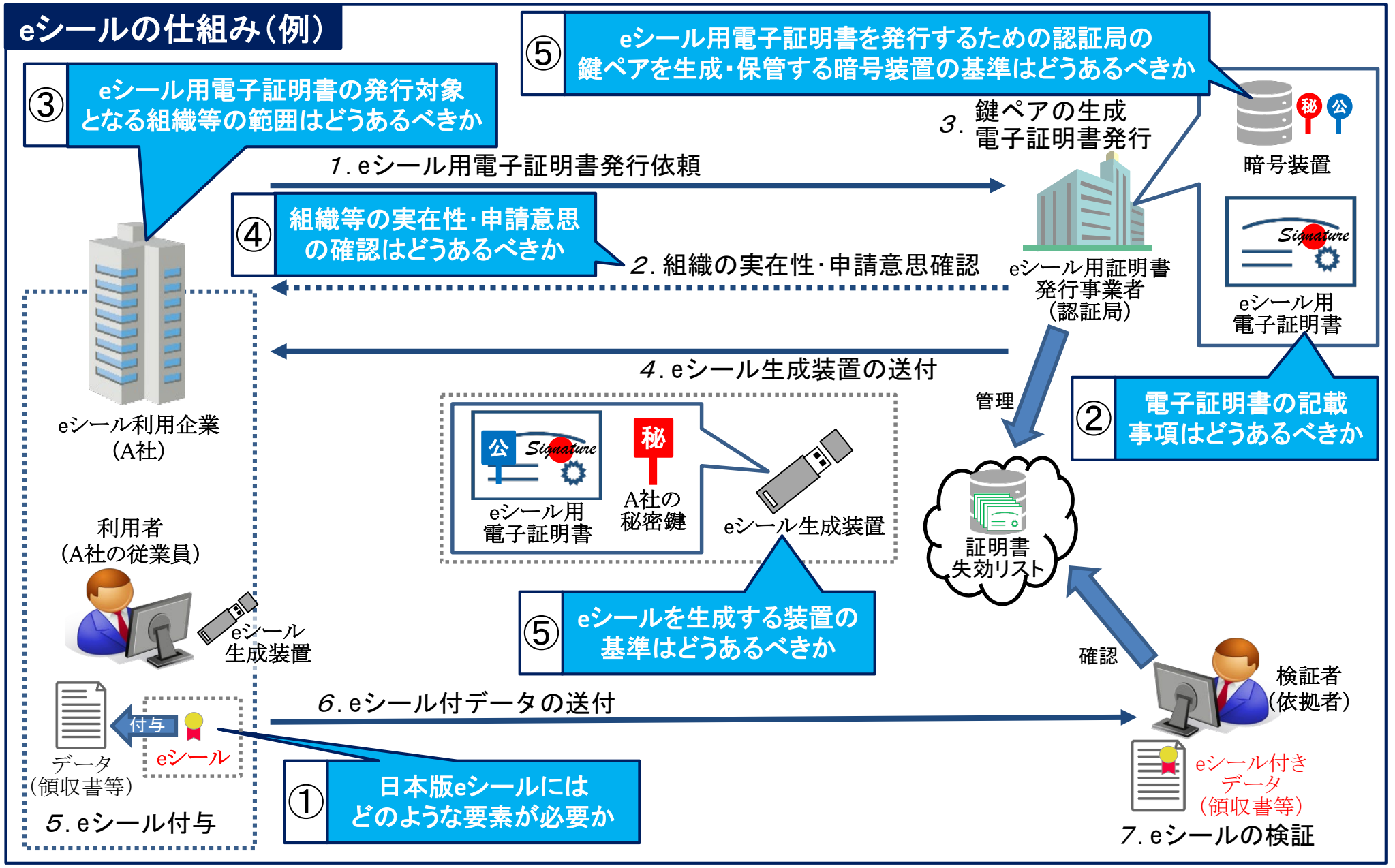
資料10－１

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（第10回）事務局資料

令　和　３　年　３　月　５　日

サイバーセキュリティ統括官室

eシールの仕組みの全体像（例）



我が国におけるeシールの検討事項の全体像

我が国におけるeシールの在り方について、主に検討すべき事項は以下のとおり。

既に検討された項目　今回検討する項目　今後検討する予定の項目　検討継続中の項目

① eシールに求められる要素

② eシール用電子証明書の記載事項

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

④ 組織等の実在性・申請意思の確認の方法

⑤ 設備（認証局側の暗号装置、ユーザー側のeシール生成装置等）の基準

⑥ その他（一定の技術基準（リモート署名方式、CRL（失効リスト）等）等）

前回検討会（第９回）の振返り

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

【検討事項】

- 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以下のどこまでを含めることが適切か。
  - 法人、個人事業主、権利能力なき社団・財団、その他の団体等の組織
  - 事業所・営業所・支店・部門等の組織内の細かい単位
  - その他（組織に所属する個人、機器等）
- 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はどうあるべきか。

【議論であがった主な意見】

- 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。
- 認証局で事業所等の実在性確認まで行わず、事業所等の情報を代表者の責任で電子証明書に記載するのであれば、当該情報はeシール付与対象のデータに直接記載されていることで十分という考え方もできるのではないか。
- 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。

【方向性】

- **eシール用電子証明書の発行対象**（認証局の責任の及ぶ範囲）**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、**eIDASとの整合性を図るため、**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。（事業所等の記載に係る責任は「組織等の実在性・申請意思の確認の方法」に記載）
- 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、**上記の発行対象（※）を前提とした場合、幅広いID・番号体系が併存し発行対象を網羅的に管理可能な識別子が現状存在しないことに鑑み、**既存のID・番号を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。

前回検討会（第9回）の振返り

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

【参考】

（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）

			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	
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	—	—	—※1	—※2	△※3	—	—
		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

※1　別体系で保持

※2　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。

※3　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。

前回検討会（第９回）の振返り

④ 組織等の実在性・申請意思の確認の方法

