資料１

令和４年２月25日
トラストを確保したDX推進SWG（第６回）

事務局説明資料

デジタル庁

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）

アウトライン

1. 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
2. Identificationアシュアランスレベルの検討
3. トラストサービスアシュアランスレベルの検討

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・強靱(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。

構造改革のためのデジタル原則の点検の方向性

デジタル技術の更なる進展も見据えた点検の方向性

①デジタル完結・自動化原則	①－１　紙の介在（書面、原本等）を見直し、申請・通知のデジタル化を基本とするとともに、行政内部のデジタル化を徹底すること ①－２　人の介在（対面、常駐、資格者配置、拠点設置、目視、立入等）を見直し、点検等の遠隔実施、自動化・機械化等の最大限のデジタル化を基本とすること ①－３　ルールをデジタルデータ化し、可能なものはアルゴリズム化することにより、機械判読可能な形で提供すること
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）	②－１　一律の様式、手法や基準（定期点検・検査等）を撤廃し、求める性能のみ規定することで、リアルタイムモニタリング等の技術活用によるコンプライアンス確保を基本とすること ②－２　資格要件としての学歴、経験や体制整備等に関する一律基準を撤廃して精緻化し、技術力やデジタルリテラシーによる代替を認めること ②－３　AI時代の安全管理手法を見直し、モニタリング・制御ソフトウェア導入、ログ保存、事故原因究明協力等の制度を整備すること ②－４　AI時代の事故責任分担について法制度・保険制度・公的救済等を含めた一体的な仕組みを整備すること
③官民連携原則 （GtoBtoCモデル）	③－１　行政サービス提供に際しベンチャーなどの民間企業のUI/UXやサービス活用を基本とすること（GtoBtoC） ③－２　公共・準公共サービスのデータ基盤はAPIを公開することを基本とすること ③－３　マルチステークホルダーによるガバナンス（第三者認証、監査、共同規制、自主規制等）の導入を拡大すること
④相互運用性確保原則	④－１　書式・様式を撤廃してデータモデル化し、システム間のデータ再利用を基本とすること ④－２　API公開・接続義務等によりシステムを疎結合化・簡素化し、ロックインを回避すること ④－３　域外適用、非対称規律解消、課徴金・制裁金の実効性確保等により、国家としての主権の確保にも留意しつつ国内外のイコールフッティングを確保すること ④－４　国際規格への準拠、国、地方公共団体、準公共間におけるルールの整合性を確保すること
⑤共通基盤利用原則	⑤－１　IDを含むベースレジストリを特定し、その参照・利用を徹底すること ⑤－２　目的外利用規制を整理することで、システム間のデータ再利用を可能とすること ⑤－３　標準データ様式や調達仕様等は共通モジュールを再利用すること ⑤－４　法令用語・タクソノミー（分類）の統一を図ること

