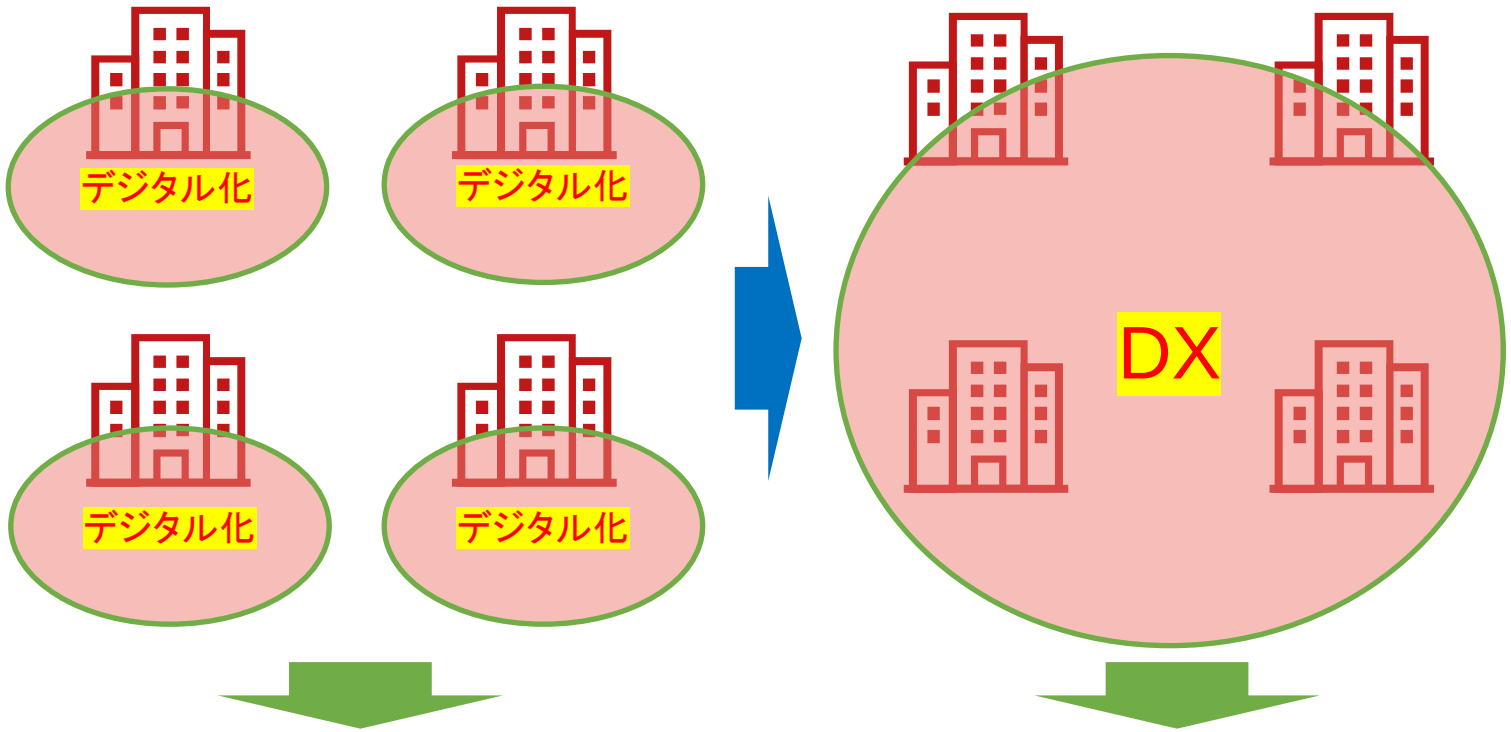
三重県　DX寺子屋
工場セキュリティ診断について

2023年2月15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

「DX × セキュリティ」の課題感と対策の方向性



サイバーセキュリティ
リスクへの対処は
自己責任

サイバーセキュリティ
リスクへの対処は
ビジネス参加条件

DX時代のサイバーセキュリティ課題

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

DX時代のサイバーセキュリティ

シェアリング・サブスク
（人材・運用・ルール）

相互連携・自動化

レジリエンス

自己紹介

佐々木　弘志

IPA 産業サイバーセキュリティセンター サイバー技術研究室 専門委員(非常勤)

