電子署名法認定基準のモダナイズ検討会（第 3 回） 議事録

日時　　令和 6 年 11 月 26 日(火) 15:00～17:00
場所　　オンライン開催
出席者（敬称略）
(委員)
漆嶌賢二　　(GMO グローバルサイン株式会社事業企画部 フェロー)
小田嶋昭浩　(電子認証局会議 理事)
松本泰　　(特定非営利活動法人日本ネットワークセキュリティ協会 フェロー)
満塩尚史　　(順天堂大学健康データサイエンス学部 准教授)
宮内宏　　(宮内・水町 IT 法律事務所 弁護士)

(オブザーバー)
大澤昭彦　(一般財団法人日本情報経済社会推進協会　デジタルトラスト評価センター)
法務省民事局
総務省サイバーセキュリティ統括官室

(事務局)
デジタル庁　デジタル社会共通機能グループ

(事務局 山之上)
ただいまより、電子署名法認定基準のモダナイズ検討会第 3 回を開始いたします。皆様、本日はお忙しいところ、お時間いただきまして大変ありがとうございます。私は事務局を務めます、デジタル庁の山之上と申します。よろしくお願いいたします。まず、事務局より資料確認をさせていただきます。資料は全部で 2 種類ございます。一つ目が記事次第。もう一点目は、モダナイズの方向性に関する追加議論の方になります。本日の資料につきましては、デジタル庁 Web サイトの方にも掲載しておりますので、傍聴の方はそちらの方をご確認ください。本日の検討会につきましては議論いただく事項・内容が多いため、議事に先立ちまして、これまでの検討会の振り返りについて、資料 1 に沿ってご説明いたします。

調査につきましては、後ほど各項目において改めて説明させていただきますが、方向性①から⑥につきましては、こちらの資料のとおり、第 1 回検討会及び第 2 回検討会において議論いただいたところです。また、本日の検討会につきましては、残論点の濃淡を踏まえ、議論いただく順番について、①②の後、⑥をご議論いただき、その後③④の流れとさせていただきます。

それでは、以降の議事進行を松本座長の方にお願いしたいと思います。それでは、松本座長よろしくお願いいたします。

（松本座長）
それでは議事に入りますけれども、第1回、第2回に引き続き、活発なご議論をお願いいたします。5つの論点がありますので、一つ一つ説明していただき、後に議論ということにやりたいと思いますので、まずは①について事務局の方からご説明をお願いいたします。よろしくお願いします。

（事務局 山之上）
事務局でございます。
資料1の7ページからご説明いたします。方向性①に関して第1回検討会においては、法改正は不要であるものの、施行規則でリスク管理の義務を明示することが必要であること、またリスクマネジメントは単なるセキュリティ対策ではなく、組織全体のガバナンスとして位置づけ、ISMAPなどのガバナンスに関する基準が規定されたものを参照に盛り込むべきとの議論がございました。第1回検討会を受け、本検討会においては追加で議論いただきたい内容としましては、組織全体のガバナンスとして盛り込むべき基準について議論いただきたいと考えております。9ページに各標準・規格の目次一覧を記載しており、このうちガバナンスに関する部分を抜粋し、10ページに記載させていただいております。11ページから15ページの概要を参考に、認定事業者等に対しては最低限要求すべき事項を整理する観点で各標準・規格を整理すると、少なくとも責任や権限の明確化および情報セキュリティに関するリスクの評価と対応の2点は共通項であるのではないかと事務局としては考えております。
以上から方向性①につきましては、3点についてご議論いただきたいと考えております。1点目は事務局として先ほど申し上げさせていただきました共通項の2点は必要な事項だと考えておりますが、他に要求すべき事項はあるか。
2点目は、責任や権限の明確化について施行規則第6条第15号ロにおいて業務に従事するものの責任、権限、指揮命令系等を適切に定め業務を実施することを求めておりますが、これに加えてさらに取締役会等に関する責任や権限の明確化（ITガバナンスに関する規定）を設ける必要があるか。
3点目は、組織全体のガバナンスとして盛り込む基準に関して16ページの下から2つ目の青字にて基準を例示しておりますが、どのような基準とすべきか、また、指定調査機関による調査方法としてどのようなものとすべきかの3点となります。事務局からの説明は以上となります。よろしくお願いします。

（松本座長）
それでは質疑に入りますけれども、ご質問ご意見がございましたら、チャット欄の方に発言希望の旨をお書きください。一応見ておりますので、お願いします。早速、漆嶌委員よろしくお願いいたします。

（漆嶌委員）
組織全体のガバナンスっていうことが、少しフォーカスされすぎているような気がしていて、なぜリスク管理を追加で規定をする必要があるか、モダナイズする必要があるかってという背景にもう一

回立ち戻った方がいいのではないかと思いました。

例えば eIDAS での EN 319 401、WebTrust for CA、また CABF の Baseline Requirements 等、そういった国際的な認証局の要求事項で、定期的なリスクアセスメントをしなさいということが求められているので、(過去のデジタル庁様の事業者ヒアリングや調査研究により)それに対する対応をしましょうといったようなことになっていたはずだったかと思います。

ガバナンス対応をしたとしても、ガバナンス対応の一環としてリスクアセスメントをするというのはわかりますけれども、何かリスクアセスメントにきちんとフォーカスをしておかないとなにか、例えば、認証事業者によって、いい加減なリスクアセスメントをした結果を提出して、実施したからそれでいいでしょうという話には多分ならないのだろうと思っています。そういった事態はやはり避ける必要があるのだろうと思っています。

例えば認証局にはある程度共通の具体的なリスクがあるのではないかと思っていまして、第 1 回目にも少し説明させていただいたと思いますけれども、例えばツーマンで操作しますといったようなことを CP/CPS で定めている運用規定で定めているのに、実際にはそうなっていなかったといったような運用が発覚するようなリスク等、例えば利用者の鍵管理は FIPS 認定品を使ってくださいというようなことを言っていても、実は OS のキーストアに入っているようなものを使ってしまって、実際に鍵の複製ができるようになっている等、そういったいくつかの具体的なリスクがあるので、これに対してそれぞれ対応しているかどうかといったようなことを、最低限、認証事業者横断で、認定調査で確認をする必要があるのではないかなと思っています。

ご参考までに、総務大臣の認定タイムスタンプでは、そうした共通のリスク項目というのを、指定調査機関がリスト化をしておりまして、例えば標準時から時刻がずれたときに、間違ったタイムスタンプを発行してしまうといったようなリスクに対してどう対応するか、また運用端末が不正操作されるリスク等、そういった具体的なものに対して、どういったリスク対策をしているか、アセスメントをしているのかということがされているので、こういったものを参考にしてはどうかと思いました。

また、責任の権限や分離明確化の話は、リスク管理の話ではなくて、例えば権限を定めているけれども、遵守されなかったリスクをどのように扱っていますかといったようなことをしなければいけないことだと思うので、権限の明確化のような話は他の項目で担保されている話なので、リスクアセスメント議論の中では、取り上げて入れる必要はないのではと思いました。私からコメント以上でございます。

(松本座長)

次は、小田嶋委員のコメントをお願いいたします。

(小田嶋委員)

小田嶋です。漆嶌さんのご意見と、実は同じことを言うような形になりますけれども、もともとリスクアセスメントに関する基準で話していたところだと思っています。ガバナンスに少し特化したような形に、今の論点の詳細のところが見えてしまっており、どちらかというときちんと認証局の中でリスクアセスメントを行って、アセスメントの結果、リスクマネジメント等、もしくは例えば残留リ

スクがもしあれば、それを受け入れることを会社として、組織として残留リスクを受け入れ、文書化しておく等がもともとの発端だったと思うので、前後が逆になっているような印象を受けています。
そういう意味では、もとのところに立ち返っていただくというのが、いいかと思っています。私からは以上です。

（松本座長）
認証事業者の立場で、漆嶌委員と小田嶋委員の方からもう少しCAに具体的に現実的に足りないところを入れなければいけないというような話だったと思いますが、次に満塩さんお願いします。コメントも一番多分、このあたりの違い等がよくわかっていると思いますので、よろしくお願いします。

