第３５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８年３月２日(月) １０：００～１２：２５

場所 AP 虎ノ門　B ルーム

開会

○岡嶋主査　皆様、おはようございます。ただいまより「第35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ています。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に、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ご連絡です。本日の会議の構成員の参加状況について、菊池構成員と佐古構成員がご欠席、柴田構成員、濱口構成員、松本座長がオンラインでの参加、山本オブザーバーがオンライン参加となっております。その他の構成員とオブザーバーは現地参加となります。

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、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、ダブルクリップで留めている資料で、議事次第、資料１、資料２－１、資料２－２、資料３－１、資料３－２、資料３－３、資料４、開催要綱、そして前回第34回のHPKI専門家会議の議事録を添付し配布しています。なお、資料１の附属書類となる参考資料１－１から１－８については、分量の関係上、紙での配布は行わず、事前に共有しているSharePoint領域にてご確認いただければと思います。資料の過不足等がありましたら、事務局までご連絡ください。

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、私はオンラインで参加させていただきます。よろしくお願いします。今日の議題は、「各種ドキュメント改定について」、「次期認証局の構成について」、「HPKI 暗号アルゴリズムの移行について」、「認証局準拠性審査実施（ルート・日本医師会・日本薬剤師会）について」の議論となります。

議事

（１）各種ドキュメント改定について

○松本座長　まず議題１について、事務局から説明をお願いします。

○河内主査　厚生労働省事務局です。資料１「各種ドキュメント改定について」をご確認ください。厚生労働省及びHPKI専門家会議で管理しているHPKIの各種ドキュメントの改定を現在計画しています。

１頁をご覧ください。まず改定実施の背景をご説明します。事務局においてHPKIポリシ関連書類を点検した結果、記載の不整合や、現在の運用・技術に即していない箇所が確認されました。また、リモート署名サービス評価基準の準拠性監査報告書様式については、

現在採用されている分散鍵方式に十分に対応できていないという点があり、今後の監査の実効性確保の観点からも、補完が必要な状況と認識しています。あわせて暗号移行関連事項についても、次期暗号アルゴリズム移行を見据え、修正項目を整理しておきたいと考えています。こうした状況を踏まえドキュメント改定を実施したいと考えています。

改定に向けては、今回の第 35 回から第 37 回の HPKI 専門家会議にかけて、段階的に議論と承認審議をお願いしたいと考えています。まず本日、第 35 回では、リモート署名サービス以外のドキュメント改定に向けて、事務局から示した論点を中心にご議論いただきたいと考えています。次回の第 36 回では、本日ご議論いただいた内容を反映したドキュメント改定案の承認審議を行い、加えてリモート署名サービス評価基準の見直しについて議論を行う予定です。第 37 回では、リモート署名サービス評価基準の改定案について承認審議をお願いしたいと考えています。

続いて 2 頁で、各種ドキュメント改定に向けた議論の進め方についてご説明します。厚生労働省が管理する HPKI ポリシ関連書類は、「厚生労働省 HPKI ルート認証局運用管理規程（ CP / CPS ）」「HPKI 認証局署名用証明書ポリシ」「HPKI 認証局認証用（人）証明書ポリシ」「HPKI 認証局認証用（組織）証明書ポリシ」の主として 4 つのドキュメントから構成されています。HPKI における最上位の規程はルート認証局運用管理規程（ CP / CPS ）となりますが、本日は共通の論点を多く含む署名用証明書ポリシの記載をもとに議論していただきたいと考えています。本日の整理結果は他の関連文書にも反映し、次回改めてご確認とご承認をお願いする予定です。事務局で今回のドキュメント改定を進めるにあたって、 3 つの作業を行っています。 1 点目に、改定対象の整理と改定作業の実施です。技術動向・技術仕様の更新により陳腐化している箇所や、参照先規格が更新されている事項、表記揺れや誤記を確認し、改定が必要な箇所を一覧化した上で整理を行っています。 2 点目に、次期暗号アルゴリズム移行に伴う改定箇所の整理です。今後の暗号移行を見据え、修正が必要となり得る箇所を抽出しています。 3 点目に、これまでの HPKI 専門家会議での指摘事項の反映についても、併せて行っています。

3 頁をご覧ください。先ほどお伝えした 3 点の改定作業を行っていますが、事務局で改定箇所を整理する中で、論点があると考えられる 3 点を中心に、本日はご意見をいただきたいと考えています。 1 点目が「鍵の更新期限の整合性について」、 2 点目が「暗号モジュールが準拠すべき標準の検討について」、 3 点目が「本人確認書類の見直しについて」です。それぞれ順にご説明します。

4 頁をご覧ください。まず、議論 1 「鍵の更新期限の整合性について」です。現行ポリシでは、鍵の更新時に関して、鍵更新手続きで初回申請時の提出書類を参照できる期間を、「初回発行から 5 年以内」と、署名用 CP の 3.3.1 項で規定しています。一方、エンドエンティティの公開鍵証明書の有効期間は 5 回目の誕生日まで、更新時は更新後 6 回目の誕生日まで有効であると、誕生日で期限が切れるように 6.3.2 項に規定しています。この 2 つの規程を踏まえると、 2 回目以降の更新手続きが必要となるタイミングは、 6 回目の誕生日

頃となりますが、そのタイミングでは鍵の発行から既に 5 年以上が経過しているため、初回提出書類を参照する更新手続きができないことになります。よって、その際の鍵発行の手続きを更新手続きと捉えるのか新規発行と捉えるのかが曖昧となり、証明書の有効期間をどのように設定すべきか、現状では不明確な状況となっています。

5 頁をご覧ください。署名用 CP の 3.3.1 項のとおり、発行から 5 年が過ぎると、初回提出書類を参照した更新手続きが認められず、再度の書類提出を必要とする一方で、署名用 CP の 4.7.1 項では、オンラインの手続きであれば、有効な電子証明書がある場合に、更新申請書に電子署名をすることで簡略的に更新ができる、としています。このため、更新手続きにおいて紙申請であれば鍵発行から 5 年が過ぎれば再度の書類一式の提出を求める一方、オンライン申請であれば、簡略的な手続きが許容される状況となっています。

6 頁に、論点を 2 点まとめていますが、初回提出書類等を参照した更新手続きを可能とする期間、電子署名による本人確認を可能とする更新手続きの期間、証明書の有効期間満了のタイミングを全てそろえる必要があると考えています。また、そもそも鍵更新の定義がポリシ内にないため、今回、ポリシ内で改めて定義することで、異なる解釈が生じないようにしたいと考えています。

7 頁をご覧ください。今回、初回提出書類の再参照もしくは電子署名による本人確認ができる期間と、証明書の有効期間満了のタイミングをそろえる方向で、改定案を作成しています。また、鍵更新の定義をポリシ内に追加で記載しています。議論していただきたい点として、今回の改定案では、電子証明書の有効期限前であれば、証明書が失効しない限り、初回提出書類を参照した鍵更新を可能としています。また、今回の改定案では、証明書の有効期限内であれば、回数制限なく初回提出書類を参照した更新を可能とする整理としています。その場合、初回提出書類を 5 年を超えて参照し続けることが可能となります。鍵更新に回数制限や再確認のタイミングを設けるべきか、また、その制限をポリシ内で定めるべきか、あるいは各サブ認証局の CPS で運用として定めるべきかについてご意見をいただきたいと考えています。HPKI は本人確認に加え、医師等の資格の確認が必要となりますが、医師等の資格の確認のみについては回数制限を設けず、初回提出書類を継続参照し続けられると整理する選択肢もあると考えています。このように書類別に整理を行う場合、ポリシで一律に規定すべきなのか、それとも CPS で具体化するほうが適切なのかについても、ご議論いただきたいと考えています。

9 頁をご覧ください。続いて、議論 2「暗号モジュールが準拠すべき標準の検討について」ご説明します。現在、医師等ユーザの私有鍵の格納モジュールに対して、FIPS 140-2 レベル 1 への準拠を要求していますが、レベル 1 では改ざん防止や物理的セキュリティ要件が十分ではないこと、実際の運用ではレベル 2 以上のセキュリティ強度が実装されていることを踏まえ、規定においてもレベル 2 以上へ引き上げる必要があるのではないかと考えています。また、FIPS 140-2 は令和 8 年 9 月をもって失効する予定であり、後続規格である FIPS 140-3 への移行を検討する必要があると考えています。

10 頁をご覧ください。直ちに FIPS 140-3 しか許容しないことにすると、調達コスト等への影響が懸念されることから、今回の改定においては「FIPS 140-2 または FIPS 140-3 への準拠」として併記することはどうかと考えています。以上より、医師等ユーザの私有鍵格納モジュールのレベル 2 以上への引き上げの妥当性、また FIPS 140-2 と FIPS 140-3 の併記について、ご意見をいただきたいと考えています。

11 頁をご覧ください。議論 3「本人確認書類の見直しについて」です。現行のポリシでは、既に廃止されている本人確認書類が記載されている状況であることから、今回、「電子署名及び認証業務に関する法律（電子署名法）」施行規則第 5 条を参考に、本人確認書類の見直しを行いました。電子署名法を参考にした追加、削除の妥当性について、ご議論いただきたいと考えています。

事務局からご提示する議論 3 点は以上となります。こちらについてご意見いただきたく、座長にお戻しします。

○松本座長　ご説明ありがとうございました。それでは、各種ドキュメント改定について、順番にお聞きしていきたいと思います。

議論 1 ：鍵の更新期限の整合性について

○松本座長　まず、議論 1「鍵の更新期限の整合性について」です。こちらについてご意見はありますか。

○山内構成員　JIPDEC の山内です。「鍵更新」という言葉について、認証局自体の秘密鍵及び公開鍵つまり鍵ペアを変えること、あるいはエンドエンティティの鍵を変えること、その両方に読めてしまいます。加入者の初回申請時に提出した書類等を参照した鍵更新は、エンドエンティティである医療従事者の鍵ペアのことだと思います。書き方をどうするかが気になりました。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ですが、デジタル庁や法務省と議論している中で、数年以内に新しい暗号へ対応していくことも含めて、認証局自体の鍵を変えていかなければいけないという話があり、「鍵更新」というと、調査員の中では認証局の鍵の話になります。これは前後を読めば、エンドエンティティである医療従事者の電子証明書に対応している鍵ペアだと読めますが、誤解がないように、うまく表現していただければと思いました。以上、コメントです。

