厚生労働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１４年度　総括研究報告書

主任研究者　坂本　憲広

平成１５（２００３）年４月

目　次

厚生労働科学研究費補助金（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

主任研究者　坂本　憲広　神戸大学医学部附属病院　教授

研究要旨

電子政府の実現に向けて個人認証は非常に重要な課題である。また、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。また、電子カルテの真正性を担保するためには、長期間に渡り有効な電子署名を電子カルテに付加する必要がある。既に医療訴訟において電子カルテが証拠能力を有しなかった事例が発生している。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。

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。本年度（平成 14 年度）は平成 13 年度の成果を活用し、医療施設間で実際に電子署名付きデータを交換する実証実験を行った。処方箋そのものについては、未だ法的に電子化することが認められていないため、今回の実証実験では処方情報、調剤情報、遺伝子情報、安全管理情報などを主体として行った。また、実際に電子署名付きデータを交換し、それをお互いに信頼するためには、各医療機関のセキュリティポリシおよび証明書ポリシの交換が必要である。そこで、本年度はこれらの実装も行った。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、山本が特にポリシ設計に関して、下川が主として実装上の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
　東京大学大学院情報学環　助教授
下川俊彦
　九州産業大学情報科学部　助教授

A. 研究目的

本研究の目的は、これからの電子政府に向けて、法的に署名もしくは記名、押印が要求されている診療録に対して、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。特に本年度はその実証実験を行い、実用化の可能性およびその際の問題点を明らかにすることを主たる研究目的としている。

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。他の分野で実用化され、あるいは実運用されている技術に関しては、安全性や問題点が既に明らかにされているものが多い。しかしながら、保健医療分野において独自に開発し、あるいは実用化しなければならない場合、その実用化に関する問題点は保健医療分野において明らかにしなければならない。そこで本研究では平成13年度に提案したプロトコルについて、本年度はその実証実験を行い、その実用性および安全性を明らかにするための研究を行う。

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

平成 13 年度は、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った。これは、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しているからである。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た。

本年度は、このユースケースおよびそれに基づいて作成したプロトコルモデルと元に、三菱社製の暗号化ライブラリ MistyCert を用いて、JAVA、Web でプロトタイプシステムを作成し、その実用性および安全性、コストなどについて評価する。

同時に、医療機関間での電子署名付き医療文書の交換に際して必要となる、セキュリティポリシ、認証局ポリシを開発し、また、個人認証を行うための IC カードについても調査を行う。

C．研究結果

1.電子署名付き医療文書交換システムのプロトタイプ実装

本年度は以下のプロトタイプシステムを開発し、神戸大学医学部附属病院の病院情報システムとの間で連携テストを行い、実証実験を行った。

本実証実験で開発または構築されたシステム、機能を以下に示す。

- LRA システム
- Sub CA システム
- 利用者認証機能
- アクセス権限管理機能
- 電子署名機能
- タイムスタンプ機能
- PKI 対応クライアントシステム

1.1. LRA（Local Registration Authority）システム

SubCA に対しシステム利用者を登録するシステムである。システムに登録される利用者のデータは XML 形式で保存されており、WEB アプリケーションから利用者の登

録、検索、更新などを行うことが可能である。

1.2. Sub CA システム

Sub CA、SSL 用 Root CA 等を構築した。

この Sub CA から、システム利用者に対して証明書が発行されている。証明書内には、利用者の氏名や国家資格、証明書の発行者などが記されている。

2.3. 利用者認証機能

各システムの利用者の認証にはSSL相互認証機能を使用した。

SSL 相互認証機能は、システム利用上の通信において、セキュリティを高めており、不正アクセス、盗聴、成りすまし、改竄などを防止するための方法である。

1.4. アクセス権限管理機能

本機能により、アクセス権限の管理、アクセスログ等の管理を行う。

階層型ＰＫＩ対応遺伝子情報システム、処方関連システム、リスクマネージメントシステムにおいて、利用者にアクセス権限を付与することで、データの登録や閲覧などの実行制限を加える。また利用者のアクセスに対し、履歴を保存、管理する。

1.5. 電子署名機能

電子署名機能はアプリケーションとして開発した。また、署名は XML 形式のデータに対して署名するため、W3C が規定した XML 署名の方法（URL：http://www.w3.org/TR/xmldsig-requirements）を使用した。

利用者がデータを作成し、システムに登録する際には、Sub CA の発行する証明書を用いた署名を行うようにした。また、登録されているデータの署名を検証することも行えるようにした。

電子署名および、その検証を用いることで、データ自体の真正性つまり、改竄などを防止することを可能とした。

1.6. タイムスタンプ機能

タイムスタンプ機能により、データを登録した時刻などを証明することが可能となる。

処方関連情報、遺伝子情報、リスクマネージメント情報などは、特にデータを登録した時刻が重要となるため、タイムスタンプをデータに付加して登録を行った。

データへのタイムスタンプの付加は署名と同時に行われる。

タイムスタンプは W3C の規定が無いため独自の方法で行った。

1.7. PKI 対応クライアントシステム

PKI 対応クライアントシステムには遺伝子情報システム、処方関連システム、リスクマネージメントシステムの 3 つから成る。

遺伝子情報システム及び処方関連システムはそれぞれ、遺伝子情報及び臨床情報の入力システムであり、入力データを格納・閲覧する機能である。データは XML 形式でサーバに保存される。サーバへの保存は、クライアント側でまずデータに署名を行い、その後 XML ファイルをアップロードする方法である。

