第３２回保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議　専門作業班合同会議

日時 令和７年５月30日(金) １６：００～

場所 AP 虎ノ門　A ルーム

（１）MEDIS 認証局　鍵更新結果の報告

○佐々木情報推進官　それでは定刻になりましたので、ただいまより、第 32 回保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議及び専門作業班合同会議を開催いたします。皆様方におかれましては、大変お忙しい中、本会議にご出席いただきまして誠にありがとうございます。本日の会議は、現地とオンラインのハイブリッド会議での開催とさせていただいておりまして、公開での開催、資料については一部公表とさせていただいております。また、正確な議事録作成やご意見を賜わったときの整理を事務局で正確に行うため、録画をさせていただきますこともご承知おきください。

次に、構成員の追加と交代のご連絡です。今回より専門家会議構成員として、明治大学総合数理学部専任教授の菊池先生に加わっていただいております。また、専門作業班構成員をお願いさせていただいておりました日本薬剤師会認証局河野様に代わり、今回より日本薬剤師会認証局石川様にご参加をいただいております。改めてよろしくお願いいたします。

本日の会議の構成員の参加状況ですが、丸山構成員、山本構成員がオンラインの参加となっております。佐古構成員に関しましては、遅れて参加見込みとのことで聞いております。

議題に入る前の留意事項ですが、速記業者が議事録を作成する際に、どなたが発言されたか分からなくなるため、皆様におかれましては、ご発言をする際、名前をおっしゃってからご発言をいただくようご協力お願いいたします。また、お手元のマイクですが、こちらも発言時のみオンにしていただくようにお願いいたします。

次に、資料の確認をさせていただきます。本日の資料は、議事次第、資料１、資料２―１、２―２、２―３、２―４、２―５、２―６、参考資料１、参考資料２をご用意しております。資料の不足等ございましたら事務局までご連絡をいただければと思います。それでは、松本座長、以降の進行をよろしくお願いいたします。

○松本座長　皆様、こんにちは。松本です。本日の議題は、MEDIS 認証局の鍵更新結果報告と今年度の準拠性審査班の指名、それから暗号アルゴリズムの移行に関しての議論となります。それでは早速ですが、議題１につきまして事務局よりご説明をお願いいたします。

○佐々木情報推進官　厚生労働省事務局でございます。それでは改めまして、資料１に沿いましてご説明を差し上げます。

まず、MEDIS 認証局の鍵更新結果に関して概要を事務局から説明させていただきます。資料１の４頁目をお願いいたします。前回の第 31 回 HPKI 専門家会議にて、日本医師会認証局の鍵更新結果についてご報告を差し上げましたが、同様に MEDIS 認証局におきましても鍵更新が行われましたので報告をさせていただきます。今回も日本医師会認証局のときと同様に、丸山先生、六川先生に立会をお願いさせていただきました。当初予定していた日程のとおりですけれども、２月 14 日にキーセレモニーを実施、その後、切り戻しを行い、約１か月後の３月 17 日に切り替え作業を行っております。この両日ともにおいて、丸

山先生、六川先生においては立会をいただいております。立会結果及び立会時のチェックリストにつきましては、参考資料２として添付をさせていただいておりますので、そちらをご確認いただければと思います。なお、鍵更新作業の完了後、HPKI の主たる利用用途である電子処方箋において、本件に起因したと思われるトラブルは、現時点では報告されていない状況にございます。

概要は以上となります。実際の立会内容については、丸山先生よりご報告をいただきます。それでは丸山先生、ご報告をお願いいたします。

○丸山構成員　丸山でございます。参考資料２にございますとおり、六川先生と私とで、MEDIS認証局の鍵更新のキーセレモニーの立会に行ってまいりました。記載のとおり、全ての作業は作業手順とおりに行われ、トラブルなく鍵更新が終了したと思っております。その結果については、資料２のとおりでございます。以上でございます。

○松本座長　丸山先生、ありがとうございました。それでは、この MEDIS 認証局の鍵更新の結果につきまして、ご質問ございますでしょうか。オンラインの方もよろしいでしょうか。

○山内構成員　作業班の山内です。JIPDEC で認証局等の評価の仕事をしています。MEDIS 認証局の鍵更新の結果は、資料２―１の保健医療福祉分野 PKI 認証局署名用証明書ポリシを使いながら確認していると理解をしていますが、少し気になるところが資料２―１にございましたので、クラリファイをさせていただきます。

まず、43 ページについて、今回私どもも初めて気づいたのですが、６．１．５項の鍵のサイズのところで、認証局の CA 証明書の鍵の最小サイズは、2048 ビットになっていますが、「エンドエンティティの証明書の鍵の最小サイズは、RSA アルゴリズム又は技術的に同等のアルゴリズムの場合、1024 ビットとする」と記載されています。私ども JIPDEC は、電子署名及び認証業務に関する法律の指定調査機関を 23 年ほど行ってきていますが、2020 年までの間に、既にエンドエンティティの電子証明書の鍵長は 2048 ビットになっており、2020 年には主務省である法務省・総務省・経済産業省による施行規則も改正されて、2048 ビットになっています。そのため、現在、認定認証業務として発行するエンドエンティティの証明書の鍵長は2048ビット以上になっています。また、マイナンバーカードの署名用電子証明書につきましても、秘密鍵の鍵長は 2048 ビットになっています。HPKI の認証局が発行するエンドエンティティの証明書は、まさに HPKI カードの中の秘密鍵に紐づいていると思いますが、それは1024ビットでも構わないということでしょうか。これが１つ目の質問です。監査人に対してではなく、事務局に対しての質問になるかもしれません。

○松本座長　では、事務局から回答できますか。

○佐々木情報推進官　ご指摘ありがとうございます。いただいた点について、今の時点で我々のほうで把握をできておりませんので、一旦持ち帰らせていただいて、後ほどご回答させていただきたいと思います。

○山内構成員　監査の内容に対する質問ではなく申し訳ありませんでしたが、エンドエン

ティティの鍵長は極めて重要で、記載にミスは許されませんので、ぜひご確認の上、必要があれば対処いただきたいと思います。

もう一つ、監査人に対して、参考資料２の HSM に関する部分について質問があります。参考資料２の立会報告書（MEDIS 認証局鍵更新）の監査様式３／３ページ、手順項番 5-15、新鍵（更新後の鍵）へのラベル付与について確認結果として HSM の機種名「ProtectServer Internal Express 2 （PSI-E2)」が明記されています。CMVP という北米での HSM を含めた暗号モジュールに関する適合性評価制度のウェブサイト等を確認したところ、「ProtectServer Internal Express 2 （PSI-E2)」に該当する HSM は４台あり、全てステータスがヒストリカルになっていました。ヒストリカルだからといってすぐに問題があるということではありませんが、基本的には HSM は、できるだけ最新の状況で基準に適合していることが認証されているということが望ましく、安全サイドに立ちますと、アクティブとなっている機器であることが望ましいです。

繰り返しになりますが、ヒストリカルだから危険ということではありませんが、ヒストリカルであることを確認されたかどうか、また、ヒストリカルであっても当面問題ないとご判断されたかどうかについて監査人に対してお聞きします。以上です。

○松本座長　ご質問ありがとうございました。監査をしていただいた丸山先生、六川先生、いかがでしょう。

○丸山構成員　まず丸山からお答えいたしますと、我々としては、記載のとおり、ProtectServer Internal Express 2 であることを確認しており、それがヒストリカルかアクティブかということまでは確認しておりません。

ただ、ヒストリカルであるからといって、直ちに危胎化しているという問題ではないと思っています。そのため、準拠性監査やキーセレモニーにおいてはこれでよく、最終的には問題ないという結論にしております。以上でございます。

○山内構成員　ご回答ありがとうございました。この会議の開催趣旨とは異なるのですが、現在デジタル庁で「電子署名及び認証業務に関する法律」のモダナイゼーションを進めており、暗号モジュールである HSM について、どのように信頼性を確認するか議論がなされているところです。デジタル庁は、６月１日まで、「電子署名及び認証業務に関する法律施行規則の一部を改正する命令案等」に対する意見募集を行っておりますので、パブリックコメントの結果も踏まえながら、HSM についての評価の仕方について、できる限り整合性を取るようにしていただきたいと思います。私からの発言は以上です。

