

ICカード・ICチップ

1. 主な事業内容

当協会では、10数年前からICカードに関する基盤技術の開発、標準化、応用システムの開発、国際的な相互運用性等についての調査研究開発事業を積極的に進めています。

最近では、全国21地域を対象とした「IT装備都市研究事業」の実施、非接触ICカードの「住民基本台帳カード」への応用分野調査、ICチップを利用した「電子パスポートの相互運用性に関する研究」等を行っており、日本国内だけでなく世界的にも大きな貢献をしています。今までに実施した主な事業は、下記のとおりです。詳細については、下記のホームページをご参照ください。

URL <http://www.nmda.or.jp/nmda/ic-card/>

1. 内容アクセスマネージャ（CAM）の開発

ICカード内データのオープン化を実現するCAM（Content Access Manager、略称CAM）ソフトウェアの開発を行っています。CAMは、当時の自治省地域カードシステムへの採用、厚生省ガイドラインにおける推奨の他に、経済産業省の事業の一環としてとして北海道滝川市、兵庫県三木市、洲本市、五色町で使用されており、改良が重ねられています。また、国際的な相互利用を可能にするG7 - CAMを、EUと役割分担し開発しています。

2. 新世代ICカード共通システムの開発

利用者がICカードを安心して便利に継続利用できるようにするため、新世代ICカードシステムの

ICカード・ICチップ事業年表

平成/年度	6年度	7年度	8年度	9年度	10年度	11年度	12年度	13年度	14年度	15年度	16年度	備 考
1.ICカード・ICチップ基盤技術の研究開発	←—————→ (ISO準拠ICカード、非接触ICカード、新世代ICカード、多機能ICチップ、次世代インターネット連携)											
CAMの開発	←—————→ (内容アクセスマネージャの研究開発)											
医療用ICカードへの応用研究	←————→ (光カードとICカードのハイブリッド化)											
ICカード日欧の連携	←—————→ (ICカードに関する日欧間の技術的整合性等調査)											
多機能ICチップ	←————→ (多機能ICチップの新領域サービス)											
2.電源地域における広域・多目的利用ICカード情報化モデル事業	←————→ (北海道滝川市)				←————→ (岐阜県益田群)				←————→ (神奈川県横須賀市)	←————→ (新潟県柏崎市)		
3.ICカードの普及によるIT装備都市研究事業								←————→ (21地域で実施)	←————→ (フォローアップ)			
ICカードフェアの開催										←————→ (ICカードの現状展示)	北の丸科学技術館にて開催	
CDCに関する研究開発・実証実験	←————→ (ICカードと連携するコミュニティデータセンタの構築)											
先進的ICカードアプリケーションの開発・実証実験										←————→ (ICカードに搭載するアプリケーション開発)		
4.非接触ICカード普及センター（CLIC）事業										←————→ (非接触ICカードの発行)	←————→ (カード/リーダの互換性検証)	住民基本台帳カードの自治体からの受託発行各種コンサルティング事業
5.バイオメトリクス（生体認証）・e-パスポート開発事業	←————→ (可搬型メディアへの応用、電子パスポートへの応用研究、顔画像の品質と顔認証精度調査)											
	←————→ (バイオメトリクスセキュリティコンソーシアム)											

具体像の提示と技術的可能性の検証を目標に開発を行いました。アンテナ内蔵非接触タイプインタフェース（ISO14443準拠）を採用し、ハイセキュリティ・マルチアプリケーション対応で、サービスの相互運用性に優れたシステムアーキテクチャを提示し、互換性を損なう様々な課題等の解決に取り組みました。

3. 日欧ICカードシステム相互運用性実現のための基盤技術開発

ICカードの利用が進んでいる欧州との間で、ICカードシステムの相互運用を実現するための技術面・アプリケーション面での協調を図る基盤技術開発を行っています。これに応じるため、ICカードとリーダ・ライタ間の非接触インタフェース、ICカードのセキュリティ基準等の技術開発や国際基準に合致する研究を実施しています。

4. セキュアICチップおよび運用フレームワークの研究

次世代のネットワーク社会では、コンピュータを始め携帯電話やPDA（小型携帯端末）等の普及とともに必要な情報を、いつでも・どこでも・安全に活用できる社会、いわゆるユビキタスコンピューティング社会が到来すると考えられています。この情報経済基盤整備事業の一環として、ネットワーク上で人や機器の安全確実な認証を実現するため、ネットワーク端末等に搭載するICチップ（多機能IC）および運用フレームワークの研究を行っています。

