第２９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６年９月１１日(水) １８：００～

場所 AP 東京八重洲　K ルーム

（1）HPKI リモート署名サービス評価基準の進め方
○井上専門官　ただいまより第 29 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を開催いたします。本日の会議の構成員の参加状況ですが、専門家会議構成員の柴田構成員、林構成員は欠席、濱口構成員、宮内構成員、横田構成員、専門作業班の西山構成員、山本構成員がオンライン参加となっております。それでは、松本座長、以降の進行についてよろしくお願いいたします。
○松本座長　皆様、本日もどうぞよろしくお願いいたします。それでは、議事に入ります。今日議事次第にありますように、３つの議論になります。最初の議題につきまして、事務局よりご説明をお願いしたいと思います。よろしくお願いいたします。
○佐々木情報推進官　松本座長ありがとうございます。事務局より、まず議題１についてご説明いたします。議題１でございます。HPKI リモート署名サービス評価基準についてですが、前回の第 28 回にて、利用用途の限定解除および電子カルテ情報共有サービスの利用についてご議論をいただいた結果、持ち越しという形となっておりますので、その続きをさせていただければと思っております。資料１の４ページ目になります。最初に、これまでの背景について改めてご説明させていただきます。現在の構成員とは異なりますが、2022 年当時の HPKI 専門家会議にて、HPKI リモート署名サービスは電子処方箋に限定をして運用することで開始をご承認いただいた次第でございます。その際、承認にあたってはクローズドネットワークの中で運用されることを前提に承認となったと聞いております。その後、HPKI 専門家会議は現体制に昨年度からなっておりまして、昨年にはリモート署名サービス評価基準を本会議の中で制定し、準拠性の審査も実施しております。評価基準の制定にあたっても電子処方箋での利用を前提として基準として作成していただきました。これらを踏まえまして、前回会議でリモート署名サービスの利用用途限定について、今後どのようにしていくのか議論させていただいている状況です。前回の議論を抜粋して資料に載せております。前回会議であがった論点としましては、「ネットワーク構成に絞ってよいのではないか」、「より一般的な基準として見直すべきではないか」、「対象文書も精査すべきではないか」、「専門家会議では、基準と監査を実施すべきで、利用するかどうかそれ自体は各サービス側で決めてもらうのが良いのではないか」といった様々なご意見をいただきました。また同時に、来年１月より予定をしております電子カルテ情報共有サービスについても、前回概要を説明させていただきました。このサービスにおいてリモート署名を利用してよいかどうかについても、その場でご議論をいただきました。こちらについても、「プライバシーインパクト」についてや、「そもそも電子署名が任意で良いのかどうか」、「リモート署名の利用については、モデル事業をやるのであれば、モデル事業側で判断をしてもらえれば良いのではないか」といったご意見をいただきました。ここまでがまず前回までの振り返りでございます。
　続きまして、資料１の５ページ目に移ります。これらのご意見を踏まえまして、事務局から進め方の案をご用意しましたので、本日はこちらの提案についてご審議いただければ

と思っております。方針案としまして、昨年度に電子処方箋用として作成したリモート署名サービス評価基準は、電子処方箋の仕様からオンライン資格確認で使っているクローズドネット、いわゆるオン資ネットで利用される前提で作成をしましたので、こちらについては電子処方箋限定の基準ではなく、他のオン資ネットを使ったサービスも含めてオン資ネット向けの基準という形で残しつつ、その他のネットワークやオープンネットワーク向けに保健医療福祉分野として一般的な基準を新たに用意するという二本立ての形で進めさせていただけないかと考えております。
これにより、HPKI 専門家会議としましては、リモート署名の基準としてカバーをする範囲を明確化し、それらの基準の準拠制審査の結果を公表することで、各サービス提供者側に専門家会議側から明瞭な形でリモート署名の状況を示すことができると思います。サービス提供者側がこれらを見て、リモート署名を自分たちは利用するのかどうか判断ができる形を整えたいと思っています。

具体的な話としまして、資料の灰色の方の現状の基準についてお話しさせていただきます。今の基準を振り返りますと、先ほどお話しさせていただいた通り、電子処方箋向けとしております。ただ、実際中身を紐解きますと、電子処方箋での特別な仕様というわけではなく、オンライン資格確認等システムの基盤での利用を前提にした記載がされており、クローズドネットワークのオン資ネット（いわゆる医療機関と政府系の医療 DX 施策として使っている、支払基金が持っているシステムを繋いでいるクローズドネットワーク）を利用する前提で記載をしております。現状この基準の中では電子処方箋という言葉が出てきまして、これら名指しで電子処方箋に使うものという基準になっております。今回の提案としては、電子処方箋向けと絞った記載をしている部分を「オン資ネット向け」と修正をさせていただきまして、オン資という医療 DX で繋がっているクローズドな世界の中だけで利用するシーンをカバーする基準にさせていただければと思います。合わせて、前回の議論の中で出させていただきました、サービス提供者は厚生労働省および実施主体が支払基金になる「電子カルテ情報共有サービス」につきましても、同様にオン資を使っているというところで、このオン資向けとする基準を用いて判断させていただければと思っております。

資料１の６ページ目に、参考資料として電子カルテ情報共有サービスのシステム構成を記載しております。これは前回も簡単にご説明をさせていただいたところでございますが、基本的に電子処方箋のシステムと署名に関わる部分は全く一緒でございます。ただ、利用用途としまして、処方箋で利用するものなのか、診療情報提供書（いわゆる紹介状）で利用するものなのかが違いとなっております。これらも踏まえまして、オン資ネット向けという形の基準として修正をさせていただけるのでありましたら、現行の基準をそのまま使用することができ、電子カルテ情報共有サービスでも本基準の準拠性の状況を見ながら、利用してよいかどうかサービス側で判断できるのではないかと考えております。

資料１の５ページ目に戻りまして薄緑で書いている部分でございます。新しい基準とし

て作成するものに関しましては、オン資ネット以外かつ医療分野という大きいくくりで作成する想定をしております。こちらについては、基準を今年度中に作るというような話ではなく、今後スコープから調査を行いつつ、デジタル庁で検討している一般向けのリモート署名の状況も踏まえながら、徐々に準備をさせていただければと思っております。

少し先のページになって恐縮なのですが、11 ページ目でスケジュールの案を記載しておりまして、この中にリモート署名の部分も少し書かせていただいております。我々の想定としましては、先ほどから説明をさせていただいている通り、現状の基準プラス新しい基準を作っていきたいと考えております。この中で周辺環境も見つつ、予算も含めた準備を来年度以降行っていきたいと考えております。まずは現行基準を維持しながら追加の基準を作成していくという方針を今日はお示しをさせていただきました。議題１について、事務局からの説明は一旦以上となります。松本座長へお戻しいたします。

○松本座長　ご説明ありがとうございました。それでは、リモート署名サービス評価基準の件につきまして、ご質問などありますでしょうか。いかがでしょうか。佐古さん、どうぞ。

○佐古構成員　佐古です。今回の資料をいただいて、気がついたところをいくつか述べさせていただきたいと思います。例えば、リモート署名の今の基準を拝見していますが、文章の中にオン資ネットに限定するという記述が特に見つかりませんでした。おそらく一般の人は、保健医療福祉分野におけるリモート署名サービスの評価基準というところで、どのような前提で作られていたのかということをこの文章だけで理解する必要があると思います。１点目は「オンライン請求ネットワークに限定している」というところがどのように読み取れるのか、お伺いしたいと思います。それが具体的にどこの文章に入ってくるのかよく分かりません。

