



切っても切れないDXとセキュリティ

製造業OTのDX推進を考える
～ヒトとテクノロジーとセキュリティの観点から～

2024/6/5

製造業DX推進アプローチ研究会

C-1分科会成果物（一部編集）

JUASとは？？

一般社団法人 日本情報システム・ユーザー協会

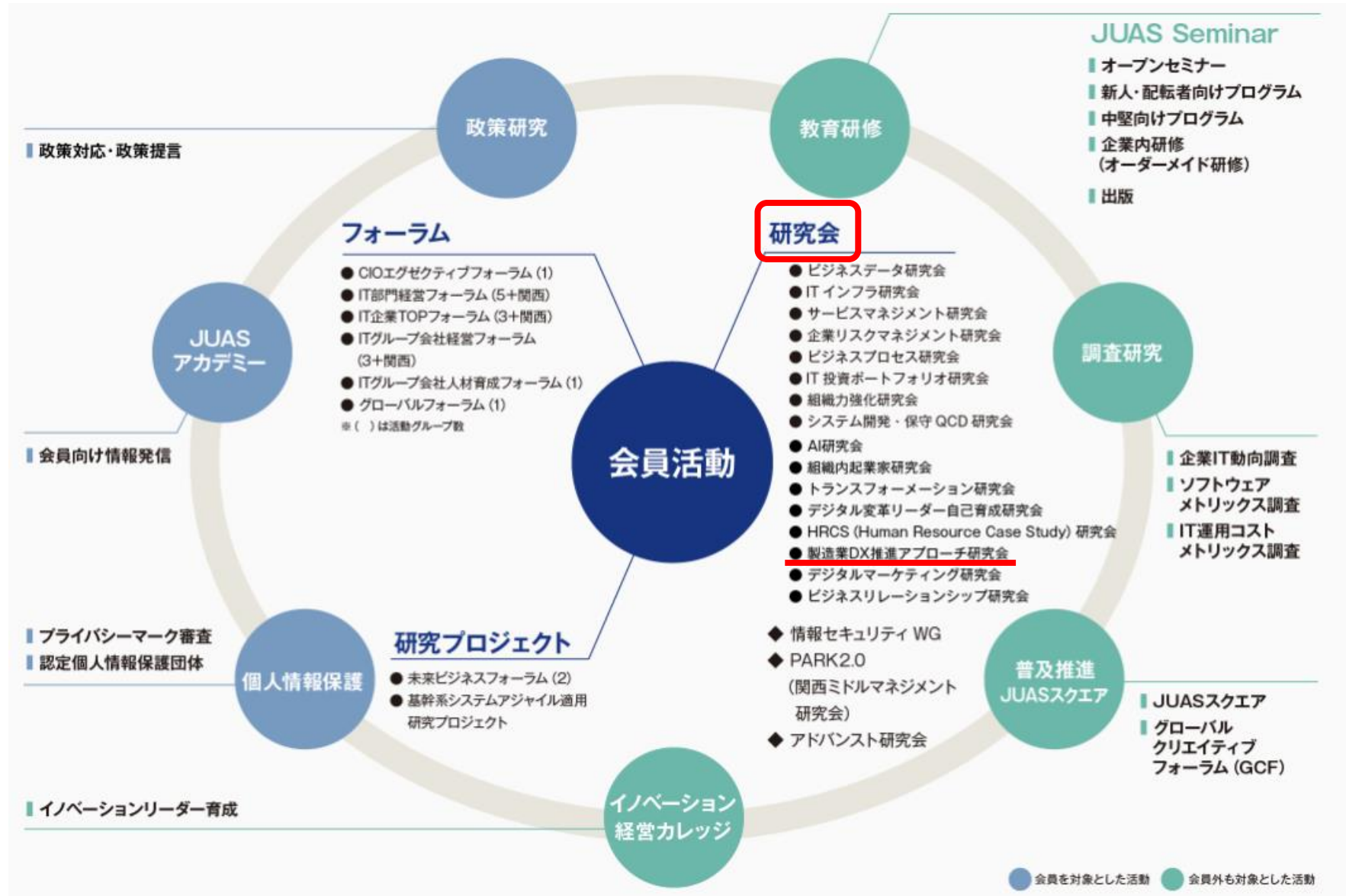
中立的なIT ユーザーの団体であり、ユーザーの立場から情報活用を推進するべく、現在、経営と情報に関するさまざまなテーマや立場に応じた40以上の研究会、委員会を開催し、年間のべ1,000名以上の会員が参加しています。

