6S－5

光・ICハイブリッドカードを用いた行政電子化サービス*

砂田 智　田代 太一　徳田 安史　岡田 謙一　松下 温†
慶應義塾大学‡

1　はじめに

次世代マルチメディアサービスの一つとして、自治体をはじめとする公的機関が国民に対して行っている公的サービスの電子化・ネットワーク化に注目が集まっている。

本研究は通産省の外郭団体であるNEDOの委託プロジェクトとして、府中市、横浜市、メーカー各社の協力の元、行政サービスの電子化問題に取り組むものである。今回のプロジェクトでは実際に「光・ICハイブリッドカード (図1)」を使用し、自治体間の住所移転、証明書発行 [2] を行なうシステムを構築し、運用実験を行なったことを報告する。

2　実験サービス

今回の実験では、サービス提供者を府中と横浜の各市役所とし、インターネットを通して提供するサービスも以下の4種類に限定した。

- 自治体間ワンストップサービス
- 電子化証明書発行サービス (2種類)
- 電子回数券発行サービス

2.1　自治体間ワンストップサービス

現在引越しの際には、様々な場所へ出向いて住所変更の手続きを行わなくてはならない。役所での転出手続き、転入手続きはもとより、その他郵便局、ガス・水道・電気会社、電話局等にも通知をする必要がある。

ワンストップサービスとは、これら複数の手続きを、役所への一回限りの届出で全て自動的に済ませるサービスである。

今回の実験では自治体間で行なわれるサービスに限定した。処理として

・転入手続き・転出手続き・印鑑登録移転手続きの3種類を自動的に行なう。

2.2　電子化証明書発行サービス

・住民票の写し・印鑑登録証明書

を電子情報化し、インターネットを通し発行する。

発行された電子証明書は光・ICハイブリッド・カード内に記録される。

2.3　電子回数券発行サービス

証明書の発行では、課金が必要である。そこで、プリペード型の電子回数券方式を決済方式として実験に用いた。

電子回数券も光ICハイブリッド・カードに記録される。

3　実験システムの概要

3.1　認証機関

本システムでは、住民にカードを発行し、デジタル署名用の鍵の割り当て・管理を行なう認証機関 (Certification Authority) の存在を前提としている。発行された全ての公開鍵には、認証機関がその正当性を保証した**公開鍵証明書**が付加される。

また、認証機関にはKerberos認証 [3] システムに基づく認証サーバ (⇒3.4) を設置し、認証チケットベースのユーザ・自治体間認証を実現する。

3.2　カードの機能

カードのIC部は、演算機能として、FEAL暗号による暗号化/復号化、E-signによるデジタル署名作成と署名検証、RSA公開鍵による暗号化が可能である。

光・ICハイブリッドカードは、このIC部の演算機能と、光部の大容量という長所を合わせ持つことにより、多くの情報を安全に記録することができる。

ただし、今回の実験では、IC部へのプログラミングを行なう余裕がないため、これらの演算機能は搭載せず、処理はクライアント端末上で行なった。

*Electronical Administrative Service using an Optical IC Hybrid Card
†Akira Sunada, Taichi Tashiro, Yasufumi Tokuda, Kenichi Okada, Yutaka Matsushita
‡Keio University

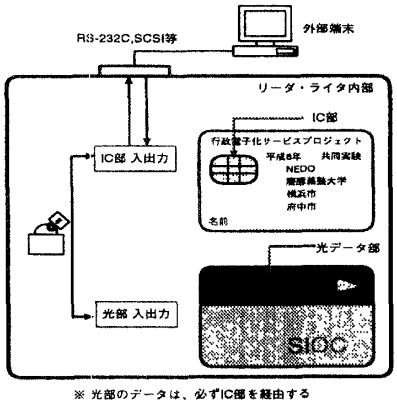

図 1: 光・IC ハイブリッドカード

3.3 認証方式

[1.ユーザ・カード間認証]

サービスを受ける時は、まずカード内に記録されている指紋情報とユーザの指紋とでユーザの認証を行なう。

[2.ユーザ・自治体間認証]

Kerberos 認証チケットとデジタル署名を応用した独自の認証方式を用いる。

3.4 サーバ/クライアント構成

サーバには大きく分けて次の3種類がある。サーバ構成は図2に示す。

- 認証サーバ
  認証機関に設置され、Kerberos 型のユーザ認証を行ない、自治体サービスを受けるためのサービスチケットを発行する。
- サービスマネージャ(proxy サーバ)
  ユーザからの要求を受けつけ、ユーザに代わって各サービス提供サーバから必要なサービスを取得する。サービス開始時には認証サーバの発行したチケットの認証を行なう。
- 各サービス提供サーバ(アプリケーションサーバ)
  ワンストップ、住民票、印鑑登録証明書、そして電子回数券それぞれのサービスを提供するサーバである。基本的に1つのサービス毎に1つのサーバが存在し、必要なデータベースへのアクセスを行なう。

クライアント情報端末にはタッチパネル・指紋読み取り装置が内蔵されている。

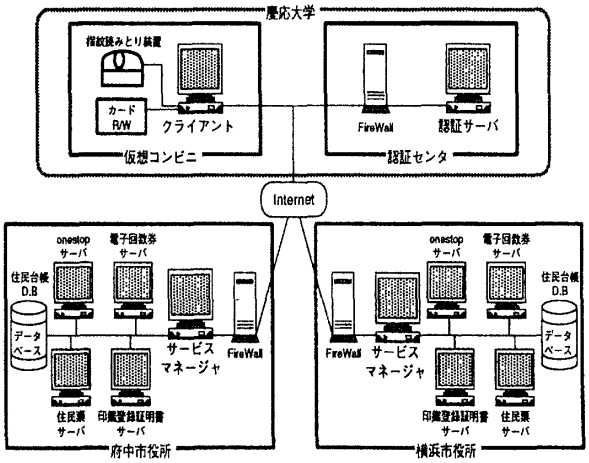

図 2: システム構成図

- サービスクライアント
  タッチパネルによるユーザからの入力受けつけ、ユーザのカードとの通信、GUI の提供、ならびに市役所のサービスマネージャとの通信を行なう。

4 おわりに

今後の課題として、カード IC 部への演算機能の実装、標準化された電子マネーへの移行、モーバイルエージェント、分散オブジェクト技術の導入を行ない、さらなる利便性、安全性の向上を検討する。

本研究は最終的に、自治体行政、郵便、警察などの公的サービスのみならず、金融、医療、流通までを含めた総合的なサービスを提供できるプラットフォームを確立し、家庭からのサービス取得を目指すものである。

参考文献

[1] 田代, 安部, 佐野, 岡田, 松下,"光カードと IC カードを組み合わせたハイブリッドカードによる個人情報管理システム", 情報処理学会第 52 回全国大会論文集, 1996

[2] 田代, 榊原, 安部, 岡田, 松下,"ネットワークを利用した電子化証明書発行システムのための安全なプロトコルに関する提案", 情報処理学会第 50 回全国大会論文集, 1995

[3] J.Kohl,B.Neuman,"The Kerberos Network Authentication Service(V5)",1993,RFC1510