資　料　５

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

医療情報ネットワーク基盤検討作業班

1. 検討の経緯

近年、情報技術の進展に伴い、個人が自らの健康情報を、自らの健康のために電子的に管理・活用することが可能になってきており、IT 戦略本部においても「個人による健康情報の集積・予防医療等への活用の推進」として「個人が自ら健康情報を管理し健康管理等へ活用するための仕組みの確立」が掲げられている。

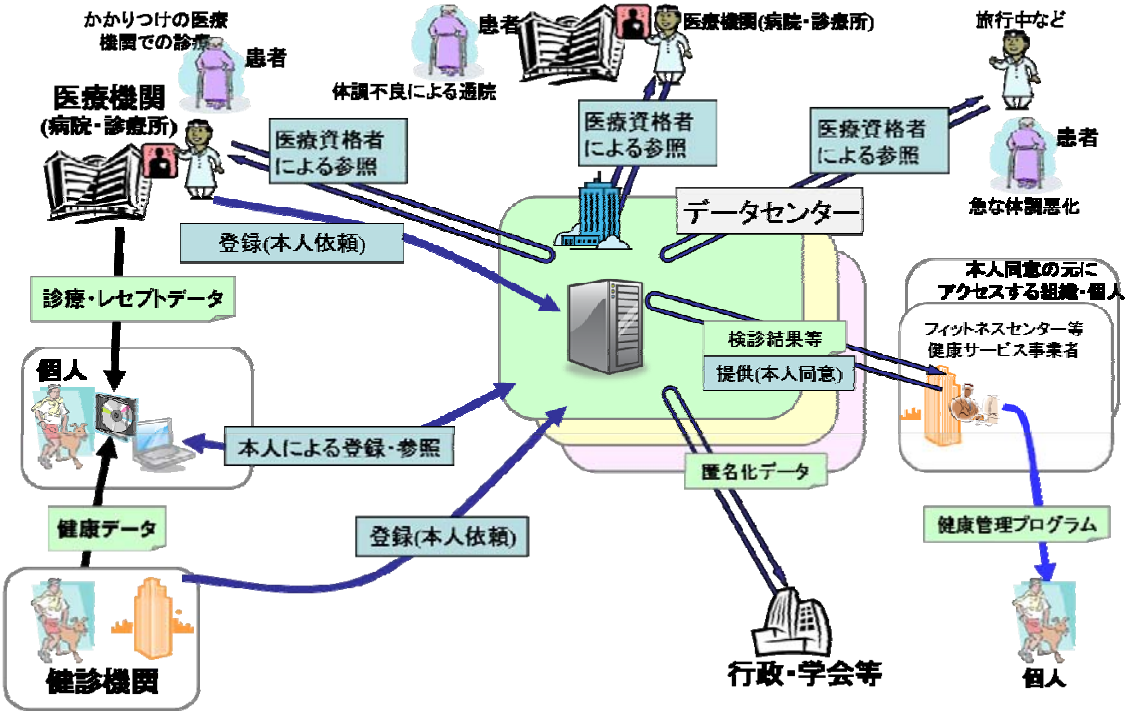
このような動向に対して、医療情報ネットワーク基盤検討会では作業班を設けて、個人自らの健康情報の管理・活用の視点から想定されるユースケースを洗い出し、医療の現場を見据えた議論を行ってきた。

議論に際しては、地域医療連携等において、医療機関等が医療情報を含む健康情報を安全に共有する際に必要な認証機能の要件や認証ポリシの必要性について検討してきたほか、個人が自らの医療情報を管理活用する方策や、その際に求められるセキュリティ等技術的要件について、検討を重ねてきた。その中でも、医療従事者が患者等の医療・健康情報にアクセスする際に必要となる認証方式については、集中して検討が必要と認識された。

2. 検討の前提と医療従事者認証の必要性

2.1 想定する環境

今回の検討は、図 1 に示す通り、個人が健診、レセプト、医療機関等からの情報提供などを通じて入手した自らの医療情報を含む健康情報を、自治体、民間などが運営するデータセンターに自らの希望で保存して管理し、必要に応じて本人、もしくは本人の委託を受けた医療従事者等が参照を行う環境が構築されていることを想定する。



