第３１回保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議　専門作業班合同会議

日時 令和７年２月５日(水) １０：００～

場所 AP 虎ノ門　B ルーム

（1）日本医師会認証局 鍵更新結果の報告

○井上専門官　定刻になりましたので、只今より第 31 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。先生方におかれましては、大変お忙しい中、本会議にご出席いただきまして、誠にありがとうございます。本日の会議は、現地とオンラインのハイブリッド会議での開催としており、公開での開催、資料については、一部公表させていただいております。また、正確な議事録作成やご意見を賜ったときの整理を事務局等で正確に行うために録画させていただきますこともご承知おき願います。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ですが、専門家会議構成員の佐古構成員、柴田構成員が欠席、横田構成員がオンライン参加となっております。濱口構成員はオンライン参加の予定ですが、追って参加されるものと思っております。その他の構成員は現地参加となっております。議題に入る前の留意事項ですが、速記業者が議事録を作成する際にどなたが発言されたか分からなくなるため、構成員の皆さまにおかれましては、ご発言をされる場合に、名前をおっしゃってから発言して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。本日の資料は議事次第、資料 1 、参考資料 1 、参考資料 2 、参考資料 3 をご用意しております。資料の不足等ございましたら、事務局までご連絡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いたします。

○松本座長　はい、皆様おはようございます。本日の議題は「日本医師会認証局　鍵更新結果の報告」と「暗号アルゴリズムの移行に関して」の議論となります。最初の議事につきまして、鍵更新結果についてのご報告を事務局よりお願いいたします。

○佐々木情報推進官　事務局の佐々木でございます。

　それでは資料 1 の 4 頁目をお願いいたします。まず、これまでの専門家会議で進め方を議論し、準備を行ってきました日本医師会認証局のサブ CA 鍵更新についての議題となっております。これまでの HPKI 専門家会議の中で予告をさせていただいていた通り、11 月 15 日にキーセレモニーを実施いたしました。また、キーセレモニー後に鍵の切り戻しも実施しており、その後、新しい公開鍵証明書を公開し、 1 ヶ月後の 12 月 14 日に新鍵への切り替えを行っております。それぞれの日程において、立会人として丸山先生、六川先生に立ち会いいただいております。今回から立会いにあたり、事務局でチェックリストを用意させていただきました。参考資料 2 として資料に入れておりますが、事業者より提供いただいたキーセレモニー自体の実施手順書を事務局で確認をさせていただき、作業内容に対して確認するポイントを示したものとなっております。丸山先生と六川先生には、この立会い時にチェックリストに記入いただきました。参考資料 3 に入れておりますので、ご確認をお願いいたします。キーセレモニー当日、新鍵への切り替えの立ち会いを行った両日ともに、特段のトラブル等の発生はございませんでした。予定通りに作業は完了しております。また、新鍵での運用開始から本日まで、電子処方箋においても日本医師会サブ CA 鍵更新に起因した署名関連での問題は報告が上がってきておりませんので、安定した運用

状況が継続できております。事務局からの概要説明は以上になります。それでは立会人の丸山先生より立会時のご報告をいただきます。丸山先生、お願いいたします。
○丸山構成員　丸山でございます。よろしくお願いいたします。私と六川先生で 11 月 15 日キーセレモニーの実施に立会いました。立会い場所はデータセンター内認証局サーバールームの中です。キーセレモニーが手順通りに行われているかどうか、結果を確認しながら進めているか等を確認し、無事実施されていることを確認いたしました。キーセレモニー後に、新鍵の発行ができるようになっていることを確認するため、12 月 14 日に同じデータセンターのサーバールームにて、六川先生とともに新鍵の切り替えも合わせて確認し、今報告にありましたように、無事に鍵更新が完了していることが確認できている状況です。私の方からの報告は以上でございます。
○松本座長　ありがとうございました。それではこの日本医師会認証局鍵更新結果につきまして、専門家会議の構成員の皆様からご質問などがございましたらお願いいたします。特によろしいでしょうか。ありがとうございました。それではこれを確認したということで進めたいと思います。丸山先生、六川先生、どうもありがとうございました。事務局の皆様もどうもご苦労さまでございました。それでは続きまして次の議事、暗号アルゴリズムの移行に関して、まず事務局よりご説明をお願いいたします。

