

## 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3回）議事要旨

### 1. 日時

令和6年7月23日（火） 15:00～17:00

### 2. 場所

オンライン開催

### 3. 出席者

（構成員）

伊地知構成員、漆寫構成員、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3-1 事務局説明資料

資料3-2 実施要項修正案（総則関係）

資料3-3 実施要項修正案（認定基準関係）

資料3-4 実施要項修正案（認定手続関係）

資料3-5 実施要項修正案（指定調査機関関係）

### 5. 議事要旨

- ◆議題（1）「事務局説明」について、事務局より資料3-1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とおり。

#### ○事務局説明資料（資料3-1）について

（基準の考え方）

- e シールに係る認定基準のうち、HSMの認証基準など、世の中の最新の状況に合わせて更新すると理解した。

（セキュリティレベルの考え方）

- 認定 e シールと認定電子署名のセキュリティレベルを必ずしも揃える必要はないと考えるが、調査

の一部省略や認証局の併用等が実現した際には、結果として同等のセキュリティレベルになる。その点について賛成する。

- セキュリティレベルについては、電子署名法側のモダナイズ検討を参照しつつ、引き続き検討していくべきである。

(適合性評価の効率化の観点)

- AATL 認定事業者が、e シール用認証業務の認定を受ける際には、特定認証業務の認定事業者と同様の認証局の併用による軽減措置を認めるべきかについて、指定調査機関がビジネスを維持するためには、e シールの認定に限らず、他のサービスとの併用が必須になる。AATL の結果を受け入れる方法は複数パターンが考えられるが、どのパターンにおいても、e シール及び AATL 並びに電子署名に対応できることが望ましく、少なくとも、同じ指定調査機関が実施した調査であれば併用できるようにすべきであるとする。他の調査結果を受け入れ、軽減措置を認める際の条件等について、今年度中に検討すべき範囲の進捗を鑑みながら、検討を判断すべきである。

(見直し及び更新頻度)

- 実施要項とガイドラインの公表後に見直し頻度について、実施要項及びガイドラインに記載すべきである。

### ○実施要項修正案（総則関係）（資料 3-2）について

(定義)

- 「e シール検証者」、「利用者 e シール検証符号」、「利用者識別符号」、「発行者署名符号」等の定義について見直しをお願いしたい。その際には、電子署名法側のモダナイズ検討及びデジタル庁からのフィードバックを受けながら適切に変更すべきである。
- e シールの「利用者」及び「利用申込者」は、電子署名法の個人とは異なり、「利用者」は e シールを発行する組織、「利用申込者」は e シール用認証業務の利用の申し込みをする組織の代表者または代理人となるため、電子署名法と同様に定義付けが必要だと考える。この点については、実施要項で定義いただきたい。

### ○実施要項修正案（認定基準関係）（資料 3-3）について

(e シールの安全性に係る基準)

- e シールの「生成」と「付与」について、区別して記載すべきである。
- バスケット条項を設ける対応方針になっているが、これは主にバックワードコンパチブル（後方互換）のために CRYPTREC の対象外となった暗号技術を維持しなくてはならない事態に対応する必要性を鑑みた方針であるため、文言を修正すべきである。
- バックワードコンパチブル以外にも、暗号技術の弱体化等のケースが起きうるため、バックワードコンパチブルだけに特化した記載は避けるべきだと考える。

(業務の用に供する設備の基準)

- 電子署名法で認められていないため実施できないとなることを避けたい。AATL 等と調査結果を併用できる可能性があるのであれば、第三者認証を受けている等の条件を示すべきである。

(利用者の真偽の確認の方法)

- 修正文において、「利用申込者」の記載が繰り返されているため、省略できるように記載を修正いただきたい。
- 修正文について、会社代表者が、代理人が利用の申込み行うことを認めた際に利用申込をすることを意図しているのかわかりづらい。電子署名法の記載と合わせて確認いただきたい。

(その他の業務の方法)

- リモート署名は本検討範囲に含まれないとのことだが、PIN の管理者と利用者は異なるため、対応方針内においても PIN の管理者及び利用者並びに署名者を区別して表現すべきである。
- 修正文において、保護環境と記載しているが、キーユーセージ及びエクステンションのような保護を想定しているのであれば、利用目的の制限等に修正すべきである。
- e シール認定制度に秘密鍵の保護環境を入れ込むのは難しいことは認識しているが、将来的な技術的相互運用性を視野に入れた場合、今後秘密鍵の保護環境を検討する必要がある、この点についても可能であれば実施要項もしくはガイドラインで記載すべきである。
- 将来的な継続課題として、非常に短期間な電子証明書において、タイムスタンプと組み合わせて活用し、CRL を作成しないという運用方法もあり、今後の検討の際に意識いただきたい。
- 「認定に係る業務」は「認定業務」と記載していいのではないか。

(技術的能力)

- 将来的な継続課題として、リスクマネジメントの観点がない点、公開鍵暗号の技術への認定が困難な点を認識いただきたい。

**○実施要項修正案（認定手続関係）（資料 3－4）について**

(認定の公示)

- e シールの検証に必要な情報は当該有効期限後も総務省ホームページに掲載するとなっているが、e シールにタイムスタンプを付与していれば、有効期限後も認定事業者が認定事業者のルート証明書のうち、長期署名の中に入っている古い証明書を検証できる点がメリットであるとの認識である。

(軽微な変更)

- 軽微な変更に関する事例として、電子署名側では JIPDEC のホームページ上で軽微な変更の情報を掲載しており、e シールにおいても同様にガイドライン等で過去の類似事例は情報共有すべきである。

(譲渡による承継の報告)

- 利用者や検証者の保護のためには、旧来の譲渡前の組織等が保有しているドメインで引続き CRL 等の提供が必要である点について、CRL の OSCP の URL が維持されないと譲渡後に利用を継続できなく

なるため、譲渡される側が引継ぐことをガイドラインで明確にすべきである。

### ○実施要項修正案（指定調査機関関係）（資料3-5）について

（指定調査機関が行う調査等又は確認に係る手数料の額の確認）

- 追加手数料及び諸経費が発生する場合は、現地調査等に関して発生するのであって、追加的な文書確認等では発生しないとの理解でよいか。指定調査機関に過剰な負担がかからないような配慮が必要と考える。
- 時刻認証業務の認定制度においては、追加手数料及び諸経費は指定調査機関側で設定している。そのため、e シールにおいて複数の指定調査機関が設けられる場合、各指定調査機関が定める必要がある。

（調査機関の指定）

- 指定調査機関に求められる条件が記載してあるが、e シールの認定認証事業者が電子署名法と同程度の規模となる場合、継続的に雇用することは困難であることをご認識いただきたい。実施要項及びガイドラインにおいて、指定調査機関に求められる条件の詳細について議論すべきである。

以上