# 被保険者証のICカード化実証実験におけるセキュリティ考察

## Security Considerations of Demonstrative Experiment of Insurance Policy using IC Card

高 島 巳 佳

**要 約** 現代では，カードを利用した仕組みにより様々なサービスが実現されている．日常生活に定着したサービスは利用者も多いが，偽造カードによる被害の増加，個人情報保護意識の高まりから，カードのセキュリティ機能についても注目されるようになった．我々がカードを利用した仕組みをビジネスとして企画する場合，カード内の情報を保護するためのセキュリティ対策が必須となる．そして，適切な対策を実施するためには，ケースごとに情報の価値，運用負担などを考慮した総合的視点での検討が必要となる．本稿では，個人情報のカード化ビジネスにおけるセキュリティ対策の検討について，「健康保険証カード化実証実験」の事例紹介を通して述べる．

**Abstract** In the present age, the structure using a card has realized various services. The service fixed to everyday life also has many users. However, it came to be observed also about the security function of the card from the increase in the damage caused by a counterfeit card, and the rise of consciousness about the personal information protection. When we plan the structure using a card as business, the security countermeasures for protecting the information recorded in a card become indispensable. And in order to implement a suitable measure, the examination with the synthetic viewpoint which took the information value, operational burdens, and etc. into consideration for every case is needed. This paper describes the examination of the security countermeasures in the card business handling personal information, introducing a case study of “demonstrative experiment of health insurance card embedded on IC card.”

## 1. はじめに

我々が通常持ち歩いているカードの平均枚数は，9.6枚という調査結果が発表されている，(インフォシーク「第10回携帯電話コンテンツ/サービス利用者調査」)．カードの種類としては，店舗が発行するポイントカード，キャッシュカードなどが多く，カードの利用が日常生活の中に定着していることがわかる．カードを利用したサービスが広くに受け入れられた理由の一つとして，カードの携帯性という特徴が挙げられるが，その反面，カードは盗難や紛失の可能性が高いという短所もある．個人情報保護法の施行に伴い，特に個人情報について敏感に意識する人が多い中，個人情報を取扱うカード化ビジネスを企画する場合には，適切なセキュリティ対策が必須となる．セキュリティ対策とは予想される脅威に対する対策であることから，予想範囲の拡大に伴って必要な対策も増加する．そのため，始めに脅威として予想する範囲，セキュリティ対策に期待する効果を明確に前提事項として定義することが必要となる．前提事項に従い，ビジネスとして収益が期待できる手段で，且つ，運用可能な手段を選定することは，カードビジネスの企画において必須の工程であろう．最近，注目されているICカード[*1]においても，現状ではカード発行コストの負担，リーダライタ装置の整備などの課題解決方法を探らなくてはならない．本稿では，個人情報のカード化ビジネスにおいて，どのようなセキュリテ

ィ対策を実施するかというテーマについて，筆者が参加した「健康保険証カード化実証実験(以下　実証実験)」の事例紹介を通して述べる．

## 2. 「健康保険証カード化実証実験」の概要

まず始めに，実証実験の概要を紹介する．本実証実験は，健康保険証（以下　保険証）を一人一枚のカードで交付し，そこに記載される情報をシステム的に利用する実証実験である．システムの目的は，健康保険組合全体において年間 140 万件を超え，健康保険組合，医療機関にとって大きなコスト負担，運用負担となっている資格過誤*2 件数の削減である[2]．資格過誤の原因は，受診時の保険証確認ミス（資格喪失後受診・旧証・該当者なしなど）によるもの，医療機関におけるレセプト*3 やカルテへの資格情報転記ミス（事務作業ミス）に起因している．

