20011224

厚生科学研究研究費補助金

医療技術評価総合研究事業

保健医療分野における電子署名の実用化に関する研究

平成１３年度　総括・分担研究報告書

主任研究者　坂本 憲広

平成１４（２００２）年４月

目　　次

厚生科学研究費補助金(医療技術評価総合研究事業)

総括研究報告書

保健医療分野における電子署名の実用化に関する研究

総括研究者　坂本 憲広　九州大学医学部附属病院講師

研究要旨

平成13年度「保健医療分野の情報化にむけてのグランドデザイン」においても、公開鍵基盤を用いた個人認証の必要性が、情報化のための基盤整備の促進の1つの課題として認識されている。公開鍵基盤の中核技術である電子署名とは、発信者本人しか使えない暗号化処理を電子文書に施すことにより、その電子文書が発信者のものであり、通信路の途中で改竄されていないことを証明するものである。保健医療文書の中にも法的に署名もしくは記名捺印が必要なものがあるが、平成13年度より電子署名法が施行されるため、この電子署名が利用できれば、電子カルテの応用範囲が広がり、より高品質の医療の実現に繋がることが期待される。逆に、電子署名を施さない限り、電子化した保健医療文書を保健医療施設間で交換し、その情報に基づいて診療を行うことは困難である。しかしながら、医療文書の電子化、あるいはその電子署名の付加に際しては、法的、技術的に様々な問題を解決しなければならない。本研究は、保健医療分野において電子署名を実用化するための様々な問題を明らかにし、それに対する現実的な解法を与えるものである。

本年度（平成13年度）では、処方箋や診療情報提供書など、保健医療施設間で頻繁に交換される保健医療文書を対象として、それに電子署名を付加するための情報モデルおよびプロトコルを研究開発した。研究の遂行にあたっては、坂本が総括及び全体設計を行い、山本が特に法的問題に関して、下川が主として技術的問題に関して研究を行い、一定の成果を得た。

分担研究者：

山本 隆一

大阪医科大学教授

下川 俊彦

九州大学大学院 助手

A. 研究目的

本研究の目的は、署名もしくは記名、押印の必要な診療録に対して、その電子化診療録に電子書名を行うことができるよう、電子署名の保健医療分野での実用化のための基礎研究を行うことにある。

診療録等の電子保存を認める厚生省通知により、電子カルテが保健医療の現場に普及しつつある。しかしながら、処方箋を始めとして、いくつかの保健医療文書は署名もしくは記名捺印が法的に要請されているため、電子カルテを活用している保健医療施設においても、それらを紙に印刷し、そこへ署名もしくは記名捺印を行っている。こうした現状は、情報技術の導入による事務作業の合理化を阻害していると同時に、電子化された情報を複数の保健医療施設間で共有することによる、高品質の医療の実現にとって大きな障害となっている。

一方、インターネットを利用した電子商取引は、教育、金融、医療等、多くの業界に及んでおり、それらを安全に行うために、政府（所管省庁：総務省、経済産業省、法務省）は、2000年5月の第147回国会で成立した電子署名法（正式名称：電子署名及び認証業務に関する法律）において、電子署名や電子認証を行う業務に一定のルールを課し、手書きの署名や押印と同様な法的位置付けを行った。

本研究は、この電子署名を保健医療分野において実用化するための技術を研究、開発しようとするものであり、電子カルテの普及、患者サービスの向上を実現する上においての基盤を提供しようとするものである。

電子署名の実用化に関する研究は様々な分野において行われているが、他分野の電子署名技術をそのまま保健医療分野に応用することはできない。例えば、一般の電子商取引における電子署名は、その電子文書が発信者のものであり、通信路の途中で改竄されていないことを証明するものである。しかし、例えば、電子署名を付加した処方箋では、その内容の真正性とともに、その処方箋が一度しか利用されないこと（単用性）が保証されなければならない。従って、保健医療分野において独自の研究を進める必要性がある。

この研究により、電子カルテの利便性、安全性が大きく向上すると期待される。

B. 研究方法

本研究においては、署名もしくは記名捺印の必要な保健医療文書のうち、最も利用が多いと考えられる、処方箋と診療情報提供書を主たる対象とする。例えば、電子処方箋が実用化されれば、薬剤の二重投与や同時服用禁忌などの問題が解決され、個人の健康に資するとともに、薬剤の副作用情報などを全国的に集計しやすくなり、公衆衛生的なメリットも大きい。

PKIの利用目的は、主として暗号化通信による秘匿性の担保と電子署名による情報源の確認である。前者は主としてVPNやSSL/TLSでの通信相手の認証と共有鍵の鍵交換に用いられる。後者は電子メールや電子文書への署名に用いられる。

電子カルテの活用や昨今の社会的要請により、医療情報をネットワークを経由して電子的に交換したいという要求が増えてきている。こうした医療情報の中には、法的要請あるいは真正性の確認、証拠性の担保の観点から電子署名付き文書として交換することが望ましいものがある。このような要求の実現にはPKIの利用が不可欠であると考えられる。ここでは、保健医療において電子署名付き文書交換を主目的としたPKI利用が要求される場面を包括的に特定し、そのトップユースケースを分析、生成することを試みる。

本年度は、電子署名の法的および技術的サーベイを行うとともに、電子署名を付加した保健医療文書のモデル化を行い、その流通性を確保し、真正性や単用性を担保するためのプロトコルを研究開発する。特に総括研究においては、研究全体を概観するために、保健医療分野におけるPKI利用のトップユースケース分析と紹介状、処方箋等の医療情報のインタラクション分析を行う。

