医師資格証の現状と今後の展望について

厚生労働省補助事業　保健医療福祉分野の公開鍵基盤HPKIセミナー

2025年3月1日

日本医師会電子認証センター
矢野　一博

Agenda

1. この1年間のアップデート

2. HPKIをめぐる動向

3. 今後の気になる動向

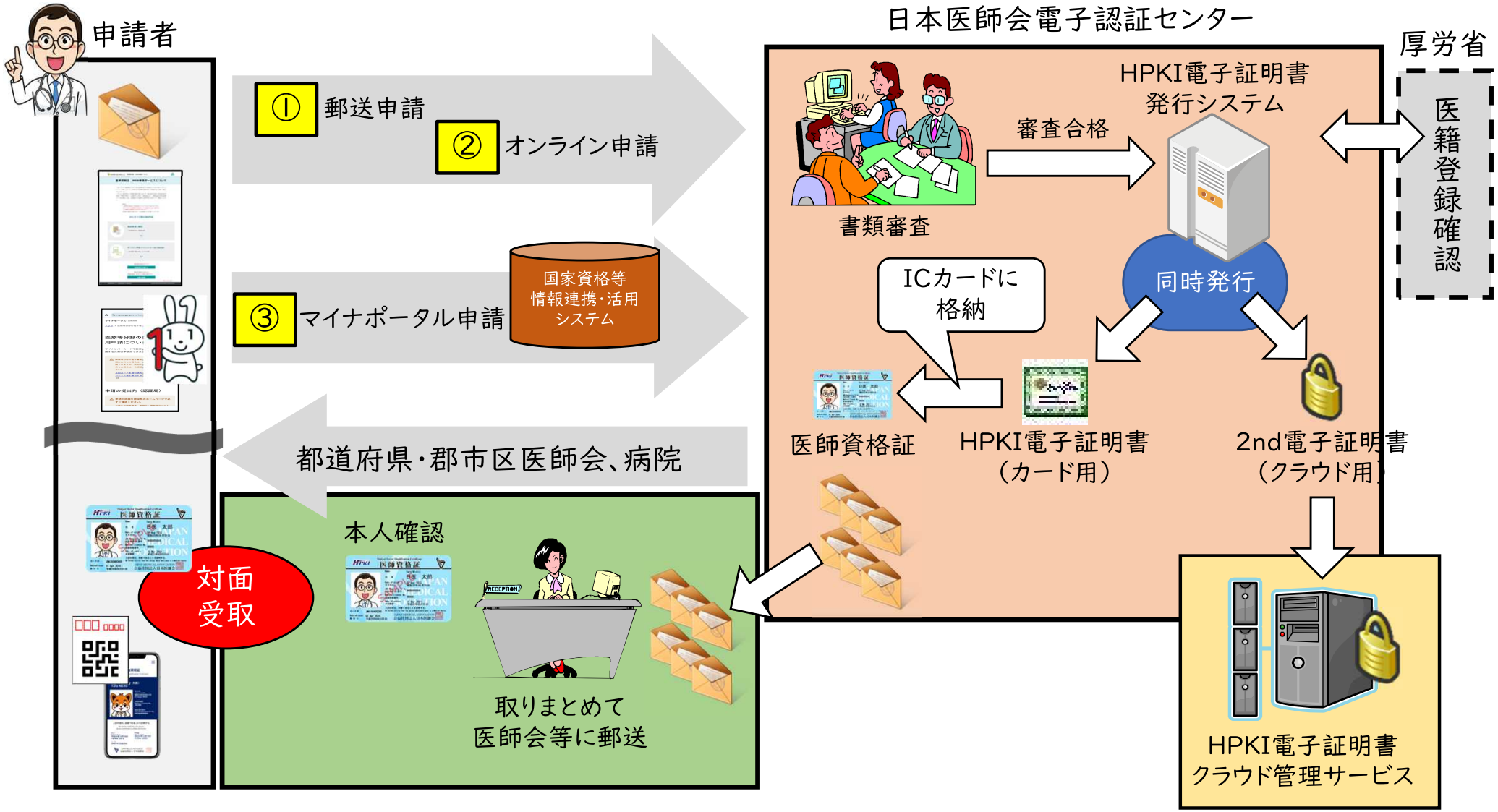
Agenda

1. この1年間のアップデート

2. HPKIをめぐる動向

3. 今後の気になる動向

医師資格証の申請方法の多様化



① 紙の郵送による申請（WEBを使った申請書作成支援を含む）。住民票の同梱必須。

② WEBの入力フォームに必要事項を入力、必要な添付書類をアップロード。マイナンバーカードでJPKI署名して申請。住民票の省略可能。

③ マイナポータルを経由して申請。申請時に国家資格等情報連携・活用システムで医師資格を予め確認。全ての添付書類を省略可能であるが、現在のところ住民票のみ省略可能。

日医発第16号（情シ）
令和6年4月2日

都道府県医師会 担当理事 殿

日本医師会 常任理事
長島 公之
（公 印 省 略）

HPKIセカンド電子証明書の先行発行および
デジタル医師資格証の公開について

令和5年6月～10月にICカード在庫不足のためセカンド電子証明書のみの先行発行を実施したが、再び在庫が不足し、現在、セカンド電子証明書のみの先行発行中

会務の運営に特段のご理解、ご支援を賜り厚く御礼申し上げます。
から10月にかけてHPKIセカンド電子証明書のみの先行発行を実施していたところ、ICカードが確保
医師資格証（ICカード）の発行再開について（令和5年10月16日付日医発第1283号（情シ））」の
の発行を再開しておりました。また、先行発行した先生方の医師資格証の発行を令和5年11月より
す。
後も継続して多くの申請をいただいたことから、**確保したICカードの在庫が再び残り僅か**になっています。
ICカードの ます。
そのため、 り替え
させていた
ただし、 ります
ので、そち
なお、す ードに
ついては、本年6月末日までに発行が完了する予定です。
（参考資料1：HPKIセカンド電子証明書を先行発行した方へのICカード発送目安）
加えて、スマートフォンで医師資格証の表示ができる『デジタル医師資格証』を公開いたしましたの たします。HPKIセカンド電子証明書のみ先行発行された先生も利用できますので、医師資格証がお手元にない際の代替手段としてご活用ください。また、デジタルの特性を生かし、券面だけでなく生涯教育講習の受講履歴や取得単位の確認もできますので併せてご利用ください。（参考資料2：「デジタル医師資格証」のご案内）
本件に関してご迷惑をおかけしますが、貴会におかれましてもご了知いただくと共に、貴会管下の郡市区等医師会ならびに会員への周知方につき、ご高配を賜りますようお願い申し上げます。
なお、医師資格証（HPKI カード）の発行を再開する目途が立った際は、改めてご案内することを併せて申し添えます。

以上

デジタル医師資格証の開発

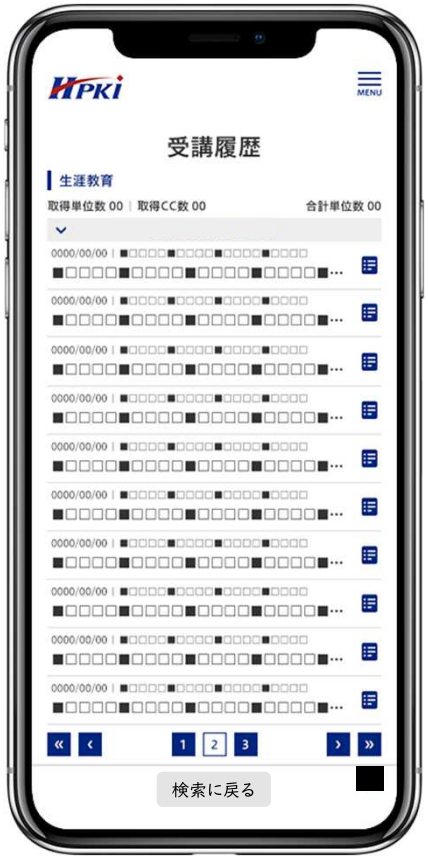
- 医師資格証の申請情報を元に、医師資格証と同等の券面（顔写真を含む）をスマートホン上に表示します。
- ログインには、HPKIセカンド電子証明書で用いる生体認証を利用して、なりすましを防止しています。また、画面を偽造できないように画面が定期的に光るようになっています。
- 生涯教育講座とかかりつけ医機能研修の受講履歴や取得単位の確認が可能です。
- 各種のお知らせをPush型で通知できます。
- HPKIセカンド電子証明書を用いて、電子処方箋にHPKI電子署名をする際のQRコード読み取りに対応しています。
- 今後、更に機能追加を予定しています。（例：講習会受付用のQRコード表示、学会の講習会との連携による受講履歴等の表示、マイナンバーカードの読取機能など）

デジタル医師資格証

TOP画面

メニュー表示

研修会受講履歴



お知らせ通知

ICカード不足への対応だけでなく、デジタルの特性も
生かして様々なサービスを付加することで、
医師資格証（HPKI）の多様性を目指すコンテンツ。

ただし、HPKIセカンド電子証明書の発行が前提

（昨年のセミナースライド再掲）

HPKIとマイナンバーカード（JPKI）のコラボ

- HPKI（カード&セカンド）による電子署名は「本人＋医師」と資格の証明ができるが、マイナンバーカードは本人の確認はできても資格の確認ができない。
- ただし、確実な本人確認手段（認証手段）として、マイナンバーカードは優れている。

