資料３－２

デジタル・サイバーセキュリティWG
第１回　事務局参考資料

2026年2月3日
デジタル庁　経済産業省

（１）デジタル

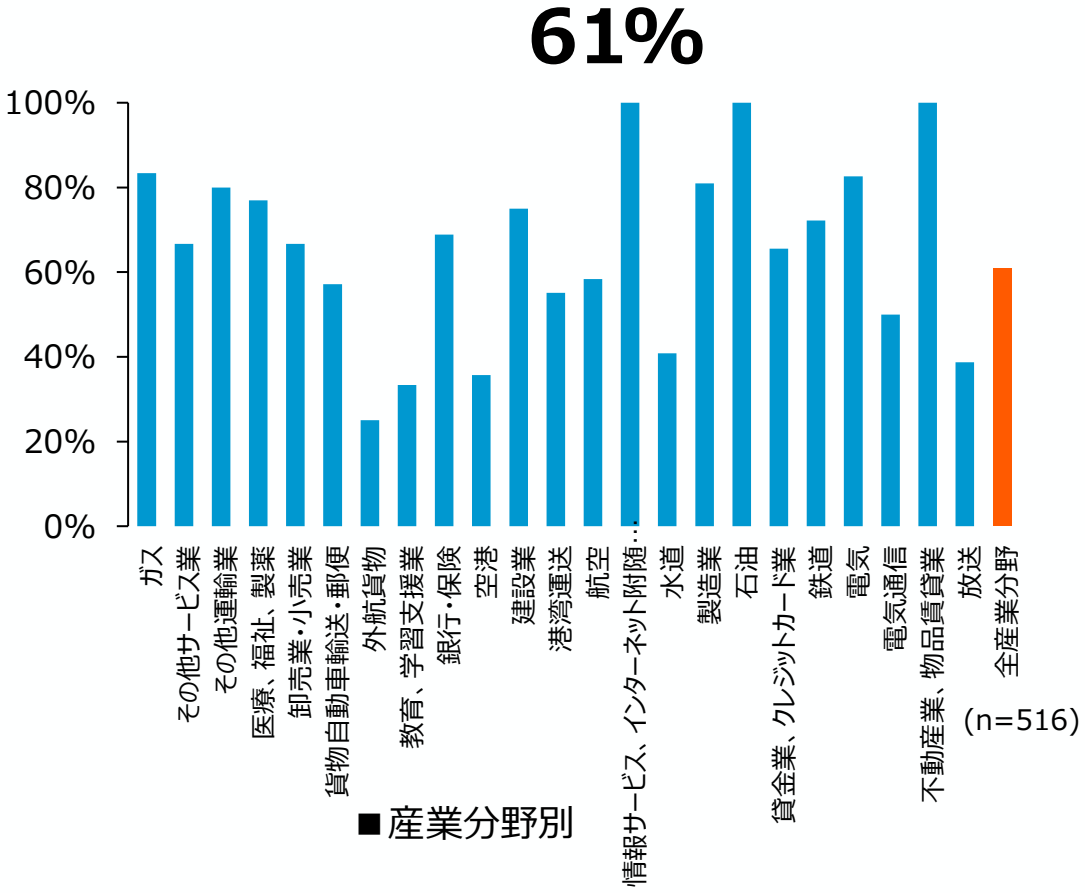
（２）サイバーセキュリティ

（３）公共・準公共

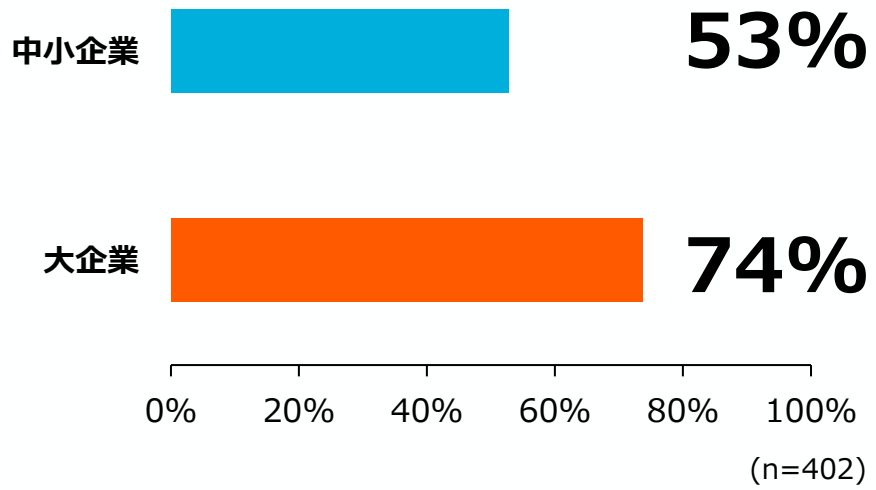
レガシーシステムの残存状況

○ 事業企業の**61%**が**レガシーシステム※を保有**している状況。中小企業よりも大企業の保有率が高い。
※：単に古いだけではない、維持保守や機能改良が困難で高コストの原因となり、経営・事業の足枷となっているシステムのこと。

○ 通常、**大規模なレガシーシステムのモダン化は数年計画におよび**、モダン化の着手後に問題化もしくは停滞等の要因により計画が見直されると、さらに長期間を要することになる。



■産業分野別



■企業規模別

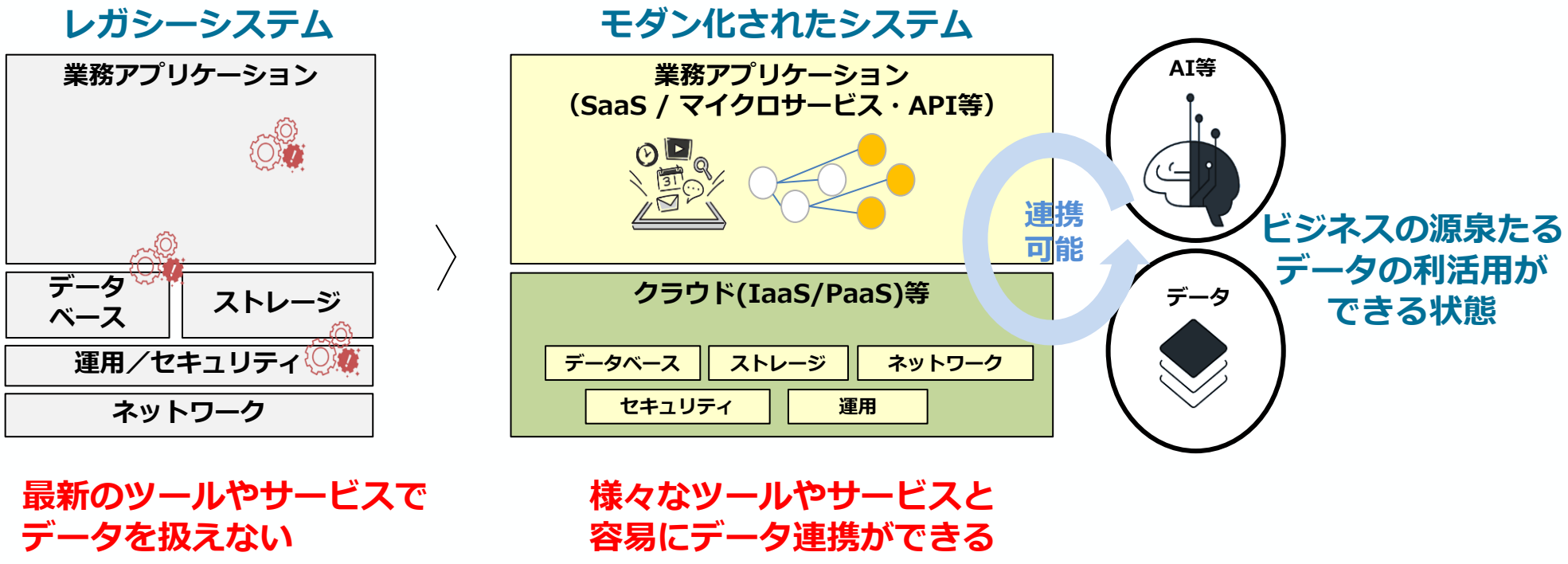
出典：レガシーシステムモダン化委員会総括レポート

レガシーシステムのモダン化の必要性

○ 技術変化に追従しなければ、**システムの保守期限の到来や機能改良の停止リスクあり**。

○ システムの作りやデータ形式が古いと、AI等の最新のツールやサービスで**データの利活用ができない**。

○ **変化への適応、データの利活用が可能な技術の導入(モダン化)**、継続的なアップデートが必要。



出典：レガシーシステムモダン化委員会総括レポート

経済安保法に基づく技術開発・計算資源整備支援（クラウドプログラム）

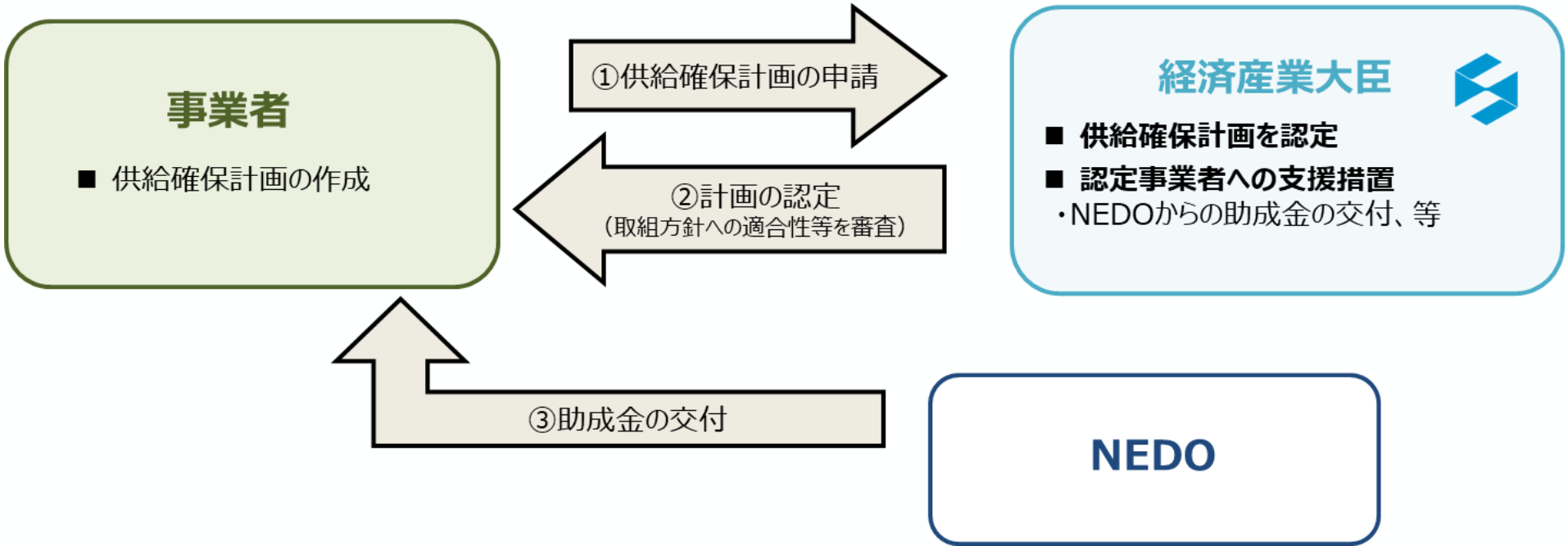
○ 経済安全保障推進法に基づく**特定重要物資**として**「クラウドプログラム※1」を政令で指定。**その安定供給確保のための民間の取組を支援する予算（基金）として、**R4年度補正で200億円を措置。**

※1：クラウドサービスの提供に必要なシステムに用いられるソフトウェアプログラムのこと。

○ 国内で重要情報を扱う事業者等がクラウドを安定的に利用できる状況を確保するため、**基盤クラウドプログラムの技術開発**に係る、**さくらインターネット社の供給確保計画**を認定。

○ また、**高度な計算資源を整備し、幅広いAI開発者等に提供する取組を計10件認定。**

経済安全保障推進法に基づく認定・支援に関するフロー



ワット・ビット連携

○ 今後、データセンターが急増する中で、**電力系統増強・脱炭素電源の活用が課題**。電力系統の先行的な整備を通じた、データセンターの大規模集積と適正立地を促すことで、電力・通信インフラ整備を効率的に行う**ワット・ビット連携**を実現する。
○ 具体的には、データセンターの大規模集積拠点の実現に向け、規制・制度改革と支援策を一体で措置する「GX戦略地域」制度を創設し、地域を公募中。

ワット・ビット連携

電力や通信等のインフラの一体的な整備「ワット・ビット連携」を通じたデータセンターの適正な立地促進

データセンターの電力需要の見通し（2025年1月時点）

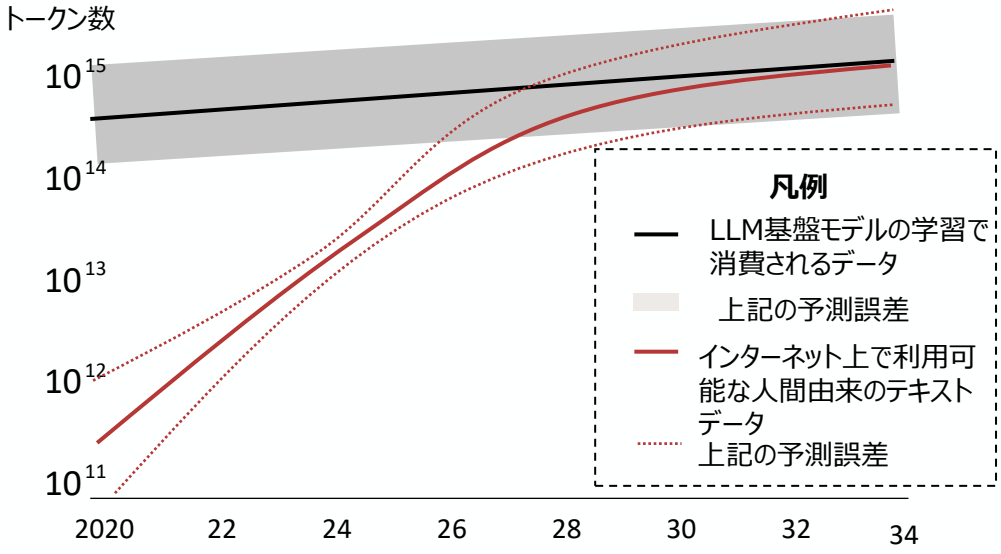
海外のDC集積事例（米国 バージニア州アッシュバーン）

AIの学習データの枯渇

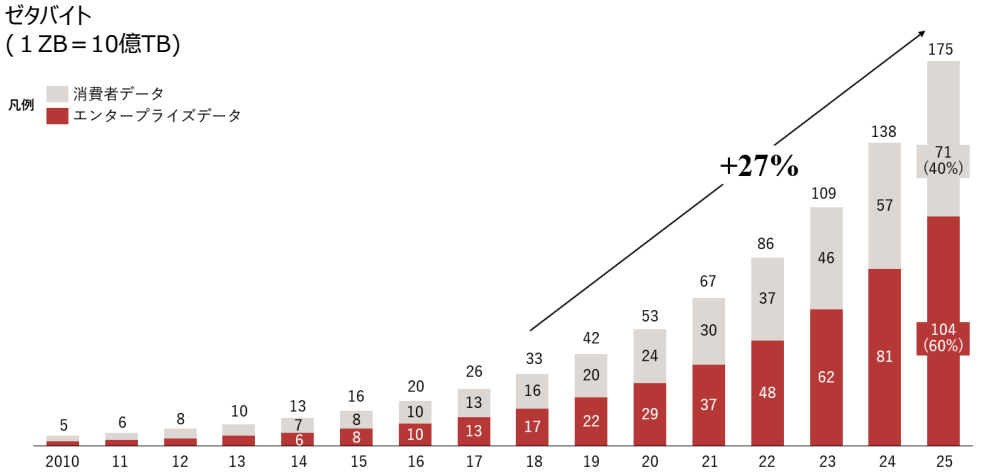
○ これまでインターネット上の大量のテキストデータを学習し、性能を向上させてきた**生成AIも、昨今では目前に迫っている「学習データの枯渇」が大きな問題になっている**。

○ 今後は、全世界で流通するデータの６割を占める**企業内データ（≒エンタープライズデータ）の利活用が産業戦略上の焦点**。特に、産業分野の豊富な**データを有する我が国にとってデータ活用のポテンシャルは非常に高く、そうしたデータをAIで利活用しやすい状態（AI-Ready化）に整備することが求められる。**

LLM基盤モデル学習におけるインターネット上のテキストデータ利用の予測 2022-34年(予測値ベース)



年間のデータ量（世界中で創出・取得・複製・消費されるデータ量）**の推移** 2010-25年 (予測値ベース)



（出典）The Digitization of the World From Edge to Core – IDC
（注）左図：IDCレポート内では、2018年に32ZB、2025年に175ZBのみ定量推測データが公開。上記グラフではCAGRを算出後、同一ベースで成長すると仮定し、2010年以降のデータを算出。
右図：2025年のデータについて、全体・金融・製造・ヘルスケア・メディアはレポート記載のCAGRをもとに算出し、その他産業は左記CAGRの平均値から算出。

データのAI-Ready化によるAIの向上

○ **現場の生データをAI-Ready化していくことで、精度が大幅に改善**されることが、ビッグテックや学術界の論文からも　多数報告されている。
○ 既に**製造業内でもAI-Readyなデータを整備し、AIモデル開発を目指す先進的な取組**も存在。

ビックテックや学術界の論文

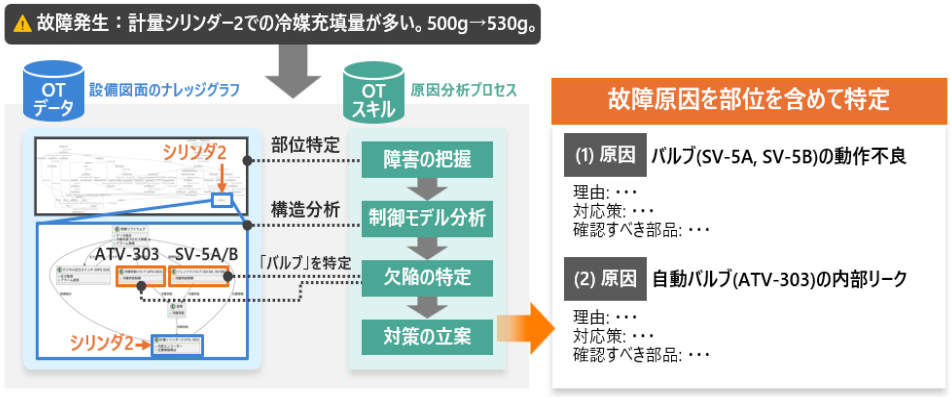
企業	タイトル	アプローチ概要	精度改善
OpenAI社	DevDay: “A Survey of Techniques for Maximizing LLM Performance” *1	RAGにおけるモデルへ与えるデータの改善をさまざま実施することで大幅な改善が見られた。例えば、チャンクサイズの最適化、リランキング、メタデータ付与、クエリ拡張、プロンプトエンジニアリング、データ取得のための外部ツールの活用など	**53ポイント改善**（45% -> 98%）
Anthropic社	Contextual Retrieval in AI Systems *2	チャンクの前後文脈を追加するなどのコンテキストデータを最適化する（Contextual Retrieval）ことで、RAG性能の向上	**取得失敗率改善**（5.7% → 1.9%）
カーネーギー大 などの共著	LumberChunker: Long-Form Narrative Document Segmentation *3	物語系長文（GutenQA）で、動的に“話の切れ目”を見つけて分割するなどし、情報検索精度を大きく改善	**7.37%改善**

*1：https://www.youtube.com/watch?v=ahnGLM-RC1Y
2：https://www.anthropic.com/engineering/contextual-retrieval
*3：https://arxiv.org/pdf/2406.17526

製造業の事例

設備故障診断AIの開発

- 日立とダイキンが共同で、工場の設備故障診断AIエージェントの試験運用を開始
- 「OTデータ」と、設備故障原因分析プロセスである「OTスキル」を組み合わせたAIで、**ダイキンの一般的な保全技術者と同等以上の故障診断を実現**

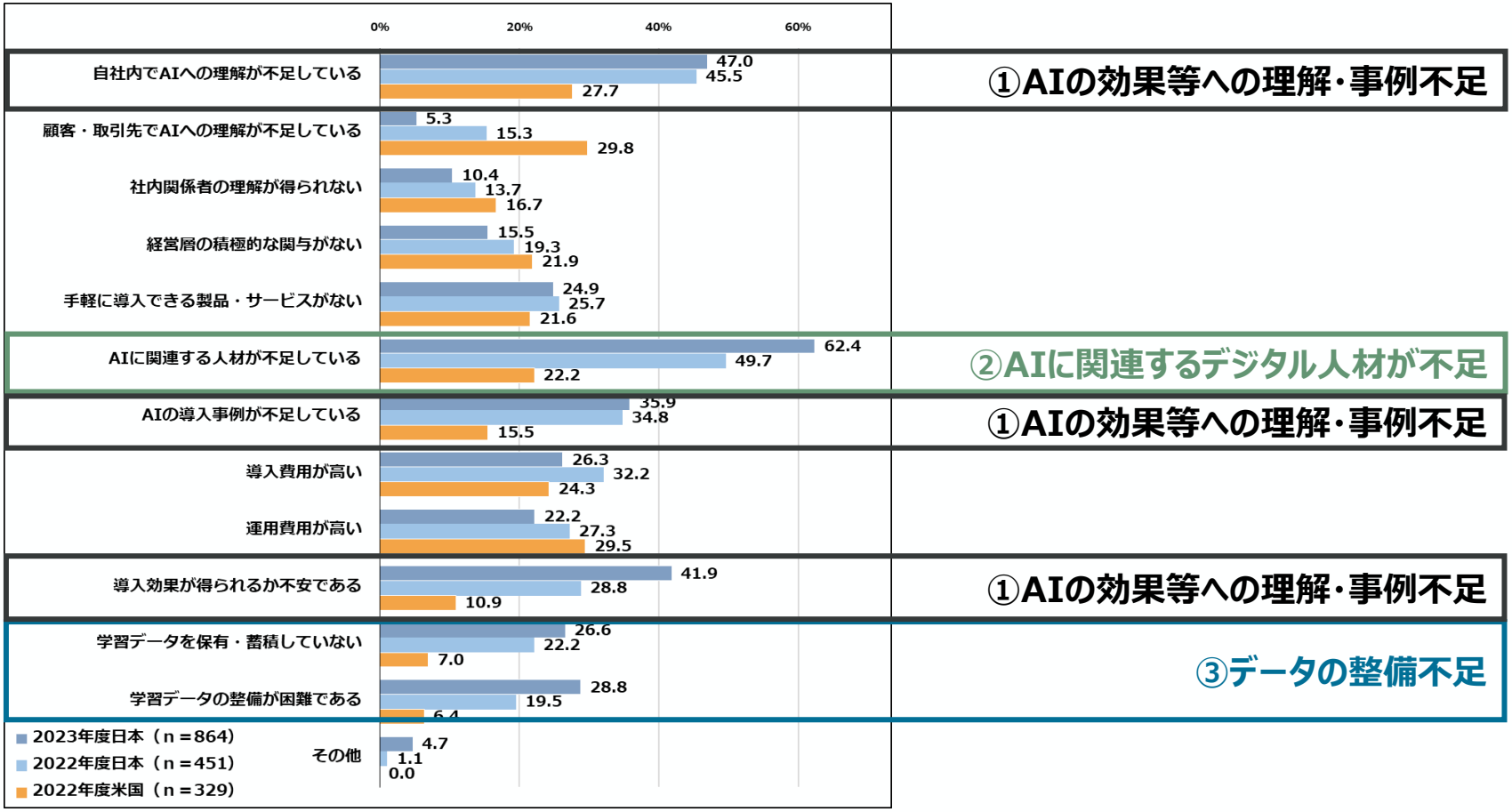


（出典）FastLabel社作成資料

企業内のデータ・AI利活用に関する課題

○ AI導入やDXにおいては、**データ整備に加え**、**AIの効果等への理解不足、デジタル人材不足が主な課題に。**

AIの導入課題（経年変化および米国との比較）



出典：DX動向調査2024, IPAより

製造業データ等のAI-Ready化の推進

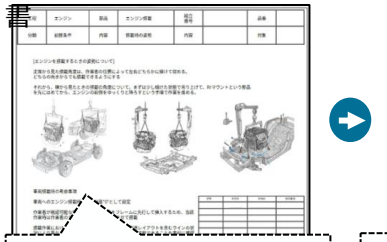
○ 製造業等の企業内データのAI活用を進めていくにあたり、データを意味・関係性付けし、AIが理解しやすい高品質データとして管理していく**AI-Ready化が不可欠**。
○ セキュリティ・ガバナンスの観点も踏まえつつ、**AI-Ready化手法の確立・標準化を支援することにより、サービサーを育成し、取組を面的に進めていくことが重要。**

