

e シールに係る検討会 最終取りまとめ

令和6年4月

e シールに係る検討会

目次

はじめに.....	1
第1章 eシールとは	2
1. 1 トラストサービスとは.....	2
1. 2 eシールとは	4
第2章 政府における検討経緯.....	5
2. 1 「トラストサービス検討ワーキンググループ」における議論.....	5
2. 2 「組織が発行するデータの信頼性を確保する制度に関する検討会」における議論.....	6
2. 3 「トラストを確保したDX推進サブワーキンググループ」における議論.....	6
2. 4 本検討会の立ち上げ.....	7
第3章 国によるeシールに係る認定制度の創設	8
3. 1 政府戦略におけるeシールの位置付け.....	8
3. 2 eシールに係る適合性評価の実現.....	8
3. 3 認定制度の在り方.....	8
3. 4 「eシールに係る指針」の改定.....	9
第4章 個別論点と方向性.....	10
4. 1 eシールの分類.....	10
4. 2 eシール用電子証明書の発行対象となる組織等の範囲.....	11
4. 3 eシール生成者の実在性・申請意思の確認の方法.....	14
4. 4 eシール用電子証明書のフォーマット及び記載事項.....	16
4. 5 認証局の秘密鍵の管理に係る基準.....	17
4. 6 eシール生成者の秘密鍵の管理に係る基準.....	17
4. 7 eシールを大量に生成する際の処理.....	18
4. 8 リモートeシール.....	18
4. 9 eシール用電子証明書の失効要求.....	19
第5章 今後に向けた検討課題.....	19
5. 1 認定制度の運用開始までに議論すべき主な事項.....	19

5. 2 eシールの普及に向けた取組	20
5. 3 国際間のデータ流通における eシール活用の可能性	22
おわりに	24

はじめに

通信インフラの高度化やデジタルサービスの普及・多様化により、我が国のネットワーク上でのデータ流通量は飛躍的に増大している。特に、Society5.0においては、実空間とサイバー空間が高度に融合し、実空間での紙や対面に基づく様々なやりとりを、サイバー空間においても電子的に円滑に実現することが求められている。

このような中、電子データを安心・安全に流通できる基盤が不可欠であり、電子データの改ざんや送信元のなりすまし等を防止する仕組みであるトラストサービスの活用が期待される。とりわけ、企業等が発行する電子データが増大する中、業務効率化や生産性向上の観点からも、企業等が発行する電子データの発行元を証明する「eシール」の活用が期待される。

このような背景から、総務省では、令和3年6月に、eシールに係る技術や運用等に関する一定の基準を示した「eシールに係る指針」を策定した。一部の企業においては、同指針も参考にしながらeシールを活用している事例が見られるものの、国による認定制度など適合性評価の枠組みが存在しないこと等もあり、依然としてeシールの世間的な認知度は高くない状況である。

本検討会は、eシールの更なる普及や活用を促す観点から、総務大臣によるeシールに係る認定制度の創設の可否も含めて議論する場として令和5年9月から開催し、令和6年1月に、本検討会における中間的なアウトプットとして「中間取りまとめ」を公表した。「中間取りまとめ」の作成に当たっては、意見公募手続（パブリックコメント）の過程で、数多くの関係者から意見を頂戴し、それらの意見も踏まえて、本検討会における議論を進め、今般、「最終取りまとめ」を取りまとめた。

本検討会での議論がeシールを始めとするトラストサービスの重要性を広く認知してもらう契機となり、トラストサービスの活用によって、電子データを安心・安全に流通できる社会的基盤の構築が進むことで、その便益が国民一人一人に還元される社会が実現することを期待してやまない。

第1章 eシールとは

1.1 トラストサービスとは

「トラストサービス」については、総務省が公表した「プラットフォームサービスに関する研究会トラストサービス検討ワーキンググループ最終取りまとめ」において、「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仕組み」と定義している¹。

Society5.0の到来や我が国が提唱するDFFT(Data Free Flow with Trust)の実現に向けて、トラストサービスは電子データを安心・安全に流通できる基盤として、重要な役割を担うことが期待されており、各種政府方針において重要課題と位置付けられている。

(参考) 各種政府方針における「トラストサービス」に関する記載

◆ サイバーセキュリティ戦略（令和3年9月28日閣議決定）

サイバー空間における多様な経済社会活動を進める上で、「信頼性のある自由なデータ流通(Data Free Flow with Trust: DFFT)」の実現に向けたデータガバナンス確保の観点を含め、その価値の源泉となるデータの真正性や流通基盤の信頼性を確保することが重要である。(中略) 送信元のなりすましやデータの改ざん等を防止する仕組み（以下「トラストサービス」という。）については、その利活用に向けて実効的な仕組みとする必要がある。

◆ デジタル社会の実現に向けた重点計画（令和5年6月9日閣議決定）

データの利活用による経済発展と社会的課題の解決を図るためには、信頼のあるデータ流通の基盤となるトラストの確保が重要であり、デジタル化の進展に伴いその必要性は一層高まっている。

これらの政府方針に基づき、政府においては、「電子署名」、「タイムスタンプ」、「eシール」を始めとする各種トラストサービスを推進している(図1)。具体的には、デジタル庁においてトラストサービス全体の枠組み及び「電子署名」を推進し、総務省において「タイムスタンプ」、「eシール」等の個別のトラストサービスを推進している。

¹ 総務省,「プラットフォームサービスに関する研究会 トラストサービス検討ワーキンググループ 最終取りまとめ」(令和2年2月7日), P.2

サービス 内容	① 電子署名 ・署名者の意思を確認できる仕組み	② タイムスタンプ ・データの存在証明の仕組み	③ eシール ・文書の発信元を確認できる仕組み	④ eデリバリー ・データの送達を保証する仕組み
	 意思に係る文書	 公文書 税務書類 契約書	 請求書 請求書 請求書	 eデリバリー 保存
	電子署名法に基づく認定制度あり。	告示に基づく認定制度あり。	技術・運用上の基準あり。	制度・基準なし。
総務省 の取組	■令和3年9月1日のデジタル庁設置に伴い、電子署名法は同庁に移管。	■平成17年に民間の認定制度が開始され、令和3年4月に、総務大臣による時刻認証業務の認定制度を創設。	■令和3年6月に、技術上・運用上の基準等を示した「eシールに係る指針」を公表。	■調査研究等を実施し、我が国での活用可能性について検討。

図1 代表的なトラストサービスの我が国における状況

なお、諸外国に目を転じると、EU では、eIDAS (Electronic Identification, Authentication and Trust Services) 規則において、トラストサービスを以下のとおり規定している^{2,3}。

(参考) eIDAS における「トラストサービス」に係る規定

Article 3 (16) ‘trust service’ means an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services;

(和訳)

第3条第16項 「トラストサービス」とは、通常有料で提供される電子的サービスで下記のサービスにより構成される。(a) 電子署名、eシール又は電子タイムスタンプ、eデリバリーサービス、電子属性証明及びこれらのサービスに関連する証明書の作成、検証、及び有効性確認 (b) ウェブサイト認証用証明書の作成、検証及び有効性確認 (c) 電子署名、eシール

² eIDAS2.0 においては、‘electronic attestation of attributes,’ (属性の電子証明) ‘the electronic archiving of electronic documents,’ (電子文書の電子アーカイブ) ‘the management of remote electronic signature and seal creation devices,’ (リモート署名及びシール作成デバイスの管理) ‘the recording of electronic data into an electronic ledger.’ (電子元帳への電子データの記録) が追加予定。

