日本における包括的なトラストの枠組み整備に係る調査研究

最終報告書

令和３年（2021 年）8月 31 日

目次

1　骨子

「データ戦略タスクフォース 包括的データ戦略」にて公表している「トラストの論点と課題」の中で示されている内容を踏まえ、我が国におけるトラストの枠組みを検討する上で必要となる、国内外のトラストに係る取り組みの動向や課題等の調査を実施した。

【調査対象】

海外：欧州 eIDAS 規則、国連 UNCITRAL、北米 WebTrust

国内：電子署名法、公的個人認証法、商業登記法、電子委任状法、民法等における通用性、タイムスタンプ関連告示等（総務省）、e シールに係る指針（総務省）、リモート署名ガイドライン

上記を踏まえ、 日本における包括的なトラストの枠組み整備に必要な論点とその具体的な在り方の調査として、ニーズ調査の対象を分類、あるべき認定の効果、認定効果を担保するための制度のあり方および、既存法制度との GAP 解消策を検討した。

今後のデータ戦略を推進するにあたりトラストサービスに関する「民間ニーズ」、「国の制度に基づく手続き」および、今後必要となる国際社会でのニーズに関し調査の具体的な対象と計画を明確にし、実地調査を踏まえ検討を深めるべきである。

2　調査の範囲と内容

「トラストに関するワーキングチーム」(以下、TWT と呼ぶ)ではトラスト基盤の構造との関係で以下が示された。

（1）トラストサービスに共通する一般原則と共通要件を整理する。

（2）各トラストサービスの個別要件は、個別事項として整理する。

（3）各トラストサービスの具体的な技術的基準等は、規格として策定する。

（4）適合性評価機関の規格は、別途策定する。

図 2-1. トラスト基盤の構造

本研究では、次節に記載した国内外のトラストに係る取り組み動向及び課題の調査を実施し、上記に従って、各要件、規格等の整理を行った。

2.1　国内外のトラストに係る取り組み動向及び課題の調査

国内外のトラストに係る法制度やサービス等の取り組み動向やその利用実態、また顕在化している課題を調査する。

2.1.1 調査事項

国内外のトラストに係る取り組み動向及び課題に関して、以下の調査を実施する。

（1）日本において、包括的なトラストの枠組み整備に関係してくる法制度。
（2）日本において、包括的なトラストの枠組み整備に関係してくる仕組み（標準規約、各種トラストサービス、 認証基盤 等）。
（3）調査した日本の関係法制度や仕組みにおいて、包括的なトラストの枠組み整備を推進するにあたり、解決すべき課題。
（4）諸外国（EU 及び UNCITRAL）における、包括的なトラストの枠組みを整備している事例やその法制度・仕組み（標準規約、各種トラストサービス、認証基盤 等）。
（5）諸外国（EU 及び UNCITRAL）における、調査した関係法制度や仕組みにおいて、その利用実態を踏まえ、考慮すべき課題。
（6）諸外国（EU 及び UNCITRAL）において、包括的なトラストの枠組みの整備にあたり、取り決めているデータの範囲。

2.1.2 調査方法

国内及び諸外国におけるトラストに係る取り組み動向及び課題に関して、以下の関連制度等を対象とし調査を行い、2.2 の分析・整理の参考 となるよう整理する。

2.1.3 文献調査

（1）eIDAS 規則及び関連技術水準
（2）国際連合国際商取引法委員会（以下 UNCITRAL）：Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services
（3）認証局にかかわる WebTrust 監査基準
（4）国内法令等
　ア. 電子署名法
　イ. 公的個人認証法
　ウ. 電子委任状法

エ. 商業登記法及び関連省令等
オ. e シールに係る指針（総務省）
カ. 時刻認証業務の認定に関する規程（令和３年（2021 年）総務省告示第 146 号）
キ. 民法、民法施行法、民事訴訟法等
ク. リモート署名ガイドライン
ケ. グレーゾーン解消制度→トラストに関する質問に対し、基準が明確でないため個別に独自判断で基準をみたす旨回答している実態に対する課題提起

2.1.4ヒアリング調査（案）

GPKI、LGPKI、公的個人認証サービス、商業登記に基づく電子認証制度、HPKI 等に対するヒアリング調査が考えられる。

2.1.5ニーズ調査の対象の洗い出し（案）

デジタル化政策におけるトラストサービスのニーズ、民間の手続き等においてトラストサービスの適用が求められる領域、業務等の調査対象を抽出することが考えられる。

2.2　日本における包括的なトラストの枠組み整備に必要な論点とその具体的な在り方の調査

「データ戦略タスクフォース」にて公表された「包括的データ戦略」の「トラスト基盤の構築に向けた主要な論点と課題」をベースとして、前項「2.1　国内外のトラストに係る取り組み動向及び課題の調査」で得られた成果物をもとに、日本における包括的なトラストの枠組み整備に必要な論点とその具体的な在り方の調査をする。

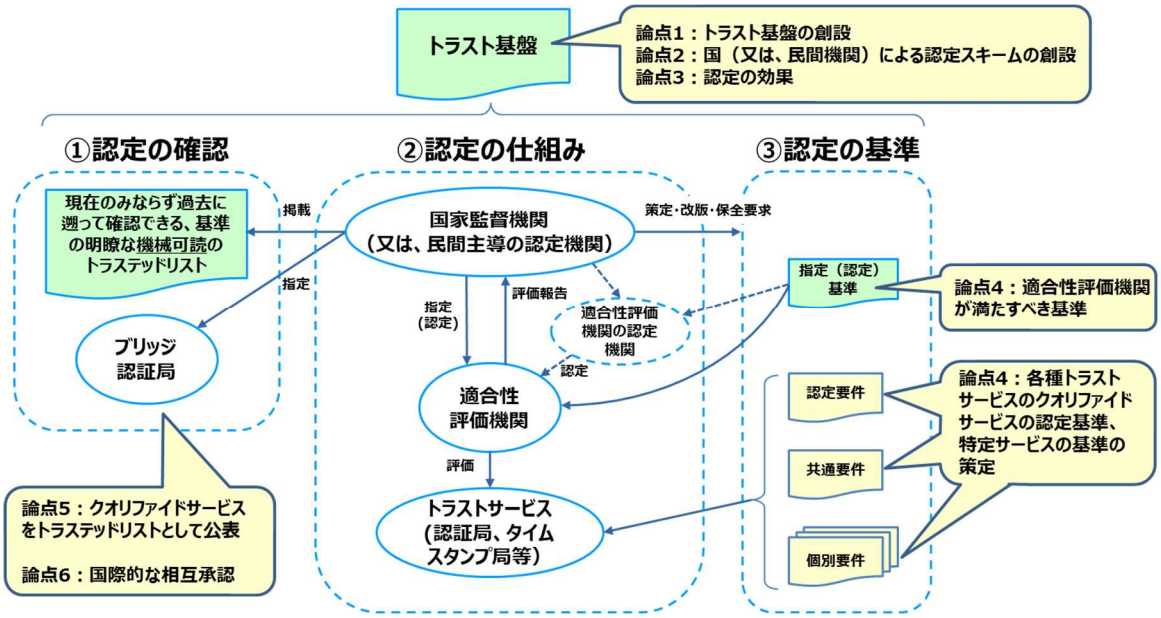
2.2.1調査事項

上記に従って調査を行い、日本における包括的なトラストの枠組み整備に必要な論点を項目に分類・整理(例：法制度、仕組み、データ範囲等)し、その具体的な在り方をまとめる。

2.2.2調査方法

「データ戦略タスクフォース」にて公表された「包括的データ戦略」の「トラスト基盤の構築に向けた主要な論点と課題」をベースとして、「2.1 国内外のトラストに係る取り組み動向及び課題の調査」の項の成果物を加味し、「トラストに関するワーキングチーム」で示された以下の論点１から論点６について、その具体的な在り方の調査をまとめる。

図 2-2.「トラストに関するワーキングチーム」で示された主な論点



（1）論点１：基盤となるトラスト制度の創設で検討する範囲
（2）論点２：基盤となるトラスト制度の創設
（3）論点３：国による基盤となるトラストサービス認定制度の創設
（4）論点４：各種トラストサービスのクオリファイドサービス認定基準、特定サービス基準の策定
（5）論点５：クオリファイドサービスをトラステッドリストとして公表
（6）論点６：トラストサービスの国際的な相互承認の実現

3　国内外のトラストに係る取り組み動向及び課題の調査結果

3.1　文献調査：諸外国

3.1.1 eIDAS 規則及び関連技術水準

3.1.1.1 eIDAS 規則

欧州では、平成 11 年（1999 年）に定められた電子署名指令に替わり、「eIDAS 規則」（注）が平成 26 年（2014 年）7 月に採択された。EU 加盟国はそれぞれ電子署名指令に従った独自の電子署名法を定めているが、これらの各加盟国の電子署名法は、すべて「eIDAS 規則」に上書されることになった。「eIDAS 規則」は、電子署名の法的効力を承認した電子署名指令を継承するものだが、その適用範囲は電子署名を含むトラストサービスと eID に拡大されている。

トラストサービスには、電子署名やタイムスタンプ、e シール、e デリバリー、ウェブ認証等が定められ、これらは経済活動の電子化促進に必要不可欠なセキュアインフラと位置付けられている。eID とは、電子

認証（つまり、電子的な本人確認）を行うことが出来る機能のことであり、「eIDAS 規則」は、この eID の認証結果を各国で受け入れ合うことを定めている。EU 全域で、トラストサービスと eID に関する統一的な法的効力を承認することで、確定申告や銀行口座の開設、入札への参加、大学への入学手続等をオンラインで申請できるようになり、また、他の加盟国への申請も行えるようになる。つまり、「eIDAS 規則」とは、eID とトラストサービスの法的効力を承認し、電子申請、オンライン決済、電子契約等における信頼性が紙の世界と同等であることを担保することで、電子化と効率化の促進を目指した法律であると言える。この電子化と効率化による競争力の向上及び経済成長を狙いとすると同時に、加盟国間の隔たりをなくすことで、欧州全体で 1 つの大きなデジタル市場を構築することを目指している。

（1） eIDAS 規則及びその下位規則に関する施行状況

表 3-1. eIDAS 規則及びその下位規則に関する施行状況

範囲	**規則／実施法**	**参照番号**	**概要**	**採択日**	**発効日**
eID+TS(Trust Services)	eIDAS regulation	2014/910	eID 及び TS の定義、 法的効力、 相互運用性を規定	2014/07/23	2014/09/17 2016/07/01（TS）
eID	ID on procedural arrangements for MS cooperation on eID (art. 12.7)	2015/296	eID の相互運用性確保のために必要な加盟国間の協力(情報公開等)について規定	2015/02/24	2015/03/17
eID	IR on interoperability framework	2015/1501	eID の相互運用性を確保するためのフレームワークを規定	2015/09/08	2015/09/29
eID	IR on assurance level for	2015/1502	eID の保証レベル(LoA)と技	2015/09/08	2015/09/29

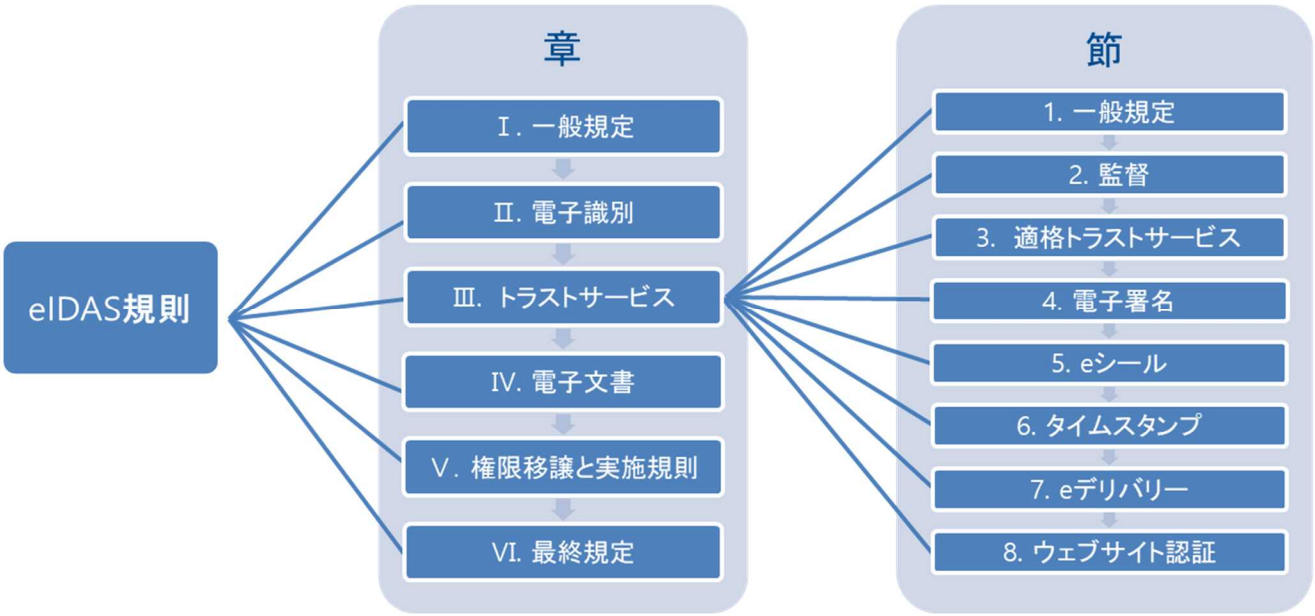
	electronic identification mean		術的要求事項の対応表を規定		
eID	ID on circumstance, formats and procedures of notification	2015/1985	eID スキームの通知方法を規定	2015/11/03	2015/11/05
TS	IR on EU Trust Mark for Qualified Trust Services	2015/806	TS が QTS であることを示すトラストマークを規定	2015/05/22	2015/06/12
TS	ID on technical specifications and formats relating to trusted lists	2015/1505	トラストリストに関する技術的仕様とフォーマットを規定。トラストリストを QTS の検証に利用することで、加盟国間の QTS の相互運用性に寄与する。	2015/09/08	2015/09/29
TS	ID on formats of advanced electronic signatures and seals	2015/1506	公的セクターで認められる先進電子署名及びシール (advanced e signature	2015/09/08	2015/09/29

			and seal)の規定		
TS	ID on security assessment of qualified signature/seal creation devices	2016/650	適格電子署名／シール生成装置の評価に関する規定	2016/04/26	2015/05/16

（2） eIDAS 規則の構成

eIDAS 規則は 6 章、52 条より成り、第 3 章にトラストサービスにつき 8 節に亘り規定されている。

図 3-2. eIDAS 規則の構成



また、第 3 章トラストサービスについては、以下の構成となっており、先ず第 1 節～3 節において一般規定や監督、適格トラストサービスの共通規定等を定めた上で、第 4 節以降に個別の要件が定められている。

表 3-3. トラストサービスの構成

第３章　トラストサービス		
	第１節　一般規定	
		第１３条　証明の責任と負担
		第１４条　国際的な側面
		第１５条　障害者のアクセシビリティ
		第１６条　罰則
	第２節　監督	
		第１７条　監督機関
		第１８条　相互支援
		第１９条　トラストサービスプロバイダに適用されるセキュリティ要件
	第３節　適格トラストサービス	
		第２０条　適格トラストサービスプロバイダの監督
		第２１条　適格トラストサービスの開始
		第２２条　トラステッドリスト
		第２３条　適格トラストサービスのためのEUトラストマーク
		第２４条　適格トラストサービスプロバイダの要件
	第４節　電子署名	
		第２５条　電子署名の法的効力
		第２６条　先進電子署名の要件
		第２７条　公共サービスにおける電子署名
		第２８条　電子署名の適格証明書

		第２９条　適格電子署名生成装置の要件
		第３０条　適格電子署名生成装置の認証
		第３１条　認証済の適格電子署名生成デバイスのリストの公開
		第３２条　適格電子署名検証の要件
		第３３条　適格電子署名の適格検証サービス
		第３４条　適格電子署名の適格保存サービス
	第５節　eシール	
		第３５条　eシールの法的効力
		第３６条　先進eシールの要件
		第３７条　公共サービスにおけるeシール
		第３８条　eシールのための適格証明書
		第３９条　適格eシール生成装置
		第４０条　適格eシールの検証と保存
	第６節　タイムスタンプ	
		第４１条　タイムスタンプの法的効力
		第４２条　適格タイムスタンプの要件
	第７節　eデリバリー	
		第４３条　eデリバリーの法的効力
		第４４条　適格eデリバリーの要件
	第８節　ウェブサイト認証	
		第４５条　ウェブサイト認証のための適格証明書の要件

（3） eIDAS 規則における各トラストサービスの定義と法的効力

第 3 章において定められている各トラストサービスの定義と法的効力は以下の通りである。

表 3-4. トラストサービスの定義と法的効力

トラストサービス	定義	法的効力
電子署名	自然人が電磁的に記録された情報について、その自然人が作成したことを示すもの。	手書きの署名と同等
e シール	文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すもの。	データの完全性と起源と正確性の推定
タイムスタンプ	電子データが、ある時刻に存在していたこととその時刻以降に改ざんされていないことを示すもの。	時刻の正確性とデータの完全性の推定
e デリバリー –	データの送受信の証明も含め、データ送信の取扱いに関する証拠を提供するもの。	送受信者の識別、データの完全性、送受信時刻の正確性の推定
ウェブサイト認証	ウェブサイトが真正で正当な主体により管理されていることが保証できることを示すもの。	ウェブサイトとその管理主体の認証結果の正確性

（4） EU トラストマーク

EU トラストマークは、実施規則 2015/806 で定められており、トラストサービスのプロバイダーおよび提供されるトラストサービスが eIDAS 規則に定められた規則に適格であり、準拠していることを保証する目的で利用される。

図 3-5. トラストマーク

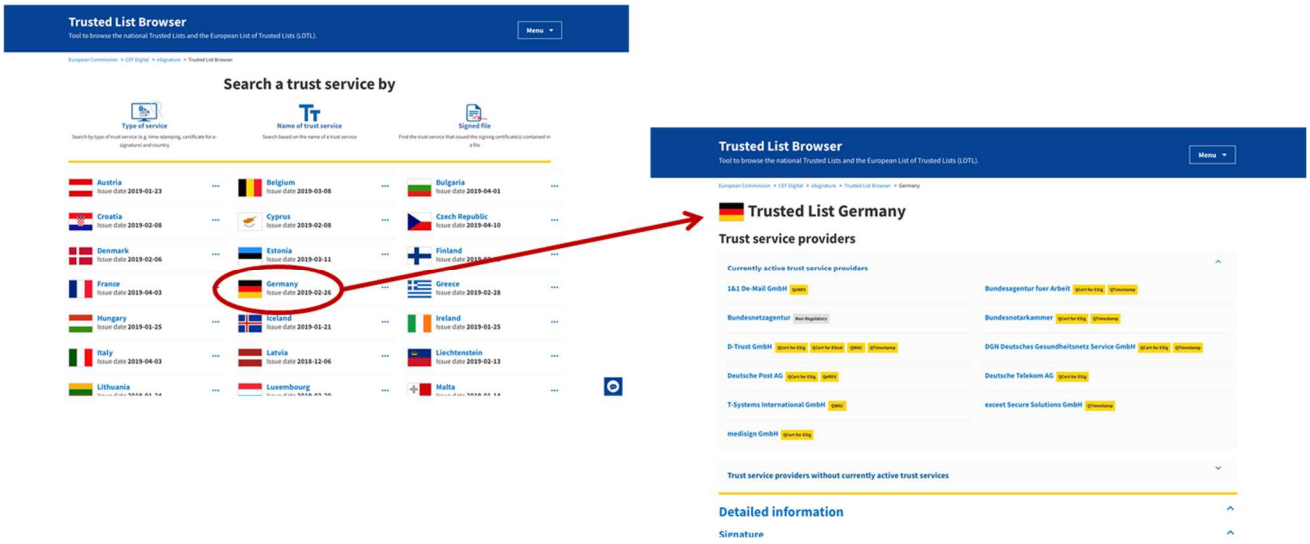
（5）トラステッドリスト

トラストサービスのステータス情報を公開する仕組みとしてトラステッドリストが第 22 条に以下のように規定されている。

eIDAS 3 章 第 *22* 条 各 *EU* 加盟国は、自らが責任を負う適格トラストサービスプロバイダに関する情報と、それらが提供する適格トラストサービスに関連する情報を含むトラステッドリストを作成、維持および公開する義務を負う。リストは、電子署名、またはシールが付された自動化されたプロセスに適した形式の安全な手段で公開される。

トラステッドリストは加盟各国が加盟国内におけるトラストサービスプロバイダの情報を掲載するものであり、監督機関の電子署名/e シールによってその真正性が保護されている。また、欧州委員会は各加盟国トラステッドリストのリストであるリストオブトラステッドリスト（LOTL）を公開しており、各加盟国のトラステッドリストに関する情報と、その真正性を検証するための情報が含まれている。以下の図 3-6.は欧州委員会が公開するトラステッドリストブラウザの表示画面であり、XML 形式で公開されている各トラストリスト及び LOTL を人が目視可能な形式で表示している。

図 3-6. 欧州委員会が公開するトラステッドリストブラウザの表示画面



3.1.1.2 eIDAS 規則の改定案

eIDAS 規則 第 49 条において、当該規則の適用をレビューし、令和 2 年（2020 年）7 月 1 日までに欧州議会及び理事会に報告することが記載されており、令和 2 年（2020 年）7 月 23 日に初期影響評価（INCEPTION IMPACT ASSESSMENT Document Ares(2020)3899583）が公開されている。平成 26 年（2014 年）に批准された eIDAS 規則に対して、その有効性を高め、

民間への適用を拡大し、全欧州市民に信頼されたデジタルアイデンティティを奨励することを目的に、令和３年（2021 年）6 月 3 日に eIDAS 規則の改定提案がなされている（パブリックコメントによる意見募集は令和３年（2021 年）9 月 2 日まで）。

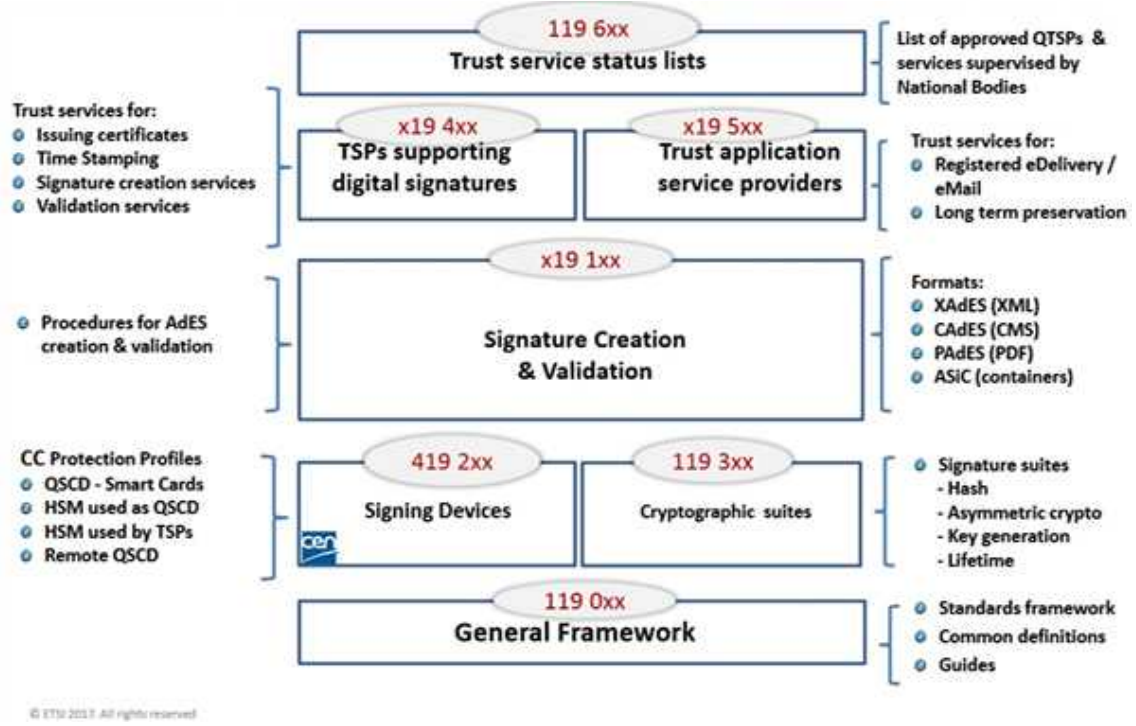
改定案の主な内容は、以下が挙げられる。

- トラストサービスとして電子アーカイブ（electronic archiving）、属性の電子証明（electronic attestation of attributes）、リモート署名/シール生成装置の管理（management of remote electronic signature）、電子台帳（electronic ledgers）を追加し、拡充
- EU Digital Identity Wallet の導入
- 下位規則について、欧州委員会は法律によって整備しなければならないと定められており、ETSI 等の技術基準と法的要件の紐づきがより明確な形となる
- 第 45 条において、ブラウザは、適格 Web サイト認証証明書を認識しなければならないと新たに明記された。

3.1.1.3 関連技術基準

eIDAS 規則におけるトラストサービスに係る技術基準については現在欧州において以下の図 3-7.のように整備されている。

図 3-7. eIDAS 規則におけるトラストサービスに係る技術基準



トラステッドリスト、デジタル署名をサポートとするトラストサービスプロバイダ、トラストアプリケーションサー

ビスプロバイダ、署名生成及び検証、署名装置、暗号スイート、一般フレームワークの 7 つの分野で技術基準が整備されている。

表 3-8. 119 6xx トラステッドリスト

規格番号	内容
ETSI TS 119 612	トラステッドリストの技術仕様
ETSI TS 119 614-1	トラステッドリストの適合性試験

表 3-9. X19 4xx デジタル署名をサポートするトラストサービスプロバイダ

トラストサービス	規格番号		内容
	共通要件	個別要件	
電子署名	ETSI EN 319 401 –	ETSI EN 319 411-1 ETSI EN 319 411-2	認証局のポリシー要件
e シール			
Web 認証			
タイムスタンプ		ETSI EN 319 421	タイムスタンプ局のポリシー要件
検証		ETSI TS 119 441	検証サービスのポリシー要件
電子署名、e シール		ETSI TS 119 431-1	リモート署名サービス事業者のポリシー要件（QSCD 管理）
電子署名、e シール		ETSI TS 119 431-2	リモート署名サービス事業者のポリシー要件（AdES 生成）
電子署名、e シール、Web 認証		ETSI EN 319 412 Part1～5	証明書プロファイル
タイムスタンプ		ETSI EN 319 422	タイムスタンプのプロトコル
検証		ETSI TS 119 442	検証のプロトコル
電子署名、e シール		ETSI TS 119 432	リモート署名のプロトコル

また、この分野においてはトラストサービスの評価に関する基準も以下のように整備されている。

表 3-10. 適合性評価

分野	規格番号	内容
適合性評価機関	ETSI EN 319 403-1	トラストサービスの適合性評価を行う適合性評価機関の要件
適合性評価機関	ETSI TS 119 403-3	適格トラストサービスの適合性評価を行う適合性評価機関の要件

表 3-11. x19 5xx トラストアプリケーションサービスプロバイダ

トラストアプリケーションサービス	規格番号		内容
	共通要件	個別要件	
保存	ETSI EN 319 401 –	ETSI TS 119 511	保存サービスのポリシー要件
保存		ETSI TS 119 512	保存サービスのプロトコル
e デリバリー		ETSI EN 319 521	e デリバリーサービス(ERDS)のポリシー要件
e デリバリー		ETSI EN 319 531	e デリバリーサービス(REM)のポリシー要件
e デリバリー		ETSI EN 319 522 Part1～Part4	e デリバリーサービスの技術仕様