■ **データセキュリティ・ガバナンス**
（統一された管理/継続的な改善）

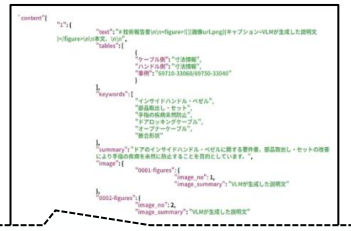
- 匿名化、暗号化などデータ保護のための処理
- データの利用権限や利用使途の管理　等

■ **AIが理解できるデータへの変換※**
（分かりやすい構造/適切なサイズ/意味付け/高い品質）

例：手順書

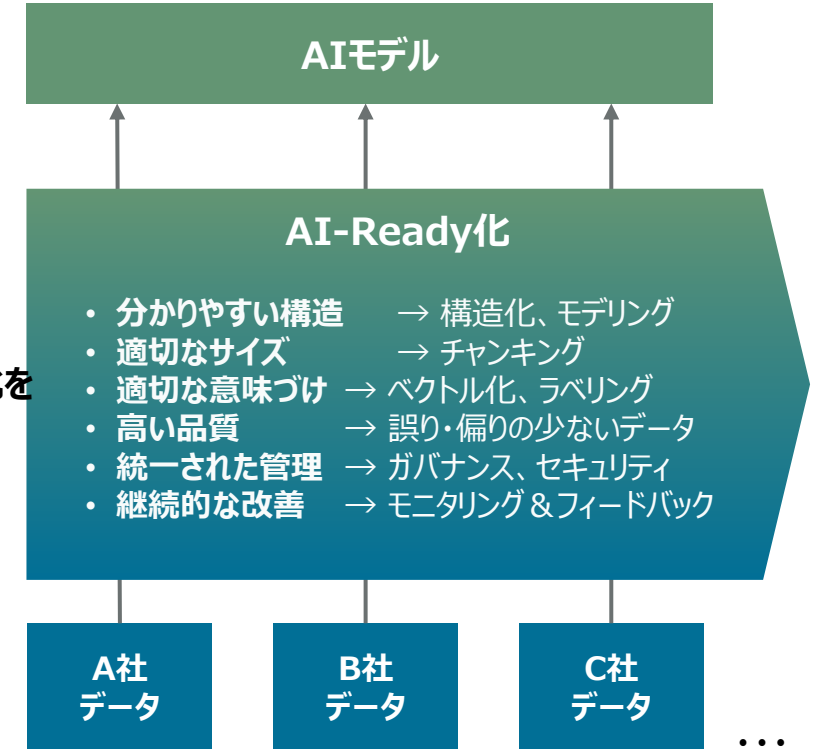


専門的な知見（図面の読み方・部品知識等）がなければ読解しにくい



データの意味情報
- 手順番号、図の説明
- 関連する部品情報（寸法等）　等

手法を標準化し、面的にAI-Ready化を推進

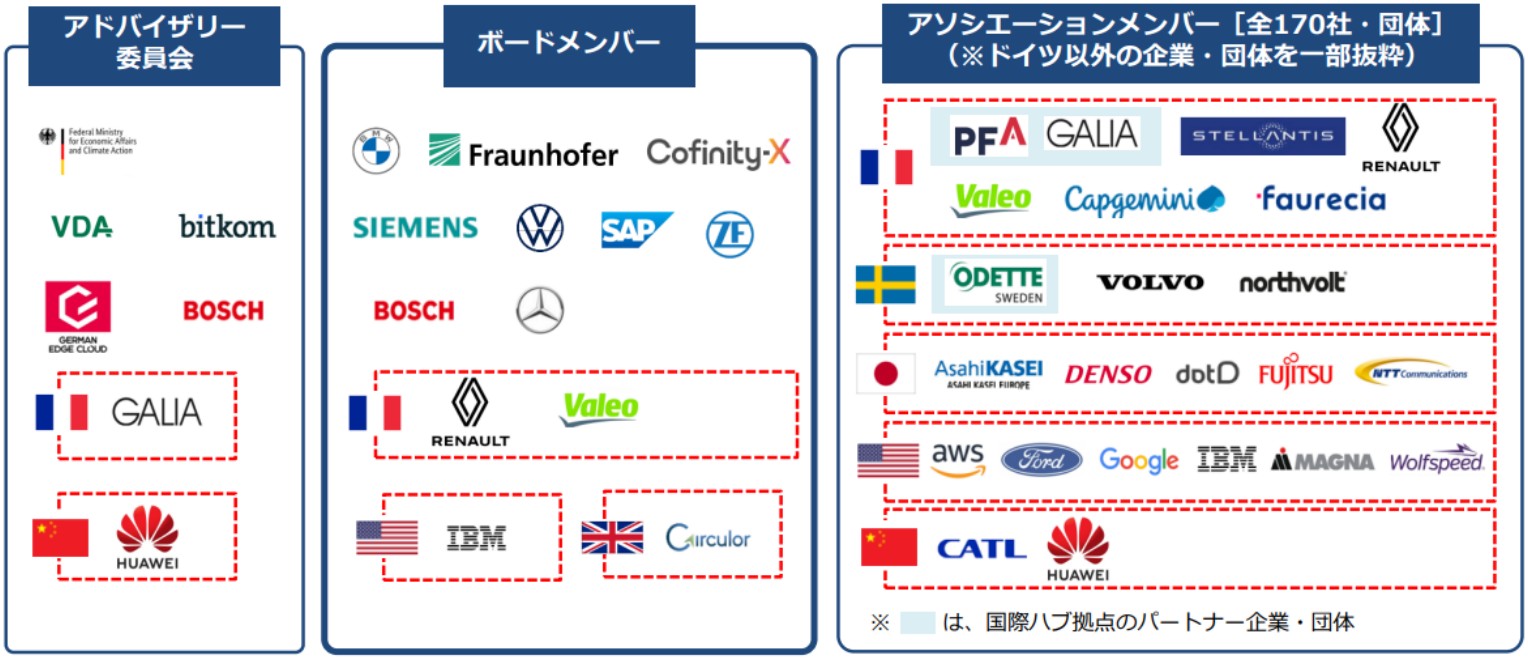


出所：フライウィール社資料より作成

データスペースに関する欧州の動向

○ 19年10月、ドイツ・フランス両政府は、**欧州独自のデータインフラ構築に向けたプロジェクトとして GAIA-X構想を発表**。21年1月、独仏の企業や研究機関によってGAIA-Xが設立。
○ GAIA-Xのうち、 BMWやSAP等によって推進される**自動車向けデータエコシステムに係るプロジェクトであるCatena-X**が、**欧州政府による巨額の支援**（約１億ユーロ＝約172億円）を受けながら、23年５月に本格稼働。
○ 制度面においては、**欧州委員会がデータ主権の原則に基づき25年９月にデータ法を施行**。

Catena-Xの主な参画企業・団体



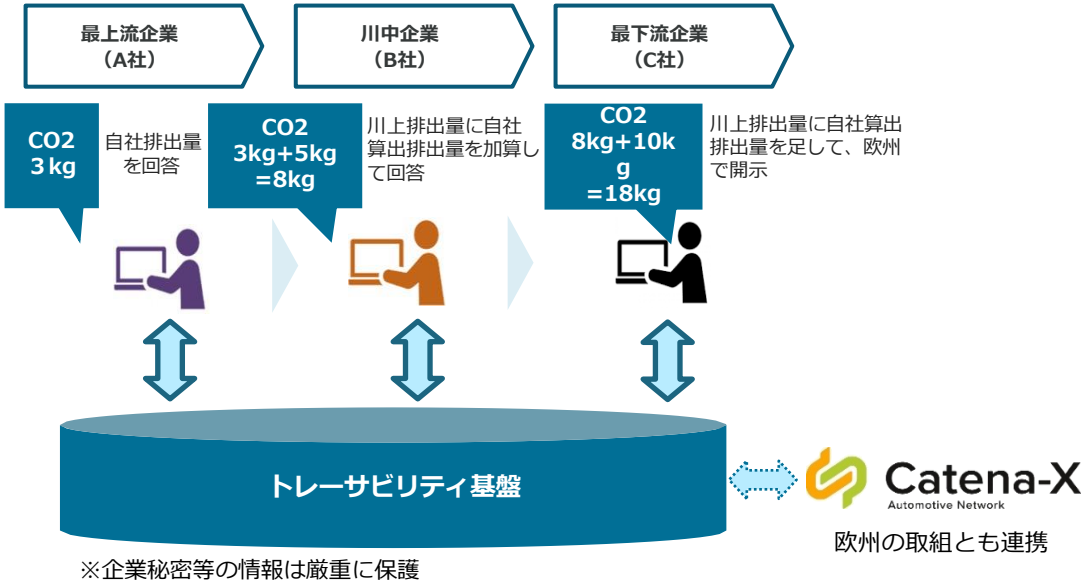
（資料）Catena-X資料より作成

企業や業界を越えたデータ連携による社会課題への対応①

○ データ連携を通じて新しい価値を生み出す企業間連携の取組を**「ウラノス・エコシステム」**と名付け、官民で連携し推進。

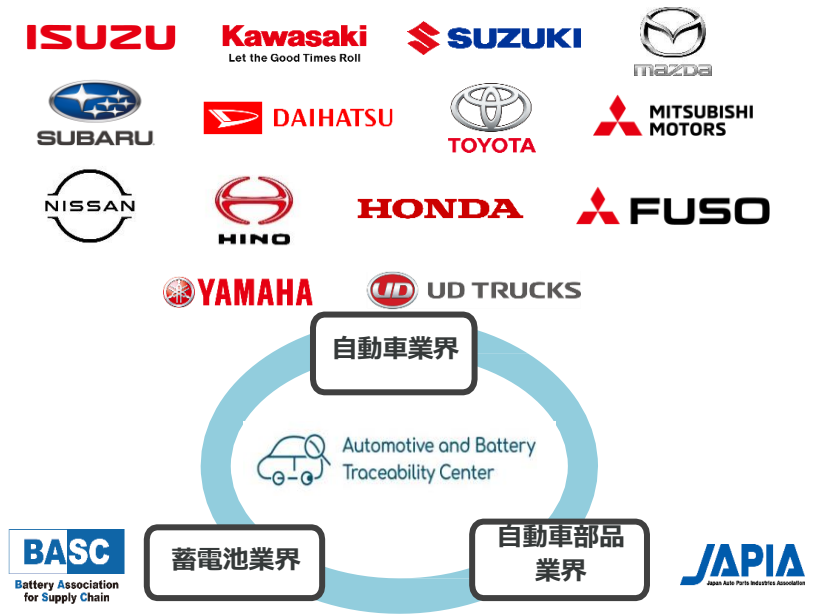
○ まずは、具体的な取組として、**CO2排出量の管理などを実現するための、自動車・蓄電池のデータ連携基盤**を構築。この取組をモデルとして、今後、化学物質管理などの**他分野での展開や、国際連携を推進**。

CO2排出量管理などのための、自動車・蓄電池のデータ連携基盤を構築



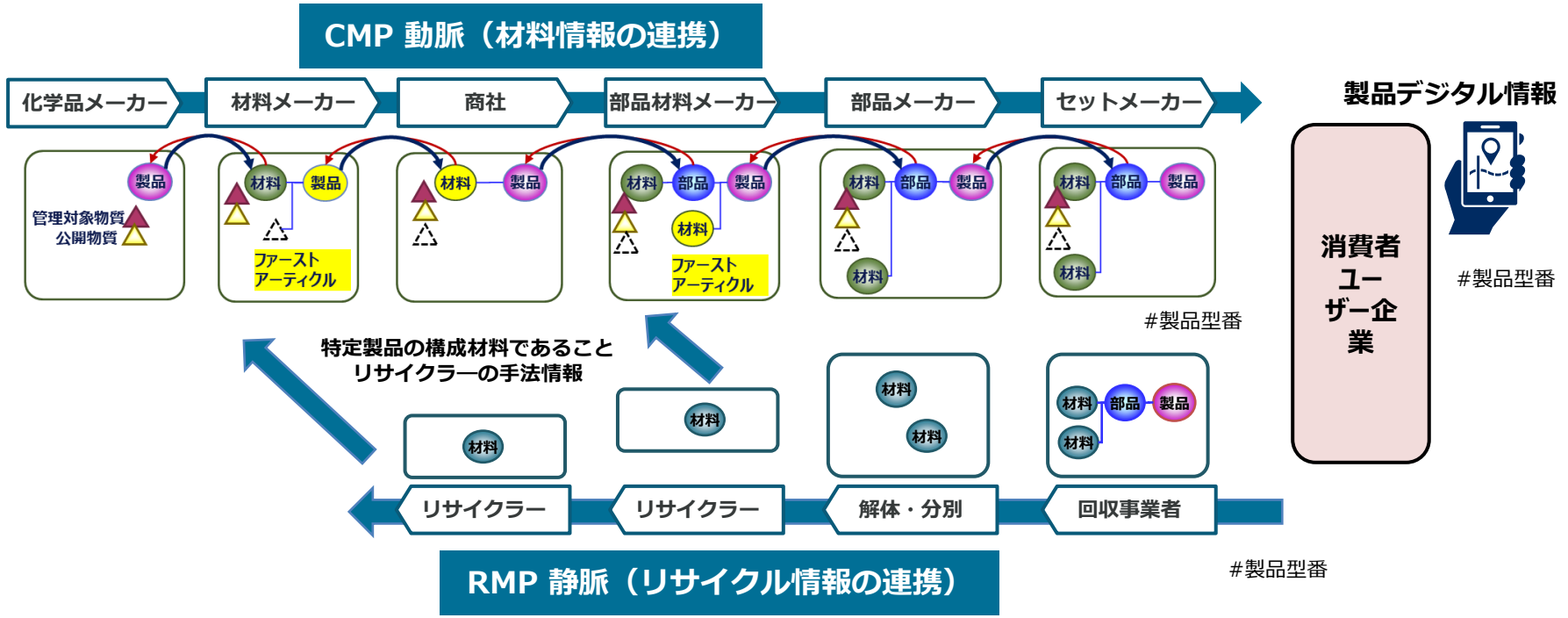
※企業秘密等の情報は厳重に保護

システム運営の担い手として、各業界団体が共同で「一般社団法人自動車・蓄電池トレーサビリティ推進センター(ABtC)」を設立



企業や業界を越えたデータ連携による社会課題への対応②

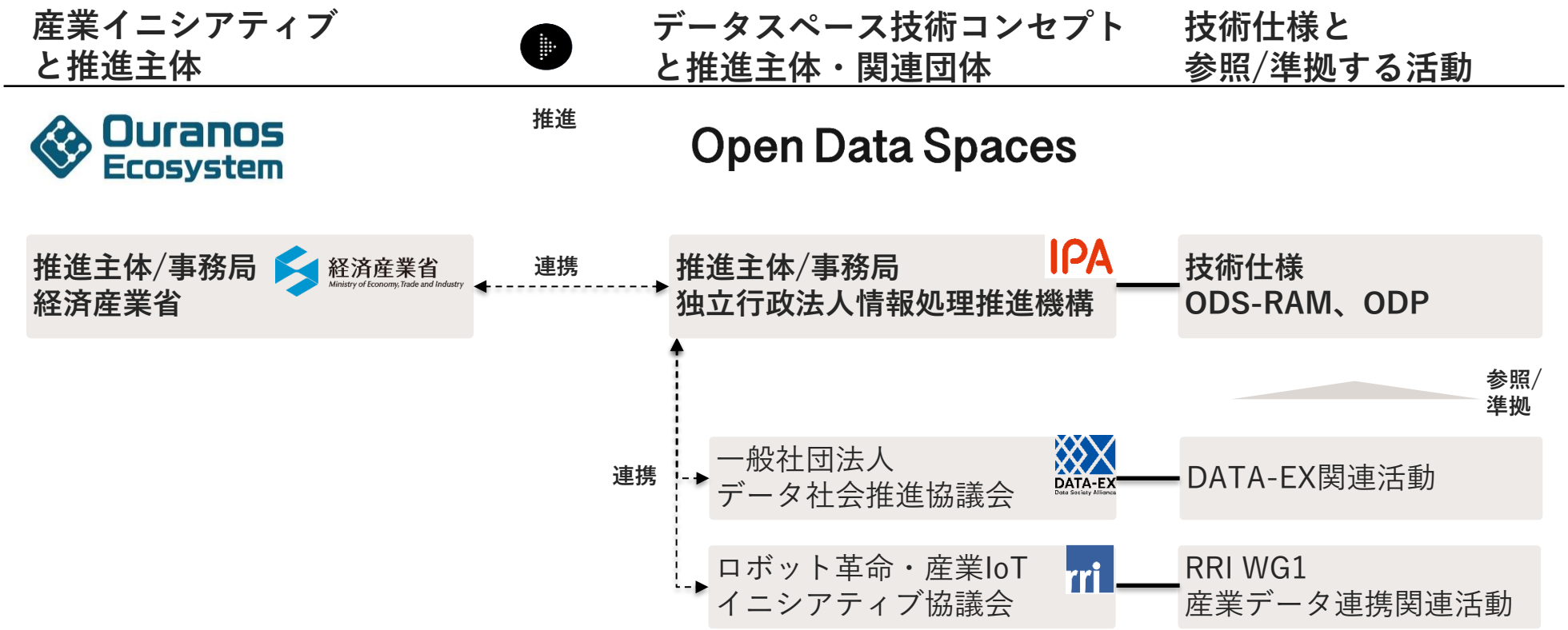
○ 諸外国による規制や囲い込みの動きに適切に対応し、**日本企業が諸外国の制度・PFに依存することなく我が国として対等な関係性を確保するための取組**が必要。特に、**化学物質管理等の資源循環分野での欧州規制等に対応することが急務**。
○ 今後は、新たに**製品含有化学物質のトレサビシステム（CMP）構築**し、**国際相互運用性の確保**等を目指していく。



- CMPタスクフォース｜CMP構想の進捗について（次世代化学物質情報伝達システムについて）
https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/chemicals/pdf/002_08_00.pdf を基に経済産業省作成

データスペース技術に関する取組

○ **信頼を伴ったデータ流通・活用環境としての「データスペース」技術**に関する日本発の共通仕様を「**Open Data Spaces**」と位置付け、**OSS（オープンソースソフトウェア）としての技術開発や国際標準化等を、IPAを事務局としてワンチームとして推進していくことを2025年10月に発表**。



デジタルエコシステム官民協議会の概要

○経団連の提言を踏まえ、2025年6月20日に発足。
○官民で連携し、**信頼あるデータ連携の仕組みであるデータスペースの技術標準化や基盤整備（法人ID等の整備）、産業利用の具体事例の組成**を促進。

＜委員構成組織＞

属性	参加主体
行政	デジタル庁※
	IPA※
	経産省
	総務省
民間	経団連※
	デジタル政策フォーラム（DPFJ）
	デジタル社会推進協議会（DSA）
	デジタルトラスト協会（JDTF）
	ロボット革命・産業IoTイニシアティブ協議会（RRI）

※官民協議会事務局

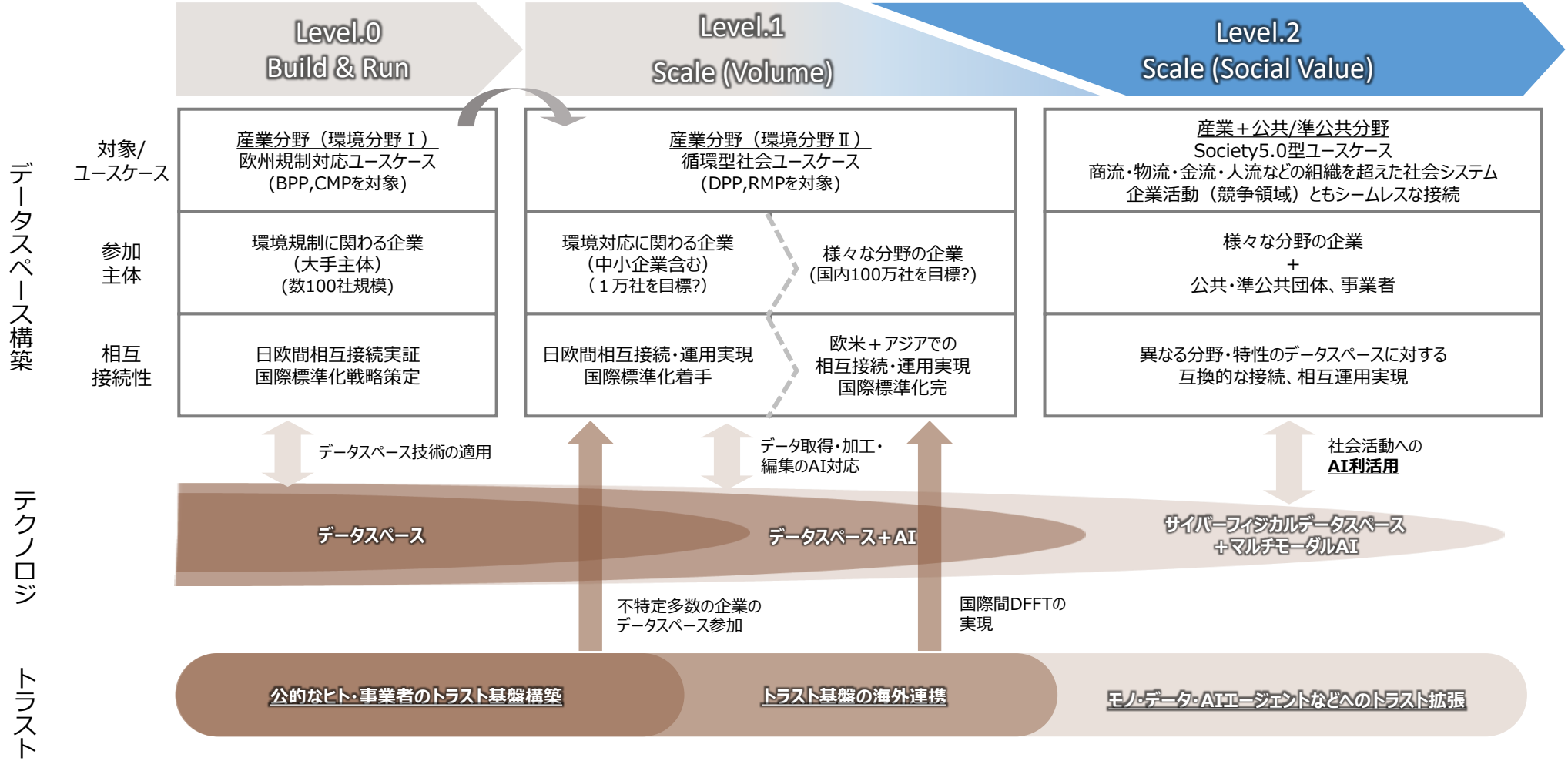
＜活動の方向性＞

取組分野	取組の方向性
データ連携のユースケース創出促進・参加組織拡大	社会的要請・国際的ニーズの高い環境分野をはじめ、データスペースの成功事例を創出
データスペース標準化・国際連携推進	データスペースの技術コンセプト・仕様の共通化を起点に、参照実装OSSの展開、国際相互運用性の確保、国際標準化を推進
データ連携における「トラスト」の整理	データ連携に係る国内のトラストサービスを整理・体系化、海外データスペースへのアクセスに係る論点を整理