○松本座長　ありがとうございました。２つ話がありまして、１つは今回の鍵更新について立会の内容をご報告いただいた件と、もう 1 つは、そのベースとなっているポリシについて、アップデートしなければいけないのではないか、あるいは誤りを正さなければならないのではないかというご指摘だと思います。後者については、事務局で持ち帰るということではございますが、幸いにも、次の今日の議題に資料もございます。今、リファレンスとして資料２―１をポイントしていただきましたが、その少し先のページにも、関係す

るところがありますので、この件についても、後で議論の項目に加えられればと思います。
　専門家会議の委員の皆様、六川先生と丸山先生のご報告について、何かご異議等ございますでしょうか。
○矢野構成員　異議ではなくて補足となりますが、先ほどの HSM がヒストリカルである件は、皆様方も認識されていると思いますが、我々は認識しておりますので、今年のリプレイスで交換いたします。そのため、ヒストリカルは認識した上で安全性に問題ないということで、現在使っております。
　また、先ほどご指摘があった 1024 ビットの件は、このポリシが作られたのが平成 17 年であり、最低のビットが 1024 ビットということで、現時点では、日医認証局、MEDIS 認証局は 2048 ビットを使っております。以上、ご報告です。
○松本座長　補足いただき、ありがとうございます。
　ありがとうございました。続きまして MEDIS 認証局の準拠性審査につきまして事務局よりご説明をお願いできますでしょうか。

（２）MEDIS 認証局　準拠性監査審査班の指名
○佐々木情報推進官　松本先生、ありがとうございます。事務局より続きまして、MEDIS 認証局の準拠性監査の審査班の指名についてご説明をさせていただきます。
　資料１の６頁目をお願いいたします。HPKI 専門家会議にて、サブ認証局に対して行っております２年に１度の準拠性審査についてです。MEDIS 認証局の審査ですが、前回 2023 年９月８日に行っておりまして、規定に従い、そこから２年以内に実施を行う必要がございます。詳細な日程は現在調整中でございますが、本年９月８日までに実施を行う必要がありまして、準拠性審査の際の審査班を HPKI 専門家会議より選出いただく必要がございます。今回の審査対象は、前回の MEDIS 認証局の審査時と同様に、HPKI サブ認証局の通常の準拠性審査に加えまして、MEDIS 認証局ではトラストサービスプロバイダーとして HPKI リモート署名サービスの運用も行っておりますので、先般改訂を行わせていただきました HPKI リモート署名サービス評価基準に従って、そちらのリモート署名の準拠性審査も併せて実施の予定となっております。
　これら、今回の準拠性審査につきまして、審査班は専門的観点が求められますことから、これまでの実績も踏まえまして、再度にはなりますが、丸山先生、六川先生にお願いをさせていただけないかと考えている次第でございます。事務局からは以上となります。ご審議のほど、お願いいたします。
○松本座長　ありがとうございました。ご意見いただけますでしょうか。
　特になければといいますか、ぜひお二人にお願いできればと思いますが、よろしいでしょうか。
〔「異議なし」と呼ぶ者あり〕
○松本座長　ありがとうございます。それでは、丸山先生、六川先生を審査班として指名

させていただきます。
○丸山構成員　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。では、続きまして、ドキュメントの改訂に関しまして事務局よりご説明をお願いいたします。資料には、厚生労働省の組織名変更に伴うという接頭語がついておりますが、先ほどの議論から、内容に対してどのように対処していくべきかというところもご意見をいただければと思っております。では、事務局よりご説明をお願いいたします。

（3）厚生労働省組織名変更に伴うドキュメント改訂
○佐々木情報推進官　厚生労働省事務局よりご説明をさせていただきます。
　資料1の8頁目をお願いいたします。今年度より、HPKI 認証局を所管させていただいております私ども厚生労働省の組織名が変更となっております。記載させていただいているとおり、もともとが「特定医薬品・医療情報担当」という形になっておりましたところ、「特定医薬品」が外れまして、「医療情報担当」のみという形に修正をさせていただきたいと思います。
　これに併せまして、ポリシ等の各種ドキュメントにおいて、お問合せ先というところで厚生労働省の記載がございますので、一律これに併せた改訂を実施させていただきたいと思います。改訂箇所に関しましてはかなり多くなりますので、個別での説明は差し上げませんが、改めて資料2―1から資料2―6に赤字で記載をさせていただいております。こちらに関してはお手元の資料にてご確認をお願いいたします。
　また、先ほど、山内構成員からご指摘いただいた点に関しまして、事務局としましても、このポリシ自体、先ほど矢野構成員からお伝えいただきましたが、かなり昔に作っていただいたものであって、少しアップデートが足りていないという認識がございます。この後、資料1の先になってしまいますが、最後、連絡事項のところで、今年度の取組としまして、どういったものをこの HPKI 専門家会議で話していくか、議題案をご用意させていただいております。その中に事務局からのご提案として、ドキュメントのアップデートもやっていきたいと、この専門家会議の中でもお話をさせていただきたいと考えておりますので、次回までに、今回いただいた宿題部分はもちろんお返しをしますが、それ以外のところにつきましても、次回以降アップデートに向けた改訂というところは、引き続き進めさせていただければと思っております。事務局からは以上になります。松本先生、よろしくお願いいたします。
○松本座長　ご説明と対処の方針につきまして、お話をいただきましてありがとうございました。皆様からご質問などございますでしょうか。
○林構成員　林達也です。かなりのボリュームの量の修正、本当にお疲れさまです。この手の文書ポリシで、こういった修正はよく起きて、当然セレモニーとしてはやはり必ず確認をしなくてはいけないということは、非常に重要なことになってくるのは、皆さんご承

知のことだと思います。一方で、組織名等の変更は必ず起きるので、できれば該当する部分を縮小しておく努力を、こういったドキュメントを書く人たちはすると思います。今回結構なボリュームがあるので、次のロードマップのお話もありましたが、変更があったときのダメージというか、変更部分の縮小化も改訂のときに少し意識してできると、そういった修正がなるべく少なく済むと思うので、考慮できればと思ったというコメントまでです。以上です。

○松本座長　ありがとうございます。もっともかと思います。要するにポイントする先をまとめて、同じ記号でここを見よとすれば、解決するなどという工夫が必要だろうということですね。

○林構成員　はい、全くおっしゃるとおりです。

○松本座長　ほかにございますでしょうか。

○宮内構成員　宮内でございます。先ほど、山内さんからご指摘いただいたのは、例えばこの資料２―１で言いますと、どこになりますでしょうか。

○佐々木情報推進官　43 ページの６．１．５になります。

○松本座長　暗号モジュールはその次のページです。44～45 ページに、「FIPS　140-2 レベル３と同等以上」という表現があり、この部分も正さないといけないと私も思っております。

○宮内構成員　この部分を中心に変更し、関連部分も変更することをご提案いただくという趣旨で伺ってよろしいですか。

○松本座長　そう理解しております。

○宮内構成員　分かりました。どうするか難しいところはあります。現在使っている人がどうなるか等の事情も踏まえて、経過措置をつけるなり、無理のない形で新しいものに変更していくことになろうかと思いますので、ご検討よろしくお願いします。私からは、以上です。

○松本座長　ありがとうございます。そのほかございますでしょうか。

○濱口構成員　慶應 SFC の濱口です。先ほど、矢野さんからヒストリカルであることは既に承知していて、安全だと確認されたというところについて、監査人に対して、こういう根拠でヒストリカルにはなっているが安全だとご説明されたという認識でよろしいでしょうか。

○矢野構成員　ヒストリカルであることはご説明した上で、データベースに出ている資料もお見せして、認識はしておりますと、説明はしております。それを踏まえてどうするか指示・要求を受けるのは我々ですが、現状の認識については説明しております。

