2026年度第８回
SICフォーラム

AI時代のDX戦略

2026.10.29

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)

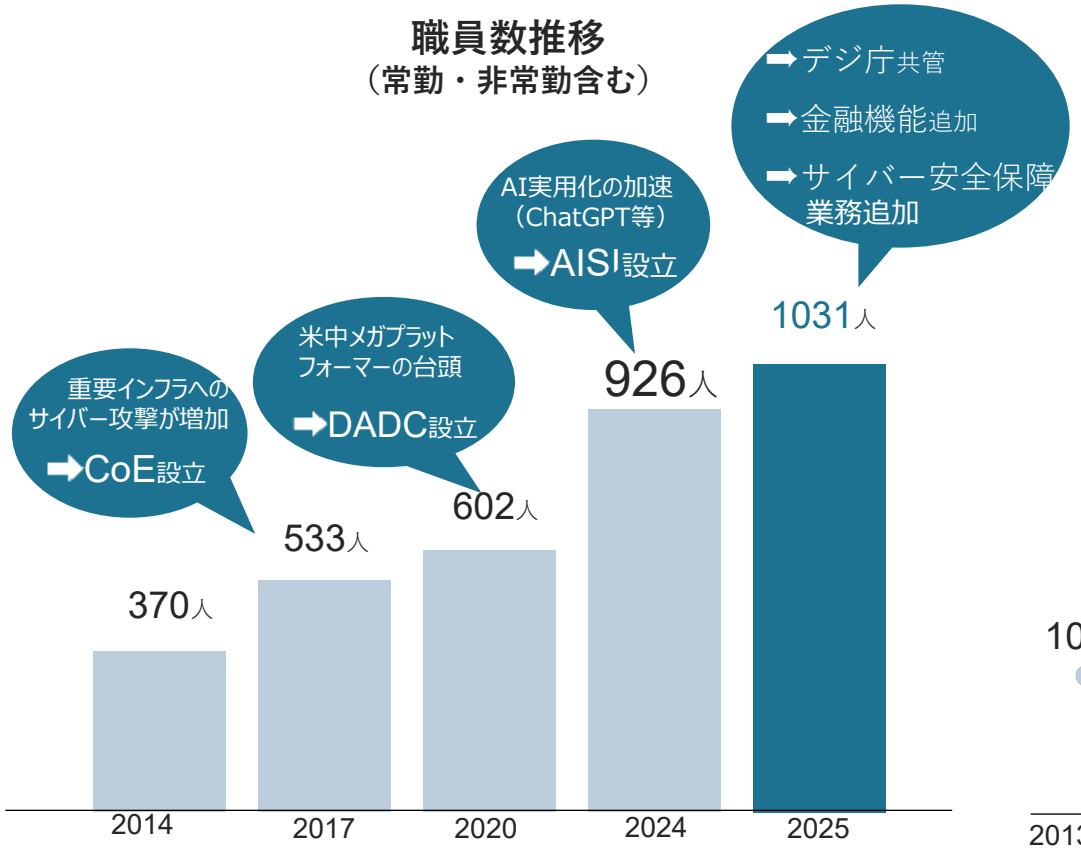
株式会社NTTデータ経営研究所において、執行役員として企業や行政機関におけるデジタル戦略立案に関連するコンサルティングを実施。経済産業省等においてDX推進、デジタル人材育成等に関する検討会座長を務める。2026年から情報処理推進機構 理事に就任。現職では、日本社会の国際競争力向上に向けて様々なデジタル政策の推進に取り組んでいる

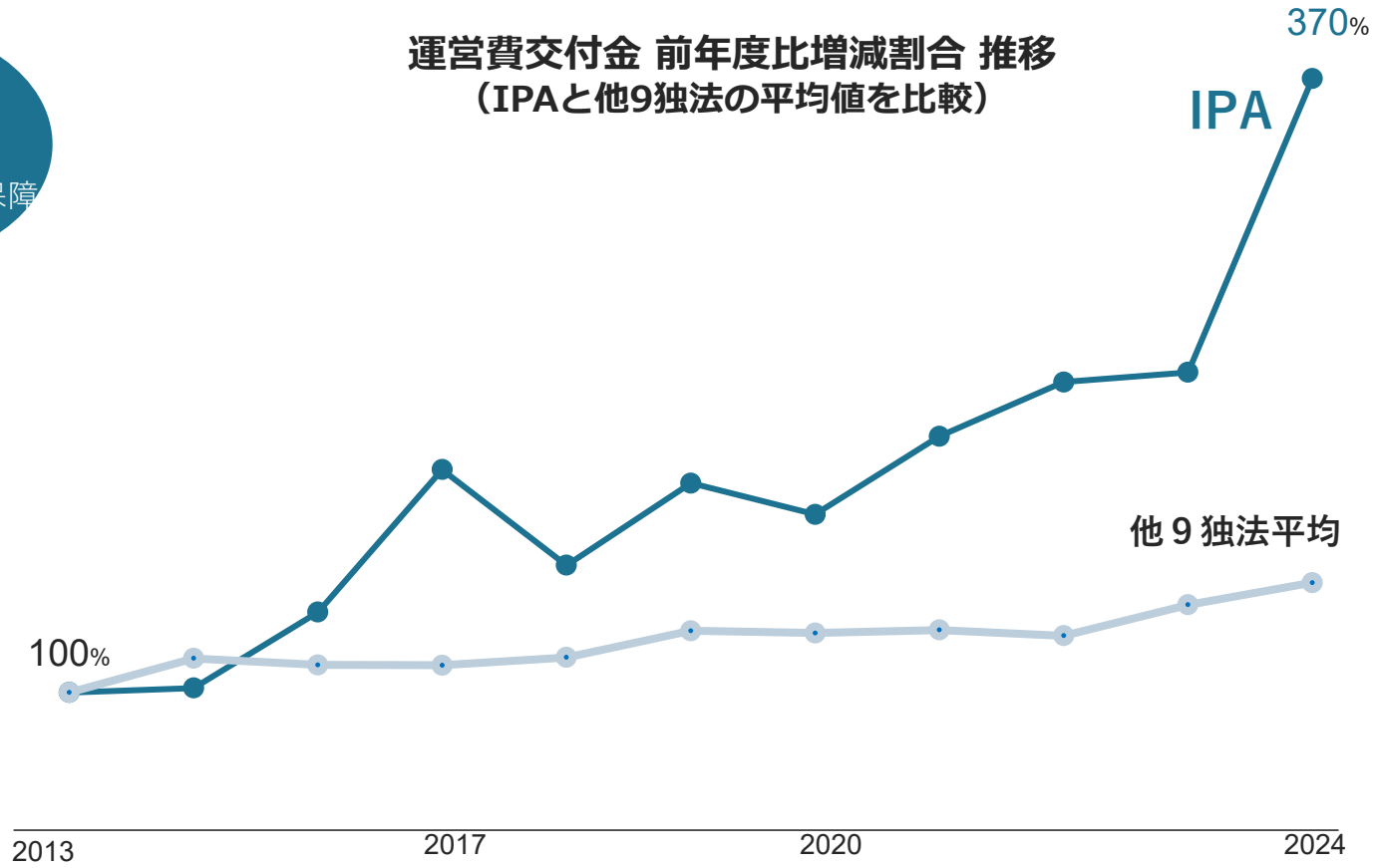
武蔵野大学国際総合研究所客員教授。東京農工大学非常勤講師、富山大学非常勤講師、山口大学非常勤講師。情報社会学会理事

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



独立行政法人

情報処理推進機構

Innovation Platform Agency, Japan

Beyond Digital

内容

- AIの台頭
- DX・AXの現状
- デジタルガバナンスコード（DXセレクション・DX銘柄）
- サイバーセキュリティの確保
- DX推進人材の育成・確保
- まとめ