デジタルエコシステム構築の全体像

2026年1月21日
デジタルエコシステム官民協議会
幹事会資料より抜粋

○ デジタルエコシステム構築に向けては、データスペース構築・テクノロジ開発・トラスト基盤構築の３テーマを連携させながら推進する必要。多岐に渡る活動を戦略的に推進するために、官民一体となり活動していく。

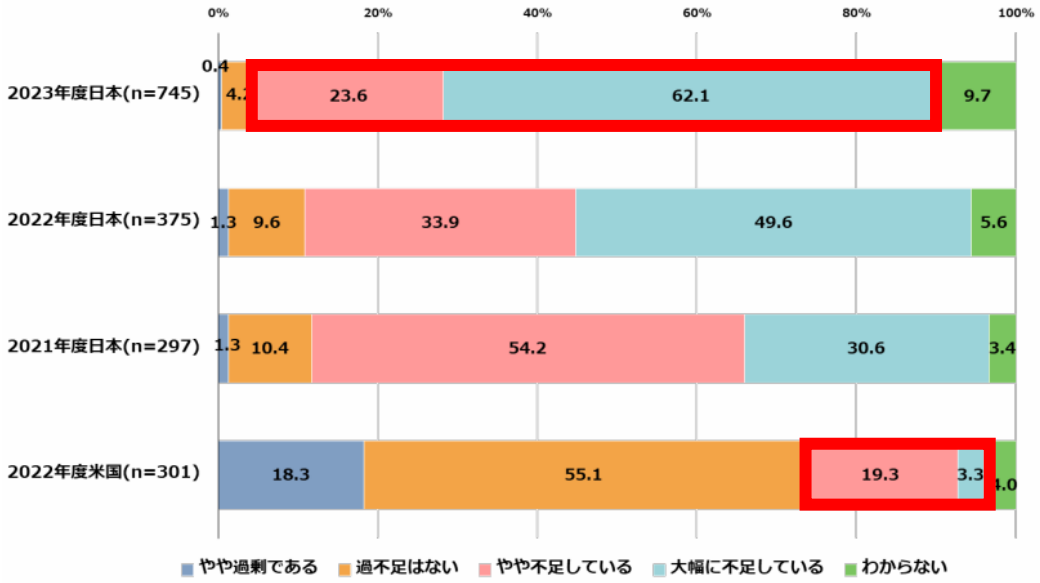


DX人材の量的不足

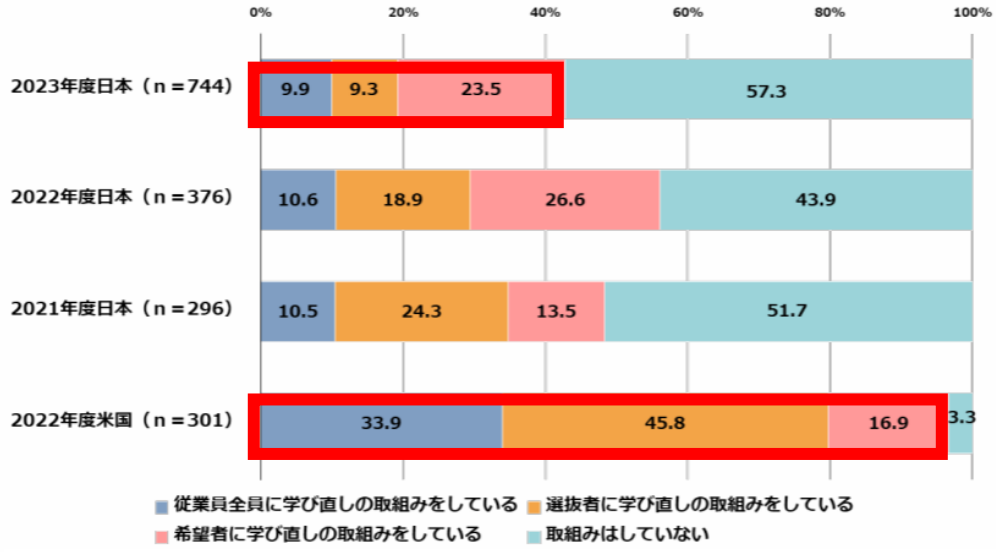
○ DXが進まない１つの要因として、日本では**85.7%の企業がDX人材不足を感じている（米国は22.6%）。近年「大幅に不足している」企業割合が急速に増加**しており、**企業ニーズに人材育成が追い付いていない状況**。

○ その一方で、何かしら社員の学び直しの取組をしている日本企業は2022年度から2023年度にかけて**減少しており**（56.1%→42.7%）、**半数以上が取組をしておらず、また全社的な取組も１割に留まる。米国では９割以上が学び直しを実施していることと比較すると日本との差は依然として大きい**。

DXを推進する人材の「量」の確保
（経年変化および米国との比較）



学び直し（リスキル）の取組状況
（経年変化および米国との比較）



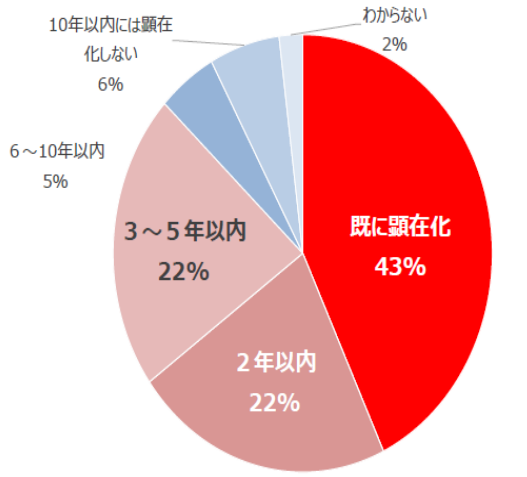
（出典）DX動向2024／情報処理推進機構（IPA）

日本型雇用システムにおける人材育成の現状について

○ 多くの企業で学び直しが必要と認識しているにもかかわらず、**諸外国と比べて、日本では企業も人材投資が少ない。また、日本人には学び直しという習慣が根付いていない**。

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。

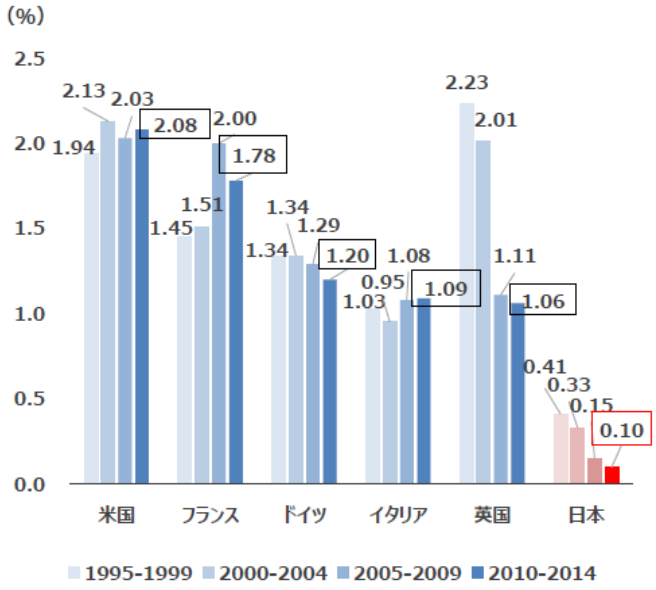
スキルギャップが顕在化する時期



（出所）McKinsey & Company “Beyond hiring: How companies are reskilling to address talent gaps”を基に経済産業省が作成。

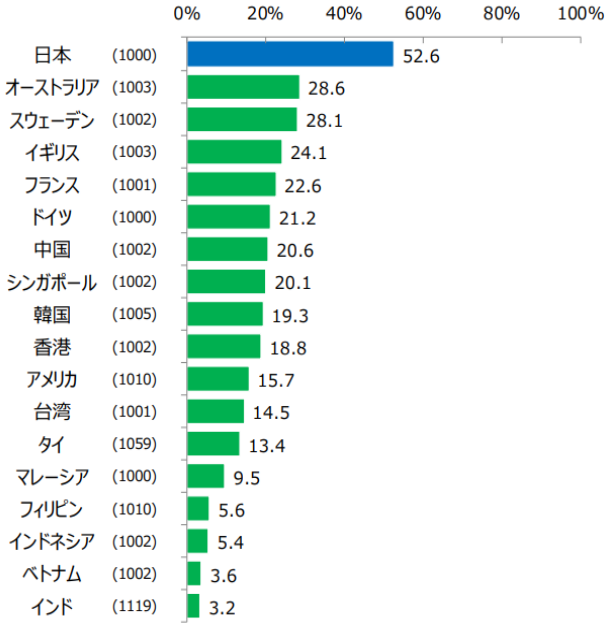
企業は人に投資せず、個人も学ばない。

人材投資（OJT以外）の国際比較（GDP比）



（出所）学習院大学宮川努教授による推計（厚生労働省「平成30年版 労働経済の分析」に掲載）を基に経済産業省が作成。

勤務先以外で社外学習・自己啓発していない人の割合



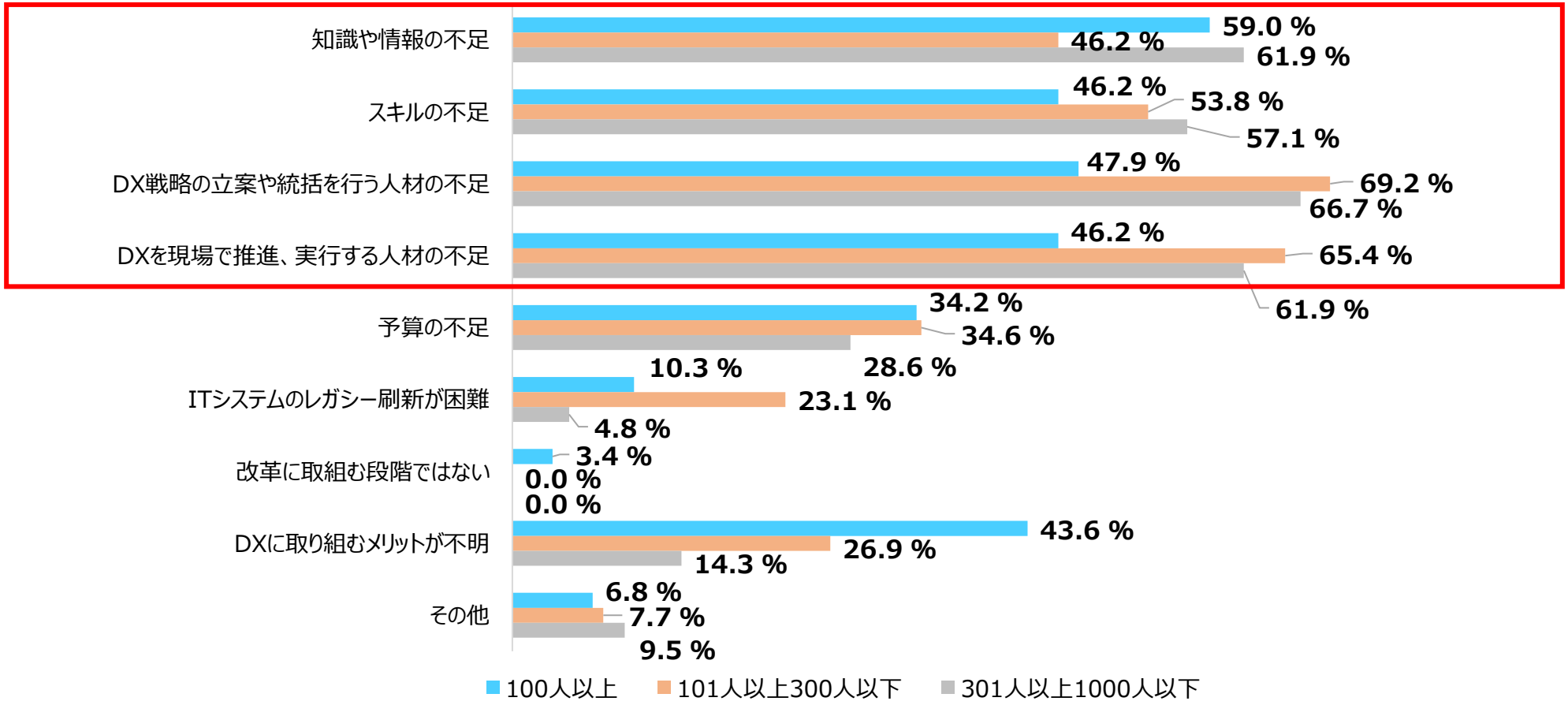
出典：パーソル総合研究所「グローバル就業実態・成長意識調査－はたらくWell-beingの国際比較」

出典：令和4年5月　経済産業省「未来人材会議　中間取りまとめ（https://www.meti.go.jp/shingikai/economy/mirai_jinzai/pdf/20220531_1.pdf ）」抜粋他

DXに取り組まない理由

○ 企業のDX推進の主な課題として、「人材不足」「知識・情報不足」「スキル不足」が上位に来ている。

○ 今日では、人材の育成確保、経営者・企業の意識改革がＤＸ推進のために重要となっている。



（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」を基に作成。

情報処理技術者試験の見直し概要（検討案）

○ DXの推進に必要となる**データ活用やデジタル技術は進化**しており、これに対応するスキルも変化しており、この**変化に柔軟に対応するため**には、**「土台」となる幅広いスキルを身につけることが必要**。

○ このため、**情報処理技術者試験**は、スキルの変化に柔軟に対応するため、幅広いスキルを身につけ、スキルベースで評価するための**試験体系に見直しを検討**。**2027年度開始**を目指す。

○ **「土台」としての国家試験**と、**先端的・実践的な民間学習サービス**をIPAにおいて検討している**「デジタル人材スキルプラットフォーム」を介して相互補完**し、スキルを可視化することで、**継続的な学びにつなげる**。

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・高度試験 再編

スキルの変化に柔軟に対応できるように、「土台」となる幅広いスキルを身につけるため、**応用情報技術者試験と高度試験**を**マネジメント・監査**、**データ・AI**、**システムの３領域に大括り化**し、**３試験に再編。３領域の習得を推奨**。

試験実施方法 変更

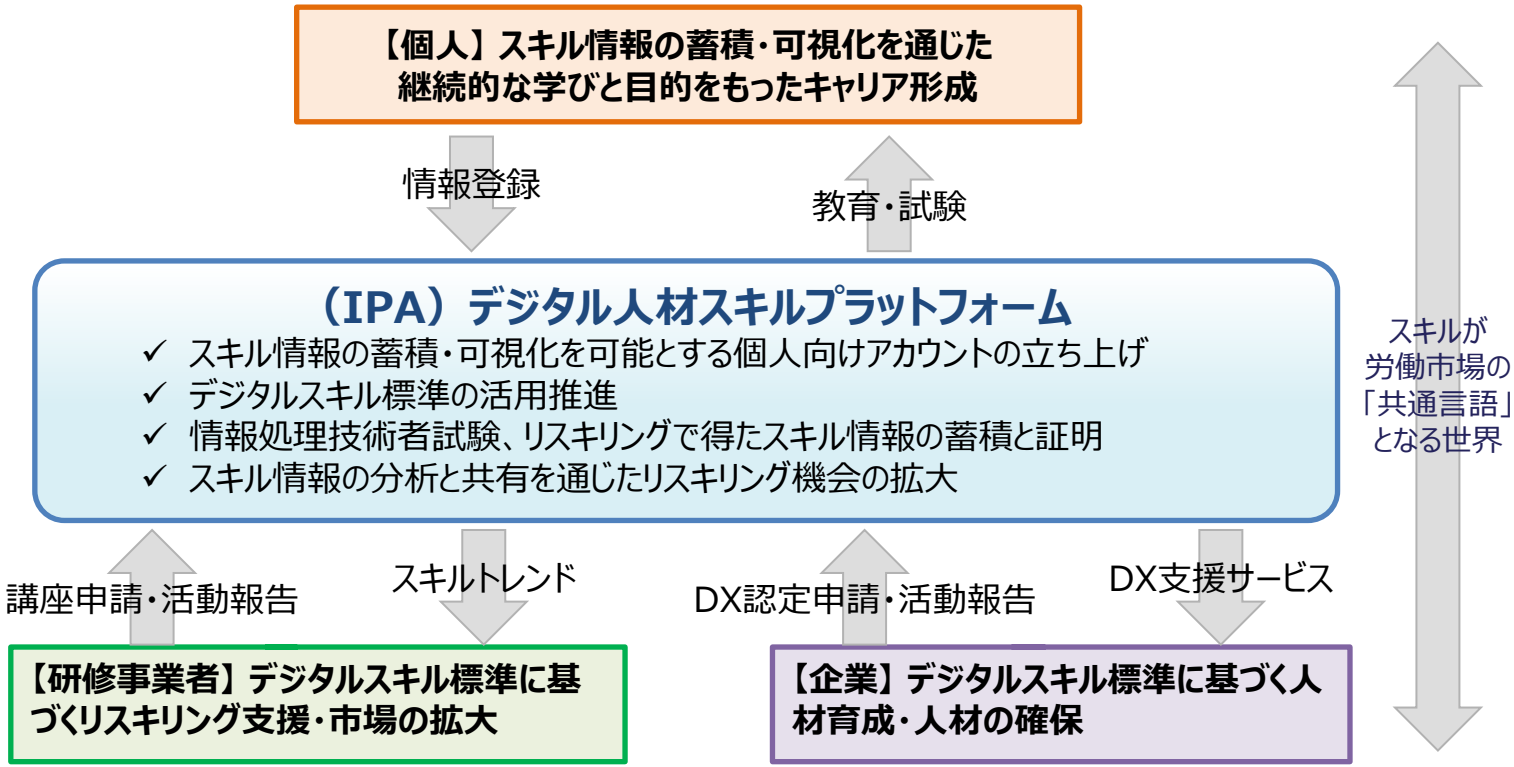
2026年度から、現行の全試験区分をペーパー方式からCBT方式※による実施方法に移行。**応用情報・高度試験**は、**見直し後の試験をCBT方式に適した出題方式へ見直し**。**論述試験のあり方**は、2028年度以降に向けて**継続検討**。

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

デジタル人材スキルプラットフォームの構築

○ 自身の目標に向けて**スキルアップを続けるデジタル人材が一層活躍できる環境整備が必要**。

○ **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**」の検討を進め、**令和８年度内のサービス構築**を目指す。



未踏事業の二期制の開始

○ 未踏事業のさらなる拡大に向けて、未踏ADの二期制（上期・下期）が2025年度よりスタート。

○ **<u>二期制の育成規模を段階的に拡大する</u>**べく、**<u>ＰＭの確保等、運用体制の強化</u>**等を今後実施。

これまでの未踏事業

MITOU 未踏IT人材発掘・育成事業

MITOU TARGET 未踏ターゲット事業

MITOU ADVANCED 未踏アドバンスト事業

年間で3つのコースを同時進行で人材育成を実施

これからの未踏事業

MITOU 未踏IT人材発掘・育成事業

MITOU TARGET 未踏ターゲット事業

MITOU ADVANCED 未踏アドバンスト事業

上期

MITOU ADVANCED 未踏アドバンスト事業

下期

未踏AD事業に新たに下期を追加。**<u>年に2回の公募機会</u>**を設けより多くの挑戦を支援。

未踏ADを支えるPM陣

未踏的な地方の若手人材発掘育成支援事業（AKATSUKI）

	日本全国版 未踏事業	地方地域版 AKATSUKIプロジェクト
目的	**IPAが中心となり、日本全国から新たな価値を創造するIT人材を育む** ITを駆使してイノベーションを創出することのできる独創的なアイディアと技術を有するとともに、これらを活用する優れた能力を持つ、突出した人材を発掘・育成[*1]	**地方・地域コンソーシアムから新たな価値を創造するIT人材・起業家を育む** 未踏事業の人材発掘・育成プログラムを全国各地においても広く展開し、地域における若手人材の自律的・継続的な育成活動の面的拡大を目指す
特徴	**❶日本を代表する各分野で活躍するPMが帯同** **❷2000人以上の未踏修了生のコミュニティ** ・2000年以降25年間続く歴史ある事業	**❶各地域ごとに異なる支援メニューを用意** **❷地域貢献・活性/地域から社会→世界へ**
人材像	**未踏的なアイデアを育てたい** ・アイデアがある・技術がある・情熱がある 「独自性・革新性があり、社会的インパクトを与え、イノベーションを創出する可能性を秘めたプロジェクト実現しようとしている若い逸材」[*2]	**地方発の未踏的なアイデアで課題解決にも取り組みたい** 左記の未踏性を有するほか、地域や特定のコミュニティに対する貢献（課題解決、起業等）マインドを有する者

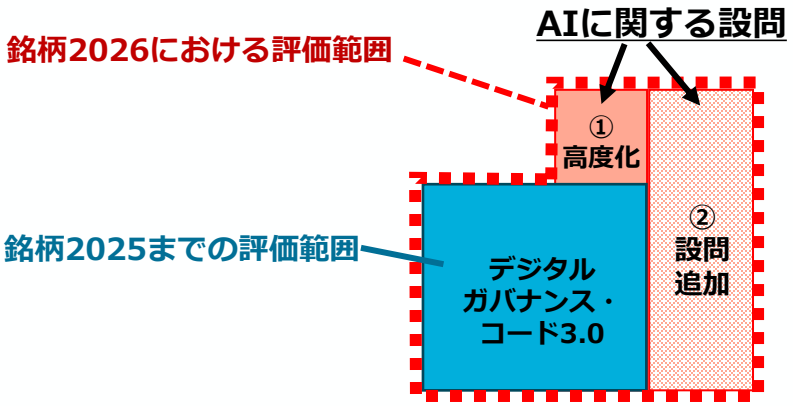
[*1]出所：IPA、「未踏事業について」、2024、https://www.ipa.go.jp/jinzai/mitou/about.html（参照2024-02-29）
[*2]出所：IPA、「未踏IT人材発掘・育成事業について」、2024、https://www.ipa.go.jp/jinzai/mitou/it/about.html（参照2024-02-29）

DX・AIXの更なる可視化（ＤＸ銘柄の変革）

○ **DX銘柄2026**では、**AIの利活用を前提に、AIの急速な技術進歩をとらえつつ、機動的・抜本的に、変革の”範囲”を拡充し、その”質”、”スピード”を高める企業を一層評価**する。

○ 今後、我が国社会・産業界が抱える課題へのDX・AIXの寄与を定量的に示し、日本全体でDX・AIXに取り組む環境を醸成した上で、**企業におけるDX・AIXの更なる可視化を目指す**。

DX銘柄2026における評価範囲



＜例＞①高度化（選択肢の追加）
- AIの利活用を前提とした変革を含むDXの推進に向けた経営ビジョンを策定できている。

＜例＞②設問追加
- AIでの利活用を可能にするデータ環境を整備できていますか。
- AIに関するリスクに対応するため、ライフサイクル管理を含む、安全性（データ保護を含む）等を確保する仕組み・体制を構築していますか。

更なる可視化に向けて

＜2026年＞
DX銘柄2026
※AIに関する設問を追加

社会・産業界が抱える課題へのDX・AIXの寄与を定量的に示す

＜2027年以降＞
企業におけるDX・AIXの更なる可視化

＜2027年以降＞
DX・AIXの取組が進む事業者への支援の重点化

「デジタル化・AI導入補助金」の概要（令和7年度補正）

○ IT導入補助金は、中小企業・小規模事業者等の労働生産性の向上を目的として、**デジタル化やＤＸ等に向けたITツール（ソフトウェア、サービス等）の導入を支援**する補助金。

