参考資料2

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

第18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

２０２２（令和４）年１２月１９日

電子処方箋におけるHPKIの鍵預かりとリモート署名について

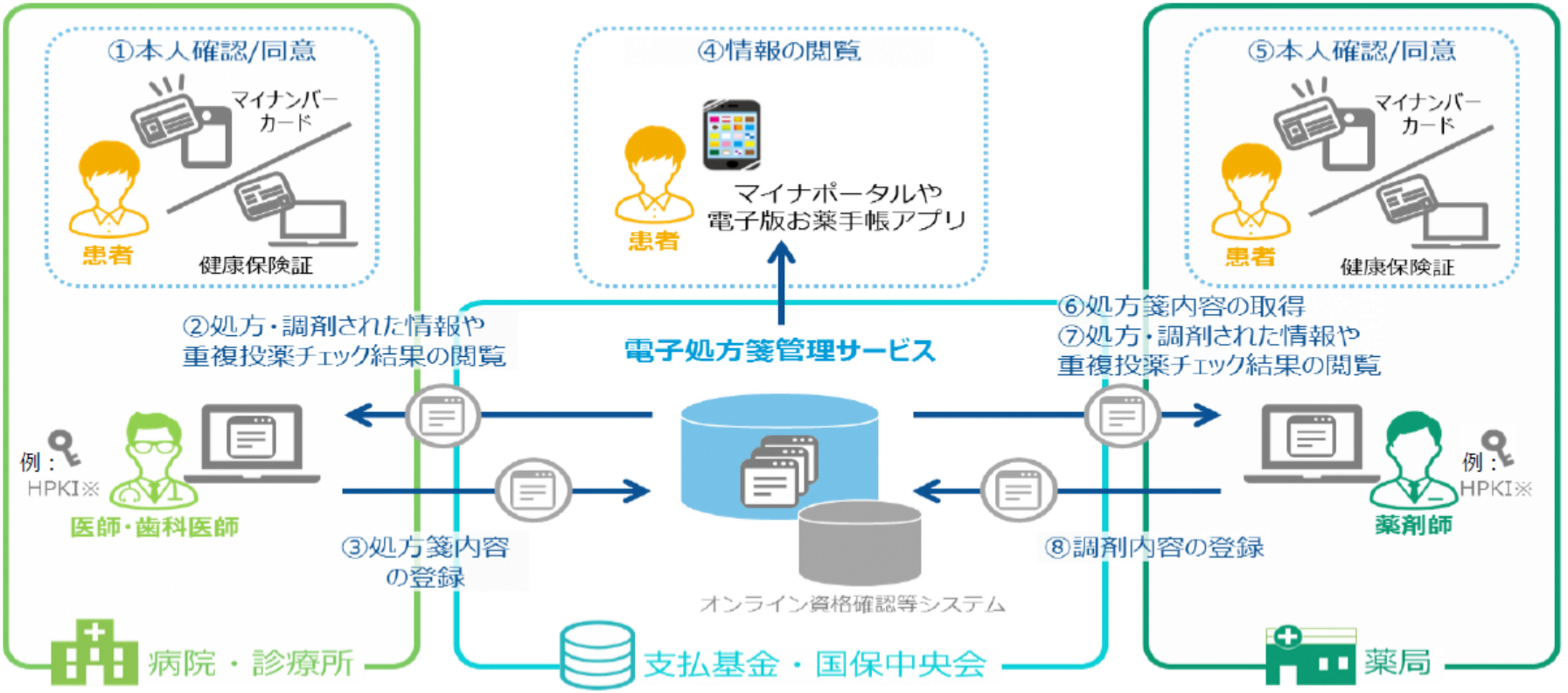
医政局特定医薬品開発支援・医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

１．電子処方箋について

第１１回健康・医療・介護情報利活用検討会
資料（令和４年10月19日）

電子処方箋とは、オンライン資格確認等システムを拡張し、現在紙で行われている処方箋の運用を、電子で実施する仕組み。オンライン資格確認等システムで閲覧できる情報を拡充し、患者が直近処方や調剤をされた内容の閲覧や、当該データを活用した重複投薬等チェックの結果確認が可能に。（令和５年（2023年）１月～運用開始予定）