デジタル臨時行政調査会で扱う論点

本日提起する論点

デジタル臨時行政調査会が扱う論点

〇構造改革のためのデジタル原則の策定 ⇦ 原則の提示

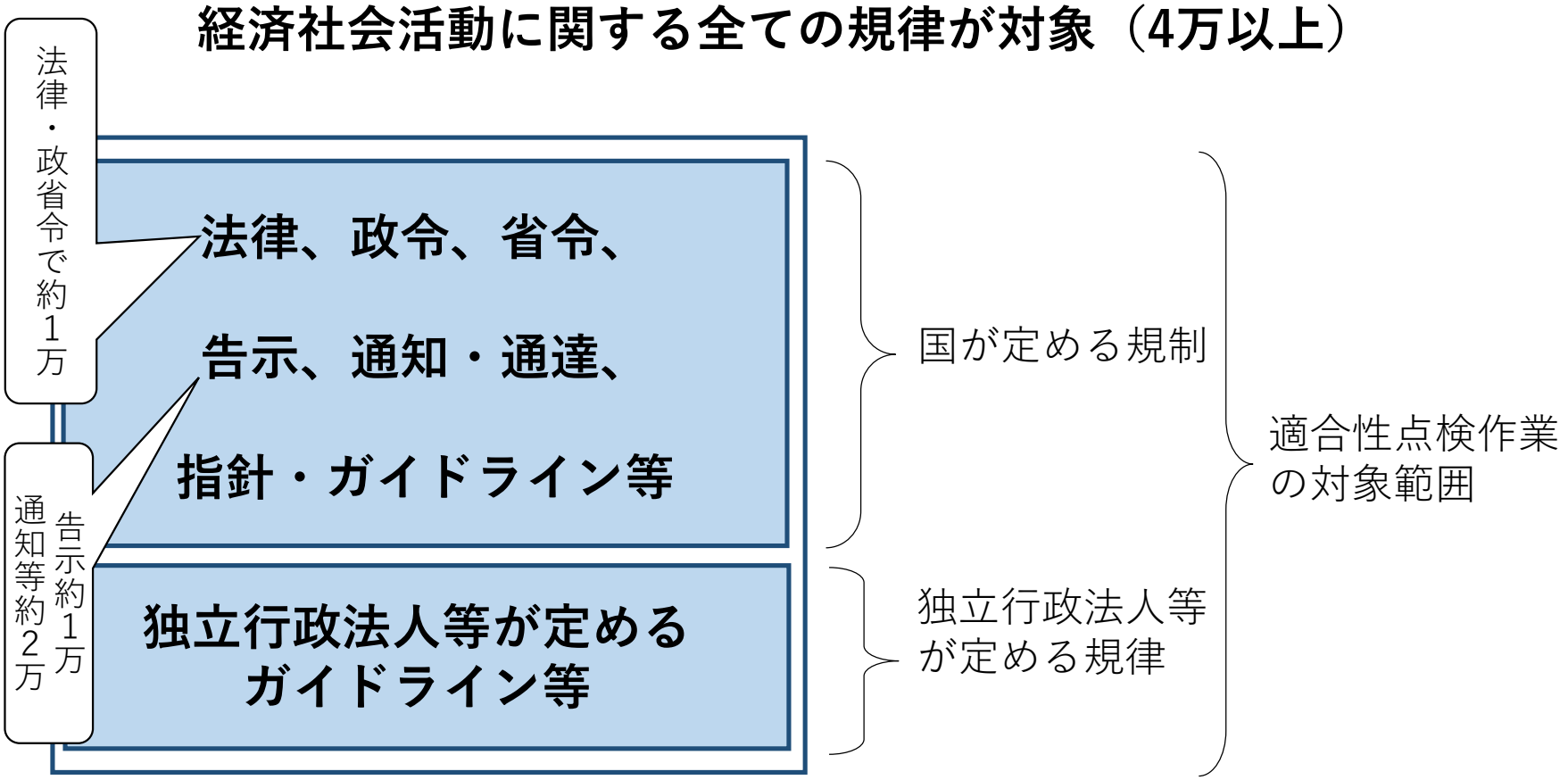
〇デジタル時代にふさわしい規制・制度の見直し ⇦ 規制と手続の見直し
- 原則への適合性の総点検
- デジタル関連一括見直しのプラン策定と具体化
- 原則への適合性を事前に確認する機能やプロセスの検討

〇デジタル基盤を活用し十分なサービスを効率的に行える政府 ⇦ 準公共分野に係る検討
- 準公共サービス改革（規制制度改革）：教育・デジタル人材/健康医療/防災/こども　など
- マイナンバー・カードの徹底普及や活用含めた国民と政府の結びつき、国と自治体、準公共など含めた共通基盤整備に関する制度課題の検討

