200732026A

厚生労働科学研究費補助金

医療安全・医療技術評価総合研究事業

安全な保健医療情報流通を促進する保健医療認証基盤整備の技術的方策に関する研究

平成１９年度　総括研究報告書

主任研究者　大山　永昭

平成２０（２００８）年　４月

別紙２

目　　次

厚生労働科学研究費補助金（医療安全・医療技術評価総合研究事業）
総括研究報告書

安全な保健医療情報流通を促進する保健医療認証基盤整備の技術的方策に関する研究

主任研究者　大山　永昭　東京工業大学像情報工学研究施設　教授

研究要旨：今後の医療の高度化やそれに伴う機能分化の促進が想定される状況下で、患者主体の診療が実施されるためには、関連する施設等の間で、電子カルテや医療情報の伝送を安全かつ動的に行っていくためのネットワーク基盤が必要である。本研究では、前年度までに検討した認証基盤の具体的な応用として、オンデマンドＶＰＮやヘルスケアＰＫＩ等の技術を組み合わせることで、安全な保健医療情報の流通を実現するとともに、個人が本人の保健医療情報を主体的に管理できる仕組みを提案し、提案手法に基づくプロトタイプシステムを構築した。さらに、公的な社会福祉に関する個人情報を管理する電子私書箱について、提案モデルと連携させる方法やその効果について検討した。

分担研究者　喜多　紘一　東京工業大学統合研究院 特任教授
土屋　文人　東京医科歯科大学歯学部付属病院 薬剤部長
八幡　勝也　産業医科大学産業生態科学研究所 准教授
秋山　昌範　国立国際医療ｾﾝﾀｰ情報ｼｽﾃﾑ部 部長
石垣　武男　名古屋大学大学院医学研究科　名誉教授
山本　隆一　東京大学大学院情報学環　准教授
梅田　徳男　北里大学医療衛生学部　教授

A．研究目的

近年の情報基盤整備の進展に伴い、保健医療分野における情報化の推進が期待されているが、電子的に保健医療情報の流通を行う場合には、個人情報の保護が極めて重要であり、そのために必要となる適切な措置を講じることが急務とされている。

ここで、個人情報の安全性を確保するためには、医療データ等を使用する者の正当性を認証すること及び、通信回線上や医療機関内での医療データ等の保護を実現することが重要である。我々は、これまでに保健医療福祉分野の情報化において必須となる電子的な認証、特に医師･看護婦等の資格認証の必要性を示し、電子認証の実施方法や問題点の調査・検討を行ってきており、本研究では、これら研究成果を踏まえ、もう１つの重要な課題である通信回線上や医療機関内部における個人情報・医療情報等の安全性を確保する技術について研究開発を進めるとともに、保健医療分野における情報の安全な流通を保証するネットワーク基盤を構築・運用する方策について検討する。さらに、保健医療福祉分野でのネットワーク基盤整備を進めるとともに、それを活用した様々な保健医療福祉サービスの充実が求められていることから、ネットワーク基盤を利用した安全性、利便性、経済性などに優れた医療サービスの実施方法を取りまとめ、さらに保健医療福祉サービスの今後の新たな展開の可能性等を示す。

B．研究方法

工学者及び医師らの研究分担者からなる研

究班として、保健、医療、福祉の各分野における情報化推進にあたっている専門家を中心として組織し、委員会を開催して各分野における電子化の状況や情報保護に対する取り組みを調査し、安全に医療情報を取り扱うための課題の抽出と実現方法の検討を行った。さらに、安全なネットワーク基盤構築に関する検討を行っている諸機関･グループとの情報交換･連携を行い、今後、医療分野における共通ネットワーク基盤にするための方策を検討した。

C．研究結果

平成１８年度までの研究において、保健医療情報を取り扱う際に必要な認証基盤を整理した。今年度は、これまでに検討した認証基盤を具体的なサービスへ適用する方法の検討として、安全な保健医療情報の流通を促進する仕組みを提案し、システムを実現するために必要となるセキュリティ要件を整理した上でプロトタイプシステムを構築し、評価を行った。

(1) 保健医療情報を取り扱う具体的なサービス例とセキュリティ要件

保健医療情報の流通を促進する試みとしては、地域ごとに地域医療情報管理センターなどを設置し、患者の保健医療情報を集中的に管理・利用する方法と、個人自らが自己の保健医療情報を管理し、その情報を健康増進や診察に役立てる方法がある。従来、我が国においては、前者の方法による様々な試みがなされてきたが、安全性の問題やセンター運営の費用などの問題から、必ずしも目的を達しているとは言い難い。

これに対し本研究では、平成19年4月に発表された「ＩＴ新改革戦略 政策パッケージ」に記載された“社会保障に関する国民個々の情報を国民が自らのものとして簡単に収集管理可能な仕組みである「電子私書箱（仮称）（電子情報アカウント）」”を利用することで、個人が保健医療情報を主体的に管理できる仕組みを提案し、後者の立場からの保健医療情報の流通促進を実現する。

具体的には、まず日本における個人保健医療情報管理の実現に必要なセキュリティ要件を整理し、これまでの研究で我々が提案した認証基盤を応用した実現モデルを検討する。

（ア） 個人による保健医療情報管理の現状

個人が主体的に保健医療情報を管理・運用する代表的な仕組みとして、Personal Health Record (PHR)がある。欧州では、医療情報を一元化・統合化する、EHR(Electronic Health Record)システムの整備が進んでおり、その拡張機能として、PHR機能を提供する仕組みの整備が進んでいる。また米国においては、民間中心の医療制度の下で様々なタイプのPHRの構築が進められている。PHRでは、「医療情報をどこから、どのように集めるか」という点が重要であるが、近年欧米で利用され始めているシステムでは、「外部接続性の確保」を重要機能として実装することで、「情報の入出力」という課題に対して対処することを目指している。

一方我が国では、欧米と比べ個人により保健医療情報管理を行うシステムへの取り組みは遅れているが、IT戦略本部で2007年7月に決定された「重点計画-2007」において、「世界最先端の国民健康情報基盤を目指し、健診結果等の健康情報を個人が活用する仕組みを2011年度当初までに構築する」こと及び「国民の社会保障に関する情報を希望する国民が自ら入手・管理できる『電子私書箱(仮称)』を検討し、2010 年頃のサービス開始を目指す」ことが盛り込まれ、個人に対する健康医療情報の提供手段としての電子私書箱への期待が高まっている。

本研究では、保健医療情報の流通を促進する仕組みとして、個人保健医療情報管理に必要となる「情報の入出力」に電子私書箱を利用し、平成18年度までの研究で明らかにした保健医療情報を取り扱う際に必要な認証基盤を組み合わせることで、個人が安全に保健医療情報を主体的に管理・運用できる仕組みを提案する。

（イ） 個人保健医療情報管理で要求されるセキュリティ技術

個人保健医療情報管理で取り扱う保健医療情報は個人情報であるため、送信された情

報を本人のみが開封可能とし、同意がある場合に限り情報の閲覧を他人に許可する仕組みなどが必要になる。ここでは、そのための要件として以下の2点を挙げる。

① 個人のアカウントへアクセスするための厳格な個人認証
② 本人のみに情報が開示される仕組み（親展通信）

①については、ICカードを用いた電子認証が有効である。特に、全国どこでも質の高い保健医療サービスを受けられる“医療のフリーアクセス”を考慮すると、ICカードは、公的な公開鍵基盤(PKI)に対応し、それを利用した電子認証を用いることが望ましい。②については、サーバに保存する保健医療情報をICカード内の公開鍵証明書(PKC)に含まれる公開鍵で暗号化し、復号化には対応する秘密鍵を用いることで実現できる。このとき、秘密鍵はICカードに格納されるため、本人以外が情報を復号化することはできない。

保健医療情報のディペンダビリティの観点からは、保健医療情報を提供する医療機関と電子私書箱や個人保健医療情報を管理する機関との間の通信路は暗号化されるべきであり、スパムやDOS攻撃を防止するためには医療機関以外からのアクセスは避けるべきである。また取り扱う保健医療情報は、正当な保健医療業務従事者から提供された情報であることを保証したい。よって以下の3点を要件として挙げる。

