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*

3Z－7

田代 太一　安部 紀之　佐野 由佳　岡田 謙一　松下 温†

慶應義塾大学 理工学部‡

1　はじめに

近年、ICカードや光カードといったカード型デバイスに免許証などの個人情報を記録し、管理しようとする試みがなされてきている[1]。筆者らはICカードと光カードを組合せたハイブリッド・カードを提案し、運転免許や病院のカルテ、クレジットカードなどの様々な個人情報を統合的に管理するためのシステムを試作し、これを実装した。

試作システムはコンビニエンスストアなどに情報端末を設置し、そこからインターネット経由でこれらの個人情報を取得・提出することを想定しており、クレジットによる電子決済を実装している。

2　光ICハイブリッド・カード

近年におけるカード技術の発展はめざましく、さまざまなカードデバイスが開発されている。その中でもICカード及び光カードには以下に示すような特徴がある。

- ICカード
  CPUを内蔵し、カード内で演算が可能であるため暗号化・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(~32KBytc)という欠点がある。
- 光カード
  追記型の記憶媒体で、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(~6Mbytc)。ICカードのような内部演算が行えないため、セキュリティ強度はやや弱い。

これらの特徴のため、現在提案されているカード利用サービスでは以下のような問題があった。

- ICカードによるサービスでは、容量不足のために1枚につき1つのサービスに限られている。また、正当な利用者であることを確認する「本人認証」[3]に、英数字によるパスワードのみしか使用できなかった。
- 光カードによるサービスでは、内部演算が行えないため、アクセス管理や本人認証をデバイスドライバやリーダライタ内のアプリケーションに頼らなくてはならなかった。

本研究で提案する光ICハイブリッド・カード(以下光ICカード)は、これら2つのカードを組み合わせることにより、互いの長所を活かした一枚のカードを構成する。この概念図を図1に示す。

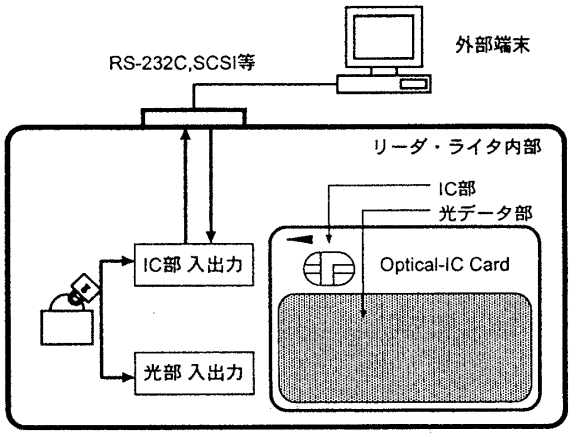

図 1: 光ICハイブリッド・カード概念図

光ICカードはその上にICチップ部と光データ部とを持つ。光データ部に記録されるデータは全てIC部によって暗号化される。IC部–光データ部間のデータ転送はリーダ・ライタ内の回路を経由して行われ、外部を経由することは決してない。この為、光ICカードは大容量かつセキュリティ強度の高いカードを実現できる。

3　光ICカード内のデータ管理

前述のように、光ICカードは内部にCPUを持ち、強力かつ柔軟なアクセス管理機能を提供できる。本研究では、カード内に行政・金融・医療・その他の4つのディレクトリを作り、さらにその下にサービス毎のサブディレクトリを構成した。また、IC部に搭載するアクセス管理プログラムの機能を以下のように定めた。

- データ毎にアクセス権を設定し、サービスIDによってアクセス管理を行う。
- 記録されるすべてのデータを暗号化/復号化する。暗号/復号に用いる鍵はカード発行時にIC部に記録し、カード毎に異なった鍵を使用。

---

*Personal Information Management System using Optical-Smart Hybrid card

†Taichi Tashiro, Noriyuki Abe, Yuka Sano, Ken-ichi Okada, Yutaka Matsushita

‡Faculty of Science and Technology, Keio University

- 外部端末との間で相互認証を行う。
- 外部端末との間でやりとりされるデータを暗号化/復号化する。
- 本人認証を行う。
- アクセスの履歴を記録する。

4 各種サービスへの適用

本章では光ICカードを種々のサービスに適用した場合について述べていく。

本人認証

本人認証はカードの利用者が正当なカードの所有者かどうかを確認することであり、全てのサービスの基本となる。

本人認証には、暗証番号やパスワード等の本人しか知らない秘密情報を使用する方法と、指紋・声紋等の生体情報を使用する方法とがある。後者の方がセキュリティ上安全であるが、多くの記憶容量を必要とする為、従来のICカードでは前者の方法がとられてきた。

しかし、光ICカードは大容量である為、あらゆる生体情報を記録して本人認証に利用できる。しかも光データ部にデータを書き込むことでデータの改ざんを完全に防ぐことができる。

カルテ

光カードに医療情報を記録・管理するシステムは伊勢原市等で試験的に導入されているが、光ICカードを利用することで光カードにはないメリットがいくつか得られる。

一つは、カードに書かれるカルテのデータをIC部によって暗号化し、アクセスを制限することでデータ漏洩を完全に防ぐことができる点である。

もう一つは、IC部のアクセス管理機能を利用することで、緊急時には医療機関が読み出せるように出来る点である。こうすることで、カードを持ち歩いてさえいれば、交通事故の発生時等に対する医療の対応を迅速に行える。

免許証

免許証は1999年までにICカード化されることが検討されているが、光ICカードを利用することにより、以下のように免許証の更新をオンラインで行える。

1. 光ICカードには先に述べたように医療情報を記録することができるので、あらかじめ近くの眼科や健康管理センタ等で視力検査を受け、結果をカード内に記録しておく。
2. コンビニエンスストア等に設置された専用の端末で旧免許証と視力検査結果のデータをネットワーク経由で警察署に送信する。
3. 警察署から新しい免許証を送信してもらい、カードに記録する。

証明書・チケット・クレジット

これらは電子情報としてネットワーク上でやりとりできるので[2]、コンビニエンス・ストアなどに設置した端末から光ICカードを利用するサービスが考えられる。

5 試作システムの実装

試作システムはSun Sparc Station + Sun OS 4.1の開発環境で実装を行った。2章で提案した光ICハイブリッド・カードならびにそのリーダ・ライタはまだ製品が存在していないため、従来の光カードとICカードを併用し、一台のWSとあわせて仮想的に図1の環境を構成した。IC部に搭載される予定のアクセス管理プログラムはWS上で動作させた。

利用サービスは

- 免許証の更新
- 証明書の発行
- 航空チケットの発行
- クレジットカードの発行

に限定し、各サービス提供者のサーバをLAN上の他のWSに置いた。また、本人認証として音声情報とパスワードを併用した方法を用いた。

暗号方式としては、DES,RSA[3],E-sign[4]を併用した。

6 おわりに

今後は府中市役所や横浜市役所と提携し、実際に光ICカードを用いて証明書の発行システムをインターネット上に構築する予定である。カード媒体及び専用リーダライタもキヤノン製のものが開発中である。

今後の課題としては、IC部に搭載するアクセス管理プログラムの高速化・軽量化、安全性に対する考察等が挙げられる。

参考文献

[1] “平成4年度 電子メディアに関する調査研究 “ICカード等多目的利用に関する調査研究 報告書” ” 1993年3月 財団法人 ニューメディア開発協会

[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.