工場セキュリティガイドラインを活用した調査結果と見えてきた国内製造業の課題

Fortinet Japan G.K.
OT Business Development

世界No.1のサイバーセキュリティ企業

55.9億ドル
2022年 取扱高
急成長、確かな収益性

70.5万以上
顧客数
顧客からの膨大なインプット

1,140万台以上
累計出荷台数
ファイアウォール世界シェア1位

1,290件
特許数
トップイノベーター

50以上
統合されたファブリック製品
攻撃対象領域を広範囲にカバー

ASIC
自社開発プロセッサー
ハイパフォーマンス

2023年9月30日時点

FORTINET

Introduction

FS Eng (TÜV Rheinland, #18131/19, Safety Instrumented System)

フォーティネットジャパン合同会社　OTビジネス開発部
藤原 健太(Kenta Fujihara)

これまでOT、製造業を中心に活動。レイヤーゼロからICSまで幅広い経験と知識を有する。システムエンジニアからキャリアスタートし、現場機器、関連する予兆保全・資産管理、無線ソリューションの市場開発に従事。直近では製造業の機能安全、リスクに関する業務を経験、これまでに多くのイベント、セミナーでの講演、業界誌への執筆を経て現在に至る。

Mission：「OTサイバーセキュリティを通してIT/OTの橋渡し役を担う！」

＜経歴＞

外資系 エナジーマネジメント&オートメーション企業（5年）
安全計装システム(SIS) 営業、機能安全リスクアセスメント、OTセキュリティビジネス市場開発

外資系 オートメーション企業（8年）
現場機器(調節弁他)、IoT機器(無線計装)、関連ソフトウェアに関する技術営業、市場開発

日系 オートメーション企業（4年）
制御システム(DCS) アプリケーションシステムエンジニア

工場セキュリティガイドライン チェックリストについて

工場セキュリティガイドラインチェックリストについて

ガイドライン付属のチェックリストを活用したWeb診断の仕組みを無料公開

カテゴリ	サブ項目	番号	確認項目 V1.0	現状評価	ヒアリング回答
組織	ガバナンス体制	1-1	工場システムのセキュリティの必要性について、決裁者（工場長、カンパニー長等）又は経営層が認識を持っており、十分な予算・人員配置などの協力を得られる状態にある。	2：部分的に実施している	認識はあるが、予算・人員の確保は難しい（途上）
	ガバナンス体制	1-2	工場システムのセキュリティ対応について情報システム部門や生産関係部門等の関係する部署・部門との間で協力・連係態勢が取られている。	2：部分的に実施している	FSIRT体制を検討中。現時点では、何かあればCSIRTが対応。
	ガバナンス体制	1-3	工場システムのセキュリティ検討組織や、担当者が準備されており、責任と業務内容が明確化されている。	2：部分的に実施している	（１－２と同じ）FSIRT体制を検討中。現時点では、何かあればCSIRTが対応。
	ガバナンス体制	1-4	事業継続計画（BCP）が策定されており、責任者が準備されていて、責任と業務内容		のみ、遠隔バックアップ、冗長構成実施
	現場教育	1-5	工場セキュリティに関する脅威の動向など り、勉強会を開いたりするなどの現場教育		リティは全社教育実施。工場セキュリティに特化したもの
運用	定期評価	2-1	システムが侵害・停止した場合の事業に	2：部分的に実施している	のみ、遠隔バックアップ、冗長構成実施（1-4と同じ）
	ルール策定・管理	2-2	工場システムにおける専用のセキュリティポリシーが規定されていて、認知されている。	1：実施していない	工場セキュリティのポリシを作成中
	ルール策定・管理	2-3	工場内のシステムからの電子メールやインターネットアクセスはポリシによって禁止している。	4：実施し、管理手順を文書化・自動化している	FW運用部門内で内部ルール化して運用。
	インシデント対応	2-4	工場システムにおけるセキュリティの異常発生時の責任者の対応が明確化されている。	2：部分的に実施している	FSIRT体制を検討中。現時点では、何かあればCSIRTが対応。
	インシデント対応	2-5	工場システムにおけるセキュリティの異常発生時の対応方法を現場作業者が理解し、訓練を実施している。	1：実施していない	
	資産管理	2-6	情報資産の検出ツールを利用するなど、工場ネットワークに接続している機器（サーバ、クライアント端末、ネットワーク機器、設備等）の台帳を作成し、システム構成図を作成している。	3：実施している	PCの台帳管理は実施しているが、１割程度が未登録。システム構成図は無い。
	資産管理	2-7	工場内に無線LANを導入している場合、ネットワークへの接続を許可された機器の台帳を作成し、無許可の機器を拒否	3：実施している	独自のWiFiはなく、生シ管理分は仕組みあり
	定期評価	2-8	システムへの侵入を可能とする攻撃手法 る、又は緩和策を講じている。（脆弱性 診断やペネトレーションテスト（侵入可否 ど）のモデル情報やファームウェア情報の 等）		は実施していない。IT/OT間にあるFW(IPS)で通信を
	ルール策定・管理	2-9	工場内に外部記録媒体（USBメモリ、フラッシュデバイス）やポータルメディアの利用・持込みに関するルールを定め、運用している。	3：実施している	田電として、私物の記録媒体禁止のルールあり。業務用の記録媒体については、台帳管理と持ち込み時のウイルスチェックのルールあり。
	ルール策定・管理	2-10	工場内のシステムのパスワードの強度や有効期限等のパスワード設定の考え方を定めたルールがある。（安全に関わる緊急対応を必要とする表示器などの端末は除く）	1：実施していない	
	ルール策定・管理	2-11	工場内のシステムへのアクセス権で使用していない古いアカウント（退職者・異動者など）を速やかに削除している。	2：部分的に実施している	共用アカウントになっている。一方で設備起動には社員証が必要。
	ルール策定・管理	2-12	工場ネットワーク内の接続機器について、事前にそれらがウィルスに感染していないことを確認する手順がある。	1：実施していない	ツール導入予定
	インシデント対応	2-13	システム機能の完全な復旧を想定したバックアップを行い、バックアップデータは保護された場所に格納するとともに、定期的にバックアップデータからの復旧テストを行っている。また、その手順が明確化されている。	2：部分的に実施している	一部のサーバのみ、バックアップは対応済。復旧訓練はしていない。
技術	端末保護	3-1	インストールできる端末にはアンチウィルスソフト又はアプリケーションホワイトリスト（許可リスト）を導入し、インストール不可能な端末では何らかの代替策（USB型のアンチウィルスなど）を導入している。	1：実施していない	ホワイトリストのツールの導入を検討している。（アンチウィルスSWは、パターンファイル更新のためだけにサーバ接続が必要になる、また、OSが古いので、サポートされていない。）
	端末保護	3-2	アプリケーション／オペレーティングシステム（OS）の重大な脆弱性については可能な限り速やかにセキュリティパッチを適用		実施していない（OSが古くパッチがない、安定稼働優先でパッチ適 ある、など）
	端末保護	3-3	端末のオペレーティングシステム（OS）の 小限とし、未使用のサービスやポートは停		ビス、ポートが不明
	物理	3-4	工場の重要設備への物理的なアクセスに 行っている（例：監視カメラ、警報装置 への関係者の付添いなど運用面での代替策を講じている。		自体の入退室管理（登録が必要）をしているエリアも サーバ室の入退室は登録者のみ。
	ネットワーク	3-5	工場ネットワーク内において、セキュリティレベルに応じたネットワークセグメント管理を行っている（VLAN等）。	2：部分的に実施している	ITとOTは分離している。OT内は分けていない。
	ネットワーク	3-6	工場システムのリモートメンテナンスなどを目的とした外部からのインターネットアクセスが可能な場合、認証（２要素認証等）やリモートユーザ毎の接続対象機器の制限、接続可能時間の制限、メンテナンス期間外の機器接続等の異常検知、ネットワーク侵入防護などの保護対策を行っている。	3：実施している	社外からのアクセスは不可（FWで遮断）。社内からは登録端末のみリモートアクセス可能。
	ネットワーク	3-7	工場内のネットワーク（情報システムとの境界やリモートアクセスを含む）の不審な通信を特定するためのネットワーク検知／防護システムを導入している。	2：部分的に実施している	IT/OT間にあるFW(IPS)で通信を監視。
	ログ	3-8	工場内のシステムのログイン、操作履歴などのイベントログを取得している。それらのログは定期的に分析し、必要日数保存している。	2：部分的に実施している	ログ保存・分析を実施しているサーバもある（1台のみ）。
サプライチェーン	外部管理	4-1	工場システムのセキュリティ事故発生時に対応ができるよう、制御システムベンダ・構築事業者と連絡・連携体制を構築している	2：部分的に実施している	メーカとの保守契約は締結。（セキュリティに特化していない）
	外部管理	4-2	工場システムのメンテナンス等に関わる協 始時及び定期的に実施している。		
	外部管理	4-3	納品された工場システムに関するセキュリ 報が速やかに共有されるように、制御シ 制を構築している。		保守契約は締結。（セキュリティに特化していない）
	外部管理	4-4	サプライチェーン（協力会社、生産子会社など）における工場システムの脅威、影響度、対応状況（内部及び/または外部監査実施など）を把握できている。	1：実施していない	
	内部管理	4-5	納入する工場システム機器に対して、一定のセキュリティ基準を満たしているかを判定するプロセスや受入検査がある。	1：実施していない	
	内部管理	4-6	新規システム導入時の設計仕様要件にセキュリティに関する要求仕様が明確化されている。	1：実施していない	