表 3-12. X19 1xx 署名生成及び検証

トラストサービス	規格番号	内容
電子署名、e シール、タイムスタンプ	ETSI EN 319 122-1 ETSI EN 319 122-2 ETSI TS 119 122-3 ETSI EN 319 132-1 ETSI EN 319 132-2	署名フォーマットの技術仕様

	ETSI EN 319 142-1 ETSI EN 319 142-2 ETSI TS 119 142-3 ETSI EN 319 162-1 ETSI EN 319 162-2	
電子署名、e シール、検証	ETSI EN 319 102-1	署名生成及び検証のプロシージャ
電子署名、e シール、検証	ETSI TS 119 102-2	署名検証レポート

表 3-13. 419 2xx 署名装置

分野	規格番号	内容
適格電子署名生成装置	ETSI EN 419 211-1 ETSI EN 419 211-2 ETSI EN 419 211-3 ETSI EN 419 211-4 ETSI EN 419 211-5 ETSI EN 419 211-6	適格電子署名生成装置のプロテクションプロファイル
リモート署名	CEN EN 419 241-1	リモート署名システムのセキュリティ要件
リモート署名向け適格電子署名生成装置	CEN EN 419 241-2	リモート署名向け適格電子署名生成装置のプロテクションプロファイル
タイムスタンプ	CEN EN 419 231	タイムスタンプシステムのセキュリティ要件

表 3-14. 119 3xx 暗号スイート

分野	規格番号	内容
暗号	ETSI TS 119 312	推奨暗号アルゴリズム及び鍵長

3.1.2 UNCITRAL：Identity Management and Trust Services

国際連合での議論

国際連合では、国際商取引法の調和を図るため、条約・モデル法・立法ガイドライン等を策定する機関として1966年に創設された、国際連合国際商取引法委員会（UNCITRAL）の電子商取引に関して検討している第４部会（WG-Ⅳ）において、トラストサービスについて議論がされている。

2011 年頃から、Identity Management (IdM) and Trust Services について作業候補として挙げられ、2015 年に採択された SDGs の以下のターゲットとも関連し、2016 年から詳細な議論が開始されたところである。

表 3-15. 関連する SDGs のターゲット

1.4	2030年までに、貧困層及び脆弱層をはじめ、全ての男性及び女性が、基礎的サービスへのアクセス、土地及びその他の形態の財産に対する所有権と管理権限、相続財産、天然資源、適切な新技術、マイクロファイナンスを含む金融サービスに加え、経済的資源についても平等な権利を持つことができるように確保する。
10.c	2030年までに、移住労働者による送金コストを３％未満に引き下げ、コストが5%を越える送金経路を撤廃する。
16.5	あらゆる形態の汚職や贈賄を大幅に減少させる。
16.9	2030年までに、全ての人々に出生登録を含む法的な身分証明を提供する。

当該WGでは、平成８年（1996年）電子商取引モデル法制定時に合意された、以下の作業を貫く原則となっている。

（1）Non-discrimination：電子的なものであるというだけの理由で法的な効果、有効性、エンフォース可能性が否定されてはならない。

（2）Functional equivalence：非電子（紙）の世界で果たされている（あるいは求められている）機能と同等の機能を電子の世界でどのようにすれば果たせるかという観点

（3）Technological neutrality：さまざまな技術の可能性を排除しないために、特定の技術や手法を前提とした制度設計を避ける

（4）Party autonomy：電子的手段の利用においては当事者の契約の自由が優先する

これらの原則の下、令和元年（2019年）の第58回会議にて、国際商取引の障害として以下の４点があると整理され、条文案として、A/CN.9/WG.IV/WP.157
“Draft Provisions on the Cross-border Recognition of IdM and Trust Services”が提示された。

（1）IdM とトラストサービスに法的効果を与える法制度が無いこと

（2）システム間の相互運用性の問題
（3）紙ベースのものを求める法制度の存在
（4）国ごとに異なる法制度の存在とクロスボーダー相互の法的承認メカニズムの欠如
そして、これらの障害を取り除くには、IdM and Trust Services 利用への信頼を高めるための法的裏付けが必要であり、そのためには、サービス提供者等当事者の義務や責任等を明確化することが重要であるとされ、法的承認及び相互承認を作業目標として特定された。
その後、この条文案は、A/CN.9/WG.IV/WP.160、A/CN.9/WG.IV/WP.162を経て、現在の作業文書は、A/CN.9/WG.IV/WP.167
"Provision on the Use and Cross-border Recognition of Identity Management and Trust Services"まで改版され、令和３年（2021 年）10 月の第 61 回での最終化を目標に議論されている。
条文案は、第１章 総則、第２章 IdM、第３章 トラストサービス、第４章 国際的側面の４章構成で、トラストサービスについては、トラストサービスの法的効果と、トラストサービスとして、電子署名、e シール、タイムスタンプ、電子アーカイビング、e デリバリー、web サイト認証が規定されており、それらサービスの信頼性判断要件、指定、責務が規定されている。
各条文案の概略を表 3-16 に記載する。

表 3-16. UNCITRAL で議論されている条文案概略

章・条	項目	概略
1 章	総則 General provisions	
1 条	定義 Definitions	
2 条	適用範囲 Scope of application	＊商取引および取引に関係するサービスにおける IdM and trust services の利用 ＊認証やトラストサービスを用いるべき場面については取り扱わない（各国・取引ごとに異なる問題） ＊プライバシーやデータ保護の問題も取り扱わない
3 条	IdM and trust services の任意利用 Voluntary use of IdM and trust services	＊本人の同意なしに IdM and trust services を使用することを求めない ＊ただし、その者の行為から同意を推測することが可能
4 条	解釈 Interpretation	＊本草案の解釈においては、国際的な性格等を考慮しなければならない。 ＊明示的に解決されないものについては、規定の根拠となる一

		般原則等に従って解決する。
2 章	Identity Management	
5 条	IdM の法的承認 Legal recognition of IdM	＊電子的なものであるというだけの理由で有効性を否定されない(non discrimination の原則)
6 条	IdM サービス提供者の義務 Obligations of IdM service providers	＊IdM サービスの提供（具体的内容について詳細に定めている）のための適切な業務規程、手続、実務、デザインを準備し、それに従うこと ＊システムのオンラインでの利用可能性と正確な動作の確保 ＊業務規程等へのアクセスの確保 ＊利用者からの通知（8 条参照）手段の確保
7 条	データ侵害（ data breach ）の場合の IdM サービス提供者の義務 Obligations of IdM service providers in case of data breach	＊データ侵害の阻止、回復、法に従った通知
8 条	利用者の義務 Obligations of subscribers	＊認証の漏洩を発見した場合にはサービス提供者に通知する義務
9 条	IdM を利用する人の identification Identification of a person using IdM	＊法が identification を要求または認めているとき、 IdM については「信頼できる手段」が用いられていれば法の要件を満たすものとする ＊11 条で指定された手段は「信頼できる手段」であると推定する
10 条	IdM サービスの「信頼性」の要件 Requirements for determining reliability of IdM [services][systems]	＊以下を含む全ての関連する状況に照らして判断される a. 6 条の義務を果たしているか b.当該サービスの業務規程等が関係する国際基準・手続（level of assurance の枠組みを含む）に即しているか（特に：ガバナンス、発行された通知およびユーザーインフォメーション、情報セキュリティマネジメント、記録管理、設備とスタッフ、技術的コントロール、監視・監査） c. 監督や認可の存在 d. 当該 Identity の利用目的

		e. 当事者間の契約（当該 Identity の利用制限を含む） ＊IdM サービスの地理的な所在は「信頼性」に影響しない
11 条	信頼できる IdM システムの指定 Designation of reliable IdM systems	＊事前に当局等で信頼できる IdM システムを指定することを認める ＊10 条の基準に従って指定する必要がある ＊信頼できる IdM システム一覧を公表する必要がある ＊国際的基準（level of assurance を含む）に適合している必要
12 条	IdM サービス提供者の（民事）責任 Liability of IdM service provider	＊契約法等一般法に委ねるか、特別の法定責任を課すか
3 章	トラストサービス	
13 条	トラストサービスの法的承認 Legal recognition of trust services	＊電子的なものであるというだけの理由で有効性を否定されない。 (non discrimination の原則)
14 条	トラストサービス提供者の義務 Obligations of trust service providers	＊ポリシーと実務に関して表明したものに従うこと ＊当該ポリシーと実務への利用者・第三者からのアクセス確保 ＊利用者からの通知（15 条参照）手段の確保 ＊データ侵害の阻止、回復、法に従った通知
15 条	利用者の義務 Obligations of subscribers	＊セキュリティ破壊を発見した場合にはサービス提供者に通知
16 条	電子署名 Electronic signatures	＊法の規定が人の署名を要求し、または認めている場合、以下のことを行うために「信頼できる手法」が用いられていればそのデータメッセージについては当該規定の要件は満たされているものとする。 a.人を特定すること、かつ b.当該データメッセージに含まれた情報について当該人の意思(intention)を示すこと ＊23 条に指定された電子署名を行う場合には、上記の信頼性があると推定される。
17 条	電子シール Electronic seals	＊法の規定が人（法人を含む）にシール付与を要求し、または認めている場合、以下のことを行うために「信頼できる手法」が用いられていればそのデータメッセージについては当該規定の要件は

		満たされているものとする。 a.当該データメッセージの出所について信頼できる確証を提供すること、かつ b.シールが付された時以後に当該データメッセージに対してなされたすべての改変（通信・保存・表示の通常の課程によって生ずるデータの裏付けや変更を除く）を発見すること。 ＊23 条に指定された電子シールを用いる方法は、上記の信頼性があると推定される。
18 条	電子タイムスタンプ Electronic timestamps	＊法の規定が文書・記録・情報またはデータに日時を関連付けることを要求し、または認めている場合、以下のこと行うために「信頼できる手法」が用いられていればそのデータメッセージについては当該規定の要件は満たされているものとする。 a.日時（タイムゾーンへの言及を含む）を示すこと、かつ b.当該日時を当該データメッセージと関連付けること ＊23 条に指定された電子タイムスタンプを用いる場合には、信頼性のある方法と推定される。
19 条	電子アーカイビング Electronic archiving	＊法の規定が文書・記録または情報が保存されることを要求し、または認めている場合、以下のことを行うために「信頼できる手法」が用いられていればそのデータメッセージについては当該規定の要件は満たされているものとする。 a.当該データメッセージに含まれる情報が以後参照可能な形でアクセスできること、 b.①アーカイビングの日時を示し、かつ当該日時を当該データメッセージと関連付け、かつ②当該データメッセージをそれが創出、送付または受領されたときの形式で保管するか、その後の変更を発見できる形で表示できる形式で保管するために、信頼できる方法が用いられていること、かつ c.データメッセージの出所および送付先およびそれが送付されまたは受領された日時を特定することができる情報があればこれを保管すること ＊23 条に指定された電子アーカイブを用いる場合には、上記の信頼性があると推定される。
20 条	電子登録デリバリー Electronic registered delivery [services]	＊法の規定が文書・記録または情報が登録された郵便またはそれに類するサービスによって交付されることを要求し、または認めている場合、以下のことを行うために「信頼できる手法」が用いられていればそのデータメッセージについては当該規定の要件は満たさ

		れているものとする。 a.当該データメッセージが受領された日時を示すこと b.当該データメッセージが交付された日時を示すこと c.当該データメッセージの正統性を保証すること、かつ d.送付者と受領者を特定すること ＊23 条に指定された電子登録デリバリーを行う場合には、上記の信頼性があると推定される。
21 条	ウェブサイト認証 Website authentication	＊法の規定がウェブサイトの認証を要求し、または認めている場合、当該ウェブサイトのドメインネームを保有する者を特定し、かつ当該人と当該ウェブサイトとを関連付けるために「信頼できる手法」が用いられていればそのデータメッセージについては当該規定の要件は満たされているものとする。 ＊23 条に指定されたウェブサイト認証が用いられる場合には、上記の信頼性があると推定される。
22 条	トラストサービスの信頼性判断の要件 Requirements for determining reliability for trust services	＊16 条から 21 条は、以下を含む全ての関連する状況に照らして判断される ・業務規程・ポリシー・実務（サービス終了時の計画を含む）、 ・国際基準・手続、業界標準、ハードウェア・ソフトウェアのセキュリティ、 ・財務的・人的資源、独立主体による監査の定期性と範囲、 ・監督主体や認可主体等による信頼性に関する言明、 当該トラストサービスの機能、当事者間の契約 cf.信頼性は機能ごとに判断される相対的な概念 ＊実際に当該機能を果たしていれば信頼性があるとみなされる。 ＊サービス提供の地理的所在は信頼性の判断に影響しない。
23 条	信頼できるトラストサービスの指定 Designation of reliable trust services	＊事前に当局等で信頼できるトラストサービスを指定することを認める。 ＊22 条の基準に従って指定する必要がある。 ＊信頼できるトラストサービス一覧を公表する必要がある。 ＊認知された国際的基準に適合している必要がある。 ＊個人、組織等は、16 条から 21 条までの規定の適用に、信頼できるトラストサービスを指定できる。 ＊トラストサービスの指定に当たっては、22 条に掲げる事項を含む一切の事情を考慮すること、および、トラストサービスプロバイダの詳細を含むトラストサービスの一覧を公表すること

		＊トラストサービスを指定するには、トラストサービスが提供される地理的所在地、および、トラストサービスプロバイダの事業所の所在地次に掲げる事項を考慮してはならない。
24 条	トラストサービス提供者の（民事）責任 Liability of trust service providers	＊トラストサービスプロバイダの責任は、法律で定めるところによるあるいは、 ＊トラストサービスプロバイダは、故意又は過失により人に生じた損害を賠償する責任を負う、ただし特定の条件下ではトラストサービスの利用によって生じた加入者の損害を賠償する責任を負わない。
4 章	国際的側面 International aspects	
25 条	IdM と Trust Services のクロスボーダーの承認 Cross-border recognition of IdM [systems][services] and trust services	＊法域の外で提供されている IdM と trust services も、同等のレベルの信頼性があれば、当該法域内のものと同等の法的効力を持つ
26 条	協力 Cooperation	＊外国の IdM と trust services の承認、指定、 level of assurance や信頼性の基準の定義等についての記載

成果物の形式は未定であるが、国家間でのやりとりとなることから、統一的な規範となるモデル法として提案されることになると推定される

3.1.3 認証局にかかわる WebTrust 監査基準

Web サイト証明書を発行する認証局は、そのルート証明書を主要なブラウザに登録する必要があり、WebTrust for CA(米国公認会計士協会及びカナダ勅許会計士協会によって共同開発された電子商取引認証局監査プログラム）監査を受けることがその要件となっている。

また、近年では Web サイト証明書に限らず、ドキュメント署名用の証明書を発行する中間認証局も上記ルート認証局の配下に存在している。

WebTrust の監査項目（WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES Version.2.2.1）の電子署名法施行規則の認定認証業務に関する基準との対比表を別添付録 1、「認定認証業務」と「WebTrust 監査」の基準の比較表に示す。

利用者の真偽確認(規則第 5 条 利用者の真偽の確認の方法)は、自然人に対して証明書の発行を行う認定認証業務は固有の基準となっているが、設備基準(規則第 4 条 業務の用に供する設備の

基準)、運用基準(規則第 6 条　その他の業務の方法)については、WebTrust 監査では記載レベルの差異はあるものの認証局の共通要件、個別要件、認定要件を抽出し共通化可能な基準として整備すべく検討を行うべきではないかと考える。

3.2　文献調査：国内法令等

3.2.1電子署名法

（1） 名称

電子署名及び認証業務に関する法律（平成 12 年法第 102 号。以下、「電子署名法」という。）

（2） 制定の経緯

公布日：平成 12 年（2000 年）5 月 31 日

施行日：平成 13 年（2001 年）4 月 1 日

（3） 目的

電子署名に関し、電磁的記録の真正な成立の推定、特定認証業務に関する認定の制度その他必要な事項を定めることにより、電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与すること。

（4） 主務省

総務省、法務省及び経済産業省

（注）デジタル庁設置法の施行に基づき、令和 3 年（2021 年）9 月 1 日にデジタル庁及び法務省に改正される予定。

（5） 政省令等の構造

電子署名法第 4 条が定める特定認証業務の認定の制度のみが、細かく規定されている。

ア. 電子署名及び認証業務に関する法律施行令：業務の認定や指定調査機関の指定の有効期間、認定申請に係る手数料の額と認可について定める。

イ. 電子署名及び認証業務に関する法律施行規則：主に法第 6 条から第 11 条に従い、特定認証業務の認定の基準等を定める。以下、電子署名法施行規則という。

ウ. 電子署名及び認証業務に関する法律に基づく指定調査機関等に関する省令：指定調査機関の指定の基準等を定める。

エ. 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針：施行規則をより詳細化し、認定の基準の細目を定めた告示。以下、電子署名法指針という。

オ. 電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針：指定調査機関の調査方針を明確化するための主務省の局長通知。以下、電子署名法方針という。

カ. 電子署名及び認証業務に関する法律第十五条第三項に規定する書類の記載事項を定め

る省令

（6） 特徴及び課題

自然人が行う電子署名とそのための認証業務（認証局）のみを対象としており、EU の eIDAS 規則等に比べてスコープが狭いと考えられる。

ア. 電子署名、認証業務及び特定認証業務の定義（電子署名法第 2 条）

(ア) 電子署名の定義として、自然人が行った措置のみを対象としており、法人等の名義で行われた措置を対象としていないと解釈されている 。

(イ) 「電子署名」を行う者が確かにそれを行ったことを確認するために用いられる事項が本人に係るものであることを証明する業務を「認証業務」として定義している。このため、いわゆる「電子認証」で用いられる公開鍵電子証明書を発行する業務は、「認証業務」ではない。また、「認証業務」は、その利用者が「電子署名」を行う環境の整備に係るものを含んでいないと解釈される。

(ウ) 「認証業務」のうち、特定の方式を用いるものを「特定認証業務」として定義しており、施行規則においては、公開鍵暗号方式（PKI)の原則のみを記しているだけであり、特定認証業務の技術基準は事実上定められていない。

イ. 電磁的記録の真正な成立の推定（電子署名法第 3 条）

(ア) 電子署名を行う者が自身の署名鍵を、リモート署名事業者のサーバ上に設置・保管し、当該署名鍵を用いて電子署名を行うユースケース（いわゆるリモート署名）において、推定効がはたらくかどうかの解釈が明らかにされていない。

(イ) 電子契約サービスの利用者が、当該サービスの提供事業者に指示をして、当該事業者自身の署名鍵を用いて電子署名を行うユースケース（いわゆる事業者署名型電子署名）において、推定効がはたらくかどうかの具体的な判断基準が明らかにされていない。

ウ. 特定認証業務に関する認定の制度（電子署名法第 4 条～第 14 条）

(ア) 認定認証業務が適合すべき基準を定める施行規則等が、法施行時からほとんど改正されていない。

a. 情報セキュリティに関するリスクマネジメントの概念が含まれていない。

b. 認証局の秘密鍵を作成及び管理する暗号装置（HSM: Hardware Security Module）の技術基準が、最新のものではない。

c. 利用者自らが鍵ペアを作成し、認証局に対して公開鍵をオンライン送信する場合には、認証局はあらかじめ利用者識別符号を利用者に送付（対面または本人限定受取郵便）しなければならない。それ以外にも公的個人認証サービスによる電子署名を付す等の方法を取れば、利用者識別符号を利用者に送付する必要はないのではないか。

d. 利用者の指示に基づきサービス提供事業者が利用者の鍵ペアを保管し、利用者の秘密鍵を用いて電子署名を行うサービス（いわゆるリモート署名サービス）が介

在する場合が想定されておらず、認証局と同サービスとの関係が一切規定されていない。

e. 公開鍵暗号方式における秘密鍵が、特定認証業務の利用者の手元で管理されることを想定している。

f. EU の eIDAS 規則における適格署名生成装置（QSCD: Qualified electronic Signature/Seal Creation Device）に相当する装置に関する規定がない。

(イ) 認定認証業務に関する情報は、官報による公告及び主務省の Web サイトによる公示により、公開されている。

a. 官報では公開鍵電子証明書のハッシュ値が記載されている。

b. 主務省の Web サイトでの公示：認定認証業務の名称、事業者の名称、認定の日付の一覧表が記載されている。

c. 機械可読性が低い上に、過去の履歴を容易に参照できない等の課題が存在する。

(ウ) 認定された特定認証業務から発行された電子証明書の効果が規定されていない。

3.2.2公的個人認証法

調査対象：

・電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成 14 年法第 153 号。以下、「公的個人認証法」という）
・電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行令
・電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則
・認証業務及びこれに附帯する業務の実施に関する技術的基準
・公的個人認証サービス利用のための民間事業者向けガイドライン 1.1 版

（1）特徴

ア. 地方公共団体情報システム機構の認証業務に関する制度等を定めている

イ. 電子署名用と利用者認証用の 2 種類の電子証明書を発行することにより、個人に対するオンライン認証手段（eID means）と電子署名機能の提供を行っている

ウ. 署名検証者等に係る届出、認定に関して規定し、証明書失効情報の利用制限が課され、証明書失効情報にアクセルするために特定認証業務を行う認証局や、署名検証サービスを行う事業者向けに総務大臣による認定制度がある。

エ. 電子証明書の発行番号の利用制限がある

（2）課題

ア. 現在広く用いられている長期署名形式の署名文書には、署名者の電子証明書が格納されているが、電子証明書の発行番号の利用制限により、本来、署名文書を利用する者に署名文

書が渡せない状況がある

イ. 電子署名法との暗号アルゴリズムの不一致（公的個人認証法施行規則 2 条）

ウ. 公的個人認証法施行規則 29 条、みなされた事業者の権利義務が不明確

エ. 電子証明書に関する国際相互承認を考慮した検討が必要である

オ. 国際的な通用性の観点から、UNCITRAL で検討中の「IdM and Trust Services」第 2 章 Identity Management の条項に対する適合性の考察が必要

カ. 諸外国における国民 ID カードの公開鍵証明書の利用制限について調査する必要がある。

キ. 類似した認定基準との共通化の検討を行うべきである

公的個人認証法第 17 条（署名検証者等に係る届出等）には地方公共団体情報システム機構（J-LIS）が管理運営する公的個人認証証明書の失効情報にアクセスし同証明書を用いて署名検証を行う者について以下の 3 つの種別の届出を求めている。

1 項 4 号 認定認証業務(電子署名法 8 条)

1 項 5 号 特定認証業務(電子署名法 2 条 3 項)

1 項 6 号 JPKI の失効情報が確認できる署名検証業務

ここで、5 号、6 号については、政令で定める基準に適合していることを総務大臣が認定する制度となっている。（以下、5 号認定、6 号認定と記す）

(ア) 5 号認定の要件

利用者の真偽確認においては、公的個人認証法施行令第 8 条第 2 号に規定される公的個人認証証明書を用いた署名検証による方法に限定され、また、欠格事項も異なる規定となっているが、それ他の設備基準、運用基準は電子署名法の認定認証業務の要件と同じ規定となっている。

		電子署名法施行規則	公的個人認証法施行規則
利用者の真偽確認	個別	第 5 条（利用者の真偽の確認の方法）	施行令第 8 条第 2 号 公的個人認証証明書を用いた本人確認に限定
欠格事項	個別	第 5 条（欠格条項）	第 26 条 1 号
設備基準	共通	第 4 条（業務の用に供する設備の基準）	第 25 条（特定認証業務の用に供する設備の基準）
運用基準	共通	第 6 条（その他の業務の方法）	第 26 条（特定認証業務におけるその他の業務の方法）

(イ) 6 号認定の要件

6 号認定を受けるものは、公的個人認証証明書に限られるが、署名検証サービス事業者であり本来、トラストサービス事業者としての共通要件を満たすべき事業者であると考えられる。

3.2.3商業登記法及び関連省令等

（1） 調査対象

ア. 商業登記法（昭和 38 年法第 125 号）

イ. 商業登記規則

ウ. 政府認証基盤(GPKI)ブリッジ認証局(BCA)との相互認証業務に関する CP/CPS

（2） 特徴

ア. 関連法制度と商業登記に基づく電子認証制度の位置づけ

商業登記法 12 条の 2 および商業登記規則 33 条の 2～18 の規定により、登記所（法務局）が電子認証局となって、商業登記に基づく電子認証制度を提供している。

イ. 商業登記に基づく電子認証制度の法的効果の有無と定義

商業登記に基づく電子認証制度が前提とする電子署名は、商業登記法の以下の記載により、電子署名法上の「電子署名」の定義を満たしていると考えられる。

(ア) (商業登記法 12 条の 2)電磁的記録に記録することができる情報が被証明者の作成に係るものであることを示すために講ずる措置であって、当該情報が他の情報に改変されているかどうかを確認することができる等被証明者の作成に係るものであることを確実に示すことができるものとして法務省令で定めるもの

商業登記法において、直接的に商業登記電子証明書による電子署名が法人代表者印相当の効果を持つと認めるものでないが、商業登記簿で管理される以下の情報を証明可能な電子署名を施すことができると解釈でき、法的効果があるものと考えられる。

(イ) 法人格の存在

(ウ) 代表権の存在

(エ) 法人代表者としての本人性

商業登記に基づく電子認証制度では、「電子証明書」の有効性（会社の商号、本店、代表者の資格・氏名等の電子証明書に表された事項に変更が生じていないか等）の確認により、登記情報に基づく上記情報をオンラインで確認することが可能であり、これは登記情報を含まない特定認定事業者等の民間が会社等法人に発行した証明書とは異なる機能と考えられる。

ウ. 商業登記認証局の運用管理基準

商業登記に基づく電子認証制度では GPKI との相互運用を行うため、商業登記電子認証局の CP/CPS を定めており、電子署名法が求める電子認証局の認定認証業務の要件と比べ一部異なる要件（【課題】に記載）もあるが、ほぼ同様の要件が示されている。

エ. 商業登記電子証明書の今後の予定

商業登記電子証明書の今後の動きとして、政府「デジタル社会の実現に向けた重点計画(令和 3 年（2021 年）6 月)」にて以下のように言及されている。

(オ) 商業登記電子証明書について、令和３年度（2021 年度）中に無償化の可否

の検討やクラウド化に向けた検討を行い、費用対効果も踏まえつつ、令和 7 年度（2025 年度）までの可能な限り早期に新規システムの運用開始を目指す

（3） 課題

ア. 商業登記電子認証局の認定要件・基準

商業登記電子認証局の CP/CPS は、GPKI との相互運用をするための自主管理基準であり、電子署名法等のような外部の認定機関等が認定するための基準とはなっていない。また、商業登記電子認証局の CP/CPS において、電子署名法で認定認証業務に求められる要件とは異なる要件がある。主なものを以下に示す。

(ア) 認証局は利用者の秘密鍵に関知せず、管理基準を定めていない（PC 上での管理が標準で、IC カード格納はオプション）。

(イ) EE 証明書に keyUsage の記載がなく、鍵の利用目的が明確になっていない。

(ウ) 外部から認定を受けておらずルート機関からの証明書もないため、商業登記電子認証局の自己署名証明書の真正性を法務省 HP に示されるメッセージダイジェスト（ハッシュ値）により検証する必要がある。

イ. クラウド化(リモート署名化)

商業登記電子証明書のクラウド化(リモート署名化)にあたり、将来的な国際連携も加味すると、JT2A リモート署名ガイドライン、欧州 eIDAS/ETSI 等の技術基準に合わせていく必要あると考えられる。

