Get Clinical Document

Interaction 14: Get Laboratory Results

EPR Client ---> Message Pool

検査結果問い合わせ

Message Type: Lab Query Get Laboratory Result

Interaction 15: Response to Get Laboratory Results

Message Pool ---> EPR Client

検査結果問い合わせ応答

Message Type: Lab Query Response to Get Laboratory Results

Interaction 16: Active Lab Order Placer - Request Activate Lab Order, Closely-coupled

EPR Client ---> Lab System(Message Pool??)

検査オーダー(予約)

Message Type: Lab Order, Closely-coupled

Interaction 17: Active Diet Order Loose

EPR Client ---> Message Pool

栄養指導箋オーダー(予約)

Message Type: Diet Order, Loosely-coupled

Interaction 18: Document Addendum Notification and Content

EPR Client ---> EPR Database

カルテ保存

Message Type: Document Header and Contents

4．電子処方箋シナリオ

4．1．ICカード使用例

4．1．1．シナリオ： 電子処方箋を本処方箋とし、患者ICカードに処方箋を格納する。

4．1．1．1．

処方箋は診療情報システムで医師が作成し、タイムスタンプと署名をする。

処方箋にはユニークなIDが必要。施設ID+医師ID+患者ID+作成時刻。

4．1．1．2．

処方箋を患者ICカードに格納する。

処方箋原本はICカード内に移動するので、この時点で診療情報システム の処方箋には発行済みのマークが必要。すなわち控えとして残る。

転送時のタイムスタンプと患者の（ICカード内の秘密鍵による）署名

4．1．1．3．

患者はICカードを任意の調剤薬局に提出する。

4．1．1．4．

調剤薬局では薬剤師の資格カードを持つ薬剤師

がICカードから調剤システムに処方箋を転送する。

薬剤師資格カードと患者カードの同時アクセスで、患者カードにより薬剤　師資格（QC）を認証し、処方箋へのアクセスを許可する。

４．１．１．５．

調剤データを調剤システムに転送する。

医師の署名を確認し、医師資格（QC）を確認した上で、ICカード内の処方　箋には転送時のタイムスタンプと薬剤師による署名を行い受領とする。

保険証がICカード化されている場合は保険情報と、もしあれば公費消費状況も転送する。

４．１．１．６．

調剤および与薬を行う。

処方箋が有効であることを確認し、調剤および与薬を行う。処方疑義が　ある場合は医師に問い合わせ、その状況を記録し、全体にタイムスタンプと署名を行う。

４．１．１．７．

調剤済み処方箋に薬剤師が署名を行い、調剤システムに保存する。

調剤済みであることを記録し、タイムスタンプと署名を行う。さらに薬剤受　領書として患者による署名を付記する。

保険証がICカード化されて、公費負担対象かつ公費残額がある場合は公費から薬剤費などの諸費用を引く。

４．１．１．８．

調剤済み処方箋をICカードに転送する。

ICカードはタイムスタンプと患者による署名を付記して、一定期間格納する。

＃保険証がICカード化されていて、公費負担対象でかつ公費残額に変化がある場合はICカードの公費残額を変更する。

４．１．１．９．Open Issue

医師資格、薬剤師資格がPKCにある場合とACにある場合がある。いずれも国家資格であり、CA、AAのいずれも当事者には周知のものとできる。

調剤薬局側が原因でICカードによる運用が不可能な状況（リーダの故障、停電など）がありえる。そのような場合に対応するためには紙の予備処方箋が必要である。予備処方箋を用いた場合には予備処方箋にICカード運用が不可能な理由を記載し、調剤薬局の判断で本処方箋として扱うべきであろう。その場合、ICカードに残っている処方箋の扱いが問題になる。少なくとも処方箋として有効性をなくさなくてはならない。

患者側の原因でICカードによる運用が不可能な状況（カードの紛失、破損など）がありえる。この場合は予備処方箋で運用をするべきではない。紛失を偽装した場合に対応できない。あらためて医師にICカードまたは紙の本処方箋

を発行してもらうしかない。
仮処方情報（現状ではFAXなど）による調剤と宅配による運用がありえる。また宅配でなくても仮処方情報による先行調剤も一般的なサービスとして存在している。先行調剤は医療機関で調剤薬局への通信機構をそなえれば対応可能。宅配を組み合わせた場合も大部分で可能であるが、往診の場合、患者宅と調剤薬局の間の通信を用意する必要がある。そもそも往診で電子処方箋を発行できれば可能かもしれない。

タイムスタンププロトコールはIETFでRFCになっている。これを採用し、TSAが存在し利用可能という前提である。

４．２．ICカードなし

４．２．１．前提

医師は電子署名用および暗号化通信用（SSLに使用する）の2種類の公開鍵証明書を有し、それらの秘密鍵は自分のICカードに保存している。
薬剤師は電子署名用および暗号化通信用（SSLに使用する）の2種類の公開鍵証明書を有し、それらの秘密鍵は自分のICカードに保存している。
患者は公開鍵証明書やICカードを持たない。
電子処方箋を発行する医療機関の処方箋サーバはインターネットに24時間接続している。
処方箋サーバは電子処方箋暗号用および暗号化通信用（SSLに使用する）の2種類の公開鍵証明書を有し、それらの秘密鍵は処方箋サーバ上に安全に保管している。
電子処方箋を受け取る調剤薬局は必要に応じてインターネットに接続可能である。
患者のICカードを前提としないのは、発行に際しての経済的な問題と、患者がICカドを確実に管理できるかどうか不明（紛失や破損、また、来院時に持ってくるのを忘れる、などがかんがえられるからである。ただし、これは現行の受診カードでも同じ問題がある。

