はじめての HPKI
～ 実装の手引き ～

2021 年 3 月

一般財団法人医療情報システム開発センター

はじめての HPKI
～ 実装の手引き ～
目　　次

1 はじめに

みなさんは HPKI をご存じでしょうか？まあ、いまこの文章を読み始めた方なので、知っているか、少なくとも興味があるから読み始めてもらえたのだと思いますけど。

HPKI は「Healthcare Public Key Infrastructure」の略で、日本語では「保健医療福祉分野公開鍵基盤」といいます。HPKI が何なのかや成り立ちについては 2 章で詳しく述べますが、そもそもこの HPKI、残念ながら認知度が低いのです。そのため、正直なところ、広く普及していません。ただ、HPKI そのものは 20 年以上も前から存在していて、しかも、厚生労働省の政策として位置付けられているものです。

HPKI が始まった時代は、IT 革命という言葉が流行った頃で、電話や FAX で仕事をしていたスタイルが電子メールに置き換わったり、図書館に行かなくてもインターネットを使って様々な情報を得ることができるようになったりなど、どちらかというと生産性や利便性の向上を目指して日本全体が IT 化というものに突き進んでいた時代でした。そのような中で、ざっくり言うとセキュリティ対策のひとつとして登場した HPKI は、あまり人気者ではありませんでした。

ところが、その後、IT が ICT ともいわれるようになり、人と人のコミュニケーションツールになった他、ビッグデータと呼ばれる膨大なデータを解析してビジネスや研究に使う時代になると、個人情報の保護やセキュリティに注目が集まるようになりました。特に医療分野では、国民が病気になって患者といわれる存在になった瞬間に、守らなくてはならない情報が他の分野に比べて飛躍的に多くなり、かつ、その情報を扱える医療従事者の識別や許可が非常に重要で大事になります。そのために HPKI は欠かせない仕組みになってきました。

ただ、これまで、あまり人気者でなかったのと、仕組みも複雑だと思われているため、HPKI に関わってきた者としては、普及するには、認知してもらうには、必要性を認識してもらうにはどうしたらよいのかと、悩みを抱えていました。そこで、「ならば、いま必要とされる HPKI について分かりやすい解説書を作ろう！」ということで、本書を編纂することになりました。

本書は、まず HPKI に関する歴史も含めた基礎知識を知ってもらいます。次に具体的に HPKI を使うためのプログラムを作る環境を示して、実際にプログラミングしてもらえるようにプログラムを解説すると共にサンプルコードを用意しました。そして、それが出来上がった時に、どこでどのように使うものなのかを適用例として説明しています。

本書は分かりやすさを心掛けました。みなさまに読んでいただくことで HPKI に関する知識を習得してもらうだけでなく、その必要性に関しても知っていただくことを目的としています。是非、本書を活用して HPKI に詳しくなっていただければと思います。

2　HPKI を知ろう

2.1　PKI の基礎知識

HPKI の話を始める前に、HPKI の基本となる公開鍵基盤（Public Key Infrastructure : PKI）について簡単に説明します。ただし、本書は HPKI の実装のための手引きですので、PKI のことをよく知っている読者の方は読み飛ばしてもらって構いませんし、より詳しく知りたい読者の方は、別途、PKI に関する解説書や Web 上の情報を参考にして知識を深めてください。

2.1.1　私有鍵と公開鍵

認証局の技術は、暗号技術の中の「公開鍵暗号」という方法を使っています。この公開鍵暗号という技術は、以下のような特殊な性質を持っています。

- ペアになる 2 つの暗号鍵を作成します。このペアの鍵を仮に鍵 A と鍵 B と呼ぶことにします。
- 普通、金庫などの鍵は鍵と鍵穴が一致すれば空きますが、このペアの鍵は不思議な仕組みになっていて、鍵 A で暗号化した電子情報は、鍵 B でしか元に戻せません（元に戻すことを「復号」と言います)。
- 逆に、鍵 B で暗号化した電子情報は鍵 A でしか復号できません。
- 次に、鍵 A と鍵 B のうち、どちらかは本人だけが扱えるように厳密な管理の上で保管します。もう一方の鍵は誰でも使えるようにインターネット等に公開してしまいます。
- 厳密に管理された鍵を「私有鍵」、公開された鍵を「公開鍵」と呼びます（以下の例では、鍵 A を私有鍵、鍵 B を公開鍵としています)。

そして、私有鍵（鍵 A）は、厳格な管理をするために、その多くは IC（Integrated Circuit : 集積回路）チップが搭載された IC カードに格納されています。IC カードには色々な種類がありますが、今のところ HPKI ではクレジットカードやキャッシュカードのような金色のチップが付いたカードが使われています。

私有鍵と公開鍵をイメージにすると、図 2.1 のようになります。

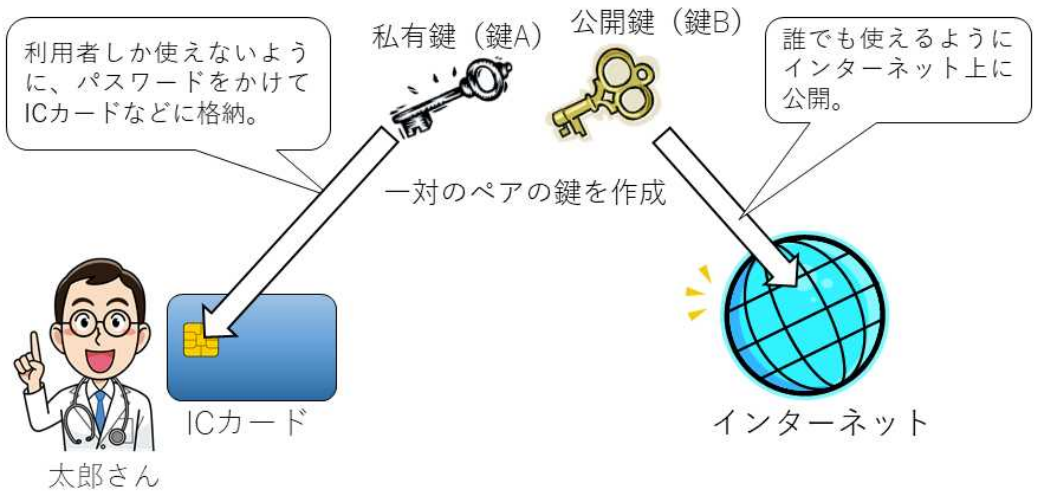


図 2.1　私有鍵と公開鍵のイメージ

さて、なぜこんな不思議な仕組みを使うのかというと、それはインターネットの発展と大きく関係しています。

公開鍵暗号方式が出てくるまでは、暗号というのは、例えば、相手に「あいうえお」と伝えたいメッセージを「うえおかき」と 3 文字ずらして暗号として伝えるというような方法を使っていました。そのため、メッセージを受け取る相手は、この暗号メッセージは「3 文字ずらしている」ということを予め知っておく必要があります。この時、この「3 文字ずらす」という情報が「鍵」になります。そのため、お互いが鍵を知らないといけないので、この暗号方式を共通鍵暗号方式と言います。

ところが、インターネットでその鍵を相手に送ると、送っている途中で鍵を盗まれてしまう可能性があります。これでは暗号の意味がありません。そのために鍵の情報だけ郵便で送るというのもインターネットがあるのに不便です。そこで考え出されたのが、公開鍵暗号方式で、不思議ですが鍵の一つをインターネット上に晒してしまっても大丈夫という仕組みができあがりました。

次からは、この不思議な仕組みの使い方を説明します。

2.1.2　鍵の使い方

不思議な仕組みを持った公開鍵暗号の使い方は 3 つあります。もちろん、暗号なので「暗号化」に使えます。それに加えて、「電子署名」と「認証」に使えます。それぞれ、次のような使い方をします。

① 暗号化

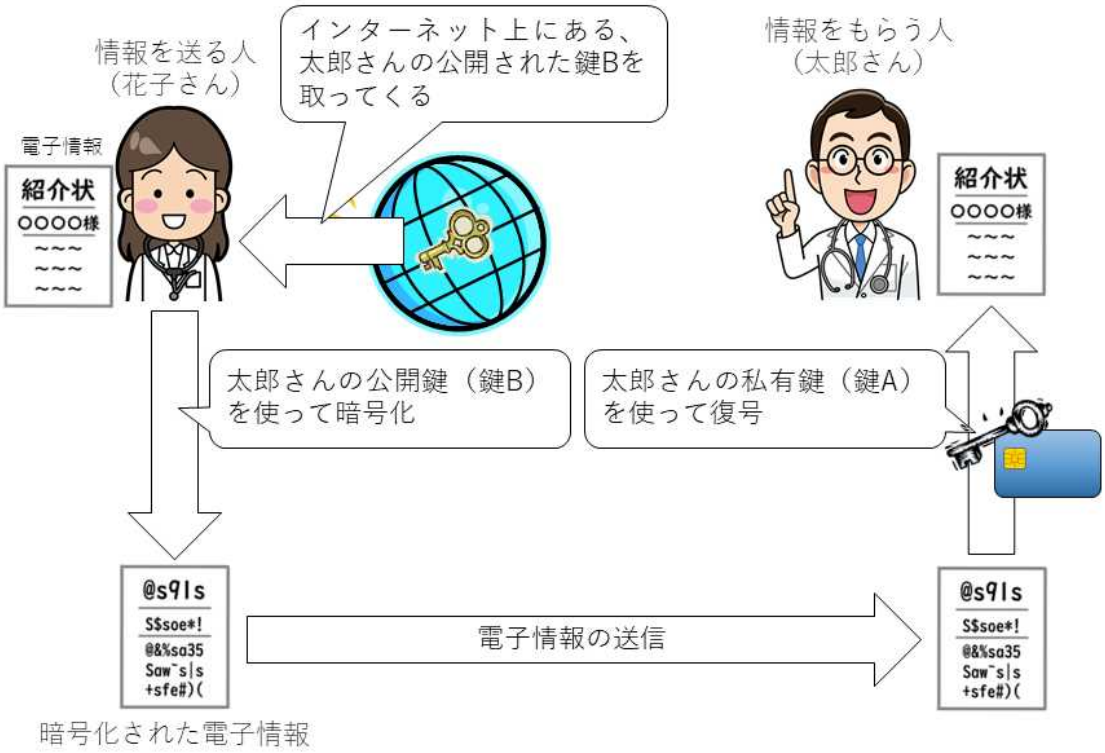


図 2.2　情報の暗号化

この例は、情報を暗号化して相手先に送る場合を示しています。太郎さんの公開鍵（鍵 B）はインターネット上にあるので、情報を送りたい人である花子さんがその鍵を入手して電子情報を暗号化します。そうすると、公開鍵（鍵 B）で暗号化された電子情報は、太郎さんだけが持つ私有鍵（鍵 A）だけでしか復号できないので、太郎さんだけしか読むことができません。そのため、他の誰にも中身を見られることなく内容を伝えることができるようになります。

ただし、公開鍵暗号は暗号処理に時間がかかるため、実際に公開鍵暗号で暗号化された情報のやり取りをするというのは広く普及していません。実際の暗号情報のやり取りは、まず旧来の暗号方式である共通鍵暗号で情報を暗号化して、その暗号化に使った「鍵」を公開鍵暗号の公開鍵（鍵 B）で暗号化して相手に送るというやり方が主流です。