（満塩委員）
半分は確認になるかもしれませんが、今お二人からご意見あったことも踏まえつつですが、私のリスク分析の理解は若干違っており、これは法律の話をしているため、もし共通のリスクであればそれは、法律で規定すべきであり、法律で規定しなくても調査票レベルできちんと書くべきことだと思っています。そういう意味では共通的なリスク分析を、一般的にやってくださいっていうことを言うことではないと私は思っています。
個々の状況におけるリスク分析をやってくれっていうのは書けないものですかね。法律でも、規則の中でも、調査票レベルでも。というのは、昨今、やはりいろいろな情勢が変わってきており、2000年に最初は電子署名法を作っていますから、その時はあまりガバナンスということは言っていませんでしたが、各企業のガバナンスを確保するためにリスク分析をするということを。細かいリスク分析をやる必要があると言っているつもりは全くなく、結論から言うと、未知なるリスク、各会社個別に想定されるリスクということを想定しているのだと思っています。そういう意味では、一定程度リスク分析というのが、各社で異なるためにリスク分析するのではないかと思っています。
ISMAPではリスク分析と言うより、ガバナンスについて規定を沢山設けているわけではなく、基本的にはCOBIT等を見ていても、ガバナンスは方針を定め、それをモニタリングし、評価するというそこに尽きるわけですから、そういう意味では経営としての方針がきちんと示されており、その中でのリスクというものがいろいろと分析され、それがリスク表になっていて、そういったものがモニタリングされていることだという理解です。
そういう意味では、今日の論点の中にもあったどのような基準なのかというのがありましたが、ここも、現実的に法律上の確認方法ということになってしまうと、実体的な確認ではなく、どちらかというと、法律上での確認方法としたら、やはり方針書等、リスク分析の中身の書類というのが整備されているかということになっています。完全に個別の中までを本当に評価できるのかというと、そこはある程度は評価できる場合もあるかもしれませんけれど、私は難しいなという理解でございます。以上でございます。

（松本座長）
わかりました。次、宮内委員お願いします。

（宮内委員）
宮内でございます。少し違った側面からのコメントになりますけれども、今ここに表示されている2つ目のポツで、取締役等に関する責任の明確化のような話があると思いますが、基本的にはまずITガバナンスに対して取締役会はどうするのかというのは、電子署名法の認定の話かどうかということで、かなり私は疑いがあり、会社全体の話でしょうか、基本的には。
したがって、会社全体としてもITガバナンスをきちんとしなさい、それはしたほうがいいと思いますが、それをわざわざ電子署名法の認定基準に書く必要はないのではないかというのが私の思いです。さらに加えて、認定の申請にあたっては、恐らく代表取締役の機関決定が行われて、この申請をしているはずなので一定の確認は、少なくとも経営陣がしているわけですから、そう思うと、わざわざここまで書かなくても良いのではないのかなというのが私の思いです。以上です。

（松本座長）
認証局側の立場と満塩委員はISMAP等が深く関与していたというのがあり、さらに法律的な話で宮内委員の方からもご意見がありましたけども、他にご意見はないでしょうか。
JIPDECの立場で認証局を見るという立場ではどうなのでしょうか。

（JIPDEC大澤様）
ここは正直、現在の電子署名法の観点からは、こういったことまで深く突き詰めて見ているわけではありませんので、実際にどういった観点で何を見るべきなのかというところを少し明確にしていただかないと難しいという感じでしょうか。

（松本座長）
前回も議論があった他のISMSのような制度と組み合わせてやる等、そういった話になるのでしょうか。時間がそろそろ次の話題に行かなければいけないのですけれど、少し結論が出ているような、出てないような。方向性としてはやるということでしょうけれども、どのようにやるのかということに関して少し意見が割れているのかなといったところがありますけれども、事務局どうしますか、このあたり何か見解はありますか。

（事務局 當波）
最初の漆嶌委員と小田嶋委員からいただいたご意見と、後半の満塩委員からいただいたご意見、宮内先生からいただいたご意見、例えば、この大きな違いとしては、認証局、もうすでに必要な基準は電子署名法のこの基準にすでに書いてあるのであるから共通する部分についてはもうすでに書いてあるから、この特別なガバナンスの基準は設けなくてもよいというところと、各認証局の事情にフィットして、そこのリスクに対するアセスメントのPCDAを回していくというような観点の違いであると考えておりまして、事務局としては、今の現時点でどちらの考えであるかというところは、はっきりはしてはおりませんが、例えば各認証局の事情というところについては、一部共感するところもご

ざいまして、例えば大きな組織改変があり、教育のようなものがおろそかになってしまったような事例も伺っておりますので、各認証局におけるアセスメントというものは、何かしら求め、電子署名法の認定基準として求めるかは別として、各認証局の取り組みとしては行っていただくべきことなのであろうとは考えております。

そこで今皆様から一周ご意見を伺ったところでありますが、今の大きなご意見の方向性と違いについて踏まえた上で、お互いの意見についてどう思われるか、もう一周お聞きしたいというところであります。少々時間を押すことにはなると思いますが、もう少しこの点については追加のご意見を伺っていただきたいと考えております。

（松本座長）
満塩委員お願いします。

（満塩委員）
宮内先生の話を聞きながら少し思ったことが一つあります。今の電子署名法の認定基準の中では、オペレーションのことだけしか書いてないと私は理解しています。そこにはもちろん行動というか、どういうことをやるべきだということが書いてあるのですが、取締役会との関係性というのは、全く何も私はないという理解です。認定認証業務の立場に立った時に宮内先生がおっしゃったとおり、会社全体の事業の話をしなさいと言っているのではなく、認定認証業務に関するところでの、会社としての経営陣としてのコミットメントっていうことだという理解をしていますので、そういう意味では、限定的な範囲の中でどのように経営層が関わるのかということが、私は必要なのではないかという意見でございます。以上でございます。

（松本座長）
実質的にはしているとは思いますが、それが明文化されてないという話ですかね。

（満塩委員）
はい。

（松本座長）
漆嶌委員お願いいたします。

（漆嶌委員）
権限分離の話はすでにこちらに書かれている。取締役会がどうこうというよりも、例えば内部監査がきちんと独立した制度で回っているかどうか等、さらに HSM を使う時のオペレーターの権限分離等、そういったところの方が重要なのだろうと思っていて、そこのところは取締役会がどうこうといったような話ではないと権限分離については思っています。

満塩委員もおっしゃられていたリスク管理表のような、リスクを評価した結果表のようなものはや

はり調査の上できちんとアウトプットとして確認をする必要があるのだろうと思っており、これに関して、例えばタイムスタンプの場合ですと、共通で言われているようなリスクの他にも、きちんと各社個別のリスクというのも追記をして提出をしたりしていますので、そういったところで、個社の事情のリスクの判断というのは、そこでカバーされていると思いました。はい、私からは以上です。

（松本座長）
若干意見が割れているというか、二つの方向性が。両方ともやるともいいのかもしれませんけども、いかがでしょうか。

（小田嶋委員）
小田嶋から一つだけコメントしてもいいですか。現状各社、程度はわかりませんけれども、必ず取締役会において、つまり経営陣に承認を得て、事業を行う等、例えば何か事故があったら取締役会に報告をして、結果どういう事後の処理を行うか等、そういったことが普通は議事録等で残されているのだと思っています。今、電子署名法施行規則や法令下ではそこの満塩さんがおっしゃっているところのガバナンスという意味では明示は確かにされていないと思っています。2000 年当時から開始されて検討の状況に至った時に、そこが足りないということ自体はわからなくはないと思っています。
論点詳細のところで書いてあるところの段落下りているところの 1 ポツ目に、情報セキュリティに関するリスク評価を実施して、組織管理として書類の記録を残す。指定調査機関は書類に関してマネジメントや、ガバナンスというところの結果が確認できるということであれば、程度は違うかもしれませんけれども、現実に行っている内容とは思っています。したがって、それほど負担にはもしかしたらならないと思いました。それから、第三者認証があれば確認できたこととするというところは、それらが含まれるのであれば問題ないと思っています。

（松本座長）
宮内委員よろしくお願いします。

（宮内委員）
取締役会どうするかというのは、少しいろいろと意見はあることですが、資料で参考に上がっている規格で取締役会や経営陣と書いてあるのは、恐らく 12 ページと 15 ページです。まず、12 ページを見ていただきますと、ここの真ん中辺に取締役会があります。これは、なぜか倫理規範と変革のリーダーシップを発揮というのは、すごく全社的な話に私は見えました。
15 ページのところで経営陣はというのがあるのですが、情報セキュリティ活動の有効性等、割と全般的な話をきちんとしているということのように見えて、ISMAP 等そういうところを狙っているのかもしれないのですが、認証局がどうのというところと、ここで言っている取締役会経営陣の、任務や責任とは少し離れているような気が私はしましたので、このようなことを仮に入れるとしたら、何も電子署名法の認定のところに入れなくてもいいのではないかと思った次第であります。以上です。

（松本座長）
認証局は CP/CPS がありますからね。CP/CPS に沿ってしているというような一般的なセキュリティよりも、よりアーキテクチャに寄り添っているというのがありますので、そこはなぜかわからないです。そういったところ、満塩委員が別に負担がある方向に行くというよりは、何らかの明文化をしたいということ、それから実際に調査表に足りないと、漆嶌委員がおっしゃるように調査表に付け加える項目はあるのではと聞こえたのですけれども、どうなのでしょうか。

