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。

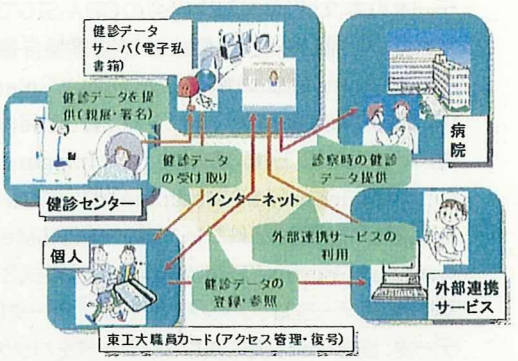

図4 プロトタイプシステムのシナリオ

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。

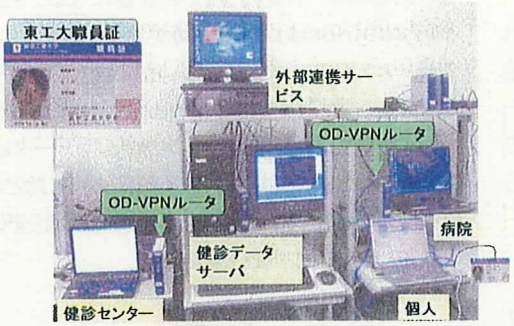

図5 プロトタイプシステムの外観

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

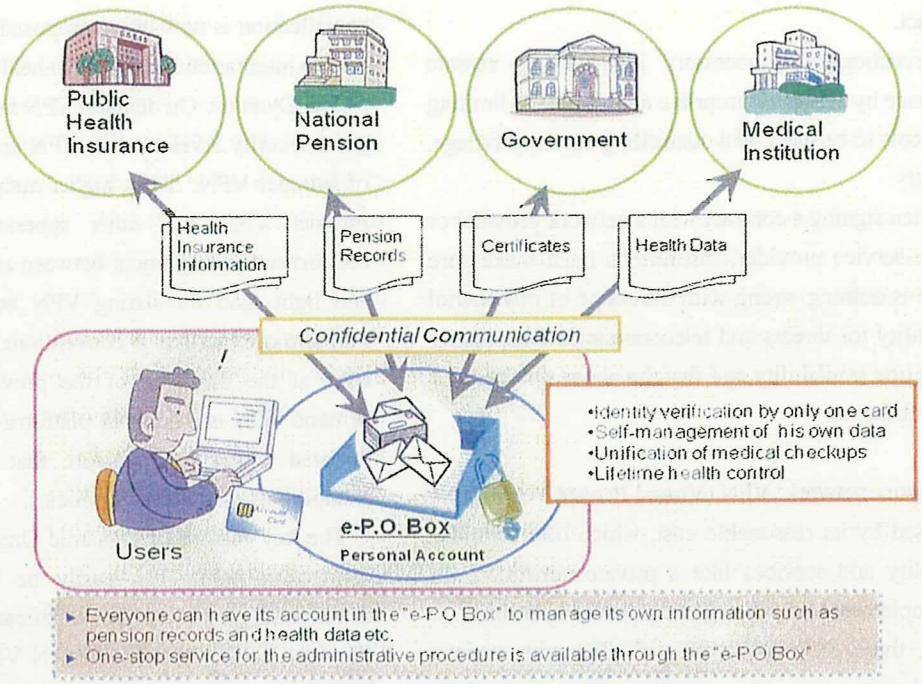

Figure 1. Concept of the e-P.O.Box

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

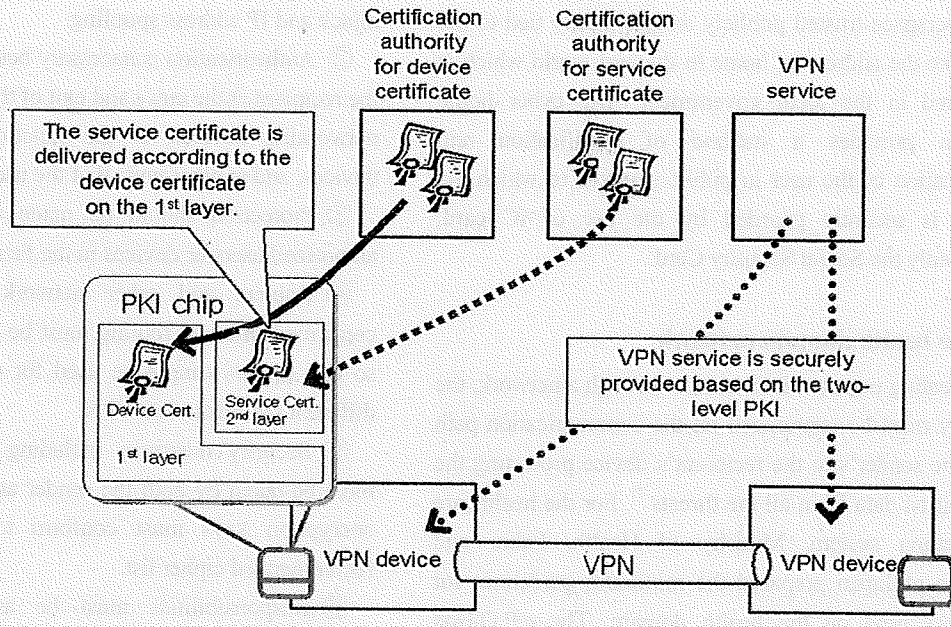

Figure 2. Device and service certificates in a PKI chip

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.