3.2.4電子委任状法

（1） 特徴

電子委任状の普及の促進に関する法律（平成 29 年法第 64 号。以下、「電子委任状法」という）は、委任関係を証明する「電子委任状取扱業務」に関する国による認定制度が規定されている。以下に挙げる同法の固有要件以外は、電子認証局に対する設備基準、技術基準、運用基準が、電子署名法の特定認証業務の認定要件と同様である。

【固有要件】

- 「代理権授与」属性に関する定義が存在。
- 電子委任状に関する「3 種類の記録方法（委任者記録ファイル方式・電子証明書方式・取扱事業者記録ファイル方式（※）」が存在。
- 電気通信事業法の登録に関するみなし規定が存在（電子委任状法第 10 条）
- 電子委任状法第 2 条第 4 項第 1 号において電子署名法・関連法令を参照する規定が存在。
- 電子証明書方式の電子委任状取扱業務の認定要件に、電子署名法に基づく特定認証業務の認定、WebTrust または ETSI 監査の取得が求められている。

【共通要件】

	電子署名法	電子委任状法
【設備基準】 ・入退室管理 ・ネットワーク管理 ・物理的アクセス管理	・電子署名法指針第４条 ・電子署名法指針第５条 ・電子署名法指針第６条	・基本指針(※)第４の２の三
【技術基準】 ・暗号装置 ・災害被害防止措置	・電子署名法方針第２の２ ・電子署名法指針第７条	・基本指針第４の２の二 ※直接暗号装置への言及は無いが、署名法の認定、もしくは WebTrust 監査又は ETSI 監査を受けることで確認される内容と判断。 ・基本指針第４の２の三
【運用基準】 ・証明書ポリシー(CP)及び認証業務規程(CPS) ・運用体制	・電子署名法施行規則第 6 条第 13 号 ・電子署名法施行規則第 6 条第 15 号	・基本指針第４の３の三

(※)基本指針：電子委任状の普及を促進するための基本的な指針をいう。以下において同じ。

（2） 課題

ア. 代理権授与にとらわれない様々な属性（例. 資格属性等）を証明する業務の制度が必要ではないか。

イ. 「代理権授与」以外の様々な属性を、電子証明書等に記載することについてトラストサービス全体で効果を認める必要があるのではないか。

ウ. 属性の確認において「ベースレジストリ」を参照することが考えられる。

エ.　その場合には、ベースレジストリから発出される情報にトラストサービス（例えば e シール）を利用することや、API 等で自動連係が行えることを検討すべきではないか。

（※）電子委任状に関する「3 種類の記録方式」
電子委任状の記録方式として下表の 3 種類が規定されている（基本指針第３の１の二）。

	記録方式名	電子署名対象文書に添付される電子証明書
(1)	委任者記録ファイル方式	受任者の電子証明書（マイナンバーカードに格納された署名用電子証明書、等） 電子委任状を発行するための電子証明書(※)は、委任者の電子証明書
(2)	電子証明書方式	受任者に発行された電子証明書（委任情報が記載） ・認定認証事業者の発行する電子証明書 ・WebTrust 監査制度等を受けた CA から発行された電子証明書
(3)	取扱事業者記録ファイル方式	受任者の電子証明書（マイナンバーカードに格納された署名用電子証明書、等） 電子委任状を発行するための電子証明書(※)は、電子委任状取扱事業者（CA）の電子証明書

※電子委任状（XML ファイルもしくは PDF ファイル）に対して電子署名を実施

3.2.5　民法等における電子文書、電子署名、タイムスタンプの通用性

3.2.5.1 電子文書の通用性

（1）民法等における電子文書の通用性

電子的だというだけの理由で効力を否定しているケースがあるので、これらについて列挙する。

ア.　契約に関する例

民法（明治 29 年法律第 89 号）522 条 2 項に規定する「契約の方式の自由」はあるが、法令による制限は可能となっている。

(ア) 法令による例外で電子化可能なものの例

a.　民法 446 条 2 項、3 項（保証契約）

b.　民法 587 条の 2 第 1 項、4 項（書面による消費貸借契約）

(イ) 法令による例外で電子化不可能なものの例

a.　民法 465 条の 6（事業のための保証には公正証書が必要）

イ.　契約以外の例

(ア) 受取証書(民法 486 条)：現行法では紙の証書(領収書)のみ請求可能。令和 3 年（2021 年）改正により電子的な受取証書の請求が可能になる。

(イ) 遺言書(967 条～970 条)。いずれも書面が必要。

（2） 民事訴訟法における電子文書の通用性

(ア) 民事訴訟法（平成 8 年法第 109 号）231 条で準文書には書証の規定が準用される。準文書は、データそのものではなく媒体等の有形物だと考えられている（ただし、データを対象として文書提出命令を認めた裁判例あり）

→ データ自体が電子文書として認められる方向で、法制審で審議中

（3） 業法等における電子文書の通用性

ア. 業法における書面の電子化

(ア) 多くの業法で紙が不要になっている。

(イ) 令和 3 年（2021 年）改正により、定期賃貸借契約等（借地借家法(平成 3 年法 90 号)22 条、38 条）、重要事項説明書（宅地建物取引業法(昭和 27 年法 176 号)35 条）等が、電子化可能になる（現時点では未施行）。

(ウ) 特定商取引に関する法律（昭和 51 年法 57 号）における訪問販売等の契約時書面、電子的方法による契約撤回も令和 3 年（2021 年）改正で電子化可能となる（現時点では未施行）。

イ. 包括的な規定の必要性

(ア) 包括的に電子化できるという規定がないと、一つひとつ確認する必要があり、利便性を損なう。

(イ) 条例で定めている交付書類等に書面が必要なものがある。このため、業種によっては、新規事業の開始にあたって条例の確認が必要だが、千数百の条例をすべて確認するのは困難であり、事業の推進の阻害要因となりえる。

(ウ) 条例で書面を要求している例（福祉用具の販売・レンタル等）

「横浜市指定居宅サービスの事業の人員、設備、運営等の基準に関する条例」238 条 3 項

- 福祉用具専門相談員は、福祉用具貸与計画の作成に当たっては、その内容について利用者又はその家族に対して説明し、当該利用者の同意を文書により得なければならない。

「札幌市指定居宅サービス等及び指定介護予防サービス等の事業の人員、設備及び運営の基準等に関する条例」274 条 4 項

- 福祉用具専門相談員は、特定福祉用具販売計画を作成した際には、当該特定福祉用具販売計画を記載した書面を利用者に交付しなければならない。

（4） 公的手続における通用性

情報通信技術を活用した行政の推進等に関する法律（平成 14 年法第 151 号。以下、デジタル手続法という)2 条 1 号等により、電子的な手続きが原則とされている。

3.2.5.2 電子署名の通用性

（1）電子署名（電子証明書）を限定している手続の例

商業登記申請において、申請書への申請者電子署名、申請書への代理人署名、添付書類への電子署名に関して、書類の種類ごとに添付すべき電子証明書が限定されている（商業登記規則 36 条、102 条）。使用可能な電子証明書は、具体的に一つひとつ列挙する方法で記載されており、使用可能となる基準については公表されていない。このため、サービス事業者が個々に法務省に申請し、法務大臣の指定を受ける仕組みとなっている。また、登記所に電子データを提出する場合（同規則 36 条）とインターネットによる電子申請の場合（同規則 102 条）で、告示の要否が異なっており、統一性を欠いている。

商業登記申請に限らず、公的機関における使用の可否は、電子署名又は電子証明書のカテゴリにより指定すべきであり、かかるカテゴリは一般的に規定し、場合によっては認定制度に係るものとすべきである。

（2）電子署名法 2 条 1 項の参照

通用性に関して、電子署名法 2 条 1 項を参照しているものが多いが、次の 2 つの問題点がある。

ア. 電子署名法 2 条 1 項には身元確認や方式の安全性についての規定がないこと

同法 2 条 1 項には、利用者の身元確認や同法 3 条かっこ書きに示す安全性についての要件はない。したがって、本人がだれなのかを特定できないもの、安全性に疑問があるものも含んでいる。このような電子署名を要求することは、紙において認印を求めることに相当するものであり、2 条 1 項の電子署名が必要なのか、2 条 1 項の電子署名で目的に対して十分かどうか、等を検討すべきである。

イ. 2 条 1 項と同じ定義を、直接記載している法令がある。利用者にとっては、それらの異同を逐一チェックする必要がある。

ウ. 電子署名法 2 条 1 項と異なる独自の要件を定めている法令も存在する。

エ. 共通的な規格がないため、このような状況が生じているものと思われる。

以下に、上記ア.ないしはウ.の例を挙げる。

a. 電子署名法 2 条 1 項を引用している法令

多数の法令が、電子署名法 2 条 1 項の電子署名を行うことを規定している。

b.　電子署名法によらずに電子署名法 2 条 1 項と同様の定義を行っているもの

電子署名法を参照せずに、電子署名法 2 条 1 項と同様の定義を行っている法令がある。少なくとも 33 の省令がこのような定義を行っている。（例：会社法施行規則 225 条 2 項）

> （電子署名）
> 第二百二十五条　次に掲げる規定に規定する法務省令で定める署名又は記名押印に代わる措置は、電子署名とする。
> （一号～十二号を省略）
> 2　前項に規定する「電子署名」とは、電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。
> 一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
> 二　当該情報について改変が行われていないかどうかを確認することができるものであること。

c.　電子署名に通用性に関する法令独自の規定

手続等で必要となる電子署名について、独自の規定を置いている法令もある。このような規定の例として建設業法（昭和 24 年法第 100 号）がある。同法 19 条 3 項に規定される建設請負契約の電子化にあたっては、同法施行規則 13 条の 4 第 2 項に規定する技術的基準に適合する措置（公開鍵暗号方式による電子署名にほぼ相当）を行う必要がある。この措置については、国土交通省の「建設業法施行規則第 13 条の 2 第 2 項に規定する「技術的基準」に係るガイドライン」に説明があり、これを満たすことが求められている。同ガイドラインに適合するかどうかは容易に判定ができない場合もあり、経済産業省のグレーゾーン解消制度の利用が多数の事業者が個別に利用するに至っている。この他に、不動産登記及び商業登記の電子申請にあたっては、電子署名に係る電子証明書が求められるが、電子証明書の発行機関等について、書類の種類（申請書、委任状、添付書類）ごとに、利用可能な電子証明書のリストを具体的に列挙する方法がとられている。このリストに掲載される基準は公開されていないため、電子署名のサービスを始めようとする者は個々に登録を申請することになるだけでなく、登記の電子申請を行おうとする者にとって見通しが著しく悪いものとなっている。

（3）電子署名の通用性に関する方向性

これらの問題点に鑑みると、認定認証業務の発行する電子証明書に基づく電子署名（たとえば「クオリファイド電子署名」とする）、電子署名法 3 条の推定効が得られるような電子署名(たとえば「特定電子署名」とする)等を定義し、法令からはこれらを参照する方向で検討すべきである。

また、電子署名法 2 条 1 項への適合性、同法 3 条カッコ書きへの適合性について判定する機関はない。このため、同法 2 条 1 項の適合性について経済産業省のグレーゾーン解消制度を使用すること

が多く、この制度が事実上のお墨付きになっている例がある。しかし、同制度は、認定に代わるものではない上に、新規事業についてのみ照会を受け付ける仕組みとなっているため、以前から事業を実施している事業者については判定が行われない等、不公平な実情が存在する。

このような事態に対応するため、共通的な規格を定めるとともに、公的又は民間において適合性を判定する仕組みを構築することが極めて重要である。

3.2.5.3 タイムスタンプの通用性

（1）法令での通用性の例

- 電子帳簿保存法施行規則 2 条 6 項 2 号ロ には、一般財団法人日本データ通信協会が認定するタイムスタンプの使用が規定されている。

（2）確定日付について

- 確定日付を要する手続き（民法 467 条 2 項＝債権譲渡の第三者対抗要件 等）がある。
- 確定日付は、民法施行法（明治 31 年法第 11 号）5 条に定義があり、公証役場で作成するもの（電子公証を含む）と内容証明郵便だけが認められている。

※ 民法施行法 4 条は令和 2 年（2020 年）4 月 1 日施行の改正で削除された。

〔証書作成日に関する証拠力〕
第四条　証書ハ確定日附アルニ非サレハ第三者ニ対シ其作成ノ日ニ付キ完全ナル証拠力ヲ有セス

- かつては、日時に関する証拠を持たせる方法が、5 条に記載のものしかなかった。しかし、情報通信技術の発展により、電子的なタイムスタンプで信頼性の高いサービスが可能となった。
- 国の認定を受けたタイムスタンプには、確定日付の効力を持たせることを検討すべきである。

3.2.6 時刻認証業務の認定に関する規程

3.2.6.1 タイムスタンプ関連規程の経緯

平成 16 年（2004 年）～平成 17 年（2005 年）：民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（平成 16 年法第 149 号。以下 e 文書法という）の施行に備えて、電子記録の真実性を保証する重要性が認識され、平成 16 年（2004 年）11 月 5 日に総務省より「タイムビジネスに係る指針 ～ネットワークの安心な利用と電子データの安全な長期保存のために～」が提示され、平成 17 年（2005 年）2 月に電子文書の存在証明の基準として、上記指針を踏まえ、時刻配信および時刻認証の業務について、技術・運用・設備等の審査基準を満たし厳正に業務が実施されているかの適合性を評価する「タイムビジネス信頼・安心認定制度」が（一財）日本データ通信協会にて創設された。

令和元年（2019 年）～令和 3 年（2021 年）：総務省において「トラストサービス検討ワーキンググループ」が平成 31 年（2019 年）1 月から令和元年（2019 年）11 月まで開催され、令和 2 年（2020 年）2 月に最終とりまとめが提示された。この取りまとめにおいて、現行の認定制度では、民間の認定制度であることと国際的な通用性への懸念から利用者が採用を躊躇することから、国による認

定制度の整備と電子文書の送受信・保存において公的に有効な手段となるよう具体的な制度化が必要であるとされ、具体的に制度検討を進めるべく「タイムスタンプ認定制度に関する検討会」が令和２年（2020 年）３月から令和３年（2021 年）３月まで開催された。

この検討会結果を反映し、総務省はタイムスタンプに係る国による認定制度として、令和３年（2021 年）４月１日総務省設置法のもと、総務省告示第 146 号（時刻認証業務の認定に関する規程）及び時刻認証業務の認定に関する実施要項（令和３年（2021 年）４月１日時点版）を発出した。

告示及び実施要項記載の指定調査機関として、（一財）日本データ通信協会が総務省により、令和３年（2021 年）６月 24 日に指定された。

3.2.6.2 総務省告示 146 号および実施要項の特徴

総務省告示及び実施要項の特徴を以下に記載する。

（1）方式はデジタル署名方式であり、国際的に利用されている基準である RFC3161 及び RFC5816 を指定している。

（2）タイムスタンプの時刻源は、日本標準時通報機関である国立研究開発法人情報通信研究機構が生成する協定世界時 UTC（NICT）を指定している。

（3）認定される事業者は、タイムスタンプと時刻源との時刻差が±1 秒以内となるよう、時刻の品質を管理及び証明する措置を講じることが求められる。

（4）総務省の HP にて、認定事業者及び業務等が公開される。

（5）タイムスタンプ生成に使用する秘密鍵保護装置である HSM が FIPS140-2 レベル３及び ISO/IEC15408（EN 419 221-5）と規定されている。

（6）TSA 公開鍵証明書を発行する認証事業者は、電子署名法の認定認証事業者または WebTrust の認証を取得した事業者であることを基準として指定されている。

（7）民間認定時には認められていなかった時刻認証事業者（TSA：Time Stamping Authority）自ら時刻の信頼を確保する方式が加えられた。

（8）認定の有効期間は２年間である。

3.2.6.3 現状の課題

利用者にとって採用の拠り所であった民間の認定制度が、総務省告示発出によって国の認定制度となり、より安心して利用できる環境は整備された。一方で日進月歩であるデジタル環境の変化への対応等を鑑み、利用者における不信感を払拭し、依拠者にとってより利便性を向上させ安心に利用できる制度とすべく、現時点での課題を下記する。

（1）タイムスタンプの法的効果に関する規程がない。

タイムスタンプは、告示第 2 条において定義されたが、確定日付を要する手続きがあるが国の認定を受けたタイムスタンプであっても利用ができない。

（2）TSA 公開鍵証明書の発行業務の監査に係る制度が無い。

現行の電子署名法では、自然人への証明書であり、組織および組織が管理する装置を証明するための監査に係る制度がなく、法的な根拠が無い。

（3）公開される情報は、機械可読でなく、発行元を証明する処理も施されない。
認定サービスであることの確認において、機械可読と情報の発行元証明措置と完全性担保は、Society5.0 実現には必須の要件である。

（4）タイムスタンプ時刻は協定世界時 UTC（NICT）と 1 秒以内の誤差であることが求められているが、TSA 自ら時刻の信頼を確保する方式において、その検証方法が明確にされていない。
タイムビジネス信頼・安心認定制度では、タイムスタンプの信頼の基である、時刻の保証を ISO-18014-4 に準じ時刻配信局が担っていた。今般の告示により当該時刻配信局が無い状態でもタイムスタンプが発行できることとなったが、付与される時刻そのものの品質基準が明確にされていない。

（5）秘密鍵、電子証明書等の定義がタイムスタンプ発行に限定的であり、トラストサービスで共通定義が必要と思われる。

（6）制度と審査基準が固定化されており、基準の環境対応が困難である。
タイムスタンプ等のトラストサービスは、将来において利用された時点の確からしさを証明するものであり、評価基準は、その透明性や国際通用性が重要である。グローバルな視点での融通性のある仕組みであることが求められる。

（7）総務大臣認定の事業者によるタイムスタンプの利用を推奨・規定する省令・ガイドライン等が未整備である。このため、提供事業者は、場合によっては、2 重での認定を取得する必要があり、過度なコスト負担が求められ、利用者への影響が懸念される。

3.2.7e シールに係る指針

（1）特徴

ア. 総務省が令和３年（2021 年）6 月 25 日に『e シールに係る指針』（総務省）を公表、e シールを「電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み」と定義。

イ. 「我が国における e シールの在るべき姿を示すとともに、e シールの信頼性を担保するために証明機関に求めるべき基準を検討するにあたっての参考とすること」が目的。

ウ. 「e シールに関するより詳細な検討や制度設計については、本指針を踏まえつつも、今後発足する予定のデジタル庁でのトラストサービスの基盤となる枠組みの検討の中で具体化され、ひいては我が国のトラストサービスの整備・発展が一層進むことを期待したい。（同指針「おわりに」から引用）

	個別/共通	電子署名法	e シールに係る指針
申請者の真偽確認	個別	電子署名法施行規則第 5 条	2.3 組織等の実在性・申請意思の確認の方法
電子証明書記載事項		電子署名法施行規則第 6 条第 5 号	2.4 e シール用電子証明書のフォーマット及び記載事項
設備基準	共通	電子署名法施行規則第 4 条	指針には明示されていないが、電子認証局を運営することから電子署名法を準用可能と想定される。
技術基準		電子署名法施行方針第 2 の 2（暗号装置）	2.5.1 認証局の秘密鍵の管理
運用基準		電子署名法施行規則第 6 条	指針には明示されていないが、電子認証局を運営することから電子署名法を準用可能と想定される。

（2）課題

ア. 「一定程度国が関与しつつも、基本的には民間の自主的な仕組み」とされているが、他のトラストサービスと同様「法的効果」を謳い、詳細制度設計が必要である。

イ. e シール用電子証明書を発行する認証局の設備基準、技術基準、運用基準は、電子署名法に基づく特定認証業務の認定基準の見直しと共に検討すべきである。

ウ. e シール用電子証明書を発行する固有な要件として、以下の継続検討が必要である。

- 適合性評価機関に関する基準
- 発行対象の明確化
- 発行対象の真偽確認方法
- 電子証明書プロファイル、組織を特定可能な識別子
- 発行される e シールのレベル、および当該レベル適合基準、等

エ. 法的効果

電子署名法で規定された法的効果（電磁的記録の真正な成立の推定、同法第 3 条）は無い。データ戦略タスクフォース第一次取りまとめ（令和２年（2020 年）12 月 21 日デジタル・ガバメント閣僚会議決定）では、「「事実・情報」：発行元証明自然人、法人や事業所等の「組織」、さらには IoT 時代において爆発的に増大する「機器」が存在するという事実と、当該機器が発行する情報等の信頼性を担保するためには、発行した自然人・組織・機器が信頼できるか、その発行方法が信頼できるのか、当該事実・情報が作成しようとした通りのものか等の証明（発行元証明）が必要である。」とされており、発行元証明に関する法的効果を

規定すべきである。

＜e シールの期待される効果＞

今後、e シールは発行元証明として様々なユースケースでの使用が期待される。

例えば、国際取引等における証憑類に使用する場面においては、当該 e シールについて国際的な整合性を求められることが想定され、行政手続における提出書類等に使用する場面においては、当該 e シールが一定の水準を満たしていることを求められることが想定される。

一方、e シールの普及・利用拡大の観点では、例えば、日常的に企業間でやりとりする資料等に e シールを付与できることに加えて、個人事業主や中堅・中小企業等において e シールを活用する場面においては、低コストで簡便に利用できる e シールのニーズも想定される。

また、EU においては、e シール、先進 e シール、適格 e シールと 3 つの e シールが定められており、用途や e シールの効力に応じてそれぞれの e シールが使い分けられている。

これらに鑑みて、我が国における e シールは、用途や活用場面に応じてレベル分けを行い、利用者自身である程度選択的に e シールを利用できるようなフレームワークにすることが適切だと考えられる。

3.2.8 リモート署名ガイドライン

（1）特徴

リモート署名と電子署名法との関係は、電子署名法研究会の平成 28 年度（2016 年度）報告書に記載されている。リモート署名ガイドラインは、民間の任意団体である日本トラストテクノロジー協議会（JT2A）が作成している（電子署名法の主務省である法務省、総務省、経済産業省は同ガイドライン作成にオブザーバーで参加している）。

（2）課題

ア. 技術要件：同ガイドラインには、利用者認証及び SIC（Signing interactive component：リモート署名サーバと接続する署名者側のソフトウェア）に関する技術要件や管理策は規定されていない。

イ. 評価・認証：同ガイドラインを用いた、評価機関による評価、又は監査機関による監査を実施していなく、同ガイドラインを用いて実際に評価・監査できるか検討が必要である。
（特に、パート 2 は CMVP 又は CC による評価が必要、パート 3 は CC による評価が必要）

ウ. 公的な基準としての位置づけ：民間の自主的なガイドラインであり、公的な基準として認められていないため、準拠への動機が乏しい。

エ. 相互運用性：欧州規格を参照しているが、相互運用のためには技術的同等性の確認が必要である。

オ. e シールへの対応：同ガイドラインは、電子署名を前提に記載しており、組織の中で複数名が同一の署名鍵を扱う可能性のある e シールに関しては未検討である。

同ガイドラインが参照している欧州規格

[1] EN 419 241-1 Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

[2] EN 419 241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

[3] EN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services

3.3 ヒアリング調査(案)

海外との相互承認に向け、その候補として考えられる公的認証基盤である、GPKI、LGPKI、公的個人認証サービス、商業登記に基づく認証制度、及び HPKI の関連法令や技術基準の調査実施に関して内閣官房 IT 総合戦略室と協議の上、今後の実施を検討する。

3.4 ニーズ調査の対象の洗い出し（案）

デジタルトラストを効果的で効率的に社会実装を促進するためには、現在の社会実装状況の的確な把握と課題の抽出、今後必要となる要件の整理が重要である。また、トラスト基盤の仕組みとトラストを期待する利用者・利用組織の二つの視点でニーズを掌握し、経済的合理性を実現することが重要である。

「民間ニーズ」及び「国の制度に基づく手続き」をそれぞれ調査し、血の通ったニーズを抽出する必要があり、調査を実施するうえで上記の考え方でニーズの類型化を掌握することが必要と考えられる。

- 民間のニーズ調査は、法に縛られない幅広い領域における民民業務について、その業務フローや現状のトラスト確認レベル、なぜそのトラスト確認が必要となっているのか等の調査が必要と考えられる。
- 国の制度に基づく手続きのニーズ調査は、関係府省庁への悉皆調査が必要で民間へ義務付けている手続きも含め、法律上なぜ要求しているトラスト確認が必要であるか、また今後どのレベルのトラストが必要となるか等の調査が必要と考えられる。

トラストサービスのニーズを調査するにあたり、トラストサービスのニーズは、以下の 4 つの観点からその必要性を考察しニーズの調査を行っていく必要があると考えられる。

（1）デジタル化政策におけるトラストサービスの戦略的ニーズ
（2）トラストサービス自身のニーズ
（3）トラストサービスの基準のニーズ
（4）トラストサービスの認定のニーズ

ユースケースの調査は民間分野、公共分野でそれぞれの手続きにおいてトラストサービスの通用性が求められる業務を下記の分類に従って調査を行うことが有効と考えられる

3.4.1デジタル化政策におけるトラストサービスの戦略的ニーズ

Society5.0 の実現に向け、ヒト、モノ、システム間での高度な情報連携が進み AI 含めデータの自動連携が社会システムの基盤となり、デジタル経済を支える信頼ある自由なデータ流通（DFFT）が国際社会の中で拡大することが想定されている。社会システムの誤作動リスクを許容レベル以下に抑え、DFFT によるデジタル経済の発展のためにはデータのトラストの実現が不可欠である。

デジタル化による新たなイノベーションを支える戦略的なトラスト法制度の整備が必要と考えられる。

3.4.2トラストサービス自身のニーズ

（1）民間分野

ア. 企業ガバナンスの観点から求められるトラストサービスの利用による経済効果

- 企業活動に伴い、作成、受領する証票書類の真正性を確保することにより得られる経済効果
  対象書類例：商取引に伴う見積書、発注書、請書、契約書、検収書、請求書、領収書等
  対象業務例：発注管理、請求管理、収入管理、会計処理、会計監査、等
- 内部統制管理：文書のデジタル化、真正性確保が求められる統制管理の抽出
- 自動化による効果：デジタルデータの真正性が確保され自動化が進むことによる経済効果
- マクロ視点：書面、押印、廃止にともないトラストサービスを用いた業務の電子化による経済効果　（例　ex.OSS（車両登録のワンストップ）

イ. 産業分野別の個別業務でのユースケース

- 準公共分野別のニーズ調査
  健康・医療・介護、教育、防災、モビリティ、農業・水産業（スマートフードチェーン）、港湾(港湾物流分野)、インフラ（「国土交通データプラットフォーム」を中心とする、データ連携基盤（「連携型インフラデータプラットフォーム」）、 インフラ（「国土交通データプラットフォーム」を中心とする、データ連携基盤（「連携型インフラデータプラットフォーム」）

ウ. 相互連携分野
電子インボイス、契約・決済、スマートシティ

エ. トラストサービスの利用の容易性に関するニーズ
リモート署名、eKYC、ベースレジストリ（法人登記情報、国家資格情報等）から発出される情報の真正性確保や API 化のニーズ等

オ. e. 民間から第三者に提出される証明書（企業調査レポート、在籍証明、資格証明、卒業証明、成績証明、弁護士意見書、監査報告書、….）

3.4.3トラストサービスの基準のニーズ

トラストサービスの信頼レベルを考慮して、今の社会で混乱を起こしている課題領域（立法事実の提示）を調査する必要がある。

（1）現状認識 1

電子署名を利用するサービスにおいて、IAL や AAL の基準が示されないまま利用が進んでいる。例えば、電子署名において、電子署名法 2 条 1 項への適合性、同法 3 条カッコ書きへの適合性について判定する機関が無いことから、以下の 2 つの制度が、利用者が利用にあたり信頼する拠所