Mission：「産業サイバーセキュリティの文化を創る」

・産業制御システム開発者（14年）
・産業制御システムセキュリティのコンサルタント（10年~）

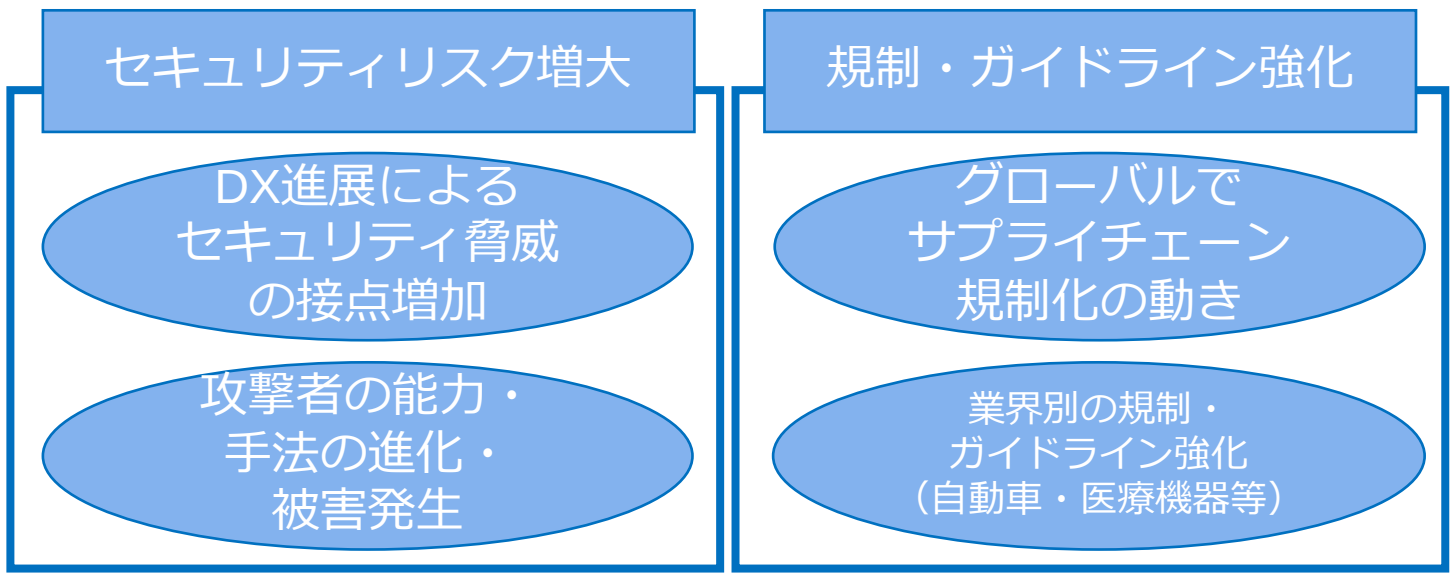
2016年5月～2020年12月,2021年7月～現在:
　・**経済産業省 サイバーセキュリティ課 情報セキュリティ対策専門官(非常勤)**
2017年７月～現在:
　・**IPA 産業サイバーセキュリティセンター サイバー技術研究室 専門委員(非常勤)**
2022年5月～現在:
　・**名古屋工業大学　産学官金連携機構　ものづくりDX研究所　プロジェクト准教授**
2021年～:
　・**産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）**
　　宇宙産業SWG セキュリティガイドライン検討委員
　　工場SWG セキュリティガイドライン検討委員(2022年1月～)

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



- 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）

経済産業省　工場セキュリティガイドライン公開（2022年11月）

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

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

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

工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン　～全体概要～

ガイドラインの背景・目的

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

→**いかなる工場でもサイバー攻撃のリスクあり**。

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

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

想定する読者の方

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

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

対策に取り組む効果

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

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

セキュリティ対策企画・導入の進め方

ステップ1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1** セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2** 業務の整理
- **ステップ1-3** 業務の重要度の設定
- **ステップ1-4** 保護対象の整理
- **ステップ1-5** 保護対象の重要度の設定
- **ステップ1-6** ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7** ゾーンと、セキュリティ脅威の影響の整理

