# 第３３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

日時 令和７年７月２３日(水) １０：００～

場所 AP 新橋　Ｉルーム

開会

○岡嶋主査　事務局です。定刻になりましたので、ただいまより「第33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」を開催します。皆様方におかれましては大変お忙しい、またお暑い中、本会議にご出席いただき、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での開催とし、公開での開催、資料については一部公表としています。また正確な議事録作成やご意見を賜った時の整理を事務局で正確に行うため、録画させていただくことをご承知おきください。

次に構成員に関する連絡です。本日の会議の参加状況ですが、柴田先生、宮内先生がご欠席、横田先生、林先生がオンライン参加となっています。林先生は後ほど現地に到着される予定です。その他の構成員の方々は現地参加となっています。

続いて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、構成員の皆様には名前をおっしゃってからご発言いただくようご協力をお願いします。また手元のマイクのオンについてもご協力をお願いします。

続きまして資料の確認をさせていただきます。本日の配布資料としまして、クリップ留めしている議事次第、資料１、資料２－１、資料２－２、参考資料１、参考資料２、また前回の HPKI 専門家会議の議事録と、本日の配置図を用意しています。資料の不足等がありましたら事務局までご連絡いただければと思います。

それでは松本座長、以降の進行について、よろしくお願いします。

○松本座長　皆様、おはようございます。本日もどうぞよろしくお願いします。議題は資料１の２頁目に４つありますが、この順番で進めたいと思います。まず事務局より、議題１に関してご説明をお願いします。

議事

（１） MEDIS 認証局　準拠性審査の実施について

○河内主査　厚生労働省事務局です。資料１に沿って MEDIS 認証局の準拠性審査についてご説明します。資料１の４頁目をお願いします。

HPKI 専門家会議にて HPKI サブ認証局に対して２年に１度行っている準拠性審査についてご報告します。MEDIS 認証局に対する前回の審査は 2023 年９月８日に行われ、規定に従い、そこから２年以内に審査を実施する必要があるため、このたび2025年８月４日に準拠性審査を行うことが決定したことをご報告します。審査班については前回の専門家会議にて選出、ご指名された丸山先生と六川先生にお願いさせていただき、了承いただいたことをご報告します。

審査対象は、前回の MEDIS 認証局の審査時と同様に、 HPKI サブ認証局としてのポリシに基づいた準拠性審査に加えて、 MEDIS 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が運用されているため、 HPKI リモート署名サービス評価基準に従い、鍵管理サービス及びデジタル署名生成サービスに関する準拠性審査もあわせて実施することを予定しています。審査方法としては、通常どおり、書類審査と実地調査を予定しています。また今回の審査から、審査の標準化を目的に、審査班向けにお手元の資料２－１及び２－２にて配布しているチェックリストを用いることを計画しています。丸山先生と六川先生には事前にチェックリストの有用性のご確認をいただいていますが、実際の審査で利用することについて、専門家会議のご了承をいただきたく、本日の審議事項としています。議題１に関して事務局からの説明は以上です。松本先生、よろしくお願いします。

○松本座長　ただいまの MEDIS 認証局準拠性審査の実施に関して、ご質問はありますか。

　まず丸山先生と六川先生に審査班を構成していただくことは既に決まっていて、審査対象は HPKI サブ認証局と、先ほどご説明のあった HPKI リモート署名サービスの鍵管理サービスと、それから HPKI リモート署名サービスのデジタル署名生成サービスで、書類審査と実地調査により行うということです。チェックリストの中身がどのようになっているのかを理解しないといけないと思いますが、それ以外に何かご質問はありますか。よろしければ事務局より、書類審査及び実地調査のチェックリストがどのように構成されているかの概要をご説明いただけますか。

○河内主査　はい。ありがとうございます。まず書類審査については、ポリシに基づく準拠性監査報告書をそれぞれ認証局に作成いただくことになりますが、その監査報告書に抜け漏れがないかについて１対１で確認する構成になっています。実地調査に関しては、これまで確認項目について、ざっくりとしか手続規則について規定をしていなかったので、具体的な確認項目についてチェックリストを用いて一つずつ確認できる体制を整えました。

○松本座長　ありがとうございます。何かご質問はありますか。佐古構成員、どうぞ。

○佐古構成員　佐古です。ご説明をありがとうございました。実地調査で、何か土台にした指針などはありますか。

○河内主査　HPKI の認証局の準拠性審査に関しては、ホームページでも公開している手続規則がありますので、その確認項目に基づいてチェックリストを設けています。

○佐古構成員　ありがとうございます。代表者インタビューなど、トップダウンで実施する確認内容を初めて拝見したので、そのように思いました。

○河内主査　今回、あくまでも審査の補助ツールという位置付けであり、既存のポリシや実施規則の要求を超えるような義務を課すものでないことは、ご了承いただければと思います。実際に審査の中でご活用いただいて、丸山先生と六川先生のご意見もいただきながら、今後アップデートも検討したいと思いますので、よろしくお願いします。

○松本座長　資料２－１では、57 頁まで「PKI 認証用証明書ポリシ」と書いてあり、58 頁からリモート署名サービスに関するものになっていると思いますが、リモート署名サービスの内容はどこまででしょうか。

