資料1

平成 26 年度第 3 回電子署名法研究会　議事要旨

1．日時
　平成26年12月19日（金）　10：00～12：00

2．場所
　経済産業省商務情報政策局第1会議室（経済産業省本館4F）

3．出席者（敬称略）
　【構成員】
　　手塚委員、小田嶋委員、大澤委員代理、中村委員、長尾委員、西山委員、早貸委員、松本委員、南委員、宮内委員

4．配布資料
　資料1　　平成26年度第2回電子署名法研究会議事要旨
　資料2　　第1回及び第2回研究会の議論のまとめ
　資料3　　指定調査機関における現地調査の簡素化について

5．議事概要

資料3に基づき、事務局から「指定調査機関における現地調査の簡素化」を説明。その後、自由討議が行われた。主な意見は、以下のとおり。

＜現地調査の簡素化について＞

1　資料3のポイント1について

○　業務手順の適正性の確認作業について、現地調査時に発行及び失効に関する実際の作業実施状況を確認して、適正に業務が行われていることを確認するというところが従来と異なる。調査を楽な方にばかり動かしていくのではなく、実際に業務手順を指定調査機関の目で、実地で確認し、それによって、今までのサンプル調査で細かく見てきたところを代替するイメージである。この部分についても事業者の委員のご意見を伺いたい。

○　(2)の 3 つ目のポツで実在確認を中心としてサンプリング調査をすると書かれているが、以前議論していた住所表記の完全一致の範囲をどのような表記まで一致とするかということについては、適合のサンプルを作成して判断するということが議論されていたかと思うが、そういったことが前提にあって確認するという理解でよいのか。

○　この場で主務省を交えて、これなら良いという事例を積み重ねていって、それに沿うようなものであれば、このレールに乗せていって良いのではないかと考えている。

○　住所表記の件については、現在データベースの元となるようなものを作成中であるため、次回以降の研究会での検討になる。

○ (1)が発行申込書及び失効申込書を除く帳簿という観点で、(2)が発行申込書、失効申込書と本人確認資料という分類になっているかと思う。現状の調査方法は、事業者が 1 年間に発行している発行枚数から比率的に、何万枚だとサンプリング数はいくつというような数を決めてサンプリングをしており、50 枚なら 50 枚とサンプリングを決めて、その中で発行申込書と失効申込書のサンプリングもするし、それに付随する発行申込書、失効申込書以外の作業の実施の記録も併せてサンプリングしてきたが、それをまず分けて考えようという理解でよいのか。

○ そのとおり。

○ そうすると、(2)は利用申込書に付随するものだから、現状と同数の発行申込書や失効申込書をサンプリングし実在確認をするとあるのだが、(1)の作業記録などのサンプリングの具体的なやり方というのが今の説明だとよく分からない。

○ 従前は、完全に 50 件なら 50 件を事前に指定しており、その指定する作業にかなりの工数がかかっていたが、今後は、例えば棚があるとするとその場で束の単位で 50 束を指定し、その 50 束の整合性について、管理帳簿と突き合わせて存在確認を実施する。それ以外はあまり変更ないと考えている。

○ 調査の現場でサンプリング案件を指定することによって、今までかかっていたどの案件をターゲットにするのかという手間を省くことができ、事業者も指定調査機関から事前に指定されたものを 1 件ずつ棚からピックアップしてきて、証明書とセットにするという手間が省ける。発行申込書と失効申込書は分けて管理されていたり、合わせて管理されていたり、いろいろな管理方法があるが、いずれにしてもサンプリング件数が多い事業者ほど、準備にかかっていた工数について削減できるのではないかと考えている。

○ 指定調査機関が複数あった時代、ある指定調査機関のやり方は、調査の初日の朝に全ての発行一覧を提出せよと言って、そこから数十件選ぶ。従って、調査の初日の朝は大変な作業があった。JIPDEC は初期の頃から事前に指定する方法だったので、そこは随分負担が軽減されたと思った。先ほどの説明で、またその場でサンプリングすると負担が増大するのではないかと思ったが、束単位での指定ということであれば、大きな問題にはならないと思う。

○ 束というのはどのように捉えれば良いのか。並んでいる書類をそのまま確認するから、一々事業者側で違う書類を整理する必要がないということなのか。

○ 通常はキングファイルに綴じて管理する方法がやりやすいため、そのファイル単位ということ。

従来だと、申込書類には、通常の法人の者、個人事業主の者、外国籍の者というバリエーションがあり、そういったものを網羅的に選べるような選び方をしていた。業務の適正性の確認という観点では、そういった選び方の方がより厳格に確認できるとは思うが、法令上そこまで求められているわけではなく、今回その点は一歩引いた形で、多数並んでいるキングファイルから選ぶということになるのだと理解している。

