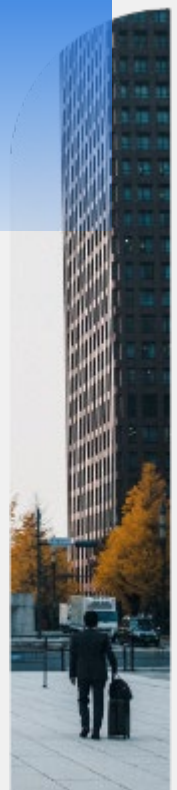
「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」のポイント解説

フォーティネットジャパン合同会社

OTビジネス開発部　部長　佐々木　弘志



自己紹介

佐々木　弘志

Mission：「産業サイバーセキュリティの文化を創る」

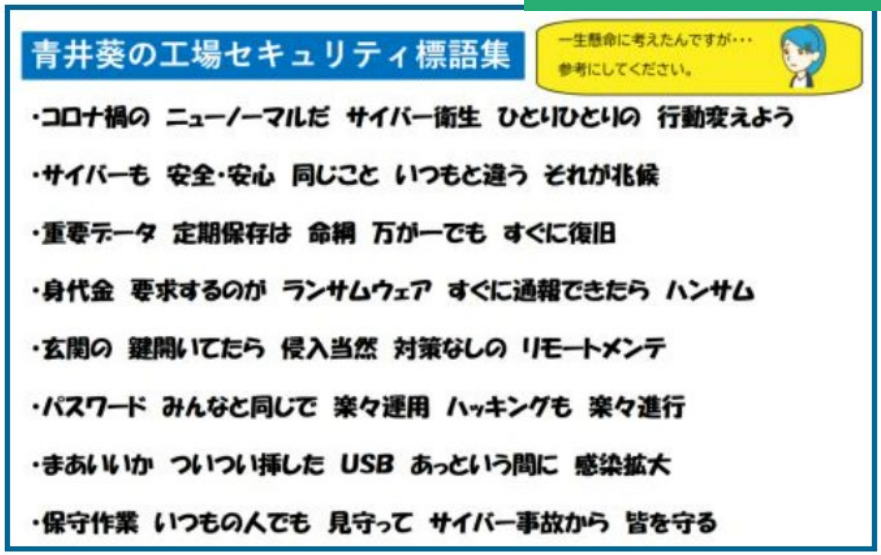
・産業制御システム開発者（14年）
・産業制御システムセキュリティのコンサルタント（11年~）

2016年5月～2020年12月,2021年7月～現在:
　・**経済産業省 サイバーセキュリティ課 情報セキュリティ対策専門官(非常勤)**
2017年７月～現在:
　・**IPA 産業サイバーセキュリティセンター サイバー技術研究室 専門委員(非常勤)**
2021年8月～現在:
　・**フォーティネットジャパン合同会社　OTビジネス開発部　部長**
2022年5月～現在:
　・**名古屋工業大学　産学官金連携機構　ものづくりDX研究所　客員准教授**
2023年4月～現在:
　・**名古屋工業大学大学院　博士後期課程　工学専攻**
2021年～:
　・**産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）**
　　宇宙産業SWG セキュリティガイドライン検討委員
　　工場SWG セキュリティガイドライン検討委員(2022年1月～)

事例で学ぶ製造業DXセキュリティ対策入門

対話形式でわかりやすく

実務に役立つおまけつき



https://monoist.itmedia.co.jp/mn/series/25623/

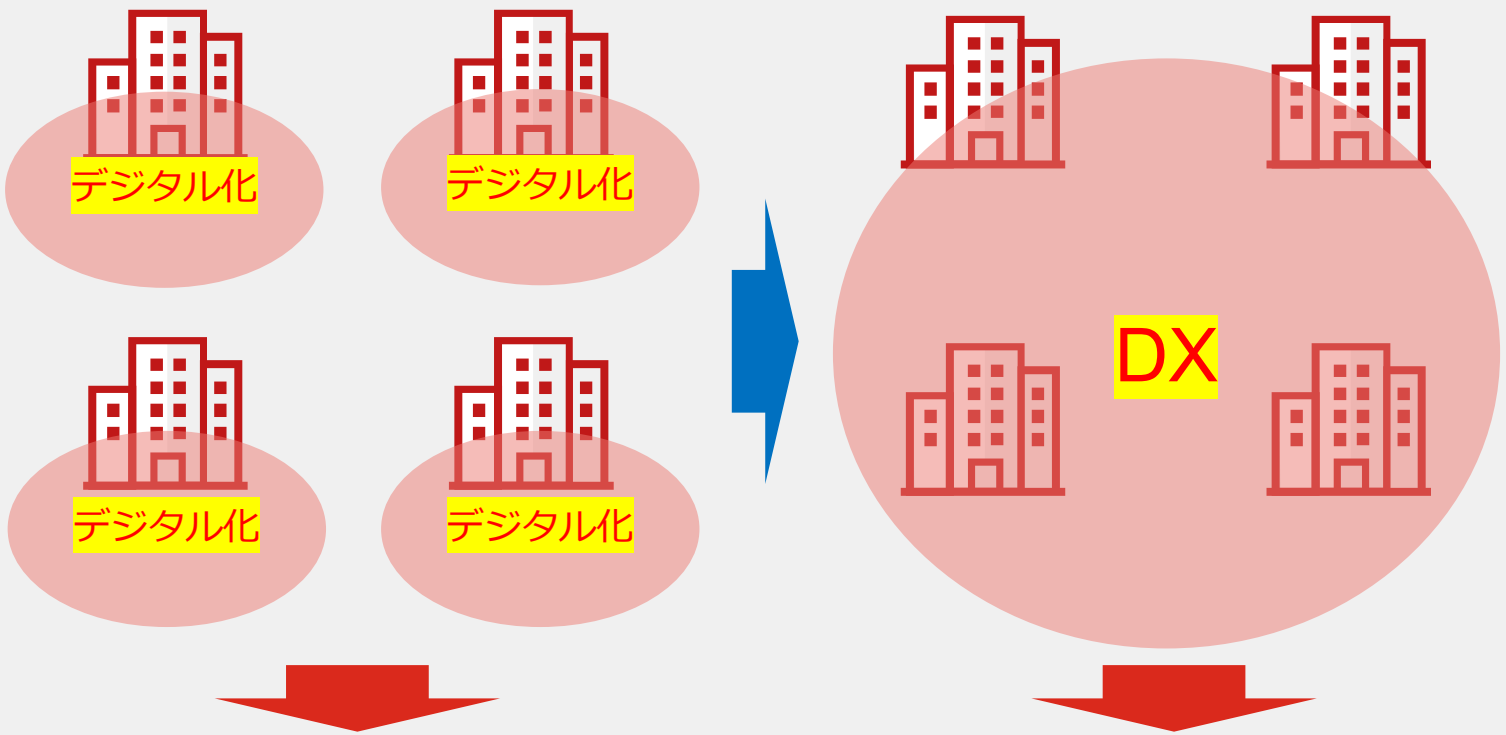
アジェンダ

- 製造業のサイバーセキュリティ最新動向
- OTセキュリティを進める上での主要な課題
- 経済産業省の工場セキュリティガイドラインの活用方法

製造業のサイバーセキュリティ最新動向

5

「DX × セキュリティ」の課題感と対策の方向性



サイバーセキュリティ
リスクへの対処は
自己責任

サイバーセキュリティ
リスクへの対処は
ビジネス参加条件

DX時代のサイバーセキュリティ課題

- サイバー攻撃の進化と深化
- セキュリティ対象範囲の拡大
- 複雑化・守り切ることが困難
- 自損事故の増加
- サプライチェーンリスク
- コンプライアンス対応
- セキュリティ人材不足

DX時代のサイバーセキュリティ

- シェアリング・サブスク（人材・運用・ルール）
- 相互連携・自動化
- レジリエンス

なぜOTセキュリティが必要なのか？

DXの進展による ビジネス環境変化

・IT/OT接続増加

・OTのIT化

工場環境が
サイバー攻撃に遭う
機会の増加

OTのIT化により
想定外の不具合が発生

「データ」のサプライ
チェーン保護が
ビジネス課題に

工場向け 脅威の進化

・政治目的・特化型から
経済目的・汎用型に変容

・サイバー攻撃の変容
機密性(C)→可用性(A)
完全性(I)

工場向け脅威が
企業にとってより
身近で深刻な課題に

工場というより
ビジネスそのものが
リスクとなる

サプライチェーン 規制・ガイドライン

・欧米・中国における
サプライチェーン
リスク規制/GL強化

・経済安保

企業・製品・サービスの
信頼性において
セキュリティの重要性
が増加

対応できないと
サプライチェーンから
締め出される恐れ

7

経済安全保障推進法　第3章
基幹インフラ役務の安定的な提供の確保に関する制度の概要

基幹インフラ役務の安定的な提供の確保に関する制度の概要
（経済安全保障推進法 第３章）

趣旨

- 基幹インフラ役務（電気・ガス・水道等）の安定的な提供の確保は安全保障上重要。
- 基幹インフラの重要設備は役務の安定的な提供を妨害する行為の手段として使用されるおそれあり。
- 基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、重要設備の導入・維持管理等の委託を事前に審査。

概要

１．基幹インフラ役務の安定的な提供の確保に関する基本指針を策定

・対象事業者の指定に関する基本的な事項（当該指定に関し経済的社会的観点から留意すべき事項を含む）
・配慮すべき事項（重要設備等を定める主務省令の立案に当たって配慮すべき事項を含む）
・対象事業者その他の関係者との連携に関する事項　等

２．審査対象

(1) 対象分野（法律で対象事業の外縁を示した上で、政令で絞り込み）

電気	ガス	石油	水道	鉄道
貨物自動車運送	外航貨物	航空	空港	電気通信
放送	郵便	金融	クレジットカード	

(2) 対象事業者・・・主務大臣が指定

・対象事業を行う者のうち、①重要設備（具体的な重要設備は主務省令で指定）の機能が停止・低下した場合に、②役務の安定的な提供に支障が生じ、③国家・国民の安全（国民の生存・社会経済秩序の平穏）を損なうおそれが大きいものとして主務省令で定める基準に該当する者

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai5/siryou8.pdf
https://www.meti.go.jp/policy/economy/economic_security/infra.pdf

特定社会基盤事業者の指定基準に該当すると見込まれる者　R５.10.4時点

対象分野（法律）／特定社会基盤事業の指定（政令）		特定社会基盤事業者の指定基準（省令）	特定社会基盤事業者（※指定基準を踏まえ、対象となることが想定される者であり、現時点において指定を行った者ではありません。）
電気	一般送配電事業	電気事業法第二条第一項第九号に規定する一般送配電事業者であること。	沖縄電力株式会社 関西電力送配電株式会社 九州電力送配電株式会社 四国電力送配電株式会社 中国電力ネットワーク株式会社 中部電力パワーグリッド株式会社 東京電力パワーグリッド株式会社 東北電力ネットワーク株式会社 北陸電力送配電株式会社 北海道電力ネットワーク株式会社
電気	送電事業	電気事業法第二条第一項第十一号に規定する送電事業者であること。	電源開発送変電ネットワーク株式会社 福島送電株式会社 北海道北部風力送電株式会社
電気	配電事業	電気事業法第二条第一項第十一号の三に規定する配電事業者であること。	指定事業者なし （現在営んでいる事業者が存在しないため）

対象分野（法律）／特定社会基盤事業の指定（政令）		特定社会基盤事業者の指定基準（省令）	特定社会基盤事業者（※指定基準を踏まえ、対象となることが想定される者であり、現時点において指定を行った者ではありません。）
電気	発電事業	電気事業法第二条第一項第十五号に規定する発電事業者であって、出力五十万キロワット以上の発電等用電気工作物を有すること。	鹿島パワー株式会社 株式会社コベルコパワー神戸 株式会社コベルコパワー神戸第二 株式会社コベルコパワー真岡 株式会社JERA 関西電力株式会社 九州電力株式会社 四国電力株式会社 常磐共同火力株式会社 相馬共同火力発電株式会社 中国電力株式会社 中部電力株式会社 電源開発株式会社 東京電力ホールディングス株式会社 東京電力リニューアブルパワー株式会社 東北電力株式会社 勿来IGCCパワー合同会社 日本原子力発電株式会社 日本製鉄株式会社 姫路天然ガス発電株式会社 広野IGCCパワー合同会社 福島ガス発電株式会社 北陸電力株式会社 北海道電力株式会社 三菱重工業株式会社

石油・ガス事業者に関連するサイバーセキュリティ規制

高圧ガス保安法の認定事業所における法令違反について

参考資料

- 現時点で、83認定事業所が存在するところ、**直近10年では、累積24件の高圧ガス保安法の違反**があった。なお、**法令違反は18事業所であり**、うち**5事業所は複数回の法令違反**を犯している。
- 現行の認定制度は、「事業所」単位で認定を行っており、現時点では、37社が83認定事業所を有しているところ、直近10年では、「事業者」単位で**6社が法令違反**を犯している。*

*：社の統合等を経た現時点での事業者数

<認定事業所における法令違反の件数推移>

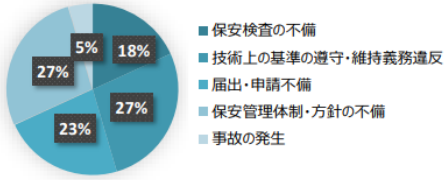
直近5年において、
法令違反は5件（2社5事業所）と減少（※）

（法令違反が減少した背景）
・認定期間中における立入検査の実施
・認定要件としてリスクアセスメントや人材育成を追加
これらは、新たな認定制度においても「維持」する。

さらに、①認定要件として、コンプライアンスを強化
（高圧ガス保安法の法適合性確認能力を確認）
②法令違反時には厳正に認定取消を実施

「安全性」を確保

<認定事業所における法令違反の類型>



（※）直近の認定事業所における法令違反案件への対応について
①経済産業省による対応：2021年9月17日、太陽石油四国事業所及び山口事業所に対して高圧ガス保安法第61条に基づく報告徴収を実施。
②愛媛県による対応：立入検査等により、太陽石油株式会社四国事業所において、2011年4月から2021年3月までの10年間に、高圧ガス設備に関する未許可の変更工事や県へのガス漏えい事故の未報告など計67件の高圧ガス保安法違反事案が確認。2021年9月22日、四国事業所に対して危害予防規程の変更・遵守命令などの行政処分を実施。

5

（参考）高圧ガス保安法における新たな制度的措置に係る認定の基準

- 新たな制度的措置の認定の基準は、スマート保安の促進の観点からテクノロジーの活用やサイバー対策を含む4つの要件で構成し、リスク管理レベル等に応じ、2つの措置（A認定・B認定）に差異化。

（※）下記の表における赤字の下線部及び赤枠は、新たな制度的措置の認定基準において、現行の認定基準から拡充するものを示す。

	A 認 定	B 認 定
①経営トップのコミットメント	現行スーパー認定事業者制度の要件に加え、コンプライアンス体制の整備（注1）、コーポレート・ガバナンスの確保	
②高度なリスク管理体制	現行スーパー認定事業者相当	現行通常認定事業者相当
③テクノロジーの活用	現行スーパー認定事業者制度における仕組み（注2）を基本とする ※認定基準において、採用することが必要となるテクノロジー（水準）を一定の幅で示し、事業者は、その中で事業実態に見合ったテクノロジーを採用。	
④サイバーセキュリティなど関連リスクへの対応	各業界におけるサイバーセキュリティガイドライン（注3）に沿った内容とする	

（注1）高圧ガス保安法についての**法適合性確認能力**（設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力）を有していることを含む。
（注2）特定認定事業者及び自主保安高度化事業者の認定について（20201218保局第1号）における認定の基準「二 先進的な技術を適切に活用していること」の項目を参照。
（注3）「重要インフラにおける情報セキュリティ確保に係る安全基準等作成指針」（内閣官房内閣サイバーセキュリティセンター）を参考に業界団体が定める「石油化学分野における情報セキュリティ確保に係る安全基準（石油化学工業協会）」、「石油分野における情報セキュリティ確保に係る安全ガイドライン（石油連盟）」。

3

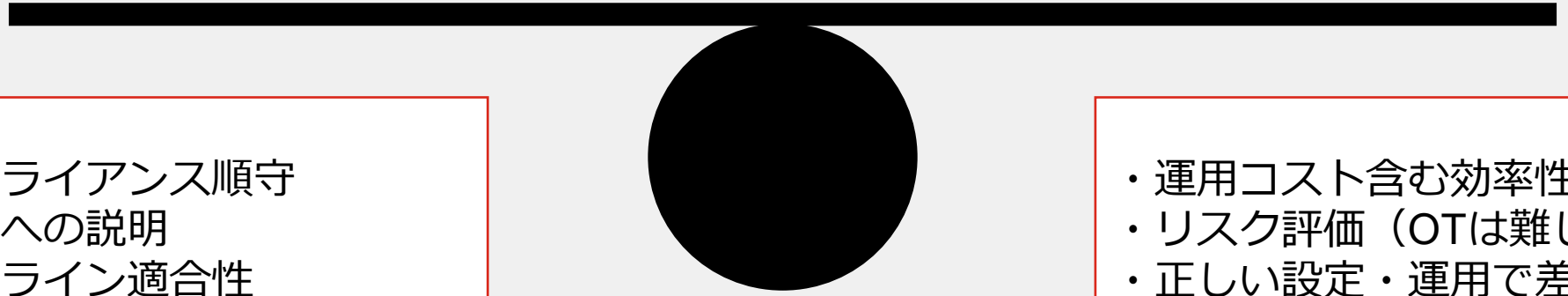
（調査の要請）

第六十条の二　経済産業大臣は、認定高度保安実施者その他の保安の確保上特に重要な者として経済産業省令で定める者において保安に係るサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）に関する重大な事態が生じ、又は生じた疑いがある場合において、必要があると認めるときは、独立行政法人情報処理推進機構に対し、その原因究明のための調査を要請することができる。

サイバーセキュリティの基本的な考え方

説明責任

実効性



・コンプライアンス順守
・取引先への説明
・ガイドライン適合性
↓

形骸化しやすいことに注意

・運用コスト含む効率性
・リスク評価（OTは難しい）
・正しい設定・運用で差がでる
↓

組織・運用・技術のバランス大事

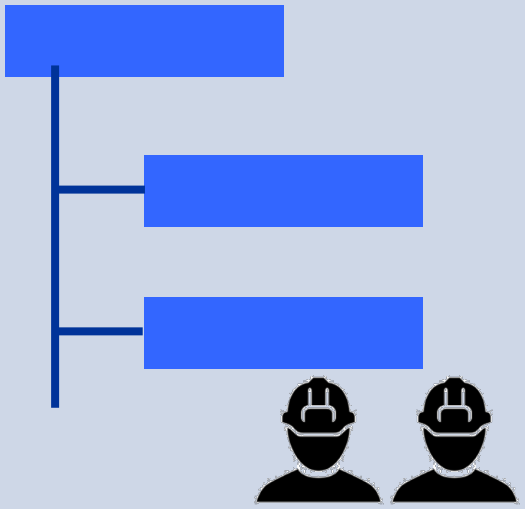
OTセキュリティを進める上での主要な課題

11

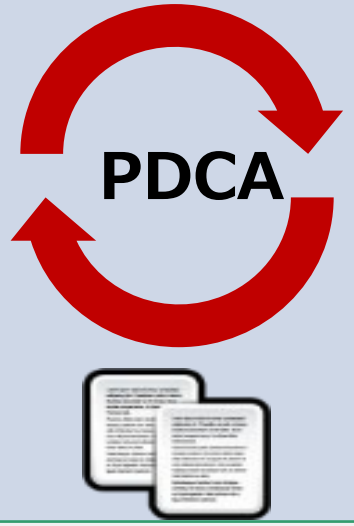
OTセキュリティの３要素

People（組織・人），Process（運用），Technology（技術）

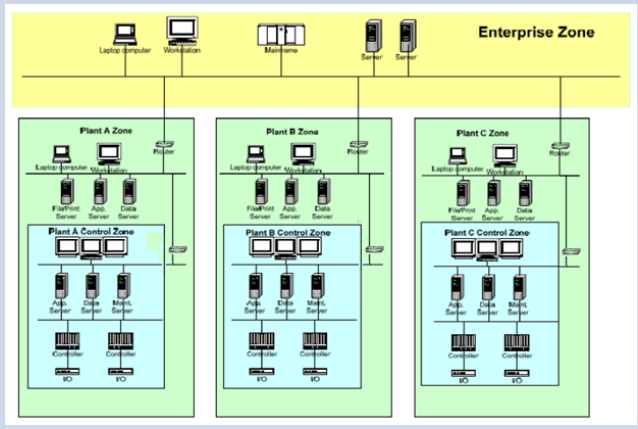
People



Process

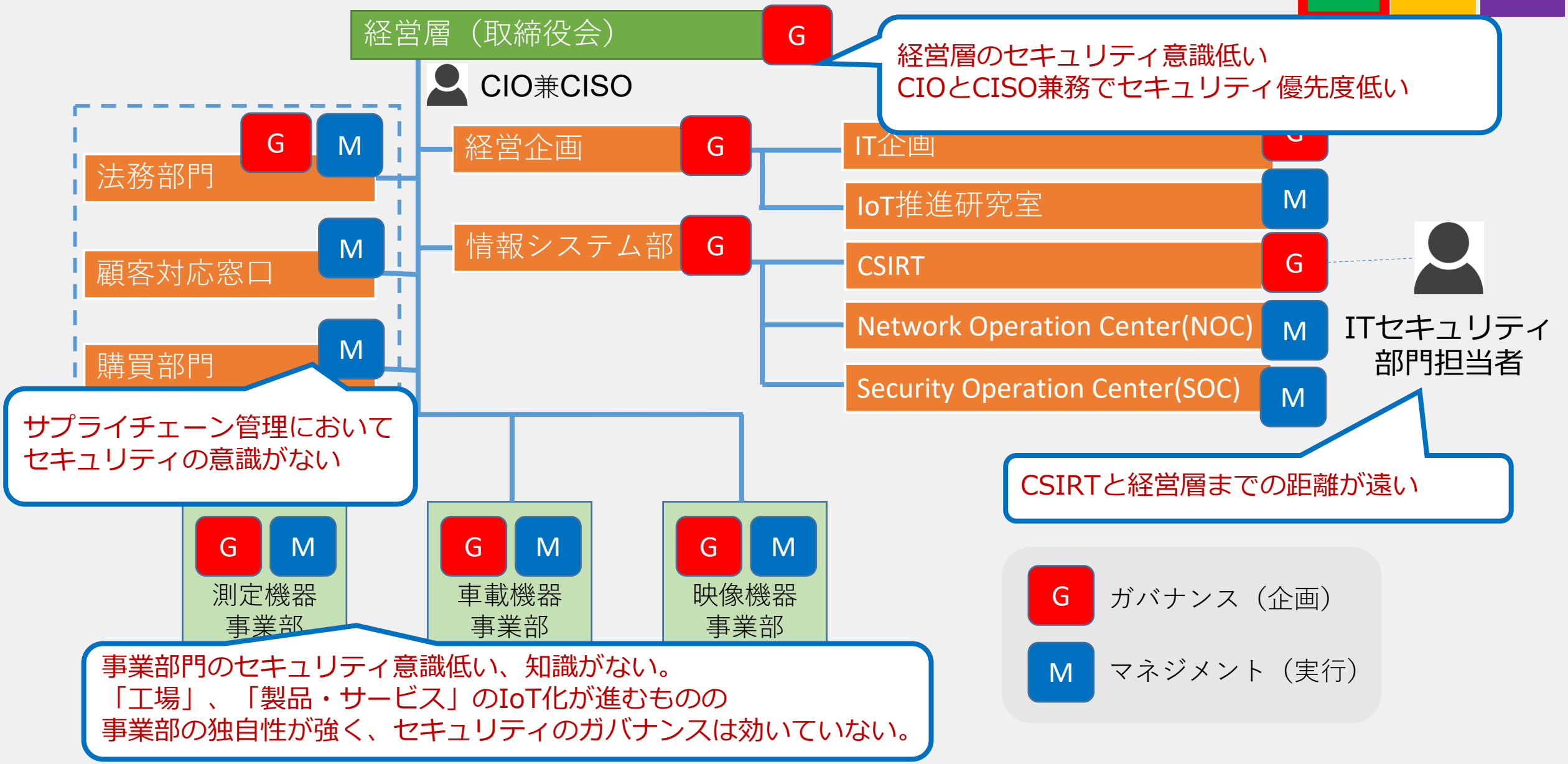


Technology



組織課題：誰も工場セキュリティ管理してない

Pe Pr Te



組織課題：ITとOTとでは異なるゴール

Pe Pr Te

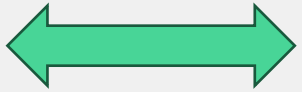
情報セキュリティ部門

情報・データを守る

Confidentiality(機密性)

Identity (完全性)

Availability (可用性)



OT部門

生産活動・ビジネスを守る

Safety (安全性)

Quality (品質)

Environment (環境影響)

Cost (コスト)

Delivery (納期)

サイバーセキュリティはOT部門のビジネス目標達成のための手段

工場の安心・安全なサイバー空間の確保とは？

<物理空間(製造現場)の保全>

- 製造業にとって本当に起きて欲しくないこと(リスク)は、**①生産・収益への影響、②安心・安全が損なわれる** こと
- リスクを起こさない為の保全のルールが徹底されている

1. **正しい規律・秩序(5S)**
2. **三現主義 (現地・現物・現実)**
3. **正しくリスクを理解する (KY)**

<サイバー空間の保全>

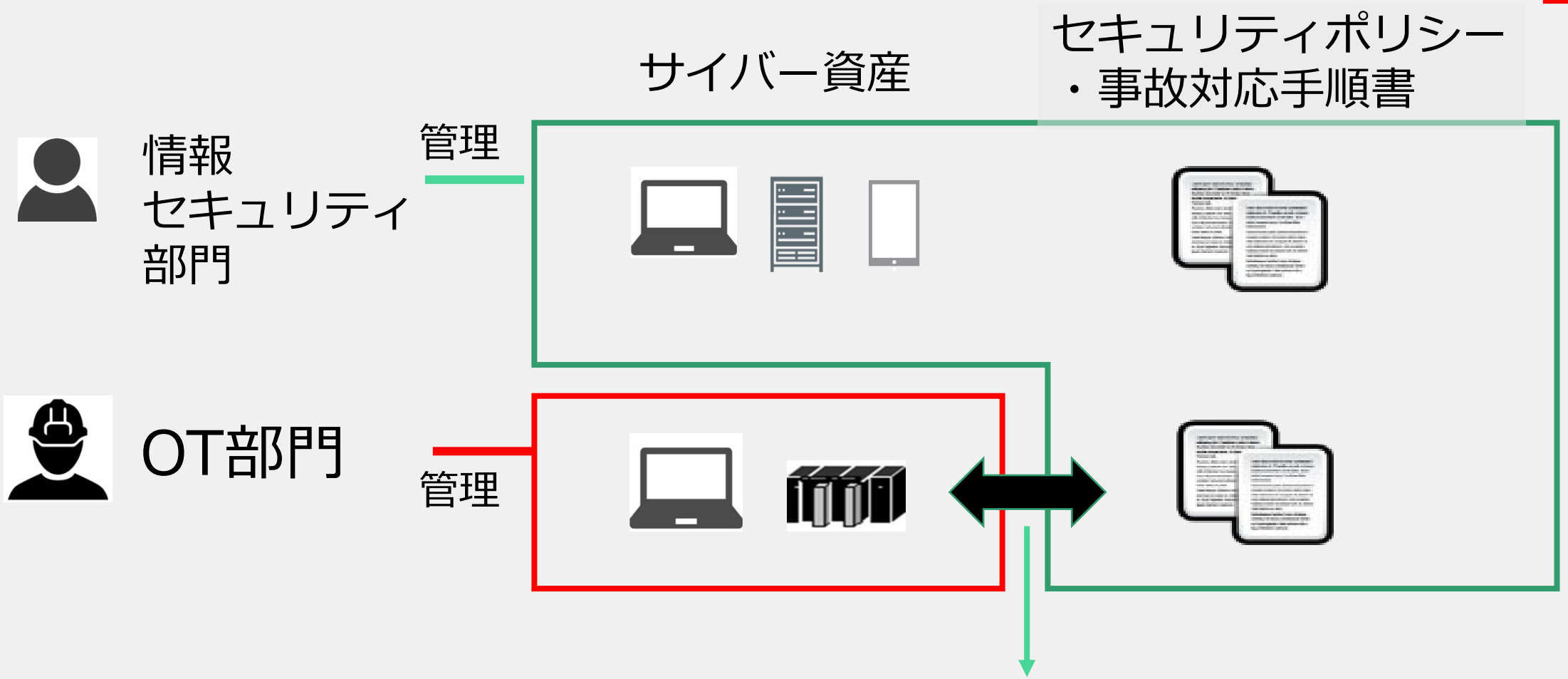
- 工場・プラントのデジタル化、クラウド活用が活発化し**OTのIT化**が進む
- 製造現場の保全と同じ様に**サイバー空間も保全**が必要

- サイバーセキュリティ対策はサイバー攻撃から**ビジネスを守る**こと、そして**「安心・安全なサイバー空間の確保」**を行うことでデジタル空間を管理、運用し**SQECDに貢献**すること

※ S: Safety, Q: Quality, E: Environment, C: Cost, D: Delivery

運用課題：OTセキュリティポリシーの形骸化

Pe Pr Te

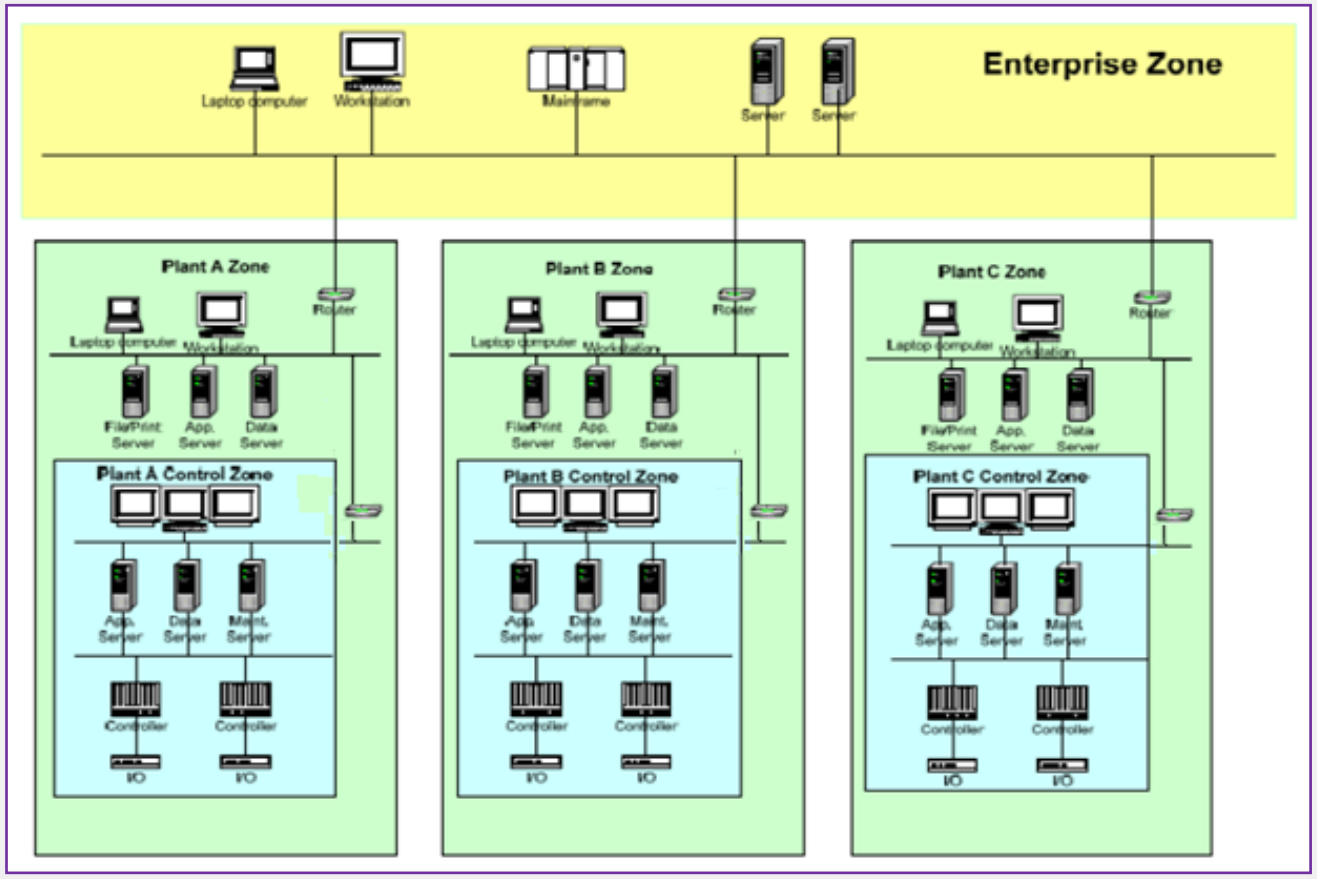


OT部門が資産管理しているためルールが形骸化しがち

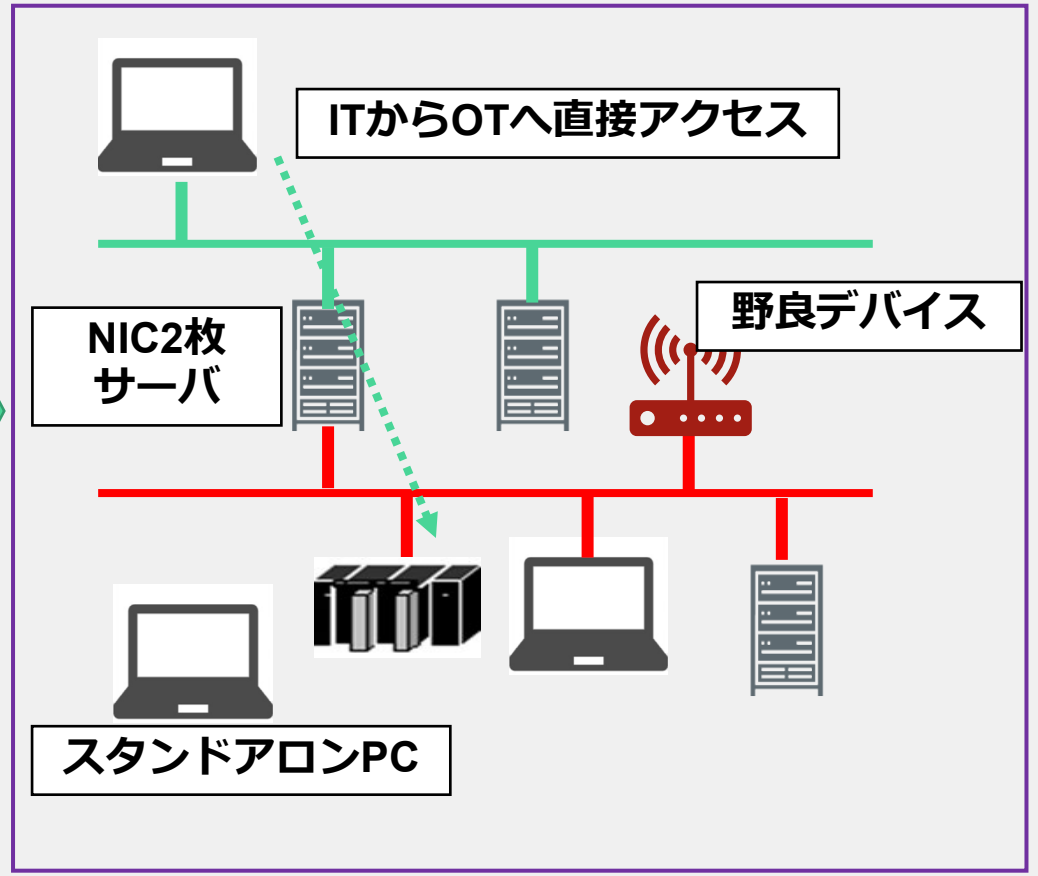
技術課題：工場ネットワークがフラット＆野放し

Pe Pr Te

教科書的な工場ネットワーク図



実際は・・・



誰も工場ネットワークで何が起こっているか知らない

経済産業省の工場セキュリティガイドラインの活用方法

18

経済産業省　工場セキュリティガイドライン概要

☑ 2022年1月6日、経済産業省は、産業サイバーセキュリティ研究会WG1（制度・技術・標準化）のサブWGとして工場SWGを設置。**ガイドライン**の取りまとめ着手。