³ 国際連合国際商取引法委員 (UNCITRAL) においては、「UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services」の Article 1. Definitions (I) にトラストサービスの定義が記載されている。

ル又はこれらのサービスに関連する証明書の保存。

1.2 eシールとは

「eシール」については、従来、eシールに係る技術や運用等に関する一定の方向性を示した「eシールに係る指針」(令和3年6月25日総務省策定)において、「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」と定義していた。

本検討会においては、

- 1) eIDAS 規則において、eシールは「データ」と定義されており、国際的な相互運用性を考えると「データ」として整理することが望ましいこと、
- 2) eシールの活用方法を見ても、「データ」として認識されていることが多いこと、等の理由から、「eシールに係る指針」における定義を見直すべきとの議論がなされた⁴。

(参考1) eIDASにおける「eシール」に係る規定

Article 3 (25) ‘electronic seal’ means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’ s origin and integrity

(和訳)

第3条第25項 「eシール」とは、他の電子形式データの出所・起源と完全性を確保するために当該データに添付され又は論理的に関連づけられた電子形式のデータをいう。

また、見直し後の定義においては、eIDAS 規則を参考とし、“origin”(出所・起源)や“integrity”(完全性)といった要素を盛り込むことが適当であると結論付けられた。

なお、「eシール」という名称については、「eシール」という名称が一定程度普及していることを踏まえ、「eシール」という名称を維持するとの整理がなされた。

以上を踏まえ、eシールの定義は以下と整理することとした。

【eシールの定義】

「eシール」とは、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

⁴ 電子署名及び認証業務に関する法律(平成12年法律第102号。以下「電子署名法」という。)において、電子署名が「措置」として定義されていることを踏まえると、eシールも「措置」として捉えることが望ましい等の意見も出された。

れるものをいう。以下同じ。)に記録された情報(以下「電子データ」という。)に付与された又は論理的に関連付けられた電子データであって、次の要件のいずれにも該当するものをいう。

- 一 当該情報の出所又は起源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確認することができるものであること。

(参考2) e シールと電子署名の異同⁵

意思表示という性質から利用者たる自然人との紐付きが強固である電子署名とは異なり、発行元となる組織等に紐づく e シールは、組織内の人事異動に伴って e シール用の電子証明書を再発行する必要がないことや、意思表示を伴わないため、大量の電子文書等に機械的、自動的に e シールを行うこともできること等のメリットがあるが、e シールが行われた電子文書等には e シールを行った自然人の意思は顕れていないことに留意する必要がある。

第2章 政府における検討経緯

2.1 「トラストサービス検討ワーキンググループ」における議論

平成31年1月から令和元年11月にかけて、総務省が開催する「プラットフォームサービスに関する研究会」の下で「トラストサービス検討ワーキンググループ」を開催し、我が国におけるトラストサービスに関する課題を整理し、その在り方について検討を行った(図2)。

同ワーキンググループにおいては、我が国におけるトラストサービスの利用動向、諸外国の動向調査の結果、トラストサービスの活用・普及による経済効果等が示された。eシールについては、その導入を進めるためには、利用者が安心して利用できるよう、信頼のにおけるサービス・事業者に求められる技術上・運用上の基準の提示等が重要であるとの議論がなされた。他方、我が国におけるeシールのサービス内容やサービス提供のための技術等が確立されておらず、国による認定制度に位置付けることで、今後の技術開発やサービス展開に影響を与える可能性について懸念が示された。

このような議論を踏まえ、同ワーキンググループの「最終取りまとめ」⁶においては、「まずは、一定程度国が関与しつつも、基本的に民間の自主的な仕組みにより、eシールを提供するサービスの立上げやその導入が促進されるよう、信頼の置けるサービス・事業者を認定する民間の仕組みの創設に向け、信頼の置けるサービス・事業者に求められる技術上・運用上の基準や認定の仕組みに関する検討を進めることが適当」と提言がなされた。

⁵ 「eシールに係る指針」(令和3年6月25日)のP.5の「1.2 eシールと電子署名の異同」より抜粋。

⁶ 総務省、「トラストサービス検討ワーキンググループ最終取りまとめ」(令和2年2月7日), P.31

2.2 「組織が発行するデータの信頼性を確保する制度に関する検討会」における議論

「トラストサービス検討ワーキンググループ」の「最終取りまとめ」における提言を踏まえ、令和2年4月から令和3年6月にかけて、「組織が発行するデータの信頼性を確保する制度に関する検討会」を開催し、我が国のeシールの在り方について検討を行った（図2）。

同検討会においては、①国内の類似制度との整合性（電子署名法上の電子署名との関係性等）、②国際的な整合性（EU等の諸外国の仕組み・制度との整合性等）、③eシールの普及・利用促進（eシールの利用者視点での分かりやすいeシールの用途の整理等）という3つの観点を軸に据えて議論が行われた。

同検討会の「取りまとめ」⁷においては、我が国のeシールの在り方について、①eシールに求められる要素、②eシール用電子証明書の発行対象となる組織等の範囲、③組織等の実在性・申請意思の確認の方法、④eシール用電子証明書の記載事項、⑤設備（認証局側の暗号装置、利用者側のeシール生成装置等）の基準、⑥その他（一定の技術基準（リモート方式、CRL（失効リスト）等）等）に関する方向性が示された。

令和3年6月に、同検討会での議論を踏まえ、eシールに係る技術や運用等に関する一定の基準を国が示す「eシールに係る指針」を策定した。

2.3 「トラストを確保したDX推進サブワーキンググループ」における議論

令和3年9月にデジタル庁が発足し、同年11月から令和4年6月にかけて、デジタル庁が開催する「データ戦略推進ワーキンググループ」の下で「トラストを確保したDX推進サブワーキンググループ」を開催し、トラストを確保したデジタルトランスフォーメーションの具体的な推進方策について検討を行った（図2）。

同サブワーキンググループの「報告書」⁸においては、eシールについて、「今後、オンライン取引・手続において、発行元に関する証明のニーズが高まることが想定されるため、総務省が令和3年6月に公表した「eシールに係る指針」に基づき、eシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向け、総務省の取組を支援すべきである。」とされた。

⁷ 総務省、「組織が発行するデータの信頼性を確保する制度に関する検討会取りまとめ」（令和3年6月25日）、P.7

⁸ デジタル庁、「トラストを確保したDX推進サブワーキンググループ報告書」（令和4年7月29日）、P.3

2.4 本検討会の立ち上げ

「トラストを確保したDX推進サブワーキンググループ」の「報告書」に基づき、総務省において、再度、「e シールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現」に向けた検討を行うこととなった。

総務省においては、e シールに関するサービス提供の実態等を把握するため、令和4年度に「e シールに関する調査研究」を実施するとともに、令和5年4月から同年5月にかけて、我が国におけるeシールサービスの状況等に関する情報提供を広く一般に依頼した⁹。

その結果、我が国において e シールの定義に合致するサービスを提供している事業者が複数存在することが判明するとともに、e シールに関する国の制度が存在しないこと等が e シール普及の阻害要因となっているという課題が明らかとなった。

これを踏まえ、e シールに係る制度について検討するため、令和5年9月より、「eシールに係る検討会」を開催することとした（図2）。同検討会においては、令和6年1月に、中間的なアウトプットとして「中間取りまとめ」を公表した。

eシールに関連した取り組み	主管箇所	2018年度	2019年度	2020年度	2021年度	2022年度	2023年度
プラットフォームサービスに関する研究会 - トラストサービス検討ワーキンググループ	総務省						
組織が発行するデータの信頼性を 確保する制度に関する検討会	総務省						
データ戦略推進ワーキンググループ - トラストを確保したDX推進 サブワーキンググループ	デジタル庁						
eシールに係る検討会	総務省						
政府方針等							