リスクマネージメントシステムは臨床の現場で起こったアクシデントあるいはインシデントについてのレポートを入力するため

のシステムである。システムは WEB アプリケーションとして機能し、ブラウザ上でデータの入力、データから XML ファイルへの作成、データの格納、登録されたデータの閲覧を可能とする。

2. セキュリティポリシのテンプレート開発

情報セキュリティポリシ策定の目的は、情報システムを構築する期間が、その情報セキュリティに対する考え方や取り組みを明確にすることにある。従って、医療機関において電子署名付き医療文書を交換しようとする際には、この情報セキュリティポリシは必ず策定しなければならない。

本研究で開発した情報セキュリティポリシには、保健医療機関が保有する情報資産と、それを保護する理由を明示している。

本年度の研究では、情報セキュリティ基本方針、および個人情報保護基本方針についてそのテンプレートを開発し、実証実験において使用した。

3．証明書ポリシ、認証局実施規程のテンプレート開発

最近、保健医療分野においては認証局を階層化し、1 つあるいは少数の保健医療機関がルート認証局を運営し、その他の医療機関はそのサブ CA とする方向性が打ち出されている。そして、その際には、証明書ポリシはそれぞれのルート認証局の証明書ポリシを用い、その他のサブ CA はその証明書ポリシに従って、認証実施規程のみを独自に作成することとなっている。従って、今後は医療機関でこの認証実施規程を作成する必要が出てくる。当然、今回のプロトタイプを用いて実証実験においてもこの認証局実施規程が必要であり、本研究においてこれを開発した。

認証局実施規程(Certification Practice Statement)は、認証局が行う証明書発行、失効、及び証明書を基礎とする公開鍵基盤(PKI : Public Key Infrastructure)の運用維持に関する諸手続きおよび証明書発行、利用にかかわる主体の責任を記述したものである。認証局実施規程には、認証局で用いる、証明書所有者の私有鍵や証明書の格納媒体を指定する。また、認証局は、CA 証明書の発行を受けるルート認証局を明らかにし、その下位認証局として活動することを宣言する。認証局実施規程は、医療従事者用公開鍵証明書、患者・保健医療福祉サービス利用者用公開鍵証明書および医療機関・保健医療福祉サービス供給組織用公開鍵証明書を発行する「ヘルスケア PKI 認証局」証明書ポリシ(以下 CP という)に従い、認証局が発行するすべての証明書に適用される。ヘルスケア PKI とは、保健医療福祉分野において医療情報を地域で連携して利用するための PKI である。

認証局実施規程と証明書ポリシが抵触する場合には、証明書ポリシが優先する。

D．考察

平成 13 年度の研究成果では、保健医療分野において、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た。本年度はその成果の実用性、安全性を検証するために、プロトタイプシステムを開発し、その実証実験を行うことを目的

とした。しかしながら、実際に電子署名付き保健医療情報を作成し、それを交換しようとすると、それを利用する保健医療機関におけるセキュリティ環境整備が非常に大きな課題であることが判明した。これはなぜならば、如何に厳密なセキュリティ技術を応用して、安全なシステムを開発したとしても、それを利用する、あるいは運用する環境のセキュリティがおざなりであれば、結局は交換される保健医療情報の信頼性が低下するからである。

こうした観点から、本研究では、保健医療機関における情報セキュリティポリシのテンプレート、および認証実施規程のテンプレートを開発した。これらの規程類はまだまだ不完全で十分なものではないが、作成には非常に大きな労力を要した。今後、これらの規程類を各保健医療期間で制定しなければならないとすると、そのコストは大変大きいとされると考えられる。

しかしながら、本研究の成果を次年度以降利用することにより、それらのコストを下げながら、確実に電子署名を用いた安全な情報交換が実現できる環境整備が可能であると考えられる。

E．結論

平成 14 年度の研究は、平成 13 年度に行った基礎的な事項の調査研究の成果の実用性、安全性を検証することが目的であった。

そのため、昨年度提案したユースケース、およびプロトコルに基づくプロトタイプシステムを開発し、その実証実験を行い、昨年度の提案が妥当であったことを証明した。同時に、実際に医療機関において、電子署名付き保健医療文書を作成し、交換するために必要となる、セキュリティ環境、すなわち、情報セキュリティポリシと認証局実施規程についてそのテンプレートを作成した。

以上の研究結果を基に、来年度はより詳細な実用化研究とその検証を行うと共に、情報セキュリティポリシテンプレート、認証局実施規程テンプレートなど、これから各保健医療期間で必要となるリソースについて更に整備を行い、それらを公開できるようにする予定である。

