第 1 回 電子署名法認定基準のモダナイズ検討会 議事録

日時　　令和 6 年 9 月 20 日(金) 13:00～15:00
場所　　オンライン開催
出席者　開催要領のとおりにつき省略

（事務局 山之上）
それでは、電子署名法認定基準のモダナイズ検討会第 1 回を始めさせていただきます。皆様、本日はお忙しい中お時間いただきありがとうございます。事務局のデジタル庁 山之上と申します。よろしくお願いいたします。早速ではございますが、事務局を代表してデジタル庁 デジタル社会共通機能グループ グループ長 楠よりご挨拶申し上げます。

（事務局 楠）
デジタル庁の楠でございます。委員の皆様におかれましてはお忙しい中本検討会にお集まりいただきましてありがとうございます。電子署名法認定基準のモダナイズ検討会の開催にあたりまして、事務局を代表して一言ご挨拶を申し上げます。

ご承知のように、我が国においてデジタル化に向けて様々なサービスが展開・検討されているところです。その中でも電子署名につきましては、平成 13 年の 4 月に施行された電子署名及び認証業務に関する法律がございます。委員の皆様におかれましては、電子署名法は、電子署名に関しまして、電子的記録の真正な成立の推定、特定認証業務にかかる認定の制度等を定めることによって、国民による電子署名の円滑な利用を確保し、電子商取引をはじめとするネットワークを利用した社会経済活動の一層の促進を図るために制定された法律に関しまして、ご議論いただけるということで、この電子署名法をきっかけにその後、いろいろな法律において電子署名を行う場合の規定が設けられておるところでして、国民生活や企業活動のさまざまな場面に影響を及ぼし得る法令であるというふうに考えています。

しかしながら、この法律に基づく特定認証業務の認定制度に関しまして、その認定基準について法施行当初から大きな改正を行っておりませんので、近年の技術動向やセキュリティに対する考え方の変化等を踏まえてこの基準を見直す必要性が示唆されているところでございます。昨年度も同様に有識者の皆様に多角的な論点から議論をいただいて、短期的に対応しうるものから長期的な検討を要するものまで幅広く論点を抽出いただいたところでございます。今年度におきましては、長期的検討の結果をいたずらに待つのではなくて、可能な部分から順次、モダナイズを進めていくべく、昨年度の議論を踏まえ大きく 6 点についてご議論いただければというふうに考えております。委員の皆様か

ら、ぜひ忌憚ないご意見をいただいて活発なご検討いただければというふうに考えております。今日はどうぞよろしくお願いいたします。

（事務局 山之上）
ありがとうございました。検討会の委員のご紹介につきましては、失礼ながら、開催要領にてご紹介にかえさせていただきます。続きまして、委員の互選により本検討会の座長を決定させていただきたいと思います。事務局といたしましては、松本先生に座長を進めていただきたいと考えておりますが、こちらよろしいでしょうか？

（一同）
異議ありません。

（事務局 山之上）
異議はございませんでしたので、検討会の座長を松本先生にお願いすることとし、以降の議事進行を松本先生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）
はい、松本でございます。ご指名いただき座長を務めさせていただきます。座長を務めさせていただくにあたって、本検討会の意義について述べたいと思いますので、よろしくお願いします。

電子署名法は、平成 13 年に施行しましたが、2000 年以前、電子社会のビジョンが語られていて、そのビジョン実現のために必要な法制度として、電子署名法が制定されたと認識しております。私自身は 2000 年当時、電子署名法の制定自身には殆ど関わっていなかったですが、本検討会のメンバーの方々は 2000 年当時のこともよく覚えておられると思います。2000 年当時は、まだサイバーセキュリティがそれほどまだ注目されておらず、サイバーセキュリティビジネスが立ち上がったところかと思います。そうした中で、我々の多くの諸先輩方々、先人の方々の大変なご苦労で、電子署名法の認定基準を作り上げたと認識しております。
この電子署名法の成立から 20 年以上経っており、世の中が大きく変化したにもかかわらず、電子署名法第 4 条以降の認定制度・認定基準に関してはほとんど議論がされてこなかったというのは、先人の方々の努力を無駄にしてしまうようなところもあって、あまりよろしいことではないのかなと考えたところもあります。

もう一つ、日本の電子署名法は特に第 4 条以降の認定制度には、1999 年の欧州電子署名指令が非常に大きな影響を与え、それを参照したところもあります。ところが、その欧州の電子署名法は、既に大きく改正されています。皆様ご存知の通り 2014 年に eIDAS 規則となり、指令から規則に変わったであるとか、それからもう一つは今年の 5 月に eIDAS2.0 と言われる、2 度目の大きな改正が行われてきました。また、そういった状況対して、日本の電子署名法は、国際的調和も求められているのかなと考えています。現在 2000 年当時の電子社会に変わって、デジタル社会ということがよく言われるわけですが、この電子署名法が日本のデジタル社会の実現に資する電子署名法とすべく、できることや今後考えなきゃいけないことを、この電子署名法認定基準のモダナイズ検討会において、活発な議論を期待しておりますので、皆様よろしくお願いいたします。

では、議事に先立って、資料の確認や議事次第の確認の説明を事務局の方からお願いいたします。

（事務局 山之上）

それでは、事務局より資料確認から順に説明させていただきます。資料は全部で 3 種類ございます。議事次第、開催要領、検討会の方針及びモダナイズの方向性に関する議論になります。本日の資料につきましては、デジタル庁ウェブサイトに掲載しております。傍聴の方はそちらを確認ください。次に議事進行についてですが、こちらウェブサイトに掲載しているので、詳細を割愛させていただきます。現在、3.検討会の進め方についてを説明しているところでございます。

開催要領について資料 1 に沿ってご説明いたします。先程グループ長である楠及び松本座長からご説明ありましたとおり、本検討会は平成 13 年 4 月に電子署名及び認証業務に関する法律が施行され、同法に基づく特定認証業務の認定制度が存在しております。しかしながら、この認定基準につきましては、ほぼ施行当初から大きな改正は行われておらず、近年の技術動向やセキュリティに対する考え方の変化等を踏まえて基準を最新化する必要性が示唆されていることから、認定基準の最新化について検討を行うものです。本検討会における検討の項目としましては全部で 6 項目を予定しており、詳細については後ほど説明させていただきます。また、本検討会には検討会の進行に必要があると認める場合には、委員、事務局以外にも必要な者をオブザーバーとして参加させ、発言・質疑を求めることができます。本検討会および資料につきましては、原則として公開いたします。また、事務局において検討会での皆様の発言を取りまとめた議事録及び議事要旨を委員の皆様の確認を受け作成いたします。ただし、検討会、検討会資料、議事要旨につきましては、企業情報の保護等のため座長が非公開とすることが望ましいと判断し、あらかじめ委員の了承を得た場合につきましてはこの限りではございません。この場合、委員およびオブザーバーにつきましては、本検討会を通じて知りえた企業秘密に関する守秘義務を負うこととなります。なお、この開催要領につきましては、必要に応じて見直しを実施いたします。事務局からの説明は以上となります。