○河内主査　書類審査に関する資料２－１は、１頁から 29 頁までが署名用のチェックリスト、30 頁から 57 頁までが認証用のチェックリスト、58 頁から 94 頁までがリモート署名サービスの鍵管理サービス、95 頁から最後までがリモート署名サービスのデジタル署名生成サービスと、４つの構成となっています。
○松本座長　分かりました。
それから実地調査ですが、これは１頁ごとにあるのでしょうか。これはどのようになっていますか。
○河内主査　実地調査に関しては、代表者インタビューをはじめとして、ヒアリングや実際の施設の確認内容を網羅的に確認できる仕組みとなっています。
○松本座長　これは先ほどの書類審査とは、どのような関係にあるのでしょうか。
○河内主査　今回、実地調査に関しては、 HPKI サブ認証局に対する実地調査と、 HPKI リモート署名サービスに対する実地調査をそれぞれ実施することになります。
MEDIS のリモート署名サービスの実態として、 MEDIS が委託しているファインデックス社がサービスを運用し、ファインデックス社は AWS のインフラを利用してサービスを提供しています。つきましてはリモート署名サービスの実地調査としては AWS に確認する必要がありますが、現実的に困難であるため、ファインデックス社の AWS の利用に関する契約書等のドキュメントベースでの確認を実地調査に代えて行うことを予定しています。リモート署名サービスとしての実地調査は資料ベースの確認となることから、実地調査に関するチェックリストは認証局としての実地調査に用いて、リモート署名サービスの実地調査では使わないことを予定しています。
○松本座長　ありがとうございました。加えて何かご質問はありますか。山内構成員、どうぞ。
○山内構成員　JIPDEC の山内です。以前から申し上げているとおり、 JIPDEC 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仕事を、デジタル庁及び法務省から指定されて行っています。その基準のモダナイゼーション、要は見直しをデジタル庁で、ここ数年かけて進めています。
その中で、認証業務を行う事業者としてリスク評価を行った上で、様々なサイバー攻撃や情報セキュリティに関するリスクを洗い出し、それに向けたセキュリティ対策を行っていく仕組みができているか、どのように評価して、その上で認定しているかということが、一つ大きな課題となっています。そういうことを認定の基準の中にきちんと入れておこうという方向性になっています。
MEDIS の認証局を調査する時に、情報セキュリティの点でのリスク評価をどのように行っていくのかについて、例えば代表者インタビュー、あるいは実際に MEDIS から委託しているベンダーの責任者の方に、そういうことを行っているかについて確認する内容を入れてはどうかと思います。
この調査票をすぐに変えろと言うつもりはありませんが、チェックリストというものに

は実は問題がありまして、チェックリストに書いていないことを一切しないということもあるわけです。委託元である MEDIS と委託先のベンダーが、それぞれの立場でどのような情報セキュリティのリスク、脅威があるか、まず脅威があり、それに基づくリスクが発生するわけですが、そのリスクがどの程度のもので、どのように対策していくかについて必死に考えなければいけません。そういう体制ができているかどうか、うまく実地調査などを通じて確認いただくことも工夫していただければと思います。以上です。
○松本座長　事務局、どうぞ。
○河内主査　基本的には抜け漏れがないように作成していますが、チェックリストだからこそ漏れなく確認できるような新しい体制も考えていきたいと思います。丸山先生と六川先生にご協力をいただきながら、アップデートも検討していきたいと考えています。
○山内構成員　このチェックリストで確認できないところがあるかどうかも含めて、よく検証してほしいと思います。認証局の主体である MEDIS と委託先のベンダーの間でしっかり対応して考えていくことを、どのように文書に表現するかは大変でして、実はデジタル庁でも困っています。そのような問題があるとお聞きしましたので、コメントさせていただきました。以上です。
○河内主査　ありがとうございます。
○松本座長　宮崎構成員、どうぞ。
○宮崎構成員　宮崎です。資料２－１の位置付けについて確認したいのですが、確認対象資料が準拠性監査報告書となっていますので、準拠性監査報告書が出来上がってから記載漏れがないかについて確認するためのチェックリストでしょうか。
○河内主査　おっしゃるとおりです。
○宮崎構成員　では準拠性監査を行う時のチェックリストはどのようになっていますか。
○河内主査　準拠性監査を行うためには、準拠性監査のための報告書というフォーマットがありますので、基本的にそれを埋めていただければ、問題なく網羅的にポリシに基づいて監査が行われていることが確認できる仕組みになっています。
○宮崎構成員　この項目に対応するような準拠性監査の各チェック項目はまた別にあって、そのフォーマットに結果を書き込んでいくのですか。
○河内主査　はい。おっしゃるとおりです。
○宮崎構成員　そのフォーマットについては、我々は確認していたでしょうか。
○岡嶋主査　それは既にポリシに含まれていて、厚労省のホームページにドキュメントで公開されており、専門家会議の中でもお諮りしているものと考えています。
○宮崎構成員　では、そちらを確認すればいいということですか。ありがとうございます。
○松本座長　他によろしいですか。林構成員、どうぞ。
○林構成員　これは審査をされるお２人は重々承知だと思いますが、議事録に残させていただきたいと思っています。
　セキュリティ分野では、チェックリスト方式の形骸化が非常に問題視されています。形

式的にチェックリストを満たすことで全てが解決したとなりがちで、これがいろいろな問題を生んでいる現状があります。ですから、このチェックリストに明記していただく必要はありませんが、チェック項目の見直しを行うことや現地での保証も含め、形骸化を防ぐことを方針に含めていただけると安心かと思いました。以上です。
○河内主査　今回から新しく導入しますが、今後、何年も同じチェックリストを用いるという運用に関しては、定期的に見直しすることなども検討させていただきたいと思います。ありがとうございます。
○横田構成員　質問してもよろしいですか。兵庫県薬剤師会の横田です。
○松本座長　はい。どうぞ。
○横田構成員　先ほどの林先生のご発言にも関連しますが、今回このチェックリストに基づいて実際にチェックされた方々から、チェックリストの見直しに関してご提案いただけると、このチェックリストがより生きてくるかと思いますので、追加のご提案です。以上です。
○河内主査　丸山先生と六川先生にはご負担をおかけしてしまいますが、ご意見いただきたいと思いますので、どうぞよろしくお願いします。
○松本座長　現時点でお２人からご発言はありますか。なければないということで結構です。ありがとうございました。矢野オブザーバー、どうぞ。
○矢野オブザーバー　日本医師会の矢野です。オブザーバーの立場で申し訳ありません。資料２－２の確認をさせてください。
　例えば項番１から４では確認対象は「代表者」と書かれていて、４頁目の項番36以降では「代表者へのヒアリング」とあります。項番１から４のガバナンスに関するところは、我々ですと担当役員が代表者をやっていますが、項番36の「各アカウントの共有は禁止されている旨、手順などで周知されていることを確認する」の部分は、ヒアリングの対象は代表者というより担当者になってくると思います。代表者の捉え方だけ教えていただければと思います。
○河内主査　ありがとうございます。その点については手続規則の中でも、代表者が具体的にどのような権限を持つ者なのかについては規定していません。今いただいたご意見も踏まえ、どこまで規定するのか、首を絞めすぎず、実際の運用に適した形にアップデートできればと思います。ご意見いただきありがとうございます。
○矢野オブザーバー　もちろん代表者と言われれば、代表で説明をしておきますが、なかなか調整がつかないと審査が回らなくなってしまうと考えます。では、そこは確認をお願いします。
○河内主査　ありがとうございます。
○岡嶋主査　実際の運用では、おそらく代表者から委任された担当者の課長・室長など、ある程度責任のある者になるかとは思いますが、事務局の中でも改めて整理させていただきたいと思います。