（2）暗号アルゴリズムの移行に関して
○佐々木情報推進官　はい、事務局でございます。それでは議題 2 の暗号アルゴリズムの移行に関して事務局より概要を説明させていただきます。資料 1 の 6 頁目をお願いします。これまでの振り返りになりますが、現状の HPKI では、SHA-256、RSA2048 を使用しております。一方で、Cryptrec から出ております、セキュリティ強度要件の基本設定方針の表にある通り、112 ビットセキュリティはすでに移行期間に入っており、2030 年までの対応が必要となっている状況です。これに関して第 29 回の HPKI 専門家会議時に、中長期の進め方について議論をいただいたと思いますが、その際に来年度以降で HPKI でも 2030 年までに移行を進める暗号アルゴリズムの選定も議論をしたいと、事務局からご提示をさせていただきました。その際、議論につきましては来年を待たずに今年度からスタートをすべきではないかというご意見をいただきましたため、本日の会でまず議論を開始させていただきたいと思っております。本テーマについて本格的な議論は本日が初回になっておりますので、まずは保健医療福祉分野において暗号移行するという点で、課題や確認をしなければならない事項、取り巻く環境との整合等、幅広にご議論をいただければと思っております。本日はまずは議論開始というところでございますので、具体的にどういった暗号にするのかという選定で確認事項等が発生するかと思います。それらを事務局の方で確認をさせていただき、次回以降の HPKI 専門家会議の中で具体的に「この暗号にしていこう」という選定を進めていきたいと思っております。
　続いて 7 頁目お願いします。移行する暗号アルゴリズムについて、本日の議論の参考情

報として、厚生労働省ではないですが同じく政府系の PKI における進捗状況について共有させていただきます。こちらはデジタル庁で運用を行っております GPKI になりますが、昨年 10 月にデジタル社会推進会議関係課長等連絡会議で承認があり、具体的にこの暗号移行に向けた形で相互運用仕様書の改定がされております。これは GPKI のホームページに公開されている情報になっており、その公開情報を抜粋したものになっております。この GPKI は表示している通り、スケジュールもホームページで公表されております。具体的には 2028 年に新暗号運用が開始される計画で記載されております。

続いて 8 頁目をお願いします。こちらも同様に公開情報になっており、GPKI は政府認証基盤相互運用性仕様書の中に記載されています。具体的に GPKI で次期暗号アルゴリズムとしてどういったものを使うのかというと、鍵長 384 ビットの ECDSA 楕円暗号を利用し、192 ビットセキュリティになるという認識です。

続いて 9 頁目お願いします。同じく参考情報としてマイナンバーカードで利用されている JPKI になります。こちらは我々から総務省へ確認を行いました。先ほど提示した GPKI と相互認証を行っている関係上、暗号アルゴリズムは GPKI の仕様に従うことになっているとのことでした。HPKI は JPKI のように、特段 GPKI と相互認証を行っているものではありません。ただし、政府系の認証局として動いているため、特段の事情がなければ足並みを揃える形でいいのではないかと事務局として考えている次第です。本日はこれらの参考情報も加味いただきながら最初にお伝えした通り、HPKI としての次期暗号、そして暗号移行の進め方等について、保健医療福祉分野という特殊な環境特性も踏まえながら幅広に議論いただき、課題や懸念事項、選定に向けて改めて事務局等で次回までに確認を進めなければならない事項について、ご議論をいただければと思っております。事務局からの概要説明は以上となります。松本先生よろしくお願いいたします。

○松本座長　はい、ご説明ありがとうございました。それでは皆様からのご意見あるいはご質問をいただければと思いますけれどもいかがでしょうか。

○林構成員　林です。初めて参加させていただいた時にこの話題を出させていただいたものとして検討事項が 2 点あると思っております。 1 点目は、これはどこでも暗号移行の際にお伝えしているのですが、本来であれば暗号危殆化は常に生じる可能性があるものです。この線表を GPKI で引かせていただいている立場でもあるのですが、本来何か危機が起きた時には、素早く切り替えられることが求められているはずです。もちろん計画的に実施すること、大事なところで足並みを揃えることは重要だと思うのですが、ものすごく長い線表を引かなければ暗号移行ができないということは、認証局として危ない状況であることを皆様にご認識いただかなければならないと思っている次第です。これは技術的な側面で運用も含めて感じているところです。また、ここにない話題で大変恐縮ですが、今各所で非常に問題視されていることについてコメントさせていただくと、「PQC（耐量子計算機暗号）」という単語が必ずつきまとってくると思います。非常に白熱しているものの、慌てて飛びつくことに関しては個人的に非常に危惧があり、ここに関しては慎重に議論を