（松本座長）
ありがとうございます。ただいまの事務局の説明にご質問・ご意見ありましたら、ご発言ください。

（一同）
（意見なし）

（松本座長）
それでは、本検討会の進め方については開催要領のとおりとさせていただきます。次に、議事に入ります。時間の都合上、議事 1 から 3 に関して、事務局の説明をまずお願いいたします。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 2 に沿ってご説明いたします。本検討会は、電子署名法及び昨年度実施された検討会の内容を振り返りつつ、検討方針について認識を合わせることを目的としております。第 1 回目となる今回は、①と②について議論を進めさせていただきます。議員の皆様にご議論いただく前に、電子署名法についてご説明させていただきます。電子署名法につきましては、電子署名に関し、電磁的記録の真正の成立の推定、特定認証業務に関する認定の制度、その他必要な事項を定めることにより、電子署名の円滑な利用の確保による情報の電磁的記録の流通及び情報処理の促進を図り、もって国民生活の向上及び国民経済の健全な発展に寄与することを目的に、平成 13 年 4 月に施行されました。主に総則や電子署名の定義、真正性の推定、特定認証業務の認定で構成されております。今回ご議論いただく電子署名法の認定基準についてですが、電子署名法に基づく特定認証業務の認定を受けようとする者が、主務大臣の認定を受けるにあたり設けられている基準でございまして、こちらの記事について委員の皆様にご議論いただくものでございます。記載のとおり政省令等において認定基準や調査方針等の具体を規定しております。

それでは、昨年度事業の振り返りについてご説明させていただきます。認定基準のモダナイズに至った経緯としては、令和 4 年度、指定調査機関である JIPDEC 様において、これまでの認定認証事業者等からの問い合わせ等を踏まえ、現状の運用や最新の技術動向に則していない部分として課題を抽出いただき、昨年度、抽出された課題についてモダナイズの必要性及び方向性をご議論いただきました。11 ページから 13 ページにかけて課題ごとに昨年度までの検討内容を記載しておりますので、課題ごとのポイントについてご説明します。

まず、①国際基準に照らし合わせた情報セキュリティに関するリスクマネジメントの規定についてですが、課題のポイントとして、国際的な基準に照らすと情報セキュリティのリスクマネジメントの

記載が必須となっていることから、昨年度の検討状況としては、法や施行規則にリスクマネジメントについての情報を追加、もしくは法改正を行わずに施行規則または方針にリスクマネジメントの要件を追加する必要があるとの議論がなされたところです。

次に、②認証局の秘密鍵を管理する暗号装置の技術規準の更新についてでございます。課題のポイントとして、暗号装置 HSM に関する技術基準が 20 年以上前の米国の基準である FIPS140-1 の規定と同等のままとなっており、国際的な水準を満たさない状況にあることから、昨年度の検討状況としては方針において FIPS140-2 及び ISO/IEC15408 に言及する規定に置き替える必要がある等の議論がなされたところです。

次に、③国際的な基準を満たしつつクラウドサービスへの拡張等が可能となるようなセキュリティ基準の検討についてでございます。課題のポイントとしては、現行の施行規則や指針において HSM に搭載し、発行者署名符号を持つ、サーバー設備電子証明書を発行する認証業務用設備は、認証設備室内に設置することを要件としておりますが、クラウド HSM であるというだけの理由で不適合となるべきではないため、方針に示される項目（ハードウェアの管理体制等）に対して審査ができればいいのではないかとの、議論がなされたところです。

次に、④認証設備室の外からの遠隔操作やパブリッククラウドサービスの利用の規定についてでございます。課題のポイントとしては、現行の施行規則や指針において電子通信回線経由の遠隔操作やパブリッククラウドサービスの利用によるメンテナンス業務について、基準に適合しないと解釈されているため、パブリッククラウドを許容するような指針について議論いただいたところです。

次に、⑤利用者の真偽の確認における自動化の規定についてございます。課題のポイントとしては、現行の方針では人が利用者の真偽の確認を行うことを前提に、利用者の申し込みに対する諾否を決定した者の氏名を記録した帳簿の保存を求めていると解釈されてきましたが、昨年度、指定調査機関を通じて利用者の真偽の確認の自動化に関する文書が発出され、すでに解決済みとなっているため、方針においてその旨を明示するものに修正するとの議論がなされたところです。

最後に、⑥公的個人認証法に基づいて署名検証者の認定を受ける特定認証業務を行う者の基準との差異の解消についてでございます。課題のポイントとしては、現行の施行規則においては、利用者署名符号を利用者が作成する場合、利用者による申し込みと同時に、利用者署名検証符号を送信する方法が規定されておらず、利用者識別符号の交付あるいは送付を行う必要があり、利用者と事業者双方に負担を強いている状況でございます。そのため、公的個人認証法において認められている方法に統一すべきではとの議論がされていたところです。

以上を踏まえ、本検討会における検討の方針と内容についてご説明させていただきます。本検討会は、今までの検討を踏まえ、6 つのモダナイズの方向性について、ニーズの把握や要件の明確化、運

用への影響度合への観点からご議論いただいた結果、速やかに対応することとされたものについては、令和７年４月１日施行を目指し、引き続き検討が必要なものについては来年度以降も検討を継続させていただきたいと考えております。先ほど申し上げました、観点についての定義についてはこちらになります。こちらに記載の観点から委員の皆様にご議論いただきたいと考えております。

本検討会と合わせて全部で３から４回を予定しており、年内に報告書にして取りまとめを行いたいと考えております。事務局からの説明は、以上になります。

（松本座長）
ありがとうございます。議事１から３に係る事務局のご説明に対してご質問ご意見がございましたら、よろしくお願いします。いかがでしょうか？

（宮内委員）
宮内でございます。よろしくお願いします。議論の方向性についていくつかコメントがございます。まず、今回の会議の目的として、可能な部分から検討を進めて、長期にわたるものは別だというようなお話が最初にありましたけども、ここでやること以外の点でも、今回の議論の中では気にすべきところが結構あると思いますので、必ずしもこの個別の論点に係るものじゃなくて、もう少し長い目で見ているものかもしれませんが。いくつかコメントさせていただきたいと思います。

まず一つは、資料２の８ページのところに、現在の法令等一覧がございます。この一番下のところというのは告示ではなく、JIPDEC の指定調査機関に対する通知になっているので、ここで重要なことを記載するというのは、果たして今後もいいのかという問題は従前より指摘されているところでございます。今回すぐにといったわけにいかないというのは重々承知しておりますけど、こういった法令の構造の全体というのもある程度、方向性を見ていく必要があるんじゃないかというふうに思っています。また、ここに関わることですけれども、その技術的な要件については、技術仕様を別のところで作るようにして、全部をデジタル庁等で作るのではなくて、専門の部局、あるいは機関というものを考えていいのではないかというふうに思います。

それから進め方につきまして、やはりこういった電子署名をやっていく上で重要なのは、AATL 等で通用して、普通のツールで検証できることが重要だと思いますので、この内容の検討に当たっては、AATL 等とどういう関係になるかというのを考えながら進めなければいけないと考えております。この点については、事務局からコメントをいただきたいと思います。

