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

電子処方箋における電子署名について

【医療機関・薬局の方々へ】

令和7年3月 1.2版

厚生労働省 医薬局

改訂履歴

版数	改訂年月日	該当箇所	主な改訂内容
1.0	令和6年4月10日	全体	初版作成
1.1	令和6年11月14日	2．電子処方箋の仕組みにおける電子署名について（2/2）	ローカル署名、リモート署名を選択する場合の準備内容についてページを追加
		3. ②リモート署名に必要な準備と運用の流れについて	「運用イメージ（医療機関の場合）」の部分について、「診察・処方内容確定」と「本人認証（1日1回）」の順序を入れ替え
		4.電子署名に関するQ&A	電子署名に関するQ&Aのページを追加
		5.参考資料　マイナンバーカードを活用した電子署名の申請方法	マイナポータル経由で医師等個人が電子署名を実施できるようにするための申請方法を示す手順書を案内するページを追加
		病院における電子署名（リモート署名）の運用事例	病院における電子署名（リモート署名）の運用事例を示すページを追加
		病院における電子署名に関するシステム構成例	導入費用を抑えるためのシステム構成例や運用例を示すページを追加
1.2	令和7年３月14日	1. 電子署名とは（1/1）	• 紙の書類に電子印鑑の印影がプリントアウトされているだけでは、法令上の署名または記名押印の要件を満たさない旨を追記
		2. 電子処方箋の仕組みにおける電子署名について（2/2）	• 令和7年4月より、リモート署名を行うためには利用料が必要となる旨を追記 • リモート署名を行うためにはクライアント証明書の申請が必要である旨を追記

目次

1. 電子署名とは（1/2）

電子的に文書をやり取りするにあたり、正当な者が文書を記録したことを証明するため、従来の紙への署名または記名・押印を電子的に実施することを“電子署名”といいます。

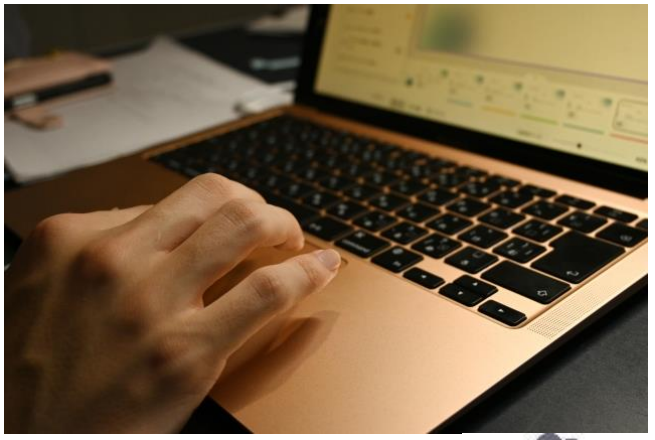
紙の文書の場合

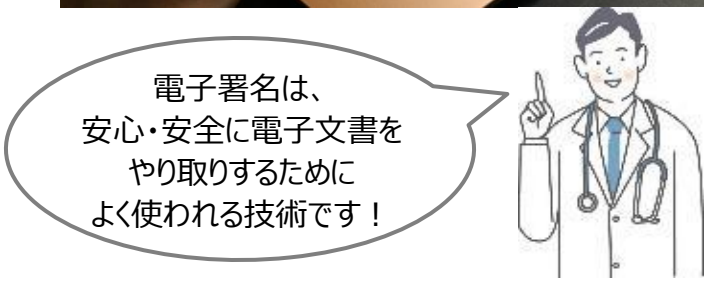
紙へ署名または記名・押印等を行う。

（注）一般的に、紙の書類に電子印鑑の印影がプリントアウトされているだけでは、法令上の署名または記名押印の要件を満たしません。

電子文書の場合

“電子署名”を行う。





1. 電子署名とは（2/2）

電子署名には、電子的に本人であることを証明する“電子証明書”の情報と、“PKI（公開鍵基盤）”という仕組みを使います。

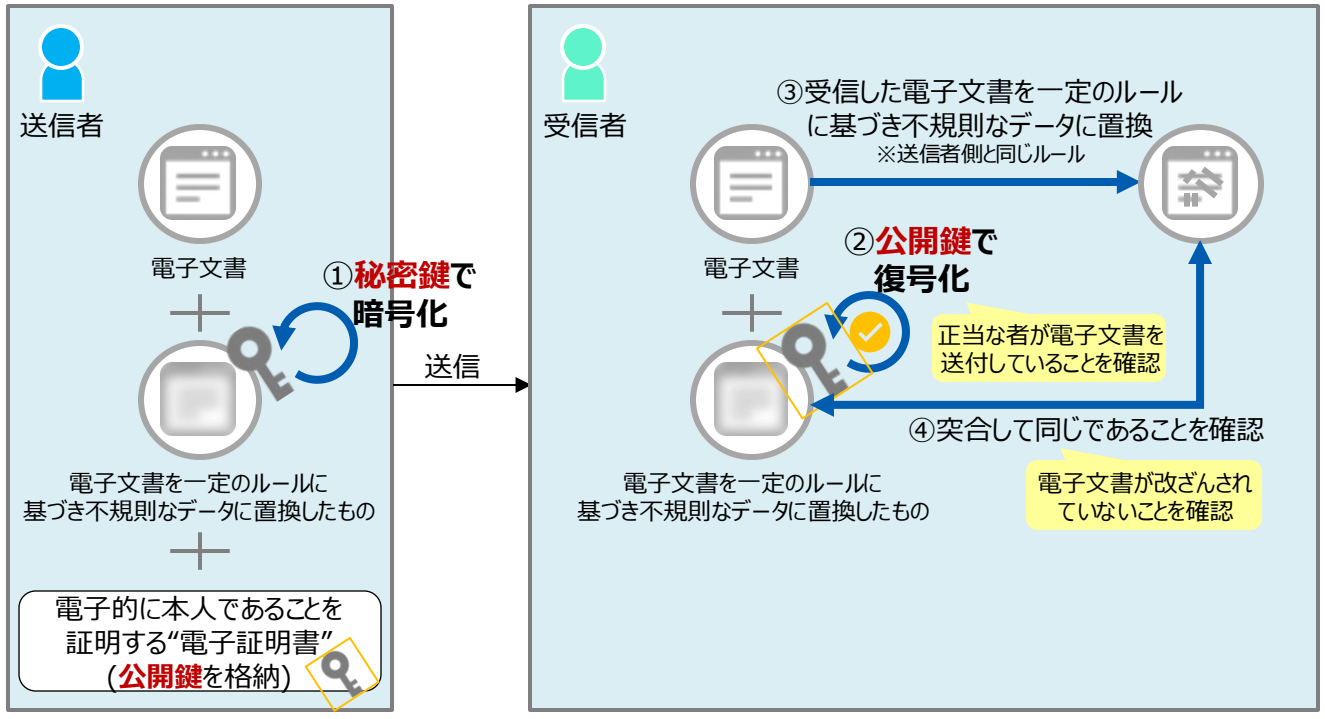
PKI（公開鍵基盤）とは

PKIとは、電子文書を安全にやり取りするための技術です。この仕組みを活用した電子署名は、e-TAXによる確定申告等、行政分野などにおいても幅広く利用されています。
電子文書の送信者しか知らない情報**"秘密鍵"**を用いてデータを暗号化した上で、それに紐づく**"公開鍵"**でしか復号化できないという仕組みを用いています。

電子署名により、
従来の筆跡鑑定よりも簡単に
以下を証明できます！

- ✓ **本人が電子文書を送信していること**
- ✓ **文書が改ざんされていないこと**

（参考）PKIを用いた電子署名の仕組み



電子署名の仕組みを運用する「認証局」とは？

電子署名の仕組みを安全に運用するためには、**公正な立場にある主体が、利用者の本人確認・審査を厳密に行った上で秘密鍵・公開鍵を発行**する必要があり、その役割を「認証局」が果たしています。
また、電子証明書には有効期限がありますが、認証局は**有効/失効の情報も管理**しています。