○ 令和7年度補正予算分からは、**「デジタル化・AI導入補助金（旧：IT導入補助金）」**と名称を変更。詳細は調整中。

（以下、IT導入補助金2025の概要）

	通常枠	複数社連携IT導入枠	インボイス枠		セキュリティ対策推進枠
			インボイス対応類型	電子取引類型	
活用イメージ	ITツールを導入して、**業務効率化やDXを推進**	商店街など、**複数の中小・小規模事業者で連携して**ITツール等を**導入**	ITツール等を導入して、**インボイス制度に対応**	発注者主導でITツールを受注者に共有し、**取引先のインボイス対応を促す**	**サイバーセキュリティ対策を進める**
対象経費	ソフトウェア購入費、クラウド利用料（最大2年分）、**導入関連費**（保守運用やマニュアル作成等のサポート費用と、IT活用の定着を促す導入後の”活用支援”）**も対象** 単独申請可能なツールの拡大	ハードウェア購入費		クラウド利用料（最大2年分）	サイバーセキュリティお助け隊サービス利用料（最大2年分）
補助上限	ITツールの業務プロセスが 1～３つまで： 5万円～150万円 4つ以上： 150万円～450万円	(a)インボイス枠対象経費：同右 (b)消費動向等分析経費： 50万円×グループ構成員数 (a)+(b) 合わせて3,000万円まで (c)事務費・専門家費：200万円	ITツール： １機能：～50万円 ２機能以上：～350万円 PC・タブレット等： ～10万円 レジ・券売機等： ～20万円	～350万円	5万円～150万円
補助率	中小企業：1/2 **最低賃金近傍の事業者：2/3** **(**令和6年10月から令和7年9月の間で3か月以上、令和7年度改定の地域別最低賃金未満で雇用していた従業員数が全従業員の30%以上であることを示した事業者。)	(a)インボイス枠対象経費：同右 (b)・(c)：2/3	～50万円以下：3/4 (小規模事業者：4/5) 50万円～350万円：2/3 ハードウェア購入費：1/2	中小企業：2/3 大企業：1/2	中小企業：1/2 小規模事業者：2/3

（１）デジタル

（２）サイバーセキュリティ

（３）公共・準公共

サイバーセキュリティにおける新たな脅威の顕在化

◯ デジタル技術の発展と社会実装の進展、地政学リスクの高まり等によりサイバー攻撃のリスクが高まっている。**直近でも、情報流出、事業活動の停止、サプライチェーンへの被害など重大な事案も発生**。

＜最近の主な事案＞

①機微技術情報等の窃取

○ 2019年以降、中国の関与が疑われるグループ「MirrorFace」による、**日本の安全保障や先端技術に係る情報窃取を目的とした攻撃キャンペーン**が実行されている。（2025年1月 警察庁及びNISC（現：NCO）が注意喚起）

②事業活動の停止

○ 2025年10月、アスクル（株）が**ランサムウェア感染により受注・出荷業務を停止**。ネット通販配送をアスクルのグループ会社に委託する良品計画（株）等においても**ネットストアの受注・出荷業務が停止**し、**情報漏えいも確認。決算発表も延期**。

○ 2025年9月、アサヒグループホールディングス（株）に対する**ランサムウェア攻撃により、国内の酒類や飲料、食品の受注や出荷業務が停止**され、**主要工場の生産も一時的に停止**するとともに、**情報漏えいも確認。決算発表も延期**。

③重要インフラの機能停止等

○ 2024年2月、米国政府機関等が、中国を背景とするグループ「Volt Typhoon」による米国の重要インフラを標的とした活動（**有事の際にサイバー攻撃を行うためにネットワークへのアクセス権限を確保するような動き**）について注意喚起。

○ 2024年12月～2025年１月の年末年始にかけて、航空事業者、金融機関、通信事業者等が**相次いでDDoS攻撃を受け、サービスの一時停止**等の被害が発生。（2025年2月 NISC（現：NCO）が注意喚起）

④サプライチェーン・委託先等への攻撃を起点とした情報漏えい・金銭等資産の窃取

○ 2025年4月、㈱インターネットイニシアティブのメールセキュリティサービスへの不正アクセス事案が発生。**メールアカウントや他社クラウドサービスの認証情報など、586の契約先において情報漏えい**が確認。（2025年4月22日時点）

サイバーセキュリティ政策に関する国際的な動向

○ 欧米を中心に、①**セキュア・バイ・デザイン***の概念に基づく**製品のサイバーセキュリティ対策に対する要請**や、②**重要インフラ事業者等に対するインシデント報告等の義務化**、③**企業のサイバーセキュリティ対策水準を整備・可視化**等する動きが加速。* IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていることを指す。

①IoT・ソフトウェア製品に対するセキュリティ要件

EU サイバーレジリエンス法（EU Cyber Resilience Act）

- **デジタル要素を備えた製品（ソフトウエア含む）の製造者に対し、**①セキュリティ特性要件に従った**上市前の設計製造**、②**上市後に積極的に悪用された脆弱性・インシデントの報告等を義務付け。**
- 2024年12月に発効。**報告義務の運用開始は2026年9月、その他は2027年12月開始。**

サイバー・トラスト・マーク（U.S. Cyber Trust Mark）

- **消費者向け無線IoT製品が対象の任意ラベリング制度。**ルータ、スマートメーター等**一部製品については、個別のセキュリティ要件が定義される見込み。**2024年7月に最終規則公表。

PSTI法
（Product Security and Telecommunication Infrastructure Act）

- **2022年12月に、消費者向けIoT機器の製造者等に対するセキュリティ基準への自己適合宣言を義務付けるPSTI法が成立。**
- 2024年4月に、適用が開始され、英国内で製造や流通、販売を行う場合には、３つのセキュリティ要件を含む同法で規定されたセキュリティ対策の遵守が義務づけられた。

※PSTI法で規定されている３つのセキュリティ要件とは、共通パスワード設定の禁止、脆弱性情報の提供、セキュリティサポート期間の明示。

②重要インフラ事業者等に対するインシデント報告等の義務

重要インフラに係るサイバーインシデント報告法
（Cyber Incident Reporting for Critical Infrastructure Act of 2022）

- 「重要インフラ」に対し、①**重大なサイバーインシデント**の認知後**72時間以内**、②**ランサム支払後24時間以内に米CISAへの報告等を義務付け。**
- 2022年3月成立、2024年4月規則案公表。

NIS 2指令（Directive (EU) 2022/2555）

- **2016年NIS指令から対象セクターを拡大。**対象の主要／重要エンティティに対し、①**サイバーセキュリティ・リスクマネジメントの強化**、②**重大なサイバーインシデント**の認知後**24時間以内に早期警告、72時間以内にCSIRT又は管轄省庁に報告等を義務付け。2023年1月発効、2024年10月18日より執行。**

※豪州においても、特定の事業者に対しランサム支払い後72時間以内の報告を義務付けるサイバーセキュリティ法（下位法の制定を経て2025年5月30日より適用予定）が存在。

③企業のサイバーセキュリティ対策水準の整備・可視化

サイバー・エッセンシャルズ（UK Cyber Essentials）

- 英NCSCが**全ての企業に対し、一般的なサイバー攻撃への防御策を提供することを目的**として設計した、自己適合、第三者診断の**二段階で構成される認証**制度。
- 一部政府及び公的機関の調達において必須要件として課される場合がある。

※豪州においても、すべての組織を対象とする４段階の基準（エッセンシャル・エイト）が存在。
※米国においても、米国防省がその請負業者等と共有する機密性の高い情報の保護を目的に設計したサイバーセキュリティ成熟度モデル認証（CMMC。2023年12月に2.0版が発効。）が存在。

米国コネクティッドカー最終規則概要

○ 米国政府は**国家安全保障上の懸念***から、**中国・ロシア関連**のコネクティッドカー向け**ハードウェア及びソフトウェア、それらを搭載した車両の輸入・販売を禁止**する等の最終規則を2025年1月に発表し、3月16日に施行済み。

○ *例えば、①SCに外国敵対者が侵入し大量の機密データを収集し流出させるリスク、②SC内の外国敵対者を買収して車両を遠隔操作するリスク 等

規制対象		移行期間
A) 自動車通信システム（VCS）関連ハードウェア **【具体的な対象】** マイコン、SoC、TCU、セルラー・モジュール、アンテナ、Wi-Fi/Bluetooth・モジュール等 ※なお、車載センサー類（ライダー、レーダー、ビデオ等）、カーナビ*、衛星ラジオ、キーフォブ等の機器は**規制対象外** *GNSS（全球測位衛星システム）	①中国又はロシア関係者*が設計/開発/製造/供給する**A）の米国への輸入**	**モデルイヤー2030から適用** (ハードウェア単体としては2029/1～)
B) VCS関連ソフトウェア/自動運転モデル **【具体的な対象】** 無線通信の送受信・変換、処理システム ※自動運転モデルは自動運転レベル3~5のソフトウェアが対象	②中国又はロシア関係者*が設計/開発/製造/供給する**B）搭載車の米国への輸入/販売**	**モデルイヤー2027から適用****
③ 中国又はロシア関連*の自動車メーカーによる A)又は B)搭載するコネクティッドカーの米国での販売		

***中国又はロシアの所有・支配下にある、もしくは司法権が及ぶ、又はこれらの国からの指示に従う個人または法人**のこと
** **2026年3月17日より前に開発されたソフトウェアは、以降に中国・ロシア関連企業による継続的な点検やアップデートがない場合、規制対象外**

免除措置	
	一般認可：一定の条件に適合する場合、商務省への通知なしで取引が認められる **特定承認：商務省の審査・承認後（ケースバイケースで判断） リスク軽減措置を講じた場合を含め企業が禁止措置に従事することが可能**

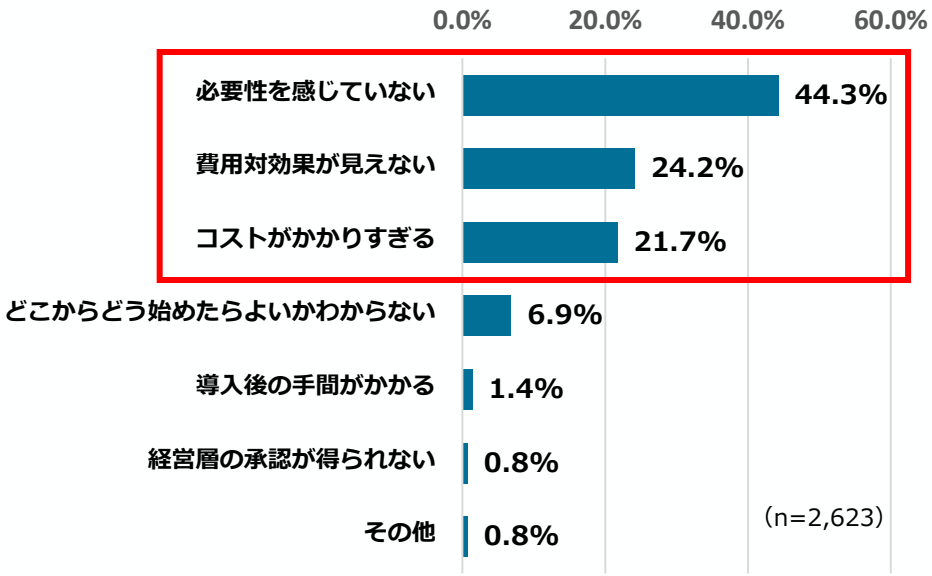
出典：米国商務省「Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles」、米国ホワイトハウス「Regulatory Freeze Pending Review January 20, 2025」等を基に経済産業省作成

中小企業のサイバーセキュリティ対策の現状

○ サイバーセキュリティ対策を行っていない中小企業には、「**必要性を感じていない**」層と**コストの高さ・費用対効果の不透明さ**を理由とする層が多く存在。

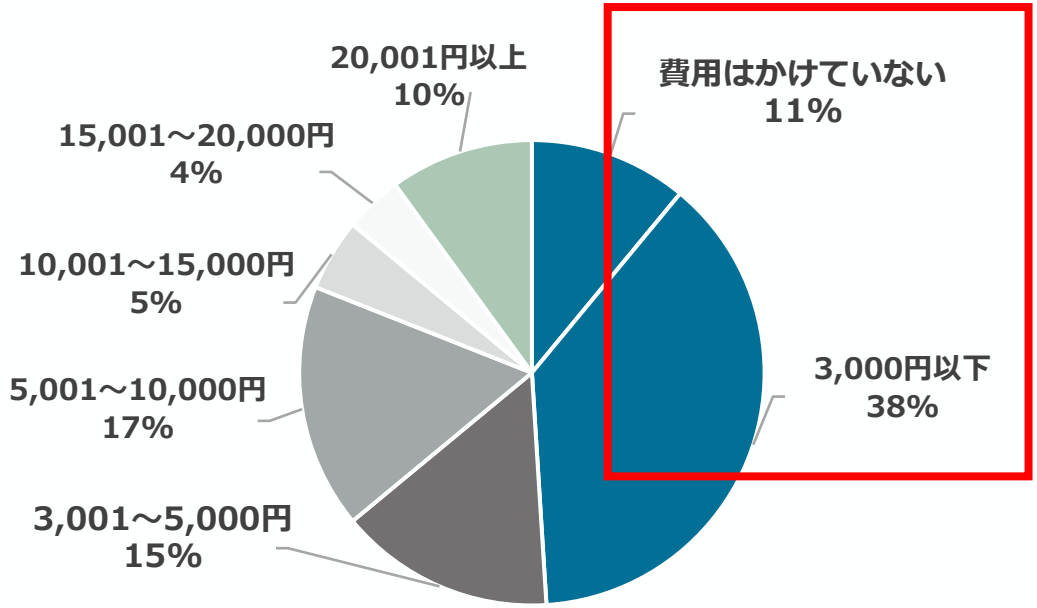
○ サイバーセキュリティ対策を行っている中小企業においても、その**半数**はセキュリティ対策にかける費用が**月額3,000円以下**となっている。

情報セキュリティ対策を行わなかった理由



出典：IPA「2024年度中小企業における情報セキュリティ対策の実態調査報告書」

セキュリティ対策にかけている費用（月額）

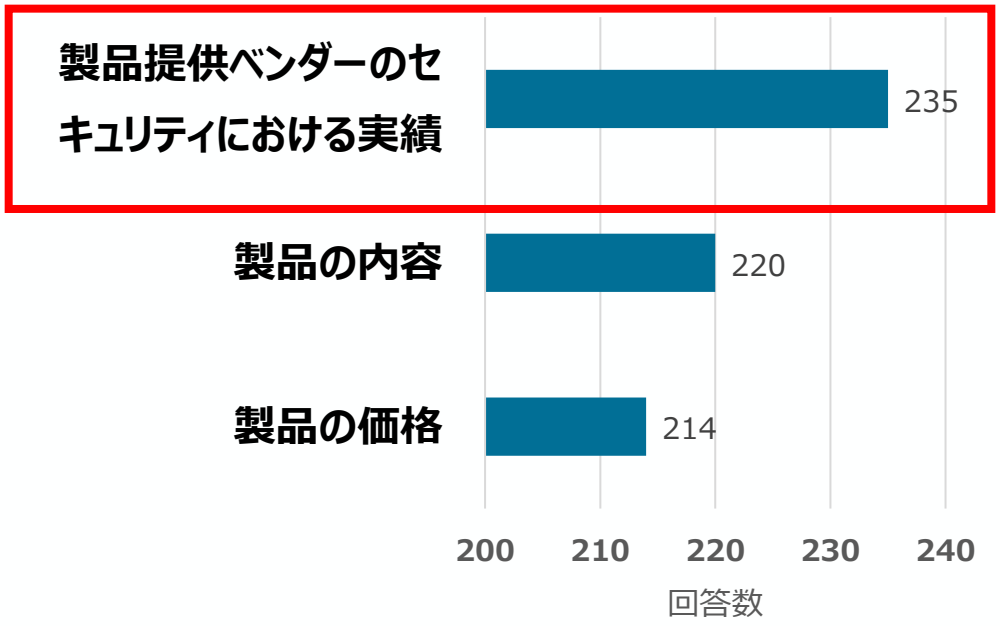


出典：東京都産業労働局「令和6年度中小企業サイバーセキュリティ啓発事業」

我が国におけるサイバーセキュリティ産業の現状

○ 国内のサイバーセキュリティ産業が育成されない原因として、以下のような現状が指摘されている。
- ユーザーは、**これまでの利用実績や価格を重視**。新規製品を発売しても、実績が重視されるため,顧客が見つからず、事業として成り立たないため、企業が育たない状況。
- 安定的な収益基盤が見通しづらいため、**製品開発・研究開発への投資が限られる**。
- 結果として、我が国セキュリティ産業は、「**買い手がつかないので儲からない**」「**儲からないので事業開発や投資が十分なされず競争力が低下**」という悪循環に陥っている。

製品を選定する際に最重要視する項目
（上位３項目、国内ユーザー企業からのアンケート）



各国のセキュリティ企業の研究開発額の比較
（2022年）

国籍/企業	主要製品分野	研究開発費（億円）（売上高に対する研究開発費比率）
カナダA社	エンドポイントセキュリティ等	310.5（31.6%）
米国B社	エンドポイントセキュリティ等	912（29.0%）
イスラエルC社	エンドポイントセキュリティ等	525（17.1%）
日本D社	エンドポイントセキュリティ等	54（2.4%）
日本E社	エンドポイントセキュリティ等	0.2（0.2%）

（出所）
（左）富士キメラ総研「2023 ネットワークセキュリティビジネス調査総覧〈ベンダー戦略編〉」より一部加工。
（右）経済産業省（PwCコンサルティング合同会社提出「令和5年度産業サイバーセキュリティ強靭化事業(サイバーセキュリティ産業の振興に関する調査) 調査報告書」）を基に作成。

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（SCS評価制度※）の整備

※　SCS（supply chain security）評価制度

○「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」等の課題に対し、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みを構築。

○ 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。

※　本制度では、サプライチェーンを構成する企業等のIT基盤が対象。

※　発注時等に、必要なセキュリティ対応状況の可視化を目的としたもので、いわゆる「格付け」制度ではない。

構築する評価制度（案）

成熟度の定義	★３	★４	★５［検討中※4］
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

※4　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。

制度の普及施策（例）

想定される課題	中小企業等における★取得の負担		中小企業等における セキュリティ専門家の確保	サプライヤー企業への ★取得要請時の関係法令の適用
普及施策	サイバーセキュリティお助け隊サービス（新類型）の創設	中小企業ガイドライン整備	専門家の活用促進	取引先への要請等に係る考え方の整理
	★3・★4に対応した、サイバーセキュリティお助け隊サービスの新たな類型創設により、安価な”★”取得を実現	中小企業の情報セキュリティ対策ガイドライン及び付録サンプル規程の整備により、”★”の取得を容易化	「中小企業向けサイバーセキュリティ専門家リスト」の整備により、中小企業と専門家とのマッチングを促進	取引先とのパートナーシップ構築促進に向けた想定事例及び解説案の策定により、費用に係る価格交渉を推進

サイバーセキュリティお助け隊サービス

○サイバーセキュリティお助け隊サービスは、**中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価（例：月額1万円以内）に提供するサービス。**

○**全国44事業者がサービスを提供**しており、**約9,200件の利用実績**（2025年12月時点）がある。

○デジタル化・AI補助金（旧：IT導入補助金）「セキュリティ対策推進枠」を活用することで、**最大150万円まで、導入費用の1/2（小規模事業者は2/3）の補助**を受けられる

○今後、SCS評価制度に沿った新サービスを創設予定。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

- ✓ **EDR・UTM等による異常監視**
- ✓ **緊急時の対応支援・駆付けサービス**
- ✓ **簡易サイバー保険**
- ✓ **相談窓口**
- ✓ **簡単な導入・運用**

➡中小企業でも導入・維持できる価格でワンパッケージで提供

サイバーセキュリティお助け隊サービスの利用はこちらから
⇒ https://www.ipa.go.jp/security/otasuketai-pr/

サイバーセキュリティ お助け隊

お助け隊マーク

- お助け隊サービスA
- お助け隊サービスB
- お助け隊サービスC

お助け隊サービス審査登録制度：
一定の基準を満たすサービスに**お助け隊マークの商標利用権を付与**

サービス提供 → **中小企業** → **自社の信頼性をアピール** → **取引先**（大企業等）

お助け隊サービス利用の推奨等の中小企業の取組支援

デジタル化・AI補助金（旧：IT導入補助金）に「セキュリティ推進枠」創設
（補助率：中小企業1/2、小規模事業者2/3
補助上限：150万円）

サイバーセキュリティお助け隊サービス（新類型）

○ SCS評価制度の**★３・★４の取得支援**を目的とする。具体的には、★３・★４の対策項目のうち**未達成の項目について、サイバーセキュリティお助け隊サービス（新たな類型）の導入により全部又は一部の対策項目を達成させる**ものとする。

○ STEP１として、サービス提供に当たって**SCS評価制度の★取得及び更新時に中小企業の対策状況を評価**することをサービスに含める。

○ STEP２として、SCS評価制度の対策項目の中には、ITツールの導入により達成できる項目や、人的支援により達成できる項目があるため、サイバーセキュリティお助け隊サービス（新類型）は「**ITツールによる支援**」のほか「**ITツール以外の支援**」を組み合わせて提供することをサービス内容とする。

サイバーセキュリティお助け隊サービス（新類型）のイメージ

STEP1：課題の可視化

✓SCS評価制度の要件項目毎に中小企業の**対策状況を診断**

✓SCS評価制度の**更新時に、各対策項目の対策状況を評価**

STEP２：対象サービスの選定と対応実施

✓診断結果に基づき、以下の支援を実施

✓**ITツールによる支援**
★３・★４取得に推奨されるITツールを導入

✓**ITツール以外の支援**
セキュリティポリシーやインシデント手順書の整備、セキュリティ教育など、中小企業が自助努力で達成しづらい項目を支援

【サービス例】

SC★４＋	★４要件に駆付け支援がプラスされたサービス
SC★４	★４要件を最低限満たすサービス
SC★３＋	★３要件に駆付け支援がプラスされたサービス
SC★３	★３要件を最低限満たすサービス

STEP3：★取得

✓ SCS評価制度の★3又は★４の**項目要件をすべて充足することで★を取得**

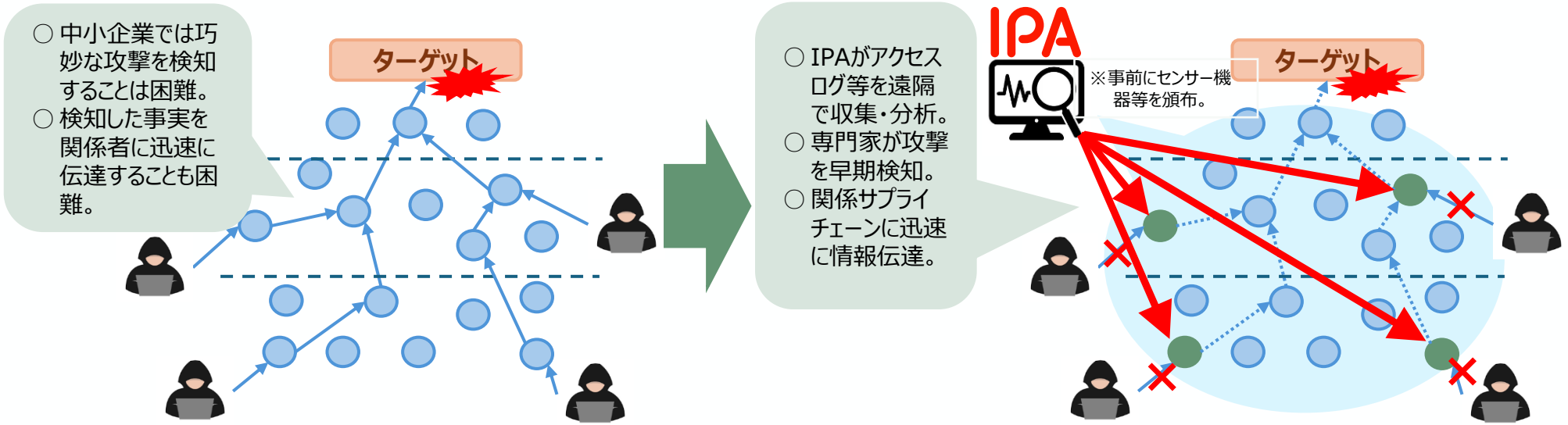
STEP1･STEP2の支援サービスを一定の価格要件の下で提供

中小企業等向け集団的防御プラットフォームの構築

○基幹インフラ事業者等を標的としたサイバー攻撃は、そのサプライチェーンの中で**比較的脆弱な中小企業等から侵入**して標的に到達しようとすることが一般的。

○一方で、**中小企業等**は、**攻撃の兆候を十分に検知することが難しい**状況。

○このため、高度なサイバー情勢分析機能を有する**IPA**が、サプライチェーン上の中小企業等への**アクセスログ等を遠隔で収集・分析**し、**サイバー攻撃の早期検知**や取引先への波及を防ぐための**情報展開を実施**する。



