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

も含めた社会保障分野以外への電子私書箱の利用拡大が盛り込まれている。また、社会保障カードの具体的な導入方策等を検討した厚生労働省の「社会保障カード（仮称）の在り方に関する検討会」が2009年4月に取りまとめた報告書[2]では、年金情報の閲覧や医療機関における健康保険の資格確認等に際して、社会保障カードが電子私書箱へのアクセスキーとして用いられることが想定されている。加えて、2009年7月にIT戦略本部が取りまとめた「i-Japan 戦略2015」[3]では、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行政サービスを実現する「国民電子私書箱（仮称）」を2013年までに実現することが盛り込まれた。

一方、2008年9月に同本部が取りまとめた「オンライン利用拡大行動計画」[4]においては、既存の電子申請等の利用が未だ低調であり、その原因の一つはサービスを利用するために必要な手続きの利便性に問題があるためであるとの認識が示され、その具体的な解決策として「中央サーバに認証機能を一部移行させることによって、個人がオンライン上で簡易にサービスを受けられる方策」が例示されている。しかしながら、電子私書箱や社会保障カードに関連する政府の検討会等において、その具体的な実現方法は検討されていない。

本研究では、これらの状況を踏まえ、電子私書箱を利用するサービスが追加される場合や、電子私書箱と連携する民間のサービス等が提供される場合に、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、アクセスキーとして用いられる社会保障カード等の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する。

2. サーバ連携型ICカードシステムの概要

2.1. 多目的ICカードを用いる場合の課題

1章で述べたように、電子私書箱は各種の社会保障サービス、行政サービスの利用や、民間分野と連携したサービスの利用が想定されるため、社会保障カード等の公的ICカードを電子私書箱などで提供されるサービスへのアクセスキーとして利用する場合、当該カードには複数のサービスを利用するための異なる認証鍵を格納する必要が生じる（図1）。すなわち、この場合、当該カードは多目的ICカードとして利用されることとなるが、これには次のような問題点がある。

(1) カードの記憶容量の制約により、利用できるサービスの数に制限が生じる。
(2) 電子私書箱が民間サービスを含め将来的にどのようなサービスに利用拡大されていくかが明らかでなく、導入時点のカードの仕様によっては利用追加ができないサービスが生じる可能性がある。
(3) カード保有者がサービス追加を行う度に窓口まで赴き新たな認証鍵の書き込みを行う必要がある。

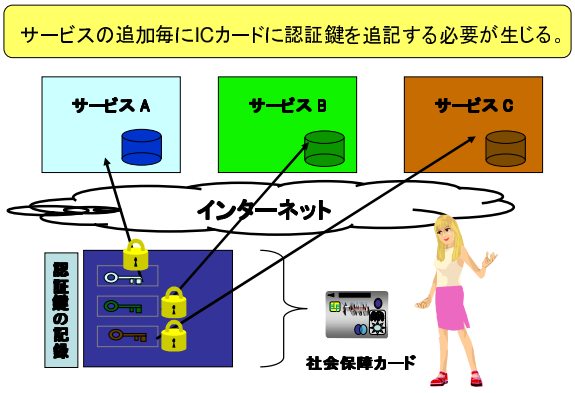

図1　多目的ICカードを用いる場合の課題

特に、社会保障カードは全国民に配布されることも検討されており、当初のカード配布だけでも膨大な窓口業務の発生が想定されているため、サービス追加の度に利用者が窓口に赴く運用を行うことは、利用者の利便性向上のみならずカードを発行・運用する国や自治体等の円滑な事務の遂行の観点からもなるべく避ける必要がある。

2.2. サーバ連携型ICカードシステムの概要

2.1.項で述べた多目的ICカードを用いる場合

の課題を解決するためには、提供されるサービスの認証鍵を統一する、あるいは特定のサービスについて利用者認証を行った上で、当該サービスと他のサービス間で認証連携を行い、シングルサインオンを実現するといった解決策が考えられるが、電子私書箱の用途を拡大するために行政や民間における多数の既存サービスの認証方法に変更を求めることは導入に要する手間や費用の点で現実的ではない。

これに対して、オンライン利用拡大行動計画において言及されているように、認証機能の一部をネットワーク上のサーバに移行させることにより、既存サービスのシステムに大きな変更を加えることを避けることができる（図2）。

