

制御システムセキュリティカンファレンス2024(配布用資料)

製造業10社の実務者で議論した、 制御系SIRTが日常で取り組みたいインシデント対応訓練

大林 世昇

株式会社資生堂 情報セキュリティ部

2024年2月7日



本講演の内容については正確な記述、表現となるよう努めておりますが、
本講演および資料に基づく運用結果について、株式会社資生堂および講
演者は一切の責任を負いかねますのでご了承ください。

自己紹介

大林世昇 OBAYASHI Tokinori

【これまでに担当してきた業務・領域の例】

- 仮想化基盤サーバ構築、オペレーション改善
- ドメインネームを軸としたサイバー空間でのブランドレピュテーション保護に関する運用、アドバイザー
- **国内新工場の建設プロジェクト（ITインフラネットワーク/次世代工場セキュリティ領域）**
- セキュリティオペレーション改善、向上に向けた企画立案、実行
- **工場セキュリティ基本指針の立案、実行マネジメント**
- **セキュリティアセスメント**
- 主要リスク指標（資生堂KRI)の設計、サイバーリスクの定量的評価と脅威予兆に関する分析
- インシデント対応訓練/教育の企画、制作、実行
- ダークウェブを含めたサイバー脅威モニタリング、ブランドレピュテーション保護
- 技術的なセキュリティ対策の動向調査、製品選定
- 社内エグゼクティブ/ステークホルダー向けドキュメンテーション、プレゼン

【資格】

CISSP、情報処理安全確保支援士、個人情報保護士など

OUR MISSION is BEAUTY INNOVATIONS FOR A BETTER WORLD

世界で勝てる日本発の グローバルビューティーカンパニーへ

私たちは、企業使命を「BEAUTY INNOVATIONS FOR A BETTER WORLD(美の力でよりよい世界を)」と定めています。

1872年の創業以来、約150年にわたって、常に「美」とともに歩み続けてきました。そのような私たちだからこそできるビューティービジネスの革新によって、企業としての成長はもちろん、社会課題の解決や、世界中の人々が幸せになるサステナブルな社会の実現をめざしています。



本講演の構成、取り扱うテーマ

JPCERT/CCと活動していた「製造業のICS(*)セキュリティ担当者コミュニティ」の中で、インシデント対応訓練に特化したワーキンググループを立ち上げ。

➡ これまでのワーキンググループの活動や成果物のご紹介、情報共有

(*)ICS:Industrial Control System,産業用制御システム

1. イントロダクション：約10分

- 本講演で使用する用語、Appendixについて
- 資生堂の生産拠点、工場セキュリティに関する取り組み等
- 本講演の背景となっているワーキンググループ活動 -立ち上げ
- 本講演の背景となっているワーキンググループ活動 -議論と成果物

2. パネルディスカッション：約20分

- ワーキンググループ参加メンバーとの対談を通して活動の詳細を共有

本講演の構成、取り扱うテーマ

JPCERT/CCと活動していた「製造業のICS(*)セキュリティ担当者コミュニティ」の中で、インシデント対応訓練に特化したワーキンググループを立ち上げ。

➡ これまでのワーキンググループの活動や成果物のご紹介、情報共有

(*)ICS:Industrial Control System,産業用制御システム

1. イン트로ダクション：約10分

- 本講演で使用する用語、Appendixについて
- 資生堂の生産拠点、工場セキュリティに関する取り組み等
- 本講演の背景となっているワーキンググループ活動 -立ち上げ
- 本講演の背景となっているワーキンググループ活動 -議論と成果物

2. パネルディスカッション：約20分

- ワーキンググループ参加メンバーとの対談を通して活動の詳細を共有

本講演で使用する用語、Appendixについて

本講演/資料で使用する用語

- **FSIRT**（Factory Security Incident Response Team）：
工場/生産現場で発生する生産設備に影響を及ぼすセキュリティインシデントを主として扱うチーム。本講演内では、「**制御系SIRT**」と同義で使用します。
- **工場セキュリティIR訓練**：
工場セキュリティ**インシデントレスポンス訓練**の略。

配布資料Appendixにて共有予定のWG成果物に関して

- 工場セキュリティIR訓練シナリオ素材案
- 成熟度セルフチェックシート

資生堂の生産拠点、工場セキュリティに関する取り組み等



【工場セキュリティに関する活動例】

- 工場長向けトップレクチャー、現地訪問による連携強化活動の方針に関する調整
- 工場セキュリティアセスメント
- 工場メンバーとの月次定例会
- 工場セキュリティIR訓練
- 直接材のお取引先さまに対するセキュリティ対策状況確認

工場セキュリティIR訓練実施後アンケートの結果

2022年度工場セキュリティインシデントレスポンストレーニング 受講後アンケート

この度は情報セキュリティ部主催の工場セキュリティIRにご参加頂きまして、誠にありがとうございました。今後、他工場も含め、実施を継続していきたく考えています。今年度受講された皆さまのご意見が今後の演習に反映されますので、ぜひとも、忌憚ないご意見をお伺いできますと幸いです。

質問No.	質問	回答
1	演習の進め方に関して、不明点なくスムーズに実施いただけましたか？	選択
2	状況付与ごとに5分間の検討時間を設定しました。時間の長さはいかがでしたか。	選択
3	2で「ちょうど良い」以外の回答の場合のみ回答)何分程度に設定すると、演習がより効果的に実施できましたでしょうか？(自由記述)	自由記述
4	今回の演習で新たな学び、気づきはありましたか。もしあれば具体的に記載をいただけると幸いです。(自由記述)	記述
5	今回の演習シナリオ/設定はいかがでしたか。シナリオが実際に所属工場内で発生しそうな、内容を理解しやすかったか、対応の検討にあたって別の情報も追加が必要だった等、自由に記載ください。 ○シナリオ:製造部門が臨時で設置したPLC管理端末リモート保守環境からの不正侵入およびサイバー攻撃による生産設備の停止と停代金要求への初期対応。	記述
6	もし今、実際に工場でサイバー攻撃が発生したら、体制面・技術面・運用プロセス面を踏まえて、十分に対応できると思いますか？さらに運用整備や演習が必要と思われますか。(自由記述)	記述
7	貴工場内でサイバー攻撃が発生した場合の対応に関して、課題・問題は何かと感じておられますか？(自由記述)	記述
8	リスクマネジメント部が発行している、「インシデントマネジメントガイドライン」はご存じでしたか？	選択
9	全工場を担当している、リスクマネージャの存在をご存じでしたか？	選択
10	今回実施したようなインシデント対応演習をまた受講したいと思いませんか？定期的に受講したいと思われる場合は、どの程度の間隔をあけて受講したいですか。(例:1年ごと/自由記述)	記述
11	その他、今回の演習に関しての感想、情報セキュリティ部へのご要望などを自由に記載頂けます。今後のコンテンツ制作、改善に活用させていただきます。(自由記述)	記述
受講後アンケートは以上です。この度は演習受講、アンケートのご回答頂きまして誠にありがとうございました。引き続きどうぞよろしくお願いいたします。ご安全に！		

【受講後アンケートより抜粋】

- HQで策定している、インシデント対応ガイドラインの認知度が低かった
- 各状況の検討時間を5分間で設定したが、やや不足（想定以上に盛り上がった。状況付与ごとに7～10分程度欲しいという回答が多かった）
- 「今後も異なるシナリオで、半年もしくは1年ごとなど定期的に受講したい」との回答：100%**

IR訓練をゼロから準備するのは、大変

自助・共助・公助

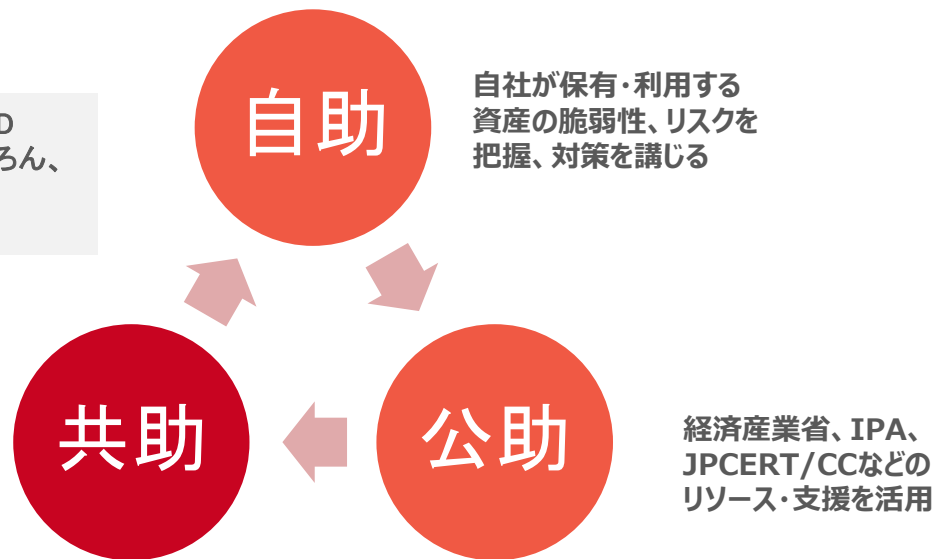
【再掲】Security Days Spring 2023 資生堂講演資料

今後、さらに他企業・製造業のセキュリティご担当の皆さまとの連携強化を図りたい

もはや「自社」だけでは、ビジネスの安定的な継続は困難。各社の経験や、脅威情報など互いに持ち寄り、日本全体でセキュリティレベル向上を目指したい。

企業使命「BEAUTY INNOVATIONS FOR A BETTER WORLD
(美の力でよりよい世界を)」のもと、企業としての成長はもちろん、
社会課題の解決や世界中の人々が幸せになる
サステナブルな社会の実現をめざしています。

企業の枠を超えて、
互いに情報や知恵を共有しあい、
全体のレベルを高める



いざ、有言実行・・・

本講演の背景となっているワーキンググループ活動 - 立ち上げ FSIRT訓練やろうの会

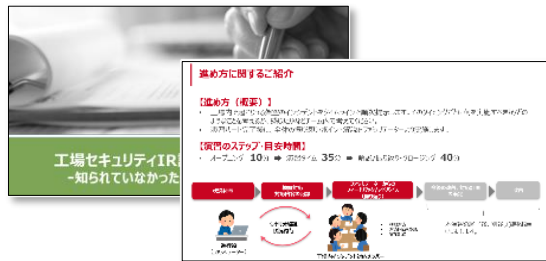
- ・ JPCERT/CCのもとで活動していた、**製造業のICS（制御システム）セキュリティ担当者コミュニティ**内で立ち上げ
- ・ 各社の経験や、各社で観測された脅威情報など互いに持ち寄り、日本全体としてのセキュリティ対策レベル向上を目指す
- ・ 企業の枠を超えて、互いに情報や知恵を共有しあい、**工場セキュリティ実務者間の連携、コミュニケーションを強化**する
- ・ 社会全体で工場に関するSIRT活動をより活性化するための、発信活動（本講演など）
- ・ **製造現場を持つ事業会社からの意見・知見を盛り込んだ、日常の中で容易に取り組むことができるIR訓練を提案**

2023年						2024年		
7月	8月	9月	10月	11月	12月	1月	2月	3月
WG立ち上げ 情報収集・調査		シナリオ検討、モデル作成				制御系システムセキュリティ カンファレンス2024		
		レビュー、ブラッシュアップ						
		✓ Meeting (オンライン×2)	✓ Meeting (オンサイト×1、 ハイブリッド×1)	✓ Meeting (オンライン×2)	✓ Meeting (個別各社複数)	✓ Meeting (オンライン×2)		

本講演の背景となっているワーキンググループ活動 – 議論と成果物

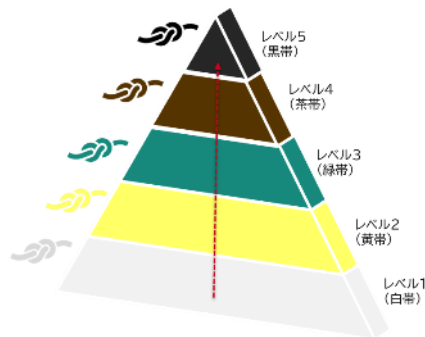
FSIRT訓練やろうの会

①工場セキュリティIR訓練シナリオ素材案



- ✓ WG内での議論も踏まえ、いくつかの代表的なシナリオ素材を作成
- ✓ 各社がすぐに使用できるように、IR訓練投影スライド案としてご提供
- ✓ 演習後の解説用スライドもセットでご提供
- ✓ 固有名詞などは各社で適宜カスタマイズして使用してください

②工場セキュリティIR訓練演習後 成熟度セルフチェックシート



- ✓ 工場IR訓練を、日々の活動の中で、定期的に繰り返し取り組むことが重要
- ✓ 自らの状況・レベルアップ目標をより判り易く確認できるように、重要な項目と達成度を5段階で提示（白帯～黒帯）
- ✓ 各社の業種、成熟度などに応じてカスタマイズして使用してください

※上記の成果物共有については本講演の収録時点における計画であり、実際の配布資料で提供される内容は予告なく変更となる場合があります。あらかじめご了承ください。

[イントロダクションパートまとめ] 工場セキュリティIR訓練のススメ

IR訓練シナリオ/物語を考える際の視点の例



- ✓ 未来を読み切れない中で、様々なリスクとその発生可能性を予想し、事前にステークホルダーと対応方針を想像、シミュレーションする
- ✓ 未来の不確実性をマネジメントするための手法のひとつとして、机上訓練を積極的に取り入れる
- ✓ **描いたシナリオに演習参加者を没入させるための工夫（未来を描いた短編動画や新聞記事etc.）**
- ✓ 起こりうるサイバー攻撃のストーリーを、現場をよく理解した実務者が考えることによりもたらされる価値
- ✓ 「いつかやってくる」に備える、平時の取り組み



本講演の構成、取り扱うテーマ

JPCERT/CCと活動していた「製造業のICS(*)セキュリティ担当者コミュニティ」の中で、インシデント対応訓練に特化したワーキンググループを立ち上げ。

➡ これまでのワーキンググループの活動や成果物のご紹介、情報共有

(*)ICS:Industrial Control System,産業用制御システム

1. イントロダクション：約10分

- 本講演で使用する用語、Appendixについて
- 資生堂の生産拠点、工場セキュリティに関する取り組み等
- 本講演の背景となっているワーキンググループ活動 -立ち上げ
- 本講演の背景となっているワーキンググループ活動 -議論と成果物

2. パネルディスカッション：約20分

- ワーキンググループ参加メンバーとの対談を通して活動の詳細を共有

パネルディスカッション：

工場セキュリティに関する各社、WGの取り組み共有

FSIRT訓練やろうの会（全10社）

代表参加者3名の所属企業

SHISEIDO



株式会社資生堂

SEKISUI



積水化学工業株式会社

Panasonic
AUTOMOTIVE



パナソニック オートモーティブシステムズ
株式会社

本パネルディスカッションアジェンダ

(1) 各社ご紹介

- パナソニック オートモーティブシステムズ株式会社
- 積水化学工業株式会社

(2) 各社xSIRT体制

(3) 各社xSIRT活動(FSIRT)

(4) WGでの議論共有

- 平時のFSIRT活動における大切な4つの要素
- 工場セキュリティIR訓練シナリオ案
- 成熟度セルフチェックシート

(5) まとめ



本パネルディスカッションアジェンダ

(1) 各社ご紹介

- ・ パナソニック オートモーティブシステムズ株式会社
- ・ 積水化学工業株式会社

(2) 各社xSIRT体制

(3) 各社xSIRT活動(FSIRT)

(4) WGでの議論共有

- ・ 平時のFSIRT活動における大切な4つの要素
- ・ 工場セキュリティIR訓練シナリオ案
- ・ 成熟度セルフチェックシート

(5) まとめ



会社概要と組織体制

社名	パナソニック オートモーティブシステムズ株式会社
所在地 (本社)	〒224-8520 横浜市都筑区池辺町4261番
設立	2022年4月1日
事業 内容	車載コックピットシステム、ADAS(先進運転支援システム) および関連デバイス、車載充電器、xEV向けシステム・デバイス などの開発・製造・販売



電車：JR横浜線「鴨居」駅（北口）徒歩約10分

タクシー：「新横浜」駅より約15分

パナソニック オートモーティブシステムズ(株)

開発本部

営業本部

事業部

インフォテインメントシステムズ事業部

IVI(イン・ビークル・インフォテインメント)、ディスプレイ・オーディオ、カーナビゲーション等の車載インフォテインメントシステムの開発・製造・販売

HMIシステムズ事業部

車載ディスプレイ、スピーカー、スイッチ・センサ等の視覚・聴覚・触覚をつなぐ車室内のデバイス・モジュールの開発・製造・販売

車載システムズ事業部

ADAS(先進運転支援システム)、ETC車載器、電動コンプレッサ、シート/ステアリングヒーター等のデバイス・システムの開発・製造・販売

フィコサ・インターナショナル(株)

リアビューシステム（ドア/ルームミラー、カメラモニタリング）、カメラ、シフター、ヘッドランプウォッシャー等のデバイス・システムの開発・製造・販売

パナソニックグループにおける位置づけ

パナソニック ホールディングス株式会社

パナソニック
株式会社



パナソニック
オートモーティブ
システムズ株式会社



パナソニック
エンターテインメント
& コミュニケーション
株式会社



パナソニック
ハウジング
ソリューションズ
株式会社



パナソニック
コネクト株式会社



パナソニック
インダストリー
株式会社



パナソニック
エナジー
株式会社



パナソニック
オペレーショナル
エクセレンス
株式会社

パナソニック ホールディングス株式会社
執行役員

プライムプラネットエナジー & ソリューションズ(株)担当

パナソニック オートモーティブシステムズ株式会社

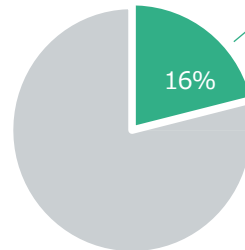
代表取締役 社長執行役員 CEO

永島 正吏



パナソニックグループにおける
オートモーティブセグメントの売上構成 (2022年度)
1兆2,975億円

※オートモーティブセグメントに含まれる事業



グループ連結 約8兆3,789億円

車載コックピットシステム

インフォテインメント

車載エレクトロニクス

HMIシステムズ
車載システムズ
FICOSA

ミッション

一人ひとりのより良い暮らしの実現のため、
持続可能なモビリティ社会を創造する

ビジョン

愛をもって人に寄り添い、
卓越した技術と知恵で新たなユーザー価値を創造し、
より快適で安心安全な移動空間の実現により、
人に幸せをもたらし続ける
最高のチーム、最高のパートナーになる

スローガン

Heartmotive ～こころ動かす出会いを創り続ける～

いつの時代もどこにいても、人は移動し、多くの人
やささまざまな感動に出会います。私たちは、人に
寄り添い、一人ひとりにストレスフリーな移動を実
現したい、それにより「こころ動かす出会い」を創り
続けていきたい。そんな思いを「Heartmotive」
というスローガンに込めて、事業活動に取り組ん
でいきます。



社 名

積水化学工業株式会社 (SEKISUI CHEMICAL CO., LTD.)

設 立

1947年3月3日

資 本 金

1,000億円

代 表 者

代表取締役社長 加藤敬太

従 業 員 数

26,838名 (2023年3月末日現在)

売 上 高

12,425億円 (2023年3月期連結ベース)

経 常 利 益

1,042億円 (2023年3月期連結ベース)

本 社

大阪本社

〒530-8565 大阪市北区西天満2丁目4番4号

東京本社

〒105-8566 東京都港区虎ノ門2丁目10番4号

U R L

<https://www.sekisui.co.jp/>



大阪本社



東京本社

グループビジョン

際立つ技術と品質により、「住・社会のインフラ創造」と「ケミカルソリューション」の
フロンティアを開拓し続け、世界のひとびとの暮らしと 地球環境の向上に貢献する

住・社会のインフラ創造

住まい

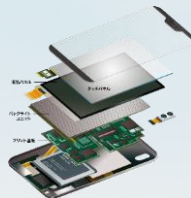


インフラ



ケミカルソリューション

高性能素材



健康・医療



新事業
(エネルギー・資源循環)

SEKISUI



高付加価値材料で、社会・暮らしを進化させるさまざまな機器の発展を支える



エレクトロニクス



モビリティ



インダストリアル

□ スマートフォン

- #タッチパネルを支える導電性微粒子
- #高透明両面テープ

□ 半導体

- #接合材用途向け、独自のエポキシ系材料
- #高接着・易剥離材料

□ 自動車

- #合わせガラス用中間膜
- #内外装向け発泡体・成形品
- #電動化、自動運転デバイス向け放熱材
電磁波対策材

□ 航空機、ドローン

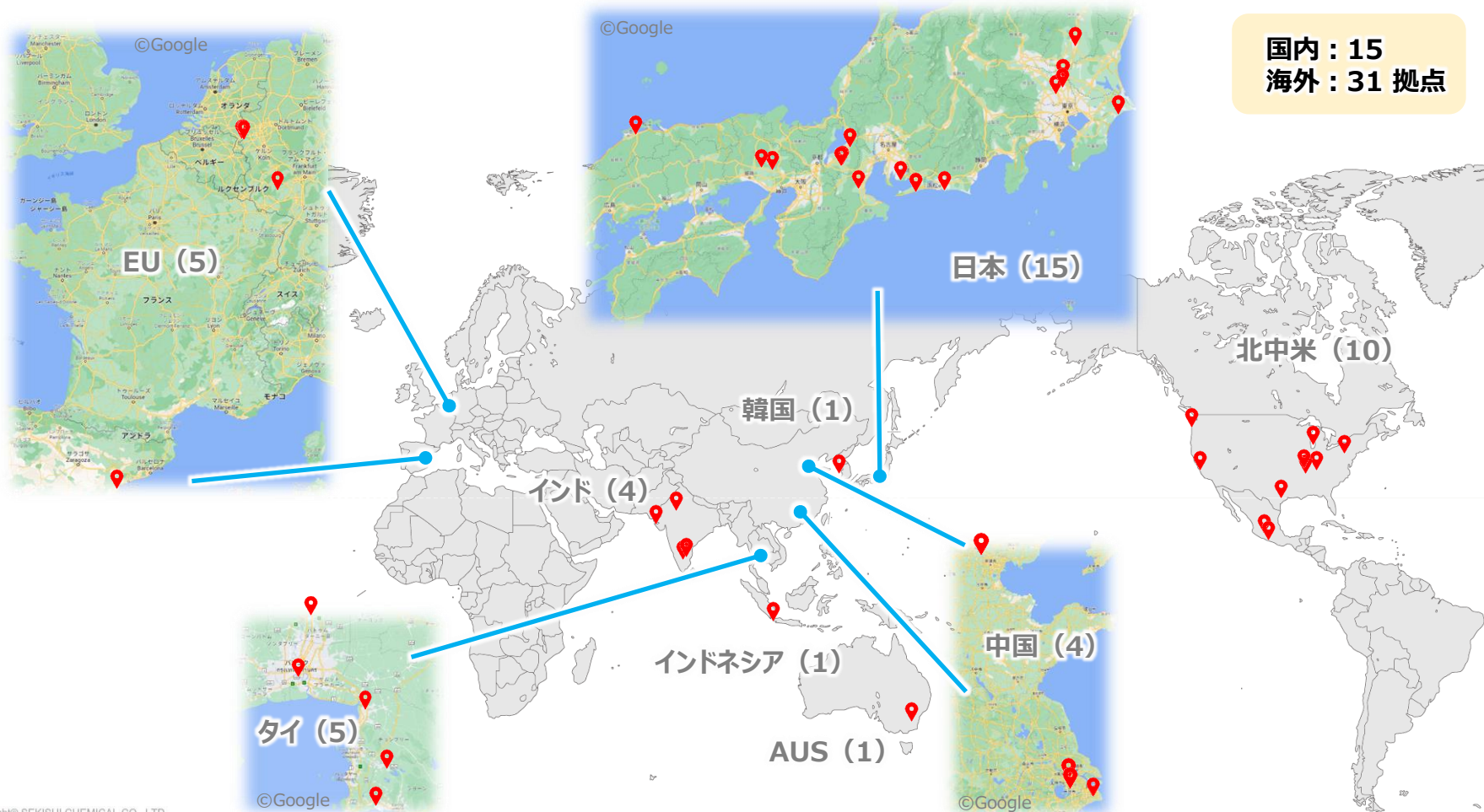
- #炭素繊維強化プラスチック 成形品
- #座席用プラスチックシート

□ 暮らし

- #見守りセンサー「ANSIEL」
- #ケアマテリアル
- #樹脂畳（MIGUSA）

□ 産業

- #包装用テープ
- #再生プラスチック製コンテナ



本パネルディスカッションアジェンダ

(1) 各社ご紹介

- パナソニック オートモーティブシステムズ株式会社
- 積水化学工業株式会社

(2) 各社xSIRT体制

(3) 各社xSIRT活動(FSIRT)

(4) WGでの議論共有

- 平時のFSIRT活動における大切な4つの要素
- 工場セキュリティIR訓練シナリオ案
- 成熟度セルフチェックシート

(5) まとめ



様々なSIRTの形態と主なスコープと活動内容の例

		主に扱う範囲（スコープ）	主な活動
	CSIRT (Computer Security Incident Response Team)	組織内の業務運営に用いる コンピュータやネットワークといった情報システム の安定稼働とそこで取り扱われる情報保護を対象として、セキュリティ・インシデントに対処する。 (設置：情報システム部門等)	- インシデントの原因分析、影響調査、問題への対応、復旧活動 - 経営層を含め社内外のステークホルダーへの報告、連絡窓口 - 平時には脆弱性対応、アウェアネストレーニング、注意喚起など
	PSIRT (Product Security Incident Response Team)	顧客に販売されネットワークに接続された製品 および顧客の安全確保・情報保護を対象として、セキュリティ・インシデントに対処する。(設置：事業部門ごとに、製品開発や品質管理を担う部署と連携する部署として等)	- CSIR訓練と分担・連携しつつ、製品に係る原因分析や影響範囲の調査、問題への対応、復旧 - 製品の顧客へのパッチ提供や対策支援等の脆弱性対応 - 活動の際には、製品開発や品質管理を担う部署と協調
	FSIRT (Factory Security Incident Response Team)	自社の工場や生産ライン の安定稼働や作業員の安全確保の為に、サイバー攻撃の監視・対応を行う。(設置：生産管理部門等)	CSIR訓練と分担・連携しつつ、工場内で発生したインシデントの原因分析や影響範囲の調査、問題への対応、復旧
	DSIRT (Digital Service Security Incident Response Team)	顧客が利用するデジタル・サービス の継続的提供・品質維持および顧客の資産保護・情報保護を対象として、セキュリティ・インシデントに対処する。(設置：デジタル・サービスを提供する事業部門と横並びの独立部署、各事業部門のセキュリティ担当を集めたバーチャル組織等)	- デジタル・サービスに係る原因分析や影響範囲の調査、問題への対応、復旧 - サービス企画時のサービスリスク分析、サービスの不正を検知する監視ロジックの設計・更新支援、大規模サービスインシデント発生時の対応

資生堂におけるSIRT体制



CSIRT

(Computer Security Incident Response Team)

主に取り扱う範囲（スコープ）

組織内の業務運営に用いる**コンピュータやネットワークと
いった情報システム**の安定稼働とそこで取り扱われる情報
保護を対象として、セキュリティ・インシデントに対処する。
（設置：情報システム部門等）

主な活動

- インシデントの原因分析、影響調査、問題への対応、復旧活動
- 経営層を含め社内外のステークホルダーへの報告、連絡窓口
- 平時には脆弱性対応、アウェアネストレーニング、注意喚起など



FSIRT

(Factory Security Incident Response Team)

自社の工場や生産ラインの安定稼働や作業員の安全
確保の為に、サイバー攻撃の監視・対応を行う。（設
置：生産管理部門等）

- CSIR訓練と分担・連携しつつ、工場内で発生したインシデントの原因分析や影響範囲の調査、問題への対応、復旧

The screenshot shows the Nippon CSIRT Association website. The main heading is "Shiseido CSIRT". Below it, there is a table with the following information:

チームの正式名称	資生堂シーサート
チームの略称	Shiseido CSIRT
所属する組織名	株式会社 資生堂
設立年月日	2016年7月1日
チームの Email アドレス	nca.shiseido.csirt@to.shiseido.co.jp
チームサイト	
所属組織サイト	http://www.shiseidogroup.jp/inquiry?rt_bt=manu-inquiry_001
加盟年月	2017 年 03 月

Shiseido CSIRT (資生堂シーサート)

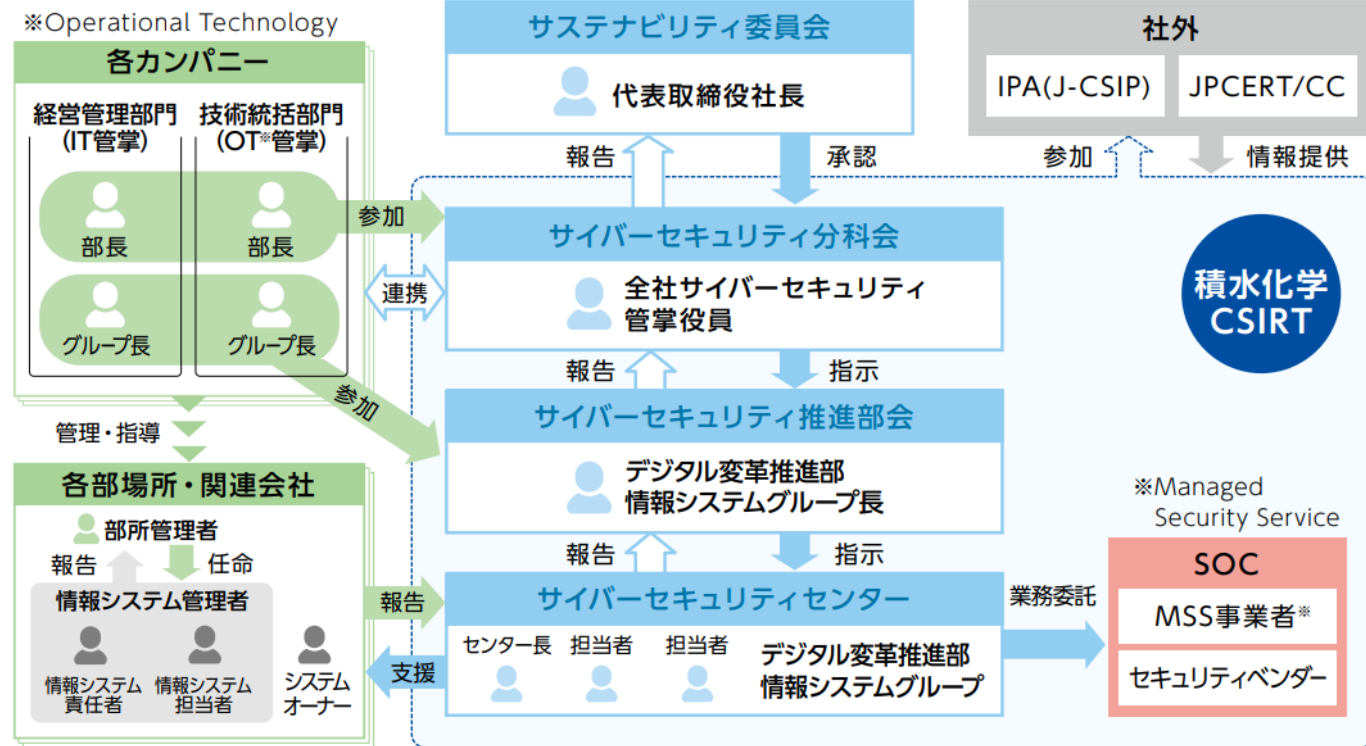
- 設立年月日： 2016年7月1日
- 加盟年月： 2017年3月

【参考出所】「DX with Cybersecurity実践に向けた人材の確保、育成、活躍促進に係る主な政策課題と方向性」
(2021年6月2日 サイバーセキュリティ戦略本部 普及啓発・人材育成専門調査会)
https://www.nisc.go.jp/pdf/council/cs/jinzai/dai15/jinzai_houkousei.pdf

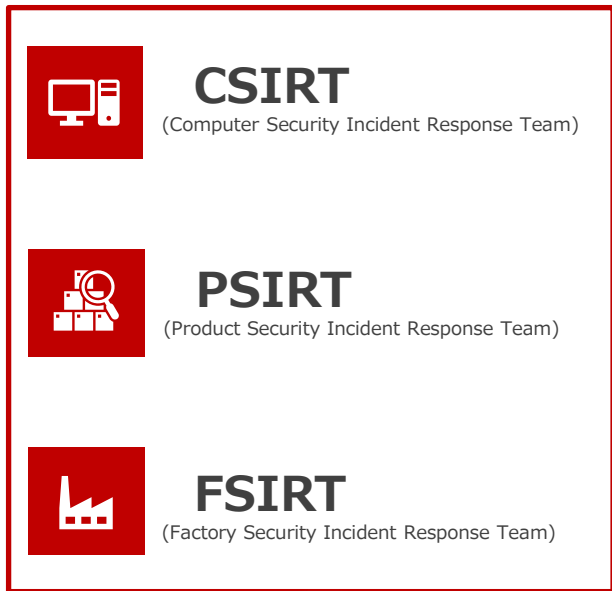
【参考出所】一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会 会員（チーム）情報 Shiseido CSIRT
<https://www.nca.gr.jp/member/shiseido-csirt.html>

積水化学グループでは、コーポレート主導によりCSIRT体制を定めています。サイバーインシデント発生時は管理体制に沿って対応と報告を実施します。

管理体制の全体像



様々なSIRTの形態と主なスコープと活動内容の例



主に扱う範囲（スコープ）

組織内の業務運営に用いる**コンピュータやネットワーク**といった**情報システム**の安定稼働とそこで取り扱われる情報保護を対象として、セキュリティ・インシデントに対処する。
(設置：情報システム部門等)

