20031106

厚生労働科学研究費補助金

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１５年度　総括研究報告書

主任研究者　坂本　憲広

平成１６（２００４）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）
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、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。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。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り、これらの実装も行った。平成 15 年度は、平成 14 年度の実証実験の成果を受け、より汎用的に活用可能な署名・検証ライブラリの開発を行った。さらに、現在、神戸大学医学部附属病院にて進められている HL7v3 対応電子カルテシステムにこの署名・検証ライブラリを組み入れるため、HL7v3 ライブラリを用いた実証システムを構築した。この実証システムにより、署名・検証ライブラリの有効性を確認し、実際の電子カルテシステムにおける電子署名あり方について明確なモデルを作成した。

分担研究者：
山本隆一
　東京大学大学院情報学環　助教授
石戸是亘
　財団法人先端医療振興財団　研究員

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。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。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、平成14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った。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。平成15年度は、前年度までの実績を実際のシステムに応用し、その有効性の検証及び課題の抽出を行った。

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。PKIの利用目的は、主として暗号化通信による盗聴・改ざんの防止と電子署名による情報源の確認である。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。
平成14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CertMisty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した。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、情報セキュリティポリシ、プライバシポリシ、認証局実施規程を開発し、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った。平成15年度は、まず、代表的な医療情報システムについてモデルシステムを検討し、電子署名が必要とされる場面、用途について整理を行った。次にその結果を踏まえ、前年度JAVAにて開発したプロトタイプを元に、より汎用性のあるライブラリの開発を行った。開発言語は、Windows端末との親和性、豊富なXML関連ライブラリという観点から、.NET C#を選択した。ま

た、開発したライブラリを中心に、HL7v3メッセージへの電子署名サービスシステムを構築し、別途研究を進めているHL7v3に対応した薬剤部門システム等と連携させ、その有効性を検証した。

C．研究結果

1．研究結果概要

平成14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、機能は以下の通りである。(1)LRAシステム、(2)Sub CAシステム、(3)利用者認証機能、(4)アクセス権限管理機能、(5)電子署名機能、(6)タイムスタンプ機能、(7)PKI対応クライアントシステム
さらに、情報セキュリティポリシのテンプレート開発を行った。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。

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。さらに、証明書ポリシ、認証局実施規程のテンプレート開発を行った。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。

本研究で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機関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。

今年度の研究結果としては、XML 電子署名ライブラリの C#での実装及び、HL7v3 メッセージへの電子署名システムの実装を行った。XML 電子署名ライブラリは、enveloping 型、enveloped 型に対応しており、スマートカードに格納された秘密鍵により署名される。CSP（Cryptographic Service Provider）ライブラリを持つ PKI 対応のスマートカードであれば、基本的に今回開発したライブラリで対応することができる。このライブラリを用いて開発したアプリケーションであれば、異なるスマートカードであっても CSP の指定を変えるだけで利用可能である。

また、このライブラリを元にした HL7v3 メッセージへの電子署名システムを、マイクロソフトの XML WEB サービスとして実装を行った。

これらの平成 15 年度の研究について、システムモデル、XML 電子署名クラスライブラリ、署名・検証 XML WEB サービス、実証システムといった４つの項目に分けて説明する。

2 システムモデル

開発を進めるに当たり、代表的な医療情報システムの処理手順について整理し、電子署名がどのような場面で、どのように利用され得るのか想定した。代表的な医療情報システムとしては、紹介状システム、検査システム、処方箋システムとした。

2.1 紹介状システム

紹介状システムの処理手順として、紹介状のサーバへの登録におけるシーケンス（2.1.2 紹介状登録）、サーバに登録された紹介状を処理するシーケンス（2.1.3 紹介状処理）に分けて整理を行った。

2.1.1 語句定義

紹介状システム処理手順において、図 2.1.2 紹介状システム登録シーケンス、図 2.1.3 紹介状システム処理シーケンス内で使用した語句は、以下のような意味を持つものとする。

・診療所医師
　紹介状を作成する医師。
・専門医
　紹介状を受理し、その患者を治療する医師。
・紹介状クライアント
　診療所医師による紹介状の作成、紹介状管理サーバへの登録、また専門医による紹介状の受理を行うクライアントアプリケーション。
・署名・検証モジュール
　電子署名を作成、検証する機能を提供するライブラリ。このモデルでは、紹介状登録クライアントに組み込まれていると想定。
・紹介状管理サーバ
　診療所医師等からの紹介状を受診し、保存・管理するサーバ。
・署名・検証サーバ
　電子署名の作成及び検証機能を提供するサーバ。