○ それは作業量的にどれほど軽減されるのか。

○ 数十カ所のキングファイルから 1 件ずつ抜いて事前に準備するというのはかなり作業的に大変なものがあるので、その分作業量が軽減される。

○ 他の指定調査機関がそういった調査方法を採用していたということは承知していたので、そのような負担がかからない形で実現できないかと今回の提案を行った。事業者によっては申込書をクリアファイルに入れて、それをボックス単位で管理しているところもあるが、いずれにせよ、現地調査の初日に、更新調査の範囲になっている棚からランダムに束単位で指定する方法で実施したい。

○ サンプリングのトータル枚数の割合は、現行と変わらないが、その選び方を合理化するという趣旨である。

○ 監査指摘事項についての対応状況のフォローというのは、指摘事項の有無について確認しなければならないと思うが、それは負担増にはならないのか。

○ 監査指摘事項については、従来から現地調査に入る前の調査申請の段階で、その有無を確認している。

○ 先ほど 50 件サンプリングするという話があったが、これは(1)の①、②、③に限って 50 件サンプリングするということか。つまり、(1)①、②、③に該当がなかった時は、サンプリングは実施しないと考えてよいのか。また、50 件のサンプリングについて、束にして 10 件ずつ選ぶというのは、資料 3 には明確に説明がない。それでよいのか。

○ (1)の①、②、③については、件数がある話ではないため、何件確認しなければならないという制約はない。こちらについては、発行・失効申請書に紐付いて確認する資料、ある特定の要件に従って帳簿を用意する資料になる。束にして選ぶという部分は、資料 3 の 3 ページ中段に「現行方式のサンプリング調査の件数と同数のサンプルを現地でランダムに指定し」という部分に記載している。

○ ランダムに指定するという部分については、もっと束で選ぶというニュアンスを出した方が、効率化されているということが一目瞭然で分かるようになる。(1)①、②、③のような何らかの特殊事情、特に③は事故なので、当然事業者は障害報告書なり事故報告書を起こしていると思うが、そういったものについては特に件数は定めないで全て確認するという理解でよいのか。

○ そのとおり。

○ 要員の異動については、適切に規程類に反映されていて監査では何の指摘もなくても、要員が異動したというだけで、選ばれてしまうのか。そうでなく、適切に体制図等をフォローしており、監査でも指摘されていなければよいということであれば、特に「要員の異動を含め」という頭書きは不要ではないか。

○ 細かな表現の問題だけのような気がするが、要員の異動があった場合には、事業者は当然組織図や任命・解任の記録を作成しており、指定調査機関もその資料を確認しないと調査ができない。従来も確認しているものであるため、「要員の異動」は、(1)では特だしされているものの、今までどおりではないかと思う。

○ (1)①、②、③については、従来どおりということを感じる。むしろ大きく変更になっているのは(2)の方で、サンプリングを事前に指定されたものを準備してやるか、現地で選定したものをやるかでは、事業者の保管方法によって多く違いが出る。棚からひとつかみ方式だと、発行の方は順番に並んでいるので楽なのだが、失効の方は、その失効申込書に紐付く発行申込書についてはバラバラに散っているため、それを突き合わせて準備するのは大変である。ただ、調査の当日が忙しいのか、前日が忙しいのかの違いでしかないので、当日の忙しさが上がるということであれば、現地調査時の時間の使い方を事業者と指定調査機関でよく考えなければならない。

○ 失効については粒度が細かいため、資料 3 には書き切れなかったのだが、失効事由によっても手続が異なってくると考えられるため、指定調査機関でこの案件を指定するということはしないが、失効事由が異なる毎に従来通り事前に準備していただくという形で、負担軽減が図れたら良いのではないかと考えている。今回は核となる方針について、構成員のご意見を賜るためにこのような粒度で資料を記載している。かえって事業者の負担が増えるようでは本末転倒であるため、方針についてご議論いただき、その結果に沿って、事業者の都合に応じてフレキシブルに対応していかなければならない。細かい部分については、個々のすり合わせも必要と考えている。

