資料６－１

事務局説明資料

令和６年２月５日

総務省　サイバーセキュリティ統括官室

「eシールに係る指針」を踏まえた論点の整理状況

- 本検討会において、「eシールに係る指針」で示されている論点に加え、認定制度の在り方に係る論点についても議論。前回会合までの議論を踏まえた、各論点の整理状況は以下のとおり。
- なお、認定制度の実施要項等で決めるべき細則については、来年度に議論する予定。

本検討会における論点	整理状況
① **eシールの定義等**：eシールの名称、定義等	整理済み
② **eシールの保証レベル**：eシールの保証レベル等	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**：組織識別子、個人事業主の扱い等	整理済み
④ **eシール生成者の実在性・申請意思の確認の方法**	**引き続き議論**
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体系等	整理済み
⑥ **認証局の秘密鍵の管理に係る基準**	**引き続き議論**
⑦ **eシール生成者の秘密鍵の管理に係る基準**	**引き続き議論**
⑧ **eシールを大量に生成する際の処理**：複数の対象データへのeシールの付与	整理済み
⑨ **リモートeシール方式における利用認証**：リモートeシールの位置付け等	整理済み
⑩ **eシール用電子証明書の失効要求**：認証局側から失効する場合の規定等	**引き続き議論**
⑪ **認定制度の在り方**：認定の対象、有効期間等	**引き続き議論**

論点④　eシール生成者の実在性・申請意思の確認の方法

論点

- eシール生成者の実在性・申請意思について、認証局はどのように確認するか。

第５回検討会の議論で挙がった主な意見（抜粋）

- eシール用電子証明書は用途として発行元証明であり、認証局が組織を確認して証明書を発行する観点から、類似の証明書としてサーバ証明書、特に法人の存在を確認して発行されるEV（Extended Validation）証明書が挙げられる。当該証明書における組織の実在性確認は、CA/Browserフォーラムのガイドラインに従い、日本を含む全世界で実施されている。①法的な存在確認、②物理的な存在確認、③運営的な存在確認の3点がある。（中略）組織の実在性確認方法として少なくとも、これら3種類が含まれると理解しており、引き続き検討が必要な項目ではないか。

第５回検討会での議論を踏まえた事務局の見解

- 認定に係るeシール認証業務において、eシール生成者の実在性確認については、法的な存在確認だけでなく、物理的・運営的な存在確認をすることとして整理したい。具体的には、指針において以下のとおり方向性を示すとともに、CP/CPSに最低限記載すべき内容等の詳細については来年度に実施要項等の策定に合わせて検討することとしたい。**（←本日結論を出したい事項）**

eシールに係る指針の改定（案）

- 「2.3 組織等の実在性・申請意思の確認の方法」を以下のとおり修正する。

（修正前）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。

（修正後）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。

確認方法の具体例を示す図表については、次ページに掲載。

論点④　eシール生成者の実在性・申請意思の確認の方法

～前ページからの続き～

- “認定対象”のeシール認証業務において、eシール生成者の実在性や申請意思の確認方法については、「eシールに係る指針」の改正版に下図の具体例を記載することとする。

＜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具体例＞

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条に基づく認定認証業務） 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。		

＜eシール生成者の申請意思の確認方法の具体例＞

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

（★）はデジタルで行える手続

※１：下記の要件を満たす第三者機関データベースとする。
１．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ている。
２．データベースの内容（正確な場所、連絡先、その他属性情報）が証明書業界以外の商取引において信頼されている。
３．データベースの内容が運営者によって少なくとも年１回更新される。

論点④　eシール生成者の実在性・申請意思の確認の方法

～前ページからの続き～

- “認定対象外”のeシール認証業務においては、前ページの確認方法に加えて、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」の改正版に記載することとしたい。

＜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具体例＞

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。

＜eシール生成者の申請意思の確認方法の具体例＞

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		

（★）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。

論点⑥　認証局の秘密鍵の管理に係る基準

論点

- 認証局における秘密鍵の管理に係る基準をどうするか。
- 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のみ記載するか。

