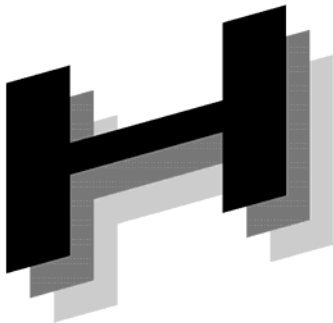


A large, bold, black letter 'J' with a 3D shadow effect, positioned at the top left of the page.

Japanese

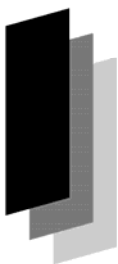
A large, bold, black letter 'A' with a 3D shadow effect, positioned below the letter 'J'.

Association of

A large, bold, black letter 'H' with a 3D shadow effect, positioned below the letter 'A'.

Healthcare

JAHIS HPKI 電子認証ガイドライン V1.0

A large, bold, black letter 'I' with a 3D shadow effect, positioned below the letter 'H'.

Information

2010年03月

保健医療福祉情報システム工業会

セキュリティ委員会

A large, bold, black letter 'S' with a 3D shadow effect, positioned at the bottom left of the page.

Systems Industry

JAHIS HPKI 電子認証ガイドライン V1.0

まえがき

本規格は保健医療福祉分野におけるヘルスケア PKI (HPKI) による認証を行うに際して、相互運用性を確保するために策定されたものである。

保健医療福祉分野においては、平成 17 年 3 月に厚生労働省により「医療情報システムの安全管理に関するガイドライン」(以下、「安全管理のガイドライン」と言う)が策定され、継続的に改定が行われている。本「安全管理のガイドライン」6.11 章において、相手先の識別と認証において PKI を利用出来る旨が C 項に記載されている。また、同年 4 月には、同省にて「保健医療福祉分野 PKI 認証局 証明書ポリシー」【1】が策定され、国際標準に準拠した保健医療福祉分野向けの PKI (HPKI) 証明書の発行ルールが確定した。さらに平成 21 年度には厚生労働省の医療情報ネットワーク基盤検討会において「保健医療福祉分野 PKI 認証局 認証用 (人) 証明書ポリシー」の策定が行われた。これにより、署名用に続き、認証用についても HPKI 証明書の発行が行えることとなった。

JAHIS は、産業界の業界団体として、これら国の施策に協力するとともに、普及促進を図るための相互運用性の確保を図ることが重要な役割であることから、今般、「JAHIS HPKI 電子認証ガイドライン V1.0」を策定することとし、ここに JAHIS 標準として公開するものである。

本ガイドラインは、JAHIS 会員各社の意見を集約し、「JAHIS 標準」の一つとして発行したものである。したがって、会員各社がシステムの開発・更新に当たって、本規格に基づいた開発・改良を行い、本規格に準拠していることをその製品のカタログ・仕様書等に示し、さらにその製品の使用においてユーザが理解すべき内容を説明する場合などに使われることを期待している。

また本規格は上記ガイドラインで示された PKI を利用した認証に関連する要求事項を、実装レベルで解説した規格であり、HPKI 認証機能を利用するシステムを導入しようとしている施設が参照し利用することは歓迎するところである。ただし、当該システムが法、政令、省令、通知、ガイドラインなどに合致しているか否かの判断は、自己責任の下で自ら判断する必要があることに留意されたい。

なお、本規格で扱う HPKI 認証要件は、参照規格や技術動向にあわせて変化する可能性がある。JAHIS としても継続的に本規格のメンテナンスを重ねてゆく所存であるが、本規格の利用者はこのことにも留意されたい。

2010 年 03 月

保健医療福祉情報システム工業会
セキュリティ委員会

<< 告知事項 >>

本ガイドラインは関連団体の所属の有無に関わらず、ガイドラインの引用を明示することで自由に使用することができるものとします。ただし一部の改変を伴う場合は個々の責任において行い本ガイドラインの準拠する旨を表現することは厳禁するものとします。

本ガイドラインならびに本ガイドラインに基づいたシステムの導入・運用についてあらゆる障害や損害について、本ガイドライン作成者は何らの責任を負わないものとします。ただし、関連団体所属の正規の資格者は本ガイドラインについての疑義を作成者に申し入れることができ、作成者はこれに誠意をもって協議するものとします。

Copyright © 2010 保健医療福祉情報システム工業会

目次

第1章	適用範囲	1
1.1	目的.....	1
1.2	策定方針	1
第2章	引用規格・引用文献.....	2
第3章	用語の定義.....	3
第4章	記号および略語.....	6
第5章	対象となるユースケース	7
5.1	医療情報ネットワーク基盤検討会で検討されたユースケース	7
5.2	院内で運用される医療情報システムでの利用者認証に用いるケース.....	8
5.3	使ってはいけないケース	9
第6章	PKI 認証の概要	10
6.1	PKI 認証方式の概要.....	10
6.2	対象となる機能範囲.....	11
6.3	HPKI アプリケーションの位置付け.....	13
6.4	PKI 認証とSAML	16
第7章	PKI 認証機能の実装要件	17
7.1	一般的なアクセスコントロールのフロー	17
7.2	一般的なPKIによる認証のフロー.....	17
7.3	クライアントの実装要件	18
7.4	サーバの実装要件	19
第8章	HPKI におけるユーザの識別.....	21
8.1	HPKI 認証用証明書の証明書プロファイル	21
8.2	hcRole 属性の利用	21
8.3	証明書失効リストのプロファイル	22
8.4	アプリケーションにおけるユーザ識別の方式	24
8.5	HPKI アプリケーションにおけるユーザ識別の方法.....	25
第9章	署名用HPKIと認証用HPKIの使い分け	26
9.1	使い分けの必要性	26
9.2	使い分けの方法.....	27
9.3	複数のEE証明書が存在する場合の対応方法	28
附属書 A	HPKI 認証用証明書プロファイル（基本領域）	30
A-1	HPKI 認証用証明書プロファイル（基本領域）	30
A-2	HPKI 認証用証明書プロファイル（拡張領域）	31
付録1	：参考文献.....	33
付録2	：作成者名簿.....	34

第 1 章 適用範囲

1.1 目的

医療情報システムの利用において、主として相手先の識別と認証を目的とした HPKI による認証を確実にを行うために、認証手続きについてのガイドラインを制定し、電子認証ソフトウェアなどの互換性を確保する。

1.2 策定方針

電子認証の互換性の確保、及びなりすまし防止のために、認証に求められる署名の生成、検証及び証明書検証において最低限行わねばならないことについて明確に定める。

また検証では医療分野特有の検証要件として、HPKI のポリシーへの準拠性を確認することが必要であることを明確に定める。これにより証明書内に記載された国家資格等の識別を活用することができる。

ユースケースを想定し、ユースケースに応じた利用方法を提示する。

認証のフレームワークについての規定は行わないが、一般的な利用方法として想定される、SSL クライアント認証ならびに独自のクライアント機能による認証を例にした実装要件を提示する。

第2章 引用規格・引用文献

個人が自らの医療情報を管理・活用する基盤を構築する際に必要となる医療従事者の認証方式について

<http://www.mhlw.go.jp/shingi/2009/02/dl/s0213-8e.pdf>

保健医療福祉分野 PKI 認証局認証用（人）証明書ポリシー（平成21年11月）

<http://www.mhlw.go.jp/shingi/2009/11/s1106-6.html>

HPKI 対応 IC カードガイドライン

<http://www.jahis.jp/standard/seitei/st08-002/st08-002.htm>

第3章 用語の定義

アプリケーション

特定の目的を果たすための機能を提供するソフトウェア。

インターフェース

プログラムや装置、操作者といった対象の間で情報のやりとりを仲介するもの。また、その規格。

改ざん

情報を管理者の許可を得ずに書き換える行為。

加入者

加入者とは、証明書所有者である。証明書所有者とは、証明書発行申請を行い認証局により証明書を発行される個人、機器、施設等をさす。証明書所有者の範囲は次のとおりとする。

- ・ 保健医療福祉分野サービスの提供者及び利用者
- ・ 上記の提供者の内、以下の者がその有する資格において、あるいは管理者として認証を行う場合は、「その資格を有していること」あるいは「管理者であること」を証明書に記載しなくてはならない。
- ・ 保健医療福祉分野に関わる国家資格を有する者
- ・ 医療機関等の管理者

(「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省))

公開鍵証明書

加入者の名義と公開鍵を結合して公開鍵の真正性を証明する証明書で、印鑑証明書に相当する。電子証明書あるいは単に証明書ともいう。公開鍵証明書には、公開鍵の加入者情報、公開鍵、CA の情報、その他証明書の利用規則等が記載され、CA の署名が付される。

