eシールに係る認定制度の関係規程策定のための有識者会議（第５回）議事要旨

1. 日時

令和６年 ９月 30 日（月）　13：00～15:00

2. 場所

オンライン開催

3. 出席者

（構成員）

伊地知構成員、漆嶌構成員、岡本構成員、小田嶋構成員、柿崎構成員、宿谷構成員、中村構成員、濱口構成員、米谷構成員

（オブザーバー）

デジタル庁

（事務局）

総務省、株式会社野村総合研究所

4. 配布資料

資料５－１　事務局説明資料　（実施要項第５条 修正案）

資料５－２　事務局説明資料　（実施要項第６条・第７条）

5. 議事要旨

◆議題（１）「実施要項修正案」、「事務局説明」について、事務局より資料５－１、５－２に基づき説明が行われた。

◆議題（２）意見交換、各構成員からのコメント。主な意見の概要は以下の通り。

〇事務局説明資料　（実施要項第５条 修正案）

（実施要項第５条第１項第１号に対応する技術・運用・設備の基準）

- 認証設備室へ搬入及び搬出可能な物品について、個人情報持ち出し等のリスクに鑑み、内規等で私物の端末をセキュアなエリア内に持っていくことは禁止されているため、私物のパソコン、スマートフォンの記載を削除し、業務用のパソコンのみ記載すべき。

（実施要項第５条第１項第２号に対応する技術・運用・設備の基準）

- 必要書類に、マルウェア検知に係る製品の OS 名とあるが、マルウェア検知に係る製品は業務用設備の上で動いているため、使用 OS 名が記載されているのは違和感がある。

- 代表的な保護措置にファイルの無害化とあるが、「検知したファイルの無害化」等、わかりやすい表現にすべき。
- マルウェア検知の対象の具体例に、e シール用認証業務用設備内のシステムのレジストリとの記載があるが、「レジストリ」は Windows の用語であり、Linux 等には適さないため、システム構成情報等と記載すべき。

（実施要項第５条第１項第４号に対応する技術・運用・設備の基準）

- 「Expire」は Common Criteria の用語であるが、同基準においては FIPS 認定に限定せず、Common Criteria も考慮して、認証ステータスが「Revoked」、「Historical」、「Expire」になった場合の対応方針を記載すべき。
- HSM で確認する内容を記載いただいているが、ESTI の EN 319 401 等では確認したことを文書化すべきとなっており、エビデンスを残すことを求めているため、同基準においても文章等のエビデンスを残すことを付記すべき。

〇事務局説明資料　（実施要項第６条・第７条）

（実施要項第６条第１項第１号に対応する技術・運用・設備の基準）

- データベースの内容について、トラストサービス業界のみならず、商取引に関わる業界においても信頼されていることを求めているが、信頼の判断方法を決めるのが難しいため、実績に関する基準の記載を再検討すべき。
- 利用者の実在性を確認するための内容が AND 条件であることがわかるように記載すべき。
- 預貯金口座の保有状況の確認を行う方法について、Verified Professional Letter(弁護士等の意見書や会計士等の報告書)により証明してもらう方法を例示すべき。

（実施要項第７条第１項第１号に対応する技術・運用・設備の基準）

- 利用者 e シール符号の複製や他人への共有をしてはならない点について、e シールの発行は組織が認める点に鑑み、組織内に複数人の担当者がいる場合もあるため、「他人」とは組織内の人間ではなく、組織に関係しない全くの第三者であることを明確にすべき。
- リモートの e シールの場合、委託を通して、正式に権限を付与して社外の人間に使ってもらう場合もある。「他人」の表現について、権限が付与されていない人への共有を禁じる趣旨に変更すべき。

（実施要項第７条第１項第２号に対応する技術・運用・設備の基準）

- 利用申込書又は利用の申込みに係る情報の記載事項について、利用申請者が在籍する組織の商号又は社名、本店又は主たる事務所の所在地、法人番号を求めているが、「利用申請者」を「利用申込者」に修正すべき。加えて、e シールでは利用申込者の氏名のローマ字表記は不要である。また利用申込者の自筆署名又は印鑑登録証明書に係る印鑑による押印ではなく、代表者の法務局に届け出ている印鑑証明書とすべき。
- 代表者の法務局に届け出ている印鑑の証明書を確認するのであれば、利用申込者の住所や生年月日は不要ではないか。他方、利用申込者の属性及び役職等は含めてもよいのではないか。

- e シール用電子証明書の用途について、具体的に確認する必要性があるか疑問である。
- e シール用電子証明書の用途を厳密に把握するより、指針で認めている範囲と異なる用途ではないことを確認することが重要なのではないか。