AIの台頭

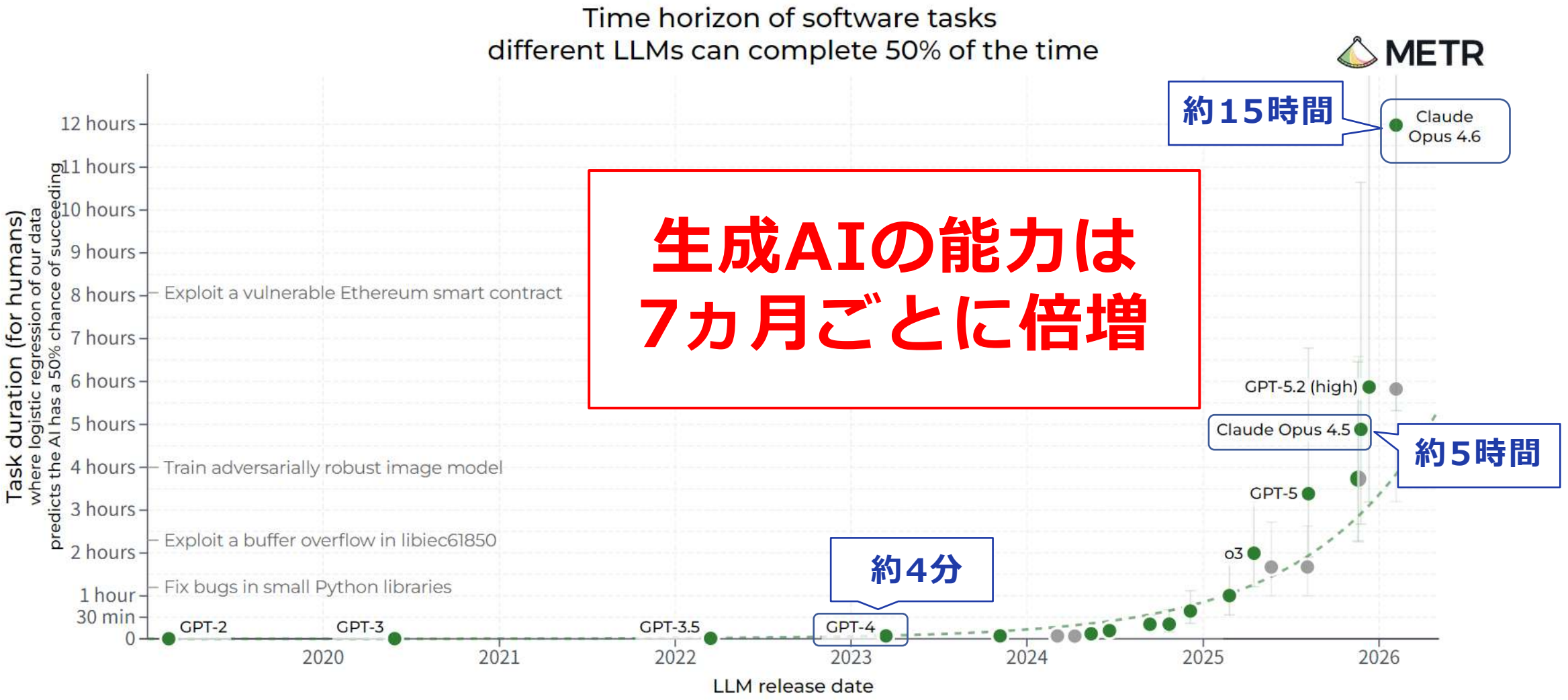
生成AIによる経済効果



- 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）

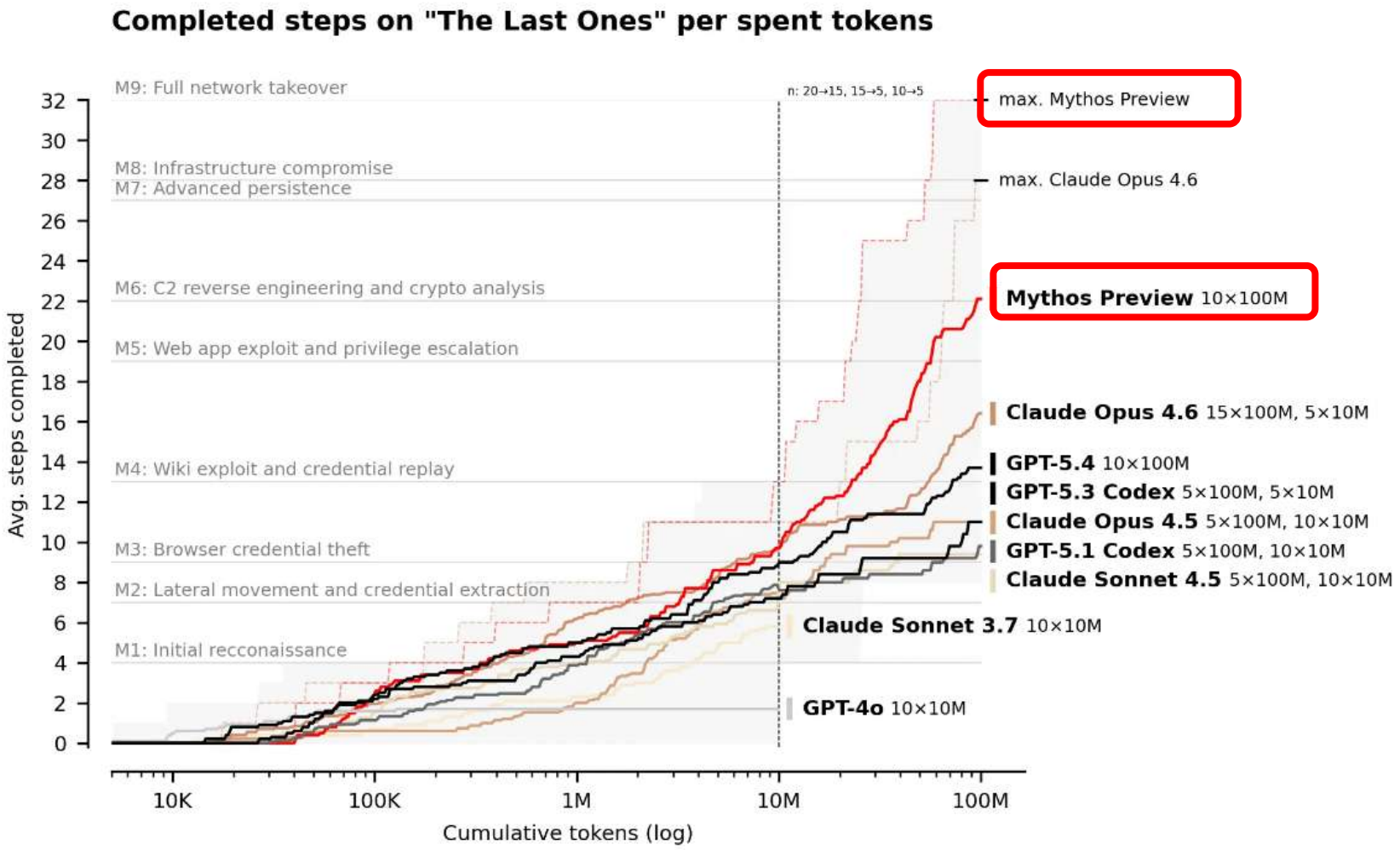
AIの能力向上は想像を超えている



生成AIの能力は
7ヵ月ごとに倍増

※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」

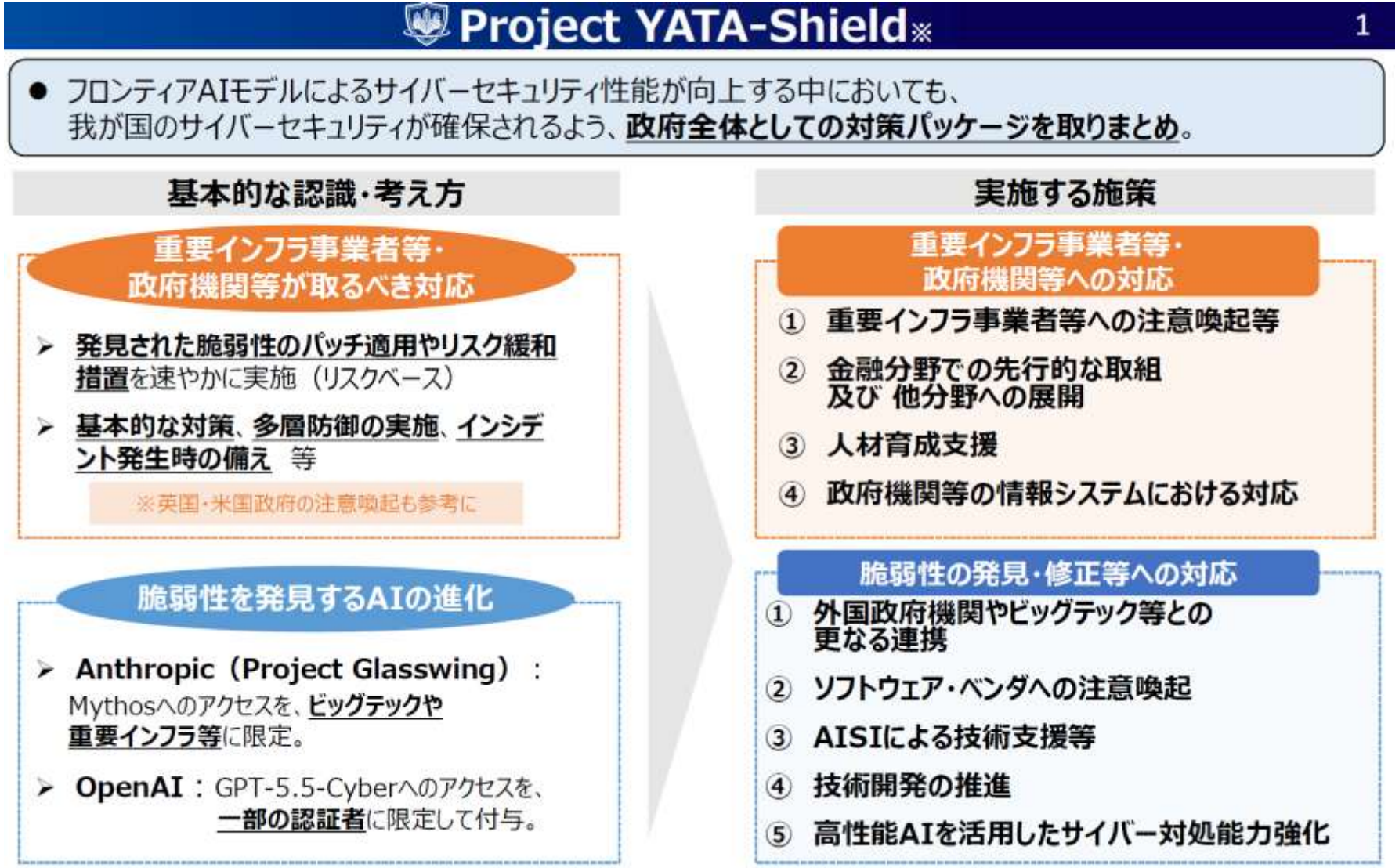
“フロンティアAI” Claude Mythosの衝撃



- **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)

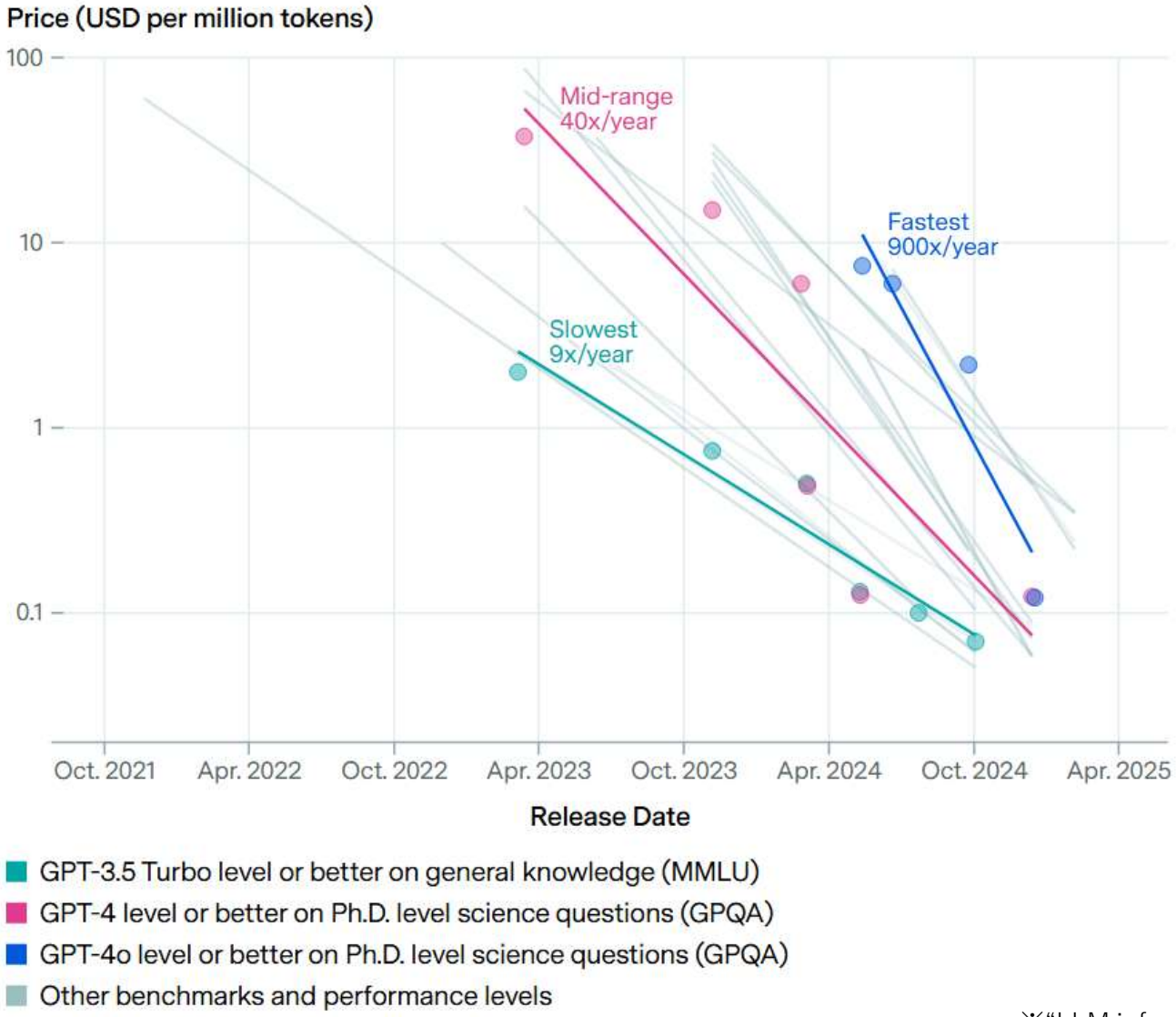
（参考）対策パッケージ「Project YATA-Shield」



- 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）

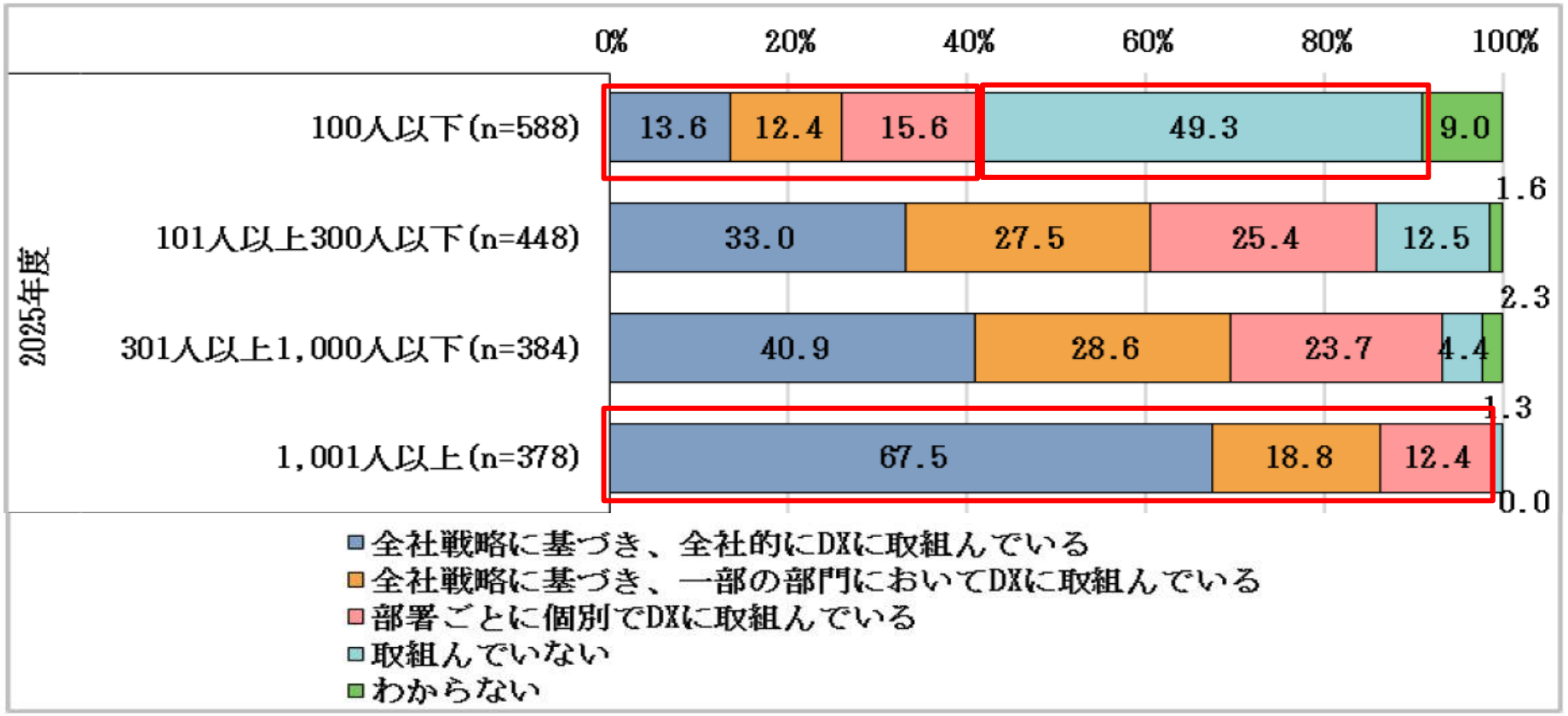
- AIに代表されるデジタル技術は、大きなポテンシャルを持ち始めている
- さらに、デジタル技術は、誰の手にでも扱えるようになってきている

