

電子署名及び認証業務に関する法律の施行状況に係る検討会（第2回） 議事要旨

1 日時

平成20年2月19日（火）9：30～11：00

2 場所

経済産業省別館 11階1120共用会議室

3 出席者（敬称略）

【構成員】

辻井 重男	情報セキュリティ大学院大学学長【座長】
石黒 義昭	株式会社コンストラクション・イーシー・ドットコム代表取締役常務
澁谷 裕以	社団法人日本経済団体連合会情報通信委員会情報化部会 IT ガバナンス WG 委員
高橋 伸和	日本ベリサイン株式会社顧問
手塚 悟	株式会社日立製作所システム開発研究所情報サービス研究センターシニアマネージャ
西村 達之	セコムトラストシステムズ株式会社代表取締役副社長（岡代理）
早貸 淳子	情報セキュリティ大学院大学セキュアシステム研究所客員研究員
藤原 宏高	日本弁護士連合会コンピュータ委員会委員
満塩 尚史	ディーディーエヌコンサルティング株式会社ディレクター

【オブザーバ】

伊藤 毅志	内閣官房情報セキュリティセンター参事官
亀田 繁	財団法人日本情報処理開発協会電子署名・認証センターセンター長
塚田 桂祐	総務省大臣官房参事官（藤井代理）
中井川禎彦	総務省行政管理局管理官（情報担当）

【関係者】

佐藤 純通	日本司法書士会連合会会長
-------	--------------

【事務局】

水野 紳志	総務省情報通信政策局情報流通振興課長
渡辺 知尚	総務省情報通信政策局情報流通振興課課長補佐
相澤 哲	法務省民事局商事課長
杉浦 直紀	法務省民事局商事課補佐官
三角 育生	経済産業省商務情報政策局長情報セキュリティ政策室長
小野塚直人	経済産業省商務情報政策局長情報セキュリティ政策室課長補佐

4 配布資料

資料2-0	議事次第（案）
資料2-1	第1回電子署名法検討会議事要旨
資料2-2	諸外国の事例について

資料2-3 報告書素案（パブリックコメント案）

5 議事の概要

(1) 開会

事務局から、開会が宣言された。

(2) 配布資料の確認

事務局から、資料2-0に沿って配布資料の確認が行われた。

(3) 第1回電子署名法検討会議事要旨の確認

事務局から、資料2-1に沿って第1回電子署名及び認証業務に関する法律の施行状況に係る検討会の議事要旨の確認が行われた。

(4) 議事

(i) 諸外国の事例について

- 事務局から、資料2-2に沿って説明が行われた。

【質疑応答・御意見】

- 1ページ目、「5. 形態」で、韓国においては「1枚の証明書を署名用と認証用の用途に使用」とあるが、「認証用」とは具体的に何か。また、韓国においては、電子署名として使われているというより、むしろ証明書レベルの認証に使われているのではないか。
- 2ページ目、「14. 電子証明書を利用したサービス」で、日本では、「電子申請、電子入札、電子契約、電子公証等」とあり、一般の人が使うアプリケーションが見えない。その意味で普及度としてどうかと思う。

(ii) 報告書素案（パブリックコメント案）について

- 事務局から、資料2-3に沿って説明が行われた。

※訂正：17ページ（1）論点の2行目、「図4-1」→「図2-5」

【質疑応答・御意見】

<電子署名法の施行状況について>

- 10ページ、「(5)まとめ」の書き方では、これまでの電子署名法の運用に何も問題がなかったように受け取れるため、今後、原因究明・制度の解明を深める等の書き方に修正すべきではないか。
- 普及度については、最初から国として義務化したかどうかによっても異なるのではないか。国民の安全に係わる部分のみを義務化するということもあるのか。
- これまでの経年変化は順調であると思うが、日本の人口に対する普及度を考えるとそうではない。

<技術的論点について>

- 内容がよくまとまっており、時期的にも適切なのではないか。ただし、15ページ6行目、「新たな

攻撃手法の発見によって急速に危殆化し得る SHA-1 の利用は」という書き方では、SHA-1 のみが弱く、新たな攻撃手法が発見され得るものであると解釈されかねない。他のハッシュ関数についても、新たな攻撃手法が見つければ同様なことが起こり得るため、書きぶりを修正する必要がある。