４．２．２．処方プロトコル

４．２．２．１．

医師は自分のICカードを処方システムに挿入し、処方を入力する。

４．２．２．２．

処方システムはその処方に医師の電子署名を行う。

４．２．２．３．

処方システムは電子署名付処方箋（電子処方箋）を医師の公開鍵証明書と共に処方箋サーバに登録する。
医師の属性証明書による資格認証は、処方箋サーバに登録時に行う。処方箋サーバは、資格認証に要した属性証明書を電子処方箋、公開鍵証明書とともに保管する。

４．２．２．４．処方箋サーバは、登録された電子処方箋を処方箋サーバの公開鍵で暗号化し、安全に保管する。

４．２．２．５．処方箋サーバは、保管した電子処方箋に処方箋引換え番号を振り、医師に通知する。

４．２．２．６．処方システムは、処方箋引換え番号と処方を印刷する。（処方箋引換え書）

４．２．２．７．医師は、処方箋引換え書を患者に渡し、処方内容を説明する。

処方箋引換え番号は、処方箋サーバを特定する値（URI）とランダムな値の組み合わせである。例えば、prescription.med.kyushu－u.ac.p：2107542989など。

実用的には処方箋引換え書には処方箋引換え番号はバーコードでも印刷される。

４．２．３．調剤プロトコル

４．２．３．１．

患者は調剤薬局の薬剤師に処方箋引換え書を提出する。

４．２．３．２．

薬剤師は自分のICカードを調剤システムに挿入し、処方箋引換え番号を（バーコード）入力する。

４．２．３．３．

調剤システムは処方箋引換え番号と現在時刻に薬剤師の電子署名を付加し（電子処方箋送信依頼書）、薬剤師の公開鍵証明書、属性証明書と共に処方箋サーバに送信する。

４．２．３．４．

処方箋サーバは、その処方箋引換え番号を調剤中とする。

４．２．３．５．

処方箋サーバは、電子処方箋送信依頼書の電子署名および薬剤師の資格を検証する。

４．２．３．６．

検証に成功すれば、処方箋サーバは保管している電子処方箋を復号し、医師の公開鍵証明書、属性証明書、及び、現在時刻と処方箋引換え番号に処方箋サーバの署名をつけた文書（電子処方箋送信書）と共に調剤システムに送信する。

４．２．３．７．

調剤システムは受信した電子処方箋、電子処方箋の送信書の電子署名を検証する。

４．２．３．８．

検証に成功すれば、調剤システムは処方を薬剤師に提示する。

４．２．３．９．

薬剤師は、患者の本人確認、処方内容の確認を行い、調剤する。

４．２．３．１０．

薬剤師は調剤システムに調剤内容を入力する。

４．２．３．１１．
調剤システムは調剤内容に薬剤師の電子署名を付加して、処方箋サーバに送信
する。
４．２．３．１２．
処方箋サーバは、薬剤師の電子署名を検証する。
４．２．３．１３．
検証に成功すれば、処方サーバは保管している電子処方箋を調剤済みとする。
４．２．３．１４．まとめ
処方箋サーバと調剤システムはインターネット上で通信するが、通信はSSLやVPNを使用するため、患者プライバシは保護される。
処方箋サーバは調剤中および調剤済みの状態の処方箋引換え番号に関する問い合わせには、一切応じない。
以上のプロトコルでは、患者は処方箋引換え書により、処方内容を確認することがで
きる、これ自身は処方箋ではないので、いくらコピーしたところで、それだけでは調剤を受けることはできない。
処方箋サーバは電子処方箋を送信する際に、薬剤師の電子署名を検証しるので（４．２．３．５．）、認証を受けた薬剤師以外が電子処方箋を受け取ることはできない。
また、処方箋引換え番号はランダムな値を含んでいますので、悪意を持った薬剤師が処方箋引換え番号を推測して、電子処方箋を受け取ることに成功する確率は非常に低いと考えられる。この確率はランダムな値の長さに依存しますので、必要なだけ下げることがる。また、適当な回数（2－3回）続けて、間違った処方箋引換え番号を送信した薬剤師との通信は処方箋サーバが拒否するような解決策もある。
処方箋サーバは、インターネットに接続されていますが、万が一、クラックされ電子処方箋を取られても、暗号化されているため患者プライバシが侵されたり、あるいはその処方箋が使用されたりする可能性はない。実際には処方箋サーバは直接インターネットに繋がず、その（リバース）プロキシサーバがインターネットに接続されるようにする。
ある調剤薬局で調剤中、あるいは調剤済みとなった電子処方箋について、処方箋サーバは重複して問い合わせに答えることはなく、一処方に付き、一調剤が保証される。
但し、薬剤師が一度獲得した電子処方箋を不正にコピーして同じ処方箋で何度も処方
した場合は、その薬剤師は監査時に処方箋サーバの電子処方箋送信書を提出できないため、コピーを否認することはできない。
また、もし、処方箋サーバが不正をして、電子処方箋の送信依頼が別の調剤薬局から
あって送信したように見せかけてコピーしよう