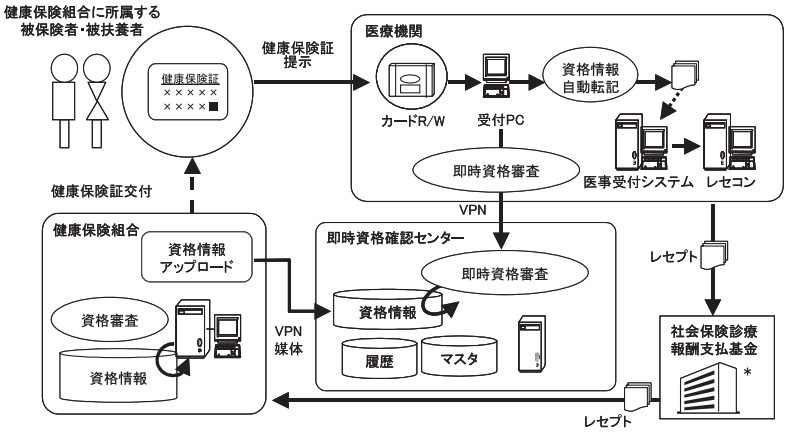
この原因解決のため，システムでは以下二つの機能を実現する．

1)　オンラインで保険資格審査を実施する「即時資格審査機能」

2)　医療機関でのレセプト作成時に保険証から情報を取込む「資格情報自動転記機能」

本実証実験プロジェクトは，2003 年 11 月，日本ユニシスを中心とし，健康保険組合，カード発行業者，クレジットカード会社というメンバにより発足した．

図 1 に実証実験のシステム概要図を示す．




＊　社会保険診療報酬支払基金：医療費の審査と支払を行う公法人

**図 1　実証実験のシステム概要図**

## 3. 個人情報のカード化ビジネスにおける検討課題

### 3.1 個人情報の取扱い基本方針の策定

個人情報を取扱うにあたり，早い段階でセキュリティ基本方針を策定する必要がある．個人情報保護の目的の他に，プロジェクト関係者内で個人情報の取扱いにおけるセキュリティ意識を統一するという目的もあるからである．そして，策定した基本方針を遵守する前提で，各セキュリティ対策について検討を開始することが望ましい．実証実験で策定した個人情報取扱い基本方針を表 1 に示す．内容は，個人情報保護法，および，その他の規範*4，各事業者のセキュリティポリシーに準じている．

表 1　個人情報取扱い基本方針

| 原則項目 | 内　　容 |
|---|---|
| 目的外利用，<br>および収集の制限 | 利用目的を本人に明示し，本人の了解を得た上で，個人情報を取得する． |
| 正確性の確保 | 保有する個人情報は利用目的に応じ，業務上必要な範囲において，正確かつ最新の状態で管理する．なお，個人情報の保有期間については原則として，業務上必要な期間とする． |
| 安全性の確保 | 情報セキュリティ対策をはじめとする安全対策を実施し，個人情報への不正アクセスならびに個人情報の紛失，破壊，改ざん，漏えいなどの予防に努める． |
| | 個人情報を保管・管理する場所を特定し，格納・管理するなど必要な措置を行う．また，業務関係者以外が容易に侵入できない措置（入退管理など）を必要に応じて行う． |
| | 個人情報を閲覧，または，利用できる者を，制御できる措置（個人情報の処理システムの利用を許可・制限するアクセス権限管理など）を必要に応じて行う． |
| | 個人情報への不当，不正なアクセス，個人情報の紛失・改ざん・破壊・漏えいに対して技術的対応策として，外部からの接続を遮断する措置，データの改ざん防止（伝送データを含めた暗号化）措置，監査証跡（アクセス／プログラム実行ログなど）の確保および定期的なモニタリング，データのバックアップなどの措置を必要に応じて行う． |
| 透明性の確保 | 個人情報に関する被保険者・被扶養者の権利を尊重し，自己情報の開示，訂正，削除には適正に対応する．また，利用もしくは提供の拒否を求められたときは，諸規定と照合し，適切に対応する． |
| 個人情報の預託 | 個人情報の情報処理あるいは廃棄などを委託するなどのために，個人情報を外部業者に預託する場合には，その安全性の確保について，十分な個人情報の管理体制および保護水準を満たしている者を選定する基準を確立し，これを満たす業者を選定するものとする． |

### 3.2　カード種類の選定

個人情報を格納するカード種類の選定は，個人情報のカード化ビジネスにおける最大のテーマとなる．カード利用目的，格納する情報の価値，カード発行コスト，運用負担などについて各ケースごとに適切なカードを選定しなくてはならない．しかし，全ての条件で最適なカードを選定できるとは限らず，格納する情報の価値，運用負担の観点から最適なカードであっても，カード発行コストが高いなどの問題があるケースがある．その際に必要となるのが，カード利用目的についての明確な優先順位である．例えば，電車乗車券の利用においては，無人で正確に改札チェックを行い，短時間に多くの処理ができることが重要と考えられる．また，大量に発行するため，カード発行コストの低さも重要である．一方，金融機関カードにおいては，無人で正確，且つ，安全にサービスを利用できることが重要であり，処理の早さよりも，窓口と同じくらいのセキュリティを実現することが優先的となるだろう．現行カード種類として，IC カード，磁気カード，バーコード付きカードを選定候補とし，以下にそれぞれの特徴を比較する．