また、ユーザー団体ならではのセミナーを連日開催しています。

その他、毎年、「企業IT動向調査」や「ソフトウェアメトリックス調査」等充実した調査研究を行い、研究報告書を刊行し、各種提言を行っています。

(“JUASについて”より抜粋)

JUAS活動



製造業DX推進アプローチ研究会 テーマ

ビジネスモデル・組織

DXのあるべき姿
～内向きと外向きの
DX～

経営資源の調達と
組織体制

スマートファクトリー

切っても切れない
DXとセキュリティ

5 S活動による
CS対策推進案

成果物はWebで公開されてます。ご興味あればリンクよりご覧ください！

アジェンダ

1. テーマ設定
2. 仮説・検証
3. 結論・提言

アジェンダ

1. テーマ設定



2. 仮説・検証

3. 結論・提言

1. テーマ設定

“製造業のDX” ブレインストーミング

テーマ設定にあたり初めにスマートファクトリー、セキュリティをキーワードにして課題出し



スマートファクトリー = “攻め”とセキュリティ = “守り”で相反するアプローチとされていたが
議論の結果、結局ガバナンス・体制等に至る

1. テーマ設定

“製造業のDX” スマートファクトリーのゴール

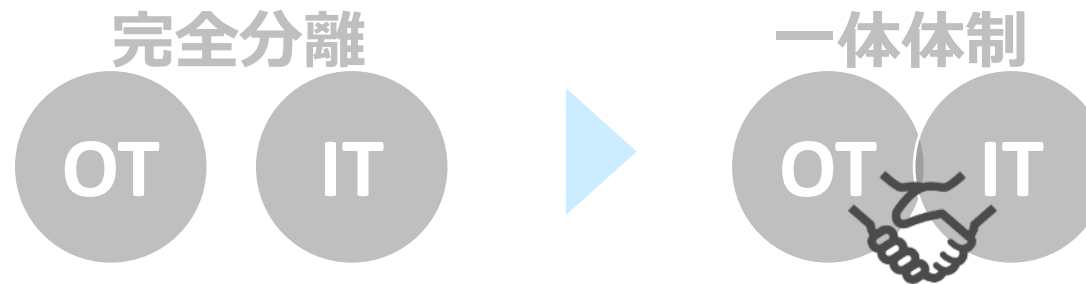
結局ガバナンス・体制等に至る

我々が考えたスマートファクトリーのゴール