1．保健医療における電子署名と公開鍵基盤の概念整理

2．保健医療分野におけるPKI利用のトップユースケース分析

3．HL7V3に基づく患者紹介状インタラクション分析

4．電子処方箋シナリオ

なお、本研究では倫理面の問題は存在しない。診療情報を対象としているが、すべて架空のデータであり、結果には個人を特定できる情報はまったく含まれていない。

C. 研究結果

1．保健医療における電子署名と公開鍵基盤の概念整理

保健医療分野においては、電子署名や公開鍵基盤については、詳細かつ包括的な説明はこれまで行われてきていない。そこで、本研究を遂行するにあたり、まず、保健医療における電子署名と公開鍵基盤についての概念整理をおこなった。

1．1．公開鍵基盤

公開鍵基盤(PKI: Public Key Infrastructure)とは、公開鍵暗号方式(public key cryptography)を利用したセキュリティ技術を広域分散環境において利用するのに必要とされるサービス群を提供するためのフレームワークである。公開鍵暗号方式を利用したセキュリティ技術としては、メッセージの暗号化による盗聴の防止、電子署名による改竄、なりすまし、否認の防止などが挙げられる。これらのセキュリティ技術を利用するためには、私有鍵(private key)および公開鍵(public key)を必要に応じて入手しなければならない。そこで、これらの私有鍵／公開鍵を生成し、管理し、配布し、あるいは廃棄するためのサービスを提供するのが、公開鍵基盤の主たる役割である。

1．2．鍵

公開鍵基盤においては、鍵は最も基本的な要素であり、その鍵を用いたメッセージの暗号化／復号化を様々に応用して、公開鍵基盤におけるセキュリティ技術を構築する。暗号鍵は、秘密鍵方式(secret key cryptography)と公開鍵方式(public key cryptography)に大別される。公開鍵基盤において前面に用いられているのは公開鍵であるが、公開鍵基盤におけるセキュリティ技術の様々な局面で秘密鍵方式も公開鍵方式と協調して用いられている。

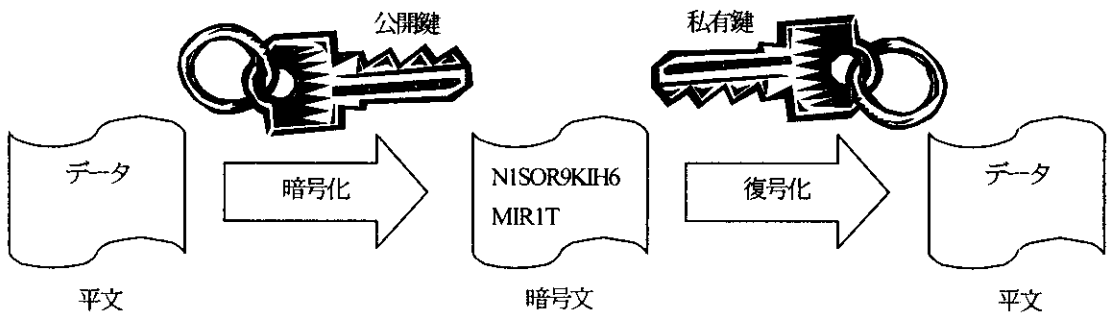
1．3．暗号方式

公開鍵基盤では、主として公開鍵暗号方式を利用する。公開鍵暗号方式は、数学的には非対称関数を利用するもので、1対の鍵ペアを使用し、一方の鍵を使用してデータを暗号化し、対になるもう一方の鍵を使用してその暗号文を復号化するという方式により、通信データを安全に交換することができる。非対称関数利用した暗号化には、一方の鍵で作成した暗号文は、対となるもう一方の鍵でしか復号化できない（もとの鍵でも復号できない）という性質があるため、暗号化通信に公開鍵暗号方式を利用する場合には、暗号化の鍵（暗号鍵）は秘密にしておく必要はなく、復号化の鍵（復号鍵）のみを秘密にし、安全に保管すればよい。

１．４．公開鍵アルゴリズム

現在、最も広く用いられている公開鍵暗号アルゴリズムは、RSA公開鍵暗号アルゴリズムである。RSA公開鍵暗号アルゴリズムは1978年に当時米国のマサチューセッツ工科大学（MIT）の暗号学者であったRon Rivest、Adi Shamir、Len Adlemanが考案した。RSA公開暗号アルゴリズムは、この3人の名前の頭文字を取って命名された。1983年にはRSA公開暗号アルゴリズムに関して米国特許が成立しており、現在ではRSA Security社が管理しており、さまざまなセキュリティ製品、電子商取引アプリケーションに組み込まれている。

RSA公開鍵暗号アルゴリズムは、大きな素数（おおよそ300桁以上）を見つけることは容易であるが、2つの大きな素数の積を因数分解することは困難であるという数学的な性質に基づいて、公開鍵係数(Public Modulus)と呼ばれる数学を応用している。RSA公開暗号アルゴリズムの安全性は,因数分解の係数因子の大きさに依存している。これまでは512ビット係数（512ビット鍵）がよく用いられてきたが、その鍵長では現在では十分安全とは考えられていないが、1024ビット鍵は現在でも十分安全と考えれており、最近では1024ビット以上の鍵が主流となってきている。



１．５．　メッセージダイジェスト(message digest)

これまでに紹介した暗号方式は、秘密鍵暗号方式にしても公開鍵暗号方式にしても、平文から作成された暗号文をもとの平文に変換することができる可逆的暗号方式である。一方で平文を変換した暗号文より元の平文を再構成することができないような非可逆型の暗号方式も存在する。これは数学的には一方向関数（入力に対して出力を計算することは容易であるが、得られた出力よりもとの入力を計算することは困難あ

