

# 事務局説明資料

---

令和6年1月17日

総務省 サイバーセキュリティ統括官室

# (報告)「中間取りまとめ(案)」パブリックコメントへの対応結果

- 「**eシールに係る検討会 中間取りまとめ(案)**」について、令和5年12月13日から令和6年1月10日にかけて、パブリックコメントを実施済み。意見提出者は以下のとおり。
- なお、前回会合で議論したとおり、パブリックコメントを踏まえた同案への修正等については座長一任となっており、**近日中に「中間取りまとめ」の最終版を公表予定**。

## ○意見提出数：15件

受付順	意見提出者	受付順	意見提出者
1	株式会社帝国データバンク	7	日本電気株式会社
2	TK業務企画	8	ヒット株式会社
3	一般財団法人日本データ通信協会	9	一般財団法人日本情報経済社会推進協会
4	一般社団法人デジタルトラスト協議会	10	一般社団法人クラウド型電子署名サービス協議会
5	セコムトラストシステムズ株式会社	11	公益社団法人日本文書情報マネジメント協会
6	サイバートラスト株式会社	—	個人（4件）

## ○パブリックコメントにおいて提出意見数が多かった項目

### 【3.2 eシールに係る適合性評価の実現】

- 「総務大臣によるeシールに係る認定制度の創設を念頭に、国による適合性評価の枠組みを議論する」との方向に対して賛同の意見が多く寄せられた。認定制度の創設に当たっては、WebTrust等の**類似の民間制度の活用の検討**を求める意見も頂いた。

### 【4.2 eシールの定義】

- 「eシール」を「データ」として捉えることに賛同の意見が多く、また、「eシール」という名称を維持すべきとの意見が多かった。

### 【4.4 eシール用電子証明書の発行対象となる組織等の範囲】

- 「法人番号」を組織識別子として使用する方針に賛同のご意見を頂いたが、今後の検討課題として、**「個人事業主」の扱いについて引き続き検討を求める**意見を頂いた。

### 【4.5 共通証明書ポリシーOID体系】

- 共通証明書ポリシーOID体系の整備に賛同のご意見を頂いた。

⇒ 各提出意見への対応方針は【参考資料5 - 1】のとおり

## ○パブリックコメントを受けて中間とりまとめの修正について

- 「1. 2 eシールとは (参考2) eシールと電子署名の異同」の記述について、これまでの議論の経緯や関係性を明確化するため、「eシールに係る指針」から抜粋した内容であることを明記。
- 電子署名法が定義する「認証業務」と混同されないように、「認証業務」を「eシール認証業務」に修正。

## 今後の議論の想定スケジュール

### 第5回会合（本会合）：令和6年1月17日

- ・ 「中間取りまとめ(案)」パブリックコメントへの対応結果の報告
- ・ これまで議論できていない又は議論が済んでいない論点の整理
- ・ eシールの活用が見込まれる事例に関する分析(3)

### 第6回会合：令和6年2月5日（予定）

- ・ 「eシールに係る指針」改定の骨子案
- ・ 「最終取りまとめ」骨子案
- ・ 国際間で流通するデータにおけるeシール活用の現状（境野構成員）
- ・ その他積み残しの論点

### 第7回会合：令和6年3月上旬（予定）

- ・ 「eシールに係る指針」改定案
- ・ 「最終取りまとめ(案)」等

※) 認定制度に係る告示については総務省にて作成の上、第7回で参考として提示予定。

## 参考) 「認定制度に係る告示」と「eシールに係る指針」の関係

- ・ 本検討会の最終取りまとめに合わせ、「**認定制度に係る告示**」を策定するとともに、「**eシールに係る指針**」を改定する予定。前者は認定制度に係る内容を規定するのに対し、**後者は、認定に係るもの以外も含めてeシールを広く対象とした基準を示すもの**である。

- 本検討会において、「**eシールに係る指針**」での整理を踏まえて議論を行っており、各論点の整理状況は以下のとおり。これらの論点に加え、今後、**認定制度の在り方に関する論点**についても議論する必要がある。

「eシールに係る指針」で示されている内容	本検討会においてこれまで議論した内容	整理状況
① eシールとは	・ eシールという用語を「措置」/「データ」のいずれと捉えるか	整理済み
	・ 「eシール」という用語に和名での正式名称を設けるか	引き続き議論
	・ eシールの定義に盛り込むべき要素	整理済み
② eシールの分類	eシールの保証レベル	整理済み
③ eシール用電子証明書の発行対象となる組織等の範囲	・ 組織等を一意に特定するための識別子（組織識別子）について	引き続き議論
	・ 「個人事業主」の扱いについて	整理済み
	・ 法人等における「事業所や営業所等」の扱いについて	引き続き議論
④ 組織等の実在性・申請意思の確認の方法		今後議論
⑤ eシール用電子証明書のフォーマット及び記載事項	共通証明書ポリシーOID体系	整理済み
⑥ 認証局/利用者の秘密鍵の管理に係る基準		今後議論
⑦ eシールを大量に行う際の処理		今後議論
⑧ リモートeシールにおける認証	リモートeシールの位置付け	整理済み
⑨ 利用者におけるeシール用電子証明書の失効要求		今後議論

