率は残念ながら依然として低迷している．一方，医療などの社会保障分野では，本格的なオンライン化が開始されたばかりである．また従来から，分野あるいは業務ごとに情報化が推進されてきたため，国民から見ると，本人確認方法，情報の入手や手続きを行う場所がバラバラで，結果として，手続き等をする度にどこでどうする，次はどことどこへ行けばよいのかわからないということが起きている．

電子私書箱の構想は，このような状況を改善し，電子政府の利便性と社会保障の透明性等を飛躍的に向上するために策定されたもので，その基本理念は，自分の情報を容易に確認でき，必要に応じて手元で管理できるようにすることである．もちろん現状では既存組織が原本管理を行っているので，本人が手にするのはその写しになるが，電子私書箱の導入により１枚のカードで，本人確認，自分にとって大切な情報の参照，確認，管理，さらには診察結果や健診結果の一元化による生涯を通じた健康情報管理などが可能になると期待されている．

この電子私書箱の最もプリミティブな機能は，電子的な郵便物を受け取ることであるが，関連機関に向けた複数の申請や届け出等を一括して行う機能を持たせれば，さらに便利になると予想される．特に，結果が出るまでに時間を要する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．例えば近年始まった年金特別便では，１億人の被保険者への通知に300億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，携帯電話，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．

2．導入時の留意点とセキュリティ

電子私書箱を実現･普及するためには，社会の受容性の確保に十分留意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，給与の振込みや公共料金等の自動引き落とし等，マネーフローを本人がコントロールするの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喩えることができる．そして，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，電子私書箱の運用に関する基本要件は，①私書箱事業者が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，の３つであると言える．

電子私書箱は機微な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，すべ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行うようにすることが必要である．そして，PKI(Public Key Infrastructure，公開鍵暗号基盤)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す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，すべ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．この時，個人向け電子署名の公的個人認証サービス(JPKI)と行政機関の電子署名(GPKIとLGPKI)等の公的な電子署名が対象となり，その検証を行うのであれば，現状制度では自治体等の公的な組織が電子私書箱を運用することが必要になる．

一方，電子私書箱の利便性を向上するには，多様なアクセス手段を確保することが強く望まれる．具体的なアクセス手段としては，ID・パスワード，携帯電話，地上デジタルテレビ等が考えられるが，これらを用いる場合には，それぞれの手段が持つ安全性のレベルを客観化し，そのレベルに応じたアクセスコントロールを行うことが妥当と考えられる．言い換えると，PKIをサポートするICカード(住民基本台帳カードや社会保障カードが候補となる)であれば全ての自己情報に，ID・パスワードでは機微でない自己情報に，その他はこの間に入るのではないかということである．このようなアクセスコントロールを行うためには，米国のNIST(National Institute

of Standards and Technology)等が示しているセキュリティレベルを参考にして，行政機関や医療機関等が管理している個人情報を本人に提供する際のセキュリティレベルを規定し，提供ポリシーとして公開することが必要である．

3．国民電子私書箱構想へ

電子私書箱の目的や基本機能，導入に当たっての留意点等は前述したとおりであるが，この私書箱のセキュリティやモデル化等の技術的な検討は，年金情報の閲覧や特定健診等の社会保障サービスの利用を想定して，内閣官房が主催する“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”において平成19～20年度の2年間にわたり行われてきた[4]．これらのアプリケーションでは，電子私書箱は，年金や健診結果等の自己情報を閲覧するための認証情報の記録と特定健診の受診券等を電子的に入手するために用いられることから，これらを可能とするために必要な機能とセキュリティ要件等が報告書にまとめられている．一方，次世代電子行政サービスの検討からは，上記の機能に加えて，行政機関からのお知らせ等をプッシュする機能および本人の希望で行政機関等から提供される電子的な証明書(例えば電子納税証明書)を添付書類として本来の申請先に提出する機能等が必要なことが明らかになった．国民電子私書箱構想は，上記2つの検討結果をマージしたものであり，その実現が強く望まれている．

おわりに

本文では，はじめに社会保障カードの構造に関する検討状況と導入効果の予測を紹介し，次に発行主体と最も信頼性の高い交付手段について解説した．そして最後に，次世代電子行政サービスと電子私書箱を一体とした国民電子私書箱について言及し，電子私書箱の目的と基本機能，社会の受容性とセキュリティの考え方等について述べた．

平成19年からの過去の2年間を見ると，社会保障カード，次世代電子行政サービス，電子私書箱は，それぞれ別々に検討され，それぞれの課題と解決策，そして実現方策の概要等が報告書として公表され，これらの報告書から整備すべきシステムには多くの共通点があることが明らかになってきた．このような背景から，IT戦略本部により国民電子私書箱構想が提案され，その実現に向けた取り組みの開始が決定されたが，社会保障カードとの関係については，現時点では未だ明らかになっていない．

また社会保障カードが，中継DBまたは国民電子私書箱へのアクセスカードとして使われることを考えると，カードに求められる基本機能は，現状の住民基本台帳カードをベースにすることも可能になると思われる．さらに，現在国会に提出されている住民基本台帳法の改正案が成立すれば，市町村をまたがって引越しをしても既存の住民基本台帳カードをそのまま利用することが可能になる．このことは，住民基本台帳カードに社会保障カードの機能を加えるときの最大の課題であったが，この課題が解決される可能性があることを意味している．

今後は，国民電子私書箱，社会保障カード，住民基本台帳カード，次世代電子行政サービスが密に連携して，システム全体の最適化と，利用者にとって真に便利なサービスの提供が実現することを強く望むものである．

文　献

1) 厚生労働省政策統括官付社会保障担当参事官室：社会保障カード(仮称)の基本的な構想に関する報告書，2008年1月
http://www.mhlw.go.jp/shingi/other.html#seisaku
2) 厚生労働省政策統括官付社会保障担当参事官室：社会保障カード(仮称)の在り方に関する検討会　これまでの議論の整理，2008年10月
http://www.mhlw.go.jp/shingi/2008/10/s1028-1.html
3) 首相官邸ホームページ
http://www.kantei.go.jp/jp/singi/it2/index.html
4) 首相官邸ホームページ
http://www.kantei.go.jp/jp/singi/it2/epo-box/houkoku1.pdf

おおやま　ながあき
東京工業大学 像情報工学研究施設 教授：〒226-8503 神奈川県横浜市緑区長津田町4259
yama@isl.titech.ac.jp

医療情報システムのセキュリティ

基本的な考え方と実施手順

東京工業大学工学部附属
像情報工学研究施設教授
大山永昭

●Summary

Security for medical information system – basic concept and implementation

This paper introduces basic concept of security: the balance of the security level and the cost. To optimize their balance, all information property handled by the medical information system should be clarified and listed up. Damages of each property are, then, estimated and measures are taken with taking into account the characteristics of each measure. Responsibility for the security of the medical information property is also discussed for the case of system outsourcing such as ASP and SaaS.