③ 情報提供者とデータサーバ間の通信路を暗号化すること
④ 医療施設からの通信のみアクセス可能とすること
⑤ 医療従事者の提供したデータであることが確認できること

③及び④についてはオンデマンドＶＰＮが有効である。平成19年3月に厚生労働省より発行された「医療情報システムの安全管理に関するガイドライン（第二版）」では、オープンなネットワーク上で医療情報を伝送する場合の安全な通信方法の一つとしてIPsec-VPNが推奨されているが、オンデマンドVPNは、専用ルータを設置することでIPsec-VPNを容易に利用可能である。また専用ルータに組み込まれたICチップを利用して機器認証を行えるため、特定の施設からのアクセスのみに制限することが可能である。⑤についてはヘルスケアPKI（HPKI）を利用した電子署名が有効である。HPKIでは、証明書に「hcRole」という医療従事者の資格情報を記述する項目があり、HPKIの署名が付与されたデータは、どのような資格を有する人に提供されたものであるかを確認することができる。

以上の要件とその対策を表１にまとめる。

表１．保健医療情報管理に要求される技術

要件	手段
厳格な個人認証	公的なＰＫＩによるＩＣカード認証
親展通信	ＰＫＣ及びＩＣカードでの鍵管理
通信路の暗号化 医療機関の施設認証	オンデマンドＶＰＮ
保健医療情報の信頼性の確認	ＨＰＫＩによる電子署名

(2) 個人の医療情報を一元的に扱う情報管理システムの検討

（ア） システム仕様設計

前節の検討を踏まえ、個人への情報提供、管理サーバへの登録、データの参照を行うPHRシステムを設計する。

PHRシステムとして想定するプレイヤーは、個人（ユーザ）、健診センター、健診データサーバ、病院、外部連携サービスとする。特に健診データサーバは、データを個人に提供する機能をもつ部分をInBox、登録・参照する機能有する部分をViewBoxと呼ぶことにし、InBoxは将来実現される電子私書箱の機能を利用することを想定している。プロトタイプシステムにおいて想定されるシナリオの概

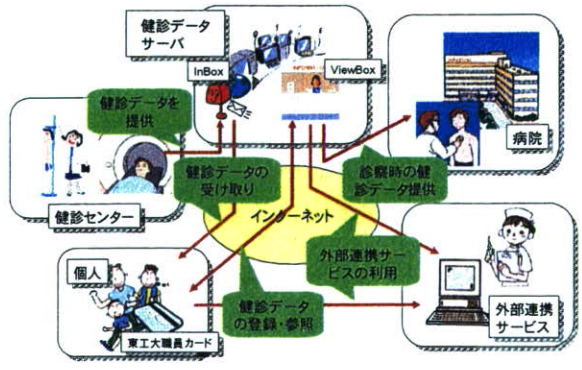

図 1. 想定する PHR システム

念図を図1に示す。

以下に機能ごとの仕様詳細を述べる。

(1)　保健医療データの個人への提供

健診データは特定健診のXMLベースの標準フォーマットに準拠させ、提供する健診データを作成する際にはデータ作成者（健診センターの医師など）の電子署名およびタイムスタンプを付与する。健診データは圧縮された上で共通鍵によって暗号化され、共通鍵はユーザのRSA公開鍵で暗号化される。健診センターから健診データサーバ（InBox）への送信はオンデマンドVPN接続で行う。ユーザが健診データサーバへアクセスする際にはICカードに格納されたPKIを用いた認証を行う。健診データは、ICカードに格納されたRSA秘密鍵を用いて復号化された共有鍵により、ユーザのPC上で復号化・解凍される。ユーザは、復号化された健診データに含まれる、検体検査、DICOM画像、心電図波形を専用ビューワーで参照でき、またデータに付与された電子署名及びタイムスタンプの検証が可能である。

(2)　保健医療データ管理サーバへの登録

ユーザが健診データベースサーバ（ViewBox）へアクセスする際にはICカードを用いた認証を行う。健診データはICカードに格納されたRSA秘密鍵を用いたXML暗号処理を施され、暗号化された状態でViewBoxへ登録されるため、ユーザ本人以外は登録された健診データを閲覧することはできない。登録時には健診データに付与された電子署名及びタイムスタンプの検証を行う。

(3)　保健医療データのオンライン参照

ユーザが健診データサーバ（ViewBox）へアクセスする際にはICカードを用いた認証を行う。健診データサーバとユーザPCの通信はSSLとするが、病院に設置されたPCより参照する場合にはオンデマンドVPN接続とし、その場合健診データのダウンロードを可能としている。健診データの参照時には、ICカードに格納されたRSA秘密鍵を用いてユーザPC側で共有鍵を復号化した後、それをサーバに送付してXML復号処理を行い、検体検査、画像、波形などのデータはWebブラウザを利用して参照する。またサーバ側には、健診データに付与されている電子署名及びタイムスタンプを検証できる機能を付与している。参照が終わったら、データを再暗号化して健診データサーバに保存するため、ユーザ本人が健診データサーバに接続している時以外は、他の者が登録された健診データを閲覧することはできない。さらに、ユーザが同意した健診データは外部連携サービス用サーバへ転送し、そのサービスを利用することができる。

(4)　医療機関間のオンデマンドVPN接続

VPN接続許可のためのポリシーマッピングを行う際に、医療機関であることを確認する。医療機関であることを確認する方法には、HPKIによる電子署名を利用する。ポリシーマッピングによって接続先が医療機関であることが確認された場合のみ、VPN接続を許可する。

（イ）プロトタイプシステムの構築及び動作実験

前節の仕様検討に基づき実験システムを構築した。個人認証用のＩＣカードとしては、ＰＫＩ機能を有する東工大の職員証を利用

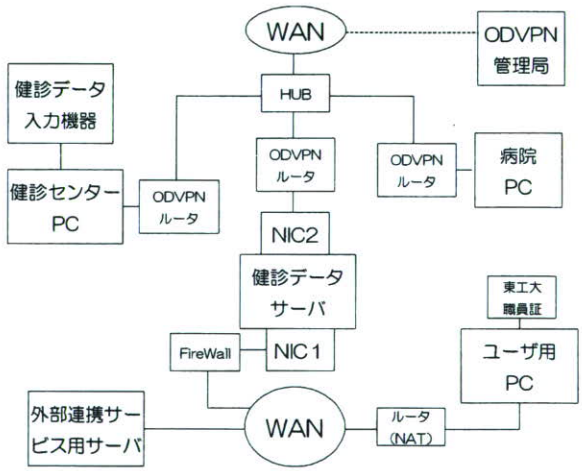

図 2. プロトタイプシステムの構成図

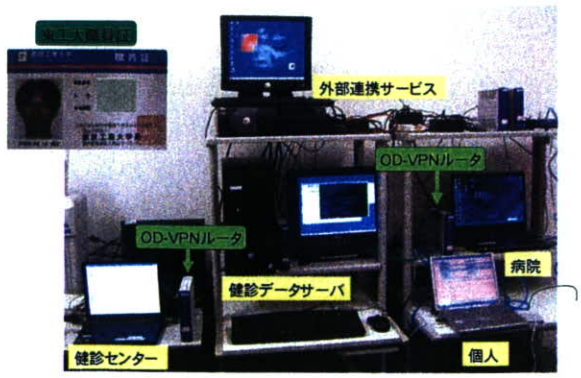

図 3. プロトタイプシステムの外観

し、またオンデマンド VPN は、㈱ＮＴＴＰＣコミュニケーションズの IP-members を利用した。システム図および外観を図 2 および図 3 に示す。

以下にそれぞれの動作結果について述べる。

(1)　健診データ入力

健診センター用 PC にインストールされた専用 AP を利用し、ユーザ情報に関する情報や健康診断に関する情報を登録した上で、検体検査、問診、画像、波形等の結果を入力する。また、検索等に必要な情報をメタデータとして入力する。ユーザ登録の際には、健診データを暗号するためのユーザの公開鍵証明書を登録する。