(「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省))

失効

有効期限前に、何らかの理由(盗難・紛失など)により電子証明書を無効にすること。基本的には、本人からの申告によるが、緊急時には CA の判断で失効されることもある。

(「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省))

失効情報

公開鍵証明書の有効性を確認できるよう、認証局から開示される情報。無効になった証明書のシリアル番号等をリストアップした失効リスト(CRL: Certification Revocation List)や、オンラインでの証明書有効性の確認要求に対し応答を返す OCSP レスポンダ(OCSP: Online Certificate Status Protocol)があるが、CRL を

採用している認証局が一般的。また、認証局は通常、証明書の有効期限を越えて失効情報を開示していない。

私有鍵

公開鍵と対になる鍵。公開せず、他人に漏れないように鍵の所有者だけが管理する。私有鍵で署名したものは、それに対応する公開鍵でのみ検証が可能である。
(「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省))

証明書ポリシー(CP: Certificate Policy)

共通のセキュリティ要件を満たし、特定のコミュニティ及び／又はアプリケーションのクラスへの適用性を指定する、名前付けされた規定の集合。
(「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省))

署名検証

電子署名が正当なものか確認する行為。以下のように証明書検証と署名値の検証から構成される。(証明書検証：証明書の正当性、有効性の検証)

- ① 署名に用いた証明書が正当な認証局から発行されたものであること
- ② 検証時に証明書の有効期間が切れていないこと
- ③ 失効していない有効な証明書で有ること
(署名値の検証：署名対象データが改ざんされていないかどうかの検証)
- ④ 署名対象文書のハッシュ値と署名データから得られるハッシュ値が等しいこと

デバイス

コンピュータに搭載あるいは接続されるハードウェア。

電子署名

電子文書の正当性を保証するために付けられる署名情報。公開鍵暗号などを利用し、相手が本人であることを確認するとともに、情報が送信途中で改ざんされていないことを証明することができる。公開鍵暗号方式を用いて生成した署名はデジタル署名ともいう。

(「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省))

電子認証

電子的に「特定の名前のもとで何かを申請したり、何かにアクセスしようとしたりする個人もしくは組織体が、実際に正当な個人もしくは組織体であること」を確立する過程のこと。

登録局(RA: Registration Authority)

登録局は、適切な申請者の本人確認、登録の業務を行い、発行局への証明書発行要求を行う。なお、証明書登録の業務は、発行、失効を含む。

但し、登録局は認証局の運営主体で定める CPS の遵守及び個人情報の厳正な取り扱いを条件に、契約を取り交わすことで業務の一部を外部に委託することができる。

(「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省))

認証局(CA: Certification Authority)

電子証明書を発行する機関。認証局は、公開鍵が間違いなく本人のものであると証明可能にする第三者機関で、公正、中立な立場にあり信頼できなければならない。

(「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省))

認証パス(Certification Path)

トラストアンカ(信頼点)となる CA から検証対象である証明書までを結ぶ一連の証明書の繋がり。

ライブラリ

ある機能を提供するプログラム部品群。単体では動作せずソフトウェアの一部として組み込まれることで機能する。

PKCS#11

米 RSA Security 社が定めた公開鍵暗号技術をベースとした規格群である PKCS (PublicKey Cryptography Standards)の内、暗号トークンに関するインターフェース標準。

AID

IC カード内のアプリケーション識別子

第4章 記号および略語

このガイドラインでは、次の記号および略語／表記を用いる。

PKI	Public Key Infrastructure	公開鍵基盤。公開鍵暗号化方式という暗号技術を基に認証局が公開鍵証明書を発行し、この証明書を用いて署名／署名検証、暗号／復号、認証を可能にする仕組み。 (「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー (厚生労働省)」)
HPKI	HealthCare PKI	保健医療福祉分野での公開鍵基盤。
CSP	Cryptographic Service Provider	Microsoft 社による暗号化のためのソフトウェアコンポーネント。
ISO	International Organization for Standardization	電気分野を除く工業分野の国際的な標準規格を策定するための団体。
OID	Object Identifier	オブジェクト識別子。オブジェクトの識別を行うため、オブジェクトに関連付けられた一意な値。 (「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー (厚生労働省)」)
SSL	Secure Socket Layer	HTTP や FTP などの上位のプロトコルで送受信されるデータを暗号化して送受信するプロトコル
CA	Certificate Authority	認証局 (認証機関)。証明書を発行し管理する機関。
EE	End Entity	CA 以外の証明書が発行される主体。
CRL	Certification Revocation List	認証局が発行する証明書失効リスト。
SSO	Single Sign-On	一度の認証によって複数のサービス等が利用可能になる認証機能
RADIUS	Remote Authentication Dial-In User Service	認証と接続記録をネットワーク上のサーバにて一元化する IP 上のプロトコル。

第5章 対象となるユースケース

認証用 HPKI を利用することで以下のメリットがある。

- ① 医療分野での利用を目的とした証明書ポリシーが一元的に定められ、相互運用性が確保されている。
- ② 証明書内に記載される hcRole により国家資格等の属性認証が行える。
- ③ 医療分野で広く利用できる基盤が整いつつある。

本章では、上記に挙げたメリットが有効なユースケースを検討する。

5.1 医療情報ネットワーク基盤検討会で検討されたユースケース

厚生労働省の医療情報ネットワーク基盤検討会では作業班を設けて、個人自らの健康情報の管理・活用の視点から想定されるユースケースを洗い出し、医療の現場を見据えた議論が行われてきている。そこで提出された成果報告書¹に下記のような3つのユースケースが示されている。

- ① かかりつけの医師が、患者の医療・健康情報を患者の同意のもと参照する場合
- ② かかりつけの医師ではないが、医療機関を受診した患者の医療・健康情報を患者の同意のもと、もしくは緊急に参照する場合
- ③ 医療専門職が旅先などでたまたま居合わせた急病人に対しケアをする際に、患者の同意のもと、もしくは緊急に患者の医療・健康情報を参照する場合

これらのユースケースでは、いずれも患者の医療・健康情報にアクセスし、参照しなければならないが、医療情報を含む健康情報は機微な個人情報であるため、許可された者のみが参照する仕組みが必要である。また、緊急時、特に本人の意識が清明でない場合においては救命活動を優先して行う必要があるため、本人同意を経由しない何らかの緊急時の情報参照の仕組みが必要となる。このような本人同意なしに情報を参照する場合、少なくとも医療の専門家（国家資格保有者）であることが担保されていなくてはならない。更に、医療分野においては、特定の医療専門職のみにしか許されていない医療行為がある。このことから、どの医療専門職であるかどうかを判別することは非常に重要である。また、ユースケースによっては、医療専門職ごとにアクセスできる権限が異なることが想定されるため、ユースケースごとのアクセス条件に応じたアクセス権の付与を行う仕組みが必要になる。このように医療専門職の資格という属性を判断し、アクセスを許可する仕組み（属性認証）を実現する方策のひとつとして HPKI 認証が有効である。

¹ 「個人が自らの医療情報を管理・活用する基盤を構築する際に必要となる医療従事者の認証方式について」（<http://www.mhlw.go.jp/shingi/2009/02/dl/s0213-8e.pdf>）

5.2 院内で運用される医療情報システムでの利用者認証に用いるケース

認証用 HPKI が構築された場合には、5.1 で想定したユースケース以外にも、地域連携や院内の病院情報システムなどにおける認証に活用が検討されることも想定される。例えば、地域連携システムにおけるアクセス制御に利用することや、医療機関の病院情報システムのアクセスに利用するなどが考えられる。

その場合、地域や院内で配布する認証用のカード等を、認証用 HPKI 認証局 から配布されるカードで代用でき、情報システム構築コストを低減できる可能性がある。

ただし、認証用 HPKI が提供するフレームワークのみでは、加入者の本人性、実在性、および医療専門職としての国家資格の有無しか担保できないため、実際の運用には不十分である。従って、認証用 HPKI 証明書は本人性、実在性、国家資格の有無の確認のみに限定し、地域連携や院内システムにおける国家資格以外の属性を含めた認証要件は、要件を明確にし、システム側で適切な管理・運営を実施しなくてはならない。また、認証用 HPKI のフレームワークを利用する際に生じるリスク（認証局が保証する保証範囲を超えた利用を行う場合の責任のあり方等）などについて分析を行い、必要な運用管理規定や認証ルールを追加構築する必要がある。

