総括研究報告概要

保健医療分野における電子署名の実用化に関する研究

主任研究者　坂本　憲広　　神戸大学大学院教授

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ているため、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非常に困難である。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　　大阪医科大学助教授
下川　俊彦　　九州産業大学助教授

A. 研究目的

本研究の目的は、署名もしくは記名、押印の必要な保健医療文書に対して、その電子化保健医療文書に電子署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。

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。
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。

C. 研究結果
1. 保健医療における電子署名の概念整理
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。
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。

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。
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、厚生労働省、社会保険支払基金、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。例：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。例：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。例：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。
2.5. 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。
2.5.1. 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。
2.5.2. 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。
2.5.3. 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。
2.5.4. 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。

3. 電子処方箋シナリオ
3.1. 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。
3.2. 処方システムはその処方に医師の電子署名を行う。
3.3. 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。
3.4. 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。
3.5. 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。
3.6. 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）
3.7. 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。
3.8. 患者は調剤薬局の薬剤師に処方箋引換え書を提出する。
3.9. 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。
3.10. 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。
3.11. 処方箋サーバは、その処方箋引換え番号を調剤中とする。
3.12. 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。
3.13. 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。
3.14. 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。
3.15. 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。
3.16. 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。
3.17. 薬剤師は調剤システムに調剤内容を入力する。
3.18. 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。
3.19. 処方箋サーバは、薬剤師の電子署名を検証する。
3.20. 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。

D. 考察
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、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。

E. 結論
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。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。
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。

G．発表
1．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
2．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