し、移行のプロセスを考えていく方がいいのではないかと思っている次第です。一旦林からは以上です。
○松本座長　ありがとうございます。最初の点はいわゆる暗号クリプトグラフィック・アジリティ等といわれていることで、暗号技術を差し替え可能な体制にしておくということも考慮するべきであろうという意見かと理解したのですが、よろしいでしょうか。
○林構成員　はい、その通りです。
○松本座長　また、耐量子計算機暗号について世の中が騒がしくなっているわけですが、この HPKI に関してはどうするのかよく判断しなくてはいけないというご意見ですね。ありがとうございました。その他ございますか。
○宮内構成員　宮内でございます。林さんがおっしゃった通りだと思うのですが、暗号移行というものは、今後認証局だけでなくシステム全体が新しい暗号に対応しなければならないという意味で、そのための準備期間がいることは理解できると思います。したがって、緊急な対応も必要ですが、この件に関してはきちんと線表を引くことが必要と思います。特に RSA でないものを使うことを将来的に考えるのであれば、システム側でも色々考えなければいけない部分が出てくる可能性もありますので、そのような意味では早めに着手した方がいいのではないかと思うところです。それから耐量子力コンピューターの話ですが、これは署名と暗号で随分様相が違うと思っています。暗号化の場合には「Harvest now, decrypt later」で、今のうちにとっておいて、将来量子コミュニケーションができた時に解読するという方法があります。一刻も早く対応しなければならないという意見がありますが、今行おうとしているのは署名なので、署名したものに対し、その時ごとに必要な長期証明等のフォーマットで安全性を高めていけば、暗号と同じようなことはないのではないかと考えている次第です。そのため本件で量子コンピューターについて何かすべきという気は全くありません。恐らく量子コンピューターが本格的に動くのは十年以上先のことなので、今取っておいたものを将来復号することを考えなくてよいのであれば、まだ無理に進める必要は無いのではないかと考えています。以上です。
○山内構成員　山内です。質問ではなく、補足的な情報提供をさせていただきます。昨年 7 月 24 日にデジタル庁及び関係省庁、そして電子署名および認証業務に関する法律に基づく認定認証事業者、地方公共団体情報システム機構、内閣サイバーセキュリティセンターなどが集まった会議が開催されました。暗号移行についての議論も平場で議論されています。そこに厚生労働省が参加されたかわからないですが、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として、認定認証事業者 7 社から今後の変更認定に関するスケジュール調整などについて相談させてほしいという話が来ています。最終的に決めるのは主務省であるデジタル庁と総務省ですが、私どももデジタル庁の仕事を支援する形で委託事業も行っているため、協力させていただく中で色々情報が入ってきています。一応念のために言いますと、この資料 1 の 7 頁目にあります GPKI の暗号アルゴリズム移行スケジュールの表の中で、下から二つ目の欄にあります「GPKI ブリッジ認証局と相互

認証する認証局」というのが、まさに電子署名および認証業務に関する法律に基づく認定認証業務です。現在、７つの事業者が行っておりますが、７つのうちの２つの事業者は２つの認証局を持っているため、９つの認定認証業務があるということです。それらの内容は守秘義務がありますからこの場で申し上げることはないし今後申し上げることもありませんが、全体的なスケジュール感などについて、差し支えない範囲でこの HPKI 専門家会議に対して必要な情報をご提供させていただこうと思っています。もちろん厚生労働省においても、デジタル庁との間で連携いただければと思っております。情報提供させていただきました。以上です。

○松本座長　周辺情報状況も含めてご協力いただけるということで、ありがとうございます。その他ございますか。オンラインでご参加の方はいかがでしょうか。それでは私から確認をさせていただきます。資料７～８頁目を見ると、暗号技術の具体的な署名アルゴリズムまで特定されている形になっています。８頁目の「BCA」は「Bridge CA」の略でブリッジ認証局のことを指すのでしょうか。その CA 鍵の鍵長は 384 ビットの ECDSA。ECDSA は楕円曲線暗号技術である「Elliptic Curve Digital Signature Algorithm」の略であり、この中でハッシュ関数として SHA384 を使うということですね。官職 CA というのは各府省のものであると思いますが、CA は同じものを使い、民間 CA は、384 ビットの ECDSA と、ECDSA with SHA384 とすることが望ましいとなっています。また、括弧で CA 鍵の鍵長云々とあります。このあたりについて、もし林さんがお詳しければ解説していただけるとありがたいのですが、可能でしょうか。JPKI は GPKI の Bridge CA と相互認証を行っていて GPKI と同じアルゴリズムを使うということなので、結局今の ECDSA with SHA384 というものを使うということだと理解しました。HPKI では相互認証を行っていないということなのですが、GPKI における民間 CA というものの位置づけというのはどうなっているのでしょうか。またそこでは官職 CA とは違うものも許されるとなっているのですが、これは Bridge CA を通じて連携するということになっているというような意味なのでしょうか。そのあたりがよくわからなかったので可能であればお願いします。

○林構成員　私も完全に理解しているわけではないので、「自分の認識では」という前提でお話ししますが、HPKI とはブリッジ認証しているわけではないという認識でいます。しかし結果として強度を揃えて今まで来ていました。また６頁にある元々の方針に関して言うと、前々回あたりに議論があったかと思いますが、ルート CA に関しては、厚生労働省が持たれているということを鑑みると、Cryptrec の方針に合わせる必要があるということで、暗号移行のビット調に関しては強度を合わせていく必要があると言われています。ただ相互に乗り入れをすることが、今まで恐らく検討されていなかったので、本質論としては独立でも良いということになろうかと思います。ただし、先日いくつか JPKI を使った署名を検討するお話があったので、そういう意味では乗り入れの部分はより進んできてしまう可能性があり、その部分については考慮事項かもしれないと思っている次第です。

