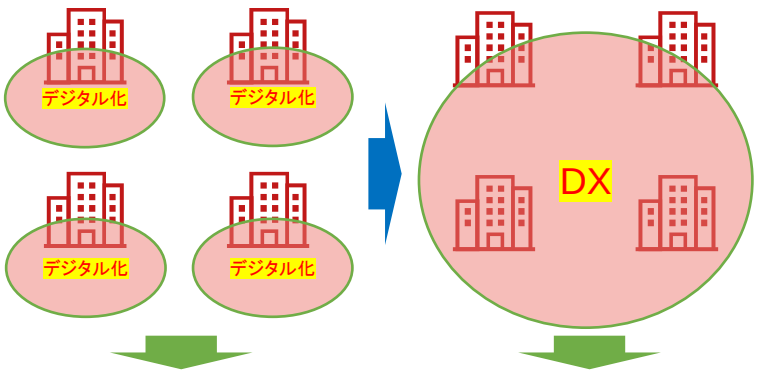
三重県　DX寺子屋
工場セキュリティ診断について

2022年12月14日
GUTP コンサルティング
DX寺子屋 工場セキュリティ診断プロジェクト
佐々木　弘志

1

「DX × セキュリティ」の課題感と対策の方向性



サイバーセキュリティ
リスクへの対処は
自己責任

サイバーセキュリティ
リスクへの対処は
ビジネス参加条件

DX時代のサイバーセキュリティ課題

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

DX時代のサイバーセキュリティ

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

2

自己紹介

佐々木　弘志

Mission：「産業サイバーセキュリティの文化を創る」

・産業制御システム開発者（14年）
・産業制御システムセキュリティのビジネス開発（10年）
講演、執筆多数。

経済産業省 Ministry of Economy, Trade and Industry
商務情報政策局　サイバーセキュリティ課
情報セキュリティ対策専門官（非常勤）

サイバー技術研究室
専門委員（非常勤）

FORTINET
OTビジネス開発部　部長

名古屋工業大学
産学官金連携機構
ものづくりDX研究所　プロジェクト准教授（非常勤）

「産官学」全ての立場から、産業界全体のセキュリティビジネス開発を推進

3

実現したいこと：日本のOTセキュリティのビジネス化

Mission：（日本の）産業サイバーセキュリティの文化を創る

・日本のOTのセキュリティリスクが　“適切な投資のもとに”　管理され、
エンドユーザーと関連事業者のビジネスが発展すること。→ 皆がきちんと儲かること

現状の課題：ビジネス環境の変化で必要性が高まっているのに対応ができていない

セキュリティリスク増大
- DX進展による セキュリティ脅威 の接点増加
- 攻撃者の能力・ 手法の進化・ 被害発生

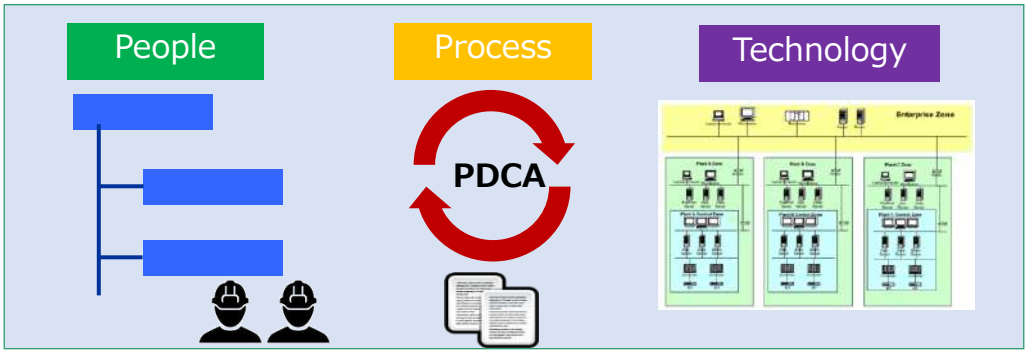
規制・ガイドライン強化
- グローバルで サプライチェーン 規制化の動き
- 業界別の規制・ ガイドライン強化 （自動車・医療機器等）

- そもそもの必要性の理解（経営層・IT/OT部門）
- どうしていいかわからない（スタンダードがない）
- どこまでやっていいかわからない（費用感・正解は？）
- やる人がいない（コンサル・SI・ベンダーにも少ない）
- 海外拠点・別事業部は対策が違う（ITほど統一的にできない）

