デジタル庁のトラストの検討と政府のDX

令和4年3月9日　デジタル社会共通機能グループ　角田　梨翔

デジタル庁

デジタル庁でのデータ戦略

デジタル社会の目指すビジョン

デジタル社会の目指すビジョン

デジタルの活用により、一人ひとりのニーズに合った
サービスを選ぶことができ、多様な幸せが実現できる社会

～誰一人取り残さない、人に優しいデジタル化～

ライフイベントに係る手続の自動化・ワンストップ化

官民の提供するライフイベントに係る手続やサービスについて、**スマホでワンストップ**で行うことができる。

出生、就学、子育て、介護などのライフステージに合わせて必要となる手続について、時間軸に沿った**最適なタイミングでプッシュ型の通知**が受けられる。

データ資源を活用して、一人一人に合ったサービスを

散在する健診情報、既往症、薬歴、日々のバイタル情報等の安全・安心な連携・活用により、いつでもどこでも、**一人一人の状況に合った健康・医療・福祉サービス**が受けられる。

リアルタイムの移動ニーズ、鉄道・バスの運行状況、カーシェアの空き状況等の連携により、**ストレスなく移動**できる

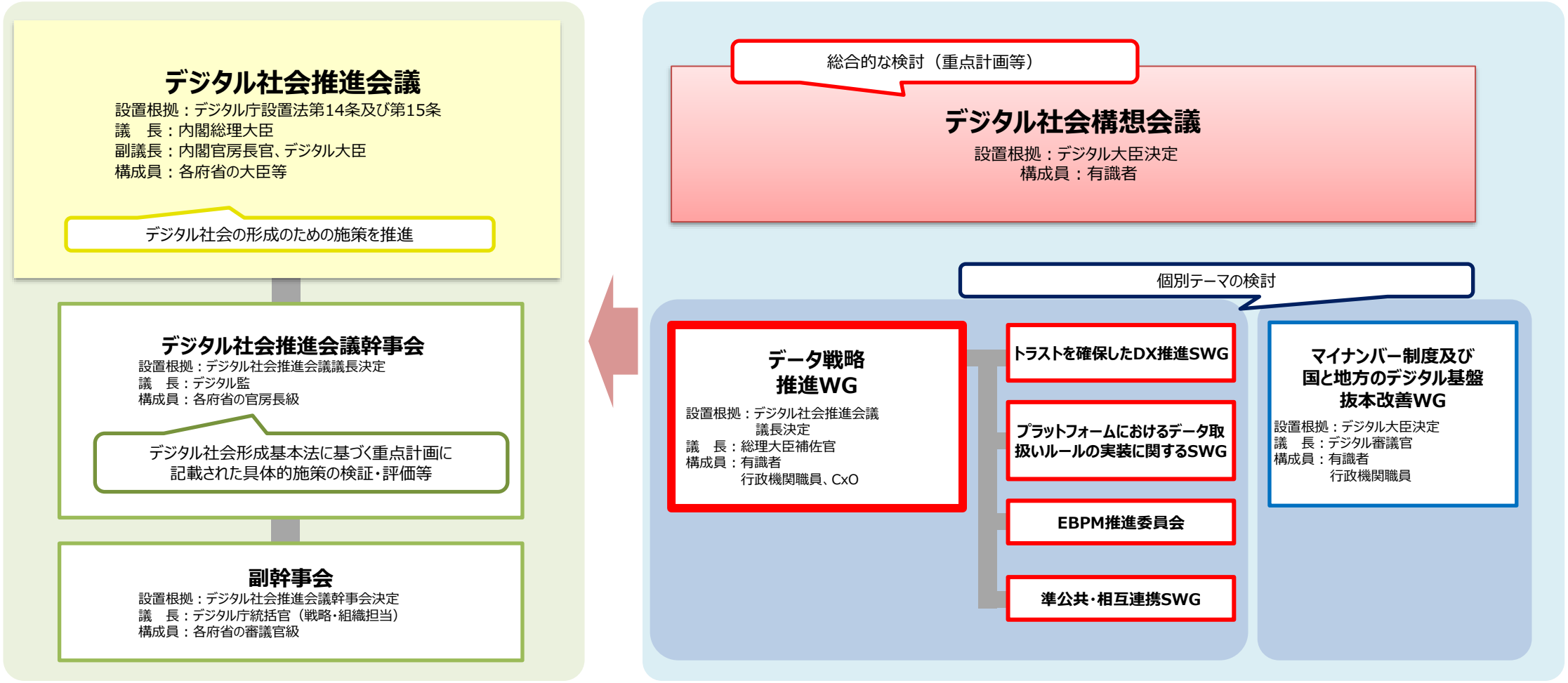
いつでもどこでも自らの選択で社会に参画

子育てや介護に適した豊かな自然環境に恵まれた場所に暮らしながら、通勤することなく**デジタル空間で仕事**ができる。

自宅に居ながら、世界中の優れた教育機関の**教育プログラムの受講**や、**文化・芸術コンテンツを体感・創作・発信**することができる。

デジタル庁でのデータ戦略の推進体制

デジタル社会推進会議：デジタル庁設置法に基づき、デジタル社会の形成のための施策の実施の推進及びデジタル社会の形成のための施策について必要な関係行政機関相互の調整を行う。



データ戦略推進WGの体制

論点と本日の議論を踏まえ、データ戦略推進WGの下に「トラストを確保したDX推進SWG」、「プラットフォームにおけるデータ取扱いルールの実装に関するSWG」、「EBPM推進委員会」、「準公共・相互連携作業グループ」を設け、具体的な検討を進める。

データ戦略推進WG

設置根拠　デジタル社会推進会議　議長決定

主査　内閣総理大臣補佐官

構成員

砂金　信一郎	LINE株式会社執行役員AIカンパニーカンパニーCEO	内閣官房デジタル市場競争本部事務局次長
遠藤　信博	一般社団法人日本経済団体連合会サイバーセキュリティ委員長 日本電気株式会社取締役会長	内閣府科学技術・イノベーション推進事務局長
太田　直樹	株式会社New Stories代表取締役	内閣府科学技術・イノベーション推進事務局審議官
佐藤　創一	一般社団法人新経済連盟政策部長	内閣府知的財産戦略推進事務局長
越塚　登	東京大学大学院教授	個人情報保護委員会事務局審議官
後藤　厚宏	情報セキュリティ大学院大学学長	総務省大臣官房総括審議官(情報通信担当)
下山　紗代子	一般社団法人リンクデータ代表理事/インフォ・ラウンジ株式会社取締役	文部科学省大臣官房サイバーセキュリティ・政策立案総括審議官
庄司　昌彦	武蔵大学教授	経済産業省商務情報政策局長
手塚　悟	慶應義塾大学教授	デジタル審議官
村井　純	慶應義塾大学教授	デジタル庁CA（Architect）
渡部　俊也	東京大学未来ビジョン研究センター教授	デジタル庁CTO（Technology）
		データ戦略統括
		デジタル庁統括官（デジタル社会共通機能担当）
		デジタル庁統括官（国民向けサービス担当）

検討項目
- ○ データ戦略の推進方策

トラストを確保したDX推進SWG

構成員
座　長：手塚　悟　　慶應義塾大学教授
有識者：トラストに関する学者、トラストサービス事業者、監査法人、弁護士など
総務省
法務省
経済産業省

検討項目
- ○ トラストスコープの再整理
- ○ DXで必要となるトラストニーズ及び実態調査
- ○ アシュアランスレベル分類
- ○ トラスト枠組みの基本的考え方

プラットフォームにおけるデータ取扱いルールの実装に関するSWG

構成員
座　長：渡部　俊也　東京大学未来ビジョン研究センター教授
有識者：法学者、法律家、データ仲介事業者など
内閣府

検討項目
- ○データ取扱いルール実装のガイダンス

EBPM推進委員会

構成員
会　　長：内閣官房副長官補（内政担当）
副会長：内閣官房内閣審議官（行政改革推進本部事務局長）
内閣府政策統括官（経済社会システム担当）
デジタル庁統括官（戦略・組織担当）
総務省行政評価局長
総務省政策統括官（統計制度担当）
会長の指定する職にある各府省庁のEBPM統括責任者