○松本座長　ありがとうございます。いろいろご意見・ご質問があると思いますが、先ほ

どの山内さんのお話では、民間の認証業務で JIPDEC が役割を持っており、7 頁の下から２行目については９認証業務が対象になっているとのことでしたが、GPKI ブリッジ認証局と相互認証する認証局となっているのでしょうか。
○山内構成員　私の理解を言うと、GPKI は総務省、デジタル庁が運用している認証局のことで、政府認証基盤と呼んでいますが、これがどの民間の認証局と相互認証するかは政府が決めているわけです。どのような時に使うかというと、例えば建設業の方々等が電子入札コアシステムを通じて電子署名を行った際、調達する側の国土交通省等関係省庁が電子署名を検証して確かに建設業者から入札が来たということを確認するわけですが、その検証の時に GPKI を使っているのではないかと想像しています。私たち指定調査機関が直接見に行っているところではないのでこちらは想像ですが、他にも総務省が運営してきている GEPS という電子調達システムのところでも同じような仕組みとなっていると思っています。20 年以上前から、各省庁が電子署名を検証する仕組みとして GPKI を使うようになっています。そのため、民間の認証局が発行している電子証明書の検証をする際、GPKI のブリッジ認証局を使いながら、先ほど申し上げた 7 社 9 業務の認証局が、発行している電子証明書の検証もできるようにしていると想像しています。具体的な運用については、総務省などにお聞きいただきたいと思っています。
○松本座長　解説ありがとうございます。林さん、どうぞ。
○林構成員　補足をさせてください。実は、今 GEPS などはデジタル庁に移管されて共管されております。先程山内委員からお話があった認定認証事業に関しては、どちらかというと電子署名法などの関連で移行のお願いをさせていただいている側面が大きいです。９社に関しては、どちらかというと法律の観点から移行をお願いするというところが大きくあると思います。もちろん相互の認証の部分は大きいと思いますが、何よりも暗号移行をしてくださいというお願いに関しては、どちらかというと法律があり、認定制度があるため移行をお願いしている側面が大きいと思っております。以上補足です。
○松本座長　よくわかりました。ありがとうございます。その他皆様、何でも構いませんので、ご意見出していただけるとありがたいですが。特に保健医療分野に関して注意しなければいけない事項など、あるいはご懸念の事項があればと思いますが、いかがでしょう。
○西山構成員　西山ですが、民間の署名法の認定を受けた認定事業者として、過去何年か暗号アルゴリズム移行の経験をしています。先程林さんがおっしゃったように、民間の署名法の認定認証事業の署名に使う暗号アルゴリズムは、署名法の施行規則と指針で定められています。基本的には Cryptrec の中から選定するようになっています。認証局が鍵更新を行うことは技術的にそれほど難しいことではありませんが、一番厄介なのは検証基盤です。証明書を使っている Relying Party といいますか、検証者の方々の検証システムが新暗号アルゴリズムに対応できているかどうか、普及状況が一番見極め時です。勝手に暗号アルゴリズムを移行しても、検証システムが対応していないと結局使えないことになるので、実務的には、検証側と認証局側がハーモナイズしながら移行の時期を決定することが一番

のポイントになろうかと思います。暗号アルゴリズムの危殆化のベースのスケジュールはもちろんありますが。したがって、保健・医療・福祉で、現在どなたがどのような検証ソフトで検証しているのか、ECDSA に仮に変えるとして、事前にそのような対応に問題がないことを確認することが非常に重要なポイントかと思います。特に ECDSA は従来の RSA よりも検証に時間がかかる場合もあるので、細かいことですが、実務的にパフォーマンス上問題ないかといった確認も必要になるかと思います。以上です。

○松本座長　ありがとうございます。その他ございますか。どうぞ。

○宮崎構成員　宮崎ですが、今回の暗号アルゴリズムの移行の考慮範囲が HPKI の認証局の話ですよね。実際には、電子処方箋等では、署名以外にもタイムスタンプも使います。もちろん厚生労働省のテリトリーではないとは思いますが、利用者の立場から、タイムスタンプ側の暗号移行についても、例えば総務省に何らかの申し入れをすることを検討してもいいかと思います。現在、タイムスタンプの認定制度の中では、移行についての考慮は全くなされてない状況です。昔、TBF や TSF など、時刻認証業務を行っているベンダーが集まっていた団体がありました。その中では、タイムスタンプを 2030 年に向けてどのように移行していこうかと団体内で検討し、「業者間ではこのようにやっていきましょう」といったことは一応決めていますが、きちんとした制度には繋がっていないという状況です。例えば厚生労働省から総務省に対して、制度内でしっかり位置づけてほしいという申し入れをしてもいいかと思いました。以上です。

○松本座長　今のお話は、厚生労働省の側で認証局を持っていたり、医師会等々の HPKI を使う認証局群、あるいは末端の医療機関等々で署名を検証したりする部分で、アルゴリズムが全部同じでなければならないという話ですね。それから、ここで挙がっているデジタル署名の方式に加えて、暗号技術ベースがほとんどだと思われるタイムスタンプという技術が使われており、現在は総務大臣が認めるという形をとっている。データ通信協会が業務の認定の審査をしているという建て付けになっていると思いますが、大本の基準等がどうあるべきなのか。実は暗号移行の話が同期していないということですね。これは要注意だというのがよくわかりましたので、検討しなければならないことの 1 つですね。ありがとうございます。それから、先程西山さんからも、Relying Party といいますか、署名を検証する側がきちんと対応しなければいけないというコメントがありました。これは先程宮内さんがおっしゃったことと符合しているかと思います。全部繋がっているため、きちんと無理なく移行できるようにしなければいけないですが、デッドラインが決まっているため、準備を様々なところで行っているであろうと思います。取りかかり始めるという点では HPKI は後発になるのかもしれませんが、その分だけ事前に検討されているものを活用できるという点では有利であるということかと思います。他にご意見等ございますでしょうか。西山さん。