要旨：本文は、セキュリティの基本である安全性レベルとそれに要する費用のバランスについて紹介し、そのバランスを最適化するためには、まず医療情報システムが取り扱うすべての情報資産を明らかにした資産台帳を作成し、次に各資産のダメージを見積もり、対抗策の特性を考慮して最適な対策を講じることが必要であることを示す。また、ASPやSaaSのようなアウトソーシングされたシステムを利用する場合の、医療情報資産の安全性管理に関する責任について検討する。

近年の急速な情報通信技術の進歩は、医療分野の情報化を飛躍的に進展させてきた。医療機関内部のシステムは、ホストコンピュータとダム端末に始まり、ネットワークを利用したサーバー・クライアント方式やASP、SaaSへとその構成は多様化している。当初は、基本的にスタンドアロンであったため、システムを導入する担当部署や機能、目的、規模等の違いにより、オーダリングシステム、放射線情報システム、PACS、電子カルテ、レセプトコンピュータなどと多種にわたるシステムが開発・導入されてきたが、患者情報の一元化やシステムの効率化等を図るために、大規模な医療機関等ではネットワークを用いた統合化が進んでいる。さらに近年では、複数の医療機関が相互連携する地域医療ネットワークシステム等の構築も行われている。

スタンドアロンのシステムは、医療機関内に設置され他のシステムと接続されていないため、必要とされるシステムのセキュリティは、例えば利用者登録とアクセス制限の設定などの基本的なもので構成されていたが、同一医療機関内での他システムとのネットワーク化、レセプト請求のオンライン化、専用回線等を用いた異なる医療機関間のネットワーク化等に従って、より高度なセキュリティ機能が用いられている。本文ではこのような背景から、医療情報システム（広義のHIS）が備えるべきセキュリティについて、運用を含むシステム形態に基づく考え方を解説する。

セキュリティの基本

近年ますます高まる病院業務等の医療情報システムへの依存や個人情報保護に対する意識の高まり、さらにはコンピュータウィルスやハッキング等による被害の発生等により、情報システムのセキュリティ確保は極めて重大な関心事になっている。しかしながら、システムの運用形態や規模などにより、想定される脅威は大きく変わるため、与えられた医療情報システムのセキュリティを適切に確保するためには、セキュリティの基本的な考え方を理解することが不可欠である。

その基本は、かける費用と損害額のバランスで決めるということである。この基本は、一般ビジネスの世界で培われたノウハウの基礎であるため、医療情報の分野にこの考え方を適用するのに違和感を持つかもしれない。しかしここでの真の目的が、業務遂行に不可欠になりつつある医療情報システムを安全かつ確実に適切な経費で運用すること、何らかの事故等で不具合が発生し結果としてある種

の損害が出るとしても、目安となる損害額等が未だ十分に明らかでないために、逆に問題を先送りしてしまうような悪癖を回避すべきこと等に鑑みれば、この基本を理解することは極めて重要であるといえる。

この基本的な考え方をより具体化すると、はじめに守るべき情報資産を定義し、次にその情報資産に対する脅威を洗い出し、要する費用を考慮して適切な対策を選択するということになる。ここで取り得る対策には、①制度、②組織、③技術の3種類があることに注意が必要である。

①の制度的な対策は、新たな制度や法律等を制定（個人情報保護法の制定はこの手法の例）することで、②の組織的な対策は、標語等を用いたキャンペーンの実施（交通安全週間は分かりやすい例になる）等による自主規制の実施で、③の技術的な対策は何らかの技術を導入する（クレジットカード等がICカード化されたのが良い例になる）ことで、想定される脅威に対抗することを意味している。

また、これらの対策には実質的な効力や要するコストなどに違いがあるため、想定される脅威の大きさと被害の度合いを見積もり、要する費用を勘案して最適な対策を講じることが肝要である。ここで、想定されるすべての脅威には必ず何らかの対策を講じることと、万が一の被害が甚大になると予想される脅威に対しては、複数の対策を組み合わせること等による対策の実効性向上を忘れてはならない。

情報資産台帳の作成と対象範囲

前述したように、情報システムのセキュリティを確実に確保するためには、まず、守るべき情報資産を明らかにしなければならない。そしてそのためには、当該情報システムが取り扱っている情報の種別や資産価値等を整理するための棚卸しを実施して、情報資産台帳を作成することが必要である。そして次に、情報資産の管理に係るリスクの所在を明らかにし、そのリスクの低減を図ることが可能となるような方策を検討するという一連の前準備が不可欠である。

情報資産の重要性自体は、個人情報の例でも分かるように、電子データ等と文書の場合で異なるわけではない。従来は、情報システムが扱う電磁的な記録のみを対象とした条例等が制定された例もあるが、近年では紙に記録される情報もその対象に含めるのが一般化している。そのため、情報資産の状況を把握する際には、医療機関等が所有するすべての文書（広義の意味で、各種検査データや画像、カルテ等も含まれる）およびネットワーク等を含む全情報システムを対象としなければならない。

そして資産台帳に記録すべき項目は、例えば、資産の種別、データ形式、資産の所在地と複製の可否、複製した場合の所在場所、資産価値、資産を扱う業務の概要、資産の管理責任者、設定されたアクセス制限と権限を有する人の名簿、資産の発生日時と保有期限、資産に対する処理履歴である。

