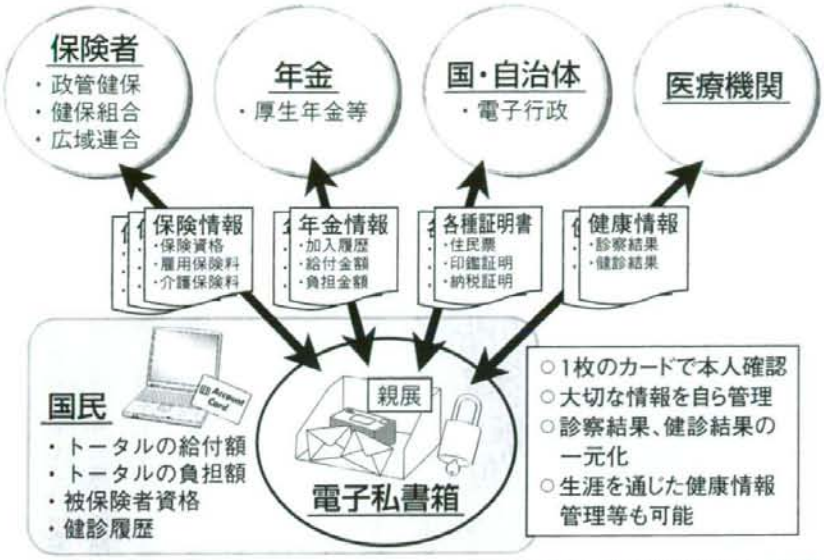
電子私書箱の概念図



第39回IT戦略本部(2006年12月)提出資料

行政手続きや健康診断では、依然として紙を用いて結果を通知しているため、多くの手間と費用を要している。たとえば近年始まった年金特別便では、一億人の被保険者への通知に三〇〇億円近くの経費を要しているばかりか、住所情報の不備等に起因して、本人に届かない例が多数あると言われている。この電子私書箱を使えば、少なくとも安全かつ確実に電子データを本人の私書箱に提供できるようになる。もちろん提供された情報は、パソコンだけではなく、郵便局やコンビニなどに設置された専用端末や多機能のコピー機、さらには地上波デジタルテレビ受像機など多様な手段で内容確認ができる環境を整備することも必要である。

実現・普及には社会の受容性と十分なセキュリティが鍵

電子私書箱を実現・普及するためには、社会の受容性を十分考慮しなければならないが、この点については銀行口座が大いに参考になる。銀行口座は、給与の振り込みや公共料金等の自動引き落とし等、本人がマネーフローのコントロールに使っているのに対して、電子私書箱は個人情報のフローをコントロールするものと例えることができる。銀行口座が社会に受け入れられている現状を参考にすると、電子私書箱においては、①私書箱事業者は社会に信頼されること、②送受信する情報の接続先は本人がコントロールできること、③電子私書箱内の情報は常に確認できることを満たすことが不可欠であると言える。

電子私書箱は機微に触れる個人情報を取り扱うので、十分なセキュリティを確保しなければならない。そのためには、全ての私書箱に鍵を掛け、開錠は本人が保持するICカード等のセキュアなデバイスでしかできないようにすることが必要である。そして、PKI(公開鍵管理システム)を用いた親展通信機能を使って、私書箱内にある情報(リンク情報またはデータ実体)を全て暗号化し、本人が使用するICカード内に記録された秘密鍵でしか復号化できないようにすれば、情報の安全性を大幅に向上させることも可能になる。さらに、送受信される情報やデータの真正性と完全性を確保するために、全ての情報等に電子署名を付し、署名の有効性を私書箱事業者が代行すれば、電子私書箱の信頼性と利便性を大幅に向上できると考えられる。

社会保障カードとの連携が活用の幅を拡げる

以上が、電子私書箱の基本的な考え方であるが、二〇〇七年度から開始された政府内の検討は、新たに公表された社会保障カードとの連携を踏まえたものになっている。社会保障カードは、年金手帳、健康保険証、介護保険証等の役割を一枚のカードに集約するものとされているが、このカードを電子私書箱へのアクセスカードにすることで、カード内に記録する情報の書き換えを極力少なくすること、各種証明書の更新時にカードを必要としないこと(新たな証明書は電子データとして電子私書箱に送られる)など、一億枚を超えるカードの運用を簡素化することも念頭に置かれている。一方、この運用方式では、健康保険証が希望者ではなく全国民を対象とすることから、いわゆるユニバーサルサービスになるため、社会保障カードと連携する電子私書箱の基本機能は、社会保障サービスの一環として提供することが不可欠になる。さらにこの運用であれば、社会保障カードと住民基本台帳カードの統合等も視野に入れることが可能となり、公的個人認証サービスの普及や機能拡張等、政府内で別途検討されている課題の解決にも資するのではないかと期待されている。

他方この考え方に従うと、電子私書箱の基本機能もまた、ユニバーサルサービスになるため、民間が直接行うことは困難となり、必然的に官主導になると思われる。現在の社会情勢を見ると、もし官設でサービス提供を行うとすれば、次世代電子行政サービスを含めた費用対効果に優れたものにすることが必要であろう。

早期実現を強く望む

どちらにしろ、本来の目的である個人の情報を電子的に本人に返し、その情報を本人の意思で活用できるようにすることが必要である。そのためには、電子私書箱、社会保障カード、公的個人認証サービス等の有機的な連携を通して、われわれ国民が、IT新改革戦略に記されているITの恩恵を、電子政府、医療等の分野で実感できる環境を早期に実現することが強く望まれる。そして本人に返される個人情報を、本人の意思で活用するためのさまざまなビジネスが創出され伸展することを期待する。

多目的利用が想定される社会保障カード その欠点をカバーする「電子私書箱」とは?

東京工業大学 像情報工学研究施設 教授　**大山永昭**

社会保障カードの導入に向けた構想と並行する形で検討が進められているのが「電子私書箱」だ。社会保障カードは厚生労働省の検討会、電子私書箱は内閣府のIT戦略推進会議と、ベースとなる議論の場は異なるが、導入が実現すればそれぞれが深く連携して運用されることは間違いない。ここでは、社会保障カードと電子私書箱双方の企画・立案者である東京工業大学の大山永明教授に、その構想について解説していただく。

社会保障カードの機能

社会保障カードの機能は「健康保険証」「年金手帳」「介護保険証」を兼ねるとされている。健康保険は、20歳未満の未成年者も含めた全国民が対象、20歳からは年金が加わり、40歳以上はさらに介護保険が加わるというのが現行の社会保障制度だ。

社会保障カードには、安全性確保の観点からICカードの採用が想定されている。

図1のように、複数のアプリケーションがICチップを共有することを想定しているが、それぞれのアプリケーションは論理的に完全に分離される。アプリケーション同士の間には、ファイアウォールに相当するものが入っており、隣のアプリケーションを覗いたり、あるいは触ることは一切できない。

この仕組みは、すでに住民基本台帳カード（住基カード）で実用化されていて、いわゆる「三者モデル」となっている。「三者」というのは、「カード発行者」「カード利用者」「サービス提供者」のこと。住基カードの場合、発行者は自治体、利用者は住民、サービス提供者は複数存在することになる。利用者が最初にカードを申請すると、基本情報だけが入ったカードが発行され、サービスは後から追加申請すればいくつでも追加できるという仕組みだ（図2）。

1.1億枚規模の発行を想定

ここで、社会保障カードの留意点をまとめてみたい。

まず、その発行規模について、健康保険証を兼ねる場合は10歳以上を対象としても1.1億枚に及ぶ。パスポートは現在4,000万冊ほど出回っていて、年間約450万冊が発行されている。現在のパスポートはICチップが入っているので、社会保障カードの発行についても同程度の手間がかかる。年間2,000万枚発行しても対象者全員に配布するには5年半かかるので、仮に有効期限を5年にした場合は全員に発行し終える前に更新のための発行が始まってしまうことになる。

