第３４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９月２５日(木) １３：００～

場所 AP 新橋　Ｄ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34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、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。本日の会議の構成員の参加状況ですが、菊池構成員がご欠席、佐古構成員、濱口構成員、林構成員がオンラインでの参加となっています。その他の構成員の皆様方は現地参加となっています。

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します。

次に資料の確認をさせていただきます。本日の資料は、議事次第、資料１、資料２－１、資料２－２、資料３、参考資料１から５、前回の HPKI 専門家会議の議事録を用意しています。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、こんにちは。よろしくお願いします。本日の議題は、（１）MEDIS 準拠性審査結果報告、（２）暗号アルゴリズムの移行に関して、（３）リモート署名サービスの活用に関して、（４）連絡事項となっています。

それでは議題（１）MEDIS 準拠性審査結果報告からご説明をお願いします。

議事

（１）MEDIS 準拠性審査結果報告

○河内主査　厚生労働省事務局です。資料１に沿って MEDIS 準拠性審査結果報告についてご説明します。資料１の３頁をお願いします。HPKI 専門家会議にて行う準拠性審査に関して、今回は一般財団法人 医療情報システム開発センター（MEDIS）を対象に、認証局としての更新申請及びリモート署名サービスとしての更新申請、双方を対象に準拠性審査が実施されたので、ご報告します。

まず認証局の審査についてです。審査対象は認証局の MEDIS であり、最新の保健医療福祉分野 PKI 認証局 署名用証明書ポリシ及び保健医療福祉分野 PKI 認証局 認証用（人）証明書ポリシへの準拠状況が審査の対象項目でした。申請区分としては更新申請であり、昨月８月４日に丸山構成員と六川構成員に審査を実施いただきました。

４頁をお願いします。審査方法は例年どおり書類審査と実地調査にて行われました。書類審査では MEDIS から提出された認証管理規程や監査報告書などを基に確認し、実地調査では代表者インタビュー、運用手順や教育訓練の確認を行い、またデータセンターに赴

き、人的・物理セキュリティの実地確認を行いました。

前回、２年前の準拠性審査からの変更点としては、マイナポータルからの HPKI の申請受付を開始したことに伴う変更があり、また軽微な点ですが、厚生労働省の問い合わせ先変更に伴うドキュメントの整備が行われていました。また、インシデント発生状況の確認も行われ、２年前から大きな問題はなく、適切に対応されていることが説明されました。

次に、５頁にて、同日に実施されたリモート署名サービスに関する MEDIS のトラストサービスプロバイダーとしての準拠性審査についてご説明します。トラストサービスプロバイダー MEDIS を対象に、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（鍵管理（署名値生成）サービス)、及び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（デジタル署名サービス）の双方への準拠状況を審査の対象項目として、申請区分は更新申請として審査が行われました。認証局審査と同日の８月４日に、同じく丸山構成員と六川構成員に審査を実施いただきました。

６頁をお願いします。書類審査では運用規程や監査報告書、利用規約に加え、リモート署名サービスで用いられるクラウド管理元である AWS（Amazon Web Services）から提出された SOC レポートなどを確認しました。実地調査では代表者インタビュー、運用手順や教育訓練の状況が確認されましたが、AWS の実地確認は現実的に困難であることから、AWS から提出された SOC レポート、いわゆる監査報告書を基に、問題なく AWS 側で運用されることを、実地調査に代えて確認を行いました。

リモート署名サービスの２年前からの主な変更点としては、リモート署名サービスを有償化したことに伴う利用規約等の変更がありました。また、インシデントの発生状況の確認も行われ、２年前から大きな問題はなく、適切に対応されていることが説明されました。

７頁にて、MEDIS の準拠性審査の結果をご報告します。認証局として、HPKI の署名用証明書ポリシ、認証用（人）証明書ポリシにおいて、適合していることが確認されました。また、トラストサービスプロバイダーとして、保健医療福祉分野におけるリモート署名サービス評価基準の鍵管理（署名値生成）サービス、及びデジタル署名サービスにおいて、適合していることが確認されました。

８頁をお願いします。今回、準拠性審査に当たっては丸山構成員、六川構成員に審査班用チェックリストをご活用いただきました。こちらは前回の専門家会議で活用が承認されたもので、実際に活用するにあたって、ポリシや評価基準等との齟齬はなく、見直しを要する点はなかったことをご報告します。一方で、形式面など今後さらにブラッシュアップする余地もあるため、審査班用チェックリストの運用方法に合わせて、引き続き事務局で検討を進めたいと思います。

MEDIS準拠性審査結果報告に関して、事務局からのご説明は以上です。続いて審査班長を務めていただいた丸山構成員から詳細な結果報告、補足があればコメントをお願いします。

〇丸山構成員　先ほど説明いただいたとおり８月４日に MEDIS に伺い、全般の実地調査

を行いました。その後データセンターに行き、実際の運用状況について、インタビューや現場の確認を含めて実地調査を行いました。資料２－１と２－２にて、審査結果や、どのようなことを行ったかをコメント欄に記載しています。今回の審査は認証局及びトラストサービスプロバイダーの両方とも適合との結論としています。先ほど説明があったように、前回の審査からの変更点を中心に確認させていただきました。以上です。
○松本座長　河内主査及び丸山構成員、どうもありがとうございました。それでは、ただいまの２件の準拠性審査結果についてご質問などはありますか。
○宮内構成員　今回の審査について問題を感じているわけではありませんが、前回の審査から話があるように、現在行われているリモート署名のシステムと、リモート署名サービス評価基準の監査報告書様式の項目が必ずしも合っていません。例えばリモート署名サービス評価基準の監査報告書様式では、基本的には署名鍵を暗号化して保存し、それを復号して使うやり方をしていて、それを前提とした管理について書いてあるのです。一方で、今使っているシステムは鍵分散でやっているので、リモート署名サービス評価基準とぴったり合っているわけではありません。このように少し違うシステムに対応するためには評価基準を拡充するなり改めるなりしなければいけないということは、去年から出ている話だと思います。この辺りの今後の進め方について事務局はどのように考えているか、説明していただけますか。
○河内主査　ありがとうございます。ご指摘のとおり、現在のリモート署名サービスの評価基準は必ずしも分散鍵に合致したものではないと事務局も認識しています。各種 HPKI のドキュメント整備を予定しているので、その際に分散鍵方式も含めたリモート署名サービスの評価基準にするのかどうか、また検討させていただければと思います。その際はご協議いただきたく、よろしくお願いします。
○宮内構成員　ぜひしっかりやっていただきたいと思います。これはそもそもシステムと評価基準が合っていないので、丸山構成員と六川構成員には大変ご苦労をかけていると認識しています。素直に審査できるように評価基準や附属の監査報告書様式などはきちんと整備していく必要があると思いますので、ぜひよろしくお願いします。
○河内主査　ありがとうございます。
○松本座長　重要なご指摘をありがとうございました。他にありますか。
○佐古構成員　前回会議で、責任者にヒアリングするという項目について議論されたのは、今回の審査の内容で正しいでしょうか。
○河内主査　ご質問ありがとうございます。代表者インタビューのことだと思います。こちらについては MEDIS の山本理事長にご対応いただいています。
○佐古構成員　責任者がどう考えていたかについて報告はありますか。
○河内主査　ありがとうございます。資料２－１と２－２の中で代表者インタビューについて、どのような内容を確認したか、またそれに対しての適合をチェックさせていただいています。

〇佐古構成員　後でまた説明があるのでしょうか。
〇河内主査　資料２－１と２－２の実地調査の代表者インタビューについて、表形式でまとまっていますので、資料をご確認ください。具体的に申し上げると、代表者インタビューの評価項目として、資料２－１では「組織概要/業務内容/経営方針」、「認証局申請のきっかけ」、「認証局管理者・監査責任者の任命プロセス、任命記録の確認」、「マネジメントレビュー（組織のガバナンス体制）」について、また資料２－２では「組織概要/業務内容/経営方針」、「TSP 申請のきっかけ」、「TSP 管理者・監査責任者の任命プロセス、任命記録の確認」、「マネジメントレビュー（組織のガバナンス体制）」について、それぞれチェック項目を設けて審査し、適合を確認しています。
〇佐古構成員　では、そちらを拝見します。ありがとうございます。
〇松本座長　よろしいですか。他になければ次の議題に進みたいと思います。

