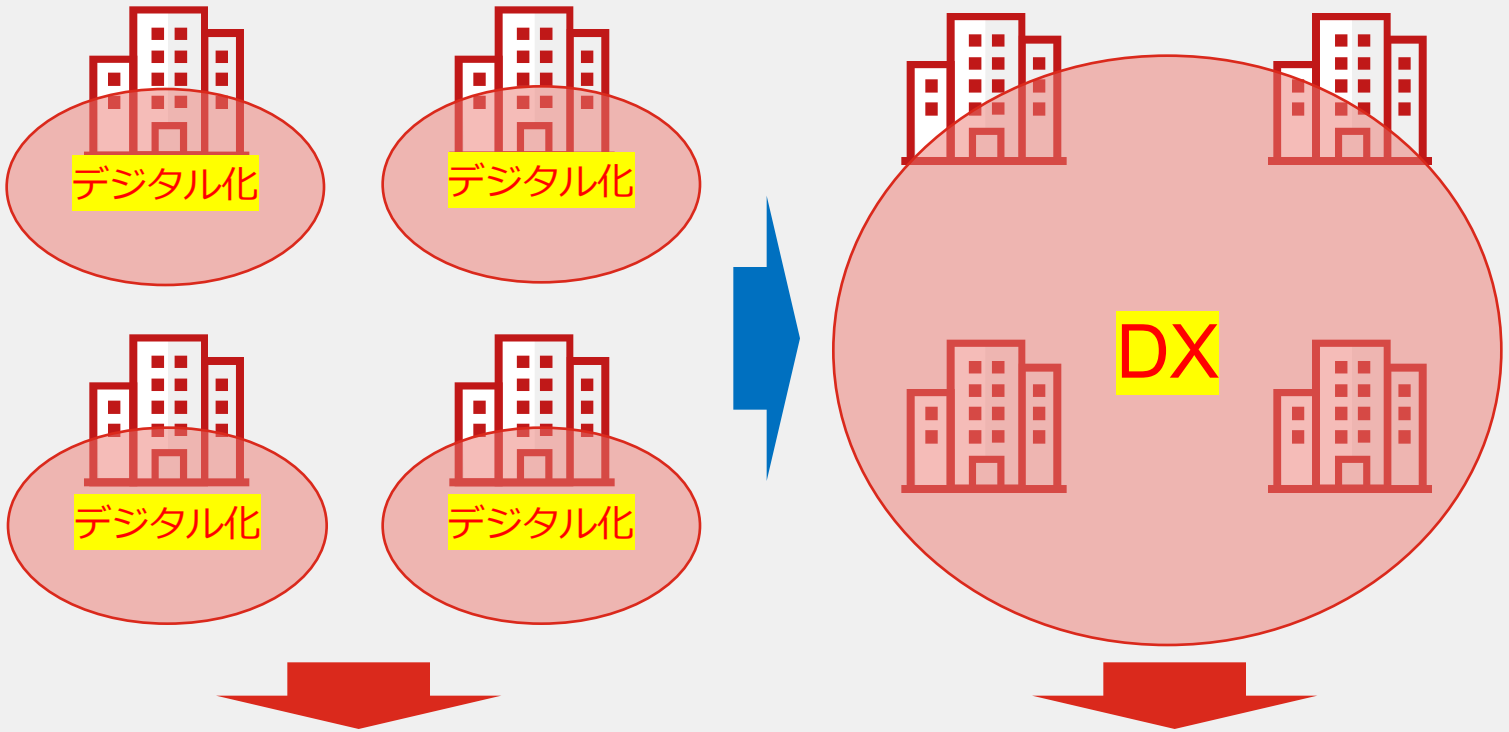
工場システムのサイバーセキュリティ課題とガイドラインの活用

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

「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

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（10年）

2012年11月～現在
　・セキュリティベンダーにて産業サイバーセキュリティのビジネス開発
　（現：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）
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)
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　プロジェクト准教授
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～)

執筆活動

・IT media/Monoist/BUILT
http://www.itmedia.co.jp/author/208471/（電力・ビル・ICS一般）
・ZDNet Japan
https://japan.zdnet.com/article/35151196/ (スマートシティ)
・EnterpriseZine
https://enterprisezine.jp/article/detail/13268（DX）
・マイナビ
http://news.mynavi.jp/author/0002071/
http://news.mynavi.jp/dp/c/t/iot_security
・インプレス
http://sgforum.impress.co.jp/type/157