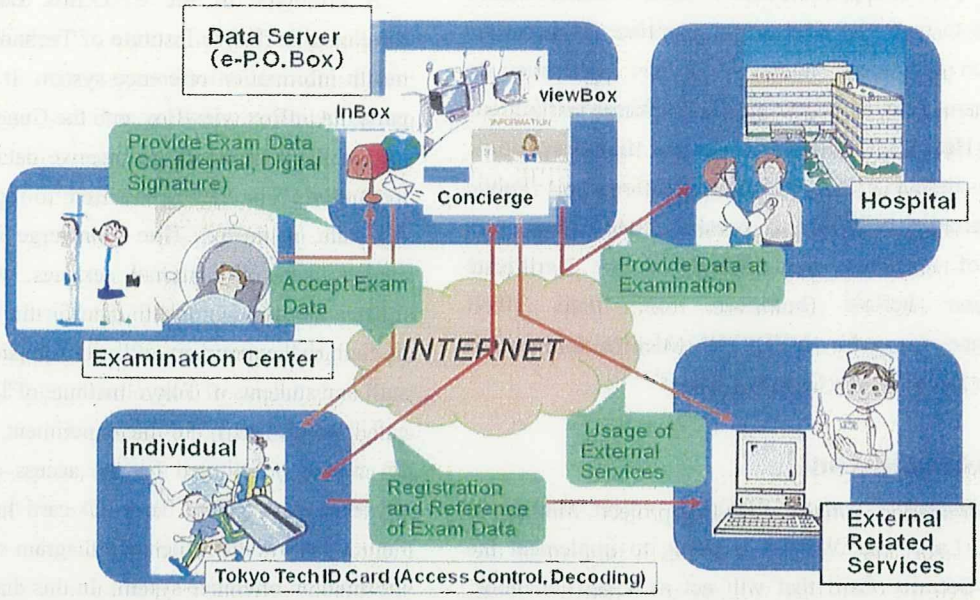

Figure 3. The schematic diagram of personal health information reference system

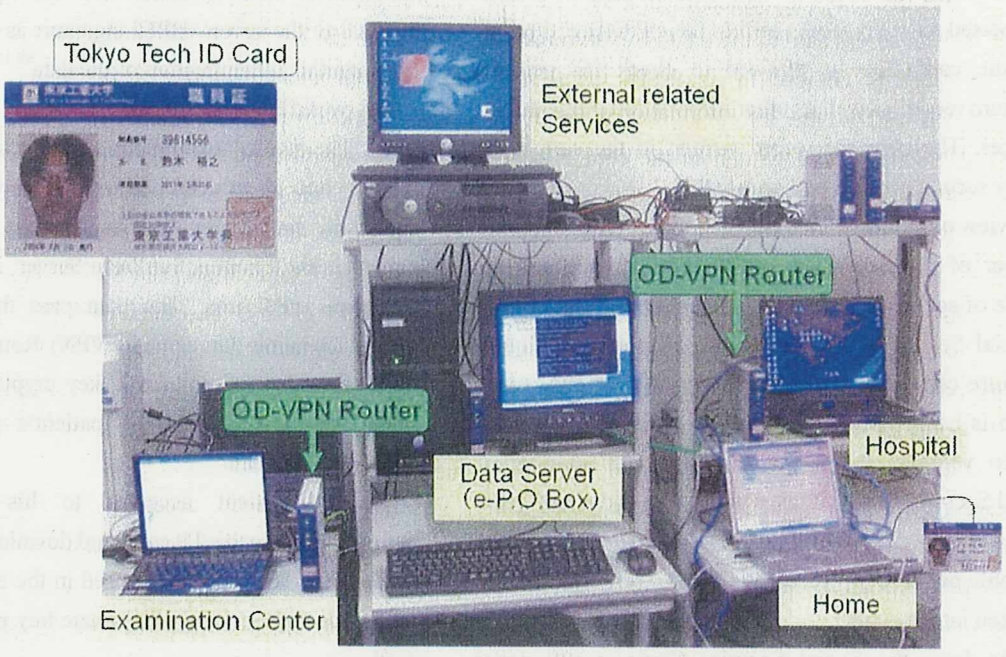

Figure 4. The arrangement of developed proto-type system

Discussion

Healthcare messages through the e-P.O.Box are necessary to be standardized to be effectively shared and usefully utilized. In the experiment of Tokyo Tech, data is converted based on the HL CDA R2 [2-21].

Access to e-P.O.Box box is necessary to consider more easily just like bank account. The server could support different access schemes: ID with password, token, IC card etc. The server opens or blocks the secure access pass to the application subject to its policy. It is recommended to have the existing Resident Registration card and net Social Security Card coexist for the access to the e-P.O. box through the use of public personal authentication service.

To spread the system for the public use, who pay the cost of the system is one of the most significant considerations in the future. It sounds reasonable that the sender of the information bears the cost. Other data such as EHR could be treated in the e-P.O.Box box at the user's choice, even more life event such as employment, retirement, graduation, move, etc. could be included with a good navigation of the Concierge function. The more widely used, the less expensively it would costs.

The access method of the system is another key factor for the diffusion of the system. The Ministry of Internal Affairs and Communications (MIC) is going to inaugurate a study group and make an examination in next year for the adoption of various terminals for the access to e-P.O.Box. Mobile phone and kiosk terminal are considered as the candidates. Access through the digital TV for terrestrial broadcast that wholly starts from Jun. 2011 is also under discussion. It is from the perspective of dissolving digital divide and providing universal service for the people who are not familiar with using computer.

