資料 14－４

e シールに係る指針（案）

令和3年〇月〇日

総　務　省

本指針は、e シールに係る認定基準を策定するにあたり、基本的な考え方として参考とすることを目的としたものである。

目 次

本指針の目的

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る。また、新型コロナウイルス感染拡大に伴い、テレワークの推進がより一層求められ、官民のあらゆるやり取りをデジタルで完結する要請が高まっている。

このような状況において、データを安心・安全に流通できる基盤が不可欠であり、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がその重要な役割を担うことが期待されている。

政府の検討においても、内閣官房のデジタル・ガバメント閣僚会議の下に設置されたデータ戦略タスクフォースにて取りまとめられた「包括的データ戦略」において、~~で~~我が国におけるトラストを担保する包括的な~~の~~枠組みの必要性が示されている議論~~されており、トラストサービスへの注目がますます高まっているところである~~。

トラストサービスの中でも、EU の eIDAS 規則[1]で規定されている発行元証明及びデータの完全性保証の~~機能を果たす~~ e シールは、電子文書等の発行元の組織等を簡便に確認でき、これまで紙で行われていた書類等の企業間のやりとりを電子的に安全に行えるようになることから、従来の郵送による手間や書類の確認コストを大幅に削減でき、業務効率化や生産性の向上が期待できる。

他方、e シールは、一部の企業において導入が見られるものの、我が国としての e シールに関する公的あるいは民間による認定制度や一定の技術・運用基準が存在していないこともあり、十分に導入が進んでいないことが課題となっている。

e シールについては、プラットフォームサービスに関する研究会[2]の下に設置されたトラストサービス検討 WG[3]の最終取りまとめ（2020 年2月）において、「一定程度国が関与しつつも、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」との提言がなされたことを踏まえ、サイバーセキュリティ統括官主催の「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」において、国内の類似制度や国際的な整合性等を踏まえた我が国の e シールの在り方について検討が行なわれてきた。

かかる状況を踏まえ、今般、e シールに係る技術や運用等の主な要素に関する一定の

---

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[2] 総合基盤局長及びサイバーセキュリティ統括官の共同開催（2018 年 10 月～）。プラットフォーム事業者による利用者情報の適切な取扱の確保の在り方等を検討。

[3] サイバーセキュリティ統括官主催の研究会（2019 年 1 月～2020 年 2 月）。我が国におけるトラストサービスの在り方等について検討。

基準を国が示すことによって、その基準に基づいた一定の信頼の置ける e シールサービスが立ち上がり、e シールがより広く普及することを期待して、本指針を策定することとした。

なお、e シールに係るサービスを提供する事業者は、本指針に沿った上で、更に自らの事業実態に応じて e シールサービスの信頼性向上に努めることが望まれる。

第１章　　ｅシールとは

１．１　我が国におけるｅシールの定義

発行元証明の機能を果たすｅシールの我が国における定義は、データ戦略タスクフォース第一次とりまとめ[4]で示されている“「事実・情報」：発行元証明[5]”を踏まえて、「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」とする。

ただし、ｅ シールは、あくまでも電子文書等が発行元の組織等から間違いなく発行されたことを示すためのものであり、当該電子文書等の内容が正しい内容であることかどうか、また、当該電子文書等の発行元の組織等自体が正当な組織等であるかどうかの信頼性を保証するものではないことに留意が必要である。

なお、EU では、eIDAS 規則[6]においてトラストサービスが包括的に規定されており、ｅシールは当該規則 Article3にて、“‘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（「ｅシール」とは、データの起源と完全性を保証する為に電子データに付され又は論理的に関係している電子形式のデータをいう）”と定義されている。

---

4 データ戦略タスクフォース第一次とりまとめ（令和２年 12 月 21 日デジタル・ガバメント閣僚会議決定）https://www.kantei.go.jp/jp/singi/it2/dgov/dai10/siryou_a.pdf

5 「自然人、法人や事業所などの「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などの証明（発行元証明）が必要である。」（データ戦略タスクフォース第一次とりまとめの P31 より抜粋）

~~6 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG~~

1．2　e シールと電子署名の異同

ここでは、e シールと同じくトラストサービスの1つである電子署名との異同について説明する。e シールも電子署名も電子文書等への暗号化等の措置が行われて以降、当該電子文書等が改ざんされていないことを確認できる点は同じであるが、e シールは1．1で示したとおり、発行元を証明する機能を果たす一方、電子署名は本人が電子文書を作成したこと、そして、当該電子文書に示された意思表示が当該本人によるものであることを証明する機能を果たすという点が異なる。電子署名については、電子署名及び認証業務に関する法律（平成十二年法律第百二号）（以下、「電子署名法」という。）において、電子署名の定義[7]が規定されている。なお、意思表示は自然人のみが行うことができ、電子署名も同様に自然人のみが行うことができることを前提とする。

電子署名は署名者の意思表示の証明であるため、例えば、電子契約や電子申請等の自然人としての意思表示が必要とされる用途に利用されている。他方、e シールは発行元証明にとどまり、例えば、請求書や領収書、見積書、その他各種証明書等の自然人としての意思表示は不要な、組織等が発行する電子文書等に利用されることが想定される。

そのため、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付く 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。

以上のように、利用者は e シールと電子署名の違いを十分に理解した上で、その目的に適した用途で使い分けることが重要である。

1．3　e シールのユースケース

e シールを用いることで、発行元の組織等の確認や電子文書等の改ざんの有無の確認を簡便に行うことができるようになるため、これまで人手を介して紙で行われていた書類等の企業間のやりとりを電子的に安全に行え、機械的、自動的に処理することもできるようになり、業務効率化や生産性の向上が期待される。

