資料１－２

eシールに係る検討状況

令和５年９月６日

総務省　サイバーセキュリティ統括官室

eシールに係る検討状況の全体像

- ✓ 組織が発行する電子データの発行元を確認する仕組みである「eシール」については、総務省において開催した「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」を踏まえ、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方向性を示した「eシールに係る指針」を公表。
- ✓ その後、デジタル庁が開催した「トラストを確保したDX推進サブワーキンググループ」で議論がなされ、令和４年７月に取りまとめられた同サブワーキンググループ報告書において、総務省がeシールに係る基準策定及び適合性評価の実現に向けて取り組むこととされた。

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検討会 － 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			デジタル社会の実現に向けた重点計画（別紙）包括的データ戦略 閣議決定 2021.6.18 デジタル社会の実現に向けた重点計画 閣議決定 2021.12.24 eシールに係る指針（総務省） 2021.6.25		デジタル社会の実現に向けた重点計画 閣議決定 2022.6.7	統合 デジタル社会の実現に向けた重点計画 閣議決定 2023.6.9	

「eシールに係る指針」の概要

eシールに係る指針の概要

- 我が国におけるeシールの定義は、「電子文書等の<u>発行元の組織等を示す目的で行われる暗号化等の措置</u>であり、<u>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</u>」とする。
- 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、eシールのレベル分けを行う。
  - レベル1：上記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もの
  - レベル3：レベル2に加えて、十分な水準を充たしたトラストアンカー※1によって信頼性が担保されたもの（組織等の実在性の確認の方法や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、第三者のお墨付きがあるもの）
- eシール用電子証明書の発行対象となる組織等は、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。

※1　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。

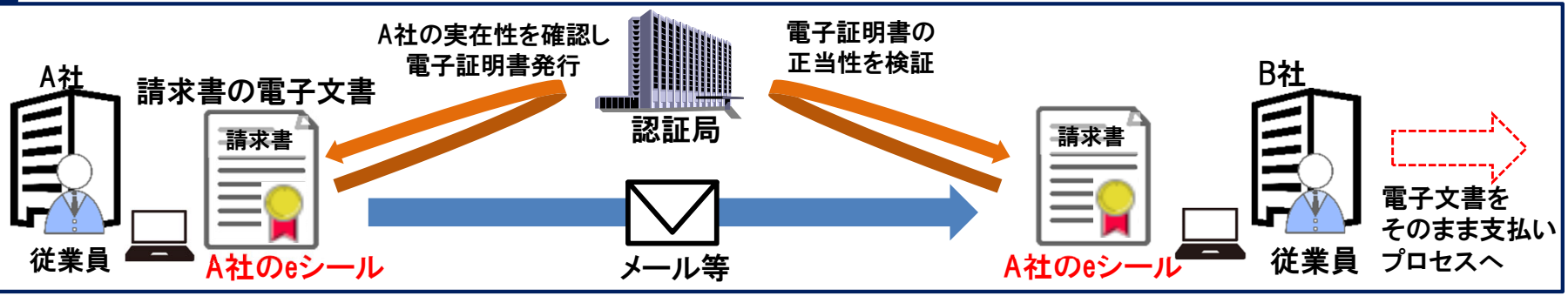
<u>レベル3のeシールの基準となる要件（抜粋）</u>

- ○ eシール用電子証明書の発行の際には、当該組織等の代表者の意思による申請に基づき、当該組織等の実在性を公的な情報（登記情報等）に裏付けられたエビデンスで確認すること。
- ○ eシール用電子証明書のフォーマットは、国際標準としても規定されているITU-T X.509を用いること。
- ○ 認証局の秘密鍵は、一定の厳しい要件を満たしたHSM※2によって厳格に管理されること。
- ○ 利用者の秘密鍵は、利用者自身で管理することとするが、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）を規定すること。

※2　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。

eシールのイメージ

【主なユースケース】
- 契約に紐付いて発生する書類
- 組織等が公開する情報（IR関連資料、広報資料等）
- 組織等が発行する証明書（各種証明書、各種保証書等）



「eシールに係る指針」で方向性が示された事項

✓ 総務省が2021年6月まで開催した「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」（以下「組織発行データ検討会」という。）では、我が国におけるeシールの在り方が検討され、「eシールに係る指針」で方向性を示した。

「eシールに係る指針」で方向性が示された事項

① eシールの分類

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

③ 組織等の実在性・申請意思の確認の方法

④ eシール用電子証明書のフォーマット及び記載事項

⑤ 認証局/利用者の秘密鍵の管理に係る基準

⑥ eシールを大量に行う際の処理

⑦ リモートeシールにおける認証

⑧ 利用者におけるeシール用電子証明書の失効要求

① eシールの分類

指針における方向性

- 我が国におけるeシールは以下のようにレベル分けを行う。

レベル3：レベル2に加えて、十分な水準※1を満たしたトラストアンカー※2によって信頼性が担保されたeシール（発行元証明として機能することに関し、第三者によるお墨付き（将来的には国による認定制度等の要否を検討）があるものを想定）