ICカードの有効期限はセキュリティを考慮すると最長でも10年が限界だろう。年間1,000万枚、10年かけて全対象

図1　多目的利用カードとネットワーク

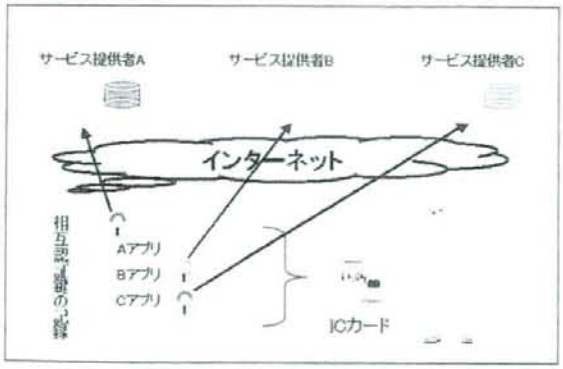
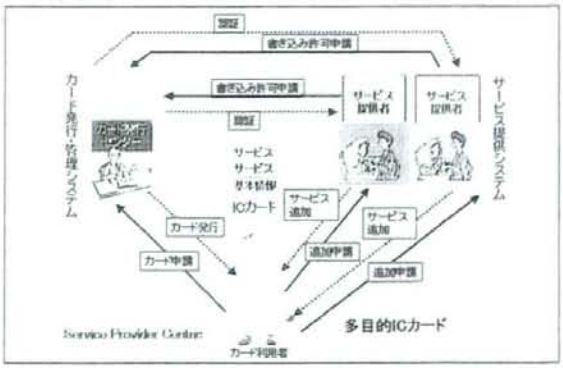


図2　多目的カードの三者モデル



者に発行していくのが順当だが、社会的な状況等を考えるとそれでは通りそうにない。最初にいきなり発行のピークが来てしまう可能性がある。

もとになる生カードやICチップについても大量生産が必要で、メーカーにはそれだけの生産設備を整えてもらわなければならない。価格については、住基カードの例もあるので、1枚500円を切ることに期待している。ただ、券面印刷とか本人確認、公的認証サービスなどをやっていると1,000円は切らないだろう。仮に1,000円でも、1.1億枚では総額1,100億となる。1年間のランニングコストは10年で割って1年で110億。110億円の価値がないと社会保障カードを発行することが難しくなる。

求められる高セキュリティ性

社会保障カードは、年金手帳、健康保険証、介護保険証の3つの機能を備えるため、現行制度のままだと、転職や引越しに伴ってカードに記録される健康保険番号や介護保険番号を書き換えなければならない。安全・確実な書き換えには、高レベルのセキュリティが求められるため、専用の書き換え装置を用意するなどの手段を講じる必要がある。

例えば、クレジットカードの書き換えを自宅でできる人はいないわけで、それを可能にしてしまえば今度は信頼されなくなり、ICカードの意味がなくなる。もし、健康保険番号や介護保険番号を基礎年金番号のように生涯不変にできれば番号の書き換えはなくなるが、依然、有効期限の変更や更新は必要だ。

カード内に記録される番号が3つあるとすれば、これに対するアクセス制限をどうするのかという問題もある。

アクセス制限をかける場合、安全性を考えると、医療従事者は健康保険の情報のみ、介護従事者は介護保険の情報のみをそれぞれ見られる資格が記録されたカードとの併用、という方法がまず考えられる。

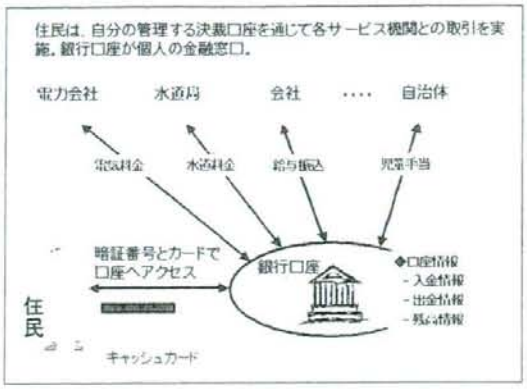
もう1つは、専用端末を使う方法だ。日本には医療関連組織が約22万あるため、クレジットカードのような立派な仕組みを作ることが医療の世界で受け入れられるかどうかはわからない。端末を専用にするというのは、大きな反発を受ける恐れもある。ただでさえ医療費が高騰していている折に、さらに数万円の専用端末の導入を医療機関に求めるのは難しいだろう。

電子私書箱のモデルは銀行口座

以上が社会保障の現状だが、一方で2005年に私が提案した「電子私書箱」という仕組みがある。現在、社会保障カードとの連携が検討されているが、これは多目的カードの欠点を克服するものとして考えられている。

日本社会は急速に高齢化が進行しているため、歳入が低下する一方で社会保障費は増加し、社会的なジレンマとなっている。これを解消するためには、国民の満足と支出のバランスを取らなければならず、用途を含めた社会保障費の透明化が必要だろう。その場合、社会保障費等の情報は機微な個人情報なので、本人開示手段を確保する必要がある。現状では紙で行われており、年金特別便がその一例だが、約1億人の対象者に通知をするのに郵送代だけで80億円、その他のコストを含めると約280億円がかかっているといわれている。

図3　銀行口座の概念



しかし、個人情報の本人開示を電子的にできれば、大幅にコストを下げることができる。電子私書箱導入の目的は、行政や社会保障関連機関が保有している個人情報を電子的に安全かつ安価な形で本人に渡すことである。

電子私書箱の概念は、類似するものとして銀行口座が挙げられる（図3）。銀行口座は、われわれが信頼する銀行に口座を開設して、その中はキャッシュカード、通帳で常に確認できるようにし、どこと接続するかを本人が決めている。もちろん複数持っている人もいて、キャッシュフローをコントロールできるようになっている。

それに対して、電子私書箱は情報フローをコントロールするためのもの（図4）。個人情報を自分が受け取るのか、いらないのか、という判断を含めてコントロールできるようにする。

従って、図式としては非常に似たものになる。私書箱があって、医療機関に検査結果を送ってもらいたい場合は、検査結果が出た時点で私書箱に直接送信してもらう。あるいは情報にひ

も付けた電子的な鍵を送ってもらい、口座を経由して情報を取りにいくという仕掛けだ。

健康保険証を社会保障カードに搭載する場合、私書箱には電子的な健康保険証の情報が送られる。多目的カードだと、医療機関などがカードのどこかを書き換えなければならなかったが、書き換えをせずに必要なリンク情報は全部サーバに置くというのが私書箱の考え方。さらには、行政からのさまざまな通知が私書箱に届いたり、自分から取りに行くことができるようになる。

電子私書箱のセキュリティ

社会保障カードと電子私書箱を連携させれば、多目的カードの欠点をかなり克服できるだろう。私書箱へのアクセスカードになるので、社会保障カードを逆に単目的化できる。また、電子空間でIDを示せば自分の私書箱と繋がるわけだから、身分証明書でも良いことになる。

これにより、住基カードとの並存の可能性も出てくる。社会保障カードと住基カードを1枚化することも考えられるだろう。私見だが、どちらのカードも電子私書箱にアクセス可能にすべきと思う。さらに民間との相乗りも可能になるだろう。