検討項目
- ○政府横断的なEBPMの取組推進
- ○統計等データの整備・改善

準公共・相互連携作業グループ

体制
リーダー：越塚登東京大学大学院教授
デジタル庁デジタル社会共通機能グループ
デジタル庁国民向けサービスグループ　　等

検討項目
- ○準公共分野・相互連携分野のデジタル化やデータ連携の推進方策の検討

包括的データ戦略の概要

■昨年末にデータ戦略タスクフォースとりまとめで示された課題について実装に向けた検討項目を整理

令和３年６月18日
閣　議　決　定

ビジョン　現実空間とサイバー空間が高度に融合したシステム（デジタルツイン）により、新たな価値を創出する人間中心の社会

データ戦略のアーキテクチャ

- 人材・セキュリティ
- 戦略・政策
- 組織（行政／民間）
- ルール（データガバナンス／連携ルール）
- 連携基盤（ツール）
- データ
- 利活用環境
- インフラ

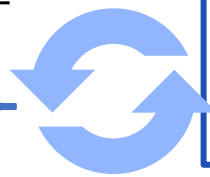
第一次取りまとめ	包括的データ戦略　検討項目
データ戦略の理念とデータ活用の原則の提唱	・データ活用原則 （①データがつながり、使える、②勝手に使われない、安心して使える、③みんなで協力する） ・行政における**データ行動原則の構築** ①データに基づく行政(文化の醸成)、②データエコシステムの構築、③データの最大限の利活用 ・**プラットフォームとしての行政**が持つべき機能
社会実装・業務改革	・デジタル庁の策定する情報システムの整備方針にデータ戦略を反映
トラストの枠組み整備	・**トラスト基盤の構築** 【デジタル庁を中心として関係省庁が協力して、2020年代早期の実装を目指す】 ・トラスト基盤構築に向けた論点整理
プラットフォームの整備	・データ連携に必要な**共通ルール**の具体化、**ツール開発** ・データ流通を促進・阻害要因を払拭するためのルールの整理 （意図しないデータ流通・利用防止のための仕組みの導入／ロックイン防止　等） 【デジタル庁と知財本部事務局は、2021年末までにガイドライン策定】 ・**重点的に取組むべき分野(健康・医療・介護、教育、防災等)**のプラットフォーム構築 【関係省庁はデジタル庁と協力して、2025年までに実装を目指す】 ・**データ取引市場のコンセプト**の提示
ベース・レジストリの整備 オープンデータ データマネジメント	・**ベース・レジストリの指定**（法人３情報、地図情報、法律・政令・省令、支援制度　等） ・ベース・レジストリの整備に向けた課題の抽出と解決の方向性の検討 【デジタル庁と関係省庁は協力して、2025年までの実装を目指す】 ・データマネジメントの強化／オープンデータの推進
引き続き検討すべき事項	デジタルインフラ：・通信インフラ（Beyond 5G）（2025年大阪・関西万博にて成果提示）、計算インフラ（富岳等コンピューティングリソースの民間利用）、半導体産業基盤の強化、データ取扱いのルール等の一体的整備 人材・組織：・データ戦略に必要な人材像、データ整備・AI活用を含むデータ戦略責任者の設置 セキュリティ：・セキュリティバイデザインの推進、安全安心なサイバー空間の利用環境の構築 国際展開：・理念を共有する国との連携や様々なフォーラムにおける**DFFTの推進** （貿易、プライバシー、セキュリティ、トラスト基盤、データ利活用、次世代インフラ） ・G７DFFTロードマップへのインプット【2023年G7日本会合を見据え成果を目指す】

トラストを確保したDX推進SWG

トラストを確保したDX推進SWGでの検討項目

官民での様々な手続・取引について、デジタル化のニーズや、必要なアシュアランスレベルを検討し、デジタル化の障壁を特定することで、官民でのDXを加速する。

1. トラストスコープの再整理
2. トラスト確保の実態調査



- デジタル化できる手続・取引の見取り図やボリュームを把握
- 手続・取引におけるデジタル化阻害要因の特定

3. ID及びトラストサービスに関するアシュアランスレベルの整理
4. 技術発展やトラストサービス利用者の利便性増大が可能となる枠組みの基本的考え方
5. トラスト確保に向けた国の関与の在り方

<u>ユースケースを特定し検証</u>

トラストを確保したDX推進SWGスケジュール

2021年12月末

- トラストスコープで集中的にニーズやユースケースを検討する範囲特定
- 電子化できる手続・取引の主要事例

2022年3月末

- トラスト実態調査分析結果に基づく対応検討
- Identificationのアシュアランスレベル整理
- トラストサービスのアシュアランスレベル整理

2022年6月末

- トラストポリシー基本方針
- ユースケース選定
- 報告書とりまとめ（日・英）

構成員・オブザーバー

構成員

手塚　悟	慶應義塾大学環境情報学部　教授 (主査)
濱口　総志	慶應義塾大学SFC研究所　上席所員
宮内　宏	宮内・水町IT法律事務所　弁護士
林　達也	LocationMind株式会社　取締役
宮村　和谷	PwCあらた有限責任監査法人　パートナー
太田　洋	西村あさひ法律事務所　パートナー弁護士
崎村 夏彦	東京デジタルアイディアーズ株式会社　主席研究員
佐古 和恵	早稲田大学　基幹理工学部情報理工学科　教授

その他関係行政機関

総務省	サイバーセキュリティ統括官付参事官
法務省	民事局商事課長
経済産業省	商務情報政策局サイバーセキュリティ課長

オブザーバー

伊地知　理	一般財団法人日本データ通信協会　情報通信セキュリティ本部 タイムビジネス認定センター長
佐藤　創一	一般社団法人新経済連盟　政策部長
西山　晃	電子認証局会議　特別会員（フューチャー・トラスト・ラボ　代表）
山内　徹	一般財団法人日本情報経済社会推進協会 常務理事・デジタルトラスト評価センター長
若目田　光生	一般社団法人日本経済団体連合会 デジタルエコノミー 推進委員会企画部会 データ戦略 WG 主査
太田　大州	デジタルトラスト協議会　渉外部会長
小川　博久	日本トラストテクノロジー協議会　運営委員長 兼株式会社三菱総合研究所　デジタル・イノベーション本部 サイバー・セキュリティ戦略グループ　主任研究員
柴田　孝一	セイコーソリューションズ株式会社　DXサービス企画統括部　担当部長 兼トラストサービス推進フォーラム　企画運営部会　部会長
袖山　喜久造	ＳＫＪ総合税理士事務所　所長・税理士
中武　浩史	Global Legal Entity Identifier Foundation (GLEIF) 日本オフィス　代表
小松　博明	有限責任あずさ監査法人 東京ＩＴ監査部　パートナー
中須　祐二	SAPジャパン株式会社　政府渉外　バイスプレジデント
小倉　隆幸	シヤチハタ株式会社 システム法人営業部　部長
島岡　政基	セコム株式会社IS研究所　主任研究員
佐藤　帯刀	クラウド型電子署名サービス協議会　協議会事務局
三澤　伴暁	PwCあらた有限責任監査法人　パートナー
小川　幹夫	全国銀行協会　事務・決済システム部長
豊島　一清	DigitalBCG Japan　Managing Director
野崎　英司	金融庁　監督局　総務課長
田中　彰子	厚生労働省 医政局 研究開発振興課 医療情報技術推進室長
肥後　彰秀	独立行政法人情報処理推進機構（IPA）デジタルアーキテクチャ・デザインセンター（DADC） インキュベーションラボ　デジタル本人確認プロジェクトチーム　プロジェクトオーナー