References

1. Priority Policy Program 2007. Available at: http://www.kantei.go.jp/foreign/policy/it/Program2007.pdf. Accessed August 28, 2008.
2. Doan MH, Lott PL, Vaclavik M, Ueckert F. K-Box: automatic structuring and exchange of medical documents based on the clinical documentation architecture (CDA). Stud Health Technol Inform 2007;129(1):513-516.
3. Ballardini L, Germagnoli F, Pagani M, Picchi M, Stoppini A, Cristiani P. Putting E-government to work in healthcare environment: a multiregional project funded by the Italian Innovation & Technology Ministry. Stud Health Technol Inform 2004;107(2): 1173-7.
4. Takeda H, Matsumura Y, Kuwata S, Nakano H, Sakamoto N, Yamamoto R. Architecture for networked electronic patient record systems. Int J Med Inform 2000;60(2):161-167.
5. Ueckert FK, Prokosch HU. Implementing security and access control mechanisms for an electronic healthcare record. Proc AMIA Symp 2002:825-829.
6. Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ. 2001;322:283–287.
7. For the Record: Protecting electronic health information. In:Board CSaT, Council NR (eds). For the Record—Protecting Electronic Health Information. Washington, DC: National Academy Press, 1997.
8. The guidelines for networks used on the health domain issued by Ministry of Health, Labor and Welfare. Available at: http://www.mhlw.go.jp/shingi/2008/03/s0301-2.html. Accessed June 28, 2008.
9. Lekkas D, Gritzalis S, Katsikas S. Quality assured trusted third parties for deploying secure internet-based healthcare applications. Int J Med Inform 2002;65(2):79-96.
10. Konerding DE. Virtual network computing: cross-platform remote display and collaboration software. J Mol Graph Model 1999;17(2):151-154
11. Hladká, E, Holub, P, Denemark, J. An active network architecture: Distributed computer or transport medium. In:3rd International Conference on Networking (ICN'04), Gosier, Guadeloupe 2004
12. Health informatics - Dynamic On-demand virtual

private network for health information infrastructure, ISO TC 215/SC 2008.
13. Altrogge M. Public-key-infrastructure: secure obstacles. Network Computing. 2003;1–2
14. Lampsas P, Vagelatos A, Papanikolaou Ch. Design principles for the implementation and functional integration of regional health care virtual private networks. Udine, Italy: MEDNET 2001; Nov 2001.
15. Takeda H, Matsumura Y, Nakagawa K, Teratani T, Qiyan Z, Kusuoka H, Matsuoka M. Healthcare public key infrastructure (HPKI) and non-profit organization (NPO): essentials for healthcare data exchange. Stud Health Technol Inform 2004;107(2):1273-1276.
16. Application service of HPKI certificate in MEDIS-D C. Available at: http://www.medis.or.jp/8_hpki/index.html. Accessed September 4, 2008.
17. Kita K, Suzuki H, Takeda T, Inomata A, Shimada H, Arima K. A secure health domain network by cooperation with HPKI and dynamic on-demand VPN;2007 Nov Kobe Japan.
18. Chousiadis C, Mavridis IK, Pangalos GI. Authentication architecture for healthcare information systems. Health Informatics Journal 2002;(8):199–204.
19. Bourka A, Kaliontzoglou A, Polemi D, Georgoulas A, Sklavos P. PKI-based security of electronic healthcare documents. Proceedings of the SSGRR 2003 Jan 6-12; L'Aquila, Italy 2003.
20. Aden T, Eichelberg M, Thoben W, A fault-tolerant cryptographic protocol for patient record requests. Proceedings of EuroPACS-MIR; 2004 Enlarged.
21. Dolin RH, Alschuler L, Boyer S, Beebe C, Behlen FM, Biron PV, Shabo Shvo A. HL7 Clinical Document Architecture, Release 2. J Am Med Inform Assoc 2006;13(1):30-39.

社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

社会保障サービスのための
電子私書箱を実現する基本システムの検討

小尾高史[1,2] 谷内田益義[2] 李　中淳[2] 本間祐次[2] 大山永昭[2,3]

柏木巧[4]　川村浩正[4]　庭野栄一[4]

1 東京工業大学　総合理工学研究科　〒228-8502 神奈川県横浜市緑区長津田町 4259
2 東京工業大学　統合研究院　〒228-8503 神奈川県横浜市緑区長津田町 4259
2 東京工業大学　像情報工学研究施設　〒228-8503 神奈川県横浜市緑区長津田町 4259
4 日本電信電話株式会社　〒
E-mail: [1] obi@ip.titech.ac.jp

あらまし　現在、社会保障に関する国民個々の情報は、機関毎に個別管理されており、これらは自らの情報であるにも関わらず、本人が必要に応じて自由にアクセスし、利活用できる状態にはない。これに対して、重点計画２００８では、国民が自ら情報を簡単に収集管理可能な仕組みである「電子私書箱（仮称）」を提供することで、安全・安心なＩＴ社会の実現を目指しているが、現在のところ社会保障関連の情報以外の健康情報や医療情報等を取り扱うには、「電子私書箱」は、どうあるべきか、どのよう機能が必要となるかという具体的な実現方策については明らかにされていない。本発表では、これらサービスを「電子私書箱」を利用して実現するために必要な機能を整理し、どのようにそれを実現するべきかを検討したので報告する。