☑ DX進展等の工場環境変化により高まるセキュリティリスクへの対策について、**工場のステークホルダー間の相互信頼の土台となる考え方を整理**

☑ 2022年11月16日、パブリックコメント版を反映したガイドラインVer1.0が公開。

https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

19

経済産業省のガイドライン付録Eのチェックリスト

達成度を「１：未実施」「2：一部実施」、「3：実施済み」、「4：実施済みで、管理手順を文書化・自動化し、定期的に対策を見直し」、「5：実施済みで、管理手順を文書化・自動化し、随時見直し」に応じて評価する

カテゴリ	No.	確認項目	達成度
組織的対策	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。	
	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。	
	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。	
	1-4	工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている。	
	1-5	工場セキュリティに関する脅威の動向などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの現場教育を行っている	
運用的対策（システム関連等）	2-1	システムが侵害・停止した場合の事業に対するリスクを検討している	
	2-2	工場システムにおける専用のセキュリティポリシが規定されていて、認知されている	
	2-3	工場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。	
	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。	
	2-5	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。	
	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、システム構成図が作成している。	
	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する仕組みがある。	
	2-8	定期的な脆弱性診断やペネトレーションテスト（侵入可否検査）を実施して、システムへの侵入を成功させるために使用できる攻撃手法や脆弱性を特定している。	
	2-9	工場内に外部記録媒体（USB メモリ、フラッシュカード）やポータルメディアの利用・持込みを制限している。	

経済産業省 公開資料より引用 https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000235644

カテゴリ	No.	確認項目	達成度
運用的対策（システム関連等）	2-10	工場内のシステムのパスワードの強度と有効期限を含むパスワードルールがある。（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）	
	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）を削除している	
	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。	
	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、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。	
技術的対策	3-1	ウィルス対策が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。	
	3-2	アプリケーション／オペレーティングシステム（OS）にセキュリティパッチを適用している。もしくは代替策を講じている。	
	3-3	制御端末のオペレーティングシステムの使用サービスやアプリケーションは必要最小限とし、未使用のサービスやポートは停止・無効化している。	
	3-4	工場の重要設備への物理的なアクセスについてレベル分けなどの十分な対策を行っている（例：監視カメラ、警報装置）。又は、入退室管理、外部の入室者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。	
	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）。	
	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）やネットワーク侵入防護などの保護対策を行っている。	
	3-7	工場内のネットワーク（情報システムとの境界含む）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。	
	3-8	工場内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するか必要日数保存している。	
工場システムサプライチェーン管理	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。	
	4-2	工場システムのメンテナンス等に関わる協力会社向けのセキュリティ教育を実施している。	
	4-3	納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダ・構築業者との連絡・連携体制を構築している。	
	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（監査実施など）を把握できている。	
	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。	
	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。	

経済産業省 公開資料より引用 https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000235644

チェックリストWeb診断ツール：オープンソース公開

Human-Centered Design and User Experience, Vol. 114, 2023, 331–337
https://doi.org/10.54941/ahfe1004251

Analysis of Cybersecurity Risk for Factory Systems

Hiroshi Sasaki[1,2], Kenji Watanabe[1], and Ichiro Koshijima[2]

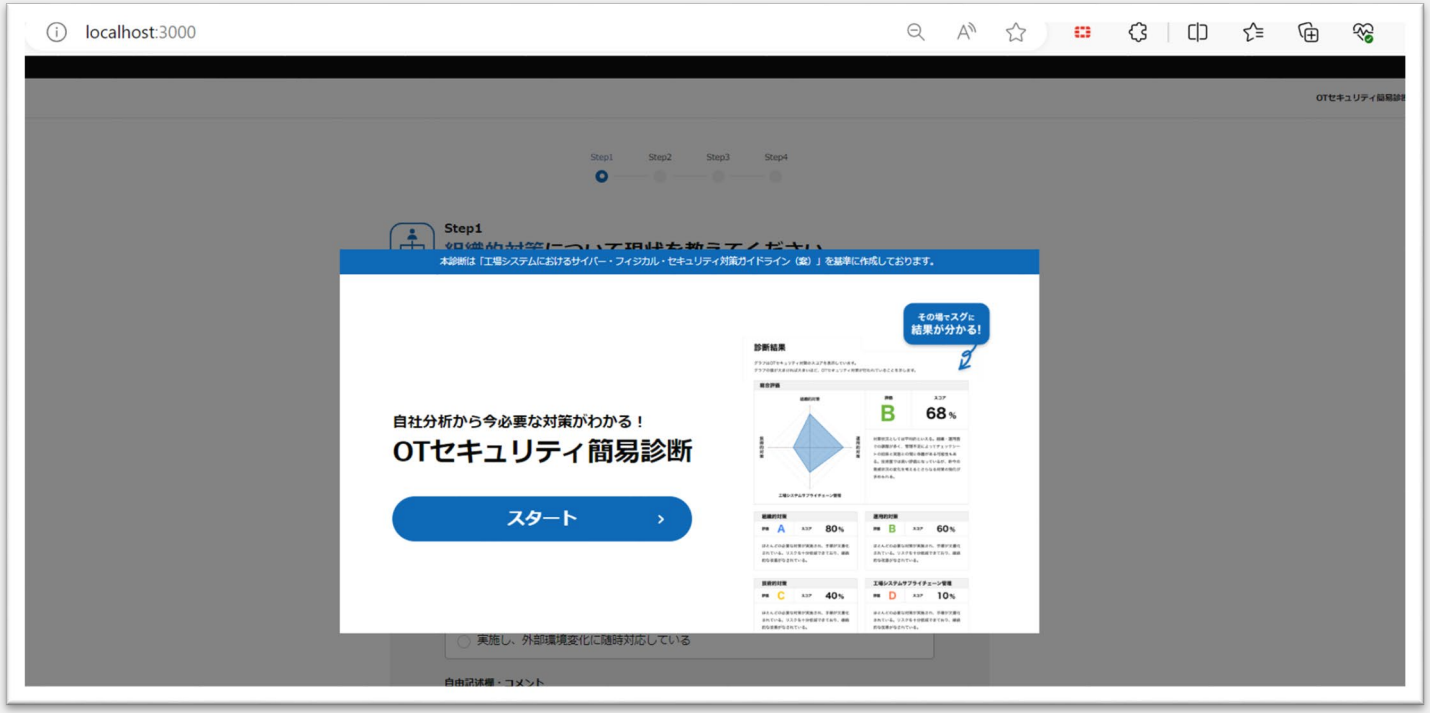
[1]Nagoya Institute of Technology, Gokiso-cho, Showa, Nagoya, Japan
[2]Manufacturing and Innovation DX Laboratory, Nagoya Institute of Technology, Gokiso-cho, Showa, Nagoya, Japan

ABSTRACT

As the digitization of factory systems progresses and the number of digital connections between factories increases, cybersecurity risks throughout the supply chain also increase. In fact, there have been many cases where factories have stopped due to damage from ransomware. For large enterprises, it is possible to secure the budget and personnel for cybersecurity, including outsourcing. However, almost all small and mediums enterprises (SMEs) are facing with the difficulties to secure them. In this paper, we used a web diagnostic tool for simple risk assessment of factory systems using the checklist for understanding the rough risk posture in the appendix of "The Cyber/Physical Security Framework for Factory Systems" formulated by the Ministry of Economy, Trade and Industry in November 2022. After analysing the survey results from 225 factory sites and interviews from some respondents, we elicited the common challenges for promoting security measures for the factory systems.

Keywords: Operational technology (OT) security, Risk analysis of cybersecurity for factory system, Risk assessment tool for factory system

https://openaccess.cms-conferences.org/publications/book/978-1-958651-90-2/article/978-1-958651-90-2_36

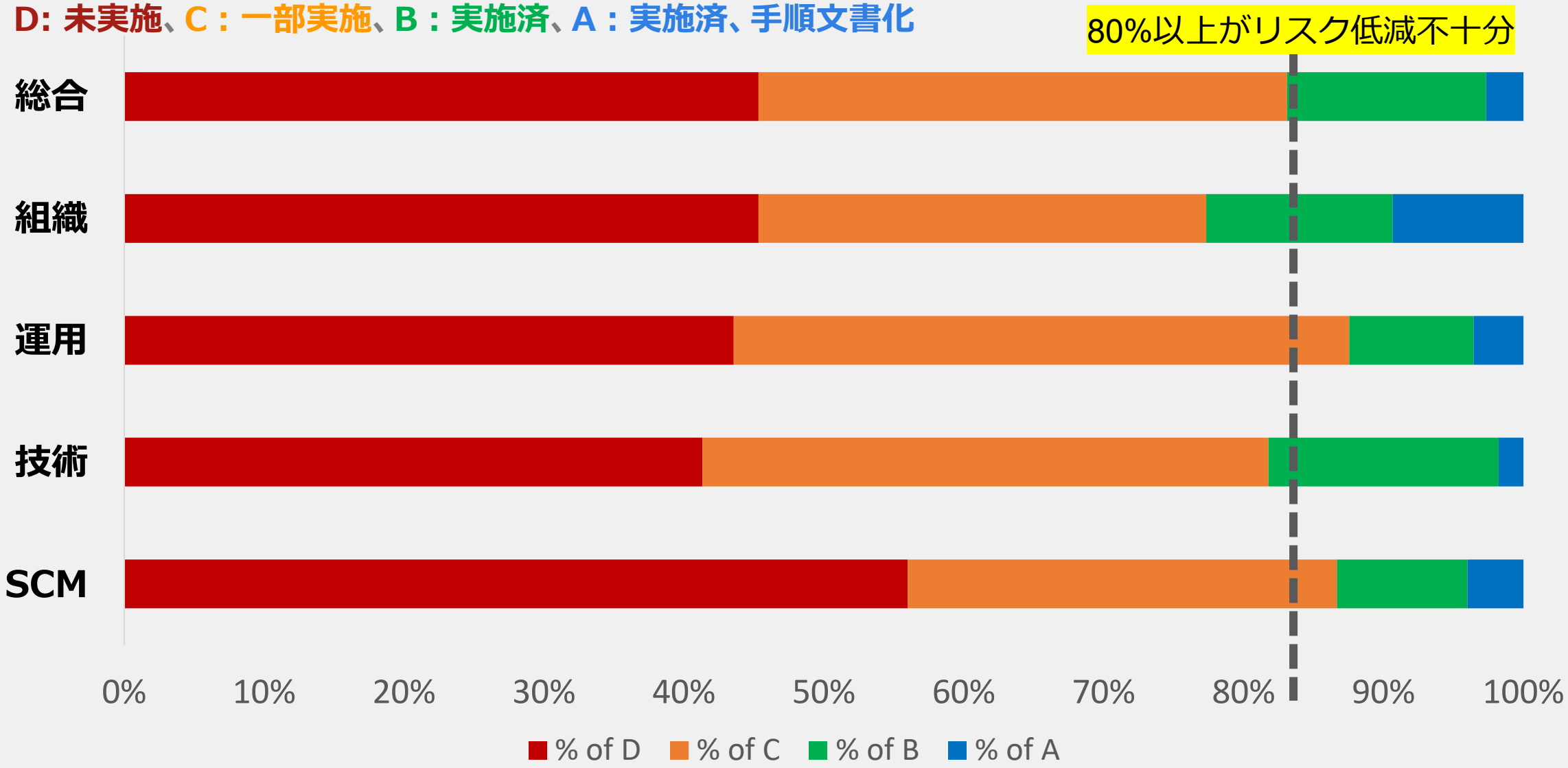


-Japanese
https://github.com/OTSec-Hiroshi-Sasaki/ja-ot-security-simple-assessment
- English
https://github.com/OTSec-Hiroshi-Sasaki/en-ot-security-simple-assessment

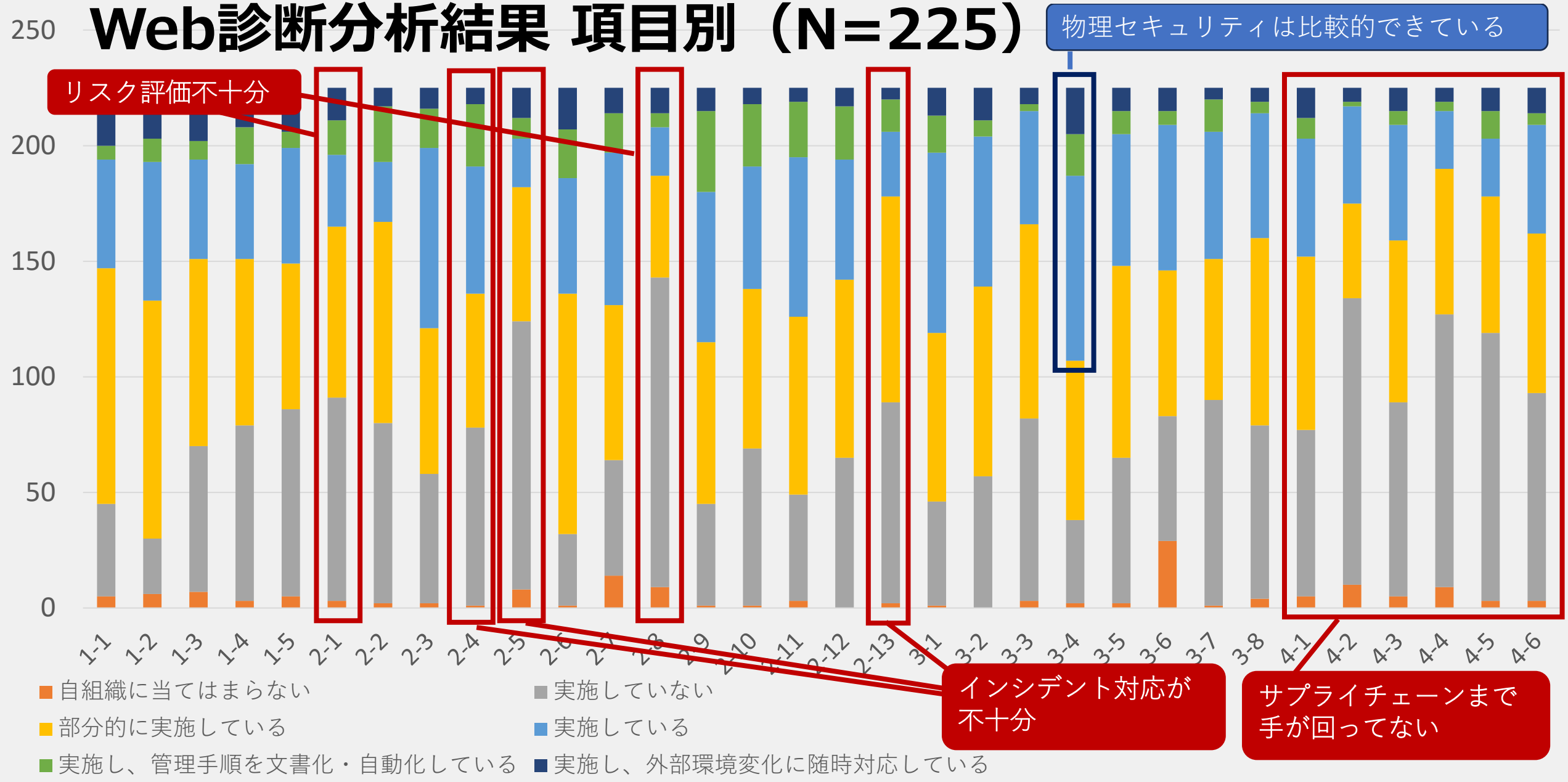
自身のPCローカルでチェックリストをもとにした診断が可能

Web診断分析結果（N=225）

D: 未実施、C：一部実施、B：実施済、A：実施済、手順文書化



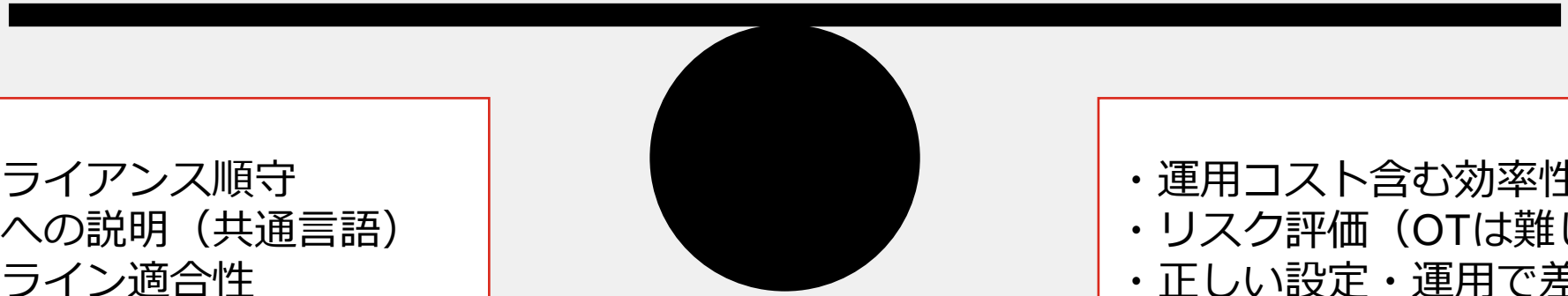
Web診断分析結果 項目別（N=225）



経済産業省の工場セキュリティガイドラインを活用して「説明責任」と「実効性」の両方を実現

説明責任

実効性



・コンプライアンス順守
・取引先への説明（共通言語）
・ガイドライン適合性
↓

但し、形骸化しやすいことに注意

・運用コスト含む効率性
・リスク評価（OTは難しい）
・正しい設定・運用で差がでる
↓

組織・運用・技術のバランス大事

“経済産業省のガイドラインに適合しています！”

“経済産業省のガイドラインを参考に自社のリスク応じた対策に落とし込んでいます！”

25

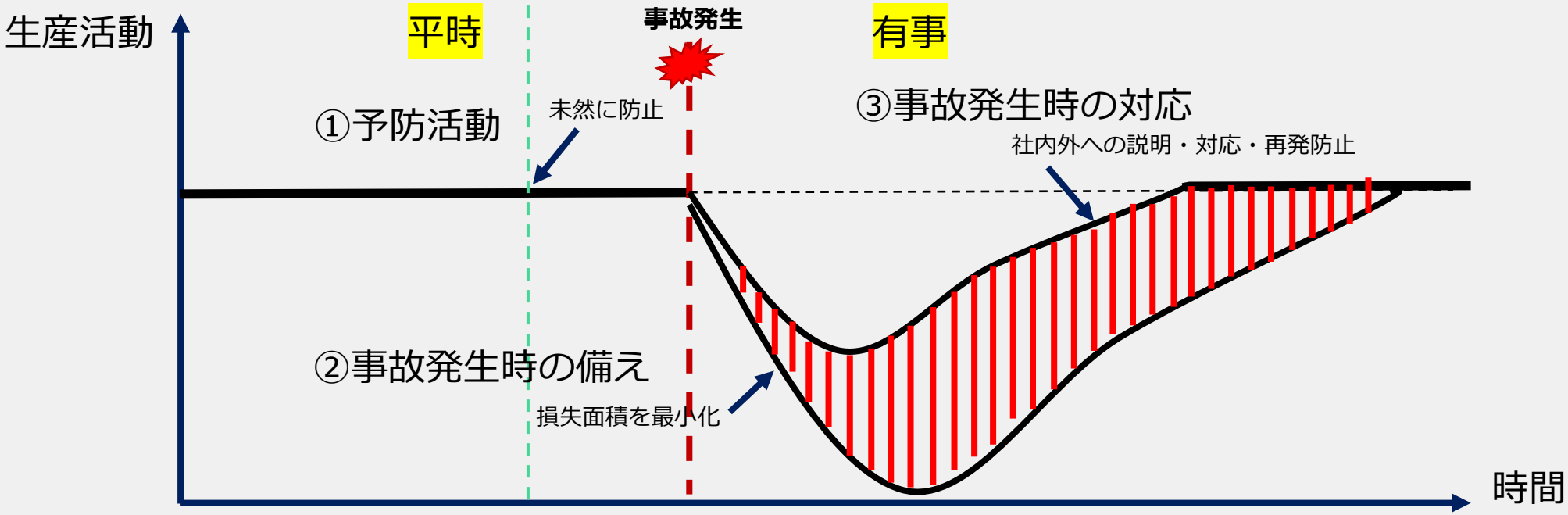
レジリエンスの考え方

「DX×セキュリティ」 = 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

①セキュリティ事故予防

②セキュリティ事故発生時の備え

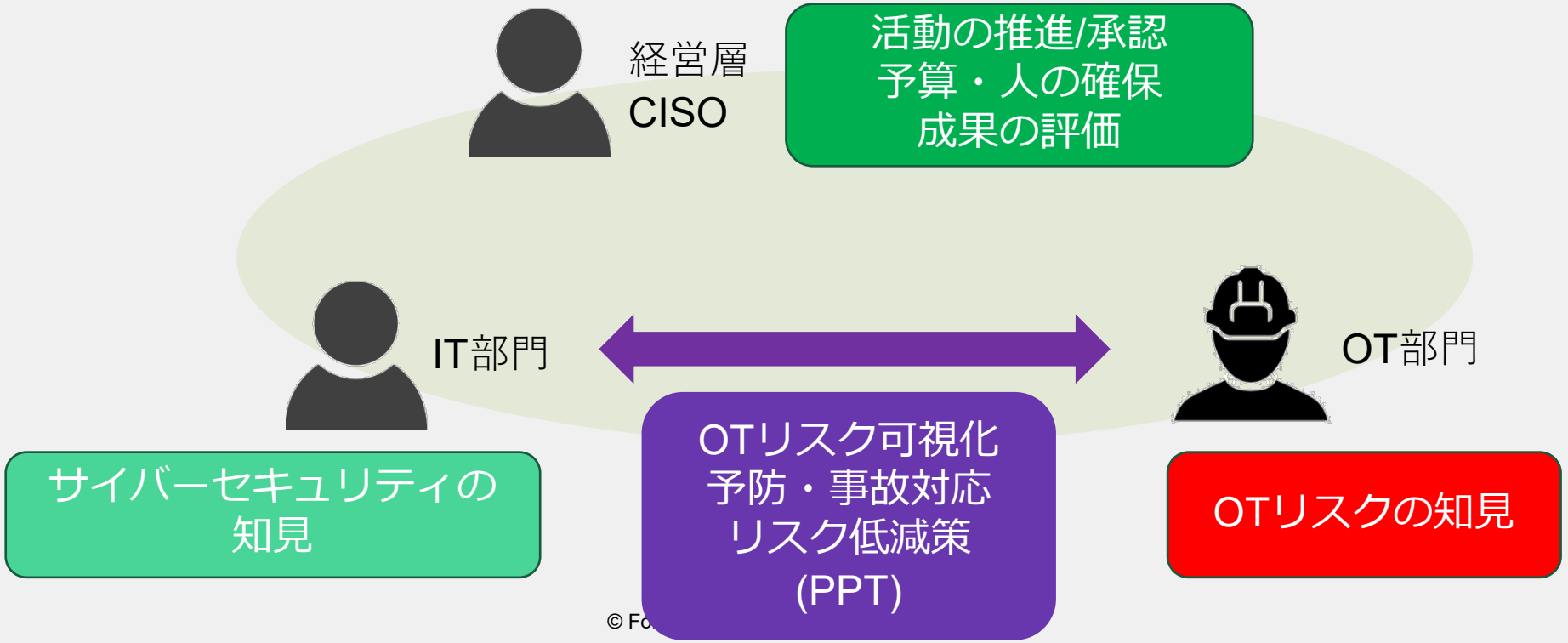
③セキュリティ事故発生時の対応



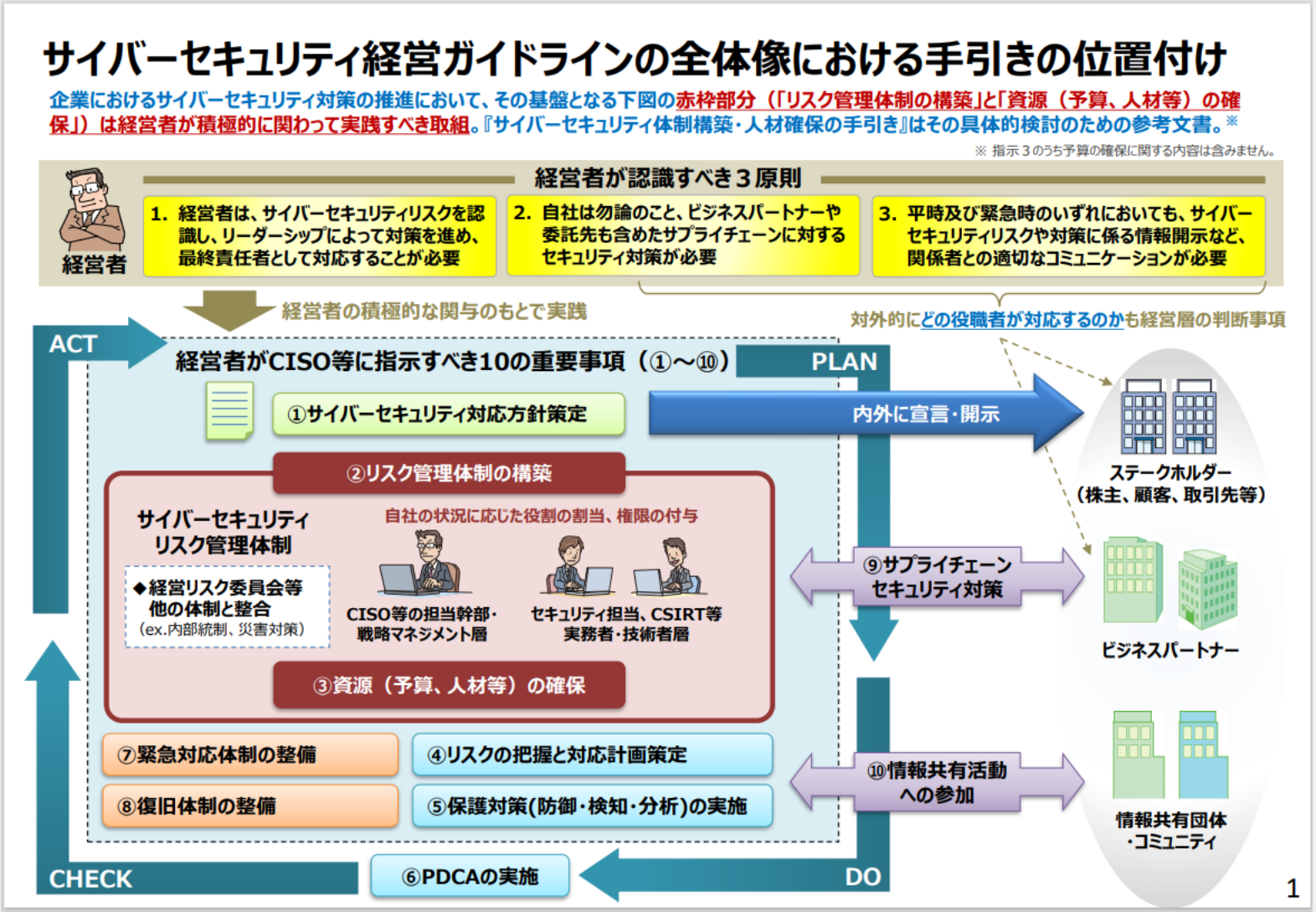
今後のサイバーセキュリティのリスク対応は「防御の高度化」から「事故対応の高度化」へとシフトする

ガイドラインを活用したIT/OT部門間連携の取組例

No.	確認項目
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。
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。
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。
1-4	工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている。



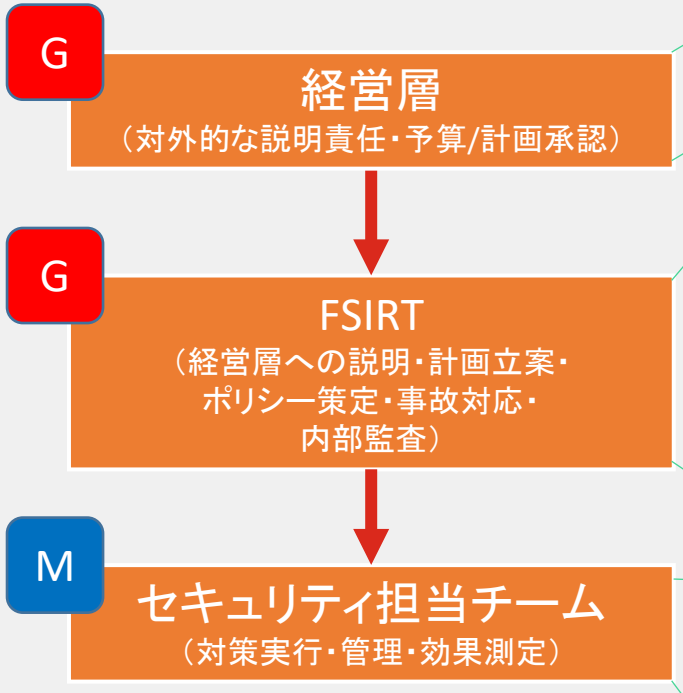
参考資料：経済産業省
「サイバーセキュリティ体制構築・人材確保の手引き」①



https://www.meti.go.jp/policy/netsecurity/tebiki_taisei_jinzai.html

自社の組織に照らした「ガバナンス体制」を考える

① 以下の体制を考えてみる

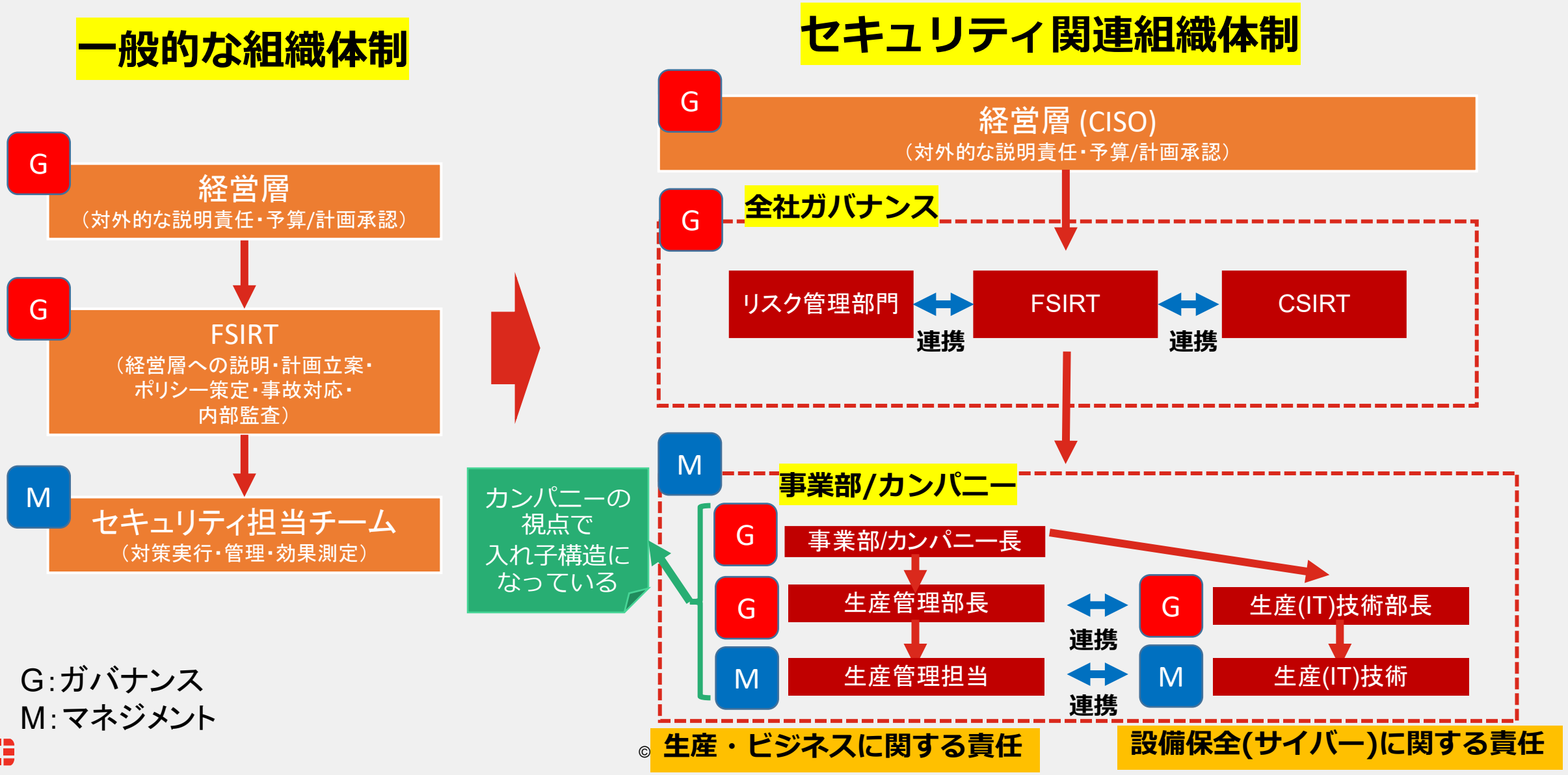


「M：マネジメント」の部分は、最終的に外部委託も可能

担当チーム	役割（予防）	役割（事故対応）
事業所長	・本社に向けての工場セキュリティ管理の説明責任 ・制御システムリスクアセスメントをもとにした対策計画の承認	・工場のセキュリティ事故時の判断責任
工場IT管理リーダー	・制御システムリスクアセスメントをもとにした対策計画の予算化立案 ・セキュリティ管理担当者の人事評価（キャリアパス構築） ・工場・プラントのセキュリティポリシー策定・更新（資産管理・脆弱性管理・リスクアセスメント・監視・事故対応） ・工場・プラントのセキュリティポリシー遵守の監査	・工場・プラントのセキュリティ事故時の判断 ・セキュリティポリシー違反者への注意・処罰
生産管理	・制御システムリスクアセスメントをもとにした対策計画の予算化立案 ・工場・プラントのセキュリティ管理の実行責任	・工場・プラントのセキュリティ事故時の判断 ・制御システムにおけるセキュリティ事故対応
生産技術リーダー	・制御システムセキュリティ対策立案・実施 ・制御システムの資産管理実施 ・制御システムにおけるセキュリティ事故対応手順策定・更新	・制御システムにおけるセキュリティ事故対応
工場IT管理担当者（子会社）	・制御システムセキュリティリスクの情報収集 ・制御システム資産管理・脆弱性管理（ベンダー、SI 管理） ・制御システムセキュリティリスクアセスメントの定期実施 ・制御システムセキュリティ監視（SOC） ・制御システムにおけるセキュリティ事故対応手順策定・更新	・制御システムにおけるセキュリティ事故対応
生産技術	・制御システムセキュリティ対策立案・実施 ・制御システムにおけるセキュリティ事故対応手順策定・更新	・制御システムにおけるセキュリティ事故対応

「製造業のサイバーセキュリティ」より抜粋

事業部・カンパニーのガバナンス体制例



G:ガバナンス
M:マネジメント

まとめ

製造業のDX推進に伴い、**サイバーセキュリティリスクが増大**し、
規制強化によって**企業の説明責任**が求められている

ガイドライン順守の**「説明責任」**だけでは形骸化する
リスク低減を意識した**「実効性」**対策を両立することが大事

経産省の工場セキュリティガイドラインの活用で
「組織」「運用」「技術」
のバランスの取れた対策を実施することが大事
まずは「組織（People）」から始めて
安全に「儲ける」ビジネスへ