② 電子署名

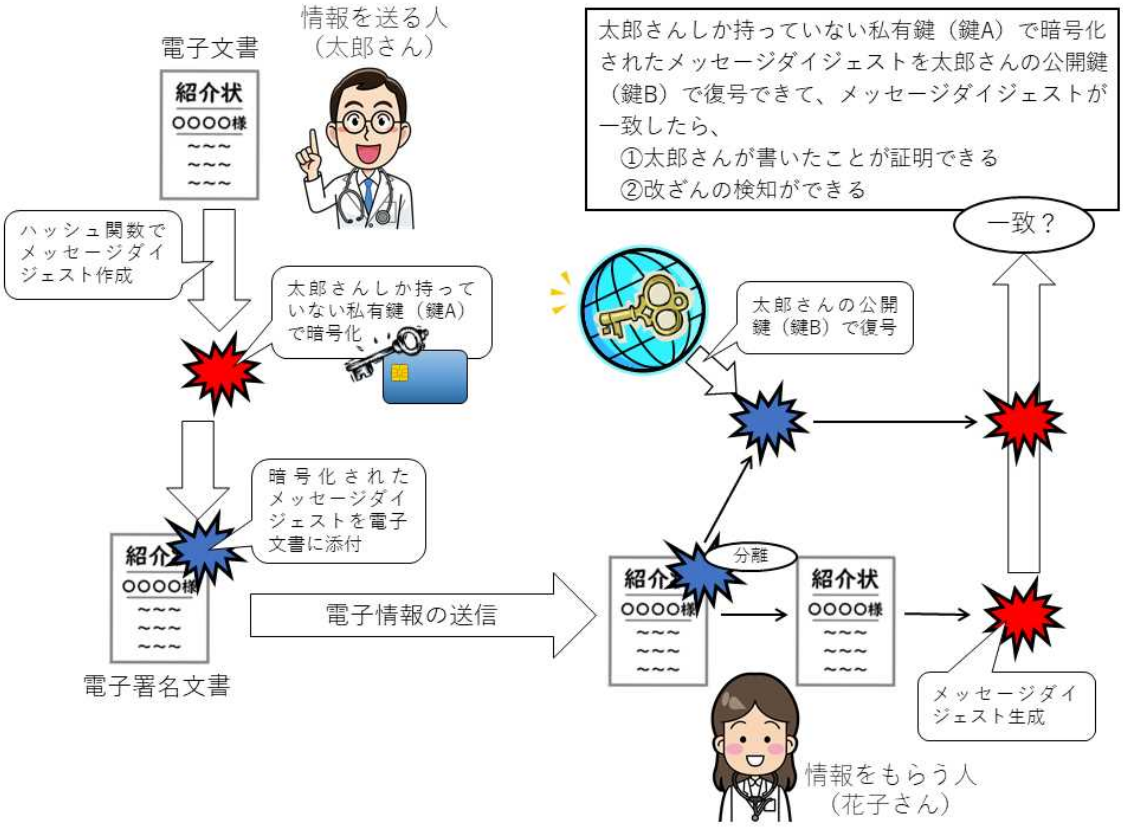


図 2.3　電子署名

この例は、電子情報を書いた人を確認するための使い方を示しています。現実の世界でも、書類を書いて、私が書きましたと証明したり保証したりするために判子を押したり、サインをして相手に渡して、受け取った人は確かにその人が書いたことを確認しますが、これと同じく電子的に判子やサインをするための使い方です。そのため、これを「電子署名」と呼んでいます。

電子署名のやり方ですが、まず太郎さんが太郎さんしか持っていない私有鍵（鍵 A）を使って電子情報を暗号化します。そして、メールなどでその情報をもらった花子さんは、インターネット上に転がっている太郎さんの公開鍵(鍵 B)を取ってきて復号します。この場合、誰でも情報を復号できるので、秘密情報のやり取りはできませんが、太郎さんしか持っていない私有鍵（鍵 A）と対になる太郎さんの公開鍵（鍵 B）で元に戻せたということは、送られてきた電子情報が確かに太郎さんによって暗号化されたことが分かります。そうすると、この電子情報は、確かに太郎さんが書いた電子情報ということになって、太郎さんが押印（サイン）した情報ということになります。

そして、ここでおまけが一つ付きます。暗号化されていた文書がどこかで変更されると、電子情報が壊れてしまうので、ペアになる公開鍵（鍵B）で復号できなくなります。そのため、そのまま元に戻せた事実から、送られるまでの間のどこかで文書に変更を加えられていないことも同時に知ることができます。このおまけのことを「改ざん検知」と言って、HPKIの世界では、特に重要なおまけになります。これは、この後の HPKI の電子署名の説明の中で、その重要性について触れます。

ここまでが電子署名の説明ですが、正確な電子署名のやり方は、電子情報全体を暗号化してはいません。電子情報をそのまま暗号化するには処理に時間がかかるため、ハッシュ関数と言われる、一度、その関数で情報を処理すると情報を元に戻せなくなるという“変わった関数”を使って、元の文書から小さい情報の塊である「メッセージダイジェスト」と言われるものを作ります。そして、それを私有鍵（鍵 A）で暗号化します。その上で、暗号化したメッセージダイジェストを送りたい電子情報と一緒にして相手に送ります。ハッシュ関数は、元の文書が一文字でも変更されると異なるメッセージダイジェストになるという特性があるため、送られた電子情報から再度メッセージダイジェストを作ります。それと暗号化されたメッセージダイジェストを公開鍵（鍵 B）で復号して、双方が一致することを確認して、電子署名した人の確認と改ざん検知をしています。

③ 認証

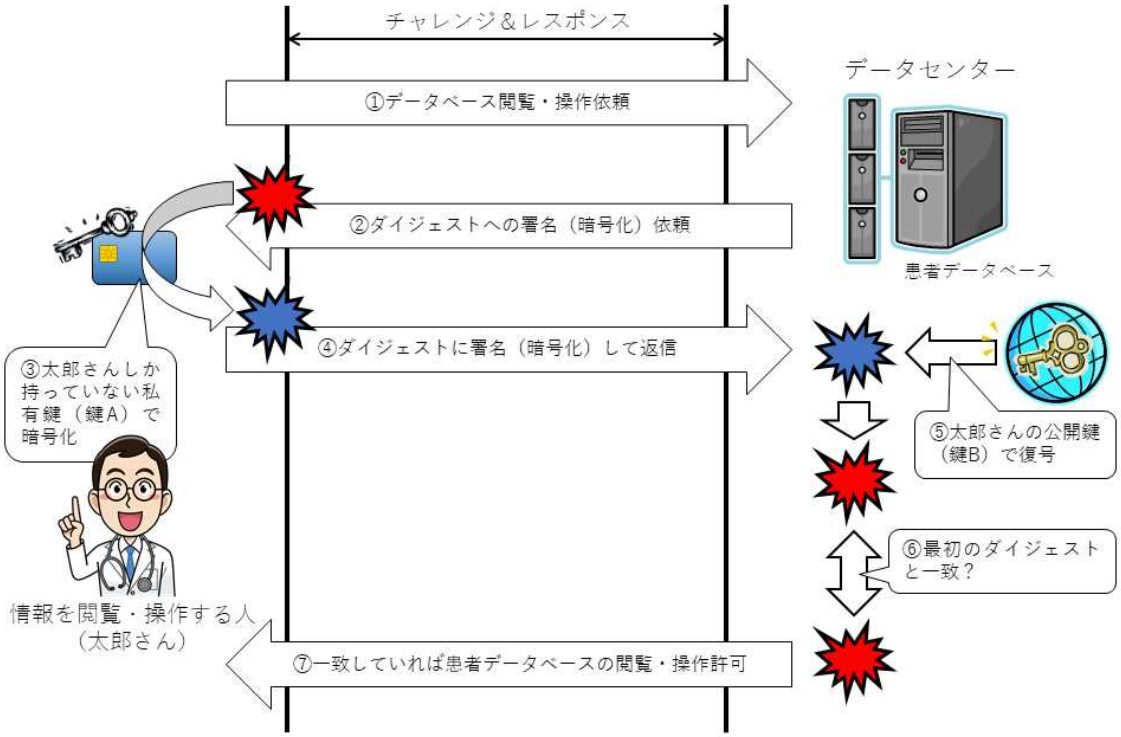


図 2.4　認証

この例では、データセンターにある（患者）情報に太郎さんがアクセスして、情報を閲覧したり、操作したりする例を示しています。

まず、太郎さんは閲覧・操作したい情報が存在する患者データベースに閲覧・操作の依頼のためにアクセスします。そうすると、データセンター（＝データベースサーバー）が、適当な情報をハッシュ関数でメッセージダイジェストにして太郎さんに送ってくるので、太郎さんは自分の私有鍵（鍵 A）でメッセージダイジェストを暗号化（署名と同じ）します。暗号化されたメッセージダイジェストを受け取ったデータセンター（＝データベースサーバー）は、太郎さんの公開鍵（鍵 B）をインターネットから取ってきて、暗号化されたメッセージダイジェストを復号して、元々送ったメッセージダイジェストと比較をします。これが一致すれば、確かに太郎さんであることが確認できるため、太郎さんに対してデータベースの閲覧・操作を許可するという流れです。ID とパスワードでログインする代わりに、公開鍵暗号を使う方法になります。なお、この一連の流れをチャレンジ＆レスポンスと呼んでいます。

2.1.3　認証局の役割

ここまで PKI の技術について説明をしてきましたが、一つだけ欠けていることがあります。電子署名や認証ができることはよいのですが、特に電子署名を使う場合、そもそも、その鍵のペアを誰が作ったのか、誰が持っている鍵のペアなのかという点が非常に重要になります。

実は、私有鍵と公開鍵のペアを作ることは、コンピューターがあれば誰でもできてしまいます。そのため、見ず知らずの人が鍵のペアを作って電子署名して送ってきたとしても、公開鍵と私有鍵が誰のものか分からないと、電子署名を信頼していいのか分かりませんよね。あなたが太郎さんのことをとてもよく知っていたとしても、誰でもコンピューターを使えば鍵を作れるとなると、誰かが太郎さんと嘘をついて鍵を作っているかもしれません。

そのため、公開鍵暗号を使う場合、「ペアになる私有鍵と公開鍵は誰が作るのか」、「誰が私有鍵と公開鍵を持っている人を保証してくれるのか」という 2 つが必要になります。

そこで、私有鍵と公開鍵を作って、その鍵の所有者を第三者として証明してあげる必要があります。そのための組織のことを「認証局」と言います。役所に行って、印鑑登録をすると印鑑登録証明書が首長さんの名前で発行されますが、それと同じで、認証局として鍵の正当性を証明する組織なので、いわば電子空間のための役所です。

このため、認証局の役割は大変重要で、私有鍵と公開鍵を作って欲しいと依頼してきた人が本当に依頼して来た本人であるか、厳密に審査して、確実に本人に私有鍵を届けなくてはなりません。

一方、依頼する側や世間からみた場合、その認証局がどこまで信頼できる組織であるか、

世間的に認知された組織であるかが重要です。聞いたこともない組織が作成した鍵のペアは信頼できないと思います。したがって、認証局は、個人的にあそこは好き、ここは嫌いという話はさて置き、「厳密な本人確認審査ができる組織であること」、「世間に一定程度認知され、信頼されていること」が必要になります。