4

OTセキュリティの３要素

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



5

経済産業省：工場サイバーセキュリティガイドライン策定（2022年）

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

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

✅ 2022年11月16日にパブリックコメントを反映したVer1.0公開。

工場SWGの設置

【現状認識・課題】

- 経済産業省は、産業・社会の変化に伴うサイバー攻撃の増大に対し、リスク源を適切に捉え、検討すべき対策を漏れなく提示するための新たなモデルとして「**サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）**」を提示した。このCPSFを実現するため、フィジカル空間とサイバー空間を繋ぐ機器・システムに対するセキュリティについても検討を行っている。
- 従来の工場内システムはインターネットには曝されないことを前提に設計されてきたが、IoT化の流れの中で、**フィジカル空間に存する個別の機械やデバイスやその関連センサーといった末端部分が直接サイバー空間のインターネットに接する**ことにより、知らない間にセキュリティホールが生じるなど、**新たなセキュリティリスク源が増加**しつつある。
- 今後、データの見える化や、遠隔制御、自動化等の進展に伴い、**IPアドレスを保有するデバイス・機器がサプライチェーンの一層広域にまで広がる**ことに鑑み、**足元でのリソースや危機意識に乏しい中小企業も含め、工場におけるセキュリティリスク対策は一層重要**になってくるものの、**ステークホルダー間の相互信頼の土台となる考え方が整理できているとは言い難い状況。**

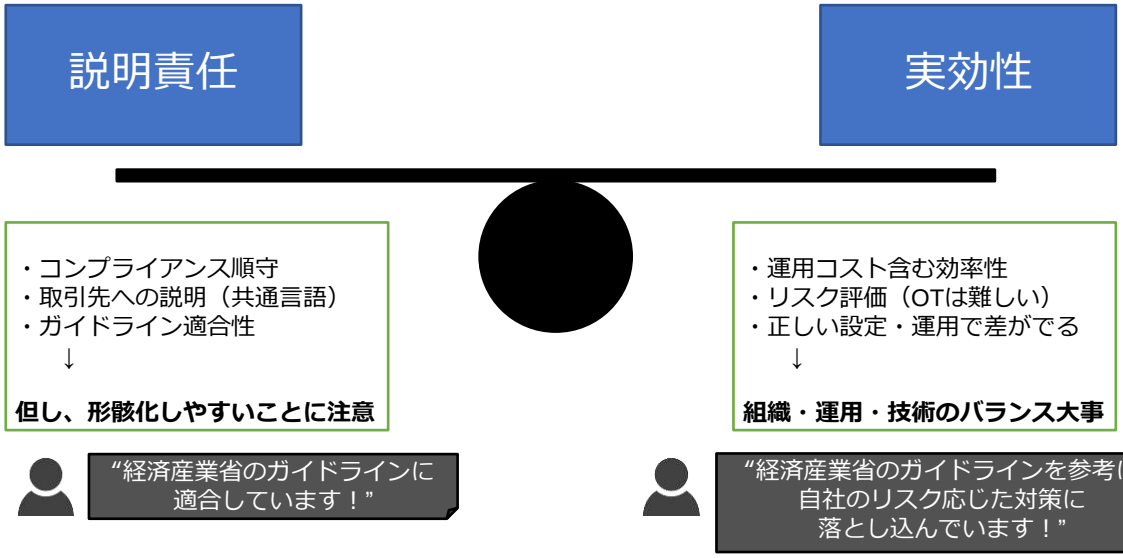
【方向性】

- このため、今年度、工場のサイバーセキュリティ対策の推進に向けた**ガイドラインを取りまとめる**ことを目標とし、産業サイバーセキュリティ研究会ＷＧ１に紐づける形で、**工場のサイバーセキュリティ関係者により構成する「工場ＳＷＧ」を設置する。**

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/pdf/001_04_00.pdf

6

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



7

工場セキュリティWeb簡易診断サービス

チェックシート

- 組織（People）
- 運用（Process）
- 技術（Technology）
- 工場システムサプライチェーン管理（SCM）

早ければ15分で回答可能

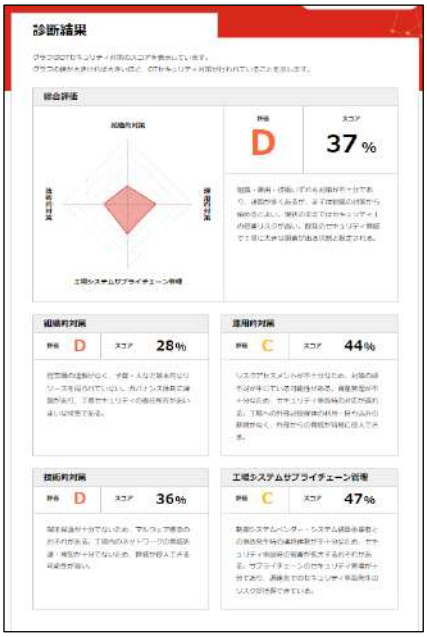
診断結果 (スグに結果が出ます！)