○西山構成員　もうご存知のことだとは思いますが、念のために申し上げますと HPKI の CP も変更する必要があるので、しっかりスケジュールの中に入れておく必要があると思

います。
○松本座長　その通りですね。
○林構成員　皆さんのおっしゃる通り、結局サプライチェーンではないですが、エコシステムの全体像の中で全部が移行しなければいけないことがおそらく一番難しく、検証が一番大変なのだろうと思っております。GPKI のスケジュールを参考にしていただくと、結構遅くなってしまうと思います。GPKI のスケジュールは様々な都合でかなり前倒しをさせていただいている事情はあるものの、かなり「もっと前に倒せ」という声が高い中での公表スケジュールになっています。「じゃあこれでいいんだ」と同じ歩調で進めると、HPKI において必ずしも適正かどうか分からないので、きちんと検討した方が良いと思います。個人的な感触では、ルート CA 局を厚生労働省が持っていることを除くと、今回や今までの検討会、リモート署名も含め、フットワーク軽く HPKI を運営していただけている認識を持っています。そのような意味では、検証を早めにスタートすることもできるのではないかと思います。線表に関しては、なるべく安心感の高い線表をリアリティのある形で作っていただくことが肝要かと思っております。自分が言うのは大変恐縮ですが、繰り返しになりますが、GPKI のスケジュールは必ずしも非常に適正なスタンダードなものではなく、所与条件を満たせるように各所との調整のようなマージンも取りながら設定されているものです。それを鑑みてスケジュールを立てていただくのがよろしかろうと思っております。以上です。
○松本座長　ありがとうございます。非常に貴重なご意見かと思います。喜多さんどうぞ。
○喜多構成員　喜多でございます。もう 1 点、IC カード自身も作り変えなければならないと思います。カードの ISO/IEC15408 の CC 認証取得について長期化が見込まれますがあまりスケジュール化されている線表を見ないので、それを含めて忘れないようにした方が良いかと思います。
○松本座長　はい、そうですね。検証側でもあり、署名をする側でもあるということかと思います。ありがとうございます。その他いかがでしょうか。
○矢野構成員　日本医師会の矢野です。 7 頁の表を見ると、現場感覚としてはドキドキします。検証基盤や署名するソフトなども考えると、もうとにかく決めてほしい。HPKI がルートサブ構成を取っていなければ、日本医師会はもう先に進めています。また、楕円で進めたとしても、ルートが変わらない限りサブ CA だけ先にやっても意味がありません。ですから、厚生労働省には「もっと早くやってください」と言いたいし、「そもそも構成を見直すのか」など、いろいろ考えなければならないので、このスケジュール見ていると心臓がバクバクします。現在電子処方箋が動いており、これから医療情報を交換するネットワークも動きます。どこまで HPKI を適用するかわかりませんが、少なくとも電子処方箋が動いている中で、様々なスケジュールが間に合わないということで HPKI が止まると、それは処方箋が出ないということで、医療が止まります。HPKI としての特殊性としては、hcRole という資格属性を持っているという特殊性はありますが、さらなる特殊性としては

医療が止まってしまうというところがあります。暗号アルゴリズム移行は、今回の鍵更新のように更新するわけではないと思います。新しい認証局を立て、ダブルで立ち上げながら、新しい方の認証局をどう監査・認定して HPKI としていくかという手順も必要だと思います。手順書でも何でも良いので、早め早めにお願いしたいと思います。
○松本座長　大変貴重なご意見であり、私ももっともかと思います。先程、今日の第１の議事で鍵更新の結果を確認させていただきました。現行のルールでは、次の鍵更新も時期が決まっていますが、それと今回の暗号方式自体を変えるということをどう整合させていくのかという話もあるかと思いました。どちらかで決めれば良いかと思いますが、「次の鍵更新までの期間があまりにも短すぎるのでスキップしてもいいとするのか」なども含めて、確かに手順が重要かと思います。他にございますでしょうか。リモート参加の先生方いかがでしょうか。濱口さんも入られていますが、発言可能でしょうか。
○濱口構成員　濱口です。よろしくお願いします。既に構成員の皆様がおっしゃっていただいた内容に同意するところでありまして、特段重ねて発言するようなところはないです。僕は暗号が専門ではありませんが、おそらく Cryptrec が ECDSA への曲線を生成するためのシード値に疑念があるというようなところも Cryptrec で評価され、今の移行のスケジュールになっているかと思います。192 ビットセキュリティへの移行という形になると思いますが、今の予定に対して特段コメントはございません。
○松本座長　ありがとうございます。
○横田構成員　よろしいでしょうか。
○松本座長　はい。
○横田構成員　横田です。今日リモートで参加させてもらっております。先程少し音声が止まったので、議論があったかもしれませんが、今回の対応によるコストもきちんと洗い出した上で、できるだけ既存の認証局に負担がないような方法について検討の余地もあるかと思います。本来のこの会議の趣旨ではないかもしれませんが、コストの問題で大変だという議論も過去にあったかと思いますので、今回の対応によってかかる費用についても考慮に入れていただけたらと感じておりました。以上です。
○松本座長　ありがとうございます。山本先生、どうぞ。
○山本構成員　山本です。コストの問題で言うと、やはり大きいのは検証側のコストの問題です。開発時間に依存しますから、早く決めて開発時間を十分に取ってあげる必要があります。また我々の方でリモート署名用の検証ライブラリは無償で GitHub で公開する予定になっていますので、新アルゴリズムに両方対応することができるようになれば、おそらく時間さえあれば各ベンダーさんはそれほどお金をかけずにできると思います。短期間でやるとなるとものすごく膨大な社会的な費用がかかる。日医さん、日薬さんに相談しなければいけませんが、認証局については、新アルゴリズムになれば、今２つあるサブ CA は１つでいいのではないかと思っています。認証局のコストは全体としてはそれほど大したことはありませんが、節約はできます。どのみち新アルゴリズムで CA を移行するので

