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４回）議事要旨

1. 日時

令和６年 ８月 20 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４－１　実施要項修正案

資料４－２　事務局説明資料

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４－１、４－２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。

○実施要項修正案（資料４－１）

（重要な事項の説明）

- 認証業務を利用する複数利用者に重要な事項を説明する必要があることは理解するが、毎年変更される可能性がある全担当者に毎年説明を行うことを義務付けるものなのか。利用者と認証事業者間には、利用約款や契約等が締結されることが想定され、その内容を担当者に守らせる責任は利用者側の契約締結者にあると考えられる。認証事業者側が利用者内のすべての担当者に説明することは想像しづらい。

○事務局資料（資料４－２）

（e シールの安全性に係る基準）

- 利用する暗号技術について、総務大臣がやむを得ない事情がある場合に暗号技術を指定する「やむを得ない事情」の具体的な場面はガイドラインの逐条解説の章に記載すると理解した。

（業務の用に供する設備の基準/認証設備室への入出場管理関係）

- e シール用認証業務用設備などを設置する個別の認証設備室の入出場口に手荷物チェックをするためのサークルゲートを設置することになれば、認証設備御室の前面は設置場所に制限がある。多くのデータセンターのサークルゲートはデータセンターの入口に設置される場合が多い。また、認定事業者は追加で大きな投資を強いられることになる。既に電子署名法の認証設備室に係る基準は生体認証の導入を必須にしており、既にヨーロッパの基準に比べても厳しい内容になっており、コスト負担も大きくなっている。
- 盗聴等のリスクに鑑み、認証設備室からの持ち出しだけではなく、認証設備室への持ち込みについても配慮すべき。
- 今後認証設備室に対するリモート調査の機会も増えていくことが考えられ、設備基準もしくは運用基準においてリモート調査の観点を入れるべき。
- e シール用認証業務に用いる端末だけではなく情報類が記録されている媒体や保守用の端末等も想定に含めることについて同意。設備基準もしくは運用基準において、入退出者による設備、ログデータ、搬入・搬出についてはあらかじめ手続きを定め、管理下のもとで行うとする等と記載することも考えられる。
- 運用に関する基準については第 7 条の業務の方法に移行してもよいのではないか。

（業務の用に供する設備の基準/e シール用認証業務用設備への不正アクセス対策関係）

- e シール用認証業務用設備におけるマルウェアに対する検知及びそれに対する保護装置について、将来的に国際相互運用等を見据えた際の備忘として、ETSI のトラストサービスの要件である ETSI EN 319-401 V3.1.1 には、外部ネットワークを通じた通信だけではなく、内部セグメント側にも脆弱性診断を行うことが含まれている。
- マルウェアに対する検知及びそれに対する保護措置はリアルタイムに行われることが重要である。
- マルウェアに対する検知及びそれに対する保護措置を講じることは外部ネットワーク経由の通信のみが重要なわけではない。また、必要書類としては、マルウェアに対する検知及びそれに対する保護措置を行う製品名、OS、そのバージョン等に関する情報も考えられる。
- マルウェア検知及びそれに対する保護措置の対象を e シール用認証業務用設備すべてとするのであれば、国際相互連携レベルになると考える。
- マルウェアに感染していないにも関わらず、利用者側のネットワークから認定認証事業者側のリポジトリがマルウェアサイトとして誤登録され、利用者側がアクセスできなくなり、誤登録の削除対応いただいた例がある。
- 利用者識別符号等受信設備が設置されている場合、利用者識別符号等受信設備から e シール用認証業務用設備への TLS 通信のプロトコルについて、正式名称で記載すべき。JIPDEC のガイドライン等に記載はないが、TLS に限定せずに記載することで、TLS と同等レベルのプロトコルも認める

べき。

（業務の用に供する設備の基準/e シール用認証業務用設備への不正操作対策関係）

- パスワードの設定について、NISC の「インターネットの安全・安心ハンドブック」ではパスワードの定期更新は不要だが、流出時にはすみやかに変更すべきとなっており、それに合わせて電子署名法の調査表も変更があったため、流出時の観点も追加すべき。また、記載方法については、電子署名法の施行規則にあわせるべき。
- パスワードの設定については推奨事項を記載すべき。例えば、担当者の個人アカウントの場合は、初回ログイン時にパスワードを変更すること等を記載してはどうか。
- ネットワーク経由の遠隔操作について全てを不可能にしてしまった場合、仮想サーバを設け、認証設備間をネットワークで繋いでいる環境に対応できないため、セキュアゾーンの外部から単一でアクセスすることは認めないというものを想定していた。具体例として、認証設備室に複数人で入室し、複数人でネットワークを相互けん制するのは認めるべきではないか。
- 重要システムに外部からアクセスする場合の多要素認証については、ログサーバやネットワークキーなどにアクセスされることをきっかけに攻撃が可能になることもあるため、重要なシステムと限定してしまうと語弊がある。CA/Browser Forum (CABF)のセキュアゾーンの定義等を援用し、信頼されたアカウントを有する人がセキュアゾーンの外部からアクセスする場合は追加の認証を行うべきとすべきではないか。
- リモート e シールサービスを阻害しないために、利用者が自分の管理と責任において作成する場合と修正することを検討いただきたい。

（業務の用に供する設備の基準/発行者署名符号を作成し又は管理する電子計算機関係）

- FIPS の認証ステータスについて、「Expire」ではなく「Revoked」と記載すべき。
- 運用中の HSM の認証ステータスが「Revoked」又は「Historical」に移行した場合は、その後の新規の発行者署名符号の生成には利用しないという点を追記すべき。
- 指定調査機関の業務上、指定調査機関が何らかの承認を行うことはあり得ないため、記載方法を適切に検討すべき。
- 暗号アルゴリズムについて、暗号移行を視野に入れてハードウェアを選択すべき。暗号アルゴリズムの変更の負担は大きく、出来る限り将来的に対応し得る暗号アルゴリズムが実装されている HSM を採用することが望ましいと明記すべき。

（業務の用に供する設備の基準/e シール用認証業務用設備への災害対策関係）

- UPS や CVCF 等の設置に関する基準に関連し、必要書類として認証設備室における単線結線図も追加すべき。
- 軟弱地盤に対する不同沈下防止措置について、電子署名法が施行されてから長く変更されていないため、更新すべき。
- バックアップ媒体を管理する設備について、e シール用認証業務用設備と別の場所に設置されていることが重要であるため、同一の災害による被害を避けられる別の場所としてはどうか。異なるビ

ルのレベルでは不十分と考えられる。

- バックアップ媒体については、別の場所と記載すべき。将来的な国際相互運用を考える際の参考だが、ETSI のトラストサービスの一般基準では、バックアップ媒体は十分な距離が離れた別の場所に設置するという記載である。
- バックアップ媒体の別の場所については、可能な限り遠隔地にすべきという含みを持たせるべき。東西でエリアをわける等厳格な制限を設ける必要はないが、近場では不十分であることが伝わればよい。
- 災害対策関係は対策の主体が、データセンター、事業者の発注者、事業者複数あり、確認先及び確認方法が異なるため、それに応じて災害対策が書きわけられるとよい。

6. 閉会

次回会合は、2024 年 9 月 30 日（月）13 時からオンラインで開催させていただく。

以上