A	管理手順の文書化
B	対策実施済
C	一部の対策実施
D	ほとんど未実施

項目は「経済産業省ガイドラインのチェックリストを活用」 https://www.fortinet.com/jp/promos/ot-security-assessment

8

工場セキュリティ簡易診断の結果例



効果：

現状をラフに可視化できて
関係者に共通認識を形成できる

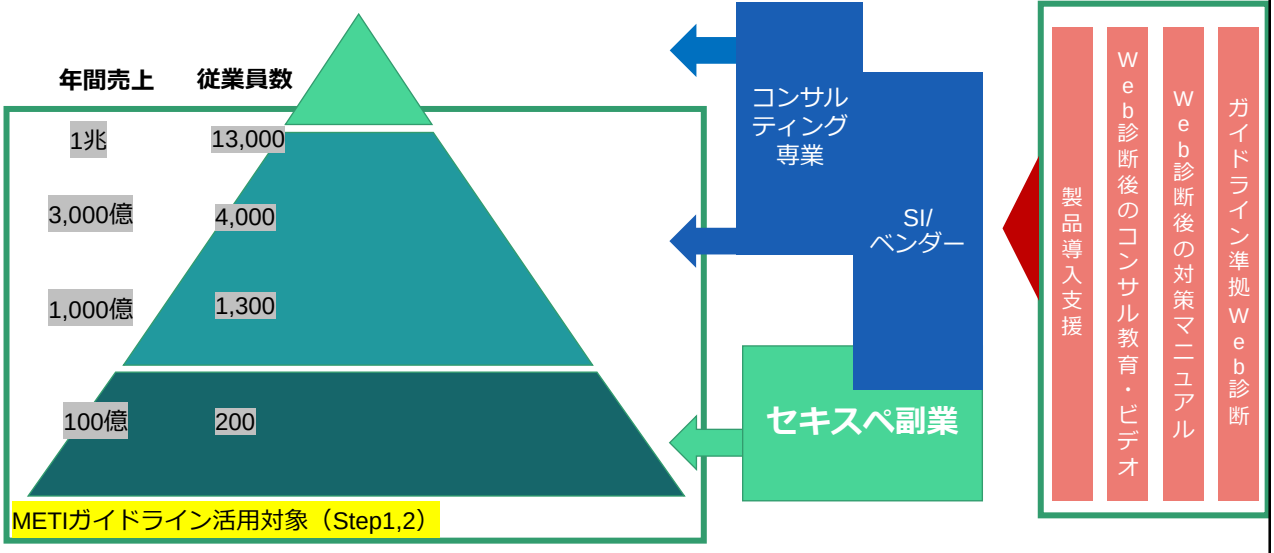
課題：

そもそも入力しかたがわからない？
これからどうするの？
どこまでやればいいの？
↓
何かしらの専門的な助言が必要

人間の健康管理に例えると
「簡易の問診票」に相当する
具体的な対策を考えるなら
更なる診断が必要

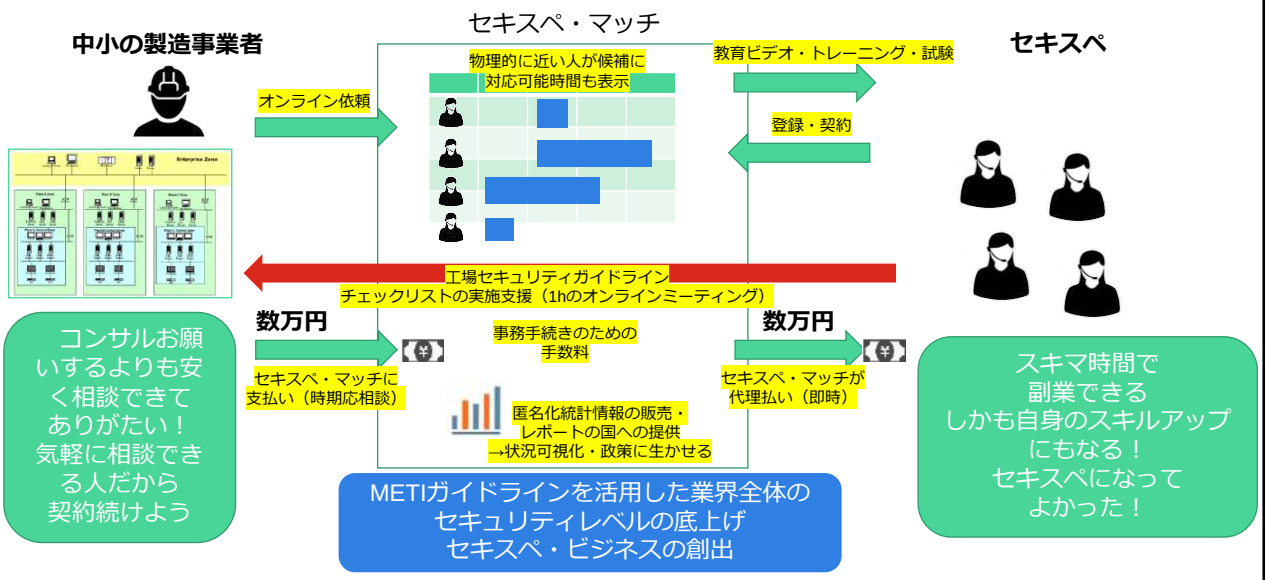
9

日本OTセキュリティのサプライチェーン全体の底上げ



10

セキスペと工場セキュリティガイドラインを活用した サプライチェーンセキュリティ底上げのビジネス化イメージ



11

三重県　DX寺子屋
工場セキュリティ診断について

2022年11月～12月

12

工場セキュリティ診断の概要　1

経済産業省が、工場のサイバーセキュリティ対策をまとめたガイドラインを策定し、11月16日に公開されました。
「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」＊1

昨今のサイバー攻撃は、大企業の対策のみでは防げず、ものづくりを行う中小企業も含めたサプライチェーン全体での対策が必須です。
DX推進とサイバーセキュリティ対策は、表裏一体です。

本ガイドラインを中小企業の現場で使いやすいものにする必要があると考え、
GUTPサイバーセキュリティWG、経産省情報セキュリティ対策専門官らの協力を得て、
本ガイドラインを基に簡易なチェックリストを作成し、ウェブでの診断を可能にしました。

