システムソフトウェアと
オペレーティング・システム 77－20
マルチメディア通信と分散処理 87－20
（1998. 2. 26）

マルチメディアサービスシステムにおける 光・ICハイブリッドカードの利用に関する考察

砂田 智　徳田 安史　岡田 謙一　松下 温

慶應義塾大学 理工学部

Abstract

現在では、インターネットに代表されるようにコンピュータネットワークが急速に発達しつつある。今後はそれに様々なサービスの電子化が加わり、ネットワーク上でのサービス提供がますます活発になると期待される。しかし、サービスの電子化・ネットワーク化には、個人情報のセキュリティ管理や、安全なネットワークシステムの構成、検討が必要不可欠である。

本稿では、次世代マルチメディアサービスシステとして期待される「光・ICハイブリッドカード」を使用した行政サービスシステムを構成し、その有用性について論ずる。

A consideration about the use of Optical-Smart Hybrid Card in the multimedia service system

Akira Sunada, Yasufumi Tokuda,
Ken-ichi Okada, Yutaka Matsushita

Dep. of Science and Technology, Keio University
3-14-1, Hiyoshi, Kouhoku-ku, Yokohama, JAPAN
E-mail: sunada@myo.inst.keio.ac.jp

A computer network which is represented in the Internet is developing rapidly at present. From now on many electronical services is added to the Internet, and it is expected that a service offered on the network will become active all the more. But, the security control of the personal information and the construction of the safe network system is indispensable.

We composed the next generation administrative service system which uses an Optical-Smart card, and introduce it's usability.

1 はじめに

インターネットに代表されるコンピュータネットワークの普及・様々なコンテンツのデジタル化が進み、ビデオ・オン・デマンドやテレビ会議等の、次世代のマルチメディアサービスが現実のものとなりつつある。

例えば、すでに駅やコンビニエンスストア等、公共の場に設置されたマルチメディアキオスク端末(MMK端末)を利用したオンラインショッピングや、インターネットアクセスのサービスが始まっている。

このような情報端末で提供されるマルチメディアサービスの一つとして、我々は、オンラインで行政サービスを提供するシステムを光・ICハイブリッドカードを利用して構築し、実験を行なった。

行政サービスが扱うデータは、例えば住民票・印鑑登録証明書・戸籍など、個人のプライバシーに深く関わるものであったり、免許証のように犯罪に深く関わるものであったりする場合が多く、万一これらのデータが悪用されれば、我々は安心して生活することすらできなくなる。

つまり公的サービスのマルチメディア化には個人情報のセキュリティ管理や、暗号技術の応用について十分な検討が必要となる。[2]。

この特に安全性を考えなければならない公的サービスを提供するシステムにおいて考察を行なうことにより、将来のマルチメディアサービスでの光・ICハイブリッドカードの可能性・セキュリティ上の課題点を明らかにしていく。最終的な目的は自治体行政、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光・ICハイブリッドカードを利用したプラットフォームの確立である。国民1人1人がそれぞれカードを所有し、様々な個人情報をその1枚のカードで個人管理するのである。

2 研究方法

インターネットは世界的に開放されたオープンネットワークであるため、セキュリティ上の安全面が危険視されている。従って、セキュリティ的な問題点・課題点は何か、いかにしてセキュリティを確保していくかを分析し、分析結果に基づいてシステムを構築することによって研究を進める。

実験を行なった行政サービスは以下の4つとした。

- 住所移転手続き(ワンストップ移転サービス)
- 住民票発行サービス
- 印鑑登録証明書サービス
- 電子回数券発行サービス

また、サービスを取得する方法は、コンビニエンスストア・郵便局などの公的な場所にインターネットに接続された情報端末を設置し、住民が最寄りの端末設置場所まで出向くものとした。

2.1 セキュリティ上の問題点

No	内容
1	証明書・申請書の偽造・改ざん検出または防止
2	証明書・申請書の複製の検出または防止
3	自治体の印鑑に相当するデータはどうするか
4	いかにして電子証明書を安全に保管するか
5	通信相手をいかにして確認(認証)するか
6	通信データをいかにして第三者から秘匿するか