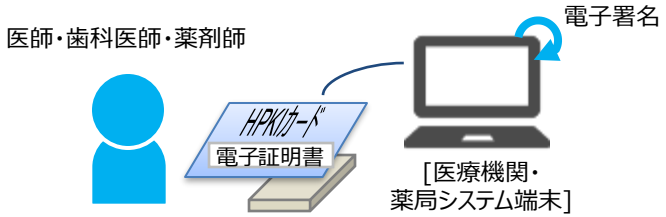
電子処方箋を発行、調剤結果登録を行う場合は、医療現場において、公的資格の確認機能を有する電子署名や電子認証を行う保健医療福祉分野の公開鍵基盤（ HPKI：Healthcare Public Key Infrastructure ）を使用しています。

2. 電子処方箋の仕組みにおける電子署名について（1/2）

電子処方箋の仕組みにおいて使用できる電子署名の方法は、
①HPKIカードの中の電子証明書を用いる方法（ローカル署名）
②本人認証を行った上でクラウドで管理されているHPKIセカンド電子証明書を用いる方法（リモート署名）の2つがあります。

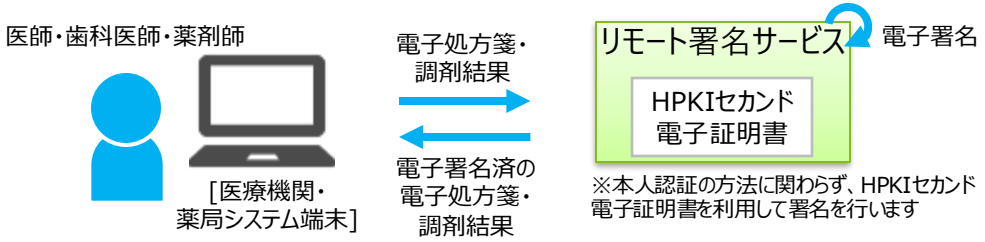
①ローカル署名

医師等は、電子処方箋を発行または電子処方箋の調剤結果を登録する度、HPKIカードをICカードリーダーにかざして電子署名を行う



②リモート署名

医師等は、事前に本人認証を行うことで、HPKIセカンド電子証明書を利用することが可能。本人認証後は、自動で電子署名を付与して電子処方箋を発行または電子処方箋の調剤結果登録をすることができる。（１日程度有効）



本人認証の方式
方法ｉ）HPKIカードまたはマイナンバーカードをICカードリーダーにかざす
方法ii）スマートフォンによる生体認証

準備内容（医師等の準備事項）

- ✓ HPKI認証局に直接申請する、または、マイナポータル経由で医師等個人が電子署名を実施できるようにするための申請を行ってください。
- ※ 各認証局への申請方法により、HPKIカードの発行の取扱いが変わります。
- ※ いずれの申請方法でもリモート署名に必要なHPKIセカンド電子証明書の利用が可能となりますが、マイナンバーカードによる本人認証方式によってHPKIセカンド電子証明書を利用可能とするには、マイナポータルから申請いただき、マイナンバーカードとの紐づけ対応をする必要があります。
- ※ HPKI認証局への申請及びマイナンバーカードとの紐付け、スマートフォンの生体認証による本人認証によってHPKIセカンド電子証明書を利用する初期対応の詳細等は P.12をご参照ください。

準備内容（施設の準備事項）

- ✓ 電子署名を行うためのパソコンの設定
- ✓ ICカードリーダーの購入
  ①ローカル署名の場合は、端末分が望ましい ②リモート署名で本人認証方式として方法ｉ）を活用する場合は、運用上で必要と考えられる数
- ✓ （リモート署名でシステム構成上必要な場合）ネットワークの設定の変更

2. 電子処方箋の仕組みにおける電子署名について（2/2）

下表は医師等個人の準備事項と施設の準備事項を記載しています。
医師等個人はHPKI認証局に直接申請するか、マイナポータルからHPKI認証局に申請を行います。それぞれの申請によって医師等個人が可能となる署名方法、リモート署名の認証方法は下表のとおりです。
例えば、医師がマイナポータルから申請した場合、ローカル署名、リモート署名のいずれの本人認証方法にも対応が可能となります。

			医師等の準備事項		施設の準備事項
			HPKI認証局に直接申請	マイナポータル申請	
ローカル署名を選択する場合			○	○ （日薬認証局の場合はカードが発行されないので×）	✓ 電子署名を行うためのパソコンの設定 ✓ ICカードリーダーの準備
リモート署名を選択する場合	本人認証方法	HPKIカードかざす認証	○	○ （日薬認証局の場合はカードが発行されないので×）	✓ 電子署名を行うためのパソコンの設定 ✓ ネットワークの設定の変更 ✓ 本人認証の運用を決定 - カード方式を利用する場合：ICカードリーダーの準備 - スマートフォンを利用する場合：生体認証機能付きのスマートフォン（既に病院で配布している公用のもの、または、私用のものでも代替可） ✓ サービス利用料の支払い※2 ✓ クライアント証明書の申請※3
		マイナンバーカードかざす認証	×※1	○	
		スマートフォンの生体認証	○	○	

※1 HPKIカードを既に持っている場合の申請方法については、P.12で案内する「マイナポータル上でのマイナンバーカードを活用した電子署名の申請」をご参照ください。
※2 令和7年4月より、リモート署名を行うためには利用料が必要となりました（年度毎）。利用料や支払方法については次のURLをご参照ください。（ローカル署名の場合も必要となるライセンス費用が発生する場合があります。） https://hp.hpki-cardless-signature.net/info_price.html
※3 お使いいただく端末が、HPKIセカンド電子証明書を管理するシステムへの接続を許可されていることを示すために、「クライアント証明書」を入手して端末内に配置する必要があります。次のURLをご参照ください。 https://hp.hpki-cardless-signature.net/#section-method

3. ①ローカル署名に必要な準備と運用の流れについて

- **ローカル署名とは、HPKIカードに格納されている電子証明書等の情報を使用する方法です。**
- **ICカードリーダーにHPKIカードをかざし、本人のみが知るPINを入力することで、電子証明書等の情報を読み取り、電子カルテシステム等で電子処方箋発行時及び電子処方箋管理サービスへの調剤結果登録時に、医師、歯科医師、薬剤師の電子署名を行います。**

ローカル署名は、リモート署名とは異なり、HPKIカードが医師等の手元に届く必要がありますが、ネットワークの構成変更・設定費用が掛かりません

準備内容

（お使いいただくシステムの改修は別途行う必要がある）

①医師等がHPKI認証局にHPKIカードの発行申請を行う。医療機関・薬局によって、申請先の認証局が異なります。

＜医師＞
・日本医師会 電子認証センター
https://www.jmaca.med.or.jp/application/
・一般財団法人医療情報システム開発センター（MEDIS）
http://www.medis.or.jp/8_hpki/index.html

＜薬剤師＞
・日本薬剤師会認証局
https://www.nichiyaku.or.jp/hpki/index.html#S30
・一般財団法人医療情報システム開発センター（MEDIS）
http://www.medis.or.jp/8_hpki/index.html

＜歯科医師＞
・一般財団法人医療情報システム開発センター（MEDIS）
http://www.medis.or.jp/8_hpki/index.html

※各認証局に対し、医師等がHPKI認証局に直接申請する、または、マイナポータル経由で申請を行ってください。
詳細は、P.12で案内する「マイナポータル上でのマイナンバーカードを活用した電子署名の申請」を参照ください。
※日本医師会電子認証 センター（認証局） ではマイナポータルからの申請に限り、当面の間非会員も費用を減免中です。
※国家資格によって、申請先の認証局や発行費用等が異なりますのでご注意ください。

② 医療機関・薬局側でHPKIカード読取用のICカードリーダーを用意する。

運用イメージ（医療機関の場合）

電子カルテシステム等にログイン
電子カルテシステムにログインする

診察・処方内容確定
診察を行い、処方内容を確定する

本人認証
医師または歯科医師が都度※1本人認証を行う

HPKIカードをICカードリーダーにかざし※2、ご使用いただく電子カルテシステム等で本人のみが知るPINを入力する

※1 お使いいただくシステムによっては、一度認証を行った後、HPKIカードを外すまでは認証が有効となり、都度の認証が不要となる場合もあります。
※2 HPKIカードをICカードリーダーに常時かざしておくことも可能です。