(2)　健診センター・健診データサーバ間のオンデマンド VPN 接続

オンデマンド VPN 用管理 AP を利用して、健診データサーバへ接続要求する。接続要求する前には、サーバ条件、クライアント条件を登録し、接続合意を取っておく。

(3)　健診センターから InBox へのデータ送付

オンデマンド VPN の接続完了後、健診センターの専用 AP を利用して健診データサーバの Inbox へデータを送付する。この際、標準フォーマットへの変換、データの圧縮、電子署名、タイムスタンプの付与が行われる。

(4)　InBoxから個人用PCへのダウンロード

ユーザPCの専用APを利用して健診データをダウンロードする。ユーザは InBox へアクセスすると認証要求が来るので、IC カードを利用してユーザ認証を行う。認証成功後、InBox 上のデータ一覧が表示されるので、必要なデータを選択し、ダウンロードする。ダウンロードしたデータは、メタデータは表示されるが、データの本体は暗号化された状態なので見ることはできない。

(5)　個人用 PC でのデータ復号化および閲覧

ユーザPCの専用APを利用して健診データの復号化を行う。復号化されたデータには参照用 Viewer ソフトが含まれているので、これを利用して健診結果のデータを閲覧する。また、参照用 Viewer を利用して電子署名およびタイムスタンプの検証を行うことができる。

(6)　個人用 PC へダウンロードしたデータの ViewBox への登録

ユーザ PC の専用 AP を利用して InBox からダウンロードしたデータを ViewBox へ登録するためのデータフォーマットへ変換する。Web ブラウザから ViewBox へアクセスし、職員証を利用したユーザ認証を行う。ViewBox へ登録するデータを選択し、登録を行う。

(7)　InBox に保存されているデータの ViewBox への登録

ユーザ PC の専用 AP を利用して InBox 上のデータを ViewBox へ直接登録する。登録が完了すると Web ブラウザが立ち上がり、健診結果を参照できる。

(8)　個人用 PC から ViewBox へ登録されている健診データの参照

ViewBox へアクセスし、ユーザ認証を行う。

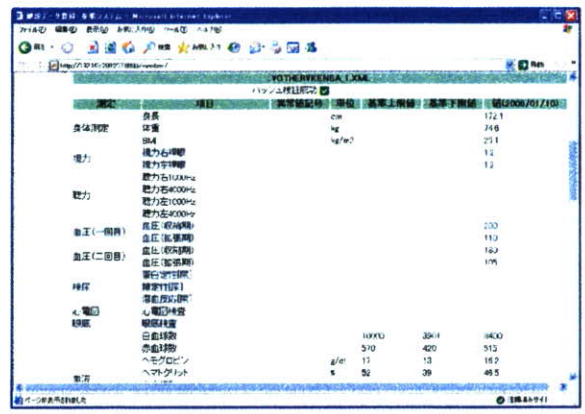

図 4.　ViewBox での参照（検体検査結果）

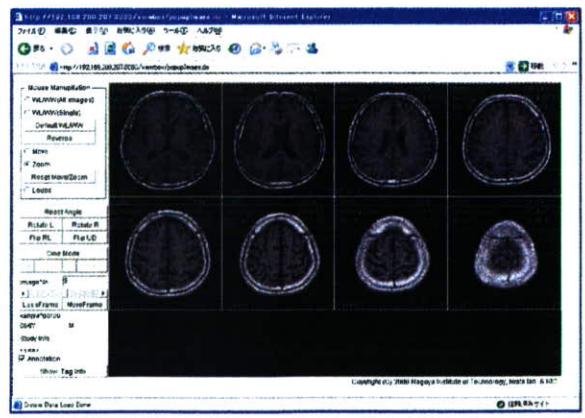

図 5.　ViewBox での参照（画像検査結果）

図 6. ViewBox での署名検証結果

メニューの中から、一覧もしくは検索によって参照するデータを選択し、健診結果を参照する(図 4)。画像や波形も Web ブラウザ上で閲覧可能である(図 5)。また、電子署名およびタイムスタンプの検証結果を確認することができる(図 6)。

(9)　外部連携サービスへ提供、利用

ViewBox での参照画面で、健診結果内に表示されている外部連携ボタンを押すと、その検体検査の結果が外部連携サービスに送付され、外部連携サービス(ヘルスアップ WEB)が別の Web ブラウザ上で起動する(図 7)。このサービスでは、送付した検体検査結果に基づき健康チェックを行うサービスである。

(10)　病院内 PC でのデータ参照及びダウンロード

病院内の PC で参照する場合には、まず病院と健診情報管理サーバとの間をオンデマンド VPN 接続する。その後ユーザの PC と同様に ViewBox へアクセスし、健診結果を参照する。また病院の場合にはデータのダウンロードも可能であり、ダウンロードしたデータはユーザ PC で復号化したデータと同様に専用 Viewer を用いてデータを閲覧可能である。

図 7. 外部連携サービスの利用

D．考察

（ア） システムの安全性について

今回構築した PHR のプロトタイプシステムでは、我々の設定したセキュリティ要件を満たしているが、暗号アルゴリズムの危殆化や悪意の第三者のよる様々な攻撃方法に対する対策についは今後検討の必要がある。

（イ） システムの利便性について

システムを利用するためには、専用ソフトウエアやICカードを利用する環境をインストールする必要があり、誰でも容易に利用可能な状況になっていない。PCを利用する場合には、プラットフォームに依存しないWebブラウザでの実装が望ましい。また、より汎用的な端末を考えた場合、地上波デジタルテレビや携帯電話のような機器での実現が望まれる。

（ウ） 実現可能性について

提案するシステムでは、我々が研究を進めてきたオンデマンド VPN を利用することで保健医療情報を提供する提供者を医療機関のみに限定することができるが、このためには専用ルータを設置する必要があり、すべての医療機関がオンデマンド VPN を利用できる環境を整えることが大きな課題となる。しかし、これについては、2010 年度までにレセプト提出及び受領の完全オンライン化がすべての医療機関に義務付けられており、オンラインレセプトを行うためには、ISDN、IP-VPN といった専用回線を利用するか、もしくは IP-sec と IKE を利用したインターネットでの VPN が必要とされている。ここで、回線速度や運用のコストを考えると、オンライン請求を行う医療機関の多くはオンデマンド VPN を利用すると予想され、提案システム導入の課題である情報流通基盤整備は、一気に進むものと考えられる。

電子認証を行う IC カードについては、すべての国民が利用可能な認証基盤が必要になるが、住民基本台帳カードと公的個人認証サービスがすでに運用されており、今後公的個人認証サービスの電子認証への拡張が実

施されれば、これを利用する方法が考えられる。また、「重点計画-2007」には、健康保険証などとしての役割を果たす『社会保障カード(仮称)』 を 2011 年度中を目途に導入することも明記されており、有力な候補である。

また、「情報の入出力」としての電子私書箱が公的な機関によって設置され、ユニバーサルサービスとしての提供が開始されれば、希望する国民はだれもが医療機関との間で安全に保健医療情報をやり取りできるようになり、保健医療情報の流通が促進されることで、新たな保健医療産業の発展が期待できる。

E．結論

本研究では、昨年度までに検討したオンデマンドVPNやHPKI等のセキュリティ技術を応用することで、個人健康医療情報の安全な流通を促進するシステムモデルを提案した。そして、現在政府で検討が進められている電子私書箱や社会保障カードと連携することで、安全・安心な保健医療情報の流通が可能であることを示した。

本研究で得られた成果は、安全なネットワーク基盤を利用した保健医療福祉サービスの研究開発に活用される予定となっている。具体的には、保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアムや現在オンデマンドVPN技術の研究開発を行っている研究グループとの間で成果を共有することで、これら研究グループが進めている医療機関相互における情報連携の実証実験や医療サービスの検討等への反映や、オンデマンドVPNを構成する技術仕様へフィードバックすることを予定している。

さらに、ネットワーク基盤の整備だけでなく、それを活用した様々なサービスの拡充が求められており、今後、本研究で得られた成果を活用して、新たな保健医療福祉サービスに関する研究開発が行われることを期待する。

