今治市DX勉強会
2026年度第2回

IPAのDX政策

- DX人材育成・DX認定・SCS評価制度等 -

2026.09.17

独立行政法人
情報処理推進機構　理事 上席執行役員　三谷 慶一郎

はじめに

※本資料は講演者個人の見解に基づくものであり、講演者が所属する組織の公式見解ではない

三谷　慶一郎（みたに けいいちろう）



独立行政法人 情報処理推進機構(IPA)

理事・上席執行役員

チーフAIオフィサー、チーフデータオフィサー

筑波大学大学院ビジネス科学研究科修了。博士(経営学)

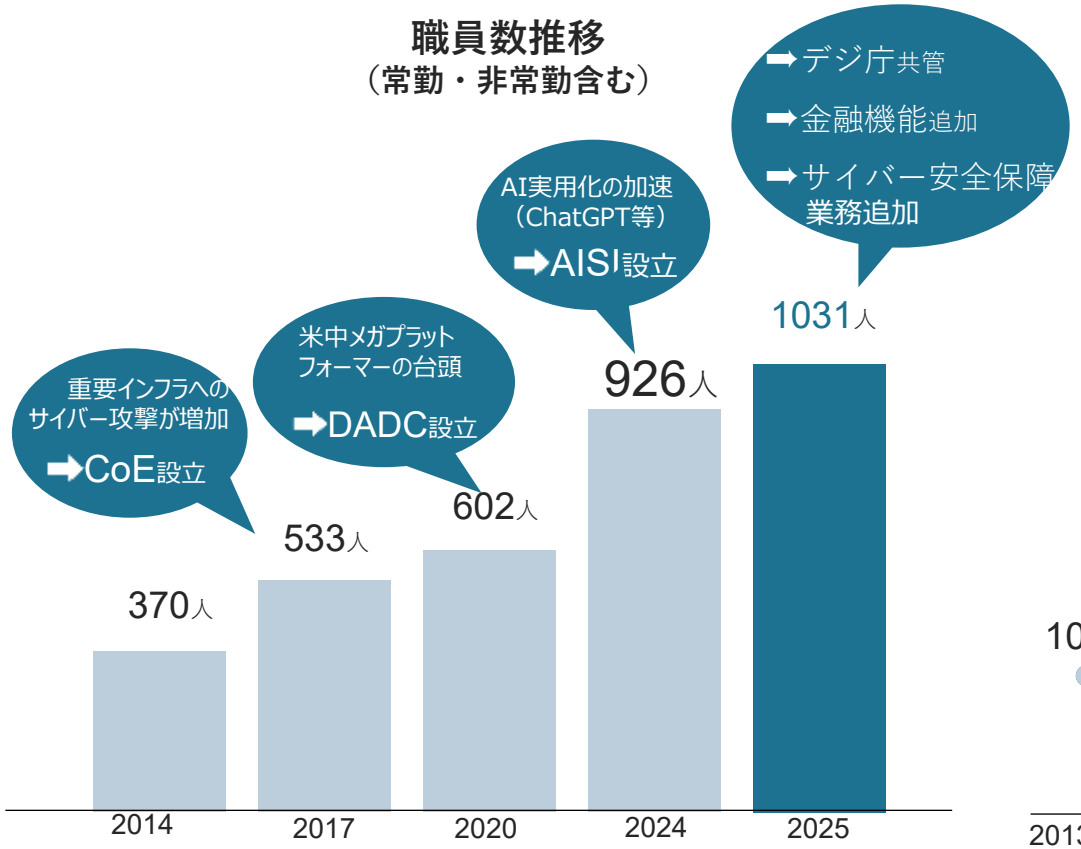
株式会社NTTデータ経営研究所において、執行役員として企業や行政機関におけるデジタル戦略立案に関連するコンサルティングを実施。経済産業省等においてDX推進、デジタル人材育成等に関する検討会座長を務める。2026年から情報処理推進機構 理事に就任。現職では、日本社会の国際競争力向上に向けて様々なデジタル政策の推進に取り組んでいる

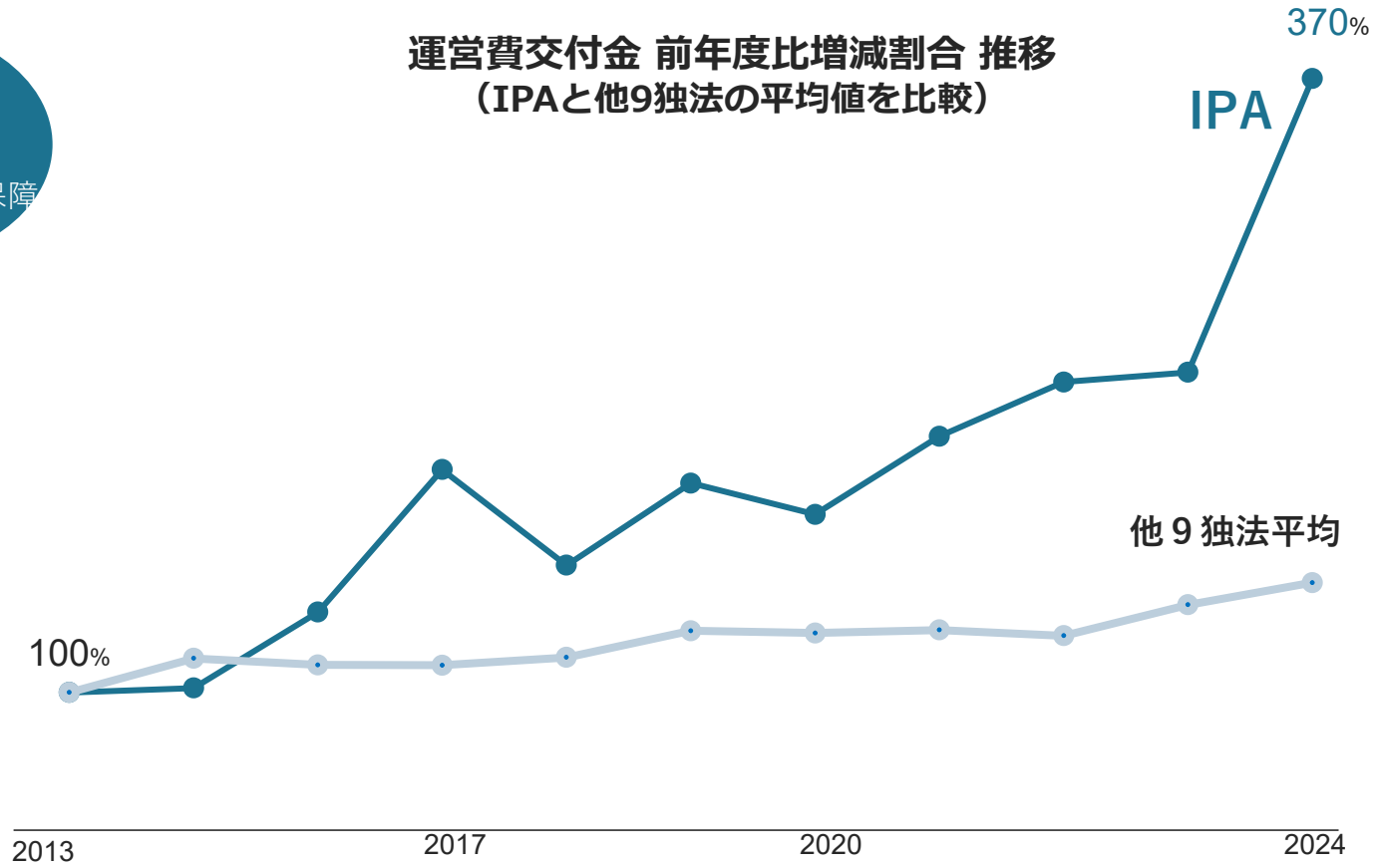
武蔵野大学国際総合研究所客員教授。東京農工大学非常勤講師、富山大学非常勤講師、山口大学非常勤講師。情報社会学会理事

共著書に「ITエンジニアのための 体感してわかるデザイン思考」、「攻めのIT戦略」、「CIOのITマネジメント」等、監訳書に「DX経営戦略」がある

独立行政法人情報処理推進機構（IPA）

- 日本のデジタル国家戦略を技術面・人材面から支えるために設立された独立行政法人。所管官庁は経済産業省。2025年4月からデジタル庁共管化。
- 急速に事業拡大。ここ10年で職員数は3倍増の約1,000人、運営費交付金は3.7倍に急増





※CoE：産業サイバーセキュリティセンター、DADC：デジタルアーキテクチャデザインセンター
AISI：AIセーフティーインスティテュート

IPAの中核事業：人材・安全・基盤















- デジタル＆AIシステムズ・デザインセンター
- デジタル人材センター
- セキュリティセンター
- 産業サイバーセキュリティセンター



Beyond Digital

独立行政法人

情報処理推進機構

Innovation Platform Agency, Japan

内容

- DXがなぜ必要なのか
- AIの台頭
- DX・AXの現状
- DX認定制度
- サイバーセキュリティの確保（SCS評価制度等）
- DX推進人材の育成・確保
- まとめ

DXがなぜ必要なのか

不確実性の高まり

社会は「VUCA」になりつつある



Volatility

変動性：変化の質・大きさ・スピードが予測不能

Uncertainly

不確実性：これから出現する問題や物事が予測不能

Complexity

複雑性：数多くの要因が複雑に絡み合う

Ambiguity

曖昧性：原因や関係性が不明瞭

世界の不確実性は確実に高まっている



「不確実性の高まりが続いていくことこそが新しい常態（ニューノーマル）である」
（IMFゲオルギエバ専務理事）

環境変化を感知する仕組みが必要

企業自身が環境変化を「感知」する能力を持つために、デジタル技術の活用が不可欠

- ダイナミック・ケイパビリティ「不測の環境変化に対応するために、組織内外の経営資源を再結合・再構成する能力」
- ポーターのポジショニング戦略やバーニーの資源ベース論は、すべて静的な環境であることが前提。不確実性が高く環境変化が激しい、動的な状況での経営論

感知
（Sensing）

企業の経営陣が競争的状況を把握し、事業が直面する変化、機会や脅威を感知する能力

捕捉
（Seizing）

企業の経営陣が、機会を捕捉し、脅威をかわすように必要に応じて既存の事業や資源や知識を様々な形で応用し、再利用する能力

変容
（Transforming）

持続的な競争優位を維持するために、企業の経営陣が企業内外の資産や知識を再編成し、ビジネス・エコシステムを形成する能力

AIの台頭

生成AIによる経済効果



- 生成AIによる生産性へのインパクトは世界経済に数兆ドルの価値をもたらす可能性がある
- 年間2.6～4.4兆ドル相当
  - 英国GDP：3.1兆ドル
  - 日本GDP：4.2兆ドル

※「生成AIがもたらす潜在的な経済効果」（マッキンゼー,2023）

スキルレベルの高い知的労働者の業務に影響大

生成AIが技術的な自動化ポテンシャルに与える影響（米国）

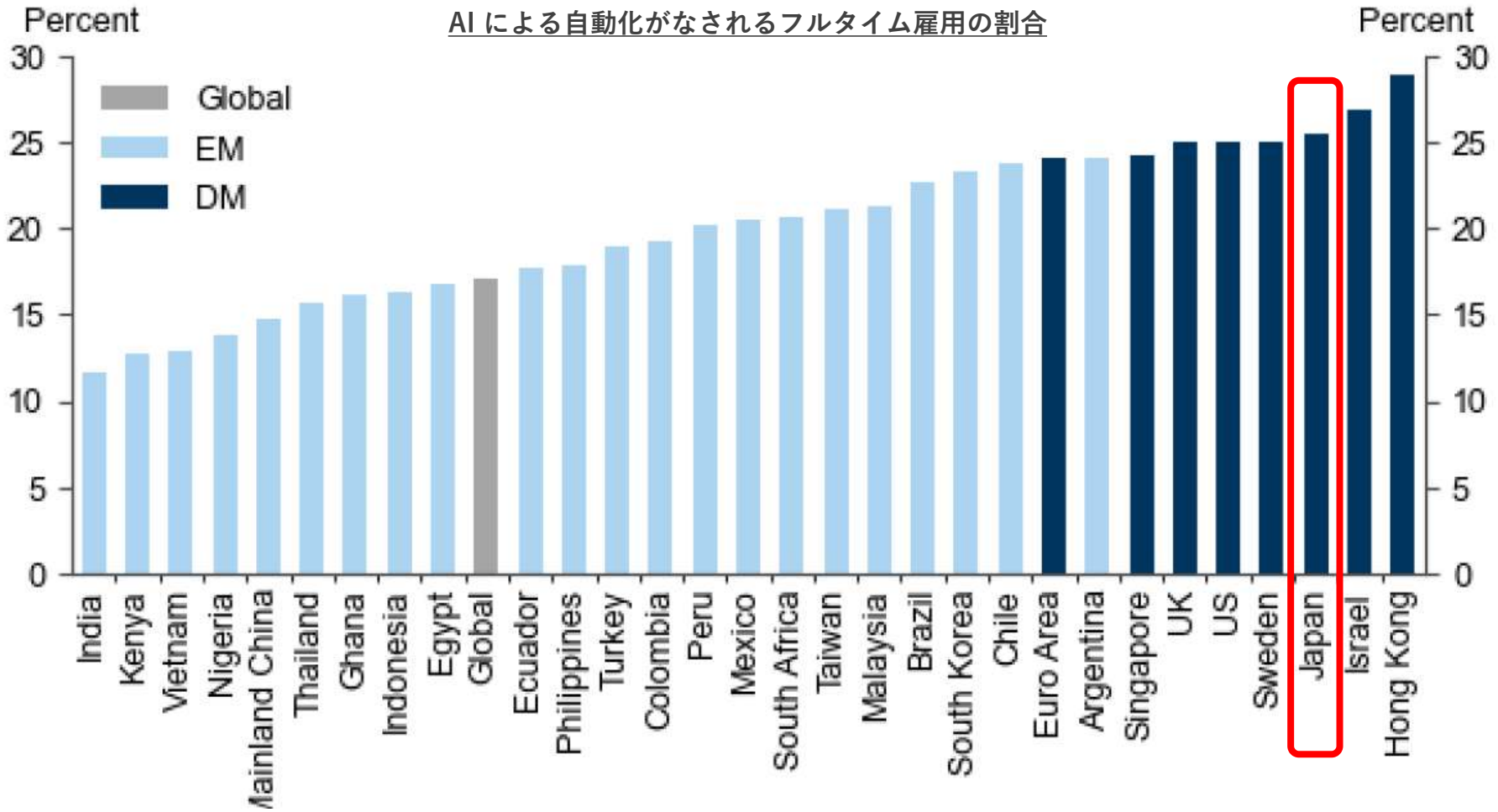


- これまでの自動化技術は「学歴やスキルレベルの低い労働者に大きな影響を与える」傾向があった
- 生成AIはそれだけでなく「高学歴でスキルレベルの高い労働者の一部業務を自動化する」可能性がある
- 賃金の高い知識労働者の業務を直撃するともいえる

※「生成AIがもたらす潜在的な経済効果」（マッキンゼー,2023）
※「生成AI導入なし」は、生成AIが出現する前に実施した、作業自動化に関する評価

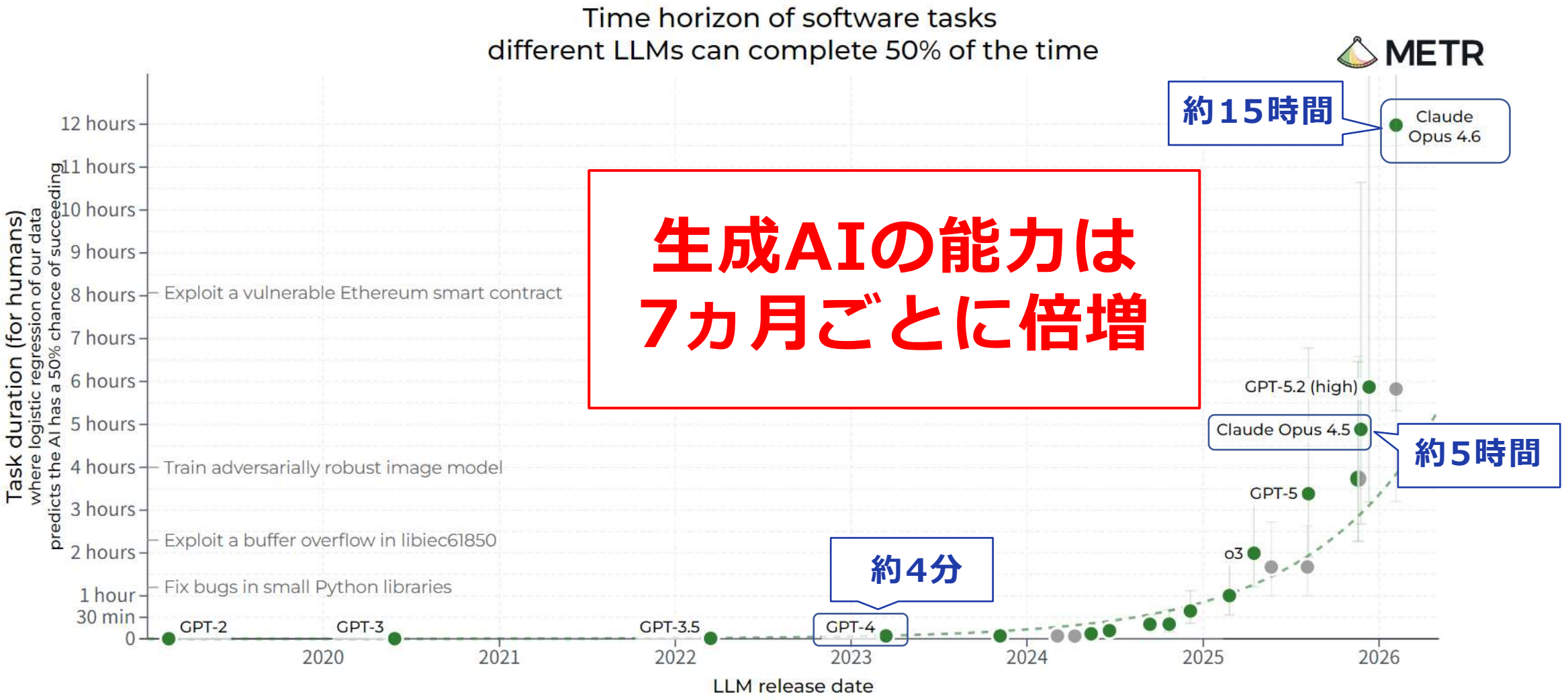
生成AIによって自動化される雇用の割合

世界全体では約18%の仕事が自動化される。産業構造の違いにより先進諸国の方が新興国よりAIによって自動化される割合が高く、日本は約25%で香港・イスラエルについで三番目に位置づけられている



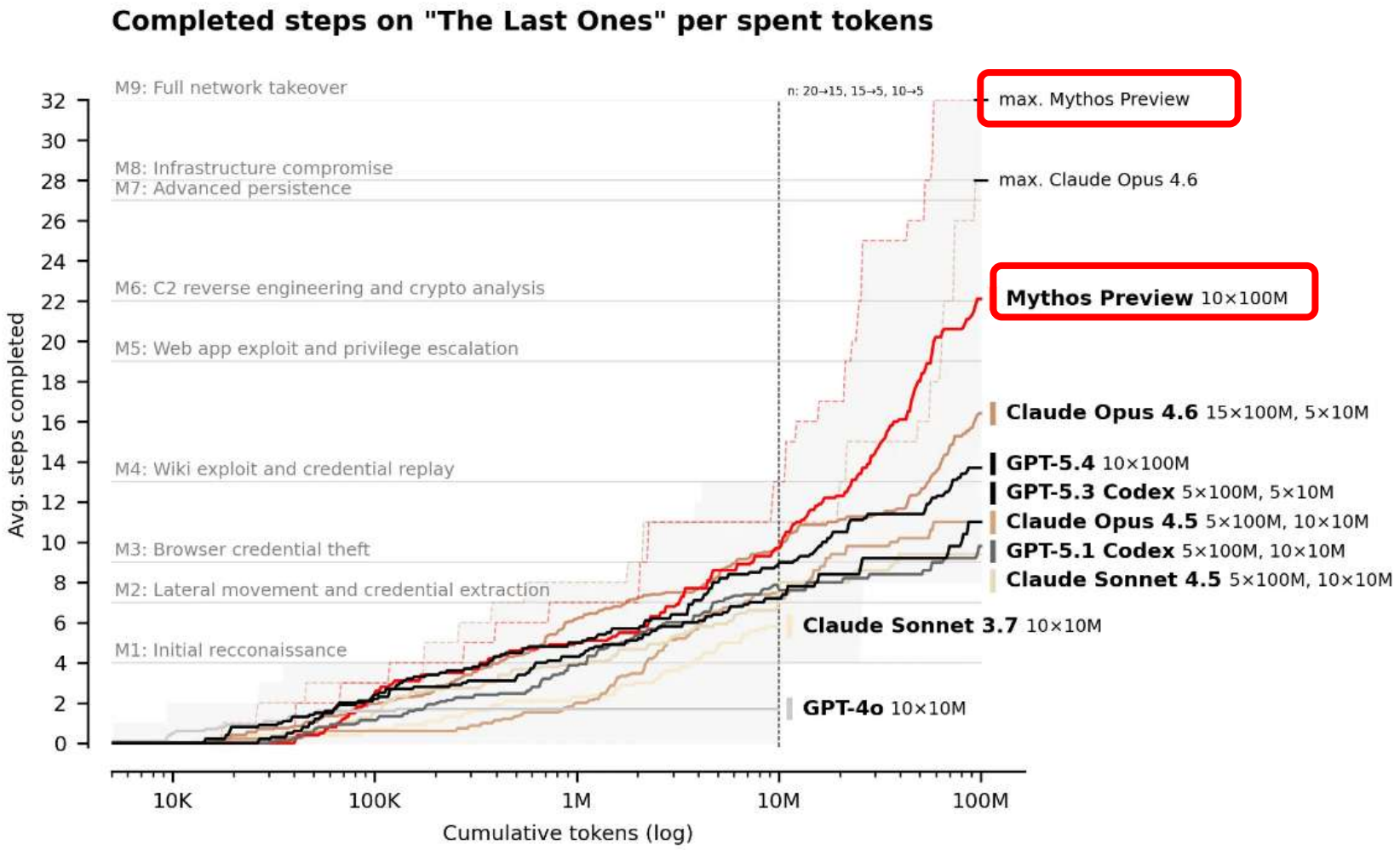
※" The Potentially Large Effects of Artificial Intelligence on Economic Growth" ,Goldman Sacks,2023
※EM：Emerging Market（新興国）、DM：Developed Market（先進国）

AIの能力向上は想像を超えている



※Model Evaluation & Threat Research（METR）“Task-Completion Time Horizons of Frontier AI Models”
※「50%タスク完了時間」（Time Horizon）：ソフトウェアエンジニアがX時間かかる課題を、AIが50%の確率で正しく完了できる」

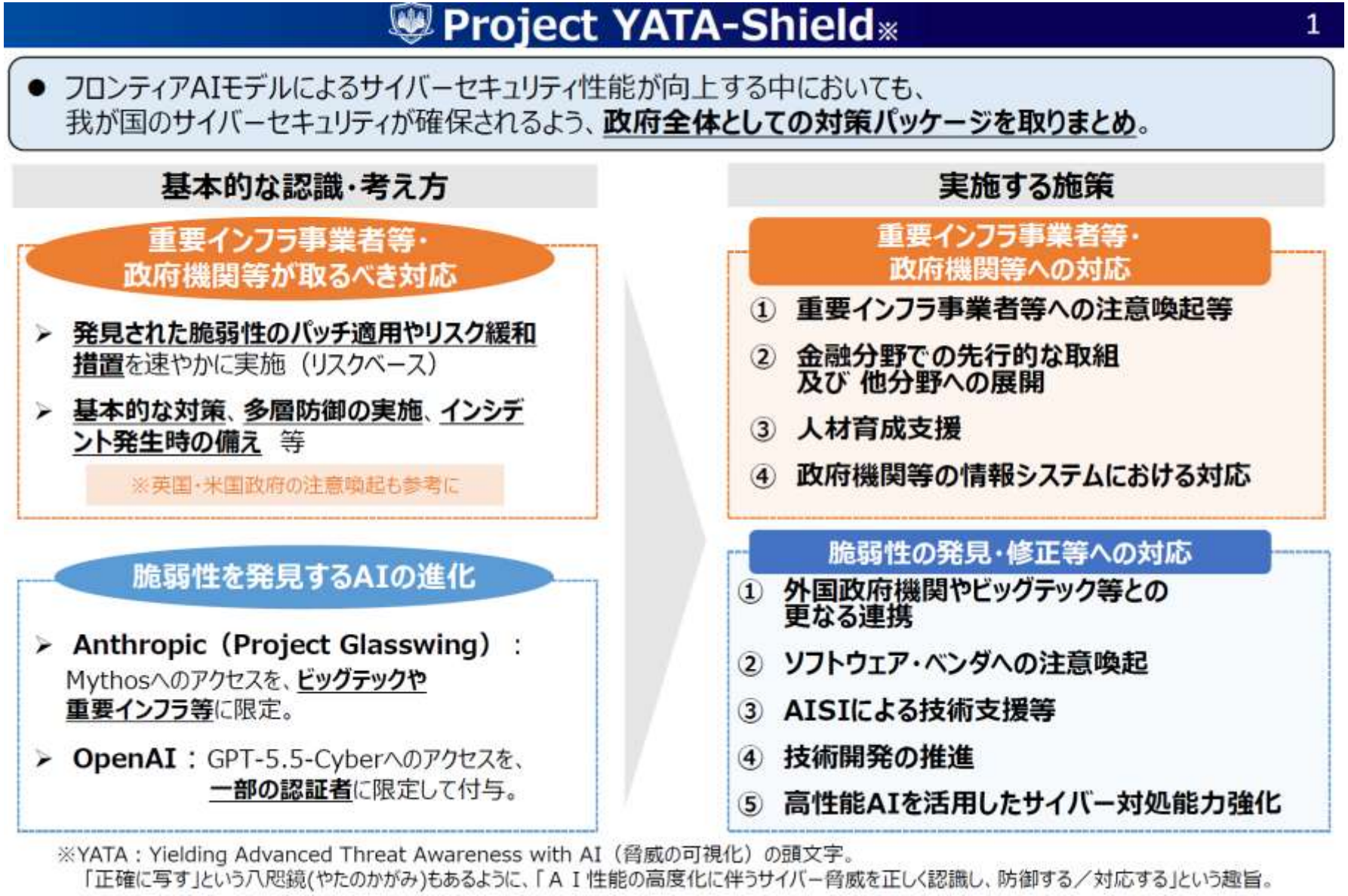
“フロンティアAI” Claude Mythosの衝撃



- Anthropic「Claude Mythos」は、１か月の非公開検証で１万件以上の重大なソフトウェア脆弱性を検出。従来のサイバー防御の常識を凌駕
- 一般公開は封印。限定組織参加による対応が開始されつつある