5.3 使ってはいけないケース

加入者本人が証明書の安全性を担保する必要があるため、共有機器に複数名の私有鍵をインストールするのは推奨しない。

共有機器を利用する場合には、加入者本人のみが所有し利用可能なトークンに私有鍵および証明書を格納すべきである。

第 6 章 PKI 認証の概要

6.1 PKI 認証方式の概要

PKI 認証とは、認証用の私有鍵と公開鍵証明書により電子認証を行う仕組みのことである。

私有鍵による署名を検証することにより本人性を確認し、公開鍵証明書の検証によって実在性を確認することで証明書所有者を認証することが出来る。なお、証明書所有者には人に限らず機器、組織となる場合があるが、本ガイドラインでは人が証明書所有者であることを前提に説明する。

PKI 認証を実装する場合の方法には様々な方式があるが、次に主な方式について概要を示す。

6.1.1 SSLクライアント認証

HTTPS で始まる URL にアクセスすることで SSL ハンドシェイクプロトコルにより、サーバからクライアントに対し証明書と署名データを求め、その証明書と署名データを検証して正当なクライアントからの接続要求であることを確認して接続を確立する WEB サイトの認証方式である。クライアントではサーバに送る証明書を選択する操作が必要になり、不特定多数が利用するクライアントでは選択が容易に行える工夫が必要となる。

認証の操作は HTTPS のセッション開始時およびセッションタイムアウト後の再接続の度に求められる。

6.1.2 ActiveX 等による独自のクライアント認証

WEB アプリケーションにおいて、業務アプリケーションの任意のタイミングで利用者認証を行う場合には、ブラウザに Microsoft 社の Internet Explorer を用いる場合を例にすると、独自のクライアント認証機能を ActiveX 技術で実装する方式がある。

独自のクライアント認証機能は IC カード等で私有鍵による署名データを生成し、これをサーバに送信する。サーバ側では送信された署名データを検証機能にて署名検証と証明書の検証を行い加入者を認証する。

6.1.3 クライアントローカルアプリケーションでの認証

クライアントアプリケーションが単独で IC カード等による利用者認証（加入者識別）を行う場合は、IC カード等に格納された私有鍵による署名を生成して、その署名検証及び証明書検証を行って加入者を認証する。

6.2 対象となる機能範囲

本ガイドラインの対象となる機能範囲は、業務アプリケーションに実装されるユーザのログイン認証機能において、ICカード等に格納された認証用 HPKI 秘密鍵と証明書を用いた PKI 認証を実行する HPKI アプリケーション機能である。