以下、活用が期待される具体的な e シールのユースケースの一例を紹介する。もちろん

---

7 電子署名及び認証業務に関する法律（平成十二年法律第百二号）

第二条　この法律において「電子署名」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れるものをいう。以下同じ。）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。

e シールの用途はこれらに限定されるものではない。

① 契約に紐付いて発生する書類（領収書、請求書、見積書等）

領収書、請求書、見積書等の契約に紐付いて発生する書類等については、受領側において、これらの書類が確かにやりとりを行っている相手から送られてきたものであるかを確認した上で、その後の処理（例えば、会計システムへの必要事項の入力及び入力内容の確認作業等）を行うことが想定される。

このような場面において、e シールを活用することで、発行元の組織等及び当該電子文書が改ざんされていないことを即座に確認できるため、従来の人手を介した発行元の組織等の確認や受領後の処理を、人の手を交えずにデジタルで完結することが可能となり、特に電子文書等の受領側において大幅な業務効率化及び生産性の向上が見込まれる。また、これまで発生していた紙での保存コストや紛失リスクがなくなることも期待できる。図 1 に請求書への e シールの活用イメージを示す。

また、契約締結時等交付書面等のに交付される、意思表示は不要だが発行元証明が必要な書類等にも e シールの活用が期待される。

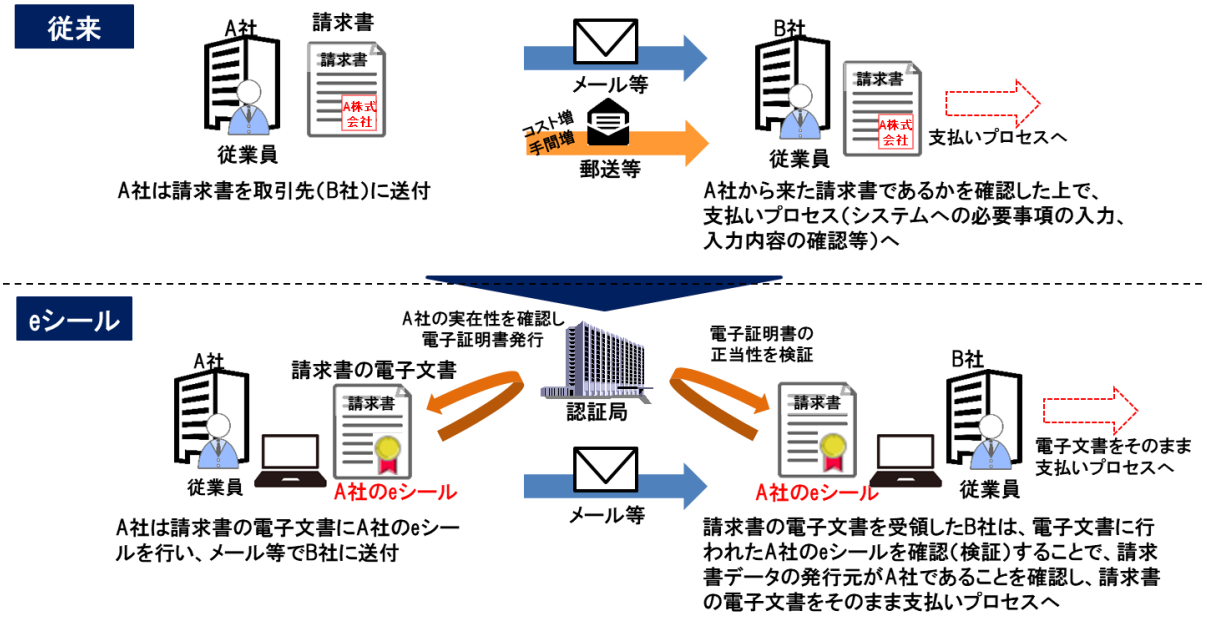


図 1 請求書への e シールの活用イメージ

② 組織等が公開する情報（IR 関連資料、広報資料等）

Society5.0 においては、あらゆる情報がデジタルで広範に流通していくことが想定される。そのような状況下では、例えば各企業の IR 関連資料、広報資料等の組織等が外部に公開する情報について、当該情報を当該組織等が間違いなく発行したかどうか（発行元の確認）が重要となる。また、当該情報が電子文書であれば、容易に改ざんが可能であることから、悪意のある者によって改ざんされた情報あるいは当該組織等になりすまして作成された情報が流通した場合は、誤った情報が流通することとなり、発行元の組織等の信頼失墜につ

ながりかねない。

このような場面において、e シールを活用することで、発行元の組織等の確認をデジタルで容易に行うことができ、かつｅシールが行われて以降改ざんされていないかどうかも確認できるため、これらの情報が安心・安全に流通することで電子文書等の二次利用も可能となり、電子文書等の利活用につながる。

③ 組織等が発行する証明書（各種証明書、各種保証書等）

各種証明書、各種保証書等の組織等が発行する証明書については、当該証明書の発行者あるいは第三者への提出・提示が必要となる場合がある。例えば、製品の保証書であれば、保証を受ける際に製品の製造元（発行元）への提出・提示が必要となる。また、資格関係の証明書であれば、企業や学校側から提出・提示を求められる可能性がある。

このような場面で e シールを活用することで、当該証明書の発行者あるいは第三者において発行元及び改ざんの有無の確認が確実に可能になり、特に各種証明書、各種保証書等の提出・提示を受ける側の確認コスト等の省力化が期待できる。また、各種証明書、各種保証書等を提出・提示する側においても、紙での保存による紛失リスクがなくなる等のメリットがあげられる。