３点目は、リモート署名の話が少しだけ出てきましたけど、これは今の施行規則のままだとリモート署名のサーバーでリモート署名側で生成した鍵ペアについて、公開鍵を認定認証業務が受け取れな

い等いろいろあると思うんですが、リモート署名との関係はこの会議だとどういうふうに進めていくのか、この点について教えていただきたいと思います。以上3点です。よろしくお願いします。

（松本座長）
はい、どうもありがとうございます。なかなか悩ましい問題が多かったように思いますけど、事務局の方、ご返答できるものありましたらよろしくお願いします。

（事務局 北井上）
ありがとうございます。事務局でございます。今、大きく3点ご指摘いただいたと認識をしてございます。

まず1点目ですね。8ページ目の中で一つが通知になっているが、と言うところでございます。ご指摘のとおり、法令の位置づけとして、政令、規則、またその下の告示というのもありますけれども、通知によってある程度の条件を設定していくというのも、行政のやり方の一つにはなっているところでございまして、従いまして、通知で、明示的な規制というよりは技術的助言というような位置づけになることもあるわけですけれども、今その現状の位置づけで極めて著しい支障がある、例えば罰則を使う時に通知では（根拠として）弱すぎるのではないかというようなご指摘があった場合には、その通知をもう少し上の段階に格上げするという議論はデジタルとは全然関係ない別の分野ではありうると承知しております。従いまして、そういった格上げをするべき何らかのしかるべき理由というものがあれば、ご指摘の点というのは、将来的に考えるということは、排除していないという認識でございます。ただ、一方で現時点でそのような状況になっているかというと、必ずしもそうではないのではないかと言うところで考えてございます。

あと、2点目の部分は、ご指摘のとおりAATLとの関係性というのは、必要な部分については慎重に議論していきたいと思っておりますし、次回以降の資料という部分でも、そういった点の考慮が必要な部分は、その点しっかりと明記しながら、資料作成等にあたっていきたいと考えております。

最後3点目、リモート署名の部分でございます。こちらそのリモート署名を今後進めていくというところの観点では、様々な課題があるというところは承知しておりまして、昨年度の議論では、そういった点も触れられていたということは承知しているところでございます。ただ先ほど全体の進め方というところで、まずはできるところから改正をして、順々にモダナイズをしていこうというのが、今回の検討会の方針でありまして、そこを考えるとリモート署名が短期的に解決する課題かというと、必ずしもそうではないというところも認識しておりまして、今回は特に短期的に解決し得るものに、集中的に今年度議論いただければというところで、敢えてこの①～⑥というところの中には位置

付けていないという状況でございます。当然課題としては、デジタル庁として認識をしているというところは付け加えさせていただきます。事務局からは以上となります。

（宮内委員）
追加でコメントさせていただきたい。1 点目について、基本的にはこの構造でも問題が起こってないというようなお話だと理解しますけれども、基本的にこの構造というのは、現在の指定調査機関が他に変わらないとか、これをやり続けるということが前提だったら、この通知でいいのですけども、本来そういうものではなくて、指定調査機関が複数あってもいいはずですし、どこかの機関への通知というのでやってると私はあまりよろしくないと思いますし、これから認定を受けようと思うところにとっても必ずしも良くないと思うので、中長期的には何とかするというのをぜひ考えていただきたいというのが私の希望でございます。私から以上でございます。

（松本座長）
はい、ありがとうございます。短期的にはできることをやる、中長期的にも今後の課題をこの検討会で発言されてもいいのではないかと思います。よろしくお願いします。

（小田嶋委員）
小田嶋です。よろしくお願いいたします。質問 3 点ございます。

宮内先生と少し重複する点もありますが、確認の意味を込めてです。15 ページのリモート署名の件で先ほどお伺いしたところで、短期ではなくて長期の課題と伺いました。右側のところ政策の実行というところで引き続き検討が必要な内容は来年度以降も継続と書いてあるので、先ほどの内容からするとリモート署名に関しては来年度以降の継続検討なのかなと思いましたけれども、その点についてお知らせいただければと思います。今日、回答なくても結構ですので次回でも構いません。

2 点目、同じく 15 ページで実行に向けた方針を具体化することがゴールということで、これはもちろんだなと思っていました。それ以外も、例えば昨年度の令和 5 年度の調査研究を拝見していて、この 6 点以外にも提案事項があったかと思います。こういったことも先ほど施策の実行のところで、例えば来年度実行に継続実施かなと思ったのですけれども、その点について教えていただきたいと思います。

3 点目、意見として取り上げていただければと思います。16 ページのニーズの把握といったところで、前提としてお伝えしようと思います。私の方では、電子認証会議の立場で出席しておりまして、署名法の認定認証事業者の集まりから出ています。昨年度の調査研究報告を参照して、①～⑥の中で

優先順位が、あるようであればお知らせくださいということで、意見をあらかじめ聞いております。その中で、もちろん認定認証事業者ごとで優先順位が異なるわけですけれども、④に関しては各社の優先順位が一番高かったというところですので、もしこの検討会で速やかに対応するとされたものが今年度検討されて来年度施行というスケジュールで優先順位付けがあるのであれば、④をぜひ優先事項としていただければと思っています。これは意見でございます。以上3点です。

（事務局 當波）

事務局でございます。3点意見を伺ったところであります。

まず1点目のリモート署名のところについては、現在の時点で具体になっているわけではございませんが、こちらの資料にも来年度以降も継続検討とあるとおり、この検討会の議論いただく点以外も含めて、今後どのように扱っていくのか、電子署名法の認定基準の中で扱っていくのか、外で扱っていくのか、も含めて継続的な検討課題であると認識しております。

2点目の昨年度デジタル庁が実施した調査研究の中で、6点以外にも提案事項があったというところについては、まだ昨年度調査を行った段階でありまして、細やかなそのニーズの把握ですとか、どういった点に手を付けなければならないのか、またその影響範囲についてまだ精査ができていないところでありますので、これについても引き続き検討してまいるところであります。

最後のニーズの把握のところについては、クラウドサービスの利用のところが一番、認証局側でのニーズが高かったということでありますが、クラウドサービスの利用につきましては、特に指定調査機関にどのように調査をいただくのかというところで、ニーズが高く、かつハードルも高いところであると思いますので、今回のその検討会の中でも、そういったハードルが高い部分も含めて、その委員の皆様からぜひご意見を伺えたらと思います。よろしくお願いいたします。

（小田嶋委員）

ご説明ありがとうございます。リモート署名に関しては、署名法の中と外のどちらでやるのかというのは、確かに議論の一つと思いますので来年度以降の継続検討課題かなと思っています。特定以外もニーズの把握に努めていただいて来年度以降の検討対象としていただければと思います。

ニーズの高かった④は、確かに指定調査機関でどのように確認するかという点は非常にハードルかなと思っております。昨年度調査報告書を見ましたところ、色んな具体的な事例をもとに出しているので、この辺りは次回になるかと思いますが、私以外の有識者の観点も含めて議論させていただければと思います。私からは以上です。ありがとうございました。