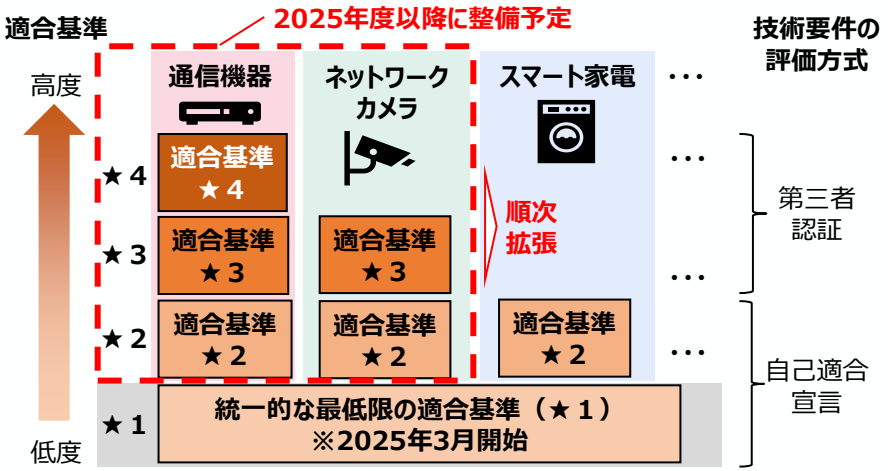
IoTセキュリティ適合性評価制度（JC-STAR）の更なる推進

○ 将来的に４段階での適合性評価を目指すこととしており、**１段階目（★１）について、2025年３月から申請の受付を開始**し、**５月より★１ラベルの「適合ラベル取得製品リスト」を公開**。

○ 今後、通信機器とネットワークカメラについて、**2025年度中により高度な基準（★２以上）を策定**するとともに、その他の製品の高度な基準の検討も順次実施予定。

○ 引き続き、**政府調達の要件化**に加え、**地方公共団体、重要インフラ事業者、その他民間企業等への普及展開を図る**とともに、**諸外国の関連制度との相互承認**を進めていく（**2026年１月から英国との相互承認を開始**）。

より高度な基準の策定（JC-STAR）



相互承認調整を進める外国制度の例

国・地域	シンガポール	英国	米国	EU
制度名	Cybersecurity Labelling Scheme (CLS)	Product Security & Telecommunication Infrastructure Act (PSTI)	U.S. Cyber Trust Mark	Cyber Resilience Act (CRA)
マーク	CYBERSECURITY LABEL CSA/IOTWABCD	–	U.S. CYBER TRUST MARK	CE
開始時期	2020年10月制度開始	2024年4月施行	2025年より基準策定開始（制度開始時期は調整中）	• 報告義務: 2026年9月 • その他: 2027年12月
任意/義務	任意	義務	任意	義務
対象	消費者向けIoT機器	消費者向けIoT機器	消費者用無線IoT製品	デジタル要素を含む製品

「サイバーセキュリティ産業振興戦略」と今後の展開

○ 我が国へのサイバー攻撃の特異性に対応し安全保障を確保する等の観点から、**製品開発の出口をまず確保**した上で、**シーズの発掘・事業拡大を後押し**するなど、**包括的な政策対応を2025年３月にとりまとめ。**

○ 「10年以内に国内企業の売上高を足下から３倍超」とのKPIの達成に向け、**具体的な取組を深化**させていく。

今後のロードマップ

■STEP１（約３年以内）【裾野の拡大】
- ✓ J-Startup選定企業をはじめスタートアップ数の拡大を図る
- ✓ プロダクトを開発する「トップガン」人材の増加を図る

■STEP２（約５年以内）【競争力の強化】
- ✓ 市場における我が国企業のマーケットシェア拡大を図る（とりわけ量子・AIなど先端的な技術への対応に資する技術の社会実装を進める）

■STEP３（約10年以内）【安全保障・経済政策への貢献】
- ✓ 優れた製品・サービス・企業について、市場や社会的な影響力を強める
- ✓ ユーザー企業が、自社の状況やリスクに応じて様々な製品・サービスを選択できる環境を構築する
- ✓ 我が国特有の攻撃への対応や企業の海外進出を通じて安全保障・デジタル赤字解消にも貢献する

「サイバーセキュリティ産業振興戦略」今後の主な対応

政府機関等による有望なセキュリティ製品・サービスの活用機会の提供

○ 足下の取組として、まずは、**IPAのセキュリティ分析・対処支援等**において、**先進のスタートアップ製品・サービスを試行的に活用**。併せて、スタートアップの製品・サービスの試行的な活用を行う**政府機関等の主体・取組を拡大**

製品・サービスのセキュリティや信頼性を確認する制度の構築・運用

○ **JC-STARの適切な運用・制度拡張**や「**サイバーインフラ事業者に求められる役割等に関するガイドライン**」「**SSDF導入ガイダンス**」を成案化／それらへの**適合を確認する枠組み構築**を含め、**必要な制度構築・活用促進に向けた施策**を検討

「トップガン」等のセキュリティ供給人材の確保に向けた新たな政策検討

○ **セキュリティ・キャンプの拡充**や**情報処理安全確保支援士（登録セキスペ）の活用促進**を通じた高度専門人材育成を進めつつ、新製品・サービスを開発・導入・評価できる**セキュリティ供給人材の育成に向けた政策対応の在り方**についても検討

アジア太平洋地域への進出を見据えた我が国のセキュリティ政策の展開

○ 日ASEAN政府間会合等を活用し、我が国企業が多く進出するアジア太平洋地域における**我が国のサイバーセキュリティ政策の普及・展開を推進。我が国サイバーセキュリティ製品・サービス提供事業者の海外進出を後押し**する素地を構築

【KPI：国内企業の売上高を足下から3倍超（約0.9兆円⇒3兆円超）】

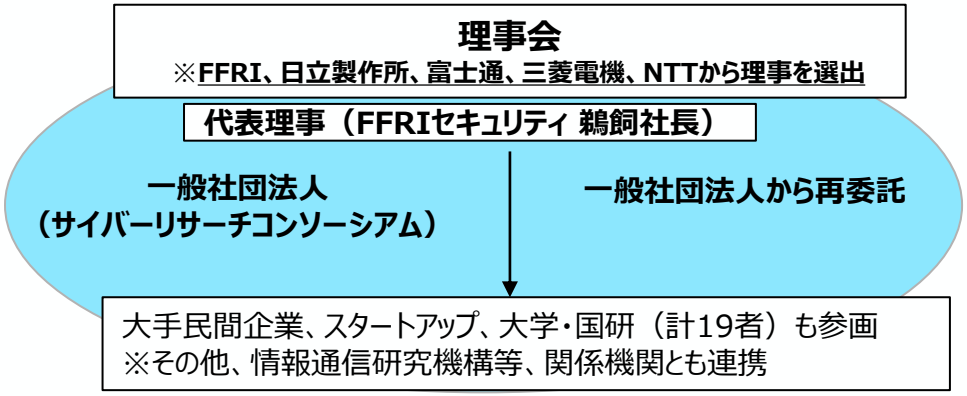
先進的サイバー防御機能・分析能力強化のための研究開発

○ 高度かつ未知の攻撃にも対処可能な**攻撃の早期発見技術**や、AIを活用したシステムの脆弱性の検知・評価技術など**防御力向上に資する技術**の開発・社会実装に向け、**約300億円／５年の研究開発プロジェクト**を立ち上げ、2024年７月からプロジェクト開始。

実施体制

一般社団法人サイバーリサーチコンソーシアム

研究開発の体制



事業規模など

- 事業規模　：　290億円以下（2024年7月～2029年3月）
- 契約形態　：　委託事業

主な研究開発内容

1）サイバー空間の情報を収集・調査する状況把握力の向上

- アーティファクト分析技術／攻撃者からより多くの情報を獲得するための技術／高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

2）サイバー攻撃から機器やシステムを守る防御力の向上

- AIを活用した脆弱性探査技術／AI等を活用した防御能力の評価・向上技術／AIを活用したOTペネトレーションフレームワーク技術
- 耐量子計算機暗号技術／耐タンパー性向上技術

3）共通基盤の整備

- 情報の効果的な連携に関わる技術
- 高度サイバー人材の評価・管理に関する技術

サイバーセキュリティ人材の確保に向けた施策の全体像

セキュリティ対策を進めるための体制・人材の考え方

○セキュリティ体制構築・人材の確保の手引き（「サイバーセキュリティ経営ガイドライン」付録F）

- 企業経営者等向けに、自社でセキュリティ人材を確保し体制を整備するための実践的な指針を提示

○人材確保・育成の実践的方策ガイド（β版）（中小企業の情報セキュリティ対策ガイドラインへの収録を想定）

- 中堅・中小企業が実施すべきセキュリティ対策と必要な人材の確保策などを段階的に提示するとともに、セキュリティ対策に関する経営者へ向けたメッセージ、外部人材の活用方策や教育・訓練機会等も提示（令和７年度中に成案化予定）

セキュリティ人材の育成

○セキュリティ・キャンプ

- 若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラスの人材を育成・発掘

○中核人材育成プログラム（IPA/ICSCoE）

IPA 産業サイバーセキュリティセンター Industrial Cyber Security Center of Excellence (ICSCoE)

- OT(制御技術）とIT（情報技術）の知見を結集させた世界レベルのサイバーセキュリティ対策の中核拠点における、１年を通じた集中トレーニング

○情報処理安全確保支援士（登録セキスペ）

- サイバーセキュリティの確保を支援するための、セキュリティに係る専門的な知識・技能を備えた国家資格

プラス・セキュリティ（※）の普及

※セキュリティを本務としない者が業務遂行にあたってセキュリティを意識し、必要十分なセキュリティ対策を実現できる能力を身につけること、あるいは身に着けている状態のこと

○地域SECUNITYにおける人材育成

- セミナーの開催を通じた人材育成支援など、各地域でのセキュリティの「共助」に向けた取組を促進

○NISCにおけるモデルカリキュラム策定

- プラス・セキュリティ知識を補充できるプログラムの普及に向けて、教育事業者や社内研修の参考となるカリキュラムを公開

○デジタル人材育成プラットフォームにおける教育コンテンツの提示・実践型教育（マナビDX）

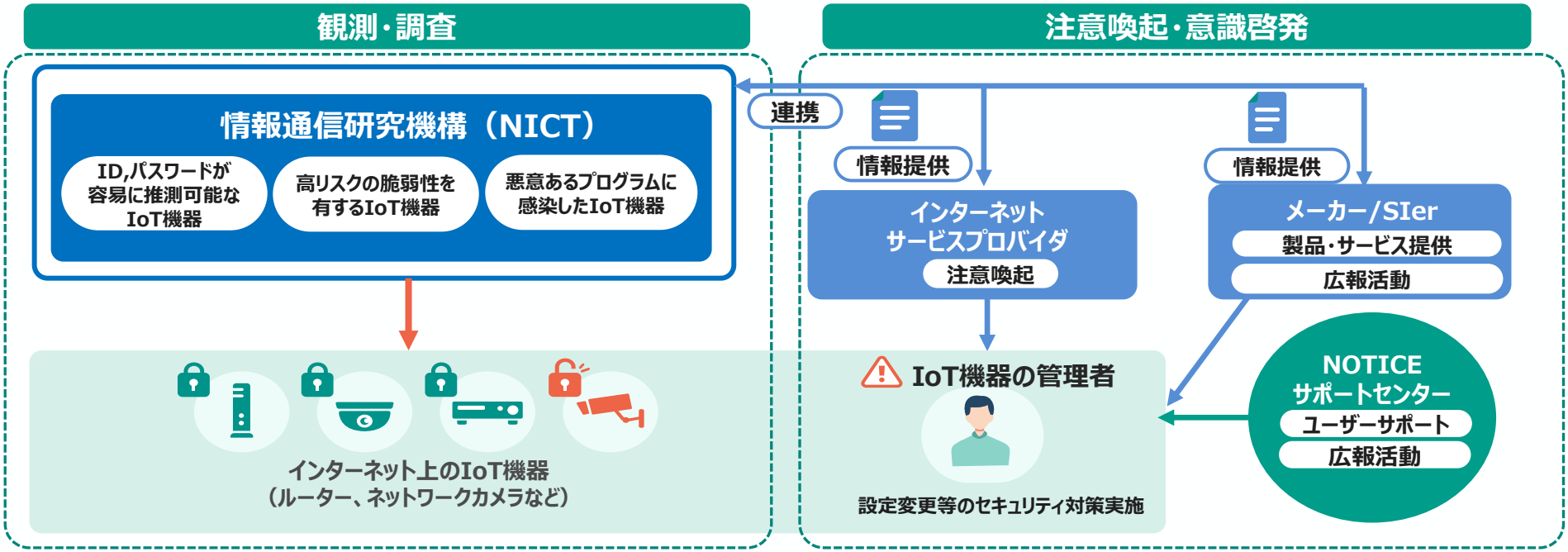
○大学・高専等と産業界との連携

IoT機器のサイバーセキュリティ対策の推進

○ 悪意あるプログラムに感染したネットワーク機器等の発見、管理者への注意喚起［NOTICE（ノーティス）］

- 情報通信研究機構（NICT）がインターネットを観測・調査し、**悪意あるプログラムに感染したネットワーク機器や、今後感染する危険性が高い脆弱なネットワーク機器を発見**
- 電気通信事業者を通じ、当該機器の**管理者に注意喚起**して対応を促すことで、被害の発生を防止

みんなで守る、IoT。 NOTiCE



2025年12月の結果

IoT機器観測総数	容易に推測可能なID,パスワードであるIoT機器	高リスク脆弱性を有するIoT機器	悪意あるプログラムに感染したIoT機器検知数
月 1.17 億件	月 13,796 件	月 2,536 件	最大 328 件/日

サイバーセキュリティに関する産学官連携の推進

○ 情報通信研究機構（NICT）では、サイバーセキュリティ関連の**最先端技術の研究開発**、実践的サイバー防御**演習等による人材育成**を推進

○ これらのNICTが有するデータ・知見を民間に広く開放し、国産セキュリティ技術の開発基盤を強化するため、**産学官の結節点となる先端的基盤として、CYNEX（CYbersecurity NEXus：サイネックス）を構築**

政策機関等におけるサイバーセキュリティ対策の強化

○ **政府端末情報を活用した情報収集・分析**［CYXROSS（サイクロス）］

- 情報通信研究機構（NICT）が開発した**国産検知ソフトウェア（CYXROSSセンサー）を政府機関の端末に導入**し、我が国独自の**一次情報**の収集・分析体制を整備することで、**政府機関等に対するサイバー攻撃の監視を強化**
- サイバー攻撃に関する情報（サイバー脅威情報）を**我が国独自に収集し、分析・検知することで、サイバーセキュリティ対策を強化**

CYXROSS Agent

サイバーセキュリティ対策の強化

①安全性・透明性を検証可能なセンサー(ソフトウェア)を開発し政府端末に導入

・悪意あるプログラム本体のファイル
・不審な端末挙動に関する端末ログ
等

サイバー脅威

サイバー脅威

サイバー脅威

②収集した情報をNICTに集約

⑤分析結果を提供

NICT
情報通信研究機構

④監視・分析

④分析・検知能力の強化

サイバー脅威情報を用いた分析・検知能力の強化

③NICTの技術と蓄積データの活用

NICTER
サイバー攻撃観測技術

STARDUST
標的型攻撃観測・分析技術

NIRVANA改
サイバー攻撃情報統合分析技術

実践的・先進的サイバーセキュリティ人材の育成

○ 情報通信研究機構（NICT）の「ナショナルサイバートレーニングセンター」に大規模な演習環境を整備し、実践的な演習プログラムの提供を通じて、**巧妙化・高度化するサイバー攻撃に対応できるサイバーセキュリティ人材の育成を支援**

CYDER
Cyber Defense Exercise with Recurrence
（サイダー）

国機関・地方公共団体・独立行政法人等を対象とした「実践的サイバー防御演習」

全国の会場で**年間計100回**、**計3,000名規模**で実施
2017年度の開始以降、2024年度までに、延べ**25,000名超**が受講

SecHack365
（セックハック サンロクゴ）

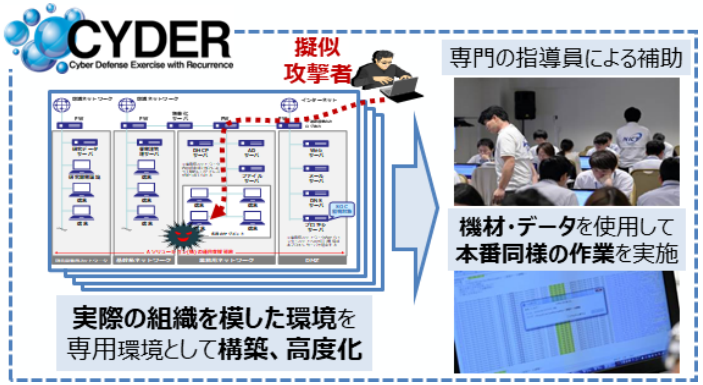
25歳以下の若手人材を対象とした「セキュリティイノベーター育成プログラム」

年間40名程度の受講者を選抜し、**１年間のトレーニング**コースを実施
2017年度の開始以降、2024年度までに、**計300名超が修了**

CYROP
（サイロップ）

分野別実践演習の開発・実施基盤「CYROP」

サイバーセキュリティ演習に必要となる基盤（仮想環境、演習教材等）を大学、民間企業等へ開放
2026年１月時点で86組織が参画、利用



実践的サイバー防御演習
CYDER

セキュリティイノベーター育成プログラム
SecHack365

分野別実践演習の開発・実施基盤
CYROP

実践的サイバー防御演習「CYDER」 (CYber Defense Exercise with Recurrence)

○ 情報通信研究機構（NICT）において、平成29年度から、**国の機関、指定法人、独立行政法人、地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習「CYDER」**を実施

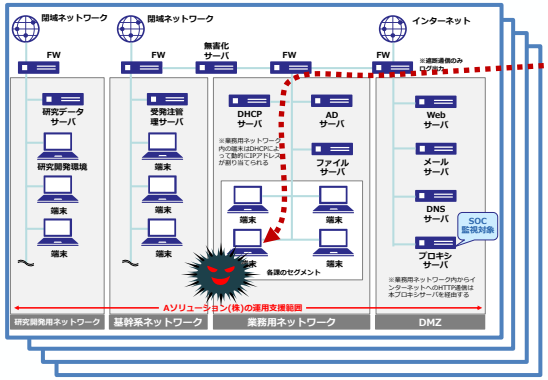
○ 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って、**外部のセキュリティ事業者の支援を受けることを前提としてサイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験**

○ **全都道府県**において、年間**100回**の計**3,000名規模**で実施(集合コース)。令和６年度は106回の**4,225名**が受講

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**

専門指導員による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和７年度の実施状況

コース名		実施方法	レベル	受講想定者（習得内容）	受講想定組織	実施地	実施回数	実施期間
CYDER	A	集合形式	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	47都道府県	78回	７月～翌年１月
	B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国８地域	10回	10月～11月
	B-2				地方公共団体以外	東京・大阪・名古屋	13回	翌年１月
	C		準上級	セキュリティ専門担当者 (初動分析を含む主体的な事案対応)	全組織共通	東京・大阪	５回	11月～翌年１月
プレCYDER		オンライン形式	-	全ての情報システム担当者 (最低限必要となる知識の習得と最新化)	全組織共通	(受講者職場等)	-	1期：５月～８月 2期：９月～11月 3期：11月～翌年１月

分野別実践演習の開発・実施基盤「CYROP」(CYber Range Open Platform)

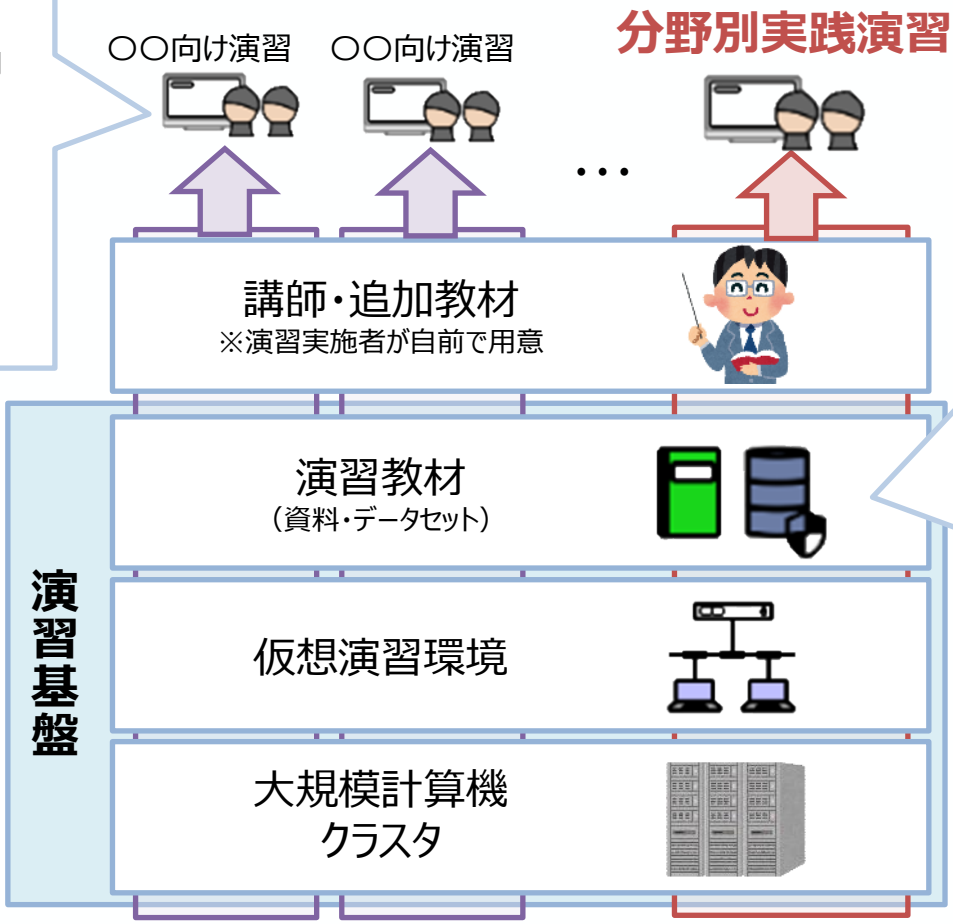
○ 情報通信研究機構（NICT）の有する**人材育成ノウハウを民間企業・教育機関等に横展開**するため、各組織が**実践的演習を容易に開発・実施可能とする演習基盤「CYROP」**※を構築。令和５年10月から提供開始

○ 「CYROP」では、サイバーセキュリティ演習の実施に必要となる**演習環境・演習教材を提供**。演習教材をカスタマイズし、自前で講師を用意することで、**分野に応じた演習を容易に実施可能**

※NICT内に設置されたサイバーセキュリティに関する産学官の結節点『**CYNEX（サイネックス）**』の取組の一つとして提供

民間企業の自社向け演習、
大学・高専での講義等で活用

CYDERと同等の演習基盤を
NICT以外の組織においても
活用可能とするサイバーセキュリティ
演習基盤を開発し、
CYROPにおいて提供



CYDERの教材のほか、
CYROP独自教材も開発

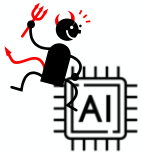
利用者は、既存の教材を編集・
カスタマイズして利用することも可能

日本成長戦略と警察におけるサイバーセキュリティ対策

巧妙化・高度化するサイバー攻撃

ランサムウェア攻撃
(試算上、R6年中で約129億円以上の調査・復旧費が発生)

国家を背景とした
暗号資産や機密情報の窃取
(R6年、約482億円相当の暗号資産が窃取)



AIの悪用

サイバー攻撃は、その背後に国家がいることもあり、放置すれば、
サイバー安全保障の危機

警察におけるサイバーセキュリティ対策の取組

【警察におけるサイバーセキュリティ対策の取組】

① 民間事業者等との緊密な連携
② 脅威情報の収集、分析等による実態解明
③ 注意喚起、パブリック・アトリビューション等の実施
④ サイバー事案の捜査
⑤ アクセス・無害化措置の実施