電子署名を行った上で電子処方箋管理サービスに登録される

3. ②リモート署名に必要な準備と運用の流れについて

- **リモート署名とは、HPKIセカンド電子証明書等の情報を使用する方法です。**
- **本人認証を行うため、**
  ｉ）ICカードリーダーにHPKIカードまたはマイナンバーカードをかざし、本人のみが知るPINを入力する認証、またはⅱ)スマートフォンによる生体認証を行い、クラウド上で電子署名を行います。

リモート署名の認証方法として、HPKIカードの認証を利用する場合はHPKIカードがお手元に届くまでに時間を要する場合がありますが、認証方法としてマイナンバーカードを用いる場合またはスマートフォンによる生体認証を行う場合は、物理的にHPKIカードを保有することが必須ではないため、比較的早期に電子署名を行うことができます。

準備内容

（お使いいただくシステムの改修やサービス利用料の支払は別途行う必要がある）

① 医師等がリモート署名の利用をHPKI認証局に対して直接申請する、または、マイナポータル経由で電子署名の申請を行う。
（P.12で案内する「マイナポータル上でのマイナンバーカードを活用した電子署名の申請」に沿ってご対応ください。）

② クライアント証明書をクライアント証明書発行事務局に申請する。

③ ｉ）（カード認証の場合）医療機関・薬局側は、マイナンバーカードまたはHPKIカード読取用のICカードリーダーを用意する。
※各端末分の購入は必須ではなく、認証に使用する端末分で構いません。

③ⅱ）（スマートフォンによる生体認証の場合）医師等が生体認証のためのスマートフォンを登録する。

② ⅱ）についてはP.12をご確認ください

運用イメージ（医療機関の場合）

電子カルテシステム等にログイン

電子カルテシステムにログインする

本人認証（1日1回）

医師または歯科医師がHPKIセカンド電子証明書を使うことを証明するため、1日1回本人認証を行う

方法ｉ）カード認証
HPKIカードまたはマイナンバーカードをかざし、本人のみが知るPINを入力

方法ⅱ）スマートフォンによる生体認証

画面上表示される二次元コードをスマートフォンで読取

スマートフォンで生体認証

診察・処方内容確定

診察を行い、処方内容を確定する
※都度、本人認証を行う必要なく、電子署名を付すことが可能。

電子署名を行った上で電子処方箋管理サービスに登録される

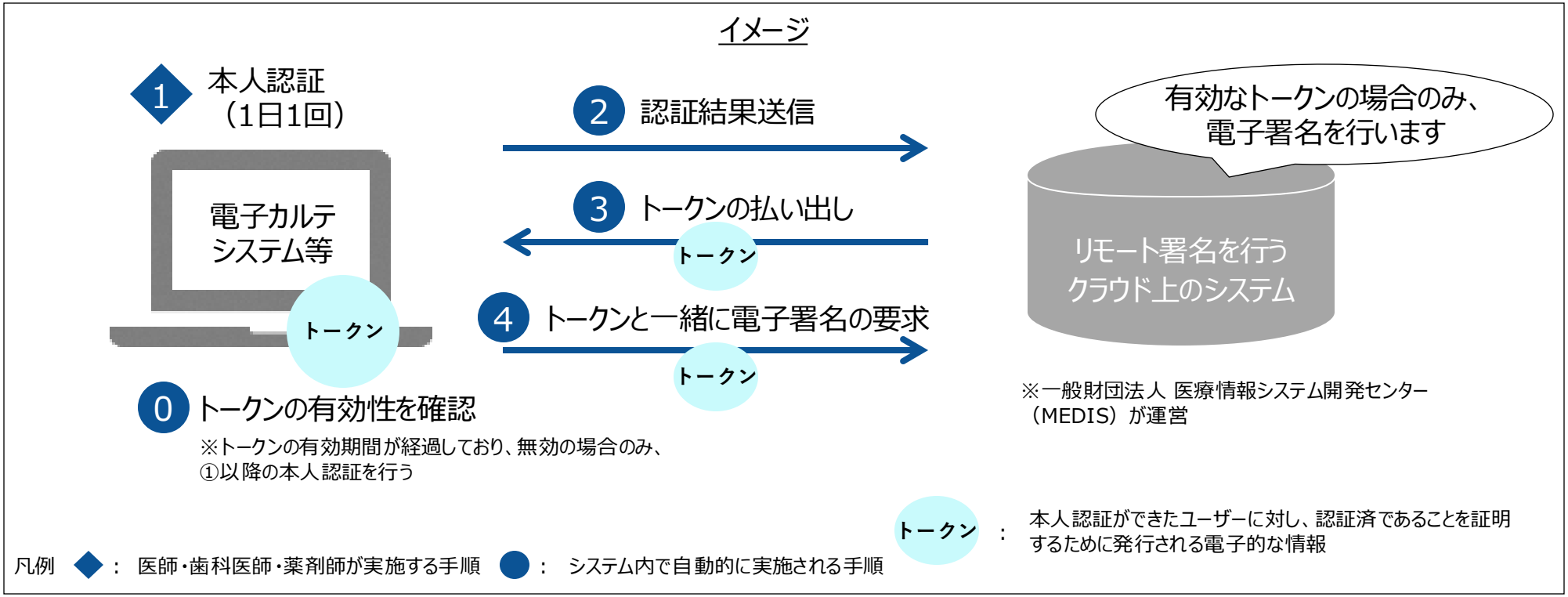
※実際にリモート署名を活用している医療機関の運用はP.18～22を参照

4. 電子署名に関するQ&A

Question	Answer
Q）リモート署名の場合、電子署名の都度、本人認証が必要となりますか？	A）いいえ、一度本人認証を行った後は1日程度有効となりますので、都度、本人認証を行う必要はありません。
Q）リモート署名の場合、本人認証の方法（P.5）は全て対応できるようにする必要がありますか？	A）いいえ、必ずしも全ての本人認証方法に対応する必要はありません。運用の流れや運用例などを参考に本人認証方式を決定してください。
Q）本人認証に私用のスマートフォンを使いたいのですが、セキュリティの観点で、院内のシステムに影響はないですか？	A）スマートフォンと院内のシステムが直接接続することはないため、私用のスマートフォンで生体認証を行うことによる院内のシステムへの影響はありません。 ※ただし、その他のセキュリティ対策については「医療情報安全ガイドライン」等に従って適切に実施する必要があります。
Q）電子署名は医師・歯科医師・薬剤師本人が行う必要がありますか？	A）はい、従来の紙の処方箋への署名または記名・押印と変わらず、医師・歯科医師・薬剤師本人が行う必要があります。 （参考） 医師及び医療関係職と事務職員等との間等での役割分担の推進について https://www.mhlw.go.jp/web/t_doc?dataId=00tb3694&dataType=1&pageNo=1
Q）医師等が端末を移動した場合、医師等とトークンが紐づいている必要がありますが、どのように紐づいているのですか？	A）院内で医師等を管理する識別子（職員ID等）とトークンが紐づいている必要があり、システム事業者に当該設定を行っていただくことになります。

5. 参考資料
リモート署名の仕組みについて

- **HPKIセカンド電子証明書を利用して電子署名を行うにあたり、医師等本人が電子証明書の所有者であることを証明するために本人認証を行います。**
- **認証後、HPKIセカンド電子証明書を利用できることを証明するための情報である”トークン”が払い出され、以降は、トークンと一緒に電子署名の要求等を行います。**



一度トークンが発行されたら、その日は有効になりますので、本人認証は原則１日１回のみとなります。
有効期間を経過した後は、再度①本人認証を行い、トークンを払い出してもらう必要があります。

5. 参考資料
リモート署名における本人認証の方法について

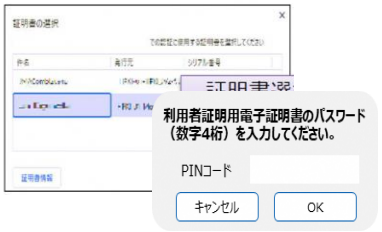
１日１回行う本人認証の方法としては、カード認証（方法ｉ）及びスマートフォンによる生体認証（方法ii）があります。
いずれの方法でも簡単に本人認証を行うことができます