○松本座長　これはチェックリストというより、元の規定でそうなっているということですか。
○岡嶋主査　そのとおりです。
○山内構成員　JIPDEC の山内ですが、担当者に任せるという方針に私は反対です。代表者と書いている限りは、代表者としっかり直接話をすべきだと思います。
　仕組みは異なりますが、国際規格 ISO/IEC 27001 に基づく ISMS 適合性評価制度においては、情報セキュリティマネジメントシステムの認証審査において、認証機関は組織のトップマネジメントの代表者にインタビューすることが通例になっています。それは技術的なことを聞くというより、その組織がどのような構成になっていて、どのような目標のためにどういうことをしているのか、業務の内容までしっかりと聞くためです。代表者が説明できないのであれば、代表者ではないので、「代表者から委任されている担当者に任せる」というような発言はやめていただきたいと思います。
○矢野オブザーバー　よろしいですか。今の発言に関して、我々としては否定させていただきたいと思います。先ほど申し上げましたように、項番 1 から 4 に関しては、もちろん代表者を出します。ただその後の具体的な業務に関しても、担当者ではなく代表者に全て答えさせるような体制を取るのですか。
○山内構成員　違います。項番 1 から 4 の代表者のインタビューのところは、代表者にやっていただくのがよいのではないかと申し上げただけです。
○矢野オブザーバー　それであれば納得できます。
○山内構成員　説明が良くなかったかもしれません。申し訳ありません。以上です。
○松本座長　おそらくこれは、今までもきちんと実施されてきたことだと思います。それをチェックリストに整理して記載していることで、このような建設的な議論ができるようになったのは、これを作ったからだとポジティブに捉えたいと考えます。審査をしたのに問題が起きたということがないように、進めていただければと思います。
　ではこの議題については、このくらいにさせていただきたいと思います。どうもありがとうございました。これで進めることで OK という結論です。

（2）暗号アルゴリズムの移行に関して
○松本座長　続いて「暗号アルゴリズムの移行に関して」の議事に入ります。まず事務局よりご説明をお願いします。
○岡嶋主査　事務局です。資料 1 の 6 頁をご覧ください。前回の専門家会議において、ルート認証局で採用する次期暗号方式への移行に向けた調査項目や検討すべき事項に関して議論を行い、耐量子計算機暗号（PQC）への移行可能性についても議論を行いました。また、次期認証局構築の要件検討に当たり、関係者への調査を実施し、調査が完了した部分から本会議にて結果を提示し、議論を行うこととした、と事務局としては認識しています。
　なお、今回の議題 2 においては PQC に関する議論は対象外とし、次の議題にて協議さ

せていただきたいと思いますので、ご承知おきください。

7 頁をお願いします。本日の議論では、前回整理した調査項目や検討すべき事項に関して、事務局より調査状況の中間報告を行います。中間報告を踏まえて、追加調査すべき点があるか等について、議論いただきたいと考えています。本日中にこの場で結論を出すことが難しいものに関しては、要点を整理の上、引き続き事務局で調査を進め、次回をめどにご報告したいと考えています。

暗号移行に向けての今後のスケジュールについても認識を共有したいと考えています。次期暗号方式でのルート認証局立ち上げの準備に向けたスケジュール上、次期暗号方式の決定は遅くとも年内に行いたく、可能であれば 10 月には次期暗号方式を決定するというタイムラインで考えています。11 月の専門家会議では、次期暗号方式を採用した後の認証局の構成についても議論を行いたいと考えています。

続いて 8 頁と 9 頁に移ります。ここからは各調査先から回収した調査結果の報告となります。まず認証局からですが、現在、日本医師会はヒアリング中であり、日本薬剤師会と MEDIS から回答をいただいています。特に HPKI カードの開発、製造について、3 年程度かかるのではないかとのご指摘をいただいています。また旧暗号方式と新暗号方式の並行運用期間中の運用への懸念、ベンダーへの周知、証明書検証部分における利用者の環境要件の明確化などについて、ご回答をいただいています。

続いて 10 頁に移ります。署名者、検証者についての調査結果です。基本的には薬局、病院、診療所が対象となりますが、今回のヒアリングは、医療機関のシステムを開発しているベンダーを通じての実施とし、一般社団法人 保健医療福祉情報システム工業会（JAHIS）を通じて各ベンダーにヒアリングを実施しています。こちらもヒアリングは継続して行っています。

前回の専門家会議において、宮内先生から医療訴訟等の有事における医療機関ではない第三者による署名検証の可能性についてご指摘をいただきました。この点について省内に設置している法務室の弁護士と相談したところ、基本的に医療訴訟においては電子カルテに登録された処方情報や調剤システムに登録された調剤結果を確認することが主で、裁判所等が直接電子処方箋の署名を見る可能性は低いのではないか、とのご意見がありました。しかしながら、平時、有事を問わず、第三者による電子署名の検証が行える環境を構築することは、重要性が高いと考えますので、この点については引き続き検討事項としていきたく考えています。

11 頁に移ります。HPKI の関連サービスとして、社会保険診療報酬支払基金に電子処方箋サービス等への影響をヒアリングしています。保存調剤情報の保存義務期間を考慮した旧証明書の検証可能な体制の存続に関するご指摘を頂戴しているところです。またパフォーマンスに関しては、一般には RSA より ECDSA のほうが高速と言われていますが、実際のパフォーマンスについては今後の検証項目となっています。また電子処方箋サービスに接続するシステム及びタイムスタンプシステムへの影響に関しては特段の懸念はいただい