のような存在となっている。

ア. グレーゾーン解消制度：

電子署名法２条１項の適合性について事業者が経済産業省のグレーゾーン解消制度を使用することが多く、この制度が事実上のお墨付きになっている例がある。しかし同制度は、認定に代わるものではない上に、新規事業についてのみ照会を受け付ける仕組みとなっているため、以前から事業を実施している事業者については判定が行われない等、不公平な実情が存在する。

イ. 法務省商業登記 HP での個別サービス掲載：

商業登記申請において、申請書や添付書類の電子化において、利用できる電子証明書が限定されている。使用可能な電子証明書は、具体的に一つひとつ列挙する方法で記載されており、使用可能となる基準については公表されていない。このため、サービス事業者が個々に法務省に申請し法務大臣の指定を受ける仕組みとなっている。

限られた利用に関する認可の公的な情報であるが、サービス事業者への事実上のお墨付きとなっている。

（2）現状認識２：

事業者署名型サービス（いわゆる立会人型）による電子契約の海外での判例

クラウドを用いた事業者署名型サービスを利用した電子契約サービスがその利便性から国内外で展開されているが、署名者の意思を証明できず、契約が成立したとはみなされない判例が出ている。

ア. オランダ：「個人役員を保証人としたビジネスローンの電子契約」において、SMS を利用して署名者を特定する方式は、十分に信頼できるものではなく、署名者と保証契約の関係は成立しないとされた事例。

イ. 米国（カリフォルニア）：「個人宅での設備設置における資金調達の電子契約」において、クラウド事業者の電子署名だけでは、個人側が契約に署名したことが立証できなかった事例。

このような事態に対応するため、共通的な規格を定めるとともに、公的又は民間において適合性を判定する仕組みを構築することが極めて重要である。

3.4.4 トラストサービスの認定のニーズ

（1）国際的な相互運用の観点からのニーズ

国際連携の観点では認定制度や法的効果のギャップを埋めないと不利になる。例えば、日本で発行された電子証明書を用いた電子署名やタイムスタンプが国際社会で認められなくなる。

3.4.5 調査例

（1）保険会社での e シールによる費用削減効果

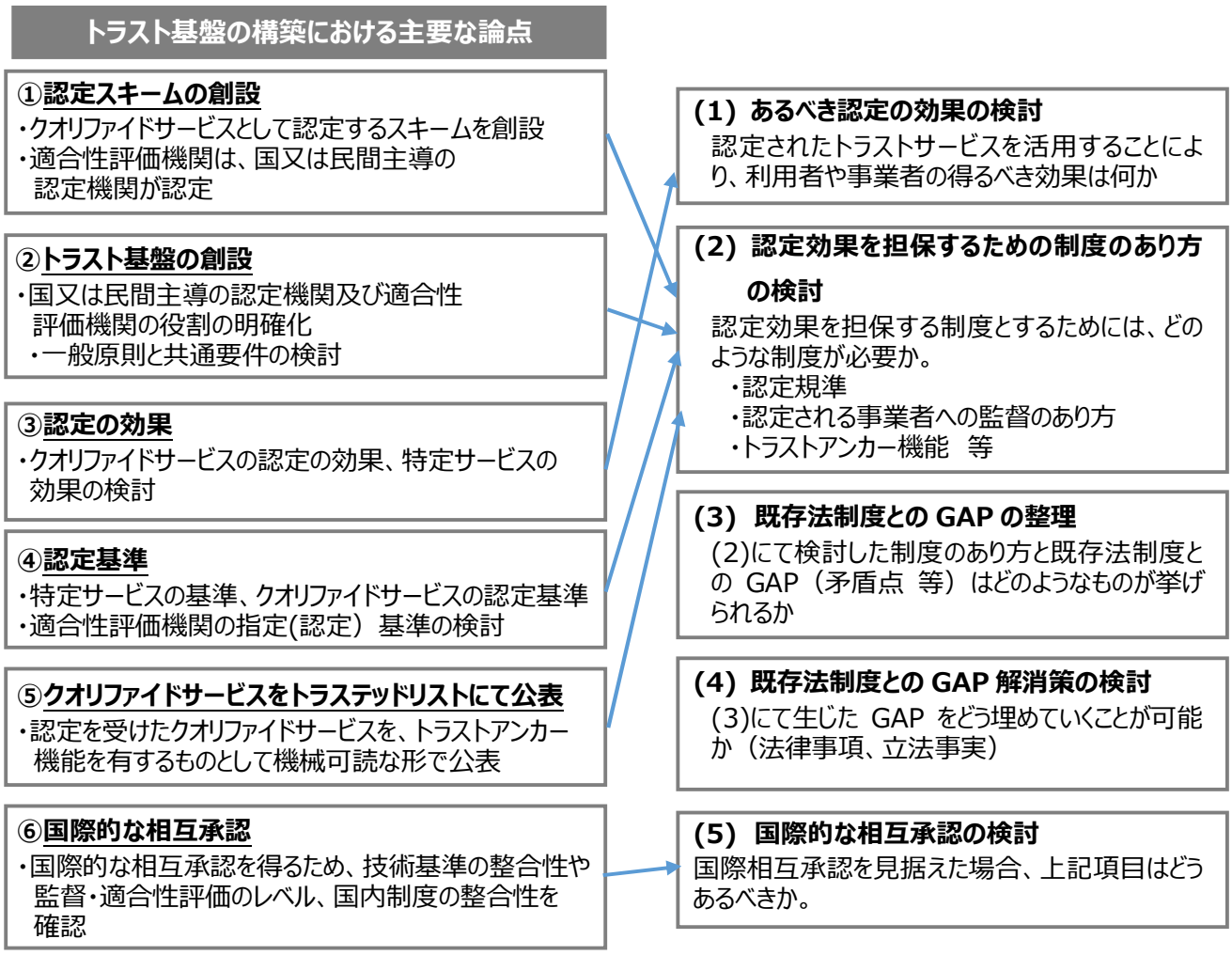
保険会社では、被保険者からの保険金の請求、支払いに係る業務で受領するすべての証票書類（被保険者が受領した請求書、領収書等）をスキャンして業務処理しており、スキャン業務に係る

費用は年間一定程度発生している。これらの証票書類の発出元から e シールを付与する等、すべてデジタルデータの真正性が担保されて受領できれば、スキャニング業務は不要となり受領したデジタルデータをそのまま保存可能となりスキャニング業務に係る費用が削減可能と考えられる。そのような業務例の定量的効果を調査し、外挿することで社会的経済効果を見積もることができると考えられる。

4　日本における包括的なトラストの枠組み整備に必要な論点とその具体的な在り方の調査結果

「データ戦略タスクフォース」にて公表された「包括的データ戦略」の「トラスト基盤の構築に向けた主要な論点と課題」をベースとして、前項「4.2.　国内外のトラストに係る取り組み動向及び課題の調査」で得られた成果物をもとに、日本における包括的なトラストの枠組み整備に必要な論点とその具体的な在り方を、下記の図 4-1.の通り、項目を分類して調査する。

図 4-1．トラスト基盤の構築における主要な論点



※データ戦略タスクフォース（第 7 回）資料より

なお、本調査結果に基にして、更に、トラストサービスに関する「民間ニーズ」及び「国の制度に基づく手続き」をそれぞれ調査し、血の通ったニーズを抽出していくことが求められる。

4.1　あるべき認定の効果の検討

認定されたトラストサービスにどのような法的効果があると社会全体のデジタル化の推進に効果的に寄与できるか検討を行う。現行の法制度のもとでは、トラストサービス（トラストサービスによって生成されたデータを含む。以下、本章において同じ。）、とりわけ認定されたトラストサービスの手続等における通用性（電子文書の有効性が認められるために、どのトラストサービスが必要か、等）は諸法令において個別的に規定されており、国民は、手続ごとに個々に対応せざるを得ない状況にある。一方、民事訴訟における効力については、電子署名による真正な成立の推定規定があるが、それ以外の効力は裁判官の自由心証に委ねられている。このような現状は、トラストサービスの法的効果についての不確実性が大きく、これが、トラストサービス利用を国民が躊躇する要因の一つとなっている。こうした状況を改善するため、法的効果を明文で規定していくことが必要であると考えられる。

4.1.1法的効果の分類

トラストサービスの法的効果を考えるにあたって、法的効果を以下の２種類に分類して検討する。

（1）トラストサービスの通用性

（2）トラストサービスの民事訴訟における効力

このうち、(1) 通用性は、公的手続における通用性（許容性）のみならず、法令により保存・作成・交付等が求められる民間文書や、民間取引における通用性も含むものとする。

4.1.2通用性

（1）通用性に係る問題点

現在、法令に基づいて公的機関に提出する書面及び保存・作成・縦覧・交付等を行うべき書面の大部分は電磁的記録で代えられることになっている。しかし、書面のすべてが電磁的記録で代替できるわけではなく、実際に、書面が要求されるものも残っている（公正証書、遺言書等。民間の契約においても、民法 465 条の 6 に規定される事業のための貸金等に係る保証契約の意思表示には公正証書が必要。）。この点、EU の eIDAS や米国の Esign Act 等においては、電子的であることだけを理由に法的効力や通用性を否定してはならない旨が規定されている。わが国においては、このような包括的な規定がないため、個々の法令及び e 文書法等の法令にあたって確認する必要があり、電子化の進展の阻害要因となっている。

電磁的記録で代えられるものについても、電子署名や電子証明書の要件が付されているものが多い。たとえば、電子署名については、前述（3.2.5.2 電子署名の通用性）のように、電子署名法 2 条 1 項を参照するもの、同項とほぼ同内容の規定を置くもの等がある他、独自の規定をおいているものも少なくない。

（2）通用性の指定のあるべき姿

このような現状に鑑みると、電磁的記録の通用性に関して、具体的な要件を法定し、これを参照する

方法が望ましいといえる。ただし、電磁的記録の内容や用途等に鑑みると、単一の基準ですべての電磁的記録に対応することは困難であるから、複数のレベルを設けて、目的に応じて適切なレベルを要件とするべきである。レベルの設定は、例えば

レベル１（無印） 電子署名、電子証明書、タイムスタンプ 等

レベル２（特定） 特定電子署名、特定電子証明書、特定タイムスタンプ 等

レベル３（クオリファイド） クオリファイド電子署名、クオリファイド電子証明書、クオリファイドタイムスタンプ等

のように設定し、各レベル記載のトラストサービスについて、その定義・要件等を規定する方法をとる。

個別の法令では、トラストサービス又はそのレベルを参照して要件を規定するとともに、これらと異なる要件の個別法令での規定を避けるべきである。これにより、国民は、共通的なトラストサービスの要件に照らして、個々の文書の通用性を判断することができるようになり、不確実性を大きく減少させることができる。

4.1.3民事訴訟における効力

トラストサービスが関与して作成されたデータ（電子署名、タイムスタンプ等）の信頼性は、民事訴訟における効力によりもたらされるものである。EU の eIDAS においては、適格トラストサービスについて、民事訴訟での推定効を規定している他、適格でないことをもって効力を否定してはならない旨を定めている。我が国の法制度においては、一定の要件を満たす電子署名について真正な成立の推定が認められている（電子署名法 3 条）が、それ以外のトラストサービスについては、民事訴訟における効力は規定されていない。

トラストサービスの民事訴訟における取り扱いは、裁判所の自由心証（民事訴訟法 247 条）への影響という形でのみ機能している。クオリファイドトラストサービスについては、裁判所が高い信用性を認めるものと期待されているものの、個々の訴訟における判断には不確実性が残っている。この不確実性が、書面の電子化やトラストサービスの利用をためらわせる一要因となっている。また、海外の裁判所での裁判において、明文の規定による効力を示すことができないため、国際間の取引への利用についての不確実性が大きい。-

包括的なトラスト基盤の構築にあたっては、トラストサービス、特にクオリファイドトラストサービスについて、民事訴訟における効力を明記し、その利用を促進することが極めて重要である。以下では、個々のトラストサービスのあるべき効力について、示すこととする。

(1) 認証局及び電子証明書

現行法では、認証業務（電子署名法 2 条 2 項）、特定認証業務（同条 3 項）及び認定を受けた特定認証業務（同法 4 条以下。本章において以下「認定認証業務」という。）が規定されているが、特定認証業務又は認定認証業務であることによる効力の規定はなく、これらが発行した電子証明書についての規定もない。また、地方公共団体情報システム機構（以下「J-LIS」という。）が発行する署名用電子証明書（公的個人認証法３条。以下「JPKI 署名用電子証明書」という。）及び利用者

証明用電子証明書（同法 22 条。以下「JPKI 利用者証明用電子証明書」という。）、法務局が発行する法人代表者等の電子証明書（商業登記法 12 条の２。以下「商業登記電子証明書」という。）、GPKI 及び LGPKI が発行する政府及び地方公共団体の官職の電子証明書（双方をあわせて、以下「官職電子証明書」という。）並びに HPKI が発行する電子証明書(以下「HPKI 電子証明書」という。）についても、その効力は規定されていない。

認定認証業務、JPKI 署名用電子証明書、商業登記電子証明書、官職電子証明書又は HPKI 電子証明書（これらを総称して、以下「クオリファイド電子証明書」という。）に基づく電子署名データ（電子署名が行われたことを示すために作成され、電子文書に関係づけて記録された情報をいう。）が電子文書に付されている場合には、当該電子文書に対して、電子証明書記載の主体が電子署名を行ったことを推定する規定を置くべきである。これは、押印に関するいわゆる二段の推定の一段目（印影からの押印行為の推定）に相当する（電子署名データから電子署名を推定する）ものであるとともに、電子証明書記載の主体による電子署名であることの推定を規定して、認定認証業務（又は、それと同等の信頼性を持つ機関による発行業務）による電子証明書の法的効力を明確にするものである。なお、電子署名法３条の推定（電子署名による、電子署名の対象たる電磁的記録の真正な成立の推定）が二段目の推定に相当する。

認定を得ていない特定認証業務が発行した電子証明書については、当該特定認証業務における電子証明書発行手続等が正当に行われたことを証明した場合に、認定認証業務による電子証明書と同様に扱う旨の規定が必要と考える。この点について、以下、検討を進める。

クオリファイド電子証明書については、上記のとおり、一段目の推定（電子署名データからの電子署名（措置）の推定）の効力を認めるべきであるが、特定電子証明書については、直ちに一段目の推定を認めるのではなく、電子証明書記載の本人と電子署名の実行者の同一性が認められれば一段目を推定するという考え方をとるべきである。このためには、電子証明書発行時の身元確認及び公開鍵又は秘密情報等（電子署名法 3 条カッコ書きにいう符号及び物件等）の受け渡しの正当性を証明することとなる。実際には、特定認証業務による管理の安全性や、証明への協力（情報提供、証言等）等が重要な要素となると考えられる。

電子署名と同様に、e シールについても、クオリファイドな発行機関に係る電子証明書については、このような電子証明書に基づく e シールデータ（e シールが行われたことを示すために作成され、電子文書に関係づけて記録された情報をいう。）が電子文書に付されている場合には、当該電子文書に対して、電子証明書記載の主体に係る者により e シールを行ったことを推定する規定をおくべきである。

なお、海外の電子証明書との対応関係の整理や相互承認のためには、上記クオリファイド電子証明書を、EU における適格電子証明書等と対応させて検討するべきである。

（2）電子署名

一定の要件を満たす電子署名が行われている場合に真正な成立を推定する現行の規定（電子署名法 3 条）の枠組みは、維持するべきだと考える。

なお、推定の前提である「本人による電子署名が行われた」ことを直接に証明するのは困難であると思われるため、電子署名データの正当性を基礎づける電子証明書に基づいて、その電子証明書の信頼性に応じた推定が得られるように規定すべきである。これは、前節に述べた通りである。

（3）e シール

クオリファイド e シールについては、発行元（電子証明書の主体たる法人等）の真正と、e シールが行われた以降の非改ざん性を推定する規定を置くべきである。なお、e シールデータから、e シールが行われたことの推定については、(1)記載の通りである。

（4）リモート署名

クオリファイドリモート署名業務を用いて行われた電子署名及び e シールは、本人の意思により行われたものと推定する規定を置くべきである。なお、(2)及び(3)記載の推定を得るためには、本人の身元について証明する必要があり、(1)記載の方法その他の方法で証明することになる。

（5）電子署名データ生成装置（Signature Creation Device）

電子署名データ生成装置の法的効力については、議論すべき点が残っている。我が国の既存法制度では、電子署名データ生成装置の利用は、真正な成立の要件になっていない。しかし、リモート署名業務を利用して行われた電子署名の場合には、リモート署名業務における処理の正当性が必要になる可能性がある。これらの点については、(12)で述べる。

（6）属性証明つき電子証明書

法務局、HPKI、又は クオリファイド電子委任状取扱事業者により、電子証明書等に記載された属性情報（クオリファイドの対象となる情報に限る）が存在する場合には、当該電子証明書等の主体がかかる属性を持つことを推定する規定を設けるべきである。

これら以外の属性についても検討が必要である。一つは、士業等の国家資格である。このような資格は、一般的に、士業の全国組織で名簿を管理している。こうした名簿に基づいて記載された資格情報について効力を検討すべきである。

また、3 情報以外の属性情報について、現在は認定認証業務の認定対象とならない（電子署名法施行規則 6 条 8 号）が、一定の属性については認定対象として認めて、電子証明書記載の 3 情報と同様の効力を持たせるべきである。

（7）タイムスタンプ

クオリファイド時刻認証業務によるタイムスタンプ（以下「クオリファイドタイムスタンプ」という。）には、タイムスタンプトークン記載の時刻の正確性及び対象たる電子文書の非改ざん性を推定する規定をおくべきである。

これに加えて、クオリファイドタイムスタンプには、民法施行法 5 条に規定される確定日付の効力を認め

るべきである。

（8）検証業務

クオリファイド検証業務による検証結果（検証結果レポートに当該サービスの e シールが付されたもの）に記載の内容が正確であることを推定する規定を置くべきである。

現行法では、公的個人認証法 17 条 1 項 6 号の認定を受けた者が、委託を受けて JPKI 署名用電子証明書及び同利用者証明用電子証明書の有効性確認を行うことが可能となっており、検証サービスの一部を担っていると評価できる。しかし、このような認定を受けた者が発行した有効性確認結果についての法的効力の規定はない。

（9）電子内容証明送付（registered e-delivery）

クオリファイド電子内容証明送付業務（日本語名称は要検討）に係る通信については、送信者の真正、受信者の真正、通信内容の非改ざん性、受信時刻の正確性を推定する規定を置くべきである。

なお、電子内容証明送付業務は、電子取引情報の授受システム等、広範な利用が予想されているため、すみやかに制度として確立する必要がある。

（10） 電子認証

JPKI 利用者証明用証明書に基づいて利用者認証を行った場合には、この認証と一体となって行われた一連の処理については当該証明書の本人に係るものであると推定する規定を置くべきである。JPKI 利用者証明用証明書以外の証明手段、たとえば、gBizID プライム により認証が行われた場合等、安全な eID means（日本語名称は要検討）による利用者認証についての規定を置くべきである。また、民間が発行する eID means についてクオリファイド等の規定をおく必要もある。

（11） 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

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（以下「事業者型電子署名」という。）については、2 通の三省Ｑ＆Ａにより、電子署名法 2 条 1 項の電子署名にあたりうること、電子署名法 3 条の推定が得られうることが示されている。

ここでは、推定を得るための条件等について、検討する。まず、サービス提供事業者が行うデジタル署名により、サービス提供事業者が記載した内容（利用者が特定した情報に対して利用者の指示によりデジタル署名を行ったこと）についてのサービス提供事業者に係る真正な成立の推定は得られる（ただし、かかるデジタル署名の主体が自然人ではなく組織やサーバの場合には、デジタル署名であっても電子署名ではないので、そもそも電子署名法の対象外である）。この推定は、サービスが記載した内容の真実性を保証するものではない（これだけでは、利用者が指示したこと等を証明できるものではない）。すなわち、利用者に関する真正な成立のためには、デジタル署名の安全性を含むプロセス（サービスによる利用者の認証等のプロセス及びサービス内部のプロセス）の安全性が必要となる。この点は、上記三省

Q&A にも記載の通りである。このような安全性及び利用者の身元確認手続を確認する仕組みとその基準を策定し、一定の水準を満たすものとして認定を受けたクオリファイド事業者型電子署名サービスを用いた場合、かかる電子署名については真正な成立の推定を認めることができると思われる。ただし、厳格な身元確認を行うとすると、迅速な利用開始等の、現在の事業者型電子署名が持つ利点が失われ、利用者本人に対する電子証明書の発行による方法に比べて優位性がないものになることを考えると、このような認定制度は実際には利用されないことも考えられるため、特定レベルの規定にとどめることも考えられる。

なお、事業者型電子署名は、公証人等の資格のある者が行うものではないので、いわゆる公証にはあたらない（たとえば、対象情報の真実性等に踏み込むものではない）ことを、利用者や Relying Party に周知する必要がある。

（12） 電子署名データ生成装置及びリモート署名業務と真正な成立の推定の関係について

ア. 問題点の所在

安全な電子署名データ生成装置での署名鍵の管理について、その法的位置づけを検討する。なお、以下では電子署名について述べるが、e シールについても同様である。

本人が署名鍵を管理している場合、本人が意識的に他人に利用させたとき又は管理の方法がずさんなために他人に署名鍵を使用されたときには、この事情について善意無過失の第三者に対しては、本人による電子署名でないことを対抗できないものとすべきである（民法 110 条又は同条の類推適用）。署名鍵の管理は、本人の責任であり、 Relying Party は管理の厳格さに関与するべき立場にないからである。

この点に関して、リモート署名事業者による署名鍵の管理をどのように位置づけるか、という問題がある。リモート署名の場合には、Relying Party は、リモート署名事業者が本人の署名鍵を管理していることを知っている可能性がある。そうすると、何らかの事情で本人以外の者により電子署名が行われた場合に、Relying Party が善意無過失だと言えるかどうかには疑問がある（他人に署名鍵を委ねていることについては知っている場合、単純には善意と断言できない）。たとえば、リモート署名業務がクオリファイドであれば、本人の意思によってのみ電子署名が行われると Relying Party が信じることには正当な理由がある（本人以外の者が電子署名したとしても、その事情について善意無過失）といえる。つまり、リモート署名については、電子署名データ生成装置とは異なり、リモート署名業務のレベルが問題になるといえる。

このように考えた場合には、電子署名データ生成装置の利用の有無は、電子署名の効力（推定効）に影響するべきではない。

ただし、クオリファイド電子署名データ生成装置に関する規定を持つ外国との取引のため、クオリファイド電子署名データ生成装置の使用について、電子証明書等に記載することを可能にすべきである（かかる記載は、我が国においては特別な効力を示すものではないが、海外において効力を持つ可能性がある）。

イ. 電子署名データ生成装置とリモート署名の比較

以下では、電子署名データ生成装置とリモート署名との比較（特に真正な成立の推定の可否）について、詳述しておく。電子署名法 3 条の推定の効力（本節において以下「推定効」という。）を得るためには、「本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）」が行われている必要がある。

クオリファイド電子証明書等により、公開鍵の本人性が証明されている状況（対応する秘密鍵が本人のものであることが証明されている状況）において、電子署名が、本人によるものであることについて、その条件を考える。

ローカル署名の場合には、我が国の法制度では、3 条カッコ書きの要件（本節において以下「固有性」という。）は、デジタル署名のアルゴリズムだけが問題であるとされてきた。つまり、署名鍵の保管方法や署名プログラムの管理方法等は、推定効に影響を与えないものと考えられてきた。これは、固有性の要件が、符号・物件を適正に管理したとすれば他人には電子署名ができない、というもの（仕組みの安全性の問題）であって、実際の適正管理の有無は問うていないためである。ローカル署名においては、符号・物件の管理は署名者の問題であり、relying party の関与するものではない、ともいえる。

仮に、ローカル署名において、何らかの原因（秘密鍵の意図的な提供、管理上のミスによる漏えい等）で本人以外の者による電子署名が行われた場合について考える。本人の印章を使って本人の意思によらずに手形に押印したケースでの判例（最判昭 43・12・24 民集 22－13－3382）は、民法 110 条(権限外の行為の表見代理)の類推適用により、本人の意思によらない押印であることに関して善意無過失の第三者は保護される（かかる第三者に対して、本人は自分の意思でないことを主張できない）旨を示している。ローカル署名で本人の意思によらない電子署名が行われた場合、一般的には relying party はこの事情を知らないし、署名対象文書の記載が異常なものである等の特段の事情がない限り、知らないことについて無過失だと考えられる。

したがって、ローカル署名の場合には、一般的には、クオリファイド電子署名データ生成装置の使用の有無にかかわらず、真正な成立の推定が得られるものと考えられる。もちろん、署名者が秘密鍵の保護のためにクオリファイド電子署名データ生成装置を用いることはありえるが、これは署名者が自分の権利を守るための措置であって、推定効の有無にかかわるものではない。

リモート署名についても、ほぼローカル署名と同様に考えられる。ただし、一つ異なっている点は、relying party が、署名者がリモート署名を用いていることを知っている可能性があることである（署名者と relying party が同じ電子契約システムを利用している場合等が、これに該当する）。この場合、そうすると、relying party は、少なくとも署名者が秘密鍵の管理を他者に委託していることを知っているため、ローカル署名の場合のようには、無過失とは認められないものと思われる。

そうすると、relying party は、「本人の意思によらない電子署名が行われない」と信じるに足る正当な理由を必要とすることになる。たとえば、リモート署名サービスがクオリファイドであれば、本人の意思によらない電子署名ができない、と信じるに足る正当な理由になるだろう。他にも、無過失を証明する方法はあるだろうが、トラストサービスとしてこれを保証するためには、リモート署名サービスの認定制度を設けることがふさわしいものと考えられる。

ウ. 電子署名生成方式等の表示

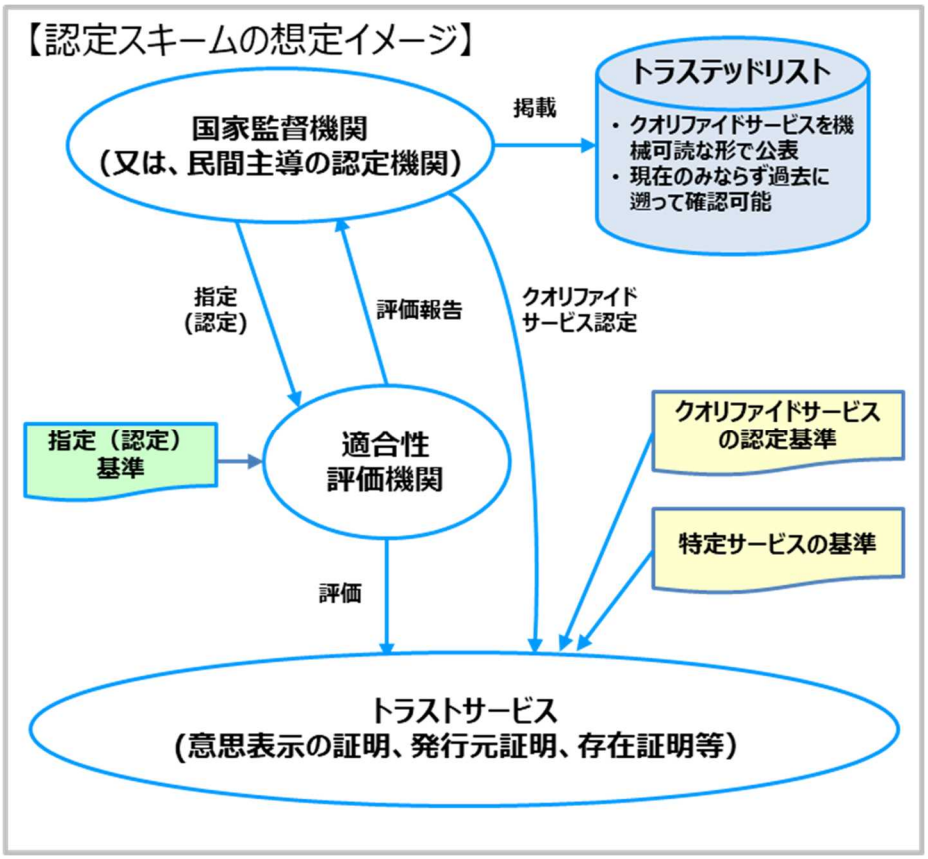
以上の考察によれば、relying party は、受領した電子文書に行われた電子署名について、それがローカル署名によるものか、クオリファイドのサービスによるリモート署名によるものである場合には、推定効を得られることになる。ここで問題となるのは、relying party は、電子署名がローカル署名によって行われたのかリモート署名によって行われたのか、リモート署名の場合にはリモート署名サービスがクオリファイドなのか否か、を知る必要があるということである。

