令和5年度
中小企業サイバーセキュリティ対策
継続支援事業

これからの企業経営で必要な攻めと守りのIT活用および
サイバーセキュリティ対策

サイバーセキュリティ
人材育成
社内体制整備支援

セミナー内容

回数	テーマ
第1回	サイバーセキュリティを取り巻く環境および中小企業に 求められるサイバーセキュリティ対策
第2回	これからの企業経営で必要な攻めと守りのIT活用および サイバーセキュリティ対策
第3回	サイバーセキュリティに関する国の方針・施策および サイバー脅威の動向
第4回	サイバーセキュリティ対策におけるフレームワークの体系
第5回	組織として策定すべき対策基準及び情報セキュリティの 三大要素【対策基準レベル①】

セミナー内容

回数	テーマ
第6回	セキュリティリスク評価及び対策基準に記載されるべき管理策【対策基準レベル②】
第7回	組織として実施すべき具体的な対策事項・手順【実施手順・実施者マニュアルレベル①】
第8回	組織的対策と人的対策【実施手順・実施者マニュアルレベル②】
第9回	技術的対策と物理的対策およびセキュリティ対策状況の有効性評価【実施手順・実施者マニュアルレベル③】
第10回	全体総括

１． 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

これからの企業経営で必要な観点：社会の動向

守りのIT投資と攻めのIT投資

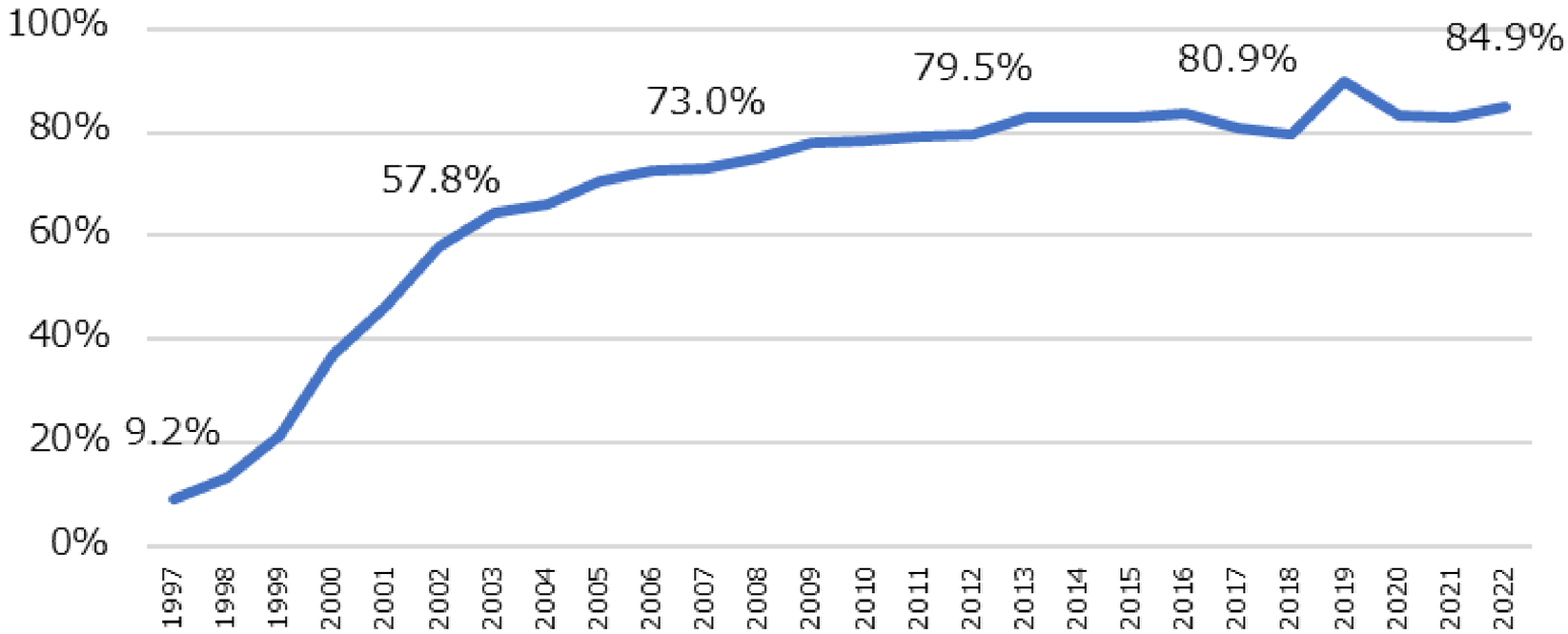
経営投資としてのサイバーセキュリティ対策

これからの企業経営で必要な観点：社会の動向

【参照：セミナーテキスト4-1-1.】

インターネットの利用率

インターネットの普及とともに、現実社会とサイバー空間が密接に結びつき、私たちの生活やビジネスに大きな変革をもたらしている。



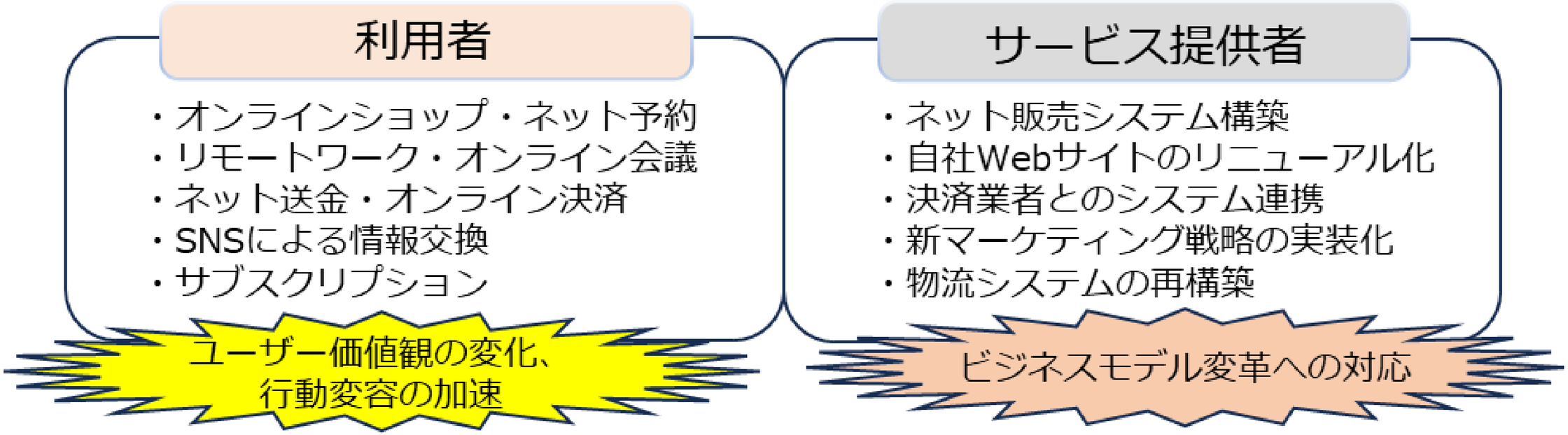
インターネット利用率（個人）の推移
（出典） 総務省「通信利用動向調査」を基に作成

