IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

# IC・ID カードの相互運用可能性の向上に係る基礎調査

## ニーズ編

## 報告書

2007 年 1 月

独立行政法人 情報処理推進機構

# ― 目 次 ―

# 1. 概要

## 1.1. はじめに

一般に IC カードと言えば、「モノとしての IC カード」に焦点が当てられてきた。普及させるための様々な検討も「モノとしての IC カード」中心に検討されてきた。しかし、本報告書では、単体の「モノとしての IC カード」よりも、IC カードに格納されている認証用データと、この認証用データを扱う端末側のミドルウェアに焦点を当てている。IC カードを使った ID カード（IC・ID カード）を IT 社会における基盤に組み入れようとする動きが世界中至るところでで見られる。この時 IC・ID カードは、フロントエンドツールであり、このフロントエンドツールはバックエンドのシステムとうまく融合して行く必要がある。そのためには、IC・ID カードを扱う環境が整備される必要がある。IC・ID カードを扱う環境が整備の大きな課題のひとつに IC・ID カードとミドルウェアから構成された IC・ID カードサービスとしての相互運用可能性の確保がある。「モノとしての IC カード」に対してソフトウェア・アーキテクチャが重要なミドルウェアの実体を理解することが難しい面がある。そのため、この相互運用可能性の問題に関して、それほど認識されていない面がある。しかし、この課題の解決なくしては、IC・ID カードが IT 社会における基盤として利用され普及することは在りえない。本報告書（ニーズ編）では、IC・ID カードにおける相互運用として求められる使用方法について整理したうえで、現在の IC・ID カードの発行や検討の状況を相互運用可能性の観点から整理し、今後の技術環境整備の方向について提言する。

## 1.2. 基本的な用語

本報告書で用いる基本的な用語について下記に整理すると共に、図 1 に示す。

IC・ID カード
　IC カードを使った ID カード
カードアプリケーション
　IC カード上のアプレット、データ
ミドルウェア
　IC・ID カードを扱うための端末上のミドルウェア
IC・ID カードサービス
　IC・ID カードとミドルウェア
カードエッジ・インターフェース
　IC・ID カードとミドルウェア間の論理的なコマンドインタフェース
　APDU(アプリケーションプロトコルのデータ・ユニット)を使ってやり取りする。
データモデル
　IC カード上のファイル構造、データ構造

認証用データ

PKI の認証及び署名に利用される鍵ペア、公開鍵証明書等のデータ。IC・ID カード内ではデータモデルに格納される。

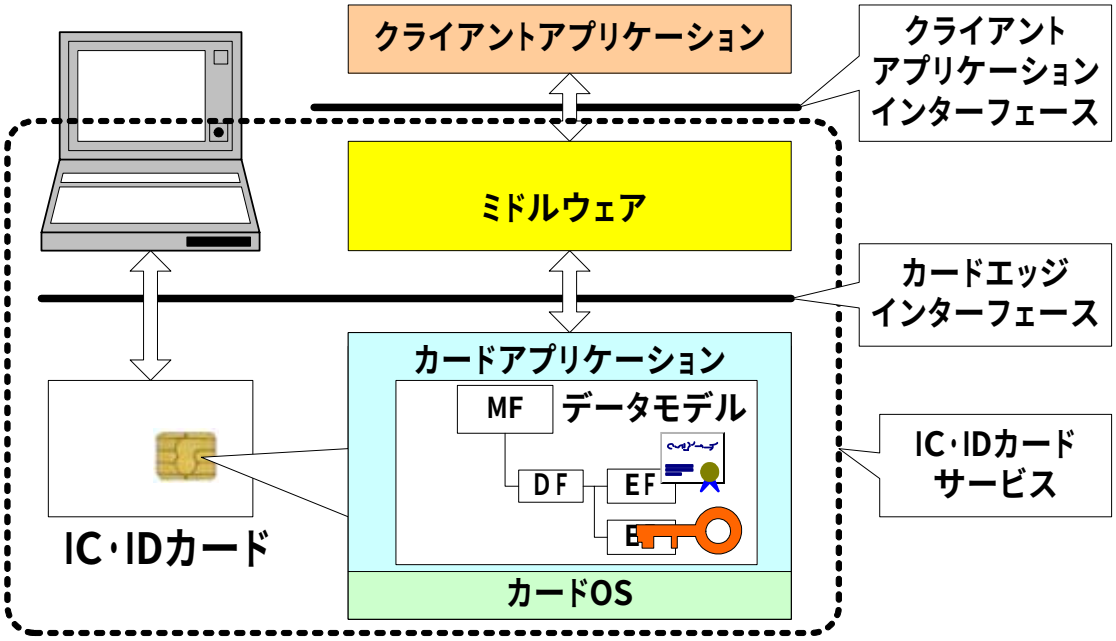



図 1　基本的な用語

## 1.3. 報告書の意図と構成

「IC・ID カードの相互運用可能性向上に係る基礎調査報告書・ニーズ編」は、以下のようなことを示すことを意図して作成されている。

(1) IC・ID カードシステムの概要（2 章）

IC・ID カードを取りまく、さまざまな関係者の役割と、それぞれに対応するシステムやカードの役割を示し、IC・ID カードが利用される環境について整理する。

IC・ID カードが利用されるクライアントにおけるデバイスやソフトウェアの構造を簡単に示す。

(2) IC・ID カードの相互運用可能性に関するニーズ（3 章）

IC・ID カードにおける相互運用可能性とは何ができることであるのかを示す。

まずは、相互運用可能性の低い現状を招いている原因となっている、IC・ID カードに係わるデバイスやソフトウェアの提供の動向について示す。

そのうえで、本調査において相互運用可能性に着目する理由、すなわち、今後 IC・ID カードの相互運用可能性が求められると予測される状況、求められると予測する分野・領域について示す。

また、相互運用可能性を向上するために、各種の技術がどのように整備されていることが望ましいのかを示す。

(3) 標準化の動向（4 章）

IC・ID カードの相互運用可能性を確保する観点で参照すべき、国際標準の制定状況や普及動向、国内での採用動向について示す。

また、実際に導入されている IC・ID カードにおける標準化の状況について示す。

(4) 国内での IC・ID カードの導入動向（5 章）

国内での IC・ID カードの導入動向について、主に技術的な観点から整理する。

まずは、現在導入されている IC・ID カードにおいて、相互運用可能性がどの程度考慮されているか、相互運用可能性が可能な技術が導入されているか、といった観点から整理する。

その上で、相互運用可能性に関する現状や関係者の立場ごとの立場から見た、現状と課題について整理する。

(5) IC・ID カードの相互運用可能性に関する課題（6 章）

現在までに導入されている IC・ID カードシステムや、供給者が供給している IC・ID カード及び関連製品では、相互運用可能性の高い IC・ID カードシステムの調達が困難となっている。これにより、すでにデメリットが生じてきている。これらの状況について示すと共に、その背景を示す。

また、顕在化しつつある IC・ID カードの相互運用性の欠如によるデメリットが今後生じないようにするために必要になる、技術的支援について考察する。

(6) IC・ID カードの標準化及び需給に向けた提言（7 章）

IC・ID カードの普及や利用を促進するため、相互運用可能性の向上を図るための環境整備について提言する。

また、提言を実現することによって期待される効果、提言内容に係わる国内外での現状、実現にあたって検討を要する課題を整理する。

## 1.4. 調査の概要

ニーズ調査では、前項に示した意図を達成するため、各種文献や資料による調査を行うとともに、関係者に対するインタビューを実施した。

インタビューの実施と並行して、IC・ID カードの相互運用可能性に関する論点の整理を行った。整理された論点は、本報告書の構成として整理されている。

インタビューは、関係者を IC・ID カードに関する役割から分類し、それぞれに対して実施した。

### 1.4.1. 文献調査

IC・ID カードのニーズ調査にあたり、現在発行、あるいは検討されている IC・ID カードについての文献により、サービスの普及状況や技術仕様の公開状況について調査した。

調査した文献の一覧については、巻末の「参考文献リスト」を参照されたい。

### 1.4.2. 関係者へのインタビュー

ニーズ調査では、IC・ID カードに係わる様々な立場の関係者に対して、合計 13 回のインタビュー調査を行った。インタビュー先の立場と調査の観点について以下に示す。なお、インタビュー先によっては、複数の関係者の立場を兼ねていることもあり、複数の観点から調査を行うことができた。

(1) 仕様策定関係者

IC･ID カードの仕様策定に係わる関係者に対しては､以下のような観点での調査を行った。インタビュー対象者のうち、仕様策定関係者にあたるのは合計 7 者であった。

- 想定されている IC･ID カードの用途
  相互運用の可能性への配慮を含む
- 仕様を策定した範囲
- 国際標準や他の標準との整合性の確保の状況
- 仕様公開の予定有無及び理由･目的
- 仕様に準拠した IC･ID カードであることの確認方法
- 仕様に準拠した IC･ID カード関連製品の調達に利用可能なツール類の開発･公開への期待の有無

(2) 調達者

IC・ID カードを発行する目的でカードやソフトウェア・ハードウェアを調達する関係者に

対して、以下のような観点での調査を行った。インタビュー対象者のうち、調達者にあたるのは合計 4 者であった。

- IC･ID カードの調達にあたって採用した技術仕様やソフトウェア
- カード発行環境を構築した際の技術的な問題点及び解決方法
- 技術仕様が標準化／公開されないことによるデメリット
- 技術仕様の標準化／公開への期待
- 相互運用可能性が確保された IC･ID カードへの期待

(3) 利用者

IC・ID カードを利用し、認証や署名等の機能を活用したアプリケーションサービスを提供する関係者に対して、以下のような観点での調査を行った。インタビュー対象者のうち、利用者にあたるのは合計 4 者であった。

- 利用者が採用した技術仕様やソフトウェア
- 利用環境を構築した際の技術的な問題点及び解決方法
- 技術仕様が標準化／公開されないことによるデメリット
- 技術仕様の標準化／公開への期待
- 相互運用可能性が確保された IC･ID カードへの期待

(4) 供給者

調達者や利用者に対して IC・ID カードや関連するソフトウェア・ハードウェアを提供する関係者に対して、以下のような観点での調査を行った。インタビュー対象者のうち、供給者にあたるのは合計 4 者であった。

- 供給する製品が準拠する仕様とデファクトとしての統一状況
- 技術仕様が標準化／公開されないことによる課題及び解決方法
  - －市場参入機会
  - －開発期間及びコスト
  - －提供先の利用環境の制限
  - －上位ソフトウェアの開発の難易度　他
- 技術仕様の標準化／公開への期待の有無
- 技術的相互運用可能性を高めるために必要な制度や仕組みに関する意見

(5) 国際標準化関係者

IC・ID カードに係わる国際標準化における国内審議団体の関係者に対して、以下のような観点での調査を行った。インタビュー対象者のうち、国際標準化関係者にあたるのは合計 2 者であった。

- 国際標準によって想定されている IC･ID カードの用途
- 想定されている相互運用の内容
- 仕様策定の範囲
- 国内での各種事業への影響
- 国際的な普及動向
- 実装による相互運用の実現に関する問題点
- 仕様準拠に利用可能なツール類の開発･公開への期待

# 2. IC・ID カードシステムの概要

## 2.1. 認証用データを利用するサービス

(1) ネットワークを通じたサービスの進展

情報技術の進展に伴い、コンピュータとネットワークを利用することによって非対面でさまざまな取引を行うことができるようになってきた。コンピュータを利用した非対面の取引には、対面の取引にはないメリットがあるため、そのニーズはますます高まってきている。

- 取引の当事者は、コンピュータ・ネットワークを通じて取引相手との情報交換ができる任意の場所で取引を行うことができる。対面の取引のように同じ場所に集合する必要がない。
- 取引の当事者は、文書の作成・受領や内容確認を、自らの都合に合わせて任意の時刻に実施できる。対面の取引のように相互に時間を調整する必要がない。
- 取引に係るコストが削減される。同一の時刻・場所に集合するための移動に要する費用及び時間、また、文書を郵便等で送受信する場合の費用と時間、などで大きなコスト削減効果が見込まれる。

(2) PKI による利用者認証の必要性

しかし、ネットワークを通じ、非対面で取引を行う場合、下記に示すようなリスクが発生する。

- 他人に成りすまして取引を行う
- 取引を行う条件（資格など）を満たさない者が満たすと詐称して取引を行う
- 第三者が通信されている文書を入手し、秘密の暴露、あるいは通信内容の改ざんを行う
- 取引成立後、保存されている文書を改ざんする
- 上記のような危険があることから、取引成立後、自身に不利な要件があった場合には、文書が改ざんされた、あるいは第三者が成りすまして取引を行ったと、取引を否定しようとする

これらのリスクを軽減する上で、PKI(Public Key Infrastructure )が大きな役割を果たしている。すなわち、ネットワークを通じた取引において、本人確認、本人の属性（資格など）の証明、当事者間での秘密通信路の確保、文書の作成者の証明、作成後改ざんされていないことの証明、などの機能を、ネットワークを通じた取引に与えている。

このように、ネットワークを通じた取引において、PKI は非常に重要な技術として活用されている。

(3) 認証用データ

PKI 技術によるサービスを実施する場合、利用者においては認証用データの活用がなされ

る。認証用データに含まれる主要な情報は以下の 2 種である。

- 鍵ペア：非対称鍵暗号の鍵の組で、一方を利用者だけが用いるプライベート鍵、もう一方を取引相手に提示する公開鍵として用いる。サービス利用時の認証や作成文書への署名付与、暗号鍵の生成等に利用される。
- 電子証明書：利用者本人の実在やサービスを利用する資格を保持することを証明する。鍵ペアのうち公開鍵を認証局に登録し、認証局からの電子署名を付与されることで登録の証明を図る。

## 2.2. IC・ID カードの役割とメリット

(1) 認証用データの管理

認証用データを用いて取引を行ったり文書を作成すれば、それは本人によるものとみなされるため、認証用データは、各個が厳重に管理する必要がある。とりわけ、鍵ペアのうちのプライベート鍵は、第三者に内容が知られたり、第三者によって認証用情報が利用されることのないように、管理される必要がある。

認証用データの保存場所は、利用するコンピュータ（PC などのクライアント、あるいはサーバ）と、携帯デバイスとに大別される。

コンピュータ内に保存される場合、当該のコンピュータや保存されている情報を他人が利用する、他人がアクセスする状況が考えられることから、パスワード等による保護や暗号化がなされ、例えコンピュータを他人が利用している場合でも、認証用データは利用できないように管理される。

コンピュータ内で認証用データの管理する場合、PKI 技術を利用した取引は、そのコンピュータでのみ実施可能となる。取引の利用環境が固定されている場合は良いが、取引環境の自由度を求めれば、取引の当事者が任意の時刻に、任意の場所で取引を行うことができるという本来の利便性の一部が損なわれる。また、本人以外がコンピュータを利用している際には、認証用データの不正利用の防止は、コンピュータ内での認証用データを管理しているセキュリティ技術に依存してしまう。

そこで、認証用情報は保存媒体に保存して本人が携帯し、コンピュータ内には常時保持しないようにする方法も利用される。保存媒体を本人がコンピュータに接続した状態でのみ認証用データが利用可能で、それ以外の時には認証用データが利用されることがないようにするのである。これによって、取引の場所と時刻に関する自由度は高くなり、かつ、本人が取引をしていない時の第三者による不正利用の危険を大幅に軽減することができる。

認証用データが何らかの媒体によって携帯されている場合、取引の際に利用するコンピュータに認証用データが複写されることや、紛失等により第三者の手に媒体が渡った際に取引がなされてしまうような事態を防止する必要がある。したがって、認証用データを携帯するための格納媒体は、それ自体がプライベート鍵による演算処理を実行でき、また取引を行おうとする

者が本人であることを確認する機能を持つことが望ましい。

(2) IC・ID カードのメリット

上記のような条件を満たす媒体としては、IC カード、USB トークン等のハードウェアトークン、携帯電話等の端末、などがある。この中で IC カードは、券面に情報が記録でき、対面での取引の際の本人確認機能や、従来の資格証明書を兼ねることができることから、公的な用途を中心に、導入が拡大しつつある。

IC カードに認証用データの格納するメリットは下記のように整理される。

- 携帯性があり、認証用データの利用を、本人がクライアントを操作しているときだけに限定可能
- 携帯性があり複数の場所、移動先で利用可能
- 券面に情報が記録でき、対面での用途との兼用が可能

このような用途に利用される IC カードを、本調査内では、ネットワーク環境で ID カードとしての役割を果たすカード、すなわち IC・ID カードと呼ぶ。

本調査では、IC・ID カードの範囲を、以下の機能を持つものに限定して扱う。

- 鍵ペアと暗号演算機能を持ち、自ら署名の付与や PC、サーバ等との暗号による双方向の認証ができる。
- 鍵ペアの一方を認証局に登録し、公開鍵証明書を付与されてカード内に保持し、カードから提供する公開鍵や利用者情報の正当性を、認証局を通じて証明することができる。

## 2.3. IC・ID カードシステムの概要

IC・ID カードシステムの概要を図 2 に示す。

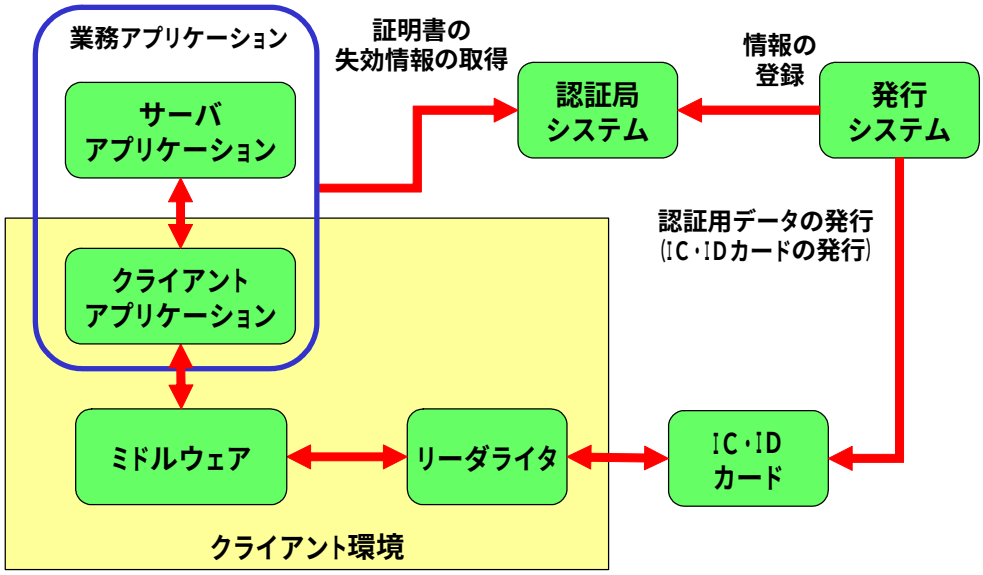



図 2　IC・ID カードシステムの概要

(1) 発行システム

IC・ID カードを発行する。発行に当たっては、認証用情報を持つ IC・ID カードを発行する機能と、IC・ID カードが証明する、カード保有者の属性を証明する機能の双方が満たされる必要がある。

(2) 認証局システム

IC・ID カードに格納されるプライベート鍵に対応する証明書を発行する。また、発行した証明書の失効情報を管理し、自らのポリシーに従って、失効情報の利用を許可する利用者に提供する。

(3) IC・ID カード

認証用データを保持し、業務アプリケーションからの要請に応じて認証、署名、暗号化等の処理を行う。なお、これらの処理は、カード保有者本人が業務アプリケーションを利用する際に限定して提供する必要があるため、IC・ID カードは、併せて PIN 等による本人確認機能を持つ。

- クライアント PC に接続したときだけ認証用データを利用可能
- カード内認証用データの扱いはパスワード等で保護
- 署名演算はカード内で実施し、外部に暗号鍵が漏れない

(4) 業務アプリケーション

IC・ID カードによって取引の正当性を確保しながら、ネットワークを通じた各種の取引を実現する。通常、業務アプリケーションの機能は、多くの場合、端末 PC 等のカード保有者が直接操作するクライアント環境に導入されているクライアントアプリケーションと、利用者が管理しているサーバ環境に導入されているサーバアプリケーションとが連動して提供される。

業務アプリケーションは、IC・ID カードの認証用データを利用して、カード保有者の認証や、署名によるカード保有者の意思の確認と保証を行う。また、この際、認証局システムを利用して認証用データの有効性を確認する。

業務アプリケーションの具体例としては、電子申告システム、ネットワーク認証システム、電子紹介状システム、電子契約システム、等がある。

(5) クライアント環境

カード保有者が IC・ID カードによって業務アプリケーションを利用する環境である。多くの場合、汎用に利用される PC 等にリーダライタの接続やミドルウェア、クライアントアプリケーションを導入して実現される。

役割としては、業務アプリケーションと IC・ID カードを接続する機能を持つ。

## 2.4. 関係者と役割

IC・ID カードに係わる関係者と役割について図 3 及び表 1 に示す。

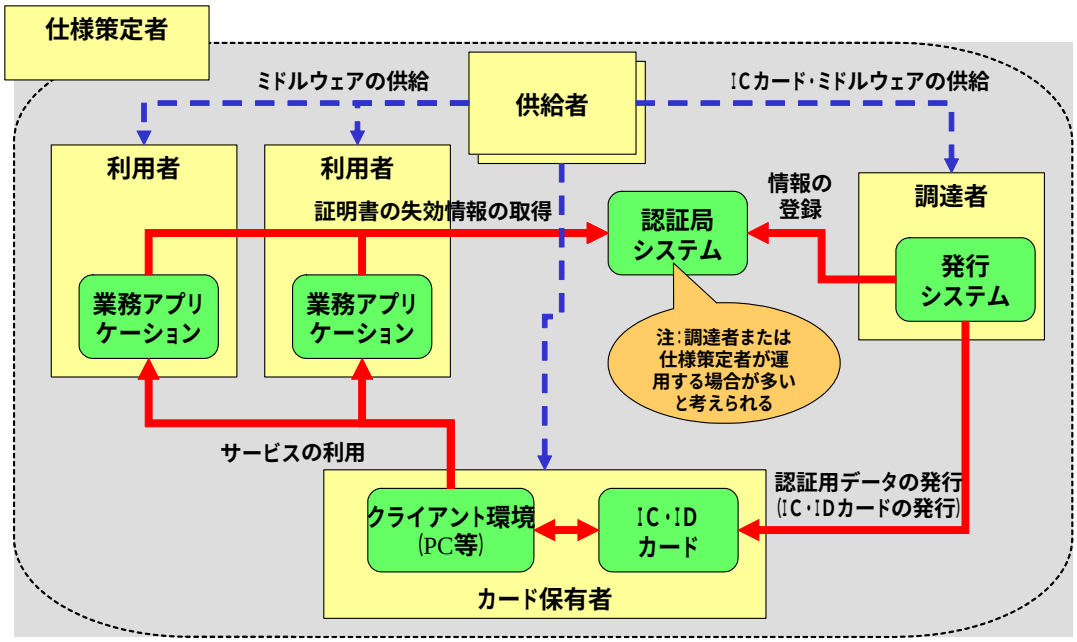



**図 3　IC・ID カードに係わる関係者の概要**

**表 1　IC・ID カードに係わる関係者と主な役割**

| 関係者 | 主な役割 |
|---|---|
| 仕様策定者 | 当該サービスにおける IC カードの仕様を策定する |
| 調達者 | 策定された仕様に沿って IC カードの調達を行い、カード保有者向けに IC カードを発行する<br>また、カード発行時に鍵ペアの発行と IC カードへの認証用データの登録を行う |
| 利用者 | 調達者が調達した IC･ID カードを持つカード保有者に対して、IC･ID カードの認証用データを利用したサービスを提供する |
| カード保有者 | IC･ID カードの発行を受け、サービスを利用する |
| 供給者 | 調達者に対して IC･ID カード、リーダライタ、クライアント上のドライバ、ミドルウェアを提供する |

それぞれの関係者の役割について、以下に示す。

(1) 仕様策定者

当該サービスにおける IC・ID カードの仕様を策定する。ただし、業務アプリケーションと IC・ID カードサービスのインタフェースのみを定めて、調達者及び供給者が提供する IC・ID カード及びミドルウェアの仕様を任意とするケースと、IC・ID カードやミドルウェアの仕様を明確に定めるケースとがある。

(2) 調達者

カード保有者の資格を証明する IC・ID カードを発行する。仕様策定者が定めた仕様に準拠した IC・ID カードを調達するが、定められている仕様の範囲が限定的な場合には、独自の仕様を追加したカードを調達する。

例えば、公的個人認証サービスにおいては、調達者は市町村であり、公的個人認証サービスの領域を持つ住民基本台帳カードを調達する際に、市町村が提供する独自のサービスを持つものとして調達することができる[1]。

(3) 利用者

調達者が発行した IC・ID カードを利用して業務アプリケーションを提供する。具体的には、電子署名付申請書の作成及び受付、クライアント認証による SSL 通信でのネットワークへの接続、委任状の署名を検証した上で代理申請の申請書を作成して署名し提出、などのサービスを提供する。

(4) カード保有者

IC・ID カードの発行を受けて、業務アプリケーションを利用する。利用者が保有するクライアント PC で IC・ID カードを利用する場合には、仕様策定者あるいは調達者の指示に従って、クライアント PC にリーダライタ及びミドルウェアを整備する必要がある。

(5) 供給者

IC・ID カード、リーダライタ、ミドルウェア、業務アプリケーション、認証局システム、等を供給する。現在までの場合、IC・ID カードと利用環境でのリーダライタ、ミドルウェアは一体での提供を行っている場合が多い。

## 2.5. IC・ID カードの実装

IC・ID カードには、PKI による機能を実現するための認証用データや機能とともに、カードとしての特性を生かした使い方をするための機能が具備される場合がある。

(1) PKI による機能

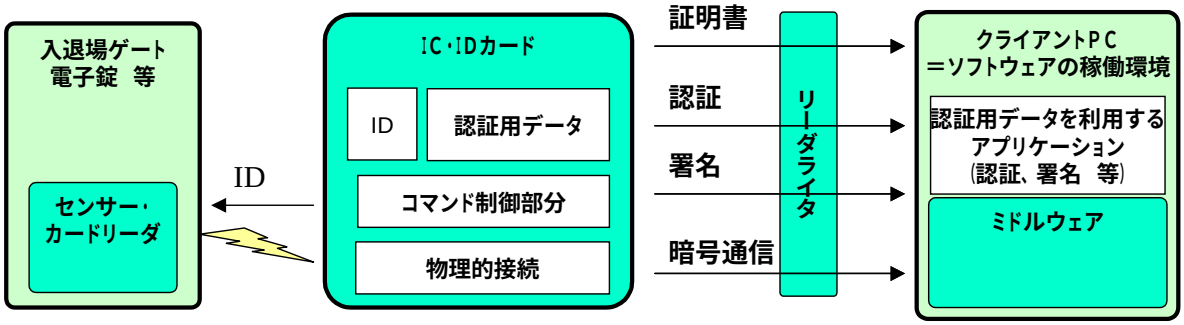
- 電子証明書の提供 （公開鍵証明、資格証明）
- 暗号による認証 （SSL のクライアント認証 他）
- 署名の付与 （文書への電子署名付与）
- 暗号通信 （セッション鍵の作成･展開 他）
- カード保有者の認証 （PKI 機能利用時に持ち主を認証：PIN のカード内照合）

(2) その他の機能

- （例） 物理的セキュリティ対応機能
  入退場ゲート、電子錠等への対応
  機能としては、ID 情報をゲート等に提供する （セキュリティカード）
  非接触カードでの実現ニーズが多い

IC・ID カードの実装例について図 4 に示す。

本報告書では、IC・ID カードに実装される機能のうち、物理的セキュリティ対応機能をはじめとした、認証用データによらないサービスのための機能は調査の対象としていない。