参考：取りまとめで示された主な用途例：国際取引等における証憑類、法的に保存義務が課されているデータ、排他的独占業務とされている士業の証明書等

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）

参考：取りまとめで示された主な用途例：行政手続における提出書類※3、民民の契約に関連する書類、IR関連資料等の公開情報等

レベル1：裸のeシール（eシールの定義には合致するが、レベル2の要件を満たす保証がないもの）

参考：取りまとめで示された主な用途例：民民における企業間で日常的にやり取りされる電子データ全般、発行元を担保したい情報等

注） eシールのレベ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。

組織発行データ検討会取りまとめ

今後、eシールは発行元証明として様々なユースケースでの使用が期待される。

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

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

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

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

※1 組織等の実在性確認の方法、電子証明書のフォーマット、認証局におけるセキュリティ要件等の一定の水準

※2 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。信頼性の起点となる認証局を想定

※3 用途によっては、レベル3が必要となるケースも考えられる

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- eシールは必ずしも完璧なものである必要はなく、例えば印鑑では印鑑登録しているものに限定していることもあれば、緩いものが使われることもあり、レベル分けされたeシールがあるのはいいこと。
- 用途等にあわせてeシールをレベル分けすることに賛同。
- eシールの法的効果として、「組織から発出されたことが推定できる」といったことを規定できるといいのではないか。

① eシールの分類

【参考】各ユースケースとeシールのレベルとの関係性の一例

	分類① 契約関係	分類② 組織が公開する情報	分類③ 組織が発出する証明書	分類④ 官民間のやりとり	分類⑤ 監査関係	分類⑥ その他
高 発出元証明による信頼性担保の必要性 レベル3	• 領収書 • 請求書 • 【契約書】 • 見積書	• 気象データ • IR関連資料 • 広報資料	• 資格証明書（排他的独占業務とされている士業等）等 • 商工会議所が発行する貿易関係書類 • 健康診断結果証明書	• 法令上保存義務のある書類（国税関係等） • 国への各種申請書類等	• 監査の合格証明書 • 残高証明書	
レベル2	• 納品書 • 受領書	• 【会社法に定める議事録】 • デジタル名刺	• 生産者証明書 • 在学、卒業証明書 • 機器測定データ • 機器の保証書、ライセンス証書	• 請負、委託業務の成果物		
レベル1 低		• 企業間でやりとりされる一般的なデータ	• 加工証明書		• 企業文書	• 情報連携基盤・クラウド環境等でやり取りされるデータ

【 】内は、本来、意思表示を目的とする“電子署名”が馴染むと考えられるユースケース

主に機械的に大量に発行するものにeシールの活用が期待

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

指針における方向性

- eシール用電子証明書の発行対象は、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の組織とする。
- それよりも粒度の細かい、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、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ができることとする。

組織発行データ検討会取りまとめ

eシール用電子証明書の発行対象については、対象とする組織自体の範囲や組織内のより細かい区分を含むかどうか等について検討が必要となる。

対象とする組織自体の範囲については、eシールの普及・利用拡大の観点から、発行対象の実在性を認証局が確認できることを前提に、法人に限定せず幅広い対象を含めることが適当だと考えられる。

他方、発行対象として組織内の事業所等を含むかどうかについては、含めることに対するニーズもあるが、認証局においてその実在性等を確認することが極めて困難である（確認できる内容に限界があり、信頼性にも課題がある）ことや、当該発行対象自体に変更（例えば、事業所統合・廃止や部署名の変更等）が生じた場合、その都度電子証明書の再発行が必要となることが想定され、利便性が著しく低下してしまう可能性があるといった課題があげられる。

なお、EUにおいては、発行対象は法人であり、事業所や営業所といった細かい単位や機器等については、電子証明書の任意のフィールドである拡張領域に記載可能になっている。

これらを踏まえて、eシール用電子証明書の発行対象は、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の組織とし、事業所や営業所といった細かい単位や組織に所属する個人や機器等については、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ができることとすることが適切だと考えられる。

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- eシールは発出元の証明であるということを考慮すると、発行対象は法人（組織）とするのがいいのではないか。
- 発行対象として、事業所等まで含めることが望ましいが、組織の体制とeシールの紐付きが強固になってしまうと、組織の体制の変更等に伴って電子証明書の更新が頻繁に発生し、eシールの利便性の低下に繋がる可能性がある。

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

指針における方向性

- eシール用電子証明書の発行対象を特定するための**識別子については、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。

組織発行データ検討会取りまとめ

eシール用電子証明書には、発行対象の組織等を一意に特定可能な識別子が必要となる。

その識別子については、eシール用電子証明書の発行対象である組織等を一意に特定可能なID・番号体系が我が国で既に存在していれば、そのID・番号体系を活用することが望ましいと考えられるが、我が国では官民どちらにおいても複数のID・番号体系が共存している状態であり、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・番号体系が現状存在していない。

また、そのような識別子（番号体系）をベースレジストリとして整理していくことも考えられるが、その整理には別途多大な時間を要することが想定され、データ戦略タスクフォース等他の検討の場で議論されていることも考慮すると、我が国におけるeシールの在り方を検討する本検討会での議論の対象外だと考えられる。

