国民電子私書箱の基本機能とシステム要件

谷内田益義[1]　小尾高史[2,1]　本間祐次[1]　李中淳[1]　大山永昭[3,1]　中井俊文[4]
鳥光淳子[5]　平野さやか[5]　遠藤直樹[5]　斯波万恵[5]　池上美千代[5]　矢野令[5]　野村真義[6]
植村芳典[6]　中山健司[6]　遠藤方洋[6]　田中祐耕[7]　松口裕重[7]　山口正一郎[7]
近藤誠[7]　坂上克男[7]　庭野栄一[8]　川村浩正[8]　石川清彦[9]　藤井亜里砂[9]　山村千草[9]
中村信次[10]　米永知泉[10]　伊東明[11]　錦織康之[11]　下江達二[11]　島田宏[11]
酒井正仁[12]　半田富己男[12]　桑田潤[12]

1 東京工業大学統合研究院　226-8503 横浜市緑区長津田町 4259 S1
2 東京工業大学大学院総合理工学研究　226-8503 横浜市緑区長津田町 4259 G2-2
3 東京工業大学大学院理工学研究科像情報工学研究附属施設　4 シャープ株式会社
5 東芝ソリューション株式会社　6 凸版印刷株式会社　7 日本電気株式会社
8 日本電信電話株式会社　9 NHK 放送技術研究所　10 株式会社日立製作所
11 富士通株式会社　12 大日本印刷株式会社
E-mail: 1 yachida@iri.titech.ac.jp　　2 obi@ip.titech.ac.jp

あらまし　2007 年 4 月に IT 戦略本部より発表された IT 新改革戦略 政策パッケージにおいて，国民視点の社会保障サービスの実現に向けた電子私書箱（仮称）の創設が記載された．その実現に向けて，内閣官房，厚生労働省等関連する省庁が中心となった検討会にて，社会保障あるいは次世代電子行政サービス基盤等の観点から，実現方法，実現に向けた課題等の検討が進められてきた．本報告は，これらの検討を踏まえ，社会保障サービスを含む国民電子私書箱を実現する場合の電子私書箱の基本機能を明らかにし，国民電子私書箱に要求されるサービス・機能・インタフェース・セキュリティ等に対する要件を提示すると共に，実現に際しての課題を明らかにする．

Basic Functions and System Requirements for the Citizen's e-P.O.Box

Masuyoshi YACHIDA[1]　Takashi OBI[2,1]　Yuji HOMMA[1]　Joong Sun LEE[1]
Nagaaki OHYAMA[3,1]　Toshifumi NAKAI[4]　Junko TORIMITSU[5]　Sayaka HIRANO[5]
Naoki ENDO[5]　Masue SHIBA[5]　Michiyo IKEGAMI[5]　Rei YANO[5]　Masayoshi NOMURA[6]
Yoshinori UEMURA[6]　Kenji NAKAYAMA[6]　Masahiro ENDO[6]　Yuko TANAKA[7]
Hiroshige MATSUGUCHI[7]　Shoichiro YAMAGUCHI[7]　Makoto KONDOH[7]
Katsuo SAKAUE[7]　Eikazu NIWANO[8]　Hiromasa KAWAMURA[8]　Kiyohiko ISHIKAWA[9]
ARISA FUJII[9]　Chigusa YAMAMURA[9]　Shinji NAKAMURA[10]　Tomomi YONENAGA[10]
Akira ITO[11]　Yasuyuki NISHIKIORI[11]　Tatsuji SHIMOE[11]　Hiroshi SHIMADA[11]
Masahito SAKAI[12]　Tomio HANDA[12]　Jun KUWATA[12]

1 Integrated Research Institute, Tokyo Inst. of Tech., 4259 Nagatsuta Midori–ku Yokohama,226-8503 Japan
2 IGS of Sci. and Engineer., Tokyo Inst. of Tech., 4259 Nagatsuta Midori–ku Yokohama,226-8503 Japan
3 I Imag. Sci. and Eng. Lab., Tokyo Inst. of Tech.　4 Sharp Corporation　5 Toshiba Solutions Corporation
6 TOPPAN PRINTING CO., LTD.　7 NEC Corporation
8 NIPPON TELEGRAPH AND TELEPHONE CORPORATION