ステップ2　セキュリティ対策の立案

- **ステップ2-1** セキュリティ対策方針の策定
- **ステップ2-2** 想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策
①ネットワークにおけるセキュリティ対策
②機器におけるセキュリティ対策
③業務プログラム・利用サービスにおけるセキュリティ対策

(2)物理面での対策
①建屋にかかわる対策
②電源／電気設備にかかわる対策
③環境(空調など)にかかわる対策
④水道設備にかかわる対策
⑤機器にかかわる対策
⑥物理アクセス制御にかかわる対策

ステップ3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策

(1)ライフサイクルでの対策
①運用・管理面のセキュリティ対策
A)サイバー攻撃の早期認識と対処（OODAプロセス）
B)セキュリティ対策管理(ID/PW管理、機器の設定変更など)
C)情報共有

②維持・改善面のセキュリティ対策
・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
・組織・人材のスキル向上（教育、模擬訓練等）

(2) サプライチェーン対策
・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認

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

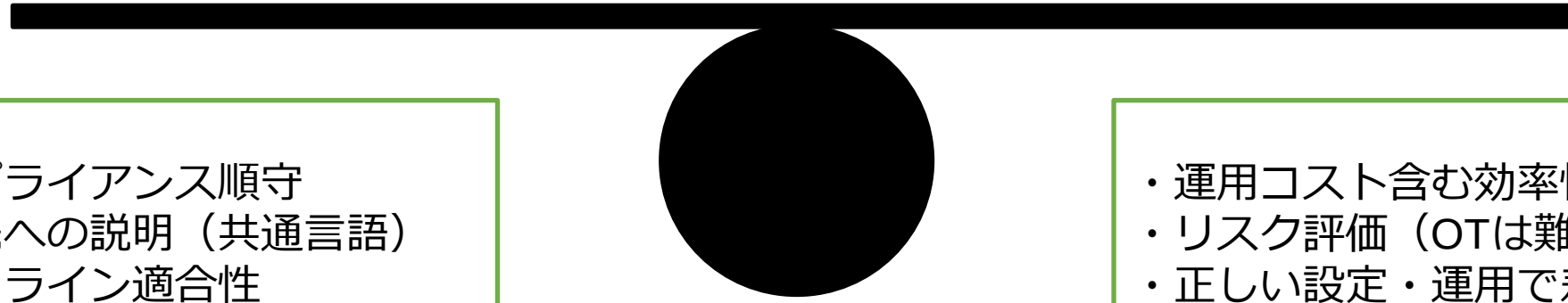
1

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

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

説明責任

実効性



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

但し、形骸化しやすいことに注意

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

組織・運用・技術のバランス大事

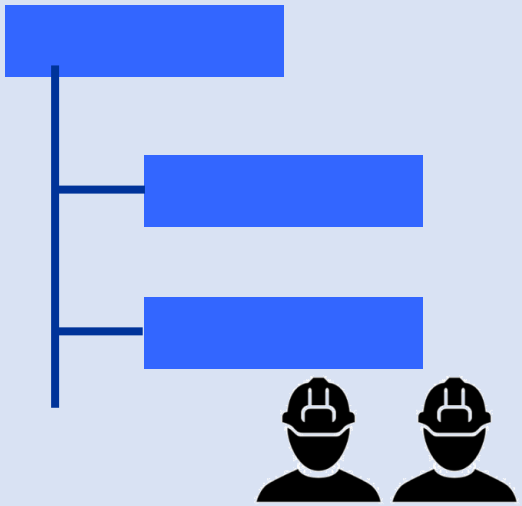
“経済産業省のガイドラインに適合しています！”

