

# 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. Identificationアシュアランスレベルにおける先行事例
2. Identificationアシュアランスレベルの検討の進め方
3. 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
4. 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
5. （情報提供）茨城県庁からのデジタル庁への要望書

# 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	—	—	✓

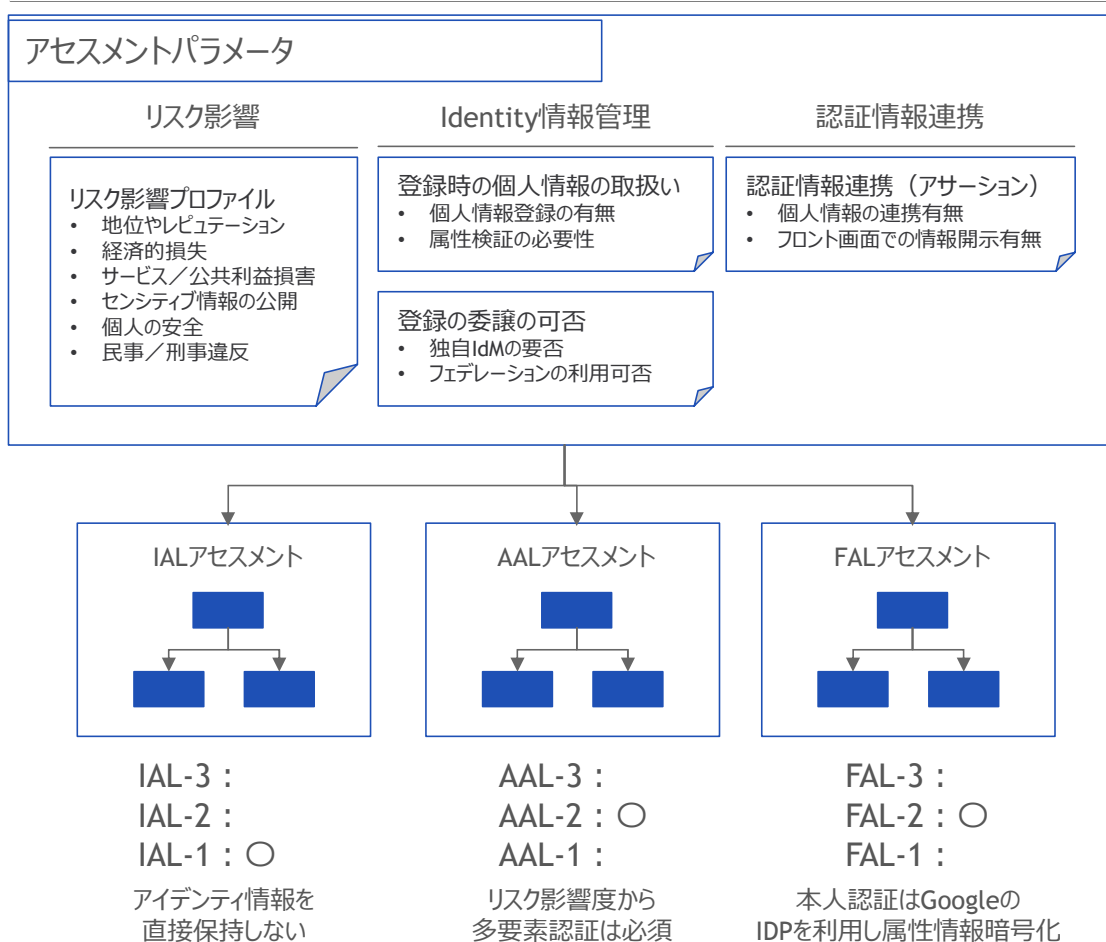
※1 SP800-63-3 におけるアシュアランスレベルの定義名を記載

※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ムのIDP機能へ委譲 (フェデレーション) する

# 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へ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る。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)

# SP800-63-3 : AALに関する要求詳細

SP800-63-3における Requirement Type※	認証要素に関する要求	Hardware-based authenticator	verifier impersonation resistance
AAL.1	either single-factor or multi-factor authentication using a wide range of available authentication technologies	<ul style="list-style-type: none"> <li>Level 1: Government agency verifiers</li> </ul>	要求しない
AAL.2	Proof of possession and control of <b>two distinct authentication factors</b> is required through secure authentication protocol(s). Approved cryptographic techniques are required	<ul style="list-style-type: none"> <li>Level 1: Government agency authenticators and verifiers</li> </ul>	要求しない
AAL.3	(AAL2の要求に加えて) shall use <b>hardware-based authenticator</b> and an authenticator that provides <b>verifier impersonation resistance</b> ; the same device may fulfill both these requirements.	<ul style="list-style-type: none"> <li>Level 2 overall: MF Authenticators</li> <li>Level 1 overall: verifiers and SF Crypto Devices</li> <li>Level 3 physical security: all authenticators</li> </ul>	要求する