※“Claude Mythos Preview: First AI to Complete a 32-Step Autonomous Cyber Attack” (AISI,2026)

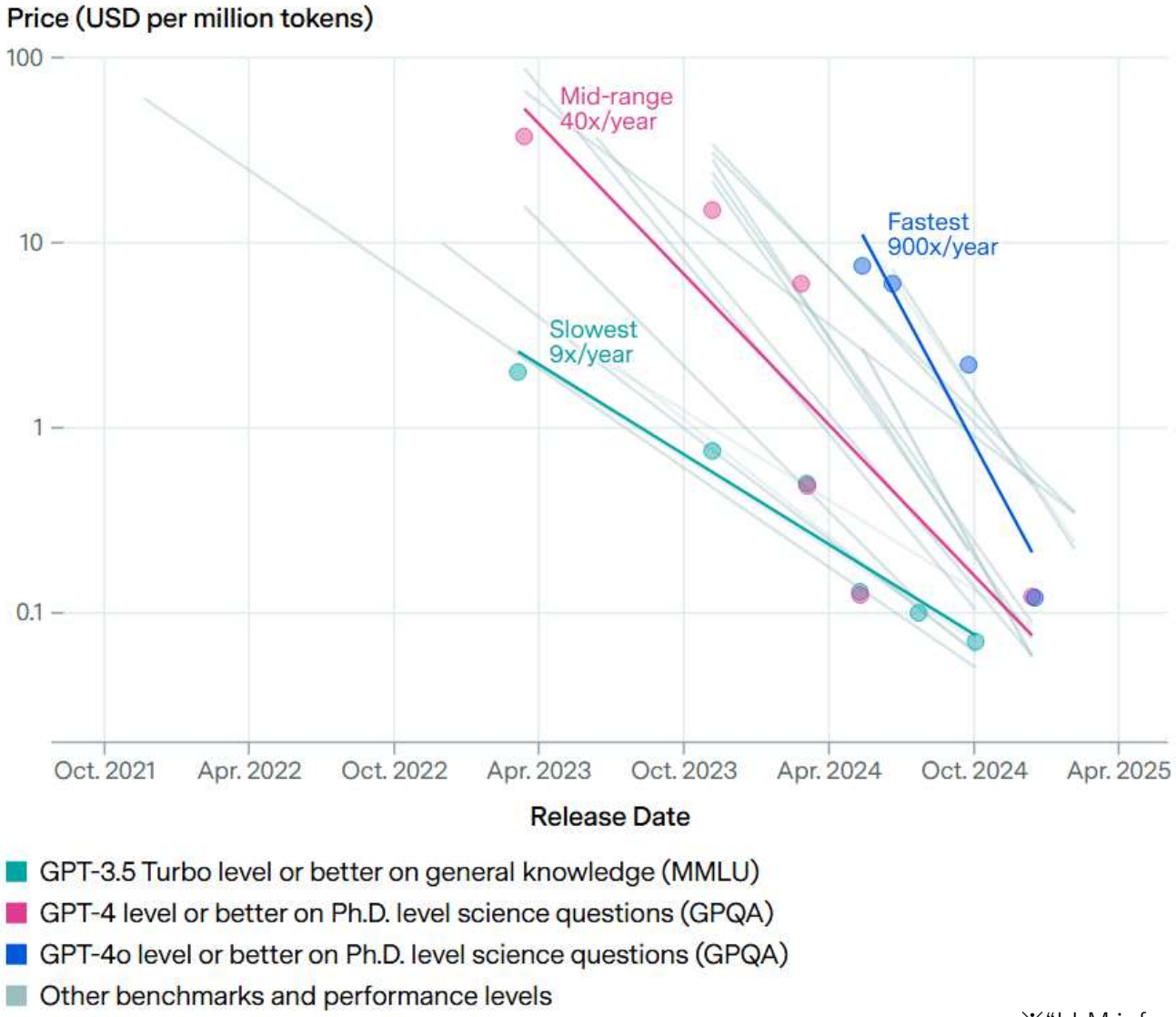
（参考）対策パッケージ「Project YATA-Shield」



- 2026年5月高市総理は、松本サイバー安全保障担当相等に、金融や情報通信など重要インフラの防衛および脆弱性の早期発見・修正対策を早急に具体化するよう指示
- フロンティアAIモデルによるサイバーセキュリティ性能の急速な向上を踏まえ、政府全体としての対策パッケージ「Project YATA-Shield」を取りまとめ、公表

※https://www.cyber.go.jp/pdf/press/20260518_AI_CS_gaiyou.pdf

AIの利用コストは急激に低下しつつある



- 生成AI利用コストは急激に低下する傾向にある
  - ✓ GPT-3.5（2022）は、年間1/9に低下
  - ✓ GPT-4o（2024）は、年間1/900に低下
- 背景には、AI開発・運用技術の改善やハードウェア性能の向上などが複合的に関係する

※“LLM inference prices have fallen rapidly but unequally across tasks”（Epoch AI,2025）

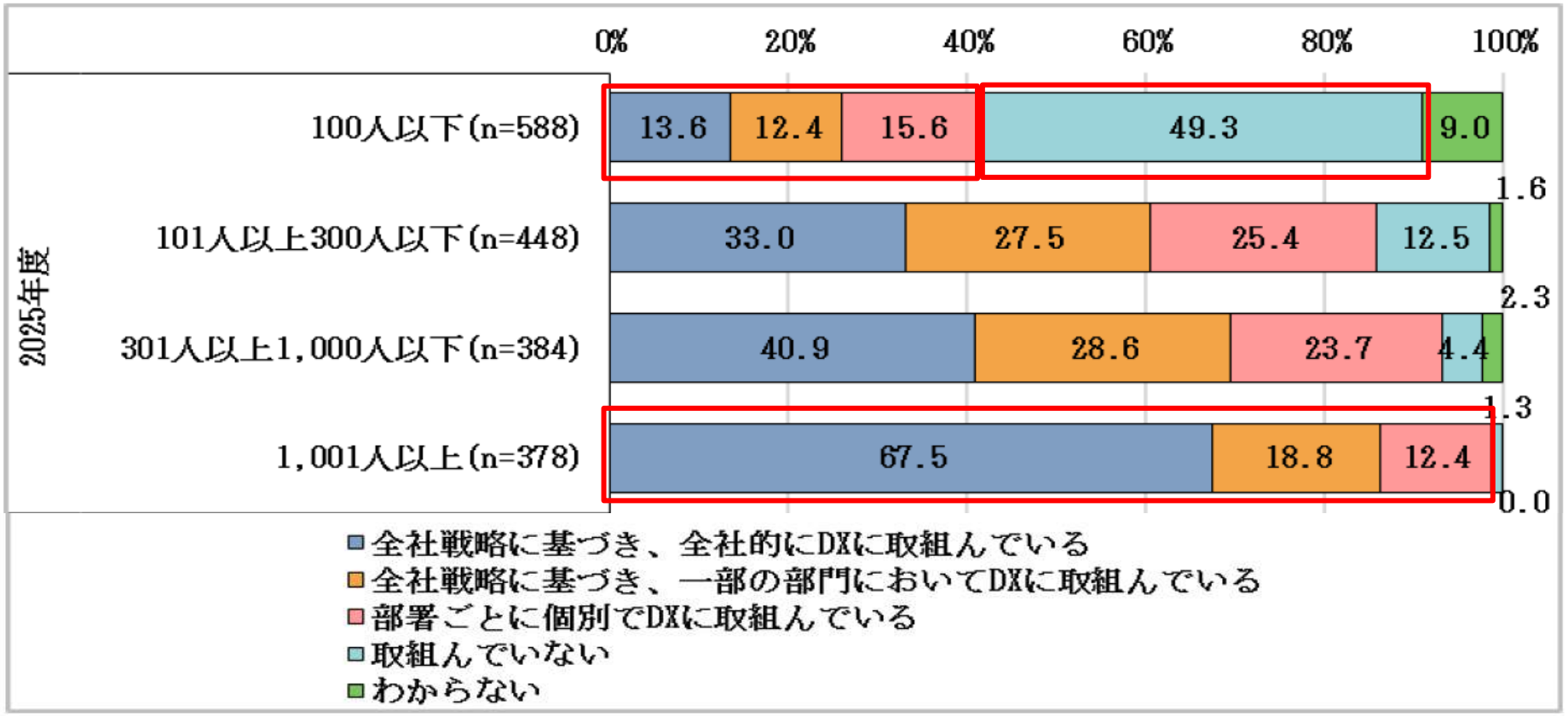
- AIに代表されるデジタル技術は、大きなポテンシャルを持ち始めている
- さらに、デジタル技術は、誰の手にでも扱えるようになってきている