方法ｉ）カード認証

電子カルテシステム等の画面上で、「HPKIカード」または「マイナンバーカード」を選択する

ICカードリーダーでHPKIカードまたはマイナンバーカードを読み取る

ご自身のマイナンバーカードの電子証明書を選択し、利用者証明用パスワードとして設定した4桁の数字を入力する



トークンが発行され、電子署名可能な状態となる

方法ii）スマートフォンによる生体認証

電子カルテシステム等の画面上で、FIDO（生体認証）を選択する

電子カルテシステム等の画面に二次元コードが表示され、予め認証用として登録済みのスマートフォンで読み取る

スマートフォンで生体認証を行う

トークンが発行され、電子署名可能な状態となる

スマートフォンの登録方法はP.14

5. 参考資料
マイナンバーカードを活用した電子署名の申請方法

マイナンバーカードを活用した電子署名の申請については、
「マイナポータル上でのマイナンバーカードを活用した電子署名の申請」
（https://www.mhlw.go.jp/content/11120000/001264397.pdf）をご確認ください。

5. 参考資料
マイナンバーカードを本人認証方法として活用したリモート署名の利用開始までの準備ステップ

まずは、利用する電子署名方式等について医療機関・薬局からシステム事業者にご相談の上、発注等を進めて下さい。
また、HPKI認証局への申請については医師・歯科医師・薬剤師個人でご対応いただく必要があります。

例）システム事業者への相談の上、「リモート署名」の中で、マイナンバーカードでHPKIセカンド電子証明書を利用する方法を選択する場合

まずはご相談を

システム事業者への相談

HPKI認証局への申請（医師・歯科医師・薬剤師側）

マイナンバーカードによる本人認証方式によってHPKIセカンド電子証明書を利用可能とするためには、マイナポータルから申請し、マイナンバーカードとHPKIセカンド電子証明書の紐付け対応をする必要があります。

HPKIカードがなくても、**審査完了後からご自身のマイナンバーカードによって電子署名が可能に**！

1.マイナポータルにログイン → 2.マイナポータルから利用申請 → 3.審査完了

※マイナポータル上でのマイナンバーカードを活用した電子署名の申請手順については、P.12にURLを案内しています。
（HPKIカードを取得済みの方の紐付け方法も掲載しています。）

お使いいただくシステムの改修（医療機関・薬局側）

1.見積依頼	2.発注・ICカードリーダー準備	3.導入・運用準備
システム事業者に見積作成を依頼します。	• システム事業者より提出された見積を確認し、発注します。 • システム事業者への発注と並行して、マイナンバーカードの読取に対応したICカードリーダーを必要数準備してください。 ※既にお使いいただくICカードリーダーが対応している場合、再購入は不要です。	電子署名の利用開始に向け、業務内容・システム操作方法を確認します。

電子署名の利用開始

5. 参考資料
生体認証のためのスマートフォンの登録（紐付け）方法

スマートフォンによる生体認証とは、HPKIセカンド電子証明書と生体認証を行うスマートフォンを登録（紐付け）しておくことで、そのスマートフォンでの生体認証を行った人が当該電子証明書の所有者であることを証明する仕組みです。

スマートフォンの登録方法

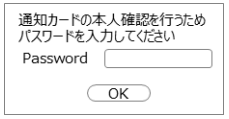
デバイス登録用の二次元コード等読取

【HPKI認証局に直接申請した場合】
- HPKI認証局から送付される通知カードにある二次元コード等を読み取ります。※

【マイナポータル経由で申請した場合】
- HPKI認証局からマイナポータルのアカウントに送信されるURLを読み取ります。※

パスワード入力

ブラウザが開くので、二次元コード等と一緒に送られてきたパスワードを入力します。

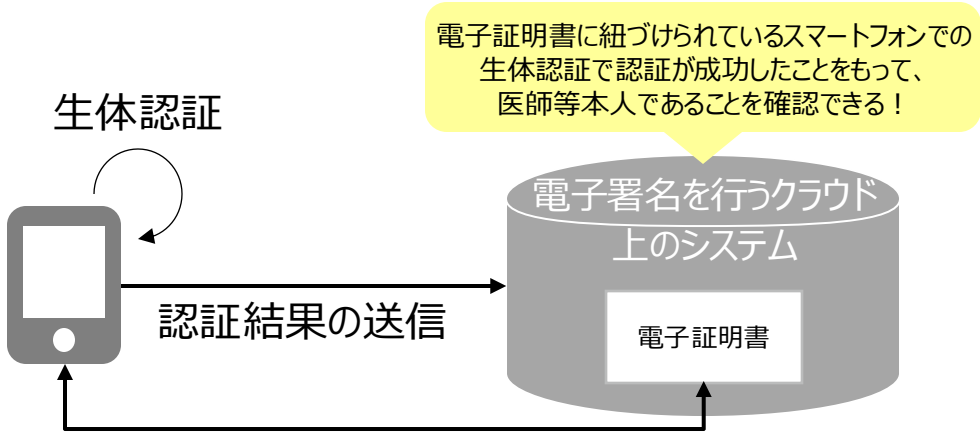


生体認証

生体認証を行います。
これにより、HPKIセカンド電子証明書とスマートフォンの紐づけが完了します。

<u>※デバイス登録用の二次元コードやURL等の有効期限</u>
・HPKI認証局から送付される通知カードの二次元コード等：※通知カードをご確認ください
・HPKI認証局からマイナポータルのアカウントに送信されるURL：3カ月

仕組み



HPKIセカンド電子証明書と、生体認証に使うスマートフォンをあらかじめ紐づけておく。
以降は、そのスマートフォンで生体認証を行った場合に限り、本人認証成功となる。

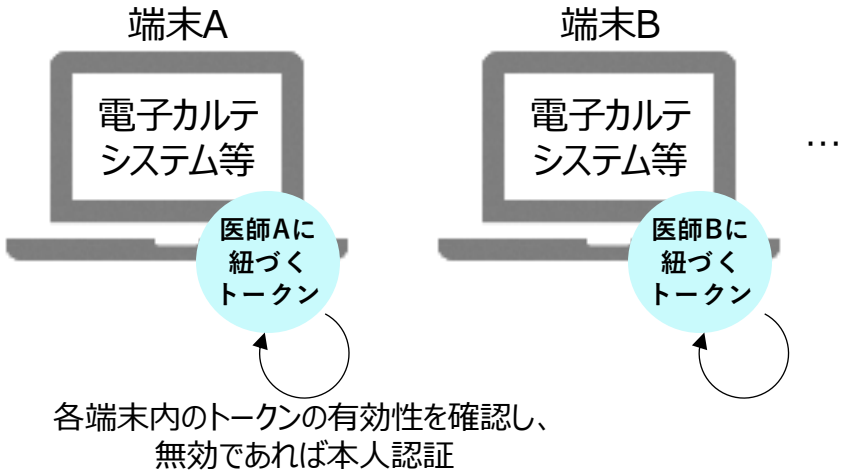
5. 参考資料
トークンの管理方法について

医師等が使用する端末が固定されていない施設において、トークンを各端末に紐づけて管理していると、別の端末を利用する度に、本人認証が必要になってしまうため、“トークンを集中的に管理する構成”をとることを推奨します。（管理方法についてはシステム事業者に相談ください）