○ 資料の書き方の問題かもしれないが、(1)①のタイトルが「調査表の記載内容に何らかの変更があった場合」とあるが、調査表の記載内容ではなく、調査表自体に変更があった場合とも読めるため修正が必要。また、「調査表の記載内容に変更がない箇所については、JIPDECは明示的に主務省に報告する」となっているが、それは具体的にどういうことか。

○ 例えば、調査表の項番1510は変更がなかった。この項番からこの項番までも変更がなかった。しかし、項番3433は変更があって、その内容はこのようなものだったということを記載するということ。主務省としては、変更の有無についても明示的に報告を受ける必要があると考えている。

○ 資料 3 の記述では分かりにくい。「措置状況、認証業務規程、事務取扱要領等は変更がない箇所は明示する」といった具合に、表現ぶりはできるだけ具体的にした方が分かりやすいのではないか。

○ (1)①、②、③とサンプリング調査との関係がよく分からない。記載内容が変更になったらサンプリング調査を行うということなのか。

○ サンプリング調査には大きく2つがあり、(2)の発行失効に対するサンプリング調査と、(1)それ以外の帳簿に対するサンプリング調査がある。(1)①、②、③の場合に該当した時は、発行・失効状況以外のサンプリング調査について従来どおりの調査を実施すると考えている。

○ そのような趣旨であれば、(1)①、②、③は「全体発行枚数に比例して現行どおり選定するサンプリング」という表現にはなじまず理解しづらいため、書き方にもっと工夫が必要。

○ (2)3 ポツ目の下に、「この場合、業務手順の適正性の確認作業も、現地調査時に発行及び失効に関する実際の作業実施状況を確認し、適正に業務が行われていることを確認することで行うこととしたい。」となっているが、これは50件のサンプリング案件の1件ずつでその業務の適正性を確認するのか。

○ そのようなことは考えていない。サンプリング調査と業務の適正性確認の調査については、言葉の連動性はなく、切り離して考えている。業務の適正性確認については、実際に現地調査の日に発行・失効されるものの作業について実地調査で見るということをイメージしている。

○ そのイメージだと、現地調査時に 1 件ちょっとやってみなさいというように読めるのだが、そういうことなのか。

○ やってみなさいというよりは、普段どおりやっているところを確認するということ。その意味では、発行に当たる日に現地調査を設定する必要がある。郵便の受付をしているところについても、普段どおりの手順を見せてくださいということになる。

○ 特にポイント1について、現地調査の経験者でない人間にとっては難解な内容になっている。経験のない人にとっても誤解の無い読み方ができるように、表現ぶりを見直していただきたい。

2 資料3のポイント2について

○ 資料３ポイント２について、「調査項番 A・B・C・・・・（※研究会で検討）」とあるが、ここで A・B・C に当てはめるような目安はあるのか。

○ 事務局で案を作成した際に、「特に劣化が早いと認められるもの」としては、例えば調査表の 1512、1513、あるいは、1522、1523 といった、大がかりな設備ではなく、我々が事務を行っている普通のビルでも見られる措置を想定していて、こういったものはこの資料でいう固定的な資産といったものには当てはまらないのではないかという疑問があって、論点として提起した。

○ 劣化が特に早いと考えられる適合例があるかどうかというところだと考えているが、特に項番 1500 番台については、ビル側の管理によってかなりしっかり措置がなされているところだと思うため、「劣化が早い」と認められるものはなく、1100 番台、1400 番台及び 1500 番台は一律に検討してよいと考える。。

○ 調査している側としては、この措置がいいかげんだということはほとんどなく、むしろ設備を置き換えた時に、この措置を忘れているというケースがある。劣化したことを理由に指摘したということはほぼない。

○ 例えば 3 年に 1 度調査するとした場合、今年は 1100 番台、来年は 1400 番台、再来年は 1500 番台という形にするか、例えば 3 年に 1 度一気に 1100、1400、1500 を調査するという形にするか、というのがあると思うが、現在はどう考えているか。

○ 現在のところ、今年は 1100 番台、来年は 1400 番台、再来年は 1500 番台という形にばらけていた方が良いと考えている。

○ 以前の研究会において、同じ事象の違う側面を捉まえるという形で、同じ調査事項について何度も別の項番で調査されるという意見があったが、その部分はクリアしているのか。そうで