組織的対策

運用的対策

技術的対策

サプライチェーン管理

- ○ 自組織に当てはまらない
- ○ 実施していない
- ○ 部分的に実施している
- ○ 実施している
- ○ 実施し、管理手順を文書化・自動化している
- ○ 実施し、外部環境変化に随時対応している

事前に簡易Web診断結果として
左記６項目から回答を受領、
回答結果よりA-Dでスコアリング

分析結果シートの見方

スコア	0～100	チェックシートの個別項目と回答(0-4)に重みづけをして、セキュリティ対策の状況をスコア化。全ての項目が「一部実施」の場合に約40%、「実施している」だと約60%となるように調整している。

評価	スコア	解説
A	80～	ほとんどの必要な対策が実施され、手順が文書化されている。リスクを十分低減できており、継続的な改善がなされている。
B	60～79	ほとんどの必要な対策が実施されているが、手順が文書化できていない。リスクを低減できているが、継続的な改善に課題がある。
C	40～59	ほとんどの必要な対策の実施が不十分。リスクが低減されておらず、セキュリティ侵害時の被害が大きいと想定される。
D	0～39	ほとんどの必要な対策が未実施。リスクが認識されておらず、セキュリティ侵害時の被害が大きいと想定される。

注意事項：この診断結果は、設問に対する回答をもとに作成した簡易的なものであるため、**回答者の主観により異なる結果が出る、実態と乖離があるなどの可能性**があります。より精度の高い診断を行うために、現地ヒアリング・通信モニタリング調査の実施をお勧めします。