2.1.2 紹介状登録

紹介状システムにおいて想定される登録処理手順について、図 2.1.2 紹介状登録シーケンスの付番に沿って説明する。

① 診療所医師が紹介状登録クライアントを用いて、紹介状を作成。

② 作成した紹介状に対し、署名モジュールを用いて診療所医師の署名を付与し、署名付紹介状を生成。

③ 署名付紹介状を紹介状管理サーバに送信。

④ 紹介状管理サーバは、紹介状に付与された署名の検証を、署名・検証サーバに依頼。

⑤ 紹介状管理サーバは、署名・検証サーバからの検証結果に基づき、登録処理を行う。また、紹介状管理サーバは、紹介状の登録結果を紹介状登録クライアントに送信。

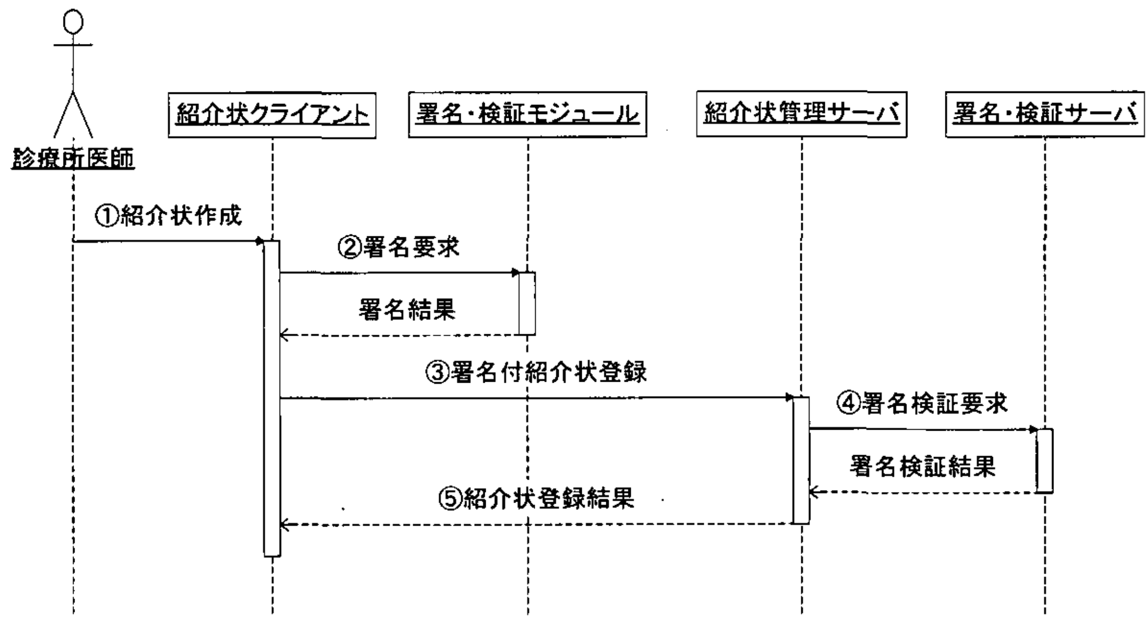

図 2. 1. 2 紹介状登録シーケンス

2. 1. 3 紹介状処理

紹介状システムにおいて想定される紹介状処理手順について、図 2. 1. 3 紹介状処理シーケンスの付番に沿って説明する。

① 専門医は紹介状クライアントを用いて紹介状の処理を開始する。
② 紹介状クライアントは、紹介状を取得するため、紹介状管理サーバにアクセスし、診療所医師の署名が付与された紹介状を取得する。
③ 紹介状クライアントは、署名・検証モジュールにより、紹介状に付与された署名を検証する。紹介状クライアントは検証結果に基づき、処理を続行する。

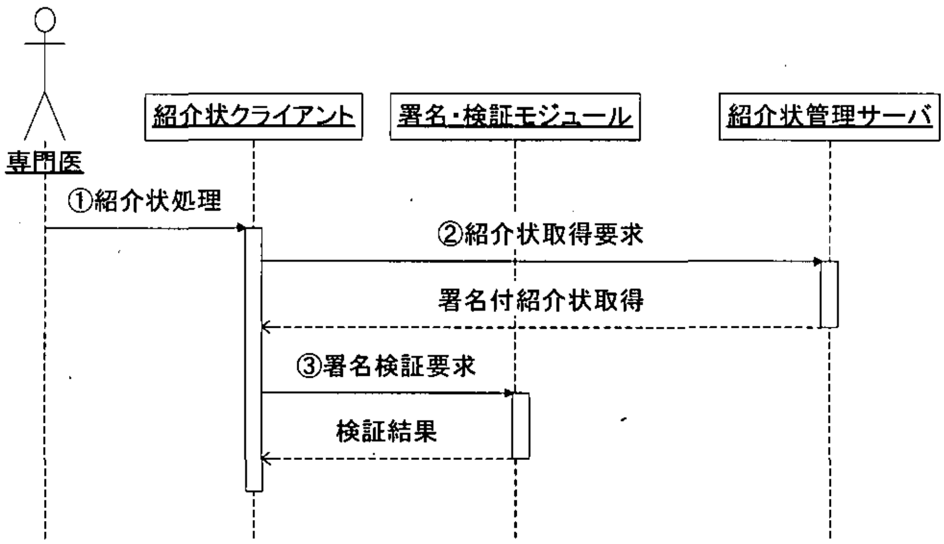

図 2. 1. 3 紹介状処理シーケンス

2．2 検査オーダシステム

署名が求められるケースとして、外注検査を想定した。

検査オーダシステムの処理手順として、外部検査サーバへの検査オーダ登録におけるシーケンス（2.2.2 検査オーダ登録）、サーバに登録された検査オーダを処理するシーケンス（2.2.3 検査オーダ処理）、検査結果を処理するシーケンス（2.2.4 検査結果処理）に分けて整理を行った。