（２）暗号アルゴリズムの移行に関して
〇松本座長　議題（２）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します。
〇岡嶋主査　事務局より暗号アルゴリズムの移行について概要をご説明します。資料１の 10 頁をご確認ください。
まず、前回の専門家会議の振り返りからご説明します。前回の専門家会議において、次期暗号移行に向けたスケジュール感や、検討すべき事項に関して議論いただきました。移行に向けた具体的なスケジュールについては、引き続き本専門家会議において議論を行うこととなっています。耐量子計算機暗号（PQC）については、松本座長より政府機関等における PQC 利用の検討状況についてご説明いただき、それを踏まえて議論いただきました。
11 頁をお願いします。本日の議論のポイントについてご説明します。前々回の第 32 回 HPKI 専門家会議にて整理した調査項目や検討すべき事項に関して、関係者への調査結果が出そろったため、今回はそちらを報告いたします。また、次期暗号移行に向けたスケジュール案についても事務局で検討しているので、ご説明します。本日は、これらの調査結果等を踏まえ、予定する次期暗号化方式への移行に関して、関連システムの対応や、そのスケジュール感について議論いただきたいと考えています。最後に、本日の議論を踏まえ、HPKI で採用する次期暗号化方式について承認いただきたいと考えています。
それでは暗号移行に関する関係者への調査結果の報告に移ります。前回の第 33 回 HPKI 専門家会議にて中間報告としてご説明したため、アップデートがあった箇所を中心にご説明します。12 頁から 14 頁は、各認証局からの回答となります。今回、日本医師会から新たにご回答いただき、認証局３局からの回答が出そろいました。日本医師会認証局からは、前回報告した日本薬剤師会、MEDIS と概ね同様の回答をいただきましたが、他調査先とは共通しない、日本医師会のみからいただいたご意見を赤字で示しています。

赤字部分についてご説明します。証明書発行プロセス等への影響として、新暗号方式での証明書発行のパフォーマンス検証が改めて必要であること、電子証明書発行のための情報（発行要求のための CSV 等）の様式に変更があればシステム改修が必要であることをお示しいただきました。また、鍵生成及び鍵管理への影響として、別途新しく認証局を構築することによって鍵生成や鍵管理に係る手順に影響はないこと、また HPKI カードへの影響として、CC（Common Criteria）認証の新規取得をする必要があるかについては本専門家会議で今後議論していく必要があることをお示しいただき、日本薬剤師会、MEDIS とも横並びで協議が必要であることをご提示いただいています。日本医師会から新たな観点でお示しいただいた内容は、以上となります。

日本薬剤師会、MEDIS からの回答内容については前回の再掲であり、お時間の関係上、改めての説明は省略します。

15 頁をお願いします。署名者の立場、検証者の立場からの回答結果をご報告します。これらは一般社団法人保健医療福祉情報システム工業会（JAHIS）を介して医療機関のシステムベンダーにご回答いただきました。

まず署名者側の調査結果の報告です。署名プロセスに係る影響として、署名モジュールの更新・入れ替えが必要となる可能性があること、また当該方針によって想定される影響を複数お示しいただきました。

システムに係る影響としては、新暗号化方式に切り替えるタイミングは病院側と薬局側で合わせる必要があること、データ互換性の観点から、電子処方箋署名共通モジュールは新旧両方の方式に対応できる必要があること、新暗号化方式の移行に際して H/W リソースの増強が必要となった場合、また新しい電子処方箋署名共通モジュールの開発が必要となった場合に、システムの価格に影響すること、異なるベンダーで作成された暗号システムで、どの組み合わせでも署名・検証が問題なく処理できるかの確認及び検証に時間を要すること、などのご指摘いただいています。

16 頁をお願いします。続いて検証者側の報告に移ります。まず検証プロセスに係る影響として、電子処方箋管理サービス・電子カルテ情報共有サービスにおいて、タイムスタンプアルゴリズム（TSA）の証明書に用いられる暗号方式を新暗号に対応させられるかの懸念があること、TSA 側の新旧証明書が混在する期間において、新旧暗号を正しく判別し適切に検証するための検証モジュールが必要であることをご指摘いただいています。リモート署名システムの対応方針や電子署名モジュールの仕様によっては、HPKI を用いたシステムとして次期暗号方式への互換性の問題が発生する可能性や、ユーザーの業務プロセスに影響する可能性の指摘をいただいています。

関係者からのヒアリング結果について、前回からのアップデート事項のサマリーは、以上となります。

次に、19 頁に調査状況を踏まえた留意点を事務局で整理した資料を用意しています。大きなカテゴリーとして、技術面、移行計画、コスト面の 3 つに分類しています。

まず技術面においては、特にリモート署名サービスにおいて、ECDSA を用いることの安全性及び性能面を検証し、新暗号アルゴリズムに追従可能であることを確認する必要があることを挙げています。MEDIS からは「ECDSA への対応は問題なく可能と考えているが、年内をめどに方向性を策定できるようにしたい」と伺っており、引き続き MEDIS の山本理事長とも連携を取りながら、進めたいと考えています。

移行計画について、検証環境の観点では、医療機関向けの検証環境の準備、また検証期間を考慮した移行計画の必要性についてご指摘をいただいています。関係システムの開発に関しても、HPKI カードやドライバの開発期間を考慮したタイムラインを策定することや、電子署名共通モジュールの新暗号方式対応について、開発ベンダーへ開発及びリリースに係る期間を確認のうえ移行計画を策定する必要がある、とのご指摘をいただいています。並行運用期間についても、移行後 5 年間の新旧証明書の検証可能な体制の確保、新暗号方式への切替タイミングの考慮、周知の必要性などの留意点を挙げているところです。

コスト面について、新暗号方式への移行に際して、H/W リソースの増強や電子処方箋署名共通モジュールの新開発によって、システム価格は現行より増大する可能性がある点に留意が必要であると考えています。

20 頁をお願いします。次期暗号移行に向けたスケジュールについて、ルート認証局部分のタイムラインをお示ししています。次期ルート認証局の構築に当たっては、早ければ今年度末には調達手続を開始し、2026 年度、遅くとも第 1 四半期中にはベンダーとの契約、設計開発を開始したいと考えています。2027、2028 年度にテスト運用を実施し、2029 年度にはサブ認証局との接続テストなどを実施するための切替期間を設け、2030 年 1 月には本格運用を始められるようにしたいと考えています。サブ認証局、またその他後続システムのタイムラインについては、関係者との調整を踏まえて改めてお示ししたいと考えています。

21 頁をお願いします。これまでの議論や調査結果を踏まえ、HPKI の次期暗号化方式は、調査を進めてきた ECDSA P-384 with SHA384 として移行を進めていくことについて、本会議にてご承認いただきたいと考えています。

この暗号方式の選定理由として 6 つ記しています。上の 3 つは一般的な点ですが、CRYPTREC 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準に適合する暗号化方式に変更する必要があること、現行の RSA でこのまま暗号強度を上げる場合、鍵長が現状より長くなってしまい、現状の IC チップの処理能力を踏まえると、署名時の処理計算の負荷が大きくなり運用に支障をきたすおそれがあること、ECDSA を採用することで、RSA と比べて短い鍵長で IC カード等の処理性能・運用負荷を抑えつつ十分な暗号強度を保てること、を挙げています。

4 点目として、これまでの関係者への調査を通じた影響確認結果を踏まえ、課題は何点かありつつも、移行を断念せざるを得ないほどの大きな課題はないと認識しています。また、5 点目として、本暗号方式の採用により、政府系の他の PKI 基盤である GPKI が本暗