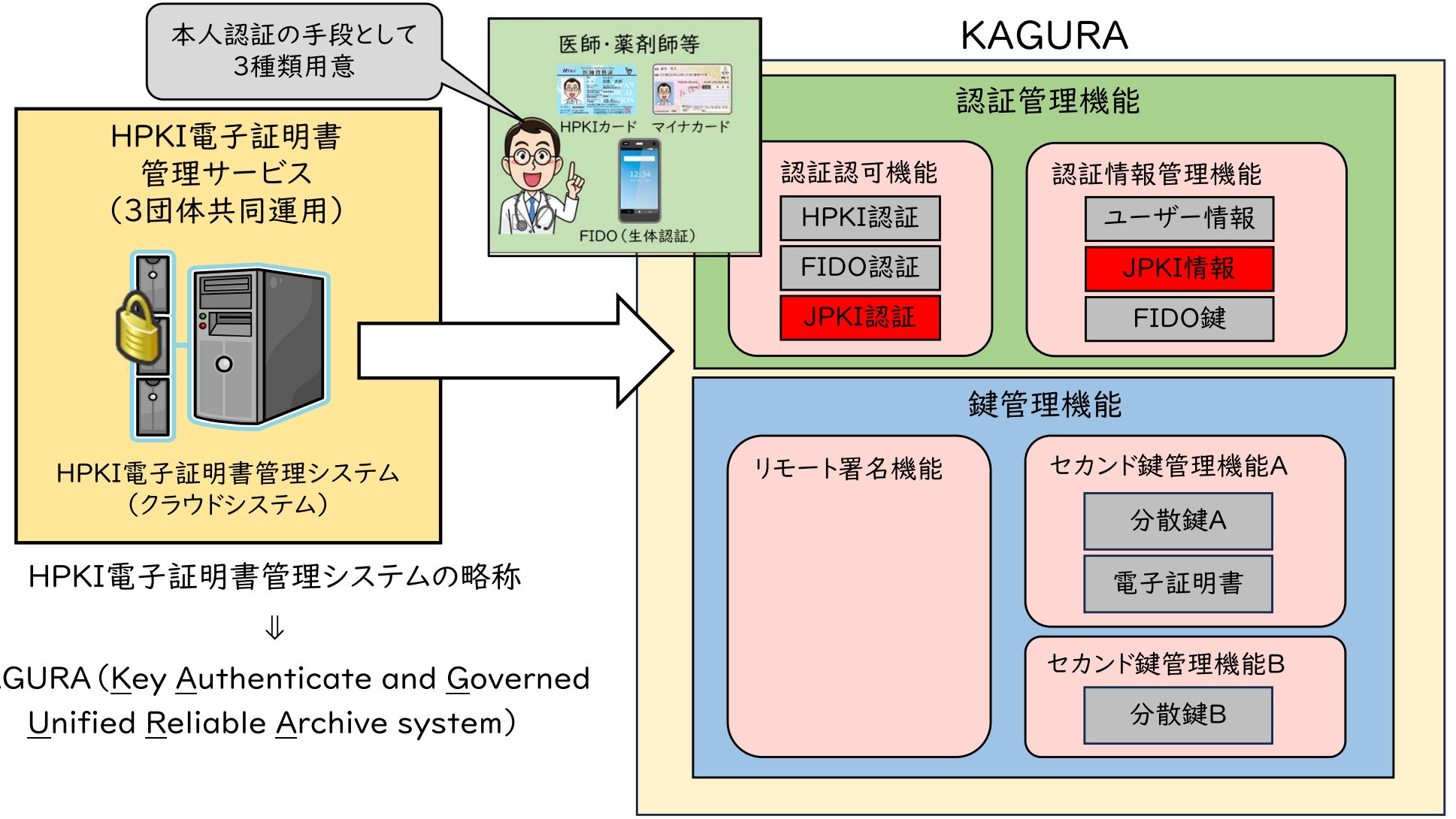
2023年12月27日
マイナポ受付開始！

HPKIセカンド電子証明書を使う時、

- 確実な本人確認手段としてマイナンバーカードを用いて認証
- その上でセカンド電子証明書を使ってHPKI電子署名をする

対立する必要はなく、双方の利点を生かした共存と相互利用を実現。

もう一度、HPKI電子証明書管理システム（KAGURA）の中身



HPKI電子証明書管理システムの略称

⇓

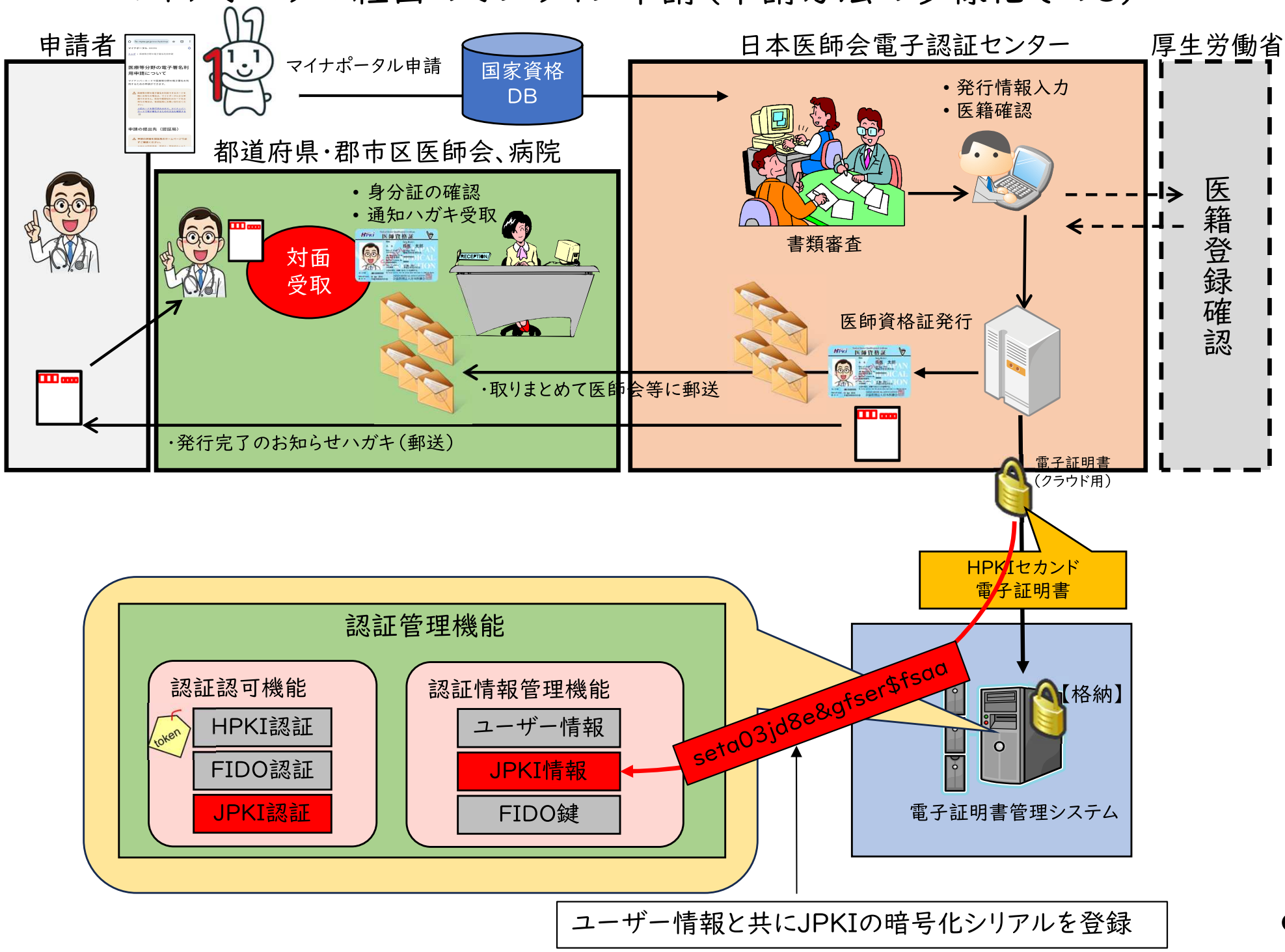
KAGURA（Key Authenticate and Governed Unified Reliable Archive system）

大きく「認証管理機能」と「鍵管理機能」に分かれる。

- 認証管理機能：HPKI認証およびFIDO認証の機能と本人ID／資格／証明書発行者／FIDO鍵等を本人ID と紐づけて管理する機能
- 鍵管理機能：セカンド電子証明書／分散鍵を本人IDと紐づけて管理する機能と本人IDに対応したセカンド鍵（分散鍵Aと分散鍵B）を用いた署名値の作成を行う機能

