別紙4

# e シールに係る指針

## （第2版）

令和6年4月

総　務　省

# 目　次

# 本指針の目的等

## 本指針の目的

本指針は、我が国における e シール用認証業務[1]等の在るべき姿を示すことによって、e シール用認証業務を提供する認証局を始めとする関係者が参考にすべき技術・運用上の基準を示すことを目的とするものである。

## 本指針策定の経緯

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。

政府が令和5年6月9日閣議決定した「デジタル社会の実現に向けた重点計画」においても、「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」とした上で、「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」こととしており、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、e シールを始めとするトラストサービスの重要性を規定している。

総務省においては、令和2年4月に開始した、「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」における議論を経て、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」（令和 3 年 6 月 25 日総務省策定。以下「旧指針」という。）を策定した。e シールの更なる普及や活用を促す観点から、令和5年9月より「e シールに係る検討会」を開催し、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との結論を得たことから、当該認定制度の創設に合わせ、旧指針を改定することとした。

[1] 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。

## 本指針と旧指針の適用関係

ｅ シールに係る認定制度の運用開始までは旧指針を適用し、認定制度の運用開始以後に本指針を適用することとする。

# 第1章　　e シールとは

## 1．1　e シールの定義

e シールは、企業等が発行する電子データの発行元を証明し、また、電子データに改ざんがないことを証明できるようにする（以下「トラストを確保する」という。）ために用いられる。これにより、電子データの発行元のなりすましや改ざんを確認可能で、これらを防止する効果が期待されている。

我が国における e シールの定義は以下のとおりとする。

「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。

## 1．2　e シールと電子署名の異同

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 12 年法律第 102 号。以下「電子署名法」という。）において、電子署名の定義[2]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

[2] 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。

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。

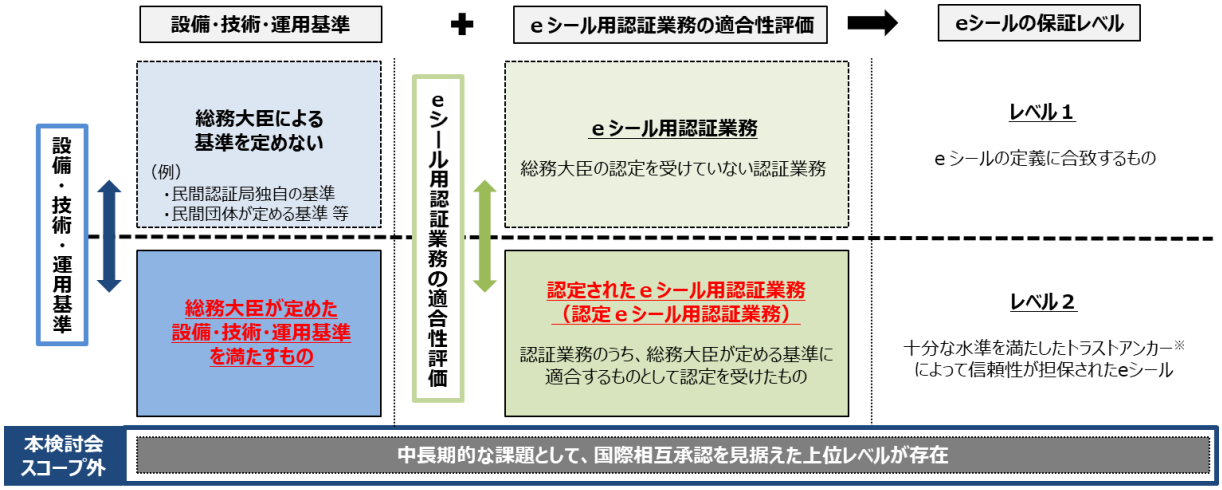
そのため、意思表示という性質から利用者たる自然人との紐付きが強固である電子署名とは異なり、発行元となる組織等に紐付く e シールは、組織内の人事異動に伴って e シール用の電子証明書を再発行する必要がないことや、意思表示を伴わないため、大量の電子文書等に機械的、自動的に e シールを付与することもできること等のメリットがあるが、e シールが付された電子文書等には e シールを行った自然人の意思は顕れていないことに留意する必要がある。

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 シールの保証レベル

「e シールの保証レベル」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（以下「認定 e シール用認証業務」という。）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と、②認定 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起源や改変が行われていないことについて高い信頼が期待される保証レベルの２段階に分ける形で整理する。