号方式を採用し準備を進めているため、足並みをそろえることが可能となります。
　なお、６点目として、前回の中間報告及び今回の最終報告を通じて明らかとなった要検討事項については、引き続き事務局で検討の上、必要に応じて専門家会議にご報告、お諮りしたいと考えています。議題（２）に関して事務局からの説明は以上です。
○松本座長　ご説明をありがとうございました。それでは、議題（２）に関してご意見ご質問等をいただければと思いますが、いかがですか。柴田構成員。
○柴田構成員　次期暗号方式について、技術面において問題がないことはそれとなく分かりました。19 頁の一番下に小さく「コスト面」と書いてありますが、現段階では暗号方式が確定していないので、現場側もしくはベンダー側がコスト的にきちんと実行できるかどうかの確認まではできないでしょうが、大まかな返事は聞いているのではないかと思います。現行の暗号方式でも現場のコストが高すぎて導入しにくいと言われている医療機関も多いので、コスト面の見込みについてぜひお聞かせください。
○岡嶋主査　柴田構成員の疑問は、事務局も持っているところです。現状、ベンダーに協力を依頼していますが、しっかりと決まったものがないと見積もりを出せないベンダーが多く、事務局としても規模感をつかみきれていません。どこかのタイミングでお示ししたいとは思いますが、現状は持ち合わせていないというのが回答となります。申し訳ありません。
○柴田構成員　ありがとうございます。現実味を持たない金額になるようであれば、実際に社会実装には至らないといいますか、ベンダーはビジネスにならない仕事はやりませんから、そうなると現場に届かないことになります。より詳細にコスト面の見込みを調べていただけると、安心して承認できるのではないかと思います。
○松本座長　どうぞ、横田構成員。
○横田構成員　おそらくコスト面はカードの部分もあるでしょうし、当然ながら医療機関や薬局の負担もあります。ベンダー側の改修を行うとはいえ、それが末端まで影響してくることはナンセンスなことだと思います。
　電子処方箋をはじめ、このような医療基盤が定着していくのは、使いやすさやコスト面の負担が大きくないことが一番のメリットであり、お金を出すところをまとめることによって、末端の受益者まで影響しない方法もあるのではないかと思います。19 頁のコスト面については、資料の記載内容以外にも留意点があるのではないかと思いますので、その辺りのご検討もぜひよろしくお願いします。以上です。
○岡嶋主査　承知しました。
○松本座長　林構成員、どうぞ。
○林構成員　21 頁について、選定理由については全く異論ありませんが、暗黙のうちに抜け落ちている、CRYPTREC のそもそもの策定の資料を踏まえて、という点は記載しておいたほうがより良いのではないかと思います。以上です。
○松本座長　林構成員、ご指摘の件は ECDSA を用いること自体についてですか。

○林構成員　それもありますし、そもそも移行のプロセスを踏まえてというところが、資料にほぼ出てきていないことが気になっています。きちんとそれを踏まえて実施していくということを、政策的にも打ち出しておく必要があるかと思います。
○松本座長　そもそもなぜ移行するのか、その根拠に結びつく話ですか。
○林構成員　おっしゃるとおりです。さらにその中でも議論されている資料を踏まえた結果、ECDSA P-384 with SHA384 を選んだという理由になるのかなと思いました。
○松本座長　そのとおりかと思います。他にありますか。山内構成員、どうぞ。
○山内構成員　JIPDEC の山内です。事務局はよくまとめていただいてありがとうございます。
12 頁の日本医師会からの調査結果で、「CC 認証の新規取得要否は、HPKI 専門家会議で議論する必要あり。HPKI で共通のカードとなることから日薬様、MEDIS 様とも協議が必要。」という部分は、お金がかかる話なので、結構重たい議論という気もしています。私ども HPKI 専門家会議で議論する必要があれば当然すればいいと思いますが、この辺りの方針について、事務局として、日本医師会、日本薬剤師会、MEDIS との間で、何か腹案をお持ちなのでしょうか。
○岡嶋主査　ありがとうございます。ご質問の CC 認証について、HPKI のポリシにおいて、どのような形で準拠してカードを発行していくかは既に定めており、改めて CC 認証を取る必要はないと考えています。その認識で良いかについては認証局ともよく協議したうえで、最終的な判断をしたいと思います。
○山内構成員　HPKI 専門家会議で議論する場合、議論に必要な情報や、関係者のご意見などをとりまとめた資料を作っていただければと思います。よろしくお願いします。以上です。
○岡嶋主査　承知いたしました。
○松本座長　今話していた、日本医師会からのコメントについて、HPKI カードが新しい暗号方式に対応した場合、CC 認証を取る必要があるのかどうかの議論をするにあたり、現状の HPKI カードは IC カードとしての CC 認証を取っているのか、それと新暗号方式に対応した場合との差分を整理する必要があると思いました。まず前提として現状のカードはどのようにセキュリティを担保しているのでしょうか。
○矢野オブザーバー　では私からご説明します。「CC 認証は必要と考えるか」については、基本的には必要ないと思いつつ、HPKI 専門家会議でご議論いただきたいというのが素直な回答です。
理由としては、現状の HPKI の IC カードは、HPKI 証明書ポリシの 6.2.1「暗号モジュールの標準及び管理」で、セキュリティに関しては「FIPS 140-2 レベル 1 と同等以上」と書いてあり、それであればポリシの改定で CC 認証を取得する必要があるなどということを書くのかなと思ったので、専門家会議でのご議論が必要との回答をさせていただきました。

○松本座長　そういう状況ですか。分かりました。要するにICカードでデジタル署名をする機能があるので、そこに収められている秘密の署名生成鍵がきちんと保護されていること、また、その署名生成鍵を使った署名生成処理などがきちんと行われることが第三者によって評価され、認証されていることが望ましいが、そのような機能を持っているICカードが全て認証を取っているわけではなく、ただしマイナンバーカードや電子パスポートなどの重要なものについては CC 認証を取っているということですね。日本では JISEC（IT セキュリティ評価及び認証制度）と言われるものであり、IPA（独立行政法人情報処理推進機構）が認証機関になっているものです。ただ、正確に言えば、JISEC の認証でなくても CC 認証はたくさんありますので、他の国で取った認証を使っているケースもあります。また銀行のカードやクレジットカードなどは、その業界や金融機関で定めた基準を満たしていればよいということで、公的な認証を取っているものとは限らず、プライベートな認証や評価をしています。　要するに、IC カードを発行して使ってもらっている側が、アタックされては自分が困るので、困らない状況を作り出しているのです。

HPKIカードに関しては、HPKIを出している側、責任ある立場の組織がどう考えるかという話になります。要するに、例えば医療従事者ではない方が偽って署名を生成することができては困るので、そうならないためにはいろいろな仕掛けが必要であり、その一番重要なところは HPKI カードであるということだと思います。現状はどうなっていますか。CC認証は取っていないですか。

○矢野オブザーバー　取っていません。

○松本座長　それから先ほどの「FIPS 140-2 レベル 1 と同等以上」というのは、セキュリティの専門家から見ると、ほとんど何もないのに等しいです。ただ暗号アルゴリズムが正しく相互に通信ができる形で実装されていることは確認できているという程度でしょうか。

ですから、現行と同じ程度の信用ができるカードであればよいとすれば、必ずしも CC 認証は必要とされない状況かもしれませんが、今後それでよいのかという議論は必要であると思います。

それでは、濱口構成員、お願いします。

○濱口構成員　慶應義塾大学 SFC の濱口です。CC 認証について少し発言させていただきます。HPKI カードについて、手元のローカル環境のみで CC 認証を取得したとして、かなり厳しいセキュアな環境を用意することが、全体の認証局のポリシ、これはリモート署名サービスの評価基準も共通ですが、統一的な水準になっているのかどうかは、改めて考える必要があるかと思います。

手元だけすごくセキュアな運用をしても、例えばリモートの鍵の管理の方法に関してはセキュリティレベルが低いと、全体のセキュリティのレベルとしては一番低いところで見るというのが、セキュリティの考え方であると思います。セキュリティのレベルが下がってしまっているのに、手元の運用方法だけ、すごくコストが上がってしまうことになります。セキュリティとしては全体として統一感のあるものにして使いやすいシステムにして