トラストスコープの再整理

※ デジタル庁省庁サービスグループ や内閣府公文書管理課等と連携

行政機関内文書管理

行政機関
（国・地公体）

申請・届出の提出

結果等の通知

法人内文書管理

法人

法人間取引

法人

行政機関間の文書

法人-個人間取引

プラットフォーム提供

シェアリング
サービス

行政機関
（国・地公体）

申請・届出の提出

結果等の通知

個人
（個人事業主を含む）

サービス提供

個人間契約

個人
（個人事業主を含む）

トラスト実態調査の考察

トラスト実態調査の調査項目

調査目的

DX推進にあたり、書面による契約等（手続・取引・保存）と同等レベルの信頼性を電子での契約等でも確保することが重要である。そのため、主要なステークホルダー間において行われる契約等について、トラストサービスに関するそれぞれの利用実態や活用への期待、ボトルネックとなっている点等を調査することで、トラストサービスに係る課題を可視化し、本SWGでの議論に活用する。

調査項目

- **国内のデジタル化実態 及び 海外先行事例の調査分析を通じた、トラストによるDX機会の洗い出し**
  - ・公的分野・民間分野のデジタル化の実態分析
  - ・トラスト普及の海外先行事例の把握
  - ・トラストポリシーの海外等先行事例の把握
  - ・トラストによるデジタル化の機会の洗い出し

- **トラストサービスのニーズ/課題の把握と期待効果の見積り**
  - ・トラストサービスのニーズ調査・分析
  - ・既存電子システムの課題分析
  - ・トラストサービスによるデジタル化の期待効果の見積もり/イメージ具体化

これらの調査結果を分析しつつ、本SWGにおいて、次のような検討を行う

- ・ID及びトラストサービスに関するアシュアランスレベルの整理
- ・技術発展やトラストサービス利用者の利便性増大が可能となる枠組みの基本的考え方
- ・トラスト確保に向けた国の関与の在り方に関する検討　　等

アンケート調査の実施概要

実施目的

トラストを確保したDX推進の検討のご参考とするため、企業/個人の現状やニーズ等を把握する

- トラストを確保したDXが求められる手続き等(≒トラストサービスのユースケース)
- トラストサービスの現状の利用状況、課題、及び、必要な方策

実施概要

	企業アンケート	個人アンケート
対象	国内企業 • 全国、企業規模・業界問わず	国内個人 • 全国、10代~70代以上・男女
実施方法	オンラインアンケート • 業界団体等にメール・電話等で協力依頼を行い、ご協力頂けた業界団体の加盟企業に回答依頼	オンラインアンケート
有効回答数	200社 (12月2日時点) • 245業界団体に協力依頼 • 32団体のご協力で、加盟企業(計 約11万社)にご依頼頂いた	4,406人 • 電子証明書の利用あり/なしで均等割付し、分析時に電子証明書の利用率でウェイトバック (重み付け)
調査期間	2021年11月24日~12月7日 (本資料は12月2日時点の結果)	2021年11月19日~11月24日
主な調査項目	• 基本属性 • トラストを確保したDXのニーズ • トラストサービスの導入/検討状況 • トラストサービスへの課題意識 • デジタル完結を実現するための検討への関心　等	• 基本属性 • トラストを確保したDXのニーズ • トラストサービスの導入/検討状況 • トラストサービスへの課題意識 • デジタル完結を実現するための検討への関心　等

トラスト確保のニーズが確認された主なユースケース

手続き分類	関連する人が多く、海外でも先行してトラストが導入された主な業種／分野						その他
	行政	民間					
		金融・保険	情報通信	不動産	医療・福祉	運輸・郵便	農林水産業、鉱業、建設業、製造業、電気・ガス等、卸売・小売、宿泊業・飲食業 等
厳格な本人確認が必要な申請/手続等	戸籍の届け出、住民票の取得、戸籍謄抄本の取得、投票、厚生年金保険の保険料口座振替申請	銀行口座の開設、証券口座の開設、保険の契約、送金、国際送金	携帯電話/スマホの契約、レンタル/シェアリングサービス登録/利用、年齢確認が必要なサービス等の登録/利用		遠隔医療、問診、PHR	-	-
内容の非改ざん性/真正性が必要な申請/交付/情報授受	住民票関連の申請、運転免許証、国際運転免許証、後見登記等の申請、旅券、在留カード、ワクチンパスポート、自動車保管場所標章	保険契約証書の発行	マーケティングのための顧客情報連携	社内での営業情報の報告	健診/検査結果の発行、診断書の発行、薬の処方、カルテの作成・保管、医療機関の間での患者情報の連携、	通学定期の発行、モビリティIoT(車両のデータ取得)	スマートグリッド(スマートメーターのデータ取得)
法的証拠能力が必要な文書/記録等の作成・授受・保存	税務申告、自動車関連の手続、補助金等の請求、年金関連の手続、健保関連の手続、労災関連の手続、労働基準法関連の届出 (36協定等)	融資/ローンの契約、貿易金融、為替取引	ネット回線の契約、有料放送の契約	不動産売買/賃貸契約	治験データの作成・保存・授受	国際物流関連の手続き (通関 等)	-

- 社外取引：経費の精算、受発注書の取り交わし、契約書の取り交わし、請求書の授受、商品等のトレーサビリティ確保
- 社内記録：会計帳簿の作成・保存、意思決定記録の作成・保存 (稟議、取締役会決議、株主総会決議など、稟議・決裁 …
- 規制対応：他の法律等で定められた台帳・帳簿・記録等の作成・保存 (医薬品・医療機器の台帳、外国為替取引の本人確認記録 等)

Source: 個人アンケート調査/企業アンケート調査

海外連携が必要な手続き等(アンケート速報からの現時点まとめ)

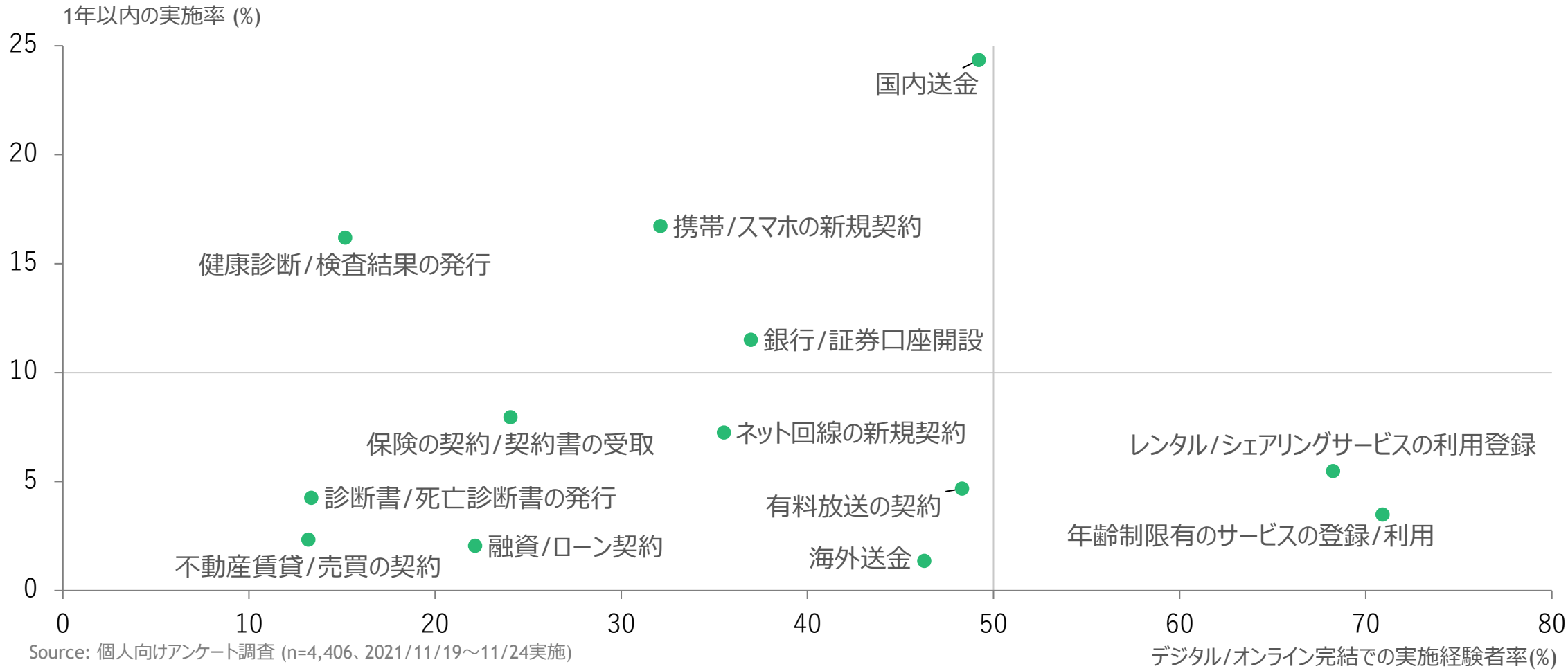
海外取引があり、本人確認や文書/データの非改ざん性/真正性が必要なものとして、
業種共通の社外取引や、「金融・保険」他の業種固有の手続き等が挙げられた

