スマートファクトリーを推進する上で避けては通れないOTセキュリティを3つのポイントから攻略

東京エレクトロン デバイス株式会社

CN BU　CN営業本部 アカウント第二営業部
インサイドセールスグループ
グループリーダー
山内 瑶太

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Agenda

- スマート化する工場
  - 工場の課題を解決するスマートファクトリー
  - 進むスマート化、進まないOTセキュリティ
  - セキュリティ脅威による影響
- OTセキュリティガイドラインの進め方
- TED OTセキュリティソリューションご紹介

onnect Beyond

スマート化する工場

工場における様々な課題

人手不足

高齢化社会の進行や若年層の
製造業離れによる、労働力の低下

技術の継承

経験豊富な技術者が退職し、
ノウハウが継承されない

生産効率

プロセスの非効率化による
生産性の低下

品質管理

品質管理に課題があり、
歩留まりを上げられない

コスト削減

物価の向上に伴い、
コスト削減に苦戦している

規制の厳格化

環境保護や省エネの観点から
規制がより厳しくなる

スマート化のレベル感

レベル⓪

従来の工場

情報がまだ活用されていない。

レベル①

データの収集・蓄積

有益な情報を見極めて収集して状態を見える化し、得られた気付きを知見・ノウハウとして蓄積できる。

レベル②

データによる分析・予測

膨大な情報を分析・学習し、目的に寄与する因子の抽出や、事象のモデル化・将来予測ができる。

レベル③

データによる制御・最適化

蓄積した知見・ノウハウや、構築したモデルによる将来予測を基に最適な判断・実行ができる。

レベル④

動的な自律制御

複数の工場または事業者が接続し、解析結果や予測を基に、各主体が自律的かつ動的に制御できる。

従来の工場

スマートファクトリー

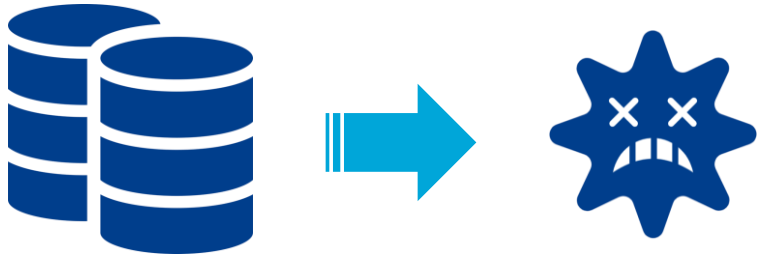
経済産業省「スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査」（2021年）を基に作成

進むスマート化、進まないOTセキュリティ

スマート化を進めることで、様々な課題が解決される。しかし……、

インターネットに接続するということは

侵入経路を開くことに繋がる



データを収集して蓄積するということは

攻撃の対象になることに繋がる

スマート化と共にOTセキュリティも同時に進めなければ、リスクを受け入れることになる。

工場システムにおいてセキュリティ脅威により生じる影響の例

- 製品事業の伸長や事業/生産の継続（BC：Business Continuity）への影響
- 工場の安全確保（S：Safety）、製品の品質確保（Q：Quality）、納期遵守・遅延防止（D：Delivery）、コスト低減（C：Cost）への影響
- 工場システム及び機器の正常動作確保、適正なフィードバック制御の実現の妨害
- 製品や生産（ノウハウ）に関わる情報やデータの外部漏えい
- 自社工場の機器を踏み台にした、エンジニアリングチェーン、サプライチェーン、バリューチェーンの連携先へのセキュリティ問題の拡大
- 意図せず製品に内包された不正な部品や悪意のある機能（マルウェア）による、外部からの不正な利用・制御や、製品の稼働の妨害、製品利用者の情報の外部漏えい
- 設備の規定外の作動による従業員の健康への影響
- 設備の規定外の作動に端を発した災害による近隣住民の生活への影響

経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」（2022年）を基に作成

OTセキュリティに悩む管理者の強い味方

工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（通称：OTセキュリティガイドライン）

工場システムのスペシャリストが集結し、制定したもの。

このガイドラインを元にセキュリティ対策が立案・実行されることで、

（１）工場のBC/SQDCの価値がサイバー攻撃により毀損されることを防止。

（２）セキュリティが担保されることでIoT化や自動化が進み、
多くの工場から新たな付加価値が生み出されること。

を狙いとしている。

OTセキュリティガイドラインの進め方

OTセキュリティガイドラインの進め方

ステップ1：内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
  セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2** 業務の整理
- **ステップ1-3** 業務の重要度の設定
- **ステップ1-4** 保護対象の整理
- **ステップ1-5** 保護対象の重要度の設定
- **ステップ1-6** ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7** ゾーンと、セキュリティ脅威の影響の整理