としても、薬剤師の電子処方箋送信依
頼書を提出できないため、監査時に否認することはできない。
例外シークエンスとしては、調剤中のままの処方ががんがえられる。

D. 考察

今年度に得られた成果はいずれも基礎的なものであり、直接活用したり、提供したりする性格のものではないが、十分に発展性のあるものと考えられる。

下川の研究により、電子商取引など他分野における電子署名関連技術をそのままでは医療分野に持ち込むことは非常に難しいことが明確となった。そのため、医療分野における電子署名の実用化に関しては本研究で行うべきであるという実証が得られたこととなる。

さらに、山本の研究により、諸外国においても電子署名を用いた電子カルテや処方箋への署名がさまざまに検討されており、本研究が対象としている公開鍵基盤を用いる方法が主流であることが明確となった。一方で、そのような方向性で進んでいるにも関わらず、どの組織においてもまだ検討段階であり、本研究のように具体的な分析や設計を行っているものが少ないことが判明した。すなわち、本研究は着眼、および手法において海外の研究をリードしているものと考えられる。

また、坂本の研究により、処方箋等を電子的に交換する際のシナリオ、ユースケース、プロトコルが明確となり、電子署名の付加方法が同定されると考えられる。

本研究の成果を次年度以降利用することにより、確実に電子署名を用いた安全な情報交換が実現可能であると考えられる。

E. 結論

平成13年度は基礎的な事項の調査研究が目的であった。

最初に、公開鍵基盤の現状および医療における適応に関して一般的なサーベイを行った（坂本）。さらには保健医療において、電子署名や公開鍵基盤が利用される場面についてユースケース分析を行った。そして、その結果を用いて、電子署名を付加すべき情報の通信モデルを作成した。

次に、国際動向についてサーベイを行った（山本）。PKIはITU-T X.509を基本にIETFのpkixで各種の標準が作成されているが、これらはすべて汎用の標準案であり、比較的自由度が高い。すなわち適応分野の特性に応じて詳細を取り決めなければ互換性のある運用は難しい。本研究では保健医療福祉分野にPKIを応用する場合の要件を抽出し、国際的な標準化の動向等を調査

し、わが国の医療分野で用いる場合のガイドラインを作成し、評価することを行った。

また、国内における他の分野におけるPKIの利用方法についてサーベイを行った（下川）。その結果、保健医療分野のように横断的にPKIや電子署名を利用している例はあまり見受けられなかった。

以上の研究結果を基に、来年度はより詳細な実用化研究を行う予定である。

F. 健康危険情報

なし。

G. 発表

1. 坂本 憲広：公開鍵証明書を用いた国立大学病院保健医療情報利用者認証システムの開発、電子情報通信学会論文誌D-I Vol. J-84-D-I No. 6 pp. 830-839 2001年6月、2001年

2. Norihiro SAKAMOTO : A New Approach for Unification of Healthcare Information Exchange Protocols Through HL7 RIM、Japanese Journal of Medical Informatics、Vol. 21, No. 1、pp. 13-22、2001年

3. Norihiro SAKAMOTO : The Construction of a Public Key Infrastructure for Healthcare Information Networks in Japan、MEDINFO 2001, V.Patel et al. (Eds), Amsterdam IOS Press, © 2001 IMIA, pp. 1276-1280、2001年

保健医療福祉分野でのPKI利用状況および背景調査とガイドラインの作成

分担研究者　山本　隆一　大阪医科大学 病院医療情報部 助教授

研究要旨　公開鍵基盤（Public Key Infrastructure 以下 PKI）は ITU-T X.509 を基本に IETF の pkix で各種の標準が作成されているが、これらはすべて汎用の標準案であり、比較的自由度が高い。すなわち適応分野の特性に応じて詳細を取り決めなければ互換性のある運用は難しい。本研究では保健医療福祉分野に PKI を応用する場合の要件を抽出し、国際的な標準化の動向等を調査し、わが国の医療分野で用いる場合のガイドラインを作成し、評価することを目的とした。今年度は ISO を主体とする実情調査と PKI を保健医療福祉分野で応用するための要件抽出をおこなった。

A．研究目的

PKI は ITU-T X.509 を基本に IETF の pkix で各種の標準が作成されているが、これらはすべて汎用の標準案であり、比較的自由度が高い。すなわち適応分野の特性に応じて詳細を取り決めなければ互換性のある運用は難しい。本研究では保健医療福祉分野に PKI を応用する場合の要件を抽出し、国際的な標準化の動向等を調査し、わが国の医療分野で用いる場合のガイドラインを作成し、評価することを目的とした。

B．方法

1　1998 年より国際標準化機構（ISO）で保健医療福祉分野の情報に関しての標準化作業が行われている。その中で WG4 として Security が取り上げられ、ISO Technical Specification（TS17090）として PKI に関するドキュメントが作成されつつある。本研究ではこのドキュメントを中心に、pkix の各種の標準およびドラフト、さらに電子署名をわが国で法的に有効にするために電子署名法と電子署名法施行規則を調査した。

2．上記で調査した結果を元に現在わが国で行われている実証実験などの実態および電子証明法に関する要件も考慮して、保健医療福祉分野で PKI を用いるための要件を抽出した。