○佐々木情報推進官　リモート署名サービス評価基準を画面投影させていただきます。

○佐古構成員　こちらは図２になっておりますが、1 点目は「オンライン請求ネットワークあるいはオン資ネットがどこに該当するのか」という質問です。2 点目は、リモート署名サービス評価基準の図２と今回の資料１の６ページに出てくる図 18 がどのように対応しているのかがわからないと、ちょっと議論が難しいと思います。３点目は、資料１の４ページの前回の議論ですが、確かにこのような発言があったと思いますが、この文面だけでは前後のコンテクストがわからないような議論になっているので、公開もされますので、一般の国民も読んで議論がわかるような文章にしていただきたいと思いました。３点です。以上です。

○佐古構成員　１点目が、「この図でオン資ネットがどこに当たるのか」と「これに限定した基準であるということがどこに書いてあるのか」ということです。

○松本座長　２番目の方がいいかもしれないですが、今事務局から表示していただいている図と、本日の資料１の図 18 との関係をちゃんと把握したいということが、まず１点。そちらから行きたいと思いますが、いかがでしょうか。佐々木さんどうですか。

○佐々木情報推進官　事務局でございます。ご指摘いただいております通り、現行のリモート署名サービス基準には「オン資向け」などそういった文言は全く入っておりません。本日の時点では、こういった二本立てにしてはどうかという方針をまずはお諮りしたいという趣旨でございました。２点目の図の中で、リモート署名評価基準の図２の中でオン資ネットはどこに当たるのかですが、今ここでお示ししている部分の中で、黄色に示している部分は医療機関側になっております。

左の「署名者」は医師や薬剤師になります。電子カルテなどが該当する「ドライバ」と「クライアントモジュール」が医療機関となっております。医療機関から出ていく際には、基本的にはオン資ネットしか繋がっておりませんので、必ずオン資ネットで出ていく形になっております。さらに、本日の参考資料として入れております、資料１の電子カルテ情報共有サービスの図18ですが、この中では「電子処方箋管理サービス」が右下の方に記載されています。これはリモート署名の方の図も同じように、右下の方に「電子処方箋管理サービス」と記載があります。この部分は、電子カルテ情報共有サービスであれば、電子処方箋管理サービスの代わりに、電子カルテ情報共有サービスが入ります。

○佐古構成員　了解しました。認証局とのネットワークは、一般のインターネットだと思ってよろしいでしょうか。そこもクローズドなネットワークなのでしょうか。緑色の一番上のところです。

○山本構成員　鍵の配送ですね。分散署名をかける配送のところは、専用線で一般のインターネットではありません。証明書執行リストの方は、これは一般のインターネットを介して証明書の執行リストを取得するようになります。

○佐古構成員　了解しました。ありがとうございます。資料１の５ページの２点目に「電子処方箋向けとなっている現在の基準は、『オンライン請求ネットワーク』に限定した基準として継続して使用する」とありますが、「限定している」という表記は今までにはなかったという理解でよろしいでしょうか。

○佐々木情報推進官　おっしゃる通りです。こういった形で限定をさせていただきたいというのが本日のご提案になっております。実際の記述等に関しましては、また別途用意をさせていただいて、お諮りするという形になると思っております。

○佐古構成員　ありがとうございます。１点目についてはクリアです。

○松本座長　２点目もわかったということですよね。

○佐古構成員　そうですね。

○松本座長　３点目というのが、今日の資料の、前回の整理の部分がこれだけだとわかりにくいのではないかということですが。

○佐々木情報推進官　事務局でございます。HPKI 専門家会議の方針としまして、セキュリティにかかる部分もありますので、公表については議事要旨という形で、議事録は丸ごと公開をしていない状況になっております。ただ、今までそういった形で運用してきましたが、今回ご議論いただいているような内容は広くお知らせしても問題ないと思いますの

で、今後議事録をどこまで出せるかは少し精査になりますが、構成員の皆様にご確認しながら、今まで以上に具体的な形で公表させていただければとは思っております。
○佐古構成員　この資料は多分公開されますよね。資料１の４ページの評価基準についての文章を読んでも、どう理解していいかわかりませんでした。例えば、「プライバシーと電子署名の関係はリモート署名だから違いがあるわけではない」というところです。確かにそのような発言があったことは理解しましたが、もう少し文脈を補ってそこだけ読んでもわかるような文章にするのがいいのではないかというご提案でございます。
○松本座長　なるほど。資料の公開はいつですか。
○佐々木情報推進官　この会議が終わった後に公開されます。資料１４ページ目の前回議論抜粋について、構成員の皆様には前回の議事録をお渡ししているので多分わかってもらえると思うのですが、確かにおっしゃる通り、国民向けという観点では少しわかりにくい文章になっておりますので、見直しをさせていただければと思います。
○松本座長　佐古さん、ご指摘ありがとうございます。それではそのようにしていただくということで、オンラインで参加していただいている濱口さんと宮内さんの手が挙がっております。まずは濱口さんからお願いいたします。
○濱口構成員　「オン資ネット向け」と「その他のネットワーク向け」の２つで、その他についてはスコープの調査研究から実施し作成するということで、新しいその他のネットワーク向けの基準を作るという点については、承知いたしましたし、賛同いたします。一方で、これまで作ってきたリモート署名基準に関して、オン資ネットを利用するということで、IP-VPN、IPSec で接続することでリスクが少なくて済むことから、軽い基準でできるというのは理解できます。ただ、そもそも、今あるリモート署名サービス評価基準は、今ご参加いただいている皆さんもご存知の通り、策定の過程から十分にリスクベースで議論した上で、十分時間を取って検討できているとは、なかなか言い難いものです。したがって、来年スコーピングや実際に調査業務を掛けて、新しいリモート署名基準を作る際に、本当に今の「オン資ネット向け」のリモート署名サービス基準が十分なのかどうかという評価も踏まえて、最終的に本当に二本立てでリモート署名基準ができるのか、あるいは新しくできるものに一本化できるのか等も含めた検討ができれば、より良い形になるのではないかと思います。
○松本座長　ありがとうございます。この点についてはどうでしょうか。本来そのようにするべきだと私も思いますが。
○佐々木情報推進官　濱口先生、ご意見ありがとうございます。事務局でございます。おっしゃる通りだと思います。今後、調査事業をどのような仕様で計画していくかにもよるかと思いますので、我々も、まずは予算の確保からスタートという形にはなりますが、追って調査事業を立てるにあたっては、今回頂いたご意見も踏まえながら、最終的にどういった形に着地するのか検討していきたいと思います。おっしゃる通り、新しいものを作るタイミングで、古いものも合わせて見直すことは、もちろん賛成いたします。そういった