私書箱の運用経費に関する留意点として、個人情報を扱うデータセンターは、情報システムよりも建物の安全性確保や職員の教育・管理に掛かる費用が大きいことが挙げられる。

電子私書箱のセキュリティに関しては、機密性と可用性、それに完全性の確保が必要となる。

機密性の確保とは、簡単に言うと「親展通信」を行うということである。暗号を解く鍵は社会保障カードの中にしかない、という状態にするべきだろう。

可用性の確保には、私書箱を経由するすべての情報が標準的な形式で記述されている必要がある。なかなか標準化が進まない分野もあるが、電子私書箱の導入が逆に標準化を加速する仕掛けになることに期待したい。

完全性の確保も非常に重要となる。例えば、診断書や証明書のようなものは、誰が責任を持って書いたのかが明記されていないと受け取った側は信用できない。例えば、医療の救急情報で、血液型をカードの中に書き込む場合、誰が確認して書き込んだのかがはっきりしなければ、安易に輸血はできないだろう。

「署名付き」というのは、今後非常に重要になる。したがって、電子私書箱に送付される情報は全て電子署名付きで発出元の身元を明確にすること、そしてその署名が有効かどうか、あるいは改ざんされていないかどうかは私書箱事業者が確認すること。これによって利用者に利便性を提供し、信頼性が向上する。

進展通信の原理

図5では、カード側に秘密鍵を格納し、公開鍵が私書箱側にあるという想定にしている。

親展通信の原理は、利用者が情報取得の申請をすると年金事業庁が本人の電子私書箱から認証用の証明書を取得し（私書箱に対するアクセス制限が掛かっているので、そうでないところは取れない）、情報を暗号化してその際に使った鍵「K」を本人の公開鍵で暗号化して「K'」にする。そうすると、この情報を復号化するには、まず「K'」を復号化する必要があり、この復号化は本人の秘密鍵しかできない。「K'」をカードに取り込み、秘密鍵で復号化して鍵「K」を取り出して、それにより元の情報を復号化する。

図6は健康保険証としての利用手順について説明している。

図4　社会保障口座（アカウント）の概念

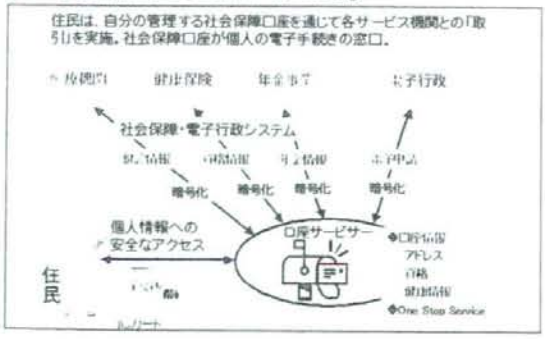


図5　親展通信の原理

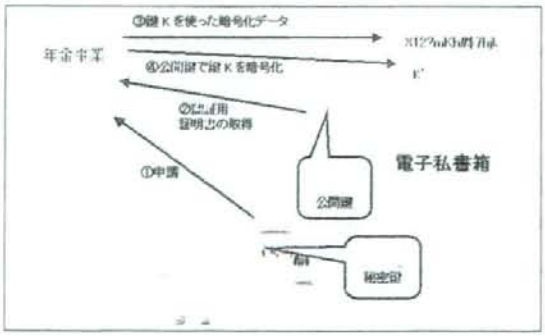
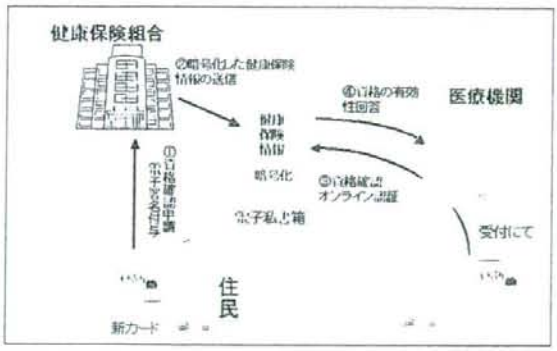


図6　健康保険証としての利用手順



これは、健康保険証用の巨大なデータベースを作らないケース。まず、社会保障カードが導入された時点で、健康保険組合にカードへのリンクを申請する。これは電子申請でもいいし、郵送のやり方もあるだろう。

健康保険組合は、被保険者であることを確認して保険証の情報を私書箱に送る。これでひも付けが終わって、本人は医療機関に行って自分のカードで私書箱内の保険証情報を読んで医療機関に返す。これだと、もしバックオフィス側で保険証の情報に変更があればバッチで送り込むこともできるので、かなり楽になると期待している。もちろんここには健康保険組合のサーバに取りに行くための鍵を置いておくだけの方法もあり得る。

社会保障カードの論点

社会保障カードについての大きな論点を整理すると、以下の4項目が挙げられる。

まず、「根拠となるデータベースをどうするか」である。新たに構築するというのが1つの方法だが、これには多大な時間とコストがかかる。もう1つの方法は、自治体に構築するやり方。これは結果として政管健保と民間保険組合の情報が自治体に帰る可能性を持っている。すでに、自治体の基幹システムの中には国民健康保険を扱っている関係から健康保険の情報を入れる枠が残っているので、そこに作る方法が一番簡単かもしれない。

2つ目の論点は、「カード機能の明確化」だ。PKIを搭載するのは間違いないだろうが、オンライン認証と呼ばれる、署名ではない新しいPKI方式を導入するかどうかを総務省の公的個人認証サービスの利活用の検討会で検討している。

3つ目は、「発行フローの確定」。1.1億枚の発行作業の手間を考えると、発行処理は一括発注だが、交付は分散というのが現実的だろう。

そしてやはり「住基カードとの並存または統合」というのが大きな課題になっていく。

電子私書箱の論点

電子私書箱についても大きな論点がいくつかある。

まず、「ユニバーサルサービスにすべきかどうか」。それに、「実施主体をどうするのか」である。官が行う場合には費用対効果の明確化が必要となるので、「官設官営」でなく「官設民営」が適当だろう。

また、電子署名について2010年問題対策が求められる。暗号の鍵長はRSA1024ビットだと強度に疑問が出てくるので、2048ビットを採用することになると思われる。

まとめ

社会保障カードは健康保険証を兼ねるから発行枚数は0歳を含めると1.2億枚を超える。10歳以上でも1.1億枚。この数をどう処理するか。

カード配布時の本人確認レベルについても、課題がある。現在の健康保険証を受け取る時にどうやって本人確認しているか、年金手帳の場合はどうやっていたか、パスポートを貰うのにパスポートセンターに行くが、その本人確認のレベルはどこまで厳格にやるかによって、交付に要する手間と時間、総経費が大きく変わる。ここも十分な検討が必要だ。

社会保障サービスを受けている外国人も対象になる。根拠となるものは外国人登録証で、自治体の協力を得ないと難しい。

カード利用者の利便性の向上、安全性の確保、カードシステムの柔軟性、次世代電子サービスへの拡張性などいろいろな観点から、電子私書箱を社会保障カードとセットで考えたほうが有効と思われる。

社会保障カードが目指す3つの社会保障サービスを実現するためには、これらを基本機能とする電子私書箱の実現を検討すべきだろう。

また、民間事業者による電子私書箱の活用にも大きな可能性があるのは間違いない。電子私書箱は官による基本サービスと、民による拡張サービスのハイブリッド構造を視野に入れるべきだろう。