Relying party が、これらの情報を得るためには、電子証明書又は電子署名データに、ローカル／リモート、リモート署名サービスの名称を記載することを義務付け、実際の措置と異なる内容を記載することを禁じる必要がある(たとえば、何の印もなければ、Relying Party はローカルだと信じてもよい、という制度が考えられる)。なお、電子証明書に記載する方法を採る場合には、電子証明書発行時に指定した方法以外での使用（ローカル署名で使用するとして電子証明書の発行を受けた後で、秘密鍵をサーバに預けてリモート署名を実施する等）を禁止する必要がある（クオリファイド電子署名サービスは、証明書に当該リモート署名サービスを利用することが書かれていない電子証明書に基づく電子署名を扱ってはならない、とする等の施策が考えられる）。

4.2　認定効果を担保するための制度のあり方の検討

データ戦略タスクフォース（第７回）の 資料 8-1「包括的データ戦略（案）の概要」で示された認定スキームの想定イメージを基に、認定されたトラストサービスの効果を担保する制度のあり方を検討し、各種規定類の概要とそれらの関係を構造化した。

図 4-2. 認定スキームの想定イメージ



出典：データ戦略タスクフォース第７回（令和３年（2021 年）５月 26 日）の
資料 8-1「包括的データ戦略（案）の概要」より抜粋

上図 4-2.を基に分析すると、トラストサービスの認定制度においては、トラストサービスを提供する事業者（以下「トラストサービス事業者」という）、トラストサービスを監督する機関、トラストサービスの適合性評価のための基準を策定する機関、トラストサービスの適合性評価を実施する機関の４つの主体（プレイヤー）が存在する。これらの主体の必要性及び役割等について、以下の通り分析した。

4.2.1 認定制度における各主体の役割

（1）トラストサービス事業者

我が国においては、電子証明書やタイムスタンプの発行等のトラストサービスの提供を規制する法律はなく、誰もがトラストサービスの提供を業として営むことが可能である。上図の「包括的データ戦略（案）

の概要」で示された認定スキームの想定イメージは、強制的なものではなく、あくまで任意の仕組みであるべきと考えられる。

近年、電子契約サービス等の普及を背景にして、電子署名等のトラストサービスの利用者がその信頼性の確保を求める一方で、トラストサービス事業者にとっても、自ら提供するトラストサービスの信頼性を確保し、対外的に示すことに対するニーズは高まっている。我が国では、EU 等諸外国に比べて、個々のトラストサービスの信頼性を評価するための基準（いわば物差し）の整備が遅れており、トラストサービス事業者の中には、WebTrust 監査等海外の基準への適合性評価に対して高額の評価料金を支払うケースも散見される。したがって、トラストサービス事業者は、国内での任意の認定制度の構築による便益を享受できると考えられる。

なお、認定制度の運営、改善に当たっては、トラストサービス事業者による意見を集約して、適切に反映させる仕組みを検討すべきである。

（2）監督機関

EU の eIDAS 規則においては、加盟国は国家監督機関を設置し、トラストサービス全体の監督を行うとともに、クオリファイドサービスについてトラステッドリストに掲示することが義務付けられている。

我が国においては、電子署名法に基づく特定認証業務の認定や総務大臣告示に基づく時刻認証業務の認定が存在する一方、認定を受けていないトラストサービスに対する国の監督は存在しない。また、国は、認定を行った特定認証業務等を官報等で公開するのみであり、機械可読のデータ形式での開示を実施していない。

今後の国内での認定制度の構築においては、電子署名やタイムスタンプのみならず、多種多様に広がりつつあるトラストサービスを監督する機関（以下「監督機関」という）を設置し、クオリファイドトラストサービスの認定及びトラステッドリストの公開・運営を行い、認定制度全体の企画立案をさせるべきである。具体的には、監督機関は、諸外国の実例を参考にしつつ、トラストサービス事業者のニーズ、適合性評価機関のあり方等を踏まえ、制度全体を改善させる責任を有する。

なお、国（デジタル庁等）が監督機関の役割を果たすのか、国が運営に関与する機関（独立行政法人等）に監督機関の任務を委ねるかについては、更なる検討が必要である。

（3）トラストサービスの公的な基準を策定する機関

国内のトラストサービスのうち特定トラストサービス及びクオリファイドトラストサービスの基準を策定する機関の設置は不可欠である。EU では、eIDAS 規則に基づくトラストサービス（Qualified and Advanced）の基準は、主に欧州標準化機関の一つである欧州電気通信標準化機構（ETSI）により作成されていること、米国では、主に連邦政府の調達基準として用いられるセキュリティ関連文書（Federal Information Processing Standards, Special Publication 800 series, etc.）が米国標準技術研究所（NIST）により発行されていること等を考慮すると、我が国としても、これらの先例を参考にし、我が国の法制度等に紐づいたトラストサービスの公的な基準を策定する機関を設置すべきである。

なお、国（デジタル庁等）が直接的に公的な基準の策定作業が行うのか、民間の標準化団体等を活用して、日本産業規格（JIS）にし、ISO/IEC の国際標準化の場に参画していくのか、あるいは、これらを適切に組み合わせるのか、様々な選択肢の中から、官民のコスト負担のあり方等を考慮しつつ、検討する必要がある。

（4）適合性評価機関

欧米諸国においては、トラストサービスの基準への適合に関する評価は、専ら適合性評価活動を業として営む民間の適合性評価機関によって実施されている。このうち EU 加盟国においては、eIDAS 規則に基づき、各国の認定機関によって認定された適合性評価機関が行った評価結果をとりまとめた適合性評価報告書を基に、国家監督機関がクオリファイドサービスをトラステッドリストに掲載している。

我が国の電子署名法に基づく特定認証業務や総務大臣告示に基づく時刻認証業務の認定においては、国は、国以外の者（以下「指定調査機関」）を指定して、当該業務が行われている現場を調査させ、その調査結果を基に認定の可否を決定している。したがって、評価の主体及び認定の主体は、いずれも国であると位置づけられる。このうち、電子署名法に基づく指定調査機関は、特定認証業務の認定をとる事業者、業務の数が少ないことから、収支面で調査を行う最小限の要員しか配置できず、調査に係る営業活動を実施していない、いわば認定の調査申請を待つ姿勢である。かつ、電子署名法施行規則等に基づく調査項目がチェックリストとして長年固定化していることから、市場ニーズに対応した評価技能の向上を図る動機を持ちにくい。

したがって、クオリファイドトラストサービスの認定においては、電子署名法の指定調査機関の仕組みを改め、認定の主体である監督機関と、適合性評価の主体である民間の適合性評価機関の間の責任を分離すべきである。

また、適合性評価機関が満たすべき基準の策定及び当該基準に基づく中立・公正な機関による適合性評価機関の認定（accreditation）の仕組みについても検討する必要がある。ちなみに、EU においては、トラストサービスの適合性評価機関は、ISO/IEC 17065「適合性評価-製品、プロセス及びサービスの認証を行う機関に対する要求事項」及び ETSI EN 319 403 Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers に適合すべきとされている。なお、欧州各国毎に設置されている認定機関（Accreditation Body）が、これらの基準への適合を審査した結果に基づき適合性評価機関を認定し、欧州認定協力機構(EA:European Cooperation for Accreditation)の枠組の下、欧州域内での相互承認（Mutual Recognition Agreement:MRA）を実現している。

4.2.2 認定制度の具体的なプロセス

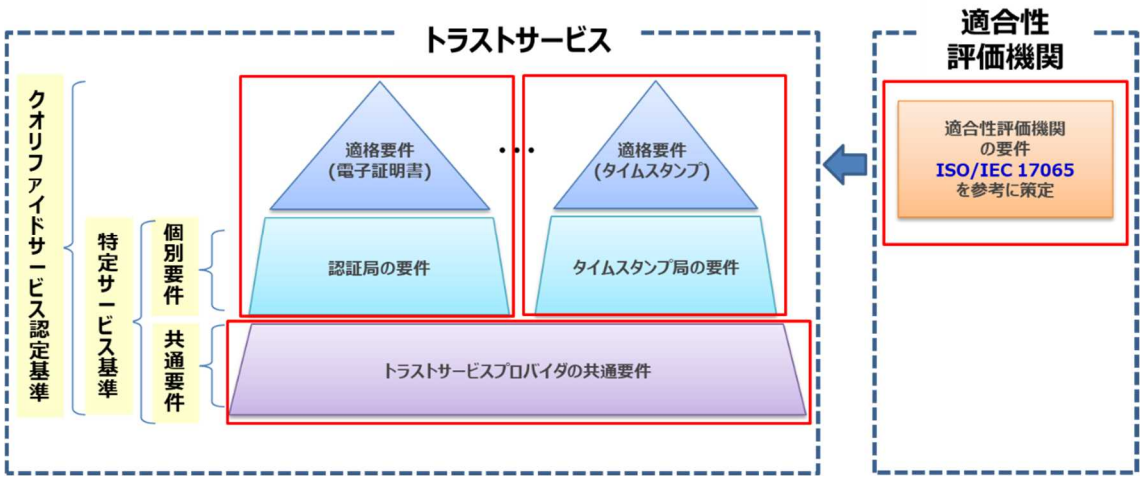
上記の役割分担の下、トラストサービスの利用者、トラストサービス事業者等のニーズに応じて、以下のような具体的なプロセスが想定される。

（1）クオリファイドトラストサービスの認定基準、特定トラストサービスの基準の作成

トラストサービスの公的な基準を策定する機関は、特定トラストサービスの基準を作成し、それに一定の基準を加えてクオリファイドトラストサービスの認定基準を作成する。これらの基準には、当該トラストサービスの定義、技術基準、真偽確認方法、設備要件、業務運営要件等を含むものとし、諸外国との整合性や最新技術動向を踏まえつつ、共通要件と個別要件、適格要件を体系化したものを作成し、公開する。

また、国内の適合性評価の結果の国際的な同等性を確保する観点から、適合性評価機関自体が満たすべき要件については、ISO 等国際標準の準拠した国内の基準を作成し、公開する必要がある。

図 4-3. クオリファイドトラストサービスの認定基準、特定トラストサービスの基準、
そして適合性評価機関との関係



出典：トラストに関するワーキングチーム第 3 回（令和 3 年（2021 年）5 月 18 日）の
資料 3「トラストの枠組みに関するとりまとめ(案)」より抜粋

（2）適合性評価機関による評価

民間の適合性評価機関は、(1)で作成された基準に基づき、トラストサービス事業者からの評価ニーズに沿った特定トラストサービスの評価を行うとともに、当該事業者がクオリファイドトラストサービスの認定を受けたい場合には、クオリファイドトラストサービスの認定基準への適合性を評価した後、適合性評価報告書を作成して、当該トラストサービス事業者に提供する。

当該トラストサービス事業者は、当該適合性評価報告書を監督機関に送付し、クオリファイドトラストサービスとしての認定の申請を行う。

(注) 現行の電子署名法においては、指定調査機関は、国が本来行う実地調査の代行を行い、調査報告書を国に提出することにより、その任務は終了するので、当該調査報告書を調査対象となった認証事業者に提出することはない。

（3）監督機関による認定及びトラステッドリストへの登録

トラストサービス事業者が提出した適合性評価報告書を基に、クオリファイドトラストサービスとしての認定の是非を決定し、認定証を発行するとともにトラステッドリストに登録する。さらに、登録したクオリファイドトラストサービスについて、深刻なインシデントが発生した場合等において、適切な調査及び指導を実

施し、改善の余地がない場合は、クオリファイドトラストサービスとしての認定を取り消す。

4.2.3 認定制度における各種規定類の構造

認定制度を公正かつ安定的に運営するためには、制度の目的、定義及び一般原則を定めるとともに、4.2.1 で示した各主体の役割等を明示し、制度に必要な各種の規定類を作成する必要がある。

各種規定類の概要とそれらの関係を構造化すると、以下の通りとなる。

（1）トラストサービスに共通な事項

電子証明書やタイムスタンプの発行等様々なトラストサービスに共通する事項として、制度の目的、共通な用語の定義、一般原則としての監督、責任、通用性、ID スキーム、表示（マーク）等とともに、トラストサービス事業者の要件等で技術中立的な部分や、適合性評価機関の満たすべき要件、トラストサービスの公表（トラステッド・リスト、相互認証）に関する事項を定める。

（2）各トラストサービスに関する個別事項

トラストサービスによって提供される電子署名、タイムスタンプ等の個別事項について、通用性、民事訴訟における効果等について定める。

（3）認定要件、技術的要件に関する規格等

個々のトラストサービスが、特定サービス又はクオリファイドサービスに該当するかの適合性評価のための規格等を定めて、法令等において引用できるようにする。

図 4-4. トラストサービスに関する共通事項と個別事項

出典：トラストに関するワーキングチーム第 3 回（令和 3 年（2021 年）5 月 18 日）の資料 3「トラストの枠組みに関するとりまとめ(案)」より抜粋

以上の認定制度のあり方については、国際相互運用性を考慮しつつ検討すべきであるが、その一方で、制度や基準、認証や監査のプロセスが国際的に整合化される場合には、海外のトラストサービス事業者との競合についても留意すべきである。すなわち、国内トラストサービス事業者の競争力維持の観点からの制度全体の最適化及び見直しが重要である。

このため、平成 28 年度（2016 年度）以前に開催されていた経済産業省主催の電子署名法研究会のような官民による検討の場を設け、トラストサービス全体を対象とした制度の課題に関する継続的な見直し及び改善に取り組むべきである。

4.3 既存法制度との GAP の整理

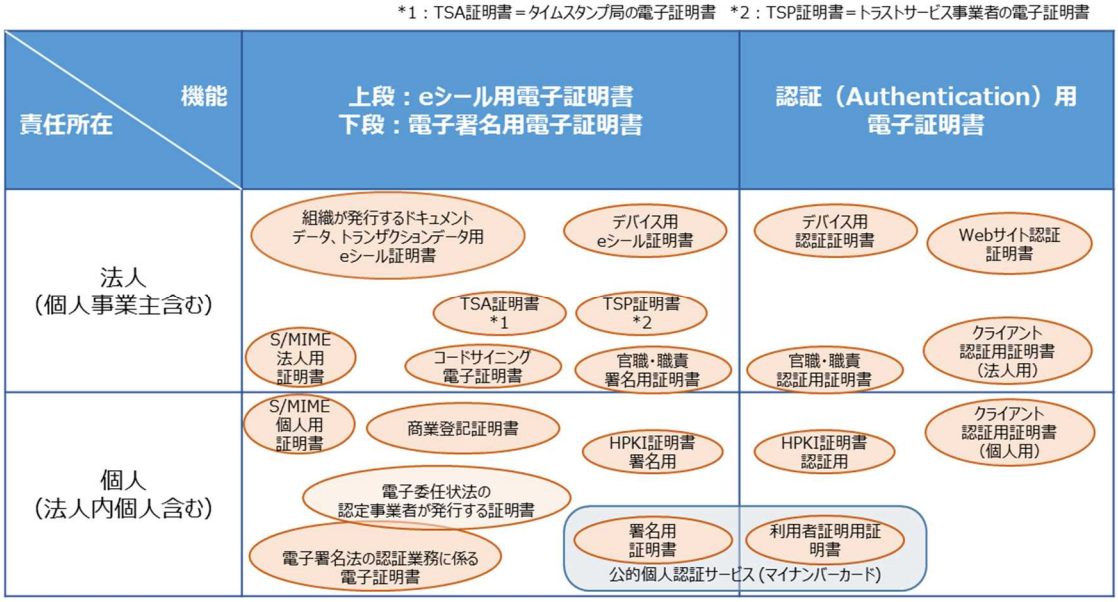
既存法制度との GAP の整理に言及する前に、電子証明書の種別に関する全体像を以下に解説する（下図 4-5.参照）。

本調査研究で言及される電子証明書を、縦軸：所在責任、横軸：機能で分別した。

個人は電子署名を行う（意思表示）のに対し、法人は発出元証明（e シール）として区別した。

なお、官職証明書・職責証明書は組織内部の機関との考え方を行ったため法人に含めている（中央部分）。

図 4-5. 電子証明書の種別の全体像



4.3.1 電子署名法

現行の電子署名法の課題を、以下の通り、整理した。

（1）電子署名、認証業務及び特定認証業務の定義（法第 2 条）

電子署名の定義として、自然人が行った措置のみを対象としており、法人等の名義で行われた措置を対象としていないと解釈されている。

（2）電磁的記録の真正な成立の推定（法第 3 条）

ア. 押印における二段の推定の一段目（本人による電子署名データであること）に該当する推定に係る判断基準が定められていない。

イ. 電子署名を行う者が自身の署名鍵を、リモート署名事業者のサーバ上に設置・保管し、当該署名鍵を用いて電子署名を行うユースケース（いわゆるリモート署名）において、推定効がはたらくかどうかの解釈が明らかにされていない。

ウ. 電子契約サービスの利用者が、当該サービスの提供事業者に指示をして、当該事業者自身の署名鍵を用いて電子署名を行うユースケース（いわゆる事業者署名型電子署名）において、推定効がはたらくかどうかの具体的な基準が明らかにされていない。

（3）特定認証業務に関する認定の制度（法第 4 条～第 14 条）

ア. 認定された特定認証業務から発行された電子証明書の効果が規定されていない。また、電子証明書に記載された、利用者の役職名、資格等の属性の証明は、電子契約や電子申請等で幅広く活用されているが、認定の対象外となっている。

イ. 認定認証業務が適合すべき基準を定める施行規則等が、法施行時からほとんど改正されていない。

- 情報セキュリティに関するリスクマネジメントの概念が含まれていない。
- 認証局の秘密鍵を作成及び管理する暗号装置（HSM: Hardware Security Module）の技術基準が、最新のものではない。
- 利用者自らが鍵ペアを作成し、認証局に対して公開鍵をオンライン送信する場合には、認証局はあらかじめ利用者識別符号を利用者に送付（対面または本人限定受取郵便）しなければならない。スマートフォンにおいて鍵ペアを作成し、近年、普及しつつあるマイナンバーカードの公的個人認証サービスを用いた電子署名を付し、公開鍵をオンライン送信する等により、利用者識別符号を省略できる可能性があるが、まだ十分に検討されていない。
- 利用者の指示に基づきサービス提供事業者が利用者の鍵ペアを保管し、利用者の秘密鍵を用いて電子署名を行うサービス（いわゆるリモート署名サービス）が介在する場合が想定されておらず、認証局と同サービスとの関係が一切規定されていない。
- 公開鍵暗号方式における秘密鍵が、特定認証業務の利用者の手元で管理されることを想定している。
- EU の eIDAS 規則における適格署名生成装置（QSCD: Qualified electronic Signature/Seal Creation Device）に相当する装置に関する規定がない。

ウ. 認定認証業務に関する情報は、官報による公告及び主務省の Web サイトによる公示により、公開されているが、以下の課題が存在する。

・官報では公開鍵電子証明書のハッシュ値が記載されているが、実用に供するものではない。
・主務省の Web サイトでの公示については、認定認証業務の名称、事業者の名称、認定の日付の一覧表が記載されているが、機械可読性が低い上に、過去の履歴を参照できない。

4.3.2 公的個人認証法

課題

（1）現在広く用いられている長期署名形式の署名文書には、署名者の電子証明書や証明書失効情報が格納されているが、電子証明書のシリアル番号の秘匿規定(*1)や証明書失効情報の利用制限(*2)により、本来、署名文書を利用する者に署名文書が渡せない状況がある。

＊1：同法 17 条 1 項 6 号 → 同法施行令 9 条 2 号 → 同法施行規則 28 条 3 号へ → 技術的基準 31 条 3 号「署名用電子証明書の発行番号等(利用者証明用電子証明書の発行番号も含む)を外部に提供しないこと」となっている。

＊2：同法 52 条（署名検証者等の受領した署名用電子証明書失効情報等の利用及び提供の制限等）

（2）署名暗号アルゴリズムを規則 2 条で直接指定しており、技術の進歩に対応した改訂に手間がかかるとともに硬直化する恐れがある。

（3）電子証明書に関する国際相互承認を考慮した検討が必要ではないか。

（4）諸外国における国民 ID カードの公開鍵証明書の利用制限について調査する必要がある。

（5）類似した認定基準との共通化の検討を行うべきではないか。

ア. 同法第 17 条 失効情報にアクセスし署名検証を行う者について以下の 3 つの種別の届出を求めている。

第 1 項 4 号 認定認証事業者(署名法第 8 条)

第 1 項 5 号 特定認証業務(署名法 2 条 3 項）を行う者であって総務大臣が認定する者

第 1 項 6 号 JPKI の失効情報が確認できる署名検証業務を行う者であって総務大臣が認定する者

イ. 5 号認定の要件

共通要件： 設備基準、運用基準は電子署名法の特定認証業務の認定要件と同じ規定となっている。

個別要件： 利用者の真偽確認、欠格事項

ウ. 6 号認定の要件

6 号認定を受けるものは、署名検証サービス事業者であり本来、トラストサービス事業者としての共通要件を満たすべき事業者であると考えられる。

4.3.3 商業登記法

3.2.3.にて検討した商業登記関連法制度と 4.2 にて検討した制度のあり方の GAP（矛盾点 等）は、以下が挙げられる。

ア. 国際連携を考慮した基準となっていない

現状の商業登記電子証明書は国内の相互運用しか考慮されておらず、将来的な国際連携等は考慮されていない。

イ. 外部認定のない独自基準で運用

商業登記認証局は外部から認定を受けておらずルート機関からの証明書等もなく、独自の基準で運用されている。具体的には、商業登記法、商業登記規則は、登記業務に係る規定が中心であり、トラストに係る記載は少ない。また、CP/CPS にはリスクアセスメントや情報セキュリティポリシに関する記載が見受けられず、全般的にセキュリティに関する記載が少ない。

ウ. 技術基準（鍵管理基準や証明書プロファイル等）の規定が不明確

商業登記認証局は利用者の秘密鍵に関知しておらず、明確な管理基準を定めていない（PC 上での管理が標準で、IC カード格納はオプション）。また、鍵の利用目的である EE 証明書プロファイル中の keyUsage の記載もない。

4.3.4 電子委任状法

現行電子委任状法に関する課題を以下のとおり、整理した。

（1）電子契約に関する代理権授与属性に限定

今後の DFFT や Society5.0 を想定すると、電子契約以外の利活用（トレーサビリティ、サプライチェーン、情報銀行等）において、代理権授与属性以外（例として、個人としては卒業証明、最終学歴、称号、許可証、専門的資格、権能等。会社組織では行政庁による認可、免許、財務データ、企業データ等）も認められるべきであるが、現状は、電子契約に関する代理権授与属性に限定されていて、利用範囲を狭めている。

（2）「代理権授与」以外の様々な属性が認定の対象外

トラストサービスにおける例として、電子署名法を例示する。

電子署名法に基づく認定認証事業者は、電子証明書の発行時に、発行対象者が所属する組織名称や住所・法人番号等の「組織属性」を真偽確認時に商業登記簿等と照合のうえ電子証明書に格納し発行している。当該電子証明書は主に電子申請（B to G）で平成 13 年（2001 年）から活用されており、電子証明書に格納された組織属性は識別等で重視されている。

また、所謂「士業」に発行される電子証明書も、「資格属性」として真偽確認時にエビデンスと照合のうえ電子証明書に格納して発行し、電子申請等で活用されているのは同様である。

ところが、電子証明書に記載された属性が当然のように活用される一方で、当該諸属性は電子署名法の認定対象外であることを余儀なくされている（※）。

※ 電子署名法施行規則第６条８号

電子証明書に利用者の役職名その他の利用者の属性（利用者の氏名、住所及び生年月日を除く。）を記録する場合においては、利用者その他の者が当該属性についての証明を認定認証業務に係るものであると誤認することを防止するための適切な措置を講じていること。

（3）ベースレジストリの信頼性

前述した様々な属性データは、電子証明書を発行する業務において確認する際に、ベースレジストリを確認することが想定される。しかし、令和３年（2021 年）現在において、ベースレジストリは必ずしも十分な保護がされているとは言い難く、提供されるデータの発出元が確認不能であったり、データの改竄有無が検知不能では、データの信頼性を高めるために活用する電子証明書の信頼性が疑われる可能性もある。

4.3.5 時刻認証業務の認定に関する規程

時刻認証業務の認定制度において、3.2.6.3 で整理した現状の課題を踏まえ、以下にタイムスタンプに係る規程等について以下の通り整理した。

（1）法的効力

ア． タイムスタンプの効力に関する規定

「時刻認証業務の認定に関する規程（令和３年（2021 年）総務省告示第 146 号）」（以下、総務省告示第 146 号）第２条に、電磁的記録に記録された情報に付与される時刻情報の総体として、存在証明と非改ざん証明を有するタイムスタンプの定義がなされた。これにより、タイムスタンプそのものは明確化されたものの、電子署名が法律によってその効力が定められているのに対しタイムスタンプは総務省の告示であり効力についての記載は無い。このことが、国際相互承認の局面において、我が国のタイムスタンプが正当に評価されない要因となる懸念がある。

また、EU においては、eIDAS 規則にて、タイムスタンプの法的手続きにおける証拠としての能力に言及しているのに対し、総務省告示第 146 号はタイムスタンプの機能を明確にするにとどまっている。

イ． タイムスタンプの通用性に関する規定

電磁的記録の利活用を容認する法令やガイドラインにおいて、情報の信頼性を確保する観点で、トラストサービスの適用による情報の真正性等の確保を求めるものが少ない。

例えば、タイムスタンプ利用に言及される省令は、電子帳簿保存法施行規則のみである。

電磁的記録は、改ざんの痕跡が残らない等の書面とは異なる特性に十分配慮し、必要性を勘案したうえでトラストサービスの適用を推奨する必要があるが、総務省告示第 146 号が施行された時点において、利活用を伴うべき法令やガイドラインの見直しには至っていない。

（2）規定すべき内容の範囲

タイムスタンプが国際的に通用するためには、タイムスタンプを発行するトラストサービスプロバイダに対する適合性評価が国際的な合意規格に基づき実施されていることが必要となる。現在、タイムスタンプの技術規格は ISO や RFC に定められ、プロバイダーの運用要件は EU の EN 規格があり環境に応じて見

直し更新がされている。一方、我が国の JIS 規格は、ISO 規格の改訂が反映されていない状況であり、総務省告示第 146 号と同時に発出された「時刻認証業務の認定に関する実施要項」では、タイムスタンプの技術規格について RFC3161 等を参照するにとどめ、詳細な技術要件・運用要件等を規定している。

本来、総務省告示第 146 号は、制度の枠組みや手続きのみを規定し、タイムスタンプの技術や時刻認証業務の運用に関する要件は、国内外の合意規格を参照する仕組みを検討することが必要である。