ステップ2：セキュリティ対策の立案

- **ステップ2-1** セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策
①ネットワークにおけるセキュリティ対策
②機器におけるセキュリティ対策
③業務プログラム・利用サービスにおけるセキュリティ対策

(2)物理面での対策
①建屋にかかわる対策
②電源／電気設備にかかわる対策
③環境(空調など)にかかわる対策
④水道設備にかかわる対策
⑤機器にかかわる対策
⑥物理アクセス制御にかかわる対策

ステップ3：セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策

(1)ライフサイクルでの対策
①運用・管理面のセキュリティ対策
A)サイバー攻撃の早期認識と対処（OODAプロセス）
B)セキュリティ対策管理(ID/PW管理、機器の設定変更など)
C)情報共有

②維持・改善面のセキュリティ対策
・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
・組織・人材のスキル向上（教育、模擬訓練等）

(2) サプライチェーン対策
・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認

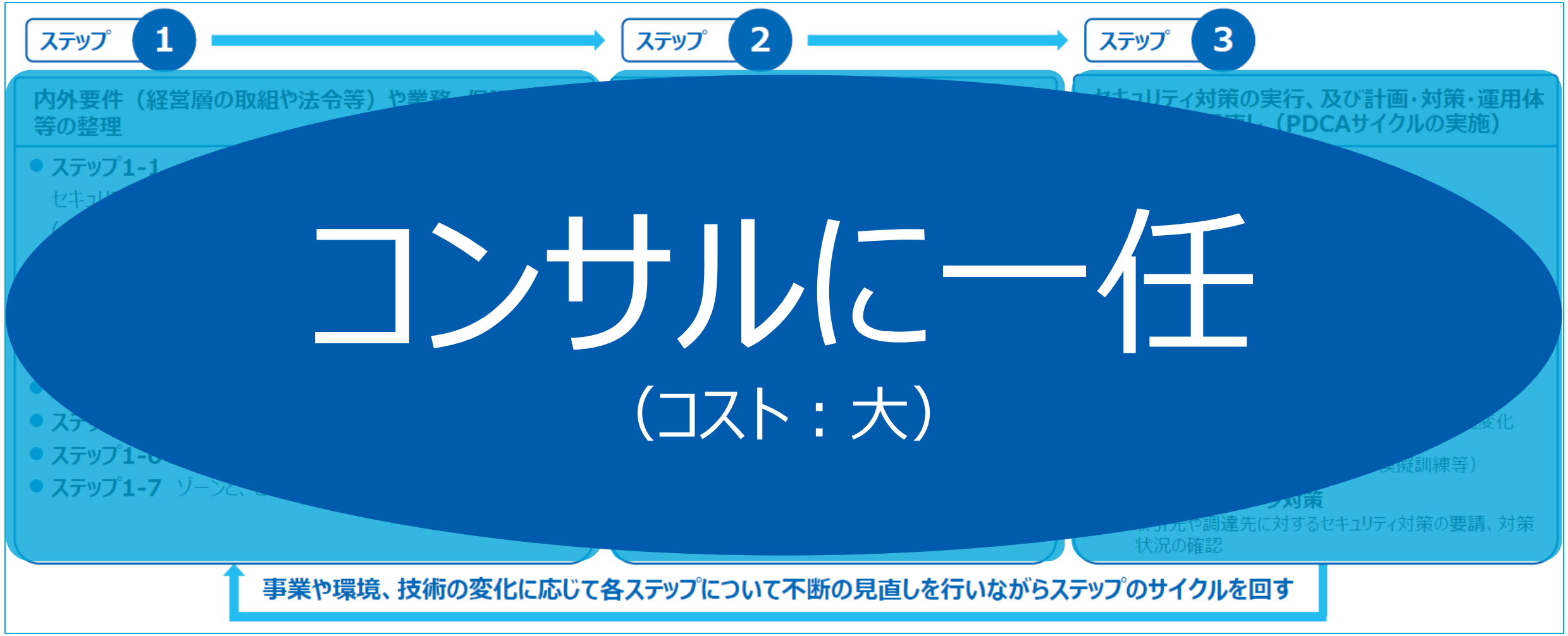
事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」概要資料（2022年）より