顧客に販売されネットワークに接続された製品および顧客の安全確保・情報保護を対象として、セキュリティ・インシデントに対処する。(設置：事業部門ごとに、製品開発や品質管理を担う部署と連携する部署として等)

自社の工場や生産ラインの安定稼働や作業員の安全確保の為に、サイバー攻撃の監視・対処を行う。(設置：生産管理部門等)

顧客が利用する**デジタル・サービス**の継続的提供・品質維持および顧客の資産保護・情報保護を対象として、セキュリティ・インシデントに対処する。
(設置：デジタル・サービス部門ごとに、サービス開発や品質管理を担う部署と連携する部署を集めたバーチャル組織等)

主な活動

- インシデントの原因分析、影響調査、問題への対応、復旧活動
- 経営層を含め社内外のステークホルダーへの報告、連絡窓口
- 平時には脆弱性対応、アウェアネストレーニング、注意喚起など

- CSIRTと分担・連携しつつ、製品に係る原因分析や影響範囲の調査、問題への対応、復旧
- 製品の顧客へのパッチ提供や対策支援等の脆弱性対応
- 活動の際には、製品開発や品質管理を担う部署と協調

- CSIRTと分担・連携しつつ、工場内で発生したインシデントの原因分析や影響範囲の調査、問題への対応、復旧

- デジタル・サービスに係る原因分析や影響範囲の調査、問題への対応、復旧
- サービスのリスク分析、サービスの不具合の調査・原因分析、サービスの設計・更新支援、大規模サービスインシデント発生時の対応

セキュリティ活動・SIRTを統括

電動化、通信ネットワーク接続、自動運転など、
ほとんどの機能をソフトウェアで実装する「走るコンピュータ」に
⇒クルマのライフサイクルを通じてサイバーセキュリティが大きな課題に

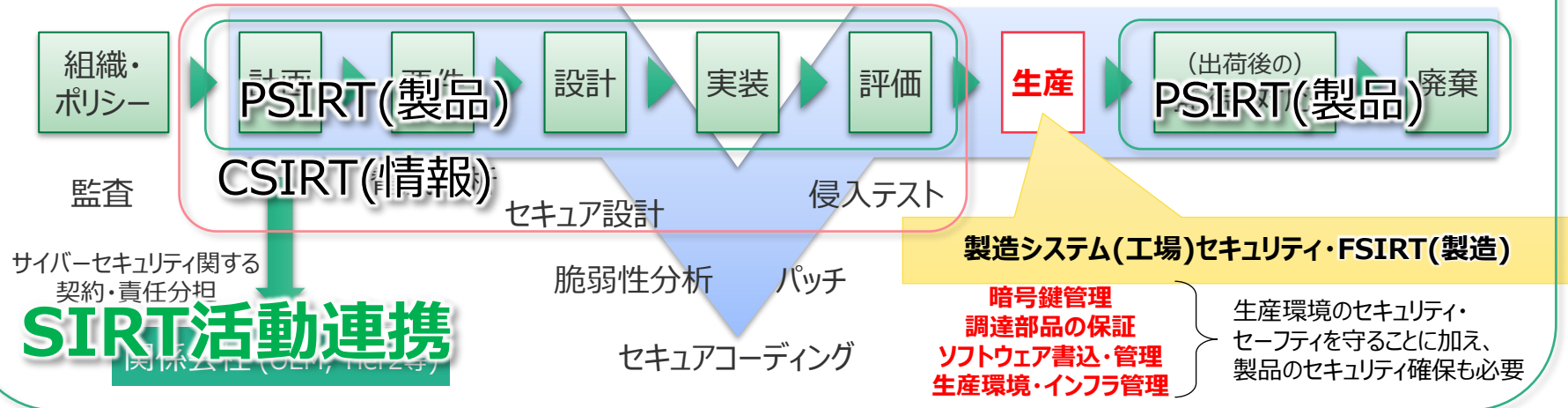
- SDV (Software Defined Vehicle) あらゆる機能をソフトウェア実装
- ECU (Electronic Control Unit) 分散制御から統合システム・ソフトウェアへ
- CASE (Connected, Autonomous, Shared & Service, Electrification)
ネットワーク接続、自動化、サービス化、電動化

UN-R155(車載サイバーセキュリティ国際法規)及び、各国関連法の遵守義務

- 日本では「道路運送車両法」(国土交通省)に組み込まれ、既に施行
- 国際規格ISO/SAE21434に基づくサイバーセキュリティマネジメントシステム(CSMS)構築が基本要件
- カーメカ・サプライヤは、これら法規・規格に準じたサイバーセキュリティ施策が必要

ライフサイクル全体(企画～廃棄)においてセキュリティレベルを維持

社内インフラ環境や、サプライチェーン管理を含む、一貫したサイバーセキュリティマネジメントシステム(CSMS)



本パネルディスカッションアジェンダ

(1) 各社ご紹介

- パナソニック オートモーティブシステムズ株式会社
- 積水化学工業株式会社

(2) 各社xSIRT体制

(3) 各社xSIRT活動(FSIRT)

(4) WGでの議論共有

- 平時のFSIRT活動における大切な4つの要素
- 工場セキュリティIR訓練シナリオ案
- 成熟度セルフチェックシート

(5) まとめ



資生堂：工場セキュリティ強化に関する活動

2021年から工場セキュリティアセスメントの取り組みを新規に立ち上げ。セキュリティアセスメント後は、工場のメンバーと情報セキュリティ部門が毎月のタッチポイントを設けて、改善/是正フェーズ（2年間）として伴走し、工場主導のフェーズへ順次移行することを計画。OTセキュリティ対応要員の社内育成を着実に推進。

Task	FY2021				FY2022				FY2023				FY2024			
	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
工場A・工場B	アセスメント実施フェーズ				改善/是正フェーズ1 People/Process系メイン				改善/是正フェーズ2 Technology系メイン				継続的セキュリティ確保の取り組み (工場主導へ移行フェーズ)			
								インシデント対応 トレーニング#1				インシデント対応 トレーニング#2				インシデント対応 トレーニング#3
工場C	アセスメント実施フェーズ				改善/是正フェーズ1 People/Process系メイン				改善/是正フェーズ2 Technology系メイン				継続的セキュリティ確保の取り組み (工場主導へ移行フェーズ)			
								インシデント対応 トレーニング#1				インシデント対応 トレーニング#2				インシデント対応 トレーニング#3
工場D					アセスメント実施フェーズ				改善/是正フェーズ1 People/Process系メイン				改善/是正フェーズ2 Technology系メイン			
											インシデント対応 トレーニング#1					インシデント対応 トレーニング#2
工場E									アセスメント実施フェーズ				改善/是正フェーズ1 People/Process系メイン			
																インシデント対応 トレーニング#1
海外工場（HQ支援）													アセスメント実施予定			
海外工場（リージョンで実施）									アセスメント実施				アセスメント実施予定			

OT領域の課題

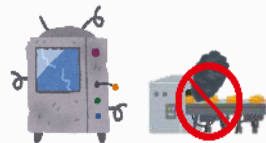


- 幅広い事業を展開。現場は**多種多様**。
国・製品によってもセキュリティ要求が異なる。
- 様々な設備／プロセスが存在し、セキュリティ対策の統一が難しく、**部分最適な対応が必要**

OT領域のリスク

工場／現場 におけるリスク

- 動作不良・誤作動
- 設備故障
- 生産停止
- センサ不良・改ざん



現場リスクから 派生するリスク

- ✓ 火災事故
- ✓ 環境影響
- ✓ 品質異常
- ✓ ケガ・労働災害



OT領域でサイバーインシデントが発生した場合、設備停止による操業影響だけでなく、異常稼働により**品質や安全**のリスクが発生する。

FSIRTの活動における課題



FSIRT

(Factory Security Incident Response Team)

【生産拠点の分散】 拠点が分散し、製品が多種多様であることによるばらつき

- ✓ 可能な限りの施策共通化による高位平準化
- ✓ 地理的分散・生産品目の違いに対応した、各拠点に適したセキュリティ施策の実装

【製品】 製造工程における品質・製品セキュリティ問題

- ✓ 製品関連情報の保護、製品生産に用いるネットワーク通信への保護
 - 機器製造では、製品ソフトウェアや機密データ(鍵など)の改竄・流出
 - 化学系では、形状・化学的性質の劣化・変質(品質課題)を防ぐため

【生産環境の安全、生産効率】 通信を介した物理制御の異常

- ✓ 製造装置の異常・暴走による事故を防ぐため、NW・物理両面の保護
 - 機器製造では、アームやコンベアなどの動作異常による破壊・怪我など
 - 化学系では、火災や爆発、有害物質流出懸念など

本パネルディスカッションアジェンダ

(1) 各社ご紹介

- パナソニック オートモーティブシステムズ株式会社
- 積水化学工業株式会社

(2) 各社xSIRT体制

(3) 各社xSIRT活動(FSIRT)

(4) WGでの議論共有

- 平時のFSIRT活動における大切な4つの要素
- 工場セキュリティIR訓練シナリオ案
- 成熟度セルフチェックシート

(5) まとめ



FSIRTの平時の活動における大切な4つの要素に関する議論

“Security”（データ・業務基盤・製品）と“Safety”（人命・環境）を守るために

- 工場セキュリティ専用のルール策定は必要か？
- 工場とそれ以外で、セキュリティインシデント対応プロセスは違いがある？



① 規程

インシデント発生時の対応方針の作成と関係者による合意、社内周知

- 工場セキュリティの取り組みをゼロから開始するとき、この4つはどこから始めるのが良い？



② 体制

インシデント発生時の社内連絡体制（連絡網の整備）



- FSIRTをどう構成するか？（会社で1つ？工場ごと？）
- FSIRTがどこまでするか？
- CSIRTとの連携や役割分担？
- セキュリティインシデント全体の統制は、どのSIRT？
- FSIRT人材育成/教育、キャリアパスの設計？

③ 訓練

方針通りに、体制が機能するか確認する演習/訓練

- どんな訓練を、どのように進めればよい？
- 実際に手を動かすような訓練も？
- リアリティのあるシナリオにするためには？
- 誰に参加してもらう？
- 年に何回くらい実施する？
- 企画運営、推進するのはどの部門で？



④ アセスメント

外部主要ガイドラインをベースとした第三者による定期的な成熟度評価



- セキュリティアセスメントの実施頻度？
- 推進主体？（工場か、本社か等）
- ISA/IEC62443
- IPA 制御システムのセキュリティリスク分析ガイド

WG成果物共有①：工場セキュリティIR訓練シナリオ素材案の検討

入口を想像

- Eメール
- (外部環境からの持ち込み)
PC、USB、SDカード等
- リモート保守用VPN機器の脆弱性
- 外部インターネットとの
アクセス制御不備
- 攻撃者の物理的な侵入
- 内部従業員による不正行為、
悪意のないオペミス etc.

起こることを想像

- マルウェアへの感染
- 外部からの不正アクセスによるシステム、
データの改ざん
- 悪意のある破壊行為
- 工場内NW通信停止/不良、
輻輳 etc.

影響/規模感を想像

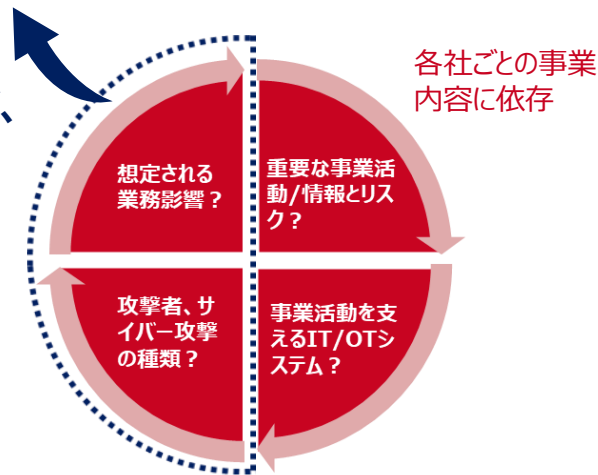
- 製造設備の異常動作、製造活動の一時停止
- 品質基準を満たさない製品の製造
- 人災、火災、爆発事故
- 工場周辺環境の汚染 etc.



シナリオNo.	テーマ名	インシデント発生における主な原因（例）
1	知られていなかった外部との通信経路 -IT部門が把握していない新たな通信経路からのマルウェア感染-	シャド-IT（ガバナンス不足）、資産管理の未徹底
2	変更作業の盲点。NW帯域の逼迫 -生産設備システムのファームウェアバージョンで想定外のNWトラフィックが発生し、輻輳-	変更作業における工場内運用ルール未整備
3	誰のUSBメモリかしら？ -不審なUSBメモリからのマルウェア感染-	アウェアネス不足、USBメモリの利用が未制御
4	管理責任者不在のVPN機器 -VPN利用時の工場内ネットワーク上の不正アクセスによる生産設備への侵入-	VPN機器の脆弱性対策不備、ベンダーとの責任範囲に関する契約書・セキュリティ
5		

製造現場を持つ事業会社実務者の意見・知見を盛り込んだ
工場で起こりそうなシナリオを目指す

業種を問わず、
ある程度、共通項目として
考えられる部分として抽出



※上記の成果物共有については本講演の収録時点における計画であり、実際の配布資料で提供される内容は予告なく変更となる場合があります。あらかじめご了承ください。

WG成果物共有①：工場セキュリティIR訓練シナリオ素材案の検討、使い方

年1回の特別なイベントから、日常で取り組む項目へ。

初動対応を中心にコンパクトに取り組むことができる工場セキュリティIR訓練を目指す

進め方に関するご紹介

【進め方（概要）】

- 工場内で起こりうる架空のインシデントをタイムラインで順次提示します。そのタイミングごとに何を実施すべきか/どのようなことを考えるか、感じたかなどチーム内で考えてください。
- 演習パート完了後に、全体の振り返り・ポイント解説をファシリテーターより実施します。

【演習のステップ・目安時間】

- オープニング 10分 ⇒ 演習タイム 35分 ⇒ 解説/振り返り・クロージング 40分



WGで議論したポイント

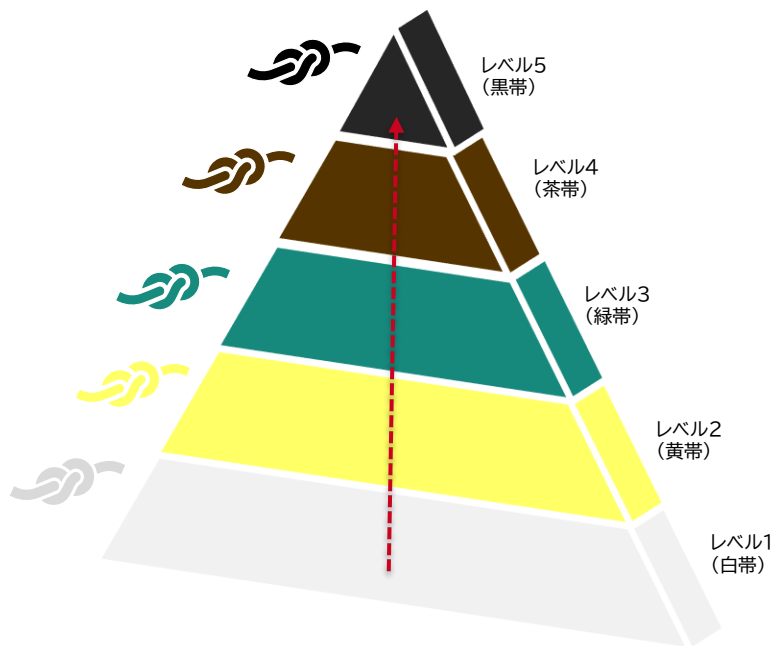
- IR訓練のシナリオスコープ、レベル設定
(初動対応にフォーカス)
- FSIRTメンバーが中心となって対応できるシナリオ
- 日々のFSIRT活動の中で取り組みやすいコンテンツ（開始から振り返りまで90分以内を目安）
- できたこと/できなかったことなど、課題の洗い出し、振り返りが大切

※上記の成果物共有については本講演の収録時点における計画であり、実際の配布資料で提供される内容は予告なく変更となる場合があります。あらかじめご了承ください。

WG成果物共有②：工場セキュリティIR訓練成熟度セルフチェックシート

成熟度を確認しながら、また次の一步へ。

主要ないくつかのポイントごとに5段階の到達目標案を設定し、積み重ねを可視化したい。



WGで議論したポイント

- 定期的に、意欲をもって取り組みを継続して頂くための工夫
- 成熟度/レベルアップの実感
- 演習後にいくつかの主要なポイントについてレベル1（白帯）～レベル5（黒帯）を設定し、到達の目安/目標を記載
- 各社の業種やビジネスモデルに応じて、自由にカスタマイズして使用

※上記の成果物共有については本講演の収録時点における計画であり、実際の配布資料で提供される内容は予告なく変更となる場合があります。あらかじめご了承ください。

本パネルディスカッションアジェンダ

(1) 各社ご紹介

- パナソニック オートモーティブシステムズ株式会社
- 積水化学工業株式会社

(2) 各社xSIRT体制

(3) 各社xSIRT活動(FSIRT)

(4) WGでの議論共有

- 平時のFSIRT活動における大切な4つの要素
- 工場セキュリティIR訓練シナリオ案
- 成熟度セルフチェックシート

(5) まとめ



パネルディスカッションまとめ

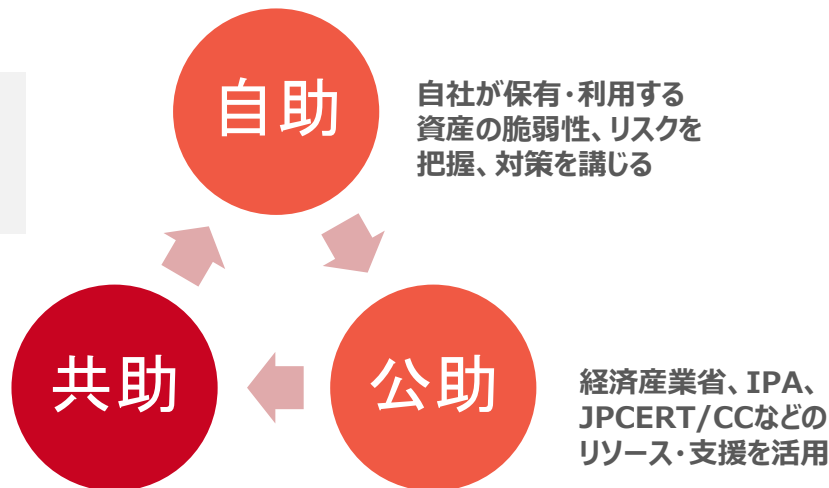
- 工場セキュリティIR訓練は、関係者が**自社の工場セキュリティについて考える良い契機**となる。
 - ✓ 業種/業界が異なるとSIRTを含めた体制は様々だが、**各社の抱えている課題や、必要なセキュリティ強化策には共通点が多い。**
 - ✓ **日々の活動の1つとして、工場セキュリティIR訓練**を取り入れ、少しずつ着実に、工場セキュリティ対策レベルの向上を目指していく。
 - ✓ **コミュニケーション開始のきっかけ**として活用し、「工場現場と情報セキュリティ/IT担当部門は分かり合えない」という思い込みを超えていく。
 - ✓ **成熟度セルフチェックシートを活用**し、毎回のIR訓練を通して自らのレベルをチェックし、継続的に取り組むモチベーションを維持し、着実なレベルアップを図る。
- **失敗から学習する組織を目指すための、工場セキュリティIR訓練**（プロジェクト管理における“事前検死”のアプローチ）
 - ✓ 「サイバー攻撃に遭うかもしれない、セキュリティインシデントが発生するかもしれない」ではなく、「サイバー攻撃により既にセキュリティインシデントが発生している」という最悪の前提に立って検討を開始し、何が問題だったのか、その理由・原因を関係者ですべて出し切ってみましょう。
（リアリティを演出するために、工場セキュリティIR訓練シナリオ案を自社向けにカスタマイズしてください）
- **工場セキュリティIR訓練シナリオ案、成熟度セルフチェックシートを実際に使用いただいたご感想、アドバイス等、皆さまからのフィードバックをお待ちしております。よろしくお願いいたします。**

【最後に】生産現場も含め、企業を守るために企業間の連携強化をさらに図っていききたい

- ◆ 業種/業界が異なると、SIRTを含めた体制は様々だが、各社の抱えている課題や、必要となるセキュリティ強化策には共通点が多い。
- ◆ 他社で発生したインシデントは将来、自社で発生する可能性も十分ある。
- ◆ 社内部門/チーム間に加えて、企業間/官民の連携（コミュニケーションの活性化）を強化していく。
- ◆ コミュニケーションの際には、コミュニティ参加者のセキュリティクリアランスや、チャタムハウスルールなど、共有された情報の取り扱いに関する安全性の担保も重要。

企業使命「BEAUTY INNOVATIONS FOR A BETTER WORLD
(美の力でよりよい世界を)」のもと、企業としての成長はもちろん、
社会課題の解決や世界中の人々が幸せになる
サステナブルな社会の実現をめざしています。

企業の枠を超えて、
互いに情報や知恵を共有しあい、
全体のレベルを高める



The background image shows a modern interior space with a series of tall, colorful vertical glass columns in shades of yellow, blue, and pink. Some columns have circular metal frames or valves attached to them. In the background, a woman in a black dress is walking, carrying a folder or bag. The floor is light-colored, and there are white circular tables and blue stools in the foreground. The ceiling is high with visible lighting fixtures.

ご清聴いただきありがとうございました。ご安全に！

Special Thanks; JPCERTコーディネーションセンター 制御システムセキュリティ対策グループ 河野一之様、堀充孝様
Presented by; 製造業ICS（制御システム）セキュリティ担当者コミュニティー内WG（FSIRT訓練やろうの会）



Appendix-1

工場セキュリティIR訓練シナリオ素材

「平時」もしくは「安全」とは、多くの人々による不断の努力の結果として
ようやく享受できる、リスクが顕在化しなかった状態のことをいう。

工場セキュリティIR訓練シナリオ案の活用方法

- 公開されているセキュリティのインシデント報告を確認すると、インシデントの結果発生した被害の大きさやビジネスへの影響の現れ方は非常に様々です。一方で、その根本原因については、それほど多くのパターンは無いと考えています。主要な原因、パターンを意識し、事前に対策をおこなっておくことで、インシデント発生確率や被害の軽減が期待できます。
- 工場セキュリティIR訓練シナリオ案は、WG内での議論も踏まえて、外部からのサイバー攻撃、社内での作業上のミス等から生産業務への影響が発生するシナリオを5つ準備しています。
- 各シナリオ内で黄色ハイライトしている部分は自社でIR訓練を実施する際に、自社の組織・部署名、担当者名などに変換して、よりリアルなIR訓練として頂ければ幸いです。また、各状況付与ごとの検討時間についても、貴社内で適切な長さに変更してください。
- IR訓練は、実施後の「振り返り」が最も重要です。課題を抽出し、見いだされた課題に対して優先順位をつけ、改善・是正アクションの計画を立てましょう。そして、次回にIR訓練を実施する際には、一段階レベルアップした状態で臨むことができれば、IR訓練の価値が最大化されます。
- 一部のシナリオでは、再発防止策の検討をIR訓練内でおこなう場合もあります。IR訓練内ではインシデントの初期調査、被害の最小化・封じ込めなどにフォーカスすることも多いですが、IR訓練の時間内で、なぜインシデントが発生したのか？ どうすれば防ぐことができたのかを関係者と考えられるように設計しています。（IR訓練は振り返りが最重要ですが、振り返りのための別枠での時間確保ができないことが多々ある、現場の状況も理解しています）
- 各シナリオ案ごとの扉スライド（タイトルスライド）では、テーマ名を記載しており、ネタバレになりますので、IR訓練時には参加者に見せないことを推奨します。

シナリオNo.	テーマ名	インシデント発生における主な原因（例）
1	知られていなかった外部との通信経路 -IT部門が把握していない新たな通信経路からのマルウェア感染-	シャドーIT（ガバナンス不足）、資産管理の未徹底
2	変更作業の盲点。NW帯域の逼迫 -生産設備システムのファームウェアバージョンで想定外のNWトラフィックが発生し、輻輳-	変更作業における工場内運用ルール未整備
3	誰のUSBメモリかしら？ -不審なUSBメモリからのマルウェア感染-	アウェアネス不足、USBメモリ利用ルール未制御
4	管理責任者不在のVPN機器 -VPNリモート保守環境からの不正アクセスによる生産設備の停止-	VPN機器の脆弱性対策不備、ベンダーとの責任範囲に関する協議不足・保守契約書への未記載
5	ランサムウェアは突然に -保守用持ち込みPCからマルウェア感染、生産設備の停止-	工場内運用ルール未整備



工場セキュリティIR訓練シナリオ素材①

-知られていなかった外部との通信経路-

工場セキュリティIR訓練 進め方に関するご紹介

【進め方（概要）】

- 工場内で起こりうる架空のインシデントをタイムラインで順次提示します。そのタイミングごとに何を実施すべきか/どのようなことを考えるか、感じたかなどチーム内で議論してください。
- 演習パート完了後に、全体の振り返り・ポイント解説をファシリテーターより実施します。

【演習のステップ・目安時間】

- オープニング **10分** ➡ 演習タイム **35分** ➡ 解説/振り返り・クロージング **40分**



シナリオ① 状況付与/Timeline-1 (11時00分)

検討時間

10min

【製造設備管理部門】のメンバーが何やら慌ただしく工場内を動き回っている。場内に緊急の業務放送が流れた。

「一部の生産設備が停止しております。現在、原因を調査中です」

【製造設備管理部門】の対応により、PLCで動いているアプリケーションがシャットダウンしたことによって生産設備が異常を検知し停止したものと判明した。事象の根本原因は不明のままだが、ひとまず生産設備を再稼働することができた。【製造設備管理部門】のメンバーは、PLC保守ベンダーへ連絡をし、ログの確認を依頼してから、順次、昼休憩に入った。【製造設備管理部門】のマネージャから工場長へ、「生産システムが約30分間停止したが、直ちに復旧した。現在、根本原因を調査している」旨を報告した。【工場セキュリティ推進部門】にはまだ何も情報は入っていない。

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
工場内ではどのような情報共有がなされそうでしょうか。

シナリオ① 状況付与/Timeline-2（13時00分）

検討時間

5min

昼休憩が終わった直後、また同じ、生産設備が緊急停止した。【製造設備管理部門】のメンバーは再度、状況を確認し、午前中と同じ対応を実施したが、今後も再発する可能性がある判断し、工場内で緊急対策会議が開催された。この会議体には、。【工場セキュリティ推進部門】のマネージャ、参加可能な担当メンバーも参加している。

工場長

「1日に2度も同じシステムが停止することは不自然である。何か設定の変更などを最近おこなっていないのか？」

【製造設備管理部門】

「PLC関連機器に関して、特に変更は実施していません」

・・・

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
（だれが、何を実施すべきでしょうか）

シナリオ① 状況付与/Timeline-3 (13時20分)

52

検討時間

10min

工場から、【情報セキュリティ/リスク管理部門のマネージャ】へ電話連絡（第一報）を実施した。PLC保守ベンダー、工場緊急対策本部、情報セキュリティ部での調査が開始された。また、【情報セキュリティ/リスク管理部門】からは、【本社ITインフラ運用部門】へも情報連携が行われ、【本社ITインフラ運用部門】にて、ファイアウォールのログ確認が開始された。

【情報セキュリティ/リスク管理部門】

「外部からの攻撃の場合、皆さんの元へ何かしら脅迫メールなどが届いている可能性も考えられますが、受信された方はいませんか。弊社でもメール受信履歴のログを確認中ですが、皆さまもメール受信トレイの確認をお願いいたします」

【工場長】

「8:50にこのようなメールが届いていたようだ」（次ページ参照）

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
（だれが、何を実施すべきでしょうか）

親愛なる【会社名】の皆さん

この文章を読んでいるということは、我々があなた方のコーポレートネットワークへのハッキングを完了できたということを意味しています。あなた方のシステムはすでに我々の管理支配下にあります。皆さんへ親切な警告をいたします。捜査機関への通報や、システム復旧の試みはシステムの壊滅的な破壊につながる恐れがありますので、推奨しません。

我々は特定の政治、宗教に関する主義主張は持っていません。ただ、利益を得ることを目的として活動しています。ビットコイン(40BTC)の支払いを完了して頂ければ、システムは元の状態にお戻しすることをお約束します。さらに、10BTCの追加支払いにより、貴社ネットワーク環境の問題点に関するアドバイザリーコメントもご提供可能です。

我々はあなた方のシステムに対して、ハッキングできている証拠として簡単なデモンストレーションをお見せします。日本時間の11時に貴社のあるシステムに異常が発生することでしょう。しっかりと確認してください。このようなデモンストレーションが1回で終わると思わない方が賢明ですよ。

皆さまの貴重な時間が無駄にならないよう、至急、ビットコインを支払い、下記へご連絡頂くことを推奨します。その際、会社名、コーポレートサイトのURLも忘れずに記載してください。

連絡先は下記:

ransomwarehelpdesk-jp@★▼●.com

早期のご連絡をお待ちしております。

シナリオ① 状況付与/Timeline-4（14時00分）

検討時間

5min

PLC保守ベンダー、工場緊急対策本部、【本社IT/情報セキュリティ部】による合同調査が開始された。

【本社IT/情報セキュリティ部】

「【ネットワーク運用チーム】からの調査結果を受領しました。ファイアウォールのログ解析をしても不審なアクセスは見当たりません。この場合、工場内に物理的に攻撃者が侵入しているか、我々が管理、把握できていないネットワーク通信経路が存在していた、もしくは新たに設置された可能性も考えるべきです。」

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
（だれが、何を実施すべきでしょうか）

シナリオ① 状況付与/Timeline-5（15時00分）

検討時間

5min

PLC管理端末に見慣れない、“WiFi”と書かれている小さな機器が取り付けられていることを発見した。**【製造設備管理部門】**がリモート保守作業の検討用に臨時で設置していた、「**LTE対応USB Dongle**」であることがわかった。

【工場セキュリティ推進部門】の中には、このような取り組みや機器の設置に関して把握できているメンバーは一人もいなかった。

この時点で、**【工場セキュリティ推進部門】**は何を実施しますか？
（だれが、何を実施すべきでしょうか）

工場セキュリティIR訓練シナリオ素材①

解説編

シナリオ① 解説

今回のシナリオでは、IPAが毎年発行している「情報セキュリティ10大脅威」の上位にランクインしている、「サプライチェーンリスク」、「標的型攻撃」、「テレワーク等のニューノーマルな働き方」を背景としたシナリオを構成した。

本ケースの問題点①

シャドーIT

情報セキュリティ部門／リスク管理部門への事前確認なく、外部からのリモートアクセス経路が構築されていた。

本ケース問題点②

外部からのアクセス許可の設定（アクセス制限不備）

任意のグローバルIPアドレスからアクセスできるようになっていた。

本ケースの問題点③

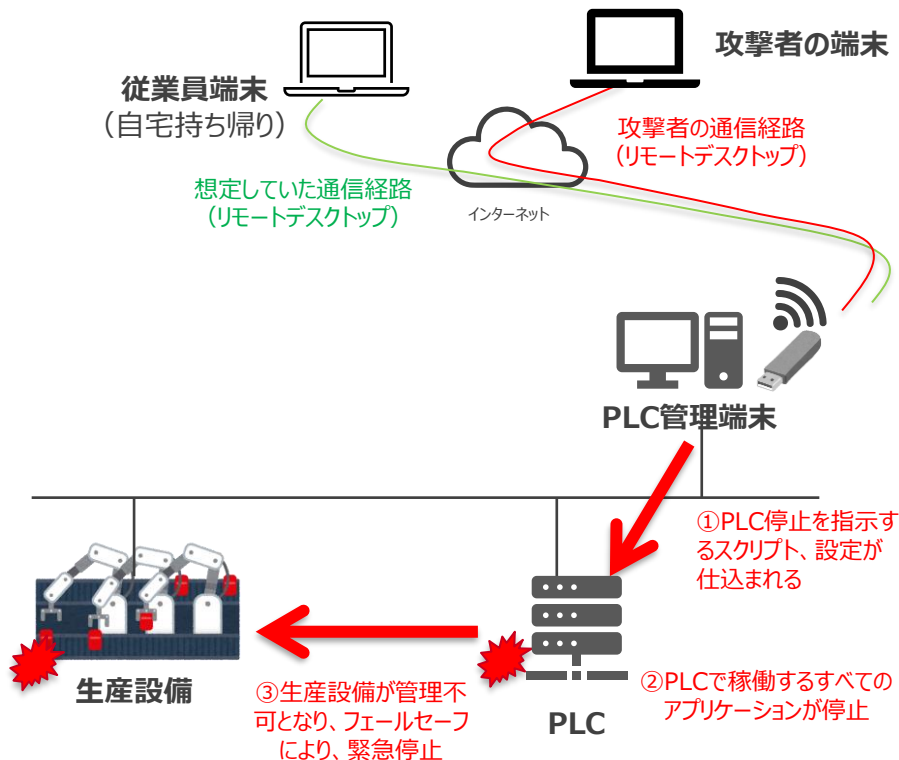
グループ内/工場内における情報連携が不十分

リモート保守検討プロジェクトに関して、一部の担当者を除き、その存在を認識できていなかった。（今回は主担当者が、勤続20年の記念休暇で海外旅行中のため、緊急対策会議には参加できなかったという設定）