注：IDと認証用データでは、コマンド制御や物理的接続を個別に実装するIC・IDカードもある

図 4　IC・ID カードの実装例

## 2.6. IC・ID カードの機能

### 2.6.1. IC・ID カードサービスの位置付け

PKI を利用することによって安全性を高めたオンラインでのサービスにおいて、業務アプリケーションは、利用者の認証用データを扱ってサービスを実現する。この際、認証用データの機能と業務アプリケーションの機能は、厳密に分離され、業務アプリケーションが、認証用

データが持つべき機能の一部を持つことはないように構築される必要がある。

一方、クライアントアプリケーションから IC・ID カードを利用するため、業務アプリケーションの下位に各種ソフトウェア（ミドルウェア）を整備する必要が生じる。ミドルウェアの役割は下記の通り。

- リーダライタの接続状態の管理
- IC･ID カードの接続状態の管理
- IC･ID カード内の認証用データの取扱い（詳細は「2.6.2　IC･ID カードサービスに要求される機能」を参照）
  - －カード保有者が入力した本人確認情報（PIN 等）の照合要求
  - －公開鍵証明書の読み出し
  - －認証用の一時情報（NONCE; 乱数等）の生成要求
  - －データへの署名要求　　他

業務アプリケーションからは、ミドルウェアとのインタフェースを通じて IC・ID カードを扱うことになるため、このインタフェースから先のレイヤは一体のものとして認識される。本調査では、この範囲を IC・ID カードサービスと呼ぶ。

上記に示した IC・ID カードの取扱いについて、図 5 に示す。図 5 では、業務アプリケーションの機能は利用環境であるクライアント PC 内にあり、ネットワークを通じて取引先や申請先に接続している。

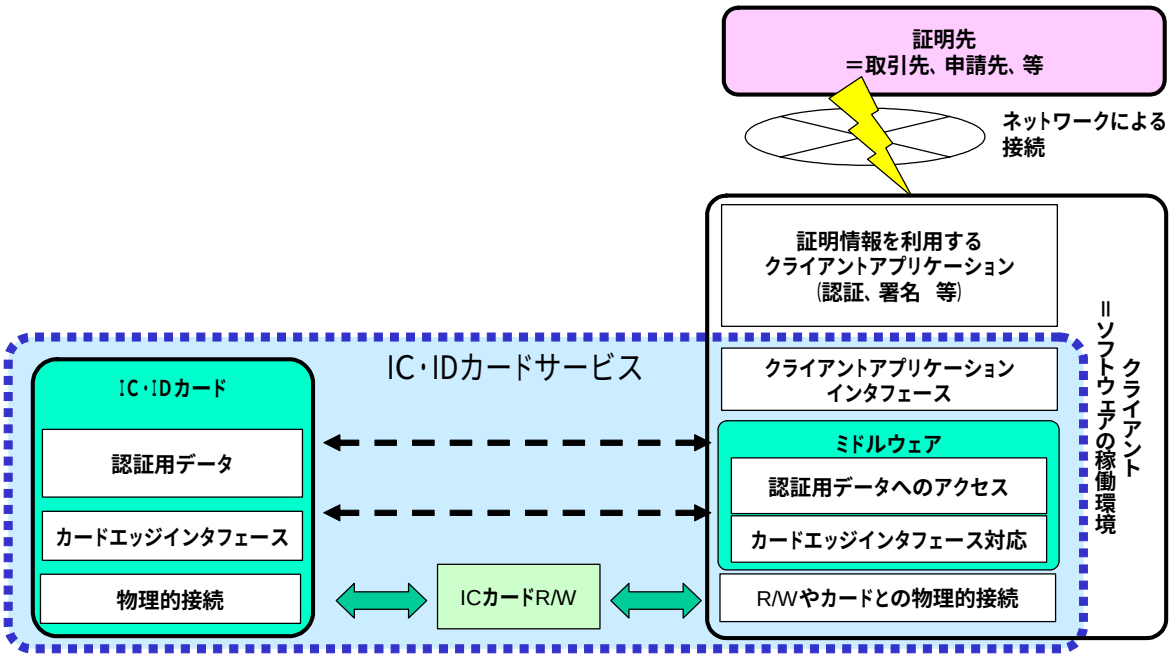



図 5　IC・ID カードサービスの位置づけ

### 2.6.2. IC・ID カードサービスに要求される機能

(1) IC・ID カードを用いた認証(Authentication)

IC・ID カードを利用した認証は、ネットワークを通じて提供されるサービスにおいて、クライアント環境を操作している者が、間違いなく、あらかじめ登録され、サーバを利用する権限を持つ者であることを確認するために、主に用いられる。この用途では、IC・ID カードに格納される鍵（プライベート鍵）の署名（演算）が利用される。図 6 に IC・ID カードを利用した典型的なチャレンジ・レスポンスによるリモート認証の例を示す。

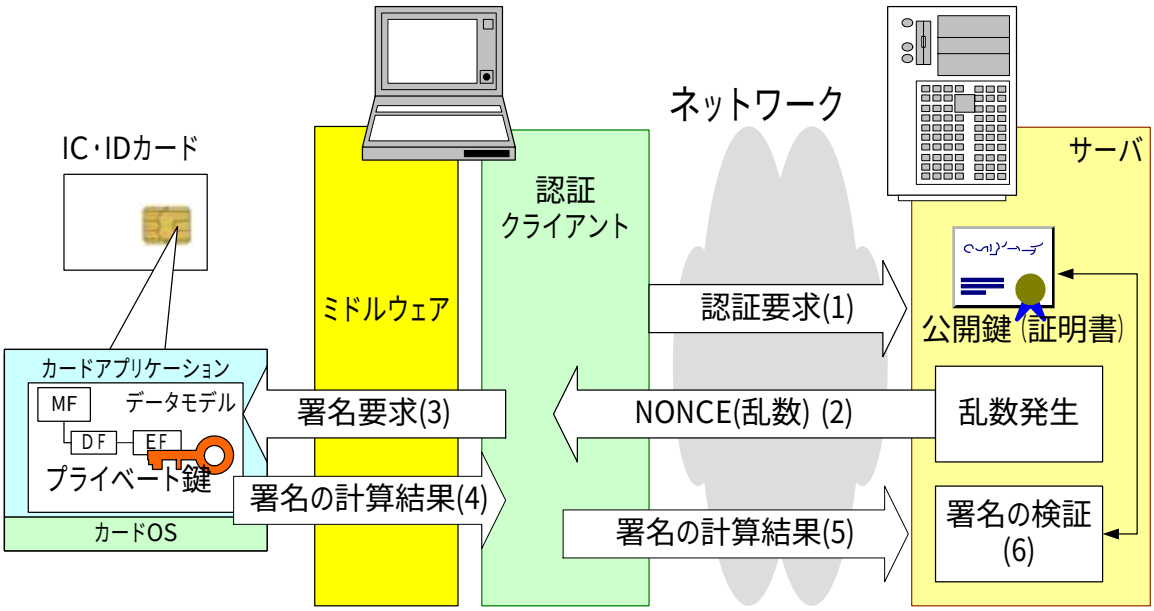



**図 6　リモート認証**

以下にリモート認証の手順を示す。

(1) 認証(Authentication)を要求する認証クライアントは、サーバに対して認証要求を行なう。
(2) サーバは認証要求に対して、この場限りの値である NONCE を生成し認証クライアントに送る。
(3) 認証クライアントは、サーバから受け取った NONCE を元に IC・ID カードに対して署名要求を行なう。
(4) IC・ID カードは、この NONCE に対してカード上で署名を施し、署名結果を返す。
(5) 認証クライアントは、受け取った署名結果をサーバに返す。
(6) サーバは、認証クライアントから送られてきた NONCE に対する署名を、公開鍵を使って検証する。

この例で分かるように、 IC・ID カードの秘密情報（プライベート鍵）は IC・ID カードから出ることはなく、ネットワーク上に流れることもない。また、 IC・ID カード保有者の秘密情報が、サービス側のサーバに格納されないことも重要な点である。サービス提供者は、IC・ID カード保有者の秘密情報（例えばパスワード）を預かる必要がない。これは IC・ID カード保有者にとっても、サービス提供者にとっても大きなメリットとなる。

(2) IC・ID カードによる署名

耐タンパー性を持った IC・ID カードにプライベート鍵が格納され、そのプライベート鍵の演算によりリモート認証を安全に行なえることを説明したが、IC・ID カードは、認証(Authentication)だけでなく、電子署名にも用いられる。

一定の要件を満たした電子署名の施された電子文書等は、「電子署名及び認証業務に関する法律」により「本人の意思に基づいて作成されたもの」（真正に成立したもの）であると推定される。

IC・ID カードを利用した文書への署名(ここでは自署名と表現する)と認証（Authentication）は、共にプライベート鍵による署名(プリミティブな操作としての署名を単に「署名」と表現する)を利用して実現される。しかし、自署名と認証では、そのプライベート鍵による署名の意味が大きく異なる。

図 7 に署名と（リモート）認証の鍵を使い分けている例を示す。

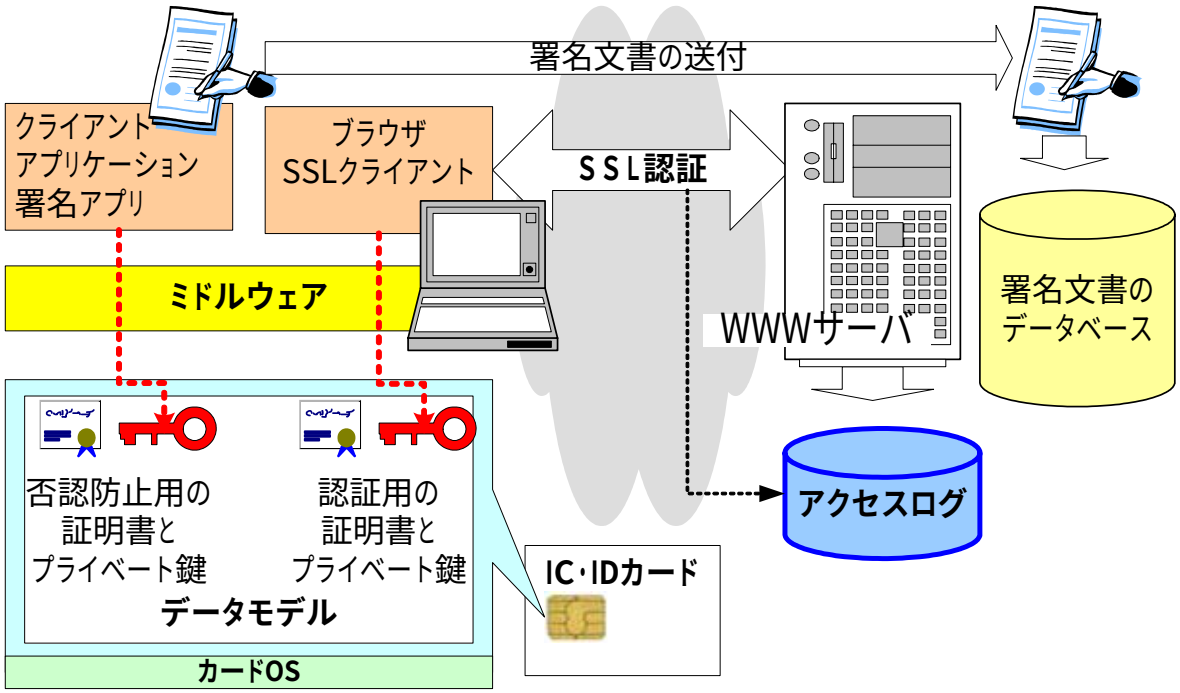



**図 7　リモート認証と否認防止の署名**

ここで IC・ID カード保有者は、カードに格納された２つのプライベート鍵による署名を使い分け、「クライアント認証」と「文書への電子署名」を行っている。IC・ID カード内のプライベート鍵による署名操作は、強い認証(Strong Authentication)機能を実現する。そして、この強い認証を利用することによりセキュアにサーバに電子文書を渡すといったことができ、サーバ側では認証のアクセスログとして残すことができる。しかし、それだけでは、電子契約などで要求される「実印での捺印」の代わりにはならない。契約文書などに自署名を施す際、IC・ID カード保有者は、この文章の内容を熟読した上で自分の意志を持って自署名を行う。

利害関係者間の文書のやり取り等では、IC・ID カード保有者の自署名が施された電子文書自身が相手に送付され、その署名された電子文書が保存されることが重要になる。このような自署名は、否認防止の署名と呼ばれる。

PKI では、この署名に使われるプライベート鍵に対応する公開鍵を証明するための電子的な証明書である公開鍵証明書が使われるが、IC・ID カードには、IC・ID カード保有者のプライベート鍵と共に、この IC・ID カード保有者の公開鍵証明書（以後、証明書）が格納される。この IC・ID カード保有者の証明書には、この証明書に対応したプライベート鍵の使用目的が記述されている。否認防止目的で使用される証明書には、証明書に含まれる証明書拡張フィールドの鍵使用目的(Key Usage)に、否認防止用を示すための non-repudiation(否認防止) bit が設定される。non-repudiation bit が設定された証明書に対応するプライベート鍵で(否認防止のための)署名を行う場合、そのアプリケーションは必ず署名者、すなわちカード保有者に自署名する文書を提示する必要がある。

(3) IC・ID カードに格納されるデータに対する操作

IC・ID カードには、プライベート鍵、証明書（カード保有者の証明書、カード保有者の信頼点になる証明書）などの他、IC・ID カードがカード保有者を認証するための認証用データ等が格納される。IC・ID カード自体が、公開鍵暗号を用いて外部機器などの認証（外部認証）を行なための公開鍵（証明書ではなく公開鍵のみ）が格納されることもある。これらの IC・ID カードに格納されるデータに対して様々な操作（オペレーション）が行なわれる。IC・ID カードサービスに要求される機能を正確に理解するためには、これらのデータが、IC カード自体、ミドルウェア、クライアントアプリケーションにおいて、どの様に扱われるか等を理解する必要がある。表２に IC・ID カードに格納されるデータとデータに対する操作を示す。

**表 2 IC・ID カードに格納されるデータとデータに対する操作**

| データ | データに対する操作 | 説明 |
|---|---|---|
| プライベート鍵 | 署名操作<br>(PSO: COMPUTE DIGITAL SIGNATURE)<br>復号<br>(PSO: DECIPHER) | プライベート鍵を使った操作を IC・ID カードで行なうため非常に重要。否認防止用の署名鍵の場合、復号に利用できないことも重要。 |
| 公開鍵 | 署名検証<br>（PSO: VERIFY DIGITAL SIGNATURE)<br>暗号<br>(PSO: ENCIPHER) | 署名（認証も含む）目的の場合 IC・ID カード上で公開鍵の演算（暗号化）を行なう必要はない。 IC・ID カード自体が外部を認証する（外部認証）の場合には、カード上での署名検証が要求される。 |
| 証明書 | READ BINARY<br>GET DATA | カード保有者が、署名検証を行う場合、カードに格納された信頼点の証明書の公開鍵を利用する。また、暗号化を行なう場合、カード保有者の証明書の公開鍵を利用する。 |
| 認証情報 | VERIFY<br>RESET RETRY COUNTER | カード保有者を IC・ID カードが認証する。 |

IC・ID カードにとって「プライベート鍵」は、最も重要なデータである。IC・ID カード上でのプライベート鍵による「署名操作」が重要なことは、前述したとおりである。その他に重要な機能として、プライベート鍵を使ったカード上での暗号の復号がある。公開鍵暗号においては、公開鍵を使って暗号化を行い、プライベート鍵を使って復号を行なう。ここで、IC・ID カード自体で利用される暗号化ではなく、クライアントアプリケーションにおける暗号化(例えば、S/MIME による暗号)は、カード保有者の公開鍵により行なわれる。これは多くの場合、カード上で行なわれる訳ではないことに注意すべきである。公開鍵を含んだ証明書が「READ BINARY」といったカードエッジ・インターフェースのコマンドを使って IC・ID カード外に取り出され、カード外で暗号操作がなされる。「プライベート鍵」と「公開鍵」の性格の違いをよく理解する必要がある。表 2 の「公開鍵」は、カード発行時等にのみに利用され、カード保有者（のアプリケーション）には利用されない場合が多いことに注意する必要がある。

# 3. IC・ID カードの相互運用可能性に関するニーズ

本章では、IC・ID カードが供給、利用されている現状を整理し、その現状を踏まえて、今後発生すると見られる、IC・ID カードの相互運用可能性へのニーズについて整理する。

## 3.1. 技術的背景

従来、IC カードは、サーバ、クライアントを含むシステム全体の中で、端末での利用者サービス、あるいはセキュリティ強化のツールとして提供されることが多かった。そのため、IC カードは、業務アプリケーション、クライアント端末（PC あるいはその他の機器）を含むソリューションの一部として提供されていた。

IC・ID カードにおいても、現在までは、リーダライタ及びドライバソフトウェアと一体のものとして、図 5 に示した「IC・ID カードサービス」の範囲がセットで提供され、仕様は供給ベンダごとに異なるケースが多い。また、IC・ID カード内部にデータを記録するファイルフォーマットやデータ記録形式も、業務アプリケーションごと個別に定められている。そのため、図 8 のように、クライアント環境、クライアントアプリケーション、ミドルウェア、リーダライタ、IC・ID カードは一体不可分の関係で提供される。

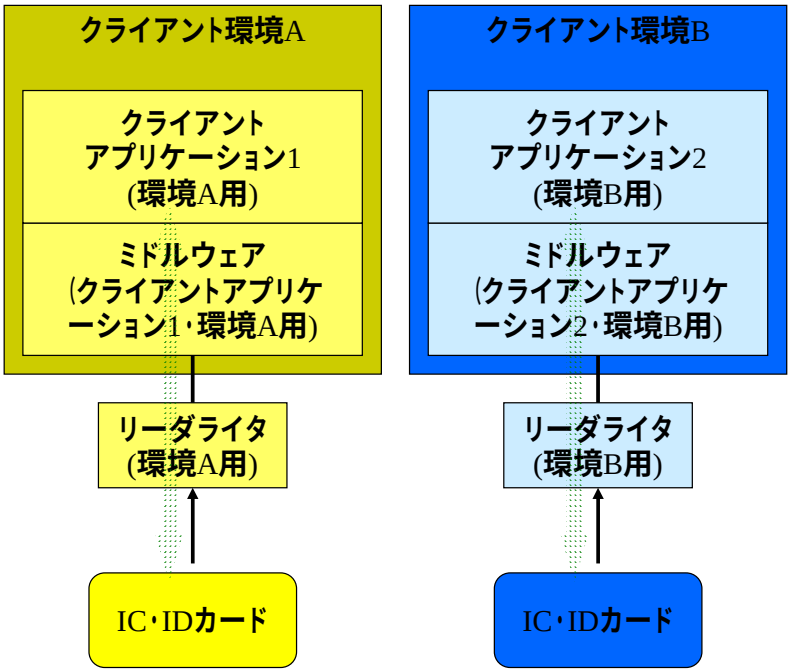



図 8　IC・ID カードの供給形態

このような状況では、IC・ID カードは対応するリーダライタ、ミドルウェア、及び、当初より予定された業務アプリケーションが実装されているクライアント環境でのみ利用可能である。すなわち、ある IC・ID カードは、その利用目的として開発されたクライアントアプリ

ケーション、ミドルウェア、リーダライタが稼動可能なクライアント環境でのみ利用される。当初予定以外のクライアント環境で利用するためには、クライアントアプリケーションだけでなく、ミドルウェアも新たなクライアント環境に合わせて開発し、リーダライタを通じた IC・ID カードの利用を可能にしなければならない。

しかしながら、IC・ID カードが業務アプリケーションと一体で利用され、また、使用が普及していない段階では、1 枚の IC・ID カードを複数の用途に利用したり、複数のクライアント環境で利用するといったニーズ自体が顕在化してこなかったため、相互運用可能性のないことが問題視されることは少なかった。

## 3.2. 認証用データの用途の広がり

e-Japan 戦略を皮切りとした一連の国内での公共分野を中心とした情報通信社会の基盤及びサービス環境の整備や、その環境を活用した民間分野でのオンラインでの各種サービスの広がり、同時にセキュリティに対する意識や対策の高まりの中で、PKI による認証や自署名の活用、すなわち IC・ID カードの活用場面が広がりつつある。

(1) ネットワークを通じたサービスでの利用者認証

情報資産に対するセキュリティ意識の広まりの中で、重要な情報を持つネットワークやデータベースへのアクセスに際しては、従来多くのケースで用いられてきた利用者による ID とパスワードの入力よりもより高度な方法での認証が求められるようになってきている。

すなわち、利用を許可された本人以外がクライアントアプリケーションを操作している場合にも、正しい ID とパスワードが入力されてしまうケースが増加していることを考慮し、本人がクライアントアプリケーションを利用していることをより確実なものとして認証できる仕組みが導入されている。

この強固な認証の方法のひとつに、PKI を活用した認証がある。具体的な手順は「2.6.2 IC・ID カードサービスに要求される機能」に示したが、IC・ID カードを活用して認証を行うことにより、登録されている本人のカードが確実にクライアントに挿入されていること、すなわち、クライアントアプリケーションを操作しているのが登録された本人であることがより確実に推定される。普及している例の一つとしては、ウェブサーバを利用したサービスにおいて、SSL（Secure Socket Layer）による暗号通信を実施する際に、IC・ID カードによってクライアント認証を実施するものがある。

(2) 電子署名の付与

電子的に行われた取引の結果は電子データで保存されるが、一般に電子データは複製や改変が簡単に可能である。したがって、保存されている電子データに文書としての証拠能力を確保

するためには、取引の実施者が自らその内容を確認していることと合わせて、作成後内容が改変されていないことが保証されなければならない。

そのため、「2.6.2　IC・ID カードサービスに要求される機能」に示したように、IC・ID カードによって取引文書に電子署名を行う方法が採用されている。PKI の仕組みを利用した電子署名とその検証は、証拠性を確保する書類を電子的に作成する際には広く用いられており、各種の手続き・取引のオンライン化の進展につれて、利用場面は広がっている。

(3) 手続き実施者の資格の証明

各種の手続きや取引の中には、その実施者が特定の資格を持つも者に限られるものが少なくない。関連する資格としては、医師、歯科医師、薬剤師等の医療従事者、行政書士、税理士等のいわゆる士業があるほか、公務員としての官職においてのみ作成可能な文書もある。これらの業務が電子的に実施される際には、業務の実施者が当該業務を行う資格を持つ者であることが保証されなければならない。

また、一般の市民や企業による申請や手続きにおいても、その実施者の存在や属性が確認されてはじめて実施可能となる手続きも少なくない。紙の手続きで住民票や印鑑登録証明書、その他の本人確認書類を添付することで成立するような手続きは、電子的に行われる際にも、実施者の身元が登録されていることが、信頼される第三者によって確認されなければならない。

そのため、上述した用途で PKI を利用する際の電子証明書は、単に公開鍵が登録されていることを証明するだけでなく、証明書の発行を受けた者の居住地、所属と権限、資格と有効期限、等、取引に必要な情報が合わせて登録されていることを証明するようになっている。カード保有者は、取引で必要とされる証明書を使い分ける。例えば、開業医は、医師として紹介状を作成する際には医師の資格を証明する電子証明書で署名を行うが、税の申告をする際には、個人として居住地の証明を受けた公的個人認証の電子証明書を用いる、といったことになる。

## 3.3. IC・ID カードの相互運用の例

IC・ID カードの利用場面が広がると、IC・ID カードは、特定の業務アプリケーション専用のツールとしてではなく、サービスの利用資格を証明し、オンラインでのサービスにおいて認証、署名等の機能を提供するツールとして、より一般的な位置づけが求められるようになる。企業が企業として利用できるサービスは 1 枚の IC・ID カードで、医師が医師の資格で利用できるサービスは 1 枚の IC・ID カードで、それぞれ利用できることが求められ、また、医師と患者相互の承認によって成立する、例えばカルテの開示のようなサービスでは、サービスの提供側と利用側の IC・ID カードの双方を利用できる環境が求められる。

すなわち、1 枚の IC・ID カードが複数のクライアント環境、複数のクライアントアプリケーション、複数のサービスに利用されるような状況が求められるようになる。また逆に、1 つのクライアント環境で、複数のクライアントアプリケーション、複数の IC・ID カードを利用できるような状況が求められるようになる。これは、今後 IC･ID カードをはじめとした IC カ

ードの個人利用の普及を図るための検討においても、必要性が指摘されている[2]。

この関係の例を図 9 に示す。

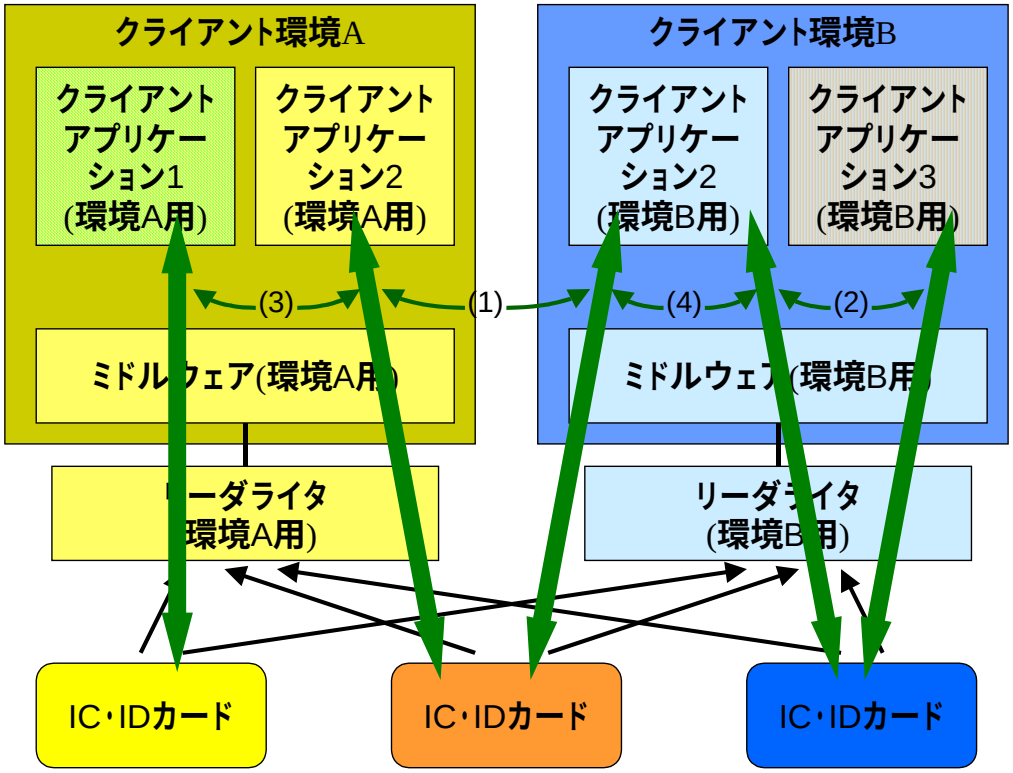



**図 9　IC・ID カードの相互運用の例**

このように、従来の利用パターンから離れて、クライアント環境、クライアントアプリケーション、IC・ID カードが互いに異なるもの同士が共存し、必要に応じて組み合わせて利用されるような状況を「IC・ID カードの相互運用」と表現する。

IC・ID カードの相互運用の具体的な姿について、以下に分類、整理する。

(1) 異なるクライアント環境での IC・ID カードの利用

以下に示すような状況では、1 枚の IC・ID カードを複数のクライアント環境で利用できることが求められる。

- 大学などの研究環境で、ネットワークを通じた研究環境、研究資源への接続時の認証に IC・ID カードを利用する場合、クライアント環境にはそれぞれの研究に適した OS やミドルウェアが導入されている。
- 医療機関で IC・ID カードが利用される場合、すでに普及している電子カルテシステムとの連動が期待されるが、現在、電子カルテとして、Windows 環境に対応したものだけでなく、Linux に対応したものも広く普及している。
- 個人の自宅からの利用を前提とした場合、個人が日常的に利用しているパソコンで利用できることが求められる。公的個人認証では、Windows 環境に対応したミドルウェアだけでなく、Mac