C．結果

1　ISO TS17090 について

ISO TS17090 は ISO の TC215（Technical Committee 215 – Health Information）ので作成された PKI に関する Technical Specification（技術仕様書）で、PKI を医療情報の国際的な交換に用いる際の要件について記載している。Technical Specification は ISO Standard ではなく、現時点で強制力はないが、3 年後に見直され ISO Standard になる可能性はある。ISO Standard になれば公共機関の入札などでは準拠する必要があり、軽視することはできない。

TS17090 は 3 部からなり、第 1 部は概念の定義を中心に記載されており、PKI の全体を説明している。第 2 部は証明書のプロファイルが中心で、技術的な要件が主体である。第 3 部は証明書発行ポリシについて記載されている。この中で実際にわが国の保健医療福祉分野に PKI を応用する場合に重要なのは第 2 部と第 3 部である。そこで第 2 部および第 3 部の特徴を列挙する。

1-A 第二部　証明書プロファイル等

基本的に ITU-T X.509 の第 3 版に準拠しており、特に証明書の基本フィールドでは規格上の変更はない。暗号アルゴリズムやハッシュアルゴリズムをいくつか挙げて推奨しているが、必須ではない。

一方、拡張フィールドではフィールドの追加はないが、Special Subject Directory Attributes に hcRole という Attribute Type を規定していて、ここに保健医療福祉分野の役割を記載することにしている。また公的資格などに用いる個人を厳密に証明する Qualified certificate statement extension について言及しているが、必須ではなく、IETF の Qualified Certificate の標準である RFC3039 をポイントしているだけである。Key Usage フィールドについては暗号化と署名を同じ鍵ペアで用いることを禁止している。

後で述べるように保健医療福祉分野では属性証明書が有効と思われるが、TC17090 第 2 部でも属性証明書を取り上げている。しかし属性証明書自体の規格が IETF でもまだドラフトであり、TC17090 でも必要性とドラフト段階でのプロファイルを ASN.1 表記で述べているに過ぎない。

タイムスタンプの記載はほとんどなく、ディレクトリサービスも具体的には触れられていない。ディレクトリサービスに関しては別アイテムとして ISO TC215 で検討される予定である。

1-B　第 3 部　証明書発行ポリシ

証明書発行ポリシは PKI の基幹を成す文書で、きわめて重要であるが、法律や制度に関係し、国際的な標準案を具体的に定めることはできない。したがって TS17090 でも証明書発行ポリシのフレームワークである RFC2527 にほぼそのまま準拠し、フレームワークを提供しているに過ぎない。

2　電子署名法および施行規則について

保健医療福祉分野で PKI を用いる目的の 1 つが電子署名であり、かつ法的に有効な電子署名である。わが国では平成 12 年に電子署名法が制定され 13 年に施行されたところであり、保健医療福祉分野でも PKI を応用するにあたって、電子署名法に準拠する必要がある。

電子署名法および施行規則では証明書のプロファ

イル自体はあまり厳格に規定されていない。したがってTS17090の要件を満たせばおおむね適合する。ただし、暗号アルゴリズムとハッシュアルゴリズムは抽象的に規定されており、それ以外は用いることができない。さらに特定認証業務に関する指針の中で厳密にアルゴリズムを指定している。

また TS17090 と同様に暗号化と署名を同じ鍵ペアで行うことは禁止されている。

3．わが国の保健医療福祉分野でのPKIの要件

保健医療福祉分野で PKI を用いるにあたっての要件を抽出するために、院外処方、外注検査、診療情報提供書などのいくつかのユースケースでシナリオを検討した。その結果、ア）法的に有効な署名、イ）法的に有効でないがコミュニティで信頼される署名、ウ）個人認証、エ）役割認証、オ）暗号化の使用用途が導かれた。それぞれについて要求事項を抽出し、整理したところ、以下のようになった。

A）署名に用いる場合、電子署名法およびその関連規則に準拠する。
B）医療記録の責任の所在を明確にするために行う署名にはタイムスタンプが必要である。
C）個人認証および役割属性のうち、長期間変化しない属性（例えば医師という属性）は公開鍵証明書で運用すべきであり、この場合の役割属性は Special Subject Directory Attribute フィールドで hcRole 属性タイプを用いて記述すべきである。
D）役割属性のうち、比較的短期間に変化する可能性のあるもの（例えば勤務先や担当病棟）は属性証明書を用いるべきである。
E）暗号化用の鍵ペアは署名や個人認証、役割認証に用いてはいけない。
F）署名用公開鍵証明書を広域で用いるためには、証明書発行ポリシを同一のものとするか、少なくとも互換性のあるものとしなければならない。
G）署名用の公開鍵証明書で電子署名法およびその関連規則と ISO TS17090 で規定されていないプロファイルについては互換性を確保するために規定する必要がある。
H）電子保存された文書の真正性確保のために電子署名を用いる場合、公開鍵の寿命を超えた検証が必要になるので、その対策が必要である。

D．考察

ISO TS17090 では保健医療福祉分野で公開鍵証明書を発行する対象として End Entity Certificates の Individual、Organization、を挙げ、さらに公開鍵を含まない属性証明書(Attribute Certificates)もついて言及している。公開鍵証明書や発行対象に応じてプロファイルをある程度さだめることが必要で、属性証明書も広域で利用する場合はプロファイルを規定する必要がある。この中で Device や Application に PKI を用いる場合、証明書のプロファイルで保健・医療・福祉分野で特別に考慮することはなく、また SSL/TLS や PKI-VPN のように各方面で応用されている例があり、それらを参考にすればよい。ただし用途によっては機器やアプリケーションに対する証明書の発行ポリシは人や組織に対するものと同等の厳格さが要求される。

