「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」

最終報告概要

令和3年（2021年）8月31日

＜報告書の章構成＞

＜報告書の章構成＞

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、以下の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

国内法令等の調査では、「トラストに関するワーキングチーム」（以下、TWTと呼ぶ）で示された、下記の分類に従って、各要件、規格等の整理を行った。

（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。

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

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、主に以下の観点から調査する。

① 日本において、包括的なトラストの枠組み整備に関係する法制度

② 日本において、包括的なトラストの枠組み整備に関係する仕組み（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 国内外のトラストに係る取り組み動向及び課題の調査

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）海外

① EU：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）
Identity Management and Trust Services

③ 認証局にかかわるWebTrust監査基準

（2）国内法令等

① 電子署名法、公的個人認証法、商業登記法、電子委任状法

② 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 時刻認証業務の認定に関する規程（令和3年総務省告示第146号）

④ ｅシールに係る指針（総務省）

⑤ リモート署名ガイドライン（民間）

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、及びHPKI

2.1.5 ニーズ調査の対象の洗い出し（案）

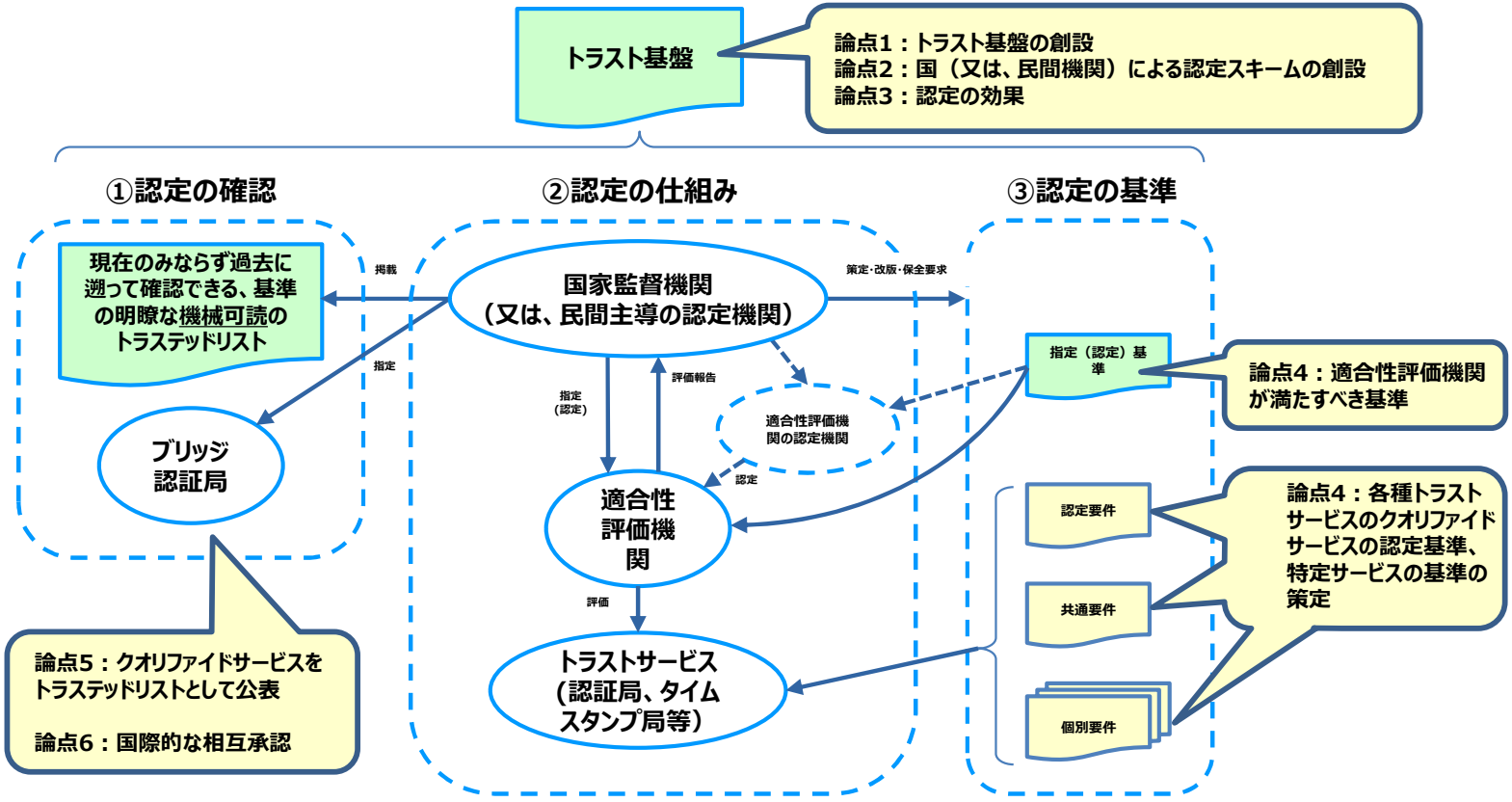
2.2 日本における包括的なトラストの枠組み整備に必要な論点とその具体的な在り方の調査

2.2.1 調査事項

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。



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

（1）欧州では、電子署名の法的効力等を規定した電子署名指令に代わり「eIDAS規則」が2014年7月に採択され、その適用範囲は電子署名を含むトラストサービスとeIDに拡大された。

（2）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。

（3）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る。

（4）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。

（5）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。

（6）本調査研究では、eIDAS規則の構成に従って、各条項の内容を最近（2021年6月）の改定案を含み概要を整理した。

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

3.1.2　UNCITRAL：Identity Management and Trust Services

（1）国際連合の、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。

（2）2015年に採択されたSDGsのターゲットの一部とも関連し、2016年からIdentity Management（IdM）and Trust Services について詳細な議論が開始されたところである。

（3）本調査研究では、IdM and Trust Services の条項案の概要を抽出し、トラストサービスの基本原則として定めている事項や定義、法的効果等を整理した。

3.1.3　認証局にかかわるWebTrust監査基準

（1）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ー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。

（2）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。

（3）本調査研究では、WebTrust監査基準と電子署名法の認定認証業務の要件の比較を行った。今後、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