端末が数台しかなく、かつ、
医師等の移動も少ない
診療所・薬局等におすすめ！

トークンを複数の端末で分散して管理

トークンを各端末で管理する方式のこと。

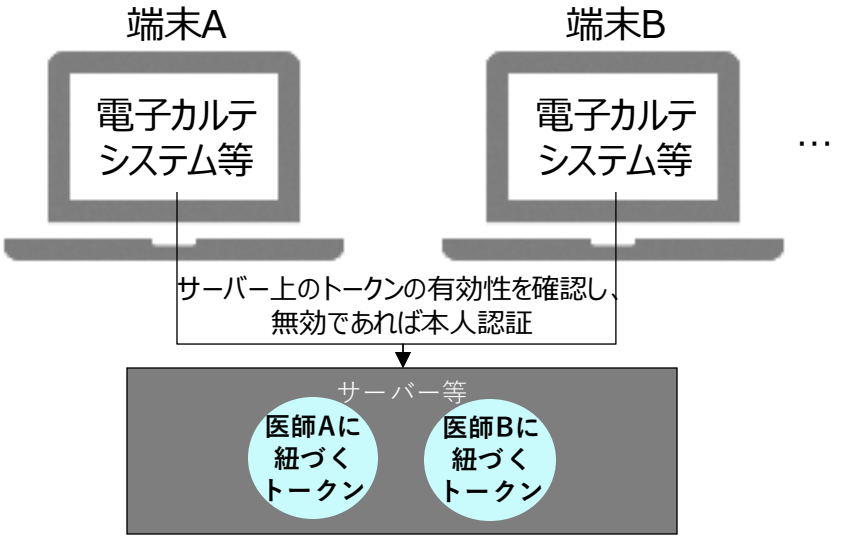


医師Aが端末Bを使用する場合、端末Bでは当該医師の有効なトークンが管理されていないため、再度本人認証が必要になってしまう

端末が複数台あり、かつ、
医師等が頻繁に端末を変える病院等に
おすすめ！

トークンをサーバー等で集中的に管理

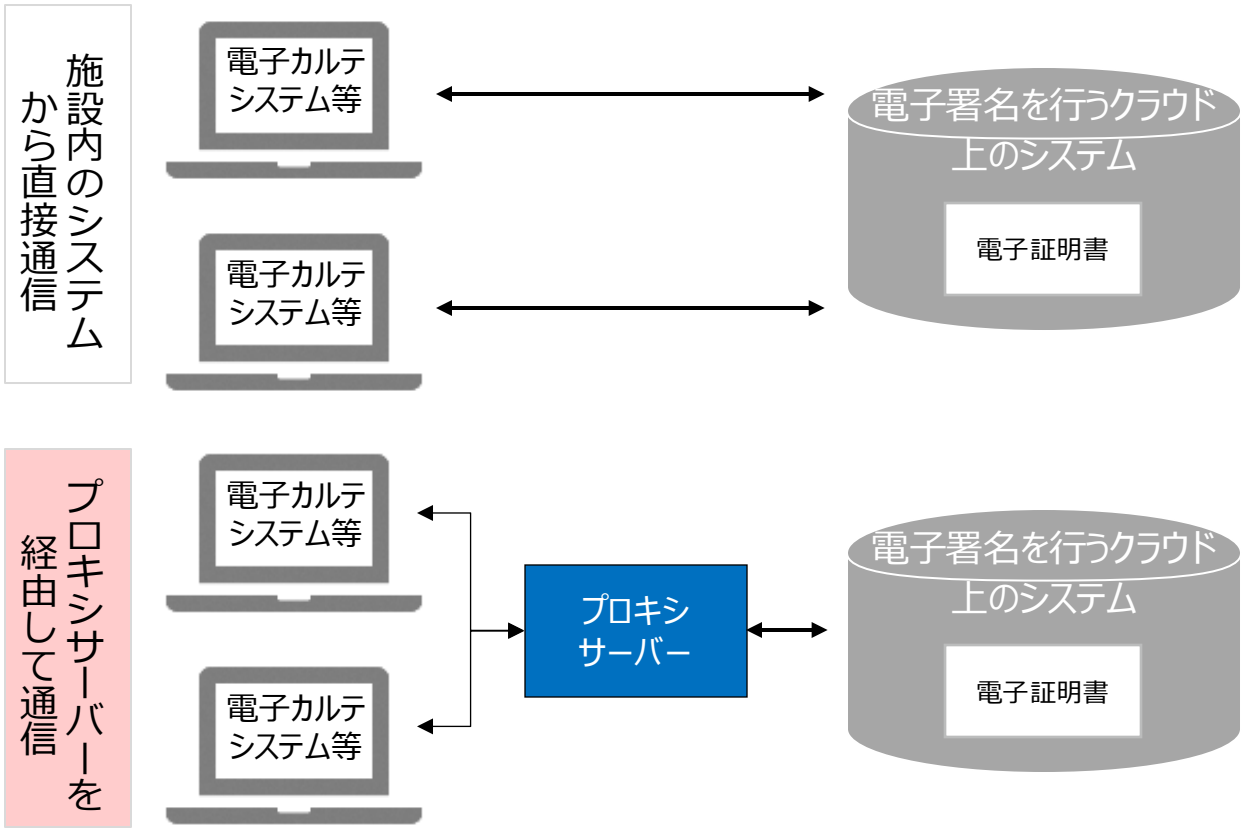
トークンを各端末ではなく、ある端末（サーバー等）で複数端末分を集中的に管理する方法のこと。



医師Aが端末Bを使用する場合であっても、端末Bからサーバー等で集中的に管理される当該医師のトークンを使えるため、都度の本人認証は不要

5. 参考資料
プロキシサーバーについて（1/2）

- **HPKIセカンド電子証明書を利用するにあたり、施設内のシステムからクラウドのシステムにアクセスする必要があります。**
- **外部のセキュリティ上の脅威から施設内のシステムを守るため、代わりにクラウドのシステムとの通信を行うためのサーバー（プロキシサーバー）を新規に用意することをご検討ください。**



悪意ある第三者により、施設内のシステムの情報（IPアドレス等）が不正に取得され、攻撃に使われる可能性がある。

※上記攻撃を防ぐため、セキュリティ対策を実装したルーター等を準備するなどの対策が必要だが、高額になる可能性あり

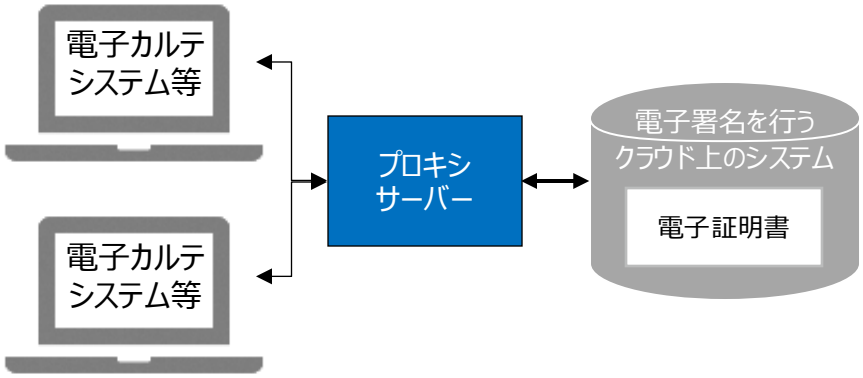
施設内のシステムに代わって外部との通信を担うプロキシサーバーを立てることで、施設内のシステムの情報を外部に公開せず通信ができる。

※プロキシサーバーの用意以外に、「医療情報システムの安全管理に関するガイドライン」に定められているその他セキュリティ対策については、これまでどおり対応をお願いします。

5. 参考資料
プロキシサーバーについて（2/2）

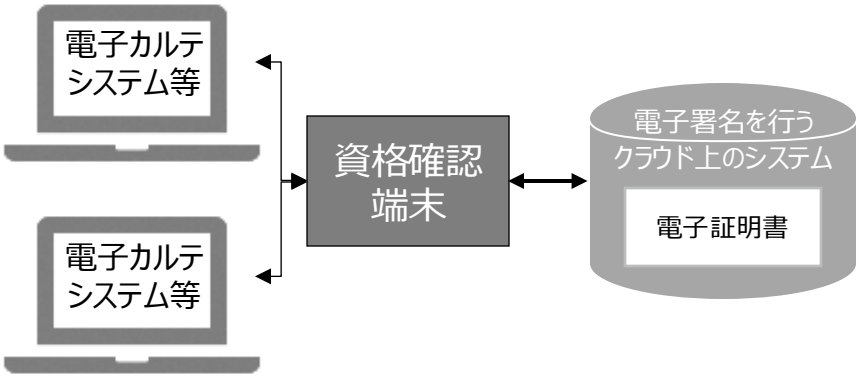
- **既に導入されている「資格確認端末」をプロキシサーバーの代わりに使う（資格確認端末上でプロキシ設定を行う）ことで、新たにプロキシサーバーを構築するよりも安価な導入を実現できる可能性があります（下右図）。**
- **ただし、資格確認端末での処理量が増えることにより、オンライン資格確認等の日々の業務に影響を与える可能性があるため、処方箋の発行量なども考慮し、システム事業者ともご相談の上で判断してください。**