○濱口構成員　再度、慶應 SFC の濱口です。ヒストリカルになった理由は、恐らく暗号アルゴリズムの部分が使われていないから安全だという理解でよいでしょうか。

○矢野構成員　そこまで細かいところまで掘っておりません。ヒストリカルであるが、今回の我々が使っている HSM に関しては、安全性能に関しては大丈夫だと、委託事業者か

ら報告を受けている形になります。
○濱口構成員　通常であれば、もちろんFIPSの認定されたバージョンを維持して使っていったり、アップデートされた新しいFIPSの認定されたバージョンでどんどん取り直していったり、かつ要求事項として 140-2 レベル3相当というのがあるのであれば、認証局側に自分たちの使っている HSM が運用期間中、FIPS の認定から外れないように継続的に監視する責任があると思われます。通常であれば、ヒストリカルになったからといってセキュリティ上いきなり問題があるわけではないというのは事実ですが、なぜ問題ないと言えるのかという分析は、認証局側ですべきだと認識しております。
○松本座長　もっともだと思いますが、一番の根本は、基準といいますか、ルールのほうが曖昧であることです。かつそれをどのように解釈して実務を運用していくのかも、きちんとその粒度では規定されていないところが私は課題だと思っていまして、そういうところを改善していく必要があるのではないかと思います。皆様、それぞれもっともなご意見をいただきまして、大変ありがとうございます。よりよいものにしてまいりましょう。よろしいでしょうか。それでは、ドキュメントを改訂していく件につきましては、以上とさせていただきます。
　それでは、続きまして、暗号アルゴリズムの移行に関しての議題です。まず事務局よりご説明をお願いできますか。

（4）暗号アルゴリズムの移行に関して
○佐々木情報推進官　松本先生、ありがとうございます。厚生労働省事務局よりご説明をさせていただきます。
　暗号アルゴリズムの移行について、資料1の10頁目をご確認お願いいたします。まずは前回の議論の振り返りをさせていただきます。前回第31回HPKI専門家会議では、暗号アルゴリズムの移行が2030年までに必要とされている背景と、併せて国のほうで運用をしております、ほかの公開鍵基盤である GPKI を参考例として提示をさせていただきご議論をいただきました。議論の結果としまして GPKI にて採用をしている ECDSA（鍵長 384 ビット、192 ビットセキュリティ）を踏襲する方向で HPKI についても検討ができないかというところで、改めて HPKI の利用用途や、システム状況等も踏まえながら調査検討を行っていくというところで認識が一致をしていると、確認をさせていただきました。また、併せて移行時期、スケジュールについても議論の中に入っておりまして、GPKI では 2028 年以降というスケジュールで進められているというところに対しまして、改めてやはり 2028 年であったとしても、それが特段早いわけではなく、ベンダーの開発期間やコストなども HPKI では変動要素になり得ますので、そういった部分も含めて考慮をしながら早い段階で議論を行い、十分な期間を設けて移行に進めていく、移行の計画を立てていく必要があるというところで承知をしております。
　続きまして、宿題事項となっていた現状の調査状況についてでございます。11 頁目をお

願いいたします。前回事務局への確認指示として具体的に頂いておりました、デジタル庁に対して GPKI にて ECDSA P-384 を選定している理由を聞き取って確認をしてくださいと宿題を頂いていた次第です。こちらに関してデジタル庁へ確認をさせていただきました。結論としましては、ECDSA P-384 につきましては、デジタル庁内部にて選定作業を行ったところでございまして、何かしら具体的にその選定の過程や理由につきまして公表をしているものはございませんでした。このため、明確な選定理由として、公的なものとしてお示しをできるものはございませんが、デジタル庁の担当者に具体的に我々からヒアリングをさせていただいて、選定時に挙がっていたポイントについて幾つか確認をすることができました。具体的には、移行において 128 ビットセキュリティとした場合は、2041 年で再度の移行を求められてしまい、利用期間が短くなってしまうということを懸念して、192 ビットセキュリティにすべきではないかという意見が内部で挙がったと聞いております。また、192 ビットセキュリティにおいても RSA を使用する場合には、鍵長が 4096 ビットより大きくなることから、対応している IC カードやシステム等が現状少ないことと、さらに処理時間そのものも増加してしまう懸念があるということが、懸念点としてデジタル庁内で議論がされたと聞いている次第でございます。デジタル庁への聞き取り結果は以上となっておりますが、これらも踏まえつつ、改めて HPKI で ECDSA P-384 を選択することに対し、どのようにこの後調査を進めていくかというところを事務局にて素案を用意させていただきましたので、続いてご説明を差し上げたいと思います。

12 頁目をお願いいたします。調査項目を選定するに当たって、対応するステークホルダーごとで分けて考えております。最初に HPKI を発行する認証局について、次期暗号に対して認証局システムの更新の必要がございます。まずは、対応するシステムを構築することができるのかどうか、具体的に電子証明書発行だけでなく、IC カードにつきましても運用することが可能なのかどうか、また移行期間における運用方法の対処が可能かといった点を軸に資料には記載をさせていただいております。このような内容でまずは調査を進めたいと思っております。2 番目に署名者につきまして、次期暗号においても、HPKI 自体の利用シーンそのものは変わりがないと考えておりますので、現在、主として利用されている電子処方箋を中心に電子カルテ等の医療情報システムで対応が可能なのかどうか、署名に必要な計算処理時間なども加味して、現場で受け入れられる程度のパフォーマンスを維持することができるのかどうかといった点を中心に調査を進めさせていただければと思います。

おめくりいただきまして 13 頁目になります。続いて署名の検証者においても、署名者同様の調査を考えております。電子処方箋においては、検証者が薬剤師となりますので、主に薬局側の調剤システム等について調査をさせていただければと考えております。続いて、下段、関連するサービス等についてです。具体的には、先ほどから申し上げております主たる利用先である電子処方箋管理サービスにおいて、クラウド上のサービス本体でも検証作業がございますので、そういった仕組みに関しても調査の対象とすべきではないかと考

えております。また、同じくリモート署名サービスにおいてもクラウド上に構築されており、こちらにつきましても用途としてもちろん利用できる必要がございますので、ECDSA P-384 で利用可能な形を維持できるのかどうかという点で調査を進めさせていただければと思っております。

おめくりいただきまして 14 頁目でございます。では、具体的に調査方法としてどのように確認を進めていくのかというところを記載させていただいております。今の段階ではあまり具体的な記載までは進んでおりませんで、申し訳ございませんが、大まかな方針として見ていただければと思います。まず、認証局システムに関しましては、もちろん現在、我々厚生労働省のほうでルート認証局を持っておりますので、これらルート認証局の委託先の事業者や、サブ認証局の皆様にもご協力をいただきながら、確認・調査を進めてまいりたいと思っております。また、署名者、検証者に関しましては、基本的に医療情報システムの中で利用されることになりますので、過去にも HPKI 関連をご協力いただいている背景から、JAHIS（保険医療福祉情報システム工業会）に依頼をさせていただけないかという調整を進めてまいる所存でございます。また、関連するサービス等につきましても、先ほどお話をさせていただいたとおり、リモート署名サービスにつきましては、MEDIS 認証局にお願いをさせていただきながら協力体制として調査を進めてまいりたいと思います。電子処方箋管理サービスや電子カルテ情報共有サービスといったサービスにつきましては、医療 DX 施策として運用をお願いしております社会保険診療報酬支払基金に対して、確認・協力を要請させていただく形で調査を進めたいと考えております。

以上が事務局側で想定している調査内容となっております。前回のご議論を受けまして、ECDSA を前提とした場合の今後の進め方というところで、まずはご議論をいただければと思います。松本座長、以降よろしくお願いいたします。

○松本座長　ご説明ありがとうございます。それでは、暗号アルゴリズムの移行に関しまして、ご意見ある方は、挙手または電子的な挙手でお願いいたします。いかがでしょうか。

○横田構成員　兵庫県薬剤師会の横田です。先ほどの電子処方箋のところで薬局という名前が出てきましたが、資料上読み取れなかったので、詳細を教えていただけますでしょうか。