資産台帳の考え方からすると、個人のUSBメモリ等の可搬媒体やパソコン等のモバイル機器を持ち込んで利用することは、いうまでもなく禁止すべきであるが、これらについては、台帳管理されたデバイスや機器に限定したとしても、それらの機関外への持ち出しや紛失には十分な注意が必要であり、そのためには、利用状況を管理する台帳の作成など手間をかけることが有効である。さらにこれらの機器を機関内等に戻す場合には、コンピュータウィルス等に感染がない等を確認することも重要である。

民間情報処理事業者への業務委託

利用している情報システムが医療機関内で閉じている場合には、情報資産の保護の責任は当該医療機関等に自己完結するが、医療情報等の外部保存やASP、SaaSのようなシステムの利用形態になると、外部機関との責任分解点や何らかの事故等が発生した場合の補償範囲等の明確化等が極めて重要になる。これらの考え方については、厚生労働省医政局が主催している〝ネットワーク基盤検討会〟により作成された〝利用情報システムの安全管理に関するガイドライン第4版〟[1]や、総務省自治行政局が作成・公表した〝地方公共団体における情報資産のリスク分析・評価に関する手引き〟[2]などが参考になる。

ここで留意すべき点としては、保管等の目的で何らかの医療情報が外部機関に置かれる場合でも、その管理責任は当該医療機関等にあるということである。そのため、情報資産

が外部委託先事業者の管理下にある場合についても、その状況を把握し、リスク分析を行うこと等により、安心して委託できる事業者を適切に選択することが望まれるが、現実に各医療機関等がリスク分析等を実施することは困難であると予想される。

他方で、診療録等を専門の民間情報処理事業者が管理することで、医療機関にとっては個人情報の漏洩等のリスクを低減することが可能になると期待される等の理由により、経済産業省からは、〝医療情報を受託管理する情報処理事業者向けガイドライン[3]〟が公表されている。

さらに、ASPやSaaSは医療機関が自ら情報システムを購入・維持・管理等を行う必要がないため、前述のリスク低減に加えて情報処理システムに要するコストを低減できることが期待されること等の理由により、総務省からは〝ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン[4]〟の発行が予定されている。

近年では行政機関や民間企業等においてASPやSaaS等の利用が進展しつつある。このように外部のサービス提供機関と連携して情報システムを運用する場合には、ユーザー組織と情報システムベンダ企業の間で、保障される内容やサービスレベル等を定めたSLA（Service Level Agreementの略）と呼ばれる契約を結ぶことが重要とされている。情報資産の管理責任が、医療機関等の内外を問わず基本的には当該医療機関等にある医療分野で、どのような内容のSLAが効果的かは未だ明確になっていないが、今後は、当事者双方に無理のない妥当な契約に資するための検討が必要であろう。

さらに、多くの大規模病院等で見られるように、業務自体が情報システムに大きく依存している場合には、災害時等におけるBCP（Business Continuity Planの略で、災害等でシステムがストップしたときにシステムの復旧・回復を含む事業継続計画）の作成も必要になると思われる。外部の情報サービス提供機関と連携している場合には、いうまでもなく、当該機関を交えたBCPの作成が必要である。

医療情報システムのセキュリティ確保には抜けのない対策が必要

本文では、医療情報システムのセキュリティを適切に確保するための手順は、まず情報資産を明確にし、次に情報資産の管理に係るリスクの所在を明らかにし、そしてそのリスクの低減を図る対策を適切に講じることであることを説明した。また、医療情報等の外部保存やSaaS等の新たな情報サービスを受ける場合の考え方等を示したガイドラインを紹介した。医療情報システムを安全かつ確実に運用するためには、本文で紹介したセキュリティの考え方を理解し、現状を分析して抜けのない適切な対策を講じることが必要である。

参考文献
1 厚生労働省ホームページ、http://www.mhlw.go.jp/shingi/2009/03/s0301-4.html
2 総務省ホームページ、http://www.soumu.go.jp/menu_news/s-news/02gyosei07_000006.html
3 経済産業省ホームページ、http://www.meti.go.jp/policy/it_policy/privacy/080331iryou-hontai.pdf
4 総務省ホームページ、http://www.soumu.go.jp/menu_news/s-news/02ryutsu02_000005.html

※ ※

大山永昭（おおやま・ながあき）●54年神奈川県生まれ。82年東京工業大大学院総合理工学研究科物理情報工学専攻博士課程修了。83年同大工学部附属像情報工学研究施設助手、86～87年米国アリゾナ大放射線科研究員（画像再構成についての研究）、88年東京工業大工学部附属像情報工学研究施設助教授を経て、93年同教授となり、現在に至る。専門分野は医用画像工学、光情報処理、工学博士。

巻頭論説 「今後の電子政府への期待」第4回

安全・便利な電子政府の実現を目指して

東京工業大学 像情報工学研究施設
大山　永昭

2006年に策定公表されたIT新改革戦略では、電子政府の利用率を向上させるために、オンラインによる電子申請・申告の利用率を2010年には50%以上にするという数値目標を設定した。この目標達成を目指して、各府省は利用率向上策を講じるとともに、内閣官房IT室も、一般の住民にとってより身近となる自治体や電気、ガス等の公共サービスを加えた次世代電子行政サービスの実現方策を検討してきた。これらの取り組みは一定の成果を挙げているが、なかでもe-Taxは操作性の改善やインセンティブ付与等の積極策をとった結果、利用率が大幅に向上した。このことは極めて高く評価できるが、他方で、自動車登録や不動産登記のように一般の個人にとっては利用頻度が少なく、さらに用語等に関する専門知識が必要な手続きを、代理人を介さずに自ら手続きをすることが、如何に難しいかも明らかになってきた。このようなことから住民が利便性を実感できる手続きとして、評価専門調査会は、結婚、妊娠、出産、子育てに関連する諸手続きを取り上げ、特別テーマ検討チームを設置して、具体的な手順等の検討を行った。その結果、順序性のある一連の手続きのワンストップ化の難しさと制度的な課題等を明らかにした。