これが認証局に求められる条件ですが、具体的な業務としては、確かに本人であることを確認してペアになる私有鍵と公開鍵を作ること、私有鍵を IC カードなどに格納して確実に本人に渡すこと、公開鍵には、認証局で確認したことを証明する情報を追加してインターネット上などに公開することになります。

ここで、もう一つ重要なキーワードがあります。この公開鍵に情報を追加されたもののことを「電子証明書」と呼びます。電子証明書には、鍵ペアを作って欲しいと依頼して来た人の情報（名前など）と共に認証局としてちゃんと本人であることを確認した証明や有効期限などの情報が追加されています。それらの追加情報と公開鍵を包んだ形にしたものが電子証明書です。

したがって、電子証明書は、電子情報に付いてくる暗号化されたメッセージダイジェスト（電子署名）を、その中に包まれた公開鍵で復号すると同時に、その公開鍵が確かに本人のものであると証明する役割を果たす大事な証明書です。そのため、電子空間上の身分証明書と言われたりもします。

以上、技術の話から、認証局という組織の話まで説明をしてきました。

技術は日進月歩であり、認証局で使われる暗号技術はこれからも進歩し続けるので、必ずしも、いま使われている公開鍵暗号が使われ続けることはなく、新たな優良な技術が登場した場合、それはその技術を使うようになるでしょう。

一方、認証局のもうひとつの側面である組織の部分に関しては、技術とは関係なく、現実世界における組織としての体制、信頼度が重要であって、それらの総合的な信頼度が「認証局」を運営しようとする組織にとって非常に重要な要因となります。

難しい話が続きましたが、次からはいよいよ本題の HPKI の話に入ります。

2.2　HPKI の歴史

ここでは、HPKI の歴史について振り返ります。HPKI は、2004 年に厚生労働省に設置されていた、「医療情報ネットワーク基盤検討会」（当時）がとりまとめた最終報告書（以下、最終報告書、という）から始まります。

この最終報告書は、今後の医療情報ネットワーク基盤のあり方について提言したもので、2005 年に全面施行を控えた「個人情報の保護に関する法律」（個人情報保護法）や 2000 年

に成立した「電子署名及び認証業務に関する法律」（電子署名法）を見据えつつ、当時の情報通信技術に基づく医療情報の取り扱いについて、技術や運用管理上の基盤整備の必要性について述べていました。

主だった内容は、(1) 公開鍵基盤、(2)書類の電子化、(3)診療録等の電子保存の 3 つです。この中の「(1) 公開鍵基盤」の検討結果が、報告書の中で「Ⅱ．医療における公開鍵基盤（Public Key Infrastructure ：PKI）のあり方について」としてまとめられています。それを要約すると、次のようなことが書かれています。

・公開鍵基盤は、医療分野の IT 化の推進には必要不可欠なシステムであると考えられる。
・本検討会としては、医師等の個人が電子署名を活用するための公開鍵基盤のあり方を優先的に検討した。
・署名自体に公的資格の確認機能を有する保健医療福祉分野の公開鍵基盤（ヘルスケア PKI；HPKI: Health Public Key Infrastructure）の整備を目指していくことが必要である。
・ヘルスケア PKI 認証局開設は、国際的標準との整合性も念頭に置き、ISO /TS 17090（国家資格の記載は hcRole)を参酌標準として位置づけるべきである。(注:現在は IS。)
・ヘルスケア PKI 全体として整合性を確保するために、各ヘルスケア PKI 認証局が準拠すべき証明書共通ポリシを早期に作成し公表すべきである。
・併せて、ヘルスケア PKI 認証局が共通ポリシに準拠することを担保するための審査を行う仕組みを設けることが必要である。
・医療機関等を組織として認証することについては、当該組織を代表する者を自然人として認証することと併せて、開設者や管理者（病院長等）としての役割を、例えば、hcRole に位置づけること等により、結果として組織の認証が可能となるという方法が考えられる。

（出典）医療情報ネットワーク基盤検討会最終報告書（平成 16 年 9 月 30 日）
https://www.mhlw.go.jp/shingi/2004/09/s0930-10a.html

厚生労働省は、この報告書を受けて、2005 年に HPKI 認証局共通の運用ルールである「保健医療福祉分野 PKI 認証局証明書ポリシ」を策定すると共に、そのルールに準拠していることを審査するための会議体として「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」（HPKI 専門家会議）を設置しました。そして、翌 2006 年 3 月には準拠していることを監査するための「保健医療福祉分野 PKI 認証局　証明書ポリシ準拠性監査報告書様式」を定めます。この一連の動きは、2005 年度の 1 年間の動きであり、一気に HPKI を国の制度として仕立て上げました。厚生労働省にしてはなかなかのスピード感です。

そして、準拠性監査報告書様式を決めた時の HPKI 専門家会議で、厚生労働省が HPKI 認証局を構築して、証明書ポリシに準拠した認証局に対して相互認証を可能とする仕組み

を提供するという認証局構築・運営事業を開始しました。この時に、相互認証の協力依頼を受けたのが、日本医師会と MEDIS の認証局でした。これが日本初の署名用 HPKI 認証局です。

ここまでは、医師などが書いた文書、例えば紹介状に医師の押印が必要なので、それを電子的に作るなら電子的な押印の電子署名が必要ということで電子署名用の認証基盤が整備されました。また、診療録を電子的に保存する時にも、改ざん（不正な変更）がされていないかを担保するのにも電子署名が必要でした。そのため、電子署名をする認証基盤の整備が先行した形になります。

しかし、これに続いて 2009 年には、同じく医療情報ネットワーク基盤検討会に今度は認証用の HPKI 認証基盤の整備の必要性が提言されました。

2005 年に個人情報保護法が全面施行されて、医療情報の電子保存に必要な様々な条件が徐々に明確になってきたこの頃から、聞いたことがあるかもしれませんが、電子的に医療情報を扱う「地域医療連携システム」が各地で使われるようになります。そうなると、当然、医師や看護師などの医療国家資格を確認してからでないと医療情報（患者の情報）を扱ってはいけないということで、ログインなどに使う認証用の HPKI の基盤整備が必要となった訳です。時代の流れですね。

以上のような歴史があって、HPKI 認証局は成り立っています。現在では、日本医師会が HPKI 専用の附属機関として設置した日本医師会電子認証センターと MEDIS に加えて、日本薬剤師会が薬剤師向けの HPKI カードを発行していて、国内の HPKI 認証局は 3 つ存在しています。

【補足：HPKI と医療情報システムの安全管理に関するガイドライン】

最終報告書では、当時、バラバラだった「診療録等の電子保存ガイドライン」、「診療録等の外部保存ガイドライン」と 2004 年に成立した「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（e-文書法）の厚生労働省令に対応した医療機関向けの分かりやすいガイドラインを作成するべきだということも提言しています。その結果出来上がったのが、みなさんよくご存じの「医療情報システムの安全管理に関するガイドライン」（2005 年 3 月に初版発行）です。

実は、このガイドラインでも、電子署名を使う場合の要件として、HPKI にも触れられています。2021 年 3 月に改訂され、現時点で最新版になる 5.1 版では「6.12　法令で定められた記名・押印を電子署名で行うことについて」の中で、C 項の最低限のガイドライン（必ず守るべきガイドラインのことです）で以下のように定められています。

1. 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局又は認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと

2. 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
3. タイムスタンプを付与する時点で有効な電子証明書を用いること

ここではリード部分だけを記載したので、それぞれの中身については、より具体的な定めがありますが、それは実際にガイドラインをお読みいただくとして、ここで重要なことは、ガイドラインで HPKI が推奨されていることと、本書ではあまり深くは触れませんが、その文書がその時間に存在していたという時間を証明する必要があること、当然ですが有効な電子署名を用いる必要があることが、必須の要件となっていることです。

時間を証明するために必要なものをタイムスタンプ、電子署名が有効か確認するための情報のことを失効情報（Certificate Revocation List：CRL）と言って、いずれも HPKI には重要な要素です。なお、タイムスタンプや CRL を使うためには、ネットワーク（インターネットに限りません）への接続が必要になってきます。特に CRL は、その電子証明書を無効にした（失効した）情報を提供する仕組みのため、誰でも入手できるようにインターネット上に公開されたサーバーに置いてあります。

また、e-文書法に対応するためにも電子署名は重要な役割を果たしていて「9. 診療録等をスキャナ等により電子化して保存する場合について」で触れられています。ただし、この場合の電子署名は HPKI の電子署名に限定されている訳ではありませんが、HPKI の電子署名が有用な手段であることには変わりありません。

このように HPKI は、それ単独で規定などがあるものではなく、様々な施策やガイドライン、通知でも登場しています。

2.3 HPKI の仕組みと必要性（署名と認証）

2.3.1 HPKI の仕組み

HPKI は最終報告書でも触れられている通り、ISO IS 17090 という国際標準に準拠した基盤として整備されています。その最大の特徴は、他の PKI と違って、電子証明書の中に、直接、厚生労働省が所管する医療の国家資格が格納されていることです。その国家資格は、hcRole という領域に格納されていて、次のように 27 の医療国家資格と 5 つの管理責任者の情報を格納できるようになっています。