1．署名について

End Entity Certificates の中で Individual、つまり医療従事者や患者などのサービス受給者に証明書を発行する場合と、Organization、つまり医療機関や保健者などの組織に証明書を発行する場合、その用途はいくつか考えられる。用途の 1 つ目は「署名」で、これには法律や規則で定められている署名・捺印を電子的に行う場合と、法律や規則で定められてはいないが、情報作成・編集の責任者を明確にするために行う場合がある。また電子署名は通常，署名の対象となる情報のダイジェストに対して行われるので、もとの情報の完全性（真正性）の保証のための 1 つの手段としての意味がありえるが、完全性については後で考察を加える。署名が法律や規則で定められている場合はわが国では「電子署名法」に準拠した証明書と署名方法が必要である。電子署名法では電子署名に用いる証明書は署名の目的のためだけに用いることが定められているので、署名に用いる証明書およびそのペアの署名鍵は他の用途に用いることはできない。法律・規則で定められていない署名に同じ証明書や署名鍵を用いるかどうかは、運用で定めなければならないが、今後の連携医療の発展を考えると、あまり狭い範囲だけで通用する証明書を用いることは推奨されない。また証明書の数が増えるとそれだけ運用に負担がかかるので、法的に有効な署名と同じものを用いるべきであろう。

2．鍵ペアの生成と否認不能性

公開鍵の生成は PKI にとって重要な部分で、署名自体や署名の検証は計算量も少なく、高速に処理できますが、鍵の生成は計算量も多く、良い鍵を生成するためには厳密な乱数の発生が必要である。したがって鍵を生成するプログラムは厳密に選ぶ必要がある。これは証明書発行局の運用規則(Certificate Practice Statement: CPS)でしっかり規定しておく必要がある。

さらに鍵をどこで生成して、どのように管理するかも PKI にとって大変重要である。電子署名が確実に本人の署名であることを証明（否認不能性）するためには、署名鍵は本人だけしか知らないということを証明することが必要である。そのためには鍵の生成を本人（証明書の所有者）が行うか、署名検証等の事後の運用で利害関係のない第 3 者が作成し、本人に送付後はただちにすべてのコピーを破棄する必要がある。証明書発行局と証明書の所有者は一般的に言って署名の検証に問題があった場合に対立関係になる可能性が高いので、電子署名を目的とする鍵は証明書発行局が生成することは、推奨されない。

3．資格認証

保健・医療・福祉分野では情報を扱う人の資格や役割が重要な場面が多くある。PKI で資格や役割をあらわすためには 2 つの方法がある。1 つは公開鍵証明書に資格や役割を示すフィールドを定義して使う方法で、もう 1 つは属性証明書を使う方法である。この 2 つの方法にはそれぞれ特徴があり、使い分けを工夫する必要がある。属性証明書は公開鍵が含まれていなくて、通常は短い有効期間で使用する。また公開鍵がないために署名との関連付けは属性証明書自体ではできないので、対応する公開鍵証明書を一緒に用いる必要がある。

属性証明書と公開鍵証明書の使い方を検討するためにA病院の内科外来を担当するX医師が紹介されて受診した患者の過去の診療記録について紹介元のB医療機関に問い合わせる場合を考える。X医師はB医療機関に対して問い合わせ書を作成して送るが、B医療機関は問い合わせて来た人の身元や属性を確認することなしに、患者情報を返送することはでき

ない。A病院の内科に患者を紹介したことはわかっているので、問い合わせて来た人がA病院の内科担当の医師であることを確認すればよい。

3－1．公開鍵証明書による資格認証

最初に公開鍵証明書だけですべての属性を証明する場合を考える。この場合証明書にはXという人で、医師であって、A病院の従業員で、内科外来担当であることが記載されることになる。そしてこの証明書はB医療機関で信頼できるものであると判断されなくてはいけない。したがって証明書の発行者はB医療機関が信頼できる組織が発行したものである必要がある。A病院が大阪にあり、B医療機関が東京であることもありえるし、それ以外の医療機関とも同様な場合が起こりうることを考えると、事実上日本中ですべての医療機関から信頼される組織が証明書を発行する必要がある。

仮にこの発行機関を○○センターと仮定する。○○センターはXが医師であることは厚生労働省に問い合わせることで理論的には確認することが可能である。またA病院が存在することも地方自治体等に問い合わせることで確認できる。これらは手間ではあるが、仕組みをうまく作れば現実にも可能である。X医師がA病院に勤務していることも保険医登録情報などを用いれば確認することができる。しかしX医師が内科外来担当であることはA病院に問い合わせる以外に確認の方法がない。証明書発行の要請があるたびにその医療機関に勤務形態を確認しなければならないので、証明書発行の運用は複雑になる。これは証明内容に責任を持つ組織が 1 つの証明書に対して多数存在するための複雑さといえる。また、もし発行したとしても内科外来担当から救急外来担当に変わった場合や、A病院からB病院に転勤した場合には証明書を廃棄して、新しい証明書を発行しなければならない。電子証明書は単なるファイルなので、いくつでもコピーできる。したがって電子証明書そのものをすべて廃棄することは不可能なので、証明書廃棄リスト（CRL）を発行し、証明書を使う人は常に最新の CRL を参照して、その証明書は廃棄されていないかどうかを確認する必要がある。転勤や担当部署の変更は全国的に見れば日常的に起こると考えられるので、大量の CRL が常に存在することになり、PKI 全体の運用に大きな負担になる。