このチェックリスト、ウェブ診断が有用かどうかを調査するため、三重県DX寺子屋参加企業の皆様にご協力頂き、実証実験を実施させていただくこととなりました。

取得した情報は匿名化した上で、実証実験の結果を今後のガイドライン普及策の立案に活用させていただきます。

GUTP：東京大学産学連携コンソーシアム
東京大学グリーンICTプロジェクト

＊1出典：経済産業省HP
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

13

工場セキュリティ診断の概要　2

三重県在中の「情報処理安全確保支援士（セキスペ）」が、オンラインでサポートし、診断させていただきます。
国家資格の秘密保持義務に加え、三重県産業支援センターとNDAを締結済みです。

参考：
情報処理安全確保支援士＝サイバーセキュリティ対策を推進する人材の国家資格

●法律上の定義：
「情報処理の促進に関する法律」の第六条に定める「情報処理安全確保支援士の業務」（一部抜粋）
「情報処理安全確保支援士は、情報処理安全確保支援士の名称を用いて、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うとともに、必要に応じその取組の実施の状況についての調査、分析及び評価を行い、その結果に基づき指導及び助言を行うことその他事業者その他の電子計算機を利用する者のサイバーセキュリティの確保を支援することを業とする」

●人材像
- セキュリティに関わる業務をITスキル標準のレベル4として実践することが出来る人材
- 資格保持者のみ資格名称を使用可能（名称独占資格）
- 登録簿の整備、登録情報の公開（IPA）
- 人物として問題ない人材のみを登録・資格継続する規定
  - 厳格な秘密保持義務
  - 信用失墜行為の禁止義務
  - 禁錮以上の刑、またはサイバー犯罪関連 の刑に処せられていない方を登録

出典：独立行政法人情報処理推進機構(IPA)　https://www.ipa.go.jp/siensi/whatsriss/index.html#section2

