

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7回）議事要旨

1. 日時

令和6年11月14日（木） 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、漆嶋構成員、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7-1 事務局説明資料（実施要項第7条・第8条・第9条・第10条修正案）

資料7-2 事務局説明資料（用語集・逐条解説案）

資料7-3 事務局説明資料（トラストサービス用OID体系の検討状況）

5. 議事要旨

◆議題（1）「実施要項修正案」、「用語集・逐条解説案」、「トラストサービス用OID体系の検討状況」について、事務局より資料7-1、7-2、7-3に基づき説明が行われた。

○事務局説明資料（実施要項第7条・第8条・第9条・第10条修正案）

（実施要項第8条の本文修正）

- 発行者署名符号に関する帳簿書類の「真正性確認に関する記録」が、改ざんされておらず真正性が担保されていることを確認している記録を想定しているのであれば、フィンガープリントの文字列が正しいことを確認した記録や、後に改ざんされていないことを確認した記録等が考えられる。しかし、改ざんされていない場合は記録が残らないため、改ざん防止措置が正常に機能していることを確認した記録とすべき。
- 発行者署名検証符号に関する帳簿書類において、リポジトリに公開されている検証用の情報が、適切な担当者によって検証されたことが記録され、その通りに実施されていることが重要である。改

ざんの検知を行っている記録や、改ざん防止対策が行なわれている記録があればよい。

- 対応方針の書きぶりが公開すること自体が目的と見えてしまうため、公開した上で、事業者がその通りに実施されていることが求められるように記載を修正すべき。

(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)

- eシール用電子証明書でも署名は可能である。ただ電子署名の用途とは異なり、eシールの電子証明書は署名者の意思を表すものではないため、署名者もしくは利用者の意思の確認を行うことを目的としていないことを記載すべき。

(実施要項第7条第1項第3号に対応する技術・運用・設備の基準)

- 受領書について触れている他の部分にも受領書の説明書きを追記いただきたい。

(実施要項第8条第2項第1号に対応する技術・運用・設備の基準)

- 当該業務という表現は「特定認証業務の認定に係る調査表」からきており、「電子署名及び認証業務に関する法律施行規則」の第12条の帳簿書類においては、作成及び廃棄の記録のみとなっているが、「特定認証業務の認定に係る調査表」の4109で配送に関する記録も追記されている。配送に関する記録は、正しく適切な本人に受領されたことを確認するための記録であるが、同記録も10年間保存すべきなのか疑問である。
- 電子署名法側における配送に関する記録は、指定調査機関が現地調査の際に確認している。配送時の差出伝票の原本は保有し続けているものの、郵便局のウェブサイトにおいて詳細なデータを確認できるのは配送から1年が上限で、それ以前に遡っての確認はできないため、10年保存の対象ではなかったと認識している。配送に関する記録は膨大な量になるため、事業者側の負担も大きい。
- 配送に関する記録は膨大な量になるだけでなく、重要性の観点からも作成および廃棄の記録と並列で記載すべきではないため、削除いただきたい。

(実施要項第9条第1項第2号に対応する技術・運用・設備の基準)

- タイムスタンプ認定制度は認定事業者による公告や公表方法を容認する書きぶりになっている。電子署名法の認定認証事業者の多くは、電子署名の対価を限度額とした賠償を前提に運営していると理解であり、eシール認定制度において特に厳しくする必要があるのか疑問である。
- 会社法に基づく公告方法と限定しているため、事業者側に対するガイドではなく、要件に読めてしまうことが懸念である。

○事務局説明資料（用語集・逐条解説案）

(用語集)

- 用語案を分類し、粒度を揃えるべき。分類が同じものをいくつかまとめて説明し、説明の中で例示としていくつかの用語を記載することや、それぞれ用語として取り上げ、相互参照すること等、わかりやすくなるように表現を工夫したい。
- 一旦候補を挙げ、世間一般的に不要である用語は落とし、重要な位置づけを持っている用語や、世間

一般的な使われ方と違う用語は残すべき。

- 用語集は、JIPDEC が作成し、電子署名法の法令集でまとめられているものがあるため、参考にすべき。

(逐条解説の検討 (第 4 条 e シールの安全性の基準))

- CRYPTREC 暗号リストは、電子政府における調達のために参照すべき暗号リストであり、法制度においては、タイムスタンプ認定制度で初めて参照された。タイムスタンプも e シールも電子政府に活用される重要なアプリケーションであることから、CRYPTREC 暗号リストを参照することは適切である。その重要性が増していることから、やむを得ない事情も踏まえた上で CRYPTREC 暗号リストは更新されるべきであり、今後の運用においても意識いただきたいと考えている。
- 認証事業者側の事情だけに触れる記載となっているが、利用者が電子文書を提出した先のシステムのシステムベンダーが暗号移行等の対応が間に合わないことも起こり得る。過去の暗号移行においても、認証局の対応が間に合わないことに比べ、電子システムの開発やシステムベンダーの対応が間に合わないことの影響が大きかった。e シールの利用用途が明確になっているわけではない現状を踏まえ、利用者の利用先の事情により、暗号移行の際に対応できないシステムが発生し得るのではないかと。

(逐条解説の検討 (第 15 条 認定効力延長の特例措置))

- ハードウェア・セキュリティ・モジュールが調達できない可能性があるという議論を踏まえ記載いただいたとの認識だが、その場合は認定の更新は難しく、認定の取消となるのではないかと。認定の更新時期において、ハードウェア・セキュリティ・モジュールが壊れ、使用不要になり、秘密鍵が保管できない状態であっても認定の更新が認められるという理解でよいか。
- 現行案では誤解が生まれるため、事業者の努力を凌駕するような不可抗力であることが分かる記載にすべき。具体的に天変地異や、大規模災害等が起きた際の特例を示すべきであると理解している。
- e シールの認定認証事業者だけでなく、様々な事情により指定調査機関側が業務を実施できない場合も考えられる。
- 契約書などでは、「戦争やテロ行為、事故、ストライキ、電力調達不能等の当事者が予見できず又はその発生を回避することができない事由」と記載することがある。

○事務局説明資料 (用語集・逐条解説案)

(用語集)

- 認定以外のローカル/リモート e シールで使用する証明書ポリシー群について、認定を取得していない事業者であっても、リモートやローカルの e シールを使用する際に活用してよいと理解した。
- 認定に係るローカル/リモート e シールで使用する証明書ポリシー群について、認証局側は認定の際にローカルかリモートかを区別する必要があると理解した。リモート署名のサービスを利用する場合はリモート e シールであると判断しやすいが、クラウド利用の際、BPO に委託する際等の場合において、どのように判断すればよいか。物理的に判断すればよいか。

6. 閉会

次回会合は、2024年12月18日（水）15時からオンラインで開催させていただきます。

以上