○ 高度な知見を有する人材の確保・育成
○ 先端技術を活用した対処能力の強化

巧妙化・高度化するサイバー攻撃の抑止のため、警察が、計画的・安定的に上記対策を推進し、サイバー攻撃への対処能力を継続して強化・高度化することが不可欠

⇒「危機管理投資」「成長投資」に直結

【警察組織の強み】

- 全国47都道府県警による**広域な情報網と捜査網**
- **民間事業者等との緊密な信頼関係**
- **同盟国・同志国との緊密な連携**
- **捜査権を有する組織**としてサイバー捜査を実施

サイバー捜査等を通じた
膨大な蓄積情報等に基づく
分析等が可能

警察におけるサイバー人材

※令和７年４月１日現在

全国のサイバー対処専従員は約3,600人

警察庁サイバー特別捜査部
約370人

※都道府県情報通信部の解析担当職員等の併任者を含む。

官民人事交流制度による採用者が幹部として活躍

解析担当技官が警察官として活躍

選抜

選抜

全国のサイバー部門の専従要員

都道府県警察サイバー捜査官
約2,600人

専門的知識・技能を有する中途採用者・特別採用者
約480人

警察庁解析担当技官
約800人

高度で専門的な知識及び技術に基づく解析による対処

選抜

選抜

全国都道府県警察のサイバー人材（基本情報技術者相当）　**約５万3,400人**

警察庁情報通信職員　**約3,600人**

※　警察庁サイバー特別捜査部の約370人には、都道府県情報通信部の解析担当職員との併任者約180人が含まれていることから、全国のサイバー捜査専従員は、併任者を除いた約3,600人になる。

（１）デジタル
（２）サイバーセキュリティ
（３）公共･準公共
- **公共**
- 医療DX
- モビリティ

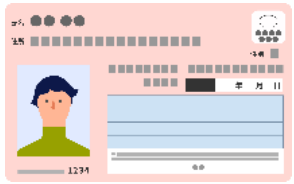
近年のデジタル政策の取組と社会の変化

○ 政府や地方公共団体のDXの推進により、暮らし、事業活動、行政に大きな変化をもたらしている。

暮らし

手続きは、「窓口にいく」から、「いつでもどこでも」へ

マイナンバーカード



- ✓ 保有枚数 1億64万枚（2025年12月）
- ✓ 保有率 80.8%
- ✓ マイナ保険証　9,041万件（2025年12月）

マイナポータル

- ✓ アカウント登録数 8,269万件（25年12月）
- ✓ 引越し 年間78万回
- ✓ パスポート 年間77万回
- ✓ 確定申告（e-Tax・公売電子入札との連携数）1,106万件

事業活動

制度や手続きは、「デジタル前提」へ

GビズID（事業者認証共通システム）

- ✓ Gビズプライム累計登録数
  142万件（2025年12月）

GビズID

e-Gov（事業者手続きサービス）

- ✓ オンライン手続きの年間件数
  3,042万件（2024年度）

政府、地方公共団体

システムは、「個別・単独」から、「共通・共同」へ

政府のネットワークの整備

- ✓ GSSの整備
  導入省庁　14機関 / ユーザー数　4.5万人（2025年7月）

ガバメントクラウドの導入（国地方が共同で利用）

- ✓ ガバメントクラウドの利用状況
  5,237システム（2025年9月末時点）

地方公共団体の標準化・ガバメントクラウドへの移行

- ✓ 標準化対象システム　34,592システム
- ✓ 標準化対象業務数　20業務

地方公共団体へのSaaSの提供

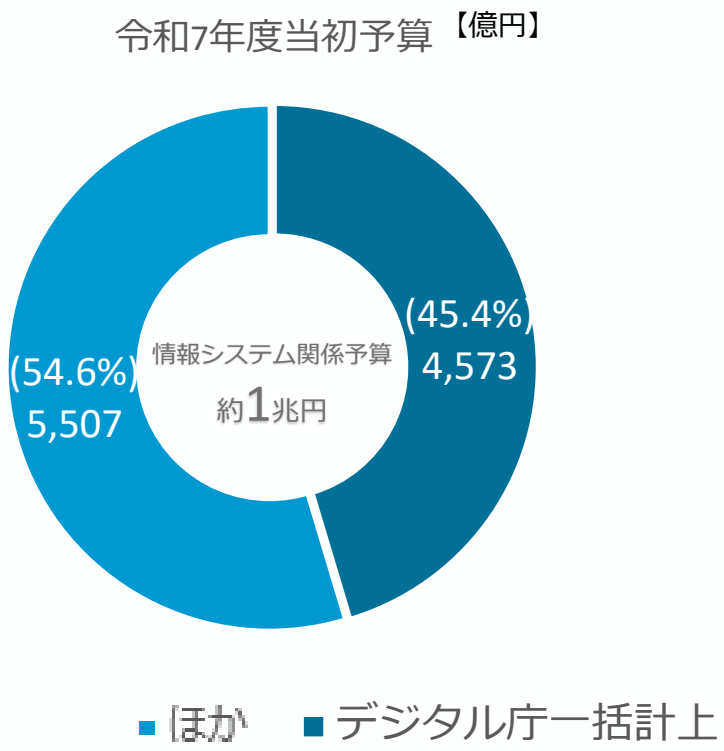
- ✓ 給付支援サービスの提供 累計108自治体
  （2025年9月末時点）

政府情報システム予算の規模・推移

○ 国の情報システムの経費は、デジタル庁所管一般会計に一括計上されるもののほか、一括計上外のものとして、特別会計等にも予算計上されている。

情報システムの予算構造

- 政府情報システムに係る当初予算は約1兆円。
- そのうち、デジタル庁一括計上予算は 5割弱を構成している。



一括計上システムの例

- ガバメントソリューションサービス（GSS）【デジタル庁】
- ガバメントクラウド【デジタル庁】
- 国税総合管理（KSK）システム【財務省】
- 登記情報システム【法務省】

一括計上外システムの例

- 記録管理・基礎年金番号管理システム【年金特別会計】
- ハローワークシステム【労働保険特別会計等】
- 年金給付システム【年金特別会計等】
- 特許事務システム【特許特別会計】

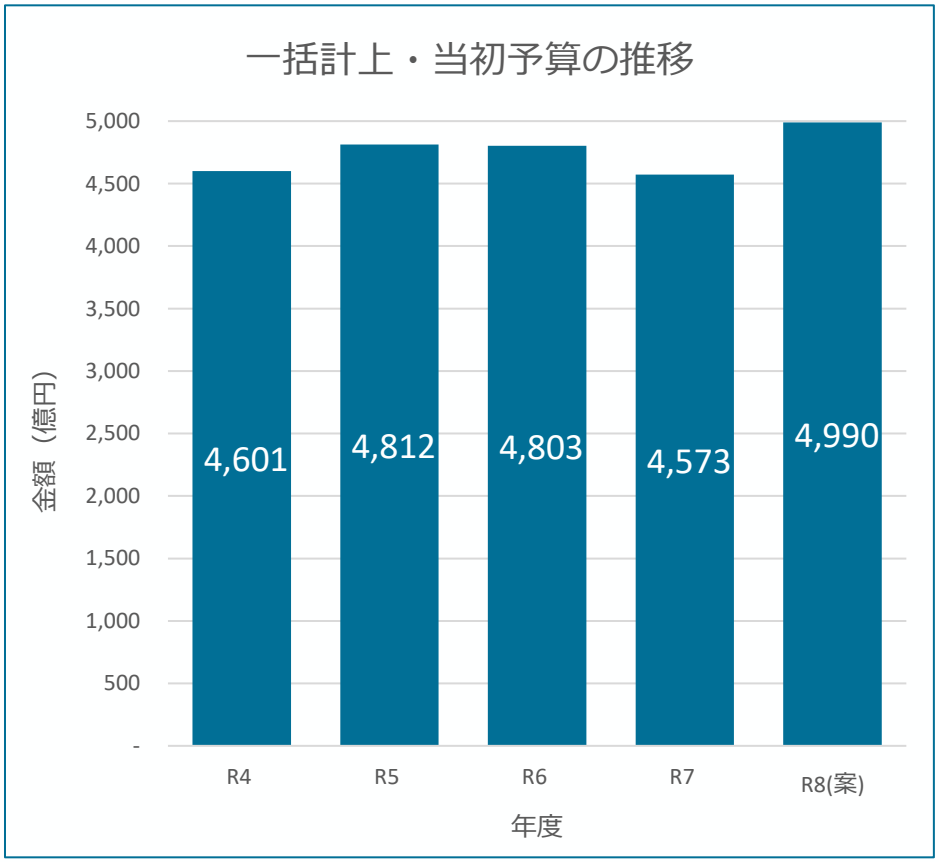
政府情報システム予算（一括計上）の推移

○ デジタル庁設立後、政府や地方公共団体のDX基盤を中心に共通機能の整備・開発を推進

○ 当初予算では、運用等経費の割合が増加傾向。また、補正予算も活用し、整備・開発を加速。

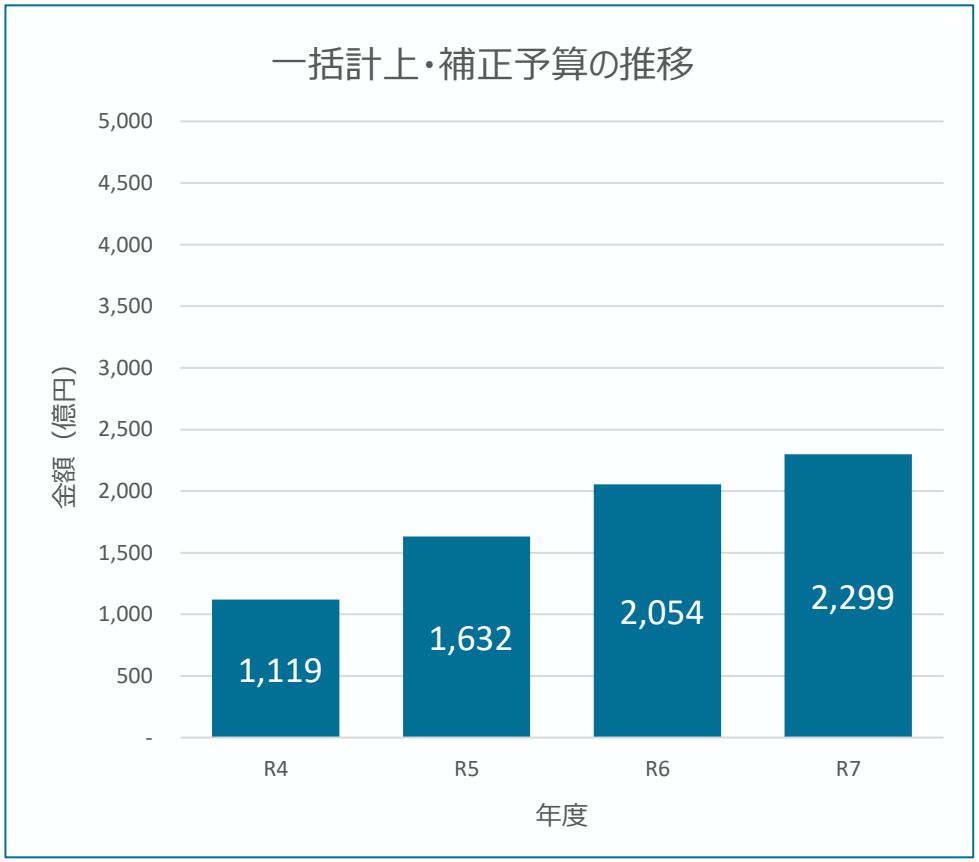
一括計上・当初予算の推移

- 年々増加。
- 運用等経費の割合は７割程度。増加傾向。



一括計上・補正予算の推移

- 年々増加。
- 補正予算措置により、整備・開発を加速。

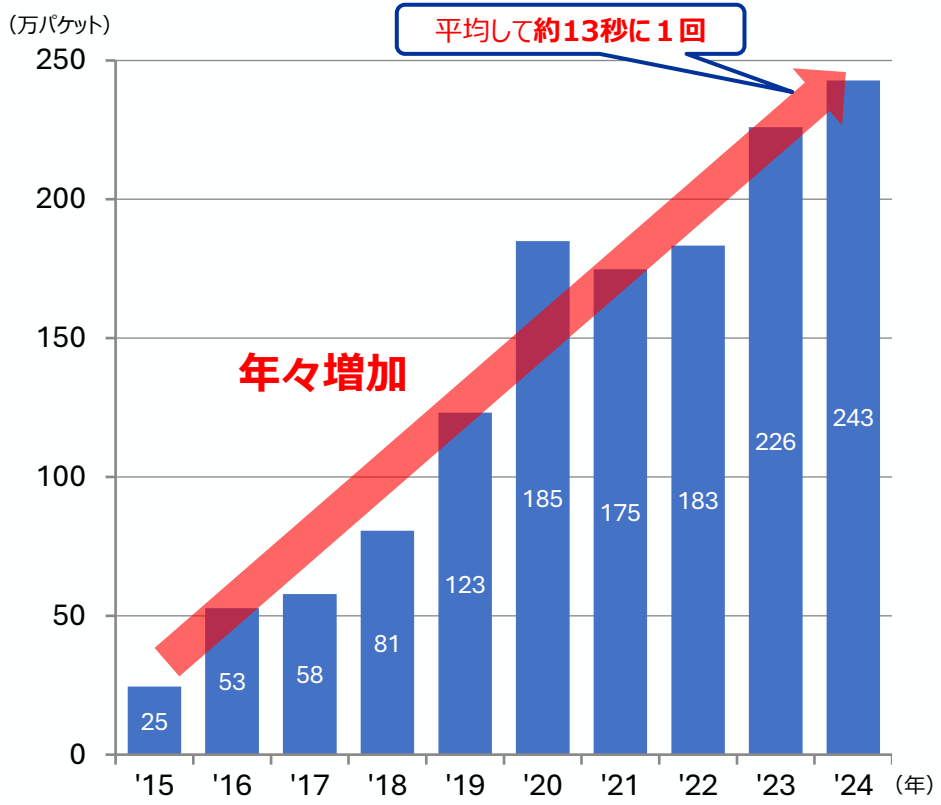


近年のサイバー攻撃の巧妙化・深刻化について

○ サイバー攻撃は巧妙化・深刻化するとともに、サイバー攻撃関連通信数や被害数は増加傾向にあり、質・量両面でサイバー攻撃の脅威は増大している。

サイバー攻撃関連通信や被害の量

NICT*1が観測したサイバー攻撃関連通信数の推移
（1つのIPアドレスで１年間に観測されるパケット*2数）



*1 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
*2 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

サイバー攻撃の巧妙化・深刻化

サイバー安全保障に関わる攻撃例

IT系システムの侵害
（暗号化・システム障害、身代金要求）
（例：2021年米コロニアルパイプライン業務停止、2022年大阪急性期・総合医療センターの業務停止、2023年名古屋港業務停止）

＋

有事に備えた重要インフラ等への侵入
（高度な侵入・潜伏能力）
（例：2014年クリミア併合、2022年ウクライナ侵略、2023年VoltTyphoonによるグアム等にある米軍施設や政府機関、重要インフラへの侵害）

＋

機微情報の窃取
（アクセス権限の獲得）
（例：2021~24年JAXAへの侵害、2023年NISCのメール窃取）

（出典：国家サイバー統括室(NCO)）

情報セキュリティインシデント事案の主な例

○ 我が国が戦後最も厳しく複雑な安全保障環境に直面する中、地政学的緊張を反映したサイバー空間を取り巻く情勢は、近年、一層深刻化。

○ 国家を背景とするものをはじめとした巧妙化・高度化されたサイバー攻撃は、我が国にとっても現に直面する安全保障上の脅威であり、重大な事態へと急速に発展していくリスクをはらんでいる。

政府機関へのサイバー攻撃の事例

- 2019 年以降、中国の関与が疑われるサイバー攻撃グループ「MirrorFace」が、日本の安全保障や先端技術に係る情報窃取を目的としたサイバー攻撃 キャンペーンを実行。
- 2022年、DDos攻撃とみられる政府機関等が運営するウェブサイトにおける閲覧障害が発生。
- 2023年、機微情報 の窃取を目的としたとみられる、内閣サイバーセキュリティセンター（NISC）への攻撃が発生。
- 国立研究開発法人宇宙航空研究開発機構（JAXA）への攻撃（2021～2024 年）が発生。
- 2025年、国土交通省近畿地方整備局のネットワークへの不正アクセス発生。

地方公共団体へのサイバー攻撃の事例

① テレワークシステム（VDI）への不正アクセス

ある地方公共団体において、テレワークシステムが脆弱性を突く攻撃を受け、攻撃者が職員のアカウントになりすましてログインする不正アクセスが行われた。

② 一部団体の対策不備によるLGWANを通じた

国のネットワークへの不正アクセス

複数団体が利用しているシステムに脆弱性があり、A町のファイルサーバに侵入され、LGWANからG-Net（国のネットワーク）へ不正アクセスが発生。

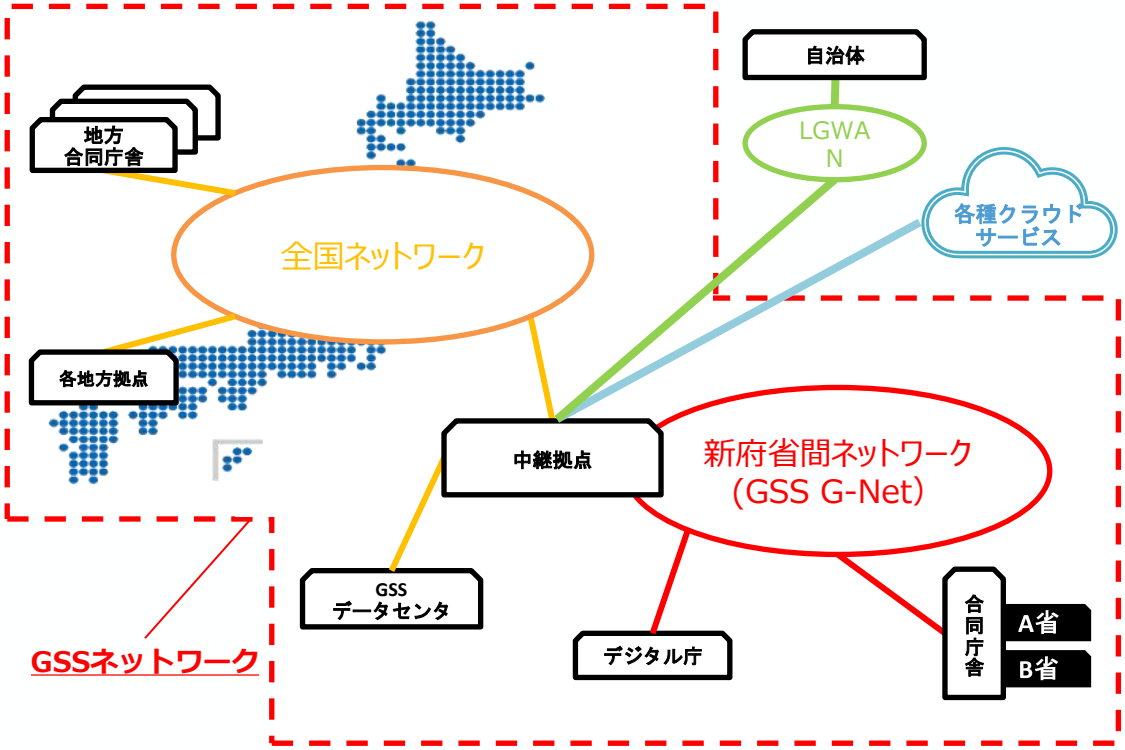
③ 印刷会社（再委託先）へのサイバー攻撃

全国の自治体の学校が委託した写真館等から卒業アルバムの印刷を請け負った事業者（再委託先）の情報システムに対して、ランサムウェアによるサイバー攻撃が行われ、児童・生徒の情報（氏名や写真）が漏えいしたおそれ。

ガバメントソリューションサービス（GSS）

○ ガバメントソリューションサービス（GSS）では、政府の共通基盤となる、柔軟で合理的なネットワークの構築と運用を行う。各府省の端末やネットワーク環境を、ゼロトラストアーキテクチャに移行（26年度末には約16万人ユーザーに倍増、今後さらに28万ユーザ規模への導入を予定）。

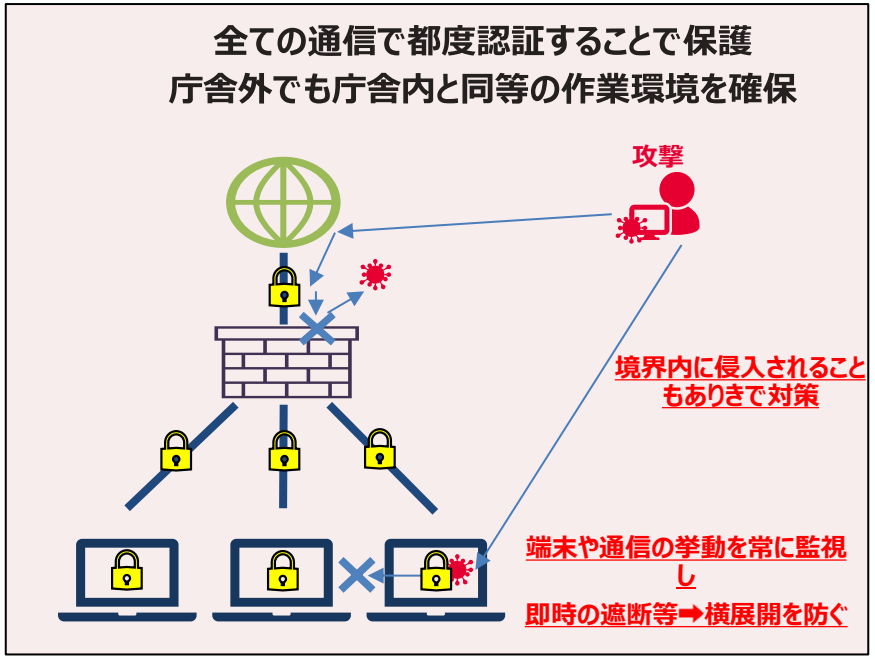
GSSネットワークのイメージ



- ✓ 各府省庁は、ネットワーク更改等を契機に、原則、GSSへの移行を進める。
- ✓ 規模拡大や高度化するセキュリティ脅威に対応するため、各府省庁の人的協力を得て、機能強化及び保守・運用体制強化を進める。
- ✓ 政府共通の標準的な業務実施環境（業務用PCやネットワーク環境）を提供。

ゼロトラストセキュリティ

- GSSでは、ゼロトラストセキュリティ（＝境界型防御＋端末防御）の採用によるセキュアな環境を実現。

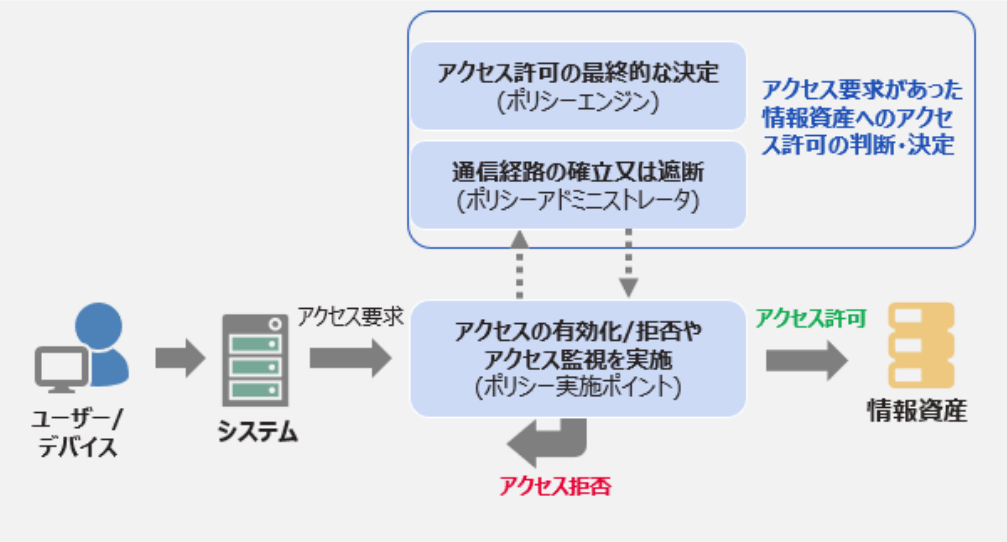


GSSにおけるゼロトラストセキュリティ

○ セキュリティ・インシデントの大多数が人的要因によるものだが、従来の境界型セキュリティ（ファイヤーウォール等による内外分離）は一か所を破れればすべてを掌握可能となってしまう