なお、図１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。




※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、信頼性の基点となる認証局を想定している。

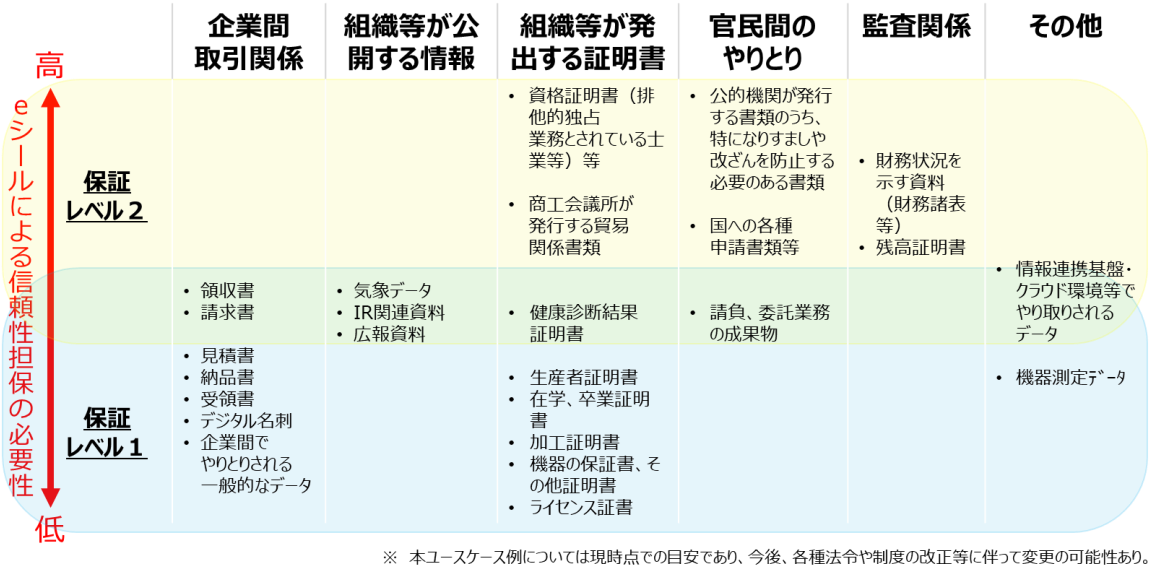
**図１　e シールの保証レベル**

## 1．4　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。また、これまで発生した紙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。

e シールの活用が見込まれる分野としては、企業間取引関係、組織が公開する情報、組織が発出する証明書、官民間のやりとり、監査関係、その他が考えられる。各分野において、e シールの付与対象となる電子文書等が求める信頼性の度合に応じて、異なる保証レベルの e シールを使い分けることが考えられ、一例として前節で示した e シールの保証レベルと各ユースケースとの関係性のイメージを図2に示す。

ただし、これは一例であり、e シールを付与する組織等においては、電子データが毀損された場合の損害の大きさや、電子データに求められる信頼性、重要性、e シールを活用する場面や利用者間でのニーズ等に応じてそれぞれの保証レベルの e シールを使い分けることが可能である。また、今後、各種法令や制度の改正等に伴って変更の可能性がある。




※　本ユースケース例については現時点での目安であり、今後、各種法令や制度の改正等に伴って変更の可能性あり。

**図2　e シールの保証レベルと各ユースケースとの関係性のイメージ**

以下、eシールの活用が期待される具体的なユースケースの一例を紹介する。もちろんeシールの用途はこれらに限定されるものではない。

### １．４．１　　保証レベル2のｅシールの活用が想定されるユースケース

① 組織が発出する証明書（排他的独占業務とされている士業等の資格証明書等）

排他的独占業務とされている士業等の資格証明書については、トラストが確保されていることに関して高い信頼性を有することが求められるため、認定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起源や改変が行われていないことについて高い信頼が期待される「保証レベル2」のｅシールを活用することが望ましい。

この場合において、図3に示すとおり、電子化されｅシールが付された資格証明書について、改ざん等がなされていないことを自動検証できるため、当該資格証明書の申請・発行においてもデジタル完結が可能となるなど、デジタル化の推進に繋がることが期待される。

