連データの収集整備 外部諮問機関との窓口
KPI 妥当性／分解／翻訳 脅威モデリング／リスク査定 生産・品質目標の達成 拠点システム最適化	プラント KPI 策定実装 脅威フィードバック CPS 基盤の実装整備	インシデント要因の改修 フォレンジック調査

統合プラント防御基盤：導入効果と今後の期待値

現在は 3 拠点スモールスタートの離陸直後、今後の方向性／可能性

システム標準化

- グループ内標準モデル確立
  - 階層アーキテクチャー
  - 統一オペレーション
- 横展開スピード向上

- 他セキュリティー基盤との連携
- 他バックオフィス基盤との連携
- ベスト プラクティスの継続改良

拠点資産の保護

- 顕在リスク資産の可視化
- 資産のリアルタイム保護

- イベント対応手順の最適化
- 潜在脅威／リスクの抽出／査定
- 標準／拠点固有規制への準拠
- 監査適合への貢献

投資対効果

- IT コスト削減
  - 製品統合、ライセンス最適消費
  - 構築期間／工数
- 人的リソースの最適化
  - グループ内 IT 人員の再組織化

- 拠点収支とリンクした KPI 策定
- キャッシュ フローの形成
  - 資産数による費用の按分
  - 業務貢献をベースに予算割当
- 資産価値の増大
  - 資産データの業務活用

CPS 防御ソリューションまとめ

1. CPS 防御には無停止／長期稼働の配慮が必須
2. ゼロ トラストで脅威を想定し対策しておく
3. 対策の中心は資産、自動的に最新に保つ仕組みを
4. 資産の価値を高めるデータ利活用を追求しましょう
5. 拠点の拡張が容易なソリューションか検討を

nozominetworks.com

Thank You

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

Nozomi Networks – CPS セキュリティー リーダー

2013 年 2 人の OT セキュリティー & AI 研究者がスイスで共同設立

1,000+
世界の総顧客数

115,000,000+
世界で管理する資産数

96 %
顧客の契約更改率

¥ 150,000,000,000
企業評価額

2018 年より日本で事業開始、2026 年に三菱電機グループ企業へ

三菱電機グループ企業として

以下の方針を堅持しつつ、日本市場へ長期的にコミットしていきます：

「企業文化の維持」– 企業理念、経営方針、組織人事は変更はなし

「製品戦略の継続」– 開発体制、製品ブランド／ロードマップは変更なし

「経営戦略の独立」– マーケティング／営業戦略は現体制下で立案する

「シナジーの創出」– グループ企業が保有する優位性は積極的に相互活用する

Transparency + Integrity = Trust

“

MITSUBISHI ELECTRIC

Nozomi は年平均成長率 (CAGR) 33% という高い成長性と、7割を超える粗利率を背景とした強い収益基盤を有している、グローバル トップ クラスの OT セキュリティ ソリューションを提供する会社です。”

漆間 啓, 三菱電機株式会社 執行役社長

https://www.nozominetworks.com/press-release/nozomi-networks-enters-next-phase-of-growth-as-mitsubishi-electric-completes-acquisition