これからの企業経営で必要な観点：社会の動向

【参照：セミナーテキスト4-1-1.】

デジタル時代の競争：革新と選択肢の拡大

インターネットの普及とともに、利用者はより価値あるサービスを選択することが可能になった。
ITサービス提供者は、常に最新のサービス提供が求められるため、革新的なアイディアと素早い行動が求められる。

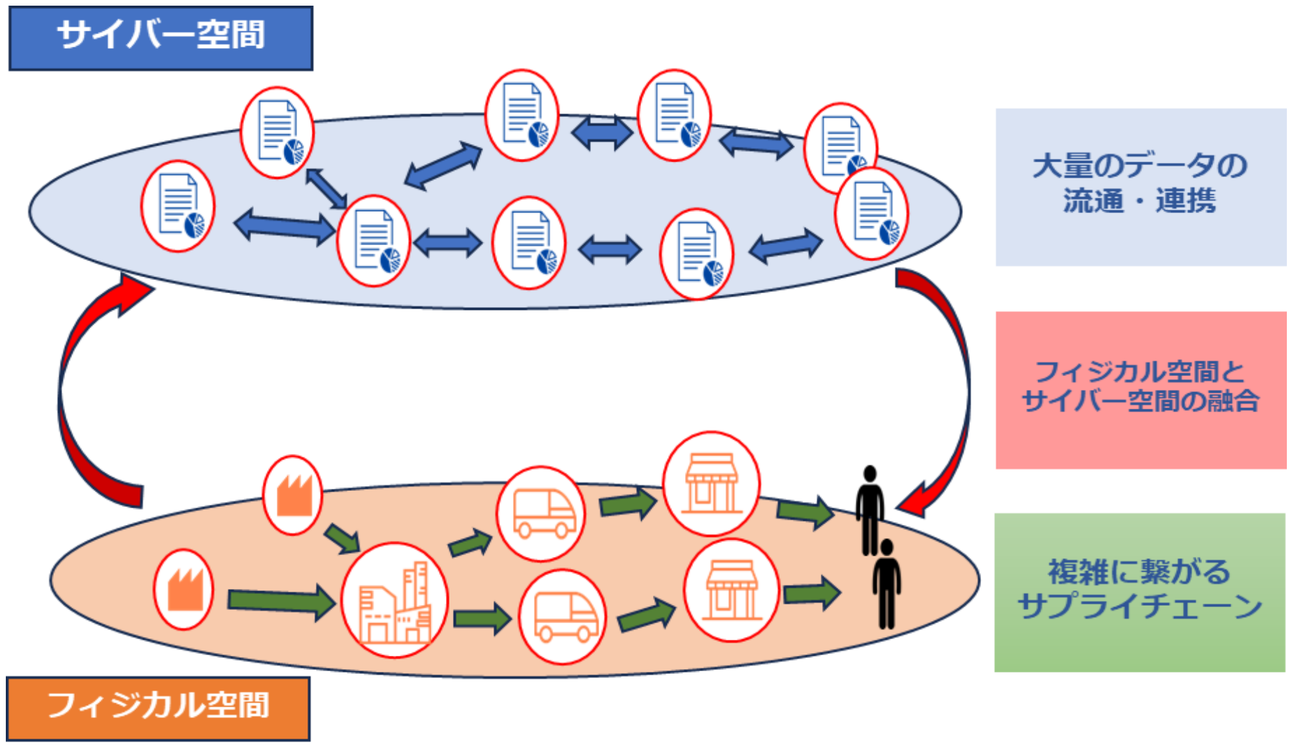


これからの企業経営で必要な観点：社会の動向

【参照：セミナーテキスト4-1-1.】

フィジカル空間とサイバー空間の融合

Society5.0で実現する社会では、サプライチェーンにIoTやAIが導入され、製造や物流がサイバー空間で監視・制御されるようになる。また、クラウドの普及に伴い情報共有が容易になることで、**サプライチェーンが可視化**され、フィジカルとサイバー空間が密接に融合する。



サイバー空間とフィジカル空間の関係図
（出典） 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワークVer.1.0」を基に作成