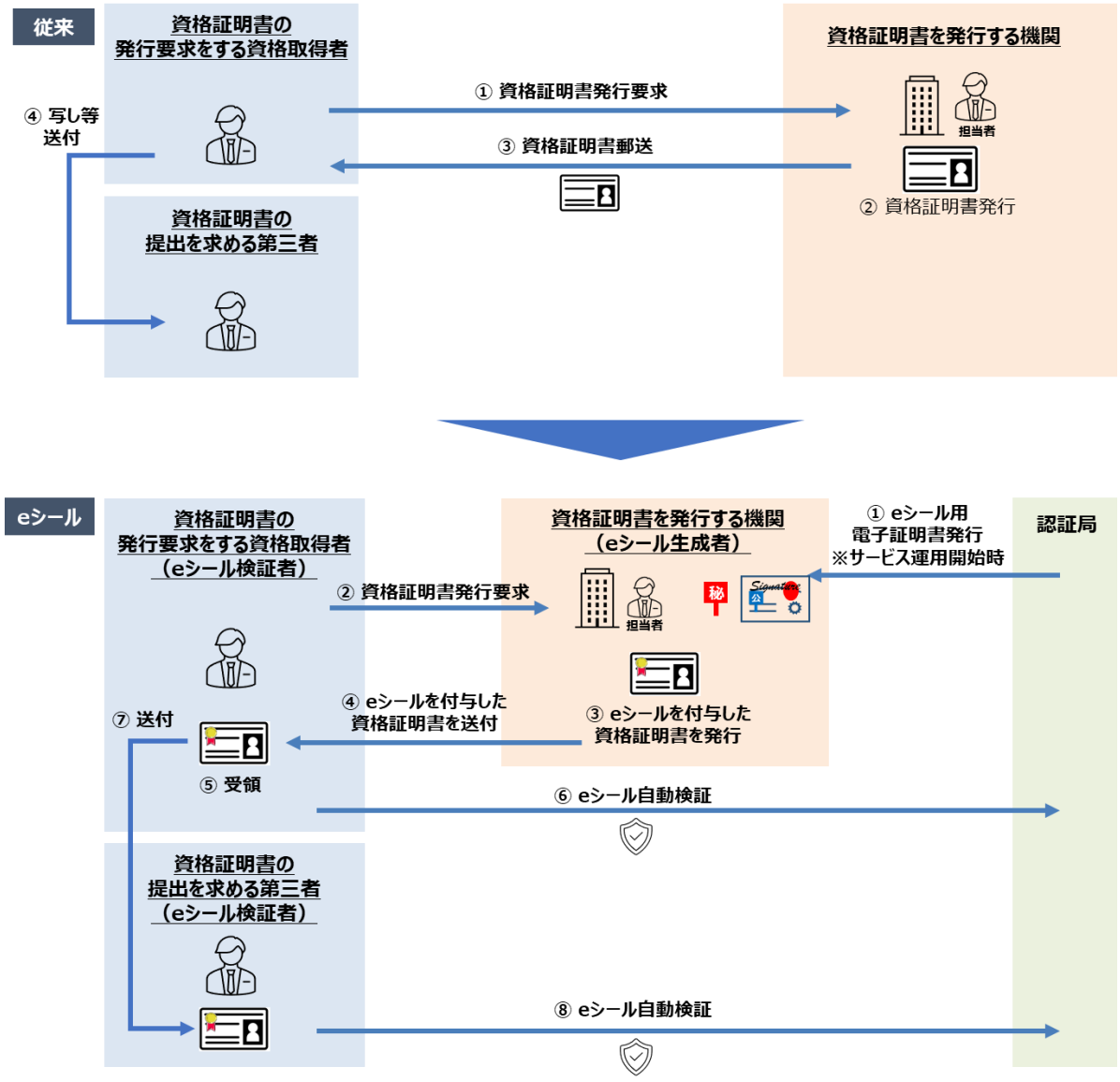



**図3　ｅシールの活用イメージ（資格証明書）**

② 官民間のやりとり（公的機関が発行する書類のうち、特になりすましや改ざんを防止す

る必要のある書類等）
官民間のやりとりの中で、公的機関が発行する書類のうち、特になりすましや改ざんを防止する必要のある書類については、トラストが確保されていることに関して高い信頼性を有することが求められると考えられる。

この場合、認定 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起源や改変が行われていないことについて高い信頼が期待される「保証レベル2」の e シールを活用することが望ましいと考えられる。

③ 監査関係（財務諸表等の監査証拠となる資料等）
会計監査において用いる財務諸表等の監査証拠となる資料等については、企業の利害関係者が経営状況を判断し、投資や取引の相手として適当か判断するために重要な資料となるものである。

したがって、当該資料等を電子化する場合、トラストが確保されていることに関して高い信頼性を有することが求められるものであり、認定 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起源や改変が行われていないことについて高い信頼が期待される「保証レベル2」の e シールを活用することが望ましい

### １．４．２　保証レベル1の e シールの活用が想定されるユースケース

① 組織が発出する証明書（電化製品の電子保証書等）
1.4.1 で示したとおり、排他的独占業務とされている士業等の資格証明書においてはトラストの確保に関して高い信頼性が求められるが、組織が日常的に発出する各種証明書等においては、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1」の e シールでも足りると考えられる。

この例として、例えば、電化製品の電子保証書が挙げられ、一部の家電量販店においては既に電子的な保証書の提供等を行っているが、電化製品の購入日の改ざんなど保証書の偽造を防ぐ観点からも、e シールを活用することで、ユーザ満足度の向上が期待される。

② 企業間取引関係（企業間で日常的にやり取りされるデータ等）
企業間で日常的にやり取りされるデータ等については、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1」の e シールの活用が期待されるケースが多いと考えられる。

例えば、我が国において、e シールが実際に活用されている事例として、工事関係書類[3]

[3] 「e シールに係る検討会」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。

や図4に示すサポート作業報告書への ｅ シールの活用が挙げられる。図4において、従来は紙で作成・共有されていたサポート作業報告書を電子化し、ｅ シールを付すことによって、紙資料の破棄コストや保管コスト等の削減といった定量的な効果に加え、顧客満足度向上やデータの信頼性向上といった定性的な効果も確認されている。本事例ではサポート作業報告書を取り上げたが、企業間で日常的にやり取りされるデータ等においても定量的・定性的な効果が期待される。