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

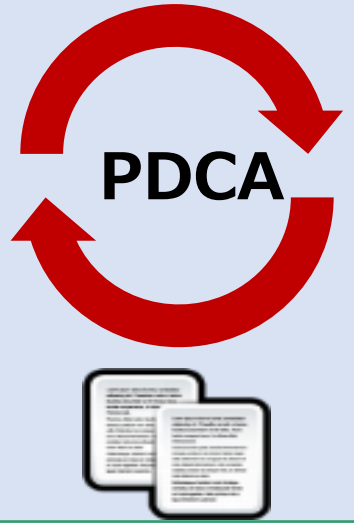
OTセキュリティの３要素

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

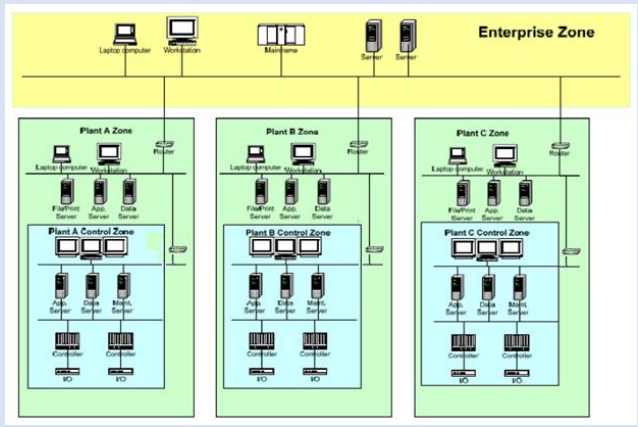
People



Process



Technology



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！)

組織的対策	
評価 D	スコア 28%
運用的対策	
評価 C	スコア 44%
技術的対策	
評価 D	スコア 36%
工場システムサプライチェーン管理	
評価 C	スコア 47%

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

工場セキュリティ簡易診断の結果例

本診断は「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」の付録Eのチェックリスト項目に準拠して作成しております。

分析結果シートの見方 ›

診断結果

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

総合評価

組織的対策
技術的対策
運用的対策
工場システムサプライチェーン管理

評価 C　スコア 41%

組織・運用・技術いずれも対策が不十分であり、課題が多くあるが、まずは組織の対策から始めるとよい。現状のままではセキュリティ上の侵害リスクが十分ある。既知のセキュリティ脅威で工場に有意な損害が出る状態と推定される。

組織的対策
評価 C　スコア 42%
経営層の理解が不十分であり、予算・人など基本的なリソースを十分得られていない。ガバナンス体制に課題があり、工場セキュリティの責任所在があいまいな状態である。

運用的対策
評価 D　スコア 38%
リスクアセスメントが不十分なため、対策の過不足が生じている可能性がある。資産管理が不十分なため、セキュリティ事故時の対応が遅れる。工場への外部記憶媒体の利用・持ち込みの制限がなく、外部からの脅威が容易に侵入できる。

技術的対策
評価 C　スコア 44%
端末保護が十分でないため、マルウェア感染のおそれがある。工場内のネットワークの脅威防護・検知が十分でないため、脅威が侵入できる可能性が高い。

工場システムサプライチェーン管理
評価 D　スコア 30%
制御システムベンダー・システム構築事業者との事故発生時の連絡体制が不十分なため、セキュリティ事故時の被害が拡大するおそれがある。サプライチェーンのセキュリティ管理ができていないため、調達先でのセキュリティ事故発生のリスクが把握できていない。