OS に対応したミドルウェアの開発を進めてきている。

- 企業のように、導入時には特定のクライアント環境での利用に限定して普及を図ることができるケースでも、普及期間が長くなるにつれて、クライアント OS のバージョンアップ等、より多くのクライアント OS を想定する必要が生じる。

以上のように、IC・ID カードの利用が広がるに連れて、クライアント環境の OS として、特定種の特定バージョンだけでなく、複数種のクライアント OS、またさまざまなバージョンが混在することを想定する必要が生じる。

(2) 1 枚の IC・ID カードの複数用途への利用

以下に示すような状況では、1 枚の IC・ID カードを、当初予定していた用途だけでなく、新たな業務アプリケーションにも利用できることが求められるようになる。

- ある特定の電子入札システムで利用するために発行された企業向けの IC カードを利用して、他の行政機関の電子調達や電子申告を行いたい。どちらのサービスも、企業と担当者の存在、所属の関係が保証されれば、利用可能である。
- ある研究機関の内部で各種の研究環境の利用者認証に使っている IC･ID カードで、他の研究機関との共同研究のための研究環境の利用者としての認証も受けたい。どちらのサービスも、当該研究機関の構成員であることが証明されれば、利用可能である。

以上のように、IC・ID カードを利用する業務アプリケーションが広がるに従い、複数のサービスに対して、証明する属性が同じならば、同じ IC・ID カードで利用したいという要求も広がってくることが想定される。

(3) IC・ID カードと業務アプリケーションの組み合わせを 1 環境で複数種利用

以下に示すような状況では、1 つの利用環境で、複数種の IC・ID カードを用途に応じて使い分けることが求められる。

- 企業において、営業担当者が電子調達用の IC･ID カードを利用して入札を行うクライアントで、新たに会計担当者が電子申告用の IC･ID カードを利用して税の申告を行ったり、登録資格に基づく申請（建築士による建築確認申請等）を行ったりする。
- 医療機関において、他の医療機関への紹介状を送受信するクライアントで、医療機関としての税の申告を行う。

以上のように、IC・ID カードを利用する業務アプリケーションが広がるに従い、前述したように 1 枚の IC・ID カードが証明する属性では利用できないような異なる用途に対して、複数の IC・ID カードを使い分ける場合であっても、1 台のクライアントに両方を利用するクライアントアプリケーションを導入し、クライアントごとに必要な IC・ID カードを挿入して利用できるようにすることが求められると想定される。

(4) 1 種のクライアントアプリケーションで複数種の IC・ID カードを利用

以下に示すような状況では、1 つの利用環境、1 種のクライアントアプリケーションでも、複数種の IC・ID カードを利用できることが求められる。

- 保健医療福祉分野の公開鍵基盤（HPKI: Healthcare PKI）では、医師向けの証明書を証明する認証局は複数存在し、それぞれの認証を受ける IC･ID カードは、都合複数のカードベンダから供給されると想定される[3]。医師が複数の医療機関に勤務する場合、医療機関側では、複数のカードベンダから供給され、それぞれの認証局の認証を受ける IC･ID カードを同様に利用できることが求められる。
- ある業務アプリケーションにおいて、長期間にわたって IC･ID カードが利用される場合には、IC･ID カードの供給ベンダから供給されるカードの種類が変わることや、特に公的な機関において、供給ベンダ自体を変更する必要が生じる可能性がある。この際に、従来利用していた IC･ID カードと新たに調達した IC･ID カードが、同じ環境で利用できることが求められる。
- 今後、住民による電子的な委任に基づいて行政書士等が代理申請を行う場合や、医師が、他の医師からの紹介状と患者の同意に基づいて、患者の電子カルテにアクセスするようなケースが考えられるが、この場合、依頼者（住民あるいは患者）の IC･ID カードと、サービスの実施者（行政書士あるいは医師）の IC･ID カードの双方による認証あるいは署名が行われて、初めてサービスを実施できるようにする必要がある[4]。このような用途では、元来異なる用途に発行された IC･ID カードを同時に利用できるクライアント環境が必要である。

後者の例として、公的個人認証では、IC・ID カードを供給するベンダが複数社ある中で、いずれの自治体においてもできるだけ多くのリーダライタが利用できるよう、財団法人自治体衛星通信機構が検証仕様書、検証プログラム、検証用 IC カードを提供し、リーダライタ製造ベンダによる適合性検証を行っている[5]。結果として、多くの自治体が発行したカードに共通で利用できるリーダライタが多数供給されており、住民が引っ越して、引越し先の自治体から新たに住民基本台帳カードの交付を受け、公的個人認証の証明書の発行を受けた場合でも、自宅にある従来のリーダライタが引き続き利用できる可能性が高くなっている。

## 3.4. 相互運用を実現するための技術的要求

前節に示した IC･ID カードの相互運用を実現するために必要な、技術的な要求を整理する。

(1) 異なるクライアント環境での IC・ID カードの利用

1 枚の IC・ID カードを異なるクライアント環境で利用できるようにするためには、利用が想定されるクライアント環境に対して、当該 IC・ID カードの利用が可能なリーダライタ、ミドルウェア、及びクライアントアプリケーションが提供されなければならない。この場合に、単一のベンダが、あらゆるクライアント環境に対するミドルウェアやリーダライタを開発・提

供するのは、あまり現実的とはいえない。ベンダによっては、ミドルウェアの開発において、クライアント OS による得手不得手があり、特定の OS に対するミドルウェアの供給が遅れることが懸念される。

一方で、それぞれのクライアント環境で利用できる IC カード、あるいはリーダライタは、それぞれに存在する。したがって、それぞれの供給ベンダが、一定のインタフェースに沿ってミドルウェアを提供すれば、クライアント環境ごとに供給されているリーダライタやミドルウェアを、それぞれ導入すれば利用できる。

また、大学などの研究機関では、自らのクライアント環境で研究・開発に必要なソフトウェアを自ら開発して自己の責任のもとに利用できる者も少なくない。特定の研究に最適化されたクライアント環境に合わせて動作するミドルウェアを自ら開発できるような仕様が整備されていれば、ベンダ側が特殊なクライアント環境に考慮する必要は少なくなる。

以上のような考察から、異なるクライアント環境での IC・ID カードの利用には、IC・ID カードに係わる技術が以下のように整理されている必要がある。

- クライアントアプリケーション、ミドルウェア、IC・ID カードの間でのセキュリティ構造が明確に定義されている
- クライアントアプリケーションとミドルウェアのインタフェースが明確に定義され、仕様が公開されている
- ミドルウェアとリーダライタのインタフェースが明確に定義され、仕様が公開されている
- カードエッジインタフェースが明確に定義され、仕様が公開されている

(2) 1 枚の IC・ID カードの複数用途への利用

1 枚の IC・ID カードを複数の用途に利用するためには、当該 IC・ID カードを利用するためのミドルウェアが、新たに利用しようとするクライアントアプリケーションでも利用できることが求められる。IC・ID カードを利用するクライアントアプリケーションは、供給ベンダが異なることが容易に想定されるため、クライアントアプリケーションとミドルウェアのインタフェースや IC・ID カードへの認証用データの記録方法であるデータモデルの仕様が非公開の場合には、関連するアプリケーションのベンダの間で、個別に協議を行う必要が生じる。また、IC・ID カード及び当初利用されるクライアントアプリケーションと、追加利用するクライアントアプリケーションの組み合わせが増えたときには、この協議の組み合わせも相当な数になってしまう。このような事態を避けるためには、IC・ID カードに関する技術が以下のように整理されている必要がある。

- IC・ID カードサービスとクライアントアプリケーション間のインタフェースが業務アプリケーションを超えて標準化され、公開されている。
- 電子証明書の検証手順等が標準化及び公開され、どの認証局へも同一の手順で利用可否の確認や電子証明書の検証ができるようになっている。

なお、手順やインタフェースが公開されていることは、どの業務アプリケーションからも証明書の検証を受け付けることを意味するものではない。どの業務アプリケーションからの証明

書検証要求に対応するかは、認証局のポリシーによって決定される。

(3) IC・ID カードと業務アプリケーションの組み合わせを 1 環境で複数種利用

IC・ID カードと業務アプリケーションの組み合わせを 1 環境で複数種利用するためには、それぞれのクライアントアプリケーションで利用するミドルウェア及びリーダライタについて、自由に切り替えて使えるように共存しているか、共用できる状態になっている必要がある。

利用者のクライアント環境に配慮すれば、リーダライタは 1 枚を共有できていることが望ましいため、リーダライタとミドルウェアのインタフェースは標準化されている必要がある。その上で、複数のミドルウェアが互いの動作を干渉することなく共存できるよう詳細に条件が定められているか、あるいは、1 種のミドルウェアで双方の IC・ID カードに対応できるようになっているかの、いずれかが求められる。

以上を整理すると、IC・ID カードに関する技術は以下のように整理される必要がある。

- ミドルウェアとリーダライタのインタフェースがベンダを超えて標準化され、公開されている。
- 複数のミドルウェアが共存できるよう、ミドルウェアの開発条件が定められ、各ベンダによって遵守されている。あるいは、ミドルウェアとクライアントアプリケーションのインタフェース、データモデル、カードエッジインタフェースのそれぞれが標準化され、仕様が公開されている。

(4) 1 種のクライアントアプリケーションで複数種の IC・ID カードを利用

1 種のクライアントアプリケーションで複数種の IC・ID カードを利用するためには、ミドルウェア、リーダライタを、挿入された IC・ID カードごとに使い分けるか、あるいはひとつのミドルウェアとリーダライタがいずれの IC・ID カードにも対応できるようになっているか、いずれかが必要である。

いずれの考え方においても、クライアント環境に配慮すれば、リーダライタは 1 台がどの IC・ID カードにも適用可能であることが求められる。

また、前者の考え方は、クライアントアプリケーションで利用する IC・ID カードの種類が少数に限定される場合には、利用しうる IC・ID カードすべてに対応するミドルウェアを導入しておけばよいが、医師と認証する患者の IC・ID カードといった、発行者が多岐にわたり、ベンダも多岐にわたることが想定されるようなカードを対象とする場合には、少なくともひとつの分野の IC・ID カードに関しては、1 種のミドルウェアがどのベンダが製造し、どの調達者が発行したものでも扱えるようになっていることが求められる。

以上を整理すると、IC・ID カードに関する技術は以下のように整理される必要がある。

- 業務アプリケーションとミドルウェアのインタフェースが明確に定義され、公開されている。
- ミドルウェアとリーダライタのインタフェースがベンダを超えて標準化され、公開されている。
- ひとつの分野の IC･ID カードにおいて、データモデルがベンダを超えて標準化されている。
- 認証用データの記述内容及び電子証明書の検証手順等が標準化及び公開され、どの IC･ID カード及び認証局へも同一の手順で利用可否の確認や電子証明書の検証ができるようになっ

ている。

なお、手順やインタフェースが公開されていることは、どの業務アプリケーションからもIC・ID カード内の認証用データを利用できることや証明書の検証を受け付けることを意味しない。同一の方法によって、クライアント環境に挿入されている IC・ID カードの認証用情報の利用や電子証明書の検証が可能であるか否かが判別できることが求められる。

# 4. 標準化の動向

## 4.1. 国際標準化の動向

### 4.1.1. IC カードシステムに関する国際標準

IC カードシステムに係わる国際標準のうち、利用分野を特定しない標準としては、ISO/IEC 7816 シリーズと、ISO/IEC 24727 シリーズがある。前者は、IC カードそのものに焦点を当てて、物理的な特性からカードの機能、記録されるデータと標準の範囲を広げてきているのに対し、後者では、広範な用途に利用できる IC カードシステムのアーキテクチャを定義した上で、機能のレイヤやレイヤ間のインタフェースを定め、その中でデバイスとしての IC カードについても、ISO/IEC 7816 シリーズの標準からアーキテクチャにあったものを選択･定義しようとしている。

(1) ISO/IEC 7816 シリーズ

ISO/IEC における IC カード関連の標準として代表的なものに ISO/IEC 7816「ID カード – IC カード」シリーズがある。7816 シリーズは、IC カード自体の規定とその利用法に関する標準である。5 つのパートが電気的な接触、つまり接触カードに関するものである。下記にその名称を示す。

- ISO/IEC 7816-1 接触カードの物理的特性
- ISO/IEC 7816-2 接触端子の寸法と位置
- ISO/IEC 7816-3 非同期カードにおける電気的インターフェースと伝送プロトコル
- ISO/IEC 7816-10 同期カードにおける電気的インターフェースとリセット応答（ATR）
- ISO/IEC 7816-12 USB カードにおける電気的インターフェースと操作手続き

他のパートは、接触・非接触を問わず IC カードに共通するものとなっている。下記にその名称を示す。

(2) ISO/IEC 24727 シリーズ

一方、多様なアプリケーションドメインにまたがった相互運用可能性を望むようなクライアントアプリケーションを実現するときに利用される標準として、ISO/IEC 24727 シリーズが提案され、現在検討がなされている。カードアプリケーションとクライアントアプリケーション間で情報やトランザクションをやりとりするにあたってのプログラミングインターフェースを提供している。2006 年 10 月現在、24727 シリーズは下記の 5 つより構成されている。

- ISO/IEC FDIS 24727-1 アーキテクチャ
- ISO/IEC FCD 24727-2 汎用カードインターフェース

- ISO/IEC CD 24727-3 アプリケーションインターフェース
- ISO/IEC NP 24727-4 API 管理（API administration）
- ISO/IEC NP 24727-5 テスト

24727-1 は、24727 全体の序説となるパートであり、概念的なフレームワークの説明を行っている。これを元に、他のパートはこの概念の技術的詳細を提供している。24727-2 は、カードコマンドレベルでのプログラミングインターフェースを定義するものであり、ISO/IEC 7816 標準群のコンセプトやデータ構造、カードコマンドを具現化するためのものである。24727-3 は、言語や実装と独立してアプリケーションレベルでのインターフェースを定義するものである。

### 4.1.2. カードエッジインタフェース

IC カードと外部との通信に利用されるカードエッジインタフェースについて、物理インタフェースとコマンドインタフェースに分けて整理する。

(1) 物理インタフェース

IC カードとリーダライタの物理的なインタフェースとしては、外部端子 IC カード（一般的には、接触型 IC カードと呼ばれる）と非接触 IC カードがある。非接触 IC カードの通信規格には、通信距離によって数種類があるが、現在一般に普及している非接触 IC カードは、近接型と呼ばれる種類であり、ISO/IEC 14443 シリーズとして国際標準化がなされている。なお、現在国内で交通分野を中心に広く普及しているカードは、IC カードとしては国際標準化がなされていないカードであり、国際標準に準拠した近接型非接触 IC カードは、国内では住民基本台帳カードや国家公務員 IC カードで採用されている。

ISO/IEC 24727 シリーズでは、IC カードの物理インタフェースについては、ISO/IEC 7816 シリーズで定める接触型 IC カードのインタフェースと、ISO/IEC 14443 シリーズで定める近接型非接触 IC カードのインタフェースに準拠している。

(2) ISO/IEC 7816 シリーズによるコマンドインタフェース

IC・ID カードに関するコマンドインタフェースは、ISO/IEC 7816 シリーズにおいて、以下のように分類、定義されている。

- ISO/IEC 7816-4 構成･セキュリティ･交換のためのコマンド
- ISO/IEC 7816-7 SCQL（Structured Card Query Language）用コマンド
- ISO/IEC 7816-8 セキュリティオペレーション用コマンド
- ISO/IEC 7816-9 カード管理用コマンド

ISO/IEC 7816-4、7、8、9 はそれぞれ IC カードに対して入力されるカードコマンドを規定したものとなっているが、これらは 2004 年から 2005 年にかけて大きく改訂されたものであ

る。改訂前では、IC カードの構成やセキュリティとして重要な概念などが分散している傾向にあった。IC カードの標準を策定していくにあたり、順次標準化されていったための結果である。改訂にあたりそれらの構成やセキュリティの概念、さらにカードコマンドの基本的な部分をすべて 7816-4 にまとめ、その上で用途別のカードコマンドを規定するものとして 7816-7、8、9 をあらためて記した。そのため、改訂前とはそれぞれのタイトルも変化していることに注意されたい。

これらの標準は、IC カードのコマンドや、その拡張機能として、非常に広範な機能を許容しており、標準に定義されている各種の機能は、ほとんどがオプションの扱いになっている。それは、これらの国際標準の制定や見直しに際し、すでに各国で発行されている IC・ID カードが標準不適合になってしまうような事態を防止するため、また、IC カードの限定的なメモリ容量や処理能力で効率よく必要な機能を実現したい個別の要求に対応しても標準不適合にならないためである。

このように制定されている国際標準に準拠した IC・ID カードは、機能面でも性能面でも多様であるため、これらすべてに対応可能なミドルウェアやリーダライタは提供されていない。したがって、仕様策定者が IC・ID カードの仕様を定めるにあたっては、単に国際標準を示すだけでは不十分であり、利用するコマンドやデータモデルを選択・指定する必要がある。結果的に、それぞれが独自の仕様となるため、国際標準に準拠していない IC・ID カードを調達するのと比較しても、相互運用可能性が高いことにはならない。

(3) ISO/IEC 24727 シリーズによるコマンドインタフェース

ISO/IEC 24727 シリーズでは、汎用に利用可能な IC カードのアーキテクチャを定義し、そのアーキテクチャに沿って利用されるカードコマンドや、IC カード内に存在する機能表示（Capability Description）が規定されている。機能表示は、カードアプリケーションの機能表示を行う ACD（Application Capability Description）とカードの機能表示を行う CCD（Card Capability Description）の 2 種類ある。CCD は IC カード内に 1 つのみ存在し、ACD は各カードアプリケーションに存在する。

ISO/IEC 24727-2 の汎用カードインターフェースで規定されているカードコマンドは、ISO/IEC 7816 で規定されているカードコマンド群から、IC カードサービスの相互運用を実現する観点から選択されている。24727-2 で規定されているコマンドは、以前の草案ではすべて必須コマンドとされていたが、2006 年 11 月時点の草案ではそれらは必須ではなく「利用されるべき」となっている[6]。

### 4.1.3. データモデル

(1)ISO/IEC 7816-15

IC・ID カードに記録される、暗号や認証、電子署名を行うために必要な情報の相互運用可

能性を確保する目的から、国際標準 ISO/IEC 7816-15 が定義されている。

この標準では、IC・ID カードの持つ機能や特性、記録される情報の保存形式やファイル構造は、一意に規定されているわけではない。

ISO･IEC 7816-15 では、認証用データを含む一群のファイル構造は暗号情報アプリケーション（CIA: Cryptographic Information Application）と呼ばれる。暗号情報アプリケーションのファイル構造の最上位には、CIA に関する基本情報を示すファイル（EF CIA Info）と、CIA に含まれる暗号情報オブジェクトとその参照を示すファイル（EF OD）が配置される。

ISO･IEC 7816－15 では、EF CIA Info 及び EF OD へのアクセス方法及び情報の記述方法が定義され、カードを発行した際に任意に作成された CIA の構造を、EF CIA Info 及び EF OD によってカード外から知ることができるようにすることで、CIA が記録された IC カード間の相互運用可能性を確保しようとしている[7]。

EF CIA Info には、カードのバージョンやシリアル番号に加え、読み取り専用、利用に認証を要する、等のカードの利用方法に関する情報が記録される。さらに、CIA のセキュリティ設定や、カード保有者や発行者等の情報等を記録することができる。

EF OD には、CIA に含まれる暗号オブジェクトと、そのオブジェクトを利用するための参照情報が記録される。証明書がどこに入っているのか、署名を計算させるために必要な鍵 PIN の照合にはどのファイル番号を指定すればよいかがわかる。

ただし、ISO/IEC 7816-15 も、さまざまな CIA を IC カード内で実現できるように標準が策定されており、また、CIA を構成する暗号鍵等を利用するためのコマンド機能は、ISO/IEC 7816-4 や 8 に代表されるコマンド群から任意に選択して利用することができる。したがって、実際には、ある IC カードが単に ISO/IEC 7816-15 に準拠して CIA が記録されている、ということだけがわかっても、CIA に含まれる認証用情報を利用できることを必ずしも示さない。

(2) ISO/IEC 24727

ISO/IEC 24727 では、CIA 等の IC・ID カードとしての用途に利用されるものを含む、IC カードがどのような用途に利用され、そのためにどのようなファイル構造を持つか、は、標準対象外としている。

### 4.1.4. クライアントアプリケーションインタフェース

(1) ISO/IEC 7816 シリーズ

ISO/IEC 7816 シリーズでは、IC カードに焦点が当てられ、IC カードと外部とのインタフェースを標準化している。したがって、IC カードと接続された外部のデバイスで、どのように IC カードを利用する環境を実現しているかといったことは、標準の対象外である。

(2) ISO/IEC 24727 シリーズ

ISO/IEC 24727 シリーズでは、クライアント環境において、クライアントアプリケーションの間で IC カードの相互運用可能性を高めることに主眼が置かれている。そのため、クライアントアプリケーションとミドルウェアの機能を明確に分離し、インタフェースの定義、標準化を図っている[8]。

ISO/IEC 24727 シリーズでは、クライアントアプリケーションインタフェースとして、クライアントアプリケーションがリーダライタを使って IC カードにアクセスする際に必要とされる機能のうち、業界横断的に必要と考えられるものを抽出し、関数として定義している。定義されている関数は、以下のように分類される。

- カードへの接続
  初期化･切断や、カードアプリケーションへの接続などの関数がある。
- カードアプリケーションの利用
  カードアプリケーション一覧の取得、カードアプリケーションの作成･削除、アクションの実行などの関数がある。
- データセットの処理
  データセット一覧の取得、データセットの作成･選択･削除などの関数がある。
- 暗号サービス
  チャレンジの取得、署名検証、署名、暗号化･復号化の関数がある。
- 認証対象の処理
  認証の対象となる差分アイデンティティ（Differential-Identity）の一覧取得･作成･削除などに加え、認証を行う関数が含まれる。
- 認可サービス
  アクセス制御リストの一覧取得と、アクセスルールの更新を行う関数が含まれる。

(3) PKCS#11

IC・ID カードシステムのクライアントアプリケーションインタフェースとしては、RSA セキュリティ社により規定された仕様であり、認証用データが記録されたトークンに対して証明書の処理や公開鍵暗号の鍵ペアを利用した演算を行うための API が規定された「PKCS#11」がある。

PKCS#11 では、認証用データが記録される媒体として必ずしも IC カードを想定しているわけではなく、他のデバイスも含めて扱う、より上位のインタフェースである。

ISO/IEC 24727-3 と PKCS#11 ではともに API を規定しているが、その粒度は大きく異なる。たとえば暗号に関連する関数では、24727-3 では暗号化・復号化、署名計算と検証、チャレンジの取得があるが、PKCS#11 ではさらに詳細にメッセージダイジェストに関する計算や乱数生成に関する関数などを含んでおりその機能が詳細にわたっている。ISO/IEC 24727 が規定しているのは IC カードが提供するサービスの相互運用に関連するものであり、認証用デ

ータを扱う関数を集約することを目的とした PKCS#11 とはスコープが異なっていることが原因であると考えられる。

### 4.1.5. IC・ID カードに関する国際標準動向の整理

以上により、IC・ID カードに関する国際標準化動向は、表 3 のように整理される。

**表 3　IC・ID カードに関する国際標準化動向**

| | | ISO/IEC 7816 シリーズ | ISO/IEC 24727 シリーズ | PKCS#11 |
|---|---|---|---|---|
| カードエッジインタフェース | 物理的接続 | 明確に規定。相互運用可能性 | ISO/IEC 7816 及び 14443 を参照 | 規定せず |
| | コマンド | 多数のコマンドを定義し、実装は基本的にオプション。相互運用可能性 | 左記から相互運用を意識してコマンドを抽出・定義 相互運用可能性 | 規定せず |
| データモデル | | データモデルの標準を定義もオプション多くコマンドも限定されず。相互運用可能性 | 規定せず | 規定せず |
| クライアントアプリケーションインタフェース | | 規定せず | 汎用用途での関数を定義も IC・ID カードにはやや不足。相互運用可能性 | 認証用データを扱う機能群の関数を詳細に定義。相互運用可能性 |

## 4.2. 国際標準の普及動向

### 4.2.1. 欧州における動向

欧州では、国際標準を活用した各種情報システムの構築が盛んに取り組まれており、IC・ID カードの分野も例外ではない。IC カードに関しても、ISO/IEC 7816 シリーズをはじめとした、国際標準の制定においても主要な役割を担ってきている。

また、EU 内では国を超えて各種のサービスを相互に利用できる仕組みを整えつつあり、IC カードをその基盤技術として活用しようとしている。例えば、医療保険の分野では、自国にて加入した医療保険を、EU 内の他の国で医療機関を利用した場合でも同様に適用が受けられるよう制度を整備すると共に、相互に母国語が異なる環境で必要な情報を確実に伝達するよう、IC カードを利用して電子データで手続きを実現しようとする取組みが行われてきている。

政府機関のサービスにおいても、同様の取組みがなされている。欧州の標準化機関であるCEN を中心に検討が進められてきており、例えば、CEN/ISSS Workshop eAuthentication では、2004 年 3 月に、「Towards an electronic ID for the European Citizen, a strategic vision」として、IC・ID カードの認証、署名機能を活用して、ヨーロッパ全体で汎用的に、ネットワークを通じて電子的に提供される公共分野のサービスを利用可能とするための技術的枠組みの案を整理している[9]。

各国での具体的な導入事例としては、フィンランド、ベルギーなどが挙げられる。いずれの取組みにおいても、ISO IEC 7816 シリーズなどの国際標準に準拠した技術体系を整備し、公開された仕様のもとにインフラ整備を行っている。

### 4.2.2. 米国における動向

2004 年 8 月、米国では連邦政府施設への物理的・論理的アクセスのセキュリティ強化のため、身分証の標準を規定する大統領令 HSPD-12 が発令された。それに従い、米国国立標準技術研究所（NIST）が政府調達基準として FIPS（Federal Information Processing Standard）PUB 201 をはじめとする一連の仕様を発行し、身分証の標準を規定した。

PIV の技術体系は、米国の政府機関におけるセキュリティ強化と目的がはっきりしており、一連の完結した技術体系として整理されている。ここでは、ISO/IEC 7816 シリーズ等の国際標準を活用はしているが、詳細な仕様においては国際標準から外れた仕様も定義されている。

PIV の技術体系における特徴としては、システム構造の定義とインタフェースの規定、試験仕様を含む相互運用可能性の確保、仕様の公開の 3 点が挙げられる。

まず、システム構造の定義とインタフェースの規定としては、IC・ID カードを利用して関係者の認証を行うシステムの構造を整理し、それぞれの部品の間でのインタフェースを明確に定義している。これにより、システムを構成する各種の部品を個別に調達することができるようになる。

さらに、調達する部品間のインタフェースの適合、相互運用可能性の確保のため、試験仕様を公開すると共に製品認定制度を運用し、政府関連のどの期間でも、個別に調達した製品を組み合わせて必要なシステムを構築できるよう体系を整備している。

仕様の公開では、インタフェースを含む技術体系について、原案の段階から公開し、広く意見を求めてセキュリティ面を中心に向上を図ってきた。早い段階から公開することにより、セキュリティ上の弱点を専門家によって洗い出し、修正することができている。

PIV に基づき、米国から、汎用的に利用可能な IC カードシステムのアーキテクチャとして、ISO/IEC 24727 が提案されている。

このように、米国では、自国で必要とされる情報システムについて、体系から国内での公開と標準化をはかり、その上で国際標準化を図るというプロセスで取り組んでいる。

## 4.3. 国内における標準化の概要

### 4.3.1. IC カードにおける標準化と相互運用可能性の経緯

(1) データ記録用途での標準化と相互運用可能性の確保

国内では、1990 年代には、保健医療分野をはじめとした公共分野において、IC カードに保有者の個人情報を記録し、セキュリティを確保したデータの読み書きを行う使用方法での情報化について研究がなされ、広域で共通に利用可能な、IC カードのコマンド仕様及びデータの記録形式の標準化が検討された。