電子行政が本来目指すべきものをあらためて考えてみると、①行政の効率向上、②国民の利便性向上、③行政の透明性の向上、④行政が保有する情報の正確性の確保などがあげられる。①の行政の効率向上は、例えば業務フローの簡略化等を図るためのBPRの実施、行政が保有する情報システムの統合やオープン化等を通したシステムの全体最適化と経費の削減を意味している。次の②は、各種手続きのワンストップサービスや対象となる住民に対する各種お知らせ等の通知サービス等の実現を図るものである。現在の行政サービスは、基本的に申請主義を採っているが、このようなお知らせや案内等を対象となる個人に直接送付すれば、注意喚起を促すことが可能になり、結果として利用者から便利で有用という評価が生まれると期待される。③の透明性の向上には、行政情報の公開や行政手続きの進行状況の本人開示などがあり、④の正確性の確保は、例えば紙で提出される各種の書類等を情勢システムに入力する際の入力ミスの防止や行政が保有する各種の個人情報の訂正を安全確実に行えるようにすることなどを意味している。

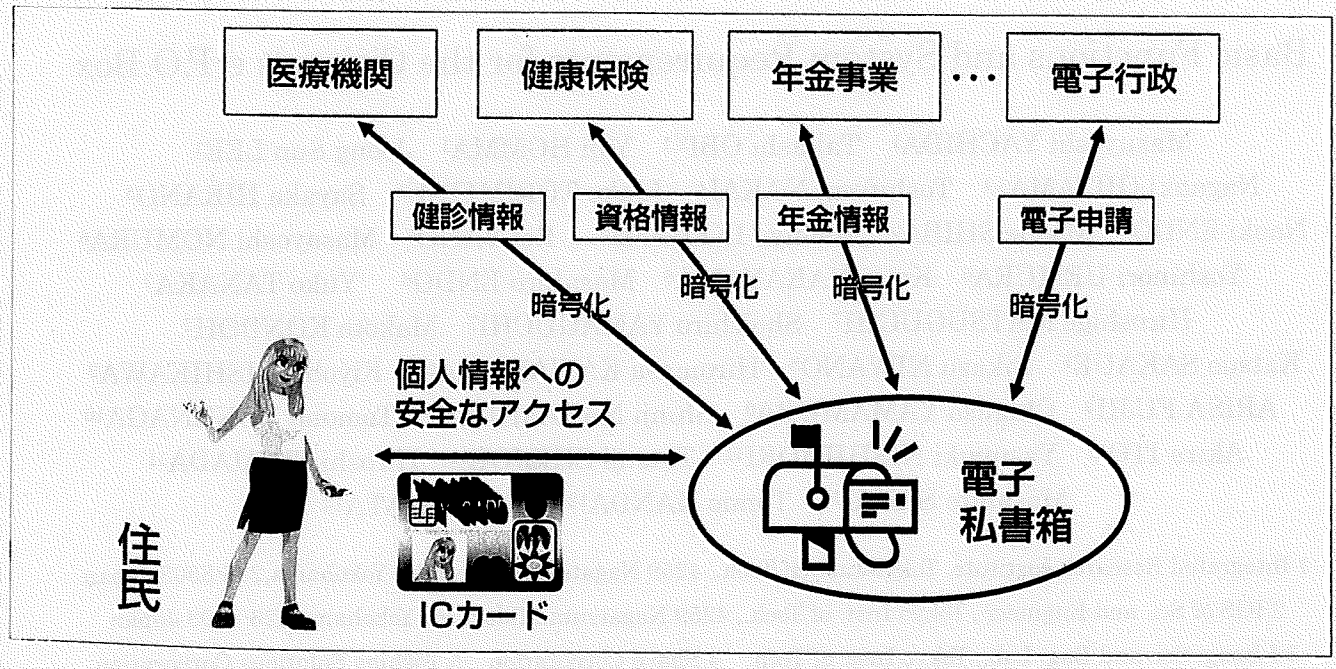
5000万件の宙に浮いた年金納付記録で社会問題になった、いわゆる年金問題を調べてみると、紙による年金納付届けの入力ミス、入力された記録情報の不正な変更、不備や誤った記録の補正、訂正が行われなかったことなどが、その原因として指摘されている。この年金問題を解決することは、言うまでも無く最重要課題であるが、今後、同じ誤りを繰り返さないようにすることも極めて重要であることから、具体的な対策を考えてみる。最初の入力ミスは、人手を介している限りゼロにならない（税の申告等、何らかのロジックを組み込めばOCRでもミスは大幅に減るが）ため、例えば届け出は原則電子化することが必要である。このことは10年来言われてきたことで、やはり電子政府を

目指すのであれば、電子データを主、紙データを従にすることを徹底すべきであろう。2番目の不正な変更に関しては、操作者を特定する認証機能や全ての変更等の履歴を残すことが有効な対策になる。そして最後の不備や誤った記録の補正、訂正については、届けられた納付記録を速やかに本人に知らせ、ミスの有無を確認してもらい、必要な訂正等を行えるようにすれば良いだろう。このように考えると、これらの防止策は年金業務に固有なわけではなく、まさしく電子政府が目指すべきものと一致していることが分かる。

2009年7月、i-Japan戦略2015が公表された。この新戦略では、電子行政、医療、教育・人材育成が3大重点領域とされ、電子政府・電子自治体の重要な政策として、2013年度を目途に国民電子私書箱を実現する旨が書かれている。電子私書箱はその概念図が示すように、健診結果や年金記録、自治体からの各種通知等、現在個人宛に郵送されている情報を、電子データのまま本人に提供する手段として提案された構想であり、その理念は、現金等のフローを安全確実にコントロールできる銀行口座に擬えて、重要な自己情報等の取得や提供を自らコントロールできるようにすることである（**図参照**）。そして機微な個人情報の安全確実なやり取りを可能とするために、ICカード等を用いた私書箱へのアクセス、親展通信を行うための公開鍵暗号方式、公的個人認証サービスやHPKI（Healthcare Public Key Infrastructure）等で提供される電子署名とその有効性を確認するための署名検証機能等のサポートが必要とされている。さらに、便利なオンライン申請・申告を実現するためのナビゲーション（各種手続きのガイド）やコンシェルジェ（一連の手続きを自動的に行う）の機能の付加も構想されている。