業務アプリケーションの形態にはWEBアプリケーション形式とクライアントアプリケーション形式に大別される

6.2.1 WEB アプリケーション形式の構成

(1) SSL クライアント認証

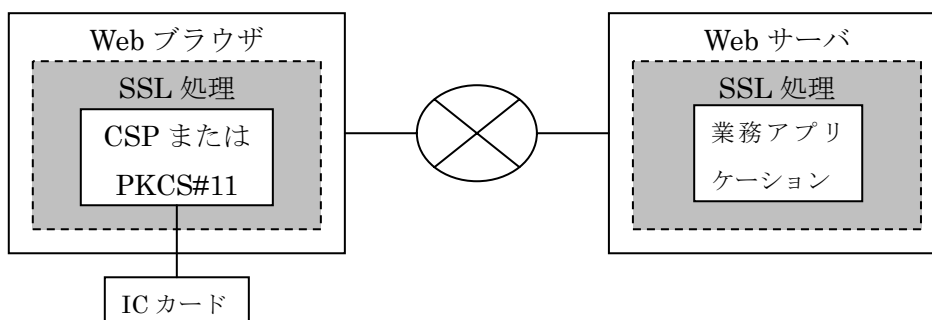


図 6.2.1 SSL クライアント認証

WEBアプリケーションにおける HPKI アプリケーション層にあたる署名と検証処理部分は SSL 処理に該当する。

(2) ActiveX による P K I 認証

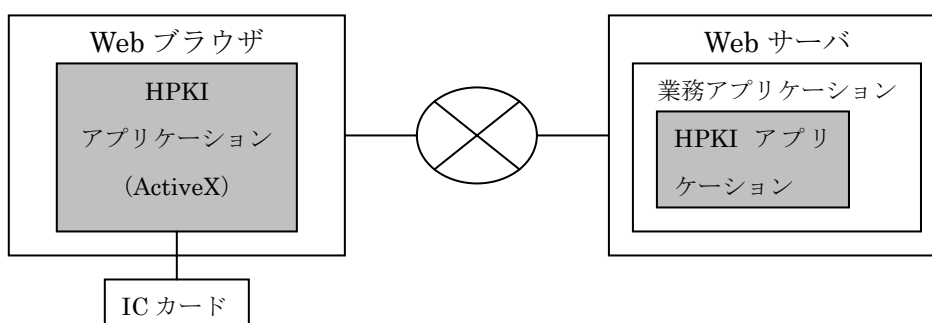


図 6.2.2 ActiveX による P K I 認証

クライアントの HPKI アプリケーション (ActiveX) にて署名を行い、サーバの HPKI アプリケーションにて署名の検証を行う。

6.2.2 クライアントアプリケーションの形式の構成

(1) アプリケーション内部に組み込むPKI認証

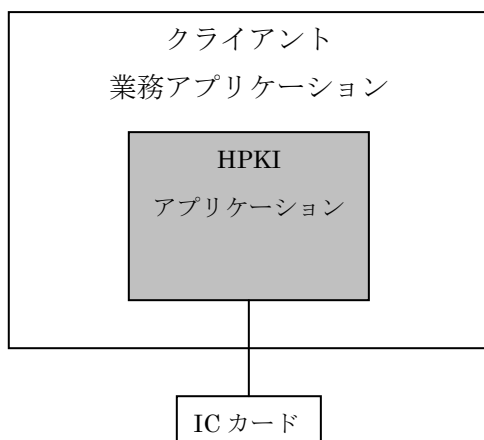


図 6.2.2 クライアントアプリケーション

クライアントの HPKI アプリケーションにて署名と署名の検証を行う。

6.3 HPKI アプリケーションの位置付け

6.3.1 WEBアプリケーション形式の位置付け

WEB アプリケーションの場合は、クライアントモジュールとサーバモジュールに HPKI アプリケーション層が存在する。

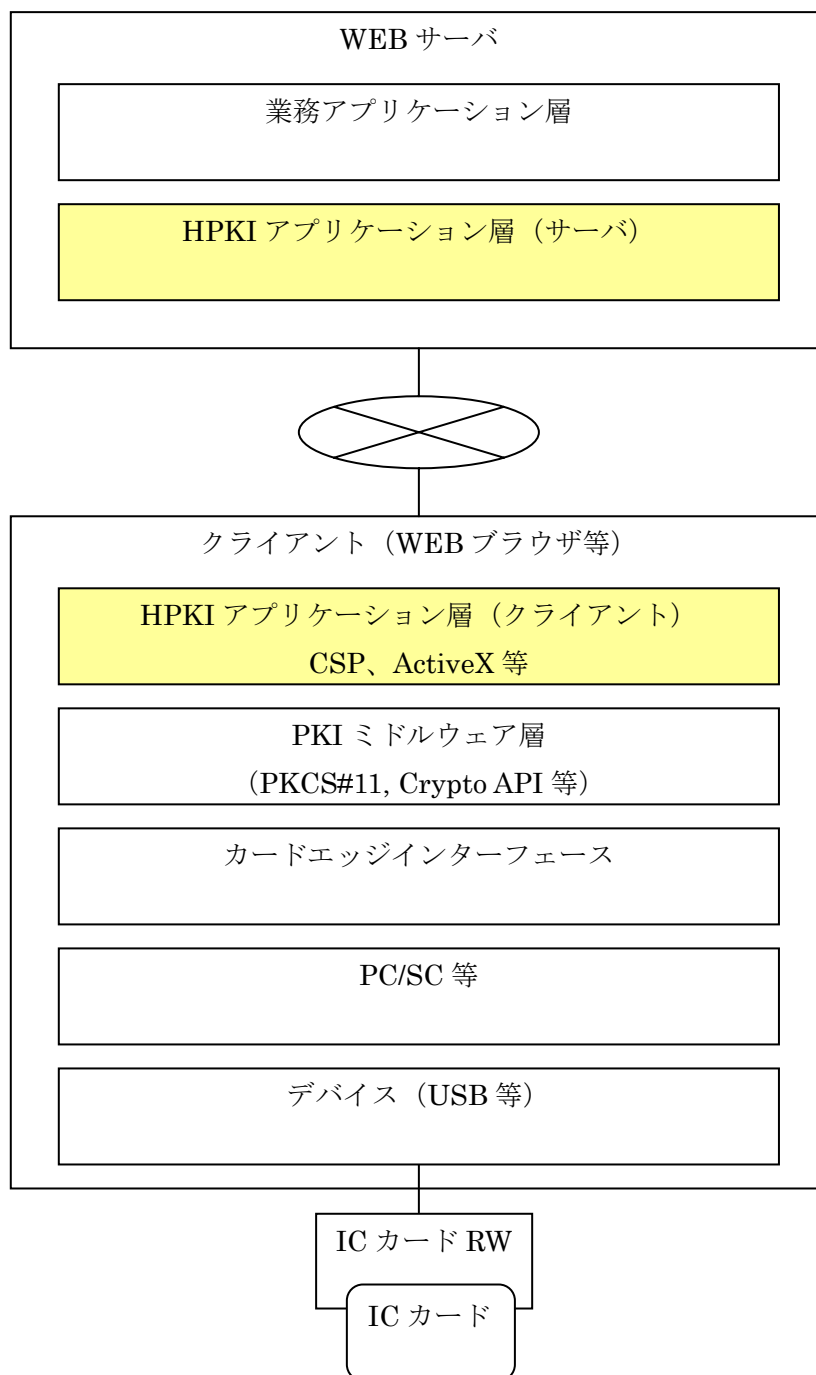


図 6.3.1 WEBアプリケーションの構成

(1) SSL クライアント認証

WEB ブラウザによる SSL クライアント認証の場合、クライアントでの HPKI アプリケーション層に該当する部分は、WEB ブラウザの SSL 処理機能と、IC カード等の秘密鍵を用いた署名処理のために用意される CSP モジュールである。

一方、サーバでは WEB サーバ機能にて SSL ハンドシェイクにてクライアントの証明書の検証が行われた後に HTTPS 通信が行われる。WEB サーバから取得する加入者の HPKI 証明書を解析して、加入者を識別し業務アプリケーション層にて権限等による認可処理を行う。HPKI アプリケーション層は WEB サーバ内の SSL 処理系部分と HPKI 証明書を解析部分が該当する。

(2) ActiveX 等の独自認証

SSL クライアント認証を用いず、独自処理で IC カード等を用いて認証を行う場合はクライアントでは ActiveX 等のクライアントモジュールを用意する。この ActiveX 等が HPKI アプリケーション層の位置付けとなる。

一方、サーバでは ActiveX 等のクライアントモジュールで署名されたデータを WEB サーバに送付しサーバ側で署名検証処理を行う部分が HPKI アプリケーション層となる。

6.3.2 クライアントアプリケーションの位置付け

クライアントアプリケーションでは、IC カード等を用いて認証を行う部分が HPKI アプリケーション層の位置付けとなる。

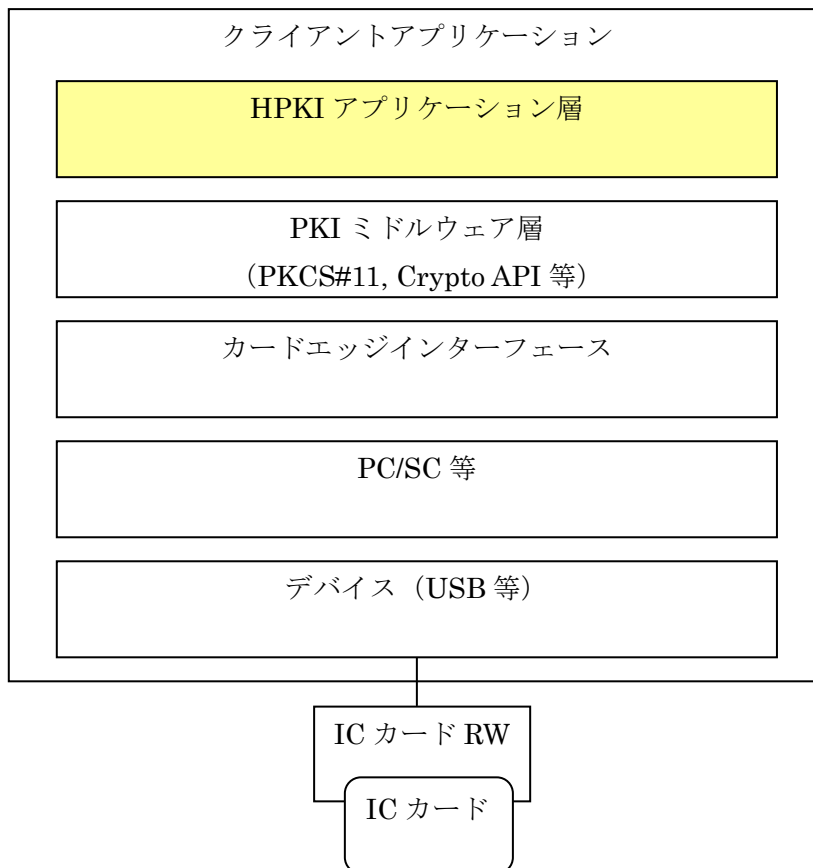


図 6.3.2 WEB クライアントアプリケーションの構成

6.4 PKI 認証と SAML

SAML (Security Assertion Markup Language) 等の認証連携のフレームワークを用いることで、アプリケーションから認証の機能を独立させることができる。SAML では認証オーソリティが加入者の認証を行い、その結果を含めた認証アサーションを発行する。アプリケーションは認証オーソリティから認証アサーションを取得することにより、加入者の本人性を確認することができる。認証オーソリティ以外に、加入者の属性情報を提供する属性オーソリティや、認可を行う認可決定オーソリティがある。この仕組みを利用することでシングルサインオンや、異なるドメイン間の ID 連携を実現することができる。

図 6.5.1 は SAML により認証を行う Web アプリケーションの一例である。

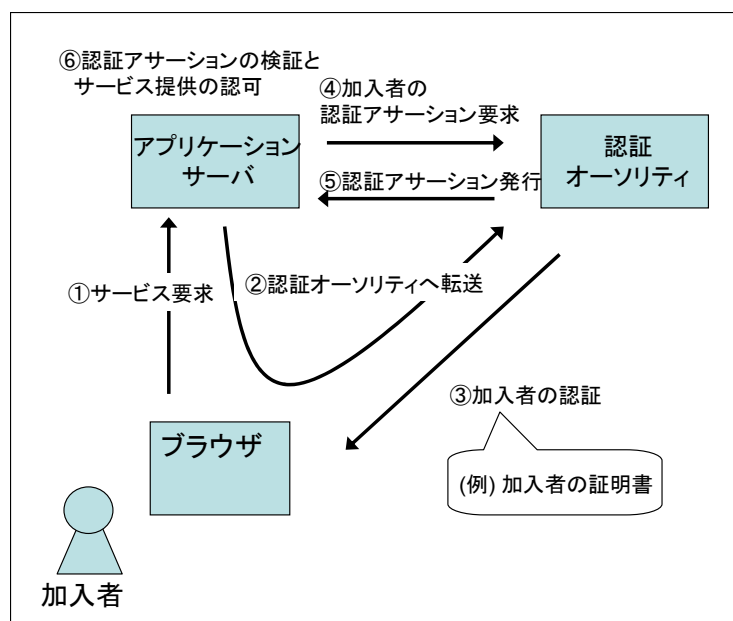


図 6.4.1 SAML による認証

SAML の仕組みは固有の認証方法には依存していないため、様々な認証方法を採用することができる。PKI による加入者の認証を行う場合には、認証オーソリティが加入者の証明書を検証する。

認証オーソリティは認証アサーションに署名をして発行するが、この署名に使用する証明書については本ガイドラインの対象外である。

認証連携のフレームワークを用いる場合には各オーソリティとそれを利用するアプリケーションやサービス提供者との間の信頼関係が必要である。適用する認証方法、情報提供の範囲や仕組み、運用方法などについての合意を形成することが求められる。

第 7 章 PKI 認証機能の実装要件

7.1 一般的なアクセスコントロールのフロー

アクセスコントロールの機能をもつ一般的なアプリケーションは加入者に対して以下の処理を行う。

(1) 加入者の識別

加入者が誰であるかを特定する。証明書に記載された本人識別情報を元に加入者の識別情報を特定する。

(2) 加入者の認証

加入者の身元が正しい者であることを確認する。PKI による認証の場合には加入者の署名と証明書を検証することで加入者の身元の正しさを確認する。一般的な PKI による認証のフローを 7.2 節で述べる。

