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３回） 議事要旨

１ 日時

平成２０年３月３１日（月）１３時００分～１５時００分

２ 場所

経済産業省本館２階　西８共用会議室

３ 出席者

【構成員】

辻井　重男	情報セキュリティ大学院大学学長【座長】
松本　恒雄	一橋大学大学院法学研究科教授【座長代理】
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
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
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	総務省行政管理局行政情報システム企画課情報システム管理官

【事務局】

中田　睦	総務省情報通信政策局大臣官房政策統括官（情報通信担当）
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情報セキュリティ政策室課長補佐

４ 配布資料

資料３－０	議事次第（案）
資料３－１	第２回電子署名法検討会議事要旨（案）
資料３－２	暗号技術検討会からの回答について
資料３－３－１	報告書案（パブリックコメント案）への対応について

資料３－３－２－１　　パブリックコメント　三菱電機
資料３－３－２－２　　パブリックコメント　日本ベリサイン
資料３－３－２－３　　パブリックコメント　電子認証局会議
資料３－３－２－４　　パブリックコメント　タイムビジネス協議会
資料３－４　　報告書案

５ 議事の概要

（１）開会

事務局から、開会が宣言された。

（２）配付資料の確認

事務局から、資料３－０に沿って配布資料の確認が行われた。

（３）第２回電子署名法検討会議事要旨の確認

事務局から、資料３－１に沿って第２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）暗号技術検討会からの回答について

● 事務局から、資料３－２に沿って説明が行われた。

【質疑応答】

○ ＲＳＡの素因数分解は線形予測が可能だが、ＳＨＡ－１は直ちに危殆化するということではないため、状況を見極めながら、一旦、緩急あったときの対応方法を決めておくということか。

（ⅱ）報告書案（パブリックコメント案）に係る御意見への対応について

● 事務局から、資料３－３－１及び資料３－４に沿って説明が行われた。

パブリックコメント期間（３月１４日～３月２４日）に、合計４つの団体から御意見を頂戴した。

【質疑応答】

＜全体について＞

○ いろいろ重要な御指摘をいただいている。「重要な」という意味は、我が国全体あるいは電子政府全体にとっては重要だが、必ずしも、本検討会の管轄ではないものもあるため、このような回答になってしまう面があるのだろう。したがって、電子政府としては、もう少し広い視野から検討していく必要があるだろう。

＜技術的論点について＞

06番:

○ 組織間の連携、情報知識の共有が一番の問題である。０６番について、「リスクの掲示をお願

いしたい」とあるが、単に啓発の問題だけではなく、リスク分析しなければならない話であり、それはＣＲＹＰＴＲＥＣ単独ではできない。例えば、文部科学省の独立行政法人である科学技術振興機構（ＪＳＴ）の社会技術研究開発センター（ＲＩＳＴＥＸ）では、技術をいかに社会的実装するかという観点で５年間、プロジェクト研究を行ってきたが、その中の暗号リスク研究チームが、どのようにユーザに説明し合意していくかということで、Security Level Agreement という概念を出し、システム実装のシミュレーションのソフトも作成したという研究成果がある。Security Level Agreement は Service Level Agreement をもじり、ユーザ、暗号供給者、設計者間の対話を進めていこうとするもので、非常によい研究成果だと思うが、そのようなものとＣＲＹＰＴＲＥＣの暗号リスクのガイドとの連携、知識の共有、情報の共有等も必要である。

○　リスク分析は、本来は、実際にその業務を行っているところでやればよいのだろうが、能力的な問題もある。現場の状況を踏まえて、どのような重要な資産に対して脅威はどうであるかというリスク分析の手法で考えると、技術的な知識だけでは対応できない。とすると、何らかの組織や相談所が必要なのではないか。単に啓発すればよいのであれば、必要ないかもしれないが。

０８番：

○　長期署名やタイムスタンプも暗号技術を使っているのだとすれば、技術的な脆弱性は同じではないかと思うが、暗号技術が脆弱化しているという前提の下に、なぜ長期署名やタイムスタンプだけが役に立つのか。