キーワード　電子私書箱, 社会保障サービス, 社会保障カード

Study of e-P.O.Box Basic System
for The Social Security Service

Takashi OBI[1,2] Yasuyoshi YACHIDA[2] Joong Sun LEE[2] Yuji HOMMA[2] Nagaaki OHYAMA[2,3]

Takumi KASHIWAGI[4]　Hiromasa KAWAMURA[4]　Eiichi NIWANO[4]

1 IGS of Sci. and Engineer., Tokyo Inst. of Tech., 4259 Nagatsuta Midori Yokohama,228-8502 Japan
2 Integrated Research Institute, Tokyo Inst. of Tech., 4259 Nagatsuta Midori Yokohama,228-8503 Japan at Tokyo
3 Imag. Sci. and Engeer. Lab., Tokyo Inst. of Tech., 4259 Nagatsuta Midori Yokohama,228-8503 Japan at Tokyo
4NTT　〒
E-mail: [1] obi@ip.titech.ac.jp

Abstract　.

Keyword　e-P.O.Box,　Social Security Service , Social Security Card

1. はじめに

現在、国民の社会保障に関する個々の情報は、医療機関や保険者等、機関毎において個別管理されており、これらは国民自らの情報であるにも関わらず、本人が必要に応じて自由にアクセスし、利活用できる状態にはない。このような状況の下、平成19年4月にIT戦略本部より発表されたIT新改革戦略 政策パッケージ[1]において、国民視点の社会保障サービスの実現に向け、電子私書箱（仮称）の創設が記載された。これを受けて、平成20年8月に発表された重点計画2008[2]では、「国民が自己の情報を安全かつ簡便に入手、閲覧及び活用することができる社会保障サービスを実現するため、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」とされているが、更に「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、社会保障カード（仮称）及び電子私書箱（仮称）の検討と連携しつつ、2008年度までに健康情報入手及び管理に関するルールや提供体制等の仕組みについて方針を示し、2011年度を目途に保険者等の情報提供機関における情報提供体制を整備し、希望者が電子的に閲覧可能な環境を構築することを目指す」とあり、社会保障分野だけでなくヘルスケア分野における電子私書箱の利用への期待が高まっている。

ここで、ヘルスケア分野における電子私書箱構想の利用については、健康情報を個人の電子私書箱へ電子的に配送し、利用者がダウンロードもしくは必要なものを健康管理のためのサーバに再登録することで、診療や健康維持のために必要な健康情報を医療機関や自宅で参照することが可能となるシステムである「個人健康情報参照システム」の研究[3]が進められており、この中で健康情報を取り扱うために電子私書箱に必要とされる機能の整理を行っている。

これら状況を踏まえ、本研究では、社会保障分野、ヘルスケア分野、さらには民間における電子私書箱の利用を想定し、これら分野において共通的に「電子私書箱」を利用するために必要となる機能を整理し、どのようにそれを実現するべきかを検討する。

2. 電子私書箱に求められる機能

2.1. 電子私書箱に対する考え方の整理

昨年度開催された「電子私書箱（仮称）による社会保障サービス等のIT化に関する検討会」では、電子私書箱（仮称）に対する情報の送付形態として、

1．電子私書箱が情報保有機関から情報をPULL型で取得し表示、必要なものは格納する
2．情報保有機関から電子私書箱に情報をPUSH型で送付し、電子私書箱に蓄積されたデータを表示する

の2通りが示されており[4]、今後その必要性を含め、さらなる検討を進めることとしている。

しかし、PULL型の場合、あくまでも情報の管理者は、情報保有者であり、利用者自身ではない。このため、情報の閲覧による監視は可能であったとしても、情報の訂正を行うに必要な情報が入手できるとは考えられない。

一例をあげると、国民から見た年金に関する最大の関心事は、“年金記録の記録漏れ”及び“厚生年金の記録改ざん”等にあるが、本質的な問題の解決には、単にこれらを発見することではなく、最終的に過去に遡り記録が正しく修正されることにある。電子私書箱がPULL型として働く場合、情報の修正を求める際の立証は、利用者自身が行う必要があり、本質的問題の解決には至らないと考えられる。

これに対して、例えば、国民年金の納付領収書などを電子私書箱へ送付し、保管することが可能であれば、仮に年金記録に誤りや改ざんが生じた場合でも、電子私書箱に保管された情報をもって、利用者は記録の訂正を求めることが可能となる。また、厚生年金については、来年度から予定されている年金定期便などを利用して標準月額報酬や年金掛け金の直接通知を行うことにより、現在の年金情報が正確に把握できるだけでなく、給与明細と合わせ内容チェックや年金記録の訂正等にも役立つとされているが、これを電子的に実現するためには、上記でいう2の形態が必須である。

また、現段階では主な検討対象となっていない医療・健康情報に関しても、同様のことが言える。例えば、現在でも先進的な医療機関等では、独自の医療ポータルサイトを提供しているが、これらサイトは、患者が医療機関に保存された自分の医療データの一部を覗き見る『窓』であり、患者が情報を所有することもコントロールすることもできない[5]とされる。