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）

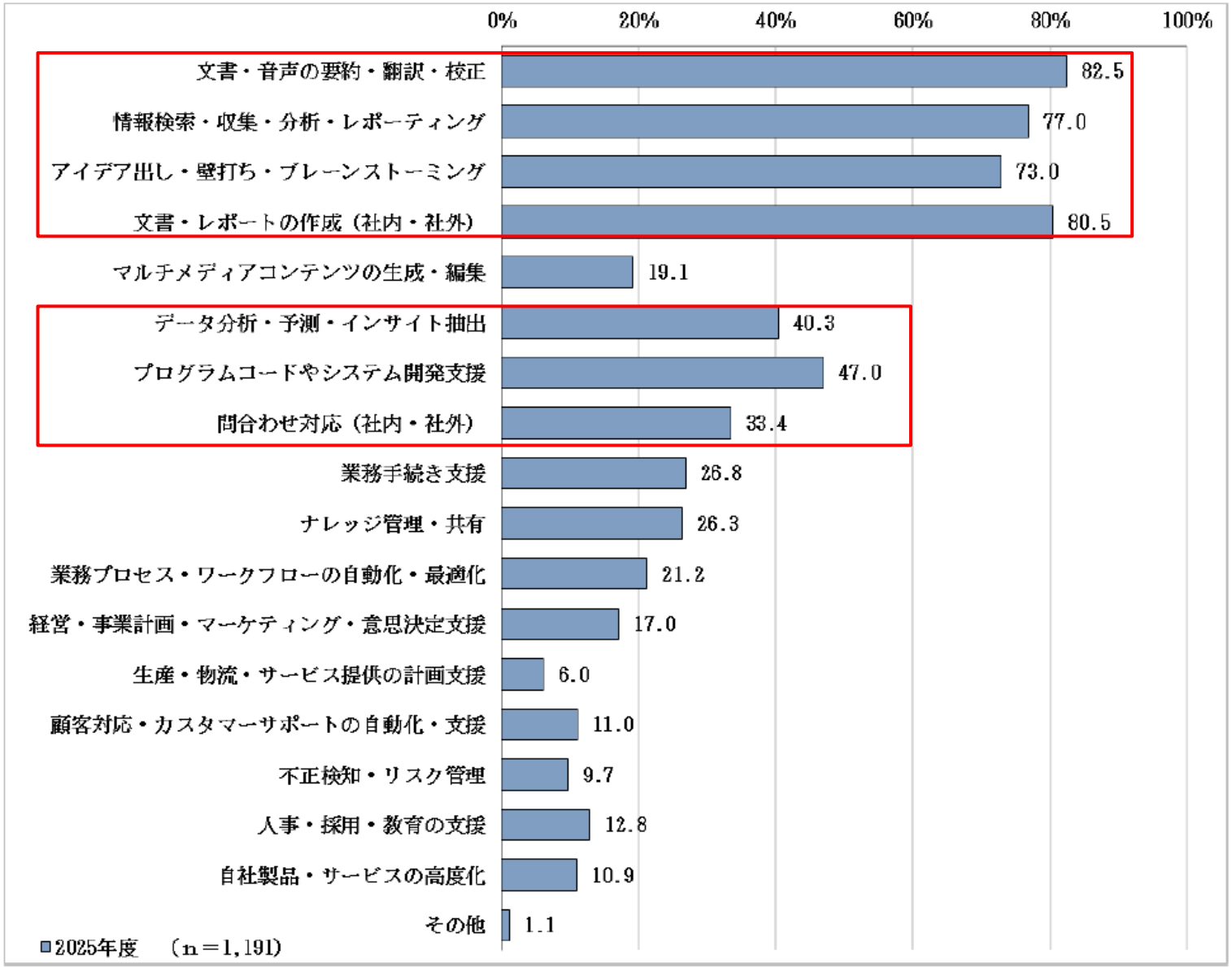


※DX動向2026,IPA

16

AI利活用は個人用途が中心

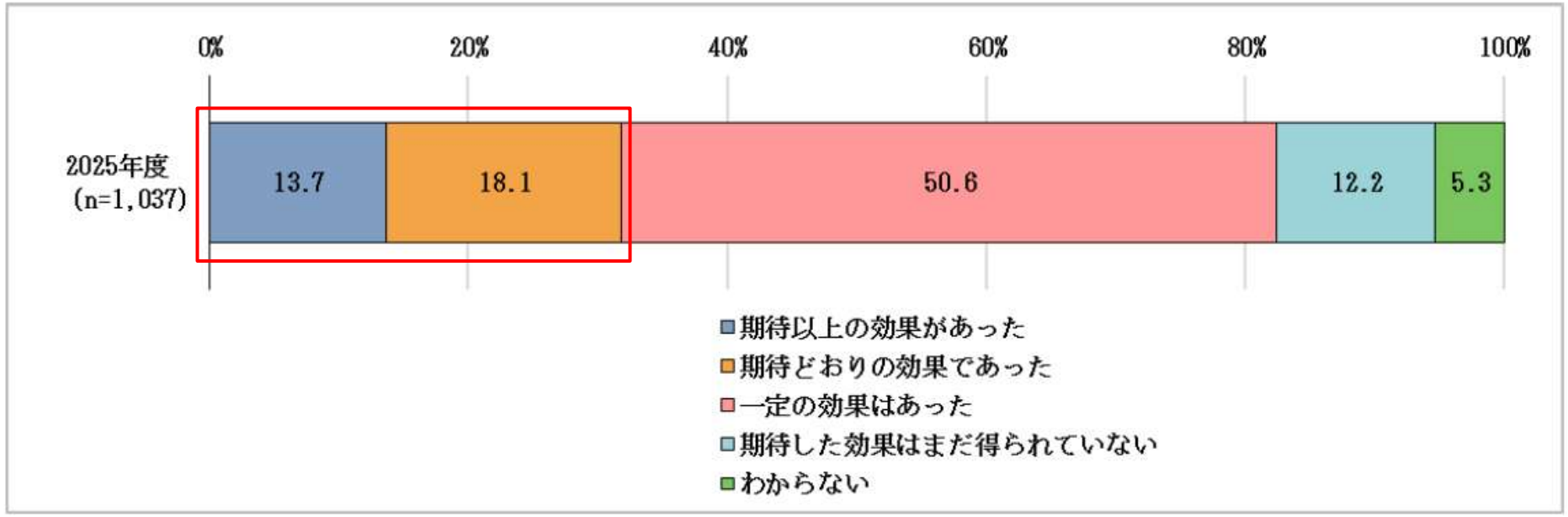
AI利活用の用途



※DX動向2026,IPA

AI利活用の効果は現れ始めている

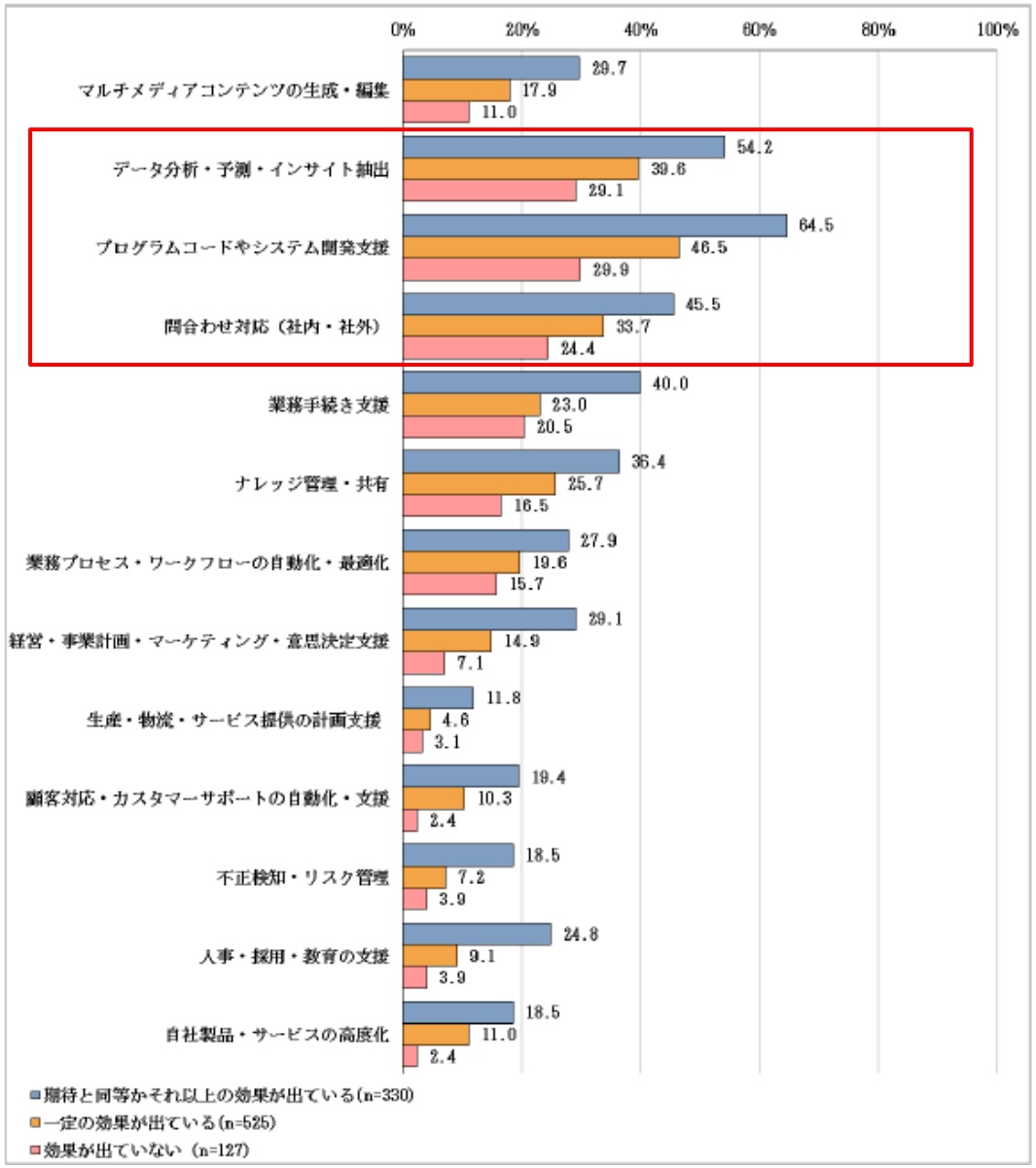
AI導入による効果の状況



※DX動向2026,IPA

データ分析やシステム開発等では効果が出ている

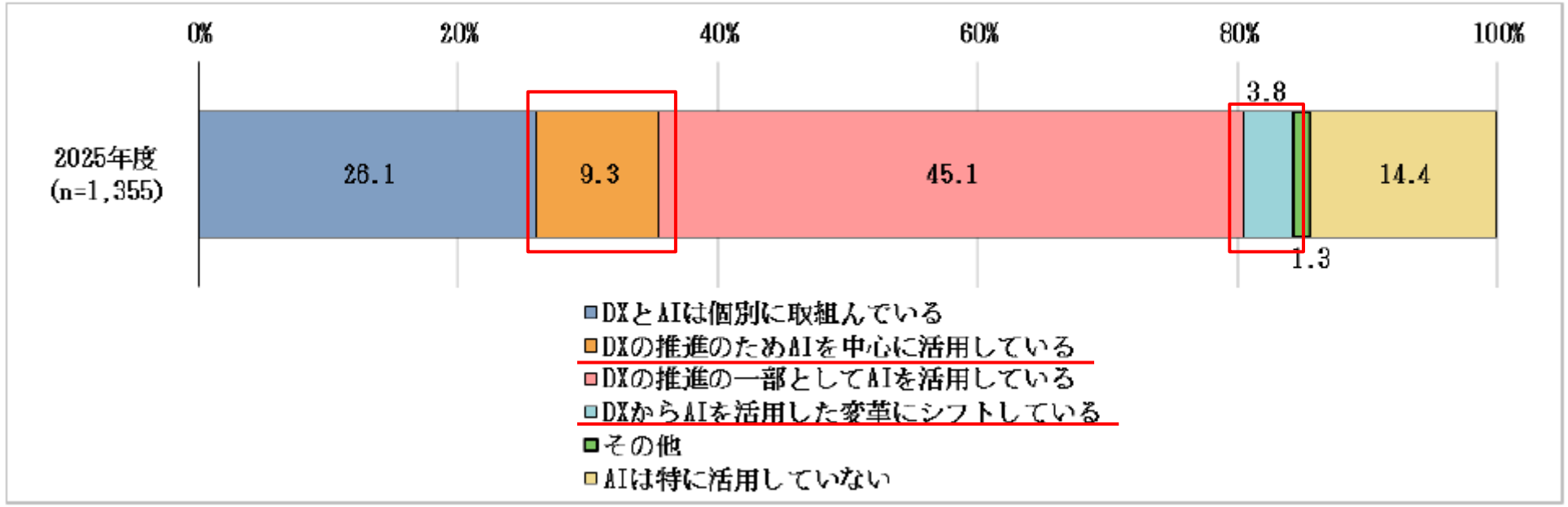
AI利活用の用途（AI導入効果別・抜粋）



※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

デジタルガバナンスコード

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

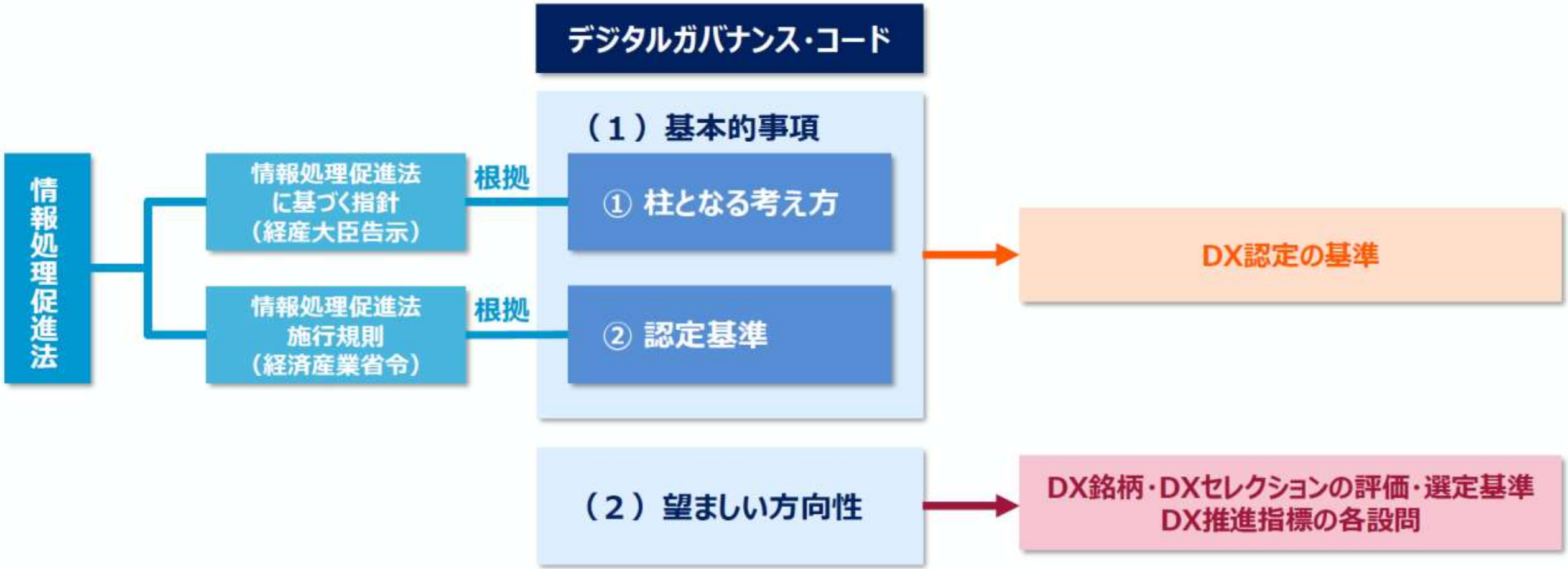
- デジタルガバナンスコードは制度上、定期的にアップデートが行われる
  - ✓ 2020年11月：「デジタルガバナンス・コード」完成・公開
  - ✓ 2022年9月：デジタル人材の育成・確保をはじめとした時勢の変化に対応するため、「デジタルガバナンス・コード2.0」に改訂
  - ✓ 2024年6月：「企業価値向上に向けたデジタル・ガバナンス検討会」を立ち上げ、「デジタルガバナンス・コード3.0～DX経営による企業価値向上に向けて～」がまとめられた

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）

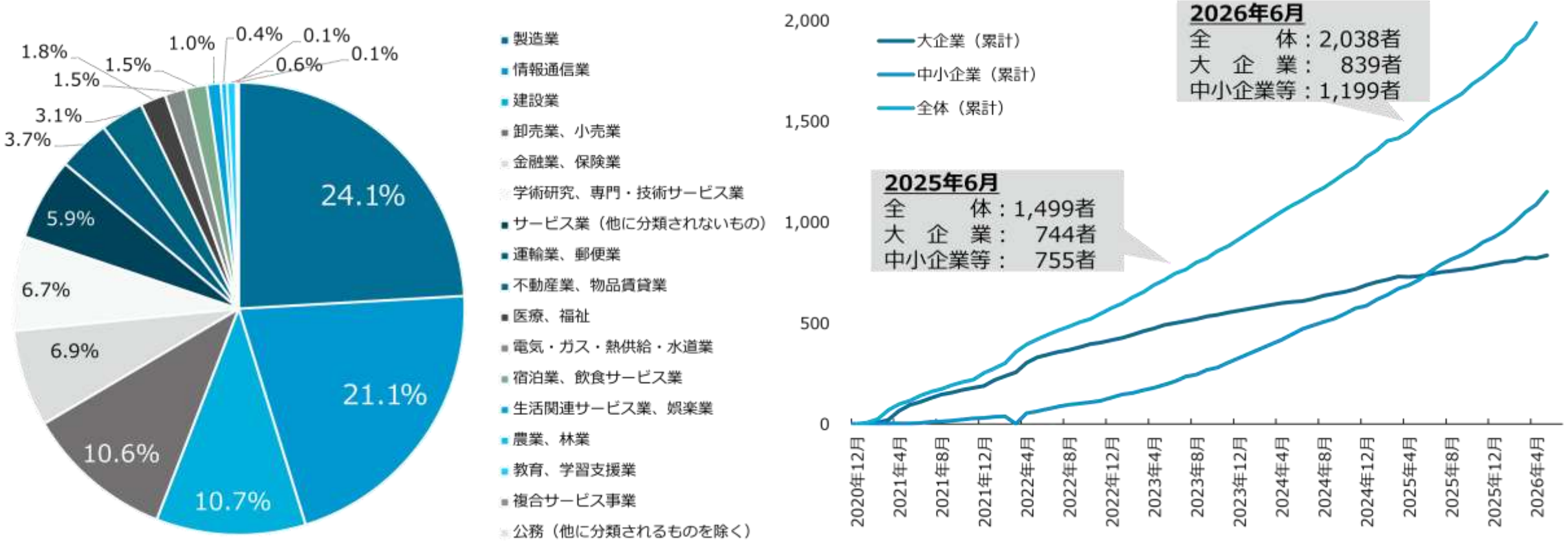
- 第三十条　経済産業大臣は、情報処理システムを良好な状態に維持し、企業経営において戦略的に利用することが重要であることに鑑み、情報処理システムを良好な状態に維持するために必要な情報処理システムの運用及び管理に関する指針を定めるものとする。
- ２　指針には、次に掲げる事項を定めるものとする。
  - 一　情報処理システムの運用及び管理に関する基本的事項
  - 二　情報処理システムの運用及び管理を適切に行うために必要な体制の整備に関する事項
  - 三　情報処理システムの運用及び管理に係る具体的な方法に関する事項
  - 四　その他情報処理システムの運用及び管理を適切に行うために必要な事項
- 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と他制度との関係