（3）適合性評価の仕組み

総務省告示第 146 号においては、時刻認証業務の適合性評価の仕組みとして、調査機関を指定することとしている。このような政府による適合性機関の指定は様々な分野で実施されているものであるが、トラストサービスの国際的潮流として、適合性評価機関に資格を与えるための認定（accreditation）が主流となっており、トラストサービス共通の課題として検討が必要である。

（4）電子証明書を発行する認証局

総務省告示第 146 号においては、タイムスタンプの生成に用いる秘密鍵とペアとなる公開鍵に係る公開鍵証明書（TSA 公開鍵証明書）を「電子証明書」と定義し、「信頼できる認証事業者」から発行されたものであることを認定の要件としている。

これは、信頼できる認証事業者であれば、電子証明書を発行するシステム等の安全性も確保され、証明書発行要求の依頼者や対応する秘密鍵の生成環境等についても確認の上、業務が実施されるであろうとの期待ができることから定められたものと思われる。

実際は、TSA 公開鍵証明書を発行する認証業務については要件が定められておらず、その安全性等は認証事業者に依存することとなっている。

（5）認定の公表

総務省告示第 146 号において、認定の公表は、対人可読形式のみが予定されているが、認定タイムスタンプであることを、利用者のシステムにおいて自動的に検証可能とするため、機械可読形式の認定の公表に期待が高まっている。

なお、タイムスタンプ付与時点で認定されていることが確認できることは元より、将来の検証時点において、過去のある時点で認定を受けていたものであるか否かを確認できるよう設計することが求められる。

4.3.6　e シールに係る指針

現行 e シールに係る指針に関する課題を以下のとおり整理した。

(1) 法的効果の欠如

トラストサービスは、それぞれ単体で利用することも可能であるが、通常はトラストサービスを組合せて

活用されることが多い（例として電子署名+タイムスタンプ、等）。令和３年（2021 年）時点でトラストサービスは「電子署名：法的効果」「タイムスタンプ：国の認定制度」「e シール：指針に基づく民間自主サービス」と、非統一な状況にある。
組合せて活用する際に、どちらが優先されるか不明であり、サービス利用者、提供者とも判断に窮することとなり、利用しづらい状況となる。また、海外との相互認証において不利益を被る可能性も存在する。

(2) ｅシール用電子証明書を発行する業務の設備基準、技術基準、運用基準が未確定
ｅシールに係る指針は公表されているが、ｅシール用電子証明書を発行する業務の設備基準、技術基準、運用基準は未確定である。これらを確定しない場合、ｅシールを発行する認証業務の基準が不一致となり、利用者の混乱を招きかねない。

(3) ｅシール用電子証明書を発行する固有な要件の検討が不充分
ｅシールに係る指針において、相応の要件は公開されているものの、以下は検討が充分ではない。これらを確定しない場合、ｅシールを発行する認証業務の基準が不一致となり、利用者の混乱を招きかねない。

ア. 適合性評価機関に関する基準
イ. 発行対象の明確化
ウ. 発行対象の真偽確認方法
エ. 電子証明書プロファイル、組織を特定可能な識別子
オ. 発行されるｅシールのレベル、および当該レベル適合基準、等

4.3.7 リモート署名ガイドライン

（1）個別課題

ア. 技術要件
JT2A のリモート署名ガイドラインには、利用者認証及び SIC（Signing interactive component：リモート署名サーバと接続する署名者側のソフトウェア）に関する技術要件や管理策は規程されていない。

イ. 評価・認証
同ガイドラインを用いた、評価機関による評価、又は監査機関による監査を実施していなく、同ガイドラインを用いて実際に評価・監査できるか不明である。

ウ. 公的な基準としての位置づけ
民間の自主的なガイドラインであり、公的な基準として認められていないため、準拠への動機が乏しい。

エ. ｅシールへの対応
同ガイドラインは、電子署名を前提に記載しており、組織の中で複数名が同一の署名鍵を扱う可能性のあるｅシールに関しては未検討である。

（2）個別課題

ア. 相互運用性

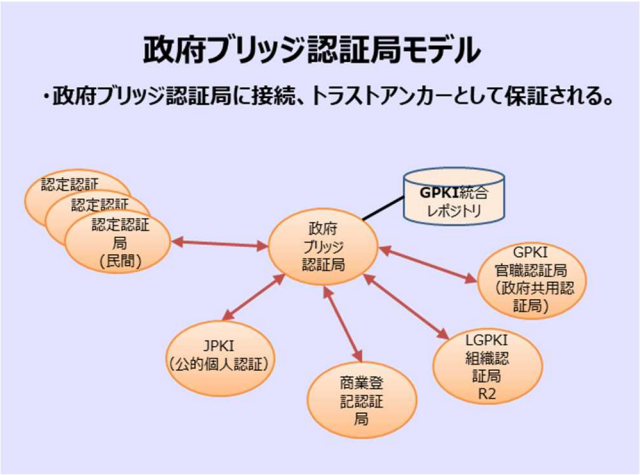
欧州規格を参照しているが、相互運用のためには技術的同等性は不明である。

4.3.8 その他

GPKI（政府認証基盤）および LGPKI（地方公共団体認証基盤）の現状と、各々に関する課題を以下に記載する。

GPKI および LGPKI は、下図のような構成モデルとなっており、政府ブリッジ認証局(GPKI ブリッジ認証局)が、官側の認証局(GPKI 官職認証局、LGPKI 組織認証局、商業登記認証局、JPKI 公的個人認証局)と民間側の認定認証局を繋ぐ役割を担っている。

図 4-6. 政府ブリッジ認証局モデル



（1）GPKI の現状

ア. GPKI は、eJapan 重点計画に基づき、申請・届出等手続のオンライン化を推進するため、申請やその結果の通知等が、申請者や行政機関の処分権者によって作成されたものか、申請書や通知文書の内容が改ざんされていないかを確認する行政機関側の仕組みとして整備されている。

イ. この GPKI は、GPKI ブリッジ認証局と GPKI 官職認証局(政府共用認証局)から構成され、それぞれ行政情報システム関係課長連絡会議了承のもと CP/CPS(証明書ポリシ及び認証実施規定)が整備され、総務省が運営している。

ウ. GPKI ブリッジ認証局は、行政機関側の認証局と民間認証局等との間の信頼関係を仲介するものである。

エ. GPKI 政府共用認証局は、府省ごとに整備された府省認証局を統合したものであり、行政機関の処分権者である大臣等の官職証明書を発行するものである。

（2） LGPKI の現状

ア. LGPKI は、「総合行政ネットワーク基本規程第３条第３項」の規定に基づき設けられる地方公共団体組織認証基盤である。

イ. この LGPKI は、LGPKI 組織認証局等から構成され、それぞれ「地方公共団体組織認証基盤の運営に関する基本要綱」のもとに CP/CPS(証明書ポリシ及び認証実施規定)が整備され、地方公共団体情報システム機構(J-LIS)が運営している。

ウ. LGPKI 組織認証局は、地方公共団体等の役職・職責等を認証するための証明書を発行するものであり、GPKI ブリッジ認証局と相互認証をしている。

（3） GPKI/LGPKI での個別の課題としては、以下が挙げられる。

ア. GPKI/LGPKI における認証局の CP/CPS は、法律に直接基づかない内規等に基づき整備されており、RFC3647 等の国際標準に則って規定はされているものの、現状国際連携を考慮したものにはなっていない。

イ. GPKI/LGPKI の官職証明書や職責証明書等は、基本的には公文書に対して署名をするものであるが、現状では私文書(契約書等)に署名するケースもあり、署名の利用用途をどこまでとするかが明確ではない。

ウ. GPKI/LGPKI の官職証明書や職責証明書等は、いわゆる公印のような使用を想定しており、自然人としての署名者には一意に紐づいていない。

（4）HPKI

ア. HPKI の概要

(ア) HPKI は、保健医療福祉分野の公開鍵基盤（Healthcare Public Key Infrastructure）の略称である。

(イ) 厚生労働省が所管する医療従事者の国家資格や医療機関の管理者資格を格納した電子証明書に基づく公開鍵基盤で、電子署名用証明書のほか、認証用証明書も対象としている。

(ウ) 根拠となる法制度は無いが、国家資格を審査するための基準が厚生労働省の「保健医療福祉分野 PKI 認証局証明書ポリシー」で定められており、それに準拠しているかを確認する準拠性監査がある。

(エ) 医療情報システムの安全管理に関するガイドライン第 5.1 版において、次のように HPKI の利用が推奨されている。

> 法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う必要がある。
> 1. 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局又は認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと
> (1) 保健医療福祉分野 PKI 認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。したがって、この保健医療福祉分野 PKI 認証局の発行する電子署名を活用することが推奨される。
>
> 以下省略

(オ) 準拠性監査を経て厚生労働省 HPKI ルート認証局のサブ CA として設置承認を受けた認証局は執筆時点では次の通りである。

- 日本医師会の日本医師会認証局
- 日本薬剤師会の日本薬剤師会認証局
- 一般財団法人医療情報システム開発センター(MEDIS)の保健医療福祉分野公開鍵基盤電子認証局

イ. 証明書に格納される属性

- 医療従事者の資格を格納するための証明書拡張領域のフィールドである hcRole（healthcare Role）及びそのフィールドに格納できる属性の定義が ISO17090（Health Informatics -Public Key Infrastructure）に規定されている。属性として、26 種類の保健医療福祉分野の国家資格と 5 種類の医療機関の管理責任者としての資格が定義される（表参照）

表 4-7. 国家資格

資格名	説明
Medical Doctor	医師
Dentist	歯科医師
Pharmacist	薬剤師
Medical Technologist	臨床検査技師
Radiological Technologist	診療放射線技師
Registered Nurse	看護師
Public Health Nurse	保健師
Midwife	助産師
Physical Therapist	理学療法士
Occupational Therapist	作業療法士
Orthoptist	視能訓練士
Speech Therapist	言語聴覚士
Dental Technician	歯科技工士
National Registered Dietitian	管理栄養士
Certified Social Worker	社会福祉士
Certified Care Worker	介護福祉士
Emergency Medical Technician	救急救命士
Psychiatric Social Worker	精神保健福祉士
Clinical Engineer	臨床工学技士
Massage and Finger Pressure Practitioner	あん摩マッサージ指圧師
Acupuncturist	はり師
Moxibustion Practitioner	きゅう師
Dental Hygienist	歯科衛生士

Prosthetics & Orthotic	義肢装具士
Artificial Limb Fitter	柔道整復師
Clinical Laboratory Technician	衛生検査技師

表 4-8. 医療機関の管理責任者としての資格

資格名	**説明**
Director of Hospital	病院長
Director of Clinic	診療所院長
Supervisor of Pharmacy	管理薬剤師
Proprietor of Pharmacy	薬局開設者
Director	その他の保健医療福祉機関の管理責任者

ウ. 準拠性監査

- HPKI の認証局として承認されるための準拠性監査は、厚生労働省医政局「保健医療福祉分野における公開鍵の整備と運営に関する専門家会議」（以下「専門家会議」という。）によって実施される。その手続は、「保健医療福祉分野 PKI 認証局署名用・認証用（人）証明書ポリシー準拠審査手続規則」によって規定され、審査業務は、厚生労働省が別に定める「保健医療福祉分野 PKI 認証局署名用・認証用（人）証明書ポリシー準拠性審査業務実施規則」に従って行われる。

エ. トラストアンカーの公開

- 厚生労働省ルート HPKI 認証局は、署名用サブ CA 証明書と認証用サブ CA 証明書を発行する。従ってこのルート CA の証明書をトラストアンカーとして利用でき、その情報は、証明書のフィンガープリントや失効情報とともに厚生労働省のリポジトリに公開される。

4.4 既存法制度との GAP 解消策の検討

4.4.1 定義

（1）トラストサービス及びトラストサービスが発行するデータ等の位置づけ

定義に先立って、トラストサービス及びトラストサービスが発行するデータ、さらにそのデータの利用に関して整理しておく。表 4-9.にトラストサービスの例と、トラストサービスが発行するデータ等について示す。ここで網掛部分は、民事訴訟において、真正な成立の推定等の効力をもたらすと思われる事項である。

表 4-9. トラストサービスと発行データ等

トラストサービス	認証業務	e シール用認証業務	時刻認証業務
トラストサービスが発行するデータ	電子証明書	e シール用電子証明書	タイムスタンプ
上記データに基づいて行われる措置	電子署名	e シール	−
上記措置において生成されるデータ	電子署名データ (eIDAS における Electronic Signature)	e シールデータ （eIDAS における Electronic Seal）	−

たとえば、（自然人の）電子証明書を発行する認証業務はトラストサービスであり、そのトラストサービスが電子証明書をデータの形で発行する。電子証明書に係る本人は、電子証明書に基づいて電子署名を行い、その結果として電子署名データが生成される。この電子署名データまでが、トラストサービスに関する検討範囲である。e シールについても同様に考えられる。

タイムスタンプの場合は、トラストサービスたる時刻認証業務がデータたるタイムスタンプを発行する。基本的に、タイムスタンプに基づく措置等があっても（検証サービス等の別のトラストサービスによる処理で無い限り）、トラストサービスに関する検討範囲とは考えない。

現行法では、電子署名法で真正な成立を基礎づけるのは電子署名であり、これは措置である。実際には、電子文書等に添付又は関連付けられ、依拠者等が取得するのは電子署名データであるが、電子署名データからただちに真正な成立の推定は得られない。電子署名データの存在から電子署名の実施を導出するという証明手続きが必要となる。この点、eIDAS においては、電子署名はデータであると定義されており（3 条 10 号）、データたる電子署名が適格であれば、これにより手書署名と同等の効力を有することが規定されている（25 条 2 項）。このような定義の違いには、注意が必要である。

なお、e シールが措置である（e シールを行う）ことには、いささかの不自然さを覚えざるを得ない（eIDASでは、eシールはデータとして定義されている（3条25号）ので、この問題は生じていない）。特に、機械的・自動的に行われた措置たる e シールの主体の在り方（その主体が e シールを行ったと言い得るのか等）には、注意を要するところである。

（2）特定及びクオリファイドの考え方

各トラストサービス及びトラストサービスが発行する情報について、「無印」及び「クオリファイド」を定義する他、必要に応じて「特定」を定義することとする。基本的に、まず無印の定義を行い、さらに要件を付加したものとして、特定、クオリファイドを定義する。以下、本章において、無印、特定及びクオリファイドを総称して「レベル」という。

トラストサービスと、トラストサービスが発行する情報のレベルは同一とする。たとえば、クオリファイドタイムスタンプ業務が発行するタイムスタンプはクオリファイドタイムスタンプであり、特定認証業務が発行する電

子証明書は特定電子証明書となる。

クオリファイドトラストサービスは、原則として、そのトラストサービスに係る認定を受けたものとして定義する（JPKI、商業登記、GPKI、LGPKI、HPKI 等）。特定トラストサービスを定義する場合には、その要件は明記するものの、公的機関による認定を予定するものではない。特定については、民間機関による判定を期待するものとする。

（3）定義の概要

以下では、トラストサービス等に係る定義の概要を示す。可能な範囲で特定及びクオリファイドについても記載しているが、一部のトラストサービス等についてはこれらを記載していない。このような事項については、今後の検討が必要である。

ア. 電子署名

無印： 電子署名法 2 条 1 項の電子署名

特定： 特定要件（特定サービスの認証局が発行した電子証明書に基づく電子署名？AdES フォーマット？）を満たす電子署名

クオリファイド： クオリファイド電子証明書に基づき、クオリファイド電子署名生成装置により行われた特定電子署名

イ. 署名者（Signatory）

電子署名又は e シールを行う主体。

ウ. 電子署名データ

電子署名の実施によって作成され、電子署名が行われたこと等を示すために電磁的記録に付属され又は関係づけられたデータ。

エ. (自然人用)電子証明書

無印： 電子署名検証情報（公開鍵・検証鍵等。PKI ベースでないものも含む）と本人との関係を証明する電子文書

特定： 特定認証局により発行された電子証明書であって、一定の身元確認に基づくもの

クオリファイド： クオリファイド認証局により発行された電子証明書

オ. トラストサービス

(無印)トラストサービス： インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止するとともに、それらを確認する仕組みであって、以下のサービスをいう

(ア) 認証業務

(イ) リモート署名業務

(ウ) 時刻認証業務

(エ) 検証業務

(オ) 電子内容証明送付業務

(カ) 事業者型電子署名業務

(キ) 保存業務

特定トラストサービス： トラストサービスごとに定められた特定の基準を満たすトラストサービス

クオリファイドトラストサービス： トラストサービスごとに定められたクオリファイドの基準を満たすトラストサービス

カ. トラストサービス事業者

無印： トラストサービスを提供する者

特定： 特定トラストサービスを提供する者

クオリファイド： クオリファイドトラストサービスを提供する者

キ. 依拠者（Relying Party）

トラストサービスの正当性に依拠して何らかの事項を証明しようとする者

ク. 利用者

トラストサービス（トラストサービスが関与して作成された情報を含む）の利用者。署名者、依拠者、検証者を含むがこれらに限られない。

ケ. 認証業務

(無印)認証業務： 自らが行う電子署名についてその業務を利用する者（署名者：自然人、法人、その他含む）その他の者の求めに応じ、当該署名者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明するトラストサービス（電子署名法 2 条 2 項を微変更）

特定認証業務： 電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務（電子署名法 2 条 3 項）

クオリファイド認証業務： 認定を受けた認証業務

コ. リモート署名業務

無印： 利用者の署名鍵を預かり、利用者の指示に従ってこれを利用して電子署名を行うトラストサービス

特定： 一定の要件を満たす利用者の認証、鍵認可を行うリモート署名業務

クオリファイド： 認定を受けたリモート署名業務

サ. 電子署名データ生成装置

無印： 電子署名を行うために用いる装置又はソフトウェア

クオリファイド： 認定を受けた電子署名データ生成装置

シ. e シール

無印： 電子データの発行元及び非改ざん性を示すための措置(電子署名法 2 条 1 項相当)

特定： PKI ベースの e シール

クオリファイド： クオリファイド e シール生成装置により行われた e シール

ス. e シールデータ

e シールの実施によって作成され、e シールが行われたこと等を示すために電磁的記録に付属され又は関係づけられたデータ。

セ. ｅシール用電子証明書

無印： 電子署名検証情報（公開鍵・検証鍵等）と発行元との関係を証明する電子文書

特定： 特定認証業務により発行されたｅシール用電子証明書であって、発行元組織についての一定の確認に基づくもの

クオリファイド： クオリファイド認証業務により発行されたｅシール用電子証明書

ソ. ｅシールデータ生成装置

電子署名生成装置と同様に定義

タ. 属性証明付き電子証明書

無印： 電子証明書であって、本人特定情報（４情報等）以外の属性が記載されているもの

チ. タイムスタンプ

無印： 対象電子データがある時刻に存在していたことと、その後の改変がないことを確認できる情報等（告示２条１項のタイムスタンプ）

特定： 特定時刻認証業務により生成されたタイムスタンプ

クオリファイド： クオリファイド時刻認証業務により生成されたタイムスタンプ

ツ. 時刻認証業務

無印： タイムスタンプを発行するトラストサービス

特定： デジタル署名方式であってUTC(NICT)との時刻差が１秒以内の時刻認証業務(告示３条１項の一部)

クオリファイド： 告示３条１項を満たすものとして認定を受けた時刻認証業務

テ. 検証業務

電磁的記録及びそれに付随した情報を用いて、その情報又はその情報を作成した措置の正当性を検証し、その結果を通知するトラストサービス

ト. 保存業務

技術有効期間を超えてクオリファイド電子署名データ、クオリファイドｅシールデータ、クオリファイドタイムスタンプ等の信頼性を拡張するための措置を行う業務

ナ. 電子内容証明送付業務

電磁的記録の送受信に関して、送信者、受信者、電磁的記録の内容、送信時刻及び受信時刻の証明を行うトラストサービス

ニ. 事業者型電子署名業務

利用者の指示に基づき業務提供事業者自身の署名鍵により暗号化等を行うトラストサービス

ヌ. 電磁的記録

電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの

ネ. 監督機関

国又は国が指定する機関。国家監督機関又は民間主導の認定機関が想定される。クオリフ

ァイドトラストサービスの認定、適合性評価機関の認定等を行うもの

ノ. 適合性評価機関

監督機関から指定を受けた機関。トラストサービスがクオリファイドの基準に適合するかどうかを評価し、結果を監督機関に報告する。

4.4.2 一般原則

（1）監督・指導

監督機関を設立し、トラストサービスに対する監督権限、クオリファイド等の認定権限（認定取消等の権限を含む）を規定すべきである。また、トラストサービスに対する指導の機能を持たせるべきである。

（2）トラストサービスの責任

民法の一般的な責任に加えて、トラストサービスの責任を明記するかどうかを検討する必要がある。

まず、一般論として、民法における損害賠償責任を概観しておく。トラストサービスの契約責任（債務不履行責任）及び不法行為責任は、民法に規定されている。契約上の義務を履行しなかったことにより損害を生じた場合には、被害者はトラストサービスに損害賠償を請求できる（民法 415 条 1 項）。契約による義務がない場合であっても、トラストサービスの故意又は過失によって損害を生じた場合には、被害者は損害賠償を請求できる（民法 709 条）。なお、トラストサービスの義務違反や、故意・過失については、被害者側に証明責任がある（それらの存在を証明できなかった＝真偽不明の場合には、損害賠償を請求できない。なお、因果関係のある損害の発生等についても被害者側が立証責任を負う）。

eIDAS においては、適格トラストサービスの不法行為責任については、その故意・過失について立証責任が転換されており（eIDAS 13 条 1 項第 2 文）、適格トラストサービス側で無過失を証明しない限り損害賠償責任を免れない（不法行為の存在、因果関係のある損害の発生については、証明責任は転換されていない）。

我が国の法制として、トラストサービスの責任を明記すること、証明責任を転換することは、利用者にとっての法的見通しをよくする意味で有効である。これは、海外の利用者について顕著である。その一方で、民法と同内容の規定を重ねて置くことには抵抗感をぬぐえない。また、認定を受けたトラストサービスの責任を加重（立証責任の転換）するのであれば、その効果や必要性を十分に評価する必要がある。このような意味で、トラストサービスの責任規定については、慎重な検討を行う必要があると考えられる。

（3）電子文書等の通用性

電子文書、電子署名等が、どのような場面でどのように使用できるか、という意味での通用性について、我が国の法制には一般的な規定はない。このため、トラストサービスを利用しようとする者が、手続上の適法性を逐一確認する必要に迫られている。電子文書等の一般的通用性について規定し、電子署名等については、一般的定義を参照する形で規定すべきではないだろうか。

ア. 電子文書

欧州、米国の法制と同様に、電子文書について、電子的な形態であることだけを理由に法的効力、証拠力、通用性等を否定してはならない、とする一般的な規定を置くべきではないか。

イ.　電子署名、e シール、タイムスタンプ等

電子署名、e シール、タイムスタンプ等のトラストサービス及びトラストサービスが関与して生成されたデータについても、電子的な形態であることだけを理由に法的効力、証拠力、通用性等を否定してはならない、とする一般的な規定を置くべきではないか。

ウ.　通用性の規定方法

公的機関や法令における電子文書、電子署名、e シール、タイムスタンプ等の通用性（許容性）については、今後創設されるべきトラストサービスの包括法における定義を参照して規定することとし、特段の事情がない限り個別法での規定を避けるべきではないか。

（4）ID スキームの通用性

国が管理し利用を認める ID スキーム（JPKI、gBizID 等）について、そのリストを公開するとともに、国の機関における通用性を明示するべきではないか。

（5）表示規制

何人も、クオリファイドの認定を受けることなく、その商品、役務又は提供する情報に「クオリファイド」と表示してはならない、とする規制を行うべきではないか。

電子署名及び e シールの生成方法（クオリファイド生成装置を利用しているか、リモートによるものか、リモートに係るトラストサービスはクオリファイドか、等）を電子署名データ等に表示する方法について規定すべきではないか。

（6）国際協調

トラストサービスが関与して作成された情報の、海外での通用性を確保する方策を講じる必要がある。

海外の制度によって、我が国と同等又はそれ以上の水準の認定を受けているトラストサービス等は、我が国のトラストサービスと同等の効力を持つことが可能となる制度を設立すべきではないか。

4.4.3　共通事項

4.4.3.1 全てのトラストサービスが満たすべき要件

クオリファイドトラストサービスに限らず全てのトラストサービスが満たすべき要件を以下のように定めるべきではないか。

(1) 提供するトラストサービスに係るリスクを管理し、セキュリティ事故の発生を予防する及び発生時の被害を最小化する適切な技術的及び組織的対策を講じること。

(2) 提供するトラストサービスの信頼性及び、保管する特定個人情報の機密性に係るセキュリティ事故発生時は遅滞なく監督機関に通知すること。

(1)の適切な技術的及び組織的対策に関しては、提供するトラストサービスの種別及びそのレベル（無印、特定及びクオリファイド）に応じて必要な要件が異なり、別途技術基準においてその詳細が定められる必要がある。また、トラストサービスの種別に拠らない要件を共通要件として技術基準を整備することで基準の作成/維持に係るコストを削減できる。

4.4.3.2 トラストサービスの認定

(1) 監督機関

多種多様に広がりつつあるトラストサービスの監督機関を設置し、クオリファイドサービスの認定及びトラステッドリストの公開・運営を行い、認定制度全体の企画立案をさせる。監督機関は、米国や EU の実例を参考にしつつ、トラストサービス事業者のニーズ、適合性評価機関のあり方等を踏まえ、制度全体を改善させる責任を有するものとする。

(2) トラストサービスの公的な基準を策定する機関

国内のトラストサービスのうち特定サービス及びクオリファイドサービスの基準を策定する機関を設置することとし、EU 欧州電気通信標準化機構（ETSI）や米国標準技術研究所（NIST）等の先例を参考にする。

(3) 適合性評価機関

クオリファイドサービスの認定においては、電子署名法に基づく指定調査機関の仕組みを改め、認定の主体である監督機関と、適合性評価の主体である民間の適合性評価機関の間の責任を分離する。また、適合性評価機関が満たすべき基準を作成する。

認定制度の具体的なプロセスについては、以下が想定される。

ア. クオリファイドサービスの認定基準、特定サービスの基準の作成
イ. 適合性評価機関による評価
ウ. 監督機関による認定
エ. 監督機関によるトラステッドリストへの登録

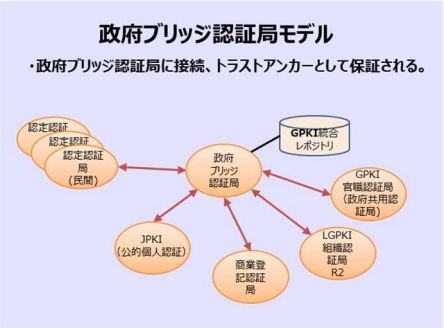
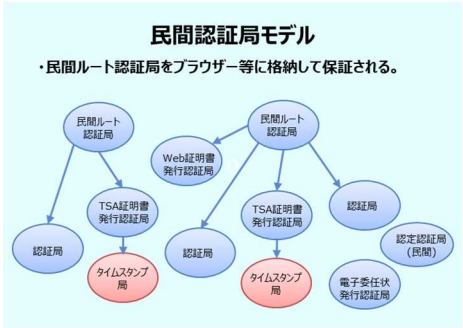
4.4.3.3 トラストサービスの公表等