14

令和４年度　三重県DX寺子屋　工場セキュリティ診断　情報処理安全確保支援士（セキスペ）紹介

氏名：髙橋　徹

所属：DIC株式会社
四日市工場

プロフィール

■専門分野・得意分野
・情報セキュリティ、サイバーセキュリティ、インターネットの安全安心な利用方法の啓発
・中小企業のサイバーセキュリティ、IT経営・DX支援
・生産管理

■資格等
情報処理安全確保支援士、情報セキュリティ監査人補、ITコーディネータ、セキュリティプレゼンター登録（IPA）、テレワークマネジャー（総務省）、インターネット利用アドバイザー、ネットセーフティ・アドバイザー、AI・IoTシニアコンサルタント、ITマスター（厚生労働省）、システムアナリスト（情報処理技術者試験）

■主な経歴
・医薬品、農薬、診断薬、工場（化学工業）の生産管理システム再構築プロジェクト（ERP、特にSAP、生産在庫管理）、工場のシステム管理（セキュリティを含む）、生産計画・生産管理・品質管理業務を経験
・中小企業情報セキュリティマネジメント指導業務実施（情報セキュリティ基本方針等の設定＆Security Action二つ星取得支援）
・テレワークセキュリティ関連業務アドバイス
・ ITC三重定例会、三重県技能士会サイバーセキュリティ研修講師
・インターネット安全教室講師
・ITネットワーク構築技能支援＆情報セキュリティ入門講師（高校生向け）

15

令和４年度　三重県DX寺子屋　工場セキュリティ診断　情報処理安全確保支援士（セキスペ）紹介

氏名：山岡 茂治

所属：
みらいこ株式会社
一般社団法人
未来の大人応援プロジェクト

プロフィール

■専門分野・得意分野
クラウドを基盤とした情報系や教育系のシステム構築や開発、そして導入提案などを得意としています。Microsoft関連とeラーニングを専門とし、企業やNPOのICT／セキュリティアドバイザーから実際の開発作業まで幅広くおこなっています。また、IT講師として新入社員研修から各種セミナー、大学での非常勤講師や高校での講師などもおこなっています。

■資格等
情報処理安全確保支援士、データベーススペシャリスト、ネットワークスペシャリスト、民間ITベンダー資格　など

■主な経歴
埼玉県川越市に生まれる。情報系専門学校卒業の後、就職先でITベンチャーの子会社を作り役員となる。その後、フリーランスを経て会社を設立し、拠点を東京から名古屋に移し活動。更に妻の実家の三重県多気町へ引っ越し、IT関連の仕事以外に子供たちの教育や地域活動により携わるようになる。２０１８年７月末に、家族との時間を増やし、より教育や地域の活動も遂行するため東京の会社を退職。伊勢にて「みらいこ株式会社」を設立。一般社団法人にも在籍。

16

本日の流れ

●概要説明・セキスペの自己紹介（5分）

●ウェブ診断ページ（チェック項目）の確認（45分）
事前入力いただいた場合はポイントのみ確認し、事前入力していない場合は順に確認します。

●診断結果・対策案内（10分）
※正式な診断結果は後日お渡しします。

時間は目安ですので、状況により多少変更があります。1時間以内での診断となります。

面談終了後の流れ

●後日、三重県事務局様を通して、 診断結果をお渡しします。

●診断結果に基づいた具体的対策を希望する方には、個別に対応します。（有償ベース）

17

経産省ガイドラインのチェックリストの有用性について

[良かった点]

- １時間の診断で基本的な事項を確認することができた。
（People, Process, Technology, OTシステム調達先管理）
  → **短時間**でポイントを抑えた現状把握が可能
- 診断結果のスコアについて違和感がないとの回答がほとんどだった。
  → **A－Dのような分かりやすい指標は有効**
- ITとOTを両方見ているという方が多く、大企業よりもガバナンスが効いて、対策がしやすい面があることが分かった。
- ヒアリングの過程で、具体的な改善アドバイスにつながるケースが多かった。

[課題]

- ITとOTが一体となっているところが多く、OTの範囲の認識合わせに苦労した。
  → 途中からネットワーク図の例（次頁参照）を用いながら会話して改善した。この意識合わせは重要！
- 課題が明確になるものの、実際の改善策に向けた取組みとのギャップがあった。
- 完全にＩＴと分離したネットワークの場合、診断項目が「対象外」となってしまうケースがあった。
  → 実際は、完全分離であるケースは少ない。**ネットワークカード2本足サーバーなど。勘違い・認識違いなどがあった。**
  → セキュリティを意識するあまり、**ITシステム/クラウド接続などに制限がかかっており、DX阻害要因**となっているケースも見られた。
- セキュリティ対策状況の外部開示となるため、診断に二の足を踏む、本社の意向でNGとなる場合があった。
  → プロジェクト参加者全員が三重県産業支援センターとNDA（機密保持契約）を締結。匿名化によるデータ利用を約束。
  → ただ、心理面の不安の払拭などに課題が残った。