これらに鑑みて、eシール用電子証明書の発行対象を一意に特定可能な識別子については、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であると考えられる。

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- 今後、インボイスでeシールが活用されることを考慮すると、公的なデータベース（識別子）として適格請求書発行事業者登録番号も検討の余地があるのではないか。

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

【参考】発行対象と既存の番号体系（一例）

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

			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、事務局にて一例として整理）

※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。

③ 組織等の実在性・申請意思の確認の方法

指針における方向性

- 組織等の**実在性の確認については、登記事項証明書や第三者機関データベース等で行い、申請意思については、電子署名、押印、署名等で行うことが必要**。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。
- **レベル3のeシール**の電子証明書の発行にあっては、**組織等の実在性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。

組織発行データ検討会取りまとめ

eシールは発行元証明であることから、架空の組織等のeシールやなりすましのeシールの流通を防止するため、eシール用電子証明書を発行する際には、発行対象の組織等が間違いなく実在していること（実在性）を確認し、かつ、発行申請が間違いなく当該組織に在籍する適切な権限を有した者（法人であれば代表者）によって行われたこと（申請意思）を確認する必要があると考えられる。

実在性の確認については、客観的に判断可能な情報である登記事項証明書や第三者機関が管理するデータベース等による確認が想定され、申請意思の確認については、当該組織等に在籍する適切な権限を有した者による電子署名や押印、署名等による確認が想定される。

ただし、レベル3のeシール用電子証明書の発行にあっては、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ため、実在性の確認は商業登記情報等の公的な機関が管理する情報に裏付けられたものであることを求めることが適切だと考えられる。なお、将来的には、データ戦略タスクフォース等他の検討の場で議論されているベースレジストリを活用して実在性の確認が行われることが望ましいと考えられる。

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- 組織の確認に際しては、確認コストも見据えて優先順位付けが必要。公的な書類やデータベースで確認することは認証局にとって手間のかからない方法になる一方、実地調査はコストが高くなってしまう。
- 第三者機関データベースは、それがしっかり管理・構築されているかを確認しその扱いについてランク付けが必要ではないか。

③ 組織等の実在性・申請意思の確認の方法

指針における方向性

- 組織等よりも細かい粒度である、**事業所・営業所・支店・部門等や担当者、機器の実在性の確認については、組織の代表者の宣言の結果を尊重**することとし、**認証局はその結果に基づいて記載**することが適当。

組織発行データ検討会取りまとめ

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可能な事業所・営業所・支店・部門等や担当者、機器等の実在性の確認について、認証局がそれらの実在性について何らか適切に確認した上で記載することが望ましいものの、確認の方法・程度によっては認証局による確認コストが大きくなり、ひいてはeシールのサービス利用料にも影響が及ぶことが想定され、eシールの普及・利用拡大の観点からも課題があると考えられる。

あくまでもeシール用電子証明書の発行対象は組織等であり、事業所・営業所・支店・部門等や担当者、機器等は、任意の拡張領域に記載されるということを踏まえると、認証局に対して、事業所・営業所・支店・部門等や担当者、機器等の実在性を確認することまで求める必要はないと考えられる。

したがって、事業所・営業所・支店・部門等や担当者、機器等の実在性の確認については、組織の代表者の宣言の結果を尊重することとし、拡張領域への記載事項については発行対象である組織等が一義的な責任を負うことが適当だと考えられる。

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- 組織の確認として、事業等の細かい単位まで網羅的に認証局が確認することは、多大な負担となり、困難ではないか。
- 認証局が組織のどこまで確認するかという問題よりも、その記載した情報に誰が責任を持つかが重要。代表者が宣言していることを認証局が確認するという方法と、認証局においても何らか一定の事業所等の確認をするという方法がある。前者であれば、その事業所等の情報をeシールの証明書に記載することに果たしてどれだけの意味があるのかということについて検討が必要。後者であれば、一定の責任が認証局に出てくるが、それにどれだけ意味が出てくるのかは検討が必要。
- 組織の確認については、認証局側ですべき確認と第三者機関（TDBやTSR等）で行っている確認との切り分けを明確に整理すべきではないか。

③ 組織等の実在性・申請意思の確認の方法

指針における方向性

- eシールに係る電子証明書の発行の手続きの整理の一例は以下の表のとおり。
  - 第三者機関データベースにて組織等の実在性確認を行う場合、レベル3にあっては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であることが求められる。

（★）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

④ eシール用電子証明書のフォーマット及び記載事項

指針における方向性

- レベル2及びレベル3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。
- 電子証明書には、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）等を記載することとする。なお、レベル2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を拡張領域に記載することを可能とする（レベル3の場合は、制度上明確化された認定主体であるため記載は自由）。レベル3、レベル2に関わらず、記載項目は変わらない。

組織発行データ検討会取りまとめ

レベル2及びレベル3のeシール用電子証明書のフォーマットについては、国内の類似制度（電子署名法における認定認証業務の電子証明書、商業登記電子証明書）や国際的な整合性に鑑みて、ITU-T X.509を使用することが適切だと考えられる。

eシール用電子証明書に記載すべき事項としては、発行元を示すための組織等の公式名称、当該組織等を一意に特定可能な識別子をはじめとして、電子証明書の有効期間、公開鍵、署名アルゴリズム等があげられる。