DX認定制度

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セレクション2026

「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

DX銘柄2026

東京証券取引所と経済産業省、IPAが共同で、上場企業の中から優れたデジタル活用の実績が表れている企業を「DX銘柄」として選定している



証券コード	法人名	東証業種分類
5108	株式会社ブリヂストン	ゴム製品
9962	株式会社ミスミグループ本社	卸売業
8316	株式会社三井住友フィナンシャルグループ	銀行業



証券コード	法人名	東証業種分類
2503	キリンホールディングス株式会社	食料品
3407	旭化成株式会社	化学
4452	花王株式会社	化学
4901	富士フイルムホールディングス株式会社	化学
4502	武田薬品工業株式会社	医薬品
4507	塩野義製薬株式会社	医薬品
4519	中外製薬株式会社	医薬品
4568	第一三共株式会社	医薬品
5201	AGC株式会社	ガラス・土石製品
6645	オムロン株式会社	電気機器
6701	日本電気株式会社	電気機器
6702	富士通株式会社	電気機器
6762	TDK株式会社	電気機器
7912	大日本印刷株式会社	その他製品
9503	関西電力株式会社	電気・ガス業
9021	西日本旅客鉄道株式会社	陸運業
9143	SGホールディングス株式会社	陸運業
9302	三井倉庫ホールディングス株式会社	倉庫・運輸関連業
9432	NTT株式会社	情報・通信業
2768	双日株式会社	卸売業
8001	伊藤忠商事株式会社	卸売業
8410	株式会社セブン銀行	銀行業
8766	東京海上ホールディングス株式会社	保険業
8253	株式会社クレディセゾン	その他金融業
3289	東急不動産ホールディングス株式会社	不動産業
2168	株式会社パソナグループ	サービス業
2181	パーソルホールディングス株式会社	サービス業

デジタルガバナンスコード4.0について

デジタルガバナンスコードのバージョンアップに向けて、「AI時代におけるデジタルガバナンス検討会」が２０２６年７月から経済産業省で開催中。まとまり次第、公表される予定

AI 時代におけるデジタルガバナンス検討会
委員名簿

〈座長〉

伊藤	邦雄	一橋大学　CFO 教育研究センター長

〈委員〉

安立	大介	株式会社日立製作所　IT デジタル統括本部統括本部長　兼 デジタル＆セキュリティ統括本部　副統括本部長
石原	直子	株式会社 FutureWork 研究室　代表取締役
志済	聡子	合同会社アイシスコンサルティング　代表
寺沢	徹	アセットマネジメント One 株式会社　運用本部 リサーチ・エンゲージメント部　エグゼクティブ ESG アドバイザー
野村	真実	特定非営利法人　IT コーディネータ協会　会長
三谷	慶一郎	独立行政法人情報処理推進機構　理事

サイバーセキュリティの確保

頻発する不正アクセス

頻発する不正アクセス事案

- 2026年9月頃から国内企業における情報漏えい・不正アクセス・ランサムウェア等の障害が頻発
- 情報漏えい規模が大きい事案：
  - ✓ Gyazo（約2,362万件）、EPARK（約2,218万レコード）、skyticket（約1,464万件）、焼肉きんぐ（1,079万件）、第一興商（約872万件）、タイムズカー（約660万件）等
- 口座の情報を含む事案：
  - ✓ イープラス、skyticket、修道学園、大和証券（証券口座番号）等
- 免許証やパスポート等なの本人確認書類を含む事案：
  - ✓ タイムズカー、HISのタイ子会社
- ランサムウェア等によって業務停止した事案：
  - ✓ 京王電鉄グループ、大阪公立大学、IDCFクラウド

※新聞・Web記事等から整理

省庁等からの注意喚起（1/3）

- 国家サイバー統括室（NCO）（10/9）
  - ✓ 特に、大量の個人情報を取り扱う事業者や機微な情報を取り扱う事業者等で対応の徹底を検討してほしい
  - ✓ ウェブシステム等の適切な管理（脆弱性管理、アカウント管理・認証、レジリエンスの向上）
  - ✓ サプライチェーンを通じた侵害への対策（委託先企業等のセキュリティ対策状況の把握、委託契約におけるセキュリティ要件の明確化、情報共有範囲の適正化、サプライチェーン全体のリスクマネジメント）
  - ✓ データの適切な管理（保有する情報資産の適切な管理、保有情報の最小化、適切なアカウント管理・アクセス管理、データ保護の徹底、ログ取得・監視・分析の強化）
- 経済産業省（10/9）
  - ✓ 自社のみならず、サプライチェーン全体でセキュリティを管理するという認識の下、①組織のトップによる主導、②脆弱性情報の早期把握と対応、③「ゼロトラスト」への移行など、一層の対策の徹底をお願いする
  - ✓ また、被害発生時には情報提供に協力してほしい
- 金融庁（10/9）
  - ✓ 公表情報等を通じて明らかとなる攻撃の原因・手口等を踏まえ、サードパーティリスク管理やインシデントが起きた場合の対応態勢も含めたサイバーセキュリティ対策について点検し、必要な措置を速やかに講じること
  - ✓ 非対面の本人確認を行うにあたっては、本人確認書類の画像、顧客の容貌の画像に不自然な点がないかの確認を徹底すること
  - ✓ 犯罪収益移転防止法施行規則の改正により、施行日である令和９年４月１日より、本人確認方法として、本人確認書類の画像送信を受ける方法は廃止し、不正対策として極めて効果が高い、ＩＣチップ情報の読取に原則一本化されるところ、現下の情勢を踏まえ、施行日を待たず、可及的速やかな対応を図ること

省庁等からの注意喚起（2/3）

- 情報処理推進機構（10/9）
  - ✓ サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
  - ✓ 速やかに行うべき点検：
    - 外部に公開しているアプリケーションの精査
    - 自組織が利用している外部サービスの洗い出し
    - 保有データの再点検
  - ✓ 速やかに取り組むべき対策：
    - 外部に公開しているアプリケーションについての対策（外部公開範囲の見直し、認証機能の強化、アカウントへの権限付与の見直し等）
    - 自組織が利用している外部サービスについての対策（認証機能の強化、アカウント付与の範囲見直し、API連携等の管理状況の見直し等）
    - 保有するデータについての対策（データ保有の是非の再検討、データ保管場所の再検討、ログ取得内容・保持期間の見直し等）
  - ✓ 総合的なサイバーセキュリティ対策の更なる推進

省庁等からの注意喚起（3/3）

- 情報処理推進機構「不正アクセス特別相談窓口」の開設（10/16）
  - ✓ IPAは、相次ぐ不正アクセスによる個人情報漏えいの発生に際し、企業や組織からの支援依頼に対応するため、「不正アクセス特別相談窓口」を開設
  - ✓ 実際に被害を受けているまたはその可能性がある事象が発生している企業や組織を対象に、不正アクセスによる情報漏えいインシデント発生における初動対応支援を行う
  - ✓ 対応内容：インシデント発生時の初動対応に関する相談
    - 起きている事象をヒアリングし、被害発生の可能性についての助言
    - 被害が発生している場合、有効な応急処置案についての助言
    - インシデント対応を行う専門業者一覧の紹介
    - 他に必要な相談・報告先等の紹介
  - ✓ 不正アクセス特別相談窓口
    - https://www.ipa.go.jp/security/support/incident-support.html