トラストサービスに関連する以下の各国内法令等の現状の課題、また規定しているトラストサービスの要件、課題を抽出し、共通要件、個別要件、認定要件として整理した。

＜対象法令等＞

3.2.1　電子署名法
3.2.2　公的個人認証法
3.2.3　商業登記法
3.2.4　電子委任状法
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
3.2.6　時刻認証業務の認定に関する規程
3.2.7　ｅシールに係る指針
3.2.8　リモート署名ガイドライン

3.2.1 電子署名法

1. 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）
   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（電子署名法第3条）
   ①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。
   ②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（電子署名法第4条～第14条）
   （１）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。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。
   ・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。
   （２）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。
   ・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。
   ・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。
   ・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。
   （３）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。
   （４）押印における2段の推定の1段目（本人による電子署名データであること）の推定基準が未整備

3.2.2 公的個人認証法

1. 調査対象法令
   （１）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
   （２）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
   （３）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
   （４）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
   （５）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

2. 特徴
   （１）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。
   （２）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
   （３）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ている。
   （４）電子証明書の発行番号の利用制限がある。

3.2.3 商業登記法

1. 特徴

（1）商業登記に基づく電子認証制度を提供

商業登記法12条の2および商業登記規則33条の2～18に規定

（2）商業登記簿で管理される「法人格の存在」「代表権の存在」「法人代表者としての本人性」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。

（3）GPKIとの相互運用を行うため、商業登記認証局のCP/CPSを定めている。

（4）政府「デジタル社会の実現に向けた重点計画（2021年3年6月）」にて、2021年度中に証明書無償化可否およびクラウド化検討を行い、2025年度までに新規システムの運用開始を目指す、と言及している。

2. 課題

（1）商業登記認証局のCP/CPSはGPKIとの相互運用をするための管理規定であり、認証局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。

（2）上記CP/CPSは電子署名法上の認定認証業務の認定要件と比較し、主に以下の点で異なる。

① 商業登記電子証明書にKeyUsageの記載がなく、鍵の利用目的が不明確

② 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のメッセージダイジェストで検証要

（3）商業登記電子証明書のクラウド化にあたり、リモート署名等の実装は、将来的な国際連携も加味し、JT2Aリモート署名ガイドライン、欧州eIDAS/ETSI等の技術基準を考慮して検討するべきである。

3.2.4 電子委任状法

1. 特徴

（１）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。

（２）「代理権授与」属性に関する定義のみが存在。

（３）電子委任状に関する3方式（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。

（４）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）。

（５）電子署名法・関連法令を参照する規定が存在（電子委任状法第2条第4項第1号）。

（６）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。

2. 課題

（１）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の検討が必要である。

（２）「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が必要である。

（３）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。
その場合には、ベース・レジストリから発出される情報へのトラストサービス（例えばeシール）の利用や、API等による自動連携の検討が必要である。

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

1. 電子文書の通用性

（1）電子文書の通用性についての包括的な規定はない（契約方法自由の原則が、民法522条2項に規定されているが、法令による例外を設定することは可能）。

（2）遺言書等、電子文書の有効性が否定されているものもある。

（3）個別規定で電子化可能にしている例が多い。条例も含めて、逐一確認する必要があり、新規事業にあたって、網羅的な調査は困難であり、包括的な規定が望まれる。

2. 電子署名の通用性

（1）JPKI、商業登記、認定認証業務の電子証明書を要件とする手続きがある。

（2）電子署名法2条1項の電子署名を要求している法令は多い。しかし、2条1項の要件には身元確認がない等、2条1項の電子署名を求める意義・効果が不明確である。また、2条1項と同内容の要件を、個別に記載している例もあり、2条1項との異同を法令ごとに個別に確認しなければならない状態にある。

（3）真正な成立が推定される電子署名を（たとえば、特定電子署名と）定義し、この定義を参照するべき。

（4）電子署名法2条1項への適合性の判定に経済産業省のグレーゾーン解消制度を用いている例がある。これは、制度趣旨に反するし、既存業者は対象にならない等の問題がある。公的又は民間の判定機関が望まれる。

3. タイムスタンプの通用性

（1）電子帳簿保存法では、日本データ通信協会の認定タイムスタンプを求めている。

（2）クオリファイドタイムスタンプには、民法施行法5条にいう確定日付の効果を認めるべき。

3.2.6 時刻認証業務の認定に関する規程

1. タイムスタンプ関連規程の経緯

（1）2004年～2005年：e文書法施行に備えて、電子記録の真実性を保証する重要性が認識され、2004年11月に総務省より「タイムビジネスに係る指針」が提示され、電子文書の存在証明の基準として、2005年2月に「タイムビジネス信頼・安心認定制度」が日本データ通信協会にて創設された。

（2）2019年～2020年：総務省において「トラストサービス検討WG」が開催され、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との結果を受けて、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検討を掲げ2020年に「タイムスタンプ認定制度に関する検討会」が開催された。

（3）2021年4月1日：上記検討会のとりまとめを反映し、総務省設置法のもと、告示第146号及び実施要項が発出された。

（4）2021年6月24日：指定調査機関として（一財）日本データ通信協会が指定された。

2. 告示146号および実施要項の特徴

（1）タイムスタンプの時刻源は、日本標準時であるUTC（NICT）。

（2）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。

（3）総務省のHPにて、認定事業者および業務等が公開される。

（4）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。

（5）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。

（6）民間認定時には認められていなかったTSA自ら時刻の信頼を確保する方式が加えられた。

（7）認定の有効期間は2年間。

3. 課題

（1）タイムスタンプの法的効果に関する規程が無い。

（2）TSA公開鍵証明書の発行業務の監査に係る制度が無い。

（3）公開される情報は、機械可読でなく、非改ざん処理も施されない。

（4）タイムスタンプ時刻は日本標準時と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。

（5）秘密鍵、電子証明書等の定義が限定的であり、トラストサービスで共通定義が必要と思われる。

（6）制度と審査基準が告示と実施要項に規定されており、指定調査機関と認定事業者の基準が書かれている。基準は別途規格等として整備すべき。

（7）総務大臣認定のタイムスタンプを利用を推奨・規定する省令・ガイドライン等が未整備である。

3.2.7　eシールに係る指針

1. 特徴

（1）総務省が2021年6月25日に『eシールに係る指針』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。