本ケースの問題点④

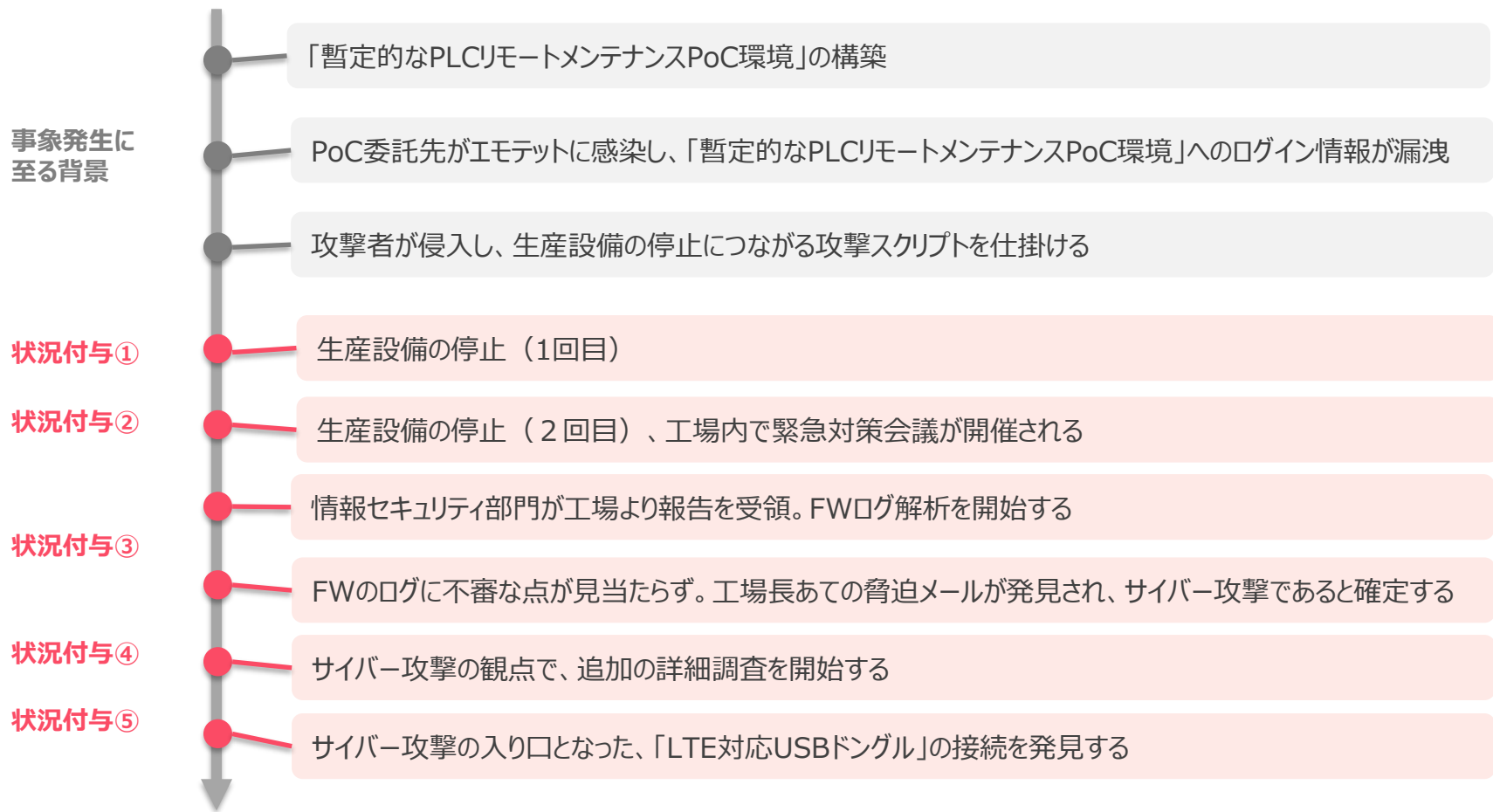
サプライチェーン/ベンダーマネジメントの不足

保守を委託している会社がEmotetに感染して、委託先からリモートアクセス環境に関する情報が漏洩していた。委託先のセキュリティチェック、インシデントに関して情報共有される体制づくりをしていなかった。



シナリオ① 状況付与/Timelineの全体像

58



シナリオ① 期待する行動例

状況付与	期待する行動（主要なもの）
① 工場内の緊急放送、 生産設備 1 回目の緊急停止	・ 別グループへの声掛け（グループ間の密な連携） ・ 生産設備停止と復旧状況に関する工場内における情報共有 ・ インシデント対応マニュアルの確認
② 生産設備 2 回目の緊急停止、工場 内の緊急対策会議	・ 情報セキュリティ部門への情報共有、連絡 ・ 工場の生産停止に関する検討や判断
③ 工場長への脅迫メール	・ 不審メールに関する工場内での注意喚起を発信（不用意に返信などをしない）
④ 原因調査難航、 情報セキュリティ部門からの助言	・ 資産管理台帳、ネットワーク物理構成図の確認 ・ 停止した生産設備と接続されている機器/通信経路の把握 ・ 工場内の機器（サーバ、PC等）について、現物を「目視」確認
⑤ LTE対応USB dongleの発見	・ 対象管理端末の管理部門、管理者の特定 ・ USBの用途特定 ・ USBの取り外し ・ 対象管理端末内のログ調査、端末設定状況確認 ・ （必要な場合には）端末の交換 ・ JPCERT/CCへのインシデント事例の共有/報告/相談

※補足：「JPCERT/CCへのインシデント事例の共有/報告/相談」について、状況付与⑤の期待する行動例として設定していますが、各社のインシデント対応／フォレンジック体制などから、各社で最適なタイミングを判断し、JPCERT/CCへコンタクトすることが良いでしょう。

シナリオ① 振り返り/今後の検討ポイント

本演習の終了後の改善フェーズで以下のような内容についても、是非ご検討ください

60

1. インシデント発生時の社内のマニュアル/ガイドラインに沿った対応を想起できたか？
2. インシデントレスポンスのための体制、環境の準備ができたか？（専用会議室の確保、ホワイトボード、電話、PC、インシデント体制図やネットワーク構成図の貼り出し）
3. 記録係、連絡係など役割分担は、あらかじめ明確化できていたか？
4. 適切なタイミングで情報セキュリティ管轄部門/CISOへの連絡をおこなえたか？
5. 工場内で報告/連絡すべき部門、グループは明確化されており、連携できていたか？
6. 発生している問題の原因分析のため、情報収集活動がおこなえていたか？
7. 混乱している工場内のコミュニケーション交通整理がおこなえていたか？（誰がすべきか？）
8. 工場全体の従業員への連絡は効率的かつ的確に行えていたか？（デジタルサイネージ、場内全館放送、メーリングリストの活用など、複数のコミュニケーション方法を想定できているか）
9. 工場長に対してはどのタイミングで連絡すべきか、場内のルールは明確化・共有されているか？
10. 発生している事象から工場内の影響範囲を特定するためのアクションをとることができたか？（資産管理台帳、ネットワーク構成図の活用、当該生産設備担当のグループ、保守委託先ベンダーとのコミュニケーションへの適切な関与）

シナリオ① 成熟度セルフチェックシート 主なチェック項目

成熟度セルフチェックシート項目一覧		
被害シナリオの想定	インシデント対応体制	役割の定義と合意
連絡方法の確立	インシデント対応マニュアルの整備と周知	制御システムに影響がある インシデント対応訓練/演習
サプライチェーンリスク管理	継続的なアウェアネス向上	外部専門機関との連携
モニタリング・検知	持ち込み機器の検査	データ分類
資産管理（IT/OT）	ネットワーク構成管理	システムへのアクセス制御
マルウェアへの対処・駆除	脆弱性管理	機器セキュリティ更新
物理的セキュリティ （入退場管理）	不要なUSBポート閉塞	サーバラック、HUBボックス等の施錠
ネットワークゾーニング（セグメンテーション）	バックアップ取得	バックアップデータの保管
リストア	外部記憶媒体の管理（USBメモリ等）	バイ・デザインのアプローチ
セキュリティアセスメント	システムアカウント管理	ペネトレーションテスト
制御システムに関する専門教育、 キャリアパスの整備	変更作業実施時の承認プロセスの整備	内部犯行への対策

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	役割の定義と合意
レベル5（黒帯）	生産停止を決定できる最上位者も含め決まっており、定期的な見直しや確認をおこなっている。
レベル4（茶帯）	生産停止を決定できる最上位者も含め決まっているが、定期的な見直しや確認をおこなっていない。
レベル3（緑帯）	現場担当者レベルではある程度決まっているが、定期的な見直しや確認をおこなっていない。
レベル2（黄帯）	社内で議論、検討したことはあるが、まだ決定に至っていない。
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	生産設備1回目の停止のタイミングから、設備故障以外の可能性も視野に、あらかじめ決められている意思決定者を巻き込んだ形で、今後の工場稼働継続に関して議論することを想定できた。生産停止を決定できる最上位者等に関して定義したドキュメントも直ちに取り出せた。
レベル4（茶帯）	生産設備2回目の停止のタイミングで、設備故障以外の可能性も視野に、あらかじめ決められている意思決定者を巻き込んだ形で、今後の工場稼働継続に関して議論することを想定できた。生産停止を決定できる最上位者等に関して定義したドキュメントも直ちに取り出せた。
レベル3（緑帯）	過去に生産停止を決定できる最上位者を定義していたが、その決定内容を記載したドキュメントは見つからなかった。緊急対策会議に参加しているメンバーで今後の工場稼働継続に関して議論することは想定できた。
レベル2（黄帯）	生産活動の停止等に関する明確な役割が定義されておらず、緊急対策会議の中で、はじめて議論・検討することとなった。
レベル1（白帯）	生産活動の停止等に関する明確な役割が定義されていない。演習内でも、今後の生産活動に関する検討の必要性に関する議論は一切なかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	連絡方法の確立
レベル5（黒帯）	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備し、定期的に機能するか検証、訓練している。
レベル4（茶帯）	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備している。
レベル3（緑帯）	連絡網（複数の連絡手段を想定）を作成している。
レベル2（黄帯）	連絡網（連絡手段1つ）を作成している。
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	生産設備1回目の停止のタイミングで、あらかじめ決められた連絡方法によって、すべての関係者に対して直ちに情報伝達した。
レベル4（茶帯）	生産設備1回目の停止のタイミングで、すべての関係者に対して直ちに情報伝達したものの、連絡方法はインシデント発生時に決めて対応した。
レベル3（緑帯）	生産設備1回目の停止のタイミングで、主要なメンバーには情報伝達されたが、関係者全員には情報が行き渡らなかった。
レベル2（黄帯）	生産設備1回目の停止のタイミングで、自身と普段から繋がるのある数名のメンバーへ個別に連絡し、情報収集を試みた。
レベル1（白帯）	生産設備1回目の停止のタイミングで、影響のあった生産ラインの関係者のみ詳細な状況を把握しており、工場内で円滑な情報共有ができなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	インシデント対応マニュアルの整備と周知
レベル5（黒帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。
レベル4（茶帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。
レベル3（緑帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。
レベル2（黄帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルは存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。
レベル1（白帯）	何も存在しない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	サイバー攻撃についても考慮された生産設備でのインシデントマニュアルが存在する。定期的に関係者で読み合わせなど内容確認をおこなっているので、スムーズに演習内でも参照できた。
レベル4（茶帯）	サイバー攻撃についても考慮された生産設備でのインシデントマニュアルが存在する。演習内で確認しようとしたが、初めて読むので理解に時間を要した。
レベル3（緑帯）	サイバー攻撃は考慮していない生産設備でのインシデントマニュアルは存在する。演習内で確認した。
レベル2（黄帯）	サイバー攻撃は考慮していない生産設備でのインシデントマニュアルは存在するが、確認しようとしなかった。
レベル1（白帯）	インシデント対応マニュアルが存在しなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	サプライチェーンリスク管理
レベル5（黒帯）	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝え、定期的な契約内容の見直しをおこない、調達先が自社で求められるセキュリティ要件を満たすようにしている。必要な際には調達先の変更も含め幅広く検討し、セキュリティの確保に努めている。また、定期的に調達先の情報セキュリティ管理体制チェック/ヒアリングをおこなっている。
レベル4（茶帯）	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝え、定期的な契約内容の見直しをおこない、調達先が自社で求められるセキュリティ要件を満たすようにしている。必要な際には調達先の変更も含め幅広く検討し、セキュリティの確保に努めている。
レベル3（緑帯）	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝えたことはあるが、調達先から強い拒否感を示され、断念した。ワークアラウンド/次善策を実施し、セキュリティリスクの軽減を図っている。
レベル2（黄帯）	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝えたことはあるが、調達先から強い拒否感を示され、断念した。
レベル1（白帯）	長年の付き合いのある調達先なので、契約内容は特に見直さず、単純更新している。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	委託先内で自社（委託元）に関する情報漏洩の可能性が判明した時点で、自社に通知してもらう契約を取り交わしている。情報漏洩の認識から通知までの時間も規定している。パスワードなど機密情報はメールでやり取りしない運用を徹底している。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	委託先には自社に関する情報漏洩の可能性が判明した時点で、早期に通知してもらえるよう依頼している。パスワードなど機密情報はメールでやり取りしない運用を徹底している。本シナリオのような状況が発生するリスクは低いと想定していることを確認した。
レベル3（緑帯）	委託先には自社に関する情報漏洩の可能性が判明した時点で、早期に通知してもらえるよう依頼している。本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	委託先と情報セキュリティリスク管理に関する議論をしたことはあるが、特段なにも取り決めや依頼はしていない。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	委託先と情報セキュリティリスク管理に関する議論をしたことがない。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	ネットワーク構成管理
レベル5（黒帯）	工場全体のネットワーク物理構成図、設計図がある。定期的に最新化されており、インシデント発生時にはすぐに取り出せる。また影響範囲について想定することができる。
レベル4（茶帯）	工場全体のネットワーク物理構成図、設計図を作成したことがあるが、その後、更新していないので、現状の構成と乖離している可能性がある。
レベル3（緑帯）	工場全体のネットワーク物理構成図、設計図は無いが、自身が担当しているライン/領域については、各担当が接続構成、影響範囲を含め個別に把握している（ドキュメント化されていない）。
レベル2（黄帯）	ネットワーク機器の配置場所や管理部門を把握している（ドキュメント化されていない）。
レベル1（白帯）	ネットワーク機器がどこにあり、誰が管理しているのか全くわからない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	工場全体のネットワーク物理構成図、設計図をすぐに取り出すことができ、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル4（茶帯）	過去に作成した工場全体のネットワーク物理構成図、設計図がどこにあるのかわからず、見つけ出すのに時間を要したが、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル3（緑帯）	ネットワーク構成図は各システムごとに作成しており、それらを使用した。しかし、工場全体を俯瞰したものではないため、インシデントの影響範囲の確認や原因調査には活用できなかった。もしくは利用したが、かなり時間を要した。
レベル2（黄帯）	ネットワーク構成図などドキュメント類はないものの、環境を把握しているメンバーの知識をもとにインシデントの影響範囲や原因分析を試みた。
レベル1（白帯）	ネットワーク構成図のようなものは一切存在しないため、インシデントの影響範囲の確認や原因調査に活用できなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	システムへのアクセス制御
レベル5（黒帯）	すべてのシステムにおいて、MFAの実装、アクセス元のグローバルIPアドレス制限等による、複数のアクセス制御を実装している。
レベル4（茶帯）	多くの主要システムで、ID、パスワードに加えて、MFAの実装やアクセス可能なアクセス元のグローバルIPアドレスを制限する等、追加の対策を実施している。
レベル3（緑帯）	ID、パスワードのみでログインできるシステムが多いが、一部の重要なシステムでは、MFAの実装やアクセス可能なアクセス元のグローバルIPアドレスを制限する等、追加の対策を実施している。
レベル2（黄帯）	すべてのシステムでID、パスワードの設定をおこなっている。
レベル1（白帯）	ID、パスワードの設定をしていない、アクセス制御なしのシステムが工場内に存在する。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	すべてのシステムにおいて、MFAの実装、アクセス元のグローバルIPアドレス制限等による、複数のアクセス制御も実装できている。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	重要な一部のシステムでは、MFAの実装、アクセス元のグローバルIPアドレス制限等による、複数のアクセス制御も実装できている。本シナリオのような状況が発生することは低いと想定していることを確認した。
レベル3（緑帯）	MFAの実装、アクセス元のグローバルIPアドレス制限等による、複数のアクセス制御の導入を開始始めているが、まだ道半ば。本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	ID、パスワードのみでアクセスできるシステムがほとんどであり、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	アクセス制御に関して重要性は認識しているものの、工場内のシステムではどのような状況になっているのか把握していない。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	物理的セキュリティ (入退場管理)
レベル5（黒帯）	茶帯の内容に加えて、顔認証、静脈認証、IDカード、監視カメラ等による多層のゲート、認証・監視システムが導入されている。特に重要な機器があるエリアには入場可能な人が厳密に規定、制限されている（ゲスト入館時には事前に身分証明書の確認、顔データの登録が必要等）。
レベル4（茶帯）	受付で事前に登録された訪問情報をもとに、受け入れ担当社員へ連絡が入り、有効期限付きのゲストIDカードを貸与したうえで、社員が同行し工場内へ入場する。入場した後もゲストの常時監視、同行をおこない、社外の人間に単独行動はさせない。
レベル3（緑帯）	受付で事前に登録された訪問情報をもとに、受け入れ担当社員へ連絡が入り、無期限のゲストIDカードを貸与したうえで、社員が同行し工場内へ入場する。入場した後もゲストの常時監視、同行をおこない、社外の人間に単独行動はさせない。
レベル2（黄帯）	受付で事前に登録された訪問情報をもとに、受け入れ担当社員へ連絡が入り、無期限のゲストIDカードを貸与したうえで、社員が同行し工場内へ入場する。しかし、入場した後はゲストの常時監視や同行はしていない。
レベル1（白帯）	受付で会社名と氏名、訪問先を伝え、顔見知りであれば、社員の同行が無くとも、社外の人間が工場内へ入場することが可能。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	状況付与④のタイミングで、物理的に外部から侵入された可能性を考慮して、社内の物理セキュリティのシステムのログ、映像確認などインシデント発生時に定められている確認対応をおこなった。もしくは担当チームへの対応依頼をおこなった。
レベル4（茶帯）	状況付与④のタイミングで、物理的に外部から侵入された可能性について演習内で言及されたが、どのような物理的セキュリティがあるのか、どのように対応すれば良いのか誰も把握しておらず、具体的なアクションに繋がらなかった。
レベル3（緑帯）	状況付与④のタイミングで、物理的に外部から侵入された可能性について演習内で多少言及された。
レベル2（黄帯）	状況付与④のタイミングで、物理的に外部から侵入された可能性は想像できたが、そのような物理的セキュリティ対策が存在しないので、この点は諦めて他の対応を優先した。
レベル1（白帯）	状況付与④のタイミングで、物理的に外部から侵入された可能性は一切考慮、想像できなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	不要なUSBポート閉塞
レベル5（黒帯）	不要なUSBポートについて、物理的に閉塞している。閉塞器具の鍵は任命された複数の管理者が利用履歴を記録し、保管している。また、追加の安全策として、工場内に導入する機器類については、USBメモリ挿入時の自動起動をしない設定を標準としている。
レベル4（茶帯）	不要なUSBポートについて、物理的に閉塞している。ただし、閉塞器具の鍵は誰でも使用できるように分かりやすい場所に配置している。また、追加の安全策として、工場内に導入する機器類については、USBメモリ挿入時の自動起動をしない設定を標準としている。
レベル3（緑帯）	工場内に導入する機器類については、USBメモリ挿入時の自動起動をしない設定を標準としている
レベル2（黄帯）	不要なUSBポートについて、物理的に閉塞している。ただし、閉塞器具の鍵は誰でも使用できるように分かりやすい場所に配置している。
レベル1（白帯）	USBポートに関する対策は何もしていない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	不要なUSBポートについて、物理的にすべて閉塞している、もしくはUSBメモリを挿入しても機能しない技術的実装を全機器で実施しており、本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	重要なシステムでは不要なUSBポートについて、物理的に閉塞もしくはUSBメモリを挿入しても機能しない技術的実装をおこなっているが、すべての機器が対象とはなっておらず、本シナリオのような状況が発生する可能性が残っていることを確認した。
レベル3（緑帯）	USBポートのセキュリティ対策導入を順次開始している。本シナリオのような状況が発生する可能性はまだ高いことを確認した。
レベル2（黄帯）	USBポートのセキュリティ対策を検討し始めてはいたものの、具体的な対策実施にいたっておらず、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	工場内のPCのUSBポートは制御されておらず、自由に使用することができる。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	バイ・デザインのアプローチ
レベル5（黒帯）	セキュリティの専門家（情報処理安全確保支援士、CISSP等）が新規のシステム導入やITを用いた施策について、企画立ち上げ・検討フェーズ初期から参画し、担当者は情報セキュリティリスクの観点からアドバイスを受けるようにしている。バイ・デザインのプロセスは、プロジェクトを推進する際の必須事項として、社内ルールに取り込まれている。さらに、社内稟議システムとしても、セキュリティの専門家によるレビューが完了しないと、プロジェクトの発注や推進ができない仕組みになっている。
レベル4（茶帯）	セキュリティの専門家（情報処理安全確保支援士、CISSP等）が新規のシステム導入やITを用いた施策について、企画立ち上げ・検討フェーズ初期から参画し、担当者は情報セキュリティリスクの観点からアドバイスを受けるようにしている。ただし、これは任意で社内ルールにはなっていない。
レベル3（緑帯）	新規のシステム導入やITを用いた施策について、セキュリティの専門家（情報処理安全確保支援士、CISSP等）に基本的に相談、情報共有することになっているが、プロジェクトの後半、システムリリース直前となることが多い。
レベル2（黄帯）	新規のシステム導入やITを用いた施策について、セキュリティの専門家（情報処理安全確保支援士、CISSP等）に相談することもあるが、稀である。
レベル1（白帯）	新規のシステム導入やITを用いた施策について、セキュリティの専門家（情報処理安全確保支援士、CISSP等）が関わることはない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	新規システム導入時には、検証PoCなど一時的なものであっても例外なく、必ず社内の専門部門と事前に相談し、内容を確認するようなバイ・デザインのプロセスが導入されている。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	バイ・デザインのプロセスが存在する。大規模システム導入の際には、社内の専門部門と事前に相談し、内容を確認してもらっている。検証など一時的なものは担当部門のみで進めることもあり、本シナリオのような状況が発生する可能性はあることを確認した。
レベル3（緑帯）	バイ・デザインのプロセスが存在する。ただし、社内ですべてのプロセスに則って対応するかどうかは任意のため、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル2（黄帯）	バイ・デザインのプロセスの導入に向けて、専門部門の立ち上げ、整備を進めている。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	各部門が独自にシステム導入を推進しており、社内ですべての専門家によるレビューなどのバイ・デザインのプロセスは存在しない。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	変更作業実施時の承認プロセスの整備
レベル5（黒帯）	変更管理手順が文書化されている。当該領域に関する専門的な知見を有する者を含めた確認者による承認プロセス（多段階承認）が整備、徹底されている。変更作業の計画時には、開発・検証環境での作業内容の事前確認などにより、変更による影響の分析を十分におこない、発生する可能性のある事象に対して、対応策および回避策が計画され、リスクの最小化が図られている。変更作業の実施前には、あらかじめ決められた連絡手段・方法で、工場内へ変更作業の内容、詳細な作業実施スケジュール、当該作業に関する責任者・問合せ先に関する情報共有をおこない、万が一の際にも、迅速なコミュニケーションが可能となるようにしている。
レベル4（茶帯）	変更管理手順が文書化されている。当該領域に関する専門的な知見を有する者を含めた確認者による承認プロセス（多段階承認）が整備、徹底されている。開発・検証環境は存在しないため、ベンダーの公開・保有情報および机上で、変更による影響の分析をおこない、発生する可能性のある事象に対して、対応策および回避策が計画され、リスクの最小化が図られている。変更作業の実施前には、あらかじめ決められた連絡手段・方法で、工場内へ変更作業の内容、詳細な作業実施スケジュール、当該作業に関する責任者・問合せ先に関する情報共有をおこない、万が一の際にも、迅速なコミュニケーションが可能となるようにしている。
レベル3（緑帯）	変更管理手順が文書化されており、当該領域に関する専門的な知見を有する者を含めた確認者による承認プロセス（多段階承認）も準備されているが、社内での運用が徹底されていない。変更作業の実施前には、担当者が任意の手段・方法により、工場内へ変更作業の内容、詳細な作業実施スケジュール、当該作業に関する責任者・問合せ先に関する情報共有をおこない、万が一の際にも、迅速なコミュニケーションが可能となるようにしている。
レベル2（黄帯）	変更作業の進め方に関する正式なプロセスは特に存在しておらず、都度、個別に相談しながら進めている。変更作業を実施する際には、周知・連絡方法は定まっていなかったものの、工場関係者に幅広く事前の情報共有を図るよう心掛けている。
レベル1（白帯）	変更作業の進め方に関する正式なプロセスは特に存在しておらず、都度、個別に相談しながら進めている。変更作業を実施する際には、所属部門コミュニティ内で事前周知している。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	工場内で変更作業を実施する際の手順や承認プロセスが確立されている。また、変更作業実施に関する場内の事前周知に関する方法も定められている。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	工場内で変更作業を実施する際の手順や承認プロセスが確立されている。変更作業の実施に関する場内の周知方法は特に決まっていなかったが、各担当により必ず何らかの全体周知がおこなわれる習慣となっている。本シナリオのような状況が発生する可能性は低いことを確認した。
レベル3（緑帯）	工場内で変更作業を実施する際の手順や承認プロセスが確立されている。変更作業の実施に関する場内の周知方法は特に決まっておらず、時折、認識していない変更作業がおこなわれていることがある。本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	工場内で変更作業を実施する際の手順、承認プロセスは一応あるが、あまり利用されておらず形骸化している。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	工場内で変更作業を実施する際の手順、承認プロセス、事前の周知方法に関するルールが特にならない。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ① 成熟度セルフチェックシートを活用した振り返りノート

	外部専門機関との連携
レベル5（黒帯）	JPCERT/CCに加えて、その他各社で個別に契約している、各社のIT/OT環境に関する構成情報を事前に熟知した、インシデント対応/デジタル・フォレンジック/リスクマネジメント専門企業への連絡先を直ちに引き出すことができ、スムーズに連絡、相談できる。
レベル4（茶帯）	JPCERT/CCへの連絡先を直ちに引き出すことができ、スムーズに連絡、相談できる。
レベル3（緑帯）	既存の生産設備の保守ベンダーのみへ連絡が可能。
レベル2（黄帯）	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない
レベル1（白帯）	どこに連絡するべきか想定がない。決まっていない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	連絡すべき外部専門機関のリストが整備されており、すぐに取り出す/確認することができた。
レベル4（茶帯）	連絡すべき外部専門機関のリストを整備していたが、保管場所が分からず探すのに時間を要した。
レベル3（緑帯）	連絡すべき外部専門機関のリストを整備を現在、推進している途中。
レベル2（黄帯）	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない。
レベル1（白帯）	どこに連絡するべきか想定がない。決まっていない。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：



工場セキュリティIR訓練シナリオ素材②

-変更作業の盲点。NW帯域の逼迫-

工場セキュリティIR訓練 進め方に関するご紹介

【進め方（概要）】

- 工場内で起こりうる架空のインシデントをタイムラインで順次提示します。そのタイミングごとに何を実施すべきか/どのようなことを考えるか、感じたかなどチーム内で議論してください。
- 演習パート完了後に、全体の振り返り・ポイント解説をファシリテーターより実施します。

【演習のステップ・目安時間】

- オープニング **10分** ➡ 演習タイム **35分** ➡ 解説/振り返り・クロージング **40分**



シナリオ② 状況付与/Timeline-1（15時00分）

検討時間

5min

【FSIRTメンバー】を対象として、下記のようなメールが届いた。

メール [X]



速報：工場生産管理システム機能不良（応答遅延）
工場セキュリティインシデント対応チーム<fsirt-irt@jp.company.com>
宛先：fsirt-all@jp.company.com
cc：factory-management@jp.company.com

2024年3月15日(金) 15:00

各位

お疲れ様です。
下記の事象に関して情報共有致します。

【発生事象】
工場内のいくつかのシステムで応答遅延が発生。
各システムは完全には停止していないが、通常の業務は遂行できない状態。

【原因、今後の対応】
原因不明。解決に向けて、FSIRTを中心として調査を継続中。

【依頼事項】
各ライン長は気づいた点をFSIRTメーリングリストまでお送りください。

以上。

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
工場内ではどのような情報共有がなされそうでしょうか。

シナリオ② 状況付与/Timeline-2（15時30分）

検討時間

5min

【FSIRTメンバー】を対象としたメールが届いてから30分が経過した。
まだ原因の特定には至っていないのか、続報のメールは届かない。
工場の生産は引き続き影響を受けているようで、生産設備の一部は安全確保のため、各設備の責任者が製造の一時停止に必要な作業の準備を開始した。
工場のメンバーのみでは、原因の特定が困難な可能性が出てきた。

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
（だれが、何を実施すべきでしょうか）

シナリオ② 状況付与/Timeline-3（16時00分）

検討時間

10min

原因調査をおこなうため、工場内のネットワーク通信の状況について【IT部門】に確認を依頼することになった。【IT部門】によるネットワーク通信ログの確認中であるが、インシデント緊急対策本部に参加していた、【情報セキュリティ部門】のメンバーより下記のコメントがあった。

【情報セキュリティ部門 インシデント対応担当者】

「外部から工場内のネットワークにアクセスできる“入口”は、本社のIT部門が管理しているもの以外に何がありますか？外部からの遠隔保守の経路などはどうでしょうか？それらの通信経路を管理するベンダーへの問合せ、ログ確認などはできていますか？今日は何か変更作業などはおこなっていませんか？」

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
（だれが、何を実施すべきでしょうか）

シナリオ② 状況付与/Timeline-4（16時30分）

検討時間

5min

【IT部門】によるネットワーク通信ログの確認結果、システムAから、システムAとの接続がある機器すべてに対して双方向の大量の通信トラフィックが発生し、そのために工場内のネットワークで輻輳が発生していることがわかった。

* 輻輳（ふくそう）：電話やデータ通信といった通信が同時に集中してしまい（通常通りに処理できなくなり）通信困難に陥る状況

* システムA：議論上、必要に応じて、工場内の具体的なシステム名で検討頂いても結構です

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
（だれが、何を実施すべきでしょうか）

シナリオ② 状況付与/Timeline-5（17時00分）

検討時間

10min

システムAでは当日、システムのファームウェアバージョン作業をおこなったのち、当該機器を再起動した。その再起動後に、大量のトラフィックが発生していたものと判明した。本変更作業の実施については、担当者とその上長の2名しか詳細を把握していなかった。インシデント緊急対策本部では今後の再発防止策について話し合いがおこなわれた。

（状況付与は以上です。この後は振り返り/解説編になります）

**どのような点が今回のインシデントの課題、原因と考えられますか？
インシデント緊急対策本部では、どのような再発防止策を提案すべきでしょうか？**

工場セキュリティIR訓練シナリオ素材②

解説編

シナリオ② 解説

今回は、外部からのサイバー攻撃起因ではなく、社内での事前検証不足・不注意により発生したインシデントをベースにシナリオを構成した。

本ケースの問題点①：

工場内関係者への情報連携が不十分

ファームウェアバージョンアップ作業に関して、一部の担当者を除き、その作業実施を十分に認識できていなかった。

本ケースの問題点②：

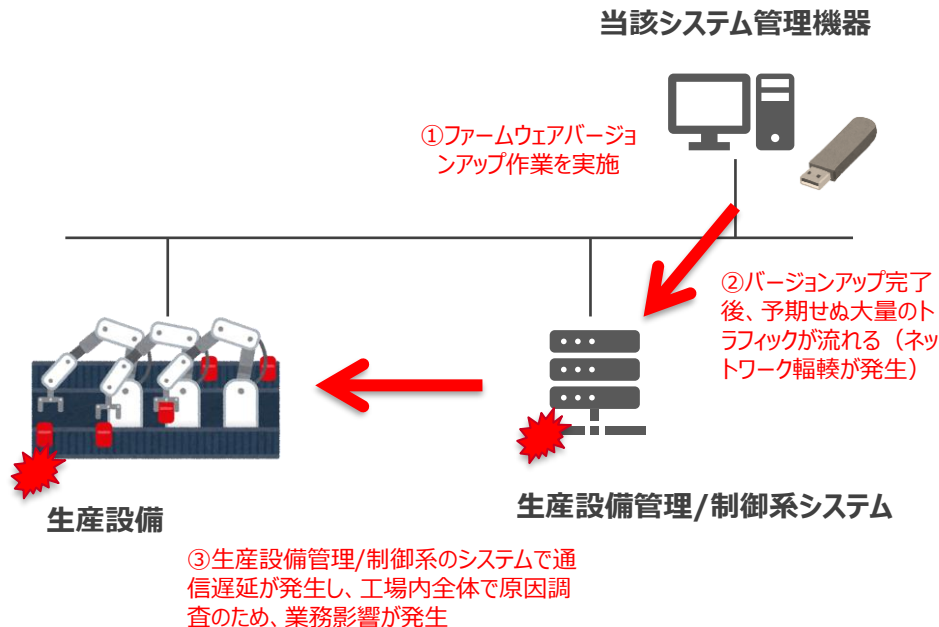
ベンダーマネジメントの不足

作業を完全に委託先のベンダーに任せきりにしており、担当者は何の作業を実施しているのか、どのような影響が発生しうるのかのベンダーとの事前のすり合わせが不足していた。また、何時何分にどのような作業をおこなったのか、詳細な作業実績管理/記録ができていなかったことも、インシデント原因の切り分けに時間を要した。