- 不正アクセスが頻発しているのは複合的な要因か？
  - ✓ 当然ながらAIの影響はありそう
- いずれにせよ、今後収束していくとは考えにくい

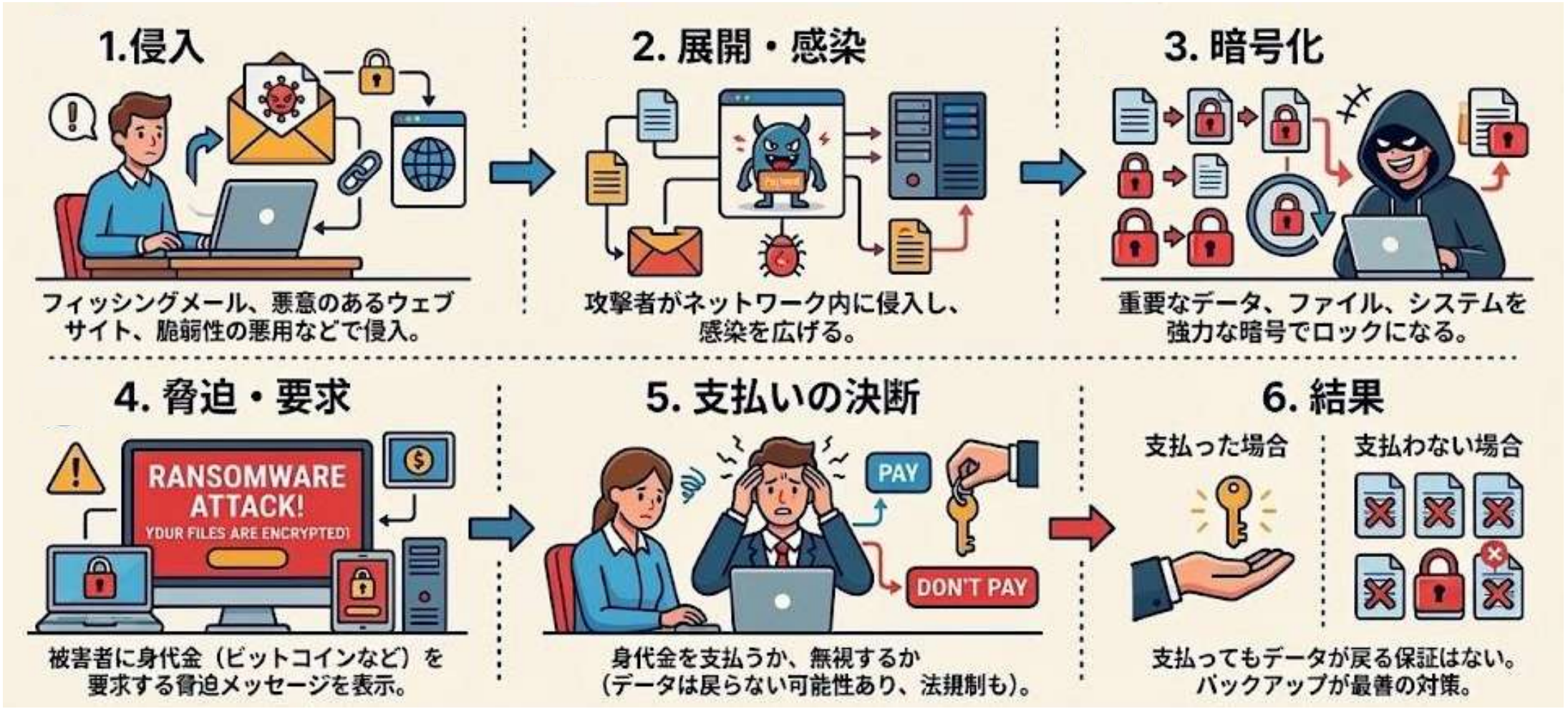
情報セキュリティ10大脅威

「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」

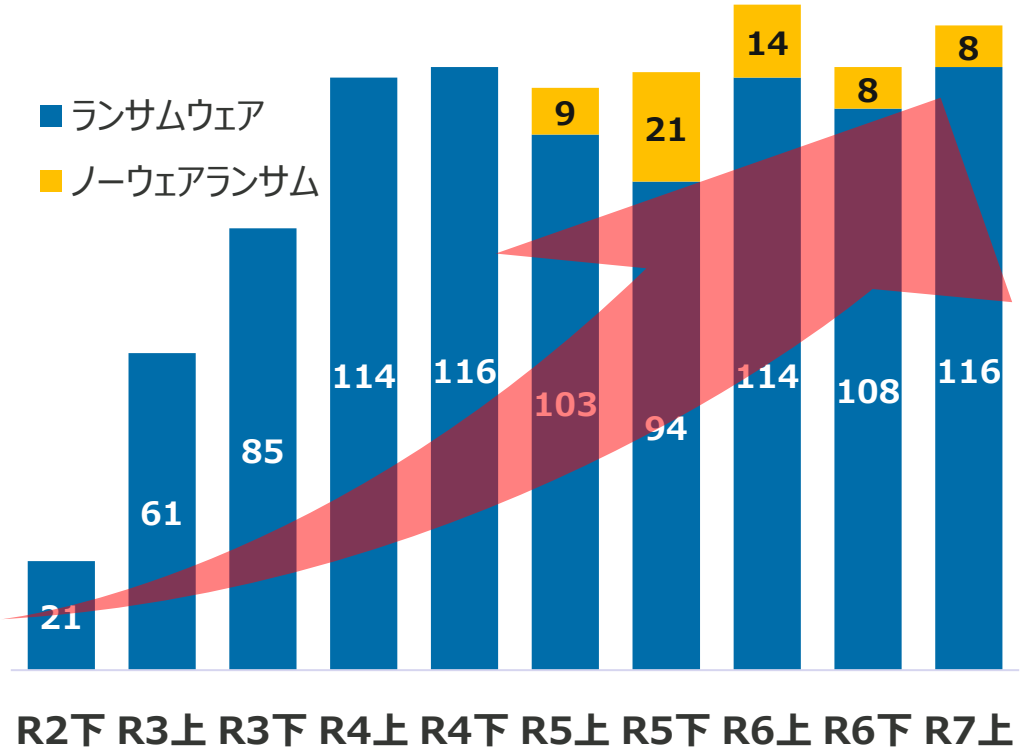
ランサムウェア攻撃の仕組み



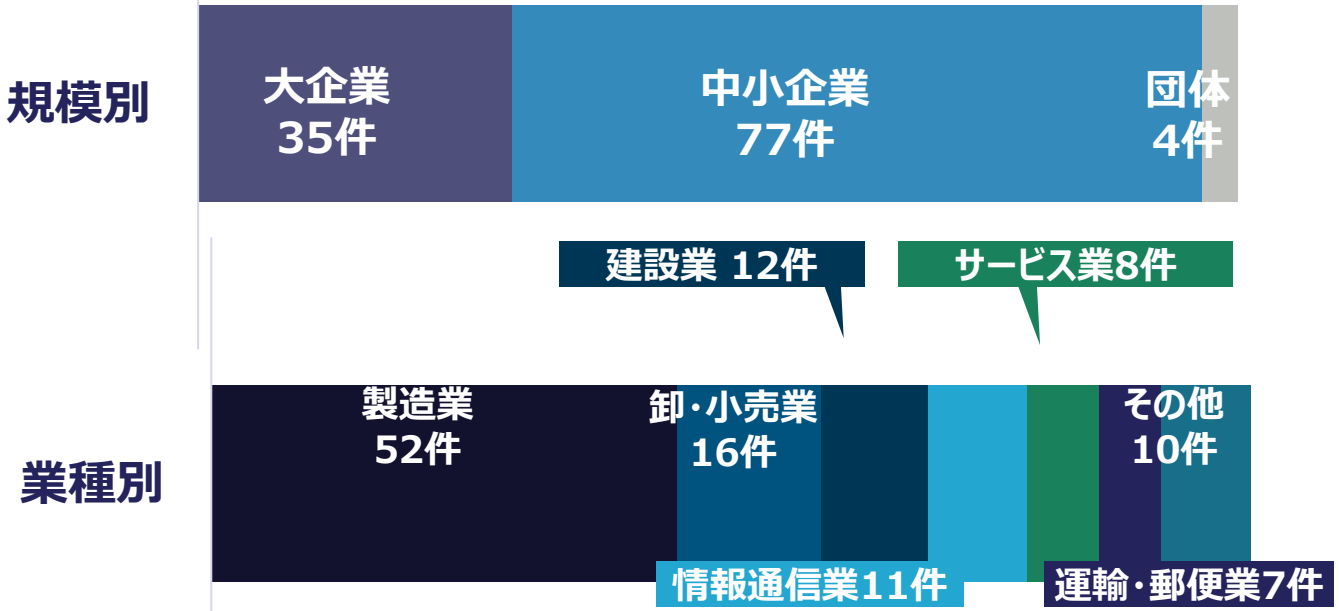
ランサムウェア攻撃による被害

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



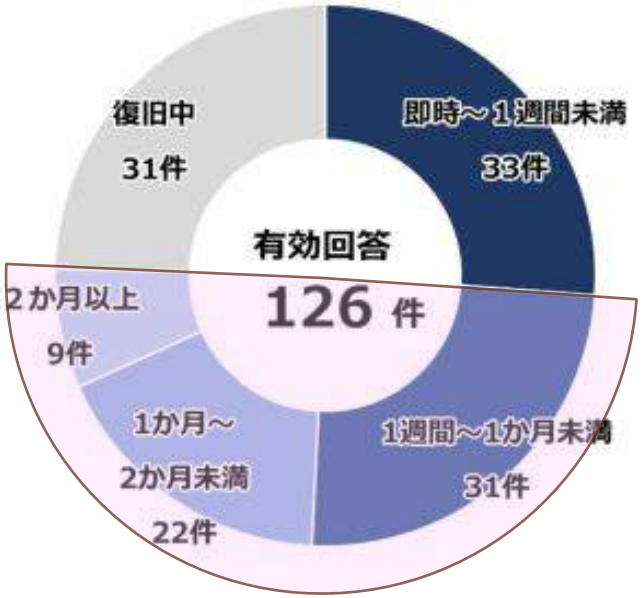
出典「令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）」をもとにIPAが作成
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

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



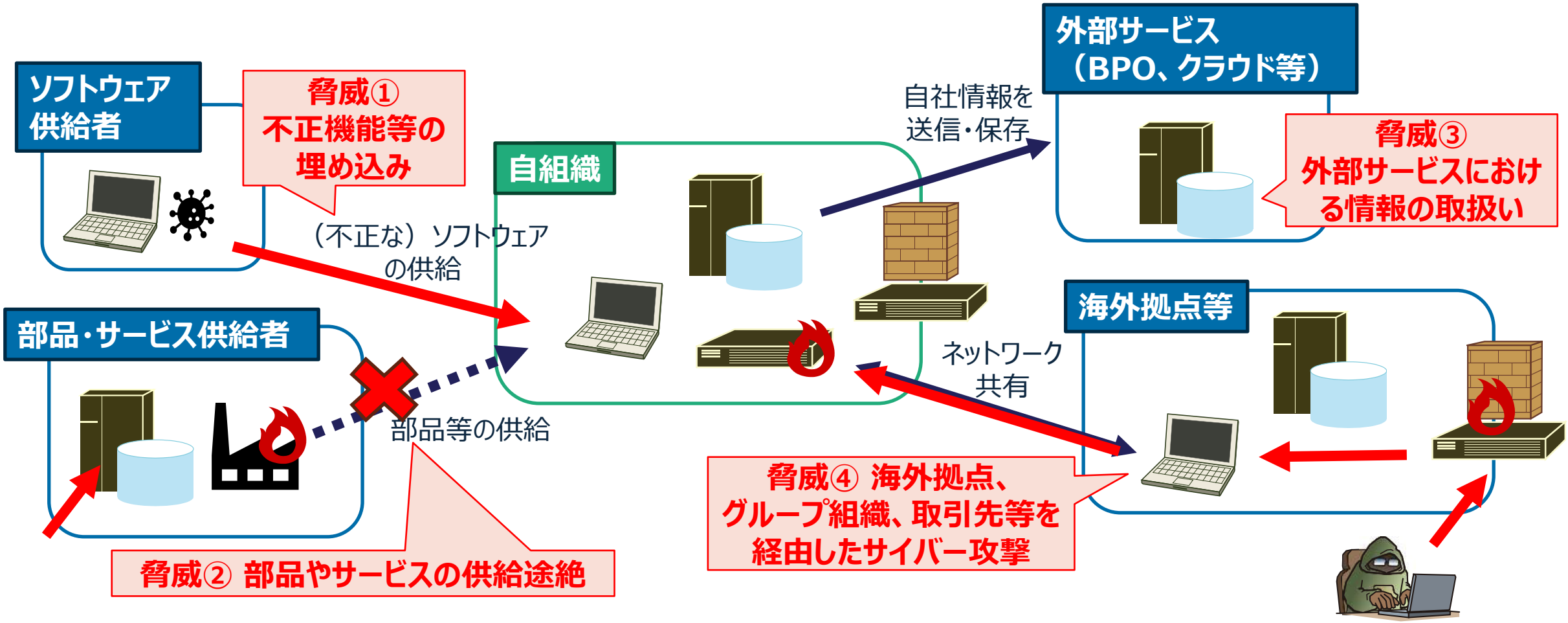
2種類のサプライチェーン

- **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

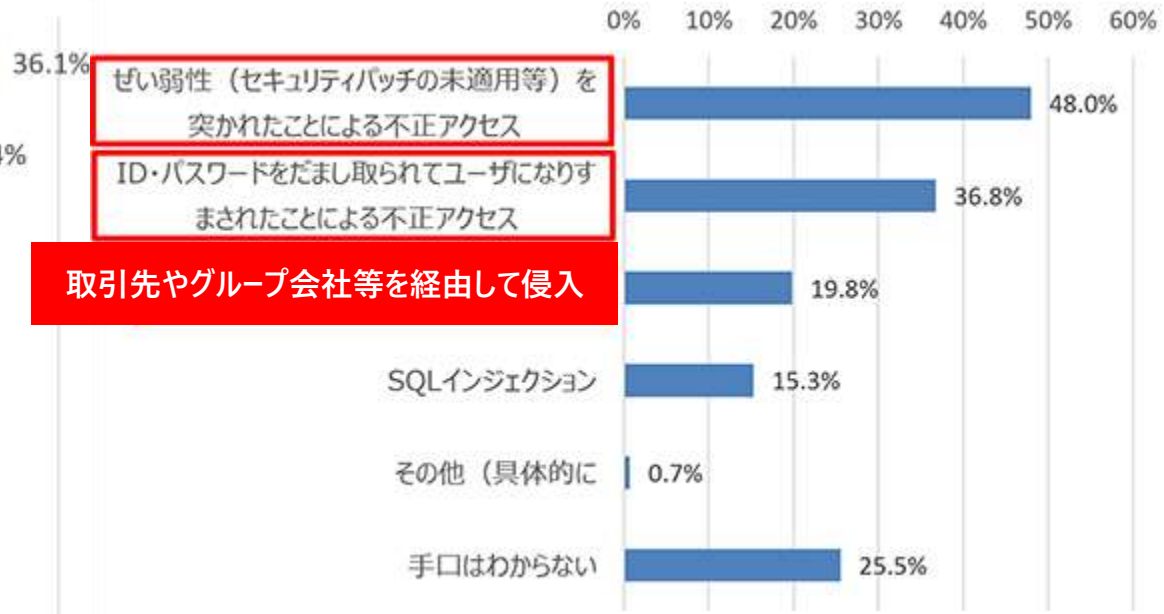
サプライチェーンや委託先を狙った攻撃

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。

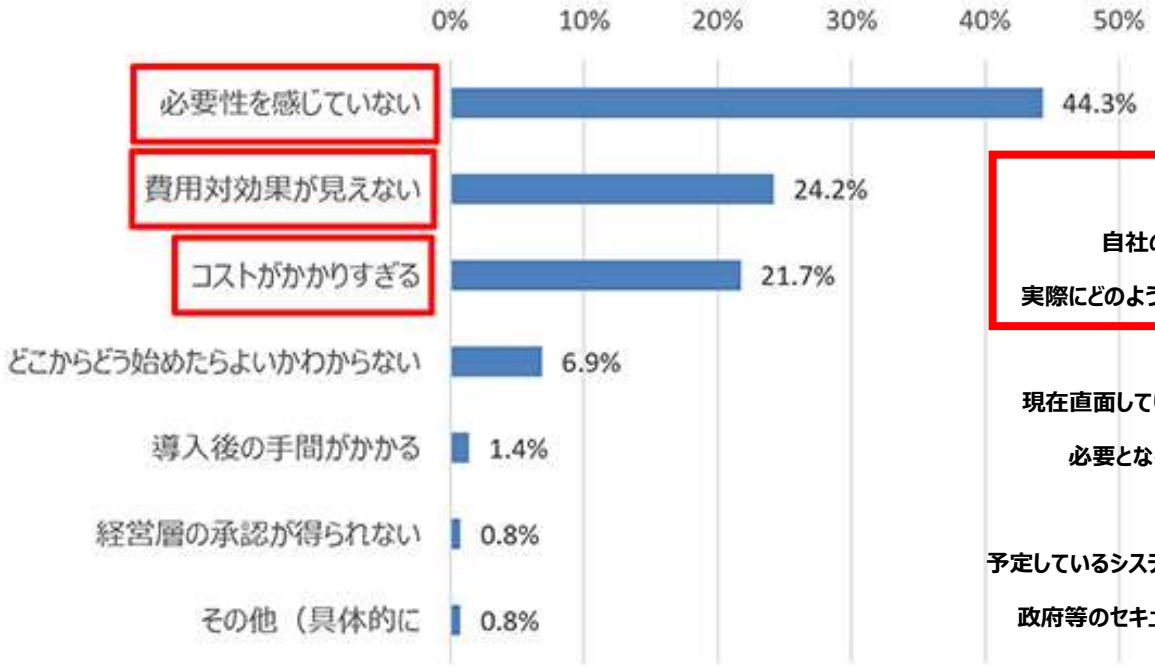
出典：「2024年度中小企業等実態調査結果」速報版（IPA）
https://www.ipa.go.jp/pressrelease/2024/press20250214.html

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

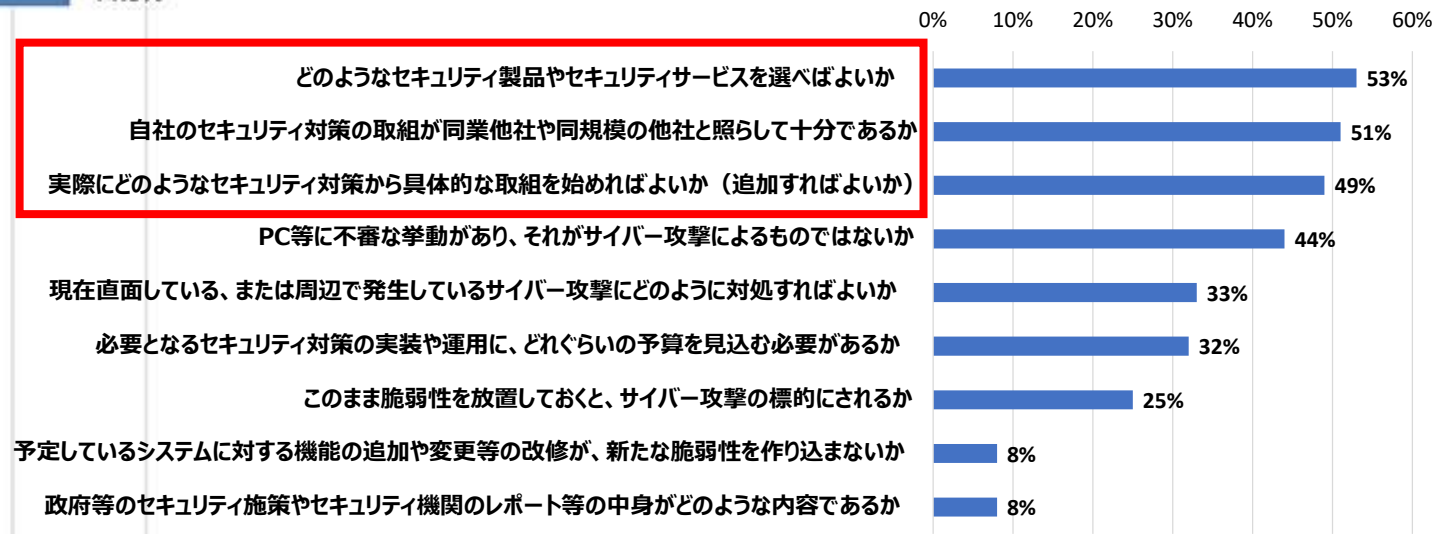
- 過去3期で**セキュリティ投資を行っていない**中小企業は**約６割**、うち、４割がセキュリティ投資の必要性を感じておらず、**約５割**が**コスト**面を指摘。
- 中小企業の**５割**が、どのような製品を導入すれば良いか、自社のセキュリティ対策が十分なのかに関心。