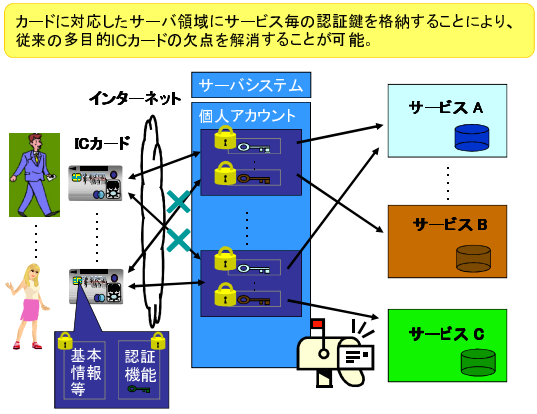

図2　サーバ連携型 IC カードシステムの概要

本発表では、認証機能の一部をネットワーク上のサーバに移行させる仕組みを、以下のような構成により実現することを提案する。

(1) サービスの利用に必要な認証鍵等をネットワーク上のサーバに格納

従来 IC カードに格納されていたサービスの利用に必要な認証鍵や関連情報をネットワーク上のサーバに格納する。

(2) サーバが利用者を認証するための認証鍵等を IC カードに格納

サーバが利用者を認証するために必要な認証鍵や利用者の基本情報を IC カードに格納する。(1)、(2)により、IC カードにはサーバへアクセスするために必要な認証鍵等の情報のみが格納されることとなる。

(3) サーバが利用者認証を実行して利用者の希望するサービスにアクセス

まずサーバが利用者の保持する IC カードとの間で利用者認証を行い、次に利用者のサービス要求に従って、サーバが自身に格納されている当該サービスに対応した認証鍵を用いてサービス提供者との間で認証を行った上で、利用者が当該サービスを利用可能とする。

以上のように、提案システムでは、利用者がサービスにアクセスするための認証に必要な認証鍵等の情報をネットワーク上のサーバに移行し、IC カードや端末など利用者側の仕組みをなるべく簡略化するとともに、サービス提供者が行う利用者認証をサーバと連携して間接的に行うことを可能とする。以下、提案システムを「サーバ連携型 IC カードシステム」と呼ぶ。

なお、多目的 IC カードとサーバ連携型 IC カードシステムを比較した場合、サービス提供者側から見ると、利用者の保有する IC カードとネットワーク上のサーバの組合せが、多目的 IC カードと同様の機能を有するものとして機能しており、前述のように本システムの導入に伴うサービス提供者側の既存システムに対する変更を少なく抑えることができる。

2.3. サーバ連携型 IC カードシステムの利点

サーバ連携型 IC カードシステムは、以下に示す利点を有しており、2.1.項で述べた多目的 IC カードにおける課題の解決を可能とする。

(1) 追加サービス開始時の効率性

提案システムでは、ネットワーク上のサーバに認証鍵を追加することにより、利用者が保持している IC カード自体にはサービス用の認証鍵を追加せずに新たなサービスを利用可能とする。このため、利用者が窓口に赴き IC カードの書き換え処理を行う必要がなくなり、利用者の負担軽減、運用者側の運用コスト削減、サービス開始に要する時間の短縮を図ることができる。

(2) 認証機能のメインテナンスの効率性

電子証明書の有効期間満了に伴う認証鍵

の更新が容易であり、また、暗号アルゴリズムの危殆化への対応や認証方式のバージョンアップ等に伴う鍵情報の変更作業も軽減される。

(3) IC カード紛失時の不正アクセス防止の容易性

万一、利用者が IC カードを紛失した場合には、サーバに対して IC カードの失効処理を行うことで即時に第三者の不正利用を防止することが可能となる。

(4) データ容量や処理能力の向上

IC カードに格納できる情報量は当該カードの記憶容量の制約を受けるが、サーバに認証情報を移行させることによりこの制約から開放される。

社会保障カードの導入に関しては、同一のカードを住民基本台帳カードとしても利用可能とすることが検討課題の一つとなっているが、我々の提案するサーバ連携型 IC カードシステムの仕組みを用いることにより、発行済の住民基本台帳カードを社会保障サービスも含めた多目的なカードとして活用することも技術的には可能となる。また、サービスアクセスに係る処理も、サーバとサービス提供者間で行う方が、高速化が図られる可能性が高い。