#### 3.2.1　IC カード

IC カードは，カード内に CPU[*5]，メモリを搭載し，情報を格納できる．読取方式により，「接触型」，「非接触型」に大きく分類される．さらに，CPU 搭載の有無，通信距離により，図 2 のように細かく分類される．

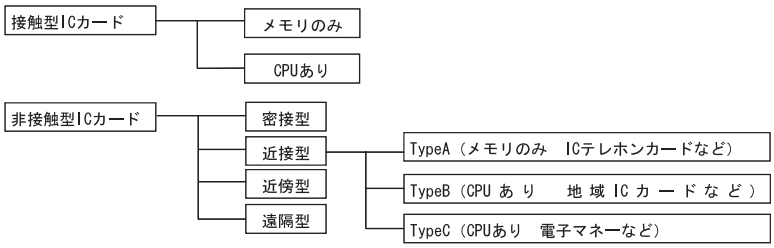



**図 2　IC カードの分類**

1)　接触型 IC カード

端子がカード表面にむきだしになっており，リーダライタ装置に差込むことで，電力の供給を受けてデータを交換する．メモリのみ，メモリと CPU を搭載するタイプに区別される．カード発行コストは，種類により異なるが，400 円～500 円程度と，他技術を利用したカードより高い．

2)　非接触型 IC カード

埋め込まれた IC チップ上のアンテナが，リーダライタ装置から発せられる電波を受信し，エネルギーに変換してデータの交換を行う．端子がカード内部に埋め込まれているため，汚れや摩擦などの悪影響にも強い．カードとリーダライタ装置の通信距離に応じて，密着型（数 mm 以内），近接型（10 cm 以内），近傍型（70 cm 以内），遠隔型（70 cm 以上）の 4 種類がある．そのうち，実用化が進んでいるのは近接型で，近接型には TypeA, B,C の 3 種類ある．カード発行コストは，種類により異なるが，TypeA が 200 円程度，他の TypeB, C は 700 円～1000 円であり，CPU 搭載の非接触型カードはコストが最も高いことになる．IC カードは偽造や，データの読み出し・改ざんが困難であり，セキュリティの安全性が高いと言われている．その理由は，IC カードのセキュリティ機能として暗号化，アクセス制御，耐タンパー性，認証といった四つの機能を備えているためである．これらの機能は IC カードが CPU を搭載することで実現できた機能であり，特徴を表 2 に示す．

**表 2　IC カードのセキュリティ機能**

| 機　能 | 特　　徴 |
|---|---|
| 暗号化 | ・CPU により，IC カード内で暗号演算が可能<br>・カード内データ，端末間の通信データの両方を暗号化可能<br>・カード内に暗号化の鍵をもつ．<br>現在流通しているほぼ全ての IC カードに共通鍵暗号（DES，FEAL*など）が搭載され，さらに高機能タイプの IC カードでは，公開鍵暗号（RSA**など）も搭載されている． |
| アクセス制御 | 正当なアクセス権限がない限り，データの読出し・解読，偽造は不可能． |
| 耐タンパー性 | 外部からの不当アクセスに抵抗する機能．<br>（チップ回路が破壊するなど） |
| 認　証 | ・本人認証　：アクセスしている人間が本当のカード所有者か確認<br>・相互認証　：IC カードとリーダライタの正当性をお互いに確認<br>・ロック機能：認証回数に制限あり<br>・IC カードとリーダライタ間のオフラインで認証可能<br>（オンラインで暗証番号を盗まれる危険性がない） |

＊　FEAL：Fast data Encipherment Algorithm の略
　　NTT が開発した暗号方式．FEAL は暗号化と復号化に同じ鍵を用いる秘密鍵型の暗号方式