（2）「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

（3）「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）

2. 課題

（1）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。

（2）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。

（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。

① 適合性評価機関に関する基準

② 発行対象の明確化

③ 発行対象の真偽確認方法

④ 電子証明書プロファイル、組織を特定可能な識別子

⑤ 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

3.2.8 リモート署名ガイドライン

1. 特徴

（1）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年度報告書※に記載されている。

（2）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（電子署名法の主務三省である法務省、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

（1）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程されていない。

（2）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）

（3）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。

（4）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。

（5）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。

※電子署名法研究会（平成28年度第4回）-配布資料（METI/経済産業省）
https://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/h28_04_haifu.html

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、商業登記に基づく電子認証制度、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（案）

1. ニーズ調査の必要性

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、以下の２点の考え方が重要である。

（１）現在の社会実装状況の的確な把握と課題を抽出し、今後必要となる要件を整理すること。

（２）トラストを期待する利用者・利用組織とトラスト基盤の仕組みの二つの視点からニーズを掌握し、経済的合理性を実現すること。

「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：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：関係府省庁へのに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。

2.トラストサービスのニーズを調査するにあたり、以下の4つの観点からその必要性を考察し、今後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体のニーズ

（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

３．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係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り、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体のニーズ

1. 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
   - （1）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
   - （2）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
   - （3）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
   - （4）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
2. 産業分野別の個別業務でのニーズ
   - （1）調査分野例
     - 「デジタル社会の実現に向けた重点計画/第２部デジタル社会の形成 に向けた基本的な施策/２．徹底したUI ・ UX の改善と国民向 けサービスの実現/（８）準公共・民間分野のデジタル化の推進の方向性」より想定
   - （2）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」）
   - （3）相互連携分野
     - 電子インボイス、契約・決済、スマートシティ
3. トラストサービスの利便性向上に対するニーズ
   - リモート署名、リモートｅシール、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
4. 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、監査報告書等
5. トラストサービス包括的な認定制度に対するニーズ
   - 認証局、タイムスタンプ局等のトラストサービス事業者、調査機関、監査会社等へのヒヤリング調査
6. 調査例
   - 保険会社でのｅシールによる費用削減効果

3.4.3 トラストサービスの基準のニーズ

1. 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）電子署名を利用するサービスにおいて、デジタル認証の基準※が示されないまま利用が進んでいる。

電子署名において、電子署名法2条1項、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、例えば以下の制度が利用者の信頼の拠所となっている。

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。

（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、登録手続きや技術・運用等の要件が明確になっていないため、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。

① 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。

② 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。

2. 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。

※デジタル認証の基準：本人確認（IAL：Identity Assurance Level）、ユーザ認証（AAL：Authentication Assurance Level）等

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。

2. 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。

3.4.4 トラストサービスの認定のニーズ

3. 新たな形態のトラストサービス

(1) 電子認証に対する制度はどうあるべきか*1

- eID means（電子認証手段）IALとAAL
- Credential（Identity）Service Providerの基準はどうあるべきか？
  (電子証明書、OTP、生体認証)
- 認証サービス（認証連携）事業者　FAL
- 民間IDとマイナンバーカードの署名用電子証明書との紐づけ*2
- 民間IDと認定認証業務の電子証明書との紐づけ
- 認証用電子証明書に対する業務の認定
- NIST　SP800 63-3に準拠した日本としての基準を整備すべき

*1　UNCITRAL A/CN.9/WG.IV/WP.153　58行目

legal guidance may be needed on the conditions to be fulfilled to provide legal recognition to identity credentials and verifications and to the output of trust services.

*2　＜デジタル・ガバメント実行計画（2020年12月25日閣議決定）＞

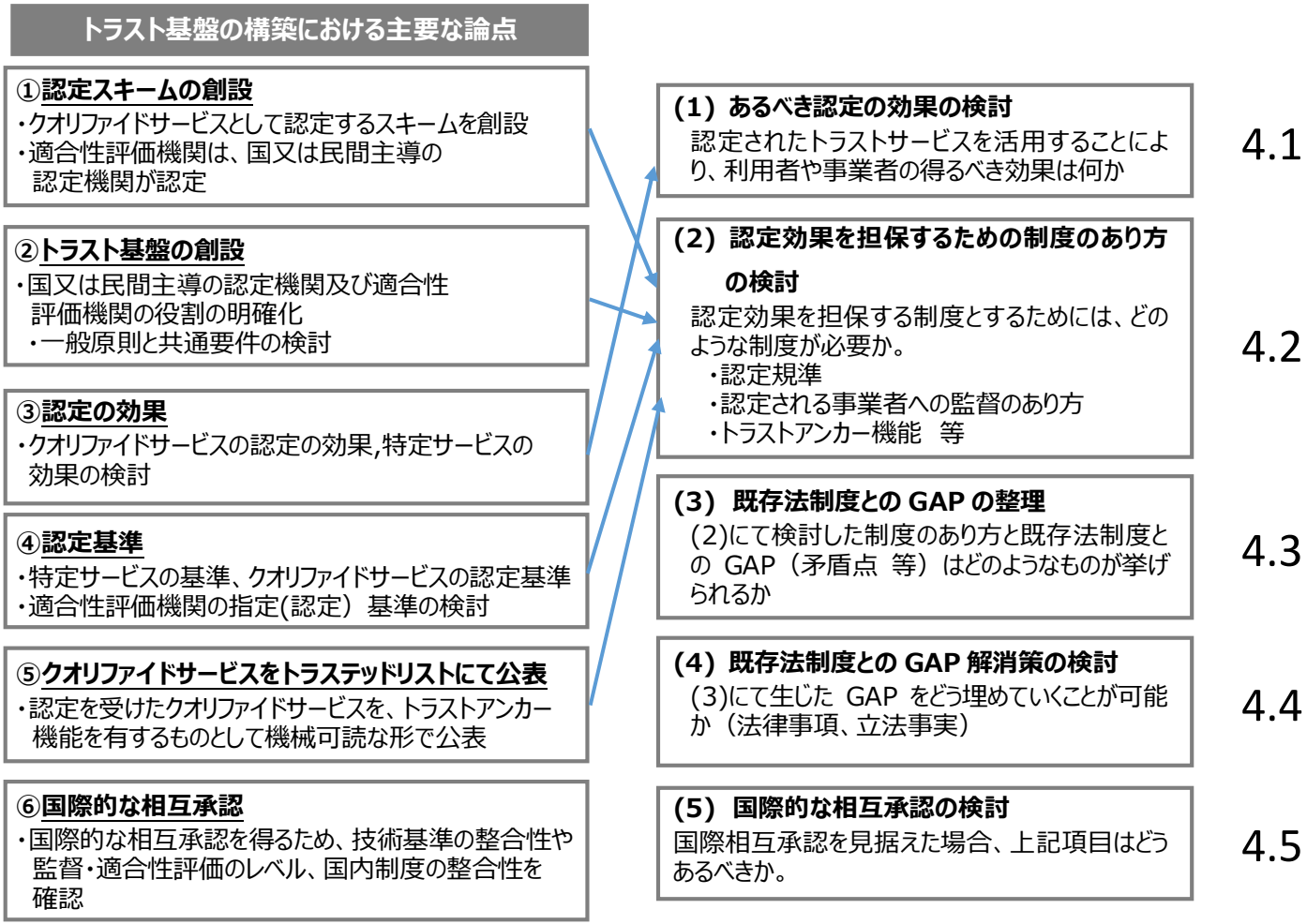
別添１「マイナンバー制度及び国と地方のデジタル基盤の抜本的な改善に向けて（国・地方デジタル化指針）
④民間IDとマイナンバーカード電子証明書との紐づけの推奨」より