手続き分類	関連する人が多く、海外でも先行してトラストが導入された主な業種／分野						その他
	行政	民間					
		金融・保険	情報通信	不動産	医療・福祉	運輸・郵便	農林水産業、鉱業、建設業、製造業、電気・ガス等、卸売・小売、宿泊業・飲食業 等
海外連携が必要なもの							
厳格な本人確認が必要な申請/手続等	戸籍の届け出、住民票の取得、戸籍謄抄本の取得、投票、厚生年金保険の保険料口座振替申請	銀行口座の開設、証券口座の開設、保険の契約、送金、国際送金	携帯電話/スマホの契約、レンタル/シェアリングサービス登録/利用、年齢確認が必要なサービス等の登録/利用		遠隔医療、問診、**PHR (個人の健康/医療履歴の一元管理)**	-	-
内容の非改ざん性/真正性が必要な申請/交付/情報授受	住民票関連の申請、後見登記等の申請、運転免許証、国際運転免許証、旅券、在留カード、ワクチンパスポート、自動車保管場所標章	保険契約証書の発行	マーケティングのための顧客情報連携	社内での営業情報の報告	健診/検査結果の発行、診断書の発行、薬の処方、カルテの作成・保管、医療機関の間での患者情報の連携、	通学定期の発行、モビリティIoT(車両のデータ取得)	スマートグリッド(スマートメーターのデータ取得)
法的証拠能力が必要な文書/記録等の作成・授受・保存	税務申告、自動車関連の手続、補助金等の請求、年金関連の手続、健保関連の手続、労災関連の手続、労働基準法関連の届出 (36協定等)	融資/ローンの契約、貿易金融、為替取引	ネット回線の契約、有料放送の契約	不動産売買/賃貸契約 (含 重要事項説明、登記 等)	治験データの作成・保存・授受	国際物流関連の手続き (通関 等)	-
	社外取引：経費の精算、受発注書の取り交わし、契約書の取り交わし、請求書の授受、商品等のトレーサビリティ確保						
	社内記録：会計帳簿の作成・保存、意思決定記録の作成・保存 (稟議、取締役会決議、株主総会決議など)、稟議・決裁 …						
	規制対応：他の法律等で定められた台帳・帳簿・記録等の作成・保存 (医薬品・医療機器の台帳、外国為替取引の本人確認記録 等)						

Source: 企業アンケート調査

個人手続きにおけるトラストが必要と考えられるユースケース

トラストが必要と考えられる手続き等で、1年以内に1割以上の人が実施する実施規模が大きいものも含め、デジタル/オンラインでの実施経験率は半分に満たないものが殆ど
(例: 国内送金、携帯/スマホの新規契約、銀行/証券口座開設、健康診断結果の発行等)



Source: 個人向けアンケート調査 (n=4,406、2021/11/19～11/24実施)

トラストサービスへの課題意識（企業全体）

認知度不足や企業間での共通化の難しさの他に、事業者/サービス選定の難しさ（「どのトラストサービス事業者を使えば適切かわからない」等）も課題に挙がっている

Note: それぞれの割合は、全回答者 (N=347)に対する割合。導入済み/検討経験ありと検討したことがないの合計は、「わからない」を除くため、合計100%にならない
矢印は明確な分析結果に基づくものではないか、関係性が深いと考えられる箇所に記載
Source: 企業アンケートよりBCG分析

Identificationアシュアランスレベルの整理

海外におけるIdentificationアシュアランスレベルの状況

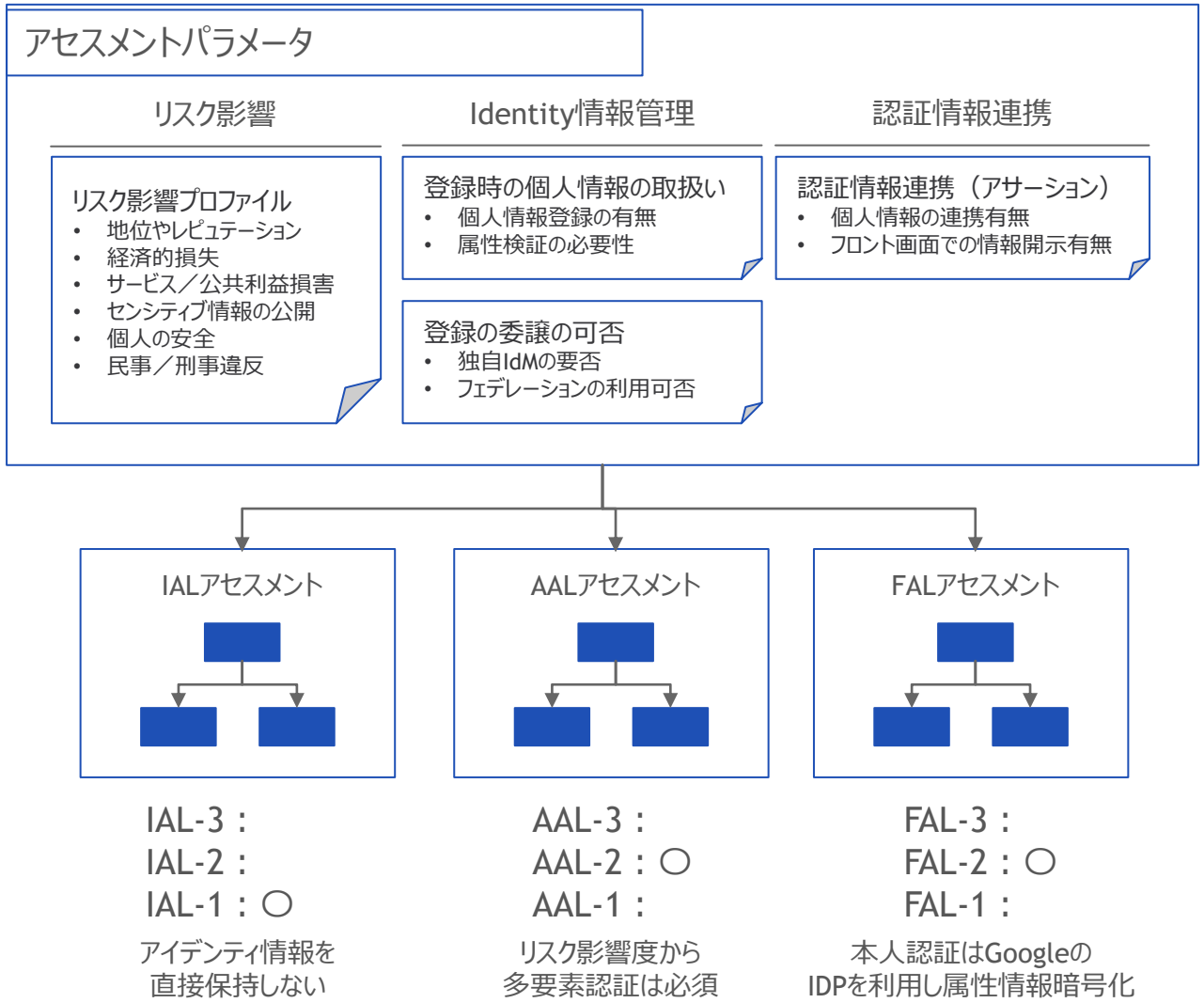
定義カテゴリ	定義内容	各国の整備有無状況（内容の差異は存在）		
		eIDAS	NIST SP800-63	NZの Identification 管理基準
本人確認（IAL※1）	本人確認方法の確からしさをレベル分けする	✓	✓	✓
認証プロセス（AAL※1）	認証プロセスによって認証強度をレベル分けする	✓	✓	✓
トラストサービス事業者の運営条件	トラストサービスの提供元が信頼できる機関であるかどうかを定めた要件を満たすかどうかによってレベル分けする	✓	–	–
認証情報連携（FAL※1）	認証した情報を別機関に連携する際の連携方法の確からしさをレベル分けする	–	✓	✓
割当（Binding※2）	RP(Relying Party)が個人や組織といったエンティティをエンティティの情報に割り当てたり、エンティティを認証プロバイダーに割り当てるプロセスの堅牢性をレベル分けする	–	–	✓