いくのか、あるいは全体のセキュリティのレベルを上げてきちんとしたシステムを作っていくのかというのは、専門家会議で検討し、方針を決めていく必要があ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。宮崎構成員、どうぞ。
○宮崎構成員　JDTF（一般社団法人デジタルトラスト協議会）の宮崎です。20 頁のスケジュールは、リモート署名用、セカンド鍵用の認証局もこのスケジュールで進めるということだと思います。そうなるとリモート署名でも 2034 年末までは RSA で署名を生成しなくてはいけない可能性が出てくるので、留意点の中にも、そういったことを含めておいたほうがよいのではないかと思いました。コスト面にも大きく影響してくると思うので、しっかり意識しておく必要があると思いました。
○松本座長　そのとおりだと思います。その他ありますか。
　佐古構成員、どうぞ。
○佐古構成員　スケジュールとしては今、宮崎構成員がおっしゃったとおり、全体をどのようにローテートして移行していくかについて、検討が必要であると思います。同時に暗号の危殆化というのはこれからも考えられます。他にもマイナンバーカードなど政府が税金を使って国民に配っているシステムがありながら、HPKI だけ独自にまたコストをかけて類似のものを作ることは、コスト面での負担も大変になると思います。その辺りの全体構想といいますか、政府全体として何をやっているかということと、うまくコストバランスを取っていくことが重要ではないかと思います。私たちが与えられた任務の中で適切に安全性を保っていこうとするとコストがかかるので、他の省庁と足並みをそろえて、うまく相乗りができる形のグランドデザインを考えるのが重要ではないか、という提案です。
○松本座長　ありがとうございます。
　この議題は「暗号アルゴリズムを何がしかのものにしてよいか」という問いかけに対し、どう答えるかという話なので、その観点で申し上げます。19 頁の留意点の整理において、技術面で「安全性等の検証」とあります。リモート署名サービスにおいては、カードでの署名をするものと、署名生成においては違う仕掛けを取るのかどうかというのが質問です。
　18 頁の一番上の行に「現在の分散鍵による署名は RSA のみ対応しており、ECDSA での実装方式や安全性・性能等の評価は検討段階」とあります。要するに生成された署名は、リモート署名でもローカル署名でも同じ形式を取っていないといけなくて、どちらで生成された署名でも検証は同じようにできるようになっていないといけない、という条件があると思います。
　ECDSA を使ってリモートで署名をするということは、リモートのクラウドサーバにたくさんの個別の署名生成鍵を預けてしまうことになります。署名生成鍵が集中すると漏えいが非常に怖いので、現行は分散しているスタイルを取っているわけです。それに対して ECDSA ではどのようにするのかがはっきりしなければ、このアルゴリズム、署名方式を選んでよいかどうか判断ができないのではないでしょうか。したがって、まだ検討段階と

いうことではなかなか納得しにくいのではないかと思います。

そこで現状の検討はどこまで進んでいるのか、見通しなどについて、山本オブザーバーにご発言いただければと思います。

○山本オブザーバー　現状の検討の状況としては、リモート署名が ECDSA P-384 でできることは確認しています。ただし 18 頁に書かれているように現在の鍵の秘密分散の方式は Colin Boyd の論文によるもので、これは RSA に依存した分散方式を取っていて、この方式が使えません。そこで、一つは CloudHSM（Cloud Hardware Security Module）を使って HSM（Hardware Security Module）に秘密鍵を保存する方法があります。もう一つは、Colin Boyd の方式ではなく、例えばシャミアの閾値法など、MPC（Multi-Party Computation）が可能な秘密分散に切り替える、その両方を検討しています。コスト的には圧倒的に秘密分散を使うほうが安いですが、HSM を使うほうが先生方には納得を得られやすいと思います。

現状 CloudHSM は、いわゆる製品の HSM と違って格納鍵数が限られています。AWS の場合、1 インスタンス当たり格納鍵数が 3,000 程度なのです。今でも 3 万や 4 万の秘密鍵を預かっているので、3,000 の秘密鍵を預かると 10 インスタンス以上必要になります。クラウド使用料は、インスタンス単位、時間単位で請求されます。発行局の私有鍵の HSM と違い、エンドエンティティの HSM は常に使われることから、ずっと HSM をつけたままにしないといません。24 時間借りていて、なおかつ数十インスタンスの HSM のクラウド料を払い続けるとなると、相当なコストになるのではないかと思います。その辺りの運用上の課題を検討しています。

秘密分散で MPC を使った方法も、リモート署名ができることは確認しています。シャミアの閾値法を使った方法について、閾値設定を（2， 3）とした場合、MPC により署名値の生成が可能であった、つまり 1 回も鍵を見ない、鍵を再合成しない状態で署名値を生成できることは確認しています。これが現状です。

○松本座長　ありがとうございます。先ほどコスト的にはどちらが圧倒的に低いとおっしゃいましたか。

○山本オブザーバー　秘密分散で MPC を使うほうが圧倒的に低いです。

○松本座長　分かりました。もう一つは、HSM を使うというのは結局、分散しない方式のことを指しているのですか。

○山本オブザーバー　分散鍵を HSM に保存することも方式としては考えていますが、利用できる HSM が MPC に対応できているかどうかまだ不明なところがあり、現在調査中です。単に秘密鍵をそのまま HSM に格納するのであれば、ECDSA P-384 が十分に対応できていることは確認できていますが、秘密分散して MPC でやることに対応している HSM があるか確認中です。分散して HSM に格納する場合、さらに 3 倍の HSM が必要になり、コストは跳ね上がると思います。

○松本座長　先ほどの私の質問について、山本オブザーバーが MPC とおっしゃっている

のは、Multi-Party Computation、別の言葉では秘密計算あるいは秘匿計算と言われているものであり、秘密の情報に基づく計算をするのにあたって、その情報をそのまま扱うのではなく、分散するということです。要するに元のデータではない、分散されたものだけを見ても何だか分からないというもので、元のデータが途中で一切現れることなく最後まで計算する、この場合は署名生成処理をそのような形で行える方式のことです。HSM というのはセキュアなコンピューターであって、そこから署名生成鍵が漏れることがないと期待されるもののことを言っています。しかし、一旦それが攻撃により漏れてしまった時の被害が大きいので、HSM に頼って大丈夫かという判断が必要だと思います。

MPC とおっしゃったほうが分散方式で、そちらはクラウドの HSM は使わない想定でコストの話をされたのだと理解しました。採用する方式をいつどのようにどう判断するのかについて、見通しはありますか。

○山本オブザーバー　おそらく今年中にはコストの試算はできると思います。コストがかかった場合にどうするかについては、何とも言いようがない話です。ECDSA P-384 に切り替えても、リモート署名が対応できるという意味では対応できます。ただ、それが現実的なコストで対応できるかどうかが問題になります。現状、有償化してユーザーにご負担いただいており、１施設当たり１年間使い放題のサブスクリプションで、薬局等は年間１万円ですから、それほどご負担なくお使いいただいています。今行われている状況では、週に 60 万署名です。現状の値段ではとても維持できない可能性があり、いろいろな意味で考えなければいけないことがありますので、コストの試算の上で結論を出せるのは、まだ先になります。

しかし RSA2048 ではやっていけないことは間違いありませんので、ECDSA P-384 を前提に実現可能なことを考えていかなければいけません。また準拠性審査等で難しい判断をお願いすることになるかもしれませんが、秘密分散と秘匿計算をあわせた方式で実装させていただければ、ほとんどコストを増やさずに対応できると思います。

○松本座長　大変詳しいお話をありがとうございます。秘密分散の方式を取る場合、それは具体的にどのような方式なのか、その検証もしないといけないと思いますので、しっかり進めていただければと思います。HSM を採用する場合、そこが鉄壁だと仮定すればコストはかかっても許容できると思いますが、万一そこがアタックされて、たくさん預かっている鍵が漏えいしてしまったら、非常に大きな問題になります。そのリスクをどのように考えるかということがあるので、単に実装やコストの問題ではないのではないかなと思いますが、皆様、いかがでしょうか。柴田構成員、どうぞ。