（宮内委員）
付け加えてもいいのですが、今ここに出ているような、会社全体でやるというようなことは恐らく書かない方がいいです。経営陣との取締役会がという話ではないというのが私の思いです。もちろん会社の規則や内規というのは、最終的には取締役の責任を作っているわけです。したがって、それ以上頑張らなくてもここに書かれている施行規則第 6 条第 15 号ロぐらいでいいのではないかと思いました。16 ページの真ん中のポチで言うと黒い字で書いている部分です。これで定めてというのは、これを定めるのが取締役の責任だとかは書かなくてもいいというぐらいの気持ちで私は言っておりました。以上です。

（満塩委員）
多分うまく稼働している時は問題ないです。恐らく、会社の事業でいろいろ問題があった場合、例えば、事故が起こった等、そういう時にうまくきちんと経営層とうまく連携することをきちんとしていてほしいという思いだと考えています。

（宮内委員）
それは理解できます。

（満塩委員）
したがって、全般的になにか大げさなことをしてくださいということはないということ、私等も CP/CPS 等、その中でやはりそういう事業、この認定認証業務そのものをきちんとしますということを、これは口だけかもしれませんけど、コミットメントしてもらうっていうのをあまり今まで見たことがないというのが私の理解です。そこを少し危惧していたのだろうという思いです。そこがカバーできれば私も松本さんもおっしゃっていたとおり、また小田嶋さんもおっしゃっていたとおり、当たり前にしている、していることなのですけれど、多分それをきちんと表明してもらうということだと理解してございます。以上です。

（松本座長）
認証局は CP/CPS があり、それに則って運用しているというものがあり、普通に回っていれば、非常に高度なセキュリティを達成していると思うのですけれど、多分、満塩さん 2000 年頃のことを

ご存知なので、当時こういう観点が足りなかったと思うので、おっしゃっているのだと思います。
細かい話というか、当然、先ほどのタイムスタンプの話である等、2000 年当時は理解できなかったようなところで、もう足りない点は見つかっているというのも、もう一つあるので、二点ぐらいが改正というか修正点なのかなと思いましたけれど、いかがでしょうか。調査できなければ致し方がないです。事務局いかがですか。

（事務局 當波）
今いただいたご意見を今日この場でまとめるということは難しいように思うのですが、共通するような部分、お互いの同意が取れるような存在したように聞こえておりまして、次回、今回いただいたご意見をまとめて、今回少々方向性に違いがあったところのオプションを、一目で見られるようにまとめた上で、共通するところについては、改めて合意をいただき、オプションについては、今回の今年の検討では、含めずに引き続き議論する等、電子署名法のこの認定基準においては、すでに実施されているような観点のため、含めないといったところの整理をいただこうというような方向性で考えております。

（松本座長）
モダナイズの方向性の②に関する議論を、次にお願いしたのですが、②について事務局の方からご説明をお願いいたします。

（事務局 山之上）
事務局でございます。資料 1 の 17 ページからご説明いたします。
方向性②に関しまして第 1 回検討会におきましては、暗号装置の技術基準を FIPS140-3 に更新すること自体は必要であるものの FIPS140-3 準拠の製品が非常に少ないため、現時点では FIPS140-2 相当以上とし、FIPS140-3 への移行時期は国内の関連製品の動向等を踏まえることも必要との議論がございました。第 1 回検討会の方を受けまして、本検討会におきましては、追加で議論いただきたい内容として、暗号装置の技術基準について、どのような内容でモデナイズを実施するべきかについて議論いただきたいと考えております。現行の暗号装置につきましては、電子署名法に基づく指定調査機関の調査に関する方針の第 2 2.に記載されているとおり、当方針第 2 2. (1)については、FIPS140-1 のレベル 3 を念頭に記載されたものであります。こちらのスライドは FIPS 140-2 のセキュリティ要件の概要を参考資料として記載しております。
以上から方向性②につきましては大きく 2 点についてご議論いただきたいと考えております。1 点目は FIPS 140-2 相当以上に変更するにあたり、求めるセキュリティレベルにつきましては、引き続きレベル 3 としてよろしいか。また、上記のセキュリティレベルを求めるとした場合、方針の改正にあたりまして、FIPS140-2 レベル 3 相当以上を要求するにあたり、欠かせない重要な要求事項は何か、例えば物理的セキュリティ、暗号鍵管理につきましては一定の変更が確認できますが、この変更をどの程度取り込むべきか、またその他の攻撃の軽減に相当すべき基準を新たに求めるべきなのか、それ以外に要求すべき事項がないかについてご議論いただきたいと考えております。よろしくお願い

いたします。

（松本座長）
質疑に入りますけれども、ご発言したい方はチャット欄でお願いいたします。
漆嶌委員お願いします。

（漆嶌委員）
レベルについては引き続きレベル 3 以上ということで、まずいいと思います。で、次のブレッド 2 個目ですけれども、ここの中でなにか個別に物理的セキュリティ、暗号鍵管理等、また他の攻撃の軽減等、個別に何か確認等をしようとしているように見えるのですが、これを私は必要ないと思っており、すでに FIPS の認定製品であれば、これらの事項はすでに確認済みであるとして、追加の確認はしなくていいのだろうと思っています。また、あえて追加で確認をすることがあるとするならば、製品の認定取得後に脆弱性などが発見されることがあり、製品の仕様上、脆弱性がそのまま放置というより、脆弱のままになっていない、そういったような利用になっていないかっていうことを確認するだけでよく、個別の先ほどの表にあったような詳細な項目について、認定調査で確認する必要はないと考えています。私からは以上です。

（松本座長）
ここに関しては、それほど皆さん意見は違わないのではないかと思うのですが、そもそも FIPS140-3 は私自身もよく知らず、採用することによって運用が変わる等、そういうのはあるのでしょうか。ほぼないのでしょうけれど、互換でしていると思うのですけれど、満塩さんどうぞ。

（満塩委員）
少し論点は今の松本さんの話とは少しずれますが、以前にもお伝えしたことですけれども、指定調査機関の皆さんに伺うと結局は FIPS140-2 なり、3 なりの証書で確認していますと、電子署名法は書かなかった過去があるため、そういう書き方にはできないのですか。漆嶌さんと同じで、別に一項目ごとに指定調査機関が確認するわけではないので、トータルで書けないのかと思っていますけれど、そこは少し法律上の記述のテクニック的な話もあると思いますが、私はそのような意見です。以上です。

（松本座長）
もともと日本の認定を取っていない HSM も使えるという考慮がだいぶあったというようなとこからそれは来ておりますか、漆嶌さん私の質問にお答えください。

（漆嶌委員）
FIPS140-2、3 とで、どう違うかという話ですけれども、運用上、特に何か変わるということはないと思います。FIPS140-3 になってから比較的とコモンクライテリアとの整合性のようなものが達成

されるようになってきており、脆弱性対応等、そういったことが盛り込まれているだけのため、運用上どうかというのは、特にそんなに大きな違いはないと思います。よろしくお願いします。

（松本座長）
製品としてのセキュリティは上がってきたという話でしたが、想定する運用は同じだというようなところですか、よくわかります。宮内委員よろしくお願いします。

（宮内委員）
少し違うまた違う話をして申し訳ないのですが、問題は FIPS を 140-2、3 のレベル 3 を取っていれば全然問題ないのですが、それ相当というところが恐らくポイントです。したがって、相当であるかどうかを確認するという作業をどのように JIPDEC にしてもらうかということで、どちらかというと相当というのをやめてしまった方が一番簡単であると思うのですけれども、皆さんはどう思われますか。今となってはもう相当をやめてしまうと、実は方針には装置ではなくても部屋で全体として安全保たれる場合もよいと書かれてありますが、それについてはどうするのかということを、実は少し考えなければといけないと思い始めまして、ご意見いただければと思います。以上です。

（松本座長）
認証事業者は実質認定製品しか使ってないと私は認識しているのですが、小田嶋委員お願いします。

（小田嶋委員）
個別の皆さん、認定認証事業者が何を使っているのかは、私はわからないため、この相当が取られるところで影響がある認証事業者がもしあるとすると、少し慎重に扱わなければならないと思っています。ただ、現行のセキュリティを考えると、基本的には相当が取られるというところは、やむを得ないだろうと認識しています。また、先ほど漆嶌さんがおっしゃったとおりだと思っておりますが、もし事務局で確認していればですけれども、FIPS140-3 で、その他の攻撃への対処で現在試験要件が整備されていないような攻撃の対象技術の仕様と書いてありますが、これは具体的にどのようなものを指すのか、もしわかればと思っています。我々がまだそこまで対応していないからですが、NIST の SP 800-140F が対象ではと思っているのですが、私たちも読み切れていないので、もし事務局の方で調べられたら、ありがたいと思っています。質問の意図はそれだけです。以上です。

（松本座長）
漆嶌委員がコメントです。相当なし、大賛成ですとなっていますけれども、いわゆる相当でこう一番困るのは調査をしている JIPDEC さんではないかと思います。特に FIPS140-3 になった時に相当と言われたらさらに困るのではないかと思うのですが、皆さんいかがでしょうか。今の認証局がどうされているのかというのは、一度触る必要があるかもしれません。

