資料１

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

第21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・作業班合同会議

医政局特定医薬品開発支援・医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

目次

１．HPKIの鍵預かりとリモート署名について
前回までの議論

HPKIのリモート署名については、令和５年１月から電子処方箋に限定して運用開始。「鍵預かり」と「リモート署名」については、今後、評価基準の作成が必要となっている。

前回までの議論

第18回専門家会議（令和４年12月19日開催）において、「HPKIの鍵預かりとリモート署名の評価体制」について議論し、以下の通り整理された。

（整理）

預託された私有鍵を用いたリモート署名について、高度な当人認証を行うため等の安全性の評価基準が、現時点では日本に存在しない。こうした状況を踏まえ、HPKIの「鍵預かり」および「リモート署名」については、次の方法で安全性等を担保する。

○　専門家会議で「鍵預かり（HPKI分野全般）」および「リモート署名（電子処方箋に限定）」の評価基準を作成の上、監査を実施

○　評価基準が作成されるまでは、各運営主体が提出した安全性に関する文書を専門家会議で確認

（※）なお、運用については下記の事項に留意する。

- HPKI のリモート署名については、当面、電子処方箋に限定した取扱いとする。
  将来的には、電子処方箋の他、紹介状等、他のサービス提供希望者が現れることも想定される。
- 現状、HPKI認証局としては、「鍵預かり」に預託する鍵は１つと想定している（2nd鍵は発行するが、3rd鍵の発行予定はない）。

今後対応が必要な事項

・「鍵預かり」と「リモート署名」の評価基準の作成
・準拠性監査の実施

1．HPKIの鍵預かりとリモート署名について
今後の進め方

評価基準を作成するにあたり、まずは、現行の仕組みを踏まえて前提条件（前提となる仕組み）を整理し、評価基準の対象範囲を明確にしてはどうか。その上で、各項目に必要なセキュリティレベルを整理し、決められたレベルを満たしているか否かを評価するための要件を策定してはどうか。

前提条件の整理

○　今回作成する評価基準の対象範囲を限定するために、まずは前提条件（どのような仕組みを前提に評価基準を作成するのか）を確認する必要がある。

○　現行のリモート署名サービスを前提とし、下記の事項についてまずは整理する。

（整理が必要な事項）

- 暗号鍵が生成される場所と手段
- 暗号鍵やその関連情報の配送先
- 暗号鍵の失効
- 暗号鍵やその関連情報の保管時及び配送時の保護方法
- 暗号鍵のライフサイクル
- 暗号鍵の廃棄　等

評価基準の作成方針案

○　整理した条件を前提に、評価基準の対象範囲を明確にする。

○　鍵生成（署名鍵の生成）、鍵インポート、鍵保持、鍵認可（署名鍵の活性化）等の事項について、必要なセキュリティレベルを整理する。その際、日本トラストテクノロジー協議会による「リモート署名ガイドライン」や「eIDAS規則」を参考にする。

○　信頼性レベルを満たしているか否かを評価するためのセキュリティ要件を策定する。

1．HPKIの鍵預かりとリモート署名について
今後の進め方

「鍵預かり」「リモート署名」の評価基準の作成後、各サービスの評価基準への適合性について、以下の手順で確認してはどうか。

評価基準への適合性確認方法

鍵預かり　：①各認証局が、サービスとして利用している「鍵預かり」の安全性を評価基準に基づき確認。
②各認証局の確認結果報告について、専門家会議で確認。

リモート署名：①鍵預かりサービス事業者が、サービスとして利用している「リモート署名」の安全性を評価基準に基づき確認。
②鍵預かりサービス事業者の確認結果報告について、各認証局が確認。
③各認証局の確認結果報告について、専門家会議で確認。

<HPKI専門家会議>
評価基準を作成

選定の妥当性を確認

<HPKIの認証局>
・日本医師会
・日本薬剤師会
・医療情報システム開発センター（MEDIS）

認証局が、評価基準を元に、サービスを確認した上で選定

<「鍵預かり」運営主体>

「鍵預かり」運営主体が、評価基準を元にサービスを確認した上で選定

<「リモート署名」運営主体>

今後のスケジュール（案）

1．　専門作業班にて評価基準（案）を作成（～８月中旬）
2．　専門家会議にて評価基準（案）の確認（～８月下旬）
3．　HPKI認証局が評価基準を元に「鍵預かり」と「リモート署名」サービスの安全性を確認（～９月上旬）
4．　専門家会議にて、３の妥当性を確認（～９月下旬）