○柴田構成員　おそらく HPKI の署名の用途範囲が今後どの時期までに何が増えていくかによってボリュームも変わってくるし、当然かかるコストも変わるし、実際に漏えいした時の被害範囲も広がることが想定されます。現状の電子署名の使われ方を想定したまま、スケジュールや技術の検証、それから実際に採用された場合のコスト検証がなされているのではないかと思いますが、おそらく用途範囲は拡張する方向で検討しているはずなので、

それも含めて事務局の見解を聞いてみたいと思います。
○岡嶋主査　現状、HPKI の署名の用途は電子処方箋のみに限定されていると認識しています。
○新畑室長　厚生労働省医政局医療情報室長の新畑です。全体的に今後どこまで広がりを見せるかというところは検討が必要かと思いますが、それも踏まえてどこまでコストをかけることができるか、この場ではおそらく結論が出ないと思うので、引き続き皆様のご意見を聞きながら検討していきたいと思います。
○松本座長　山本オブザーバー、どうぞ。
○山本オブザーバー　HPKI の署名の用途を拡張するという議論は既にあります。やはりDX の時代で、電子化されたドキュメントに対して職種を明確にして責任を明確にするという意味では、HPKI が望ましいことは間違いないと思います。
　一方で、処方箋というのは圧倒的に数が多く、それ以外はそれほど多くありません。例えば死亡診断書や診療情報提供書に電子署名をしても、処方箋に比べれば数は 100 分の 1 程度しかないと思いますので、処方箋を前提として動いていれば、用途が増えたからコストが増えるということは、あまりないのではないかと思います。電子処方箋が順調に成長し普及していく前提で話をすると、それに対応できれば、もし用途が広がっても、それほど大きな問題はないのではないかと思います。
○松本座長　柴田構成員は、その回答でよろしいですか。
○柴田構成員　署名対象によってセキュリティ強度の考え方は変わってくるのではないかと思いますが、現状、対象が明確ではないので質問は控えます。
○松本座長　宮崎構成員、どうぞ。
○宮崎構成員　今の議論で少し注意しておくべき点があると思います。例えば分散署名の場合と HSM を使う場合、鍵の漏えいの観点からは HSM のほうが断然強度が高く安全です。ただし、鍵の漏えいも重大なインシデントなので、防がなくてはいけない面はあると思いますが、リモート署名の場合は認証した上で署名を生成するので、認証を突破すると、悪意を持った他人が署名生成できてしまいます。それは HSM を使おうが、分散署名を使おうが同じなのです。その辺りは区別して考える必要があると思います。HSM にすればどちらも完全に安全だというわけではないというのは、一つ重要なところです。
　また今回、署名は必ずタイムスタンプを打つようにしているので、署名生成時刻が証明できます。漏えいが発覚した場合、その日時が正確に把握できれば、それ以降に生成された署名は全て無効とみなす運用も可能です。そのような面も考えながら運用の方法も検討していけば、より全体として安全な仕組みができるのではないかと思います。
○松本座長　認証と言っているのは、署名するサーバ側が署名生成指示を認証して、この指示に従って署名生成処理またはその一部を行ってよいかどうか判断する部分です。そこが脆弱で、アタックされたり何か不具合があったりすると、本人は署名生成指示を出した覚えがないにもかかわらず、その本人の署名が作られてしまうことになるということです。

認証の部分は、リモート署名における署名生成の部分に加えてきちんと守らなければいけないというご指摘ですが、そのとおりかと思います。

山内構成員、どうぞ。

○山内構成員　JIPDEC の山内です。補足のコメントとして、事前に事務局に情報提供させていただいていますが、法務省の商業登記電子証明書のリモート署名システムの設計・開発・運用を、国内の有力なトラストサービスの会社の一つであるサイバートラスト社が落札して検討していくようです。

リモート署名についてのリスクは、エンドエンティティの鍵の漏えいだけではなく、今、宮崎構成員がおっしゃったエンドエンティティの方々それぞれに対して悪意のある人がなりすましを行い、知らないうちに電子処方箋や診断書のようなものが署名されるケースもあります。それは医療だけでなく、商業登記でもあり得る話だと思います。仕組みがだいぶ違うとは思いますが、他の省庁や公的な機関が行うリモート署名サービスの実装について情報収集していただき、リスク対策では共通するところがあると思うので、検討していただければと思います。私ども JIPDEC もいろいろお手伝いできることがあるかと思います。以上、情報提供でした。

○松本座長　ありがとうございます。その他、ありますか。宮内構成員どうぞ。

○宮内構成員　安全性などの問題は用途に関わってくるというのは、おっしゃるとおりだと思います。ただ、今の電子処方箋は、ある意味では身内の限られた範囲での署名の検証をやっていて、次に出てくるものも、おそらく検証するところはローカルの範囲内だと思います。もっと広い範囲で検証しなければならなくなると署名が重要な意味を持ってきます。そのような視点で用途の広がりは考えていかなければいけないのです。今のところ、特定のクローズな範囲でしか使わないというのであれば、それなりのセキュリティで許容するということもあり得る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した。ECDSA P-384 with SHA384 という方式を使うことを承認いただきたいということですが、私は条件を付けさせていただきたいと思います。本日いろいろなご意見をいただきましたので、そちらにきちんと対処していただくことです。特にリモート署名が使えないと、HPKI の場合、今後実際に使用されないことになりかねませんので、どのような方式でリモート署名を構築するかという部分も明らかにしたうえで、最終的に決断することが望ましいのではないかと思いますが、皆様、いかがですか。

非常に大変な課題ではありますが、後回しにして済ませられるものではないと感じるので、このような発言をしています。

佐古構成員、濱口構成員、林構成員がこの辺の技術に詳しいと思いますが、いかがですか。

○佐古構成員　早稲田大学の佐古です。おっしゃるとおりだと思います。一方で、先ほど「リモート署名がないと実際に使用されない懸念がある」というお話でしたが、実際にど

のくらいの頻度でリモート署名が使われているか、そういうデータとあわせて検討するのがいいのかなと思いました。以上です。
○松本座長　林構成員も何かコメントをいただければと思います。
○林構成員　松本座長のおっしゃるとおりだと思います。先ほどから、セキュリティの脅威評価において認証の部分も重要であることや、秘密分散と呼ばれているモデルの評価、また商業登記電子証明書のリモート化の話が出ていたと思いますが、全体のアーキテクチャーをきちんと評価し、それを踏まえたうえで、HSM はどうか、どういうアルゴリズムであればセキュリティ強度が保てるのかを考えないといけません。暗号アルゴリズムの安全性だけ評価しても、全体のセキュリティ強度が評価できなければ、結果的に利用する時の安全性は保てません。全体像としてアーキテクチュアルなところをきちんと評価したうえで、最終的にはこの方式でいきましょうと、並行して進めていただくことが重要かと思いました。以上です。
○松本座長　ありがとうございます。では、今の林構成員の言葉を借りれば、ECDSA 方式をどのように使うのかという部分の検討を加速していただきたいということです。
　HPKI の時期暗号化方式を ECDSA P-384 with SHA384 に決定することについて、承認できないという方はいらっしゃいますか。それでは、条件付きで承認としたいと思います。どうもありがとうございました。

（3）リモート署名サービスの活用に関して
○松本座長　それでは次の議題に進みたいと思います。まず事務局からご説明をお願いできますか。
○新畑室長　厚生労働省医政局医療情報室長の新畑です。現在検討を進めている、死亡届及び死亡診断書（死体検案書）提出のオンライン・デジタル化における HPKI リモート署名の活用について、皆様方に今後ご審議いただきたいと思いますので、ご説明させていただきます。
　HPKI リモート署名の活用については、オンライン資格確認等システムおいてネットワークを介して、閉域網のみという条件で使用できる状況であると認識しています。本日は現在進めている取組やシステムフローの概要をご説明し、次回以降の会議でリモート署名サービスの基準の適合性について改めてご説明したいと思います。
　はじめに資料3に基づき、本取組の概要についてデジタル庁からご説明します。
○デジタル庁上田参事官　デジタル庁参事官の上田と申します。死亡届及び死亡診断書（死体検案書）提出のオンライン・デジタル化の取組の概要について、資料3の1頁からご説明します。
　死亡に伴い、遺族に対して様々な行政手続等が発生します。国内の年間死亡数は 160 万人を超え、今後死亡する方の人数が増えていく中で、死亡・相続に関する手続のオンライン・デジタル化について、デジタル庁として検討を進めており、遺族の負担軽減、利便性