デジタル技術を積極的に活用する企業と、使わない企業との差は、確実かつ決定的に大きくなる

DX・AXの現状

DXの取組は大企業では日常化。
中小企業では二極化している

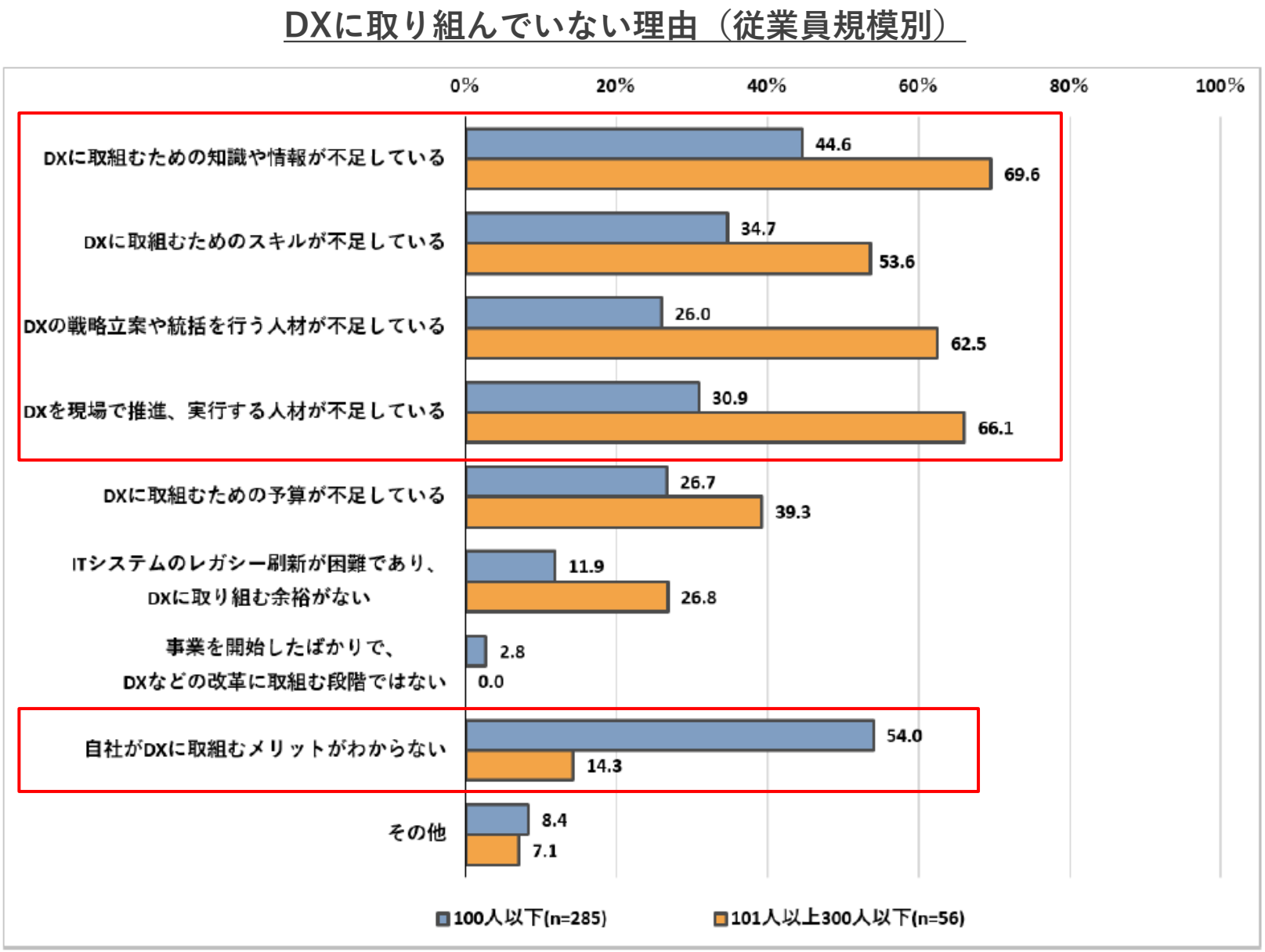
DXへの取り組み状況（従業員規模別）



※DX動向2026,IPA

23

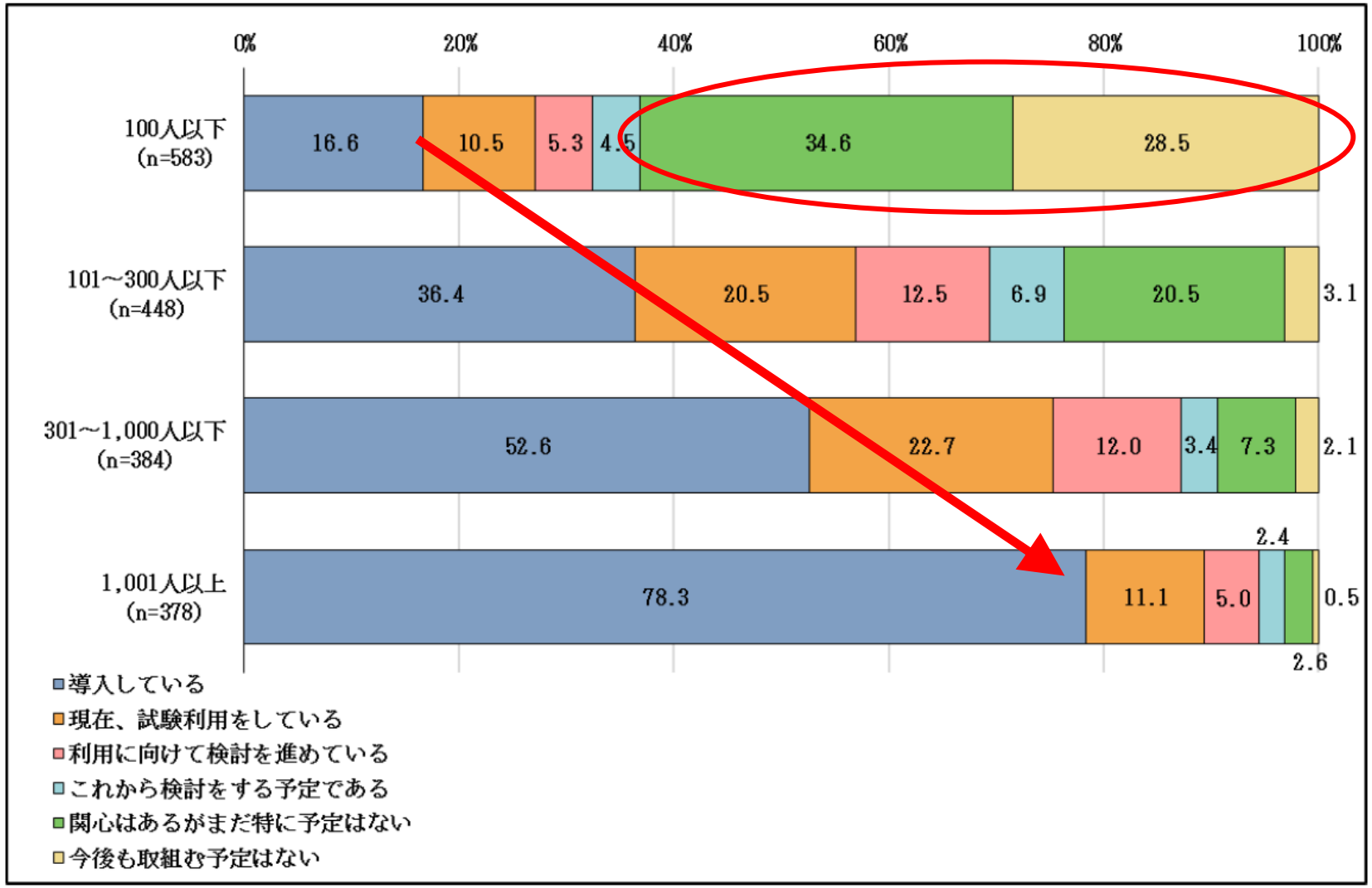
小規模企業はDXのメリットがわからない



※DX動向2026,IPA

AI導入は着実に進展、但し中小企業はまだ途上

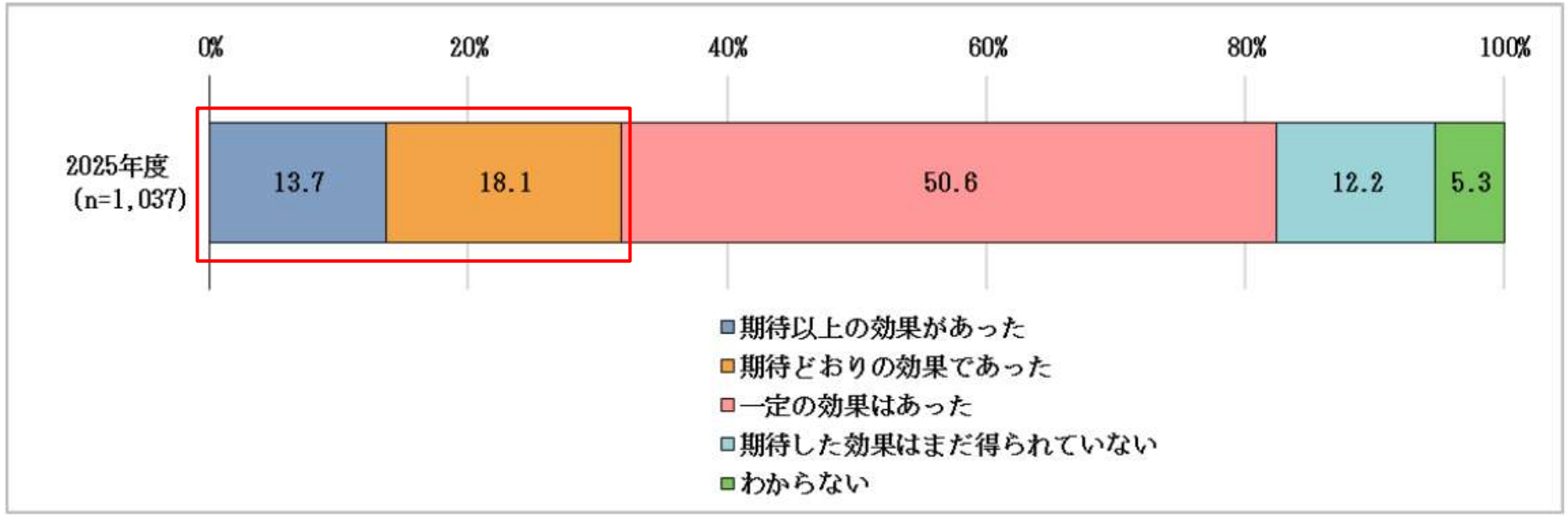
AIの導入状況（従業員規模別）



※DX動向2026,IPA

AI利活用の効果は現れ始めている

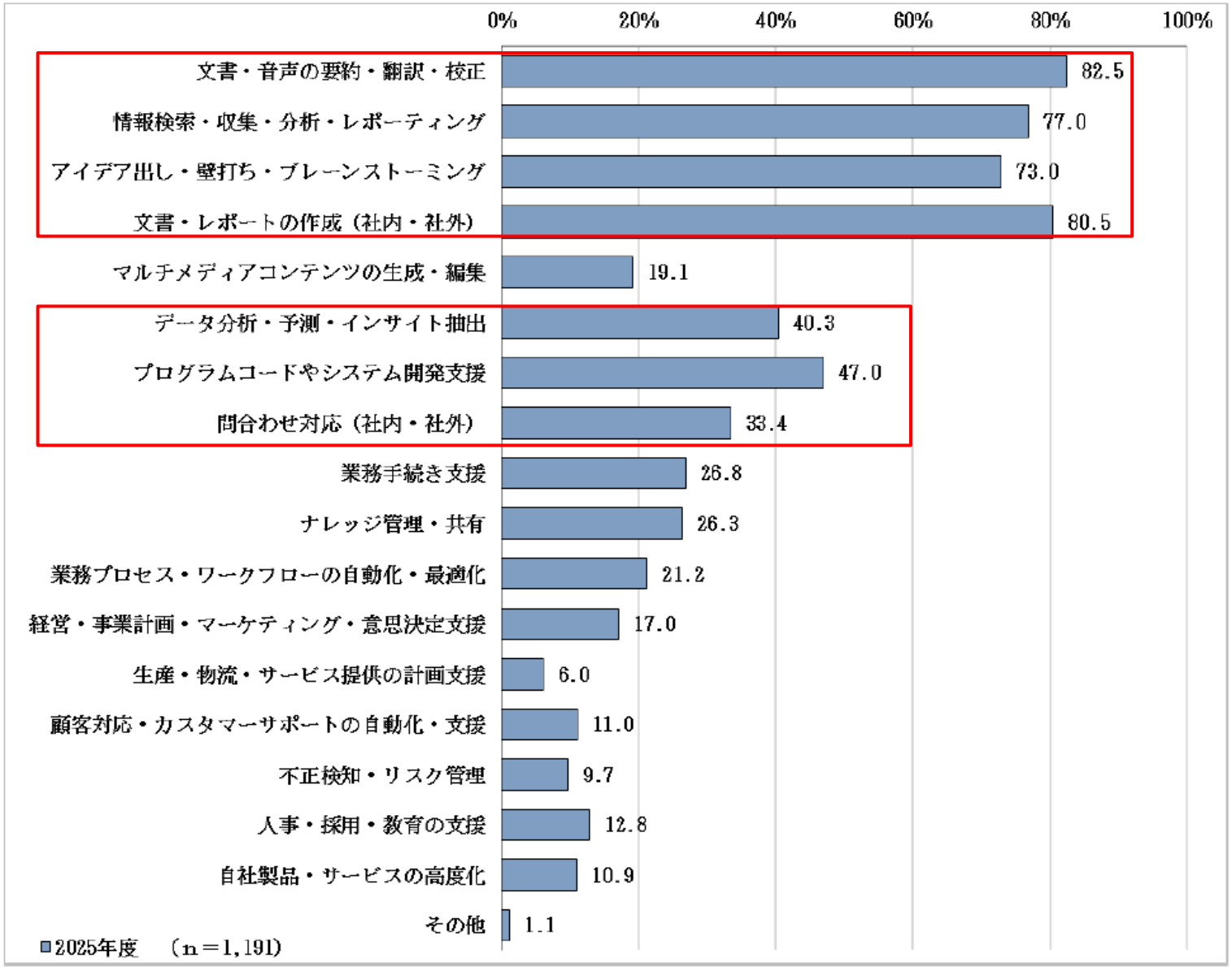
AI導入による効果の状況



※DX動向2026,IPA

AI利活用は個人用途が中心

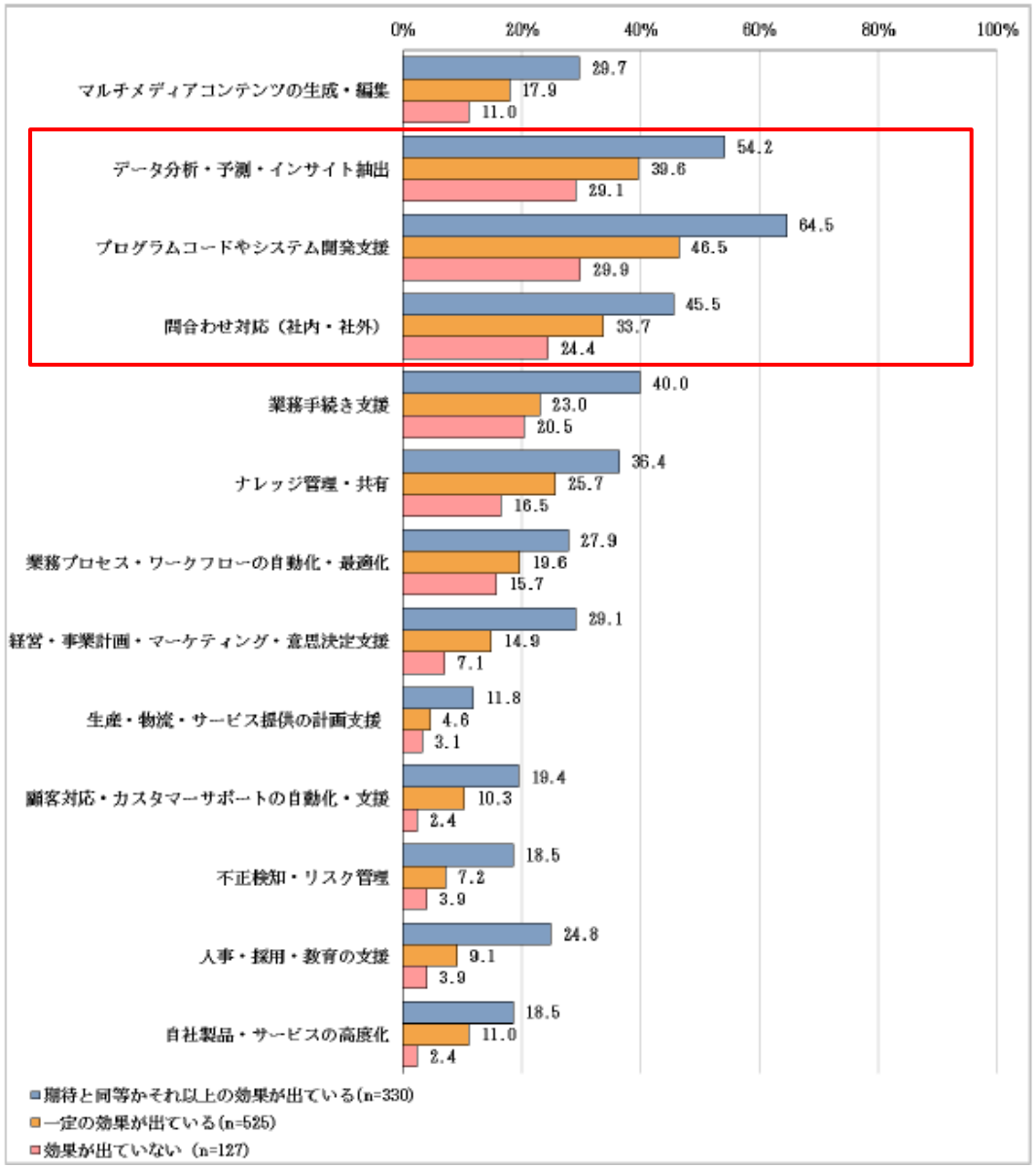
AI利活用の用途



※DX動向2026,IPA

データ分析やシステム開発等では効果が出ている

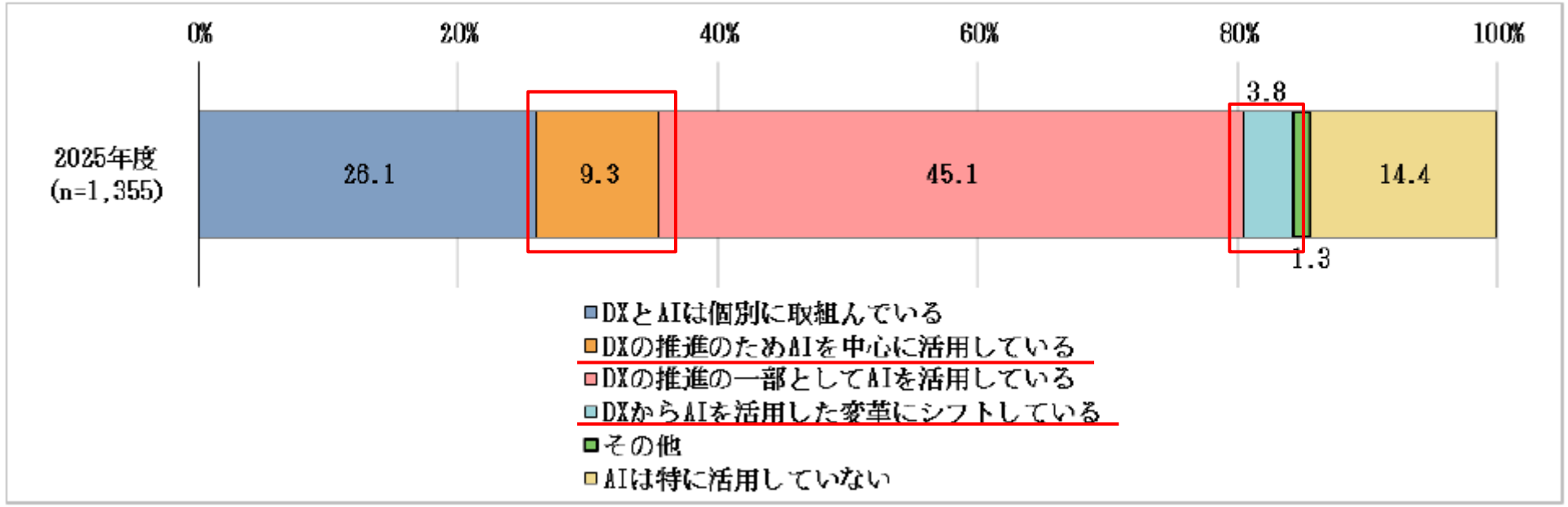
AI利活用の用途（AI導入効果別・抜粋）



※DX動向2026,IPA

DXはAXへと進化し始めている

AI利活用のDX推進に対する位置づけ



※DX動向2026,IPA

DX認定制度

デジタルガバナンスコード

- 持続的な企業価値向上のためには、ITシステムとビジネスを一体的に捉え、新たな価値創造に向けた戦略を描いていくことが重要であり、企業全体の組織構造や文化の改革等を行う観点から経営者の関与が不可欠であるという認識のもとで、経営者に求められる企業価値向上に向け実践すべき事柄をとりまとめたもの
- デジタルガバナンス・コードは、企業がＤＸの取り組みを自主的・自発的に進めることを促すとともに、経営者の主要な役割として、ステークホルダー（顧客、投資家、金融機関、人材等）との対話を捉え、対話に積極的に取り組んでいる企業に対して、資金や人材、ビジネス機会が集まる環境を整備していくことを目指している

- デジタルガバナンスコードは制度上、定期的にアップデートが行われる
  - ✓ 2020年11月：「デジタルガバナンス・コード」完成・公開
  - ✓ 2022年9月：デジタル人材の育成・確保をはじめとした時勢の変化に対応するため、「デジタルガバナンス・コード2.0」に改訂
  - ✓ 2024年6月：「企業価値向上に向けたデジタル・ガバナンス検討会」を立ち上げ、「デジタルガバナンス・コード3.0～DX経営による企業価値向上に向けて～」がまとめられた
  - ✓ 2026年7月から「AI時代におけるデジタルガバナンス検討会」が開催。AIをクローズアップしたアップデートが検討されている

情報処理の促進に関する法律（抜粋）

（情報処理システムの運用及び管理に関する指針）

- 第三十条　経済産業大臣は、情報処理システムを良好な状態に維持し、企業経営において戦略的に利用することが重要であることに鑑み、情報処理システムを良好な状態に維持するために必要な情報処理システムの運用及び管理に関する指針を定めるものとする。
- ２　指針には、次に掲げる事項を定めるものとする。
  - 一　情報処理システムの運用及び管理に関する基本的事項
  - 二　情報処理システムの運用及び管理を適切に行うために必要な体制の整備に関する事項
  - 三　情報処理システムの運用及び管理に係る具体的な方法に関する事項
  - 四　その他情報処理システムの運用及び管理を適切に行うために必要な事項
- ３　経済産業大臣は、指針を定めるに当たつては、我が国産業における情報処理システムの利用の状況及び情報処理技術の動向を勘案するものとする。
- ４　経済産業大臣は、指針を定めようとするときは、総務大臣その他の関係行政機関の長に協議しなければならない。
- ５　経済産業大臣は、指針を定めたときは、遅滞なく、これを公表しなければならない。
- ６　経済産業大臣は、おおむね二年ごとに指針に検討を加え、必要があると認めるときは、これを変更するものとする。
- ７　第三項から第五項までの規定は、前項の規定による指針の変更について準用する。

デジタルガバナンスコード3.0の全体像



2

※経済産業省資料より


中堅・中小企業等
大企業
支援機関を通じたDX推進
DX Selection
（対象：中堅・中小企業等）
DX銘柄
Digital Transformation
（対象：上場企業）
DX先進企業
模範となるDXの取組を実施している企業
DX推進指標（対象：全事業者）
DXに取り組んでいる企業
これからDXに取り組む体制を整備している企業
DX認定
DX認定（対象：全事業者）
DX支援ガイダンス
これからDXに取り組む企業
経営ビジョンの策定や、戦略・体制等の整備に、これから取り組む企業
DX推進指標（対象：全事業者）
中堅・中小企業等向けDX推進の手引き
“デジタルガバナンス・コード3.0～DX経営による企業価値向上に向けて～”
✓ 経営者が企業価値を向上させるために実践すべき事柄を取りまとめたもの
1 経営ビジョン・ビジネスモデルの策定
2 DX戦略の策定
3 DX戦略の推進
4 成果指標の設定・DX戦略の見直し
5 ステークホルダーとの対話
デジタル化支援施策
IT導入補助金
デジwith

DX認定制度（1/2）

経済産業省では2020年12月から「DX認定制度」を開始。これは、国が策定した指針（デジタルガバナンス・コード）を踏まえ、優良な取り組みを行う事業者を、申請に基づいて認定するもの

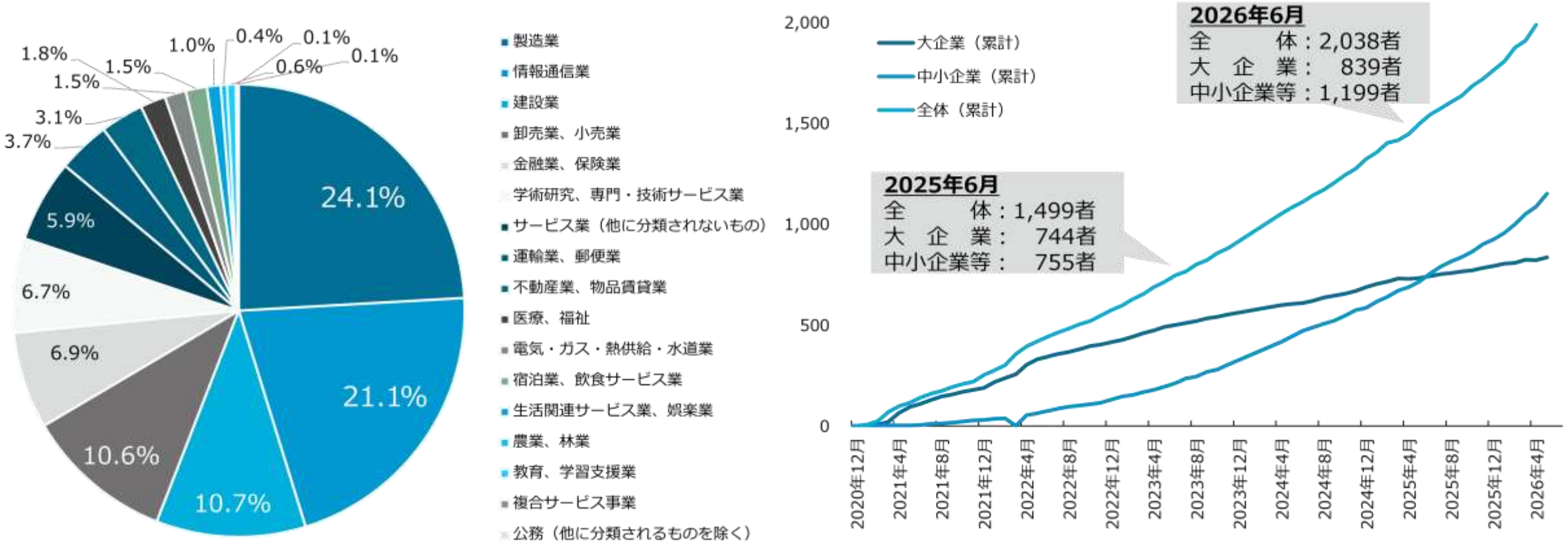


- 認定事業者は2024年6月時点で1,083者
- 認定事業者はIPAホームページで公表されるとともに、ロゴマークが利用可能
- 各種支援措置が受けられる
  - ✓ 日本政策金融公庫による金利優遇
  - ✓ 中小企業者信用保険法の特例
  - ✓ DX投資促進税制
  - ✓ 人材開発支援助成金

※https://www.meti.go.jp/policy/it_policy/investment/dx-nintei/dx-nintei.html

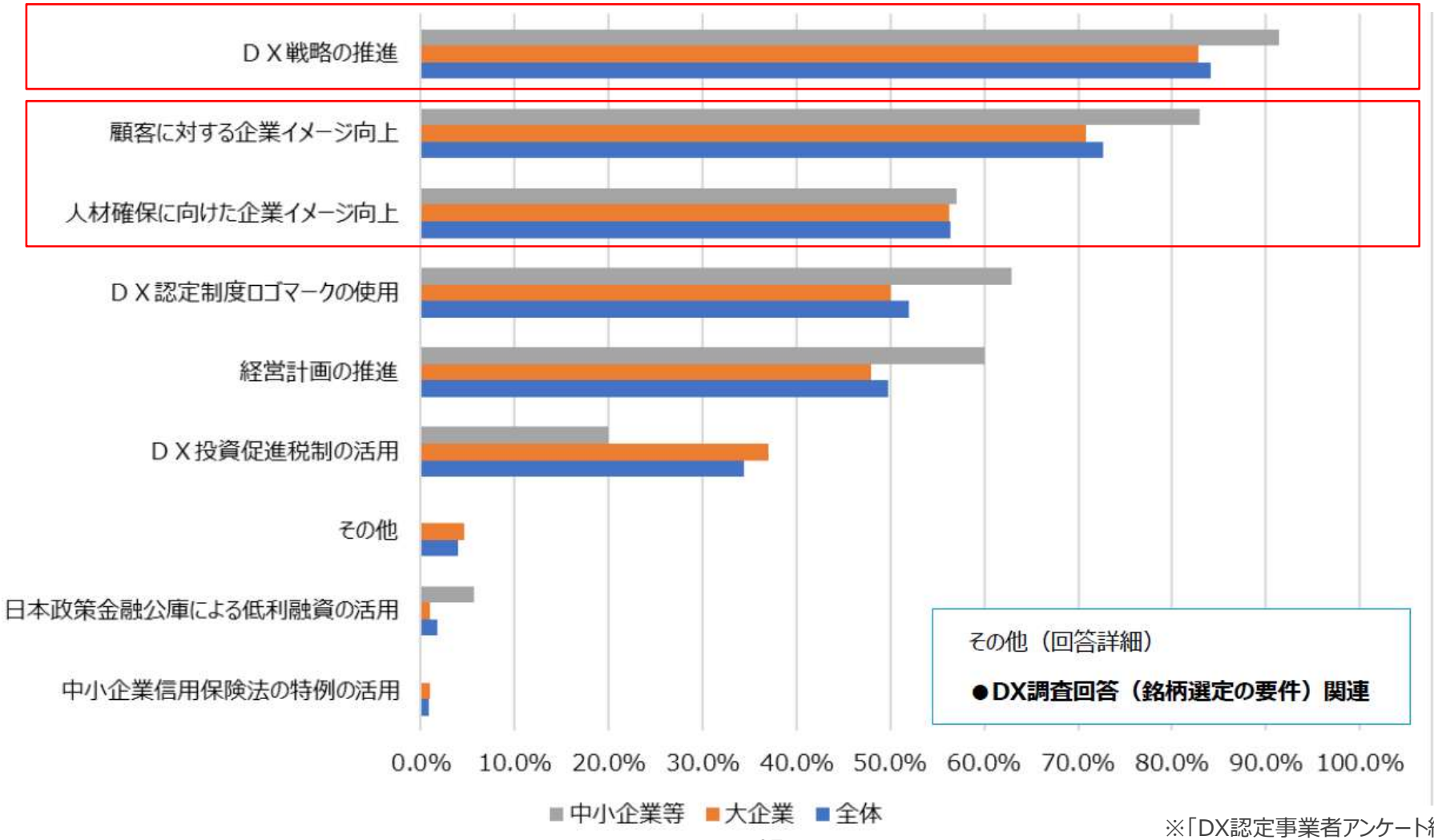
DX認定制度（2/2）

2026年６月時点で2,000社を超えている。業種としては、情報通信業や製造業での取得割合が高い。また、中小企業等では約1.6倍と全認定事業者数の増加を牽引



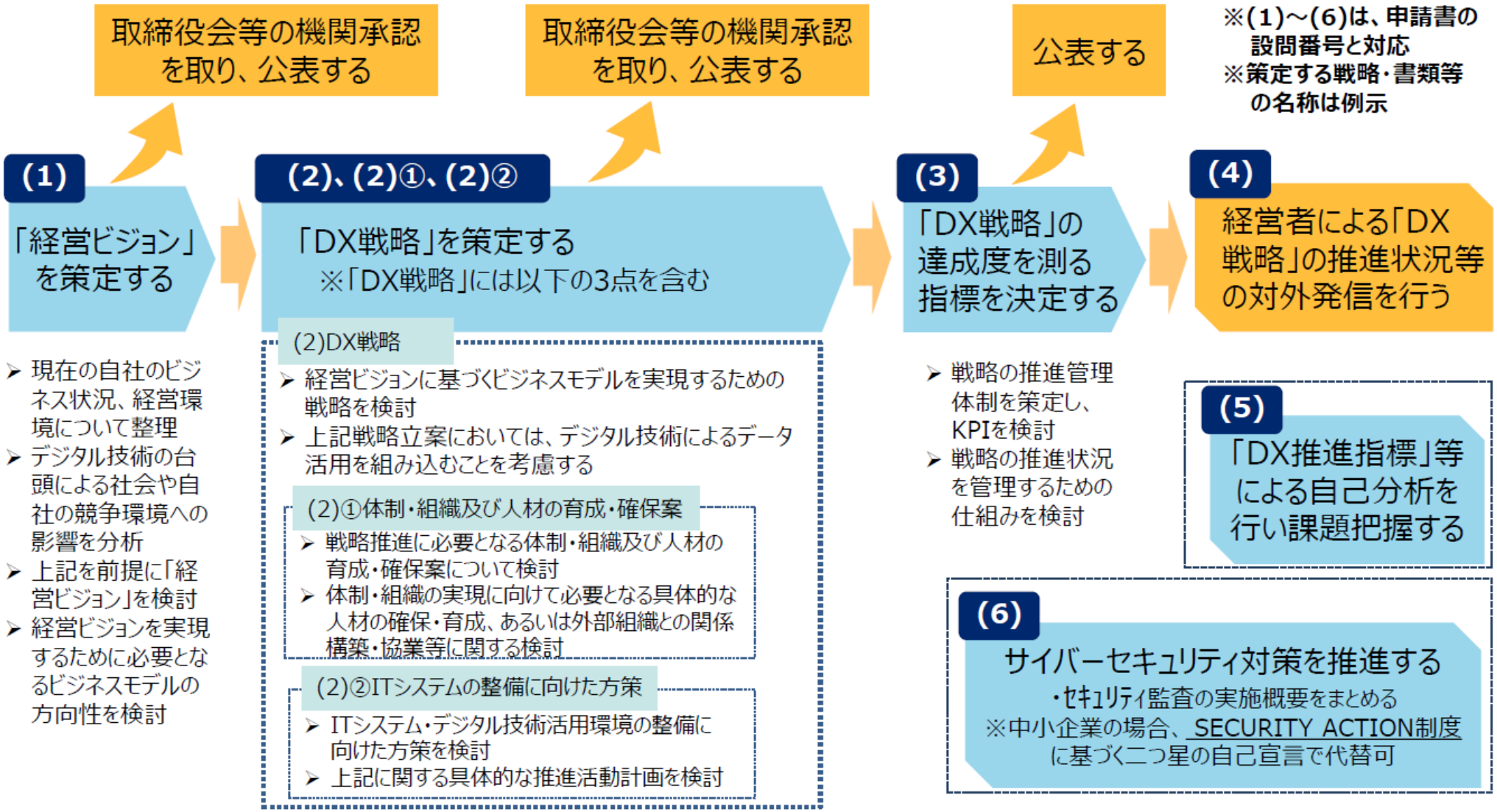
DX認定取得によるメリット

DX推進を行う上での「最初のゴール」に設定することはおススメ。税優遇や低利融資だけでなく、企業のイメージ向上も大きなメリット、若い人材への強力なアピールにもつながる



※「DX認定事業者アンケート結果」（経済産業省,2022）

DX認定取得のための手順



※「DX認定制度概要」（経済産業省,2022）

DX認定が求めていること／気にしなくていいこと

求めていること

- 経営者が一人称で取り組んでいること
  - ✓ 「経営者による自社取組の情報発信」
- 全社として取り組んでいること
  - ✓ 一部組織だけが勝手に行っているのではなく、全社として正式に行っていること
- 実施していることを正確に外部に公表していること

気にしなくていいこと

- 現時点で成果が出ていなくてもよい（「DX-Readyであること」（企業がデジタルで自らのビジネスを変革する準備ができている状態」だけが条件）
- 検討した戦略などの内容自体の是非は問わない
- 他の事業者と比較して評価するわけではなく、基準をクリアしたものは全て合格

DX認定をとるためのハードルは決して高くない

DXセレクション

「DXセレクション」は、中堅・中小企業等のモデルケースとなる優良事例を選定するもの。地域内や業種内での横展開を図り、各地域でのDX推進の取組を活性化することを目的としている







企業名	所在地
プーラビダ株式会社	福岡県



企業名	所在地
株式会社ヒューマングループ	長崎県
三行合成樹脂株式会社	新潟県

企業名	所在地
コマツ株式会社	大阪府
株式会社川六	香川県
株式会社ヤマナミ麺芸社	大分県
株式会社エヌエスケーケー	兵庫県
株式会社ネクサスエージェント	大阪府
旭光電機株式会社	兵庫県
株式会社加藤工務店	愛知県
株式会社三城	北海道

サイバーセキュリティの確保

サイバー攻撃とは

サイバー攻撃の目的は？

金銭窃取



情報窃取



機能妨害



影響工作



サイバー攻撃者は誰？

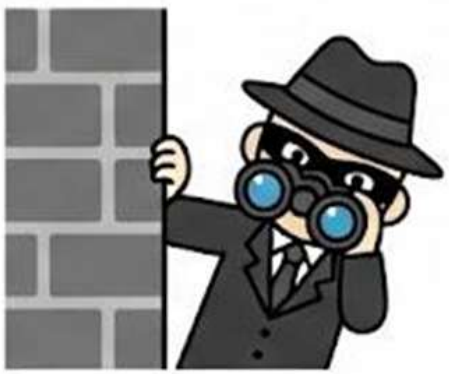
犯罪者
[e-Crime]





サイバー活動家
[ハクティビスト]

国家
[スパイ？]





内部不正者
[インサイダー]