◆標準化と技術確立のサイクルを組み入れること

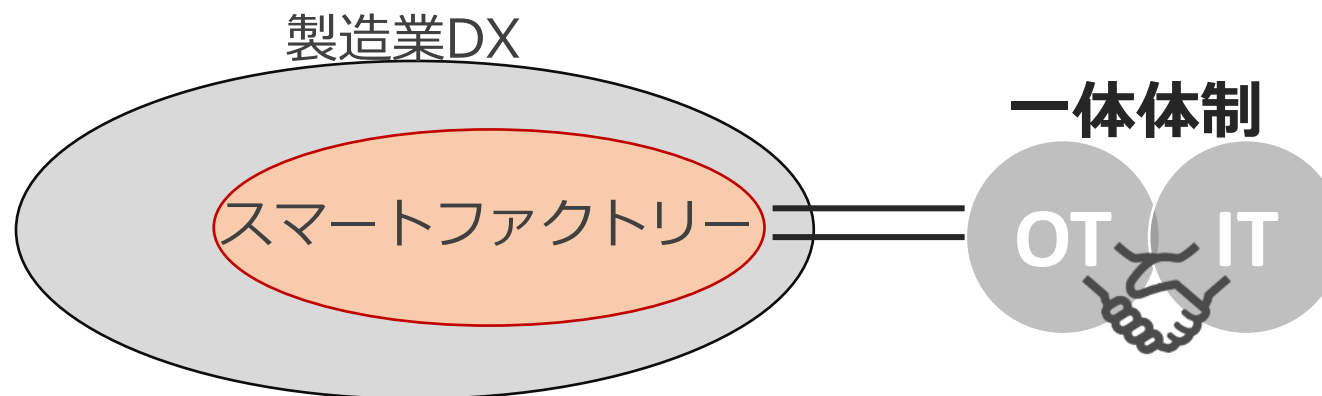
◆OTとITの一体体制(融合)によるビジネスへの貢献

※スマートファクトリー=AIやロボット活用に限定した話ではない



1. テーマ設定

IT・OT一体体制への到達とその過程



【1】スマートファクトリー実現のステップ

【2】自社の現在地

【3】セキュリティとの関連

上手く言語化し、取り組むべきワークを明確にしたい

アジェンダ

1. テーマ設定

2. 仮説・検証



3. 結論・提言

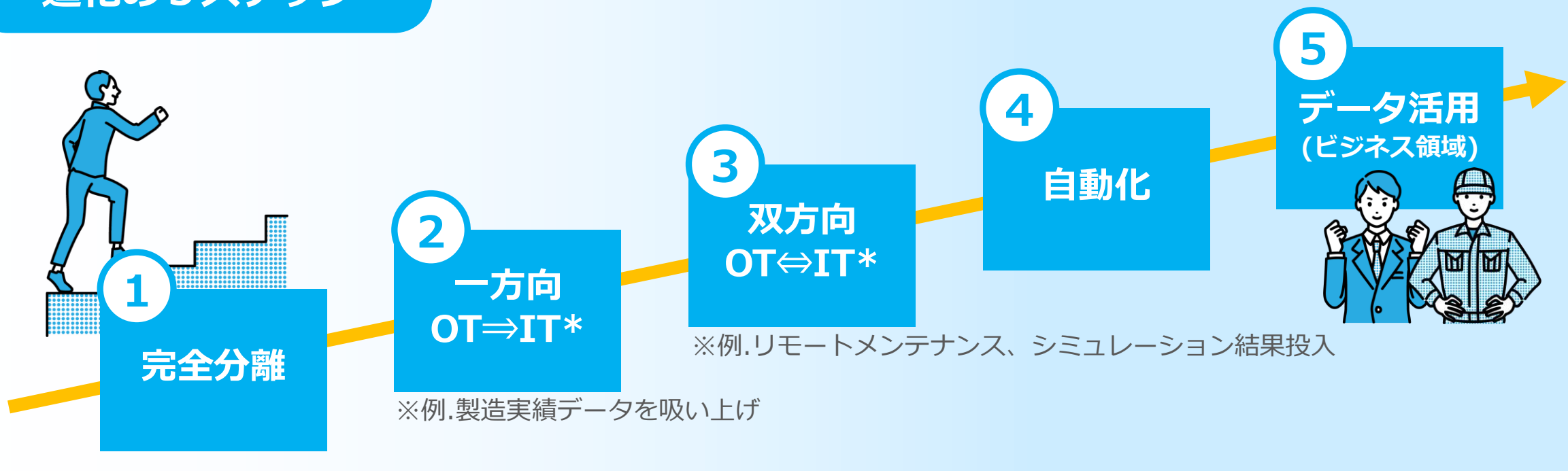
2. 仮説・検証

OT・IT一体体制への道

OT(現場)とITの一体体制を理想とした場合、どのような進化過程があるか？

⇒段階的に5つ程度のステップでフェーズ分けできるのでは？

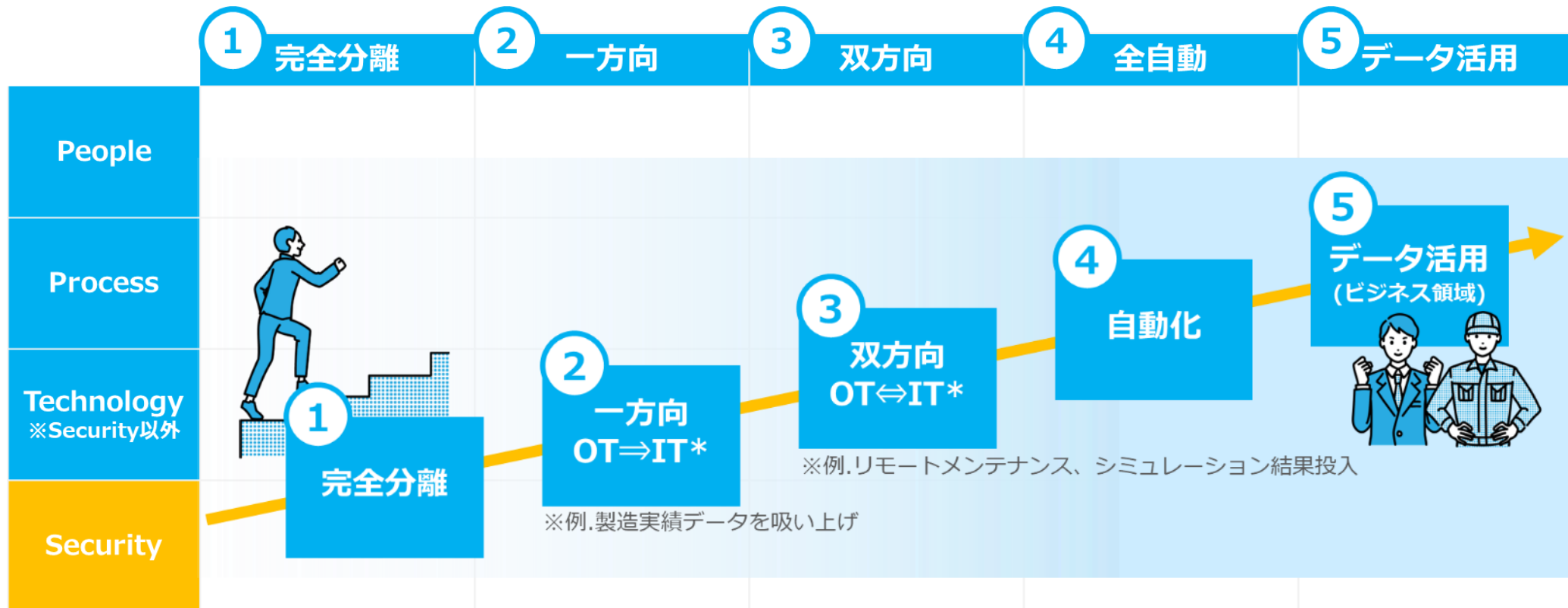
進化の5ステップ



2. 仮説・検証

各ステップのPeople, Process, Technology

各々のフェーズの特長を考えると、ひとつのロードマップとなりうるか？



2. 仮説・検証

各ステップの在り方と現在地の確認

下表がひとつの回答足りうる。では推進における鍵はなにか？

	① 完全分離	② 一方向	③ 双方向	④ 自動化	⑤ データ活用