図2 政府におけるこれまでの検討経緯

⁹ 我が国における e シールサービスの状況等に関する情報提供依頼

https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00163.html

第3章 国による e シールに係る認定制度の創設

3.1 政府戦略における e シールの位置付け

「デジタル社会の実現に向けた重点計画」(令和5年6月9日閣議決定。以下「重点計画」という。)において「eシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現にも取り組む」こととされており、重点計画の工程表(図3)では、総務省において「eシール基準案等の検討」に取り組むべき旨が示されている。

(参考) 政府方針における「eシール」に関する記載

◆ デジタル社会の実現に向けた重点計画 (令和5年6月9日閣議決定) (抜粋)

今後、オンライン取引・手続等において、発行元に関する証明のニーズが高まることが想定されるため、eシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現にも取り組む。

◆ デジタル社会の実現に向けた重点計画 工程表 (抜粋)

取組名	取組内容	2022年度 (令和4年度)				2023年度 (令和5年度)				2024年度 (令和6年度)				2025年度 (令和7年度)				2026年度 (令和8年度)				担当府省庁
		1Q	2Q	3Q	4Q																	
①トラスト ・eシール、タイムスタンプ	eシールの国内ニーズ等の調査																					総務省
	eシール事業者の現状把握																					総務省
	eシール基準案等の検討																					総務省

図3 eシールに係る検討工程

3.2 eシールに係る適合性評価の実現

重点計画に記載された方針のうち、「eシールの民間サービスの信頼性を評価する基準策定」については、令和3年6月に策定された「eシールに係る指針」において技術や運用等に関する一定の基準が既に示されている。他方、重点計画に記載された方針のうち、「適合性評価の実現」については、現状として国による適合性評価の枠組みが存在していない状況である。

こうした状況を受け、本検討会での議論では、国による適合性評価の枠組みとして、総務大臣による eシールに係る認定制度を創設することが適当であるとの結論を得た。

3.3 認定制度の在り方

トラストサービスについて総務大臣による認定制度を設けた前例として、タイムスタンプに係る認定制度が挙げられ、同制度は総務省告示によって制度を設けている(図4)。同制

度も参考にしながら、「e シール用認証業務¹⁰」を認定の対象^{11,12}として、e シールに係る認定制度の創設に向けた議論を進めた。

具体的には、「e シールに係る指針」において一定の整理がなされている状況を踏まえ、第4章「個別論点と方向性」に記載する各論点について議論を行った。なお、「e シールに係る検討会」において示された方向性を踏まえ、「e シールに係る指針」の改正を実施することとする。

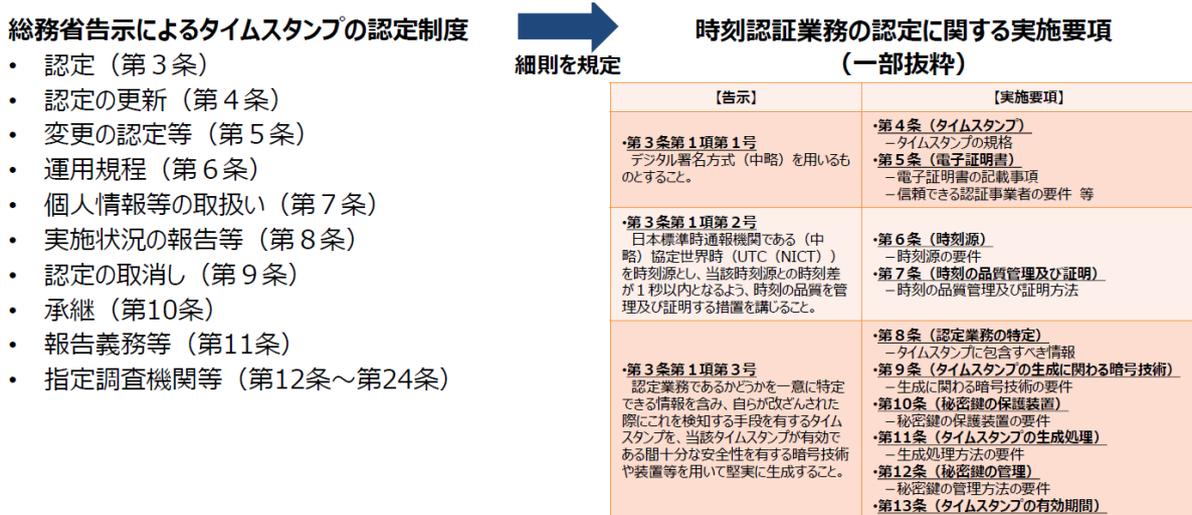


図4 総務省告示によるタイムスタンプの認定制度

3.4 「e シールに係る指針」の改定

「e シールに係る指針」は、節2.2で示したとおり、「組織が発行するデータの信頼性を確保する制度に関する検討会」での議論を踏まえ、令和3年6月に我が国における 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の技術や運用等の基準を示す指針として策定された。「e シールに係る検討会」で示された方向性を受け、図5に示すとおり、「e シールに係る指針」を改定する。

¹⁰ e シールを生成する組織等を認証する業務をいう。以下同じ。

¹¹ 「e シール」と技術的に共通する部分が多い「電子署名」についても、「認証局が行う認証業務」を対象に認定制度を設けている。

¹² 認定の有効期間は2年とし、認定の審査に係る業務の一部を「指定調査機関」に行わせることを可能とすることが適当との結論を得た。

骨子案		主な改正内容
本指針の目的等		・ 本指針と旧指針の適用関係等について記載
第1章	eシールとは	
1.1	eシールの定義	・ eシールの定義について修正
1.2	eシールと電子署名の異同	
1.3	eシールの保証レベル	・ 第2章に記載されていたeシールの分類（保証レベル）を第1章に移行 ・ eシールの保証レベルについては、再定義した保証レベル1や保証レベル2について記載
1.4	eシールのユースケース	・ 再定義した保証レベルごとに想定されるユースケースを新たに記載
1.5	eシールを用いてトラスト確保の仕組み	
1.6	eシールの生成方式 (ローカルeシール方式/リモートeシール方式)	・ 第1回資料を基に図表を説明及びアップデート
第2章	我が国におけるeシール用認証業務の在り方	
2.1	eシール用電子証明書の発行対象となる組織等の範囲	・ 総務大臣認定のeシール用電子証明書の発行対象について記載 ・ eシール用電子証明書に格納する組織識別子について記載
2.2	eシール生成者の実在性・申請意思の確認の方法	・ eシール生成者の実在性確認等の方法について、法的存在に加えて物理的・運営的存在確認に係る指針を記載
2.3	eシール用電子証明書のフォーマット及び記載事項	・ eシール用電子証明書のフォーマットについて記載 ・ 共通証明書ポリシーOID体系を整備する方向性を記載
2.4	認証局の秘密鍵の管理に係る基準	・ 認証局における秘密鍵の管理について、HSMの技術基準については実施要項等で示す方向性を記載
2.5	eシール生成者の秘密鍵の管理に係る基準	
2.6	eシールを大量に生成する際の処理	
2.7	リモートeシール方式における利用認証	
2.8	eシール用電子証明書の失効要求	・ eシール生成者からの失効要求に加えて、認証局側からの失効要求が可能な場合について記載
おわりに		