サイバー攻撃の手口は？

詐欺メール（フィッシング）



偽メールで、パスワードを盗む、マルウェアを仕込む

不正アクセス



ソフトウェアの脆弱性をついて侵入する

大量アクセス（DDoS攻撃）



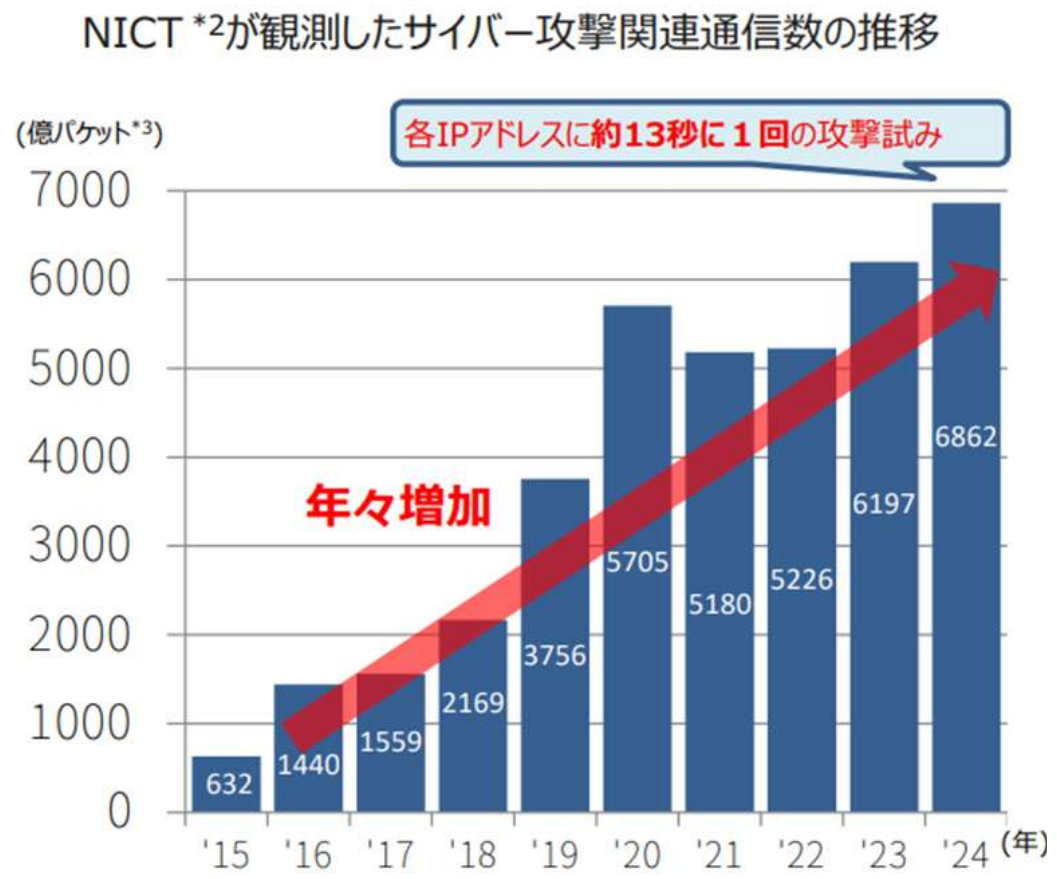
大量アクセスでウェブサイトなどをパンクさせる

データの人質化（ランサム）



データをロックして、身代金を要求する

サイバー攻撃は増加の一途



*2 国立研究開発法人 情報通信研究機構
（National Institute of Information and Communications Technology）の略。
*3 １度に届くデータの塊のこと。センサーがデータを受信した回数と同義。



■図 1-1-8　年度別フィッシング報告件数（2017～2023 年度）
（出典）フィッシング対策協議会「月次報告書」（2017 年 4 月～ 2024 年 3 月）を基に IPA が作成

情報セキュリティ10大脅威

「情報セキュリティ10大脅威」とは？

- IPA が2006年から毎年発行
- 前年に発生したセキュリティ事故や攻撃の状況等から、国内のセキュリティ専門家等からなる選考会で選出
- 「個人」と「組織」の２つの立場で脅威を解説

- 詳細な内容は以下のURLをご覧ください



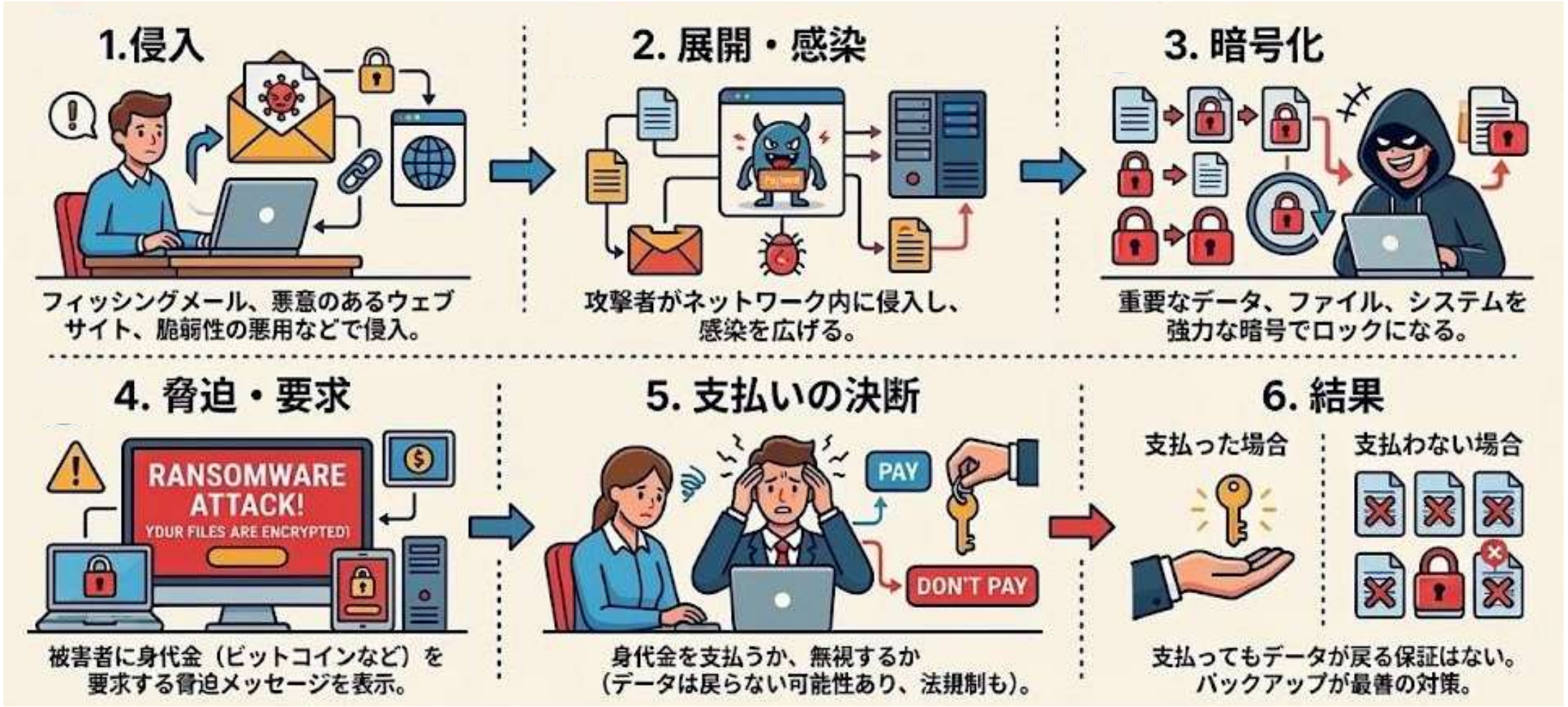
https://www.ipa.go.jp/security/10threats/10threats2026.html

「情報セキュリティ10大脅威2026」

順位	2024	2025	2026
1	**ランサムウェアによる被害**	**ランサムウェア攻撃による被害**	**ランサムウェア攻撃による被害**
2	**サプライチェーンの弱点を悪用した攻撃**	**サプライチェーンや委託先を狙った攻撃**	**サプライチェーンや委託先を狙った攻撃**
3	内部不正による情報漏えい等の被害	システムの脆弱性を突いた攻撃	**AIの利用をめぐるサイバーリスク【新規】**
4	標的型攻撃による機密情報の窃取	内部不正による情報漏洩等	システムの脆弱性を悪用した攻撃
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	機密情報を狙った標的型攻撃	機密情報を狙った標的型攻撃
6	不注意による情報漏えい等の被害	リモートワーク等の環境や仕組を狙った攻撃	**地政学的リスクに起因するサイバー攻撃（情報戦を含む）**
7	脆弱性対策情報の公開に伴う悪用増加	**地政学リスクに起因するサイバー攻撃**	内部不正による情報漏えい等
8	ビジネスメール詐欺による金銭被害	分散型サービス妨害攻撃（DDoS攻撃）	リモートワーク等の環境や仕組みを狙った攻撃
9	テレワーク等のニューノーマルな働き方を狙った攻撃	ビジネスメール詐欺	DDoS攻撃（分散型サービス妨害攻撃）
10	犯罪のビジネス化（アンダーグラウンドサービス）	不注意による情報漏洩等	ビジネスメール詐欺

第１位 「ランサムウェア攻撃による被害」

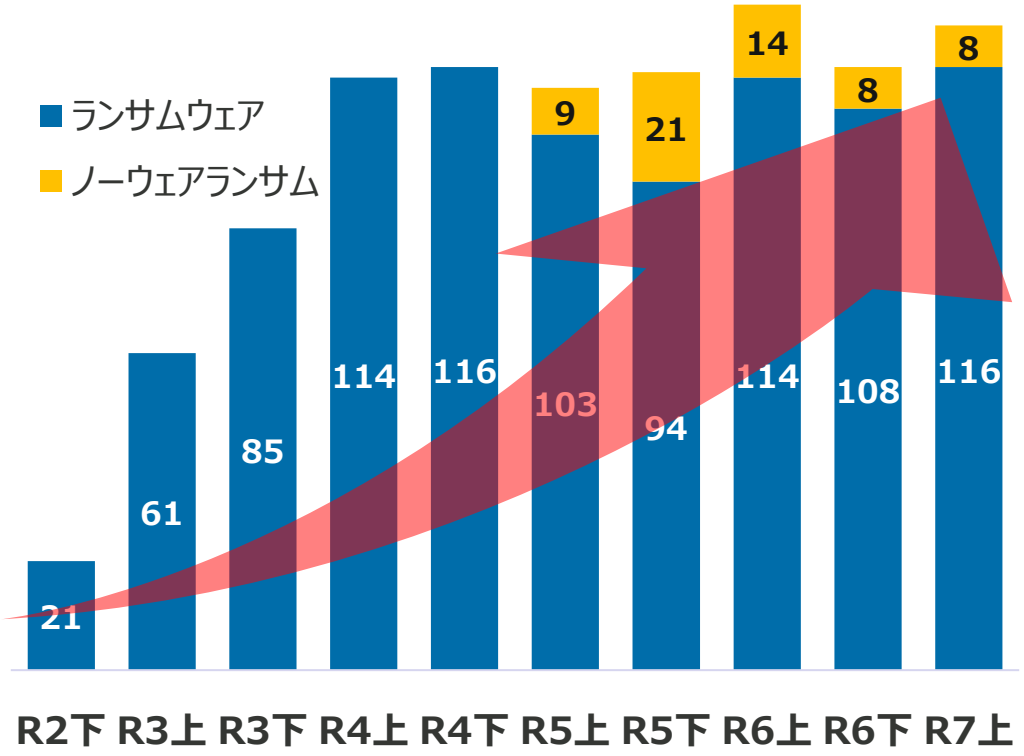
ランサムウェア攻撃の仕組み



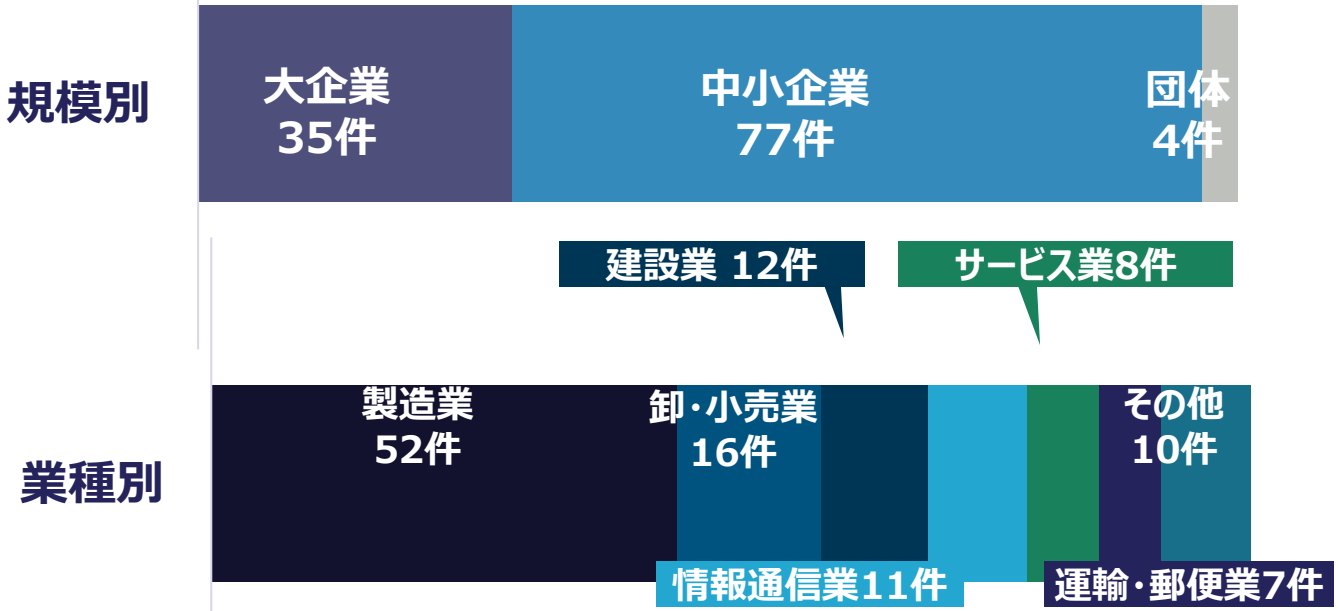
ランサムウェア攻撃による被害

ランサム被害は高止まり、大規模かつ長期に亘るケースも

ランサムウェアの被害報告件数推移



ランサムウェア被害の規模別・業種別内訳



出典「令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）」をもとにIPAが作成
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

ランサム攻撃による被害

2025年の具体事例

■ 飲料会社の事例

- 2025年9月、ランサム攻撃によるシステム障害が発生。飲料等の稼働停止、受注・出荷停止等の影響。
- 攻撃者は、グループ内の拠点にあるネットワーク機器経由でデータセンターのネットワークに侵入し、ランサムウェアを一斉に実行。

■ 商流会社の事例

- 2025年10月、ランサム攻撃でシステム障害が発生し、グループの受注・出荷が停止、他社のECや医療機関向け消毒薬・マスクの物流にも影響。
- 攻撃者は同年6月に業務委託先の管理者アカウントで初期侵入し、内部アクセスを拡大して事前設定時刻に一斉暗号化を実行した。

■ 自動車メーカーの事例

- 2025年8-9月、ランサム攻撃を受け、工場での生産停止、受発注・物流システム等を停止。部品サプライヤ等にも影響が及び、英国政府がサプライチェーン企業の資金繰り支援を表明。

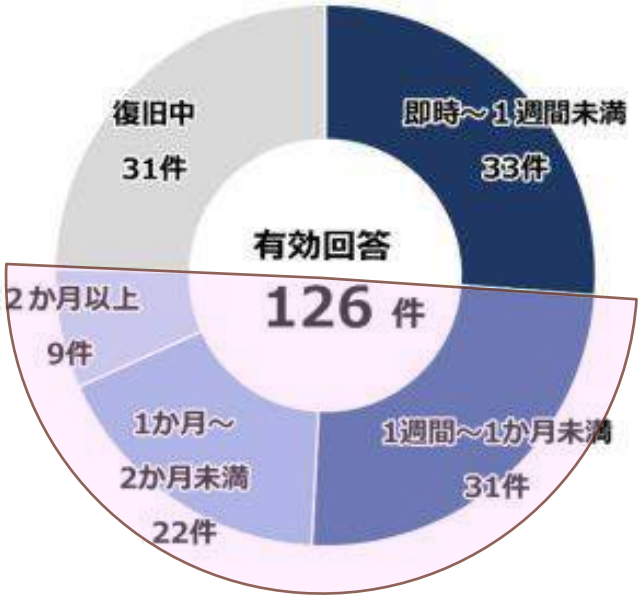
52

ランサムウェア攻撃による被害

ランサムウェア被害の影響は甚大

- 復旧に要した期間**1週間以上が約半数**
- **6割強**が調査・復旧に**500万円以上**を要していた。

復旧に要した期間



調査・復旧費用の総額



令和６年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）：
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

第２位　サプライチェーンや委託先を狙った攻撃

サプライチェーン攻撃とは？

サプライチェーンの中でセキュリティ対策が甘いところを狙った攻撃



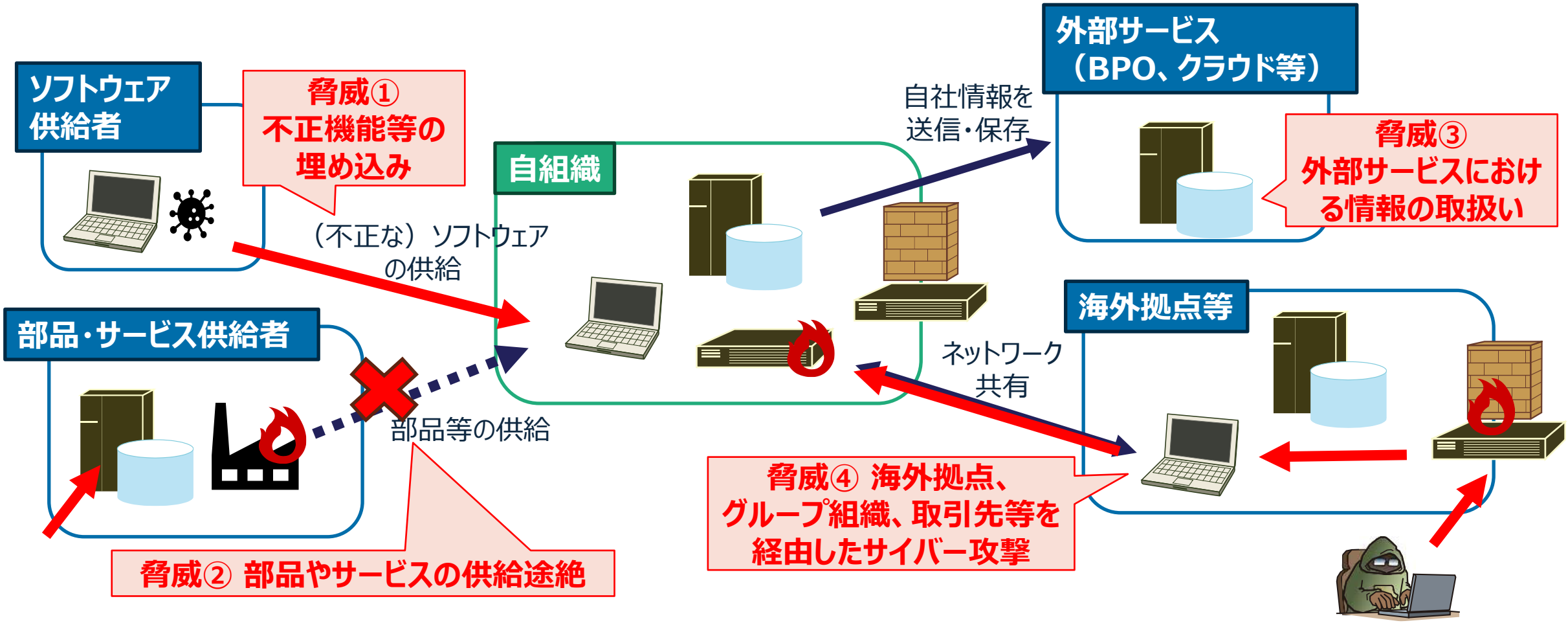
2種類のサプライチェーン

- **取引サプライチェーン（調達、製造、在庫管理、物流、販売、委託等の一連の商流）**
  - 取引先、委託先、グループ企業
  - 利用している外部サービス
- **ソフトウェアサプライチェーン（ソフトウェア開発・販売・運用・廃棄のライフサイクル）**

サプライチェーンや委託先を狙った攻撃

サプライチェーン攻撃の手口

- サプライチェーンに対する攻撃では、**セキュリティの弱い部分が狙われて、被害が伝播する。**



【出典】「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」（NISC）に基づきIPA作成

サプライチェーンや委託先を狙った攻撃

委託先での情報漏えいで被害を受けるケースが頻発

最近の業務委託先インシデント事例　（2024年報道より）

業種	物流業	物流業	ソフトウェア開発	情報処理・BPO	建設業
概要	ランサムウェア攻撃	ランサムウェア攻撃	ランサムウェア攻撃	ランサムウエア攻撃	不正アクセス
影響	取引先の入出庫処理の停止または遅延	個人情報漏えいの可能性	個人情報漏えいの可能性	個人情報漏えい	個人情報漏えいの可能性
影響	**約47社**	**5社 約30万人**	**7社 約18万件**	**約50社 約100万人**	**51社 約177件**

⇒　**サイバーインシデントは自社だけでなく複数の取引先や場合によってはサプライチェーン全体に影響が及ぶ**

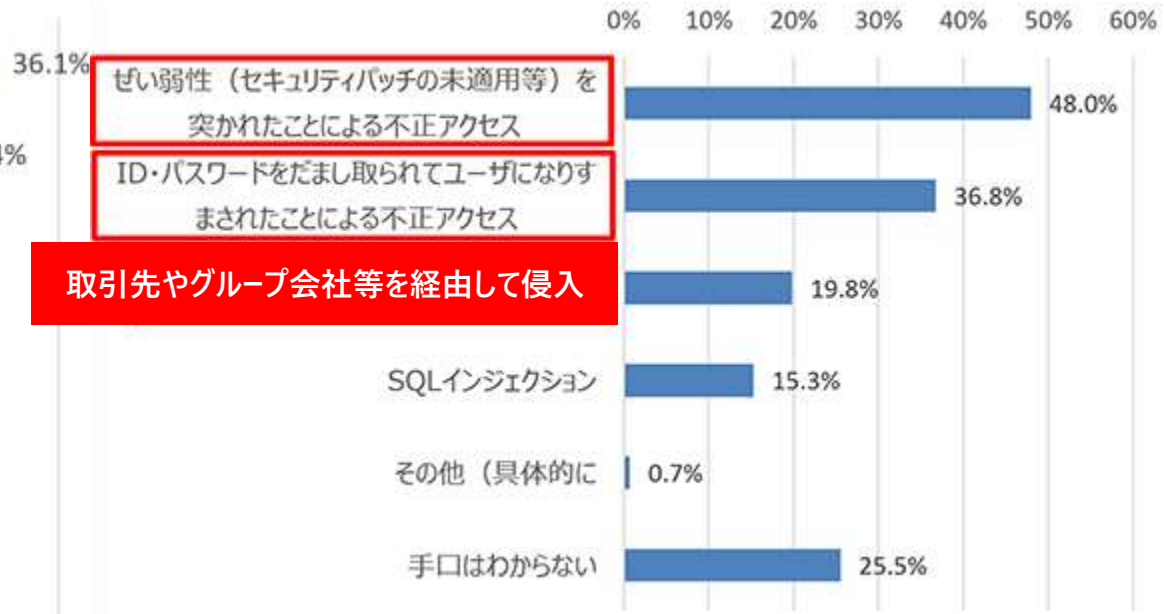
サプライチェーンや委託先を狙った攻撃

サプライチェーン経由で被害者にも加害の起点にもなりうる

- サイバーインシデントにより取引先に影響があった企業は**約７割**。
- また、インシデントの**２割**は取引先やグループ会社等を経由した侵入が原因。



質問：サイバーインシデントにより貴社の取引先（サプライチェーン）に影響はありましたか。影響が及んだ場合はその内容について教えてください。



質問：貴社が受けたサイバー攻撃の手口について教えてください。

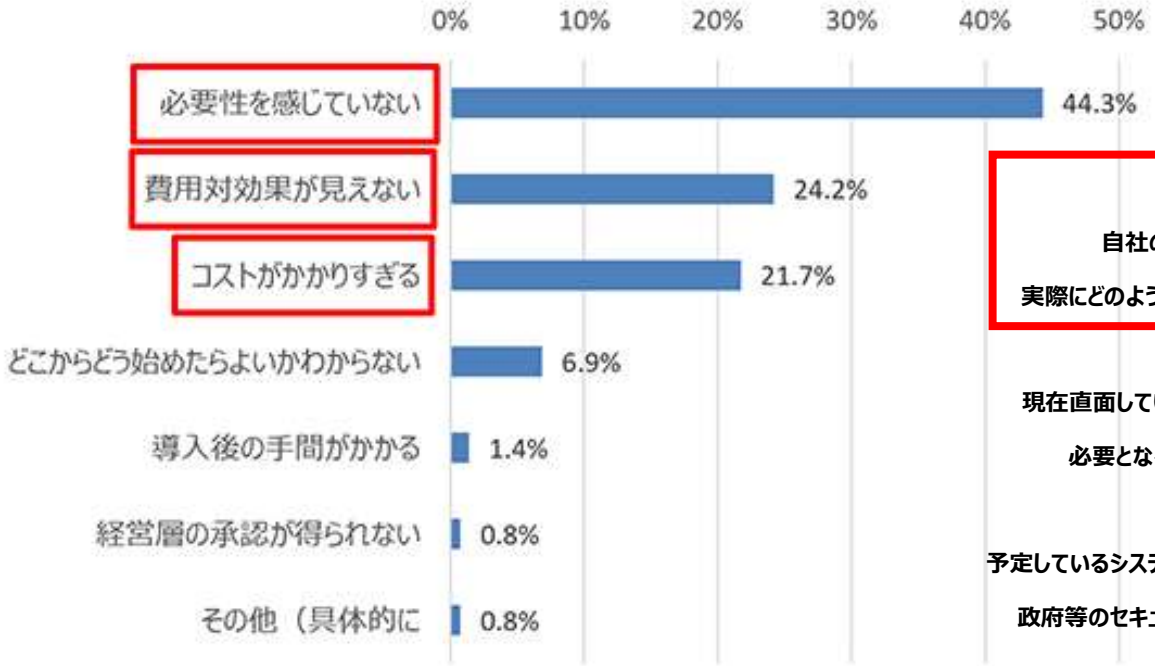
出典：「2024年度中小企業等実態調査結果」速報版（IPA）
https://www.ipa.go.jp/pressrelease/2024/press20250214.html