F．健康危険情報

なし。

G．研究発表

1．論文発表

なし。

2．学会発表

なし。

H．知的財産権の出願・登録状況

1．特許取得

なし。

2．実用新案登録

なし。

3．その他

なし。

厚生労働科学研究費補助金（医療技術評価総合研究事業）
分担研究報告書

電子署名付き医療文書交換システムのプロトタイプ実装に関する研究

主任研究者　坂本　憲広　神戸大学医学部附属病院　教授

研究要旨

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。本年度（平成 14 年度）は平成 13 年度の成果を活用し、医療施設間で実際に電子署名付きデータを交換する実証実験を行った。処方箋そのものについては、未だ法的に電子化することが認められていないため、今回の実証実験では処方情報、調剤情報、遺伝子情報、安全管理情報などを主体として行った。

実験は神戸大学病院を中心として行い、その実運用されている病院情報システムとも連携を取る形で行った。保健医療文書に電子署名を付け、それを管理、交換し、署名を検証することは、確実に行えることを実証し、昨年度提案したユースケース、およびプロトコルが妥当であったことを証明した。一方で、電子署名を大規模な保健医療機関や広域環境で利用する場合には、証明書利用者の管理、認証局の管理、私有鍵の管理など、運用上の問題が様々あることが明らかになった。また、長期に保存しなくてはならない保健医療文書の場合、電子署名の有効期間とその検証に関して、まだ解決すべき問題があることも指摘した。

分担研究者：
山本隆一
　東京大学大学院情報学環　助教授
下川俊彦
　九州産業大学情報科学部　助教授

A. 研究目的

本研究の目的は、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。他の分野で実用化され、あるいは実運用されている技術に関しては、安全性や問題点が既に明らかにされているものが多い。しかしながら、保健医療分野において独自に開発し、あるいは実用化しなければならない場合、その実用

化に関する問題点は保健医療分野において明らかにしなければならない。そこで本研究では平成 13 年度に提案したプロトコルについて、その実証実験を行い、その実用性および安全性を明らかにするための研究を行う。

広域分散化した利用者を効率的に管理し、セキュリティ保護レベルを高め、情報への厳密なアクセスコントロールを実現し、証拠性の高い監査ログを記録する包括的な方法としては、公開鍵基盤技術（PKI：Public Key Infrastructure）がもっとも有効であると考えられる。これまで、いくつかの保健医療機関において公開鍵基盤技術を利用したシステムが用いられている。しかしながら、これらのシステムは single CA（Certificate Authority）構成であり、他の保険医療機関と連携するための階層型等の multiple CA 構成には対応していない。つまり、今後他の保健医療機関と連携し、運営していくためには独自のポリシを用いて運営していくのではなく、multiple CA 構成の中で CA を構築し、運営していくことが他との連携に対して有効であると考える。

本研究の目的は、平成 13 年度に提案したユースケースおよびプロトコルに基づいて、階層型 CA を利用した組織間の相互認証、電子署名、及びその検証を可能とするプロトタイプシステムを研究することである。本研究では神戸大学医学部附属病院をモデル機関として、その病院情報システムを一部利用しながら、1,000 人を超える職員に対してシステム利用者管理を行い、署名の必要な医療文書の電子化に際して電子署名を行えるようにする。

本研究では、プロトタイプシステムの開発、運用を通じて、公開鍵証明書を用いれば、大規模なシステム利用者管理を効率的に行えること、また、階層型 PKI を利用すれば異なる実装の CA の相互運用が実用的に行われること、そして保健医療 PKI の公開鍵証明書を用いれば厳密な電子署名付き保健医療文書の交換が可能なことを実証する。

B．研究方法

本研究では、昨年度作成したユースケースおよびそれに基づいて作成したプロトコルモデルと元に、三菱社製の暗号化ライブラリ MistyCert を用いて、JAVA、Web でプロトタイプシステムを作成し、その実用性および安全性、コストなどについて評価する。

実証実験は神戸大学病院の実際の病院情報システムと連携して行う。実証実験を行うに先立ち、実証実験実施場所となる神戸大学医学部付属病院に各システムの構築ならびに各環境の設定を行う。まずは、実験対象の利用者に対して、CP・CPS に基づいた hcRole に定められた職種に対してその資格の確認を行い、IC カード発行の妥当性を確認し、必要書類のファイリング等を行った後、発行管理データベースへの登録及び IC カード発行の作業を行う。

さらに、署名用証明書発行用 SubCA、SSL クライアント証明書発行用 SubCA、SSL クライアント証明書発行 SubCA 用 RootCA を構築した。また、ＬＲＡシステム機能システムの利用者管理システム用サーバと PKI 対応 Web アプリケーション用サーバに対し、利用者認証機能の設定を行う。次に、LRA システム機能システムの利用者管理システム用サーバと PKI 対応 Web アプリ

ケーション用サーバに対し、アクセス権限管理機能の設定を行う。また、PKI 対応 Web アプリケーション用に接続し、電子署名を行うクライアントマシンに XML 署名ツール、IC カードリーダ、Netscape Navigator の設定を行う。

最後に、神戸大学医学部附属病院 SubCA が発行した証明書を使用し、各 Web アプリケーションで作成した XML データに署名を行う。署名に際しては、各 XML スキーマに則り作成した XML データに対し署名を行い、登録の実験を行う。