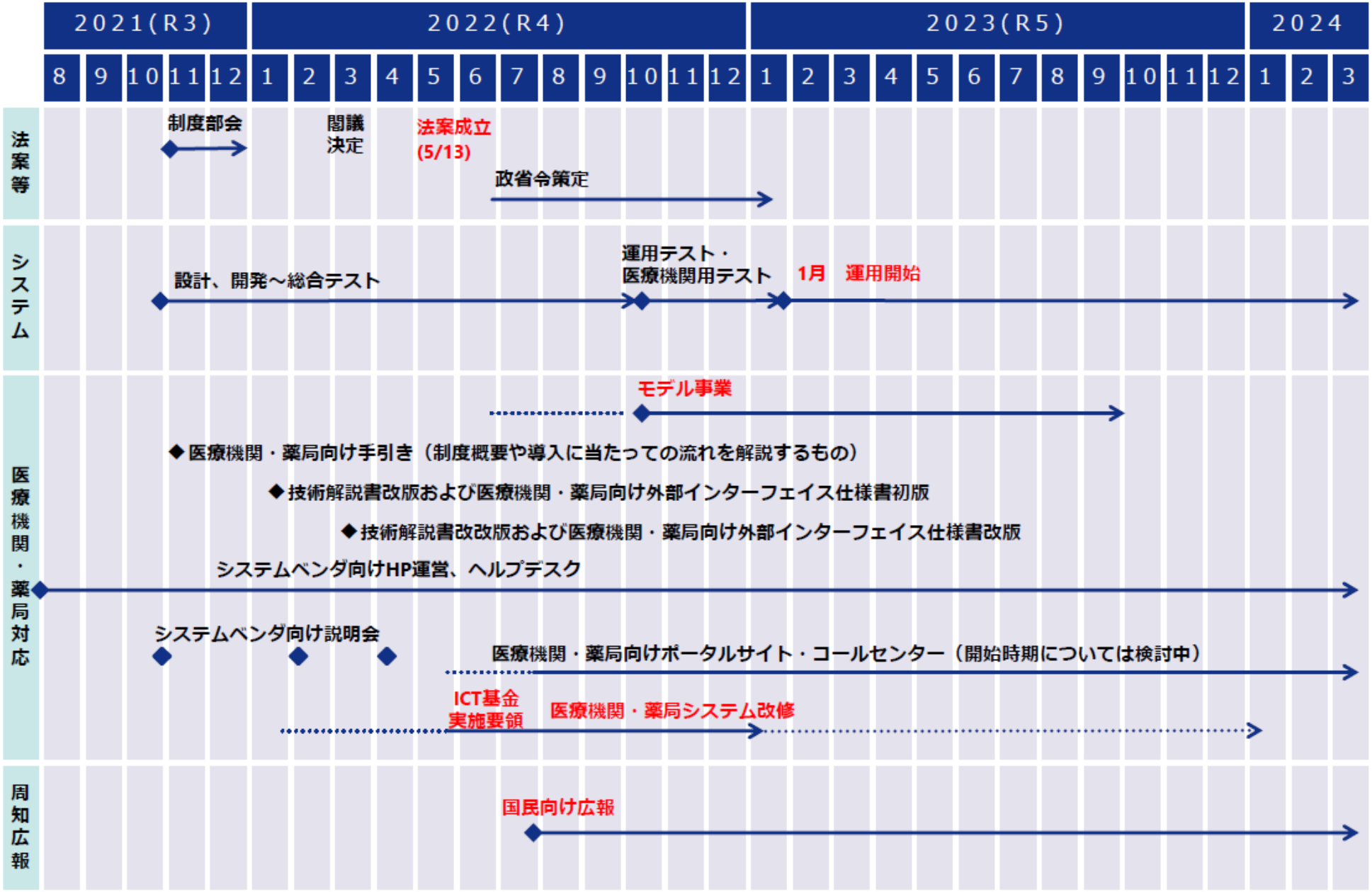
※HPKI（Healthcare Public Key Infrastructure） 医師、薬剤師等の国家資格と院長、管理薬剤師等の管理者資格を証明することのできる保健医療福祉分野の電子証明書