31


FORTINET

「スマート工場化での システムセキュリティ対策事例調査 報告書」 ご紹介

2024年2月26日

独立行政法人情報処理推進機構
セキュリティセンター　脆弱性対策推進部

IPA Better Life with IT

本日の講演内容

１．報告書の位置づけ

- 工場SWGにおけるIPA
- 報告書の目的・特長

２．報告書の全体像

- 目次構成、工場セキュリティガイドライン工場との対応関係
- セキュリティ対策実施例の記載内容

３．報告書の記載内容（抜粋）

- 事業者のセキュリティガバナンス体制
- 生産システムのシステム構成図とデータフローの整理
- セキュリティ対策状況

1. 報告書の位置づけ

工場SWGでのIPAの位置づけ

◆工場SWGとIPAの関係

経済産業省・工場SWG：工場システムのセキュリティ対策を実施する上で
参考となるような**考え方やステップ**を提示

- **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（工場セキュリティガイドライン）**
- **チェックリスト**

Webページ相互参照

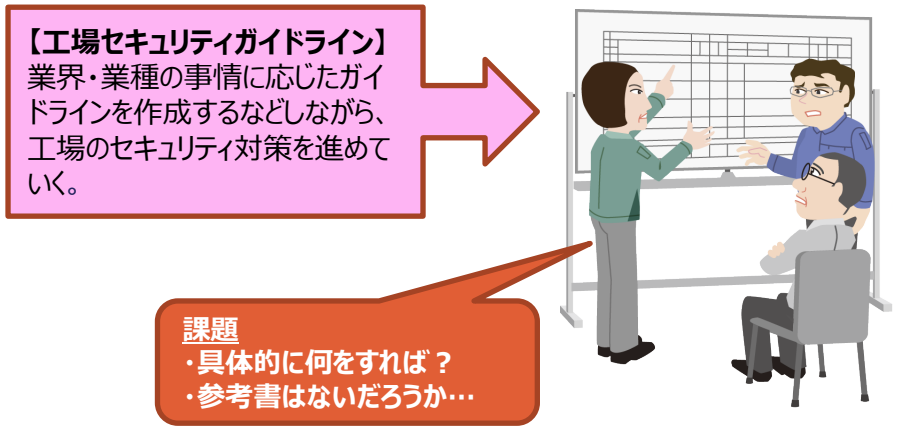
IPA セキュリティセンター脆弱性対策推進部：
工場セキュリティガイドラインに沿った工場での実践例を紹介

- **スマート工場化でのシステムセキュリティ対策事例 調査報告書**
- **産業用制御システム向け侵入検知製品等の導入手引書**

「スマート工場化でのシステムセキュリティ対策事例調査 報告書」
報告書の目的・特長

◆報告書の目的

工場セキュリティガイドラインに沿った工場セキュリティ対策の実装を支援し、
国内企業のスマート工場化が進むことを支援。
＜工場の生産システムにおけるセキュリティ対策を実施する際の参考書＞



◆報告書の特長

- 汎用的なセキュリティ対策の提示
  国内モデル事業者1社の調査、国内事業者8社の追加ヒアリングでの汎用化
- 工場のライフサイクルに沿ったセキュリティ対策の整理（次スライド）
- 「工場セキュリティガイドライン チェックリスト35項目」との対応関係の明示

◆想定読者

- 工場セキュリティ担当者
- 工場を保有する事業者のセキュリティ担当者

https://www.ipa.go.jp/security/controlsystem/securityreport-smartfactory-2023.html
よりダウンロード可能

2023年7月31日公開
報告書127頁, 別紙1頁

生産システムのライフサイクルに沿った調査

◆工場のライフサイクルに沿って対策を整理

- 生産システムの「設計・開発」から、「運転・運用」、「保守」、「廃棄」の各フェーズで実施されているセキュリティ対策を調査。

- また、各フェーズで共通する「調達」「情報管理」「人員管理」「インシデント対応」も調査。

生産システムのライフサイクルにおける対策実施例の調査

設計・開発	・リスク分析の実施　・外部接続への対策 ・ネットワークへの対策　・計算機への対策　など
運転・運用	・アカウント管理　・資産の管理 ・権限の設定　・ネットワークの構成の管理　など
保守	・資産の管理　・情報記憶メディアの管理 ・変更の管理
廃棄	・情報記憶メディアの廃棄

調達・情報管理・人員管理・インシデント対応

・取引先の信頼性の検証、
調達時のセキュリティ要求仕様の提示
・保管情報の管理、内部監査の計画、
制限区域の監視人員の管理、
セキュリティ教育と訓練　等

2. 報告書の全体像

全体目次構成

※青字はセキュリティ対策記載した箇所

生産システム設計開発の目次構成 ：3.1

制御システムのネットワーク、PCサーバー（計算機）、コントローラやIoT機器（制御機器）におけるセキュリティ対策事例について、細かく記載している。

3.1.2. ネットワークへの対策
- 3.1.2.1. ゾーン分割と監視
- 3.1.2.2. ネットワーク境界の保護
- 3.1.2.3. 無線 LANへの対策
- 3.1.2.4. 不正機器接続への対策

3.1.3. 外部接続への対策
- 3.1.3.1. DMZの設置
- 3.1.3.2. リモート接続の認証
- 3.1.3.3. 通信やデータの保護と制限

3.1.4. 計算機への対策
- 3.1.4.1. アカウント管理
- 3.1.4.2. 警告メッセージによる抑止
- 3.1.4.3. 権限の設定
- 3.1.4.4. セッションのロック
- 3.1.4.5. 外部メディア利用の制限
- 3.1.4.6. 通信の管理
- 3.1.4.7. 通信の完全性の保護
- 3.1.4.8. ソフトウェアの管理
- 3.1.4.9. マルウェア対策
- 3.1.4.10. ログの取得・確認
- 3.1.4.11. セキュリティ機能の確認
- **3.1.4.12. 入力値の確認**
- 3.1.4.13. エラーメッセージ
- **3.1.4.14. 安全な停止**
- 3.1.4.15. リソースの監視
- 3.1.4.16. DoS攻撃対策
- 3.1.4.17. 機器のバックアップと復旧

3.1.5. 制御機器への対策
- **3.1.5.1. 物理的な保護**
- 3.1.5.2. 警告メッセージによる抑止
- 3.1.5.3. 外部メディア利用の制限
- 3.1.5.4. ソフトウェアの管理
- **3.1.5.5. ログの取得・確認**
- 3.1.4.6. セキュリティ機能の確認
- **3.1.4.7. 入力値の確認**
- 3.1.4.8. エラーメッセージ
- 3.1.4.9. 安全な停止
- 3.1.4.10. リソースの監視
- 3.1.4.11. 機器のバックアップと復旧

※赤字は制御システムならではのセキュリティの取り組みについて、記載がある。

工場セキュリティガイドライン(付録E)との対応関係：1.2／別紙

本報告書に記載されたセキュリティ対策事例と、工場セキュリティガイドライン（付録E）との対応関係について、別紙（Excelファイル）にまとめている。

＜別紙抜粋＞

No.	実施例該当箇所	CPSFにおける対応項目	「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」における対応項目
4	3.1.1 リスク分析の実施	AM-7,BE-3,GV-4,RA-3,RA-4,RA-5,RA-6,RM-1,RM-2,SC-2,RP-3,CO-2,CO-3	0-1,0-2,0-3,2-1,2-2
5	3.1.2 ネットワークへの対策		
	3.1.2.1 ゾーン分割と監視	AC-7	0-2,3-5
	3.1.2.2 ネットワーク境界の保護	AC-7,AC-8,CM-1	2-3,3-7
	3.1.2.3 無線LANへの対策	AC-3,AC-8	2-7
	3.1.2.4 不正機器接続への対策	AC-8,CM-1,CM-6	
6	3.1.3 外部接続への対策	AM-5,DS-9,PT-2,CM-4	2-3
	3.1.3.1 DMZの設置		
	3.1.3.2 リモート接続の認証	AC-6,AC-8,AC-9	3-6
	3.1.3.3 通信やデータの保護と制限	CM-5,DS-2,DS-3,DS-4,DS-5	3-3
7	3.1.4 計算器への対策		
	3.1.4.1 アカウント管理	AC-1,AC-4	2-10
	3.1.4.2 警告メッセージによる抑止		
	3.1.4.3 権限の設定	AC-5	
	3.4.1.4 セッションのロック	AC-4	
	3.4.1.5 外部メディア利用の制限		
	3.4.1.6 通信の管理	AC-8	
	3.1.4.7 通信の完全性の保護	DS-11,CM-4	
	3.1.4.8 ソフトウェアの管理	DS-10,IP-2	3-3
	3.1.4.9 マルウェア対策	CM-3	2-12,3-1
	3.1.4.10 ログの取得・確認	AM-3,MA-2,PT-1,AN-3	3-8

セキュリティ対策事例の記載内容(1)：2章以降

- 実施例

  モデル事業者の取り組みについて記載

  ✓ セキュリティ規定文書

  ✓ 規定内容

- 関連帳票

  取り組みの内容を実施するにあたり作成している帳票のサンプル

3.1.7. 資産の管理

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ 資産台帳の作成

資産の一覧を記載した台帳を作成し、定期的に棚卸を実施し、記載漏れや誤りがないことを確認する。これらの台帳は、定められた期間保管するとともに、意図せず改ざんされないように対策を行う。

・ 法令や契約を遵守した取得・保有

特にソフトウェアについて、不正コピーやライセンス違反など、法令や契約に違反する形で取得・保有していないことを定期的に確認する。

- 関連帳票

✓ 資産台帳の作成

資産の用途、設置場所、管理者等の情報を管理している。

表 5 資産台帳

#	ID	名称	種類	用途	ソフト	設置場所	管理者
1	XXX	ロボット PC	サーバ	ロボットへの指示を作業単位で管理	・OS:XXX ・ミドル:XX	XXX	XXX
2	YYY	XX 制御	コントローラ	ロボット制御	-	YYY	YYY
3	…						

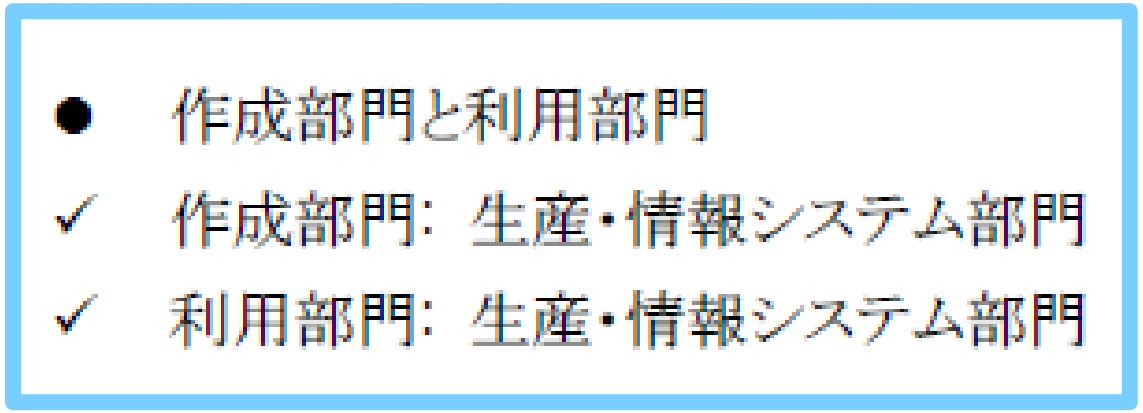
セキュリティ対策事例の記載内容(2) ：2章以降

- 作成部門と利用部門

  社内で取り組みの内容を規定する規則を作成する部門と、その規則を利用する部門を示す。

- 必要度

  モデル事業者において、取り組みへの対応を必須としているか推奨としているかを示す。



セキュリティ対策事例の記載内容(3) ：2章以降

- **脅威**

  取り組みがどのような脅威を想定したものであるかを示す。

- **実施例により低減されるリスクと残留リスク**

  取り組みにより低減されるリスクと、残留するリスクを示す。残留するリスクは、別の取り組みを組み合わせることによって対応が必要となる。

- **スマート化に際しての考慮事項**

  スマート化に際しての課題と留意点に対し、考慮している事項を示す。

- 脅威

  対策が不十分な資産を目標として攻撃される可能性がある。

- 実施例により低減されるリスクと残留リスク

  把握が漏れることにより、対策が未実施となる資産を減らすことができる。
  一方で、対策内容の妥当性については、別途リスク分析により検討をする必要がある。

- スマート化に際しての考慮事項

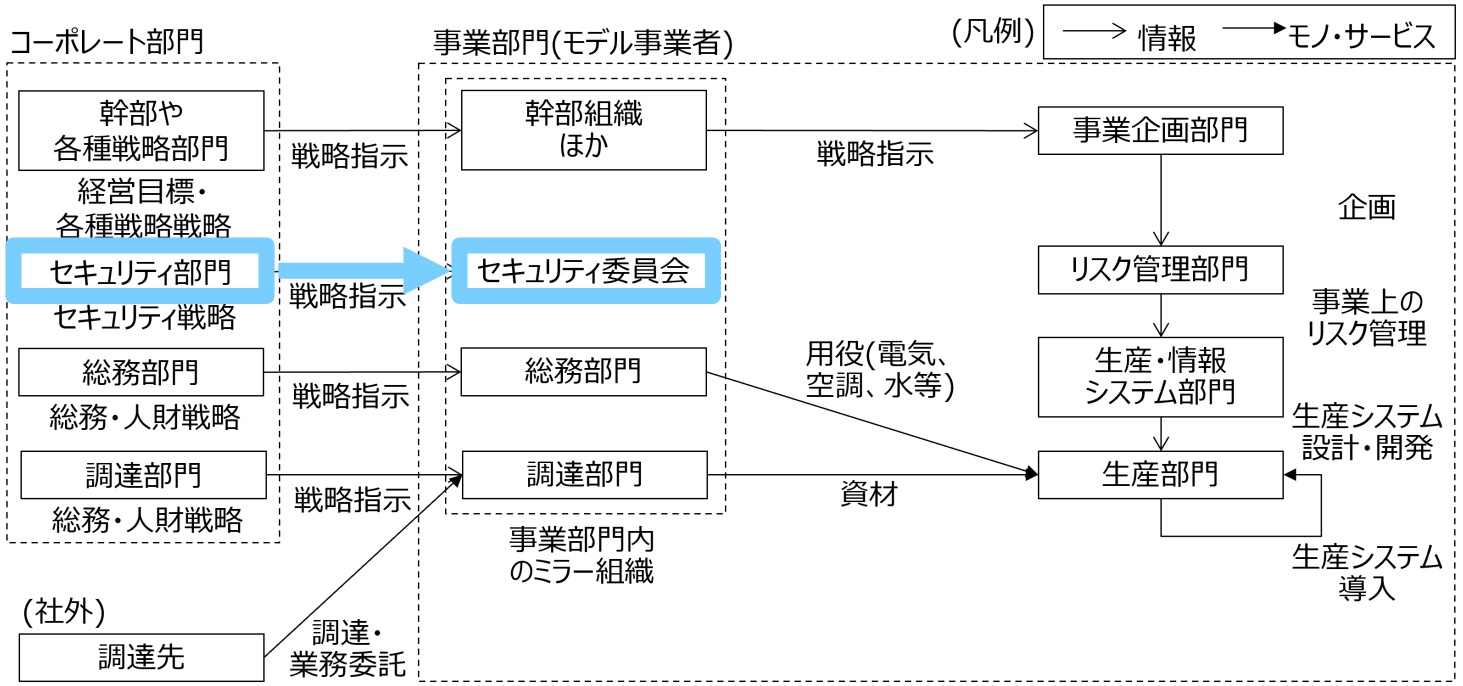
  スマート化のための IoT 機器を含む資産類は、他組織からの借用による導入の場合や、従来の PC/サーバと比べ消耗(交換)の期間が短い場合が多い。そのため、資産管理の内容に借用期間や借用元、交換時期、効果に予定時期などの記載を追加することが望ましい。また、各種期間や時期に合わせて従来よりも高頻度で管理台帳の更新・点検が求められる。さらに、管理機器が従来よりも増加する点にも留意が必要である。そのため、自動化ツールやサービスを導入する場合もある。

3. 報告書の記載内容（抜粋）

モデル事業者全体のガバナンス体制 ：1.3.1(1)

付録E	組織的対策 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。

- コーポレート部門（本社機能）のセキュリティ部門
- 事業部門（工場）のセキュリティ委員会
  コーポレート部門（本社機能）にあるセキュリティ部門に対応するミラー組織。



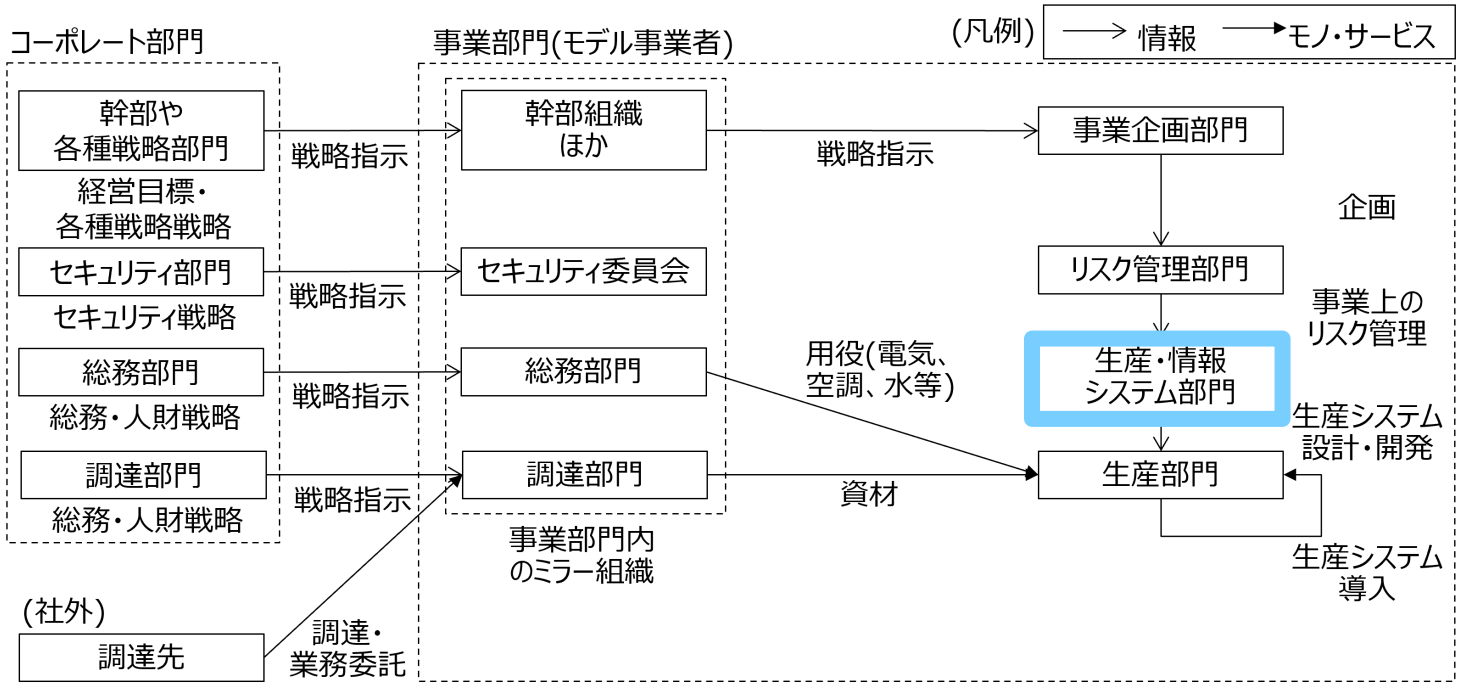
コーポレート部門と事業部門（工場）の関係

モデル事業者全体のガバナンス体制 ：1.3.1(1)

付録E	組織的対策 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。

- 生産・情報システム部門

  このモデル事業者では生産システムも情報システムも同じ部門が一括で担当。ネットワークでつながった生産システムと情報システムを同一の部門で管理。



コーポレート部門と事業部門（工場）の関係

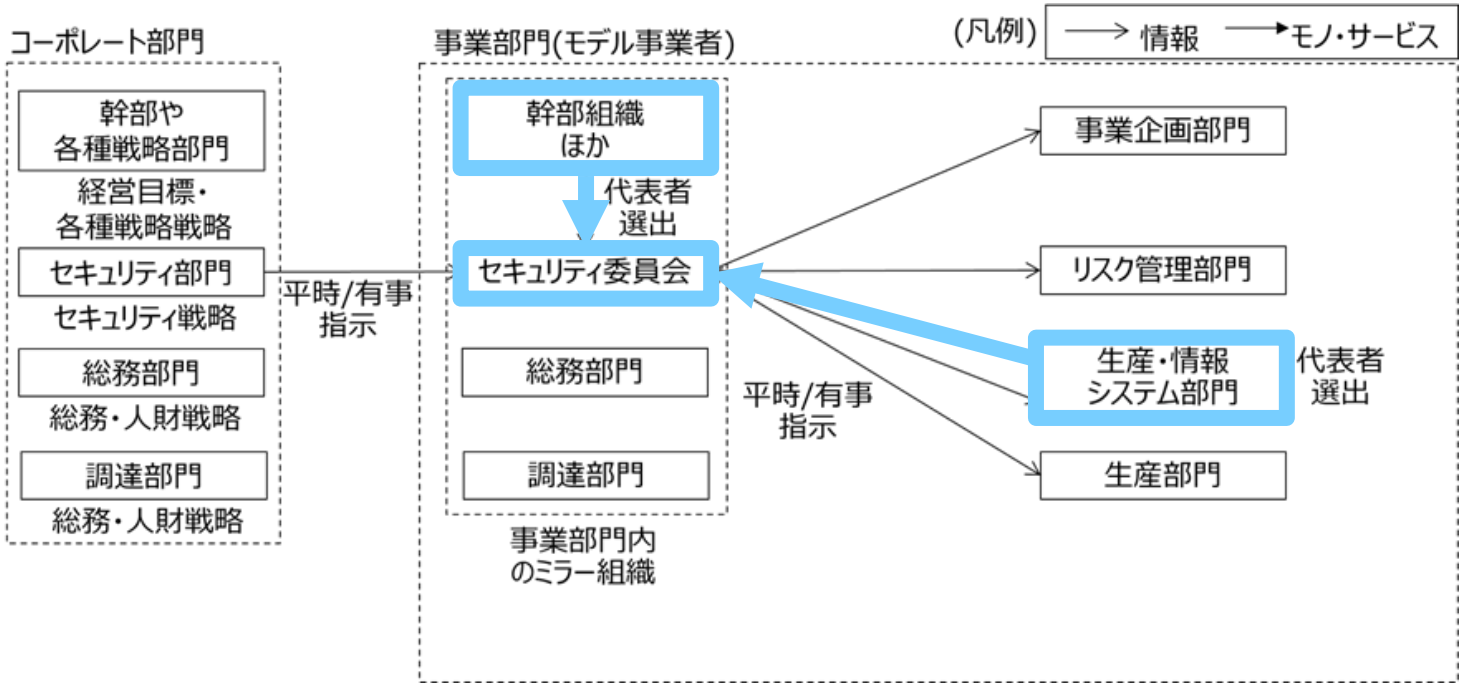
工場のセキュリティガバナンスの仕組み：1.3.1(1)

付録E	組織的対策 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。
	組織的対策 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。

- 事業部門（工場）のセキュリティ委員会

  幹部組織や生産・情報システム部門から選出された代表者で構成するセキュリティ委員会が存在する。

  生産・情報システム部門や生産部門などに対して指示を行うガバナンス機能をもつ。



平時・有事におけるセキュリティガバナンス

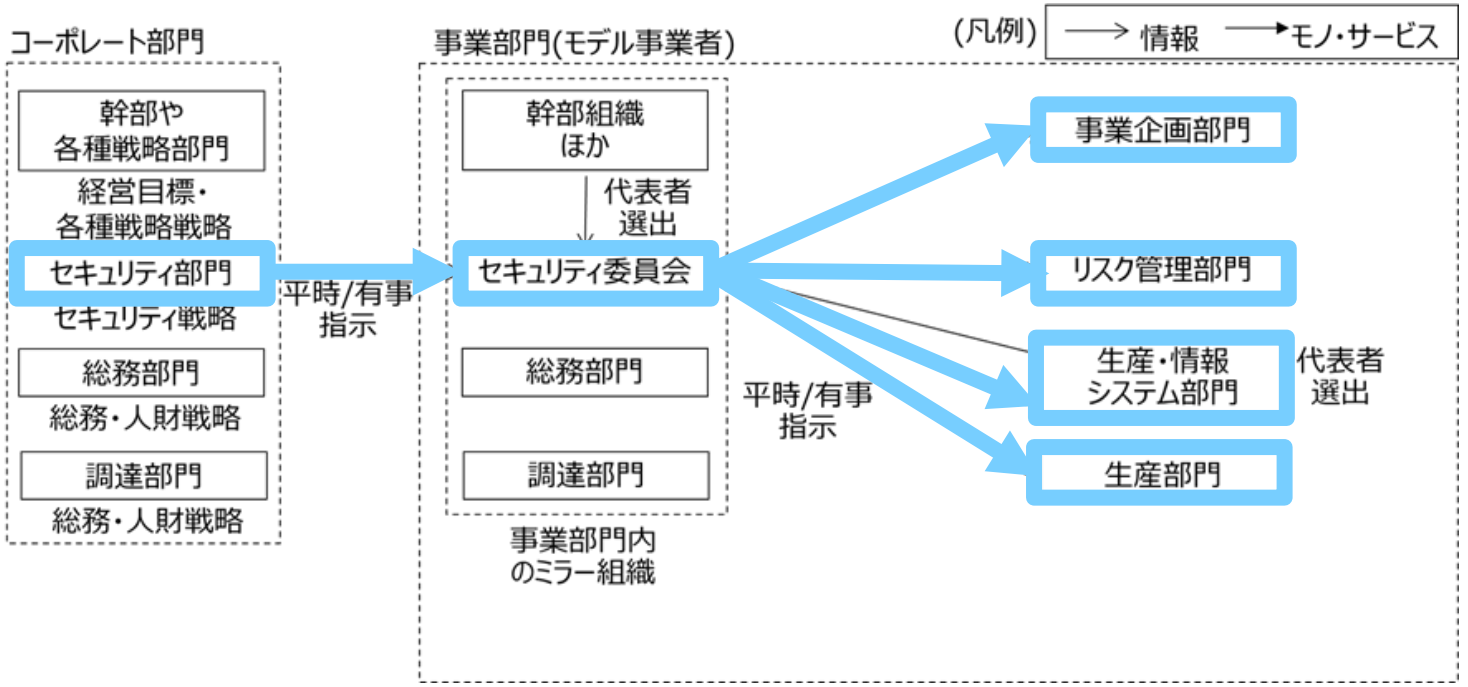
工場のセキュリティガバナンスの仕組み：1.3.1(1)

付録E	組織的対策 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。
	組織的対策 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。

- 事業部門（工場）のセキュリティ委員会

  幹部組織や生産・情報システム部門から選出された代表者で構成するセキュリティ委員会が存在する。

  生産・情報システム部門や生産部門などに対して指示を行うガバナンス機能をもつ。



平時・有事におけるセキュリティガバナンス

生産システムの脆弱性対応の流れ：1.3.1(1)

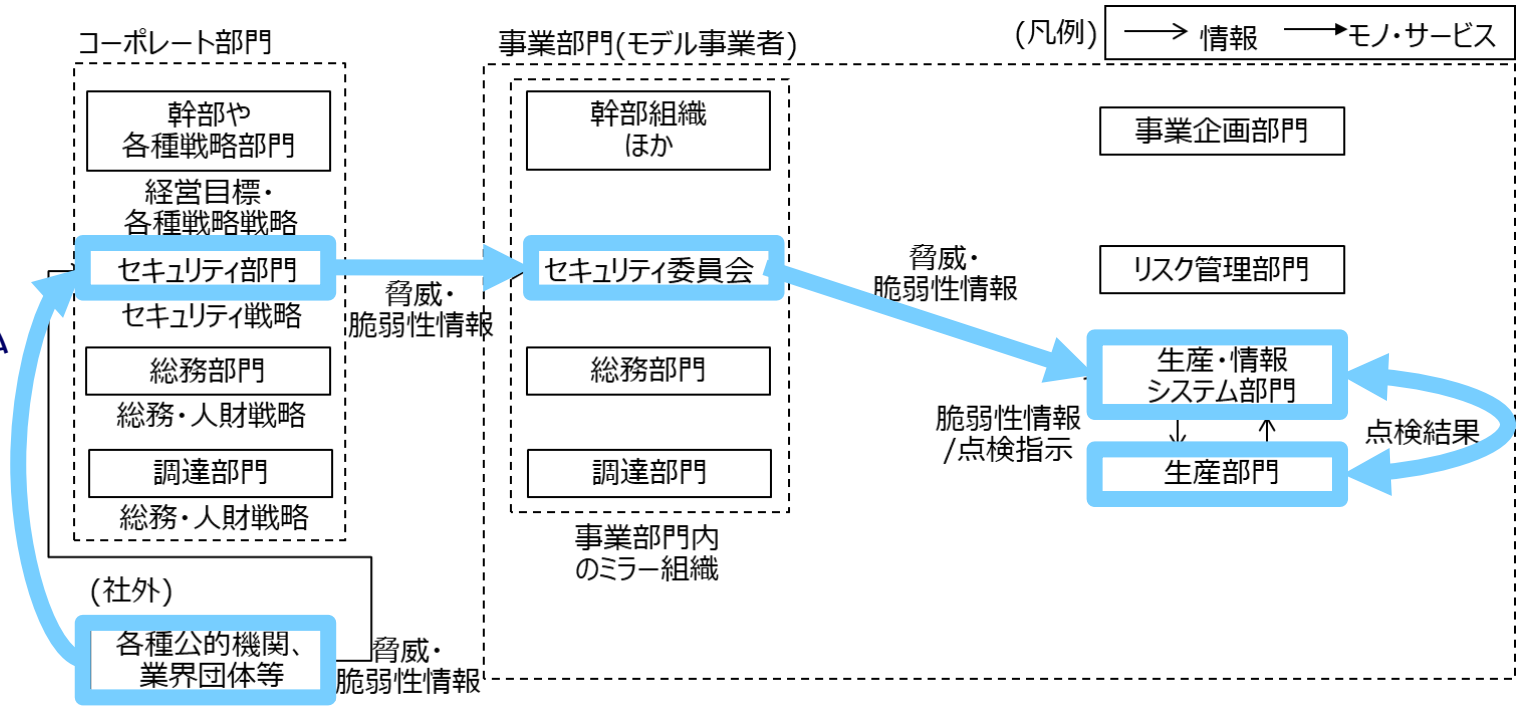
付録E	組織的対策 1-5	工場セキュリティに関する脅威の動向などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの現場教育を行っている。

- 生産システム（制御システム）の脆弱性対応フロー

(1)コーポレート部門（本社）が社外の脅威・脆弱性情報を収集、事業部門（工場）のセキュリティ委員会へと展開

(2)事業部門のセキュリティ委員会が生産・情報システム部門へ情報を展開

(3)生産・情報システム部門が対応の必要性を判断し、生産部門と連携して脆弱性点検や対応を実施

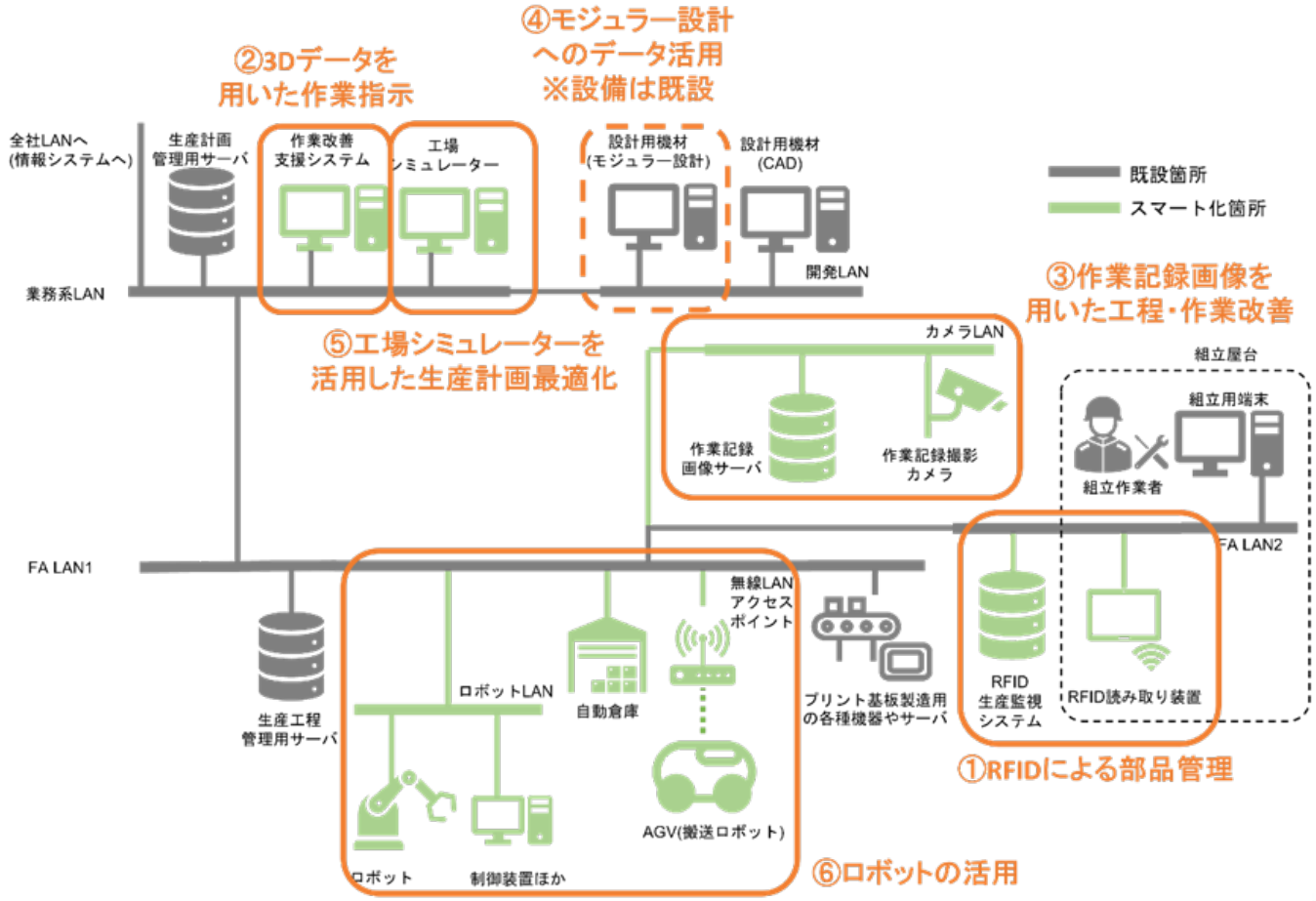


生産システムの脆弱性対応

モデル事業者の生産システム構成：1.3.1(2)

付録E	運用的対策 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。

モデル事業者では、設計や生産工程を効率化するために、生産システムから様々な情報を収集したり、収集した情報を基に設計データや生産工程を最適化するための仕組みを導入したりすることで工場をスマート化している



モデル事業者の生産システムにおけるスマート化の取り組み

生産システムのデータフロー抜粋：1.3.1(2)