形で調査事業を立てられるように準備をしてまいります。
○濱口構成員　ありがとうございます。よろしくお願いいたします。
○松本座長　それでは宮内さん、どうぞ。
○宮内構成員　宮内でございます。大きく分けると２点あります。まず１点目。オン資ネットとその他のネットワークの二分類にするというのは、大きく考えると、「医療側が一定のセキュリティがある場合」と「一定のセキュリティがないかもしれない場合」に分けて、一定のセキュリティがある場合しか、上側のオン資ネットのサービスは使わせないという意味だろうと理解しております。この理解が正しいかどうかも答えていただきたいですが、その場合に果たして接続のネットワークだけのことを考えればいいのかというところがよくわからないです。つまり、一定のセキュリティを満たす医療機関のみが利用するのであればオン資ネット向けの基準でもよいが、そうではない場合には、オン資ネット向け以外の基準という意味合いだと理解していますが、ネットワーク以外のところも考えなければならないのではないかというのが１つ目の質問です。もう１つは、灰色（オン資ネット向け）と緑（オン資ネット以外向け）のリモート署名の基準がどの程度違うのかはなかなか難しいところですが、おそらく、現在の灰色の部分をやっている場合にある一定の前提を置いているからこれでいいというところがあると私は理解しています。ですから、そのような部分を洗い出して、「灰色と緑の差分」をしっかり見極めることになろうかと思います。そこで、医療機関側のセキュリティを前提としているわけではない部分については、両者共通になりそうだと思っています。議論の進め方としてそのようなやり方もあるのだとご理解いただきたいと思います。
○松本座長　ありがとうございました。すいません。オン資ネットワークは正確には何と言いますか。
○佐々木情報推進官　事務局でございます。文言が正確には決まっていないため、一般的に使っている「オンライン請求ネットワーク」という言葉を使っておりますが、ケースによっては「オンライン資格確認ネットワーク」と略す場合もあります。さらに省略する場合は、「オン資ネット」という呼称を使っています。
○松本座長　それはちゃんと定義しないとダメです。
○佐々木情報推進官　厚労省側として言葉の定義ができておらず申し訳ございません。
○松本座長　どれが一番まともな言葉でしょうか。「オンライン資格確認」ですか。
○河野構成員　オンラインレセプト請求のネットワークが最初にあって、それを拡張するような形でオンライン資格確認を使うようになり、それがさらに今来ているので、全部が多分混じっている。
○松本座長　それを「オン資ネット」と略すのは非常に困りますね。「資格」の「資」がないのにも関わらず出てきてしまうというのは。
○河野構成員　最初にオンラインレセプト請求ネットワークが始まり、オンライン資格確認が大きく入ったので、利用者側がその認識が非常に強いのもあって多分こうなっている

かと思います。
○松本座長　「ネットワーク」がどこまでを指しているかですね。宮内構成員のご質問あるいはご指摘とも関係するかと思います。どういう要件を満たしているのかということですが。今日は何と呼べばいいですか。
○佐々木情報推進官　本日は「オン資ネット」と呼ばせていただければと思いますが、ここに関しては、言葉の定義を明確にするようにいたします。
○松本座長　今は「オン資ネット」と呼ぶことにします。けれども「オン資ネット」と言っているのが、単なるネットワークじゃないということですよね。要するに、システムであって、通信以外のそれに対応するシステムが動いているところについても要件があり、それを全部満たしているものが「オン資ネット」というものでしょうか。「オン資ネット」の定義自体が曖昧だというのが混乱の元であると思いますが。
○佐々木情報推進官　事務局でございます。ここに関しては本当に申し訳ございません。レセプト請求や電子処方箋、電子カルテ情報共有など、政府の医療 DX の施策として使っている支払基金に置いている諸々のシステムで利用されるネットワークのことを総称して、「オン資ネット」と呼んでおります。「オンライン資格確認」のネットワークということで、「オン資ネット」と呼ばせていただいておりますので、こちらに関しては、それぞれのサービスごとに、技術仕様を厚生労働省から出しております。その中でもシステムを組むにあたって、先ほど宮内先生がおっしゃった通り、セキュリティに関しても一定の要件を課しております。そういった中で、リモート署名の基準の中における「オン資ネット」、「セキュリティ」がどこまで入っているのかも含めまして、基準には具体的に記載させていただければと考えている次第でございます。
○松本座長　「オン資ネット」の定義がないのですね。
○宮内構成員　ちょっとよろしいですか？そもそも「オン資ネット」というのは具体的な今あるネットワークですが、この絵の中央の左の方に「オン資ネット」と書かれているところは、具体的な「オン資ネット」というネットワークだけじゃなくて、それ以外の IP-VPN、IPSec でもいいわけなので、なかなか難しいと思っています。「オン資ネット」と言われている、固有名詞のネットワークにつながっているものだけを指していますか。
○松本座長　そういうつもりだと思います。
○宮内構成員　そういうつもりなのですね。
○松本座長　資料１の５ページ左側の「オン資ネット」と書いてあるところは、「オン資ネット」を易しく説明しようとして、このような記述になっているのではないかと想像します。
○宮内構成員　ですが、灰色の部分の「対象サービス」を見ると、「オン資ネット等で提供されるサービス」と書いていますよね。だから私は他にもあるのかと思っていました。要するに、概念として、灰色の部分と緑色の部分は何で分けているのかを明確にする必要があると思います。先生のおっしゃる通り、「オン資」の定義がよくわからないから、ま

すます分からないですが、灰色と緑を区別するメルクマールは何かを明確にして、こういうものは上、こういうものは下と示さないと難しくなってしまう。
○松本座長　これは「オン資ネット」に限定ということですよね。「オン資ネット」が何なのか、我々全員が正確にわかってはいない現状ではありますが、事務局で用意していただいたのは「オン資ネット」に限定した話ですよね。これから定義されるかわからないですが、同等の技術を使っていれば、医療系でなくても良いという話ではないということですよね。
○佐々木情報推進官　事務局でございます。松本先生のおっしゃる通りでございます。まずは「電子処方箋管理サービスで使っているオン資ネット」と全く同じ環境の中では、この基準を使わせてもらえればと考えております。
○宮内構成員　趣旨としては分からなくはないですが、今後この分け方で基準を作っていこうという場合に、やはりもう少し高い視点から見た時に、こういうものとこういうものは分ける、例えば、「電子処方箋と電子カルテは灰色の方に該当する」という方が、話の流れとしては真っ当な気がします。これは私の意見です。
○松本座長　分かりました。ありがとうございます。私の感想ですが、それをやる余裕がないということでこうなっているのではないかと想像します。筋は宮内さんが言っているのが正しいような気はします。

○宮内構成員　もう一点質問ですが、先ほど申し上げましたように、２つの基準を作るときに、「オン資ネット」と言われるところで「オン資ネット」のセキュリティを前提としている部分を切り出してやっていくというのはいかがですかという指摘をしたつもりだったのですが、この点については、コメントをいただけますか？
○佐々木情報推進官　事務局でございます。おっしゃる通りだと思います。「オン資ネット」について、今回非常に広めに書いてしまいましたが、まずは電子処方箋に対してというところでこれまでも考えてきましたので、電子処方箋で使っているものが何なのか、そこで使っている「オン資ネット」がどういう定義であって、そこで使われているセキュリティの基準というのがどこまで対応しているものなのかを一度明確化してお示しできればと思っております。
○宮内構成員　分かりました。そのように進めていただければと思います。私からは以上でございます。
○松本座長　横田さん、どうぞ。
○横田構成員　横田です。宮内先生の話に関連することを先にお話しした上で本来の質問に入らせていただいてもよろしいですか。
○松本座長　はい。
○横田構成員　資料１の５ページで、先ほどご指摘があった通り、オンライン資格確認等システムが繋がっているネットワークを「オン資ネット」と呼んで、この資料では「オン