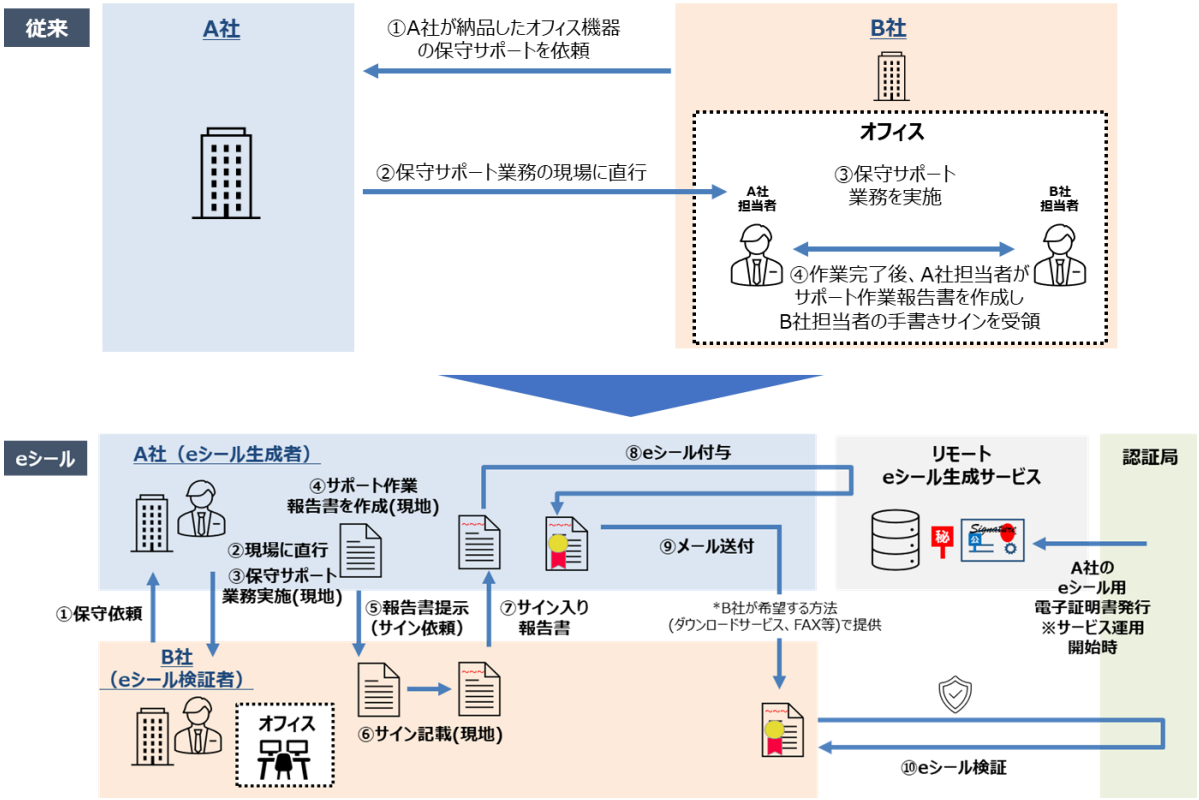



**図4　ｅシールの活用イメージ（サポート作業報告書）**

③ 組織が一般公開する情報（広報資料等）

企業等において自らのホームページに掲載する広報資料等について、当該資料が第三者に流通した際に改ざん等がなされる可能性があることを踏まえると、トラストを確保するためにｅシールを活用することが考えられる。

この場合において、企業等が日常的に公開する広報資料等については、必ずしも認定 ｅシール用認証業務によって保証されてはいる必要はなく、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１」のｅシールでも足りる場合も多いと考えられる。

## 1．5　e シールを用いてトラストを確保する仕組み

図5に e シールを用いてトラストを確保する仕組みの一例を示す。この例は公開鍵暗号基盤（PKI）を用いた例である。e シール用電子証明書を発行する認証局が鍵ペアを生成する場合、認証局が発行した e シール用電子証明書と秘密鍵を格納した媒体（以下「格納媒体」という。）を e シール生成者に送付し、e シール生成者は格納媒体を用いて電子データに e シールを付す。e シール生成者は e シールが付された電子データを受信者（e シール検証者）に送信し、e シール検証者は e シール用電子証明書が失効されていないことを確認し、電子データに改ざんがないことを検証することで、電子データのトラストを確保することが可能となる。

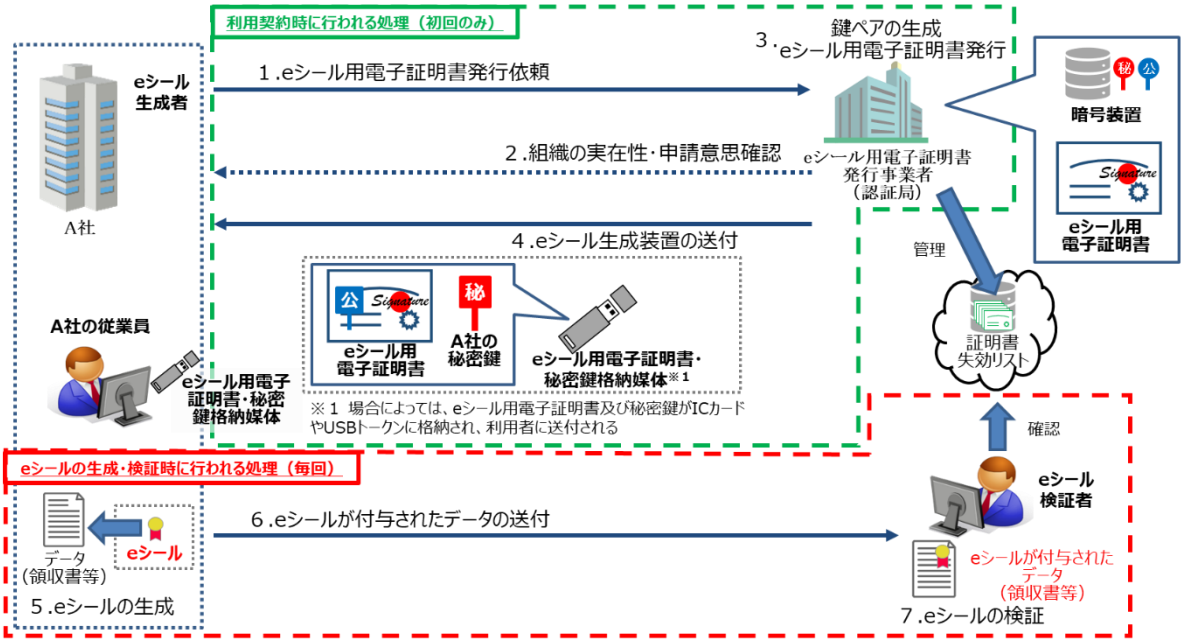



**図5　PKI を用いた e シールの仕組みの例**

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。

## 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）

e シールの生成方式は、e シール生成者の秘密鍵が保持される環境の違いによって、ローカルで秘密鍵を保持して発行する e シール生成方式（以下「ローカル e シール方式」という。）とリモートで秘密鍵を保持して発行するする e シール生成方式（以下「リモート e シール方式」という。）に大別される。以下、それぞれについて簡単に紹介する。

### 1．6．1　ローカル e シール方式

ローカル e シール方式は、e シール生成者の管理下にある環境で秘密鍵を保持し、この環境で e シールを生成する方式である。鍵ペア（秘密鍵と公開鍵）の生成される場所によって更にいくつかのパターンに分かれる。例えば、認証局で e シール生成者の鍵ペア及び当該公開鍵を生成し、秘密鍵と公開鍵に対して発行された e シール用電子証明書を e シール生成者に送付するパターン（図6）や、e シール生成者が自ら鍵ペアを生成した後に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 e シール生成者に送付するパターンが想定される。