9 NHK Science & Technology Research Labs.　10 Hitachi, Ltd　11 FUJITSU LIMITED
12 Dai Nippon Printing Co., Ltd

Abstract　Japanese government has a plan to introduce e-P.O.Box system for all citizens to use and manage their own information related to various public services, including medical and pension plan information. Several ministries have issued reports on the e-P.O.Box system, but they only cover a part of public services and do not show the details of the system. We analyzed the reports and clarified the function of the e-P.O.Box. This paper presents the result of the analysis and the requirements for services, system, security and interfaces of the e-P.O.Box. Problems to be solved for realizing the e-P.O.Box system are also described.

1　はじめに

電子私書箱構想とは，主として様々な行政のサービス提供者（国，地方自治体，保険者，医療機関等）である情報保有機関が保有する国民の情報を，安心かつ容易に本人が入手・閲覧・管理・活用できる仕組みの実現を目標としたものである．その実現に向けて，2007 年度には「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」が，2008 年度には「電子私書箱（仮称）構想の実現に向けた基盤整備に関する検討会」が開催され，そのコンセプト，技術的要件，制度的課題などの検討が進められてきた[1-2].

他方，電子私書箱構想と並行して，次世代電子行政サービスや社会保障カード構想についての検討が進められてきた．次世代電子行政サービスについては，2007 年 10 月に「次世代電子行政サービス基盤等検討プロジェクトチーム」が設置され，国民や企業にとって簡素で便利かつ効率的な行政サービスの実現に向けた検討が進められており，2008 年 6 月には「次世代電子行政サービス（e ワンストップサービス）の実現に向けたグランドデザイン」が策定されている[5]．また社会保障カード（仮称）については，2007 年 9 月に「社会保障カード（仮称）の在り方に関する検討会」が設置され，2011 年度中の導入に向けて検討が行われており，2009 年 4 月には「社会保障カード（仮称）の基本的な計画に関する報告書」が公開されている[3-4].

このような中，2009 年 3 月に IT 担当大臣から「国民電子私書箱（仮称）」を推進していく旨が表明されると共に，2009 年 4 月には「デジタル新時代に向けた新たな戦略～三か年緊急プラン～」（IT 戦略本部）において，「国民本位の新しい電子政府・自治体の推進のための国民電子私書箱（仮称）」構想が示された．この国民電子私書箱は，従来の電子私書箱構想及び社会保障カード構想を発展させ，社会保障分野のみならず広い分野でのワンストップの行政サービスを提供するためのものと位置づけられている．更に，「デジタル新時代に向けた新たな戦略（案）」（IT 戦略の今後の在り方に関する専門調査会）においても，国民電子私書箱は「希望する国民・企業等に提供される電子空間上で安心して年金記録等の情報を入手し管理できる専用の口座であり，社会保障分野のみならず幅広い分野でワンストップの行政サービスを提供するもの」として，電子政府・電子自治体分野における中核的な方策に位置づけられている．

利用者である国民の視点で見ると，これらのサービスを提供するシステムは，最適な形態で構築された共通インフラとして提供されるべきである．本報告は，従来電子私書箱構想にて検討されてきた内容に社会保障カード（仮称）及び次世代電子行政サービスから電子私書箱に求められる要件を加えることによって，共通インフラとして提供される国民電子私書箱及びそれを利用したサービスの機能，国民電子私書箱に必要とされる主な要件を明らかにする．

2　電子私書箱の基本サービスと基本機能

検討に当たっては各外部検討会の報告書[1]-[5]を基に，各検討会が電子私書箱に相当する基盤に求める要件を抽出して整理することにより，各検討会の構想を実現する共通部分となるプラットフォームを明らかにする．さらに，実現するためのサービス，機能，運用などに課せられる要件を，電子私書箱構想にて検討された内容に社会保障カード及び次世代電子行政サービスでの検討結果を加える方針で検討した．