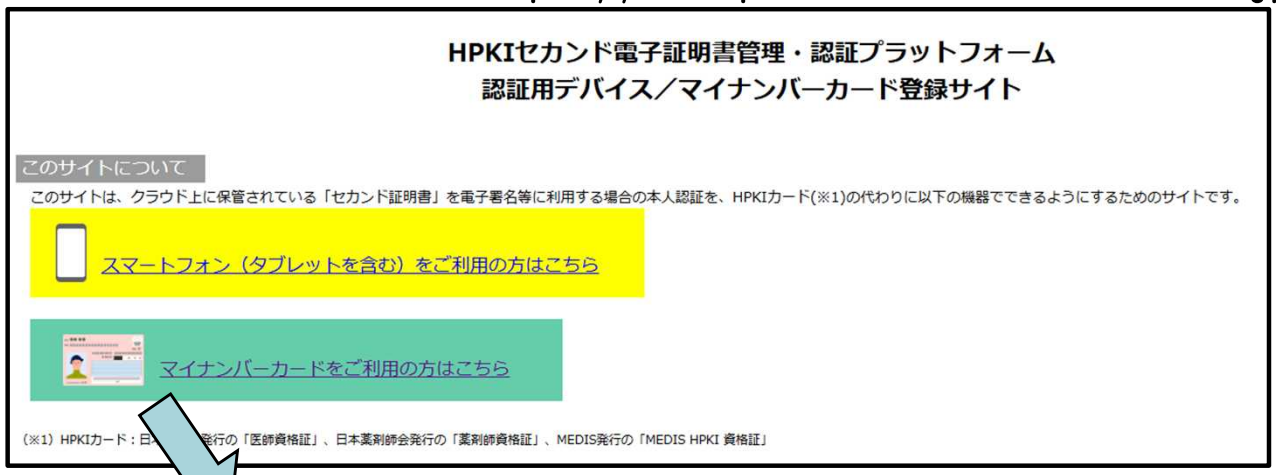
（JCMI43スライド再掲）

マイナポータル経由のオンライン申請（申請方法の多様化その3）



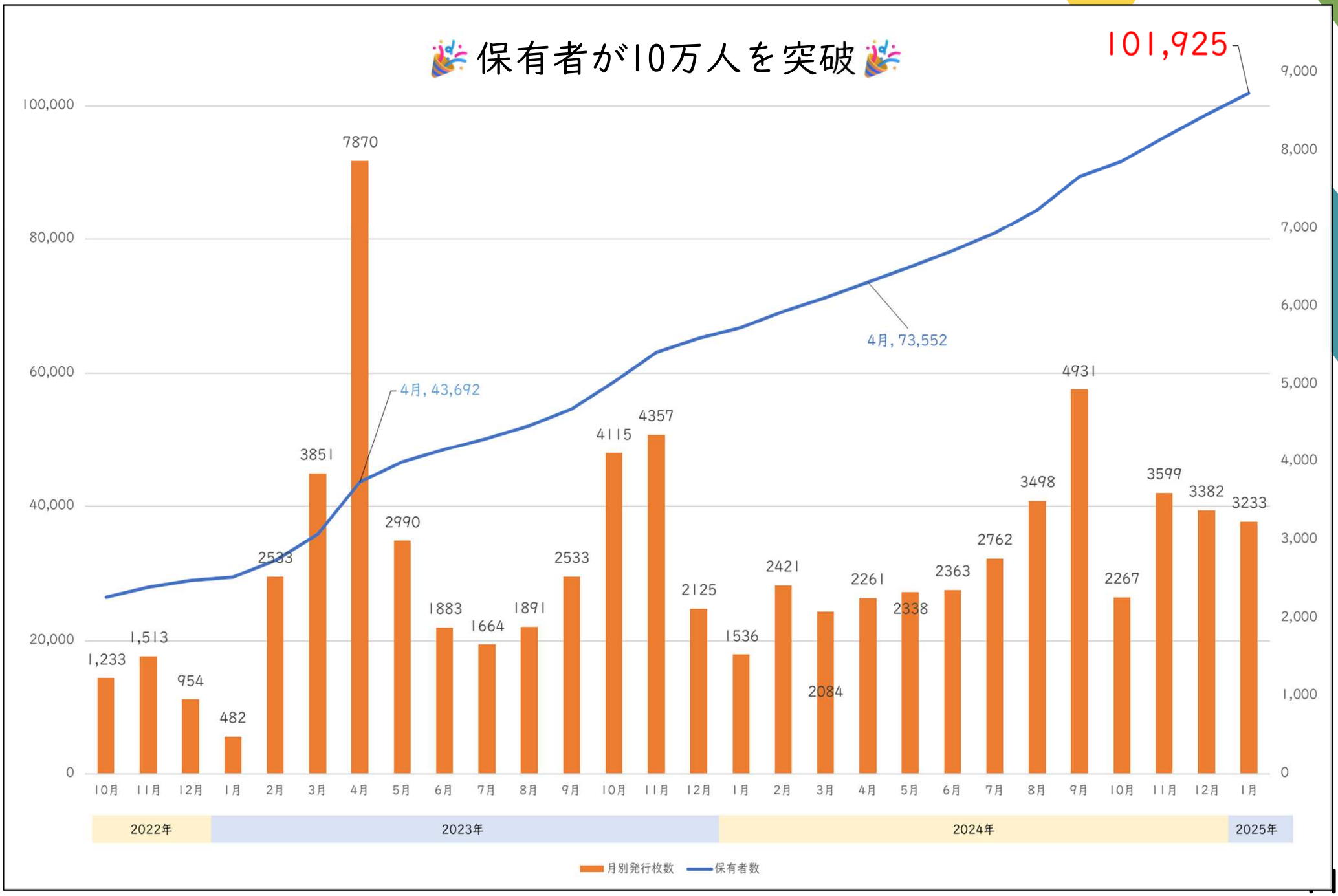
HPKIカードを使った後から紐付けも可能

HPKIカードが手元にある場合は、以下のサイトからマイナンバーカードと後から紐付けも可能
https://mahpki-srv.2nds.medis.or.jp/index.html



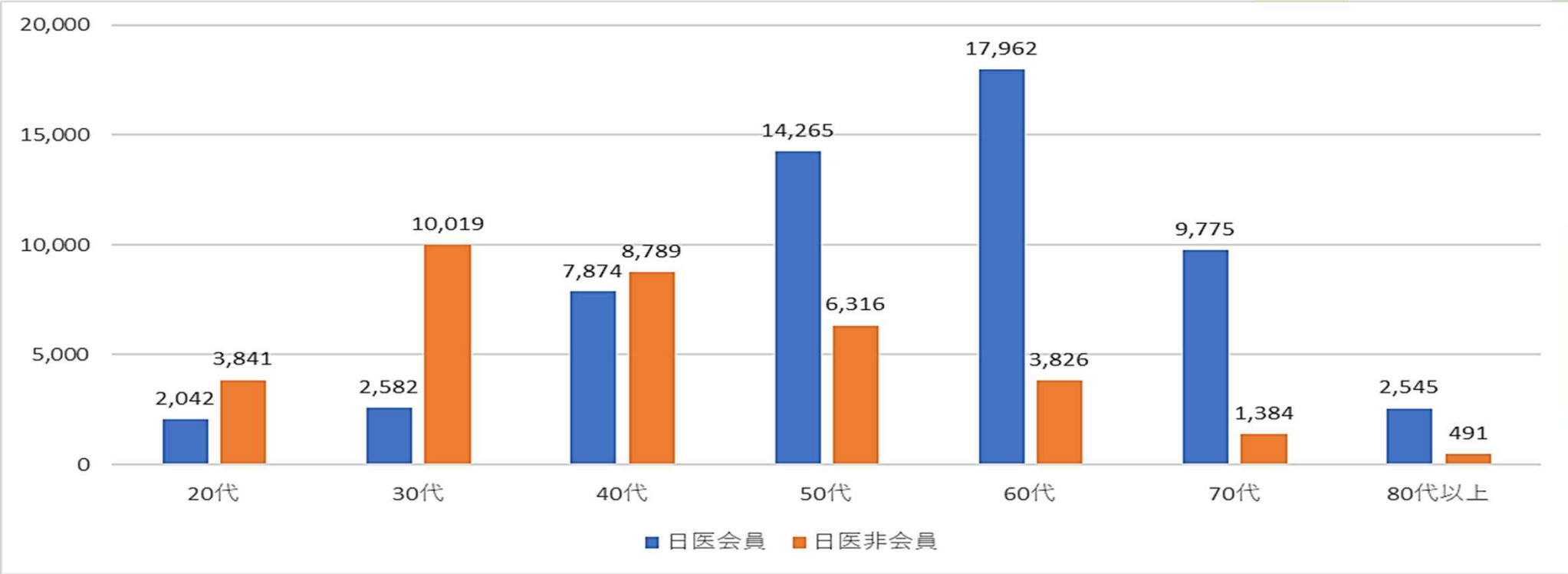
医師資格証（HPKIカード）発行推移
（2025年1月末現在）

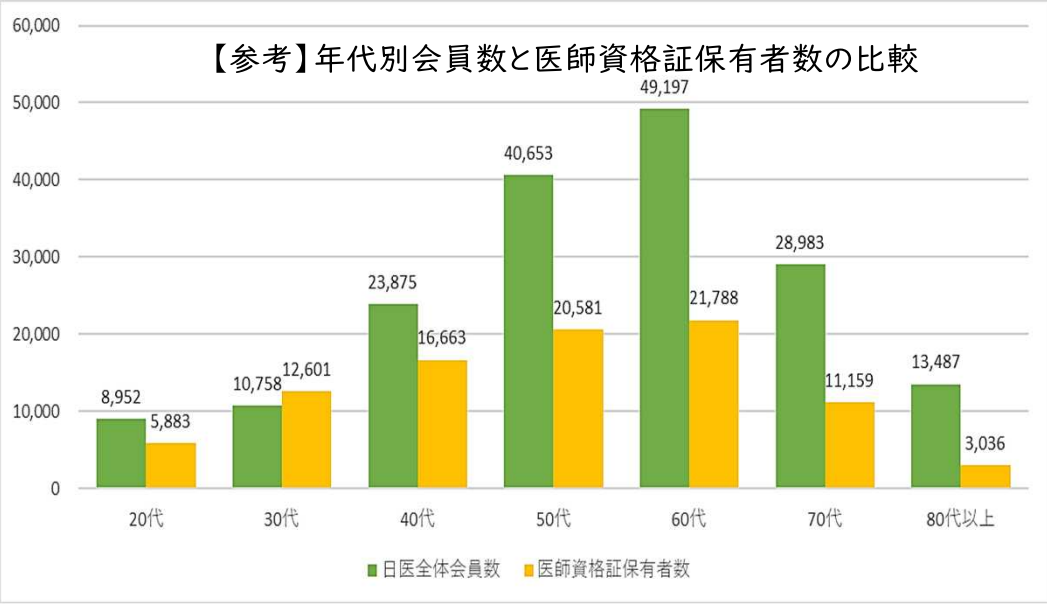
日医会員取得率：34.9%
全国医師取得率：29.7%



【ちょっと中身を分析】医師資格証の年齢階級別保有者分布

年代別医師資格証保有者数【会員／非会員別】





- 非会員の医師資格証の保有者は若手が多い。
- 一方、会員の保有者数と全体の保有者数で比較すると、日医の会員年齢分布と同じ傾向。

- これまでの日医会員向けのサービスという捉えられ方から、電子処方箋の影響などにより、（本意ではなくとも）医師が使うサービスとなりつつあるのではないか。
- なお、デジタル医師資格証のダウンロード数は、13,084人（'24/11/19 15:00）であり、こちらも多くは若手が利用しているのではないかと推測される。

Agenda

1．この1年間のアップデート

2．HPKIをめぐる動向

3．今後の気になる動向

Agenda

1．この1年間のアップデート

2．HPKIをめぐる動向　①デジタル資格者証

3．今後の気になる動向

デジタル資格者証の発表

【スマホのマイナポータル画面】

【印刷用PDF】

デジタル庁の資料から抜粋

医師の場合に想定される記載事項例（デジタル庁資料から）	
資格名称（医師）	QRコード
氏名	交付機関名（厚生労働省）
生年月日	本人写真（医師の場合なし）
登録番号	その他項目
登録日	