OTセキュリティガイドラインの進め方

経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」概要資料（2022年）より

OTセキュリティガイドラインの進め方（パターン１）

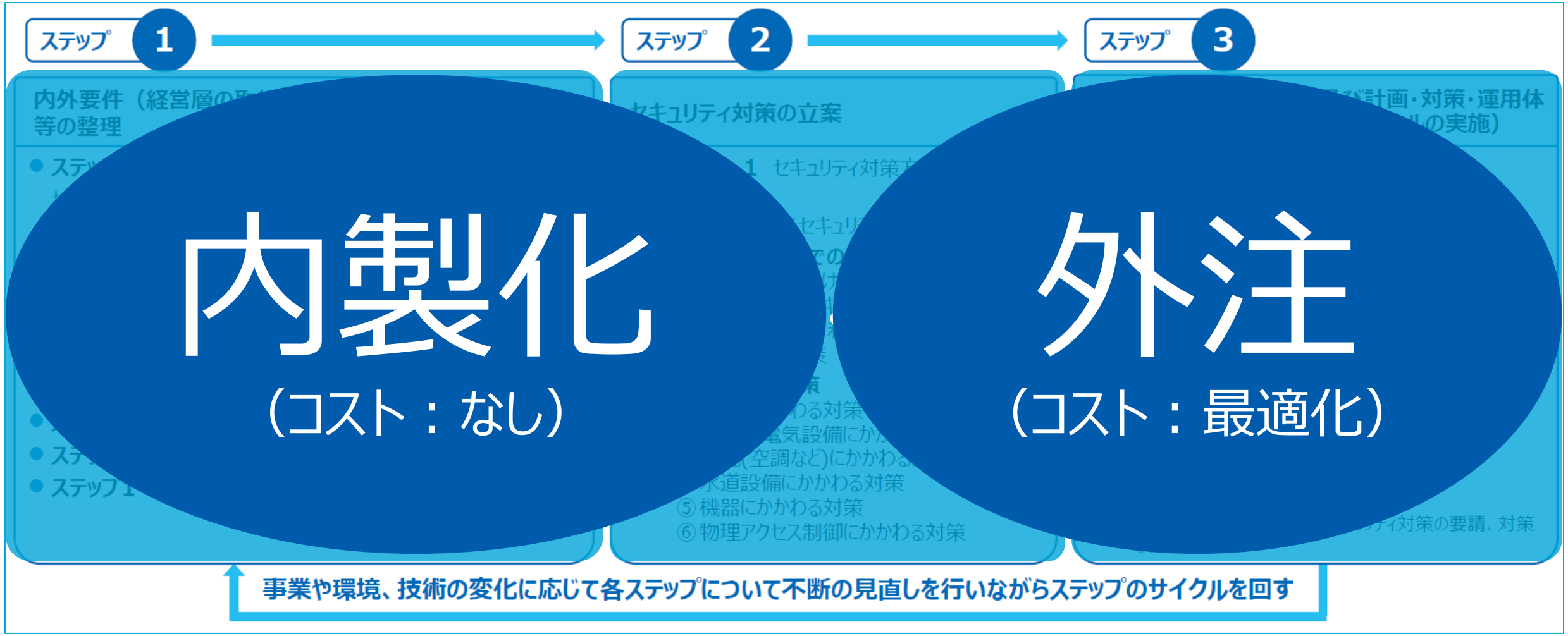


コンサルに一任

（コスト：大）

経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」概要資料（2022年）より

OTセキュリティガイドラインの進め方（パターン２）



経済産業省「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」概要資料（2022年）より

セキュリティ対策の立案・実行における３つのポイント

システム構成面でのセキュリティ対策

① ネットワーク

② 機器

③ 業務プログラム・利用サービス

×

考慮すべき３つのポイント

① 侵入防止

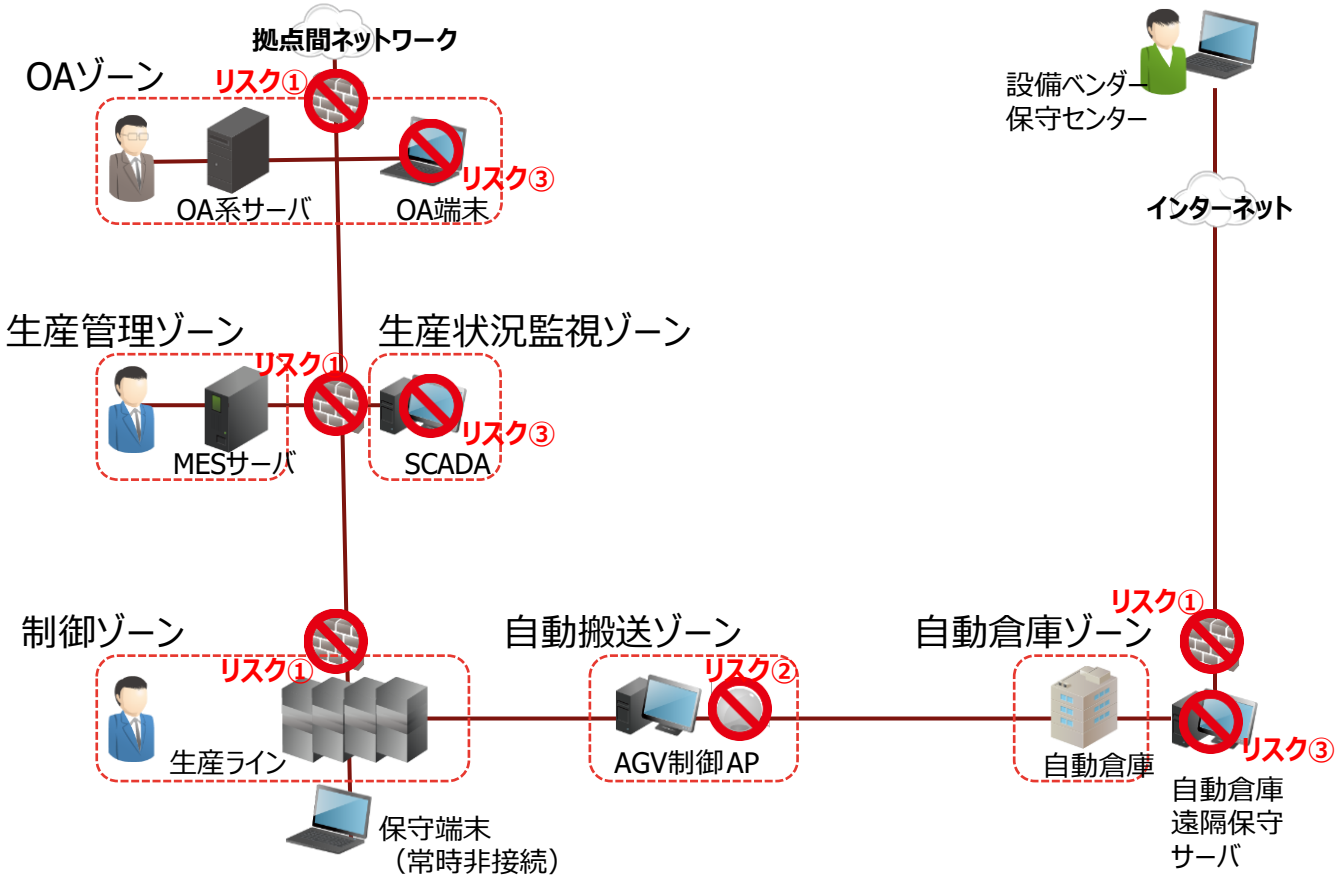
② 活動抑止

③ 運用

TED OTセキュリティソリューション

TED OTセキュリティソリューションが保護するエリア

想定システム（ゾーン）



侵入防止と活動抑止

・フェイズ① ネットワーク/機器/
業務プログラム・利用サービス

・フェイズ② ネットワーク

・フェイズ③ 業務プログラム・利用サービス

運用

・セキュリティ専門家 TED-SOCによる