上記以外にも、法令上保存義務のある書類等を含む各種行政手続における提出資料やデジタル監査における証憑類等の幅広い分野へのｅシールの活用も想定され、ｅシールを行う対象の電子文書等の発行側やｅシールが行われた電子文書等の受領・確認側のいずれにおいても、発行元及び改ざんの有無を簡便に確認することができ、業務効率化や生産性の向上、ひいては DX の推進に寄与することが期待される。

１．４　ｅシールの仕組み

図 2 に e シールの仕組みの一例を示す。なお、本指針では公開鍵暗号基盤（PKI）を活用した方式を例示したが、技術の進展により将来的には様々な方式が出てくることも考えられ、技術中立性の観点からはこれらの方式が排除されるものではない。

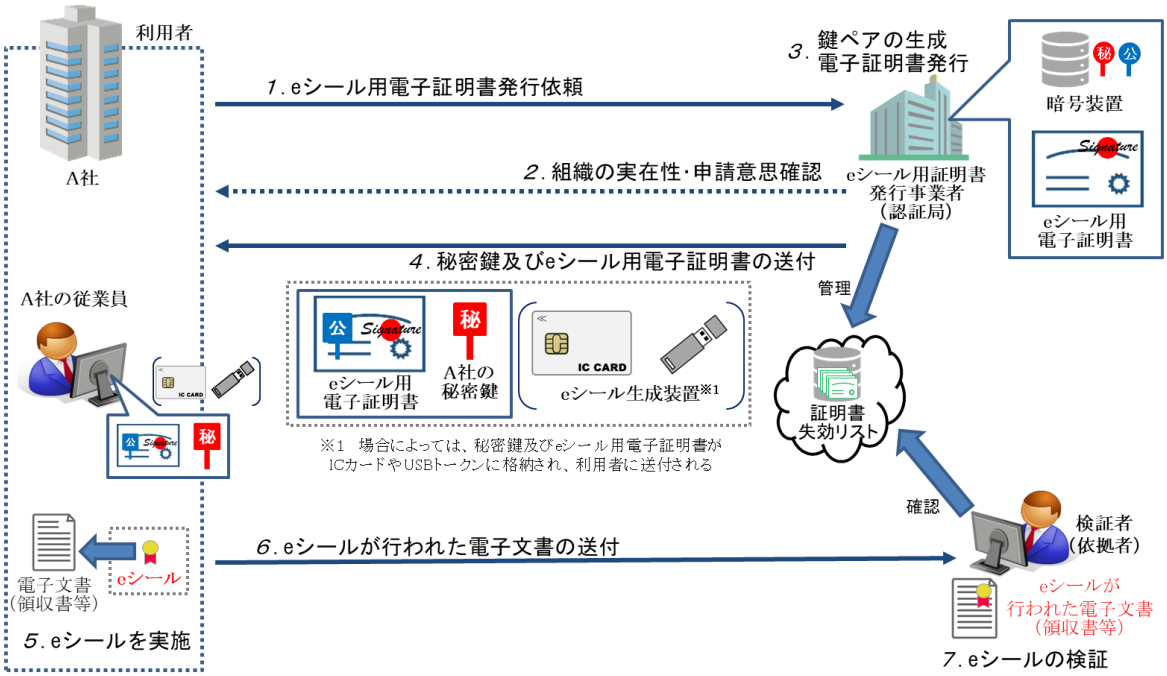


図 2　e シールの仕組みの一例

1. 5　e シールの方式(ローカル/リモート)

e シールを行う方式は、利用者の秘密鍵が保持される環境によって、主にローカル方式で行われる e シール(以下、「ローカル e シール」という。)とリモート方式で行われる e シール(以下、「リモート e シール」という。)が想定される。以下、それぞれについて簡単に紹介する。

1. 5. 1　ローカル e シール

ローカル e シールは、利用者の手元で秘密鍵を管理し、ローカル環境で e シールを行う方式である。具体的な方式については、鍵ペア(秘密鍵と公開鍵)の生成される場所によってパターンが分かれるが、例えば、認証局で生成された利用者の鍵ペア及び当該公開鍵に対して発行された e シール用電子証明書を利用者に送付するパターン(図 3)や利用者自身で利用者の鍵ペアを生成し、認証局が当該公開鍵に対して発行した e シール用電子証明書を利用者に送付するパターンが想定される。