これに対して、「電子私書箱」は、国民が情報を自らのものとして簡単に収集管理可能な仕組みとして期待されており、従来のPersonal Health Record System(PHR)構築の際の課題となっている、「医療・健康情報をどこから、どのように集めるか」、また「集められた情報をどのように利用するか」という問題に対して有効な解決方法を提示できる可能性があると考えている。このように、特に公的分野における電子私書箱の導入を考えた場合、情報の送付は、電子私書箱の基本的機能として重要な位置づけになると考えている。

次に、情報の送付を現実社会で行う場合を考える。例えば、キャッシュカードやクレジットカード、各種証書、年金定期便等に代表される機微な情報の送付には、個人の氏名、住所を利用した郵便等が利用されることが多い。これは、氏名・住所は確実に特定の個人と結びついていることを公的機関が暗黙のうちに保証しているからだと考えることができる。

これに対して、ネットワークの世界において、確実に個人と結びついた信頼点を探すことは難しいことが、電子的に様々な情報を本人に確実に送付することを困難にしているといえる。

これに対して、我々の考える電子私書箱とは、ＩＴ社会における信頼点となるべき場所であり、

- 現実社会における住所のようなもの
- 信頼点であることを公的な機関が保証
- 確実に本人と結び付けられている
- 利用者自身の情報のホームポジション

などの特徴をもつものと定義する。これにより、電子私書箱に対して情報の送付を行うことで、確実に個人に対して情報を送付したことを保証可能な情報伝達基盤を実現することが可能となる。

2.2. 電子私書箱へのアクセス手段

現実社会における鍵と同様に電子私書箱へのアクセスには、利用者の本人確認を行うためのトークンのようなものが必要となる。これに対しては、重点計画2008 において、「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」とあり、「社会保障カード（仮称）の検討にあたっては、住民基本台帳カード及び公的個人認証サービスの普及に関する検討と一体的に進める」となっていることから、電子私書箱のアクセスカードとしての利用が期待できる。本研究では、オンライン認証に対応した社会保障カードの登場を想定し、これをアクセスカードとして利用することを前提とする。このときカードには、アクセス制御又は進展通信に利用する秘密鍵、これに対応する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）、個人の私書箱が登録されている電子私書箱の識別子（NAI 形式の ID 等）が記載されていることが必要である。

2.3. 電子私書箱で取り扱われる情報

例えば、現実社会において、個人におけるホームポジションである個人の住居を考えると、

- 敷地内にあるが、第３者により設置され、資格を持った第３者も確認できる情報
- 住居の中にあり、本人のみが管理、利活用できる情報
- 実印や貸金庫の鍵など他のサービスを利用するための鍵となるもの

が存在する。

電子私書箱においても同様に、

- 資格確認情報の用に電子私書箱内に、第３者（保険者など）により格納され、資格を持った第３者（医師など）も確認できる情報
- 電子私書箱を利用して、本人のみが閲覧、管理、利活用できる情報
- 他のネットワーク利用のサービスを利用するための鍵となる情報

を取り扱うことが想定される。

2.4. 電子私書箱の基本要件

以上の考え方を踏まえ、ＩＴ社会における信頼点である電子私書箱は、

- 本人確認手段や本人の資格等確認手段の提供
- 本人に対する情報フローの中心的存在（情報の蓄積・利活用）
- 様々なサービスを受けるための情報（鍵）の保管

などの機能を有することが要求される。

2.5. 電子私書箱の構成

電子私書箱の具体的構成については、現在

2.4 の基本要件を踏まえ電子私書箱のシステムを考えた場合、図１に示すように、利用者の本人確認手段や資格等確認手段の提供を行う機能、本人に対して情報を伝達するための機能、及び他のサービスを受けるための鍵を保管するための機能を有する基本システムと、蓄積または基本システムを介して伝達された情報を利用・管理する電子私書箱支援システムに分割することができる。

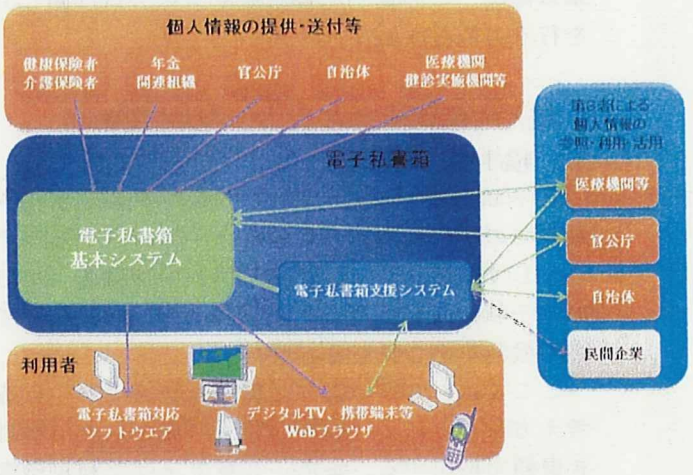

図１　電子私書箱のシステム構成

このような構成をとることにより、例えば、電子私書箱で扱う情報が、社会保障関連情報、電子申請関連、健康情報、電子処方箋等の薬剤情報など、多岐に渡ったとしても、情報の利用・活用については支援システムが行うこととなるため、単一の電子私書箱システムを構築する場合と比較してシステムの肥大化を抑えることができるだけでなく、支援システムと基本システムの運営主体が異なる場合への対応や利用者が自己の判断で電子私書箱と連携するサービスを選択することも可能となる。