スマートシティのセキュリティを考える


M2M/IoT時代に登場した新たなセキュリティの脅威とその防衛策


いきなり社長に呼ばれたらDXセキュリティ対策を丸投げされた件

https://www.shoeisha.co.jp/book/detail/9784798171067

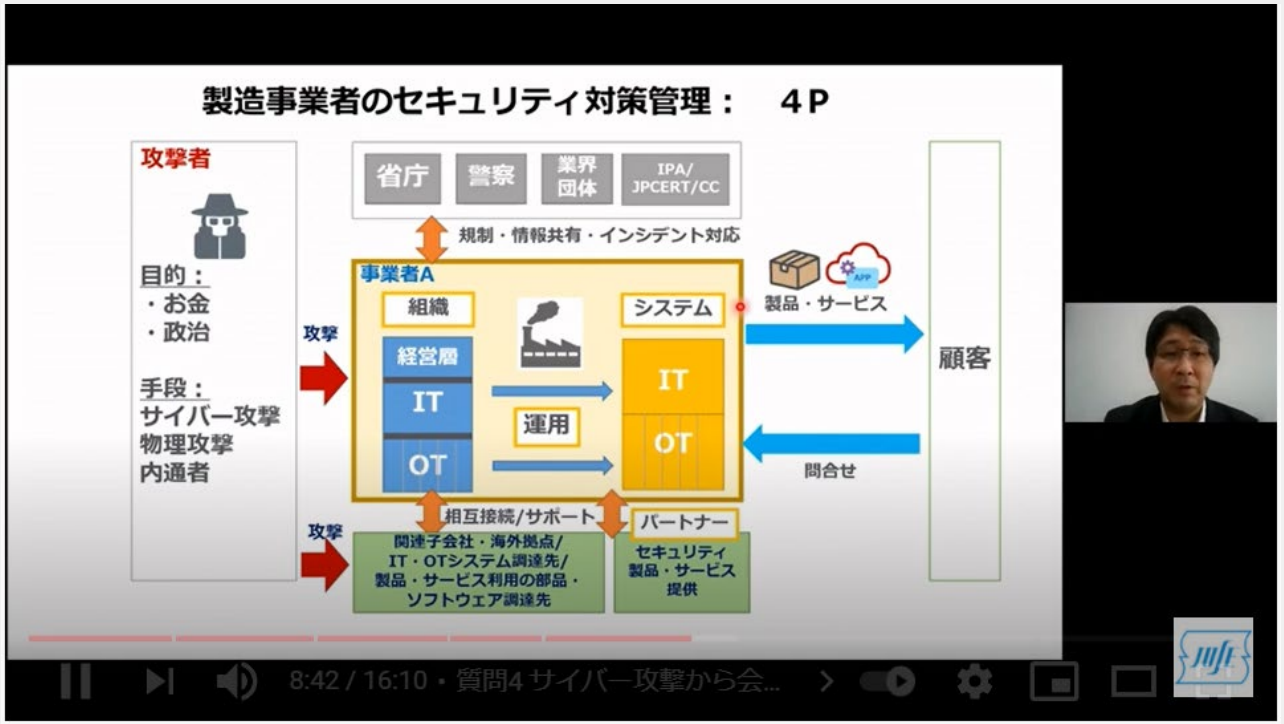
製造業のサイバーセキュリティ（2021/4/22発売）

製造業のサイバーセキュリティ管理対象の体系的な整理/実践的な対策の解説

https://www.juse-p.co.jp/products/view/859

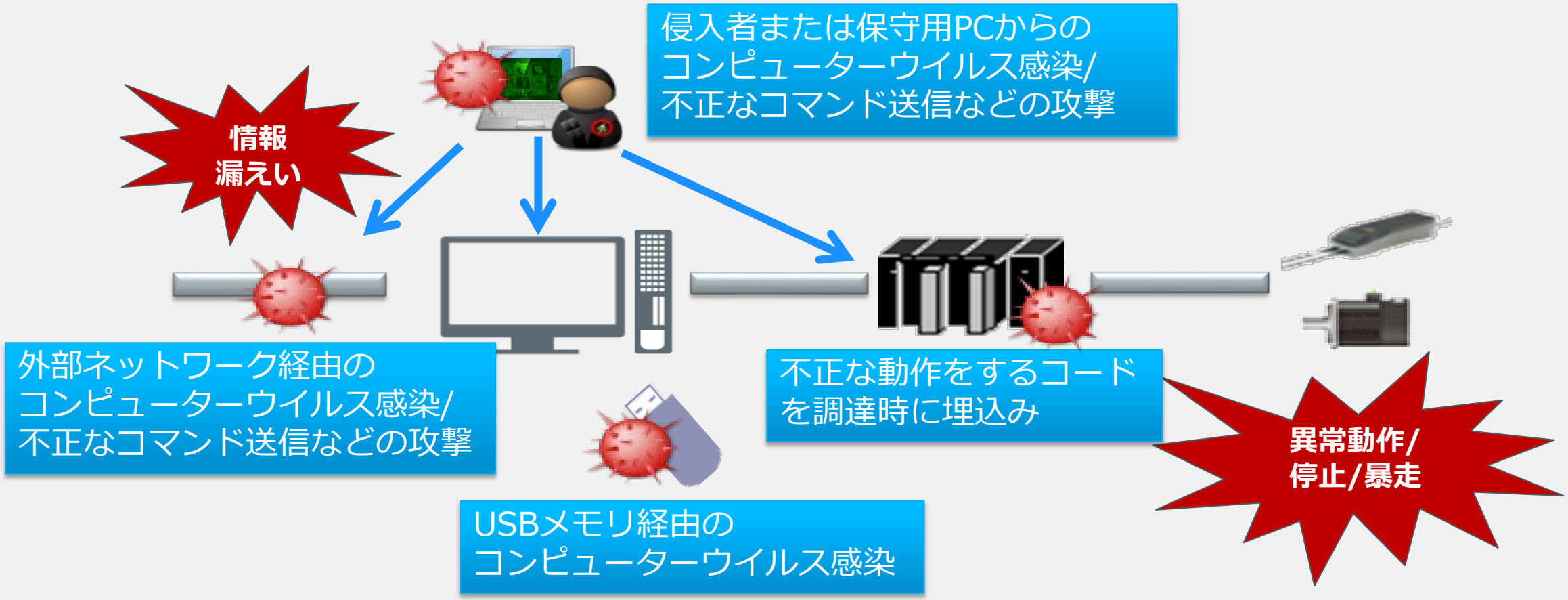
第1章　製造業のサイバーセキュリティ脅威
第2章　製造業セキュリティ対策の全体像
第3章　製造業セキュリティ対策
第4章　ガイドライン、フレームワーク
第5章　仮想企業によるセキュリティ対策実施例
付録　FA-C2M2 チェックリスト解説