3. サーバ連携型 IC カードシステムの実現方法

3.1. サーバ連携型 IC カードシステムへの要求条件

我々の提案するサーバ連携型 IC カードシステムを実現する場合、その前提として、2 章で述べたように、既存サービスのシステムに大きな変更を加えることなく導入可能であることが求められる。また、将来新たなサービスを実現する場合においても、新サービスの導入が容易な構成となっていることが望ましい。これらを前提とすると、サーバ連携型 IC カードシステムへの要求条件を以下のように整理することができる。

(1) 既存システムで実現されている事項からの要求

① サービス内容

IC カードを用いた主要な既存サービスと同等の内容のサービスが提供可能であること。

② セキュリティ

IC カードを用いた主要な既存サービスと同等のセキュリティが確保可能であること。従来 IC カードに格納されていた認証鍵等の情報は耐タンパー領域に書き込まれていたことから、当該情報をネットワーク上のサーバに移行させる場合も、運用上同等レベルのセキュリティが確保されるようにする必要がある。

③ スケーラビリティ

IC カードを用いた主要な既存サービスと同等規模のサービス提供が可能であること。すなわち、IC カードの発行枚数×提供サービス数の認証鍵をネットワーク上に適切に配置されたサーバに格納しながら安定的な運用を行うことが求められる。

④ 利用者インタフェース

IC カードを用いた主要な既存サービスと同等の利用者インタフェースを確保可能であること。

⑤ 運用性・可用性

IC カードを用いた主要な既存サービスと同等の運用性・可用性が確保可能であること。すなわち、計画的なメインテナンスのための最小限のサービス停止を除き、原則 24 時間連続運用が可能であることが求められる。

(2) 新サービス実現からの要求

⑥ サービス提供者インタフェース

サーバ連携型 IC カードシステムが提供する認証機能を各サービス提供者のアプリケーションサーバが容易に利用可能となるような標準的なインタフェースを有すること。

⑦ 認証の最適化

本人認証レベルの異なった業務サービスへの仲介を情報の重要性やセキュリティ等を考慮した上で最適化可能であること。すなわち、IC カードを用いた利用者認証を基

本とするものの、幅広い利用を想定する観点からそれ以外の ID・パスワードによるアクセス等も許容し得ることが求められる。

3.2. 耐タンパーサーバの実装方法の検討

3.1 項で示した要求条件を実現するためには、サーバの実装方法及びネットワークの構成方法についての検討が必要となる。本節では、提案システムの実現に当たってより優先度が高いと考えられるサーバの実装方法について述べる。

3.1 項で示した要求条件②から導かれるように、サーバ連携型 IC カードシステムに用いられるサーバは、認証鍵の格納に当たって IC カードと同等の耐タンパー性が要求されることとなる。以下、このような機能を有するサーバを耐タンパーサーバと呼ぶ。

ここで、耐タンパーサーバの実装に利用可能と考えられる要素技術としては以下を挙げることができる。

(1) HSM（Hardware Security Module）

IC カードと同様に物理的な耐タンパー性を有し、内部で鍵の生成・管理・廃棄を行うことができるハードウェアである。ただし、既存の製品では 1 台の HSM で管理できる鍵の数は数百程度のオーダーであり、費用対効果を考えると社会保障カードが想定しているような大規模なサービスに直接対応した台数の HSM を用意することは現実的とは言い難い。

(2) TPM（Trusted Platform Module）

物理的な耐タンパー性を有するセキュリティチップであり、PC 等で端末の個別識別や OS のセキュリティ確保等に用いられている。HSM 同様に単体の TPM で管理できる鍵の数は限られており、費用対効果の観点から多数の TPM を用意して大規模なサービスに対応することは現実的ではない。なお、TPM を後述の VM 技術により仮想化した技術の検討も行われている。

(3) セキュア OS

セキュリティ機能を強化した OS であり、ユーザ毎のアクセス権制御、複数管理者間の権利分散、ファイルやプロセス毎の機密ラベル制御等の機能を有する。セキュア OS 自体はソフトウェアであるので、IC カードと同等の物理的な耐タンパー性を確保するには別途の工夫が必要となる。