（松本座長）
はい、どうもありがとうございます。クラウドに関しては次回であると思いますけれども、今回いろんな論点があると思いますので、そのあたりもよろしくお願いいたします。次、満塩委員から 2 点進め方で質問させてくださいとあります。よろしくお願いいたします。

（満塩委員）
6 ページのところで、電子署名法全体像の構造が書かれていたと思います。認定認証業務に関しましては 3 章から書かれていると理解していますが、それ以外の議論を今後どうされる予定なのか、もしくはどこかで意見が言えるタイミングがあるのかというのを事務局の方に伺いたいと思っています。特に私の方でここ何年か見ていて、日米デジタル貿易協定に書かれている電子署名法に関するところが気になっておりますので、そのあたりがどこかでお話ができればと思っています。そのタイミング教えていただければと思います。

もう 1 点は、今回私も 2001 年の施行の時の認定認証業務の基準を検討してきたメンバーですので、中身としてもちろん理解しているつもりでございますが、やはりその時にも比べて日々技術が変わってくるスピード感がかなり上がってきていると思っています。リモート署名や、クラウド、この後は AI の話も出てくるかもしれないが、個別テーマとして今回認定認証業務の認定基準を検討するということは全然やぶさかではございませんが、今後このままの認定基準のスキームでいくかというのは、どこかで意見交換した方がいいんじゃないかなと思いましたので、そこのあたりのお考えお聞かせいただければと思います。以上です。

（松本座長）
ありがとうございます。だんだん本質的な質問で、事務局が答えるのが難しいかもしれませんが、よろしくお願いします。

（事務局 北井上）
事務局でございます。ご指摘、ご意見いただきましてありがとうございます。
今回の検討会は、検討会のタイトルにもありますとおり、認定基準のモダナイズを考えるということもございます。またその中でも特に短期的に改善し得る部分をまずはやっていこうというところを第一の目的・目標としております。従いまして、まずはそちらの議論を集中的にやらせていただきまして、最後にその議論のまとめなどをするタイミングで全体論というところについても、もし時間が取れれば、論じる場というのは可能であれば設けることを検討させていただければと思います。恐縮ですが、今後の検討会はあくまでも認定基準をモダナイズ化で短期的にし得るものというところに、集中的にご議論いただければと考えております。以上でございます。

（満塩委員）
はい、重々私も理解しており、是非そのタイミングだけ最後にでも作っていただければと思っています。今の議論を邪魔するつもりは全くございません。よろしくお願いします。

（松本座長）
例えば、2 条にある特定認証業務は、認定じゃない特定認証業務って何の基準もなくていいのかとかですね。認定のための基準と言っているが、基準は別に認定がなくても本当は重要で、そういった基準が広くいろんなところで利用されればいいんだけど、そういうことになってないんじゃないとか、私自身もいろいろ思うとこあるんですけど。そういったところもですね、念頭に今回の基準の議論をさせていただければいいかと思っております。

続いて、議事の 4.モダナイズの方向性に関する①と②に関して、事務局の方からご説明をよろしくお願いいたします。

（事務局 山之上）
事務局でございます。資料 2 の 18 ページからご説明いたします。まず課題①について説明します。昨年度の検討内容については、先ほど申し上げました通り、具体的基準に照らしますと、特定認証業務の認定に係る基準においても、情報セキュリティに係るリスクを評価し、適切な管理策を実施するマネジメントシステムの概念を盛り込むべきとし、各認証事業者自身がアセスメントをし、各認証事業者自身がその結果に基づいた対策を実施することが必要との議論がございました。
それを受けた本検討会での議論の方針としましては、危機管理等の観点により、情報セキュリティに関するリスクマネジメントについては現行規定においても存在するとも考えられるがいかがか。また、リスクマネジメントの基準として規定すべき内容を整理する必要があることから、課題①については 2 点、要件の明確化を行いたいと考えております。

まず、1 点目について、現行の施行規則等において、危機管理に関する規定は既に存在すると考えられますが、リスクマネジメントが法第 6 条第 1 項第 3 号が委任する範囲に含まれるかという点でございます。具体的に申し上げますと、法第 6 条第 1 項第 3 号に基づき、施行規則第 6 条第 1 項第 15 号トに危機管理に関する事項が規定されていることを踏まえれば、情報セキュリティに係るリスクマネジメントは法委任の範囲に含まれると解釈してよいか、また施行規則の危機管理に関する事項について、リスクマネジメントの意味を含むものとして解釈できるかという内容でございます。

2 点目については、ETSI は標準規格上で、TSP にリスクのアセスメントや評価等を要求しておりますが、事業者に求めるリスクマネジメントの基準として、どのような内容を盛り込むべきかという点でございます。具体的に申しますと、ただ今申し上げたとおり、ETSI は標準規格上で、事業者にリスクのアセスメントや評価、軽減措置、定期的な見直し、文書化と記録を要求しておりますが、電子署名法に取り込むべき項目は何か、また他に盛り込むべき内容は何か、という内容でございます。以上から、課題①については、こちらの論点詳細の部分により委員の皆様にご議論いただきたいと考えております。

次に課題②についてです。昨年度の検討内容については、先ほど申し上げましたとおり、暗号装置に関する技術基準が 20 年以上前の米国の基準と同等のものとなっているため、現行の方針を FIPS140-2 及び ISO/IEC15408 に言及する規定に置き換える必要があるというご議論がございました。これを受けて、本検討会での議論の方針としては、FIPS140-2 への更新であれば、暗号基準の更新を行うこと自体には、新規参入の障壁にならないと思われますが、FIPS140-2、FIPS140-3 いずれの内容に合わせるべきか、また FIPS140 シリーズの変遷を踏まえ検討いただく必要があることから、要件の明確化及び運用への影響について議論いただきたいと考えております。まず、要件の明確については、FIPS140 シリーズについて、どのタイミングや内容でモダナイズを実施するべきか、という点でございます。具体的に申し上げますと、現行の暗号装置に関する技術基準は、平成 6 年に発行された FIPS140-1 と同等となっており、電子署名法が施行された平成 13 年 4 月の翌月に FIPS140-2 が発行。また、平成 31 年に FIPS140-3 が発行されましたが、技術基準の改正がされていないところでございます。しかしながら、問題点の中断に記載している通り、FIPS140-2 の有効期間が令和 8 年 9 月 21 日で終了するため、翌 22 日からは FIPS140-3 へ完全移行することになっています。一方で、机上調査によりますと、今年に入ってから FIPS 140-3 準拠の認定を受けた製品が一定程度増加したものの、一部のプロバイダに限られるため、FIP140-2 に比べれば 1/6 程度の製品数に留まるため、移行と普及には一定の期間を要する可能性あるという問題点がございます。

次に、運用への影響については、FIPS140-2/3 のいずれかに合わせた暗号基準にした場合、特定認証業務の影響はどんなものがあるかという点でございます。以上から、課題②について論点詳細により委員の皆様にご議論いただきたいと考えております。事務局からの説明は以上となります。よろしくお願いいたします。

（松本座長）

はい。ありがとうございました。①と②がありますが、内容がかなり違うので、発言される方も多少違うと思います。まず①に関してまず議論していきたいと思います。ご意見ある方よろしくお願いします。