※Permitted authenticator types、Reauthenticationなど他の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



# (ご参考) 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.

	<i>Security Level 1</i>	<i>Security Level 2</i>	<i>Security Level 3</i>	<i>Security Level 4</i>
<b>Cryptographic Module Specification</b>	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.			
<b>Cryptographic Module Ports and Interfaces</b>	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.	
<b>Roles, Services, and Authentication</b>	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
<b>Finite State Model</b>	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
<b>Physical Security</b>	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
<b>Operational Environment</b>	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.
<b>Cryptographic Key Management</b>	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 shall be entered or output encrypted or with split knowledge procedures.	
	Secret and private keys established using manual methods may be entered or output in plaintext form.			
<b>EMI/EMC</b>	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).	
<b>Self-Tests</b>	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
<b>Design Assurance</b>	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.
<b>Mitigation of Other Attacks</b>	Specification of mitigation of attacks for which no testable requirements are currently available.			

# Identification アシュアランスレベルにおける検討の進め方

# Identification アシュアランスレベルへの前回の主なご意見

## 身元確認や認証プロセスの基本的考え方

既存の国際標準等を参照した上で、日本の実情に応じたIdentificationの基準の設定が提案された

- 基本的考え方はISOや「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」を参照すれば十分
- 住民基本台帳、印鑑登録制度、商業・法人登記制度に基づくベースレジストリが整備され、マイナンバーカードの公的個人認証証明書や商業登記電子証明書がある日本の実情に応じて、これらを活用した身元確認や当人確認の実現検討すべき
- 認証連携やバイディングも当然基準に入れるべき

## 考慮すべきユースケース

行政からのユースケースの具体化、マイナンバーカードを様々なサービスの認証に一層活用をすることが提案された

- 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の程度及び証明書の発行形態は、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
- デジタル庁の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例
- デジタル庁でのスモールスタートをして、行政の領域からユースケースとして具体化していくべき
- オンライン登記事項証明書へのeシールの付与により、登記事項証明書取得者からの第三者へ提出可能となり、マイナンバーカードと組み合わせて利用することによりオンラインでの法人代表者の証明や電子委任状の作成が容易となる
- マイナポータル「自己情報取得API」との連携においては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。Identificationユースケースの検討においては、行政データとの連携が可能な仕組みや要件整備も期待

# (参考)各IALにおけるユースケースのマッピング案

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
	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 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。



# (参考) 認証プロセスとユースケースのマッピング初期案

ご議論いただきたいこと

	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	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
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

- 1 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。



# Identification アシュアランスレベルについて議論いただきたいこと

- 1 身元確認や認証プロセスの基本的考え方は、「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」を参照することで対応可能か？
- 2 マイナンバーカードの電子署名用電子証明書などの多岐にわたるユースケースや課題が出ている中で、Identification アシュアランスレベルに関する本SWGでのゴールをどうするべきか？ Identification アシュアランスレベルを整理するだけでなく、ユーザビリティの高いIdentificationを普及させるため、多岐にわたる議論が必要か？

# 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

# 主な意見①（トラストサービスアシュアランスレベルの基準）

既存電子署名法令の技術基準をベースに、国際的基準や官民の制度との整合性を取りながらトラストサービスの保証レベルを整理すべき。整理にあたっては、トラストサービスに共通となる要件と個々の要件を分けて考えるべき、という意見が出た

- トラストサービスのアシュアランスレベルを考えることは、IDプロバイダーのトラストを確保する上でも重要
- 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保証レベル（TAL：Trust service Assurance Level）として整理すべき
- 電子署名法6条1項の認定における設備基準をベースに、国際的基準（ISO/IEC 27000シリーズ、CA/Browser Forum baseline requirements、ETSI、CEN規格、Web trust監査基準等）との整合性を考慮し、国際相互運用性を見据えた基準作りをするべき
- ユースケースで必要となるトラストのレベルに対応する基準や官民の制度との整合性を取るべき
- トラストサービス固有の脆弱性に対する「脅威耐性」ベースでの検討を行うべき
- 各基準は国の関与の下、クオリファイドレベルとアドバンスドレベルに応じて作成すること
- トラストサービスの種別によらず共通的な要件と個々のトラストサービスの要件を分けて洗い出す必要がある



# 主な意見②（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」が挙げられているが、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
- 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。