付録E	運用的対策 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。

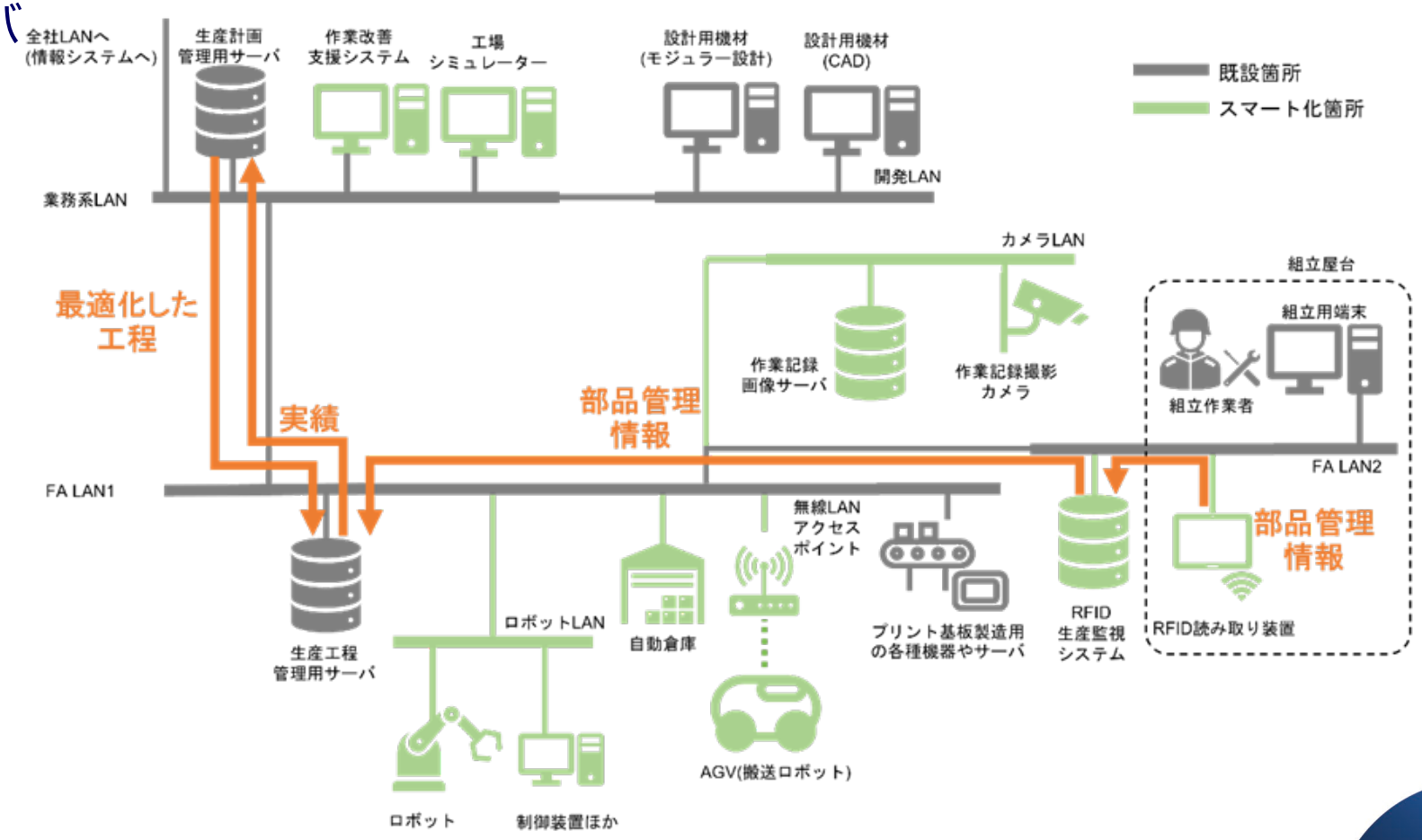
業務系LAN： 生産計画管理サーバ

FALAN1: 生産工程管理用サーバ

FALAN2:

RFID読み取り装置

RFID生産監視システム



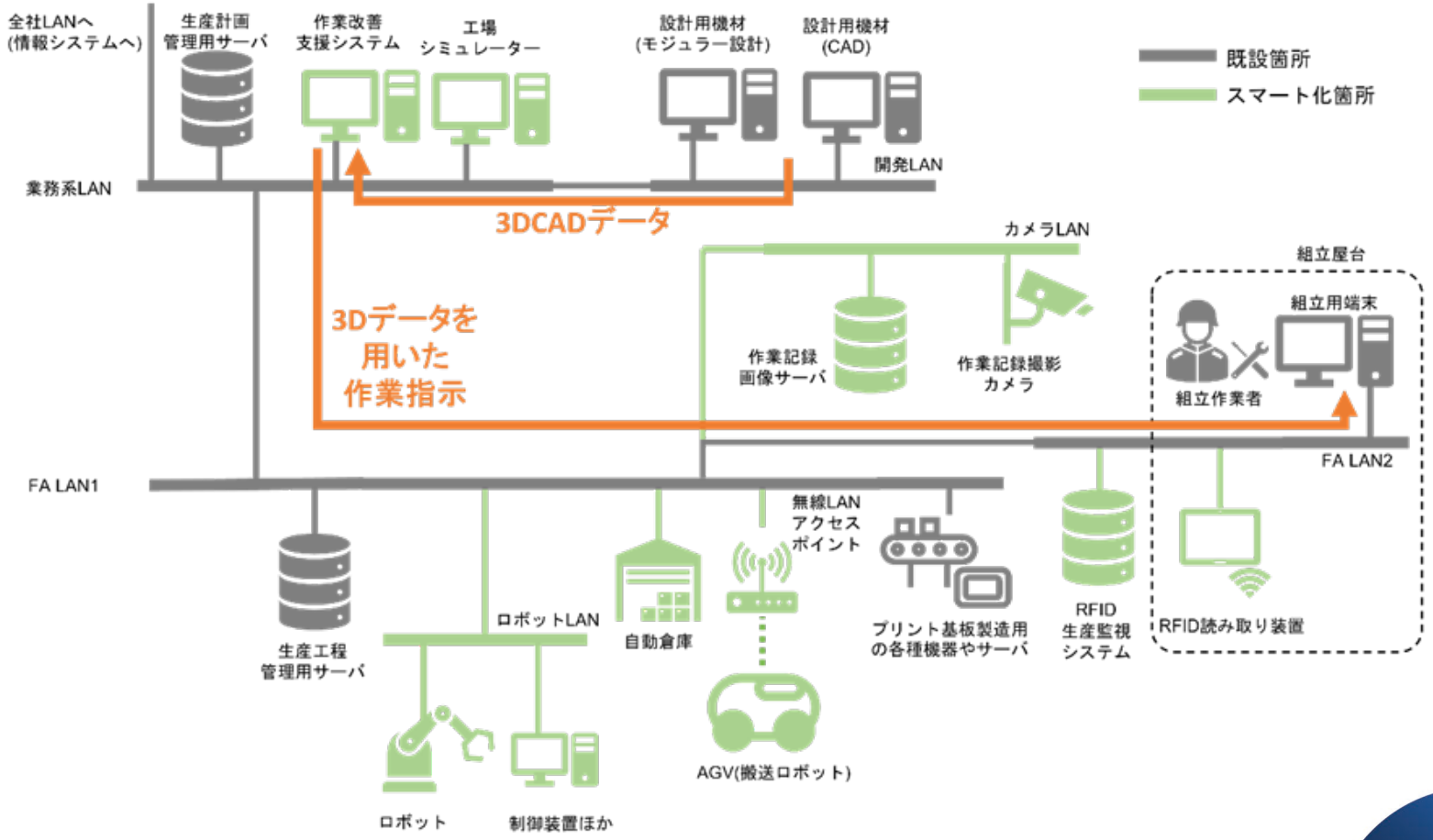
RFIDによる部品管理のデータフロー

生産システムのデータフロー抜粋：1.3.1(2)

付録E	運用的対策 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。

業務系LAN： 生産改善支援システム
開発LAN： 設計用機材

FALAN2:
RFID読み取り装置
RFID生産監視システム



3Dデータを用いた作業指示のデータフロー

ゾーン分割と監視：3.1.2.1

付録E	運用的対策 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。
	技術的対策 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）。

- 実施例

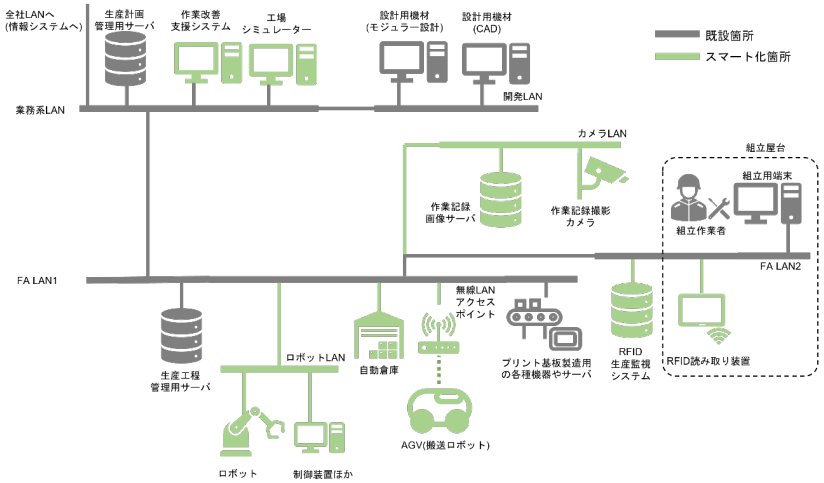
  セキュリティ規定文書：　セキュア開発手順

  以下のようにネットワークを分割する。

  ①IT環境とOT環境、②重要機能と補助機能、③外部ネットワークと内部ネットワーク

  ④生産管理システムと各生産ライン、⑤有線ネットワークと無線ネットワーク

  非常時には、これらのネットワーク間で通信を遮断し、最低限の事業を継続できるように設計する。



- 脅威

  ネットワークを経由してサイバー攻撃の被害が拡大する可能性がある。

- 低減されるリスクと残留リスク

  ネットワークを経由してサイバー攻撃の被害が拡大するリスクを低減することができる。

  システムの仕様上、分割困難なネットワークが残留する可能性がある。

  残留リスクを減らすためには、**システム設計の段階からセキュリティ上好ましいネットワーク分割を行えるように検討する必要がある。**

ログの取得・確認：3.1.5.5

付録E	技術的対策 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。

- 実施例

  セキュリティ規定文書：　セキュア開発手順

  - ログの取得対象

    制御機器ではログ機能がない場合もあるため、制御機器の立ち上げやシャットダウン時刻、変更時の内容などを台帳管理しておくとともに、それらの情報を改ざんされないように保存しておく。

  - ログの確認

    保守時には、前回保守の設定と比較し、不正変更がないことを確認する。

- 脅威

  制御機器の不正操作などによるサイバー攻撃が発生する可能性がある。

- 低減されるリスクと残留リスク

  ログを確認することで、過去に発生したサイバー攻撃を検知できる場合がある。

  サイバー攻撃そのものの発生を防止することはできないため、各種対策が必要。ログの定期確認をするまではサイバー攻撃の有無を確認できないほか、ログが削除された場合や、ログに記録が残らないような攻撃の場合は検出が不可能であるため、**インシデント対応などにより被害を最小化するといった対策も必要**。

機器のバックアップと復旧：3.1.5.11

付録E	技術的対策 3-12	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。

- 実施例

  セキュリティ規定文書： セキュア開発手順

  - バックアップ

    機器のデータバックアップを定期的に行う。

  - 復旧

    代替機を準備しておくほか、バックアップデータを基に**復旧するための手順を整理**しておく。

    また、**実際に復旧を行えることを事前に検証**しておく。

ランサムウェア対策を考慮する場合、
バックアップデータのオフライン保管、
イミュータブル化（不変化）が必要

- 脅威

  攻撃されたシステムを元の状態に復元できない可能性がある。

- 低減されるリスクと残留リスク

  システムを攻撃前の状態に復元できない可能性を低減できる。

  攻撃に利用された脆弱性は、システムを復旧しても残留したままであるため、別途根本的な対策が必要となる。

資産の脆弱性の管理： 3.1.10

付録E	技術的対策 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している。もしくは代替策を講じている。
	工場システム SC*管理 4-3	納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダ・構築業者との連絡・連携体制を構築している。

* SC: サプライチェーン

- 実施例

  セキュリティ規定文書： セキュア開発手順

  - 脆弱性情報の一覧管理

    資産の管理と連動し、関連する脆弱性情報を収集する。

    主に、関連資産に対してパッチの適用を検討することになるが適用の可否や適用タイミングなどは事業への影響や対処を見送った場合の影響などを考慮して決定する。

- スマート化に際しての考慮事項

  利用するIoT機器やサービスが多様化した際、それらの脆弱性・パッチ管理を自組織のみで実施するのは管理負荷が大きくなる可能性があるため、**機器やサービスの提供ベンダーとの協力体制を構築することが重要である**。また、上記のベンダーに対して、**該当機器やサービスの脆弱性が見つかった際の報告義務について契約時に合意する必要がある**。

脆弱性管理台帳

#	関連資産	脆弱性 (CVE-IDなど)	深刻度 (CVSSなど)	パッチ適用可否	パッチ適用時期	パッチ適用状況
1	XXX	CVE-XX	大	可	即時	済
2	XXX	CVE-YY	小	可	保守に合わせて実施	未適用
3		…				

取引先の信頼性の検証： 3.2.1

付録E	工場システムSC*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。

＊ SC: サプライチェーン

- 実施例

  セキュリティ規定文書： 調達基準

  ◆ 取引先の確認

  取引先が十分な品質のサービスや製品を提供できる組織であることを確認する。

  ①直近の決算状況、②離職率などの組織としての健全性

  ③近年の人員や売上等の変化と原因 ④各種認証などの取得状況

  ⑤調達先での製造工程での品質管理

- 脅威

  品質が不十分な製品、サービスを利用することで、それらを利用したサイバー攻撃を受ける可能性がある。

- 低減されるリスクと残留リスク

  組織が設定した品質水準に満たない製品・サービスを導入してしまい、そこを利用した攻撃を受ける可能性を低減できる。

  一方で、個々の製品・サービスのセキュリティ要件については本要件では保証しておらず、**別途セキュリティ要件や契約書の形で取引先に提示し、それらを順守させることでセキュリティを担保する必要がある**。

調達時のセキュリティ要求仕様の提示： 3.2.2

付録E	工場システム SC*管理 4-3	納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダ・構築業者との連絡・連携体制を構築している。
	工場システム SC*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。

＊ SC: サプライチェーン

- 実施例

  セキュリティ規定文書： 調達基準

  - セキュリティ要求仕様の提示

    ①全般的な要件:対応すべきセキュリティ規格・ガイドライン(ISMS、IEC 62443 等)

    ②サービスや製品の提供元に対しての要件

    開発環境の物理的なセキュリティ、遵守すべき規則、サードパーティ製品の脆弱性確認、出荷前のウイルス検査

    ③サービスや製品に対しての要件

    データの保護、通信の保護(特にリモート接続など)

- 脅威

  組織が要求するセキュリティ水準に満たない機器を導入することで、それらを利用したサイバー攻撃を受ける可能性がある。

- 低減されるリスクと残留リスク

  提示したセキュリティ要件を調達先が満たすことで、脆弱な機器を利用した攻撃のリスクを低減できる。

  一方で、提示するセキュリティ要件の妥当性は組織が責任をもって検証する必要があるほか、調達先が提示したセキュリティ要件を満たしていることを受け入れ検査時に確認する必要もある。

インシデントへの対応と体制：7.2.1

付録E	組織的対策 1-4	事業継続計画（BCP）が策定されており、工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている。
	運用的対策 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。
	工場システム SC*管理 4-1	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。

＊ SC:　サプライチェーン

- 実施例

  セキュリティ規定文書：　情報セキュリティマネジメント規則

  - ◆ 必要な対応

    ①検知と分析　②封じ込め、根絶と復旧　③インシデント後の対応

  - ◆ 体制

    ①検知と分析　現場運転員が機器の異常としてあげた方向を見落とさないよう、

    ②封じ込め、根絶と復旧：事業継続に責任のある幹部層をトップとして適切な指示が出せるよう、全社的な連絡体制を構築する等。

    ③インシデント後の対応：　インシデント対応を通して得られた知見を組織間で共有できるよう、情報発信する組織、担当システムへの対象を検討する組織の整備。

- スマート化に際しての考慮事項

  モジュラー設計システムや工場シミュレーターなどを外部のサービスを利用して実現する場合や、ロボットやIoT機器などが他ベンダーからの借用や管理下にある場合、**関係するサービスプロバイダーやベンダーなどの他組織との連携を念頭に置いたインシデント対応計画が重要**。

\Orchestrating a brighter world NEC

セ事推-23-164

何してる？ 工場のセキュリティ対策

～ 工場セキュリティ対策の事例紹介 ～

2024年 2月 26日 (月)

NECプラットフォームズ株式会社　澤田 利幸

アジェンダ

1. 背景
2. 工場セキュリティ対策の実践とアセスメント
3. サイバー攻撃対応BCPと訓練
4. おわりに

会社紹介

商号	NECプラットフォームズ株式会社 (英文：NEC Platforms, Ltd.)
本社	東京都千代田区神田司町2-3
代表者	代表取締役 執行役員社長　河村 厚男
資本金	103億3千1百万円 (NEC全額出資)
売上高	単独 3,601億円 <2023年3月期>
社員数	単独 7,001名 <2023年3月末現在> (契約社員、パート、嘱託を含む)
主要事業	ICTシステム機器の開発、製造、販売、設置、保守およびシステムソリューション
開発・生産拠点	国内 14 (仙台、白石・米沢、福島、那須、我孫子、中河原、府中、玉川、高津、掛川、甲府、大月、関西OBP、松山)
営業拠点	国内 17 (東日本、関東甲信越、中部、関西、西日本の主要都市)
子会社	国内 1　(NEC静岡ビジネス) 海外 4　(NEC Platforms Thai Company Limited) (NEC Platform Technologies (Suzhou) Co., Ltd.) (NEC Platform Technologies Hong Kong Limited) (NEC Enterprise Communication Technologies, Inc.)

主要拠点

- **開発・生産拠点 14**
- **営業拠点 17**
- **子会社 5社**
  （国内1社、海外4社）

東京本社

国内開発・生産拠点 14

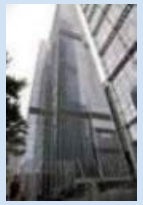
東北 北関東	 仙台事業所	（白石） 	（米沢）  白石・米沢事業所	 福島事業所	 那須事業所
首都圏	 我孫子事業所	 中河原事業所	 府中事業所	 玉川事業所	 高津事業所
東海 関西 四国	 掛川事業所	 甲府事業所	 大月事業所	 関西OBP事業所	 松山事業所

国内営業拠点 17

東日本、東京、中部、関西、西日本に17拠点

海外子会社 4社

NEC Enterprise Communication Technologies, Inc.



NEC Platform Technologies Hong Kong Ltd.

NEC Platforms Thai Co., Ltd.

NEC Platform Technologies (Suzhou) Co., Ltd.

国内子会社 1社

国内子会社：NEC静岡ビジネス

事業分野・提供技術

幅広い技術力を活かした製品やソリューション・サービスを提供します。

グローバル One Factory

**社内の開発・生産拠点が協調して1つのファクトリーのように振る舞い、
お客さまやパートナーと共創して、社会価値を創造します。**

各工場の強みによる提供価値

- 長期・耐環境 信頼性
- 小型化・軽量化
- カスタマイズ・受注生産(BTO)
- グローバルコスト
- 海外拠点での日本品質

共通基盤

- 情報システム
- セキュア生産
- 生産技術
- 自働化プラットフォーム
- 需給管理プロセス
- 開発プロ設計ライフ

セキュア
（安心・安全）

- 工場のセキュリティ対策
- 事業継続計画(BCP)
- サステナブルなサプライチェーン

自己紹介

澤田 利幸

NECプラットフォームズ株式会社 セキュリティ事業推進室長
CISSP PMP 情報処理安全確保支援士(第026522号)

- 出身　栃木県 宇都宮市
- 経歴　1997年～ 重要インフラシステムのソフトウエア開発担当・PLCプログラマ
  2016年～ セキュリティ会社にて MSSセールスエンジニア・PCI-DSSコンサルティング
  2019年～ NEC生産子会社にて PSIRT/FSIRT部門を統括 (現職)
- 著書　『開発-生産-保守 サプライチェーン全体で始めるための手引き』

第1章 セキュリティが大切と上司はいう
第2章 手っ取り早くやっつける
第3章 周辺の会社(パートナー)
第4章 手抜きは命取り：運用
第5章 基礎教育編(わからなくなったら読んでみて)
第6章 実践編　工場主体でつくるセキュリティ組織
第7章 工場セキュリティ対策の進め方
第8章 やってはいけない失敗の数々
第9章 セキュリティ関連情報

著者　渡辺裕之 (編著), 澤田利幸 (著)
出版者　オーム社
出版日　2023/3/31

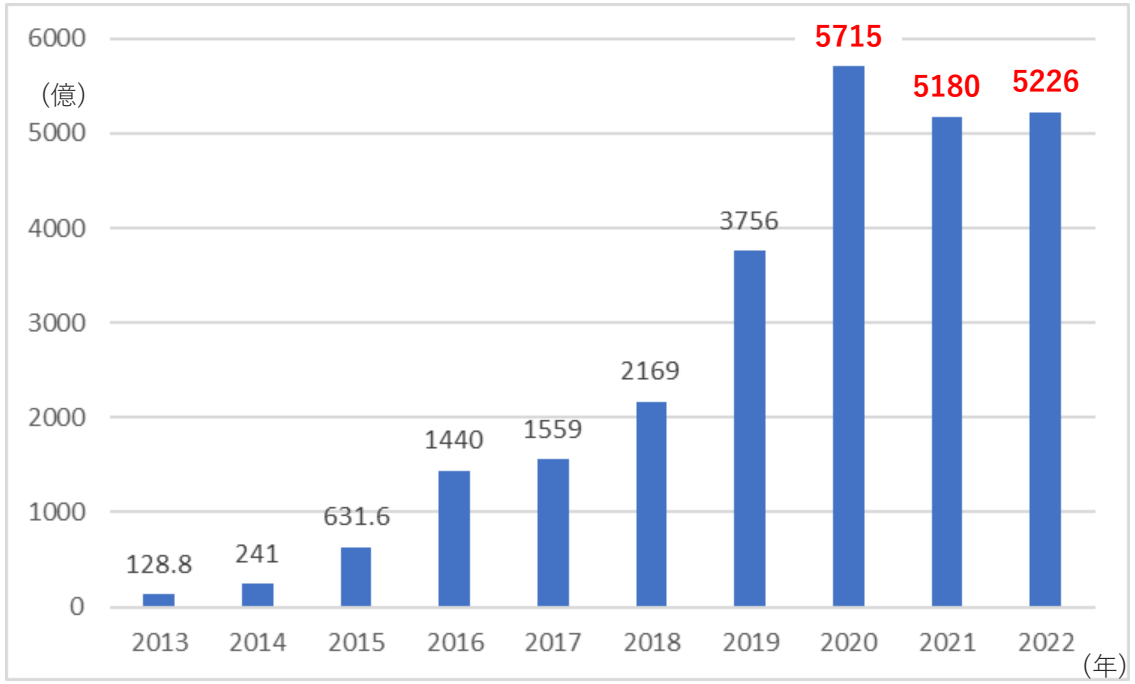
1. 背景

NECの工場に、セキュリティが必要だった理由

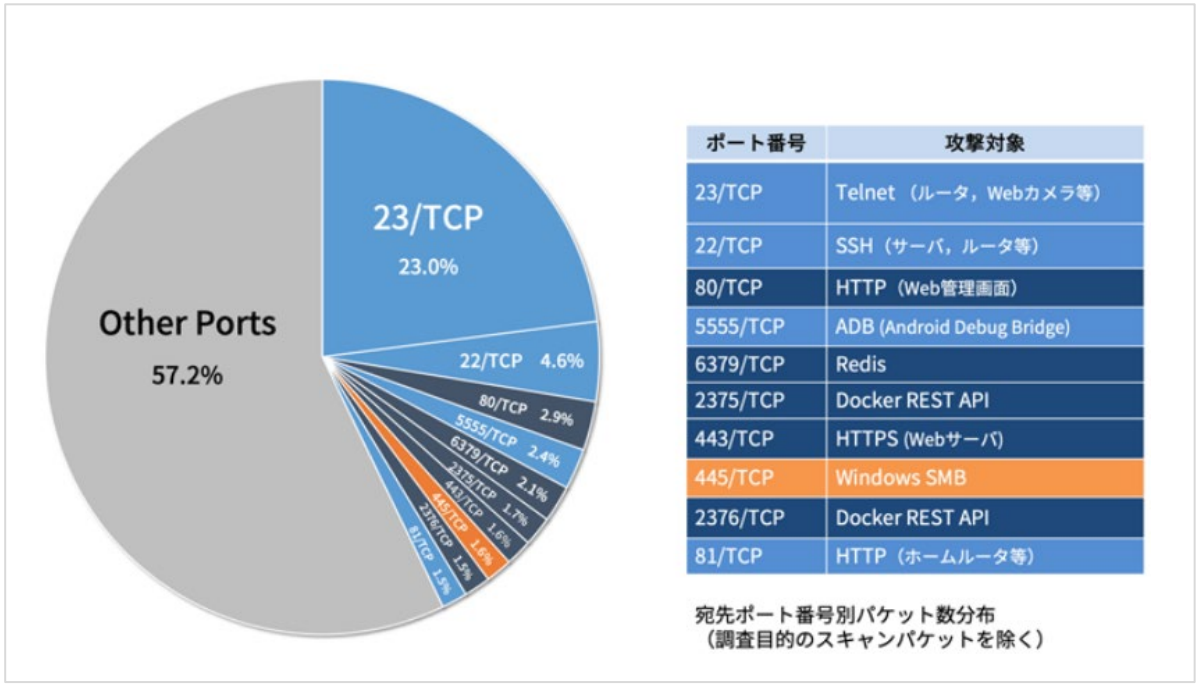
工場が狙われている

2020年以降、年間5,000億パケット以上の攻撃が観測されている
そのうち約３割はIoT機器を狙ったもの

◆ サイバー攻撃関連の通信数の推移
（NICTER分析）



◆ 宛先ポート別パケット分布
（NICTER分析）



ポート番号	攻撃対象
23/TCP	Telnet（ルータ，Webカメラ等）
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Web管理画面）
5555/TCP	ADB (Android Debug Bridge)
6379/TCP	Redis
2375/TCP	Docker REST API
443/TCP	HTTPS (Webサーバ)
445/TCP	Windows SMB
2376/TCP	Docker REST API
81/TCP	HTTP（ホームルータ等）

宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

【出展】NICTER観測レポート＜ https://www.nict.go.jp/press/2023/02/14-1.html ＞

もはやSF映画の世界ではない

重要インフラや産業システムを狙ったサイバー攻撃被害
どんどん身近に、明日は我が身

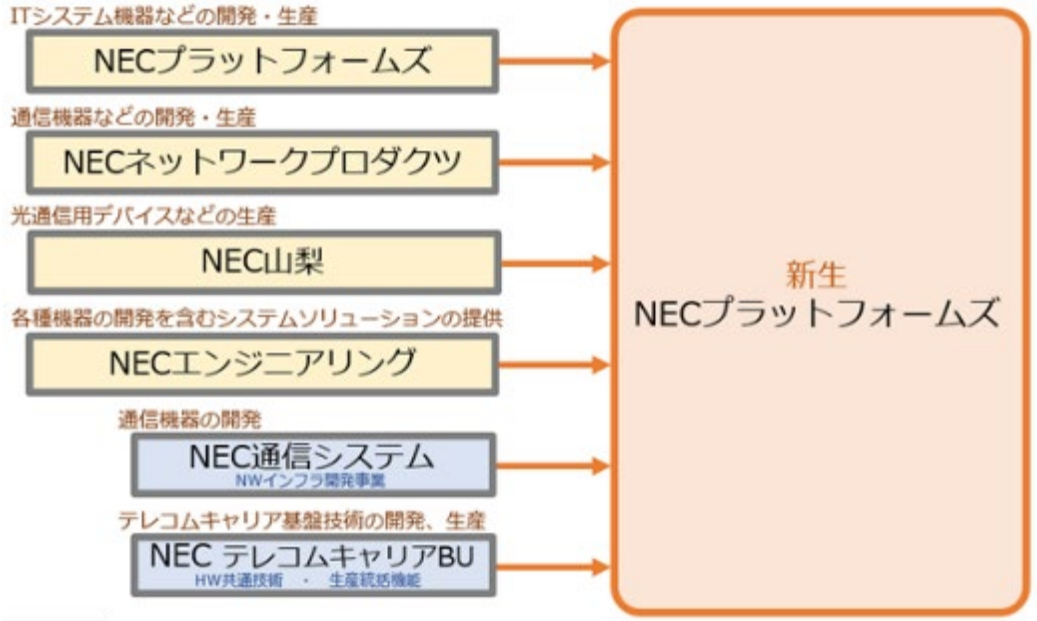
【出展】朝日新聞デジタル 2023年3月25日 記事<https://www.asahi.com/articles/ASR3T6HW2R3SULZU003.html>
【出展】PEN TEST PARTNERS <https://www.pentestpartners.com/security-blog/hacking-defcon-23s-iot-village-samsung-fridge/>
【出展】WIRED 2015.7.23 記事<https://wired.jp/2015/07/23/connected-car-bug/>
【出展】技術研究組合制御システムセキュリティセンター「制御システムセキュリティの脅威と対策の動向およびCSSCの研究概要 (2018年5月11日)」

当社の事情

グループ方針に伴うハードウェア開発/生産拠点の集約
経営課題は製品セキュリティレベルの平準化

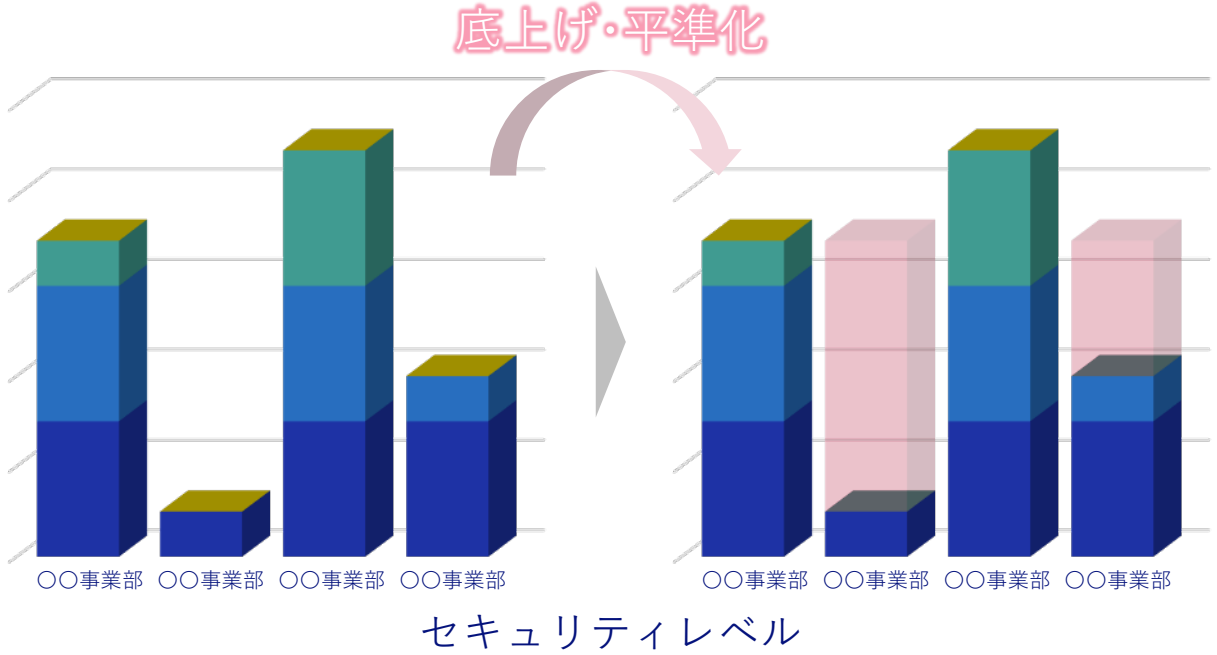
◆ 開発・生産拠点の統合

2014年にグループ4社が統合、2017年に5社が合流
ハードウェア開発・生産機能を集約



◆ セキュリティレベルのばらつき

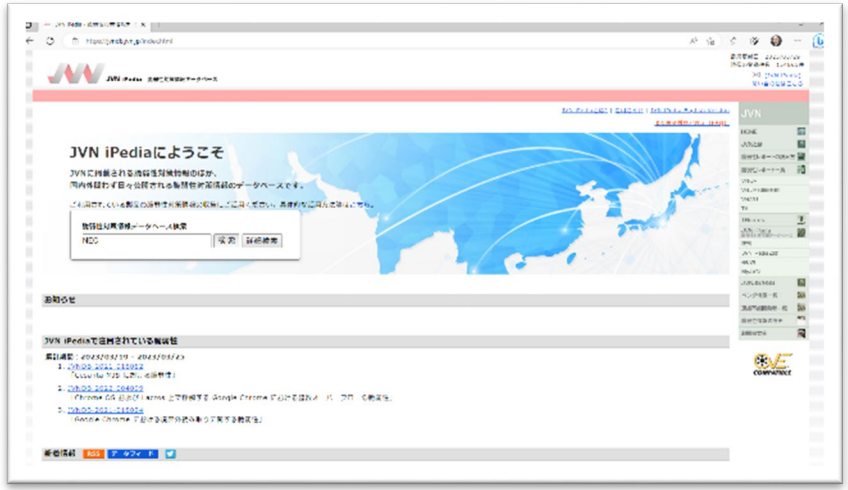
統合前は、個社の基準・体制で製品セキュリティ対策
事業/製品毎に異なるセキュリティレベルの解消が不可欠