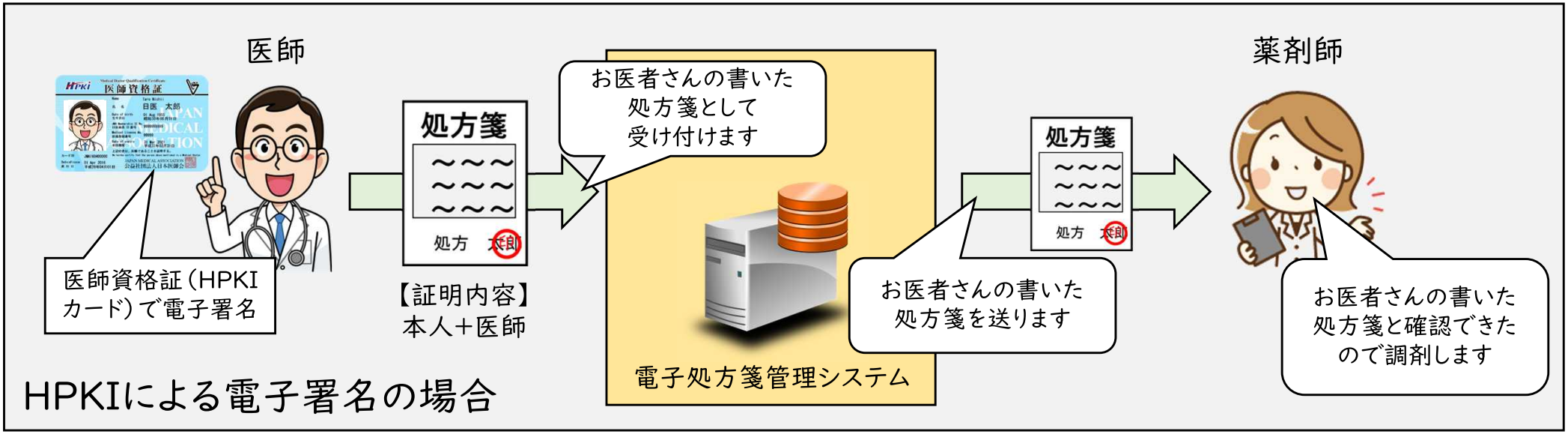
※あくまでデジタル庁の資料から想定したもの

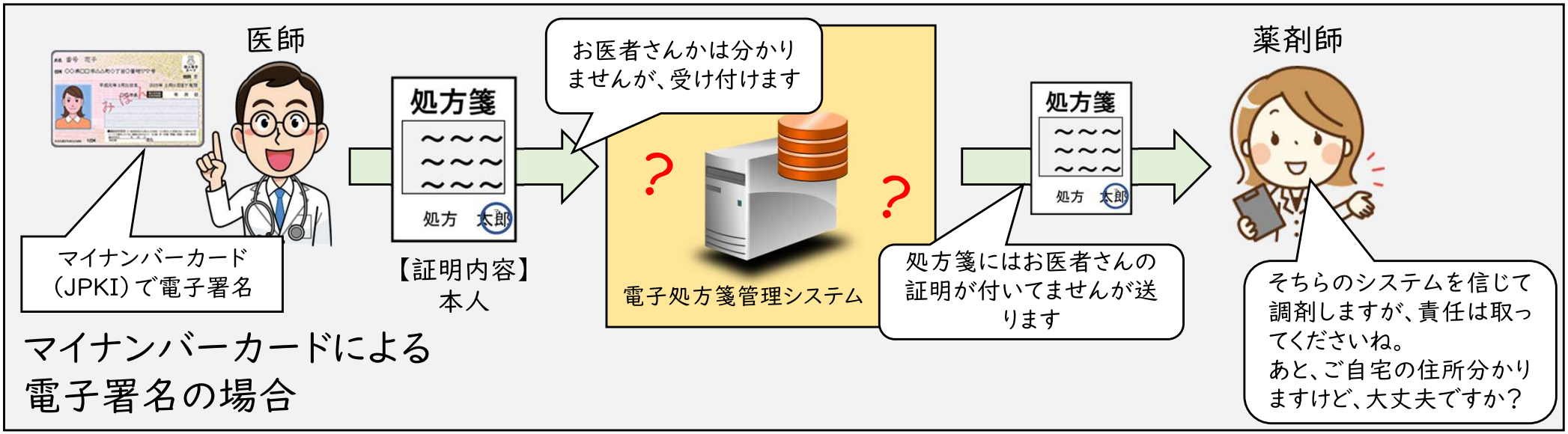
- 2024年8月6日から「国家資格のオンライン・デジタル化」を開始すると発表（医師は今夏頃まで延期）
- 国家資格に係る手続きを、マイナポータルを通じてオンライン申請できるようにするための仕組み
- 機能のひとつとして「デジタル資格者証」を取得することができる

⇩

（一部で）再びHPKI不要論（何回目だ。。。）

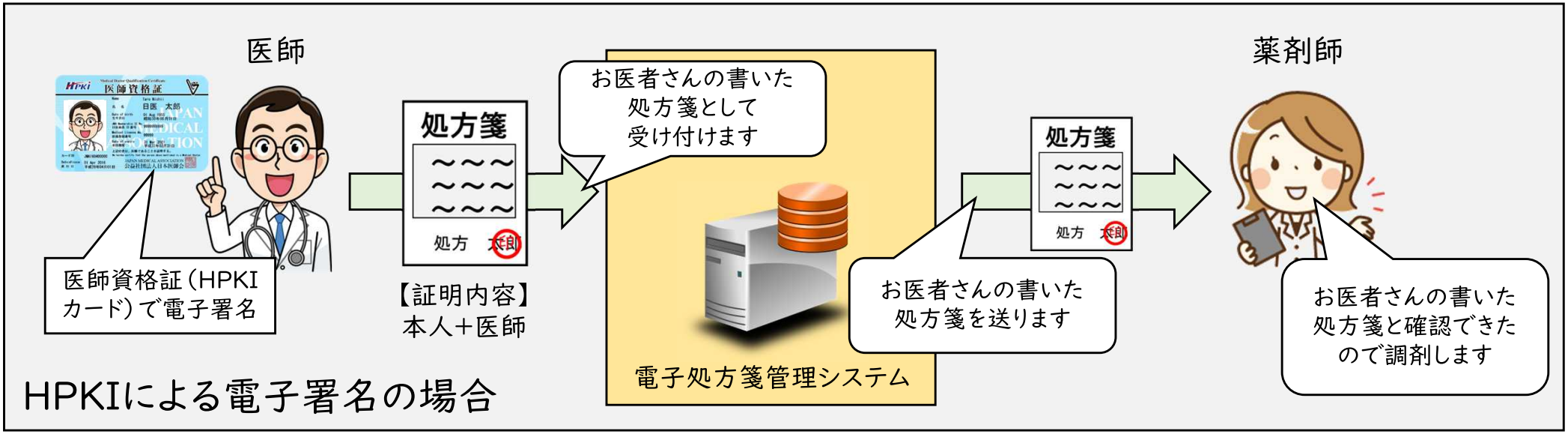
HPKIとJPKIでの電子署名対比
（電子処方箋を例として）

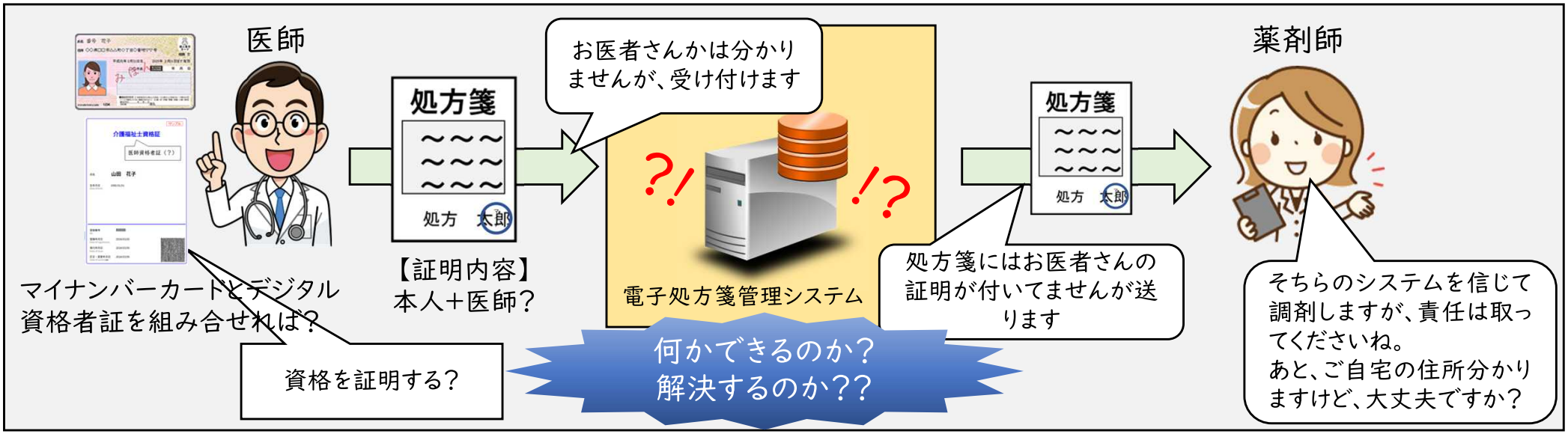




これ自体は特に何か変化があった訳ではないが

HPKIとJPKIでの電子署名対比
（電子処方箋を例として）





考えられなくはないけど、公的個人認証法もあって、そのままでは無理です。。。

医師資格証とマイナンバーカード

		医師資格証	マイナンバーカード
券面・発行者		 （表）  （裏）	 （表）  （裏）
		発行者：日本医師会	発行者：市区町村長
表面	主な記載事項	• 氏名 • 生年月日 • 日医会員ID（会員の場合） • 医籍登録番号 • 有効期限	• 氏名 • 住所 • 性別 • 生年月日 • 有効期限
	証明事項	本人であることに加えて「医師」であること ※公的な証明力は、厚労省通知（採用時の提示）の範囲	本人であること ※公的身分証明書
ICチップ（裏面）	格納情報	電子証明書（電子署名用・認証用） 医師等の資格	電子証明書（電子署名用・認証用）、顔写真データ 住民票住所 ※公的個人認証法第7条3項（住基台帳法第7条に定める事項）
	証明事項	電子的に本人であることに加えて「医師」であることの証明。 医師等の業務のために利用可能。	本人であること。 行政手続きに利用可能。
有効期限		券面および電子証明書（ICチップ格納情報）、いずれも5年	券面は10年、電子証明書（ICチップ格納情報）は5年