ていないものの、こちらも今後の検証の必要性についてご指摘をいただいています。
　また総務省にはタイムスタンプ制度についての確認を実施しています。総務省が発行している「タイムビジネスに係る指針」及び「時刻認証業務の認定に関する実施要領」に記載の要件に準拠する必要があるとのご指摘をいただいていますが、今回採用を予定している ECDSA P-384 については、11 頁に記載している 3 つの要件に準拠していると考えています。
　続いて 12 頁に移ります。関連サービスとして MEDIS に、リモート署名システムへの影響について確認しています。現在の分散鍵による署名は RSA 暗号のみ対応し、 ECDSA での実装については検討段階と伺っています。また暗号切り替えの際に証明書の発行者情報の変更があった場合に関するご指摘と、並行運用期間中の運用に関する懸念、パフォーマンスへの影響についてもご指摘がありました。
　調査結果のサマリーの中間報告は以上です。引き続き調査結果の回収を進め、次期暗号方式移行に関する要点整理を実施していきたいと思います。本議題についての事務局の説明は以上です。松本先生、よろしくお願いします。
○松本座長　ご説明ありがとうございました。それでは暗号アルゴリズムの移行に関してご意見ご質問があれば、お願いします。佐古構成員、どうぞ。
○佐古構成員　ご説明ありがとうございました。11 頁のタイムスタンプシステムへの影響に関してお聞きしたいのですが、どのようなタイムスタンプシステムを使われているのかという点と、調査結果に「ECDSA で署名された電子データへのタイムスタンプ付与」と書いてあり、これは電子データに ECDSA 署名がされたのであって、タイムスタンプの署名アルゴリズムが何かについては言及していない文章だと思いました。しかし次の総務省の調査結果では「時刻認証業務のデジタル署名で用いられる署名アルゴリズム」とあり、これはいかなるデータにせよ、タイムスタンプをする時の署名の話をしていると思うので、少し食い違いがあると思ってお聞きしました。
○岡嶋主査　支払基金で採用しているタイムスタンプシステムについては、申し訳ありませんが、改めて回答させていただきたいと思います。
○佐古構成員　はい。分かりました。
○松本座長　下から 2 点目で、署名付きのデータに対してさらにタイムスタンプを付与すると書いてありますが、本当ですかというご質問ですか。
○佐古構成員　いいえ。それはいいと思いましたが、次の「タイムスタンプ制度との整合性・懸念点」の調査結果では、対象データではなく、タイムスタンプとして使うデジタル署名の話をしているような気がしました。
○松本座長　そちらはそのとおりだと思います。デジタル署名方式のタイムスタンプ生成の方式について、どのデジタル署名を使うかということを言っています。
○佐古構成員　はい。今回は両方とも対象ですかということもお聞きしたかったのです。
○松本座長　支払基金様の最後の調査項目「タイムスタンプシステムへの影響」について、

タイムスタンプ付与はどこで行うものを指しているのか、というご質問だと思います。
○岡嶋主査　タイムスタンプ付与については、電子処方箋管理サービスの中で行われているものだと思いますが、こちらも確認させてください。申し訳ありません。
○佐古構成員　ありがとうございます。
○松本座長　他にありますか。基本的に現行 RSA 方式で行っているものを ECDSA に変える、それに伴うもろもろの課題を洗い出していただいていると思います。資料に書いてあるもので、今のように何を指しているかをよく理解したいという意味での質問などありましたら、お願いします。
　日本医師会様へのヒアリングは、いつ頃、収束する見込みですか。
○岡嶋主査　こちらも現在確認させていただいているところです。今 HPKI カードの対応について確認を進めていただいており、その部分が確認でき次第、回答いただける見込みと聞いています。
○松本座長　7 頁のスケジュールで、次回専門家会議は 9 月実施となっていますが、その時には調査報告は全部そろっているのでしょうか。
○岡嶋主査　その予定で動いています。
○松本座長　いかがですか。特に重たい課題について、ここで議論できればと思います。林構成員、どうぞ。
○林構成員　林です。もちろん中間報告であることは認識していますが、松本座長からもおっしゃっていただいたとおり、IC カードのところが、おそらく一番重くなるだろうと思います。他のシステムはソフトウェアなので、と言うと担当の方に怒られてしまうかもしれませんが、やはり調達を考えると IC カードの部分が一番重いと思います。
　今 HPKI カードがどの程度の機能を持っているのか、例えば既存の CC 認証などを取られている IC カードを使われていると思いますが、既存のカードの流用ができるのか、流通しているものを使っているのか、それとも完全にカスタムしているのか、ソフトウェアがどの程度の量を作られているのかなど、そういったことが多分この粒度の調査だと全く見えないと思います。これで次回、暗号アルゴリズムもスケジュールも決めようというのは、少し厳しいのではないかと思ったというのが素直な感想です。ですから、ここはかなり掘り下げて、もし途中で必要であれば文書等を回していただいて検討したほうがよいのではないかと思いました。以上です。
○松本座長　そのご意見はもっともかとは思いますが、おそらくどこでもやっているような話なので、やると決めてお金をかければ、すぐにできるものだと私は基本的に思っています。しかし、項目をきちんと整理して、それぞれどのような課題があり、このような理由で解決するのだ、あるいはできているのだということを、まとめる必要はあると思います。理解して、我々のこの会議でゴーサインを出せるようにしたいと思います。
　ご意見はありますか。どうぞ、菊池構成員。
○菊池構成員　菊池です。一般的な質問でもよろしいですか。12 頁で、現在、分散鍵によ

る署名が行われているとのことですが、分散する署名は一体誰と誰に分散しているかという基本的なことです。

もう一つ、別の質問ですが、12 頁の調査結果の最後のところに、署名アルゴリズム指定ロジックの追加が記載されています。既存の例えば CMS などの一般的なデジタル署名の方式では、通常は署名アルゴリズムも同時に記載する仕様になっているのではないかと思います。現在の電子処方箋サービスにおける署名の仕様は何を使っているかについて、教えていただけますか。

○松本座長　これはリモート署名システムの話をされていますか。

○菊池構成員　はい。そのとおりです。

○松本座長　現行どういう方式で、それから ECDSA にした場合にどうなるのかは検討段階と書かれていますが、検討がどの程度進んでいるのかも含めて確認しないといけないと思います。

2 点目のご質問は、「並行運用期間中は」という前振りがあって「署名アルゴリズムを指定するロジックの追加が必要」とのことですが、最初は 1 種類しかなかったので、そもそもそういう項目はないのかというご質問でよろしいですか。

○菊池構成員　はい。

○松本座長　いかがですか。これは事務局から回答可能でしょうか。

○岡嶋主査　できれば、MEDIS に回答いただきたいと思います。

○山本オブザーバー　よろしいですか。

○松本座長　お願いします。

○山本オブザーバー　署名アルゴリズム自体は、[redacted] でやっています。分散鍵は[redacted]株式会社で[redacted]分散データベースを管理していただき、それを我々が監査しています。[redacted]分散の秘密分散を使っているので、データベースとしては 2 つです。それは鍵の管理の話ですが、 ECDSA に移管した場合、移行中は両方の私有鍵の署名のリクエストが来るため工数が増えます。切り替わってしまえばそれほど問題はないと思いますが、切り替えの間の 5 年間は 2 つのアルゴリズムに対応しなければならないという意味で、ここに書かれていると理解しています。分散鍵に関しては今、 HSM を使うことに移行できるかどうかを検討中です。