内容紹介動画（YouTube）https://www.youtube.com/watch?v=a7sYy7SkON



工場のサイバーセキュリティ課題
（現場のヒアリングからみる実態）

工場におけるサイバーセキュリティ脅威の入口



工場のデジタル化に伴い外部とのサイバー的なつながりが増え、
“現場の運用”だけではリスクが低減できなくなってきた

ことに気づかず、組織・運用を見直さず技術に頼る施策で“失敗”する企業が多い

工場システムデジタル化の主要なセキュリティ課題

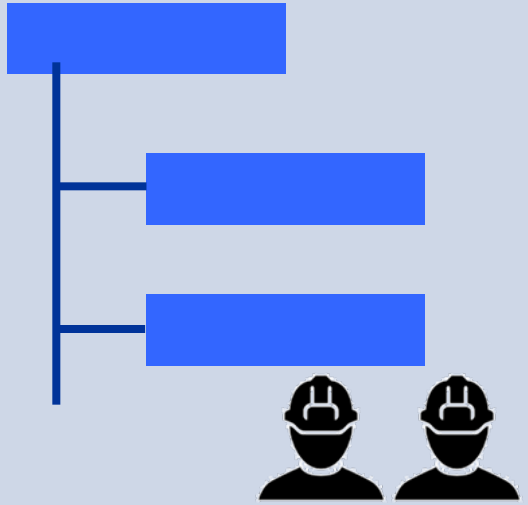
ビジネス目標：高収率の実現, 工場リモートメンテナンス, 需要への素早い対応

工場向けプロジェクト: クラウド上のAI活用した工場データ解析,
リモートアクセスシステムの導入, 受発注システムとの連携

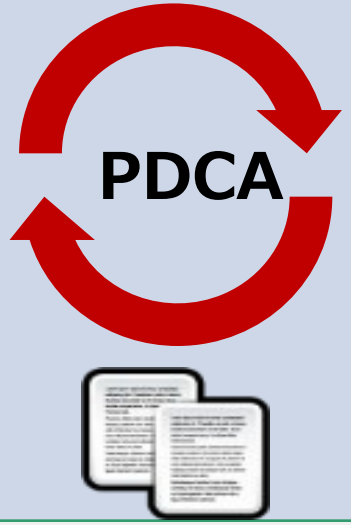
サイバーセキュリティ上の課題がDX推進の大きな障害となっている

People（組織）, Process（運用）, Technology（技術） の課題

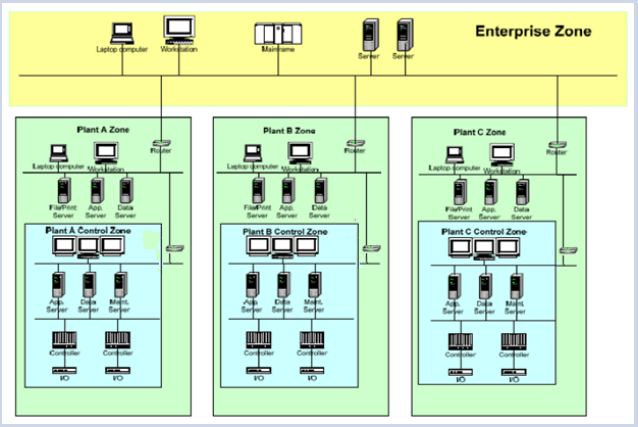
People