※赤字は主な改正箇所

図5 「eシールに係る指針」の主な改正内容

第4章 個別論点と方向性

4.1 eシールの分類

(1) 論点

「eシールに係る指針」において、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3つの段階にレベル分け¹³を行っており、このレベル分けの考え方を踏襲するのかといった点が論点となる。

その際、電子署名法等においては、「認証業務」に着目し、「認証業務」、「特定認証業務」及び「認定認証業務」¹⁴と規定していることにも留意する必要がある。

¹³ 「eシールに係る指針」では、eシールに対するレベル分けがなされており、レベル1:eシールの定義に合致するもの、レベル2:一定の技術基準を満たすeシール、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を担保されたeシール、とされている。

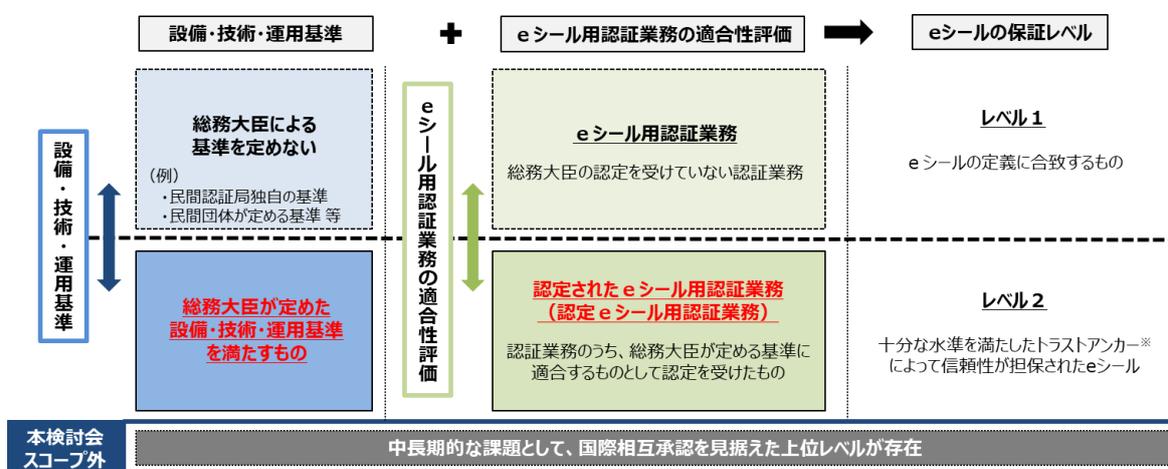
¹⁴ 電子署名法等において、「認証業務」とは、自らが行う電子署名についてその業務を利用する者その他の者の求めに応じ、当該利用者が電子署名を行った者であることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう、と定義されている。「特定認証業務」は、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務と定義されている。また、特定認証業務を行おうとする者のうち、主務省令で定める基準に適合すると認められた者は主務大臣の認定を受けることができ、その認定を受けた認証業務を「認定認証業務」という。

(2)方向性

「e シールの保証レベル」¹⁵として、その用途に応じ、①総務大臣による認定を受けた e シール用認証業務によって保証されてはいないが、より低コスト・簡易な手続で大量発行される e シールに期待される保証レベル(例:企業間で日常的にやり取りされる電子データ等に活用)と、②総務大臣による認定を受けた e シール用認証業務によって保証され、e シールが付された電子データの出所・起源や完全性について高い信頼が期待されるレベル(例:排他的独占業務とされている土業等の資格証明書等に活用)の2段階に分ける形で整理することが必要と考えられる。

図6における整理は、総務大臣の認定制度に着目したものであり、これ以外に、認証局の e シール用認証業務の信頼性を確保するために民間団体が自主的に行う取組を妨げるものではない。

また、構成員からは、e シールを生成する組織等にとって導入コストの観点からレベル分けの議論は重要であり、これらのレベル分けの整理がユーザ企業にも分かりやすく伝わるように留意すべき旨の議論がなされており、この点も踏まえて制度の周知啓発を図ることが適当であると考えられる。



※インターネットなどで行われる、電子的な認証の手続きのために置かれる基点のこと。本取りまとめにおいては、信頼性の基点となる認証局を想定している。

図6 e シールの保証レベル

4.2 e シール用電子証明書の発行対象となる組織等の範囲

e シール用電子証明書¹⁶の発行対象となる組織等の範囲については、「e シールに係る

¹⁵ 将来的な課題として、諸外国との国際相互承認を見据えた上位レベルにおいては「適格 e シール生成装置」に係る要件等も検討する必要があるが、今回のレベル分けは「e シール用認証業務」に着目したものであるとしている。

¹⁶ e シール用電子証明書の一例を、「(参考) e シール用電子証明書 (ITU-T X.509) の記載の一例 (イ

指針」において、「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」としており、この整理を維持するか等について議論が行われた。

4.2.1 組織を一意に特定するための識別子(組織識別子)について

(1)論点

eシール用電子証明書の発行対象となる組織等には、当該組織を一意に識別できる識別子が必要となるため、その識別子をどのように設定するかといった点が論点となる。

(2)方向性

本検討会において、認定に係るeシール用電子証明書に使用する識別子として、国際的に使用されているプレフィクス(接頭辞)^{17,18}と公的機関が発行する既存の番号体系を組み合わせるという提案がなされた。これを踏まえて、法人等についてはプレフィクス「NTRJP」を使用し、既存の番号体系「法人番号」と組み合わせ、組織識別子を構成することとする¹⁹。なお、認定に係るeシール用電子証明書には、公的機関が発行する番号体系を用いた組織識別子を少なくとも1つ記載することを要件とするが、取引主体識別子(LEI)²⁰や後述の民間企業コードを用いた組織識別子を追加で記載することは可能とする。(図7)

【凡例】◎：全てに付番(悉皆性) ○：基本的には付番可 △：一部に付番可 -：付番対象外

保証レベル2の認定eシール用認証業務におけるeシール用電子証明書に使用する組織識別子	必須	法人番号に追加して使用可能			
	法人番号	TDB企業コード	標準企業コード	TSR企業コード*1	LEI
	公的機関が管理する番号体系	民間が管理する番号体系			
識別子プレフィクス	NTRJP*2	TD:JP	JI:JP	TS:JP	LEIXG*3*4
組織識別子例	NTRJP-1234567890123	TD:JP-123456789	JI:JP-123456	TS:JP-123456789	LEIXG-12345678901234567890
【参考】					
既存番号体系の付番対象	法人	◎	○	○	○
	権利能力なき社団・財団	○	○	○	—
	その他任意の団体	—	○	○	—
	個人事業主	—	○	○	○
	その他の個人	—	—	—	—

*1：「D-U-N-S® Number」はTSR企業コードとリンクしている。

*2：政府機関や地方自治体については「GOVJP」を使用可能とする。

*3：CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates Version 1.0.0のAppendix Aに基づく。

*4：電子証明書の拡張領域へのLEIの格納形式はISO 17442-2:2020 Financial services - Legal entity identifier (LEI) - Part 2: Application digital certificatesで定義されている。

図7 保証レベル2の認定eシール用認証業務におけるeシール用電子証明書に使用する組織識別子

メッセージ)に示す。

¹⁷ CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates Version 1.0.1, August 11, 2023

¹⁸ ETSI, ETSI TS 119 412-1 V1.3.11, 2019-08

¹⁹ 政府機関や地方自治体が認定に係るeシールを付す場合、プレフィクス「GOVJP」を使用可能とする。

²⁰ eシール用電子証明書へのLEIの格納形式については、ISO 17442-2:2020 Financial services - Legal entity identifier (LEI) - Part 2: Application digital certificatesで定義されている。