〇政策形成・評価のデジタル化（EBPM） ⇦ EBPMに係る論点
- 人材、資金、政策形成・評価を含めて検討

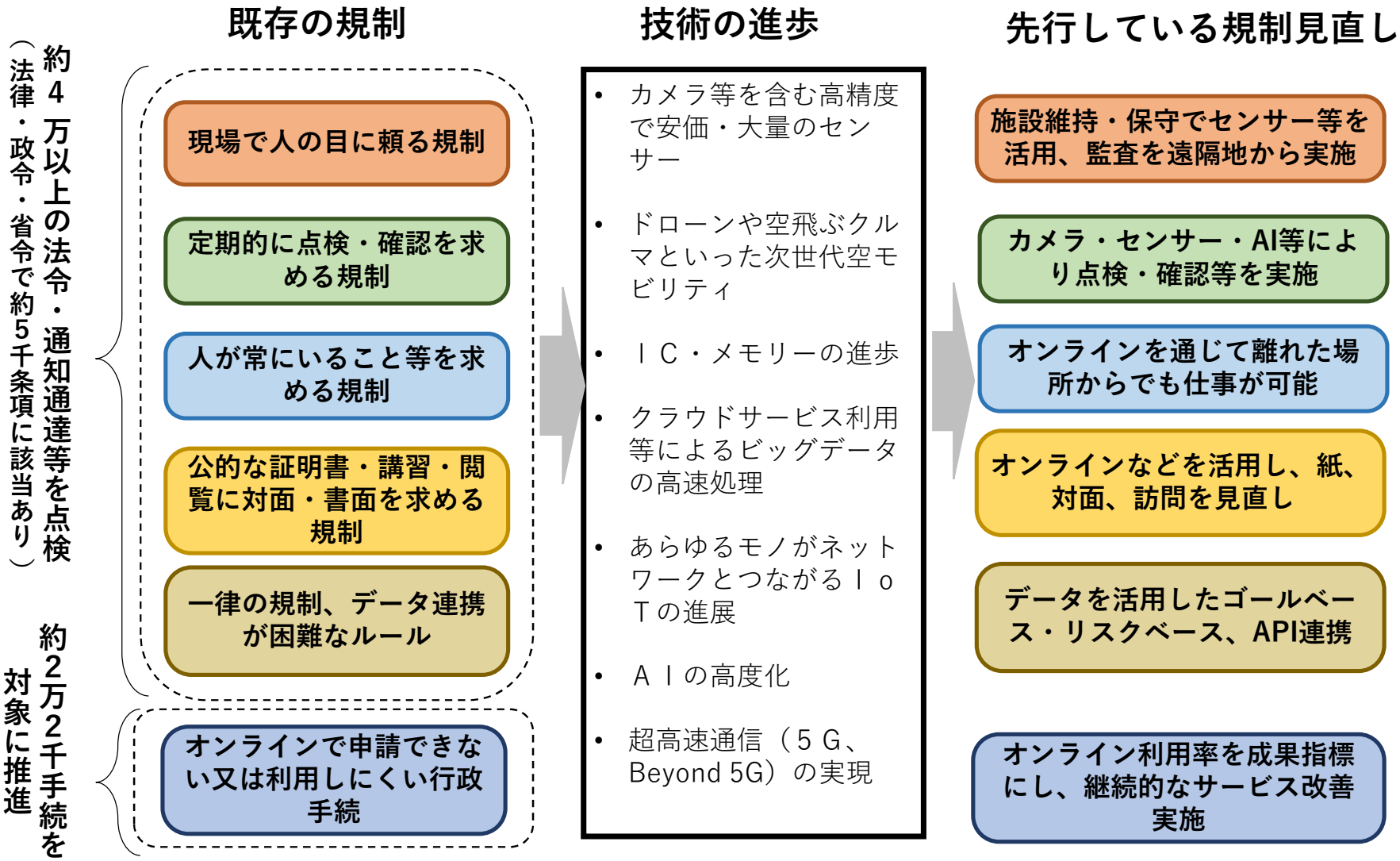
〇官民ともに不足するデジタル人材の需給構造の抜本改革

構造改革のための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）

構造改革のためのデジタル原則を踏まえ制度・規制を見直す考え方
～先行取組の横展開～



原則への適合性の点検対象①

既存の規制（※以下は法律・政令・省令を対象に洗い出した件数・例）

現場で人の目に頼る規制

〈**目視規制**〉
現場での点検や調査の際に、人が赴き、目で見て確認を求めている規制　1,843件

〈**実地監査規制**〉
人が現場に赴き、書類や建物を人の目で確認をすることを求めている規制　195件

デジタル技術の活用

先行して取組んでいる規制見直し

- トンネル、橋などの道路を構成する施設等の維持修繕のための目視点検について、ドローン、レーダー、センサー等を活用した新技術による代替を可能とするよう取組を推進。
（橋梁約72万橋、トンネル約1万本（平成31年3月））
- 太陽光発電所の月次の点検における目視点検について、監視カメラやセンサーによるデータ取得システムなどの遠隔監視技術による代替を可能とした。（電気事業者の太陽光発電所数約3,272発電所（令和3年7月））