○松本座長　これは誤解されないよう、認証局の鍵の更新ではないことについて明記といいますか、一言どこかに書いておけば十分だと、山内構成員はお考えですか。

○山内構成員　注記でも十分かと思いますが、実地調査や監査をする方々の立場によって言葉の解釈が異なるので、誤解がないようにさえしていただければよいという意味です。

○松本座長　事務局、この件に関してはいかがですか。

○河内主査　今回は署名用証明書ポリシを代表例として記載していますが、各種資料に反映させる時に誤解を生まないように明記したいと考えています。

○松本座長　他にご意見はありますか。

○林構成員　まず、大前提のところで恐縮です。これはコメントですが、常に暗号アルゴリズムは危殆化する可能性があるという前提を忘れないようにしていただきたいと思います。今回は暗号移行もあるため計画的にできますが、計画的にできないことがある旨をシステムに織り込んでいただきたいのです。再三再四お伝えしていることですが、危殆化した場合早急に対応しなければいけない項目であり、今回のように計画的にできないこともあることは常に意識しながら、全体を進めていただければと思います。

個別の議論について、まず5年というタームが果たして適切なのか、懸念があります。特に昨今、一般に分かりやすい用語で「KYC」と呼ばれるもの、これは署名者の本人確認書類を5年間のうちであれば使い回してよいことを指しています。5年を繰り返すと10年でも20年でも、20歳の時の本人確認書類を50歳まで使い回すことができます。そのようなもので本人確認ができるということは、おそらくないと考えられるので、本当に5年でよいのか、ポリシでしっかり考えていただく必要があると思います。

もう一つは、事実上それしか選択肢がないことは分かっているので、どこかに明記していただければと思いますが、FIPSを採用している理由です。これは米国の基準であり、我が国の基準でもなく、国際標準でもありません。それを採用している理由については、どこかできちんと書いておかないと、疑義が出てくるのではないかと思いました。

○松本座長　FIPSに関する内容は、議論2でお願いできればと思います。

今のセッションでは、議論1、2、3があり、議論1が「鍵の更新期限の整合性について」で、議論2がFIPSに関する話です。

○林構成員　失礼しました。最後に、鍵更新の期間について、今後多くの方々が、いわゆる電子証明書と呼ばれるものを更新する数が、増えていくと思います。合わせる合わせないの議論はあると思いますが、更新期限があまりにも異なっていると、非常にやりにくいと思います。誕生日という基準が適正なのかに関しても、疑問があります。他の証明書について、マイナンバーカードも含め、更新するタイミングを整合させるという、一般常識的なところになるべく落ち着かせるのが適正ではないかと思います。以上です。

○松本座長　林構成員、ご発言の1点目は「暗号アルゴリズムが更新され、危殆化して対応しなければならないこともある」ということで、これは今の議論と関係ないと思いますが、いかがですか。

○林構成員　議論1には関係ありませんが、本日の議論全体のコメントをするタイミングということで、コメントさせていただきました。また、2番目のFIPSの件は、議論2で扱うと伺ったので、そこに持ち越していただければと思います。

○松本座長　具体的に論点を絞られていることをお認めいただくとすると、7頁に「CP記載修正案」がありますが、ここではどのようなご主張でしょうか。

○林構成員　本人確認に対する更新期間の長さと、その取扱の適正性の条件が一つです。もう一つは、その条件面、どこを閾値にするかということが他の一般的な電子証明書に関する手続きと合致しているか、この2点です。

○松本座長　有効期限をどう定めるかについては、「CP 記載修正案」には記載がないので、修正案の範囲を超えたご指摘になると思いますが、それでよろしいでしょうか。
○林構成員　議論 1 の参考として 8 頁に期限が記載されているものの、今回の 7 頁「CP 記載修正案」の「現状の記載内容」では「5 年以内」という記述があり、「記載修正案」ではその記述が消えているので、おそらく期限の記載がどこかに追い出されているのだと思います。ですから、追い出した先できちんと手当てしていただく必要があると思いました。
○松本座長　事務局にお聞きしたいのですが、その点はいかがですか。
○河内主査　厚生労働省事務局です。改定前では、提出済書類を利用した鍵更新ができる期間を鍵が発行されてから 5 年以内と限定していたところ、修正案では、証明書の有効期限前であれば更新手続きができると記載を変更しています。ですから今回は 5 年というリミットを削除している形になります。林構成員のご指摘としては、5 年という期間は残すべきではないか、という認識で合っていますでしょうか。
○林構成員　まず、5 年が適切なのかを議論する必要があると思っています。
○松本座長　有効期限はどこに書いてあるのでしょうか。赤字で示された修正案でも「有効期限前」や「有効期限を過ぎた」と記載があります。有効期限がどのように定まるのかについては、CP の中でどこに書かれていますか。
○河内主査　6.3.2 項に鍵証明書の有効期間の記載があり、加入者の 5 回目の誕生日、更新時は 6 回目の誕生日と規定しています。今回その点については改定する予定がないことから、7 頁の「CP 記載修正案」には記載していません。
○松本座長　それを踏まえて、林構成員、もう一度ご意見をいただけますか。
○林構成員　ですから、当然、参照先の内容を踏まえて、この部分の記述を行うべきだと思います。
○松本座長　そうなっているという認識ではないかと思います。
○林構成員　それは、参照先について別途この後議論できるという意味で捉えてよいですか。
○松本座長　違います。本日の準備としては、そこは変えない前提で議論しましょう、ということになっています。有効期間自体を変える議論もしたらどうか、というご意見ですか。
○林構成員　はい。するべきだと思っています。
○松本座長　その緊急性は、どの程度あるとお考えですか。
○林構成員　個人的には、今回の議論で改定する必要はないと思いますが、定期的にポリシが更新できるのかというところと併せて考える必要があると思っています。例えば 10 年や 20 年このままというわけにはいかないと思うので、今回の改定に入れないのであれば、次回の改定時期とセットになるかと思います。
○松本座長　HPKI に関して、中長期的にどのような課題があり、それをどのタイミング

で変えていくかという中に、今のお話も入れて議論を進めていければと思いますが、そういう形でもよろしいでしょうか。本日は、赤字で記載された修正案でよいかどうか、あるいは、修正するとしたらどのように修正するかに論点を絞って話をしたいと思います。ご指摘のように有効期間、有効期限について、そもそもどのようにするのが合理的か、医療PKI は他の PKI とも関係しているので、検討していくべきだというご意見だと伺いました。

本日はいただいたご意見は棚上げしますが、ご指摘いただいた内容は中期的計画の中に入れて議論しましょうということです。林構成員、その形でよろしいですか。

○林構成員　かしこまりました。

○松本座長　他に議論１に関してご意見はありますか。

○矢野オブザーバー　日本医師会の矢野です。棚上げされ件について、補足です。HPKIの有効期限は５回目の誕生日、更新にあたっては６回目の誕生日とするのは、JPKI、要は「行政手続における特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）」に合わせてあります。現在、証明書の有効期限を短くする傾向があると思いますが、有効期限についてはマイナンバー法と平仄を合わせて議論すればよい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。

○宮内構成員　宮内です。内容について特に反対はありませんが、７頁の２つ目、3.3.1 項に「証明書の有効期限前であれば」と記載があります。これだと、新しく発行された２回目の証明書の有効期限前でも、ここに含まれるように見えなくもないと思います。要するに、以前は記載されていた「初回の」の文言が消えているのです。１回更新したら、既存書類・記録の再参照又は電子署名による鍵更新は、そこから６年しかできないのであり、そこで新たに証明書を発行したら、また６年の再参照可能な期間が始まるという意味ではないことを表現する必要があります。つまり、初回のものに限るという趣旨の文言に整理して書いていただきたいと思います。私からは以上です。

○松本座長　今の点については、ご指摘のとおりではないかと思いますが、事務局、いかがですか。つまり、3.3.1 項の１行目の赤字の下線が引いてある「証明書の有効期限前」の前に「初回の」と３文字を入れるということですが、いかがですか。

○河内主査　ご指摘のとおり、今の修正案では、証明書の有効期間前であれば、同じ書類を参照し続けられるような記載ぶりになっていることは、事務局としても認識しています。回数制限について、このポリシ内で設けるべきなのか、それとも、サブ認証局側の運用規程で設けるべきなのかについては、皆様にご議論していただきたいと考えています。

○宮内構成員　宮内です。今おっしゃっていることは、ごもっともだと思います。まず事実として行いたいのは、１回目の発行時に身元確認を行い、それは２回目に発行する時も有効であり、３回目の時にはもう一回身元確認をしなければいけないが、それはきっと４回目までは有効なのだと理解しています。初回とは何かというと、きちんと身元確認を行った発行から６年程度はよいと言っているので、１回目に行えば２回目は身元確認がなく

てもよく、３回目に行えば４回目はなくてもよいと、おそらくそういう趣旨だと思います。それが分かるように書いてもらいたいというのが、まず１点です。

それから、サブ認証局の CP / CPS で決めるか否かというのは、両方あり得ると思いますが、大原則としては、「これ以下にしなさい」と規程で決めて、その範囲内で CP / CPS で決める形がよいと思います。ただ、記載として 100 か所も 200 か所もあるならともかく、数か所しかないのであれば、一つにまとめて書いてもよいのではないかというのが、私の意見です。よろしくお願いします。

○松本座長　今のご意見は要するに、ポリシに記載すべき記述のレベルについてで、それについてはいかがですか。他にご異論がある方はいらっしゃいますか。山本オブザーバー、お願いします。

○山本オブザーバー　今の議論は非常に大事です。おそらく現実的に問題になるのは、資格保有者が亡くなられたときで、それを使い続けるようなことがあると困ると思います。したがって、生存確認、本人確認の書類の再参照は、やはり２回を限度にしておく必要があると思います。一方、医師免許や薬剤師免許は、医道審議会等で剥奪される例もありますが、多くて年に１人～２人程度ですから、医師の免許証のコピーに実印を押して毎回提出するのも、あまり現実的ではないと思います。したがって、本人確認、生存確認の書類に関しては、CP 上で２回を超えては使えないということを記載いただき、その他の HPKI のヘルスケアの資格確認に関しては、CPS で定めるとしていただくのが妥当ではないかと思いますが、いかがでしょうか。