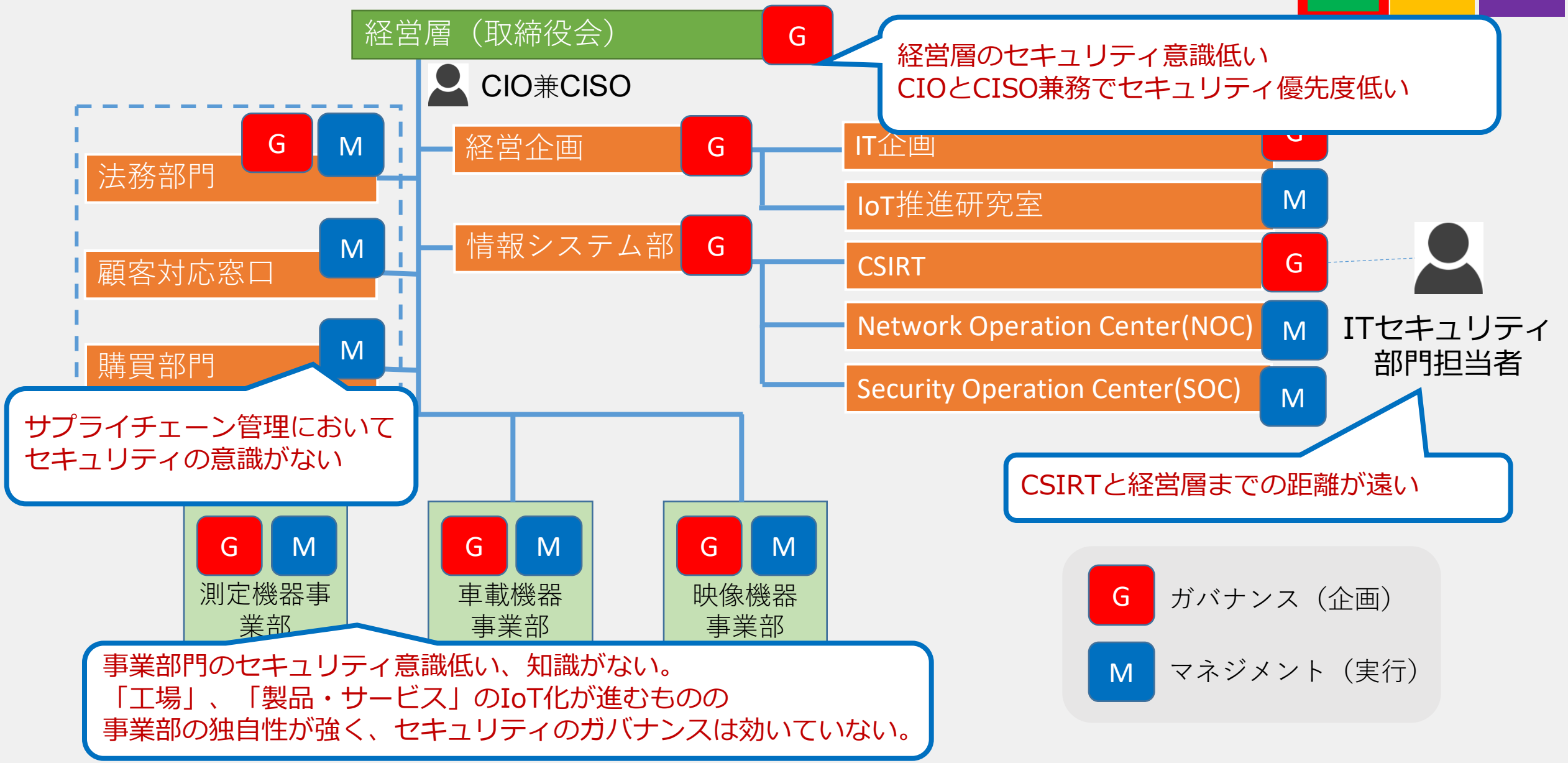
Process



Technology

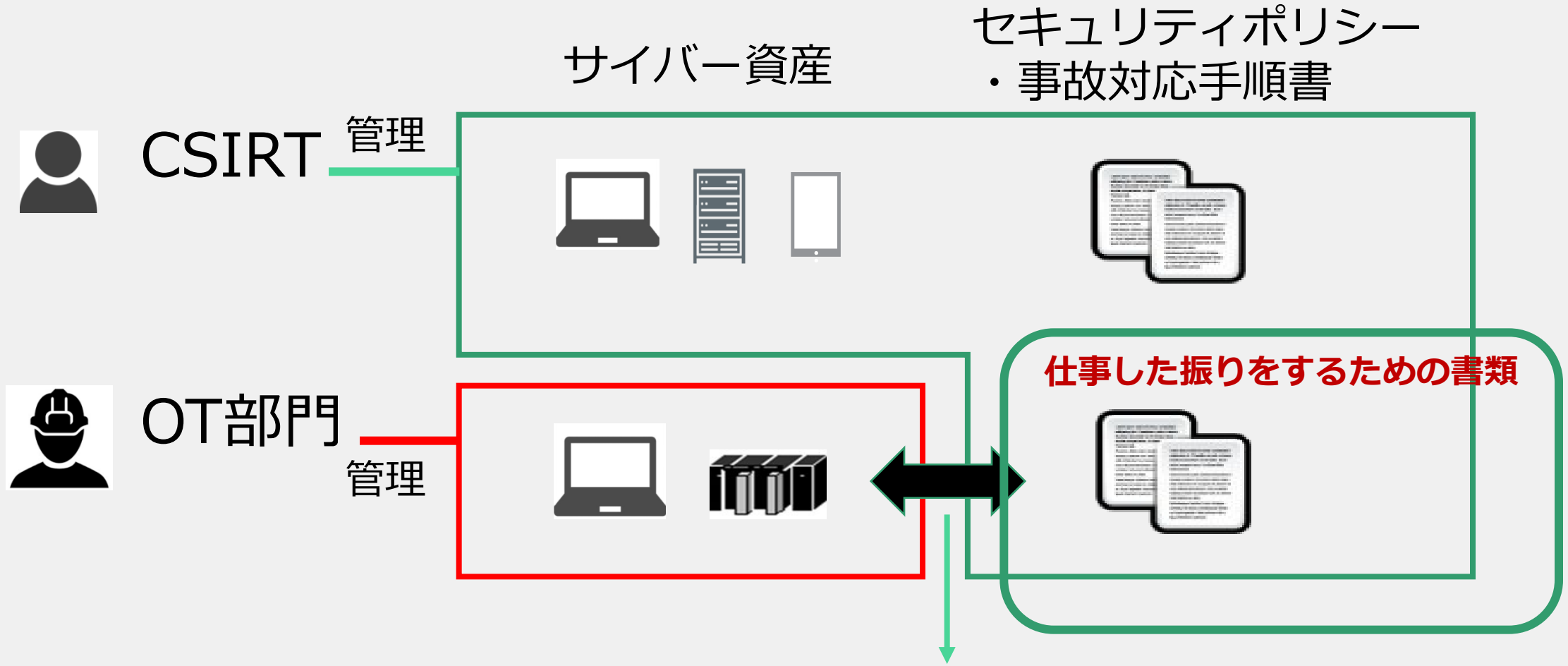


組織課題：誰も工場セキュリティ管理してない



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

本当にあった怖い話

Pe Pr Te

本当にあった怖い話①

・情報システム部が策定した工場セキュリティポリシーで**「工場のUSBメモリ原則禁止」**が定められ、全てのPCに鍵付きのUSBポート蓋が設置された
・半年後、情報システム部が監査に訪れると、USBポートの蓋は閉まっていたがほとんどの**PCの横に鍵が置かれていた**

専用引抜ツールで引き抜く

本当にあった怖い話②

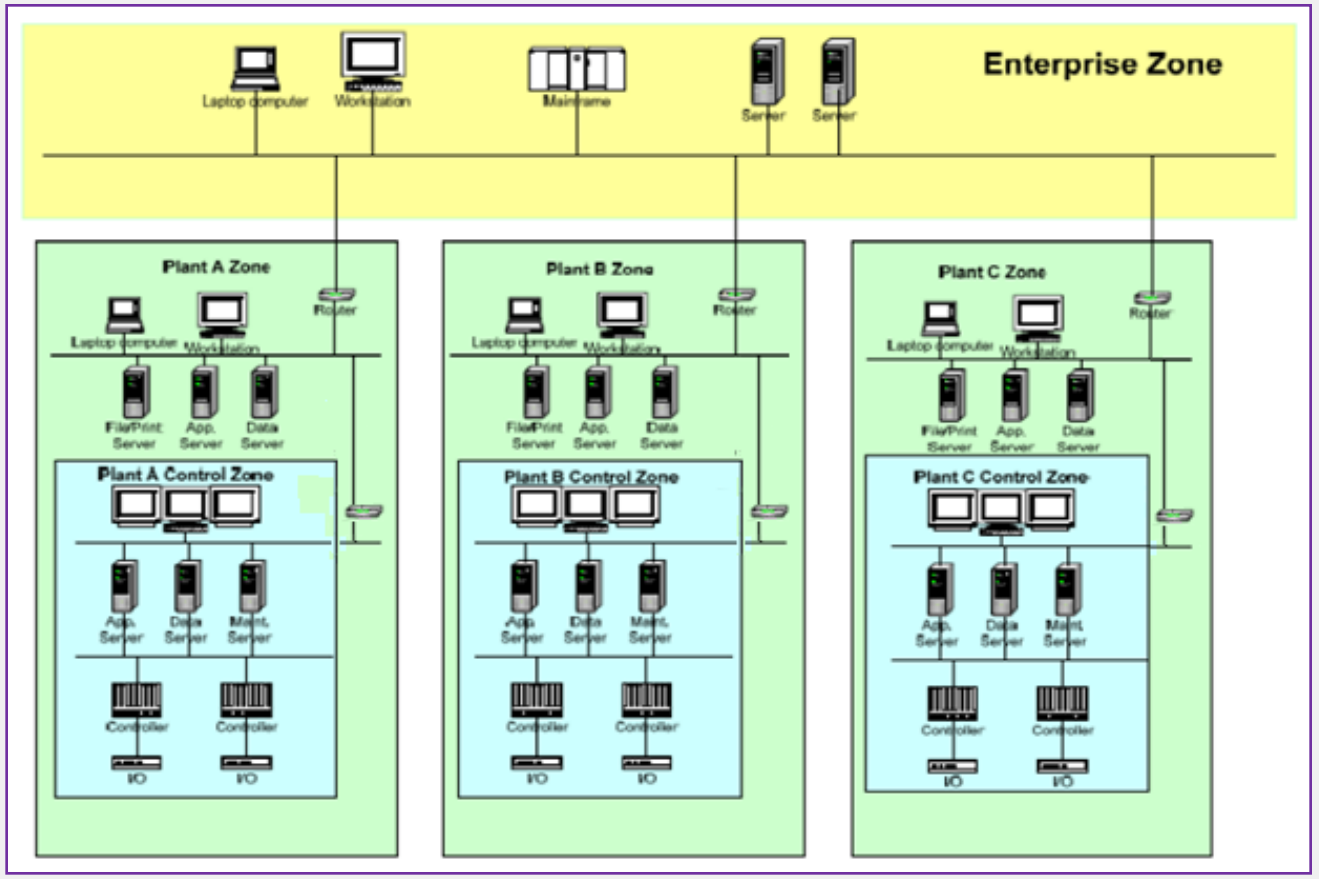
・情報システム部が工場と相談して、セキュリティ機能をもった**高機能のネットワークスイッチを導入**
・しばらくして情報システムが現場に訪れると、全てのイーサネットのケーブルが、前に使用していたスイッチに戻っていたのを発見
・チョコ停の原因調査で、新しいスイッチに疑いがかかり、**一時的な処置（原因不明なので）のまま放置していた**