これからの企業経営で必要な観点：社会の動向

【参照：セミナーテキスト4-1-2.】

日本のデジタル化は後れている！！

後れをとった6つの理由

1. ICT投資の低迷
2. 業務改革などを伴わないICT投資
3. ICT人材不足・偏在
4. 過去の成功体験
5. デジタル化への不安感・抵抗感
6. デジタルリテラシーが十分ではない

これからの企業経営で必要な観点：社会の動向

【参照：セミナーテキスト4-1-2.】

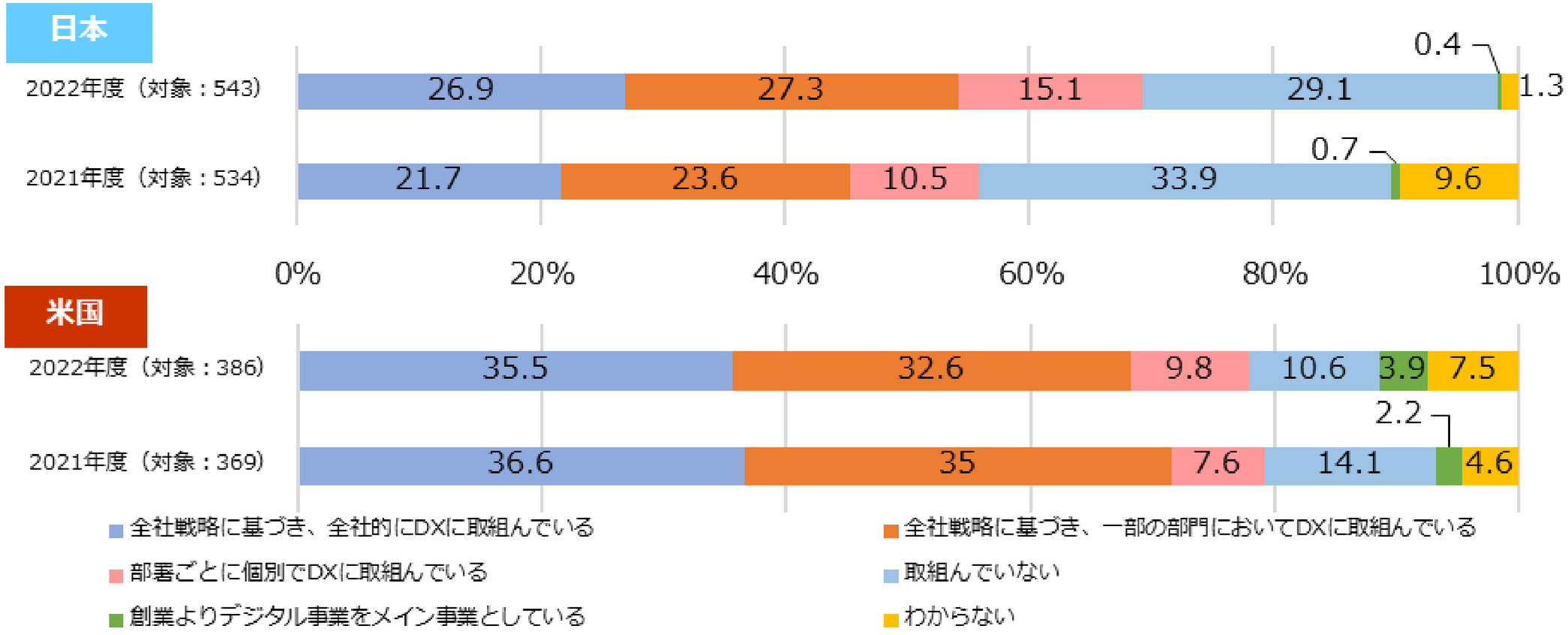
1. ICT投資の低迷

- 我が国のICT投資は1997年をピークに減少中。
- ICT投資の8割は現行ビジネス維持・運営に使われ、レガシーシステムが多い。
- 現代の変化に適応するアジャイル開発が推奨されるが、ウォーターフォール型が主流でアジャイル導入が遅れている。
- オープン化、クラウド化、業務・データ標準化の対応が遅れ、業務効率化・データ活用が不十分。

これからの企業経営で必要な観点：社会の動向

【参照：セミナーテキスト4-1-2.】

DXの取組状況

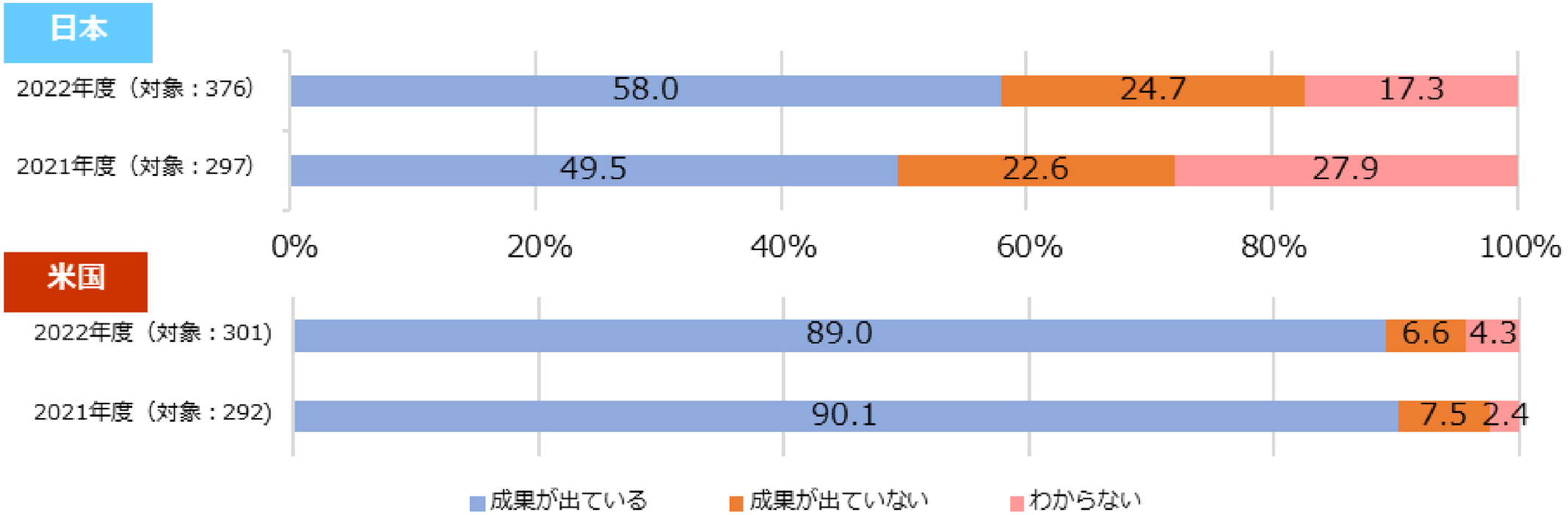


DXの取組状況
（出典） IPA「DX白書2023」を基に作成

これからの企業経営で必要な観点：社会の動向

【参照：セミナーテキスト4-1-2.】

DXの取組の成果



DXの取組の成果
（出典） IPA「DX白書2023」を基に作成

これからの企業経営で必要な観点：社会の動向

【参照：セミナーテキスト4-1-2.】

2. 業務改革などを伴わないICT投資

- 我が国のICT導入は、主に業務の効率化の手段として使用される。
- 情報システム開発はコア業務とは見なされず、外部企業への依存が高まっている。
- この外部委託の依存により、ノウハウやスキルの蓄積が委託元企業で不足。
- 業務改革を伴わないICT導入が多く、十分な効果が発揮されず、デジタル化への更なる投資が後れている。
- ICT投資の効果を最大化するには業務改革や組織の改編が必要。