(2) 従来の認定制度に係らない新たなサービス形態の出現

- マイナンバーカードの署名用電子証明書を用いた本人確認と5号認定を受けない特定認証業務の組み合わせ
- 秘密分散型の署名生成装置（SCD）の認定
- その他

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（第７回）の資料８－１　包括的データ戦略（案）の概要（https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai7/siryou8-1.pdf ）で示された「トラスト基盤の構築における主要な論点」を基にして、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について、下記のように分類して調査を実施した。



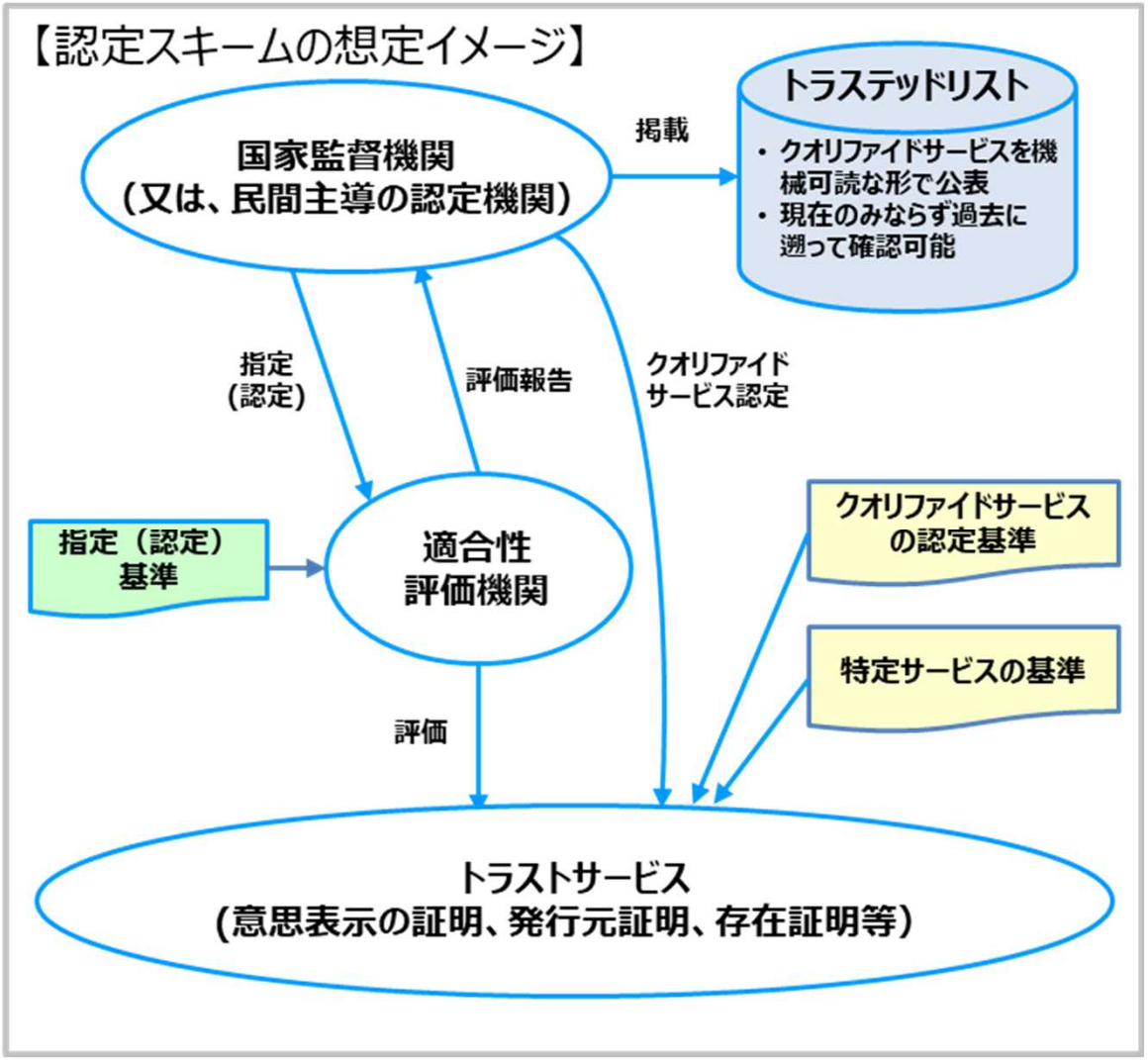
なお、本調査結果を基にして、更に、トラストサービスに関する「民間ニーズ」及び「国の制度に基づく手続き」をそれぞれ調査し、血の通ったニーズを抽出していくことが求められる。