（例）eIDAS規則では、以下の2つの文脈で相互承認が使われている。

①加盟各国の電子識別手段（第2章第6条で規定する相互承認）：

EU域内での電子識別手段について加盟各国から通知されたものを域内において認め合う。

②トラストサービス（第3章第14条で規定する国際的観点）（認証局が対象）

EU域外の第三国との国際相互承認に関する協定に基づき、相手国のトラストサービスを自国の制度の下で認める

# 主な意見③（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げられた。

## 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

# トラストサービスアシュアランスレベルについて議論いただきたいこと

- 1 トラストサービスアシュアランスレベルにおける、トラストサービスの定義（どのようなサービスを指しているか）
- 2 トラストサービスのアシュアランスレベルで担保したいものは何か？
- 3 Identificationの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との関係性はどう考えるか？

# 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 <sup>じん</sup> 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	<b>原則① デジタル完結・自動化原則</b> 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	<b>原則② アジャイルガバナンス原則</b> (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	<b>原則③ 官民連携原則</b> (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	<b>原則④ 相互運用性確保原則</b> 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楽しむことができるよう、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	<b>原則⑤ 共通基盤利用原則</b> 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・分野ごとの縦割り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。
第1層 インフラ	

# 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

<p><b>①デジタル完結・自動化原則</b></p>	<p>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</p> <p>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</p> <p>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</p>
<p><b>②アジャイルガバナンス原則</b> (機動的で柔軟なガバナンス)</p>	<p>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</p> <p>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</p> <p>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</p> <p>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</p>
<p><b>③官民連携原則</b> (GtoBtoCモデル)</p>	<p>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)</p> <p>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</p> <p>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</p>
<p><b>④相互運用性確保原則</b></p>	<p>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</p> <p>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</p> <p>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トイングを確保すること</p> <p>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</p>
<p><b>⑤共通基盤利用原則</b></p>	<p>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</p> <p>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</p> <p>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</p> <p>⑤-4 法令用語・タクソノミー（分類）の統一を図ること</p>