第５回検討会の議論で挙がった主な意見（抜粋）

- FIPS相当と記載されているが、「相当」の解釈について調査機関の判断が難しくなる点を心配している。（中略）総務大臣のタイムスタンプの認定制度では、鍵管理やHSMの基準はこれらの点をわかりやすく明瞭になるように制度が設計されているので、タイムスタンプのHSMの基準を採用した方がよいのではないか。
- 基準の同等性については電子署名法の認証局の秘密鍵の管理と、eシール用電子証明書を発行する認証局の秘密鍵の管理は同等であるべきと考えている。他方で、タイムスタンプ認定制度ではHSMの基準に対してよりクリアに書かれていて調査もしやすいという状況にある。これは電子署名法の規定が古いため、電子署名法の規定を改定していかなければならないという課題に根ざしている。

第５回検討会での議論を踏まえた事務局の見解

- 認証局における秘密鍵の管理に係るHSM自体の基準及びHSM自体の管理に係る基準については、基本的に電子署名法を準用するとした「eシールに係る指針」を維持するものの、実施要項等の細則についてはタイムスタンプの認定制度も参考に議論していく。**（←本日結論を出したい事項）**
- また、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の細則に記載し、「eシールに係る指針」では最新の規格を参照できるように規定を定める。**（←本日結論を出したい事項）**

論点⑥　認証局の秘密鍵の管理に係る基準

～前ページからの続き～

eシールに係る指針の改定（案）

- 「2.5.1 認証局の秘密鍵の管理」を以下のとおり修正する。

（修正前）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、（中略）、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。

（修正後）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、認定eシール認証業務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、（中略）、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※１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。

※１：認定制度に係る設備・技術・運用基準は別に定める基準で規定する。

論点⑦　eシール生成者の秘密鍵の管理に係る基準

論点

- eシール生成者における秘密鍵の管理に係る基準を設けるか。

第５回検討会の議論で挙がった主な意見（抜粋）

- 電子証明書を発行するということは証明書のペアになる秘密鍵についても一定程度認証局からのポリシーが反映されるはず。最低限こういうことはやるべきということを記載した方がよいのではないか。
- CP/CPS等で利用者が適切に鍵を管理することを確実にしておかないといけない。実施要項等ではきちんと確認する等、完全に自由にさせるわけにはいかない。
- 秘密鍵の管理が不十分で問題が起こったときにはその管理者の責任ということを明らかにすれば、その責任のもと利用者側で好きなようにやればよいのではないか。（中略）秘密鍵の管理が不十分だった場合には、秘密鍵の管理者が責任を負うべきことを明確にし、さらにCP/CPSに記載するとよい。

第５回検討会での議論を踏まえた事務局の見解

- eシール生成者側の秘密鍵の管理については、「eシールの指針」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整理したい。なお、CP/CPSに最低限記載すべき内容等の詳細については来年度に実施要項等の策定に合わせて検討することとしたい**（←本日結論を出したい事項）**

論点⑩　eシール用電子証明書の失効要求

論点

- eシール生成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。

第５回検討会の議論で挙がった主な意見（抜粋）

- 電子署名においては、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）において、一定の場合の認証局からの失効について規定されており、これと同様に、認証局から失効してもよいと指針に記述していいのではないか。
- CP/CPSに今後どのようなことを規定しないといけないのかについては今後検討が必要と考える。

第５回検討会での議論を踏まえた事務局の見解

- 電子署名法に基づく認定認証業務においては、認証局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※１」、「利用者署名符号が危殆化したおそれがあるとき※２」等が挙げられており、eシールに係る認定制度においても、同様の場合において認証局から電子証明書を失効可能であると整理したい。なお、CP/CPSに最低限記載すべき内容等の詳細については来年度に実施要項等の策定に合わせて検討することとしたい**（←本日結論を出したい事項）**