4.1 あるべき認定の効果の検討

1. 認定されたトラストサービス等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。
2. 通用性（4.1.2）
   - ① 公的手続だけでなく、民間取引における通用性も対象とする。
   - ② eIDAS等には、包括的な通用性の規定（電子的であるという理由での効力否定の禁止）があるが、我が国でもこれに対応する包括的な通用性の規定を置くべき。
   - ③ 個別の手続での通用性（許容性）は、一般法の定義を参照する形で行い、個別の法令での具体的規定は避けるべきである。一般法では、トラストサービスやその生成情報につき、無印・特定・クオリファイドをそれぞれ定義するべきである。
3. 民事訴訟における効力（4.1.3）
   - ① 電子署名法3条カッコ書きを満たす電子署名には、真正な成立の推定を認める（現行通り）
   - ② クオリファイド電子証明書に基づく電子署名データにより、電子署名が行われたことを推定すべき。
   - ③ クオリファイドタイムスタンプにより、存在時刻とその後の非改ざんを推定すべき。また、確定日付の効力を持たせるべき。
   - ④ シール、属性証明付電子証明書、リモート署名、検証業務、電子内容証明送付、電子認証がクオリファイドの場合の民事訴訟における効力を規定すべき（推定規定）。

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（https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai7/siryou8-1.pdf ）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。



4.2 認定効果を担保するための制度のあり方の検討

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

（１）認定制度を通じて、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。

（２）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。

2. 監督機関

（１）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、認定制度全体を企画立案。

（２）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）に任務を委ねるかについては、更なる検討が必要。

3. トラストサービスの公的な基準を策定する機関

（１）EUの欧州標準化機関（ETSI等）、米国標準技術研究所（NIST）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。

（２）国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）にするのか、様々な選択肢から検討する必要。

4. 適合性評価機関

（１）クオリファイドトラストサービスの認定においては、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。

（２）適合性評価機関が満たすべき基準の策定及び中立・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。

4.2 認定効果を担保するための制度のあり方の検討

4.2.2 認定制度の具体的なプロセス

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

（１）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。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。

（２）適合性評価機関が満たすべき要件についても、ISO等国際標準の準拠した国内の基準を作成し、公開。

2. 適合性評価機関による評価

（１）民間の適合性評価機関は、トラストサービス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、当該トラストサービス事業者に提供。

（２）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を申請。

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

（１）監督機関は、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、認定証を発行とともにトラステッドリストに登録。

（２）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、その認定を取り消す。

4.2　認定効果を担保するための制度のあり方の検討

4.2.3　認定制度における各種規定類の構造

1. トラストサービスに共通な事項

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、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

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

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。

4.3 既存法制度とのGAPの整理

4.3.1 電子署名法
4.3.2 公的個人認証法
4.3.3 商業登記法
4.3.4 電子委任状法
4.3.5 時刻認証業務の認定に関する規程
4.3.6 ｅシールに係る指針
4.3.7 リモート署名ガイドライン
4.3.8 その他

4.3.1 電子署名法

現状及び課題

1. 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）

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（電子署名法第3条）

（１）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。

（２）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（電子署名法第4条～第14条）

（１）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。

① 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。
② 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。
③ 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。
④ 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。
⑤ 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。
⑥ 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。

（２）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。

① 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。
② 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。
③ 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。

（３）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。

（４）押印における2段の推定の1段目（本人による電子署名データであること）の推定基準が未整備である。

4.3.2 公的個人認証法

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

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：法17条1項6号 → 施行令9条2号 → 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：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ある

①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（電子署名法第8条）

第1項5号　特定認証業務（電子署名法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

②5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

③6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

制度のあり方とのGAP

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

課題

（1）電子契約に関する代理権授与属性に限定

代理権授与属性以外（例．個人：卒業証明、専門資格等、会社組織：行政許認可、免許、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、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

電子署名法に基づく認定認証事業者が発行する電子証明書は発行対象者の「組織属性」を確認して発行され、主に電子申請（B to G）で2001年から活用、組織属性は識別等で重視されているものの、電子署名法施行規則第６条８号により組織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。

（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、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や改竄有無が判明しない状況では、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かねない。

4.3.5 時刻認証業務の認定に関する規程

総務大臣認定制度とあるべき姿とのGAP

（１）法的効力

①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年総務省告示第146号）」第2条に、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が、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。

②タイムスタンプの通用性に関する規定

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

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

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。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