F．健康危険情報

該当なし

G．研究発表

1．論文発表

- 丸山剛, 喜多紘一, 鈴木裕之, 小尾高史, 谷内田益義, 山口雅浩, 大山永昭：医療分野における自己情報コントロールを目的としたアクセス制御方法に関する研究；電子情報通信学会論文誌, J90-D(12), 3170-3180(2007)

2．学会発表

- 鈴木裕之, 喜多紘一, 谷内田益義, 小尾高史, 山口雅浩, 大山永昭：ＨＰＫＩによる電子署名を利用した健康管理データ提供・参照システム；ワイヤレス・テクノロジーパーク 2007 講演予稿集, 56-57(2007)
- 喜多紘一, 平井正明, 鈴木裕之, 谷内田益義, 山口雅浩, 小尾高史, 大山永昭：CDA R2 に準拠した個人提供用健康診断結果報告書を利用した個人健康情報管理システム；第 27 回医療情報学連合大会 (第 8 回日本医療情報学会学術大会) 予稿集, P7-4 (2007)
- 喜多紘一, 鈴木裕之, 竹田忠雄, 猪俣彰浩, 島田宏, 有馬一閣：HPKI とダイナミック・オンデマンド VPN との連携によるセキュアな医療ドメインネットワーク；第 27 回医療情報学連合大会 (第 8 回日本医療情報学会学術大会) 予稿集, 1-H-3-2 (2007)
- 喜多紘一, 鈴木裕之, 竹田忠雄, 猪俣彰浩, 島田宏, 有馬一閣：VPN 接続許可をポリシー制御可能なダイナミック・オンデマンドＶＰＮ；SCIS2008 (暗号と情報セキュリティシンポジウム) 予稿集, 4C2-2 (2008)
- 岡野　翔, 鈴木裕之, 小尾高史, 山口雅浩, 谷内田益義, 大山永昭, 喜多紘一：個人情報の利活用を可能とするサービス基盤に関する研究；電子情報通信学会 2008 年総合大会講演予稿集, 520(2008)

厚生労働科学研究費補助金（医療安全・医療技術評価総合研究事業）
分担研究報告書
認証業務等提供事業者、医療機関における運用方法の検討、
国際的な医療情報保護の取り組みとの整合性の調査・検討
分担研究者　喜多紘一
東京工業大学　統合研究院　特任教授

研究要旨　「電子私書箱構想による個人健康情報参照システム」のプロトタイプを構築してHPKIの保健医療福祉分野に適した公開鍵基盤の構築」及び、医療機関内外において個人情報・医療情報等の安全性を確保するために必要となる「公開鍵基盤を活用するための技術的方策」を検討した。主にHPKIによる電子署名の実施および検証を実証した。

健診機関と電子私書箱間および、電子私書箱と医療機関間のセキュアなチャネルとしてHPKIと連携することによりフリーアクセスが可能となるダイナミック・オンデマンドVPNを使用した。その結果、システム構築上、インターネットに接続できない状況が発生し、ＣＲＬチェックを必要とする場合はタイムスタンプの実施や署名、暗号化ができない。　また、署名検証やタイムスタンプ検証ができない。

対策としては、新たなＬＡＮの口を作り、ファイアウォールルータで特定のＣＲＬやＴＳＡとしか接続できないように設定する必要がある。あるいは、ダイナミック・オンデマンドVPNサービス提供者がＶＰＮを経由してＣＲＬやＴＳＡに安全に結合する方法、オフラインでＣＲＬを提供する方法がある。具体的には実証が必要で今後の課題である。

また、長期にデータを保管する場合はカード紛失、更新や緊急アクセスにそなえてキーエスクロや代理カードのポリシを定めておく必要がある。

また、証明書ポリシはISO 17090 と整合性がとられている。しかし、既存のＩＥ付属のブラウザでは表示できない項目もあり専用の検証プログラムを作成する必要がある。

A. 研究目的

分担研究として「認証業務等提供事業者、医療機関における運用方法の検討、国際的な医療情報保護の取り組みとの整合性の調査・検討」を行う。本研究では、医療に関する施設の間で電子化された診療情報を交換又は共有する場合などに、安全な医療情報の流通を推進する際に必要となる、「保健医療福祉分野に適した公開鍵基盤の構築」及び、医療機関内外において個人情報・医療情報等の安全性を確保するために必要となる「公開鍵基盤を活用するための技術的方策」を明らかにすることを目的とする。平成19年度は、保健医療分野における認証基盤を応用したシステムのプロトタイプとして「電子私書箱構想による個人健康情報参照システム」を構築した上で、HPKI（保健医療福祉分野PKI）利用の具体的な課題の検討をおこなった。

B. 研究方法

1．電子私書箱構想

電子私書箱構想は重点計画2007 [1] [2]の中に「国民視点の社会保障サービスの実現に向けての電子私書箱（仮称）の創設」の項があり、「医療機関や保険者等に個別管理されている情報を、希望する国民が自ら入手・管理できる「電子私書箱（仮称）」を検討し、2010 年頃のサービス開始を目指す。」と記述されている。これは図１にしめすように、保険情報、年金情報、各種証明書、健康情報を電子私書箱を通じて自ら入手できる仕組みである。

「自らの情報を一元化し、自らの意思で利活用できる仕組み」とされ、「電子私書箱にアクセスすれば、知りたい情報が一目瞭然」で「医療機関別に個別管理されている健康情報を一元管理」、「年金の加入履歴・トータルの給付額を簡単に把握」、さらに、「国民が電子私書箱の情

報を自らのものとして利活用」でき、「情報の整理・分析」、「他の手続き等への利用」が謳われている。現在、実現に向けて各種委員会が開かれている。

2．社会保障カード構想

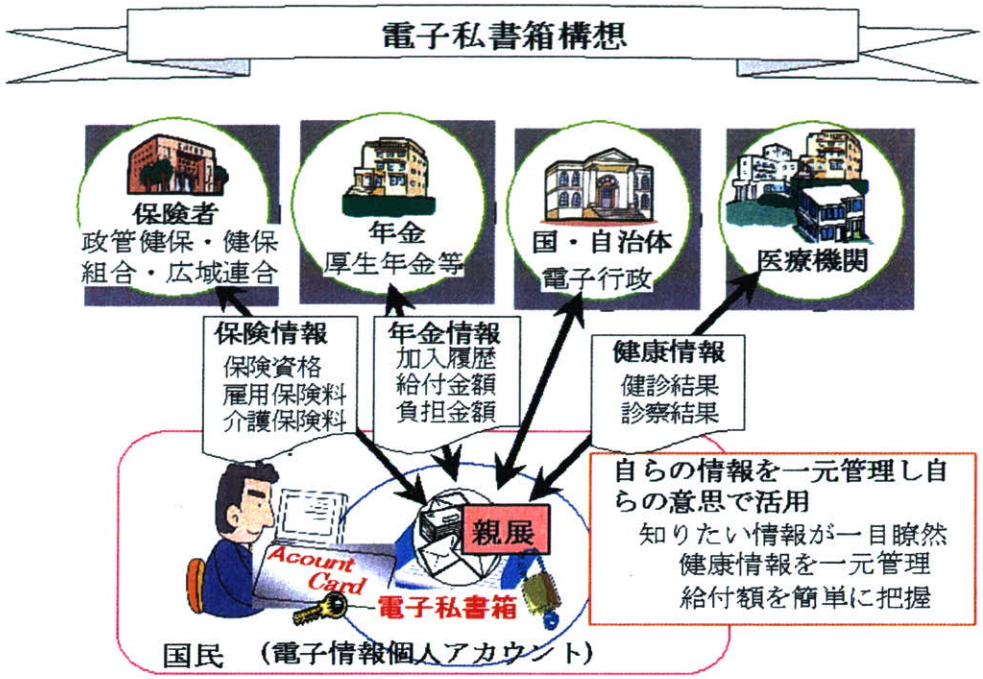

図１電子私書箱構想

同様に、重点計画2007において、社会保障カードの推進が記載されている。これは「年金手帳や健康保険証、更には介護保険証としての役割を果たす「社会保障カード（仮称）」を2011年度中を目途に導入することを目指す。その際、電子私書箱（仮称）の検討と連携しつつ、希望する個人が健診情報等の健康情報の閲覧・管理に役立てるための仕組みの導入に向け、システム基本構想等について検討を行い、2007年内を目途に結論を得る。」となっていて、電子私書箱のアクセスカードとして期待できる。