これからの企業経営で必要な観点：社会の動向

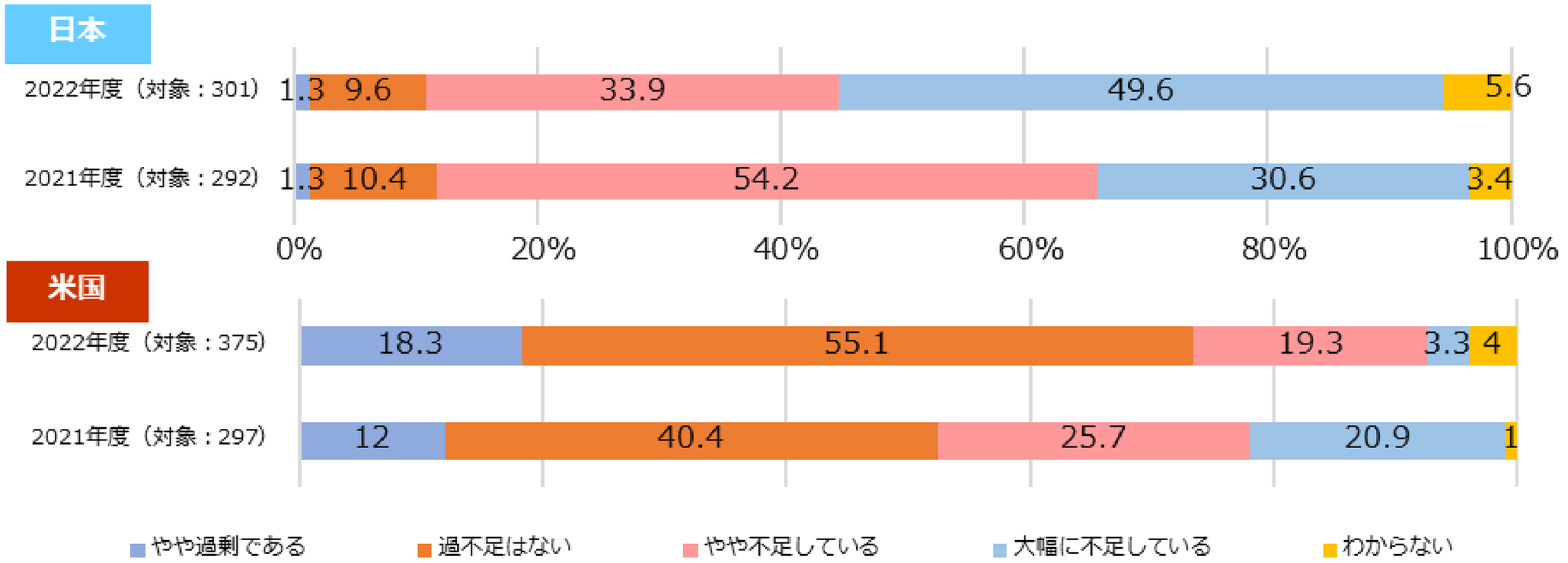
【参照：セミナーテキスト4-1-2.】

3. ICT人材不足・偏在

- ICT人材はデジタル化の推進に不可欠。
- IPAの2022年度調査：IT人材の量について、83.5%が「大幅に不足」または「やや不足」と回答。
- 時代に応じて変わるICT人材の要件：情報セキュリティやアジャイル開発などの高度なスキルが求められる。
- IT人材の質に関しても、86.1%が「大幅に不足」または「やや不足」と回答。
- 我が国のユーザー企業は、ICT人材の量・質ともに不足していると認識。
- 我が国では外部ベンダーへの依存度が高く、ユーザー企業内でのICT人材の育成・確保が不十分。

これからの企業経営で必要な観点：社会の動向

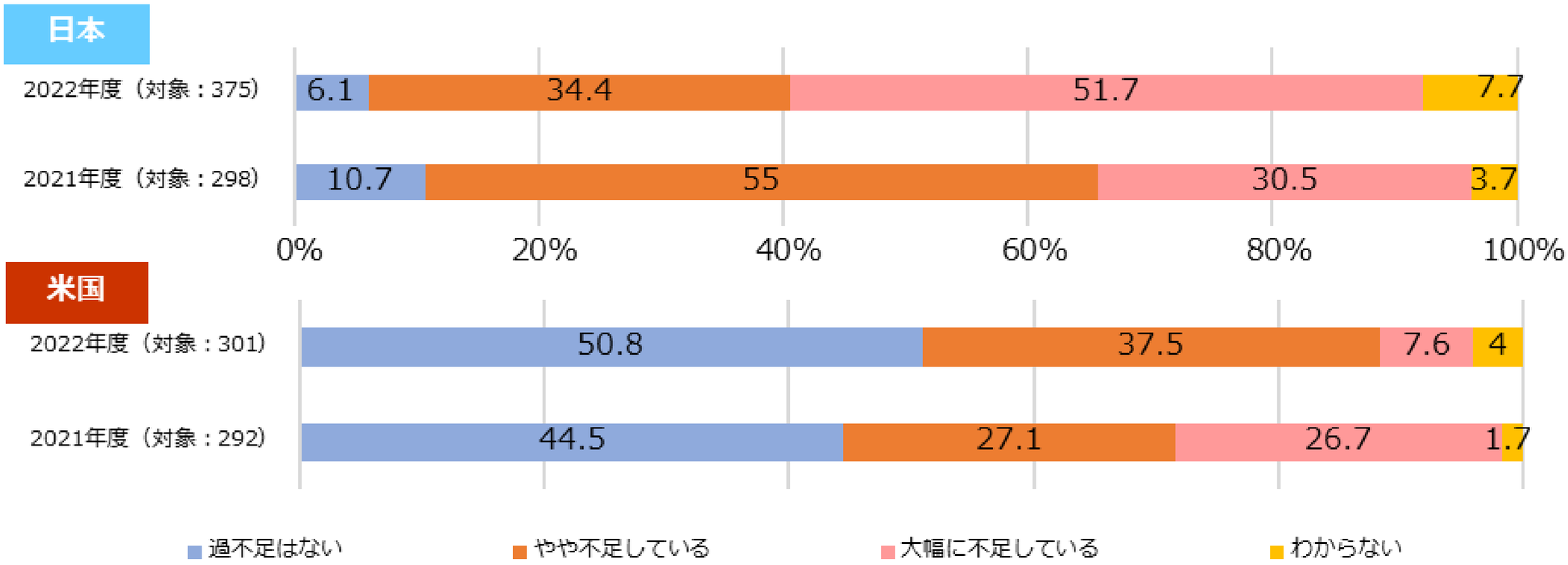
DXを推進する人材の「量」の確保



DXを推進する人材の「量」の確保
（出典） IPA「DX白書2023」を基に作成

これからの企業経営で必要な観点：社会の動向

DXを推進する人材の「質」の確保



DXを推進する人材の「質」の確保
（出典） IPA「DX白書2023」を基に作成

これからの企業経営で必要な観点：社会の動向

【参照：セミナーテキスト4-1-2.】

4. 過去の成功体験

- 我が国は高度経済成長期後、世界の経済大国となり、「電子立国」と称された。
- 2000年代に、ICT関連製造業の生産・輸出が減少。
- 以前の成功に固執し、デジタル化への適応が不十分。
- 国民生活・社会活動は維持できており、デジタル化の緊急性を感じていない。
- 技術での解決を、人材の質・量で補っている。
- デジタル化による生産性向上の余地があるが、「ゆでガエル現象」の可能性。
- 新興国では、制約の少ないデジタル環境で「リープフロッグ」が起きている。

これからの企業経営で必要な観点：社会の動向

【参照：セミナーテキスト4-1-2.】

5. デジタル化への不安感・抵抗感

- デジタル化に対する不安感・抵抗感を持つ人が存在する。
- デジタル化により、情報セキュリティなどの新しい脅威が出現。
- 総務省調査：デジタル化が進んでいない主な理由は「情報セキュリティやプライバシー漏洩への不安」（52.2%）。
- パーソナルデータの不適切な利用、ネット上の偽情報、デジタル操作への不慣れなどが不安感・抵抗感の要因。