効果：

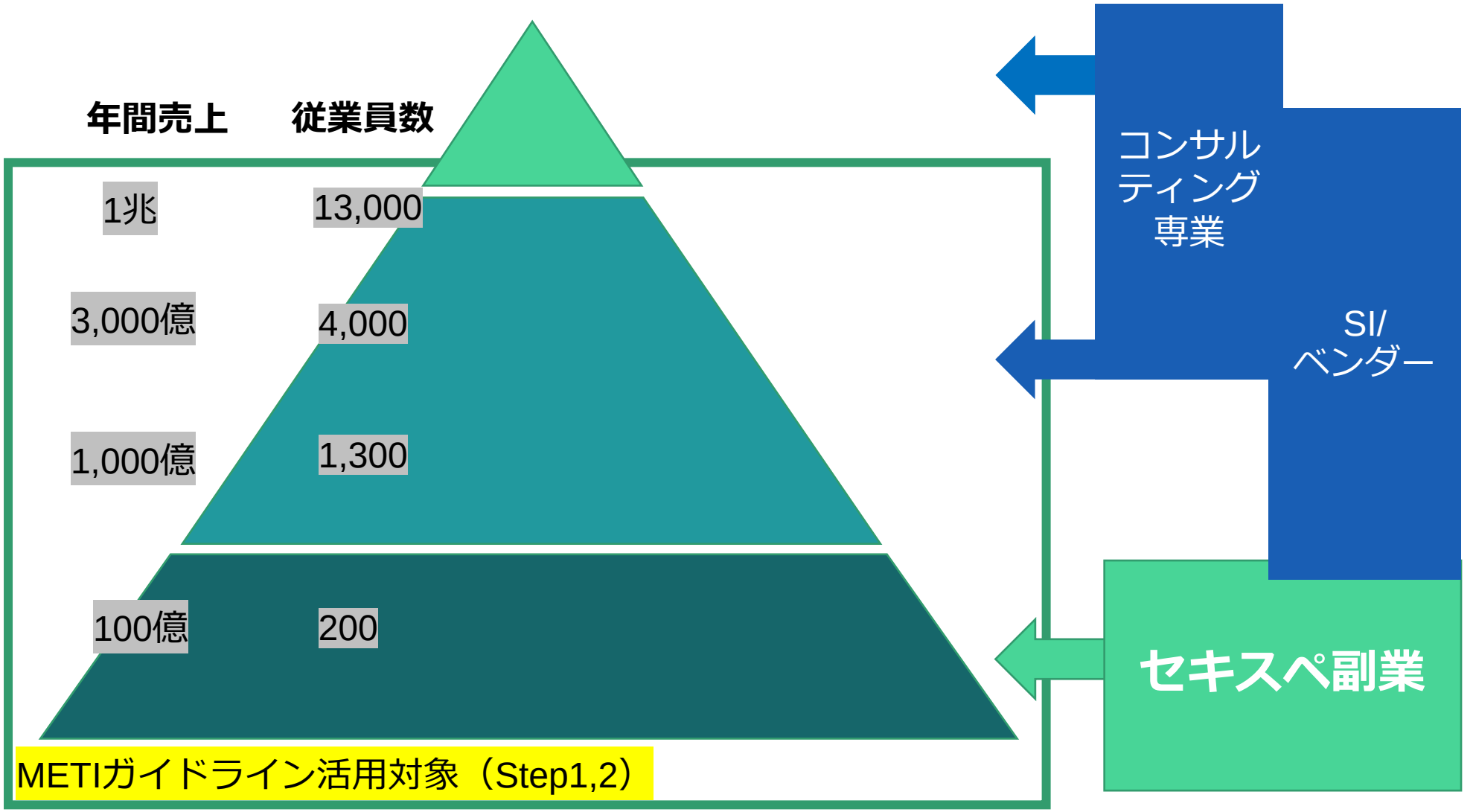
現状をラフに可視化できて
関係者に共通認識を形成できる

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

日本OTセキュリティのサプライチェーン全体の底上げ



コンサルティング専業

SI/ベンダー

セキスペ副業

製品導入支援

Web診断後のコンサル教育・ビデオ

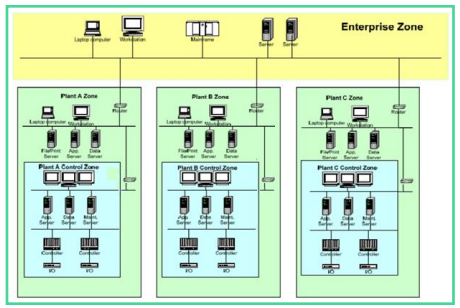
Web診断後の対策マニュアル

ガイドライン準拠Web診断

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

セキスペ・マッチ

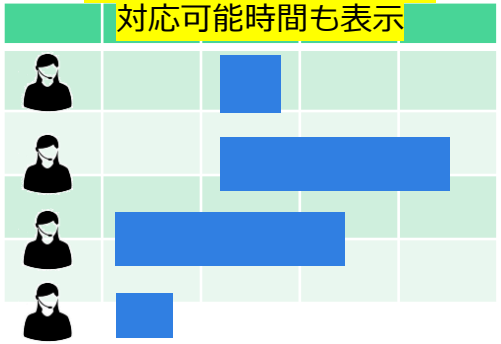
中小の製造事業者



コンサルお願いするよりも安く相談できてありがたい！
気軽に相談できる人だから契約続けよう

オンライン依頼

物理的に近い人が候補に
対応可能時間も表示



教育ビデオ・トレーニング・試験

登録・契約

セキスペ

工場セキュリティガイドライン
チェックリストの実施支援（1hのオンラインミーティング）

数万円

セキスペ・マッチに
支払い（時期応相談）

事務手続きのための
手数料

数万円

セキスペ・マッチが
代理払い（即時）

匿名化統計情報の販売・
レポートの国への提供
→状況可視化・政策に生かせる

スキマ時間で
副業できる
しかも自身のスキルアップ
にもなる！
セキスペになって
よかった！

METIガイドラインを活用した業界全体の
セキュリティレベルの底上げ
セキスペ・ビジネスの創出

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