住基カードの時から、国民に厳密な認証を求めるのであれば、より厳密性が求められる医療情報を提供する医療資格者の認証がないのは著しくバランスを欠くという考えから検討が始まり、実現している仕組みがHPKI。

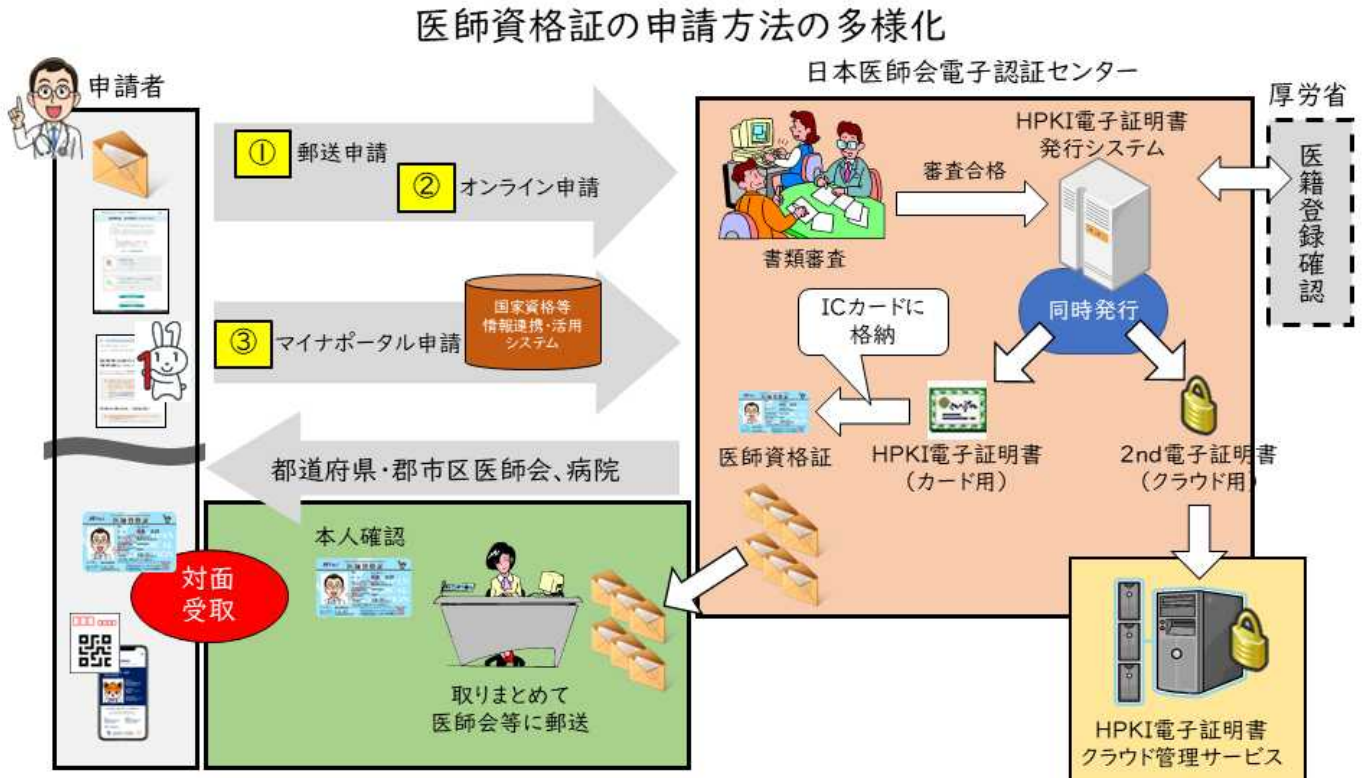
医師資格証とデジタル資格者証の共通点と相違点

	医師資格証 （デジタル医師資格証）	デジタル資格者証
医師資格の提示	○	○
本人の証明	○	×
電子署名	○	×
サービス	日医や医療分野に特化したサービスに利用。制度の組み方によっては、国民向けサービスにも利用可能	行政手続きを主として、国民向けサービスに利用

- 医師の資格を提示できることは共通であるが、デジタル資格者証では「本人であることの証明」や「電子署名」はできない。
- デジタル庁も「デジタル資格者証は提示された資格者証の有効性及び真正性を検証するものであり、当該資格者証が、それを提示した本人のものであることを保証するものではありません。本人確認が必要な場合は、別途マイナンバーカード等による確認を行ってください。」とホームページ上に明記している。

そもそも役割が異なる

再びコラボ？



デジタル資格者証

ここを有効に使う！

① 紙の郵送による申請（WEBを使った申請書作成支援を含む）。住民票の同梱必須。

② WEBの入力フォームに必要事項を入力、必要な添付書類をアップロード。マイナンバーカードでJPKI署名して申請。住民票の省略可能。

③ マイナポータルを経由して申請。申請時に国家資格等情報連携・活用システムで医師資格を予め確認。全ての添付書類を省略可能であるが、現在のところ住民票のみ省略可能。

- ①と②は、コピーであれ、画像のアップロードであれ、医師免許証の情報を元に厚労省へ医師資格保有確認をアナログで実施。
- ③の場合も医師免許証情報がないと真偽確認の方法がないため、現在は画像をアップロード。

デジタル資格者証の送付もしくは国家資格等情報連携・活用システムと直接API連携ができれば、完全ペーパーレスの申請が可能になる。

Agenda

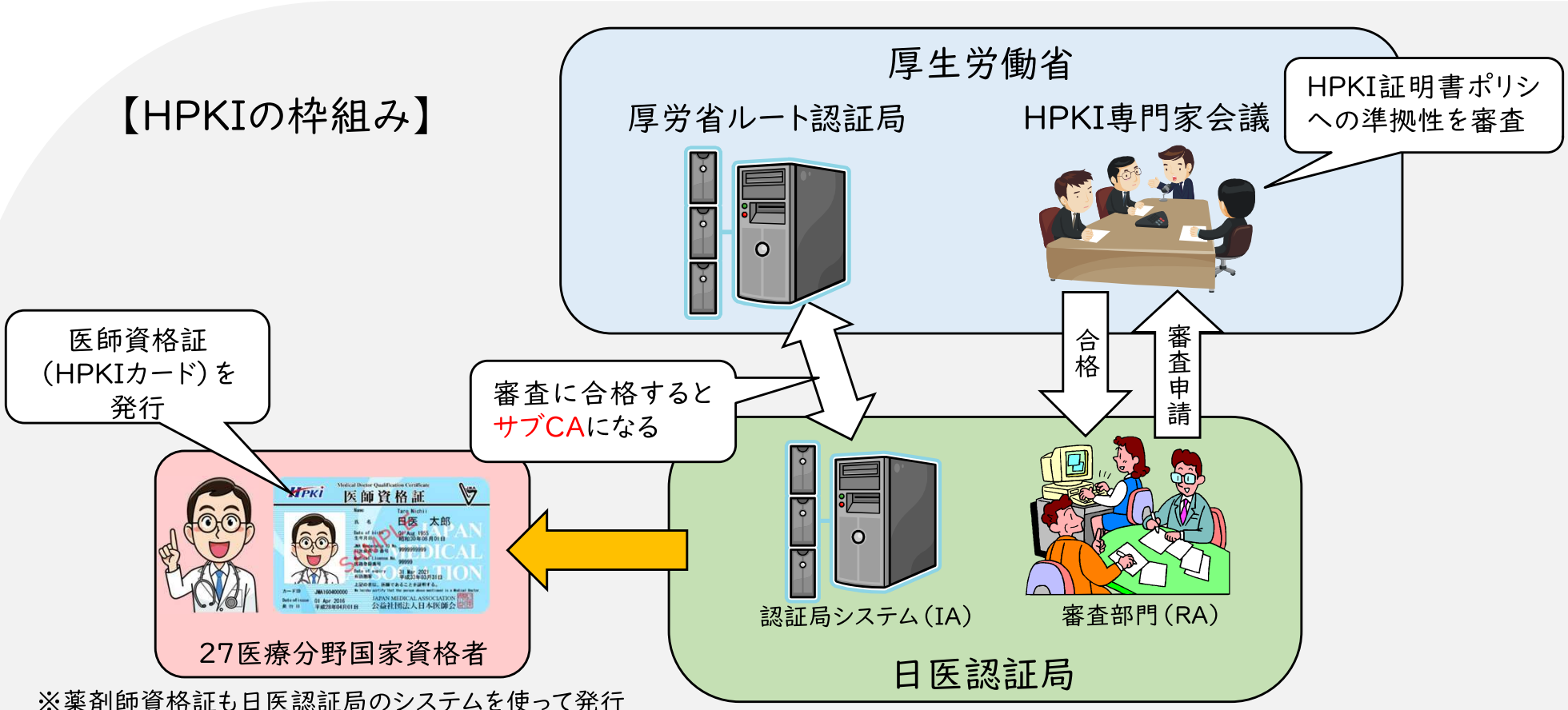
1．この1年間のアップデート

2．HPKIをめぐる動向　②サブCA（日医認証局）鍵更新

3．今後の気になる動向

日本医師会認証局について

- 日本医師会認証局は、厚生労働省の定める「保健医療福祉分野PKI認証局証明書ポリシ（HPKI証明書ポリシ）」に準拠して運用している認証局
- 準拠性は、厚生労働省による準拠性監査により担保されている
- 準拠性監査に合格しているので、HPKI認証局を名のることができ、厚生労働省ルート認証局の『サブ認証局（CA）』となっている