サプライチェーンや委託先を狙った攻撃

コスト（対策コスト、探索コスト）がボトルネック

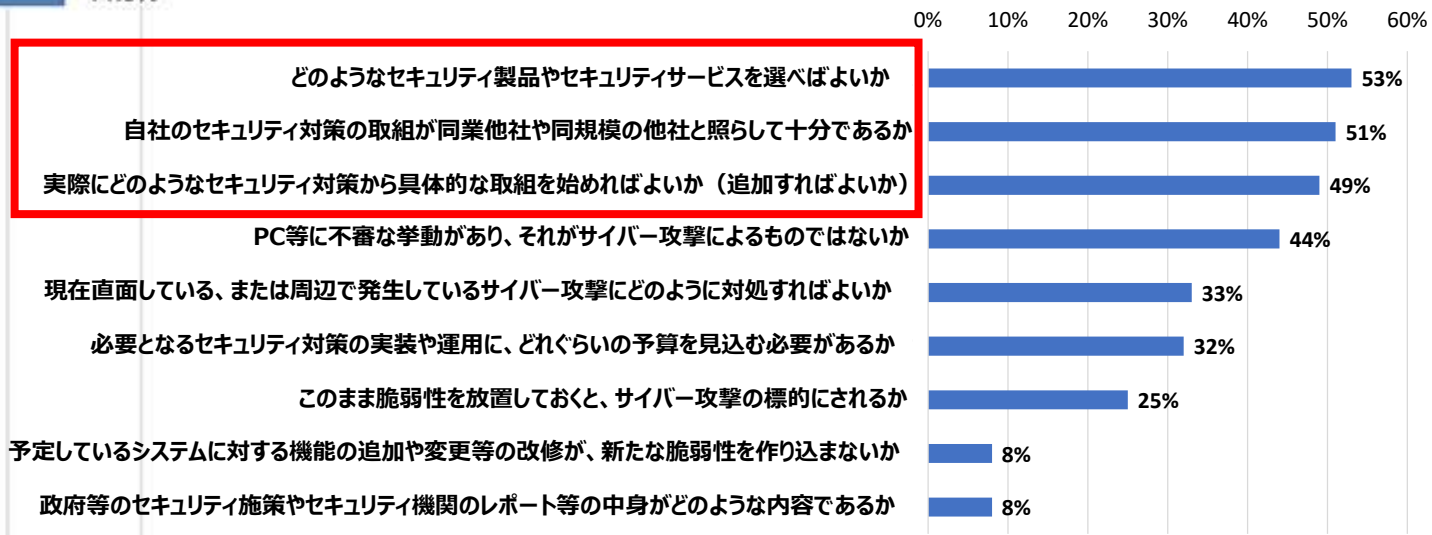
- 過去3期で**セキュリティ投資を行っていない**中小企業は**約６割**、うち、４割がセキュリティ投資の必要性を感じておらず、**約５割**が**コスト**面を指摘。
- 中小企業の**５割**が、どのような製品を導入すれば良いか、自社のセキュリティ対策が十分なのかに関心。

質問：前問で情報セキュリティ対策投資額について「投資をしていない」とお答えになった一番の理由について教えてください。（SA）



(n=2623)

中小企業のお客様からセキュリティ面の課題について多く寄せられる相談内容（N=146）

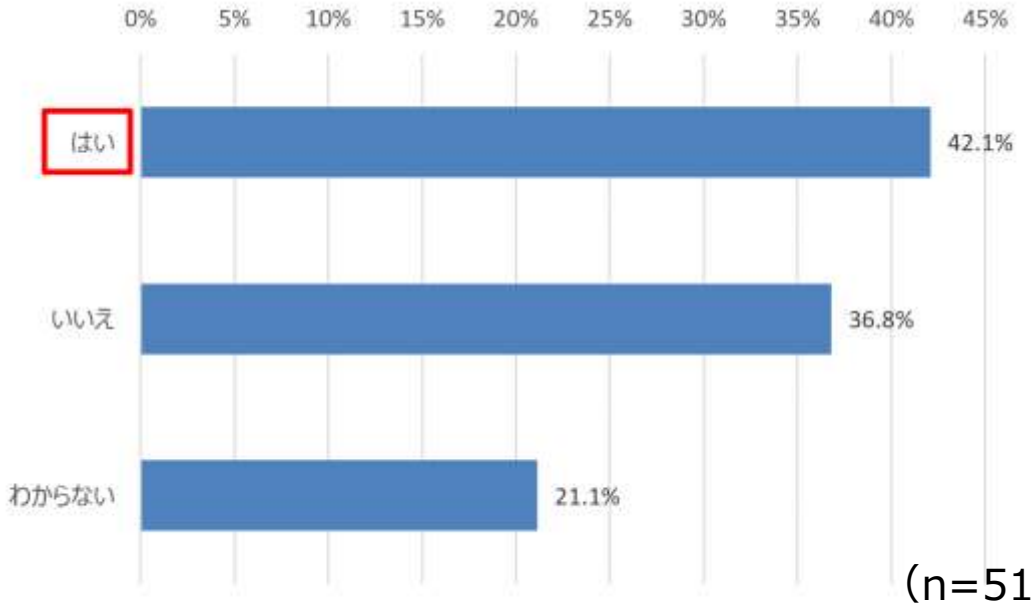


出典：「2024年度中小企業等実態調査結果」速報版（IPA）https://www.ipa.go.jp/pressrelease/2024/press20250214.html

サプライチェーンや委託先を狙った攻撃

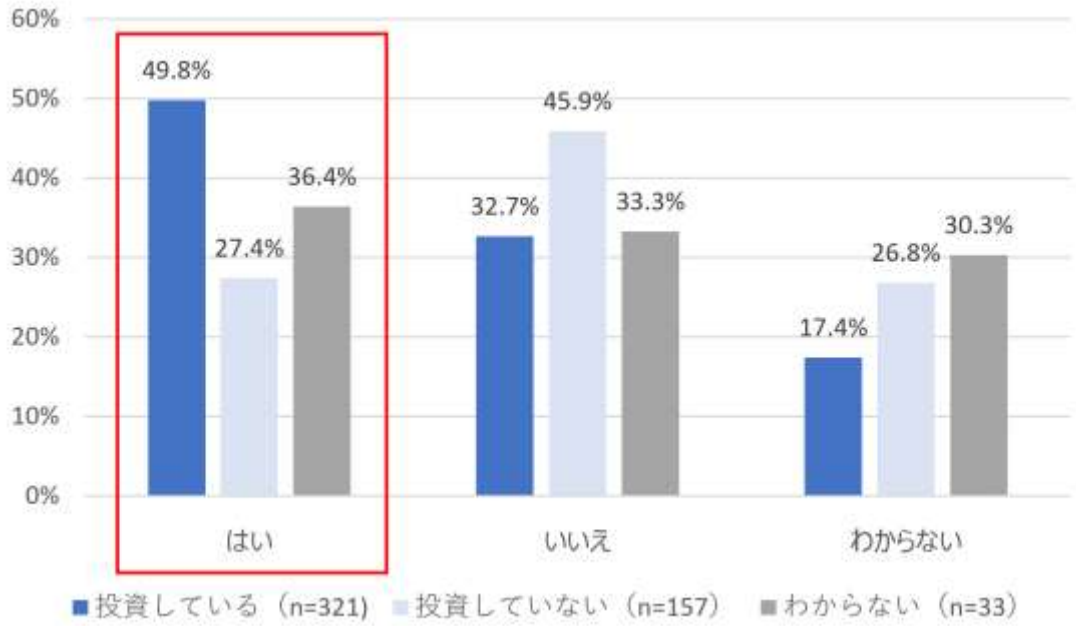
セキュリティ対策の実施は、取引拡大の契機に

- 取引先から要請された情報セキュリティ対策を行ったことが**取引につながった**と回答した企業は**約４割**
- 情報セキュリティ対策投資別では、対策投資を行っている企業の約５割が、取引につながったと回答



（n=511）

質問：貴社は取引先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。（SA）



左の質問と、情報セキュリティ対策投資を行ったかどうかの質問とのクロス集計

SCS評価制度（サプライチェーン セキュリティ対策評価制度）

セキュリティ対策の基本

- 多数の脅威があるが「攻撃の手口」は似ている
- 基本的な対策方法は年月が経っても変わらない
- 下記の「情報セキュリティ対策の基本」は常に意識

攻撃の手口	情報セキュリティ対策の基本	目的
パスワード窃取	**パスワードの管理・認証の強化**	パスワード窃取によるリスクを低減する
ソフトウェアの脆弱性の悪用	**ソフトウェアの更新**	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	**セキュリティソフトの利用**	攻撃をブロックする
設定不備の悪用	**設定の見直し**	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	**脅威・手口を知る**	手口から重要視するべき対策を理解する

SECURITY ACTION（セキュリティ対策自己宣言）

「★一つ星」を宣言

これから「情報セキュリティ6か条」に取り組むことを宣言（対策実施前でも申し込める）

1. **OSやソフトウェアは常に最新の状態にしよう！**
2. **ウイルス対策ソフトを導入しよう！**
3. **パスワードを強化しよう！**
4. **共有設定を見直そう！**
5. **バックアップを取ろう！**
6. **脅威や攻撃の手口を知ろう**

「★★二つ星」を宣言

「5分でできる！情報セキュリティ自社診断」を実施した上で、「情報セキュリティ基本方針」を策定・外部公開し、情報セキュリティ対策に取り組むことを宣言するもの



診断項目	No	診断内容
Part 1 基本的対策	1	パソコンやスマートフォンなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマートフォンなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1は最新の状態にしていますか？
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4	データの共有設定を必要な人に限定していますか？
	5	故障や誤操作、ウイルス感染などによる重要情報※2の消失に備えて定期的にバックアップを取得していますか？
	6	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
Part 2 従業員としての対策	7	電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？
	8	電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？
	9	重要情報の受け渡しは、暗号化など安全な手段で行っていますか？
	10	無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
	11	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書棚などに安全に保管していますか？
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
	14	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
	15	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	16	関係者以外の事務所への立ち入りを制限していますか？
	17	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
Part 3 組織としての対策	18	内部ネットワークを守るため、不正アクセス対策機能を設定していますか？
	19	ウェブサイトで公開すべきでない情報を公開していませんか？
	20	従業員に情報セキュリティに関する教育や注意喚起を行っていますか？
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
	25	情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？

※「SECURITY ACTION」公式サイト（制度概要）https://www.ipa.go.jp/security/security-action/index.html

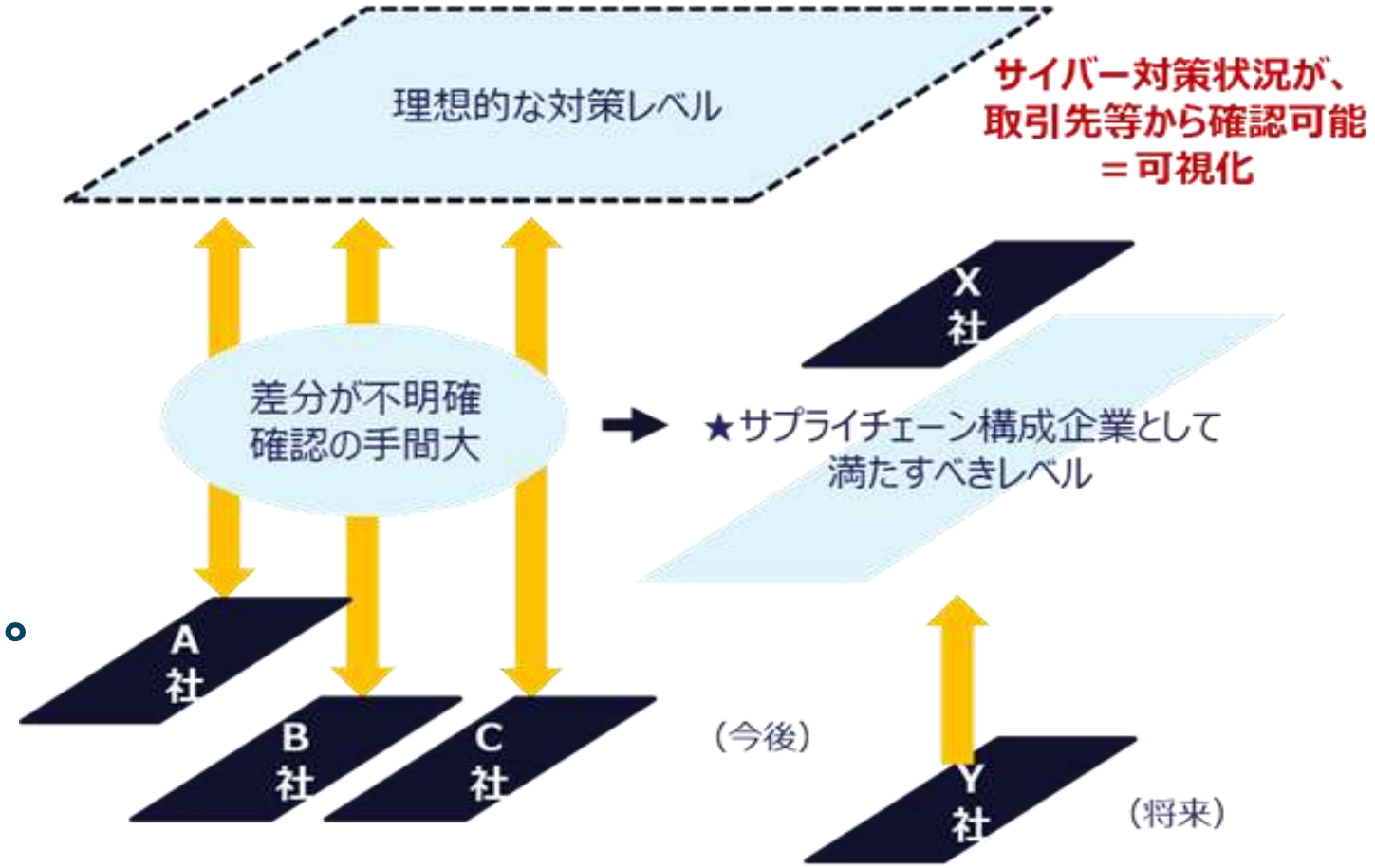
SCS評価制度（サプライチェーンセキュリティ対策評価制度）：目的

サイバー対策レベルの可視化による全体的な底上げ

「対策状況は外部から判断が難しい」

「複数の取引先から様々な対策を要求される」

などの課題に対し、サプライチェーンにおける重要性を踏まえた上で満たすべき対策を提示しつつ、その状況を可視化する仕組を構築。



出典：経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針（案）」（SCS評価制度の構築方針（案））
https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html

SCS評価制度：概要

- **２社間の取引契約等において、発注企業が、受注側に適切な段階の”★”を提示し、示された対策を促すとともに実施状況を確認することを想定。本制度の活用促進を通じ、サプライチェーン全体でのセキュリティ対策水準の向上を図る。３段階の水準のうち、★３・★４について、令和８年(2026年)度末頃の制度開始を予定。**

構築する評価制度（案）

成熟度の定義	★３	★４	★５［検討中※］
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等が到達点として目指すべき対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
評価スキーム	**専門家確認付き自己評価**	**第三者評価**	第三者評価

※ ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

出典：経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針（案）」（SCS評価制度の構築方針（案））
https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html

SCS評価制度：求められる対策

NIST Cyber Security Framework(CSF)の機能に対応した対策を提示（サイバーセキュリティの動向等を踏まえ定期的な見直しを想定）

大分類	★3	★4	NIST CSFにおける機能
ガバナンスの整備	**企業として最低限のリスク管理体制の構築** ・自社のセキュリティ担当の明確化 [No.1-2-1] ・セキュリティ対応方針の策定 [No.1-3-1]	**継続的改善に資するリスク管理体制の構築** ・定期的な経営層への報告、不備の是正等 [No.1-4-1]	統治(GV)
取引先管理	**取引先に課す最低限のルール明確化** ・他社との機密情報の取扱い明確化 [No.2-1-2] ・接続している外部情報サービスの把握 [No.3-1-3]	**取引先の管理・把握及び取引先との役割・責任の明確化** ・機密情報共有先の把握 [No.2-1-1] ・重要な取引先等の対策状況把握 [No.2-1-3] ・インシデント発生時の他社との役割等の明確化 [No.2-1-4]	
リスクの特定	**自社IT基盤や資産の現状把握** ・情報資産やネットワークの把握 [No.3-1-1,3-1-2] ・外部情報サービスの管理 [No.3-1-3]	**脆弱性など最新状況の把握と反映** ・脆弱性管理体制、管理プロセスの明確化 [No.3-2-1]	識別(ID)
攻撃等の防御	**不正アクセスに対する基礎的な防御** ・ID管理手続、アクセス権限の設定[No.4-1-1,4-1-2] ・パスワードの安全な設定及び管理 [No.4-1-4,4-1-5] ・内外ネットワーク境界の分離・保護 [No.4-5-1] **端末やサーバーの基礎的な保護** ・適時のアップデート適用、不要ソフトウェアの削除[No.4-4-1,4-4-4] ・端末等へのマルウェア対策 [No.4-4-1,4-4-4]	**多層防御による侵入リスクの低減** ・重要な保管データの暗号化 [No.4-3-1,4-3-2] ・ログの収集・定期的な分析の実施 [No.4-4-3] ・社内システムにおける適切なネットワーク分離 [No.4-5-1] ・社外への不正通信の遮断(出口対策) [No.4-5-2]	防御(PR)
攻撃等の検知	**ネットワーク上の基礎的な監視等** ・ネットワーク接続・データの監視[No.5-1-1]	**迅速な異常の検知** ・情報機器等の状態、挙動の監視・対応や分析[No.5-1-1,5-1-2]	検知(DE)
インシデントへの対応	**インシデント発生に備えた対応手順の整備** ・インシデント対応手順の作成 [No.6-1-1]	*大分類「インシデントへの対応」において、★４での追加項目はなし	対応(RS)
インシデントからの復旧	**インシデント発生から復旧するための対策の整備** ・インシデント発生から復旧するための対策の整備[No.7-1-1]	**インシデントからの復旧手順等の整備** ・復旧ポイント、復旧時間を満たす手順等の整備[No.7-1-1]	復旧(RC)

SCS評価制度：セキュリティ専門家と評価機関

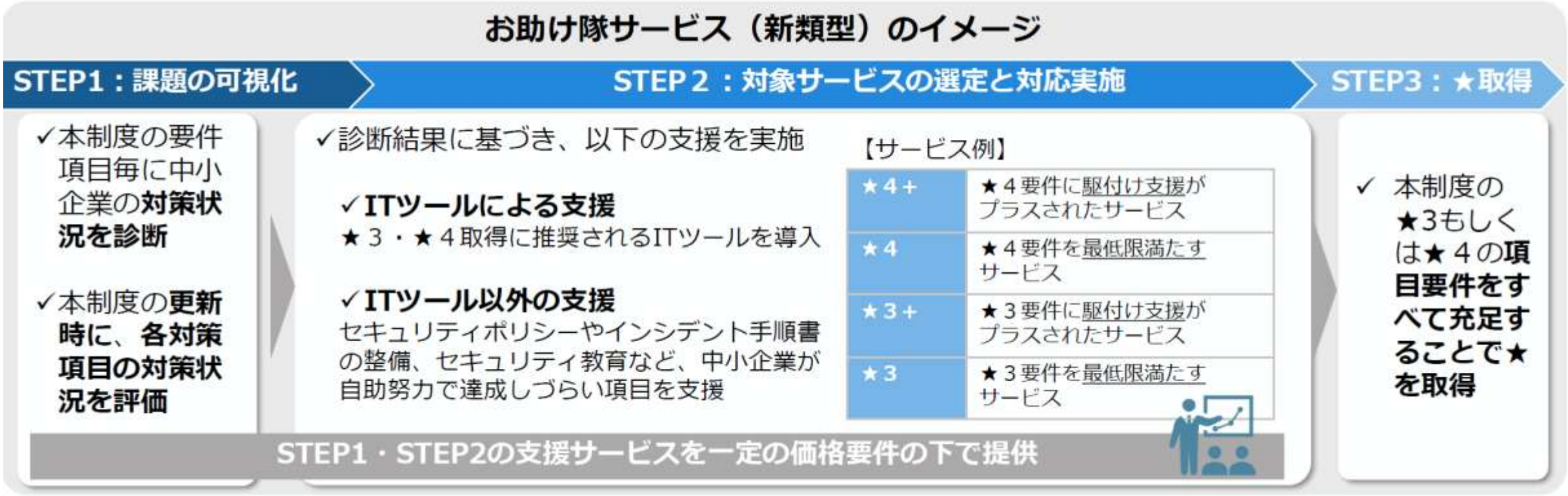
★３では、セキュリティ専門家が、取得希望組織が作成した書類の確認を行う。

★４では、評価機関・技術検証事業者が、文書確認に加え、実施審査および技術検証（脆弱性検査）を行う。

評価プロセス	所要期間(想定)	実施内容等	
		★3	★4
文書確認 (提出書類の確認)	1日~2日程度	• 取得希望組織が作成した自己評価の結果を確認する。 (主に、記載内容に矛盾がないか、評価基準から見て十分な事項が記されているかの確認を想定) • 文書確認の結果、記載内容に明らかな不適合が認められない場合、 ✓ ★3では、取得希望組織は事務局に申請を行い、申請内容に問題等がなければ★3を取得することができる。 ✓ ★4では、実地審査及び技術検証に進む。	
実地審査 (取得希望企業へのヒアリング、規程、操作画面等の確認による評価) ※リモートでの実施も可	1日~2日程度 ※ 事前準備、報告書作成は除く	(実施なし)	• 相対的に重要性が高いと考えられる対策事項について証跡確認を含めた評価を実施 [実地審査で確認すべき事項(例)] ✓ 脆弱性の管理体制、管理プロセス ✓ セキュリティインシデント対応手順 ✓ 事業継続要件に沿った復旧準備
技術検証 (取得希望企業の管理する対象機器に対して既知脆弱性の悪用等の一般的な攻撃パターンを試行)	1日~2日程度 ※ 事前準備、報告書作成は除く	(実施なし)	• 取得希望組織がインターネットに公開している機器のうち、脆弱性を悪用等された場合に組織内部に侵入されるリスクが高い機器(例：VPN装置、ルータ)を対象として、技術的な検証として脆弱性検査を実施する(検証対象とする評価基準：4-4-4-3) ※ 当該検証の実施結果に相当する証跡(例：直近における対象機器への脆弱性検査の実施結果)の提出及び確認をもって検証実施の代替とみなすことも検討する。
合格基準	-	• ★3･★4ともに、原則として、全ての評価基準への適合を求める。	
不適合の指摘及び改善	-	• 評価結果に不適合が発見された場合であっても、適切に是正対処し、セキュリティ専門家から当該是正について了承を得られれば★3を取得可能。	• 不適合事項の是正報告を、指摘時から一定期間内(例:評価機関からの指摘事項が通知されてから1ヶ月以内)に提出し、内容について了承を得られれば★4を取得可能。