# 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

○構造改革のためのデジタル原則の策定

◁ 原則の提示

○デジタル時代にふさわしい規制・制度の見直し

- 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

◁ 規制と手続の見直し

○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

◁ 準公共分野に係る検討

○政策形成・評価のデジタル化（EBPM）

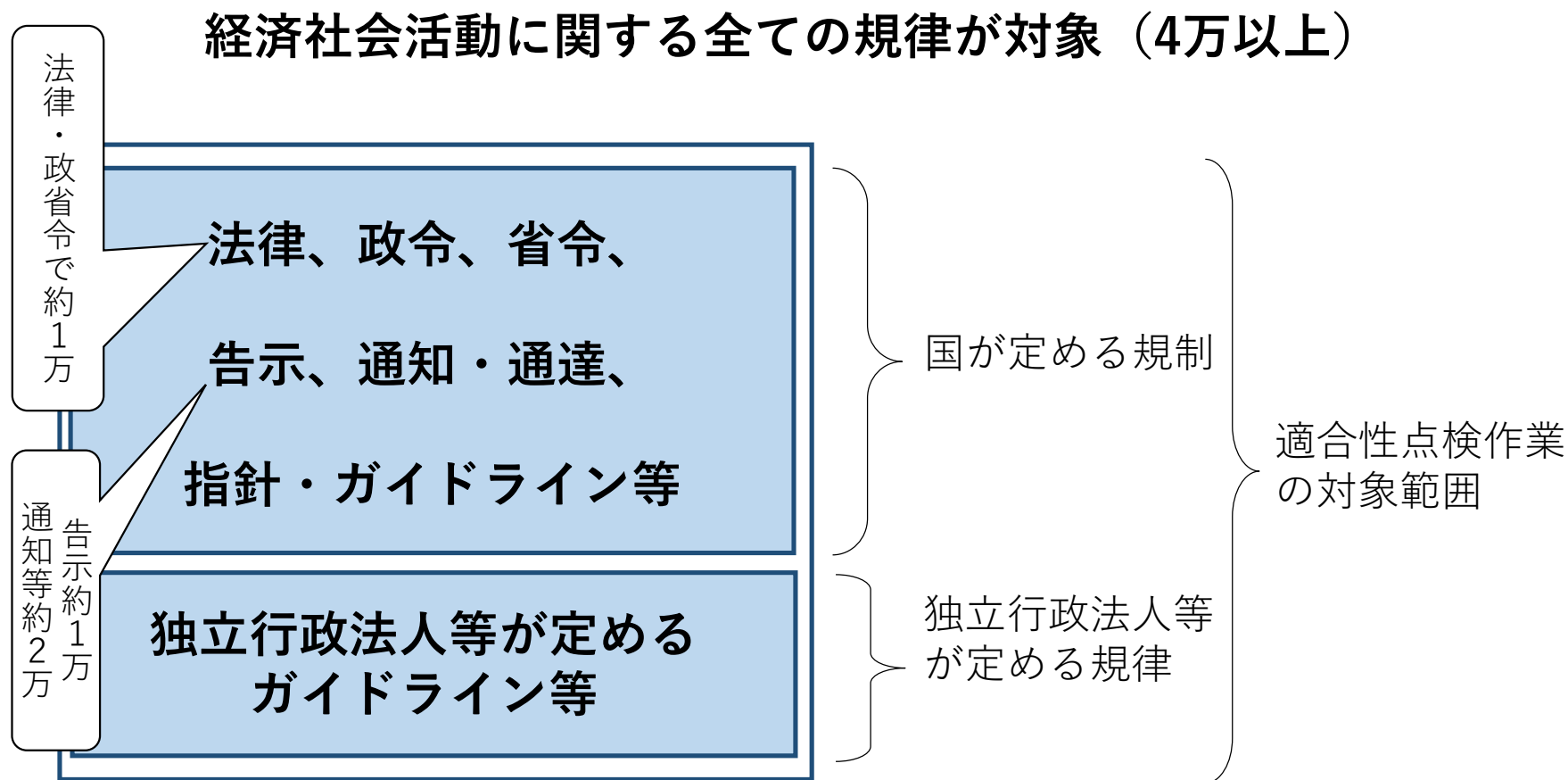
- 人材、資金、政策形成・評価を含めて検討

◁ EBPMに係る論点

○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

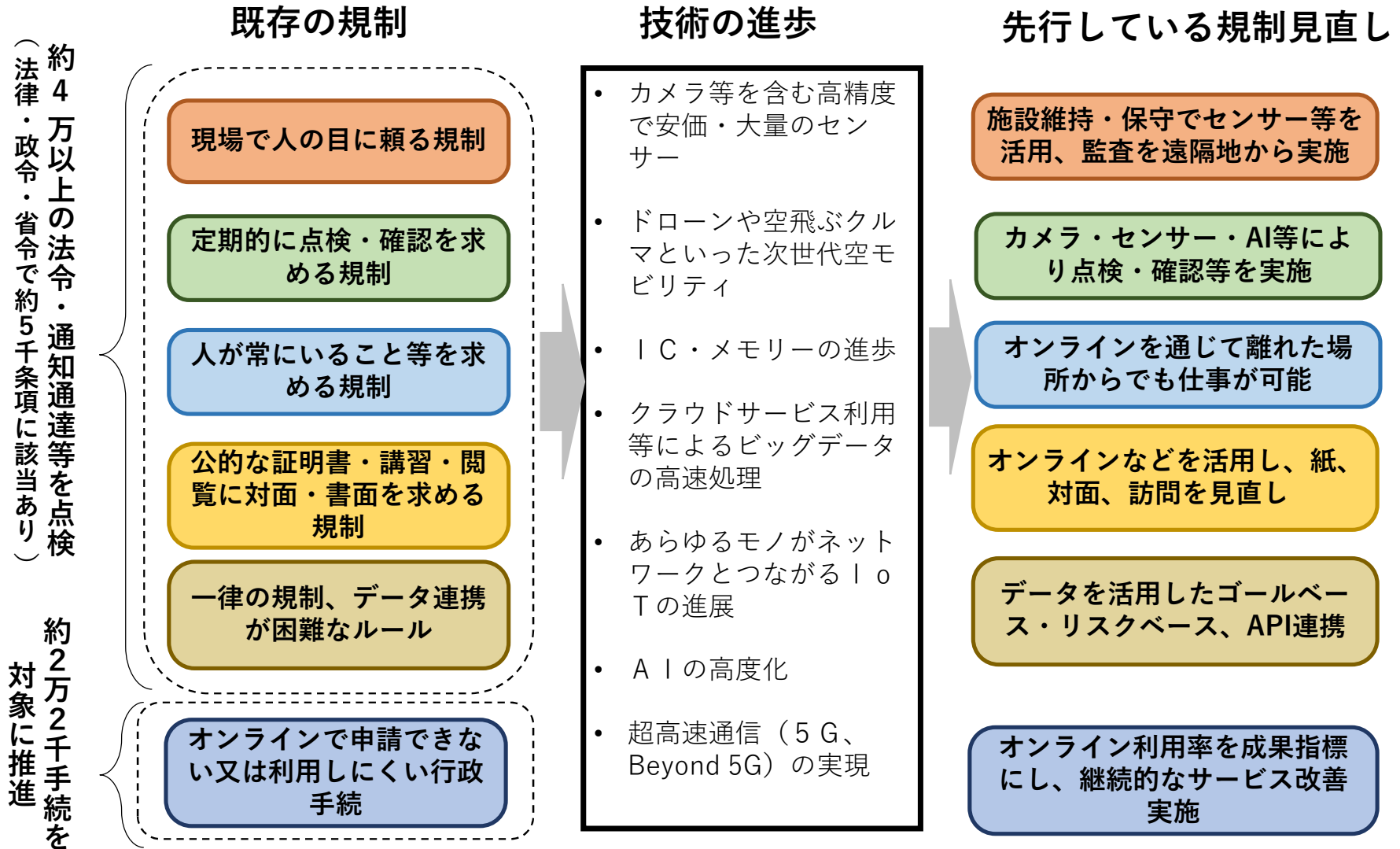


# 構造改革のためのデジタル原則への適合性の点検対象の規律の範囲



※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



情報提供：  
茨城県庁からのデジタル庁への要望書

# 「職責による電子署名」の導入に関する要望

## 課題1: 電子証明書の定義

○ 電子署名と併せて送付する「電子証明書」は、原則として自然人に対して発行することが前提とされており、法令上、「職責による署名」が利用可能か不明確で、各省の省令の「電子証明書」の定義も統一されていない。

電子証明書の定義 (例)	省名等
マイナンバー, 認定認証事業者が発行する証明書, 商業登記法の証明書 ※1	総務省
上記規定に加えて, <u>総務省以外の省庁では、右に記載のとおり「行政機関等」が作成・指定等をした電子証明書に関する追加規定あり</u> ※2	農林水産省、環境省 (行政機関等が作成する電子証明書) 国土交通省, 経済産業省 (大臣が告示で定める電子証明書) デジタル庁 (その他行政機関等が指定する電子証明書)