情報フローを自らコントロールする住民中心サービスは、世界にまだ例がない。日本はその先駆けとして、この取り組みを世界にはっきりと示すべきではないだろうか。

電子私書箱構想による 個人健康情報参照システムの実現

喜多 紘一　鈴木 裕之　平良 奈緒子　谷内田 益義　本間 祐次　小尾 高史
山口 雅浩　山本 寛繁　大山 永昭

IT戦略本部でまとめられた「重点計画-2007」では「個人が自ら健康情報を管理し健康管理等に活用するための仕組みの確立」および「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の創設」が謳われている。この為には健康情報を個人の自己管理できるサーバに電子的に配送し、患者がダウンロードし、必要なものをサーバに登録し、診療や健康維持のために必要なものを医療機関や自宅で参照するシステムが考えられる。こうした「個人健康情報参照システム」を電子私書箱構想により実現するためのプロトタイプを作成した。今後、東工大の職員の自己の健康管理を想定して実証試験を行う予定であるが、その為には提供データの標準化、GUIの改良および、セキュアなCRLの確認やタイムスタンプの為の制限されたインターネットサイトとの結合を含めたセキュリティポリシーの検討が必要である。コンセルジュ機能の活用も今後の課題である。

キーワード: 電子私書箱, 個人健康情報参照システム, 健康診断, 社会保障カード, 保健医療福祉PKI

The Personal Health information Referring System Based on E-post-office Box Concept : Kita Kouichi Suzuki Hiroyuki Taira Naoko Yachida Masuyoshi Yachida
Homma Yuji Obi Takashi Yamaguchi Masahiro Yamamoto Hiroshige
Ohyama Nagaaki

The IT strategy headquarters of the government organized the Priority Policy Program 2007, in which "Establishment of the structure for every citizen to be able to manage and utilize his health information by himself" and "Foundation of the e- post-office box for the realization of the social security service in aspects of people" are declared. For this purpose, a health information system is considered that health information are delivered electronically to a server where the data is to be individually self-administrated by the owner. A patient can download his dta, register selected necessary data on the server, and refer to selected data for medical examination, treatment and health preservation in any medical institution or home when necessary. We made a prototype system to realize such a "Personal Health Information Referring System" based on the e- post-office box concept. We intend to demonstrate it experimentally on the assumption that it will be used for the self healthcare management of the staffs of Tokyo Institute of Technology. For this experiment the standardization for the format of delivered data, the improvement of GUI and examinations of security policy that includes connections with limited sites through the Internet for the secure confirmation of CRL and "Time Stamp" would be made. Practical use of the concierge function is the further discussion.

Keywords: e-post-office box, personal health information referring system , checkup, social security card, HPKI

東京工業大学　Tokyo Institute of Technology
〒226-8503　横浜市緑区長津田町4259−S1
TEL: 045-924-5303
FAX: 045-924-5747
E-mail: k.kita@gakushikai.jp

1. 目的

1.1. 背景

近年の少子高齢化社会の流れにおいて豊かで創造的な生活を安心しておくる為には、個人ごとに病歴や体質に応じた適切な医療サービスを提供することが必要になる。平成17年12月にまとめられた医療制度改革大綱にもとづく医療制度改革において4疾病(がん、脳卒中、急性心筋梗塞、糖尿病)、5事業について医療計画制度の下で「地域連携クリティカルパス」を基にした医療連携体制の構築が進められ、地域単位の医療機能の分化・連携の推進により、切れ目のない質の高い医療の提供を行うことが要求されている。

また、IT新改革戦略では、重点計画2007において「①病歴や体質に応じた医療の提供、②継続性のある医療の提供、③根拠に基づいた医療の提供を実現するための世界最先端の国民健康情報基盤の構築を目指し、健診結果等の健康情報の個人による活用・全国規模での分析を行う仕組みを2011年度当初までに構築する。」ことが明記されている。具体的には「個人が自ら健康情報を管理し健康管理等に活用するための仕組みの確立」として、個人が健康情報を電子的に入手し、自ら健康管理や診療時における提示等に活用できるよう、健康情報入手及び管理に関するルール等の仕組みについて、2008 年度までに方針を示す。」ことになっている。

1.2. データベースからの観点

データベースの観点から整理すると図1のように大きく分けて3つの観点が考えられる。即ち「診療情報の共有」、「統計情報」および「個人健康管理情報」の観点からのデータベース構築が考えられる。「診療情報の共有」は主に地域連携クリティカルパスのための「専門医からみた情報共有」と、「かかりつけ医からみた情報共有」、その他診療スタッフの利便性を目的としたデータベースである。

「統計情報」の観点からの「データベースは「行政、研究、経営管理のための情報共有」である。「個人健康管理情報」の観点からのデータベースは「個人から見た情報共有」即ち「個人の自己健康管理のための情報共有」である。

前者の2つは今まで議論がなされ、実際にこれまで各種プロジェクトで実証試験あるいは実用化が進められてきたが、個人のデータを生涯記録するためには個人情報保護の観点から言うと情報提供の同意などの実現で満足の行くシステムを構築するには制約が多く、複雑なアクセス制御が必要になる。

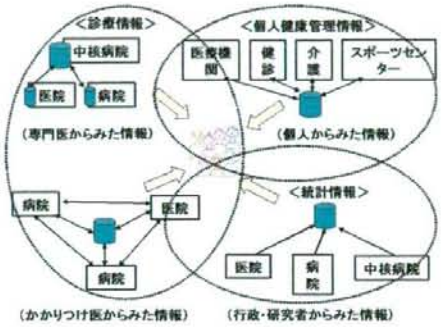


図1 データベースの観点

一方、個人が主体となって構築する方式によるデータベース活用の有効性を指摘する考え方もでてきて幾つかのシステムが検討されはじめている[1]。現在の医療は診療部門や施設が疾患別に細分化して、データが集約されていず、また、医療機関側の保存義務は通常5年であるので、生涯にわたり医療情報を保持するためには個人が主体的に収集することがその解決のひとつと考えられる。

1.3. コミュニケーション手段としての観点

以下のようなシナリオにおいて、医療スタッフと患者あるいは家族間の健康情報共有化の為のコミュニケーション手段が適切な診療にあたり望まれる。

1.3.1. プライマリーケアの場面

患者は自分や家族の病歴を医療スタッフに伝えるのに苦労している。特に複数の病気を持っている場合は他病院での処方を含めた処置や自分の処置の注意点や日ごろの状態を説明する必要がある。こうした場合、記憶があいまいだったり、うまく伝わらない事があり、本人および医療スタッフ側に不満が残るばかりでなく、適切な医療が受けられなくなる

場合がある。過去の検査結果や退院サマリー処方歴があると適切な情報を医療スタッフに提供することができれば医療スタッフとより適切なコミュニケーションがはかれ納得のいく医療サービスを提供されまた、受けることができるようになる。

1.3.2. 検査結果の早期通知

健診結果や定期検査結果を患者にオンラインで提供できれば、結果が提出され次第、患者にしらせることができ、受診者に提供できれば、健診の結果報告の配達や次回の受信日まで不安な気持ちで過ごす必要がなくなる。

1.3.3. 健康相談

データが手元にあれば、セカンドオピニオン等、他の専門家にじっくり別の視点で見てもらうことがやりやすくなる。

1.3.4. 治療経過のコミュニケーション

慢性病や術後の自宅療養において、検査結果を次回までまたずに通知できれば、患者は安心できるとともに、それになった行動をタイムリーにできるようになる。また、患者の日常の症状を記録しおき、医療スタッフに提供できれば適切な治療指針を作成することができる。

1.3.5. 診断書や紹介状のオンライン入手

診断書や紹介状は診療の合間に書かれることが多く、依頼したその日にはもらえず、後日連絡があって取りにいくことが多い。将来電子化されオンラインで受け取ることも構想されている。

1.4. 関連制度の動向

こうした個人へ健康情報を提供する手段として利用可能と思われ、現在検討されている制度として以下のものが期待される。

1.4.1. 電子私書箱

重点計画2007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始を目指す。」と記述されている。これは図2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。