これからの企業経営で必要な観点：社会の動向

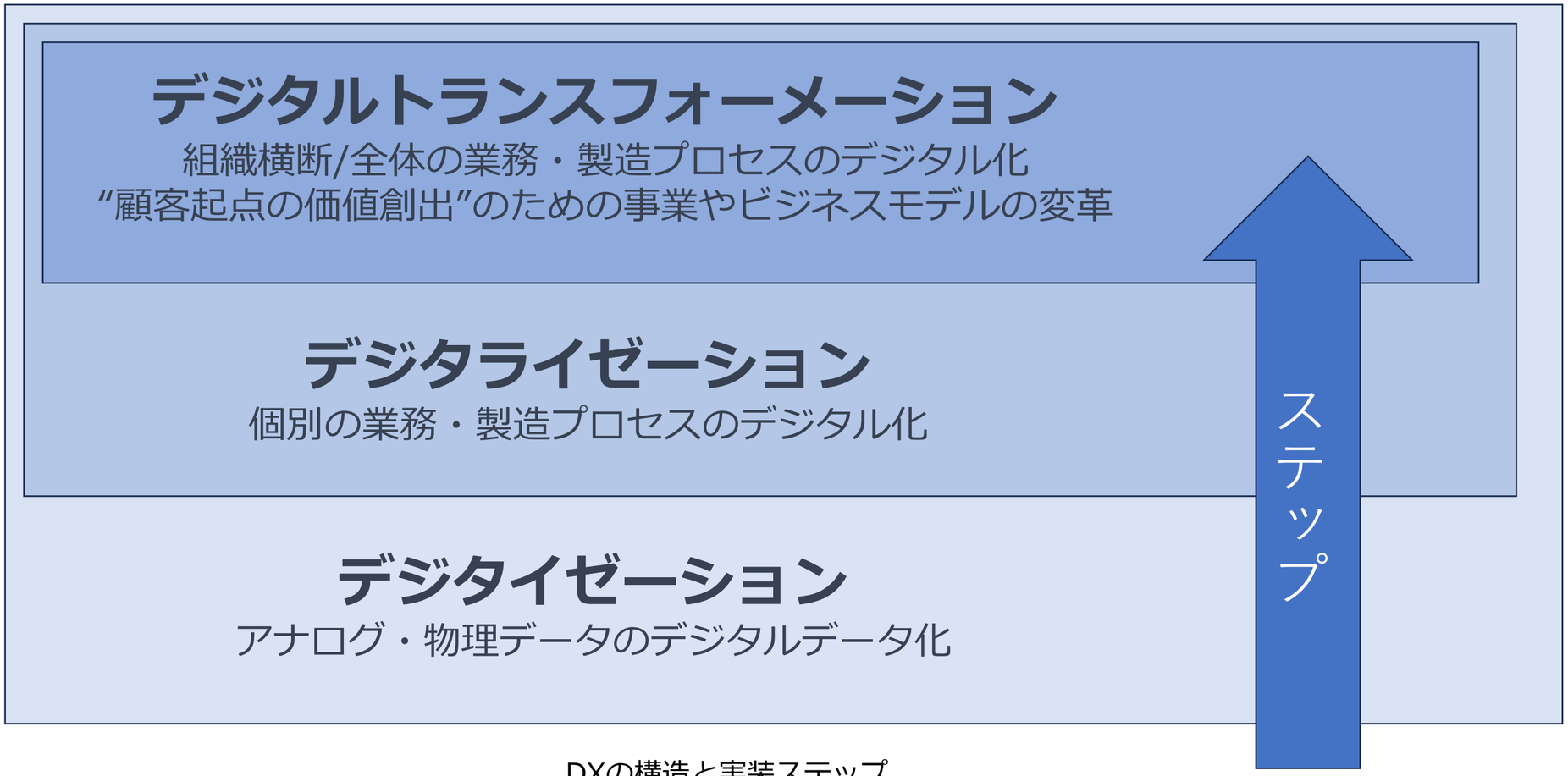
【参照：セミナーテキスト4-1-2.】

6. デジタルリテラシーが十分ではない

- 情報セキュリティや偽情報対応には情報リテラシーが必要。
- 総務省の調査: デジタル化未進の理由の2番目は「利用者のリテラシー不足」(44.2%)。
  ※1番目は前述の「情報セキュリティやプライバシー漏洩への不安」（52.2%）。
- デジタルリテラシー不足は、デジタル化推進への消極的態度の原因となる可能性。

守りのIT投資、攻めのIT投資

DXの構造と実装STEPを理解する



DXの構造と実装ステップ
（出典） 経済産業省「DXレポート2」を基に作成

守りのIT投資、攻めのIT投資

DXフレームワーク

	未着手	デジタイゼーション	デジタライゼーション	デジタルトランスフォーメーション
ビジネスモデルのデジタル化				ビジネスモデルのデジタル化
製品／サービスのデジタル化	非デジタル製品/サービス	デジタル製品	製品へのデジタルサービス付加	製品を基礎とするデジタルサービス デジタルサービス
業務のデジタル化	紙ベース・人手作業	業務/製造プロセスの電子化	業務/製造プロセスのデジタル化	顧客とのE2Eでのデジタル化
プラットフォームのデジタル化	システムなし	従来型ITプラットフォームの整備		デジタルプラットフォームの整備
DXを進める体制の整備	ジョブ型人事制度 リカレント教育	CIO/CDXOの強化 リモートワーク環境整備	内製化	

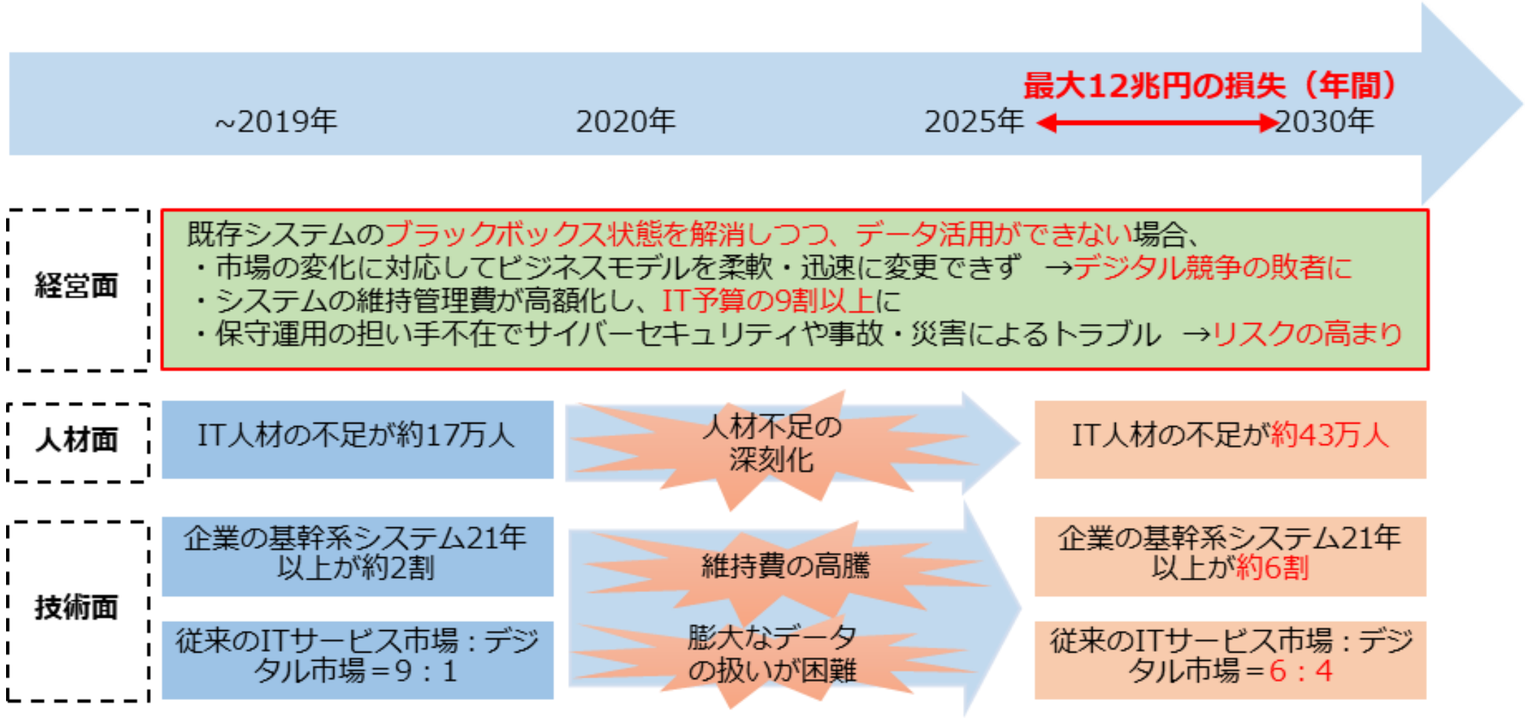
DXフレームワーク
（出典） 経済産業省「DXレポート2」を基に作成

2025年の崖

【参照：セミナーテキスト4-2-2.】

2025年の崖が示す課題

項番	課題
課題1	既存システムのレガシーシステム化
課題2	IT人材不足の深刻化
課題3	システム維持費の高騰
課題4	サイバーセキュリティや災害リスクの高まり
課題5	各種システムのサポート終了