一般的なセキュリティガイドラインチェックリストとの違い

一般的なセキュリティガイドラインチェックリストは、、、

- **情報資産に対する機密性保持を主目的としている**

  例) 製造業に対して工場に特化したセキュリティガイドラインの建付けがなく、情報セキュリティに関するガイドラインのみの為、無理やり工場側に適応している

  ⇒ **情報セキュリティのみならず“工場システム”や“運用ルール”目線でチェックリストが構成されている**

- **チェック項目が多い（100項目以上）分リスク把握が精緻な一方で実施に時間とコストがかかる**

  例)「全工場チェックするのに３年かかりました。。。〇がついている個所は対策済なので大丈夫です。」

  ⇒ **当ガイドラインチェックリストは32項目、〇/×ではなく実施度合いでレベル分けされている**

- **組織責任体制が整っている前提の要求項目となっている**

  例）NIST CSF 資産管理の要件 ⇒ 誰が管理するの？

  ⇒ **当ガイドラインチェックリストは「組織」カテゴリ要件で、まず責任体制の有無を確認できる**

これから工場セキュリティ対策にとりかかる企業に対してのリスク把握に有効

工場セキュリティガイドライン対象範囲おさらい

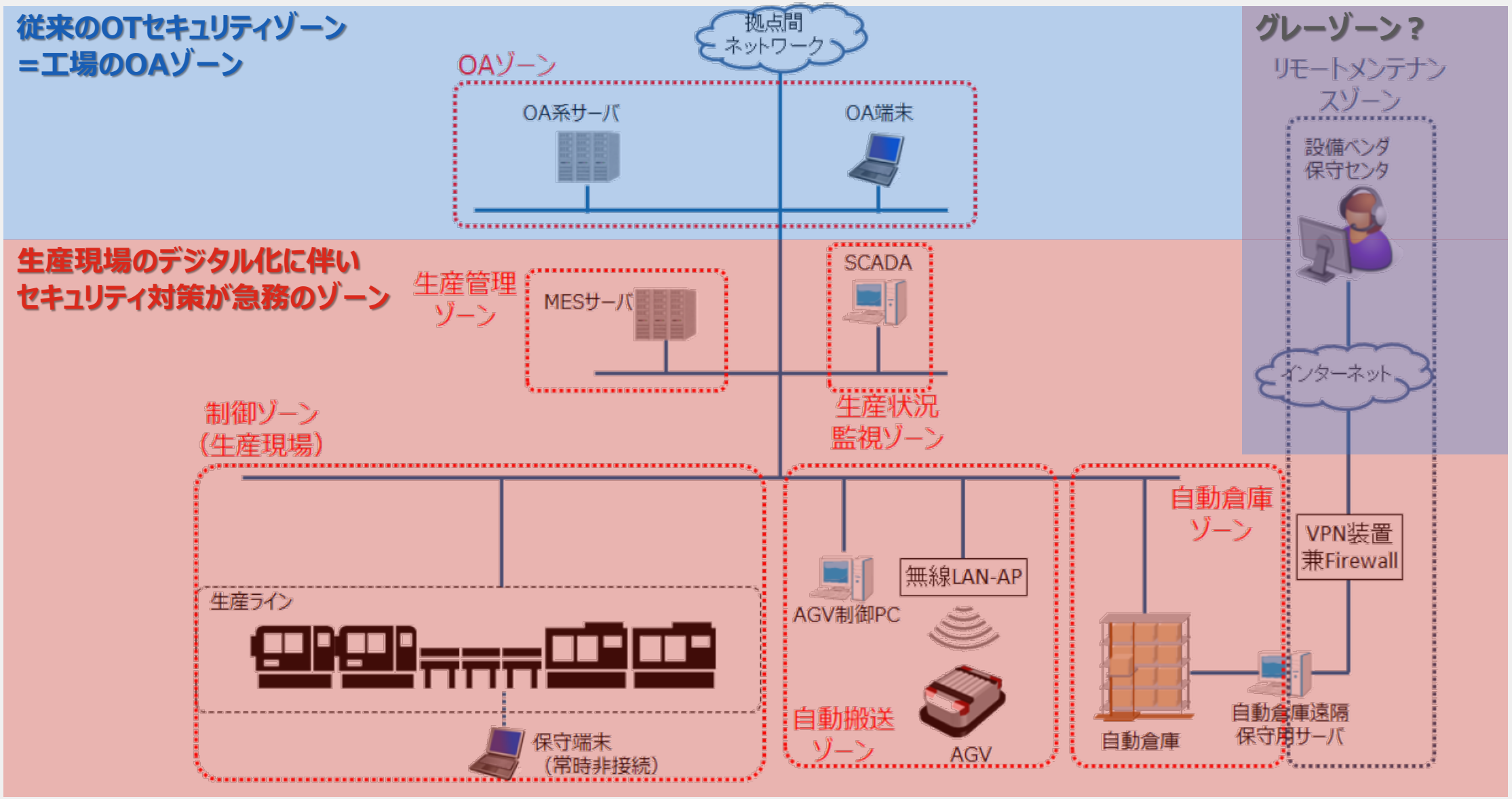


図 ゾーンの定義例 （工場セキュリティガイドライン概要編より抜粋）

チェックシートの分類について

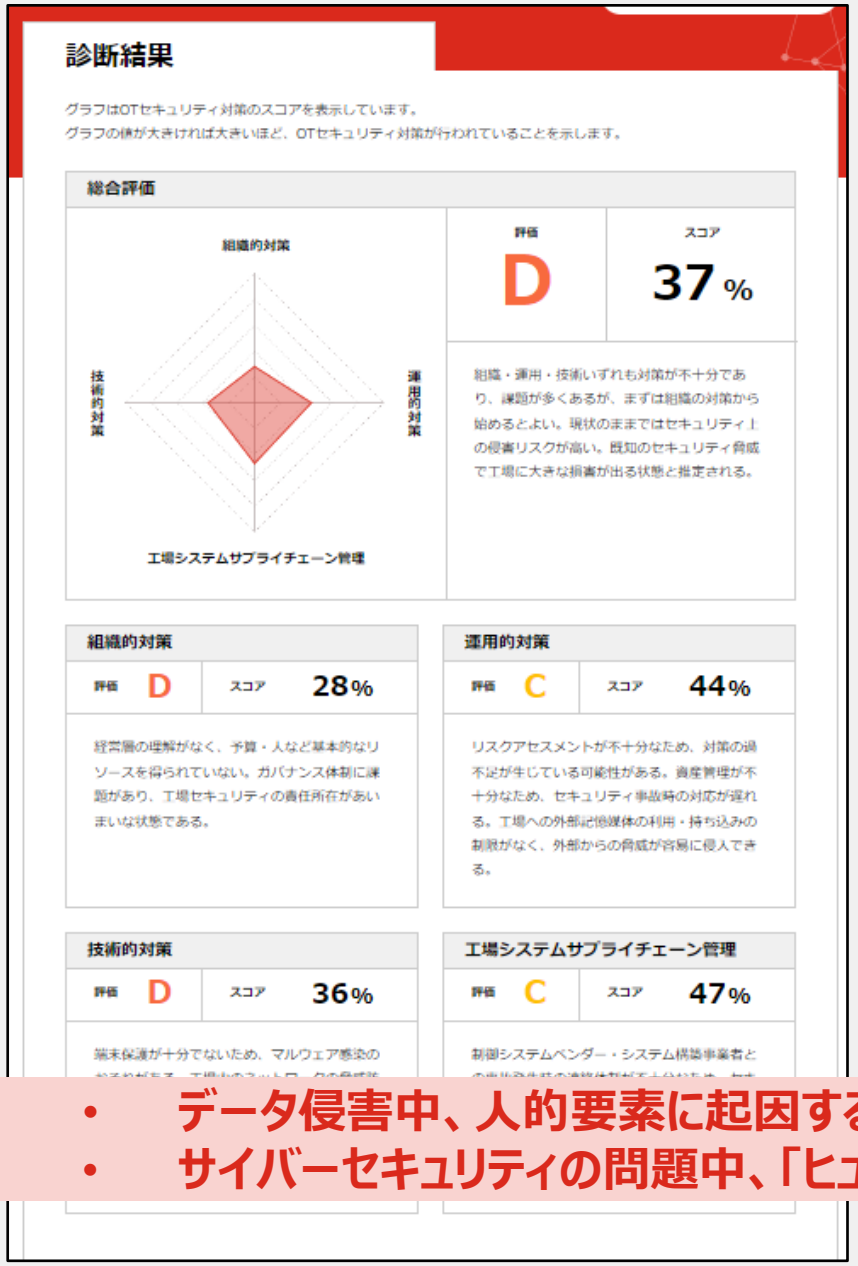
↓ フォーティネットで分かりやすくサブ項目毎に分類

大項目	サブ項目	チェックリスト項目
組織的対策（People）	ガバナンス体制	1-1,1-2,1-3,1-4
	現場教育	1-5,
運用的対策（Process）	定期評価	2-1,2-8
	インシデント対応	2-4,2-5,2-13
	資産管理	2-6,2-7
	ルール策定・管理	2-2,2-3,2-9,2-10,2-11,2-12
技術的対策（Technology）	端末保護	3-1,3-2,3-3,
	物理	3-4
	ネットワーク	3-5,3-6,3-7,3-8
	ログ	3-9
工場システムサプライチェーン（SCM）	外部管理	4-1,4-2,4-3,4-4
	内部管理	4-5,4-6