また、レベル2のeシールについては、例えば第三者による評価を受けたeシールが今後登場することも想定されるが、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、当該eシール用電子証明書の検証時に当該eシールが第三者（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）による評価を受けたeシールであることが判別できるように拡張領域に記載することを認めることが信頼性確保の観点からは適切だと考えられる。

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- eシール用電子証明書のフォーマットとして、X.509を採用することには異論なし。
- 発行対象を一意に特定可能な識別子は記載する必要がある。

④ eシール用電子証明書のフォーマット及び記載事項

【参考】eシール用電子証明書（ITU-T X.509）の記載の一例

	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	**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

⑤ 認証局/利用者の秘密鍵の管理に係る基準（認証局側）

指針における方向性

- レベル3のeシールにおける認証局側のHSMの基準は、基本的には電子署名法を準用することとする。
- ただし、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。

注）電子署名法の現行の基準はFIPS140−1 レベル3相当

組織発行データ検討会取りまとめ

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んでしまうため、認証局の秘密鍵はHSM等で厳格に管理されることが必要となる。

eシールにおける認証局の秘密鍵の管理の重要性については、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における認証局の秘密鍵の管理と同等だと考えられるため、認証局の秘密鍵の管理に係る具体的な基準については、電子署名法の認定認証業務で規定している基準を準用することが適切だと考えられる。

ただし、国際的な整合性も踏まえて、電子署名法の基準は現行化すること※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要検討）を求めることが適切だと考えられる。

※ 電子署名法の現行の基準はFIPS140-1 レベル3相当であるが、理想的には現状の脅威に対抗できる要件が必要であり、例えば、現時点においてはFIPS140-2 レベル3相当にアップデートすることが望ましいとのご意見があった。

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- 国内の類似制度や国際的な通用性に鑑みて、ISO/IEC 15408（コモンクライテリア）のEAL4+又はFIPS140−2 レベル3を求めることが適当ではないか。
- 現状の日本の認証局の数を考えると、HSMの基準として日本独自のプロテクションプロファイルを作成するのはコストがかかり過ぎるので、望ましくない。ISO/IEC 15408は国際相互認証されており、プロテクションプロファイルはそのためにあるので、それを適用するのがよいのではないか。
- 電子署名法と同等の基準を設けるということでよいと思う。現状の電子署名法の規定では、特定の認証取得製品に限定しておらず、FIPSでもISO/IEC 15408でも使用できるような記載になっているため、同じような記載でいいのではないか。その上で、実際にどのような製品（FIPS認証製品なのか、ISO/IEC 15408認証製品なのか、その他の認証製品なのか等）を使っていくかは別の議論。
- 電子署名法の基準を準用するということでよいと思うが、電子署名法の現行の基準はFIPS140−1 レベル3相当であるため、まずはFIPS140−2 レベル3相当にアップデートすることが必要ではないか。

⑤ 認証局/利用者の秘密鍵の管理に係る基準（認証局側）

【参考】HSMについて

- HSMとは、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。

～電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針～（抜粋）

注） FIPS140-1 レベル3の基準がベースになっていることに留意

2. 暗号装置関係

(1) 規則第4条第4号に規定する「専用の電子計算機」（以下「暗号装置」という。）とは、発行者署名符号の漏洩、破損、消失等の事象の発生を可能な限り低い確率に抑えるための以下の機能を備えたものをいう。

ア 暗号化されていない状態の暗号符号や認証データ等、保護されていない形式の重要なデータに係る暗号装置への入出力が行われるインタフェースが存在する場合は、そのインタフェースは他のデータの入出力を行うインタフェースとは物理的に独立したものであること。

イ 暗号装置は、以下の機能を有するものであるとともに、暗号装置の操作者ごとに機能ごとの権限の有無が特定されているものであること。

(ｱ) 操作者機能: 暗号化、署名等、通常の暗号化機能を実施するための機能

(ｲ) 管理者機能: 暗号装置自体の初期化、署名符号などの重要パラメータの投入等、暗号装置を管理するための機能

ウ 発行者署名符号等のデータの盗難を回避するため、暗号装置は、以下のいずれかの物理的なセキュリティ対策が講じられていること。

(ｱ) 暗号装置が IC チップ単体からなる場合、IC チップが強固で除去困難な材質の不透明なコーティングで覆われていること。

(ｲ) 暗号装置にカバーが施されている場合、物理的な侵入行為に対し、暗号装置の機能の停止、内部データの無効化等の耐タンパ対策が講じられていること。

(ｳ) 暗号装置の筐体に排気用スリットもしくは空孔が存在する場合、それらは十分小さく、かつ、検出されずに筐体の中をプローブされることを防止する対策が講じられていること。