今後の展開（法令で2,038件を点検）

施設維持・保守でセンサー等を活用/遠隔地から監査を実施

例）
- 堤防などの維持修繕のための点検
- 貯水施設、配水施設などの維持修繕のための点検
- ごみ処理施設などの維持管理のための検査
- 港湾施設の管理に係わる監査

原則への適合性の点検対象②

既存の規制

定期的に点検・確認を求める規制

〈定期検査・点検〉
定期的に人に特定の場所への点検を求めたり、特定の対象物の確認を求めたりする規制

デジタル技術の活用

先行して取組んでいる規制見直し

- IoT等の新技術の活用及び高度なリスクアセスメントの実施などの高度な保安の取組を行うプラント事業者について、完成検査・保安検査にかかる規制を合理化し、連続運転期間の自由設定（原則４年→最大８年）等を可能にした。
- 大型浄化槽について、遠隔監視技術の活用により、保守頻度を２週間に１回から月１回に緩和した。
（処理対象人員51人以上の浄化槽（新構造基準）数：13万9,666基（令和元年度末））

今後の展開（法令で1,068件を点検）

カメラ・センサー・AI等により点検・確認等を実施

例）
- バス、トラックなどの事業用自動車の定期点検
- 消火器、火災報知機などの定期点検
- ホテル、百貨店、病院などの定期調査・検査

原則への適合性の点検対象③

既存の規制

人が常にいること等を求める規制

〈常駐専任規制〉
人を特定の場所へ常時配置または別の場所での仕事の兼務を禁止している規制

デジタル技術の活用

先行して取組んでいる規制見直し

・宅地建物取引業者の事業所への宅地建物取引士の常駐規制を緩和
（宅地建物取引事業数：127,215事業者（令和３年３月末））
・事業所における産業医の常駐規制を緩和
（認定産業医数：99,799人（平成30年11月））
・マンション管理者の事業所への管理業務主任者の常駐規制を緩和
（マンション管理事業者数：674事業者（平成31年４月））

今後の展開（法令で218件を点検）

オンラインを通じて離れた場所からでも仕事が可能

例）

- 浄化槽の保守点検における管理者の専任
- 倉庫の管理に係わる専任
- 特定の住居施設における管理者の専任

原則への適合性の点検対象④

既存の規制

公的な証明書・講習・閲覧に対面・書面を求める規制

〈資格等の対面講習規制〉
国家資格等の講習をオンラインではなく対面で行うことを求めている規制　172件

〈資格等の証明書の掲示規制〉
国家資格等、公的な証明書等を対面確認や紙発行で、特定の場所に掲示することを求めている規制　635件

〈公的情報の閲覧縦覧規制〉
公的な情報を得るのにオンラインではなく役所等へ訪問して閲覧・縦覧を課している規制　1,065件

デジタル技術の活用

先行して取組んでいる規制見直し

・株式会社設立時の公証人による定款認証のオンライン化　（株式会社設立数：85,688社（令和２年））
・介護支援専門員更新研修のオンライン化　（資格所有者数：698,612人（令和２年９月末））
・建築士定期講習のオンライン化（一級～三級建築士）（資格所有者数：1,162,869人（令和２年４月））

今後の展開（法令で1,872件を点検）

オンラインなどを活用し、紙、対面、訪問を見直し

例）
・公証人による公正証書の作成
・小型船の安全に係る講習
・自動車整備に係る研修
・食品衛生に係る講習
・飲食店における許可証の掲示
・薬局に係る許可証の掲示
・不動産価格に係る縦覧
・建築に係る概要書の閲覧

原則への適合性の点検対象⑤

一律の規制、データ連携が困難な基盤・ルール

1．データを活用したゴールベース・リスクベース規制への転換

（例）
- 一定の施設が必要な事業の許可において、設備の異常や周辺環境への影響などをIoT、AI等でリアルタイムデータで計測する場合には、許可基準を合理化可能か検討
- モノの移動に係る場所のリスクに応じて、規律を合理化可能か検討

2．官民のデータ利活用の基盤・ルールの整備

（例）
- 新規企業の参入等を促進することを企図して、関係する事業者におけるAPI公開・接続義務の実効性を高める方策を検討
- 地下埋設物（水道管、ガス管、電線、上下水道管等）の工事の際に、図面が異なる主体毎に紙ベースで管理されているために関係各所に連絡する必要があることなどから、一定の行政主体が地下空間情報の電子データを整備・管理・提供することを検討
- 法令や通達の情報をデジタルデータ化する動きを官民連携で加速することを検討