○佐々木情報推進官　事務局でございます。薬局と申し上げたところは、13 頁の検証者の補足としてでございます。実際には資料には記載させていただいているとおり、検証プロセスを行っている先に確認をさせていただきたいというところで、具体的に電子処方箋の中で、HPKI による電子署名の検証者としましては、薬局の調剤システムにおいて署名検証を行っていることから、実際その調査先としましては、調剤システムを含めて調査を行わせていただきたいと考えております。

○横田構成員　分かりました。これはあくまでも調査項目の案なので、これからもう少し具体的に、今、補足があったような内容が記載されていくのか、この内容でもって実際に項目案として進めていくのか、どちらでしょうか。さらにこれから詳細版が改めて出てく

るという理解でよろしいですか。
○佐々木情報推進官　はい。調査と並行して行ってまいりますので、まずは調査できるところは、先立って進めさせていただこうと思っております。この HPKI 専門家会議の次回の開催日程がまだ決まっておりませんが、調査状況に合わせて開催をさせていただければと思っておりますので、今後もちろん詳細な記載はさせていただきますが、併せて今回ご議論いただいた内容は、一旦事務局で宿題として持ち帰らせていただき、その内容をできる限り次回までに調査して、次回またお諮りさせていただこうと考えております。
○横田構成員　ありがとうございます。もう一点よろしいですか。前回もたしかコストの話が出ていたと思います。結局これを入れることによって、実際に、電子処方箋を運用している医療機関や薬局に新たなコストがかからないようなところを、最終的には私の所属から言っても望んでいるところではあります。最初のスタートからエンドまでのところでいろいろなものが出てくることは十分理解しているものの、やはりコストのところが最終的に負担がないようにしていただきたいと思いますので、この調査項目の中でコストも少し意識していただけたらと思います。要望でございます。以上です。
○松本座長　ありがとうございます。何かコメントはございますか。
○佐々木情報推進官　事務局でございます。承知いたしました。今、調査項目案のところは、基本的には、そのシステム・技術的なところで移行が可能かどうかを主に記載させていただいておりましたが、ご意見いただきましたとおり、もちろんコストに関しましても実際の医療現場において重要視される部分でございます。その部分も改めて、今、認識をさせていただきましたので、今後調査の項目に入れて進めさせていただきたいと思います。よろしくお願いします。
○松本座長　ほかにございますか。
○林構成員　林です。今のコメントを聞いてしまったのでちょっと欲が出たところがあります。コストのことを検討するということは、恐らくスケジュールのことも検討する必要があるだろうと思っております。どんどん調査項目が増えてしまい事務局にはご負担をかけてしまいますが、もしやるとしたらコストに対しては多分時間、スケジュールもセットで出てくるだろうというところで、追加をお願いしたいと思っています。項目を増やしてしまい大変恐縮ですが、コメントさせていただいた次第です。以上となります。
○佐々木情報推進官　事務局でございます。ありがとうございます。もちろんスケジュールに関しても、調査項目としてはもともと想定をしておりまして、前回の第 31 回会議のときに、山本先生からも、ある程度の時間を設けなければ、ベンダー側の開発期間が短くなってしまうとコストがかかるのではないかといったご指摘も前回いただいておりますので、そういった点も併せながら調査は進めてまいります。併せてもちろん 2030 年までという期限もございますので、そことの整合というところで、事務局よりある程度の素案というところは、まずは次回もしくは次々回に出させていただこうと思っております。よろしくお願いします。

○宮内構成員　宮内でございます。先ほどの検証者の話に関係するところで、検証者というのは誰を想定されているかというのが、電子カルテについてよく分からないなと思っています。例えば電子カルテの開示を求めた患者、それからそれを提出された裁判所、あるいは調停や仲裁等のいわゆる ADR、そういうところでこれを検証する可能性も一応ありそうな気はしますが、今回の調査で検証者というのは、どこまでを想定してヒアリング等を行うのかを教えてください。
○佐々木情報推進官　事務局でございます。ご指摘ありがとうございます。現在、想定していた検証者に関しましては、先ほど申し上げたような具体的にその薬剤師側のシステムであったり、平時の運用の中で利用される電子処方箋管理サービス、クラウド上のサービス本体であったり、そういった部分をまずは想定しておりました。確かにご指摘いただいたとおり、裁判等になりますと、そのような方、場合によっては検証者としてほかの部分が、平時ではないものが登場するところもございますので、そちらも併せて調査項目として入れさせていただきたいと思います。ありがとうございます。
○宮内構成員　電子処方箋は分かっているつもりですが、電子カルテ情報共有サービスを実際に検証する人はシステム上、誰と考えているのかが分からないので、そのあたりをお聞きしたかった次第です。
○柴田構成員　現場で電子カルテを使っている柴田です。現在 HPKI の用途として、医療機関側が認識しているのは電子処方箋における署名行為であって、診療記録及びその記載内容に対する署名そのものは行われていないのが現状です。そのため、検証する対象が存在しないと認識しています。以上です。
○矢野構成員　多少補足すると、例えば、紹介状は法廷ではないにせよ、電子署名を打ったとすると、それは診療諸記録になりますから、電子カルテとセットで保存されている記録となります。そちらのほうは何かあれば、もちろん検証したとして裁判で提出せよと言われれば裁判官等に回ってきますが、電子カルテそのものに対しての署名行為は、現時点においてはありません。
○宮内構成員　事情は大体分かりました。ご説明の中で、署名者のあたりで、電子処方箋と電子カルテが対象だとおっしゃっていたので、電子カルテも当然この後のほうでも関係するのかと思っていましたが、現在は特別そういうことは行われていないから、今後のことも考えて、ヒアリングすることが考えられるが、現在のシステム上そうなっているわけではないという理解でよろしいでしょうか。
○佐々木情報推進官　ご理解のとおり、先ほど矢野構成員からお伝えいただいたような、いわゆる紹介状につきましては、今後、想定をしておりますので、そこの部分に関しては、その想定の中で、もちろん調査の項目としては含む形で行わせていただきたいと思っております。
○佐古構成員　佐古です。今回、調査対象の署名アルゴリズムとして ECDSA というキーワードだけが挙がっています。ECDSA の細かいパラメーターについてよく分かっていな

いのですが、曲線がどういう曲線かによって安全性が変わったり、実装が変わったりするということがあるのではないかと思っています。今回 ECDSA P-384 というキーワードも出てきていますが、その ECDSA のバリエーションについては、どういう範囲で調査されようと思っていますか、というのが１つ目の質問です。

２つ目は、先ほど山内さんからエンティティ証明書の鍵の長さということもありましたが、今回、認証局が証明する鍵の長さなのか、エンティティが持つ鍵の長さなのか、それを今は RSA だと別にしているようですが、ECDSA では同じようにするのかということが確認したかったです。

３つ目は、先ほど口頭で説明していただいた内容が、14 頁の資料に含まれていないと思っておりまして、最後の関係するサービス等のところでは、前の 13 頁には HPKI セカンド電子証明書の話がありますが、14 頁には、こちらに対する調査対象が書いていないと思いまして、ここを確認したいです。また、13 頁では、新証明書をクラウド保管するためという、割とライトウェイトなストレージがあればよいと読めますが、実は内部ではいろいろな処理をしないといけないと思っておりまして、そこが RSA ではなくて ECDSA になることによって、想定されていた安全性が担保できるのかというのも大変気になっております。佐古からは、以上３点でした。

○佐々木情報推進官　事務局からお答えをさせていただきます。

まず、ECDSA のバリエーションにつきまして、今の時点で本日具体的なものを何かお示しできるということはございませんが、基本的には一番最初に申し上げましたとおり、GPKI で選定されているものを、HPKI に関しましても同じ政府系の認証基盤、もちろん相互認証は行ってはおりませんが、同じ認証基盤でございまして、実際その JPKI につきましては GPKI と相互認証しておりますので完全に踏襲するということで聞いておりまして、あわせて HPKI のほうも、できればそういった形で同じ政府として踏襲できないかというところの検討からスタートをしております。