エ 暗号装置に係る発行者署名符号の管理に関し、以下の措置が講じられていること。

(ｱ) 暗号装置内で発行者署名符号の生成を行う場合、安全な擬似乱数生成アルゴリズムを用いるものであること。

(ｲ) 暗号装置への発行者署名符号の入出力を行う場合には、以下のいずれかの方式であること。

① 発行者署名符号は暗号化された上で入出力されること。

② 発行者署名符号を2つ以上の構成要素に分割して入出力を行う場合は、暗号装置に対して直接行うこととし、発行者署名符号の各構成要素に対する操作者の認証が行われること。また、発行者署名符号の各構成要素は、暗号装置内で分割、結合されること。

(ｳ) 発行者署名符号を暗号化されていない状態で暗号装置内に保管する場合は、外部からアクセスできない仕組みとすること。

(ｴ) 発行者署名符号を廃棄する際には、発行者署名符号その他のセキュリティパラメータを無効化する機能を有すること。

(2) 省略

⑤ 認証局/利用者の秘密鍵の管理に係る基準（認証局側）

指針における方向性

- レベル3のeシールにおける認証局側のHSMの管理に係る基準は、基本的には電子署名法を準用することとする。

組織発行データ検討会取りまとめ

認証局のHSMの管理については、秘密鍵を管理しているというその重要性に鑑みて、HSMが配置される部屋への入出場に係る基準、HSMに対する不正アクセス防止に係る基準、災害対策に係る基準等が一般的に求められると考えられる。

eシールにおける認証局のHSMの管理の考え方については、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における認証局のHSMの管理の考え方と同等だと考えられるため、認証局のHSMの管理に係る具体的な基準については、電子署名法の認定認証業務で規定している基準を準用することが適切だと考えられる。

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- 電子署名法の認定認証業務で要求している基準と同等の基準を求めることが適切ではないか。

⑤ 認証局/利用者の秘密鍵の管理に係る基準（認証局側）

【参考】電子署名法の認定認証業務におけるHSMの管理に係る規定

～電子署名及び認証業務に関する法律施行規則第４条第１項（抜粋）～

（認証設備室への入出場の管理に関する規定）

１　申請に係る業務の用に供する設備のうち電子証明書（利用者が電子署名を行ったものであることを確認するために用いられる事項（以下「利用者署名検証符号」という。）が当該利用者に係るものであることを証明するために作成する電磁的記録をいう。以下同じ。）の作成又は管理に用いる電子計算機その他の設備（以下「認証業務用設備」という。）は、入出場を管理するために業務の重要度に応じて必要な措置が講じられている場所に設置されていること。

（認証業務用設備へのアクセス等の管理に関する規定）

２　認証業務用設備は、電気通信回線を通じた不正なアクセス等を防止するために必要な措置が講じられていること。

（認証業務用設備の作動権限等の管理に関する規定）

３　認証業務用設備は、正当な権限を有しない者によって作動させられることを防止するための措置が講じられ、かつ、当該認証業務用設備の動作を記録する機能を有していること。

４　HSM自体の基準のため省略

（災害対策に関する規定）

５　認証業務用設備及び第一号の措置を講じるために必要な装置は、停電、地震、火災及び水害その他の災害の被害を容易に受けないように業務の重要度に応じて必要な措置が講じられていること。

注）　これらの規定は、HSMに限らず、認証業務用設備全般についての規定であることに留意

⑤ 認証局/利用者の秘密鍵の管理に係る基準（利用者側）

指針における方向性

- 利用者の秘密鍵の管理は発行対象である組織等の管理に委ねることとする。
- ただし、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（複製は望ましくない等））を規定することが適切。

組織発行データ検討会取りまとめ

利用者の秘密鍵の管理次第では、当該秘密鍵が漏えいして悪用される懸念があることから、秘密鍵の管理は厳格に行われる必要がある。他方、仮にeシールに係る認定制度ができた場合でも、利用者側が所持している秘密鍵（生成装置に格納している場合は生成装置）の具体的な管理の在り方に関して、フレームワーク上で何らか利用者側に義務を課すことは困難であることが想定される。

電子署名法の認定認証業務においては、利用者の秘密鍵の管理に係る直接的な規定はないが、認証局に対する要求事項として、秘密鍵は十分注意を持って管理する必要がある旨を利用者に説明することが規定されており、秘密鍵の管理は利用者に委ねられている。

EUの適格eシールにおいても、秘密鍵（適格eシール生成装置）の管理は法人の管理下にあることが規定されているのみ（ただし、適格eシール生成装置を用いるため、秘密鍵の複製は不可）となっている。