【検討事項】

- レベル3のeシール用電子証明書の発行に当たり、どのような手続・手段で確認することが必要か。
- 登記よりも小さい単位（事業所・営業所・支店・部門等）については、当該組織の代表者による宣言の結果を尊重することが適切か、または認証局が事業所等の実在性を直接確認することが適切か。
- 機器は事業所・営業所・支店・部門等と同様に扱うか。

【議論であがった主な意見】

- 組織の確認として、事業所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。
- 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。
- 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。
- 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。
- 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。

【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、申請意思の確認については、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、**認証局の責任の範囲外**であることが適当。

前回検討会（第9回）の振返り

④ 組織等の実在性・申請意思の確認の方法

- eシールに係る電子証明書の発行の手続きの整理は主に以下の表のとおり。
  - 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

前回検討会（第９回）の振返り

② eシール用電子証明書の記載事項等

【検討事項】

- eシール用電子証明書に記載すべき事項として何が考えられるか。

＜例＞公式名称（eシール用電子証明書の発行対象の組織等）、有効期間、公開鍵、署名アルゴリズム、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

- eシール用電子証明書のフォーマットはどうあるべきか。

＜例＞ITU-T X.509

- eシールのレベルに応じて記載事項を検討する必要があるか。

【議論であがった主な意見】

- 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。

【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、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で第三者による評価を受けている場合は、評価を行った第三者機関を拡張領域に記載することを認める（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。
- eシールのレベルを判別するための呼称（eIDASの例：適格（Qualified）、先進（Advanced）、裸のeシール）については将来決定することが必要。

前回検討会（第９回）の振返り

② eシール用電子証明書の記載事項等

【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
	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） 赤字は具体的な記載方法について、今後検討が必要な項目

検討事項

⑤ 設備（認証局側暗号装置、ユーザー側のeシール生成装置等）の基準

〇設備自体の基準

【検討事項】

- レベル3のeシールにおける、認証局側の設備であるHardware Security Module（HSM※1）の基準はどうあるべきか。

※1 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

➡ 国内の類似制度の状況や国際的な通用性の観点から、ISO/IEC 15408（コモンクライテリア）のEAL4+（プロテクションプロファイルについては、別途検討が必要）又はFIPS140-2 レベル3を求めることが適当か。