はなく、CA を 2 つ立てなければならないため、旧 CA と両方、おそらく 5 年間は運用する必要があります。医療全体でみても 30 万人程度ですので、2 つ CA がある必要もないのではないかと思っています。以上です。
○松本座長　今のお話はかなり重たい議題かなと思います。林さん、どうぞ。
○林構成員　林です。今のお話は本当に重たい話かと思っています。1 点、経緯を知らないというところも含めてコメントです。サブ CA が 2 つあるというのは、BCP 観点で 2 つ用意されているということではないのですか。
○山本構成員　単に 2 つ偶然できてしまったということです。最初は MEDIS だけでしたが、メインユーザーである日本医師会が、自分たちの医師資格証の制定も含めて独立した CA をお持ちになりたいということで、多分作られたのだと思います。それはそれで全く問題はなく、MEDIS や日医ではなく、日本 HPKI 認証局にしてしまえば、RA として医師会も薬剤師会も MEDIS も動けば良いだけの話です。もっと言えばルート CA をなくしてもいいかなと思います。
○松本座長　矢野さんどうぞ。
○矢野構成員　厚生労働省が審査という現業をできないということもあったので、審査を行うために MEDIS が最初に立たれ、その後に日本医師会、日本薬剤師会が立ち、サブ CA 構成にして実際の審査現業をするという構成になっています。ですので、私もルートサブではなく HPKI はルートを 1 個にして、そこに現業の仕事として、我々三師会と MEDIS が入るような構成でいいのではないかと思っています。
○松本座長　河野さん。
○河野構成員　薬剤師会は、職能団体の共通の認証局のような形で日本医師会の認証局ですが、登録の審査等は少し差がありますので、登録局（RA）としての仕事は別としても、証明書発行局（IA)としては 1 つでもいいのではないかということで、現在日本医師会と一緒に行っています。もう 1 つ、先程喜多先生からもお話がありましたが、IC カードの設計と調達におそらく数年単位かかるのではないかと思っています。現在調達に 2 年ぐらいかかっているので、前倒しになるとおそらく相当大変なことになるのではないかと心配しております。
○松本座長　ありがとうございます。林さん、ご質問に対する回答としてはよろしいですか。
○林構成員　はい、理由も分かりました。逆に言うと単一になってしまって大丈夫なのか、アーキテクチャーを見直すタイミングなのかもしれないと思いました。ルート CA 局だけでよいのではないか、アーキテクチャーを見直してコスト削減など、検証コストを削減するタイミングでもあるのかもしれません。おっしゃる通り IC カードの調達については非常に困難であると存じておりますので、様々なものを前倒しで検討を始めるということに尽きるのかなと思った次第です。以上です。
○松本座長　ありがとうございます。その他ございますか。どうぞ。