（漆嶌委員）
まず 1 点目、今回の法律・指針・施行規則で、リスクマネジメントが含まれているのかどうかが①の議論だと思います。その中で、これまで法律・指針・施行規則に照らしてリスクマネジメントをやって来なかったと言ったような現状があるので、これが含まれていたと後から言うのは無理があると思っています。法律は変えないまでも指針や施行規則に追記をして、今回対象になっているのは、単なるリスクマネジメントではなくて、情報セキュリティマネジメントなので、そのことを明記をして、義務付けるというのが良いのかなと思っています。これがまず 1 点目でございます。

2 点目、資料の方に ETSI のリスクマネジメントがあるから、これを検討しなきゃいけないという議論になっていることについて違和感を持っています。一般的な情報セキュリティマネジメントの観点、ISMS の観点からリスクマネジメントもやらないといけないという観点で、ETSI に習うからではなく、ISMS 国際規格に照らしてやる必要があるということは言っておく必要があると思っています。

最後の 3 点目、前から気になっているのが情報セキュリティリスクマネジメントをやると言っていますが、事業者によって遂行能力やリスクの評価能力にばらつきがあるのではないかということをとても気にしています。例えばファイヤーウォールを入れたから、中身は脆弱性スキャンをしなくていい、などの乱暴な議論になってしまうのではないかということを気にしていまして、リスクの評価方法とか対応方法というのは ISMS や NIST のガイドラインで、リスクの評価方法、対策方法、判断基準が定義されているので、これによって対策をしたほうがいいのではないかと思っています。

4 点目、今回リスクマネジメントで扱う部分というのは、認定認証事業における情報セキュリティリスクの話なので、例えば具体的には CA の鍵管理、利用者の鍵管理、証明書の発行方法で誤りが起きるとか、本人確認の誤りなどの、事業者共通で想定されるリスクファクターというのは必ずあるだろうと思っています。そういった観点で、事業者には各社同じような基準で、ここまではできているのかどうかといったような確認をする方法を取られるのがいいと思っています。そういったリスクの中にも既に施行規則や指針で対策・カバーされているものについてはあえてやる必要がないと思うんですけども、そこから抜け漏れているリスクについてはちゃんと確認をするといったようなことは必要なのかなと思っています。私から以上 4 点でございます。

（事務局 北井上）
ありがとうございます。1 点目の部分だけ補足的に回答をさせていただければと思います。おっしゃるとおりで、全く改正なしで、これまでも求められていたからこれからも求めます、指針だったり方針だったりも含めて何も変えませんということを申しているつもりはなく、今の法律の規定だったり、規則の状況を考えれば、おそらく、法律まで変えにいくというよりは、規則ないし、その下の指針だったり方針だったりでしっかりと改正をして求めていくということをしても、特にその施行規則

の危機管理に関する事項というところもありますので、その下の下位規定で、しっかりと必要な部分を定めていくということはあり得るのではないかと事務局としては考えているところでございます。従いまして、全く改正しないで、リスクマネジメントをこれまで求めてきているのだから事業者の認定基準としてこれまでもあったのだということを申し上げるつもりは現時点ではないので、その点は補足的に回答をさせていただければと思いました。我々事務局からは以上です。

（松本座長）
ありがとうございます。ISMS というか、そもそも電子署名法 2000 年で ISMS 以前なので、その後 IT-BCP の国際標準などは全て電子署名法の後なので、後付けすれば対策が盛り込まれているかというと、それは足りない部分もきっとあるんじゃないかなというふうに思いますね。あと ETSI は、認証局のインシデントがあった場合、それに対してどんどん基準を改定してきているので、そういう枠組み自身がなかったというが問題なんじゃないかと聞いてて思いました。

（事務局 當波）
漆嶌委員のコメント 2 点目以降について私からコメントさせていただければと思います。2 点目以降のコメントは、漆嶌委員、松本座長の話のとおりであると考えておりまして、よくこの認証局の基準について語る際に、ETSI の基準を参照してしまうということがありがちではありますが、特に漆嶌委員の、WebTrust であったり、他の認定制度のご知見についても、ぜひこのような形でコメントいただき、反映させていただければと思いますので、今後ともコメントよろしくお願いいたします。あと、最後にコメントされていた点、すでに情報セキュリティリスクマネジメントの基準について、すでに存在している認証業務の基準でカバーされているところがあるのではないか、カバーされていないところについて手当をするべきではないか、というところについて、今回でなくてもよいですので、もしここから実際に抜け漏れているであろうという点の候補を、我々としてもそこの点を調査したいと思いますので、そういったところの助言をいただければ、事務局としても作業がしやすくなり、大変助かります。よろしくお願いいたします。

（松本座長）
指定調査機関 JIPDEC の大澤さん次よろしいでしょうか？

（JIPDEC 大澤様）
サイバー攻撃とか頻発している今日ですので、重要インフラについて対策を講じるということが、この電子署名法が制定された当初よりもはるかに一般的になっているんだろうと思っています。

認定認証業務用設備につきまして、現在重要インフラということに含まれてはおりませんけれども、セキュリティ上の安全確保の観点からリスクマネジメントを行うことが必要であることについて、問題意識を持っているというところが実情でございます。

先ほど、漆嶌委員からも国際規格に照らしてやるのではないかというようなご発言がございましたように、具体的には ISO/IEC27001 に基づく ISMS 適合性評価制度の認証結果につきまして、調査要件に対する適合性の判断の一材料として取り入れてはいかがと考えている次第でございます。私からは本件につきまして以上です。よろしくお願いいたします。

（松本座長）
ありがとうございます。漆嶌委員が言われたことに非常に近いと思いました。

それともう一つ、重要インフラじゃないという話もそうなんですけれども、欧州の NIS2 指令では、デジタルインフラストラクチャというセクターがありまして、その中にトラストサービスが入っていて、NIS2 指令の枠組み入るということで、トラストサービスは、欧州においては重要インフラとみなされることになります。そのため重要インフラとしての要件が認証局に課せられるようなところがあって、ある意味それを国際的な流れでもあるのかなと聞いていて思いました。ありがとうございます。

ISMS は一般的な情報システムなんですが、認証局の方はアーキテクチャがはっきりしてるというか、もともと守られる仕組みが内在していると思います。そういった意味で、2000 年に作られた電子署名法の基準も結構網羅的に作られているんですよね。それに対して、いくつかやっぱり足りない部分があるんじゃないかというふうには思うところがあります。ありがとうございます。

次、満塩さんよろしくお願いします。①に関するコメントよろしくお願いします。

（満塩委員）
ありがとうございます。まず私が一つ疑問があるのは、リスクマネジメントを入れるという話をするんですか？それとも私の理解だと、ガバナンス基準みたいなものを導入するということではないかなと思っています。

それとまずごめんなさい、昨年の議論を私がちゃんと理解してないんですけど、そこは明確にリスクマネジメントなんですか？

要は、私のイメージの中ではガバナンス基準の中にリスクマネジメントが入ります。一方リスクマネジメントと言ってしまうと、先ほどの PDCA が本当に入るかと言われると、そこまで実はリスクマネジメントの流れは入らない可能性も出てくるなと思ったので、どちらかというとガバナンス基準ではないですか？