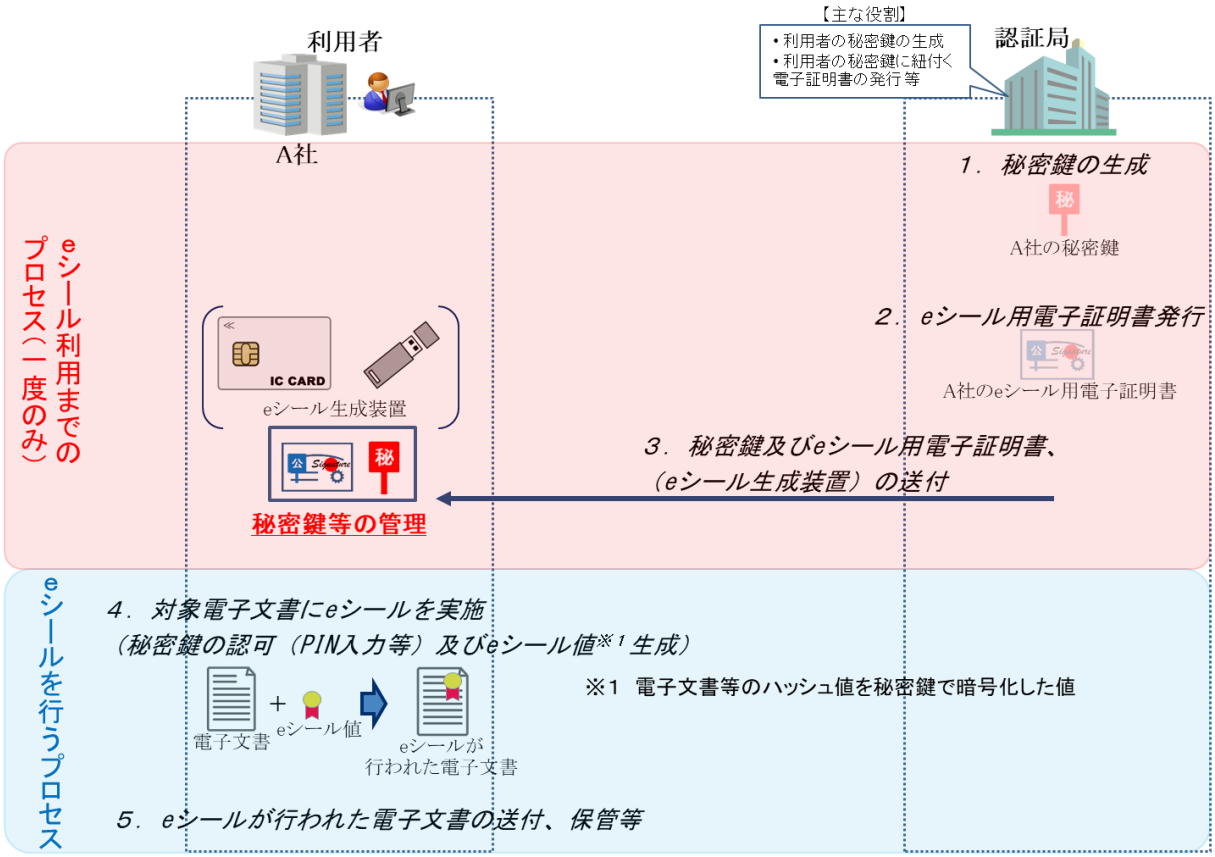


図 3 ローカル e シールの一例

1．5．2 リモート e シール

リモート e シールは、利用者がクラウド等のリモート環境にある利用者自身の秘密鍵にアクセスして e シールを行う方式であり、例えば、利用者はリモート e シールサービスを提供する事業者（以下、「リモート e シールサービス提供事業者」という。）が管理するクラウド等で管理されている秘密鍵にアクセスしてリモート環境で e シールを行うといったことが想定される。

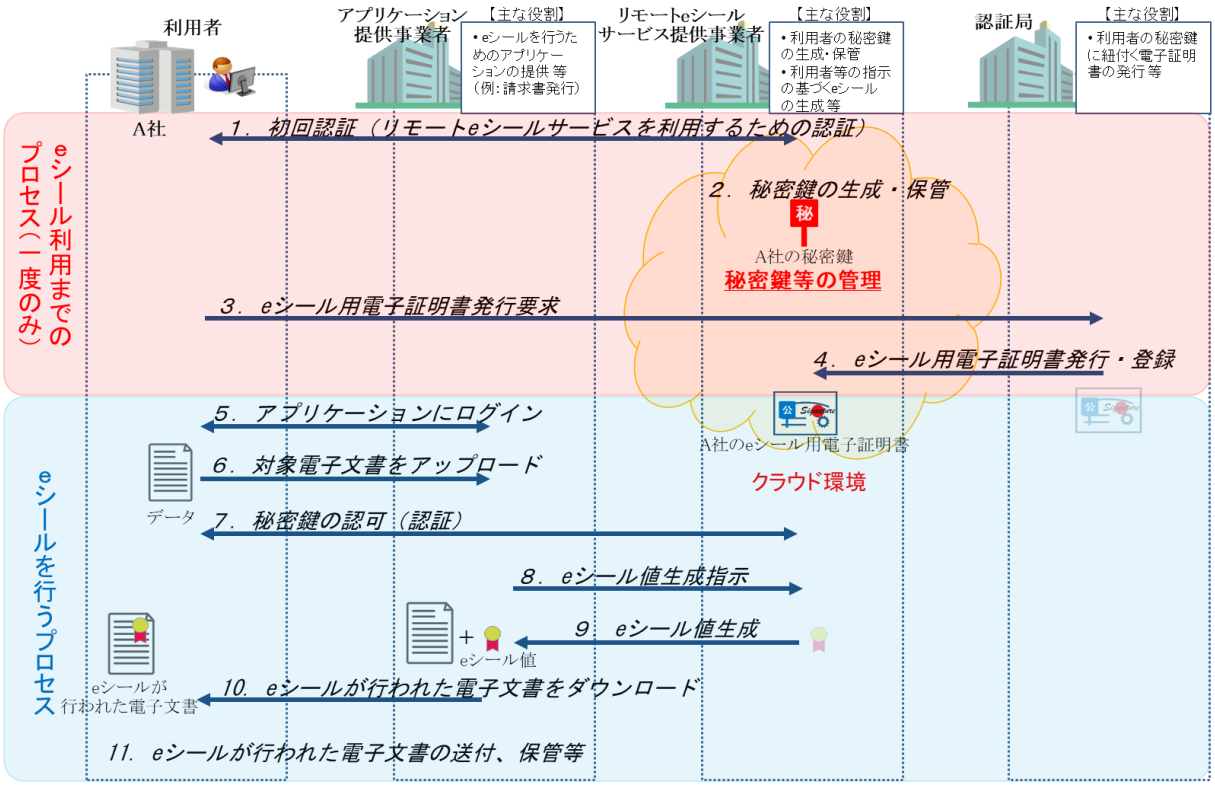
図 4 にリモート e シールの一例を示す。リモート e シールでは、利用者の秘密鍵の管理を行ったり e シールの生成を行ったりするリモート e シールサービス提供事業者が登場すること、場合によっては e シールを活用するアプリケーションを提供する事業者（以下、「アプリケーション提供事業者」という。）がリモート e シールサービス提供事業者とは別に登場することに留意されたい。