People (人・文化)	IT/OTが独立・属人化	情報共有の取り組み 部分的なセキュリティ理解	一部がDXリテラシー保有 データサイエンスの取組	多数がDXリテラシー保有 SOC, CSIRT 現場とITの会話の質 マネジメント層の意識	DXのマインド・文化 (市場に目を向けた状態、 OT/ITが一体化した状態)
Process (規定・ポリシー)	IT/OTが独立・属人化 (全社の方針に基づくが、 IT/OT間の整合性が欠如)	一部のIT/OT通信を 例外的に許可	一部のIT/OT通信を 手続きベースで許可	IT/OT接続許認可の 煩雑な手続きからの脱却	シームレスな データ利活用体系
Technology ※Security以外	OT/ITが連携する 仕組みがない, 乏しい (管理系と現場系の独立)	IT/OTの接続 プロトコルの変換 システムの密結合	IT/OTの個別最適化 エッジコンピューティング	IT/OTの全体最適化 データレイク システムの疎結合化	デジタルツイン (売上予測～製造、調達等 サプライチェーン最適化)
Security	物理的な対策 (USB, シュレッダー)	NWのACL, 帯域制約 EPP導入	FW, IPS等による 境界型セキュリティ	GW経由のOT/IT間の通信 (シャドーIT防止) ログ・アクセスの即時解析 AIによる振舞検知	サプライチェーンを 含めたセキュリティ