また、認定外のeシール用電子証明書は公的機関が発行する番号体系を用いた組織識別子を使用することを要件とはせず、民間企業が提供する番号体系のみを使用しても良いこととする。なお、認定に係るeシール用電子証明書と同様、複数の番号体系を利用することも可能とする。民間企業の番号体系に基づいた組織識別子で使用するプレフィクスは我が国独自で決定する必要があり、国際的な相互運用性を考慮し、「●●:JP」(●●には識別子プレフィクスが入る。)を使用することを「eシールに係る指針」等で推奨することとする。(図8)

【凡例】◎：全てに付番(悉皆性) ○：基本的には付番可 △：一部に付番可 -：付番対象外

保証レベル1のeシール用認証業務におけるeシール用電子証明書に使用する組織識別子	いずれかの組織識別子を使用することを推奨					
	法人番号	TDB企業コード	標準企業コード	TSR企業コード*1	LEI	
	公的機関が管理する番号体系		民間が管理する番号体系			
識別子プレフィクス	NTRJP*2	TD:JP	JI:JP	TS:JP	LEIXG*3*4	
組織識別子例	NTRJP-1234567890123	TD:JP-123456789	JI:JP-123456	TS:JP-123456789	LEIXG-12345678901234567890	
【参考】						
既存番号体系の付番対象	法人	◎	○	○	○	○
	権利能力なき社団・財団	○	○	○	○	—
	その他任意の団体	—	○	○	○	—
	個人事業主	—	○	○	○	○
	その他の個人	—	—	—	—	—

※1：「D-U-N-S® Number」はTSR企業コードとリンクしている。

※2：政府機関や地方自治体については「GOVJP」を使用可能とする。

※3：CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates Version 1.0.0のAppendix Aに基づく。

※4：電子証明書の拡張領域へのLEIの格納方式はISO 17442-2:2020 Financial services – Legal entity identifier (LEI) – Part 2: Application digital certificatesで定義されている。

図8 保証レベル1のeシール用認証業務におけるeシール用電子証明書に使用する組織識別子例

4.2.2 「個人事業主」の扱いについて

(1) 論点

「個人事業主」の扱いについては、「個人事業主」を特定するための識別子として、重点計画に記載のある「個人事業主の番号体系」や適格請求書発行事業者登録番号を活用することが可能であるかという点が論点となる。

(2) 方向性

重点計画に記載のある「個人事業主の番号体系」については、現在デジタル庁において、GビズID内で付番される個人事業主管理番号を用いる方向で検討を進めている最中である。

また、適格請求書発行事業者登録番号については、個人事業主の場合、公表サイトにおいて掲載される情報が、基本的に、「登録年月日」、「登録番号」及び「名称」に限られており、同姓同名の個人事業主を確実に見分ける方法が存在していない。

さらに、適格請求書発行事業者登録番号を識別子として用いる場合、非課税の個人事業主をどのようにして捕捉するかという課題も残る。

従って、個人事業主を識別するための識別子については、本年度中に早急に結論を出すことはせず、保証レベル2の認定 e シール用認証業務における e シール用電子証明書の発行対象として個人事業主は含まないこととし、デジタル庁における「個人事業主の番号体系」の検討状況も注視しながら、引き続きの検討課題とする。

なお、認定制度の対象となるためには公的な番号体系を識別子として用いる必要があるが、認定制度の対象外であれば民間コード等を活用することも可能であるため、認定制度の枠外では、eシール用電子証明書の発行対象として個人事業主を含むことは可能である。

4. 2. 3 法人等における「事業所や営業所等」の扱いについて

(1) 論点

「e シールに係る指針」において、「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」としており、この整理を維持するかが論点となる。

(2) 方向性

事業所や営業所等が、e シールの活用主体とはなり得るものの、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から、「e シールに係る指針」での整理を維持し、事業所や営業所等については、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することとする。

4. 3 e シール生成者の実在性・申請意思の確認の方法

(1) 論点

「e シールに係る指針」において、e シール生成者の実在性の確認の方法として「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」とし、申請意思の確認の方法として「電子署名、押印、署名等で行うことが想定される」としており、この整理を維持するかが論点となる。

(2) 方向性

組織を確認して証明書を発行する点で、eシール用電子証明書と類似の証明書としてEV

(Extended Validation) 証明書がある。同証明書における組織の実在性確認は、CA/Browser Forum のガイドライン²¹等に従って、①法的な存在の確認、②物理的な存在の確認、③運営的な存在の確認の3点が必要とされており、e シール用電子証明書も同様に整理することが適当であると考える。

これを踏まえ、e シール生成者の実在性及び申請意思の確認の方法のイメージとして、CA/Browser Forum のガイドライン等を参考に以下のとおり一例を整理する²²。(図9～図12)

eシール生成者の分類	eシール生成者の実在性の確認		
	法的実在性確認	物理的実在性確認	運営的実在性確認
・法人 ・権利能力なき社団・財団	以下のいずれかの方法で確認する。 1. 法人の代表者の電子署名の有効性を確認(★) (商業登記法第12条の1第1項、第3項の規定で証明されているものに限る。) 2. 組織等の属性を格納した電子証明書による電子署名の有効性を確認(★) (電子署名法第4条に基づき認定認証業務) 3. 登記事項証明書の確認 (もしくは第三者機関データベース ^{※1} の確認)	以下のいずれかの方法で確認する。 1. 申請された住所と登記事項証明書に記載の住所を確認 2. 申請された住所と第三者機関データベース ^{※1} の登録住所を確認(★)	以下のいずれかの方法で確認する。 1. 登記事項証明書に記載の成立年月日を確認し設立から3年以上経過していることを確認 2. 第三者機関データベース ^{※1} の登録を確認(★) 3. 免許・許可・登録等を受けている金融機関の預金口座の保有状況を確認
事業所・営業所・支店・部門等、担当者、機器	組織等の代表者の宣言の結果を尊重することとし、発行対象である組織等が一義的な責任を負うことを前提として、認証局は利用申込の宣言の結果に基づいてeシール用電子証明書の拡張領域に記載することを可能とする。		

図9 保証レベル2の認定 eシール用認証業務における eシール生成者の実在性及び電子証明書へ格納する情報の確認方法のイメージ

eシール生成者の分類	eシール生成者(代表者)の意思の確認	eシール生成者の代表者の在籍の確認
	・法人 ・権利能力なき社団・財団	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(★) 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り)

【甲：意思の確認が①の場合】
第三者機関データベース^{※1}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】
第三者機関データベース^{※1}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

図10 保証レベル2の認定 eシール用認証業務における eシール生成者の申請意思の確認方法のイメージ

eシール生成者の分類	eシール生成者の実在性の確認
・法人 ・権利能力なき社団・財団 ・その他の任意の団体	申請された内容と第三者機関が管理するデータベース ^{※1} (★)に登録内容を確認
個人事業主	各種身分証明書の確認(運転免許証等)
事業所・営業所・支店・部門等、担当者、機器	組織等の代表者の宣言の結果を尊重することとし、発行対象である組織等が一義的な責任を負うことを前提として、認証局は利用申込の宣言の結果に基づいてeシール用電子証明書の拡張領域に記載することを可能とする。

図11 保証レベル1の eシール用認証業務における eシール生成者の実在性及び電子証明書へ格納する情報の確認方法のイメージ

²¹ Guidelines for the Issuance and Management of Extended Validation Certificates Version 1.8.0, CA/Browser Forum, 30 November, 2022