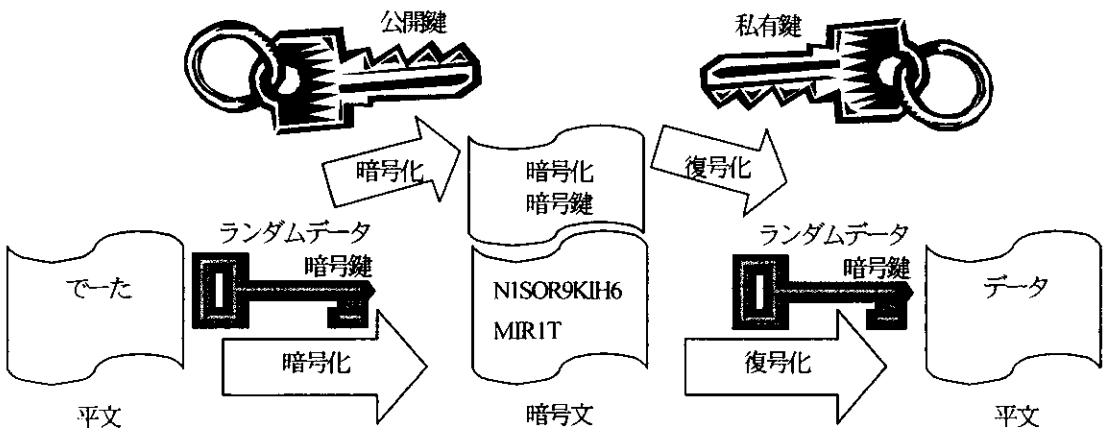
るいは不可能な関数）である。この機能は電子署名などを行うには必須であり、ハッシュ関数(hash function)あるいはメッセージダイジェスト機能と呼ばれる。すなわち、平文であるメッセージをハッシュ関数に入力すると、暗号文としてメッセージダイジェストが出力される。メッセージダイジェストは一般的には128ビットであり、どのような長さの入力メッセージに対しても同じ長さのメッセージダイジェストが生成される。

様々なハッシュ関数の内、現在広く用いられているものはRSA Security社の開発したMD4(Message Digest 4)およびMD5(Message Digest 5)と、米国政府の開発したSHA(Secure Hash Algorithm)である。SHAは160ビットのメッセージダイジェストを生成するため、他の128ビットのメッセージダイジェストを生成するハッシュ関数と比較してより安全であると考えられている。

1．6． 公開鍵基盤の利用

公開鍵基盤の利用方法には、暗号化通信と電子署名の二つの方法がある。公開鍵を利用した暗号化通信はVPNにおいても利用されている。

公開鍵暗号を利用した暗号化通信では、個々の通信文の暗号化に際して、ランダムに秘密鍵を生成し（ランダムデータ暗号鍵）、そのランダムデータ暗号鍵で通信文を暗号化する。一方、ランダムデータ暗号鍵を受信エンティティの公開鍵で暗号化し、秘密鍵暗号アルゴリズムに関する情報を暗号化した秘密鍵に添付して、暗号化した通信文と共に受信エンティティに送信する。ランダムデータ暗号鍵は一度限り使用されるので、通信エンティティが保管する必要もなく、またシステムによって自動的に生成され、