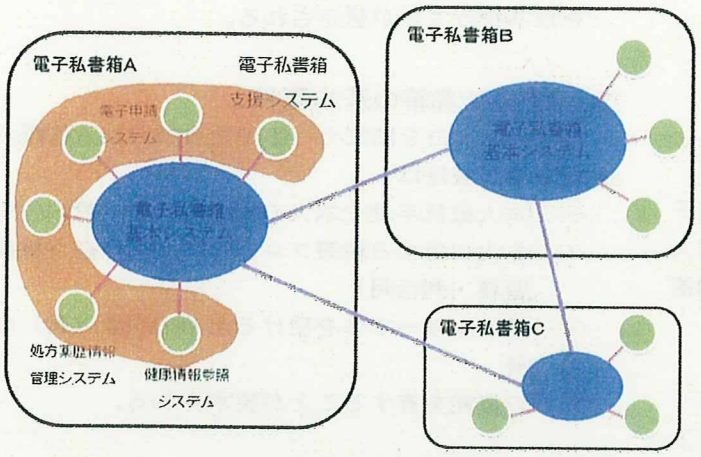

図２　電子私書箱の構成

また現実には、複数の電子私書箱事業者が存在する場合が想定されるが、この場合には、図２のように情報の伝達機能を有する基本システム部分が連携し、相互に情報の伝達等を行うことになる。

本研究では、社会保障分野、ヘルスケア分野、さらには民間における電子私書箱の利用を想定し、これら分野において共通的に「電子私書箱」に必要となる機能を整理することを目的としているため、３章以降で、この電子私書箱基本システムに関して検討を行うものとする。

3. 電子私書箱基本システムの基本機能

3.1. 検討すべき課題

電子私書箱の機能については本年末までの予定で政府での検討が進められており、ユニバーサルサービスとして提供される機能やオプション機能、また民間の電子私書箱が担う機能等の切り分け等については、その検討状況を見守る必要がある。

ここでは、２章で述べた電子私書箱に対する基本的考え方をもとに、一般的な利用形態をもとに検討すべき課題を抽出する。また、２章で上げた利用形態・構成のほかに、医療機関からの情報提供や民間での利用も想定する。この場合には、電子私書箱は複数あり情報提供機関及び受信者（利用者）は、いずれかの電子私書箱にアカウントを有すると想定され、情報提供機関は自分が利用している電子私書箱に情報を提供すると、受信者の電子私書箱を探索して私書箱間での情報伝達を行うことが予想される。また、電子私書箱の情報を利用して様々なサービスを行う支援サービスが存在する場合には、何らかの手段で電子私書箱と情報を連携させる必要がある。このような利用形態を実現するための機能については、これからのサービスモデルの検討状況により変更となる可能性もあるが、現段階で我々が電子私書箱基本システムに期待する機能・課題は以下のようになる。

- 管理・設定機能
  - 「電子私書箱アカウント」の開設方法
  - 「電子私書箱アドレス」の付与方法
  - アクセスカード（社会保障カード）と利用者の「電子私書箱」の関連づけ方法
  - 社会保障関連の情報と利用者の「電子私書箱」の関連づけ方法
  - 情報保有機関の利用者情報を入手するために必要となる情報と利用者の「電子私書箱」の対応付け方法
- 認証・資格確認等実施機能
  - 公的な個人認証基盤としての本人確認と一定レベルの信頼性確保を実現
  - 公的情報提供機関等と「電子私書箱」の連携
  - 公的資格の情報の確認方法
  - 本人以外の第３者に対する資格情報の確認手段の提供
  - 電子証明書の保管・提示・提出
- 情報伝達機能
  - 情報伝達に対する事業者責任の明確化
  - 配達証明の実施
  - 「電子私書箱」と関連付けられた本人への情報伝達を保証する親展通信の実施
  - 署名検証の実施
  - 送信者費用負担の実現
  - 引受け時刻証明の実施
  - 個人データの登録方法
- 情報制御機能
  - 利用者によるポリシー管理の実施
  - 利用者の意思に基づく、情報の参照の許可・不許可の設定

- メタデータによる処理
- 社会保障情報のリアルタイム確認
- 情報伝達にかかわる否認防止のための証跡管理
- データの長期保存
- 原本管理・原本参照・提供

・ 私書箱連携機能
- 支援システムに対する情報提供
- 利用者に対する利用性向上
- 複数の「電子私書箱」の連携による情報伝達
- 複数の「電子私書箱」間の連携による認証

3.2. 電子私書箱基本システムの機能一覧

本節では、3.1 で整理した課題をもとに、電子私書箱基本システムに要求される機能をまとめる。

まず、管理・設定を行うために必要となる機能は、表１のように整理される。

表１　管理・設定に必要な機能

電子私書箱の初期化	電子私書箱と利用者本人の社会保障カードを関連づけ、電子私書箱アカウント（アドレス）を開設する
各種公的情報保有機関との関連づけ	利用者本人の年金基礎番号、健康保険番号、介護保険番号と電子私書箱アカウント（アドレス）を関連づける
利用者によるアドレス変更	利用者は自由に電子私書箱アドレスを変更することが可能であり、変更した場合に、電子私書箱アカウント（アドレス）と連携しているすべての情報が新たな電子私書箱アカウント（アドレス）と関連付けられる
社会保障カードの紛失時の対応	利用者が社会保障カードの再発行を受けた場合、再度、電子私書箱アカウント（アドレス）との関連づけを行う
ポリシー設定	利用者は、電子私書箱を介した情報伝達や、私書箱に蓄積された情報の利用、私書箱と連携するサービスの利用等に関するポリシーを設定できる