ですので、具体的にそのバリエーションがどうなっているのかという点は、今、明確にお答えはできないのですが、こちらはデジタル庁が所管しております GPKI で、具体的にどういったバリエーションを使うのかというところを我々、事務局のほうで確認させていただきたいと思います。

２つ目でございますが、エンドエンティティの鍵長と認証局の鍵長が異なるのかどうかという点につきましては、この専門家会議の中で今こういった具体的にセキュリティの懸念としていただきましたので、この専門家会議の中で引き続きご議論をいただければと考えております。

３点目でございますが、14頁目の関係するサービス等のところでございますが、13頁目ではリモート署名サービスについての記載がありましたが、14 頁目では記載が漏れておりまして、大変失礼いたしました。関係するサービスの中で、もちろんその鍵を預かる作業を行っておりますリモート署名サービスも関係するサービスでございますので、こちらに

関しましては、実際現在運用をしていただいております MEDIS 認証局と協力をさせていただいて調査を進めていきたいと考えております。よろしくお願いします。
○松本座長　最後の点は、先ほど口頭ではおっしゃっておりましたね。よろしいでしょうか。ありがとうございます。
　私もいろいろ言いたいことがあるのですが、まず皆様のほうからいかがでしょうか。そのほかございませんでしょうか。
○菊池構成員　明治大学の菊池です。松本先生の質問が待っているので、手短かに伺いたいと思いますが、移行に関して、旧アルゴリズム RSA と ECDSA が混在する時期はありますでしょうか。時期的には、あと 5 年で 2030 年を迎えることになるわけですが、マイナンバーカードの場合ですと、5 年ごと 10 年でエクスパイアしますので、当然、今発行されたマイナンバーカードと、新アルゴリズムが入っているカードが混在する時期があると思いますが、そこはどのようになっているのか教えてください。
　実際には、混在している時期を考慮して移行をなさるのか、それとも、旧アルゴリズムは強制的にエクスパイアさせて新アルゴリズムにして移行するのか、いろいろな考え方があるのではないかと思いますが、どのようになっているか、もし決まっていましたら教えていただければと思います。
○佐々木情報推進官　厚生労働省事務局でございます。結論としては、混在する時期があるという認識でございます。HPKI におきましては、有効な期間が 5 回目の誕生日までという形になっておりまして、約 5 年間ということでございます。今回、暗号移行に当たりましては、新しい認証局のシステムとして次期暗号において認証局システムの立ち上げを行う形になっております。そういう形で予定しておりますため、いわゆる約 5 年間に関しましては、少なくとも並行運用を行う期間があるというところで承知をしておりまして、今回の調査に関しましても、そういった形で並行運用を前提として移行が可能なのかどうかという点も併せて調査を行いたいと考えております。
○菊池構成員　十分配慮済みであることを承知いたしました。そうなりますと、認証局、署名者、それから検証者と、種類がいくつかあるわけですが、今回の場合ボトルネックになりますのは、署名者あるいは検証者がいろいろな数がいてリプレイスが大変だという理解でよろしいでしょうか。
○佐々木情報推進官　ご認識のとおりかと思います。署名者、検証者に関しましては、今回エンドエンティティ、具体的には医療機関や薬局で利用されるシステムになっておりますので、そこの数がもちろん一番多くなっております。また、認証局システムに関しましても、我々、厚生労働省ルート認証局とサブ認証局様のほうで少し議論をしていかなければならないという認識はございます。ですので、どちらも併せて調査をさせていただければと思います。
○菊池構成員　承知しました、ありがとうございます。
○松本座長　ありがとうございました。ほかにございますでしょうか。

○喜多構成員　喜多でございます。14 頁で、とっかかりとして、この 4 種類から入っていくのはいいと思いますが、あとカード会社がカードをちゃんと作れるか、カード用のドライバーがどうなるか、そういう具体的な周辺技術の開発状況や、デジタル庁等での新カードや周辺分野の開発状況も忘れないようにどこかに欄をつくって書いておいたほうがよいのではないかと思いました。それから、電子処方箋以外に用途をもう少し広げるという話は、これから後なのかもしれませんけれども、スケジュール上は必要だと思うので、それも含めて何か差し支えが出てこないか等も加えたらどうかと思いました。以上です。
○佐々木情報推進官　事務局です。ご指摘ありがとうございます。確かに、用途に関しましては、先ほど申し上げたとおり電子処方箋及び紹介状につきまして、考えていたところではございますが、将来的にほかの用途にも広がる可能性はもちろんございますので、これ自体が 2030 年を目的としておりますので、長期的なプランも見据えながら、どういったもので HPKI の利用が広がっていくかという点も併せて調査の対象とさせていただきたいと思います。
○松本座長　ありがとうございます。よろしいですか。
○矢野構成員　日本医師会の矢野です。まず、この次の暗号を早く決めてください、認証業運営者として急いでいただきたいというところでお願いして、今日整えていただいてありがとうございます。作業範囲として、その際に、そもそもの認証業の構成のあり方、ルート認証局サブ CA になっている、この構成のあり方についても、もうルート 1 本でいいのではないか等、ご議論いただきたいとお願いしたいのが一つと、もう一点、それに併せて、先ほども出てきましたが、GPKI との相互接続の可能性も、調査項目を増やして申し訳ございませんが、お願いしたいと思います。
　関連して、前回もお話ししましたが、例えば、介護の主治医意見書は、自治体が検証しています。だから、自治体と接続するかどうかは別として、医師なり薬局なり、そういう医療機関、薬局、薬剤師とかだけではなく、自治体等の広がりも出てくるかもしれませんので、検証者の範囲は少し丁寧に、もう少し議論というか調査をされたほうがいいかなと思います。以上です。
○松本座長　そうですね、そのとおりかと思います。ほかにございますか。
○宮崎構成員　JDTF の宮崎です。前回も少し申し上げましたが、特に、検証者に関わるところについて、現に電子処方箋でもタイムスタンプをつけています。もちろん総務省が担当になっていますので、こちらから注文をつけたりすることは多分できないと思いますが、少なくとも総務省側でどう考えているか、総務大臣認定をどう考えているか、移行時期をどのくらいと考えているか、どういうアルゴリズムを本当に使おうとしているのかといったことも押さえておかないと、システムベンダー側が、困るところが出てくるかと思いましたので、そのあたりもご留意いただければと思います。
○松本座長　よろしいでしょうか。
○佐々木情報推進官　事務局でございます。前回、宮崎構成員からもご指摘いただいてい

るところを把握しておりますので、改めまして具体的な調査の段階に入りましたら、総務省にも問合せをさせていただきまして、順次進めさせていただきたいと思います。ありがとうございます。
○松本座長　ありがとうございます。
○山内構成員　JIPDEC の山内です。14 頁で、調査をしていくということですが、まず、そもそも調査主体は厚生労働省と HPKI 専門家会議の両方だと私は認識していますが、よろしいでしょうか。
　そのときに認証局が、まさに厚生労働省が委託している先の事業者などにいろいろ確認や調査をすることはよいと思いますが、署名者、検証者には多くの方がいらっしゃるにもかかわらず、システムベンダーを通してのみヒアリングをするように読めました。つまり「想定される確認先」という日本語がわかりづらく、署名者や検証者からいろいろな問題点や意向を聞くときに、JAHIS(保健医療福祉情報システム工業会)を通じてシステムベンダーからしか聞かないのか、気になりました。署名者や検証者が抱える問題や要望、意見を聞く方法は、システムベンダーを通じてでも構いませんが、それ以外の方法というのもしっかりと検討していかれるべきではないかと思いました。以上です。
○佐々木情報推進官　事務局でございます。先ほどからほかの委員からもご指摘をいただいておりますので、改めてそもそもその検証者というところが、どこまでの範囲を見るのかどうかというところも併せて調査をさせていただき、それに見合う形で確認先も検討させていただければと思います。
○山内構成員　もちろん検証者だけではなくて署名者についても、直接、全ての医師から全部ヒアリングするのは無理なわけですが、いろいろなパイプを使って、しっかりとニーズを把握していただくような書き方にしておかれたほうがいいと思いました。以上です。
○松本座長　ありがとうございます。ほかにございますか。よろしいですか。
　では、私のほうから少し質問とコメントという形で申し上げたいと思います。まず、デジタル庁にヒアリングしていただきましてありがとうございました。そのときに、積極的に ECDSA をとるということについての理由は聞けていないという状況でしょうか。
○佐々木情報推進官　ご認識のとおりです。デジタル庁担当者から聞いている範囲としましては、内部でこのような、今お示しをさせていただいたような議論としては、こういった懸念点が議論の際には挙がって、最終的に内部で決定を下したと聞いております。
○松本座長　分かりました。普通に、この時期に暗号の移行ということをアルゴリズムの移行と考えると、耐量子計算機暗号はどうするのかという論点が必ず出てくると思います。それで、日本はぐずぐずしていたんですが、先週、5 月 29 日に、耐量子計算機暗号への移行を進める体制をとるということをサイバーセキュリティ戦略本部で決めて、今年度の計画に入れることになりました。それから、暗号技術検討会 CRYPTREC でも、PQC（Post-Quantum Cryptography、耐量子計算機暗号）を使えるような形に整えていくという方針で今年度活動することになっております。