C．研究結果

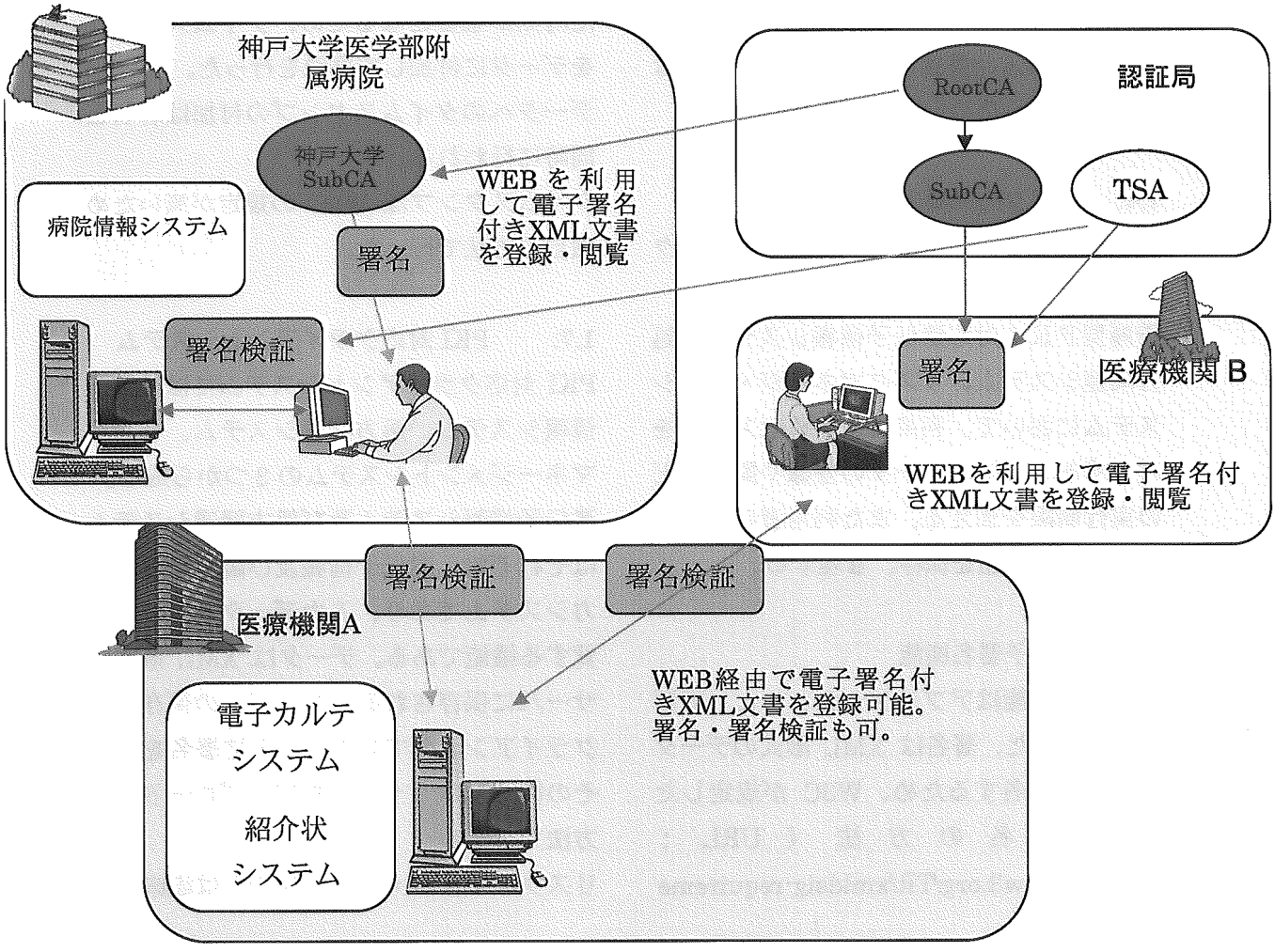
本年度は以下のプロトタイプシステムを開発し、神戸大学医学部附属病院の病院情報システムとの間で連携テストを行い、実証実験を行った。

本実証実験で開発または構築されたシステム、機能を以下に示す。

- LRA システム
- Sub CA システム
- 利用者認証機能
- アクセス権限管理機能
- 電子署名機能
- タイムスタンプ機能
- PKI 対応クライアントシステム

1.1. LRA（Local Registration Authority）システム

SubCA に対しシステム利用者を登録するシステムである。システムに登録される利



用者のデータは XML 形式で保存されており、WEB アプリケーションから利用者の登録、検索、更新などを行うことが可能である。

1.2. Sub CA システム

Sub CA、SSL 用 Root CA 等を構築した。

この Sub CA から、システム利用者に対して証明書が発行されている。証明書内には、利用者の氏名や国家資格、証明書の発行者などが記されている。

2.3. 利用者認証機能

各システムの利用者の認証にはSSL相互認証機能を使用した。

SSL 相互認証機能は、システム利用上の通信において、セキュリティを高めており、不正アクセス、盗聴、成りすまし、改竄などを防止するための方法である。

1.4. アクセス権限管理機能

本機能により、アクセス権限の管理、アクセスログ等の管理を行う。

階層型ＰＫＩ対応遺伝子情報システム、処方関連システム、リスクマネージメントシステムにおいて、利用者にアクセス権限を付与することで、データの登録や閲覧などの実行制限を加える。また利用者のアクセスに対し、履歴を保存、管理する。