（松本座長）
事務局コメントをお願いします。確かに IT-BCP のことを指していると思ってしまいますね。

（事務局 當波）
ご指摘の通りで、今回の資料でも記載のとおり、ETSI でもリスクアセスメントという言葉があるように、その言葉に引っ張られている箇所があることを認識しております。実際にガバナンスの中にリスクマネジメントが入っている、ガバナンスがなければスクマネジメントを導入しても意味がないというところは理解しています。今回の基準の中では、そこの箇所が明確に議論できていないところではありますので、今回の議論を踏まえ事務局のほうで考えたいと思います。議員の皆様からもガバナンスを認証局に構築する、それを認定基準とするべきなのか？という点についてコメントがあればいただければと思います。

（満塩委員）
わかりました。それでは前提としてガバナンスというイメージでこの後 2,3 点ほどコメントさせていただきます。

一つは、歴史的な背景というかタイミングの問題として、電子署名法は 2001 年に施行されていますし、松本座長からもお話があったように ISMS も 2001 年だったという理解です。その周辺でですね、私も参加しましたが COBIT というガバナンスに関する基準も、1990 年代から整理されてきているので、そういう意味ではこの電子署名法を作成する際に、あまりガバナンスという概念は取り入れていなかったというのが正直思っていますので、入れたほうが良いと思っています。テクニカルな話として、20 ページの第 6 条第 3 号の中で、設備要件、本人確認プロセスの要件、それ以外をその他にしたという記憶があるので、ガバナンスも入ると解釈し法改正はしないとできるかと思います。ただし、先ほどお伝えした通り、ガバナンスが今大分重要視されてきているので、可能であればガバナンスを外出ししたほうが良いと法施行的な話として思っているところでございます。

あと、基準なんですが、これも他の方々に賛成で、ETSI の個別の電子署名法関係のところを参考にするというよりは、ISMS や私も関与している ISMAP も整理としてガバナンス基準、マネジメント基準、管理策基準という言い方をしておりますので、そういう意味ではそこのあたりのマネジメン

ト基準というのがほぼ該当するところだと思いますし、あとは経産省のシステム監査基準のほうでも、ガバナンスに関する項目というものが整理されていますので、そのあたりを参考にするのが良いのではないかと私は思っております。以上でございます。

（松本座長）
ありがとうございます。

満塩委員は 2000 年当時の電子署名法から当時の ISMS ですね、皆さんご存知なんですけれども、ここで何故こういうものがあるのかでしたり、こういうものはないのかというのはちゃんと言っておかないと我々の後輩はもう既にわからなくなりつつあると考えていますので、是非ともここでいろいろ発言していただいて、直すところは直していただければいいんじゃないかなと思っています。

よろしいですか？それでは次へ進みますね。小田嶋委員から①について 3 点コメントとありますがよろしくお願いします。電子認証局の立場としてコストもかかることであり色々あると思いますのでよろしくお願いいたします。

（小田嶋委員）
まず 24 ページのところで法範囲に含まれるかというところですけれども、法規則の第 6 条第 1 項第 15 号は、基本的には指定調査機関の調査の内容からすると、どちらかというと認証局の秘密鍵の危殆化に関する事項に現実は限られています。そうするとリスクマネジメントというかリスクアセスメントと言ったわけですかね、ガバナンスと言った方がいいかもしれませんけれども、そういったところは厳密には入ってないだろうと思っています。

一方では法の修正のしにくさも理解しているので、なるべくデジタル庁さんのお手間がかからないような形で、ただ現実には含まれてないと理解していますので、修正の方法はともかく、反映した方がいいと思っています。それが 1 点ですね。

2 点目ですけれども、先ほどの何かしら反映された後、認証局の方も指定調査機関もそれを実施する、もしくは調査する立場になります。そのときにどういったことを行えば、双方に対して、先ほど座長がおっしゃっていただいたとおりなんですけれども、コストをなるべく軽減できるような方法が必要だと思っています。その辺りも含めて勘案いただければと思いますし、私以外の委員の方でご知見をいただければありがたいなと思っています。

何とも言いようがないことに近いですけれど、先程の ETSI 319 401 を引っ張ってきていますが、あれはどちらかというと ETSI がどうこうというよりかは、先ほど満塩さんの言ったことが近いと思

いますが、ちょっとガバナンスに近いことをしてきてるんだと思っています。例えば、資料にも書いていただいているとおりですが、例えばリスクを 4 つに分けて、それぞれどういうふうにしていくか、あとマネジメント、最終的にはリスクを許容するところは会社のトップレベルで承認されるべきだとか、そういったところを含めてだと思っています。最終的には ISMS だけですとそういったところが入らないとするならば、そこは含めていただいた方がいいのかなと思っています。以上 3 点です。コメントですので特に何かコメント求めるものではないです。

（松本座長）
　特に質問ではないとのことでしたが、事務局から何かございますか？コメントあればよろしくお願いします。よろしいでしょうか？それでは次へ進みます。

宮内委員より 1 点コメントがございます。よろしくお願いします。

（宮内委員）
論点 1-1 について私の意見を述べさせていただきます。まず結論から言いますと、法律を変える必要はないけれども施行規則は変えたほうが良いと思っております。

まず法律を変える必要がないという理由について説明しますと、この法第 6 条第 1 項 3 号に対応するものはここにも書かれておりますように、施行規則法第 6 条第 1 項なんですね。1 号から 15 号があって、15 号がさらに細分化されてるわけですけど、この中で監査の事故とか色々なものがすごく含まれていて、第 1 項第 3 号には申請にかかる業務が主務省で定めるチェックをするというのは非常に広い範囲に含まれるので、第 1 項第 3 号にリスクマネジメントを入れようとしても含まれるだろうと考えます。ですから法律自体を変える必要はないと考えているんですが、施行規則の方は第 15 号トに関する規定は方針の第 4 項第 8 号の(3)に該当するのですが、実は危殆化のことしか書いていないんですよね。ですから現在の危機管理は割と狭く理解されてるという風にも見えますので、このままではなくてここにリスクマネジメントあるいはガバナンスが入るという文言を改正するか、トの次にチを作ってそのリスクマネジメント等が含まれることを明示するとどちらかの方法でその施行規則を変更してリスクマネジメント等に関する事項を明示するのが良いと思っております。私から以上です。

（松本座長）
ありがとうございました。重要な観点だと思いますね。法律自身もやっぱりあるべき姿に変えていかないと、今後時間が経つとわけがわからなくなるんじゃないかなと聞いてて思いました。ありがとうございます。

最後に、漆嶌委員の方からもう 1 回コメントの希望がありますけど、時間も大丈夫なのでよろしくお願いします。

（漆嶌委員）
ありがとうございます。先ほどの満塩委員の方からガバナンスとして入れたらどうかとコメントいただきました。国際相互承認みたいなことを考えたときに例えば WebTrust であったり ETSI の規格であったり、リスクマネジメントを実施されていることの明文化されることが重要なのかなと思ってまして、そういった観点でその施行規則でも何でも良いのですが、どこかしらで電子署名法の認定認証はリスクマネジメントがちゃんと行われていることがわかるようになっているといいのかなと思いました。