そのため、まだ現状では、なかなかすぐ、広く使えるという環境にはないのですけれども、大きくそちらのほうに動いていく可能性はございます。これは、量子計算機で暗号解読に十分な力を発揮するようなものがいつできるかという問題とも関係してくるのですけれども、もはやいつできるかは関係なく移行していこうということに大筋ではなってくるかと思います。

そうしますと、この時期に決定するというのは、非常に難しいんですけれども、いわゆる耐量子計算機暗号ではない、従来からの公開鍵暗号技術の一つである楕円曲線デジタル署名アルゴリズム、ECDSA のうち、192 ビットセキュリティを持っている P384 があります。P というのは素数で、整数の中でその数及び 1 以外では割り切れない数のことを素数と言っておりますが、素数で 384 ビットの素数は数多くありますけれども、その中のある選択されたものを使うという意味で、ECDSA―P384 と表現されます。佐古構成員からもありましたように、384 と言ってもいろいろあるので、どれなのかというところがありますが、それは、いわゆる常識的に大丈夫なものが選ばれてくるということになっているのかと思います。GPKI でもそうなんだと思います。そのため、デジタル庁は、現実策として PQC、耐量子計算機暗号を次の移行で行うのは無理だと判断したということでしょうか。

○佐々木情報推進官　事務局でございます。耐量子計算機暗号に関しましては、今回デジタル庁とは話を一切しておりませんで、今回、ご指摘いただきましたので、改めて今のデジタル庁の状況は確認をさせていただきます。

○松本座長　聞かれたほうも多分困ると思いますが、一応そういうことであり、現実解として耐量子計算機暗号ではなく、従来からの暗号技術を選択せざるを得ないということで、当専門家会議も考えなければいけないのかどうかというあたりでありまして、皆様のご意見を伺いたいと思います。

○林構成員　皆様ご存じのとおり、大変発言にしにくい立場におりまして、どこまでお話ししていいのかというところはございますが、GPKI では、少なくとも今出ていたような課題感は認識した上で選択しているところはお話ししてもいいのかと思っております。私、今日はデジタル庁の人間ではないので、細かいところはぜひもう一回、エビデンスをきちんと集めるという意味でお問合せいただければ、どういうディシジョンが行われて、どういう決定で今に至ったかというお話が GPKI 担当班からデジタル庁としてお返事できるのではないかと思っております。

ただ、今、松本座長からお話があったとおり、GPKI 側で、恐らくですけれども、決めた時期と、その閣議決定が行われたタイミングというのは、現時点で既に物事が変わってしまっているので、我々が GPKI の決定を踏襲していいのかというところに関しては、こちらできちんと考えなくてはいけないというところは出てくるのだろうと思っています。

ただ一方で、PQC に関しては、話題が加熱しているところもあるので、現実的に地に足の着いた取組をしていくというところは、個人的には必要になってくると思っています。例えば、対応ハードウエアですとか、当然、鍵長が非常に大きくなってしまうところもあ

って、実際にどのぐらいの量子コンピューターの実用性みたいなインパクトがどのぐらいなのかは、今、非常に多くのペーパー等が出ているところもありますので、それらを踏まえて、かなり専門的に、かつ現実的な路線で、きちんと地に足の着いた議論がこちらでもなされる必要があるのではないかと個人的には思いました。以上です。
○松本座長　ありがとうございます。ほかにございますか。
○宮内構成員　宮内でございます。考えていかなければいけないのは、全くそのとおりだと思いますが、前にも言いましたけれども、暗号文を作るのと署名を作るのは少し別かもしれないと私は思っています。暗号文については、今得た暗号文を将来、量子計算機ができたときに解読する方法がありますが、署名については、長期署名のフォーマット等でしっかりやっていれば、そのおそれというのはかなり小さくできると思っているので、署名は、暗号文に比べたらそこまで急がなくてもいいのではないかという感覚をまず持っているのが1点です。
　それから、もう1つは、2026年に予定されている新しいマイナンバーカードはPQCではなく、ECDSAでやると私は聞いています。これは10年間使うものですので、大体、署名のほうは、そのくらいのタイムピリオドで考えていてもいいのかなと私は思っています。ですから、10年後までに、例えば、2026年からだと2036年ですか、実用的な量子計算機ができることはあんまりないのではないかというのが世間的な思いだと思っており、そのくらいの時期で考えていったらどうかというのが私の思いです。以上、2点でした。
○松本座長　ありがとうございます。署名のほうが、機密性（Confidentiality）の観点では、暗号よりもゆっくりやっていいのではないかというお考えだと思いますが、私はそれは間違っていると思います。なぜかといいますと、公開鍵方式である以上は、公開鍵で共通鍵暗号の鍵を共有するとか、あるいは暗号化をそのまませる等をしますので、そのための公開鍵の証明書が必要になります。これは、やはりデジタル署名を使うわけですので、そこでメッセージに対する処理が、たとえその署名がなかったとしても、その公開鍵証明書に関しては、署名が必ず必要になると。セットできいてくるはずではないでしょうか。ということで、あまりここで議論をするつもりはないですが、もし反論があればお願いします。
○宮内構成員　おっしゃることは分からないでもないのですが、要は長期署名を行うことによって対応できるかできないかは、暗号化と署名で違うのかなと少し思っているところがあります。
○松本座長　要するに、暗号化を先に対応しなければいけないということですよね。
○宮内構成員　おっしゃるとおりです。
○松本座長　でも、そのときに同時に、署名も必要ですということを私は申し上げているので、だから同時ですということにならざるを得ないのではないでしょうか。
○宮内構成員　必ずしも納得したわけではないですが、分かりました。
○矢野構成員　矢野です。全く違う視点から、HPKIは、もちろん医療のデータが電子化

されて、医師が書いた、薬剤師が書いた、しかも改ざんされていない責任を取るためにきちんと署名をしなさいというものだと思いますが、正直現場に関して言うと、どうしてこんな面倒くさいことをするのか、なぜ署名が必要なのかと、医者に言われます。我々は、HPKI の重要性、なぜ資格証明が必要なのかという議論を、論を待たないぐらい当たり前のこととしてお話していると思いますが、現場からすると、そういう感覚ですので、例えば、今回、楕円になった、耐量子計算機暗号になったでもよいのですが、突然決まって、それになりますとなれば、現場では大改修となり、お金がかかる。また分からないものを持ってこられるとなると、HPKI は不要ではないかという議論になってしまいます。暗号の話はもちろん大事ですし、暗号方式を決めたのであれば、そこに向かってまずは認証局が準備しなくてはいけない、あと現場を懐柔しないといけない、それを導入しないといけない、医療機関にはお金がかかる、薬局にもお金がかかるというスケジュールで動いていますというお話になります。そのため、今のお話は、私も理系なので大好きなんですけれども、耐量子計算機暗号にするならしていただいていいし、楕円曲線するならしていただいていいのですが、急いでほしいと思います。