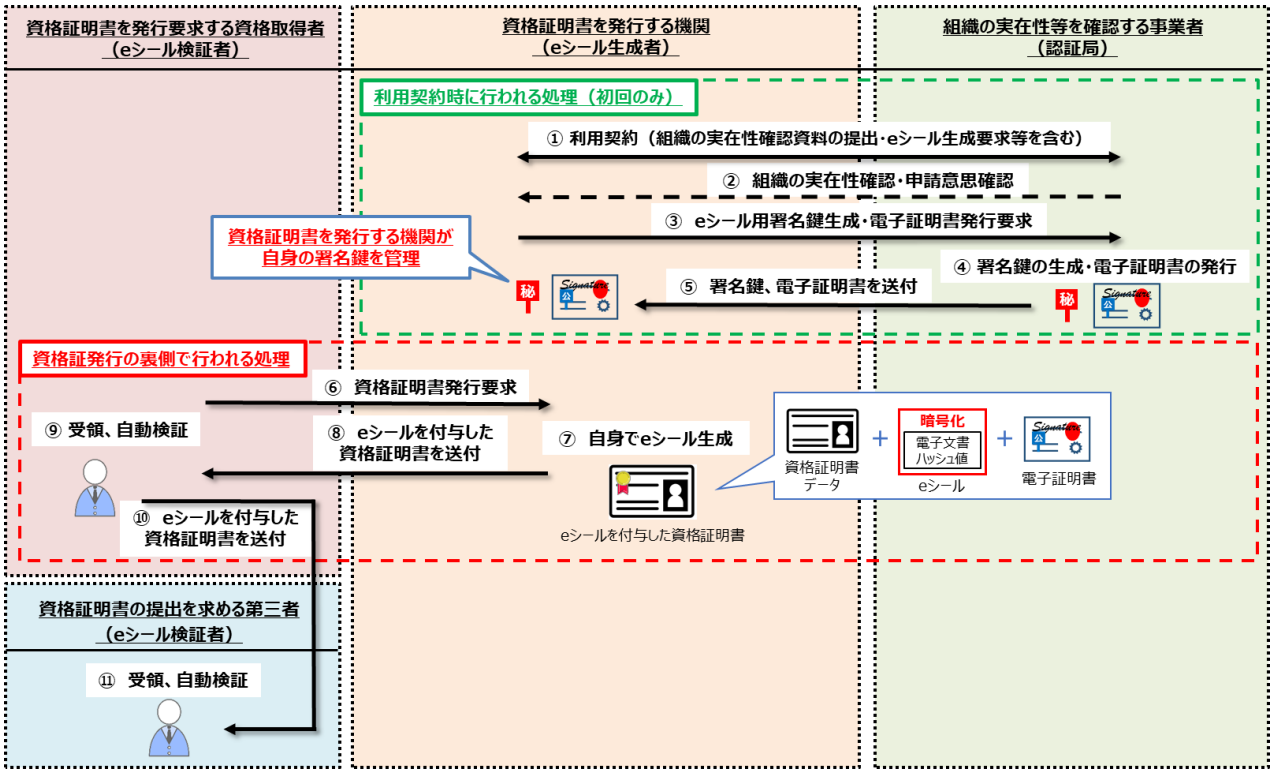



**図6　ローカル e シール生成方式の一例（資格証明書データに対して e シールを付与する事例）**

### 1．6．2　リモート e シール方式

リモート e シール方式は、e シール生成者がクラウド等のリモート環境に秘密鍵の管理を委ね、リモート環境にアクセスして e シールを生成する方式である。例えば、e シール生成者がリモート 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に秘密鍵の管理を委ね、同クラウドにアクセスしてリモート環境で e シールを生成するといったことが想定される。

図7にリモート e シール生成方式の一例を示す。リモート e シール生成方式では、リモート e シールサービス提供事業者が、クラウド等において e シール生成者の秘密鍵の管理を行い、e シール生成者の指示に基づいて e シールを生成する。また、本事例で示すように、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、認証局やリモート e シールサービス提供事業者とサービス連携して、電子デー

タに機械的かつ自動的に e シールを付与するサービスを提供可能であることも留意されたい。

なお、リモート e シール方式はリモート署名[4]と共通する部分が多いため、リモート e シール方式に求められ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[5]」が参考になり得る。