○矢野オブザーバー　日本医師会の矢野です。補足をさせていただきます。宮内構成員がおっしゃったとおり、最初は「初回」と書いていませんでした。そうすると、３回目も４回目も同じ書類が使えることになってしまう、ということで「初回」という文言を入れました。初回は、最初に発行した時だと解釈すると、次の更新の５年目の時は同じ書類を使ってよく、10 年目の時に新しい書類をもらうという規定ですが、それを更新と見なすか、初回と見なすかによって、有効期限が変わります。初回と見なすと有効期限は５回目の誕生日ですが、更新と見なすと６回目の誕生日となります。５回目の誕生日、６回目の誕生日にするのは、要は有効期限を約５年にそろえていこうという趣旨で改定をしたのですが、「初回の電子証明書」と書いたために、10 年目の更新が果たして更新なのかということにより解釈が変わるので、今回、何か工夫をしていただきたいと思います。

山本オブザーバーも宮内構成員もおっしゃったとおり、10 年目の更新の時は必要な書類を集めるべきだと思いますし、その運用を行っています。ただ実際、日本医師会は２回目の更新時期が来て、「初回の電子証明書」に解釈の揺らぎがあるので、改定をする、解釈をしっかりする等、お願いしたいというご提案です。

○松本座長　具体的にはどのように直せばよいでしょうか。今の修正案でよろしいというお考えですか。それとも、より明確にするために、さらに直したほうがよいとお考えですか。

○矢野オブザーバー　このままの書き方だと 15 年後も 20 年後も同じ書類が使えると解釈できるので、明確にしたほうがよいと思います。文言の案はいまここで直ぐに出てきませんが、「初回の」という言葉ではなく何か文言を入れて、10 年目、20 年目にはもう一回書類をきちんと提出すること、という形にしたほうがよいと思います。
○松本座長　ありがとうございます。他にご意見はありますか。
○林構成員　林です。明確に本人確認をする時期を、きちんと「本人確認」と記載するのが一番ストレートだと思います。「本人確認」は、日本でも比較的厳密に定義されている用語だと思います。むしろ「更新」は定義が曖昧になるので、そちらもきちんと手当てをして記載をそろえていくほうが、分かりやすいのではないかと思いました。以上です。
○松本座長　申し訳ありません。その趣旨は分かりますが、具体的に今ここで直すことはできないということでしょうか。時間の関係もありますので、事務局で引き取って、もう一度案を出していただくという形でいかがですか。
○宮内構成員　宮内です。案の提案があるのですが、申し上げてもよいですか。
○松本座長　お願いします。
○宮内構成員　「CP 記載修正案」に赤字で記載されている「証明書の有効期限前」を、「3.2.3 個人の認証 を経て発行された証明書の有効期限前」と直せば、１回目や３回目は、3.2.3 の個人の認証を経ているから、５年目、15 年目にはそれを使えることになるかと思います。これを軸に考えていただければと思います。よろしくお願いします。
○松本座長　ご提案をありがとうございます。詳細を検討しないと見落としがありそうなので、文書ベースでもう一回整えて確認することにしたいと思いますが、事務局いかがですか。
○六川構成員　構成員の六川と申します。７頁について、実質的な内容については、先生方のご意見のとおりだと思います。
　形式面について、１点コメントです。宮内構成員も私も弁護士業界にいて、普段、民事裁判で、契約書の一字一句のどこがどう違っているということで、それを裁判官に対して強烈に攻め込んでいくということをしています。７頁「CP 記載修正案」をよくご覧いただきたいのですが、長方形の４つの欄があり、一番上の欄と２番目の欄には「有効期限」という言葉が多く出てきます。ところが３番目の欄では、今度は「有効期間」という言葉が出てきます。鍵の更新ならびに有効期間の論点では、ここが大変重要だと思いますので、「有効期限」と「有効期間」はどちらかにそろえていただきたいと思います。「有効期限前」という言葉が２番目にありますが、例えば「有効期間満了前」としたほうが、もし将来何か紛争が起こった時に、統一的な文言を提示できるのではないかと思います。
○松本座長　六川構成員にお聞きしたいのですが、「有効期間」というのは、いつからいつまでというものなのか、それとも長さを指しているのか、どちらの使い方なのでしょうか。
○六川構成員　「有効期限」は、実際その期間が終わる頃、終わるというタイミングにス

ポットライトを当てた言葉となります。ところが、4 頁の 6.3.2 項では、「証明書の有効期間」を表題の定義として使っています。「期間」は、最初から終わりまで、5 年間全部を指す言葉になります。
○松本座長　「CP 記載修正案」の赤字の部分を書いた事務局は、どのような解釈で「期間」と「期限」を使い分けていますか。
○河内主査　特段の意図はなく、こちらは「有効期間」と「有効期限」いずれかの記載に統一して表現することが可能と思いますので、記載ぶりを合わせていきたいと考えています。
○松本座長　分かりました。
○山内構成員　JIPDEC の山内です。「有効期間」は、おそらく長さを意味していると思うので、5 年ということを決める時には、「有効期間」という言葉も残さなければいけないのではありませんか。有効期間は 5 年ということで、それが長いか短いか、そもそも議論するかということが、最初に少し話題になっていたと思います。
○松本座長　「有効期間」の「期間」をタームという意味で使うのか、要するに、ある時刻から別の時刻までの間の期間を指しているのか、それとも期間の長さを指しているのかという問題があると思います。「期限」と言った場合、期間の終了時点を指すと思います。その辺りをこの文書の中で明確にするといいますか、誤解がないよう、一般的な定義をそのまま使うかというだけかと思います。また、有効期間という概念自体は、山内構成員がおっしゃるように私も必要だと思いますので、その関係がよく分かるように整えるということで、お願いしたいと思います。
　皆様、よろしいでしょうか。そのような整理の仕方で進めたいと思いますが、事務局、よろしいでしょうか。
○河内主査　かしこまりました。今いただいたご意見を中心に修正案を作成し、皆様にまた確認をお願いさせていただきます。

議論 2 ：暗号モジュールが準拠すべき標準について
○松本座長　では次の議論 2 に移りたいと思います。先ほど林構成員から、なぜ FIPS なのかという話がありました。まず、それ以外のご意見もいただいてから議論したいと思います。いかがでしょうか。
○林構成員　10 頁の 2 ポツ目「現時点では FIPS 140-3 に準拠している製品が少数であり、調達可能な製品の選択肢が狭まることによってコストや納期に影響することが懸念されるため」という記載は非常に重要な項目だと思いますが、エビデンスがないと判断に困ると思います。現在、移行が進んでいることは皆様ご存じのとおりだと思いますが、本当に記載のとおりなのか確認が必要だと思いました。以上です。
○松本座長　ありがとうございます。
○谷内田参与　参与の谷内田と申します。FIPS 140-3 は、2 ～ 3 頁程度の文書で、ISO の

文書を参照しているだけですので、実質的には同じであり、内容的には米国の標準にのっとっていると言えると思います。ただ継続性の観点から考えると、いきなりここで ISO の番号を出すよりは、米国の標準が進化したものだと提示したほうが理解しやすいのではないかという印象は持っています。以上です。
○松本座長　ISO/IEC 19790 という標準規格が今、谷内田参与がおっしゃった国際標準で、米国版のローカライズをしたものが FIPS 140-3 になります。
　一番重要な点は、米国の標準の暗号アルゴリズムが ISO/IEC 19790 には入れてあるということです。それが数頁、補足があるということですが、もう少し詳細に見るとパートが複数あり、それぞれのところで、米国ではこのように定める、あるいは modify するという内容が入っています。したがって、FIPS 140-3 のメジャーなところは基本的には国際標準の ISO/IEC19790 であると考えてよいと思います。
　ですから、FIPS 140-3 レベル 3 への準拠は、ISO/IEC 19790 のレベル 3 に基づき認証されたこと、その認証は CMVP（Cryptographic Module Validation Program）ですが、それを規定する内容です。濱口構成員から Zoom のチャットで「FIPS 140 を ISO 化したものが ISO/IEC 19790 である」とコメントがありましたが、そうではなく、ISO/IEC 19790 のほうが先にできています。ISO/IEC 19790 の作成に関わっていたので、事情はよく知っています。濱口構成員、そのような認識でよろしいでしょうか。
○濱口構成員　濱口です。ISO/IEC 19790 の初版は、2000 年代だったと記憶しており、FIPS は 1990 年代からだと思います。
○松本座長　ISO/IEC 19790 の初版はたしかに 2000 年代ですが、今は、FIPS 140-3 の話をしています。
○濱口構成員　なるほど。 FIPS 140-3 に関しては、おっしゃるとおりです。
○松本座長　FIPS 140-2 から 140-3 に移行する時に非常に時間がかかってしまいました。FIPS 140-2 から 140-3 に、通常 5 年で変えるということでしたが、その間いろいろな事情があり、なかなか FIPS 140-3 が定まりませんでした。そうこうしているうちに国際的な標準にしようという話になり、国際標準 ISO/IEC 19790 を先に作り、ローカライズしたものとして FIPS 140-3 になったという経緯です。
○濱口構成員　私も同じ認識です。FIPS 140-2 が、2001 年頃に出て、その後、ISO/IEC 19790 が出たのが 2005 年か 2006 年でしょうか。
○松本座長　おっしゃるとおりです。
○濱口構成員　その後、FIPS 140-3 が出て、また ISO/IEC 19790 が FIPS 140-3 をベースに改定されたと認識していますが、合っていますか。
○松本座長　ISO/IEC 19790 はアップデートされていますが、そのアップデートされたものに基づいて FIPS 140-3 ができました。
○濱口構成員　初版の ISO/IEC 19790 と整合を取ったのが FIPS 140-3 ということですか。
○松本座長　ですから、今、最新版は同期しています。何を申し上げたいかというと、

「ISO/IEC 19790 のレベル何々に基づき認証されている鍵格納モジュールを使いましょう」という言い方にすれば、米国標準に基づいていると言わなくてよいという解決策にはなるということです。ただし、ISO/IEC 19790 に基づく暗号モジュール試験認証制度は、我が国にも JCMVP があり、これは米国の CMVP と等価のものですが、JCMVP では扱ってよいアルゴリズムが米国のアルゴリズムと完全に一致はしていません。また、事実上、認証が開店休業状態になっており、FIPS 140 のレベル 3 あるいは 2 に基づいて、CMVP で認証された製品しか使えない状況になっているかと思います。これが現状認識です。

今日の論点は、この際、FIPS 140-2 のレベル以上の規格に準拠する、以上というのは、レベル 3 や 4 があるのですが、そういったレベル以上の規格に準拠する、という規定について、基準自体は ISO/IEC 19790 に変えても問題ないと思います。いかがでしょうか。