コマンド仕様については、国際標準化以前、NTT データを中心とした国内関連企業 16 社によって、汎用に利用できる IC カードの国内共通仕様である「S 型カード」が 1988 年に制定されていた。その後、基本コマンドの国際標準化とあわせて、国内で汎用に利用可能な IC カードの標準として、国際標準に基づく JIS 規格（JIS X6306）には、必須のコマンドを規定した。また、発行後の IC カード内のアプリケーションの管理に利用されるコマンドを含めた、IC カードの相互運用可能性の確保について、日本 IC カードシステム利用促進協議会（JICSAP）で検討がなされ、国際標準に含まれないいくつかのコマンドを追加し、相互運用可能性を確保可能な実装規約として「JICSAP 仕様　1.0 版」を 1996 年に制定、翌 97 年に公開された[10]。

一方、データの記録形式に関する検討結果は「保健医療カードシステム標準化マニュアル（財団法人　地方自治情報センター）」等に整理された[11]。また、IC カード内に記録されているデータの相互読み出しを実現するため、財団法人ニューメディア開発協会により、クライアントに導入されるミドルウェアとして、内容アクセスマネージャ（CAM, Content Access Manager）が、保健医療分野や自治体による公共サービスの分野等で幅広く用いられた[12]。

このように、コマンドとデータの記録形式についてそれぞれ標準化を図ることにより、公的な分野でカード保有者の情報を記録・管理する IC カードの相互運用可能性を確保することができた。具体的には、IC カードに記録された保健医療情報のうち、救急情報については、お互いの地域で互いに読み合うことができ、一方医療情報は特定の地域でのみ読み出すことができる、といったような条件での運用が可能になった。また、JICSAP 仕様を規定することにより、システムで利用する IC カードとして、いずれのカードベンダから調達した IC カードでも利用できるようになった。

(2) IC カードの多様化

その後、IC カードコマンドに関する国際標準化の進展、非接触 IC カードの普及、カード内にアプリケーションプログラムを追加できるプラットフォーム型 IC カードの登場といった、IC カードに関する技術の進展にあわせて、2003 年には JICSAP 仕様第 2.0 版を公開している。ここでも、ISO/IEC 7816 シリーズで規定されている多くのコマンドのうち、相互運用を考慮

した際に必要と考えられるコマンドを抽出して、実装規約として整理を図っている。一方で、セキュリティ分野での IC カードコマンドは、IC カードの CPU、メモリ等の性能によって実装できる範囲が異なることなどから、JICSAP 仕様第 2.0 版では、コマンド機能を必須とせず、オプション機能の扱いとしている。したがって、JICSAP 仕様第 2.0 版を利用して、カードエッジインタフェースでの IC カードの相互運用可能性を確保するためには、単にこの仕様を参照するだけでは不十分であり、利用するコマンドの範囲を規定する必要がある。

### 4.3.2. IC・ID カードに関する標準化の現状

(1) IC カードの標準化動向

IC カードの物理的インタフェースとコマンドについては、国際標準と JICSAP 仕様第 2.0 版に抽出されるコマンド仕様はある程度定められている。

この中では、物理的な接続方法、通信の制御方法、データの読み書きを中心とした低機能のコマンドは、標準化がなされているといえる。

一方で、IC カード内のデータの記述方法は、原則として自由である。国内の公的分野で、カード保有者の情報を記録して携帯する IC カードにおいて、データの記録方法の標準化がはかられたが、IC・ID カードの分野ではそのような取組みは見られない。

IC･ID カードの相互利用には、カード内に記録された認証用データを読み合う必要がある。現在のままでは、それぞれのカードの認証用データを読むためのミドルウェアを別途調達する必要が生じる。

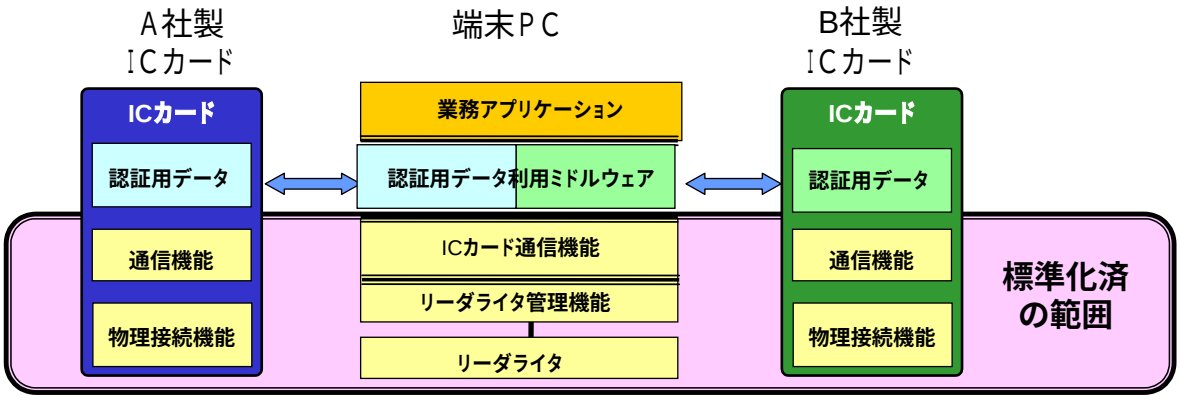



**図 9　IC・ID カードに関する標準化の現状**

(2) 公的分野における連携 IC カード技術仕様

公的分野で発行される IC カードについては、公的分野における IC カードの普及に関する関係府省連絡会議での申し合わせによる「公的分野における連携 IC カード技術仕様」が定められており、行政機関が自ら IC カードを発行する際には、表 4 に示す「必須仕様」に定めら

れた各種コマンドを利用しなければならない[13]。

**表 4　公的分野における連携 IC カード技術仕様　必須仕様に定義されているコマンド**

| コマンド分類 | 必須仕様に定められたコマンド | 準拠仕様 |
|---|---|---|
| 照合･認証系コマンド | VERIFY<br>GET CHALLENGE<br>EXTERNAL AUTHENTICATE | JIS X 6306:1995 |
| レコードアクセス系コマンド | READ RECORD(S)<br>APPEND RECORD<br>UPDATE RECORD | JIS X 6306:1995 |
| | WRITE RECORD<br>ERASE ALL RECORDS<br>UPDATE RECORD | :JICSAP Ver2.0: 2001 |
| 鍵ファイル管理運用コマンド | UNLOCK KEY<br>CHANGE KEY | JICSAP Ver1.1: 1998 |
| | または<br>CHANGE REFERENCE DATA<br>RESET RETRY COUNTER | JIS X 6300-8:2001 |
| PKIコマンド | COMPUTE DIGITAL SIGNATURE<br>VERIFY DIGITAL SIGNATURE<br>VERIFY CERTIFICATE | JIS X6300-8:2001 |

これらのコマンドにより、IC・ID カードでの PKI を利用した認証および署名のサービスに対しては、同一のコマンドが利用可能である。

しかしながら、これらは、行政機関が自ら発行する IC カードに関する申し合わせである。公的分野のサービスに利用する IC カードであっても、民間機関が発行する IC カードには適用されない。そのため、たとえば電子入札コアシステに利用するため、企業に対して民間の認証局が発行する IC・ID カードでは、必ずしもこれらのコマンドが適用されているとは限らない。

(3) IC・ID カードの認証用データに関する標準化の現状

公的分野における連携 IC カード技術仕様では、コマンドについては標準化がなされているが、クライアント環境に導入されるミドルウェアや、IC・ID カード用途の場合、カード内に記録される認証用データのデータモデルについては、規定されていない。

認証用データを扱うミドルウェアは、予め設定された読み方でしか IC カード内の認証用データを読むことができない。したがって、図 10 に示すように、利用者認証機能が標準化され

ていない場合、複数種の IC カード内認証用データへ対応するには複数のミドルウェアが必要になる。

したがって、公的分野における連携 IC カード技術仕様に沿って IC・ID カードが調達された場合、どの企業から調達したカードにも同じ認証用データを搭載できる可能性はあるが、発行された IC・ID カードの間での認証用データの相互運用可能性については、考慮されてはいない。

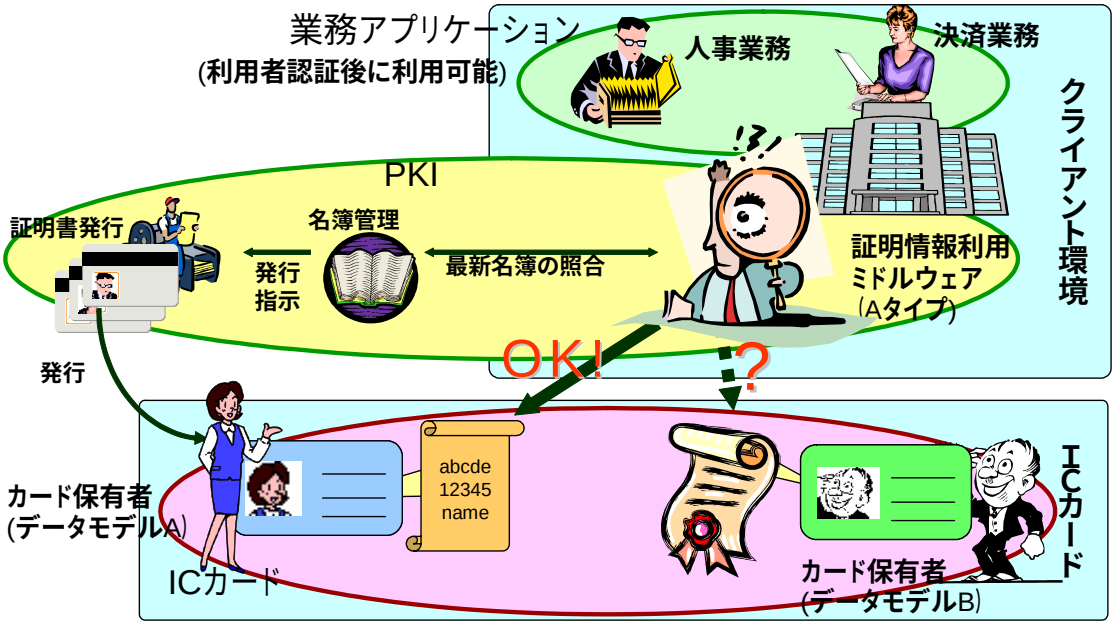



**図 10　データモデルの違いによる IC・ID カードアクセス可否**

国内で個人向けに広く発行されている IC・ID カードである公的個人認証では、複数の調達者が調達した IC・ID カードをクライアントで利用可能な環境が実現されている。すなわち、

- どの市町村がどのベンダから調達した住民基本台帳カードでも、公的個人認証サービスの認証用データを扱うことができる
- 多くの市町村の住民基本台帳カード上の IC･ID カードが、公的個人認証に適した多くのリーダライタで互いに利用可能である。
- クライアントアプリケーションインタフェースは公開されており、公的個人認証サービスを利用した新たな公的分野のアプリケーションを迅速に開発することができる

ただし、公的個人認証の IC・ID カードについて、認証用情報や IC カードコマンドは公開していない。セキュリティの観点から公開しないことにしているとのことである。

なお、公的個人認証の政策的な位置づけから、認証局による証明書検証は、民間用途には開放されていない。

# 5. 国内での IC・ID カードの導入動向

国内での IC・ID カードの導入動向について相互運用可能性の向上の観点から整理する。

## 5.1. 導入されている IC・ID カードの種類と動向

国内では、これまで、公的個人認証 IC カード、電子入札、電子申請等の分野で、IC・ID カードが発行されてきている。また、医療分野や大学の、セキュリティの厳格な管理を必要とする情報システムを取り扱う分野で、IC・ID カードを導入することによって高いセキュリティを確保しながらネットワークを通じたサービスの導入による生産性の向上やサービスの高度化が検討されている。

### 5.1.1. 公的個人認証

(1) IC・ID カードの目的・用途

行政手続きをオンラインで実施する際に、氏名、住所、性別、生年月日を証明する電子証明書を利用して、手続きを行った者の本人確認を実現する。

電子証明書は、住民が居住する市町村の窓口で都道府県知事により発行され、手続き書類への電子署名を行うのに利用される。

なお、民間の認証業者に配慮し、公的個人認証サービスの署名検証に際して証明書の有効性を確認できる者は、行政機関に限定されていた。しかしながら、代理申請が通例の手続きや、添付書類を必要とする手続きに支障を与える恐れがあることから、平成 18 年 11 月 1 日より、司法書士、行政書士等の行政手続等の代理を行う者や、公証人、医師等の行政手続等に必要な添付書類を発行する者が、連合会等の所属団体を通じて有効性を確認する際にも利用できるよう、拡大されている。また、金融機関等本人確認法の省令及び外国為替法の省令を改正により、金融機関の口座開設時等における本人確認にも、用いることができる[14]。

このように、公的個人認証サービスの用途は、住民の利便性向上と、民間の認証サービスへの配慮の両立を図りながら、公的な分野や法律に基づく手続きを中心に、範囲の拡大が検討されている。

(2) IC･ID カードの調達と発行

現在のところ、公的個人認証サービスの認証用データの保存は、住民基本台帳カードに限られる。

市町村が発行した住民基本台帳カードの交付を受けた住民が、市町村の窓口にて公的個人認証サービスの証明書の発行を受けることが出来る。

具体的には、申請者が市町村の窓口にある鍵ペア生成装置を用いて鍵ペアを生成し、公開鍵を都道府県認証局に登録し、公開鍵証明書の発行を受ける。申請者の住民基本台帳カードには、プライベート鍵と公開鍵証明書が記録される。

住民基本台帳カードは市町村ごとに調達されており、複数のベンダから調達されている。非接触（ISO/IEC 14443 TypeB）のインタフェースを必須としているが、端子（ISO/IEC 7816）のインタフェースを合わせて持つカードも多い。

なお、本来ならば、住民が IC カードを持参して居住する市町村の窓口に認証用データの登録を申請した際に、住民が持参した IC カードは、認証用データを登録することのできる IC カードとしての機能、性能を持ち、正しく持参者に発行されたものであることを、確認する必要がある。しかしながら、現在は、公的個人認証サービスの認証用データは、住民基本台帳カードにのみ、また、住民基本台帳カードを発行した市町村の窓口にて登録されるため、認証用データを登録する際には、自らが発行した住民基本台帳カードであることを確認詩さえ刷ればよく、事実上、IC・ID カードが必要な機能・性能を持つものであることを確認する必要は生じていない。

将来、認証用データを登録可能な IC・ID カードの範囲を広げる場合には、住民が持参した IC カードへの認証用データの登録可否を判断する方法を確立する必要が生じる。

(3) 利用環境

公的個人認証は、主として住民の自宅からネットワークを通じて行政手続きを行う際に利用される。そのため、利用する住民は、個人で所有する PC に、公的個人認証の IC・ID カードを利用する環境を整備する必要がある。具体的には、リーダライタを接続し、リーダライタ用のソフトウェア及び公的個人認証サービスの利用者クライアントソフトウェアをインストールする。

利用できるクライアント PC は、Microsoft 社製 OS に限られていたが、Apple 社製 OS でも使えるよう開発と試験が進められている。

リーダライタは、複数のベンダから提供されており、住民基本台帳カードとリーダライタのベンダの間で、公的個人認証サービスに対応した利用者向けＩＣカードリーダライタの適合性検証が行われている。そのため、住民基本台帳カードの仕様の違いによっては若干利用できない機種もあるが、それぞれの市町村から発行された住民基本台帳カードに多くのベンダから提供されているリーダライタを利用することができ、多くの場合に、住民が引越しをして、引越し先の市町村で住民基本台帳カードと公的個人認証サービスの電子証明書を新たに発行を受けた場合でも、従来利用していたリーダライタをそのまま利用できる。

(4) 仕様の公開状況

公的個人認証サービスについて、利用者クライアントソフトの上位アプリケーション、すなわちクライアントアプリケーションインタフェースが公開されている[15]。したがって、行政

機関は､公開されている情報を用いて公的個人認証サービスを利用した業務アプリケーションを開発することができる。

リーダライタインタフェース、カードエッジインタフェース、データモデルは、セキュリティの観点から公開されていない。ただし、カードエッジインタフェースは、公的分野における連携ＩＣカード技術仕様の基礎になっており､国際標準への準拠が考慮されたものであることが想定される。

### 5.1.2. 国家公務員 IC カード

(1) IC･ID カードの目的・用途

各府省職員の身分証明書として 4 万枚、通行証として 6～7 万枚の発行を見込んでいる。当面は、全府省共通で、建物入口ゲートや特定ゾーン入口扉等の IC カードリーダにかざすなどで職員等の確認を行い、通行可否を判断する用途に利用される。その他、各府省独自のアプリケーションや共通のアプリケーションを追加可能とする。

現在のところ、職員の認証に PKI を使用する方針はなく、いずれの府省から発行している国家公務員 IC カードも、IC・ID カードではない。

総務省行政管理局では、全国の国家公務員 45 万人（80 万人から特別職を除いた職員 30 万人と非常勤職員等)、の利用者認証情報とパスワード、所属、官職、氏名、職員番号等を一元的に管理し、ネットワークを通じた業務アプリケーションへの主体認証を実施する、職員等利用者認証基盤の検討を進めているが、現在のところ職員の ID の一元化が大きな課題であり、また、主体認証の手段についても、職員等利用者認証基盤が全府省に共通で提供する方法としては、当面 ID とパスワードのみとしている。

IC カードに新たなアプリケーションを追加することもできる。追加方法は各府省の調達仕様による。

(2) IC・ID カードの調達と発行

IC カードは、府省ごとに調達される。公的分野における連携ＩＣカード技術仕様に沿った技術仕様で調達が行われ、また、入退管理システムのための IC カード内アプリケーションの仕様は全府省共通で定められている。

(3) 利用環境

入退管理システムは、各府省の入館ゲートや、より厳密に入室許可者を管理するエリアの入口などに設置される｡無効なカードに関する情報を共有する方法についても全府省共通の仕様を定めている。

(4) 仕様の公開状況

関係府省連絡会議での検討内容について、概要は公開されている。

IC カードの仕様は、セキュリティに係わる部分も含めて一式が一冊になっているため、供給者（入札参加希望者）と NDA（Non-Disclosure Agreement：秘密保持契約）を結んで情報提供を行っている。IC カードの納入を希望する企業には、入札に際して NDA 締結の上で仕様を開示するため、調達先が限定されるとは考えていないようである。また、IC カードが利用される範囲は庁内に限られるため、詳細な仕様の公開や国際標準への厳密な準拠を考慮する必要性はないとの判断がなされていると考えられる。

### 5.1.3. 電子入札コアシステム

住民個人からの行政手続きには公的個人認証サービスが利用されるが、法人からの申請、申告、調達には、あらゆる手続きに共通に利用される IC・ID カードはない。電子署名が付与された文書にて手続きを実現するためのシステムとしては、電子入札・開札システム、電子入札コアシステム、電子申請受付等システム、電子申告・納税システム等が開発され、それぞれが利用可能な電子証明書を指定している。電子証明書の格納媒体を IC カードに限定しない行政機関もあり、あらゆる行政手続きに利用可能な IC・ID カードは、明確に示されていない[16]。

以下に、法人からの行政手続きに利用される IC・ID カードの一例として、電子入札コアシステムについて記述する。

(1) IC･ID カードの目的・用途

電子入札コアシステムを利用して官公庁への入札を行う企業に発行され、企業名と担当者名が合わせて登録されている。入札に際して、電子署名を付与するために利用される。

電子入札コアシステムは、国土交通省の電子入札システムをベースに、財団法人日本建設情報総合センター（JACIC）における電子入札コアシステム開発コンソーシアムが主体となって開発したもので、平成 18 年 10 月までに中央省庁の 8 機関、公社、機構等 2 団体、都道府県 36 団体、政令指定都市 12 市、その他市町村 367 団体で導入・運用されている[17]。

IC・ID カード用にクライアント環境に導入されるドライバの上位インタフェースが他のシステムのクライアントアプリケーションインタフェースと合致する場合には、電子入札コアシステム以外の、電子申請や電子申告等の行政手続きにも使用できるものがある。すなわち、IC・ID カードが電子入札コアシステム以外の行政手続きに使用できるか否かは、発行したベンダごと、また他の行政手続きのシステムごとに事情が異なる。

(2) IC・ID カードの調達と発行

電子入札コアシステムに応札する企業は、電子入札コアシステム開発コンソーシアムに対応する民間認証局から IC・ID カードの発行を受けて、入札を行う。

民間認証局は、IC・ID カードと合わせて、電子入札コアシステム関連ソフトウェアを配布し、入札する企業は、自社のクライアント環境に導入する。

(3) 利用環境

電子入札コアシステムに入札する企業のクライアント環境としては、Windows の特定のバージョンが指定されている。さらに、民間認証局によっては、発行する IC・ID カードの動作環境として更に特定の OS を指定する可能性もある。利用環境は、電子入札コアシステムが稼動する Windows のバージョンの中で、認証局が発行する IC・ID カードが動作可能な環境、と整理される。

(4) 仕様の公開状況

電子入札コアシステムの仕様は、行政機関にシステムを導入するベンダや、IC・ID カードを発行する民間認証局には開示されているが、一般には公開されていない。

IC・ID カードの仕様は特定されておらず、電子入札コアシステムのクライアントアプリケーションインタフェースに合わせた IC・ID カード及び関連ソフトウェアを民間認証局ごとに提供する。民間認証局では、電子入札コアシステム関連ソフトウェアとして、自社が発行する IC・ID カード用のミドルウェア（ドライバ）の上位に、ラッパーと呼ばれるソフトウェアを追加して、電子入札コアシステムのクライアントアプリケーションインタフェースに適合させている。

### 5.1.4. 国立大学における認証基盤

国立大学には、学内ネットワークの認証基盤として IC・ID カードを導入している大学がある。また、国立情報学研究所を事務局として、大学の PKI 間での連携を図るための UPKI のとりくみが行われている。

(1) IC・ID カードの目的・用途

東京工業大学では、学内ネットワークを通じた各種システム利用時の本人確認にのための認証基盤として、IC・ID カードが導入されている[18]。SSL のクライアント認証を利用することとしており、電子署名を付与する用途は導入していない。

また、PKI 以外の IC カード内アプリケーションも設定されており、暗証番号の照合でカード保有者の ID を読み出す機能によって証明書の交付や図書館での貸し出しを行ったり、非接触インタフェースによる建物の入館管理を行う業務アプリケーションも提供されている。

UPKI に参加している大学では、学内ネットワーク利用時のシングルサインオンや、電子文書への署名、セキュリティを確保する領域への入退管理が検討され、一部実験や導入がなされている。

(2) IC・ID カードの調達と発行

東京工業大学では、常勤職員、非常勤職員、学部学生、修士学生、博士学生、各種研究生、客員研究員、建物管理者等の様々な関係者に、合計 16,000 枚の IC カードが発行されている。IC カードの発行に当たり、本人の確認を行う必要があるが、身分証明書発行のプロセスを利用して行っている。

(3) 利用環境

東京工業大学では、IC カードリーダによる認証が利用できるクライアントは、現在 Windows と一部の MacOS に限られる。ドライバソフトはベンダーから供給される必要があるため、ベンダーのサポート範囲でのみ利用可能となる。

実験を行っている大学には、Windows、 Mac OS、Linux のいずれの環境でも動作することを求めた大学もあるが、提供できるベンダが限られることになっている。

(4) 仕様の公開状況

東京工業大学の IC・ID カードにおいて、認証用データのファイルフォーマットは独自のものであるが、ドライバソフトを通じた上位アプリケーションとのインタフェースは PKCS#11 及び CSP に対応している。今後学内で開発するシステムでの利用者認証は、PKCS#11 あるいは CSP をインタフェースとし、学内では共通の基盤として利用される。

認証データのデータモデルについては、ベンダ側が権利を持っており、東京工業大学の判断で公開できない。

### 5.1.5. HPKI

(1) IC・ID カードの目的・用途

厚生労働省のヘルスケア PKI は、以下の 2 点を目的とした署名用証明書（ISO/IEC17090 のサブセット、自然人のみ対象）のためのフレームワークである。

①資格を持っていることを本人認定と同時に確認するもの

②医療機関の管理者であることを確認するもの

HPKI を利用して実現されるのは、医療分野の各種サービスの電子化、オンライン化である。具体的には、以下のような文書の発行と利用が考えられる[19]。

- 医療受給者が作成する文書 （外来予約、入院承諾書、手術承諾書、カルテ開示要求等）
- 医療供給者が作成する文書 （診療情報提供書、診断書、処方箋、診断レポート、外注検査依頼等）
- 機関が作成する文書 （検査結果報告、診療報酬請求、各種届出、各種統計調査、診断書要求、保険資格確認等）

全省庁で医師による証明がなされた添付文書が必要な申請は 140 程度ある。これを電子申請化したとき、医師資格証明のための電子署名でどのような確認ができれば有効性が担保されるのかが議論されている。

医療機関の従事者、専門家のみが IC・ID カードを持つのではなく、患者側の IC・ID カードとあわせて活用すれば、保健医療関連の情報を個人と医療機関が共有し、相互の活用で健康増進を推進するような取組みにも活用されることが期待できる。ただし、この方法で患者が保有する IC・ID カードについては、公的個人認証でよいのか、別途いずれかの機関が発行する必要があるのかも含めて、まだ検討されていないようである。

(2) IC・ID カードの調達と発行

平成 18 年度には、全国の HPKI 認証局のルート認証局となる「厚生労働省 HPKI 認証局」が構築される見通しである。厚労省 HPKI 認証局は、共通ポリシーに準拠した個別認証局あるいはその中間認証局に対し、相互認証を可能とする仕組みを提供する。当面は、日本医師会 CA 及び医療情報システム開発センターCA を個別認証局として実証を行う予定である。

HPKI の認証用データは、個別認証局より、保健医療福祉分野サービス提供者及び利用者に対してのみ発行される。なお、その提供者である以下の者はその資格、役割を証明書内に記載することができる。

- 保健医療福祉分野に関わる国家資格所有者
- 医療機関等の管理者

また、証明書の用途は、

①医療従事者等の保健医療福祉分野サービス提供者の署名検証用

② 患者等の保健医療福祉分野サービス利用者の署名検証用

に限定される[20]。

(3) 利用環境

医師等の資格は、保健医療分野の公開鍵基盤の技術仕様書である ISO/IEC17090 に定められた電子証明書の local extension を利用して記録されている。そのため、証明書を検証するためには、一般に提供されている証明書検証モジュールのみでは不十分であり、HPKI の専用検証モジュールを利用する必要がある。

利用者側のクライアント環境としては、2 点の問題が指摘されている。医療機関では、ネットワーク周りのセキュリティが重視されており、院内 LAN は、外部のネットワークに接続し

ないことを基本となっている場合が多い。一方、署名の検証には認証局との接続が必要になるため、インターネットと院内 LAN の接続方法が問題になる。当初は、HPKI を利用した紹介状の作成や検証を、診療室ではなく、地域連携室のようなところで行うことになることが考えられる。

また、HPKI の用途として、電子カルテシステムとの組み合わせが期待されているが、現在広く普及している電子カルテのシステムには、クライアント環境が Windows であるものとあわせて、Linux であるものがある。医師が複数の医療機関に勤務する場合があることを踏まえれば、HPKI で用いられる IC・ID カードは、Windows 環境と Linux 環境双方で使用できることが求められる。

(4) 仕様の公開状況

厚生労働省は「保健医療福祉分野 PKI 認証局 証明書ポリシー」(CP：Certificate Policy)を作成、公開している。CP には、証明書フォーマットや、認証局の方針などが記されている。hcRole として、医療関係者の資格属性を格納する証明書フォーマットを、ISO/IEC 17090 に準拠して定めている。