成長戦略フォローアップ（令和３年６月18日閣議決定）

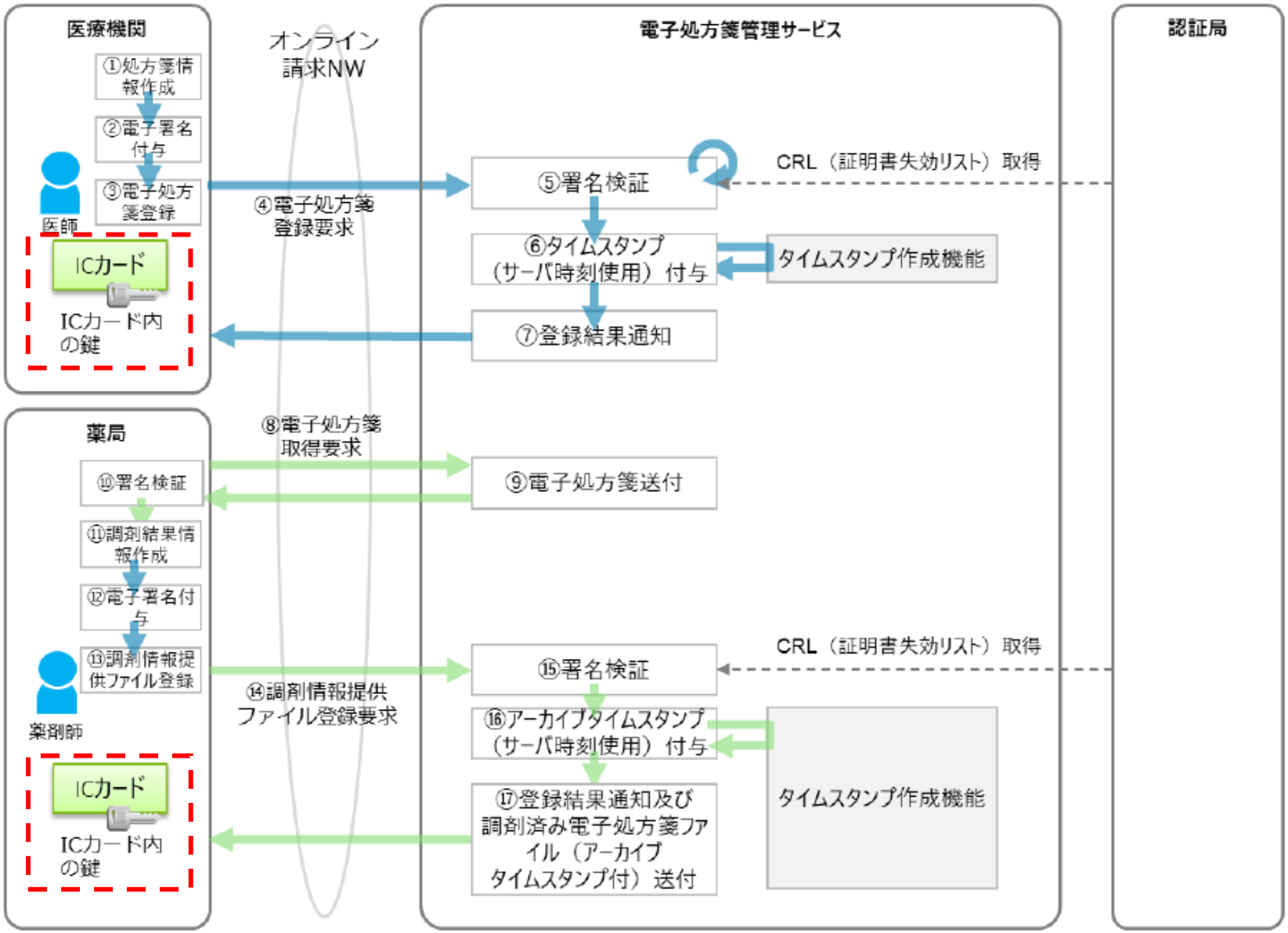
・ オンライン資格確認等システムを基盤とした電子処方箋の仕組みについて、実施時における検証も含め、安全かつ正確な運用に向けた環境整備を行い、2022年度から運用開始する。