表 2.1　hcRole に格納できる資格情報

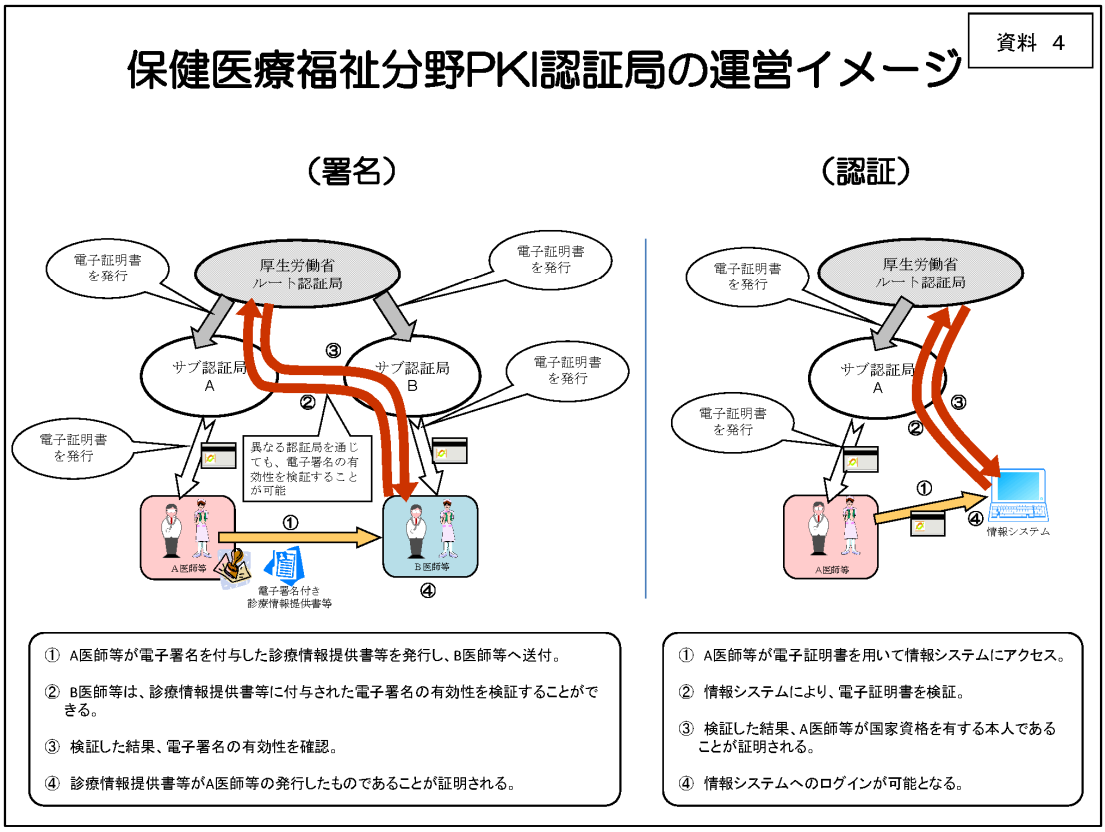
資格名【国家資格】	
医師 (Medical Doctor)	社会福祉士 (Certified Social Worker)
歯科医師 (Dentist)	介護福祉士 (Certified Care Worker)
薬剤師 (Pharmacist)	救急救命士 (Emergency Medical Technician)
臨床検査技師 (Medical Technologist)	精神保健福祉士 (Psychiatric Social Worker)
診療放射線技師 (Radiological Technologist)	臨床工学技士 (Clinical Engineer)
看護師 (Registered Nurse)	あん摩マッサージ指圧師 (Massage and Finger Pressure Practitioner)
保健師 (Public Health Nurse)	はり師 (Acupuncturist)
助産師 (Midwife)	きゅう師 (Moxibustion Practitioner)
理学療法士 (Physical Therapist)	歯科衛生士 (Dental Hygienist)
作業療法士 (Occupational Therapist)	義肢装具士 (Prosthetist and Orthotist)
視能訓練士 (Orthoptist)	柔道整復師 (Judo Therapist)
言語聴覚士 (Speech Therapist)	衛生検査技師 (Clinical Laboratory Technician)
歯科技工士 (Dental Technician)	公認心理師 (Certified Public Psychologist)
管理栄養士 (National Registered Dietitian)	
資格名 【医療機関の管理責任者】	
病院長 (Director of Hospital)	
診療所院長 (Director of Clinic)	
管理薬剤師 (Supervisor of Pharmacy)	
薬局開設者 (Proprietor of Pharmacy)	
その他の保健医療福祉機関の 管理責任者 (Director)	

この辺りの詳細は、参考文献にも記載している保健医療福祉分野 PKI 認証局証明書ポリシの「7.1.10　保健医療福祉分野の属性（hcRole)」に詳しく書かれていますので、そちらをご覧ください。

また、厚生労働省は、相互認証を可能とするための認証局構築・運営事業で「厚生労働省ルート認証局」と言われるものを構築しました。認証局の相互接続は、それぞれの認証局同士がお互い認め合って接続する方法もありますが、これでは複数の認証局が出てきた場合、それぞれに話し合いをする必要があります。もちろん、技術的な接続も必要になります。

これでは効率が悪いので、HPKI の仕組みでは、一つ親になる認証局を作ることにしました。これが厚生労働省ルート認証局です。こうすることで、HPKI 認証局になろうとする組織が、保健医療福祉分野 PKI 認証局証明書ポリシに従って運営体制と認証局のシステムを準備した上で、準拠性監査報告書様式に則って審査を受けて合格すると親の認証局に接続することができます。

接続と言っても回線で繋がっている訳ではなく、親の認証局から子供の認証局に対して、「あなたは HPKI ですよ」と認めてもらった電子証明書を受け取って、それを組み込むことで実現しています。細かな技術論には触れませんので、厚生労働省が公開している資料を参考までに示しておきます。



（出典）第 4 回 HPKI 専門家会議（平成 25 年 5 月 16 日）資料 4
https://www.mhlw.go.jp/stf/shingi/2r985200000327wq-att/2r98520000032are.pdf
図 2.5　HPKI 認証局の運用イメージ

こうすることで、例えば、日本医師会の認証局から発行された電子証明書は公式に厚生労働省から認められた電子証明書ということになり、また、同じく子供である MEDIS の認証局でも日本医師会の認証局の電子証明書を確認することができるため、相互に認証・確認し合うことが可能になります。

なお、図 2.5 の資料は左側が電子署名、右側が認証の説明になっています。2009 年には認証用の証明書ポリシは完成していて、それを受けた実証事業は実施されていましたが、国の仕組みとしては、2013 年に厚生労働省ルート認証局が認証用に対応して、現在の署名用と認証用の HPKI となりました。

2.3.2　HPKI の必要性（署名）

HPKI の仕組みでも触れた通り、HPKI が通常の PKI でなく、HPKI と呼ばれる最大の特徴は、電子証明書に厚生労働省が所管する医療の国家資格が格納されていることです。単に私有鍵と公開鍵があって、認証局が公開鍵に本人であることを保証する情報や有効期限を追加するだけでなく、医師などの医療国家資格の情報も追加して格納されています。そのため、HPKI は電子証明書だけで医療国家資格の保有者であることを確認することができ

ます。

この仕組みを用いない場合、例えば、通常の PKI で電子署名をしても、署名された電子情報は確かに本人が署名して、改ざんがされていないことは分かっても、医師であるということを確認できません。そのため、別に医師であることを確認できるテーブルや対応表を用意して、電子証明書や何かの識別子と紐付けして管理や確認をする必要があります。お互いに知っている人同士でやり取りしているだけなら、送信者が本人であって、改ざんされてないことが分かれば、対応表を用意するまでもありませんが、不特定多数の人とやり取りする場合はそうはいかなくなります。

・医療国家資格を証明することの必要性

さて、そのような特徴を持つ HPKI が、なぜ必要かという話をします。答えは単純です。HPKI の歴史の中でさらっと触れましたが、医療の世界では、その資格を持った人が責任を持って書類に押印やサインをすることや資格を提示した上で情報に触れる（アクセスする）ことが非常に重要だからです。

あなたが診療所に行って、より詳しく検査を受けるために病院に紹介してもらう場合、紹介状というものを診療所の医師に書いてもらうはずです。この紹介状、正確には診療情報提供書といいますが、これは医師があなたを診察した時の状況や飲んでいる薬や検査の情報を書いて、紹介する先の病院の医師に症状に関する情報を伝えるものです。

当然、症状に関する情報、薬や検査の情報が書かれているので、医師でなくては書いてはいけません。そして、それを証明するために紹介状を書いた医師は、押印やサインをしています。それだけではなく、法律で押印やサインをしなくてはならないと決められているものもあります。ざっと挙げみても、次のようなものがあります。

○出生証明書（医師法等）、○死亡診断書、死体検案書、死産証書（医師法等、死体解剖保存法等）、○処方せん（医師法等）、○照射録（診療放射線技師法等）、○難病指定医、協力難病指定医の診断書（難病の患者に対する医療等に関する法律等）、○小児慢性特定疾病医療費の支給を受けようとするときに提出する指定医の診断書（児童福祉法等）、○脳死に至ったという判定が的確に行われたことを証する書面（臓器の移植に関する法律等）、○要介護認定等に係る主治医意見書（介護保険法等）、○傷病手当金支給申請書（健康保険法等）、○治験責任医師等の作成する症例報告書（薬機法等）

これらが全て電子化されている訳ではないですが、少なくとも紙から電子情報にする場合に、「医師本人であることの証明」をする必要があります。これを実現できるのが HPKI です。

なお、本書を執筆している時点で、政府もデジタル庁の設置や行政のデジタル化などデジ

タル改革を進めています。この中では、電子的な文書の扱いについて電子署名や電子認証のサービスを活用することが言われていることから、今後、いっそう HPKI の重要性が増すことになります。

・否認防止の必要性

もう一つ、HPKI の電子署名には重要な役割があります。これまでは、電子署名をすることによって、本人であること、医師であること、改ざんされていないこと、この 3 つが保証できると説明してきました。

処方箋を例に取ると、電子的な処方箋に HPKI で電子署名されていれば、医師本人であることと、処方箋の内容が書き換えられていないことが分かります。処方箋を受け取った患者さんは、安心して電子情報を取り扱うことができます。この話は裏を返せば、電子署名を行うためには、本人しか知りえない情報（パスワード）や専用の媒体（HPKI カード）が必要となるため、本人以外が作成することは不可能ですので、医師がその処方箋を間違いなく書いたということになります。この電子署名の役割のことを「否認防止」と言います。

薬の場合、種類によっては服用する量を間違えると重篤な副作用や最悪の場合、死に至る可能性もあります。

あまり例示したくないですが、仮に医師が薬を処方する時に 10mg を処方するところ、間違って 100mg と書いて処方してしまって患者さんに重篤な副作用が出たとします。その時、誰が間違えたのかを判断する際に、医師が「私は書いていない。別の人間が私になりすまして書いたものだ」とか、「私は確かに 10mg と書いた。電子情報なので、途中で誰かに書き換えられた。」などと抗弁することが考えられます。電子的な処方箋で HPKI の電子署名をしていた場合、確かに医師本人が文書の作成責任を負い、文書が改ざんされていないことが確実に分かるため、上記のような抗弁は否定され、医師は間違いなく 100mg と書いたことになります。

電子署名には、否認防止と改ざん検知の機能がありますが、これは、電子署名を行うことで、その電子情報に対して責任を持つという意味を持ちます。処方箋の例に示す通り、医療分野において否認防止は非常に重要な役割になります。

そのため、HPKI の電子署名は、HPKI 認証局証明書ポリシに従って否認防止用の電子署名にしか使えないように証明書に用途が記載されています。

2.3.3　HPKI の必要性（認証）

HPKI の認証での利用は、署名とは別の用途であり、今後の医療分野の ICT 化を考えると、重要性が増すと考えられます。

これまで説明したように、認証という機能は、分かりやすく言えば通行証のような仕組みで、コンピューターにログインする時や SNS にログインする時の ID とパスワードに相当するものです。

ただ、ID とパスワードのように人の頭にある記憶だけに頼るのと違って、現在の HPKI 認証局は、認証用の電子証明書を IC カードに格納して発行していますので、IC カードと IC カードに設定されたパスワードに相当する PIN（Personal Identification Number）が必要になります。ATM でお金を下ろす時に、キャッシュカードを入れて暗証番号を押しますが、あれと同じです。IC カードと PIN のように 2 つの要素がないと使えない認証方式のことを 2 要素認証と呼んでいます。

さて、2 要素認証で用いることができる HPKI の認証での利用ですが、いまのところ、まだそれほど多くは利用されていません。

しかし、医療情報システムの安全管理に関するガイドラインでは、電子カルテなどの医療情報システムへのログインは、2027 年度までに 2 要素認証を採用するように定めています。

特にこれまでは、病院の電子カルテにログインする時も、ほとんどは ID とパスワードで、病院としてその ID が医師や看護師などと分かれば十分でした。また、地域医療連携でも、申し込みの時に医師などの資格を確認して、その ID がその資格者であると識別できれば、医師以外に見せてはいけない情報や薬剤師まで見せていい情報などのコントロールをすることができました。