1.5. 電子署名機能

電子署名機能はアプリケーションとして開発した。また、署名は XML 形式のデータに対して署名するため、W3C が規定した XML 署名の方法（URL：http://www.w3.org/TR/xmldsig-requirements）を使用した。

利用者がデータを作成し、システムに登録する際には、Sub CA の発行する証明書を用いた署名を行うようにした。また、登録されているデータの署名を検証することも行えるようにした。

電子署名および、その検証を用いることで、データ自体の真正性つまり、改竄などを防止することを可能とした。

1.6. タイムスタンプ機能

タイムスタンプ機能により、データを登録した時刻などを証明することが可能となる。

処方関連情報、遺伝子情報、リスクマネージメント情報などは、特にデータを登録した時刻が重要となるため、タイムスタンプをデータに付加して登録を行った。

データへのタイムスタンプの付加は署名と同時に行われる。

タイムスタンプは W3C の規定が無いため独自の方法で行った。

1.7. PKI 対応クライアントシステム

PKI 対応クライアントシステムには遺伝子情報システム、処方関連システム、リスクマネージメントシステムの 3 つから成る。

遺伝子情報システム及び処方関連システムはそれぞれ、遺伝子情報及び臨床情報の入力システムであり、入力データを格納・閲覧する機能である。データは XML 形式でサーバに保存される。サーバへの保存は、クライアント側でまずデータに署名を行い、その後 XML ファイルをアップロードする方法である。

リスクマネージメントシステムは臨床の現

場で起こったアクシデントあるいはインシデントについてのレポートを入力するためのシステムである。システムは WEB アプリケーションとして機能し、ブラウザ上でデータの入力、データから XML ファイルへの作成、データの格納、登録されたデータの閲覧を可能とする。

上記のシステム環境において、神戸大学医学部附属病院 SubCA より発行された証明書を使用し、各保健医療文書への XML 署名はすべて成功した。

次に、署名した電子署名の検証を行った。検証には RootCA の公開鍵証明書、CRL と神戸大学医学部附属病院 SubCA 公開鍵証明書、CRL と SubCA 公開鍵証明書、CRL を使用し検証を行った。

また、CRL の情報が正常に使用されているか確認するため、検証には CRL を用いる場合と用いない場合の２パターンで検証を行った。ルート CA の公開鍵証明書、CRL と神戸大学医学部附属病院 SubCA 公開鍵証明書、CRL と SubCA 公開鍵証明書、CRL を使用し検証を行った結果、検証は正常に行えた。ルート CA の公開鍵証明書と神戸大学医学部附属病院 SubCA 公開鍵証明書と SubCA 公開鍵証明書を使用し検証を行った結果、検証は正常に行えた。

さらに、神戸大学医学部附属病院 SubCA 発行の証明書を使用した署名に対し、タイムスタンプの付加を行ったところ、正常にタイムスタンプの付加は行えた。

次に、XPath 入りの署名付き XML 文書例を示す。

```
<?xml version="1.0" encoding="UTF-8"?>
<incident>
  <doc>
      タガメット　1錠　朝　28日分
  </doc>
<Signature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
    <CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference URI="">
      <Transforms>
        <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <Transform
Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">

<XPath>ancestor-or-self::doc</XPath>
        </Transform>
      </Transforms>
      <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>[ダイジェスト値]</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>[署名値]</SignatureValue>

  <KeyInfo>
    <X509Data>
      <X509Certificate>[公開鍵証明
```

書]</X509Certificate>
</KeyInfo></Signature></incident>

異なるＣＡの発行した証明書の相互運用性

本実証実験では神戸大学医学部付属病院内SubCAが発行した証明書と他のSubCAが発行した証明書を使用し、署名、検証の試験を行った。

処理時間に関して述べると、神戸大学医学部附属病院内のSubCAで発行された証明書を用いた署名は15秒要し、検証にも15秒要した。この時の検証に要する処理時間は、異なるCAの発行した証明書による署名データの検証の場合とほぼ同じ処理時間であった。

D．考察

本実験では、利用者に対して公開鍵証明書を発行するが、そのときに私有鍵をどのようにして安全に管理するかが重要である。

本実験では、ICカードに私有鍵を保管することとしたが、これは非常に有効な方法だと考えられる。例えば私有鍵をサーバなどの端末内に保管することと比較すると、端末から離れる場合にでも携帯することが可能であるので、他人に盗まれ、解読される可能性が減る。そして、ディスク故障などによって誤って私有鍵を消去することがなくなる。またICカードリーダライタがあればどの端末からでも容易に利用することが可能となる。