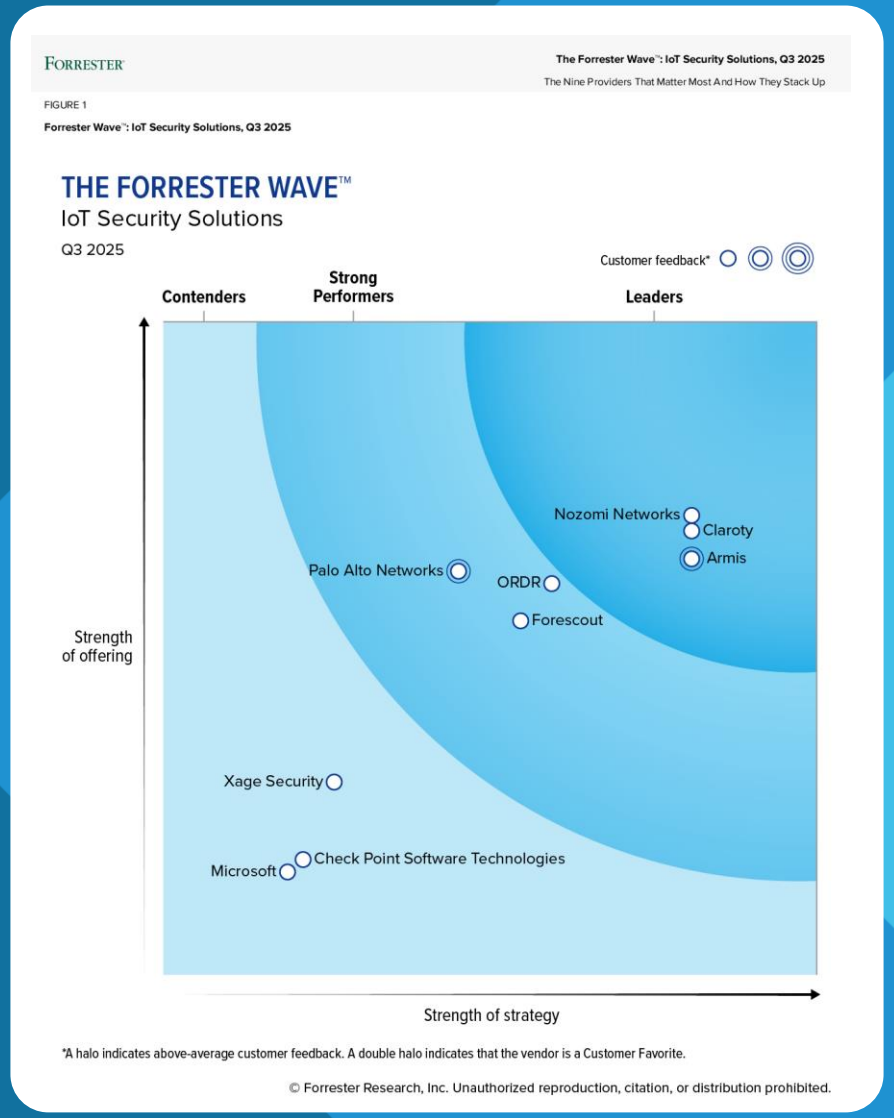
A Leader. Again.