1．電子処方箋について

第11回健康・医療・介護情報利活用検討会
資料（令和４年10月19日）

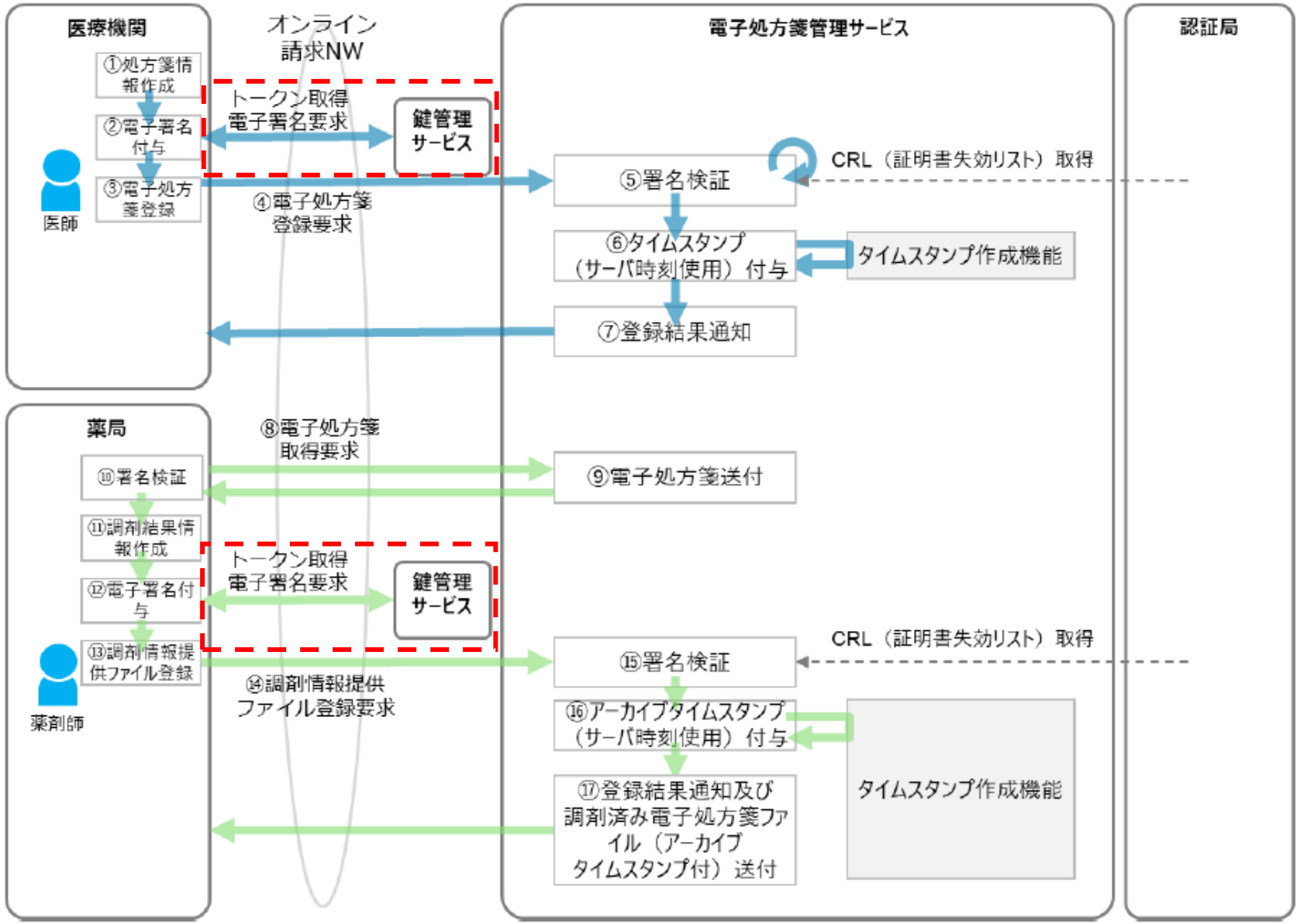


1．電子処方箋の電子署名について（ローカル署名のイメージ）



Ref. 技術解説書

1．電子処方箋の電子署名について（リモート署名のイメージ）



Ref. 技術解説書

2．HPKIの鍵預かりとリモート署名について

保健医療福祉分野における電子署名については「医療情報システムの安全管理に関するガイドライン第5.2版」にて基準が示され、その現実的な方策として３つの方法が示されている。HPKIはそのうちの1つという位置付けである。