＊＊　RSA：Rivest Shamir Adleman の略
　　対になる二つの鍵を使ってデータの暗号化・復号化を行なう公開鍵暗号方式の一つ

また，IC チップの構造は，図 3 のようになっている[1]．

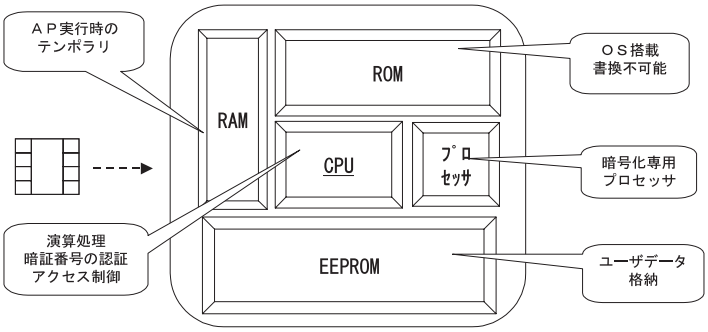



**図 3　IC チップの構造**

CPU が暗号化，認証，アクセス制御を可能にしている．ROM には OS，権限の情報などを格納するが，書換えできない仕組みとなっている．書換え可能なユーザのデータは EEPROM に格納している．このように IC カードは複数のセキュリティ対策をもち，複雑な構造となっているため，IC カードの回路を解析し，データを解読するには，高価な設備と高い技術が必要となり，偽造防止につながる．

### 3.2.2　磁気カード

磁気カードは，カード内に黒い帯状の磁気ストライプがあり，＋と－によって情報を表現する．情報量は，約 72 Bytes である．偽造，データの盗聴，解析が容易であるため，セキュリティ面での安全性は低い．

### 3.2.3　バーコード搭載カード

バーコードは，バー（黒い線）とスペース（白または印字していない部分）の縞模様パターン（バーコードシンボル）に，数字やその他の文字・記号を置き換え，機械で光学的に解読可能な形で情報を表現する．バーコードシンボルにより差があるが，読取率が 100% ではないこと，印字面積の確保などの考慮が必要である．バーコードシンボルの配置方法により，「1 次元バーコード」，「2 次元バーコード」に大きく分類される．情報量は，1 次元バーコードで約 20 Bytes,2 次元バーコードは約 1 kbyte である．カード発行コストは安いが，2 次元バーコードのリーダライタ装置は 15 万円程度と高額である．偽造，データの盗聴，解析が容易であるため，セキュリティ面での安全性は比較的低い．

1）　1 次元バーコード

バーコードシンボルキャラクタを直線的に並べ，幅の違いで情報化を行う．一般的によく使われているのは JAN,CODE 39,ITF．バーコードの誤読率は ITF がもっとも高く，CODE 39 が最も低い．

2）　2 次元バーコード

シンボルキャラクタまたはそれに相当する情報単位を縦横に配置して情報化を行う．バーコードに比べ，10 倍から 100 倍の情報量と情報化密度をもち，360 度どの方向からでも読取可能．バーコードを積み重ねたような形の「スタック型」，碁盤の上に石を並べたよ

うな形の「マトリックス型」に分類される．アメリカを中心に世界的に最も普及しているのは PDF 417，日本で最も普及しているのは，QR コードである．

### 3.2.4　各カードの比較

カード種類選定の検討資料として，表 3 に IC カードの比較，表 4 に磁気カードとバーコードの比較を示す．

**表 3　IC カード比較表**

| | IC カード（接触型） | IC カード（非接触型） | | |
|---|---|---|---|---|
| インタフェース | リーダライタとの接触による通信と電源供給 | リーダライタの電波による非接触な通信と電源供給 | | |
| 情報量 | ～32K | | | ～4K |
| 保存内容 | データのみ，または，データとプログラム | Type A | Type B | Type C |
| | | データのみ | データと<br>プログラム | データと<br>プログラム |
| リライト | 可能 | | | |
| セキュリティ | 耐タンパー性*，認証機能（個人認証，相互認証），データの暗号化により，データの盗聴，解析は困難<br>CPU 搭載の場合，CPU 通信の制限，接点による通信により，データの盗聴，解析はさらに困難 | | | |
| 偽造対策 | 特殊な IC チップのため，解析，複製は困難 | | | |
| 通信距離 | 接触 | 10cm 以内 | | |
| 機器メンテナンス | 定期的に接触部分の清掃が必要 | メンテナンス不要 | | |
| 耐久性 | 磁気：強い<br>衝撃：やや弱い<br>曲げ：やや弱い<br>磨耗：やや弱い<br>汚れ，湿気：弱い<br>静電気：弱い | 磁気：強い<br>衝撃：やや弱い<br>曲げ：やや弱い<br>磨耗：強い<br>汚れ，湿気：強い<br>静電気：強い | | |
| カード 1 枚のコスト | 400～500 円 | 200 円 | 700～1000 円 | 700～1000 円 |
| リーダライタ装置コスト | 5，000 円～ | 20，000 円～ | 20，000 円～ | 20，000 円～ |
| 用途例 | 金融機関カード，クレジットカード | テレホンカード | 住基カード | Suica**，edy*** |