画像は再現イメージ

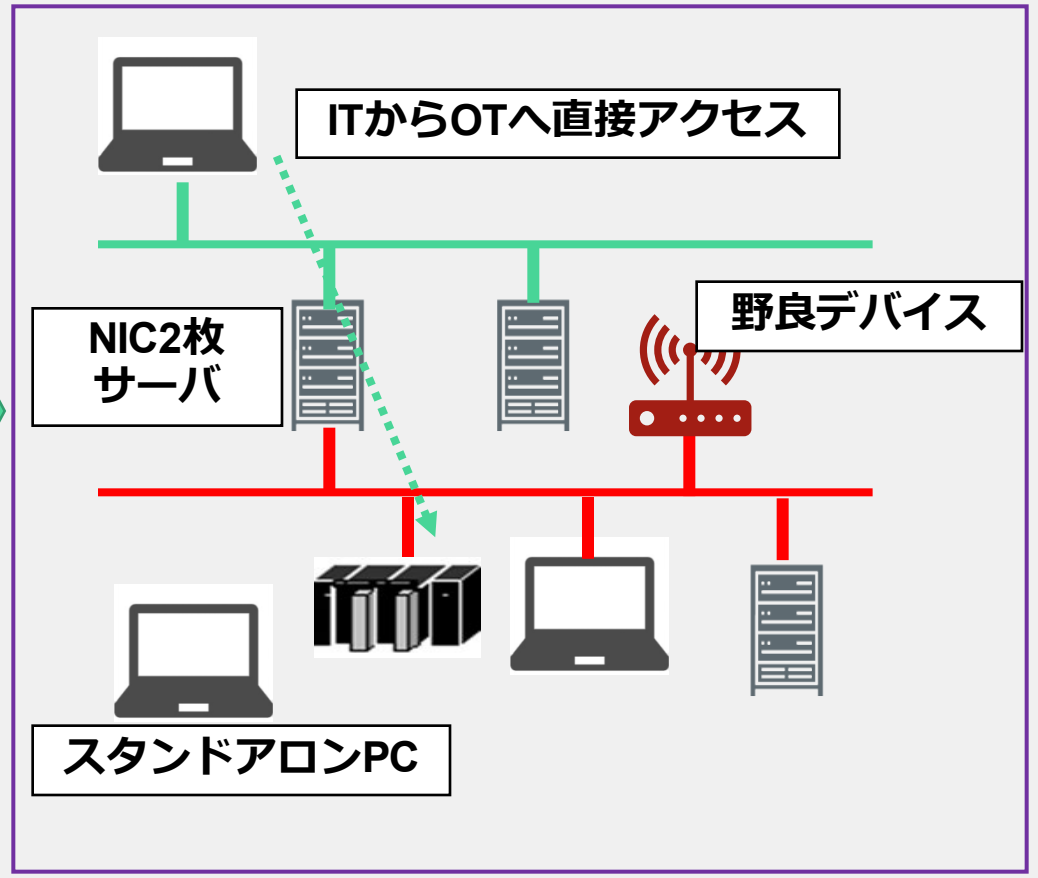
技術課題：OTネットワークがフラット＆野放し

Pe Pr Te

教科書的なOTネットワーク図



実際は・・・



誰もOTネットワークで何が起こっているか知らない

ガイドライン活用

経済産業省　工場セキュリティガイドライン公開（2022年11月）

☑ 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。

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　～全体概要～

ガイドラインの背景・目的

- 工場のIoT化によるネットワーク接続機会の増加に伴いサイバー攻撃リスクが増加。また、ネットワークの接続に乏しい工場であっても不正侵入者等による攻撃の可能性あり。
- 意図的な攻撃の場合もあれば、たまたま攻撃される場合もある。

→**いかなる工場でもサイバー攻撃のリスクあり**。

- 本ガイドは業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを示した「手引き」。

→**各業界・業種が自ら工場のセキュリティ対策を立案・実行**することで、**工場のセキュリティの底上げを図ることが目的**。

想定する読者の方

- ITシステム部門
- 生産関係部門（生産技術部門、生産管理部門、工作部門等）
- 戦略マネジメント部門（経営企画等）
- 監査部門
- 機器システム提供ベンダ、機器メーカ
  （サプライチェーンを構成する調達先を含む）

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。

対策に取り組む効果

- **工場のBC／SQDC※の価値がサイバー攻撃により毀損されることを防止**。
- セキュリティが担保されることでIoT化や自動化が進み、多くの工場から新たな付加価値が生み出されていくことを期待。

※ 安全確保(S：Safety)、
事業／生産継続(BC：Business Continuity)
品質確保(Q：Quality)
納期遵守・遅延防止(D：Delivery)
コスト低減(C：Cost)