ところが、地域医療連携が進んで来ると、これまでの自分の地域の医療機関や薬局との連携だけでなく、隣の地域医療連携との接続、特に県境で患者さんが県を跨いで受診するような場合、少し状況が変わってきます。

自分達のエリアであれば、顔見知り同士で繋がることができても、エリアが広範になってくると、お互いそれほどよく知らない者同士で診療情報をやり取りすることになります。また、いま国が進めている「全国で医療情報を確認できる仕組み」が実現すると、これはもう確実に一医師や一医療機関で医療国家資格を確認することは不可能になります。

このような流れを考えると、今後、認証用の HPKI は重要であると共に、必ず使わなければならないものになることも考えられます。

3　必要なものを揃えよう

本章では、PKI を利用するためのソフトウェアを動作させるための条件等について、説明します。

3.1　動作されるために必要な環境

3.1.1　前提条件

① HPKI を利用するためのソフトウェアの動作する環境

HPKI の標準類は、特定の OS やハードウェアを前提としていません。そのため、ターゲットにした環境で必要なカードリーダやソフトウェアの構成要素が揃えば、それを組み合わせて HPKI の利用環境を構築することができます。

IC カードの利用環境は、交通系 IC カードやマイナンバーカード等が使える環境としてスマートホン等でも利用が可能なものが増えてきていますので、IC カードは Windows、iOS, Linux や Android 等様々な OS 環境で利用することが可能です。しかしながら一般的な医療機関での利用を前提とした HPKI では、各認証局が配布している HPKI カードアプリケーションの入出力を制御するドライバーレベルのソフトウェアは Windows に対応しています。もちろんこの部分のドライバーを標準類を参照しながら独力で開発することも可能です。

今回のサンプルプログラムでは、サンプル HPKI カードによって最低限度の労力で動作させることを前提としますので、Windows の環境が対象となります。

様々な OS やカードリーダの対応状況に関する情報は、「JAHIS HPKI マルチプラットフォーム対応ガイド」を参照してください。

② インターネットとの接続

端末（PC）にカードリーダを続するだけなのに不思議に思われるかもしれませんが、インターネットと接続できる環境が必要となります。これは HPKI の証明書の有効性を確認する際に、認証局から証明書の執行リスト（CRL）を取得する必要があるためです。もちろん動作させる PC がインターネットに接続されていなくとも、他の PC で認証局にアクセスして CRL を取得し、それを動作させる PC にコピーして利用することでも問題ありません。

ただし、IC カードを使って電子署名をするだけなら、IC チップ内の演算処理で電子署名をするだけなのでインターネットは必要ありません。今回のサンプルソフトウェアでは検証用のソフトウェアは CRL の確認までは含んでいませんので、動作確認を行うレベルであればインターネットとの接続がなくとも動作検証は可能です。

③ テスト用 HPKI カード

標準類に準拠して HPKI の証明書と私有鍵を格納した IC カードを自力で作成するのは困難です。3.1.5 と付録を参考にしてテスト用 HPKI カードを提供している認証局から入手してください。

3.1.2　端末

3.1.1 で説明した通り、自力で環境を整えるのであれば、特に HPKI を利用する端末の条件はありません。端末によっては接点付き IC カードあるいは非接触 IC カードに対応したカードリーダが搭載されたものがありますが、多くの場合にはカードリーダは搭載されていませんので、3.1.3 で説明するカードリーダが別途必要となります。カードリーダは USB での接続が一般的ですので、少なくとも USB のデバイスが接続できる USB ポートが必要となります。3.1.1 で述べたように、インターネットとの接続も必要となる場合がありますので、有線あるいは Wi-Fi 等でインターネットに接続するためのインタフェースも必要となります。

サンプルプログラムを動作させる場合の端末ですが、3.1.1 で説明した通り、Windows 10 の動作する PC を用意してください。標準的な PC は、ネットワークの接続と USB デバイスの接続が可能であると思われますので、ほとんどの場合にはサンプルプログラムを動作させるために新たな PC が必要とはならないはずです。

3.1.3　カードリーダ

一部の PC では、カードリーダが搭載されています。その場合には新たにカードリーダを準備する必要はありません。念のため、搭載されているカードリーダが PC/SC で動作することを確認してください。

カードリーダが搭載されていない PC の場合には、別途市販されているカードリーダを準備する必要があります。HPKI カードの場合、接点付き及び非接触の両方のインタフェースに対応しているので、どちらのカードリーダでも構いません。一般的には接点付きのカードリーダのほうが安価です。中には接点付きと非接触の両方のインタフェースを備えたカードリーダもあります。いずれにせよ、安心して利用できるカードリーダはマイナンバーカードで動作確認が検証されたカードリーダですので、関連するサイトの情報 https://www2.jpki.go.jp/prepare/pdf/num_rwlist11.pdf を参照して準備してください。

カードリーダを利用するためには、カードリーダのドライバーが必要となります。利用する OS 等の条件に対応したドライバーがあるかは、カードリーダの製造者の HP 等で確認し、入手してください。

多くのカードリーダは、Windows　10 の環境で動作するための PC/SC ドライバーがメーカーから提供されています。サンプルプログラムを利用する場合に必要ですので、HP からダウンロードする等によって入手してください。

なお、一部の非接触のカードリーダによっては、HPKI が対応している ISO/IEC 14443 の タイプ B で動作させるためのアドオンソフトウェアが必要となる場合がありますので、カードリーダ製造者の情報をご確認ください。

3.1.4　ネットワーク

3.1.2 で説明した通り、証明書の有効性を確認するには認証局への問い合わせが必要となり、そのための CRL を認証局から取得するためにはインターネットへの接続が必要となります。インターネットへの接続環境をご用意ください。

有効性確認を行わない場合、もしくは別の PC から取得してきて動作させる場合には必要ありません。

3.1.5　テスト用 HPKI カードの入手

現在 HPKI の認証局を運用しているのは、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となります。PC/SC を通じて IC カードにアクセス可能な HPKI 対応の HPKI ドライバー（PKCS＃11 及び CSP のライブラリー）も提供されています。開発用にテストカードを提供している認証局がありますので、各認証局へお問い合わせください。（付録 参照）

3.1.6　検証環境

HPKI の動作を確認する、あるいは利用するためには、別途ソフトウェアが必要となります。サンプルプログラムでは、電子署名を付与することができますので、詳細は 4 章を参照してください。電子署名の検証には、Open SSL を利用します。そのため、Open SSL の利用できる環境を用意してください。

3.1.7　環境のまとめ

これまで説明した HPKI を利用するために必要な環境をまとめると、以下の表のようになります。

表 3.1　ハードウェア環境

	一般	サンプルソフト
端末	PC 等 ・USB ポート ・ネットワークポート	PC（Windows 10） ・USB ポート ・（ネットワークポート）
カードリーダ	OS で動作確認されたもの	PC/SC に対応したもの
サンプル IC カード	認証事業者提供	認証事業者提供

表 3.2　ソフトウェア環境

	一般	サンプルソフト
検証用アプリケーション	自作またはベンダー提供	自作またはベンダー提供（Open SSL）
HPKI ドライバー	事業者提供/自作	認証事業者提供
カードリーダドライバー	PC/SC(Windows) PCSC-Lite(LINUX) Open SC(Windows, Mac OS X, LINUX 等) 等カードリーダで動作確認されたもの（注）	PC/SC（カードリーダ製造者提供）

注：詳細は、「JAHIS HPKI マルチプラットフォーム対応ガイド」を参照のこと

3.2　準備（環境を整える手順書）

3.1 では、必要な環境等について説明しましたが、ここでは設定方法などについて概略を説明します。

①端末（ＰＣ）の準備（その１）：カードリーダドライバーのインストール

PC にカードリーダが内蔵されている場合には、不要となります。ただし、ドライバーが最新のものであるかは確認し、アップデートしてください。

・カードリーダの接続

カードリーダの説明書に従って、PC に接続してください。

・ドライバーのインストール

カードリーダの説明書に従って、PC/SC に準拠したソフトウェアを入手してください。多くの場合はカードリーダ製造者の HP からダウンロード可能です。続いて説明書に従ってドライバーをインストールしてください。

②端末（ＰＣ）の準備（その２）：HPKI カードドライバーのインストール

認証局から配布される HPKI カードドライバーをインストールします。認証局からサンプルカードと共に配布されますので、説明書に従ってインストールしてください。

③追加のソフトウェアの準備

HPKI の動作を確認するためのソフトウェアが必要です。Open SSL には署名検証で利用できるコマンドがありますので、ここでは Open SSL について説明します。

・Open SSL の入手

Open SSL のソースは　https://www.openssl.org/ から入手可能です。ただし、実行可能なバイナリ形式の配布は行われていませんので、提供されるソースからご自分でバイナリを作成する必要があります。

・Open SSL の入手（バイナリ）

自身で Open SSL のバイナリを作成するのが難しい場合には、別途バイナリを提供している企業から必要なものを入手してください。入手に関する情報は https://wiki.openssl.org/index.php/Binaries にあります。インストールの方法は、各提供先の HP の情報に従ってください。尚、インストールの具体的な例は、 https://1-notes.com/windows10-openssl-install-and-uninstall/ 等にありますので、適宜参照してください。

Open SSL には脆弱性が発見されて修正されることがあります。常に最新の情報に注意して、必要なアップデートを実行してください。https://jvn.jp/vu/JVNVU94508446/

3.3　関連情報の取得

環境の設定は、条件等によってうまくいかない場合があるかもしれません。その場合には関連する HP を検索して対応することをお薦めします。

○テスト用 HPKI カードおよび HPKI カードドライバー

付録を参照し、各認証局にお問い合わせください。

○PC/SC ドライバー

カードリーダの製造者の HP を参照してください。

○OpenSSL

初期設定やインストールでトラブルが発生した場合には、

“OpenSSL”、“インストール” あるいは “OpenSSL”、“インストール”、“トラブル”

で関連する HP を検索してください。その他トラブルが発生した場合には、

“OpenSSL”、 “トラブル”

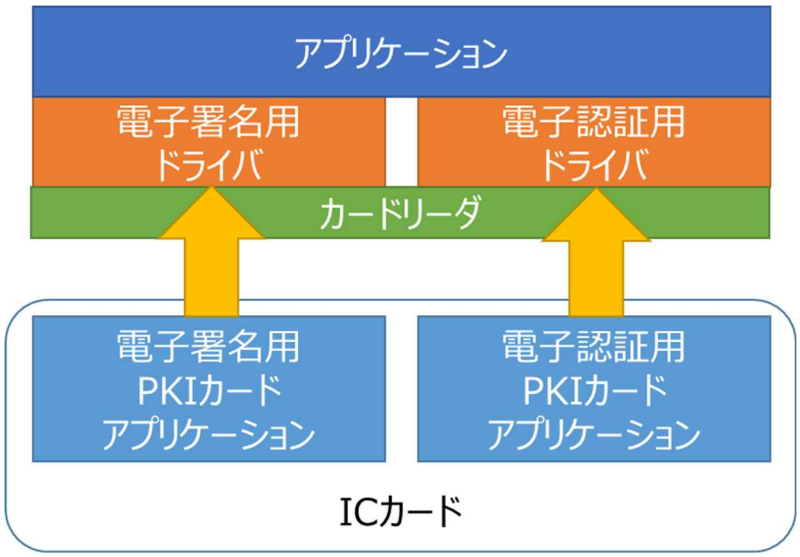
で関連する HP を検索してください。

4　サンプルプログラムによる HPKI 利用の解説

4.1　HPKI 利用の構造

実際に HPKI を利用するためには、IC カードへアクセスを行い、格納されている HPKI の証明書を利用して、署名や認証の処理を行うことになります。

１つの認証事業者が電子署名用及び電子認証用の両方の証明書を発行する場合、1 枚の IC カードに２つのアプリケーションを搭載することが可能となり、その場合の基本的な構造は下図となります。