A．制度上の要求事項

「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

二 当該情報について改変が行われていないかどうかを確認することができるものであること。

（電子署名及び認証業務に関する法律（平成12年法律第102号）第2条第1項）

C．最低限のガイドライン

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、以下の条件を満たす電子署名を行う必要がある。

1. 以下の電子証明書を用いて電子署名を施すこと

(1) A 項の要件を満たす電子署名を施すこと。なお、これはローカル署名のほか、リモート署名、立会人型電子署名の場合も同様である。

(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、以下の（a）～（c）のいずれかにより、医師等の国家資格の確認が電子的に検証できる電子署名等を用いること。

(a)HPKI

(b)認定認証事業者又は認証事業者の電子署名であり、当該電子署名を施された文書を受け取る者が、医師等の国家資格の確認を電子的に検証でき、電子署名の検証を正しくできること等

(c)JPKI+電子署名に紐づく医師等の国家資格が検証時に電子的に確認できること等

2. 必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること

2．HPKIの鍵預かりとリモート署名について

従来、HPKIは専門家会議の審議により、第三者評価を行う特定認証事業者と同等の水準として運用をしてきた。今回導入するリモート署名は、現時点では特定認証事業者の業務として位置づけられていない。それらを踏まえ、対応案の通りとしてよいかご審議をお願いしたい。

「鍵預かり」と「リモート署名」の概況

どの「鍵預かり」と「リモート署名」サービスを信頼するかは、本来、各HPKI認証局の判断であり、その判断の妥当性を確認（準拠性監査）するのが、HPKI専門家会議である。

一方、現在、右記の理由によりリモート署名に関する審査の具体的方法は示されていない。

HPKI認証局が、リモート署名ガイドラインに基づき、第三者機関が評価したサービスを選定できれば、多くの問題は解決すると考えられるが、現在、第三者認証は存在していない。

HPKIと電子署名法上のリモート署名の扱い

HPKIは、専門家会議という第三者会議で承認をしているため、電子署名法上の認定はないが特定認証業務を行う事業者の水準に近いと考えられ、従前からそれに準じた基準で運用してきた。

今回導入しようとしている「リモート署名」は、現在、電子署名法第3条の推定が得られるかは定かではない。

電子署名及び認証業務に関する法律（平成十二年法律第百二号）

第二条　この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

二　当該情報について改変が行われていないかどうかを確認することができるものであること。

２　この法律において「認証業務」とは、自らが行う電子署名についてその業務を利用する者（以下「利用者」という。）その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。

３　この法律において「特定認証業務」とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。

第三条　電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

電子署名Q&A

Q27. リモート署名は電子署名法の推定が得られますか？

A. 得られると考えられますが、現時点では定まっていません。電子署名法主務3省(総務省・法務省・経済産業省)の Q&Aを素直に解釈すれば、推定が得られると期待されます。

（※）参考　リモート署名ガイドライン（JNSA、2020/11/2） https://www.jnsa.org/result/jt2a/2020/index.html　電子署名Q&A（JNSA、2020/9/16）https://www.jnsa.org/result/e-signature/e-signature-qa/

2．HPKIの鍵預かりとリモート署名について

（参考）　電子署名Q&A抜粋

Q18. クラウド署名とはなんですか？

A. 一般にクラウド署名は、ローカル署名方式と対比して、ネット上のサービスとして署名機能を提供するものです。リモート署名もその一種ですが、他にも色々な方式があります。

Q19. リモート署名とはなんですか？どういう利点がありますか？

A. ローカル署名では秘密にする署名鍵を自分で管理していますが、リモート署名では署名鍵をリモート（サーバ）上で管理して、利用時にどこからでも利用者の認証によって署名することが可能になります。またJNSAの関連団体JT2Aから ガイドラインも公開されていますので安心して利用できます。リモート署名を利用することで、デジタル署名の利用が簡単になります。