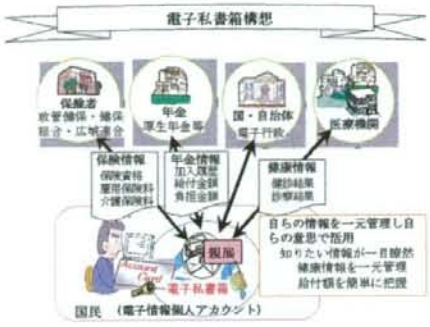


図2 電子私書箱構想

「平成19年3月 IT新改革戦略 政策パッケージ（案）の概要について」をアレンジ

「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。

1.4.2. 社会保障カード（仮称）の推進

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。

1.5. 個人健康情報参照システムの提案

以上の医療改革大綱や重点計画2007を実現する為には、患者や家族の健康管理や医療スタッフとのコミュニケーション手段として、個人ベースで管理されたデータベースが必要になる。

この為には健康情報を個人が自己健康管理できるサーバに電子的に配送し、患者がダウンロードし、必要なものをサーバに登録し、診療や健康維持のために必要なものを医療機関や自宅で参照するシステムが考えられる。

こうした「個人健康情報参照システム」を社会保障カードに期待されるPKI機能と類似した機能を持つ東工大職員カードを利用し、電子私書箱構想により実現するためのプロトタイプを作成したのでその結果を報告する。本構想の実現により、重点計画の「個人が自ら健康情報を管理し健康管理等に活用するための仕組みの確立」にも寄与できることを期待している。

2. 方法

2.1. 電子私書箱の機能

電子私書箱の機能は本年末までに内閣官房の関連検討会で仕様を検討することになっている。ユニバーサルサービスとして実装する部分やその基本部分、オプション部分また民間電子私書箱の担う部分等議論は多いのでどのような実装形態化になるかは見守る必要がある。

電子私書箱を運用するためのアクターを図3に示す。電子私書箱は複数あって、情報提供者および情報受理・管理者はどれかひとつと結合されていて、情報提供者は自分が結合されている電子私書箱に情報を提供すると、その情報の受領者の電子私書箱を探索して受領者の私書箱に提供する。一方、電子私書箱の情報を利用して、サービスを行う、サービス提供者およびバックヤードサービスはすべての電子私書箱に結合できるか、ローミング機能を電子私書箱に持たせる必要がある。実際にどこまで実装されるかはこれからのビジネスモデルの検討によるが、期待される機能を列挙すると以下のようなものが挙げれる。

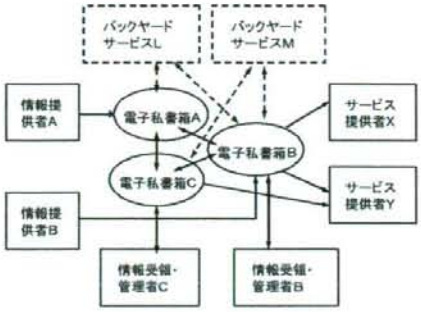


図3 電子私書箱に関連するアクター

① 受取・配送・参照機能(セキュアな本人確認・アクセス制御)
- 公的個人認証としての本人確認と一定レベルの信頼性確保機能
- アクセス管理機能・メタデータによる処理管理機能
- 暗号化機能
- 署名検証機能
- 到達通知機能
- 他の私書箱への転送機能(提供者が提供したデータ)
- 集配機能(受取人が投函したデータ)
- 代行アクセス機能

② 長期保存機能
- 検索・参照機能(参照制御機能・緊急時対応機能)・提供
- キーエスクロー機能
- 個人データ登録機能

③ バックヤードサービスとの連携(WebAPI等)
- シングルサインオン機能(セキュアノード)
- ワンストップサービス機能

④ 電子証明書保管・提示・提出
- 原本管理(コピー制御)機能
- 原本参照・提供機能

2.2. アクセスカードとしての機能

電子私書箱に安全にアクセスするためにはアクセスカードが予想され、社会保障カードがその候補と

して挙がっている。その場合、健康保険証、介護保険証および年金手帳をかねたものが検討されているので、カードの保存情報や発行方式がそこからの制約で決められてくるが、電子私書箱のアクセス機能として最低必要なものは以下である。

① 進展通信及びアクセス制御の為の秘密鍵
② 公開鍵証明書あるいは公開鍵証明書が取得できる識別子(URI等)
③ 個人の私書箱が登録されている電子私書箱の識別子(URI等)

2.3. 個人健康情報参照システムの構成

電子私書箱の機能は本年末までに内閣官房の関連検討会で仕様を検討することになっているので、ここでは、電子私書箱をInBox(受診部分)、ViewBox(登録・保管・参照部分)、コンセルジュ(他のシステムとの連携を行う部分)の機能を持つとした。

また、電子私書箱へのアクセスは社会保障カードなどが議論されているが、本プロトタイプでは東工大の職員を対象に実証試験を行うことを計画しているのでPKI機能をもった職員カードを活用した。

健康管理データに関しては、HPKI署名により真正性を保証し、医師などの公的資格や医療機関等の検証を行うことにより責任の所在を明確にした。

サーバへ登録あるいは参照するシステムのプロトタイプを想定した。この時、医療機関から参照する場合にダイナミック・オンデマンドVPNを使用した。

2.4. プロトタイプシステムのプレイヤーとシナリオ

実験システムを構築するにあたり、以下のプレイヤーを想定する。

個人(ユーザ)
健診センター
健診データサーバ(電子私書箱)
病院
外部連携サービス

特に「健診データサーバ」では、データを個人に提供する機能(提供サーバ相当)をInBox、登録・参照する機能(管理サーバ相当)をViewBoxとする。

また実験システムにおいて想定されるシナリオの概念図を図4に示す。

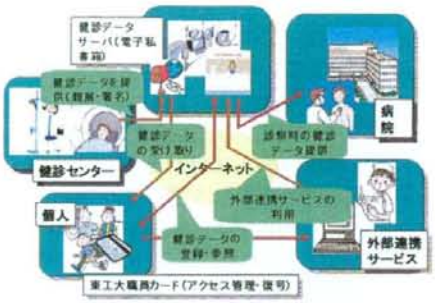


図4 プロトタイプシステムのシナリオ

この詳細を以下に記す。

①健診センターで検体検査、画像診断、心電図、問診等を受診し、健診データ入力アプリケーションによってデータを入力する。

②健診センターと健診データサーバ間をオンデマンドVPN接続する。

③入力された健診データを標準フォーマットに変換し、メタデータ、電子署名、タイムスタンプを付与した上で健診データサーバのInBoxへ送付する。

④ユーザが健診データサーバへアクセスし、自分のInBox内に届いている健診データを個人用PCへダウンロードする。

⑤個人用PCへダウンロードしたデータを復号化し、健診結果を閲覧する。

⑥個人用PCへダウンロードしたデータをViewBoxへ登録する。(選択後)

⑦InBoxに保存されているデータをViewBoxへ登録する。(部分選択無)

⑧個人用PCからViewBoxへ登録されている健診データを参照する。その際電子署名やタイムスタンプの有効性を確認する。

⑨ViewBoxへ登録されているデータを外部連携サービスへ提供し、外部連携サービスを利用する。

⑩病院内のPCからViewBoxへ登録されている健診データを参照またはダウンロードする。その際電子署名やタイムスタンプの有効性を確認する。

2.5. プロトタイプシステムの仕様

2.5.1. 健康管理データ

データの本文は日本HL7協会のCDA-SIGで検討されている「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)に準拠する。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)形式とした。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[2]。