本ケースの問題点③：

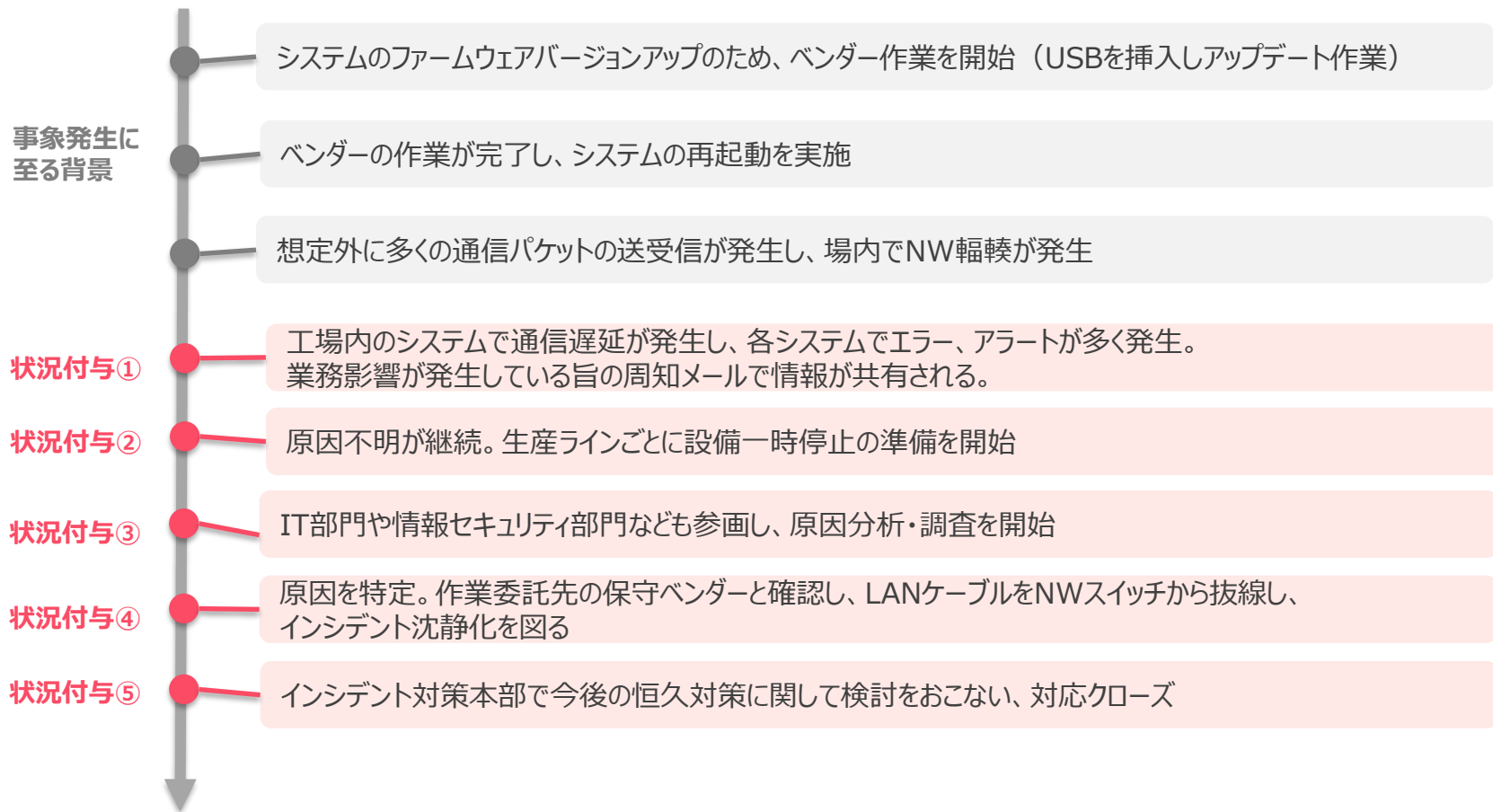
変更作業実施時の工場内ルール未整備／周知不足

変更作業を実施する際、可能であれば、当該機器を場内NWから切り離れた（LANケーブル抜線した）うえで、作業をおこなうことが望ましいという場内ルールがあった。また、変更作業を実施する際の工場内での事前承認・確認プロセスが整備されていなかったことも改善の余地があった。



シナリオ② 状況付与/Timelineの全体像

82



シナリオ② 期待する行動例

状況付与	期待する行動（主要なもの）の例
① 工場内の緊急放送、生産設備管理システムの応答遅延	- 工場内における詳細な情報収集、コミュニケーションを開始。関連するグループへの相談・連絡の実施 - インシデント対応マニュアルの確認
② 最初のメールから30分経過、原因不明が継続	リスク管理部門、本社IT部門、情報セキュリティ部門などへの連絡/追加連絡、情報共有
③ 原因分析、大量のトラフィック発生元のシステムを特定へ	- 工場内での当日のすべての変更作業の洗い出し “入口”に関する総点検 - 遠隔保守関連の通信機器についてベンダーへ状況共有、確認 - 資産管理台帳、ネットワーク物理構成図の確認 - 当該システムと接続されている機器/通信経路の把握
④ 作業委託先の保守ベンダーと確認し、LANケーブルをNWスイッチから抜線	- 当該システムの通信が遮断されることに関する2次被害の発生の可能性を確認。 - 保守運用ベンダーの担当者へのLANケーブル抜線など - 変更作業実施時のベンダー推奨確認事項の再チェック
⑤ インシデント対策本部で今後の恒久対策に関して検討をおこない、対応クローズ	- 工場内での変更作業実施に関する関連部門への情報共有ルール整備 - 本番作業に関する承認プロセス/ルールの整備、見直し、再周知等 - ベンダーへの原因調査・再発防止策に関する報告書の提出依頼 - JPCERT/CCへのインシデント事例の共有/報告/相談

※補足：「JPCERT/CCへのインシデント事例の共有/報告/相談」について、状況付与⑤の期待する行動例として設定していますが、各社のインシデント対応／フォレンジック体制などから、各社で最適なタイミングを判断し、JPCERT/CCへコンタクトすることが良いでしょう。

シナリオ② 成熟度セルフチェックシート 主なチェック項目

成熟度セルフチェックシート項目一覧		
被害シナリオの想定	インシデント対応体制	役割の定義と合意
連絡方法の確立	インシデント対応マニュアルの整備と周知	制御システムに影響がある インシデント対応訓練/演習
サプライチェーンリスク管理	継続的なアウェアネス向上	外部専門機関との連携
モニタリング・検知	持ち込み機器の検査	データ分類
資産管理（IT/OT）	ネットワーク構成管理	システムへのアクセス制御
マルウェアへの対処・駆除	脆弱性管理	機器セキュリティ更新
物理的セキュリティ （入退場管理）	不要なUSBポート閉塞	サーバラック、HUBボックス等の施錠
ネットワークゾーニング（セグメンテーション）	バックアップ取得	バックアップデータの保管
リストア	外部記憶媒体の管理（USBメモリ等）	バイ・デザインのアプローチ
セキュリティアセスメント	システムアカウント管理	ペネトレーションテスト
制御システムに関する専門教育、 キャリアパスの整備	変更作業実施時の承認プロセスの整備	内部犯行への対策

シナリオ② 成熟度セルフチェックシートを活用した振り返りノート

	役割の定義と合意
レベル5（黒帯）	生産停止を決定できる最上位者も含め決まっており、定期的な見直しや確認をおこなっている。
レベル4（茶帯）	生産停止を決定できる最上位者も含め決まっているが、定期的な見直しや確認をおこなっていない。
レベル3（緑帯）	現場担当者レベルではある程度決まっているが、定期的な見直しや確認をおこなっていない。
レベル2（黄帯）	社内で議論、検討したことはあるが、まだ決定に至っていない。
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	速報メールを受信したタイミングから、設備故障以外の可能性も視野に、あらかじめ決められている意思決定者を巻き込んだ形で、今後の工場稼働継続に関して議論することを想定できた。生産停止を決定できる最上位者等に関して定義したドキュメントも直ちに取り出せた。
レベル4（茶帯）	速報メールを受信したタイミングから、設備故障以外の可能性も視野に、あらかじめ決められている意思決定者を巻き込んだ形で、今後の工場稼働継続に関して議論することを想定できた。生産停止を決定できる最上位者等に関して定義したドキュメントを探し出すのに時間を要した。
レベル3（緑帯）	過去に生産停止を決定できる最上位者を定義していたが、その決定内容を記載したドキュメントは見つからなかった。緊急対策会議に参加しているメンバーで今後の工場稼働継続に関して議論することは想定できた。
レベル2（黄帯）	生産活動の停止等に関する明確な役割が定義されておらず、緊急対策会議の中で、はじめて議論・検討することとなった。
レベル1（白帯）	生産活動の停止等に関する明確な役割が定義されていない。演習内でも、今後の生産活動に関する検討の必要性に関する議論は一切なかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ② 成熟度セルフチェックシートを活用した振り返りノート

	連絡方法の確立
レベル5（黒帯）	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備し、定期的に機能するか検証、訓練している。
レベル4（茶帯）	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備している。
レベル3（緑帯）	連絡網（複数の連絡手段を想定）を作成している。
レベル2（黄帯）	連絡網（連絡手段1つ）を作成している。
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	速報メールを受信したタイミング以降、あらかじめ決められた連絡方法によって、すべての関係者に対して直ちに情報伝達した。
レベル4（茶帯）	速報メールを受信したタイミング以降、すべての関係者に対して直ちに情報伝達したものの、連絡方法はインシデント発生時に決めて対応した。
レベル3（緑帯）	速報メールを受信したタイミング以降、主要なメンバーには情報伝達されたが、関係者全員には情報が行き渡らなかった。
レベル2（黄帯）	速報メールを受信したタイミング以降、自身と普段から繋がりのある数名のメンバーへ個別に連絡し、情報収集を試みた。
レベル1（白帯）	速報メールを受信したタイミング以降、影響のあった生産ラインの関係者のみ詳細な状況を把握しており、工場内で円滑な情報共有ができなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ② 成熟度セルフチェックシートを活用した振り返りノート

	インシデント対応マニュアルの整備と周知
レベル5（黒帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。
レベル4（茶帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。
レベル3（緑帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。
レベル2（黄帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルは存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。
レベル1（白帯）	何も存在しない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	サイバー攻撃についても考慮された生産設備でのインシデントマニュアルが存在する。定期的に関係者で読み合わせなど内容確認をおこなっているので、スムーズに演習内でも参照できた。
レベル4（茶帯）	サイバー攻撃についても考慮された生産設備でのインシデントマニュアルが存在する。演習内で確認しようとしたが、初めて読むので理解に時間を要した。
レベル3（緑帯）	サイバー攻撃は考慮していない生産設備でのインシデントマニュアルは存在する。演習内で確認した。
レベル2（黄帯）	サイバー攻撃は考慮していない生産設備でのインシデントマニュアルは存在するが、確認しようとしなかった。
レベル1（白帯）	インシデント対応マニュアルが存在しなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ② 成熟度セルフチェックシートを活用した振り返りノート

	持ち込み機器の検査
レベル5（黒帯）	工場内での運用ルールが策定されており、十分に周知されている。外部から持ち込まれる機器（USB、PC等）は都度、セキュリティチェックがおこなわれ、安全性が担保されたうえで、接続、利用することが徹底されている。
レベル4（茶帯）	工場内での運用ルールが策定されているが、周知活動が未だ十分ではない。外部から持ち込まれる機器（USB、PC等）は多くのケースで都度、セキュリティチェックがおこなわれ、安全性が担保されたうえで、接続、利用されている。
レベル3（緑帯）	工場内での運用ルールを策定し、一部の部署でルールに基づいた運用がおこなわれつつある。
レベル2（黄帯）	工場内での運用ルールは策定されているが、形骸化しており、セキュリティ対策状況が不明な機器（USB、PC等）の持ち込み、利用が可能な状態となっている。
レベル1（白帯）	工場内での運用ルールがなく、特段の確認をおこなわず、セキュリティ対策状況が不明な機器（USB、PC等）の持ち込み、利用を可能な状態となっている。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	状況付与⑤の再発防止策の検討の中などで、今回のインシデントと直接的な関係はないものの、持ち込みUSBメモリや保守用端末の利用前のセキュリティチェックに関して、改めて工場内プロセスについて問題がないことを議論、確認することができた。（※インシデントの原因そのものに限定せず、その周辺のリスクとなり得る要因に対して、幅広く目配りができていた）
レベル4（茶帯）	持ち込みUSBメモリや保守用端末の利用前のセキュリティチェックに関して、場内でルールが定まっているが、演習内では特に議論されなかった。
レベル3（緑帯）	持ち込みUSBメモリや保守用端末に関して、工場内設備への接続に際しての運用ルールを定めよう対応中で、演習内でも話題となった。
レベル2（黄帯）	持ち込みUSBメモリや保守用端末に関して、工場内設備への接続に際しての運用ルールを定めようとしているが、演習内では特に議論されなかった。
レベル1（白帯）	持ち込みUSBメモリや保守用端末に関して、工場内設備への接続に際しての運用ルールがなく、これまでにセキュリティ対策を検討したこともない。演習内でも特に議論されなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ② 成熟度セルフチェックシートを活用した振り返りノート

	資産管理 (IT/OT)
レベル5 (黒帯)	資産管理を自動化、効率化する仕組みが導入されており、新たな資産が自動的に検出され、資産管理台帳へ更新される。インシデント発生時には、資産管理台帳をすぐに取り出せる。
レベル4 (茶帯)	資産管理台帳を作成しており、四半期に1回程度、手動で棚卸をおこない最新化するようにしている。
レベル3 (緑帯)	資産管理台帳を作成しており、年に1回程度、手動で棚卸をおこない最新化するようにしている。
レベル2 (黄帯)	資産管理台帳を過去に作成したことがあるが、その後、一度も更新されていない。
レベル1 (白帯)	資産の可視化をしたことがない。資産管理台帳は無い。

本シナリオにおける到達目標の設定例	
レベル5 (黒帯)	資産管理台帳をすぐに取り出すことができ、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル4 (茶帯)	過去に作成した資産管理台帳がどこにあるのかわからず、見つけ出すのに時間を要したが、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル3 (緑帯)	工場内で統合された資産管理台帳はなく、各部門/生産ラインごとに作成しているため、それらを確認したが、かなり時間を要した。
レベル2 (黄帯)	資産管理台帳などドキュメント類はないものの、環境を把握しているメンバーの知識をもとに、インシデントの影響範囲や原因分析を試みた。
レベル1 (白帯)	資産管理台帳や、環境を把握したメンバーが社内不存在せず、インシデントの影響範囲の確認や原因調査が難航した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り&次回に向けての課題：

シナリオ② 成熟度セルフチェックシートを活用した振り返りノート

	ネットワーク構成管理
レベル5（黒帯）	工場全体のネットワーク物理構成図、設計図があり、定期的に最新化されており、インシデント発生時にはすぐに取り出せる。また影響範囲について想定することができる。
レベル4（茶帯）	工場全体のネットワーク物理構成図、設計図を作成したことがあるが、その後、更新していないので、現状の構成と乖離している可能性がある。
レベル3（緑帯）	工場全体のネットワーク物理構成図、設計図は無いが、自身が担当しているライン/領域については、各担当が接続構成、影響範囲を含め個別に把握している（ドキュメント化されていない）。
レベル2（黄帯）	ネットワーク機器の配置場所や管理部門を把握している（ドキュメント化されていない）。
レベル1（白帯）	ネットワーク機器がどこにあり、誰が管理しているのか全くわからない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	工場全体のネットワーク物理構成図、設計図をすぐに取り出すことができ、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル4（茶帯）	過去に作成した工場全体のネットワーク物理構成図、設計図がどこにあるのかわからず、見つけ出すのに時間を要したが、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル3（緑帯）	ネットワーク構成図は各システムごとに作成しており、それらを使用した。しかし、工場全体を俯瞰したものではないため、インシデントの影響範囲の確認や原因調査には活用できなかった。もしくは利用したが、かなり時間を要した。
レベル2（黄帯）	ネットワーク構成図などドキュメント類はないものの、環境を把握しているメンバーの知識をもとにインシデントの影響範囲や原因分析を試みた。
レベル1（白帯）	ネットワーク構成図のようなものは一切存在しないため、インシデントの影響範囲の確認や原因調査に活用できなかった。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ② 成熟度セルフチェックシートを活用した振り返りノート

	変更作業実施時の承認プロセスの整備
レベル5（黒帯）	変更管理手順が文書化されている。当該領域に関する専門的な知見を有する者を含めた確認者による承認プロセス（多段階承認）が整備、徹底されている。変更作業の計画時には、開発・検証環境での作業内容の事前確認などにより、変更による影響の分析を十分におこない、発生する可能性のある事象に対して、対応策および回避策が計画され、リスクの最小化が図られている。変更作業の実施前には、あらかじめ決められた連絡手段・方法で、工場内へ変更作業の内容、詳細な作業実施スケジュール、当該作業に関する責任者・問合せ先に関する情報共有をおこない、万が一の際にも、迅速なコミュニケーションが可能となるようにしている。
レベル4（茶帯）	変更管理手順が文書化されている。当該領域に関する専門的な知見を有する者を含めた確認者による承認プロセス（多段階承認）が整備、徹底されている。開発・検証環境は存在しないため、ベンダーの公開・保有情報および机上で、変更による影響の分析をおこない、発生する可能性のある事象に対して、対応策および回避策が計画され、リスクの最小化が図られている。変更作業の実施前には、あらかじめ決められた連絡手段・方法で、工場内へ変更作業の内容、詳細な作業実施スケジュール、当該作業に関する責任者・問合せ先に関する情報共有をおこない、万が一の際にも、迅速なコミュニケーションが可能となるようにしている。
レベル3（緑帯）	変更管理手順が文書化されており、当該領域に関する専門的な知見を有する者を含めた確認者による承認プロセス（多段階承認）も準備されているが、社内での運用が徹底されていない。変更作業の実施前には、担当者が任意の手段・方法により、工場内へ変更作業の内容、詳細な作業実施スケジュール、当該作業に関する責任者・問合せ先に関する情報共有をおこない、万が一の際にも、迅速なコミュニケーションが可能となるようにしている。
レベル2（黄帯）	変更作業の進め方に関する正式なプロセスは特に存在しておらず、都度、個別に相談しながら進めている。変更作業を実施する際には、周知・連絡方法は定まっていなかったものの、工場関係者に幅広く事前の情報共有を図るよう心掛けている。
レベル1（白帯）	変更作業の進め方に関する正式なプロセスは特に存在しておらず、都度、個別に相談しながら進めている。変更作業を実施する際には、所属部門コミュニティ内で事前周知している。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	工場内で変更作業を実施する際の手順や承認プロセスが確立されている。また、変更作業実施に関する場内の事前周知に関する方法も定められている。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	工場内で変更作業を実施する際の手順や承認プロセスが確立されている。変更作業の実施に関する場内の周知方法は特に決まっていなかったが、各担当により必ず何らかの全体周知がおこなわれる文化となっている。本シナリオのような状況が発生する可能性は低いことを確認した。
レベル3（緑帯）	工場内で変更作業を実施する際の手順や承認プロセスが確立されている。変更作業の実施に関する場内の周知方法は特に決まっておらず、時折、認識していない変更作業がおこなわれていることがある。本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	工場内で変更作業を実施する際の手順、承認プロセスは一応あるが、あまり利用されておらず形骸化している。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	工場内で変更作業を実施する際の手順、承認プロセス、事前の周知方法に関するルールが特になかった。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ② 成熟度セルフチェックシートを活用した振り返りノート

	外部専門機関との連携
レベル5（黒帯）	JPCERT/CCに加えて、その他各社で個別に契約している、各社のIT/OT環境に関する構成情報を事前に熟知した、インシデント対応/デジタル・フォレンジック/リスクマネジメント専門企業への連絡先を直ちに取り出すことができ、スムーズに連絡、相談できる。
レベル4（茶帯）	JPCERT/CCへの連絡先を直ちに取り出すことができ、スムーズに連絡、相談できる。
レベル3（緑帯）	既存の生産設備の保守ベンダーのみへ連絡が可能。
レベル2（黄帯）	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない
レベル1（白帯）	どこに連絡するべきか想定がない。決まっていない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	連絡すべき外部専門機関のリストが整備されており、すぐに取り出す/確認することができた。
レベル4（茶帯）	連絡すべき外部専門機関のリストを整備していたが、保管場所が分からず探すのに時間を要した。
レベル3（緑帯）	連絡すべき外部専門機関のリストを整備を現在、推進している途中。
レベル2（黄帯）	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない。
レベル1（白帯）	どこに連絡するべきか想定がない。決まっていない。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：



工場セキュリティIR訓練シナリオ素材③

-誰のUSBメモリかしら？-

工場セキュリティIR訓練 進め方に関するご紹介

【進め方（概要）】

- 工場内で起こりうる架空のインシデントをタイムラインで順次提示します。そのタイミングごとに何を実施すべきか/どのようなことを考えるか、感じたかなどチーム内で議論してください。
- 演習パート完了後に、全体の振り返り・ポイント解説をファシリテーターより実施します。

【演習のステップ・目安時間】

- オープニング **10分** ➡ 演習タイム **35分** ➡ 解説/振り返り・クロージング **40分**



シナリオ③ 状況付与/Timeline-1（13時00分）

検討時間

10min

【生産管理部】では、【設計図面を制作するシステム】がOTネットワークゾーンにあり、その図面をITネットワークゾーン（通常のオフィス）のPCで使用する際には、USBメモリを使用し、データをコピーし、持ち運びしている。

ある日、いつも使用しているUSBメモリが見当たらず、引き出しの中を探していると、「業務用USBメモリ ●●工場」とラベルされたUSBメモリが見つかった。いつものUSBメモリではないものの、業務用と記載されていること、また、急ぎで対応が必要だったことから、そのUSBメモリを使用し、データの授受をおこなった。

その直後、ITネットワークゾーンで使用しているPCに搭載されているアンチマルウェア製品よりアラートが発報した。**マルウェア検出(自動駆除失敗)**と表示されている。
マルウェアの検出を受けて、当該作業をおこなっていた担当者は、【FSIRT】へ連絡した。

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
実際に発生した場合、工場内ではどのような情報共有がなされそうでしょうか。

シナリオ③ 状況付与/Timeline-2（13時30分）

検討時間

5min

当該作業員から報告を受けてから、30分が経過した。

【FSIRT】が【CSIRT】と協業し調査したところ、現時点では下記の状況であることがわかっている。

- ITネットワークゾーンのPCから外部へ通信を試みるログが検出されていたが、技術的対策により、その不正通信は自動的にブロックされていた。他のPCからは、マルウェア感染に関するアラートは確認されなかった。
- OTネットワークゾーンの機器にはアンチマルウェア製品が導入されていないため、マルウェア感染の全体像、状況をまだ把握できていない。今のところ、工場設備の異常は報告されていない。

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
（だれが、何を実施すべきでしょうか）

シナリオ③ 状況付与/Timeline-3（14時00分）

検討時間

5min

初期報告から1時間が経過した。

OTネットワークゾーンでもマルウェア感染の状況を掌握できつつある。

今回、USBメモリを挿入した【設計図面を制作するシステム】から外部への通信の試みがあったものの、当該システムはインターネットへの接続ができないため、通信は失敗に終わっていた。また、物理的に同一ネットワークに接続されているシステムは少数だったので、持ち運び可能なUSBメモリタイプのセキュリティスキャンツールを用いて確認したところ、同一ネットワーク内に接続していたすべてのシステムにおいて、先に確認されたものと同じマルウェアへの感染が確認された。

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
（だれが、何を実施すべきでしょうか）

シナリオ③ 状況付与/Timeline-4（15時30分）

検討時間

15min

OTネットワークゾーンでのマルウェア駆除作業も完了した。
本インシデントを受けて、【FSIRT】と【CSIRT】は合同で、インシデント再発防止
検討会を開催することとした。

どのような点が今回のインシデントの課題、原因と考えられますか？
インシデント再発検討会では、どのような再発防止策を提案すべきでしょうか？
【FSIRT】の立場から、検討してください

工場セキュリティIR訓練シナリオ素材③

解説編

シナリオ③ 解説

今回は、工場内では多く使用されている「USBメモリ」を題材としたシナリオを構成した。USBメモリは非常に便利である一方で、セキュリティインシデントの温床にもなりつつある。物理的に分離されたネットワーク間のデータ移動を低コスト、かつ簡便におこなうことができるため、直ちにUSBメモリ等の外部記憶媒体を完全に廃止することは困難かもしれないが、**外部記憶媒体を使用する際のマニュアルを整備し場内へ周知するなど、本リスクについては優先度高く、対策強化・改善をおこなってほしい。**

本ケースの問題点①：

工場内における外部記憶媒体利用のルール未整備

定期的にUSBメモリのマルウェア感染確認のためのスキャンを実施し、クリーンであることを確認してから使用する必要がある。また、USBメモリは事前に資産登録されたものだけが使用できるような制御（技術的対策）を実施しておくことが望ましい。

本ケースの問題点②：

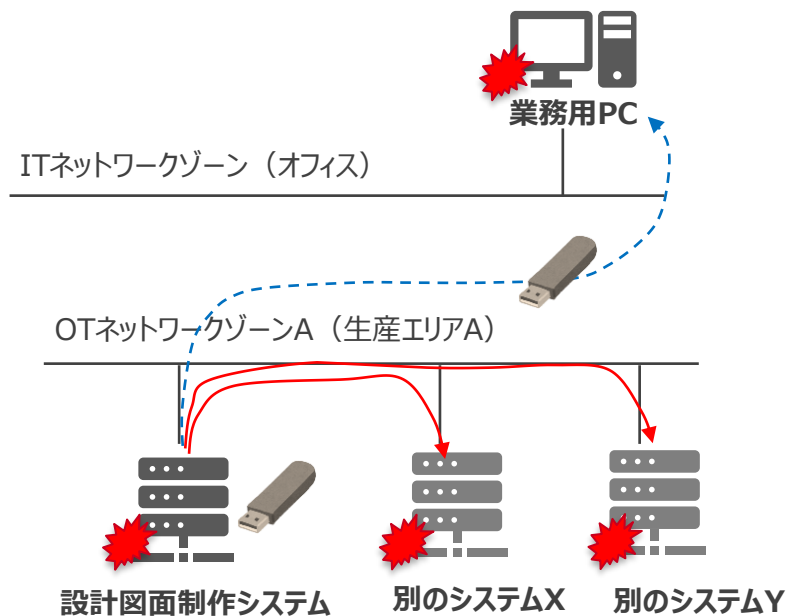
作業担当者のアウェアネスの不足

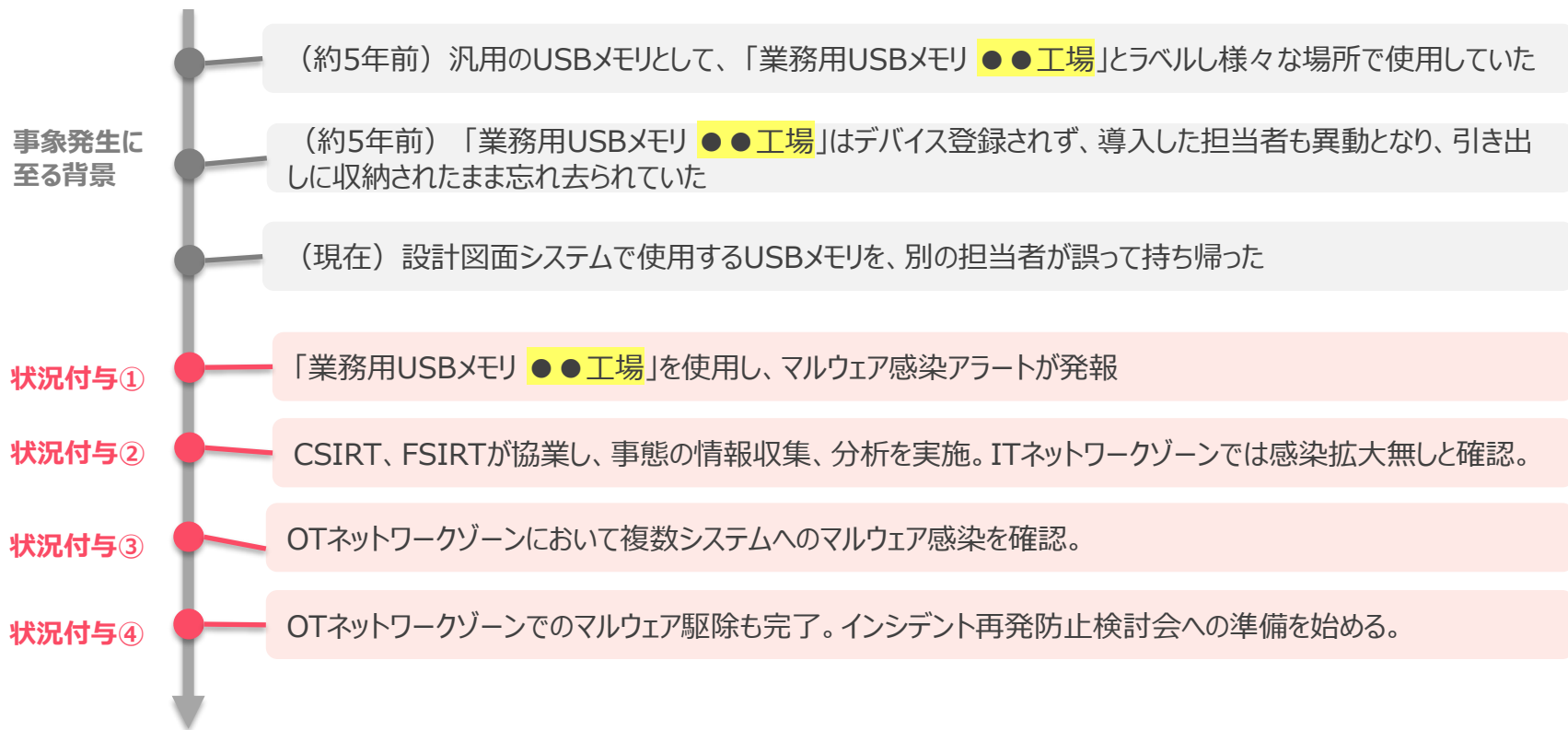
見慣れないUSBメモリを使用しない等の基本的な作法や、USBメモリ使用時のマルウェア感染確認のためのスキャン手順の周知など含め、USBメモリを使用する全従業員のアウェアネスを高めるための施策を検討する必要がある。

本ケースの問題点③：

OTネットワークゾーン内で通信制御がない

今回のシナリオではITネットワーク内の各端末間での感染拡大は確認されなかったが、OTネットワーク内では同一ネットワーク内のシステム間ですべての通信が許可されており、感染拡大の要因となった。通信制御の実装を検討する必要がある。





シナリオ③ 期待する行動例

状況付与	期待する行動（主要なもの）の例
① 見知らぬUSBメモリを使用し、マルウェア感染アラートが発報	- インシデント対応マニュアルの確認 - 当該作業員への詳細ヒアリング - FSIRTチームメンバー内での情報共有 - 当該感染端末を再スキャン/マルウェア駆除を試みる。必要に応じてコーポレートネットワークから当該感染端末を隔離 - CSIRTへ依頼し、ITネットワークゾーン監視システムでアラートを確認（別のPCやサーバへの影響有無を確認） - FSIRTメーリングリスト等を使用し、工場内の関係者へ本インシデントに関する情報共有（生産設備への何らかの異常が確認された場合に早期に連絡をもらえる体制を整備） - いつも使用していたUSBメモリが盗難された可能性も含め、利用部門へ調査を依頼（内部不正に関する考慮）
② FSIRT、CSIRTの調査によりITネットワークゾーンでの感染拡大がないことを確認	- 資産管理台帳、ネットワーク物理構成図の確認 - FSIRTメーリングリスト等を使用し、工場内の関係者へ本インシデントに関する進捗の共有を継続（生産設備への何らかの異常が確認された場合に早期に連絡をもらえる体制を整備） - 持ち運び可能なセキュリティスキャン／マルウェア駆除ツールの使用準備を開始（定義ファイルの最新化ができているか確認する等）
③ OTネットワークゾーンにおいて複数システムへのマルウェア感染を確認	- 当該感染システムの保守ベンダーへ連絡し対処方法を相談する - 持ち運び可能なセキュリティスキャン／マルウェア駆除ツールを用いて、マルウェア駆除を実施する
④ OTネットワークゾーンでのマルウェア駆除も完了。インシデント再発防止検討会への準備	【再発防止に向けた提案例】 - 工場内でのUSBメモリなど外部記憶媒体の利用実態を調査、棚卸を行い、デバイス管理簿を作成する。また、管理部門を決定し、定期的な棚卸がおこなわれる体制を構築する - 工場内でのUSBメモリ利用に関するガイドライン、マニュアルを整備する - 工場内でセキュリティウェアネス向上のためのセミナーやトレーニングなどを企画、実施する - OTネットワークゾーン内におけるシステム間の通信制御の実装を検討する - JPCERT/CCへのインシデント事例の共有/報告/相談

※補足：「JPCERT/CCへのインシデント事例の共有/報告/相談」について、状況付与④の期待する行動例として設定していますが、各社のインシデント対応／フォレンジック体制などから、各社で最適なタイミングを判断し、JPCERT/CCへコンタクトすることが良いでしょう。

シナリオ③ 成熟度セルフチェックシート 主なチェック項目

成熟度セルフチェックシート項目一覧		
被害シナリオの想定	インシデント対応体制	役割の定義と合意
連絡方法の確立	インシデント対応マニュアルの整備と周知	制御システムに影響がある インシデント対応訓練/演習
サプライチェーンリスク管理	継続的なアウェアネス向上	外部専門機関との連携
モニタリング・検知	持ち込み機器の検査	データ分類
資産管理（IT/OT）	ネットワーク構成管理	システムへのアクセス制御
マルウェアへの対処・駆除	脆弱性管理	機器セキュリティ更新
物理的セキュリティ （入退場管理）	不要なUSBポート閉塞	サーバラック、HUBボックス等の施錠
ネットワークゾーニング（セグメンテーション）	バックアップ取得	バックアップデータの保管
リストア	外部記憶媒体の管理（USBメモリ等）	バイ・デザインのアプローチ
セキュリティアセスメント	システムアカウント管理	ペネトレーションテスト
制御システムに関する専門教育、 キャリアパスの整備	変更作業実施時の承認プロセスの整備	内部犯行への対策