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

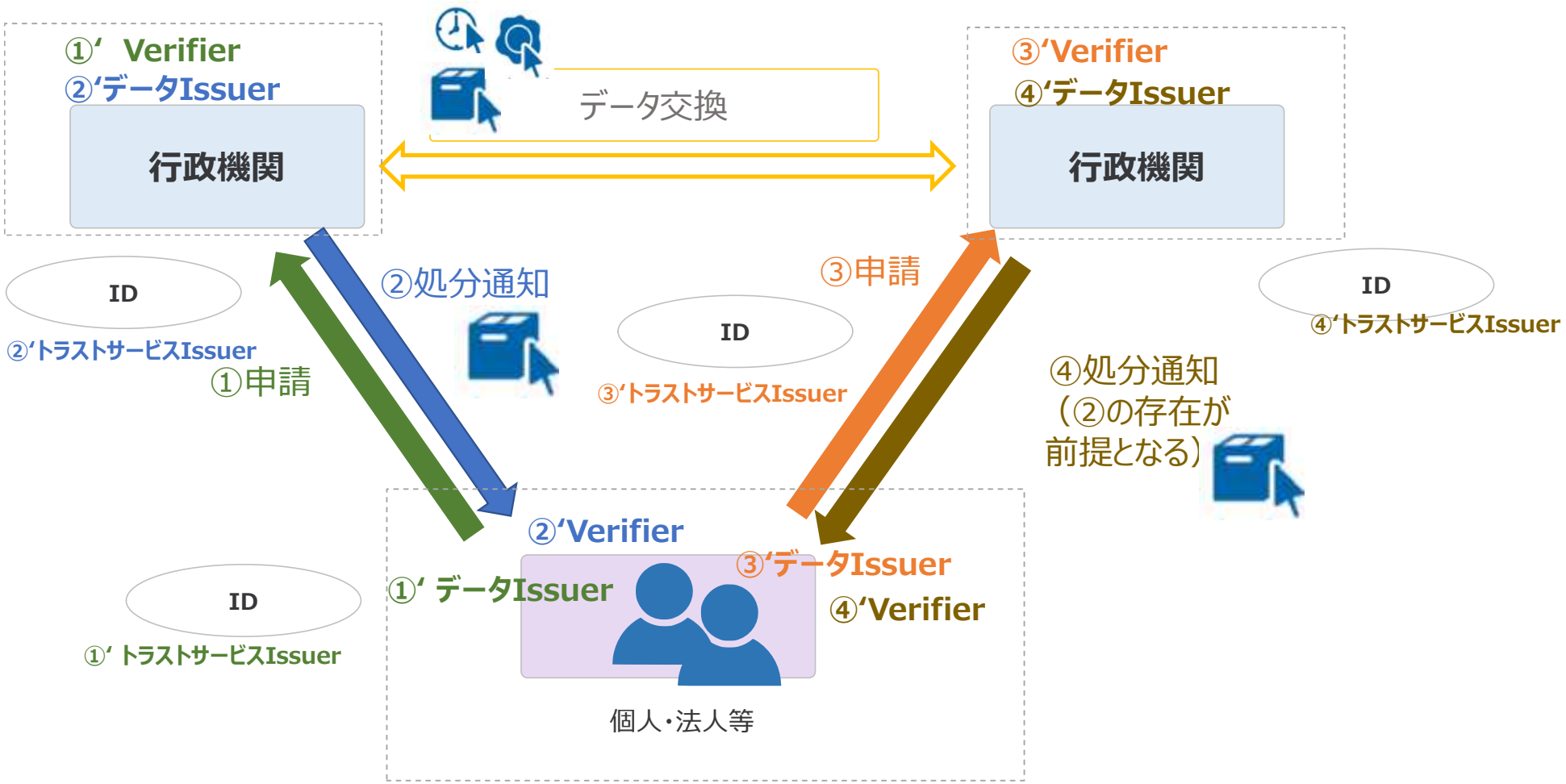
議論いただきたいこと

1. 「デジタル完結・自動化原則」に資するトラストサービスはどのようなものか？

2. 手続・取引での紙、対面、一部分のみのオンラインではなく、「デジタル完結」を実現するための要素として求められるトラストサービスの要件はどのようなものがあるか？