2. 仮説・検証 各ステップの“壁”

- 物理的・予算的制約及び、組織的な要因が障害となりうるのでは？ ⇒(a)DX推進要素
- どのフェーズにおいても、セキュリティの取組は必須なのは？ ⇒(b)セキュリティ推進要素

	1 完全分離	2 一方向	3 双方向	4 自動化	5 データ活用
People (人・文化)	IT/OTが独立・属人化	情報共有の取り組み 部分的なセキュリティ理解	一部がDXリテラシー保有 データサイエンスの取組	多数がDXリテラシー保有 SOC, CSIRT 現場とITの会話の質 マネジメント層の意識	DXのマインド・文化 (市場に目を向けた状態、 OT/ITが一体化した状態)
Process (規定・ポリシー)	IT/OTが独立・属人化 (全社の方針に基づくが、 IT/OT間の整合性が欠如)	一部のIT/OT通信を 例外的に許可	一部のIT/OT通信を 手続きベースで許可	IT/OT接続許可の 煩雑な手続きからの脱却	シームレスな データ利活用体系
Technology ※Security以外	OT/ITが連携する 仕組みがない、乏しい (管理系と現場系の独立)	IT/OTの接続 プロトコルの変換 システムの密結合	IT/OTの個別最適化 エッジコンピューティング	IT/OTの全体最適化 データレイク システムの疎結合化	デジタルツイン (売上予測～製造、調達等 サプライチェーン最適化)
Security	物理的な対策 (USB, シュレッダー)	NWのACL, 帯域制約 EPP導入	FW, IPS等による 境界型セキュリティ	GW経由のOT/IT間の通信 (シャドーIT防止) ログ・アクセスの即時解析 AIによる振舞検知	サプライチェーンを 含めたセキュリティ