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）

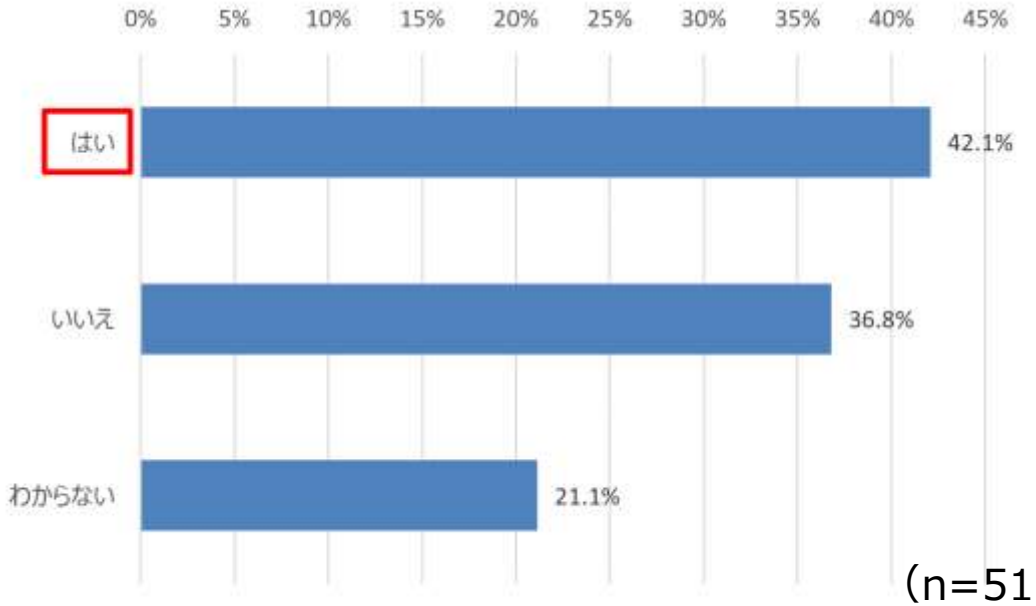


出典：「2024年度中小企業等実態調査結果」速報版（IPA）https://www.ipa.go.jp/pressrelease/2024/press20250214.html

サプライチェーンや委託先を狙った攻撃

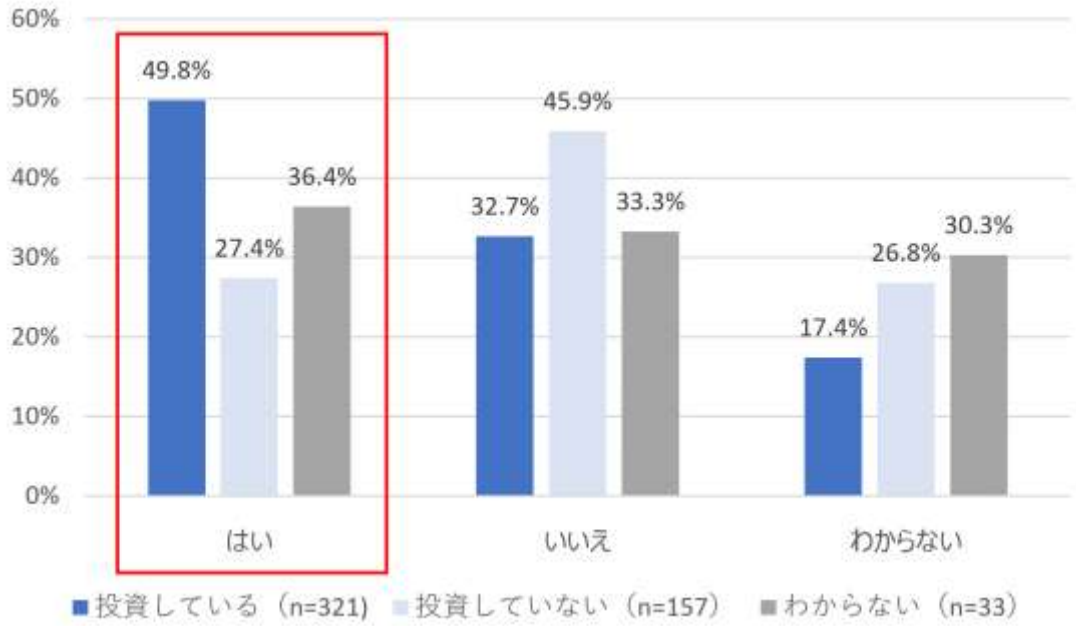
セキュリティ対策の実施は、取引拡大の契機に

- 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）

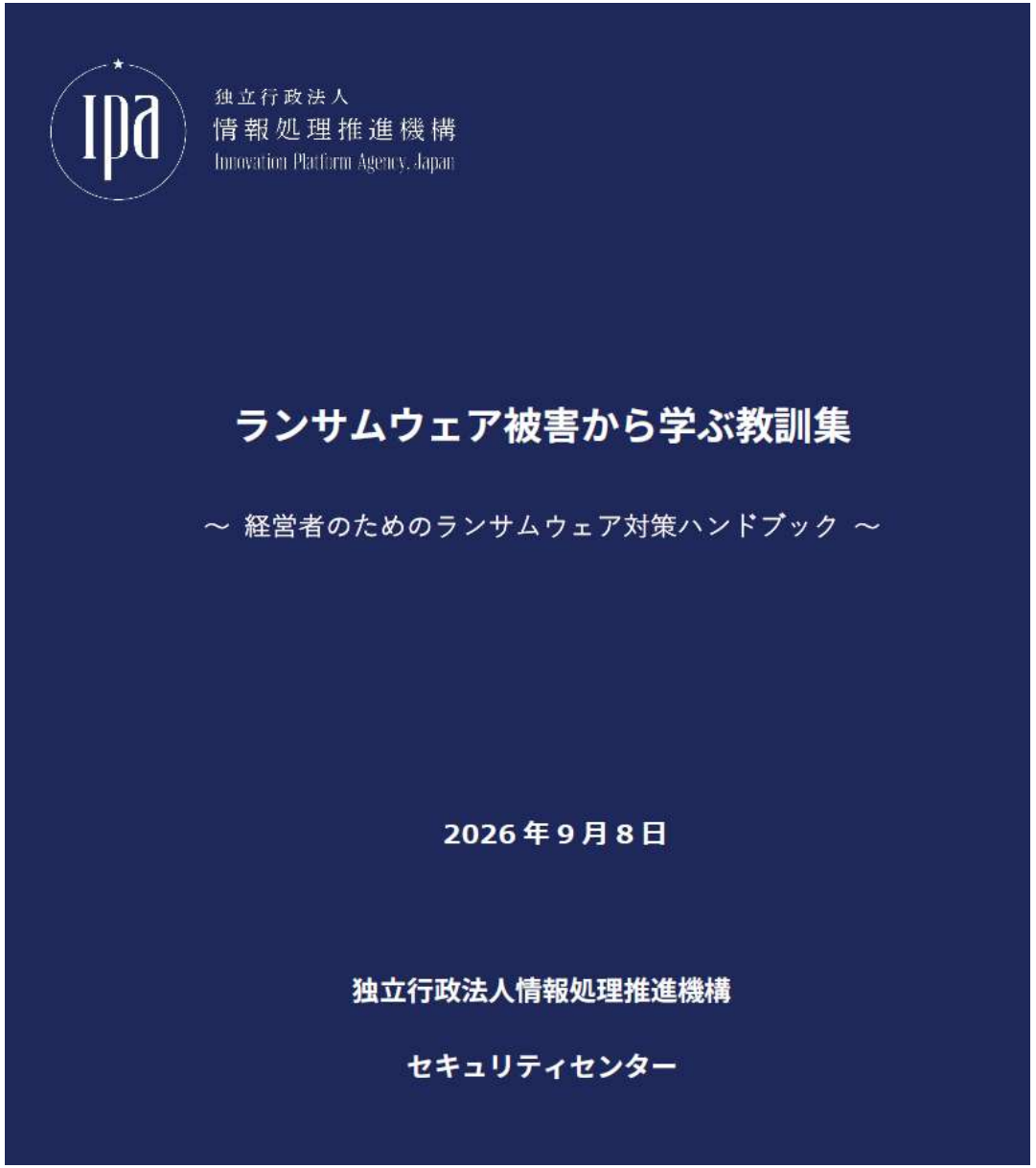
質問：貴社は取引先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。（SA）



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

「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）



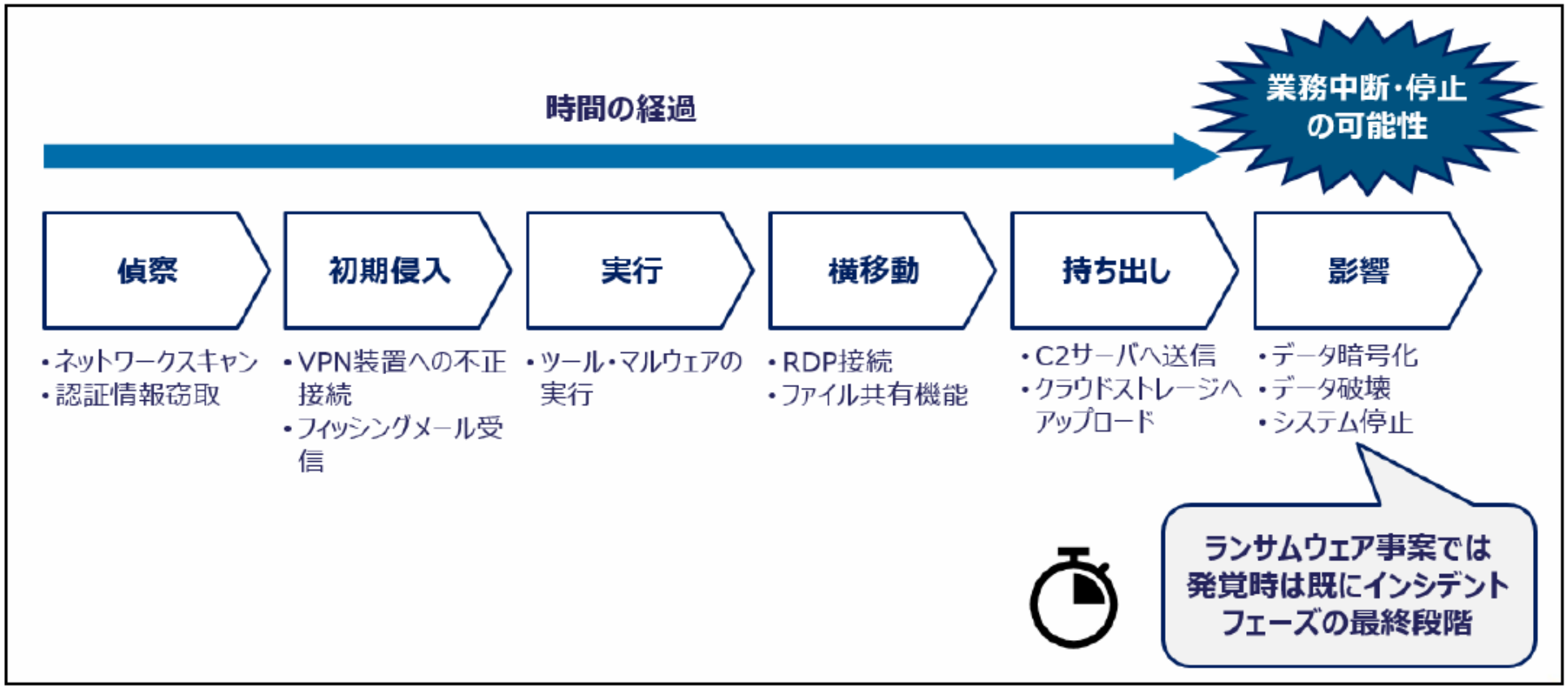
- ランサムウェア攻撃の被害が組織の規模を問わず多発している状況が継続しています。
- コンピュータウイルス・不正アクセス届出窓口では、国内の複数の被害組織へインタビューをおこない、被害発生当時、組織でどのようなことが発生し、どのような対応をしたかを振り返っていただきました。それらの中から他の組織でも起こり得ること等を抽出し、教訓として取りまとめ、経営者向けとインシデント対応部門向けに分けて整理しました。
- そして、ランサムウェアの脅威に立ち向かうには、経営者の理解と関与が非常に重要であることをお伝えするべく、サブタイトルを「経営者のためのランサムウェア対策ハンドブック」としました。
- 今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

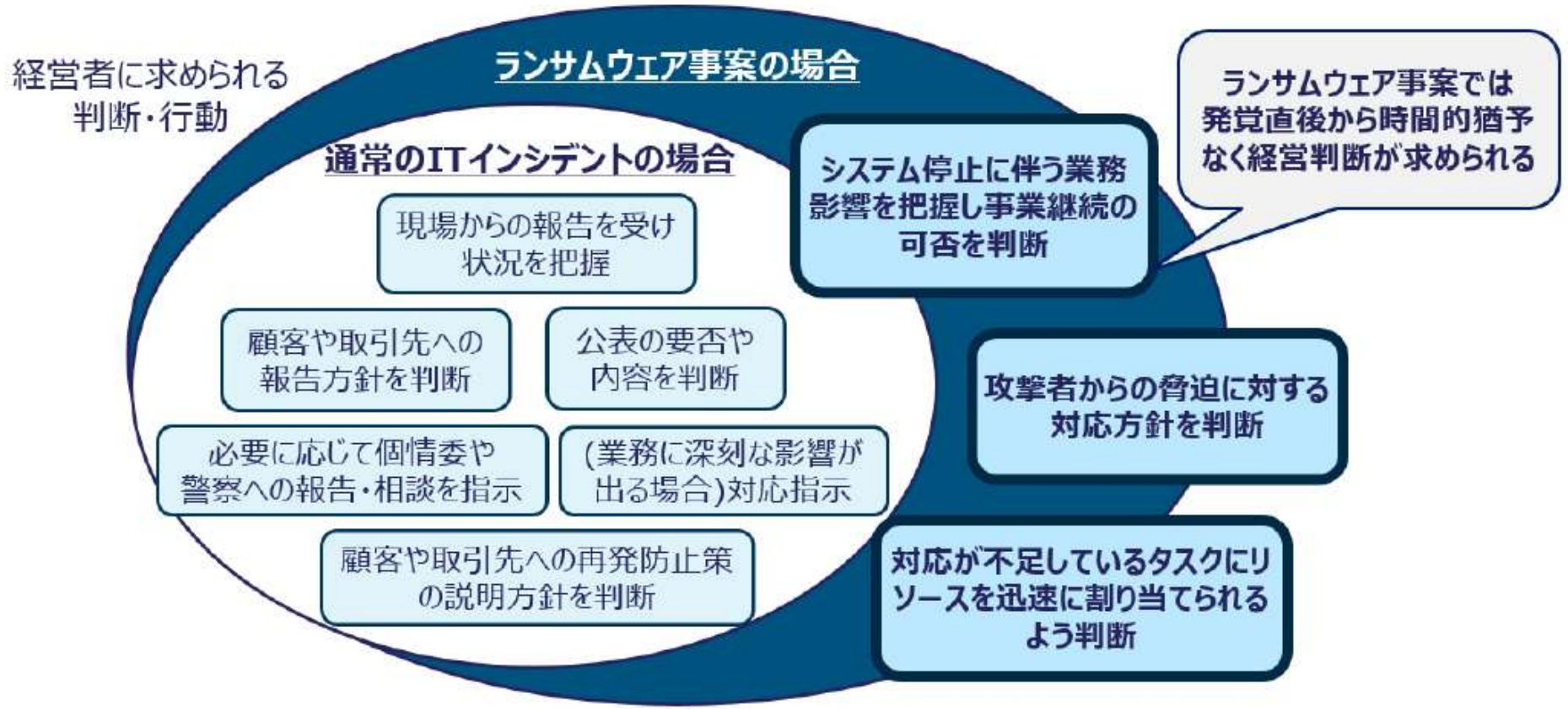


※「ランサムウェア被害から学ぶ教訓集」（IPA）

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）

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）

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、書庫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