18

ネットワーク例

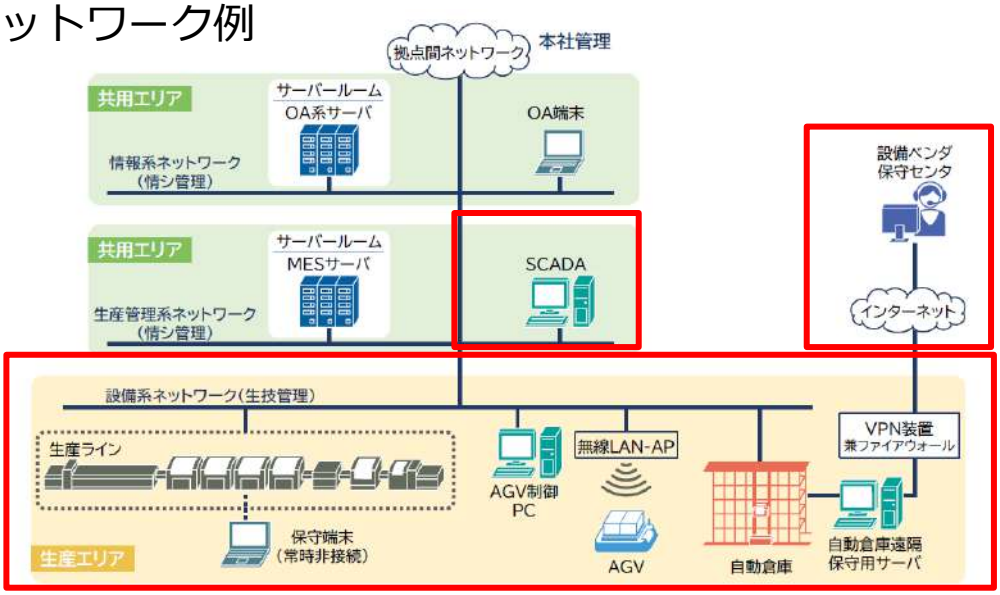


図 2-1 工場システムの例

19

セキスペ副業オンライン支援のビジネス化について

[良かった点]

- お二人とも、コンサルティングを生業としていることもあり、診断対象の担当者と関係をうまく構築しながら、**時間コントロール・経験に基づくアドバイス**など、適切な診断が実施できた。
- オンラインであることの弊害は想定以上に少なく、スムーズに進められた（一部Zoom不調なケースがあった）。
- 工場セキュリティは、本来のお二人の専門領域でない部分ではあったが、ITとOTのネットワークが分かれていないことが多く、結果的に、もともとのサイバーセキュリティ知識・経験が生きる内容となる場合が多かった。
- 工場セキュリティ・ガイドライン診断に関する教育ビデオ（4時間）を事前に視聴いただいたが、それなりに効果があった。
- 高橋様のように、リタイア後の人材スキル活用としては非常に有用である。（地域に根付いた町医者のイメージ）

[課題]

- ガイドライン診断のスキルよりは、短時間の対象者との関係構築が重要なことが分かった。今回の2名が特別に優秀だったこともあり、本業であまりコンサルティングをしていない方が対応できるのか。要はセキスペ人材の何%がこの事業に向いているかが不明。

  → もう少しサンプル数がほしい。スキマ副業という観点からは、オンラインが前提となるため。

20

総評

- 経済産業省のガイドラインチェックリストは、課題はあるものの
  中小企業の工場セキュリティのリスク把握に十分活用可能。
- セキスペによる工場セキュリティ診断（32項目）とアドバイス提供を1時間で実施できることがわかった。
  →ビジネス化に向けては良い結果
- ほとんどの対象者が「ひとりの詳しい方」「専業ではない方」にIT/OT両方のセキュリティ対策を頼っている状態。
  →ガバナンスは効きやすい反面、リソース不足の会社が多い。

DX推進においては、クラウド活用などのデジタル化が不可欠だが、
適切なセキュリティ対策を行うことで、ある程度リスクを取る判断がビジネスの発展につながる。
まずはセキュリティ対策を「自分事」として捉えることから始めましょう！

21