工場セキュリティガイドライン チェックリストを活用した調査結果

Web診断調査結果

Total：約317件（2023/12/08現在）


診断結果

グラフはOTセキュリティ対策のスコアを表示しています。
グラフの値が大きければ大きいほど、OTセキュリティ対策が行われていることを示します。

総合評価

組織的対策
技術的対策
運用的対策
工場システムサプライチェーン管理

評価 D　スコア 37%

組織・運用・技術いずれも対策が不十分であり、課題が多くあるが、まずは組織の対策から始めるとよい。現状のままではセキュリティ上の侵害リスクが高い。既知のセキュリティ脅威で工場に大きな損害が出る状態と推定される。

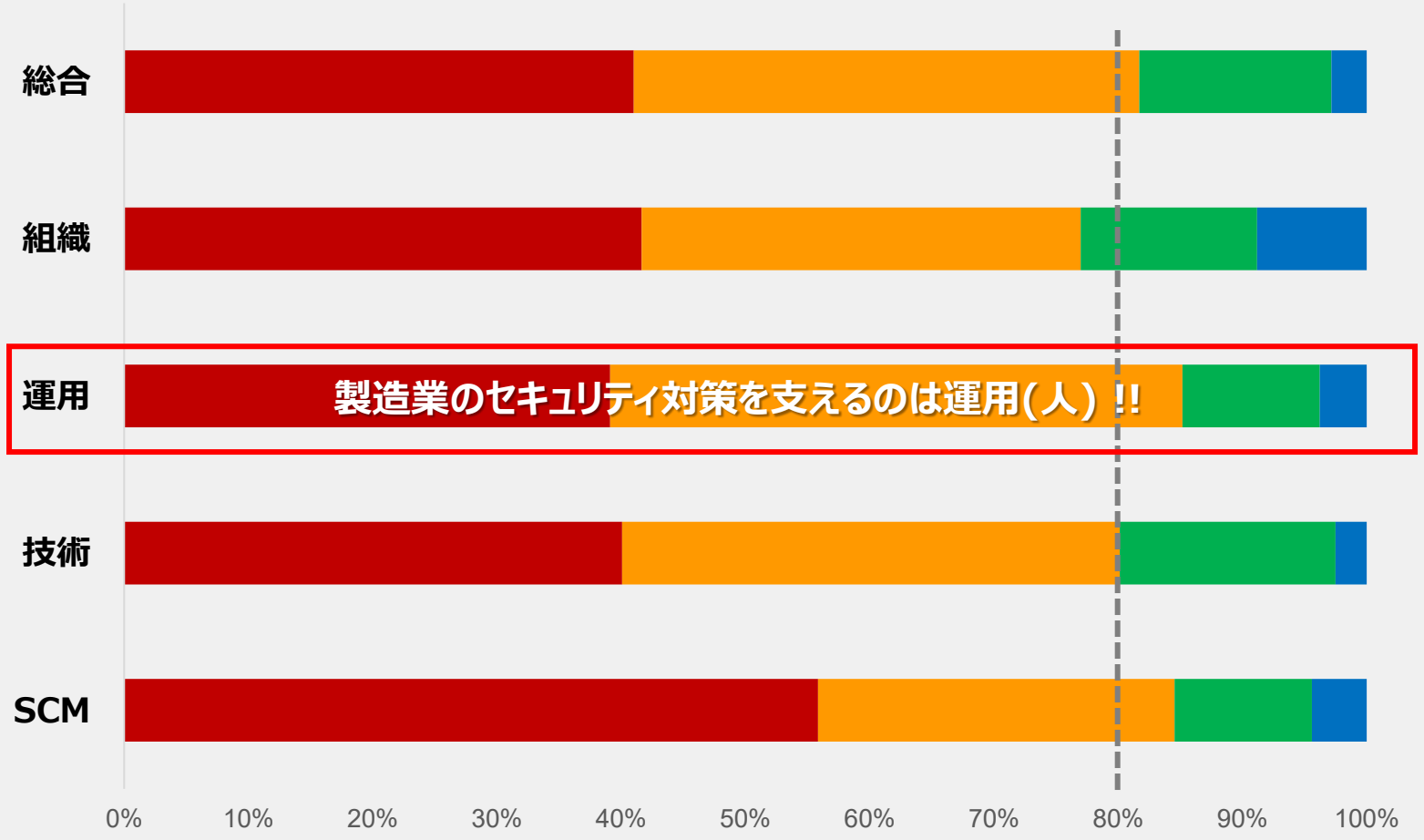
組織的対策
評価 D　スコア 28%
経営層の理解がなく、予算・人など基本的なリソースを得られていない。ガバナンス体制に課題があり、工場セキュリティの責任所在があいまいな状態である。

運用的対策
評価 C　スコア 44%
リスクアセスメントが不十分なため、対策の過不足が生じている可能性がある。資産管理が不十分なため、セキュリティ事故時の対応が遅れる。工場への外部記憶媒体の利用・持ち込みの制限がなく、外部からの脅威が容易に侵入できる。