○山内構成員　JIPDEC の山内です。私は長い間、国際標準の仕事をしてきたので、ISO/IEC の規格をこういう文書に書き入れて、その適合をしっかり示していくべきだと個人的には思いますが、規格の話と適合性評価の話は切り分けて考えなければいけないのが実情です。といいますのは、規格があっても、松本座長がおっしゃったとおり日本国内では ISO/IEC 19790 への適合を認証するための事業が開店休業状態になっていると思います。米国やカナダで長く運用されている CMVP の制度に基づくものが、世界ではデファクト・スタンダードになっています。適合性評価の世界で議論する時には、現在、世界でデファクト・スタンダードとなっている FIPS 140-3、といった言葉のほうが分かりやすいのではないかと感じています。これはコメントです。

○松本座長　他の方からご意見をいただけるとありがたいのですが、いかがですか。きっかけをいただいた林構成員は、いかがですか。

○林構成員　林です。私も山内構成員と比較的同じ肌感です。JCMVP に関しても同じ認識です。結局 CMVP の製品を調達せざるを得ないことも、そうだと思います。我が国も ISO には貢献しているところもあります。ISO/IEC と FIPS の併記について、併記する方法は一つあり得るかとは思いますが、実態としては、おそらく FIPS になるだろうとも思っています。

先ほどコメントしたとおり、私はむしろ FIPS 140-2 を併記する話が気になっています。併記しないと調達が難しいということが 10 頁の趣旨だと思いますが、これは本当だろうかということが一番気になっています。

○松本座長　FIPS 140-2 を基準として残すかどうかということでしょうか。

○林構成員　まず、ISO の記述を入れるかというのが 1 点あると思います。もう一つは、FIPS 140-2 を残すのかということであり、これは現場の調達状態のエビデンスに合わせて記載するべきではないかと思います。以上です。

○松本座長　事務局に確認ですが、「準拠している」というのは、きちんと認証を取っている、という意味で書かれていますか。

○河内主査　はい。おっしゃるとおりです。

○松本座長　そうすると、FIPS 140-2 は近々失効するので、新たに発行されないということと、FIPS 準拠ではなくなるわけです。FIPS 140-3 はかなり前からスタートしているので、FIPS 140-2 が認証対象ではなくなっています。ですから、FIPS 140-2 に準拠するというのは、かつて米国標準に準拠していたということでしかなくなる理解ですが、そのようなものでよいかというのが、林構成員がおっしゃっていることです。ただし、FIPS 140-3 の製品が十分にアベイラブルかを気にされており、実態に合わせるべきだとおっしゃっています。そのような理解でよいですか。
○林構成員　10 頁 2 ポツ目に「準拠している製品が少数であり」とあり、それが併記の理由になっていることから、そのように考えました。以上です。
○松本座長　この記載でよいとおっしゃっているのでしょうか。
○林構成員　松本座長がおっしゃるとおり、かなり前から移行も進んでいるため、FIPS 140-3 に準拠している製品が少数であることに関して私自身は若干懐疑的であるので、本当かどうかを確認するべきではないかと思っています。
○松本座長　これも事務局にお聞きしたいのですが、少数であるというのは何か具体的な根拠はありますか。
○河内主査　こちらについては「少数」という曖昧な表現をしてしまいましたが、FIPS 140-3 しか受け入れないという、いきなりの切り替えが可能かどうかというところを懸念し、今回は併記の提案をさせていただきました。
○濱口構成員　私も林構成員と同じ意見です。本当に FIPS 140-3 の製品が少ないのか、一度調べていただきたいと思っています。移行期間がなく、いきなりという話もありますが、そもそも FIPS の認証プログラムに移行期間が設けられています。おそらく、この夏頃には全ての FIPS 140-2 の認証製品がヒストリカルリスト入りし、有効ではなくなる状況を迎えると思います。HSM の世界の中では、十分移行期間が設けられていたと認識しています。以上です。
○松本座長　私もそのように考えています。何か特殊な事情があってこのように書いているのかどうか、というところなのですが、もし FIPS 140-2 を併記するのであれば、いつまでは、ということを限定しないといけないと思います。
　ですから、まずは FIPS 140-3 のレベル 3 や 2 を先に書き、「ただし、いつまでは FIPS 140-2 のレベル 3 や 2 でよい」と整えるほうが合理的かと思います。事務局、これはいかがですか。
○岡嶋主査　事務局です。松本座長、まとめていただきありがとうございます。そのような方向が可能かどうかも含めて持ち帰り、次回の会議でご提示したいと思います。
　FIPS 140-3 に対応した製品が既に存在していることは、事務局としても当然認知しており、国際的にも既に使われている状況であると理解しています。ただ資料でもご説明しているとおり、すぐにレベル 3 のみにすることについては、ある程度 HPKI としてどう考えるかということもありますので、運用については、今、松本座長からご指摘いただいた点

も踏まえ、検討させていただきます。
　林構成員からご指摘いただいたISOについては、厚生労働省のHPKIだけがISOを併記するのは少し勇気が必要なため、他の政府系のJPKIやGPKIがどのような動向かも含めて、中長期的な議論の一つとして検討させていただければと思います。以上です。
○丸山構成員　丸山ですが、一言だけよろしいですか。併記の書き方ですが、FIPS 140-3をベースに、FIPS 140-2は失効するので落としてもよいと思います。「FIPS 140-3ができない時は同等以上の規格に準拠する」という例外的な書き方にしないと、表に出る文書において失効する規格を残すのは見栄えが良くないので、そのような方向がよいと思います。
○岡嶋主査　ご指摘ありがとうございます。先ほど松本座長が提示された案で、大体その方向性で進められるかと思いますので、そのような方向性で検討できればと思います。
○松本座長　ありがとうございました。では、そのように進めていただければと思います。

議論３：本人確認書類の見直しについて
○松本座長　議論３を表示してください。CP 記載修正案について、ご議論ご意見いただければと思いますが、いかがですか。
○林構成員　見直しは当然必要だと思います。住民基本台帳カードが2025年12月末になくなり、これはその後に更新される内容だと思いますので、適切な本人確認書類に修正することは非常に重要だと思っています。
　本人確認は私の業務の一つではあるものの、各業法全ては把握していないのですが、HPKIのカードと医師の本人確認をどのように行うかという法律に関わる事項だと思うので、そこを鑑みなければいけないと思います。写真付きでなくてはならないなど、条件面も含め、どのような基準でこれらを候補に挙げているのか、また、もし参考にしたものがあれば、事務局にコメントいただければ幸いです。
○松本座長　これは電子署名法における本人確認書類と平仄を合わせたということで、回答になりますか。
○岡嶋主査　資料に記載のとおりで、認識相違ありません。
○林構成員　電子署名法の改訂プロセスも見ていたので、特段違和感はありません。電子署名法における電子署名の目的と、これは結局のところHPKIカードの配布条件にもひもづくという認識で正しいのでしょうか。電子署名法とは目的があまり一致していないように思うので、そこには若干懸念があります。
○岡嶋主査　資格の確認と本人の確認は、おそらく別の話かと考えています。今この資料に記載している書類は、あくまで本人の実在性の確認の書類としてご提示しています。林構成員からのご意見としては、他の手法などもあるのではないか、ということかもしれませんが、少なくとも現在、我が国で他に動いているPKIや、マイナンバーカードのJPKIの本人確認書類や電子署名法の本人確認書類と平仄を合わせることで、厚生労働省としても対外的な説明がしやすくなるかと考え、今回このようなご提案をしています。以上です。

○林構成員　ありがとうございます。
○山内構成員　JIPDEC の山内ですが、簡単に補足します。「電子署名及び認証業務に関する法律」における認証業務とは、本人確認を行い、電子証明書を本人に渡すことですが、本人確認については、今事務局から話があったように、属性については一切法的な保証をするものではありません。つまり、その人物が自然人として存在していることを確認することは、法令上、利用者の真偽の確認として決まっていますが、医師であることや薬剤師であることを保証するものは、「電子署名及び認証業務に関する法律」の中には一切ありません。
　HPKI については、本人確認をした上で、医療従事者である資格の確認をさらに付加した形で運用していると思います。ベースの本人確認のところは全く同じなので、このような形の整理でよいかと思います。以上、補足です。
○松本座長　確認ができましたので、特にご異論がなければ、この修正案でよいとしたいと思いますが、いかがですか。では議論３については、このまま進めることにしたいと思います。
　宿題といいますか、もう一度案を作って議論しなければならないことがありますので、これについては準備を進めていただきたいと思います。よろしいですか。追加でご意見がある方がいましたら、お願いします。
○岡嶋主査　会場でも挙手はありません。事務局としても本日ご議論いただいたところを踏まえ、次回以降、修正案をご提示したいと思います。
○松本座長　ありがとうございました。

（２）次期認証局の構成について
○松本座長　それでは続いて、議題２「次期認証局の構成について」に移りたいと思います。本日、日本医師会、日本薬剤師会、MEDIS から連名で資料提出があります。事務局から本議題の背景等を説明した後、代表して矢野オブザーバーからご説明いただき、続いて事務局から事務局案のご説明をお願いしたいと思います。まず事務局からお願いできますか。
○岡嶋主査　時間が押しており、資料は事前に個別にご説明していますので、簡単に概要のみご説明します。
　資料２－１の１頁をご覧ください。現在、HPKI 暗号アルゴリズムの移行期間にさしかかり、本会議においても、ECDSA における HPKI 認証局のシステムをどのようにするのか、問題提起をいただいています。もし既存の方式を採用したとしても、今後、次期 HPKI 認証局の構成に向けた開発には、数年程度かかると伺っています。これらを考慮すると、なるべく早期に次期 HPKI 認証局の構成を決定し、サブ認証局や医療機関等システムなどの改修に着手できるようにする必要があると考えています。先ほど松本座長からもご説明があったように、本日、サブ認証局を運営されている皆様から、次期 HPKI 認証局