○松本座長　そのとおりだと思います。

○矢野構成員　決めていただいて結構ですが、スケジュール感を見ていただいた上で早く決めていただきたいというのはあります。あとは、HPKI は現場に波及する効果がすごく大きいです。そのため、議論をきちんとしていただいて、決めていただいて、それに対して受ける現場はこちらですから、ちゃんと準備をして対応していきますので、決めていただきたいと思っております。以上です。

○松本座長　ありがとうございます。

それと、あと２点ほどありまして、１点目は、今回、先ほどの、調査をする際のご質問もそうですけれども、どういうサービスが主力であると考えているのかと、それらに対応できる HPKI のアーキテクチャーはどうなっているのか、というところをしっかりと再整理する、再把握する必要があるのではないかと思います。そのときに、先ほども出てきましたけれども、多分、私の前任の方々が、ともかく突貫で作ったいろいろなルールやドキュメントを何とか使って回してきたというのが現状なので、この際、よりよくすべき点があるのであれば、うまくそれを今回のタイミングで入れられるといいのかなと思っております。そのときに、例えば、リモート署名サービスは非常に有益な技術だと思いますけれども、今までの方式と、今回 ECDSA にすることによって変わってしまうのではないかと思いますが、どうでしょうか、大きく違ってくるのでしょうか。このあたり、宮内さんを中心として、セキュリティのリクワイアメントは何か、それをきちんと満たしている方式なのかということで、テクニカルな部分からは、少し認めましょうというのが最初にあって、ある種ブラックボックスの議論にしてしまったのですが、ちゃんと信用できる大丈夫なものなのかと思っています。現行動いている方式が駄目だと言っているわけでは全くないのですけれども、そのエビデンスがしっかりと示されていないという点では、私は少し

不満に思っています。つまり、昔オーストラリアにおられた先生（Colin Boyd）が提案した論文が根拠で、その内容をベースにしていますということですが、実際にどのようなリモート署名になっていて、その実装が本当に大丈夫なのかというところは、もし今回そこも影響が及ぶのであるならば、よく見ておく必要があるのではないかと思いました。何かそんなことは必要ないとかいうことを言っていただければと思いますが、いかがでしょう。

○山本構成員　ありがとうございました。リモート署名に関しては、松本先生のおっしゃるとおりだと思います。エビデンスをもって証明しておかないといけないと思いますので、そういう意味で、今の鍵、秘密分散を使った鍵分割方式が本当にいいのかどうかというのは、考え直さないといけないかもしれないと思います。それは、ECDSA になったからといって変わらないと思います。ですから、そこは別問題として議論をしていただければいいと思います。

少し議論を遡って恐縮ですけれども、矢野君の言うこともそのとおりで、保健医療分野でこういったITのセキュリティを考えるときに、安定した技術を使うことがおそらく非常に大事で、実験的なことはできないんですね。ですから、やった以上は、社会実装して患者さんが関わる話になるので、駄目でしたとは言えないことがあるので、それなりに安定した技術を使わないといけないので、そういう意味で PQC が非常に重要であると私もよく理解していますけれども、NIST 等を見ていても、昨年あたりでもまだ PQC に関してふらついてるところがあったような気がします。松本先生にお聞きしたいのですが、もう大丈夫なのでしょうか。

○松本座長　暗号アルゴリズム自体のセキュリティについて、これは、よってたかって評価をしているので、一定の安定感はありますが、今回の PQC の標準は、鍵サイズはどんどん延長していってもよく、フレキシブルな標準になっています。あとは、暗号のアルゴリズム自体、メッセージに対して署名をかけるとか暗号化するとか、そういった基本的なアルゴリズムしか、まだ定まっていないわけでして、それを使ったプロトコル、暗号技術を使ったプロトコルについても、いろいろと標準化活動はなされていますけれども、かつ例えば、OpenSSL というライブラリーの中に、この４月から PQC 対応のものが入ってきて、やろうと思えばみんな使えます、といった状況になってきてはいます。しかし、従来の暗号技術のほうが、ある種枯れていて信用ができると、まだ出てきて間もない標準化がなされつつある耐量子計算機暗号だといろいろと不備があるかもしれないので両方を併用しましょうというアプローチもとられていたり、あるいは、そんなものは必要なくて PQC １本でいきましょうという、ある種、流派が幾つかありますという段階なので、山本先生がご懸念のように、まだ安定していないというのが現状だとは思います。ただ、冒頭から申し上げましたように、量子計算機がどう進展するかにかかわらず、もう置き換えてしまおうという非常に大きな流れはあるんですね。それを見通して、実装をしたり、実務面であるいはビジネスをしようという人たちはたくさんいて、日本にもいるのですが、残念ながら諸外国のほうが勢いが強くて、前から行っていたので実績もあったりすると。放って

おくと、そういうところの技術を全部使わざるを得ない状況になってしまう、追い込まれてしまうという可能性がございます。ということで、自分たちの論理で必要ないだろうとなかなか言い切れない面が、この問題の難しさの一つかなと考えております。山本先生、私はこんな感じで考えております。

○山本構成員　必要ないとは全く思っておりませんが、社会保障の現場に導入する以上は相当の覚悟が要りますので、もし、引き続き議論をしていただいて、これだったら多分入れても大丈夫だとなった時点で、あんまり時間を置かずに入れるほうがいいのではないかと思います。私も当然ながら、将来的には PQC に移行することが必須だろうと思っていますので、それをいつにするかという話をやはり考えておかないといけないとは思います。

○松本座長　そうですね。アメリカは2035年までに、今までの暗号は使わないようにすると言っていますが、どうなのでしょうか。とても守れそうにないと思いますけれども。ヨーロッパもそういうことを言っている国がありますし。最初、2030 年と言っているところもありました。

○山本構成員　それは無理でしょうね。分かりました。ありがとうございます。

○松本座長　すみません、ちょっとお時間を使ってしまいましたが、この件について何かございますか、そのほか。よろしいでしょうか。

HPKI でも、耐量子計算機暗号に対してどう臨むかという課題はありますということを申し上げたかっただけです。ありがとうございました。

そのほか、この暗号アルゴリズム移行に関しまして、ご意見ないでしょうか。なければ、この件はこれで終わりということにさせていただきたいと思います。大変ありがとうございました。

（5）連絡事項

○松本座長　それでは、事務局よりご連絡事項などありましたら、お願いいたします。

○佐々木情報推進官　事務局でございます。連絡事項でございます。

あと改めて、今後の課題というところも少しこのページで示させていただきます。資料1の 16 頁目になっております。まず、次回の第 33 回 HPKI 専門家会議について、先ほどまでのご議論を受けまして、特に暗号移行につきまして調査、恐らく次回までに全ていただいた宿題事項全てを調査することはできないのかもしれませんが、まずは進捗状況につきましては、ご報告をさせていただければというところで思っております。日程につきましては、別途ご調整させていただきたいと思っております。

また今回、この第32回が今年度初めての専門家会議でございます。今年度ですが、どういったことをこの専門家会議の中で議論をさせていただきたいのか、まずは事務局のほうで簡単に頭出しだけさせていただきました。もちろん、今回お話をいただきました暗号アルゴリズムについてというところもございますが、先ほど矢野構成員からもございましたが、ルート認証局を含めて認証局としての体制も、今回、暗号アルゴリズムの移行の際に