2.5.2. メタデータ

メタデータは、宅配便に添付された荷札のように、健康管理データの中身が誰のどのような種類のデータであるかを特定できる情報のみを記述する。メタデータはXML形式のファイルとして記述し、健康管理データとセットで管理する。

2.5.3. 電子署名

健康管理データに付与する電子署名は、HPKIに基づく電子署名とする。HPKIに基づく電子署名では、証明書の記載内容により資格を確認することができる。電子署名の方式については、Helics規格に準拠してW3C(World Wide Web Consortium)で定める「XML Signature Processing and Syntax」に準拠したEnveloping型の方式とした。

2.5.4. 暗号化・復号

健康管理データは、健診センターで暗号化され、ユーザPCへダウンロード後、もしくは健康情報管理サーバ上に登録されたデータの参照時に復号される。その際の暗号化・復号の仕様は以下である。

①健康管理データ作成時の暗号化

健康管理データの暗号化自体には共通鍵暗号方式で暗号化し、共通鍵暗号の暗号鍵をユーザの公開鍵で暗号化するハイブリッド方式を採用する。暗号化された共通鍵は、健康管理データのメタデータに格納する。

②ユーザPC上での復号化

メタデータ内の暗号化された共通鍵をユーザの職員証内の秘密鍵で復号化し、復号化した共通鍵で健康管理データを復元する。

③健康情報管理サーバ上での復号化

健康情報管理サーバに登録されているデータを参照する際には、参照する健康管理データのメタデータ内に格納されている暗号化された共通鍵をユーザに送付し、ユーザは職員証内の秘密鍵で復号化する。復号化した共通鍵は健康管理サーバへ送付し、管理サーバは受け取った共通鍵で健康管理データを復号化し、ユーザへ情報を提示する。

2.5.5. ユーザ認証

ユーザが健康情報管理サーバへアクセスする際には、東工大職員証を用いたICカード認証を行う。認証方式は、公開鍵暗号方式を用いたチャレンジ&レスポンス方式とした。認証が成功した場合はクライアント側へトークン(Cookie)を発行する。

2.5.6. オンデマンドVPN接続

オンデマンドVPN接続の際は、医療機関のみ接続可能とするため、ポリシーマッピングの条件に医療機関であることを条件とし、その確認方法としてHPKIに基づく電子署名を利用した[3]。

2.5.7. 外部連携

ViewBoxへ登録したデータの中からいくつかのデータを選択し、外部連携サービスを提供するサーバへ出力した。外部連携サービスは送付されたデータを元にサービスを実施し、ユーザへ提供する。今回は健診のデータに対してメタボリックシンドロームに対しての健康相談ができるシステムへのデータ送付とそのシステムの利用を行った。

3. 結果

3.1. 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。

図5 プロトタイプシステムの外観

3.2. 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。

3.2.1. 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化するためのユーザの公開鍵証明書を登録した。

3.2.2. 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。

3.2.3. 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。

3.2.4. InBoxから個人用PCへのダウンロード

ユーザPCの専用APを利用して健康管理データをダウンロードした。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った。認証成功後、InBox上のデーター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。

3.2.5. 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を行った。復号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及びタイムスタンプの検証を行うことができた。

3.2.6. 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した。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った。ViewBoxへ登録するデータを選択し、登録を行った。

3.2.7. 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上のデータを個人用PCへダウンロードせずに直接ViewBoxへ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。

3.2.8. 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。

3.2.9. 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ことを確認した。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を受けることができた。

3.2.10. 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接続した。その後ユーザのPCと同様にViewBoxへアクセスし、健診結果を参照した。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。

4. 考察

4.1. オフライン提供とオンライン提供

個人にデータを提供して生涯管理する場合、オフラインでたとえばUSBメモリーに入れて持ち歩けば良いとの考え方もある。しかしこうした場合、健康情報の提供側のデータが揃うまで待つか、USBを預けておくなど運用に制限がでてくるので、電子私書箱のように中継できるノードを介するほうが運用効率が上がると考えられる。

4.2. 私書箱とS/MIMEとの比較

健康情報を暗号化して送るならS/MIMEで十分との議論がある。しかし、電子私書箱の特徴は配送先が住民票に裏打ちされたレベルでの本人確認ができているノードであることやセキュリティ上高度に保護されていることなど、送り手や受け手に対する安心感や個人情報保護や法的な本人到達の根拠としても使えることが期待される点で異なっている。

4.3. キーエスクロー

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り、変更した場合に復号できなくなる。何らかの代理カード等の手段が必要になる。今回のシステムのInBoxは保存期間が比較的短期であるのでキーエスクローは必要ないかと思われるが、長期にわたって保存されるViewBox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。

5. 結論

今後、東工大の職員の自己の健康管理を想定して実証試験を行う予定であるが、その為には提供データの標準化、GUIの改良および、セキュアなCRLの確認やタイムスタンプの為の制限されたインターネットサイトとの結合を含めたセキュリティポリシーの検討が必要である。コンセルジュ機能の活用も今後の課題である。

6. 謝辞

セキュリティの基礎技術開発は情報通信研究機構委託研究:「ネットワーク認証型コンテンツアクセス制御技術の研究開発」において行われた。
電子私書箱の医療応用構想部分は文部科学省科学技術振興調整費による支援を受けている。

参考文献

[1] 静岡県版電子カルテシステム. http://www.mi.hama-med.ac.jp/emr/. Michio Kimura, Hamamatu University Hospital.

[2] 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.

[3] 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.

Review Article

The Personal Health Information Reference System based on e-P.O.Box Conception

Kouichi Kita, Joong-Sun Lee, Hiroyuki Suzuki, Naoko Taira, Masuyoshi Yachida, Hiroshige Yamamoto, Yuji Homma, Takashi Obi, Masahiro Yamaguchi, Nagaaki Ohyama

Tokyo Institute of Technology

Abstract

IT Strategic Headquarters of the Japanese government compiled the Priority Policy Program 2007, in which "Establishment of the structure for every citizen to be able to manage and utilize his health information by himself" and "Foundation of the e- Post-Office box for the realization of the social security service in aspects of people" are declared. For this purpose, a health information system is considered that delivers healthcare data to the server, where the data is to be individually self-administered by the owner. A patient can register his data, and download or reference it from any medical institution or home when necessary. We made a prototype system to realize such a personal health data referring system based on the e- post-office box concept. The system is to be used in field trial experiment with the staffs and students of Tokyo Institute of Technology using their ID Card. This prototype system is expected to be available for the policy suggestion in the realization of the e-P.O.Box stated in the Priority Policy Program of the government.
(Journal of Korean Society of Medical Informatics 14-3, 213-220, 2008)

Key words: PHR, e-P.O.Box, e-government, VPN, PKI, HPKI, Health Card

Corresponding Author: Lee, Joong-Sun Ph.D, Associate Professor, Integrated Research Institute
Tokyo Institute of Technology Rm.312-2, S1 Bldg. 4259 Nagatsuta, Midori-ku, Yokohama 226-8503, JAPAN
Tel: +82-45-924-5303, **E-mail:** j-lee@isl.titech.ac.jp

Introduction

Japan is facing unprecedentedly rapid aging society of longevity and low birth-rate shrinking labor force and economic growth with the problems of pension funds and public fiscal sustainability. The medical expenses are expected to rise apace in the coming years making it difficult to keep the balance between satisfaction of service and financial resource. Accordingly, the government is struggling to improve the disease prevention and early detection, and the quality and efficiency of health care, in addition to the health disparity.