○松本座長　HSM はどこに置く想定でしょうか。

○山本オブザーバー　AWS 上です。

○菊池構成員　回答をありがとうございました。前半の分散に関しては、[redacted]わざわざ分散署名をする必要性もそれほど高くないのではないかと感じました。また[redacted]分散で閾値法でもないとのことなので、技術的にはそれほど難しいものでもないよ

うに思います。例えば２つ署名してもいいわけで、今回の移行に当たり、すごくクリティカルな条件ではないと私は感じました。
○松本座長　２つ署名することはできません。
○菊池構成員　そうなのですか。
○松本座長　アルゴリズムは同じで、検証はカードで署名した場合と全く同じようにできないといけないので、違う方式で署名することはできません。
○菊池構成員　ただ閾値法ではないので、秘密鍵を２つに分割して、うまく分散署名するようなことは、DSA でもできそうな気がしました。
○松本座長　できるとは思いますが、具体的にどのような方式で、それで大丈夫なのかを確認する必要があると思います。
○菊池構成員　分かりました。前半についてはかなりクリアになりました。教えていただきありがとうございました。後半の部分の署名アルゴリズムの指定についてはいかがですか。署名アルゴリズムを指定するような署名方式が一般的だと思ったのですが。
○山本オブザーバー　先ほど申し上げましたが、２つのアルゴリズムが混在する時期が５年間あります。
○菊池構成員　単一のアルゴリズムでも、自分がどういう方式で署名しているかは、OID などで指定して署名するのが一般的だと思います。
○山本オブザーバー　もちろんそうですが、対応するアプリケーションが必要になるという意味です。
○菊池構成員　分かりました。署名のフォーマットとしては、元々署名アルゴリズムは明記されていたので、それを検証側がきちんと検査することが追加で必要であると理解しました。
○山本オブザーバー　検証は、当然アルゴリズムを見て検証するので問題ないのですが、鍵管理サービスにおいて署名値を生成する時にどちらのアルゴリズムを使うのか、もちろん菊池先生がおっしゃるとおりアルゴリズム自体は指定されていますが、それをスイッチして実施するためのアプリケーションが必要になります。そのため、工数、リソースが倍になります。大したことはないと思いますが、そういう意味での困難さがあります。
○菊池構成員　分かりました。どうも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。他にありますか。宮崎構成員、どうぞ。
○宮崎構成員　宮崎です。今回のヒアリングや調査の対象とすべきか分かりませんが、HPKI サブ認証局に関しては今いろいろと調査していますが、この間、サブ認証局の鍵更新があり、今度はルートから変えなければいけないため、その時の影響も検討を始める必要があるかと思いました。以上です。
○松本座長　事務局、いかがですか。
○岡嶋主査　ルート認証局を変える形であると認識していまして、現在それに向けた予算取りも含めた準備といいますか、調査も進めているところです。

○松本座長　林構成員、どうぞ。
○林構成員　林です。今のお話が出たので発言させていただくと、以前も話題に出ましたが、結局、証明書の寿命と併用期間のスケジュール表を作り始めないといけないのではないかと思います。サンセットプランと重複期間と新しい暗号アルゴリズム状態への完全移行のスケジュールは、結構複雑になるはずです。今、線表は 1 本ですが、場合によっては、これは可能なのかというところもありますが、あくまで方法論の一つとして、発行する証明書の有効期間を短くしていくことによってサンセットを容易にするようなプロセスも検討されていると、私自身は認識しています。それを採用するのか否かについても検討事項として挙がってくると思います。今のところ、まず暗号アルゴリズムを決めることも当然重要ですが、移行プランの全体像についても並行して考えていかないと、開発ベンダーのスケジュールも厳しくなると思います。実際の運用が一番重要だと思いますが、薬局も含め、現場の方々のスケジュールが見えてこないと、ゴールにたどり着けない可能性があると思い、コメントさせていただきました。以上です。
○松本座長　一番遅くて、いつから開始しないといけないという制約はありますか。
○岡嶋主査　現在使っている暗号アルゴリズムが2030年までですので、それまでには移行を完遂させる必要があると考えています。
○松本座長　2030 年のいつからですか。
○岡嶋主査　具体的な日にちまでは認識していません。
○松本座長　そこまでにはスタートしないといけないといいますか、望めば全ての人が利用できるようにしないといけないということですか。
○岡嶋主査　スタートしていないといけないと考えています。望めばといいますか、新しい暗号規格に対応したカードを発行できるようにしないといけないと認識しています。
○松本座長　今、林構成員がおっしゃったのは、そのようなことも含めて併存期間はいつまでなのか、ある時期から先は古いシステムを使ってはいけないということも含めてスケジュールを立てないといけないだろうということです。ただ、おそらく概要は検討されていて、ここに出していないだけではないかと思われますが、どうですか。
○岡嶋主査　座長のご指摘のとおりです。事務局としても、林先生がおっしゃったことの必要性は認識していて、今、頑張って絵を描こうとしていますが、あまりにも複雑すぎて、なかなか追いつかないのが現状です。今回の会議には間に合わなかったのですが、なるべく次回には出せるように準備します。
○松本座長　ありがとうございます。他にありますか。では横田構成員、どうぞ。
○横田構成員　横田です。今の議論に関連して、実際に今、電子処方箋サービスは既に動いているとすると、薬局あるいは医療機関において新たなサービス利用者にコストがかかると思います。そういった負担の部分も含めて、スケジュールの調整が必要なのではないかと思います。以上です。
○松本座長　ご指摘をありがとうございます。事務局、どうぞ。

○岡嶋主査　横田先生にご指摘いただいたとおり、医療機関や薬局様の負担はどうしても生じるのではないかと考えています。今回の暗号移行が電子処方箋の普及阻害になってはいけないと考えますので、そうならないようにスケジュールについてはしっかりと段取りを立てて進めていく必要があると認識しています。
○横田構成員　ありがとうございます。よろしくお願いします。
○松本座長　他にご意見ご質問はありますか。よろしいですか。これは非常に大きなテーマで作業量も多くなるかと思いますが、情報をきちんと収集した上で判断できるように準備を整えていただければと思います。よろしくお願いします。それでは、ひとまずこの議題は以上とします。