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。



Identificationアシュアランスレベル検討

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

ご議論いただきたいこと

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

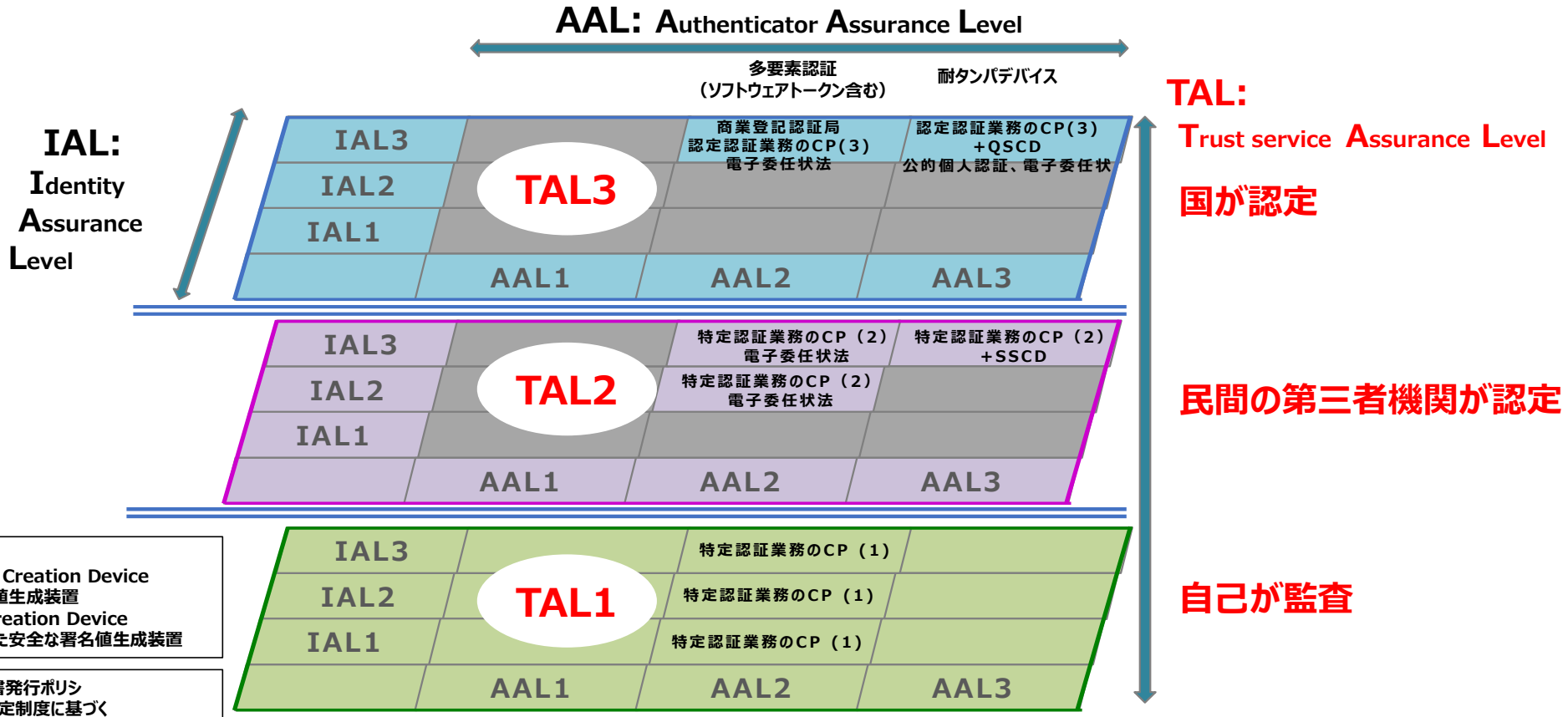
ご議論いただきたいこと

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検討

（参考）論点1：アシュアランスレベルの基準

- アシュアランスレベルの基準はIAL、AAL、TALの組み合わせから構成される。（下図は認証局を例にしたイメージ）
- IDプロバイダー、クラウド署名サービス、認証局、タイムスタンプ局等に対してユースケースに応じた基準を作成すべき。