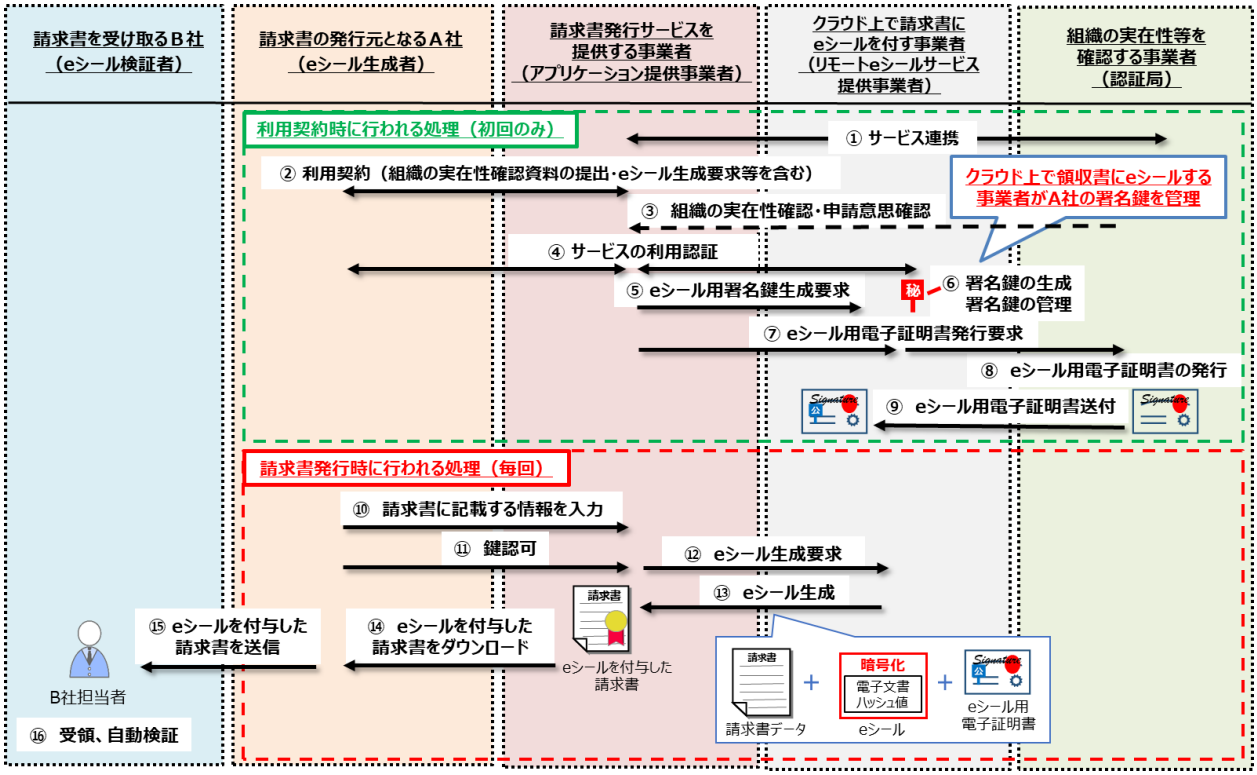



**図7　リモート e シール生成方式の一例（請求書データに対して e シールを付与する事例）**

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

[5] 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

# 第2章　　我が国における e シール用認証業務の在り方

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電子署名法やタイムスタンプに係る認定制度等を参考とし、PKI の利用を前提とした上で、認定 e シール用認証業務に求められる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 シール用電子証明書の発行対象となる組織等の範囲
- e シール生成者の実在性・申請意思の確認の方法
- e シール用電子証明書のフォーマット及び記載事項
- 認証局の秘密鍵の管理に係る基準
- e シール生成者の秘密鍵の管理に係る基準
- e シールを大量に生成する際の処理
- リモート e シール方式における利用認証
- e シール用電子証明書の失効要求

## 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

eシール用電子証明書の発行対象となる組織等、すなわち e シール生成者を識別するためには、当該組織を一意に識別できる識別子が必要となるが、e シール用電子証明書の発行対象となる組織等の範囲は、当該組織識別子の発番対象となる組織等の範囲に依存する。

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） [6,7] と公的機関が発行する既存の番号体系を組み合わせて使用する。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」と組み合わせて、組織識別子を構成することとする[8,9]。なお、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は、法人番号を使用した組織識別子を記載することを要件とするが、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。

また、保証レベル1の e シール用認証業務の e シール用電子証明書については、民間

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

[7] ETSI, ETSI TS 119 412-1 V1.3.11, 2019-08

[8] 政府機関や地方自治体が認定に係るeシールを使用する場合、プレフィクス「GOVJP」と「法人番号」を組み合わせて使用可能とする。

[9] 「個人事業主の番号体系」については、適格請求書発行事業者登録番号が候補として挙がったが、公表サイトにおいて掲載される情報によって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こと等により、引き続きの検討課題とした。

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 e シール用認証業務に係る 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。その場合、プレフィクスについては、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。)[10]を使用することを推奨する[11]。

なお、組織内における事業所・営業所・支店・部門単位や、組織の担当者(意思表示を伴わない個人)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保証レベル 2 及び保証レベル 1 ともに、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[12]。

上記を踏まえて、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格納する組織識別子については図8のとおり整理することとし、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ついては、図9のとおりいずれかの組織識別子の使用を推奨する。

【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**

[10] 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。
[11] 取引主体識別子(LEI; Legal Entity Identifier) については「LEI:XG」を使用することを推奨する。
[12] 電子機器に対して e シール用電子証明書の発行対象としてのニーズがあるが、電子機器が e シールの生成主体となることについて、技術面及び制度面で十分な検討が行われていない。

【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9 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**

## 2．2 e シール生成者の実在性・申請意思の確認の方法

e シールの信頼性は、e シール用電子証明書の発行対象となる組織等（すなわち、e シール生成者）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。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場合は厳格な方法による確認が必要であり、保証レベル 1 の e シール用認証業務の場合はより低コストで簡易な方法による確認を可能とする。

e シール生成者の実在性の確認については、①法的な存在、②物理的な存在、③運営的な存在の 3 点について確認することが想定される。具体的な確認方法として、法的な存在については登記事項証明書等を用いて確認することとし、物理的・運営的な存在については第三者機関データベース等を用いて確認することが想定される。

また、e シール生成者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。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。

上記を踏まえて、CA/Browser Forum のガイドライン[13]等を参考に、保証レベル2の認定 e シール用認証業務における組織等の実在性確認方法のイメージを図 10、申請意思の確認方法のイメージは図 11 のとおり整理する。

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

| 組織等の分類 | 組織等の実在性の確認 | | |
|---|---|---|---|
| | 法的実在性確認 | 物理的実在性確認 | 運営確認 |
| ・法人<br>・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。<br>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、同第3項の規定で証明されているものに限る。）<br>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条に基づく認定認証業務）<br>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。<br>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<br>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。<br>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<br>2. 第三者機関データベース※1の登録を確認（★）<br>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 10 保証レベル2の認定ｅシール用認証業務における組織等の実在性確認方法のイメージ**

| 組織等の分類 | 組織等（代表者）の意思の確認 | 組織の代表者の在籍の確認 |
|---|---|---|
| ・法人<br>・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<br><br>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】<br>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（★）<br><br>【乙： 意思の確認が②、又は甲で確認できない場合】<br>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 11 保証レベル2の認定ｅシール用認証業務における申請意思確認方法のイメージ**