（図 1）

2.2　想定するユースケース

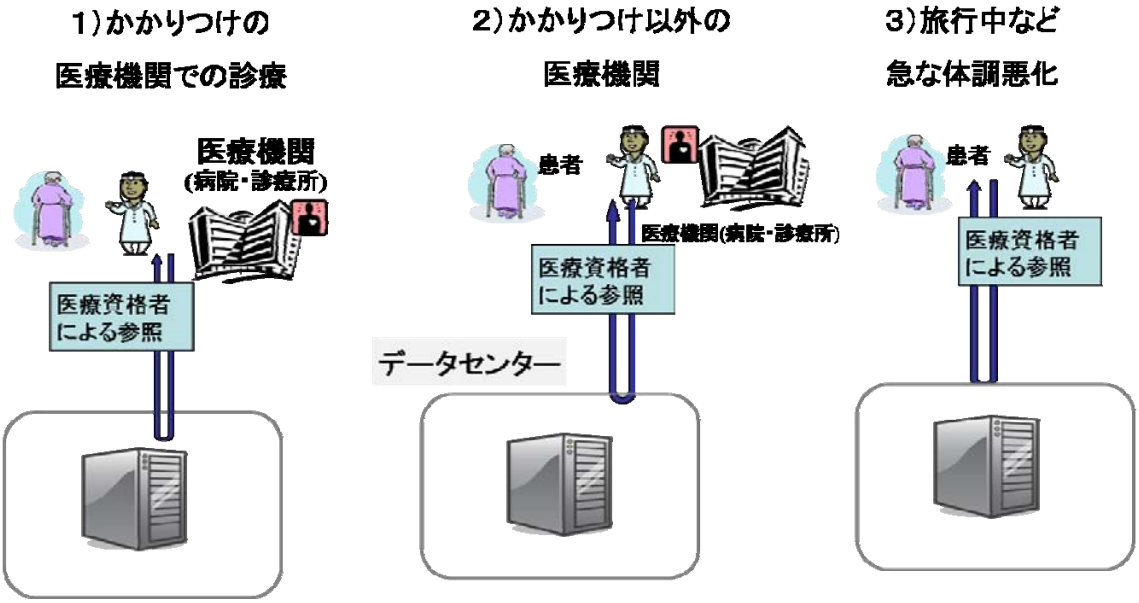
全体としては図 1 のような広範な環境を想定するが、今回の検討は図 2 のような、医療分野に限定した環境を想定する。具体的なユースケースとしては、個人が自らの希望で蓄積した医療情報を含む健康情報を、本人の診療目的のために、国家資格を持つ医療専門職が参照するケースとする。

この際、参照するケースとしては、更に以下の 3 パターンを想定する。

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。



（図２）

2.3　医療従事者認証の必要性

今回想定したユースケースでは、いずれも患者の医療・健康情報にアクセスし、情報を参照しなくてはならない。この場合、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が、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り、何らかの緊急時の情報参照の仕組みが必要となる。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。

従って、当該医療行為を行うために必要な資格を保有しているかどうかを判断し、機微な個人情報へのアクセスの基本要件とすることは医療分野における必要条件である。

この資格という属性を判断し、アクセスを許可する仕組みを属性認証と呼び、実現する方策のひとつとして公開鍵基盤（PKI : Public Key Infrastructure）がある。

今回想定したユースケースでは、この PKI を活用した医療従事者の認証が有効であり、また、必要でもあるとの認識から検討を進めた。

3. 医療従事者認証に必要な要件

3.1 本人性の確認

資格（属性）の確認の前の大前提として、まず非対面で情報がやり取りされる電子世界の中で、本人が本当に本人であるかを確認しなくてはならない。本人が本人であることを「本人性」と言う。

この、本人性を確認する方法として、厚生労働省の「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、記憶（パスワード等）、生体認証（指紋、静脈等）、物理媒体（IC カード等）の三つの要素を示しており、このうちの二つの要素を組み合わせた確認方法（二要素認証）を要求している。

本人性確認方法としてさまざまな認証手段があるが、認証する側は、これらの手段で認証のために使われる情報が確かであることを、何らかの形で管理、運用しなければならない。

単独の医療機関内に限定された環境では、それぞれが独自にルールを決めて採用すればよいが、今回想定する環境においては、全国いずれの場所からでもアクセスできなければならないため、全国共通の本人性確認ルールが必要となる。全国共通の本人性確認ルールを策定する場合は、全国的な規模においても信頼できるスキームを構築する必要がある。