また私有鍵をハードウェアトークンに保存することは外部に私有鍵を取り出すことが不可能であるため、他人に私有鍵を盗まれる心配がほとんど無い。

問題点としては処理能力が低いため、頻繁に使用する場合には不向きかもしれない。しかし、PCカード型のハードウェアセキュリティモジュール（HSM）などに比べればコスト的に安価に入手が可能という利点がある。もう1つは、ICカードが軽く、小さなものであるという見た目のために、利用者に対するICカードの大切さということが伝わりづらいと考えられる。

今後の課題として、ICカードを家などに忘れてきたために、システムの利用が出来なくなる場合が生じると考えられる。その時の対応策を考えていくことが必要である。

また、看護師、研修医などの場合はWebアプリケーションなどのシステムの使用は勤務と同時に必要となるが、証明書の発行時には免許の交付がまだされていない場合も多い。

これではCPに則った正規の証明書を発行してしまうと、hcRoleが無いため必要であるシステムの使用ができなくなってしまう。免許の交付後に証明書の再発行は、古い証明書の失効により即行えるが、免許の交付が勤務開始後、約一ヵ月後という場合もあり、回避策が必要である。

現在、もっとも容易に行える方法としては免許交付時には仮の証明書を発行（hcRoleもあり）し、免許交付後に正規の証明書を再発行する方法である。しかし、この方法ではCNに免許番号が付加される為、再発行前の証明書からの更新では無く、新規発行となる。他の方法としては、アクセス制限などに資格情報を使用する時は、資格情報などの変更を行いやすい属性証明書の使用も考える必要もあるのではないかと考える。ただし、現在のところ属性証明書を使

用できる製品が少なく、属性証明書を利用したシステムの構築は難しいのではないかとも考える。

本実証実験では証明書を IC カードに格納し、証明書保有者が管理する方法を取ったが、実際の運用時にはICカードを自宅に置き忘れたなどの事態が発生する可能性は非常に高い。このような場合、システムを使用ができなくなり診療行為などに悪影響が出てしまう。かといって、証明書の危殆化が起こったわけではなく、証明書を失効し、再発行を行うのも良い方法であるとはいえない。よって、一時的な証明書の発行機能というのが必要になってくるのではないかと思う。しかし、一時的に発行できる証明書は認証用のみとし、署名用の一時的発行は行わないのが基本となる。

本実証実験で作成したシステムのエンドエンティティが使用する認証用証明書はSSL相互認証に使用するため、署名用の証明書のように一定期間検証可能な署名を作成しないので、有効期限が非常に短い認証用証明書（本システムではSSLクライアント証明書）を作成することができる。有効期限を短くすることで、一時的に発行した認証用証明書が悪用されることを防ぎ、またCRLの肥大化を防ぐことも可能である。

ただし、SSL相互認証時にSSLサーバ側でクライアントの公開鍵証明書の情報をログに残し、アクセスの記録を残す場合には一時的に発行されている証明書が誰に対して発行されているか記録が必要になってくる。しかし、公開鍵証明書の情報でのログ管理では私有鍵を使用した署名値では無いためアクセス否認防止には使用できない。

保健医療分野では長期間にわたる検証が必要なシステムがある。一般に、CAが発行するエンドエンティティ証明書は3年の有効期限であるが、署名後3年経た後にも検証が可能である必要がある。医療訴訟などは過去に報告されていた情報が改ざんされていないか検証することが重要となってくるからである。

また、電子カルテシステムにPKI技術を組み込む場合、慢性疾患のカルテは RootCAの公開鍵証明書の有効期間よりも長期間に渡り使用されることもある。しかし、HPKIに限らずPKIシステムは長期間にわたる検証が行いにくく、新たな検証システムの構築が必要である。

異なるＣＡの発行した証明書の相互運用性

本実証実験では神戸大学医学部付属病院内SubCAが発行した証明書と他のSubCAが発行した証明書を使用し、署名、検証の試験を行った。

結論として、異なる CA の発行した証明書の相互運用は可能であり、処理時間に関しても実用的に問題ないと考えられる。ただ今後の課題として、上述のように検証が正常に行われなかった問題を克服するため、W3Cで規定されているXML署名の方式を用いたとしても、XML署名ライブラリにおける実装レベルに差を生じないような規定を作成する必要があると考えられる。例えば今回の実証実験での例を挙げるならばXML 内の署名対象の指定方法について差異が生じないよう規定を設けることである。さらに、長期間の検証を可能にする方法を検討する必要がある。

本実証実験で長期間の検証に必要な公開鍵証明書のリポジトリはRootCA、SubCAの

公開鍵証明書である。エンドエンティティの公開鍵証明書は XML 署名時に X509Certificate タグ内に格納されるためリポジトリに残しておく必要は無いと考えられる。

長期間経てからの検証時には、XML 署名が行われた時点での RootCA、SubCA の公開鍵証明書をリポジトリより取得し、検証を行うことにより XML データの改ざん判定は可能である。また、検証を行う時は署名が行われた時間での検証を行わないと公開鍵証明書に記述されている有効期間から外れているため、検証に失敗してしまう。

検証を行った時間は本実証実験の場合、タイムスタンプトークンより取得可能であった。

次に検証時には証明書失効リスト（CRL）を用いる必要がある問題である。検証時には各 CA が発行した CRL も使用しなければ、私有鍵が漏洩した時の第三者による署名の偽造を判別できない。しかし、公開鍵証明書内に記述されている有効期限が切れている場合、最新の CRL には有効期限外の失効情報は記述されておらず最新の CRL を使用したのでは公開鍵証明書が失効しているかの判別は不可能である。