また、保証レベル 1 の ｅ シール用認証業務における組織等の実在性確認については、図 10 に加えて図 12 に示す確認方法が考えられる。また、認定ｅシール用認証業務における申請意思の確認方法は、図 11 に加えて、図 13 に示す確認方法が考えられる。

| 組織等の分類 | 組織等の実在性の確認 | | |
|---|---|---|---|
| | 法的実在性確認 | 物理的実在性確認 | 運営確認 |
| ・法人<br>・権利能力なき社団・財団<br>・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 12 保証レベル1のｅシール用認証業務における組織等の実在性確認方法のイメージ**

| 組織等の分類 | 組織等（代表者）の意思の確認 | 組織の代表者の在籍の確認 |
|---|---|---|
| ・法人<br>・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<br><br>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】<br>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（★）<br><br>【丁： 意思の確認が②、又は丙で確認できない場合】<br>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 13 保証レベル1の認定ｅシール用認証業務における申請意思確認方法のイメージ**

なお、ｅ シール生成者における事業所・営業所・支店・部門単位や、組織の担当者（意思表示を伴わない個人）については、それらが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それら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。

## 2．3　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、保証レベル2の認定 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、発行対象となる組織等（すなわち e シール生成者）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（認証局）、その他属性情報（営業所、事業所、機器等）等とし、図 14 に記載の一例を示す。

また、e シール用電子証明書にあっては、「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記載事項を設けることとする。EU においては、トラストサービスの種別ごとに OID（Object IDentifier）を規定し、電子証明書の記載事項の一つである証明書ポリシーに記載することで、電子署名とeシール等の電子証明書を区別しているところ、国際相互運用性の観点からも、共通証明書ポリシーとして OID を記載することとする。

| | フィールド名 | 値（サンプル） |
|---|---|---|
| 基本領域 | バージョン | V3 |
| | シリアル番号 | 01ab45678cdfe |
| | 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） |
| | 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、<br>当該組織を識別する情報(organization Identifierに組織識別子を格納) |
| | 公開鍵情報 | RSA (2048bit) 等 |
| 拡張領域 | 鍵使用目的 | digitalSignature, nonrepudiation |
| | 基本制約 | cAフラグ=FALSE |
| | 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 |
| | 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 |
| | 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**

## ２．４　認証局の秘密鍵の管理に係る基準

認証局の秘密鍵は、認証局が発行する電子証明書及び証明書失効リストに署名する際に使用され、ｅ シールを生成する際に使用する秘密鍵とは用途が異なるものである[14]。このため、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[15]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 自体の基準及び管理に係る基準について、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[16]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を準用することとする。ただし、HSM 自体の技術基準は、別に定める基準のとおり、現行化することを前提とする。

## ２．５　ｅシール生成者の秘密鍵の管理に係る基準

ローカル ｅ シール方式における ｅ シール生成者の秘密鍵の管理については、認証局から ｅ シール生成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 ｅ シール生成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、ｅ シール生成者の秘密鍵等を保管する媒体に関する規定や ｅ シール生成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、ｅ シール生成者の秘密鍵の管理は ｅ シール生成者自身に委ねられている。

したがって、認定 ｅ シール用認証業務においても、当面は ｅ シール生成者の秘密鍵等を保管する媒体（以下「ｅ シール生成装置」という。特に、第三者機関による認証を受けた ｅ シール生成装置を「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、ｅ シール生成者の秘密鍵の管理は発行対象である組織等（すなわち ｅ シール生成者）に委

[14] 認証局の秘密鍵が万が一漏洩した場合、悪意を持った第三者が認証局になりすまし、偽造した電子証明書や失効リストが発行されてしまう。
[15] 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。
[16] 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。

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ｅシール生成者に対する説明事項について

ｅシール生成者の秘密鍵の管理は当事者に委ねるものの、当事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ｅシール用電子証明書の発行対象者（すなわちｅシール生成者）に対する説明事項として、秘密鍵の管理に係る事項として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、ｅ シール生成者側での秘密鍵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 ｅ シール生成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。また、認証局が ｅ シール生成者の秘密鍵を生成する場合、認証局からｅシール生成者に秘密鍵を送付後、認証局が秘密鍵を消去することも含めて、秘密鍵の管理方法については、事前に認証局と ｅ シール生成者の間で合意がなされておくべきという点も留意が必要である。ｅシール生成者の秘密鍵の管理の一例を図 15 に示す。