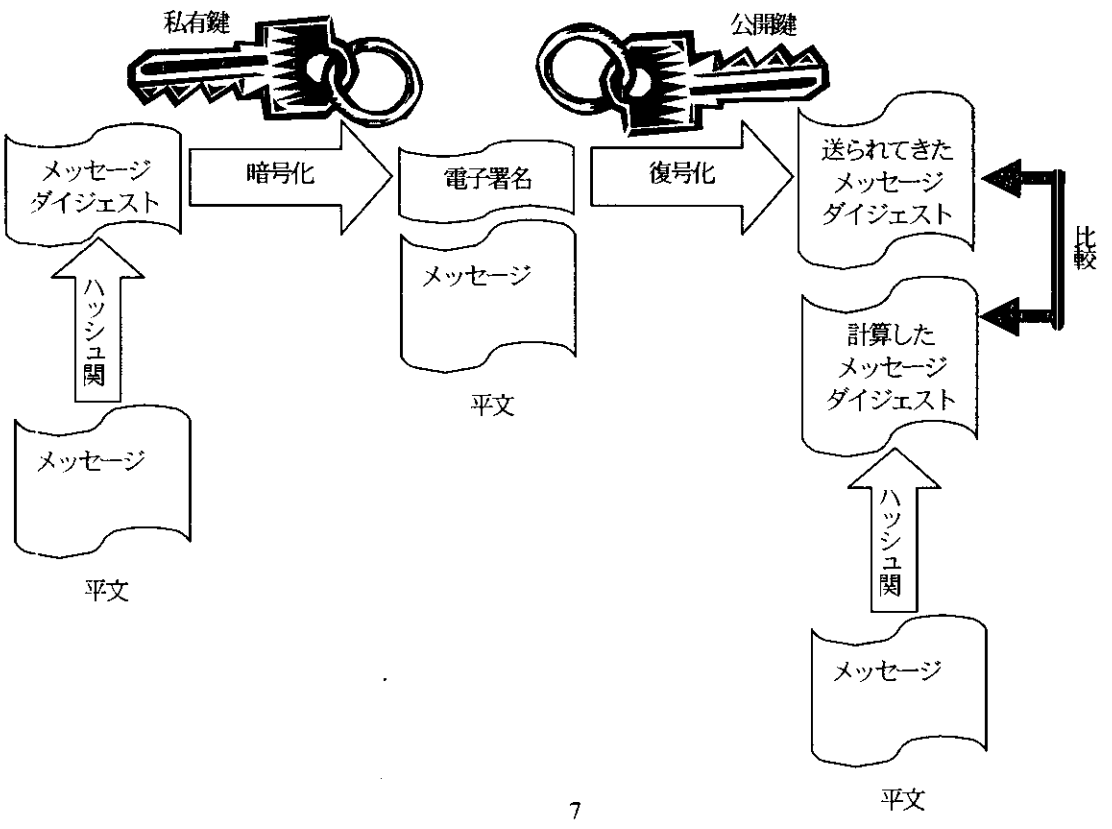


使用されるので通信エンティティがその存在を意識することは通常ない。

電子署名では、発信エンティティの私有鍵を暗号鍵としてメッセージを暗号化し、その暗号文を平文のメッセージと一緒に受信エンティティに送信する。受信エンティティは発信エンティティの公開鍵を復号鍵として暗号文を復号化し、添付された平文と比較して同じであれば、メッセージが完全であることを知る。同時に、ある公開鍵で正しく復号化できるのはそれと対をなす私有鍵で暗号化されたメッセージだけであり、また私有鍵はその所有者以外には使用できないという事実から、受信エンティティは送信エンティティを特定し確認することができる。

１．７．　認証局と証明書

これまで公開鍵暗号を用いて暗号化や電子署名など有用なセキュリティサービスを実現できることを説明してきた。公開鍵暗号方式で広域分散環境において安全に通信しようとする際の最大の問題は、ある公開鍵が誰のものであるかをどのようにして知り、どのようにして確認するかにある。秘密鍵暗号方式では、通信エンティティは実際の通信に先立って通信相手と何らかの安全な方法で秘密鍵を受け渡ししなければならない。そのため通常はこの際に、ある特定の通信エンティティとその秘密鍵を関連付け、確認することができる。しかし、公開鍵暗号方式では、ある通信エンティティと通信したいとす



ると、ネットワーク上に公開されているその通信エンティティの公開鍵を取得して、その公開鍵を用いて、メッセージの暗号化や、電子署名の確認を行う。このようにして公開鍵を取得するだけで安全な通信が行えることが公開鍵暗号方式の大きな利点ではあるが、同時にネットワーク上の公開鍵をその所有者（公開鍵ユーザ）である特定の通信エンティティと関連付け、確認することは大変困難な問題である。例えば、A病院のA医師に患者紹介状を送りたいとする。インターネット上でA医師のメールアドレスと公開鍵が公開されていたので、それらを用いて患者紹介状を暗号化し、電子メールで送信したとする。しかしながら、このメールアドレスと公開鍵はたまたま同姓同名の別のA医師のものであったかも知れないし、悪意のある第三者がA医師の名前を使って勝手に架空のメールアドレスと公開鍵を公開しているものであったかも知れないし、また、メールアドレスは本来のA医師のものであるが、公開鍵は架空のもので、悪意のある第三者がその私有鍵を持ち、A医師宛の暗号化されたメッセージを盗聴し、復号化しようとしているものであったかもしれない。いずれの場合においても、公開鍵暗号方式は正しく機能しているにも関わらず、偶然か故意かに関わらず、患者プライバシを保護することはできない。

1．8．　認証局

上記のような問題を解決するためには、公開鍵と公開鍵ユーザを正しく関連付ける仕組みが必要である。その仕組みの1つとして考えられるのが、公開鍵基盤における認証局(CA: Certification Authority)である。認証とはエンティティが正しくそうであると主張している通りであるかどうかを確認し、証明することである。従って、公開鍵基盤における認証局とは、通信エンティティがある公開鍵の所有者であるという主張に対する信頼を付与する機関である。認証局は関連する通信エンティティ全てから信用された機関でなければならず、こうした機関を信頼できる第三者機関(TTP: Trusted Third Party)と呼ぶ。認証局が、公開鍵ユーザを認証する際には、一般的には認証を要求するユーザ（主体者）が認証局に出向き（存在証明）、公開鍵と共に身分証明書などを提示する（本人証明あるいは同一性証明）。認証局は、それらを確認し、公開鍵を登録する。その後、認証局はあるエンティティの公開鍵に対する問い合わせや、ある公開鍵ユーザに関する身元問い合わせなどに権威をもって応えることができる。

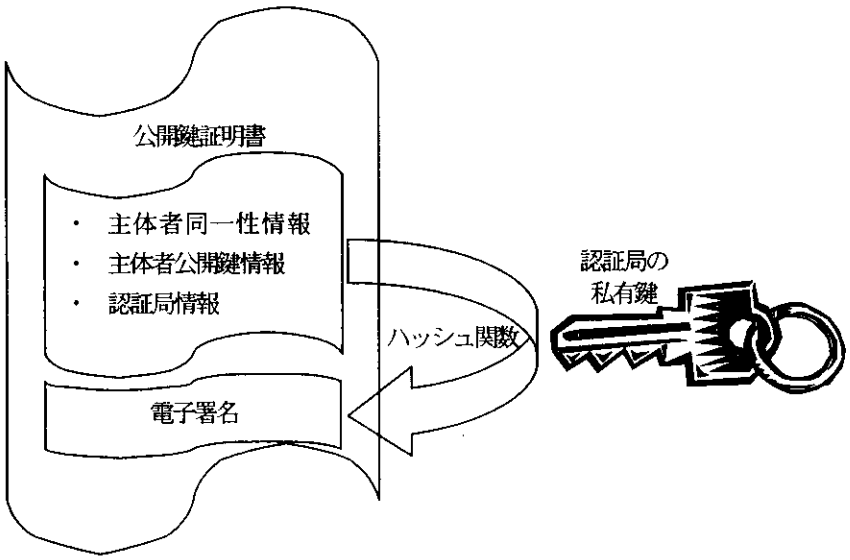
認証局は公開鍵ユーザを認証する際に存在証明や本人証明などネットワークを介しては難しい作業を行う必要があり、全世界あるいは全国で1ヶ所の認証局で全てを執り行うことは現実的に