※1 SP800-63-3 におけるアシュアランスレベルの定義名を記載
※2 ニュージーランドのIdentification管理基準におけるアシュアランスレベルの定義名を記載

SP800-63-3：基本的な考え方

各事業者がリスク影響度や個人情報の取扱い有無等をインプットに、適切なアシュアランスレベルを選択する基準を提示

アシュアランスレベルのアセスメントフロー



アセスメントの意義／効果

- ビジネス／セキュリティ／プライバシーのための適切なリスクマネージメントの実現

  各サービス事業者が、サービスが取り扱うIdentityのリスク影響度を６カテゴリで定義し、規定された共通のアセスメントロジックによりアシュアランスレベルを個別に選択できるようにする。

  例）本来必要とされるレベル以上のアシュアランスを実現するため、コスト増大するようなケースを抑止する。

- マイクロサービス化されたIdentity ソリューションへの対応

  政府システムにおいてもIdentityソリューションは単一ベンダーが全機能を提供するモノリシックなものとは限らない。

  分散マイクロサービスによるアイデンティティ管理／認証連携を前提とするアシュアランスレベル選択を可能とする。

  例）Identity Management／認証はプラットフォーマーのIDP機能へ委譲（フェデレーション）する

Source:NIST Special Publication 800-63 Revision 3 (NIST)(https://pages.nist.gov/800-63-3/sp800-63-3.html)等を元に作成

SP800-63-3：アシュアランスレベル一覧

各事業者がリスク影響度や個人情報の取扱い有無等をもとに、ユーザーの身元情報、ユーザー認証、連携方法の確からしさからアシュアランスレベルが定義されている

定義内容	定義LoA	LoAの詳細	
ユーザ身元確認の確からしさ	IAL（Identity Assurance Level）SP 800-63A	IAL.1	身元確認不要、自己申告の登録でよい。メールアドレスの到達確認など
		IAL.2	識別に用いられる属性をリモートまたは対面で確認する必要あり
		IAL.3	識別属性を対面で確認する必要があり。検証担当者は有資格者
ユーザ認証の確からしさ	AAL（Authentication Assurance Level）SP 800-63B	AAL.1	1要素もしくは2要素による認証
		AAL.2	2要素認証、NIST/FIPSで認可された暗号化手法の利用が必須
		AAL.3	AAL2に加えて、ハードウェアベースおよびなりすまし耐性を持つ認証子の利用が推奨
連携方法の確からしさ	FAL（Federation Assurance Level）SP 800-63C	FAL.1	アサーション（RPに送るIdPでの認証結果データ）への署名
		FAL.2	FAL.1に加え、対象RPのみが復号可能な暗号化
		FAL.3	FAL.2に加え、Holder-of-Key アサーションの利用（ユーザごとの鍵とIdPが発行したアサーションを紐づけてRPに送り、RPはユーザがそのアサーションに紐づいた鍵を持っているか（ユーザの正当性）を確認）

Source:NIST Special Publication 800-63 Revision 3 (NIST)(https://pages.nist.gov/800-63-3/sp800-63-3.html)

SP 800-63-3：AALに関する要求詳細

	認証要素に関する要求	**Hardware-based authenticator**	**verifier impersonation resistance**
SP800-63-3における Requirement Type※	AAL２以上では、二要素認証および FIPS/NISTで認可された暗号化手法が要求される。 AAL3では加えてフィッシングやOTP侵害等に対応するハードウェア認証子の利用をしなければならない(shall use)とされる	• FIPS 140 validation 認証子や暗号化デバイスに加えて、認証者、フィジカルセキュリティに関して、FIPS 140-2に規定されるレベルを満たすことが要求される	• verifier impersonation resistance フィッシング等のなりすましに対する耐性 PKIを使った認証要求者とのチャネル確立等 • verifier compromise resistance 認証処理への侵害に対する耐性 生成したOTPを盗まれるリスクへの対応等
AAL.1	either single-factor or multi-factor authentication using a wide range of available authentication technologies	• Level 1: Government agency verifiers	要求しない
AAL.2	Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required	• Level 1: Government agency authenticators and verifiers	要求しない
AAL.3	（AAL2の要求に加えて）shall use hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device may fulfill both these requirements.	• Level 2 overall: MF Authenticators • Level 1 overall: verifiers and SF Crypto Devices • Level 3 physical security: all authenticators	**要求する**

※Permitted authenticator types、Reauthenticationなどその他要件も定義されているが、本スライドでは要求一覧より主要な要求事項を抜粋して掲載

Identificationアシュアランスレベルで考慮すべきユースケース

マイナンバーカードをサービスの認証に一層活用するなど、行政からのユースケースの具体化が提案された

- **マイナンバーカードの電子署名用電子証明書及び利用者証明用電子証明書**の本人確認及は、世界的にも最高レベルであるため、様々なサービスの認証における信頼の起点として活用するべき
- **新型コロナワクチン接種証明書アプリ**は、マイナンバーカードを利用して簡単に登録できるという点で、ID Proofingのユーザビリティやコストが改善された
- **前橋市の「まえばしID」**のように、マイナンバーカードでの電子署名を起点として作られた別のIDのユースケースも念頭に置くべき
- **Identificationと行政データの連携が可能な仕組みの整備**が必要。（マイナポータルの「自己情報取得API」において、マイナポータルアプリによる公的個人認証を用いたログインが必須となっている。）

IALにおけるユースケースのマッピング案

既存の国際標準等を参照した上で、行政手続を中心に、日本の実情に応じたIdentificationアシュアランスレベルの整理が提案された。

IAL	Identifier	本人確認方法	ユースケース
IAL-3	信頼できる機関により電子的に身元証明可能なもの	対面で確認	マイナンバーカードを使用した対面での申し込み
		非対面	マイナンバーカードを用いた電子署名
	発行元保証されている身元証明可能なもの	対面での有資格者による確認	対面での身分証明必須のID/PASSの発行 (e-Tax 等)
		対面相当オンライン (eKYC)	オンラインでの身元証明書上の本人写真とリアルタイム本人画像のマッチング
	⋮	⋮	⋮
?	発行元保証されている身元証明可能なもの	オンライン登録後対面で確認	オンラインでの銀行口座開設→カード受け取り時本人確認
IAL-2	信頼できる機関により電子的に身元証明可能なもの	非対面で確認	オンラインでのマイナンバーカードリーダーを用いた口座開設
	発行元保証されている身元証明可能なもの	非対面で確認	オンラインでの本人確認書類 (画像アップロード 等)を用いたECサイト会員登録
IAL-1	身元確認のない自己表明可能なもの	身元確認なし	サービス登録時におけるメールアドレスでの通達確認