トラストサービスの公表等に関わる既存制度との GAP 解消策に向けた検討事項を記載する。

（1）既存制度

日本では認証局の信頼性を確認する方法として、下図に示す 2 つのモデルが存在している。

表 4-10. 政府ブリッジ認証局モデルと民間認証局モデルの比較

モデル	政府ブリッジ認証局モデル	民間認証局モデル
特徴	・政府ブリッジ認証局と接続する方法 ・電子署名法に基づく認定認証局は接続できる	・民間ルート認証局をブラウザ等に格納する方法
イメージ		
課題	・トラストサービスは、認証局に限られる ・相互認証できる民間認証局は電子署名法の認定を受けた認定認証局に限られる ・廃業した認証局の履歴を確認できない	・民間制度であり、電子署名法の認証局が公開対象外等、対象が限られる ・トラストアンカーをあらかじめ登録しておく必要がある。 ・廃業した認証局の履歴を確認できない

また、国際的には、認証局の信頼性を確認する方法として、米国におけるブリッジモデル、EU におけるトラステッドリストが存在している。

表 4-11. ブリッジモデルとトラステッドリストの特徴

モデル	ブリッジモデル（米国）	トラステッドリスト（EU）
特徴	・FBCA（Federal Bridge CA）をトラストアンカーとするモデル	・LOTL（List Of Trusted List）を EU のトラストアンカーとし、各加盟国の TL と相互参照するモデル

（2）あるべき姿（仮）

「包括的データ戦略」で示されたトラスト基盤の構築に向けた論点と課題では、以下の「クオリファイドトラストサービスの公表」が示されている。

> ⑥ クオリファイドトラストサービスの公表
>
> クオリファイドトラストサービスについては、利用者が相互に適格性を確認できることが求められ、クオリファイドトラストサービスの公表が必要となる。その際、クオリファイドトラストサービスは機械可読の形で公表することが必要となる。

※包括的データ戦略から抜粋・加工（包括的データ戦略では、クオリファイドサービスと記載であるが、当該報告書ではクオリファイドトラストサービスの用語に統一）

（3）GAP 解消策の検討事項

クオリファイドトラストサービスの公表においては、以下の事項を検討する必要がある。

ア. 認定を受けたクオリファイドトラストサービスであることを、トラストサービスの利用者（検証者、依拠者）が、必要なときに確認できる仕組みを検討すべきではないか。（公表する主体を含め）

イ. クオリファイドトラストサービスを利用する者の間では、相互に相手が利用するサービスの適格性が確認できる仕組みを検討すべきではないか。

ウ. 利用者の利便性の観点からは認定を受けたクオリファイドトラストサービスは、機械可読の形態で開示する、又は相互接続することを検討すべきではないか。

エ. 認証局以外のトラストサービスを扱うことを検討すべきではないか。

オ. トラストサービスの認定を受けた日付等、過去、有効なトラストサービスであったことを確認できる検討が必要である。

カ. 廃業したトラストサービスの履歴を確認でき、引き続き扱えることを検討すべきではないか。

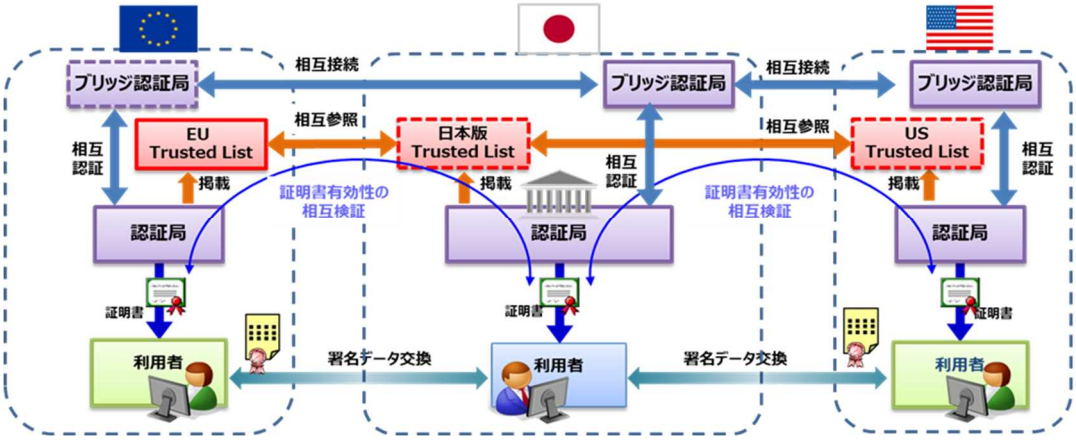
キ. クオリファイドトラストサービスを確認する仕組みは、下図 4-13.が考えられるが、既存制度を活用しつつ、新たにトラステッドリスト公表する方法を検討すべきではないか。

表 4-12. ブリッジモデルとトラステッドリストの比較

方 式		対象となる認証局等	一意に特定	可読性		廃業TSPの検証	日本での制度運用	課題
				人	機械			
ブリッジ	ブリッジ認証局と相互認証	GPKI、認定認証局（署名法認定）	○	×	○	×	○	官側の検証は問題ないが、検証に必要な情報が民間開放されていない。
リスト	官報にCA認証局のハッシュ値を公開	認定認証局（署名法認定）	○	△	×	×	○	実際の確認が困難
	ホームページでサービス名を公開	認定認証局（署名法認定） タイムスタンプ（デ協認定）	×	○	×	×	○	実際の検証時に本物の証明書か不明
	ブラウザーにルート証明書を登録（Common CA Data Base:CCADB）	Webサーバー証明書を発行するパブリック認証局（WebTrust監査、ETSI監査）	○	○	○	×	○	民間団体（CAブラウザーフォーラム）による運用であり制度安定性が課題
	アドビ製品に登録（AATL）	ドキュメント署名用のパブリック認証局（WebTrust監査、ETSI監査）	○	△	○	×	○	民間企業による自社製品での運用。PDF署名に限定
	トラステッドリストで公開（EU Trusted List）	EUのトラストサービス事業者（CABの適合性監査）	○	○	○	○	×	認証局だけでなくタイムスタンプ局等も取り扱い可能。EU域内で相互運用されているが国際的な相互運用はトライアル中

ク. 国際的にクオリファイドトラストサービスを確認できる仕組みについては、下図 4-13.のような国際相互参照・相互承認の仕組みが必要となる。制度や技術の同等性の確認等、期間・体制を要するため、マイルストーンを定めて段階的に整備すること検討すべきではないか。

図 4-13. 国際的なクオリファイドトラストサービスを確認できる仕組み



4.4.3.4 適合性評価機関

4.2.1 (4)で示した通り、クオリファイドサービスの認定においては、電子署名法に基づく指定調査機関の仕組みを改め、認定の主体である監督機関と、適合性評価の主体である民間の適合性評価機関の間の責任を分離すべきではないか。

そして、トラストサービスの適合性評価機関の要件を定める国際的な整合性を持った基準として、EU の例を参考にしつつ、JIS Q 17065：2012 適合性評価－製品、プロセス及びサービスの認証を行う機関に対する要求事項と、 ETSI EN 319 403 Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers 等をベースにした国内標準を策定するべきではないか。

さらに、ISO に基づく適合性評価制度を参考にしつつ、策定された国内標準を用いてトラストサービスの適合性評価機関を評価・認定する機関（Accreditation Body）のあり方についても、国内の事情を鑑み、検討するべきではないか。

表 4-14. 日本国の法令等、及び国際標準に基づく適合性評価の比較

【我が国】 法令等に基づく指定調査機関による適合性調査	【諸外国】 国際標準に基づき認定された適合性評価機関による適合性評価	
電子署名法	ISO/IEC 17065 （製品、プロセス及びサービスの認証を行う機関に対する要求事項）	ETSI EN 319 403 （トラストサービス評価特有の追加基準）
第四章 指定調査機関等 第一節 指定調査機関 （指定調査機関による調査） （指定） （欠格条項） （指定の基準） （指定の公示等） （指定の更新） （秘密保持義務等） （調査の義務） （調査業務規程） （帳簿の記載） （適合命令） （業務の休廃止） （指定の取消し等） （主務大臣による調査の業務の実施） 第二節 承認調査機関 （承認調査機関の承認等） （承認の取消し）	1.適用範囲、2.引用規格、3.用語と定義	適宜追加
	4.一般要求事項	4.2.1 公平性に抵触しない活動
	5.組織構成に関する要求事項	追加無し
	6.資源に関する要求事項	6.1 認証機関の要員
	7.プロセス要求事項	7.1 一般 7.3 申請のレビュー 7.4 評価 7.6 認証の決定 7.7 認証文書 7.8 認証されたサービスの登録簿 7.9 サーベイランス 7.10 認証に影響を与える変更
	8.マネジメントシステム要求事項	追加無し

※データ戦略タスクフォース トラストに関するワーキングチーム（第２回）資料４（論点 4-4）より抜粋

4.4.3.5 規格の参照

インターネットを介して瞬時にグローバルに展開できてしまうデジタル情報の信頼性を確保するトラストサービスの信頼を判断する基準は、国際的に共通する技術規格に準ずる必要がある。さらに、信頼するための基準は明確であって、その基準に準じて提供されていることを利用者が利用目的によって判断できる必要がある。

この判断基準は、技術要件のみならず運用要件も含まれ、特にセキュリティ面では、環境にあわせて逐次更新されるものである。

一般利用者において、この複雑な要件を確認することは不可能でサービス提供事業者に依存することとなる。このため、不安を払拭できずデジタル活用を躊躇する可能性は否定できない。

利用者が安心してサービスを利用するには、第三者機関にてトラストサービスがこれら変化する基準を満たしていることを調査・監査したうえで認定しお墨付きを付与する制度が運用されることが求められる。

国際的に、デジタルセキュリティにおいて規格を検討、策定している機関は、ISO（International Organization for Standardization）、IEC（International Electro technical Commission）、EU では CEN（Comité Européen de Normalisation）、ETSI（European Telecommunications Standards Institute）、USA では NIST（National Institute of Standards and Technology）、インターネット社会では、W3C（World Wide Web Consortium）、IETF（Internet Engineering Task Force）、CAB/F（CA/Browser Forum）、CSC（Cloud Signature Consortium）等がある。

我が国の認定基準の策定に当たっては、これら機関において検討・策定されている基準を参考にトラストサービス共通要件と各サービス固有要件の規定を整備することが望まれる。

グローバルで DFFT を実現するためには、トラストサービスについて、これらの機関と情報を共有し、規

格策定に継続的に関与する 4.2.1（3）記載の機関の設置が肝要である。

4.4.4 個別事項

各制度等に関して抽出した課題に対する解消策を個別に記述

4.4.4.1 電子署名

（1）電子署名法

電子署名等の国際的な相互運用性の確保の観点、とりわけ EU の eIDAS 規則等に比べてスコープが狭いことを踏まえつつ、以下の GAP 解消策を実現するための法的枠組みを整備するべきである。

ア. 自然人が行った措置のみを対象とする電子署名に加えて、法人等の組織が発行するデジタルデータの発行元証明の手段としての e シールを定義する（4.4.4.5 e シール 参照）とともに、それらの認定効果として法的効果を明らかにする（4.2 認定効果を担保するための制度のあり方の検討 参照）。

イ. 電磁的記録の真正な成立の推定について、電子署名を行う者が自身の署名鍵を、クラウド環境のサーバ上に設置・保管し、当該署名鍵を用いて電子署名を行うユースケース（いわゆるリモート署名）における解釈を明らかにする（4.4.4.6 リモート署名/e シール参照）。

ウ. 電子契約サービスの利用者が、当該サービスの提供事業者に指示をして、当該事業者自身の署名鍵を用いて電子署名を行うユースケース（いわゆる事業者署名型電子署名）において、推定効がはたらくかどうかの具体的な基準を明らかにする（4.4.4.7 事業者署名型サービス参照）。

エ. ベースレジストリの参照等による自然人の属性証明としてのトラストサービスの活用の方向性に合わせて、特定認証業務として発行される電子証明書に記載された利用者の役職名、資格等の属性の証明に関する認定の効果について検討する（4.4.4.3 属性証明）。

オ. 従来、暗号化方式に関する簡単な要件しか存在しなかった特定認証業務の具体的な基準を、新たにトラストサービスの公的な基準を策定する機関において作成するとともに、電子署名法施行時からほとんど改正されていない特定認証業務の認定基準を刷新する。当該認定基準への適合性が適合性評価機関により認証された特定認証業務について、監督機関はクオリファイド認証業務として位置付ける。トラストサービスの公的な基準を策定する機関による策定された特定認証業務及びクオリファイド認証業務の基準については、施行規則等に直接書き込まず、法令で引用する仕組みとする。

カ. 上記「オ」の基準の標準化に際しては、以下の観点を踏まえるものとすべきである。

(ア) ISMS 適合性評価制度等を参考にしつつ、情報セキュリティに関するリスクマネジメントの概念を含める。

(イ) 認証業務用設備における電子証明書の発行者が暗号化する際の秘密鍵（発行者署名符号）を作成及び管理する暗号装置（HSM: Hardware Security Module）の技術基準を、世界水準に整合化したものとする。

(ウ) スマートフォンを用いて、利用者自らが鍵ペアを作成し、電子証明書の発行者に対して公開鍵をオンライン送信するユースケースを想定し、マイナンバーカードの公的個人認証サービス等による電子署名を活用することにより、対面又は本人限定受取郵便による利用者識別符号の受け渡しを省略する方法を規定するとともに、その際のセキュリティ確保のための基準を策定する。

(エ) 上記「ウ」で明らかにされたリモート署名/e シールに関する解釈に基づき、それらのユースケースにおける特定認証業務が満たすべき認定基準を明らかにする。

(オ) EU の eIDAS 規則におけるクオリファイド署名生成装置（QSCD: Qualified electronic Signature/Seal Creation Device）に相当する装置に関する規定の必要性について検討する（4.4.4.8 電子署名/e シールデータ生成装置 参照）。

キ. 監督機関に対して、クオリファイド認証業務に関する情報は、機械可読式のトラステッドリストにより、公開する義務を課す。その際、クオリファイド認証業務の過去の履歴を容易に参照できる仕組みとする(4.4.3.3. 共通事項 トラストサービスの公表等 参照)。

（２）公的個人認証法

ア. 現在広く用いられている長期署名形式の署名文書には、署名者の電子証明書や証明書失効情報が格納されているが、電子証明書のシリアル番号の秘匿規定(*1)や証明書失効情報の利用制限(*2)により、本来、署名文書を利用する者に署名文書が渡せない状況がある。

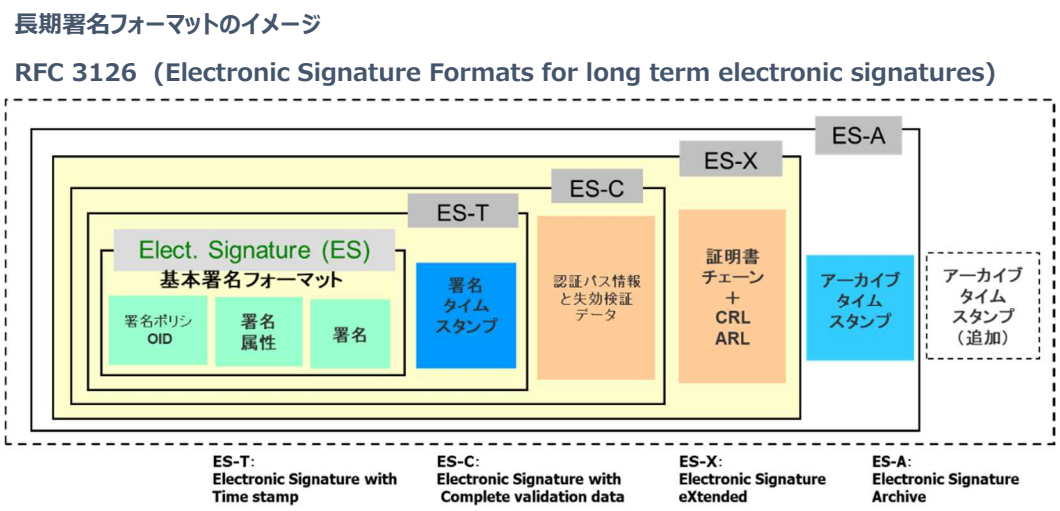
＊1：公的個人認証法 17 条 1 項 6 号 → 同法施行令 9 条 2 号 → 同法施行規則 28 条 3 号へ → 認証業務及びこれに附帯する業務の実施に関する技術的基準 31 条 3 号「署名用電子証明書の発行番号等(利用者証明用電子証明書の発行番号も含む)を外部に提供しないこと」となっている。

＊2：同法 52 条（署名検証者等の受領した署名用電子証明書失効情報等の利用及び提供の制限等）

＜解決策＞

長期署名（CAdES、XAdES、PAdES 等の Advanced Electronic Signature）形式の署名文書には、署名者の電子証明書や認証局の証明書（CA 証明書）および証明書失効情報が埋め込まれている。一方、上記*1, *2 の利用制限により、署名者の公開鍵証明書や証明書失効情報は同法 17 条 1 項 6 号の認定を受けた署名検証事業者等から外部へ提供することが禁じられている。このため、本来、電子署名文書を利用する者が長期署名形式の電子署名済み文書を入手できず、不合理な状況が生じている。従って（一般的に証明書失効情報を流通させるべきかはともかくとして）少なくとも、長期署名形式の署名データに格納された署名者の公開鍵証明書と失効情報を電子署名文書を利用する者が受け取ることを容認すべきではないか。

図 4-15. 長期署名フォーマットのイメージ



イ. 署名暗号アルゴリズムを同法規則 2 条で直接規定しており、技術の進歩に対応した改訂に手間がかかるとともに硬直化する恐れがある。

＜解決策＞

アルゴリズム等の技術基準は別途、独立した規格文書として整理の上、関連法令から参照する構造とするべきではないか。

ウ. 電子証明書に関する国際相互承認

＜解決策＞

欧州 eIDAS 規則における加盟国間で相互承認している eID の要件や UNCITRAL の「IdM and Trust Services」(案)第 2 章 Identity Management の条項に対する適合性の比較を行い、eID や電子証明書の国際相互承認に向けた検討を行う必要がある。

エ. 諸外国における国民 ID カードの公開鍵証明書の利用制限の調査

＜解決策＞

ウの一環として調査を行うべきではないか。

オ. 類似した認定基準との共通化の検討

以下のように、公的個人認証法においては個別の認定制度が行われている。

(ア) 法第 17 条 失効情報にアクセスし署名検証を行う者について以下の 3 つの種別の届出を求めている。

第１項４号　認定認証事業者(署名法第８条)
第１項５号　特定認証業務(署名法２条３項）を行う者であって総務大臣が認定する者
第１項６号　JPKI の失効情報が確認できる署名検証業務を行う者であって総務大臣が認定する者

(イ) 5 号認定の要件

共通要件：設備基準、運用基準は電子署名法の特定認証業務の認定要件と同じ規定となっている。

個別要件：利用者の真偽確認、欠格事項

(ウ) 6 号認定の要件

6 号認定を受けるものは、署名検証サービス事業者であり本来、トラストサービス事業者としての共通要件を満たすべき事業者であると考えられる。

＜解決策＞

5 号認定、6 号認定については電子署名法の特定認証業務等の要件を取り込んだトラストサービスの包括的な監査・認定制度への一体化を検討すべきではないか。

（３）商業登記法

現状の商業登記との GAP 解消策として、以下が挙げられる。

ア．国際連携を考慮した基準

＜解決策＞

現状の商業登記電子証明書は国内の相互運用しか考慮されていないため、将来的な国際連携やクラウド化(リモート署名化)を加味すると、JT2A リモート署名ガイドライン、欧州 eIDAS/ETSI 等の技術基準に合わせていく必要があり、国際連携を考慮した基準の見直しを行うべきではないか。

イ．外部認定のない独自基準

＜解決策＞

外部から認定を受けておらずルート機関からの証明書もないため（商業登記電子認証局の自己署名証明書の真正性を法務省 HP に示されるメッセージダイジェスト（ハッシュ値）により検証する必要があり）、独自基準を見直し、業界標準や、他の認証局と足並みを揃え、トラストおよびリスクアセスメントや情報セキュリティポリシに関する内容を考慮した基準の策定、CP/CPS の公開方法等を検討するべきではないか。

ウ．技術基準（鍵管理基準や証明書プロファイル等）の規定

＜解決策＞

認証局は利用者の秘密鍵に関知していないため、明確な管理基準を定めておらず（PC

上での管理が標準で、IC カード格納はオプション）、鍵の利用目的である EE 証明書プロファイル中の keyUsage の記載もないため、秘密鍵の格納先（媒体、リモート含む）に対する基準の策定や適切な証明書プロファイルの見直しを行うべきではないか。

4.4.4.2 電子認証

公的個人認証サービスでは、電子署名用と利用者認証用の 2 種の電子証明書を発行しているが、電子署名法の認定認証業務においては署名用の電子証明書のみの扱いとなり、利用者認証用の証明書発行は認められていない。また公的個人認証サービスの電子証明書と紐づけられた民間 ID 等、電子認証に用いる eID 手段（eID means）に関する基準は存在せず制度の欠落ポイントとなっている。

関連するガイドラインには、米国の NIST SP 800-63-3「Digital Authentication Guideline」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（平成 31 年（2019 年）2 月 25 日各府省情報化統括責任者（CIO）連絡会議決定）」がある。4.1.3 民事訴訟における効力（10）で検討した効果を得るためにそれらガイドラインを参考とし、トラストサービスの 1 つとして電子認証手段を提供するサービスの共通要件、クオリファイド要件等を策定の上、包括的トラストサービス認定制度の中に位置づけるべきではないか。

4.4.4.3 属性証明

（1）電子委任状法

既存「電子委任状法」との GAP 解消策として、以下が挙げられる。

ア. 海外動向も踏まえ、代理権授与にとらわれない様々な属性（例. 資格属性等）を証明する業務の制度を検討

現行「電子委任状法」は、電子契約等の推進を目的とし、「会社組織等における委任・受任に関する属性」を取り扱っている。しかし、様々なデータに対する信頼性向上の観点からは、委任・受任だけにとらわれず、様々な属性情報を制度として盛り込む必要がある。

例示すると、電子委任状の「取扱事業者記録ファイル方式」では、委任者が作成した PDF ファイルや XML ファイルに記載された委任属性を、電子委任状取扱事業者が電子署名を行う。当該 PDF ファイルや XML ファイルに、委任属性のみならず、例えば卒業証明属性を認めれば、電子的「卒業証明書」を作成することが可能となる。卒業証明は、現行でも依然として紙媒体による発行が主であるが、電子データでの授受が可能となれば、出身校へ出向いたり、郵送したりといったことが省略可能となる（卒業証明取得のための電子申請には、マイナンバーカードによる認証も想定できる）。

なお、EU においては eIDAS 規則の改訂が進行中であり、改訂される内容には「属性の電子証明（e-Attestation of Attribute）」も追加対象となっており、当該動向も参考にできる。

提案段階ではあるものの、「附属書 VI 属性の最低限リスト」として属性項目が挙げられている。

① 住所

② 年齢
③ 性
④ 婚姻状況
⑤ 家族構成
⑥ 国籍
⑦ 最終学歴、称号、許可証
⑧ 専門的な資格、肩書き、権能
⑨ 行政庁による認可及び免許
⑩ 財務データと企業データ

上記の⑦、⑧、⑨は日本においても利用が可能と想定される（⑦や⑧は当該属性証明書、⑨は当該属性免許証、等）。⑩は、企業を識別する属性として、様々な識別子が考えられる（例示すると、「適格請求書発行事業者の登録番号」、「法人番号」、「Legal Entity Identifier（LEI）」や、民間企業コード等が挙げられる）。

なお、属性の確認方法は定義が必要と考えられる。ベースレジストリであれば自明であるが、申請者の情報を基に行う場合も想定される（例として、組織内の役職、等。組織代表者の宣言を信じて発行する、等）。

イ. 「代理権授与」以外の様々な属性を、電子証明書等に記載することについてトラストサービス全体で効果を認める検討

例として、電子署名法に基づく認定認証事業者は、電子証明書の発行時に、発行対象者が所属する組織名称や住所・法人番号等の「組織属性」を真偽確認時に商業登記簿等と照合のうえ電子証明書に格納し発行している。当該電子証明書は主に電子申請（B to G）で平成 13 年（2001 年）から活用されており、電子証明書に格納された組織属性は識別等で重視されている。

また、所謂「士業」に発行される電子証明書も、「資格属性」として真偽確認時にエビデンスと照合のうえ電子証明書に格納して発行し、電子申請等で活用されているのは同様である。トラストサービスでは e シールも検討されているが、これらと同様に属性は重要であり、商業登記法を含め、トラストサービス全体で属性に関する効果を認める必要がある（効果としては、例えば属性が記載された電子証明書は、信頼できる属性として電子的に利用しなければならない、等）。

ウ. ベースレジストリの信頼性

前述した様々な属性を電子証明書に格納する目的のために参照されるベースレジストリは、データが信頼できるソースであることは勿論のこと、データが改竄されていないこと、データの発出元が明示され判明することが必要であり、ベースレジストリから発出されるデータは、トラストサービス（例えば e シール）の活用が重要である。

なお、属性ベースレジストリを民間で作成し情報銀行等で活用することも想定される。この場合においても、当該データの発出元、および通信途中での改竄有無が判明すべきではないか（トレーサビリティ、サプライチェーン等の場面が挙げられる）。

（2）HPKI

ア. HPKI 認証局をトラストサービスの認定制度に位置付けることの是非

(ア) トラストアンカーの公開を(トラストテッドリスト等で)統一的に行うメリット

4.3.8（2）ア でも述べたとおり、保健医療副分野では、HPKI と並び、電子署名法に基づく認定認証業務から発行される証明書に基づく電子署名を利用することも許容される。従って、この分野における電子署名の検証にあたっては、トラストアンカーの公開がトラストテッドリスト等で統一されていることが望ましい。

(イ) 国際相互運用の必要性

証明書のプロファイルは国際標準規格である ISO17090 で規定されているため、構文に関しては国際相互運用性が既に実現されている。ただし、それぞれの資格の持つ意味内容や効力については、各国の事情に応じて制度化する必要がある。制度化の有無も国により異なる状況であり、制度化された場合の、それぞれの資格の持つ権限等の相違についても整理されておらず、実質的には国際相互運用性は実現されていない。このような意味論的な内容は、保健医療福祉分野固有の事情によるところが大きいため、その分野における議論に任せたい。

イ. 認証局の共通要件、個別要件と HPKI CP の差異の確認の必要性

HPKI は保健医療福祉分野の各種資格を厳密に反映するという点で認定認証業務とは証明書ポリシー等が大きく異なるものの、共通要件も少なくないと思われる。HPKI における現行の準拠性監査は、電子署名法に基づく特定認証業務の調査や認定とは関係付けられておらず、監査内容も監査主体も異なっている。また、認証局の事業者自体も、HPKI と認定認証業務に共通の事業者は存在しない。

認証局の共通要件と個別要件を明確化することで、認証業務の提供と監査業務の提供の双方において、社会経済的なコスト削減に資すると思われる。

ウ. 属性を証明する認証業務として HPKI を参考とすべき点

HPKI が対象とする属性、特に保健医療福祉分野の国家資格は、比較的長期にわたり安定的であり、医師資格等を正確に確認できる情報システム（厚生労働省が提供：GUI のみなのでなく API の提供、情報への e シールの付与等が望まれる）が存在するという特徴を持つ。このような場合、証明書に資格属性を含めることは、認証業務の面でも利用面でも有利な点が少なくないと思われる。HPKI におけるこれらの特性を整理し、類似の特性を有する属性については、HPKI と同様な手法を採用することも検討すべきであろう。