つまり医療で必要なすべての属性を 1 つの公開鍵証明書に盛り込むことは現実には不可能といえる。複数の公開鍵証明書を組み合わせて使う方法も考えられるが、もとの情報と証明書を関連付けるためには電子署名を行う必要があり、公開鍵証明書の数だけ電子署名を重ねる必要がある。そのため電子署名の順序など複雑な取り決めをしなければならないし、CRL が大量に発生する問題は解決できない。

3－2．属性証明書による資格認証

属性証明書は技術的には公開鍵証明書の簡略版であり、比較的簡単に発行できるし、通常は数時間～数日といった短期間で無効になるようにするために、資格や役割の変更があっても CRL を発行する必要性はほとんどない。一方、属性証明書には公開鍵がないので、電子署名と直接対応付けることはできない。公開鍵証明書と組み合わせて用いる必要がある。つまり属性証明書で資格認証を行うということは、公開鍵証明書を属性証明書の使い分けを考えることにほかならない。

公開鍵証明書だけで資格認証を行う場合にうまくいかない理由は証明内容に責任を持つ組織が複数存在することと、CRL が大量に発生することであった。従ってこれらの障害を取り除くことができるような属性証明書と公開鍵証明書の使い分けを考えればよい。公開鍵証明書は基本的には公開鍵が誰のものか証明するものである。この「誰」に対して責任を持つ組織が単純であり、「誰」があまり変化しなければ公開鍵証明書の運用は単純になり、それ以外の属性を属性証明書で証明すればよいことになる。このような「誰」の定義には２つの場合を考えることができる。

1 つ目は個人や法人といった人格を「誰」として扱う場合である。このような公開鍵証明書に対する署名は個人「実印」や法人の「公印」に相当すると考えてもよい。証明に責任を持つ組織は住民票情報を管理している地方自治体や法人登記または医療機関登録を管理している組織が適当である。法人登記の電子化や公的個人認証基盤は政府の e-Japan プロジェクトの一環として整備されつつあり、制度的な問題は別として技術的には比較的容易に運用可能である。先の例で言えばXさんとA病院、B医療機関がそれぞれ公開鍵証明書を 1 つもつことになる。Xさんが医師であること、A病院の勤務医であること、内科外来担当医であることはすべて属性証明書で運用することになる。この方法では CRL はほとんど発生しないし、属性証明書を証明内容ごとに複数使うことにすれば、証明内容に対する責任組織も単純になる。ただし一般には属性証明書は有効期間が短いものなので、しばしば必要になる医師の資格を示す属性証明書もその都度、発行を要求しなければならない。医師の資格に責任を持つのは厚生労働省であるから、たとえ地方自治体に業務を委託するとしても医師資格属性証明書の要求は多数が集中する可能性が高く、運用上の負荷になりうる。医師のような公的資格は変更が極めて少ないので、属性証明書の有効期間を長くすることも考えられる。しかしこの場合は少ないとはいえ、資格喪失などがあるために、属性証明書の CRL の発行を考えなければならない。CRL の発行はそれほど難しいことではないが、属性証明書を使うシステムがすべて CRL を検索しなければならなくなり、実装上の負荷になる可能性が高い。また属性証明書は公開鍵証明書に関連付ける必要があるが、属性証明書の有効期間が公開鍵証明書の有効期間を超えることはできないために、公開鍵証明書の有効期間が残り少なくなっている場合などは属性証明書の有効期間を変えなければならず、発行自体も複雑になる。

2 つ目は公的な資格を含めた個人を「誰」として扱う場合である。法人や組織は１つ目の場合と同じである。先の例では「医師であるXさん」を公開鍵証明書で資格認証し、「A病院の勤務医」、「A病院の内科医外来担当医」を属性証明書で資格認証する。この場合は運用がもっとも単純になる。公的資格はほとんど変化しないので、CRL の発生は少なく、証明内容の責任の所在も単純で明確であり。唯一の問題はXさんが医師として署名する場合と、個人として署名する場合に証明書や署名鍵を使い分ける必要があることだが、あまり大きな問題にはならないと考えられるし、心情的にはかえって好まれるかも知れない。公的資格には「医師」のような国家資格や「保険医」のような地方自治体に対する登録資格があり、現在の管理体制では責任の所在が異なる以上は証明書を分ける必要があるが、これは制度的な整備や「保険医」の属性証明を医療機関や医師会な

どに委任することで、解決することが可能である。

4．暗号化

PKI は暗号化に用いることもできる。PGP や S/MIME は公開鍵証明書を用いた認証と暗号化を組み合わせたプロトコールで広く使用されている。アプリケーションやライブラリも数多く存在し、また保健医療福祉分野で特別な要素もないので、PKI を暗号化に用いること自体はあまり問題がない。しかしただ 1 つ注意しなければならないことは、法的に有効であることが求められる署名に用いる証明書や署名鍵は暗号化に使ってはいけないということである。また保健医療福祉分野の情報は利用できなければ意味がない。暗号化によって万が一にも利用性が阻害されることがないように注意する必要がある。通信途中のような一時的な暗号化は問題が少ないが、データベースそのものを暗号化するような場合は、事故などがおこっても必要なときに速やかに復号できる必要がある。