2.2.1 語句定義

検査オーダシステム処理手順において、図 2.2.2 検査オーダ登録シーケンス、図 2.2.3 検査オーダ処理シーケンス、図 2.2.4 検査結果処理シーケンス内で使用した語句は、以下のような意味を持つものとする。

・検査依頼医師
　検査オーダを作成し、検査を依頼する医師。

・検査技師
　検査オーダに基づいて、検査を実施する技師。

・検査処理クライアント
　検査処理クライアントは、検査システムのクライアントアプリケーションを意味し、検査オーダ、検査結果メッセージの作成、検査管理サーバへの登録、また、検査結果メッセージを取得し、その確認処理を行うための機能を有する。

・署名・検証モジュール
　電子署名を作成、検証する機能を提供するライブラリ。このモデルでは、紹介状登録クライアントに組み込まれていると想定。

・検査オーダ管理サーバ
　検査オーダの受信、管理、検査結果メッセージの受信、管理及び検査依頼元への検査結果の送信を担うサーバ。

・署名・検証サーバ
　電子署名の作成及び検証機能を提供するサーバ。

・検査結果受信サーバ
　検査結果を受信し、管理するサーバ。

2.2.2 検査オーダ登録

検査オーダシステムにおいて想定される検査オーダ登録手順について、図 2.2.2 検査オーダ登録シーケンスの付番に沿って説明する。

① 検査依頼医師は検査オーダクライアントを用いて、検査オーダを作成。
② 検査オーダクライアントは、署名・検証モジュールを用いて検査依頼医師の署名を付与。
③ 検査オーダクライアントは、署名付検査オーダを検査オーダ管理サーバに送信。
④ 検査オーダ管理サーバは、署名・検証サーバに検査オーダに付与された署名の検証を依頼。
⑤ 検査オーダ管理サーバは登録結果を検査オーダクライアントへ送信。

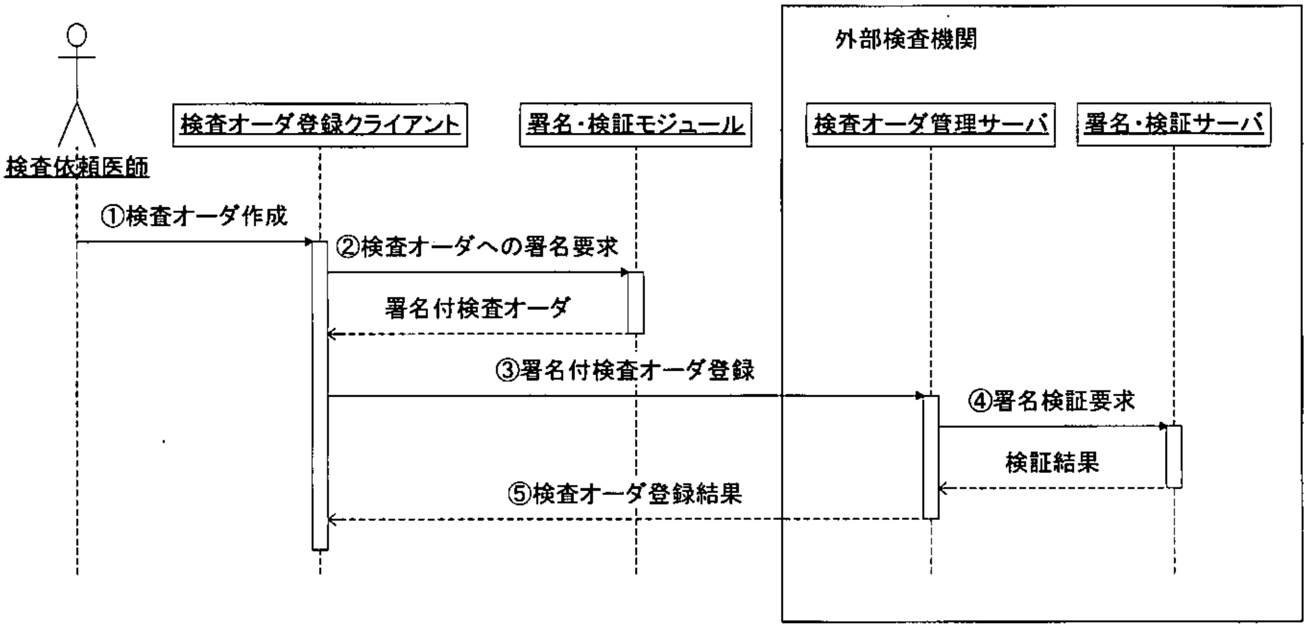

図 2. 2. 2 検査オーダ登録シーケンス

2.2.3 検査オーダ処理

検査オーダシステムにおいて想定される検査オーダ処理手順について、図 2.2.3 検査オーダ処理シーケンスの付番に沿って説明する。

① 検査技師は、検査オーダクライアントを用いて、検査オーダ処理を開始。

② 検査オーダクライアントは検査オーダ管理サーバに対し、検査オーダを要求。
検査オーダ管理サーバは該当する署名付検査オーダを返信。

③ 検査オーダクライアントは、署名・検証モジュールを用いて検査オーダに付与された署名を検証。
検証結果に基づき処理を続行。
検査技師は検査結果に基づき、検査結果メッセージを作成。