ライン請求ネットワーク」と呼ばれていると理解しました。それから、灰色の「対象サービス」のところですが、「電子処方箋管理サービス、電子カルテ情報共有サービスなどのオン資ネット等で提供されるサービス」のところの平仮名の「など」を取る。後ろの「オン資ネット等」の「等」も取った方が、今回の限定的なものになるのではないかというのが私の意見です。
○松本座長　これについてはいかがでしょう、佐々木さん。
○佐々木情報推進官　事務局でございます。ここで「など」を入れている経緯としましては、我々が医療 DX で作っている「オン資ネット」を今後も利用する予定でございまして、いろいろなシステムをこれから追加で作っていくことを想定しています。そのたびに専門家会議に諮らせていただくのか、それとも同等レベルのセキュリティであれば、そのまま利用していいのかという意味合いで「など」をつけさせていただきました。
○松本座長　分かりました。今横田さんからご提案があったところはそのままとし、その代わり、「オン資ネット」が何なのかを明確にし、その上で行われるサービスは全部認めるという方針で検討しますということですね。そうしましたら横田さん、次のご質問お願いいたします。
○横田構成員　分かりました。では、本来の質問ですが、私の理解が少し古かったら訂正していただけたらと思います。今回、厚生労働省のワーキング資料で、３文書６情報を標準規格として２文書６情報を標準化し、２文書の中の一つが今回の電子カルテ情報共有サービスで保存される診療情報提供書、もう一つの退院時サマリーもそこでは１文書として定義されておりました。もし今後電子カルテ共有サービスの中で、退院時サマリーも交換されるのであれば、「電子カルテ情報共有サービスにおける診療情報提供書等」というように、「等」をつけるのはいかがでしょうか。実際の署名が行われるかどうか私もわかりませんが、もう少し共有サービスで共有される情報があるのであれば、「等」をつけたらどうかという意見でした。
○松本座長　今の話は何ページですか？資料１の６ページの表の右上でしょうか。
○横田構成員　６ページのところです。
○松本座長　電子カルテ情報共有サービスでは利用用途が診療情報提供書しかないのですか、というご質問かと思います。
○横田構成員　そうですね。そのように考えて結構でございます。
○田中参事官　退院時サマリーについては規格が定まっていますが、単独で情報を共有するという仕組みではなく、あくまで診療情報提供書に添付ができるという形での共有を考えております。退院時サマリーに単独で署名をするというよりは、診療情報提供書にくっつくような形になりますので、今後文書を拡張していく可能性はあるものの、現時点では電子署名の対象としての利用用途としては、診療情報提供書のみでございます。
○松本座長　横田さんよろしいでしょうか。
○横田構成員　今の補足で十分理解できました。どうもありがとうございました。

○松本座長　それでは続きまして、西山さんどうぞ。
○西山構成員　西山です。資料１の 6 ページ目の図はちょうどよくわかると思いますが、前回作ったリモート署名の基準は、電子処方箋管理サービスを使って電子処方箋に署名をするという前提で、皆さん議論いただいていたと思いますが、オンライン資格確認ネットワークに接続しているアプリケーション全般に広げるという意識で作っていなかったというのが私の意識です。リモート署名の基準は、ネットワークが強固であれば同じ基準でいいのかというとそうではないと思っています。あくまでも前段のアプリケーション、例えば、電子処方箋であれば電子処方箋管理サービスのサーバーの堅牢性や、外部からの攻撃への防御対策、あるいはアプリケーションのユーザー認証がしっかりしているなど、様々な要素があって、それを前提にそこから呼び出す電子署名リモートサービスなので、例えばユーザー認証や脆弱性の問題は、前段のアプリケーションである程度担保されているという想定で、リモート署名サービスの基準を作っていました。したがって、同じリモート署名基準を使うのであれば、電子カルテ情報共有サービスのシステムの堅牢性やユーザー認証の強固性はどうなっているのか。それが電子処方箋管理サービスと同等だと言えるのであれば、そこから繋ぐリモート署名サービスの基準は同等なものでも良いのかもしれないですが、ネットワークの堅牢性が同じだからといって、十把一絡げに「リモート署名サービスの基準は同等でいい」とはならないのではないかと思います。したがって、先ほどの区分が、オン資ネットワークにつながっているシステムであれば「ある基準」、そうでなければ「別の基準」という切り分けは若干乱暴です。アプリケーションのセキュリティレベルも合わせて勘案しながら、どの基準を当てはめていくか議論するべきだと思います。
○松本座長　ご指摘ありがとうございます。先ほどのオン資ネットワークの定義次第で、「オン資ネットワークに接続できるシステムは何なのか」というところまでオン資ネットの定義の中に入っていれば大丈夫だと思いますが、そうではなくて、「電子処方箋に限定して個別に要件を満たしているものであったから、今までの基準で大丈夫」ということならば、西山さんのおっしゃる通りだと思います。この辺はどうでしょうか。
○佐々木情報推進官　事務局でございます。先ほど宮内先生からいただいたご意見と近しい内容だと思っております。セキュリティをどこまでご用意しているかという観点になってくるかと思います。
○松本座長　正確にはセキュリティというのは、ネットワークというのがどこまでをネットワークと呼ぶかということで、線の部分だけでなくてそれに繋がっているシステムのセキュリティの話をおっしゃっているのであればよろしいですが、単にセキュリティと言うとどこのセキュリティかわからないので。
○佐々木情報推進官　アプリケーション側のセキュリティに関しましても、基本的には電子処方箋管理サービスで定義しているものがございますので、そちらの内容を落としてきて、例えばネットワークの構成はどうなっているのか、アプリケーションのセキュリティはどうなっているのか、要件として整理をして、いわゆる「オン資ネット向け」と呼ぶ方

の基準について、ここはネットワークだけに限らず、アプリケーションの方も考慮して確認してまいります。
○松本座長　西山さん、ご指摘いただいた点について、確認をした上で進めていくということですが、よろしいでしょうか？
○西山構成員　はい、承知しました。よろしくお願いします。
○松本座長　お待たせしました。山内さん。
○山内構成員　JIPDEC の山内です。西山構成員のご懸念と似ていますが、資料１の５ページで見ると、厚生労働省としては、「オン資ネットを使っているサービスへのリモート署名」と、「オン資ネット以外（オープンなインターネットを使っているその他の保険医療福祉分野のサービスにおけるリモート署名）」と二段階で考えておられるように見えています。ネットワークがクローズドかオープンかというのは非常に大きな問題だと思いますが、実はアプリケーションのところで「リモート署名を行うのは本人である」ということを間違いなく担保できているか、そのレベル分けがむしろ重要です。リモート署名サービスの基準を去年から作ってきている中で、非常に重要なポイントとしては、ソールコントローラーシェアナサレベルと言って、ヨーロッパでは単にアプリケーションにログインするときの本人確認だけではなく、実際に本人が本人の意思に基づいて、暗号化を行うところまで含めて本人かどうかを確認する。二重の本人確認といいますか、ソールコントローラーのレベルが高いものか低いものかで分けていくのが、リモート署名サービスのレベル分けの話です。ポイントとしては、世の中に対してメッセージを出すときに、「オン資ネット」については去年から作ってきているリモート署名サービス評価基準、「その他」はオープンなのでもっと厳しいレベルの評価基準を作ればいいというように、２つの文章だけ作ればそれでよいという誤解が生じないようにしなければいけない。つまり、ネットワークの閉鎖性と開放性の話だけではなく、あくまでリモート署名サービスとして、アプリケーションとつながった一体の中で本人確認ができるかという、ソールコントローラーレベルのことも含めてレベル分けがなされているという体系的な基準が、最終的な仕上がりとして重要かと思いコメントさせていただきました。表現が難しいので大変ですが、「オン資ネット」の基準と、「オン資ネット以外」の基準を２つ作っただけで終わりではなく、それぞれの中でもレベル分けが必要じゃないかということを申し上げました。
○松本座長　オン資ネットではない方については、どういう区分をしなければいけないかという話に持っていくのか、それとも最初に宮内さんがおっしゃったように、そもそもこのリモート署名の利用を認めるという条件が何なのかということを純粋に定義して、「オン資ネットおよび現行のオン資ネットに接続されているシステムでは、条件を満たしているから同じ基準でよい」とする話ですよね。そうでないものについてはどのように扱うかは、今は棚上げして別途考えようということを言っていると思いますが、そこは２つですと言い切ってしまっていいのかという話ですね。
○山内構成員　そうですね。「文書を２つ作って切り離してしまう」ということですが、