→タイムスタンプと長期署名の話は技術的には少し違い、長期署名というのは、例えばＲＳＡ１０２４がいつまでもつか、長期的にもつように保証していかなければならないという話しである一方、タイムスタンプは、デジタル署名のような技術で行うため、時間軸が少し異なる。電子署名法ではタイムスタンプについては言及していないが、本来は、合わせて議論すべき問題だろう。

○　タイムスタンプを含めて暗号すべてに完璧なものはないが、それを国民が理解しているか。または、国民が負えるリスクになっているかというところが難しい。国民に普及啓発しながら理解していただくとともに、制度としても、それをみながら実装していくことを行わなければならない。

９番：

○　０９番の御意見は、括弧の中で有効期間の問題について触れられており、それに対する検討会の考え方は原案どおりということになっているが、認定認証業務を運用されている方々からすると何とかしてくれないかというところが出てきているのではないか。ただ、ＣＲＹＰＴＲＥＣからの御意見を考えると、今回の検討会の考え方も納得できる。

１０番：

○　電子認証局会議について、特定認証事業者の方々から意見が出ているのが、今回の例えば暗

号アルゴリズムの変更に関して、国民への短絡的な不安を煽るような話にはならないようにしてほしいということだと思う。これだけの短期間で、十数個の認定認証局が同じ方法でよいのかということもあるが、アルゴリズムを移行していかなければいけないというのは、やはり経験したことがないため、不安があると思われる。早期にということをまず一つのキーワードとして、関連組織と綿密な調整をしていただきたい。

- ○ 認証業務を預かっている立場で言うと、移行のプロセスにはまだ不安があるため、その部分を詰めさせていただきたいという趣旨である。
- ○ ＳＨＡ－１やＲＳＡ１０２４がある時点でなくなると、その時点で認証局をリボークすべきではないのではないかという御意見があったが、現時点ではリボークすべきではないかと思う。もう少し検討しなければならない。
- ○ リボークの時期が来たときには、主務３省から御指導いただけるか。いただけない場合には、私どもが主務３省にお伺いを立てて結論を出し、最終的には私どもは認証事業者にリボークすべきかどうかということで、方針をどちらか決めなければいけない。認証事業者の適合性について調査をする立場にあるため、ある時点では定めなければならないと考えている。
- ○ 移行時期については、やはりいろいろなリスクを考慮した上で、決めるべきところは決めないと社会のシステムが回らなくなるため、本検討会の意見を基に是非整理いただきたい。
- ○ 電子契約サービスをしている民間の会社として、今の認証局のリボークの話も踏まえて、実際に新しいアルゴリズムに切り替わっても、古いアルゴリズムで署名した契約書が数年保管されている状態で今、運営することになる。署名検証というのは起こるが、その場合、古いアルゴリズムは一切面倒を見ていただけないのか、それとも、その場合でもそれはすべて民間側の検証業務にゆだねられることになってしまうのか。
- ○ 移行時期については年数のスケジュールがこの報告書案に示されているが、現実に使われている証明書（例えば３年間等、年数を決めて発行されるわけだが）の有効期間の終了するまでは検証環境は残すべきだと考える。今の電子署名法の世界は、長期署名のことを謳っているわけではないため、常に電子署名をされた電子文書を、そのときの証明書の有効期間が切れた後どうするかということについては、現行の電子署名法の範囲ではなく、他のところで解決すべき問題であると考えている。
- ○ 法律の議論としては、推定効があるため、明らかに暗号技術が破られている状況になっていなければ、事実上の推定効はまだ働くと思う。したがって、紛争になった場合には、先行きそこで決着が着くだろうが、事前の行為準則のようなものとして、どの段階でどのように政府として認証局等に行動させるべきかというのは、まさにその次元で、紛争を予防することが重要であるため、そのような観点から早い段階で考えていく必要があると思う。新しい、より強度の強いアルゴリズムに標準が変わったからといって、それ以前の古い証明書が、まだ現実にリスクが顕在化していない段階において事実上の推定効を破られることはないだろう。
- ○ 今回のアルゴリズムの変更というのは特殊なことではない。ＰＫＩである以上、今後も変更され続けるため、どこかで検討していただく必要がある。