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	役割の定義と合意
レベル5（黒帯）	生産停止を決定できる最上位者も含め決まっており、定期的な見直しや確認をおこなっている。
レベル4（茶帯）	生産停止を決定できる最上位者も含め決まっているが、定期的な見直しや確認をおこなっていない。
レベル3（緑帯）	現場担当者レベルではある程度決まっているが、定期的な見直しや確認をおこなっていない。
レベル2（黄帯）	社内で議論、検討したことはあるが、まだ決定に至っていない。
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	FSIRTが連絡を受領したタイミングから、設備故障以外の可能性も視野に、あらかじめ決められている意思決定者を巻き込んだ形で、今後の工場稼働継続に関して議論することを想定できた。生産停止を決定できる最上位者等に関して定義したドキュメントも直に取り出せた。
レベル4（茶帯）	FSIRTが連絡を受領したタイミングから、設備故障以外の可能性も視野に、あらかじめ決められている意思決定者を巻き込んだ形で、今後の工場稼働継続に関して議論することを想定できた。生産停止を決定できる最上位者等に関して定義したドキュメントを探し出すのに時間を要した。
レベル3（緑帯）	過去に生産停止を決定できる最上位者を定義していたが、その決定内容を記載したドキュメントは見つからなかった。緊急対策会議に参加しているメンバーで今後の工場稼働継続に関して議論することは想定できた。
レベル2（黄帯）	生産活動の停止等に関する明確な役割が定義されておらず、緊急対策会議の中で、はじめて議論・検討することとなった。
レベル1（白帯）	生産活動の停止等に関する明確な役割が定義されていない。演習内でも、今後の生産活動に関する検討の必要性に関する議論は一切なかった。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	連絡方法の確立
レベル5（黒帯）	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備し、定期的に機能するか検証、訓練している。
レベル4（茶帯）	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備している。
レベル3（緑帯）	連絡網（複数の連絡手段を想定）を作成している。
レベル2（黄帯）	連絡網（連絡手段1つ）を作成している。
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	FSIRTが連絡を受領したタイミング以降、あらかじめ決められた連絡方法によって、すべての関係者に対して直ちに情報伝達した。
レベル4（茶帯）	FSIRTが連絡を受領したタイミング以降、すべての関係者に対して直ちに情報伝達したものの、連絡方法はインシデント発生時に決めて対応した。
レベル3（緑帯）	FSIRTが連絡を受領したタイミング以降、主要なメンバーには情報伝達されたが、関係者全員には情報が行き渡らなかった。
レベル2（黄帯）	FSIRTが連絡を受領したタイミング以降、自身と普段から繋がりのある数名のメンバーへ個別に連絡し、情報収集を試みた。
レベル1（白帯）	影響のあった生産ラインの関係者のみ詳細な状況を把握しており、工場内で円滑な情報共有ができなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	インシデント対応マニュアルの整備と周知
レベル5（黒帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。
レベル4（茶帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。
レベル3（緑帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。
レベル2（黄帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルは存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。
レベル1（白帯）	何も存在しない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	サイバー攻撃についても考慮された生産設備でのインシデントマニュアルが存在する。定期的に関係者で読み合わせなど内容確認をおこなっているため、スムーズに演習内でも参照できた。
レベル4（茶帯）	サイバー攻撃についても考慮された生産設備でのインシデントマニュアルが存在する。演習内で確認しようとしたが、初めて読むので理解に時間を要した。
レベル3（緑帯）	サイバー攻撃は考慮していない生産設備でのインシデントマニュアルは存在する。演習内で確認した。
レベル2（黄帯）	サイバー攻撃は考慮していない生産設備でのインシデントマニュアルは存在するが、確認しようとしなかった。
レベル1（白帯）	インシデント対応マニュアルが存在しなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	継続的なアウェアネス向上
レベル5（黒帯）	定期的にセキュリティ専門家（情報処理安全確保支援士、CISSP等）から、最新の脅威状況について、社内での発生インシデントやトレンドを含めてインタラクティブなコミュニケーションの機会があり、改善が必要なポイントがあれば速やかに対処している。また、半年に1回以上の頻度で机上訓練、標的型メール訓練、その他の専門的なトレーニングをおこなっている。
レベル4（茶帯）	年に1回程度、社内のセキュリティルール/ポリシーに関するトレーニングを受講している。 また、四半期に1回以上の頻度で机上訓練、標的型メール訓練、その他の追加トレーニングをおこなっている。
レベル3（緑帯）	年に1回程度、社内のセキュリティルール/ポリシー等に関するトレーニングを受講している。 また、半年に1回以上の頻度で机上訓練、標的型メール訓練、その他の追加トレーニングをおこなっている。
レベル2（黄帯）	年に1回程度、社内のセキュリティルール/ポリシー等に関するトレーニングを受講している。
レベル1（白帯）	入社したときに1度セキュリティ研修を受講したが、それ以来、受講した記憶がない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	USBメモリがマルウェア持ち込みの原因の1つとなりうることを工場の全従業員が認識するよう、定期的に工場従業員向けにカスタマイズされた、独自のアウェアネストレーニングをおこなっており、本シナリオのような状況が発生する可能性は非常に低いことを確認した。
レベル4（茶帯）	USBメモリがマルウェア持ち込みの原因の1つとなりうることを工場の全従業員が認識するよう、年1回程度、全社共通のアウェアネストレーニングの中でカバーしている。本シナリオのような状況が発生する可能性が低いことを確認した。
レベル3（緑帯）	年1回程度、全社共通のアウェアネストレーニングはしているが、USBメモリに関する内容は含まれておらず、本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	入社時に1度、セキュリティ教育を受講したが、その後、定期的なアウェアネストレーニングは特に無く、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	アウェアネストレーニングなどは社内ですら実施しておらず、本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	モニタリング・検知
レベル5（黒帯）	アンチマルウェアソフトやEDR等の常時監視のツールを利用しており、LOGの定期確認をしている。さらにFSOC(Factory Security Operation Center)チームもモニタリングしており、1時間以内に検知、対処が可能。
レベル4（茶帯）	アンチマルウェアソフトやEDR等の常時監視のツールを利用しており、LOGの定期確認をしている。数時間以内に対処可能。
レベル3（緑帯）	アンチマルウェアソフトやEDR等の常時監視のツールを利用している。数時間以内に対処可能。
レベル2（黄帯）	定期的に、マルウェア検出・駆除ツールを用いてスキャンしている。
レベル1（白帯）	明らかに目に見えてわかる事象が発生するまで、気づけない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	IT、OTに関わらず、すべてのシステムに常時モニタリングできるアンチマルウェアソフトやEDR等が導入されている。マルウェア感染や不審な振る舞いを検知した際には隔離/駆除が自動的に起こられる設計となっている。またそのアラートはFSOCなどの専門チームが確認している。本シナリオのような状況が発生する可能性は非常に低いことを確認した。
レベル4（茶帯）	ITではある程度の対策が進んでいるが、OT環境では常時モニタリングできるアンチマルウェアソフトやEDR等の導入を現在対応している状況。まだ全体をカバーできていないが、9割以上は対応済みとなっており、残りについても対応の目途がついている。本シナリオのような状況が発生する可能性が低いことを確認した。
レベル3（緑帯）	IT環境での導入が完了している。常時モニタリングできるアンチマルウェアソフトやEDR等について、OT環境への展開を計画しているが、まだ実現できていない。本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	OT環境では常時モニタリングできるツールの導入は重要システムに限られており、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	IT環境、OT環境共に常時モニタリングできるツールが導入されているかどうか不明で、かなり被害が拡大するまで気づくことができないと想定している。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	資産管理 (IT/OT)
レベル5 (黒帯)	資産管理を自動化、効率化する仕組みが導入されており、新たな資産を自動的に検出される。資産管理台帳への更新に活用することができるインシデント発生時には、すぐに取り出せる。
レベル4 (茶帯)	資産管理台帳を作成しており、四半期に1回程度、手動で棚卸をおこない最新化するようにしている。
レベル3 (緑帯)	資産管理台帳を作成しており、年に1回程度、手動で棚卸をおこない最新化するようにしている。
レベル2 (黄帯)	資産管理台帳を過去に作成したことがあるが、その後、一度も更新されていない。
レベル1 (白帯)	資産の可視化をしたことがない。資産管理台帳は無い。

本シナリオにおける到達目標の設定例	
レベル5 (黒帯)	資産管理台帳をすぐに取り出すことができ、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル4 (茶帯)	過去に作成した資産管理台帳がどこにあるのかわからず、見つけ出すのに時間を要したが、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル3 (緑帯)	工場内で統合された資産管理台帳はなく、各部門/生産ラインごとに作成しているため、それらを確認したが、かなり時間を要した。
レベル2 (黄帯)	資産管理台帳などドキュメント類はないものの、環境を把握しているメンバーの知識をもとに、インシデントの影響範囲や原因分析を試みた。
レベル1 (白帯)	資産管理台帳のようなものは一切存在しないため、インシデントの影響範囲の確認や原因調査に活用できなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り&次回に向けての課題：

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	ネットワーク構成管理
レベル5（黒帯）	工場全体のネットワーク物理構成図、設計図があり、定期的に最新化されており、インシデント発生時にはすぐに取り出せる。また影響範囲について想定することができる。
レベル4（茶帯）	工場全体のネットワーク物理構成図、設計図を作成したことがあるが、その後、更新していないので、現状の構成と乖離している可能性がある。
レベル3（緑帯）	工場全体のネットワーク物理構成図、設計図は無いが、自身が担当しているライン/領域については、各担当が接続構成、影響範囲を含め個別に把握している（ドキュメント化されていない）。
レベル2（黄帯）	ネットワーク機器の配置場所や管理部門を把握している（ドキュメント化されていない）。
レベル1（白帯）	ネットワーク機器がどこにあり、誰が管理しているのか全くわからない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	工場全体のネットワーク物理構成図、設計図をすぐに取り出すことができ、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル4（茶帯）	過去に作成した工場全体のネットワーク物理構成図、設計図がどこにあるのかわからず、見つけ出すのに時間を要したが、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル3（緑帯）	ネットワーク構成図は各システムごとに作成しており、それらを使用した。しかし、工場全体を俯瞰したものではないため、インシデントの影響範囲の確認や原因調査には活用できなかった。もしくは利用したが、かなり時間を要した。
レベル2（黄帯）	ネットワーク構成図などドキュメント類はないものの、環境を把握しているメンバーの知識をもとにインシデントの影響範囲や原因分析を試みた。
レベル1（白帯）	ネットワーク構成図のようなものは一切存在しないため、インシデントの影響範囲の確認や原因調査に活用できなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	マルウェアへの対処・駆除
レベル5（黒帯）	持ち運び可能なマルウェアスキャン・駆除ツールが現場にある。パターンファイルも最新に更新されており、誰もがすぐに取り出すことができる。十分な数が配備されている。
レベル4（茶帯）	持ち運び可能なマルウェアスキャン・駆除ツールが現場にある。パターンファイルも最新に更新されており、誰もがすぐに取り出せるものの、配備数が少ない。
レベル3（緑帯）	持ち運び可能なマルウェアスキャン・駆除ツールが現場にあるが、パターンファイルが全く更新されていない。
レベル2（黄帯）	持ち運び可能なマルウェアスキャン・駆除ツールが現場になく、金庫/鍵のかかったキャビネット内に保管されている（利用できる者が限定的）。
レベル1（白帯）	持ち運び可能なマルウェアスキャン・駆除ツールを持っていない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	駆除ツールが現場にあり、パターンファイルも最新に更新されている。誰もがすぐに取り出すことができる状態となっていることを確認できた。
レベル4（茶帯）	駆除ツールが現場にあるものの、パターンファイルの更新作業が行われていない為、すぐには使用できない状態、運用になっていることを確認した。
レベル3（緑帯）	持ち運び可能なマルウェアスキャン・駆除ツールは購入済みではあったが、鍵のかかったキャビネット内に保管しており、鍵の管理者が不在の場合には使用できないケースがあることを確認した。
レベル2（黄帯）	持ち運び可能なマルウェアスキャン・駆除ツールは過去に購入しているが、最近使用しておらず、どこで保管されているのか不明な状態となっていることを確認した。
レベル1（白帯）	持ち運び可能なマルウェアスキャン・駆除ツールを保有しておらず、確認する術がなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	機器セキュリティ更新
レベル5（黒帯）	常に最新版へ更新されている。
レベル4（茶帯）	更新をしているが、一部のシステムでEOLになったままのものがある。ただし、社外には一切繋がっていない。
レベル3（緑帯）	システム導入以来、更新していない。ただし、社外には一切繋がっていない。
レベル2（黄帯）	システム導入以来、更新していない。社外とは、proxy経由でつながっている。
レベル1（白帯）	システム導入以来、更新していない。社外の環境とは直接接続されている。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	常に最新版に更新されている。ゼロデイを除き、機器の脆弱性が原因となるインシデントが発生する可能性は非常に低いことを確認した。
レベル4（茶帯）	基本的に更新をしているが、一部のシステムでEOLになったままのものがある。機器の脆弱性が原因となるインシデントが発生する可能性があることを確認した。
レベル3（緑帯）	社外環境とは一切接続していないものの、システム導入以来、一度も更新していない。機器の脆弱性が原因となるインシデントが発生する可能性があることを確認した。
レベル2（黄帯）	社外とは、proxy経由でつながっている。また、システム導入以来、一度も更新していない。機器の脆弱性が原因となるインシデントが発生する可能性が高いことを確認した。
レベル1（白帯）	社外の環境とは直接接続されている。また、システム導入以来、一度も更新していない。機器の脆弱性が原因となるインシデントが発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	ネットワークゾーニング (セグメンテーション)
レベル5（黒帯）	ファイアウォールに加えて、産業用IDS/IPSも導入されており、不正な通信に関する制御も多層防御となっている。用途ごとにネットワークゾーニング（セグメンテーション）がおこなわれている。
レベル4（茶帯）	ファイアウォールを導入し、用途ごとにネットワークゾーニング（セグメンテーション）をおこなっている。
レベル3（緑帯）	OT領域は他のネットワークと完全に分離している。
レベル2（黄帯）	IT、OTの区分は一応あるが、いわゆる、サーバのNIC2枚刺しで分離しているような状態になっている。
レベル1（白帯）	IT、OTのネットワーク上の区別は無く、すべての通信が制御なく許可されている。インターネットからのアクセスもID、パスワードを知っていれば可能。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	OTネットワークゾーン（セグメンテーション）を設けており、同一ネットワークゾーン内でも各システム間ごとに業務上、必要となる最小限の通信のみを許可している。産業用IDS/IPSも導入されている。本シナリオのような状況が発生する可能性は非常に低いことを確認した。
レベル4（茶帯）	OTネットワークゾーン（セグメンテーション）を設けており、同一ネットワークゾーン内でも各システム間ごとに業務上、必要となる最小限の通信のみを許可している。本シナリオのような状況が発生する可能性が低いことを確認した。
レベル3（緑帯）	OTネットワークゾーン（セグメンテーション）を設けているが、同一ネットワークゾーン内では自由な通信が可能となっている。本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	一応のネットワークゾーニングはあるものの、技術的には不完全/未熟で、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	IT、OTすべての通信が特に制御なく許可されている。本シナリオのような状況が発生する可能性が高いことを確認した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	外部記憶媒体の管理 (USBメモリ等)
レベル5 (黒帯)	許可された外部記憶媒体しか接続しても使用できないように各機器で技術的な対策をおこなっている。また、USBを使用した場合にはログから確認することができる。さらに、年に1回以上、工場内の全部門に外部記憶媒体の棚卸調査(用途、本数、管理者等)をおこない、利用状況/実態の把握をおこなっている。
レベル4 (茶帯)	年に1回以上、工場内の全部門に外部記憶媒体の棚卸調査(用途、本数、管理者等)をおこない、全量の把握をおこなっている。
レベル3 (緑帯)	新規利用開始時には要申請としており、管理台帳で管理している。ただし、管理台帳の定期的な更新はおこなわれていない。
レベル2 (黄帯)	部分的に把握しているが、利用用途の全量を把握できているかどうか定かではない。
レベル1 (白帯)	何をどこで使用しているのか工場全体の実態を全く把握できていない。

本シナリオにおける到達目標の設定例	
レベル5 (黒帯)	許可された外部記憶媒体しか接続しても使用できないように各機器で技術的な対策をおこなっている。昔に購入されたものを含め、すべての外部記憶媒体の棚卸をおこなっており、管理対象外の外部記憶媒体は存在しない。棚卸は年1回継続的におこなっている。本シナリオのような状況が発生する可能性は非常に低いことを確認した。
レベル4 (茶帯)	昔に購入されたものを含め、すべての外部記憶媒体の棚卸をおこなっており、管理対象外の外部記憶媒体は存在しない。棚卸は年1回継続的におこなっている。本シナリオのような状況が発生する可能性が低いことを確認した。
レベル3 (緑帯)	昔に購入されたものを含め、すべての外部記憶媒体の棚卸を過去に1度実施した。その後、定期的な棚卸はおこなっていない。本シナリオのような状況が発生する可能性があることを確認した。
レベル2 (黄帯)	近年に導入されたUSBメモリなど外部記憶媒体は管理できているが、管理体制確立前に購入された昔のものについては、棚卸や管理の対象となっていない。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1 (白帯)	USBメモリなど外部記憶媒体の管理を一切おこなっていない。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	内部犯行への対策
レベル5（黒帯）	IPA発行の『組織における内部不正防止ガイドライン』の内容を参照し、内部不正防止の基本5原則と25分類について理解し、対策例を参考に工場内で内部不正が発生しにくい環境づくりを実践している。
レベル4（茶帯）	IPA発行の『組織における内部不正防止ガイドライン』の内容を参照し、内部不正防止の基本5原則と25分類について、工場内で今後の方針について議論、追加の対応計画策定に着手しており、今後の具体的なアクションや対応スケジュールが明確になっている。
レベル3（緑帯）	IPA発行の『組織における内部不正防止ガイドライン』の内容を参照し、内部不正防止の基本5原則と25分類について、工場内で参照し始めている。
レベル2（黄帯）	内部犯行への対策の必要性を感じており、情報収集は開始しているものの、具体的な対応はできていない。
レベル1（白帯）	従業員に対して性善説で対応しており、何ら対応や検討を社内でおこなっていない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	USBメモリは原則利用を禁止しており、必要なケースではITサポートチームが代理でUSBメモリでのデータコピー対応をおこなうことになっている。またIPAのガイドラインを参考に、内部不正に関する対策もおこなっており、内部不正が発生しにくい環境づくりを推進している。そのため、本シナリオのような状況が発生する可能性は非常に低いことを確認した。
レベル4（茶帯）	通常使用しているUSBメモリが見当たらなかった為、紛失や盗まれた可能性を考え、社内ルールに則り、必要な手続き・報告をおこなった。IPAのガイドラインを参考に、内部不正に関する対策もおこなっており、内部不正が発生しにくい環境づくりを推進している。
レベル3（緑帯）	通常使用しているUSBメモリが見当たらなかった為、紛失や盗まれた可能性を考え、社内ルールに則り、必要な手続き・報告をおこなった。
レベル2（黄帯）	通常使用しているUSBメモリが見当たらなかった為、紛失や盗まれた可能性を考えたが、必要な社内手続きがわからなかった。
レベル1（白帯）	従業員に対して性善説で対応しており、盗まれた可能性は考慮しなかった。通常使用しているUSBメモリが見当たらなかったものの、管理部門への紛失届など手続きや報告も特におこなわなかった。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ③ 成熟度セルフチェックシートを活用した振り返りノート

	外部専門機関との連携
レベル5（黒帯）	JPCERT/CCに加えて、その他各社で個別に契約している、各社のIT/OT環境に関する構成情報を事前に熟知した、インシデント対応/デジタル・フォレンジック/リスクマネジメント専門企業への連絡先を直ちに引き出すことができ、スムーズに連絡、相談できる。
レベル4（茶帯）	JPCERT/CCへの連絡先を直ちに引き出すことができ、スムーズに連絡、相談できる。
レベル3（緑帯）	既存の生産設備の保守ベンダーのみへ連絡が可能。
レベル2（黄帯）	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない
レベル1（白帯）	どこに連絡するべきか想定がない。決まっていない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	連絡すべき外部専門機関のリストが整備されており、すぐに取り出す/確認することができた。
レベル4（茶帯）	連絡すべき外部専門機関のリストを整備していたが、保管場所が分からず探すのに時間を要した。
レベル3（緑帯）	連絡すべき外部専門機関のリストを整備を現在、推進している途中。
レベル2（黄帯）	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない。
レベル1（白帯）	どこに連絡するべきか想定がない。決まっていない。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：



工場セキュリティIR訓練シナリオ素材④

-管理責任者不在のVPN機器-

工場セキュリティIR訓練 進め方に関するご紹介

【進め方（概要）】

- 工場内で起こりうる架空のインシデントをタイムラインで順次提示します。そのタイミングごとに何を実施すべきか/どのようなことを考えるか、感じたかなどチーム内で議論してください。
- 演習パート完了後に、全体の振り返り・ポイント解説をファシリテーターより実施します。

【演習のステップ・目安時間】

- オープニング **10分** ➡ 演習タイム **35分** ➡ 解説/振り返り・クロージング **40分**



シナリオ④ 状況付与/Timeline-1

検討時間

10min

工場セキュリティ実査がおこなわれている。

ある生産設備を管理するシステムに接続され、床に置かれた状態になっている機器に関して実査責任者から、実査立ち合いの【FSIRTメンバー】と以下の会話があった。

実査責任者

「このアンテナのようなものが付いている機器はどのような用途で使用されていますか？」

【FSIRTメンバー】

「資産管理簿で確認します。（確認後）これは掲載されていないかもしれません」

この時点で、【工場セキュリティ推進部門】は何を実施しますか？

シナリオ④ 状況付与/Timeline-2

検討時間

5min

工場内の一通りの目視確認も完了し、翌日、工場セキュリティ実査後ミーティングがおこなわれている。

実査責任者

「アンテナのようなものが付いている機器以外については、特段、大きな問題はみつかありませんでした。その後、あの機器については何かわかりましたか？」

【FSIRTメンバー】

「当該システムの担当者へ確認したところ、外部からベンダーがリモート保守する際に使用するLTEルータとのことでしたが、トライアル利用とのこと、今月中に撤去予定とのことでした。」

実査責任者

「わかりました。ご確認ありがとうございます。」

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
(だれが、何を実施すべきでしょうか)

シナリオ④ 状況付与/Timeline-3

検討時間

5min

1か月後、LTE対応VPNルータ機器が接続されていた生産管理システムが停止した。

状況を確認すると、撤去されるはずだった、外部からベンダーがリモート保守する際に使用するためのLTE対応VPNルータ機器は接続されたままの状態で放置されており、その機器の脆弱性を外部の攻撃者につかれ、システムの重要なプログラムが破壊、パラメータが書き換えられていることが判明した。

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
(だれが、何を実施すべきでしょうか)

シナリオ④ 状況付与/Timeline-4

検討時間

15min

当該システムはバックアップを取得していなかった為、システムの新規再構築を余儀なくされ、完全復旧まで、約2ヶ月を要した。その間、生産ラインは大幅な縮退運転となり、経営へのインパクトも甚大なものとなった。システム再構築にあたっては、既存ベンダーは見直され、別のベンダーと契約を新たに締結し推進した。システム再構築完了後の保守についても、新しいベンダーへ委託する予定である。

現在、工場内ではインシデント再発防止に向けて、外部の有識者も含めたセキュリティ強化タスクフォースが組織され、【FSIRTメンバー】も参画している。来週、初回の方針検討会議が開催される予定となっている。

どのような点が今回のインシデントの課題、原因と考えられますか？
インシデント再発防止検討会では、どのような再発防止策を提案すべきでしょうか？
【FSIRT】の立場から、検討してください

工場セキュリティIR訓練シナリオ素材④

解説編

シナリオ④ 解説

今回は、多くのセキュリティインシデントの原因となっている、「VPN機器の不適切な設定、運用管理」を題材としたシナリオを構成した。VPN機器は社外から、会社のネットワークに入ってくる専用の穴を開けるための機器であり、適切に設定、運用管理されれば多様な働き方の実現や、保守サポートレベルの向上に寄与する。しかし、VPN機器の脆弱性が放置されたり、不適切な設定のままであることを外部攻撃者に突かれて、社内システム侵害の被害に遭っている企業が多い。工場が発生した場合には、生産停止へつながる。**最優先の項目として、工場内のVPN機器利用および管理状況の棚卸、対策強化・改善をおこなってほしい。**

本ケースの問題点①：

VPN機器の利用状況が把握できていない

ベンダーがリモート保守用に設定する機器の通信経路は、IT部門が管理する正規の通信経路以外で、独立した形で構築されるケースも多い。IT部門も見えない穴がひとつできあがっているわけである。自社にとって、24/7の遠隔保守サービスが本当に必要か再考し、もし必要で設置する場合には、当該VPN機器について漏れなく、管理対象とし、資産管理台帳に記載しなければならなかった。

本ケースの問題点②：

VPN機器の脆弱性に対処する責任者の定義が曖昧な契約

VPN機器の脆弱性の対処に関して、契約上、役割分担が曖昧になっていた。設備の保守ベンダーが遠隔保守を行うために導入する場合には、当該機器の脆弱性管理を委託先ベンダーの責任でおこなうよう、契約書に明記しておく必要があった。パッチ適用/セキュリティプログラムの更新などの作業実施の対応手順はあらかじめ、委託先と確認し、合意しておく方がよい。

本ケースの問題点③：

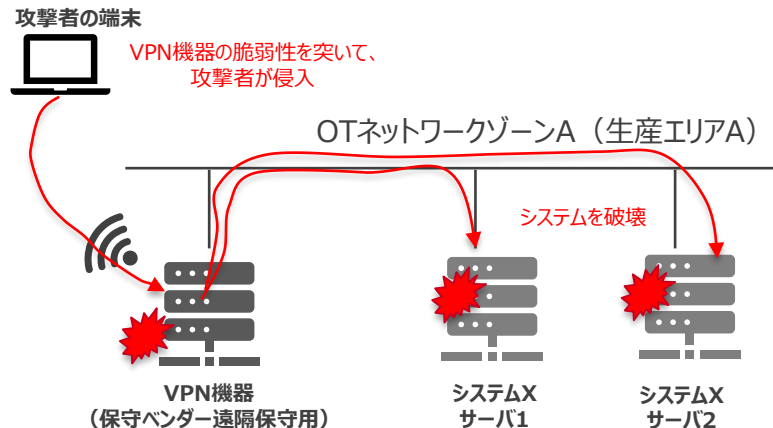
重要なシステムのバックアップ未取得、リストア不可

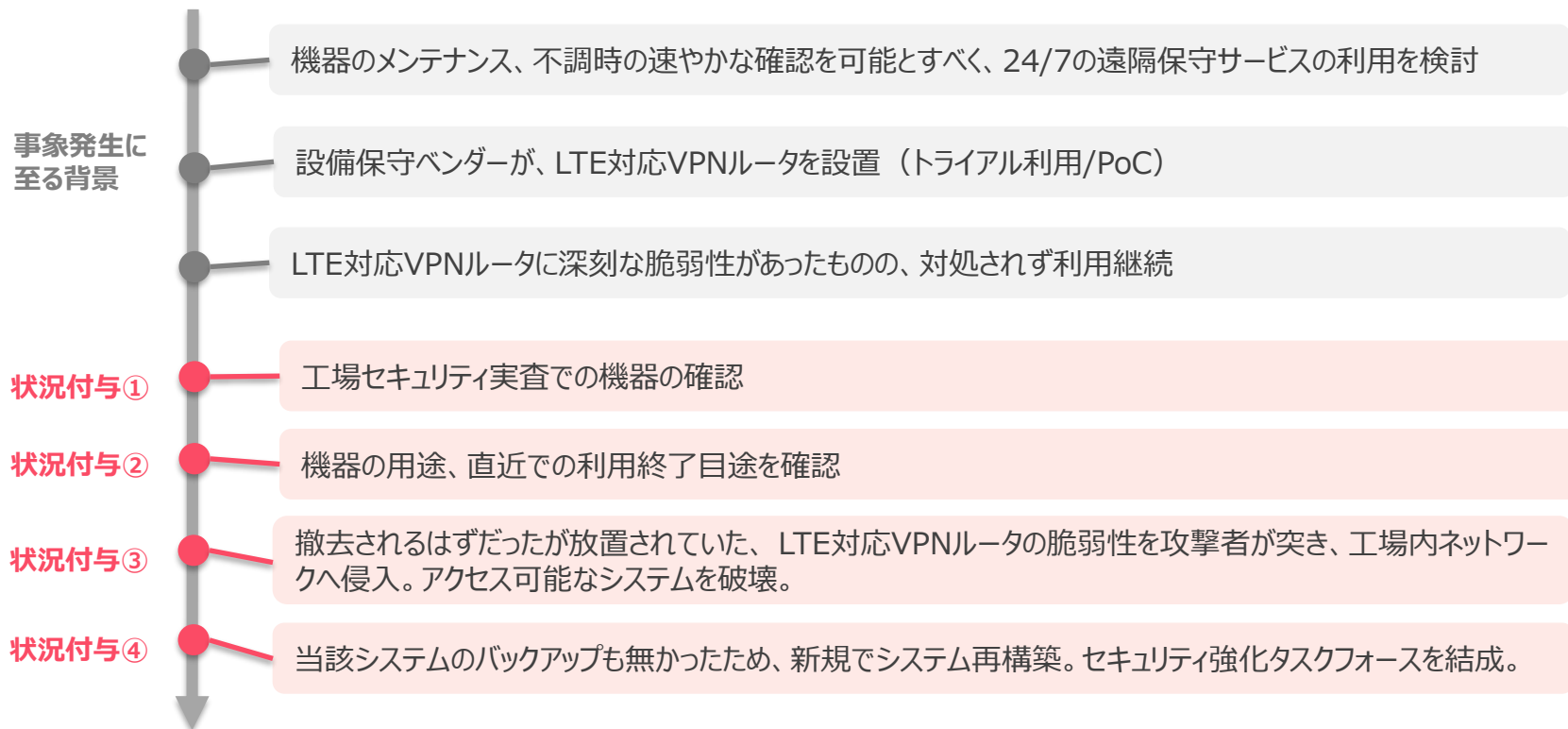
今回のシステムではバックアップが一切取得されておらず、当然ながら、システム復旧時に通常おこなわれるバックアップデータからのリストア作業も不可能な状況だった。このようなケースではゼロからシステムの再構築をおこなわざるを得ない場合もあり、時間を要する。システム再構築が完了するまで業務が停滞し、経営へのインパクトは大きくなる。

本ケースの問題点④：

バイ・デザイン、セキュリティの文化が工場内に浸透していない

実査で指摘後も1か月以上にわたって放置されており、セキュリティへの認識が不十分と言わざるを得なかった。また、このような新たな通信経路の設置や新規のシステム導入時にはセキュリティの専門家が企画・検討フェーズから参画する、バイ・デザインのアプローチで対応するべきだった。





シナリオ④ 期待する行動例

状況付与	期待する行動（主要なもの）の例
① 工場セキュリティ実査（今回のインシデントの発生を防ぐ最後のチャンスだった）	・ インシデント対応マニュアルの確認 ・ 当該生産システムの管理責任者へ、謎の機器に関する詳細ヒアリング ・ 資産管理台帳、ネットワーク物理構成図の確認
② 機器の用途、直近での利用終了用途を確認	・ 当該生産システムの管理責任者とFSIRT間で、機器撤去に関する具体的なスケジュールをすり合わせ ・ 機器撤去後の状況を確認する予定について、スケジューラやタスク/プロジェクト管理システム等に登録し、失念することを防止する
③ LTE対応VPNルータの脆弱性を攻撃者が突き、工場内ネットワークへ侵入。アクセス可能なシステムを破壊。	・ 生産システムの管理責任者に確認したうえで、VPN機器を生産設備から切断 ・ 破壊されたシステムの保守ベンダーへ連絡。復旧方法を確認 ・ 当該生産システムの停止に関して、場内の関係者へ全体周知 ・ 他にも同様のVPN機器がないか、場内の関係者へ再度全体ヒアリング
④ 当該システムのバックアップが無く、新規でシステム再構築。セキュリティ強化タスクフォースを結成。	・ 重要なシステムを対象として、バックアップ取得システムを工場内に整備する ・ バックアップデータからのシステムリストア試験をおこなう ・ 新たに契約する保守委託先ベンダーとの契約書内にセキュリティの安全性確保の責任、役割分担に関して明記・合意する ・ 工場内の資産管理簿の更新プロセス徹底のための運用見直し ・ 工場内で新規システム導入時のプロセスを整備、工場内へ周知する（どのようなシステムであっても、導入時には必ず情報セキュリティの専門部門のレビューを受けてから推進する。もしくはプロジェクト企画フェーズから体制に情報セキュリティの専門メンバーを加えて推進する） ・ 社員の戦略的育成を見据えたキャリアパスの設計、スキルアッププログラムなど、工場セキュリティ対策を担うことが可能な社内実務者の増強に繋がる提案をおこなう。 ・ JPCERT/CCへのインシデント事例の共有/報告/相談