※1 総務省は、商業登記を除くと自然人のみが対象とされており、「職責を含む電子署名」は利用不可

※2 「行政機関等」には、地方自治体も含まれると規定 (情報通信技術を活用した行政の推進等に関する法律第3条(定義)) されており、茨城県では、農林水産省や環境省の省令であれば、国が解釈を明確化することにより、導入した「職責による電子署名」が直ぐに利用可能と解釈できるものと認識

## 課題2: 各省の省令の条文が不統一

○ 各省の省令ごとに、処分通知の方法や電磁的記録による手続き方法等に関する条文があり、要件や文言が統一されていないため、法令に基づき事務を行う地方自治体にとって、デジタル化の阻害要因となっている。

※条文の詳細は6ページのとおり



# 「職責による電子署名」の導入に関する要望

## 要望

1. 各省の省令の規制緩和を図るとともに、 地方自治体では、各省の省令を参照して事務を行わなければならないため、「電子証明書」の定義や「処分通知の方法」等の条文を全て統一又は統合されたい。

### 【例】

- ・ 電子証明書の定義  
農林水産省や環境省の省令の定義に各省の省令を統一 → 「行政機関等が作成する電子証明書」に統一
- ・ 処分通知の方法の規定  
デジタル庁の省令の文言に各省の省令を統一 → 「行政機関等の使用に係る電子計算機から入力して行う」に統一

2. 茨城県が導入した「職責による証明書」が国の法令で定められた事務においても利用可能となるよう、 省令の解釈の明確化、又は各省令の「電子証明書」の定義に次の条文【例】を追加されたい。

### 【例】（追加条文）

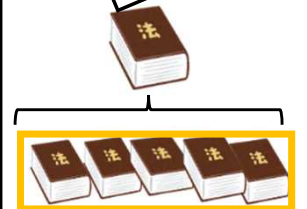
前各項に掲げるもののほか、地方自治体においては、地方自治体の長が定める電子証明書

茨城県

各省で省令が定められており  
職責による署名  
ができるの??