このとき、私書箱アドレス付与については、電子私書箱を設置する公的機関は、本人のアクセスカード(社会保障カードなど）と関連付けられた「電子私書箱」を開設するとともに、利用者に対して NAI 形式の ID を発行し、その情報を社会保障カードに書き込むことを想定している。

各種関連付けについては、カードもしくは私書箱開設時に電子私書箱開設時に、利用者は現在発行されている健康保険証、介護保険証、年金手帳をもとに公的機関の窓口において対面で各種公的情報管理機関との対応をとることを想定する。

次に情報伝達に必要な機能は、表２のように整理される。

表２　情報伝達に必要な機能

送信者の確認	受信者の電子私書箱は、データを送付する送信者（公的情報機関や医療機関等）の身元確認が行える
受信者の確認	送信者は、これから送信を行う受信者の存在確認を行うとともに、とともに、受信者の電子証明書等を入手できる
親展通信	送信者は、入手した受信者の電子証明書等を用いて送信するデータを暗号化し、送付できる
データの送付	送信者は自分の電子私書箱を経由して受信者の電子私書箱にデータを送付できる
安全な通信路の確保	医療機関等の情報提供機関からの情報送付の際には、情報提供機関―電子私書箱間の通信路の安全性を確保する
到達確認	送信者は、自分の送信したデータが受信者の電子私書箱に到達したことを確認できる
受信確認	送信者は、受信者が送付したデータを受信・開封したことを確認できる
代行受信	受信者の電子私書箱は、あらかじめ設定された第３者のデータを受信することができる

情報伝達においては、少なくとも、現在の郵便で実現されていることをネットワーク上で実現することを想定し、送受信者のなりすましや、通信内容の傍受、改ざんに対する安全性の確保、認証の機能や暗号鍵の安全な交換などの仕組み、SPAM やネットワークの脅威等を防止可能であること、自分が許可した人からの情報のみを受信することなどが実現できることが必要である。

さらに、認証・資格確認等を行うために必要な機能は、表３のように整理される。

この機能は、利用者本人が電子私書箱を経由して様々なサービスを受けるために必要な機能や、健康保険、介護保険の資格情報など確認及びこれら情報を本人以外の第３者が確認するための手段の提供を行うための機能をまとめたものである。

表３　認証・資格確認等を行うために必要な機能

利用者認証	利用者本人の社会保障カードを用いて電子私書箱にアクセスすることができる

資格等情報設定	公的な資格情報を発行する機関が、電子私書箱に資格情報へのディレクトリ情報又は、資格情報そのものを格納できる
認証ディレクトリ	利用者が電子私書箱を経由して、公的機関・医療機関等が独自に管理する ID 情報と連携する
認証ゲートウエイ	利用者が電子私書箱を経由して、公的機関等が提供するサービスへアクセスできる
証明書認証	電子私書箱内に各種証明書を保管し、利用者本人あるいは第３者等に証明書情報の認証を行う
受信データ（公開情報）の参照	受信者もしくは資格を有する第3者は、資格情報のような電子私書箱に保存されている受信データ（公開情報）を参照できる
受信データ（公開情報）の検索	受信者もしくは資格を有する第3者は、資格情報のような電子私書箱に保存されている受信データ（公開情報）を検索できる

利用者にとって情報制御に必要な機能は、表４のように整理される。健康情報等の蓄積された情報を利用・活用する場面においては、電子私書箱支援システムにおいて取り扱われることを想定し、情報制御に必要な機能としては、最低限必要と考えられるものをまとめている。

表４　情報制御に必要な機能

受信データ（個人情報）の参照	受信者は、電子私書箱に保存されている受信データなどの個人データのうち暗号化されていない情報もしくは電子私書箱での復号を許可した個人情報を参照できる
受信データ（個人情報）の検索	受信者は、電子私書箱に保存されている受信データなどの個人データのうち暗号化されていない情報もしくは電子私書箱での復号を許可した個人情報を検索できる
署名検証	電子私書箱は受信者に代わり、送付されたデータに付与されている署名の検証を行うことができる
利用者クライアントへのダウンロード	受信者は電子私書箱で受信したデータを自分の意志で、利用者のクライアントにダウンロードできる
原本性保証	電子私書箱は、利用者もしくは参照が許可された第３者に対して、保存されているデータが原本であることを保証できる
個人データ保存	利用者は、自らのデータを自分の電子私書箱に保存できる
暗号化機能	必要があれば、利用者は自分のデータを社会保障カードを用いて暗号化できる
第３者アクセス	利用者が設定した第３者、または資格を有する者については、特定のデータについてのアクセスを許可する
長期保存	利用者は自分のデータを生涯にわたり、蓄積・利用できる

最後に、電子私書箱の連携に必要な機能は、表５のように整理される。

表５　電子私書箱の連携に必要な機能

外部電子私書箱への情報転送	利用者は、自分の情報を他の電子私書箱へ移動することができる
電子私書箱支援システムとの連携	利用者は、電子私書箱と連携する電子私書箱支援システムの提供する外部サービスに対して、利用者の設定したポリシーのもとで、情報を提供し、利用・活用できる
コンシェルジュサービス	電子私書箱支援システムや外部サービスとの連携に際して、電子私書箱に保存されているデータの内容をもとに、利用者に適したサービスの提示を行うことができる