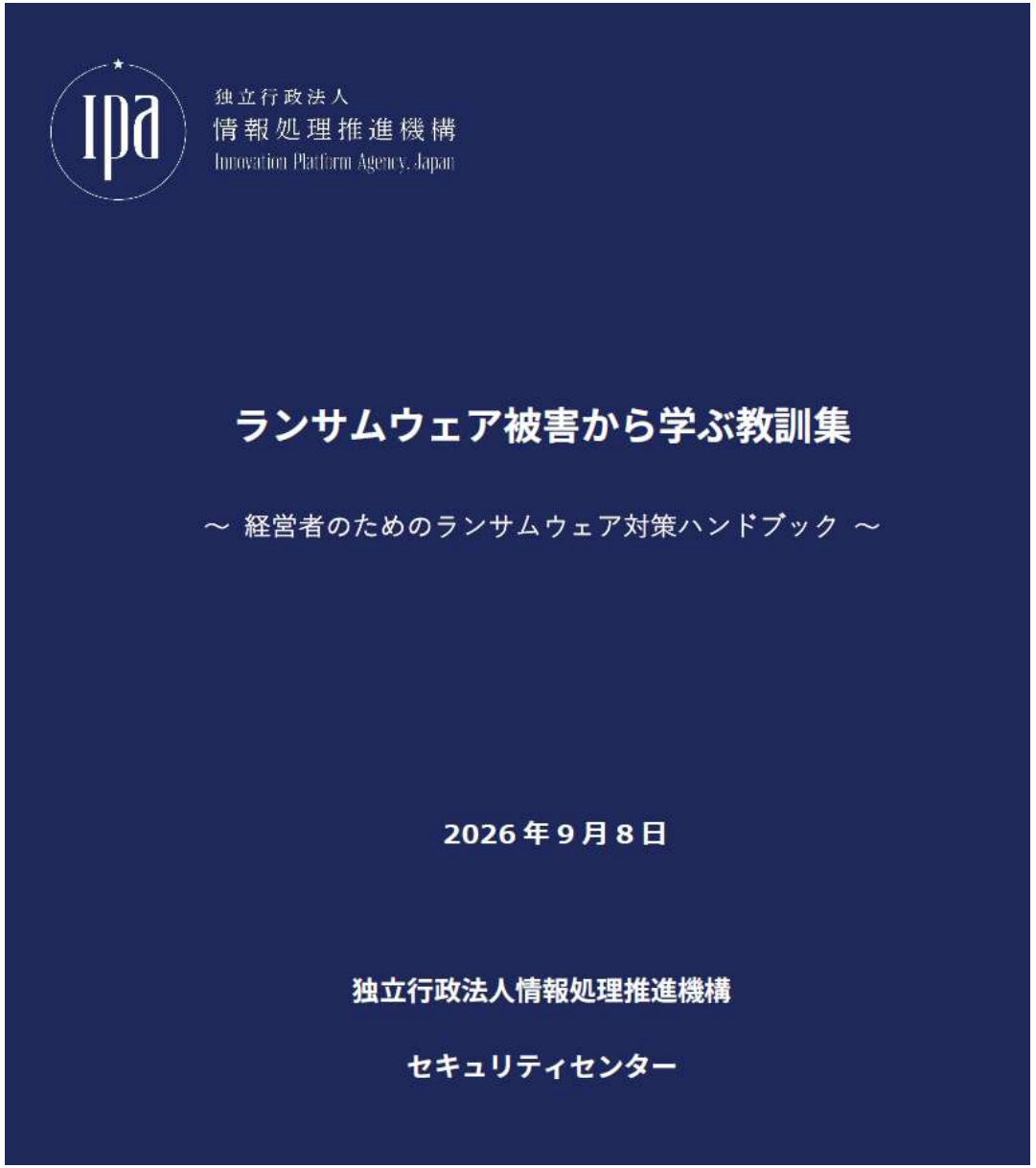
SCS評価制度：お助け隊による支援

「サイバーセキュリティお助け隊サービス（新類型）」によって、★３・★４の取得支援を行う。2026年度中に実証事業を予定している



「ランサムウェア被害から学ぶ教訓集」

「ランサムウェア被害から学ぶ教訓集」（IPA）



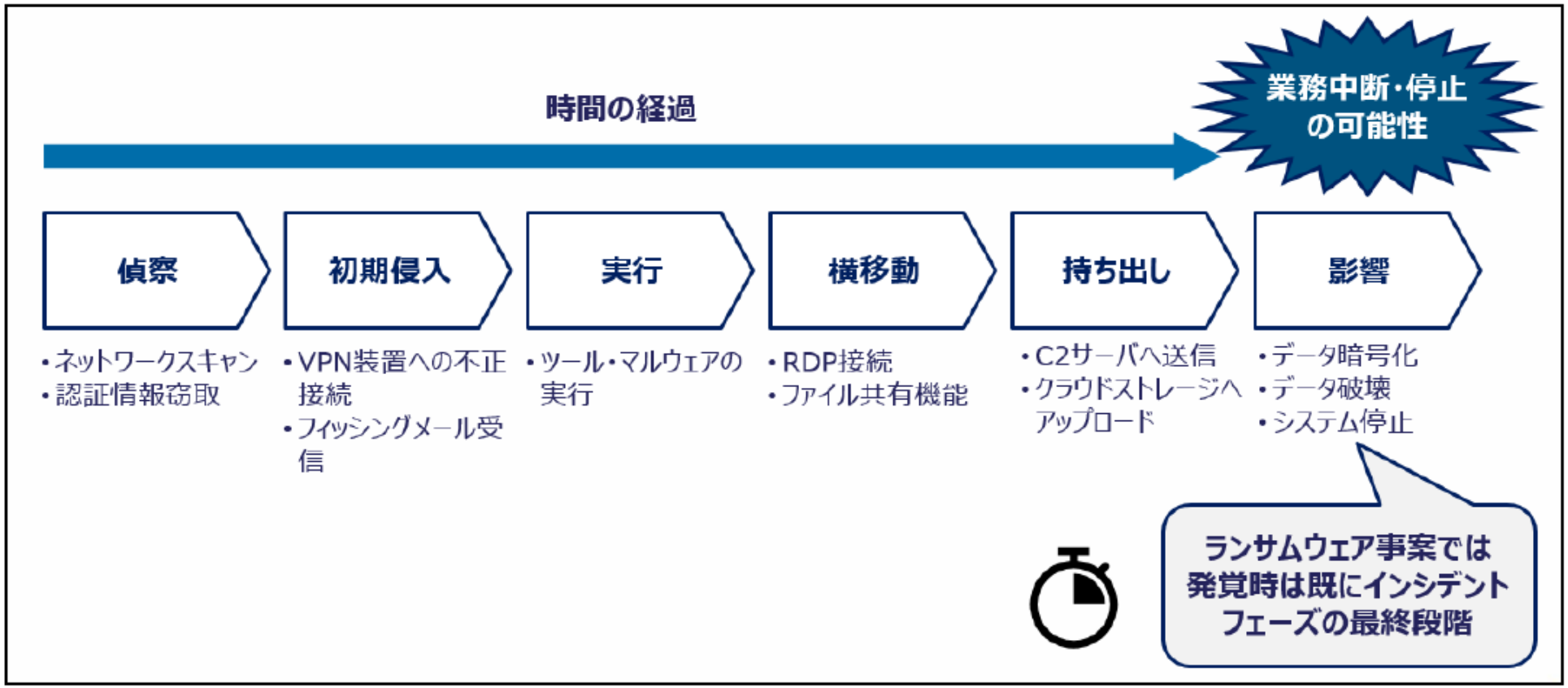
- ランサムウェア攻撃の被害が組織の規模を問わず多発している状況が継続しています。
- コンピュータウイルス・不正アクセス届出窓口では、国内の複数の被害組織へインタビューをおこない、被害発生当時、組織でどのようなことが発生し、どのような対応をしたかを振り返っていただきました。それらの中から他の組織でも起こり得ること等を抽出し、教訓として取りまとめ、経営者向けとインシデント対応部門向けに分けて整理しました。
- そして、ランサムウェアの脅威に立ち向かうには、経営者の理解と関与が非常に重要であることをお伝えするべく、サブタイトルを「経営者のためのランサムウェア対策ハンドブック」としました。
- 今後起こり得るランサムウェア事案への備えとして活かしていただくとともに、インシデント対応計画や事業継続計画（BCP（Business Continuity Plan））の更なる充実強化に役立てください。

※https://www.ipa.go.jp/security/todokede/crack-virus/ransomware_lessons_learned.html

事案の特性：ランサムウェア対応には時間的猶予がない

ランサムウェア事案は、何らかのデータが暗号化されてから被害に気付いた場合、事案発覚時において既に「インシデントフェーズの最終段階」となっており、対応の時間的猶予が限られる。すなわち、発覚時点で、一般的なITインシデント発生に求められる種々の対処について、「短期間」に実施することを余儀なくされる。

インシデントの主なフェーズ

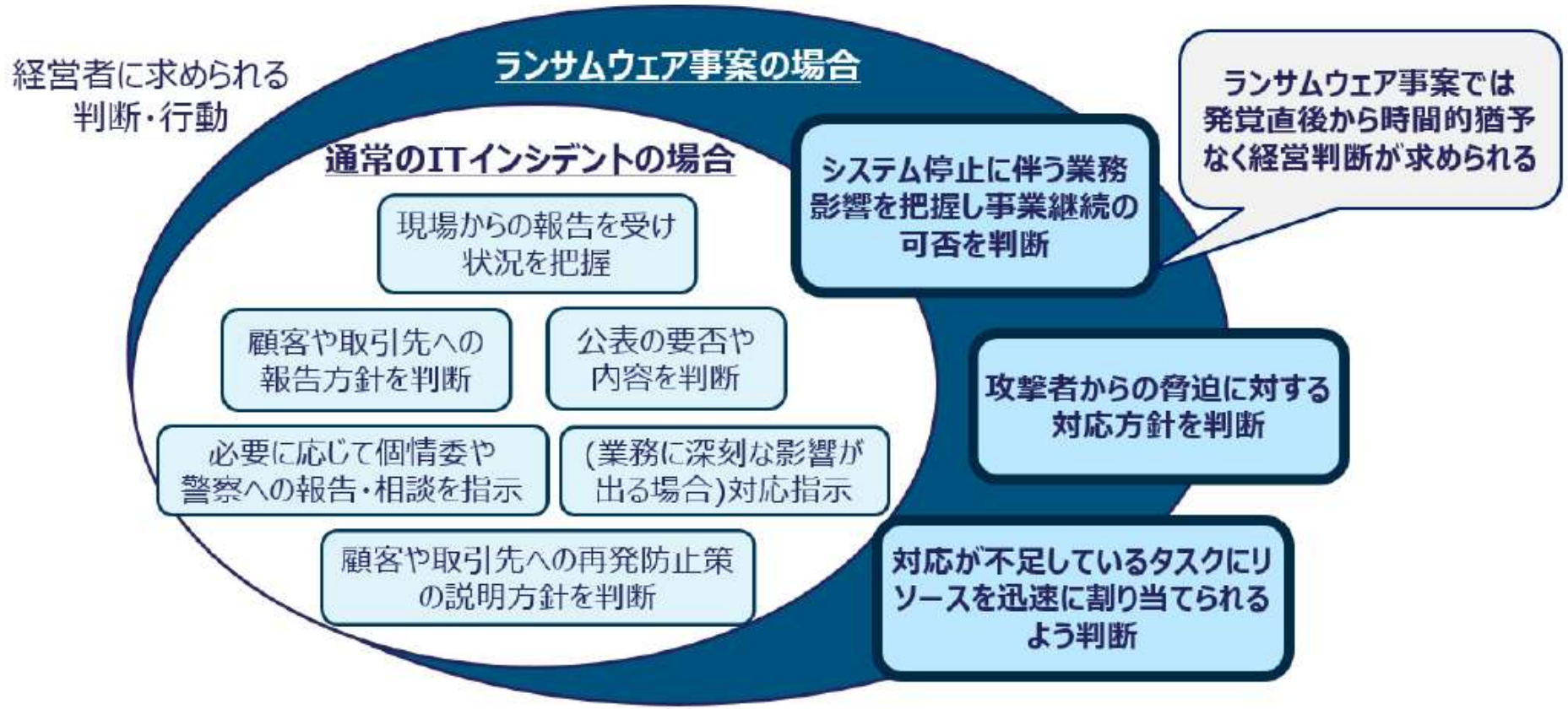


※「ランサムウェア被害から学ぶ教訓集」（IPA）

事案の特性：経営者に求められる判断・行動が増加する

ランサムウェア事案は、通常のITインシデントの場合以上に、経営者に求められる判断・行動が増加していく

経営者に求められる判断・行動



※「ランサムウェア被害から学ぶ教訓集」（IPA）

経営者やリスク管理部門が重視すべき教訓（1/2）

(1) 経営者による迅速な経営判断と明確な関与

- ランサムウェア事案対応には時間の猶予がない。発覚直後から業務中断や脅迫への対応、メディア対応等における経営判断を迫られる。経営者は事前に発生し得るリスクを認識し、緊急時に迅速な意思決定を行えるよう、判断基準や意思決定プロセスをあらかじめ整備しておく。

(2) インシデント対応体制の整備

- ITインシデントという特徴から情報システム部門に負荷が集中する傾向がある。しかし、ランサム事案は公表対応、法務対応、取引先対応、外部連携組織を含めた多方面の対応が必要となる。経営者は事前に情報システム部門、総務部門、広報部門、法務部門、営業部門を含めて全社的に役割分担を明確にしておく。

(3) 事業継続計画（BCP）への反映

- ランサムウェア攻撃によるシステム停止は業務停止に直結し得る。システムの停止・復旧の判断には、事業部門の関与が必須。経営者は事前に情報システム部門と事業部門の協力のもとサイバー攻撃に対応した事業継続計画（BCP）の策定を指示しておく。

※「ランサムウェア被害から学ぶ教訓集」（IPA）

経営者やリスク管理部門が重視すべき教訓（2/2）

(4) 個人情報を含むデータの現状把握

- 流出・暗号化されたデータの内容を後から特定するのは、フォレンジック調査を行っても困難であることが多い。経営者は事前にデータを管理する部署に向けて個人情報を含むデータの台帳を整備するよう指示しておく。

(5) 経営者主導の意思統一

- 組織内の意識のずれが大きいと混乱を招き、円滑な事案対応を阻害する。経営者は情報発信や権限委譲等の工夫を凝らし、組織の意思統一やスピード感のある対応を実現する。

(6) 窃取されたデータの暴露への備え

- 身代金を支払ってもデータの回復や暴露中止は保証されない。経営者はこの前提で窃取されたデータがダークウェブ上で暴露されるリスクに備えつつ、データ及びシステムの復旧を図る。

個人情報保護法における漏えい等報告の義務付け（民間事業者）

① 要配慮個人情報が含まれる個人データの漏えい等(又はそのおそれ)

② 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等(又はそのおそれ)

③ 不正の目的（不正アクセスによる漏えい／個人データが暗号化され復元できなくなった場案を含む）をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データの漏えい等(又はそのおそれ)

④ 個人データに係る本人の数が1,000人を超える漏えい等(又はそのおそれ)

※「ランサムウェア被害から学ぶ教訓集」（IPA）

（参考）身代金の支払いについて公的機関・団体が提唱する方針

- ランサムウェアに対する多国間会合「カウンターランサムウェア・イニシアティブ（CRI）」
  - ✓ 金銭支払いを避けることを強く推奨。多くのランサムウェア・インシデントにおいて、サイバー犯罪者はデータも盗むようになっており、身代金を支払えば盗まれたデータを削除するという約束を信用してはならないこと、身代金を支払ってもデバイスやデータへのアクセスが保証されるわけではないことに注意するよう促している
- 警察庁
  - ✓ 「暗号化されたデータを復号するための対価と称して、ランサムウェア攻撃グループから要求される金銭等を支払うこと」に関し、「犯罪グループ等の活動資金となることが懸念される」「暗号化されたデータの復号が保証されるわけではない」旨を被害者に対して説明するとともに、要求された金銭等の支払いの有無も含む、ランサムウェア被害に係る情報の提供をはじめとした捜査への協力を求めている
- 経済産業省
  - ✓ 「データ公開の圧力から、攻撃者からの支払い要求に屈しているケースは少なくないとの報告は存在するが、こうした金銭の支払いは犯罪組織に対して支援を行っていることと同義であり、また、金銭を支払うことでデータ公開が止められたり、暗号化されたデータが復号されたりすることが保証されるわけではない。さらに、国によっては、こうした金銭の支払い行為がテロ等の犯罪組織への資金提供であるとみなされ、金銭の支払いを行った企業に対して制裁が課される可能性もある。こうしたランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである」

※「ランサムウェア被害から学ぶ教訓集」（IPA）

インシデント対処にあたる部門が重視すべき教訓（1/2）

(1) バックアップとログの整合性確保

- バックアップは、汚染された可能性があるとシステム復旧に活用できない。少なくとも侵入開始時期よりも前の時点のバックアップは安全であることから、侵入開始時期を特定することの重要性は高い。そのため、必要なログを保存し、安全な復元時点を判断できるようにしておく。

(2) 基本的な対策の徹底

- ランサムウェアの被害の多くは基本的な対策ができていないことに起因する。基本的な対策を徹底・継続する。加えて、境界防御に隙を作らず、内部ネットワークが安全ではないことを前提にした対策とその維持を徹底する。

※ヒアリング調査においては、初期侵入後の侵害拡大は「安易なパスワード」、「アップデートしていないNAS」、「管理者アカウントでの運用管理」等が主原因であった

(3) EDR導入と定期ログ監査

- 従来型のウイルス対策ソフトのみでは、攻撃者の活動を十分に検知することができない場合がある。EDR等を導入するとともに、アラートに迅速に対応できる監視体制を整備し、定期的にログを確認・分析する。

※ EDR(Endpoint Detection and Response)：サーバおよびPC内の処理や外部との通信等の不審な振る舞いを検知することで迅速な対応を可能にする。

※「ランサムウェア被害から学ぶ教訓集」（IPA）

インシデント対処にあたる部門が重視すべき教訓（2/2）

(4)「漏えいなし」の証明は困難

- 顧客や取引先に対して「情報漏えいがなかったこと」を証明することは極めて困難。顧客や取引先には、フォレンジック調査等から判明した事実や経過観察の状況を、必要な範囲で丁寧に報告していくことになる。

※フォレンジック調査：PCやサーバへの攻撃者の活動痕跡を詳細に把握する調査。ただし、調査のコストが高額であり、調査時間もある程度必要なため、対象機器の全てに実施することが難しい場合は、攻撃の起点になったと思われる機器を優先する

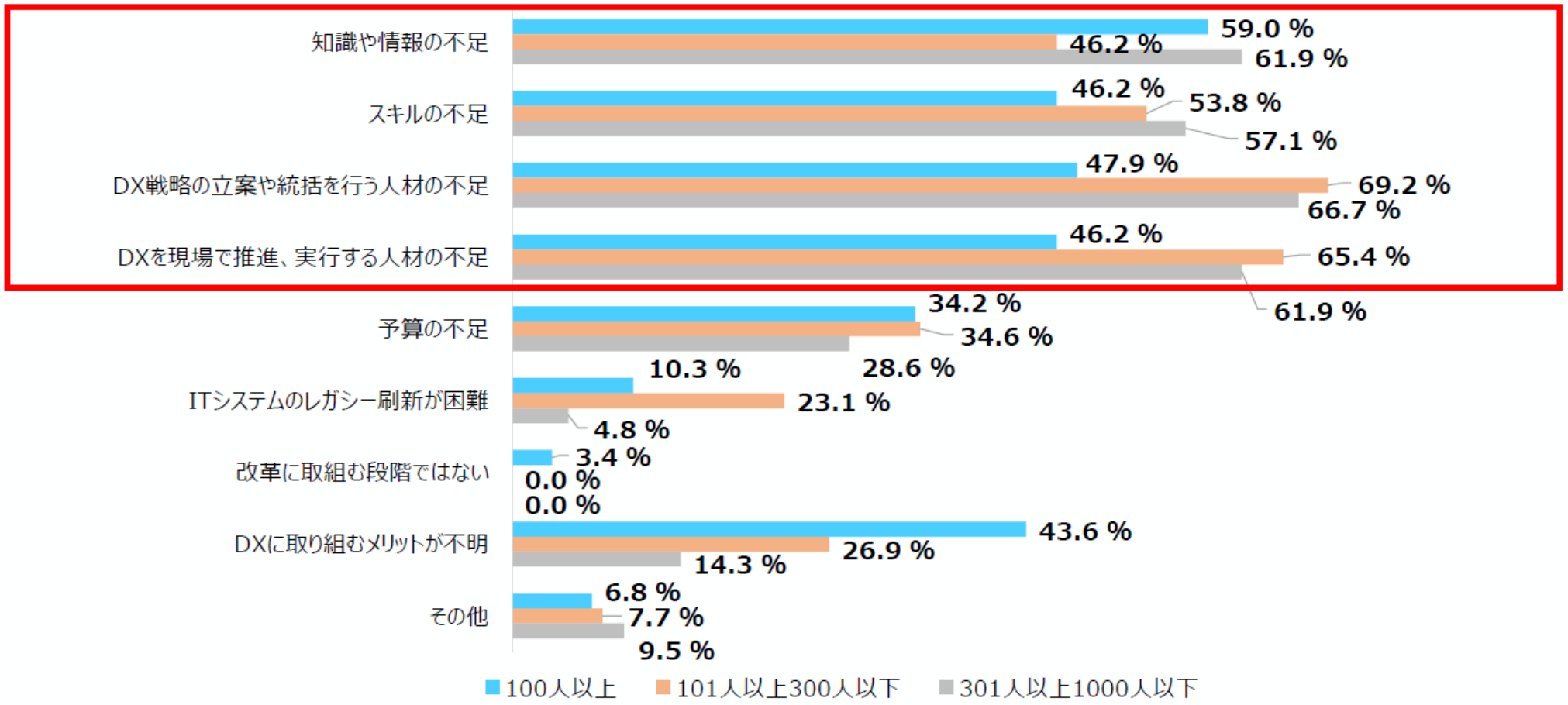
(5) セキュリティベンダーとの関係構築

- ランサムウェア事案への対応において、セキュリティベンダーが果たす役割は非常に大きい。一方、セキュリティベンダーに求められる役割は、組織の体制やインシデントの状況によって異なり、ベンダーごとに対応可能な範囲も異なるため、平時から必要な役割と対応範囲を把握し、適切なベンダーを選定し関係を構築しておく。

※「ランサムウェア被害から学ぶ教訓集」（IPA）

DX推進人材の育成・確保

DXに取り組めない理由は、予算ではなく人材・スキル

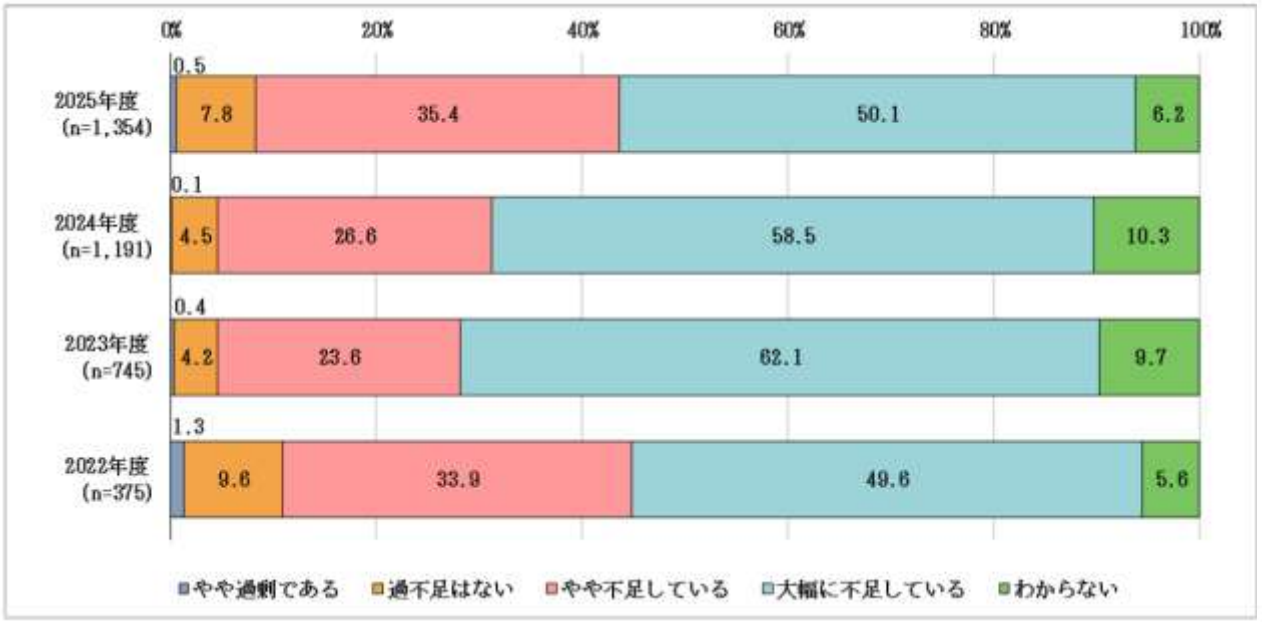


（注）DX取組予定で「DXに取組む予定はない」「DXに取り組むか、分からない」と回答した企業が対象であり、「1,001人以上」はn数が1であったためグラフからは除外。
出典：情報処理推進機構「DX動向2024（本文）」（2024年6月27日）を基に作成。