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

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

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）

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。

OTセキュリティ簡易診断のWebサイト（15分程度）

＊ 実証実験の専用サイト

診断実施の当日の流れ（全体1時間）

●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、診断結果をお渡しします。

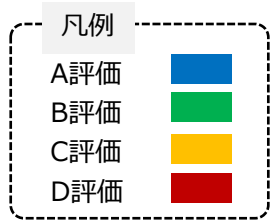
●診断結果に基づいた具体的対策を希望する方には、個別に対応します。（有償ベース）

三重県DX寺子屋の
工場セキュリティ診断の結果報告

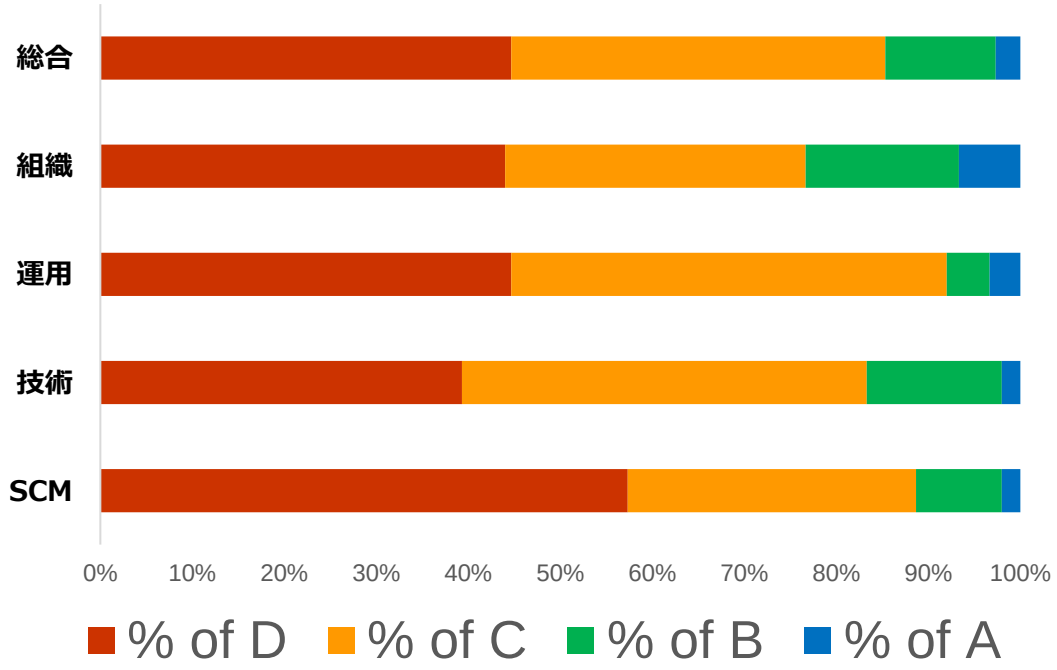
工場セキュリティ診断のまとめ

- 全16社実施
- カテゴリごとの平均スコア・評価

総合	43.3	C
組織	48.1	C
運用	40.1	C
技術	45.2	C
SCM	31.9	D



参考）別実施分の評価分布（約150社対象）



		総合	組織	運用	技術	SCM
150サイト	平均スコア	44.0%	45.6%	43.5%	44.7%	38.4%

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）

  → OTセキュリティの他のガイドラインに比べて、より基礎的（入門的）なものであり、**短時間**でポイントを抑えた現状把握が可能。
  中小企業の情報セキュリティガイドラインの「5分でできる情報セキュリティ自社診断」に相当。