リプレイスをすると、システム上も入れ替えを行って並行運用をするという話でございますので、そういった大きなリプレイスが行われるタイミングに併せて、再編等も含めて本来 HPKI としてどのような形が最も効果的に運営がされることができるのかという点で、これに関しましても議論の一つとさせていただければと思っております。また、冒頭にもございましたが、ポリシ等、ドキュメントにつきまして、こちらもかなり古いものになっておりまして、どうしても今の状況にアップデートがされていない部分がございますので、それらはアップデートをさせていただきたいと考えております。今後の準拠性審査及び認証局の監査のあり方についてでございます。こちらについてですけれども、今回 MEDIS 認証局の監査を、おそらく 8 月にやらせていただくことになるかとは思いますが、ここから先に関しまして、現在、こちらの CP を基に監査をさせていただいておりますが、これらの CP のアップデートも行わせていただきたいと思っておりますので、それに併せまして監査のあり方も改めてこの会議の中で議論をさせていただき、どういった形で準拠性審査を行っていくべきなのか、正確にきちんとした手順書のようなものも作っていきたいと考えている次第でございます 。また、これは昨年度から行っておりますが、リモート署名サービスの評価基準、こちらも先ほど松本座長からお話をいただいたとおりではありますが、電子処方箋拡大の中で、かなり性急な議論をし、このリモート署名サービス評価基準を作ってきたという経緯がございます。これに関しましては、改めて今回も暗号移行もありますし、このリモート署名サービスを一体どこまで拡大をするのかというところで、この基準につきましても、改めて本来あるべき形をしっかり議論をいただいて、HPKI で使用すべきリモート署名サービスの評価基準を今回、電子処方箋以外も含めましてご議論をいただきたいというところで議題としては考えております。まず、目先に関しましては、暗号アルゴリズムの移行を中心にお話をさせていただきながら、今年度進めていただければというところで思っております。事務局からは以上となります。それでは、松本先生お返しいたします。

○松本座長　ありがとうございます。今のご連絡事項に関しまして、何かご質問やコメント等ありますでしょうか。

○林構成員　基本的にはカバーしていただけていると思うのですが、今までの議論を踏まえて、あえて議題という形で整理していただいているのでコメントさせていただきますと、結局これは HPKI を中心としたエコシステムの全体をちゃんと見直して、グランドデザインをちゃんと見ていくということを議題の中に入れていただいて、個別のところもきちんと見ていくと。全体像のところも見ていくというところを、すごく大きな課題を増やしてしまって恐縮ですけれども、入れていただくのがより望ましいのかなと思った次第です。林からは以上です。

○松本座長　ありがとうございます。今日、様々なご意見出ましたので、議事録を早めに作っていただいて、それを確認し、次回の議題、議事項目に反映させていただくというのがよろしいのかなと思います。

○山内構成員　もう一点いいですか、すみません。非常に重要な局面に来ているということが分かってきましたので、あえて申し上げたいと思うのは、実は私自身、PKI についてはかなり長く仕事で関与させていただいておりますが、HPKI というもの自体についても実際に自分が触ったことないので分からない面が結構多いんですね。どういうことを言っているかというと、どのように電子証明書を検証するかというのは、実際に自分で手を動かしてみて、その電子署名がなされている画面を、例えばPDF であれば、電子証明書を検証する際に、どんなデータ、どんなことが記載されているかというのをチェック等して、それで、なるほどこういう形で電子証明書の有効期限があるとか、どこがこの電子証明書を発行しているのが、どのように見えているのかとかいうことを、確認することは私たち JIPDEC の職員はやっています。だから、いわゆる認定認証業務と言われているものについても、それは当然、当たり前のことはやっていますけれども、私達は HPKI を用いて実際に電子署名する立場でもないし、電子署名を検証する立場にもなく、普段触ることはないので、どんな画面が出てきているのか、その電子証明書の検証はどういう形で行われて、どういうふうにそこに書かれているのかというのは知らないんですよね。なので、これから HPKI 全体のエコシステムみたいなことを検討していくことを思うと、実際にどういうふうに電子署名がなされていて、それがどのように検証されているか、どのような手順でどういうふうにやっているか、どういうふうに見えているかということなども、ちょっと勉強させていただいたほうが役に立つかなと思い、コメントさせていただきました。それはどのような形であればいいか分かりませんが、意外と PKI の専門家と言いながらも、それぞれの PKI ごとに流派も違うし、全然分からないことが多いということも、この 10 年の間でよく分かってきましたので、コメントさせていただきました。以上です。
○松本座長　貴重なご意見ありがとうございます。それはそうですよね。我々も、そういう理解が進むような、何らかの活動ができるといいのかなと思いますが、いかがですか。
○佐々木情報推進官　事務局でございます。ご意見承知いたしました。改めて、今、ご用意させていただいているのは、基本的にはドキュメントベースのみになっておりますので、具体的な利用シーン、これまで HPKI が利用シーンとしては、やはり電子処方箋が、かなり大きいものとして、この数年で一気に出てきたというところでございますので、そこを中心に先生方にもご理解いただけるような形で、何らかの資料、もしくは体験できるような形というのは何かしらご用意させていただければと思います。検討させていただきます。
○山内構成員　よろしくお願いいたします。
○菊池構成員　本日の議題で、MEDIS 認証局の準拠性審査班がお二人、六川先生と丸山委員が決まったかと思いますが、そこに山内委員も加わっていただくのはいかがでしょうか。JIPDEC で長く携わっていらっしゃいますし、この機会に、その中身に関しても、山内さんが内部まで見ていただければ、我々としてもすごく安心できるかと思うのですが、いかがでしょうか。難しいでしょうか。
○山内構成員　私自身は「電子署名及び認証業務に関する法律」に基づく指定調査機関の

調査員ではないんですよ。だから、そういうことを行う人間を JIPDEC の中で決めていって、ご要望があればお手伝いさせていただくことは検討させていただきますけれども、実際に認定認証業務などの実地調査をしている人間を、どのように法律の垣根を越えて、あるいは省庁の垣根を越えて使っていただくかというのは行政の話なので、厚生労働省様のほうでご検討いただければありがたいと思います。

○佐々木情報推進官　事務局でございます。ありがとうございます。また厚生労働省としまして、どういった形でお願いができるのかというところは、省内ルールもございますので、改めて JIPDEC 様とご確認をさせていただきます。今回、これまで HPKI 専門会議において、この準拠性審査に関しましては、あくまで HPKI 専門家会議として派遣をいただいているものでございまして、基本的には国からの諸謝金で行っていただいているようなものでございます。別途、監査という形での調査事業みたいなものを立てるべきなのかというところも、できればこの会議の中で、今後、あり方としては外部監査をするとか、そういった選択肢もあるとは思っておりますので、引き続きのご議論をいただければと思っております。

○松本座長　ありがとうございます。

○横田構成員　兵庫県薬剤師会の横田です。資料に関して、前回の議論を踏まえた今回の資料だったと思いますので、もしよろしければ、前回の議事録の最終版を資料としてつけていただくと、さらに理解が深まるのかなというのが１点。あと、今回、組織が変わったからということで、印刷物があるのですが、結構量があるので、もしよろしければ、電子データでも送っていただいていますので、紙の資料、いる、いらないでもって、事務局も、多分コストを削減できると思いますので、そのあたりも、先ほどの前回の議事録の掲載とあわせて、資料の削減を検討していただけたらと思いました。

○佐々木情報推進官　事務局でございます。ご指摘ありがとうございます。次回以降の開催につきましても、改めてアルゴリズムの移行については継続的にお話をさせていただくものでございますので、前回議事録プラス今回議事録もおつけした形で、次回は開催をさせていただきたいと思います。また、紙につきましても、エコな形になるように、少し検討させていただきます。

○田中参事官　ちなみに皆さんは、この会場でご自身の PC を御覧になっている先生もいらっしゃると思います。電子データにするといったときに、こちらでタブレットを用意する検討会等もございますが、タブレットの数がそんなに多くなく、厚生労働省では、異常なまでに会議が開催をされておりまして、タブレットを全員分用意ができないことがございますので、場合によっては先生方にご協力をいただくようなことも検討しないと、なかなか電子データのみという形式ができないのかなという気がしております。

○松本座長　そうですね。少なくとも、このメインの資料と、議題書、議事録等は紙であったほうが明らかにいいのではないでしょうか。ポリシ等の資料は電子でもいいのかなとは思いますが、さっと見られるかどうかという点では紙も優れているので、印刷が大変だ

ったり、それをまた回収して破棄していただくとかもあり、要するにあまり先進的でないと思われるかもしれませんが、紙も結構よいのではないかというのが、私のコメントです。最適解を編み出していただければと思います。

　ではよろしいでしょうか。皆様、どうもありがとうございました。これにて閉会といたします。

以上