（満塩委員）
今、各社が相当を使っていないかどうかというのは、少し私もよくわかっていないので、最終的にそこは確認だと思いますけれど、多分、今の認定認証業務の人たちは殆ど FIPS を使っていると思われるため、そうすると相当なしでいいと思います。一方、ここの最後の問題は産業育成的な観点です。その観点で本来であれば上位のルールでは相当にしといて、下の方では現状今これはこれでしかないため、追加の場合は別途検討することにならないかと少しテクニカルに逃げられないかなと思っています。法律上で全部相当なしにしてしまうと、少し産業育成的なところがなくなるような気がしており、少し気にはしています。そこは法律の規則の書き方になりそうな気がしていいますが。そのような意見です。

（松本座長）
FIPS140 で、例えば国産暗号も含めようとすると、FIPS モード外さなければいけない等、そういうことはあります。漆嶌委員、相当についてコメントお願いいたします。

（漆嶌委員）
相当の製品を認めることの弊害もあるのではないかと思っています。例えば FIPS 製品の調査認定等は、HSM の専門家が見てこれは準拠しているかどうかといった判断を下せます。それが、例えば JIPDEC は多分 HSM の専門家ではないと思っているため、FIPS の基準に照らしてどうかっていったようなことをきちんと判断するのがまず難しいと思っているのと、新しい FIPS の規定では、5 年おきに製品の認定更新っていうのが義務付けられているため、5 年過ぎた後、どうこうといったような話を相当なしの時にはどのように判断するのかということも、また考えなければいけないと思います。そういった意味で割と JIPDEC さんの方で調査をするのは HSM 製品については難しいだろうと思っており、相当という基準はきちんと専門機関にお任せをするというのがいいのではないかと思っています。

（松本座長）
本当はそうですが、専門機関で本当は期待できる JCMP の暗号モジュールの評価制度もやめてしまったので、日本に専門的にそれをできる機関があるのかという問題は恐らく別途あります。体制としては、相当はなしと書いていいのかというのは、先ほど産業育成力というのはありましたけど、そもそもこれから先、HSM は非常に重要なので、そこも配慮しなければいけないと思いました。
JIPDEC 的にはやはり相当っていうのは相当困りますよね。

（JIPDEC 大澤様）
相当困ります。

（松本座長）
原則相当なしで、例外を何らかの形で認める等、そういったことかもしれません。

（宮内委員）

今、松本さんがおっしゃったとおりで原則は相当なしにしておいて、どうにかして別途定めるものをただしというのが多分定石ですが、実は決めているのが方針なので、方針でそのようなことを言えるのかと、これは事務局の方で考えていただきたいのですけれども、これが例えば施行規則ということで書いてあれば、別途大臣が決めるもの等というのはいいですが、方針の中でどうできるのかというのは少し検討していただきたいと思います。私からは以上です。

（松本座長）

だいたい意見としては出揃ったのではないかと思いますけれども、事務局いかがでしょうか。

（事務局 北井上）

事務局でございます。ご議論いただきまして、ありがとうございました。おっしゃるとおり HSM の中で FIPS140-2 は、そもそも認定取得している製品を使うであろうというものがほとんどであろうというところで、ご議論いただいたと考えてございます。

その上で、ただ、というところで申し上げると、我々の方で定めるような規則なのか方針なのかというのは諸議論あると思いますけれども、そういったところに「FIPS の認定を受けていること」のような内容で基準を書けるかというと、前回第 1 回にもご議論いただいたとおりですけれども、なかなか苦しい部分もありまして、したがって今のとおり、必要な部分の要件だけをピックアップして書き下しているというのが現行の方針という理解でおります。そうなった時に、今回も恐らく同様の整理になるのではないかというところを考えると、方針で FIPS140-2 の製品を使うことのようなことが書けるかというと、法技術的な話でやや疑問が残る部分でもあるのではないかと思っております。そういった時に、140-2 であるというところを方針にどう表せばよいかというところがやや疑問としてまだ残っていまして、実態として確認するのは、これまでのご議論のとおり、FIPS140-2 をとっている製品を使うこと、JIPDEC さんを含め、指定調査機関にご確認いただくということだと思うのですけれども、それをご確認いただく前の基準としてどういった中身を書いていれば良いのかというところ、140-1 から 140-2 への違いを、方針の中でどう表せばいいのかというところが、我々事務局として今苦しんでいるところでありまして、そういった点でもしお知恵をいただけるようであれば、ありがたいと思いました。ひとまず事務局から以上でございます。

（松本座長）

結局、FIPS140-1 で 20 年間放棄されたというと少し語弊がありますけれど、そのあたりがよくどうしていいのかわからないため、ある意味ではそのままになっているという側面も恐らくあります。本来ならば日本の JCMVP のようなところが機能していき、そこが基準に定めてそれを参照するとなればよかったですが、そうはならなかったような感じです。これからも更新されるため、それにどうやって追従していくのか、追従する仕組みをどうやって法律に反映させるかというような難しい問題に当たっているような気がしますが、認証局的には少し繰り返しますけど、相当なしでそのまま単純に行くのが一番嬉しいで

す。JIPDEC さんのような指定調査機関も、それに対して日本で作った基準ではない問題が浮上してしまったという感じです。

（小田嶋委員）
調査表 1410 番台の箇所の表現のため、事務局がおっしゃったとおり、直接記載できないというのはそのとおりだろうと思っています。どちらかというと適合例の回答として、認証局は FIPS のいくつを使っていますという表現で確認してもらって調査していただいているという状態のため、一旦、どのようにするのかは結論が出ないと思うため、少し工夫していただくしかないかなと思っています。実態としては先ほどの 140-2 以上ですというところはもうやむを得ない状況だと思っています。

（松本座長）
だいたい意見としては出揃ったかと思いますけども、どう記述するのかということに関しては、結論が出てないかもしれませんけど、よろしいでしょうか。

(JIPDEC 大澤様)
一言で申し上げるとすると、やはり調査し、あるいは確認しやすい記述で、方針に反映いただきたいというところは切にお願いしたいです。したがって、相当ということはやはりなしに、いろいろ明確に判断ができる書き方をしていただきたいと思います。

（松本座長）
結局、FIPS140-2 を前提に運用も決まっているため、本当はそこが運用等、ファシリティ等でカバーできることがあるとしても、レパートリーが多くなりすぎると、実質的に難しいということです。FIPS140-2 というのは明確に製品で要求のスペックが決まっているため、運用もできる、あるいは決まるというのがあるため、ここは相当になると、そこがまたばらけるため、実質的に調査は難しいというような気もしました。実質的には相当なしが一番平和である一方で、これから色々なところで HSM を使われるため、そのようなところも日本の産業として育てていかなければという側面は恐らくあると思いました。

（満塩委員）
事務局は書けないということなので、単なる質問ですが、これは ISO では書けないのでしょうか。

（松本座長）
ISO でも、互換性がある方向ではあったのですけどね。3 の場合は。2 はないです。

（満塩委員）
難しいですか。

（事務局 北井上）

事務局です。まず 140-2 のレベル 3 というところは、特段大きな異論がなかったところかなと思っておりまして、その上で、相当のようなところと、確認の運用自体というところはさておき、基準としてどう書いていくかというところは、少し我々の方でも引き続き考えたいと思いますので差し支えなければ、またお知恵いただければと思います。追加のご意見等がないようであれば、次の論点に進めたいと考えております。以上です。