ないと、3 年に 1 度調査するとしても、結局毎年調査をしていることにならないか。

○ 設備関係の 1000 番台（1000 番台から 1500 番台全体）に関しては、重複しているということはないと思う。

○ 1200 番台のネットワークの設定に関する調査項番は、簡素化の対象外なのか。

○ 対象外である。

○ 今回のポイント2は、変更認定が必要なものは変更認定で見る。変更認定でないものついては、隔年や 3 年で調査を実施するというものだと理解した。

○ 変更認定をする時には、大体何年ぐらい耐用年数がある設備なのかということを確認することにもなるので、その時に聴取した内容に沿って、例えばそれが 2 年なのか 4 年なのか、そういった事情というのもあるため、それに沿って指定調査機関に確認をしてもらうということもあり得るかもしれない。

○ そうすると、まずは調査項番の平準化という方向で動くとして、2 年又は 3 年というのはどうか。

○ 資料や議論の流れでは 3 年ということだが、特に意見がないようなので 3 年ということにする。

○ 1400 番台の暗号装置の件だが、これは認証業務の一番重要な装置でもあり、全く見ないという話ではないと思うが、どのように考えれば良いのか。

○ 暗号装置については、以前だと見た目で認識できた。ハードウェアセキュリティモジュールという大きな箱があり、火を見るより明らかだった。しかし、現在は小型化されており、RA サーバ、IA サーバに内在する筐体の一部として入っているケースもあり、そうすると目視さえできない。どこで確認するのかというと、外していないか、ログから活性化・非活性化しているかを確認するしか方法がない。事業者がこっそりと取り替えているのではないかということを疑い出すと切りがないところ。

○ 過去の事例で気になっている点があるのだが、現行の施行規則では米国連邦標準規格である FIPS140 に準拠している、あるいは、それ相当という言い方でやっている。指定調査機関としても FIPS140 に準拠していることを、認証書を用いて確認しているのだが、過去の事例で、これは事業者というかベンダーの知識不足によるものだと思うが、ファームウェアがバージョ

ンアップされたということで、勝手にファームウェアを変えてしまっていることがあった。FIPS140 の規則上は、ファームウェアをアップデートするとその時点で認証が取り消されてしまう。従って、ファームウェアだけは毎年確認しなければならないのではないかと考えている。

○ そこは確認した方がよいと思う。これは何と言っても認証業務で一番重要な部分である。事業者としても問題ないか。

○ 現状も HSM に関連するソフトウェア、コンピュータ上の汎用性の高いプログラム、ドライバー、ファームウェアのバージョンは確認しており、それはツールで簡単に確認ができるため、毎年確認されても特に大きな問題はない。

○ 必ずしもお願いする内容ではないのだが、一つの事業者で複数の認定認証業務を持っていると、認証設備室を共有している場合もあるため、せっかく現地調査を隔年化しても、結局毎年調査を実施しているという実態になりかねない。その部分はご配慮いただきたい。

○ そこは現在でも悩ましい部分があるが、運用上工夫したい。

3 資料3のポイント3について

○ 資料 3 のポイント 3 について、「調査表に記載されたとおりに該当する帳簿が、該当する保存場所に保存されている。」という部分は、特に契約書などの場合を想定しているが、指定調査機関が調査しない年については、事業者自らが確認し、更新調査年次における事業者自らの確認日付を記載してもらうことで、指定調査機関が見に行くことの代わりとしたいと考えている。

○ 調査頻度については、3 年で良いと考える。

○ 例えば、大震災等があって、その保存倉庫がある場所が環境的に大きな変化があったという場合には、例外的に間の年で確認するということが必要ではないか。

○ その点については、冒頭で説明した「主務省が必要と認め、調査を指示する」という部分でカバーできると考える。

4 資料3のポイント4について

○ 資料 3 のポイント 4 について、事業者が記載する調査表はかなり詳細な措置状況まで記載している場合があるため、大変かと思うが、よろしくお願いしたい。

○ 今回の簡素化によって、変更があった箇所を中心に現地調査を行うことになる。そうする以上、事業者が変更箇所全てに関する記録を適切に管理していることを JIPDEC が確認する必要がある。変更の管理方法について、現在想定されているものがあれば説明願いたい。

○ 現在考えているのは、更新調査の申請時に提出資料で、現在も当該事業者が管理しているドキュメントの一覧を提出してもらっているが、その一覧の中に、当該更新調査の期間（1 年）に変更があった規程について明瞭化していただく。そうすることによって、指定調査機関は 1 年間で変更があった規程が分かる。まずは変更があった規程を確認し、ドキュメント上適切に変更が行われているか確認する。そして、規程というのは必ず関連性があり、下位の規程に変更があれば、たいていは上位の規程に波及する（逆もまた然り）ため、波及する部分についても確認を行い、変更があった部分が調査表のどの項番に影響を及ぼすのかを見極め、調査表に影響を及ぼすということは、調査表の措置状況についてもその変更が適切に反映されていなければならないため、そういった部分で判断していきたい。