○西山構成員　よろしいでしょうか。話が少し広がっているので、少し脱線してしまうかもしれないのですが、今回の新しい暗号アルゴリズムに移行後は、鍵長が長くなるため、例えばAdobeのAATL（Adobe Approved Trust List）に組み込む技術要件を満たすことができます。そうすると、今まではAdobeのAATLに入れようとしても鍵長の問題で入れられませんでしたが、基本的な技術基準はクリアできると思います。しかもICカードの場合は署名生成装置を使っているので、Adobe の要件を満たすことができます。AdobeのAATLに登録をすると、普通のAdobeのリーダーで、HPKIの署名の検証ができます。例えば今後、診療情報提供書などを広く先生方にご提供する場合に、PDF のフォーマットであれば、手元のリーダーで検証ができるということも実現できます。暗号アルゴリズムの移行問題とは違いますが、移行後はそういった技術要件を満たすことができるので、AdobeのAATLに入れることを検討することも考えられるのではないかと思いました。以上です。
○松本座長　ありがとうございます。他はよろしいですか。宮崎さん、どうぞ。
○宮崎構成員　宮崎です。今のお話の件ですが、少し考えた方がいいかと思ったのは、Adobe の AATL 認定認証の基準の中で、例えば hcRole という属性は「こういうところでしか入れてはいけない」というものがあれば、そのような使い方もできると思います。しかし、それがない場合、他の技術要件を満たしていても、認証局がhcRoleを設定する資格がないのに設定することが可能になってしまいます。その際、何のチェックもなく Adobe のソフトで検証ができてしまいます。しかも、その中からhcRoleというデータもアプリケーションで取り出せます。それを本当に信用できるのかどうかというチェックがないということになってしまうと、問題が発生する可能性があります。したがって、AATL を安易に使いやすいからと考えない方がいいかと思っています。
○西山構成員　おっしゃる通り、hcRole の検証部分はリーダーではサポートできないので、別の方法で確認をするということを補足的にやらなければいけないかもしれないですね。おっしゃる通りだと思います。
○宮崎構成員　すいません。hcRole が検証できるかできないかではなく、さまざまなアプリケーションで検証できたとしても、hcRole が本当に信用できるものかどうかは、厚生労働省のルート CA から発行されている証明書だから信用できるのであって、厚生労働省のルートかどうかということは別途検証する必要があります。AdobeのAATLで自動的に検証というだけでは済まないという状況は変わらないので、あまりそこは詰めて考えなくてもいいかなと少し思いました。
○松本座長　ありがとうございます。様々な論点が出てきたかと思います。単純に現状のルート CA やサブ CA の体制のままで暗号技術だけ変えるというやり方がありますが、この際、HPKI を健全にかつ持続可能な形で進めていくにあたって、改良してしまうほうが結局は得なのではないかというご意見が出てきたかと思います。アーキテクチャーまで変えるということになると、なおさら早く検討して更新を定めないといけないということと、

既存のアーキテクチャーで進んでいるものとの移行の話が必ず出てくると思いますので、その考慮なども必要だということで、これは結構楽しい作業になるのではないかということでございます。厚生労働省の方から何かご意見等ございますでしょうか。
○佐々木情報推進官　事務局でございます。いただいたご意見を踏まえまして、この後次回に向けて調査等行ってまいりますが、調査にあたって1点ご確認をさせていただきたいことがございます。今回お示しをさせていただきました、いわゆる GPKI と足並みを揃えるという形で、前提としてはECDSA（鍵長384ビット、192ビットセキュリティ）で一旦考えたうえで、今回ご意見をいただいたような、例えば電子処方箋の検証システムやHPKIタイムスタンプについても検討する。HPKIスタンプは少し独特で、電子処方箋の場合には支払い基金でタイムスタンプを打っているというところもありますので、支払い基金やさらには総務省にも確認をしていく中で、基本的には前提条件としましては ECDSA で一旦調査を始めてもよろしいでしょうか。
○松本座長　いかがでしょうか。私は違和感はありません。林さん、どうぞ。
○林構成員　私も違和感はありません。おそらく、何種類か理由を提示した方がいいと思います。まず、GPKI が移行のアルゴリズムを示しております。Cryptrec からも出ています。いくつかの諸条件を踏まえると、適正な選択なのではないかと思っている次第です。一旦以上です。
○松本座長　丸山さん。
○丸山構成員　丸山です。私も違和感ありませんが、GPKI がこれを選定したときの背景を一応確認しておいた方がいいかなと思いました。もし彼らにとって特別な要件があれば、それを除いて考えないといけないケースもあるかもしれないので。以上です。
○松本座長　それは事務局からデジタル庁の方にご確認をお願いいたします。
○矢野構成員　少し自由に話をさせてもらうと、仮に単一のルートにするとすれば、GPKI とブリッジの可能性も確認していただけないかなと思っています。応用としては、例えば主治医意見書については、提出先は自治体です。自治体がどこまで認証をブリッジしているかは分からないですが、今は自治体が検証をする際には HPKI で出している検証ソフトを使って検証しています。hcRole をどう扱うかという課題はあると思いますが、ブリッジができたら、もしかすると自治体の方から GPKI に聞き、そこのブリッジを通じて HPKI の確認をするなど、コストや開発に直結するようなところもあるかもしれませんので、可能性で結構ですので調査は加えていただきたいです。
○松本座長　よろしいですか。
○佐々木情報推進官　事務局でございます。承知いたしました。まずは GPKI で ECDSA を選定した理由の背景をデジタル庁に確認させていただきます。さらに、GPKI は現在ブリッジ認証局、相互認証局を持たれておりますが、我々もあまりそれがどのような使われ方をしているのか正確に把握できておりませんので、その点に関しましても合わせて調査を行います。HPKI でも使用の道があるのかどうか、さらにその先で相互認証させていた