（松本座長）
⑥について、事務局からご説明お願いいたします。

（事務局 山之上）
事務局でございます。方向性⑥に関しまして第 2 回検討会においては、公的個人認証法と電子署名法の基準を統一した方がいいが、マイナンバーカードとの仕様の差異については考慮を要する。また、利用者の意思表示や失効していない有効な電子証明書の確認がアプリケーションのログやデータベースによって証明される形となるため、それらを正確に確認する方法の模索が必要との議論がございました。
第 2 回検討会を受け、本検討会においては追加で議論いただきたい内容としまして、モタナイズを行う場合、電子署名法の特定認証業務の認定にあたり、確認すべき事項はどこかについて議論いただきたいと考えております。
前回の検討会において少し説明させていただきましたが、そもそも鍵ペアを利用者が自ら作成する場合、利用申し込み時に紙の申込書や住民票、印鑑登録証明書の送付と合わせて利用者署名検証符号を電気通信回線を通じて認定事業者に送信するとしても、認定事業者が当該利用者を識別できなければ電子証明書を作成することができないことから、平成 15 年 6 月に施行規則第 6 条第 3 号の次に第 3 号の 2 を加える形で改正され、審議確認を行った後、認定事業者が利用者識別符号を作成し利用者へ送信。当該利用者が利用者署名検証符号を送信する際に合わせて、当該識別符号と利用者情報を送信することで、認定事業者は当該利用者を識別、電子証明書を発送する方式が認められるようになりました。その後、平成 16 年 4 月に公的個人認証サービスで発行された電子証明書に係る電子署名による利用者の真偽確認を行う方法を新たに施行規則第 5 条第 1 項第 2 号のとおり追加され、電子のみで申し込みや本人の真偽確認、当該利用者の識別等も可能であるにもかかわらず、現在も利用者識別符号の送受により、利用者の識別を要する形となっており、利用者及び認定事業者の双方に負担をしている形になっております。
前回の第 2 回検討会におきましては、公的個人認証法で認められている方法を電子署名法においても認める方法で検討するべきとする一方、利用者が電子証明書の利用申し込みと同時に利用者署名検証符号を送付した場合、発行申請書と利用者署名検証符号の紐付けや改ざん防止等の措置の取り扱いについて、あらかじめ整理する必要があるとの意見があり、伴って認定事業者は上記意見に対してどのような方法により何を確認する必要があるのか、また、指定調査機関はどのような方法により調査するべきなのかについて整備する必要があるかを議論いただく必要があると思われます。
以上より、方向性⑥につきましては、3 点についてご議論いただきたいと考えております。1 点目は電子証明書の発行申請と利用者署名検証符号を一度に送付するとした場合、発行申請書と利用者署名検証符号の関連付けや改ざん防止等の措置について、どのように担保されている必要があるか。2 点目は認定基

準の統一に伴い、申し込みに付される電子署名についてどのような基準を設ける必要があるか。また、他に認定基準として設ける事項はないか。3 点目は電子署名法の認定に関わる調査を実施する際に確認するべき事項は何か。また、どのような方法があるかの 3 点です。事務局からの説明は以上となります。よろしくお願いいたします。

（松本座長）
利用者の環境の話があるため、そこは割と難しいです。一方で、公的個人認証サービス、マイナンバーカードの普及はもうほぼ全国民に行き渡っているようなところがあり、それを生かすと今までのやり方は非常にあまり合理的ではないという問題も含めて、議論はあると思いますけど、皆さん、同じく意見のある方はチャットでお願いいたします。宮内委員よろしくお願いします。

（宮内委員）
電子署名についての基準を設ける必要があるとは思いますけれども、基本的には JPKI 又は認定認証業務の現在生きているもので、きちんと証明書に住所等が書かれているものということでしょうか。証明書にそれは恐らく誰も反対しない、初めからするつもりでいると思っています。少しわからないのが、改ざん防止といっても、署名をするのですよね。発行申請書と利用者署名検証符号を一纏めにして、何かしらフォーマットで一纏めにして、それに署名すれば、改ざん防止も関連付けもできると思いますが、それほど難しいことをやろうとしているわけではないと思っています。また、27 ページの真ん中辺の矢のマークの 2 つ目、1 つ目は改ざんされていないことについて、それはきちんとした証明がされているのだったらいいのではないかということです。2 つ目は本人と言えるのかということについては、すでに施行規則 5 条の 1 項 2 号等で、JPKI の署名で出来る方法ですので、本人確認するということが書かれているのは、今さらのような気がします。これを言えるのが前提のもとで施行規則 5 条 1 項 2 号は作られていると考えていますので、ここはそんな心配いらないと思っています。私からは以上です。

（松本座長）
今回のことというよりは元々署名者の環境は何も定義していないため、今のやり方でも同じだというところに近いです。実際、JPKI 署名を証明書で行っているので、それが改ざん防止になっているという話だと思いますが、いかがでしょうか。今と同じレベルという意味においては、何も問題がないような気がします。

（満塩委員）
そのような意味では、2000 年の時は、それこそスマホを使うということをあまり想定していなかったルールだったと思っていますと。今回 JPKI 等もこのやり方は殆どスマホ等を使うことを想定しつつあると思いますが、若干色々細かい議論をしていくと、いろいろ複雑な脅威を考えなくてはいけないです。

（松本座長）
脅威自体はあると思います。

（満塩委員）
ある程度はあると思います。私もそれは否定していません。ただし同等レベルというか、そういう意味で行くと、今のところ同じにしてもいいのではないかと思っています。それで、そういう意味では引き続き JPKI も含めてだと思いますけれども、どういう脅威があるかというのを注意、ウォッチしていくことが当然必要だと思いますけれど、今は同等なところでの使い方、いわゆるスマホのレベルも含めて、そういうことにあるのではないか、同等でいけるというようなレベルなのではないかと思っています。以上です。

（松本座長）
この話よりももっと根深い、欧州との比較で言うと、欧州で言っている QSCD が日本には何も定義されなかったということもあり、そこは署名法の範囲外になっているので、利用者が鍵ペアを作る環境含めての問題なので、元々リスクがあるところでもあったわけです。それに対して、この新たなものが同等ではあるということです。調査できるかという問題は皆さんいかがでしょうか。同じでしょうか。認証業務側からするとできることは恐らく同じでしょうか。小田嶋さん、このあたりは、認証局会議等では議論ないですか。

（小田嶋委員）
利用者の秘密鍵と公開鍵を自身で作るパターンは多くないです。どちらかというと CA が作って、それを安全に送り届けるというところですので、あまり目立った議論というわけではないです。

（松本座長）
ただ、スマホを相手にすると今後出てくるというのもありそうです。結局今、世の中の動きとしては、スマホに入れるという方向に向いているため、スマホ向けに証明書を発行するという話は、こういったやり方を取られる可能性があるけれども、本当はこの時にスマホの中のセキュリティモジュールで鍵ペアを生成した等、本当はそういうのを恐らく検討されるべきです。

（小田嶋委員）
先程、宮内先生がおっしゃったとおりだと思っており、鍵ペアを作ってそれをマイナンバーカードの電子証明書で電子署名をして、それをすべて関連付けておけば現行認められている方法だと思っているので、それでいいと思っています。したがって、先ほど満塩さんがおっしゃっていた、どのようなリスクがあるのかというところは、世の中の動きというものも含めてですけれども、継続して確認しなればとは思いました。

（JIPDEC 大澤様）
指定調査機関 大澤ですけれども、宮内先生がおっしゃったことというのは全くそのとおりで、同意しますということですけれども、事務局からの資料でこうお願いした点で、私の方からフォローさせていた

だくとすると、OCSP で JPKI の証明書を確認した証跡について、情報の保管という観点から、認定認証事業者はどこまで保存をしておく必要があるか等、私たち指定調査機関はどこまでそれを見なければいけないのかという点で、OCSP のレスポンス結果をどのように保存しなければいけないのかという要件というのは今調査表上と言いますか、方針の中というか、どこにも書かれていない。ただ、そこに踏み込むとなると、また少し新しい議論というよりか、違う観点でこの議論を詰めていっていただかないといけないのでは、そこが新たな課題として今回は整理いただこうかなという気がいたしました。

（松本座長）
証跡としてどのように扱うか、今までやっていなかったのでというところですね、よくわかります。

（小田嶋委員）
小田嶋ですけれども、帳簿書類の保管になると思っていましたので、署名した時とそれを CA の方で受けた時に必ず署名検証をして、署名検証の結果をエビデンスとして保管するのであれば、それこそ有効期限の 10 年保管の対象であると思いましたけれど、そういう認識の範疇でよいでしょうか、大澤さんのおっしゃっていたところの署名検証結果というのは。

（JIPDEC 大澤様）
そうですね、もちろん最終的には 10 年保存ということではあると思いますけれども、認定認証業務の証明書で電子署名された時の検証の結果というのは一定程度事例があり、実際に調査の中でも確認させていただいているという事実があります。ただし、JPKI の証明書を検証した時の結果について、何を事業者さんとして残さなければいけなくて、我々として証跡の具体的に何を残しておかなければいけないかというところで、煮詰まり切れていないところがあるのだろうと思っていますというところです。

（小田嶋委員）
わかりました。理解しました。

（松本座長）
このとおりに行こうとしても、調査の関係でまだ調べきれていないことがあると認識しました。

方向性としては JPKI をそのまま電子署名法の施行規則に入れるという方向で検討するようですが、調査である等、そういったところではまだ検討しなければいけない点があると認識しました。次の論点③に関して、事務局の方からご説明お願いいたします。

（事務局 當波）
事務局でございます。こちらの 30 ページと 31 ページの方には、前回の検討会においても、利用した資料の方を再掲させていただいております。こちらの③の論点のところにつきましては、クラウド HSM の利用に関する点でございまして、前回ご意見をいただいたところといたしましては、クラウド HSM の利

用、これは CSP であったり、HSM ベンダーが提供するパブリッククラウドにおけるクラウド HSM サービスの利用についてはまだ認定の範囲内とすることは、難しいのではないかというご議論いただいたと認識しております。ただし、プライベートクラウドに設置された HSM の利用であるなど、それから、ネットワーク型の HSM の利用に関しては、例えば指定調査機関である等、我々主務省庁、主務大臣による立ち入りとの調査が可能であるということで、一部対象とする論点がある可能性がありますという、ご議論をいただいたとも、認識しております。