＊　耐タンパー性：内部構造や記憶データなどの解析が困難な性質
＊＊　Suica ： Super Urban Intelligent Card の略
　　JR 東日本などが首都圏で導入している，定期券・プリペイドカード機能を持つ非接触式 IC カード
＊＊＊　edy：ソニーが発行している電子マネー
　　ソニーが開発した非接触 IC カード技術である「FeliCa」を利用したプリペイド型電子マネー

以上のように，各カード種類の特徴などを比較し，各ケースに適切なカードを選定する．実証実験では，検討の結果，非接触 IC カード TypeB を使用することとなった．カードに格納する情報は，保険証に記載される個人情報であるため，高いセキュリティが必要である．そのため，カード発行コストが高いことよりも，セキュリティの高さを優先した．また，非接触 IC カード TypeB は，公共事業で利用されていることから，マルチアプリケーションの可能性や，リーダライタ装置の普及が期待できることから，将来性があると判断した．

**表 4　磁気カード，バーコードを利用したカード比較表**

| | 磁気カード | バーコード | |
|---|---|---|---|
| インタフェース | リーダライタと磁気ヘッドの接触 | バーコードリーダの光センサにより検知<br>（予め決められたキャラクタのバーパターンと比較照合することによってキャラクタに変換） | |
| 情報量 | ～72Bytes | 1次元バーコード<br>～20Bytes | 2次元バーコード<br>～1K |
| 保存内容 | データのみ | データのみ（数字，記号，アルファベット（種類により扱える文字が異なる） | データのみ（数字，記号，アルファベット，仮名，漢字，図形，バイナリーコード） |
| リライト | 可能 | 不可 | |
| セキュリティ | データの盗聴，解析が容易 | データの盗聴，解析が容易 | データの盗聴が容易．データの暗号化ができるため，データの解析は困難 |
| 偽造対策 | 偽造が容易．（データの解読，コピーが容易）<br>対策は，ホログラムなど券面オプション加工に頼るのみ | 偽造が容易．（データの解読，コピーが容易） | |
| 通信距離 | 接触 | 数 mm～10cm 以内（バーコードリーダにより異なる） | |
| 機器メンテナンス | 定期的に磁気ヘッドの清掃が必要 | メンテナンス不要 | |
| 耐久性 | 磁気：弱い<br>衝撃：強い<br>曲げ：強い<br>磨耗：やや弱い<br>汚れ，湿気：やや弱い<br>静電気：強い | 磁気：強い<br>衝撃：強い<br>曲げ：強い<br>磨耗：やや弱い<br>汚れ，湿気：やや弱い<br>静電気：強い<br>（端から端まで光があたる部分があれば読取可能） | 磁気：強い<br>衝撃：強い<br>曲げ：強い<br>磨耗：やや弱い<br>汚れ，湿気：弱い<br>静電気：強い |
| カード 1 枚のコスト | 100 円 | 20 円 | |
| リーダライタ装置コスト | 146，000 円 ～ | 1次元 ： 30，000 円～<br>2次元 ： 150，000 円～ | |
| 用途例 | 乗車券，テレホンカード，切符 | 在庫管理，出荷検品 | |

### 3.3　本人認証について

カード利用時のセキュリティ対策として，本人認証という手段がある．本人認証とは，個人の識別を行って，事前に登録されている本人であることを確認し，第三者による不正使用を防止するための対策である．代表的な手段として，免許証など「所有物」を利用するもの，本人の「写真」を利用するもの，磁気カード，IC カードなどで暗証番号（パスワード）などの「秘密情報」を利用するもの，指紋や声紋[*6]，網膜パターン[*7] などの「身体的特徴（バイオメトリクス[*8]）」を利用するものなどがある．カード種類の選定と同様に，カード利用目的，格納する情報の価値，カード発行コスト，運用負担の観点から，必要に応じて，適切な本人認証の手段を選定する必要がある．主な本人認証の技術と，それぞれのメリット，デメリットの比較を表 5 本人認証技術比較表に示す．