3．HPKI（保険医療福祉分野PKI）[3]

医療分野では記名押印にかわる電子署名として HPKI の構築が厚生労働省を中心に進められている。図２に示すように公開鍵証明書内に医療関連の国家資格あるいは施設管理責任者情報を格納できるので、通常の PKI 証明書のような自然人の確認だけではなく国家資格保有者や施設管理責任者を確認することができる。

HPKI は厚生労働省が厚生省が証明書ポリシ[4]を作成して、ルート認証局を運営し、MEDIS-DC 認証局が加入者証明書発行サービスを行っている。

図２　HPKI（保健医療福祉分野PKI）

また、本証明書ポリシはＩＳ化されたISO17090 Public key infrastructure [5] Part1～3との整合性が取れている。

4．HPKIと連携ダイナミック・オンデマンドVPN（フリーアクセス可能なＶＰＮ）[6]

個人健康情報参照システムを実現する場合のネットワークへの要求事項は電子私書箱からみると接続相手は固定ではなく、データを提供する施設および、データを見せる場合は複数となり、接続先を切り替える必要がある。現状の医療分野のセキュアネットワークでは専用線、ISDNもしくはIP－VPNが用いられることが多い。インターネット上で安価に使用するために、インターネットVPNが使用され始めている。

しかし、通常使用されているインターネットVPN仕様は１対１(Fixed VPN)の固定接続であり、パラメータもマニュアルで設定されて、接続相手を追加するには手間がかかり、また、マニュアルなので瞬時に追加することはできない。医療機関同士の通信ではN対Nで相手を自由に切換えられるＶＰＮが要求される。この要求を満たすものとしてダイナミック・オンデマンドVPNが開発されてきている。

通常のオンデマンドＶＰＮは、接続先をあらかじめ通話を許可した相手を相互に登録しておくか、都度、相手先を申請して相手側も同時に接続申請をした場合に接続を許可される方式となっている。緊急時に新しい接続を行うことは接続条件の成立に手間がかかり、間に合わない。

接続先の施設からあらかじめ「医療機関であれば接続を許可する」旨のポリシが登録されている場合には、接続先から新規接続申請者に対して、それぞれ接続したい旨の申請が個々になされていなくても、接続申請時に「医療機関であること」がオンラインで確認できれば、医療機関との接続を許可すれば医療機関と包括的に接続できる方式を実現することができる。

この為に、本プロトタイプシステム構築では、機器所有者登録あるいは接続許可申請時に登録文書にHPKIで署名を行うこととした。接続許可時、医療機関の管理責任者名および医療機関名の真正性が保証され、成りすましを防ぎ、フリーアクセスを確保することができる。図３にその概要を示す。

こうした包括的なポリシを実現するネットワークは健診情報システム、遠隔医療システム、医療地域連携システム等の医療サービス提供者の施設が予め登録できない場合に有効である。サービス提供者をあらかじめ登録する必要がないので、サービス提供者を自由に選択することができ、患者の囲い込みを防ぎ、医療機関であることは確認されるので信頼できる医療ドメインを形成することができる。

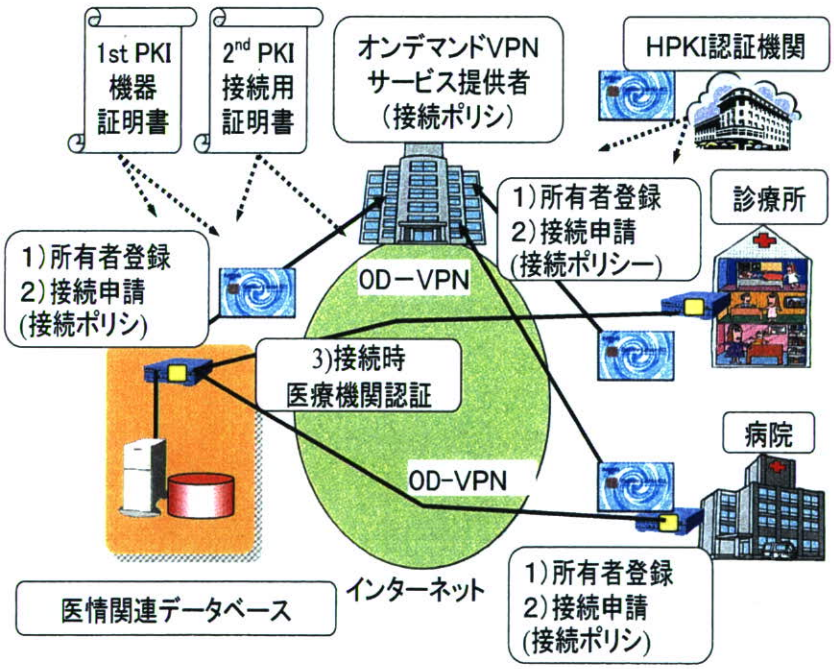

図３　ＨＰＫＩ連携ダイナミック・オンデマンドＶＰＮ

ダイナミック・オンデマンドVPNはセキュアチップによる２階層PKIを利用してオンラインで接続相手先を容易に切り替える事ができる。ダイナミック・オンデマンドVPN方式の医療応用はHEASNET(保健・医療・福祉情

報セキュアネットワーク基盤普及促進コンソーシアム)を中心に普及活動が行われている。[7]
特にオンラインレセプトの場合にインターネットを経由して支払機関へ接続するための受信手段の一つとして支払機関側が準備している。[8]

6．個人提供用健康診断結果報告書

日本HL7協会のCDA SIGでは患者診療情報提供書のCDA R2準拠フォーマットでの標準化を行い、HELICS規格としても採用された[9]。一方、特定健診による生活指導が2008年より始まり、健診データの保険者による保管と健診機関からの電子データの送付が計画され、そのフォーマットの規格化が進められている[10]。

特定健診でのフォーマットは波形や画像をデジタルで提供することを目的としていない。また、健康保険組合等が健康指導を行う為のもので、個人へ提供し、個人が健康管理や診療に活用することを直接の目的としていない。そこで、特定健診のフォーマットと互換性があり、必要により波形や画像もデジタルで提供可能で且つ、個人に提供することを目的としたフォーマットを提供することを目的とした個人提供用健康診断結果報告書の検討がHL7協会のCDA-SIGで行われている。

今回のシステム構築に当たっては、データの本文は検討されている「個人提供用健康診断結果報告書」V0.4に基づいたXMLの標準形式(CDA Release2.0)に準拠した。その中で画像データについては、医用画像の標準であるDICOM (Digital Imaging and Communication in Medicine)形式で保存し、心電図等の医用波形についてはMFER (Medical waveform Format Encoding Rule)形式とされている。健康管理データは、データ本文、添付データ(画像データ、波形データ等)及びメタデータをパッケージ化し、パッケージデータを圧縮して取り扱う。圧縮の際はこのフォルダ構成を保ったまま圧縮し、フォルダ構成はIHE-PDIに準拠した[11]。

7．「電子私書箱構想による個人健康情報参照システム」の構築

以上、説明してきた電子私書箱構想、社会保障カード構想、HPKI連携ダイナミック・オンデマンドVPN, 個人提供用健康診断結果報告書様式を用いて「個人健康情報参照システム」のプロトタイプを構築した。図4に詳細を示す。

現在、健診システムの結果報告は現在、紙で配布されているのが通常であるが、これを、デジタルデータで入手するためにオンラインで電子私書箱と呼ばれるサーバに送付する。このデータは親展扱いで、受診者の公開鍵で暗号化されている。受診者はこれを医師に見せたいものあるいは保管したいものを暗号化して電子私書箱に保