※「Society 5.0時代のデジタル人材育成に関する検討会」資料（経済産業省,2024）

DX推進人材は質・量ともに不足傾向が続いている

DXを推進する人材の「量」の確保（経年比較）



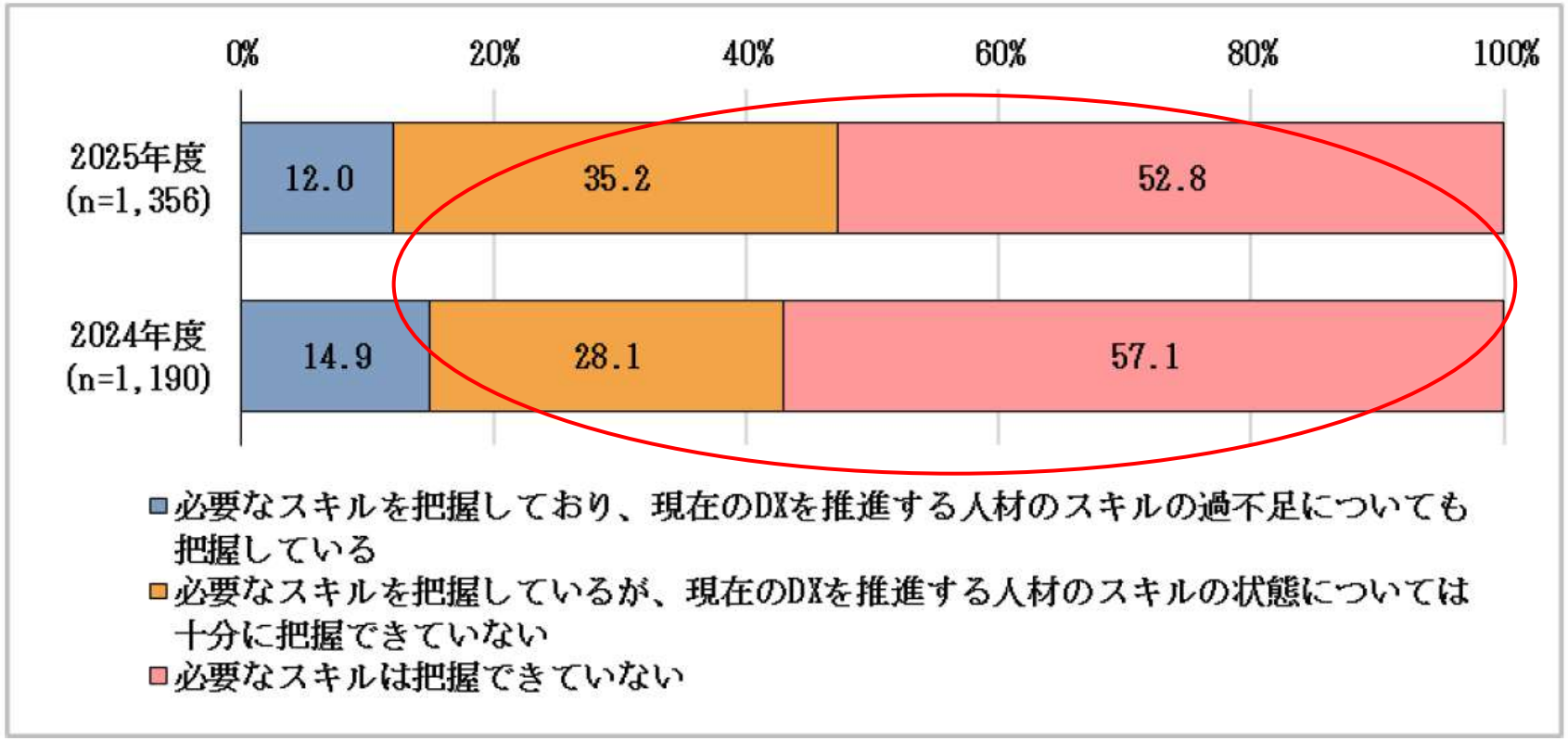
DXを推進する人材の「質」の確保（経年比較）



※DX動向2026,IPA

DX推進人材に必要なスキル把握は不十分

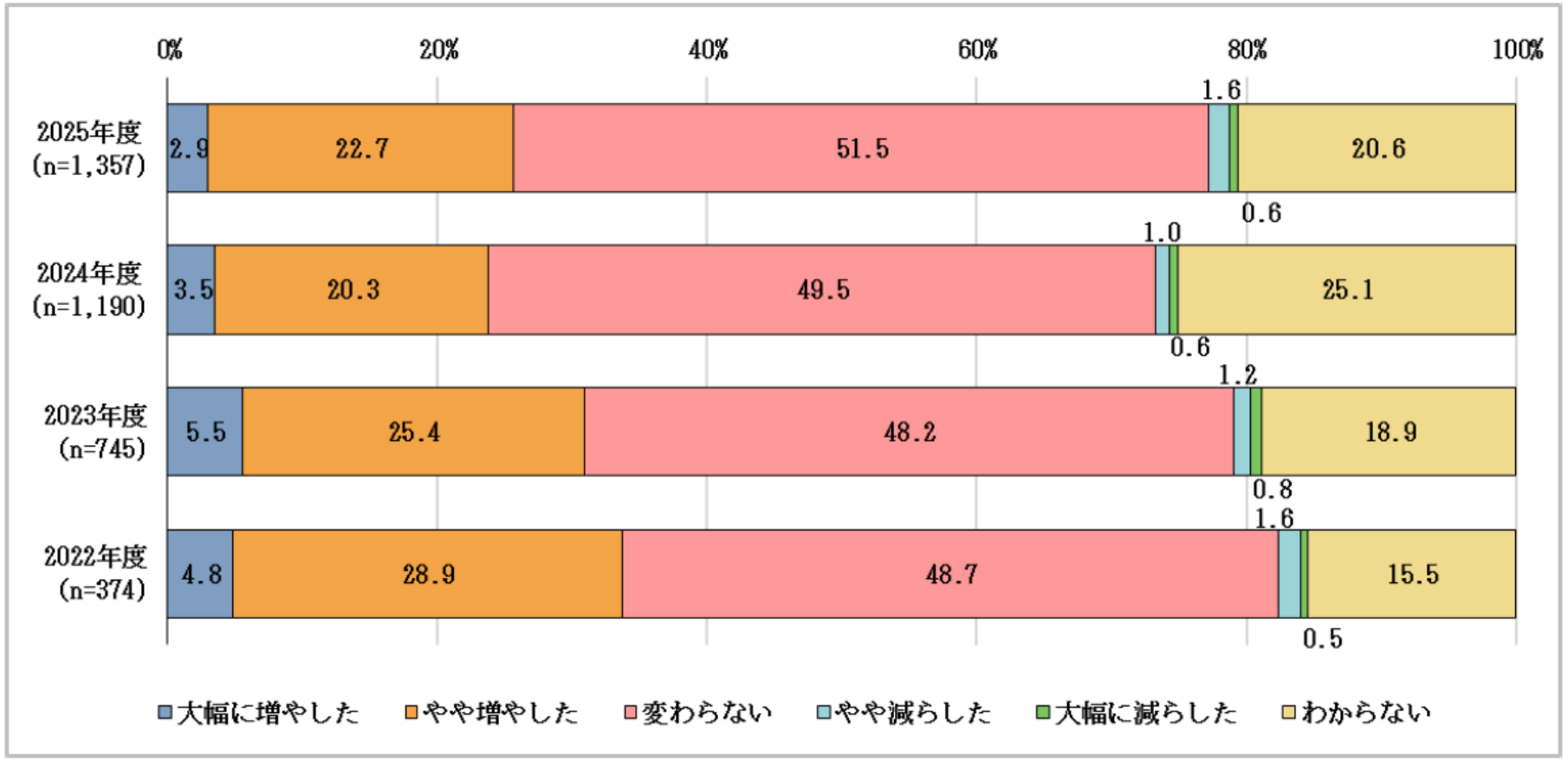
DX推進に必要なスキルの把握状況（経年比較）



※DX動向2026,IPA

DX推進人材の育成予算規模はあまり変わっていない

DXを推進する人材を育成する予算の増減（経年比較）



※DX動向2026,IPA

デジタル関連職種は求められるスキル変化が激しい

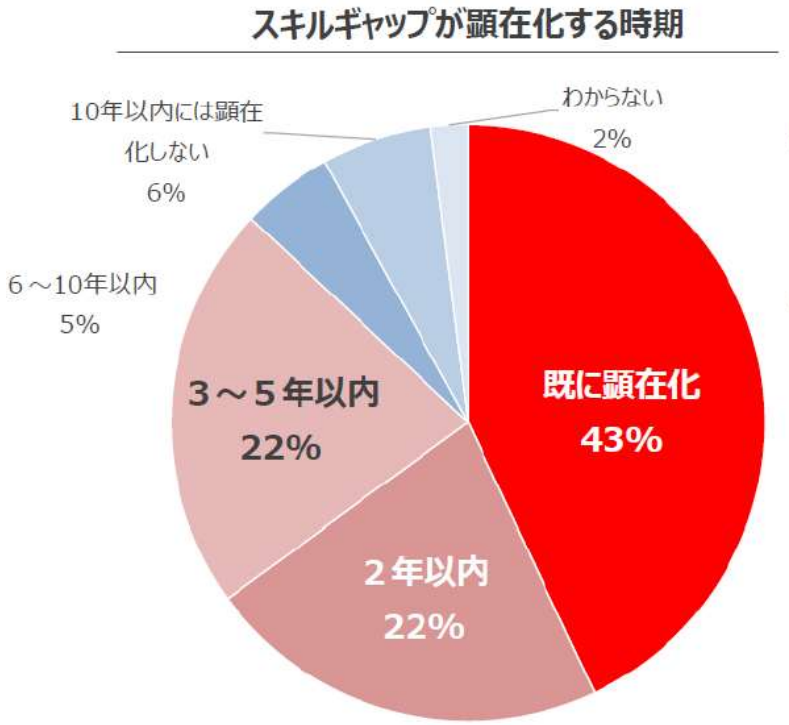


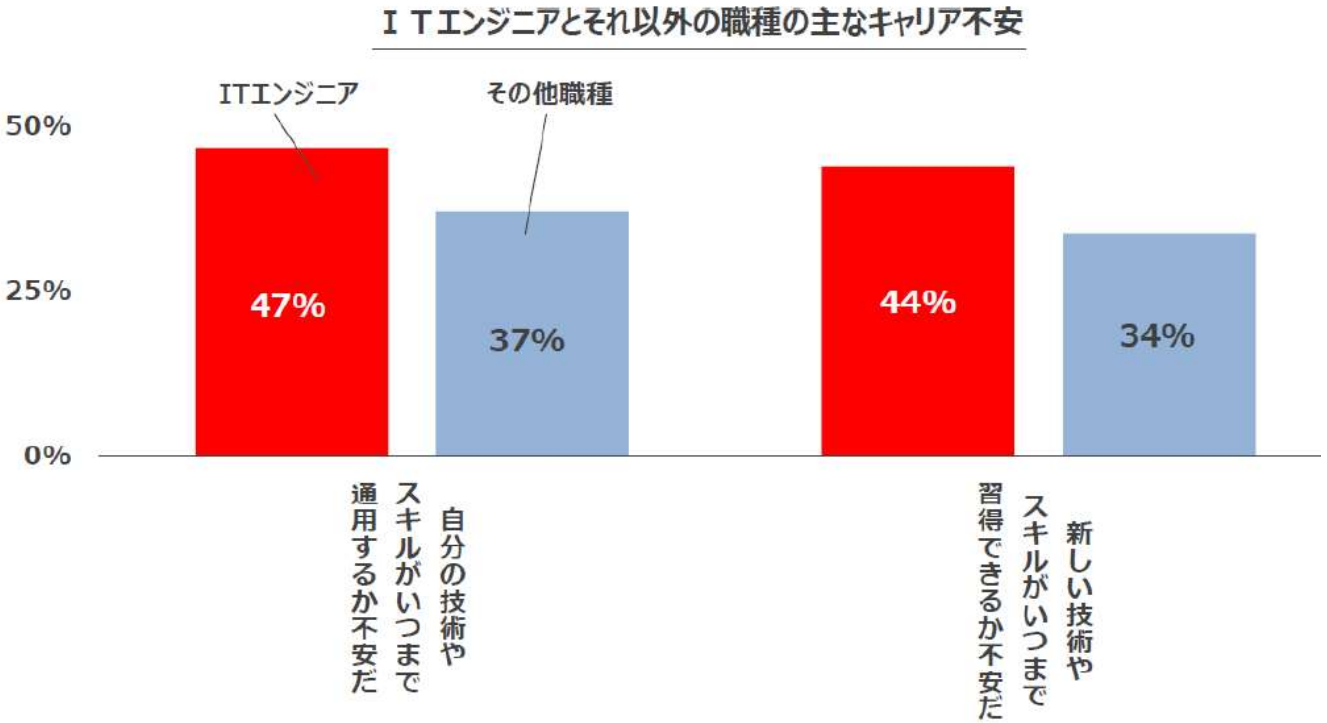
注：2017 年から 2022 年の間の同一職業内のスキル構成の変化率を標準化し、0～100 に指数変換した指標。
有効な求人票数が 100 に満たない職業は分析対象から除外している。
出所： Lightcast ジョブポスティング・データより三菱総合研究所作成

※「Society 5.0時代のデジタル人材育成に関する検討会」資料（経済産業省,2024）

ITエンジニアはスキル陳腐化への不安を抱えている

- ４割以上の企業は、「技術革新により必要となるスキル」と、「現在の従業員のスキル」との間のギャップを認識している。
- 半数近くのITエンジニアが「技術やスキルの陳腐化に不安」を抱えている。





※「未来人材ビジョン」（経済産業省,2022）

デジタルスキル標準(DSS)の改訂

デジタルスキル標準（DSS） （2022年12月策定、2026年4月Ver.2.0公表）

- 企業がDX（ビジネスモデルの変革等による企業価値向上）を実現するために、「全員がDX推進を自分事ととらえ」、変革の受容性を高めることが重要。加えて、 DXに関する専門性（テクノロジー・ビジネス変革）を持ち、変革を推進する人材の確保・育成が必要。
- 個人の学習及び企業の人材確保・育成の指針として策定。

全てのビジネスパーソン（経営層含む）

<DXリテラシー標準>

全てのビジネスパーソンが身につけるべき知識・スキルを定義

- ビジネスパーソン一人ひとりがDXに参画し、その成果を仕事や生活で役立てる上で必要となるマインド・スタンスや知識・スキル（Why、What、How）を定義し、行動や学習項目の例を提示

Why
DXの背景
社会、顧客・ユーザー、競争環境の変化

What
DXで活用されるデータ・技術
ビジネスの場で活用されているデータやデジタル技術

How
データ・技術の利活用
データやデジタル技術の利用方法、活用事例、留意点

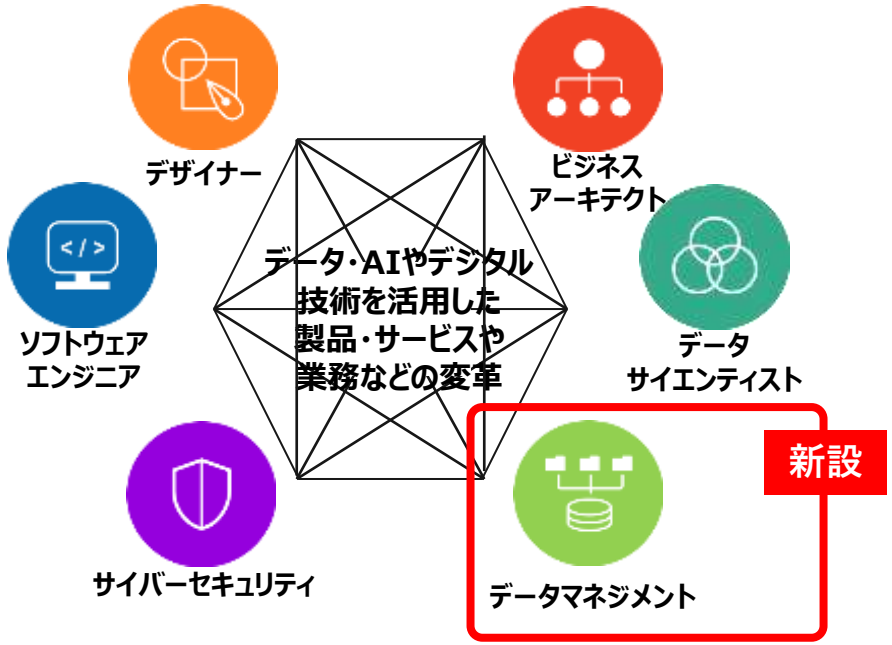
マインド・スタンス
不確実性の高い時代において、新たな価値を生み出すために必要な意識・姿勢・行動をデザインの素養に基づいて定義

DXを推進する人材

<DX推進スキル標準>

DXの推進に必要な役割の類型や習得すべきスキルを定義

- DX推進に主に必要な６つの類型、ロール、必要なスキルを定義し、各スキルの学習項目例を提示



DSS改訂のポイント

- DXの実現に不可欠なテクノロジーとしてAI活用が進む。AI・データ活用を推進するため、事業や業務プロセスにおいて生じるデータを、**ビジネス上の様々な目的に対し、データの安全性と信頼性を確保し活用する仕組みの構築**が重要。高品質なデータ精製によるAI-Ready化を促し、 AI活用により創出される価値の向上につながる。
- 企業のDX推進が進む中で、個別事業やプロジェクトの効率化や高度化だけでなく、**ビジネス変革や組織変革のスキル**の重要性が増している。
- 求められる役割及びスキルの変化に合わせデジタルスキル標準を改訂する。

①データマネジメント類型の追加

安全性と信頼性を確保しデータ活用を推進するため

- データを収集・提供する仕組みの構築を主導し、組織内にデータによる価値創出を促進させる**データマネジメント類型**を追加
- 事業部門と特に連携して、データの信頼性を向上させる**データスチュワード**、データを効果的に流通させる仕組みや運用プロセスを設計する**データアーキテクト**、データ整備等を担う**データエンジニア**の３つのロールに区分
- 各ロールにおいて重要なスキルを見直し

②AIの進展に伴うスキル項目の拡充

AIの進展に伴い、多くのロールがAIを活用するため

- 共通スキルリストに、AIの実装やその運用において求められるスキルとして、**AI実装・運用**を追加
- **AIガバナンス**について、スキルや学習項目として拡充

③ビジネス変革に関するロールやスキル項目の見直し

ビジネス変革や組織変革領域について

- 経営戦略を理解し、実装する事業部門やIT部門をつなぐビジネスアーキテクトのロールを、**ビジネスアーキテクト、ビジネスアナリスト、プロダクトマネージャー**の３つに見直し
- ビジネスアーキテクトのロール見直しに伴うスキルを拡充
- 様々な関係者の連携や共創を、デザインの素養を基に促す**デザインマネジメント実践**に関するスキルを追加

④その他必要な見直し

デザイナーの活躍する領域を見直し、企業及びプロジェクトのブランドメッセージやコンテンツ制作に反映するコミュニケーション領域におけるロールを、**コミュニケーションデザイナー**として定義

（出典）経済産業省「第7回Society 5.0時代のデジタル人材育成に関する検討会（R8.4.13）」資料を加工

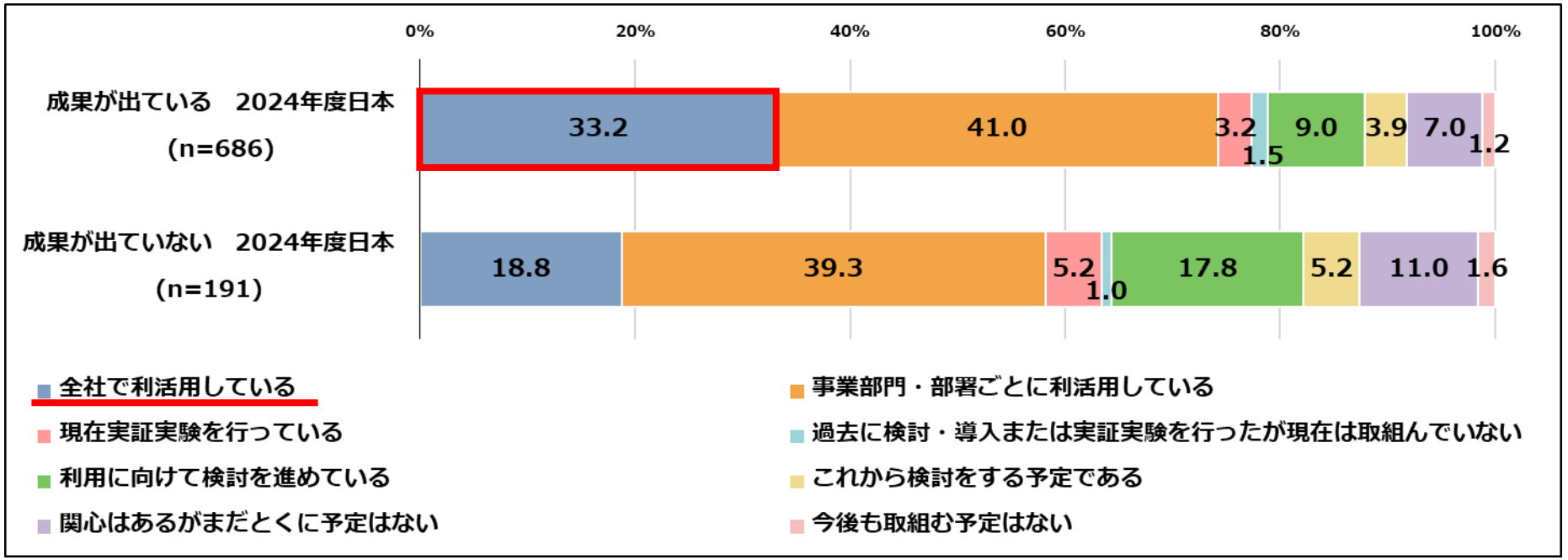
DX推進スキル標準｜ロール一覧

類型	ロール	担うべき責務
ビジネスアーキテクト	ビジネスアーキテクト	組織や事業を俯瞰する立場から、経営戦略を全体最適の事業構造に落とし込み、これを実現する変革のロードマップ（プロダクト/プログラムポートフォリオ）を立案する。また、これに関する経営者の投資判断/意思決定の支援を行う
	ビジネスアナリスト	プロダクト/プログラムにおける業務・組織・システムの分析を担い、要求の整理と実装担当者（エンジニア）への伝達を行う。また、取組関係者のコミュニケーションハブとなり、利害調整を行う
	プロダクトマネージャー	特定のプロダクト（製品・サービス）の責任者として企画から構築、その後の継続的改善やビジネスの拡大などライフサイクルでチームの運営を担う。また、明確な成果責任を持つ
デザイナー	サービスデザイナー	社会、顧客・ユーザー、製品・サービス提供における社内外関係者の課題や行動から顧客価値を定義し製品・サービスの方針（コンセプト）を策定するとともに、それを継続的に実現するための仕組みのデザインを行う
	UX/UIデザイナー	バリュープロポジションに基づき製品・サービスの顧客・ユーザー体験を設計し、製品・サービスの情報設計や、機能、情報の配置、外観、動的要素のデザインを行う
	コミュニケーションデザイナー	ステークホルダーやユーザーとのタッチポイントを横断し、ブランド理念とビジョンを言語化。一貫したメッセージングとビジュアル・コンテンツで製品・サービスの意義や使い方を正しく伝える体験を設計する。制作から運用まで統括し、顧客データやフィードバックを活用してコミュニケーション施策を継続的に最適化する
データサイエンティスト	データビジネスストラテジスト	事業戦略に沿ったデータ・AIの活用戦略を考えるとともに、戦略の具体化や実現を主導し、顧客価値を拡大する業務変革やビジネス創出を実現する
	データサイエンスプロフェッショナル	データの処理や解析を通じて、顧客価値を拡大する業務の変革やビジネスの創出につながる有意義な知見を導出する
データマネジメント	データスチュワード	事業ドメイン知識に基づき、データの品質・信頼性・安全性の確保に向けた運用を担うとともに、事業部門・現場組織におけるデータマネジメントの浸透・定着、およびデータ利活用の促進を担う役割
	データエンジニア	データの現状を把握し、収集・統合・加工・提供などの各プロセスにおけるデータ整備、前処理の実施、データパイプラインの設計・実装を通じて、組織全体の継続的なデータ利活用を支える役割を担う
	データアーキテクト	組織・事業全体のデータ構造や流れ、利活用のあり方を俯瞰し、事業戦略に沿ってデータライフサイクル全般を見据えたデータアーキテクチャを設計・継続的な見直しを行うことで、全社横断的なデータ利活用とガバナンスの両立を実現する役割を担う
ソフトウェアエンジニア	フロントエンドエンジニア	デジタル技術を活用したサービスを提供するためのソフトウェアの機能のうち、主にインターフェース（クライアントサイド）の機能の実現に主たる責任を持つ
	バックエンドエンジニア	デジタル技術を活用したサービスを提供するためのソフトウェアの機能のうち、主にサーバサイドの機能の実現に主たる責任を持つ
	クラウドエンジニア/SRE	デジタル技術を活用したサービスを提供するためのソフトウェアの開発・運用環境の最適化と信頼性の向上に責任を持つ
	フィジカルコンピューティングエンジニア	デジタル技術を活用したサービスを提供するためのソフトウェアの実現において、現実世界（物理領域）のデジタル化を担い、デバイスを含めたソフトウェア機能の実現に責任を持つ
サイバーセキュリティ	サイバーセキュリティマネージャー	顧客価値を拡大するビジネスの企画立案に際して、デジタル活用に伴うサイバーセキュリティリスクを検討・評価するとともに、その影響を抑制するための対策の管理・統制の主導を通じて、顧客価値の高いビジネスへの信頼感向上に貢献する
	サイバーセキュリティエンジニア	事業実施に伴うデジタル活用関連のサイバーセキュリティリスクを抑制するための対策の導入・保守・運用を通じて、顧客価値の高いビジネスの安定的な提供に貢献する

（出典）IPA「デジタルスキル標準ver.2.0」を加工

データ利活用の状況（DX成果別・国内）

- DXの成果が出ている企業では「全社で利活用している」と回答した企業の割合が高い。



（出典）IPA「DX動向2025（データ集）」を加工

データを正しく安全に活用するためデータマネジメントが不可欠

- データ・AI活用の推進に向けて、データのAI活用を進めていくにあたり、まずは企業内に散らばるデータの探索、収集、抽出等を担い、正しく安全なデータの管理・活用を推進するデータマネジメントが不可欠。
- 組織全体でデータ・AIを使いこなすためには、加えて、AIが理解しやすい高品質データとするため、データを意味・関係性付けするデータ精製等のAI-Ready化が必要。

データマネジメントの取組
- データの品質（信頼性等）の確保と改善
- 活用目的に応じたデータ及び活用ルールの設計
- 収集から整備・管理までの組織内のデータの流れを仕組化（設計・基盤）等