2.1　電子私書箱を実現する基本サービス

電子私書箱を活用する利用面からの要求事項として，電子私書箱構想では，

・自己の情報を一元的に入手閲覧する，

・所得した情報を長期間保管可能とする，

社会保障カードの検討では，

・中継 DB により，利用者の情報へのアクセス要求を，各保険者に振り分けることにより，医療機関の窓口から医療保険資格情報などの確認を実現する，

次世代電子行政の検討では

・イベントに関連する手続きのワンストップサービスを実現する，

が挙げられている．これらを実現するためには，表1のサービスが必要となる．

表１　電子私書箱の基本サービス

サービス名	サービス内容
本人確認サービス	サービスの利用を要求する利用者が，利用者本人であることを認証するとともに，電子私書箱サービスの利用者としての識別（個人利用者，代理人，医療従事者等の識別を含む）を行う
閲覧サービス	利用者の要求により，情報保有機関が保持する情報を取得，閲覧，保存する
通知（親展）サービス	情報保有機関が保持する情報を利用者の私書箱へ送付し，利用者がこれを閲覧する
管理（蓄積）サービス	利用者の電子私書箱内に管理蓄積されている情報（閲覧や通知（親展）により保存された情報の他に，利用者のアカウント情報，ポリシー情報，アクセス履歴情報等も含む）の参照，検索，更新，削除等を行う
申請サービス	利用者の要求により，情報保有機関に対して申請情報を送付する　（次世代電子行政）
資格確認サービス	医療従事者の専用サービス．医療従事者の要求により，情報保有機関が保持する医療サービスを受ける人の保険資格を確認する　（社会保障カード）

2.2　エンティティモデル

国民電子私書箱の基本サービスを実現するために必要となるエンティティの定義においては，文献[1]における検討内容に基づき，利用者，電子私書箱ポータル，電子私書箱プラットフォーム，情報保有機関にエンティティを区分した．電子私書箱ポータルや電子私書箱プラットフォームと異なる運用主体によりサービスの提供が想定されうる認証サービス部分について，これを独立したエンティティ(IdP)として定義する．さらに，公的個人認証基盤(JPKI)や医療分野の認証基盤(HPKI)の活用が示唆されていることを踏まえて，公開鍵証明書の発行サービスにかかる部分についても，これを独立したエンティティ(証明書発行システム)として定義することとした．エンティティのモデルを，図１に示す．

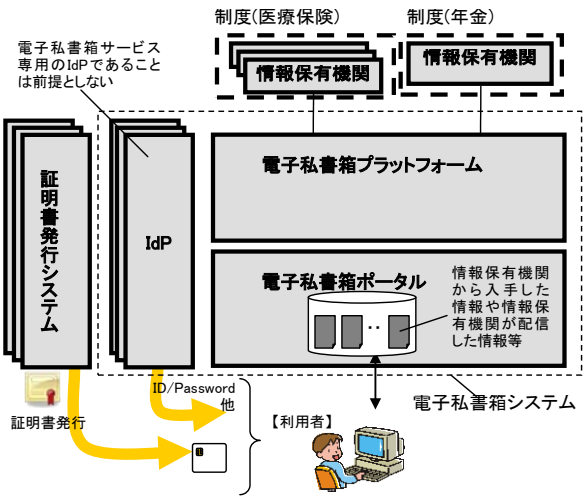

図1　電子私書箱システムに関するエンティティモデル

2.3　各エンティティの機能

表 1 の機能を実現するためには，図1に示した各エンティティは，以下の機能を提供する必

要がある.

(1)電子私書箱ポータル

各種の情報保有機関が保有する国民のさまざまな情報を，当該国民，あるいはその代理人等がインターネット等を通じて入手し利用するためのサービスを提供するとともに，通知（親展）サービスで利用者宛に送付された情報や，閲覧等のサービスにおいて保存された情報を蓄積し，必要に応じて照会，活用できる機能を提供する

(2)電子私書箱プラットフォーム

情報保有機関における利用者識別情報ならびに電子私書箱ポータルにおける電子私書箱アドレスを適切に結びつけ，情報保有機関と国民とが電子私書箱ポータルを通じて国民の情報の送受を安全に行う機能を提供する.