向上、市区町村等における手続の効率化のための取組を実施しています。本年６月に閣議決定された「デジタル社会の実現に向けた重点計画」においても、資料にありますように「具体的なシステム設計・開発に関する検討を進める」と記されているところです。

次に２頁では、システムのおおよその流れをご説明します。全体的な流れとしては、医療機関が死亡診断書（死体検案書）（以下、「死亡診断書等」）を発行し、その後、遺族等届出人がマイナポータルでログイン操作をし、自治体に提出します。

もう少し細かく説明すると、まず図の左上の医療機関で①死亡診断書等を作成し、②医師の電子署名を付与していただきます。その診断書を、③PMH（Public Medical Hub）と呼ばれるシステムに送付し、④二次元コードを付与しPDF形式で発行します。⑤死亡診断書等PDFを印刷し、遺族等届出人にお渡しします。遺族等届出人は⑥二次元コードを読み込みマイナポータルにログインします。二次元コードに死亡診断書等に関する識別子も埋め込まれているので、⑦PMH から電子データとなっている死亡診断書等を取得します。⑧マイナポータルで死亡届を作成し、⑨自治体に死亡届と死亡診断書等をセットで提出いただくという流れです。

３頁は PMH のご説明です。今回の取組以外でも、医療費助成、予防接種、母子保健、自治体検診等に関して自治体と医療機関等をつなぐ情報連携システムです。基本的には自治体の事業となっているものが多く、それについて医療機関と自治体の情報連携をするものです。

次の４頁は本取組に係るシステム関係の開発スケジュールです。まず今年度は既に要件定義を始めており、その後、システムの構築をしながら、医療機関システムと PMH の接続検証、また医療機関の運用が成り立つかどうかの検証までを今年度のゴールとしています。

ただ、今年度では実運用することは基本的に考えていないため、ダミーデータを使いながら導入の流れを検証します。その後、来年の夏頃に実証事業（スモールリリース）を行います。この時期にはマイナポータルも含めて開発が終わっているので、自治体、マイナポータル、PMH、医療機関の大きな流れについて、まずはスモールに実証的な事業を進めていきます。さらにマイナポータルの改修を進め、来年度中に本格稼働し、順次自治体の数を増やしたいというスケジュールです。

○新畑室長　厚生労働省医政局医療情報室長の新畑です。こうした取組において死亡診断書等における電子署名についてどのように考えていくか、その背景とご相談事項を５頁でご説明します。死亡診断書等を電子化した場合には、死亡診断書は医療機関等で作成する医療情報を含んだ文書であるため、これを取り扱うシステムには「医療情報システムの安全管理に関するガイドライン」が適用されることとなります。

現状「医療情報システムの安全管理に関するガイドライン」において、どのように記載されているか、下の①と②でご説明しています。①法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合に、②法令で医師等の国家資格

を有する者による作成が求められている文書については、医師等の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等を用いることとさせていただいています。そうした中でローカル署名での実装に加え、現在、電子処方箋等も含めてリモート署名が普及していることから、リモート署名の使用に関しても検討しています。こうした取組においてリモート署名を使うことについて、皆様方のご意見をお聞きしたいところです。

資料6頁では、現在取組が進んでいる電子処方箋管理サービス/死亡届及び死亡診断書等提出のオンライン・デジタル化のシステムにおける HPKI 署名の流れ、ローカル署名とリモート署名について、今回の取組の概要をイラストでお示ししています。

図の上側が電子処方箋管理サービスについてです。まず医療機関で医師が処方箋に電子署名をし、電子処方箋管理サービスで署名検証を行い、医師が作成した処方箋であることを確認して受領します。また薬局は、電子処方箋管理サービスが署名検証した処方箋をマイナ保険証で受領し、処方箋に基づいて調剤した後に、薬局から調剤結果を登録する際に、薬剤師が HPKI カードを用いた電子署名をして電子処方箋管理サービスに登録します。現在、このような流れを行っています。

図の下側が、今回の死亡届/死亡診断書等のオンライン提出に関する連携システムのフローです。医療機関で死亡診断書等を発行する際に、「死亡診断書等情報ファイル」に署名を行い、オンライン資格確認ネットワークを通って PMH にこのファイルが流れていきます。そこで署名検証を行い、署名検証の証跡を付与した後にマイナポータルに流し、そして、自治体に流れていくことを想定しています。

以上、取組及びシステムの概要となります。冒頭で説明したとおり、詳細な基準等への適合等は今後ご説明させていただき、皆様方にご審議いただきたいのですが、今回は概要に対して、ご意見をいただければと思います。資料の説明は以上です。

○松本座長　ありがとうございました。それでは、ただいまご説明いただいた内容について、ご質問ご意見をいただければと思いますが、いかがですか。宮内構成員。

○宮内構成員　最後の6頁の図を見ると、署名検証が PMH でのみ行われ、その後は行われておらず、署名検証の証跡により署名が検証されたことを届出人や自治体が確認するという仕組みになっていると思います。電子処方箋の場合、薬局において署名検証を行うのに対して、自治体ではなぜ署名検証できるようにしないのでしょうか。もう一点、PMH で署名検証証跡を付与していますが、この証跡が確かに PMH が付けたものであることを、届出人や自治体はどのように確認するか、教えていただきたいと思います。以上、お願いします。

○デジタル庁上田参事官　我々としては PMH で署名検証を行うことで、自治体の代わりに検証していることになると思いますので、自治体で署名検証をする必要はないのではないかと考えています。一方で、PMH で署名検証したかどうかをマイナポータルや自治体で分かるようにする必要があるという話は、重要なご指摘かと思いますので、開発の中で検討していきたいと思います。

○宮内構成員　死亡診断書等がそれで問題ないとされるのであれば、電子処方箋についても「電子処方箋管理サービスで署名検証しました」と言えば、薬局はいちいち一つずつ署名検証しなくてもいいことになってしまいます。しかし、それはあまりよろしくないと私は思います。第三者機関が確認したからいいというのではなく、書類に付いている署名を自分で確認することが大原則であり、基本です。その基本を踏襲せずに、途中で第三者機関が署名検証したものを信じてやりとりをするというのが、なぜそのようにしなければいけないのか、よく分からないのでお聞きしています。

自治体が HPKI 署名を検証できれば、そもそも何の問題もないわけです。その方向に進めるほうがいいのではないかと思いますし、署名の検証のライブラリは、薬局でも自治体でもそれほど大きな違いはないと思います。そういう意味では電子処方箋と同じようにやったらどうかと思います。いかがですか。

○デジタル庁上田参事官　薬局との関係は、両方見ている厚生労働省からご説明していただくことだと思いますが、まず自治体で署名検証をする意味がどこまであるか、ということが問題になると思います。自治体に署名ライブラリを入れることになれば、当然それなりにコストをかけることになります。そうした中で、PMH で署名検証を行うことでコストを抑えつつ信頼性を確保できないかということです。

○新畑室長　電子処方箋管理サービスと死亡診断書等との違いについては、自治体においては、薬局とは異なり LGWAN である閉域網を通ります。また、自治体職員が改ざんをするリスクも低いと思われます。先ほど上田参事官からもご説明があったとおり、それぞれの自治体でモジュールを導入することの費用対効果も含め、総合してこのような案でどうかと考えています。

○宮内構成員　今のお話によると、薬局よりも自治体を信用できるか、という議論になってしまうと思います。自治体は署名が適切に行われていることを確認する責任があります。資料 5 頁にあるように、「医療情報システムの安全管理に関するガイドライン」において「電子的に検証できる電子証明書を用いた電子署名等を用いること」とされているので、自治体の責任として署名が正しく付いていることを確認すべきだと思います。それを第三者である PMH に任せるのは、私は賛同できない部分があります。

そのようにやるのであれば、署名検証の証跡を付与したのが PMH であることを確認するための確実な方法が必要となりますが、それを確立するくらいならば自治体が署名を直接検証すればいいのではないかと、個人的には思います。