現状では、欧米やアジア諸国に比して、残念ながら遅れているといわれる我が国の電子行政ではあるが、電子私書箱を実現すれば、社会保障と電子行政サービスの両方を受けることが容易になる。住民、医療機関、行政機関等を直接結ぶ新たなインフラの上に描かれる将来像を見据えた継続的な努力が、安全・便利な電子政府を実現するために必要である。

図　電子私書箱の概念図



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．

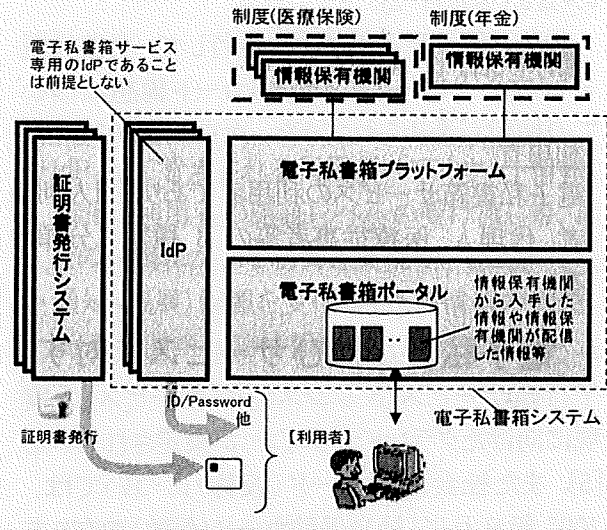


図1　電子私書箱システムに関するエンティティモデル

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

国民電子私書箱を利用した退職ワンストップサービスの検討

小尾高史[1,3]、谷内田益義[3]、本間 祐次[3]、山本寛繁[2,3]、李中淳[3]、大山永昭[2,3]

1 東京工業大学 総合理工学研究科、〒226-8502 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、3 東京工業大学 統合研究院

obi@ip.titech.ac.jp, {yachida, homma, j-lee}@iri.titech.ac.jp, {yamamoto, yama}@isl.titech.ac.jp

あらまし 我々は、国民が自らの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）」に関して、その具体的な実現方策について検討を進めており、それを利用した安全・安心なＩＴ社会の実現を目指している。さらに、本年４月のデジタル新時代に向けた新たな戦略～三か年緊急プラン～では、従来の「電子私書箱」に対して、様々な電子行政サービスを実現するための機能を追加した「国民電子私書箱（仮称）」構想が提案され、あらゆる公共サービスに対する総合口座を実現することが求められるとともに、今後は、次世代電子行政サービス、社会保障カード、（従来の）電子私書箱を一体化した議論をすることが要求されている。これに対して、本研究は、「国民電子私書箱」を利用するワンストップサービスの実現方法を整理し、退職時の様々な手続きを例として、具体的な国民電子私書箱の利用方法を検討したのでその結果を報告する。

Study of an one-stop service for the retirement procedure using the e-P.O.Box System

Takashi Obi[1,3], Masuyoshi Yachida[3], Yuji Homma[3], Hiroshige Yamamoto[2,3],
Joong Sun LEE[3], Nagaaki Ohyama[2,3]

1 Interdisciplinary Grad. School of Science and Engineering, Tokyo Institute of Technology
4259 Nagatsuta-cho Midori-ku Yokohama Kanagawa 226-8502 Japan

2 Imaging Science and Engineering Laboratory, Tokyo Institute of Technology

3 Integrated Research Institute, Tokyo Institute of Technology

obi@ip.titech.ac.jp, {yachida, homma, j-lee}@iri.titech.ac.jp, {yamamoto, yama}@isl.titech.ac.jp

Abstrct It is the current situation that people's social security information is separately managed by each organization and the people cannot access freely to these their own information. On the other hand, e-P.O.Box, a new mechanism collecting individual information easily and providing user-oriented one-stop service, is introduced in "i-JAPAN Strategy 2015". The service of the e-P.O.Box will begin in around 2013. In our research, we deliberate how to use the e-P.O. box in the e-government and discuss how to achieve it.

１．はじめに

現在、国民の社会保障、行政情報などに関する個々の情報は、医療機関や保険者、地方自治体等、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」とされたことを受け、我々は、これまで社会保障サービスに資する電子私書箱の基本機能の検討を行ってきた[3,4]。

しかし、平成21年4月に発表されたデジタル新時代に向けた新たな戦略～三か年緊急プラン～[5]において、希望する個人又は企業に提供される高度なセキュリティ機能を持った電子空間上のアカウントとして、従来の「電子私書箱（仮称）構想」及び「社会保障カード（仮称）構想」[6]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に提供される国民電子私書箱（仮称）が提案された。

そして、平成21年7月のi-Japan戦略2015[7]において、「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である。」と再定義され、「「国民電子私書箱（仮称）」を、広く国民・企業等の間に普及、定着させることなどにより、顧客である国民に対し、以下に掲げる行政サービスを提供する。」とされたサービスの1つとして、幅広い分野におけるワンストップ行政サービスが挙げられることとなった。

我々はこのような状況の下、新たな私書箱構想である国民電子私書箱に関する技術的要求項目を明らかにし、要求定義をまとめる作業を行っている[8]が、本研究では、これら状況を踏まえ、「国民電子私書箱」を利用するワンストップサービスの実現方法を整理し、退職時の様々な手続きを例として、具体的な国民電子私書箱の利用方法を検討したのでその結果を報告する。

2．電子私書箱を利用したワンストップサービスの考え方

ワンストップサービスには、様々な提供形態が考えられるが、本章では、公共的分野に関連するワンストップサービスの考え方を整理するとともに、電子私書箱を利用したワンストップサービスの考え方についてまとめる。