To achieve these goals, measures are described in the Priority Policy Program 2007 compiled by the IT Strategic Headquarters of the Japanese government[1]. These measures include the establishment of the structure for every citizen to be able to manage and utilize his own health information and to receive adequate care that is particular to his constitution and medical history. By such structure, interruptions in the health information of patients between various medical institutions are prevented, and higher quality medical care is anticipated based on the analysis of pathologic information and clinical data. The information infrastructure Japanese government will construct is provisionally titled the Personal Digital Documentation Box, alias the e-P.O.Box, aiming for the start of its service in FY2010. With the mechanism of the e-P.O.Box, citizens take control over their own health information that is currently managed separately by medical institutions and health insurers.

We introduce a prototype of the e-P.O.Box Basic System developed for personal health information reference system, whereby health information is delivered from medical institutions to the server, i.e. e-P.O.Box, for patient to manage his own. The patient can access to the server using his ID card, download his information, register other necessary information, and refer to them when required for the treatment or health maintenance from a medical institution or from home.

We plan to do field trial experiment of the developed system with the staffs and students of Tokyo Institute of Technology using their ID Card. This prototype system is expected to be available for the policy suggestion in the realization of the e-P.O.Box stated in the Priority Policy Program of the government.

Methods

Concepts of e-P.O.Box

The introduction of the e-P.O.Box is for the purpose of disclosure of information on a person to the person himself by administrative and social security-related organization. Every Japanese resident is given a personal account in the cyberspace, not mandatorily but by the voluntary application, which is for good social acceptance.

It is just like a bank account through which people manage his monetary flow trusting the baking service provider. The use of the account is fully under the holder's control and the status could be checked at anytime. In the e-P.O.Box service, there are additional functions, such as navigation of public services, letter box to receive and send the confidential mails, and validity check of digital signature etc., having loose connections to the back offices.

The concept of the e-P.O.Box was proposed in the meeting of IT Strategic Headquarters of Dec. 2006, and adopted in the Priority Policy Program 2007. The e-P.O.Box project is supported by the Cooperation of the Cabinet Secretariat, Ministry of Internal Affairs and Communications (MIC), and Ministry of Health, Labor and Welfare (MHLW)[1].

All the e-Government services are expected to be converged aiming for the one stop service, including the social security status check, national pension, health insurance, employment insurance etc. as well as healthcare service of private sector.

The e-P.O.Box is similar to the portal sites and PHR (Personal Health Record) systems already exist in the Internet sites[2-3-4]. However such systems are presently servicing with management of information flow under the service provider's control, not users who usually having 'windows' or 'gates' only for seeing their information. Moreover, the existent services are separately provided by

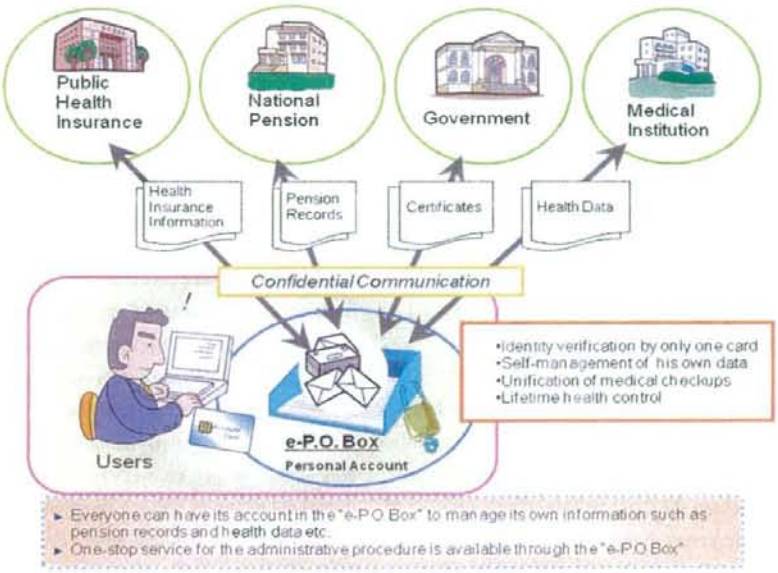


Figure 1. Concept of the e-P.O.Box

local governments, health insurers, and medical institutions. In private services, protection of user's privacy is always concerning matter[5-6].

The e-P.O.Box account has a role of reliable point in the cyberspace trusted publicly and definitely tied to the user, like the address of home in the real world which is registered in the local government. The cyber home position provides a method of certification and qualification of the user in public services to which the access is securely guarded by the use of IC card, supposedly the Social Security Card.

Secure health domain network

In treating personal information through a network, the security must be guaranteed on the communication path from the sender's to the recipient's device protecting the transmitted data from all the threats [7]. For the healthcare information system, Ministry of Health, Labor and Welfare of Japan prepared the minimum guidelines for networks used on the health domain. The e-P.O.Box system is necessary to meet the guidelines to deal with personal health information. The second revision of the guideline issued in March 2007 is as follow[8]:

① Protection must be taken against the threats tampering such as virus injection into the network, wiretapping by crackers, and spoofing such as session hijack and IP address spoofing.

② Authentication is necessary between the sender and the recipient at the entry and exit of their facilities, at their networking devices, at the functional units of these devices, and at other units that the user wants to use.

③ Protection should be made against spoofing as authorized users or devices in the facility.

④ Routers and other network devices must be confirmed safe and routing must be properly configured, so that routers cannot be used for communication with different facilities via a VPN.

⑤ Security measures including encryption of data must be taken by both the sender and the recipient. The encryption keys must conform to the e-government recommended cipher list.

⑥ Responsibilities must be assigned to relevant organizations involved in telecommunication and demarcation points of the responsibility must be clarified

by contract.

⑦ Prevention of unnecessary login during remote maintenance by setting appropriate access points, limiting the protocols to be used, and controlling access privilege, if necessary.

⑧ When signing a contract with a network provider or an online service provider, institutions must make sure that there is nothing wrong with the scope of managerial responsibility for threats and telecommunications quality including line availability and that the above guidelines 1 and 4 are followed.

As a secure network, VPN (Virtual Private Network) is widely used by its reasonable cost, which offers similar functionality and services like a private network even though implemented on the existing shared networks[9-10]. However, there are many types of VPN with various security levels, some not satisfying the government guideline to use in healthcare domain, and others expensive in popular use, but most of them have to do troublesome environment setup whenever to connect with new point. The Dynamic On-demand VPN is considered to be one of the solutions for the problems[11]. The specification is now being proposed to ISO/TC215 WG4 for the international standard in health informatics[12].

The Dynamic On-demand VPN has both advantages of good security level as in IP-VPN and of inexpensiveness of Internet VPN. It has higher authentication level than Internet VPN, and other superiority, such as easy connection establishment between any points on demand and light load for setting VPN environment of users. Furthermore, unlike a conventional network, which is built at the initiative of the providers, Dynamic On-demand VPN is a network platform positioned as a user-initiated social infrastructure that allows dynamically changing user connection policies.