生体認証やパスワード管理を全国統一で実施するためには、全ユーザーの個人情報を統合管理し、維持する必要があるため、一定の安全性を確保し、可用性を担保するための仕組みを構築することは難しい。電子政府や公的個人認証基盤において PKI が採用されているように、安全性の定量的な担保という点においては PKI が有効な手段として認識されている。また、PKI を IC カードに格

納することにより、PKI 利用時にパスワードによる確認を行えるため、ガイドラインの要求する二要素認証（物理媒体+記憶）を満たすことが可能である。

3.2　役割をベースとした属性認証

医療分野においては、資格を保有しているかを判断し、個人情報へのアクセスを許可する仕組みは必要条件であることは既に述べた。ただし、医療行為の実施や患者個人情報へのアクセスに関連する業務アプリケーションに対する、より厳密なアクセス制御を行う場合には、医療専門職の役割に応じた属性認証が必要になる。例えば、「医師」と「看護師」では患者個人情報にアクセスできる範囲が異なるかもしれない。

従来は、各医療機関内や地域内で独自の属性認証の仕組みを個別に構築していたため、施設間や地域間での互換性がない状況であったが、今回想定するユースケースにおいては全国共通の認証基盤が必要となる。

4　認証用 HPKI 環境の構築

4.1　署名用 HPKI フレームワークの適用

医療分野においては、署名用 PKI としてヘルスケア PKI（以下 HPKI）が構築されている。HPKI であれば、一つの証明書検証で、HPKI 認証局が信頼されていれば全国どの組織においても本人性と属性（国家資格）を一度に確認できる。

これを認証フレームワークに適用すると、国家資格という全国共通の属性を各地域で管理する必要がなくなる。すなわち、国家資格の保有について、ルート認証局が信頼点となり保証する環境が構築されれば、異なる地域に属する組織間において属性が担保される。この環境を、現在の署名用の HPKI と区別するために認証用 HPKI とする。

認証用 HPKI は、既存の署名用 HPKI のポリシを証明書の発行ルールに流用可能であるため、最小限の検討によってフレームワークを構築することが可能である。

ただし、実際の発行に当たっては、現在、署名用証明書の発行を行っている諸団体との調整が必要になるため、運用方式や連携方法などについて検討を行う必要がある。

4.2　地域ごとに国家資格管理を行う場合のデメリット

仮に、属性認証に認証用 HPKI を利用しない場合、各地域で各人の国家資格保有の有無を確認し、管理する必要が生じる。利用者は地域ごとに国家資格保有証明を個別に行わねばならなくなる。これは運用管理者にとっても、利用者にとっても非効率的であり、全国共通の確認スキームがあればこの問題は発生しない。

5. 認証用 HPKI の適用範囲の検証

5.1　想定ユースケース以外の認証用 HPKI の活用

認証用 HPKI が構築された場合には、今回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 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、利用者の本人性、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 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。

5.2　各地域等における独自システムに対するアクセス制御

各地域等において構築される地域連携システム等における個人情報へのアクセスにおいては、業務ごとに国家資格以外の属性を含めたアクセス制御が求められる。その場合、各地域等における業務システムやアプリケーションは独自の属性のコントロール（独自の属性定義とその管理）を必要とするため、全国共通で管理すべき属性と各地域等において管理すべき属性を分けて考える必要が生じる。

医療分野においては認証フレームワークとしてISOやHL7などで役割ベースのアクセス制御の国際標準化が進んでおり、役割をベースとしてアクセス権を設定することで、様々な利用シーンにおけるアクセスを可能にする仕組みが提唱されている。各地域等において属性を独自に定義する際にはそれら国際標準を参考にすべきである。

5.3　各地域の自由度を確保した認証フレームワーク構築

各地域が個々に管理するには煩雑で、全国共通の基盤で管理するほうが利用者、管理者にとって有利なものを全国共通フレームワークとすべきである。地域の独自性を許容し、地域の特性に応じた認証基盤を構築するためには、全国的に担保するのは認証用HPKIにおいて担保される、「本人性、実在性、国家資格」までとし、それ以外の役割ベースの認証基盤は、地域等ごとにルールを決めて構築するのが現実的である。

医療分野において各医療情報システム間の相互接続を意識した認証フレームワークの検討がIHEやHL7において行われている。これらの認証フレームワークにおいては、本人確認のベースとしてPKIを利用することが可能であり、今回検討を行っている認証用HPKIも利用可能である。本人性、実在性、国家資格を認証用HPKIで担保し、それ以外の属性の管理を上記の認証フレームワークで管理することで、全国共通の信頼スキームと、地域ごとの自由な認証フ