不可能である。従って、地域毎、あるいは認証しようとしている主体者の属性などによって多数のカテゴリの認証局が運営される必要がある。

１．９．　公開鍵証明書

ある公開鍵ユーザが公開鍵暗号方式を利用するたびに、その公開鍵に対する問い合わせが認証局に対して発生するとすると、現在のインターネットのような多数のユーザが存在する状況では、認証局の作業量は膨大なものとなり、また公開鍵暗号方式を利用したメッセージを受信したエンティティの手間や待ち時間も大きくなる。そこで認証局が随時個別の問い合わせに応えるのではなく、公開鍵の登録時にその公開鍵が申請の主体者である公開鍵ユーザのものであるということを証明する文書を発行し、その証明書を用いて各受信エンティティが通信に使用されている公開鍵の正当性を確認できるようにしたものが、公開鍵証明書(Public Key Certificate)である。すなわち、公開鍵証明書は、私有鍵の所有者の実体とネットワーク上でのエンティティである公開鍵を関連付け、その関連を保証するものである。そのため、ある通信エンティティからの暗号化メッセージや電子署名がある公開鍵証明書が証明する公開鍵で復号化できたとすると、それらのメッセージや署名は確かに公開鍵証明書に記載された主体者のものであることが確認される。

一般に公開鍵証明書には、公開鍵と共に、その公開鍵証明書が証明しようとする公開鍵ユーザの身元に関する情報である主体者同一性情報、この公開鍵証明書を発行しようとしている認証



局名が含まれており、さらにこれらの情報に対する認証局の電子署名が添付されている。

１．１０ X.509標準形式公開鍵証明書

現在、公開鍵証明書として最も広範に用いられている標準形式はX.509バージョン3である。X.509標準はISO/IEC/ITUが制定した標準で、1988年にバージョン1、1993年にバージョン2、1996年にバージョン3と改定されている。X.509バージョン3形式公開鍵証明書は以下の領域からなる。

- 証明書形式バージョンナンバー領域
- 証明書シリアルナンバー領域
- 証明書発行認証局電子署名アルゴリズム識別子領域
- 発行者名前領域
- 有効期限（開始日時(not before)／終了日時(not after)）領域
- 主体者（認証対象）名前領域
- 主体者公開鍵情報（アルゴリズム識別子、パラメータ、公開鍵値）領域
- 発行認証局ユニーク識別子領域
- 主体者ユニーク識別子領域
- 拡張領域
- 発行認証局電子署名領域

例えば、証明書発行認証局電子署名アルゴリズム識別子領域には、RSA/MD5（公開鍵暗号アルゴリズムはRSAで、ハッシュ関数はMD5である）といった情報がコード化して格納される。これらの領域の内、発行認証局ユニーク識別子領域と主体者ユニーク識別子領域は、バージョン2で追加された領域であり、拡張領域はバージョン3で追加された領域である。拡張領域は、拡張型、重要／非重要区分、拡張領域値の3つ組の繰り返しである。この拡張型は基本的には自由に定義することができるため、拡張領域は様々な用途に用いることができ、現実的な有用性が高い。しかしながら、拡張型にはいくつかの標準拡張型が定義されており、鍵と方針情報、主体者と発行者属性などが含まれている。例えば、鍵と方針情報の拡張では鍵の利用に関する情報が記述でき、鍵の使用目的がデータ暗号なのか、鍵暗号なのか、電子署名なのか或いは証明書署名に使用できるのかなどが示せるようになっている。

主体者の身元確認情報である主体者同一性情報は、主体者名前領域に格納される。ここに記述される名前は、バージョン1および2ではX.500名前形式でなければならなかったが、バージョン3では他の形式でも許されるようになった。例えば、インターネットメールアドレスのnori@med.kyushu-u.ac.jpは、X.500名前形式では {Country=JP, Organization=Kyushu University, Organizational Unit=Med, Common

Name= Norihiro SAKAMOTO]と表される。従来どおり、主体者名前領域にはX.500名前を記入し、拡張領域にはインターネットメールアドレスを記入するなどの運用を行うことによってより多くの同一性情報を伝達することができる。

１．１１．　公開鍵証明書の運用

上述の様々な暗号方式、公開鍵証明書と認証局などの公開鍵基盤の技術要素をうまく利用すれば安全な情報交換は技術的には可能である。ただし、公開鍵基盤を現実の社会に広範囲に導入し、円滑に運用するためには法的な整備が必須である。また、公開鍵証明書のライフサイクルを理解し、それに合わせた証明書の利用が重要である。公開鍵証明書のライフサイクルはおおよそ以下の通りである。

- 公開鍵／私有鍵ペアの作成
- 公開鍵証明書の申請
- 公開鍵証明書の発行
- 公開鍵証明書の配布と利用
- 公開鍵証明書の廃棄
- 公開鍵証明書の有効期限終了