今回におきましては、こちらのプライベートクラウドに設置された HSM の利用とネットワーク型 HSM の利用のこの 2 点に関して、スコープを絞って、これらを認められるか否かと、また認める場合にどのような基準が必要であるかというところについて、引き続きご議論をいただきたいと考えております。こちらの 34 ページの方に、前回の第 2 回検討会におきまして、この論点③に関していただいたご意見の方を並べさせていただいております。今回少しお時間もありませんので、こちらのコメントの修正点のようなところ、認識違いのようなところがあれば、後でコメントをいただければと考えております。

こちらのページの太字にしている点につきましては、今回のプライベートクラウドに伝えたい HSM の利用、ネットワーク型 HSM の利用に関する議論においても、留意が必要な点と認識しております。今回はこちらのポツで記載していた点、こちらの 35 ページの方にも抜粋、再掲させていただいておりますが、前回いただいたご意見も優位しながら、このプライベートクラウドに設置された HSM/ネットワーク型 HSM に範囲を限定してご議論いただきたいと考えております。以上であります。

（松本座長）

議論するのは結構難しいです。前回もネット HSM とクラウド HSM は違うのかというような話がありましたけど、漆嶌委員よろしくお願いします。

（漆嶌委員）

表のところで、プライベートクラウドに設置された HSM とネットワーク型 HSM を一括りにしているのですけれども、これは少し何か乱暴なような気がしました。例えば、ネットワーク型 HSM を認証設備室内で利用するケースも多分あると思います。例えば認証設備室外からネットワーク HSM を利用操作するようなケースもあると思いますので、その辺はきちんと分けて整理等をしないといけないと思いました。

認証設備室外から保守用 PC を通じて HSM 操作をするといったような可能性がある場合に、保守用 PC の利用環境についてきちんと確認をする必要があると思っています。保守用 PC を利用する環境に、例えば IC カードによってきちんと入退管理をしますか等、覗き込み防止ができないか等、不正操作防止のものがある等、更に、操作記録を取れている等、そのような一連の確認は必要だと思っており、認証設備室内であればそのような変なことは起きないと思うのですけれど、例えばリモートで自宅から保守しますといったようなケースがあると、やはり、例えば入退の記録等取れるわけがないので、そのようなこともいろいろ考慮しながらやる必要があるのではと思いました。私からは以上です。

（松本座長）

難しい、これはネット HSM 単体の話じゃないですから、ネット HSM が置かれている環境、さらに言えば通常の証明書発行時の話ではなくて、キーセレモニー、キーバックアップである等、それをどのような環境で行えるかの話です。

論点③について他にご意見ないでしょうか。確かに、ネット HSM のクラウド事業者、プライベートクラウド、これは同一事業者をどちらにしてもイメージしているのでしょう。

（事務局 當波）

漆嶌委員からの意見について、事務局からコメントさせていただければと思います。

ネットワーク型 HSM であるとしても、この認証設備室内から使うのか、認証設備室外から操作を行うのか、また保守用の場合はどうなのだというようなところのご意見をいただきましたが、大変申し訳ございませんが、まだ事務局の方ではそこも踏まえた整理まではできておりません。ただ事務局のこちらの姿勢と考え方といたしましては、事業者からの需要が高い点、電子署名法以外の認定基準で、すでに認められているのに電子署名法のこの基準では認められていないというような乖離がある点については、早期に対応を行えればということを考えておりまして、こちらの先ほどの、設備室内・設備室外保守用というところに関わらず、今の一般的な認証局の運営の形態におきまして、特に需要が高い点、このような使われ方をされているという点がありましたら、まずそこのニーズのようなところについて、コメントをいただければと考えております。

また、保守用のところにつきましては、こちらの論点③だけではなく、論点④のところでの若干ご議論いただいていくところと考えておりまして、保守用というところについては、HSM にも LAN のポートが保守用のポートが開いていて、そちらについては外に出してもいいのではないかといったところの整理は必要とは考えておりますので、こちらの論点③と④の混ぜ方がと大変なところもございますが、一旦最初のニーズのところについてコメントいただければと考えております。

（JIPDEC 大澤様）

漆嶌さんからも賛同いただけたようなのですけれども、漆嶌さんがご心配されていることを明確にするためには、スライド 47 に適切な整理されいただいている表がございますので、これらの設備のうち、どこまでであればクラウドの利用、あるいは遠隔操作といったものを認めるのかというのがある上で、こちらの話を進めていくともう少し整理が早いということで少し書かせていただいた次第です。

（松本座長）

元々一番大変というよりは、認証設備室内で検査も含めて監査も含めて、牽制が効く形でやらなければいけない作業のようなものをどのように扱うかだと思うのですけれども、この点よくご存知なのは誰だろう。前回も出ましたけれど、何らかの形で今後クラウド HSM のようなものを利用することも念頭において、そのためにはどのような要件があるのかといったところを議論しなければいけないのですけれど、まだ少しそこまで議論ができるような状況ではないと理解しています。新しい HSM の話だと思いますので、このメンバーだけではそういう意味では、足りないかもしれないです。

（小田嶋委員）
いろいろな選択肢が増えること自体は認証局にとっては、ありがたいことだと思っています。パブリッククラウドまでは容易にはいけないかもしれませんけれども、少なくともパブリックではない、プライベートクラウドもしくはネットワーク HSM は先ほど漆嶌さん、大澤さん等がおっしゃったところの懸念もあるため、そこは分解能を上げていただいた上で整理できればありがたいと思っています。以上です。

（松本座長）
シェアードサービスになればなるほど、ある意味では調査は難しくなる方向に行くと恐らく言えます。

（満塩委員）
これを見ていて今思いましたのは、このプライベートクラウドやネットワーク HSM というレベルだけでは少し判断が効かないような気がしており、漆嶌さんが恐らくその辺をおっしゃったと思うのですけれど、ネットワーク構成でどこで繋がっていて操作するのか等、そういうイメージをもうワンランク落とさないと、そこのあたりのクライテリアが決まってくると思っています。

（松本座長）
漆嶌さんの質問に近いのですけれども、元々ネット HSM ではない HSM の場合、HSM はポートがキーセレモニー等をするような時のポートと、ただ単に署名を打つ時の操作は別ポートだと思いますが、そこがアイソレートされていて、別ポートの操作するときに、認証設備室に入らないとできないというような構造になっていると思います。ネット HSM あたりはどのようにしているのですか。

（漆嶌委員）
そんなには変わらないと思っています。

（松本座長）
このネットワーク図ではその辺りは書ききれていないですよね。

（漆嶌委員）
そうです。だから CA サーバに直結に PCMCIA で繋がっているのか、もしくはイーサーネットの線で繋がっているのか、どちらかの違いです。通常はネット HSM と CA サーバ使うときに変な機器から接続できない場に前段にファイヤウォール等を設けたりします。

（松本座長）
そこが一番高セキュアの話というのは、まさに HSM のアーキテクチャに依存しているところがあり、そこは容易に説明がつかないということです。証明書発行自身は、RA がリモートなので、リモートから HSM で署名の要求は出せるけれど、署名鍵をバックアップする等、鍵更新するというのはできない。鍵更新するときに恐らく人数が揃わないとできないような構造をしていると思います。私もよく知らないけ

れども、似たようなこと行っているDNSSECのルートゾーンの鍵更新があり、昔は権限者が全員現地に赴いて鍵更新したようですが、今はリモートから行っているようです。それによって、全員がいなくてもできる。全員が現地にいなくてもいいようにしているようです。そういう仕組みは、どのようにして行っているのかと思ったりしています。

（漆嶌委員）
例えば、HSMがこの図の中でネットワークに接続されていて、ネットワーク型HSMに操作テンキーのようなものがあり、そこをドングルでさしたり、キーコードを打ったりして、複数人で操作するような感じになります。

（松本座長）
ただ、ホスティングで、この辺りが複雑になるというよりは、シェアードサービスになればなるほど、調査は恐らく難しくなります。

（満塩委員）
先ほどありましたとおり、例えばこのネットワーク図の中ではキーセレモニー等は恐らく変わらないとおっしゃっておりましたので、これに書き入れていないということだと思いますけれど、キーセレモニー等はきちんとしたところで行うのだろうと思っています。そのようなところを少し整理すると、正直あまり変わらないような気がしますが、そこは少し私は見きれていないため、その辺りを整理していただいて、違いが本当にどこなのかということということが明確に見えるように整理が必要だと思っています。以上です。

（松本座長）
鍵の分散バックアップ等の時も、どのように証跡を保つのか等、少しこの図だけでは少し説明は難しいです。これは、どちらかというと通常のオペレーション時の図に近いです。

（小田嶋委員）
確かに松本さんがおっしゃるとおりで、通常の運用のところの図だと思っています。CAの発行者署名符号での例えば鍵更新である等、バックアップというところは出てこないところです。