Q20. 事業者署名型(第三者署名型)の電子契約サービスとはなんですか。

A. 利用者がサービス提供事業者のサイトに電子文書を送信し、当該サイト上で利用者の意思表示等の操作記録を残すことにより電子契約を成立させるサービスです。 当該電子文書や操作記録に対して利用者の指示に基づき、サービス提供事業者の署名鍵により暗号化されます。なお、立会人型署名と呼ばれることもあります。

参考：電子署名法の主務３省(総務省・法務省・経済産業省)の Q&Aでは、技術的・機能的に見て、サービス提供事業者の意思が介在する余地がなく、利用者の意思のみに基づいて機械的に暗号化されたものであることが担保され、電子文書について行われた当該措置が利用者の意思に基づいていることが明らかになる場合には、これらを全体として１つの措置と捉え直すことにより、「当該利用者の電子署名」（電子署名法第２条第１項第１号）の要件を満たすことになるものと考えられる旨が示されています。

Q21. 本人型（当事者型）・立会人型署名とはなんですか？

A. 本人型（当事者型）署名とは、申請や契約の当事者のデジタル署名を用いる署名方法です。第三者型署名（立会人型署名）については、上記Q20を参照してください。

Q22. どのようなリモート署名サービスを使うべきですか？

A.　日本の法制度で求められる基準や認定はありませんが、JNSAの関連団体JT2Aが関係省庁のレビューを受け、電子署名法に準拠するレベルのリモート署名のための「リモート署名ガイドライン」を発行しています。これに照らして検討されることをお奨めします。

Q34. 立会人型署名でも電子署名法の推定は得られますか？

A. 電子署名法主務3省(総務省・法務省・経済産業省)の Q&Aによれば、サーバ等が本人の指示に基づいて、第三者の意思の介在しない形で自動的に署名を生成する場合には、一定の条件のもとで本人の電子署名として認められると考えられます。このQ&Aにより電子署名法第3条の推定効の認められる可能性が出てきたと思われます。9月4日の Q&Aには、推定効の条件についての見解が示されました。同3条が適用されるためには、本人による電子署名であることと、同3条かっこ書き※を満たす必要があります。このうち、同3条かっこ書きを満たすためには、電子署名のプロセスについて次の2点が要件とされてます。

①利用者による指示であることについて、2要素認証などの安全な方法で確認すること

②事業者の行うプロセスについて十分な固有性を満たされていること

ただし、①及び②の具体的要件は必要条件も十分条件も示されていませんので、どの程度の運用やシステムであれば良いかは現時点では判断できません。

※かっこ書き=「当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。」

（※）参考　電子署名Q&A（JNSA、2020/9/16）https://www.jnsa.org/result/e-signature/e-signature-qa/

本日の論点

令和５年１月より電子処方箋の仕組みを運用開始するにあたって、電子署名にはHPKIが活用される。その際、ローカル署名に加えて、リモート署名の仕組みの準備も進められている。

リモート署名の実現にあたっては、①HPKIの鍵預かりとリモート署名の評価体制、②電子処方箋に用途を限定させること　の２点を論点としたい。

（論点１） HPKIの鍵預かりとリモート署名の評価体制について

- あるべき姿と当面の進め方

（論点２）電子処方箋に用途を限定させることについて

- 署名用証明書への対応策

3．（論点１）HPKIの鍵預かりとリモート署名の評価体制

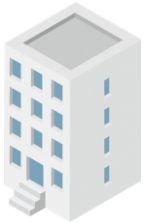
電子処方箋におけるリモート署名の活用については、喫緊の課題として「鍵預かり」と「リモート署名」が必要となる。ただし、HPKIにこれまで無かった「鍵預かり」と「リモート署名」の機能を設けるには、それに応じた評価体制が必要となる。ここでは、評価体制のあるべき姿を示す。

A．あるべき姿

「鍵預かり」と「リモート署名」を行うにあたり、セキュリティを担保するためのあるべき姿は、「鍵預かり」および「リモート署名」の運営主体は、安全性等の第三者評価に合格することに加え、HPKI認証局が選択を予定する「鍵預かり」運営主体の妥当性の判断に「鍵預かり」運営主体が行う「リモート署名」運営主体の妥当性の判断を含め、「リモート署名」運営主体には、原則として第三者評価されていることを要件とする形となる。