²² 法人の実在性確認において、法人ベース・レジストリの活用も考えられるため。法人ベース・レジストリの検討状況も注視する必要がある。

eシール生成者の分類	eシール生成者（代表者）の意思の確認	eシール生成者の代表者の在籍の確認
・法人 ・権利能力なき社団・財団	代表者（又は申請者※ ² ）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（又は申請者※ ² ）の署名又は押印…②	【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※ ¹ に登録されている代表者（又は申請者※ ² ）の住所と電子証明書に記載されている代表者（又は申請者※ ² ）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※ ¹ に登録されている電話番号等を通じた代表者（又は申請者※ ² ）本人に対する当該申請の有無の確認
個人事業主		

図 12 保証レベル1の eシール用認証業務における eシール生成者の申請意思の確認方法のイメージ

4.4 eシール用電子証明書のフォーマット及び記載事項

(1) 論点

「eシールに係る指針」において、eシール用電子証明書のフォーマットは「ITU-T X.509」を使用することとした上で、eシール用電子証明書への記載事項については「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」としており、この整理を維持するかが論点となる。

特に、「電子署名」用電子証明書と「eシール」用電子証明書を機械判読可能な形で区別できる必要があり、これを共通証明書ポリシーOID (Object Identifier) 体系で整備することが考えられる。その際、判別可能な情報として、電子署名/eシールの区別その他、認定の有無やローカル/リモートの別も判別可能にすることが考えられるため、どのように共通証明書ポリシーOID 体系を整備するかが論点となる。

(2) 方向性

原則として「eシールに係る指針」における整理を維持しながらも、「電子署名」用電子証明書と「eシール」用電子証明書を機械判読可能とする観点と国際相互運用性の観点から、共通証明書ポリシーOID 体系を整備することが適当であると結論付けた。共通証明書ポリシーOID 体系の具体的内容については認定制度の運用開始に間に合うように検討を進める。

なお、共通証明書ポリシーOID 体系に関連し、認証局における運営コスト削減のためにも、一つの秘密鍵から複数の証明書を発行できるようにすることが重要であるとの議論がなされた。

4.5 認証局の秘密鍵の管理に係る基準

(1)論点

「e シールに係る指針」において、認証局における秘密鍵の管理については、「基本的に電子署名法の規定(FIPS140-1 レベル3相当)」を準用する」とした上で、「HSM 自体の技術基準は現行化(FIPS140-2 レベル3相当)することを前提とし、念頭に置くレベルはFIPS140-2 レベル3相当もしくは、ISO/IEC 15408 の EAL4+相当(プロテクションプロファイルは別途検討が必要)とする」としている。

このように「e シールに係る指針」上で連邦情報処理標準(FIPS)の規格等の技術基準まで記載してしまうと、技術の進展等に応じて指針の見直しが必要となるが、設備・技術・運用基準をどのように定めるかが論点となる。

(2)方向性

認証局における秘密鍵の管理について、基本的には電子署名法の規定を準用するという「eシールに係る指針」の考え方を維持することが適当である。なお、実施要項等において細部を検討するに当たっては、タイムスタンプの認定制度等も参考にすることが望ましい。

その上で、HSM の技術基準として満たすべき FIPS の規格を始め、技術・設備・運用基準については、技術の進展等に応じて変化していくため、国際動向等も踏まえて機動的に見直しができるよう、「e シールに係る指針」とは別に定め、「e シールに係る指針」はそれを参照する形で規定することが適当である。

4.6 eシール生成者の秘密鍵の管理に係る基準

(1)論点

「eシールに係る指針」において、eシール生成者における秘密鍵の管理については、「発行対象である組織等に委ねることとする」としているが、この整理を維持するかが論点となる。

(2)方向性

eシール生成者側の秘密鍵の管理については、「eシールに係る指針」の記載を維持し、認証局から eシール生成者に対して秘密鍵の管理の重要性等を説明することとした上で、eシール生成者の秘密鍵の管理の責任は eシール生成者自身にあるとすることが適当である。

4.7 eシールを大量に生成する際の処理

(1)論点

総務大臣認定に係る e シールについて、複数の対象データに一括で e シールを付与することを認めるかが論点となる。

(2)方向性

機械的・自動的に複数の対象電子文書等に対して一括で e シールを付与するニーズが想定されるため、「e シールに係る指針」で示している方向性に基づき、総務大臣認定に係る e シールについても、複数の対象データに一括で e シールを付すことを認めることとする。

4.8 リモート e シール

(1)論点

本検討会の関係者ヒアリングとして実施した「e シールの活用が見込まれる事例に関する分析(第2回)」において、ユーザが e シールを意識せずに利用することが可能な形態であるリモート e シール活用へのニーズが示されており、認定制度においてリモート e シールをどのように位置付けるかが論点となる。

(2)方向性

リモート署名とリモート e シールについては、後者は複数の電子データにシステム上で大量に e シールを付すことが可能であること等の差異はあるものの、両者が技術的に共通する部分が多いことから、リモート署名における検討を踏まえてリモート e シールについて検討を進める必要がある。

リモート署名については、現在、デジタル庁において、リモート署名生成事業者に係る論点を含めて議論を進めているところであり、e シールの認定制度を検討していく上でも、これらの議論を注視する必要がある。

従って、「リモート e シール生成事業者」に係る規律については、引き続きの検討課題とし、本検討会で議論する内容としては、リモート署名における検討も踏まえつつ、「認証局」に係る論点に絞って議論を行った²³。

²³ リモート署名の電子署名法上の位置付けについては、当時の電子署名法主務省である総務省、法務省、経済産業省が令和2年5月12日の規制改革推進会議 成長戦略ワーキング(第10回)で公表している。「リモート e シール」についても同様の整理とし、「e シール」の定義を満たすものについては認定制度上における「e シール」に該当するものとする。

<https://www8.cao.go.jp/kisei-kaikaku/kisei/meeting/wg/seicho/20200512/200512seicho04.pdf>

4.9 eシール用電子証明書の失効要求

(1)論点

「eシールに係る指針」において、eシール用電子証明書の発行を要求できる者に限定して失効要求もできることとしているが、一定の場合に、認証局側からeシール用電子証明書を失効することを可能とするかが論点となる。

(2)方向性

電子署名法に基づく認定認証業務においては、認証局側から電子証明書を失効可能な場合として、「電子証明書に記録された事項に事実と異なるものが発見されたとき²⁴」、「利用者署名符号が危殆化したおそれがあるとき²⁵」等が挙げられており、eシールについても、同様の場合には、認証局側からeシール用電子証明書を失効可能とする。

第5章 今後に向けた検討課題

5.1 認定制度の運用開始までに議論すべき主な事項

本検討会での議論を踏まえ、「eシールに係る指針」(令和3年6月総務省策定)を改定するとともに、総務省告示によりeシールに係る認定制度を創設する。同制度の創設に向けては、来年度以降に実施要項等の検討を行うこととするが、本検討会における議論を踏まえ、特に以下の点について検討を行う。

(1)技術・設備・運用の基準策定

総務大臣によるeシールに係る認定制度では、総務省において、eシールに係る技術・設備・運用の基準をあらかじめ定めた上で、総務大臣認定に係る申請がなされた際には、申請に係る認証業務がこれらの基準に適合しているかを評価することが適当である。したがって、総務省において、実施要項等の策定の際には、eシールに係る技術・設備・運用の基準についても検討を進める²⁶。