プロキシサーバーを新規に構築



- **プロキシサーバーを新規に構築する費用が必要**
- ただし、**資格確認端末での処理量増加を防ぐことができる**

資格確認端末上でプロキシの設定を行う



- **プロキシサーバーを新規に構築する費用は不要**
- 資格確認端末のOS上の設定でプロキシを設定する必要あり
- ただし、**資格確認端末での負荷が増加する可能性がある**ため、システム事業者と相談が必要

病院における
電子署名（リモート署名）
の運用事例

地方独立行政法人山形県・酒田市病院機構　日本海総合病院での運用例

日本海総合病院では、令和５年７月よりリモート署名を利用しています。スマートフォンによる生体認証（FIDO認証）とカード認証を医師がその日ごとに選択して利用することができます。

- ✓ **当日外来がある医師が、電子カルテへのログイン時等任意のタイミングで認証**（※）を行い、リモート署名を有効化します。
  ※　電子処方箋発行時に有効なHPKI認証がなされていない場合は、自動で認証画面が表示されます。
- ✓ リモート署名では**スマートフォンによる「FIDO（生体認証）」又は「HPKIカード」による本人認証を１日１回行い、HPKIセカンド電子証明書の利用・電子処方箋発行時の電子署名の自動付与を可能となります。**
- ✓ 退勤時に必要な作業はありません。

職員コードとパスワードを入力後、「国家資格認証」をクリック

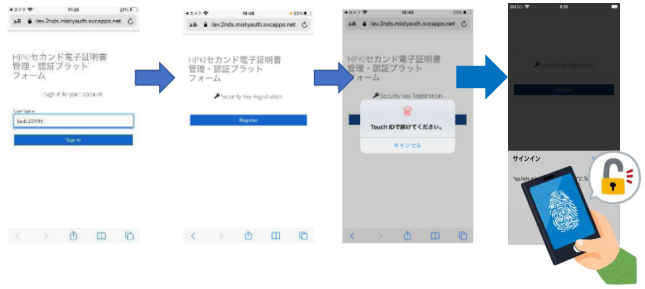
「FIDO」又は「HPKIカード」をクリック

スマートフォンによる生体認証

電子カルテに表示される二次元コードを、予め認証用として登録済みのスマートフォン（※）で読み取る。

電子カルテの画面上の二次元コードを読み取る内海副院長

スマートフォン上に表示されたUsernameが正しいことを確認してSign Inボタンをタップ。
Registerボタンをタップ。
生体認証を行う。



トークンが発行され、電子署名可能な状態となる。

（※）日本海総合病院では、もともと医師全員に業務連絡用としてモバイルデバイス管理されたスマートフォンを貸与しており、原則病院貸与のスマートフォンを認証端末としています。ただし、個人のスマートフォンであっても認証端末とするための手続きを経ており、電子カルテと直接通信することはなくセキュリティ上の問題はないと考え、貸与していない応援医師等が個人のスマートフォンを用いて認証を行うことも可としています。

カード認証

ICカードリーダーでHPKIカードを読み取る。

パスワードとして設定した4桁の数字を入力する。

地方独立行政法人山形県･酒田市病院機構　日本海総合病院での運用例

✓ 日本海総合病院では、管理課で手順書を作成し医師に説明をしています。
✓ リモート署名を始める前の、認証するスマートフォンの登録で戸惑う医師が多いため（※）、重点的にフォローしています。

医　師　各　位

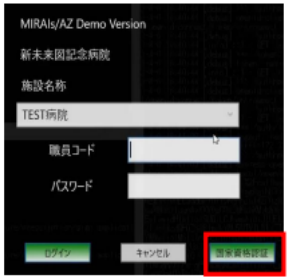
管理課長

電子処方箋に係る HPKI 署名の運用変更について

令和５年７月３日（月）より、電子処方箋発行の際の認証を HPKI セカンド証明書によるリモート署名に変更いたします。変更点については以下のとおりとなります。

【認証に必要なもの】
従来・・・HPKI カード
変更後・・・HPKI カードまたは認証機器として登録したスマートフォン

【認証方法】



職員コードとパスワードを入力後
「**国家資格認証**」ボタンをクリック

認証方法を選択する
※どちらを選択しても HPKI セカンド対応になります
HPKI カード･･･従来どおりカードリーダーに HPKI カードを置き、PIN 入力
FIDO･･･HPKI セカンド認証機器として登録済みのスマートフォンによる生体認証

FIDO 認証の流れ

「FIDO 認証」をクリック後に表示される QR コードを登録済みスマートフォンで読み取る⇒
スマートフォン上に表示された Username が正しいことを確認して SignIn ボタンをタップ⇒
Register ボタンをタップ後に生体認証を行う⇒
電子カルテ上で認証が完了する

【認証の有効期間】
HPKI セカンド証明書は一度認証すれば 20 時間有効で、ユーザーID に紐づくため、電子カルテからログアウトしても、端末を変えても利用可能です。
HPKI の認証状態はカルテ画面で確認することができます。
HPKI ボタンをクリックすることで有効期限の確認や再認証が可能です。

有効期間内（緑背景）

認証が必要な状態（黄背景）

担当：管理課情報システム係

内線

(※)参考：スマートフォンの登録方法

デバイス登録用の二次元コード読み取り

HPKI認証局から送付される通知カードにある二次元コードを読み取ります。
※有効期限があるためご注意ください。

パスワード入力

ブラウザが開くので、二次元コードと一緒に送られてきたパスワードを入力します。

生体認証

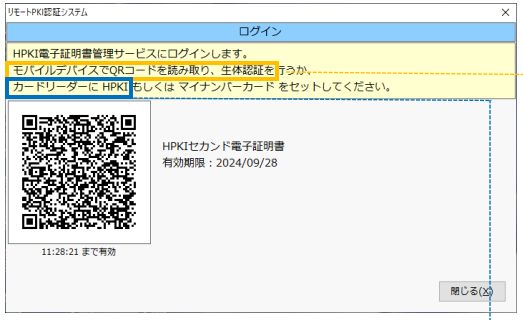
生体認証を行います。
これにより、HPKIセカンド電子証明書とスマートフォンの紐づけが完了します。

（注1）【認証に必要なもの】中の従来の「HPKIカード」は、HPKIカードの中の電子証明書を用いるローカル署名を行うにあたり、電子署名のために必要なものとして記載しています。
変更後の「HPKIカード」は、クラウド上の電子証明書（HPKIセカンド電子証明書）を用いるリモート署名を行うにあたり、本人認証のために必要なものとして記載されています。
（注2）本手順書は令和５年６月作成のものですが、現時点ではHPKIセカンド電子証明書の認証有効時間は18時間となっています。
（注3）病院内の担当者名等はマスキングを行っています。

社会医療法人財団董仙会　恵寿総合病院での運用例

恵寿総合病院では、電子処方箋導入時よりリモート署名とローカル署名を併用し、医師が選択して利用できるようにしています。

- ✓ **<u>当日外来がある医師が、出勤時又は診察開始前に、各診察室の電子カルテ、医局内端末、共用の端末のいずれかで認証</u>**を行い、リモート署名を有効化します。
- ✓ リモート署名では**スマートフォンによる「FIDO（生体認証）」又は「HPKIカード」による本人認証を１日１回行い、<u>HPKIセカンド電子証明書の利用・電子処方箋発行時の電子署名の自動付与が可能となります</u>**。
- ✓ FIDO認証に必要な手続きをしていない医師や非常勤医師は、HPKIカードを用いたリモート署名又はHPKIカードでのローカル署名を行っています。
- ✓ ローカル署名もできるよう、ユニバーサル外来、救急センターに各１箇所、共用のカードリーダーを設置しています。
- ✓ 退勤時に必要な作業はありません。
- ✓ 電子処方箋の導入にあたり、電子署名については、病院内のシステム担当部署から手順書を配布し、説明会を開催して周知しました。