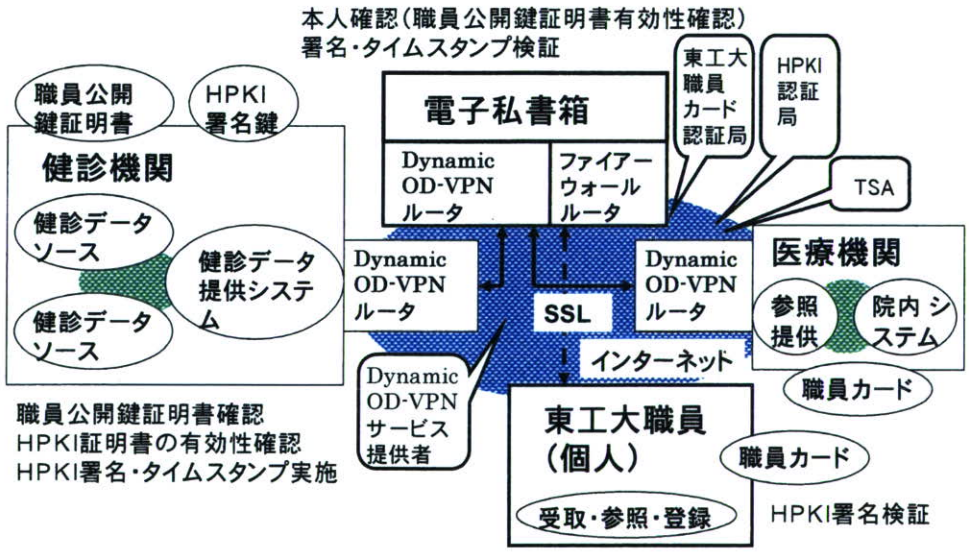

図4　電子私書箱構想による個人健康情報参照システム

管する。このとき、提供データには健診機関の署名およびタイムスタンプを施す。

また、オンデマンドVPNは健診機関と電子私書箱間および電子私書箱と健診データを参照する医療機関の間のセキュアなネットワークとして利用した。ダイナミック・オンデマンドVPNはHPKIの署名を行いフリーアクセス可能なＶＰＮを構成した。

個人が電子私書箱にアクセスする場合はコストパフォーマンスを配慮してＳＳＬを用いた。アクセスカードは社会保障カードはまだ検討中であるので、東工大の職員カードがそれに近いものと予想されるので東工大の職員カードを用いておこなった。

本「電子私書箱構想による個人健康情報参照システム」のプロトタイプ構築により公開鍵基盤を活用するための技術的方策」の検討をおこなった。

C. 研究結果

1．プロトタイプシステムの構築

本方式により、個人宛に送られた画像や波形を含めた健診機関からのデータを電子私書箱に相当するサーバ経由、PKIカードによりアクセス認証および暗号を復号して安全に受け取り、必要なデータを電子私書箱に登録して、必要に応じ、医療機関に提示できることを確認した。また、データの真正性をHPKI署名の確認によりおこなえることを確認した。

図5に構築したプロトタイプシステムの外観を示す。

2．プロトタイプシステムの動作確認

シナリオに基づき、動作確認を行った。以下にそれぞれの動作について述べる。

2．1 健診データ入力

健診センター用PCにインストールされた専用APを利用し、ユーザ情報に関する情報や健康診断に関する情報

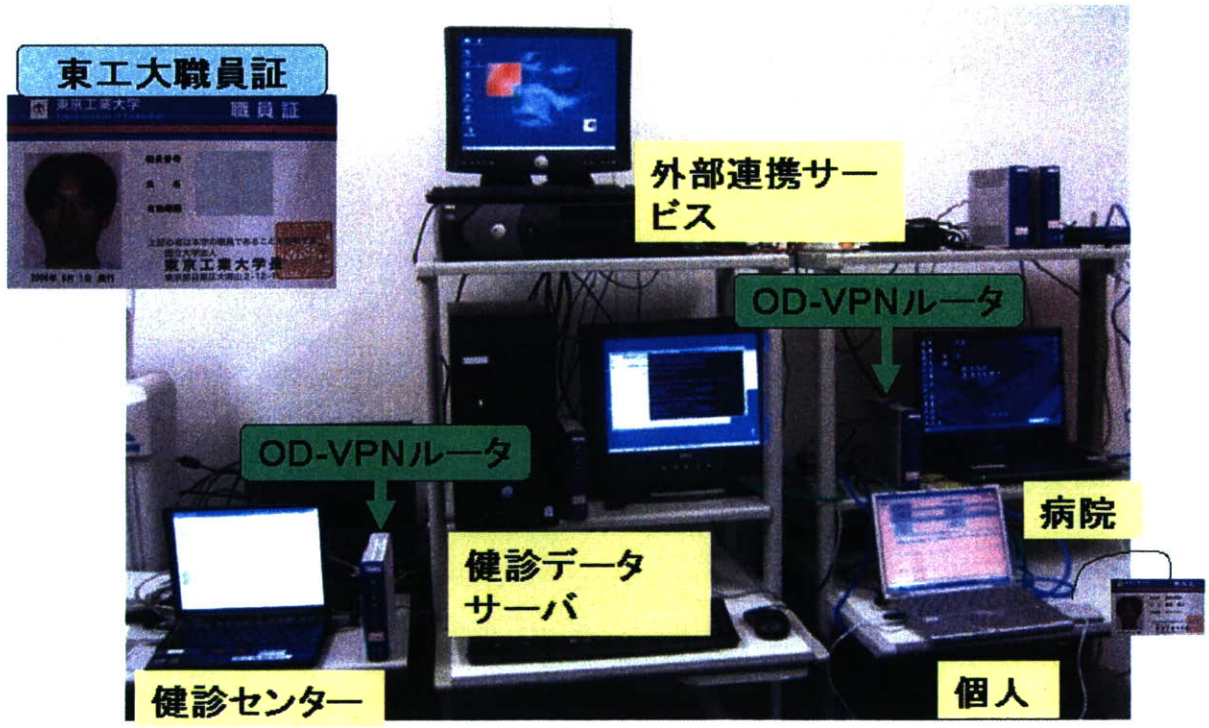

図5　プロトタイプシステムの概観

を登録した上で、検体検査、問診、画像、波形等の結果を入力した。また、検索等に必要な情報をメタデータとして入力した。ユーザ登録の際には、健康管理データを暗号するためのユーザの公開鍵証明書を登録した。

2．2　健診センター・電子私書箱のオンデマンド VPN 接続

オンデマンド VPN 用管理 AP を利用して、電子私書箱へ接続要求をおこなった。接続要求する前には、サーバ条件、クライアント条件を登録し、接続合意を取った。

2．2　健診センターから電子私書箱へのデータ送付

オンデマンド VPN の接続完了後、健診センターの専用 AP を利用して電子私書箱へデータを送付した。この際、標準フォーマットへの変換、データの圧縮、電子署名、タイムスタンプの付与が行われるのを確認した。

2．4　電子私書箱から個人用 PC へのダウンロード

ユーザ PC の専用 AP を利用して健診データをダウンロードした。ユーザは電子私書箱へアクセスすると認証要求が来るので、東工大職員カードの IC カードを利用してユーザ認証を行った。認証成功後、電子私書箱上のデータ一覧が表示されるので、必要なデータを選択し、ダウンロードした。ダウンロードしたデータは、メタデータは表示されるが、データの本体は暗号化された状態なので
見ることはできないことを確認した。

2．5　個人用 PC でのデータ復号化および閲覧

ユーザ PC の専用 AP を利用して健康管理データの復号化を行った。復号化されたデータには参照用 Viewer があるので、これを利用して健診結果のデータを閲覧した。また、参照用 Viewer を利用して電子署名およびタイムスタンプの検証を行うことができた。

2．6　個人用 PC へダウンロードしたデータの電子私書箱への登録

ユーザ PC の専用 AP を利用して電子私書箱からダウンロードしたデータを電子私書箱へ登録するためのデータフォーマットへ変換した。Web ブラウザから電子私書箱へアクセスし、職員証を利用したユーザ認証を行った。電子私書箱へ登録するデータを選択し、登録を行った。

2．7　健診機関より提供されたデータの電子私書箱への直接登録

ユーザ PC の専用 AP を利用して電子私書箱上の健診機関より提供されたデータを個人用 PC へダウンロードせずに直接電子私書箱の参照可能なように登録する機能を確認した。登録が完了すると Web ブラウザが立ち上がり、健診結果を参照できた。