④ 検査オーダクライアントは、署名・検証モジュールを用い、検査結果メッセージに検査技師の署名を付与。

⑤ 検査オーダクライアントは、署名付検査結果メッセージを検査オーダ管理サーバに送信。

⑥ 検査オーダ管理サーバは、署名・検証サーバに検査結果メッセージに付与された署名の検証を依頼。

⑦ 検査結果メッセージの登録結果を検査オーダクライアントへ送信。

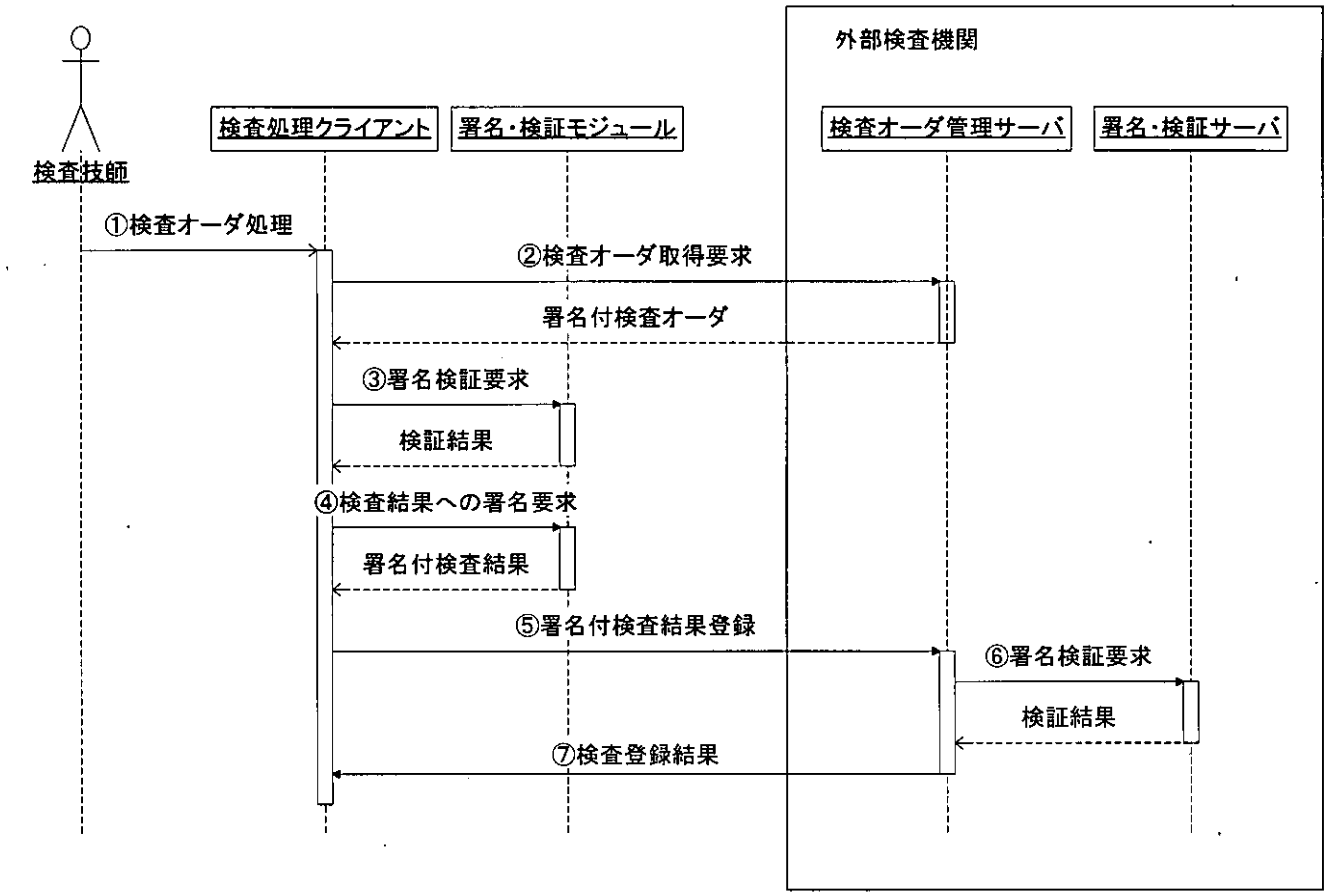

図 2. 2. 3 検査オーダ処理シーケンス

2.2.4 検査結果処理

検査オーダシステムにおいて想定される検査結果処理手順について、図 2.2.4 検査結果処理シーケンスの付番に沿って説明する。

① 外部検査機関の検査結果管理サーバは、検査結果が登録されると、検査依頼元の検査結果受信サーバに署名付検査結果メッセージ送信。