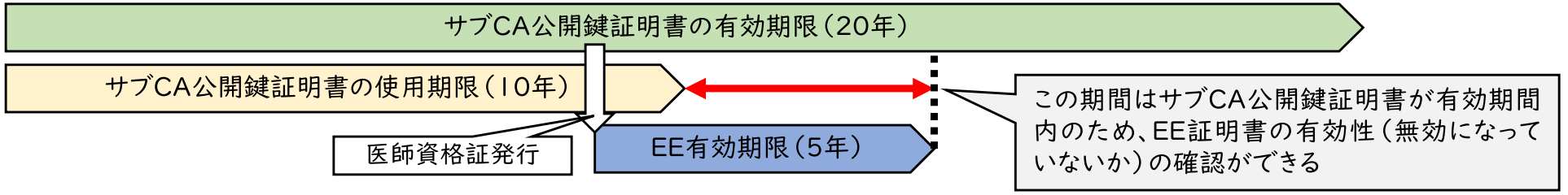


公開鍵証明書の有効期間について

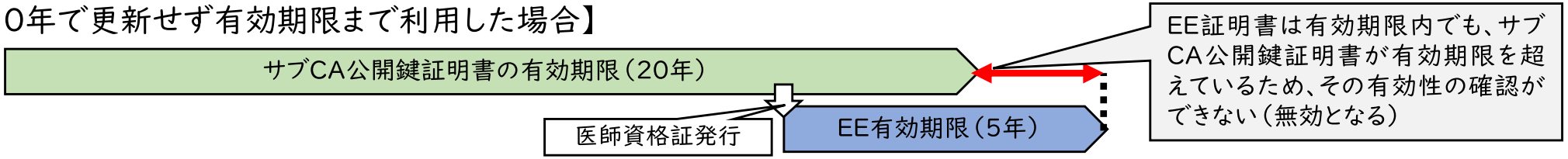
HPKI認証局の公開鍵証明書の有効期間は「HPKI証明書ポリシ」で定められていて、以下の通り。

- サブCA公開鍵証明書の有効期間
  - 有効期間は20年。ただし、その使用は10年を超えないものとする。
    - つまり、日医認証局（サブCA）の公開鍵証明書の有効期間は20年であるものの、使ってもよい期間（≒その認証局から医師資格証を発行してよい期間）は10年。
    - 有効期限が定められている理由は、暗号技術の進歩による安全性レベルの低下（危殆化）に対応するため。
    - 20年有効でも10年で更新するのは、医師資格証の有効期限（5年）内にサブCA公開鍵証明書の有効期限（20年）を迎えないようにするため。
      ※したがって、論理的には15年で更新しても問題はない。

【鍵更新の考え方】



【10年で更新せず有効期限まで利用した場合】



※EE：エンド・エンティティ＝医師資格証

日医認証局（サブCA）の鍵更新について

- 日医認証局（サブCA）の公開鍵証明書の開始日は「2014年1月17日」
- したがって、HPKI証明書ポリシに則れば「2024年1月16日」が使用期間の満了日
- このため、本来、既に鍵更新を実施していたはずのところ、鍵更新に係るHPKIとしてのルールの未整備やサブCAとして初めての鍵更新であったため、HPKI専門家会議での審議（2023年12月20日開催）の上で、最大「2024年7月16日」まで半年延長
- これを受けて、鍵更新の準備を進め「2024年5月30日」に鍵更新予定とした
- しかし、鍵更新は問題なくできるものの、準備の過程で、ベンダーが提供している電子署名の検証モジュールの一部に問題が生じ、鍵更新を強行すると電子処方箋を筆頭に影響が広範に及ぶ可能性が出てきた

HPKI専門家会議において、
「2024年5月30日」の鍵更新は、最大1年となる「2025年1月16日」まで再度延期され、その間のどこかで実施することになった

日医認証局（サブCA）の鍵更新について

＜前提＞

- 日医認証局（サブCA）はサブCAのため、トラストアンカーは厚労省ルートCAになる
- そのため、RFC4210で言及されている**リンク証明書**（OLD with NEW、NEW with OLD）は、ルート認証局の鍵更新の場合に発行するもののため、サブCAである日医認証局の鍵更新では**発行しない**。

＜鍵更新の流れ＞

① 新サブCAで新鍵ペアを生成後、厚生労働省HPKIルートCAから「新サブCA証明書」を発行

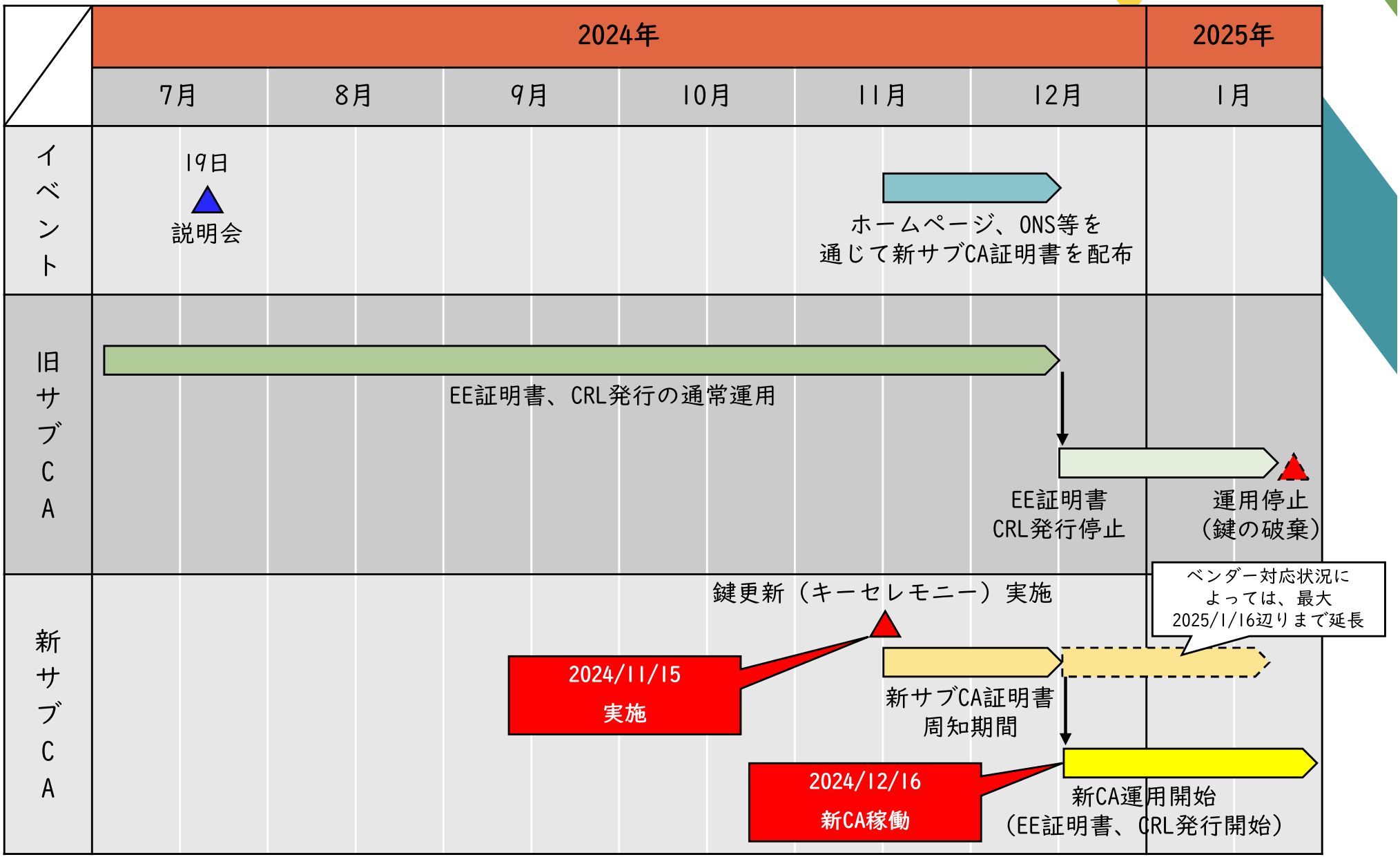
② 発行を受けても直ちに適用せず、一旦、旧サブCA証明書で運用継続

③ 日医電子認証センターのホームページ等で「新サブCA証明書」を公開、ダウンロード可能にして1カ月程度の周知期間を用意

④ 1ヶ月後を目途に鍵を切替（旧鍵の使用を終了し、新鍵でEE証明書やCRLを発行開始）

⑤ 新サブCA稼働後（概ね1ヵ月後）旧鍵を廃棄

日医認証局（サブCA）の鍵更新スケジュール



日医認証局（サブCA）の新中間証明書のダウンロード先

＜電子認証センターのダウンロード先URL＞
https://www.jmaca.med.or.jp/guide/agreement.html

＜厚生労働省からもダウンロード可能＞
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/pki-policy/repository.html
→サブCAの公開鍵証明書から

＜日本薬剤師会からもダウンロード可能＞
https://www.nichiyaku.or.jp/hpki/vendor.html
→◆中間CA証明書から

※ ただし、厚生労働省、日本薬剤師会のダウンロードは、署名用・認証用の証明書をZIPで固めたものを掲載。

※ 証明書の真正性は、電子認証センターのホームページでフィンガープリントを確認してください。

Agenda

1．この1年間のアップデート

2．HPKIをめぐる動向　③リモート署名利用限定解除議論

3．今後の気になる動向

HPKIセカンド電子証明書の電子署名は電子処方箋に限定

事　務　連　絡
令和５年１月 26 日

各 ［都道府県知事／保健所設置市市長／特別区長／地方厚生（支）局長］ 殿

厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室
厚生労働省医薬・生活衛生局総務課

HPKIのリモート署名における電子署名について

平素より厚生労働行政につきまして、格別のご理解賜り厚く御礼申し上げます。

厚生労働省では、データヘルス改革の一環として、令和５年１月より電子処方箋の運用を開始しております。電子処方箋の発行、調剤結果への記録の際、医師や歯科医師、薬剤師の資格確認が行われた電子署名を適切に付す必要があり、現時点では、保健医療福祉分野の公開鍵基盤（HPKI：Healthcare Public Key Infrastructure）の電子証明書を内蔵した IC カード（以下「HPKI カード」という。）が使用されているところです。

今般、HPKI カードの紛失・破損等に対応するためのリモート署名の取扱いに関して、下記の通りお示ししますので、貴職におかれては、内容を御了知の上、貴管下の医療機関、薬局等に周知いただくようお願いいたします。