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

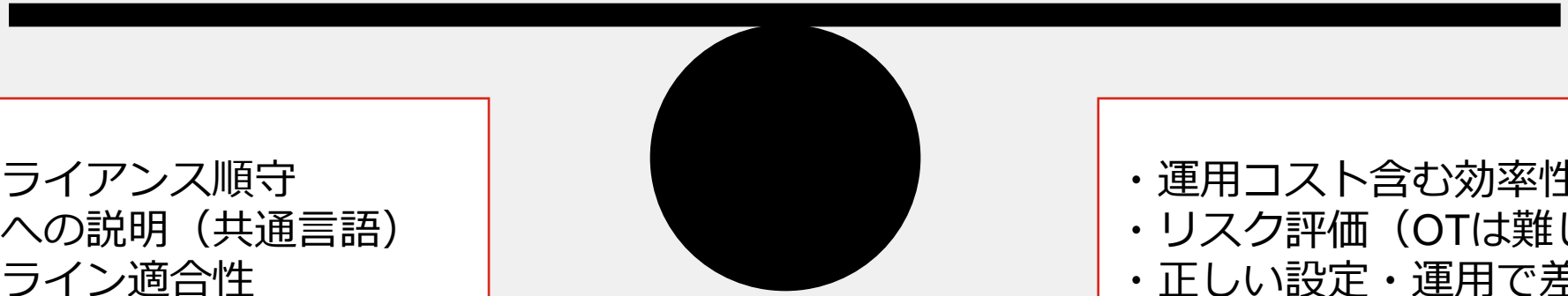
1

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

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！”