の構成について資料を提出していただいているので、まずそちらをご説明いただき、続いて事務局から案をご提示したいと思います。以上です。
○松本座長　それでは、矢野オブザーバーからお願いします。
○矢野オブザーバー　3認証局を代表して、資料2－2についてご説明します。
先に2頁をお願いします。ご存じのとおり、現在 HPKI 認証局は、厚生労働省のルート認証局があり、サブ CA として日本医師会と日本薬剤師会が共同で運営している日本医師会の認証局と、MEDIS の認証局という形で、ルートとサブの構成になっています。サブ CA になるためには HPKI 準拠性審査を受けるということで、特に限定しているわけではなく、門戸は開かれた形となっています。
1頁にお戻りください。先ほど申し上げたような形で HPKI 認証局が運用されていますが、現時点においては、日本医師会・日本薬剤師会と MEDIS の2つの認証局しかないという状況です。したがって、次期暗号方式への移行にあたり、ルートとサブではなく、ルート1本に集約してはいかがかというのが、ご提案の趣旨です。認証局の構成がルートとサブになっており煩雑だということが理由にありますが、1頁の下部に記載しているとおり、他にも理由があります。ルートとサブになっていると、システムベンダーで中間証明書の仕組みをよく理解していない方がおり、必要な中間証明書の設定をしないなどシステム構築時のトラブルが見受けられます。また、先般のサブ CA の鍵更新の時に、SSL クライアント認証のサブ CA の更新は数多あると思いますが、署名用の IC カードを配っているような認証局としてサブ CA 更新はあまり前例がなかったので、いろいろ苦労して、ベンダーが署名検証に対応できないという事態も招きました。また、GPKI とのブリッジの話もありますが、おそらくサブ CA を抱えている認証局をブリッジすることは前例がないと思うので、現時点の構成では実現可能性が低いと思われます。ただ GPKI をブリッジすることによって JPKI と HPKI は親和性ができるので、医療 DX の基盤を進める中では、もう少しシンプルになるのではないかと思います。何よりも、HPKI 全体としての社会的コストを下げられるのではないかと思っています。
3頁をご覧ください。ルートとサブという構成を廃して、厚生労働省にルート認証局を1本持っていただく場合の構成案です。ただ署名用と認証用でそれぞれ IA、認証局 CA がありますので、これを立てていただきたいと考えています。セカンド用 IA にクラウドタイプを出していますが、これを分離するかどうかは今後の検討として、少なくとも厚生労働省のルートに各団体が登録局（RA）として審査した情報を連携し、電子証明書を発行する、このような構成にしてはいかがかというご提案です。署名用 IA に関しては、GPKI とブリッジすることによって JPKI との親和性も高くなるだろうと考えます。
4頁をご覧ください。3頁の図で示したように厚生労働省のルート認証局は一つで、現在 HPKI 認証局を構成している陣営に関しては RA はそのまま準拠性審査を受けつつ、門戸を開きながら運営すればよいと考えます。ただ課題としては、厚生労働省の IA が発行要求を受けて電子証明書を発行する処理をどうするかということがあります。この課題につ

いて、３つの案があります。案１は、厚生労働省が自ら人員・予算をかけて発行する形ですが、当然、実際は外注です。発行した電子証明書を RA 側で受けて IC カードに書き込んで、エンドエンティティである医師、薬剤師、歯科医師等に発行するという流れです。案２は、厚生労働省から各運営組織（日本医師会・日本薬剤師会・MEDIS）への委託という形を取り、IA の利用権限を付与してもらう形です。IA に対して発行要求が出せる状態にしてもらった上で、今までどおり実作業を各運営組織が実施します。案３は、システム開発が必要になりますが、RA からの発行依頼を受けて、自動で電子証明書を発行できる仕組みを構築するという案です。案１は、厚生労働省が自ら人員・予算をかけて、 J-LIS（地方公共団体情報システム機構）のようなことをやってほしいという案ですが、これにはやはり予算もかかります。そのため案１を除き、案２、案３であれば、我々 RA 各団体で審査をして、厚生労働省 IA は電子証明書を生成だけすればよく、今までどおり各運営組織が予算を組み、IC カードへの書き込みなどを実施する形がとれないかと考えています。また、各運営組織も IA を抱えずに済むため、経費の削減が見込め、その分、新たな投資や支出もできるようになります。IA にかかる費用を他に回すこともできるだろうと考えています。

GPKI とのブリッジに関しては、JPKI の活用がより容易になるのではないかと考えています。

ごく簡単にはなりますが、ルート・サブという構成を次期暗号方式への移行のタイミングで廃止し、準拠性審査は維持し、HPKI をやりたい方々に対しては門戸を開きつつ、ルートを１本にしてはいかがか、というご提案です。ただ激変するのは大変なので、一つの提案としてご議論いただければと思い、本日資料を提出しました。説明は以上です。

○松本座長　それでは続きまして、事務局案をご説明いただければと思います。

○岡嶋主査　ご説明します。資料２－１にお戻りいただき、２頁に事務局案を整理しています。これまでの HPKI 専門家会議の議論においても、今回ご提案いただいた趣旨のご意見を頂戴しており、本日も日本医師会、日本薬剤師会、MEDIS の連名で具体的な提案をいただいたと認識しています。今回ご提案いただいた内容については、HPKI をより効率的、安定的に運用していく一つの案として理解しており、事務局としても重要な課題であると認識しています。一方、現在のルート認証局が担っているサブ認証局に証明書を発行する役割から、サブ認証局が現行担っているエンドエンティティ向けの証明書も発行することに変われば、HPKI の制度設計の位置付け、また、形を変えることによる法制面や制度面の取扱、費用負担のあり方等も含めた整理・調整が必要となり、相応の期間を要するものと考えています。HPKI については既に電子処方箋等で広く使われており、HPKI の継続性と安定稼働は必須であり、事務局としては、まずは目の前に迫った ECDSA への暗号移行を確実に完遂させることを最優先と考えています。認証局構成については今回の暗号移行では変更せずに、暗号移行に向けた開発になるべく早く着手し、サブ認証局の開発、また医療機関等のシステムの時間的・費用的な負担をなるべく抑えるようにしたいと考えて

います。

以上を踏まえ、２頁の一番下に記載しているとおり、事務局としては、現行の認証局構成を維持し、来年度早期から移行に向けて準備を開始するのが妥当と考えています。一方、先ほどのご提案にもありましたように、現行構成は社会的コストが大きいことも事実であると認識していますので、医療 DX 全体の施策や技術動向も踏まえながら、今回ご提案いただいた内容も含めて、将来的なあり方については引き続き検討を行いたいと考えています。以上です。

○松本座長　それでは、次期認証局の構成について、ご意見をいただければと思います。いかがでしょうか。

○宮崎構成員　当面は現在の構成を維持するとのことで、少し安心しています。

ルート認証局単独構成の場合、ルートの秘密鍵を頻繁に使うことになり、危険性が高まります。これは非常に重要な鍵で、普通の運用では鍵をかけてしまっておくような形で、あまり使わないことが多いです。ですからサブ認証局を作り、そこからエンドエンティティに向けて署名をすることが多いのです。そのような構成においては、サブ認証局は頻繁に使うため、その分危険性は高まりますが、サブ認証局の秘密鍵に問題があり失効させなければいけない場合、ARL（認証局の証明書の失効リスト）を出して失効させる技術的な対処法があります。しかし、ルートの秘密鍵がそのようなことになると、失効させざるを得ない時に、ルートに対する失効リストは、どこも出せません。ですから、その時には違う方法で対処しなければならず、非常に厄介なことになります。

これらを踏まえると、ルート認証局単独構成は、コスト的にメリットはあると思いますが、非常にリスクが高く、何かあった時の対応も難しいので、なるべく避けたほうがよいのではないかと思います。以上です。

○松本座長　ありがとうございます。他にご意見はありますか。

○山内構成員　JIPDEC の山内です。結局、「電子署名及び認証業務に関する法律」に基づく認証業務との比較の話になるのではないでしょうか。現在、事業者が７社いて、そのうち２社が２つずつ認証業務を持っているので、７＋２で合計９つの認証業務があり、それを内閣総理大臣と法務大臣が認定していますが、これは全部ルートやサブという概念はなく単独です。ですから、宮崎構成員がおっしゃったような、非常にリスクが高いと見えるものを、国として進めてきています。だからこそ極めて厳しい認定基準を作って、それに基づく指定調査機関として、国から認められた調査員が毎年実地調査をしています。

私自身はここで、こうすべきだという意見はありませんが、一般的にはルート CA と中間 CA の２段階構造になっているほうがリスクは低いとされています。それをやめて１段階構造のルートが一つしかない仕組みにするのであれば、かなりしっかりとした実地調査や監査をしなければいけないと考えられます。そこをどうするかを論点として今後議論されたらどうかと思います。あくまで論点を示すために今、発言しました。以上です。

○松本座長　ありがとうございます。他にご意見はありますか。

○矢野オブザーバー　日本医師会の矢野です。ルート・サブ構成をやめる提案をした立場として、少しご意見させていただきます。

ルート単独にすることについて、特に強くこだわっているわけではありません。確かにセキュリティリスクを考えると、ルートとサブがあったほうがよいと思います。一方、山内構成員がおっしゃったように、JPKI は単独ルートで１億人以上の国民にカードを出していて、何かあったらどうするのかという状況であることも事実です。ご議論いただいて将来的な構成を考えていただくのは良いのですが、私が議論いただきたかったのは事務局の資料２－１の２頁にある HPKI の制度的位置付けです。今回この議論を通して、HPKI を制度的にどう位置付けるかを将来的な議論にしていただきたいと思っています。

HPKI は、最近でこそ普及してきましたが、日本医師会も民間ですので、残念ながら「あれは民間がやっていることだ」と、よく言われます。しかし、我々としては、厚生労働省の証明書ポリシがあり、準拠性審査を受けて、厚生労働省の制度のもとで HPKI を出していると認識しています。ですから、HPKI とは何なのか、この議論をきっかけとして、一番重要な将来的な位置付けについて議論いただきたいと考えています。その議論の上で、ルート認証局は単独がよいか、セキュリティの観点も含めてルート・サブの構成を維持するのかをご議論いただければと思い、今回ご提案しています。

次期の暗号に移行しますので、そこからさらに 10 年ほどたつと、今度は耐量子計算機暗号が出てくると思いますし、どこかでこの議論は出てきますので、位置付けをしっかりとご議論いただきたいと考えています。HPKI 専門家会議の位置付けについても、準拠性審査をしていただく委員会ですから、全ての位置付けをきちんと整理した上で、HPKI を改めてご定義いただければと思ってのご提案です。補足として、以上です。