ガバナンスに関しては、文言に入れるというよりは、例えばその CP/CPS 全体を見ても、ガバナンスに関することが書かれていて散りばめられているので、ガバナンスについて一言どこかで書くというのは難しいのかなという気もしています。私からのコメントは以上でございます。

（松本座長）
ありがとうございます。今回の範疇ではないですが、国際的なハーモナイズというのは要求されつつあるという現実もあり、それに向かってどうするのかというのが今回の議論の背景にもあると感じておりますので、もっともな話だと思いました。

ということでだいたい意見は出揃ってきており、大体肯定的であり、何らかの法律、規則、先ほど宮内委員からあったように施行規則の改正であるとか、実際にそういったことは必要だという意見が大体だったかと思います。

では次の 2 つ目の議題ですね。だいぶ違う話ですけれども、FIPS140 について議論したいと思います。

これに関してご意見のある方、チャットに書き込んでください。でもこれひどいですよね。今だに 140-1 というのはすごいですね。よろしくお願いします。まず HSM についてとてもお詳しい漆嶌委員の方からお願いします。

（漆嶌委員）

ありがとうございます。まずその HSM についてなんですけども、今その FIPS 140-2 から 140-3 への移行の過渡期だと思うんですね。140-3 の製品というのはまだそんなには出揃ってないという印象ですので、今のところはその 140-2 か 140-3 の製品を認めるといったような形でやっていくのがいいのかなと、まずは思っています。

あといろんな面で明確化・明文化をしていただいた方がいいようなところがあるのかなと思ってまして、まず FIPS や Common Criteria 含め、5 年おきに FIPS Active の状態が期限切れになる可能性が高いことになっていますので、その事を念頭に制度設計をしておかなければいけないんだろうと思っています。例えば FIPS が Historical の状態になった場合には、その扱いをどうしましょうか？原則だめでいいと思うんですけども、ただそのときにいつの時点で FIPS Active になっていることを求めるかと、これも申請時点なのか、調査中なのか、あるいはその途中運用過程で切れたときにどうするのか、そういったことを明確化しておかないといけないと思っています。

あと認証局に必要とされる HSM の機能に、瑕疵が見つかった場合に Revoked になったという時には仕方がないと思うんですけど、関係ない理由で Revoked、Historical になるといったようなケースもあるんだろうと思っています。

例えば、AES 暗号の実装のところに瑕疵が見つかり Revoked になりましたと。そういった時には認証局の運用には関係がないので、関係なければこれを使い続けてもいいんだといったようなことが、基準としてはっきりなってるとより状況が緩和できていいのかなと思っています。

最後、ここのところは資料に書かれていないんですけど、レベルの明確化について記述の必要があるんだろうと思っています。FIPS 140 の場合の Level-3 以上や、Common Criteria の場合 EAL4+以上等ですね。そういったレベルについて、どうするのかといったようなことは基準で記載されているといいのかなと思っています。私からのコメントは以上でございます。

（松本座長）
中身的にも漆嶌さんが一番よくご存知かと思いますけれども、今時 HSM 一番たくさん購入しているのはクラウド事業者ですからね。ある意味で何処でも使ってるので、認証機関に限らず皆様どうしているのかなというのは気になりました。ありがとうございます。

次は満塩委員ですね。よろしくお願いいたします。

（満塩委員）

指定調査機関への質問になってしまうんですが、質問としては、審査の時に結局 FIPS の認証書の確認をしているのではないかと推測するんですが、そういう理解でいいですかということです。というのは、先に申し上げておくと、私の理解だと FIPS と書いていなくて、FIPS のところを全部日本語に書き下したものが書いてあるという理解なんですけど、あれは当時 2001 年あたりにこういった方法しかなかったと話を伺ったことはありました。先ほど漆嶌委員の話もあって、もう〇〇Level 以上や認証書と書いても良いと思っていますので、そういう意味では記述に関しても、私は明示的に書いた方が良いと思います。

ただし FIPS が日本の制度ではないということも伺っていましたので、そこは理解した上で、ISO などで書けるのであれば、そちらもあるでしょうし、そういったところが改善するべきではないかということだけは申し上げておきます。以上でございます。

（事務局 當波）
事務局からコメントさせていただきます。まず漆嶌委員のこの FIPS140-2 相当か 3 相当かというところで現状は 2,3 両方を認めるという形で良いのではと思うということで、そこのところは事務局としても気にかけていたところで、ご意見いただきありがとうございます。

満塩委員も、合わせてその明確化、明文化、FIPS の基準を具体的に引いた方が良いのではないか、ただし米国の基準ということもありますし、直接認定基準の方にそのような文章を書くことは厳しいのではないかというところも含めて、そういった需要があるというについては貴重なご意見かなと思います。

我々としても、必要がありそういった表現が出来るのであればそのようにした方が良いと思いつつ、ご意見があった通り米国の基準でありますので、日本の認証局の基準としてこれを引っ張るのが引用する形が良いのかというのが、また今回のところに表れてない議論なのであるかなと思います。

ほかの皆様も意見があればお伺いできればと思います。

（松本座長）
満塩委員はよくご存じだと思うんですけど、2000 年当時、実は国産の HSM が各社ありました。それを受け入れる必要があるというのがあり、あまりいいことではないんですが、みんな撤退されてしまいました。ちょうど今年の夏にあった CRYPTREC で松本勉先生が日本製 HSM がないことを嘆いておられましたけども、産業政策として日本に HSM がないというのは本当は色々な意味で非常によろしくなくて、そこにいろんなトラストアンカーが繋がっているという状況があるというのは非常に好ましくないですが、一方認証局の立場からすればデファクトに近い FIPS140 を取っていることが

世界的なデファクトになってるという現状があり、認証局はあまり困らないというか、それを考慮する必要はないですが、結構 HSM が重要だというところはもう 1 回再認識しなきゃいけないと思いました。

はい。次一番現状をよくご存じの JIPDEC の大澤さん、よろしくお願いします。

（JIPDEC 大澤様）
まずは満塩さんへご回答させていただきます。確かに FIPS の 140-1 や 140-2 の認証結果を確認しているというのが正直なところでございます。本件についての指定調査機関としての意見につきましては、現在指針と呼ばれている令和 2 年に最終改正を行われているものがございますけれども、そちら指針の方には残念ながら暗号装置の技術基準についての言及がございません。指定調査機関としましては、実地調査において方針と言います、デジタル庁さんのデ社第 5 号あるいは法務省さんの民商第 157 号といった形で指定調査機関に対して示されている方針といったものに基づいて、暗号装置の信頼性を確認しています。

ただし、この方針につきましては、暗号装置の具体的な技術基準といいますよりも、今経緯の説明もありました通り、2001 年当時のアメリカ連邦情報処理規格、いわゆる FIPS140-1 のセキュリティ要件の部分を抽出して書かれたものであると解釈されて、今日まで参っております。