なお、リモート署名[8]と共通する全般的なセキュリティ対策や具体的な方式に関しては、電子署名に関する「リモート署名ガイドライン[9]」が参考になり得る。

---

8 利用者がクラウド等のリモート環境にある利用者の秘密鍵にアクセスして電子署名を行う方式。

9 日本トラストテクノロジー協議会（JT2A）が作成したリモート署名に関する技術的な基準を示したガイドライン。
https://www.jnsa.org/result/jt2a/data/RemoteSignatureGguide_All-r1.pdf



注） 認証局、リモートeシールサービス提供事業者のそれぞれを同一の事業者が行う場合もあり得る

図 4 リモート e シールの一例

第2章　　我が国におけるｅシールの在り方

ｅ シールの定義や特性に鑑みて、本指針で取り上げる事項は以下のとおりとする。ただし、これらの事項はあくまでもｅシール特有の事項に焦点を当てたものであり、本指針はｅシールに必要な事項を網羅的に示したものではないことに留意されたい。

- ｅシールの分類
- ｅシール用電子証明書の発行対象となる組織等の範囲
- 組織等の実在性・申請意思の確認の方法
- ｅシール用電子証明書のフォーマット及び記載事項
- 認証局/利用者の秘密鍵の管理に係る基準
- ｅシールを大量に行う際の処理
- リモートｅシールにおける認証
- 利用者におけるｅシール用電子証明書の失効要求

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[10]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。

10 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。本指針においては、信頼性の起点となる認証局を想定している。

図 5 に各ユースケースと e シールのレベルとの関係性を一例として示す。ただし、これは一例であり、e シールを利用する組織等においては、e シールを活用する場面や利用者間でのニーズに応じてそれぞれのレベルの e シールを使い分けることが可能である。

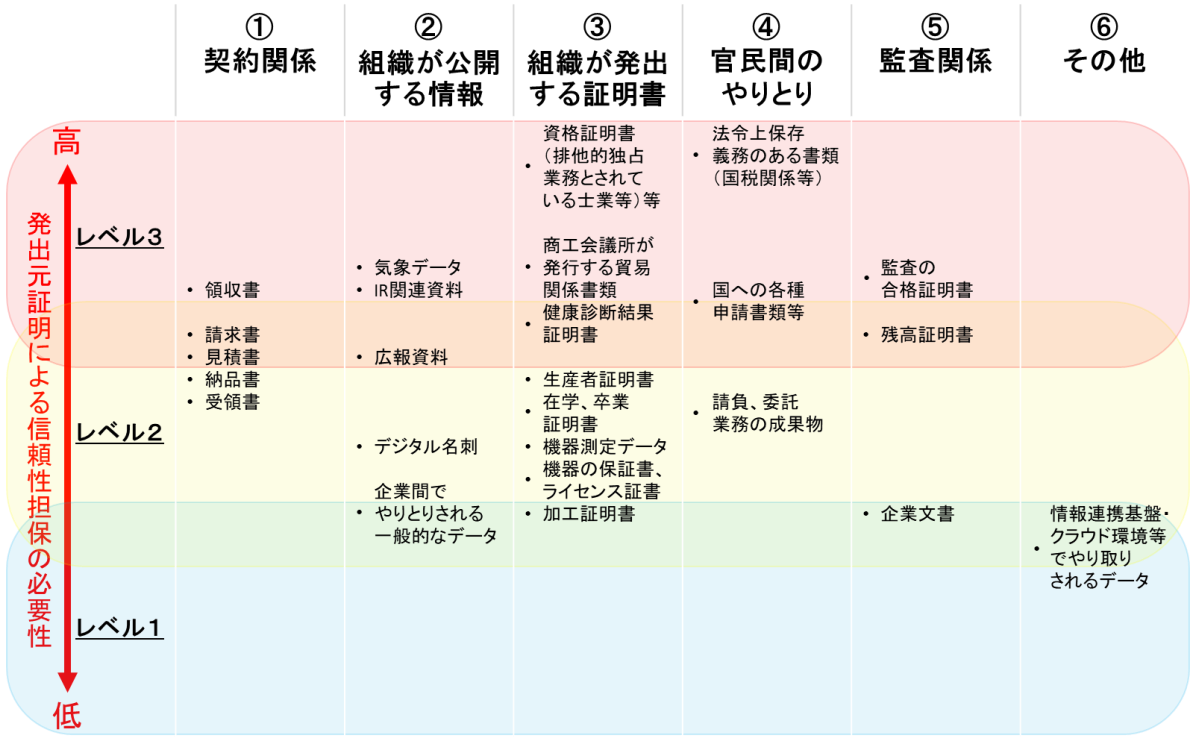


図 5 各ユースケースと e シールのレベルとの関係性の一例

2. 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。

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。

なお、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。

図 6 に e シール用電子証明書の発行対象と既存の番号体系について、ヒアリング等の

結果に基づいて整理したものを示す。もちろん、これらの番号体系は 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の候補になり得る。