論点

1. 「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」にインプットするにあたり、各マスに入れるべきユースケースはどのようなものがあるか
2. ユースケースは、技術進化とともに、継続的な見直し、反映が必要になるが、国の役割はどうあるべきか。

AALとユースケースのマッピング案

既存の国際標準等を参照した上で、行政手続を中心に、日本の実情に応じたIdentificationアシュアランスレベルの整理が提案された。

	認証プロセス	ユースケース
AAL-3	AAL2に加えて、ハードウェアベースおよびなりすまし耐性を持つ認証子の利用が推奨	マイナンバーカードの利用者証明用電子証明書による認証 ICカード方式・リモート署名利用による申告 ID/PASS+ハードウェアトークンによるワンタイムパスワードによる認証及びなりすまし耐性を持つ認証子の利用
AAL-2	要素認証、NIST/FIPSで認可された暗号化手法の利用が必須	Smart-ID方式・リモート署名利用による申告 ID/PASS+ソフトウェアトークンによるワンタイムパスワードによる認証
⋮	⋮	⋮
AAL-1	一要素認証	ネット証券口座利用におけるID/PASSによるログイン及び取引時に別パスワード利用 サービス利用時におけるID/PASS
AAL-0	認証なし	宅配便の受け取り メールアドレスの送達確認のみ

論点

1. 「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」各レベルに入れるべきユースケースはどのようなものがあるか
2. ユースケースは、技術進化とともに、継続的な見直し、反映が必要になるが、国の役割はどうあるべきか。

トラストサービスアシュアランスレベルの検討の進め方

トラストサービスアシュアランスレベルの基準で担保すべきもの

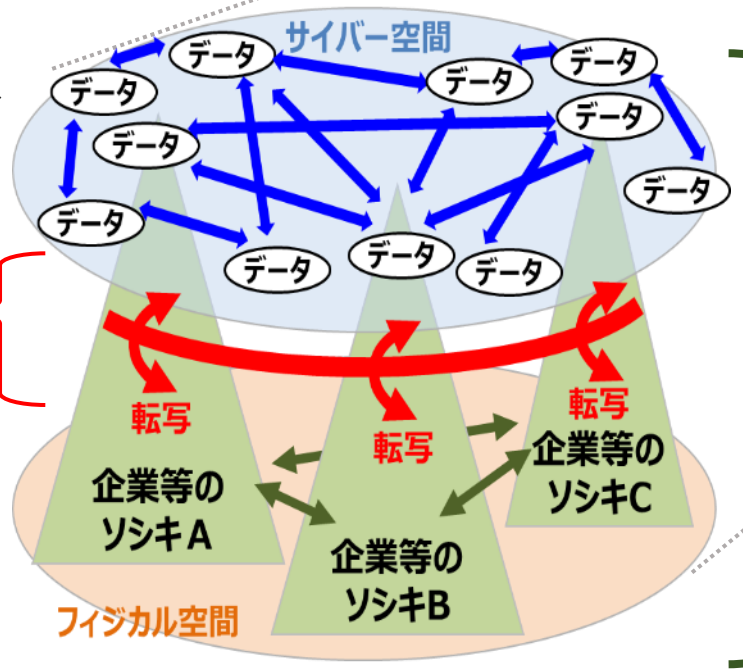
トラストサービスアシュアランスレベルでは、データの信頼性のみならず、フィジカル空間とサイバー空間のつながりにおけるトラストや、時間経過後のトラストも考慮するべきだと指摘された。

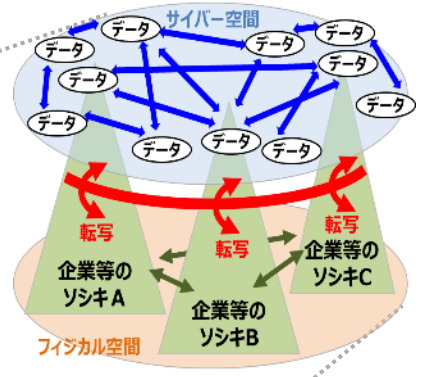
「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保





将来的な担保：
時間経過後のトラスト

現状の担保：
紙が持つ真正性・非改ざん性をデジタルに持ち込むこと

将来的な担保：
情報の発出者（ソシキ、ヒト、モノ）と、当該情報を表現する媒体に関わらず改ざんされていないことを担保するときに必要になるトラスト

図出典：経済産業省、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）のポイント

トラストサービスアシュアランスレベル策定における課題

トラストサービスのアシュアランスレベルを策定するにあたり、最高レベルを国が担保する確立体制の困難さ、アシュアランスレベルを規定する要件の整理、継続的な監査を担保するメタデータ連携の必要性等の課題が提示された。

- **国の役割**：トラストサービスのアシュアランスレベルの最も高いレベルを国が担保するとした場合、国として最新の仕様をメンテナンスし続け、監査する体制が確保できない可能性がある
- **策定作業**：技術基準について、欧州ETSI、CENで標準化されている技術基準と同レベルのものを想定するのであれば、膨大な作業を防ぐ上でも、既にある基準をベースに作業を省略していく工夫が必要
- **対象：**何をもっての正当かがユースケースによって異なる中で、レベルではなく、何の正当性について議論しているのか整理が必要ではないか
- **軸の関係性**：Identificationアシュアランスレベルとトラストサービスアシュアランスレベルは、相互依存性の無いパラメーターにするべき
- **監査要件**
  - 認定事業者の認証の際の監査体制において、一時点の監査ではなく、運用に対する透明性をAIによる自動検査などでメタデータ連携を行い、担保していくことが重要
  - 監査要件は、認定手続の中に入るのであれば理解できるが、アシュアランスレベルそのものの中に監査要件が入ってくるというのはやや違和感

トラストアシュアランスレベルで担保する内容が多岐に渡りかつ策定にあたり考慮すべき課題が多いため、
まずはユースケースにフォーカスした議論を進めるべきではないか

（参考）主な意見（国際的通用性）

トラストサービスのアシュアランスレベルにおける国際的通用性の検討においては、議論を深めるにあたり、**「相互承認」の定義についての共通認識**の醸成や、EUのeIDASで**相互承認国が存在していない理由の深掘り**が必要との意見が出た。

国際的通用性の確保に向けて

国際的基準との整合性及び関連基準（ISO/IEC 27000シリーズ、CAB/F　baseline requirement、ETSIやCEN規格、Webtrust監査基準等）を参照した上で、各トラストサービスに対し、これらの基準への適合性評価を行う機関の要件を国際標準（ISO/IEC17065、ETSI EN 319 403など）を参考に規定するべき

議論の進め方についての課題

- **eIDASでEU域外との相互承認国が存在しない理由・障害となっている点を明らかにするべき**。障害となっている事由や実現可能性の有無を確認したうえでの議論が必要
- 国際的通用性が必要な取引として「国境を越えた契約書」が挙がっているが、**契約書は準拠法を書くのでInteroperabilityは不要**ではないか。一方、**DFFTにおいては、契約書とは別に流通していくデータについてのトラスト確保が必要**
- **Interoperabilityを確保すれば、相手国の法律が準拠法であっても、自国のトラストサービスが利用できる**のではないか。例えば、日本法が準拠法となる場合に、外国企業でも日本の法律に基づいて判断されるため、外国企業も日本のトラストサービスを利用する必要が出てくる。逆に、欧州の法律が準拠法なら、日本企業は、日本のトラストサービスではなく欧州のトラストサービスを使うことが必要になってくるのではないか。
- **相互承認（Mutual Recognition）という用語への共通認識**を持った上で、何を目的とした何に関するどの国（地域）との相互承認を検討するのか明確にすべき。 何らかの相互承認を目指す場合は、その対象は下記①②のどちらなのか。