2026 Gartner® Magic Quadrant ™ for CPS Protection Platforms

NOZOMI NETWORKS

A Leader

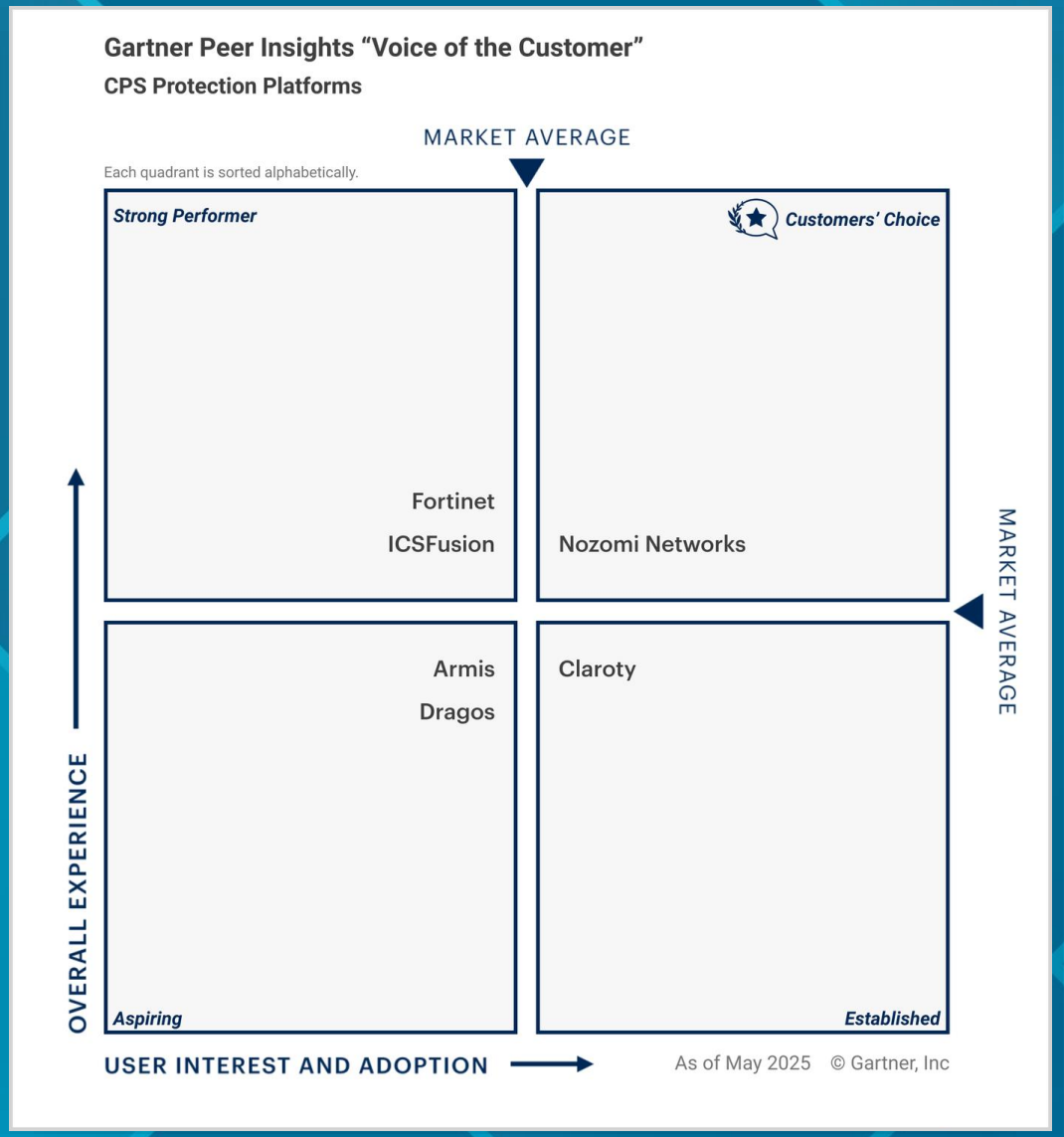
In The Forrester Wave™: IoT Security Solutions, Q3 2025