この内、公開鍵証明書の円滑な運用に重要なのは、証明書の配布と破棄である。

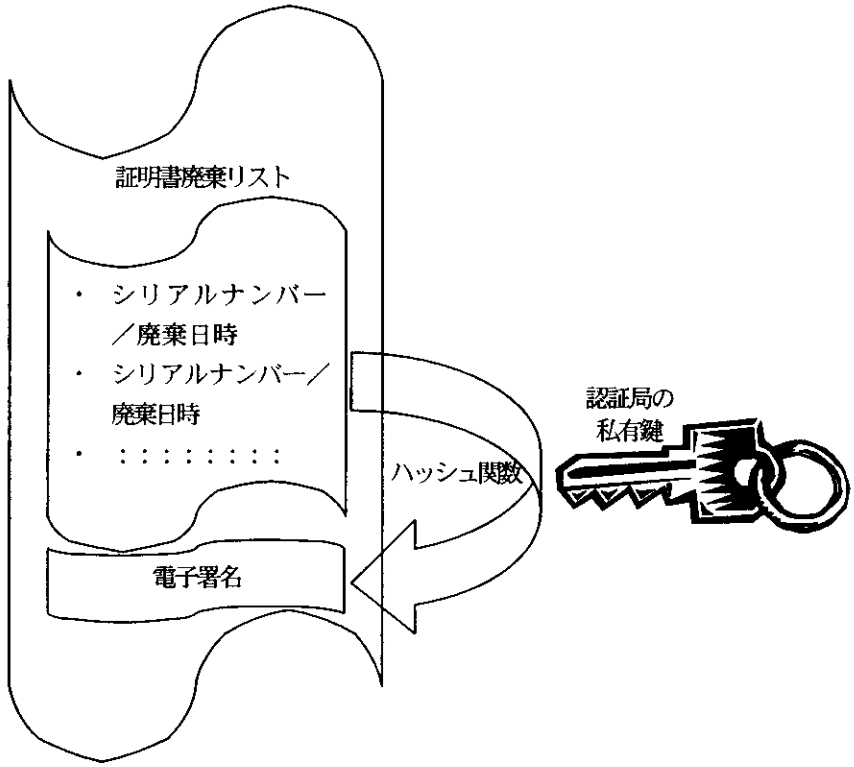
１．１２．　公開鍵証明書の配布

公開鍵証明書は主として、暗号化通信と電子署名に用いられる。電子署名を付したメッセージの送信に際しては、電子署名を確認するために必要な公開鍵証明書を同封し、配布するのが一般的である。電子署名を確認するために必要な公開鍵証明書とは、送信エンティティの公開鍵証明書と受信エンティティがその公開鍵証明書を検証するための証明書パスに存在する公開鍵証明書である。

暗号化通信を行う際には、送信エンティティは受信エンティティの公開鍵証明書をそのメールアドレスなどから検索し、取得する必要がある。この公開鍵証明書の検索を支援する技術がディレクトリサービスである。Microsoft Exchange Server、Lotus Directoryなどがディレクトリサービスの実用例であり、X.500標準プロトコルを用いて公開鍵証明書を配布する。一方最近ではX.500標準プロトコルを単純にしたLDAP(Lightweight Directory Access Protocol)がインターネット標準となり、OpenLDAPやNetscape LDAP Serverなどこれを利用した公開鍵証明書の配布も広まってきている。

１．１３．　公開鍵証明書の廃棄

様々な方法で配布された公開鍵証明書は配布先に留まり、あるいはコピーされて再配布されて利用される。公開鍵証明書には有効期限が記入されており、一般的にはその長さは1年から2年



であることが多い。公開鍵証明書を利用する際には、その有効期限を確かめ、有効期限外であればそれを信頼することはないが、有効期限内であれば検証されたと見なされる。しかしながら、勤務先を変わった場合や特定の資格を失った場合、あるいは私有鍵が盗まれた（外部に知られた）場合などは、現在の公開鍵証明書を廃棄し、利用できないようにする必要がある。ある公開鍵証明書が廃棄されたことを利用者に知らせる方法が、証明書廃棄リスト(CRL: Certificate Revocation List)である。証明書廃棄リストは、廃棄された公開鍵証明書の証明書シリアルナンバーと廃棄日時のペアの集合であり、公開鍵証明書と同じく、その発行認証局の電子署名が添えられる。

証明書廃棄リストは一般に公開鍵証明書の配布と同じくX.500標準ディレクトリサービスあるいはLDAPディレクトリサービスにより配布されることもあるが、特定のURL等に定期的に公開する方法もある。公開鍵証明書を利用する際は、発行者の確認、有効期限の確認と共に、最新の証明書廃棄リストを何らかの方法により取得し、その公開鍵証明書が廃棄されていないことも確認する必要がある。このようにして初めて公開鍵証明書がそのライフサイクルのどの段階にあるのかが確認され、安全に利用することが可能

となる。

2．　保健医療分野におけるPKI利用のトップユースケース分析

2．1．スコープ

ユースケース分析の一般的な手法に基づき、保健医療における電子署名付き文書交換に際しての、アクタ、トリガイベント、インタラクションを抽象的に同定する。従って、ここでは、個々のユースケースは扱わず、それぞれの一事例としてのみ挙げるに留める。また、ここで扱う電子署名はアプリケーションレベルでの署名であり、それより下層での電子署名やそれに類するデータ完全性のための署名はスコープ外である。同様に、PKIはデータの暗号化にも利用されるが、本分析では、データのコンフィデンシャリティはVPN等の汎用の手段で担保されることを前提として、スコープ外と考える。

2．2．アクタ

電子署名付き文書交換でのアクタとは、それ自身の責務においてある文書に署名し、発行できる役割を有する個人あるいはオブジェクトをいう。想定されるアクタは以下のとおりである。