「2025年の崖」の概要図
（出典）経済産業省「DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～」を基に作成

2025年の崖

【参照：セミナーテキスト4-2-2.】

2025年の崖の解決策

項番	課題
解決策1	DX推進システムガイドラインの策定
解決策2	「見える化」指標、診断スキームの構築
解決策3	ITシステムの刷新
解決策4	DX人材の育成・確保
解決策5	ユーザー企業・ベンダー企業との新しい関係性構築

守りのIT投資、攻めのIT投資

【参照：セミナーテキスト4-2-1.】

守りのIT投資（デジタルオプティマイゼーション）

- ITによる業務効率化
- コスト削減

攻めのIT投資（デジタルトランスフォーメーション）

- 新しい事業展開
- 新しいビジネスモデル創出

守りのIT投資、攻めのIT投資

【参照：セミナーテキスト4-2-3.】

守りのIT投資

【投資目的】

- 業務効率化・コスト削減
- デジタル活用するための環境整備

【進め方】

1. 業務内容・業務フローの可視化
2. 削減・短縮可能な業務の洗い出し
3. 改善や対応の実施
4. 業務改革の実現

守りのIT投資、攻めのIT投資

【参照：セミナーテキスト4-2-3.】

守りのIT投資事例

課題

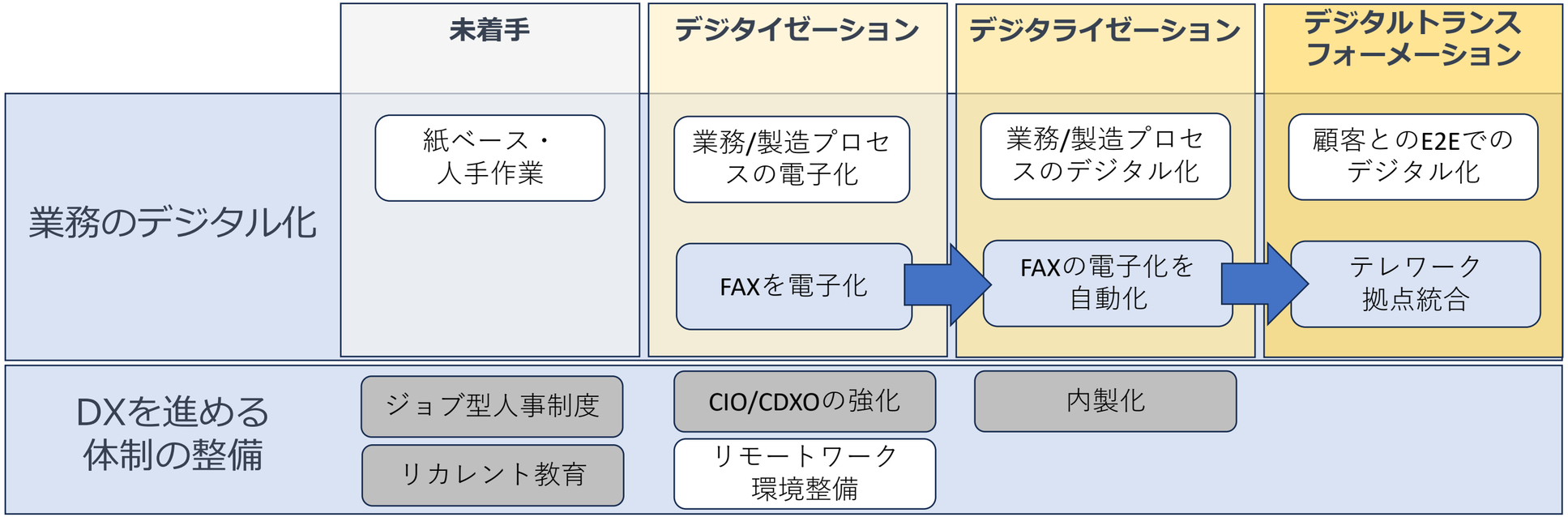
- 新型コロナウイルス対応のため、テレワークへの切り替え
- 書類処理のための出社

【進め方】

手順１：業務内容・業務フローの可視化
問題となる業務は、「お客様や仕入れ先様からFAXで届いた見積書や注文書に対して、紙で返信する業務」であることが判明
手順２：削減・短縮可能な業務の洗い出し
紙ベースの書類を電子データに切り替えることで、出社する手間を削減
手順３：改善や対応の実施
RPAを導入し、FAXデータをPDFファイルに自動変更しサーバに保存
手順４：業務改革の実現
出社回数が激減し、完全テレワークが実現