(2)電子署名法の認定制度等を用いた適合性評価等の効率化

総務大臣によるeシールに係る認定制度の創設に当たっては、認定を取得するために認証局が支払うコストがサービスの価格に転嫁される可能性があるとの認識を持つことから、認定に係るコストを軽減するための検討を進める。具体的には、電子署名法における認定制度等との連携等について、実施要項等の策定の際に検討する。

²⁴ 電子署名及び認証業務に関する法律施行規則第6条第10号参照。

²⁵ 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第8条第3号参照。

²⁶ 「4.5 認証局の秘密鍵の管理に係る基準」でも言及したとおり、「eシールに係る指針」においては、HSM等の技術基準等自体は記載せず、eシールに係る技術・設備・運用の基準の基準を参照できるようにする。

(3)CP/CPS に最低限記載すべき事項の整理

本検討会での議論においては、認証局における組織等の実在性・申請意思の確認の方法や、認証局側から e シール用電子証明書²⁷の失効を要求できる場合、その手続の方法、失効状況の確認方法等の整理を始め、認証局の運用規程となる CP/CPS において最低限記載すべき事項等について具体的に整理していくことの必要性が確認された。この観点から、CP/CPS において最低限記載すべき事項等について、実施要項等の策定と合わせて検討を進める必要がある。

(4)共通証明書ポリシーOID 体系の整備

本検討会での議論においては、認証局における運営コスト削減等の観点から、共通証明書ポリシーOID を用いて 1 つの認証局の秘密鍵から「電子署名用」の電子証明書と「e シール用」の電子証明書を発行することを許容する方向で検討すべき等の議論がなされた。この点も含め、実施要項等の策定に合わせ、共通証明書ポリシーOID 体系の整備について、デジタル庁と総務省が協力して検討を進めることが適当である。

また、上記事項の検討に加え、来年度以降、e シールの普及状況についての実態把握を定期的に観測することで、本検討会において想定していた前提とのギャップ、制度運用上の課題、利用者のニーズ等を把握し、制度の普及促進を図るための取組を進めることが望ましい。

5.2 e シールの普及に向けた取組

e シールを社会に広く普及させる上では、e シールを付す者が、自らの経営判断により e シールの活用を選択する必要があり、そのためには、

- ① e シールを活用した形でのデジタル化が進むことによって削減される人件費等のコストが、e シールを利用するために必要となるコストを上回るとともに、
 - ② e シールを活用することで、上記の定量的な効果に加え、安心・安全な形でデータ流通を促進することが可能となること、
- について認識を広げてもらうための周知啓発²⁷が重要である。

その際、「e シールの保証レベル」の考え方を基に、e シールを付すことによって確保される信頼性のレベルと、それを実現するために必要なコストの関係に対する理解を広めていくことが必要である。

また、e シールの有効性を社会に浸透させていくためには、e シールを受領した側が適切

²⁷ 署名者の意思を示す電子署名と比べ、大量発行が見込まれる e シールはスケールメリットが働くことが予想され、このような差異も踏まえて、効果的に周知啓発を図ることが重要と考えられる。

に検証できることが前提となるため、e シールを始めとするトラストサービスに関するリテラシーを向上させていくことも必要となる²⁸。

こうした観点から、本検討会では、工事関係書類²⁹やオフィス機器のサポート作業報告書にeシールが活用される事例を取り上げた上で、eシールを活用することの定量的・定性的な効果等について分析を行った。

工事関係書類においてeシールが活用される事例の分析では、一定の仮定を置いた上で、eシールを付す側とeシールを検証する側の双方の視点から、eシール活用による便益(書類の確認等に係る人件費の削減等)とeシール導入に伴うコスト(サービスの契約等)について試算がなされた。

同試算によると、文書の発行元確認に係る人件費や印刷・郵送等の削減によって、従来のプロセスで発生していたトータルコストの約3分の2を削減できるという定量的な効果が確認できたほか、安心・安全な形でデータ流通を促進することが可能となるとの結論を得た。

また、オフィス機器のサポート作業報告書の事例(図 13)については、大塚商会における実際の事例を基にした試算を行い、複写紙のコスト等の削減によって、従来のプロセスで発生していたトータルコストの約4割が削減できるという定量的な効果が確認できたほか、安心・安全な形でデータ流通にも活用されることで、電子データの信頼性向上や、それに伴う顧客満足度向上に繋がるとの効果が確認された。

²⁸ 検証に係る技術的な側面については、「デジタル署名検証ガイドライン」(NPO 法人 日本ネットワークセキュリティ協会 電子署名ワーキンググループ)等で整理されており、これらの民間団体の取組も参考にすることが望ましい。

<https://www.jnsa.org/result/e-signature/2021/>

²⁹ 本検討会の事例分析では、公共工事において提出される各種工事関係書類については、保証レベル2のeシールを活用することも考え得るとの議論があった。

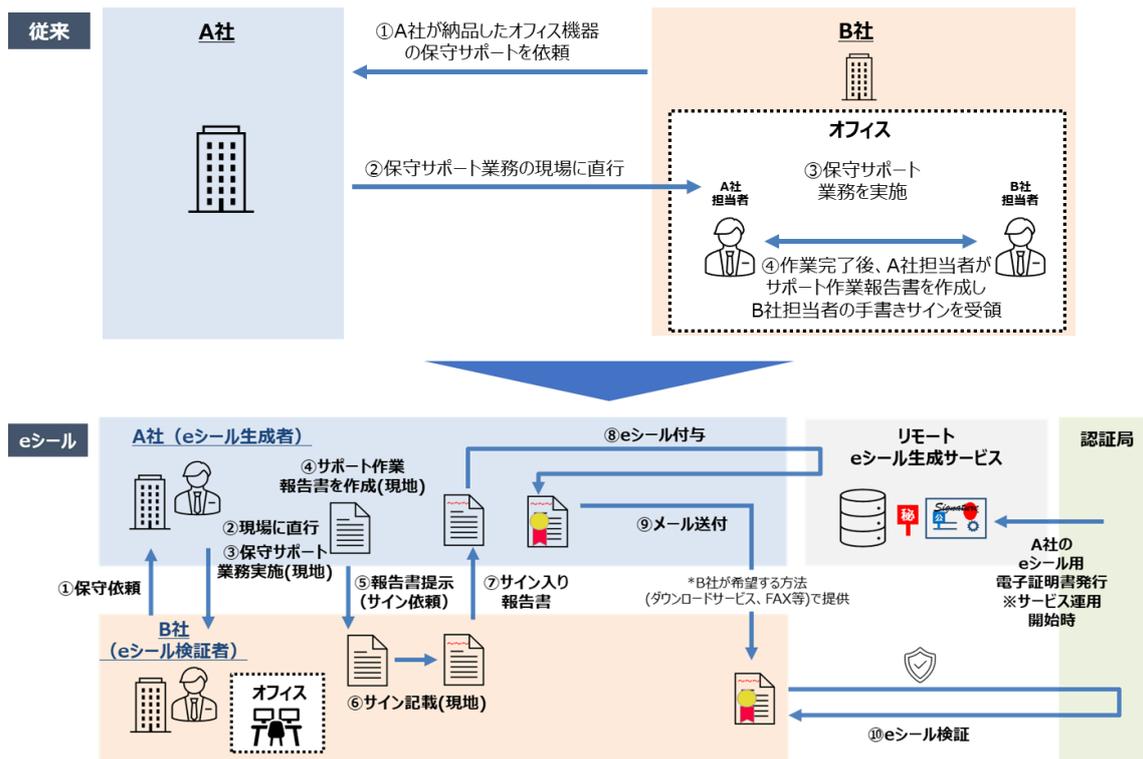


図 13 e シールの活用イメージ(サポート作業報告書)