＜制度的論点について＞

○　今回の検討範囲でないことは承知しているが、電子署名法とＧＰＫＩ、ＪＰＫＩと言われている公的個人認証、民間で使われているＳＳＬ等、いわゆるブラウザ等に標準搭載されている認証のトラスト範囲、トラスト・ドメインをどのように関連づけるか、設計するかが重要で、その部分が日本全体として関連性が薄い。勿論、ＢＣＡとも関連づけていると理解しているが、もう少し有機的に結び付けないか検討が必要ではないか。一方、ＰＫＩは歴史的に浅いため、容易に信頼関係の構造を構築するのはできるが、実際、人間社会における複雑な信頼関係をどう構築するのか、ＰＫＩの業界としても研究していただきたい。その辺りは今回のパブリックコメントの中でも見えてきたのではないか。

○　できれば今後省庁間をまたいだ電子署名やＰＫＩという認証をどのように国民に利用してもらうのかを検討をする場があってもよいのではないかと思う。

○　他の機関、公的個人認証、ＧＰＫＩ、ベンダー等様々なものが関わっているが、その中で実際にシステムとしてとらえた場合に、社会制度とどういうふうな関わりを持つのかという点では、かなり複雑になっているところがあり、電子署名法が５年経過した今、見直す必要があるのではないか。技術的な側面からいうと、やはり今回こういうアルゴリズムの問題が出ると、やはりそのアルゴリズムも当然ベンダーとしては開発をし、供給していくわけだが、スケジュールが最も重要になってくる。国民に迷惑がかからないようにするにはどうするのかという視点で、長期的視野で慎重に検討しなければならない。電子署名法だけではなく、社会制度のインフラを考えた場合に、ほかのＧＰＫＩや公的個人認証とも連動し、ある基盤のところは協調しあうなどしていかなければならないが、民間も交えて検討することが重要。

○　法務的な検討も平行して行っていただきたい。アルゴリズムを変更してしまうときに法的にどう考えるべきかは、電子署名法の条文だけ見ていても理解できない。

＜ビジネス的論点について＞

○　ＰＫＩといっても、ＧＰＫＩやＪＰＫＩ、ヘルスケアＰＫＩ等、さまざまなＰＫＩを使った制度が出てきている。これは事業者からすると、すべての運用基準から求められるセキュリティレベルが全く異なるため、非常に困難である。１つの例で言えば、電子証明書を発行する際に、署名用の証明書と認証用の証明書を１つの認証局から発行できないというのが現行の電子署名法の規定だが、これを許していただかなければ、認証局を複数建てなければならなくなり、これば事業者にとっては切実な問題。アプリケーションがないということもあるが、さまざまなＰＫＩがあり、それぞれの運用形態、取得形態すべてが異なるということがＰＫＩ全体の普及の阻害要因になっているのではないか。脆弱性について議論することも重要かとは思うが、現在の発行状況をみて、まずはどのようにしたら普及するのかという観点で、報告書の中に記載したほうがよいのではないか。

→　今回は、期間的な問題があり、ビジネス面についての論点にまで、踏み込めてないことは認識している。それについては来年度は体制を立て直してやらせていただきたい。

（iii）報告書案について

○　報告書の１７ページ二番目の問いの、「ＳＨＡ－１、ＲＳＡ１０２４ｂｉｔに基づく電子署名を将来、無効とする旨を、どのように規定すべきか」について、まず、「電子署名を将来、無効とする旨」というのは曖昧な書き方で、署名の有効、無効については電子署名法でも規定していないため、書き方を見直す必要がある。また、問いに対する結論が合っていない。本質的な問題として「どのように規定すべきか」という問いでありながら、１９ページの答えは、制度面の課題として推定効への影響の検討を行うことが適当であると書かれており、どう規定するのかという質問に答えていない。そのような書き方に直すか、質問を「いつ削除すべきか」にして、削除時期のみを明らかにして、その他の適用関係の整理や規定についてはシステムを運用している関係者の体制等、合わせて検討していくという書き方にするなど工夫が必要。