2．マイナンバーカードを活用したHPKIリモート電子署名について

HPKIセカンド電子証明書※とマイナンバーカード（以下「MNC」という。）のシリアルを紐付けることで、MNCの利用者認証機能を用いて電子処方箋にHPKIのリモート電子署名ができる仕組みをHPKI認証局において検討中。 HPKIポリシとの関係については下記のとおり整理してはどうか。（※鍵預かりに預けたHPKI暗号鍵。HPKI認証局の独自の呼称。）

背景

○ HPKIのリモート署名については、HPKIカードを補完する位置づけとして、令和５年１月以降、電子処方箋に限定して運用しているところ。
○ 他方で、デジタル原則からみた医療DXにおいて「マイナンバーカード１枚で患者等が様々な医療・福祉サービスを受けることができ、医師等も医療サービス提供に必要な認証ができる」ことが求められている。
○ また、半導体不足の影響でHPKIカードが不足していることを踏まえ、HPKI認証局及びデジタル庁において、HPKIカードの本人認証の代わりにMNCによる利用者認証を用いることで電子処方箋へのHPKIのリモート電子署名ができる仕組みの構築を検討中。稼働後は、HPKIカードの発行がなくとも電子署名が可能となるので、カード不足にも対応。

方針案

リモート署名の際に、利用者証明を行う方法については、下記の理由から、HPKIカードに加えてMNCの活用を進めてもよいと整理してはどうか。

○ HPKIカードは、国家資格証明だけでなく、厳密に実在性及び本人性を立証するものであるが、MNCも当然に、厳密に実在性及び本人性を立証する手段である。
○ MNCは、HPKIカードと異なり、国家資格保持の確認機能を有していないが、MNCのシリアルとHPKIセカンド電子証明書が紐付くことで、国家資格確認が可能となる。

※MNCによる電子署名の場合、署名者の住民票住所が含まれるが、HPKIは住民票住所は含まれず、今回の仕組みであれば、署名者のプライバシーや安全の確保が可能。

③マイナンバーカードを活用した電子署名：具体的な制度設計（現時点のイメージ）

参考

令和5年度第1回電子処方箋等検討ワーキンググループ資料
（令和５年６月８日）

○ HPKI認証局及びデジタル庁において、HPKIとマイナンバーカード（以下「MNC」という。）を紐付けることで、MNCでもHPKIの仕組みで電子処方箋への電子署名ができる仕組みを構築を検討中。

① 電子署名については、HPKIリモート署名の仕組みを用いて医師・歯科医師・薬剤師個人の現住所を含まないプライバシーに配慮した形での署名が可能（※）HPKI認証局への利用申請は引き続き必要（マイナポータルを活用し画面を構築予定）

② 原則MNCで１日１回PIN入力することで、処方箋発行時に自動で署名付与

➡ 本年10月以降は、 HPKIカードに加えてMNCを活用したHPKIリモート署名が可能となる予定。
稼働後は、認証局の判断により、HPKIカードの発行可否を決められるので、現下のカード不足の対応やコスト削減も可能。