○松本座長　HPKI 専門家会議に加わって以来、HPKI 周りの方針をきちんと整備しなければいけないと常々思っています。これまでの経緯を踏まえて歴史的に現在のようになっているわけですが、この形で今後もずっと運営していけるのか、現在の方法のほうが良いという案もあれば、ルート CA をメインとし、RA だけ各団体が行って、IA は厚生労働省が持つ形に一本化したほうが良いのではないかという案もあり、この辺りを検討していかなければいけないと思います。

事務局案としては「暗号アルゴリズムの移行もあるので、形式としては現行構成で進めたい。ただし医療 DX 全体を考えた場合にどうあるべきかの議論は、引き続き検討したい」ということです。これも中長期的にどう考えていくかを整理しなければいけないという先ほどの議論の一環として、もし構成を変えるとしたら、どのように変えるのか、その判断をどこかできちんとしなければいけないと思います。将来どちらの構成にしていくかの議論をきちんと行った上で決めなければいけないのですが、次期暗号方式における HPKI 認証局構成は、事務局案どおり進めてよろしいでしょうか。ただし、そもそもの構成のあり方について議論を開始するという条件付きでいかがでしょうか。

○林構成員　林です。暗号移行は進めざるを得ないことなので、個人的には、まず現行構

成を維持する方向にせざるを得ないと思っています。HPKI 専門家会議に参加させていただいてからたびたび発言しているとおり、グランドデザインがあり、その一部のフェーズなのか、その一部分としてなのかは分かりませんが、改考を行っていくということであれば、全体のコスト削減も考えられます。

しかし、グランドデザインがないまま、進めなければいけないので取りあえずこれを進める、次にまたこれが来たのでこれを進める、というような方法で進めていくと、コストが増大していきます。これはシステムにおいて鉄則だと思うので、やはりきちんと議論を継続することが重要だと思います。もちろん手前に考えなければいけない議題はたくさんありますし、議論をすると時間が過ぎていくところも、非常にトレードオフがあって悩ましいとは思いますが、グランドデザインを作ることを念頭に置いた上で、この方針で進めるということであれば、最終的なコスト削減にもつながり、運用もスムーズにいくのではないかと思います。コメントとなりますが、以上です。

○松本座長　ありがとうございます。

○丸山構成員　丸山です。まさに松本座長がおっしゃったとおりで、時間的制約があってできないのであれば、現行構成のまま進めるしかないのでしょうが、現行構成がよいとはとても思えないところも幾つかあります。

費用や効果も含め、どちらの案がよいかは、方針に基づいてきちんと決めていく必要があると思いました。今回は事務局案で進めることに対しては、他の代替案がよいとは言い切れないので、仕方がないと思います。しかし、今後きちんと検討することを前提として、皆様で合意した上で、次々回の更新の時には方針をきちんと示せるようにしておかないといけないと思いました。

矢野オブザーバーからのご提案も山内構成員のご意見も、ごもっともだと思いました。ありがとうございます。以上です。

○松本座長　ありがとうございます。他にご意見はありますか。

○矢野オブザーバー　日本医師会の矢野です。ルート 1 本でという提案をしている者としてはルート単独案をすぐさま取り下げるというのは心情的には苦しいですが、今の議論の流れを踏まえてルート・サブ構成を維持することに関しては、それで良いと思います。

ただし、議事録に残す形で条件を付けさせていただきたいと思いますが、やはりきちんとした制度的位置付けを検討すべきです。例えば CP は省令事項にし、準拠性審査基準を通知で出すなど、具体的な CP や準拠性審査の位置付けを省内でご検討いただき、次期暗号はその体制で進めるということを、検討・議論していただき、その結果をお示しいただきたいと思います。それをもって次期暗号の移行に関してはルート・サブ構成を維持すると決まれば、もちろん我々としては、サブ CA の切り替えに向けて準備を始めたいと思います。以上です。

○松本座長　それでは、繰り返しになりますが、事務局案どおり現行方式を採用する、ただし、中長期的に将来的なあり方についての議論を始めていかなければいけないというこ

とで合意した、ということにさせていただきたいと思います。
一般的に、方式を変えると現行方式と併存する移行期間、マイグレーションが必ず生じてしまいます。認証局群のアーキテクチャをどう変えるかも非常に大きく関わってくるので、次の更新に向けてというより、平時に継続して議論しておかなければいけない話だと思いますので、よろしくお願いします。

（3）HPKI 暗号アルゴリズムの移行について
○松本座長　それでは、議題3「HPKI 暗号アルゴリズムの移行について」に移ります。本日、山本オブザーバーから資料をご提出いただいているので、事務局のご説明後に、山本オブザーバーからご説明いただければと思います。まず事務局よりお願いします。
○岡嶋主査　事務局よりご説明します。資料3－1をご覧ください。議論のポイントを2つ用意しています。まず一つ目のポイントであるリモート署名について事務局から説明した後、山本オブザーバーにご説明いただきたいと思います。
1頁をご覧ください。前回、第 34 回 HPKI 専門家会議にて、次期暗号方式として「ECDSA P-384 with SHA-384」への移行を、リモート署名サービスの構築方法が明確化されることを前提として条件付き承認されたと認識しています。今般、リモート署名サービスのトラストサービスプロバイダーである MEDIS にて、ECDSA 方式に対応したリモート署名サービスの実装方式を検討いただいた結果、クラウド HSM を用いた鍵管理方式を採用する旨の報告をいただいています。その中で、当該方式において ECDSA 方式でのリモート署名サービスが実装可能であることを検証いただいています。事務局としても、今回 MEDIS にて検討いただいた ECDSA 方式でのリモート署名サービスの鍵管理方式は、現在のリモート署名サービスに係る HPKI ポリシに準拠していると考えています。本日ご議論いただきたい内容は、今回のリモート署名サービスの運用方式が明確になったことを受け、次期暗号アルゴリズムへの移行を条件付き承認となっているところを、「ECDSA P-384 with SHA-384」への暗号以降を進めることについて正式に承認いただきたいということです。以上です。
○松本座長　それでは、山本オブザーバーからご説明いただければと思います。
○山本オブザーバー　資料3－2の1頁をご覧ください。ECDSA P-384 対応について、今まで使っていたリモート署名の鍵管理サービスは、[redacted]、ECDSA P-384 の私有鍵に適用できないことが問題となっていました。ECDSA への移行に際して、可能な鍵管理サービス及びリモート署名モジュールの対応について検討しました。
1頁下部の表のとおり、ECDSA に移行しても5年間は RSA も併存する状態なので、併存した状態をどのような形で実装していくかについて、RSA、ECDSA ともに現行の秘密分散＋Multiparty computation（MPC）を使う方法、クラウド HSM を使う方法、オンプレミスの HSM を使う方法が考えられます。

２頁をご覧ください。RSA を変更すると、今まで発行していた HPKI の証明書を再発行する必要があります。リモート署名で鍵を再構成することが特別に許されれば、それは可能ですが、さすがに[redacted]現実的ではないため、現状の RSA は現行方式を今後５年間継続することになります。ECDSA に関しては、秘密分散＋ MPC を使う方法、クラウド HSM を使う方法、オンプレミスの HSM を使う方法を検討してきました。

３頁の表のとおり、秘密分散＋MPC を使う方法について、どのようなものがあるかをリサーチすると、論文等で３つの方法が[redacted]できました。現実に使われているものは Lindell の方式が多く、それ以外の方法はほとんど論文ベースの話で、あまりに実証されていません。Lindell の方式は Blockchain 等への実装例があるので、取りあえず使った上での安全性は検討されていることになります。これを署名の私有鍵の分散に使ったという事例は、調べた範囲では見つかりませんでした。したがって、Lindell の方式を実装するとなると、HPKI が初めて電子署名用の鍵分散を実装することになるという問題があります。

続いて資料３－３をご覧ください。我々は２頁に記載の方式を検討しています。一つは、現行の方法はこれまでどおり、秘密分散＋MPC 方式で行います。署名要求が来た場合に、ECDSA に関する証明書の要求であれば、[redacted]という方法です。

第 34 回 HPKI 専門家会議でお話ししたように、クラウド HSM は保有できる鍵の数をかなり制限しているものが多く、現在使われている数万の私有鍵を HSM 内に保存しようとすると、数十台の HSM が必要となり、コスト面で現実的ではありません。そうではなく[redacted]、現状の 700,000 署名／月ほどのプロセスであれば、万が一の場合のバックアップは必要なので、１台というわけにはいきませんが、アクティブな１台の能力で署名要求から署名値を返すまでは 500ms 以内で実施できることが確認できました。

Lindell の方式で秘密分散＋MPC という方法もあり得ますが、先ほど申し上げたようにリモート署名で実装された例がないため、全て我々がオリジナルで実装しなければならず、今この仕組みを作っているベンダーへのベンダー・ロックインが生じやすくなると考えます。また、クラウド HSM の場合は、それほど特別な技術を使っていないため、特定のベンダーにロックインする可能性は低いです。少なくとも ECDSA に切り替えて５年経過した時点では、ベンダー・ロックインを避けることができるので、こちらにしようかと、考えが傾いているところです。安全性に関しては、どちらも同じで問題ありません。

資料３－３の４頁をご覧ください。構築・運用コストを整理しています。クラウドHSM 方式のほうが構築費用は若干安いです。秘密分散＋MPC 方式の場合は、先ほど申し上げたように、秘密分散の仕組みも MPC の仕組みも理論は既に公開されていますが、全てオリジナルで実装しなければいけないため、構築費用が若干高くなっています。運用経費については、クラウドHSM 方式は、クラウドHSM の利用量の増加に伴い年間 2,000 万円ほど増えますが、秘密分散+MPC 方式は 500 万円ほどの追加ですむだろうと考えています。若干運用経費が増える分、つらいのですが、説明がしやすいことと、ベンダー・ロックインを避けられるということで、クラウドHSM 方式がよいと考えています。

資料３－２の２頁に記載のとおり、オンプレミスの HSM を使う方法もあります。この場合はHSM の本来の能力の鍵保有数に耐えることができるので、それほど大量のHSM は必要ではありませんが、一方で HSM 設置のためのデータセンターを用意しなくてはいけません。しかもリモート署名関連システムがオンライン資格確認ネットワークと連結しており、それがある[redacted]上で構築・稼働しているため、どうしてもその[redacted]と、全く別のオンプレミスの HSM が設置されているデータセンターの間を接続しなくてはならず、非常に複雑な構造になってくるため、あまり現実的ではないと考えています。

したがって、MEDIS としては、クラウドHSM 方式で ECDSA P-384 に対応することが適切ではないかと思います。１年程度の期間で構築が可能ですので、今年度内に方式を決めることができれば、移行のスケジュールには問題がないと考えています。以上です。