NOZOMI NETWORKS

A Customers' Choice

2025 Gartner® Voice of the Customer for Cyber-Physical System Protection Platforms



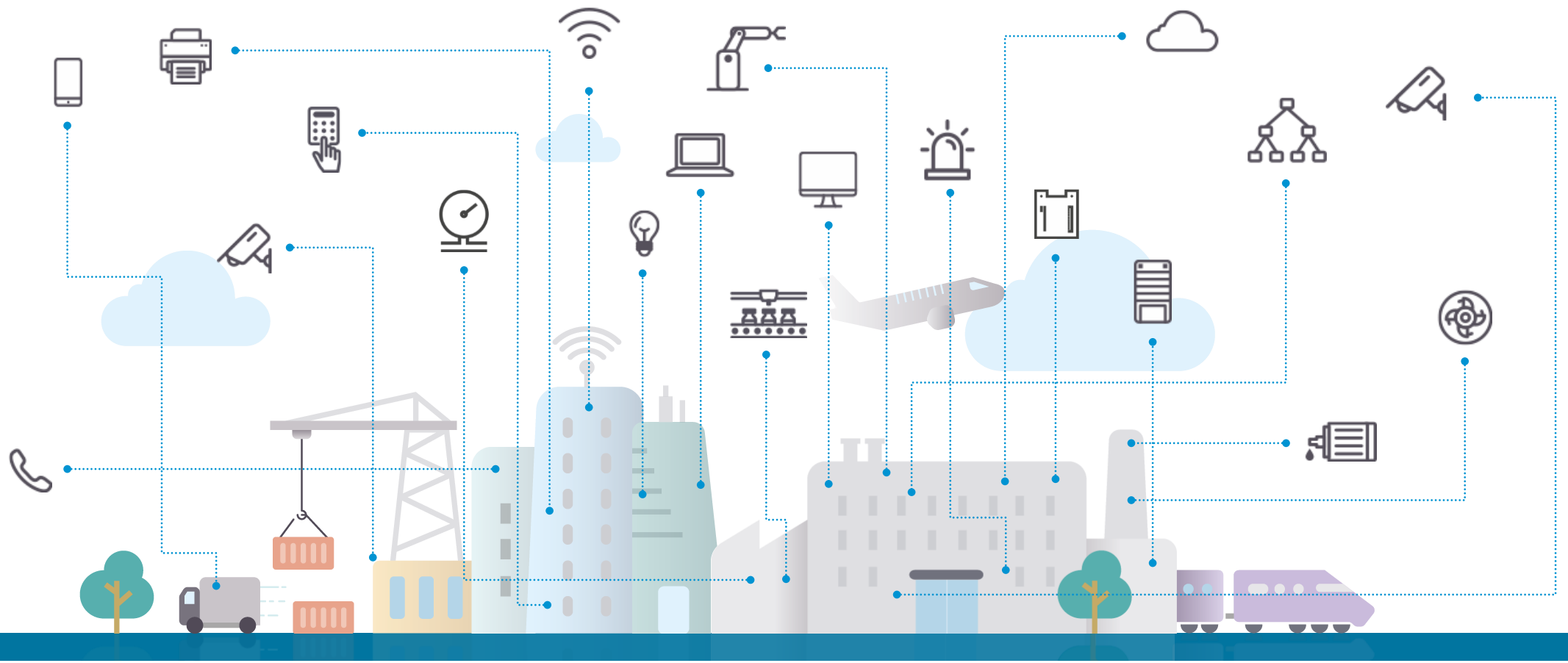
NOZOMI NETWORKS

CPS – Industry 4.0, スマート環境の舞台

守るべき**モノ**が稼働し IT 制御が効いていないシステム – *x* 施設、*y* 設備

運輸送
病院
工場
ビル
自治体
・・・

車輌 | 船舶
発送電
エレベーター
公共設備
IoT デバイス
・・・



CPS セキュリティー脅威の現況

334

公開されたインシデント数 – モノへの直接攻撃, 2010 - 2025*

$1M

ランサムウェアの平均要求金額, 2025*

1152

公開されたランサムウェア被害企業数, 2025*

$3M

ランサムウェアの平均被害金額, 2025*

*データ出典：*Nozomi Networks, Waterfall Security, Sophos, NetDiligence*

OT vs IT

	IT	OT
セキュリティーの優先事項	データの漏洩と損失の防止	人の安全、資産の継続稼働
システム稼働の性質	多種多様、遅延や再起動に一定の理解	リアルタイム、遅延や再起動は想定外
システムの想定耐用年数	5 年程度	10 年以上
サイバー セキュリティー対応	十分なリソースが配分されやすい	リソース不足が常態
ゼロ トラスト	通信経路で信用しない、常に認証／最小権限	認証がない場合も多い
ネットワーク プロトコル	相互運用性が高い、関連情報が豊富	ベンダー固有が多い、関連情報が少ない
システム更新	緊急対応も可能、標準化・自動化が進む	事前計画が必須、サポート切れも想定内
システムへの疎通性	接続元／先間の疎通あり、接続方法も簡易	閉域環境が多い、環境固有の接続方法

プラットフォーム全体像

管理コンソール

VANTAGE
- *SaaS*
- *FIPS-compliant*

CENTRAL MANAGEMENT CONSOLE
- *On-Premises*
- *FIPS-compliant*

Nozomi Networks AI Engine

センサー

NETWORK SENSORS

GUARDIAN
- *ANSSI-certified*
- *FIPS-compliant*

REMOTE COLLECTOR

GUARDIAN AIR

ENDPOINT PROTECTION SENSORS

ARC

ARC EMBEDDED

インテリジェンス

- VANTAGE IQ
- SMART POLLING
- ASSET INTELLIGENCE
- THREAT INTELLIGENCE
- TI EXPANSION PACK POWERED BY MANDIANT

センサーの配置

Guardian
- スイッチ／ルーターの SPAN / ミラーポート
- ネットワーク TAP
- 上記に類する仮想／アプライアンス基盤

Guardian Air
- ワイヤレス可視化

Arc
- PC ベースの ICS システム

Arc Embedded
- 対応機器 (MELSEC PLC / Schneider RTU)

Remote Collector
- 小規模環境
- 環境上の制約から **Guardian** の配置が困難