物理的な壁
※リソースの制限
人、金、物

組織的な壁
※ポリシー統一の難しさ

個別最適からの全社最適への変革の壁

全社最適からのサプライチェーン全体最適の壁

2. 仮説・検証

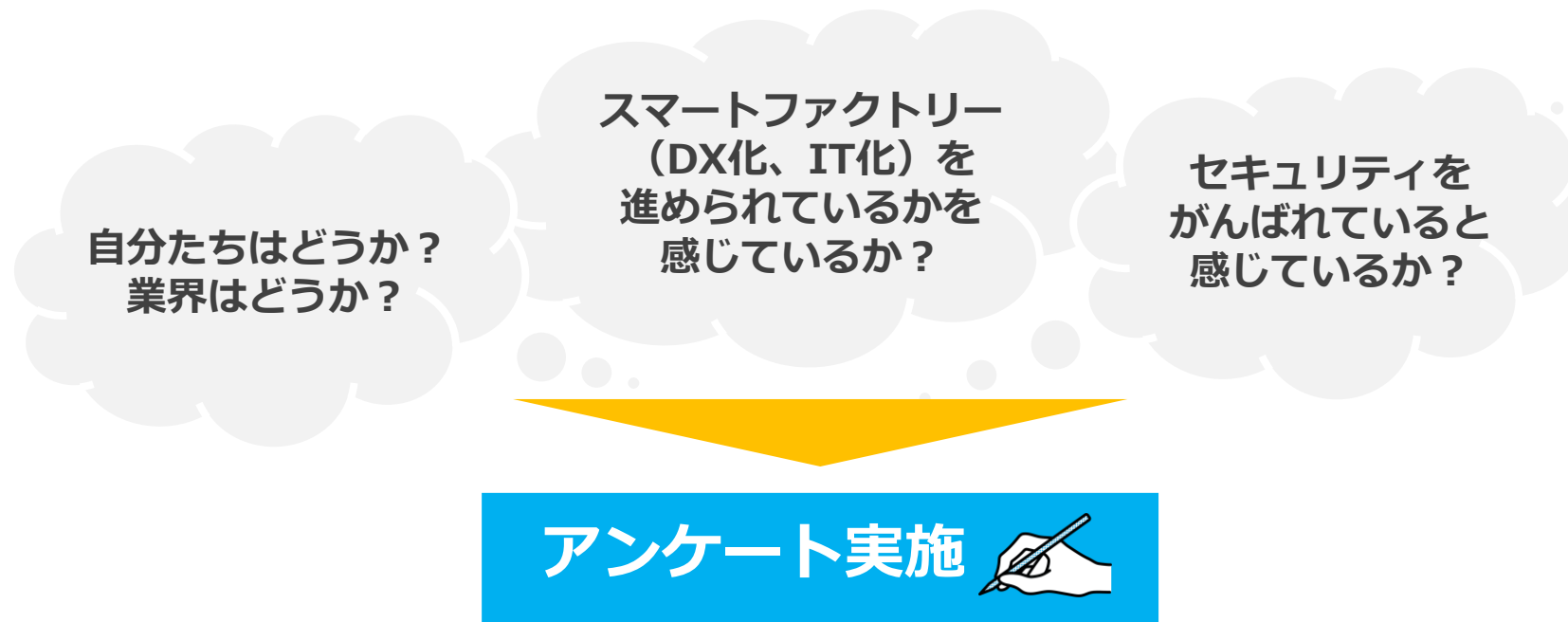
傾向分析：アンケート

(a)DX推進要素

この定性的な2要素を見える化することで、

(b)セキュリティ推進要素

スマートファクトリー推進の傾向・知見が得られるのではないか？



アンケートの設問はすでにある以下の指標をベースに作成

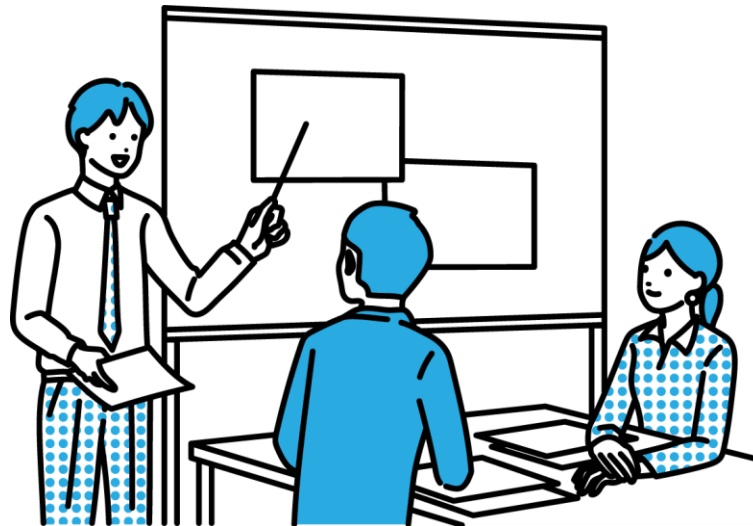
- ◆工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
- ◆DX推進指標自己診断フォーマットver2.4