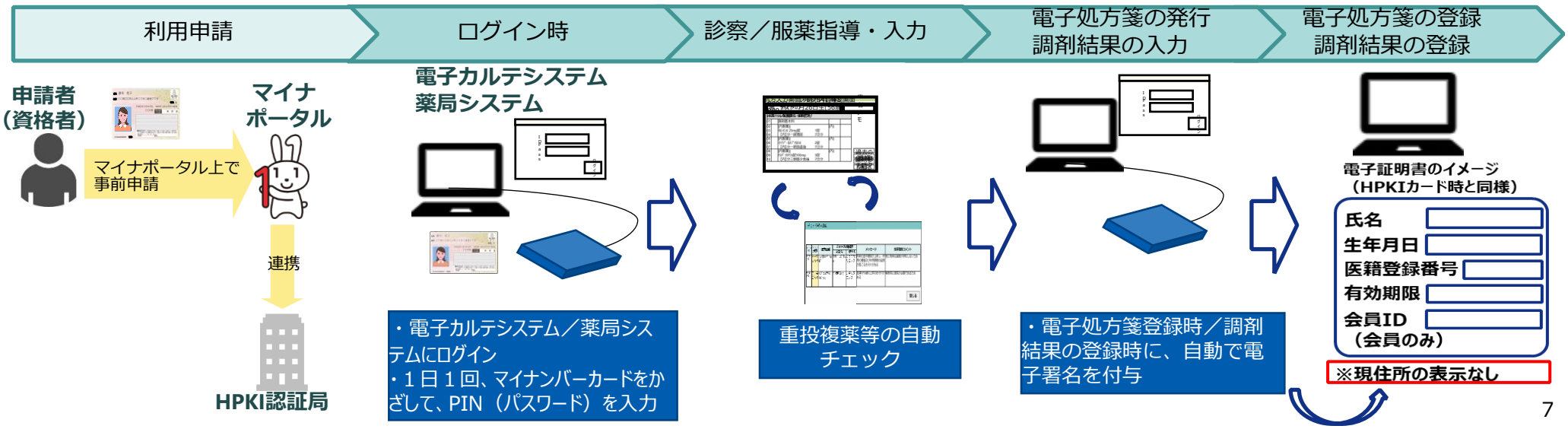
（具体的な利用場面等）

○ HPKIカードが不足する中、カード発行を待たずに、既に保有しているMNCを活用したHPKI署名が可能となる。

○ HPKI申請時にマイナポータルやMNCを活用し、現在提出を求めている住民票（写）や身分証のコピー等が不要となる。

○ HPKI申請からカードレス発行までに係る時間が短縮される見込みであるため、人事異動時で急遽、医師・歯科医師・薬剤師が電子処方箋に対応が必要となった場合に、医療機関における対応の円滑化が期待される。

<医療現場・薬局における運用フロー（イメージ）>



３．マイナポータル経由でのHPKI利用申請について

○　HPKIの利用申請手続きの簡略化を目指し、本年10月目処で、マイナポータル経由でのオンライン申請を可能とする仕組みの構築をHPKI認証局にて検討中。
○　設計内容次第では、HPKIポリシとの整合性確認する必要があり、その際は改めて相談させて頂きたい。

ポリシ該当箇所抜粋

【ポリシ3.2.3 個人の認証】
＜オンラインの場合＞
　証明書を申請しようとする個人は、認証局の定める手続きに従い、公的個人認証サービスを利用した申請者個人の電子署名、保健医療福祉分野PKI認証局の発行する署名用証明書を用いた電子署名、若しくはそれに準じた電子署名を提供することにより、実在性及び本人性及び申請者個人の申請意思を立証しなくてはならない。
　なお、公的個人認証サービス、保健医療福祉分野PKI認証局の署名用証明書等による電子署名は、当該本人しか実行できないことから、電子署名の提供によりこれらの意思を立証したものとみなされる。

【ポリシ4.2.1 本人性及び資格確認】
(3) オンラインの場合
　登録局からオンラインにより国家資格発行機関若しくはそれに代わる台帳を備えた機関に問い合わせを実施して、国家資格発行機関から申請者の国家資格保持の有無について回答を得る。
　国家資格発行機関等によりオンラインの資格確認手段が提供されていない場合は、持参若しくは郵送と同等の資格確認を実施する。
なお、確認に用いた証明書等は、登録局で保存年限を定めて保存しておくものとする。

４．HPKI認証局運用規約関連資料の改訂について

○　署名アルゴリズムのSHA-1（Secure Hash Algorithm 1）及び組織名称について、下記のとおり規約関係資料を改定してはどうか。

ご確認事項①

○　署名アルゴリズムのSHA-1（Secure Hash Algorithm 1）は既に使用していない。
○　資料２－１、２－２のように「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」を改定してよろしいか。
（※）　当該アルゴリズムについての記載を削除する。

ご確認事項②

○　厚生労働省ルート認証局の運用管理規程（CPS）Ver 1.3（令和４年10月12日）の承認は「1.5.4 CPS承認手続き」にて、HPKI認証局専門家会議によって承認されるものとされている。
○　署名アルゴリズムのSHA-1（Secure Hash Algorithm 1）は既に使用していない。
○　資料３のように厚生労働省ルート認証局運用管理規程（CPS）を改定してよろしいか。
（※）　当該アルゴリズムについての記載を削除する。

ご確認事項③

○　資料４－１及び４－２のとおり、組織改編に伴い「保健医療福祉分野PKI認証局署名用・認証用（人）証明書ポリシ準拠性審査手続規則」及び「保健医療福祉分野PKI認証局署名用・認証用（人）証明書ポリシ準拠性審査業務実施規則」を改定してよろしいか。
（※）「医政局長」を「大臣官房医薬産業振興・医療情報審議官」、「研究開発振興課医療情報技術推進室」を「特定医薬品開発支援・医療情報担当参事官室」に修正する。