（松本座長）
実際には一番のセキュリティというのが鍵更新等ですからね。他に論点等はございませんでしょうか。これは、前回も出ていましたが、CAをクラウドで運用するためにどうしたらいいのかという課題を挙げていて、何らかの形でやれることは検討されていると思うのですけれど、それは恐らくHSMもそれ用に作られなければいけない可能性もあるのではないかと気がしています。

（事務局 當波）

この図だけではなくキーセレモニーを行う場合と、この一般の場合、そしてあとこの図についてもHSM から線がただ一本出ているというような図ではなく、保守用である等、鍵の生成の時の線のようなところをきちんと区別して、行うべきなのかなというのを今のご意見を伺ったところで思っているところであります。

事務局といたしましても、この HSM の使用方法というところに関する知見が、委員の皆様よりあるわけではございませんので、実際にどのような運用になっているのかというところの知見はぜひとも皆さんから追加でいただきたく、場合によってはそのようなところのイメージであるようなものを、事務局側にメールなりでご共有いただけると我々の理解も高まりますので、ありがたく思います。ただ、今の検討会のこの公開の場でお話しいただけるところについては、また今後の方針をまとめる上で、そこの参考といたしますので、一旦今日この場で言いたいところについては、引き続きコメントいただければと思います。

（松本座長）

まだ少しプライベートクラウドの HSM を含めて、まだ検討しなければいけないことは多々あるのではないかと思いました。

次の論点④に関して、事務局の方からご説明お願いします。これも少し非常に広い範囲なため、議論が発散してしまうかもしれませんけれども、よろしくお願いします。

（事務局 當波）

事務局でございます。こちらの論点④につきましては、前回こちらの資料を再掲しておりますが、こちらの A、B、C、D、それぞれクラウドに認証局の設備を持っていくというところでした。また、このために遠隔操作というものをどこまで許容するかという論点でございました。

こちらの論点は、今のこの A、B、C、D、と分けさせていただいたところ、また観点をいくつかに分けてご議論をいただいておりまして、そのうち少々議論が進んで整理ができるような点、また、まだ方向性というものを定めるには、早い議論が不足している点というものがございますので、今回はこのニーズが高い、低いというところ、また、議論が進んでいる進んでいないというところを踏まえながら、このような 40 ページのような形での議論の方を進めさせていただきたいと考えております。

具体的には、まずニーズが高い認証局のリポジトリにおける利用に関する整理をご確認いただいた後、ISMAP、ISMS のクラウドの認証での制度等、そういった調査・審査の方法に関する整理に関する、ご確認・補足をいただければと考えております。またその後、お時間がありましたら、認証局の保守運用における利用、また、それ以外の点に関する第 2 回検討会におけるご意見からさらに続きのご議論をいただくというようなことを考えております。

事務局からこちらのリポジトリにおける利用(A)のテーマについてご説明させていただきますので、一旦ここでお返しにさせていただいて、こちらの(A)の 4-1 の件に関する議論が終わった後に、また続きの方をご説明させていただければと考えております。4-1 認証局のリポジトリにおける利用につきましては、前回認証局のこのリポジトリについては、基本的には可用性が求められており、この機密性・完全性に関するリスクは限定的であるというような、方向性でご議論をいただきまして、パブリッククラウドに

おいても、利用においての問題点は少ないのではないかというお話があったところです。こちらの下に確認事項と書かせていただいておりますが、認証局のリポジトリにおいて、パブリッククラウドサービスを使用するという方向性でまとめる上で、この 2 点に関して明確化を行いたいと考えている点でございます。

1 点目につきましては、本当にこの可用性だけを求めているということで ISMAP、ISO の 27017 等、そのようなクラウドサービスのセキュリティの認証に関する制度である等、そのようなところの安全性、安全なクラウドであるというところを求めない形でも本当に問題がないのでしょうかというところの点。2 点目につきましては、これまで認証局の運用業務において、任意でバックアップサーバである等、そのようなところが行われてきたわけでございますが、そこでクラウドにおいて利用をされる場合に冗長性等、可用性の基準を求める必要がないかという 2 点に関して記載させていただいております。あくまでこちらの確認事項につきましては、事務局として確認させていただきたい点でありますので、これ以外の点についても、この認証局のリポジトリにおける利用というところは、認める上で追加議論すべき点がございましたら、それについて別途コメントいただければと思います。以上でございます。

（松本座長）

これに関しては少しニーズも高く、リスクも限定的なため、今日なるべく結論に近いところでいきたいなと思います。小田嶋委員コメントお願いいたします。

（小田嶋委員）

まず、優先順位としては、やはり(A)が一番高いというところは、各認証事業者の意見を得たところでのトップでした。可用性に関しては、クラウドを使うということが、そもそもそういう意図だと思っていますので、そこに関しても特に異論はないです。確認事項のところで、パブリッククラウドサービスについても ISMAP 等、ISO27017 まで求めなくてもいいのではないかと思っています。リポジトリとしてはそこまで求められていないと思っています。一方で、署名検証に必要な情報をリポジトリに載せていますので認証局としては、リポジトリの重要性は十分認識しているところだと思っています。以上です。

（松本座長）

他にいかがでしょうか。漆嶌委員よろしくお願いします。

（漆嶌委員）

ISMAP 等、そのようなセキュリティ認証が必要ないというのは、私もいいと思うのですけれども、その時に、例えば機密性の高いログである等、そのような情報に対して、例えば暗号化の措置をとっている等、何かしらのセキュリティ対策は別途必要だと思います。そこは、やはり調査の中で確認をされた方がいいのではないかと少し思いました。よろしくお願いします。

（松本座長）

満塩委員よろしくお願いします。

（満塩委員）

これは、A のところでよろしいのでしょうか。要は今の漆嶌さんのログが入らないという認識で、大丈夫でしょうか。以前にもコメントしておりますので、2 回目になるかもしれませんけれど、ご承知のとおり NISC の統一基準の中でも機密性がないところに関しては、ISMAP の管理基準は求めないということでいいと思うので、そのような意味ではそうした方が私もいいと思っています。

2 個目のものは、確かに冗長性・可用性というのは求めた方がいいですが、私の理解だとクラウドベンダーさんは恐らく可用性に関しては SLA 設定をしていないため、クラウドでも冗長性は、実はそれこそアベイラビリティゾーン、リージョン、複数の異なるクラウドを使う等、レベル感はかなりいろいろあるので、そこはそんなに難しいことを要求するつもりは全くないですけれど、少なくともアベイラビリティゾーンを 2 つ作ること等、その辺の普通のことをしてほしいというレベルで、何かしら書いてもいいのではと少し思いました。以上でございます。

（松本座長）

認証事業者にとっては、リポジトリは本当にアベイラビリティが一番重要なので、そこをコストの兼ね合いでいかに合理的に実現できるかという観点で、アベイラビリティを求めるというのは、普通なのでないかと思いましたけども、他にご意見はないでしょうか。

（事務局 當波）

事務局でございます。一点目のとこのセキュリティクラウドサービスのセキュリティの認証制度に関しては、求めなくても良いという方向性で今ご議論いただいているところかと思いますが、こちらのところが、現行の基準で、明文で求めておらずともこれまでと一般的な認証局において実施されてきた措置というものがあると考えております。そのような点が、主要な CSP を利用いただく分には相当程度安全であるということであるかと思いますが、そのような基準がない場合に、凄く低レベルのサービスを利用されてしまうという場合もあると考えておりまして、そのような際のリスクというものがあるのかというところは、再度少しコメントをいただき、事務局としてはその点に関して安心をしてから基準と方向性を定めたいと考えております。もう少しここの点について、ご議論いただければと思います。

（松本座長）

これはいかがでしょう。満塩さんどうぞ。

（満塩委員）

まさにおっしゃるとおりで、1 個目で全く求めていないというよりか、セキュリティは CIA ですので、そのような意味では(A)は求めてくださいということなのです。それは、イコール ISMAP ではないです。そのような意味では私も 2 個目のものは小さく書いてありましたが、レベル感としては、最低限アベイラビリティゾーンの複数個を想定するということ当然だと思いますので、そのレベルかどうかというのはありますけれど、そこのあたりの(A)はやはり求めてくださいというのが私の意見です。以上です。

（松本座長）
これは認証事業者の立場からは、先ほど小田嶋委員の方からありましたけれども、恐らく認証事業者からすれば、既存のクラウドサービスを使用した方がアベイラビティは上がると考えていると思います。自分たちで 365 日、全く止めないシステムを作るというよりは、シェアードサービスなので、基本的にはクラウドの方がアベイラビリティは保ちやすいと考えているため、今より悪くなるというと少し語弊がありますけれども、そのような考えで(A)のニーズが高いと理解しておりますけれど、よろしいでしょうか。