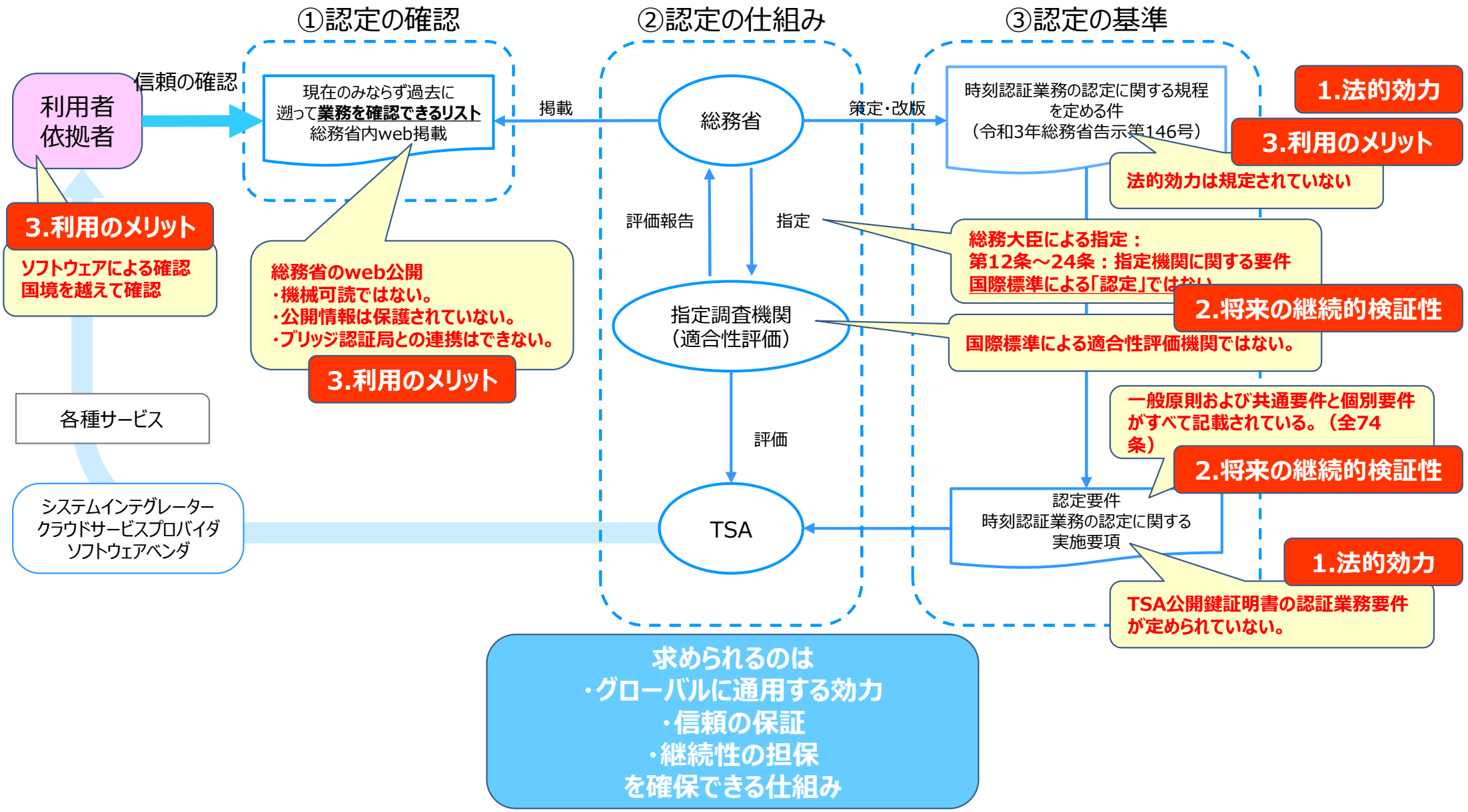
タイムスタンプの生成に用いる秘密鍵とペアとなる公開鍵の証明書（TSA公開鍵証明書）を「信頼できる認証事業者」から発行されたものであることを認定の要件としているが、TSA公開鍵証明書を発行する認証業務については要件が定められておらず、その安全性等は認証事業者に依存することとなっている。

（５）認定の公表

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。

【参考資料】4.3.5 時刻認証業務：総務大臣認定制度とあるべき姿とのGAP



4.3.6　ｅシールに係る指針

課題

（1）法的効果の欠如

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：総務省の認定制度」「eシール：総務省指針に基づく民間自主サービス」と、非統一な状況にある。

トラストサービスは単体利用もさることながら、複合活用が多い（例．電子署名+タイムスタンプ、等）。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し、利用しずらい状況となる。
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）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シールに係る指針で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ない。発行業務基準の不一致は、利用者の混乱を招き、不利益を被りかねない。

①適合性評価機関に関する基準

②発行対象の明確化

③発行対象の真偽確認方法

④電子証明書プロファイル、組織を特定可能な識別子

⑤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

（1）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。

（2）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。

（3）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。

（4）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. 共通課題

（5）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、LGPKI>

1. 現状（GPKI）

（１）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。

（２）行政情報システム関係課長連絡会議了承のもとCP/CPSが整備され、総務省が運営。

（３）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。

（４）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。行政機関の処分権者である大臣等の官職証明書を発行。

2. 現状（LGPKI）

（１）LGPKIは「総合行政ネットワーク基本規程第３条第３項」の規定に基づく地方公共団体組織認証基盤であり、LGPKI組織認証局等から構成。

（２）「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が整備され、地方公共団体情報システム機構（J-LIS）が運営。

（３）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。GPKIブリッジ認証局と相互認証。

3. 課題

（１）GPKI/LGPKIの認証局のCP/CPSは、法律に直接基づかない内規等に基づき整備。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。

（２）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。しかし現状では私文書（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。

（３）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。

4.3.8 その他

<HPKI>

1. 現状

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

（２）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。

（３）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」で規定。

（４）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」によって実施。

（５）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（hcRole：healthcare Role）及び属性の定義がISO17090（Health Informatics -Public Key Infrastructure）で規定。

（６）属性として、26種類の保健医療福祉分野の国家資格（医師、歯科医師、薬剤師、看護師等）と5種類の医療機関の管理責任者（病院長、管理薬剤師等）としての資格が定義。

（７）トラストアンカーとなる厚生労働省ルートCAの証明書が、厚生労働省のリポジトリで公開。

2. 課題

（１）HPKIの認証局のCP/CPSは、法律に直接基づかない厚生労働省の内規等に基づき整備。

（２）準拠性監査は、電子署名法に基づく認定認証業務の調査とは関連付けられずに実施。

（３）保険医療福祉分野ではHPKIに加え、認定認証業務の利用も許容されるが、トラストアンカーが統一的に扱われていない。

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

（１）電子署名の場合は、「認証業務」が「電子証明書」を発行し、その電子証明書に基づいて「電子署名」が行なわれ、「電子署名データ」が生成される。以下の区分に従って、それぞれ定義する。

- トラストサービス： 認証業務
- 情報（データ）： 電子証明書・電子署名データ
- 措置： 電子署名

2. 無印・特定・クオリファイドの考え方

（１）トラストサービス等（情報や措置を含む）のそれぞれについて、無印・特定・クオリファイドの定義を行う。

（２）トラストサービスと発行情報等とは同一のレベルとする（例：特定認証業務が発行する電子証明書は特定電子証明書）

3. 定義の対象

（１）監督機関、適合性評価機関、トラストサービス、トラストサービス事業者、署名者、利用者、依拠者

（２）電子署名、電子署名データ、電子証明書、属性証明付き電子証明書、電子署名データ生成装置

（３）eシール、eシールデータ、eシール用電子証明書、eシールデータ生成装置

（４）タイムスタンプ

（５）認証業務、リモート署名業務、eシール用認証業務、時刻認証業務、保存業務、電子内容証明送付業務、事業者型電子署名業務

（６）電磁的記録

4.4.2 一般原則

1. 監督・指導

トラストサービスに対する監督、クオリファイド等の認定等に関する権限を持つ監督機関（国又は国が指定する機関）を規定し、トラストサービスに対する指導の機能を持たせる。