※補足：「JPCERT/CCへのインシデント事例の共有/報告/相談」について、状況付与④の期待する行動例として設定していますが、各社のインシデント対応／フォレンジック体制などから、各社で最適なタイミングを判断し、JPCERT/CCへコンタクトすることが良いでしょう。

シナリオ④ 成熟度セルフチェックシート 主なチェック項目

成熟度セルフチェックシート項目一覧		
被害シナリオの想定	インシデント対応体制	役割の定義と合意
連絡方法の確立	インシデント対応マニュアルの整備と周知	制御システムに影響がある インシデント対応訓練/演習
サプライチェーンリスク管理	継続的なアウェアネス向上	外部専門機関との連携
モニタリング・検知	持ち込み機器の検査	データ分類
資産管理（IT/OT）	ネットワーク構成管理	システムへのアクセス制御
マルウェアへの対処・駆除	脆弱性管理	機器セキュリティ更新
物理的セキュリティ （入退場管理）	不要なUSBポート閉塞	サーバラック、HUBボックス等の施錠
ネットワークゾーニング（セグメンテーション）	バックアップ取得	バックアップデータの保管
リストア	外部記憶媒体の管理（USBメモリ等）	バイ・デザインのアプローチ
セキュリティアセスメント	システムアカウント管理	ペネトレーションテスト
制御システムに関する専門教育、 キャリアパスの整備	変更作業実施時の承認プロセスの整備	内部犯行への対策

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	役割の定義と合意
レベル5（黒帯）	生産停止を決定できる最上位者も含め決まっており、定期的な見直しや確認をおこなっている。
レベル4（茶帯）	生産停止を決定できる最上位者も含め決まっているが、定期的な見直しや確認をおこなっていない。
レベル3（緑帯）	現場担当者レベルではある程度決まっているが、定期的な見直しや確認をおこなっていない。
レベル2（黄帯）	社内で議論、検討したことはあるが、まだ決定に至っていない。
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	生産管理システムの停止を検知したタイミングから、設備故障以外の可能性も視野に、あらかじめ決められている意思決定者を巻き込んだ形で、今後の工場稼働継続に関して議論することを想定できた。生産停止を決定できる最上位者等に関して定義したドキュメントも直ちに取り出せた。
レベル4（茶帯）	生産管理システムの停止を検知したタイミングから、設備故障以外の可能性も視野に、あらかじめ決められている意思決定者を巻き込んだ形で、今後の工場稼働継続に関して議論することを想定できた。生産停止を決定できる最上位者等に関して定義したドキュメントも直ちに取り出せた。
レベル3（緑帯）	過去に生産停止を決定できる最上位者を定義していたが、その決定内容を記載したドキュメントは見つからなかった。緊急対策会議に参加しているメンバーで今後の工場稼働継続に関して議論することは想定できた。
レベル2（黄帯）	生産活動の停止等に関する明確な役割が定義されておらず、緊急対策会議の中で、はじめて議論・検討することとなった。
レベル1（白帯）	生産活動の停止等に関する明確な役割が定義されていない。演習内でも、今後の生産活動に関する検討の必要性に関する議論は一切なかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	連絡方法の確立
レベル5（黒帯）	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備し、定期的に機能するか検証、訓練している。
レベル4（茶帯）	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備している。
レベル3（緑帯）	連絡網（複数の連絡手段を想定）を作成している。
レベル2（黄帯）	連絡網（連絡手段1つ）を作成している。
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	FSIRTが連絡を受領したタイミング以降、あらかじめ決められた連絡方法によって、すべての関係者に対して直ちに情報伝達した。
レベル4（茶帯）	FSIRTが連絡を受領したタイミング以降、すべての関係者に対して直ちに情報伝達したものの、連絡方法はインシデント発生時に決めて対応した。
レベル3（緑帯）	FSIRTが連絡を受領したタイミング以降、主要なメンバーには情報伝達されたが、関係者全員には情報が行き渡らなかった。
レベル2（黄帯）	FSIRTが連絡を受領したタイミング以降、自身と普段から繋がりのある数名のメンバーへ個別に連絡し、情報収集を試みた。
レベル1（白帯）	影響のあった生産ラインの関係者のみ詳細な状況を把握しており、工場内で円滑な情報共有ができなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	インシデント対応マニュアルの整備と周知
レベル5（黒帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。
レベル4（茶帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。
レベル3（緑帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。
レベル2（黄帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルは存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。
レベル1（白帯）	何も存在しない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	サイバー攻撃についても考慮された生産設備でのインシデントマニュアルが存在する。定期的に関係者で読み合わせなど内容確認をおこなっているので、スムーズに演習内でも参照できた。
レベル4（茶帯）	サイバー攻撃についても考慮された生産設備でのインシデントマニュアルが存在する。演習内で確認しようとしたが、初めて読むので理解に時間を要した。
レベル3（緑帯）	サイバー攻撃は考慮していない生産設備でのインシデントマニュアルは存在する。演習内で確認した。
レベル2（黄帯）	サイバー攻撃は考慮していない生産設備でのインシデントマニュアルは存在するが、確認しようとしなかった。
レベル1（白帯）	インシデント対応マニュアルが存在しなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	サプライチェーンリスク管理
レベル5（黒帯）	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝え、定期的な契約内容の見直しをおこない、調達先が自社で求められるセキュリティ要件を満たすようにしている。必要な際には調達先の変更も含め幅広く検討し、セキュリティの確保に努めている。また、定期的に調達先の情報セキュリティ管理体制チェック/ヒアリングをおこなっている。
レベル4（茶帯）	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝え、定期的な契約内容の見直しをおこない、調達先が自社で求められるセキュリティ要件を満たすようにしている。必要な際には調達先の変更も含め幅広く検討し、セキュリティの確保に努めている。
レベル3（緑帯）	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝えたことはあるが、調達先から強い拒否感を示され、断念したが、ワークアラウンド/改善策を実施し、セキュリティリスクの軽減を図っている。
レベル2（黄帯）	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝えたことはあるが、調達先から強い拒否感を示され、断念した。
レベル1（白帯）	長年の付き合いのある調達先なので、契約内容は特に見直さず、単純更新している。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	リモート保守用VPN機器に関して、導入した生産設備保守委託先と脆弱性に関する対応を含め、情報セキュリティ管理に関する役割分担を事前に定義、合意できており、契約書にも明記されている。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	リモート保守用VPN機器に関して、導入した生産設備保守委託先と脆弱性に関する対応を含め、情報セキュリティ管理に関する役割分担を事前に定義、合意できているが、契約書には記載されていない。本シナリオのような状況が発生するリスクは低いことを確認した。
レベル3（緑帯）	リモート保守用VPN機器に関して、導入した生産設備保守委託先と脆弱性に関する対応を含め、情報セキュリティ管理に関する役割分担について、議論を開始しており、今後決定予定の見込み。現時点では、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル2（黄帯）	委託先と情報セキュリティリスク管理に関する議論をしたことはあるが、特段なにも取り決めや依頼はしていない。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	委託先と情報セキュリティリスク管理に関する議論をしたことがない。本シナリオのような状況が発生する可能性が高いことを確認した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	資産管理 (IT/OT)
レベル5 (黒帯)	資産管理を自動化、効率化する仕組みが導入されており、新たな資産を自動的に検出される。資産管理台帳への更新に活用することができるインシデント発生時には、すぐに取り出せる。
レベル4 (茶帯)	資産管理台帳を作成しており、四半期に1回程度、手動で棚卸をおこない最新化するようにしている。
レベル3 (緑帯)	資産管理台帳を作成しており、年に1回程度、手動で棚卸をおこない最新化するようにしている。
レベル2 (黄帯)	資産管理台帳を過去に作成したことがあるが、その後、一度も更新されていない。
レベル1 (白帯)	資産の可視化をしたことがない。資産管理台帳は無い。

本シナリオにおける到達目標の設定例	
レベル5 (黒帯)	資産管理台帳をすぐに取り出すことができ、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル4 (茶帯)	過去に作成した資産管理台帳がどこにあるのかわからず、見つけ出すのに時間を要したが、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル3 (緑帯)	工場内で統合された資産管理台帳はなく、各部門/生産ラインごとに作成しているため、それらを確認したが、かなり時間を要した。
レベル2 (黄帯)	資産管理台帳などドキュメント類はないものの、環境を把握しているメンバーの知識をもとに、インシデントの影響範囲や原因分析を試みた。
レベル1 (白帯)	資産管理台帳のようなものは一切存在しないため、インシデントの影響範囲の確認や原因調査に活用できなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り&次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	ネットワーク構成管理
レベル5（黒帯）	工場全体のネットワーク物理構成図、設計図があり、定期的に最新化されており、インシデント発生時にはすぐに取り出せる。また影響範囲について想定することができる。
レベル4（茶帯）	工場全体のネットワーク物理構成図、設計図を作成したことがあるが、その後、更新していないので、現状の構成と乖離している可能性がある。
レベル3（緑帯）	工場全体のネットワーク物理構成図、設計図は無いが、自身が担当しているライン/領域については、各担当が接続構成、影響範囲を含め個別に把握している（ドキュメント化されていない）。
レベル2（黄帯）	ネットワーク機器の配置場所や管理部門を把握している（ドキュメント化されていない）。
レベル1（白帯）	ネットワーク機器がどこにあり、誰が管理しているのか全くわからない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	工場全体のネットワーク物理構成図、設計図をすぐに取り出すことができ、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル4（茶帯）	過去に作成した工場全体のネットワーク物理構成図、設計図がどこにあるのかわからず、見つけ出すのに時間を要したが、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル3（緑帯）	ネットワーク構成図は各システムごとに作成しており、それらを使用した。しかし、工場全体を俯瞰したものではないため、インシデントの影響範囲の確認や原因調査には活用できなかった。もしくは利用したが、かなり時間を要した。
レベル2（黄帯）	ネットワーク構成図などドキュメント類はないものの、環境を把握しているメンバーの知識をもとにインシデントの影響範囲や原因分析を試みた。
レベル1（白帯）	ネットワーク構成図のようなものは一切存在しないため、インシデントの影響範囲の確認や原因調査に活用できなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	脆弱性管理
レベル5（黒帯）	脆弱性管理ツールを導入し、優先付けをおこないシステム各要素の脆弱性に速やかに対処している。
レベル4（茶帯）	ネットワーク機器とサーバOS、システム内に含まれるミドルウェア、OSSの脆弱性対応を手動で管理し対応している。
レベル3（緑帯）	ネットワーク機器とサーバOSの脆弱性対応を手動で管理し対応している。
レベル2（黄帯）	ネットワーク機器だけは脆弱性対応を手動で管理し対応している。
レベル1（白帯）	何をすればよいかわかっているが、具体的な対応策はわからない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	脆弱性管理ツールが導入されており、工場内のすべてのシステムを対象としている。週次などの頻度で、定期的に脆弱性がスキャンされ、優先付けをおこないシステム各要素の脆弱性に速やかに対処している。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	脆弱性管理ツールが導入されている。週次などの頻度で、定期的に脆弱性がスキャンされ、優先付けをおこないシステム各要素の脆弱性に速やかに対処している。ただし、工場内のシステムのカバー率は80%程度で引き続きの導入範囲拡大の対応が必要と認識している。本シナリオのような状況が発生するリスクは低いことを確認した。
レベル3（緑帯）	ネットワーク機器とサーバOSの脆弱性対応を手動で管理し対応している。手動管理のため、確認の頻度も月次程度にとどまっており、本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	ネットワーク機器だけは脆弱性対応を手動で管理し対応している。手動管理のため、確認の頻度も月次程度にとどまっており、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	脆弱性管理について何をすればよいのか具体的にわかっておらず、本シナリオのような状況が発生する可能性が高いことを確認した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	バックアップ取得
レベル5（黒帯）	毎日、バックアップを取得している。バックアップの3-2-1のルールを理解し、バックアップデータを取得している。
レベル4（茶帯）	月次でバックアップを取得している。
レベル3（緑帯）	3か月に1回程度はバックアップを取得している。
レベル2（黄帯）	初回導入時に1回取得したのみで、それ以降、バックアップは取得していない。
レベル1（白帯）	バックアップを取得する運用は一切存在しない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	工場内の重要なシステムに関して、毎日、バックアップが取得できていることを確認した。
レベル4（茶帯）	工場内の重要なシステムに関して、月次でバックアップが取得できていることを確認した。
レベル3（緑帯）	工場内の重要なシステムに関して、3か月に1回程度、バックアップが取得できていることを確認した。
レベル2（黄帯）	初回導入時に1回取得したのみで、それ以降、バックアップは取得していないことを確認した。
レベル1（白帯）	バックアップを取得する運用は一切存在しないことを確認した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	バックアップデータの保管
レベル5（黒帯）	バックアップデータ保管に関する社内統一基準が定まっている。バックアップの3-2-1のルールを理解し、バックアップデータを保管している。バックアップデータをネットワークの観点で分離された別の環境で保管している。ネットワーク上分離されたクラウドサービス上や、外付けハードディスク、磁気テープ等をオフラインで保管し、ランサムウェア被害のリスクを最小化している。さらに、地震などの自然災害も考慮して、システム稼働地域から地理的に離れた遠隔地でも、バックアップデータを保管している。
レベル4（茶帯）	バックアップデータ保管に関する社内統一基準が定まっている。バックアップデータをネットワークの観点で分離された別の環境で保管している。ネットワーク上分離されたクラウドサービス上や、外付けハードディスク、磁気テープ等をオフラインで保管し、ランサムウェア被害のリスクを最小化している。
レベル3（緑帯）	バックアップデータ保管に関する社内統一基準が定まっている。バックアップデータを同一筐体内/同一ネットワーク内の環境下で保管している。
レベル2（黄帯）	バックアップデータ保管に関する社内統一基準が定まっておらず、重要なデータか否かが考慮されないまま、システム導入時のシステム担当者の判断で、様々な形態でバックアップデータが保管されている。
レベル1（白帯）	バックアップデータがどこにあるのかわからない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	バックアップデータ保管に関する社内統一基準が定まっている。バックアップの3-2-1のルールを理解し、バックアップデータを保管できている。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	バックアップデータ保管に関する社内統一基準が定まっている。バックアップの3-2-1のルールを理解しているが、ネットワークから分離したオフラインのバックアップデータは準備できていない。本シナリオのような状況が発生するリスクはあることを確認した。
レベル3（緑帯）	バックアップデータ保管に関する社内統一基準や仕様を定めよう対応を開始している。本シナリオのような状況が発生するリスクはあることを確認した。
レベル2（黄帯）	バックアップデータ保管に関する社内統一基準が定まっておらず、システムごとにバックアップの仕様が様々なため、リスクレベルもシステムによって大きく異なる。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	バックアップデータが取得できているのか、どこにあるのかわからない。本シナリオのような状況が発生する可能性が高いことを確認した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	リストア
レベル5（黒帯）	システム復旧に関する社内統一基準が定まっている。システムが2重化されており、短時間（1時間以内）で復元できる。年に1回程度、重要なシステムに関して、リストアテストをおこなっている。（システム障害が発生しても、ビジネスで許容可能なリスクレベル以下に抑えられている）
レベル4（茶帯）	システム復旧に関する社内統一基準が定まっている。バックアップから短時間（数時間程度）で復元できる。（システム障害が発生しても、ビジネスで許容可能なリスクレベル以下に抑えられている）
レベル3（緑帯）	システム復旧に関する社内統一基準が無い。リストアは可能だが、バックアップからの復元に数日程度かかる。（ビジネスで許容できないリスクレベルとなっている）
レベル2（黄帯）	システム復旧に関する社内統一基準が無い。リストアは可能だが、再インストール、再設定作業等で復旧まで数週間程度かかる。（ビジネスで許容できないリスクレベルとなっている）
レベル1（白帯）	リストアしたことがない。もしくは、そもそも、バックアップデータがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	システム復旧に関する社内統一基準が定まっている。年に1回程度、重要なシステムに関して、リストアテストをおこなっている。1時間以内でシステムを復旧でき、当該ビジネスで許容可能なリスクレベル以下となっていることを確認した。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	システム復旧に関する社内統一基準が定まっている。数時間以内でシステムを復旧することができ、当該ビジネスで許容可能なリスクレベル以下となっていることを確認した。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル3（緑帯）	システム復旧に関する社内統一基準が無い。リストアは可能なはずだがリストアテストを定期的におこなっておらず確信は持てない。システム復旧までに数日程度を要すると確認した。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル2（黄帯）	システム復旧に関する社内統一基準が無い。リストアは可能なはずだがリストアテストを定期的におこなっておらず確信は持てない。システム復旧までに数週間程度を要すると確認した。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	リストアしたことがない。もしくは、そもそも、バックアップデータがない。本シナリオのような状況が発生する可能性が高いことを確認した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	バイ・デザインのアプローチ
レベル5（黒帯）	セキュリティの専門家（情報処理安全確保支援士、CISSP等）が新規のシステムやITを用いた施策について、企画立ち上げ・検討フェーズ初期から参画し、情報セキュリティリスクの観点からアドバイスを受けるようにしている。バイ・デザインのプロセスは、プロジェクトを推進する際の必須事項として、社内ルールに取り込まれている。さらに、社内稟議システムとしても、セキュリティの専門家によるレビューが完了しないと、プロジェクトの発注や推進ができない仕組みになっている。
レベル4（茶帯）	セキュリティの専門家（情報処理安全確保支援士、CISSP等）が新規のシステムやITを用いた施策について、企画立ち上げ・検討フェーズ初期から参画し、情報セキュリティリスクの観点からアドバイスを受けるようにしている。ただし、これは任意で社内ルールにはなっていない。
レベル3（緑帯）	新規のシステムやITを用いた施策について、セキュリティの専門家（情報処理安全確保支援士、CISSP等）に基本的に相談、情報共有することになっているが、プロジェクトの後半、システムリリース直前となることが多い。
レベル2（黄帯）	新規のシステムやITを用いた施策について、セキュリティの専門家（情報処理安全確保支援士、CISSP等）に相談することもあるが、稀である。
レベル1（白帯）	新規のシステムやITを用いた施策について、セキュリティの専門家（情報処理安全確保支援士、CISSP等）が関わることはない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	新規システム導入時には、検証PoCなど一時的なものであっても例外なく、必ず社内の専門部門と事前に相談し、内容を確認するようなバイ・デザインのアプローチが導入されている。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	バイ・デザインのプロセスが存在する。大規模システム導入の際には、社内の専門部門と事前に相談し、内容を確認してもらっている。検証など一時的なものは担当部門のみで進めることもあり、本シナリオのような状況が発生する可能性はあることを確認した。
レベル3（緑帯）	バイ・デザインのプロセスが存在する。ただし、社内ですべてのプロセスに則って対応するかどうかは任意のため、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル2（黄帯）	バイ・デザインのプロセスの導入に向けて、専門部門の立ち上げ、整備を進めている。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	各部門が独自にシステム導入を推進しており、社内ですべての専門家によるレビューなどのバイ・デザインのプロセスは存在しない。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	セキュリティアセスメント
レベル5（黒帯）	1年に1回程度、アセスメントの基準や委託先を変えて、多角的な視点からアプローチし、セキュリティ上の課題を幅広く見出すようにしている。社内のメンバーも積極的にアセスメントに関与しており、日々の簡易アセスメントレベルであれば、内製で対応できるケイパビリティも有している。
レベル4（茶帯）	数年に1回程度、アセスメントの基準や委託先を変えて、多角的な視点からアプローチし、セキュリティ上の課題を幅広く見出すようにしている。社内のメンバーはアセスメントの実務プロセスに関与しない。
レベル3（緑帯）	数年に1回、毎回同じ基準に基づいて、同じ専門企業にアセスメントを委託している。社内のメンバーはアセスメントの実務プロセスに関与しない。
レベル2（黄帯）	過去に1度実施したことがある。
レベル1（白帯）	実施したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	セキュリティアセスメントの重要性を認識し、指摘事項に関しては直ちに対処する体制やルールが工場内で整備されている。本シナリオのように指摘され多事項を放置されることは想定しにくい。また、社内で簡易なセキュリティアセスメントを実施できる体制もあり、セキュリティアセスメントに関する社内の理解や文化が醸成されている。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	セキュリティアセスメントの重要性を認識し、指摘事項に関しては直ちに対処する体制やルールが工場内で整備されている。本シナリオのように指摘され多事項を放置されることは想定しにくい。本シナリオのような状況が発生するリスクは低いことを確認した。
レベル3（緑帯）	セキュリティアセスメントの重要性は多くのメンバーが認識している。一方で、指摘事項に関しては直ちに対処する体制やルールが工場内で整備されていないため、担当者によって対応レベルに差がある。本シナリオのような状況が発生する可能性はあることを確認した。
レベル2（黄帯）	セキュリティアセスメントを実施したことはあるため、一部の関係者はその重要性を理解しているが非常に限定的となっている。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	セキュリティアセスメントを実施したことがなく、その重要性も理解できていない。本シナリオのような状況が発生する可能性が高いことを確認した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	ペネトレーションテスト
レベル5（黒帯）	システムの機能改修やクラウド環境の変化も鑑みて、半年に1回以上の頻度で、資産管理台帳をもとにすべての資産を対象とした、ペネトレーションテストを実施している。また、資産管理台帳に抜け漏れがないか、把握できていない資産がないかを検出できるようなサイバー空間のモニタリングを平時からおこなっている。
レベル4（茶帯）	毎年1回、資産管理台帳をもとにすべての資産を対象とした、ペネトレーションテストを実施している。
レベル3（緑帯）	毎年1回、資産管理台帳をもとに特に重要な資産を対象にペネトレーションテストを実施している。
レベル2（黄帯）	対象のシステムに関して検討を開始しており、今年度実施する予定がある。
レベル1（白帯）	実施したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	資産管理台帳などと照合しながら、工場に存在する、インターネットと接しているすべてのネットワーク機器、サーバ（外部公開資産/Attack Surface; アタックサーフェス）に対して、本番利用開始前や設定変更作業後に、都度、ペネトレーションテストを実施している。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	資産管理台帳などと照合しながら、工場に存在する、インターネットと接している一部のネットワーク機器、サーバ（外部公開資産/Attack Surface; アタックサーフェス）に対して、年に1回程度、ペネトレーションテストを実施している。本シナリオのような状況が発生するリスクは低いことを確認した。
レベル3（緑帯）	資産管理台帳などと照合しながら、工場に存在する、インターネットと接している一部のネットワーク機器、サーバ（外部公開資産/Attack Surface; アタックサーフェス）に対して、年に1回程度、ペネトレーションテストを実施している。ただし、自社の資産ではない、生産設備ベンダーが導入・設置した機器は実施対象外としており、本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	ペネトレーションテストを実施する対象システム/機器の選定を開始しており、実施の目途がついている。ただし現時点では未実施のため、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	ペネトレーションテストを実施したことがない。 本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	制御システムに関する専門教育、 キャリアパスの整備
レベル5（黒帯）	担当者が外部の専門的な研修や活動（IPA；CyberREX、CyberSTIX、中核人材育成プログラム、そのほか社外WG活動等）に積極的に参加することができるように予算措置や業務アサイン時の考慮がおこなわれている。また確実に受講・活動ができるような社内チーム内での協力関係、深い理解がある。さらに、社内における専門家としての明瞭なキャリアパスも示されており、担当チーム全体としてモチベーションを維持し、継続的にケイパビリティを高められる持続可能性の高い職場環境となっている。
レベル4（茶帯）	担当者が外部の専門的な研修や活動（IPA；CyberREX、CyberSTIX、中核人材育成プログラム、そのほか社外WG活動等）に参加することができるように予算措置しており、毎年一定数の受講者がいる。ただし、社内での明瞭なキャリアパスは特に提示されていない。
レベル3（緑帯）	担当者が外部の専門的な研修や活動（IPA；CyberREX、CyberSTIX、中核人材育成プログラム、そのほか社外WG活動等）に参加することができるように予算措置はしているものの、業務過多で計画通りに外部研修の受講や活動がさせることができないことが多い。社内での明瞭なキャリアパスは特に提示されていない。
レベル2（黄帯）	担当者が独自に情報収集や学習をおこなっている。社内での明瞭なキャリアパスは特に提示されていないが、書籍購入など、情報収集に係る少額なコストは会社で負担している。
レベル1（白帯）	担当者が独自に情報収集や学習をおこなっている。社内での明瞭なキャリアパスは提示されておらず、完全に本人の自主性に任せている。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	インシデント再発防止検討会（セキュリティ強化タスクフォース）に向けて、工場セキュリティに関わる人材に必要な専門的な研修などを受講できるよう、具体的な予算確保の提案をおこなった。また、外部の有識者とともに、工場セキュリティの専門家としての社内でのキャリアパスや待遇面に関しての整備をおこなうよう提言した。
レベル4（茶帯）	インシデント再発防止検討会（セキュリティ強化タスクフォース）に向けて、工場セキュリティに関わる人材に必要な専門的な研修などを受講できるよう、具体的な予算確保の提案をおこなった。
レベル3（緑帯）	インシデント再発防止検討会（セキュリティ強化タスクフォース）に向けて、人材に関するテーマも取り上げられた。詳細まで詰められなかったものの、人材育成に関する一定の予算確保の提案準備をおこなった。
レベル2（黄帯）	インシデント再発防止検討会（セキュリティ強化タスクフォース）に向けて、人材に関するテーマは挙がったものの、具体的なアクションに繋がる提案はなかった。
レベル1（白帯）	インシデント再発防止検討会（セキュリティ強化タスクフォース）に向けて、人材の育成に関するテーマは特に議論の想定はなかった。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ④ 成熟度セルフチェックシートを活用した振り返りノート

	外部専門機関との連携
レベル5（黒帯）	JPCERT/CCに加えて、その他各社で個別に契約している、各社のIT/OT環境に関する構成情報を事前に熟知した、インシデント対応/デジタル・フォレンジック/リスクマネジメント専門企業への連絡先を直ちに引き出すことができ、スムーズに連絡、相談できる。
レベル4（茶帯）	JPCERT/CCへの連絡先を直ちに引き出すことができ、スムーズに連絡、相談できる。
レベル3（緑帯）	既存の生産設備の保守ベンダーのみへ連絡が可能。
レベル2（黄帯）	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない
レベル1（白帯）	どこに連絡するべきか想定がない。決まっていない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	連絡すべき外部専門機関のリストが整備されており、すぐに取り出す/確認することができた。
レベル4（茶帯）	連絡すべき外部専門機関のリストを整備していたが、保管場所が分からず探すのに時間を要した。
レベル3（緑帯）	連絡すべき外部専門機関のリストを整備を現在、推進している途中。
レベル2（黄帯）	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない。
レベル1（白帯）	どこに連絡するべきか想定がない。決まっていない。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：



工場セキュリティIR訓練シナリオ素材⑤

-ランサムウェアは突然に-

工場セキュリティIR訓練 進め方に関するご紹介

【進め方（概要）】

- 工場内で起こりうる架空のインシデントをタイムラインで順次提示します。そのタイミングごとに何を実施すべきか/どのようなことを考えるか、感じたかなどチーム内で議論してください。
- 演習パート完了後に、全体の振り返り・ポイント解説をファシリテーターより実施します。

【演習のステップ・目安時間】

- オープニング **10分** ➡ 演習タイム **35分** ➡ 解説/振り返り・クロージング **40分**

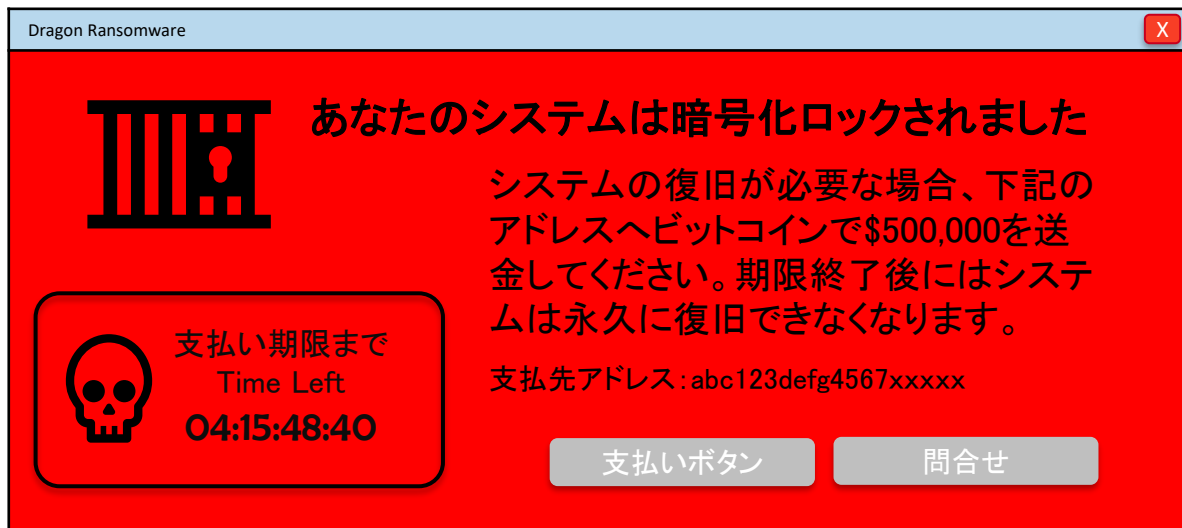


シナリオ⑤ 状況付与/Timeline-1

検討時間

10min

【製造設備管理部門】のメンバーが、生産管理システムの画面で以下の表示を発見し、【FSIRT】へ報告した。



この時点で、【工場セキュリティ推進部門】は何を実施しますか？
工場内ではどのような情報共有がなされそうでしょうか。

シナリオ⑤ 状況付与/Timeline-2

検討時間

5min

【FSIRT】が工場内の各システムの調査を速やかに実施したところ、このような身代金要求の画面が表示され、使用不可となっているシステムは工場内の**全40システム**のうち、現時点ではIoT導入検証のためのデータ保管・分析を目的として、パブリッククラウド環境等との直接接続を許可していたOTネットワーク**VLAN-TestA**（検証テスト専用VLAN。設計上、他のVLANとの通信は許可されていない）に接続されている**5システム**に留まっていることがわかりました。



* VLAN

「Virtual Local Area Network」の略。

物理的な接続形態とは別に、論理的（仮想的）にLANを分割する技術。VLAN間のネットワーク通信を制御することで、セキュリティ強化にも寄与する。

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
（だれが、何を実施すべきでしょうか）

シナリオ⑤ 状況付与/Timeline-3

検討時間

5min

【FSIRT】は【CSIRT】と協業し、インシデント緊急対策本部を立ち上げ、直近の対応について緊急で協議しています。

【FSIRTメンバー】

「現在は**VLAN-TestA**のみでシステムの暗号化による使用不可が確認されており、それ以外の生産設備に関わるシステムは正常に稼働していることを確認できています。**VLAN-TestA** はすでにインターネットとの通信切断が可能と確認しました。また、これ以外で外部環境との通信を許可している環境についても、設定を含め至急、確認、見直しを進めています。」

【CSIRTメンバー】

「ありがとうございます。確認されたインシデントはいわゆるランサムウェア攻撃ですが、基本方針として犯罪者へ金銭を支払うことはありません。ところで、暗号化されてしまったシステムのバックアップは別の場所に保管されていますか？」

【FSIRTメンバー】

「はい。バックアップのデータは業務ネットワークから分離されたクラウド環境で日次で保管されています。また、磁気テープでも取得し、週次で工場敷地内の別のビル内で保管しています。」

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
(だれが、何を実施すべきでしょうか)

シナリオ⑤ 状況付与/Timeline-4

検討時間

15min

VLAN-TestAを使用していた環境以外には設定上の問題は確認されなかった。また、VLAN-TestAに接続し暗号化された5つのシステムについて、バックアップデータからシステムの復旧をおこなうことができた。さらに、マルウェアスキャンをおこない、駆除されずに残っているマルウェアは、検知可能な範囲においては存在しないことを確認した。

今回のインシデント発生を受け、インシデント再発防止検討会が開かれることになった。本会議体は【CSIRT】が主催となるが、【FSIRT】のメンバーも参加する。

この時点で、【工場セキュリティ推進部門】は何を実施しますか？
インシデント再発防止検討会では、どのような再発防止策を提案すべきでしょうか？
【FSIRT】の立場から、検討してください

工場セキュリティIR訓練シナリオ素材⑤

解説編

シナリオ⑤ 解説

今回は、被害の拡大が続いている、「ランサムウェア攻撃」が工場内のシステムで発生した場合のシナリオを描いた。ランサムウェア攻撃は発生した“場所”によって、そのビジネスへの影響の現れ方は異なるが、原因と基本的な対応は変わらない。平時から、DLP(Data Loss Prevention)、アクセス制御、バックアップの取得、バックアップデータからのリストア試験など基本の徹底を図りたい。

本ケースではバックアップの取得、適切なバックアップデータの保管、FSIRTメンバーの初動の速さから被害の拡大を食い止めることができたが、さらに以下のような対策、確認もできていればシステムの暗号化自体を防ぐことができたかもしれない。

本ケースの問題点①： ネットワークゾーニングの未徹底

検証・テスト専用のネットワーク環境であったとしても、例外なく、ネットワークゾーニングのルールが徹底されるべきだった。インターネットとOTネットワークゾーンが直接通信することは回避するべきである。