○ このため、GSSでは組織内外の人、デバイス等全てを「決して信用せず、常に把握・検証」することを前提とするゼロトラストセキュリティを採用している。

ゼロトラスト・アーキテクチャの概念図



引用元　NIST「NIST800-207　ゼロトラスト・アーキテクチャ」をもとに作成

ゼロトラスト・アーキテクチャの検証対象

ユーザ	▸システムへアクセスしたユーザーが正しいユーザーかを確認する。
システム	▸許可されたデバイス又はシステムからのアクセスか確認する。 ▸アクセス許可の条件を満たした状態のシステムかを確認する。
アクセス履歴	▸不正なアクセス等をしていないか確認する。 ▸サイバー攻撃等の兆候があるか分析する。

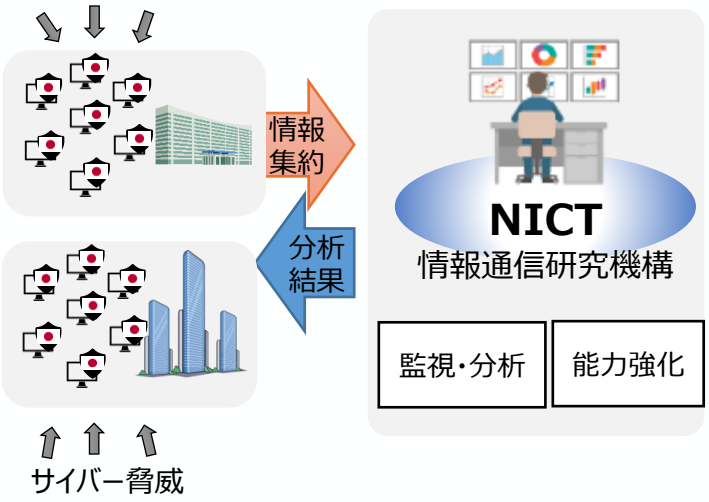
政府において今後導入・運用が想定される最先端又は高水準のセキュリティ製品・サービスの例

○ 国の行政機関や地方公共団体が率先して最先端又は高水準のセキュリティ製品・サービスを導入・運用していくことを通じて、国内のセキュリティベンダーの実績を創出することが重要。

○ こうしたベンダーが民間企業を含めた国内市場において国内高水準のセキュリティ製品・サービスの普及役となることで、民間企業におけるセキュリティ投資も促進。

CYXROSS（サイクロス）

- 国産のエンドポイントセキュリティ製品サービスをGSS移行省庁に導入し運用していくことで、独自の脅威インテリジェンスを生成。
- 民間の製品・サービスの性能評価・顕彰等にも活用していく。



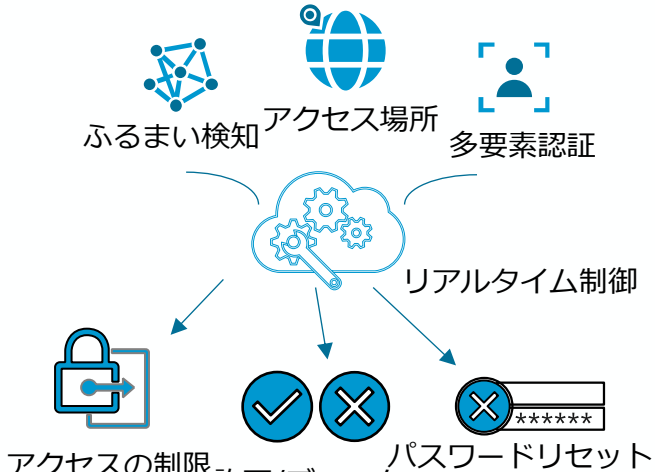
総合運用監視におけるAIも活用した最先端のセキュリティ製品サービスの導入

- AIによるサイバー攻撃に対応するためAIエージェントによる防御を行う最先端のセキュリティ製品・サービスを導入。
- デジタル庁の各情報システムからログを収集し、横断的にセキュリティ監視を実施していく。

GSSにおける高水準なセキュリティ製品サービスの導入例

ゼロトラストセキュリティを支える動的なアクセス管理

- さまざまな機器・サービスのログを統合的に収集・分析し、アクセス拒否、パスワードリセットなどの制御をリアルタイムに実行する。
- AIを含む高度な分析手法を用いることで、従来検知困難だった高度な攻撃（APT）をも検知可能に。



（参考）政府機関等におけるPQCへの移行について

○ 政府機関等における耐量子計算機暗号（PQC）への移行の方向性を整理するため、関係府省庁連絡会議において、中間とりまとめ（令和７年11月）が行われており、引き続き、工程表（ロードマップ）の策定に向け、検討を進めていくこととされている。

○ 同中間とりまとめの工程表（ロードマップ）（骨子）において、PQCへの移行期限について示している。

政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）（抜粋）
（令和７年11月 政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議）

政府機関等の耐量子計算機暗号(PQC)への移行に向けた工程表(ロードマップ)(骨子)

４．耐量子計算機暗号（PQC）への移行期限及び暗号技術の利用に係る停止の時期
（１）耐量子計算機暗号（PQC）への移行期限

原則として、2035 年を目処に、耐量子計算機暗号（PQC）へ移行を行うこととする。ただし、情報の重要性や暗号技術の利用状況等を把握した上で、どのように移行を進めるかを検討し、適切に判断する必要がある。例えば、特に機微な情報や保護期間が非常に長期となることが想定されている情報等を扱う場合等においては、より早期に移行を行うことも含め、情報システムごとに適切に検討を行うこととする。

ガバメントクラウド

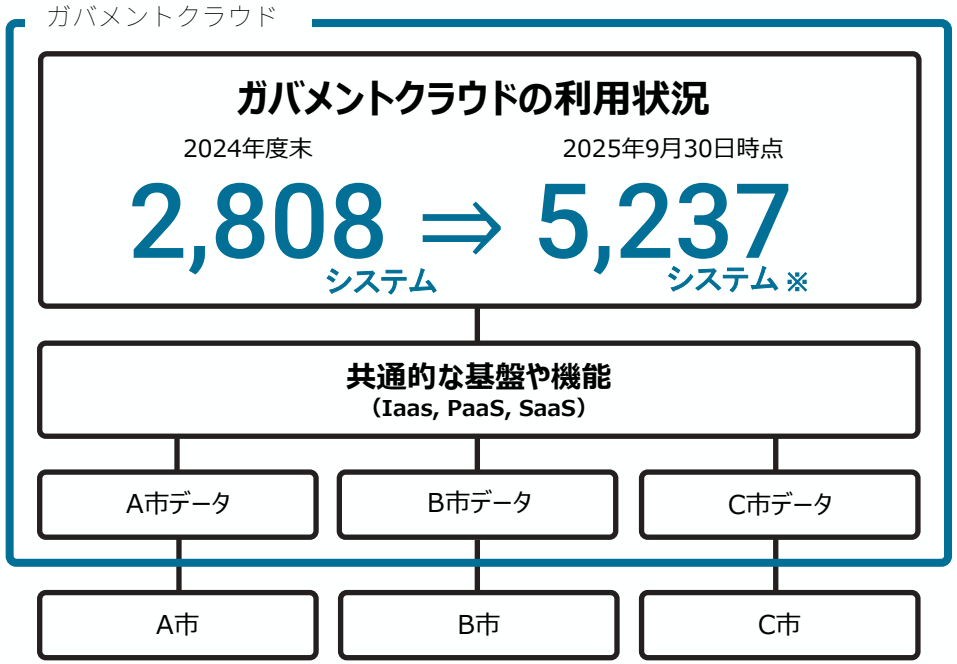
○ 従来は、行政機関はそれぞれ独自に業務システムの開発や保守運用を実施。利便性の高いサービスをスピーディに提供、改善するため、国や地方公共団体、準公共分野等で共通のクラウドサービス利用環境をガバメントクラウドとして提供。

○ 5つのサービスを提供し、5,237システムで利用（25年9月末現在）。

選定したクラウドサービス（2021年度～）

Amazon Web Services （アマゾン ウェブサービス）
Google Cloud （グーグル クラウド）
Microsoft Azure （マイクロソフト アジュール）
Oracle Cloud Infrastructure （オラクル クラウド インフラストラクチャー）
さくらのクラウド （※2025年度末までに全ての要件を満たす条件付き） （さくらインターネット株式会社）

ガバメントクラウドの利用状況



※内訳：国 147システム、地方公共団体 5,090システム

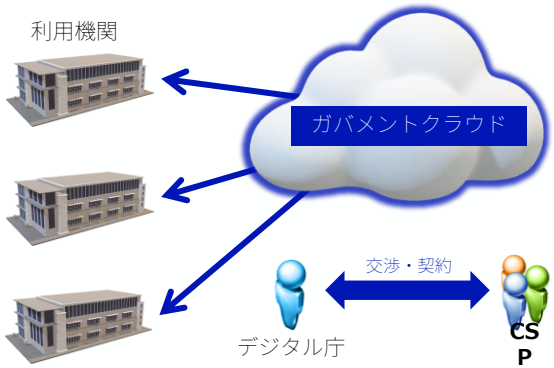
ガバメントクラウドへの移行の意義

○ 従来少子高齢化社会が進み、急速な人口減少社会に突入する中で、質の高い公共サービスを維持し、国民のニーズの多様化に柔軟に対応していくためには、国・地方公共団体・独立行政法人等の公共情報システムが共同で利用するガバメントクラウドの推進が重要。

○ ガバメントクラウドへの移行は、事務の効率化、公共情報システム全体のセキュリティレベルの高度化、大規模災害対策の実現等にも資する。

事務の効率化

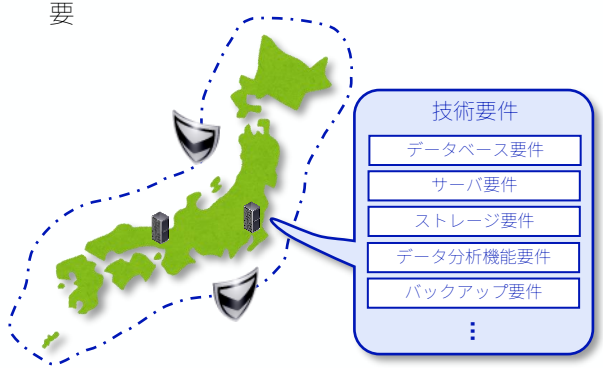
◆ クラウドサービス事業者との交渉等は全てデジタル庁が行うため利用機関の負担が軽減



セキュリティレベルの高度化

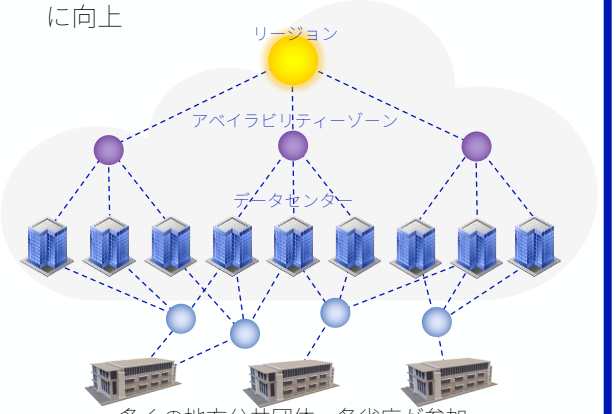
◆ 海外のデータセンターの利用禁止や各種セキュリティ設定の制御など最高水準のセキュリティ対策をデジタル庁が一括して行うため、公共情報システム全体のセキュリティレベルの向上を実現

◆ 各機関ごとに行っていたセキュリティツール、データ分析ツールなどの調達や制御が不要



大規模災害対策の実現

◆ 日本国内に分散して設置されているクラウドサービス提供事業者の複数のデータセンターにシステムとデータを保管しているため、大規模災害発生時のシステム障害・停止やデータ紛失の可能性が低減し、業務継続性が大幅に向上



自治体情報システムの標準化・ガバメントクラウド移行

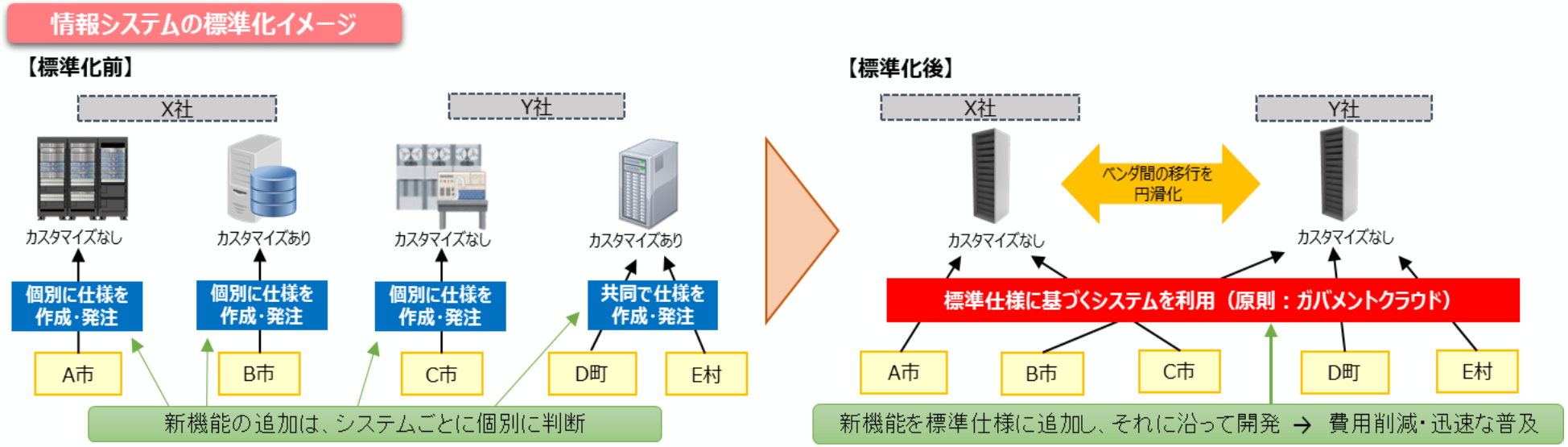
○ 自治体情報システムの標準化は、自治体情報システム（住民基本台帳、戸籍、地方税など20の基幹業務）の機能やデータについて、標準仕様に適合させることを通じて、制度改正等への迅速な対応、事業者間の競争性等を確保し、地方自治体の人的・財政的負担を軽減することを目指すもの。

○ 事業者にとっても、人材確保が困難となる中、自治体ごとのカスタマイズや保守・管理による負担の軽減により、成長分野への経営資源の投入等が可能になることが期待される。

○ ガバメントクラウドは、政府・地方自治体共通のクラウド利用環境（デジタル庁が整備・運用）であり、地方自治体の移行を促進。高度なセキュリティ、大規模災害対策の実現に資する。

○ 原則として令和７年度（2025年度）末までに、令和8年度（2026年度）以降の移行とならざるを得ないシステム（特定移行支援システム）の場合は令和12年度（2030年度）末までに、標準準拠システムへの移行を進める。

標準化対象業務数　20業務／標準化対象システム　34,592システム
（うち令和７年10月末時点での特定移行支援システム※数　5,009システム））

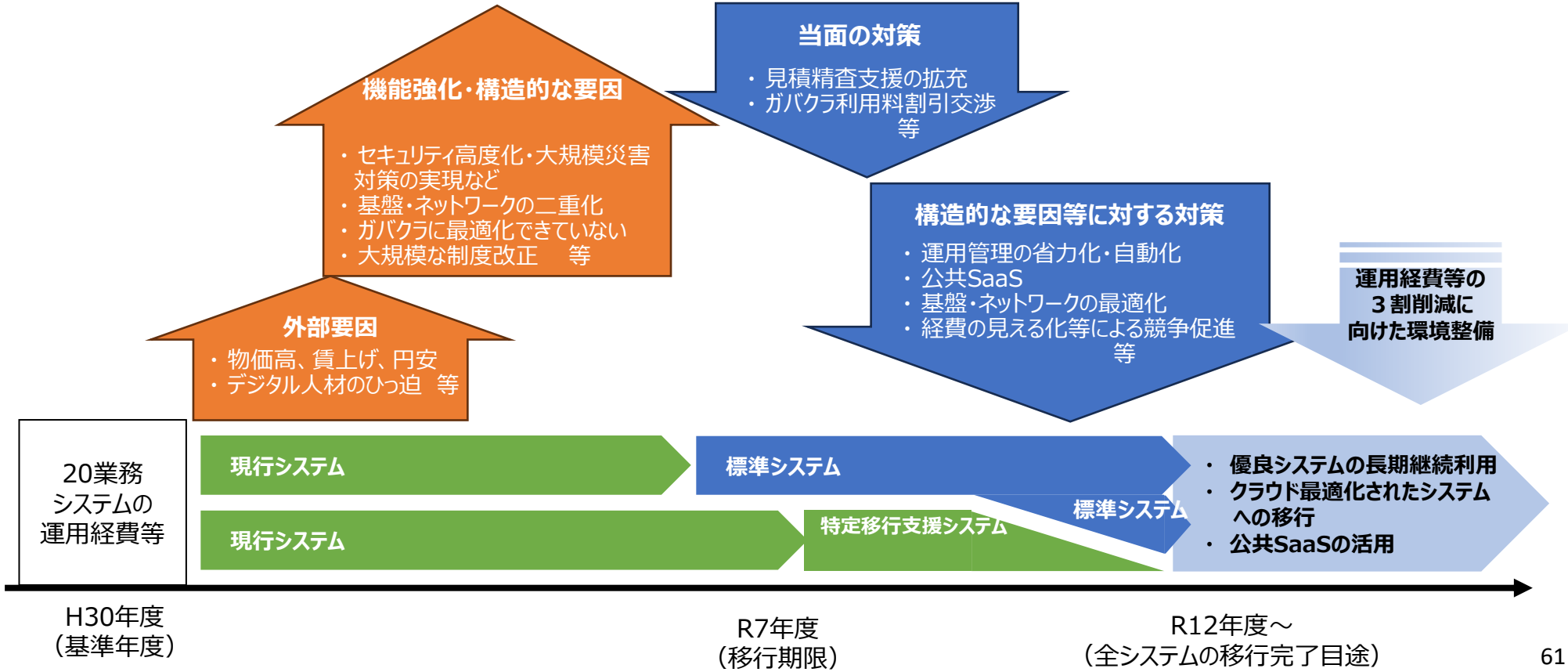


自治体情報システムの標準化・ガバメントクラウド移行

○ 一方で、移行後の運用経費が、各地方自治体の見積等によると移行前の水準より大きく増加する傾向にあることが判明。今後、国の支援の下、標準化・ガバクラ移行後に一時的に増加している運用経費の抑制・適正化を含めた運用の最適化を図っていく。

○ その際、デジタル人材の確保やリスキリング、クラウドに最適化されたシステム構築、公共SaaSの開発等、官民が連携した取組が必要。

自治体情報システムの標準化・ガバクラ移行後の運用経費に係る総合的な対策（概要）



地方公共団体のサイバーセキュリティ対策（地方自治法改正概要・今後の取組例）

○ 地制調答申において、これまでの地方自治を基盤としつつ、事務の種類に応じて、他の地方公共団体や国等と連携・協力し、デジタル技術を最適化された形で効果的に活用することが重要であるとともに、国・地方公共団体等のネットワークを通じた相互接続がますます進展する中で、地方公共団体のサイバーセキュリティ対策の実効性を担保することが必要との提言があったことを踏まえ、以下の改正を行った。（令和６年通常国会成立）

改正前

○ 現在の地方自治法には、情報システムについての**規定は置かれていない**。

○ サイバーセキュリティについては、総務省において**技術的助言**として「地方公共団体における情報セキュリティポリシーに関するガイドライン」を示すとともに、各地方公共団体はこれを踏まえ、個々の判断でセキュリティポリシーを定めている。

改正後

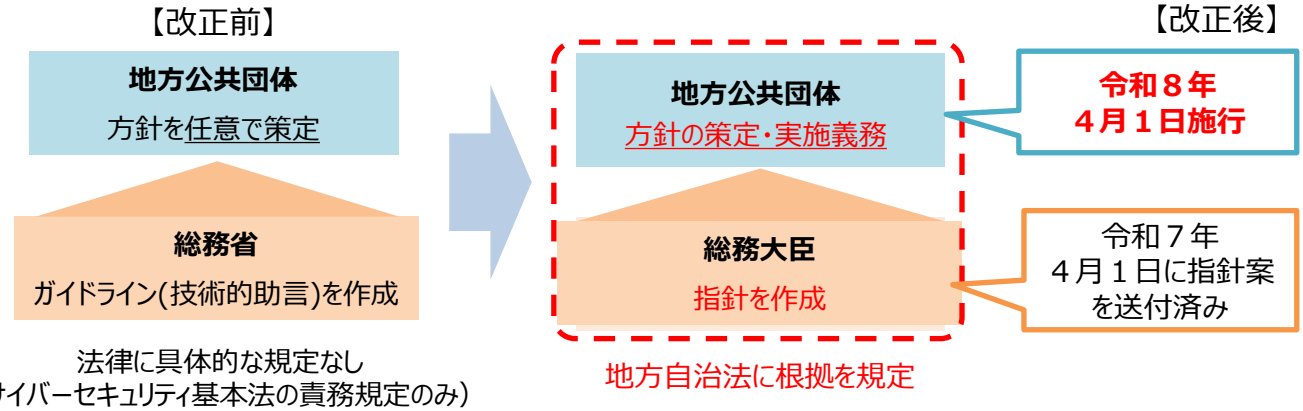
○ 地方公共団体は、**事務の種類・内容に応じ**、**情報システムを有効に利用**するとともに、**他の地方公共団体又は国と協力**し、**その利用の最適化を図るよう努める**。

○ 地方公共団体は、**サイバーセキュリティの確保**、個人情報の保護※など、**情報システムの適正な利用を図るために必要な措置**を講じなければならない。

○ **サイバーセキュリティの確保**について、地方公共団体の議会及び長その他の執行機関は、**方針を定め、必要な措置を講じる**。**総務大臣は、方針の策定等について指針を示す**。