**表5　本人認証技術比較表**

| 方　式 | 主な技術 | 長　所 | 短　所 |
|---|---|---|---|
| 所有物 | ICカード<br>（パスワードなし） | ・利便性が高い<br>・導入コストが安い<br>・経年変動がない | ・誰にでも読まれる<br>・盗まれる可能性がある |
| 写真 | 顔写真 | ・利便性が高い<br>・導入コストが安い | ・経年変動する<br>・認証する側の判断能力に左右される |
| 秘密情報<br>＋所有物 | パスワード<br>＋ICカード | ・経年変動がない | ・パスワードを忘れる可能性がある |
| バイオメトリクス | 指紋 | ・経年変動がない<br>・偽造に対する耐久性が高い | ・厳格なプライバシー保護が必要<br>・導入コストが高い |
| | 声紋 | ・暗闇でも使用できる<br>・偽造に対する耐久性が高い | ・経年変動することがある（体調など）<br>・騒音のある場所では使えない<br>・導入コストが高い |
| | 網膜パターン | ・経年変動がない<br>・偽造に対する耐久性が高い | ・導入コストが高い |

本人認証の手段として写真を利用した場合，特に成長期の子供などは成長が早いため，写真の更新に伴う再発行が頻繁に必要となってしまう．また，パスワードを利用した場合は，パスワードの忘失により，運用が複雑化する可能性がある．バイオメトリクスについては，指紋，網膜パターンを利用した場合，上記二つの問題は回避できるが，認証専用端末の価格が高いことから現時点では普及が困難と考える．どの本人認証を実施した場合でも，現状よりもコスト負担や運用負担の増加，利便性の低下は発生してしまうため，優先事項を決めて適切な手段を選定することが必要となる．実証実験では，医療機関受付という多忙な状況での利用が前提であったため，大きな運用負担，コスト負担は避けなくてはならず，パスワード入力による本人認証を有力手段として検討した．しかし，医療機関受付で利用者の待ち時間が長くなること，医療機関の利用者には高齢者も多く，パスワード忘失の可能性が高いと思われる点が懸念され，実施が難しいという現場関係者の意見があったため，実証実験中は本人認証を実施せず，実証実験終了後にアンケートなどを実施し，本人認証の技術動向も踏まえて解決策を継続検討することとした．

### 3.4　その他のセキュリティ対策

これまで，カード種類と本人認証についてのセキュリティ対策を検討してきたが，カードから読み出したデータが流れるネットワークについてもセキュリティ対策を検討する必要がある．実証実験では，医療機関と即時資格確認センター間の接続，健康保険組合と即時資格確認センター間の接続，健康保険組合とカード発行業者間の接続について，SSLとVPNを候補として検討した．SSLとは，米Netscape社が提唱したプロトコルで，データの暗号化と認証を行うことによって，第三者によるデータの盗用や改ざんを防ぐものである．一方，VPNとは，通信相手との間の仮想的なトンネル上で通信し，暗号化したデータを送受信することにより，データの盗聴や改ざんなどの不正アクセスを防ぐものである．現在のVPN装置は，トンネリングのほかに，暗号化機能，認証機能，ファイアーウォール機能などさまざまな機能を備えているものが多く，VPNの構築により，SSL機能が実現できる．実証実験ではSSL機能を満た

すVPNを構築することとなった.

### 3.5 保険者とカード発行業者間のセキュリティ対策

セキュリティ上，外部とのネットワーク接続ができないケースもある．その場合，媒体でのデータ送付を検討することとなるが，データの改ざん，送付主のなりすましを防御するための対策を検討する必要がある.データを暗号化することによりデータの改ざんを防ぐことに加え，CA局を設立し，証明書を発行することにより，送付主のなりすましを防ぐことができる．実証実験では，保険者とカード発行業者間の接続において，保険者によっては外部との接続ができない場合があるため，格納データの暗号化，CA局による証明書発行を実施することとした．図4に実証実験での媒体データの送付方法を示す.