2. 仮説・検証

対象 : 製造業DX推進アプローチ研究会 + α

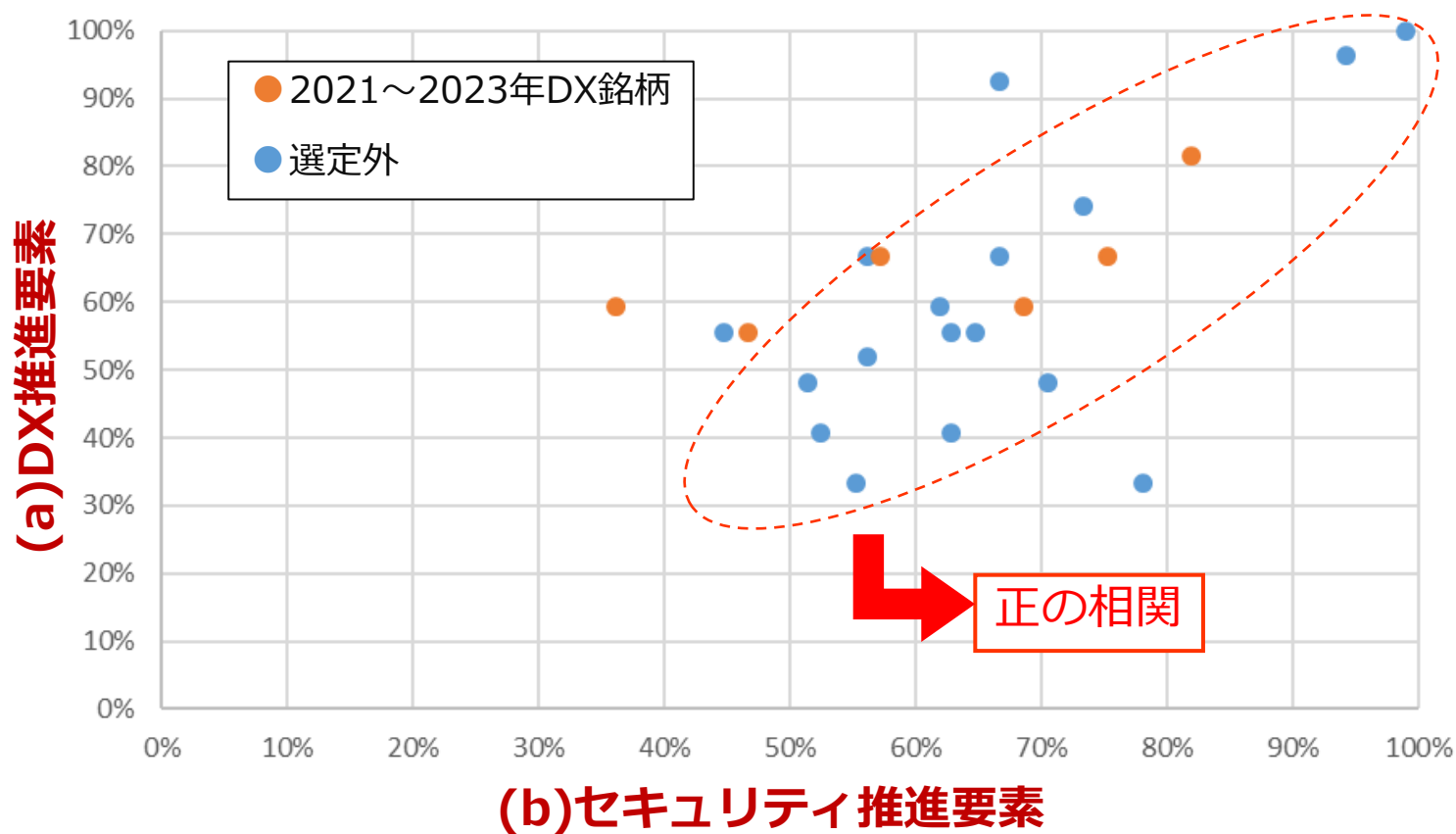
回答数 : 24名

ご回答いただいた皆さま、ありがとうございました！



2. 仮説・検証

DX要素とセキュリティ要素は協調



縦軸：◆DX推進指標自己診断フォーマットver2.4

横軸：◆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

評価：○→3pt, △→2pt, ×/不明→1ptとして比率で表示

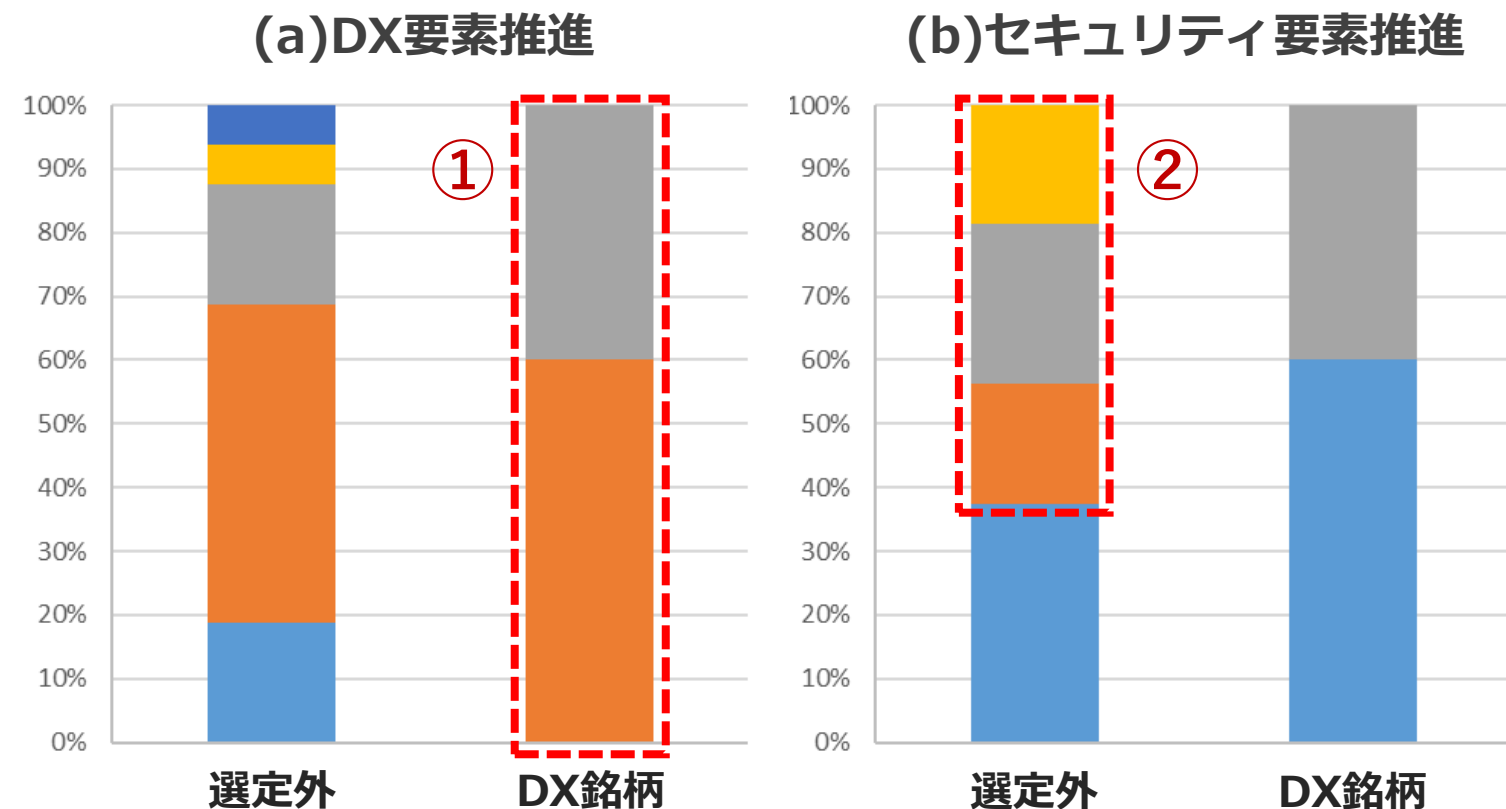
➤ (a)(b)の推進具合は正の相関

➤ DX銘柄は(a)のバラツキが小さい

Fig.1 DX推進指標×セキュリティ対策指標

2. 仮説・検証

各要素の推進度合い



自社の推進度合い

- 100% (充分に取り組んでいる)
- 80%
- 60%
- 40%
- 20% (あまり取組めていない)

- ① : DX銘柄は、DX要素推進に関し40-60%と安定
- ② : 選定外企業は、セキュリティの強化が目下の取組課題

Fig.2 “DX推進銘柄”による層別

アジェンダ

1. テーマ設定

2. 仮説・検証

3. 結論・提言



3. 結論・提言

アンケート結果より

- DX推進は…
 - ① **組織の文化が重要**
⇒選定企業：リーダーが文化を醸成した（している）状態
まずはリテラシの高いキーパーソンを！
 - ② **セキュリティの推進が必要**
⇒IT/OTの情報資産をまもり活用する基盤を！
- DXとセキュリティは正の相関＝推進の両輪である

3. 結論・提言

製造業のDX、スマートファクトリーとは

- 社内の体制・ガバナンス、DX文化を醸成する
- 個別から全体最適へ移行する
- 製造現場（OT）とIT環境間で能動的なデータ活用ができる
- 現場作業のノウハウやスキルをデジタル化する
- 仮想製造環境（デジタルツイン）を活用して検証やシミュレーションができる

切っても切れないDXとセキュリティ、
みんなで壁を突破しましょう！



END

ご清聴ありがとうございました。