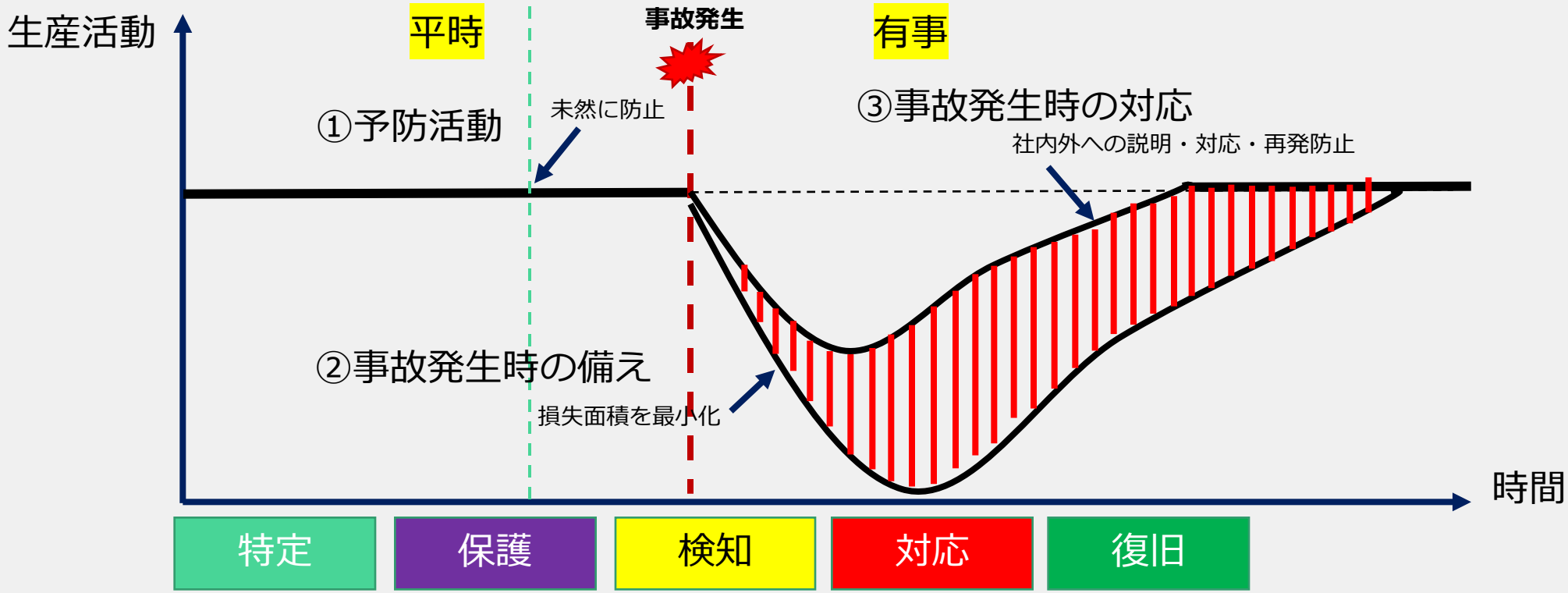
レジリエンスの考え方

「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

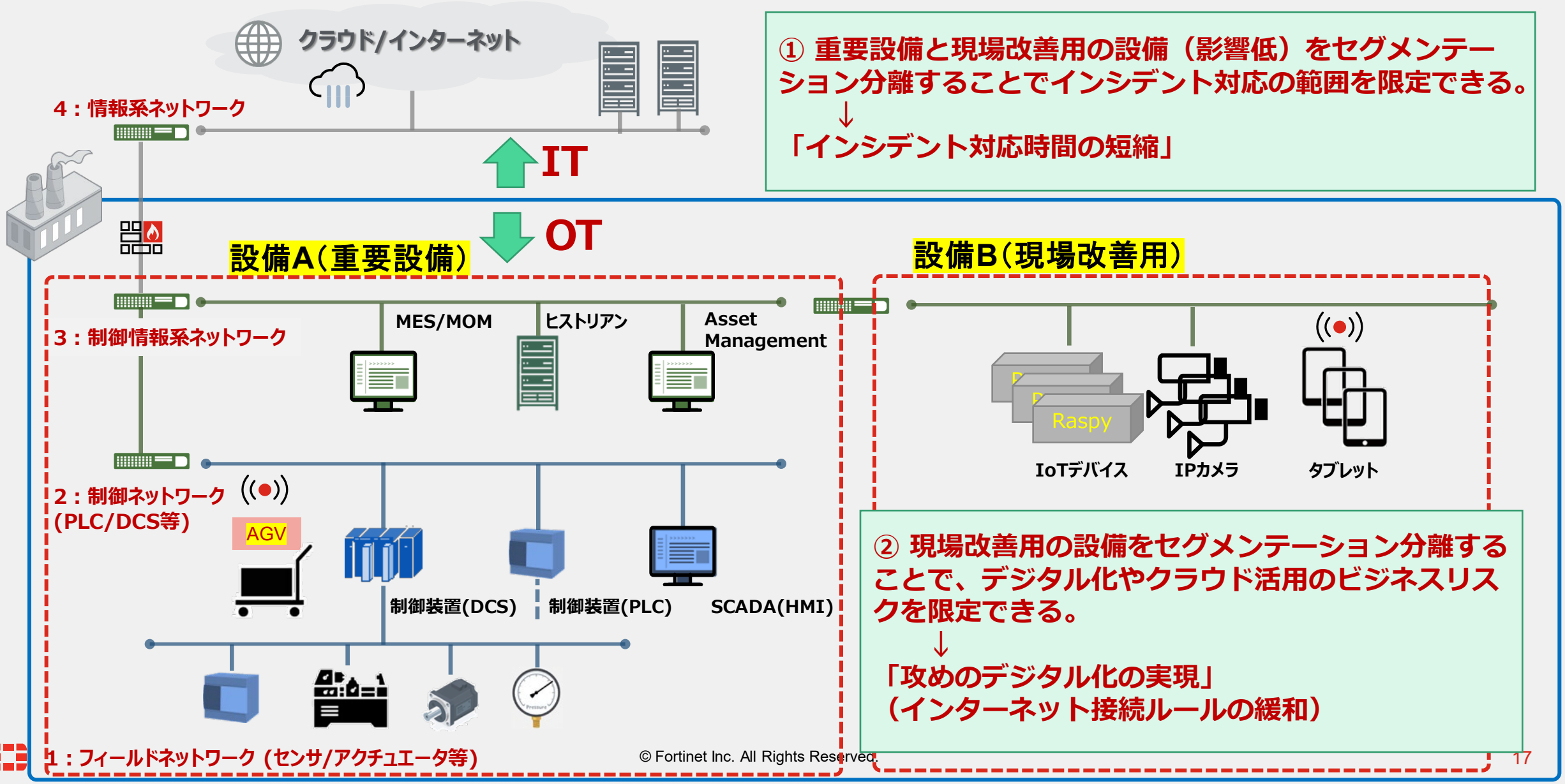
②セキュリティ事故発生時の備え

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

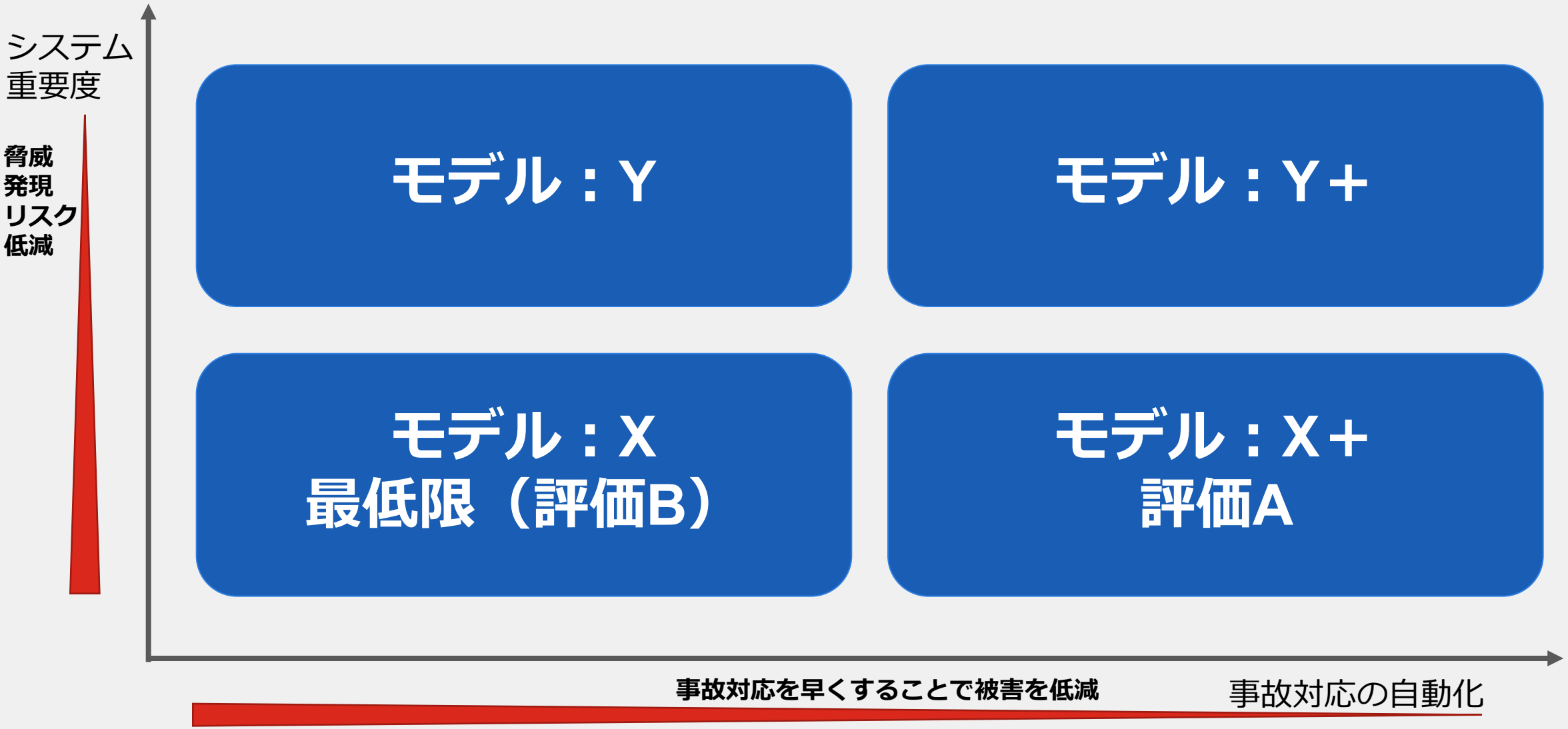
OTネットワークセグメンテーションの重要性



① 重要設備と現場改善用の設備（影響低）をセグメンテーション分離することでインシデント対応の範囲を限定できる。
↓
「インシデント対応時間の短縮」

② 現場改善用の設備をセグメンテーション分離することで、デジタル化やクラウド活用のビジネスリスクを限定できる。
↓
「攻めのデジタル化の実現」
（インターネット接続ルールの緩和）