署名検証の証跡付与についてはシステム上考えていくという話が先ほどありましたが、自治体が直接署名検証するのと同じぐらい安全な方法が得られるのか疑問に思いますし、それを考えるならば薬局と同じように直接署名検証するほうが安全性が確保できていいのではないかと思います。

○松本座長　柴田構成員、どうぞ。

○柴田構成員　医療機関側から死亡診断書等を出す相手先について、まず PMH は自治体

であるのかという質問です。つまり PMH という機関がどの立ち位置にあるのか、自治体からきちんとした委託や委嘱を受けて、正式に死亡診断書等を出していい機関である場合、６頁の図の薄塗りの四角形の「PMH」、「LGWAN」、「自治体/法務省」が全部くくられて、医療機関は安心して死亡診断書等を出せる相手になるのではないかと思います。その見解についてはいかがですか。
○デジタル庁上田参事官　死亡診断書の法的関係はまだ未整備の部分もありますが、先行して始めている PMH の例えば医療費助成や母子保健については、自治体からの委託業務として整理していて、実際に委託契約を結んでいる関係性になっています。よって、署名検証については自治体の代わりに行うものだと思いますので、委託契約などが必要と考えているところです。全体としてこのシステムをどのように法的に実現するか、もう少し検討は必要ですが、署名検証の部分はそのような整理と考えています。
○柴田構成員　ありがとうございます。
○松本座長　横田構成員、どうぞ。
○横田構成員　兵庫県薬剤師会の立場から補足として申し上げます。先ほど宮内先生がおっしゃった部分について、薬局は署名検証するだけなく、薬局も調剤情報を電子処方箋サービスに戻す時に、HPKI カードで電子署名してタイムスタンプが押されますので、若干今回のフローとは異なります。また、先ほど柴田先生がおっしゃったように、PMH に入っているものの確からしさについて、医師が認めたうえで、その中に入った死亡診断書等情報ファイルをマイナポータルまで流すためには、ここに何らかの承認等が必要な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した。林構成員、どうぞ。
○林構成員　改ざん検知の観点でコメントがありましたが、電子署名は改ざん検知の目的だけではないことは、忘れないようにしていただく必要があると思います。山内構成員をはじめ他の構成員の方々からもご意見が出ていましたが、署名検証行為に一定量価値があることは忘れないようにしなくてはいけないと思ったのが、一点です。
　また、今システム構成上まとめて記載されていると思いますが、自治体と法務省では法的・制度的位置付けが違う可能性があるので、この部分は分けて考えるほうがいいかと思います。林からは以上です。
○松本座長　ありがとうございます。山内構成員、どうぞ。
○山内構成員　JIPDEC の山内です。電子署名に関わる仕事をしている者としては、宮内構成員と全く同じ印象を受けています。公的個人認証サービスの場合、法律に基づいて署名検証者が限定されていることは皆さんご存じだと思いますが、HPKI の場合、特に「署名検証をするのは何々に限る」ということではなく、むしろ公的機関である自治体や法務省が署名検証することに何の問題もないわけです。署名検証を HPKI のルールに基づいて CRL（Certificate Revocation List）や OCSP（Online Certificate Status Protocol）などを使って確認することは難しいことではないので、あえて PMH で検証する理由が分かりませ

んでした。
　もしPMHで電子的な処理を全て自治体から委託を受けて行うのであれば、PMHの中でしっかりとしたプロセスで署名検証証跡付与のシステムが動いていることを外部の監査によって証明するなど、信頼性を確保することが大事だと思います。ただ、それをやるためにはコストもかかるでしょうから、どちらが最終的にいいのか、自治体・法務省が署名検証するほうがいいのか、PMH で委託を受けて行うほうがいいのかについては、全体のコスト論や法的な面も含めた信頼性の観点でご検討いただければと思います。以上です。
○松本座長　デジタル庁、厚生労働省から何かコメントはありませんか。
○デジタル庁上田参事官　今おっしゃっていただいているとおりだと思います。我々としては、実質的な懸念はコスト論にあると思います。LGWAN 回線を通して CRL や他のやり方で署名検証する仕組みを構築するコストのほうが、高いのではないかということです。
　一方で、信頼性の担保のため、署名検証の証跡をきちんと追えるようにすることの必要性も認識しました。コスト論だけではない部分もあると思いますが、おっしゃっていただいたように証跡を追跡できる仕組みを構築するほうがコストがかかるということであれば、我々の本来の意図とは違うので、その辺りの検討を深めていきたいと考えています。
○松本座長　ありがとうございます。横田構成員、どうぞ。
○横田構成員　確か Ai（オートプシー・イメージング）では画像データも扱われていたと思います。そのデータが法務省の「死亡診断書等情報ファイル」の中にあると考えると、この情報ファイルが PMH の中にあることに少し違和感があります。先ほどご説明いただいたように、PMH が自治体・法務省と一体だということであれば、6頁の図を少し直すことによって、制度、運用についてもう少し見えてくるのかなと思いました。以上です。
○松本座長　丸山構成員、どうぞ。
○丸山構成員　PMHの運営主体はデジタル庁ですか。国ということでしょうか。
○デジタル庁上田参事官　現状はデジタル庁で運営しておりますが、分野によって、社会保険診療報酬支払基金や国民健康保険中央会に順次移管します。先ほど申し上げたように死亡診断書はまだ法的構成がしっかりと整理しきれていませんが、現状、医療費助成は自治体からデジタル庁が委託を受けていて、支払基金に移管する予定であり、その後は自治体が支払基金に委託する、という構成になっています。
○丸山構成員　いろいろな仕組みがあるものを今まとめて PMH と言っていますが、今後仕組みごとにばらばらに運営するということですか。
○デジタル庁上田参事官　おっしゃるとおりです。PMH は分野ごとに分離できるようになっているので、その分野ごとである程度出来上がっている状況になれば、それぞれの適切な運用主体に移管していくことになります。
○丸山構成員　今はデジタル庁であるが、将来的には、例えば厚生労働省に PMH の死亡届のモジュール、システムが移行していく可能性があるということですか。
○デジタル庁上田参事官　その可能性もないわけではありませんが、これからの議論にな

ると思います。
○丸山構成員　分かりました。ありがとうございます。
○松本座長　本来は、全体的なプランやポリシを共有し「このような条件を満たすものを作らなければならない」ということを決めた上で、具体的なシステムの構成やどのやり方が最も望ましいかという議論に進められるといいと思います。他の議題も、先に具体的なひな型が出てきて「これでいいでしょうか」という問いかけが多いので、もう少しトップダウンで議論ができるように進めていったほうがいいのではないかと、今回も思いました。ご考慮いただければと思います。
　佐古構成員、どうぞ。
○佐古構成員　死亡診断書は例えば会社で忌引きを取る時や保険を下ろす時など、民間でもよく使われています。今回、自治体でも直接確認できない仕様になっているようですが、ゆくゆくは国民が HPKI で医師が作成したものであることが検証できる仕組みにしていただきたいという要望をお伝えします。以上です。
○松本座長　上田参事官、どうぞ。
○デジタル庁上田参事官　原本を発行している例もあるかもしれませんが、現状でも例えば自治体に死亡診断書を出す前に、勤務先や保険会社にはコピーを取ってお渡しするケースもあると伺っています。デジタルの利点として、同じものを簡単に複写できることがあるので、将来的にはそのようなことも検討課題としたいと思いますが、足元としては自治体に出すところを検討していくということです。
○松本座長　柴田構成員、どうぞ。
○柴田構成員　私は、死亡診断書のコピーを取り忘れて苦労した経験があります。マイナポータルもしくは医療機関から発行するなど、複写がもう 1 枚必要な時に手に入る仕組みがあると、国民にとって忙しい時に非常に助かるので、この仕組みは早く実装したほうがいいと個人的には思います。
○デジタル庁上田参事官　マイナポータルを介して行うことの利点として、そのようなこともあると思います。マイナポータルの機能は基本的には行政機関への手続や、行政からの情報取得が主たるものですが、現状でもマイナポータルの API を出すなど、民間との連携もいろいろな形で行っていますので、そのような形で拡張できると思います。ニーズは当然我々も承知していますので、そちらにも取り組みたいと思いますが、まずは足元をしっかり固めたいと考えています。
○松本座長　ありがとうございます。宮内構成員、どうぞ。
○宮内構成員　上田参事官の先ほどの話について、署名検証をしようと思うとコストがかかることは理解できますが、現状でも自治体は JPKI の署名など、いろいろな部局で検証して扱っています。例えば電子契約の場合、しかるべき証明書を使って相手方の電子署名を検証するなど、そもそも署名検証はいろいろ行っているはずです。いろいろな届出についても、JPKI が多いと思いますが、検証するモジュールは当然システムの中に入っているは