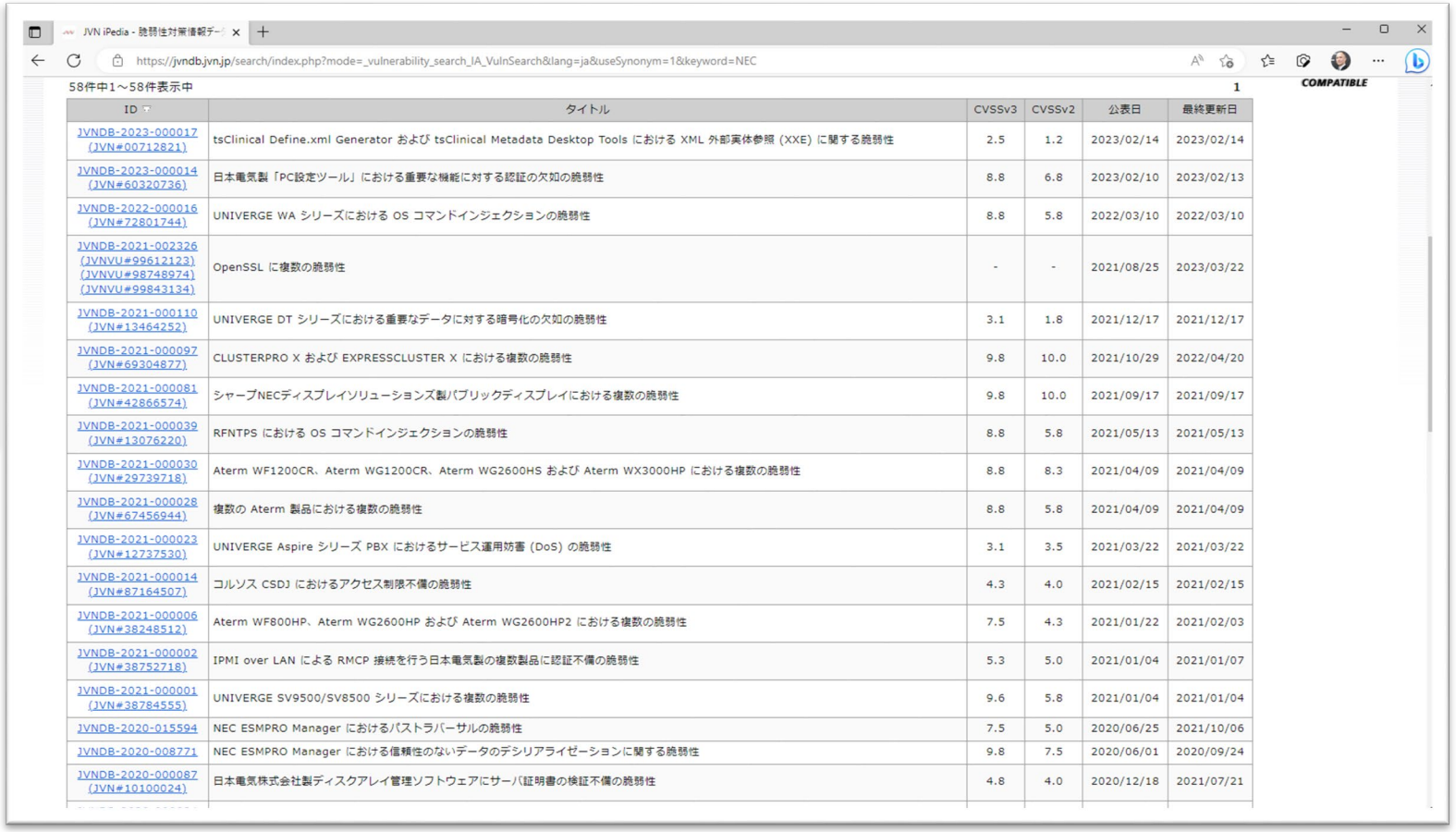


【引用】NECプラットフォームズ <https://www.necplatforms.co.jp/company/company2017.html>

当社の事情

IT製品の脆弱性に関する国内外からの指摘は増加の一途
公的機関を通じた当社製品に対する指摘が複数発生





58件中1～58件表示中

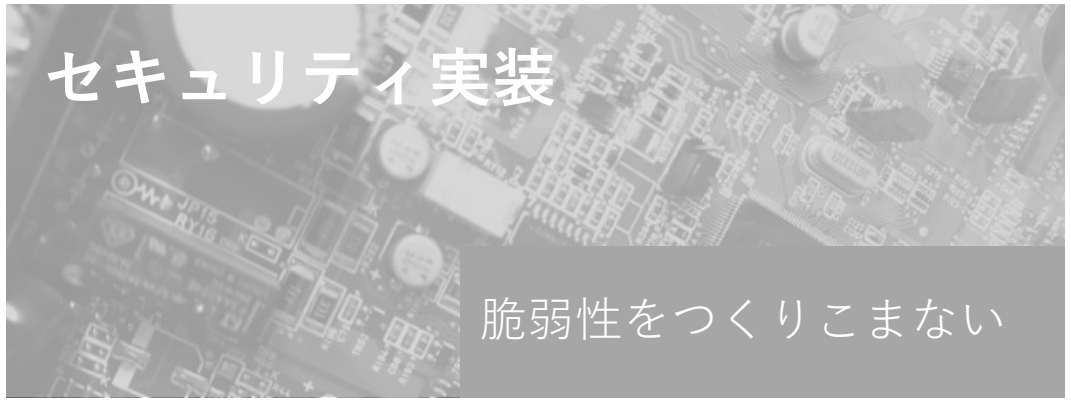
ID	タイトル	CVSSv3	CVSSv2	公表日	最終更新日
JVNDB-2023-000017 (JVN#00712821)	tsClinical Define.xml Generator および tsClinical Metadata Desktop Tools における XML 外部実体参照 (XXE) に関する脆弱性	2.5	1.2	2023/02/14	2023/02/14
JVNDB-2023-000014 (JVN#60320736)	日本電気製「PC設定ツール」における重要な機能に対する認証の欠如の脆弱性	8.8	6.8	2023/02/10	2023/02/13
JVNDB-2022-000016 (JVN#72801744)	UNIVERGE WA シリーズにおける OS コマンドインジェクションの脆弱性	8.8	5.8	2022/03/10	2022/03/10
JVNDB-2021-002326 (JVNVU#99612123) (JVNVU#98748974) (JVNVU#99843134)	OpenSSL に複数の脆弱性	-	-	2021/08/25	2023/03/22
JVNDB-2021-000110 (JVN#13464252)	UNIVERGE DT シリーズにおける重要なデータに対する暗号化の欠如の脆弱性	3.1	1.8	2021/12/17	2021/12/17
JVNDB-2021-000097 (JVN#69304877)	CLUSTERPRO X および EXPRESSCLUSTER X における複数の脆弱性	9.8	10.0	2021/10/29	2022/04/20
JVNDB-2021-000081 (JVN#42866574)	シャープNECディスプレイソリューションズ製パブリックディスプレイにおける複数の脆弱性	9.8	10.0	2021/09/17	2021/09/17
JVNDB-2021-000039 (JVN#13076220)	RFNTPS における OS コマンドインジェクションの脆弱性	8.8	5.8	2021/05/13	2021/05/13
JVNDB-2021-000030 (JVN#29739718)	Aterm WF1200CR、Aterm WG1200CR、Aterm WG2600HS および Aterm WX3000HP における複数の脆弱性	8.8	8.3	2021/04/09	2021/04/09
JVNDB-2021-000028 (JVN#67456944)	複数の Aterm 製品における複数の脆弱性	8.8	5.8	2021/04/09	2021/04/09
JVNDB-2021-000023 (JVN#12737530)	UNIVERGE Aspire シリーズ PBX におけるサービス運用妨害 (DoS) の脆弱性	3.1	3.5	2021/03/22	2021/03/22
JVNDB-2021-000014 (JVN#87164507)	コルソス CSDJ におけるアクセス制限不備の脆弱性	4.3	4.0	2021/02/15	2021/02/15
JVNDB-2021-000006 (JVN#38248512)	Aterm WF800HP、Aterm WG2600HP および Aterm WG2600HP2 における複数の脆弱性	7.5	4.3	2021/01/22	2021/02/03
JVNDB-2021-000002 (JVN#38752718)	IPMI over LAN による RMCP 接続を行う日本電気製の複数製品に認証不備の脆弱性	5.3	5.0	2021/01/04	2021/01/07
JVNDB-2021-000001 (JVN#38784555)	UNIVERGE SV9500/SV8500 シリーズにおける複数の脆弱性	9.6	5.8	2021/01/04	2021/01/04
JVNDB-2020-015594	NEC ESMPRO Manager におけるパストラバーサルの脆弱性	7.5	5.0	2020/06/25	2021/10/06
JVNDB-2020-008771	NEC ESMPRO Manager における信頼性のないデータのデシリアライゼーションに関する脆弱性	9.8	7.5	2020/06/01	2020/09/24
JVNDB-2020-000087 (JVN#10100024)	日本電気株式会社製ディスクアレイ管理ソフトウェアにサーバ証明書の検証不備の脆弱性	4.8	4.0	2020/12/18	2021/07/21

【引用】情報処理推進機構 脆弱性対策情報データベース JVN iPedia <https://jvndb.jvn.jp/index.html>

セキュリティへの取り組みを強化

「セキュア開発」と「セキュア生産」の２本柱でセキュリティ強化
工場は主要機能である調達・製造・物流を一気通貫でセキュアに

◆ **セキュア開発**（製品セキュリティ）



＋

◆ **セキュア生産**（工場セキュリティ）

2. 工場セキュリティ対策の実践とアセスメント

まずはやってみて、必要に応じ専門家を頼る

実践のステップ

step 1 組織化

- **統括部門の発足**

2019年、社内有志により
「セキュリティ統括部門」
を新たに設置

step 2 調査と計画

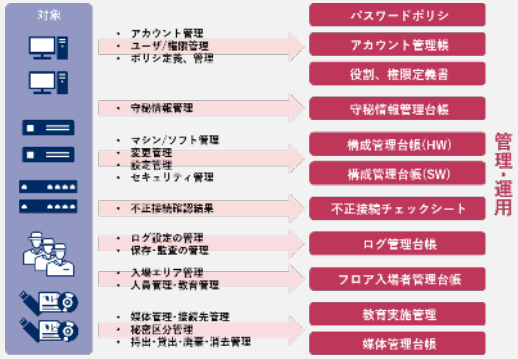
- **現状把握と基準策定**

自社工場のセキュリティ対策状況を実態把握し
工場セキュリティの「あるべき姿」を設定
現状とのギャップに基づいて対策を計画

step 3 実行

- **施策の具体化と実行**

抽出した課題に基づき
セキュリティ対策を具体化
ロードマップを設定



現状把握・方針策定

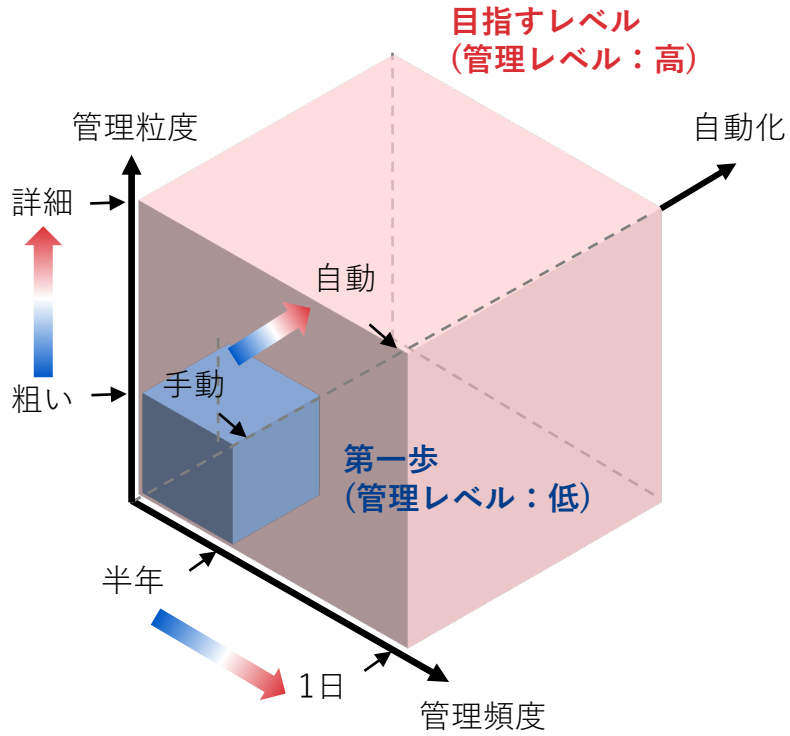
国際的なガイドラインを参考に
第一歩は 管理されていない状態 から 最低限管理された状態 へ引き上げ

◆ グローバル標準を意識したベースライン

NIST SP800-171 のセキュリティ要件（14ファミリ/110項目）			
1	アクセス制御(22)	8	メディア保護(9)
2	意識向上と(3)	9	人的セキュリティ(2)
3	監査と責任追跡性(9)	10	物理的保護(6)
4	構成管理(9)	11	リスクアセスメント(3)
5	識別と認証(11)	12	セキュリティアセスメント(4)
6	インシデント対応(3)	13	システムと通信の保護(16)
7	メンテナンス(6)	14	システムと情報の完全性(7)

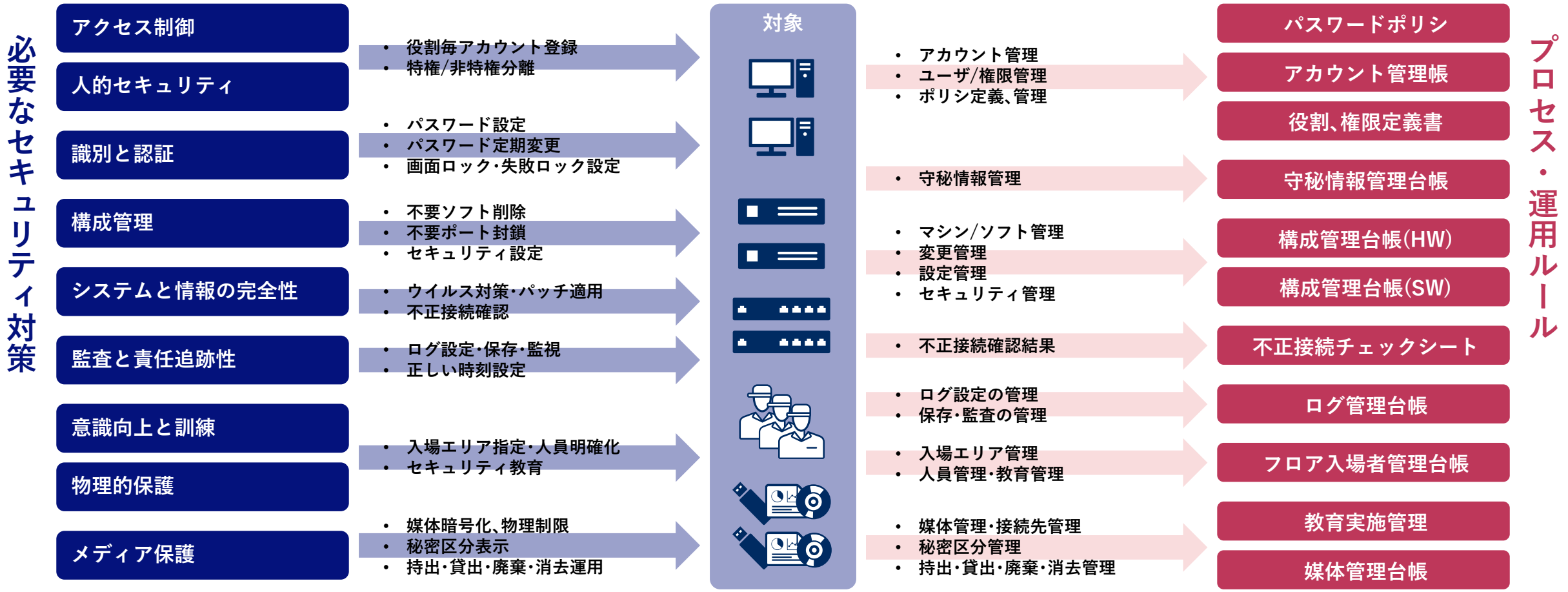
◆ 管理レベルの考え方(アクセス制御の例)

	第一歩　管理レベル：低	目指すレベル　管理レベル：高
管理粒度	**社員 or 作業者**のアクセス区分	**役割/職務**に応じた個々の権限
管理頻度	**1～6ヶ月** で更新／棚卸	**1日以内** の更新／管理
自動化	管理は**手動**	管理は**自動**で実施



組織的対策　－まずはプロセス・運用ルールをつくる－

業界標準・ガイドラインを参考に具体的なセキュリティ施策に落とし込み
説明責任(アカウンタビリティ)に重点を置き、台帳管理を強化



技術的対策　－基本的なセキュリティ対策－

工場の最初の課題はIT/OT資産の管理
セキュリティリスクの可視化+ラベリングと、統合管理を実装

◆ IT/OT資産のリスク可視化とラベリング

リスク小

青 ウイルス対策確認シール
- ウイルス対策ソフト導入済
- イントラネットから定義ファイルを自動更新

黄 ウイルス対策確認シール
- ウイルス対策ソフト導入済
- イントラネット非接続

指定の頻度もしくは起動時に定義ファイルを更新

赤 ウイルス対策確認シール
- ウイルス対策ソフト未導入
- USB型対策ソフト使用

・接続する媒体を都度スキャン
・指定の頻度もしくは起動時に本機器をスキャン

黒 ウイルス対策確認シール
- ウイルス対策ソフト未導入
- USB型対策ソフト使用不可

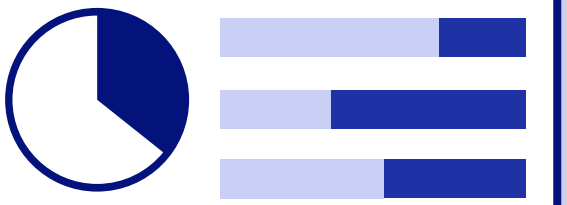
接続する媒体を都度スキャン

リスク大

◆ 管理ツール

物品管理システム

レ 対策実施チェック
レ 対策実施チェック
レ 対策実施チェック
…



ルール遵守徹底　　**徹底状況の可視化**

システムの主な目的はルール遵守徹底と可視化

導入効果

物品管理	台帳運用	リスク可視化
情報の横断共有 物品の状況把握 証跡保存可	メールによる自動通知	自動集計 組織横断集計 集計結果可視化

技術的対策　－基本的なセキュリティ対策－

工場にあるサーバやPCに、基本的なセキュリティ対策を実施

ログインの設定

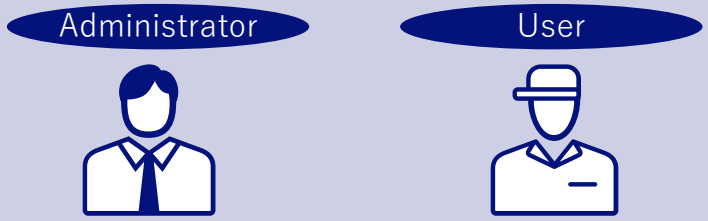
- パスワードを設定
  - 複雑性(文字数/文字種の指定)
  - 再利用を禁止
- 失敗時のロック回数・回復時間を設定
- スクリーンセーバーを設定

ログ設定

- PCのログ記録機能を有効化
  - 利用状況と保存期間からログサイズを算出
- 時刻同期機能を有効化

権限分離

- 管理者(社員)権限と一般(作業員)権限を分離



必要最小限化

- 不要なソフトウェアの削除
  USBポート・LANポートの封鎖
- ガードキーを取り付け

これまでの活動をふりかえり、改善へ

第三者の評価を取り入れ、次なるセキュリティ対策の道しるべに

セキュリティ推進者の悩み

- 気付いていないリスクは無いか？
- 現在の対策内容は妥当なのか？
- 現在のセキュリティ対策のレベルは？

第三者による客観的な評価を受けて疑問をクリアに！

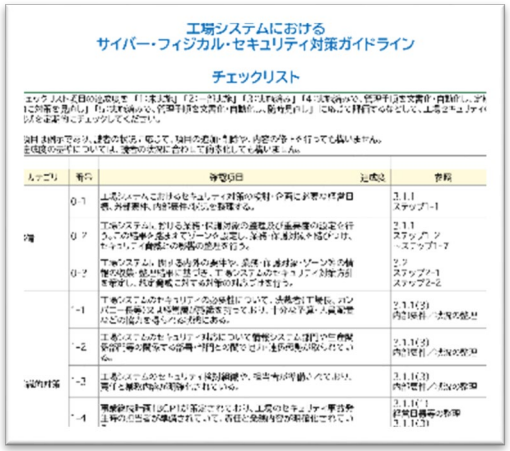
- 第三者観点での新たなリスクの把握
- 対策の妥当性評価と改善アドバイス
- 定量的な評価

これまでの活動をふりかえり、改善へ

「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」に基づく第三者評価を、継続的改善に活用

◆ ガイドラインの概要

- 国内製造業(工場)のセキュリティ対策標準
- 2022年11月16日に、経済産業省が発行
- FA/OTシステムに特有の要件にフォーカス
- 必要最小限に絞った基本要件を定義



◆ 診断の結果

- 全体的に高評価(上位10%以上)
- 「運用・技術・SCM」対策に改善の余地

体制・ルール・BCPについて高評価

システム化・SC管理に改善の余地

項目	当社主要工場	他社平均 (参考)
総合	B	C
組織	A	C
運用	B	C
技術	C	C
SCM	C	D

3. サイバー攻撃対応BCPと訓練

「防御の高度化」から「事故対応の高度化」へのシフト

BCPの策定

BCP

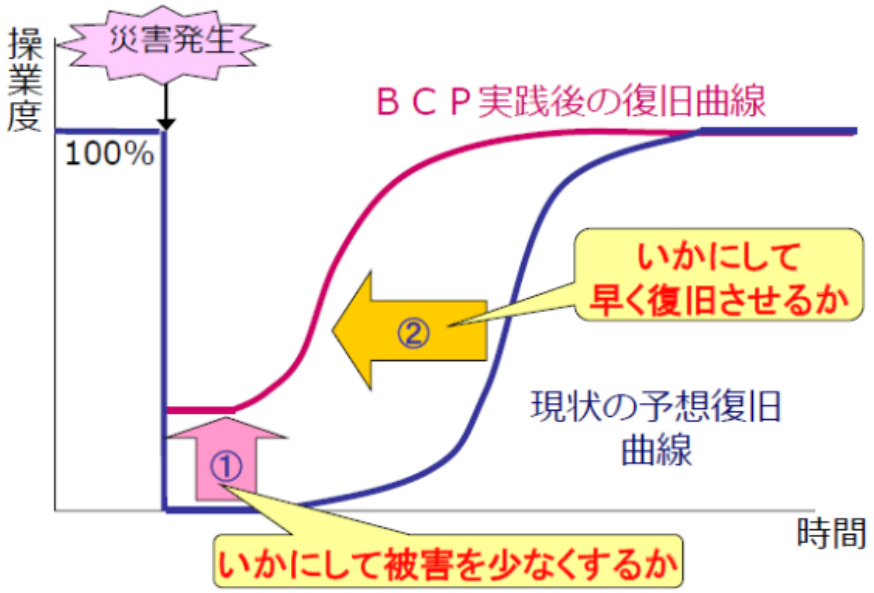
Business **C**ontinuity **P**lan

BCPの策定　－「侵入される」ことを前提に復旧計画を準備－

自然災害とサイバー攻撃の違いを切り口に
サイバー攻撃対応BCPの必要性を関係者に説明

◆ BCPの考え方

本質は「起こることを前提に事業を継続するための計画を立てておく」こと



◆ 自然災害とサイバー攻撃の違い

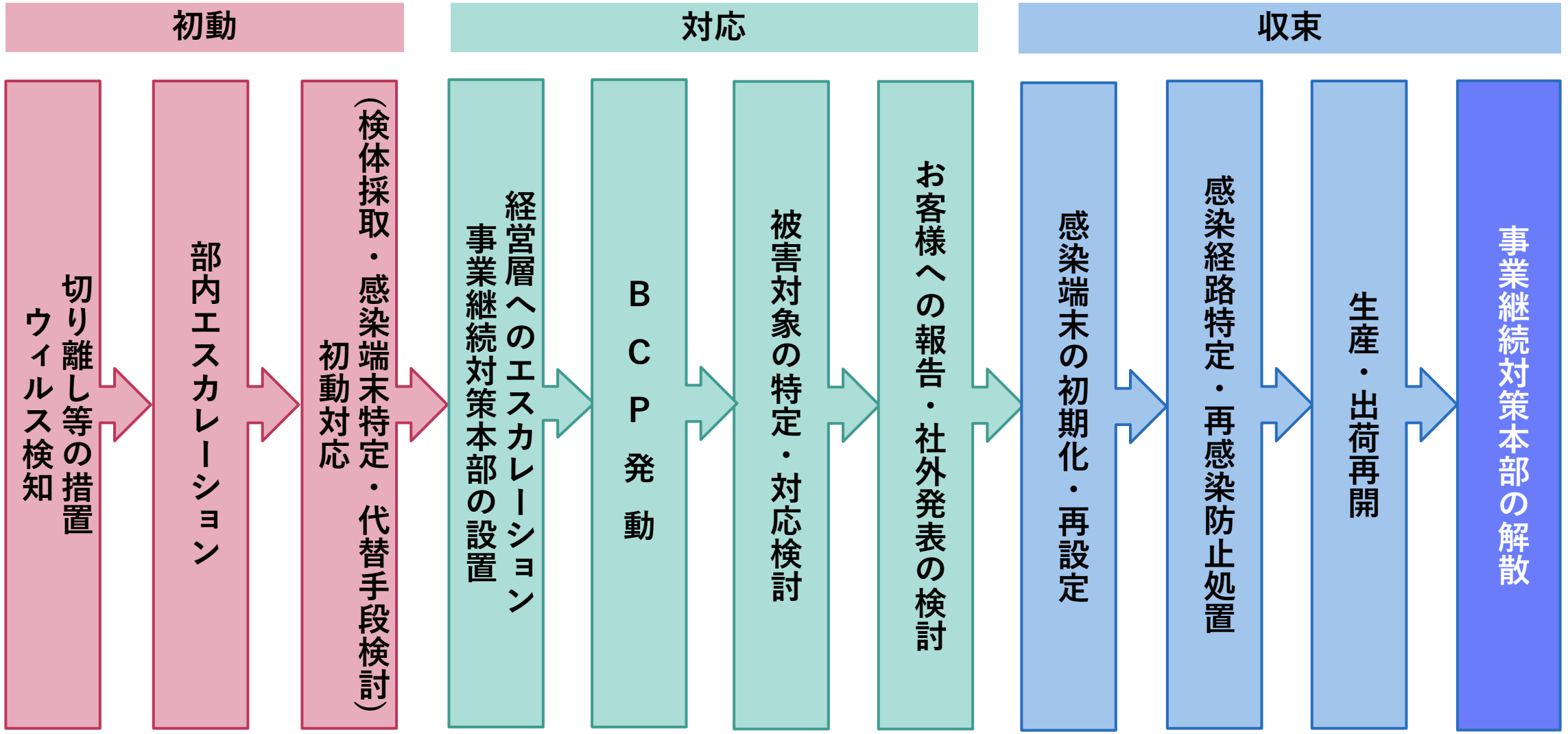
自然災害	サイバー攻撃
● **発生と検知** 発生が明確	● **発生と検知** 発生が不明確 （発生と発見のタイムラグ）
● **対応と復旧** 機器の修理・交換	● **対応と復旧** 原因分析の結果に応じた対応
● **減災対策** 水害対策 耐震対策	● **減災対策** マルウェア対策 NWセキュリティ対策

BCPの策定　－「侵入される」ことを前提に復旧計画を準備－

自然災害BCPとの親和性を考慮しながら
サイバー攻撃のリスクを考慮した事業継続計画を策定

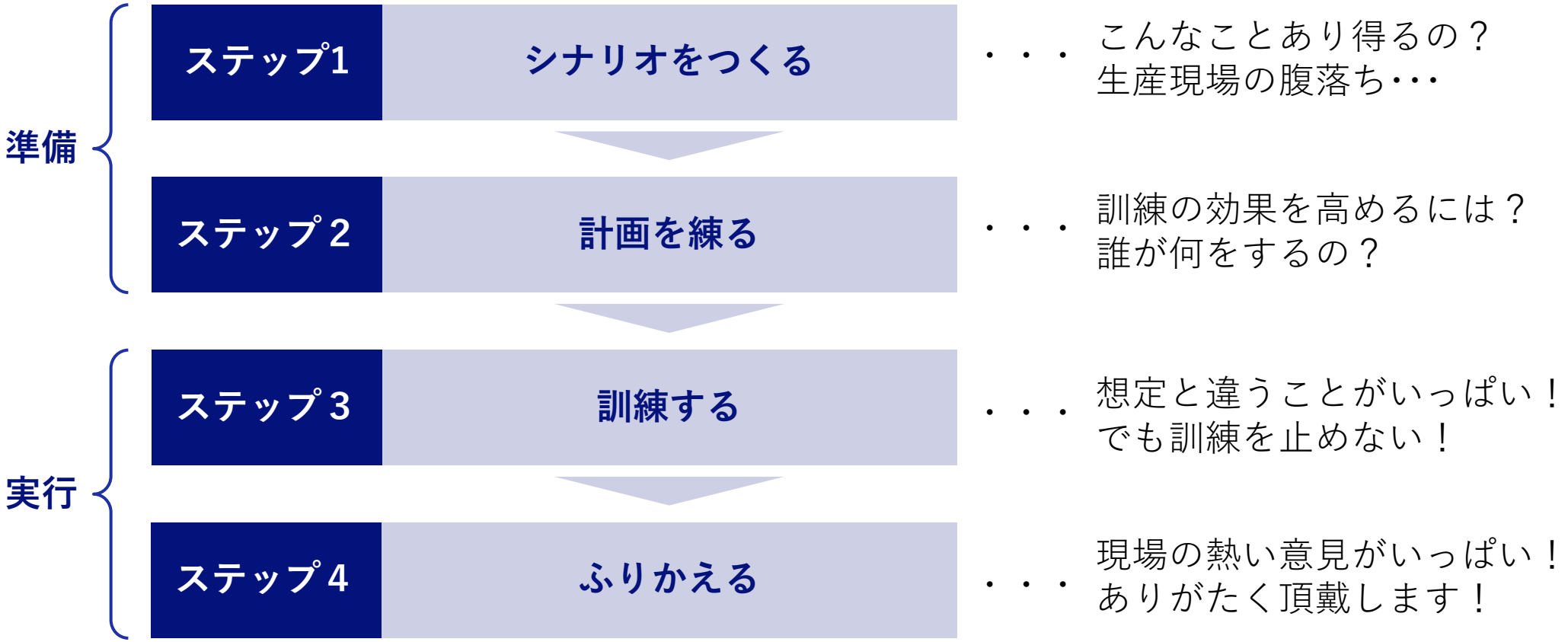
◆ 策定プロセス

BCPの策定　－対応フローの文書化－



訓練　－備えあれば憂いなし－

「訓練だけで対応はできない。されど訓練なくして対応はできない。」
形骸化の防止と、実効性の担保



訓練　－ステップ１：シナリオをつくる－

関係者と一緒に各工場にカスタマイズした訓練シナリオを作成
現場の運用に合わせた現実味のある内容に

内閣府「「企業の事業継続訓練」の考え方」を参考にシナリオを作成

セキュリティ部門

セキュリティの知見
- 工場で想定される攻撃/被害
- 各役割に期待する行動

生産部門

工場の知見
- 生産機器や現状の対策状況
- 復旧対応時の役割分担
- 工場の生産製品

まずは･･･　セキュリティ部門でシナリオのベースを作成
つぎに･･･　各工場の実態を取り込みカスタマイズ

POINT

現実的なストーリー
- 起こり得る攻撃/被害を想定
- 各工場における運用実態を反映
- 実際の役割･役職で自分事化

役割ごとに期待する行動を明示
- BCPで示しきれない役割の詳細な行動を示す
- 参加者の理解度への配慮が必要

訓練　－ステップ１：シナリオをつくる－

BCPのフローにおける各フェーズで行動するために必要な情報を提示

「状況」の情報

BCPの内容

	実施項目	実施内容	担当	プレイヤ(バイネーム)	実施場所	プレイヤに期待する行動
1	状況付与 【〇〇月××日(水)14:00】 ▽▽▽ラインで使っている検査用PCが、通常表示しない画面になり、検査が途中で止まった。 画面の表示は身代金要求画面で、ランサムウェアに感染したと思われる。感染経路は、現状では不明。					
2	検知	・異常を検知した時点でラインを停止 ・該当PCのネットワークを切断 ・電源は切らない ＜異常現象＞ ・ウイルス対策プログラムまたはIDSの警告 ・ファイルが暗号化されている ・明らかにウイルス感染が疑われる表示	製造部 生産技術部	発見者：〇〇 ラインリーダ：×× 生産技術部　：□□	▽▽▽ ライン	・発見者　　：異常を確認し、ラインを停止 ラインリーダへ報告 ・ラインリーダ：ウイルス感染を疑い、該当PCのネットワークを切断 生産技術部を招集し、状況を共有 訓練では質問への回答をもって行動したとみなす 【質問】 Q:発見者はどの様な行動をとりますか？ A:ラインを停止し、ラインリーダ××へ連絡します。 Q:ラインリーダはどの様な行動をとりますか？ A:該当PCのLANケーブルを抜きます。 生産技術部□□と状況を共有します。
3	エスカレーション	…	…	…	…	
	…	…	…	…	…	

BCPに対する行動の詳細
（プレイヤ、実施場所、期待する行動）

訓練　－ステップ２：計画を練る－

訓練は「段取りで８割」「実施で２割」
生産業務への影響を最優先に配慮しつつ、関係者と連携して実施計画を作成

事前準備

- **日程**
  生産影響が出ないよう
  工場側の都合を優先
- **参加者**
  工場幹部(工場長、部門長)
  ライン作業者
- **シナリオ確認**
  訓練するライン選定
  シナリオの確認

実施計画

１日目：前日準備

① 下見
（ラインや事務所・機器の運用など）

② シナリオの妥当性確認
（実施場所/被害など想定条件の評価）

③ 段取りの最終整合
（進行・役割の確認）

２日目：訓練当日

① オープニング

② 訓練

③ 結果の整理
（参加者と実施結果を確認）

④ ふりかえり
（参加者と意見交換）

POINT

- 現場で方針判断する幹部の参加を必須化
- 副次効果で他の参加者の参加意欲も高まる
- 日程は３ヶ月前に確保

訓練　－ステップ３：訓練する－

現実に近い状況で、各フェーズで行うべき行動ができるかを確認
肝は「検知」→「エスカレーション」→「初動対応」の迅速性

◆ 対応の流れ

①検知

②部内エスカレーション

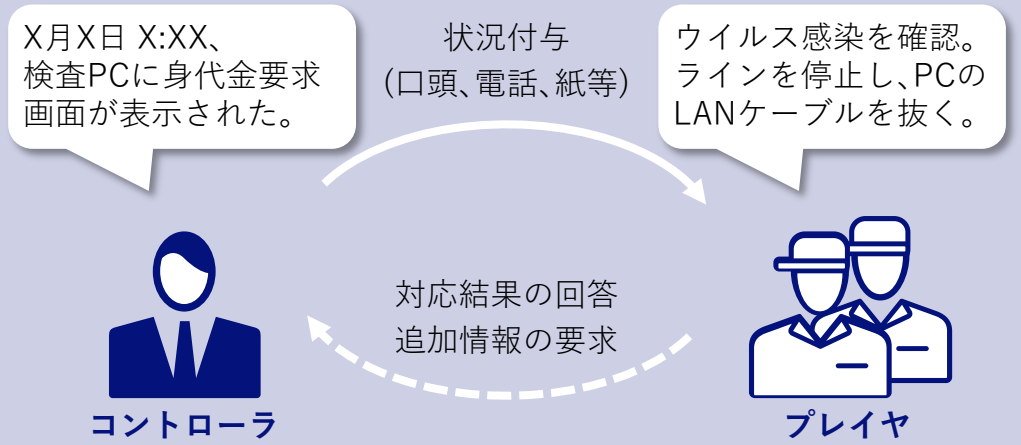
③初動対応の協議

④初動対応
（検体採取）

⋮

◆ 訓練の手法

ロールプレイング方式



① コントローラが全体進行、プレイヤへ状況付与もしくは質問
② プレイヤは、状況を基に判断し、BCPに従って行動
③ コントローラは、プレイヤの行動を確認

POINT

失敗を恐れない
- 発見した不備・過失・気付きが多いほど、訓練の価値は高い

訓練を止めない
- 想定外の事態が発生しても臨機応変に対応

訓練　－ステップ４：ふりかえる－

終了後すぐに（記憶の新しいうちに）意見交換
訓練の都度、現場の意識が向上し改善につながる

2021年度訓練から得られた課題	フィードバック
現場からのコメント • 生産･出荷再開判断のプロセスの記載がない • 5M/1E管理の記録に合わせたい **発見した気づき** • バックアップからの復旧はしたことない	**BCP改版** • 「生産・出荷再開判断」をプロセスとして追加 • PC交換などの処置内容を記録する事を追記 **次年度訓練の改善** • バックアップからの復旧訓練を追加

2022年度訓練から得られた課題	フィードバック
現場からのコメント • 生産･出荷再開判断は別プロセスにすべき • 現場のエスカレーションルールと合わせたい • シナリオ配布の訓練ではなく、プレイヤはBCPだけを参照する実践的な訓練にすべき	**BCP改版** • 「生産再開」と「出荷再開」の判断プロセスを分割 • 既存のエスカレーションルールと整合 **次年度訓練の改善** • プレイヤにシナリオを配布しない訓練に変更

訓練の風景

◆ 目的

- インシデント対応の考え方と手順を習得
- インシデント発生時に必要な心構えの理解深耕
- サイバー攻撃対応BCPの有効性を確認

◆ ポイント

- セキュリティインシデント発生のシナリオに沿ったロールプレイング
- あらかじめ用意した事業継続計画に基づいて、適切なエスカレーション・対策本部設置・調査が実施できるかを検証