⇒ 次ページに、「これまで議論できていない又は議論が済んでいない論点」の一覧を整理。

- スライド4で提示した整理状況を踏まえ、今後議論が必要な論点は以下のとおり。

## 【eシールに係る主要な論点】

- **論点① eシールの名称**
  - 「eシール」という用語に和名での正式名称を設けるか。
- **論点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に使用する組織識別子の範囲をどうするか。
  - 法人等における「事業所や営業所等」等の扱いをどうするか。
- **論点③ 組織等の実在性・申請意思の確認の方法**
  - 組織等の実在性や申請意思の確認をどのように実施するか。
- **論点④ 認証局/利用者の秘密鍵の管理**
  - 認証局における秘密鍵の管理基準をどうするか。
  - 利用者における秘密鍵の管理基準をどうするか。
- **論点⑤ eシールを大量に行う際の処理**
  - 複数の対象データに一括でeシールを付すことを可能とするか。
- **論点⑥ 利用者におけるeシール用電子証明書の失効要求**
  - eシール用電子証明書の失効要求ができる者の範囲はどこまでとするか。
- **論点⑦ 認定制度の在り方**
  - 認定制度をどのように設計するか。

## 論点

- 「eシール」という用語が既に一定程度定着しつつあることを踏まえると、正式名称としては「eシール」という用語を残すことが適切と考えられるが、それとは別に和名での名称は必要か。

## 方向性案

- 本検討会での議論内容やパブリックコメントで提出された意見を踏まえると、**「eシール」という名称を正式名称とする**ことが適切との意見が大半であり、そのとおり整理することとしたい。**(←本日結論を出したい事項)**
- なお、参考として、これまでの議論等で挙げた和名候補を下図に掲載する。

No.	和名候補	読み方	備考
1	組織保証	ほしきほしょう	eシールの定義を「データ」とすることを踏まえると適していない。
2	電子押印	でんしおういん	
3	電子刻印	でんしこくいん	
4	電子社印	でんししゃいん	
5	電子組織標示	でんしそしきひょうじ	
6	電子表章	でんしひょうしょう	
7	電子標章	でんしひょうしょう	
8	電子標付	でんししるしつけ	eシールの定義を「データ」とすることを踏まえると適していない。
9	電子封印	でんしふういん	eシールの定義を「データ」とすることを踏まえると適していない。
10	電子紋章	でんしもんしょう	
11	電子データ発行元証明	でんしでーたはっこうもとしょうめい	eシールの定義を「データ」とすることを踏まえると適していない。

## 論点

- eシール用電子証明書に使用する組織識別子として、これまでの議論においては、法人番号、TDB企業コード、標準企業コード、TSR企業コード、LEIが挙げられたが、これ以外に対象とすべき組織識別子はあるか。
- 「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任意のフィールドである拡張領域に記載できる」とした「eシールに係る指針」の整理を維持するか。

## 方向性案

- “認定対象”の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下図のとおり整理することとし、「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」の扱いについては「eシールに係る指針」の整理を維持することとしたい。 (← **本日結論を出したい事項**)
- 【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

“認定対象”のeシール用電子証明書	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	<b>NTRJP※2</b>	<b>TD:JP</b>	<b>JI:JP</b>	<b>TS:JP</b>	<b>LEIXG※3※4</b>
組織識別子	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。

～前ページからの続き～

## 方向性案

- “認定対象外”のeシール用電子証明書については、下図のいずれかの組織識別子の使用を推奨することを「eシールに係る指針」の改正版に記載することとし、「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」の扱いについては「eシールに係る指針」の整理を維持することとしたい。**（←本日結論を出したい事項）**

【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

“認定対象外”のeシール用電子証明書	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	<b>NTRJP※2</b>	<b>TD:JP</b>	<b>JI:JP</b>	<b>TS:JP</b>	<b>LEIXG※3※4</b>
組織識別子	NTRJP-1234567890123	TD:JP-123456789	JI:JP-123456	TS:JP-123456789	LEIXG-12345678901234567890
<b>【参考】</b>					
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。

## 論点

- 組織等の実在性・申請意思について、認証局においてどのように確認するか。

## 方向性案

(★) はデジタルで行える手続 ※ 1 : 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 ※ 2 : 個人事業主に限る

- “認定対象”のeシール認証業務については、「eシールに係る指針」も踏まえ、下図のとおり整理することとしたい。 (←本日又は次回で結論を出したい事項) 「eシールに係る指針」からの主な変更点は下線箇所

組織等の分類	組織等の実在性の確認	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 ・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 (★)		
	登記事項証明書 又は 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。） (★)	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  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（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
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。		

- “認定対象外”のeシール認証業務については、上記確認方法に加えて下図に示す確認方法を推奨例として「eシールに係る指針」の改訂版に記載することとしたい。 (←本日又は次回で結論を出したい事項)