（実施要項第７条第１項第３の２号に対応する技術・運用・設備の基準）

- 利用者の識別に用いる利用者識別符号の生成の際、擬似乱数生成アルゴリズムを用いるとの記載があるが、擬似に限定せず「乱数生成アルゴリズム」としてはどうか。昨今は量子由来の乱数もあり、安全な乱数生成アルゴリズムであれば十分である。
- 利用者の識別に用いる利用者識別符号の生成は複数人によって行われる点がわかりづらいため、記載を修正すべき。
- 利用者 e シール符号の作成主体が利用者等となっているのは、リモート対応があり得るためと理解している。その場合、同等の安全性が確保できる環境や、複数人によって行われることが利用者側の管理にも求められるわけではなく、あくまで認証局側に求められる要件であると理解している。

（実施要項第７条第１項第４号に対応する技術・運用・設備の基準）

- e シール用電子証明書の有効期限について、正確な計算方法を記載すべき。
- 有効期限について、実施要項に合わせ５年以下と修正すべきである。そうであれば、実務者は可否判断日から日づけベースで考えることができるため、５年ちょうどで解釈しやすくなる。
- 電子署名法においては、電子証明書の発行日から５年が有効期限となっている。電子署名法側の実態も踏まえて記載を検討すべき。

（実施要項第７条第１項第５号に対応する技術・運用・設備の基準）

- e シール用電子証明書の拡張領域に、鍵使用目的と基本制約を記録していることとあるが、「鍵使用目的」は鍵用途とすべきではないか。基本制約は Basic Constraints を想定しているのであれば必須なのか確認いただきたい。
- 補足だが、RFC 5280 では、e シール用電子証明書であるエンドエンティティ証明書では基本制約はオプションとなっている。

（実施要項第７条第１項第７号に対応する技術・運用・設備の基準）

- e シール証明書の申請のリクエストや CSR にも電子署名は行う。そのため、発行者署名符号の用途に当該認証業務の e シール用電子証明書の CSR も含めるべき。

（実施要項第７条第１項第８号に対応する技術・運用・設備の基準）

- e シール検証者に対する説明事項について、「e シール用電子証明書を信頼すべきか否かの判断する際は、」を、「e シール用電子証明書を信頼すべきか否か判断する際は、」に修正すべき。また、同基準は事業者が e シール検証者に求めていることを示しているため、事業者が具体的かつ適切な確認手段を提示して、利用者に確認させることにすべき。
- 改ざん防止措置について、e シール用電子証明書の失効情報に改ざん防止措置は不要ではないか。電

子署名法の調査表で求められているのは、電子証明書及びフィンガープリントのみであるため、一般的な改ざん防止措置を講じるべきなのは「発行者の e シール用電子証明書及びフィンガープリント」だけに修正すべき。

- 失効情報は署名されているため、それが改ざん防止措置にあたるのではないか。

（実施要項第７条第１項第 14 号ニに対応する技術・運用・設備の基準）

- 監査結果の報告について、各認定事業者が直接報告する必要があるのか疑問である。
- タイムスタンプでは指定調査機関の調査が２年に１回、監査が年に１回と義務付けられているため、毎年各認定事業者が総務大臣に報告し、総務大臣が適宜指定調査機関に確認させることが規定により可能になっている。この際、各認定事業者の報告にはフォーマットがなく、任意の書式で報告している。このため、タイムスタンプの内容を踏襲しているのであれば現行の記載でよい。各認定事業者において、複数の指定調査機関を利用する可能性も残っており、各認定事業者側でどの指定調査機関に報告するか選択の余地があることに鑑みた結果、タイムスタンプでは各認定事業者が直接総務大臣に報告となっている。
- 電子署名法では調査機関が内部監査の結果等を確認した上で、指定調査機関が主務大臣に報告となっており、各認定事業者からの報告とはなっていない。

（実施要項第７条第１項第 15 号に対応する技術・運用・設備の基準）

- 認証設備室の入退出に関する記録を保存することを明記すべきである。その上で、同記録について指定調査機関の調査が入る期間は少なくとも保有し続けなくてはならないことを記載すべき。映像記録ではなく、記録簿のようなものを想定している。
- 電子署名法では、調査表 3D22 に記載に基づき、やむを得ず入室権限を有しない者を入室させる場合の記録も含め、年に１回の指定調査機関の調査までは保持すべきとなっている。
- 参考だが、弊社は CPS において、入退出の記録は次回の認定更新を受ける日まで保存することと規定している。
- 認証設備室に権限のないものを入室させる場合は、権限を有する者を複数同行させなければならない点がわかりづらいため表現を修正すべき。

6. 閉会

次回会合は、2024 年 10 月 24 日（木）13 時からオンラインで開催させていただく。

以上