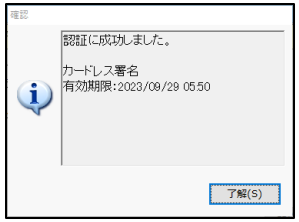


スマートフォンによる生体認証

電子カルテに表示されている二次元コードを、予め<u>認証用として登録済みのスマートフォン（※）</u>で読み取る。

スマートフォン上に表示されたUsernameが正しいことを確認してSign Inボタンをタップ。
Registerボタンをタップ。
生体認証を行う。

トークンが発行され、電子署名可能な状態となる。

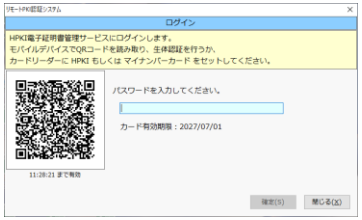


（※）恵寿総合病院では、FIDO認証に用いるスマートフォンの私用/公用は、各医師の判断に任せています。

カード認証

ICカードリーダーでHPKIカードを読み取る。

パスワードとして設定した4桁の数字を入力する。

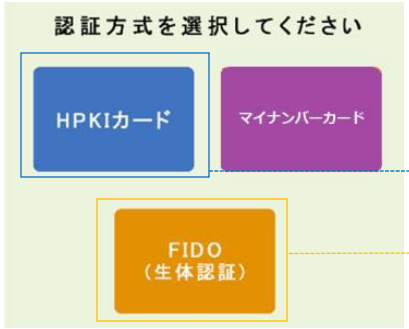


白山石川医療企業団　公立松任石川中央病院での運用例

公立松任石川中央病院では、電子処方箋導入時よりリモート署名を利用しています。スマートフォンによる生体認証（FIDO認証）を主として運用しつつ、カード認証にも対応できるよう運用しています。

- ✓ **FIDO認証の場合は、当日外来がある医師（非常勤を除く）が、診察開始前又は出勤時に、医局内端末、各診察室の電子カルテのいずれかで認証**を行い、リモート署名を有効化します。**HPKIカードでの認証の場合は、病院内のシステム担当部署に設置した共用のカードリーダーで 認証**を行い、リモート署名を有効化します。
- ✓ リモート署名では**スマートフォンによる「FIDO（生体認証）」又は「HPKIカード」による本人認証を１日１回行い、HPKIセカンド電子証明書の利用・電子処方箋発行時の電子署名の自動付与が可能となります**。
- ✓ 本人認証の方法として、**スマートフォンによる「FIDO（生体認証）」を主**としつつ、FIDO認証に必要な手続きをしていない医師や非常勤医師、カードを忘れた場合やスマートフォンの不具合時などFIDO認証が使用できないときはHPKIカードを用いたリモート署名を行っています。
- ✓ 退勤時に必要な作業はありません。
- ✓ 電子署名を行う医師に対しては、医師の申請したHPKI認証キーが届いたタイミングで、病院内のシステム担当部署から、スマートフォンの初期登録と認証操作方法を説明しています。

職員コードとパスワードを入力後、「国家資格認証」をクリック



「FIDO」又は「HPKIカード」をクリック

スマートフォンによる生体認証

医局内端末又は各診察室の電子カルテで、二次元コードを、予め認証用として登録済みのスマートフォン（※）で読み取る。

スマートフォン上に表示されたUsernameが正しいことを確認してSign Inボタンをタップ。Registerボタンをタップ。生体認証を行う。

トークンが発行され、電子署名可能な状態となる。

（※）公立松任石川中央病院では、診察室にスマートフォンを持参しない医師は医局内端末で認証しますが、持参する医師は各診察室の電子カルテでも認証できるようにし、認証場所は各医師の判断に任せています。また、FIDO認証には私用のスマートフォンを利用しています。

カード認証

ICカードリーダーでHPKIカードを読み取る。

パスワードとして設定した4桁の数字を入力する。

スマートフォンを有していない常勤医師等はHPKIカードを利用します。
出勤時に病院内のシステム担当部署の部屋に行き、共用のカードリーダーで認証を行います。

病院における
電子署名に関する
システム構成例

リモート署名の考慮事項

- **電子処方箋におけるリモート署名の運用やシステム構成のパターンは複数考えられます。**
- **ローカル署名とリモート署名の両方を必ずしも実装いただく必要はありません。ローカル署名もライセンス費用が発生する場合があります。**
- **自院の運用に合ったシステム構成例を検討し、システム事業者へとご確認ください。**

1日1回の本人認証方法

- HPKIカードをICカードリーダーにかざし、PINを入力する※
- マイナンバーカードをICカードリーダーにかざし、PINを入力する
- スマホの生体認証を使う

医師1人1人が本人認証の方法を選択できるようにする。カードを活用した認証方式はICカードリーダーが必要になりますが、１日１回の本人認証の運用等を踏まえて必要数をご検討ください。

※HPKIカードを既に保有する場合は、HPKIカードによる認証も可能ですが、HPKIカードの発行状況に留意が必要。

トークンの管理方法

- トークン集中管理型
  ※既存の電子カルテサーバーで集中的にトークンを管理（P.15）
- トークン分散管理型

医師が診察室を移動し、複数の電子カルテ端末を使用する場合は都度本人認証を行うことがないよう、**「トークン集中型」を選択する**。

プロキシの設定方法

- 既存のプロキシサーバーを活用
- 新規のプロキシサーバーを構築
- 資格確認端末を活用
  （資格確認端末のOS設定、プロキシのソフトウェアインストール等）

既存のプロキシサーバーで代替できる場合は、活用する方が費用低減可能。
（資格確認端末を活用する方法もありますが、病院の場合は通信量が多くなり、性能が低下する可能性がある点に留意）