2．8　個人用 PC から電子私書箱に登録されている健診データの参照

電子私書箱へアクセスし、ユーザ認証を行った。メニューの中から、一覧もしくは検索によって参照するデータを選択し、健診結果を参照した。画像や波形も Web ブラウザ上で閲覧可能であった。また、電子署名およびタイムスタンプの検証結果を確認することができた。

2．9　病院内 PC でのデータ参照及びダウンロード

病院内の PC で参照する場合には、まず病院と健診情報管理サーバとの間をオンデマンド VPN 接続する。その後ユーザの PC と同様に電子私書箱へアクセスし、健診結果を参照する。また病院の場合にはデータのダウンロードも可能であり、ダウンロードしたデータはユーザ PC で復号化したデータと同様に専用 Viewer を用いてデータを閲覧可能であった。

D．考察

1．「法令で定められた記名・押印を電子署名で行うことについて」の最低限のガイドライン

記名・押印を電子署名で行うことに対して、「医療情報システムの安全管理に関するガイドライン」の第6．12章にあげられているので、考察の参考とするために抜粋する。[12]

1．1　厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野PKI認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと

1）　保健医療福祉分野PKI認証局については、電子証明書内に医師等の保健医療福祉に係る資格が格納された認

証基盤として構築されたものである。保健医療福祉分野において国家資格を証明しなくてはならない文書等への署名は、この保健医療福祉分野PKI認証局の発行する電子署名を活用するのが望ましい。
ただし、当該電子署名を検証しなければならない者すべてが、国家資格を含めた電子署名の検証が正しくできることが必要である。

2）　電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくても制度上の要件を満たすことは可能であるが、少なくとも同様の厳密さで本人確認を行い、さらに、監視等を行う行政機関等が電子署名を検証可能である必要がある。

3）　「電子署名に係る地方公共団体の認証業務に関する法律」（平成１４年法律第１５３号）に基づき、平成16年１月29日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者がすべて公的個人認証サービスを用いた電子署名を検証できることが必要である。

１．２　電子署名を含む文書全体にタイムスタンプを付与すること。
1）　タイプスタンプは、「タイムビジネスに係る指針ーネットワークの安心な利用と電子データの 安全な長期保存のためにー」（総務省、平成16年11月）等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能であること。

2）　法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。

3）　タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を講じる必要がある。

１．３　上記タイムスタンプを付与する時点で有効な電子証明書を用いること。
1）当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば、電子署名を含めて改変の事実がないことが証明されるために、タイムスタンプ付与時点で、電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。

１．４　要求事項に対するプロトタイプシステムの結果
ガイドラインにそってHPKIによる署名および指定されたタイムスタンプを利用した。

2.「電子保存の要求事項について」の内、「真正性の確保について」で使用する場合
真正性確保のための推奨されるガイドラインの中に電子署名の要求事項が記載されている。
以下に抜粋する。
２．１　作成・記録責任者の識別及び認証
1）記録の作成入力に関与する利用者識別・認証用に電子証明書を発行し、本人しか持ち得ないよう私有鍵をICカード等のセキュリティ・デバイスに格納する。

2）本人が私有鍵を活性化する際にはパスワードや生体認証等の認証情報を用い、その認証情報が暗号化されずにネットワークへ流れることのないような手段を用いること。また、電子証明書をシステムへの認証用に用いる際は少なくとも端末へのログオン毎に、電子署名用に用いる際には署名毎に私有鍵の活性化を求めること。

２．２　情報の確定手順の確立と、作成・記録責任の識別情報の記録
1）「記録の確定」に際し、作成責任者の電子署名を行うこと。また、確定操作がいつ行われたかを担保するために、確定操作後速やかに信頼できる時刻源を用いたタイムスタンプ署名を行うこと。

2）「記録の確定」に際し、その作成責任者の識別情報が電子署名により記録情報に関連付けられること。この際、署名はICカード等のセキュアなトークン内で行われ

るか、利用者の端末内で行われる場合は署名後に私有鍵の情報が一切残らない方式を用いること。

3）電子署名は保存が義務づけられた期間より長期にわたり署名時点での証明書及び署名の有効性が確認できること。

4）「確定操作」を行うにあたり、責任者による内容の十分な確認が行われたことを確認する手続きを義務づけること。

2．3更新履歴の保存

1）一旦確定された情報は、後からの追記・書き換え・消去等の事実を正しく確認できるよう、当該事項の履歴が保存され、その内容を容易に確認できること。追記・書き換え・消去等の確定操作を行う際には当該部分の変更履歴を含んだ電子署名をおこなうこと。

2．4　要求事項に対するプロトタイプシステムの結果

ガイドラインにそってHPKIによる署名および指定されたタイムスタンプを利用している。

3．健診機関でのＣＲＬチェックおよびＴＳＡ

図４に於いて健診機関は外との接続はダイナミック・オンデマンドVPNだけなので、HPKIで署名を行うときインターネット上にあるＣＲＬ（Certificate Revocation List）にアクセスできないので、健診機関の署名を健診データに施すとき、使用中の証明書が無効になっているか確認できない。

東工大職員カードの有効性もインターネットに接続できないので、データを進展通信するために暗号化する際、受診者の有効な証明書かどうか確認できない。

また、タイムスタンプの為に、ハッシュをＴＳＡへ送付する必要があるが、インターネットに接続していないのでタイムスタンプをつけることができない。

解決策としては

1）ファイアウォール付ルータの併用

2）ダイナミック・オンデマンドVPNサービス提供者経由でＣＲＬおよびＴＳＡに接続する方式がある。具体的には実証が必要で今後の課題である。

前者はファイアウォールに指定されたＣＲＬやＴＳＡとしか、アクセスできないように設定を行う。ファイアウォールの設定は専門的な知識が必要となる。

4．電子私書箱での署名検証

電子私書箱もＶＰＮ接続側はインターネットと接続できないが、ファイアウォールルータ経由でＳＳＬを個人アクセスには許可しているのでＣＲＬとＴＳＡは接続可能である。

5．個人および医療機関での署名検証

個人はインターネットに接続できるのでＣＲＬおよびタイムスタンプの有効性を確認できる。

医療機関はＩＥベースで動いているので、電子私書箱が検証するので医療施設側の機器で検証する必要はない。

6．検証画面

現在は健診データを表示する時に検証ルーチンも走らせて、その結果を表示している。デジタルは簡単に内容が変更できるので、実際の検証範囲がどこまで含まれるか把握できない。

これは今後の課題であり、何らかの検証されたデータの指示ができるようなＧＵＩを検討する必要がある。

7．内部システムとインターネットに接続された機器との接続

正当な理由がない限り、内部システムとインターネットは接続されないのが一般的である。その場合、図４において健診機関においては、健診データソースと健診データ提供システムの間はウイルスチェックやＦＴＰが機能しないなどのアクセス制御機能をもったセキュアなデータ交換を配慮する必要がある。

また、医療機関においても「参照・提供」システムと院内システムの間は同様なセキュアなデータ交換が必要である。

8．キーエスクロ

生涯にわたって健康情報を電子私書箱に保管しておくとなると、暗号化されていると、アクセスカードを紛失

した場合や、変更した場合にアクセスできなくなる。

今回のシステムの健診機関からデータの受取部分は比較的短期であるのでキーエスクロは必要ないかと思われるが、長期にわたって保存される参照部分は何らかの工夫が必要である。また緊急に必要なデータは患者のカードがなくても閲覧できる機能も有効と考えられるが安易に付加せず医療の救急体制全体を勘案してモデル化する必要がある。

9．国際的な医療情報保護の取り組みとの整合性

Healthcare PKIの規格であるISO17090と整合性をはかった。公的資格を示すhcRole もこの規格に整合して定義されている。しかし、ＩＥを利用して証明書の検証を行うと、OID表示になってしまう。