			法人番号	会社法人等番号	企業コード				その他
					TDB企業コード	TSR企業コード	D-U-N-S® Number	LEI※1	
eシール用電子証明書を発行する対象	組織・団体等	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	—	—	—	—	—	—	マイナンバー、運転免許証、旅券番号 等
拡張領域に記載する対象	その他	事業所・営業所・支店・部門等	—	—	—※2	—※3	△※4	—	—
		担当者	—	—	—	—	—	—	社員番号 等
		機器	—	—	—	—	—	—	型番、シリアルナンバーの組合せ 等

（ヒアリング等の結果に基づき、一例として整理）

※1 Legal Entity Identifier： 取引主体識別コード。金融商品の取引を行う当事者（法人、ファンド等）を識別するための国際的な番号。
※2 別体系で保持。
※3 日本国内に存在する事業所にはTSR 企業コードは付与せず、事業所コードを付与。
なお、事業所コードは単独では発番せず、TSR 企業コードに必ず付随する。
※4 事業所単位で付番。
日本企業の場合、同一ビル内や事業所内にビジネスユニットが複数存在する場合、D-U-N-S®Numberを発番できるのは１箇所のみとなる。

図 6 e シール用電子証明書の発行対象と既存の番号体系の一例

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、~~より~~厳格な確認によって発行される~~レベル3の~~ 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~~レベル1、2の~~ 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

なお、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そのものではないことや組織等の実在性の確認に係る認証局のコストが膨大になることが想定されること、実空間においても各組織のルール等にしたがって文書等にこれらの情報を記載している実情（例えば、文書内に記載されている事業所名や営業所名等）があること等に鑑みて、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、認証局はそ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とする。

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。

なお、レベル3の e シールは認定主体が制度上明確である一方、レベル2の e シールはそもそも制度上の位置づけが明確でないため、レベル2の e シールサービスで第三者（当該 e シールサービスについて技術基準等を満たしているか否かの評価を行う機関）による評価を受けている場合は、評価を行った当該第三者機関の名称を拡張領域に記載するこ

とを可能とする。

	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	WWWWWWWWW
	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://xxxxxxxxxxxxxx
	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

2.5 認証局/利用者の秘密鍵の管理に係る基準

2.5.1 認証局の秘密鍵の管理

認証局の秘密鍵は、例えば悪意のある第三者に盗まれて悪用された場合、当該認証局の発行するeシール用電子証明書の信頼性が著しく損なわれてしまい、当該認証局からeシール用電子証明書の発行を受けた全ての組織等に影響が及ぶため、認証局の秘密鍵はHSM[11]等で厳格に管理されることが必要となる。また、当該HSMが配置される部屋のセキュリティ対策や不正アクセスに対する対策等も当然必要となる。

認証局のHSM自体の基準及びHSM自体の管理に係る基準について、レベル3のeシールではそのセキュリティ要件等において十分な水準を満たす必要があり、同じトラストサービスの1つである電子署名の認定認証業務[12]における認証局の秘密鍵の管理と同等の水準が求められると想定されることから、基本的には電子署名法の規定（FIPS140[13]-1 レベル3相当）を準用することとする。

---

11 Hardware Security Module の略。耐タンパー機構による物理的な安全性が確保された鍵管理機能を備えた暗号処理装置。

12 電子署名法において、特定認証業務（認証業務のうち、安全性の高い電子署名について行われるもの）のうち、業務の実施に関する厳格さの基準（利用者の真偽の確認等）に適合するものについて、主務大臣が認定した特定認証業務。

13 Federal Information Processing Standardization 140 の略。暗号モジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格。

ただし、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[14]の EAL4+[15]相当（プロテクションプロファイル[16]は別途検討が必要）とする。

2.5.2 利用者の秘密鍵の管理

ローカル e シールにおける利用者の秘密鍵については、認証局から利用者への秘密鍵の受け渡しが安全かつ確実に行われれば、それ以降は利用者の管理の問題となる。

この点については、意思表示の目的で使用され、推定規定が法定されている電子署名においても、利用者の秘密鍵等を保管する媒体に関する規定や利用者の秘密鍵の管理の仕方に関する規定は設けられておらず、利用者の秘密鍵の管理は利用者自身に委ねられている。

したがって、レベル3の~~ee~~ シールにおいても、当面は利用者の秘密鍵等を保管する媒体（例えば一定の基準を満たしたICカードやUSBトークン等の e シール生成装置（以下、「認証 e シール生成装置」という。））に関する規定を認定の要件とはせず、利用者の秘密鍵の管理は発行対象である組織等に委ねることとする。

ただし、以下の2点について、特に留意が必要である。

（1） 認証局から利用者に対する説明事項について

利用者の秘密鍵の管理は発行対象である組織等に委ねるものの、利用者自身がその管理の重要性[17]について理解する必要があることから、認証局から利用者に対する説明事項として、秘密鍵の管理に係る事項（秘密鍵の管理は厳格に行うこと（例えば、複製は望ましくない等））を規定することが必要である。なお、利用者側での複製が望ましくないことを考慮すると、当然、認証局側での利用者の秘密鍵の複製も望ましくないことに留意が必要である。利用者の秘密鍵の管理の一例を図 9 に示す。