本当はアプリケーションにおいて、どこまでソールコントローラーシェアナサレベルが必要なのかというところも違ってくるし、そういうアプリケーションごとの文書も本当は必要なのかもしれないなという気も少ししているので、文書を２つだけ作って、それぞれバラバラな形で運用されていくというのが良いのかどうか、少し疑問に思いました。
○松本座長　その懸念はあると思うのですが、リモート署名が保険医療福祉分野ではないところでルールが整備されていないところも問題だということで、自前でなんとかしようとされているわけですよね。そういう制約の中で、どのように振る舞っていくのがリーズナブルなのかという話かなと思うのですが、事務局いかがでしょうか。
○佐々木情報推進官　ありがとうございます。ソールレベルにつきましても、今後の検討事項だと認識いたしました。我々としましては、まずは電子処方箋に関しては認めていただいているという状況下でございますので、そちらに関しましては少なくともそこの部分は定義を明確にして整備をし、進めさせていただければと思います。緑色の部分に関しましては、もちろん１個でいいのかという議論もこれからしていくべき内容だと理解しましたので、こちらに関しても必ず１文書にしなければならないということもございませんので、そこも含めて来年度以降、調査研究も行っていく中で対応させていただければと思います。
○松本座長　資料１の５ページの「対応方針」というところの２つ目のポツの最後のところに「基準は２パターンとなる」と書いたが、書いておかなければよかったのにということですよね。今日の議論の結果、２パターンと言い切れないということでしょうか。
○山内構成員　要は、灰色と緑色の２つの文書だけに決め打ちできないというのが私の意見だったので、２つの文書だけ作ればいいということを意味しているとすれば、「基準は２パターンとなる」は削除した方がいいかもしれません。
○松本座長　私も同じことを申し上げました。削除しても特に実害はないですよね。他にご質問はよろしいでしょうか。
○松本座長　六川さんお願いします。
○六川構成員　専門作業班の六川と申します。厚労省様に要望が１点と、質問が１点ございます。まず、資料１の６ページの表を出していただきたいのですが、私は時々病院での業務と調剤薬局での業務を担当しておりまして、６ページの図については、電子カルテ情報共有サービスの技術解説書より抜粋と書いてあるので、薬剤師の人間像と調査薬局の場面が載っていない。今後専門作業班構成員として検証作業をするにあたっては、調剤薬局と薬剤師の先生の業務も含めた形で、医療全体構造の観点から検証しなければいけないので、今後作っていただく図については、ドクターの下の方に薬剤師を入れるということと、調剤薬局の業務を入れていただきたいというのが１点でございます。
　もう１点は質問なのですが５ページの表で、今日先生方がディスカッションされている下の緑の図で、リモート署名評価基準を新規作成して、「オン資ネット以外向け」ということで、これから検証作業をされるということなのですが、今厚生労働省の事務局で考え

ていただいているこの下の方の緑のスコープは、病院と調剤薬局の分野でどういうことを想定していらっしゃるのでしょうか。これが質問でございます。
○松本座長　では、先にこちらに回答をお願いいたします。
○佐々木情報推進官　事務局でございます。まず１点目の図に薬剤師と調剤薬局が入っていないというところでございますが、我々は電子カルテ情報共有サービスのチームとはまた別のチームでございますので、この場でこれを入れますというお答えはできないのですが、改めてそちらのチームの方に今日こういうご懸念をいただいたというところはお伝えをさせていただきます。
２点目は「オン資以外の場合にどのような利用を想定しているのか」というところかと思いますが、今のところまずは地域医療連携ネットワーク等で HPKI を使用しているものがあると聞いていますので、まずはそちらでの利用を念頭に置きながら、その他のものに関しましては、医療 DX 施策を進める中で民間のサービス事業と繋がれるようなものがないかなどを、調査をしながら進めていこうと思っております。今の時点でこのアプリケーション、このサービスに対して想定をしているというものは明確にはございませんが、一旦そのような形でお答えさせていただければと思います。
○松本座長　よろしいでしょうか。それでは矢野さんお願いします。
○矢野構成員　まず前提として、資料１の 5 ページの上の方の電子処方箋と紹介状に関して、今の基準で進めて良いのではないかというところに対して、それでいいのではないかという点があります。
６ページに移っていただいて、まずオンライン請求ネットワークなのですが、左の医療機関等システムのところに書いていないのですが、レセコンが入ります。図の右のギリギリのところに黒い四角が２つ上下に並んでいると思いますが、ここにレセコンが入ります。医療機関と薬局で構図は違いますが、下の方の黒い四角にレセコンが繋がっているので、これをレセコンと読み替えてください。上の方の黒い四角が外に出ていくネットワークのルーターで、これが IP-VPN か IPSec で繋がるルーターになっているので、ここから先が暗号化されたネットワークになっていくという仕組みになっています。この図には書いていませんが、図にある「実施機関」は支払基金で、支払基金にレセプト請求を受けるシステムがあります。医療機関のレセコンから出て、支払基金のレセプト請求を受けるシステムに入っていくというのが１つで、これがオンライン請求ネットワークです。
今回そこにマイナンバーカードでの資格確認や電子カルテも含めて、上の方の黒い四角のルーターを応用して使った上で、繋ぐ先をオンライン資格確認システム、電子カルテ情報共有サービス、電子処方箋管理サービスと拡張しています。オンライン請求ネットワークは実は途中から分かれていきます。しかもオンライン請求ネットワークは IPv4 ですが、オンライン資格確認は IPv6 で流れています。ネットワーク的には少し違いますが、線としてはそういう風になっています。この支払基金に繋がっていくネットワークをオン資ネットワークと全体的に言っています。そういう意味では完全に閉じたネットワークとして動い