② 検査結果受信サーバは、検査結果メッセージに付与された書名の検証を署名・検証サーバに依頼。検証結果に基づき登録処理を実施。

③ 検査依頼医師は、検査オーダクライアントを用いて、検査オーダ結果の確認を開始。

④ 検査オーダクライアントを用いて、検査オーダ結果を検査オーダ受信サーバから取得。

⑤ 検査オーダクライアントは、署名・検証モジュールを用いて、受信した検査オーダ結果に付与された署名を検証。検証結果に基づいて処理を続行。

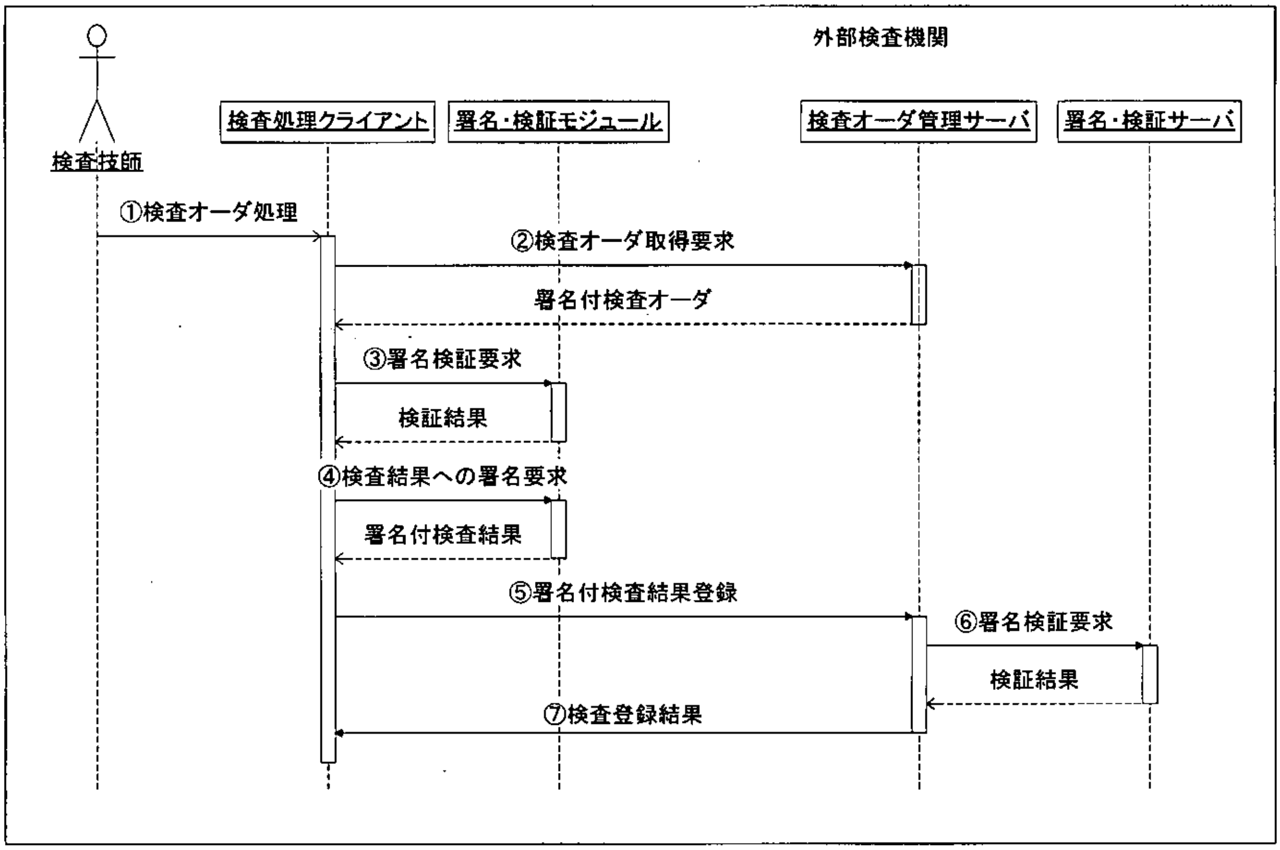

図 2. 2. 4 検査結果処理シーケンス

2.3 処方箋システム

処方箋システムの処理手順として、処方箋管理サーバへの処方箋登録におけるシーケンス（2.3.2 処方箋登録）、サーバに登録された処方箋を処理するシーケンス（2.3.3 処方箋処理）に分けて整理を行った。