<HPKI専門家会議>

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）**

各運営主体が原則として第三者評価を受けていることを確認した上で妥当性を判断して選定

<「鍵預かり」運営主体>

安全性等の第三者評価に合格している

<「リモート署名」運営主体>

３．（論点１）HPKIの鍵預かりとリモート署名の評価体制

現状においては、あるべき姿に必要な第三者評価（評価基準）はまだ定まっていない。これを踏まえ、HPKI専門家会議及び作業班において、評価基準案の作成と妥当性の確認を諮ることが考えられる。現時点では評価基準案が無いため、運営主体より提出される安全性に関する文書の妥当性を確認することとしてはどうか。

B1.　専門家会議にて各運営主体が提出した安全性に関する文書を確認

時期：B2にて評価基準が作成され、認証局が準拠性審査で承認されるまでの間

1．各運営主体が安全性に関する文書を認証局へ提出

2．認証局がHPKI専門家会議に当該文書を準拠性審査の中で提出

3．HPKI専門家会議にて、当該文書の安全性を確認

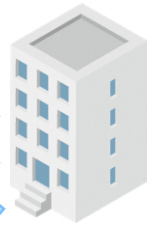
（準拠性審査）

・専門家会議作業班での検討に、当事者である認証局は入らない

・第三者評価が確立した際には、”準用”を外すことを検討する
（変更の際には電子証明書を切り替える）

＜HPKI専門家会議＞

運営主体より提出される安全性に関する文書の妥当性を確認



＜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）

各運営主体が安全管理方策、署名方法等の文書を提出

＜「鍵預かり」運営主体＞

現状において
第三者評価（評価基準）
が定まっていない

＜「リモート署名」運営主体＞

3．（論点１）HPKIの鍵預かりとリモート署名の評価体制

今後、HPKI専門家会議にて評価基準が作成され、認証局が準拠性審査で承認された際には、改めて評価基準に基いた監査を実施する。

B2. 専門家会議にて評価基準を作成し、監査実施

1．HPKI専門家会議にて電子処方箋に限定し、HPKIを準用する評価基準を作成する。

- 「HPKIを準用するための鍵預かり」基準
- 「電子処方箋用リモート署名」基準

2．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する。

3．専門家会議にて、２の選定の妥当性を確認（準拠性監査）

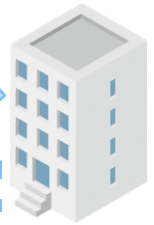
（留意事項）

・専門家会議作業班での検討に、当事者である認証局は入らない

・第三者評価が確立した際には、”準用”を外すことを検討する（変更の際には電子証明書を切り替える）

<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、評価基準案を元にサービスを確認した上で選定

<「鍵預かり」運営主体>

現状において第三者評価（評価基準）が定まっていない

<「リモート署名」運営主体>

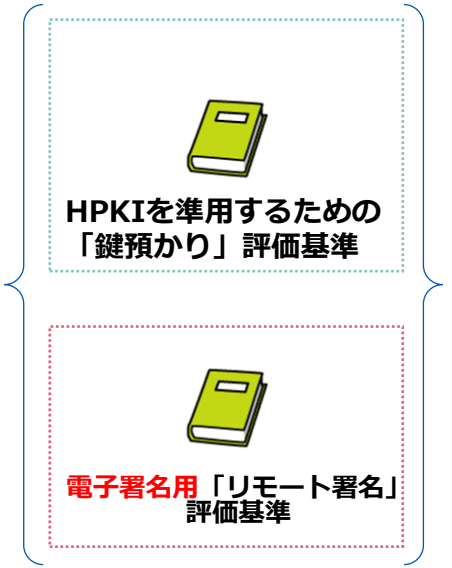
（論点１）
現時点では、A（あるべき姿）のリモート署名に関する第三者評価がないため、当面の間、B1,B2の評価体制とすることでどうか。