本書のサンプルプログラムでも、HPKI カードには電子署名用アプリケーションと電子認証用アプリケーションが含まれています。今回利用する HPKI カードドライバにも、電子署名用と電子認証用を使い分ける別々のドライバが含まれているため、使い分けが必要となります。

今回は、電子署名のサンプルとなっています。

4.2　サンプルプログラムの概要

本書に示されているサンプルプログラムは、Pkcs#11 のインタフェースの一部を用いた C 言語によるサンプルです。JAHIS HPKI 対応 IC カードガイドライン Ver.3.0 に従い、作成しています。合わせて参照してください。

実際のサンプルプログラムのソースは付録に示しています。なお、Crypto API によって実現したサンプルプログラムのソースについても、分冊に示していますので、参考にしてください。

本サンプルプログラムは 、pkcs11.h ならびに OpenSSL を利用しています。開発環境によりますが、パス設定など[1]で利用可能な環境にしておいてください。

---

[1] 開発環境の設定で、include、lib ディレクトリの指定や、libcrypto.lib を追加指定する、

サンプルプログラムの利用方法は、コマンドプロンプトにて下記のコマンドを実行することで利用できます。

HPKISignVerifySampleP11 <PKCS#11 Library_Type> <PIN>

・パラメータの説明
＜PKCS#11 Library_Type＞： 署名用の場合” sign”、認証用の場合” auth”
＜PIN＞：HPKI カードの PIN

Pkcs#11 インタフェースを利用する際は以下の DLL を使い分けます。

- 電子署名用 DLL：HpkiSigP11_MPKCS11H.dll
- 電子認証用 DLL：HpkiAuthP11_MPKCS11H.dll

＜PKCS#11 Library_Type＞を署名用にして実行した結果の例は、下記のようになります。値はあくまでも例となります。

————————＜実行結果例　ここから＞————————
証明書取得処理 開始
Certificate:
30 82 05 13 30 82 03 fb a0 03 02 01 02 02 02 31
25 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00
30 81 83 31 0b 30 09 06 03 55 04 06 13 02 4a 50
31 22 30 20 06 03 55 04 0a 0c 19 4a 61 70 61 6e
20 4d 65 64 69 63 61 6c 20 41 73 73 6f 63 69 61
74 69 6f 6e 31 23 30 21 06 03 55 04 0b 0c 1a 44
69 67 69 74 61 6c 20 43 65 72 74 69 66 69 63 61
74 65 20 43 65 6e 74 65 72 31 2b 30 29 06 03 55
04 03 0c 22 48 50 4b 49 2d 30 31 2d 48 50 4b 49
5f 4a 56 32 2d 66 6f 72 4e 6f 6e 52 65 70 75 64
69 61 74 69 6f 6e 30 1e 17 0d 31 37 30 36 31 35
31 35 30 30 30 30 5a 17 0d 32 32 30 36 31 35 31
34 35 39 35 39 5a 30 3a 31 0b 30 09 06 03 55 04
06 13 02 4a 50 31 16 30 14 06 03 55 04 03 0c 0d
4a 4d 41 43 6f 6d 62 69 32 30 33 39 35 31 13 30

Windows 環境変数 Path に OpenSSL のインストール先の bin を追加する等の方法で、環境を整える必要があります。

11 06 03 55 04 05 13 0a 54 45 53 54 43 32 30 33
...
証明書取得処理 成功: HPKI END ENTITY CERTIFICATE

署名処理 開始
SHA256 HASH:
af a2 7b 44 d4 3b 02 a9 fe a4 1d 13 ce dc 2e 40
16 cf cf 87 c5 db f9 90 e5 93 66 9a a8 ce 28 6d

Signature:
59 91 c0 13 1f c3 eb bb 07 11 87 dc 18 9c 3d 2b
a4 d1 9f 98 5a 91 38 f1 57 a3 1a 16 47 eb e8 a9
7c 13 fc 57 a9 a7 b0 f5 71 c3 63 89 3b c9 e5 df
84 7e 9b 23 f3 5d 7b f0 a8 02 5d 13 2a 28 69 e1
6f 5f ee ee ad bf c4 59 da 0c 84 82 1c de b1 af
86 14 fa 50 9f cf 20 42 55 38 00 6a 17 15 34 97
45 c1 1e 75 9a 8d 75 c3 09 15 88 dc 58 51 fe 68
21 01 7d d1 e2 88 06 d9 3a cb d5 1f 74 e2 ae 3e
22 41 5b 44 54 50 7d f8 09 64 07 ed 30 1e be df
c5 70 57 06 00 f2 63 78 64 60 9a d4 95 2d 1e 91
56 81 c0 a8 27 08 50 25 3e 21 14 28 d5 45 6a 8c
22 ee 3f e9 d2 65 a4 39 fd 99 c2 2a 2c ca b8 66
1a 1b 8d 36 d3 33 5c 16 4c 62 51 f1 f6 ed 36 ba
ed 32 5d f4 c5 31 81 8c 8a 85 15 c7 59 d8 f3 cf
55 5d 3e 6c ac 12 b6 a6 49 32 b7 37 17 5d 90 6c
7e b3 ec d3 bc 3f 20 ac 11 58 e9 d6 f6 4c 84 4b
...
署名処理 成功

検証処理 開始
検証処理 成功
――――――＜実行結果例　ここまで＞――――――

今回のサンプルプログラムによって実現している検証は、署名値（改ざん有無）の確認のみを行っており、署名者（証明書）の確認までは実施していません。

サンプルプログラムの処理に関する大きな流れは図 4.1 のようになっています。

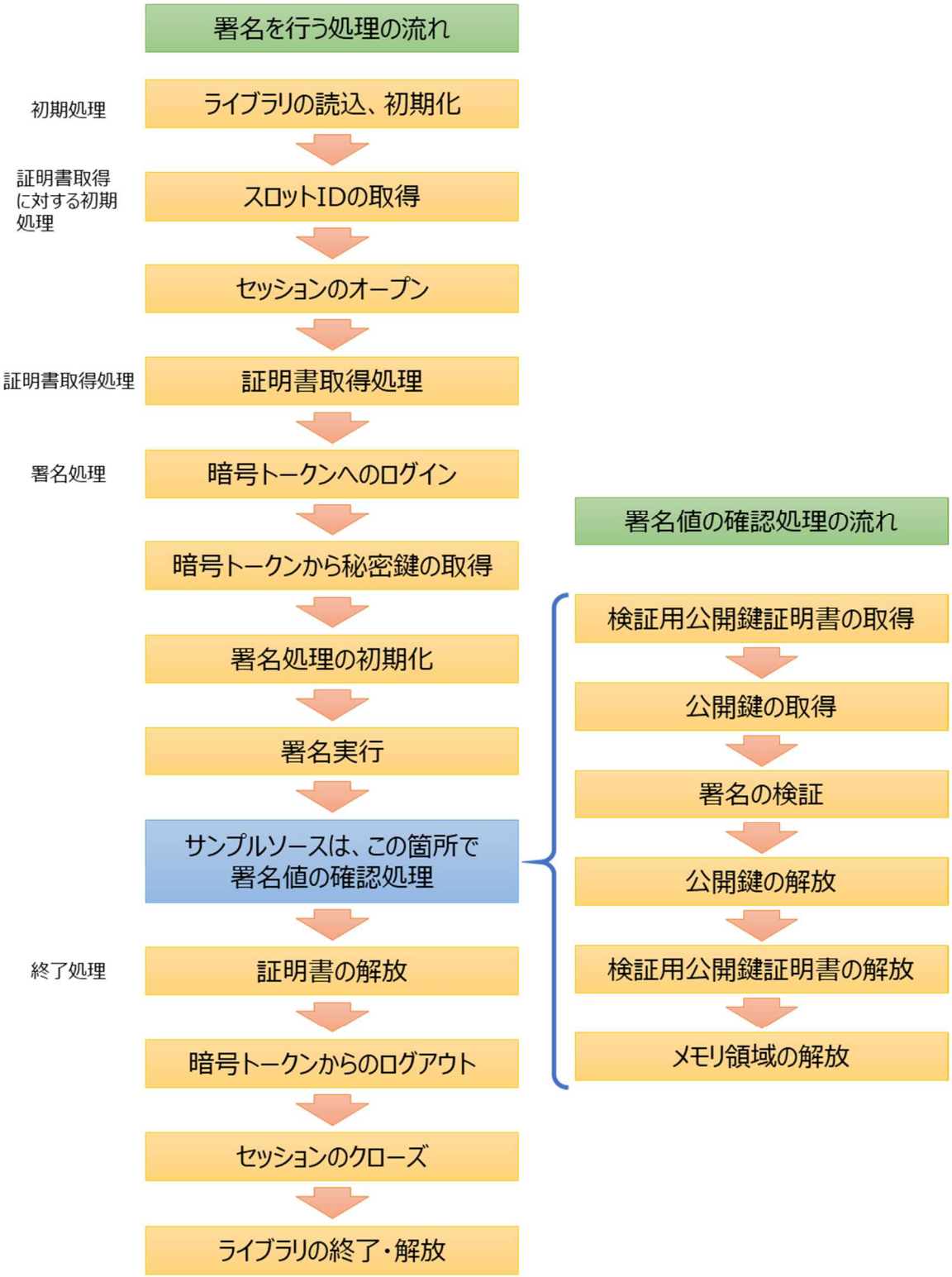


図 4.1　サンプルプログラムの動作の流れ

4.3　PKCS#11 の相互運用性のための機能

HPKI では、PKCS #11 での相互運用性のために、下表の機能の一覧が実装されることになっています。これらの機能を利用することで、HPKI カードにアクセスし、証明書を使った処理を行うことができます。

（JAHIS HPKI 対応 IC カードガイドライン Ver.3.0　5.2.2. PKCS #11 インタフェース 表 2 PKCS #11 の関数一覧より引用）

PKCS #11 の関数一覧 No	API名	概要
1	C_GetFunctionList	関数ポインタリストを取得する。
2	C_Initialize	PKCS #11ライブラリを初期化する。
3	C_Finalize	PKCS #11ライブラリを終了する。
4	C_GetInfo	ライブラリ情報を取得する。
5	C_GetSlotList	スロットリストを取得する。
6	C_GetSlotInfo	スロット情報を取得する。
7	C_GetTokenInfo	トークン情報を取得する。
8	C_GetMechanismList	サポートメカニズム（アルゴリズム）を取得する。
9	C_GetMechanismInfo	メカニズム（アルゴリズム)情報を返す。
10	C_OpenSession	セッションを確立する。
11	C_CloseSession	セッションを切断する。
12	C_CloseAllSessions	すべてのセッションを切断する。
13	C_GetSessionInfo	セッション状態を取得する。
14	C_Login	トークンをログイン状態にする。
15	C_Logout	トークンをログアウト状態にする。
16	C_FindObjectsInit	オブジェクトの検索を開始する。
17	C_FindObjects	オブジェクトの検索を行う。
18	C_FindObjectsFinal	オブジェクトの検索を終了する。
19	C_GetAttributeValue	オブジェクトの属性値を取得する。
20	C_SignInit	署名処理を初期化する。
21	C_Sign	データに署名を行う。