技術的対策
評価 D　スコア 36%
端末保護が十分でないため、マルウェア感染の

工場システムサプライチェーン管理
評価 C　スコア 47%
制御システムベンダー・システム構築事業者と

D: 未実施、C：一部実施、B：実施済、A：実施済、手順文書化



- データ侵害中、人的要素に起因する割合　・・・　74%
- サイバーセキュリティの問題中、「ヒューマンエラー」に起因する割合　・・・　95%

How OTセキュリティ？
～OTセキュリティリスクの考え方と課題～

フォーティネット OTセキュリティソリューション全体像

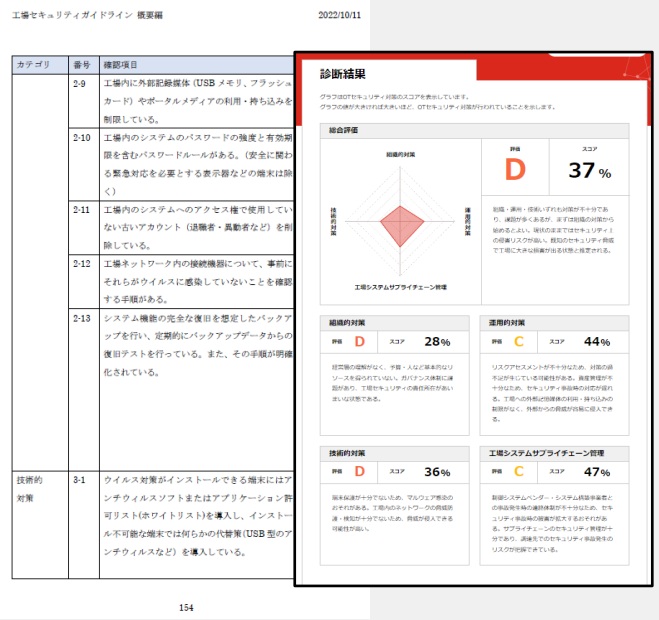
現状把握からサプライチェーン強化迄ワンストップで支援します

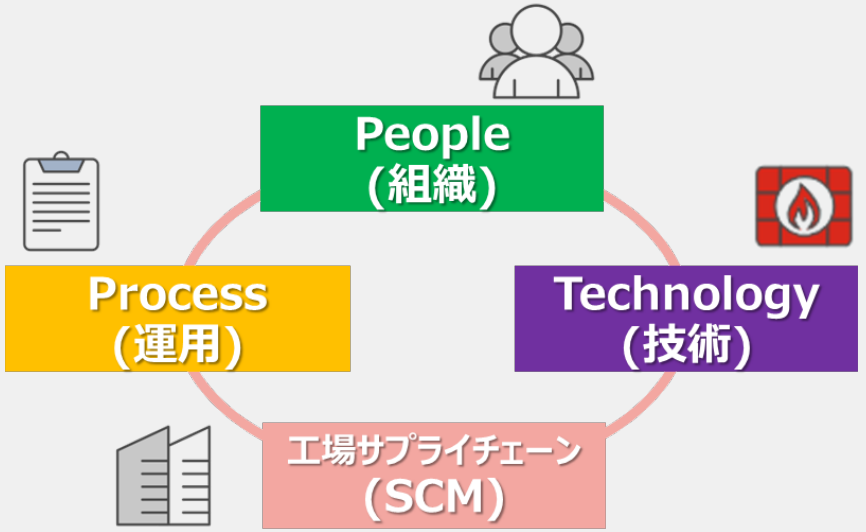
① 現状把握

② リスクの正しい理解と計画

③ ソリューション導入
(モデル工場へ)

④ 全拠点展開&サプライチェーン





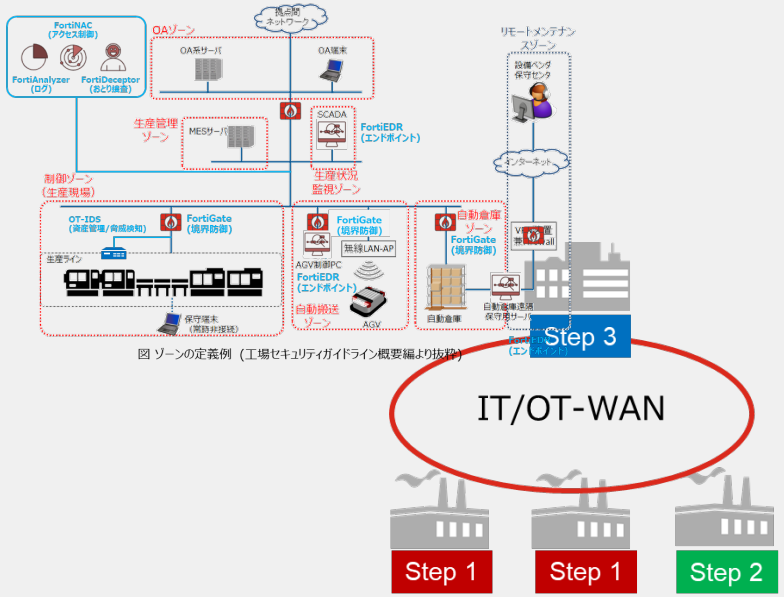


図 ゾーンの定義例（工場セキュリティガイドライン概要編より抜粋）

OTセキュリティ簡易診断

工場セキュリティガイドライン
チェックリストを活用して
「説明責任」、「実効性」の両輪を実現

現地アセスメントとコンサルティング

ITとOTのリスクの違いを理解し、組織・運用・技術・
(SCM)のバランス対策を実施

OTセキュリティレベルの底上げ

ベストプラクティスを活用した横展開

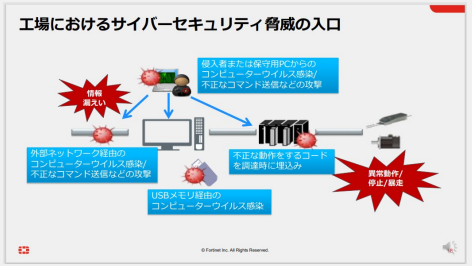
OTセキュリティの基礎知識、リスクの考え方を習得するトレーニング

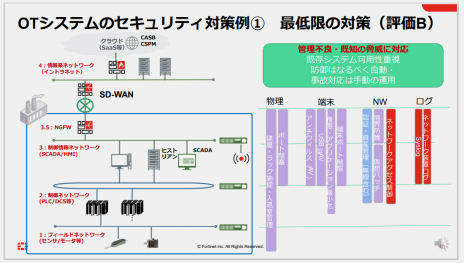
当サービス開始から約1年で380名以上の方に本トレーニングを受講頂きました！
OTセキュリティの重要な考え方を習得しユーザー/パートナー共に実効性のある対策実施に向けた準備が可能となります！

Part.1：座学ビデオ (自主学習)+事前課題 ※ 約4時間+α

<ビデオ第１部：OTセキュリティの基本>
- サイバーセキュリティとは？
- 制御システムのセキュリティ脅威
- ビジネス環境の変化
- OTセキュリティの課題と対策の３つの観点

<ビデオ第２部：OTアセスメントの進め方>
- アセスメント概要
- 日程・計画・成果物イメージ
- チェックシート項目別説明
- 実機検証の結果分析例
- 想定被害・リスクシナリオの作成方法

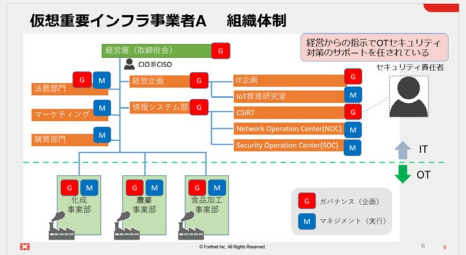




Part.2：ワークショップ (物理開催) ※ 3 - 4時間

工場セキュリティガイドライン、アセスメントを仮想企業に対して実践ワークショップ
(1回 最大16名：3 - 4グループ)

- 仮想企業へのアセスメントを通してOTセキュリティの考え方を学ぶ
- 製造業のリスクの考え方を通して製造業にとって起きて欲しくないことを学ぶ
- グループワークを通して、成果物の作成、発表、意見交換、評価
- ワークショップ終了後、のビジネスモデルの建付け支援