耐タンパデバイス
QSCD：Qualified Signature Creation Device
国により認定された署名値生成装置
SSCD：Secure Signature Creation Device
国際規格により認定された安全な署名値生成装置

CP: Certificate Policy 証明書発行ポリシ
認定認証業務のCP (3)：国の認定制度に基づく
特定認証業務のCP (2)：信頼できる民間の監査制度に基づく
特定認証業務のCP (1)：上記以外の認証業務

（参考）論点1：アシュアランスレベルの基準

- トラストサービスのアシュアランスレベルに関して、どのような基準が考えられるか

● トラストサービス事業者（IDプロバイダー、クラウド署名サービス※、認証局、タイムスタンプ局等）の運営ポリシーをトラストサービスアシュアランスレベル（TAL：Trust service Assurance Level）として整理すべきである。
  - 組織要件（組織の責任）
  - 設備要件（ファシリテイ要件）
  - 技術要件（暗号技術等）
  - 鍵管理要件（適格署名生成装置等）
  - 運用要件（複数人による相互牽制）
  - 監査要件（内部監査、外部監査、適合性監査、認定）
  - その他

● これらをトラストサービスに共通する基準、個別の基準として整理し、TAL1、TAL2、TAL3のアシュアランスレベルを定義する。それぞれの認定主体としては以下を想定する。

  TAL3：国が認定
  TAL2：民間の第三者機関が認定
  TAL1：自己が監査

※　当事者の署名鍵によるリモート署名サービスおよび利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービス（令和2年7月17日　主務三省Q&Aより）

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

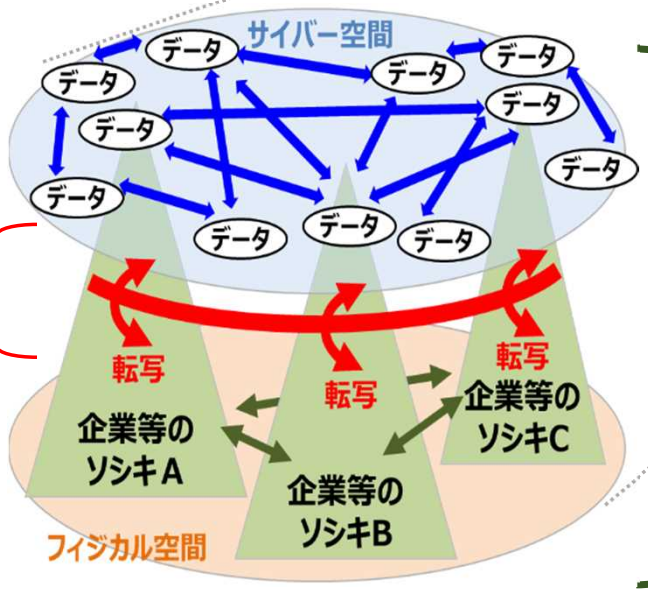
トラストサービスアシュアランスレベルでは、データの信頼性のみならず、フィジカル空間とサイバー空間のつながりにおけるトラストや、時間経過後のトラストも考慮するべきだと指摘された。

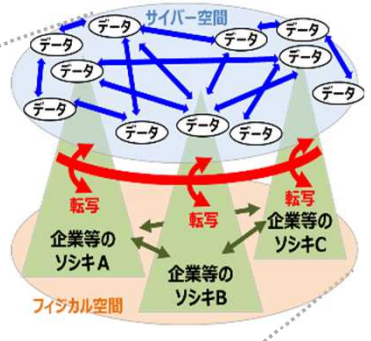
「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