医療受給者：患者、保護者、代理人、身元引受人、など

医療供給者：医師、歯科医師、看護婦、薬剤師、整骨医、など

機関：医療機関、保健所、厚生省、保険支払基金、保険会社、検査会社など

2．3．トリガイベント

2．3．1．医療受給者がトリガイベントを起こす

外来予約、入院承諾書、手術承諾書、カルテ開示要求

2．3．2．医療供給者がトリガイベントを起こす

診療情報提供書、診断書、処方箋、診断レポート、外注検査依頼

2．3．3．機関がトリガイベントを起こす

検査結果報告、診療報酬請求、各種届出、各種統計調査、診断書要求、保険資格確認

2．4．インタラクション

インタラクションは、インターネット上での情報交換という観点から、ステートレス（コネクションレス）とトランザクションに分類することができる。ステートレスのインタラクションでは、実質的にトリガイベントのみで、そのレスポンスは存在しない。トランザクション型のインタラクションでは、トリガイベントが発生するとそれに応じた一連の文書交換が発生する。

２．４．１．コネクションレス型

入院承諾書、手術承諾書、診療情報提供書、診断書、診断レポート、外注検査依頼、検査結果報告、各種届出

２．４．２．トランザクション型

外来予約、カルテ開示要求、処方箋、診療報酬請求、各種統計調査、診断書要求、保険資格確認

２．５．インタラクション

インタラクション中でそのサブインタラクションとして、電子署名に関する確認が必ず発生する。この電子署名の確認に際して、電子署名のみ確認すればよい場合（本人認証）とその属性を確認（属性認証）しなければならない場合とがあると考えられる。