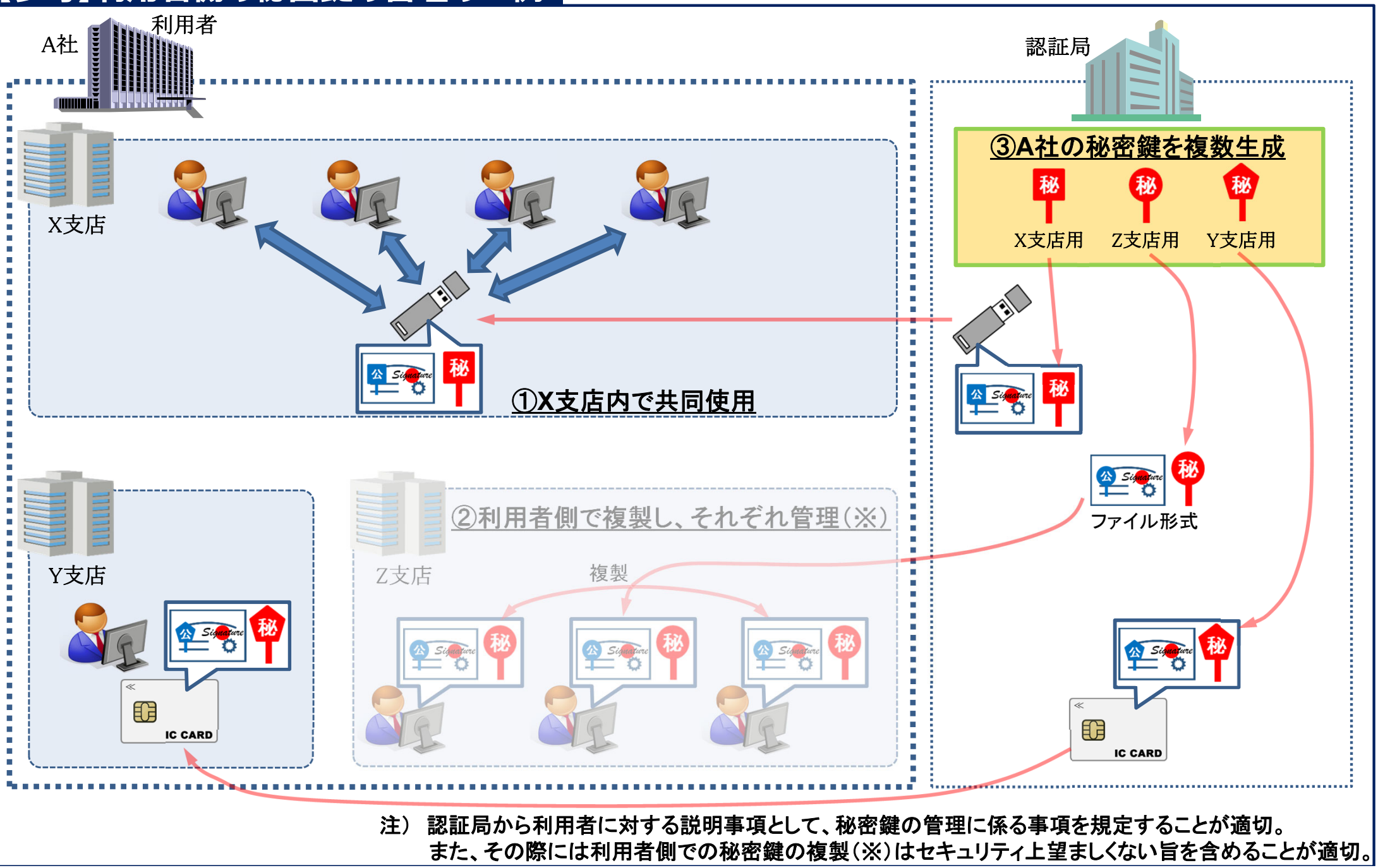
これらに鑑みて、利用者の秘密鍵の管理は発行対象である組織等に委ねることが適切だと考えられる。ただし、認証局から利用者に対する説明事項として、秘密鍵の管理は厳格に行うこと（複製は望ましくない等）を規定することが適当だと考えられる。なお、秘密鍵の管理が利用者に委ねられ、利用者側での複製が望ましくないことを考慮すると、当然、認証局側での利用者の秘密鍵の複製も望ましくない。

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- EUでは法人の管理下にあることが求められており、電子署名法でも実質的には同じルールになっているため、特段の要件は不要ではないか。
- QSCDを求めない以上、ファイル形式で利用者に秘密鍵を渡すことも可能であるため、ユーザー側でも複製ができてしまうことになると思うが、特にレベル3のeシールにあっては、利用者の秘密鍵を利用者側で複製できるのは望ましくないのではないか。
- 利用者の秘密鍵の管理については、少なくとも認証局から利用者への重要事項説明として規定するべきではないか。
- 有事の際のバックアップを考えると、利用者側での秘密鍵自体の複製ができないと困るのではないか。
- 利用者の秘密鍵の複製については、同一の組織に複数のeシール用電子証明書（及び秘密鍵）を発行することで対応可能。

⑤ 認証局/利用者の秘密鍵の管理に係る基準（利用者側）

【参考】利用者側の秘密鍵の管理の一例



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が適切。
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が適切。

⑤ 認証局/利用者の秘密鍵の管理に係る基準（利用者側）

【参考】電子署名法の認定認証業務における認証局から利用者への説明事項に係る規定

～電子署名及び認証業務に関する法律施行規則～（抜粋）

第六条　法第六条第一項第三号の主務省令で定める基準は、次のとおりとする。

一　利用申込者に対し、書類の交付その他の適切な方法により、電子署名の実施の方法及び認証業務の利用に関する重要な事項について説明を行うこと。

～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～（抜粋）

第八条　規則第六条第一号に規定する利用申込者に対して説明を行うべき事項とは、次の各号に掲げる事項を内容として含むものとする。

一　認定認証業務においては、虚偽の利用の申込みをして、利用者について不実の証明をさせた者は、法第四十一条の規定により罰せられること。

二　電子署名は自署や押印に相当する法的効果が認められ得るものであるため、**利用者署名符号については、十分な注意をもって管理する必要があること。**

三　利用者署名符号が危殆化（盗難、漏えい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。以下同じ。）し、又は危殆化したおそれがある場合、電子証明書に記録されている事項に変更が生じた場合又は電子証明書の利用を中止する場合においては、遅滞なく電子証明書の失効の請求を行わなければならないこと。