(3) 加入者に対する認可

加入者にアプリケーションの操作や情報へのアクセスに対する認可を与える。加入者の ID（もしくは所属するグループ）に対して定義されたアクセスコントロールリストを元に認可を行う場合や、加入者の属性情報（例えば hcRole 属性など）に対応づけられた操作権限により認可を行う場合などがある。

加入者の識別や認可の実装方法はアプリケーションに依存している。

この章では PKI による認証機能に対して認証プロトコルに依存しない共通の実装要件を述べる。

第 8 章では HPKI における加入者の識別方法と適用例を述べる。

7.2 一般的な PKI による認証のフロー

ここでは PKI による加入者の認証方法の代表的な例として署名を用いた認証処理のフローを述べる。

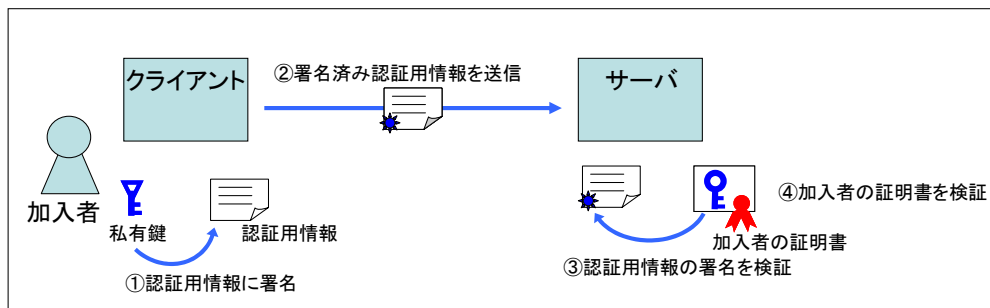


図 7.2.1 署名を用いた一般的な認証処理のフロー

認証処理は主に以下のような流れになる。

- ① クライアントが認証用情報に対して私有鍵で署名する。
 認証用情報とはサーバが加入者を認証するために使用する情報で認証プロトコルにより異なる。例えば、サーバクライアントの間で共有している情報から認証用情報が生成される場合や、サーバがクライアントに対して発行した乱数（チャレンジ）を用いる場合などがある。一般的に、このような認証用情報は加入者が直接知ることは無く、クライアントによって処理が行われる。クライアントは認証用情報への署名を行うために、加入者に対して認証用の私有鍵に対する PIN 入力を促す。
- ② クライアントは加入者の署名済み認証用情報をサーバへ送信する。このとき、加入者の証明書や検証に必要な中間認証局の証明書をサーバへ送信することもある。
- ③ サーバはクライアントから送られてきた署名済み認証情報の署名を検証する。サーバは、サーバが保持している（もしくは算出した）認証用情報と加入者の証明書から取得した公開鍵を用いて、加入者の署名を検証する。
- ④ サーバは加入者の証明書を検証し、加入者の身元の正しさを確認する。加入者の証明書から信頼の起点となる認証局の証明書（トラストアンカ）までのパスが有効であることを検証する。

認証用情報の処理に関しては認証プロトコルの規格に従い実装することが求められる。加入者の署名や証明書の扱いに関しては PKI による認証機能に共通のものとして次節以降の要件を満たす必要がある。

7.3 クライアントの実装要件

クライアントの実装における実装要件を以下に示す。

表 7.3.1 クライアントの実装要件

要求レベル	項目名	内容	説明
オプション	私有鍵選択時の鍵使用目的の確認	私有鍵を使用する前に、私有鍵に対応する証明書の鍵使用目的が認証用の鍵使用目的と適合することを確認する。	署名用の私有鍵を誤用しないように、安全のため、認証用途のものであることを確認したうえで使用することを強く推奨する。
オプション	私有鍵選択時の証明書の有効性確認	私有鍵を使用する前に、私有鍵に対応する証明書のパス検証を行い、トラストアンカまでのパス構築、有効期限や失効状態などを確認する。	サーバでの認証を受ける前に、クライアント側で有効な証明書であることを確認する。クライアント側での検証処理の負荷を考慮して、実装の有無を選択できる。

7.4 サーバの実装要件

サーバの実装における実装要件を以下に示す。

表 7.4.1 サーバの実装要件

要求レベル	項目	内容	説明
必須	トラストアンカの適切な設定と管理	<p>トラストアンカとして厚生労働省 HPKI ルート認証局が設定できること。</p> <p>トラストアンカの設定を安全に管理すること。</p>	<p>加入者の証明書を検証するには、トラストアンカの設定が必須である。トラストアンカの設定が不適切な場合には、意図しない不正な証明書を受け入れてしまう危険性があるため、トラストアンカに対する適切な設定と安全な管理が必要である。</p>
必須	加入者の公開鍵を用いた署名の検証	<p>加入者の公開鍵を用いて、クライアントから送られてきた加入者の署名を検証すること。</p>	<p>加入者の署名、加入者の証明書から取得した公開鍵、サーバが保持している（もしくは算出した）認証用情報を用いて、署名値が正しいことを確認する。</p> <p>公開鍵による署名の検証を行うことにより、署名がその公開鍵と対となる私有鍵によって生成されたことを確認することができる。</p>
必須	加入者の証明書の認証パスの有効性確認	<p>加入者の証明書からトラストアンカとなる厚生労働省 HPKI ルート認証局までの認証パスを検証できること。</p> <p>検証方法は RFC5280 のパス検証に従う。</p> <p>代表的な検証項目として以下のものがある。</p>	<p>トラストアンカまでの認証パス上にある証明書の有効性を検証することで、加入者の身元の正しさを確認する。</p>
		<p>加入者からトラストアンカまでのパス構築</p>	<p>証明書に記載されている発行者名と、その発行者となる認証局証明書の主体者名が一致するパスを構築する。トラストアンカとなる厚生労働省 HPKI ルート認証局まで到達するパスを構築する。</p>
		<p>証明書に付与された認証局の署名の検証</p>	<p>認証パス上の証明書に対して、証明書を発行している認証局の署名がついていることを確認する。証明書の署名</p>

			を認証局証明書の公開鍵で検証する。
		認証局証明書の CA フラグの確認	認証パス上の認証局証明書について、証明書の基本制約フィールドに CA フラグがあることを確認する。CA フラグがない場合には、認証局としての業務を認められない者 (例えばエンドユーザ) が証明書を発行していることになるため、認証局証明書として受け入れてはならない。
		証明書ポリシーの確認	認証パス上の証明書に対して、証明書ポリシーの OID が HPKI 認証用証明書ポリシーと適合することを確認する。
		証明書の鍵使用目的の確認	加入者の証明書の鍵使用目的が認証用の鍵使用目的と適合することを確認する。
		認証パス上の証明書の有効期限確認	認証パス上の証明書について、現在時刻において証明書の有効期限が切れていないことを確認する。
		認証パス上の証明書の失効確認	認証パス上の証明書について、現在時刻において証明書が失効されていないことを確認する。
		失効情報に付された署名の検証	失効情報に付された署名が、正しい認証局により付されたものであることを確認する。
オプション	hcRole 属性の取得	加入者の証明書から hcRole 属性を取得する。	hcRole によるアクセスコントロールを行う場合など、アプリケーションの要件に応じて実装する。

第 8 章 HPKI におけるユーザの識別

電子証明書による当該システムに対する本人認証が行われた後、そのアカウントに予め割り当てられた個々のシステムまたはアプリケーションに設定される権限に相応したアクセスコントロールによりユーザ識別が行われる。

8.1 HPKI 認証用証明書の証明書プロファイル

HPKI 認証用証明書は、X509 Version 3 フォーマット証明書形式で作成される。また、HPKI 認証用証明書は、X.500 識別名（Distinguished Name、以下 DN という）により一意に識別される。HPKI 認証用証明書のプロファイルについては、附属書を参照されたい。

8.2 hcRole 属性の利用

HPKI 認証用証明書には、ISO/TS 17090 で規定される hcRole 属性が記載される。この属性情報を定義する HPKI hcRole 属性プロファイルには、証明書中の subjectDirectoryAttributes に表 8.2.1 の HPKI 資格名テーブルの国家資格、また必要であれば医療機関の管理責任者としての資格情報が含まれる。これらの資格情報を当該システムに対する権限情報としてユーザ識別を行う。