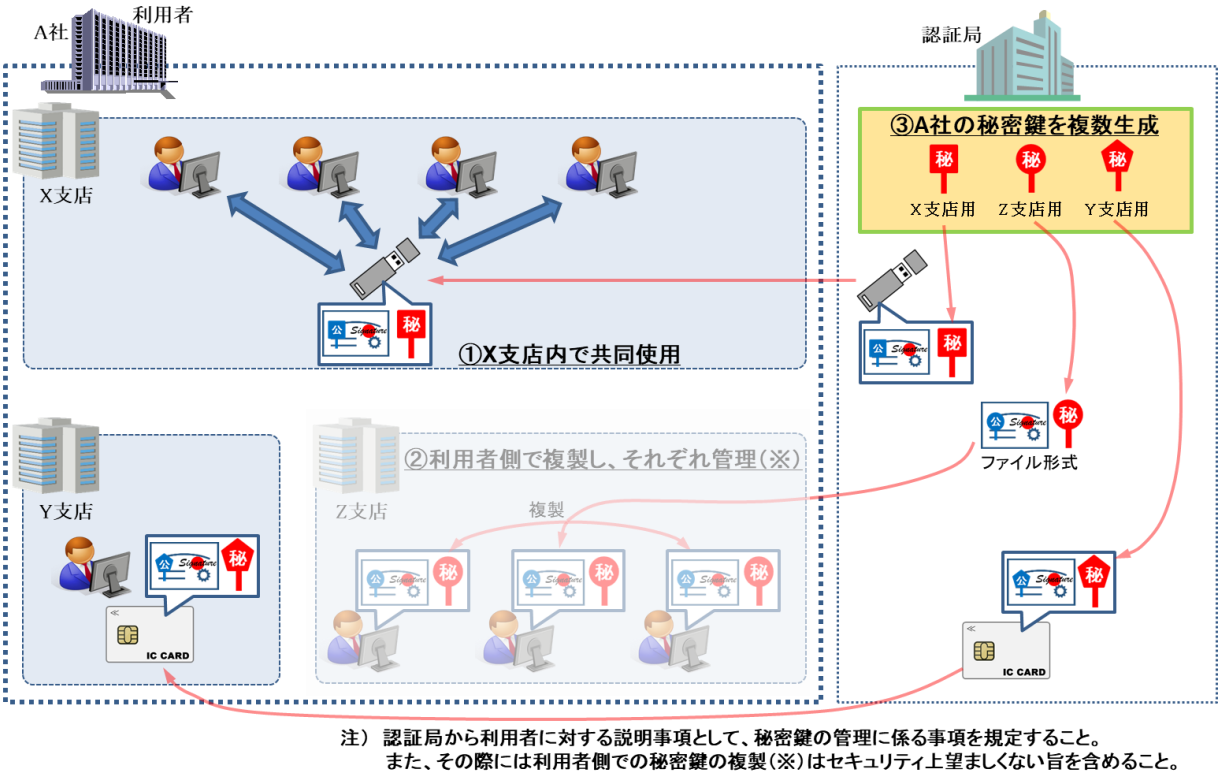
---

14 情報技術セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格。（コモンクライテリア）

15 Evaluation Assurance Level の略。実装の確かさの評価方法についてのレベル付けが決められており、政府機関向けには EAL4 が使用されている。

16 ISO/IEC 15408 で規定された、IT やシステム等に分類される一定の製品群のセキュリティ要件をまとめた文書。

17 レベル３の e シールにあっては、当該 e シールが行われた電子文書等の受領者側では、当然信頼性の高い e シールとして認識・処理されることが想定され、当該 e シールを行うために必要な利用者の秘密鍵の管理は慎重な取り扱いが求められる。



注） 認証局から利用者に対する説明事項として、秘密鍵の管理に係る事項を規定すること。
また、その際には利用者側での秘密鍵の複製（※）はセキュリティ上望ましくない旨を含めること。

図 9 利用者の秘密鍵の管理の一例

（2） e シール生成装置の使用について

e シール生成装置に関する規定はレベル3の e シールの認定の要件とはしないものの、国際的な整合性の観点では、認証 e シール生成装置が必要となる場面も将来的には想定されることから、認証 e シール生成装置を用いてもよいこととし、認証 e シール生成装置を用いて行われた e シールであるかどうかを検証者が判断できる仕組みとしておくことが望ましい。

なお、電子署名法も含め、将来的にセキュリティ上の問題が生じた場合には、改めて生成装置の要否について検討が必要となるが、仮に生成装置を求めることになった場合は、現状の電子署名法の認定基準の強化（これまで認められていたものが認められなくなる）となる点に留意が必要である。

2．6 e シールを大量に行う際の処理

e シールにおいては、業務効率化の観点から、ローカル/リモート e シールにかかわらず、機械的、自動的に複数の対象電子文書等（例えば領収書等）に対して一括で e シールを行うニーズが想定される。

一括処理については、我が国における実空間での手続においても複数の対象文書に対してまとめて決裁・押印することが一般的に行われており、また、そもそも e シールは意思表示を伴わず、発行元証明にとどまることに鑑みて、レベル3の e シールであったとしても、

複数の対象電子文書等に一括でｅシールを行うことを認める。

ただし、一括でｅシールを行う際には、当然利用者が指定した電子文書のみにｅシールが行われることが求められることから、特にリモートｅシールにおいては、利用者がｅシールを行う対象とした電子文書に、他の電子文書が紛れ込むことがないことを ｅ シールサービス提供事業者側で担保する必要がある。

２．７　リモートｅシールにおける認証

２．７．１　　リモートｅシールを行う際の認証

ローカルｅシールにおいては、一般的に利用者自身が管理している秘密鍵を PIN コード等によって鍵認可[18]を行い、ｅシールを行う形式が想定される。他方、リモートｅシールでは、利用者の秘密鍵を利用者自身で管理するのではなく、リモート ｅ シールサービス提供事業者が管理するため、レベル3のリモートｅシールを行う際の認証について検討が必要となる。