- 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。

ネットワーク例

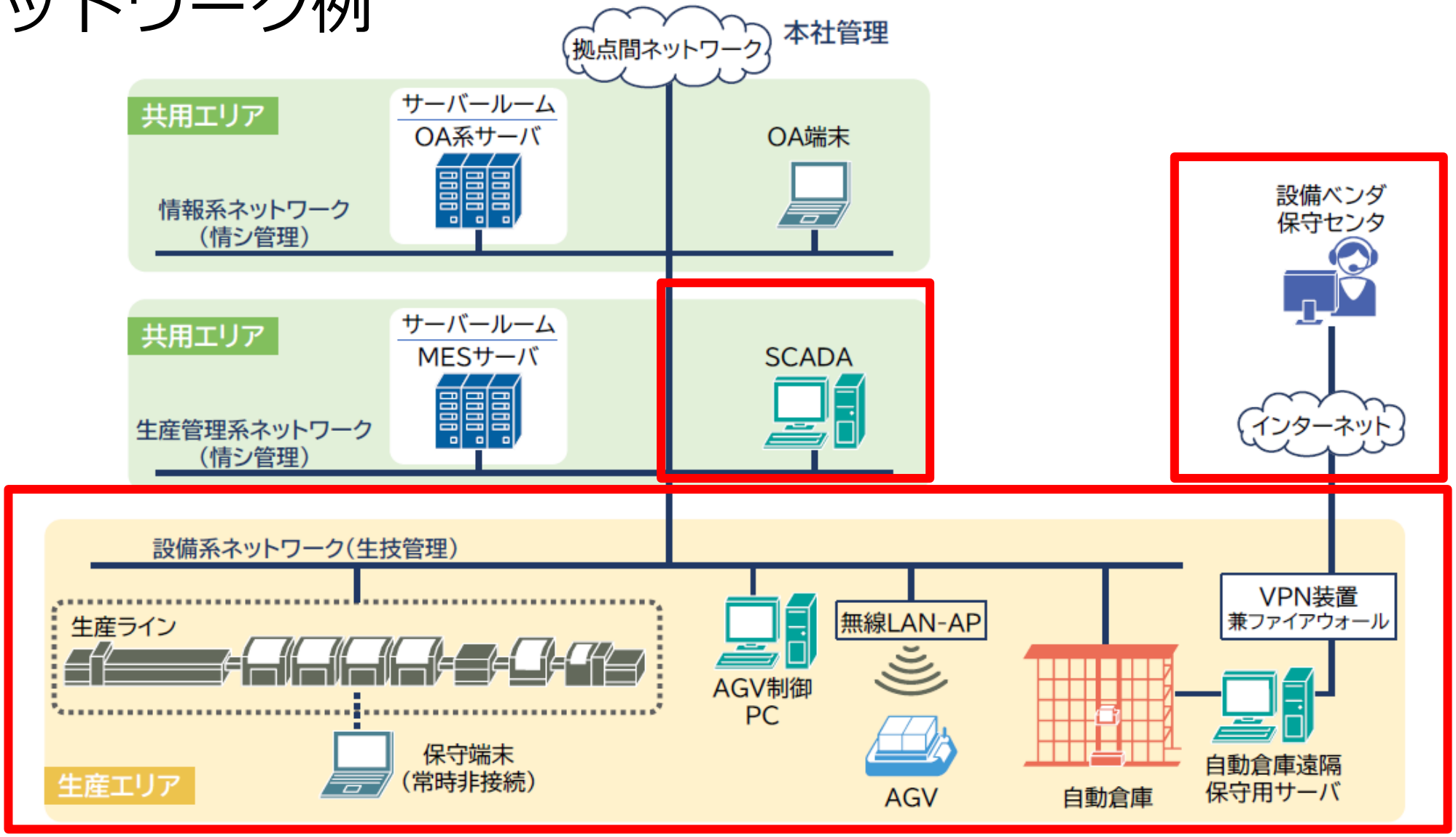


図 2-1　工場システムの例

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。

- チェック項目について、セキスペの方から、会社によっては判定に迷う、または違った判定をした部分があったとの声があった。

  → **診断側の判定基準の統一**という点からも、サンプル数を増やす必要がある。