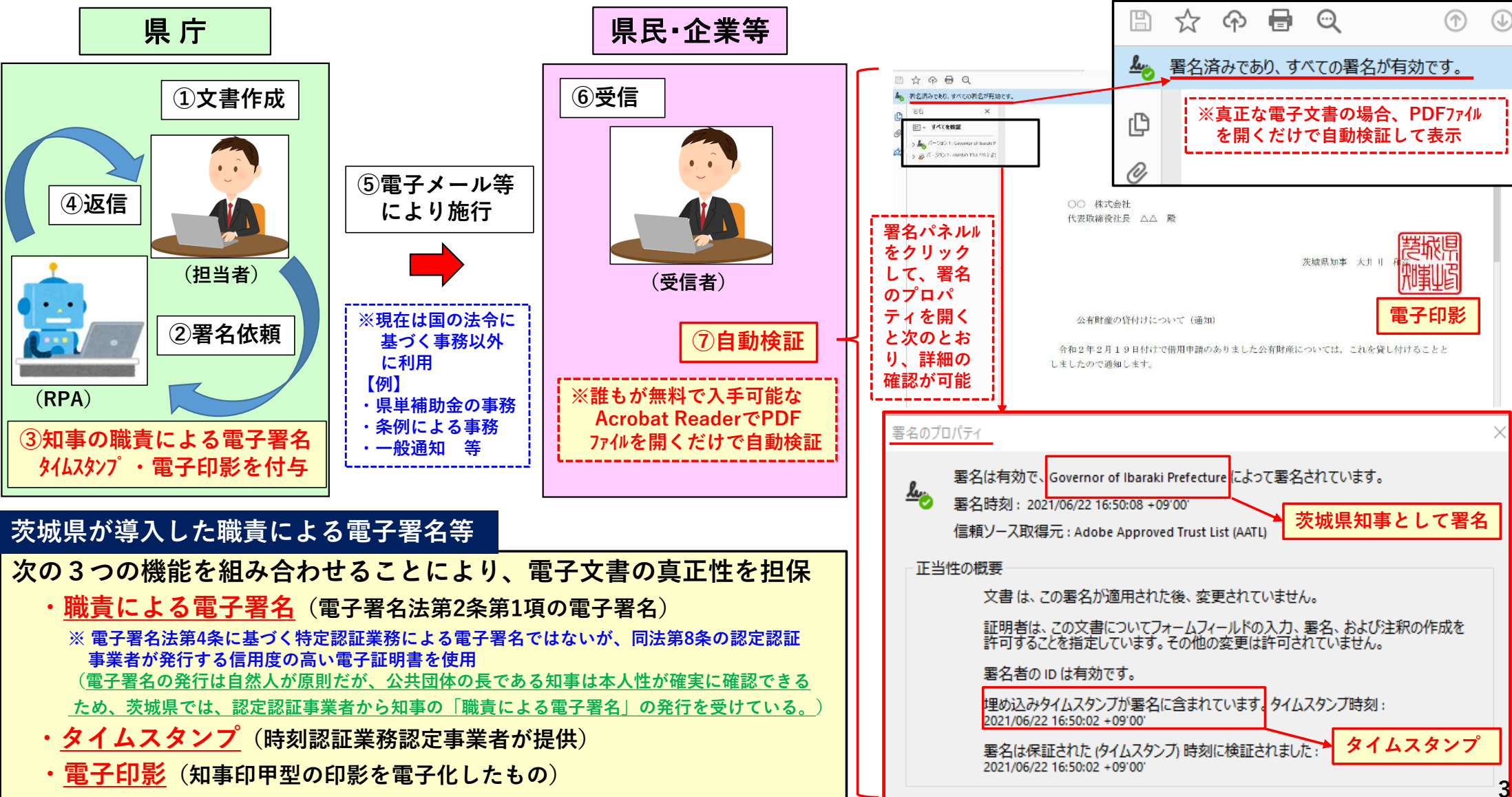
各省の省令の  
文言を統一し  
職責による署名  
を利用可能に



※ 茨城県が導入した「知事の職責による電子署名」は次ページのとおり

# 茨城県で導入した知事の「職責による電子署名」等

令和3年8月導入



## 茨城県が導入した職責による電子署名等

次の3つの機能を組み合わせることにより、電子文書の真正性を担保

- ・ **職責による電子署名** (電子署名法第2条第1項の電子署名)
  - ※ 電子署名法第4条に基づく特定認証業務による電子署名ではないが、同法第8条の認定認証事業者が発行する信用度の高い電子証明書を使用  
(電子署名の発行は自然人が原則だが、公共団体の長である知事は本人性が確実に確認できるため、茨城県では、認定認証事業者から知事の「職責による電子署名」の発行を受けている。)
- ・ **タイムスタンプ** (時刻認証業務認定事業者が提供)
- ・ **電子印影** (知事印甲型の印影を電子化したもの)