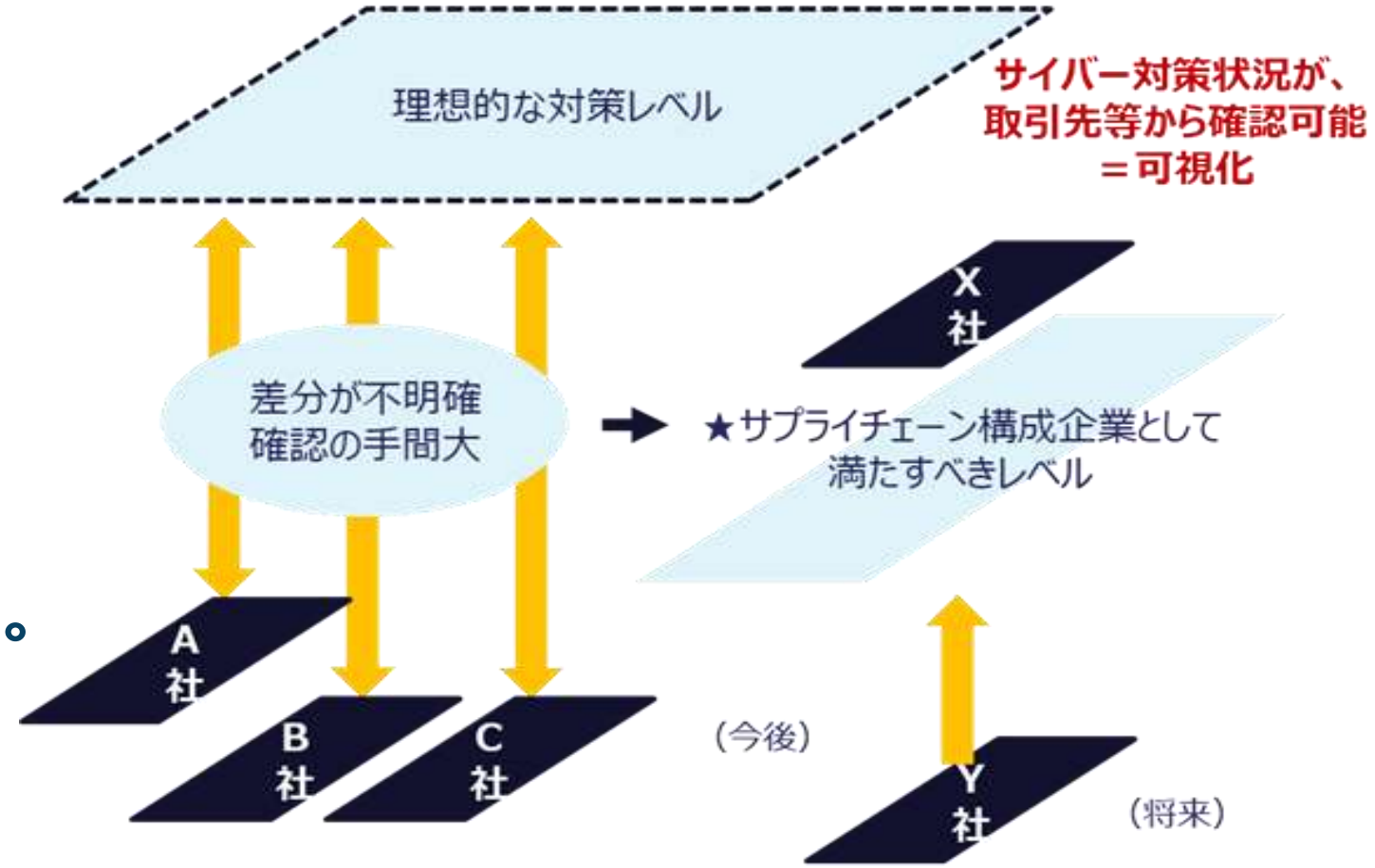
SCS評価制度（サプライチェーンセキュリティ対策評価制度）：目的

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：セキュリティ専門家と評価機関

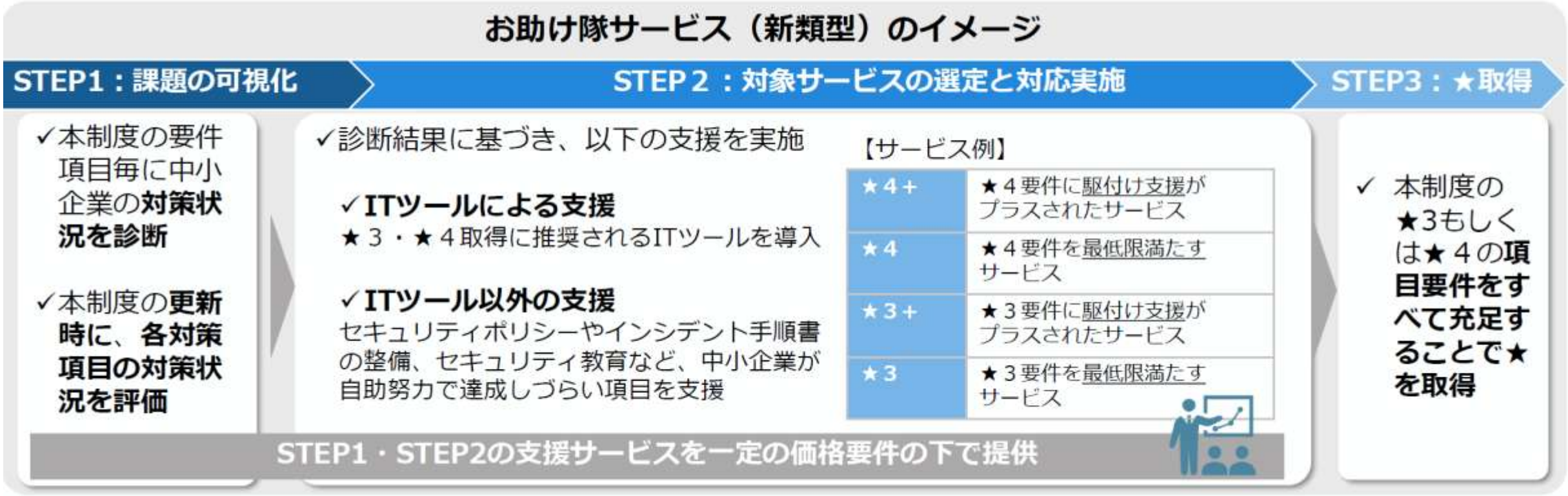
★３では、セキュリティ専門家が、取得希望組織が作成した書類の確認を行う。

★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。

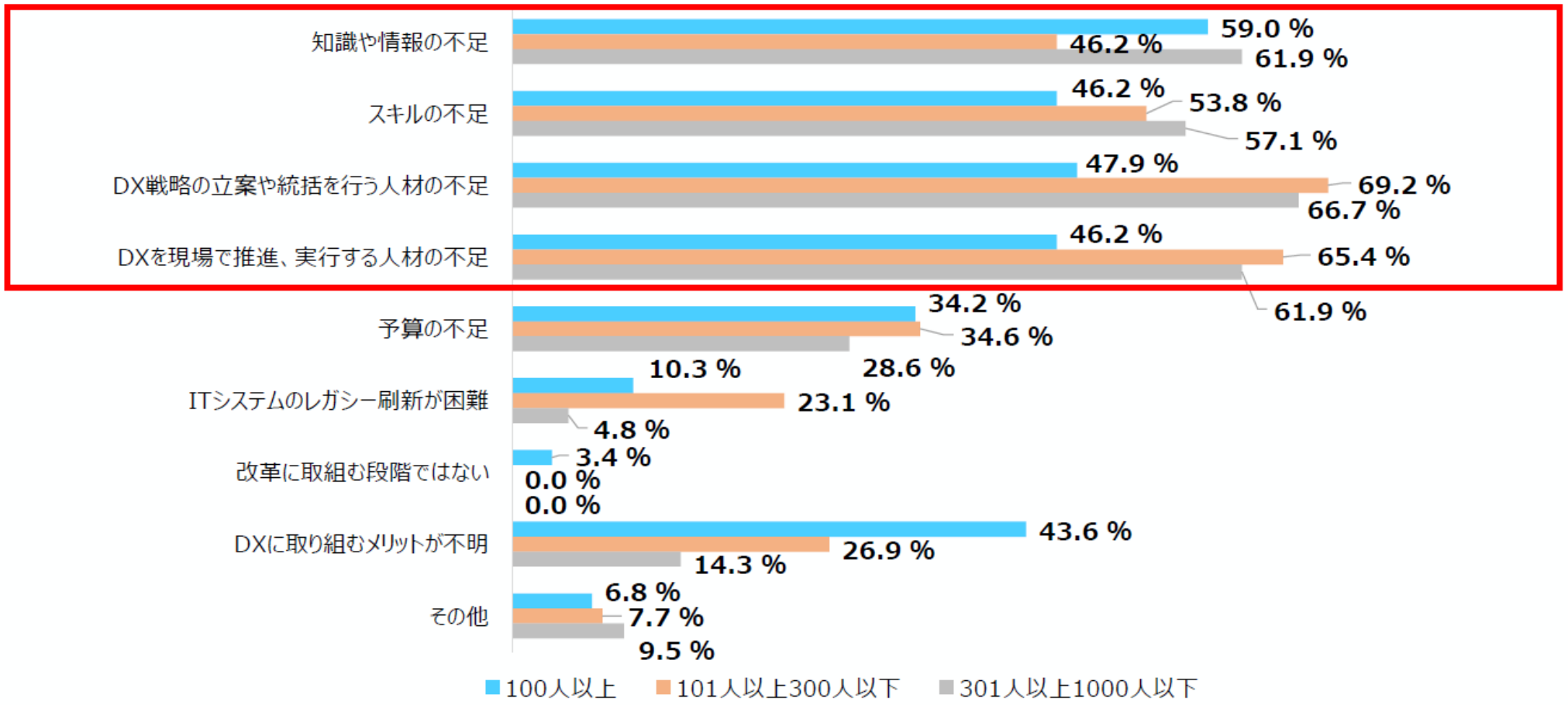
SCS評価制度：お助け隊による支援

「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



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

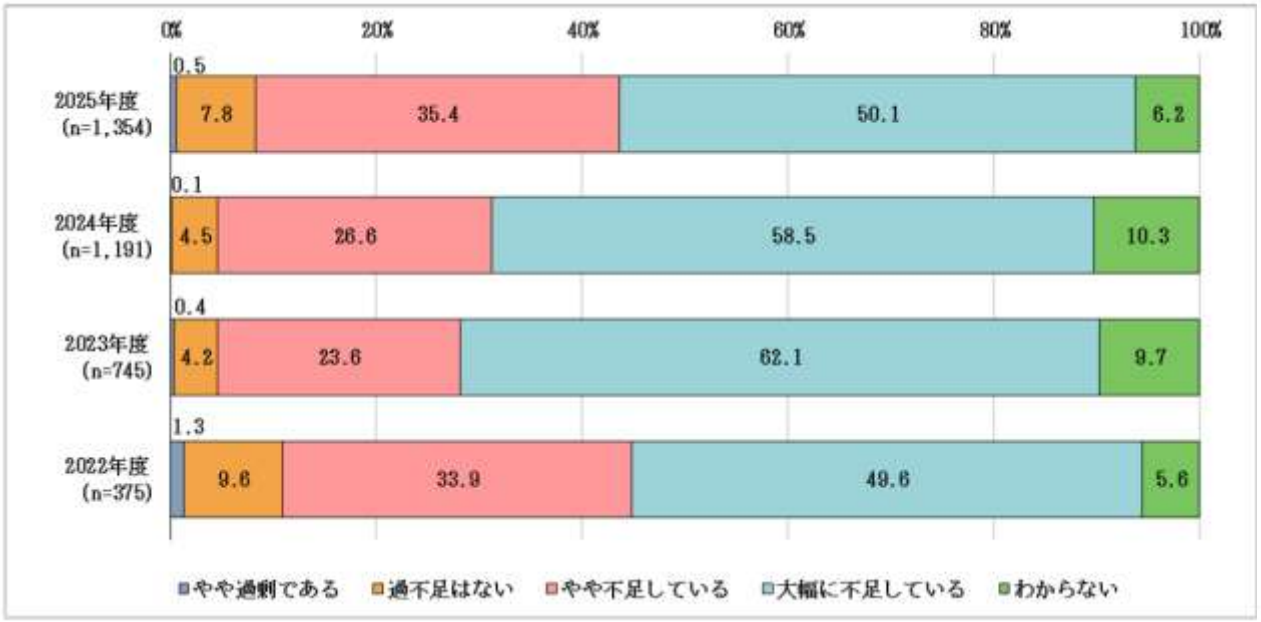


（注）DX取組予定で「DXに取組む予定はない」「DXに取り組むか、分からない」と回答した企業が対象であり、「1,001人以上」はn数が1であったためグラフからは除外。
出典：情報処理推進機構「DX動向2024（本文）」（2024年6月27日）を基に作成。

※「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

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

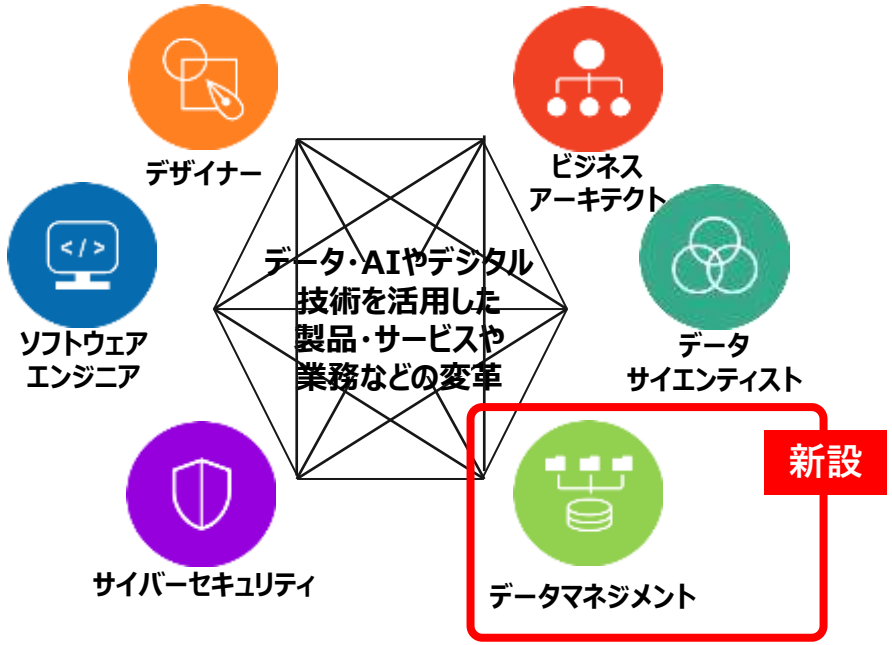
マインド・スタンス
不確実性の高い時代において、新たな価値を生み出すために必要な意識・姿勢・行動をデザインの素養に基づいて定義