重要度と緊急度に応じたセキュリティモデル分類図



OTセキュリティの技術的対策分類（例）

予防 ⟵ ⟶ 事故後

項目	特定	防御	検知	対応	復旧
エンドポイント	・資産管理ツール ・アクセス認証 ・権限最小化 ・端末FW	・アンチウィルス ・USB型アンチウィルス ・ホワイトリスト	・EDR	・EDR ・フォレンジックツール	・EDR
ネットワーク	・資産管理ツール **（OT-IDS）** ・ネットワークアクセス制御（NAC） ・アクセス認証 ・無線管理	・セグメンテーション ・ファイアウォール ・アンチウィルス ・IPS ・通信暗号化 ・SSL inspection ・**データダイオード**	・ネットワーク監視（L2/L3/L4） ・サンドボックス ・**OT-IDS** ・**デコイ（デセプション）**	・ネットワークアクセス制御（NAC） ・フォレンジックツール ・VLANによる隔離	
ログ収集・分析			・Syslogサーバー ・SIEM（相関分析） ・EDR	・SOAR ・EDR	・SOAR ・EDR
物理的対策	・入退管理システム ・IDカード認証 ・生体認証	・工場内入退管理（電子ゲート） ・建屋施錠管理 ・ラック施錠管理 ・ポート閉塞	・監視カメラ ・赤外線センサー		

#	モデル	SC	特定	防御	検知	対応	復旧
X	最低限の対策 （既知脅威対応） 評価[B]	端末	資産管理ツール （手動・定期的） 脆弱性管理ツール （手動・定期的）	USB型メモリAV（手動・定期的）or AV（定義ファイル更新頻度低） 端末FW 不要App削除・権限最小化			手動検疫(AV) バックアップ からの復旧 （手動）
		NW	無線接続管理	ネットワークアクセス制御(L2/L3/L4) セグメンテーション(Zone) 境界防御（IPS + SSL inspection） WAF(Web Application FW) 通信暗号化(VPN)・2要素認証 データダイオード	既知の脅威検知 （IDS + SSL inspection） WAF(検知のみ) ＊防御が可用性に よって難しい場合	ネットワークアクセス制御（NAC）隔離(手動)	
		ログ				Syslogサーバ NW機器ログ保存	
X+	既知脅威対応の 自動化 評価[A]	端末	資産管理/認証(Agent) （自動/リアルタイム） 脆弱性管理ツール(自動)	AV（定義ファイル更新頻度高） ホワイトリスト			
		NW	ネットワークアクセス制御（NAC）による資産管理	通信暗号化(VPN)・2要素認証	既知の脅威検知 （IDS + SSL inspection） WAF(検知のみ)	ネットワークアクセス制御（NAC）隔離（自動：検知連携）	
		ログ			NW機器ログ分析		
Y	既知＋未知の脅威 対応の対策	端末			EDR	EDR	EDR
		NW	OT-IDSによる資産管理 （脆弱性管理）		OT-IDS or デコイ or デセプション or サンドボックス	ネットワークアクセス制御（NAC）隔離（手動）	
		ログ			SIEM	SIEM	
Y+	既知＋未知の脅威 対応の対策自動化	端末					
		NW				ネットワークアクセス制御（NAC）隔離（自動：検知連携）	
		ログ			SIEM	SIEM/SOAR	SOAR

モデルX（評価B）の要求仕様詳細例

	機能	項目	機能詳細	備考
端末	資産管理ツール（手動・定期的）	**必須**	同一Zone内の資産（パソコンなど汎用OS含むもの）一覧（IP/MACアドレス/OSなど）を管理できる状態。	どこまで自動化するかは、台数と事故対応に許容される時間に依存。
	脆弱性管理ツール（手動・定期的）	推奨	Zone内の資産の脆弱性情報の定期的な収集・管理。	モデルXでは脆弱性対処の負荷が高すぎるため、実施する場合でも重要性高い端末のみ。
	脅威防御（手動・定期的）	**必須**	アンチウィルス等の既知の脅威に対して端末を保護する機能。手動でも良いので定期的に定義ファイルを更新する。	USB型AV、ホワイトリストでも良い。サポート切れOS、可用性重視端末には、NW仮想パッチなどリスク低減策を許容する。
	端末FW・不要App削除・権限最小化	**必須**	工場端末の端末FW、不要App削除・権限の見直しを手動で実施。新たな技術導入はなくて良い。	可用性に留意すること。
NW	無線接続管理	**必須**	無線安定稼働、未管理端末接続を防止する機能をもつこと。	無線機器そのものの管理も含む。
	セグメンテーション(Zone)	**必須**	VLANなどを用いて論理的に他のZoneと分離すること。物理的な分離でもよい。Zone間の通信には、境界防御（IPS）を行うこと。	工場内で、生産に重要なシステムと、そうでない補助的なシステムとはセグメンテーションによる分離が必須。
	境界防御 (IPS)	**必須**	NWアンチウィルス・IPS機能など、通信内容（第7層）レベルで、Zoneの境界を保護すること。	エンドポイントでの検知技術とは別のベンダー、方法であることが望ましい。
	境界防御 (SSL inspection)	推奨	Zoneの境界通信のHTTPS通信の中身についても、暗号化を解いて、境界防御(IPS)相当の処理を行うこと。	HTTPSの割合が多い(7割以上)工場は、実施を強く推奨する。通信元が証明書配布が可能な端末かどうか確認。可用性留意。
	ネットワークアクセス制御・隔離(手動)	**必須**	ネットワーク上の端末をコマンド等で隔離すること。他の防御・検知機能との連携はなしでもよい。	事故対応では、隔離までにかかる時間が重要。
ログ	エンドポイントログ保存	**必須**	Zone内の端末のアンチウィルスなどのログを定期的に収集して保存。分析まではしなくてよい。	保存場所は、Zone内でなくてもよい。他のZoneと共有でも構わない。
	ネットワークログ保存	**必須**	Zone内の境界防御等のネットワーク装置のログを定期的に保存。分析まではしなくてよい。	保存場所は、Zone内でなくてもよい。他のZoneと共有でも構わない。


FORTINET