また、有効期限内であっても、私有鍵漏洩前の正当な署名であるか、私有鍵漏洩後の不正な署名であるかは署名から時間が経過しているため、最新の CRL を使用しなければ判別できない。よってタイムスタンプトークンより取得した署名時間の時点での最新の CRL を取得し検証を行う必要がある。これ行うには発行されたすべての CRL のリポジトリも必要となり、発行パターンによっては膨大な量になりうるため、ベース CRL とデルタ CRL を使用する仕組みが適当かと考えられる。

ただし、上記の方法での CRL を用いた検証ではエンドエンティティが私有鍵の漏洩を認識してから証明書の破棄を申請し CRL が発行されるため、私有鍵の漏洩から最新の CRL にエンドエンティティの証明書のシリアルナンバーが記載されるまでにはタイムラグができる。これにより私有鍵漏洩から最新 CRL の発行までに間に第三者による不正な署名は判断できなくなってしまう。

この方法では署名時刻を署名データ内に付加されたタイムスタンプトークンより取得するため、タイムスタンプトークンより取得できる時刻の正当性のチェックも重要となる。本実証実験での現行の本システムの検証機能でも信頼する RootCA の公開鍵証明書を用いタイムスタンプトークンの検証を行っているため、タイムスタンプトークンの正当性のチェックには問題はない。また過去の署名データを検証するときも証明書リポジトリより署名時の RootCA の公開鍵証明書を取得しタイムスタンプトークンの検証を行う事により署名時間の正当性は確保できると考えている。

E．結論

平成 14 年度の研究は、平成 13 年度に行った基礎的な事項の調査研究の成果の実用性、安全性を検証することが目的であった。

そのため、本研究では、昨年度提案したユースケース、およびプロトコルに基づくプロトタイプシステムを開発し、その実証実験を行い、昨年度の提案が妥当であったこ

とを証明した。
同時に、電子署名を大規模な保健医療機関や広域環境で利用する場合には、証明書利用者の管理、認証局の管理、私有鍵の管理など、運用上の問題が様々あることが明らかになった。
また、長期に保存しなくてはならない保健医療文書の場合、電子署名の有効期間とその検証に関して、まだ解決すべき問題があることも指摘した。
以上の研究結果を基に、来年度はより詳細な実用化研究とその検証を行い、署名ライブラリ、署名検証ライブラリなどはフリーソフトとして公開できるようにする予定である。

F．健康危険情報

なし。

G．研究発表

1．論文発表

なし。

2．学会発表

なし。

H．知的財産権の出願・登録状況

1．特許取得

なし。

2．実用新案登録

なし。

3．その他

なし。

厚生労働科学研究費補助金（医療技術評価総合研究事業）
分担研究報告書

情報セキュリティポリシ、認証局実施規程に関する研究

主任研究者　坂本　憲広　神戸大学医学部附属病院　教授

研究要旨

本研究においては、電子署名を保健医療分野において実際に活用する際に必要となる、セキュリティに関する規程類を調査、研究し、そのテンプレートを作成することである。われわれの研究では、昨年度に電子署名付き保健医療文書を作成し、交換するためのモデルやプロトコルを研究開発した。さらに、本年度はその実用性を検証するための、実証実験を行っている。これらはあくまで研究あるいは実験レベルであり、実際の運用に際しては、さまざまな運用手順書や規程類が必要となる。これらの規程類がなければ、一般の医療機関において、電子署名を正しく、安全に活用することはできない。

そこで、本研究では、これらの規程類を開発し、今後保健医療機関で電子署名を活用する際の一助となるようにすると共に、今年度の実証実験においてもこれらの規程類に基づいて検証が行えるようにする。

分担研究者：
山本隆一
　東京大学大学院情報学環　助教授
下川俊彦
　九州産業大学情報科学部　助教授

A. 研究目的

本研究の目的は、電子署名を保健医療分野において実際に活用する際に必要となる、セキュリティに関する規程類を調査、研究し、そのテンプレートを作成することである。

われわれの研究では、昨年度に電子署名付き保健医療文書を作成し、交換するためのモデルやプロトコルを研究開発した。さらに、本年度はその実用性を検証するための、実証実験を行っている。これらはあくまで研究あるいは実験レベルであり、実際の運用に際しては、さまざまな運用手順書や規程類が必要となる。これらの規程類がなければ、一般の医療機関において、電子署名を正しく、安全に活用することはできない。

そこで、本研究では、これらの規程類を開発し、今後保健医療機関で電子署名を活用する際の一助となるようにすると共に、今年度の実証実験においてもこれらの規程類に基づいて検証が行えるようにする。

B．研究方法

本研究では、セキュリティに関する規程類の内、特に基本となる、情報セキュリティポリシ、プライバシポリシと、認証局を実際に運用するために必要となる認証局実施規定を対象として研究を執り行う。