（3）耐量子計算機暗号（PQC）について
○松本座長　「耐量子計算機暗号（ PQC ）について」に移ります。前回、耐量子計算機暗号（PQC）もこれから使っていこうという動きになっているので、現行の暗号技術のアルゴリズムあるいは鍵長を変える時期と PQC をどう取り扱えばいいか、非常に悩ましい時期になっているとの議論がありました。 PQC について専門家会議のメンバー間で認識を共有できればよいのではないかということで、事務局より、何か説明するよう依頼されましたので、3頁分だけ資料を用意してきました。
　2頁、お願いします。これは私のオリジナルの図で、コピーライトを付けてあります。間違っているかもしれませんが、ご容赦ください。
　図の右側に書いてあるように、量子計算機（量子コンピュータ）は、量子力学の現象を利用して並列計算を実現し、従来型の電子計算機（スーパーコンピュータ）では効率的に解けなかった問題の一部を効率よく解けると期待される次世代の計算機のことである、と一応定義します。
　この図の右下に「理想的な量子コンピュータが得意な計算可能問題」とあり、※が付いていて、下に「指数関数的に巨大なユニタリ行列（ベクトルの長さを不変に保つ行列）の乗算として表せる問題」と書いてありますが、こういうものについて非常に得意で、効果を発揮するだろうと言われています。
　理想的にはそうなのですが、現実にはまだ全く開発できていません。できると信じて頑張っている研究者がたくさんいらっしゃるという状況です。ただ否定的な人もいるので、本当にどうなるかはまだ分からないところではありますが、量子計算機技術の進展に伴い、従来型の計算機に対してセキュリティを有している一部の暗号技術について、将来セキュリティが低下する、いわゆる危殆化について懸念が示されています。
　図の補足をすると、図の左側に「従来型の電子計算機（スーパーコンピュータ）が得意な計算可能問題」と書いてありますが、私がわざわざ「計算可能問題」と言っているのは、どのようなコンピュータを使っても計算できない問題があるということが頭にあるため、しつこいですが「計算可能」と書いています。

それで、従来型のスパコンでは簡単に解けないであろう問題をベースにして、赤い丸で書いてある RSA 暗号や楕円曲線暗号が作られて使われている状況です。

ところが、まだできていませんが理想的な量子コンピュータができた時に、赤い丸のところは量子コンピュータが得意な計算問題になってしまいます。従って、強力な量子コンピュータが出てくると、今使っている暗号技術が危なくなってしまう恐れがあるのです。そのため、理想的な量子コンピュータができたとしても、それが不得意である、あるいは得意とは言えない問題をベースにするような暗号技術を考えようというもの、それが耐量子計算機暗号です。青い丸で書いてある問題をベースにするものであり、従来のコンピュータも新しく出てくるかもしれない理想的な量子コンピュータも、いずれも不得意な問題をベースにして作るものが耐量子計算機暗号であると理解していいかと思います。

一つ前の議題は、赤い丸の中の RSA 方式を ECDSA 方式に変えるという話でした。それに対して PQC を使っていくということは、青い丸のほうに行かなければいけないので、全く違う方式になりますし、アルゴリズムからして大きく異なります。昔は大変だと思われていましたが、既に実用化されていて、使おうと思えば使っていけます。ただし標準化をしっかりとしなければいけません。また世の中で IoT など、末端に近いところにも暗号技術がどんどん使われるようになり、全部に対応できるようにしないといけません。IC カードから何からそのようにしていかなければいけないということになるので、これを置き換えるのは、そう簡単な問題ではないということになります。

3 頁をお願いします。我が国では、二十数年前から政府系の機関で使う暗号技術について、しっかりとセキュリティや実装性を評価し、使っても大丈夫な暗号を「電子政府推奨暗号リスト」に入れています。それから、セキュリティが保たれていることが確認できているが使用実績がまだない、世の中で使おうと思ってもアベイラビリティが低いものについては、「推奨候補暗号リスト」があります。また、今まで使っていたが危殆化してセキュリティが十分でないことが分かったので、互換性維持のためのみに使って構わないリスト「運用監視暗号リスト」も用意してあります。これら 3 種類の暗号リストを総称して「 CRYPTREC 暗号リスト」と言っています。

右側に書いているように、 CRYPTREC とは Cryptography Research and Evaluation Committees の略で、最後が複数形になっているのが特徴ですが、先ほど申し上げた一つ目の電子政府推奨暗号リストなどに掲載されている暗号等の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討すること等を通じ、セキュアな IT 社会の実現を目指すプロジェクトのことです。デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会と、国立研究開発法人情報通信研究機構（ NICT ）と独立行政法人情報処理推進機構（ IPA ）が共同で運営する暗号技術評価委員会及び暗号技術活用委員会から成り立っています。また、それぞれの委員会の下にはワーキンググループ等があります。現在、私が暗号技術検討会の座長と暗号技術活用委員会の委員長を務めています。暗号技術評価委員会の委員長は、東京大学の高木先生が担当されています。ここは、我が国の暗号関係

の研究者が、ある種予備役のような形でリザーブされていて、何かあった時には集まって検討できる体制があります。そのような盤石なネットワークを持っていることが強みであり、一定の信用をされているのではないかと思われます。

CRYPTREC も、かなり前から耐量子計算機暗号に着目し、調査は続けてきました。その最新版が 3 頁左側の 1 番目にある「耐量子計算機暗号ガイドライン（2024 年度版）」で、これは少し難しいのですが、かなり詳しくサーベイがなされています。

２番目の「量子コンピュータが共通鍵暗号の安全性に及ぼす影響（2024 年度版）」では、共通鍵暗号も耐量子計算機性を持っていないといけないということで検討しています。CRYPTREC の外部評価で、ある方にお願いして調査していただいたものを踏まえて議論しました。汎用量子アルゴリズムには、Grover のアルゴリズムとそれを少し改良したものがあるのですが、ある種ブルートフォースで計算するような量子コンピュータでは、ビット数を倍にすれば今と同じセキュリティが保てるというような古典的なコンピュータに対する計算困難性を表すビットを n ビットとした時に、2n ビットにしておけば十分だろうということが分かりました。ですから、耐量子計算機暗号の実装を進める時に、共通鍵暗号についても考えなければいけないのですが、そちらの問題は相対的には軽く、重たいのは公開鍵方式になっています。