レームワークの構築が両立できる。

5.4　地域ごとの認証フレームワークの相互運用性

認証用 HPKI の適用範囲については、地域や院内等で活用する場合、「本人性、実在性、国家資格」の確認までとすべきである。

ところが、各地域が提供する認証フレームワークには、全国共通のユースケースと地域独自のユースケースが存在することもある。この場合、全国共通のユースケースにおいては本人性、国家資格をベースとしたアクセス制御を実施し、地域独自のユースケースにおいては地域が設定した役割をベースにした属性を規定することで、全国共通のユースケースにおいては一定レベルの相互運用性が確保される。

しかし、地域独自のユースケースにおいても特定地域間において情報共有を行うなど、全国共通のユースケースよりも高度な属性管理を地域間で担保したいニーズも想定できる。その際に地域間の相互運用性を担保するためには、各地域が定義する役割が相互に解釈可能でなければならない。相互に解釈可能にするためには、属性を表現する用語やコードを合わせることでも対処できるが、全国共通の属性定義は地域間の調整が困難になることが予想される。そのため、地域独自で定義した属性について、組織的役割を機能的役割にマッピングし、機能的役割をベースにした認証ポリシを構築することが必要となる。また、各地域等が発行した属性について相手方が信頼できることが必須となる。

6　その他の検討項目

6.1　署名用証明書の認証用途での利用

新たに認証用 HPKI を整備しなくても、署名用 HPKI を利用して認証する方法も存在する。

この方式は、署名用証明書を使って署名付チケットで認証する方法であるが、署名付チケットの有効期限が長期間でなければ可用性に問題（チケットに署名する際に GUI 等で署名対象を確認することならびに PIN 入力が必須）となる。

また、チケットを長期利用する場合はチケットの偽造対策など別のセキュリティフレームワークが各地域において必要になる。

また、署名用証明書は実印と同等の効力を持っているため、悪用されないための配慮を十分に行う必要があるが、認証用途で利用する場合、署名用途専用で利用するのに比べ、利用機会が増大するため、悪用される機会も増大する。

6.2 認証用 HPKI の適用範囲とは異なるユースケース

例えば、保険情報などの個人情報に保険請求目的等でアクセスするユースケースが存在する。被保険者証の資格確認や地方公費における確認作業などが代表例としてあげられる。

この場合、利用者は医療専門職ではなく、一般の医事課職員等であることが想定されるため、ここで検討した認証用 HPKI のフレームワークの適用は難しい。この様なユースケースでは、医療機関等に対する職責認証の機能を持つ、職責認証のためのフレームワークが別途必要になる。つまり、認証用途に違いはないが、認証するターゲットが医療従事者個人ではなく、医療機関の医事課職員というような職責となり、医事課職員が「誰か」が問題ではなく、「医事課職員」が認証の対象となる。

この様なフレームワーク構築に当たっては施設の実在性を確認し、施設に対して必要な数の職責に対する認証権限を発行することとなるため、認証用 HPKI を転用することは好ましくない。認証用 HPKI とは異なる別の認証フレームワークの作成が必要となる。

7 結論

これまでの検証結果より、以下のように結論を述べる。

- 想定するユースケースにおいて本人性、実在性、国家資格保有を確認できる全国共通のフレームワークは有用であり、09 年度以降に具体化に向けた検討を行うことが求められる。特に認証ポリシの検討、運用方式の検討、署名用

HPKI 発行主体との連携などについて検討を行う必要がある。

・ 認証用 HPKI の環境を構築することで、地域連携システムや院内の医療情報システムにおける認証部分の構築コスト低減や標準化、共通化を促進することができるため、個人が医療情報を活用する事例以外のユースケースにおいても有効である。利用にあたっては各地域等において個別に運用ルールなどを構築する必要があるが、構築できれば地域等ごとの自由な認証フレームワークに活用できる。この点においても認証用 HPKI を推進すべきである。

・ 署名用証明書の認証用途への利用は不可能ではないが、安全性、可用性の観点からは積極的には推奨できない。また、上記の 2 点において認証用証明書の有用性が確認できるため、あえて署名用証明書を認証用途に利用するよりは、認証専用のフレームワークを構築するほうが社会インフラを提供する観点からは望ましい。

・ 国家資格をもつ医療専門職の本人性・実在性・国家資格を認証する仕組み以外の認証フレームワーク構築の必要性も考えられるので、継続して検討を実施する必要がある。