5. 多目的利用ICカードシステム実証実験

多目的利用ICカードシステム（CAMを使用することによって、ICカードに商店街ポイントサービスと健康管理サービス機能を持たせたシステム）の実証試験を北海道滝川市で実施しました。また、ICカード上のサービス機能の追加・削除を可能とする広域・多目的利用実験（自治体による広域での証明書等発行と保養施設ポイントサービス）を岐阜県益田地域で実施しました。

さらに、新世代ICカード共通システムの成果をベースにして、安全に共通利用できる次世代ICカードシステムの実証実験を神奈川県横須賀市で実施しました。

6. ICカードの普及等によるIT装備都市研究事業

ICカードは、IT社会の参加者が自分の情報を安全確実に管理・利用することを可能とする重要な

キーデバイスです。本研究事業は、住民がICカードを利用して簡単にIT社会に参加することができ、その多大なメリットを享受できることを明確にしました。この成果は今後のIT社会推進のモデルとなる事例です。

当協会は、平成13年度において経済産業省から委託を受け、全国21地域で100を越えるICカード応用システムを開発し、120万枚のICカードの配布と9,000台のリーダ・ライタの提供を行い、システムの相互互換性や運用・管理方法といった技術的側面や多目的利用を前提とした費用分担等の社会的側面等、各地域における大規模な実証実験を行いました。

7. IT装備都市研究事業を基礎とした先進的ICカードアプリケーションの開発

IT装備都市研究事業の実施内容を活用し、ICカードの利用をさらに促進する下記の先進的なICカードアプリケーションの研究開発および実証実験を行いました。

- マルチアプリケーションICカード環境下での電子チケット・サービスの研究
- 地域行政と地域商店街および大規模量販店における官民ポイント互換サービス等の研究
- IT装備都市カードによる広域の決済・ポイント・コンビニ民間連携サービス等の研究

8. IT装備都市研究事業を基礎としたコミュニティ連携を推進するデータセンター（CDC）の開発

マルチアプリケーション対応ICカードシステム、その他のシステム運用、リソースの共有化およびASP機能等を担うコミュニティ・データセンター（CDC）に関する研究開発・実証実験を行いました。

9. 多機能ICチップ等を活用した新領域ITサービスに関する研究開発・実証事業

ユビキタスネットワーク社会が到来すると考えられますが、そこにおいては十分な安全性を備え、利用者に安全感を与え、利便性を享受できるセキュアでかつ適切な認証の実現が不可欠です。これらが実現可能な要素技術であるセキュアICチップ等を活用した新領域ITサービスの実証実験によりシステム導入に伴う技術面・利用面での課題を検証します。

10. 住基カードへのIT装備都市事業アプリ応用事業

複数の地域において、IT装備都市研究事業で開発され広く利用されているアプリケーションを新

たな住基カードに移植し、地域におけるICカードを中心とする情報インフラ整備に寄与しています。

11. 非接触ICカード普及センター（CLIC）の運用、「住民基本台帳カード」含む非接触ICカードの発行受託

平成15年5月1日付けで当協会内に「非接触ICカード普及センター」（CLIC：Contact-Less IC card deployment center）を設立しました。CLICでは、下記の業務を行っています。

(1) 非接触ICカード発行業務

市区町村、法人等からの委託により、国際規格に準拠した非接触近接型ICカードタイプBの各種カード発行業務を行っています。

(2) 互換性検証業務

非接触ICカードや非接触リーダ/ライタの互換性を検証します。互換性が検証された製品については、メーカーおよび製品名の公表と、該当メーカーには互換性検証確認済の証明書を発行します。

(3) 技術コンサルティング業務

地方自治体が非接触ICカード、リーダ/ライタ、カード発行機等を導入する際の技術的な問題解決のため、また、標準仕様の普及活動のために技術的なコンサルティングを実施しています。

12. バイオメトリクスを可搬型メディアに応用するための技術調査

バイオメトリクスの可搬型メディアに関して、

顔画像の認識システムを国内統一して開発するための共通仕様技術を作成し、非接触ICカードの互換性に関する評価試験方法等を確定し、小ロットの実証実験を実施するとともに国際標準化確定のための提案を行っています。

13. 電子パスポートの相互運用性

電子パスポート用の「近接型通信インタフェース実装規約書（案）第1.0版」の公開を行いました。（2004年4月28日）

本実装規約書は、当協会が平成15年度のビジネス機械・情報システム産業協会（JBMA）の委託を受けて、次世代の電子パスポートである、「バイオメトリクス旅券の相互運用性調査」の付属資料として関連企業との間で検討し、とりまとめ提案したものです。