5．電子保存の真正性と長期にわたる署名の確認

PKI は公開鍵暗号を基礎においているが、公開鍵暗号の安全性は時間的に有限とされている。例えば 1024 ビットの RSA 暗号を用いる場合は２～３年程度の安全期間を前提に運用されることが多い。単純な情報交換やある時点での資格認証には問題がないが、保存された情報の署名の有効性を長期にわたって確認する必要がある場合には問題が生じる。法的に保存が義務付けられた情報は３～５年、あるいはそれ以上の間、真正性を保って保存しなければならない。例えば２年の寿命の公開鍵暗号を用いる場合、公開鍵が作成され証明書が発行された直後に署名を行っても、その署名が確認できる、つまり PKI で真正性が保証されるのは高々２年である。したがって PKI を利用して電子保存の真正性を求める場合は工夫が必要になる。

1 つは署名そのものの有効期間を延長する方法である。簡単に言えば有効期間が切れる前に新しい署名鍵と公開鍵証明書を作成し、再署名する。この方法は単純であるが、署名者ごとに署名の有効期間を管理し、再署名を依頼する必要があり、個別に再署名する限り、ほとんど不可能と考えてよいだろう。システムで自動的に再署名する方法も考えられるが、署名鍵にシステムがアクセスできる必要があり、署名の否認不能性に影響を与える。

2 つ目は署名の確認者を置く方法である。例えばすべての署名は有効期間が 1 ヶ月以上ある署名鍵および公開鍵証明書を用いて行うことと決めておき、その時点で確認されていないすべての署名を一ヶ月に一度確認する。そして有効であった署名のなされた情報のリストを作り、そのリストに確認者が署名を行う。これを確認済みリストとし、さらに確認者の署名の有効期間が過ぎる前に確認済みリストの署名確認を行い、そのリストを作成し、署名を行う。これを何度か繰り返せば一定期間の真正性は確認者の信頼性のもとに保証される。

2 つ目の方法の応用として、確認リストを作成した時点で機能上および運用上で改ざん不可能な媒体（例えば第三者が監査可能な金庫保管した CD-ROM など）に固定して厳重に管理することも可能である。

いずれにしても単純に電子署名をしたから長期の保存の真正性が確保されると考えることはできない。

6．タイムスタンプ

電子署名によって署名時点での真正性が証明可能であり、また前節にのべたような工夫を行えば一定期間の真正性も確保できると考察したが、保健医療福祉分野の場合、情報が作成された時刻や、順番が重要である。虫垂炎と診断した時点と虫垂炎の手術を行った時点がこの順か、逆の順かで大きく意味が変わる。したがって一般に保健医療福祉分野では電子署名を行った時刻が大変重要で、信頼性のある時刻情報を付加する必要がある。訴訟等で証明力を確保しようとすると、時刻の信頼性は第三者にとっても信頼できるものでなければならない。

第三者に信頼される時刻情報を付加するためにはタイムスタンプ発行局は保健医療福祉機関から独立した信頼できる第三者機関（Trusted Third Party : TTP）が行うことが求められるが、しっかりした監査によって信頼性が説明可能であれば、保健医療福祉機関内部やそのグループ内に置くことも可能と考えられる。

E．結論

PKI の保健医療福祉分野への応用について、ISO における標準化の動向および、わが国の電子署名法とその関連規則を調査し、また現在行われている実証実験の実情を勘案し、PKI の保健医療福祉分野での要件を抽出した。おおむね ISO TS17090 と電子署名関連法規に準じればよいことがわかったが、タイムスタンプの必要性と長期間の真正性確保に関して保健医療福祉分野に特化した要件があった。また属性証明書を有効に活用することで、PKI 全体の運用を合理化できることが判明した。

F．発表・参考文献

著書・論文

1．医療経済研究機構監修、医療白書 2001 年度版（プライバシー保護としての医療情報のセキュリティ対策　山本隆一）、日本医療企画、東京、2001

2．財団法人四国産業・技術振興センター編、電子カルテネットワーク（診療情報交換とセキュリティ、電子カルテネットワークの技術的課題－セキュリティ　山本隆一）、エムイー振興協会、東京、2001

3．山本隆一、医療情報のセキュリティ、システム／制御／情報、44、576-582、2000

4．　山本隆一、電子保存新基準について　－運用規定策定の試みと評価－、映像情報、32(2)、92-96、2001

5．　山本隆一、医療情報システムのセキュリティモデル、医学のあゆみ、196、277-281、2001

6．　山本隆一、ネットワーク時代の身分証明と安全性確保 － 電子化された診療情報のセキュリティについて －、治療、83、245-251、2001

7．　山本隆一、ネットワーク時代の医療情報の安全性、BIO Clinica、16、721-725、2001

8．山本隆一、増田　剛、濱田松治、生体識別（Biometrics）、Innervision、16(7)、14-16、2001

9．　山本隆一、医療情報のセキュリティ、Mebio、18(5)、132-138、2001

発表

1．山本隆一、シンポジウム医療情報の国際標準-ISO TC215 の活動をめぐって-　Security - Public key infrastructure など、第 21 回医療情報学連合大会、東京、2001