24時間365日の監視・運用支援

TED OTセキュリティソリューション

フェイズ①

■FortiGate
・各ゾーンの境界防御

■FortiNAC
・通信の可視化

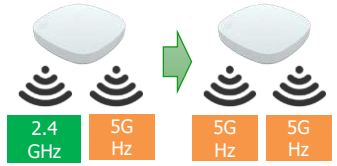
■FortiAnalyzer
・セキュリティログの分析

FORTINET

フェイズ②

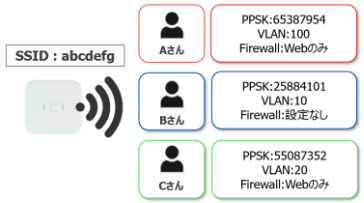
■Extreme AP
・安定した通信品質

Dual 5GHz



すべてのクライアントの通信を5GHzで利用することで安定した通信品質を提供

プライベートPSK認証



802.1x 認証と同等レベルのセキュリティ
（RADIUSサーバー不要）

Extreme networks

フェイズ③

■ランサムウェア対策
・振る舞い検知
・端末の自動隔離
・ロールバック

SentinelOne

SOC（Security operations center）

■監視サービス
・死活監視（リモート）

■運用サービス
・インシデント発生時の対応
・設定変更の代行（オプション）
・定例会の開催（オプション）

東京エレクトロン デバイス

OTセキュリティ対策のまとめ

現状把握は内製化

セキュリティ対策のキーワード
侵入防止と活動抑止を抑える

運用の内製化にはセキュリティの専門家が5人必要
外注が得策

onnect Beyond

ご清聴いただき、ありがとうございました。