HPKI検証専用のソフトウエアを提供する必要がある。この場合、チェック項目が正しくチェックされるか検証する第三者機関が必要となる。

E．結論

「電子私書箱構想による個人健康情報参照システム」を構築してHPKIの保健医療福祉分野に適した公開鍵基盤の構築」及び、医療機関内外において個人情報・医療情報等の安全性を確保するために必要となる「公開鍵基盤を活用するための技術的方策」を検討した。

健診機関と電子私書箱間および、電子私書箱と医療機関間のセキュアなチャネルとしてHPKIと連携することによりフリーアクセスが可能となるダイナミック・オンデマンドVPNを使用した。

その結果、インターネットに接続できない状況が発生し、ＣＲＬチェックを必要とする場合はタイムスタンプの実施や署名、暗号化ができない。また、署名検証やタイムスタンプ検証ができない。

対策としては、新たなＬＡＮの口を作り、ファイアウォールルータで特定のＣＲＬやＴＳＡとしか接続できないように設定する必要がある。あるいは、ダイナミック・オンデマンドVPNサービス提供者がＶＰＮを経由してＣＲＬやＴＳＡに安全に結合する方法、オフラインでＣＲＬを提供する方法がある。いずれにしても具体的には実証が必要で今後の課題である。

また、長期にデータを保管する場合はカード紛失、更新や緊急アクセスにそなえてキーエスクロのポリシを定めておく必要がある。

また、証明書ポリシはISO 17090 と整合性がとられている。しかし、既存のＩＥ付属のブラウザでは表示できない項目もあり専用の検証プログラムを作成する必要がある。

F．参考文献

[1] 重点計画2007 本文, 2007, http://www.kantei.go.jp/jp/singi/it2/kettei/070726honbun.pdf

[2] 重点計画2007 概要、2007, http://www.kantei.go.jp/jp/singi/it2/kettei/070726gaiyou.pdf

[3] 保健医療福祉分野PKI 認証局 証明書ポリシ, 2006年3月 http://www.mhlw.go.jp/shingi/2006/03/dl/s0330-8a.pdf

[4] MEDIS-DC HPKI 署名用電子証明書発行サービス, http://www.medis.or.jp/8_hpki/index.html

[5] ISO17090, Health informatics - Public key infrastructure -

[6] 喜多紘一. HPKI とダイナミック・オンデマンドVPN との連携によるセキュアな医療ドメインネットワーク. 第27回医療情報学連合大会, 2007, 1-H-3-2

[7] 保健･医療･福祉情報セキュアネットワーク基盤普及促進コンソーシアム, http://www.heasnet.jp/

[8] 社会保険診療報酬支払基金, インターネットによるオンライン請求について, http://www.ssk.or.jp/claimsys/claimsys09.html, 2008

[9] HELICS 協議会,「医療情報標準化指針」提案申請･採択状況, http://helics.umin.ac.jp/

[10] 大江和彦, 健診データの電子的管理の整備に関するホームページ, http://tokuteikenshin.jp/

[11] 喜多紘一, CDA R2 に準拠した個人提供用健康診断結果報告書を利用した個人健康情報管理システム, 第27回医療情報学連合大会 2007, P7-4

[12] 厚生労働省, 医療情報システムの安全管理に関するガイドライン 第3版, http://www.mhlw.go.jp/shingi/2008/03/s0301-2.html

厚生労働科学研究費補助金（医療安全・医療技術評価総合研究事業）
分担研究報告書

薬務関連における個人情報管理の実施方策の調査・検討

分担研究者　土屋文人　東京医科歯科大学歯学部附属病院薬剤部部長

研究要旨　薬物療法が中心の我が国において、患者に使用されている薬剤の情報を共有することは極めて重要であるが、現行の情報システムでは対応がうまくできていないのが現状である。持参薬と平成20年度から実施される後発品推進策を中心として、患者の薬物療法に関する情報管理の現状調査と情報を有効に活用するための方策について検討を行った。現行の病院情報システムの薬剤関連マスタ、データベース構造は抜本的な改造が必要であり、第一段階としては全件マスタの採用が必要不可欠である。これにより、従来使用されることが少なかった医薬品標準マスタが広く普及すると思われる。また、患者の薬物療法に関する情報共有のためには、調剤情報の電子化による共有化が有効だり、これは処方せんの電子化とは別に検討が可能であることから、早急に調剤情報の電子化のための検討を行うべきである。

A. 研究目的

平成19年4月に施行された改正医療法により、医薬品の安全使用に関する手順書を定めることが全ての医療機関及び医療提供施設である薬局に義務化された。厚生労働省医政局長通知により、手順書に最低限含む項目として示されたものの一つに、医療機関と他の医療機関・薬局との連携に関する項目がある。このことは、外来であれ、入院であれ、薬物療法を受けている患者に対して、切れ目のない薬剤師による支援が行われていることを目的としているが、これを情報として考えるならば、患者が入院時に持参する医薬品、即ち「持参薬」に関して、情報の共有化を行うことを促しているととらえることができる。

我が国においては、処方せんの電子化については、ｅ－文書法においても例外とされ、また、今年度の厚労省の検討会においても、時期尚早との結論になっている。しかしながら、医療安全の観点から前述のごとく、患者が服用（使用）している医薬品に関する情報を共有することが極めて重要であることから、処方せんの電子化は別として、処方された薬剤の情報を共有化する仕組みを検討することが求められることになる。

そこで本研究においては、患者に使用される薬剤の情報管理をどのように行うかを検討することを目的として、持参薬に関する問題点及び平成20年度から実施される後発品推進策における情報処理上の問題点について調査・検討を行う。

B. 研究方法

昨年度の調査で明らかになった、持参薬及び後発品に関する諸問題の解決状況を調査するとともに、依然として残されている

問題や新たに出てきた問題についても調査を行うこととする。

（1）持参薬に関する情報共有について

持参薬管理に関する学会発表や各種団体等が持参薬管理について行っている調査を基本として、情報管理の電子化がどのような状況にあるのか、また、それを解決するための方策について調査検討を行う。

（2）後発品推進策が情報共有化等に及ぼす影響について

平成20年度に実施される後発品推進策が患者が使用している薬剤に関する情報共有化にどのような影響を及ぼすのかをベンダーや薬局薬剤師から情報収集し、その対応策を検討する。

C. 研究結果

（1）持参薬に関する情報共有について

持参薬に関しては、各医療機関で様々な対応がとられているが、それらの多くは自己の施設における情報管理が殆どで、情報共有を示す事例は殆ど見られなかった。医療機関が持参薬の調査を行う場合には、多くのところで、持参薬そのものの鑑別を自施設で行っていた。お薬手帳を利用している施設も存在するが、お薬手帳が必ずしも情報の一元管理にはなっていないため、その利用には限界があることが示されている。一方、病院情報システムでは、持参薬に対応できるシステムは殆どなく、システム化している施設においても、薬剤部門システムでの対応にとどまっており、医療機関で情報共有を一元管理できない実態が確認された。また、病院情報システムにおいては、相変わらず採用薬マスタを使用しており、持参薬や後発品への変更に対応するために全件マスタとしている施設は殆ど存在していないことが明確になった。

（2）後発品推進策が情報共有化に及ぼす影響について

平成20年度に実施される後発品推進策は、処方医が後発品への変更を禁止しない限り、原則として後発品への切替を医師への問い合わせなしにできるようにするものである。これにより、処方情報と調剤情報は原則的には一致しないという事態を迎えることとなる。

後発品推進策に対する医師側の懸念は、後発品に対する不安、特に後発品への切替による新たな副作用の発生及び有効性が異なることがあり得ることに対する不安が主なものであった。また、情報処理の面からは、保険薬局から調剤情報が返却されても、現行の病院情報システムではそれを反映するような受け皿が構造上用意されていないことから、事実上対応不能であることに対する大きな懸念が示された。

D. 考察

持参薬の問題にせよ、後発品推進策に関する問題にせよ、現状の病院情報システムでは、その構造上対応ができないことは大きな問題である。この問題を解決するためには、まず病院情報システムで使用するマスタを現状の採用薬マスタから全件マスタへと変更することが必要となる。このことは、現状の病院情報システムにおいて多少の改造を行えば対応可能である。我が国においては医薬品標準マスタが存在しながらそれが使用されない実態が存在する。しか