(3)IdP

利用者の認証を行い，その認証結果を提供することで，電子私書箱ポータルあるいは電子私書箱プラットフォームにおける利用者の識別・認証を可能とする機能を提供する

(4)証明書発行システム

IdPにおける利用者の認証に使用する公開鍵証明書（クレデンシャル）を発行する

(5)情報保有機関

国民の情報を保有する機関（国，地方自治体，各種保険者，医療機関等）であり，国民の情報を安全かつ確実に提供する機能を提供する

(6)利用者

電子私書箱サービスの利用者であり，個人利用者，代理人，医療従事者等の 3 種類に分類する

3 電子私書箱及びサービスに対する要件

3.1 電子私書箱基本サービスの要件

各報告書で挙げられている要件を表1に示した基本サービスに対してまとめると，次の通りとなる.

(1)サービス共通

・ポリシー情報により実行が許可される場合のみ，サービスが提供されること
・誰が，いつ，どの情報に対してサービスを利用したかの履歴情報を管理できること

(2)本人確認サービス

・利用者から提示されたクレデンシャル情報を利用して，サービス要求者が利用者本人であることを認証できること
・認証された利用者について，電子私書箱サービスにおける利用者としての識別（個人利用者，代理人，医療従事者の識別を含む）を行えること

(3)閲覧サービス

・利用者の要求により，情報保有機関が保有する利用者自身の情報を安全に取得，表示するとともに，電子私書箱内に安全に保存できること
・代理人が個人利用者の情報を閲覧する場合には，代理人による当該情報へのアクセスが当該個人利用者により事前に許容されていること

(4)通知（親展）サービス

・情報保有機関の要求により，利用者の私書箱に対して，利用者の情報を利用者のみが閲覧できるよう安全に送付，保存できること
・情報保有機関から利用者の私書箱への情報の送付において，私書箱への到達確認及び利用者による開封確認ができること
・代理人が個人利用者の通知（親展）情報を閲覧する場合には，代理人による当該情報へのアクセスが当該個人利用者により事前に許容されていること

(5)申請サービス

・利用者の要求により，情報保有機関に対して，利用者の情報を安全に送付できること
・申請情報が情報保有機関により受理されたことを，利用者に対して通知できること
・代理人が個人利用者の情報を申請する場合には，代理人による当該情報の申請行為が当該個人利用者により事前に許容されていること
・申請した情報を自身の電子私書箱に保存できること

(6)管理（蓄積）サービス

・利用者の要求により，電子私書箱内に保存された情報を表示，検索，削除できること

・利用者の要求により，利用者自身のアカウント情報やポリシー情報を参照，更新，削除できること
・代理人が個人利用者の情報にアクセスし操作する場合には，代理人による当該情報へのアクセスが当該個人利用者により事前に許容されていること
・利用者の要求により，利用者自身の情報に対するアクセス履歴情報を提示できること

(7)資格確認サービス

・医療従事者の要求により，情報保有機関が保有する個人利用者（患者等）の医療保険等の資格情報を，安全に取得，表示できること
・上記資格情報の確認対象となる個人利用者を特定するための情報を当該個人利用者の ICカードから読み出す場合，利便性，緊急性の観点から，当該個人利用者の本人確認情報（PIN等）を必要とすることなく読み出すことができること

3.2 電子私書箱基本機能の要件

図1に示した，基本機能に対する主な要件は以下のようになる．

(1)電子私書箱ポータル

・アカウント管理：電子私書箱アドレスの変更及び，代理人情報の登録が行えること
・IdP 連携：利用者としての識別，認証方法に応じた認証レベルの判別ができること
・ポリシー管理：情報の取得，保存，代理人への提供について，情報の所有者本人の意思を示すポリシー情報を設定，管理できること
・ポリシー制御：電子私書箱ポータルにて管理された情報に対するアクセス時に，ポリシー管理にて管理される各種のポリシー情報を総合的に評価（調整）し，その結果を依頼元（各種操作機能）に提供できること
・到達確認：通知（親展）サービスにおいて情報保有機関からの情報が正しく利用者の私書箱に到達したことを，電子私書箱プラットフォームへ通知できること
・送受信制御：通知（親展）情報が私書箱に到達したことを，利用者に対して電子メール，携帯メール等の別手段により通知できること