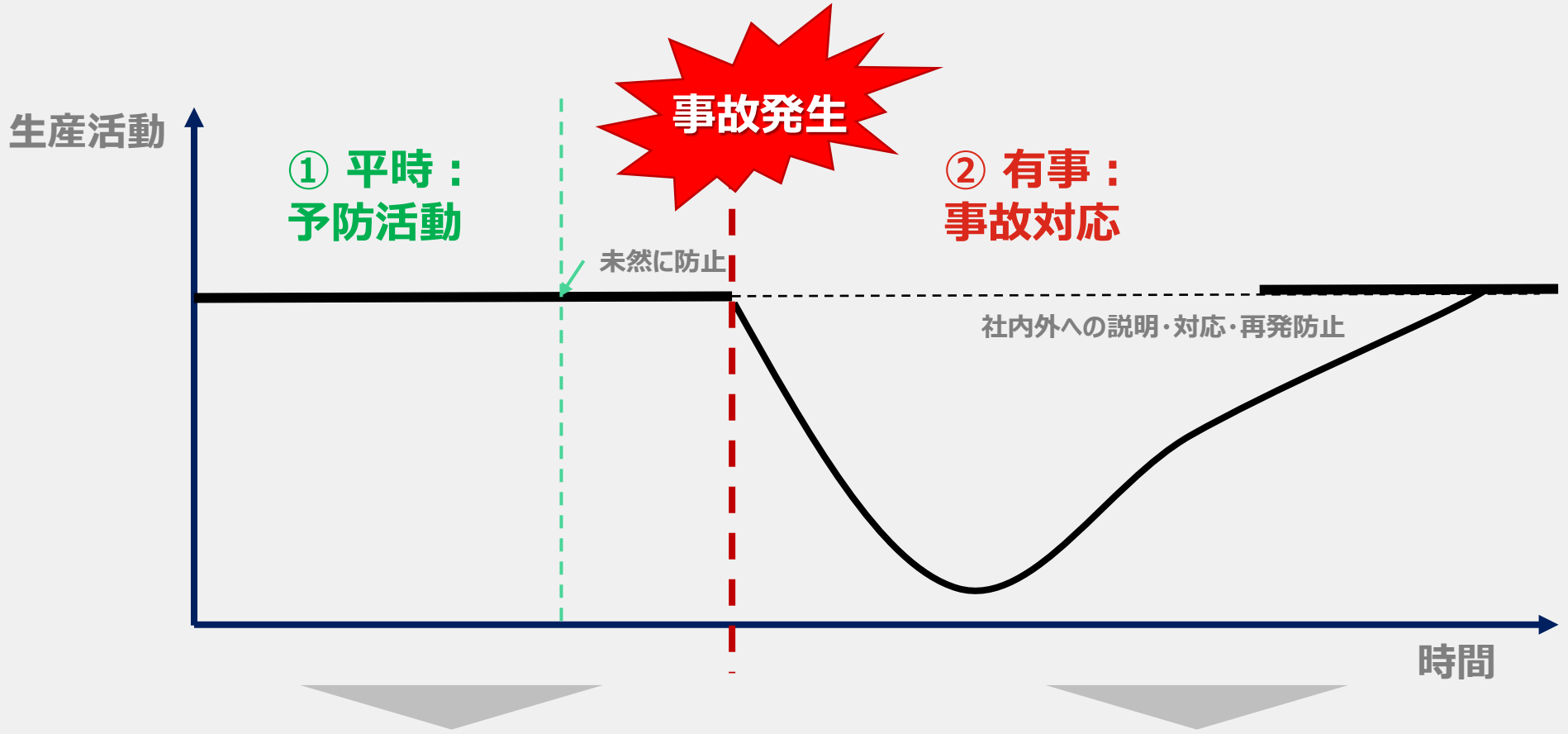


※　受講後の共有された資料・動画コンテンツは社内で再利用可能です

まとめ

OTセキュリティのやることは２つ、①平時の予防活動と②有事の事故対応

予防活動だけで終わっていませんか？本当に重要なのは事故発生時にいち早く通常操業へ復旧すること！



技術導入が進めやすい反面
定量的に効果を判断しづらい

セキュリティ事故を100%防ぐことは困難、事故発生時の組織と運用の建付け、復旧→通常操業まで誰が何をしなければならないかの訓練が重要

デジタル化を進めつつ、同時に**サイバー空間を安心・安全に保つ**ことで生産活動の**ゴール(SQECD)を達成**

OTセキュリティ対策の本当の目的は何ですか？

工場(OT)で本当に起きて欲しくない事象(リスク) とは？

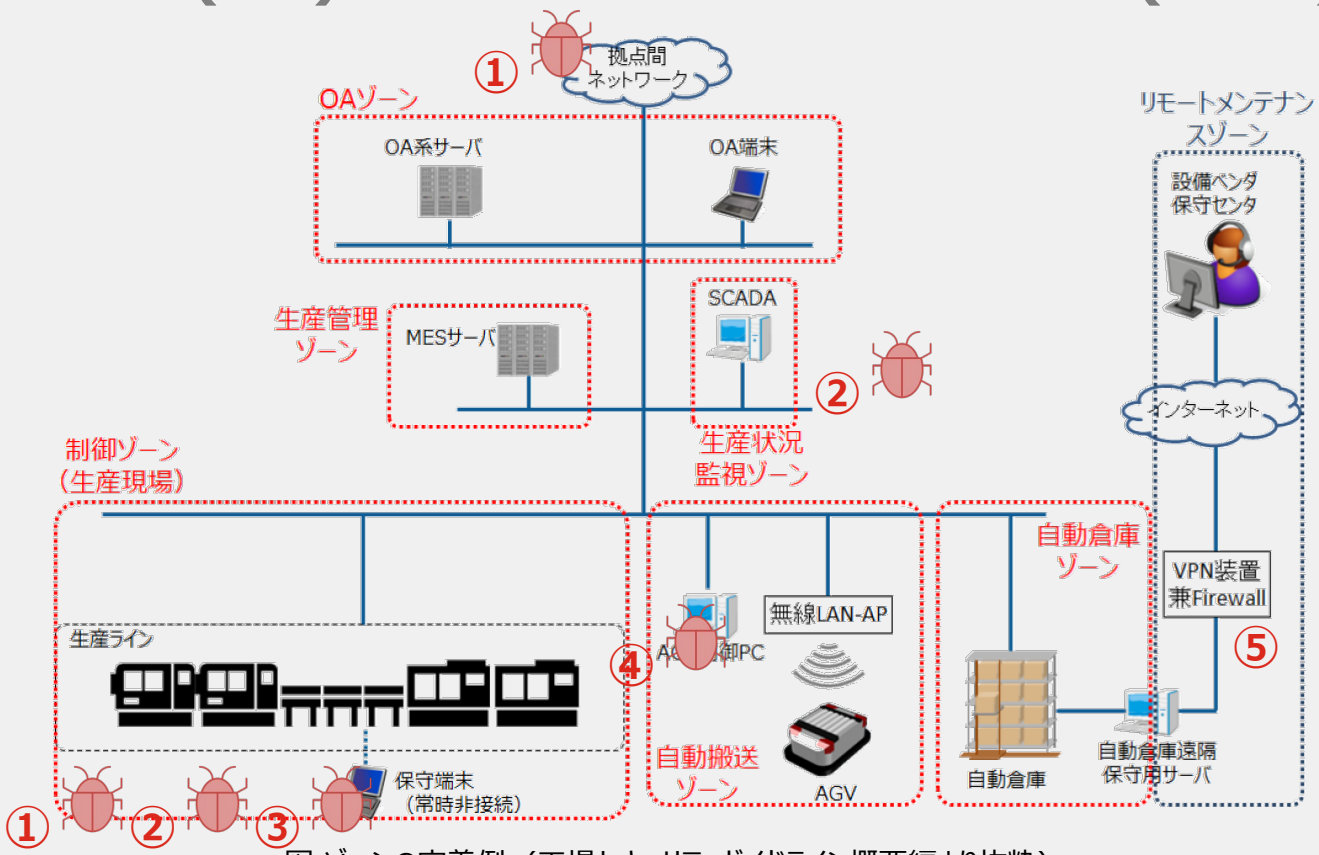


図 ゾーンの定義例 (工場セキュリティガイドライン概要編より抜粋)