管理者向けの訓練

◆ 目的

- 緊急対策本部長の役割・対応手順を習得
- インシデント発生時、管理者に必要な心構えの理解

◆ ポイント

- 対策本部長になり得る管理者同士によるグループワーク研修で、実例に則したインシデントへの対応を協議
- 初動対応から業務復旧までの行動をシミュレーションし、その結果に対する講師からのフィードバックで理解深耕

研修の構成

座学講習

インシデント発生時の対応をディスカッション

4. おわりに

これまでの成果、これからの取り組み

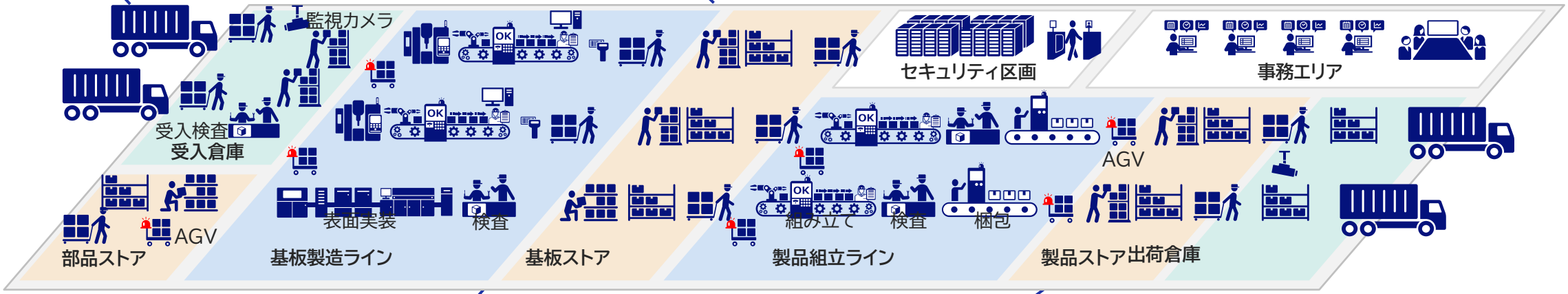
これまでの成果

セキュア調達

- **サプライチェーン対策**
  お取引先さまへのセキュリティ対策要請
- **調達品の受入検査**
  受入検査の模倣品・バックドア・マルウェアの流入対策

セキュア製造

- **IT資産管理**
  独自システムで社内の情報資産はIT/IoT機器を一元管理
- **ネットワークセキュリティ**
  生産ネットワークの細分化(セグメンテーション)と統合脅威管理(UTM)
- **物理的セキュリティ**
  ICカード＋生体情報(顔認証)による、入退場管理



社会貢献・セキュリティ啓発

- **工場セキュリティガイドライン策定の協力**
  公的機関への事例共有やアンケート協力
- **社外への事例発信**
  イベント・セミナーを通じた事例発信
- **書籍出版**
  当社の取り組みを書籍化

セキュリティ運用

- **セキュリティルールの整備**
  米国のガイドラインを参考に独自のルールを定義
- **セキュリティアセスメントの受診**
  専門家による第三者評価
- **サイバー攻撃対応BCPと訓練**
  サイバー攻撃に対応した事業継続計画の整備と定期訓練

セキュア物流

- **倉庫のセキュリティ対策**
  米国のガイドラインを参考に独自のルールを定義
- **搬入・搬出施設の映像監視**
  個人を識別可能なレベルの監視映像
- **トレーサビリティ強化への取り組み**
  真正性確保とトレーサビリティ強化を検討

これからの取り組み

「運用・技術・SCM」の改善を中心に今後の対策を検討

◆ アセスメントから導き出された課題

項目	当社主要工場	他社平均（参考）
総合	B	C
組織	A	C
運用	B	C
技術	C	C
SCM	C	D

体制・ルール・BCP について高評価

システム化・SC管理 に改善の余地

診断結果を参考とした対策の検討
運用・技術・SC管理に係わる対策を強化

全生産拠点のリスクアセスメントを実施
生産拠点のリスクを洗い出し計画的に対策

◆ 人手不足への対策

FSIRT（Factory Security Incident Response Team）
工場で生じるセキュリティ課題の対応を専門におこなう体制
体制・ルール

FSOC（Factory Security Operation Center）
工場のNWや機器を監視し、攻撃の検知や対応を行う仕組み
システム化

セキュリティ担当は孤独･･･

組織･企業･業界の枠を超えた連携で
ともに“セキュリティ”を底上げしましょう！

#つくるでささえる

Together with “MONOZUKURI”,
creating a sustainable society

\Orchestrating a brighter world

NEC

NECプラットフォームズ

IPA コラボレーション・プラットフォーム(第27回) 向け

第2部　パネルディスカッション「サイバー・フィジカル時代の工場セキュリティ対策にどのように取り組めば良いのか？」

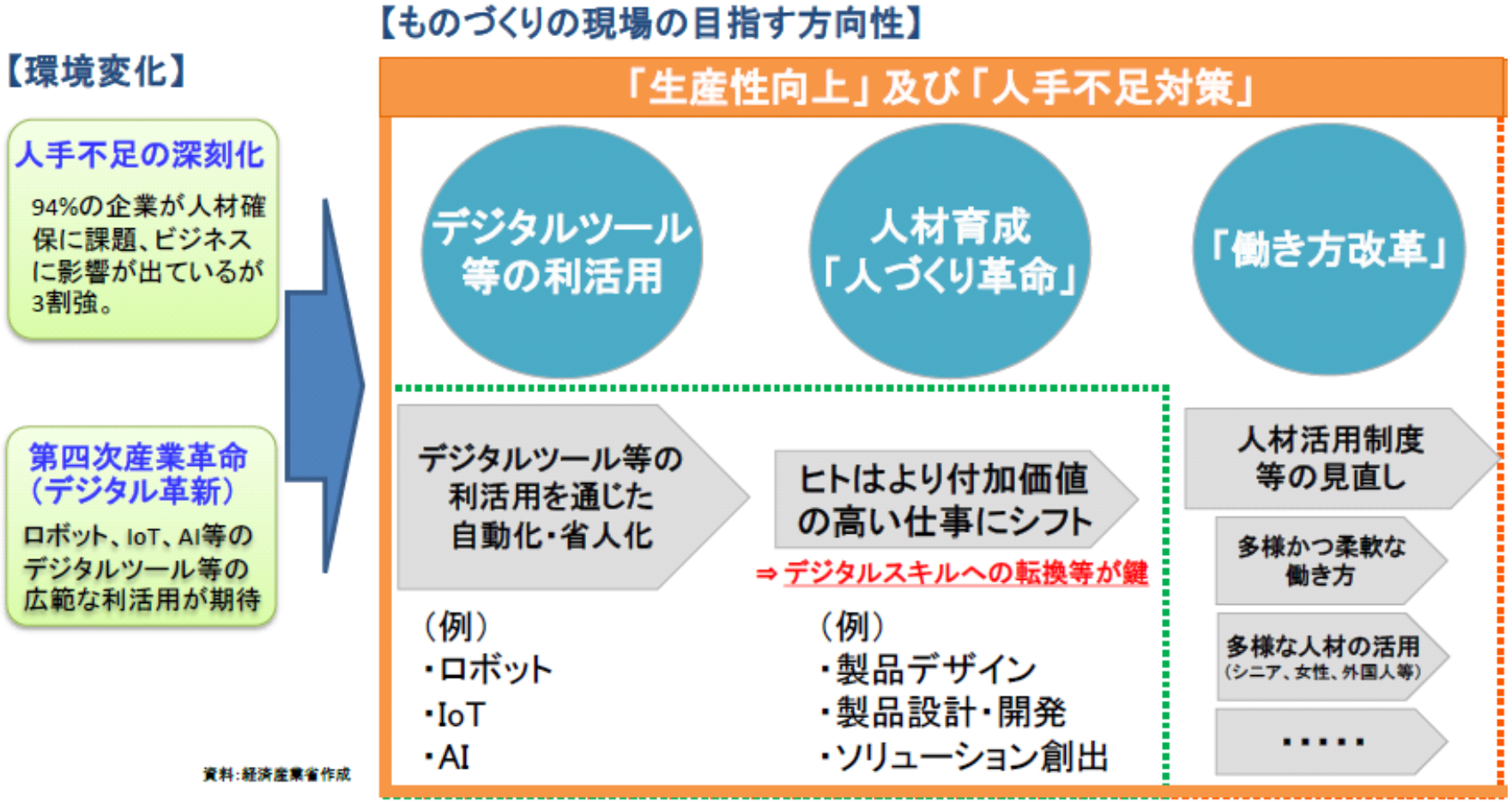
2024年 2月 26日

日本電気株式会社
セキュリティ事業統括部　IoT/OTセキュリティグループ　ディレクタ
桑田 雅彦

製造業／工場は今、
どのような環境に置かれているのでしょうか？

製造業／工場を取り巻く環境動向（1／3）

工場は、**生産性向上**や**人手不足／働き方改革**の対策に迫られている状況



Covid-19対策／New Normal 対応の必要性

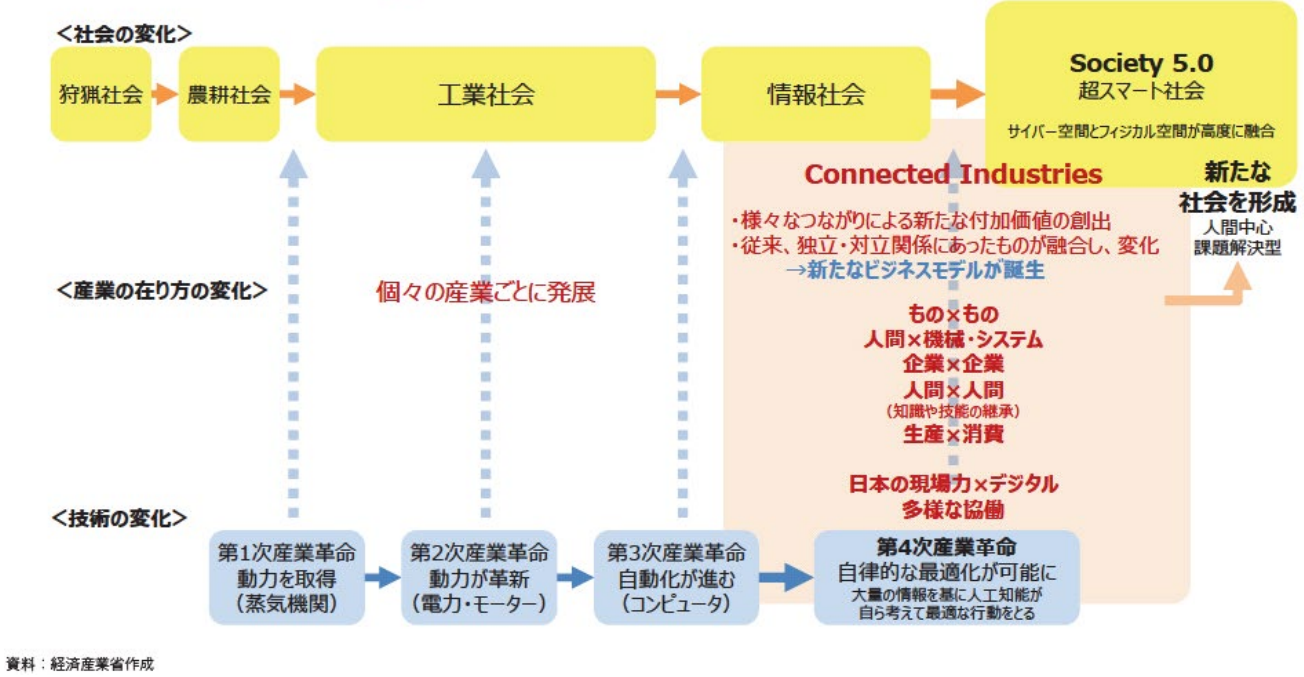
- **BCP／テレワーク（生産現場も公平に）**
- **変化への迅速な適応**
- **柔軟なサプライチェイン、業務改革**

出典：経済産業省「2018年版ものづくり白書」を基にNEC作成

製造業／工場を取り巻く環境動向（2／3）

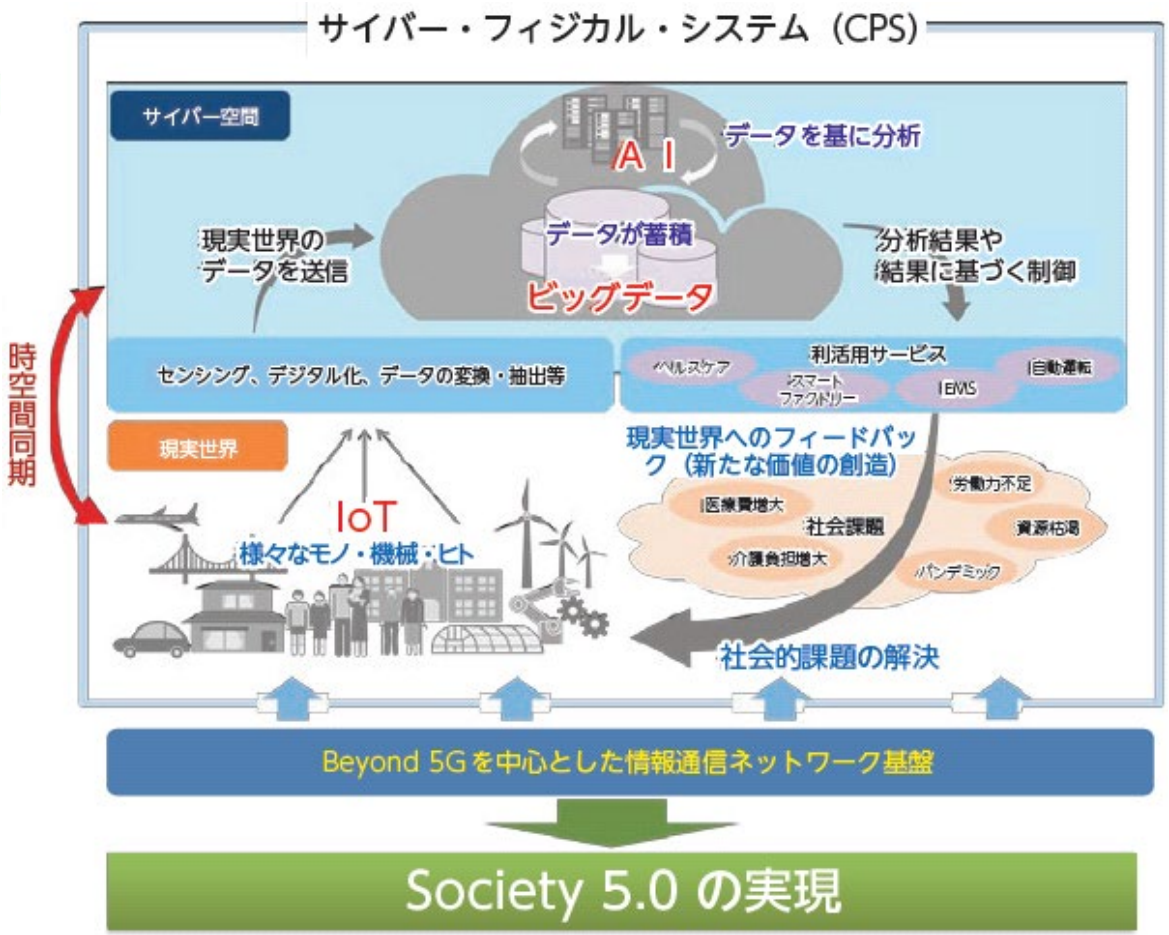
グローバルで**第4次産業革命**の時代となり、**サイバー・フィジカル融合**の推進が必要

図 131-2　第四次産業革命を Society 5.0 につなげる Connected Industries



資料：経済産業省作成

出典：経済産業省「2018年版ものづくり白書」

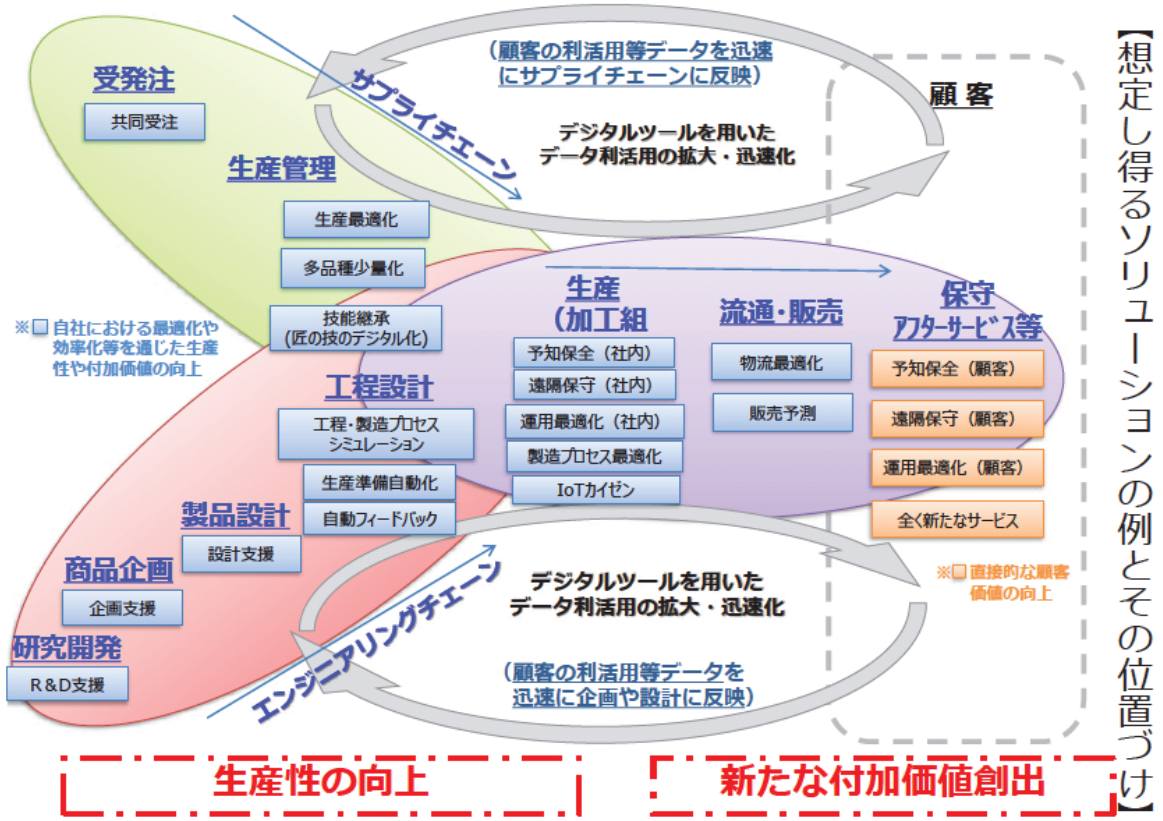


出典：総務省「Beyond 5G 推進戦略」（2020）

製造業／工場を取り巻く環境動向（3／3）

サイバー・フィジカル融合の推進は、一つの工場内に閉じることではなく、
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まで対象

図 131-1　想定し得るソリューションの例とその位置づけ



資料：経済産業省作成

出典：経済産業省「2020年版ものづくり白書」を基にNEC作成

- **取引先からの連携要求**
- **変化への迅速な適応、柔軟なチェーン**
- **SDGs／ESG投資／グリーン(カーボンニュートラル)を目的とした推進**

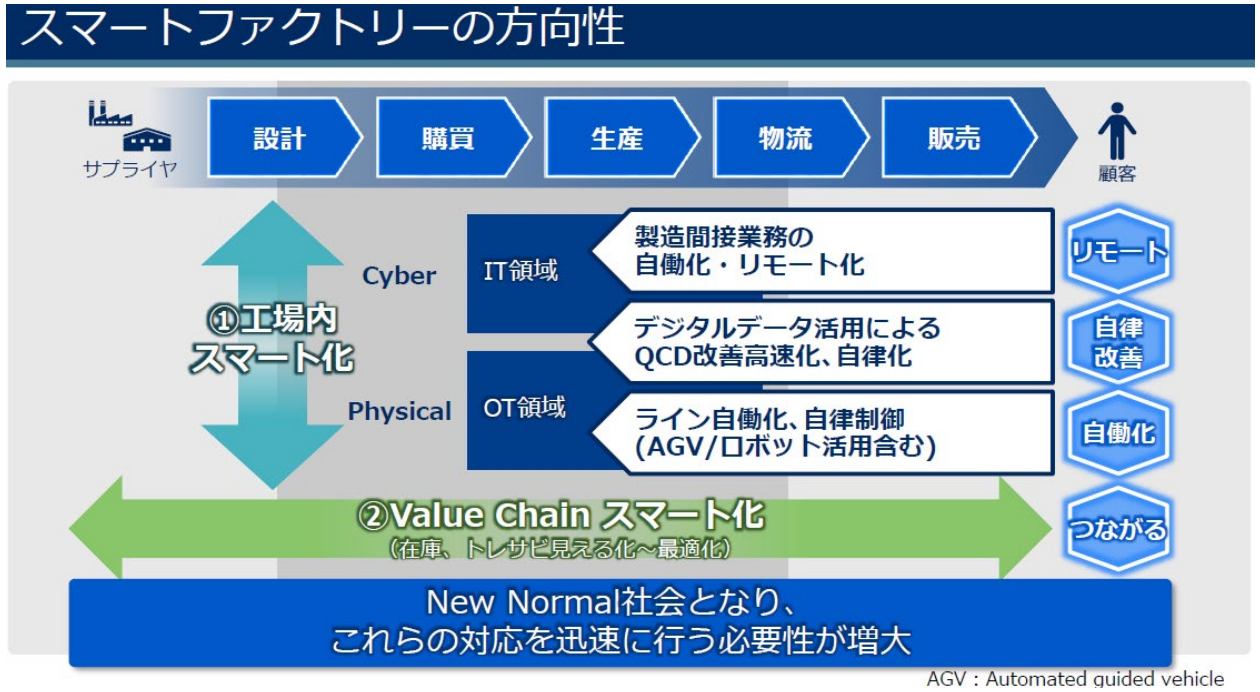
工場FA／OTシステムのIT連携（CPS化）・DXの進展

工場FA／OTシステムのサイバー・フィジカル融合、スマート化、DXが進展開始

※ FA：Factory Automation
※ OT：Operation Technology

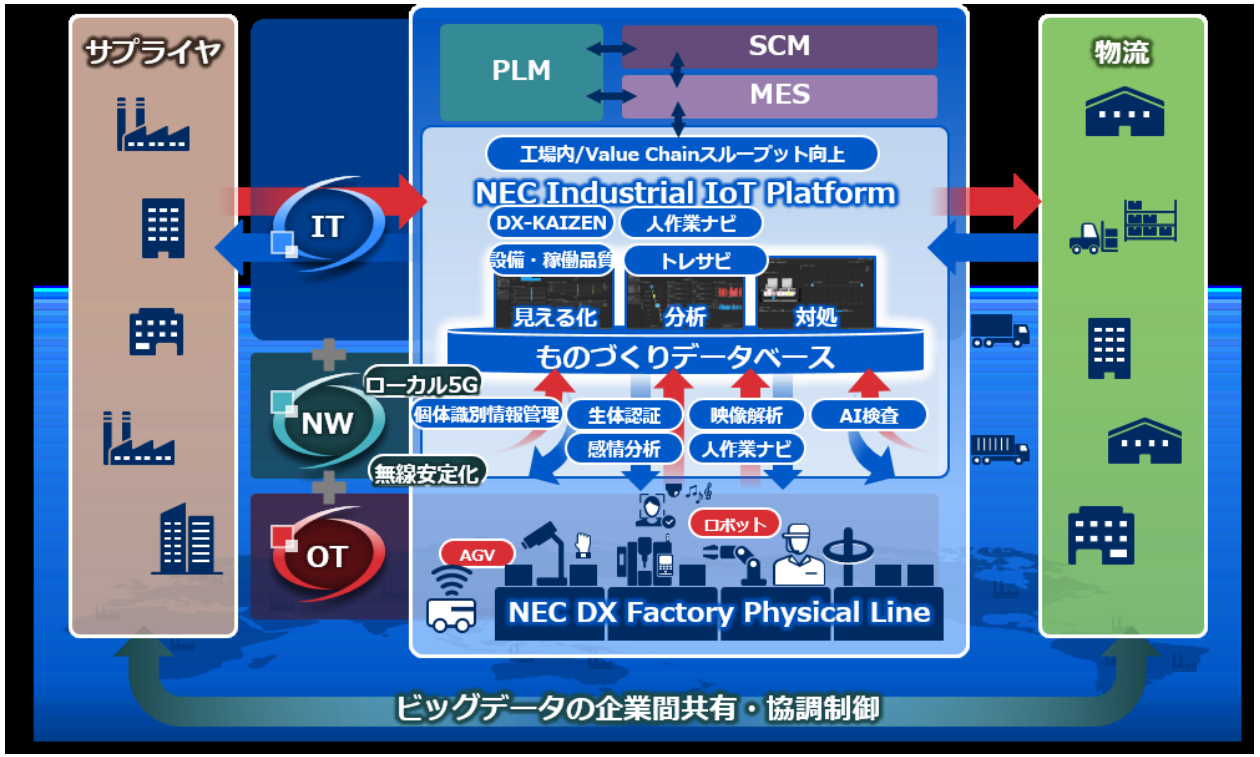
※ DX：Digital Transformation

スマートファクトリーの方向性



AGV：Automated guided vehicle

NEC DX Factory 全体イメージ



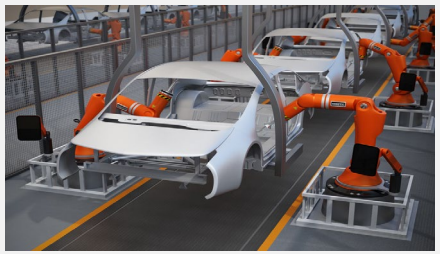
NEC DX Factory Webサイト：https://jpn.nec.com/manufacture/monozukuri/iot/nec_dxf.html

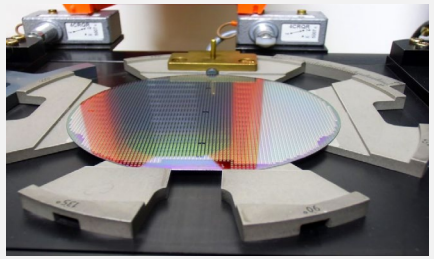
サイバー・フィジカル融合／スマート化／DXが進展しつつある工場FA／OTシステムは、安全・安心に利用できるのでしょうか？

工場FA／OTシステムにかかわるセキュリティ事故／リスクが増大

工場で、生産停止／設備被害に繋がる事故、制御システムを狙った攻撃・被害が増大

	自動車メーカ	半導体メーカ	製鉄所
被害	複数工場の生産停止 （被害総額 約1,400万ドル）	複数工場の生産停止 （四半期売上高の約3%）	生産設備の損傷
原因	Zotobウイルス	WannaCryウイルス亜種	トロイの木馬
感染経路	持込PC or NW	ウイルスチェック未実施 端末のNW接続	電子メールの 添付ファイル





工場FA／OTシステムにかかわるセキュリティ事故の事例

工場FA／OTのセキュリティ事故／リスクが増大している理由

現在、世界的に、工場が攻撃者から狙われていることに加え、サイバー・フィジカル融合（CPS）／IoT化の進展により、ますます狙われ易くなる傾向

1. 製造業／工場は狙われている　サイバー

- 世界で起こるセキュリティ事故の23%（最多）は製造業が対象※1
- 工場は対策不足で攻撃し易く、攻撃の被害による影響度が大きい（工場の操業停止、製品品質の問題発生等）

2. CPS／IoT化の進展により高まるリスク　サイバー

- 最新のサイバー攻撃の過半数はIoT機器が対象※2
- SCADA Modbus OTデバイスの偵察が22倍に増加※3
- 受変電や空調などのファシリティも攻撃対象に

3.工場内従業員による不正も発生　内部不正

- 世界のセキュリティ事故発生要因の2位は現役従業員の犯行※4
- 品質・検査データ改ざんは、国内製造業全体の課題に発展

※1,3：IBM Security X-Force「脅威インテリジェンス・インデックス2022」より引用
※2：国立研究開発法人情報通信研究機構公開資料（NICT NICTER観測レポート2021）より引用
※4：ICS-CERT Report 2016（The Industrial Control Systems Cyber Emergency Response Team ）より引用

サプライチェーンリスクも増大

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	標的型攻撃による機密情報の窃取
4	内部不正による情報漏えい
5	テレワーク等の ニューノーマルな働き方を狙った攻撃
6	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
7	ビジネスメール詐欺による金銭被害
8	脆弱性対策情報の公開に伴う悪用増加
9	不注意による情報漏えい等の被害
10	犯罪のビジネス化 （アンダーグラウンドサービス）

出典：IPA「情報セキュリティ10大脅威 2023」

複雑なサプライチェーンによる脅威の例①：
ランサムウェア"WannaCry"の猛威

参考：産業サイバーセキュリティ研究会第1回にて配布

- 平成29年５月、世界の少なくとも約150か国において、Windowsの脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。
- **感染した欧州企業から、サプライチェーン経由で国内企業も感染。**

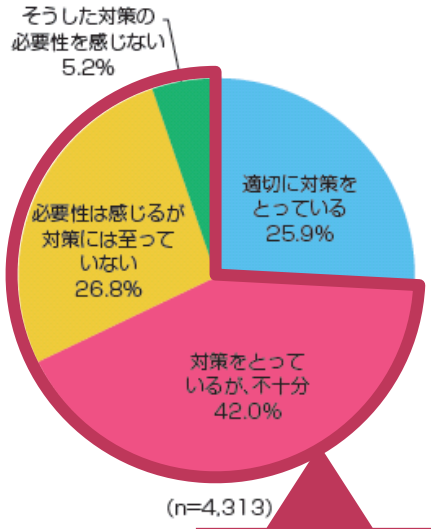
出典：経済産業省　産業サイバーセキュリティ研究会資料

工場FA／OTシステムのセキュリティ対策は、十分に実施できているのでしょうか？

製造業／工場におけるセキュリティ対策の状況

工場のセキュリティ対策は不足しており、課題を抱え進んでいない状況

図 135-4　セキュリティ対策の状況



74%が不足

資料：経済産業省調べ（2017年12月）

図 135-18　ものづくり企業におけるサイバーセキュリティ対策の方向性

課題点①：中小企業を中心にサイバーセキュリティの必要性を感じていない　危機意識喚起
（例）不安を感じないと回答した中小企業のうち６割「自社がターゲットになるとは思えない」
⇒対策の方向性：リスク認識の向上
具体策：（１）サイバーセキュリティリスク評価指標・ツール　（２）セミナー開催等

必要性は理解したが・・

課題点②：何をしたらいいかがわからない　対策方針指南
（例）ｻｲﾊﾞｰｾｷｭﾘﾃｨ上対策の障害:「何をしたらいいかがわからない」が中小企業で14%
⇒対策：対策として必要な考え方・手段を周知
具体策：（３）サイバーセキュリティ経営ガイドライン・中小企業の情報セキュリティ対策ガイドライン（IPA）
（４）サイバー・フィジカル・セキュリティ対策フレームワーク、（５）ベストプラクティス集の作成
（６）自己宣言制度（Security Action）（７）情報セキュリティ安心相談窓口等の設置（IPA等）

対策法が把握できたが・・

課題点③：担い手となる人材がいない　“人”
（例）対策の障害:「人材がいない」が中小企業で43%
⇒対策：★自社内で対策を講じる人材育成
☆専門業者への委託

課題点④：コストがかかり投資が困難　“金”
（例）対策の障害:「投資が困難」が大企業で52%
⇒対策：ソフトウェアや設備導入の際のコスト緩和
具体策：（８）コネクテッド・インダストリーズ税制

★（９）産業サイバーセキュリティセンターでの人材育成（IPA）
★☆（10）情報セキュリティスペシャリストの活用
☆（11）セキュアなベンダー・ツールの見える化（中企庁）
☆（12）セキュリティサービス審査登録制度

対策を講じたが・・

課題⑤：対策が十分かがわからない、実際に攻撃を受けたらどうしたらいいのかわからない　対策レビュー
（例）これまでのｻｲﾊﾞｰ攻撃による被害は全体で1割（大企業では１/４）
⇒対策：対策度合いの客観的評価が可能な仕組み、攻撃を受けた際の相談先・ガイドラインに則った対応策
具体策：（１）、（６）

資料：経済産業省作成

必要？

必要な対策は何？

対策を実施する人は？金は？

実施済みの対策で十分？

出典:経済産業省「2018年版ものづくり白書」

工場のセキュリティ対策は、なぜ必要・重要なのでしょうか？

⇒工場にとっての価値軸の視点で、目的を捉えることが重要

Fortinet 佐々木様の資料より引用

組織課題：ITとOTとでは異なるゴール

Pe Pr Te

情報セキュリティ部門

情報・データを守る

Confidentiality(機密性)

Identity (完全性)

Availability (可用性)

OT部門

生産活動・ビジネスを守る

Safety (安全性)

Quality (品質)

Environment (環境影響)

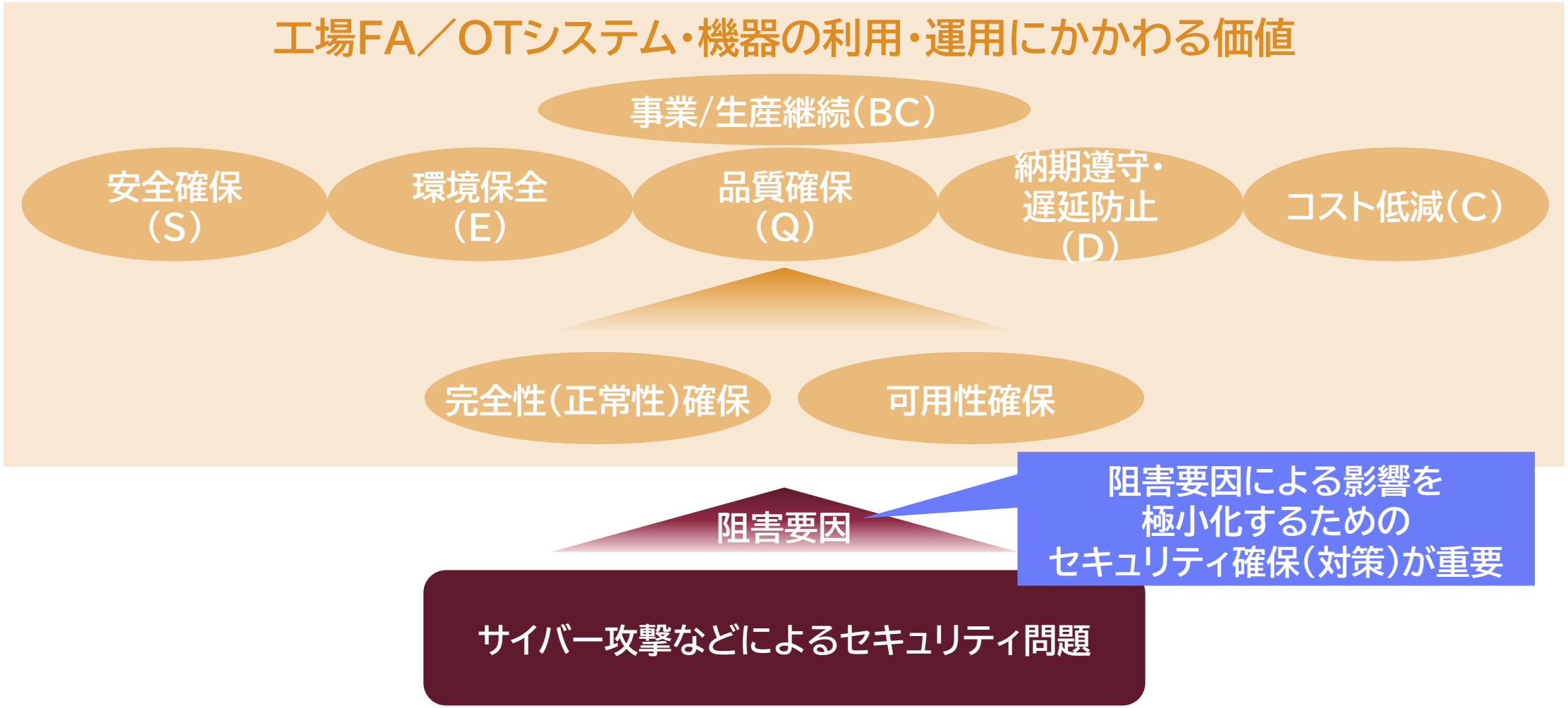
Cost (コスト)