C．研究結果

1．情報セキュリティポリシ

情報セキュリティポリシに関しては、下記の項目についてテンプレートを作成した。下記にそのテンプレートの概要を示すと共に、その一部は添付資料１に示す。

1.1 情報セキュリティ基本方針

1.1.1 情報セキュリティの定義と基本方針策定の目的

保健医療機関 XXX（以下「XXX」と称する）においては、個人の機微な情報を含むデータベースが、施設の内外のネットワークに接続されたコンピュータシステムにより運営されている。XXX 内部でのリスク対策を確実に行うことで、医療従事者が自らの業務を継続することはもとより、医療受給者が安心して診療、研究を任せられる環境を提供するために「情報セキュリティ基本方針」を定める。

本情報セキュリティ基本方針は、XXX 建屋内にある、保健医療情報データベースや仕様書等の情報資産、業務ソフトウエア等のソフトウエア資産、コンピュータ機器やネットワーク機器等の物理的資産、電源・空調等のサービスを適用範囲とする。

1.1.2 情報セキュリティの目標

XXX では、外部からの利用者を含めそこで働く人々の取り扱う、保健医療情報が、不当に暴露されたり、内容を改竄されたり、処理を妨害されたりしないようにすることを目標とし、必要な管理策をとる。また、保健医療情報のような個人情報の利活用には、提供者のインフォームドコンセントによる意向が反映されることを目標とする。

1.2. 適用範囲

1.3. 情報セキュリティ標準(第二文書)

1.3.1. サーバ対策

1.3.1.1. ユーザ認証標準

本標準は、情報を守る為に使用されるユーザ認証に関して、セキュリティを確保しつつ利便性を実現する運用を目的として記述されている。ユーザ認証に用いられるパスワードの長さや文字の種別、更新頻度、対象機器については、実現方法に関する技術の進歩が著しいので、技術動向を見極めた上で、本標準が適宜更新されることが望ましい。

当保健医療機関ではICカードを利用したユーザ認証/アクセス制御を行うことをベースとしている。ICカードの利用/運用標準に関しては別途『ＸＸＸＸＸ標準』にて定義する。

1.3.1.2. アカウント管理標準

アカウントは、当センターを利用する利用者にのみ発行され、必要最小限の権限が与えられていなければならない。また、現実の組織運営においては、組織変更や人員異動などが頻繁に行われることが少なくないので、変化に追従しながらもセキュリティを保つ為に、本標準を遵守しなければならない。 当保健医療機関では IC カードを利

用したユーザ認証/アクセス制御を行うことを基本としている。IC カードの利用/運用標準に関しては別途『ＸＸＸＸＸ標準』にて定義する。

1.3.1.3.　外部公開サーバに関する標準

本標準は、当保健医療機関がシステムをインターネットに接続する場合に、ネットワーク犯罪の被害者や加害者、あるいは踏み台になることなく、円滑かつ効率的なビジネスを継続することを趣旨としている。

インターネットへの接続は、当保健医療機関の業務効率の向上をもたらす反面、インターネット上の脅威にさらされる可能性もある。そのためインターネットへの接続にあたっては接続そのものの企画から、管理、運用まで慎重に行わなければならない。当センターは、外部へ公開する情報、情報システムに関して、セキュリティレベルの維持、向上、管理を趣旨として、以下の外部公開サーバに関する標準を実施する。

1.3.1.4.　サーバ等に関する標準

本標準は各サーバの OS を含めたソフト、ハード、及び、運用の規定をし、サーバに格納されている情報の保護を目的とする

1.3.1.5.　ソフトウェア・ハードウェアの購入及び導入標準

本標準は、当保健医療機関の業務で使用するソフトウェア／ハードウェアの標準製品を定めて運用管理することにより、センター内において統一されたセキュリティ対策の実現を容易にし、管理の効率化を図り、導入時の設定ミス等を防止することを目的とする。

1.3.2.　クライアント対策

1.3.2.1.　電子メール利用標準

本標準は、当保健医療機関内の電子メールサーバを使用して電子メールで受け渡される情報の安全性を確保し、電子メール利用にあたって発生し得る各種の問題を未然に防ぐことを目的とする。

1.3.2.2.　Web サービス利用標準

本標準は、Web ブラウザを使用し、当保健医療機関内及び保健医療機関外のサイトを利用するにあたって発生し得る各種の問題を未然に防ぐことを目的とする。

1.3.2.3.　クライアント PC 等におけるセキュリティ対策標準

本標準は、クライアント PC 上の機密性・完全性を確保し、発生し得る各種問題を未然に防ぐことを目的とする。

1.3.2.4.　ウィルス対策標準

本標準は、ウィルス等不正ソフトウェアによって引き起こされる情報漏えいやシステム破壊の被害を未然に防ぐことを目的とする。

1.3.3.　ネットワーク対策

1.3.3.1.　ネットワーク構築標準

本標準は、当保健医療機関のネットワーク構築をする際に必要なセキュリティに関して記載するもので、インターネット接続環境、保健医療機関内ＬＡＮ環境、保健医療機関内ＷＡＮ環境においてネットワーク機器及び各種サーバの構築の条件、及び運用・管理の実施方法の遵守事項を規定する。