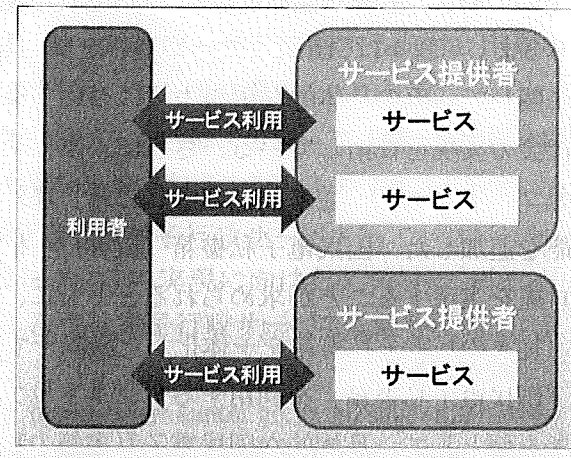


図1　従来型のサービス利用・提供

一般的に、ワンストップサービスとは、利用者が一か所もしくは一度の手続きで必要とする関連作業を一括して完了できるよう設計されたサービスのことを指し、従来は利用者がサービス提供者との間で個別に行っていた手続きなどのサービス利用を（図1参照）一括して行えるようにするものである。

ワンストップサービスの最も代表的な例としては、引っ越しなど住民のライフイベントに沿って必要となる複数の機関等にまたがる様々な申請・届出を一括して手続きできるようにしたものがあり、引っ越し手続き、結婚手続き、出生手続き、退職手続きなどがその対象として挙がっている。

ここで、今回の国民電子私書箱構想によるワンストップサービスの検討を待つまでもなく、従来からワンストップサービスを実現するための検討は行われてきた。先に述べたように、ワンストップで取り上げられる手続きには、ライフイベント

に関するものが多いため、住民などの利用者から見た際には、自治体等を直接の窓口としたものが多い。自治体等で提供されるサービスの内容は様々であるが、ワンストップサービスとしては、大きくは「申請手続き型」「情報照会型」の二つに分類することができる。

「申請手続き型」は、従来の行政サービスの申請手続きをベースとしてワンストップ化を図ったものであり、申請や届出を受け、決められた業務の流れに従って処理を行うサービスである。具体的には、利用者からの複数のサービスに対する申請・届出を一括して手続きするものであり、ポータルサイトにおいて利用者の申請や届出を受けて、処理の結果を返すものである。手続き例としては、引っ越し、結婚、出生など、ライフイベントに沿って必要となる複数の申請・届出を、一括して行う手続きがあり、一種のワークフローに従って、順次処理が行われるため、各サービス提供者による作業が順次必要となる手続きでは、申請から結果通知という一つのワンストップサービスが完了するまでに時間がかかる場合も考えられる。

「情報照会型」は、利用者が、一度に複数のサービスから情報を照会または検索するものであり、複数のサービス提供者から、同時に情報を収集し、利用者に対して必要な情報を返すものである。このサービスは、利用者からの情報取得の要求に応じて複数のサービスから情報を取得し、これら情報を合わせて提供するサービスであり、利用者に対する新たな付加価値をもったサービス提供の可能性を含んでいる。手続き例としては、複数のサービス提供者や複数の業務で管理されている情報について、新たな観点や別の視点から関連する情報をまとめて利用者に提示したり、検索結果を返還するものなどが考えられ、現状の考えられるものとしては、地域の図書検索サービスなどがある。

その他に、これらをまとめた総合的なワンストップサービスも考えられるが、ここでは省略する。

このような、ワンストップサービスを実現するために必要となる技術要素として、「ポータル」、「認証・署名」、「バックオフィス連携」、「標準化」が挙げられており、従来型ワンストップサービスにおいては、特に、「バックオフィス連携」を充実させることにより、行政機関間の連携を実現し、添付書類などを省略することを目指している（図2参照）。

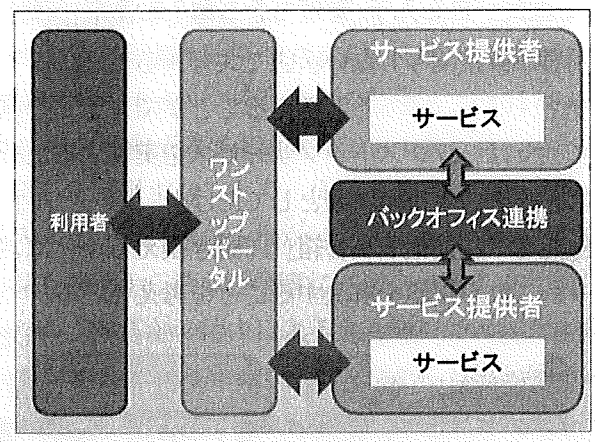


図2　従来型ワンストップサービスの考え方

しかしながら、現在ワンストップの対象となる様々なサービスは、サービス提供者ごとに独自のシステムを利用して行っており、関係する機関間で連携できる既存の仕組みは存在しない。このため、バックオフィス連携を実現するためには、すべてのサービス提供者間で新たなインタフェース仕様を決める必要があるだけでなく、以下のような課題を解決する必要がある。

1. バックオフィス連携を効率的に実施するためには、行政機関等のサービス提供者におけるデータ等の標準化を進める必要がある。
2. セキュリティリスクを考慮して、取り扱う情報は一カ所に蓄積して集中管理せずに各機関で保有し、各機関が保有するデータベース間の連携は疎結合により実現することが望まれる。
3. サービス提供者で個人情報を共同利用する際は、必ず利用者本人の同意を得る必要がある。
4. 利用者が自分の情報がいつ、どこからどこへ送付されたか確認できる仕組みが必要である。
5. 利用者の情報を共同利用する機関に対して、

バックオフィス連携のための機関（電子行政分野では、「行政情報の共同利用支援センター（仮称）」などが提案されている）を介して得た情報の蓄積および目的外の利用を禁止する必要がある。

ここで、課題2から5は、利用者の情報を利用者が直接関与しない状態で共有することにより発生する問題であると考えることができる。そこで我々は、ワンストップサービスを実現するために必要となる技術要素としてあげた「ポータル」、機能を「国民電子私書箱」に置き換えることにより、これら課題を解決することを考えている。