推定効について

○　政府が指定した技術を使っていれば、自分の側では証明しなくても大丈夫だということになるということであるため、基準が変わったとしても、従来の技術が容易に破られたことが明確でないのであれば、事実上の効力は続くのではないか。その辺りは裁判になった場合の事実上の推定の話ではないか。

○　事実上の立証手続を当事者に負わせないための法律であるにもかかわらず、このような改正をすることで、あとは事実の立証によるとするのは、無責任な印象を受ける。一定の推定効が認められる基になっていた技術を要件から外すときには、外したことに伴ってそれまでされていたものに与えられた法的効力はどうなるのかという、いわば、経過措置のような運用関係に関する規律は当然規定中に記載があって、どちらが何を立証すべきか整理される必要があるのではないか。改正のタイミングで、以降、推定力は全く働かないというものと、このような措置を執ることにより推定効が継続することがあるというものの両方を検討することが必要。

○　既に署名されてしまっているものが、後で当該技術はリストから削除された場合と、技術がリストから削除された後でなお新たな署名をするというのとでは、分けた方がよいのではないか。

○　法として推定効を与えるにふさわしいレベルのものでなければ、推定効の規定は置けないため、ある時点で推定効を与えるにふさわしくない状態であれば、それからは推定効が働いてはならない。その場合に、検証する際に推定効が及ばないことになるのか、ならないのかということは、その時点で整理せざるを得ない。いずれにしても、従前の電子署名について認められていた効力が、その時点でどう取り扱われるべきかということは、その時点での技術から判断されるべきことであると思われるため、その時点で整理がされなければならないことは間違いないが、その方針について、今この時点で決めることは難しいと思う。

○　移行規定で、過去のものについては何年間かは有効と推定するという規定を置くとすると、ではその時点までは安全なのか、新たに署名してもよいのではないかという話になりかねないので難しい。この種の問題について、既にできているものにだけ法律上の推定をそのまま

延長するというのは、少し論理矛盾ではないか。万一の場合を考えて、安全基準を作成していることを鑑みると、事実上は大丈夫ということで、非常に強い事実上の推定は残るという扱いが一番妥当ではないか。署名が有効だという側がそれを証明しなければならないが、それは従来の政府が指定していた基準どおりにやっているといえば、それで事実上の推定が働き、反対する側が、反証しなければならないという程度の運用でよいのではないか。

→　１９ページの一番下から２行目のところに、制度面の課題として「推定効への影響」とか引き続き検討事項と書いているが、注釈か何らかの形で、そのような議論があったということ、何を議論すべきかということについて付け加える。

報告書の対象者について

○　本報告書は広く一般国民を対象に出すものなのか、それとも有識者を対象に出すものなのか。もし一般国民に対して出すということであれば、先ほどから議論があるとおり、ＲＳＡやＳＨＡ－１等が本当に危険な状態にあるのかどうかについて、もう少し丁寧に説明する必要がある。

→　専門家や関係事業者の中で、意思確認、全体の歩調を合わせるための第一歩のものであると考えている。これをもう少し整理したものが、一般国民向けになると思う。

（ⅳ）その他

○　検討会としては第３回をもって終了とさせていただくが、この後、いただいた御意見を踏まえて事務局で報告書を修正し、電子メールで改めて御意見を伺い、報告書を完成させたい。

（５）閉会

総務省中田大臣官房政策統括官（情報通信担当）から、挨拶があった。

辻井座長から、開会が宣言された。

以上