記

地域における医療及び介護の総合的な確保の促進に関する法律（平成元年法律第 64 号）による電子処方箋の仕組み（以下「電子処方箋管理サービス」という。）については、本日、令和５年１月 26 日から運用開始となる。電子処方箋の発行の際又は電子処方箋に基づく調剤後においては、電子署名（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）（以下「電子署名法」という。）における電子署名をいう。以下、同じ。）が必要となるところであるが、現行の「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」（令和４年３月）における要件を満たす電子署名の仕組みとして、HPKI が存在する。HPKI には HPKI カードを用いて署名を行う方法と、HPKI カードを用いず署名を行う方法（以下「HPKI リモート署名」という。）があり、HPKI リモート署名については、HPKI カードの紛失・破損等に対応するために有用な方策である。

HPKI については、保健医療福祉分野公開鍵認証基盤専門家会議（以下「HPKI 専門家会議」という。）において、電子署名法第４条における特定認証業務と同程度の水準として監査を受検した認証局が、私有鍵を物理媒体（IC カード）に格納して交付することを前提として認められている。また、認証局が私有鍵の預託先の安全性などを確認した上で、HPKI カードの紛失、破損等の対応の有用性に鑑み、私有鍵を預託することも可能である。他方、我が国では、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存在しない。

そのため、今般の HPKI リモート署名においては、HPKI 専門家会議において定められる従来の HPKI と同等水準の安全性確保に求められる評価基準を用いた適切な評価が行われるまでは、各認証局が安全性を確認したリモート署名の運営主体において電子署名が付されることとなる。

他方、電子処方箋管理サービスを介した電子処方箋のやりとりについては、医療機関・薬局から社会保険診療報酬支払基金及び公益社団法人国民健康保険中央会のオンライン資格確認等システムのネットワークを介して閉域網の中で行われるものであり、電子処方箋は、限定された組織でのみ運用される。

また、預託された私有鍵を用いた電子署名に関しては、電子署名法第２条第１項第１号及び第２号に定められる要件を満たす場合、電子署名法上の電子署名に該当するものと解釈される。

以上のことから、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。

以上

（参考）

省・法務省・経済産業省、令和２年９月４日）
・リモート署名ガイドライン第一版（日本トラストテクノロジー協議会、令和２年４月 30 日）
https://www.jnsa.org/result/jt2a/2020/index.html
・電子署名 Q&A 第１版（NPO 法人 JNSA 日本ネットワークセキュリティ協会 電子署名ワーキンググループ、令和２年９月 16 日）
https://www.jnsa.org/result/e-signature/e-signature-qa/

以上のことから、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。

HPKI専門家会議で議論開始

【第28回HPKI専門家会議資料から（2024年6月20日開催）】

Ministry of Health, Labour and Welfare of Japan

1．認証局準拠性審査結果報告

審査：厚生労働省ルート認証局

審査：日本医師会認証局

審査：日本薬剤師会認証局

2．HPKIリモート署名サービスに関して

審議１：リモート署名サービス評価基準の今後の進め方について

審議２：リモート署名サービスの利用用途限定について

審議３：電子カルテ情報共有サービスにおけるリモート署名利用について

3．連絡事項

ひと、くらし、みらいのために

厚生労働省

Ministry of Health, Labour and Welfare

HPKI専門家会議で議論開始

【第28回HPKI専門家会議資料から（2024年6月20日開催）】

審議事項２
HPKIリモート署名サービスの利用用途限定について

第18回HPKI専門家会議（2022年12月）において「保健医療福祉分野におけるリモート署名サービス」については電子処方箋の用途限定が議論され、下記の通りの結論となっている。

- 電子処方箋はオンライン資格確認等システムのネットワーク（閉域網）の中で行われるものであり限定された組織でのみ運用されるため、暫定的にHPKIの利用を認めるものとする。
- また、第三者評価までは暫定的にHPKI専門家会議にてリモート署名基準を作成し監査を実施する。
- 用途限定の方法として証明書のプロファイルによる利用限定対応は行わず、代替として厚生労働省より自治体へ通知を出すことで周知を行う。

限定解除に向けての議論

どのような形であれば限定解除としてよいか、ご議論お願いします

- 第18回の専門家会議において第三者評価が必要としていたが、方針に変更はないか
- HPKI専門家会議によるリモート署名サービス基準での準拠性審査で代用はできないか
- その場合、リモート署名サービス基準をどこまで整備した時点で用途限定の解除を認める形にもっていってよいか
- 例えば今年度、リモート署名サービス基準の見直し、改定を行った後に準拠性審査を行った場合は用途を限定しないとしてはどうか
- 審査班は現状２名体制だが、今後増員やローテーション等進めていくべきか

（※審査班は専門家会議が指定することが条件ため、班員になるための制限等が現状ない）

HPKI専門家会議で議論開始

【第28回HPKI専門家会議資料から（2024年6月20日開催）】

審議事項３
電子カルテ情報共有サービスにおけるリモート署名の利用について

電子カルテ情報共有サービスへの対応

目前の対応として、厚生労働省が進めている医療DX施策のうち、「電子カルテ情報共有サービス」について**来年１月よりモデル事業**、来年度以降に本格運用開始を予定している

「電子カルテ情報共有サービス」では任意にて電子署名を求める仕様としており、電子処方箋同様にリモート署名を行えるものとしたい

審議事項２の結論次第だが、３月のMEDIS監査を待って限定解除となった場合１月のモデル事業時点で利用出来ないため、電子処方箋同様の扱いとして進めさせて頂きたい

審議事項

下記理由より**「電子カルテ情報共有サービス」は「電子処方箋」同様の扱いとしてリモート署名を利用してよいと考えるがどうか**

- オンライン資格確認等ネットワーク（閉域網）を利用することで電子処方箋はリモート署名の利用をよいとしている
- 電子カルテ情報共有サービスは電子処方箋同様に支払基金が実施主体となり、オンライン資格確認等システムの閉域網による接続となる

※リモート署名サービス評価基準では、電子処方箋に限定しているということの記載は元々していないため、電子カルテ情報共有サービスについては追記を行わない

周知方法

HPKIリモート署名について、電子カルテ情報共有サービスも利用可能であることを、電子処方箋で対処した際と同様に自治体向けに通知を発出し、医療機関等に周知することで、利用可としてはどうか

HPKI専門家会議で議論開始

【第28回HPKI専門家会議資料から（2024年6月20日開催）】

【参考】電子カルテ情報共有サービスの概要

令和６年６月版

❶ 診療情報提供書送付サービス：診療情報提供書を電子で共有できるサービス。（退院時サマリーについては診療情報提供書に添付）
❷ 健診結果報告書閲覧サービス：各種健診結果を医療保険者及び全国の医療機関等や本人等が閲覧できるサービス。
❸ 6情報閲覧サービス：患者の6情報を全国の医療機関等や本人等が閲覧できるサービス。
❹ 患者サマリー閲覧サービス：患者サマリーを本人等が閲覧できるサービス。

共有情報の詳細

文書情報	診療情報提供書	・退院時サマリーは診療情報提供書に添付扱い
	健診結果報告書	・特定健診 ・後期高齢者健診 ・事業主健診(一般定期健康診断) ・学校職員健診 ・その他健診
患者サマリー		・傷病名(主傷病＋副傷病) ・療養上の計画・アドバイス ＋薬剤アレルギー等、その他アレルギー等、感染症、検査、処方情報(電子処方箋)
臨床情報	5情報	・傷病名 ・薬剤アレルギー等 ・その他アレルギー等 ・感染症 ・検査(救急、生活習慣病に関する項目)
	6情報	・5情報 + 処方情報(診療情報提供書)

HL7 FHIR は、HL7協会の登録商標です

HPKI専門家会議で議論開始

【第29回HPKI専門家会議資料から（2024年9月11日開催）】

HPKIリモート署名サービス評価基準の進め方

現状の運用体制（2022年12月～）

1. 対象サービス（現状は電子処方箋のみ）についてHPKI専門家会議にて審議し、リモート署名の利用を承認
2. 厚生労働省にて当該サービスにおいてリモート署名を利用してよいことを都道府県に対し周知
3. 2023年9月　リモート署名サービス評価基準を制定し審査を実施（**※電子処方箋を前提とした基準**）

前回の議論（抜粋）

● リモート署名サービス評価基準の今後の進め方について
HPKIリモート署名サービス評価基準について、将来的な改定に向けた議論は引き続き、本専門家会議を中心に行っていく方針とした。

● リモート書目サービスの利用用途限定について
個別の限定解除ではなく、HPKIリモート署名サービス基準が保健医療福祉分野において汎用的な評価基準とすることを目的として基準改定を進めていくこととした。

● 電子カルテ情報共有サービスにおけるリモート署名利用について
電子処方箋における限定要件を再度確認し、電子カルテ情報共有サービスが該当するかどうか、次回の専門家会議の議論へ持ち越しとした。

HPKI専門家会議で議論開始

【第29回HPKI専門家会議資料から（2024年9月11日開催）】

HPKIリモート署名サービス評価基準の進め方

対応方針

前回の議論を受けて、下記の進め方としてはどうか

- 電子処方箋だけではなく、保健医療福祉分野全般の利用を想定した基準を新たに作成する
  （新基準は必要に応じて複数パターンになることも検討）
- 電子処方箋向けとなっている現状の基準は「オンライン資格確認ネットワーク」（以下オン資ネット）に限定した基準として継続して使用する
- 電子カルテ情報共有サービスについては電子処方箋と同様のシステム構成（オン資ネットの利用）のため、現状の基準で判断し利用できることとする

	対象サービス	ドキュメント	専門家会議の対応
オン資ネット IP-VPN、IPSec+IKEにて接続され、医療機関とオンライン資格確認等システムを繋いでいるネットワーク環境	**「電子処方箋管理サービス」 「電子カルテ情報共有サービス」 などのオン資ネット等で 提供されるサービス**	**【現状】 リモート署名評価基準 （オン資ネット向け）**	□ オン資ネット向けの基準として継続利用 □ 準拠性審査も本基準で継続実施
その他のネットワーク オン資ネット以外のインターネット等と接続しているネットワーク環境	**地域医療情報連携 ネットワーク等 その他のサービス**	**【新規作成】 リモート署名評価基準 （オン資ネット以外向け）**	□ スコープ（対象文書）の調査研究から実施し作成 □ 本専門家会議にて新たに基準を作成し準拠性審査も別で実施 □ デジタル庁のリモート署名検討状況を踏まえながら、来年度以降に案を準備し、専門家会議にて内容を議論