３番目の暗号技術検討会は、昨年度末の 3 月 25 日に開催し、PQC への対応について議論し、CRYPTREC 暗号リストへの掲載に向けた PQC の技術的検討と、PQC への移行方針の検討を両輪として並行に進めていくことを合意しました。これまでも「日本はどうするのか」ということは外国からも内部からも言われていながらなかなか走りだせない状況でしたが、いよいよお尻に火がついて、CRYPTREC 暗号技術検討会もきちんとやっていくということです。米国国立標準技術研究所（NIST）が米国の標準を作っていて、FIPS の 203、204、205 が出ていますが、非常に影響力が大きいため、安全性・実装性能の評価を先行して実施していこうということにようやくなりました。

それを受けて今年度、４番目の暗号技術評価委員会の PQC に関する活動（2025 年度）として、今の FIPS-203、FIPS-204、FIPS-205 について評価をし始めたということと、もろもろの動向等の調査をしていくということで始まっています。

それから 5 番目の暗号技術活用委員会の PQC に関する活動（2025 年度）について、これも同様に単に技術論だけではなく、各国が PQC をどんどん採用していこう、移行していこうという動向になっているので、それについてどうすべきか、暗号技術を活用するという観点で項目を洗い出したり調査したりする活動を開始しました。

この辺りの状況については、今月 25 日に開催される CRYPTREC シンポジウム 2025 でも議論します。まだ参加可能のようですので、よろしければお申し込みください。

４頁をお願いします。このように CRYPTREC もきちんとやるということになったので、政府系では 5 月 29 日にサイバーセキュリティ戦略本部で「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」として、PQC への移行について次期サイバーセキュリ

ティ戦略に盛り込むことが決まりました。それを受けて、参考資料1にあるように、内閣官房のとりまとめで「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議」が6月30日に設置されました。年内に工程表の骨子をとりまとめ、サイバーセキュリティ戦略の改定に反映することになっています。この参加者には重量級の方々が入っています。スケジュールとしては、まず7月から 11 月に課長級会合によって検討し、11 月頃に第2回の関係府省庁連絡会議にて工程表の骨子を定め、第3回は来年度中に開催し、工程表を策定することになっています。

検討すべき論点は、参考資料1のほうが見やすいかと思いますが、「1．量子計算機の開発・普及状況及びそれに伴い危殆化する公開鍵暗号等の特定とその時期について」、「2．諸外国の動向の把握について」「3．耐量子計算機暗号（ PQC ）の安全性等の評価・確認とその時期について」「4．耐量子計算機暗号（ PQC ）への移行期限及び危殆化した公開鍵暗号等の利用に係る停止の時期について」「5．政府機関等の移行への対応に必要な支援策等について」「6．政府機関等の移行に向けた工程表（ロードマップ）の策定について」「7．その他」となっています。

いろいろな課題がありますが、世界中でこのように動こうとしていますので、我が国もうまく振る舞わなければならない状況です。情報としては既に公表されていることばかりですが、まとめてみました。何かご意見やご質問があれば、お願いします。

このような状況になっており、どれほど急いでいるかというと、例えばコンフィデンシャリティ、守秘性、いわゆる暗号化しなければいけないものについては、今はまだ解読マシンができていませんが、将来できるかもしれないので、「今から将来できるかもしれない解読マシンに耐えられる暗号技術を使って通信など記録をしておかなければならない」という議論があります。そういう観点で「早く移行しないといけないのではないか」「少なくとも使えるようにしなければいけないのではないか」という議論があります。

それからデジタル署名についても、同じように後で偽造や改変ができるマシンが作られてしまうので、その時期までに施されたデジタル署名が信用できなくなってしまいます。従って、これも同時に考えていかなければいけないということです。特に HPKI においては公開鍵証明書や署名技術そのものが脅かされることになります。もろもろの暗号技術は機密性保持のための暗号技術も同時に使われていきますので、コンフィデンシャリティとインテグリティ両面の暗号技術について耐量子計算機性を持たせていかないといけない状況になっています。そのため、いつ本当に量子計算機ができるかは分からなくても移行を考えなければいけないというのが、非常に難しいところです。

○山内構成員　先生、質問してもいいでしょうか。

○松本座長　どうぞ。

○山内構成員　松本座長からの丁寧なご紹介ご説明、本当にありがとうございました。7月 25 日の CRYPTREC シンポジウム 2025 については、JIPDEC の職員を行かせるようにします。

質問は、量子計算機に対応した PQC の利用について検討する体制ができて、参考資料１の（資料３）に「検討すべき論点（案)」と書いてありますが、私自身がよく整理できていないのは、今日この HPKI 専門家会議でも議論していますが、2030 年までに暗号移行していかなければいけない、他の政府系の PKI、あるいは「電子署名及び認証業務に関する法律」に基づく認定認証業務における認証局の対応についても、2027 年頃までにやらなければいけないというように、 HPKI も含め現場で動いている話と、関係府省庁連絡会議で議論していく話はどのような関係にあるのでしょうか。一般の方でも分かるように先生の分析を教えていただきたいと思います。

○松本座長　HPKI もそうですが、JPKI やその他全部、暗号技術を変更しようという状況になっている中で PQC が出てきたのですが、これを避けていた人たちが多いのです。これは私見ですが、もっと前からきちんと議論しておけばよかったのに、と思いますが、そうも言っていられません。PQC に変えることが決まっているのであれば、既存暗号の更新を遅らせる可能性すらあり得ると思いますが、今はそうはなっていません。PQC はまだよく分からないので、いつから使うのか、本当に使うのかということが全く決まっていないという状況かと思います。

○山内構成員　決まっていないということが分かりました。ありがとうございました。

○松本座長　しかし、検討は真面目にし始めた、という状況です。林構成員、どうぞ。

○林構成員　PQC の移行に関してはいろいろな議論があると私も伺っています。その際に考えなくてはいけないこととして、暗号学的な側面以外に、おそらくリスクベースの話があると思います。例えば処方箋は処理されて 1 週間以内には大体消費されて、その機能を失うわけですが、それに対して PQC の危険性がどの程度のリスクがあるのか、リスク評価のようなもので、どこの部分にはどの程度必要なのか、例えばルート認証局においては当然必要であろうといった区分があると個人的には思っています。過去の処方箋を書き換えられたら困るケースも、もしかしたらあるかもしれません。そういうことも含め、分析をしっかりやらなければいけないと思っています。