Delivery (納期)

サイバーセキュリティはOT部門のビジネス目標達成のための手段

工場FA／OTシステム・機器におけるセキュリティ確保の位置づけ

工場FA／OTシステム・機器において**重視される価値:“BC/SEQDC”の視点**を中心に、どのようなセキュリティ確保(対策)が求められるのか？を考えることが必要かつ重要



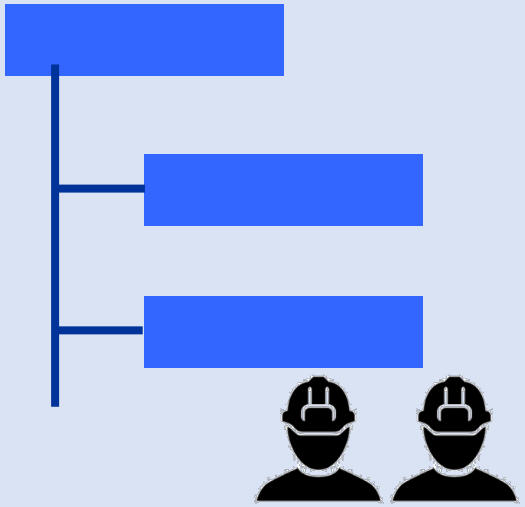
どのようなセキュリティ対策から
取り組めば良いのでしょうか？

Fortinet 佐々木様の資料より引用

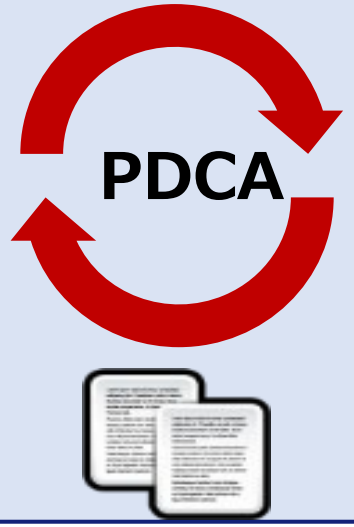
OTセキュリティの３要素

People（組織・人），Process（運用），Technology（技術）

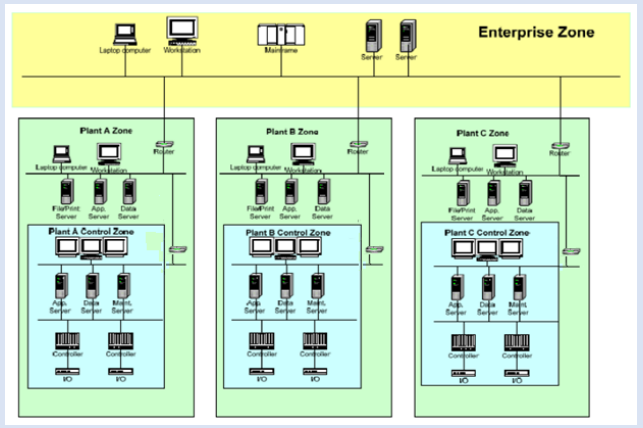
People



Process



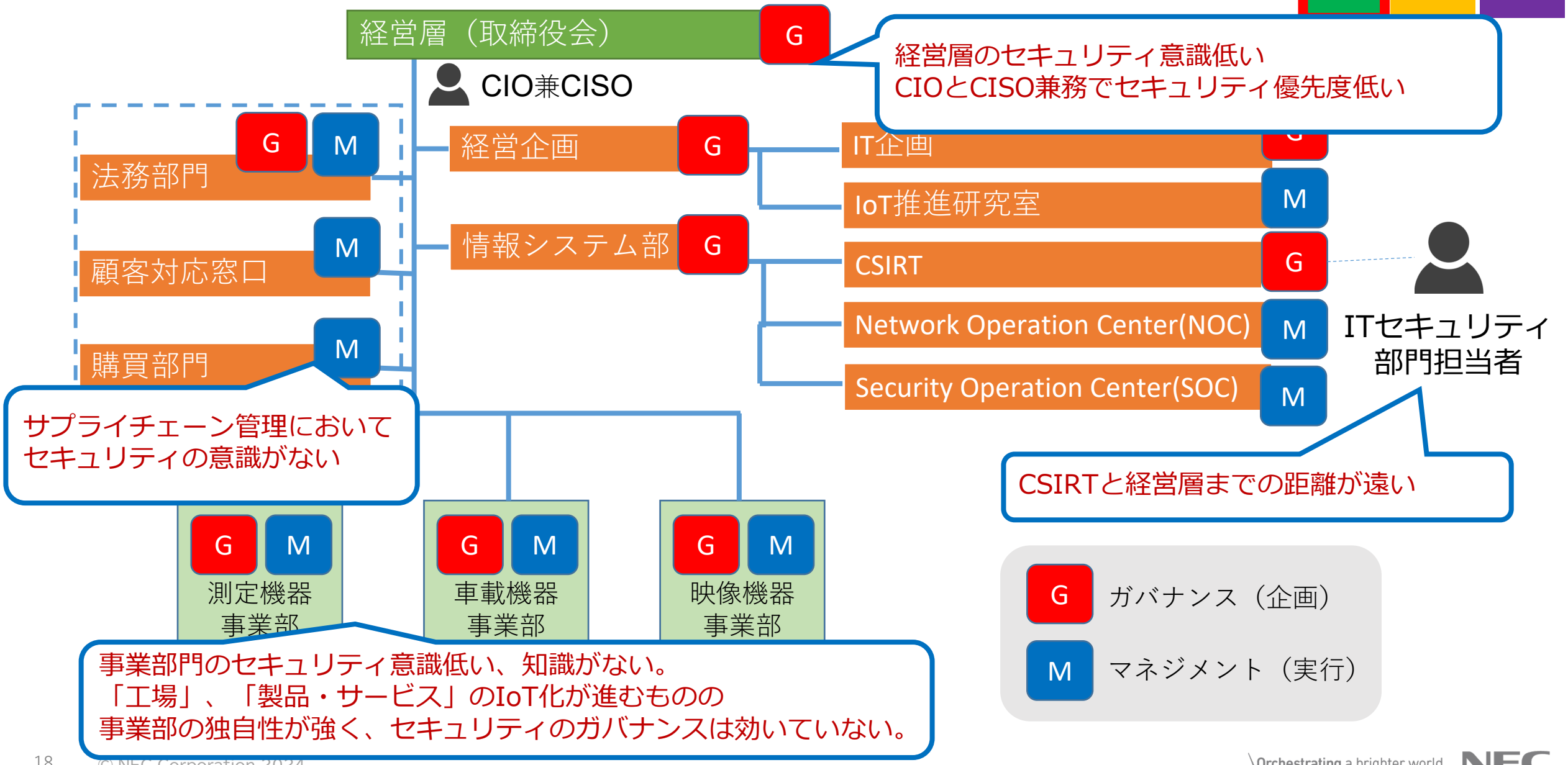
Technology



Fortinet 佐々木様の資料より引用

組織課題：誰も工場セキュリティ管理してない

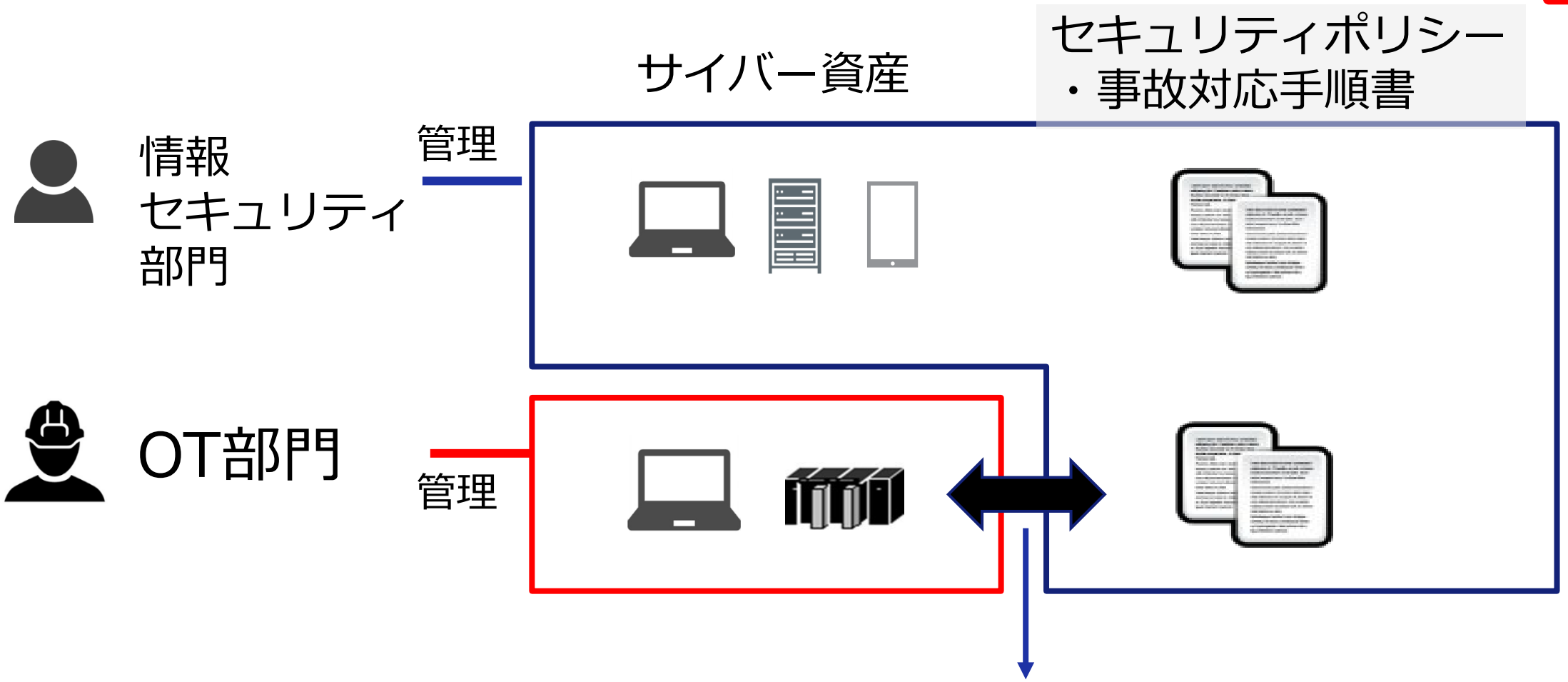
Pe Pr Te



Fortinet 佐々木様の資料より引用

運用課題：OTセキュリティポリシーの形骸化

Pe Pr Te



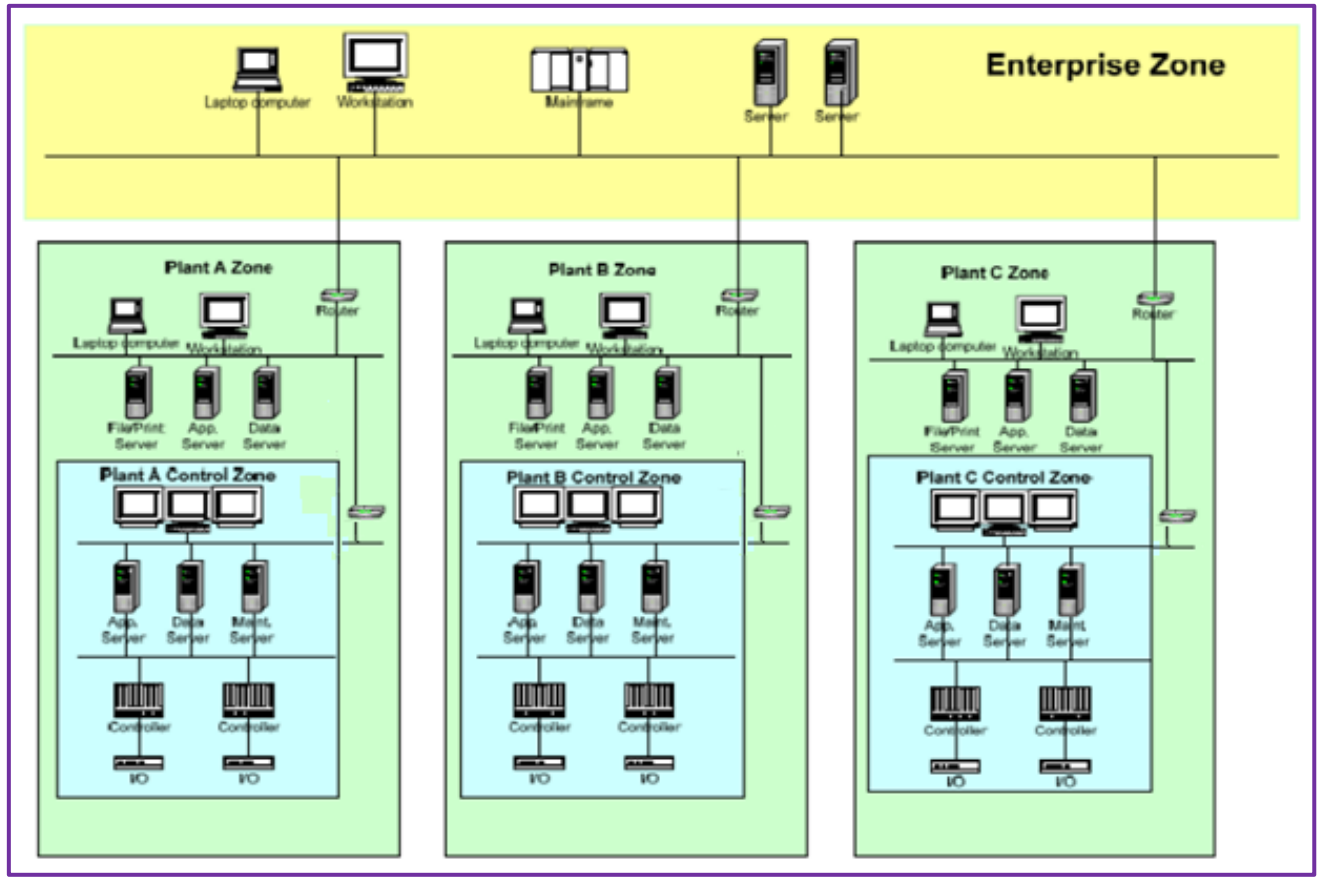
OT部門が資産管理しているためルールが形骸化しがち

Fortinet 佐々木様の資料より引用

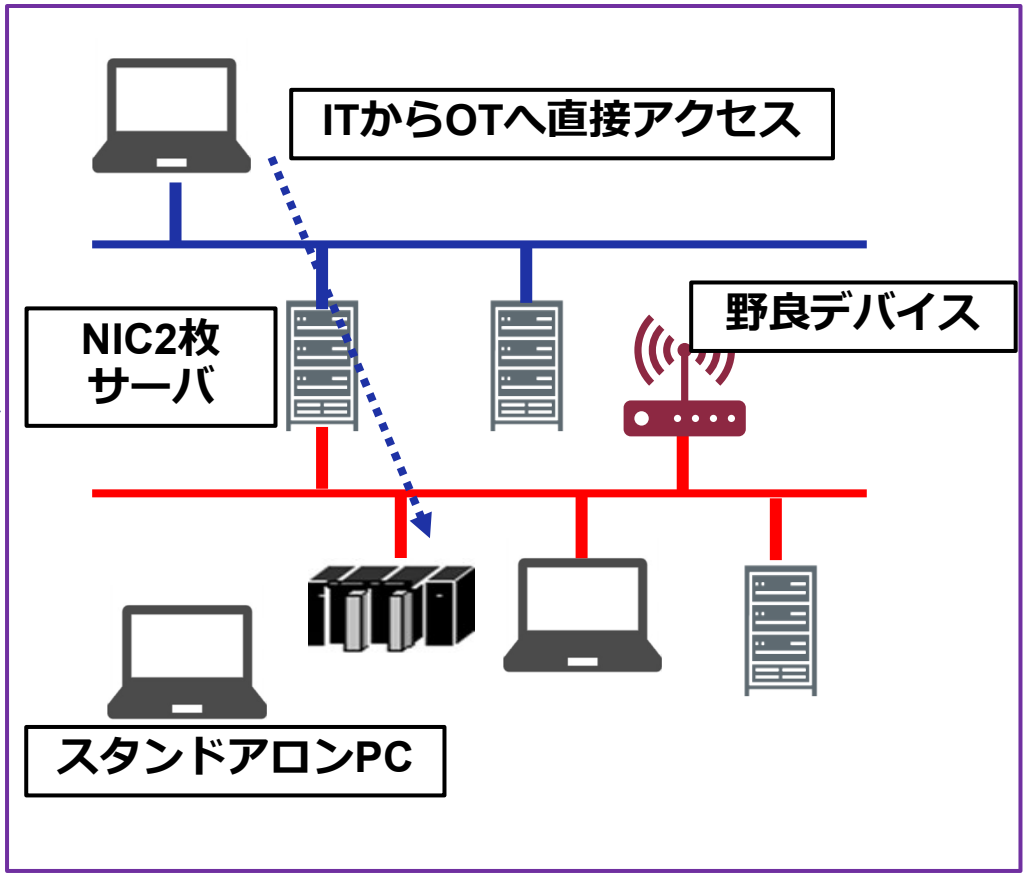
技術課題：工場ネットワークがフラット＆野放し

Pe Pr Te

教科書的な工場ネットワーク図



実際は・・・



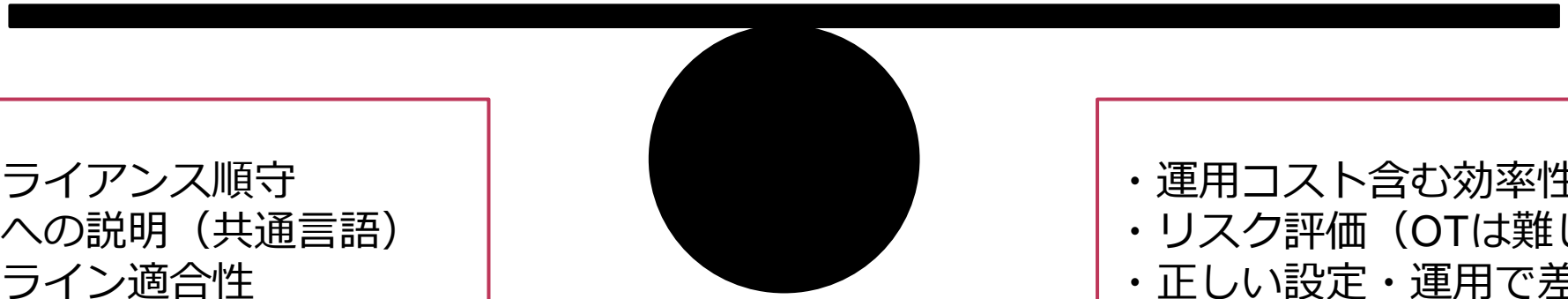
誰も工場ネットワークで何が起こっているか知らない

Fortinet 佐々木様の資料より引用

経済産業省の工場セキュリティガイドラインを活用して「説明責任」と「実効性」の両方を実現

説明責任

実効性



・コンプライアンス順守
・取引先への説明（共通言語）
・ガイドライン適合性
↓

但し、形骸化しやすいことに注意

・運用コスト含む効率性
・リスク評価（OTは難しい）
・正しい設定・運用で差がでる
↓

組織・運用・技術のバランス大事

“経済産業省のガイドラインに適合しています！”

“経済産業省のガイドラインを参考に自社のリスク応じた対策に落とし込んでいます！”

Fortinet 佐々木様の資料より引用

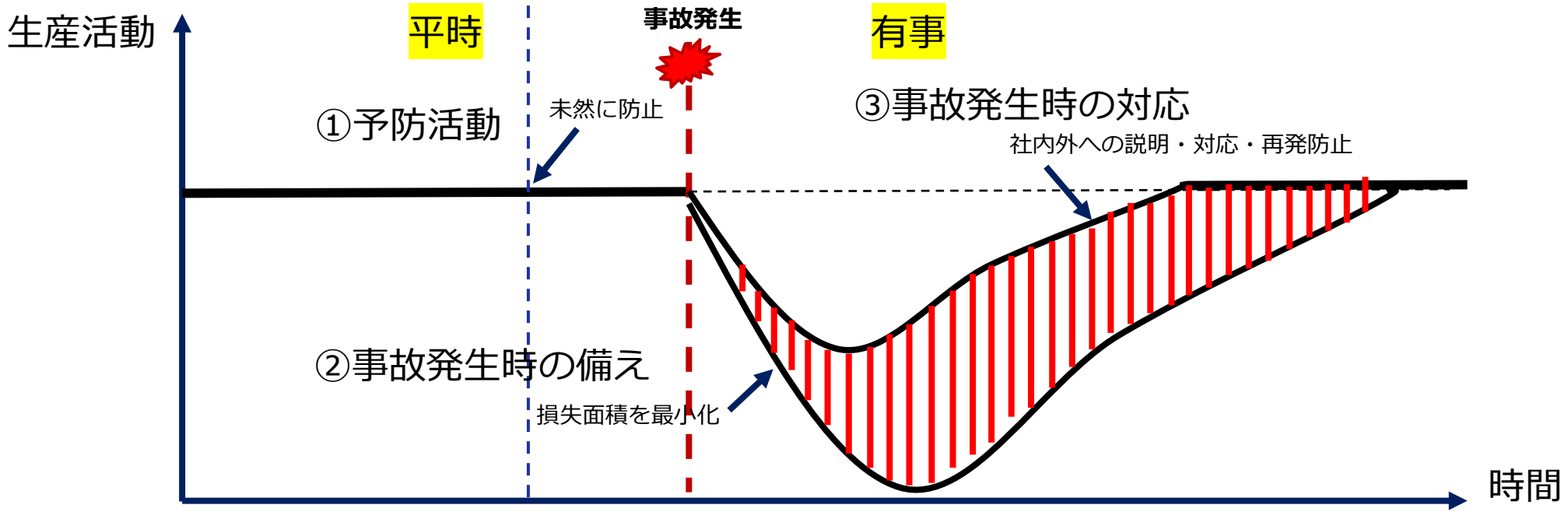
レジリエンスの考え方

「DX×セキュリティ」 = 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

①セキュリティ事故予防

②セキュリティ事故発生時の備え

③セキュリティ事故発生時の対応



今後のサイバーセキュリティのリスク対応は「防御の高度化」から「事故対応の高度化」へとシフトする

因みに、ガイドラインにて、どのようなセキュリティ対策が必要だと述べられているかというと…

【参考】経済産業省/工場セキュリティガイドラインの対策企画・導入の進め方

セキュリティ対策企画・導入の進め方

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

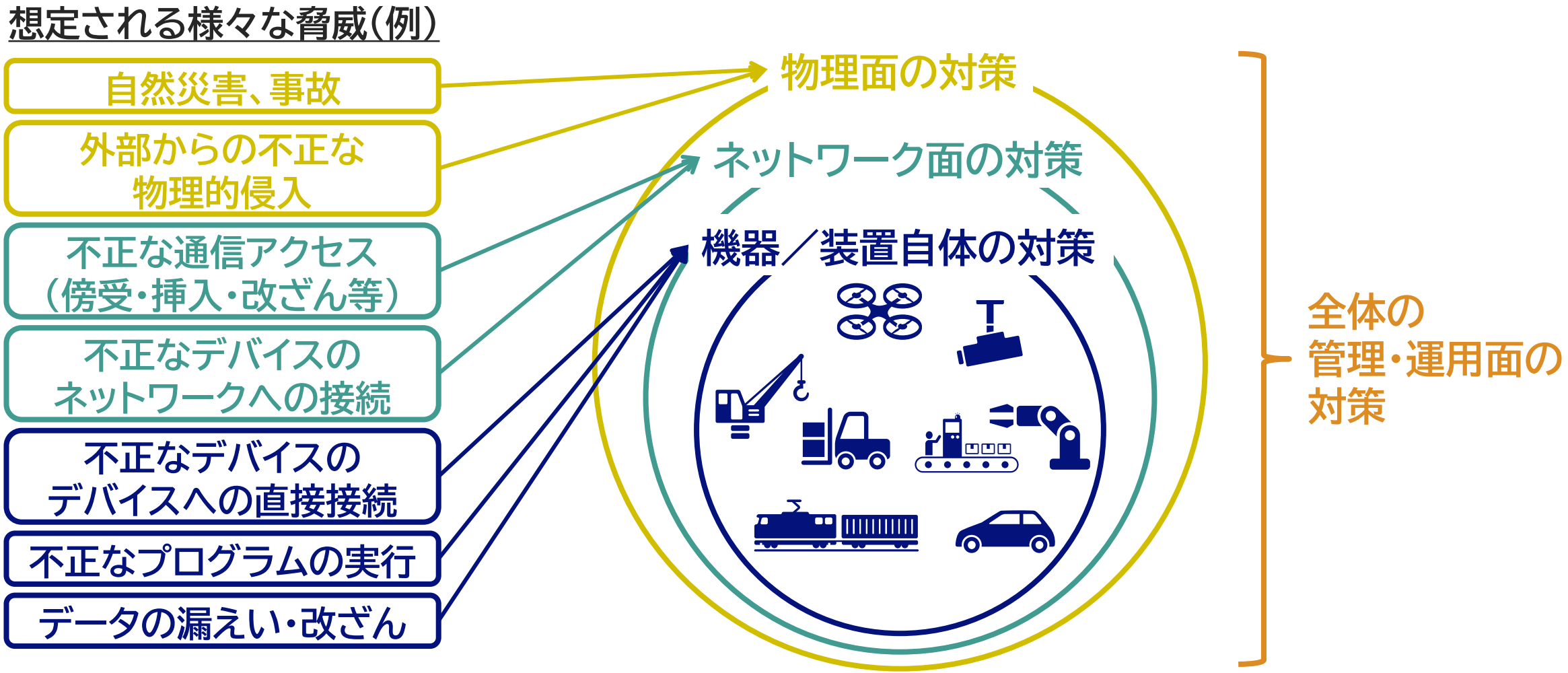
事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

1

出典：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」

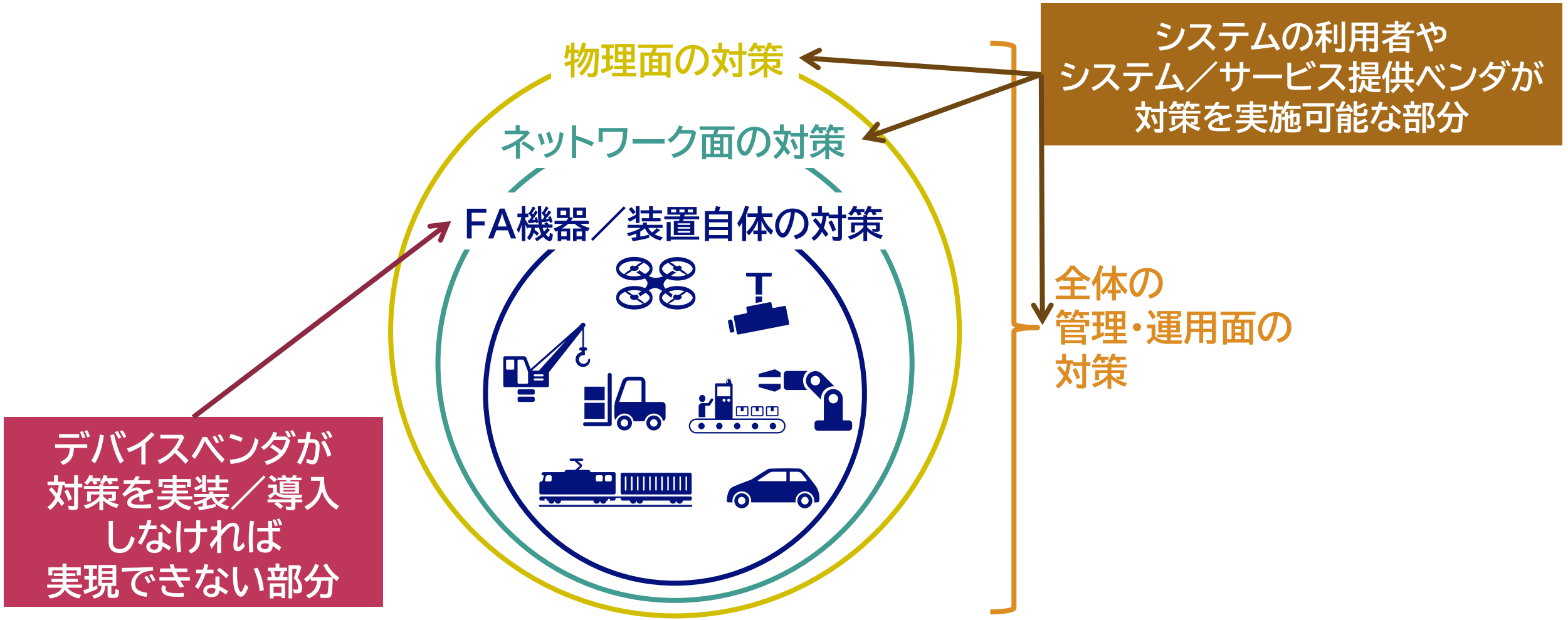
工場FAシステムにおいても多層防御を実現するセキュリティ対策が必要

工場FAシステム全体としての物理面、ネットワーク面、管理・運用面の対策に加え、
構成要素であるFA機器／装置自体のセキュリティ対策も併せて実施する必要あり



FA機器／装置のセキュリティ対策はデバイスベンダの責務

FAシステムの利用者やシステム／サービス提供ベンダがFA機器／装置自体の対策を実装／導入することは難しく、**デバイスベンダがその責務を果たすことが必要かつ重要**



セキュリティベンダが提供するサービス／製品の活用

セキュリティ対策実施に必要なスキル／人財／体制を確保できない場合には、
セキュリティベンダへアウトソーシングし支援を受ける選択肢を取ることも可能

◆ 活用できる主なサービス／製品の例：

- セキュリティ対策検討・企画支援
  - ポリシ策定支援、リスクアセスメント支援、要件定義支援など
- セキュリティ対策設計・導入支援
  - 設計支援、導入支援、製品提供など
- セキュリティ管理・運用支援
  - リモート管理・運用代行、問題監視・検知・対処、製品提供など
- セキュリティ維持・改善支援
  - 脆弱性／脅威情報提供、リスクアセスメント支援、脆弱性診断、製品提供など

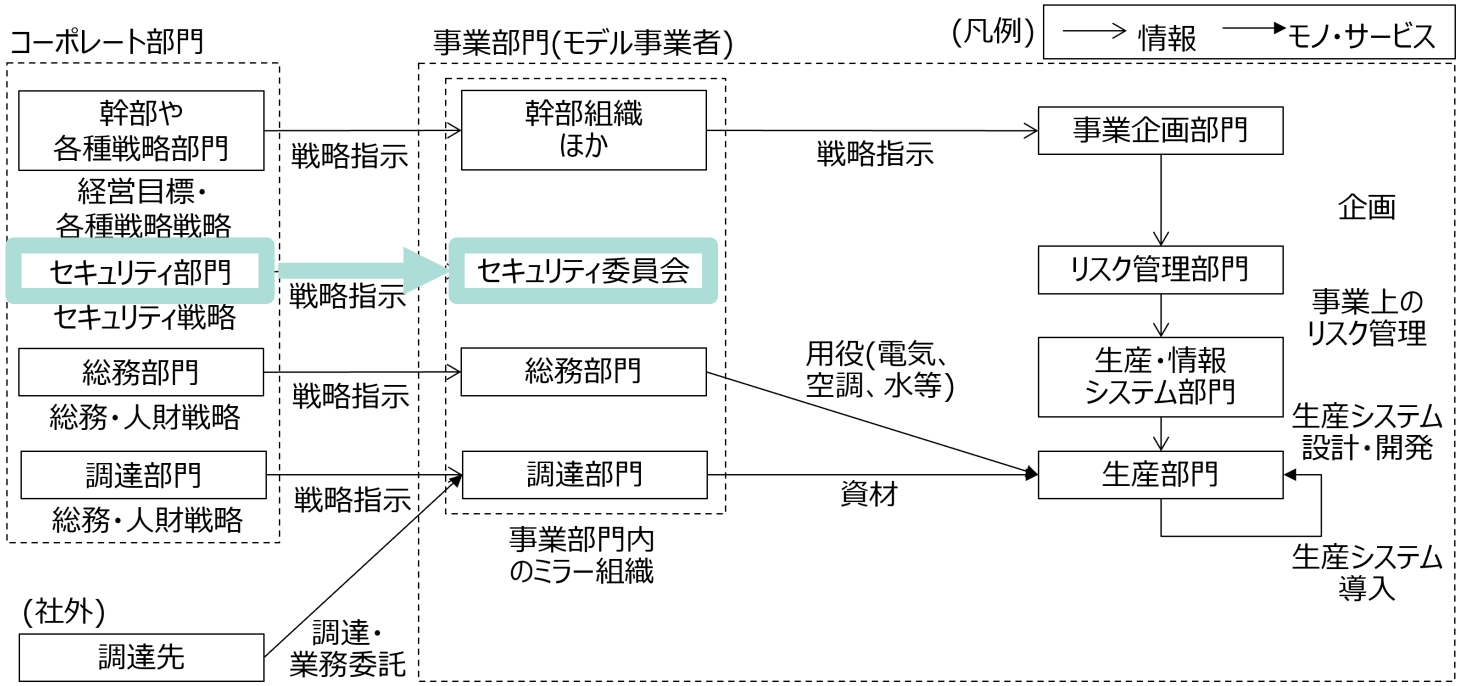
事例調査結果では、まずはどのような対策から実施されている状況でしょうか？

IPA 小助川様の資料より引用

モデル事業者全体のガバナンス体制 ：1.3.1(1)

付録E	組織的対策 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。

- コーポレート部門（本社機能）のセキュリティ部門
- 事業部門（工場）のセキュリティ委員会
  コーポレート部門（本社機能）にあるセキュリティ部門に対応するミラー組織。