本ケースの問題点②： クラウド利用時の設定不備（クラウドセキュリティ管理）

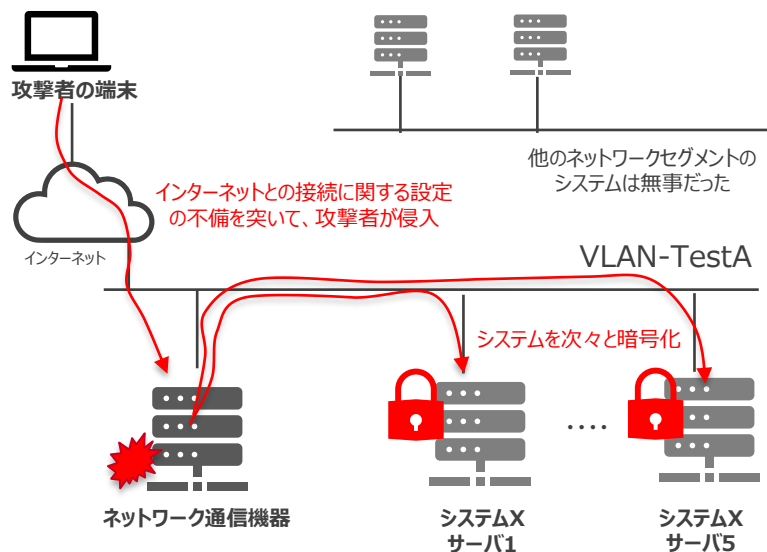
今回のシナリオでは、工場内のシステムで取得したデータをクラウド環境にアップロードし、クラウド上でデータを分析し生産効率向上を図る取り組みを推進していた。その際の、クラウド環境の設定に不備があり、攻撃者がクラウド環境を経由して、工場内のネットワークに侵入してきた。クラウドのセキュリティの設定はユーザー側の責任（責任共有モデル）となるため、CSPM（Cloud Security Posture Management）のツールを活用するなど、クラウド環境の設定不備を速やかに検出、是正できる仕組みを整備する必要がある。

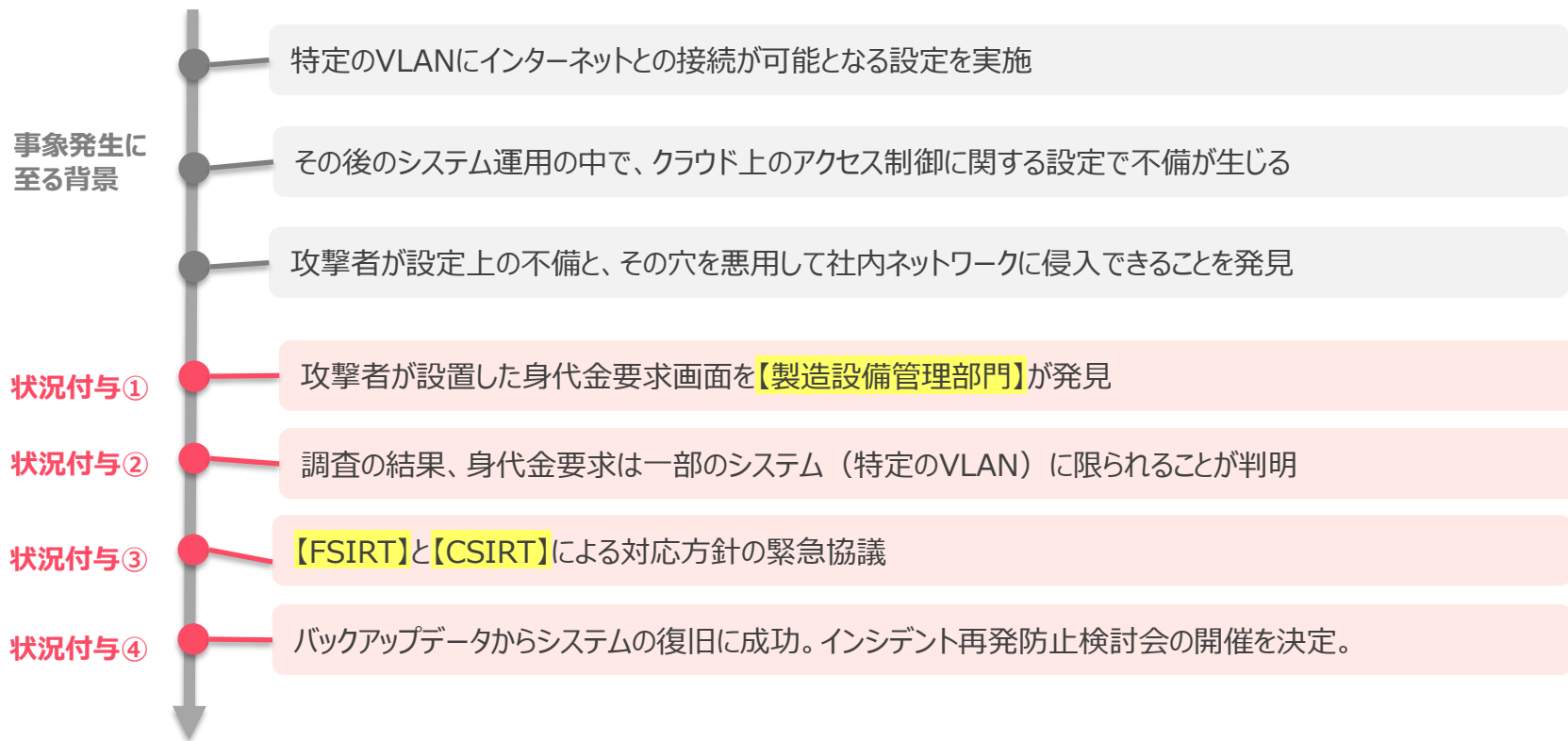
**本ケースの問題点③：
システムへのEDR、ネットワークトラフィック監視システム/体制未導入**
工場内のシステムにもアンチマルウェア製品だけでなく、不審な振る舞いを検知できるEDRを原則導入するべきである。また、ネットワークトラフィックの異常な変化を監視できるツール、体制の整備も望まれる。

本ケースの問題点④：

ペネトレーションテスト未実施

資産管理簿、サーバ台帳が都度更新され、管理できていることが前提となるが、ペネトレーションテストにより侵入経路の確認がおこなえていれば、事前に攻撃者によって悪用される「穴」を塞ぐことができた可能性もある。





シナリオ⑤ 期待する行動例

状況付与	期待する行動（主要なもの）の例
① 攻撃者が設置した身代金要求画面を【製造設備管理部門】が発見	・ インシデント対応マニュアルの確認 ・ 【FSIRT】から【CSIRT】など、社内の連携部門/チームへ情報共有 ・ 当該生産システムの停止に関して、場内の関係者へ全体周知 ・ 他にも同様の事象が発生していないか、場内の関係者へ緊急確認 ・ 緊急対策本部の立ち上げ、基本方針の確認
② 調査の結果、身代金要求は一部のシステム（特定のVLAN）に限られることが判明	・ 資産管理台帳、ネットワーク構成図から影響する可能性がある範囲の特定 ・ 当該クラウド環境の管理者権限を有するチームへの連絡、設定状況などの調査依頼
③ 【FSIRT】と【CSIRT】による対応方針の緊急協議	・ バックアップデータの確認 ・ VLAN-TestAについてインターネット（クラウド環境等）との接続許可設定を停止 ・ 暗号化されたサーバのネットワーク論理隔離/通信制御 ・ バックアップデータからのシステム復旧対応
④ バックアップデータからシステムの復旧に成功。インシデント再発防止検討会の開催を決定	・ クラウドセキュリティ管理の強化 ・ ペネトレーションテストの実施計画 ・ EDRの導入検討 ・ ネットワークトラフィックの監視システム、体制の導入検討 ・ JPCERT/CCへのインシデント事例の共有/報告/相談

※補足：「JPCERT/CCへのインシデント事例の共有/報告/相談」について、状況付与④の期待する行動例として設定していますが、各社のインシデント対応／フォレンジック体制などから、各社で最適なタイミングを判断し、JPCERT/CCへコンタクトすることが良いでしょう。

シナリオ⑤ 成熟度セルフチェックシート 主なチェック項目

成熟度セルフチェックシート項目一覧		
被害シナリオの想定	インシデント対応体制	役割の定義と合意
連絡方法の確立	インシデント対応マニュアルの整備と周知	制御システムに影響がある インシデント対応訓練/演習
サプライチェーンリスク管理	継続的なアウェアネス向上	外部専門機関との連携
モニタリング・検知	持ち込み機器の検査	データ分類
資産管理（IT/OT）	ネットワーク構成管理	システムへのアクセス制御
マルウェアへの対処・駆除	脆弱性管理	機器セキュリティ更新
物理的セキュリティ （入退場管理）	不要なUSBポート閉塞	サーバラック、HUBボックス等の施錠
ネットワークゾーニング（セグメンテーション）	バックアップ取得	バックアップデータの保管
リストア	外部記憶媒体の管理（USBメモリ等）	バイ・デザインのアプローチ
セキュリティアセスメント	システムアカウント管理	ペネトレーションテスト
制御システムに関する専門教育、 キャリアパスの整備	変更作業実施時の承認プロセスの整備	内部犯行への対策

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	被害シナリオの想定
レベル5（黒帯）	従業員の家族・ステークホルダー・近隣住民・社会的信用回復までのワーストケースを最高責任者を含め想定できている。
レベル4（茶帯）	1週間以上の操業停止を含む社内への影響について想定している。
レベル3（緑帯）	FSIRT、CSIRT等の自社内で関連するステークホルダーと連携し、一定程度の範囲について検討している。
レベル2（黄帯）	自部署内で検討したことがある。
レベル1（白帯）	具体的な想定を持っていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	工場へのサイバー攻撃が発生した際の被害として、従業員の家族・ステークホルダー・近隣住民・社会的信用回復までのワーストケースを最高責任者を含め、あらかじめ想定できている、対応手順や方針に関して定まっていることを確認した。
レベル4（茶帯）	工場へのサイバー攻撃が発生した際の被害に関して、1週間以上の操業停止を含む社内への影響について想定していることを確認した。実際に攻撃の被害に遭った際の対応手順や方針に関して定まっていることを確認した。
レベル3（緑帯）	工場へのサイバー攻撃が発生した際の被害に関して、FSIRT、CSIRT等の自社内で関連するステークホルダーと連携し、一定程度の範囲について検討していることを確認した。実際に攻撃の被害に遭った際には、ある程度の初動はできそうであることを確認した。
レベル2（黄帯）	工場へのサイバー攻撃が発生した際の被害に関して、自部門内で議論・検討したことはある。実際に攻撃の被害に遭った際に、現場が混乱するであろうことを確認できた。
レベル1（白帯）	工場へのサイバー攻撃が発生した際の被害に関して、具体的な想定を持っていなかった。社内で議論、検討したことがなかった。実際に攻撃の被害に遭った際に、現場が混乱するであろうことを確認できた。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	インシデント対応体制
レベル5（黒帯）	アウトソーシングなどで社外専門家、人的リソースも積極的に活用し、社内でも正式に承認された形で、FSOC(Factory Security Operation Center) の体制が構築、運営されており、インシデント発生時には24/7 で対応可能となっている。
レベル4（茶帯）	社内の限られた要員体制ではあるが、夜間休日でも対応すべきアラート／インデントを検知した際には、おおむね、1時間以内に確認、対処可能な体制が構築できている。
レベル3（緑帯）	社内の限られた要員体制ではあるが、夜間休日でも対応すべきアラート／インデントを検知した際には、おおむね、数時間以内に確認、対処可能な体制が構築できている。
レベル2（黄帯）	社内の限られた要員体制ではあるが、平日日中であれば、対応すべきアラート／インデントを検知した際には対応可能な体制が構築できている。（代理要員のアサインも可能な冗長性のある体制）
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	FSOCにより、サーバやネットワークトラフィックでの不審な振る舞い、異常が直ちに検知され、被害拡大の前に環境の隔離、駆除など必要な対処がおこなわれる体制が構築されているため、本シナリオのような状況が発生する可能性は非常に低いことを確認した。
レベル4（茶帯）	社内の限られた要員体制ではあるが、夜間休日含め対応できる体制は構築できているため、少ない被害のうちに対処できる想定であることが確認できた。本シナリオのような状況が発生する可能性が低いことを確認した。
レベル3（緑帯）	社内の限られた要員体制ではあるが、夜間休日含め対応できる体制は構築できているため、壊滅的な被害が発生する前に対処できる想定であることが確認できた。本シナリオのような状況が発生する可能性が低いことを確認した。
レベル2（黄帯）	工場内でのインシデント対応体制は決まっているものの、平日日中帯のみの為、休日夜間帯で発生した場合には、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	工場内のインシデント対応体制が決まっておらず、常時、本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	役割の定義と合意
レベル5（黒帯）	生産停止を決定できる最上位者も含め決まっており、定期的な見直しや確認をおこなっている。
レベル4（茶帯）	生産停止を決定できる最上位者も含め決まっているが、定期的な見直しや確認をおこなっていない。
レベル3（緑帯）	現場担当者レベルではある程度決まっているが、定期的な見直しや確認をおこなっていない。
レベル2（黄帯）	社内で議論、検討したことはあるが、まだ決定に至っていない。
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	生産管理システムでの異常を検知したタイミングから、あらかじめ決められている意思決定者を巻き込んだ形で、今後の工場稼働継続に関して議論することを想定できた。生産停止を決定できる最上位者等に関して定義したドキュメントも直ちに取り出せた。
レベル4（茶帯）	生産管理システムでの異常を検知したタイミングから、あらかじめ決められている意思決定者を巻き込んだ形で、今後の工場稼働継続に関して議論することを想定できた。生産停止を決定できる最上位者等に関して定義したドキュメントも直ちに取り出せた。
レベル3（緑帯）	過去に生産停止を決定できる最上位者を定義していたが、その決定内容を記載したドキュメントは見つからなかった。緊急対策会議に参加しているメンバーで今後の工場稼働継続に関して議論することは想定できた。
レベル2（黄帯）	生産活動の停止等に関する明確な役割が定義されておらず、緊急対策会議の中で、はじめて議論・検討することとなった。
レベル1（白帯）	生産活動の停止等に関する明確な役割が定義されていない。演習内でも、今後の生産活動に関する検討の必要性に関する議論は一切なかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	連絡方法の確立
レベル5（黒帯）	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備し、定期的に機能するか検証、訓練している。
レベル4（茶帯）	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備している。
レベル3（緑帯）	連絡網（複数の連絡手段を想定）を作成している。
レベル2（黄帯）	連絡網（連絡手段1つ）を作成している。
レベル1（白帯）	決まっていない。社内で議論、検討したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	FSIRTが連絡を受領したタイミング以降、あらかじめ決められた連絡方法によって、すべての関係者に対して直ちに情報伝達した。
レベル4（茶帯）	FSIRTが連絡を受領したタイミング以降、すべての関係者に対して直ちに情報伝達したものの、連絡方法はインシデント発生時に決めて対応した。
レベル3（緑帯）	FSIRTが連絡を受領したタイミング以降、主要なメンバーには情報伝達されたが、関係者全員には情報が行き渡らなかった。
レベル2（黄帯）	FSIRTが連絡を受領したタイミング以降、自身と普段から繋がりのある数名のメンバーへ個別に連絡し、情報収集を試みた。
レベル1（白帯）	影響のあった生産ラインの関係者のみ詳細な状況を把握しており、工場内で円滑な情報共有ができなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	インシデント対応マニュアルの整備と周知
レベル5（黒帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。
レベル4（茶帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。
レベル3（緑帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。
レベル2（黄帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルは存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。
レベル1（白帯）	何も存在しない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	サイバー攻撃についても考慮された生産設備でのインシデントマニュアルが存在する。定期的に関係者で読み合わせなど内容確認をおこなっているので、スムーズに演習内でも参照できた。
レベル4（茶帯）	サイバー攻撃についても考慮された生産設備でのインシデントマニュアルが存在する。演習内で確認しようとしたが、初めて読むので理解に時間を要した。
レベル3（緑帯）	サイバー攻撃は考慮していない生産設備でのインシデントマニュアルは存在する。演習内で確認した。
レベル2（黄帯）	サイバー攻撃は考慮していない生産設備でのインシデントマニュアルは存在するが、確認しようとしなかった。
レベル1（白帯）	インシデント対応マニュアルが存在しなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	モニタリング・検知
レベル5（黒帯）	アンチマルウェアソフトやEDR等の常時監視のツールを利用しており、LOGの定期確認をしている。さらにFSOC(Factory Security Operation Center)チームもモニタリングしており、1時間以内に検知、対処が可能。
レベル4（茶帯）	アンチマルウェアソフトやEDR等の常時監視のツールを利用しており、LOGの定期確認をしている。数時間以内に対処可能。
レベル3（緑帯）	アンチマルウェアソフトやEDR等の常時監視のツールを利用している。数時間以内に対処可能。
レベル2（黄帯）	定期的に、マルウェア検出・駆除ツールを用いてスキャンしている。
レベル1（白帯）	明らかに目に見えてわかる事象が発生するまで、気づけない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	IT、OTに関わらず、すべてのシステムに常時モニタリングできるアンチマルウェアソフトやEDR等が導入されている。マルウェア感染や不審な振る舞いを検知した際には隔離/駆除が自動的におこなわれる設計となっている。またそのアラートはFSOCなどの専門チームが確認している。本シナリオのような状況が発生する可能性は非常に低いことを確認した。
レベル4（茶帯）	ITではある程度の対策が進んでいるが、OT環境では常時モニタリングできるアンチマルウェアソフトやEDR等の導入を現在対応している。まだ全体をカバーできていないが、9割以上は対応済みとなっており、残りについても対応のめどがついている。本シナリオのような状況が発生する可能性が低いことを確認した。
レベル3（緑帯）	IT環境での導入が完了している、常時モニタリングできるアンチマルウェアソフトやEDR等について、OT環境への展開を計画しているが、まだ実現できていない。本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	OT環境では常時モニタリングできるツールの導入は重要システムに限られており、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	IT環境、OT環境共に常時モニタリングできるツールが導入されているかどうか不明で、かなり被害が拡大するまで気づくことができないと想定している。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	資産管理 (IT/OT)
レベル5 (黒帯)	資産管理を自動化、効率化する仕組みが導入されており、新たな資産を自動的に検出される。資産管理台帳への更新に活用することができるインシデント発生時には、すぐに取り出せる。
レベル4 (茶帯)	資産管理台帳を作成しており、四半期に1回程度、手動で棚卸をおこない最新化するようにしている。
レベル3 (緑帯)	資産管理台帳を作成しており、年に1回程度、手動で棚卸をおこない最新化するようにしている。
レベル2 (黄帯)	資産管理台帳を過去に作成したことがあるが、その後、一度も更新されていない。
レベル1 (白帯)	資産の可視化をしたことがない。資産管理台帳は無い。

本シナリオにおける到達目標の設定例	
レベル5 (黒帯)	資産管理台帳をすぐに取り出すことができ、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル4 (茶帯)	過去に作成した資産管理台帳がどこにあるのかわからず、見つけ出すのに時間を要したが、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル3 (緑帯)	工場内で統合された資産管理台帳はなく、各部門/生産ラインごとに作成しているため、それらを確認したが、かなり時間を要した。
レベル2 (黄帯)	資産管理台帳などドキュメント類はないものの、環境を把握しているメンバーの知識をもとに、インシデントの影響範囲や原因分析を試みた。
レベル1 (白帯)	資産管理台帳のようなものは一切存在しないため、インシデントの影響範囲の確認や原因調査に活用できなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り&次回に向けての課題：

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	ネットワーク構成管理
レベル5（黒帯）	工場全体のネットワーク物理構成図、設計図があり、定期的に最新化されており、インシデント発生時にはすぐに取り出せる。また影響範囲について想定することができる。
レベル4（茶帯）	工場全体のネットワーク物理構成図、設計図を作成したことがあるが、その後、更新していないので、現状の構成と乖離している可能性がある。
レベル3（緑帯）	工場全体のネットワーク物理構成図、設計図は無いが、自身が担当しているライン/領域については、各担当が接続構成、影響範囲を含め個別に把握している（ドキュメント化されていない）。
レベル2（黄帯）	ネットワーク機器の配置場所や管理部門を把握している（ドキュメント化されていない）。
レベル1（白帯）	ネットワーク機器がどこにあり、誰が管理しているのか全くわからない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	工場全体のネットワーク物理構成図、設計図をすぐに取り出すことができ、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル4（茶帯）	過去に作成した工場全体のネットワーク物理構成図、設計図がどこにあるのかわからず、見つけ出すのに時間を要したが、今回のインシデントによる影響範囲や原因調査に活用できた。
レベル3（緑帯）	ネットワーク構成図は各システムごとに作成しており、それらを使用した。しかし、工場全体を俯瞰したものではないため、インシデントの影響範囲の確認や原因調査には活用できなかった。もしくは利用したが、かなり時間を要した。
レベル2（黄帯）	ネットワーク構成図などドキュメント類はないものの、環境を把握しているメンバーの知識をもとにインシデントの影響範囲や原因分析を試みた。
レベル1（白帯）	ネットワーク構成図のようなものは一切存在しないため、インシデントの影響範囲の確認や原因調査に活用できなかった。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	システムへのアクセス制御
レベル5（黒帯）	すべてのシステムにおいて、MFAの実装、アクセス元のグローバルIPアドレス制限等による、複数のアクセス制御を実装している。
レベル4（茶帯）	多くの主要システムで、ID、パスワードに加えて、MFAの実装やアクセス可能なアクセス元のグローバルIPアドレスを制限する等、追加の対策を実施している。
レベル3（緑帯）	ID、パスワードのみでログインできるシステムが多いが、一部の重要なシステムでは、MFAの実装やアクセス可能なアクセス元のグローバルIPアドレスを制限する等、追加の対策を実施している。
レベル2（黄帯）	すべてのシステムでID、パスワードの設定をおこなっている。
レベル1（白帯）	ID、パスワードの設定をしていない、アクセス制御なしのシステムが工場内に存在する。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	すべてのシステムにおいて、MFAの実装、アクセス元のグローバルIPアドレス制限等による、複数のアクセス制御も実装できている。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	重要な一部のシステムでは、MFAの実装、アクセス元のグローバルIPアドレス制限等による、複数のアクセス制御も実装できている。本シナリオのような状況が発生することは低いと想定していることを確認した。
レベル3（緑帯）	MFAの実装、アクセス元のグローバルIPアドレス制限等による、複数のアクセス制御の導入を開始始めているが、まだ道半ば。本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	ID、パスワードのみでアクセスできるシステムがほとんどであり、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	アクセス制御に関して重要性は認識しているものの、工場内のシステムではどのような状況になっているのか把握していない。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	ネットワークゾーニング (セグメンテーション)
レベル5 (黒帯)	ファイアウォールに加えて、産業用IDS/IPSも導入されており、不正な通信に関する制御も多層防御となっている。用途ごとにネットワークゾーニング (セグメンテーション) がおこなわれている。
レベル4 (茶帯)	ファイアウォールを導入し、用途ごとにネットワークゾーニング (セグメンテーション) をおこなっている。
レベル3 (緑帯)	OT領域は他のネットワークと完全に分離している。
レベル2 (黄帯)	IT、OTの区分は一応あるが、いわゆる、サーバのNIC2枚刺しで分離しているような状態になっている。
レベル1 (白帯)	IT、OTすべての通信が制御なく許可されている。インターネットからのアクセスもID、パスワードを知っていれば可能。

本シナリオにおける到達目標の設定例	
レベル5 (黒帯)	OTネットワークゾーン (セグメンテーション) を設けており、同一ネットワークゾーン内でも各システム間ごとに業務行必要最小限の通信のみを許可している。産業用IDS/IPSも導入されている。本シナリオのような状況が発生する可能性は非常に低いことを確認した。
レベル4 (茶帯)	OTネットワークゾーン (セグメンテーション) を設けており、同一ネットワークゾーン内でも各システム間ごとに業務行必要最小限の通信のみを許可している。本シナリオのような状況が発生する可能性が低いことを確認した。
レベル3 (緑帯)	OTネットワークゾーン (セグメンテーション) を設けているが、同一ネットワークゾーン内では自由な通信が可能となっている。本シナリオのような状況が発生する可能性があることを確認した。
レベル2 (黄帯)	一応のネットワークゾーニングはあるものの、技術的には不完全/未熟で、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1 (白帯)	IT、OTすべての通信が特に制御なく許可されている。本シナリオのような状況が発生する可能性が高いことを確認した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	バックアップ取得
レベル5（黒帯）	毎日、バックアップを取得している。バックアップの3-2-1のルールを理解し、バックアップデータを取得している。
レベル4（茶帯）	月次でバックアップを取得している。
レベル3（緑帯）	3か月1回程度はバックアップを取得している。
レベル2（黄帯）	初回導入時に1回取得したのみで、それ以降、バックアップは取得していない。
レベル1（白帯）	バックアップを取得する運用は一切存在しない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	工場内の重要なシステムに関して、毎日、バックアップが取得できていることを確認した。
レベル4（茶帯）	工場内の重要なシステムに関して、月次でバックアップが取得できていることを確認した。
レベル3（緑帯）	工場内の重要なシステムに関して、で3か月1回程度、バックアップが取得できていることを確認した。
レベル2（黄帯）	初回導入時に1回取得したのみで、それ以降、バックアップは取得していないことを確認した。
レベル1（白帯）	バックアップを取得する運用は一切存在しないことを確認した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	バックアップデータの保管
レベル5（黒帯）	バックアップデータ保管に関する社内統一基準が定まっている。バックアップの3-2-1のルールを理解し、バックアップデータを保管している。バックアップデータをネットワークの観点で分離された別の環境で保管している。ネットワーク上分離されたクラウドサービス上や、外付けハードディスク、磁気テープ等をオフラインで保管し、ランサムウェア被害のリスクを最小化している。さらに、地震などの自然災害も考慮して、システム稼働地域から地理的に離れた遠隔地でも、バックアップデータを保管している。
レベル4（茶帯）	バックアップデータ保管に関する社内統一基準が定まっている。バックアップデータをネットワークの観点で分離された別の環境で保管している。ネットワーク上分離されたクラウドサービス上や、外付けハードディスク、磁気テープ等をオフラインで保管し、ランサムウェア被害のリスクを最小化している。
レベル3（緑帯）	バックアップデータ保管に関する社内統一基準が定まっている。バックアップデータを同一筐体内/同一ネットワーク内の環境下で保管している。
レベル2（黄帯）	バックアップデータ保管に関する社内統一基準が定まっておらず、重要なデータが否かが考慮されないまま、システム導入時のシステム担当者の判断でバックアップデータが、様々な形態で保管されている。
レベル1（白帯）	バックアップデータがどこにあるかわからない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	バックアップデータ保管に関する社内統一基準が定まっている。バックアップの3-2-1のルールを理解し、バックアップデータを保管できている。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	バックアップデータ保管に関する社内統一基準が定まっている。バックアップの3-2-1のルールを理解しているが、ネットワークから分離したオフラインのバックアップデータは準備できていない。本シナリオのような状況が発生するリスクはあることを確認した。
レベル3（緑帯）	バックアップデータ保管に関する社内統一基準や仕様を定めよう対応を開始している。本シナリオのような状況が発生するリスクはあることを確認した。
レベル2（黄帯）	バックアップデータ保管に関する社内統一基準が定まっておらず、システムごとにバックアップの仕様が様々なため、リスクレベルもシステムによって大きく異なる。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	バックアップデータが取得できているのか、どこにあるかわからない。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	リストア
レベル5（黒帯）	システム復旧に関する社内統一基準が定まっている。システムが2重化されており、短時間（1時間以内）で復元できる。年に1回程度、重要なシステムに関して、リストアテストをおこなっている。（システム障害が発生しても、ビジネスで許容可能なリスクレベル以下に抑えられている）
レベル4（茶帯）	システム復旧に関する社内統一基準が定まっている。バックアップから復元が短時間（数時間程度）でできる。（システム障害が発生しても、ビジネスで許容可能なリスクレベル以下に抑えられている）
レベル3（緑帯）	システム復旧に関する社内統一基準が無い。リストアは可能だが、バックアップからの復元に数日程度かかる。（ビジネスで許容できないリスクレベルとなっている）
レベル2（黄帯）	システム復旧に関する社内統一基準が無い。リストアは可能だが、再インストール、再設定作業等で復旧まで数週間程度かかる。（ビジネスで許容できないリスクレベルとなっている）
レベル1（白帯）	リストアしたことがない。もしくは、そもそも、バックアップデータがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	システム復旧に関する社内統一基準が定まっている。年に1回程度、重要なシステムに関して、リストアテストをおこなっている。1時間以内でシステムを復旧でき、当該ビジネスで許容可能なリスクレベル以下となっていることを確認した。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	システム復旧に関する社内統一基準が定まっている。数時間以内でシステムを復旧することができ、当該ビジネスで許容可能なリスクレベル以下となっていることを確認した。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル3（緑帯）	システム復旧に関する社内統一基準が無い。リストアは可能なはずだがリストアテストを定期的におこなっておらず確信は持てない。システム復旧までに数日程度を要すると確認した。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル2（黄帯）	システム復旧に関する社内統一基準が無い。リストアは可能なはずだがリストアテストを定期的におこなっておらず確信は持てない。システム復旧までに数週間程度を要すると確認した。本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	リストアしたことがない。もしくは、そもそも、バックアップデータがない。本シナリオのような状況が発生する可能性が高いことを確認した。
本シナリオでの対応状況振り返り記録ノート	
実施日：	
振り返り＆次回に向けての課題：	

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	ペネトレーションテスト
レベル5（黒帯）	システムの機能改修やクラウド環境の変化も鑑みて、半年に1回以上の頻度で、資産管理台帳をもとにすべての資産を対象とした、ペネトレーションテストを実施している。また、資産管理台帳に抜け漏れがないか、把握できていない資産がないかを検出できるようなサイバー空間のモニタリングを平時からおこなっている。
レベル4（茶帯）	毎年1回、資産管理台帳をもとにすべての資産を対象とした、ペネトレーションテストを実施している。
レベル3（緑帯）	毎年1回、資産管理台帳をもとに特に重要な資産を対象にペネトレーションテストを実施している。
レベル2（黄帯）	対象のシステムに関して検討を開始しており、今年度実施する予定がある。
レベル1（白帯）	実施したことがない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	資産管理台帳などと照合しながら、工場に存在する、インターネットと接しているすべてのネットワーク機器、サーバ（外部公開資産/Attack Surface; アタックサーフェス）に対して、本番利用開始前や設定変更作業後に、都度、ペネトレーションテストを実施している。本シナリオのような状況が発生するリスクは非常に低いことを確認した。
レベル4（茶帯）	資産管理台帳などと照合しながら、工場に存在する、インターネットと接している一部のネットワーク機器、サーバ（外部公開資産/Attack Surface; アタックサーフェス）に対して、年に1回程度、ペネトレーションテストを実施している。本シナリオのような状況が発生するリスクは低いことを確認した。
レベル3（緑帯）	資産管理台帳などと照合しながら、工場に存在する、インターネットと接している一部のネットワーク機器、サーバ（外部公開資産/Attack Surface; アタックサーフェス）に対して、年に1回程度、ペネトレーションテストを実施している。ただし、自社の資産ではない、生産設備ベンダーが導入・設置した機器は実施対象外としており、本シナリオのような状況が発生する可能性があることを確認した。
レベル2（黄帯）	ペネトレーションテストを実施する対象システム/機器の選定を開始しており、実施の目途がついている。ただし現時点では未実施のため、本シナリオのような状況が発生する可能性が高いことを確認した。
レベル1（白帯）	ペネトレーションテストを実施したことがない。 本シナリオのような状況が発生する可能性が高いことを確認した。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

シナリオ⑤ 成熟度セルフチェックシートを活用した振り返りノート

	外部専門機関との連携
レベル5（黒帯）	JPCERT/CCに加えて、その他各社で個別に契約している、各社のIT/OT環境に関する構成情報を事前に熟知した、インシデント対応/デジタル・フォレンジック/リスクマネジメント専門企業への連絡先を直ちに引き出すことができ、スムーズに連絡、相談できる。
レベル4（茶帯）	JPCERT/CCへの連絡先を直ちに引き出すことができ、スムーズに連絡、相談できる。
レベル3（緑帯）	既存の生産設備の保守ベンダーのみへ連絡が可能。
レベル2（黄帯）	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない
レベル1（白帯）	どこに連絡するべきか想定がない。決まっていない。

本シナリオにおける到達目標の設定例	
レベル5（黒帯）	連絡すべき外部専門機関のリストが整備されており、すぐに取り出す/確認することができた。
レベル4（茶帯）	連絡すべき外部専門機関のリストを整備していたが、保管場所が分からず探すのに時間を要した。
レベル3（緑帯）	連絡すべき外部専門機関のリストを整備を現在、推進している途中。
レベル2（黄帯）	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない。
レベル1（白帯）	どこに連絡するべきか想定がない。決まっていない。