(2)電子私書箱プラットフォーム

・ポリシー管理：情報へのアクセスコントロールは，その情報の特性（認証レベルやプライバシーレベル）に依存して，セキュリティポリシー，プライバシーポリシー，プライバシープリファレンス等のポリシー情報を設定できること
・アカウント管理：情報保有機関の ID（健康保険情報，介護保険情報，年金情報等）と電子私書箱アドレスとの関連付けができること

(3)IdP

・アイデンティティ管理：電子私書箱ポータル，電子私書箱プラットフォームの利用者アカウント（あるいはその仮名）と，IdP の利用者アカウントとの間のアカウント連携情報を管理できること
・クレデンシャル管理：クレデンシャルは，情報の機微度に応じたもの（パスワード，電子証明書など）にすることが可能なこと

3.3 外部インタフェース要件

電子私書箱に特徴的となる主な外部インタフェースの要件は，以下の通りとなる．

・システム間のインタフェースは，HTTP，XML，SOAP，SAML など標準化されたプロトコルを使用し公開可能とすること
・HPKI など，社会保障カード以外のカード利用も考慮すること
・IdP にて管理される利用者のアカウント情報の参照，利用者の認証レベルの受け渡し等，IdPとの連携にかかる制御を実現できること
・通知（親展）情報を受信し，当該情報の到達確認及び開封確認情報を送付できること

3.4 セキュリティ要件

電子私書箱に特徴的となる主なセキュリティ要件は，以下の通りとなる．

・第三者への情報の提供は，本人の意思，情報の性質，利用目的等に応じて設定されたポリシー情報に基づいて行うこと
・情報伝達にかかわる否認防止のための証跡管理が行えること

3.5　運用要件

一般的に求められる可用性以外の要件としては，医療機関の窓口等において医療従事者等が資格確認サービスを利用する際に，資格情報の確認対象となる個人利用者を特定するための情報を IC カードから読み出す場合，利用者の本人確認情報（PIN 等）を必要とすることなく読み出すことができることが挙げられる．

4　まとめ

本報告においては，共通の基盤となるべき国民電子私書箱の持つべき機能とそれらに要求される主な要件を提示しした．国民電子私書箱の実現に当たっては，

・代理人の任命・権限の付与と範囲

・各エンティティの運営主体と責任範囲・分解点

・各ポリシー情報の具体化

等の課題が残っており，今後検討を進める予定である．また，国民電子私書箱の全体構想を実現し，普及させるためには，

・企業等法人向けの電子私書箱サービス

・公共以外の情報保有機関，情報活用機関，民間の電子私書箱ポータルとの連携

・利用者に適切なサービスの提示等を行うコンシェルジュ，エージェント等

の検討も必要となる．なお，本報告の検討は電子私書箱サービス研究会の活動として行った．

参考文献

[1] 電子私書箱（仮称）構想の実現に向けた基盤整備に関する検討会報告書，電子私書箱（仮称）構想の実現に向けた基盤整備に関する検討会，2009
http://www.kantei.go.jp/jp/singi/it2/epo-box2/houkoku1.pdf

[2] 電子私書箱（仮称）プラットフォーム　基本設計　Ver1.1，電子私書箱（仮称）構想の実現に向けた基盤整備に関する検討会、ユースケース検討ワーキンググループ，2009，
http://www.kantei.go.jp/jp/singi/it2/epo-box2/kihonsekkei.pdf

[3] 社会保障カード（仮称）の基本的な計画に関する報告書，社会保障カード（仮称）の在り方に関する検討会，2009
http://www-bm.mhlw.go.jp/shingi/2009/04/dl/s0430-4b.pdf

[4] 医療等の現場での利用を念頭に置いた社会保障カードの活用シナリオ，社会保障カード（仮称）の在り方に関する検討会作業班，2009，
http://www-bm.mhlw.go.jp/shingi/2009/04/dl/s0430-4c.pdf

[5] 次世代電子行政サービス（e ワンストップサービス）の実現に向けたグランドデザイン，次世代電子行政サービス基盤等検討プロジェクトチーム，2008，
http://www.kantei.go.jp/jp/singi/it2/nextg/pdf/granddesign.pdf

[6] 電子私書箱サービス研究会活動報告，電子私書箱サービス研究会，2009，
http://www.iri.titech.ac.jp/research/project/pdf/03_01.pdf