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

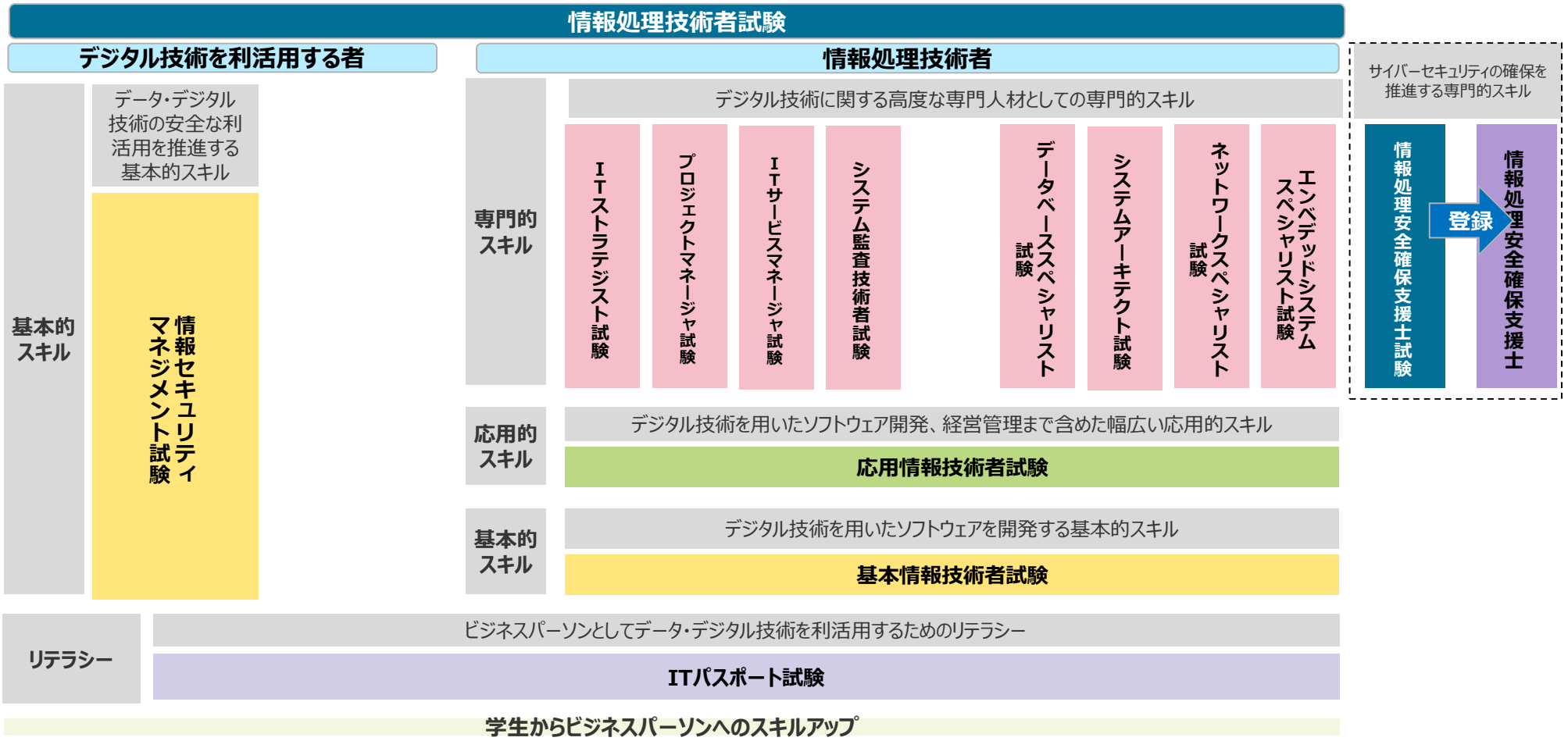
デザイナーの活躍する領域を見直し、企業及びプロジェクトのブランドメッセージやコンテンツ制作に反映するコミュニケーション領域におけるロールを、**コミュニケーションデザイナー**として定義

（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

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）」

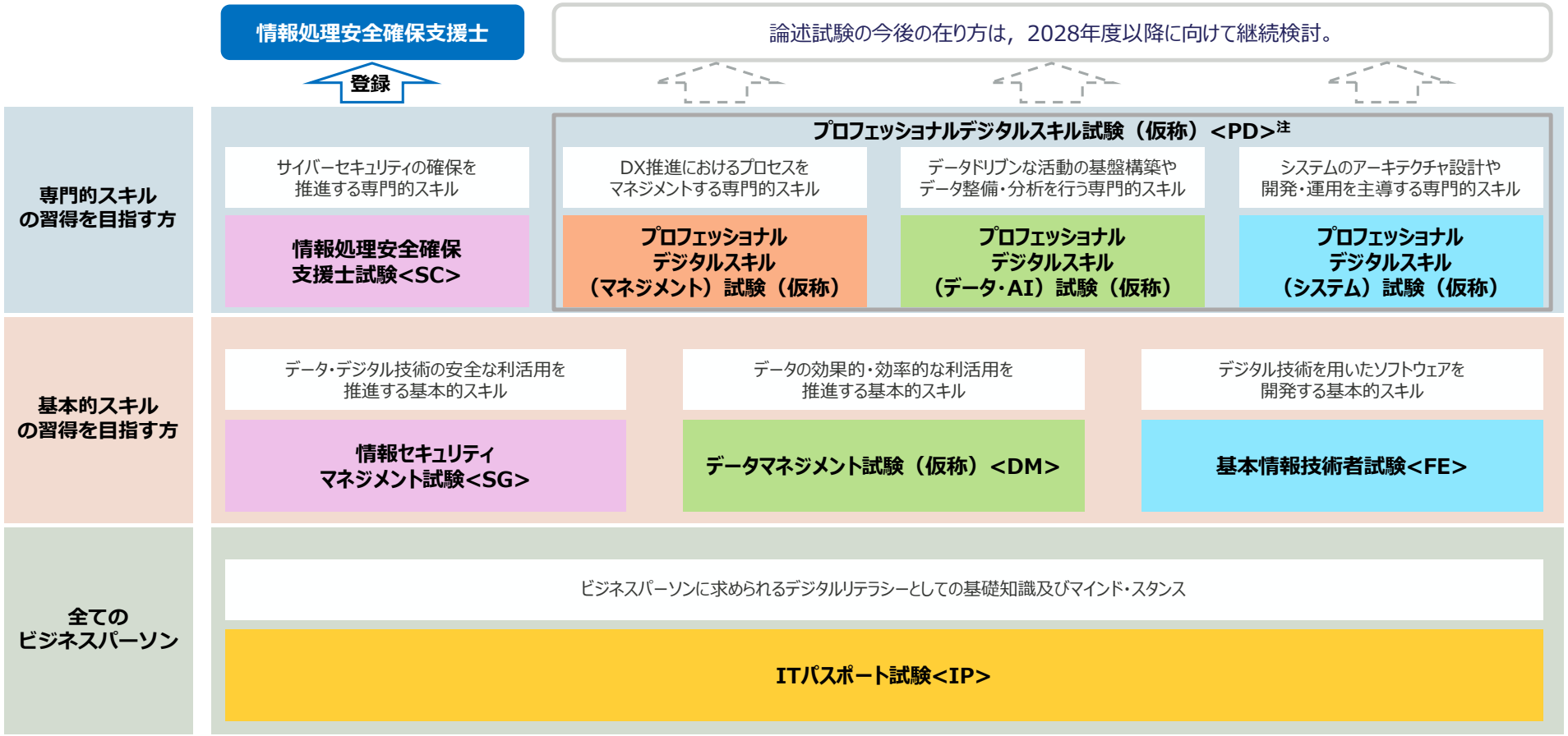
※3 Computer Based Testing：コンピュータを利用した試験方式

※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

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＞



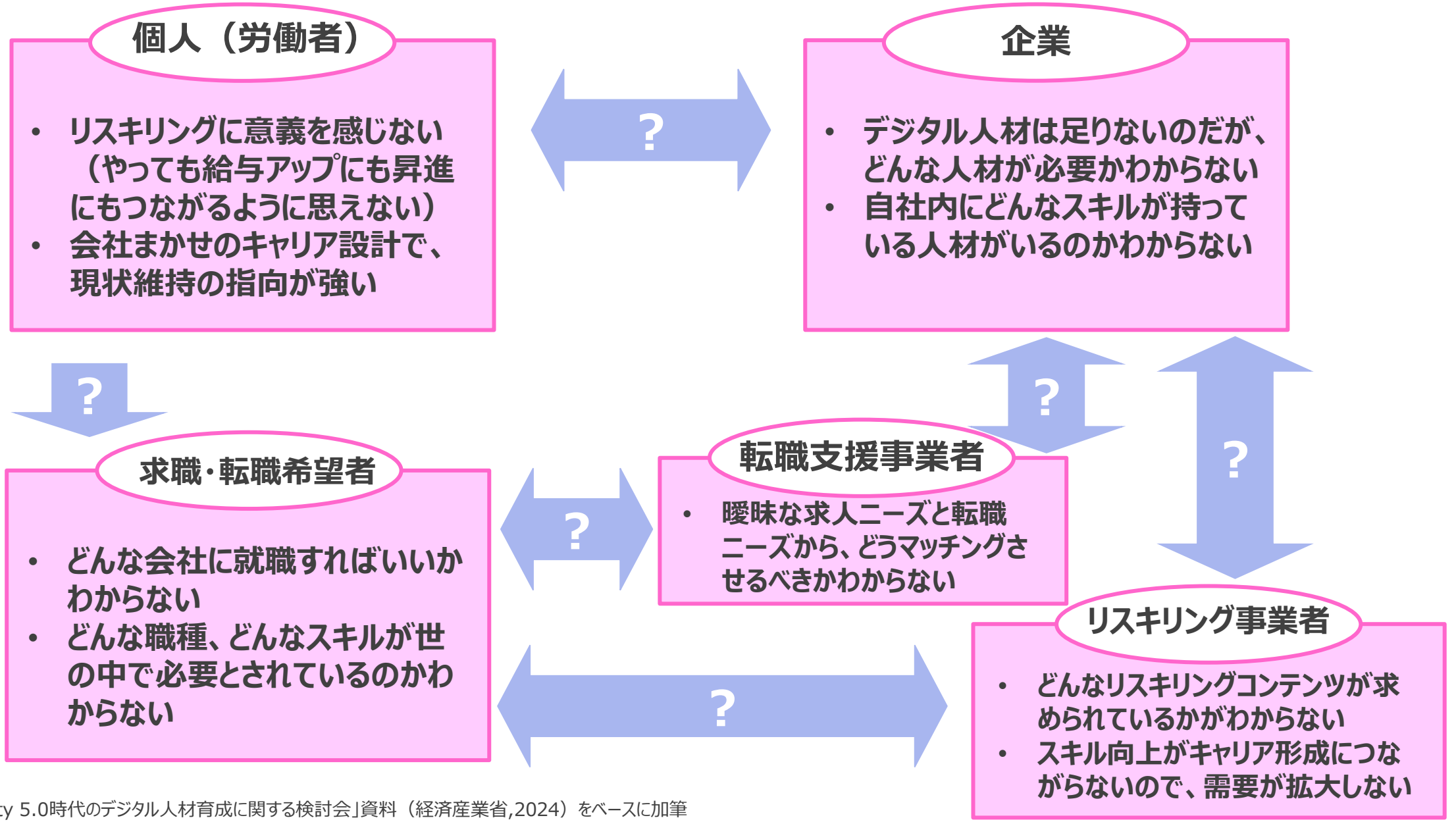
注：PDの科目A-1において基準点以上の成績を達成することでデジタル証明の発行を検討。
　　また、PDの3試験全てに合格することで「AI時代におけるフルスタックスキル」のデジタル証明の発行を検討。

＜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”

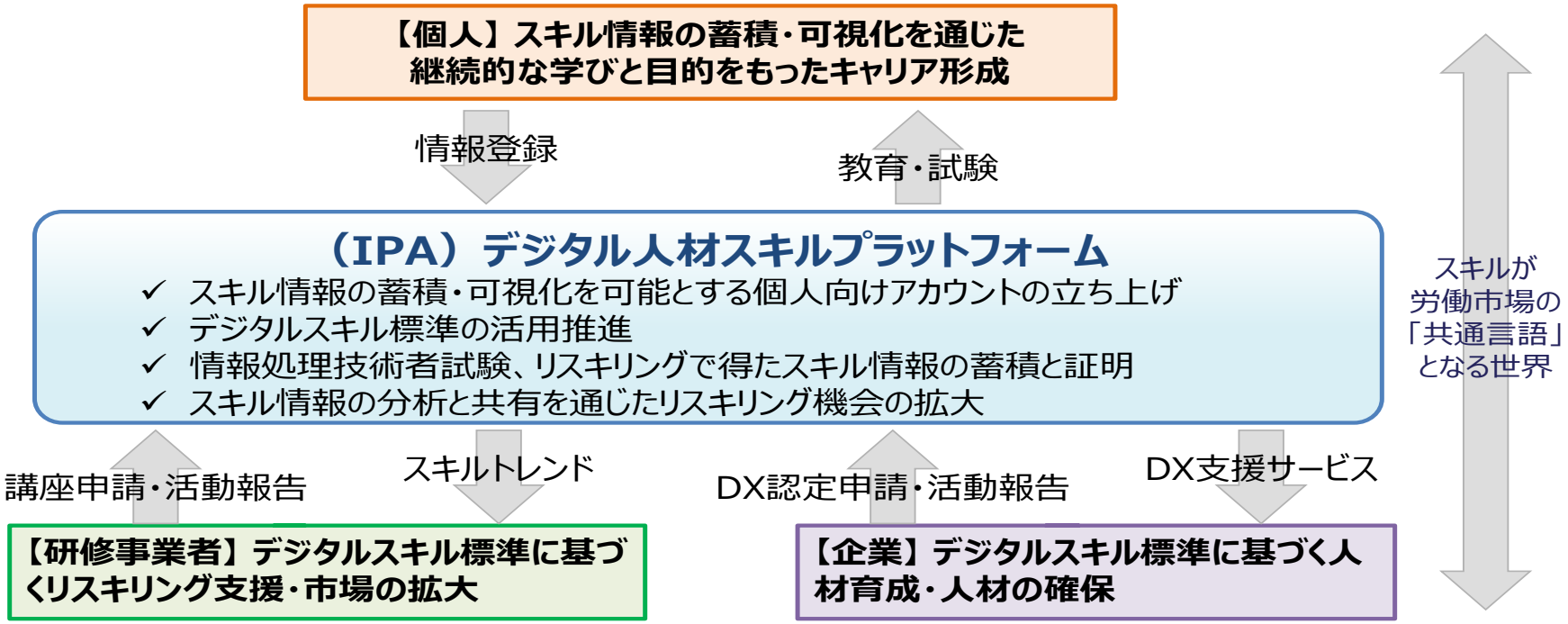
- 「事業推進上、必要になるスキル」に直結した採用が可能になる
- 自社の人材が保有しているスキルを把握し、適正に評価できるようになる
- 必要となるスキルを内部人材に取得させることができるようになる

- 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

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
- DXの延長上として、AX（AIを活用した企業変革）を視野に入れるべき。新しく公表される「デジタルガバナンスコード」に注目し、「DX銘柄」の取得等にもチャレンジしてほしい
- 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
- 企業に必要なスキルを特定し、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」、今後公開される「デジタルスキルプラットフォーム」を積極的に活用してほしい

Thanks for your attention !