それぞれの関数の詳細については、HPKI 対応 IC カードガイドライン Ver. 3 0 の「5.2.2. PKCS #11 インタフェース」を参照してください。

4.4　サンプルプログラムでの処理の流れ

サンプルプログラムでの処理の流れと、処理を行うために利用する PKCS #11 の関数、及び OpenSSL の関数について示します。

No.	処理概要	処理内容	PKCS #11/OpenSSL の利用
1	初期処理	ライブラリの選択、ロード	
2		動作させるための DLL 内の関数(アドレス)を取得	
3		関数ポインタリストの取得（使うメモリの指定)	C_GetFunctionList
4		PKCS #11 ライブラリを初期化する。	C_Initialize
5	証明書取得に対する初期処理	スロットリストを取得する（メモリ割り当て)	C_GetSlotList
6		スロットを取得する	C_GetSlotList
7		先頭のスロットに対するセッションを確立する	C_OpenSession
8	証明書取得処理	オブジェクトの検索の初期化	C_FindObjectsInit
9		オブジェクトの検索を行い、先頭の証明書を指定する	C_FindObjects
10		オブジェクトの属性値を取得して、証明書のサイズを取得	C_GetAttributeValue
11		メモリの確保を行い、証明書を取得する	C_GetAttributeValue
12		オブジェクトの検索を終了する	C_FindObjectsFinal
13	署名処理	先頭のスロットのトークン情報を取得する	C_GetTokenInfo
14		暗号トークンにログイン（PIN を利用)	C_Login
15		暗号トークン中の署名用生成用秘密鍵の検索条件を設定	
16		オブジェクトの検索の初期化	C_FindObjectsInit
17		オブジェクトの検索を行い、先頭の秘密鍵を取得する	C_FindObjects
18		オブジェクトの検索を終了する	C_FindObjectsFinal
19		署名を行うデータの生成	

20		署名対象メッセージのハッシュ値生成	(OpenSSL)SHA256
21		ハッシュ値の DigestInfo 生成	(OpenSSL)i2d_X509_SIG
22		署名メカニズムの設定	
23		署名処理の初期化	C_SignInit
24		データに署名を行う	C_Sign
25	署名値（改ざん有無）の確認	メモリ確保	(OpenSSL) BIO_new_mem_buf
26		公開鍵証明書の復号	(OpenSSL) d2i_X509_bio
27		公開鍵の取得	(OpenSSL)X509_get_pubkey (OpenSSL)EVP_PKEY_get1_RSA
28		署名検証	(OpenSSL)RSA_verify
29		公開鍵の解放	(OpenSSL)RSA_free (OpenSSL)EVP_PKEY_free
30		公開鍵証明書の解放	(OpenSSL)X509_free
31		メモリ領域の解放	(OpenSSL)BIO_free
32	終了処理	証明書の解放	
33		暗号トークンからのログアウト	C_Logout
34		セッションをクローズする	C_CloseSession
35		ライブラリの終了	C_Finalize
36		ライブラリの解放	

今回のサンプルプログラムでは、サンプルプログラムとして内容が固定されている箇所がありますので、ポイントの解説を行います。こちらの解説について、必ずしも覚えなければならないということではありません。ただし、実行環境の変化や、サンプルプログラムを参考として、自分のやりたいことに変更していく際の助けになると思います。

- No.7 で、スロット[2]に対するセッションの確立を行うことについては、先頭の 1 つに限定してあります。これは、接続されているカードリーダが 1 つであることを想定しているためです。
- No.9 で、オブジェクトの検索を行い、先頭の証明書を指定しているのは、HPKI カード内の証明書が 1 つとの前提を置いています。

[2] スロットは暗号装置を装着する物理的な場所を抽象化したものです。ここでは PC/SC (Personal Computer/Smart Card)でアクセスするカードリーダと考えておけばよいです。

- No.13 で、先頭のスロットのトークン情報を取得することも No.9 と同様の理由です。
- No.17 で、オブジェクトの検索を行い、先頭の秘密鍵を取得することも No.9 と同様の理由です。
- No.19 の署名対象メッセージについては、固定となっています。

```
pMessage = "hello-world";
```

- No.20 の署名対象メッセージに対するハッシュ値の生成に関するアルゴリズムについても、SHA256 で固定してあります。

```
SHA256(pMessage, messageLen, hash);
```

- No.21 の署名アルゴリズムについても SHA256 で固定してあります。

```
sig.algor->algorithm = OBJ_nid2obj(NID_sha256);
```

仮にエラー[3]が起こった場合は、Web 等で検索すれば情報が得られるが、地方公共団体情報システム機構(J-LIS)が、公的個人認証サービスの利用者クライアントソフトに係る技術仕様を公開しており、その中の「公的個人認証サービス 利用者クライアントソフト API 仕様書 【カード AP ライブラリ PKCS#11 編】」[4]に詳しく記載があるので、参考にするとよいです。主なエラーの例を下記に示します。

pkcs11.h に定義されているエラーコード	値	主なエラーの内容
CKR_FUNCTION_FAILED	0x06	失敗
CKR_TOKEN_NOT_PRESENT	0xe0	カードが挿入されていないまたはカードが抜かれた
CKR_TOKEN_NOT_RECOGNIZED	0xe1	不正な IC カードを検出した
CKR_DEVICE_REMOVED	0x32	カードが挿入されていないまたはカードが抜かれた
CKR_PIN_INCORRECT	0xa0	パスワード指定誤り
CKR_PIN_LOCKED	0xa4	パスワードがロックされている

[3] エラーコードは、pkcs11.h に定義されていて、CKR_XXXXXXX(XXXXXXX はエラーの内容を識別できる文字列)として記載されています。

[4] https://www.j-lis.go.jp/data/open/cnt/3/2187/1/03_siyou_CardAPI_2_PKCS.pdf

4.5　関連情報の取得

環境に関しては、お使いの OS もキーワードとして加えると、情報に行き当たりやすいです。

・C 言語　環境設定
・環境変数　パス
・C 言語　ソースコード　コンパイル
・ライブラリ　コンパイル時　指定
・C 言語　アロー演算子

5　適用例

本章では HPKI 署名を適用可能なユースケースについて解説を行います。5.1 節では積極的に HPKI を適用すべき文書について、5.2 節では他の PKI を利用することも可能であるが HPKI が適用可能な文書について述べています。

5.1　国家資格の確認が必要な文書

医療専門職としての国家資格を保有していることは、国の HPKI 専門家会議が承認した正当な手続きにより HPKI 認証局によって確認されています。そのため、HPKI を用いた場合は改ざん検知や否認防止という PKI の基本機能に加え、本人性、実在性、国家資格が同時に確認できます。そのため、例えば診断書のような特定の国家資格を保有していないと作成できない文書について、受領者が国家資格の保有の有無を確認することができます。もし、HPKI ではない PKI で電子署名が行われていた場合、署名者が必要な国家資格を保有しているかどうかを確認するには、別の運用的な手段などが必要となるため、文書の受領者にとって大きな手間となることが考えられます。よって HPKI 署名を積極的に採用することが業務を円滑に進めるうえで重要です。以下に具体的な文書について説明します。

5.1.1　診療情報提供書（紹介状）

診療情報提供書とは一般的には紹介状と呼ばれるもので、他の医療機関等に対して患者を紹介する際に作成されるものです。平成 28 年度の診療報酬改定の際に「検査・画像情報提供加算及び電子的診療情報評価料の算定要件」が規定され、電子的に送受する際の要件が明確化されました。施設基準等において「診療情報提供書を電子的に提供する場合は、HPKI による電子署名を施すこと。」とされ、HPKI による電子署名が求められています。書式の例が以下のサイトより入手できますので、参考にしてください。

https://www.mhlw.go.jp/file/06-Seisakujouhou-10800000-Iseikyoku/0000056840.pdf

5.1.2　診断書

診断書は症状についての所見や診断内容、治療内容などを証明するものです。特に形式は法的には定められていませんが、死亡診断書のみは記載すべき事項が医師法施行規則 20 条ならびに歯科医師法施行規則 19 条の二で定められています。死亡診断書においては医師・歯科医師の記名押印もしくは署名が法律にて定められており、電子化する際には電子署名が必須となります。

書式の例が以下のサイトより入手できますので、参考にしてください。

https://www.mhlw.go.jp/toukei/manual/dl/examination_h30.pdf

それ以外の診断書においても、例えば労災保険給付や民間保険会社の保険請求の診断書などでは、受領側の指定するフォーマットにより、作成者の記名押印もしくは署名を求められる事例が殆どであり、電子化する際には HPKI を用いた電子署名を用いることが推奨さ

れます。

5.1.3　処方箋

処方箋は治療上必要と判断した医療用医薬品の種類や用法、用量、服用する日数が記載された文書です。厚生労働省により「電子処方箋の運用ガイドライン」が定められており、それに従った形式で発行する必要があります。ガイドラインでは PKI を用いた電子署名が必須とされており、同時に国家資格の確認が可能な HPKI の利用が推奨されています。

書式の例が以下のサイトより入手できますので、参考にしてください。

https://elaws.e-gov.go.jp/data/332M50000100015_20201001_502M60000100024/pict/2FH00000032227.pdf

上記は紙の処方箋の書式例ですので、電子化の際にフォーマットが変わる可能性があります。実際に電子処方箋を作成する際には厚生労働省の「電子処方箋の運用ガイドライン」等の関連法規等を遵守した形式にて作成してください。

5.1.4　放射線照射録

放射線照射録は人体に放射線を照射した際に作成が義務付けられた文書です。診療放射線技師法により、「診療放射線技師は、放射線を人体に対して照射したときは、遅滞なく厚生労働省令で定める事項を記載した照射録を作成し、その照射について指示をした医師又は歯科医師の署名を受けなければならない。」とされており、電子化する際には電子署名が必須となります。署名者が医師もしくは歯科医師であることが確認できなければならないので、HPKI による電子署名が推奨されています。

5.1.5　その他

その他の文書では、例えば治験における治験責任医師が作成する文書や、要介護判定に用いられる自治体に提出する主治医意見書など様々な文書において特定の国家資格を持たないと作成できない文書があります。これらの文書においては HPKI を用いることが強く推奨されます。

5.2　HPKI 署名が利用可能なその他ケース

HPKI 署名は国家資格以外に本人性、実在性を担保するので e 文書法で求められている電子署名として取り扱うことが可能です。国家資格確認が必ずしも必要でない文書に対しても改ざん検知と否認防止のために HPKI 署名を利用することができます。以下に具体的な文書について説明します。