## 【各省の省令ごとに定められるデジタル手続に関する条文】

茨城県

課題：デジタル手続に関して、各省の省令ごとに規定され、要件等が異なるため、地方自治体の事務作業が煩雑

省庁名	省令名
デジタル庁	デジタル庁の所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
総務省	総務省関係法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
外務省	外務省の所管する法令の規定に基づく情報通信技術を活用した行政の推進等に関する規則
環境省	環境省の所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
経済産業省	経済産業省の所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
原子力規制委員会	原子力規制委員会の所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
厚生労働省	厚生労働省の所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
国税庁	国税関係法令に係る情報通信技術を活用した行政の推進等に関する省令
国土交通省	国土交通省の所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
財務省	財務省関係法令の情報通信技術を活用した行政の推進等に関する法律施行規則
農林水産省	農林水産関係法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
法務省	法務省の所管する法令の規定に基づく情報通信技術を活用した行政の推進等に関する法律施行規則
文部科学省	文部科学省関係の行政手続等における情報通信の技術の利用に関する省令
税関関係	税関関係法令に係る情報通信技術を活用した行政の推進等に関する省令
内閣府（金融）	内閣府の所管する金融関連法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
内閣府（本府）	内閣府の所管する内閣府本府関係法令に係る行政手続等における情報通信技術の利用に関する法律施行規則
消費者庁	内閣府の所管する消費者庁関係法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則
関係行政機関	関係行政機関が所管する法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則



# 【主な省庁で異なる電子証明書の条文】

課題：省令の電子証明書の定義が異なり、「職責による署名」が利用可能か不明確

## 【各省庁の省令の電子証明書の定義】

- ①地方公共団体情報システム機能の認証業務に関する法律第3条第1項に規定する電子証明書
- ②電子署名及び認証業務に関する法律施行規則第4条第1項に規定する電子証明書
- ③商業登記法第12条の2第1項及び第3項の規定に基づき登記官が作成した電子証明書
- ④その他



省庁名	電子証明書の定義	④その他の証明書
デジタル庁 内閣府（本府）	① ③④	内閣総理大臣が告示で定める電子証明書 行政機関等が指定する電子証明書
総務省	①②③	
環境省	①②③④	行政機関等が作成する電子証明書
経済産業省	① ③④	経済産業大臣が告示で定めるもの
原子力規制委員会	①②③④	原子力規制委員会が定める電子証明書
厚生労働省	①②③④	行政機関等が指定する電子証明書
国土交通省	① ③④	国土交通大臣が告示で定める電子証明書
農林水産省	①②③④	行政機関等が作成する電子証明書
文部科学省	①②③④	行政機関等が定める電子証明書



※ 地方自治体においては、環境省・農林水産省の条文が対応しやすい。

## 【主な省庁の省令の処分通知の方法（法第7条第1項関係）の条文が不統一】

茨城県

課題：省令の処分通知の方法の条文が異なり、デジタル庁の要件よりも他省庁は要件は厳しくなっている。

省令の規定	省庁名	疑義内容
<p>行政機関等が法第7条第1項の規定により処分通知等を電子情報処理組織を使用する方法により行うときは、当該処分通知等を書面等により行うときに記載すべき事項を行政機関等の使用に係る電子計算機から入力して行うものとする。</p>	デジタル庁	
<p>法第7条第1項の規定により電子情報処理組織を使用する方法により処分通知等を行うときは、当該処分通知等を書面等により行うときに記載すべきこととされている事項を行政機関等の使用に係る電子計算機に備えられたファイルに記録しなければならない。</p>	総務省	<p>条文の意図が不明確で、行政機関等がファイルに記録する旨の記載であるため、ファイル共有システムが別途必要と認識する懸念あり</p>
<p>電子情報処理組織を使用する方法により処分通知等を行う行政機関等は、当該処分通知等につき規定した他の法令の規定において書面等に記載すべきこととされている事項を行政機関等に使用に係る電子計算機から入力し、当該事項についての情報に電子署名を行い、当該電子署名に係る電子証明書であって第四条第二項各号に掲げるものと併せて当該行政機関等に使用に係る電子計算機に備えられたファイルにこれを記録しなければならない。行政機関等は、処分通知等を受けるものが当該処分通知等をその使用に係る電子計算機に備えられたファイルに記録することが可能となったときから24時間以内に当該処分通知等を記録しない場合その他行政機関等が必要と認める場合は、書面等により当該処分通知等を行うことができる。</p>	環境省 経済産業省 原子力規制委員会 厚生労働省（ただし24時間以内の規定は無し）	<p>上記同様、条文上、ファイル共有システムが別途必要と認識する懸念あり （特に24時間以内に相手方が記録しない場合の対応が定められているため、ファイル共有システム等が無い場合は対応不可と認識）</p>
<p>電子情報処理組織を使用する方法により処分通知等を行う行政機関等は、当該処分通知等を書面等により行う場合において法令の規定により記載すべきこととされている事項を行政機関等の使用に係る電子計算機から、電子情報処理組織を使用する方法により処分通知等を行う場合において従うこととされている様式に入力し、処分通知等を行わなければならない。電子署名を行い、その情報を当該電子署名に係る電子証明書であって第五条第一号二に掲げるものと併せて送信すること。</p>	農林水産省	<p>処分通知等を行う場合は、電子的な方法で様式をあらかじめ定めておく必要がある</p>
<p>行政機関等が、法第7条第1項の規定により処分通知等を電子情報処理組織を使用する方法により行うときは、当該処分通知等を書面等により行うときに従うこととされている様式に記載すべき事項を前条の行政機関等の使用に係る電子計算機から入力し電子署名を行い、その情報を当該電子署名に係る電子証明書であって国土交通大臣が告示で定めるものとともに前条の処分通知等を受ける者の使用に係る電子計算機に備えられたファイルに記録できる状態に置かなければならない。前項の規定に基づく処分通知等を受ける者が当該処分通知等をその使用に係る電子計算機に備えられたファイルに記録することが可能となったときから行政機関等が指定する期限までに記録しない場合その他行政機関等が必要と認める場合は、行政機関等は、書面等により当該処分通知等を行うことができる。</p>	国土交通省	<p>処分通知を受ける者の使用に係る電子計算機に備えられたファイルに記録できる状態に置くことまで規定する必要性が不明確。 相手方から電磁的記録による通知を受ける旨の届け出のみで足りると認識。</p>