PQC は今回、手前の暗号移行の話に対して変更部分は非常に大きく、鍵サイズが大きくなることも含め、かなり影響範囲が広いと認識しています。また松本座長もお話しいただいたとおり、まだ解読されるマシンが存在しない状況で、どこまでリスクに対して投資をするのかをしっかり整理しないと、適正なリソースの投入や計画がしにくいだろうと思います。ただ、この分析そのものにコストがかかるため、そこも含めて全体を見ていただく必要があるかと思います。以上です。

○松本座長　他にありますか。

○岡嶋主査　今、林先生からコメントをいただきましたので、事務局として考えていることを補足させていただきます。今回、2030 年に向けて暗号移行していく話をする中で、PQC を国全体として 2035 年、2040 年までに絶対やらなければいけないと言われた時に、今やっていることと同じことを 5 年後、10 年後にもやらなければいけません。我々事務局

が楽をしたいわけではありませんが、医療機関、薬局、サブ認証局の負担も同程度かかります。こうした社会的コストを考えると今、難しい局面にいると考えています。

先ほどの議論の中で横田先生からのご指摘に対して申し上げましたが、暗号移行について、我々専門家会議の中では絶対にやらねばならないというコンセンサスは得ていると認識しています。しかし実際に利用する医師、薬剤師、また国民の皆様に対して、社会的コストをかけることについての理解がどの程度得られているかというと、かなり厳しいものがあるのではないかと考えています。

ですから、移行に関しては利用者の目線に立って適切な形で進めていければと考えていますし、 PQC に関してもどの程度移行が望まれるものなのか、リスク分析に関しても併せて行わなければいけないと思います。電子処方箋に限れば、基本的にオンライン資格確認等システムのネットワークに存在しているものなので、どの程度許容できるのか、逆にどの程度許容されないのかも含めて、医政局医療情報担当参事官室というより厚生労働省として考えるべき課題だと考えています。以上です。

○松本座長　どうぞ、山本オブザーバー。

○山本オブザーバー　処方箋は有効期限の短いものなので、あまり影響はないと思いますが、問題は調剤記録です。記録としてずっと残るもので、かなり時間を置いてからも参照されるので、書き換えられると結構影響が大きいと思います。電子処方箋という名前は、あまり詳しくない方は処方箋だけだと思われるかもしれませんが、処方箋と調剤記録のペアであって、調剤記録への影響は大きくなるかと思います。

松本座長にお伺いしたいのですが、米国では PQC への移行の開始は 2030 年と理解していますが、実現されるのでしょうか。

○松本座長　少し前には 2030 年と言っていましたが、現在は 2035 年になっています。それすら本当にできるかどうかは分かりません。必ずやるとは言っていて、10 年以上前から準備している状況ですので、やるのだろうと思います。

あとはベンダーといいますか、実装面やビジネス面もかなり PQC に舵を切っているところが多いので、計算能力が高い、トラフィックが多いところから進んでくる可能性はあります。それからスマートカード、IC カード、クレジットカードも、そちらのほうになるかもしれません。スマートフォンなどのメッセージングサービスで、特にプライバシーを気にして、将来にわたっても絶対に自分たちの通信は解読されないようにしたいと強く望んでいる人たちもいるため、そういったところから先行して使われていく可能性は十分あると思います。

スマートフォンやスマートカードで皆が PQC を使っている状況になると、それに合わせて他のサービスも全部 PQC への移行が進む可能性はあると思いますが、当然併用期間が発生する中で、いつからそうなるのか、あるいは、どのようにうまく移行していくのか、これが一番悩ましいところかと思います。非常に難しくて、本当に悩んでいる方が多い状況かと思います。大した答えになっていませんが、以上です。林構成員、どうぞ。

○林構成員　難しいことをさらに難しくするような話で恐縮ですが、本当に量子計算機を使ってまで特定の人の薬剤情報を改ざんするかと言われると、量子計算機が世の中に転がっている状況にならない限り、なかなかないだろうと考えます。例えば要人であった場合には狙われるかもしれませんが、そういったリスクと実際の攻撃可能性などを見ていかないと、費用対効果が合わないと思います。ですから、どこに PQC が必要なのかをしっかりと見定めることが第一歩だと思います。しかし残念なことに、量子計算機の進歩の部分がまずよく分からない、進んではいるけれども判断が難しい、それが問題をより難しくしていると思います。コメントまでで恐縮ですが、以上です。
○松本座長　他にありますか。そういう状況で私がどう思っているかをご披露しました。ありがとうございました。それでは３番目の議題は終了します。

（４）連絡事項
○松本座長　続いて連絡事項について、事務局よりご説明をお願いします。
○岡嶋主査　松本先生、無理なお願いを受けていただき、ありがとうございました。大変勉強になりましたし、会議の中でも改めて認識を一致させることができたのではないかと思います。誠にありがとうございました。
　次回の専門家会議は、先ほどの議題でも少し触れましたが、２か月後の９月を予定しています。こちらについては別途日程の調整をさせていただきたいと思います。
　議論内容としては、８月に行う MEDIS 認証局準拠性審査の結果の報告と、また今回、暗号移行に向けた懸念点等について中間報告をさせていただきましたが、そちらの最終結果がおそらくまとまっていると考えていますので、その報告、及び暗号移行の規格の決定について、とりまとめを行いたいと考えています。
　先ほど委員の皆様からもご指摘いただいたように、９月、10 月に決めていくことについては少々無理があるといいますか、厳しいスケジュールになると考えています。従って、委員の皆様のご都合がつけば、次回に関しては事前に資料のご説明の機会をいただきたいと考えています。ご説明の段階でどの程度、粒度の高い資料が用意できるかは実際に進めていく中での判断となりますが、事前説明についても改めて日程調整をさせていただきたいと考えています。事務局からは以上です。
○松本座長　ありがとうございました。ただいまのご連絡事項に関して、何かご質問などはありますか。よろしいですか。

閉会
○松本座長　今日もたくさんのご意見をいただき、ありがとうございました。引き続き、重たい課題が山積していますので、事務局の皆様、ぜひよろしくお願いします。次回会議の開催前に個別のご説明等があるとのことですので、その折には構成員の皆様もどうぞよ

ろしくお願いします。それでは本日はこれで閉会とします。ありがとうございました。リモートの横田先生もありがとうございました。

以上