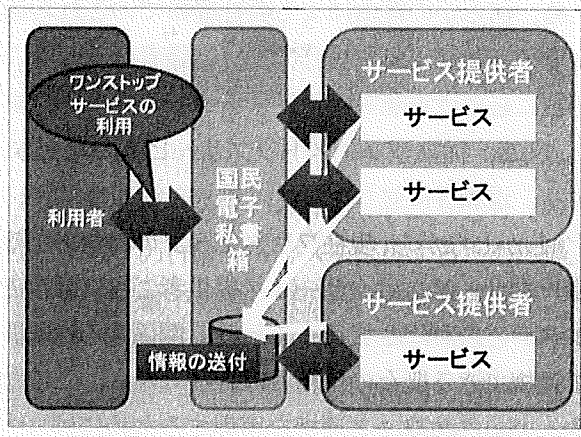


図3　国民電子私書箱を利用したワンストップサービスの考え方

例えば、バックオフィス連携ができない機関がある場合には、図2に示すワンストップサービスを提供できない。そこで、連携に必要な情報を電子的に国民電子私書箱に交付し、電子私書箱を起点としてワンストップサービスを行う仕組みを提供する。さらに、国民電子私書箱側に情報を交付することにより、国民電子私書箱の有するコンセルジュ機能を用いて利用者が気付いていない手続を利用者に提示するなど、付加価値の高いサービスを提供可能となり、利便性の高いワンストップサービスを実現できる。また、利用者が自分の情報の制御に積極的に関与することになるため、従来問題になっていた、利用者に対する自己情報コントロール権付与の問題を解決できる可能性があると考えられる。

このように、従来型電子行政サービスで考えられていたポータル機能を国民電子私書箱に置き換えることにより、国民電子私書箱を経由して得られる情報や私書箱内に保存された情報を利用して、これら情報を起点とする新たな付加価値を有するサービスを展開することが可能となる。

3．電子私書箱を利用した退職ワンストップサービスの実現

現在、企業は従業員の退職に伴い、年金、医療保険、雇用保険、国税、地方税に関する手続をそれぞれ別々に行う必要がある。これら手続は、非常に煩雑であることが知られており、企業担当者、退職者は、社会保険事務所や健康保険組合など6ヶ所以上の機関を訪問し、健康保険被保険者証や出勤簿、賃金台帳など15種類以上の書類を添付した申請などを行う必要がある。

このようなことからも、退職者自身は、自分の退職に際して、何のために何をしなければならないのかを正確に把握することは困難であり、企業でも退職者への説明にかなりの時間が割かれているのが現状である。

このような現状を受け、平成19年10月に設置され、様々な行政手続を基本的にワンストップで簡便に行える次世代の電子行政サービス基盤の検討を行っている「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」では、平成20年6月の「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」において、優先的に検討すべきワンストップサービスの具体例として、退職手続を挙げている。

しかしながら、現在までの検討では、主にバックオフィス相互間の連携やフロントオフィスとバックオフィス、民間手続との連携等を図ることにより、それを実現するものとしており、前章で述べた利用者主体の情報管理によるワンストップサービスを実現する方法は明らかになっていない。

本章では、我々が検討を進めている国民電子私書箱の有する機能[8]を利用して、どのように退職ワンストップを実現するかを示す。

電子私書箱の機能構成についての検討を別途進めているが、基本的なシステム構成は、図４で示すものになると考えられる。基本システムを構成する各機能は、利用者が電子私書箱へアクセスするために利用する認証機能、電子行政、社会保障サービス等の入り口となるポータル機能、利用者の情報の制御及び送受信を行う私書箱サービス機能、公的情報保有機関と電子私書箱との関連づけを行う私書箱プラットフォーム機能の４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プラットフォーム機能を介して送付される。

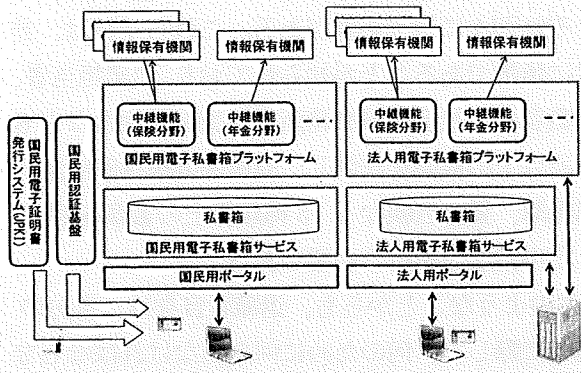


図４　国民電子私書箱のシステム構成

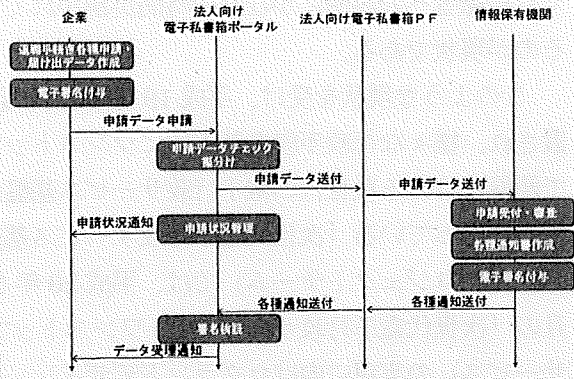


図５　企業の行う手続きのフロー概略

さらに、企業等については、国民向けと同等の機能を有する法人向け電子私書箱が提供され、企業と情報保有機関間の情報のやり取りには、法人向け私書箱が利用され、法人から国民への情報送付は、法人向け私書箱プラットフォームと国民向け私書箱プラットフォームが連携することで行われる。

まず、退職時の企業が行う退職手続き（図５）は、企業内で一括して申請書類を作成したのち、これらをまとめて法人向け電子私書箱ポータルに送付することにより行われる。このとき私書箱ポータルは、ポータル利用者を支援するコンセルジュ機能を有しており、送られてきた情報をその内容をもとに振り分け、適切な情報保有機関へ送付する働きをする。これにより、企業側は必要な処理をワンストップで行えるようになり、事務処理等の負担は大きく減ることになる。