## 【その他の各省の省令の条文も不統一】

課題：その他にも各省の省令ごとに要件等が異なり、全ての省令に合致する手続きの把握は困難

## ○ 電子申請で行うことが難しい場合の要件（法第6条第6項関係）

次の例のように要件が統一しておらず、取り扱いにおいて混乱することが想定される。

- 【例】・経済産業省：デジタル庁の条文に「有体物を提出する場合」が追加  
 ・厚生労働省：デジタル庁の条文に「虚偽が無いかどうかを対面により確認する必要がある場合」が追加

(デジタル庁の条文)

- ・対面により本人確認をするべき事情があると当該申請等が行われる行政機関等が認める場合
  - ・申請等に係る書面等のうちにその原本を確認する必要があるものがあると当該申請等が行われるべき行政機関等が認める場合
- なお、申請等のうちに電子情報処理組織を使用する方法により行うことが困難と認められる部分の提出は、電子情報処理組織を使用して申請等を行った日から一週間以内にしなければならない。



## ○ 処分通知を受領できる方式（法第7条第1項関係）

※「行政機関等」には地方自治体も含む  
 (デジタル手続法第3条)

次の例のように、デジタル庁に比べて要件が厳しくなっている。

- 【例】総務省や環境省：デジタル庁の「前2号に掲げるもののほか、行政機関等が定める方式」の条文なし  
 経済産業省：「処分通知等を受けるものが、あらかじめ申請を行う方法により処分通知を受ける旨を届け出る」の条文のみ

(デジタル庁の条文)

- ・電子情報処理組織を使用して行う識別番号及び暗証番号の入力
- ・電子情報処理組織を使用する方法により処分通知等を受けることを希望する旨の行政機関等の定めるところにより行う届出
- ・前2号に掲げるもののほか、行政機関等が定める方式



## ○ その他

- ・電子情報処理組織による申請方法等の条文
- ・法第6条第5項に規定する手数料の条文
- ・法第7条第5項の処分通知のうち電子処理組織を使用する方法が困難な場合の条文 等



# ご議論いただきたいこと

- 1 デジタル原則の「デジタル完結・自動化原則」の実現に向けて、トラストサービスが活用可能なユースケースはどこだと考えるか。
- 2 茨城県庁からの要望書について

# (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)	太田 洋	西村あさひ法律事務所 パートナー弁護士
濱口 総志	慶應義塾大学SFC研究所 上席所員	崎村 夏彦	東京デジタルアイデアーズ株式会社 主席研究員
宮内 宏	宮内・水町IT法律事務所 弁護士	佐古 和恵	早稲田大学 基幹理工学部情報理工学科 教授
林 達也	LocationMind株式会社 取締役	その他関係行政機関	
宮村 和谷	PwCあらた有限責任監査法人 パートナー	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	袖山 喜久造	S K J 総合税理士事務所 所長・税理士
佐藤 創一	一般社団法人新経済連盟 政策部長	中武 浩史	Global Legal Entity Identifier Foundation (GLEIF) 日本オフィス 代表
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)	小松 博明	有限責任あずさ監査法人 東京 I T 監査部 パートナー
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	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
若目田 光生	一般社団法人日本経済団体連合会 デジタルエコミー 推進委員会企画部会 データ戦略 WG 主査	小倉 隆幸	シヤチハタ株式会社 システム法人営業部 部長
太田 大州	デジタルトラスト協議会 渉外部会長	島岡 政基	セコム株式会社IS研究所 主任研究員
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	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
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	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