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固有の規定を追加するか、故意・過失についての立証責任を規定するか、等を検討すべきである。

3. 電子文書等の通用性

電子文書、電子署名、eシール、タイムスタンプ等についての、一般的な通用性を規定すべきである。個別法では、一般的な定義を参照して、手続等における通用性を規定することとする。

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）のリストを公開し、通用性を明示すべきである。

5. 表示規制

（１）クオリファイドの表示について規定をおくべきである。

（２）リモート署名業務や電子署名データ生成装置の利用を電子署名データ等に表示する規定を検討すべきである。

6. 国際協調

トラストサービスが関与して生成された情報の海外での通用性の確保を検討すべきである。

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

（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。

4.4.3 共通事項

4.4.3.2 トラストサービスの認定

（１）監督機関

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、認定制度全体を企画立案。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）に任務を委ねるかについては、更なる検討が必要。

（２）トラストサービスの公的な基準を策定する機関

EUの欧州標準化機関（ETSI等）、米国標準技術研究所（NIST）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。国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）にするのか、様々な選択肢から検討する必要。

（３）適合性評価機関

クオリファイドトラストサービスの認定においては、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。また、適合性評価機関が満たすべき基準の策定及び中立・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。

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。

①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
②適合性評価機関による評価
③監督機関による認定
④監督機関によるトラステッドリストへの登録

4.4.3 共通事項

4.4.3.3 トラストサービスの公表等

（１）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ある。
（２）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ある。
（３）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ある。
（４）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ある。
（５）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等を確認できることの検討が必要である。
（６）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ある。
（７）クオリファイドトラストサービスを確認する仕組みは、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ある。
（８）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、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、マイルストンを定めて段階的に整備すること検討すべきである。

4.4.3 共通事項

4.4.3.5 規格の参照

（１）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。
（２）信頼の基準は明確であり、その準拠性を利用者が利用目的によって判断できる必要がある。
（３）基準には、技術要件、運用要件等があり、技術革新や環境変化にあわせて逐次更新されるものである。
（４）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する制度が運用されることが求められる。
（５）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、国際標準化機関としてはISO/IEC及びITU-T、EUではCEN及びETSI、USAではNIST、インターネット社会ではW3C、IETF、CAB/F及びCSC等がある。
（６）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。
（７）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

4.4.4.1　電子署名
(1) 電子署名法
(2) 公的個人認証法
(3) 商業登記法
4.4.4.2　電子認証
4.4.4.3　属性証明
4.4.4.4　タイムスタンプ
4.4.4.5　ｅシール
4.4.4.6　リモート署名/eシール
4.4.4.7　事業者署名型サービス
4.4.4.8　電子署名/eシールデータ生成装置
4.4.4.9　今後のトラストサービス

4.4.4.1　電子署名

（１）電子署名法

ア.　法人等の組織向けの電子証明書の発行とeシールの法的効果を明らかにする。
イ.　電磁的記録の真正な成立の推定について、リモート署名における解釈を明らかにする。
ウ.　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。
エ.　特定認証業務の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を明らかにする。
オ.　特定認証業務の具体的な基準を、公的な基準を策定する機関においてクオリファイド基準として作成、刷新し、法令で当該基準を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　署名生成装置 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。

4.4.4.1　電子署名

（２）公的個人認証法

ア．民間取引においては、電子証明書のシリアル番号の秘匿規定や証明書失効情報の利用制限により、本来、電子署名文書を利用すべき者に電子署名文書が渡せない。

＜解決策＞

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ある。

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ある。

ウ．電子証明書に関する国際相互承認

＜解決策＞

eIDAS規則のeIDの要件やUNCITRALの「IdM and Trust Services」（案）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ある。

オ．類似した認定基準との共通化の検討

＜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ある。

4.4.4.1　電子署名

（3）商業登記法

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ある。

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、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ある。

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、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、リモート署名システムを含む）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ある。

4.4.4.2　電子認証

（１）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利用者認証用の証明書発行は定められていない。

（２）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、電子認証に用いる電子認証手段（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。

（３）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（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）「4.1.3 民事訴訟における効力（10）電子認証」で検討した効果を得るために、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ある。

4.4.4.3 属性証明（電子委任状法）

（１）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べきである。

（２）「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

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）。

（３）属性確認時のベース・レジストリ参照とベース・レジストリの信頼性向上

前述した様々な属性を電子証明書に格納するためには、信頼された証跡データが必要である。包括的データ戦略でも検討されているベース・レジストリが改ざんされていないこと、データの発出元が明示され判明することが必要である。

4.4.4.3 属性証明（HPKI）

（１）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の検討

保健医療福祉分野では、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ため、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。

（２）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の検討

HPKIは保健医療福祉分野の資格の厳密な反映という点で認定認証業務とは証明書ポリシ等が大きく異なるが、共通要件も少なくない。認証局の共通要件と個別要件を明確化し、可能な部分を共通化することで、認証業務の提供と監査業務の提供の双方において、コスト削減に資すると思われる。

（３）属性を証明する認証業務としてHPKIを参考とすべき点の検討

HPKIでのように、比較的長期にわたり安定的であり、資格等を正確に確認できる仕組みが存在する場合、証明書に資格属性を含めることの有利な点が少なくない。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。

4.4.4.4 タイムスタンプ

（１）法的効力

①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、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。

②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

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。

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

トラストサービスの分野における適合性評価機関は、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。

（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。

4.4.4.5　eシール

（１）他のトラストサービスと同様に「法的効果」を含めた詳細制度設計の実施

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、トラストサービスは複合活用されることが多いことから、他のトラストサービスと同様「法的効果」を謳い、詳細制度設計を行うべきである。

（２）ｅシール用電子証明書の発行業務の認定基準の検討

組織の真偽確認等運用の一部を除き、設備基準、技術基準、運用基準等の基準は、電子署名法に基づく特定認証業務の認定基準と同一と考えられることから、同法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を実施