ているものが、オン資ネットワークというものです。
　そういうことを前提にして、５ページの上のリモート署名を電子処方箋と紹介状で使うことに対して、私はその方向でいいと思います。その他のネットワークについては、想定として地域医療連携ネットワークはわかるのですが、他には医療 DX の全体の世界の中で、今後オン資ネットの横の方に介護情報連携基盤、PMH（Public Medical Hub）等、要は介護と自治体に繋がっていく仕組みも全部入ってきます。介護に関しては、先ほどのオン資ネットワークではなく、インターネット上に TLS1.3 で接続をするということで話が進んでいるはずなので、セキュリティが保たれたインターネットの基盤が後ろで繋がっていく。そうなった時に、その他というのにもグラデーションがあるので、そのグラデーションで分けて考えていただいた方がいいのではないでしょうか。
○松本座長　分かりました。すでに山内さんがおっしゃったような話にも関連するというところで、事務局は了解されているかと思いますので、よろしいでしょうか。
○矢野構成員　もう１つよろしいですか。HPKI のターゲットとしてそちらに行くのは、介護の主治医意見書と死亡診断書（法令で定められて医師の署名捺印が必要なもの）です。受取先は基本自治体になりますので、全てが医療機関や薬局で閉じているネットワークではなくて、サードパーティーとして自治体が出てくるというところで、その構成も考えた上で、下の方の「その他」というのはどう考えるかというのはあった方がいいのではないかと思います。
○佐々木情報推進官　ありがとうございます。ご意見承りました。目先の話としましては、死亡診断書が動いている最中でございますので、そこもまだ PMH（Public Medical Hub）がどういう繋がりをするかというのが、我々のところまで正確なところも落ちてきていない状況でございますので、そちらが来ましたら、この専門家会議の中でも少し揉んで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した。山本先生、ご質問やコメントはございますでしょうか。
○山本構成員　ありがとうございます。皆さんのご意見はそれぞれごもっともだと思うのですが、現に今許可していただいている電子処方箋のリモート署名もそうなのですが、ユーザー認証というのはアプリケーションに依存しているわけではありません。これはリモート証明システムの中でユーザー認証を独自にやっております。これは HPKI の認証サービスを使うか、公的個人認証サービスの個人確認サービスを使うか、あるいはどうしてもやっていきたい場合にはファイル認証を行うというレベルで、利用者認証はそこでやっているので、「アプリケーションによって利用者認証のレベルが違う」というのは少し違うと思います。その辺を少しご理解いただいてご議論いただければと思います。
○松本座長　コメントありがとうございました。
○佐古構成員　今のところで非常に純粋な疑問で、本人確認のためにマイナンバーカードや HPKI カードを使うのであれば、リモート署名する理由がよくわからなかったのですが。

○松本座長　これについて、どなたか答えていただけますか。
○山本構成員　リモート署名をする理由ですか。
○佐古構成員　そうです。
○山本構成員　例えばマイナンバーカード使うときに、マイナンバーカードを使って署名しているわけではなく、本人確認をしているだけです。署名は HPKI のセカンドだけを使って署名をしています。マイナンバーカードで署名してしまうと、ご本人の現住所が入ってきますので、とても医療では使えない署名になりますので HPKI を使っています。HPKI を使う時も HPKI の署名を使っているわけではなく、HPKI カードの中には署名用の署名と認証用の証明書が入っていますから、認証を使っているだけです。
○佐古構成員　そこでなぜ署名を使わずに、あえてリモート署名にするのかというところが。
○山本構成員　署名を使っていただいてもいいのですが、署名を使うとその度に署名用の PIN を打たないといけないということになりますから、かなりご本人としては負担だと思いますので、確実に認証できればトークンを発行しますので、そのトークンで署名していただけるので、随分と工数的には楽になると思います。
○佐古構成員　そもそもリモート署名を導入する理由は、PIN を認証用のものは打てるけれども、署名用のものは長くて受け付けたくないからですか。
○山本構成員　そういうわけではなくて、そもそもリモート署名を投入する理由は、カードがなかったからです。要するに IC チップ不足でカードがなくて、カードに入った署名を発行することが、このままスムーズに電子処方箋が普及すると間に合わないので、リモート署名ができないと電子処方箋の普及を阻害することになるということで、リモート署名サービスを始めたわけです。使っていただくと、多分リモート署名の方が便利なので、そちらを使う人が増えるとは思いますが、動機としてはそういうことです。
○佐古構成員　そうすると HPKI カードが発行されていない人にとっては、マイナンバーカードで認証してリモート署名するということでしょうか。
○山本構成員　そうです。今 HPKI の申請はマイナーポータルからできるようになっていますので、マイナーポータルから申請いただけると、HPKI と公的個人認証サービスの方に個人サービスのリンク付けを自動的にできるようにデジタル庁で対応いただいていますので、それを使って証明ができるようになる。ただ、署名はあくまでも HPKI の署名用の証明書を使って署名をするということになります。
○佐古構成員　リモート署名の必要性が今やっと理解できました。ありがとうございます。
○松本座長　その他にございますでしょうか。よろしいでしょうか。それでは、今日の整理として、先ほど矢野さんからオン資ネットの定義を口頭で説明していただいたのですが、それをきちんと資料として理解可能なようにするということと、それから先ほど山本さんからもご指摘がありましたし、他の方々からもご指摘いただいているのですが、電子処方箋システムで認めていたからといって、オン資ネットに繋がっているものであれば自動的

に同じ基準でよいのかというところがありまして、これはオン資ネットと言っているものの規定だけでよいのかどうか。オン資ネットに繋げてよいかどうかの基準というか規定というのはあるのでしょうか。
○矢野構成員　基本的にはあります。マイナンバー保険証の端末を置く時に、セキュリティ監査というかセキュリティ基準がありますので、そこが基本的には医療機関に課せられているセキュリティ基準です。
○松本座長　その辺も含めてオン資ネットとは何かというところをきちっと明確にして、その中で、電子処方箋システムでリモート署名の基準を決めたわけですが、リモート署名サービスという観点では同等に扱ってよいものについては認めましょうという結論が導けるように、きちんと整備をして問題が起こらないようにしましょうということであろうかと思いますが、よろしいでしょうか。はい、ありがとうございました。
それでは３つある議題のうちの１つ目が終わりました。続いて、サブ CA 鍵更新の件です。お願いいたします。

（２）サブ CA 鍵更新の日程について
○佐々木情報推進官　それでは事務局より２つ目の議題についてご説明させていただきます。資料の方は資料１の８ページ目になります。まず今年度進めさせていただいております鍵更新、これまで議論させていただいた次第ですが、まずはこの対応状況報告になります。前々回の専門家会議の中で鍵更新の方法を決めさせていただいた次第ですが、その後、日本医師会認証局と JAHIS と実施機関のそれぞれ合わせて、厚生労働省も一緒にベンダ向けの説明会をさせていただいております。この中で各ベンダに対して、厚生労働省がフォローアップをしている状況でございますが、現時点で対応が間に合わないというような報告はいただいておりません。問題なく切り替えが実施される見通しとなっております。
本日はまず現状報告が１点目でありますが、もう１点は、前回までは日本医師会認証局の方のサブ CA 鍵更新の話でしたが、実は MEDIS 認証局の方のサブ CA 鍵更新も更新期限が来年（令和７年）の４月 19 日となっておりまして、こちらも迫ってきているという状況でございます。こちらに関しましても同じ方法で鍵更新を実施するということで予定をしておりまして、日付としましても２月 14 日にキーセレモニーを予定している次第でございます。こちらに関しましても、前回専門家会議の中でキーセレモニーの立会人を出していただくという形で決定しておりますので、改めて MEDIS 認証局の方のキーセレモニーに関しましても、立会人をお願いできればと思っております。毎度のことになってしまい申し訳ございませんが、今回も丸山先生と六川先生にぜひお願いさせていただければというところでご審議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。
○松本座長　ご説明ありがとうございました。これについてご質問等ございますでしょうか。オンラインの方でもご質問は特にないと判断いたしましたので、丸山先生と六川先生よろしくお願いいたします。