だくためには、どのような手続きやコストがかかるのかどうかという点も合わせて調査をさせていただきたいと思います。
○松本座長　林さんどうぞ。
○林構成員　何度も申し訳ありません。林です。これは外から見える話ですが、実はデジタル庁の方で、令和5年12月に日本政府認証局の運営を開始しています。もしかすると、こちらとの整合も必要かもしれません。GPKI 担当の班になるので、問い合わせ先は変わらないかもしれないですが、その点を含みおきいただけると良いかと思います。特にGPKI は、私が認識している限りでは、現時点では官職証明しか出していません。そのような意味では、汎用性という点では、HPKI との整合はもう少し幅広にご紹介をいただいた方が先方もお返事しやすいかと思いました。以上です。
○松本座長　ありがとうございます。宮内さん。
○宮内構成員　皆さんおっしゃる通りだと思っています。政府の中で CVS（Certificate verification System）を使って検証する際に、GPKI のブリッジ認証局を介した相互認証もきちんとチェックしてくれると聞いています。ですから、HPKI が仮に GPKI のブリッジCA と相互認証すれば、CVS で自動的に見られるようになるはずです。先程お話がありました、地方自治体が CVS とどのような関係になっているのか私は全然存じていないので、そのような点も含めて確認していただければと思っております。はい。以上です。
○松本座長　LGPKI は GPKI とどのような関係にあるのですか。
○宮内構成員　相互認証されていますね。
○松本座長　相互認証ですよね。
○宮内構成員　そうです。LGPKI の関係システムで CVS を使っていれば、おそらく相互認証可能だと思いますが、地方自治体の検証環境との関係がどうなっているのか確認していただきたいと思っています。
○松本座長　ありがとうございます。よろしいですか。それでは、たくさんのご意見、ご質問が出て良い議論ができたのではないかと思いますが。つまり、線表を引くにあたって、いろいろ前提とすべきところや制約条件などもたくさんあるということが分かってきました。それから、HPKI であるがゆえに挙がってくる事項も確かにあるということが確認できたかと思います。事務局の皆さまには今日の議論を整理していただき、次回に向けて準備を始めていただければと思います。よろしいでしょうか。それではこの議題につきましては終了ということにさせていただきまして、最後に事務局より連絡事項はございますでしょうか。

（3）連絡事項
○佐々木情報推進官　ありがとうございます。それでは、最後に連絡事項について事務局よりご説明差し上げたいと思います。11 頁目をお願いいたします。次回 32 回の HPKI 専門家会議についてでございます。年度が変わりまして、2025 年の 5 月頃に開催をさせてい

ただければと思いますので、また追って日時は調整をさせていただきます。議題案としましては、本日お話をさせていただきました暗号アルゴリズムの移行につきまして、まずは調査を進めてまいります。この段階で調査が完了した部分に関しましては、お示しをさせていただきながら、引き続きご議論をさせていただければと思っております。また、この2月に日本医師会認証局に続きまして、MEDIS 認証局におかれましても、同様に鍵更新がございますので、そちらの内容も同様にご報告させていただく予定となっております。また、来年度からは構成員を一名追加させていただきたいと思っております。松本先生よりご推薦いただいておりまして、次回より明治大学の菊池先生にも、専門家会議構成員としてご参加をいただく予定となっておりますのでよろしくお願いいたします。続いて 12 頁目をお願いいたします。本専門家会議でございますが、構成員の任期としては2年となっております。現体制になってから、次の6月でちょうど2年となっております。専門家会議構成員の皆様におかれましては、改めて継続可否について、個別に意思確認をさせていただきたいと思っております。これまではリモート署名サービスの基準作成等もあり、毎回作業班との合同開催とさせていただきましたが、任期更新のタイミングで、一旦体制を少し整備させていただきます。次次回以降、合同開催ではなく、専門家会議単独での開催を基本とさせていただければと思っております。内容によりけりにはなりますが、作業班会議は別で設けさせていただき、必要に応じて招集をさせていただければと思います。一方で、現在毎回合同開催をさせていただき、質の高い議論をさせていただいている次第でございますので、その点は引き続きできる体制を取ってまいりたく、7月以降、下記の通り、構成員の皆様の追加をさせていただければと思っております。具体的には、現在作業班に入っていただいている丸山先生、六川先生、宮崎先生には HPKI 専門家会議構成員として、引き続きのご参加をいただければと思っております。また、JIPDEC 様にも1名選出いただけないか現在ご相談をさせていただいており、調整中でございます。また、これまで日本医師会認証局、日本薬剤師会認証局、MEDIS 認証局につきましては、作業班という形でのご参加をいただいていたのですが、7月以降に関しましては、オブザーバーとして引き続き専門家会議にはご参加をいただく形とさせていただければと思っております。事務局からの連絡事項としましては、以上になります。

○松本座長　はい、ありがとうございました。今のご連絡事項につきまして、何かご質問ありますでしょうか。大丈夫でしょうか。それでは、今日は実に中身が濃いのですが、時間的には 12 時までかからず終えることができそうです。皆様どうもありがとうございました。本日はこれで閉会とさせていただきます。リモートの方もありがとうございました。失礼いたします。

以上