○ 例えば、要員管理や設備の改変記録等の調査表に現れない部分についてはどうなるのか。

○ これはあくまでドキュメント上の話であり、要員管理や設備の改変記録については、ポイント 1 に記載しているとおりである。

○ 変更の記録は内部統制をしっかりするということで良いのだが、変更がないことの確認は難しい。暗号装置の中の秘密鍵が維持されているというのは非常に重要なことで、HSM のログを適切に残しておき、ログが継続されていることをもって変更がないことを確認するとか、あるいは、ログが変更できなくなっているとか、そのような仕組みがあれば良いように思うがどうか。

○ ログの改ざん防止措置を行わなければならない点は、現在の署名法では求められていない。また、そういった仕組みをもった装置を導入している事業者もいない。その代わりとして自ら CDR に保存してそれをさらに密封して、ログについて変更されていないことを担保している事業者もいるが、それはあくまで事業者自身による工夫であって、署名法上求められていることではないため、そのような仕組みを導入することは難しい。

○ 暗号装置について変更がないことを確認できるような記録を残しておくという趣旨のご発言は、認証局の秘密鍵が変わっていないかということか。それとも発行の履歴が適切な手順どおりの発行しかないということをログで確認するということなのか。

○ 設備の変更となると、変更というのは割と小さな問題だが、秘密鍵が変わっているとか、改ざんされているというのは致命的な問題なので、それについては守られているということをログ

で保証するという仕組みが必要と考えている。ログの継続性や変更できないというところをもって担保するという仕組みがあれば、他の手続は大幅に軽減できるのではないかと考えている。

○ 秘密鍵が変わっていないということは、ログによらず、署名検証すれば一目瞭然で確認ができるため、ログの監査は不要かと思う。さすがに秘密鍵が変わっていると、発行済み証明書の署名検証をすれば一目瞭然なので、さすがにそれが変わるというのはログで確認するまでもないかと考えられる。むしろ適切な発行以外の発行が本当にないのかという観点でログの監査が必要と考える。

○ 秘密鍵が盗まれていないかということも含むのだが、その点はどうか。

○ HSM からの鍵の漏出に関しては、FIPS140 等でバックアップ以外は HSM から鍵を持ち出すことができないということが求められているため、FIPS140 等の認証を取得済みの製品であれば、技術的に担保されているといって差し支えない。

○ 秘密鍵が盗まれるであるとか、秘密鍵が不正に鍵更新されていたといった話は、HSM 等を使った認証局の仕組みが確立して以来、一度も聞いたことがない。しかしこの正規の秘密鍵を使って不正な署名操作が行われるといったことに関して、近年いろいろな事件が起きている。特に 2011 年にオランダの認証局 DigiNotar が攻撃され、結果、不正な SSL 証明書が発行されてしまったという事件があり、この不正発行が認証局において検出できなかったという問題がある。こうした問題の対処は、今後強化を考えなければならないと思っている。

○ 一般的な話としてログ等は重要であるため、改ざんできない仕組みを、今後様々な方法を検討していかなければならない。特に電子署名を扱っているため、保存対象のログに対し電子署名を打った上で保存するなどの方法も考えられる。ただ、現在の法律では特に記載がないため、そこは運用で今後どうしていくかということではないか。現在のところ、今実施している調査の方法、認定の方法でそこは十分担保できているのではないかと考える。

5 その他

○ 資料 3 のポイント 1 については、帳簿保存の確認をすることと、1 件ずつの業務の手続が適正であったかを確認することが混ざってしまっているので、書き分けたらどうか。

○ 資料 3 については、事務局で引き取っていただき、文章を修正した上で、委員に流して確認したという段取りにしたい。

○ 現地調査の簡素化については、いつから適用されるのか。来年の 2 月に実施する実務者説明会で説明した上でいつから実施するということを明示してもらえるとよいのだが。

○ おっしゃるとおり、制度を変える場合は、周知期間をおいて、双方理解した上でということが重要。そのタイミングにまさに実務者説明会を活用するということで、主務省と指定調査機関ですり合わせを行いたい。