ずです。何を増やさなければいけないかというと、HPKI の認証局の証明書を取ってくること、そこを見れば OCSP はつながる場所が決まっているので、一般的な証明書とあまり大きな違いはありません。そういう意味では、それほどコストがかかるものだと思えません。また、今後このような種類のものを次々にこのような仕組みでやることは、あまりよろしくないと思います。やはり電子証明書をきちんと見て署名を検証するという形で対応していくほうが、私はいいのではないかと思います。

これらについてはデジタル庁ではなく、総務省に聞かなければいけないのかもしれませんが、全体的な枠組みをどのように考えていらっしゃるのか、教えていただきたいと思います。

○デジタル庁上田参事官　我々として少しちゅうちょしているのは、LGWAN を介して CRL データも含めて署名検証していかなければいけないところについて、どこまでコスト感があるかという懸念を持っているためです。

○宮内構成員　OCSP は LGWAN を通さなくてもいいのではありませんか。薬局は署名検証をしているわけですから、私は薬局と同様にすればいいと言っているのです。そもそも OCSP を通すのに、どこのネットワークでなければいけないということはないでしょう。

○デジタル庁上田参事官　どこのネットワークでなければいけないということはもちろんありませんが、自治体で通貫しているのがインターネットではなくて、LGWAN など、幾つか階層があるのです。

○宮内構成員　分かります。

○デジタル庁上田参事官　その中で今回使うのが LGWAN なので、LGWAN の階層の中で CRL データなり OCSP ができるかということです。

○宮内構成員　そういう自治体のネットワークに制約があるということですか。

○デジタル庁上田参事官　おっしゃるとおりです。

○宮内構成員　LGWAN からしか見られないかどうかなど、それだと困ることもたくさんあると思うので、いろいろ工夫はされていると思います。自治体は 1,700 以上あるので、いろいろご苦労はあると思います。今後このシステムだけではなく、届出側から何らかの署名をされたものが来ることは非常にたくさんあると思うので、まとめて署名検証ができるようにきちんと考えておいたほうがいいのではないか、というのが私の思いです。

○デジタル庁上田参事官　おっしゃるとおりだと思います。自治体の環境はマイナンバー系、LGWAN 系、インターネット系の３層構造で、ネットワークがそれぞれ分離され、データの流通もあまりできないことは以前から問題視されています。なんとかしなければいけないということは、私とは別の部局で議論しています。おそらくそのようなことをやっていけば、今のような懸念もどんどん減り、コスト的なハードルも下がると思いますが、現状はまだそこまで行き着いていないことを前提に議論しています。

○宮内構成員　分かりました。どうもありがとうございます。ご検討いただければと思います。

○松本座長　矢野オブザーバー、どうぞ。
○矢野オブザーバー　補足をさせていただきます。まず HPKI は OCSP を持っていなくて CRL 方式です。電子処方箋の CRL 検証は、オンライン資格確認ネットワークの中、閉域網にプロキシを立てて普通にできているので、同じように LGWAN にプロキシを立てていただければ簡単にできます。素直に死亡診断書の署名検証をすればいいのではないかと思います。以上です。
○松本座長　山本オブザーバー、どうぞ。
○山本オブザーバー　むしろ HPKI のルート証明書、厚生労働省ルートを GPKI、LGPKI とブリッジングしていないのです。したがって、自治体はこの署名が信頼できるかどうかを判断できません。やろうと思うと、各自治体がこのルート証明書を信用するという手続をしなければいけません。簡単ですが、それを 1,700 以上の自治体においてやらなければいけないのです。それから HPKI といっても普通の X.509 ですから、電子署名としての確認は普通のプログラムでできるのですが、HPKI 独特のサブジェクトディレクトリ属性に入っている「医師である」という資格の表示は普通の検証プログラムではできません。それを見たいと思うと HPKI のサブジェクトディレクトリ属性を見るためのルーティンが入った検証プログラムをインストールしなければいけませんので、若干手間がかかります。ただ、例えば検証用のプログラムは、我々は GitHub に無償で公開しているので、組み込んでいただければライセンス費用がかかるわけではなく見ることができます。一番の問題はブリッジングしていないために信用をいちいち手動でやらなければいけないことでしょうか。それほどお金のかかる話ではないですが、手間はかかるのではないかと思います。
○松本座長　明記されていない条件がいろいろあるということで、それを満たす解として、資料 6 頁の図を提示いただいているものと思います。PMH はランサムウェアの格好の対象になり、PMH を人質に取ると大変なことになってしまうと思います。死亡診断書等の話に限らず、たくさんのものが PMH 上に構築されるという図が 3 頁にありますが、大丈夫なのでしょうか。どのくらい強く作ろうとされているのでしょうか。
○デジタル庁上田参事官　基本的に 1 か所といっても、それぞれデータベースを置いて運用していくものですから、一つのデータベースに全部の情報が入っているわけではありません。また、先ほど申し上げたように、分野ごとにそれぞれ関係する運用主体に移管することを考えています。
○松本座長　そうすると、3 頁で PMH の定義がよく分からないと思いました。「PMH 関連システム」とは何ですか。
○デジタル庁上田参事官　わざわざ「関連」と入れているのは、例えば予防接種は昨年度まで PMH の中でデジタル庁が運用していましたが、今年度からは国民健康保険中央会に移管しています。その中でも PMH の中の識別子を振り分ける制御はネットワークで行っており、ネットワークは PMH を通しつつ予防接種は国民健康保険中央会で行っているということもあり、それで「関連」という言い方をしています。

○松本座長　柴田構成員、どうぞ。
○柴田構成員　これは全部、同じネットワーク基盤の上にはあるのでしょうか。
○デジタル庁上田参事官　そういうことだと思います。
○柴田構成員　分かりました。
○松本座長　「関連システム」と言っているのは、３頁の図の中央の大きな四角形の中に描いてある部分の全部が PMH ではなく、元 PMH だったということですか。
○デジタル庁上田参事官　おっしゃるとおりです。
○松本座長　分かりました。ありがとうございます。お時間の関係もありますので、この議題については以上とさせていただきたいと思います。ありがとうございました。

（４）連絡事項
○松本座長　それでは続いて、事務局から連絡事項等があればお願いします。
○岡嶋主査　本日も長時間の議論をありがとうございました。次回の HPKI 専門家会議は２か月後の 11 月頃の開催を予定しています。日程調整については改めてご連絡します。次回は、次期認証局システムの構成に関する議論、暗号移行等に伴う HPKI ポリシ関連書類の影響度や改訂要否に関する議論を行いたいと思います。議題（２）において座長から条件付き承認された、この条件解除に向けては、改めて松本座長、MEDIS の山本オブザーバーとも打ち合わせながら、どのタイミングの専門家会議でお示しするかご相談させてください。
　HPKI ポリシ関連書類について、暗号移行以外の観点でもし改訂が必要な点があれば、第 35 回 HPKI 専門家会議に向けて 10 月 10 日をめどに、事務局の河内、岡嶋までご連絡いただければと思います。
　また次回の HPKI 専門家会議においても、今回と同様に資料の事前説明の機会を頂戴したいと考えています。以上です。
○松本座長　ありがとうございました。ただいまのご説明について何かご不明な点等はありますか。

閉会
○松本座長　それでは第 34 回の HPKI 専門家会議を終了します。どうもありがとうございました。

以上