5.2.1 保存が義務付けられた文書の電子保存

例えばカルテや調剤録のような医療機関等において保存が義務付けられた文書を電子化する際には、真正性・見読性・保存性の要件を満たす必要があり、特に真正性を技術的に担保する手段として PKI を用いることが可能です。詳しくは厚生労働省の「医療情報システムにおける安全管理に関するガイドライン」に記載されていますので、そちらを参照してください。https://www.mhlw.go.jp/stf/shingi/0000516275.html

5.2.2 他の組織との電子契約

電子契約とは、従来紙の契約書にて行っていた契約を電子文書にて行うものです。契約当事者の合意を確認するための書類ですので、確実な否認防止を行うことが重要となります。例えばオンライン決済などのような簡易な同意方法で電子契約を行う場合は電子署名を用いずに別の本人確認手段にて本人確認を行うことも可能ですが、後に「そんな約束はしていない」、「契約したのは別人で無効である」などのクレームが発生することがあり、このような事態を防止するために、より強力な否認防止手段として電子署名が有効になります。HPKI では医療機関の責任者であることを示す hcRole を持つ証明書を発行することが可能ですので、当該組織の契約責任を持つ人の署名であることも確認できます。

5.2.3 HPKI 証明書の申請手続き

既に HPKI 証明書を保有している場合、HPKI 証明書の更新処理などの際に本人確認手段として HPKI 電子署名を用いることが可能です。これにより各種証明書類を準備することなく、簡易に手続きを行うことが可能となります。

5.2.4 その他

HPKI を用いれば、e 文書法において電子化が可能となった各種文書に対して否認防止を確実にするために電子署名法に基づく電子署名が可能です。様々なユースケースがありますので、「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」 https://elaws.e-gov.go.jp/document?lawid=417M60000100044 の別表を参照ください。他の省の所轄分野については、各省の省令を参照ください。https://www.c-a-c.jp/about/guideline.html

6　おわりに

最後まで読み進めていただき、ありがとうございます。

いかがでしたか？HPKI について、本書を手にした時よりも興味を持ってもらえましたか？理解を深めてもらえましたか？

今回、なかなか進まない HPKI の普及を促進するために、医療情報システム開発センター（MEDIS）が事務局となり、日本医師会、日本歯科医師会、日本薬剤師会及び JAHIS をメンバーに含めた HPKI 実装検討会を立ち上げました。

現在、HPKI 認証局は、日本医師会、日本薬剤師会、MEDIS の 3 団体が運営しており、日本歯科医師会も認証局立ち上げの検討をしているところです。HPKI 認証局は手順に従ってそれぞれの HPKI カードを発行します。日本医師会は医師資格証を、日本薬剤師会は薬剤師資格証を、MEDIS は 27 の国家資格と 5 つの管理者資格の HPKI カードを発行する業務を行っています。

しかし、認証局を運営していると、HPKI カード発行業務以外に様々な問い合わせが入ります。その問い合わせを分析すると、特に、HPKI 対応アプリケーションの不足が HPKI 普及の足かせになっている感が否めません。

そこで、本検討会で HPKI 対応のアプリケーションを開発してもらうため、なるべく分かりやすい解説をした実装手引書を世に出すことにしました。タイトルは「はじめての HPKI」と少々砕けたタイトルですが、これまで HPKI に興味がなかったり、難しいものと思っていた方々の手に取ってもらえるようにとの思いを込めたタイトルです。

本実装手引書を読むことで、PKI の基礎知識や認証局の役割、HPKI の歴史及び必要性はもちろんのこと、HPKI を使用するための環境も分かったかと思います。また、添付されたサンプルプログラムを使って実際のプログラムを組むことができ、HPKI 署名がどのように使われているかも理解できます。参考文献には、関連の CP やガイドラインを載せました。読み解くには難しい文書もありますが、HPKI に関わる文書・規定類を網羅していますので、是非、参考にしてみてください。

ICT 活用時代において、マイナンバーカードが国民の身分を証明するだけでなく、今後、健康保険証や運転免許証のような資格を証明するのと同様、HPKI カードが医療従事者の身分を証明すると同時に、その医療関連資格を証明することになり、それがこれからの時代に必ず必要となることをご理解いただけると幸いです。

本実装手引書が、皆様のお役に立ち、HPKI の普及が一層進むことを心から願います。

執筆者一同

HPKI 認証局

＊公益社団法人日本医師会電子認証センター
https://www.jmaca.med.or.jp/
＊公益社団法人　日本薬剤師会認証局
https://www.nichiyaku.or.jp/hpki/index.html
＊一般財団法人医療情報システム開発センター
http://www.medis.or.jp/8_hpki/

＝＝

参考文献

◇証明書ポリシ
厚生労働省　HPKI 認証局証明書ポリシ（CP）
＊保健医療福祉分野 PKI 認証局署名用証明書ポリシ 1.6 版 令和 2 年 12 月
https://www.mhlw.go.jp/content/000712102.pdf
＊保健医療福祉分野 PKI 認証局認証用（人）証明書ポリシ 1.5 版 令和 2 年 12 月
https://www.mhlw.go.jp/content/000712103.pdf
＊保健医療福祉分野 PKI 認証局 認証用（組織）証明書ポリシ 1.1 版 平成 22 年 3 月
https://www.mhlw.go.jp/content/000466966.pdf

◇運用関連
厚生労働省 HPKI ルート認証局運用管理規程（CP/CPS）
＊厚生労働省 HPKI ルート認証局運用管理規程 Version 1.2 令和 2 年 10 月
https://www.mhlw.go.jp/content/10808000/000682267.pdf
公益社団法人日本医師会
＊日本医師会認証局運用規程(CPS) version 4.2 令和 3 年 1 月
https://www.jmaca.med.or.jp/guide/data/CPS.pdf
公益社団法人　日本薬剤師会
＊日本薬剤師会認証局運用規程(CPS) version 1.03 平成 30 年 1 月
https://www.nichiyaku.or.jp/hpki/pdf/cps_v1.03.pdf
一般財団法人医療情報システム開発センター
＊MEDIS ヘルスケア電子証明書発行サービス実施規程 Version 1.6 2020 年 7 月
https://www.medis.or.jp/8_hpki/pdf/jissikitei.pdf

国際標準

＊ISO 17090-1: Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services

＊ISO 17090-2: Health informatics — Public key infrastructure — Part 2: Certificate profile

＊ISO 17090-3: Health informatics — Public key infrastructure — Part 3: Policy management of certification authority

◇IC カード関係

JAHIS 標準

＊JAHIS 標準 18-001「JAHIS HPKI 対応 IC カードガイドライン Ver.3.0」2018 年 5 月
https://www.jahis.jp/files/user/04_JAHIS%20standard/18-001_JAHIS%20HPKI%E5%AF%BE%E5%BF%9CIC%E3%82%AB%E3%83%BC%E3%83%89%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3Ver.3.0.pdf

国際標準

＊ISO/IEC 7816-4: Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange

＊ISO/IEC 7816-8: Identification cards -- Integrated circuit cards -- Part 8: Commands and mechanisms for security operations

＊ISO/IEC 7816-15: Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application

◇署名

JAHIS 標準

＊JAHIS 標準 18-006「JAHIS ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.2.0」2019 年 2 月
https://www.jahis.jp/files/user/04_JAHIS%20standard/18-006_JAHIS%E3%83%98%E3%83%AB%E3%82%B9%E3%82%B1%E3%82%A2PKI%E3%82%92%E5%88%A9%E7%94%A8%E3%81%97%E3%81%9F%E5%8C%BB%E7%99%82%E6%96%87%E6%9B%B8%E3%81%AB%E5%AF%BE%E3%81%99%E3%82%8B%E9%9B%BB%E5%AD%90%E7%BD%B2%E5%90%8D%E4%BC%81%E7%94%BBVer.2.0.pdf

＊セキュリティ委員会報告書「JAHIS HPKI マルチプラットフォーム対応ガイド」

2020 年 3 月
https://www.jahis.jp/files/user/03_bukai%20joho/%E3%80%8CJAHIS_HPKI%E3%83%9E%E3%83%AB%E3%83%81%E3%83%97%E3%83%A9%E3%83%83%E3%83%88%E3%83%95%E3%82%A9%E3%83%BC%E3%83%A0%E5%AF%BE%E5%BF%9C%E3%82%AC%E3%82%A4%E3%83%89%E3%80%8D_HPKI%E9%9B%BB%E5%AD%90%E7%BD%B2%E5%90%8D%E8%A6%8F%E6%A0%BC%E4%BD%9C%E6%88%90WG_20200319a.pdf

国際標準

＊ISO 17090-4: Health informatics — Public key infrastructure — Part 4: Digital signatures for healthcare documents

＊IETF/RFC3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

＊IETF/RFC3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

◇認証

JAHIS 標準

＊JAHIS 標準 14-005「JAHIS HPKI 電子認証 ガイドライン V1.1」2014 年 09 月
https://www.jahis.jp/files/user/images/JAHIS_HPKI_V1.1.pdf

国際標準

＊ISO 17090-5: Health informatics — Public key infrastructure — Part 5: Authentication using Healthcare PKI credentials

＝＝

引用文献

＊医師法施行規則
https://elaws.e-gov.go.jp/document?lawid=323M40000100047

＊歯科医師法施行規則
https://elaws.e-gov.go.jp/document?lawid=323M40000100048

＊厚生労働省「電子処方箋の運用ガイドライン」
https://www.mhlw.go.jp/content/11121000/000626327.pdf

＊診療放射線技師法

https://elaws.e-gov.go.jp/document?law_unique_id=326AC1000000226_20150801_000000000000000

＊厚生労働省「医療情報システムにおける安全管理に関するガイドライン」

https://www.mhlw.go.jp/stf/shingi/0000516275.html

＊e 文書法

・民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律

https://elaws.e-gov.go.jp/document?lawid=416AC0000000149

・民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律

https://www.kantei.go.jp/jp/singi/it2/hourei/16-150gou/honbun.html

＊電子署名及び認証業務に関する法律

https://elaws.e-gov.go.jp/document?lawid=412AC0000000102

＊厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令

https://elaws.e-gov.go.jp/document?lawid=417M60000100044

＊公的個人認証サービス 利用者クライアントソフト API 仕様書 【カード AP ライブラリ PKCS#11 編】

https://www.j-lis.go.jp/data/open/cnt/3/2187/1/03_siyou_CardAPI_2_PKCS.pdf

HPKI実装検討会　委員名簿

有馬　一閣
JAHIS医療システム部会　セキュリティ委員会　HPKI電子署名規格作成WGリーダー

河野　行満
公益社団法人　日本薬剤師会　医薬情報管理部　部長

玉川　裕夫
公益社団法人　日本歯科医師会　医療管理・情報管理　嘱託

茗原　秀幸
JAHIS医療システム部会　セキュリティ委員会　委員長

谷内田　益義
JAHIS医療システム部会　セキュリティ委員会　セキュアトークンWGリーダー

矢野　一博
公益社団法人　日本医師会　電子認証センター　システム開発研究部門長

問い合わせ先
一般財団法人医療情報システム開発センター
医療情報利活用推進部門
メール：hpki-ad@medis.or.jp

発行

〒162-0825
東京都新宿区神楽坂一丁目 1 番地
電話　03-3267-1922
一般財団法人医療情報システム開発センター
医療情報利活用推進部門