では、３番目の議題「各種ドキュメント改訂に向けた議論」です。ご説明お願いいたします。

（３）各種ドキュメント改定に向けた議論

〇佐々木情報推進官

それでは、事務局から議題３について説明をさせていただきます。資料１の 10 ページ目をお願いいたします。まず本日議論させていただきたい内容としましては、ドキュメントの改定をどのように行っていくかというところと、HPKI 専門家会議で HPKI 認証局をどのような形で進めていけばいいかというマイルストーンを次のページでお示しをさせていただこうと思っておりますので、そこに関してご意見やご議論をいただければと思っております。

まず、ドキュメント改訂に向けた方針なのですが、これまで専門家会議の中でも、議題以外の様々な部分について、例えば「このポリシーの部分は少し疑問がありますよ」といったご意見をいただいていたと思います。合わせてこの 7 月にも各種ドキュメントをご確認いただいて、気になる点があれば教えてくださいということでお願いをさせていただき、ご意見を聴取させていただいた次第です。そのような内容を今表示はしておりませんが、資料２の方でお配りしているものの中に、いただいたご意見やその内容につきまして抜粋したものを入れておりますので、適宜ご確認いただければと思っております。ドキュメント改定の大きい方針としまして、2030 年に暗号の移行を予定しております。こちらに合わせてマイルストーンを引かせていただき、その中でドキュメントの改定の準備や、議論も順々にしていければと考えている次第です。

次の 11 ページになります。こちらの方に具体的なマイルストーンを記載させていただいている次第です。まずは今年度論点整理から入りまして、来年度早々には次期暗号の方式を早めに決定させていただければと考えております。そこからルート認証局ですとか、IA の統合などという話も少し上がってきている状況でございますので、HPKI をどのように事業運営していけば良いのか、継続運用をしていくためにどういったところでやっていけばいいのかというシステム構成も含めて、議論を継続してさせていただければと思っております。最終的には調査やドキュメントアップデートの作業を行っていく中で、2030 年に向けて次期暗号が始まる段階で、認証局システムにつきましては、マイグレーションを行う予定で考えております。このような方針で進めるにあたって、本日から要点整理の議論を進めさせていただきつつ、先ほども少しお話ししました資料２に入れております今までのご議論の中で出てきた点につきましても、今回ご議論をいただければと思っております。今回資料２に入れさせていただいている項目に関しましては、将来的にドキュメントへの反映が必要だろうというところで認識をしておりますので、そういったことも想定をして、本日はご議論をいただければと思っております。まずはこのマイルストーンと、HPKI 専門家会議としての進め方、資料２に記載をしております各種いただいたご意見につきまし

て、本日はご議論いただければと思います。事務局からの説明は以上となります。松本座長よろしくお願いします。
○松本座長　それではただいまご説明いただいたことにつきまして、ご質問等ございませんでしょうか。佐古さんどうぞ。
○佐古構成員　資料1の 11 ページのリモート署名評価基準というところで、「新基準の要件整理」とありますが、新基準というのは現在のものよりも拡大するというものを新基準と言われているという認識でよろしいでしょうか。
○佐々木情報推進官　その通りでございます。
○佐古構成員　先ほど濱口委員からもきちんとリスクベースで考えていこうという話があったかと思いますが、現基準に関してはどういう見直しが起こり得るでしょうか。
○佐々木情報推進官　現基準に関しても、先ほどのお話の中で「同様に見直した方が良いのではないか」というご意見をいただきましたので、この新基準の要件整理に合わせまして、セットで現基準の見直しもさせてもらおうと思います。時間軸としては同じような時間軸で想定をしていきたいと思っております。
○佐古構成員　ありがとうございます。
○松本座長　他にございますでしょうか。宮内さんどうぞ。
○宮内構成員　今のご意見と少し関係があるのですが、リモート署名評価基準の中で、前々回ぐらいに私が申し上げたと思うのですが、鍵分割の方法をきちんとその基準の中で評価できるようにするということが非常に大きな課題としてあると思うのですが、それと今ここで言っている新基準とその他の検討についてはどうなっているのか、この辺を少し教えていただきたいと思います。お願いします。
○松本座長　では佐々木さんお願いします。
○佐々木情報推進官　宮内先生からのご指摘の点につきましては、散々この専門家会議の中でもご指摘いただいている内容でございます。ただ、一旦旧基準と言いますか、現行の基準で、電子処方箋で認めていただいている分散につきましては、このままという形で進めさせていただければと思いますが、改めて新基準を作成するときにあたっては、分散の部分も含めましてご議論いただきまして、リモート署名のアプリケーションであったり、サービスありきではなくて、どういったものであれば世間一般として使っていけるものなのか、保険医療福祉分野として使っていけるものなのかという形でご議論いただければと考えている次第でございます。
○宮内構成員　正直よくわからなかったのですが、つまり鍵分散方式はどういう風になるのですか。どういう風に扱われるということを言っているのですか。
○佐々木情報推進官　鍵分散方式に関しましては、少なくとも現基準ではお認めいただいておりますので、一旦電子処方箋であったり、この後想定しております電子カルテ情報共有サービスに関しましては、基本的にはそのままご使用いただくという形で想定をしていて、そこから先の新基準に関しましては、またゼロベースで議論をして進めさせていただ

ければと思っております。
○宮内構成員　認めたというのは微妙なところなのですが、つまり現基準をそのままにして、新基準の中でどうするかを考えるということですね。
○佐々木情報推進官　ご認識の通りでございます。
○宮内構成員　分かりました。この中できちんと鍵分散が普通に認められるようにしないと困ってしまうと思います。今回認められたというのも、動かないと困りますので、かなりいろいろなところで無理をして認めたという面が非常に強いので、そういうことが今後ないように、きちんとこの新基準というのを作成していかなくてはならないという風に考えます。
○松本座長　貴重なご意見だと思います。現行のものも研究レベルと言いますか、他のシステムでも、攻撃者側が有利な条件でもセキュアだと示せる方式があるわけです。それを今回は使ってはいないというのは私の見方なのですが、それでも様々な工夫によってセキュアだという風に考えてよろしいでしょうということにしているわけなので、「かなり苦労をして認めた」とおっしゃったのはそういう意味であるという風に私も思います。ありがとうございました。
○松本座長　それでは喜多さんどうぞ。
○喜多構成員　次期暗号方式の議論というのはすごく時間的に短いように思うのですが。楕円関数とか、この間の松本先生のシンポジウムでお話が出た耐量子暗号など、そういう検討も含まれているのでしょうか。その辺は先生のご意見もあるとは思いますが。
○松本座長　次期暗号というのは、どういうものを念頭に置かれているのかご説明いただけますか。
○佐々木情報推進官　我々としましては、松本先生は専門家ですのでお願いしたい部分ではございますが、政府として HPKI という分野に限らず暗号方式に関しましては、やはりより大きく使われております GPKI や JPKI がございますので、そちらの方の次期暗号を HPKI でもある程度踏襲をしなければいけないのではないかという想定ではおります。まずは一旦それらの情報を得ながら、この会の中で揉んでいただければと思っております。
○松本座長　まず、耐量子計算機暗号でないものを「固定暗号（クラシカル）」と言っているのですが、そちらの範囲で多分考えるということだと思います。PQC（Post-Quantum Cryptography）の方は耐量子計算機暗号という風に日本では言うことになっているのですが、そちらの方に移ってしまった方が良いのではないかという意見もありますが、まだ不安定なところもあり、十分そういう履行の準備はできていないということかと思います。これからやっていかなくてはいけない話だと思いますので、今この線表に載せられるのはこのくらいのことなのだろうなという風な感想を持っておりますが、そういうことでもよろしいでしょうか。いずれにしろ保健医療福祉分野だけが何か突出してということは多分できないと思われるので、先ほどの GPKI などを睨みつつ進めていくということになるのでしょう。