３．（論点１）HPKIの鍵預かりとリモート署名の評価体制

HPKI専門家会議にて作成する評価基準は、「HPKIを準用するための鍵預かり（鍵預かり）」と「電子処方箋用リモート署名（リモート署名）」に分けて考えることとしてはどうか

- 現時点では、「鍵預かり」は１つ、「リモート署名」は電子処方箋用に１つが想定されている。
- 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）。
- 「リモート署名」は、電子処方箋用の他、紹介状用等、他のサービス提供希望者が現れることも想定される。第三者機関が立ち上がる前に、電子処方箋と同様に医療側ニーズが高い他サービスの運用開始を求められた場合、新たなニーズ用のリモート署名の評価基準等を作成する必要がある。

セットにしてしまうと新たなニーズ毎に「鍵預かり」の評価基準を作成する必要がある。



上記を踏まえ、評価基準も「鍵預かり」と「電子処方箋用リモート署名」を分けて検討することにより、専門家会議作業班での作成作業や、認証局での評価作業も実施しやすくなると想定される。

電子処方箋のような新たなニーズが生まれれば、新たなニーズ用のリモート署名の評価基準を議論・作成する。

３．（論点１）HPKIの鍵預かりとリモート署名の評価体制

HPKI専門家会議にて作成する評価基準は、「HPKIを準用するための鍵預かり（鍵預かり）」と「電子処方箋用リモート署名（リモート署名）」に分けて考えることとしてはどうか

- 「鍵預かり」は、汎用的な側面を有する。
- 「電子処方箋用リモート署名」は、オンライン請求NWと支払基金への限定接続等により、限局されたサービスになると認識。
- 「鍵預かり」と「電子処方箋用リモート署名」が一体的に進めることにより、「鍵預かり」も電子処方箋専用となる可能性が出てくると想定。
- 「鍵預かり」部分を先行して協議して妥当性が確認され、「鍵預かり」のみサービスインしても「電子処方箋用リモート署名」の妥当性が判断されなければ、現実的には2nd鍵を利用できない。

上記を踏まえ、評価基準の作成に当たっては

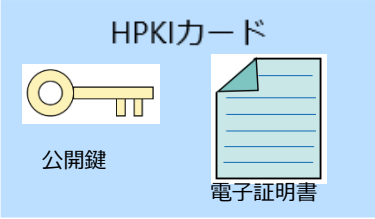
「鍵預かり」と「リモート署名」を分けて検討することとしてはどうか

４．（論点２） 署名用証明書の用途を限定させる方法について

電子処方箋限定でリモート署名を行うには、署名用証明書の用途を限定させる必要がある。原則、鍵預かりサービスにて閉域網（オンライン請求NW）の中で利用され、電子処方箋のみに利用されると考えられる。

万一、閉域網の外に署名が流出した際に、用途限定であることが分かるようにしておく必要がある。

そのためには、（A）と（B）の２つの方策がある。



方策	留意点
（A） 証明書のプロファイルにて、セカンド鍵であることを記述する。	署名単体では「セカンド鍵であり電子処方箋限定用途とする」であることが読み取れない。
（B） 証明書のプロファイルの拡張領域にて「電子処方箋限定用途とする」と記述する。	認証局のIAの改修が必要であり、設計に時間及び費用を要する。

（論点２）

今回は、原則閉域網のみで利用されることを想定することから、（A）の方式で進めることとしてはどうか。

なお、CPSにて、セカンド鍵は電子処方箋限定用途であることを記述することとしてはどうか。

５．今後の予定

令和５年１月の電子処方箋の運用開始にあたり、日薬CPSは年内の承認が必要である。

本会議後、書面審査を進めることとしたい。

○12月19日（月）

HPKI専門家会議・作業班合同開催（本日）

電子処方箋のご説明、MEDISの鍵の預託・リモート署名の仕組みのご説明、評価体制の審議

○12月28日（水）までに

HPKI専門家会議・作業班にて、審議した評価体制を元に、鍵預かり運営主体提出の評価シート及び日本医師会サブ認証局及び日本薬剤師会サブ認証局のCPSの書面審査/承認

○1月以降

「HPKIを準用するための鍵預かり」基準、「電子処方箋用リモート署名」の基準案を審議、審議するための専門家会議体制の検討