3.3. 電子私書箱基本システムの機能構成

先に述べたように、電子私書箱の機能構成については現在政府での検討が進められているが、仮に、電子私書箱を公的機関が運営すると想定した場合には、基本システムは、図３で示す機能構成になると考えられる。基本システムを構成する各機能は利用者が IC カードを利用し電子私書箱へアクセスするために利用するクライアント機能、利用者に対してユーザインターフェースを提供する UI 機能、利用者及び有資格者の認証等を行う認証機能、情報の制御及び送受信を行い基本機能、公的情報保有機関と電子私書箱との関連づけをおこなう中継 DB 機能の５つとなり、公的情報保有機関からは、基本機能に対して直接または中継 DB 機能を介して送付される。

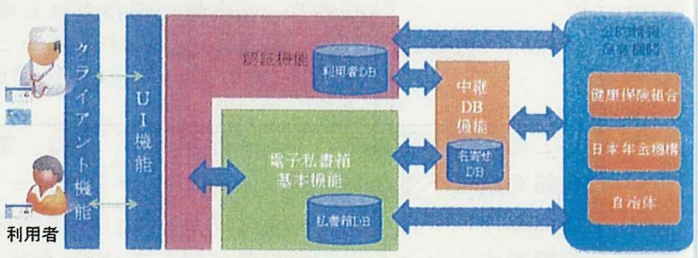

図３　電子私書箱基本システムの機能構成

今後は、基本機能を民間等が運用する場合の機能構成についても検討を行う予定である。

4. まとめ

本発表では、我々が想定する電子私書箱の基本システムに必要な機能の整理とそれを実現するために必要となる基本システムの機能構成に関して検討を行った。

今後は、電子私書箱のサービスパターンを整理するとともに、基本システムの機能一覧で整理した各機能を、電子私書箱基本システムの機能構成で示した各機能を利用してどのように実装するかの検討を行い、実際に資格情報の確認や社会保障情報の閲覧を行うためのシステムを構築する予定である。

5. 謝辞

本研究の一部は、文部科学省科学技術振興調整費及び厚生労働科学研究費による助成を受けておこなわれている。

文　献

[1] IT 新改革戦略 政策パッケージ, http://www.kantei.go.jp/jp/singi/it2/kettei/070405honbun.html, Apr.2007.

[2] 重点計画-2008, http://www.kantei.go.jp/jp/singi/it2/kettei/080820honbun.pdf, Aug.2008.

[3] 喜多紘一, 猪口正孝　他, “電子私書箱構想による個人健康参照システムの実証実験, ”第２８回医療情報学連合大会, Nov.2008.

[4] 電子私書箱（仮称）による社会保障サービス等の

[5] IT 化に関する検討会【報告書】, http://www.kantei.go.jp/jp/singi/it2/epo-box/houkoku1.pdf, Mar. 2008.

[6] “Distinguishing Features of Indivo,” INDIVO HEALTH, http://www.indivohealth.org/

個人を主体とした処方薬歴情報の提供管理システムの提案

松平　彩[1]　鈴木　裕之[2,3]　小尾　高史[1,3]　喜多　紘一[3]　山口　雅浩[2,3]
李　中淳[3]　谷内田　益義[3]　大山　永昭[2,3]

1 東京工業大学総合理工学研究科　〒226-8503 神奈川県横浜市緑区長津田町 4259
2 東京工業大学像情報工学研究施設　同上
3 東京工業大学統合研究院　同上

E-mail:　matsudaira.a.ab@m.titech.ac.jp

あらまし　現在，医療情報ネットワーク基盤検討会等において，処方箋の電子化に関する検討[1]が進められており，処方情報や調剤情報を含めた電子処方薬歴管理を行うにあたっては，政府が運用を予定している電子私書箱の利用が期待されている．しかしながら，電子処方箋を取り扱うシステムを運用するに当たり，電子私書箱との連携をどのようにとるかなど，具体的な要件の検討は未だなされていない．

本研究では，電子私書箱と連携することで患者の処方情報，調剤情報から服薬情報までを個人を主体として管理できるシステムを提案し，その基本仕様についての検討を行ったのでその詳細について報告する．

キーワード　電子私書箱，社会保障カード，電子処方箋，薬歴

A suggestion of the offer and management system of the individual prescription and medication history

Aya MATSUDAIRA[1]　Hiroyuki SUZUKI[2,3]　Takashi OBI[1,3]　Kouichi KITA[3]
Masahiro YAMAGUCHI[2,3]　Jhong LEE[3]　Masuyoshi YACHIDA[3]　Nagaaki OHYAMA[2,3]

1 Interdisciplinary Graduate School of Science and Engineering, Tokyo Institute of Technology
4259 Nagatsuda-tyou, Midori-ku, Kanagawa, 226-8503 Japan
2 Imaging Science and Engineering Laboratory, Tokyo Institute of Technology
3 Integrated Research Institute, Tokyo Institute of Technology

E-mail:　matsudaira.a.ab@m.titech.ac.jp

Abstract　Now the investigative committee on the medical information network infrastructure examines about the digital prescription. And when the individual medication history including the digital prescription and dispensing information is managed, the use of “e-post-office box” to which the government is scheduling operation is expected. However its concrete requirements haven’t examined yet.

In this study, I suggest that the system could manage the digital prescription, dispensing information and information of taking medicine by cooperation with “the e-post-office box”. And I repot on the details of the examination of the basic requirement of this system.

Keyword　e-post-office-box,　social security card,　digital prescription,　medication history