2.3.1 語句定義

処方箋システム処理手順において、図 2.3.2 処方箋登録シーケンス、図 2.3.3 処方箋処理シーケンス内で使用した語句は、以下のような意味を持つものとする。

・ 処方箋クライアント

処方箋クライアントは、処方箋システムのクライアントアプリケーションを意味し、処方箋の作成、処方箋管理サーバへの登録、また、処方箋を取得する機能を有する。

・ 署名・検証モジュール

電子署名を作成、検証する機能を提供するライブラリ。このモデルでは、処方箋クライアントに組み込まれていると想定。

・ 処方箋管理サーバ

処方箋の受信、管理、処方箋の単用性の確保、処方完了確認メッセージの作成

・署名・検証サーバ

電子署名の作成及び検証機能を提供するサーバ。

2.3.2 処方箋登録

処方箋システムにおいて想定される処方箋登録手順について、図 2.3.2 処方箋登録シーケンスの付番に沿って説明する。

① 処方医師が処方箋登録クライアントを用いて、処方箋作成。

② 作成した処方箋に対し、署名モジュールを用いて処方医師の署名を付与。

③ 署名付処方箋を処方箋管理サーバに送信。

④ 処方箋管理サーバは、受信した処方箋の署名の検証を、署名・検証サーバに依頼。

⑤ 署名・検証サーバは、検証結果を処方箋登録サーバに返信。

⑥ 処方箋登録サーバは、署名・検証サーバからの検証結果に基づき、処方箋の登録結果メッセージを作成。作成された処方箋登録結果メッセージに対し、処方箋管理サーバの署名を付与。

⑦ 処方箋管理サーバは、署名付処方箋登録結果メッセージを処方箋クライアントに送信。

⑧ 処方箋クライアントは、署名モジュールを用いて処方箋登録結果に付与された署名を検証。

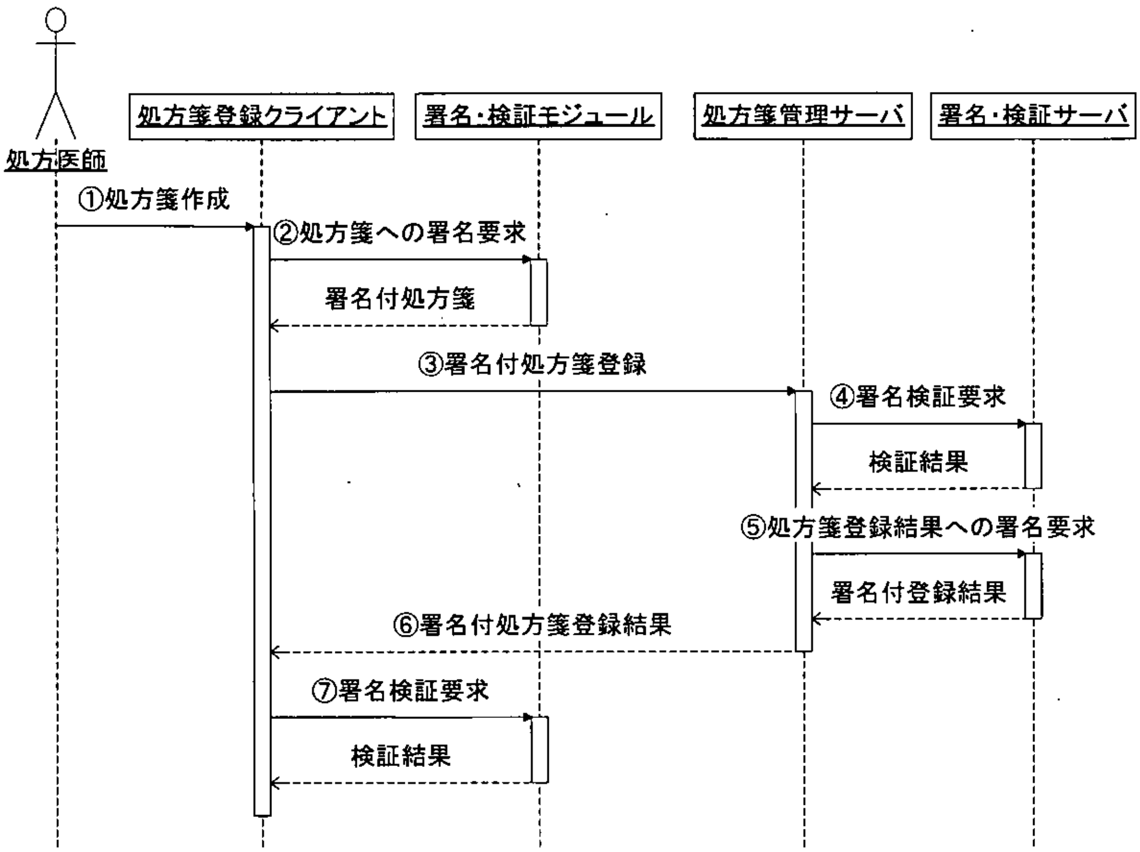

図 2. 3. 2 処方箋登録シーケンス

2.3.3 処方箋処理

処方箋システムでは、先に述べた２つのシステムと異なり、処方箋の単用性の確保も重要な課題となる。電子署名を用いて単用性を確保するモデルを検討した。

処方箋システムにおいて想定される処方箋処理手順について、図 2.3.3 処方箋処理シーケンスの付番に沿って説明する。

① 処方を受けた患者は、その処方箋が存在するネットワーク上のアドレスが記述された媒体（バーコード、IC カード等）を処方を行う薬剤師に渡す。
薬剤師は、処方箋の存在するアドレスが記述された媒体を用い、アドレスを処方箋クライアントに入力。