<OTセキュリティ脅威の入口>

① **外部ネットワーク経由**のサイバー攻撃・設定不良
② **USBメモリ**経由のサイバー攻撃
③ **外部からの持ち込みデバイス**・設定不良
④ 不正な動作をするコードを**調達時に埋込み**

フォーティ君

<OTリスクとは?>

1. 生産活動が継続できなくなること

例) ①～④ のサイバー要因で制御システムや生産管理システムへ影響が発生、且つ初動対応や復旧ルールがない(機能しない)為、影響が長期化する

2. 従業員を始めとする人に対して、安心・安全が損なわれること

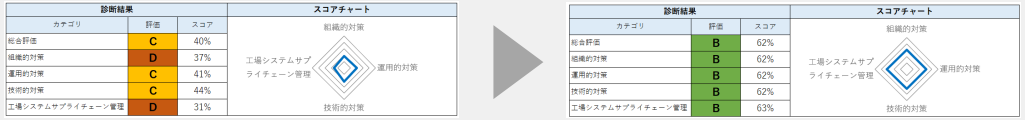
例) ①～④ のサイバー要因を多層的に防御することが出来ず、制御システムや機器への到達、乗っ取りや悪意のある正常なプログラム指示により、作動不良が発生し従業員を怪我をさせる、悪品を流通させ消費者の人体へ影響を及ぼす

3. その他、固有のリスクが発生しビジネスに影響を及ぼすこと

例) ①～④ のサイバー要因で生産設備と出荷設備に侵害の疑い、出荷設備は予防によって健全性が確保されたが生産設備は被害が確認され停止、復旧には余剰在庫分1週間の停止を大幅に超過する4週間の停止を余儀なくされた為、顧客信頼関係を失いビジネス機会の損失を受ける

OTセキュリティ対策と進め方

ガイドラインを活用して組織・運用・技術・SCMをバランスよく対策することで実効性のあるOTセキュリティを実現



ガイドラインで対策実施先ずは 評価 ALL「B」を目指す

PPT項目	サブ項目	評価「B」達成に必要な成果物	各項に対するFTNTソリューション		
組織（People）	ガバナンス体制	組織体制「役割」、「機能」の定義 組織体制キャリアパスの定義	コンサルティング		予防 / 事故対応
	現場教育	現場向けサイバーセキュリティ教育プログラム	コンサルティング		予防 / 事故対応
運用（Process）	定期評価	定期評価手順書	コンサルティング、脆弱性情報の把握	OT-IDS	予防
	インシデント対応	インシデント対応手順書	コンサルティング		事故対応
	資産管理	工場システムの資産管理手順書・技術	ネットワーク内の通信端末可視化と制御	FortiNAC / OT-IDS	予防
	ルール策定・管理	サイバーセキュリティ関連ルール・教育組込	コンサルティング		予防 / 事故対応
技術（Technology）	端末保護	工場システム端末のセキュリティ対策	• クライアント保護と一元管理 • 仮想パッチの適用 • アプリケーションホワイトリストまたは指定通信の遮断 • おとり捜査によるアクティブディフェンス	FortiGate / FortiDeceptor / OT-IDS	予防 / 事故対応
	物理	工場の物理セキュリティ対策実施	物理対策実施のこと(カメラ、入退館管理等)	FortiCamera	予防
	ネットワーク	工場ネットワークのセキュリティ対策	• VLANによるセグメンテーションとセキュリティ対策 • ネットワーク内の通信端末可視化と制御	FortiGate / FortiNAC / OT-IDS	予防 / 事故対応
	ログ	工場のセキュリティログ取得・保存	通信ログの保存とレポート	FortiGate / FortiAnalyzer	事故対応
工場資産サプライチェーン	外部管理	SI/ベンダーセキュリティ管理ルール	コンサルティング		予防 / 事故対応
	内部管理	工場資産調達時のセキュリティ管理ルール	コンサルティング		予防