他分野におけるあ電子署名技術の利用動向調査

九州大学大学院システム情報科学研究院情報工学部門　下川俊彦

A. 研究目的

電子署名技術は、今後の IT 社会において、重要な社会基盤の一つとなるものである。保険医療分野への電子署名技術の導入にあたっては、他分野における電子署名技術導入事例を参考にすることは大変有効である。そこで、本研究では、他分野における電子署名技術の利用動向調査研究を行った。

B. 結果

1. 電子商取引分野

現在実用化されている電子署名技術を利用した分野には以下のようなものがある。

- 暗号化電子メイル
- 暗号化通信
- VPN (Virtual Private Network)
- インターネットクレジットカード決済
- IC カード電子貨幣

保健医療分野への電子署名技術の導入において、その大きなターゲットの一つは電子処方箋システムである。電子処方箋システムへの電子署名技術の適用を前提にすると、これは電子貨幣システムとの類似性が高いことが予想された。そこで、まず電子商取引分野での電子署名技術に関して調査を行った。

1.1 Web ベース電子商取引

この分野では暗号化通信の中で電子署名技術が利用されている。現在 Web ベース電子商取引の中で広く利用されている暗号化通信技術には以下の二つがある。

- SSL (Secure Socket Layer)
- TLS (Transport Layer Security)

SSL は Netscape 社が規定した暗号化通信技術である。公開されているものとしては Version 2 プロトコルと Version 3 プロトコルの二つがある。draft-freier-ssl-version3-02.txt という Internet Draft によって Version 3 プロトコルの規格が公開されている。

TLS は SSL version 3.0 を基盤として、インターネット上で利用される技術の標準化を行う団体である IETF (Internet Engineering Task Force) の TLS ワーキンググループによって規定された暗号化通信技術である。RFC2246 によって規格が公開されている。トランスポート層で通信路を暗号化するため、アプリケーションに日依存である。また公開鍵暗号技術をベースとして、サーバ・クライアント間で相互認証を可能としている。

1.2 電子貨幣

電子貨幣システムで用いられている電子署名機能は主に以下の 3 つである。

- 発行期間の真正性の証明
- 一貫性の証明
- 相手認証

電子貨幣システムを分類すると以下のようになる。

・ 電子貨幣決済型

  ➢ プリペイドカード型

  ➢ ネットワーク型

  ➢ IC カード型

・ クレジットカード決済型

1.2.1 プリペイドカード型電子貨幣

これは、プリペイドカードを電子商取引に持ち込んだものであり、以下のような特徴をもつ。

・ 購入したプリペイドカードに ID を記載

・ 購入時に ID を入力

・ 小額決済向き

・ 認証機能なし

実システムの例としては WebMoney, BitCache がある。

1.2.2 ネットワーク型電子貨幣

専用ウォレットソフトを PC にインストールし利用する。ウォレットに連動した銀行口座・クレジットカードから支払いを行う。

実システムの例としては CyberCoin, Millicent, Ecash がある。

1.2.3. IC カード型電子貨幣

IC カード内に貨幣情報を格納するものである。使い切り型と補充可能型がある。

実システムの例としては Mondex, VISA キャッシュがある。

1.2.4 クレジットカード決済型電子貨幣

実システムとして SET(Secure Electronic Transaction) がある。これは、Visa と MasterCard 両者によって策定された規格である。このシステムではカードホルダと小売業者がデジタル証明書を持ち、相互認証を行う。カードホルダの証明書は電子ウォレットにインストールする。

SET は図 1 のようなシステムになっている。

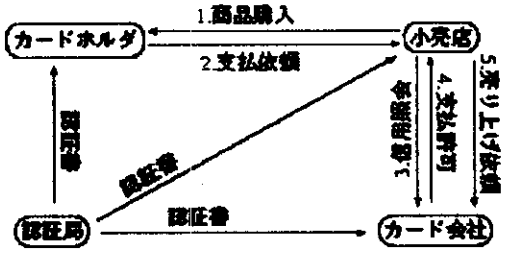

図 1 SET

このシステムではカードホルダからの注文書と支払書を小売店へ渡す。小売店では支払書の情報を読むことはできない。また、クレジット会社では注文書の情報を読むことはできない。

C. 考察とまとめ

電子商取引分野での電子署名技術の導入は、実際にはほとんど進んでいないことが分かった。既存のシステムの中では、SET のシステムが、電子カルテシステムとの対比を考えると類似点が多いのではないかと考える。今後は、さらに詳細な考察を進めたい。

研究成果の刊行に関する一覧表

書籍

著者氏名	論文タイトル名	書籍全体の編集者名	書　籍　名	出版社名	出版地	出版年	ページ

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
Norihiro SAKAMOTO	A New Approach for Unification of Healthcare Information Exchange Protocols Through HL7 RIM	Japanese Journal of Medical Informatics,	Vol. 21 No. 1	13-22	2001
Norihiro SAKAMOTO	The Construction of a Public Key Infrastructure for Healthcare Information Networks in Japan	MEDINFO 2001, V.Patel et al. (Eds), Amsterdam IOS Press	© 2001 IMIA	1276-1280	2001

20011224

以降のページは雑誌/図書等に掲載された論文となりますので
「研究成果の刊行に関する一覧表」をご参照ください。