AI-Ready化
- データの意味・関係付けを行うメタデータの充実化
- AI学習できる高品質で多様なデータ精製の実現　等

不十分なデータ活用
- 組織内でデータが散在、把握できていない
- 必要だがデータ化されていないアナログ情報がある
- データ活用ルールが未整備

データを正しく安全に活用
- データ収集・整備・管理の仕組みを構築（製造工程の管理）
- データ安全性と信頼性が確保され、運用改善している

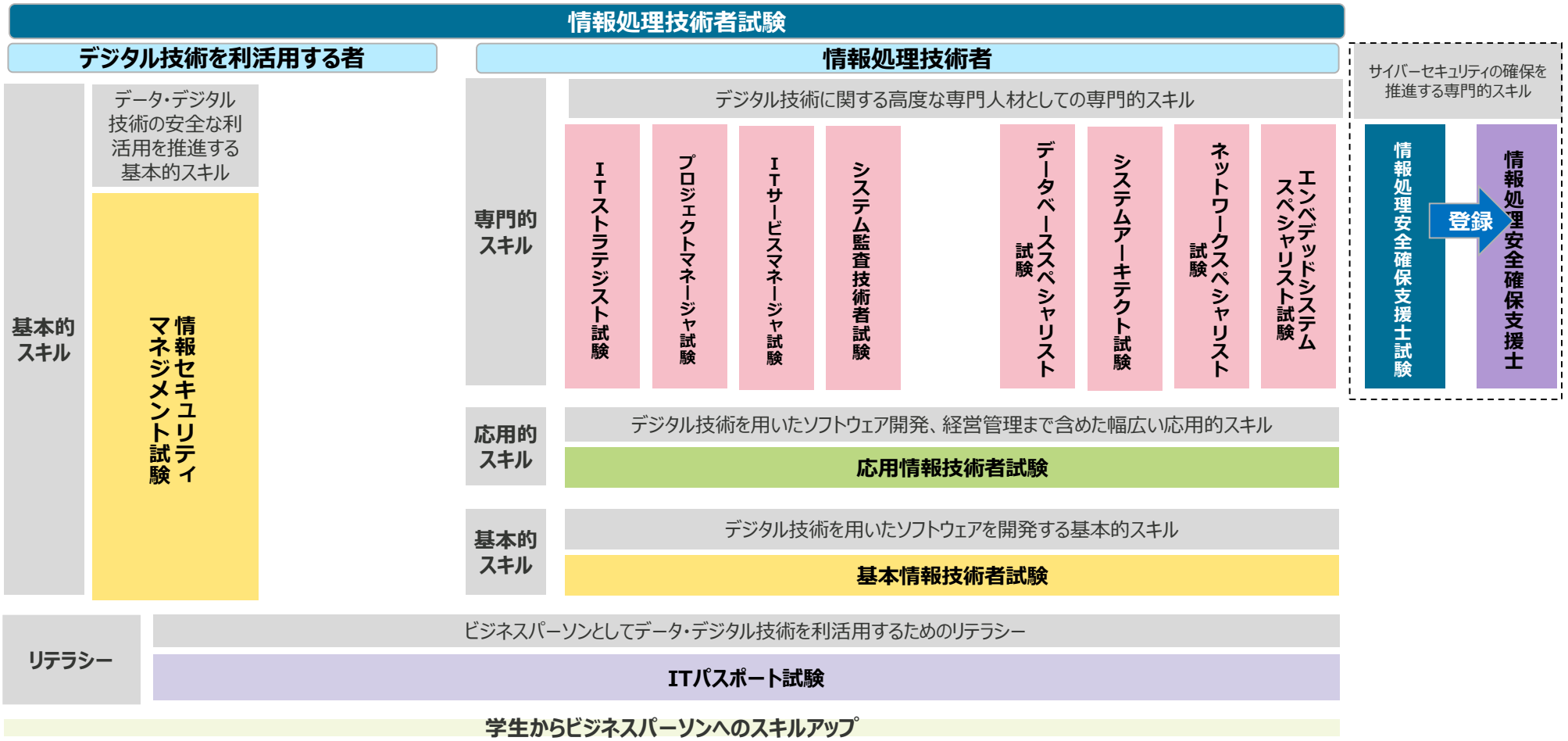
データ・AIを高度に活用
- 組織全体で使いこなす
- データを学習したAIモデルを活用した意思決定
- 資産として企業間取引

（出典）経済産業省「第7回Society 5.0時代のデジタル人材育成に関する検討会（R8.4.13）」資料を加工

情報処理技術者試験の見直し

現行の情報処理技術者試験・情報処理安全確保士試験

- **「情報処理の促進に関する法律」**に基づき、デジタル人材の能力が一定以上の水準であることを認定する**国家試験。国内最大級の国家試験、**2025年度は**年77万人応募、合格者25.5万人。**
- 情報システムを構築・運用する「技術者」から、利用する「エンドユーザー」まで、**幅広いデジタル人材を対象**に、**デジタル技術に関する知識・技能を客観的に評価し、人材育成・確保に貢献**。



情報処理技術者試験の見直し概要（検討案）

データマネジメント試験（仮称） 新設

ＡＩ を活用するためには、**データを活用可能な状態に整備・管理する必要**があり、このスキルを習得し、評価するための**新たな試験を創設**。

ITパスポート試験 最適化

全ての人が変化を敏感に捉えられるように**DXのマインド・スタンス、データマネジメントの基礎に関する出題追加、AI時代に対応した倫理の出題強化**など。

応用情報技術者試験・高度試験※1 再編

ＤＸやＡＩ利活用を進める観点から、「根幹」となる幅広いスキルを身につけることで、ＡＩも活用して新たな価値創造を行う人の目標となるように、**応用情報技術者試験と高度試験**を大括り化し、**マネジメント、データ・ＡＩ、システムの3領域、３試験※2に再編。３領域の習得を推奨**。

試験実施方法 変更

2026年度から、ペーパー方式である応用情報技術者試験・高度試験をＣＢＴ方式※3に移行し、全試験区分をＣＢＴ方式で受験可能に※4。2027年度の**見直し後の試験**では、記述式・論述式を**CBT方式に適した出題形式へ見直し**。

論述試験のあり方は、2028年度以降に向けて**継続検討**。

※1 高度試験：ITストラテジスト試験、システムアーキテクト試験、プロジェクトマネージャ試験、ネットワークスペシャリスト試験、データベーススペシャリスト試験、エンベデッドシステムスペシャリスト試験、ITサービスマネージャ試験、システム監査技術者試験

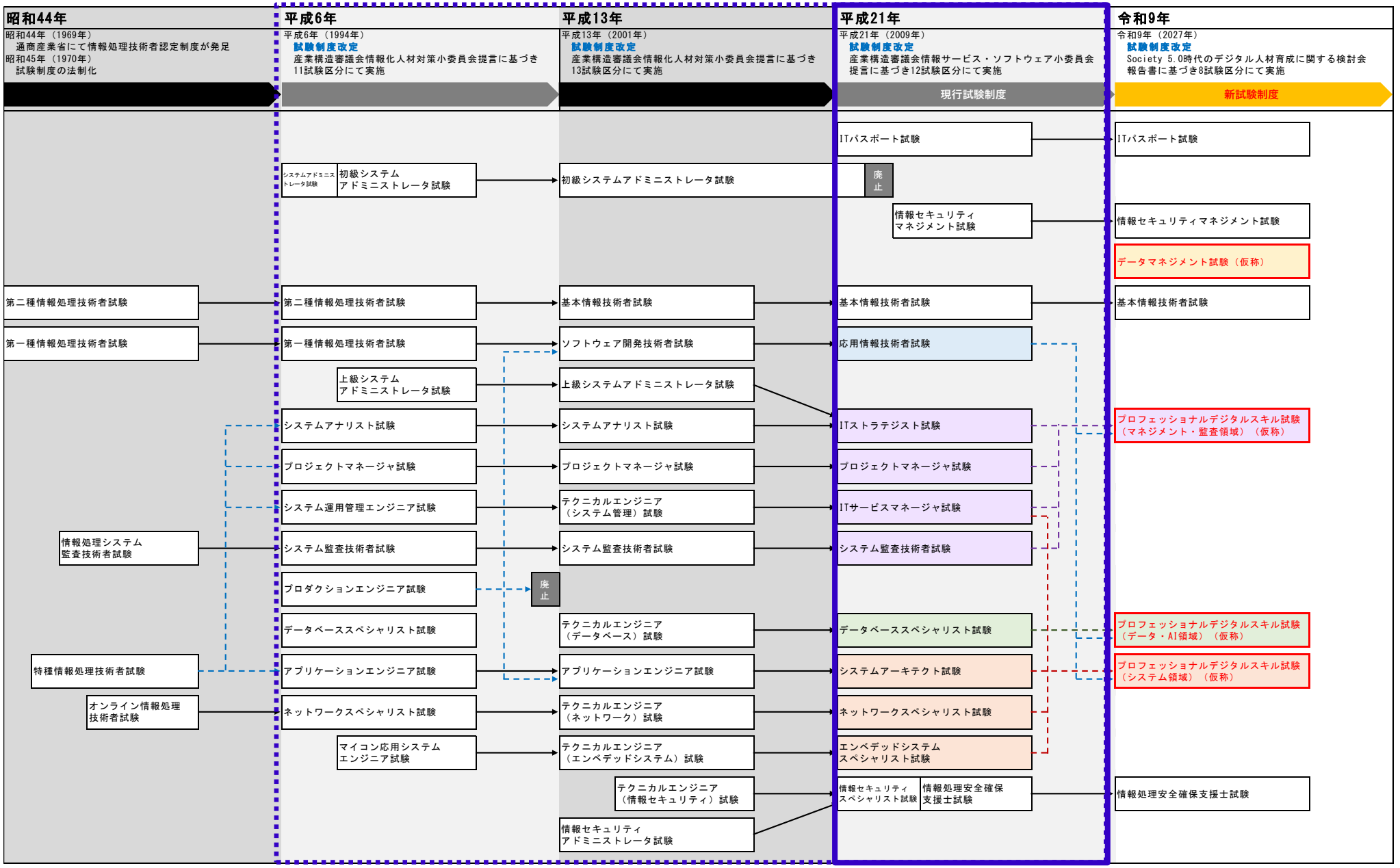
※2 ３試験の総称は「プロフェッショナルデジタルスキル試験（仮称）」

※3 Computer Based Testing：コンピュータを利用した試験方式

※4 情報処理安全確保支援士試験についても2026年度よりCBT方式に移行。2027年度には、同様に、CBT方式に適した出題形式へ見直し。

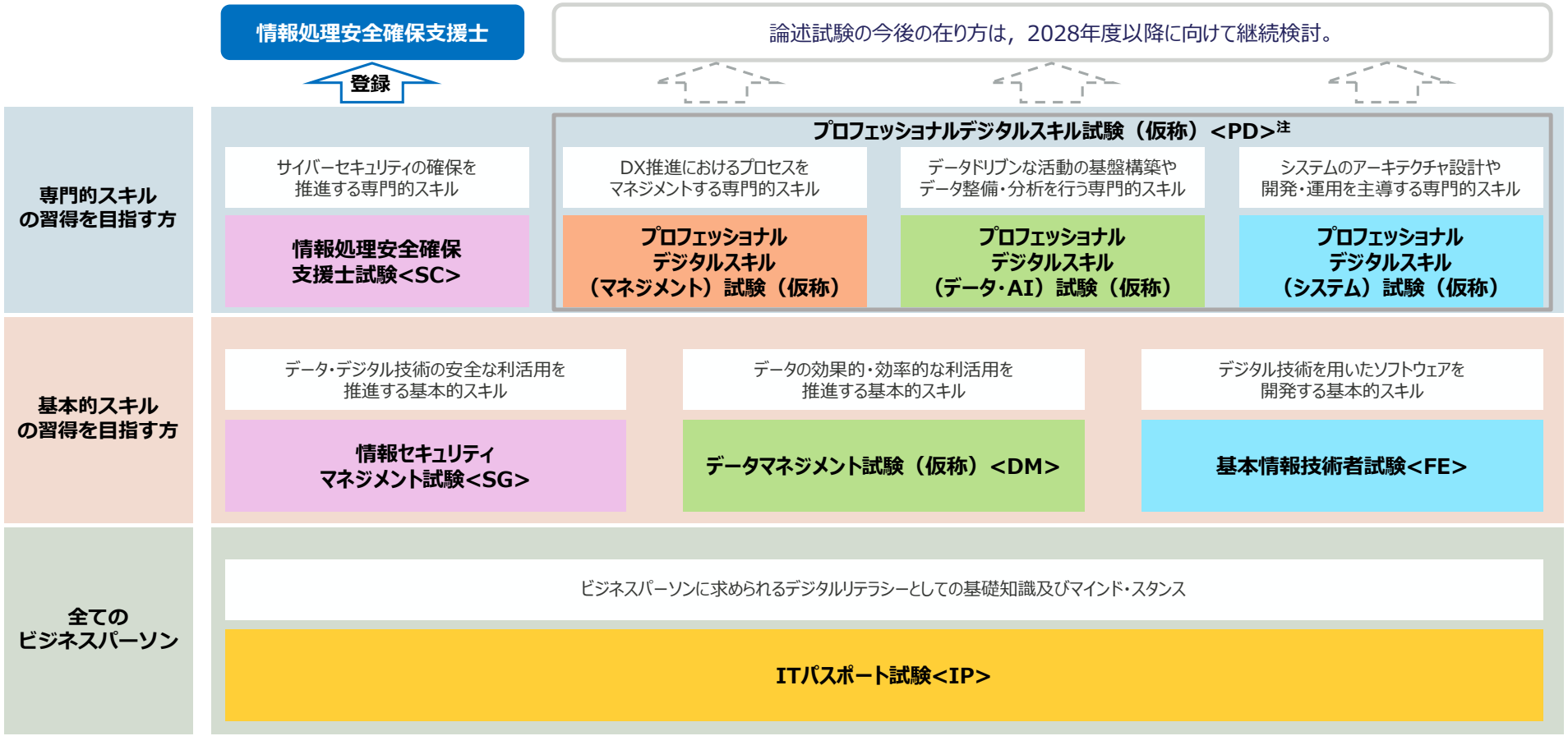
（出典）経済産業省「第7回Society 5.0時代のデジタル人材育成に関する検討会（R8.4.13）」資料を加工

（参考）試験制度の変遷（昭和44年～新試験制度案）



見直し後の試験区分体系図（イメージ）

＜ＡＩ時代に必要となるデジタルスキルを習得・評価する試験へ＞



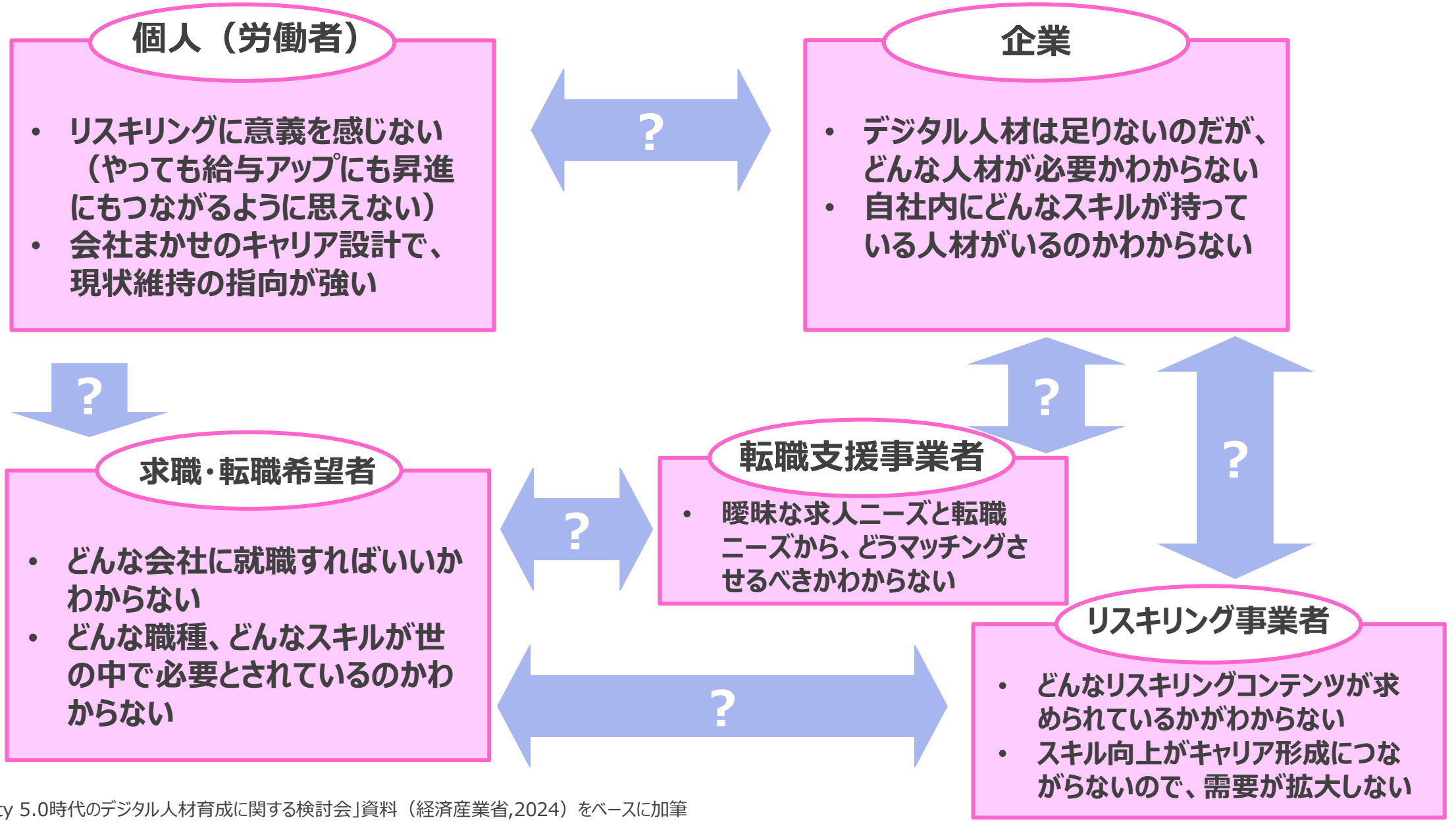
注：PDの科目A-1において基準点以上の成績を達成することでデジタル証明の発行を検討。
　　また、PDの3試験全てに合格することで「AI時代におけるフルスタックスキル」のデジタル証明の発行を検討。

＜論述試験＞

- 例えば、経営者への説明の観点から、デジタル技術の社内適用・ガバナンス体制の構築について、受験者の業務経験も踏まえて論述する内容とするなど、そのあり方も含めて、2028年度以降に向けて継続検討。
- プロエッショナルデジタルスキル試験のうち、１つの試験又は全ての試験に合格することを受験条件にすることを想定。

デジタル人材スキルプラットフォーム

日本の労働市場の課題は「不明瞭」であること



※「Society 5.0時代のデジタル人材育成に関する検討会」資料（経済産業省,2024）をベースに加筆

「スキル」を共通言語にする

個人（人材）

“Skill Based Learning”

- 「目指すキャリア実現のために必要となるスキル」に直結した学びが可能になる
- 個人が主体となったキャリア設計ができる
- スキルに見合った評価・待遇が受けられることで、学びへのモチベーションがさらに向上する

スキルの共通言語化

スキルデータの社会全体としての蓄積

企業

“Skill Based hiring”

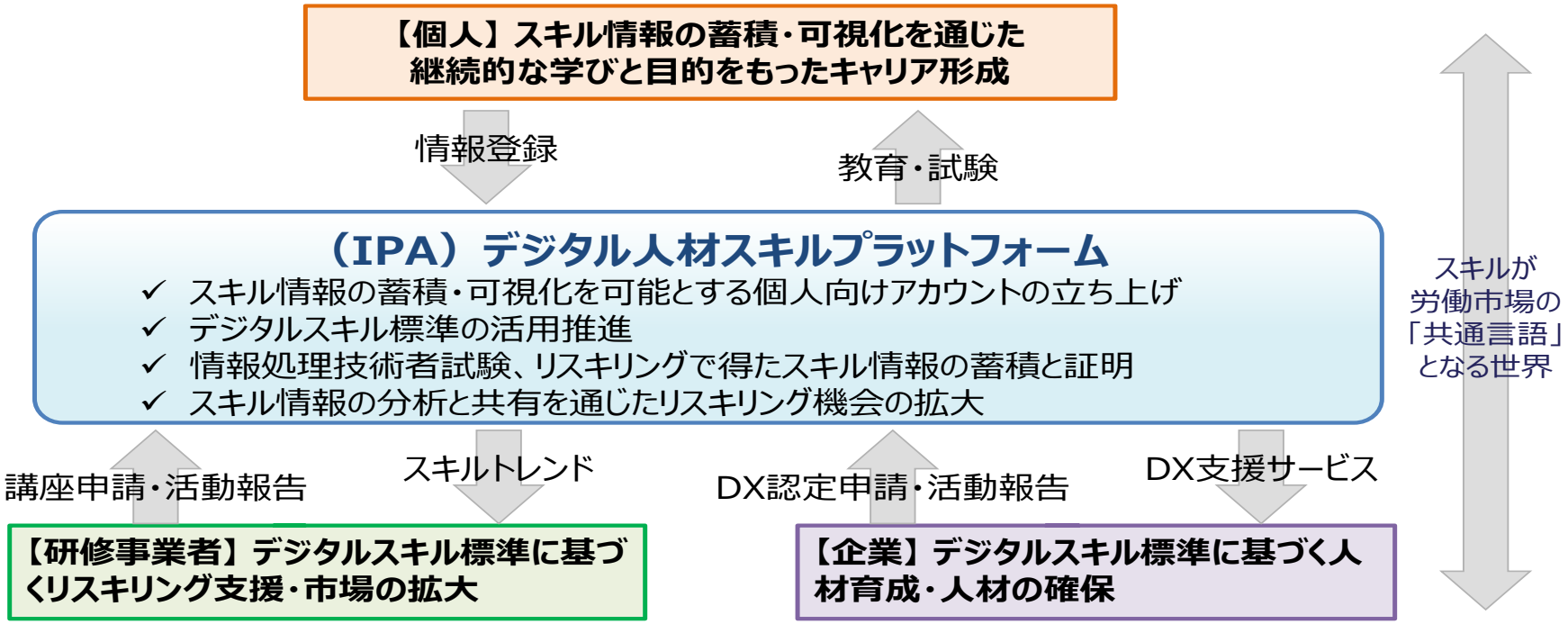
- 「事業推進上、必要になるスキル」に直結した採用が可能になる
- 自社の人材が保有しているスキルを把握し、適正に評価できるようになる
- 必要となるスキルを内部人材に取得させることができるようになる

- 社会全体として環境変化に応じた最適な人材配置（適材適所）が可能になる
- 社会全体として現在足りていないスキル、さらには今後必要となるスキルが可視化される

デジタル人材スキルプラットフォームの構築

- 個人のデジタルスキル情報の蓄積・可視化により、デジタル技術の継続的な学びを実現するとともに、スキル情報を広く労働市場で活用するための仕組みとしてIPAにおいて、「デジタル人材スキルプラットフォーム」の構築に向け、システム開発を進めている。

■イメージ



■提供価値

①スキル情報の蓄積・可視化	②動的なスキル把握
③スキル情報のビッグデータ化	④ともに学び合うコミュニティ形成

産業横断の人材・スキル情報のデジタルプラットフォーム

- AX時代を見据え、戦略分野等における人材育成を加速するにはスキル情報の一体提供が重要。
- 関係省庁の連携の下、**人材、スキル情報を一体的に提供する横断的なデジタル基盤を構築。**

デジタル人材スキルプラットフォーム（仮称）

デジタル庁、厚生労働省、文部科学省、経済産業省の連携の下、独立行政法人IPAが構築。
2027年春頃から順次サービスを開始していく。

公的なスキルタクソノミーと、マイナンバーと連携した個人のスキルIDによる関連情報の一体提供

スキル可視化

1. **各職種に求められるスキル**
   職種毎の詳細スキル定義
   分野・職種間の共通スキル
   関連する資格情報
2. **個人のスキル証明/ギャップ**
   保有スキルと希望職種の差
3. **スキルトレンド、動的更新**
   最新の必要スキルの収集分析

リスキリング

1. **各スキルを取得できる講座**
   大学、高専、工業高校
   専修学校、職業訓練校
   民間講座　等
2. **受講を推奨する講座例**
   希望に合致する講座候補
3. **公的支援の情報**
   教育訓練給付の対象講座

マッチング

1. **各スキルの需要、処遇**
   職種・スキル毎の求人動向
   職種・スキルと賃金の関係
2. **スキルに紐付いた求人情報**
   HWの具体的な求人情報
3. **スキル需給の足下将来動向**
   全国/地域のスキル需給分析

他の公的DBとの情報連携（例）

- 職業情報：**jobtag**
- 講座情報：**マナパス、まなびDX 教育訓練講座検索システム**
- 雇用情報：**ハローワーク**

民間サービスへの活用（例）

- **人材関連企業**
  スキル情報による求人、転職サービス
- **教育機関・講座提供事業者**
  スキル需要を踏まえた講座の提供
- **産業界、企業**
  必要な人材の採用・育成計画への活用

※「経済産業省の17戦略分野等におけるリ・スキリング・人材確保の主な支援策」（戦略分野・社会インフラ関連分野の人材育成・確保を推進するための関係府省庁連絡会議（第１回：内閣官房）,2026.6.16）

まとめ

まとめ

- 急速な進化を見せるAIを、経営に積極的に導入し変革を行う企業と、そうでない企業との格差は、今後想像以上に大きくなっていく
  - ✓ 中小企業は既に、二極化し始めている
- DX・AXを確実に推進していくためにも「DX認定」を取得し、十分な準備ができている企業であることを内外ともに示すところからスタートすべき
- サイバー攻撃が、企業経営にとって大きな脅威になっていることを経営者自らが自覚し、「SCS評価制度」「ランサムウェア教訓集」等を活用し、サイバーセキュリティに関するリスクを最小化すべき
- 企業に必要なDX推進人材を迅速に育成・確保するために、「デジタルスキル標準」「情報処理技術者試験」「デジタルスキルプラットフォーム」を積極的に活用するべき

Thanks for your attention !