守りのIT投資、攻めのIT投資

守りのIT投資事例とフレームワーク



守りのIT投資、攻めのIT投資

【参照：セミナーテキスト4-2-4.】

攻めのIT投資

【投資目的】

- ビジネス環境の急激な変化に対応するため
- 多様化する顧客のニーズに応えるため

【進め方】

1. 経営ビジョン・戦略の策定
2. 変革の準備・課題の抽出
3. デジタル技術・業務改革による課題の解決
4. 顧客に新たな価値を提供・他社のDXに貢献

守りのIT投資、攻めのIT投資

【参照：セミナーテキスト4-2-4.】

攻めのIT投資事例

課題

- 従来の機械加工ではビジネスの継続が困難

【進め方】

手順１：実現したいことを明確にする

ビジネスモデルを、自らサービス提供していくモデルへ転換することに設定した。

手順２：課題の明確化、関係者の意識改革を実施する

機械加工による製品の開発や販売だけでなく、自ら市場を開拓できるような新たな価値の創出を課題として挙げた。

手順３：デジタル技術による、課題解決

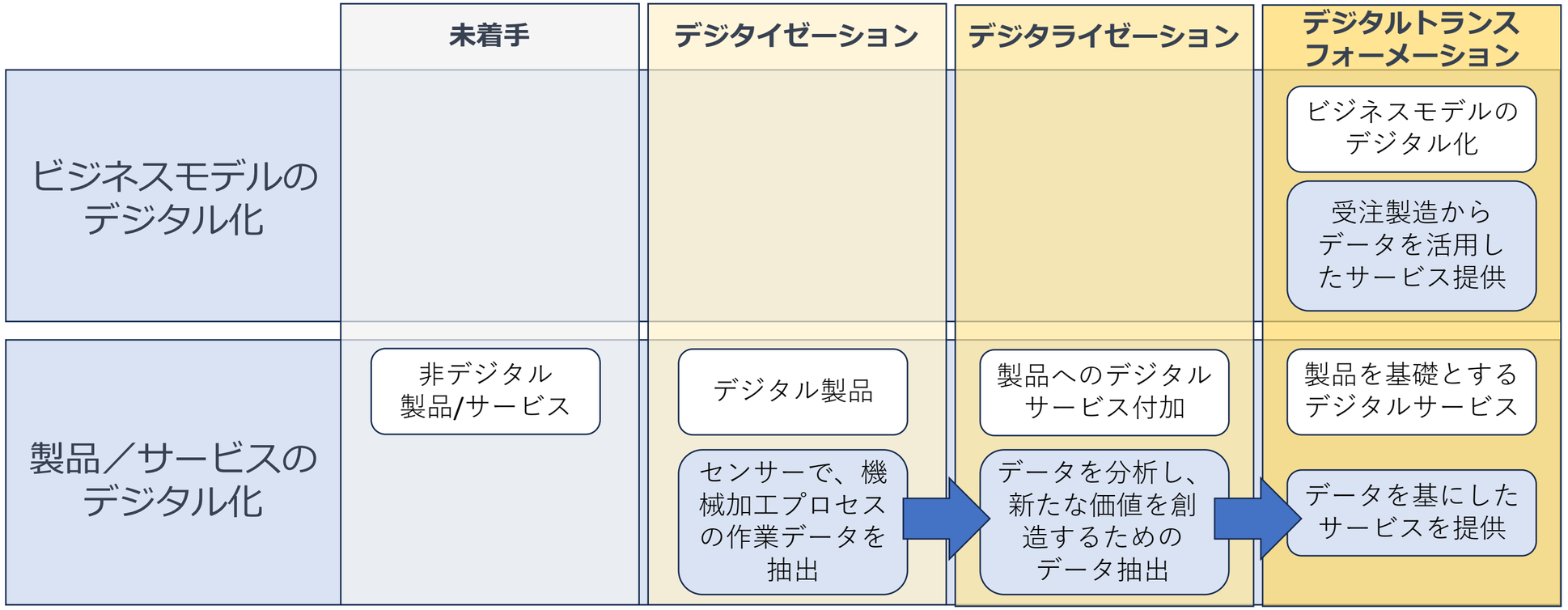
機械加工を行う機器にデータを計測するセンサーをつけ、加工データをリアルタイムで計測してデータを抽出し分析して得た情報をもとに、新規事業の展開に繋げた。

手順４：顧客に新たな価値を提供・ビジネスモデルの転換

機械加工の現場における生産性の向上や品質の改善、人材の育成などの課題を解決するサービスを提供できるようになり、受注だけに頼らないビジネスモデルを構築できた。

守りのIT投資、攻めのIT投資

攻めのIT投資事例とフレームワーク



次世代技術を活用したビジネス展開

【参照：セミナーテキスト4-2-5.】

活用する技術

技術	概要	活用方法例
AI	膨大な情報を処理し、判断や予測を行うことができる。	• 需要の予測や在庫の最適化 • 不良品の自動検出 • 対話型AIによる、問い合わせ対応の自動化 • コンテンツの生成
IoT	現実世界の様々なモノが、インターネットと繋がる。収集したデータが、インターネットに送信・蓄積され、データを分析・活用することで、新たな価値の創出に繋がる。	• 生産設備にセンサーを設置し、振動データを取得し分析することで、部品の故障予知や性能維持が可能 • 生産設備の稼働状況を可視化したことで、全ての拠点での生産状況をリアルタイムに把握可能
クラウドサービス	自社で機器やシステムを保有しなくても、インターネット経由で様々なサービスを利用できる	• 社内情報の一元管理 • システムを開発・実行するためのツールや環境構築作業の省略 • 場所やデバイスに依存せずに作業の継続が可能

次世代技術を活用したビジネス展開

【参照：セミナーテキスト4-2-5.】

次世代技術の活用事例１

【課題】
- システム開発において、仕様変更が多すぎる。
- 適切な情報共有ができない。

【解決への取り組み】
- 情報共有のための社内SNSを利用。
- クラウドサービス（Iaas）を導入し、システム構築を簡略化。

【結果】
- システムを短期間で開発可能となる。
- 修正を即座に反映できるようになる。
- 情報の共有、工程管理の効率化を実現。

【＋α】
- 地域の製造業者に共有することで、効率化のコンサルティング、開発依頼の受注。

想定すべきセキュリティリスク
- 社内SNSへの攻撃による情報漏洩・サービス停止
- 個人用スマホからの情報漏洩
- 社用PC以外のPCからの利用による情報漏洩
- クラウド（Iaas）環境への攻撃による情報漏洩・サービス停止
- データ連携時の情報漏洩

次世代技術を活用したビジネス展開

次世代技術の活用事例１（リスク対策）

項番	想定すべきセキュリティリスク	一般的なリスク対策
1	社内SNSへの攻撃による 情報漏洩・サービス停止	• Web Application Firewall（WAF）サービスの導入 • 多要素認証の導入（利用者の特定） • 定期的なアカウント棚卸 • データの暗号化
2	個人用スマホからの情報漏洩	• 会社用スマホの支給＋Mobile Device Management（MDM） • Mobile Application Management（MAM）サービスの導入
3	社用PC以外のPCからの 情報漏洩	• テレワーク用持ち出しPCの支給 • 外部リモートデスクトップ接続用、社内端末の設置 • 社内SNSサービスの接続元IP固定化＋VPN接続
4	クラウド環境への攻撃による 情報漏洩・サービス停止	• 管理画面のログインに多要素認証の導入 • ファイアウォールの適切な設定 • 仮想サーバへのSSH、RDPの接続元IP固定 • 社内とクラウド環境の拠点間VPN
5	データ連携時の情報漏洩	• 社内とクラウド環境の拠点間VPN（経路の暗号化） • データの暗号化

次世代技術を活用したビジネス展開

【参照：セミナーテキスト4-2-5.】

次世代技術の活用事例２

【課題】

- 「つくる力」と「とどける力」を強化するため、管理面を強化する。

【解決への取組み】

- 農家における栽培環境の点検作業にIoTを導入し、自動化することを決定。
- IoT導入のために、電子機械に詳しい人材の確保。
- IoT活用方法を検証し、マニュアル作りを実施。

【結果】

- 栽培環境における点検作業の自動化に成功。
- 勘と経験に頼らない栽培作業の平準化に成功。

想定すべきセキュリティリスク

- IoT機器への攻撃による情報漏洩・機器停止・データ改ざん
- Wifiアクセスポイントへの攻撃による機能停止
- 制御システムへの攻撃による情報漏洩・サービス停止
- IoT機器から制御システムへのデータ連携時の情報漏洩