The key feature of Dynamic On-demand VPN is that connection points can easily be changed by simply downloading a new service certificate from VPN Service Provider, so that enabling N-to-N VPN connections. It is allowed by using the double-layered PKI (Public Key Infrastructure) function incorporated in a PKI chip (IC chip) used in a VPN device, router. At the first layer, device authentication is performed using PKI certificate for the device which is registered at purchase by the VPN service provider with the PKI chip. After device

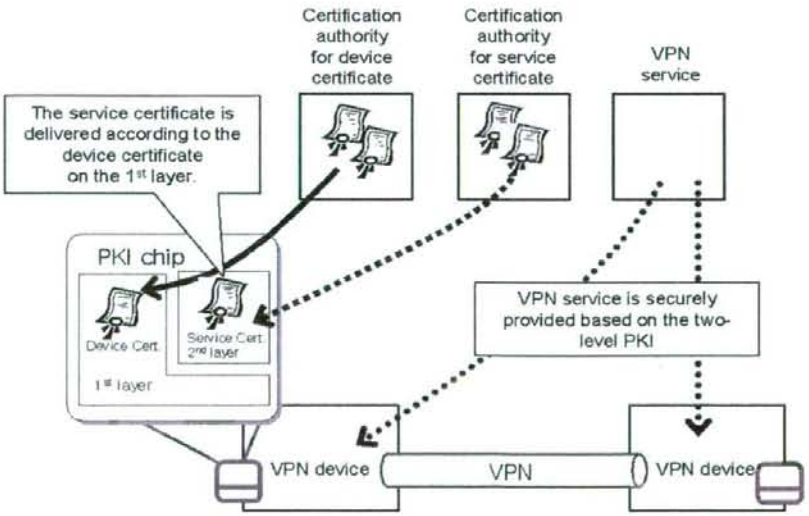


Figure 2. Device and service certificates in a PKI chip

validation, a necessary service certificate is downloaded. At the second layer, the service authentication is carried out using the PKI certificate for the service, and connection information is downloaded, then the VPN service starts securely[13].

With security and flexibility in use, the Dynamic On-demand VPN is applicable as a suitable communication scheme to meet the government guideline for networks used on the health domain[14]. In the application to healthcare region, it is desirable for healthcare institutions to use HPKI(Healthcare PKI) for the digital signature. HPKI is defined in ISO 17090(Health Informatics - Public Key Infrastructure), which contains qualifications and titles of healthcare professionals in the Certificate Extension- hcRole (healthcare role) field. HPKI certificate is issued by MEDIS-DC (Medical Information System Development Center) in Japan[15-16-17].

Social Security Card

In coordination with the e-P.O.Box project, Ministry of Health, Labor and Welfare is going to implement the Social Security Card that will act as a pension book, health insurance card and nursing care insurance card etc. The facial photo of the cardholder would be printed on the surface if required as photo identification card. The card is expected to be an access card to the e-P.O.Box through that the cardholder is allowed to check his pension premium record as well as other information of the public services. The personal record written in the card is so rigidly secured that no one can steel it.

In view of the situation of the health insurance card, the number of the new cards would be 110 millions for people of age 10 or older. The amount of work in issuing a Social Security Card with photo attached and digital signature certificate is comparable to that of e-Passport, which is being issued 4.5 millions per year of total 40 million volumes. As for issue of the total number of Social Security Cards, it takes about five and a half years even at the pace of 20 millions of a year. The fact that the available period of an IC card is at most ten years should be taken into account.

Who issue the Social Security Cards is still under discussion and linking with the resident registration network or not is not yet determined. The Priority Policy Program 2007 states that the Social Security Cards start to be delivered in FY 2011.

Outline of the prototype system

A prototype of the e-P.O.Box Basic System was developed in Tokyo Institute of Technology for personal health information reference system. It consists of three parts, the inBox, viewBox, and the Concierge. The inBox has the function mainly to receive data from healthcare institutions. The viewBox is used to register, store, refer the data in inBox. The Concierge is a bridge for cooperation with external services, which effectively utilizes the personal health data for the user. We plan to do field trial experiment of the developed system with the staff and students of Tokyo Institute of Technology (often called Tokyo Tech). For the experiment, The Tokyo Tech ID card is substituted for the access card of is the e-P.O.Box. The Tokyo Tech ID card has PKI function. Figure 3 shows the schematic diagram of personal health information reference system. In this diagram, the part of the Examination Center is taken out of the laboratory and put in the hospital near Tokyo Tech to collect the medical examination data of users. For the upload from the hospital to the server, HPKI signature is used to confirm the potential authentication of the data[18-19].

The workflow is as follow;

(1) The medical examination data including diagnostic images and electrocardiograms, if any, are digitally signed by the doctors and sent to the account of the patient in the Examination Data Server, i.e. inBox of the prototype e-P.O.Box. The data pass through the OD-VPN(a Dynamic On-demand VPN) Router is encrypted by a secret key of symmetric key cryptography and the secret key is encrypted by patient's public key and attached to the data [20].

(2) The patient accesses to his account with authentication by his ID card, and download the data from the hospital. The secret key used in the encryption of the data is decrypted using his private key packed in the ID card.

(3) The data is decrypted by the secret key. The medical examination data with digital signature of the doctor is securely registered in viewBox at patient discretion.

(4) Dynamic On-demand VPN authenticates the sender to be a healthcare professionals by HPKI and the connection control is performed by the policy.

(5) By HPKI, the referring side of the data can confirm that it is provided by healthcare institution or by a source of the public responsibility.

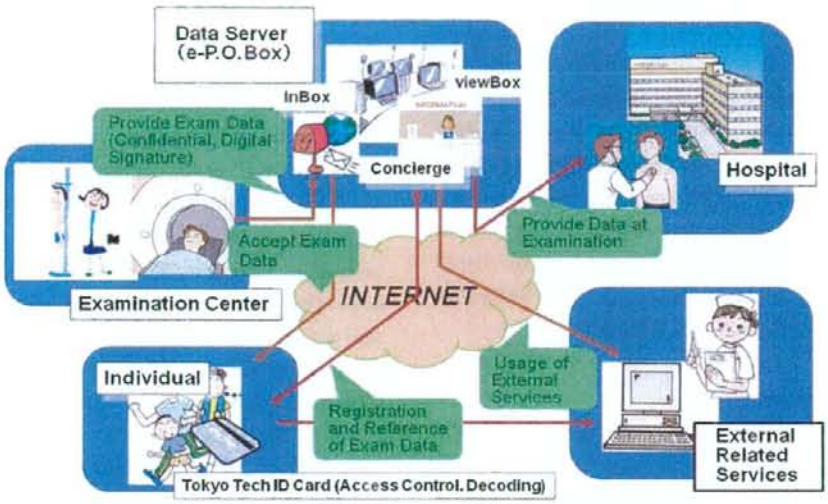


Figure 3. The schematic diagram of personal health information reference system

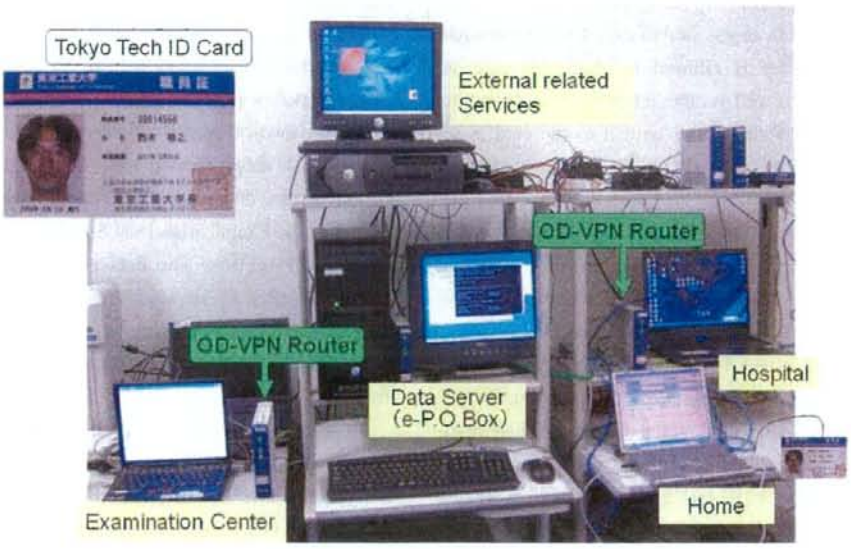


Figure 4. The arrangement of developed proto-type system