表1: 行政サービスの電子化に際する問題点

現在紙ベースで処理されている上記サービスを、電子情報化してネットワークで取得することになるため、表1のような問題があげられた。

2.2 解決方法

表1の分析結果に基づき、種々のセキュリティ技術[3]を適用した解決方法をまとめると表2のようになる。

No	解決方法
1	情報作成者のディジタル署名付加
2	書類使用時に使用者のディジタル署名付加
3	自治体のディジタル署名を付加
4	光ICハイブリッドカードの使用
5	Kerberos認証チケットの応用・指紋照合
6	データの暗号化

表2: セキュリティ技術の適用

1~3については**NTT**の**E-sign**、4については**CANON**が試作した**光・IC**ハイブリッドカード、5については**Kerberos**システムを拡張した独自の認証方式、6については**NTT**の**FEAL**を使用した。

3 実装システム構成

府中・横浜各市役所様の御協力を得ることにより、インターネット上に図1に示すシステムを実装し、動作実験を行なった。

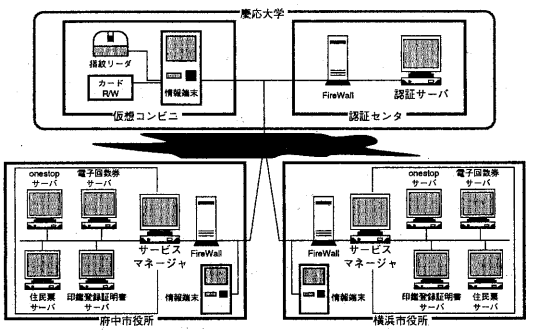

図 1: システム構成図

3.1 ワンストップ移転サービス

引越しをして住所が変わる時のことを考えると、我々は実に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。まず現在いる市町村の役所へ行き、転出手続きを行う。次に引越し先の役所へ行き、転入手続きを行う。その他郵便局、ガス・水道・電気会社、電話局にも通知を行わなくてはならない。

ワンストップ移転サービスとは、このような引越しに伴う面倒な手続きを、市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。

今回のプロジェクトでは2自治体間でのサービスに固定し、転入する市役所へ住所変更を届け出れば、自動的に転出側の自治体で転出処理を行う。処理には

- 転入手続き
- 転出手続き
- 印鑑登録移転手続き

が含まれる。

3.2 電子化証明書発行サービス

既存の紙媒体による証明書のうち、

- 住民票の写し
- 印鑑登録証明書

を電子情報化し、発行する。取得した電子証明書の利用方法には以下の2方式が考えられる。

1. 紙媒体に印刷して使用
2. 電子情報のまま使用

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。

3.3 電子回数券発行サービス

上記サービスの発行に際し、何らかの手段で課金が必要である。現在提案もしくは実験が行なわれている電子支払方式には CyberCash,MONDEX,E-Cash 等があるが、いずれも処理が複雑であり、100円単位の単純な固定額支払である行政サービスの決済方式としては適さない。そこで、回数券形式の電子決済方式を新たに考え、実験に用いる。電子回数券もまた光ICハイブリッド・カードに記録される。

4 光ICハイブリッド・カード

4.1 光ICハイブリッド・カードとは何か

光ICハイブリッド・カード (以下光ICカード) とは、現在注目を浴びている2種のカードデバイス、光カードとICカードを合体させた、新しいカードデバイスである。これらのカードは、単体では以下のような特性を持つ。

- ICカード
  CPU を内蔵し、演算可能なため暗号化・アクセス管理をカード内で行える。高いセキュリティを誇る。記憶容量が小さい (~32KByte) という欠点がある。
- 光カード
  追記型 (Write-Once) の記憶媒体で、データの消去が不可能であるためデータの改ざんには強い。また、記憶容量が非常に大きい (~6Mbyte)。ICカードのような内部演算が行えないという欠点がある。