①適合性評価機関に関する基準

②発行対象の明確化

③発行対象の真偽確認方法

④電子証明書プロファイル、組織を特定可能な識別子

⑤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

4.4.4.6 リモート署名

（１）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、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。

（２）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・監査できるかを試行検証する必要がある。

（３）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。

（４）リモート署名による署名データであることの確認方法

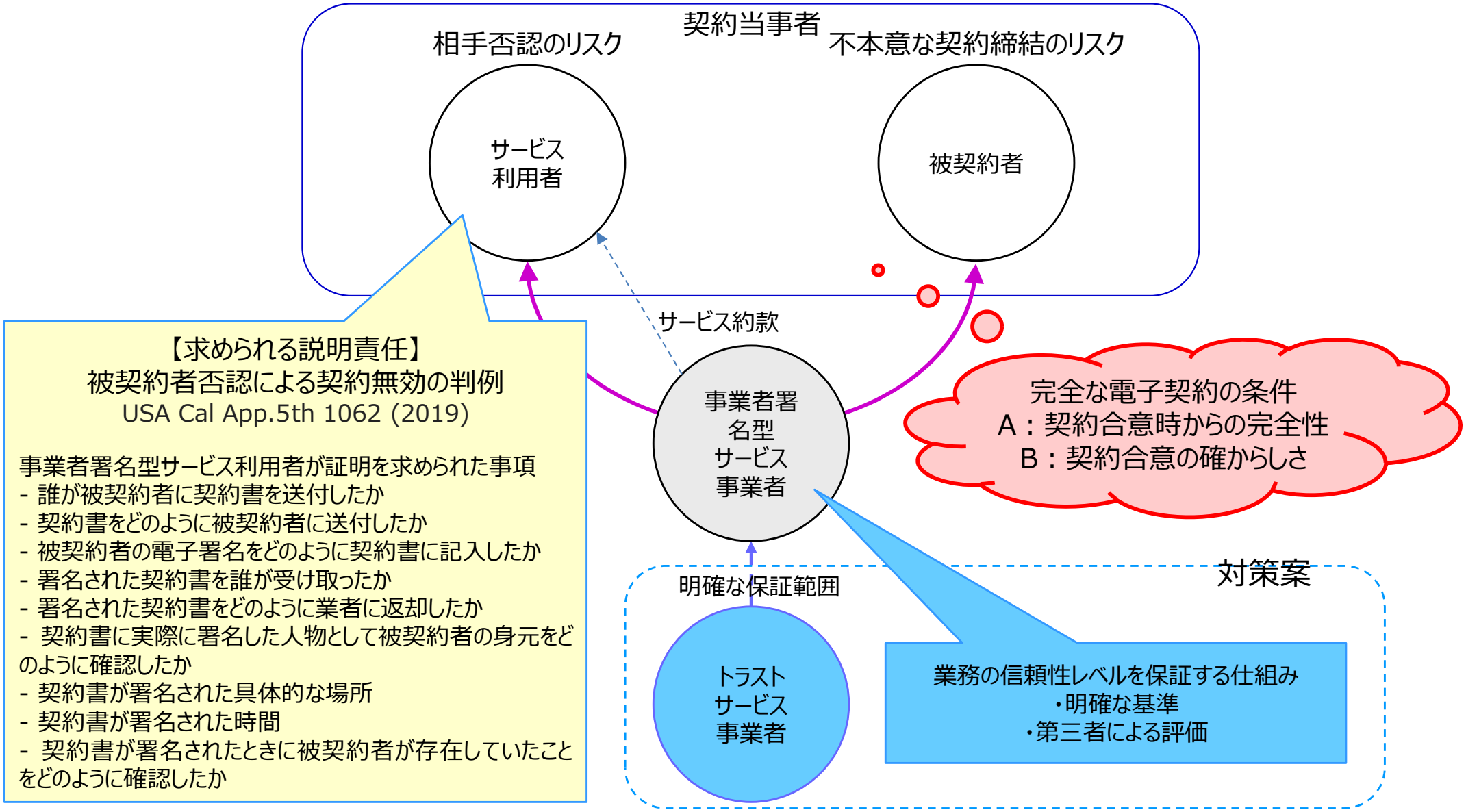
4.1.3に示した通り、民事訴訟における効力を考慮した場合、ローカルによる署名ではなく、リモート署名を用いて生成した署名データであることがわかる（確認できる）必要があり、これらの確認方法について検討する必要がある。詳細は、本書4.1.3の（12）を参照。

（５）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

課題：事業者署名型サービスの信頼性を確認するための基準がない。
リスク：サービスを利用する契約当事者において、不本意な契約や事後否認のリスクがある。
対策案：明確な保証範囲が規程されているTSPの利用。事業者署名型サービスの契約合意意思の確からしさ基準の設定。



4.4.4.8 電子署名/eシールデータ生成装置

電子署名/eシールデータ生成装置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電子署名/eシールデータ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。

（１）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。

（２）技術基準についてはeIDAS規則における適格電子署名/e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。

（3）電子証明書のプロファイルに、秘密鍵が安全な電子署名/eシールデータ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、電子署名/eシール検証者が安全な電子署名/eシールデータ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
   （１）取引の安全性確保等のため、内容証明郵便に相当するサービスが必要である。
   （２）電子内容証明送付業務の要件や、クオリファイドの要件を明確にする必要がある。
2. 検証業務
   （１）利用者(特に依拠者)が、民事訴訟等においてトラストサービス等の正当性を証明するのは、一般的には困難である。これを補完するサービスが期待されている。
   （２）検証業務による正当性証明を民事訴訟等で活用できるように法制化すべきである。
3. 保存サービス
   （１）電子署名、eシール等が付与された電子データ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必要がある。
   （２）保存対象文書等は意図しない消去のリスクがあり、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る恐れがある。
   （３）これらの対応に向け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クラウドを利用したサービスが考えられるが、類似する既存サービスや法的効果等の相違や関係を整理した上で基準等を検討する必要がある。
4. Webサイト認証
   （１）国内の認証業務による電子証明書を、ブラウザベンダ等が信頼できるものとして使用するように、基準及び制度を整備する必要がある。

4.5 国際的な相互承認の検討

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。

① 法制度
② 監督・監査
③ 技術標準
④ 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を下表に整理する。

	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