コーポレート部門と事業部門（工場）の関係

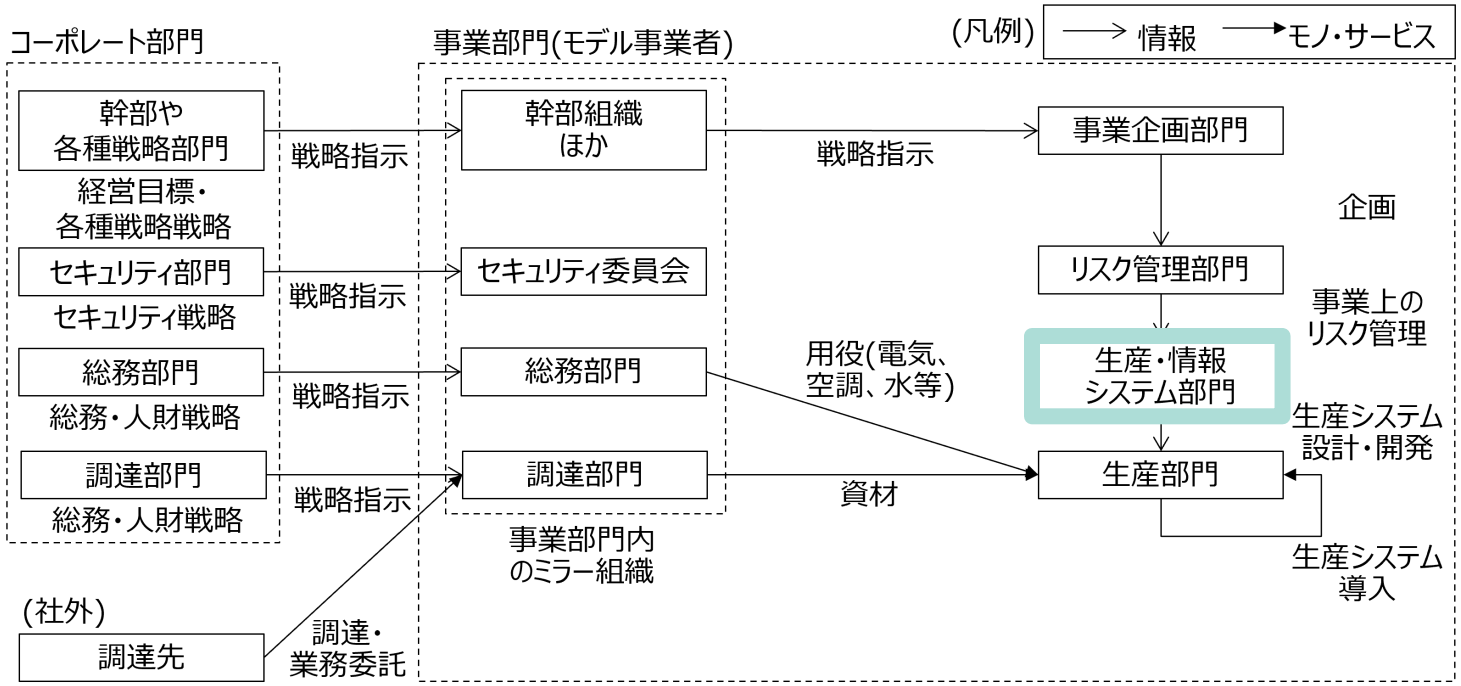
IPA 小助川様の資料より引用

モデル事業者全体のガバナンス体制 ：1.3.1(1)

付録E	組織的対策 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。

- 生産・情報システム部門

  このモデル事業者では生産システムも情報システムも同じ部門が一括で担当。ネットワークでつながった生産システムと情報システムを同一の部門で管理。



コーポレート部門と事業部門（工場）の関係

IPA 小助川様の資料より引用

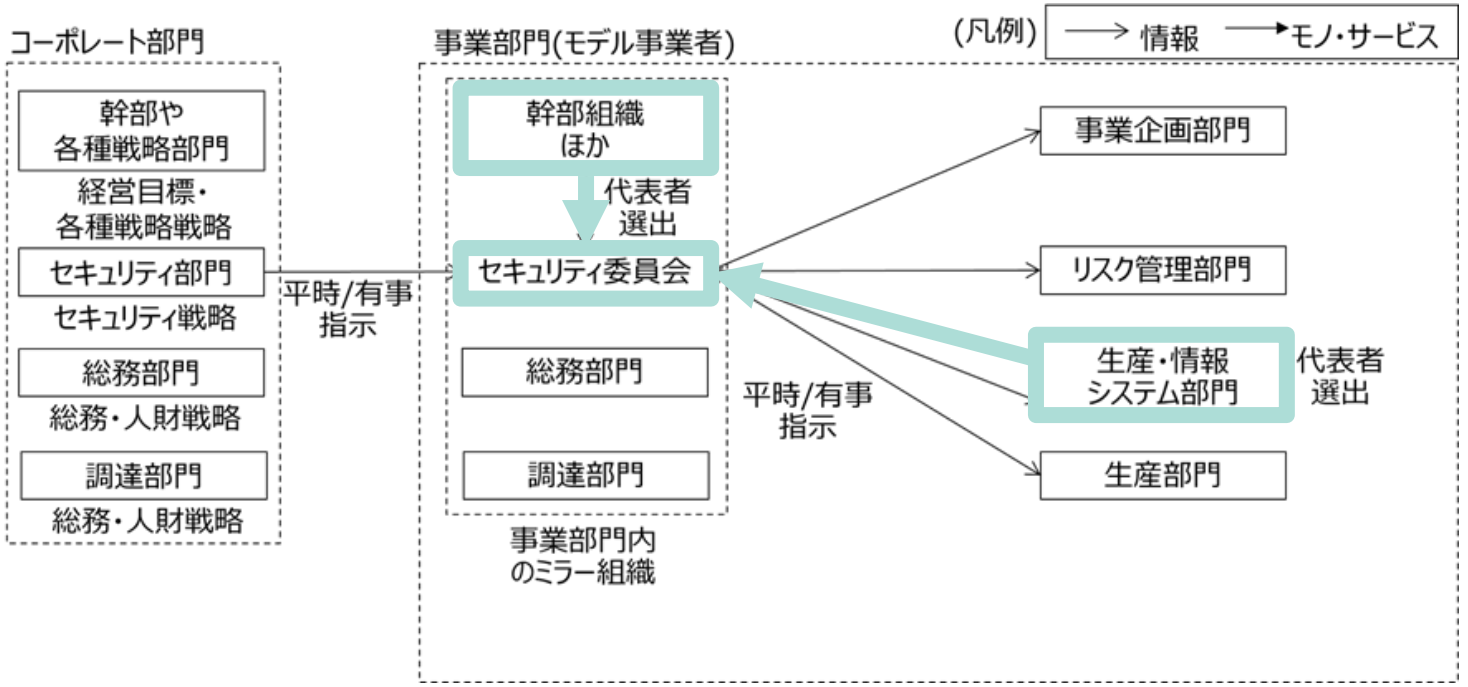
工場のセキュリティガバナンスの仕組み：1.3.1(1)

付録E	組織的対策 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。
	組織的対策 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。

- 事業部門（工場）のセキュリティ委員会

  幹部組織や生産・情報システム部門から選出された代表者で構成するセキュリティ委員会が存在する。

  生産・情報システム部門や生産部門などに対して指示を行うガバナンス機能をもつ。



平時・有事におけるセキュリティガバナンス

IPA 小助川様の資料より引用

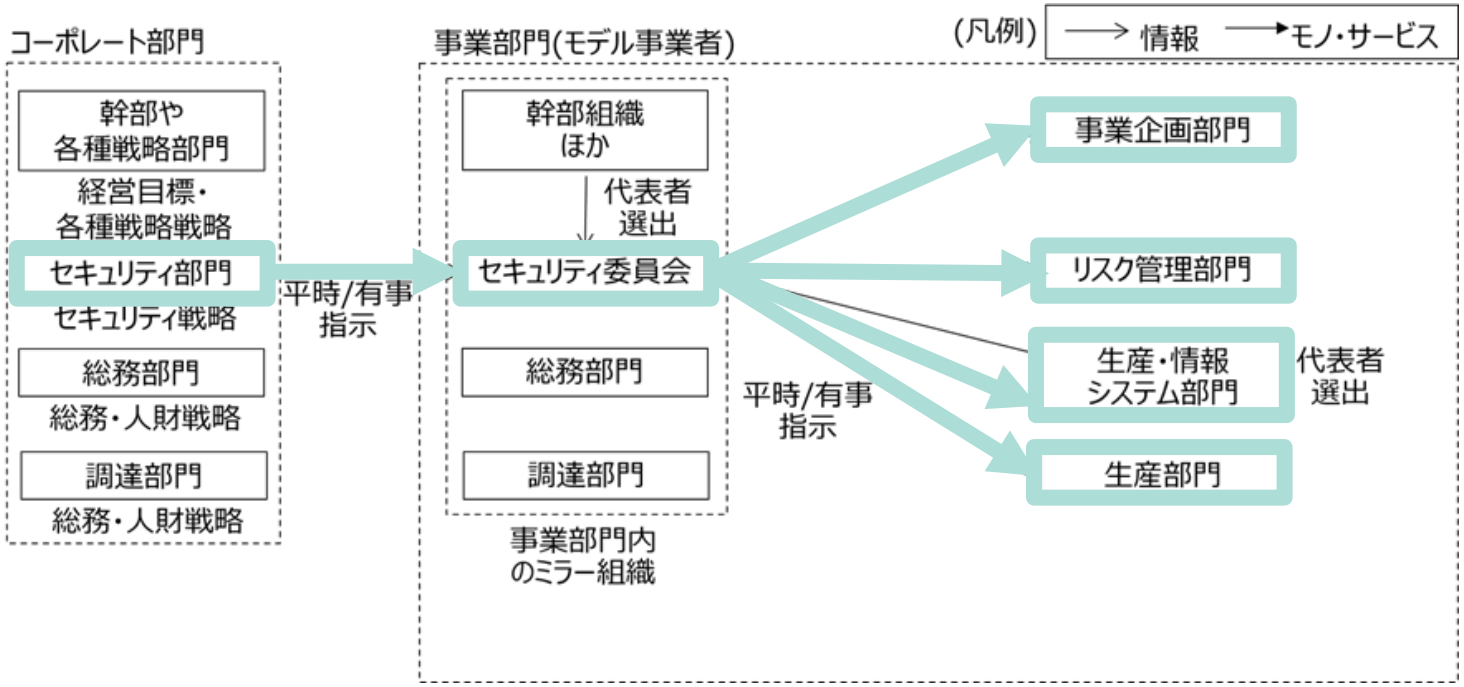
工場のセキュリティガバナンスの仕組み：1.3.1(1)

付録E	組織的対策 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。
	組織的対策 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。

- 事業部門（工場）のセキュリティ委員会

  幹部組織や生産・情報システム部門から選出された代表者で構成するセキュリティ委員会が存在する。

  生産・情報システム部門や生産部門などに対して指示を行うガバナンス機能をもつ。



平時・有事におけるセキュリティガバナンス

IPA 小助川様の資料より引用

生産システムの脆弱性対応の流れ：1.3.1(1)

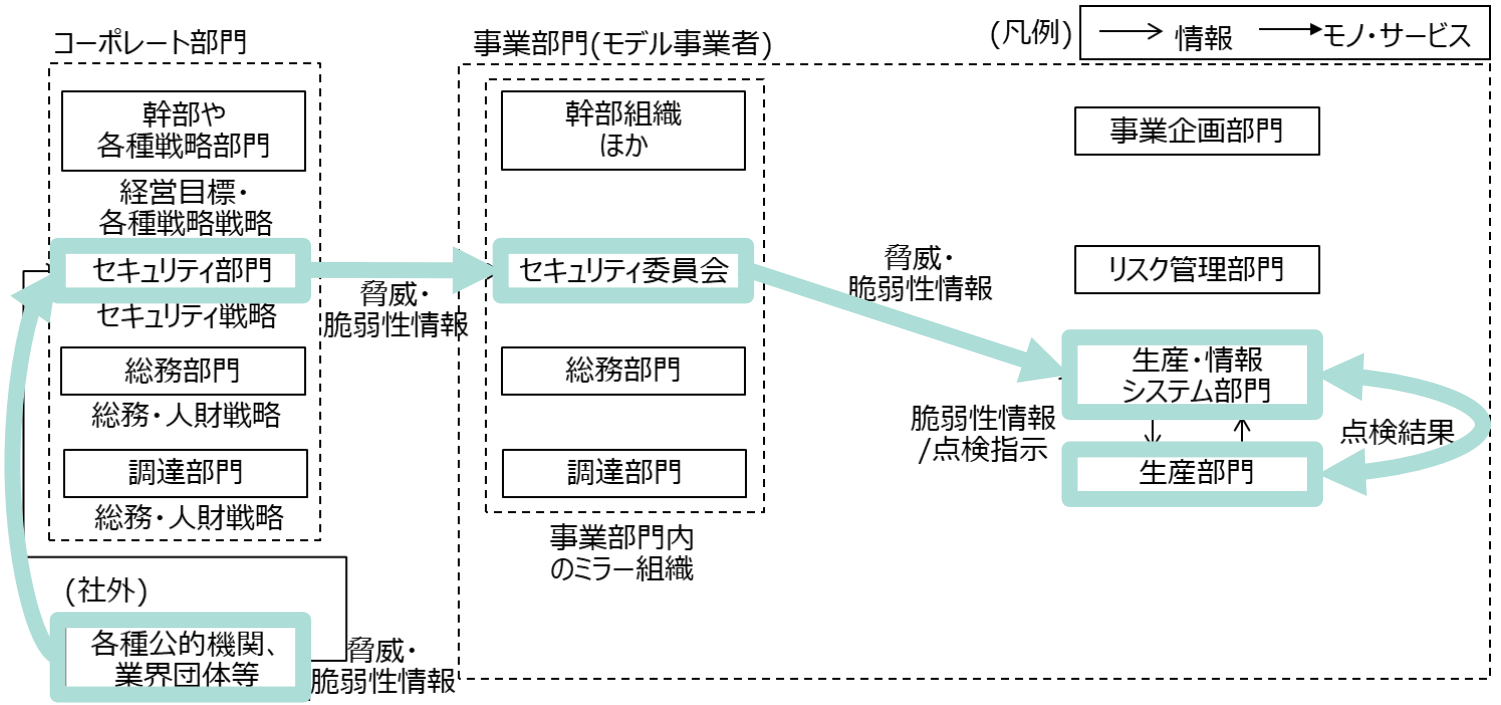
付録E	組織的対策 1-5	工場セキュリティに関する脅威の動向などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの現場教育を行っている。

- 生産システム（制御システム）の脆弱性対応フロー

(1)コーポレート部門（本社）が社外の脅威・脆弱性情報を収集、事業部門（工場）のセキュリティ委員会へと展開

(2)事業部門のセキュリティ委員会が生産・情報システム部門へ情報を展開

(3)生産・情報システム部門が対応の必要性を判断し、生産部門と連携して脆弱性点検や対応を実施



生産システムの脆弱性対応

IPA 小助川様の資料より引用

ゾーン分割と監視：3.1.2.1

付録E	運用的対策 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。
	技術的対策 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）。

- 実施例

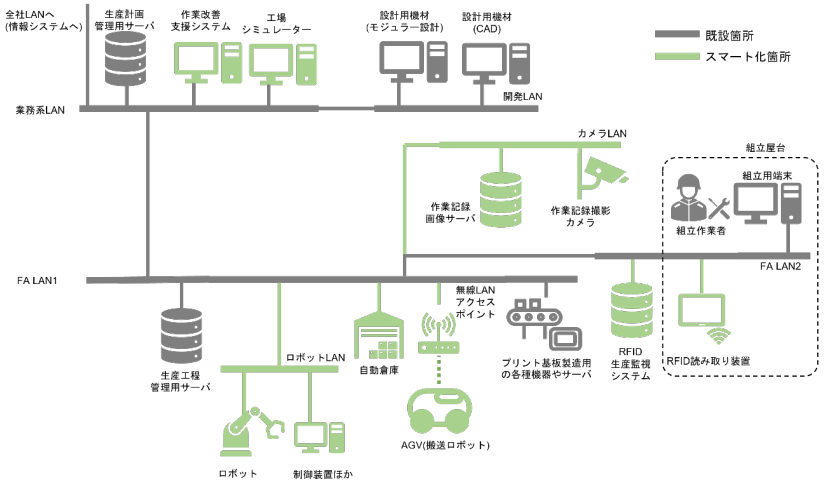
  セキュリティ規定文書：　セキュア開発手順

  以下のようにネットワークを分割する。

  ①IT環境とOT環境、②重要機能と補助機能、③外部ネットワークと内部ネットワーク

  ④生産管理システムと各生産ライン、⑤有線ネットワークと無線ネットワーク

  非常時には、これらのネットワーク間で通信を遮断し、最低限の事業を継続できるように設計する。



- 脅威

  ネットワークを経由してサイバー攻撃の被害が拡大する可能性がある。

- 低減されるリスクと残留リスク

  ネットワークを経由してサイバー攻撃の被害が拡大するリスクを低減することができる。

  システムの仕様上、分割困難なネットワークが残留する可能性がある。

  残留リスクを減らすためには、**システム設計の段階からセキュリティ上好ましいネットワーク分割を行えるように検討する必要がある。**

IPA 小助川様の資料より引用

機器のバックアップと復旧：3.1.5.11

付録E	技術的対策 3-12	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。

- 実施例

  セキュリティ規定文書： セキュア開発手順

  - バックアップ

    機器のデータバックアップを定期的に行う。

  - 復旧

    代替機を準備しておくほか、バックアップデータを基に**復旧するための手順を整理**しておく。

    また、**実際に復旧を行えることを事前に検証**しておく。

ランサムウェア対策を考慮する場合、
バックアップデータのオフライン保管、
イミュータブル化（不変化）が必要

- 脅威

  攻撃されたシステムを元の状態に復元できない可能性がある。

- 低減されるリスクと残留リスク

  システムを攻撃前の状態に復元できない可能性を低減できる。

  攻撃に利用された脆弱性は、システムを復旧しても残留したままであるため、別途根本的な対策が必要となる。

IPA 小助川様の資料より引用

資産の脆弱性の管理： 3.1.10

付録E	技術的対策 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している。もしくは代替策を講じている。
	工場システム SC*管理 4-3	納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダ・構築業者との連絡・連携体制を構築している。

* SC: サプライチェーン

- 実施例

セキュリティ規定文書： セキュア開発手順

◆ 脆弱性情報の一覧管理

資産の管理と連動し、関連する脆弱性情報を収集する。

主に、関連資産に対してパッチの適用を検討することになるが適用の可否や適用タイミングなどは事業への影響や対処を見送った場合の影響などを考慮して決定する。

脆弱性管理台帳

#	関連資産	脆弱性 (CVE-IDなど)	深刻度 (CVSSなど)	パッチ適用可否	パッチ適用時期	パッチ適用状況
1	XXX	CVE-XX	大	可	即時	済
2	XXX	CVE-YY	小	可	保守に合わせて実施	未適用
3		…				

- スマート化に際しての考慮事項

利用するIoT機器やサービスが多様化した際、それらの脆弱性・パッチ管理を自組織のみで実施するのは管理負荷が大きくなる可能性があるため、**機器やサービスの提供ベンダーとの協力体制を構築することが重要である**。また、上記のベンダーに対して、**該当機器やサービスの脆弱性が見つかった際の報告義務について契約時に合意する必要がある**。

IPA 小助川様の資料より引用

インシデントへの対応と体制： 7.2.1

付録E	組織的対策 1-4	事業継続計画（BCP）が策定されており、工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている。
	運用的対策 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。
	工場システム SC*管理 4-1	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。

＊ SC: サプライチェーン

- 実施例

  セキュリティ規定文書： 情報セキュリティマネジメント規則

  - 必要な対応

    ①検知と分析 ②封じ込め、根絶と復旧 ③インシデント後の対応

  - 体制

    ①検知と分析 現場運転員が機器の異常としてあげた方向を見落とさないよう、

    ②封じ込め、根絶と復旧：事業継続に責任のある幹部層をトップとして適切な指示が出せるよう、全社的な連絡体制を構築する等。

    ③インシデント後の対応： インシデント対応を通して得られた知見を組織間で共有できるよう、情報発信する組織、担当システムへの対象を検討する組織の整備。

- スマート化に際しての考慮事項

  モジュラー設計システムや工場シミュレーターなどを外部のサービスを利用して実現する場合や、ロボットやIoT機器などが他ベンダーからの借用や管理下にある場合、**関係するサービスプロバイダーやベンダーなどの他組織との連携を念頭に置いたインシデント対応計画が重要**。

NECPFの事例では、まずはどのような対策から
実施されている状況でしょうか？

NECプラットフォームズ 澤田様の資料より引用

実践のステップ

step 1 組織化

- 統括部門の発足

2019年、社内有志により
「セキュリティ統括部門」
を新たに設置

step 2 調査と計画

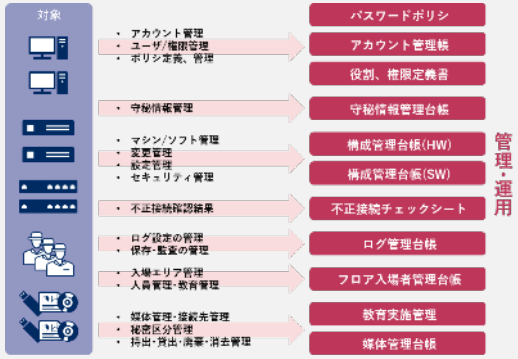
- 現状把握と基準策定

自社工場のセキュリティ対策状況を実態把握し
工場セキュリティの「あるべき姿」を設定
現状とのギャップに基づいて対策を計画

step 3 実行

- 施策の具体化と実行

抽出した課題に基づき
セキュリティ対策を具体化
ロードマップを設定



NECプラットフォームズ 澤田様の資料より引用

技術的対策 －基本的なセキュリティ対策－

工場の最初の課題はIT/OT資産の管理
セキュリティリスクの可視化+ラベリングと、統合管理を実装

◆ IT/OT資産のリスク可視化とラベリング

リスク小

青 ウイルス対策確認シール
- ウイルス対策ソフト導入済
- イントラネットから定義ファイルを自動更新

黄 ウイルス対策確認シール
- ウイルス対策ソフト導入済
- イントラネット非接続

指定の頻度もしくは起動時に定義ファイルを更新

赤 ウイルス対策確認シール
- ウイルス対策ソフト未導入
- USB型対策ソフト使用

・接続する媒体を都度スキャン
・指定の頻度もしくは起動時に本機器をスキャン

黒 ウイルス対策確認シール
- ウイルス対策ソフト未導入
- USB型対策ソフト使用不可

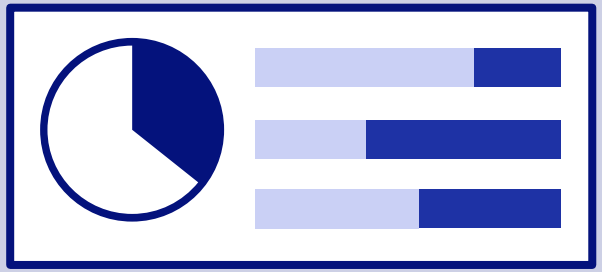
接続する媒体を都度スキャン

リスク大

◆ 管理ツール

物品管理システム

☑ 対策実施チェック
☑ 対策実施チェック
☑ 対策実施チェック
…



ルール遵守徹底　　徹底状況の可視化

システムの主な目的はルール遵守徹底と可視化

導入効果

物品管理	台帳運用	リスク可視化
情報の横断共有 物品の状況把握 証跡保存可	メールによる自動通知	自動集計 組織横断集計 集計結果可視化

NECプラットフォームズ 澤田様の資料より引用

技術的対策 －基本的なセキュリティ対策－

工場にあるサーバやPCに、基本的なセキュリティ対策を実施

ログインの設定

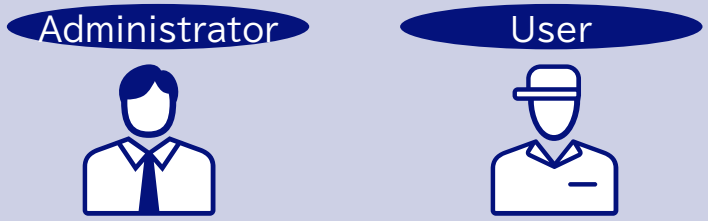
- パスワードを設定
  - 複雑性（文字数/文字種の指定）
  - 再利用を禁止
- 失敗時のロック回数・回復時間を設定
- スクリーンセーバーを設定

ログ設定

- PCのログ記録機能を有効化
  - 利用状況と保存期間からログサイズを算出
- 時刻同期機能を有効化

権限分離

- 管理者（社員）権限と一般（作業員）権限を分離



必要最小限化

- 不要なソフトウェアの削除
- USBポート・LANポートの封鎖
- ガードキーを取り付け

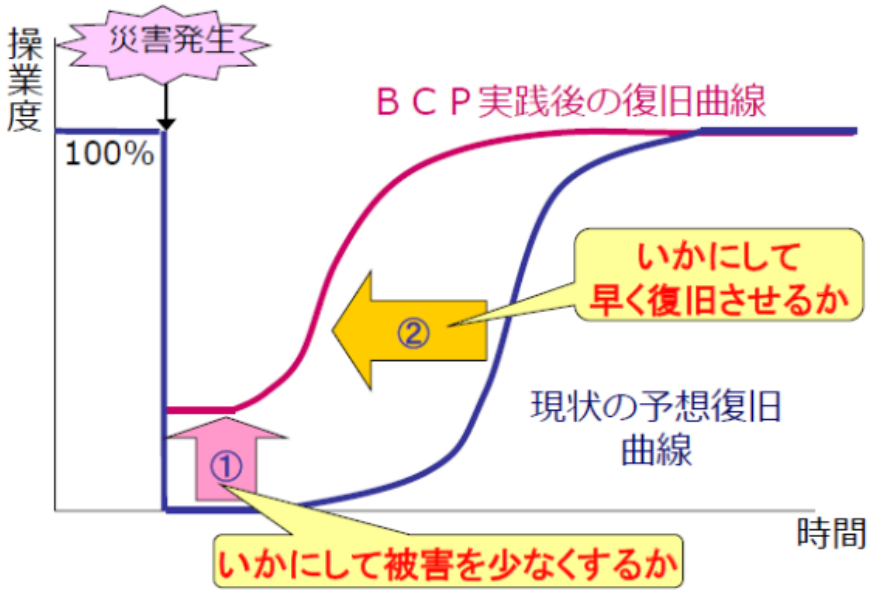
NECプラットフォームズ 澤田様の資料より引用

BCPの策定 –「侵入される」ことを前提に復旧計画を準備–

自然災害とサイバー攻撃の違いを切り口に サイバー攻撃対応BCPの必要性を関係者に説明

◆ BCPの考え方

本質は「起こることを前提に事業を継続するための計画を立てておく」こと



◆ 自然災害とサイバー攻撃の違い

自然災害	サイバー攻撃
● **発生と検知** 発生が明確	● **発生と検知** 発生が不明確 （発生と発見のタイムラグ）
● **対応と復旧** 機器の修理・交換	● **対応と復旧** 原因分析の結果に応じた対応
● **減災対策** 水害対策 耐震対策	● **減災対策** マルウェア対策 NWセキュリティ対策

NECプラットフォームズ 澤田様の資料より引用

訓練 －ステップ1：シナリオをつくる－

関係者と一緒に各工場にカスタマイズした訓練シナリオを作成
現場の運用に合わせた現実味のある内容に

内閣府「「企業の事業継続訓練」の考え方」を参考にシナリオを作成

セキュリティ部門

セキュリティの知見
- 工場で想定される攻撃/被害
- 各役割に期待する行動

生産部門

工場の知見
- 生産機器や現状の対策状況
- 復旧対応時の役割分担
- 工場の生産製品

まずは・・・ セキュリティ部門でシナリオのベースを作成
つぎに・・・ 各工場の実態を取り込みカスタマイズ

POINT

現実的なストーリー
- 起こり得る攻撃/被害を想定
- 各工場における運用実態を反映
- 実際の役割・役職で自分事化

役割ごとに期待する行動を明示
- BCPで示しきれない役割の詳細な行動を示す
- 参加者の理解度への配慮が必要

NECプラットフォームズ 澤田様の資料より引用

訓練 －ステップ2：計画を練る－

訓練は「段取りで8割」「実施で2割」
生産業務への影響を最優先に配慮しつつ、関係者と連携して実施計画を作成

事前準備

- **日程**
  生産影響が出ないよう
  工場側の都合を優先
- **参加者**
  工場幹部(工場長、部門長)
  ライン作業者
- **シナリオ確認**
  訓練するライン選定
  シナリオの確認

実施計画

1日目：前日準備

① 下見
（ラインや事務所・機器の運用など）

② シナリオの妥当性確認
（実施場所/被害など想定条件の評価）

③ 段取りの最終整合
（進行・役割の確認）

2日目：訓練当日

① オープニング

② 訓練

③ 結果の整理
（参加者と実施結果を確認）

④ ふりかえり
（参加者と意見交換）

POINT

- 現場で方針判断する幹部の参加を必須化
- 副次効果で他の参加者の参加意欲も高まる
- 日程は3ヶ月前に確保

NECプラットフォームズ 澤田様の資料より引用

訓練 －ステップ3：訓練する－

現実に近い状況で、各フェーズで行うべき行動ができるかを確認
肝は「検知」→「エスカレーション」→「初動対応」の迅速性

◆ 対応の流れ

①検知

②部内エスカレーション

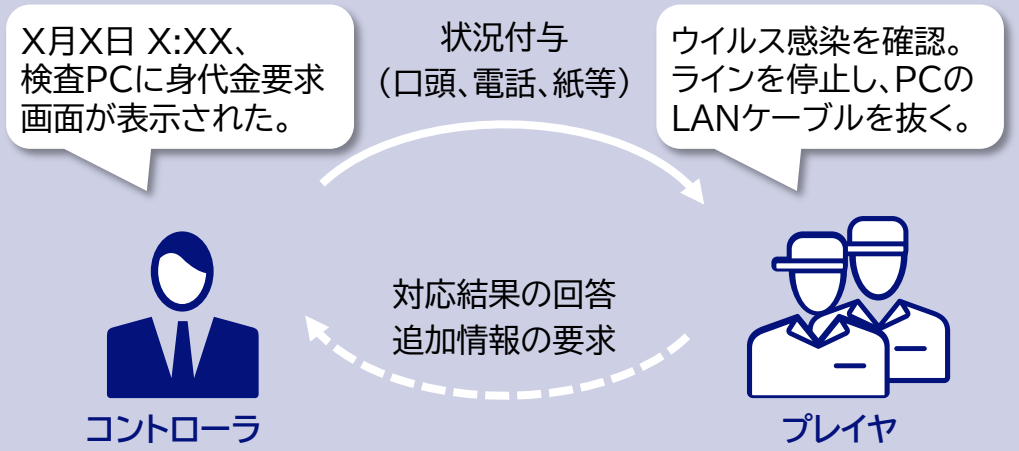
③初動対応の協議

④初動対応
（検体採取）

⋮

◆ 訓練の手法

ロールプレイング方式



① コントローラが全体進行、プレイヤへ状況付与もしくは質問
② プレイヤは、状況を基に判断し、BCPに従って行動
③ コントローラは、プレイヤの行動を確認

POINT

失敗を恐れない
- 発見した不備・過失・気付きが多いほど、訓練の価値は高い

訓練を止めない
- 想定外の事態が発生しても臨機応変に対応

NECプラットフォームズ 澤田様の資料より引用

訓練 －ステップ4：ふりかえる－

終了後すぐに(記憶の新しいうちに)意見交換
訓練の都度、現場の意識が向上し改善につながる

2021年度訓練から得られた課題	フィードバック
現場からのコメント • 生産・出荷再開判断のプロセスの記載がない • 5M/1E管理の記録に合わせたい **発見した気づき** • バックアップからの復旧はしたことない	**BCP改版** • 「生産・出荷再開判断」をプロセスとして追加 • PC交換などの処置内容を記録する事を追記 **次年度訓練の改善** • バックアップからの復旧訓練を追加

2022年度訓練から得られた課題	フィードバック
現場からのコメント • 生産・出荷再開判断は別プロセスにすべき • 現場のエスカレーションルールと合わせたい • シナリオ配布の訓練ではなく、プレイヤはBCPだけを参照する実践的な訓練にすべき	**BCP改版** • 「生産再開」と「出荷再開」の判断プロセスを分割 • 既存のエスカレーションルールと整合 **次年度訓練の改善** • プレイヤにシナリオを配布しない訓練に変更

NECプラットフォームズ 澤田様の資料より引用

訓練の風景

◆ 目的

- インシデント対応の考え方と手順を習得
- インシデント発生時に必要な心構えの理解深耕
- サイバー攻撃対応BCPの有効性を確認

◆ ポイント

- セキュリティインシデント発生のシナリオに沿ったロールプレイング
- あらかじめ用意した事業継続計画に基づいて、適切なエスカレーション・対策本部設置・調査が実施できるかを検証

NECプラットフォームズ 澤田様の資料より引用

管理者向けの訓練

◆ 目的

- 緊急対策本部長の役割・対応手順を習得
- インシデント発生時、管理者に必要な心構えの理解

◆ ポイント

- 対策本部長になり得る管理者同士によるグループワーク研修で、実例に則したインシデントへの対応を協議
- 初動対応から業務復旧までの行動をシミュレーションし、その結果に対する講師からのフィードバックで理解深耕

研修の構成

座学講習

インシデント発生時の対応をディスカッション

NECPFでは、今後はどのような維持・改善活動に
取り組んでいくご意向でしょうか？

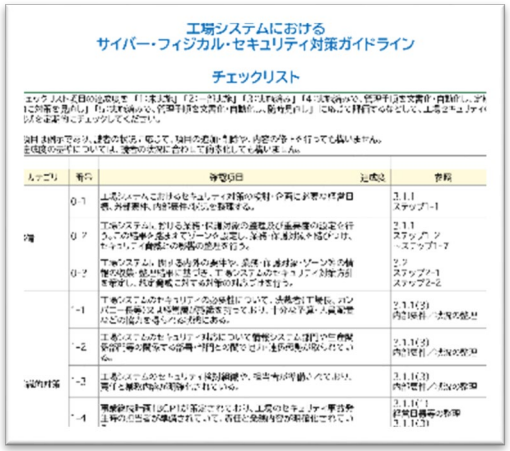
NECプラットフォームズ 澤田様の資料より引用

これまでの活動をふりかえり、改善へ

「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」に基づく第三者評価を、継続的改善に活用

◆ ガイドラインの概要

- 国内製造業(工場)のセキュリティ対策標準
- 2022年11月16日に、経済産業省が発行
- FA/OTシステムに特有の要件にフォーカス
- 必要最小限に絞った基本要件を定義



◆ 診断の結果

- 全体的に高評価(上位10%以上)
- 「運用・技術・SCM」対策に改善の余地

体制・ルール・BCPについて高評価

システム化・SC管理に改善の余地

項目	当社主要工場	他社平均 (参考)
総合	B	C
組織	A	C
運用	B	C
技術	C	C
SCM	C	D

NECプラットフォームズ 澤田様の資料より引用

これからの取り組み

「運用・技術・SCM」の改善を中心に今後の対策を検討

◆ アセスメントから導き出された課題

項目	当社主要工場	他社平均（参考）
総合	B	C
組織	A	C
運用	B	C
技術	C	C
SCM	C	D

体制・ルール・BCP について高評価

システム化・SC管理 に改善の余地

診断結果を参考とした対策の検討
運用・技術・SC管理に係わる対策を強化

全生産拠点のリスクアセスメントを実施
生産拠点のリスクを洗い出し計画的に対策

◆ 人手不足への対策

FSIRT（Factory Security Incident Response Team）
工場で生じるセキュリティ課題の対応を専門におこなう体制
体制・ルール

FSOC（Factory Security Operation Center）
工場のNWや機器を監視し、攻撃の検知や対応を行う仕組み
システム化

まとめ

- 「**工場のCPS化／スマート化／DXの進展**」は、
  製造業／工場のビジネスや社会にとって、多大な価値をもたらす
- 「**工場のセキュリティ対策不足（脆弱なところ）を突く脅威**」により、
  「**影響度の大きな問題・被害（工場の操業停止等）**」が多発している
- 工場FA／OTシステム・機器のセキュリティ対策はどうすれば良いのか？
  - 「**工場セキュリティガイドライン**」を活用
  - **製造業／工場が重視する価値軸：BC/SEQDC**の視点を中心に検討・推進
  - **技術・システム面**の対策だけに頼らず、**組織面**、**管理・運用面**の対策を**バランスよく**、**一歩ずつ段階的に向上**
  - 多層防御を実現する**デバイスのセキュリティ対策導入は、デバイスベンダの責務**
  - **セキュリティベンダへアウトソーシングし支援を受ける選択肢**
  - セキュリティは**“協調領域”**⇒「**組織・企業・業界の枠を超えた連携**」で全体を底上げ
- 「**必要なセキュリティ対策を実施し、工場FA／OTシステム・機器を安全・安心に活用する**」ことで、新たな価値を手にしよう

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。


Orchestrating a brighter world
NEC