② 薬剤師は、処方箋の存在するアドレスが記述された媒体を元に、処方箋管理サーバに対し、処方箋を要求。

③ 処方箋管理サーバは、該当する処方箋に対し、処方箋管理サーバの署名を付与。署名・検証サーバは、30 分や 1 時間といった比較的短期の有効期限を持つ署名を生成。処方箋管理サーバは、処方箋の単用性確保のため、この有効期限の間は、他からのこの処方箋への要求には応じない。

④ 処方箋管理サーバは、署名付処方箋を処方箋クライアントへ送信。

⑤ 処方箋クライアントは、署名付処方箋を受信し、署名・検証モジュールを用いて署名を検証。

⑥ 検証結果に基づき、処理を続行。処方が完了後、処方箋クライアントを用い、処方完了メッセージを作成。作成した処方完了メッセージに対し、署名・検証モジュールを用いて薬剤師の署名を付与する。

⑦ 署名付処方完了メッセージを処方箋管理サーバに送信。

⑧ 処方箋管理サーバは、署名・検証サーバに処方箋完了メッセージに付与された署名の検証を依頼。同時に処方箋管理サーバは、署名付処方完了メッセージが元となる処方箋に付与された処方管理サーバの署名の有効期限内に返信されているかを確認。有効期限内であれば、この処方箋を処理済として処理する。有効期限外であれば、この完了報告を無効とし、処方箋管理サーバの署名付完了確認メッセージを返信しない。その場合、この処方箋は、再度未処理の処方箋として扱われる。③の処理とあわせ、処方箋の単用性を確保する。