○松本座長　それでは議論をお願いしたいと思いますが、もう一つ議題があり、時間が足りません。事務局、延長しても構いませんか。

○岡嶋主査　構成員の皆様のご都合が問題なければ、引き続き議論をさせていただきたいと思いますが、会場が 13 時までとなっており、その点だけご理解いただければと思います。よろしくお願いします。

○松本座長　なるべく早く終わりたいとは思いますが、12 時には終えられない前提で進めます。まずご提案いただいたことについて、ご質問コメントをいただけますか。濱口構成員、お願いします。

○濱口構成員　濱口です。まずクラウド HSM について、認証局やリモート署名サービスの事例を見て、当然HSM に対する要求事項、例えばFIPS の認証を取得していること等は、クラウドHSM でも充足は可能だと思いますが、例えば相互けん制の働いた環境下でHSM が運用されていること等、HSM の運用に関わる要求事項が幾つかあると思います。これらに関する要求事項の充足は、基本的には現地審査にて HSM がきちんと管理されていることを審査していると思います。eIDAS あるいは Web Trust 等もそうだと思います。米国の FPKI も含めて、クラウド HSM も使って、それらの要求事項の審査の充足が可能かということについて、議論が行われているかと思います。その結論としては、基本的にはクラウド HSM だと実地審査ができない、またクラウドサービスプロバイダーが提供するレポートは、現状 HSM の管理に求められている要求事項と整合性のあるものではないとさ

れています。したがって、クラウド HSM を使う方向で要求事項を満たしていくのは、なかなか難しいのではないかと個人的には思っています。以上です。
○松本座長　濱口構成員としてのご意見はありますか。「クラウド HSM では現行の条件を満たしにくい。したがって、もう一つの方式でいくべきだ」ということでしょうか。そこまで強い意見ではないということでしょうか。
○濱口構成員　クラウド HSM では難しく、今の監査基準の制定経緯から考えると、やはりオンプレミスで HSM で実施する方法が一番安全だと考えています。これが、私の意見です。
○松本座長　ありがとうございます。他にご意見はありますか。時間もありませんが、これは非常に重要な課題ですので、皆様から端的にご意見をいただければと思います。いかがでしょうか。
○林構成員　林です。HSM の実運用を経験したわけではないので、明確なことは言えないことをエクスキューズさせていただきますが、現実に今後クラウド HSM の利用はどんどん進んでいくだろうと思います。濱口構成員がおっしゃるように、現行の監査基準を満たさないことも事実だと思います。今後どう変わっていくのか、個人的には、監査できるように社会のシステムが変わっていくだろうと予測されるので、それを踏まえて次のあり方を考えるのが一番理想だと思います。
　例えば、日本にはありませんが、軍事領域などでは当然オンプレミスの HSM を使わざるを得ません。また、建物の基準までしっかり作る必要があります。では HPKI においてどこまでの基準を求めるのかということが問われ、監査基準に反映されていくと思います。本来はこの議論をしっかりしなくてはならないと思いますが、今回はスケジュールの都合があることも鑑みて、何らかの判断が必要だと思います。監査における安全性評価については私自身も知見がないので、皆様のご知見をいただければと思いました。以上です。
○山内構成員　JIPDEC の山内です。JIPDEC は、デジタルトラスト評価センターにおいて、２つの事業を実施しています。一つは、「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です。現状、認定基準の中では、そもそもリモート署名は対象になっていないため、リモート署名についてクラウド HSM を使うかどうかは、この法律の中では特に触れられていません。ただ、少なくとも認証局の実地調査をする時に、クラウド HSM は実地調査ができないため、先ほど濱口構成員がおっしゃったとおり、認証局ではクラウド HSM をどうするかは、今後の検討課題となっています。リモート署名サービスについては、この法律の枠外であるため、JIPDEC は自主的な民間の事業として、JIPDEC トラステッド・サービス登録（リモート署名サービス）として、例えば、サイバートラスト社の iTrust リモート署名サービスなどの現地審査もしてきており、オンプレミス環境におけるリモート署名サービスに関する知見はあります。
　今後の方向性としては、民間レベルにおけるリモート署名サービスが普及していく中で、クラウド HSM を使っていこうという話が出てきますので、それらの動向を見ながら検討

していくことになると思います。HPKIのリモート署名サービスについてクラウドHSMを認めていくのは、相当先進的といいますか、かなり前に進んだ話となります。どのように実地調査あるいは現地審査をするかは課題となりますが、ニーズは高まっていくので、チャレンジングに検討していくテーマであると思います。
○松本座長　ありがとうございます。他にご意見はありますか。
○丸山構成員　山本オブザーバーにお聞きしたいのですが、クラウド HSM のサービスは、SOC２ などを取っているサービスがあれば、その報告書をベースに監査ができるのではないかと思っています。おそらくそういうニーズは各国いろいろな事業所から来ていると思いますので、どこのクラウドを使うかは分かりませんが、そのようなことも事前に調べていただければ、議論がしやすいかと思いました。以上です。
○山本オブザーバー　SOC２ レポートにはクラウド HSM は含まれていますので、それは可能です。一方、SOC２ のレポートはある意味サンプリングの監査であり、自分たちの使っているところが確実に監査されているかどうか分からないことになります。
　もう一つは、現在使用しているクラウド基盤 に問い合わせたところ、法制度に基づく利用に関する監査であれば、クラウド HSM の場合はハードウエアが当然存在しますから、どこのデータセンターを使うか、ある程度コントロールができますが、現地審査を受け入れると聞いています。先ほどの矢野オブザーバーの議論の中でもありましたが、HPKI の位置付けが制度としてきちんとできるのであれば、現地審査も全く不可能ではないだろうと思っています。以上です。
○丸山構成員　分かりました。おそらく HSM クラウド上に並べているものを、誰のものでも同じように取り扱っているから、サンプルで OK となっていると思いますので、サンプルだと確実に利用しているものに当たっていないから問題であるということではないと思いますが、その辺りのルールも含めて決めないと、決めきれないと思いました。どちらがよいかは私もよく分かりませんし、本当に比較検討をきちんとしないといけないと思いました。以上です。
○松本座長　ありがとうございます。
○宮内構成員　宮内です。クラウド HSM を使うとしたら、我々としてもしっかりとした監査基準を作らなければいけないことは、皆様も同意されると思いますが、それを一生懸命作って監査ができる状態になったときには、PQC が来てしまうのではないかという心配もあります。タイムスケジュール上、そのような基準を作って進めることが果たして合理的かどうか。私はそれを心配しており、それを作るぐらいであれば、仕方がないのでオンプレミスでやるしかないのではないか、とも思います。私の意見としては以上です。
○松本座長　ありがとうございます。
○宮崎構成員　クラウド HSM は現地審査の問題があり、分散署名はベンダー・ロックインが生じやすく、また、署名に対する適用がこれまでにないということですが、署名に対する適用例がないことに関しては、きちんと評価すればどうであるか、また、こういう補

助的な仕組みを作れば実現できるかということは、確認できると思います。ベンダー・ロックインに関しても、ソースの公開を義務付けるなどの形で避ける方法もあるのではないかと思いますので、その辺りを考慮した上で比較評価すると良いと思いました。以上です。
○松本座長　今のご発言は「どちらがよいとは、なかなか言い難い」というご意見ですか。それとも「クラウド HSM ではないほうが良い」というご意見でしょうか。
○宮崎構成員　実現性と評価のしやすさからすると、やはりオンプレミスの HSM を使うことになるかと思いますが、それらを横並びにして、もう一度評価をし直してもよいと思いました。以上です。
○濱口構成員　濱口です。丸山構成員から SOC２ の話があったと思いますが、FPKI のポリシマネジメントチームのアドホックチームといいますか、Cloud Tiger Team がレポートを出していて、「SOC２ では充足できない」という結論だったと思いますし、ENISA（欧州連合サイバーセキュリティ機関）のレポートでも同様の結論になっていたと思います。SOC２ だからといってクラウド HSM で認証局の鍵やリモート署名の鍵の管理ができるとはならないのではないかというのが、私の認識です。クラウド HSM や現在の秘密分散方式の延長で進めていくことを認めるのであれば、全体的に達成したい保証レベルを下げていくことが前提になると、個人的に認識しています。以上です。
○六川構成員　構成員の六川と申します。山本オブザーバーに質問があります。山本オブザーバーが作成された資料３－２の２頁の一番上に、オンプレミスの HSM に関するかなり否定的なご意見が記載されています。上から４行目から５行目に「HSM だけのためにデータセンターを確保することはあまり現実的ではなく、～合理的とは言えない」との記載があります。この辺りについてもう少し詳しく山本オブザーバーのご意見をお伺いしたいと思います。お願いします。
○山本オブザーバー　データセンターそのものを確保することは難しくありませんが、[redacted]と密に結合する必要があります。なおかつ、オンライン資格確認ネットワークのセキュリティポリシーに準拠した形で進めないといけないので、かなり複雑な作業となり、相当難しいことになるだろうと思います。つまり、オンライン資格確認ネットワーク側にデータセンターの接続を認めてもらう必要があります。現在はリモート署名システムが同じ クラウド基盤上で動いているので、それなりに安全に結合できることを一応認めていただいていますが、外部のネットワークを通して接続することになると、相当抵抗があるのではないかと考えています。
○六川構成員　既存のオンライン資格確認ネットワークと、これから新たに作るデータセンターの中のオンプレミスの HSM の連携といいますか、そういう新しいものも始まってくるので、大変複雑になってしまうのではないかということが、山本オブザーバーのご意見ですか。
○山本オブザーバー　はい。そうです。
○六川構成員　ありがとうございました。