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

（参考）
Identificationのアシュアランスレベルにおける先行事例

海外におけるIdentificationアシュアランスレベルの状況

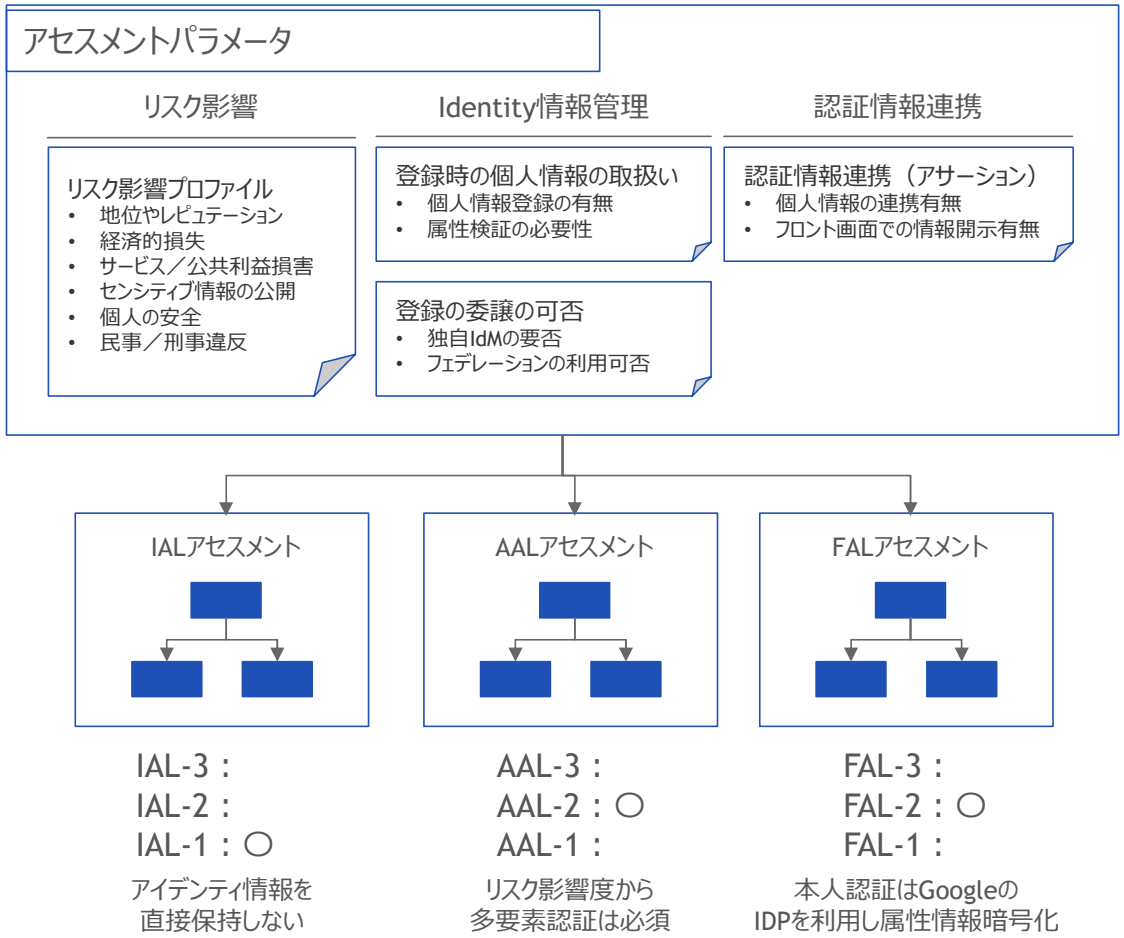
定義カテゴリ	定義内容	各国の整備有無状況（内容の差異は存在）		
		eIDAS	NIST SP800-63	NZの Identification 管理基準
本人確認（IAL※1）	本人確認方法の確からしさをレベル分けする	✓	✓	✓
認証プロセス（AAL※1）	認証プロセスによって認証強度をレベル分けする	✓	✓	✓
トラストサービス事業者の運営条件	トラストサービスの提供元が信頼できる機関であるかどうかを定めた要件を満たすかどうかによってレベル分けする	✓	–	–
認証情報連携（FAL※1）	認証した情報を別機関に連携する際の連携方法の確からしさをレベル分けする	–	✓	✓
割当（Binding※2）	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)

SP800-63-3：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

FIPS 140-2に規定される要求レベル

4. SECURITY REQUIREMENTS

This section specifies the security requirements that shall be satisfied by cryptographic modules conforming to this standard. The security requirements cover areas related to the design and implementation of a cryptographic module. These areas include cryptographic module specification; module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; and design assurance. An additional area concerned with the mitigation of other attacks is currently not tested but the vendor is required to document implemented controls (e.g., differential power analysis, and TEMPEST). Table 1 summarizes the security requirements in each of these areas.

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

（参考）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