デジタル庁さんにおまとめいただいた資料の中にもありますように、また漆嶌委員からもご発言がありましたように、世界中の認証局につきましては暗号装置がすでに FIPS140-2 どころか 140-3 への移行時期にあるという現状がございますので、この件につきましては数年前から JIPDEC といたしましても、主務省庁さんに対して、あるいはこういった平場の各所の会議におきまして申し上げておりますとおり、その認定基準を可能であれば一刻も早く明確に指針の中でも読めるようにしていただいて、なるはやでご検討が行われるということは理解しておるところですけれども、今後一刻も早く改正いただけるとよろしいのではないかと考えております。私からは以上です。

（松本座長）
ありがとうございます。事務局から大澤さんのご発言に関して何かございますか？

（事務局 當波）
大丈夫です。

（松本座長）
はい。次は小田嶋委員ですね。3 点コメントがあるとのことで、認証局側の立場だと思いますが、よろしくお願いいたします。

（小田嶋委員）
はい。②に関して 3 点です。

先ほど資料にもありましたとおりなんですけれども、FIPS140-2 と 140-3 がちょうどあまり良い時期じゃない、あまり良い時期じゃないという言い方が適切かどうかわかりませんが、認証局としても実は困っている状況にもあります。140-2 を選んだとすると、ゆくゆく残念な結果になるということは分かっていますし、とは言っても 140-3 だと今簡単に入手するのもなかなか難しいということも実は聞いています。

直接取引ではなくて何段階かかけて取引を行いますので、例えばですけれども CA のシステムを提供するベンダー自体が対応困難だったりするといった現実もあります。そうするとなかなか今難しいところで、かつ先ほど CRYPTREC のお話もありましたけれども、2028 年の秋頃ですけれども次世代の暗号移行というのも、認証局はイベントとして控えています。この時に向かって今どうして行くべきか、HSM も簡単に変えられればもちろんすぐに対応するでしょうけれども、そういった状況ではないと言うところです。そうすると簡単に決断も実は難しくて、例えば今回なるべく早期の改正に関しては来年度の施行という話もありますけれども、この②に関して言うとなかなか簡単ではないということが現実だと思っています。特に、先ほど歴史の話もしていただいて 2000 年代の国産のメーカーの話で、今国産のものは事実上なくて、事実上限られた社しか発注もできないというところで、お問い合わせをしても簡単に回答も帰ってこないといった状況も実はあります。総じて、技術基準のモダナイズという意味では改正するべきだと思いますけれども、現実を見ていただいて最終的には主務省庁に判断をいただきたいと思っています。

3 点目ですけれども、認定認証事業者の事業継続性の観点をお伝えしたいと思っています。過去、新規で入ってきて途中で辞めていった事業者というのも存在しています。撤退の大部分はコストです。コストがかかるというところはやはり事業継続性からして相当なインパクトだと思っています。今回の①②に関しては、もちろんモダナイズの観点でとても重要なことだと認識していますが、一方で認定認証事業者の事業継続性というところの観点も重要だと思っていますので、この辺りを意識していただければと思っていますし、費用かかるようであればそれは署名者、利用者に跳ね返ることにももちろんつながりますので、そういった観点から国民の経済を考えた上でも重要なところというふうに思っています。言いづらいことではあるんですけれども、認定認証事業者の切なる意見ということでコメントさせていただきました。回答求めるものではありません。以上です、ありがとうございました。

（松本座長）
ありがとうございます。多分、実態は小田嶋さんなどの電子認証会議のメンバーや指定調査機関の大澤さんのところが実態としてどうなのかというのが一番よくご存知で、それに対して基準をどう整合させるかというのがあるかと思いますけれども、大まかに言って FIPS140-1 というレベルの話じゃないですよねというのが、大局的な意見じゃないかなというふうに思いました。ありがとうございます。

だいたい②に関しても意見は出揃ったのかなと思います。最後の議事に参りたいと思います。議事 5 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 山之上）
事務局でございます。資料 2 の 28 ページについてご説明いたします。次回の第 2 回につきましては、本日の議論内容を振り返りと課題③から課題⑥について対面で議論いただく予定しております。検討会の開催場所は日時については追って委員の皆様の方へご連絡させていただきます。第 2 回検討会の検討状況を踏まえ、第 3 回の検討会を 11 月下旬に開催させていただき、第 4 回検討会につきましては報告書を元にした検討内容の振り返りとさせていただきたいと考えておりますのでよろしくお願いいたします。事務局からの説明は以上となります

（松本座長）
ありがとうございます。何か皆様方のご意見等はないでしょうか？次回の③から⑥の方が重たいなと感じてるんですけども、今日の①・②は基準を高め、先ほど小田嶋委員からあったようにコストがかかる方法の話に近い話なんですけど、③から⑥はどちらかというと今後認証局に対してより合理的な証明書発行みたいなところをやるようにしようという話で、そうすると今度はそれを評価するのが難しくなるという問題であり、非常に厄介な問題かなと感じてますが、ここがちゃんとできないとそもそも認証局自身の競争力、日本の競争力が失われていくような話でもあるので、次回はとても大切な議論になるんじゃないかという気がしております。

（小田嶋委員）
まずスケジュールのところで、第 4 回が 12 月頃、早ければ来年 4 月に必要なものに関して、施行まで行くという話だったんですけれども、そこまでの日程を確認したいです。例えばパブリックコメントとかあると思いますけれども、実際指定調査機関の調査を受けるとしたときに、その調査票の修正等の時期や期間で想定があれば教えていただきたいと思っています。今回の内容すべてをもし例え

ばなるとすると調査票の内容を変えるだけでなく、調査機関の金額、調査手数料に跳ね返る場合もあると思うので、確認したいと思っています。

もう 1 点、先ほど補足できればと思ったんですけれども、ガバナンスの件で、完全に一致はしないんですけれども、施行規則第 6 条 15 号のロに「業務従事する者の責任および権限並びに指揮命令系統」という内容があります。これは今どちらかというと狭い範囲にもしかしたら閉じているような書き方ですけれども、先ほどガバナンスという観点で言うと、もしかしたらふさわしいのかなというふうに思いました。以上です。

（松本座長）
ありがとうございます。最初の質問に関しては、多分今回のことだけじゃなくて、次回の議題にも関係あるかもしれませんが、何かコメントがあればお願いします。

（事務局 北井上）
事務局でございます。1 点目の部分について回答させていただければと思います。第 4 回以降の流れですけれども、ご指摘のとおり、基本的には規則などの改正というのが今回あり得るだろうと考えておりまして、そういった場合も考えますと、実際に改正するとなった場合はパブリックコメントをするのだろうと考えているところでございます。その中で調査の具体の費用について具体的に細かく指定調査機関とご相談ができているわけではありませんので、この場で回答できるところがありませんけれども、しかるべきタイミングでしっかりと検討して充分前もってお伝えできる形でやらせていただければと思っております。明確な回答にならず恐縮でございます。以上です。

（松本座長）
ありがとうございます。その他次回以降の進め方やご意見があればよろしくお願いします。特段質問がないようであれば、第 1 回の検討会はここで閉会したいと思います。皆様次回もよろしくお願いいたします。本日はどうもありがとうございました。

以上