他にご意見ご質問ございませんでしょうか。山内さんどうぞ。
○山内構成員　質問ではなく、状況のご説明も含めて共有したいことがあります。JIPDEC は電子署名および認証業務に関する法律の特定指定調査機関として、民間の認証事業者が行う特定認証業務を、デジタル庁および法務省が認定するときの指定調査機関の仕事をしています。これは民間の認証局なので全て手数料をいただいて、JIPDEC の調査員が現地に行き実地調査を行いまして、基準に適合しているかということをデジタル庁と法務省に報告した上で、認定が毎年更新されます。実はこの暗号移行についても、今から検討しなくてはいけないということになっていて、民間の認定を受けている認定認証事業者も新しい認証局を立てるのか、今の鍵更新だけで済ませるかという議論も始まっているところです。その時に我々JIPDEC の方としては、暗号移行時の実地調査について、業務量が 2 倍ぐらいになるかもしれないというころで、今から調査員をどのように教育していくのかということで、場合によっては人を増やさなくてはいけないというぐらい追い込まれている状況にあります。これは JIPDEC 側の話です。もし JIPDEC が対応できなければ、JIPDEC 自身も更新をやめてしまうかもしれない。そうすると実地調査がなくなってしまうので、電子署名法自体が終わってしまうわけです。それはなかなかできないので、JIPDEC としてはできるだけ指定調査機関の仕事は継続していかなくてはいけないと思っているのですが、何を言っているかというと、暗号移行に伴う新局立ち上げや鍵更新など、いずれにしてもそれが新しい暗号方式に基づいて行われるのが 3 ～ 4 年後に起きてくることを考えたら、今から準備をしておかないと間に合わないということで、これはデジタル庁と私どもでも共有しながら、事業者の方々とも相談しているという状況です。私が少し気になっているのは、この HPKI の専門家会議で議論されているのは、ドキュメントの改訂のところが中心になっていて、新局立ち上げなり、鍵更新という時に、様々な周りのシステムの改変とかも必要になってきて、それをどのようにドキュメントに対応した適合性評価をするかというところの議論があまりされないようなアジェンダに見えている。もちろんドキュメントをきちんと作っていくというのは、HPKI 専門家会議の一番の仕事だと思いますが、それに対応していつ頃のタイミングに誰が実際に実地に行って、ドキュメントで決められた基準に適合しているかということを審査していくのかというところの議論も合わせてやっていかないと、私ども JIPDEC は今日は専門作業班の一員として来ているだけで、それ以上の責任もなく、うちが実地調査をするわけではないので、それに対して何か言う立場ではないのですが、少なくとも電子署名法においては、民間に認定されている認定認証事業者の方々からすれば、審査を受けるための準備とか、それにかかるコストも掛かりますし、JIPDEC 側の人をきちんと教育して、暗号移行に関する知識を得るとともに、どのように実地調査をさせるかというところも人の手当てをしなくてはいけない。そういったところの議論も含めて、HPKI の制度について、この機会にいろいろ検討されるのもいかがかなと思いまして、状況説明に加えまして、 1 つの考え方をお示ししました。
○松本座長　ありがとうございます。この HPKI 認証局専門家会議というものがあるわけ

ですが、それ以外に厚生労働省としては、保健医療福祉分野における PKI を含むセキュリティや各種サービスについて、今回の場合ですとリモート署名をどうするかという話であるとか、その適用範囲を広げるといった話、さらには鍵を更新していくとか、暗号方式を変えていくというような問題についてどう扱っていくのかというのを、どういう体制で審議して進めていくのかというあたりについて、全体像がちょっとわからないということですよね。

○山内構成員　全体像ということに加えて私が申し上げましたのは、実際にその文書を作ってもそれに適合していることを審査するなり評価する人たちをどのようにしていくのかということが見えない。もしきちんとした実地調査なり審査をするとなると、予算もつけて、その人たちに審査費用を払わなくてはいけないわけです。そういったところの議論がされているかどうかもわからない。

○松本座長　そのあたりは厚生労働省に聞かないとわからないですがいかがでしょうか。

○佐々木情報推進官　現在、準拠性審査は丸山先生と六川先生にお願いしておりますが、今のドキュメントの整備も含めていろいろ足りない部分があるとは思っております。現在、基本的には支援事業者も入っておらず、厚生労働省の事務官のみで対応している状況でございますので、できれば来年以降に関しましては、ある程度そういった支援も含めまして、先ほど調査事業もしたいというようなことをお話しさせていただいた次第ですが、その中で監査に関しましても、我々もいろいろ勉強している最中ではございますが、どのような監査の形がいいのか、そもそも監査の手順等もやはり厚生労働省の方から明確に出すべきではないかという風には考えておりますので、まだ調査段階ではございますが、追々やっていけたらなと思っております。もちろん 2030 年のシステム更新に関しましては、大きいことになると思っておりますので、その中で順を追って対応していければという風に考えます。

○山内構成員　どうもありがとうございました。個々の省庁ごとや法律ごとに別々に基準ができて、評価制度があるというところを統一していくことがデジタルトラストということで、別のところでも議論しているのですが、できるだけベストプラクティスを共有することなどを通じて、効率的な基準作りや評価体制ができればいいと思います。できることがありましたら、私どもも協力させていただきます。

○松本座長　ありがとうございました。その他ございますか。矢野さんどうぞ。

○矢野構成員　山内さんとほぼ同じようなことになるのですが、議論を急いでいただきたいと思っています。現場運用的に言うと、まず暗号方式が決まります。そうすると認証局を作ります。IC カード使っているので、IC カードの方式、チップの仕様を決めなくてはいけない。ドライバーを作らなくてはけないです。これを使っている電子処方箋や、現場のアプリケーション側にも技術提供をしていかなくてはいけないですという風になっていきますので、正直 2030 年の暗号移行というのはどれほど縛られているものかわからないのですが、今から動かないと間に合わないぐらいの勢いでいます。ぜひ議論を加速いただけれ

ば大変ありがたいと思います。よろしくお願いします。
○松本座長　今貴重なご意見をいただきましたので、これを踏まえて進めていただければと思います。では、以上で３つの大きな議題は終了ということになります。続きまして連絡事項などございましたらお願いいたします。
○佐々木情報推進官　最後に連絡事項でございます。次回の第 30 回 HPKI 専門家会議ですが、今のところは来年１～２月頃の開催を予定しております。こちらは日本医師会認証局の鍵更新を 12 月もしくは１月頭を予定しておりますので、最終的にそこの結果も踏まえまして、この会の中でご報告を差し上げようと思っておりました。また本日の議論を受けまして、やはり先ほどの暗号化移行の話も加速をした方が良いというところでございますので、この１～２月の前にもう１回挟むのかどうかも含めて、事務局の方で検討させていただき、追って次回の会議の日程に関しましては、ご連絡をさせていただければと思います。連絡事項は以上となります。
○松本座長　ありがとうございました。それではよろしいでしょうか。では、本日はこれで閉会ということにさせていただきます。今日も活発なご議論ありがとうございました。

以上