リスク低減の為のOTセキュリティ対策（技術的対策例）

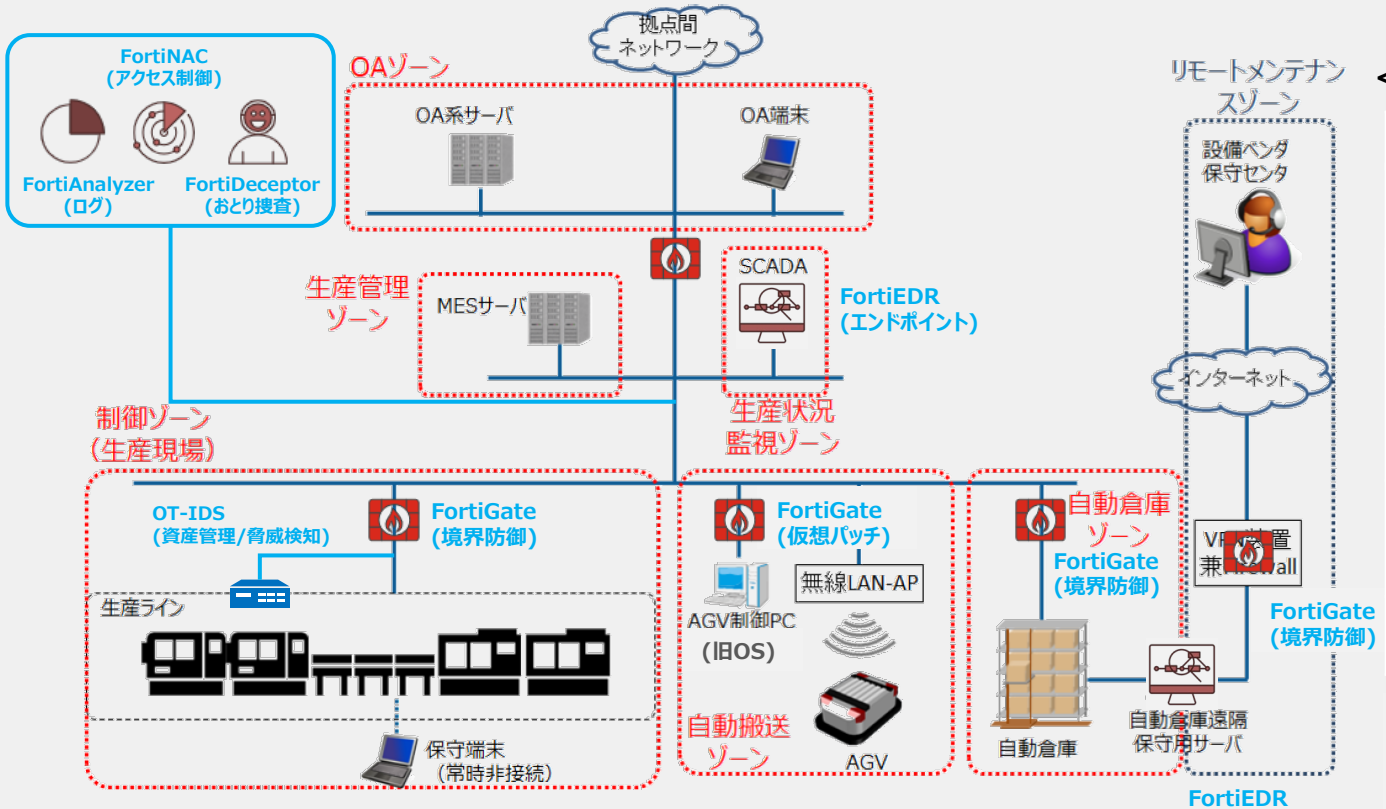


図 ゾーンの定義例 （工場セキュリティガイドライン概要編より抜粋）

<OTセキュリティ脅威の入口>

① **外部ネットワーク経由**のサイバー攻撃・設定不良
② **USBメモリ**経由のサイバー攻撃
③ **外部からの持ち込みデバイス**・設定不良
④ 不正な動作をするコードを**調達時に埋込み**

フォーティ君

<工場セキュリティガイドラインチェックリスト 概要編より技術面で対応できる項目の抜粋>

サブ項目	項目	各項に対する連携ソリューション
資産管理	2-6 2-7	ネットワーク内の通信端末可視化と制御
定期評価	2-8	脆弱性情報の特定
端末保護	3-1 3-2 3-3	• クライアント保護と一元管理 • 仮想パッチの適用 • アプリケーションホワイトリストまたは指定通信の遮断
ネットワーク	3-5 3-6 3-7	• VLANによるセグメンテーションとセキュリティ対策 • ネットワーク内の通信端末可視化と制御
ログ	3-8	通信ログの保存とレポート

<リスクに応じた技術的対策として>

① ITとOTのNW境界防御・各Zoneの境界防御 (FortiGate)
② OTのNWセキュリティログ・監視 (FortiAnalyzer)
③ マルチベンダー環境下の資産・及びアクセス制御 (FortiNAC)
④ 脅威の検知、封じ込め、修復を行うエンドポイント保護ソリューション、侵害後の保護を実現し、セキュリティインシデントの最中でも高可用性を維持(FortiEDR)
⑤ おとり捜査により正確な検知を提供する早期警告システム (FortiDeceptor)
⑥ OT資産可視化&脅威検知、仮想パッチと境界防御連携による予防対応 (OT-IDS)

導入事例：リコー様

現場目線で取り組み、現場の課題解決にフォーカスしながら進めること

FORTINET 導入事例

RICOH

「自分たちの工場のセキュリティは自分たちで守る」
現場とグループ統括、専門家が一体となって進めた
工場セキュリティジャーニー

デジタルサービス企業への変革に取り組むリコーでは、情報セキュリティ、プロダクトセキュリティは推進してきたものの、「工場セキュリティ」をどう実現するかが課題となっていた。同社はまず現状把握からスタートし、現場の意見を大切にしながらリファレンス工場での対策を推進。そのモデルを国内外の各工場に展開しようとしている。

株式会社リコー
本社所在地　東京都大田区中馬込1-3-6
設　　立　1936年2月
連結従業員数　81,017名
連結対象子会社・関連会社　240社
（2023年3月31日現在）

株式会社リコー
セキュリティ統括センター
セキュリティ・安全保障エキスパート
若杉 直樹氏

リコーインダストリー株式会社
執行役員
東北事業所 所長
プリンタ生産事業部 事業部長
庄司 勝氏

導入・構築のポイント

(1) アセスメントを通じて現状を把握することから始め、専門家の意見を得ながら段階的に対策を実施
(2) 現場の課題解決にフォーカスし、人とプロセス、フォーティネットの技術を生かし成熟度を向上
(3) リファレンス工場の成功モデルを、国内外の各工場に展開する形で無理なく対策を推進

ITやプロダクト面での対策を推進してきた一方、欠けていたファクトリーセキュリティ体制

「"はたらく"に歓びを」というビジョンを掲げるリコーは、今まさに、OAメーカーからデジタルサービスの会社への変革に取り組んでいる最中だ。デジタル複合機などエッジデバイス領域での強みを生かしつつ、クラウドなどを活用した新たなサービスの実現に取り組んでいる。

ただ、外の世界とつながるということは、セキュリティがいっそう不可欠になることも意味する。
以前から同社は、CEO直下にセキュリティ統括センターを組織化し、5つのビジネスユニットと連携しながらグループ全体で情報セキュリティ推進体制を整えてきた。そしてグローバル各国のさまざまなセキュリティ法制度や規制を踏まえながら戦略に取り入れ、世界的なガイドラインとなっているNIST SP800-171への準拠も目指している。
この体制の中で、CSIRTを中核とした「コーポレートセキュリティ」とPSIRTを中核とした「プロダクトセキュリティ」、2つの推進体制を整備して対策に取り組んできた。しかし「1つ足りないところがありました。それは、ファクトリーセキュリティの推進体制であるFSIRT（Factory SIRT）です」（株式会社リコー セキュリティ統括センター セキュリティ・安全保障エキスパート 若杉直樹氏）
サイバー攻撃者はしばしば「弱いところ」「止まっては困るところ」を突いてくるが、その意味で、生産データや工場の稼働は格好のターゲットになりつつある。現に、ランサムウェアをはじめとするサイバー攻撃によって、情報システムが影響を受けるだけでなく生産ラインが停止するといった深刻な被害が国内でも複数発生していることを踏まえ、リコーでも次の一手の必要性を感じていた。NIST SP800-171対応、そして変化する世界情勢の中での安全保障やリスク管理といった観点からも、工場のセキュリティ対策の緊急度は高まっていた。

全体推進
- 全体の計画策定・推進
- 各WGの推進状況確認
- 現場の課題解決

組織 ガバナンスWG
- セキュリティ組織体制、コミュニケーションパスの再構築
- インシデント対応ルール・フローの改善
- ペネトレーションテスト、脆弱性診断プロセスの改善

運用 ルール策定・教育WG
- セキュリティ教育体系の構築
- ルール（教育、内部/外部管理等）の策定
- 資産/管理プロセスの改善

技術 技術検討WG
- 端末・ファシリティー・ネットワーク対策
- ログ・SOC検討
- 資産管理ツール導入検討

事例紹介動画

株式会社リコー｜フォーティネット導入事例インタビュー
https://www.youtube.com/watch?v=vtYIQ2KNhQQ&t=9s

OTセキュリティといえばフォーティネット

FORTINET®