※ 個人情報については、漏えい防止等の安全管理措置を講じるなど、引き続き、個人情報保護法に基づき適切に対応することが求められる。

＜地方公共団体におけるサイバーセキュリティ対策＞



＜今後の取組例＞

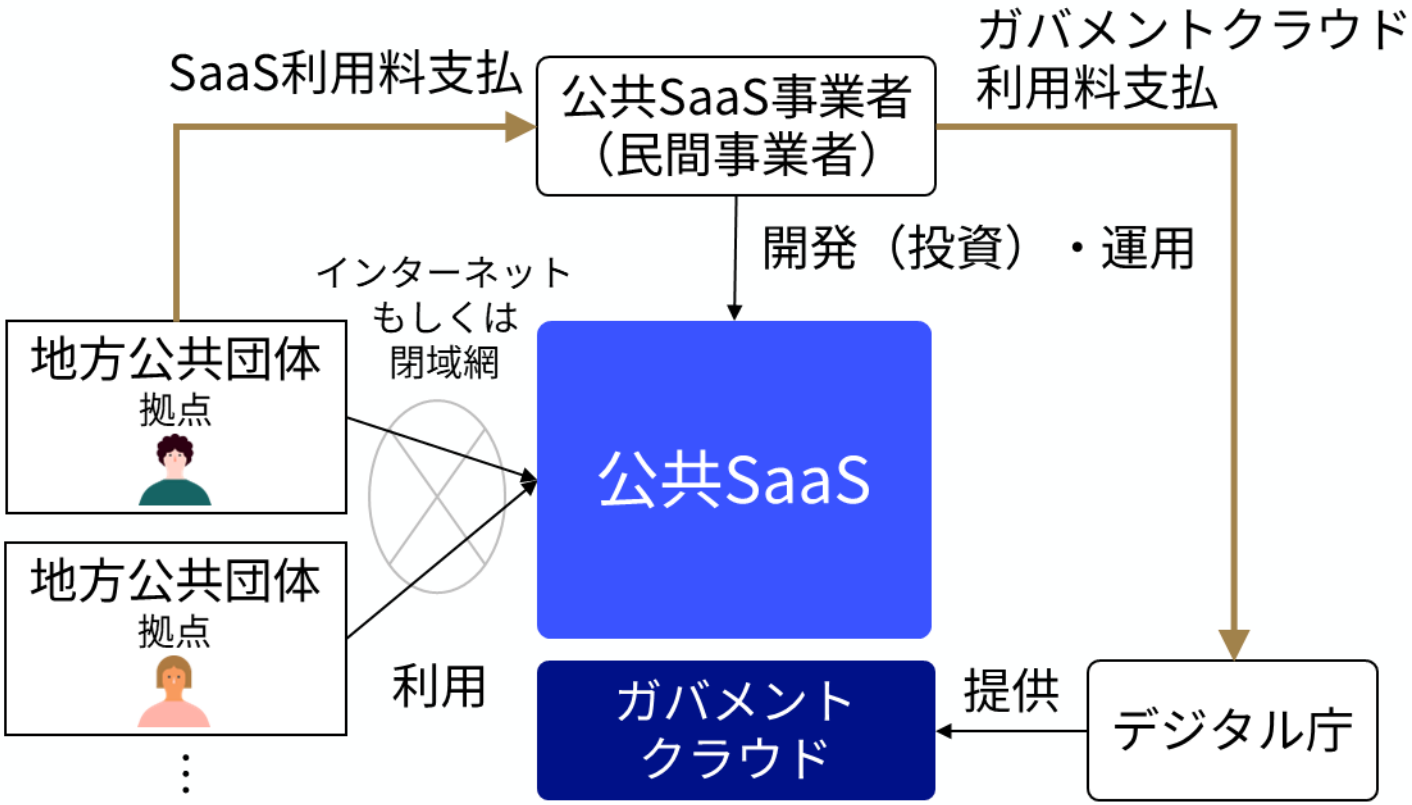
- セキュリティ人材の育成・確保。
- サプライチェーンリスク対策等における国地方連携の強化。
- ゼロトラストアーキテクチャの考え方の導入やネットワークの強靭化等によるセキュリティの強化。

公共SaaSの概要

○ 公共SaaSとは、ガバメントクラウド上で、公共向けシステムを、SaaSとして提供する形態。

○ ガバメントクラウドで一定のガバナンスを実現した上で、民間事業者（公共SaaS事業者）が、自らサービスを開発（投資）を行い、提供。

○ 地方公共団体はじめ各種団体は、所定の手続き後アクセスするだけで業務システムの利用が可能（従来は各団体が個別にシステムを開発）。



（１）デジタル
（２）サイバーセキュリティ
（３）公共･準公共
- 公共
- **医療DX**
- モビリティ

電子カルテシステムの普及に向けた取組の全体像

○ **「遅くとも2030年には概ねすべての医療機関において必要な患者の医療情報を共有するための電子カルテの導入**を目指す」（2023.6.2 医療ＤＸ推進本部、医療 DX の推進に関する工程表）。
○ **カスタマイズされたオンプレ型電子カルテから、クラウドネイティブ・廉価なものに移行**を図る方針。
○ **2026年夏までに、電子カルテ／電子カルテ情報共有サービスの具体的な普及計画を策定**する予定。

診療所
（約10.5万施設）

・約45%が電子カルテ未導入
・ここ数年で、クラウドネイティブの電子カルテベンダーのシェアが拡大している

✓診療所向け電子カルテの標準仕様の策定（R7年度中）
✓ 標準型電子カルテの開発（R8年度完成）

オンプレの診療所 約4.7万
（クラウドネイティブ電カルの診療所 約１万）
→ 標準仕様に即した低価格のクラウド型電子カルテの普及促進
※標準仕様では電子カルテ共有サービス等の対応を要件とする予定。

未導入の診療所 約4.7万
→ 標準型電子カルテ(導入版)の普及

病院
（８千施設）

・200床未満の病院の約40%が電子カルテ未導入
・小規模病院を中心に、クラウドネイティブの電子カルテが普及し始めている

✓病院向け電子カルテの標準仕様、部門システムとの連携仕様の策定（R7年度中）
↓
民間ベンダーによる標準仕様に即した電子カルテの開発（R8年度～）
↓
小規模病院等から段階的普及

中小規模の病院（200床未満）
- **オンプレ** 約３千 →
- **未導入** 約２千 →

→ 標準仕様に即した低価格のクラウド型電子カルテの普及促進

注）現状、病院向けにクラウド型電子カルテを提供しているベンダーが限られている。

大規模な病院

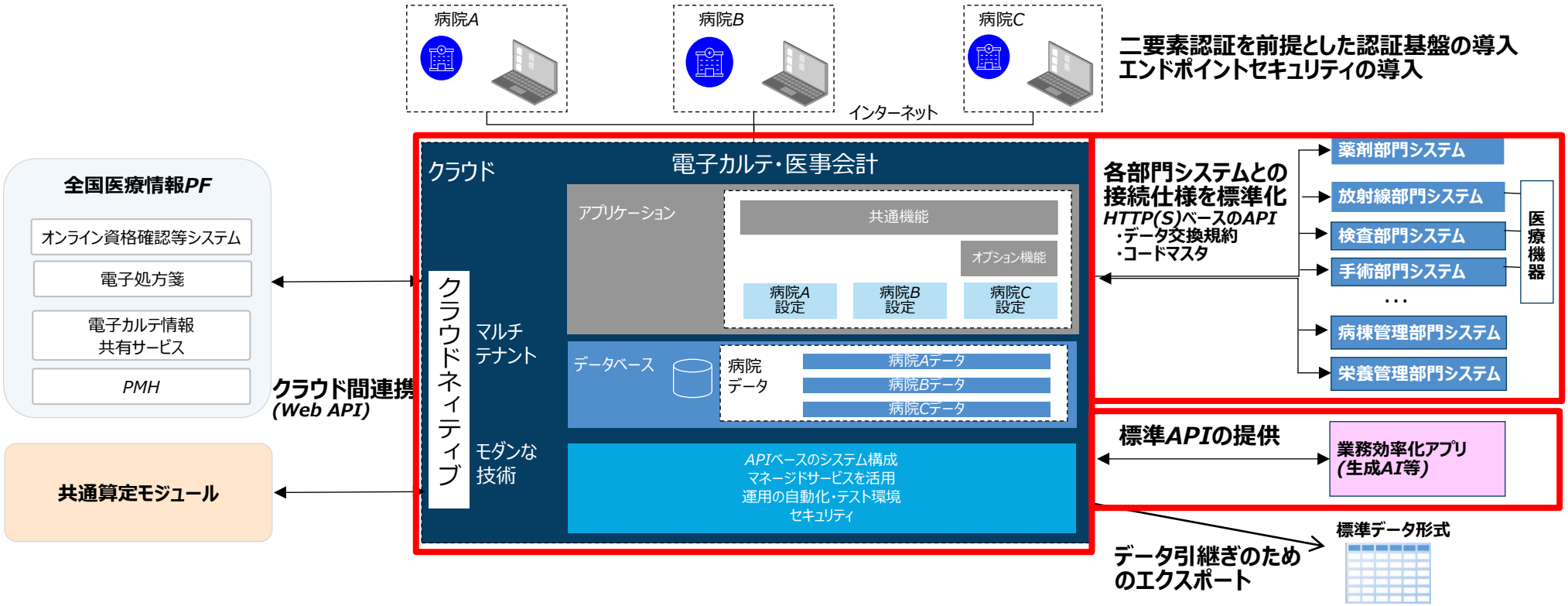
標準仕様に即した製品の拡充
大規模な病院への段階的な拡大

クラウドネイティブな電子カルテ開発に向けた取組【病院】

○ 病院向け電子カルテの標準仕様作成

令和７年度中に病院向け電子カルテの標準仕様を策定し、令和８年度から民間事業者がその標準仕様に準拠した製品を開発することを目指す。その際、ガバメントクラウドの活用を検討。

〔 病院向け情報システム（電子カルテ・医事会計）のイメージ 〕



病院における主なランサム攻撃の事例

発生	都道府県	医療機関名	病床（発生時）	医療機関の役割等	攻撃経路等
2021年10月	徳島県	つるぎ町立半田病院	120床	災害拠点病院 へき地医療拠点病院	外部ネットワークとの接続点（保守用VPN装置）の脆弱性の放置等
2022年10月	大阪府	大阪急性期・総合医療センター	865床	基幹災害拠点病院 高度救命救急センター ほか	外部委託業者（給食事業者）のシステム接続点（リモートデスクトップ）からの侵入等
2024年5月	岡山県	岡山県精神科医療センター	255床	精神科救急医療施設 応急入院指定病院 ほか	外部ネットワークとの接続点（保守用VPN装置）の脆弱性の放置等

✓ 中・大規模病院は多数の部門システムで構成されており、外部ネットワークとの接続点が網羅的に把握できていないことが研究*でも指摘されている。

＊厚生労働科学研究費補助金
「医療分野の情報化の推進に伴う医療機関等におけるサイバーセキュリティ対策のあり方に関する調査研究（令和3-4年度，研究代表者：近藤博史）」

✓ 外部ネットワークとの接続点が網羅的に把握できていないため、ネットワーク機器の脆弱性の管理や監視機器の効果的な導入が困難。

医療機関におけるサイバーセキュリティ対策に関する調査

医療機関のサイバーセキュリティ確保に関する現地調査

（目的）ネットワーク構成図等の情報資産やバックアップ整備状況に関する現地調査
（実施期間）令和４年１月～３月

●結果等
- 情報資産台帳等で**把握されていない**情報機器及び外部接続部が存在。
- 下記2パターンがあり
  - ① 外部接続部が数カ所に集約化
  - ② 検査機器毎の保守回線等、**外部接続点が多数**
- 医療機関ごとの状況は様々である。（外部接続部：**７～47**カ所/医療機関）

医療機関のサイバーセキュリティに関する意識調査

（目的）サイバーセキュリティ対策の実施状況や施設内の運用規程の有無
インシデント発生時の対応方法等に関するアンケート調査
（実施期間）令和４年9月～11月

●結果等
- 多くの院内ネットワークが異なったベンダーにより形成されており、**全体図を俯瞰的に把握できていない**
- **バックアップ接続時の設定**が適切になされていない
- ネットワークセキュリティのための必要最低限の設定がなされていない
- インシデント発生時に対応できる**人材の不足**

医療機関におけるサイバーセキュリティ確保事業

Ｒ６年度～R7年度

✓　電子カルテ導入病院を中心に外部ネットワークとの接続点の安全性の検証・検査等を実施（厚労省から委託した専門業者が実施）。
（令和５年度補正予算　36億円・令和６年度補正予算　13億円・令和７年度当初予算　11億円）

✓　多くの医療機関において外部接続点が多数存在し、管理が困難となっている実情が明らかとなった。（R6年度：1363病院を実施）

Ｒ８年度～

✓　外部ネットワークとの接続点が多数存在する医療機関に対して、その適正化まで事業対象を拡充、接続点の維持管理体制づくり等の支援を実施。
（令和７年度補正予算　１４．７億円）

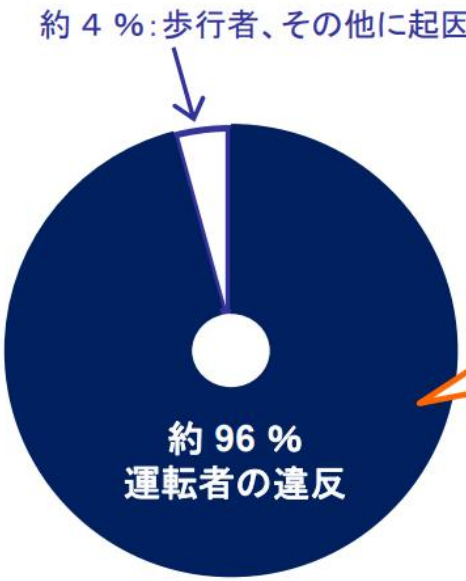
・厚生労働省委託業者によるネットワーク統合計画作成等の支援
・ネットワーク統合に必要な物品等に係る費用を医療機関に対して補助

（１）デジタル
（２）サイバーセキュリティ
（３）公共･準公共
- 公共
- 医療DX
- **モビリティ**

自動運転の意義・期待される効果

○ 自動運転の実現により「交通事故の削減」、「地域公共交通の維持・改善」、「ドライバー不足への対応」、「国際競争力の強化」、「渋滞の緩和・解消」等が期待される。

法令違反別死亡事故発生件数（令和6年）



令和7年の交通事故死傷者・負傷者数

死者数	2,547人
負傷者数	338,294人

出典：警察庁

自動運転の効果例

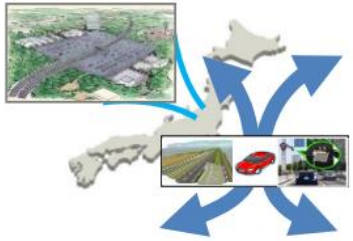
交通事故の削減

地域公共交通の維持・改善

運行の効率化

ドライバー不足への対応

国際競争力の強化



渋滞の緩和・解消

（出典）国土交通省自動運転社会実現本部第1回事務局資料から抜粋

自動運転サービスの実装に向けた海外の状況

○ 米中をはじめとして、**各国では自動運転技術の社会実装が始まっており、一部地域では既にレベル4の商用サービスが開始**。日系OEMとの連携も進む。

海外における自動運転の社会実装状況

WAYMO

【Waymo One】
- 2018年12月、アリゾナ州フェニックスで有料のレベル4商用サービス開始
- 現在、カリフォルニア州やテキサス州等の特定エリアでも一般向けサービスを提供
- **GO、日本交通と提携し、東京にも進出。2025年4月よりデータ収集を開始**
- **2025年4月、トヨタとの協業を発表**

TESLA

【Tesla】
- 2024年10月、**完全自動運転で個人/法人の利用を想定したサイバーキャブを発表**。**2026年の量産開始に向け、2025年から既存車両による自動運転タクシーの実用化を計画**
- 2025年6月、テキサス州オースティンで**自動運転タクシーの運行を開始（車種：モデルY）**

apollo

【Apollo Go（Baidu）】
- 2021年5月、北京で有料ドライバーレスサービスを開始
- **2025年10月時点で、中国国内11都市で無人自動運転サービスを展開**

pony.ai

【Pony.ai】
- 2022年5月、広州市南沙で有償の無人自動運転タクシーサービスを提供開始
- 2024年11月、米国ナスダック証券取引所に株式上場
- **2025年10月時点で、中国国内無人自動運転タクシーサービスの提供エリアを北京市・広州市・深圳市・上海市に拡大。**

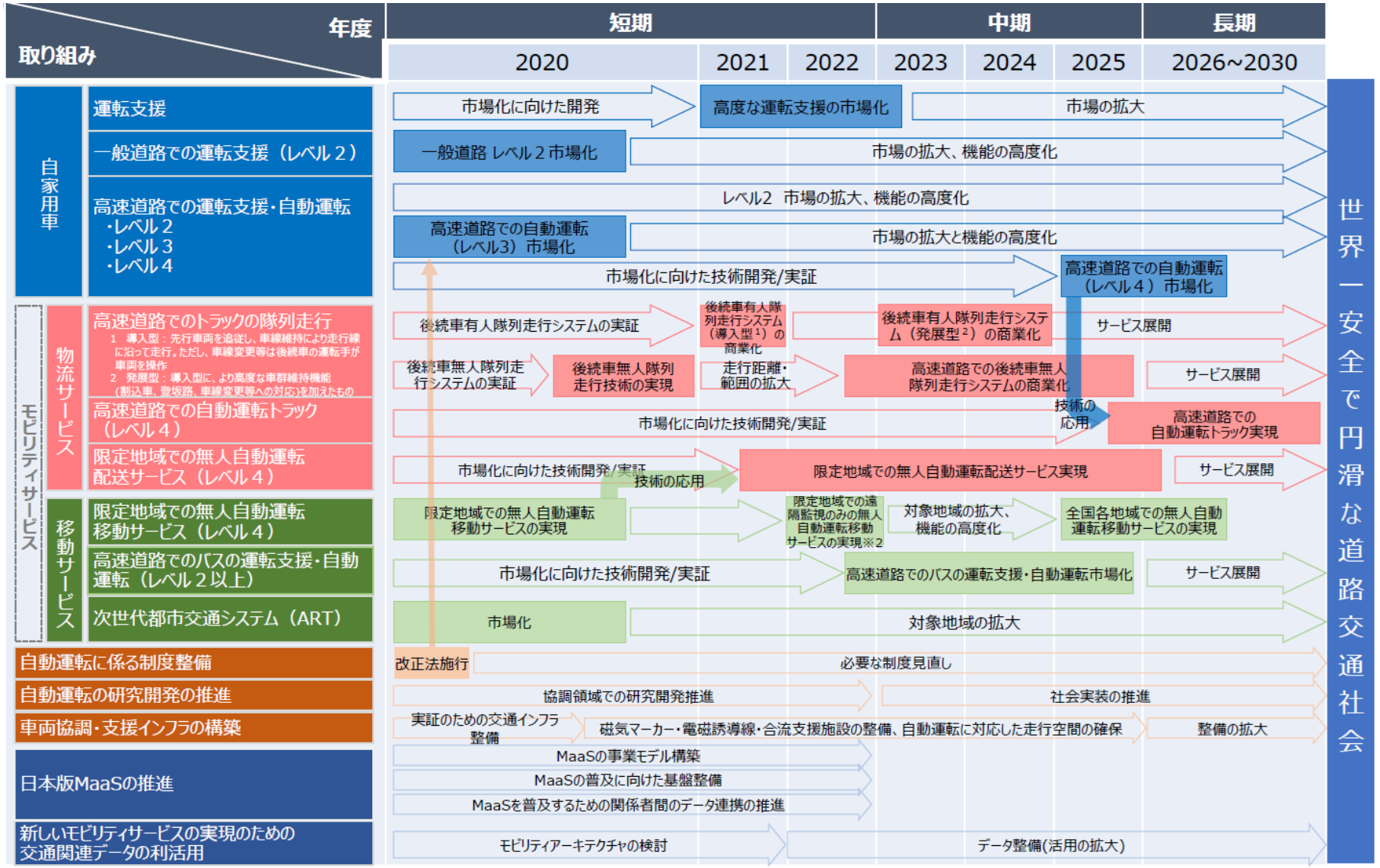
WAYVE

【Wayve】
- 2019年、ロンドンで公道実証実施。
- **2023年6月、生成AIを活用した自動運転向けの世界モデル（GAIA-1）を発表。**商用車に加え、乗用車含むあらゆる車両に適用可能な自動運転モデルを構築。高額なライダー等が不要であり、低価格での乗用車の自動運転化が可能
- 2024年10月、サンフランシスコでの公道実証を開始
- **2025年4月、日産との協業を発表**

出典：各社HP、公開情報等を基に経済産業省作成

これまでの自動運転システム・サービスの実現見通し／目標（１）

官民ITS・ロードマップ２０２０（出所）内閣官房情報技術（IT）総合戦略室



※１民間企業による市場化が可能となるよう、政府が目指すべき努力目標の時期として設定

※２無人自動運転移動サービスの実現時期は、実際の走行環境における天候や交通量の多寡など様々な条件によって異なるものであり、実現に向けた環境整備については、今後の技術開発等を踏まえて、各省庁において適切な時期や在り方について検討し、実施する。

これまでの自動運転システム・サービスの実現見通し／目標（２）

デジタル田園都市国家構想総合戦略

(出所)内閣官房デジタル田園都市国家構想実現会議事務局（2022年12月23日）

地域交通のリ･デザイン

- **MaaS等のデジタル技術の活用**等により、持続可能性と利便性の高い地域公共交通ネットワークを再構築。（*p11*施策の方向にも記載）

九州における広域MaaS（同一PF/アプリ基盤の導入）（九州全域）

- 関係省庁が連携し、**地域限定型の無人自動運転移動サービスを2025年度目途に50か所程度、2027年度までに100か所以上で実現**し、これに向けて意欲ある全ての地域が同サービスを導入できるようあらゆる施策を講じる。

国内初のレベル3無人自動運転移動サービス（福井県永平寺町）

「モビリティ･ロードマップ2025」工程表

(出所)デジタル社会推進会議／モビリティワーキンググループ

時間軸	2025年度	2026年度以降
自動運転技術のビジネスモデル		
	事業採算性の検討（経産／国交）	
	自動運転サービス等の導入に向けた指針の策定（内）	
	データの統合・相互利活用基盤の検討（内）	
	モビリティサービスをけん引する人材の育成（内）	
「交通商社機能」の確立		
	「交通商社機能」の取組に関する支援（デジ）	
	共通基盤に関する支援（デジ）	
路車協調技術など必要な技術の開発と普及		
	自動運転システムの開発支援（経産）	
	主要技術（高精度地図）の低コスト化（経産）	
	主要技術（ライダーシステム）の低コスト化（内）	
	路車協調システムの検討（国交）	
	V2X通信規格の検討・策定（総務）	
	V2N通信環境の検討（総務）	
	安全性評価環境の構築（経産）	
	混在空間における協調型システムの検討・確立（経産）	
	信号情報提供技術の検討・確立（警察）	

時間軸	2025年度	2026年度以降
路車協調技術など必要な技術の開発と普及		
	乗換・積替等のための集約拠点の整備（経産）	
	自動運転サービス支援道の整備（経産）	
	複数モビリティの協調制御技術の検討（デジ）	
事故等に対応する体制の整備・社会的受容性の向上		
	社会受容性向上のための手引きの策定（経産／国交）	
	走行空間の検討（国交）	
	審査手続の透明性・公平性の確保（警察／国交）	
	自動運転をめぐる社会的ルールの明確化（国交／警察）	
初期導入費用の低減、合理的な分業体制の確立と協調領域の設定		
	自動運転車両のリース・レンタルを促す仕組の検討（デジ）	
	自動運転がもたらす効果の評価方法の検討（国交）	
先行的事業化地域の選定及び各府省庁施策の集中投入		
	集中投入すべき施策の検討	

デジタルライフラインの全国整備

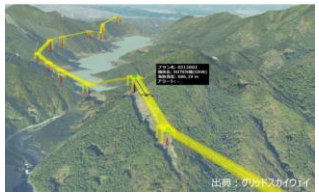
○ 23年３月の**デジ田会議における総理指示**を受け、**デジタルによる恩恵を全国津々浦々に行き渡らせるため**、約10年の中長期実装計画である**「デジタルライフライン全国総合整備計画」を24年６月に策定**。

○ デジタルライフラインの**共通の仕様や規格等を策定**し、**事業者等に遵守**を求めることで、**重複投資を回避**した官民による集中的な投資を行うことで、ドローン・自動運転等の地方における**「実証から実装へ」**の移行を加速。

○ **アーリーハーベストプロジェクト**として、**2024年度から先行地域での取組を開始**し、**①ドローン航路の整備**、**②自動運転支援道の設定**、**③インフラ管理のDX**、**④奥能登版デジタルライフライン**の早期実現に取り組む。

①ドローン航路

- 中山間地域の送電線点検や物流・河川点検のために、**ドローンを安全かつ簡便に飛行できる航路を整備**。



送電線：**埼玉県 秩父地域**
河川：**静岡県 浜松市（天竜川）**

②自動運転サービス支援道

- **自動運転車の運行を支援するセンサー**を道路側に整備し、合流支援情報の提供などを実施。

出典：ひたちBRT

<ハンズ・オフ実証の様子>
出典：T2

高速道路：**新東名高速道 駿河湾沼津SA～浜松SA間**
一般道　：**茨城県　日立市(大甕駅周辺)**

③インフラ管理DX

- 地下埋設された電気・ガス・水道等のインフラ管理情報を**デジタル化**。**点検・工事の生産性向上**を実現。

<地面を透過して埋設物を表示> 出典：Earthbrain

埼玉県　さいたま市、
東京都　八王子市

④奥能登版デジライン

- **有事に人がどこにいるかを把握するための共通の仕組み**を平時から活用するためのインフラを整備

奥能登地域