Agenda

1．この1年間のアップデート

2．HPKIをめぐる動向

3．今後の気になる動向

次期暗号方式の検討（暗号方式の移行）

HPKIで使用している方式

ハッシュ：SHA-256（128ビットセキュリティ） 2050年まで

暗　　号：RSA2048（112ビットセキュリティ） 2030年まで

表 5　セキュリティ強度要件の基本設定方針

想定運用終了・廃棄年／利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112 ビット セキュリティ	新規生成 ((a)参照)	移行完遂期間 ((c)参照)	利用不可	利用不可	利用不可	利用不可
	処理 ((b)参照)		許容			
128 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	移行完遂期間 ((c)参照)	利用不可	利用不可
	処理 ((b)参照)				許容	
192 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	利用可	利用可	利用可
	処理 ((b)参照)					
256 ビット セキュリティ	新規生成 ((a)参照)	利用可	利用可	利用可	利用可	利用可
	処理 ((b)参照)					

Cryptrec 暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準より抜粋

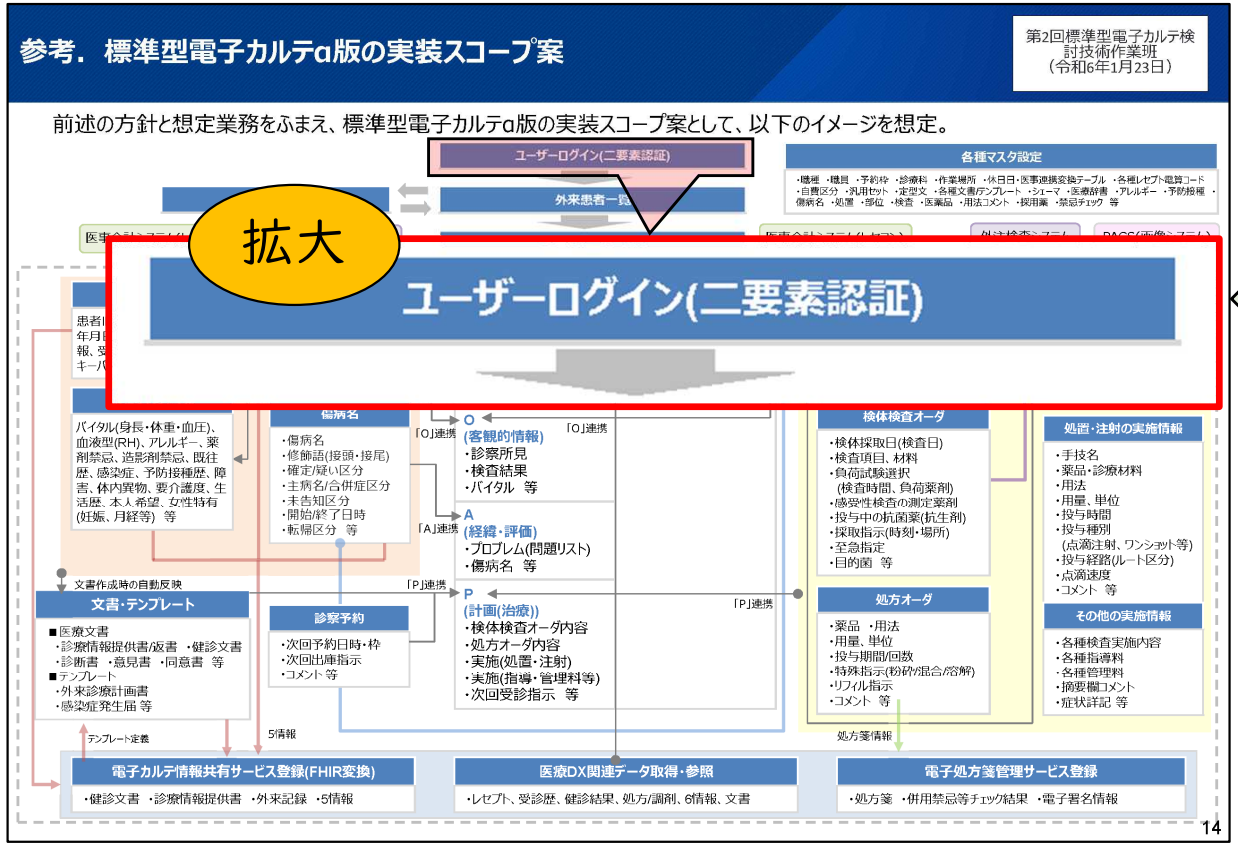
2030年に向けてHPKI専門家会議で次期暗号方式（楕円曲線？）の検討も始まることが予想される。議論を注視すると共に電子証明書格納ICカードや署名モジュールの対応について留意して行く必要がある。

二要素認証（令和9年度以降）

◆ 医療情報システムの安全管理に関するガイドライン第6.0版
システム運用編

14. 認証・認可に関する安全管理措置
⑤ 利用者認証にパスワードを用いる場合には、令和9年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新するに際しては、**二要素認証を採用するシステム**の導入、又はこれに相当する対応を行うこと。

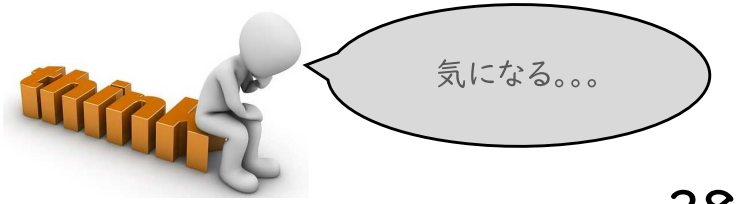
◆ 第2回標準型電子カルテ検討ワーキンググループ資料1
（令和6年3月7日）



✓ ガイドラインで、令和9年度時点で稼働しているシステムは二要素認証を採用するシステムへの対応を行うことと明記。

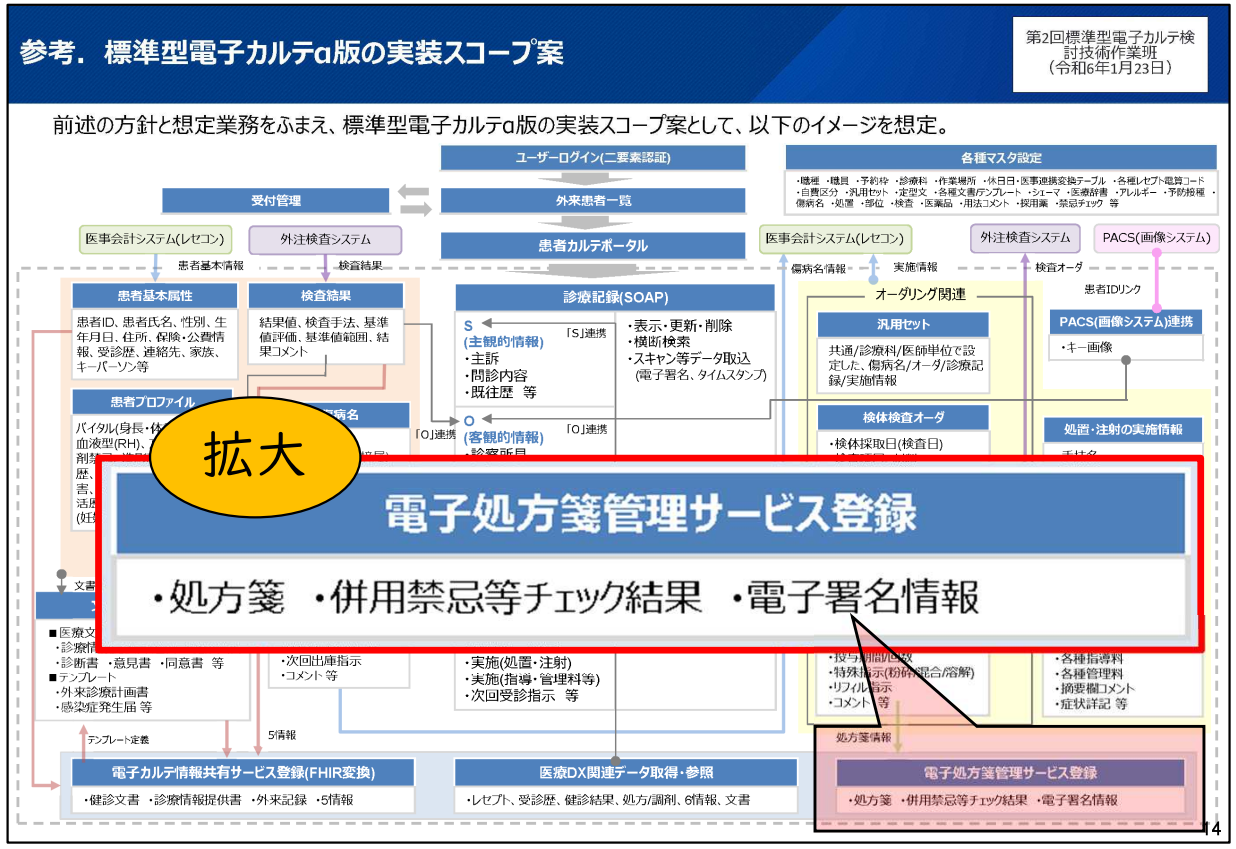
✓ ガイドラインのQAでは、その採用例として、以下を例示（P.100）
- ユーザID+パスワード+指紋認証
- ICカード+パスワード
- ICカード+静脈認証等

マイナンバーカードも認証機能（利用者証明書）があるけど、HPKIにも認証機能あります。FIDO認証（生体認証）も使えます。

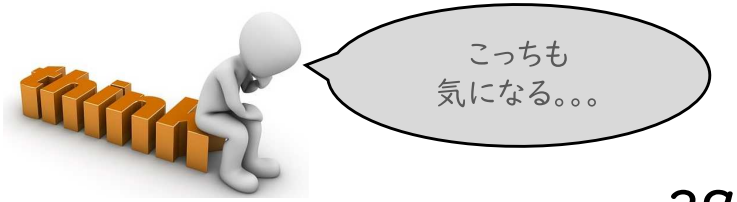


標準型電子カルテ

◆ 第2回標準型電子カルテ検討ワーキンググループ資料1
（令和6年3月7日）



電子処方箋はHPKI電子署名必須だけど、標準型電カルでもHPKI電子署名を使うよね？



ご清聴ありがとうございます