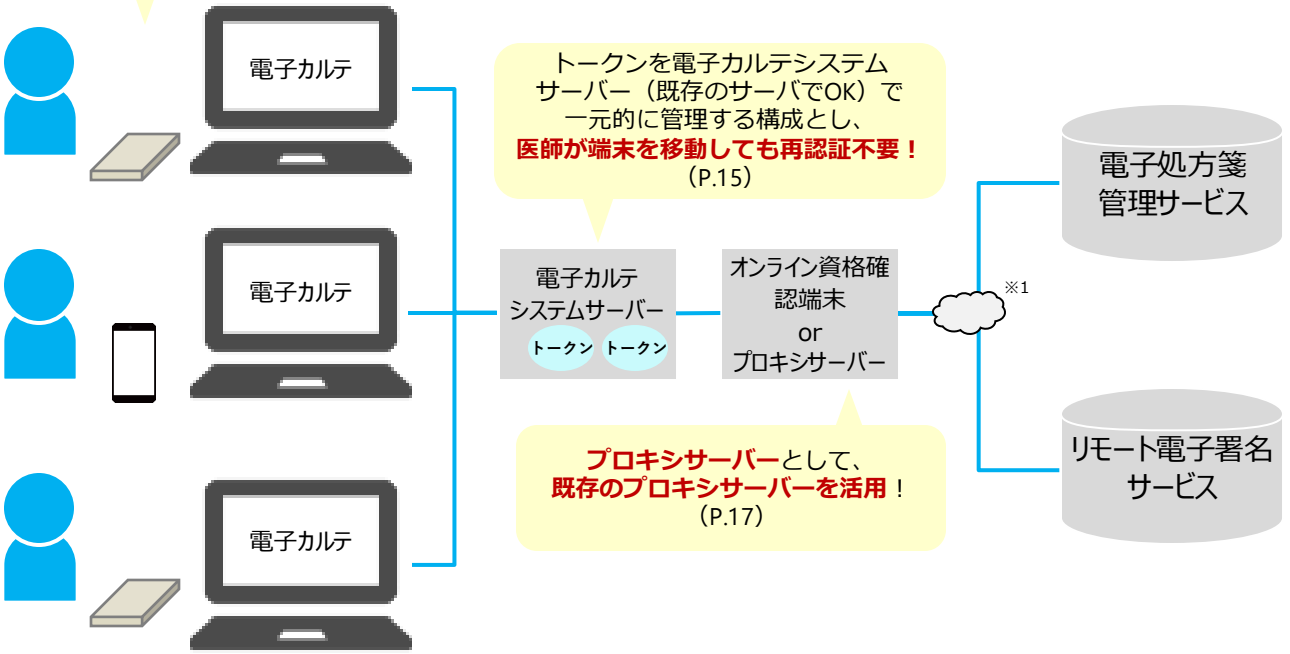
システム構成例は次ページ

システム構成例1（リモート署名）

POINT
①医師が診察室を移動することが多い病院に最適！
②スマホがあればスマホ、マイナンバーカードがあればマイナンバーカードで本人認証！

（資格確認端末を使用し、オンライン資格確認等システムと接続しているケースを想定）

本人認証方法は院内で統一する必要はなく、
マイナンバーカードの人はマイナンバーカード、
スマホの人はスマホでOK！
全端末分のICカードリーダー購入等が不要に！



※1 基本的には、リモート電子署名サービスに接続するためのネットワーク設定が必要となります。

システム事業者に伝えること

- ✓ スマホで認証する医師も多いため、ICカードリーダーは○○台のみ必要
- ✓ トークンを電子カルテ端末ではなく、中央のサーバーで一元的に管理することで診察室を移動する度に本人認証を行う手間を省きたい
- ✓ プロキシサーバーは既存のプロキシサーバーを活用したい

最低限必要な費用（電子署名部分以外含む）

- ✓ お使いいただくシステムのソフトウェア更新費用（電子処方箋対応版に更新）
- ✓ 署名モジュールのライセンス費用
- ✓ ICカードリーダー×必要台数分
- ✓ リモート署名サービスに接続するためのネットワークの設定費用
  ※「リモート電子署名サービス」に接続するための設定が必要です。

システム構成例2（リモート署名）

POINT

①医師が診察室を移動することが多い病院に最適！

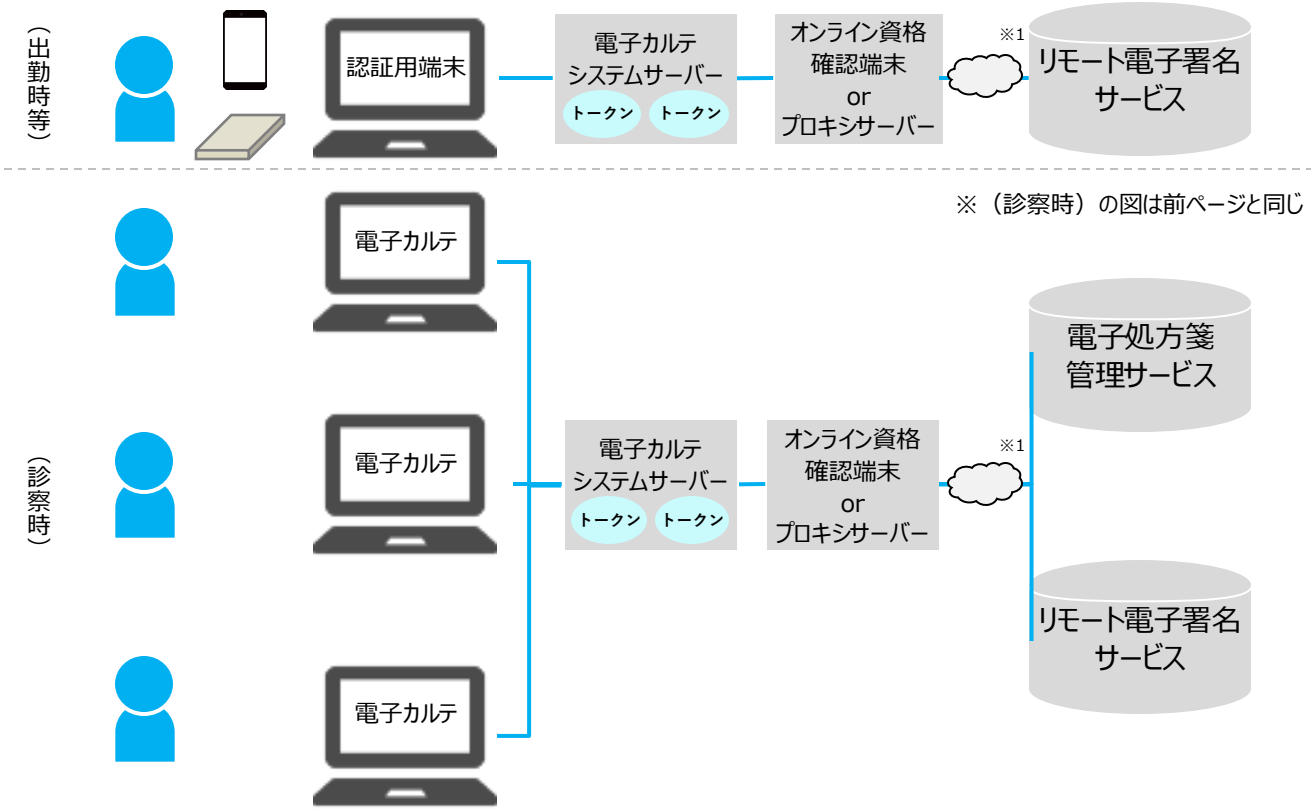
②スマホがあればスマホ、マイナンバーカードがあればマイナンバーカードで本人認証！

③本人認証に使うICカードリーダー・端末を一部端末に集約！

本運用を系列病院間で統一することで、更なるコスト削減＆運用の簡素化が実現！

（資格確認端末を使用し、オンライン資格確認等システムと接続しているケースを想定）

本人認証を一部端末でのみ行う運用とし、出勤時等に1回認証を行う。
これにより、ICカードリーダーの費用削減に繋がるだけでなく、端末によってカード認証ができない等を防げる。



システム事業者に伝えること

- ✓ 認証用の端末を設けるため、ICカードリーダーは当端末数分必要
- ✓ トークンを電子カルテ端末ではなく、中央のサーバーで一元的に管理することで診察室を移動する度に本人認証を行う手間を省きたい
- ✓ プロキシサーバーは既存のプロキシサーバーを活用したい

最低限必要な費用（電子署名部分以外含む）

- ✓ お使いいただくシステムのソフトウェア更新費用（電子処方箋対応版に更新）
- ✓ 署名モジュールのライセンス費用
- ✓ ICカードリーダー×認証用の端末分
- ✓ リモート署名サービスに接続するためのネットワークの設定費用
  ※「リモート電子署名サービス」に接続するための設定が必要です。

※1 基本的には、リモート電子署名サービスに接続するためのネットワーク設定が必要となります。

導入費用に関するQ&A

Question

Q) 大規模病院の場合、ICカードリーダーを端末分購入することで導入費用が高くなります。
費用を抑える方法があれば教えてください。

Answer

A) リモート署名の場合はICカードリーダー数を低減できるため、導入費用を抑えることができる可能性があります。
リモート署名の場合、1日1回本人認証を行った上で電子署名ができるようになるため、本人認証の機能を特定の端末（最低1台）でのみ実装し、出勤後等に医師等が当該端末で本人認証を行う運用とすることが可能です。（P.26）
※本人認証は、HPKIカードまたはマイナンバーカードをICカードリーダーにかざす方法（カード認証）とスマートフォンによる生体認証（FIDO認証）がありますが、病院内で統一させる必要はありません。
これにより、ICカードリーダーを端末分購入する必要はないため、購入費用を削減できます。
なお、認証用の端末を設けず診察室内の各端末でカード認証で本人認証を行う場合、ICカードリーダーの購入費用を抑えると、医師が使用する診察室によっては、端末にICカードリーダーが接続されておらず、カード認証を行いたい医師が認証できない事態が発生する可能性があります。
※FIDO認証はICカードリーダーを使用しませんので、端末にICカードリーダーが接続されていなくとも本人認証が可能です。
そのため、P.26のように、認証用の端末を設け、当端末で全ての本人認証方法に対応できるような運用や、FIDO認証も併用できるような運用にした場合は、ICカードリーダーの購入費用を抑えつつこのような事態も防ぐことができます。運用上も問題ありませんので、病院の実態に合わせて運用方法をご検討ください。