表 8.2.1 HPKI 資格名テーブル

資格名（国家資格）	説明
'Medical Doctor'	医師
'Dentist'	歯科医師
'Pharmacist'	薬剤師
'Medical Technologist'	臨床検査技師
'Radiological Technologist'	診療放射線技師
'Registered Nurse'	看護師
'Public Health Nurse'	保健師
'Midwife'	助産師
'Physical Therapist'	理学療法士
'Occupational Therapist'	作業療法士
'Orthoptist'	視能訓練士
'Speech Therapist'	言語聴覚士
'Dental Technician'	歯科技工士
'National Registered 'Dietitian'	管理栄養士
'Certified Social Worker'	社会福祉士
'Certified Care Worker'	介護福祉士
'Emergency Medical Technician'	救急救命士

'Psychiatric Social Worker'	精神保健福祉士
'Clinical Engineer'	臨床工学技師
'Masseur'	あん摩マッサージ指圧師/はり師/きゅう師
'Dental Hygienist'	歯科衛生士
'Prosthetics & Orthetic'	義肢装具士
'Artificial Limb Fitter'	柔道整復師
'Clinical Laboratory Technician'	衛生検査技師
資格名 (医療機関の管理責任者)	説明
'Director of Hospital'	病院長
'Director of Clinic'	診療所院長
'Supervisor of Pharmacy'	管理薬剤師
'Proprietor of Pharmacy'	薬局開設者
'Director'	その他の保健医療福祉機関の管理責任者

注) 資格名のワード間の空白は一個の Space (x20)となる。

「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省) より

8.3 証明書失効リストのプロファイル

HPKI 認証用証明書を発行する認証局は、X.509CRL フォーマット形式のバージョン 2 に従う CRL (証明書失効リスト) を発行する。

表 8.3.1~3 の「◎」は必須、「○」は場合により必須、「△」はオプション、「×」は設定しないことを表している。

表 8.3.1 CRL プロファイル (基本領域)

フィールド	設定	説明
Version	◎	Ver2 とする。
Signature	◎	HPKI 認証用証明書の Signature と同様とする。
Issuer	◎	英数字のみ使用する。(CountryName は Printable、それ以外は UTF-8 で記述する)
CountryName	◎	c=JP(固定)とする。
LocalityName	△	
OrganizationName	◎	
OrganizationUnitName	△	
CommonName	◎	認証局のポリシーを示す文字列を記載する。
ThisUpdate	◎	CRL の更新日時を示す。
NextUpdate	◎	次回の CRL 更新日時を示す。

RevokedCertificates	◎	
UserCertificate	◎	失効した証明書の serialNumber を記載。
RevocationDate	◎	失効日時を記載する。
CrlEntryExtensions	◎	拡張領域 (crlEntryExtentions) 参照
CrlExtentions	◎	拡張領域 (crlExtentions) 参照

表 8.3.2 CRL プロファイル (CRL エントリ拡張領 crlEntryExtentions)

フィールド	設定	説明	Critical
ReasonCode	◎	証明書の失効理由を表す。	FALSE
HoldInstructionCode	×	ReasonCode で「保留」が指定された場合の処理方法を指定する。	FALSE
InvalidityDate	×	証明書が無効となったと推定される日時を示す。	FALSE
CertificateIssure	×	証明書の発行者を示す。特に間接 CRL の場合に使用する。	TRUE

表 8.3.3 CRL プロファイル (CRL 拡張領域 crlExtentions)

フィールド	設定	説明	Critical
AuthorityKeyIdentifier	◎	発行者が複数の鍵の中から CRL に署名する場合、それぞれを区別するために使用する。	FALSE
IssuerAltName	△	発行者の別名を示す。	FALSE
CRLNumber	◎	CRL の通し番号であり、新しい CRL が発行される度に 1 つ増加する。	FALSE
DeltaCRLIndicator	×	分割 CRL のベース CRL 番号を示す。	TRUE
IssuingDistributionPoint	○	分割 CRL を用いる場合は必須	TRUE
FreshesCRL	×	分割 CRL の位置を示す。	FALSE

8.4 アプリケーションにおけるユーザ識別の方式

HPKI 認証用証明書を利用したクライアント認証では、一般的な SSL クライアント認証に加え、電子証明書内の **hcRole** を利用したユーザ識別を行うことができる。SSL クライアント認証では、クライアントは電子証明書およびデジタル署名された証明書情報をそれぞれ対象の認証サーバに送信する仕組みになっているが、電子証明書の記載内容の組み合わせにより、より厳格なアクセスコントロールや権限管理などに活用できる。HPKI アプリケーションでは以下の方式のユーザ識別が考えられる。

① 公開鍵証明書を予め DB 等に登録する方式

加入者の電子証明書を、予め DB 等に登録しておき、認証時に提示された証明書との記載内容の同一性によりユーザ識別を行い、**hcRole** に紐づく権限を付与する方式。

② 公開鍵証明書の記載内容を予め DB 等に登録する方式

加入者の電子証明書の記載内容を、予め DB 等に登録しておき、認証時に提示された証明書との同一性によりユーザ識別を行い、**hcRole** に紐づく権限を付与する方式。

③ 公開鍵証明書の **hcRole** で判定する方式

認証時に提示された証明書の **hcRole** によりユーザ識別を行い、権限を付与する方式。**hcRole** の判定のみに依存するため、緊急時の医師による参照等に利用される。

上記の場合、電子証明書の記載内容と **hcRole** を組み合わせて厳格なクライアント認証を行うことが重要となる。HPKI 認証用証明書を一意で識別するためには、電子証明書の加入者名 (**subjectDN**) に含まれるシリアル番号 (**SN**) と、認証局の名称 (**issuerDN**) を判別する。加入者の氏名 (**commonName**) を確認することも可能であるが、対象となる認証サーバ等へ予め認可するすべてのシステム加入者の情報をセットしておかなければならないため、これらを最新の情報に保つための仕組みが必要となる。そのため、HPKI 認証用証明書を利用するシステムでは、加入者 DB と認証サーバが連携する **RADIUS** や **SSO** への拡張が期待される。

8.5 HPKI アプリケーションにおけるユーザ識別の方法

SSL 通信では、サーバ側と加入者間で図 8.5.1 のようなハンドシェイクプロトコルが行われる。加入者にとってほとんどの工程はブラウザや PKI アプリケーションによって自動的に進むが、サーバ側の PKI アプリケーションでは図中⑨の Certificate Verify で加入者の証明書と署名、また必要であれば CRL を検証する。

HPKI 認証用証明書を利用したクライアント認証では、一般的な PKI アプリケーションで行う DN 値の判別や CRL の確認とともに、証明書に記載されている hcRole の情報を利用して 8.4 で示す方式などでユーザ識別を行うことでアクセスコントロールを実現する。

加入者の氏名が記載される CN (CommonName) や、医療福祉機関名が記載される OU (OrganizationUnitName) を証明書ごとに判別するためには、LDAP 等のデータベースにこれらの加入者情報を参照するために予め登録されている必要がある。