光ICカードは、それぞれの長所を活かし、より安全かつ大容量のデバイスを実現するというコンセプトに基づいて提案された。光ICカードの概念図は図2のようになる。カード上にIC部と光部とを持っており、IC部ではデータへのアクセス管理、暗号/復号、認証処理などの演算が可能である。データはIC部・光部のいずれにも保存できるが、光部に保存されるデータはすべてIC部を経由し、暗号化された上で書き込まれる。IC部のデータは何度でも消去可能だが、一度光部に保存されたデータは Write-Once の性質により消去不可能である。

4.2 光ICカードの安全性

IC部に記録されるデータはICによって保護されるので、不正な読み出しを 100% 防ぐことができるが、光部は専用のリーダを用意することで自由にデータを読み出せてしまう。そこで、いかに光部を保護するかが問題となる。

この点は、データを一度IC部で暗号化した後、光部に書き込むことにより、解決できる。暗号/復号鍵はカード発行時にIC部に記録し、カード毎に異なる

鍵を用いる。処理の高速化のため、暗号系としてはDES[3],FEAL[3] に代表される共有鍵暗号を用いる。

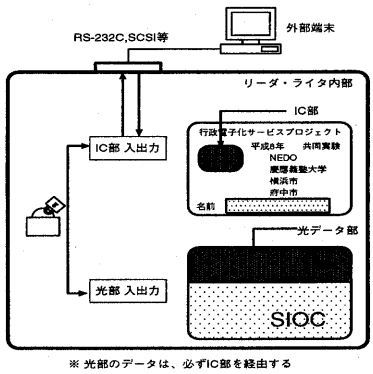

図 2: 光 IC カード概念図

5 実験システムの詳細

5.1 認証機関

住民にカードを発行し、デジタル署名 [3] 用の鍵の割り当て・管理を行なう認証機関 (Certification Authority) が存在すると仮定する。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。

ここでの認証機関は、ユーザの認証を他に代わって行なうのではなく、あくまで公開鍵証明書によってユーザの公開鍵を保証するだけである。

5.2 カード発行

今回の実験では、カードの発行方式までは考えない。あらかじめユーザは前述の認証機関からカードの発行を受けており、カード内には表 3のデータが登録済みであるとする。下記データ中、居住証明書のみは現在住んでいる市町村が発行する。

登録データ	備考
指紋情報	ユーザ認証に用いる
暗号鍵	デジタル署名作成 E-sign 秘密鍵 データ暗号化用 FEAL 鍵 認証機関の E-sign 公開鍵
公開鍵証明書	ユーザの E-sign 公開鍵を保証
居住証明書	カードの所有者の身元を保証

表 3: カード発行時の登録情報

5.3 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[4] によるデジタル署名作成と署名検証、RSA[3] 公開鍵による暗号化が可能であるとする。

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う。

5.4 認証方式

[ユーザ・カード間認証]

指紋情報を用いる。すなわち、ユーザはサービスを受けるときには、まず端末にカードを挿入し、パスワードの代わりに指紋を入力してユーザの認証を行なう。ただし、あくまでもカードとユーザを対応づけるだけであり、これで自治体へ自由にアクセスできるわけではない。

[ユーザ・自治体間認証]

デジタル署名を使用した独自の認証方式を用いる。

5.5 サーバ/クライアント構成

サーバには大きく分けて次の 2 種がある。サーバ構成は図 1に示す。いずれのサーバも、各市役所のネットワークの入口にあるファイアウォールの内側に配置し、セキュリティを高める。

- サービスマネージャ
  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ユーザの認証を行なう。ワンストップ移転サービスの場合には他の自治体との間で認証処理やデータ処理を行なう。
- 各サービス提供サーバ
  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。このように、データベースへアクセスできるサーバを限定することで不正なアクセスによる犯罪を防ぐ。

また、クライアントは 1 種類であり、慶応大学、市役所に設置された情報端末上で動作する。情報端末にはタッチパネル・指紋読み取り装置・プリンタが内蔵され、銀行の ATM に似たユーザ・インタフェイスでユーザを支援する。