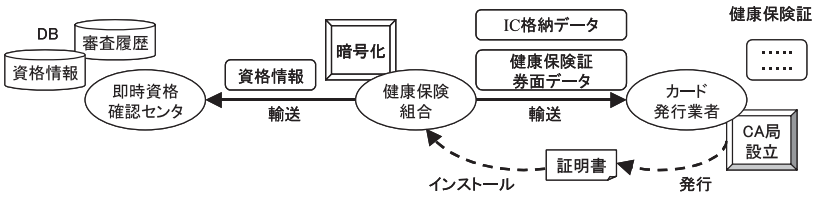



**図4 媒体でのデータ送付方法**

保険者からデータをカード発行業者に送付する場合，カード発行業者にCA局を設立し，公開鍵，証明書を発行する．保険者側では，カード発行業者で発行した証明書をインストールし，公開鍵でデータを暗号化する．暗号化されたデータをカード発行業者に輸送し，カード発行業者側で秘密鍵を使って資格情報を複合化する流れとなる．しかし，CA局の設立，証明書の発行，鍵管理が必要となり，コスト負担，運用負担ともに大きい．また，郵送による送付では媒体の紛失など，セキュリティ対策として脆弱性が高いため，可能な限りVPNを利用した接続を推奨した.

## 5. おわりに

本稿ではカード化ビジネスにおけるセキュリティ対策の検討事例として，実証実験における検討内容を紹介した．実証実験で採用することとなったICカードは，認証などのセキュリティツールとしての一面，また，流通・小売などで利用されるCRMツールとしての一面に期待が集まっており，ICカード市場はさらに拡大していくと予想されている．今後のICカードビジネスには，便利で確実な個人認証の実現や，ICカードシステムと既存システムや他システムとの連携，連携を見据えた統合的で標準化されたセキュリティ対策が求められるだろう．ICカードビジネスの企画は既に多数存在するが，例えば，医療保険や生命保険などの仕組みは個人ごとに加入の条件なども異なり，万一の場合に保険がどのように適用されるかを自分でシミュレーションするのは難しいというイメージがある．そこで，保険加入者にICカード型の保険証書を発行し，各保険会社システムと連携することで加入内容の確認やシミュレーションなどが自分で簡単にできるようにすることは，加入者にとって保険会社を選択する際の魅力的なサービスのひとつとなりえるため，ビジネスとして有益ではないかと考える．現状，ICカードビジネス推進の障害となっている「カード発行価格の高さ」,「リーダライタ装置の低い普及率」という課題は，ICカードの普及に伴い，プロジェクト参加機関，搭載アプリケーション，

ICカード発行枚数の増加が実現されれば解決されると期待できる．これまでICカードのセキュリティ機能に着目して述べてきたが，ICカードを利用してもセキュリティを維持するためには徹底した運用管理が不可欠であることも忘れてはならない．我々システム提供側もこれまで以上に業務に密着した視点でシステム化を企画し，継続的にセキュリティを維持していけるシステムを提供していけるよう努めたい．最後に，本稿の執筆にあたり多大なご協力を頂いた関係者の皆様に心よりお礼申し上げたい．

＊1　ICカード：キャッシュカード大のプラスチック製カードに極めて薄い半導体集積回路（ICチップ）を埋め込み，情報を記録できるようにしたカード
＊2　資格過誤：被保険者・被扶養者の保険資格を誤ること
＊3　レセプト：医療機関が保険者に医療費を請求する際の明細書
＊4　その他規範：個人情報保護に関するコンプライアンスプログラムの要求事項（日本工業規格-JISQ 15001,1993/3制定），クレジット産業における個人信用情報保護・利用に関する自主ルール（2001/3制定），健康保険組合における個人情報の保護について（2002/12/25付，保保発第1225001号）
＊5　CPU：Central Processing Unitの略
コンピュータの中で，各装置の制御やデータの計算・加工を行なう中枢部分
＊6　声紋：声の特徴をデジタルデータ化したもの
＊7　網膜パターン：目の網膜にある毛細血管の模様をデータ化したもの
＊8　バイオメトリクス：身体的特徴によって本人確認を行なう認証方式

**参考文献**　［1］　岩田　昭男，「図解よくわかるICカードビジネス」，実業之日本社，2003年，P. 34-41
［2］　社会保険診療報酬支払基金HP URL：http：//www.ssk.or.jp/

**執筆者紹介**　高　島　巳　佳（Mika Takashima）
1975年生．1998年神奈川大学法学部法律学科卒業．1998年日本ユニシス・ソフトウェア(株)入社．コールセンターシステム，CRMアプリケーションの設計開発業務に従事後，ICカードビジネスの企画に従事し，現在はクレジット・信販業務向け受付審査システム，債権管理システムの設計開発業務を担当．