⑨ 検証結果に基づき、処方完了確認メッセージを作成。作成された処方箋完了確認メッセージに対し、処方管理サーバの署名を付与。

⑩ 処方箋管理サーバは、署名付処方完了確認メッセージを処方箋クライアントに送信。

⑪ 処方箋クライアントは、署名付処方完了確認メッセージを受信し、署名・検証モジュールを用いて署名の検証。処方箋クライアントは検証結果に基づき、処理を続行。

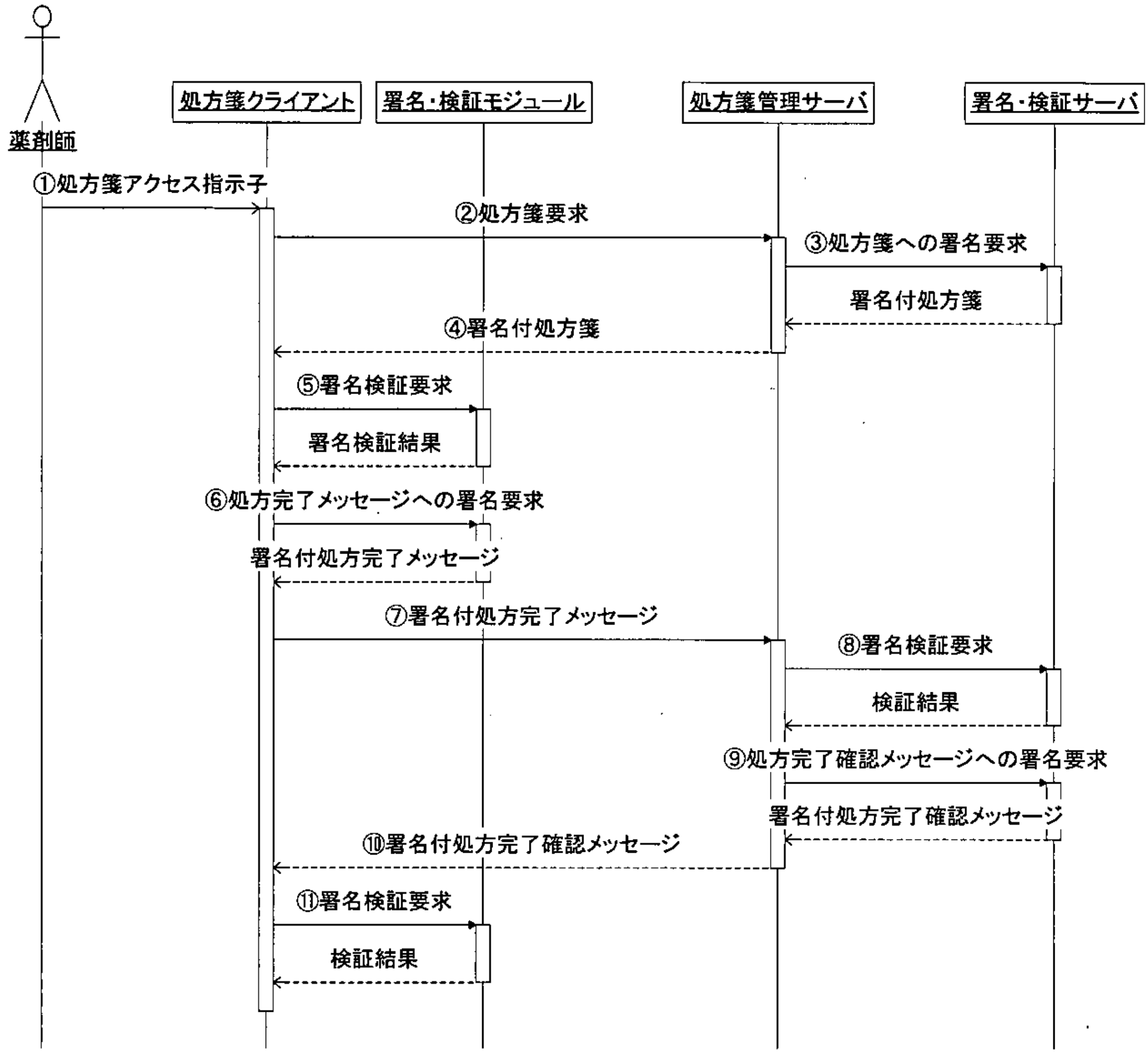

図 2. 3. 3 処方箋処理シーケンス

3. XML 電子署名クラスライブラリ

3.1 クラス概要

XML 電子署名クラスライブラリの基本構成は、署名生成用クラス、鍵ストアクラス、署名検証クラスの３つである。署名生成用クラスは、XmlSigner という抽象クラスに、Enveloped 型 XML 電子署名を生成する EnvelopedXmlSignature クラスと Enveloping 型 XML 電子署名を生成する EnvelopingXmlSignature クラスという２つの実装クラスを用意した。鍵ストアクラスは、SigningKeyStore という抽象クラスに対し、SigningKeyStoreWithCapicom という実装クラスを用意した。署名検証クラスは、XmlVerifier である。

クラス構成図は、図 3.1 署名モジュールクラス構成の通りである。SigningKeyStore は、XmlSigner のコンストラクタの引数となっている。署名用鍵を指定して EnvelopedXmlSigner、EnvelopingXmlSigner はインスタンス化される。

3.2 クラス構成

実装した、クラス、型は以下の通りである（詳細については、添付資料１参照）。

１）署名生成用クラス

・ XmlSigner

XML 電子署名クラスの抽象クラス。

・ EnvelopedXmlSigner

Enveloped 型 XML 電子署名を行うクラス。

・ EnvelopingXmlSigner

Enveloping 型 XML 電子署名を行うクラス。

２）鍵ストアクラス

・ SigningKeyStore

署名用証明書を選択する処理を実装するための抽象クラス。

・ SigningKeyStoreWithCapicom

CAPICOM を使用し、署名用証明書を選択するクラス

・ KeySpec

鍵のタイプを指定する型。署名用もしくは鍵交換用のタイプが指定可能。

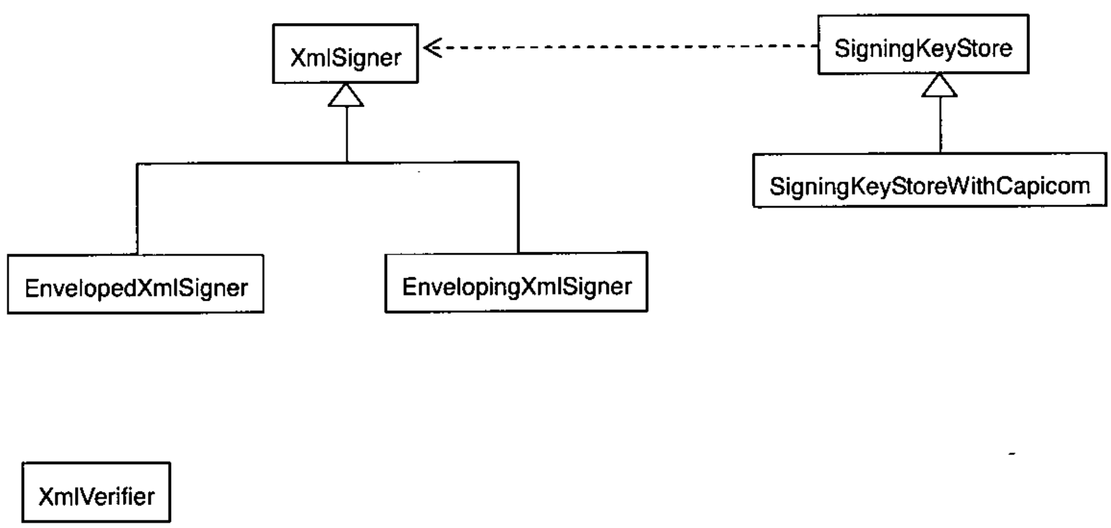

図 3.1　署名モジュールクラス構成