この中で、認証用データの保存場所は、US FIPS 140-2 レベル 1 と同等以上の規格に準拠する、耐タンパ性を持つ媒体であることが求められているが、IC カードに限定されてはいない。ただし、現在までの段階では、日本医師会 CA 及び医療情報システム開発センターCA とも、IC カードで認証用データを発行している。

また、保存媒体の内部での格納方法については定められていないため、CP では、IC・ID カードのデータモデルやカードエッジインタフェースについて何ら規定されない。

保健医療福祉情報システム工業会（JAHIS）は、工業会の立場として、HPKI で共通に採用すべき、IC カードシステムの標準的なフレームワークを検討している。この中では、カードエッジインタフェースだけでなく、認証用データのデータモデルについても、ISO/IEC 7816-15 に準拠した標準化を行う方向で検討を進めている。ガイドライン制定後は各方面に提供し、IC カードを発行するサービサーや IC カード製造ベンダに準拠していただくよう働きかけを行うようである。

## 5.2. 相互運用可能性にかかわる現状

### 5.2.1. 調達時の考慮

現在導入されている IC・ID カードシステムにおいて、導入された IC・ID カードが相互運用される可能性の考慮状況について表 5 に整理する。特徴としては、以下のようなことが挙げられる。

- 公的個人認証では、国や地方の各種手続に広範に利用できる基盤とすることを当初から想定していたこともあり、仕様の標準化が図られ、IC･ID カードが調達される市町村間、認証用情報

が発行される都道府県間で、相互運用可能性が確保されている。ただし、国際標準への準拠は明示されていない。また、他の種類の IC･ID カードカードとの相互運用可能性は考慮されていない。

- 電子入札コアシステムでは、IC･ID カードサービスのインタフェースを規定してはいるが、他の電子的な手続きとの間での相互運用可能性を考慮したものとはなっていない。また、IC･ID カードの相互運用可能性については、考慮されていない。
- HPKI では、IC･ID カードの相互運用可能性を確保する必要性が課題として顕在化しており、当初より国際標準も視野に入れた検討を行っている。

**表 5　IC・ID カードの仕様における相互運用可能性への配慮**

| | 公的個人認証 | 国家公務員※1 | 電子入札コア | 国立大学 | HPKI※2 |
|---|---|---|---|---|---|
| (1)複数クライアント環境 | Mac OS 対応は遅れているが整備中 | 調達府省次第として考慮せず | クライアントは Windows に限定 | Mac OS は一部のみ対応 | Windows と Linux 双方への対応必須 |
| (2)1 枚を複数用途 | クライアントアプリケーションインタフェースを公開して幅広い行政手続きに利用 | IC カードにアプリケーションを追加可能としている | クライアントアプリケーションインタフェースを認証業者にのみ公開、他の業務は考慮せず | 学内での認証インフラとしてクライアントアプリケーションインタフェースを整備 | 将来に向けて様々な用途が検討されており、クライアントアプリケーションインタフェースを検討 |
| (3)1 環境で複数のカード･用途 | 考慮していない | 考慮していない | 考慮していない | 対応しきれずカードを全て発行しなおし | 電子申請等との共存が必要になるか |
| (4)1 環境に複数種のカード | 複数市町村のカードを利用 | 入退館では全府省のカードに対応必須 | 考慮していない | 考慮していない | 患者カードとの組み合わせ利用を検討 |

※1　現在のところ、IC･ID カードとして発行されていない

※2　本格的な導入･普及の段階には入っていない

### 5.2.2.　標準化及び仕様公開の状況

現在導入されている IC・ID カードシステムにおいて、技術要素やインタフェースごとの標準化、公開状況について表 6 に整理する。特徴としては、以下のようなことが挙げられる。

- クライアントアプリケーションインタフェースは統一されており、IC･ID カードサービスの複数社からの調達、あるいは、IC･ID カードを本人確認用の基盤として、今後複数の業務アプリケー

ションの開発を可能としている。

- 電子入札コアシステムや国立大学では、IC･ID カードサービスとして IC･ID カードとミドルウェアがセットで提供されているため、他社製の IC･ID カードあるいはその他の IC カードとの共存が困難であることが懸念される。
- HPKI では相互運用可能性への要求がすでに顕在化しているため、標準化や公開の可能性があると考えられる。

**表 6　IC・ID カード関連仕様の標準化及び公開の状況**

| | 公的個人認証 | 国家公務員※1 | 電子入札コア | 国立大学 | HPKI※2 |
|---|---|---|---|---|---|
| 業務アプリケーション開発 | 行政機関が任意に開発可 | 府省ごと自由に可 | コアシステム専用 | 各種を開発して接続予定 | 各種を想定して検討中 |
| クライアントアプリケーションインタフェース | 複数種の開発言語用を公開（PKCS#11, CSP 等） | 入退管理のみ統一。公開されていない | 統一されているが公開されていない | 認証用のインタフェースを整備（PKCS #11, CSP） | 公開あるいは開示の見通し |
| ミドルウェア機能 | 統一されているが公開されていない | 入退管理のみ統一 | 認証局別にカードとセットで提供 | ベンダ独自仕様 | 認証局別に検討中 |
| リーダライタインタフェース | 統一されているが公開されていない | 入退管理のみ統一 | 認証局別にカードとセットで提供 | ベンダ独自仕様 | 認証局別に検討中 |
| カードエッジインタフェース | 統一されているが公開されていない | 入退管理のみ統一 | 認証局別にカードとセットで提供 | ベンダ独自仕様 | 標準化を睨みガイドライン検討中 |
| データモデル | 統一されているが公開されていない | 府省ごと独自、PKI ではない | 認証局別にカードとセットで提供 | ベンダ独自仕様 | 標準化を睨みガイドライン検討中 |

※1　現在のところ、IC･ID カードとして発行されていない

※2　本格的な導入･普及の段階には入っていない

## 5.3.　各主体の現状と課題

それぞれの導入例や供給者の現状にもとづき、IC・ID カードを取り巻く各主体の現状と課題について、以下に概括する。

### 5.3.1. 仕様策定者

公的分野での IC・ID カードの調達・導入は、政府の「行政（国・地方公共団体）内部の電子化、官民接点のオンライン化、行政情報のインターネット公開・利用促進、地方公共団体の取組み支援等を推進し、電子情報を紙情報と同等に扱う行政を実現し、幅広い国民・事業者の IT 化を促す」（「e-Japan 戦略（要旨）」より）方針に基づいて実施されてきている[21]。この目的に鑑みれば公的分野で IC・ID カードが調達される際には、単に当該サービスにおいて特定の供給者だけが IC・ID カードを供給できるような仕様を回避するだけでなく、幅広い国民・事業者の IT 化の先鞭となるべき取り組みとして実施され、検討された仕様が行政のみならず民間においても、幅広く利用できるような仕様を定め、普及が図られるべきである。

しかしながら、ニーズ調査において公的分野での IC・ID カード導入に関わるさまざまな関係者へのインタビューを行った結果、自らのサービスのために策定した仕様を IC・ID カードの標準仕様として公共、民間を問わず幅広く活用させようという意図を示した仕様策定者、供給者等はなく、それぞれの IC・ID カードの仕様は一般には開示されていない。電子申請や電子調達の分野では、クライアントアプリケーションインタフェース、カードエッジインタフェース、データモデルについて、同一の仕様を応用して相互運用を図ることが可能と考えられるが、公開を通じた標準化などは図られていない。

逆に、IC・ID カードに関して、データモデルからクライアントアプリケーションインタフェースまでが揃っており、複数の企業からの調達が可能な公開された仕様が存在しないため、使用策定者は、自ら実現しようとするサービスのために、仕様を検討しなければならない状態にある。

ただし、IC・ID カードの相互運用可能性を考慮する必要が明らかになっている事例は少ないため、クライアントアプリケーションインタフェースを定めて IC・ID カードを供給しようとするベンダに開示すれば当該サービスの実現は可能といった事態が多い。例えば、電子入札コアシステムでは IC・ID カードを保持する企業（入札企業）は、電子入札するための社内のクライアント環境で、特定の供給者からの IC・ID カードで入札できる環境が整備できればよいと考えられる。

### 5.3.2. 調達者

現在の IC カードには、ベンダを超えて「この仕様で買えばどこでも使える」製品がない。そのため、使用策定者が策定した仕様に準拠した IC・ID カード及びミドルウェアは、個別に供給者から調達する必要がある。また、各社のカードエッジインタフェースは非公開であるため、ミドルウェアはカード別に調達する必要がある。

調達した IC・ID カード及びミドルウェアをカード保有者に提供するにあたっては、多くの場合、カード保有者に対して、同一のクライアント環境で他社製の IC・ID カードを利用しないよう求める必要が生じる場合が多い。

そのため、何らかの理由で従来と異なるベンダから IC・ID カードを調達する必要が生じた

場合には、クライアント側のミドルウェア及び IC・ID カードを全てと交換する必要が生じる場合がある。

上記のような状況になっている原因としては、IC・ID カードに関するカード・ミドルウェアの標準化・公開がなされていないことが挙げられる。

### 5.3.3. 利用者

利用者にとっては、業務アプリケーションを実現することが重要であり、IC・ID カードは利用者認証を実現するための一連のサービス、すなわち IC・ID カードサービスとして捉えられる事が多い。

IC・ID カードに求める認証内容が既に発行されている IC・ID カードと同一であり、また自身が提供しようとする業務アプリケーションに発行されている IC・ID カードを利用できる場合は、発行済みの IC・ID カードのミドルウェアにあわせて業務アプリケーションを開発することになる。

一方、既存の IC・ID カードが利用できない場合は、自らのサービスを実現するために、IC・ID カードを新たに調達する必要が生じる。クライアントアプリケーションインタフェースとして、PKCS#11 や CSP といった汎用インタフェースを利用する場合には、結果的に、比較的多くの IC・ID カードを利用してサービスを提供できる可能性がある。

自らが利用する、あるいは制定したインタフェースに会うミドルウェアがあれば、ミドルウェアから下位のリーダライタ及び IC・ID カードが特定のベンダに固定されてしまっても、短期的には問題が生じないケースが大半である。

しかしながら、長期的には、クライアント環境の多様化や、IC・ID カードの供給先の変更といった事態が生じる可能性がある。この場合に、ミドルウェアから下位が固定されているベンダから供給を受けている場合、新たなクライアント環境に対応するミドルウェアが調達できない、あるいは、複数社製 IC・ID カードを使い分けられるミドルウェアが調達できないといった事態が生じる可能性がある。

### 5.3.4. 供給者

現在までに供給されている IC・ID カードは、ベンダ各社が、主に認証用アプリケーションと対になったカードとして供給してきており、国際標準への準拠や他の IC・ID カードとの相互運用可能性よりも、独自製品としての最適化を優先して開発されている。そのため、IC・ID カードの仕様の策定にあたっては、特定の供給者が供給しやすい IC・ID カード仕様が指定されたり、クライアントアプリケーションインタフェースだけを独自に制定し、供給者に IC・ID カードとミドルウェアの供給を任せるといった方法が採用されたりといったことになる。結果的に、他の仕様策定者が制定した仕様との間での IC・ID カードの相互運用可能性は、確保されることが少ない。

これまで、調達者や利用者からのニーズとしても、個別の用途に限った調達が多く、標準的

な製品を求めるニーズが顕在化していないことから、IC・ID カードの処理能力にも制限がある中、最低限の機能、限定された環境での利用に絞り込んだ機能を搭載する方が、IC・ID カードの性能が確保しやすく、短期的には価格も抑えることができていた。

一方で、IC・ID カードに関わる国際標準化が進んできており、関連するカードコマンドについても、「JICSAP 仕様第 2.0 版」として標準化が図られ、JIS X6319 として国内標準化もなされている。しかしながら、上記のような背景から、国際標準や JICSAP 仕様第 2.0 版に準拠した IC・ID カードは、あまり盛んには製造されていない。同様の機能であっても、アプリケーションに合わせて最適化を図った、独自のコマンドで実現している例が多いとのことである。

そのため、複数社の IC・ID カードの間での相互運用可能性の確保や、複数社から提供されるクライアントアプリケーションで利用するためには、ベンダ間の調整が必要になる。各社は、自社製のミドルウェアのクライアントアプリケーションインタフェースが、仕様策定者が定めるインタフェースと合致しない場合には、インタフェースを整合させるためのソフトウェアを追加提供する場合もある。ただし、クライアントアプリケーションインタフェースとして、PKCS#11 や CSP のインタフェースを具備しているものは、比較的多くのクライアントアプリケーションに対応可能になっている。

顧客側が多種のクライアントでの利用を求めたり、自社が提供したリーダライタとミドルウェアの環境で複数の IC・ID カードを利用したいという要求が現れた場合には、対応に苦慮している。現実的には、ベンダが指定する環境で、自社が提供する IC・ID カードおよびそれによって動作する業務アプリケーションの範囲で、IC・ID カードや IC・ID カード対応業務アプリケーションを導入するよう利用者を促しているようである。

# 6. IC・ID カードの相互運用可能性に関する課題

## 6.1. 要求の整理

従来の IC・ID カードでは、1 枚の IC カードに対して 1 台の PC、1 種のサービスを想定して利用すればよかったため、IC・ID カードの間での相互運用可能性を検討する必要はなかった。

しかしながら、近年、IC・ID カードが、組織横断的に「利用者認証基盤システム」「電子申請システム」「電子署名システム」等での利用者認証に使われる方向に向かっている状況で、相互運用可能性が必要とされる状況が顕在化しつつある。

3 章での整理に基づき、ここでは、IC・ID カードの相互運用可能性を、以下の用途での利用可能性と位置づける。

① 異なるクライアント環境での IC･ID カードの利用
② 1 枚の IC･ID カードの複数用途への利用
③ IC･ID カードと業務アプリケーションの組み合わせを 1 環境で複数種利用
④ 1 種の業務アプリケーションで複数種の IC･ID カードを利用

上記を実現するためには、以下に示すように、IC・ID カードシステムに係わる技術要素が明確に定義される必要がある。

- クライアントアプリケーション、ミドルウェア、IC･ID カードの間でのセキュリティ構造が明確に定義されている
- クライアントアプリケーションとミドルウェアのインタフェースが業界やベンダを超えて標準化され、仕様が公開されている
- ミドルウェアとリーダライタのインタフェースが業界やベンダを超えて標準化され、仕様が公開されている
- カードエッジインタフェースが業界やベンダを超えて標準化され、仕様が公開されている
- データモデルが標準化され、公開されている
- 証用データの記述内容及び電子証明書の検証手順等が標準化及び公開され、どの認証局へも同一の手順で利用可否の確認や電子証明書の検証ができるようになっている。
- 複数のミドルウェアが共存できるよう、ミドルウェアの開発条件が定められ、各ベンダによって遵守されている。あるいは、ミドルウェアとクライアントアプリケーションのインタフェース、データモデル、カードエッジインタフェースのそれぞれが標準化され、仕様が公開されている。

## 6.2. 現状におけるデメリット

### 6.2.1. すでに発生しているデメリット

国内では、IC・ID カードとして分類される IC カードを利用し、PKI によってネットワー

ク経由のサービスを実現する取組みが、下記に挙げられるように複数実現されてきた。

- 公的個人認証サービス
- 商業登記に基づく法人認証制度
- 電子入札コアシステム
- 電子入札･改札システム
- 電子申請システム

これらにおいては、クライアントアプリケーションのインタフェース、認証用データの管理に IC・ID カードを利用する場合の IC カードの仕様等が個別に検討されてきている。標準的なインタフェースを利用しているクライアントアプリケーションと、標準的なインタフェースをサポートしているミドルウェアで稼動する IC･ID カードの仕様がたまたま一致している場合には、たとえば電子入札コアシステム用に発行された IC・ID カードを利用して電子申請システムを利用することができる場合もあるが、一般的に、どの法人用 IC・ID カードであってもどのサービスにも利用できる、という状況にはなっていない。また、IC・ID カードは複数のサービスに利用可能であっても、クライアントアプリケーションが求めるクライアント環境、たとえば JRE (Java Runtime Environment)の種類、バージョンが異なるために、複数のクライアントシステムを使い分けなければならない、といった事態が発生している。

IC・ID カードの普及に伴い、カード保有者の利用環境で IC・ID カードによるサービスを複数利用したいニーズが顕在化してきている。これにより、わずかずつではあるが、個別仕様であることの弊害が現れてきている。すでに現れている弊害について、以下に整理する。

- サービスごとに異なる IC･ID カードを利用する必要があるだけでなく、カードごとにミドルウェアが必要
- 複数のミドルウェアを 1 台のクライアント PC の中で実現できないため、サービスごとにクライアント PC を準備する必要が生じる
- すでに保持している IC･ID カードを新たに提供されるサービスに利用可能か否かが明示されない
- 現在ミドルウェアが提供されているクライアント PC 以外の OS 環境で利用できないため、クライアント PC を買い換えると IC･ID カードも新たに購入する必要が生じる
- 従来 IC･ID カードを発行していたベンダが同じ仕様の IC カードの製造を中止したが、カード間での相互運用可能性を確保できないため、全カードを発行しなおす必要が生じる

### 6.2.2. 今後発生が予想されるデメリット

今後、各種仕様の標準化・公開がなされずに IC・ID カードの普及が進んだ場合は、以下に示すようなデメリットの発生が懸念される。

① 新たな IC･ID カードとの相互運用を行うための開発費が別途発生する
② 業務アプリケーション開発におけるミドルウェアへの依存性が高まる
③ 新たに適用が求められる IC･ID カードに対して迅速に対応できない

以下、それぞれのケースについて解説する。

(1) 新たな IC・ID カードとの相互運用を行うための開発費が別途発生

IC・ID カードを利用してネットワークを通じたサービスを提供しようとする利用者は、通常、特定の IC・ID カードを対象として業務アプリケーションおよびミドルウェアを導入する。

しかしながら、他の調達者から各種の IC・ID カードが提供されるに伴い、サービスの拡大とともに、利用可能な IC・ID カードの対象を拡大する必要が生じる可能性がある。

この場合に、当初より利用している IC・ID カードと、新たに利用しようとする IC・ID カードとの間に相互運用可能性が確保されていない場合、下記に示すような新たな機能の開発が必要になるため、費用と期間を要する。

- 相互運用先 IC カード内の認証用データを扱えるようにするための機能の開発が必要
- データモデルに対応した IC カード内の認証用データを扱う用ミドルウェアを複数管理する機能の開発が必要
- 双方の IC カード開発ベンダや利用者認証システム開発ベンダ間で調整が必要のため相互運用開始までの期間が長期化

IC・ID カードの詳細な仕様が供給者から提示されない場合は、従来利用していた IC・ID カードと異なる供給者による IC・ID カードを同一の環境で利用できるようにするためには、相当な困難を要する場合もある。

上記のような課題は、他種の IC・ID カードとの相互運用において発生するだけでなく、IC・ID カードシステムを長期間利用する過程で IC・ID カードの入替が必要になった場合にも、同様に生じる可能性がある。最悪の場合、カードは全て買い替え、ミドルウェアの入替に併せて業務アプリケーションにも相当の改修が必要になる。

以上について、図 11 に示す。

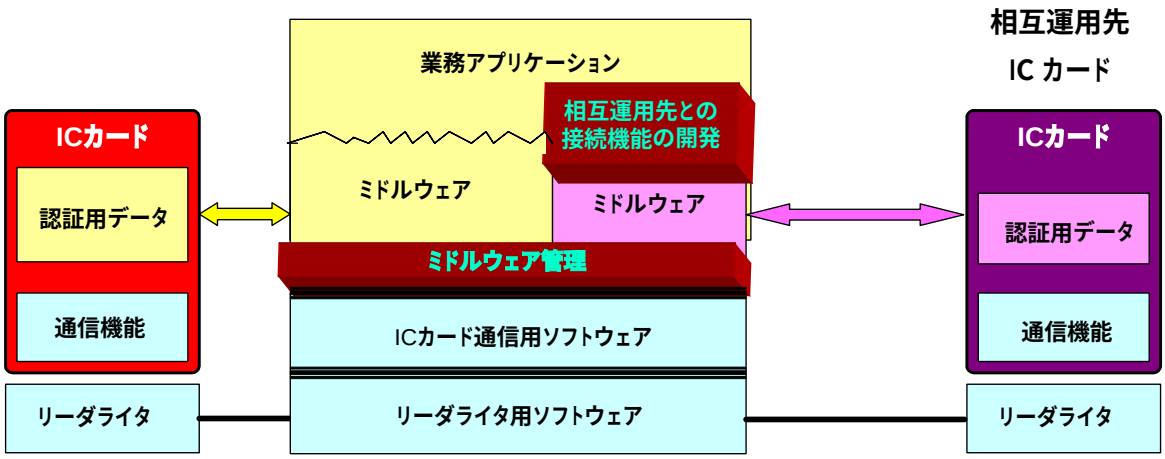



**図 11 相互運用のための開発費の発生**

(2) 業務アプリケーション開発におけるミドルウェアへの依存性が高まる

ネットワークを通じて実施されるサービスは拡大の傾向にある。あるクライアントで IC・ID カードを利用している環境においても、導入後に利用可能なサービスを増やすために、新たなクライアントアプリケーションを調達・導入する必要が生じることが考えられる。

ここで、クライアントアプリケーションインタフェースが標準化されていない場合、ミドルウェアとクライアントアプリケーションのインタフェースは独自の仕様で接続している。この環境で新たなサービスを利用可能とするためには、導入されているミドルウェアが持つ、独自仕様のクライアントアプリケーションインタフェースにあわせて新規のクライアントアプリケーションを開発・導入する必要がある。

ミドルウェアの独自仕様のインタフェースは、多くの場合広範に開示されることはないため、追加導入するクライアントアプリケーションを開発する供給者は、ミドルウェアの供給者との間で秘密保持契約を結んだ上で開発を進めるなどの手順を踏む必要が生じ、また、他の環境に供給するのとは異なるミドルウェアのインタフェースに対応する必要が生じる。ミドルウェアのクライアントアプリケーションインタフェースの独自性が高い場合には、追加導入するクライアントアプリケーションを調達できる供給者が限定される可能性もある。

これによって、下記のようなデメリットが生じると懸念される。

- 開発費が肥大化
- 開発･導入までの期間が長期化
- 独自開発の IC カード内認証用データ用ソフトウェアに依存するため受注できるベンダが限定される

以上について、図 12 に示す。

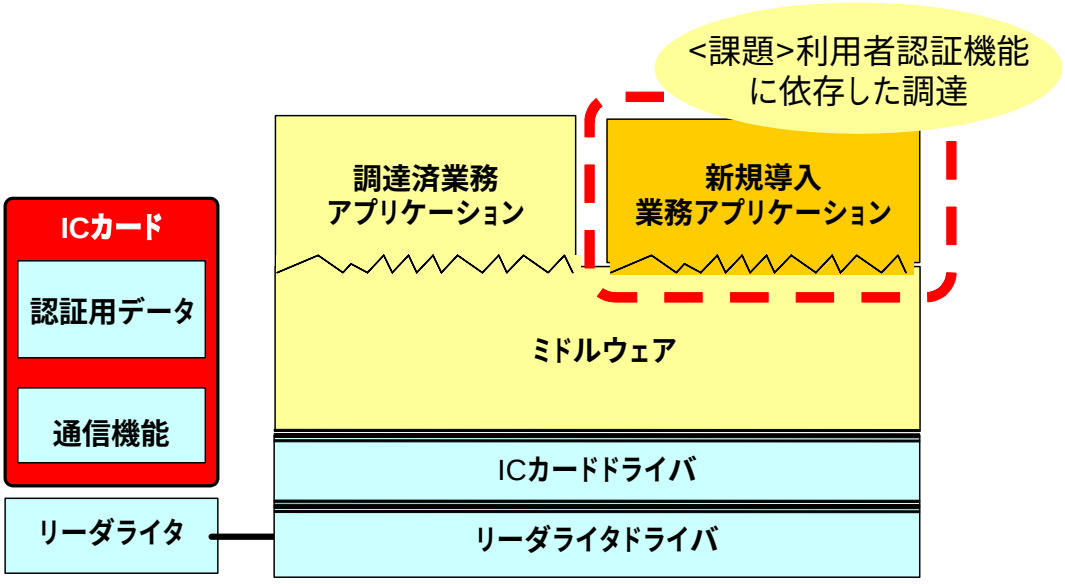



**図 12　業務アプリケーションの開発におけるミドルウェアへの依存**

(3) 新たに適用が求められる IC・ID カードに対して迅速に対応できない

病院や公共機関など、多数の関係者との取引や手続きが行われる環境では、複数の調達者が調達・発行した IC・ID カードを利用してサービスを提供する必要が生じることが考えられる。たとえば医療機関において、医療従事者の IC・ID カード、患者の IC・ID カードが、それぞれの認証機関や保険者によって独自に調達されており、これらを組み合わせてサービスを提供する必要が生じるような場合である。

ここで、それぞれの IC・ID カードを取り扱うためのミドルウェアが標準化されていない場合、新たに発行された IC・ID カードを取り扱うためには、都度クライアントにミドルウェアを導入する必要が生じる。

以上により、下記のようなデメリットが生じる。

- 初期に対応可能なカードが限定的になる
- さまざまなカードに対応したいシステムは、継続的なミドルウェアの追加導入やそれに伴うクライアント環境のメンテナンスが煩雑になる

なお、ミドルウェアのクライアント OS との関係が異なる場合には、ひとつのクライアント環境に複数のミドルウェアを導入して、カード保有者が持参したカードにあわせたミドルウェアが稼動するといった使い分け自体が実現しない危険性もある。

以上について、図 13 に示す。

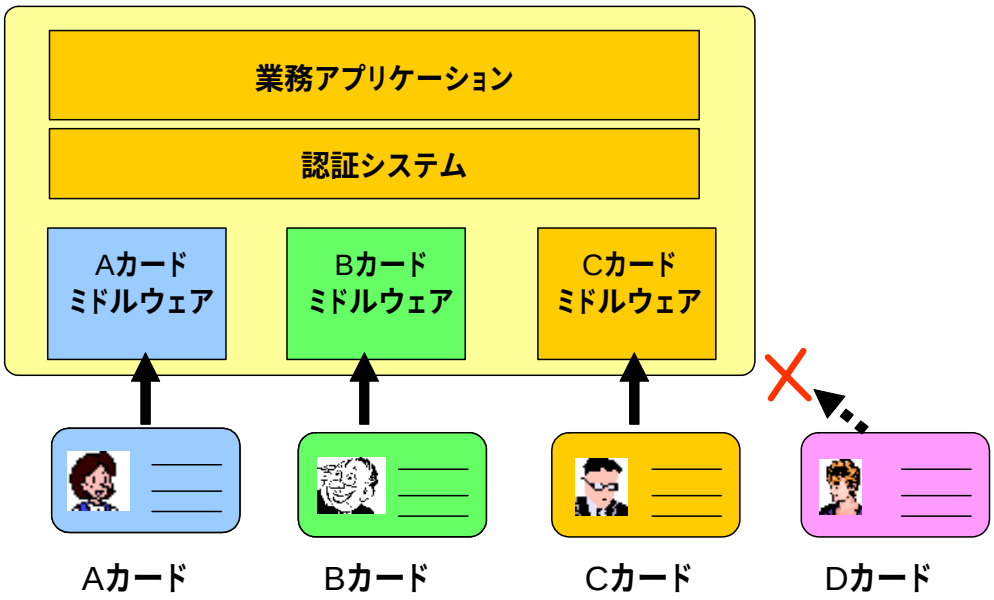



**図 13 新たな IC・ID カードへの対応の遅れ**

## 6.3. 実現していない背景

IC・ID カードの相互運用可能性を向上するためには、各種仕様の体系化、標準化、公開を

図り、準拠製品の普及を図ることが必要である。

しかしながら、これまで、IC・ID カードの分野では、そのような取り組みはほとんど行われておらず、結果的に、3 章に示したような IC・ID カードの相互運用を実現できるような環境にはなっていない。