（参考）主な意見（その他考慮すべき要素）

基準の機動性を確保するため、規格策定と継続的な検証を専門とする組織を設置するべきであること、電子署名法の技術基準の見直しや他のトラストサービスの信頼性担保の検討を行うべきとの意見が挙がった。

機動性の確保するための考え方

- 規格を技術進化、国際標準、社会環境に準じて柔軟にバージョンアップを行うべく、規格策定及び継続的に検討する**専門的な組織の設置の検討**が必要
- 各基準は法令から参照される**独立した技術規格として策定されるべき**であり、変化する技術進化や国際標準に対応したメンテナンス性が確保されることが必要

既存の制度との整合性

- トラストサービスの議論を深めるにあたり、**電子署名及び認証業務に関する法律の見直し（技術標準の活用を含む。）の検討**は避けて通れない
- 電子署名やeシール等の有効活用を促進するためには、認定認証業務に代表される**信頼性の高いトラストサービスについて推定効などの法的効果を検討する必要**がある

ユーザービリティ

- どのレベルを満たしたトラストサービスであるか**利用者にわかりやすい形での基準策定や仕組み（認定トラストサービスの機械可読な形での公開、当該トラストサービスに基づく情報の検証）の検討**が必要
- 電子文書の通用性は、例外なく電子的な形式であるという理由で否定されないとすべき

デジタル原則の実現におけるトラストサービスの活用可能性

デジタル臨時行政調査会設置の意義

デジタル化の恩恵を享受できる社会へ規制・制度を構造改革

第１回資料「デジタル臨時行政調査会における論点（案）について」より抜粋

○今世紀に入ってから、我が国の官民を通じたデジタル化の遅れは深刻。**既存の規制や行政などの構造は維持されたままで、経済、社会、産業全体のデジタル化につながらず**。

○デジタル庁設立でデジタル改革の推進体制は整備されたが、**規制・行政のあり方まで含めて本格的な構造改革をしなければ、デジタル化の恩恵を国民や事業者が享受し、実感することは困難**。

○コロナが浮き彫りにした日本のデジタル化の遅れは、他の全ての分野に通じる本質的課題。

○国民がデジタルを活用したより良いサービスを享受し、**成長を実感できるためには、国を構成する「国民」「社会」「産業」「自治体」「政府」といった主体・分野にまたがる本質的「構造改革」が必要**。

○「国民や地域に寄り添う」とともに「個人や事業者がその能力を最大限発揮」できる社会をデジタルの力で実現。

○**全ての改革（デジタル改革、規制改革、行政改革）に通底する「構造改革のためのデジタル原則」を共通の指針として策定**。

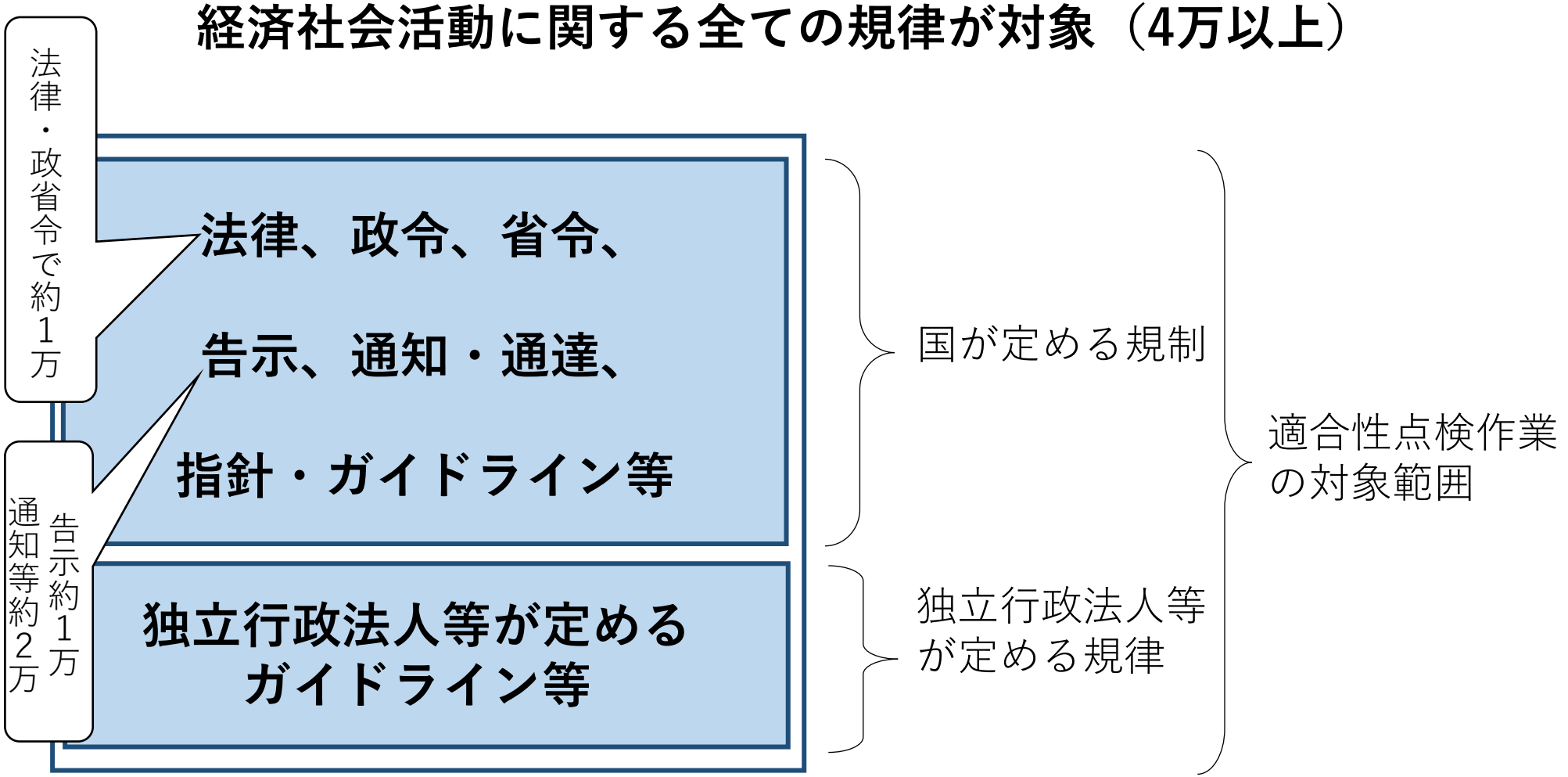
○デジタル原則の下、法律、行政組織、デジタル基盤等の経済社会制度を構成する重要な要素を早急に作り直す（＝「新しい資本主義」を実現するための構造改革）。