上記以外にも様々な場面で e シールが活用されることが考えられ、今後、保証レベル2 の e シールの活用が望ましい場面についても実際の事例が出てくることで、一層、e シールの普及が進むことが期待される。

このような e シールの効果等について、デジタル庁・総務省においては、関係省庁等とも連携しながら、今後も継続的に、DX の推進や安心・安全な形でのデータ流通におけるトラストサービスの有効性を発信していくことが必要であると考えられる。

5.3 国際間のデータ流通における e シール活用の可能性

本検討会においては、中長期的なトラストサービスの活用可能性について検討材料を収集する観点から、カーボンフットプリントにおける e シール活用の事例を取り扱うとともに、「国際データ連携基盤 Catena-X/Cofinity-X における利用企業の審査・認証・登録のしくみと e シール」に関するヒアリングを行った。

カーボンフットプリントについては、欧州では蓄電池に関する「欧州バッテリー規則」が検討されており、2024 年以降、蓄電池のカーボンフットプリントが義務付けられる見込みであるため、将来的には、欧州に蓄電池及び蓄電池に関わる部品等を納品する日本企業も規制に対応することが求められる可能性がある³⁰。

³⁰ 総務省，資料 2-3 eシールの活用が見込まれる事例に関する分析(1)(カーボンフットプリント)，eシール

本事例分析では、蓄電池を始めとする各商品のサプライチェーンは多様な国のサプライヤーからサプライチェーンが構成され、我が国はサプライヤー(e シールを付す側)となることもあればメーカー(e シールを検証する側)となることも考えられることから、e シールを付す側と検証する側の両者の視点から検討を進めることの必要性が指摘された。

また、「国際データ連携基盤 Catena-X/Cofinity-X における利用企業の審査・認証・登録のしくみ と e シール」のヒアリングにおいて、欧州のデータ連携基盤を日本企業が活用使用とする場合に、我が国において欧州の eIDAS 規則や Gaia-X DCH に相当する法制度やトラスト基盤が存在しておらず、欧州法人の ID によってログインせざるを得なかった事例について紹介があった。

同ヒアリングでは、総務大臣による e シールに係る認定制度の創設は大きな一歩だとしてつつもの、今後引き続き、欧州と日本の間で相互運用・相互接続可能なトラスト基盤等の整備について検討を進める必要があると指摘された。

上記の議論に加え、欧米等における状況も参考にしながら、我が国における包括的なトラスト基盤の構築の要否や認定に係る公表方法等を含めて、戦略的に制度設計等を検討していく必要があることが指摘された。国際間のデータ流通におけるトラストサービスの活用は、上記の国際データ連携基盤以外も含め我が国が提唱する DFFT 等とも整合的であり、デジタル庁及び総務省においては、国際的な基準・規格等も踏まえながら戦略的に検討を進める必要がある。

おわりに

令和5年4月29日及び30日に群馬県高崎市で開催された「G7 群馬高崎デジタル・技術大臣会合」において議論された6つのテーマの1つとして、「越境データ流通と信頼性のある自由なデータ流通(DFFT)の推進」が位置付けられており、その重要性が強く認識されている。

その中でも、電子データは人々が生活していく上での不可欠な要素となっていることを踏まえると、安心・安全が確保された形でデータ流通を促進していくことは、デジタル化の進展に欠かせない視点となっている。

我が国において、「e シール」を始めとする「トラストサービス」の活用は、徐々に浸透しつつあるものの、依然として十分に活用されているとは言い難い状況にある中、本検討会における議論のアウトプットである「総務大臣による e シールに係る認定制度」の創設は、我が国において電子データを安心・安全に流通させるための基盤作りの大きな一歩と言える。

今後、本取りまとめを基に、認定制度の創設に向けた議論を具体化していくこととなるが、デジタル庁及び総務省においては、引き続き緊密な連携を取りながら、我が国のトラストサービスの在り方を大局的な視点から検討していくことが期待される。

(参考) e シール用電子証明書 (ITU-T X.509) の記載の一例 (イメージ)

e シール用電子証明書 (ITU-T X.509) の記載方法の一例を図 14 のとおり示す。また、図 15 に e シール用電子証明書の証明パスの表示例を示す³¹。

(補足: 図 14 の見方)

本取りまとめ案の本文で示した事項と図 14 の記載の関係は以下のとおり。

- ① 4.2.1 で示した「組織識別子」(e シール用電子証明書の発行者)については、基本領域の「発行者名」欄に記載。
- ② 4.2.1 で示した「組織識別子」(e シール生成者)については、基本領域の「主体者名」欄に記載。
- ③ 4.2.3 で示した「事業所や営業所等」については、拡張領域の「主体者別名」欄に記載。
- ④ 4.4 で示した「共通証明書ポリシーOID」については、拡張領域の「証明書ポリシー」欄に記載。

	フィールド名	値 (サンプル)
基本領域	バージョン	V3
	シリアル番号	01ab45678cdf
	署名アルゴリズム	SHA256withRSA/SHA512withRSA 等
	発行者名	発行者を識別する情報 (organization Identifierに組織識別子を格納) ①
	有効期限の開始時刻	2023年12月8日 12時30分45秒 UTC
	有効期限の終了時刻	2025年12月8日 12時30分45秒 UTC
	主体者名	発行対象となる組織等の公式名称、当該組織を識別する情報 (organization Identifierに組織識別子を格納) ②
	公開鍵情報	RSA (2048bit) 等
	鍵使用目的	digitalSignature, nonRepudiation
	基本制約	cAフラグ=FALSE
拡張領域	発行者鍵識別子	kid=1234abcd...
	主体者鍵識別子	4567cdef...
	証明書ポリシー	[1]CA固有の証明書ポリシー [2]共通証明書ポリシー ④
	主体者別名	「事業所・営業所・支店・部門名」や「組織等の和文商号」等 ③
	CRL配布点	http://example.co.jp/ica.crl
	機関情報アクセス	[1]CA証明書のURL [2]OCSPのURL
	LEI (取引主体識別子)	123456789012345ABCDE

図 14 e シール用電子証明書の記載事項の一例 (イメージ)

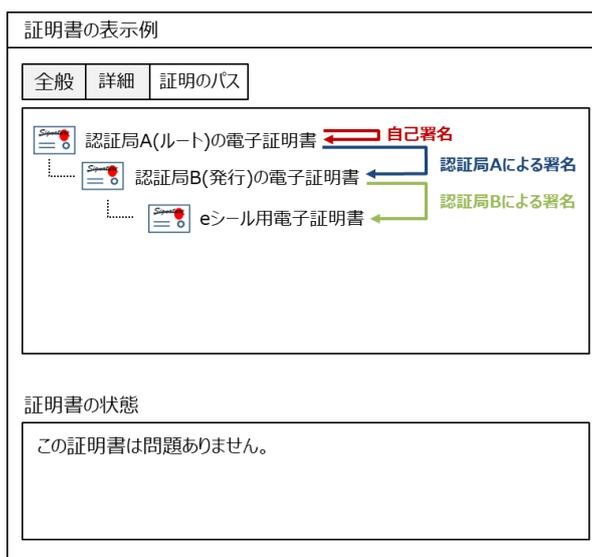


図 15 e シール用電子証明書の証明パスの表示例

³¹ e シール用電子証明書自体にも、認証局による電子署名がなされており、e シール用電子証明書の発行者の確認及び改ざん検知が可能となっている。