5 章に示した各主体の現状に基づき、IC・ID カードの相互運用可能性が実現していない背景を、以下に整理する。（これらの解決に向けた支援策を「6.4　普及に必要な技術的支援」で提案する。）

### 6.3.1. 仕様策定および調達の観点

IC・ID カードシステムの導入にあたり、仕様策定者が策定する仕様や調達者が調達する IC・ID カードにおいて、相互運用可能性が配慮されていない背景について、下記に整理する。

(1) 相互運用可能性を確保できる調達仕様が存在しない

4 章に示したように、IC・ID カードに関わる国際標準は、幅広い範囲の IC カードを許容する仕様であるため、これらすべてに対応可能なミドルウェアやリーダライタは提供されていない。したがって、仕様策定者が IC・ID カードの仕様を定めるにあたっては、利用するコマンドやデータモデルを選択・指定する必要があるため、結果的に、それぞれが独自の仕様となる。国際標準に準拠していない IC・ID カードを調達するのと比較しても、相互運用可能性が高いことにはならない。

一方、市場で実績のある IC・ID カードは多くがミドルウェアと一体で供給されており、カードエッジインタフェースやデータモデルが公開されている例は少なく、他の供給者が供給する IC・ID カードの相互運用可能性の確保は困難になるケースが多い。

結果的に、仕様策定者や調達者にとっては、調達仕様書に記載でき、準拠する IC・ID カードを複数のベンダが提供しているような IC・ID カードの仕様が、事実上存在しない。

(2) 相互運用へのニーズ・モチベーションが低い

ニーズ調査において公的分野での IC・ID カード導入に関わるさまざまな関係者へのインタビューを行った結果、自らのサービスのために策定した仕様を IC・ID カードの標準仕様として公共、民間を問わず幅広く活用させようという意図を示した仕様策定者、供給者等はなく、それぞれの IC・ID カードの仕様は一般には開示されていない。そのため、公的分野のいずれかの IC・ID カードの仕様を基準にして広範に相互運用可能性が確保されるといった状況は期待しにくい。

(3) ベンダ間相互運用を求めるサービスの規模が小さい

現在までに導入されている IC・ID カードでは、少しずつ相互運用可能性が確保されていないことによる弊害が現れつつあるが、それぞれに規模の小さな問題として、個別に対処されている。今後導入を予定されている分野でも、たとえば HPKI では、複数の認証局が認証する IC・ID カードの相互運用の必要性、すなわち、IC カードベンダを超えた相互運用可能性が指摘されているが、当初の IC・ID カードの発行対象は、医療機関および従事者合わせた枚数を想定すれば 4 万枚程度であるため、IC・ID カードベンダに対して、相互運用可能な製品の供給を促すには至っていない。

このため､分野を超えて相互運用可能性を確保するための仕様を策定しようという動きが見られず、個別の対応にとどまっている。

### 6.3.2. 製品供給の観点

ニーズ調査の結果、IC・ID カードを供給するベンダの視点からは、現在の状況は、短期的には IC･ID カードの相互運用可能性を向上する動機づけになるような環境ではないことがわかった。その背景について下記に整理する。

(1) 相互運用可能性は既得市場喪失の脅威

IC・ID カードとして利用可能な IC カードは、ベンダ各社が、認証用アプリケーションと対になった機能として、最適化を図り、供給してきている。そのため、他のベンダが供給する IC・ID カードとの相互運用可能性を確保することは、既存市場喪失の脅威として映る。

(2) 技術的難易度が高い

現在各社から提供されている IC・ID カードは、IC・ID カード、リーダライタ、ミドルウェアがセットで提供され、個別に最適化が図られている。

相互運用可能性を向上させるためには、IC・ID カードとリーダライタ、ミドルウェアが互いに異なる場合にも同様に動作する必要がある。しかしながら、IC カードの標準は技術面での許容範囲が広く、同じコマンドであっても、許容範囲に対する解釈の違いによって、特に正常の処理が行われなかった場合に、反応が異なる。これらの相違を克服するには、技術的な困難が大きい。

(3) 市場規模が小さい

HPKI は、単独の市場として捉えた場合、IC カードの発行対象が医療機関および従事者合わせてせいぜい 4 万枚であり、IC カードベンダにとって新たな仕様のカードを開発する対象としては非常に小さい。また、電子入札や国家公務員 IC カードといった他の用途でも、IC・ID カードの複数のサービスへの利用や、複数ベンダが提供したカードの同時利用といった、

相互運用可能性の確保を求める用途は、あまり顕在化してはいない。すなわち、相互運用可能性が求められる IC・ID カードの市場はまだまだ小さく、量的な観点からは、新たな製品を開発するだけの魅力を示してはいないといえる。したがって、IC・ID カードベンダとしては、他社製の IC・ID カードとの相互運用可能性の向上を積極的に追求しようとはしない。

(4) 処理性能の向上が遅れ気味

国際標準に準拠した場合の IC・ID カードの性能が、独自に整備した製品と比較して劣るか否かについては、ベンダによって意見が異なる結果となっているが、相互運用可能性を確保した製品は、各ベンダの製品としては後発である場合が多く、導入実績の面では劣ることが多い。一方で、ユーザの立場としては、短期的には、まだ必要性が顕在化していない相互運用可能性を考慮するよりも、明確になっている用途の範囲で最適な性能が発揮されることを求めることが多い。

## 6.4. 普及に必要な技術的支援

ここまで、IC・ID カードの相互運用可能性が求められる状況が現れつつあり、今後関連サービスの普及によってさらに顕在化する可能性があること、放置すれば、調達者や利用者のデメリットが生じる可能性があるが、現状の延長では相互運用可能性の向上はあまり期待できないことを整理した。

今後、IC・ID カードの導入・利用に伴うデメリットが生じないようにするためには、どのような技術的な環境を整備する必要があり、そのためにそのような支援が必要なのかについて、考察する。

### 6.4.1. ユーザの視点

IC・ID カードのユーザである仕様策定者、調達者、利用者、さらにカード保有者にとっては、IC・ID カードの調達・利用に際して、以下に示すような環境が整備されることが望ましい。

(1) 調達仕様書に利用可能な一般的な仕様が整備されていること

仕様策定者や調達者が、IC・ID カードのカードエッジインタフェースやデータモデルの仕様を自ら検討、制定して IC・ID カードの調達を行うことは現実的ではない。発行しようとする IC・ID カードの用途、設定したいセキュリティ条件に沿った仕様を容易に定義でき、複数の供給者から関連製品が供給されるような技術的な標準が整備されていることが望ましい。

(2) 個別の要素ごとに導入可能であること

今後、IC・ID カードを利用したサービスの普及に伴い、すでに導入した環境において、IC・ID カードの追加、新たな用途への利用といった追加ニーズが発生することが想定される。このときに、当初導入したベンダが提供できる範囲でのみ追加ニーズへの対応が可能といった事態は、避けなければならない。また、IC・ID カードシステムを長期間利用していれば、関連製品の供給停止や、ベンダからの関連製品の供給が得られなくなるといった事態も生じる可能性がある。

したがって、今後は、IC・ID カードシステムを構成する IC・ID カード、リーダライタ、ドライバ、クライアントアプリケーションといった各要素は、個別に調達して組み合わせ利用ができる必要がある。

(3) クライアント環境の変化に対応できること

IC・ID カードを利用するクライアントシステムの環境は、現在は Windows が多いため、リーダライタやミドルウェアが Windows の特定のバージョンにのみ対応して供給されている IC・ID カードも少なくない。しかしながら、今後 IC・ID カードが広範に利用されるようになれば、Mac OS や Linux といったクライアント環境でも利用できること、Windows を含む各種 OS のバージョンアップに際しても利用できることが求められる。この際、調達済みの IC・ID カードのベンダが、利用者が求めるクライアント環境に必ずしも迅速に対応できるとは限らないが、いずれかのベンダが対応製品を提供した場合には、これを利用できることが求められる。

(4) 相互運用可能性が保障された製品が調達できること

(1)から(3)に示したような状況が実現されれば、IC・ID カードの長期的、広範な導入、利用を目指した関連製品の調達に関して、利便性が飛躍的に高まることになる。一方で、このような状況は、提供されている製品が互いに異なるベンダによって提供されるため、不具合が発生した場合には、原因究明やベンダによる対応が困難になる可能性が高い。

したがって、供給される IC・ID カード関連製品の間で、あらかじめ相互運用可能性の確認がなされ、導入後に不具合が明らかになった場合でも、その原因と対応の必要性が検証できるような環境が整備されていることが必要になる。

### 6.4.2. ベンダの視点

IC・ID カードの関連製品を提供するベンダにとっては、今後広範に IC・ID カードが普及し、利用されるならば、以下に示すような環境が整備されることが望ましい。

なお、ニーズ調査に対して、IC カードベンダからは、関連製品をいずれのベンダからも供

給できるようになることは、既存顧客への継続供給の機会に対して脅威になるとの意見も出されている。また同時に、自社が供給する IC・ID カードの利用環境として、広範なクライアント OS を想定する必要が生じる場合に、あらゆるクライアント OS に対するリーダライタやミドルウェアを自社で提供する必要が生じるのではなく、他社が供給する製品を利用することができれば、ミドルウェアの開発コストが低下し、製品を市場に早く供給できるようになるとの意見もある。

(1) 市場規模の明確化

現在は各社各様の仕様で供給されている IC・ID カードについて、相互運用可能性を確保するために標準仕様を定めるにあたっては、標準仕様に沿って供給される IC カードを調達・利用して IC・ID カードを発行する調達者の範囲、すなわち標準仕様の市場規模について、ある程度明確になっていることが望ましい。

(2) 製品に対する責任範囲の明確化

IC・ID カードに関連する仕様が標準化された環境では、不特定多数のベンダから関連製品が提供されることが想定される。ベンダの立場では、自社が供給する IC・ID カード関連製品が接続し、通信する他の関連製品として、不特定多数の製品との通信を想定する必要が生じる。この場合、他者が提供するあらゆる製品との相互運用可能性を保証することも、不具合が発生した場合の対応を約束することも、非常に困難になる。したがって、他社から標準に準拠しているとして製造・供給される IC・ID カード関連製品について、標準への準拠状況が保証されていることが求められる。

このためには、標準に準拠した IC・ID カード関連製品を供給する前に実施する試験方法が確立されるとともに、試験を通過し、相互運用可能性が確認された製品が標準準拠品として市場に供給されるような仕組みが必要になる。

(3) 製品認定コストの軽減

IC カードに関する製品認定制度は、IC クレジットカードや IC キャッシュカードの分野で運営されており、特定の用途を実現するための IC カードの機能面での相互運用可能性や、セキュリティの確保がなされている。これらの認定制度では、仕様に準拠した IC カードであることを認定するための指定認定機関を設置したり、仕様に準拠し、セキュリティを確保した製造場所で IC カードが製造されていることを確認するための認定作業を行ったりしている。これらの手順を踏むことにより、これらの IC・ID カードや関連製品の相互運用可能性は高いレベルで確保されているが、一方で製品を供給するまでに必要な手順が多く、コストもかかる。このような仕組みは、金融分野のようにすでにサービスの市場が大きく、カードの普及が確実に見込まれる分野では成立するが、これから普及を図ろうとする IC・ID カードの分野では、

できるだけ少ない手順で、供給者が短期間、少ないコストで製品を供給できるよう留意する必要がある。

# 7. IC・ID カードの標準化及び普及に向けた提言

ニーズ調査及びシーズ調査の結果を踏まえ、今後国内において IC・ID カードの相互運用可能性を実現するための環境整備を提案する。

本章では、IC・ID カードの相互運用可能性を確保するために必要な、IC・ID カードシステムに関するアーキテクチャの標準化について提案した上で、標準化に必要な環境整備の具体的な推進方法について提案する。

## 7.1. IC・ID カードシステム関連技術の標準化及び供給・調達への環境整備

今後、将来にわたって IC・ID カードがネットワーク社会におけるインフラとして活用されるために、IC・ID カードシステムに関する技術仕様の標準化を行い、あわせて、供給者が標準に準拠した製品を開発、供給するとともに調達者や利用者が、調達、導入するための環境整備を提案する。

標準に準拠した IC・ID カードシステムを活用することにより、それぞれの主体は、必要な技術要素を自由に組み合わせて個別に調達、導入して IC・ID カードによるサービスを提供、あるいは利用することができるようになる。

### 7.1.1. 概要

IC・ID カードのシステムにおける相互運用可能性を確保するために、以下に示すような仕組みを整備し、相互運用可能な IC・ID カードおよびそれを利用する環境が提供されるような環境を実現することを提案する。

① IC･ID カードシステムの機能及びセキュリティの構造
② IC･ID カードシステムの実装規約
③ 参照実装
④ テスト環境
⑤ 製品認定（certification）の仕組み

IC・ID カードや関連製品の供給者は、上記に沿って自社製品の設計・開発および相互運用可能性の確認を行い、また調達者や利用者は、相互運用可能性の確保された関連製品を導入・利用することができる。

これらの関係を図 14 に示す。

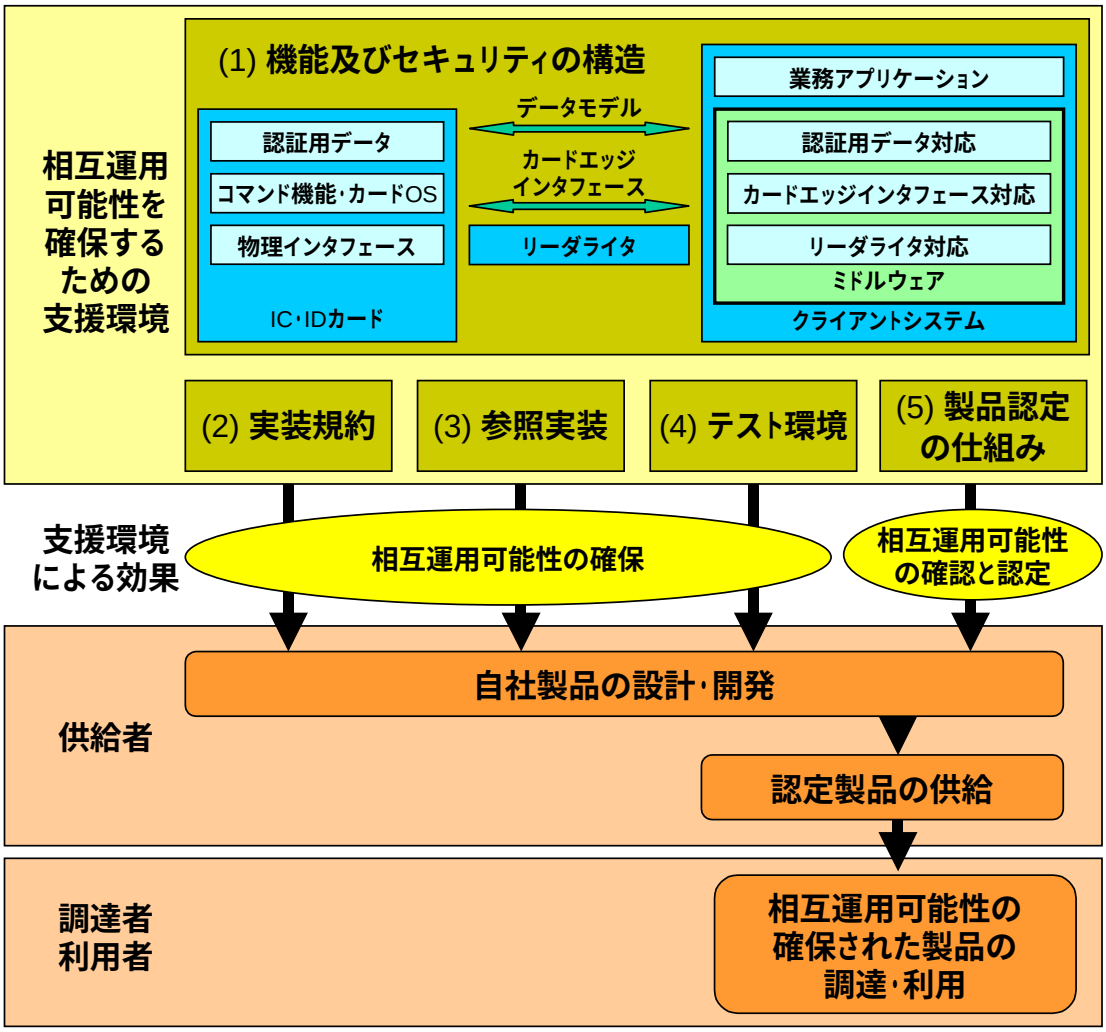



**図 14 相互運用可能性を確保するための環境**

(1) IC・ID カードシステムの機能及びセキュリティの構造

IC･ID カードシステムの構成要素それぞれが提供する機能と、セキュリティ面から整理した役割や位置づけを定義する必要がある。

これにより、実装規約に準拠した製品と準拠していない製品が混在した場合においても、IC･ID カードによって保護される業務アプリケーションのセキュリティが脅威に晒されることがないことを示し、関係者が安心して開発、供給、利用できる基礎となる。

(2) IC・ID カードの実装規約の策定

国際標準に準拠し、国内で汎用的に利用可能な IC・ID カードシステムの仕様は、実装規約によって定義される必要がある。

国際標準で許容されている技術仕様の中から、近い将来を見通して汎用的に利用可能で、ミドルウェア等を通じて製品間の相互運用可能性を確保できる範囲を抽出し、実装規約を策定す

る必要が認識されていた。そのため、文部科学省の科学技術振興調整費による研究プロジェクト（科振費プロジェクト）が本年度より開始されたところである。。

(3) 参照実装の開発

実装規約で定義する各種のインタフェースに準拠した、アプリケーション、ミドルウェア、IC カード内認証用情報等をフリーソフトウェアとして実現した、参照実装を開発する必要がある。そのため、科振費プロジェクトが本年度より開始されている。

IC・ID カード、ミドルウェア、クライアントアプリケーション等の供給者は、参照実装の該当する部分を参考にしながら新規製品の開発を行い、また、接続する部分とのインタフェースの確認を行うことができる。

(4) テスト環境の開発

IC・ID カード製品が実装規約に準拠し、相互運用可能性のあるものであることを検証するためのテスト環境を開発することが望ましい。テスト環境は、IC カード本体等のハードウェア以外に、テストに利用されるソフトウェア、テストの手順、及びテストデータ等によって構成される。供給者は、実装規約に準拠した自社製品の出荷前に、テスト環境を利用して実装規約への準拠性を検証することができる。同一のテスト環境でテストされた製品が供給されることにより、実際の利用環境で、任意の関連製品が組み合わせて導入される場合の相互運用可能性を高めることができる。

(5) 製品の相互運用可能性の証明(certification)の仕組み

市場における IC・ID カード関連製品間の相互運用可能性を継続的に確保するための、製品認定の仕組みを整備することが望ましい。この仕組みを通じて、供給される関連製品の実装規約への準拠性が確認されるとともに、準拠性が確認された関連製品に関する情報が調達者や利用者に提供され、供給された製品による相互運用可能性の確保が実現されると考えられる。

### 7.1.2. IC・ID カードシステムの機能及びセキュリティの構造

実装規約の検討に先立ち、IC･ID カードシステムの構成要素それぞれが提供する機能と、セキュリティ面から整理した役割や位置づけを定義することを提案する。

(1) 定義の必要性

IC･ID カードと業務アプリケーションの相互運用がなされる環境では、IC･ID カードや業務アプリケーションの供給者は、クライアント環境やそこに導入されているソフトウェア等に

ついて、あらかじめ限定することが困難になる。

一方、実装規約等が公開されることは、逆に、実装規約のインタフェースを一部利用しながら、全体としては実装規約の機能やセキュリティを満たさないミドルウェア等の開発をも可能にする。

従って、実装規約に準拠した IC･ID カードシステムの構成要素が、準拠していない他のソフトウェアやハードウェアによって、混乱をきたしたり、セキュリティ面で脅威に晒されるような場合には、IC･ID カードや業務アプリケーションの供給者は、特定の IC･ID カード、特定のミドルウェア、特定の業務アプリケーションの組み合わせでのみ動作可能とするような仕組みを検討する必要が生じる。これでは、IC･ID カードの相互運用は、実質的には広がらないことが懸念される。

(2) 定義内容の概要

IC・ID カードの認証用データ、データモデルの構造、カードエッジインタフェース、リーダライタ、ミドルウェア、クライアントアプリケーションのそれぞれの要素が、IC・ID カードを利用した認証機能の実施にあたり、どのような情報を扱い、どのように処理するのかを明確に定める必要がある。

これにより、実装規約に準拠した製品と準拠していない製品が混在した場合においても、IC･ID カードによって保護される業務アプリケーションのセキュリティが脅威に晒されることがないことを示し、関係者が安心して開発、供給、利用できる基礎となる。

特に、IC･ID カードによって確保されている業務アプリケーションのセキュリティは、実装仕様に準拠していない他の要素（IC･ID カード、リーダライタ、ミドルウェア、業務アプリケーション、その他のソフトウェアやハードウェア）との通信によっても、脅威に晒されないように定義する必要がある。

例えば、認証用データのセキュリティを確保するために必要な情報は、IC・ID カードと業務アプリケーション内部でのみ扱い、中間の要素ではその内容を知ることができないように通過させなければならない。また、認証用データのセキュリティを弱めるような機能を、中間の要素が持つ余地があるような機能構造を許容してはならない。

### 7.1.3. 汎用的な「IC・ID カード実装規約」の整備

今後ある程度の長期間にわたって、IC・ID カードとしての利用が見込まれ、相互運用可能性が確保でき、かつ広範な用途で利用可能な、実装規約を検討、定義し、国内の IC・ID カードの相互運用を実現する必要がある。

(1) 目標

実装規約の目標は、以下のように整理される。

- IC･ID カードシステムを構成する要素の間でのインタフェースとセキュリティ上の役割分担が明確に定義される
- システム間、ベンダ間での「認証用データの利用」における相互運用可能性を確保する。
- 内外のベンダや研究者が関連製品となるソフトウェアやハードウェアを開発できる情報を提供する
- 実装仕様を参照することで認証用データを利用する機能の調達を可能に
- 実装仕様を参照して調達した業務アプリケーションは技術的には相互運用可能になる

(2) 規定の対象

この実装規約には、以下の範囲に関する規定を含む。

- クライアントアプリケーションインタフェース
- リーダライタインタフェース
- 物理インタフェース
- カードエッジインタフェース
- データモデル
- 記録された認証用データへのアクセス手順

実装規約で整理する IC・ID カードシステムの構造を図 15 に示す。

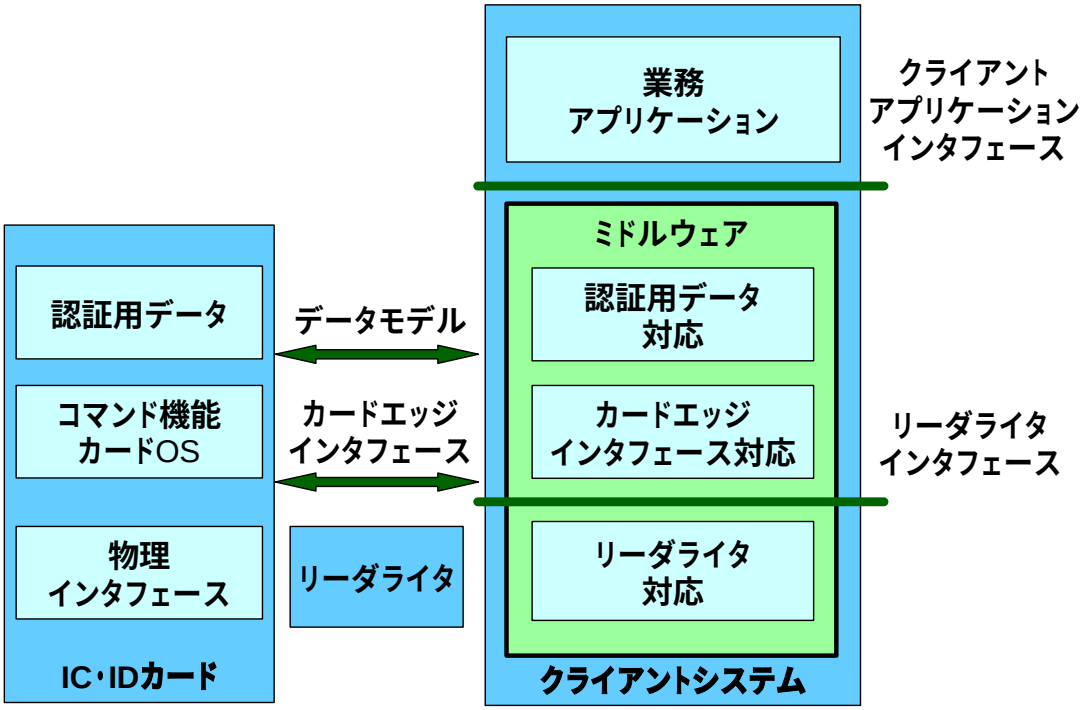



図 15　IC・ID カードシステムの実装規約の構造

それぞれの位置付けについて以下に示す。

ア．　クライアントアプリケーションインタフェース

クライアントアプリケーションインタフェースは、クライアントに導入されている業務アプリケーションとミドルウェアの間のインタフェースであり、業務アプリケーションがIC・IDカードを用いて実施する動作とその結果の入出力について定義する。

業務アプリケーションは、ミドルウェアから先の構造を、クライアントアプリケーションインタフェースを通じて、IC・IDカードサービスとして認識する。

クライアントアプリケーションインタフェースの標準化により、利用者は、IC・IDカードやミドルウェアの供給者や製品を意識することなく、業務アプリケーションを開発することができるようになる。

イ．　リーダライタインタフェース

リーダライタインタフェースは、ミドルウェアとリーダライタの間のインタフェースであり、ミドルウェアがリーダライタを通じてIC･IDカードを認識･操作するための機能を定義する。

リーダライタインタフェースと、後述する物理インタフェースを定義することにより、利用者やカード保有者はリーダライタを自由に選択できるようになる。クライアントPCのOSのバージョンアップ等の事態で従来利用していたリーダライタが利用できないといった事態にも、必要に応じて適用可能なリーダライタを選択・交換することができるようになる。

ウ．　物理インタフェース

リーダライタは、リーダライタインタフェースによってクライアント環境から操作され、既に標準化がなされているICカードの物理インタフェースによってIC･IDカードと接続する。

エ．　カードエッジインタフェース

カードエッジインタフェースは、リーダライタを通じてクライアント側ソフトウェアとIC・IDカードが通信するインタフェースであり、IC・IDカードが実施する機能を定義する。

カードエッジインタフェースを定義することにより、様々な供給者から供給されている
IC・IDカードを、同一のミドルウェアを通じて同様に操作することができるようになる。

オ．　データモデル

データモデルは、IC・IDカード内での認証用データの記録方式を定義する。

データモデルを定義することにより、IC・IDカードに記録されている認証用データを、カードの種類を意識することなく、クライアントアプリケーションから利用することができるための技術的な条件が整備される。

実際には、すべての IC・ID カードの認証用データが自由に利用されるのではなく、クライアントに接続された IC・ID カードの認証用データや機能の中から、当該利用者、当該クライアントアプリケーションに許可されている範囲のデータや機能を利用することができる。

カ.　認証用データへのアクセス手順

クライアントアプリケーションインタフェースでは、認証用データへのアクセスを試みるための関数が定義されるが、認証用データは、正しい手順でアクセスしなければ、認証用データの構造をミドルウェアやクライアントアプリケーションが知ることもできず、また、認証用データを取り扱うこともできない。

したがって、相互運用可能性を確保するため、実装規約の一環として、IC・ID カードの認証用データにアクセスするためのコマンド及び処理手順を定義する。

### 7.1.4. 参照実装やテスト環境の整備

実装規約の制定と合わせて、参照実装及びテストツールの整備を提案する。参照実装及びテストツールの開発により、供給者による実装規約に準拠した IC・ID カード関連製品の開発を促進するとともに、供給される製品間の相互運用可能性を向上する。