※１：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。
※２：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「危殆化」とは「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。」と規定。

eシールに係る指針の改定（案）

- 「2.8 利用者におけるeシール用電子証明書の失効要求」を以下のとおり修正する。

（修正前）　（略）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。

（修正後）　（略）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」、「利用者署名符号が危殆化したおそれがあるとき」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。

論点⑪　認定制度の在り方

論点

- 認定の有効期間は何年とすべきか。

第５回検討会の議論で挙がった主な意見（抜粋）

- 大量にeシールを発行する場合、システム対応も想定され、５年や７年などシステム構築期間を含める結構長い間サービスとの連携が必要になるため、２年でサービスが終了してしまうと利用者への影響が大きい。そのあたりを具体的にどう配慮していくべきか、検討してほしい。
- 「電子署名及び認証業務に関する法律」では、認定は1年ごとの更新となっている。国の認定は非常に重いものであり、基本的に全体のスキームの整合性をとるのであれば「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の有効期間と同じように1年間とするのが素直ではないか。
- 元々発行していた事業者が認定を取り消された場合、eシールの効力はどうなるのか。

第５回検討会での議論を踏まえた事務局の見解

- eシール認証業務の認定期間については、認定に係るコストがeシール生成者が負担するコストにも影響を及ぼすため、認定の有効期間は２年としたい。なお、eシール用電子証明書自体の有効期間については、来年度以降、実施要項等の細則の検討時に議論することとする。　**（←本日結論を出したい事項）**
- また、認定に係る認証局が廃業した場合等の扱いについては、電子署名と同様、eシール生成者に事前に通知した上で当該認定に係るeシール用電子証明書を失効させることとしたい。具体的には、来年度以降、実施要項等の細則の検討時に議論することとする。**（←本日結論を出したい事項）**

「eシールに係る指針」改訂版の骨子案

骨子案		主な改正内容
本指針の位置付け		• 本指針と旧指針の適用関係等について記載
本指針の目的		
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シールを用いた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をについて記載 • 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・運営的の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		

（参考）現在の「eシールに係る指針」の目次

目次	
本指針の目的	
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
1.2	eシールと電子署名の異同
1.3	eシールのユースケース
1.4	eシールの仕組み
1.5	eシールの方式（ローカル/リモート）
第２章	我が国におけるeシールの在り方
2.1	eシールの分類
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
2.3	組織等の実在性・申請意思の確認の方法
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
2.5	認証局/利用者の秘密鍵の管理に係る基準
2.6	eシールを大量に行う際の処理
2.7	リモートeシールにおける認証
2.8	利用者におけるeシール用電子証明書の失効要求
おわりに	

最終取りまとめ（案）の骨子案

はじめに

第１章　eシールとは：eシールの定義等について記載

第２章　政府における検討経緯：中間取りまとめと同様の構成

第３章　国によるeシールに係る認定制度の創設：認定制度の在り方等について記載

第４章　個別論点と方向性

４．１　eシールの分類

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

４．３　eシール生成者の実在性・申請意思の確認の方法

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

４．５　認証局の秘密鍵の管理に係る基準

４．６　eシール生成者の秘密鍵の管理に係る基準

４．７　eシールを大量に生成する際の処理

４．８　リモートeシール方式における利用認証

４．９　eシール用電子証明書の失効要求

第５章　今後の課題

５．１　来年度以降、認定制度創設に向けた実施要項等の検討時に議論すべき主な事項

（本検討会で意見の挙がった具体例）

・eシール生成者の実在性・申請意思確認の規定方法

・電子署名法に基づく認定認証業務との関係性の整理

- 例）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複数の電子証明書を発行することを許容するか

・適合性評価に必要な設備・技術・運用基準と文書体系の在り方

・認定eシール認証業務の公開の在り方　等

５．２　中長期的なトラストサービスの在り方に関する検討

おわりに