構造改革のためのデジタル原則（案）の全体像

○「包括的データ戦略」（令和3年6月）にて提示された７層のアーキテクチャを参考に、**デジタル社会の実現に向けた構造改革のための５つの原則**を整理。

第７層　新たな価値の創出	改革を通じて実現すべき価値 （デジタル社会を形成するための基本原則：①オープン・透明 ②公平・倫理 ③安全・安心 ④継続・安定・強靭(じん) ⑤社会課題の解決 ⑥迅速・柔軟 ⑦包摂・多様性 ⑧浸透 ⑨新たな価値の創造 ⑩飛躍・国際貢献）	
アーキテクチャ	構造改革のためのデジタル原則（案）	
第６層　業務改革・BPR／組織	**原則① デジタル完結・自動化原則**	書面、目視、常駐、実地参加等を義務付ける手続・業務について、デジタル処理での完結、機械での自動化を基本とし、行政内部も含めエンドツーエンドでのデジタル対応を実現すること国・地方公共団体を挙げてデジタルシフトへの組織文化作りと具体的対応を進めること。
第５層　ルール	**原則② アジャイルガバナンス原則** （機動的で柔軟なガバナンス）	一律かつ硬直的な事前規制ではなく、リスクベースで性能等を規定して達成に向けた民間の創意工夫を尊重するとともに、データに基づくEBPMを徹底し、機動的・柔軟で継続的な改善を可能とすること。データを活用して政策の点検と見直しをスピーディに繰り返す、機動的な政策形成を可能とすること。
第４層　利活用環境	**原則③ 官民連携原則** （GtoBtoCモデル）	公共サービスを提供する際に民間企業のUI・UXを活用するなど、ユーザー目線で、ベンチャーなど民間の力を最大化する新たな官民連携を可能とすること。
第３層　連携基盤	**原則④ 相互運用性確保原則**	官民で適切にデータを共有し、世界最高水準のサービスを享受できるよう、国・地方公共団体や準公共といった主体・分野間のばらつきを解消し、システム間の相互運用性を確保すること。
第２層　データ 第１層　インフラ	**原則⑤ 共通基盤利用原則**	ID、ベースレジストリ等は、国・地方公共団体や準公共といった主体・分野ごとの縦割で独自仕様のシステムを構築するのではなく、官民で広くデジタル共通基盤を利用するとともに、調達仕様の標準化・共通化を進めること。

デジタル原則への適合性の点検対象の規律の範囲



※上記を踏まえ、地方公共団体の取組を後押し
（例：国の見直し結果等の情報提供や地方公共団体での先進的な取組事例を紹介等）

既存の規制に関する適合性点検作業の進め方

R3.12月下旬

規制の適合性点検対象リスト洗い出し作業（対象：法令、約5千条項に該当あり）の進め方の照会と各省庁への情報提供

R4.１月

各府省と連携し、通知通達、独法の規律も含めて、点検・見直しの作業方針を確定。
※事務局及び規制改革推進室において、国民･産業界等の要望や追加的な洗い出し作業を実施し各省庁に情報提供

〈作業部会の設置〉
各省庁による自主的な見直し⇒規制見直しプランに反映
見直しに関する課題がある事項⇒作業部会において検討

各省庁と事務局で見直し方針を協力して確認

R4.春

規制見直しプランの取りまとめ（自治体の後押しの方策含め具体化）

法律
⇒一括見直しの累次具体化

政令省令通知・通達、運営要領等
⇒スピード感をもって改正

技術的検証やシステム整備等の検討

集中改革期間（3年程度）で原則への適合を実現

デジタル原則を踏まえ制度・規制を見直す考え方

約４万以上の法令・通知通達等を点検
（法律・政令・省令で約5千条項に該当あり）

約2万2千手続を対象に推進

既存の規制

- 現場で人の目に頼る規制
- 定期的に点検・確認を求める規制
- 人が常にいること等を求める規制
- 公的な証明書・講習・閲覧に対面・書面を求める規制
- 一律の規制、データ連携が困難なルール
- オンラインで申請できない又は利用しにくい行政手続

技術の進歩

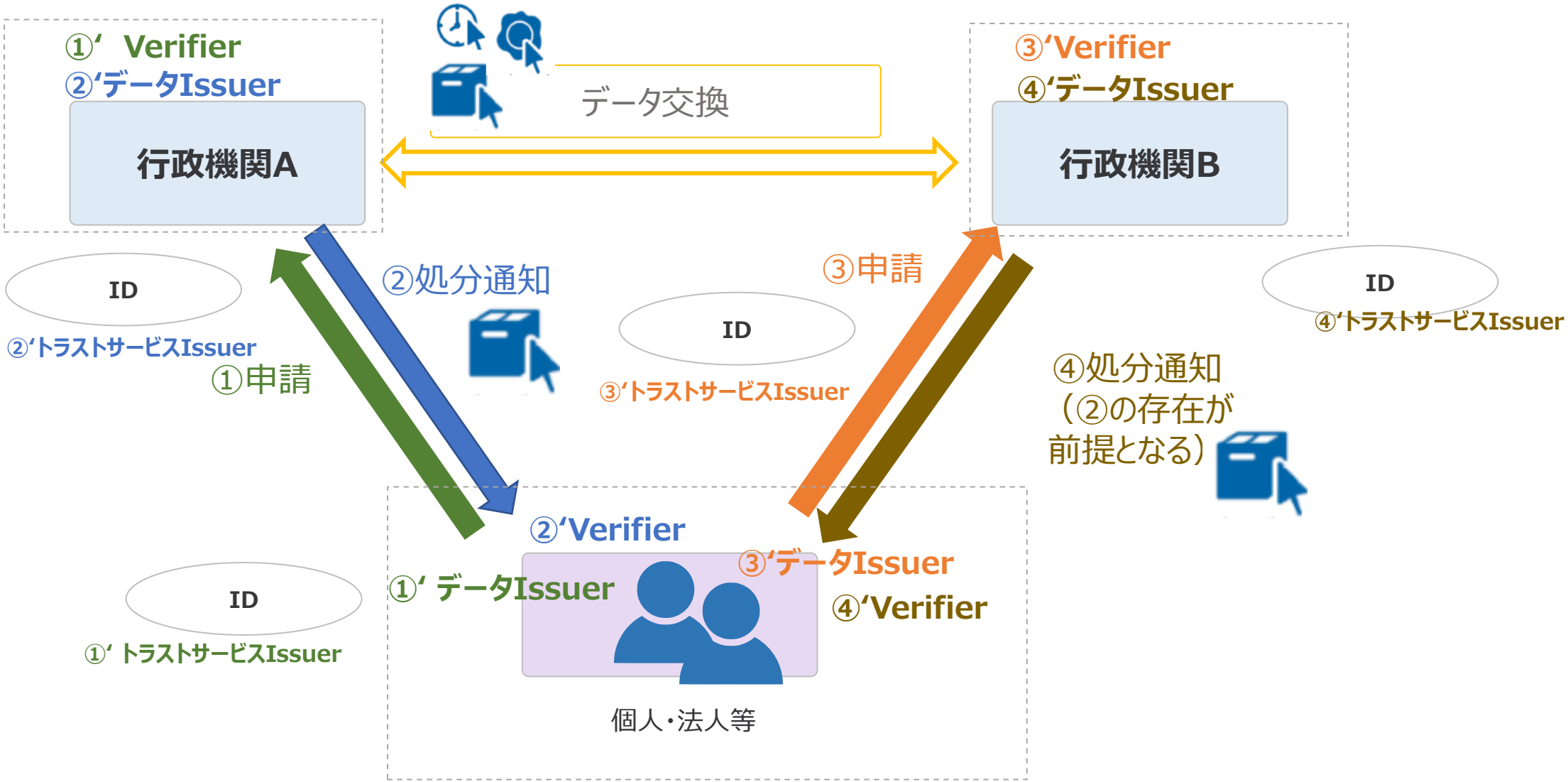
- カメラ等を含む高精度で安価・大量のセンサー
- ドローンや空飛ぶクルマといった次世代空モビリティ
- ＩＣ・メモリーの進歩
- クラウドサービス利用等によるビッグデータの高速処理
- あらゆるモノがネットワークとつながるＩｏＴの進展
- ＡＩの高度化
- 超高速通信（５Ｇ、Beyond 5G）の実現

先行している規制見直し

- 施設維持・保守でセンサー等を活用、監査を遠隔地から実施
- カメラ・センサー・AI等により点検・確認等を実施
- オンラインを通じて離れた場所からでも仕事が可能
- オンラインなどを活用し、紙、対面、訪問を見直し
- データを活用したゴールベース・リスクベース、API連携
- オンライン利用率を成果指標にし、継続的なサービス改善実施

例）行政分野でデジタル完結を可能とするためのトラスト基盤イメージ

- 手続・取引に応じた本人・組織の真正性及びアクセス管理のユースケース及び必要となるトラストサービスが存在する。



Thank you

デジタル庁デジタル社会共通機能グループ

角田 梨翔 <RikTsunod@digital.go.jp>