２．５．１．本人認証のみ

外来予約、入院承諾書、手術承諾書、カルテ開示要求、外注検査依頼、診療報酬請求、各種届出、各種統計調査、診断書要求、保険資格確認

２．５．２．属性認証

診療情報提供書、診断書、処方箋、診断レポート

２．６．トップレベルユースケース

以上から、保健医療における電子署名付き文書交換のトップユースケースは大まかに以下の4種類に分類されると考えられる。

２．６．１．コネクションレス型-本人認証のユースケース

アクタは電子署名付き文書を発行する。

受信者は、その電子署名を確認し、本人認証を行う。

２．６．２．コネクションレス型-属性認証のユースケース

アクタは電子署名付き文書を発行する。

受信者は、その電子署名を確認し、本人認証を行う。

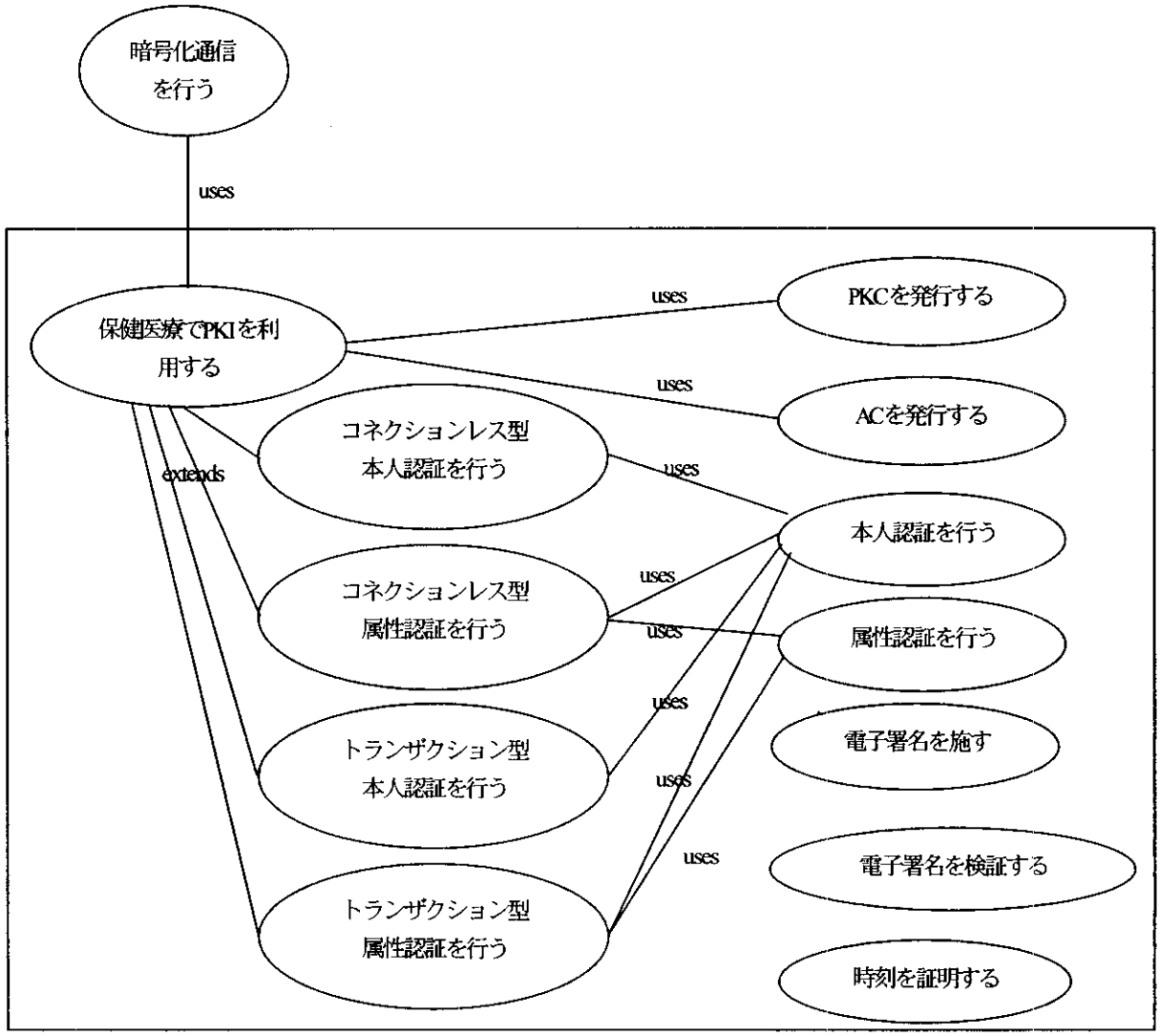
受信者は、送信者の属性認証を行う。

２．６．３．トランザクション型-本人認証のユースケース

アクタは電子署名付き文書を発行する。

受信者は、その電子署名を確認し、本人認証を行う。

受信者は、レスポンスに電子署名を付与し、送信者に返送する。



２．６．４．トランザクション型-属性認証のユースケース

アクタは電子署名付き文書を発行する。

受信者は、その電子署名を確認し、本人認証を行う。

受信者は、送信者の属性認証を行う。

受信者は、レスポンスに電子署名を付与し、送信者に返送する。

２．７．下位ユースケース

２．７．１．紹介状／診療情報提供書を交換する

２．７．２．保険証資格を審査する

２．７．３．レセ電算オンラインで行う

２．７．４．放射線画像を読影する

２．７．５．処方箋を発行する

２．８．紹介状／診療情報提供書を交換する

２．８．１．Open Issue

紹介状／診療情報提供書の送信に際しては、紹介先が特定できている場合と、特定できていない場合とでユースケースが異なると考えられる。しかしながら、患者が指定された医師（医療機関）以外に、その紹介状を持参することはありえるであろう。その際、その紹介状は有効であるのか？もし、それが有効であるとすれば、紹介状の交換も処方箋等と同じく、予め特定の医療機関に送信することはせず、紹介状サーバにプールしておき、患者が紹介先を受診して始めて、紹介状が届けられるようにするべきであろう。一方、患者が受診する前に伝えておきたい情報（受診予約など）もあるかもしれない。このような情報は紹介状以外であつかうべきか、否か？また、紹介状は患者自身が見ることが出来るべきか否か？

今後の研究にあたっては、上記の問題を明らかにする必要がある。

２．８．２．トリガイベント

患者が紹介元を受診する

患者が紹介先を受診する

２．８．３．ユースケース　紹介元が紹介状を送信する

紹介元が紹介状を作成する

紹介元が紹介状に電子署名を施す

紹介元が紹介状リファレンスを患者のICカードに保存する

紹介元が紹介状を紹介状サーバに送信する

２．８．４．ユースケース　紹介先が紹介状を取得する

紹介元が患者ICカードより紹介状リファレンスを取得する

紹介元が紹介状リファレンスと共に紹介状要求メッセージを紹介状サーバに送信する

紹介状サーバが紹介状要求メッセージと要求者の属性を検証する

紹介状サーバが紹介状を紹介先に送信する

２．９．保健医療PKIへのシステム要求

上記のユースケース分析により、保健医療PKIに関して、以下の要求が明らかになった。

２．９．１．通常のPKI要素に関して

PKCには医療国家資格を示すhcRoleが記入されていること

その他の資格（専門医、医師会員など）を授与する組織はその資格をACとして証明する

こと

各組織は所属する職員の職位、職階、役割などをACとして証明すること

上記に関して早急な用語の統一が必要

TSAサービスの提供

２．９．２．PKI以外の要素に関して

医療供給者はICカードを用いた電子署名ができること

医療受給者はICカードを有し、そこに発行された医療文書が格納できること

医療機関は医療文書を受け取るポストオフィスサーバを有すること

ポストオフィスサーバは、個人医師宛の紹介状等、および、あて先の特定されていない紹介状あるいは処方箋等を一時的に保管する

上記に関して、ポストオフィスサーバプロトコルの早急な策定が必要

３．HL7V3に基づく患者紹介状インタラクション分析

３．１．受診時のやりとり その1

Interaction 1: Get Clinical Document

EPR Client ---> EPR Database

カルテ問い合わせ

Message Type: Document Query Get Clinical Document

Interaction 2: Response to Get Clinical Document

EPR Database ---> EPR Client

カルテ問い合わせ応答

Message Type: Document Query Response to Get Clinical Document

Interaction 3: Get Patient Referral

EPR Client ---> Message Pool

電子紹介状問い合わせ

Message Type: Referral Query Get Patient Refferal

Interaction 4: Response to Get Patient Referral

Message Pool ---> EPR Client

電子紹介状問い合わせ結果

Message Type: Referral Query Response to Get Patient Refferal

Interaction 5: Active Lab Order Placer - Request Activate Lab Order, Closely-coupled

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

検査オーダー

Message Type: Lab Order, Closely-coupled

Interaction 6: Document Addendum Notification and Content

EPR Client ---> EPR Database

カルテ保存

Message Type: Document Header and Contents

３．２．受診時のやりとり その2

Interaction 7: Get Clinical Document

EPR Client ---> EPR Database

カルテ問い合わせ

Message Type: Document Query Get Clinical Document

Interaction 8: Response to Get Clinical Document

EPR Database ---> EPR Client

カルテ問い合わせ応答

Message Type: Document Query Response to Get Clinical Document

Interaction 9: Get Laboratory Results

EPR Client ---> Message Pool

検査結果問い合わせ

Message Type: Lab Query Get Laboratory Result

Interaction 10: 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 11: Document Addendum Notification and Content

EPR Client ---> EPR Database

カルテ保存

Message Type: Document Header and Contents

３．３．受診時のやりとり その3

Interaction 12: Get Clinical Document

EPR Client ---> EPR Database

カルテ問い合わせ

Message Type: Document Query Get Clinical Document

Interaction 13: Response to Get Clinical Document

EPR Database ---> EPR Client

カルテ問い合わせ応答

Message Type: Document Query Response to