【＋α】

- 計測データをAI分析することで、最適な栽培条件の絞り込みができるようになる。
- 品質向上、作業の平準化、生産量の拡大が期待できるようになる。

次世代技術を活用したビジネス展開

次世代技術の活用事例2（リスク対策）

項番	想定すべきセキュリティリスク	一般的なリスク対策
1	IoT機器への攻撃による情報漏洩・機器停止・データ改ざん	• ファイアウォールの適切な設定 • 接続アカウントとパスワードの適切な設定 • ファームウェアのアップデート運用
2	Wifiアクセスポイントへの攻撃による機能停止	• SSIDをデフォルトから変更 • パスフレーズの適切な設定 • WPA2以上の暗号化強度を使用 • ファームウェアのアップデート運用
3	制御システムへの攻撃による情報漏洩・サービス停止	• WAFの導入 • ファイアウォールの適切な設定 • 管理画面のログインに多要素認証の導入 • データの暗号化
4	IoT機器から制御システムへのデータ連携時の情報漏洩	• データ転送経路の暗号化（SSLなど） • データの暗号化

次世代技術を活用したビジネス展開

【参照：セミナーテキスト4-2-5.】

チャットボットとは

- 自動会話プログラム
- 事前に設定したルール、選択肢などに基づいて利用者と文字形式でコミュニケーションをとることができる

【利用シーン】

- サポートサイトのFAQ
- 社内SNSの自動応答

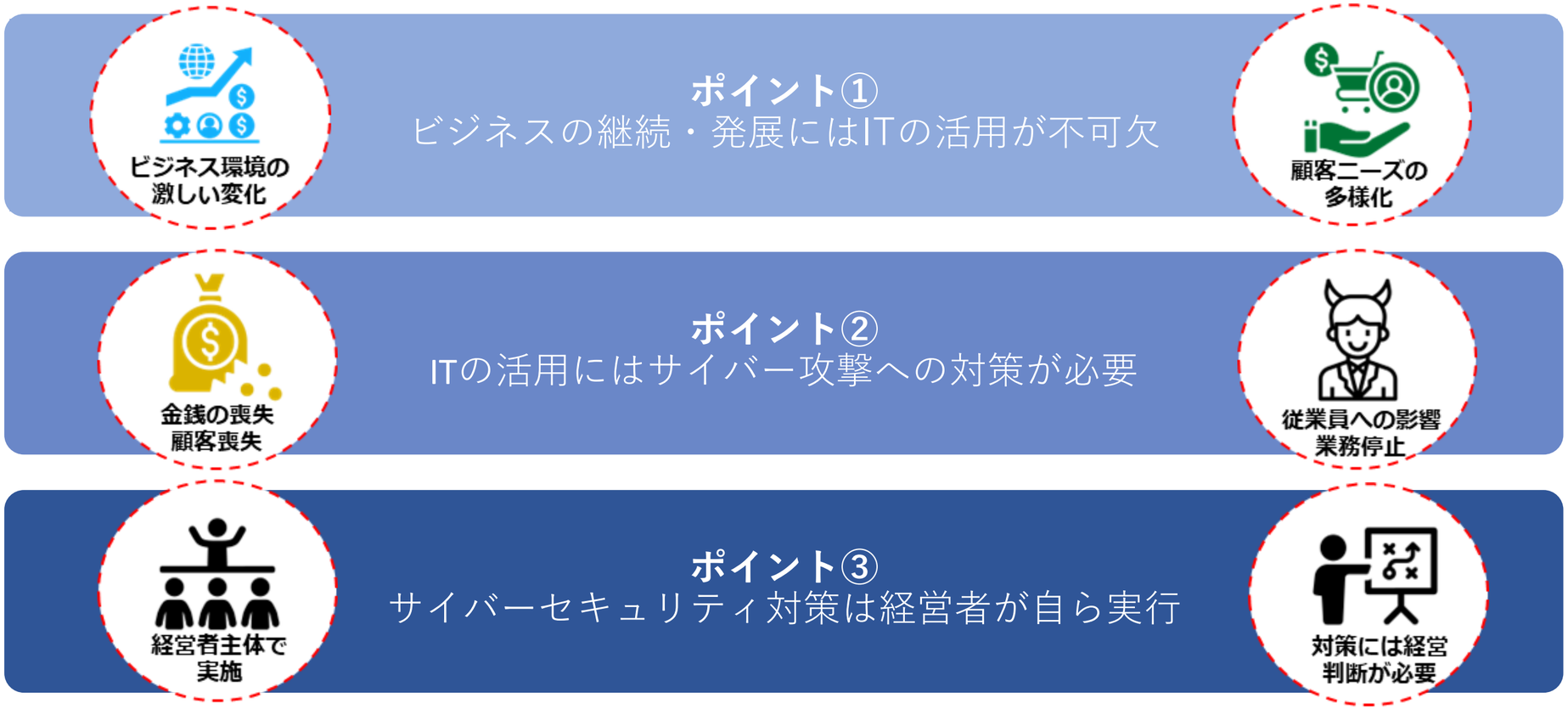
【今後の発展】

- チャットボットのAI連携

サイバーセキュリティ対策の重要性

【参照：セミナーテキスト4-3-1.】

経営者が重要視すべき3つのポイント



ITの活用とサイバーセキュリティ対策の関係性
（出典） 東京都産業労働局 「MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響」

経営者が重要視すべき3つのポイント

【参照：セミナーテキスト4-3-2.】

ポイント１：ビジネスの継続・発展にはITの活用が不可欠

【中小企業の重要課題】

- 業務の効率化
- 生産性の効率化
- 人材確保
- DX化

【課題解決のアプローチ】

- 運用コストの削減・効率化のために、デジタルオプティマイゼーション
- 競争力維持・強化のために、デジタルトランスフォーメーション

経営者が重要視すべき3つのポイント

【参照：セミナーテキスト4-3-2.】

ポイント２：ITの活用にはサイバー攻撃への対策が必要

DX推進のためにはIT活用は必須

↓

IT活用のためにはインターネットの活用は必須

↓

インターネットの活用にはサイバーセキュリティ対策は**最優先事項！**

守りや攻めのIT投資によってDXを推進しても、たった1度のサイバー攻撃による被害で、すべてを失います。

経営者が重要視すべき3つのポイント

【参照：セミナーテキスト4-3-2.】

ポイント３：サイバーセキュリティ対策は経営者が自ら実行

【その理由】

- 経営者による経営判断が必要
  - サイバー攻撃のリスクの許容範囲をどの程度にするのか
  - セキュリティ投資をどこまで行うのか
- セキュリティインシデントが発生した際に、経営者が責任を負う

法令	条項	要約
民法	415条 債務不履行による損害賠償責任	サイバー攻撃により仕事が停滞した場合、 会社および第三者に対する、契約違反による賠償義務を負う。
	644条 取締役の善管注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対して、善管注意義務違反による賠償義務を負う。
会社法	330条 取締役の善管注意義務違反 423条 1項 任務懈怠による損害賠償責任 429条 1項 第三者に対する注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対する、善管注意義務違反による任務懈怠（けたい）に基づく損害賠償義務を負う。

情報セキュリティ対策が不備の場合に責任追及の根拠とされる主な法律
（出典） IPA 「中小企業の情報セキュリティ対策ガイドライン 第3.1版」から抜粋

令和5年度
中小企業サイバーセキュリティ対策
継続支援事業