- スケジュールは妥当であるが、2013 年から 2014 年にかけてのスケジュールがかなりタイトである。一認証事業者だけでなく日本全体としてのスケジュールを考える必要がある。
- 16 ページ下の「また、以上の移行を円滑に進めるため」の下に列挙されている項目について、今後、どう取り組んでいくのか。
→来年度以降、詰めていきたい。
- 危殆化は、またいつか起こりうるものである。今回の経験を整理し、次に起きることに備えるため、関係者全体でどう議論していけばよいのかということについてはどう考えるか。
→今回の経験を整理、公開していくとともに、散逸しないように管理することが重要であると考えている。

<制度的論点について>

- 既に電子証明書を発行されている人が更新するとき、新規と全く同等な手続を取らなければいけないのかという点に関してはどうか。
→18 ページ図 2-5 のタイプ 3 の方法が認められている。

<ビジネス的論点について>

- 20 ページ、「◎公的個人認証サービスとの連携」とあるが、同列に書くと誤解を招きかねない。
→公的個人認証サービスの電子証明書を取得していれば、認定認証事業者が発行する電子証明書についてもオンラインで申し込むことができる既存の枠組みがあるため、今後その活用方策が色々と考えられるのではないかという意味で記載している。
- 20 ページ、「◎新たな取組の検討例」で、電子署名の普及促進なのか、電子証明書の普及促進なのかによって異なる。電子署名に限定せず電子証明書も含めて広く普及したほうが、安全な社会に貢献すると思う。その観点から、電子署名に限定せず、電子証明書の普及も含めた利用のガイドラインを策定するのはどうか。
- 20 ページ、「◎新たな取組の検討例」で、「検討例」とあるが、例に挙げられてなくとも関連する事項は検討すると理解してよいか。例えば、指定調査機関の調査工数の削減について、外部監査結果の利用検討のほか、審査のサイクルの見直しなども検討に含むと理解してよいか。
→そのとおりである。
- 20 ページ、「◎新たな取組の検討例」で、「指定調査機関の調査による認定認証事業者の負担を更に軽減」とあるが、結びは「指定調査機関による調査の工数を削減できるかどうか」とあり、上は事業者の話、下は指定調査機関の話となっており読みづらい。
→整理したい。

<その他の諸課題について>

- 21ページ、「4. その他の諸課題」の「(1)認定認証業務の電子証明書の発行対象」の「考え方」の最後の部分で、「認定認証業務以外」として、それを使うことは自由であるということを行いながら、その利用を促すような書き方にすると矛盾があるのではないか。また、「(2)認定認証業務の電子証明書に記載する属性情報」について、属性認証したときにどのような問題が発生するか、検討すべきである。
→その他の諸課題も、引き続き検討しなければならないと認識している。
- 21 ページの「4. その他の諸課題」で、韓国の事例と比べても、日本の場合は署名用途だけでよいのかということも含めて考えるとよいのではないかと思う。
- e 文書法に係る主務省令が電子署名法を参照している。そのため、企業において、数千万件ある申込書の電子保存のために、処理する人(パートタイマー含む)の印鑑証明を取ってきて、実印を押すということになっている。例えばここで一般の認証業務の利用推進を検討していくのであれば、例えば、国税庁において一般の認証業務を認める方向にならないか等、踏み込んで検討してもらいたい。
- 検討するスケジュール目標も、報告書に入れていただいた方がいい。

(iii) その他

- サーバ証明書を始めとする電子認証は普及してきているのに対し、電子署名は仕組みが難しく、なかなか普及してきていない。何らかのインセンティブか、義務化を考えなければ、本格的な普及は難しいのではないか。根本的なところから考えれば、電子商取引を進めることが効率化、ひいては国力の向上に繋がるとし、積極的に普及を図っている諸外国の例もあるため、来期以降、議論を継続してもらいたい。
- 今回 4 土業会から要望が出てきたが、今後、法律で設置等が規定された団体から要望が出てきた場合を念頭において、一般的にそのような団体については、同様の真偽確認方法を広めていけるように規定した方がよいのではないか。
- 利用者証明書は有効期間が最大で5年のものもある。そういったものが一定の期間で有効期間が全部終わってしまうということになると問題が出てくると思うので、新しい証明書への移行にあたっては、エンドユーザの使いやすさも考慮した指針を示すとよい。

(5) 次回会合について

次回会合は3月下旬を予定。事務局から連絡する。

(6) 閉会

辻井座長から閉会が宣言された。

以上