○松本座長　これも非常に結論を出しにくい議題ですが、いかがでしょうか。もう一度、横並びで評価した上で確認して決めたいというご意見も複数の構成員・オブザーバーからいただきました。このような調査をした上で進めることにしたいと思いますが、事務局はこの形のまとめでも構いませんか。時間的に非常に押しているため、どのように今後進めていくかというところですが、いつまでに結論を出さないといけないかという制約について、お知らせいただけますか。
○岡嶋主査　次の議論ともリンクするところですが、事務局としては2030年1月に新しい暗号方式での認証局で HPKI の発行を開始したいと考えています。そこから逆算すると、今日は決めず、次回の専門家会議で決めることになった場合、開発が間に合うかどうか、まず山本オブザーバーにコメントいただければと思いますが、いかがですか。
○山本オブザーバー　2030 年1月に使えるという意味では、開発期間はほぼ1年で十分だと思うので、2029 年の最初までに決まっていれば構築は可能です。一方で、やはり相当程度テストする必要がありますし、医療機関等のシステムベンダーが対応しないといけません。非常に多くの薬局や医療機関のベンダーが対応できるようになることを考えると、ベンダー対応期間として少なくとも1年ほどあったほうがよいのではないかと思います。
　以上から、来年度には構築に入りたいので、時間的な余裕としては半年ほどでしょうか。2026 年の夏頃までに決まれば何とかなるかと思いますが、薬局情報システムや医療情報システムのベンダーには、かなり急いでもらう必要があると思います。
○林構成員　解決になるのか分かりませんが、視点を少し増やして解決に結び付けることができればと思っています。現行、秘密分散＋MPC 方式で行われており、この場合、オンプレミスの HSM は使っていないという認識でよろしいですか。
○山本オブザーバー　はい、使っていません。
○林構成員　それを鑑みると、現行の方式での基準とオンプレミスの HSM の監査基準を比較するのは、そもそも土俵が違うのではないかと思いました。つまり現行のものに対する評価基準は、携わっていないので経緯は分かりませんが、何かしらの形で導き出されたと思っています。それと同じような形で、同じ基準の監査基準がもしクラウド HSM で満たせるのであれば、もちろん暗号基準を変えるので、現行以上にしなくてはいけないという議論はあるかもしれませんが、現行と同等というラインは、もしかすると出てくるのではないかと思ったので、一言コメントさせていただきました。以上です。
○松本座長　松本です。いずれにせよ、今の段階で事務局からのサポートもあるクラウド HSM でいきましょうということには、なりにくいのではないかと思います。
○濱口構成員　これまで話してきたことの繰り返しになりますが、林構成員のおっしゃるとおり、現行基準上は OK になると思いますが、そもそも基準を作る時に、複数の構成員が懸念を表明していたと思います。今回は時間的に制約があって、仕方なくこの方式を認めるが、本来あるべき姿ではないし、基準そのものも見直していかなければいけないこと、また今回認めることで、以降も同じレベル、この線引きでいくことにならないようにして

いただきたいことを、過去の検討時にも懸念として申し上げていたことだけは、事実としてお伝えしたいと思いました。以上です。
○松本座長　それでは、やはりこれも今日は決められないので、もう一度議論したいと思います。ただ次回の HPKI 専門家会議は、暗号移行に関する全体のスケジュールも勘案した上で開催時期を考えることにしたいと思いますが、その方針で事務局はよろしいですか。
○岡嶋主査　事務局です。ルート認証局やサブ認証局のリモート署名以外の部分については、なるべく早く開発に着手したいと考えています。本日の議論においては、MEDIS にて検討した結果をご報告いただき、新暗号方式でリモート署名サービスが対応可能との結論は導けたと考えています。議論を分けさせていただき、ECDSA への暗号移行については、今回の議論でご承認いただければと考えています。リモート署名をどのように対応させていくかは、また別の議題として整理させていただきます。
　また次回は、冒頭の資料１の１頁にも記載しているとおり、リモート署名サービスの監査要求事項についても議論させていただく予定です。どのように対応させていくかというところについては、事務局としても問題意識を持っていますので、その点も含めて、暗号移行の ECDSA に対応する話と、リモート署名をどのようにして追従させていくかは、少し議論を分けて進めたいと考えていますが、いかがでしょうか。
○松本座長　それでは、このように整理したいと思います。ECDSA に移行することについては、今日をもって合意したと考えます。前回、ECDSA 方式でもきちんとリモート署名サービスができるということが条件になっていましたが、それについては具体的にできることが分かったと認識しています。ただ、どの方式を採用していくべきかについては、監査基準も併せて考える必要がありますが、その検討は次回の HPKI 専門家会議で結論を出したいというスケジュールで進められればと思います。
　以上の整理について、ご同意いただけますか。できればリアクションでお願いできればと思います。「いいね」を出していただけると、ありがたいです。
〔「異議なし」と呼ぶ者あり〕
○岡嶋主査　皆様から「いいね」のリアクションをいただいています。
○松本座長　ありがとうございます。では、そのように進めたいと思います。ぜひ事務局には、リモート署名の実現方式について、先に方式を決めて監査基準を後付けで合わせるのではなく、そもそもどのような方針にするべきかという大前提を起点として方式を定め、それから監査基準も整えるというスタイルで準備を進めていただければと思います。よろしくお願いします。
○岡嶋主査　ご指摘ありがとうございます。いただいた形で進めさせていただきたいと思います。
○松本座長　それでは、次の議題に進めたいと思います。
○岡嶋主査　引き続き資料３－１にお戻りいただき、２頁の「今後の暗号移行に向けたスケジュールのご報告」についてご説明します。次の３頁のスケジュールの矢羽根と一緒に

ご覧いただければと思います。CRYPTREC の暗号強度要件に関する設定基準において、現行の RSA 2048 ビットの暗号、112 ビットセキュリティは、2031 年以降、署名生成を認めていません。一方で、３頁で矢羽根を引いているとおり、スケジュールを考慮すると、旧暗号による署名生成は 2031 年を多少はみ出してしまう可能性があると考えています。その場合のリスクとして、２頁の３ポツ目以降の内容が考えられる一方で、2031 年以降、直ちに危殆化して不正な署名が発行される可能性も低いのではないかと考えています。そのため事務局としては、2029 年 12 月末まで現行暗号で HPKI が発行されるので、発行されたものについては有効期間満了まで現行暗号での署名生成を許容し、2030 年１月以降、順次入れ替える形で、最大５年間の並行期間が存在することを許容いただきたいと考えています。また、厚生労働省情報セキュリティポリシーとの兼ね合いについても引き続き省内関係部局と調整する予定です。以上です。

○松本座長　それでは、暗号移行に向けたスケジュールについて、ご意見をいただけますか。ご意見がある方は挙手またはオンライン上で手を挙げていただければと思いますが、いかがですか。

○林構成員　少し分からないところがあったので、事務局に質問させていただきたいと思います。基本的に事務局としては、現行暗号による署名生成を延ばしたいという意思があるという認識でよろしいでしょうか。PQC はさておき、暗号移行に関しては危殆化のリスクがあると認識しています。延ばすということは、そのリスクを事務局、厚生労働省が受け入れる形になると思いますが、それが好ましいのかどうか、ここには記載されていません。当然コストやスケジュール、その他もろもろを勘案して結論を出すことだと思いますが、まずそのリスクを受容される事務局として、どちらが好ましいのかというご意見があれば、教えていただきたいと思いました。

○岡嶋主査　好ましいとは思えないというのが、率直なところです。ただスケジュールから考えて、どうしても一定程度許容しないといけないところもあります。今、林構成員にご指摘いただいた、国として、厚生労働省として許容できるかについては、なお書きにも記載させていただいたとおり、厚生労働省の情報セキュリティポリシーに定められた要件とは一致しない形となるため、この会議の場で結論をいただいた後に、本当に許容可能かどうかについて、改めて省内で調整したいと考えています。以上です。

○宮崎構成員　宮崎です。今更ながらの確認ですが、ECDSA P-384 with SHA-384 は、エンドエンティティの署名まで含めて、ということでしょうか。また、タイムスタンプの話をよくさせていただいていますが、電子処方箋で利用されているタイムスタンプは大臣認定ではないですが、大臣認定に準拠して構成し直すということですか。

○岡嶋主査　電子処方箋のタイムスタンプについては、基本的にはご指摘のとおりですが、タイムスタンプ認証局を運営している社会保険診療報酬支払基金で検討される事項と考えているので、この HPKI 専門家会議の議論とは少しずれてしまうと考えています。

○宮崎構成員　承知しました。ただベンダーとしては、総務大臣認定に準拠となると、

2029 年から ECDSA の新しい 128 ビットセキュリティのタイムスタンプが発行されることになるので、それを解釈できるソフトを準備しなくてはいけないことになります。ですから、その辺りも含めてベンダー側にはいろいろ伝えていただきたいと思いました。以上です。
○松本座長　事務局、よろしいですか。
○岡嶋主査　宮崎構成員からご指摘いただいたところは、電子処方箋で利用しているタイムスタンプ認証局が大臣認定を取っていないこと、また、タイムスタンプ認証局の暗号移行と HPKI の暗号移行のスケジュールはよく調整してほしい、というご意見かと承知しました。それについても引き続き省内で連携しながら調整していきたいと思います。以上です。
○松本座長　他にご意見はありますか。よろしいですか。では今いただいたコメントを含め、進めていくことになるかと思います。よろしくお願いします。

（４）認証局準拠性審査実施（ルート・日本医師会・日本薬剤師会）について
○松本座長　それでは「認証局準拠性審査実施（ルート・日本医師会・日本薬剤師会）について」、ご説明をお願いします。
○岡嶋主査　資料 4 に移ります。 1 頁をご覧ください。厚生労働省ルート認証局（IA のみ）、日本医師会認証局（RA 及び IA）、日本薬剤師会認証局（RA のみ）の準拠性審査の期限が間もなく到来するため、改めて実施が必要です。審査班については引き続き丸山先生と六川先生にお願いしたいと考えており、これについてご審議、ご承認をいただきたいと思います。以上です。
○松本座長　こちらについて、このとおりに進めてよろしいですか。皆様、ご意見があればお願いします。
○岡嶋主査　ご異議なしという形で、皆様、うなずいていらっしゃいます。
○松本座長　了解しました。それでは、事務局案のとおりに審査班を指名することを承認したいと思います。では次に進めていただければと思います。

（５）連絡事項
○岡嶋主査　本日はご議論いただき、ありがとうございました。最後に連絡事項です。次回の HPKI 専門家会議について、時期は決めかねているところですが、本日議論いただいた内容を事務局内で整理した後、日程調整を進めたいと思います。なお、次回は、HPKI の関連書類のポリシの改定について、また、先ほど引き続き議論する形になったリモート署名のあり方を中心に取り上げることを予定しています。以上です。
○松本座長　連絡事項について、ご質問等はありますか。

閉会

〇松本座長　今日はたくさんの議題があり、内容も濃かったことから、予定時間を25分オーバーしてしまいました。大変申し訳ありません。ありがとうございました。本日はこれで閉会とします。

以上