四　認定認証業務に係る電子証明書を使用する場合における電子署名のためのアルゴリズムは、認証事業者が指定したものを使用する必要があること。

⑤ 認証局/利用者の秘密鍵の管理に係る基準（利用者側）

指針における方向性

- 当面は、一定の基準を満たしたeシール生成装置を用いることを認定の要件とはしないことが適当。ただし、第三者機関による認証を受けたeシール生成装置（以下、「認証eシール生成装置」という。）を用いてもよい。
- また、認証eシール生成装置を使用していないにも関わらず、認証eシール生成装置を使用していると誤認させる表示は禁じる。一方、国際的な整合性の観点から、認証eシール生成装置を用いている場合、当該eシールが認証eシール生成装置を用いて行われていることを検証者が判断可能な仕組みとすることが適切。

組織発行データ検討会取りまとめ

利用者の秘密鍵が悪意のある第三者に盗まれた場合、利用者の意図しないところでeシールが悪用されることが想定され、EUの適格eシールにおいては、利用者の秘密鍵を耐タンパー性を備えた適格eシール生成装置（QSCD）に格納して利用することを求めている。

他方、利用者の秘密鍵は認証局の秘密鍵とは異なり、盗まれて悪用された際の影響はeシール用電子証明書の発行を受けた組織等に限定され、認証局から利用者への秘密鍵の受け渡しを安全かつ確実に行えば、その先は利用者側の管理の問題という考え方もできる。

なお、意思表示のために使用され、推定規定が法定されている電子署名であっても、署名生成装置に関する規定が設けられていない。

これらを踏まえて、当面はeシールにおいても、一定の基準を満たしたeシール生成装置を用いることを認定の要件とはしないことが適当だと考えられる。

ただし、国際的な整合性の観点から、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適切だと考えられる。

なお、電子署名法含め、将来的に利用者側の生成装置に関して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。ただし、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。

⑤ 認証局/利用者の秘密鍵の管理に係る基準（利用者側）

～前ページからの続き～

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- 日本でも少なくともQSCD相当のものを使用して耐タンパ性能が確保されたところで秘密鍵が管理されるよう規程の整備が必要ではないか。Society5.0やDFFTを実現していく上で、データを自動で検証して処理し、更にそのデータが自動処理されていくということを想定していくと、検証時に秘密鍵が適切な環境で保護されているかどうかを確認できる必要がある。レベル3のeシールでQSCDを求めるかどうかは別の議論になるが、EUのQCステートメントのように、少なくとも検証時において、QSCDを使用していることがわかるような制度にした方がいい。
- 電子署名法とのバランスが重要である一方、EUとの相互運用の関係もあるので非常に難しい問題。商業登記や法的効力のある電子署名法でも署名生成装置は規定されておらず、また、実世界でも実印の管理については規定がないため、QSCDの規定は設けないという考え方が1つある。電子署名には推定効というものがあるが、eシールがそれ以上の効力を持つことは考えられないのでeシールにのみQSCDを求めるというのは全体のバランスを欠くのではないか。
- QSCDの規定を設ける場合、QSCDの使用/未使用によってeシールの効力にどれだけ違いが出るのかについては、レベル2、3問わずeシールには現段階では法的効力がないことを考えると、EUの適格として通用するかどうかではないか。
- 選択肢としては、電子署名法でもeシールでも両方QSCDを求めるか、あるいは両方求めないか、という2択になるのではないか。両方求める場合は、現状規定のない電子署名法は規制強化になってしまうことが懸念される。他方、両方求めない場合はEUと相互運用を目指す際に課題となる。従来の我が国の法制度の中での秘密鍵等の管理は本人に任されていて本人の責任であるという考え方を維持するのであれば、QSCDは必須にしないが、秘密鍵等の管理の方法として、QSCDを使用する方法もあるということやEUとやりとりする際のオプションとして使用することをガイドライン等に記載するのはどうか。
- eシールの普及という観点では、国内での申告や申請等に利用するということでレベル2の世界で考え、レベル3については欧州等の諸外国との相互運用に値する他国に恥じない基準にすることが適切ではないか。
- EU等の諸外国との相互運用の観点も重要であるが、QSCDの規定を設ける場合は実際の企業側の運用と基準がどうフィットするのかについても検討が必要ではないか。

⑥ eシールを大量に行う際の処理

指針における方向性

- レベル3のeシールにおいて、複数の対象データに一括でeシールを行うことを認めることが適当。

eシールにおいては、業務効率化の観点から、ローカル/リモート方式に限らず機械的に複数の対象データ（例えば領収書等）に対して一括でeシールを行うことに対するニーズがある。