ローカルｅシールにおける認証を踏まえると、リモートｅシールにおいては、まずは利用者の秘密鍵が保管されているリモート ｅ シールサービス提供事業者のクラウド環境等にアクセス（以下、「利用認証」という。）し、その後、鍵認可を行ってｅシールを行う必要がある。

すなわち、レベル3のリモートｅシールにおいては、少なくとも利用認証（ｅシールを行うことができる権限者（リモート ｅ シールサービスへの登録者）であることを示すための認証）と鍵認可（実際にｅシールを行うために利用者の秘密鍵を利用できる状態にすること）を別に行うことが求められる。なお、意思表示を伴う電子署名は推定規定[19]が法定されていることもあり、リモート署名に関する「リモート署名ガイドライン」において、利用認証と別に鍵認可を行うことに加え、鍵認可は複数要素認証を要求しているが、リモートｅシールの鍵認可においては、ｅ シールが意思表示を伴わない発行元証明にとどまることに鑑み、単要素認証でも可とする。

２．７．２　　鍵認可で使用する要素の管理

利用者の秘密鍵をリモートｅシールサービス提供事業者が管理することになるリモートｅシールにおいて、例えば、リモート ｅ シールサービス提供事業者が PIN コード等の鍵認可で使用する要素（以下、「認証要素」という。）も管理し、利用者に断りなくｅシールを行うことができる可能性がある場合は、ｅ シールを行った利用者、すなわち発行元が誰であるかの判断ができなくなる可能性がある。仮にレベル3のリモート~~ee~~ シールにおいて、認証要素の管理が適切に行われない可能性がある場合には、信頼性が損なわれたレベル3の~~ee~~ シールが存在・流通し、制度の安定性そのものに影響を与えかねない。

---

18 利用者の秘密鍵を活性化し、利用できる状態にすること。

19 電子署名及び認証業務に関する法律（平成十二年法律第百二号）
第三条　電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について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。）が行われているときは、真正に成立したものと推定する。

また、電子署名を活用した電子契約サービスの場合には、文書の名義人間で、どのような方式を取るかの合意があるため、リモート署名サービスの利用について、双方の合意があるとみなす余地がある一方、~~ee~~ シールの場合には、~~ee~~ シールが行われた電子文書等の受領者（例えば領収書の受領者）は、リモート~~ee~~ シールサービスの利用について協議を受けられない蓋然性が高い。

これらを勘案し、認証要素の管理は基本的には利用者が行うこととする。また、e シールとしての用をなさないレベル3の e シールが存在、流通することを防止するため、レベル3の ~~ee~~ シールをリモートで行う事業者（リモート e シールサービス提供事業者）のサービスについては、一定の基準（例えば認証要素の管理は不可とする等）が必要である。なお、レベル3のリモート e シールについて、認証要素をアプリケーション提供事業者が管理することは、当然望ましくない。

2．8　利用者における e シール用電子証明書の失効要求

利用者の秘密鍵が危殆化[20]したり、組織等の統廃合が発生したりした場合は、適切なタイミングでの当該 e シール用電子証明書の失効が求められる。特に、利用者の秘密鍵の危殆化については、第三者によるなりすまし等の悪用のおそれがあることから、当該秘密鍵に係る e シール用電子証明書は、可及的速やかに失効される必要がある。

電子署名の場合は利用者の秘密鍵とそれを扱うことができる者が1対1であるのに対し、e シールの場合は、利用者の秘密鍵一つにつき、組織内の複数人が利用することが想定され、当該秘密鍵の失効を要求できる者について検討が必要となるが、失効要求には、e シール用電子証明書の発行申請と同様に意思表示が伴うことから、失効要求できる者は e シール用電子証明書の発行を要求できる者（法人であれば代表者又は代表者から委任を受けた者）に限定することとする。

[20] 秘密鍵の情報が第三者に漏洩、またはそのおそれがある場合や秘密鍵の PIN コード等を紛失した場合など、セキュリティレベルが著しく低下した状態。

おわりに

データが価値の源泉となり、重要な価値を持つデータ駆動型社会においては、データの信頼性の確保、そして安心・安全なデータ流通を支えるための堅牢なトラスト基盤の構築が鍵を握る。

特に新型コロナウイルスの感染拡大への対処が引き続き求められ、~~リモート~~テレワークなどの新たな働き方が推進される社会状況の中で、官民を問わずあらゆる手続を電子的にスムーズに完結することに対するニーズは飛躍的に増大した。

このような中、既存の制度である、意思表示を伴う電子署名ではカバーしきれないその他諸々の情報の起源や完全性をより容易かつ手軽に保証する仕組みへの期待も日に日に高まってきている。

さらに、このような流れに加えて、日本企業を取り巻くビジネス環境も時々刻々と変化し、益々国際間のビジネスが飛躍的に増加する中で、海外の取引先等との円滑なデータのやり取りを可能ならしめる仕組みへの要請も高まってきた。

かかる状況を受け、総務省は昨年４月から「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」（e シール検討会）を開催し、e シールの活用が期待されるユースケースの発掘に始まり、国内や諸外国の類似のトラストサービスに関する事例・制度を参考にしながら、我が国における e シールの在り方について検討を行った。

併せて、昨秋来の内閣官房におけるデータ戦略タスクフォースでのトラストサービスの枠組みの整備の検討に関する議論や世の中のニーズに応えて検討を加速させ、想定よりも短期間で主要な論点を網羅し充実した検討・議論を行い、その結果を本指針という形でまとめた。

本指針が e シールの認定制度の開始の一助となるとともにそれに弾みをつけ、データ流通の信頼性確保の向上に繋がることを願ってやまない。

なお、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。