次に退職者本人の手続き（図６）だが、電子私書箱を利用することで、従来退職時の会社経由で入手しなければならなかった各種通知書は、情報保有機関から直接退職者に送付されることになるため、何らかの理由による会社経由でのこれら通知書の入手が困難な場合でも、退職者はその後の処理に必要は書類等を入手することができる。また、私書箱ポータルの有するコンセルジュ機能により、退職者に対して、送付された情報をもとにその後、どのような手続きをどのような理由で行うのか、必要な手続きにはどのようなものが存在するかを適切に提示することができ、退職者は、必要な手続きを正しく正確に実行できるようになると予想される。

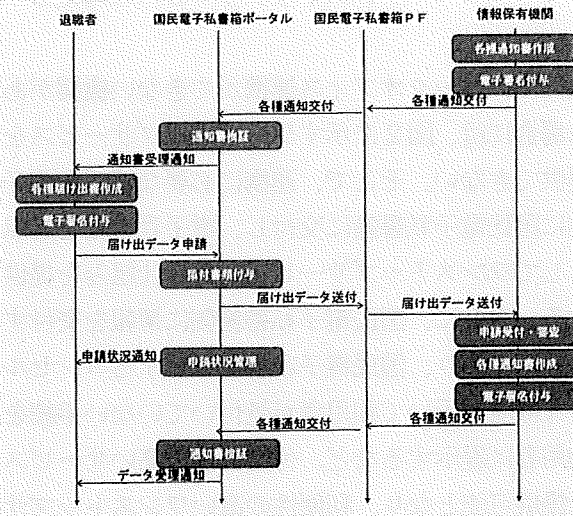


図６　退職者本人の行う手続きフロー概略

４．まとめ

本発表では、我々が想定する国民電子私書箱を利

用したワンストップサービスの実現方法を整理し、退職時の様々な手続きを例として、国民電子私書箱の利用方法を検討した。

今後は、今回の検討結果をもとに、国民電子私書箱が具備すべき機能を整理し、各機能を利用してどのようにシステムを構築するかの検討を行い、実際に退職ワンストップをデモンストレーションするためのシステムを構築する予定である。

5．謝辞

本研究は、文部科学省科学研究費（課題番号21651072)、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。

参考文献

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 小尾、柏木他、“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,” 信学技報, IEICE-108, pp.15-22, 2008

4 柏木、小尾他、“電子私書箱で実現するサービスの検討,” SCIS2009, Jun. 2009

5 デジタル新時代に向けた新たな戦略～三か年緊急プラン～, http://www.kantei.go.jp/jp/singi/it2/kettei/090409plan/090409honbun.pdf , Mar. 2009

6 社会保障カード（仮称）の基本的な計画に関する報告書, http://www.mhlw.go.jp/shingi/2009/04/dl/s0430-4b.pdf, Mar. 2009.

7 i-Japan戦略2015, http://www.kantei.go.jp/jp/singi/it2/kettei/090706honbun.pdf, Jul. 2009.

8 谷内田、小尾他、“国民電子私書箱の基本機能とシステム要件,” CSS2009, Oct., 2009.

様々なサービスへの対応を可能とする サーバ連携型 IC カードシステムの実現方式の検討

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

1 東京工業大学 統合研究院 〒226-8503 神奈川県横浜市緑区長津田町 4259
2 東京工業大学 総合理工学研究科 〒226-8502 神奈川県横浜市緑区長津田町 4259
3 東京工業大学 像情報工学研究施設 〒226-8503 神奈川県横浜市緑区長津田町 4259
E-mail: [1] homma {yachida,j-lee}@iri.titech.ac.jp, [2]obi@ip.titech.ac.jp, [3]yama@isl.titech.ac.jp

あらまし 現在、政府は社会保障や電子行政分野において、個人単位で自己の情報を管理・閲覧できる仕組みである電子私書箱の導入に向けた検討を進めている。電子私書箱へのアクセスには、社会保障カード等の個人認証機能を有する公的 IC カードの利用を想定しているが、将来的には、金融決済などの民間サービスについても電子私書箱を介して対応することが想定されており、公的 IC カードに搭載された公的な個人認証機能を利用できないサービスの出現も想定される。また、仮に公的 IC カードに民間の提供する認証機能が追加可能であったとしても、その処理は非常に煩雑である。これに対して、本発表では、ネットワーク上のサーバへ認証鍵の追加を行うことにより IC カードの取扱いを簡便化するサーバ連携型 IC カードシステムの基本構成と、それをどのように実現するべきかを検討したので報告する。

Study of Implementation Method for Server Cooperated I C Card System Corresponding to Various Services

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

1 Integrated Research Institute, Tokyo Inst. of Tech., 4259 Nagatsuta Midori Yokohama,226-8503 Japan
2 IGS of Sci. and Engineer., Tokyo Inst. of Tech., 4259 Nagatsuta Midori Yokohama,226-8502 Japan
3 Imag. Sci. and Engeer. Lab., Tokyo Inst. of Tech., 4259 Nagatsuta Midori Yokohama,226-8503 Japan
E-mail: [1] homma {yachida,j-lee}@iri.titech.ac.jp, [2]obi@ip.titech.ac.jp, [3]yama@isl.titech.ac.jp

Abstract. Japanese government is considering introducing e-P.O.Box which makes it possible for people to manage their own information on an individual basis. It is assumed that official IC Cards having certification function such as the Social Security Card are used to access to e-P.O.Box, private services such as a financial settlement being expected to use it. However, the certification function of the IC Cards cannot be applied to some newly added services, or the processing of the certification would be complicated. In this paper, we deliberate basic architectures of Server Cooperated IC Card System to solve the problem, and discuss how to implement it.

1. はじめに

現在、政府は国民視点に立った電子政府の実現を政策目標に掲げており、その一環として、2007 年 4 月に IT 戦略本部が取りまとめた「IT 新改革戦略 政策パッケージ」[1]に、これまで医療機関や保険者等、機関毎に個別管理されていた情報を個人単位で管理・閲覧することが可能となる電子私書箱（仮称）の創設や、年金手帳、健康保険証、介護保険証としての役割を果たす社会保障カード（仮称）の導入、さらには民間