（小田嶋委員）
松本さんのおっしゃるとおりでして、オンプレよりも可用性という意味ではクラウドの方が高いと思っていますので、先ほど品質の悪いものを選ぶ可能性もある等という話もありましたけど、それでしたら意味がないので、そのようなことはないと思っています。

（松本座長）
認証事業者の立場からすると、先ほどの認証局の運用のためのファシリティ等、機密性であるというのは、一般論としてクラウドよりは上で、逆に言えば可用性の部分に関してはやはりクラウドの方が上で、それをうまく組み合わせてサービスができるべきというのは恐らくここの背景にあると思います。

（小田嶋委員）
おっしゃるとおりです。少なくとも署名検証の情報に関しては、とても重要だと思っています。さらに言うと、政府認証基盤にも繋がっていれば、責任もあると思っています。

（松本座長）
わかりました。ここに関しては、特に議論の余地はないかと思いましたけれど、それをどのように文面に落とし込む等、そのようなことはまだあると思いますけども、方向性が殆ど一致していると思いました。よろしいでしょうか。

（JIPDEC 大澤様）
調査する立場から 1 点だけよろしいでしょうか。見識がなくて申し訳ないのですが、アベイラビリティゾーンを複数取るとお伝えしたことについては、何をもって確認すればいいのですか。アマゾンウェブサービスであれば、そのようなことは、仕様等に書いてあるということなのか、そういうことでよろしいですか。

（漆嶌委員）
仕様では恐らくわからないため、認証事業者さんがアベイラビリティゾーンをどこ使っているといったようなシステムの設計の資料を基に確認をすることになると思います。

（小田嶋委員）
まだ使っているわけではないため、確かなことは言えませんが、今、漆嶌さんがおっしゃったとおりだと思っています。

（満塩委員）
だから設定画面見せてくださいっていうことレベルと思っています。その以前のレベルには設計書があるとは思いますが。最終的にはそこから先はクラウドを信じることにはなるわけですけれど、設定画面があればそこでいいと理解しています。以上です。

（宮内委員）
宮内ですけれども、皆さんのおっしゃるとおりだと概ね思いますが、それは AWS ならばそうですが、宮内が個人的に運用しているクラウド等であれば大丈夫ですかと、そのようなことは心配しなくても大丈夫なのでしょうか。

（満塩委員）
逆に、全くそれが確認できないようなことは恐らくないと思います。コマンドラインでもいいですし、特に設定画面のような GUI の綺麗なものではなくてもいいのですけれども、何かしら見えないと、それは実際にも設定もできない。

（宮内委員）
あるということは必要条件だと思いますが、それで十分条件だと思っていいのでしょうかということを言っています。設定画面があるからとはいえ、そのとおりに宮内の運用しているものがどのようになっているかどうかはわからないのでないでしょうか。

（満塩委員）
おっしゃるとおりで、設定画面の裏側で本当に設定されるかどうかっていうのは、クラウドを信じることになります。

（宮内委員）
信じることもいいのですけれども、いかがなものかと思いまして質問しました。

（満塩委員）
大事な話だと思っております。難しいです。

（JIPDEC 大澤様）
難しいしわ寄せがこちらに来るのは非常に厳しいです。

（満塩委員）
それは重々承知しております。少し考えますが、一旦誰かお願いします。

（JIPDEC 大澤様）
知見のある方から、アベイラビリティゾーンを複数取るといったような、最低限確認しなければいけない要件というものがあるのだとすると、このようなやり方で確認ができるので、このようなことが条件であればいいだろうというような具体的な情報をいただけましたら、この場でも検討が深まると思いました。よろしくお願いします。

（松本座長）
実際設計すると、それはもう少し見えてくると思います。

（満塩委員）
アベイラビリティゾーンを複数設けなければいけないといったような要求事項を、現時点で存在していないと思っており、そうすると、アベイラビリティゾーンを複数使っていますといったことを確認する必要もないと思います。システム設計図上で複数使用しているというのを見れば、それ以上の確認は必要ないと思います。

（松本座長）
ここで議論するのは、少し辛いです。そういう選択を取るだけの話だと思います。

（事務局 當波）
宮内先生からいただいた自分のクラウドでも大丈夫なのかというところは、そもそものクラウドサービスという言葉の定義が定まっていないというところに問題があるのではないかなということを考えているところでありますが、一般的なクラウドサービスプロバイダの利用を想定してもご議論いただいているかと思うのですが、一般的ではないクラウドサービスを持ち込まれたときに、どのようにするべきか、それを適正でないとはじくべきなのか、はじくための基準はどのようなものであるのかというところは、もう少々コメントいただければということを考えておりますが、いかがでしょうか。
お時間がありませんので、残りの論点に関しては、後ほどメールを送付いただくなり、個別に事務局からヒアリングというような形でこの後答えをさせていただこうと思いますので、一旦この残りの論点については本日の議論はなしということにさせていただきまして、事務局から再度ご連絡いたしますので、それをお待ちいただければと思います。こちらについてだけについて、ある程度綺麗に終わらせてから今日は終わらせていただきたいと思います。

（松本座長）
何らかのアベイラビティがこのように保証されるよってことを言明するのでしょうね

（満塩委員）
松本さんおっしゃるとおりで言明でしかない気はしていて、そこはいくら掘っていっても、最後にITがどうなっているかっていうのは、CCの一番レベル高い世界の話と同様になってしまうので、そこは現実的ではないのでしょう。そうするとやはり言明的な話になっちゃうと、それは誰が言明したかって話にもなるので、それは組織としてのやはりトップマネジメント的なところでの言明をきちんとなんて言いますかねということも含めて、そういう意味では最近の少し認証の仕方っていうのは細かいところ詰めていってもバリエーションが複数作りこみすぎてあまり最終的な答えがない気がしていて、そうするとやはりある程度のバスケットクローズ的なところは最初の話になった経営陣が真面目にやりますってきちんと宣言するところも含めて、そこに帰着しているのではないかなと思っているところです。以上でございます。

（松本座長）
アベイラビリティも突き詰めるとコストとのトレードオフになるので、世の中で一般的にそれなりのやり方で、コストとのトレードオフで着地点が決まると思っています。

（小田嶋委員）
再掲にはなりますけれども、リポジトリ特に署名検証環境に関しては、必要な義務を負っていると思っています。クラウドに持っていくところに関して言えば、少なくとも可用性を求めるために、残念なクラウドを使うつもりは毛頭なくて、基本的には使えるものを用意するというところだと思いますので、先ほど満塩さんおっしゃったとおりで突き詰めていくと、底なし沼だと思っていますので、基本的には認証局が宣言としてこういったことでこういうふうにやっていますというのを確認していただくっていうところで落ち着かせるところかなと思っています。以上です。

（松本座長）
SLAを宣言するのかに近いような話ですね。

（小田嶋委員）
もしSLAを設定しているのであれば、SLAはこのぐらいですっていうことを言うこと自体はできると思いますけど、それを厳密に求めすぎてしまうと、今度本当に泥沼になってしまうので、やめたほうがいいと思います。

（事務局 當波）
ありがとうございます。一旦、本日の議論といたしましては、引き続きこちらの認証局のリポジトリにおける利用については、認められるという方向性、またその中で一定程度の可用性を求めること自体は問題がないのではないかというところであったと意識しております。
そこで、こちらの証跡としてどのような形で主務省庁また指定調査機関が確認するのかというところについては、もう少し詰めなければならない点があるかと思いますが、例えば、先ほど小田嶋委員からもお

話しいただきました自己宣言というようなものや、SLA というようなものや、利用しようとしているクラウドサービスのこれまでの稼働の実績のようなものを、証跡として確認することになるのではないかなということを考えております。この点については、またこちらの基準を具体で詰めていく上で、皆様に引き続きお知恵をいただければと思います。また、今回の報告書、方向性のようなものがまとまった後にもこの詰める作業の中で、皆様にご相談させていただくことがあるかと思いますので、その際はよろしくお願いいたします。最後に、この後のスケジュールについて、事務局からご説明させていただければと思います。

（松本座長）

では、議事 2 ですが、次回開催、今後のスケジュールについて事務局の方からご説明お願いいたします。

（事務局 山之上）

事務局でございます。資料 1 の 52 ページの方より説明させていただきます。本日の検討会の方を踏まえまして、事務局としましては、第 4 回検討会の方を 1 月 17 日の方に設定させていただこうかなというふうに考えております。時間の方は一応午前 10 時から 12 時の方を予定しておりますので、また再度事務局より検討会の資料を送付させていただくというところで考えておりますので、随時ご共有させていただければと思いますので、よろしくお願いいたします。事務局の説明は以上となります。よろしくお願いします。

（松本座長）

はい、特に意義はないと思いますので、本日はここまでにしたいと思います。本日も活発なご議論どうもありがとうございました。それでは本日の電子署名法認定基準モダナイズ第 3 回検討会を閉会とします。どうも皆様ありがとうございました。