一括処理について、我が国における実空間での手続では、複数の対象文書（例えば委嘱状等）に対して、まとめて処理（決裁・押印）することは一般的に実施されている。

また、EUの適格eシールにおいては、ローカルeシールについては特段の規定がないが、リモートeシールについてはCENの技術基準において、複数の対象データに一括で署名（eシール）指示することが認められている。

eシールの普及・利用促進の観点や国内における実運用、EUの制度を踏まえ、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ということに鑑みて、レベル3のeシールであっても、複数の対象データに一括でeシール行うことを認めることが適当だと考えられる。

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データのみにeシールが行われることが求められることから、利用者が対象データに対してeシールを行う指示を行って以降、他のデータが紛れ込むことがないことはeシールサービス側で担保する必要がある。

⑦ リモートeシールにおける認証

指針における方向性

- 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）であることを認証するための認証）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）を別に求めることが適切。
- ただし、上記の鍵認可の場面で複数要素認証（例えば、所持認証＋知識認証）までは要求しない。

注） レベル2のリモートeシールは、利用認証と鍵認可を別々に行わなくてもよい。

組織発行データ検討会取りまとめ

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を行い、eシールを行う形式が想定される。

ローカルeシールにおける認証を踏まえると、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と考えられる。

なお、リモート署名ガイドライン※のレベル2（電子署名法における認定認証業務と同等の信頼性を想定）においては、サービス提供を受けるための利用認証と秘密鍵（署名鍵）を利用するための鍵認可を分けて行い、かつ鍵認可は複数要素認証を行うことを要求している。

また、EUの適格eシール（リモート方式）においては、リモート署名ガイドラインのレベル2の要件に加えて、鍵認可はISO/IEC 15408（コモンクライテリア）の認証（プロテクションプロファイル： EN 419 221-5）を取得した署名活性化モジュールにて行うことを要求している。

他方、電子署名は意思表示であり、我が国でもEUでも推定規定があるのに対し、eシールは発行元証明にとどまり、我が国では現状は推定規定もないことに鑑みて、レベル3のリモートeシールを行う際には、利用認証と鍵認可（単要素認証でも可）を別に求めることで十分だと考えられる。

※ 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

【参考組織発行データ検討会の議論であがった主な意見（抜粋）

- レベル3のリモートeシールにおいて、組織によっては鍵認可の際は複数要素認証であったとしても単純な認証だけでは認められないことも考えられ、よりレベルの高いもの（例えばVPNを使ったシステム間連携等）を要求する可能性もある。

⑦ リモートeシールにおける認証

指針における方向性

- **認証要素の管理は基本的には利用者が行う**こととし、eシールとしての用をなさないレベル3のeシールの生成、流通を防止するため、**レベル3のe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（認証要素は利用者本人が管理すること等）を設ける**ことが適切。

組織発行データ検討会取りまとめ

リモートeシールにおいて、仮に利用者の秘密鍵を管理しているリモートeシールサービス提供事業者が認証要素も管理して、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、そもそも認証要素としての意義が失われ、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想定され、基本的には認証要素は利用者のみが管理することが望ましいと考えられる。

加えて、eシールの場合には、eシールが行われたデータを受け取る者（例えば領収書の受領者）には、リモートe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（電子署名の場合には、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）。

このため、仮にレベル3のリモートeシールにおいて、eシールを行う際の鍵認可で使用する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eシールが存在・流通してしまうことが想定され、制度の安定性そのものに影響を与えかねないと考えられる。

なお、EUにおいては、認証要素の管理は法人に委ねられ、アプリケーション提供事業者が管理することも否定はされていない一方、リモート署名ガイドラインにおいては、利用者本人のみが秘密鍵（署名鍵）を活性化（鍵認可）できることを要求している。

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し、eシールとしての用をなさないレベル3のeシールの生成、流通を防止するため、レベル3のeシールをリモートで行うする事業者（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）が必要になると考えられる。なお、当然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望ましくない。

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- リモートeシールサービス提供事業者に関しては、一定の基準が必要ではないか。

⑧ 利用者におけるeシール用電子証明書の失効要求

指針における方向性

- 失効要求できる者は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）に限定することが適切。

組織発行データ検討会取りまとめ

電子証明書と自然人の紐付けが1対1である電子署名とは異なり、eシールは1つのeシール用電子証明書を組織等の中の複数人が使用することが想定されるため、当該eシール用電子証明書の失効を要求できる者の範囲をどこまでとするかについて検討が必要となる。

その範囲については、①eシール用電子証明書の発行を求めることができる者に限定するか、②それに加えて当該eシールを行う権限を有する者でも可とするか、③当該eシール用電子証明書の発行を受けた組織等に属する者であれば誰でも可とするか、が主な選択肢としてあげられるが、失効要求は、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と考えられることから、失効要求できる者は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）に限定することが適切だと考えられる。

【参考】組織発行データ検討会の議論であがった主な意見（抜粋）

- 失効要求ができる者は、基本的には代表者もしくは委任を受けた者といった制限をかけるのがよいのではないか。