(4) VM（Virtual Machine）技術

単独のハードウェアを仮想的に複数のハードウェアとして機能させるソフトウェア技術である。これにより、ある VM におけるセキュリティ上の脅威が同一ハードウェア上の他の VM に波及することを回避することができる。

以上のように、各要素技術単独では耐タンパーサーバに対する要求条件を満たすことが困難であるため、複数の要素技術を組み合わせたり、鍵情報の保護方法に工夫を加える等の手法も併用する必要がある。本発表では、現実可能性の高い方法として、以下の 2 種類の実装方法を提案する。

3.2.1. VM、セキュア OS、TPM を組み合わせる方法

サーバ上に VM 技術を利用して各サービス認証及び利用者認証機能を提供する VM を構築する。各 VM 上ではセキュア OS を稼働させ、それぞれの認証鍵を管理する。また、各 VM のアクセス管理に用いる鍵をサーバに実装された TPM または VM 毎に設けられた仮想 TPM に格納する。利用者認証又はサービス認証を行う場合、まず TPM に格納された管理鍵を用いて希望する VM にアクセスし、VM 内で利用者認証又はサービス認証を行う（図 3）。

各認証鍵は格納されている VM の外に持ち出されることがなく、VM へのアクセス鍵も TPM によって管理されているため、IC カードと同等の物理的な耐タンパー性を実現できる。また、TPM に格納する管理鍵の数も提供サービスの種類と同程度のオーダーに留まるため、ハードウェアの規模も現実的な範囲に抑えることができる。

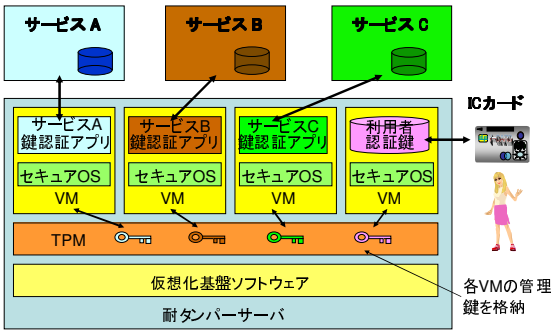

図3　VM、セキュアOS、TPMの組み合わせによる耐タンパーサーバのイメージ

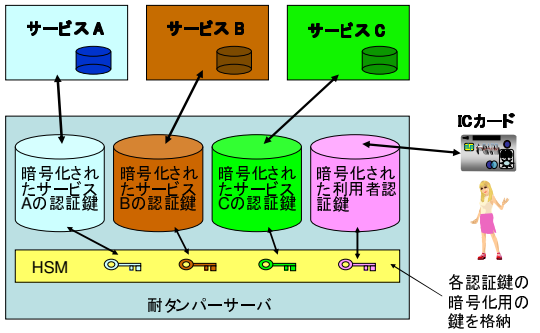

図4　HSM及び認証鍵の暗号化の組合せによる耐タンパーサーバのイメージ

3.2.2. HSM及び認証鍵の暗号化を組み合わせる方法

利用者認証鍵及びサービス認証鍵を暗号化してサーバに格納し、当該暗号化に用いた鍵をHSMに格納する。認証鍵を用いる際には、暗号化された認証鍵をHSM内で復号した上で利用者認証やサービス認証を行う。鍵情報はHSMの外に持ち出されることはないため、ICカードと同等の耐タンパー性を実現できる一方、HSMに格納する情報は暗号に用いる鍵のみでよいため、複数の暗号用鍵を用意するとしてもHSMの数を大幅に減少させることが可能となる。

4. まとめ

本発表では、我々が想定するサーバ連携型ICカードシステムの満たすべき要求条件と、それを実現するための耐タンパーサーバに注目した基本的なシステム構成及び実装方法の検討を行った。

今後は、ネットワークも含めたサーバ連携型ICカードシステムの実現方法及びバックアップや連続運用等に関する運用方法についても検討を行い、政府における電子私書箱や社会保障カードのシステム構築検討に際してサーバ連携型ICカードシステムが有用であることを示していく予定である。

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] 社会保障カード（仮称）の在り方に関する検討会報告, http://www.mhlw.go.jp/shingi/2009/04/s0430-4.html, Apr.2009

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

[4] オンライン利用拡大行動計画, http://www.kantei.go.jp/jp/singi/it2/kettei/080916honbun.pdf, Aug.2008