＜参考＞

- ✓ EU： ISO/IEC 15408（コモンクライテリア）のEAL4+又はFIPS140-2 レベル3
- ✓ 電子署名法※2： FIPS140-1 レベル3以上
- ✓ タイムスタンプ告示（予定）： FIPS140-2 レベル3又はISO/IEC 15408（コモンクライテリア）のEAL4+以上
- ✓ 公的個人認証法： FIPS140-2 レベル3相当

※2 実態として、FIPS140-2 レベル3認証以上の製品を使用

- レベル3のeシールにおける、ユーザー側のeシール生成装置の基準を求めることが適切か。求める場合、その基準はどうあるべきか。

➡ ユーザー側のeシール生成装置の基準を求める場合、当該基準の整備に時間を要する上、当該基準を満たした製品の調達は問題なくできるかどうかが課題となること、また、当該基準を満たした製品の調達は追加的なコスト負担が生じ、普及の妨げになり得ることに留意が必要ではないか。

＜参考＞

- ✓ EU： ISO/IEC 15408（コモンクライテリア）のEAL4+（ALC_DVS.2、AVA_VAN.5）
- ✓ 電子署名法： 規定なし
- ✓ 個人番号カードの調達仕様： ISO/IEC 15408（コモンクライテリア）のEAL4+（ALC_DVS.2、AVA_VAN.5）
  個人番号カードプロテクションプロファイル第1.00版（https://www.ipa.go.jp/security/jisec/certified_pps/c0431/c0431_it4485.html）

検討事項

⑤ 設備（認証局側暗号装置、ユーザー側のeシール生成装置等）の基準

○設備自体の基準

【参考： HSMのイメージ】

- 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

検討事項

⑤ 設備（認証局側暗号装置、ユーザー側のeシール生成装置等）の基準

〇設備の管理に係る基準

【検討事項】

- 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どうあるべきか。

➡ 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か。

＜参考＞

✓ EU： HSMに対するアクセスに関する規定、災害等に対する措置 等（資料10-2参照）
✓ 電子署名法： HSMに対するアクセスに関する規定、災害等に対する措置 等（P12参照）
✓ 公的個人認証法： HSMに対するアクセスに関する規定、災害等に対する措置 等

- レベル3のeシールにおける、ユーザー側のeシール生成装置の管理に係る基準はどうあるべきか。
  - ➢ 1つのeシール生成装置を複数人で共同で使用することを認めるか。
  - ➢ 又は、同一の秘密鍵を複数のeシール生成装置に格納し、複数人がそれぞれ管理して使用することを認めるか。
  - ➢ 又は、同一の組織等に対して複数のeシール用電子証明書を発行することを認めるか。

➡ いずれかを認めなければ、eシールとそれを使用できる（付すことができる）者が1対1となり、著しく利便性が低下して実質的に制度としての効果が限定される可能性があることに留意。

- ➢ 単にeシールを機械で自動的に付すことを認めるか。認める場合、特段の要件を求める必要があるか。

➡ eシールは発行元と非改ざん性を証明するものであり、eシールを付与する対象データの中身を証明するものではないことを考慮すると、不要とすることが適切か。

＜参考＞

✓ EU： 各法人の適切な管理に委ねられており、法人のガバナンスの問題と捉えられている。ただし、適格eシールの場合は適格eシール生成装置（QSCD）を使用するため、同一の秘密鍵の複製は不可

検討事項

⑤ 設備（認証局側暗号装置、ユーザー側のeシール生成装置等）の基準

〇設備の管理に係る基準

【参考】

- 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

（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

次回の検討事項（予定）

① eシールに求められる要素

② eシール用電子証明書の記載事項

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

④ 組織等の実在性・申請意思の確認の方法

⑤ 設備（認証局側の暗号装置、ユーザー側のeシール生成装置等）の基準

⑥ その他（一定の技術基準（リモート署名方式、CRL（失効リスト）等）等）

検討に当たっての主な観点

１．国内の類似制度との整合性

- 同じトラストサービスの1つである電子署名法上の電子署名との関係性
- 商業登記に基づく電子認証制度上の電子署名との関係性　等

２．国際的な整合性

- EU等の諸外国の仕組み・制度との整合性
- ISO等国際標準との整合性　等

３．eシールの普及・利用促進

- eシールの利用者視点で、わかりやすいeシールの目的・用途
- eシール用電子証明書発行事業者視点で、参考となるeシールの仕組みや技術基準　等