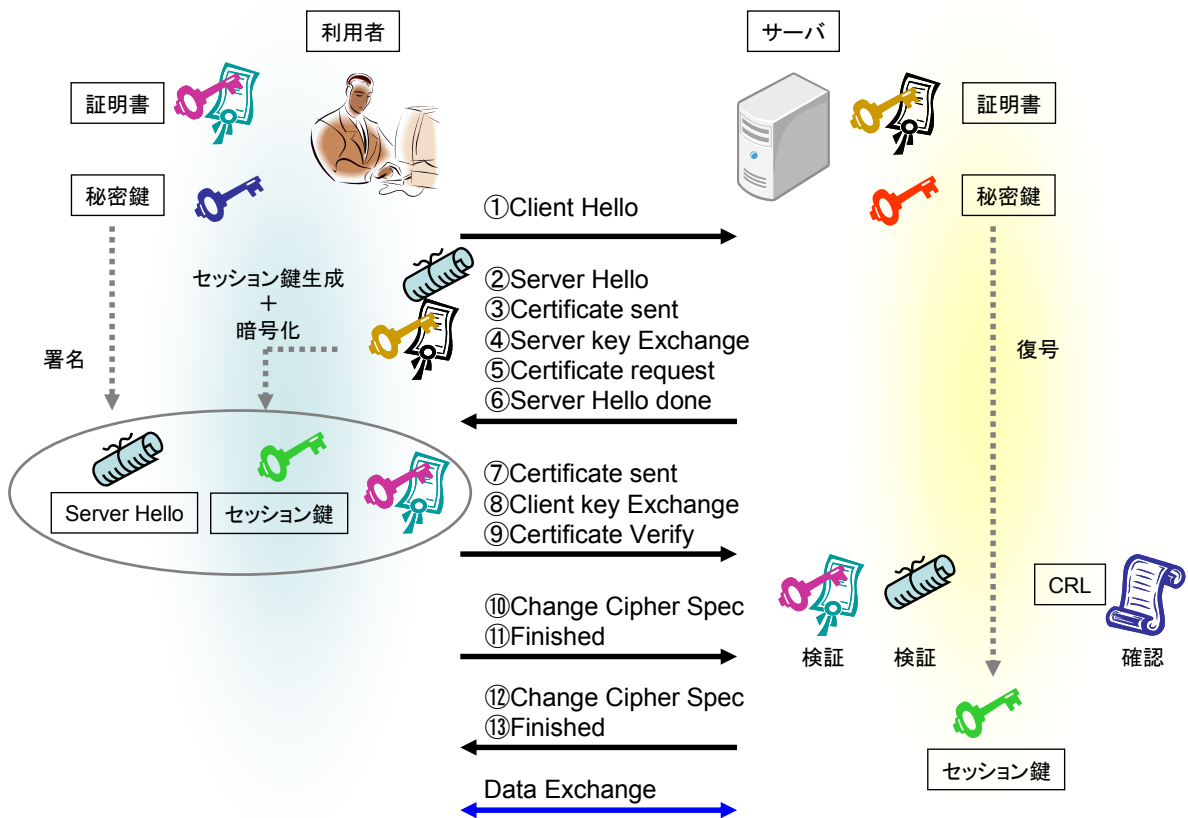


図 8.5.1 SSL クライアント認証におけるハンドシェイクプロトコル

第9章 署名用 HPKI と認証用 HPKI の使い分け

1枚の HPKI 用 IC カード内に署名用の鍵（私有鍵）と認証用の鍵（私有鍵）とが共存する可能性がある。本章では、署名用の鍵と認証用の鍵を区別して使い分けることの必要性和 HPKI における両者の使い分けの方法について述べる。

9.1 使い分けの必要性

PKI は、秘匿（親展）、認証（ログイン時等の本人認証）、署名（電子署名）に用いられる。これらのうち認証と署名は私有鍵による暗号化処理、つまり署名値の生成処理を基本とする²。

認証と署名では基本的な処理は同等（署名値の生成処理を基本とするという意味で）であるが、署名値の生成者（つまり私有鍵の保持者）にとって結果として生じる意味的な効果は大きく異なる。認証の場合、署名値の生成者に対する効果はサービスの利用が許可されるか拒絶されるかであるが、署名の場合は、署名値の生成者は署名した対象文書の内容に依存した責務を負うことになる場合がある。署名用の鍵を認証用を使用することに伴うリスクを次に説明する。

PKI による認証においては、チャレンジ&レスポンス方式が用いられる場合が多い。単純なチャレンジ&レスポンス方式では、認証主体が生成したチャレンジ（乱数）を対象に被認証者側のクライアントソフトが署名値を生成・送付し、それを認証主体が検証するといった手順が用いられる（図 9.1.1）。

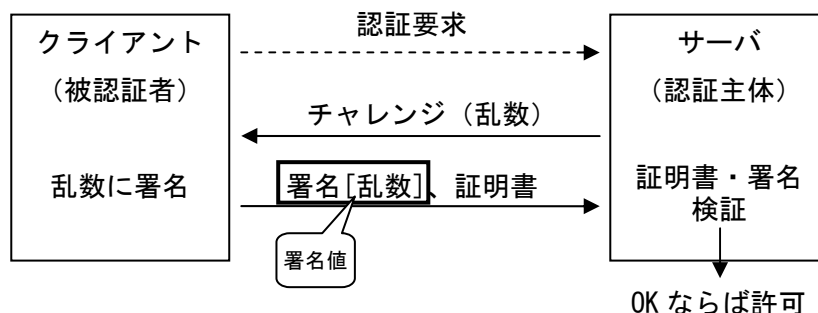


図 9.1.1 単純なチャレンジ&レスポンス方式による認証手順

このような方式では、認証主体側が有意な文書のハッシュ値をチャレンジとして送付したとしても被認証者側ではそのことを認識することは不可能であるため、被認証者側で

² SSH での公開鍵暗号によるユーザ認証方式のように親展（公開鍵による暗号化処理）に基づく認証方式もあるが、この方式は本章で述べるようなリスクを伴わないため、ここでは言及しないこととする。

は通常の処理に従ってそのハッシュ値に対して署名値を生成し送り返すことになる。このとき、認証主体側では元の文書と受け取った署名値とを組み合わせることによって容易に被認証者が署名したと見做せる文書を生成することができる。例えば借用書のハッシュ値をチャレンジとして用いた場合、被認証者は意図せず借用書に署名をしてしまい、その結果金銭を要求されるというリスクにさらされることになる（図 9.1.2）。

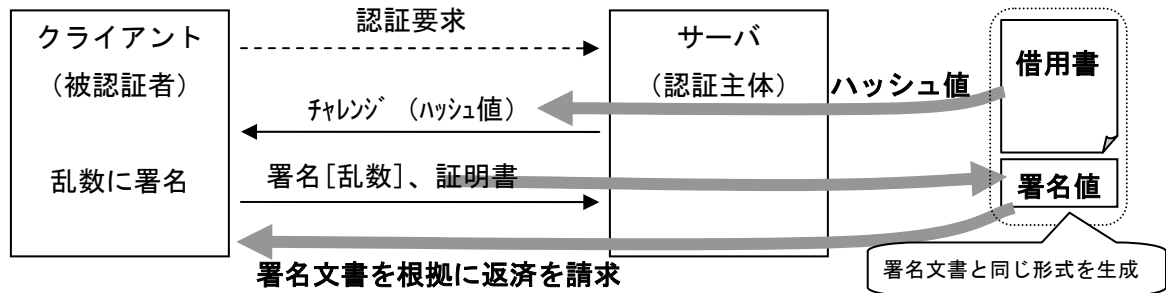


図 9.1.2 意図せぬ電子署名の生成

このリスクへの対策として、署名用の鍵と認証用の鍵の区別をそれぞれの公開鍵証明書の証明書ポリシー、鍵使用目的などに明記しておくことが効果的である。これらの情報に基づいて署名用の鍵を認証に用いないようにしたり、あるいは認証用の鍵で意図せぬ電子署名付き文書が作成されたとしても、ポリシーによってその電子署名を無効とみなすようにすることが可能となる。

上記のようなリスク回避の観点の他、求められる暗号アルゴリズムあるいはそのパラメータの強度の違いから両者を使い分けることが有効である場合が考えられる。認証の場合、署名値の検証は認証主体によって認証時のみに行えばよいが、電子署名の場合は対象文書の保存期間にわたって署名値を検証できる必要がある場合がある。従って、認証用のアルゴリズムおよびパラメータよりも署名用のアルゴリズムおよびパラメータにより高い強度が求められる。例えば RSA 暗号を用いる場合、より高い強度を要求される署名用の鍵長を 2048 ビットとし、認証用の鍵長を 1024 ビットとするなどの使い分けが考えられる。

9.2 使い分けの方法

HPKI 対応 IC カードガイドラインによると、認証用 HPKI カードアプリケーションと署名用 HPKI カードアプリケーションが規定され、それぞれ別々の IC カードアプリケーション識別子 (AID) が割り当てられる。

1 枚の IC カードには、認証用 HPKI カードアプリケーション、または署名用 HPKI カードアプリケーションのいずれか一つのカードアプリケーションしか存在しない場合と、それぞれ 1 つずつで 2 つのカードアプリケーションが存在する場合が想定されている。ま

た、それぞれのカードアプリケーション内には、私有鍵とそれに対応するエンドエンティティ（EE）公開鍵証明書は一つずつしか存在しないことが想定されている。

HPKI 対応の PKCS#11 ライブラリは、認証用 HPKI と署名用 HPKI のそれぞれに対して異なる dll 等として実装することが HPKI 対応 IC カードガイドラインで推奨されている。それぞれの PKCS#11 ライブラリには対応するカードアプリケーションの AID が保持されているため、PKCS#11 ライブラリの利用者が AID を意識する必要はない。認証用 HPKI 対応 PKCS#11 ライブラリと署名用 HPKI 対応 PKCS#11 ライブラリはファイル名で区別する(例えば、認証用：HpkiAuthP11.dll、署名用：HpkiSigP11.dll)。