実現されたソフトウェアは、オープンソースソフトウェアとして公開し、供給者側、調達者や利用者側の誰もが、自由に利用できるようにする。

参照実装及びテスト環境を利用することにより、開発者は、自社製品の開発や検証を促進することができる。一方、利用者は、自身が提供するサービスに係わるクライアント環境に必要なミドルウェアを調達、検証したり、必要に応じて自ら開発して利用することができる。

以上について、図 16 に示す。

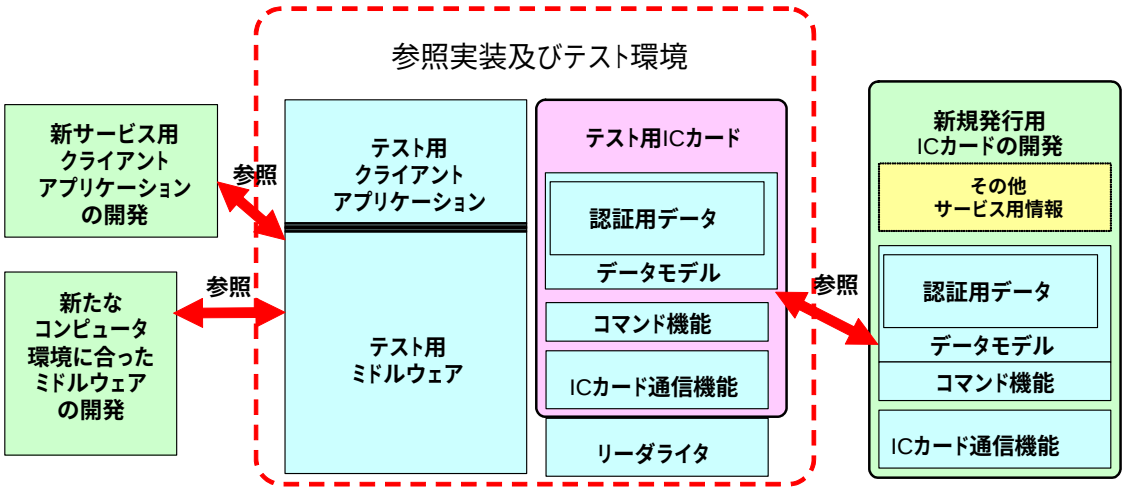



図 16 参照実装及びテスト環境

(1) 参照実装

参照実装は、実装規約で定義した仕様の実現例を示すものである。IC・ID カードシステムを構成する各層をソフトウェア的に実現する。

供給者は、実装規約の文書だけでなく、実装例を参照することにより、より短期間での開発を促すことができる。参照実装は、同時に、関連製品を開発する多数の供給者の間での、実装規約への理解の統一化を図ることにも寄与する。

(2) テスト環境

テスト環境は、テストに利用されるソフトウェアと、テストの手順、テストデータ等によって構成され、主として関連製品を開発・供給する供給者によって利用される。供給者は、実装規約に準拠した自社製品の出荷前に、テスト環境を利用して実装規約への準拠性を検証することができる。同一のテスト環境でテストされた製品が供給されることにより、実際の利用環境で、任意の関連製品が組み合わせて導入される場合の稼動可能性を高めるとともに、導入後の各種製品のメンテナンスを容易にする。

また、実際のクライアント環境に各種の製品を導入する際の、システム試験にも活用することができる。

このように、テスト環境は、実装規約に準拠した製品を提供する新たなベンダの市場参入を促進するとともに、品質確保に貢献する。

(3) 期待される効果

IC・ID カードシステムの参照実装やテスト環境の開発によって期待される効果と、IC・ID カード導入に係わるニーズの有無に関する評価は表 7 のように整理される。

**表 7　参照実装及びテスト環境により期待される効果**

| ニーズの種類 | 具体的な効果 | 参照実装及びテスト環境へのニーズの評価 |
|---|---|---|
| (1) 異なるクライアント環境での IC・ID カードの利用 | ベンダーや利用者自身が新たな環境で IC・ID カードを利用するためのミドルウェアを短期間に開発できる | 多様な端末利用環境に導入したい場合 |
| (2) 1 枚の IC・ID カードの複数用途への利用 | 調達・発行した IC・ID カードで利用できるサービスの開発が容易になる | 汎用目的で発行したい場合<br>他分野のカードとの相互利用を指向する場合 |
| (3) IC・ID カードと業務アプリケーションの組み合わせを 1 環境で複数種利用 | 調達・発行した IC・ID カードで利用できるサービスの開発が容易になる | 端末利用者のニーズは高いが調達側にはニーズ少ない |
| (4) 1 種の業務アプリケーションで複数ベンダーの IC・ID カードを利用 | テスト環境で確認されたカードならばベンダーが異なっても利用可能 | 多数の主体が調達したカードが 1 箇所で使われる場合<br>ベンダーは独自サポートで継続的に供給したい |
| (5) 1 種のサービスで同時に複数種の IC・ID カードを利用 | テスト環境で確認されたカードならば異なる種類も利用可能 | 他の調達者が発行する IC・ID カードと組み合わせて利用する用途が中心的な場合 |

### 7.1.5.　製品認定の仕組みの整備

実装規約や参照実装、テストルールの普及と合わせて、それらに準拠した IC・ID カード関連製品と、準拠が保証されない製品とを明確に区分し、調達者や利用者が安心して製品を調達できるような仕組みを整備することが重要である。

(1) 製品の相互運用可能性の証明(certification)の目的

相互運用可能な IC・ID カードは、相互運用できない IC・ID カードと明確に区別されなければならない。

相互運用可能性の確保された製品を調達したい調達者および利用者が IC･ID カードおよび関連製品を調達、利用しようとする際には、どの供給者のどの製品が実装規約に準拠した製品であるかを確認した上で調達したい。しかしながら、実装規約への準拠を供給者の自己申告だけに頼って確認する場合、将来的に各種製品の供給者が増えた場合に、確認が不十分な製品や、限定的な機能についてのみ準拠した製品が、「実装規約に準拠」した製品として供給される可能性が否定できず、「一般に、相互運用を図ることができない」状況が変化しないため、策定した標準に準拠した IC・ID カード関連製品が普及しないことが懸念される。

製品の相互運用可能性の証明の目的は、以下のように整理される。

- 相互運用可能性が確保された製品を調達者や利用者、カード保有者が安心して調達できること。
- 相互運用可能性のある IC･ID カードやﾘｰﾀﾞﾗｲﾀ、ﾐﾄﾞﾙｳｪｱ等を調達可能であることを明

示し、公的機関での調達条件として採用しやすくなること。

- 「安心して使えるカード」としてのブランドを確立し、製品認定を通じて国際標準に準拠し、相互運用可能性の高い IC･ID カードを普及しやすくなること。
- 以上が、IC カードベンダにとって過度な負担なく実現されること

(2) 製品の選別

製品認定の仕組みは、以下のような観点で、実装規約に準拠し相互運用可能性の確保された製品と、そうでない製品を区別できる仕組みとすべきである。

- 開発･製造された IC･ID カードが実装規約に準拠していることを確認できること
- 実装規約に準拠した IC･ID カードを他のカードと区別できる方法を提供すること
- 調達側が実装規約に準拠した IC･ID カードを調達し、準拠していることを確認できる方法を提供できること

(3) 仕組みの検討と整備

認定による製品への品質保証の確かさ、調達者や利用者に対する訴求効果とあわせて、供給者の製品開発の迅速性及びコスト面での負担の最小化を考慮し、関係者の参画を得ながら、製品認定の仕組みを検討、整備されることが望ましい。

検討に当たっては、国内外の IC カードに関する認定の仕組みが参考になると考えられる。

## 7.2. 対象分野と進め方

IC・ID カードの相互運用可能性を実現するための実装規約、参照実装等の環境整備は、具体的に利用される用途を見込んで開発し、当初のユーザで十分に成果を示して複数の分野に普及を図るシナリオで進める必要があると考えられる。

以下に、IC・ID カードの相互運用可能性に関する環境整備の進め方が考えられる。

### 7.2.1. 開発の対象とする分野

既に発行されている IC・ID カード、現在大規模に IC カードが発行、普及している分野、さらに、今後導入が期待される IC・ID カードについて、参照実装やテスト開発へのニーズの有無を評価し、表 8 に開発の対象とすべき分野の抽出を行った。

**表 8　開発の対象とすべき分野**

| 分類 | 分野 | 状況 | 評価 |
|---|---|---|---|
| 大規模に普及 | 電子マネー | 大規模に普及している例は FeliCa により実現されており、一般には PKI に利用できず、IC･ID カードにはならない | × |
| | 交通 | | × |
| | キャッシュカード | 全銀協の仕様により、キャッシュカード用途専用に発行。他の用途との相互運用は考慮されていない | × |
| | クレジットカード | EMV 仕様により国際的に統一。多くは署名済データは持つが IC･ID カードではない。クレジットサービス専用に発行 | × |
| 既存導入分野 | 社員証 | 導入先企業の業務に合わせて IC･ID カードの仕様を最適化し、クライアントも統一が可能。IC･ID カードはあまり普及していない | × |
| | 企業向け証明書 | 既に発行されている IC･ID カードは独自仕様。今後相互運用のニーズが顕在化してくれば、対象になる可能性あり、 | △ |
| | 公的個人認証 | 独自仕様で必要な範囲の相互運用を実現済み。他の公的分野との相互運用ニーズがあれば、対象になる可能性あり | △ |
| 検討中の分野 | HPKI | HPKI を推進する方向での診療報酬の改訂がなされれば普及が急速に進む。様々なクライアント環境での利用が必須とされる | ◎ |
| | 国家公務員 IC カード | 職員のオンラインでの本人認証に利用されれば、IC･ID カードとしての利用される可能性がある | ○ |
| | 大学･UPKI | 研究や学内事務において、大学個別に相互運用可能性のある IC･ID カードの利用を検討する可能性がある | ○ |
| | 保健医療分野 | IT 新改革戦略[22]に記載。住民の保健医療福祉分野で本人認証に広く使われる可能性。医療同様に様々な場所での利用が必須 | ○ |

凡例：◎強いニーズあり　○ニーズあり　△ 普及すれば利用の可能性あり　×ニーズなし

上表を考慮すれば、HPKI を中心に国家公務員証や保健医療分野、大学といった用途での普及が期待できると考えられる。

### 7.2.2. 環境整備の進め方

HPKI を中心に普及を図るためのスケジュールとしては、JAHIS が現在行っている、IC カードに関するガイドラインの検討の後に詳細な仕様を検討できるよう進めることが望ましいと考えられる。

HPKI に関しては、現在 JAHIS で IC カードガイドラインの検討が行われており、その後、それぞれの HPKI 認証局にて、本格導入期に調達する、相互運用可能性の高い IC・ID カードの仕様の検討が行われると考えられる。医療機関が本格的に検討するとすれば、早くても平成 20 年春に予定されている診療報酬改訂以降ではないかと考えられる。したがって、その段階までに、詳細な実装規約が整理され、参照実装及びツールの開発に目処が立ち、認証局での調

達、医療機関での導入に活用できることが望ましい。

本調査の終了後、継続的に各分野での調達者、利用者、供給者との情報交換を進め、相互運用可能性の必要性について関係者の理解を得るとともに、実装規約のあり方をはじめとした、相互運用可能性を実現するための環境整備の進め方について調整を図ることが適当である。引き続いて平成 19 年度前半に本格的な実装規約の検討を行い、それに基づいてツールの仕様を検討し、参照実装及び試験ツールを開発することが期待される。

## 7.3. 提言の実現により期待される効果

### 7.3.1. IC・ID カードの相互運用可能性への効果

IC・ID カードシステムの相互運用可能性確保に資する環境を整備することにより、下記に示すような効果が期待される。

(1) IC・ID カードシステムの調達における利便性の向上

新たに IC・ID カードによるサービスを提供しようとする仕様策定者や調達者、また、提供されている IC・ID カードを利用してネットワークを通じた安全なサービスを実現しようとする利用者は、自らが実現しようとする IC・ID カードシステムを検討する際に、実装規約によって定義された IC・ID カードシステムの構造を活用してシステムの設計を行うことができる。また、製品の調達にあたっては、実装規約に沿った製品を指定して調達することにより、任意の供給者から必要な製品を調達することができる。

特に、公的分野での調達者や利用者は、調達仕様書を作成して供給者を公募するにあたり、実装規約を指定することによって供給される製品の機能および性能を確保することができるだけでなく、システム一体ではない、一部部品の独立した調達も可能になる。

(2) 導入した IC・ID カードの相互運用可能性の確保

環境を活用することにより、導入された IC・ID カードの相互運用可能性が確保される。具体的には、下記のような利用が可能になる。なお、下記に示す利用の具体的な内容については、「3.3　IC・ID カードの相互運用の例」に記述している。

- 異なるｸﾗｲｱﾝﾄ環境での IC･ID カードの利用
- 1 枚の IC･ID カードの複数用途への利用
- IC･ID カードと業務ｱﾌﾟﾘｹｰｼｮﾝの組み合わせを 1 環境で複数種利用
- 1 種の業務ｱﾌﾟﾘｹｰｼｮﾝで複数種の IC･ID カードを利用
- 1 種のサービスで同時に複数の IC･ID カードを利用

(3) IC・ID カードシステムの維持管理における柔軟性の向上

環境を活用することにより、調達者や利用者が導入した IC・ID カードシステムの利用・維持にあたっても、柔軟な対応が可能になる。IC・ID カードシステムの長期的な維持管理に際しては、当初の供給者が利用者側における利用条件や要求の変化に対応した製品の供給を十分に実施的ない場合もあるが、実装規約に準拠した製品を供給する供給者が複数存在する状況においては、市場から広く代替製品を調達することができるようになる。

- 当初と同じ、あるいは追加･変更された機能や認証用情報での、IC･ID カードの追加調達
- クライアント利用環境の追加や変更に合わせたリーダライタやミドルウェアの調達
- 新たなクライアントアプリケーションの開発と追加

### 7.3.2. 費用面で期待されるメリット

上述した効果によって、調達者や利用者が IC・ID カードシステムを調達、管理するに当たって、費用面で以下に示すようなメリットが生じることが期待される。

(1) 他の IC カードとの相互運用を容易に実現可能

IC・ID カードを利用してネットワークを通じたサービスを提供しようとする利用者が、導入当初とは異なる IC・ID カードを利用しようとする場合に、最小限の追加開発で実現することができるようになる。

すなわち、すでに導入されているミドルウェアおよびリーダライタが実装規約に準拠しているものであれば、実装規約に準拠した他の IC･ID カードに対してもそのまま適用可能である。クライアントアプリケーションの側では、従来の IC・ID カードと新たに利用しようとする IC・ID カードとの間の、認証用データの仕様やセキュリティ設定の差異を把握し、クライアントアプリケーションに対して、双方の IC・ID カードを認識した上でそれぞれの認証用データの仕様やセキュリティに沿って利用するよう最小限の機能追加を行えばよい。

これにより、従来の環境によるデメリット（「6.2.2　今後発生が予想されるデメリット」を参照）と比較して、新たな開発費用の削減とおよび実現までの期間の短縮が図られる。

以上について、図 17 に示す。

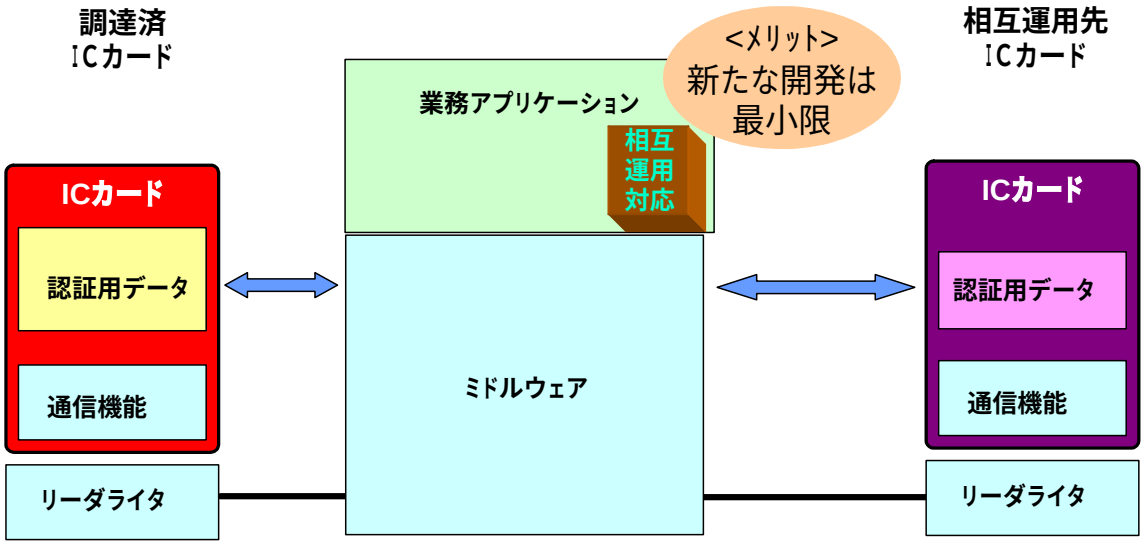



**図 17　他の IC カードとの相互運用を容易に実現**

(2) 業務アプリケーション単独での調達が可能

IC・ID カードを利用してネットワークを通じたサービスを提供しようとする利用者が、導入当初とは異なるサービスに IC・ID カードを利用しようとする場合に、最小限の追加開発で実現することができるようになる。

すなわち、すでに導入されているミドルウェアおよびリーダライタが実装規約に準拠しているものであれば、新たに利用しようとするクライアントアプリケーションも、実装規約に準拠したクライアントアプリケーションインタフェースに準拠して開発すればよい。

クライアントアプリケーションを提供する供給者は、ある環境に対して提供したクライアントアプリケーションを他の同様な環境にも供給可能である。また、喫緊の調達がなされていない場合であっても、すでに発行されている IC・ID カードへの適用を幅広くにらんで、実装規約に準拠したクライアントアプリケーションを独自に開発することができる。

これにより、従来の環境によるデメリット（「6.2.2　今後発生が予想されるデメリット」を参照）と比較して、新たな開発費用の削減とおよび実現までの期間の短縮が図られる。

以上について、図 18 に示す。

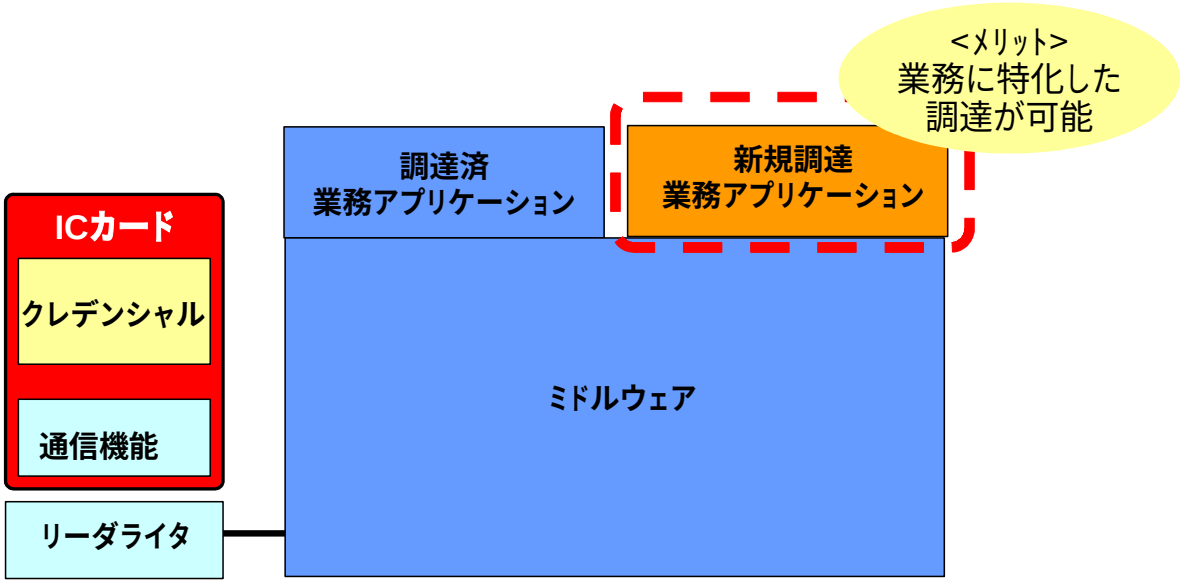



**図 18　業務アプリケーション単独での調達が可能**

(3) 各種の IC・ID カードに自由に対応可能

クライアント環境において、複数の調達者によって発行された IC・ID カードに対応する際に、IC・ID カードの調達者や供給者、適用できる業務アプリケーションを意識する必要がなくなる。

実装規約によって各種のインタフェースが標準化されていれば、あるクライアントにおいて、同一の仕様の元に発行された IC・ID カードは、どの供給者、どの調達者から提供されたものであっても、同一のミドルウェアを通じて使用することができるため、利用対象の調達者が増えたり、ある調達者が IC・ID カードの共有者を変更したりした場合であっても、クライアント環境のミドルウェアを追加したり変更したりすることなく、新たな IC・ID カードの保持者に対してもサービスを提供することができる。

以上について、図 19 に示す。

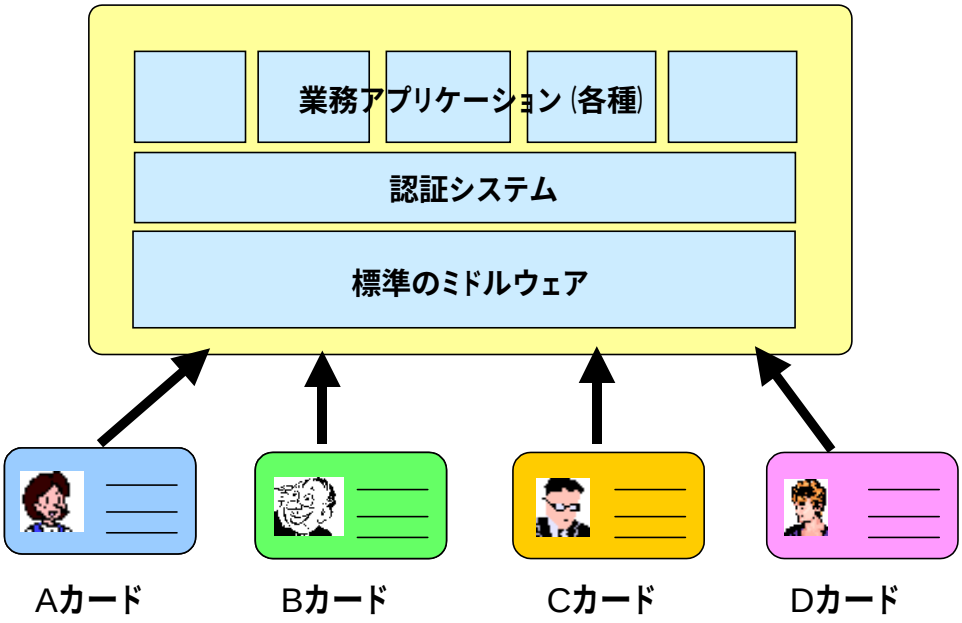



図 19　各種の IC・ID カードに自由に対応可能

## 7.4.　提言に係わる国内外の状況

IC・ID カード仕様の標準化及びに関しては、欧州や米国で積極的に取り組まれているのに対して、日本国内では現在までのところ取組みは見られない。米国、欧州で IC・ID カードシステムの標準化、公開が受け入れられている理由と、国内で普及していない理由について、調査結果に基づき整理する。

### 7.4.1.　海外で受け入れられている理由

欧州や米国では、それぞれの地域で国際標準に沿った IC・ID カード仕様の標準がなされている。そこには、技術の標準化につながるサービスの標準化や、セキュリティの確保に向けた考え方において、日本とは異なる事情があると理解できる。

(1) 米国における事情

ア.　セキュリティに関するフレームワークの明確化

米国では、2001 年 9 月の同時多発テロ以降、情報セキュリティのマネジメント及び技術的なフレームワークに関する取り組みが大きく変化した。2002 年 12 月に制定された連邦情報セキュリティマネジメント法（FISMA：Federal Information Security Management Act of 2002）では、連邦政府機関が情報セキュリティを強化することを義務付け、国立標準技術研

究所(NIST: National Institute of Standards and Technology）に対しては、そのための規格やガイドラインの開発を義務付けている。FISMA に従い、NIST では、FISMA リスクマネジメントフレームワークという、 情報セキュリティを継続的に改善・向上させる枠組みや多くの規格、ガイドラインを開発している。

このように、米国では、情報システムのセキュリティに関して、技術的フレームワークを整備し、政府機関の情報システムがこのフレームワークに沿って、要素技術ごとのセキュリティ要件とその優先度を明確にし、セキュリティに関して評価・認証を受けた製品を導入することが求められている。

イ． PIV における技術フレームワークの明確化

連邦政府の従業員及び委託業者の個人識別に関する PIV についても、要素技術ごとのセキュリティ要件を明確化する必要がある。ここで、IC・ID カード、リーダライタやミドルウェアといったそれぞれの要素技術のセキュリティ要件を明確化するためには、要素技術ごとの機能及び入出力する情報の種類や状態を明確に定義する必要がある。そのため、PIV では、ホームランド・セキュリティ大統領指令 12（HSPD-12）[23]（連邦政府職員と契約業者の共通識別基準のためのポリシー）を最上位のポリシーとして、連邦従業員及び委託業者の個人識別情報の検証に係わる技術について、トップダウンで仕様の整理がなされている。

ウ． 仕様の公開によるセキュリティの向上

PIV では、仕様自体が公開されているだけでなく、PIV(カードとミドルウェウェア)の仕様、PIV のテスト仕様、PIV のレファレンス実装、PIV のテストツールなどがセットで提供されている。その上で、PIV に提供されるベンダ各社の製品に対して、PIV の準拠性に対する認定を行なっている。これらは、本来、セキュリティを確保するためのフレームワークであるが、同時に、IC・ID カードの相互運用可能性を確保するためのフレームワークにもなっている。

また、各種仕様の制定に当たっては、原案の段階から公開し、幅広く意見を求めている。上記のように要素技術のフレームワークを明確化する以上、技術仕様は公開されることが前提となるため、セキュリティ上の弱点はできるだけ早い段階から認識、改善を図るという考え方によると見られる。

(2) 欧州における事情

ア． サービスの相互運用と技術要素の標準化

多数の国家が陸続きで連なっている欧州では、古くから生活や商行為において、国境を超えた往来が日常的に行われてきた。近年の EU 統合の動きによりその傾向はますます加速し、いまや毎日の通勤が国境を超えることも珍しくはない状況である。

このように､居住している地域と日常生活を行っている地域が異なる国といった状況下において､住民が利用できる各種のサービスが､どこでも同様に受けられることが求められてきている。

このような背景から､各種の公的なサービスが国境を超えても利用できるよう､制度面での整備や関連する書面､手続き等の共通化､標準化が進められてきた。たとえば医療保険の分野では､紙面による医療保険の請求に関わるサービスを皮切りに､被保険者証の券面表記､さらには IC カードに記録されるデータと､国境を越え､自らの被保険者証を記述した地域とは異なる母国語を持つ地域であっても､国内と同様に医療保険の適用が受けられるよう､順次手続きや技術の標準化を進めてきている。

イ.　欧州における標準化の考え方

欧州では､単独の国家を市場としてみた場合には､人口､経済規模の両面で大きな市場にはなっていない。そのため､各国で利用する技術の標準化を進め､欧州全体をひとつの市場として成立させることにより､域内の経済の活性化と産業の育成を図ってきた。欧州では､各国の参加により欧州標準（EN: European Standard）が整備され､各国の国内標準との整合を図っている。また､同時に､EN を国際標準である ISO や IEC､ITU に提案する動きも活発に行っており､欧州内の産業の国際競争力を高めようとしている。