- 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。

6 各サービスのワークフロー

本章では各サービスの処理手順について述べる。

6.1 全てのサービスに共通な処理

1. ユーザ ichiro が自分のカード card1 を端末に挿入する (同時にカードの IC 部に電源が入る)。
2. ユーザが端末の指紋読み取り機に指紋を入力する。
3. カード内の指紋データと読み取られたデータが比較され、ユーザ認証が行なわれる。

この時点で、ユーザ ichiro が確かにカード card1 の所有者であることが確認される。生体情報を認証に用いるので、他のユーザがカードを盗んで ichiro になりすますことはできない。

1. ユーザは受けたいサービスを情報端末の画面で選択する。

サービス選択後、それぞれのサービス固有の処理に移る。

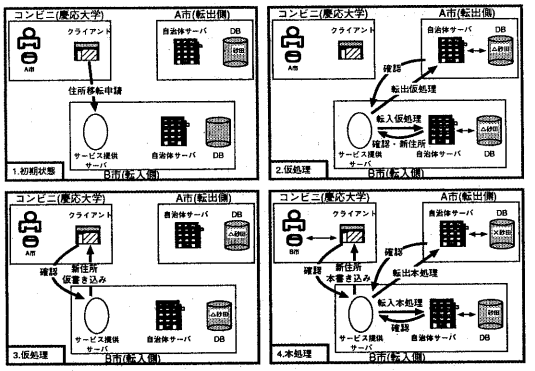

図 3: ワンストップ移転サービスのワークフロー

6.2 2 自治体間ワンストップ移転サービス

府中市から横浜市へ引っ越す場合を考える。

1. ユーザは転入先の県名 (神奈川県) と市町村名 (横浜市) を選択する (市町村データはクライアント端末内にある)。
2. さらに住所名を選択する (住所データを横浜市のサーバから自動的にダウンロードし、番地は手で入力する)。
3. クライアント端末は入力されたデータを元に住所移転申請書を作成し、カードに記録された居住証明書とともに転入先 (横浜市) の役所のサービスマネージャに送信する。転出元 (府中市) の住所はユーザの入力を必要とせず、カード内に記録されている居住証明書を用いる。送信データにはカードのデジタル署名が施される。

次に通信先の認証を行なう。

1. 横浜市のサービスマネージャはユーザのデジタル署名と居住証明書を検証し、ユーザ認証を行なう。
2. ユーザが認証されたならば、サービスマネージャは府中市のサービスマネージャとの間で相互認証を行なう。

この時点で、ユーザ・横浜市間、横浜市・府中市間の認証が完了し、安全な通信路が確定する。これ以降は住所移転手続きとなり、仮手続き・本手続きの 2 段階で処理することでデータベースの整合性を保つ。

1. 横浜市のサービスマネージャは横浜・府中各市の onestop サーバに以下の要求を出す。ただし、府中市については府中市のサービスマネージャが要求をリダイレクトする。

要求先	要求内容
横浜市	新住所に対する居住証明書の発行 住民台帳への転入仮処理
府中市	印鑑登録データの横浜市への転送 住民台帳への転出仮処理

表 4: onestop 仮処理要求

2. 次に横浜市のサービスマネージャは横浜市の onestop サーバへ印鑑登録データの仮登録要求を出し、同時にクライアント端末へ新しい居住証明書を送信する。
3. サービスマネージャは処理完了を確認する。
4. サービスマネージャは本処理を行なうため、以下の処理要求を出す。

要求先	要求内容
横浜市	印鑑登録データの本登録 住民台帳への転入本処理
府中市	印鑑登録データの無効化 住民台帳への転出本処理
クライアント	新しい居住証明書のカードへの書き込み