Crypto API の場合も同様で、電子署名用の CSP と認証用の CSP がそれぞれを用意することが推奨されている。両者はプロバイダ名で区別され、例えばそれぞれ"HPKI Crypto Service Provider for Non Repudiation"、"HPKI Crypto Service Provider for Authentication"となる。やはりこの場合も Crypto API の利用者が AID を意識する必要はない。

HPKI アプリケーションは、認証用 HPKI を利用するか署名用 HPKI を利用するかを意識して実装する必要がある。HPKI アプリケーションが認証用 HPKI カードアプリケーションにアクセスする場合は、認証用 HPKI 対応 PKCS#11 ライブラリ（上記例では HpkiAuthP11.dll）をロードして利用する。また、HPKI アプリケーションが署名用 HPKI カードアプリケーションにアクセスする場合は、署名用 HPKI 対応 PKCS#11 ライブラリ（上記例では HpkiSigP11.dll）をロードして利用する。

Crypto API の場合、プロバイダハンドルを得るときに署名用であるか認証用であるかの用途に応じたプロバイダを上記のプロバイダ名で指定する。

なお、PKCS#11 および Crypto API のインターフェースとコーリングシーケンスの詳細については HPKI 対応 IC カードガイドラインの最新版を参照されたい。

9.3 複数の EE 証明書が存在する場合の対応方法

HPKI 対応 IC カードガイドラインでは、1 枚の IC カードには、認証用 HPKI カードアプリケーションおよび署名用 HPKI カードアプリケーションがそれぞれ一つまでしか存在しないことが想定されており、またそれぞれのカードアプリケーション内には、私有鍵とそれに対応する EE 証明書は一つずつしか存在しないことが想定されている。また、認証用 HPKI を利用するか署名用 HPKI を利用するかによって HPKI アプリケーションは PKCS#11 ライブラリあるいは CSP を使い分けるため、常に HPKI アプリケーションには利用できる証明書（と対応する私有鍵）は高々一つしか見えない。従って、HPKI 対応 IC

カードガイドラインが推奨する IC カードを利用するのであれば、複数の EE 証明書が存在する場合の対応方法を考慮する必要はない。

一方、HPKI 対応 IC カードガイドラインの推奨に従っておらず利用できる EE 証明書を複数格納する IC カードを利用する場合、鍵を利用するにあたり、まずクライアント側で候補となる EE 証明書を取得し、各証明書について、トラストアンカ、証明書ポリシー、鍵使用目的、サブジェクト、有効期間、失効状態などをチェックし、利用する私有鍵を選択するという手順を必要とするかもしれない。ただし、認証の場合は証明書検証を厳密に行う必要があるのは加入者を受け入れるサーバ側であり、クライアント側では証明書にかかわる処理を必要最低限として応答性能を重視しようという考え方もある。9.1 でも述べたとおり、署名の場合と比較して、認証の場合はクライアント側で誤った証明書（と私有鍵）を利用した場合のリスクが少ないと考えられるからである。ただし、やはり 9.1 で述べた署名用の鍵を認証に用いた場合のリスクを考えると鍵使用目的のみは確実にチェックするように実装することを強く推奨する。

附属書 A HPKI 認証用証明書プロファイル（基本領域）

A-1 HPKI 認証用証明書プロファイル（基本領域）

表 A.1 HPKI 認証用証明書プロファイル（基本領域）

項目	設定	説明
Version	◎	Ver3 とする。
SerialNumber	◎	同一認証局が発行する証明書内でユニークな値とする。
Signature	◎	
Validity	◎	
NotBefore	◎	
NotAfter	◎	
Issuer	◎	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	◎	c=JP（固定）とする。
LocalityName	△	
OrganizationName	◎	
OrganizationUnitName	△	
CommonName	◎	認証局のポリシーを示す文字列を記載する。 （「HPKI-01-*-forAuthentication-forIndividual」とする。なお、文字列中の"01"は、CP の版数である"第 1.0 版"を示す。また、"*"は CA を唯一に識別できる文字列とする。）
Subject	◎	英数字のみ使用する。（CountryName、SerialNumber は Printable、それ以外は UTF-8 で記述する）
CountryName	◎	c=JP（固定）とする。
LocalityName	△	
OrganizationName	○	加入者が医療機関等の管理者の場合は必須。 その場合は医療福祉機関名をローマ字あるいは英語名で
OrganizationUnitName	○	OrganizationName に記載し、OrganizatioUnitName に” Director” の文字列を格納する。
CommonName	◎	加入者の氏名をローマ字で記載する。
GivenName	×	
SurName	×	
e-Mail	×	
SerialNumber	△	医籍登録番号などを記載することができる。

SubjectPublicKeyInfo	◎	
Algorithm	◎	RSAEncryption とする。
SubjectPublicKey	◎	
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	◎	拡張領域 (Extensions) 参照

表中の、「◎」は必須、「○」は場合により必須、「△」はオプション、「×」は設定しないことを表している。

「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省) より

A-2 HPKI 認証用証明書プロファイル (拡張領域)

表 A.2 HPKI 認証用証明書プロファイル (拡張領域)

項目	設定	説明	Critical
authorityKeyIdentifier	◎		FALSE
subejctKeyIdentifier	◎		FALSE
KeyUsage	◎		TRUE
DigitalSignature	◎		-
NonRepudiation	×		-
KeyEncipherment	×		-
DataEncipherment	×		-
KeyAgreement	×		-
KeyCertSign	×		-
CRLSign	×		-
EncipherOnly	×		-
DeciphermentOnly	×		-
extendedKeyUsage	△		FALSE
privateKeyUsagePeriod	×		FALSE
certificatePolicies	◎		TRUE
policyMapping	×		FALSE
subjectAltName	△		FALSE
issuerAltName	△		FALSE
subjectDirectoryAttributes	◎	医療従事者等の資格 (hcRole) を記載。	FALSE
AttrType	○	加入者が国家資格保有者及び医療機関等の管理者の場合は必須。その他(患者等)の場合は省略可。	-

AttrValues	○	HCActor の codeDataFreeText に資格名テーブルの英表記を UTF8String で設定。subject が複数の資格を有する場合は、HCActorData に資格数分の HCActor を設定する。	-
basicConstraints	×		TRUE
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		TRUE
policyConstraints	×		TRUE
cRLDistributionPoints	◎	DirectoryName あるいは URI で、CRL の配布点を指定する。	FALSE
subjectInfoAccess	×		FALSE
authorityInfoAccess	△		FALSE

表中の、「◎」は必須、「○」は場合により必須、「△」はオプション、「×」は設定しないことを表している。

「保健医療福祉分野 PKI 認証局 (人) 証明書ポリシー」(厚生労働省) より

付録 1：参考文献

厚生労働省・医療情報システムの安全管理に関するガイドライン 第四版

<http://www.mhlw.go.jp/shingi/2009/03/s0301-4.html>

独立行政法人 情報処理推進機構(IPA)・PKI 関連技術解説

<http://www.ipa.go.jp/security/pki/>

(財) 医療情報システム開発センター・行政情報ライブラリ セキュリティ基盤

<http://www.medical-it-link.jp/lib/index.shtml#sk>

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

<http://www.jahis.jp/standard/seitei/st07-005/st07-005.htm>

ISO 17090-1:2008

Health informatics -- Public key infrastructure -- Part 1: Overview of digital certificate services

ISO 17090-2:2008

Health informatics -- Public key infrastructure -- Part 2: Certificate profile

ISO 17090-3:2008

Health informatics - Public key infrastructure - Part 3: Policy management of certification authority

付録 2 : 作成者名簿

東芝住電医療情報システムズ (株)	岡田 康
富士通 (株)	熊野 顕生
セコム (株)	佐藤 雅史
日本電気 (株)	島 成佳
日本電気 (株)	対比地 幹雄
日本電気 (株)	高野 敏男
三菱電機インフォメーションシステムズ (株)	瀧 勝也
(株) 島津製作所	西田 慎一郎
セコム (株)	西山 晃
JAHIS 特別委員	長谷川 英重
サイバートラスト (株)	松本 義和
三菱電機 (株)	宮崎 一哉
三菱電機 (株)	茗原 秀幸

日付	バージョン	改定履歴 内容
----	-------	------------

(JAHIS 標準 10-005)

2010 年 03 月発行

～ J A H I S H P K I 電子認証ガイドライン V1.0～

発行元 保健医療福祉システム工業会

〒105-0001 東京都港区虎ノ門 1 丁目 19-9

(虎ノ門 TBL ビル 6F)

電話 03-3506-8010 FAX 03-3506-8070

(無断複写・転載を禁ず)