組織等の分類	組織等の実在性の確認	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 ・権利能力なき 社団・財団 ・その他任意の 団体	第三者機関が管理するデータベース※ <sup>1</sup> (★)	代表者（又は申請者※ <sup>2</sup> ）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	【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※ <sup>1</sup> に登録されている代表者（又は申請者※ <sup>2</sup> ）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※ <sup>2</sup> ）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※ <sup>1</sup> 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※ <sup>2</sup> ）本人に対する当該申請の有無の確認
個人事業主	各種身分証明書	申込書への代表者（又は申請者※ <sup>2</sup> ）の署名又は押印…②	
事業所・営業所・支店・部門等、担当者、機器	組織等の代表者（又は申請者※ <sup>2</sup> ）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。		

## 論点

- 認証局における秘密鍵の管理に係る基準を設けるか。
- eシールに係る指針にはHSM（Hardware Security Module）の技術基準を記載しているが、この場合、技術的進歩に応じて当該指針の改定が必要となるため、設備・技術・運用基準を規定する実施要項等にも記載するか。

## 方向性案

- 「eシールに係る指針」に基づき、総務大臣認定を受ける認証業務を提供する認証局におけるHSMの基準については、基本的に**電子署名法を準用**することとする。（←本日又は次回で結論を出したい事項）
- HSMの技術基準として満たすべき連邦情報処理標準（FIPS）の規格名等は、技術の進歩によって将来的に変化していくため、それらを実施要項等に記載し、eシールに係る指針において最新の規格を参照するよう規定する。（←本日又は次回で結論を出したい事項）

### 「eシールに係る指針」より抜粋

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（FIPS140-1 レベル3相当）を準用**することとする。

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。

## 論点

- 利用者における秘密鍵の管理に係る基準を設けるか。

## 方向性案

- 「eシールに係る指針」に基づき、総務大臣認定に係るeシールについても、**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。（←本日又は次回で結論を出したい事項）
- また、認証局とは異なる事業者がリモートeシール生成サービスを提供する場合、リモートeシール生成サービス事業者が利用者の秘密鍵を管理することとなるが、管理方法等についてはデジタル庁におけるリモート署名に係る議論を今後も引き続き注視していく。

### 「eシールに係る指針」より抜粋

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 e 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 I Cカードや U S B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。**

#### （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。

#### （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。

## 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。

## 方向性案

- 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」の方向性に基づき、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シールを行うことを認める**こととする。（←本日結論を出したい事項）

### 「eシールに係る指針」より抜粋

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で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。

## 論点

- 利用者において、eシール用電子証明書の失効要求ができる者の範囲はどこまでとすることが適切か。
- 利用者からの失効要求だけでなく、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。

## 方向性案

- 失効要求はeシール用電子証明書の発行申請と同様の意思表示が伴うことから、「eシールに係る指針」に基づき、**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。**（←本日結論を出したい事項）
- 認証局側からeシール用電子証明書を失効する可能性がある場合は、**認証業務運用規程**（CPS; Certification Practices Statement）**に失効に係る条項を規定することとする**※<sup>1</sup>。（←本日結論を出したい事項）

### 「eシールに係る指針」より抜粋

利用者の秘密鍵が危殆化したり、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。**

※1：eシールが付された「失効届出」が利用法人から提出された際に、当該届出に基づき認証局で失効すること等が考えられる。また、利用法人の利用規約違反や料金未納、破産などの事由に基づき認証局で失効すること等も想定される。

- タイムスタンプにおける総務大臣認定制度の例も参考に、**告示によって制度の大枠を規定し、細則については実施要項等で定める**こととしたい。（なお、本検討会では告示に規定する内容について議論し、実施要項の作成については、来年度に別途有識者を集めて議論することとする。）
- 告示に規定すべき内容として議論が必要な論点は以下と考えられるが、以下について意見を伺うとともに、これ以外にも考慮すべき論点があれば議論いただきたい。（←本日又は次回で結論を出したい事項）

## 論点と方向性案

### 認定の対象

- 認定の対象は、eシール用電子証明書を発行する**「認証業務」に対して認定を与える**こととしたい。

### 認定の基準等

- 実施要項等で別に定める**設備・技術・運用の基準**に合致しているかを審査する。その際、技術基準については、当面の間は、**公開鍵暗号方式（PKI）によるものだけを認定を受けたeシール用認証業務の対象**とする。
- タイムスタンプの例に倣うと、**認定の有効期間は2年**として、2年ごとに更新を受けなければ効力を失うこととする。
- 認定時の要件に該当しなくなった場合には、**認定の取消しも可能となるよう規定を整備**する。

### 指定調査機関

- 設備・技術・運用基準への適合性評価は総務大臣が指定する**「指定調査機関」に全部又は一部を行わせることができる**ものとする。
- 「指定調査機関の指定」に係る一連の手続は、タイムスタンプにおける認定制度を参考に設計することとする。

### 実施状況の報告

- 認定を受けた事業者が、認定に係る事業の運用の適正性について、自己監査又は第三者による監査を受けることが求められるが、タイムスタンプの認定制度に倣い、頻度は**年1回**とするか。