表 5: onestop 本処理要求

5. クライアント端末の画面にサービスが完了した旨を表示し、カードを排出して全て終了となる。

6.3 電子化証明書発行サービス

府中市から住民票を取得する場合を考える。

1. ユーザは必要な証明書の枚数を入力する。
2. カードは必要な額の電子回数券にデジタル署名を施し居住証明書と共にクライアント端末に渡す。

3. クライアント端末は証明書の申請書を作成し、電子回数券、居住証明書とともに府中市のサービスマネージャへ送信する。
4. サービスマネージャはユーザのデジタル署名と居住証明書を検証し、ユーザ認証を行なう。
5. ユーザが認証されると、サービスマネージャは電子回数券サーバと住民票サーバに次の要求を出す。

要求先	要求内容
回数券サーバ	電子回数券の有効性の確認 使用する電子回数券の無効化
住民票サーバ	住民票発行

表 6: 住民票発行時のサーバへの要求

6. 最後にサービスマネージャはクライアントに発行された証明書を送信する。

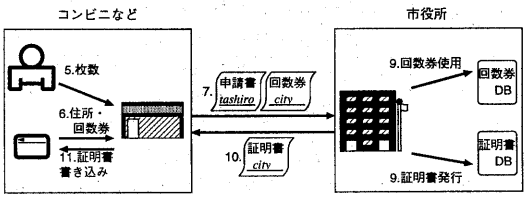

図 4: 電子化証明書発行サービスのワークフロー

6.4 電子回数券発行サービス

府中市から住民票を取得する場合を考える。

1. ユーザは必要な回数券の枚数を入力する。
2. クライアント端末は回数券の申請書を作成し、居住証明書とともに府中市のサービスマネージャへ送信する。
3. サービスマネージャはユーザのデジタル署名と居住証明書を検証し、ユーザ認証を行なう。
4. ユーザが認証されたら、サービスマネージャは電子回数券サーバに電子回数券の発行を要求する。
5. 最後にサービスマネージャはクライアントに発行された電子回数券を送信する。
6. ユーザは最後にクライアント端末が設置された場所で代金を支払う (例えばコンビニエンスストアならレジで支払えばよい)。

7 おわりに

インターネット上に行政サービスを構築するに当たり生じる問題は、各種セキュリティ技術を巧みに組み合わせることにより解決可能であることがわかった。また実際にシステムを構築し、動作実験を行なった結果、光・IC ハイブリッドカードや指紋認証への抵抗

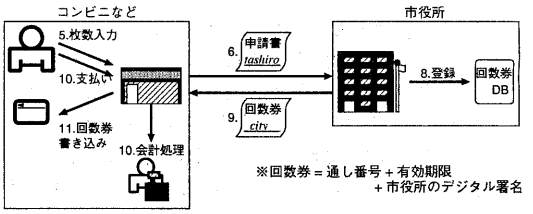

図 5: 電子回数券発行サービスのワークフロー

も少なく、次世代のネットワークサービスとしても十分実用的であると判明した。

今後、検討すべき事項には、以下の項目がある。

- **[サービス提供者の拡張]**
  現在は 2 自治体であるが、郵便局や警察署、医療機関などにも拡張していかなくてはならない。
- **[ネットワークエージェントの使用]**
  参加機関が増加すると、現在のワンストップ移転サービスの提供方式では処理に限界がある。そこで、ネットワークを自在に移動しユーザの代理人として動作するネットワークエージェントを使用したシステムも検討する必要がある。
- **[本人以外によるカードの使用]**
  基本的に本人以外がカードを使用することは考慮されていない。カードの所有者が死亡した場合カード内の情報をどう扱うか、代理人が本人に代わってサービスを受けるにはどうすればよいのか、など検討が必要である。
- **[光 IC ハイブリッドカードの暗号機能の実装]**
  今回は動作実験は端末で行なっている。IC 部での演算能力の評価も検討しなければならない。

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] 辻井重男・笠原正雄 編著: “暗号と情報セキュリティ”, 昭光堂, 1990.

[4] 岡本龍明, 藤岡淳, 岩田雅彦, “高速ディジタル署名方式 ESIGN”, NTT R&D, Vol.40, No.5, pp.687-696, 1991.