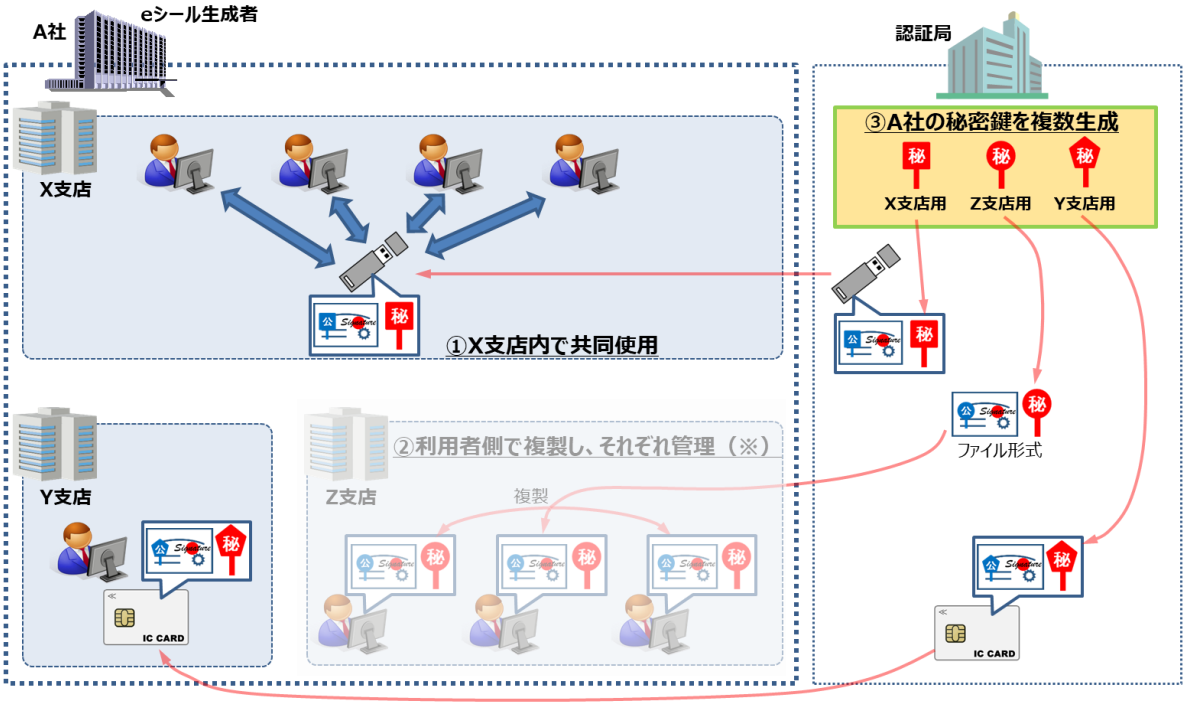



**図 15 ｅシール生成者の秘密鍵の管理の一例**

（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、ｅ シール用認証業務の認定の要件とはしないもの

[17] 保証レベル2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ｅシール生成者の秘密鍵の管理は慎重な取り扱いが求められる。

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良いこととし、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、改めて生成装置の認証の要否について検討が必要となるが、仮に生成装置の認証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 シールを大量に生成する際の処理

e シールにおいては、業務効率化の観点から、ローカル e シール方式/リモート e シール方式にかかわらず、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 シールを付与する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、認定 e シール用認証業務についても、複数の対象電子文書等に一括で e シールを生成することを認める。

ただし、一括で e シールを生成する際には、当然 e シール生成者が指定した電子文書のみに e シールを生成することが求められることから、特にリモート e シール方式においては、e シール生成者が e シールを付与する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リモート 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 シール方式における利用認証[18]

### ２．７．１　リモート e シール方式で e シールを生成する際の利用者認証

ローカル e シール方式においては、一般的に e シール生成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[19]を行い、e シールを生成する形式が想定される。他方、リモート e シール方式では、e シール生成者の秘密鍵を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に管理を委ねているため、保証レベル2のリモート e シールを生成する際の利用認証について検討が必要となる。

---

[18] リモート e シールサービス提供事業者に係る論点については、デジタル庁におけるリモート署名サービス提供事業者に係る論点を含めた議論の動向を踏まえて対応する必要があり、引き続きの検討事項として整理している。

[19] e シール生成者が e シールを発行するために秘密鍵を活性化し、利用できる状態にすること。

ローカル e シール方式における鍵認可を踏まえると、リモート e シール方式においては、まずは e シール生成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できる e シール生成権限者を認証（以下「利用認証」という。）し、その後、鍵認可を行って e シールを生成する必要がある。

すなわち、リモート e シール方式で認定 e シール用認証業務を行う場合は、少なくとも利用認証と鍵認可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[20]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 シール方式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 鍵認可で使用する認証要素の管理

e シール生成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 シール方式において、例えば、リモート e シールサービス提供事業者が鍵認可で使用する PIN コード等の認証要素も管理し、e シール生成者に断りなく e シールを行うことができる可能性がある場合は、e シール生成者が誰であるかの判断ができなくなる可能性がある。特に保証レベル2のリモート e シール方式において、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保証レベル2の e 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。

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、どのような方式を採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、e シールを活用した電子データのトラスト確保の場合には、e シールが付さ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 e シールサービスの利用について事前に協議を受けられない蓋然性が高く、双方の合意があるとはみなせない。

これらを勘案し、認証要素の管理は基本的には e シール生成者が行うこととする。また、e シール生成者が認証要素の管理を行っていない e シールが存在、流通することを防止するため、認定 e シール用認証業務をリモート e シール方式で提供するリモート e シールサービス提供事業者に対しては、一定の基準（例えば事業者による認証要素の管理は不可とする等）が必要である。

---

[20] 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。

## ２．８　ｅシール用電子証明書の失効要求

ｅ シール生成者の秘密鍵が危殆化[21]したり、ｅ シール用電子証明書の発行対象組織等（すなわち ｅ シール生成者）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、ｅ シール生成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。

電子署名の場合は署名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、ｅシール生成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必要であることから、失効要求できる者は、原則として、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。

なお、認証局側から失効を要求できる場合として、電子署名及び認証業務に関する法律施行規則（平成十三年総務省・法務省・経済産業省令第二号）等において、「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[22]」、「利用者署名符号が危殆化したおそれがあるとき[23]」等が定められており、ｅシールについても、これを参考に CP/CPS 等を定めていくことが望ましい。

---

[21] 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鍵認可に用いる 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。

[22] 電子署名及び認証業務に関する法律施行規則 第六条十号にて規定。

[23] 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 第八条三号に規定。「危殆化」については、「盗難、漏洩等により他人によって使用され得る状態になることをいう。」と定義されている。

## 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。

新型コロナウイルスの感染拡大を契機として、テレワークなどを含めて働き方に関する企業や個人の捉え方も多様化する社会状況の中で、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。

このような背景の中、既存の制度である、意思表示を示す電子署名や時刻証明となるタイムスタンプ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高まっている。

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、総務省は令和2年4月～令和3年6月に「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、我が国における e シールの在り方等を示した旧指針を策定した。その後、eシールの更なる普及や活用を促す観点から、令和5年9月から「e シールに係る検討会」を開催して、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との結論を得たことから、当該認定制度の創設に合わせて、旧指針を改定することとした。

本指針が e シール用認証業務を提供する認証局を運営する事業者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期待したい。