エ. 今後のヒアリング調査の必要性

根拠とする法制度の整備、トラストアンカーの公開方法、準拠性監査の民間開放の可能性等については、厚生労働省に対してヒアリング調査する必要があると思われる。

4.4.4.4 タイムスタンプ

(1) 法的効力

ア. タイムスタンプの効力に関する規定

トラストサービスを包括的に定める法律において、トラストサービスの一つとして時刻認証業務を定義し、時刻認証業務が発行するタイムスタンプには、法的手続きにおける証拠としての能力を規定することが必要である。

イ. タイムスタンプの通用性に関する規定

トラストサービスを包括的に定める法律の施行に合わせ、電磁的記録の利活用を容認、推奨する法令やガイドラインについて見直しを行い、時刻認証業務が発行するタイムスタンプを付すことによりそれぞれの法制度の要件を満たすことを明確にし周知を図る必要がある。

(2) 規定すべき内容の範囲

トラストサービスを包括的に定める法律等には、制度の枠組みや手続きのみを規定し、トラストサービス提供業務の技術や運用等に関する要件は、合意規格を参照する必要がある。タイムスタンプにおいては、業務提供事業者により付与される時刻の信頼性が重要であり、技術・運用等にて時刻の品質を確保する必要がある。

そのためには、技術や運用等に関する要件が規格化されている必要があり、国際規格を優先しつつ不足または国内事情に沿わない部分については、国際的な通用性に配慮した上で国内の合意規格を策定しておく必要がある。なお、国内規格は国際規格との整合に配慮が必要であり、我が国が先行して策定する規格は国際規格化を図る必要もあるため、既存の国内及び国際の標準化団体等の機能を活かしつつ、必要性や役割分担を検討の上、トラストサービスに関する規格等に関するイニシアチブを執る機関の設置の検討が必要である。

(3) 適合性評価の仕組み

時刻認証業務に限らず、トラストサービスの分野における適合性評価機関は、4.2.1（4）で示した通り、国際的な整合性をもった基準を参考に仕組みを構築する必要がある。

(4) 電子証明書を発行する認証局

TSA 公開鍵証明書を発行する認証業務について要件を定め、認定の仕組みを構築する必要がある。詳細は、認証局の項を参照されたい。

(5) 認定の公表

タイムスタンプの利用者は、トラストサービスを直接利用する者に限らず、転々流通する対象データの検証において、長期にわたり広範囲となる。認定の公表については、トラストサービス共通の課題として解決する必要がある。詳細は、認定の公表の項を参照されたい。

4.4.4.5 e シール

既存「e シールに係る指針」との GAP 解消策として、以下を想定した。

(1) e シールに係る指針では「一定程度国が関与しつつも、基本的には民間の自主的な仕組み」とされているが、他のトラストサービスと同様「法的効果」を謳い、詳細制度設計が必要である。
トラストサービスは、それぞれ単体で利用することも可能であるが、通常はトラストサービスを組合せて活用されることが多い（例として電子署名+タイムスタンプ、等）。
2021 年時点でトラストサービスは下表のとおり、それぞれ「法的効果」「国の認定制度」「指針に基づく民間自主サービス」と、非統一な状況にある。包括的データ戦略で打ち出されているとおり、トラストサービス全体での「法的効果」を謳う制度設計が必要である。

表 4-16. トラストサービスの現況

トラストサービス	トラストサービスの現況
電子署名	電子署名法に基づき、法的効果が認められている
タイムスタンプ	総務省告示に基づき、国の認定制度が定められている
e シール	総務省指針に基づき、民間での自主サービスが想定されている

(2) e シール用電子証明書を発行する認証業務の設備基準、技術基準、運用基準は、電子署名法に基づく特定認証業務の認定基準の見直しと共に検討すべきである。

認証業務の視点からは、e シール用電子証明書は、設備基準、技術基準、運用基準は電子署名法と同様と想定される（真偽確認方法等、運用の一部を除く）。

- 電子署名用電子証明書：自然人（組織内要員等）に対して発行
- e シール用電子証明書　：法人に対して発行

そのため、「3.2.1 電子署名及び認証業務に関する法律」の「（5）特徴及び課題」で記載したとおりの課題が共通で存在すると考えられ、電子署名法に基づく特定認証業務の認定基準の見直しと共に検討すべきである。

(3) e シール用電子証明書を発行する固有な要件として、以下の継続検討が必要である。

令和３年（2021 年）６月 25 日に総務省から「e シールに係る指針」が公表された。
当該指針において各種基準の概要は言及されているが、詳細内容までは記載されておらず、このまま民間の自主的サービスに任されてしまうと、基準やサービスが統一されず、最終的には利用者がサービスを選択する際に戸惑い、更には不利益を被ることも想定される。また、一部内容は「継続検討」とされていることからも、早急に以下に挙げる内容を検討し公表すべきである。加えて、実際に e シールの認定するにあたり、e シール電子証明書に格納される属性のニーズ調査を踏まえた e シール認証業務や適合性評価機関業務の実証事業を行い、指針の内容を詳細化すべきではないか。

ア. 適合性評価機関に関する基準

e シールを発行する認証業務が「公表する運用規程（CPS）に基づいて正しく運営されている」「設備基準、技術基準、運用基準が適合している」ことを評価する機関に関して、基準を明確にすべき（詳細は、4.4.3.3 適合性評価機関を参照）。

イ. 発行対象の明確化

総務省「e シールに係る指針」では、以下を発行対象としている。

> 「e シール用電子証明書の発行対象すなわち e シールが示す発行元となり得る組織等の対象は、e シールの普及・拡大の観点から、幅広い対象を含めることとし、法人、個人（主に個人事業主を想定）、権利能力なき社団・財団、その他任意の団体等とする。」（「e シールに係る指針」より引用）

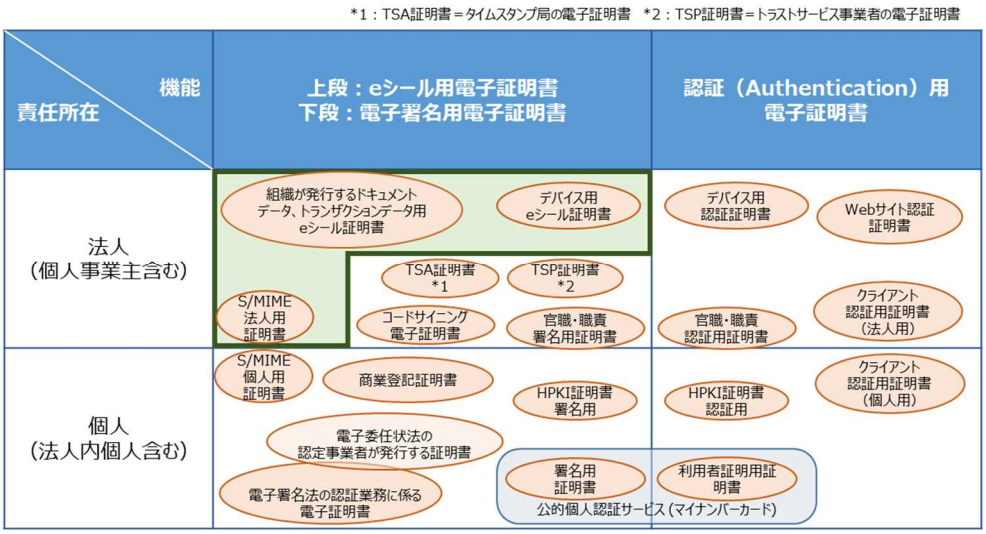
上記以外としては、以下にも言及がある。

> 「他方、それよりも粒度の細かい、組織内における事業所・営業所・支店・部門単位や、担当者（意思表示を伴わない個人）、機器については、e シール用電子証明書の発行対象としてのニーズが一定程度あるものの、その実在性を認証局において正確に確認することは困難であること等に鑑みて、e シール用電子証明書の任意のフィールドである拡張領域に記載できることとし、それらの確認方法や記載方法については２． ３に記載する。」（「e シールに係る指針」より引用）

なお、今後トラストサービス全体を考慮した場合に、以下は e シールとは区別する。理由としては、例えばデバイス用 e シール電子証明書とは管理者や利用方法が明確に異なるためである。(下図 4-17.を参照。緑色網掛け部分が e シールの対象と想定)。

- 各トラストサービスの認証局（CA）の自己署名証明書
- タイムスタンプ局（TSA）証明書、等

図 4-17. 各種電子証明書の区分



ウ. 発行対象の真偽確認方法

前述した発行対象の明確化を含め、詳細な真偽確認方法の確立が必要である。

総務省「e シールに係る指針」では、以下のとおり記載されている。

> ２．３ 組織等の実在性・申請意思の確認の方法
>
> e シールの信頼性は、e シール用電子証明書の発行申請時に必要となる組織等の実在性・申請意思の確認により担保されることになるため、その確認の方法が重要になる。組織等の実在性・申請意思の確認方法の水準により、厳格な確認によって発行される e シール用電子証明書もあれば、簡易な確認によって発行され、低コストで利用しやすいｅシール用電子証明書もあり得る。
>
> 組織等の実在性の確認の具体的な方法については、登記事項証明書や第三者機関データベース等を用いることが想定される。
>
> また、組織等の申請意思の確認の具体的な方法については、電子署名、押印、署名等で行うことが想定される。ただし、当該申請者（電子署名、押印、署名等をした者）が間違いなく当該組織の代表者又は代表者から委任を受けた者（委任状等によって委任を受けていることを確認できる場合に限る。）であることを確認できることが必要となる。
>
> 図 ７にｅシール用電子証明書発行時に必要な組織等の確認の方法の一例を整理したものを示す。レベル３のｅシール用電子証明書の発行にあたっては、十分な水準を満たした組織等の実在性の確認を行う必要があることから、その確認に用いるエビデンスが公的な情報に裏付けられたものであることが必要である。

（★）はデジタルで行える手続

	組織等の実在性の確認	組織（代表者）の意思の確認	組織の代表者の在籍の確認
レベル3	• 商業登記電子証明書による電子署名が行われた利用申込（★）		
	• 登記事項証明書	• 申込書への押印（代表印に係る印鑑証明書が添付されている場合に限る）	
	• 第三者機関が管理するデータベース（*商業登記情報等の公的な機関が管理する情報と照合されたものに限る。*）（★）	• 代表者のマイナンバーカードの署名用電子証明書又は認定認証業務に係る電子証明書等による電子署名が行われた利用申込（★）…① • 申込書への代表者の署名又は押印…②	【甲：意思の確認が①の場合】 • 第三者機関が管理するデータベース（*商業登記情報等の公的な機関が管理する情報と照合されたものに限る。*）に登録されている代表者の住所と電子証明書に記載されている代表者の住所の一致の確認（★） 【乙：意思の確認が②、又は甲で確認できない場合】 • 第三者機関が管理するデータベース（*商業登記情報等の公的な機関が管理する情報と照合されたものに限る。*）に登録されている電話番号等を通じた代表者本人に対する当該申請の有無の確認
レベル2	• 第三者機関が管理するデータベース※（★）		【丙：意思の確認が①の場合】 • 第三者機関が管理するデータベース※に登録されている代表者の住所と電子証明書に記載されている代表者の住所の一致の確認（★） 【丁：意思の確認が②、又は丙で確認できない場合】 • 第三者機関が管理するデータベース※に登録されている電話番号等を通じた代表者本人に対する当該申請の有無の確認

※ 定期的に更新され、信頼できるデータソースとしてみなされるデータベース

図 7 eシール用電子証明書発行時に必要な手続の一例

エ. 電子証明書プロファイル、組織を特定可能な識別子

電子証明書プロファイルについて、総務省「e シールに係る指針」では以下のとおり記載されている。未確定な項目もあることから、詳細を検討し我が国のｅシールプロファイルを確立することが必要である（例として、QC ステートメントやサブジェクト、サブジェクト別名）。

２．４ ｅシール用電子証明書のフォーマット及び記載事項

国内外の類似制度との整合性に鑑みて、レベル３及びレベル２の ｅ シール用電子証明書のフォーマットは、ITU-T X.509 を使用することとする。

e シール用電子証明書の記載事項については、レベル３、レベル２に関わらず、発行対象となる組織等の公式名称、当該組織等を一意に特定可能な識別子、有効期間、公開鍵、署名アルゴリズム、ｅシール用電子証明書の発行者、ｅシールのレベルを判別可能な情報、その他属性情報（営業所、事業所、機器等）等とし、図 8 に記載の一例を示す。

	フィールド名	値（サンプル）
基本領域	バージョン	V3
	シリアルナンバー	WWWWWWWW
	署名アルゴリズム	sha256RSA/sha512RSA
	署名ハッシュアルゴリズム	sha256/sha512
	発行者	**eシール用電子証明書の発行者を識別する情報**
	有効期限の開始時刻	Monday, January 5, 2020 5:00:00 PM
	有効期限の終了時刻	Thursday, January 5, 2022 5:00:00 PM
	サブジェクト	**発行対象となる組織等の公式名称、当該組織等を一意に特定可能な識別子等**
	公開鍵	RSA (2048bit)
	公開鍵パラメータ	05 00 …
拡張領域	認証機関アクセス情報	[1]CA証明書のURL [2]OCSPのURL
	サブジェクト鍵識別子	YYYYYYYYYY
	QCステートメント	**eシールのレベルを判別可能な情報等**
	証明書ポリシー	[1]0.4.0.194112.1.1/0.4.0.194112.1.3 [2] http://xxxxxxxxxxxxx
	サブジェクト別名	**「事業所・営業所・支店・部門名、担当者、機器」や「組織等の和文商号」等**
	CRL配布ポイント	http://xxxxxxxxxxxxxxxCA.crl
	基本制約	Subject Type = End Entity
	鍵使用目的	Non-Repudiation (40)

注） 下線太字は具体的な記載方法について、今後検討が必要な項目

図 8 eシール用電子証明書の記載事項の一例

また、組織を特定可能な識別子についても、以下に引用のとおり「今後検討することが必要」とあり未確定であることから、更なる検討および確立が必要である。

例として、「適格請求書発行事業者の登録番号」、「法人番号」、「Legal Entity Identifier（LEI）」や、民間企業コード等が挙げられる。また、当該識別子を格納する際のルール決めも同様に確立が必要である（例．当該識別子を表現するプレフィクス等）。

> e シール用電子証明書の発行対象の組織等を特定するための識別子については、e シール用電子証明書への記載を必須とする（２． ４参照）が、我が国において官民どちらにおいても複数の ID・番号が共存しており、発行対象を網羅的に管理可能な識別子として使用可能な ID・番号が現状存在しないことに鑑みて、既存の ID・番号も含めて包括的に表現可能な方式（OID：Object Identifier（オブジェクト識別子）等）を軸として今後検討することが必要となる。（以上、「e シールに係る指針」より引用）

オ. 発行されるｅシールのレベル、および当該レベル適合基準、等

総務省「ｅシールに係る指針」では、以下のとおり記載されている。

3 種類に分類されているものの、更なる具体化が必要であり、「特定要件」「クオリファイド要件」を他のトラストサービスと同様に検討すべきである。

> ２．１ ｅシールの分類
> 我が国における e シールは、発行元証明の信頼性を担保するための措置の水準に応じて、以下のとおりレベル分けを行う。
> ・ レベル１： ｅシール
> e シールの定義（電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み）に合致するもの。
> ・ レベル２： 一定の技術基準を満たすｅシール
> 技術的には発行元証明として十分機能することが確認できるもの。
> ・ レベル３： レベル２に加えて、十分な水準を満たしたトラストアンカーによって信頼性が担保されたｅシール
> 組織等の実在性の確認の方法や認証局における設備のセキュリティ要件等について、十分な水準を満たしたトラストアンカーによって信頼性が担保され、発行元証明として機能することに関し、第三者のお墨付き（将来的には国による認定制度等の要否を検討）があるもの。
> なお、レベル１～３の e シールを判別するための呼称については将来決定することが必要となる。
> （以上、「ｅシールに係る指針」より引用）

4.4.4.6 リモート署名/e シール

（1）個別課題

ア. 技術要件

JT2A のリモート署名ガイドラインには、利用者認証及び SIC（Signing interactive component：リモート署名サーバと接続する署名者側のソフトウェア）に関する技術要件や管理策は規定されていない。そのため、日本国内で実施している利用者認証や実装事例等を調査し、EU での SIC 等の検討動向を把握するとともに、技術要件や管理策を検討し、その基準を作成し、同ガイドラインへ追加を行う必要がある。

イ. 評価・認証

同ガイドラインを用いた、評価機関による評価、又は監査機関による監査を実施していない。そのため、同ガイドラインを用いて実際に評価・監査できるかを施行検証する必要である。特に、同ガイドラインのパート 2（署名活性化モジュール）は暗号モジュール試験及び認証制度(JCMVP)、CMVPJCMVP/CMVP（ISO/IEC 19790）又は IT セキュリティ評価及び認証制度(JISEC、JISEC/CC(ISO/IEC 15408)による評価が必要であり、同ガイドラインのパート 3（署名値生成モジュール）は JISEC CC による評価が必要である。そのため、ISO/IEC 17025 に適合した評価機関又は試験機関による評価や試験が求められる。一方で、これらの評価コストや試験コストは高額になる可能性もあるため、効率的な評価や試験を検討する必要もある。

ウ. 公的な基準としての位置づけ

同ガイドラインは、民間の自主的なガイドラインであり、公的な基準として認められていないため、準拠への動機が乏しい。そのため、同ガイドラインを公的な基準として認める等を検討する必要がある。

エ. e シールへの対応

同ガイドラインは、電子署名を前提に記載しており、組織の中で複数名が同一の署名鍵を扱う可能性のある e シールに関しては未検討である。そのため、4.4.4.5 に示した e シールの検討も踏まえ、必要に応じて、e シールとリモート署名が関連する技術や要件については、リモート署名ガイドラインでの追記も検討する必要がある。

オ. リモート署名による署名データであることの確認 e シールへの対応方法

同ガイドラインは、電子署名を前提に記載しており、組織の中で複数名が同一の署名鍵を扱う可能性のある e シールに関しては未検討である。そのため、4.4.4.5 に示した e シールの検討も踏まえ、必要に応じて、e シールとリモート署名が関連する技術や要件については、リモート署名ガイドラインでの追記も検討する必要がある。4.1.3 に示した通り、民事訴訟による効力を考慮した場合、ローカルによる署名ではなく、リモート署名を用いて生成した署名データであることがわかる（確認できる）必要があり、これらの確認方法について検討する必要がある。詳細は、本書 4.1.3 の(12)を参照。

（2）共通課題

ア. 相互運用性

同ガイドラインは、欧州規格を参照しているが、相互運用のためには技術的同等性が不明である。そのため、同ガイドラインと欧州規格との技術的同等性を検証する必要がある。

4.4.4.7 事業者署名型サービス

クラウドでの電子署名サービスがその利用しやすさから、国内外で展開され始めている。

クラウドサービスによる電子署名のうち、事業者署名型のサービスは、署名鍵の電子証明書による方法とは、別の手段で、本人確認と本人意思確認を実施し、事業者の署名鍵による電子署名をすることで、一定程度の対象情報の真正性を担保する方式のサービスである。

この場合、実際に署名した本人から、否認される余地を残すこととなり、実際に海外では、本人否認による裁判が行われ、本人意思が認められず、契約が成立しない判決例も出ており、今後社会的問題に発展する可能性を示している。

事業者署名型による電子契約サービスは、契約当事者のみならず、クラウド環境で介在する事業者および、その事業者が利用するトラストサービス事業者等が存在し、それぞれの責任範囲が複雑に絡み合っている。

このため、サービス利用者による不本意な契約や署名者による否認等の課題を解決するには、サービ

ス利用者においてサービス保証レベルが曖昧な状況で利用されてしまう懸念を払しょくする必要がある。

対象情報の真正性（情報の完全性のみならず内容について正しいこと）を保証するには、以下の 2 点を将来にわたって証明できる必要がある。

A 電磁的記録が合意した時点から改ざんされていないこと。（完全性）
B 契約当時者自身の意思で署名がされたこと。（内容が正しいこと）

このうち、A は、トラストサービスであるタイムスタンプを利用することで解消できると考えられる。実際に我が国において現在展開され始めている事業者型電子契約サービスでは、日本データ通信協会のタイムビジネス信頼・安心認定制度によって認定された事業者が発行するタイムスタンプが利用されている。

一方、B については、対象情報内容についての合意意思の証跡であるべき署名が、本人のみが管理しうるなんらかの手段を利用して、合意意思として処理をしたことを後日証明できるだけの証拠保全が必要になる。

アメリカにおいて、事業者署名型電子契約サービスを利用した業者と被契約者間における契約有効性が争われる裁判があり、被契約者の合意意思の証拠を業者側が提示できず契約無効となった判例がある。

そのとき、裁判所が求めた証拠を下記に記す。これらの証拠保全について、当該サービスを利用する当事者が明確に把握したうえで、サービスを利用するなんらかのルール設定が必要である。

- 誰が被契約者に契約書を送付したか、
- 契約書をどのように被契約者に送付したか、
- 被契約者の電子署名をどのように契約書に記入したか、
- 署名された契約書を誰が受け取ったか、
- 署名された契約書をどのように業者に返却したか、
- 契約書に実際に署名した人物として被契約者の身元をどのように確認したか
- 契約書が署名された具体的な場所
- 契約書が署名された時間
- 契約書が署名されたときに被契約者が存在していたことをどのように確認したか。

4.4.4.8 署名生成装置

署名生成装置についてその技術基準を整備し、評価/認証制度を確立し、電子署名及び e シールについて安全な署名/シール生成装置を利用して生成されているか否かを識別できる仕組みを設けるべきである。

ア. 評価/認証制度についてはこれまでの評価/認証実績、eIDAS 規則との同等性及び製品ベンダーにおける評価/認証取得コスト等の観点から独立行政法人 情報処理推進機構が運

営するＩＴセキュリティ評価及び認証制度（JISEC）或いは暗号モジュール試験及び認証制度（JCMVP）を用いることが望ましいと考えられる。

イ. 技術基準については eIDAS 規則における適格電子署名/シール生成装置の基準をベースに、必要に応じて我が国独自のプロテクションプロファイルを整備すべきである。

ウ. 電子証明書のプロファイルに、対となる秘密鍵が安全な署名/シール生成装置で保護されていることを示す識別子を含めることで、署名/シール検証者が安全な署名生成装置の利用について検証できるようにすべきである。

4.4.4.9 今後のトラストサービス

（1）電子内容証明送付業務（ERDS）

取引の安全性のためには、紙の場合の内容証明郵便に相当する電磁的記録の送信が必要となる。内容証明郵便と同様な効果を持つ電子内容証明送付は、電子取引情報の授受システム等での必要性が認識されており、広範な利用が予想されている。その一方で、送付の実施は、あらかじめ登録された受信者にしか行えないため、制度の普及には懸念も持たれている。

今後の取り組みとして、早期に電子内容証明送付及びそのクオリファイドの基準を明確にし、公的又は民間の電子内容証明送付業務を立ち上げるとともに、一定の範囲の者（国・地方公共団体と取引関係にある者や、上場企業等が考えられる）には、電子内容証明送付業務への利用者登録を義務付ける方法が考えられる。

（2）検証業務

トラストサービスの利用者とりわけ依拠者は、トラストサービスが関与して作成されたデータ（電子署名データ、e シールデータ、タイムスタンプ等）の正当性を検証する必要がある。しかし、利用者に、正しく検証する能力があるとは限らず、また、訴訟等の手続において正当性を証明することには困難がある。

こうした問題を解決するため、検証業務及びクオリファイドに関する基準を早期に明確にし、公的又は民間の検証業務を立ち上げるべきである。なお、検証業務については、司法における活用が望まれるため、裁判所又はその指定を受けた者が行うことも考えられる（裁判所指定の検証業務による検証結果は、裁判において一定の効果を持つ等の在り方が考えられる）。

（3）保存サービス

電子署名、e シール、タイムスタンプは、電子データや文書につき、本人の意思、発出起源、存在時刻等を証明できるが、そのためには利用者が対象の電子データや文書と関連付けて管理する必要がある。また、それらの有効性を長期にわたって維持するためには、長期署名フォーマットに従って、タイムスタンプを重ねて付与する等の措置を利用者の責任において実施する必要がある。更に、対象文書等は利用者の管理下にあるため、文書そのものが消去されてしまうことがあり、その場合、対象文書等の真正性はもとより、その文書が存在していたこと自体を証明することすら困難となり、それに伴う事象（取引を実施したという事実、組織内で意思決定が行われたという事実等）そのものが隠滅される恐れがある。

こうした事態に対処するため、電子データや文書の完全性、出所の正確性、存在時刻、法的有効性を必要な期間にわたって保証するために、電子データまたは文書の受領、保存、削除、暗号化による保護等を確実に行うサービスや制度を創設することが考えられる。その際には、公証人による電子公証制度に基づく電子公証サービスや国立国会図書館のオンライン資料収集制度（e デポ）等の類似と思われる既存サービスとの間で趣旨や法的効果等の相違や関係を整理した上で検討する必要がある。

（4） Web サイト認証

Web サイト認証は Web サーバの管理主体に対して認証局が電子証明書発行し、管理主体がその利用者に対して自身の身元を証明する仕組みであるが、現状我が国においては制度が存在せず、各ブラウザベンダの独自制度に基づいて国内の認証局が信頼できる認証局として登録されているのが実態である。Web サイト認証の電子証明書を発行する認証局の信頼性については、各ブラウザベンダが採用する基準及び監査制度（WebTrust for CA 及び ETSI）が用いられており、国内の認証局もこれらの基準及び制度に基づいた評価を受けている。

このような現状を踏まえた上で、次の観点から我が国においても Web サイト認証の信頼性を保証する制度を整備すべきである。

ア. Society5.0 及び DFFT が実現するデータドリブン型の社会においては、Web サーバの管理主体の信頼性についてブラウザに拠る検証以外の方式が必要となる。

イ. 認証局事業者の監査及び認定対応コストを抑える為には、複数のトラストサービスの認定を同時に取得可能な制度とすることが必要であり、また、我が国の制度における評価及び認定結果を以って各ブラウザベンダに対して信頼できる認証局としての登録を要請できるようにすべきである。

4.5　国際的な相互承認の検討

Society5.0 の実現に向け、ヒト、モノ、システム間での高度な情報連携が進み AI 含めデータの自動連携が社会システムの基盤となり、デジタル経済を支える信頼ある自由なデータ流通（DFFT）が国際社会の中で拡大することが想定されている。欧州における邦人のデジタル手続き（例、国際間取引や決済、会社法で定める決算書類等や関税書類への電子署名）や日本における外国人のデジタル手続き（成長戦略フォローアップ（令和３年（2021 年）６月１８日閣議決定）で打ち出された対日直接投資促進戦略での法人設立登記申請等）を見据えたトラストサービスの国際相互承認の早期の実現が望まれる。

トラストサービスの国際相互承認の実現に向けた検討には以下の ４ つの観点での同等性の確認が必要となる。

(ア) 法制度
(イ) 監督・監査
(ウ) 技術標準
(エ) トラストアンカー間の接続の仕組み

４つの観点に対する国際相互承認のために必要な施策は

表 4-18. 国際的な相互承認に向けた必要施策

	項目	国際相互承認のために必要な施策
1	法制度	・トラストサービスの認定に係るフレームワークの同等性 ・国（又は、民間機関）による認定フレームワークの確立 ・トラストサービスの効果の同等性
2	監督・適合性評価	・適合性評価機関の要件の同等性 ・指導・監督の仕組みの確立
3	技術標準	・技術標準の作成・維持の体制の整備 ・技術標準の同等性に関する検討
4	トラストアンカー間の接続の仕組み	・クオリファイドサービスを公表 ・トラステッドリスト方式とブリッジ方式の併用 ・それぞれの方式において国際間の相互参照や相互接続を行う必要があり、具体化策や管理体制に関し協議が必要