ウ.　オープンソースによる開発

IC・ID カードにおいては､各国単独では人口もさほど多くなく､独自の仕様で調達するにはコスト高になるという状況もあってか､フィンランドの FINID の取り組みを皮切りに､各国が導入する IC・ID カードおよび関連システムの仕様を公開し､オープンソースソフトウェアによるミドルウェアの実装も公開されている。これらオープンソースソフトウェアの実装を活用して､各国での普及・導入が進んでいるものと見られる。

### 7.4.2.　国内で普及していない理由

一方､日本国内では､認証データを扱う IC・ID カードシステムに係わる各種技術のアーキテクチャについて､これまで積極的に標準かが取り組まれてはこなかった。その背景として代表的と考えられるものを､以下に 2 点挙げる。

(1) 分野別での情報化の推進

日本では､従来から､担当省庁において個々に情報関連の政策を実施してきた経緯があり､関連技術の標準化や体系整理が充分に統一的に行われてこなかった。

国内では､IC・ID カードとして分類される IC カードを利用し､PKI によってネットワーク経由のサービスを実現する取組みが､府省や都道府県等によって個別に実施されており､技

術的な仕様も個別に定められている。利用される IC・ID カードの仕様に関しては、複数のサービスに利用される IC・ID カードを 1 枚にまとめられるようにとの配慮から、IC カードの仕様に関してはある程度の標準化を図っているが、クライアントの利用環境については標準化が図られていない。

(2) 垂直統合的な供給体制

国内には、サーバシステムから周辺機器までを一貫して企画、開発、販売できる、いわゆる総合電機メーカーと呼ばれるベンダが複数存在する。これらのベンダは、自社の企画、設計により、独自のインタフェース仕様を持つ製品によって特定の機能に対して最適化した部品を組み合わせることにより、特定用途に対する一貫した情報システムを提供することができる。

このように提供された製品は、利用者にとっては、当面の用途を最適の機能、性能で満たし、部品の故障時にも、単一の窓口で速やかにメンテナンスがなされるなどのメリットがあり、一方、ベンダにとっても、部品の故障時に必ず自社製品によって代替される、顧客を囲い込むメリットが生じる。また、国内の人口規模及び産業規模は、これらの独自仕様による製品を維持し、欧州基準や国際標準、米国の基準に沿った製品への集約を行わなくても、ある程度の市場規模として見込むことができる。

このように一貫した情報システムを企画、設計、提供できるベンダが複数存在するため、公的な分野においても、情報システムの導入に際して、技術的な構造を意識することなく、実現すべき機能あるいは業務のみを示しても、調達先の選定に際して競争環境が維持される。

以上のような背景から、ベンダ個別仕様による、情報システム全体での供給がなされてきており、その構成要素の標準化が進んでこなかったといえる。

## 7.5. 提言の実現に係わる課題

IC・ID カードシステム関連技術の標準化及び供給・調達への環境整備を実現するに当たって、検討を要する課題について、下記に示す。

### 7.5.1. IC・ID カードの実装規約

(1) 技術とセキュリティの構造

最近の実現例として、ミドルウェアが持つべき機能のうち、カードエッジインタフェースやデータモデルに対応する機能はサーバアプリケーションに具備し、クライアント環境にはリーダライタによって IC・ID カードとの物理的な接続を制御する機能のみを持たせる方法も存在する。この構造での実装は、一般的な実装と比較してクライアント環境とサーバのセキュリティ分担の考え方が異なると考えられる。IC・ID カードサービスの機能の全てがクライアント環境に収まっておらず、その内部にインターネットによる通信を含むケースであるとの解釈も

できる。

実装規約の検討にあたっては、IC・ID カードサービスの実現形態が異なる場合を想定すべきである。

(2) 関係者の協力の獲得

ISO/IEC 7816 シリーズに代表される国際標準では、IC カードのコマンドや認証用データを IC カード内に記録される記録形式について、従来製造・供給されている IC カードを幅広くオプションとして許容しているため、相互運用可能性を確保するのに十分な規定がなされていない。すなわち、あらゆるオプションに対応するミドルウェアの開発はほとんど不可能な状況である。また、IC カードとリーダライタの接続においても、同様の問題により、ある IC カードと通信可能なリーダライタに、同じコマンドを持つはずの他社カードを挿しても動作しない場合がある。

したがって、実装規約の策定にあたっては、国際標準に規定される機能の中から、国内で導入、利用される IC・ID カードにおいて汎用に利用可能な機能を選択し、相互運用可能な範囲に絞り込む必要がある。

一方で、汎用の用途を目指す場合、以下の点において、実用性に欠ける仕様になってしまう危険がある。

- 汎用性を意識して機能を多く盛り込みすぎてしまい、実装の難易度が上がる、あるいは処理性能の面で最適化が図られないなど、使用に耐える製品が供給されない
- 規定の詳細度が不十分で、処理が正常に終わらなかった場合の対応方法に一貫性が確保できず、カードごと、ミドルウェアごとの差異が出てしまう
- 実現性を重視して機能を絞り込みすぎてしまい、ニーズの多い特定の分野で実装仕様が適用できない

以上のような事態を避けるために、実装規約に盛り込むコマンドやデータモデルは、各種の実現例や今後導入を予定している分野でのニーズを十分に取り込むよう留意する必要がある。また、IC カードやリーダライタに関するベンダの経験を十分に活用し、製品間の差異に起因する処理の一貫性のなさが生じないように留意する必要がある。

すなわち、実装規約の検討に当たっては、具体的な IC・ID カードシステムへのニーズの面、将来的な国際標準動向との強調を図る面、技術的な実現性の高い仕様とする面、それぞれの観点で、さまざまな関係者の協力を得て進める必要があると考えられる。

- 様策定者や利用者として、近い将来 IC･ID カードの普及や相互運用可能性への高いニーズが想定される分野の関係者。例として HPKI を中心とした医療分野や大学、各種の代理申請に係わる業種が考えられる。
- 国際標準関係者として、ISO/IEC JTC1 の国内審議団体の関係者
- 供給者として、IC･ID カードやﾘｰﾀﾞﾗｲﾀ、関連ｿﾌﾄｳｪｱの提供者。とりわけ、IC･ID カードのコマンド仕様とのたたき台として有力と考えられる、JICSAP 仕様第 2.0 版の関係者の協力を求める必要がある。

一方で、様々な技術的な条件に留意して実装規約の策定を進める場合には、これらの条件が技術的な制約として見え、これらの制約を満たす「実現可能な」実装規約とすることが自己目的化してしまう懸念もある。技術要素間の機能とセキュリティの構造や、実現可能なニーズの範囲を明確に定義し、一貫性のある実装規約を策定するよう、留意しなければならないと考えられる。

### 7.5.2. 参照実装及びテストツール

参照実装及びテストツールの開発に当たっては、これまでに欧米を中心に取り組まれてきた標準化の推進において開発、活用が図られてきた先進例を参考にして、効率的な開発とともに実効性のある普及を検討する必要があると考えられる。

(1) 参照実装

参照実装の開発においては、Open SC プロジェクトをはじめとした、海外で提供されているオープンソースでの参照実装の活用を考慮すべきである。

(2) テストツール

以下に、PIV におけるテスト環境として、テストの方法論、及びテスト環境を、図 20、表 9、及び図 21 で示す[24][25][26]。

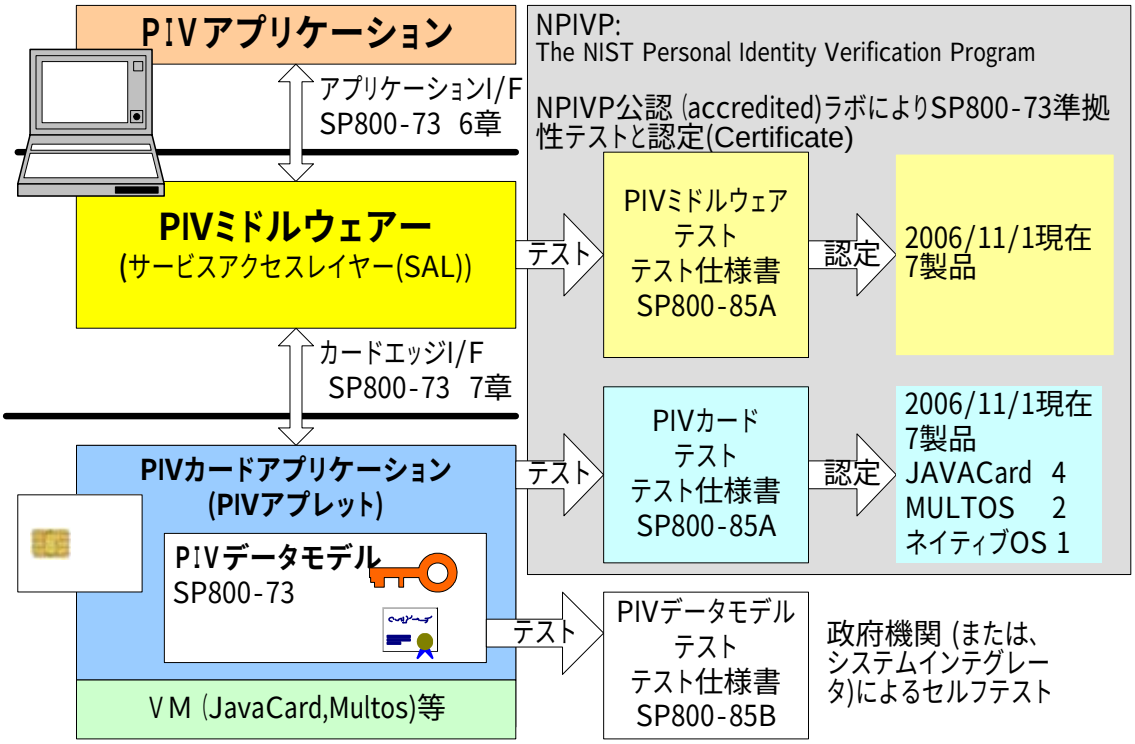



**図 20　PIV におけるテスト方法論**

**表 9　PIV におけるテスト一覧**

| テスト対象 | 誰によるテスト | 何時テストされるか | テスト仕様書 |
|---|---|---|---|
| PIV ミドルウェア I/F | 公認された(Accredited) NPIVP ラボ | 政府機関の調達前 | SP 800-85A |
| PIV カードアプリケーション I/F | 公認された(Accredited) NPIVP ラボ | 政府機関の調達前(カードのパーソナライゼーション以前) | SP 800-85A |
| PIV データモデル (カード上のコンテンツ) | 政府機関 (または、システムインテグレータ) | カード発行の間 (パーソナライゼーション) | SP 800-85B |

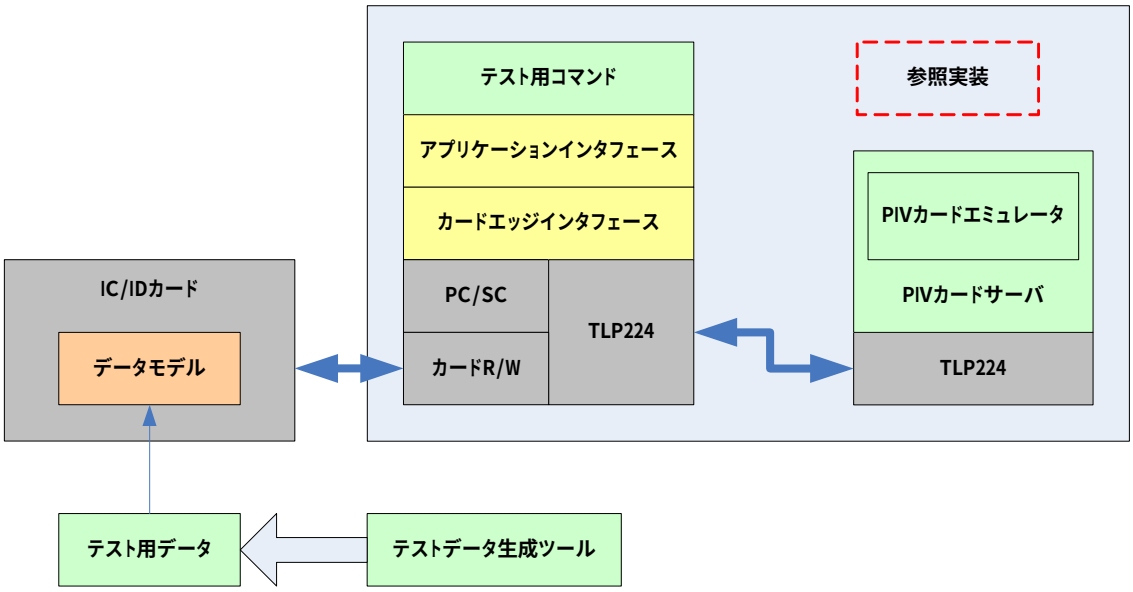



図 21　PIV におけるテスト環境の模式図

### 7.5.3.　製品認定の仕組み

(1) 先進例の活用

製品認定の仕組みの整備に当たっては、これまでに内外で取り組まれてきた各種の IC カードにおける製品認定の仕組みを参考にする必要がある。

以下に、参考になると考えられる先進事例について例示する。

ア.　PIV における製品認定の仕組み

PIV では、製品の認定を行うのは NPIVP であるが、試験は NPIVP が認め、テストツールキットを提供された公認の試験機関が行う。認定された試験期間での試験に合格した場合には、試験機関から発行されるテスト報告書に沿って、NPIVP より認定書が発行される。

PIV における製品認定スキームを図 22 に示す。

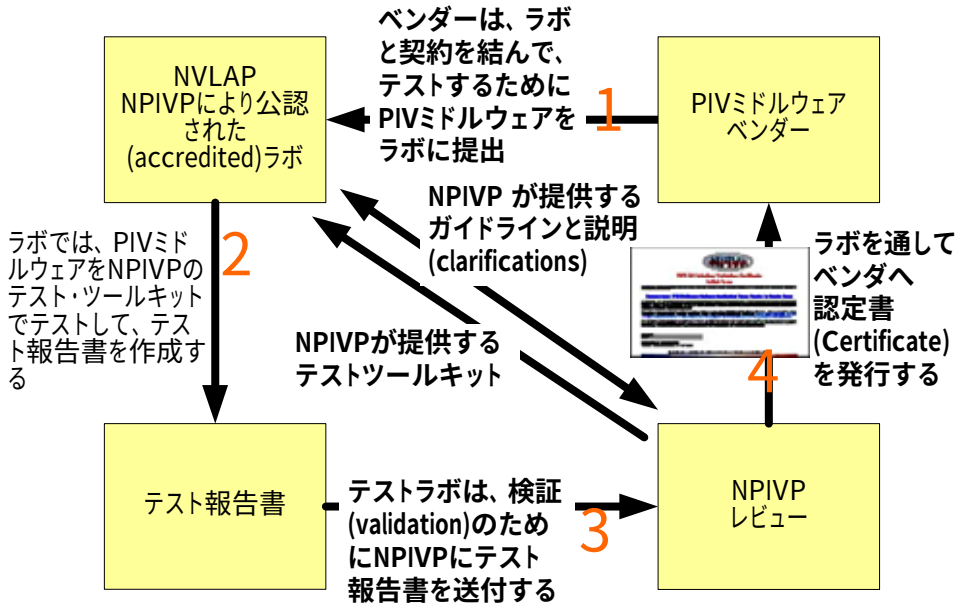



図 22　PIV における製品認定スキーム

イ．　全銀協 IC キャッシュカードにおける製品認定の仕組み

全銀協では、IC キャッシュカードの認定を行うため、IC キャッシュカード認定制度運営協議会（以下本項では「協議会」という）を運営している。IC キャッシュカード関連製品を提供しようとするベンダは、協議会に認定申請を行う。試験は、協議会から指定を受けた指定試験機関が行い、結果を協議会に通知する。

協議会が認定した商品は、IC キャッシュカードシステムに提供される。

以上について、図 23 に示す[27]。

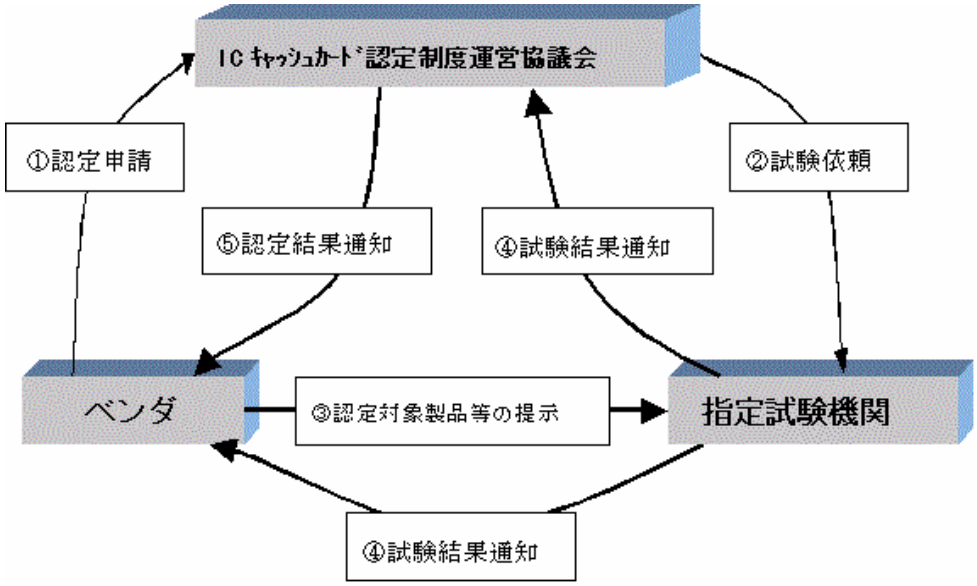



図 23　IC キャッシュカードの認定スキーム

(2) バランスの良い認定制度の検討

製品の認定を厳密に行うためには、上記の先進例に示したように、第三者機関による詳細な試験を行う方法がある。しかしながら、汎用の用途で、これから普及を図ろうとする実装規約においては、試験の時間的、金銭的コストが上昇することは、利便性と調達における安心以前に、普及の妨げになってしまうことが懸念される。

ベンダが新製品を開発･供給するための金銭的､時間的コストを極力小さくするよう検討し、国内で IC・ID カードの相互運用の実現と、供給者各社の製品開発・供給への負担の少なさをバランスよく実現する仕組みを検討する必要があると考えられる。

ひとつの案として、定められた環境で試験ツールを利用し、試験手順に沿って試験をした場合は、試験環境および結果の公表を条件に、社内のテストでも製品の証明を認める考え方もある。

これにより､事実上開発ベンダが社内でテストツールを利用してテストした製品を供給可能な環境が整備されることになるため､製品認定のためのコストや市場に提供されるまでの期間が短縮されることになるため、標準に準拠した製品の普及が期待される。

### 7.5.4. 認証用データの相互運用環境の整備

技術的な内容を整備することにより、IC・ID カードの相互運用可能性を確保することは可能になるが､一方で､認証用データの利用､認証局による証明書の検証が､特定用途に限らず、一定の認証ポリシーのもとで、汎用的に認証を受けられなければ、相互運用可能性が生かされることはない。

IC・ID カードの認証データを実際に相互運用するためには、認証データを発行して IC・ID カードに格納し、また、IC・ID カードの暗号処理を証局の関係者間での協調が必要である。

認証用データの用途を相互に解放することや、認証局が外部からの検証に対応すること、認証局同士が相互認証することで複数の認証局が認証する IC･ID カードが相互に利用できるようにすること、などの環境整備が必要と考えられる。

# 8. 調査のまとめ

シーズ調査とニーズ調査を通じた、「IC・ID カードの相互運用可能性向上に係る基礎調査」の成果について、下記に総括する。

調査報告書をまとめるにあたり、シーズ調査においては、多くの標準化文書と関連した技術文書を読み下した。また、かなりの量のミドルウェアの実装のソースコードを読んだ。海外の事例研究を行なったため、結果的に海外におけるいくつかの相互運用可能性の問題を解決するためのアプローチを知ることもできた。

相互運用可能性の問題を解決するための IC カードの仕様の標準化活動は、これまでにも様々な努力がなされている。これは、もちろん非常に重要なことであり、こうした努力なしでは、相互運用可能性の問題の解決はありえない。しかし、本調査では、これまでと異なった見方、ないし、足りない点がないかということを探し出すことも大きなテーマであった。こうした観点では、米国の PIV と欧州の OpenSC は、新しい流れに見えた。

HSPD-12 がドライブとなっている PIV は、米大統領令からのトップダンな施策の産物であり、OpenSC は、オープンソースと言うことで、ボトムアップなものであり、まったく正反対のプロジェクトである。しかし、双方からの知見は、複雑な標準仕様の相互運用可能性の問題を解決は、標準仕様からだけのアプローチでは成し得ないかもしれないということであった。

PIV の Certification 制度である NPIVP は、暗号製品の評価基準 FIPS-140 の Verification 制度である CMVP に似た制度となっている。FIPS-140 は、米国政府機関が暗号製品を調達する際の基準であるが、実際には、産業界においても暗号製品のデファクトの標準となっている。暗号製品の評価の難しさ故、客観的な評価がもとめられ、CMVP のような評価・認定制度が重要な意味を持つ様になった。そして、米国連邦政府機関の調達がドライブ役となり、産業界においても暗号製品のデファクトの基準となった経緯がある。同様に、IC・ID カードの相互運用可能性を確保した製品も同じように非常に評価が難しい。NPIVP のような評価・認定制度がデファクトの標準を作り出す可能性がある。

OpenSC は、多くのカード OS(カードエッジ・インターフェース）をサポートし、また、欧州各国の eID を動作させることができる。OpenSC プロジェクト自体の目標は、既存のカード、既存の eID をサポートするということであって、必ずしも標準化を推進するものではない。しかし OpenSC でなされている努力は、標準がどうあるべきかと示し、また、机上の空論でない実装を示している。

ニーズ調査のインタービューにおいて仕様策定関係者、調達者、利用者、供給者、国際標準化関係者と、それぞれの視点からの有意義で貴重なご意見を頂き、多くの知見が得られた。同時に、幅広い関係者間で共通の認識を持つことの難しさも実感し、改めて本調査でやるべきことの意義を再認識させられた。

IC・ID カードの実装、展開には、マルチセクター、マルチベンダー、マルチプラットフォームでの利用、すなわち、従来考えられていた利用範囲、応用範囲等のドメインの枠を超えた

幅広い相互運用可能性の確保が欠かせないが、こうした相互運用可能性の確保の問題解決については、様々な関係者による、幅広い標準技術や実装技術等の適切な理解と、積極的な取り組みが必要になると考えられる。

また、ビジネスとして成り立つだけのフレームワークの確立も非常に重要な要素である。ビジネスとして成り立たなければ、標準化された IC・ID カードの実装と展開は進まない。

提言では、シーズ調査とニーズ調査の結果を踏まえ、また、ビジネスが成り立つフレームワークの確立と言うことも含め、ミドルウェアを含めた IC・ID カードサービスとしての「実装規約」、「参照実装」、「テスト環境」、「Certification 制度」などの整備に関する提案をしている。これらは、かなりチャレンジャブルな提案ではあるが、こうしたことは、海外においてもその兆しが見えるということが認識される必要がある。

最後に、本調査報告書が、今後の IC・ID カードの相互運用可能性の問題の解決に寄与し、そして、よりよい IT 社会の実現に向けての一助になれば幸いである。

# 参考文献リスト


[1] 公的個人認証サービス都道府県協議会, “公的個人認証サービス利用者ガイド”, 2006 年 11 月, http://www.jpki.go.jp/guide/jpki_sgd_usersguides.pdf

[2] 総務省, “IC カード個人利用の普及課題検討報告書”,2006 年 3 月

[3] 厚生労働省, “厚生労働省 HPKI 認証局の構築･運営事業について（案）” (第2回 保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議 資料), 2006 年 3 月, http://www.mhlw.go.jp/shingi/2006/03/dl/s0330-8c.pdf

[4] 財団法人ニューメディア開発協会, “代理申請の制度的･技術的課題について”, 2002 年 3 月, http://www.nmda.or.jp/nmda/soc/pdf1/dairi20020322.pdf

[5] 財団法人自治体衛星通信機構, “公的個人認証サービスに対応する IC カードリーダライタの仕様及び適合性検証の実施について”, http://www.lascom.or.jp/jinfo/bosyu.pdf

[6] ISO/IEC JTC 1, “ISO/IEC FCD 24727-2 Identification cards -- Integrated circuit card programming interfaces -- Part 2: Generic card interface”, Dec. 2005

[7] ISO/IEC JTC 1, “ISO/IEC 7816-15:2004 Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application”, Jan. 2004

[8] ISO/IEC JTC 1, “ISO/IEC CD 24727-3 Identification cards -- Integrated circuit card programming interfaces -- Part 3: Application interface”, Dec. 2005

[9] CEN/ISSS Workshop eAuthentication, “Towards an electronic ID for the European Citizen, a strategic vision”, Oct. 2004

[10] 有限責任中間法人 日本 IC カードシステム利用促進協議会 ウェブサイト, http://www.jicsap.com/

[11] 財団法人医療情報システム開発センター, “保健医療カードシステム標準化マニュアル” 1994 年 3 月

[12] 財団法人ニューメディア開発協会 ウェブサイト, http://www.nmda.or.jp/

[13] 公的分野における IC カードの普及に関する関係府省連絡会議, “公的分野における連携ICカード技術仕様”, 2004 年 3 月改定, http://www.kantei.go.jp/jp/singi/it2/others/siyou040312.pdf

[14] 総務省自治行政局自治政策課 (第13回住民基本台帳ネットワークシステム調査委員会 資料), “公的個人認証サービスの最近の動向”, 2006 年 9 月, http://www.soumu.go.jp/c-gyousei/daityo/pdf/060908_1_s10.pdf

[15] 財団法人自治体衛星通信機構, “公的個人認証サービス利用者クライアントソフト 技術仕様書“, 2004 年 12 月, http://www.lascom.or.jp/jinfo/software.html

[16] 日本商工会議所, “ビジネス認証サービス”(ウェブサイト) , http://ca.jcci.or.jp/

[17] 電子入札コアシステム開発コンソーシアム ウェブサイト, http://www.cals.jacic.or.jp/coreconso/

[18] 東京工業大学, “東工大ポータル”(ウェブサイト) , http://portal.titech.ac.jp/guide/index.html

[19] 財団法人医療情報システム開発センター, “医療用公開鍵基盤ガイドライン（暫定版）”, 2004 年, http://www.medis.or.jp/6_pki/file/hpki_gl.pdf

[20] 厚生労働省, “保健医療福祉分野 PKI 認証局 証明書ポリシー”, 2005 年 4 月, http://www.mhlw.go.jp/shingi/2005/04/s0401-1.html
[21] 高度情報通信ネットワーク社会推進戦略本部, “e-Japan 戦略”, 2001 年 1 月, http://www.kantei.go.jp/jp/singi/it2/index.html
[22] 高度情報通信ネットワーク社会推進戦略本部, “IT 新改革戦略”, 2006 年 1 月, http://www.kantei.go.jp/jp/singi/it2/index.html
[23] G. W. Bush, “Homeland Security Presidential Directive/Hspd-12", Aug. 2004, http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html
[24] D. Branstad, et al., “Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations”, NIST Special Publication 800-79, Jul. 2005, http://csrc.nist.gov/publications/nistpubs/800-79/sp800-79.pdf
[25] R. Chandramouli, et al., “PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)”, NIST Special Publication 800-85A, Apr. 2006, http://csrc.nist.gov/publications/nistpubs/800-85A/SP800-85A.pdf
[26] R. Chandramouli, et al., “PIV Data Model Test Guidelines”, NIST Special Publication 800-85B, Jul. 2006, http://csrc.nist.gov/publications/nistpubs/800-85B/SP800-85b-072406-final.pdf
[27] IC キャッシュカード認定制度運営協議会 ウェブサイト, http://www.ictac.jp/kaisetsu3.htm