本シナリオでの対応状況振り返り記録ノート
実施日：
振り返り＆次回に向けての課題：

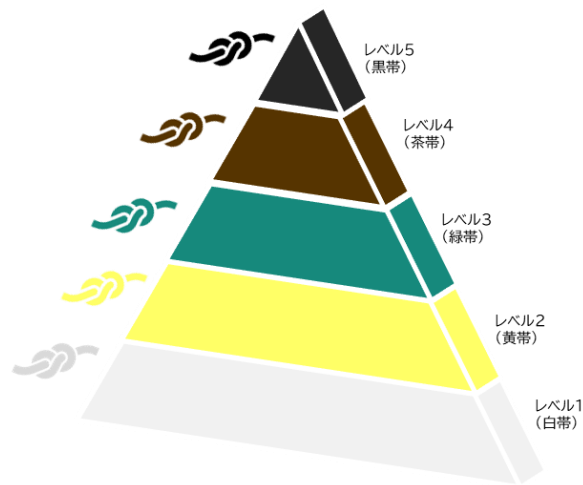


Appendix-2

成熟度セルフチェックシート

有事の際に助けとなるのは、
それまでに積み重ねてきた日々の研鑽と、平時から繋がっている仲間。

成熟度セルフチェックシートの活用方法



- 定期的かつ、意欲的にIR訓練の取り組みを継続して頂くための工夫の一環として、WG内で「成熟度セルフチェックシート」を作成しました。
- 成熟度/レベルアップをIR訓練の都度、実感することでモチベーションを維持し取り組みを継続することができるのではないかと考えています。
- 工場セキュリティの安全性を確保するうえで、特に重要/主要であると考えたポイントについて、**レベル1（白帯）～レベル5（黒帯）を設定し、それぞれについて到達の目安/目標を記載しました。**
- 本成熟度チェックシートはFSIRTの活動に視点を置いています。CSIRTであれば、大規模インシデント発生時には法務部門や広報部門などの多くの関連部門との連携、コミュニケーション等も重要な要素となりますが、**FSIRTは工場において発生したインシデント発生の際に、CSIRTと連携して対応するという前提のもとで項目を選別しています。**
- 項目は必ずしも、工場セキュリティIR訓練のシナリオ案で登場する内容とは限りません。工場セキュリティを維持、向上するうえで必要な項目も挙げています。
- 「成熟度セルフチェックシート」はあくまでも一例ですので、**各社の業種やビジネスモデルに応じて、自由にカスタマイズして使用して頂ければ幸いです。**
- **セキュリティに「ゴール」は無く、「習慣」です。**レベル5（黒帯）に到達した後も、さらにその上、師範（赤帯）を想定し、研鑽を怠らず、歩みを進めましょう。
- 各社のベストプラクティス、インシデント対応における教訓については、JPCERT/CCや他の製造業の仲間に**積極的に共有**するなど、日本全体のセキュリティ対策レベルの底上げへの貢献にも、ぜひ興味・関心を持っていただけることを願っています。自社で発生したインシデントは他社でも発生しうるものです。

成熟度セルフチェックシート 項目一覧

成熟度セルフチェックシート項目一覧		
被害シナリオの想定	インシデント対応体制	役割の定義と合意
連絡方法の確立	インシデント対応マニュアルの整備と周知	制御システムに影響がある インシデント対応訓練/演習
サプライチェーンリスク管理	継続的なアウェアネス向上	外部専門機関との連携
モニタリング・検知	持ち込み機器の検査	データ分類
資産管理（IT/OT）	ネットワーク構成管理	システムへのアクセス制御
マルウェアへの対処・駆除	脆弱性管理	機器セキュリティ更新
物理的セキュリティ （入退場管理）	不要なUSBポート閉塞	サーバラック、HUBボックス等の施錠
ネットワークゾーニング（セグメンテーション）	バックアップ取得	バックアップデータの保管
リストア	外部記憶媒体の管理（USBメモリ等）	バイ・デザインのアプローチ
セキュリティアセスメント	システムアカウント管理	ペネトレーションテスト
制御システムに関する専門教育、 キャリアパスの整備	変更作業実施時の承認プロセスの整備	内部犯行への対策

成熟度セルフチェックシート

	被害シナリオの想定	インシデント対応体制	役割の定義と合意	連絡方法の確立
レベル5（黒帯）	従業員の家族・ステークホルダー・近隣住民・社会的信用回復までの Worst Case を最高責任者を含め想定できている。	アウトソーシングなどで社外専門家、人的リソースも積極的に活用し、社内でも正式に承認された形で、FSOC(Factory Security Operation Center) の体制が構築、運営されており、インシデント発生時には24/7 で対応可能となっている。	生産停止を決定できる最上位者も含め決まっており、定期的な見直しや確認をおこなっている。	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備し、定期的に機能するか検証、訓練している。
レベル4（茶帯）	1 週間以上の操業停止を含む社内への影響について想定している。	社内の限られた要員体制ではあるが、夜間休日でも対応すべきアラート／インデントを検知した際には、おおむね、1 時間以内に確認、対処可能な体制が構築できている。	生産停止を決定できる最上位者も含め決まっているが、定期的な見直しや確認をおこなっていない。	すべての社内関係者に効率的に情報連携できる複数の連絡手段（メーリングリスト、チャットグループ、電話等）を整備している。
レベル3（緑帯）	FSIRT、CSIRT等の自社内で関連するステークホルダーと連携し、一定程度の範囲について検討している。	社内の限られた要員体制ではあるが、夜間休日でも対応すべきアラート／インデントを検知した際には、おおむね、数時間以内に確認、対処可能な体制が構築できている。	現場担当者レベルではある程度決まっているが、定期的な見直しや確認をおこなっていない。	連絡網（複数の連絡手段を想定）を作成している。
レベル2（黄帯）	自部署内で検討したことがある。	社内の限られた要員体制ではあるが、平日日中であれば、対応すべきアラート／インデントを検知した際には対応可能な体制が構築できている。（代理要員のアサインも可能な冗長性のある体制）	社内で議論、検討したことはあるが、まだ決定に至っていない。	連絡網（連絡手段 1 つ）を作成している。
レベル1（白帯）	具体的な想定を持っていない。社内で議論、検討したことがない。	決まっていない。社内で議論、検討したことがない。	決まっていない。社内で議論、検討したことがない。	決まっていない。社内で議論、検討したことがない。

成熟度セルフチェックシート

	インシデント対応マニュアルの整備と周知	制御システムに影響がある インシデント対応訓練/演習	サプライチェーンリスク管理
レベル5（黒帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。定期的な見直しや周知、教育活動もおこなっており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。	半年に1回以上の頻度で実施している。実際に大規模インシデントが発生した際に、生産停止の判断をおこなう最上位者（工場長、経営者等）や、生産設備保安担当等も含め、幅広いステークホルダーが参加している。	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝え、定期的な契約内容の見直しをおこない、調達先が自社で求められるセキュリティ要件を満たすようにしている。必要な際には調達先の変更も含め幅広く検討し、セキュリティの確保に努めている。また、定期的に調達先の情報セキュリティ管理体制チェック/ヒアリングをおこなっている。
レベル4（茶帯）	サイバー攻撃についても考慮した、生産設備でのインシデント発生時の対応マニュアルが存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。	半年に1回以上の頻度で実施している。ただし、参加者は工場内の一部の有志メンバーに限られる。	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝え、定期的な契約内容の見直しをおこない、調達先が自社で求められるセキュリティ要件を満たすようにしている。必要な際には調達先の変更も含め幅広く検討し、セキュリティの確保に努めている。
レベル3（緑帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルが存在しており、関係者がインシデント発生時にすぐに閲覧、活用できる状態となっている。	主要担当者の退職、人事異動など、担当者が変わったタイミング等に、数年に1回程度の頻度で実施している。	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝えたことはあるが、調達先から強い拒否感を示され、断念した。ワークアラウンド/次善策を実施し、セキュリティリスクの軽減を図っている。
レベル2（黄帯）	サイバー攻撃に関しては考慮していないが、生産設備でのインシデント発生時の対応マニュアルは存在する。ただし、定期的な見直しや周知、教育活動はおこなっていない。	過去に一度実施したことがあるが、継続的な取り組みとならなかった。	生産に関わる設備やシステムの調達先へ自社のセキュリティ要求・要件を伝えたことはあるが、調達先から強い拒否感を示され、断念した。
レベル1（白帯）	何も存在しない。	実施したことがない。	長年の付き合いのある調達先なので、契約内容は特に見直さず、単純更新している。

成熟度セルフチェックシート

	継続的なアウェアネス向上	外部専門機関との連携	モニタリング・検知	持ち込み機器の検査
レベル5（黒帯）	定期的にセキュリティ専門家（情報処理安全確保支援士、CISSP等）から、最新の脅威状況について、社内での発生インシデントやトレンドを含めてインタラクティブなコミュニケーションの機会があり、改善が必要なポイントがあれば速やかに対処している。また、半年に1回以上の頻度で机上訓練、標的型メール訓練、その他の専門的なトレーニングをおこなっている。	JPCERT/CCに加えて、その他各社で個別に契約している、各社のIT/OT環境に関する構成情報を事前に熟知した、インシデント対応/デジタル・フォレンジック/リスクマネジメント専門企業への連絡先を直ちに取出すことができ、スムーズに連絡、相談できる。	アンチマルウェアソフトやEDR等の常時監視のツールを利用しており、LOGの定期確認をしている。さらにFSOC(Factory Security Operation Center)チームもモニタリングしており、1時間以内に検知、対処が可能。	工場内での運用ルールが策定されており、十分に周知されている。外部から持ち込まれる機器（USB、PC等）は都度、セキュリティチェックがおこなわれ、安全性が担保されたうえで、接続、利用することが徹底されている。
レベル4（茶帯）	年に1回程度、社内のセキュリティルール/ポリシーに関するトレーニングを受講している。 また、四半期に1回以上の頻度で机上訓練、標的型メール訓練、その他の追加トレーニングをおこなっている。	JPCERT/CCへの連絡先を直ちに取出すことができ、スムーズに連絡、相談できる。	アンチマルウェアソフトやEDR等の常時監視のツールを利用しており、LOGの定期確認をしている。数時間以内に対処可能。	工場内での運用ルールが策定されているが、周知活動が未だ十分ではない。外部から持ち込まれる機器（USB、PC等）は多くのケースで都度、セキュリティチェックがおこなわれ、安全性が担保されたうえで、接続、利用されている。
レベル3（緑帯）	年に1回程度、社内のセキュリティルール/ポリシー等に関するトレーニングを受講している。 また、半年に1回以上の頻度で机上訓練、標的型メール訓練、その他の追加トレーニングをおこなっている。	既存の生産設備の保守ベンダーのみへ連絡が可能。	アンチマルウェアソフトやEDR等の常時監視のツールを利用している。数時間以内に対処可能。	工場内での運用ルールを策定し、一部の部署でルールに基づいた運用がおこなわれている。
レベル2（黄帯）	年に1回程度、社内のセキュリティルール/ポリシー等に関するトレーニングを受講している。	外部専門機関の想定はあるものの、具体的な連絡先はすぐにはわからない	定期的に、マルウェア検出・駆除ツールを用いてスキャンしている。	工場内での運用ルールは策定されているが、形骸化しており、セキュリティ対策状況が不明な機器（USB、PC等）の持ち込み、利用が可能な状態となっている。
レベル1（白帯）	入社したときに1度セキュリティ研修を受講したが、それ以来、受講した記憶がない。	どこに連絡するべきか想定がない。決まっていない。	明らかに目に見えてわかる事象が発生するまで、気づけない。	工場内での運用ルールがなく、特段の確認をおこなわず、セキュリティ対策状況が不明な機器（USB、PC等）の持ち込み、利用を可能な状態となっている。

成熟度セルフチェックシート

	データ分類	資産管理（IT/OT）	ネットワーク構成管理
レベル5（黒帯）	セキュリティの問題が発生した場合に組織が受ける影響について社内で考慮、認識されている。また、データ/情報資産の重要度、機密度に応じてラベリングする仕組みがあり、定期的なアセスメントなどを通して利用状況のモニタリングができています。また、モニタリングの結果に応じて、必要な修正、是正が速やかにおこなわれている。	資産管理を自動化、効率化する仕組みが導入されており、新たな資産が自動的に検出され、資産管理台帳へ更新される。インシデント発生時には、資産管理台帳をすぐに取り出せる。	工場全体のネットワーク物理構成図、設計図がある。定期的に最新化されており、インシデント発生時にはすぐに取り出せる。また影響範囲について想定することができる。
レベル4（茶帯）	セキュリティの問題が発生した場合に組織が受ける影響について社内で考慮、認識されている。また、データ/情報資産の重要度、機密度に応じてラベリングする仕組みがあり、定期的なアセスメントなどを通して利用状況のモニタリングができています（定量的な評価が可能）。	資産管理台帳を作成しており、四半期に1回程度、手動で棚卸をおこない最新化するようにしている。	工場全体のネットワーク物理構成図、設計図を作成したことがあるが、その後、更新していないので、現状の構成と乖離している可能性がある。
レベル3（緑帯）	セキュリティの問題が発生した場合に組織が受ける影響について社内で考慮、認識されている。また、データ/情報資産の重要度、機密度に応じてラベリングする仕組みがあり、おおむね対応できている（定性的評価に留まる）。	資産管理台帳を作成しており、年に1回程度、手動で棚卸をおこない最新化するようにしている。	工場全体のネットワーク物理構成図、設計図は無いが、自身が担当しているライン/領域については、各担当が接続構成、影響範囲を含め個別に把握している（ドキュメント化されていない）。
レベル2（黄帯）	セキュリティの問題が発生した場合に組織が受ける影響について社内で考慮、認識されており、データ/情報資産の重要度、機密度に応じてラベリングする仕組みがあるが、ほぼ活用されていない。	資産管理台帳を過去に作成したことがあるが、その後、一度も更新されていない。	ネットワーク機器の配置場所や管理部門を把握している（ドキュメント化されていない）。
レベル1（白帯）	データ/情報資産の重要度が決まっていない。セキュリティの問題が発生した場合に組織が受ける影響について社内で考慮、認識されていない。	資産の可視化をしたことがない。資産管理台帳は無い。	ネットワーク機器がどこにあり、誰が管理しているのが全くわからない。

成熟度セルフチェックシート

	システムへのアクセス制御	マルウェアへの対処・駆除	脆弱性管理	機器セキュリティ更新
レベル5（黒帯）	すべてのシステムにおいて、MFAの実装、アクセス元のグローバルIPアドレス制限等による、複数のアクセス制御を実装している。	持ち運び可能なマルウェアスキャン・駆除ツールが現場にある。パターンファイルも最新に更新されており、誰もがすぐに取り出すことができる。十分な数が配備されている。	脆弱性管理ツールを導入し、優先付けをおこないシステム各要素の脆弱性に速やかに対処している。	常に最新版へ更新されている。
レベル4（茶帯）	多くの主要システムで、ID、パスワードに加えて、MFAの実装やアクセス可能なアクセス元のグローバルIPアドレスを制限する等、追加の対策を実施している。	持ち運び可能なマルウェアスキャン・駆除ツールが現場にある。パターンファイルも最新に更新されており、誰もがすぐに取り出せるものの、配備数が少ない。	ネットワーク機器とサーバOS、システム内に含まれるミドルウェア、OSSの脆弱性対応を手動で管理し対応している。	更新をしているが、一部のシステムでEOLになったままのものがある。ただし、社外には一切繋がっていない。
レベル3（緑帯）	ID、パスワードのみでログインできるシステムが多いが、一部の重要なシステムでは、MFAの実装やアクセス可能なアクセス元のグローバルIPアドレスを制限する等、追加の対策を実施している。	持ち運び可能なマルウェアスキャン・駆除ツールが現場にあるが、パターンファイルが全く更新されていない。	ネットワーク機器とサーバOSの脆弱性対応を手動で管理し対応している。	システム導入以来、更新していない。ただし、社外には一切繋がっていない。
レベル2（黄帯）	すべてのシステムでID、パスワードの設定をおこなっている。	持ち運び可能なマルウェアスキャン・駆除ツールが現場になく、金庫/鍵のかかったキャビネット内に保管されている（利用できる者が限定的）。	ネットワーク機器だけは脆弱性対応を手動で管理し対応している。	システム導入以来、更新していない。社外とは、proxy経由でつながっている。
レベル1（白帯）	ID、パスワードの設定をしていない、アクセス制御なしのシステムが工場内に存在する。	持ち運び可能なマルウェアスキャン・駆除ツールを持っていない。	何をすればよいかわ具体的にはわかっていない。	システム導入以来、更新していない。社外の環境とは直接接続されている。

成熟度セルフチェックシート

	物理的セキュリティ (入退場管理)	不要なUSBポート閉塞	サーバラック、HUBボックス等の施錠
レベル5（黒帯）	茶帯の内容に加えて、顔認証、静脈認証、IDカード、監視カメラ等による多層のゲート、認証・監視システムが導入されている。特に重要な機器があるエリアには入場可能な人が厳密に規定、制限されている（ゲスト入館時には事前に身分証明書の確認、顔データの登録が必要等）。	不要なUSBポートについて、物理的に閉塞している。閉塞器具の鍵は任命された複数の管理者が利用履歴を記録し、保管している。また、追加の安全策として、工場内に導入する機器類については、USBメモリ挿入時の自動起動をしない設定を標準としている。	工場内のサーバラック、HUBボックスは原則として施錠管理されている。鍵は任命された複数の管理者が利用履歴を記録し、保管している。
レベル4（茶帯）	受付で事前に登録された訪問情報をもとに、受け入れ担当社員へ連絡が入り、有効期限付きのゲストIDカードを貸与したうえで、社員が同行し工場内へ入場する。入場した後もゲストの常時監視、同行をおこない、社外の人間に単独行動はさせない。	不要なUSBポートについて、物理的に閉塞している。ただし、閉塞器具の鍵は誰でも使用できるように分かりやすい場所に配置している。また、追加の安全策として、工場内に導入する機器類については、USBメモリ挿入時の自動起動をしない設定を標準としている。	工場内のサーバラック、HUBボックスは原則として施錠管理されている。ただし、鍵は誰でも使用できるように分かりやすい場所に配置している。
レベル3（緑帯）	受付で事前に登録された訪問情報をもとに、受け入れ担当社員へ連絡が入り、無期限のゲストIDカードを貸与したうえで、社員が同行し工場内へ入場する。入場した後もゲストの常時監視、同行をおこない、社外の人間に単独行動はさせない。	工場内に導入する機器類については、USBメモリ挿入時の自動起動をしない設定を標準としている	サーバールーム内の重要なサーバが保管されているサーバラックのみ施錠されている。ただし、鍵は誰でも使用できるように分かりやすい場所に配置している。
レベル2（黄帯）	受付で事前に登録された訪問情報をもとに、受け入れ担当社員へ連絡が入り、無期限のゲストIDカードを貸与したうえで、社員が同行し工場内へ入場する。しかし、入場した後はゲストの常時監視や同行はしていない。	不要なUSBポートについて、物理的に閉塞している。ただし、閉塞器具の鍵は誰でも使用できるように分かりやすい場所に配置している。	サーバラック、HUBボックスの設置場所や管理部門については把握しているが、常に開錠されている。
レベル1（白帯）	受付で会社名と氏名、訪問先を伝え、顔見知りであれば、社員の同行が無くとも、社外の人間が工場内へ入場することが可能。	USBポートに関する対策は何もしていない。	サーバラック、HUBボックスがそもそもどこにあるのか、管理状況を含め把握していない。

成熟度セルフチェックシート

	ネットワークゾーニング (セグメンテーション)	バックアップ取得	バックアップデータの保管	リストア
レベル5（黒帯）	ファイアウォールに加えて、産業用IDS/IPSも導入されており、不正な通信に関する制御も多層防御となっている。用途ごとにネットワークゾーニング（セグメンテーション）がおこなわれている。	毎日、バックアップを取得している。バックアップの3-2-1のルールを理解し、バックアップデータを取得している。	バックアップデータ保管に関する社内統一基準が定まっている。バックアップの3-2-1のルールを理解し、バックアップデータを保管している。バックアップデータをネットワークの観点で分離された別の環境で保管している。ネットワーク上分離されたクラウドサービス上や、外付けハードディスク、磁気テープ等をオフラインで保管し、ランサムウェア被害のリスクを最小化している。さらに、地震などの自然災害も考慮して、システム稼働地域から地理的に離れた遠隔地でも、バックアップデータを保管している。	システム復旧に関する社内統一基準が定まっている。システムが2重化されており、短時間（1時間以内）で復元できる。年に1回程度、重要なシステムに関して、リストアテストをおこなっている。（システム障害が発生しても、ビジネスで許容可能なリスクレベル以下に抑えられている）
レベル4（茶帯）	ファイアウォールを導入し、用途ごとにネットワークゾーニング（セグメンテーション）をおこなっている。	月次でバックアップを取得している。	バックアップデータ保管に関する社内統一基準が定まっている。バックアップデータをネットワークの観点で分離された別の環境で保管している。ネットワーク上分離されたクラウドサービス上や、外付けハードディスク、磁気テープ等をオフラインで保管し、ランサムウェア被害のリスクを最小化している。	システム復旧に関する社内統一基準が定まっている。バックアップから短時間（数時間程度）で復元できる。（システム障害が発生しても、ビジネスで許容可能なリスクレベル以下に抑えられている）
レベル3（緑帯）	OT領域は他のネットワークと完全に分離している。	3か月に1回程度はバックアップを取得している。	バックアップデータ保管に関する社内統一基準が定まっている。バックアップデータを同一筐体内/同一ネットワーク内の環境下で保管している。	システム復旧に関する社内統一基準が無い。リストアは可能だが、バックアップからの復元に数日程度かかる。（ビジネスで許容できないリスクレベルとなっている）
レベル2（黄帯）	IT、OTの区分は一応あるが、いわゆる、サーバのNIC2枚刺しで分離しているような状態になっている。	初回導入時に1回取得したのみで、それ以降、バックアップは取得していない。	バックアップデータ保管に関する社内統一基準が定まっておらず、重要なデータか否かが考慮されないまま、システム導入時のシステム担当者の判断で、様々な形態でバックアップデータが保管されている。	システム復旧に関する社内統一基準が無い。リストアは可能だが、再インストール、再設定作業等で復旧まで数週間程度かかる。（ビジネスで許容できないリスクレベルとなっている）
レベル1（白帯）	IT、OTのネットワーク上の区別は無く、すべての通信が制御なく許可されている。インターネットからのアクセスもID、パスワードを知っていれば可能。	バックアップを取得する運用は一切存在しない。	バックアップデータがどこにあるのかわからない。	リストアしたことがない。もしくは、そもそも、バックアップデータがない。

成熟度セルフチェックシート

	外部記憶媒体の管理 (USBメモリ等)	バイ・デザインのアプローチ	セキュリティアセスメント
レベル5 (黒帯)	許可された外部記憶媒体しか接続しても使用できないように各機器で技術的な対策をおこなっている。また、USBを使用した場合にはログから確認することができる。さらに、年に1回以上、工場内の全部門に外部記憶媒体の棚卸調査(用途、本数、管理者等)をおこない、利用状況/実態の把握をおこなっている。	セキュリティの専門家(情報処理安全確保支援士、CISSP等)が新規のシステム導入やITを用いた施策について、企画立ち上げ・検討フェーズ初期から参画し、担当者は情報セキュリティリスクの観点からアドバイスを受けるようにしている。バイデザインのプロセスは、プロジェクトを推進する際の必須事項として、社内ルールに取り込まれている。さらに、社内稟議システムとしても、セキュリティの専門家によるレビューが完了しないと、プロジェクトの発注や推進ができない仕組みになっている。	1年に1回程度、アセスメントの基準や委託先を変えて、多角的な視点からアプローチし、セキュリティ上の課題を幅広く見出すようにしている。社内のメンバーも積極的にアセスメントに関与しており、日々の簡易アセスメントレベルであれば、内製で対応できるケイパビリティも有している。
レベル4 (茶帯)	年に1回以上、工場内の全部門に外部記憶媒体の棚卸調査(用途、本数、管理者等)をおこない、全量の把握をおこなっている。	セキュリティの専門家(情報処理安全確保支援士、CISSP等)が新規のシステム導入やITを用いた施策について、企画立ち上げ・検討フェーズ初期から参画し、担当者は情報セキュリティリスクの観点からアドバイスを受けるようにしている。ただし、これは任意で社内ルールにはなっていない。	数年に1回程度、アセスメントの基準や委託先を変えて、多角的な視点からアプローチし、セキュリティ上の課題を幅広く見出すようにしている。社内のメンバーはアセスメントの実務プロセスに関与しない。
レベル3 (緑帯)	新規利用開始時には要申請としており、管理台帳で管理している。ただし、管理台帳の定期的な更新はおこなわれていない。	新規のシステム導入やITを用いた施策について、セキュリティの専門家(情報処理安全確保支援士、CISSP等)に基本的に相談、情報共有することになっているが、プロジェクトの後半、システムリリース直前となることが多い。	数年に1回、毎回同じ基準に基づいて、同じ専門企業にアセスメントを委託している。社内のメンバーはアセスメントの実務プロセスに関与しない。
レベル2 (黄帯)	部分的に把握しているが、利用用途の全量を把握できているかどうか定かではない。	新規のシステム導入やITを用いた施策について、セキュリティの専門家(情報処理安全確保支援士、CISSP等)に相談することもあるが、稀である。	過去に1度実施したことがある。
レベル1 (白帯)	何をどこで使用しているのか工場全体の実態を全く把握できていない。	新規のシステム導入やITを用いた施策について、セキュリティの専門家(情報処理安全確保支援士、CISSP等)が関わることはない。	実施したことがない。

成熟度セルフチェックシート

	システムアカウント管理	ペネトレーションテスト	制御システムに関する専門教育、 キャリアパスの整備
レベル5（黒帯）	当該システム管理者は、どのようなアカウントがあるか把握している。各システムごとにアカウントには必要な最小権限のみを付与している。特に、特権アカウントに関しては利用前の申請および承認が必須となるプロセスを導入しており、システム化により管理を効率化し、本プロセスが徹底されるよう工夫している。人事異動のタイミングなど、半年に1回以上は定期的なアカウントの棚卸をおこない不要なアカウントを遅延なく削除している。	システムの機能改修やクラウド環境の変化も鑑みて、半年に1回以上の頻度で、資産管理台帳をもとにすべての資産を対象とした、ペネトレーションテストを実施している。また、資産管理台帳に抜け漏れがないか、把握できていない資産がないかを検出できるようなサイバー空間のモニタリングを平時からおこなっている。	担当者が外部の専門的な研修や活動（IPA；CyberREX、CyberSTIX、中核人材育成プログラム、そのほか社外WG活動等）に積極的に参加することができるように予算措置や業務アサイン時の考慮がおこなわれている。また確実に受講・活動ができるような社内チーム内での協力関係、深い理解がある。さらに、社内における専門家としての明瞭なキャリアパスも示されており、担当チーム全体としてモチベーションを維持し、継続的にケイパビリティを高められる持続可能性の高い職場環境となっている。
レベル4（茶帯）	当該システム管理者は、どのようなアカウントがあるか把握している。各システムごとにアカウントには必要な最小権限のみを付与している。また、1年に1回、定期的にアカウントの棚卸をおこない、不要なアカウントを遅延なく削除している。	毎年1回、資産管理台帳をもとにすべての資産を対象とした、ペネトレーションテストを実施している。	担当者が外部の専門的な研修や活動（IPA；CyberREX、CyberSTIX、中核人材育成プログラム、そのほか社外WG活動等）に参加することができるように予算措置しており、毎年一定数の受講者がいる。ただし、社内での明瞭なキャリアパスは特に提示されていない。
レベル3（緑帯）	当該システム管理者は、どのようなアカウントがあるか把握している。また、1年に1回、定期的にアカウントの棚卸をおこない、不要なアカウントを遅延なく削除している。ただし、個別のアカウントごとに必要最小限の権限ではなく、等しく特権（管理者最高権限）を与えている。	毎年1回、資産管理台帳をもとに特に重要な資産を対象にペネトレーションテストを実施している。	担当者が外部の専門的な研修や活動（IPA；CyberREX、CyberSTIX、中核人材育成プログラム、そのほか社外WG活動等）に参加することができるように予算措置はしているものの、業務過多で計画通りに外部研修の受講や活動がさせることができないことが多い。社内での明瞭なキャリアパスは特に提示されていない。
レベル2（黄帯）	当該システム管理者は、どのようなアカウントがあるか概ね認識はしているが、定期的なアカウントの棚卸はおこなっていない。	対象のシステムに関して検討を開始しており、今年度実施する予定がある。	担当者が独自に情報収集や学習をおこなっている。社内での明瞭なキャリアパスは特に提示されていないが、書籍購入など、情報収集に係る少額なコストは会社で負担している。
レベル1（白帯）	各システムごとにどのようなアカウントが存在するのか把握していない。定期的なアカウントの棚卸もおこなっていない。	実施したことがない。	担当者が独自に情報収集や学習をおこなっている。社内での明瞭なキャリアパスは提示されておらず、完全に本人の自主性に任せている。

成熟度セルフチェックシート

	変更作業実施時の承認プロセスの整備	内部犯行への対策
レベル5（黒帯）	変更管理手順が文書化されている。当該領域に関する専門的な知見を有する者を含めた確認者による承認プロセス（多段階承認）が整備、徹底されている。変更作業の計画時には、開発・検証環境での作業内容の事前確認などにより、変更による影響の分析を十分におこない、発生する可能性のある事象に対して、対応策および回避策が計画され、リスクの最小化が図られている。変更作業の実施前には、あらかじめ決められた連絡手段・方法で、工場内へ変更作業の内容、詳細な作業実施スケジュール、当該作業に関する責任者・問合せ先に関する情報共有をおこない、万が一の際にも、迅速なコミュニケーションが可能となるようにしている。	IPA発行の『組織における内部不正防止ガイドライン』の内容を参照し、内部不正防止の基本5原則と25分類について理解し、対策例を参考に工場内で内部不正が発生しにくい環境づくりを実践している。
レベル4（茶帯）	変更管理手順が文書化されている。当該領域に関する専門的な知見を有する者を含めた確認者による承認プロセス（多段階承認）が整備、徹底されている。開発・検証環境は存在しないため、ベンダーの公開・保有情報および机上で、変更による影響の分析をおこない、発生する可能性のある事象に対して、対応策および回避策が計画され、リスクの最小化が図られている。変更作業の実施前には、あらかじめ決められた連絡手段・方法で、工場内へ変更作業の内容、詳細な作業実施スケジュール、当該作業に関する責任者・問合せ先に関する情報共有をおこない、万が一の際にも、迅速なコミュニケーションが可能となるようにしている。	IPA発行の『組織における内部不正防止ガイドライン』の内容を参照し、内部不正防止の基本5原則と25分類について、工場内で今後の方針について議論、追加の対応計画策定に着手しており、今後の具体的なアクションや対応スケジュールが明確になっている。
レベル3（緑帯）	変更管理手順が文書化されており、当該領域に関する専門的な知見を有する者を含めた確認者による承認プロセス（多段階承認）も準備されているが、社内での運用が徹底されていない。変更作業の実施前には、担当者が任意の手段・方法により、工場内へ変更作業の内容、詳細な作業実施スケジュール、当該作業に関する責任者・問合せ先に関する情報共有をおこない、万が一の際にも、迅速なコミュニケーションが可能となるようにしている。	IPA発行の『組織における内部不正防止ガイドライン』の内容を参照し、内部不正防止の基本5原則と25分類について、工場内で参照し始めている。
レベル2（黄帯）	変更作業の進め方に関する正式なプロセスは特に存在しておらず、都度、個別に相談しながら進めている。変更作業を実施する際には、周知・連絡方法は定まっていないものの、工場関係者に幅広く事前の情報共有を図るよう心掛けている。	内部犯行への対策の必要性を感じており、情報収集は開始しているものの、具体的な対応はできていない。
レベル1（白帯）	変更作業の進め方に関する正式なプロセスは特に存在しておらず、都度、個別に相談しながら進めている。変更作業を実施する際には、所属部門コミュニティ内で事前周知している。	従業者に対して性善説で対応しており、何ら対応や検討を社内でおこなっていない。

参考文献など

- 『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 Ver1.0』(産業サイバーセキュリティ研究会ワーキンググループ1 (制度・技術・標準化) 工場サブワーキンググループ, 2022年11月16日)
- 『制御システムのセキュリティリスク分析ガイド第2版』(IPA 独立行政法人 情報処理推進機構セキュリティセンター, 2020年3月)
- 『セキュリティインシデント事例①半導体製造業の事例 Ver.1.0.0』(Edgecrossコンソーシアムテクニカル部会 セキュリティガイドライン策定WG, 2022年3月)
- 『工場セキュリティガイドライン概要編 1.0.0版』(東京大学グリーンICTプロジェクト・Edgecrossコンソーシアム合同 工場セキュリティWG, 2022年10月11日)
- 『推奨プラクティス：工場用制御システムにおけるサイバーセキュリティインシデント対応能力の開発』(米国国土安全保障省 国家サイバーセキュリティ部門/邦訳 一般社団法人 JPCERTコーディネーションセンター, 2009年10月)
- 『制御システムのセキュリティ分析ガイド補足資料 制御システム関連のサイバーインシデント事例3：2017年 安全計装システムを標的とするマルウェア』(IPA 独立行政法人 情報処理推進機構セキュリティセンター, 2019年7月)
- 『制御システムのセキュリティ分析ガイド補足資料 制御システム関連のサイバーインシデント事例9：2021年 米国最大手のパイプラインのランサムウェア被害』(IPA 独立行政法人 情報処理推進機構セキュリティセンター, 2021年10月)
- 『スマート工場のセキュリティリスク分析調査 調査報告書』(IPA 独立行政法人 情報処理推進機構セキュリティセンター, 2022年6月)
- 『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』(IPA 独立行政法人 情報処理推進機構セキュリティセンター, 2023年7月)
- JPCERT/CC セキュリティインシデント年表 (<https://www.jpcert.or.jp/magazine/chronology/>)
- 『失敗の科学 失敗から学習する組織、学習できない組織』(マシュー・サイド著、ディスカバー・トゥエンティワン)
- 『組織における内部不正防止ガイドライン 第5版』(IPA 独立行政法人 情報処理推進機構, 2022年4月)

更新履歴（工場セキュリティIR訓練シナリオ案）

- 2024年1月5日 Ver1.0 FSIRT訓練やろうの会

更新履歴（成熟度セルフチェックシート）

- 2024年1月5日 Ver1.0 FSIRT訓練やろうの会

- 本文書はFSIRT訓練やろうの会（以下、WG）メンバーが活動成果物の一環として独自に制作したものであり、一般社団法人JPCERTコーディネーションセンターがその内容の監修や、正確性の保証等をおこなったものではありません。
- 既存コンテンツの改訂／修正、有志メンバーから寄せられたアイデア・経験に基づく新たなシナリオ案の追加、海外工場への展開を見据えた英語翻訳版の制作など、様々な後続のWG活動が想定、期待されますが、今回は発行時点でのWG活動状況に関して、一般への情報共有を目的として、配布資料（Appendix）に添付しております。

SHISEIDO