非接触近接型ICカードの実装規約（第2.0版）をベースに、非接触近接型通信インタフェースをバイオメトリクス旅券に適用した場合の実装規約案であり、今後、国内だけでなくSC17やICAO等の国際標準化機関に提案していくこととしています。

「バイオメトリクス旅券用近接型通信インタフェース実装規約書（案）」

URL <http://www.nmda.or.jp/epas/kiyaku1.0ver.pdf>

14. バイオIDにおける各種顔画像の品質と顔認証精度に関する調査

Personal ID Documents用の各種顔画像の品質と顔認証精度に関する調査レポートです。電子パスポートの基礎技術となる部分です。（2004年3月31日）

2. プロジェクト事例

- (1) ICカードの国際標準化と最新の動向
- (2) ICカードに関する日欧間の技術的整合性等
- (3) ICカードの普及等によるIT装備都市研究事業

- (4) 非接触ICカードの互換性確保への取り組み
- (5) 電源地域情報化推進モデル事業
- (6) バイオメトリクスとは

ICカードの国際標準化と最新の動向

（出典：研究成果レポート8号 2002.11）

1. 外部端子付ICカードの開発背景

1981年のISO/TC97/SC17専門委員会（当時は磁気ス

トライプ付識別カードと関連機器を担当）国際総会において、フランス標準協会から新しく「外部端子付ICカード」に対する国際規格開発の必要性が提案された。SC17専門委員会（以下SC17と略）では、ISOガイドラインの手続を経て、1982年に規格開発グループSC17/WG4を発足させた。しかし、当時は、各国共に磁気ストライプ付カードが拡大期であったこと、半導体集積回路（以下ICチップと称す）は、汎用CPUが8bit、メモリーは

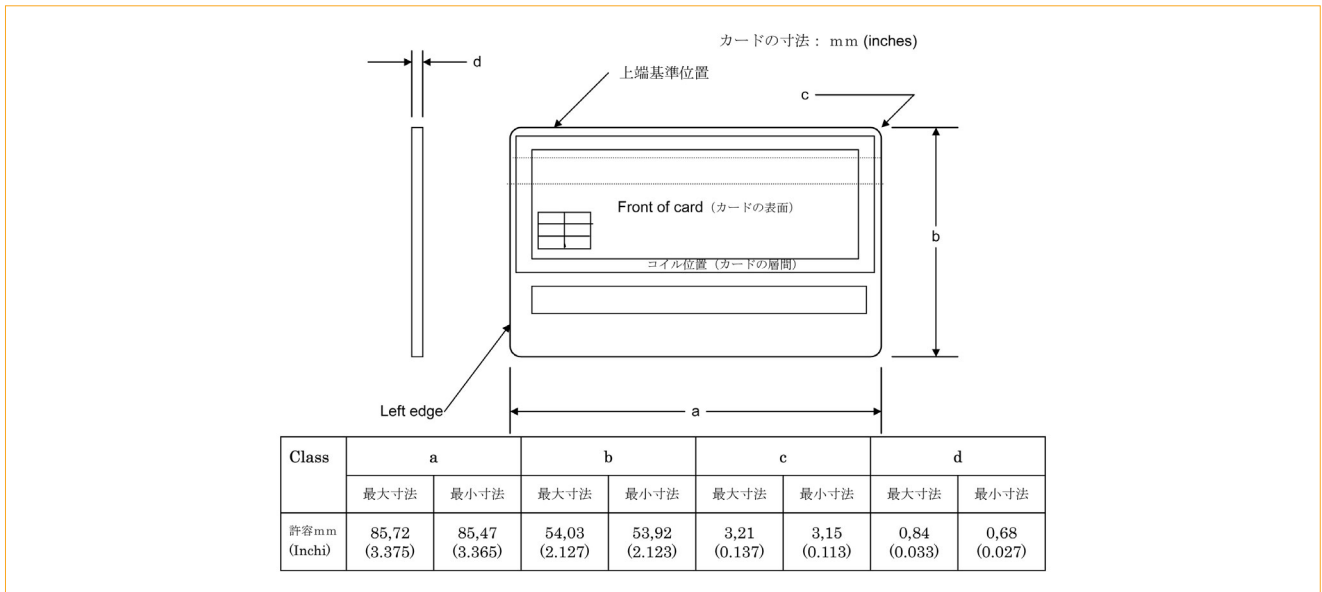


図1 ICカードの外形寸法図

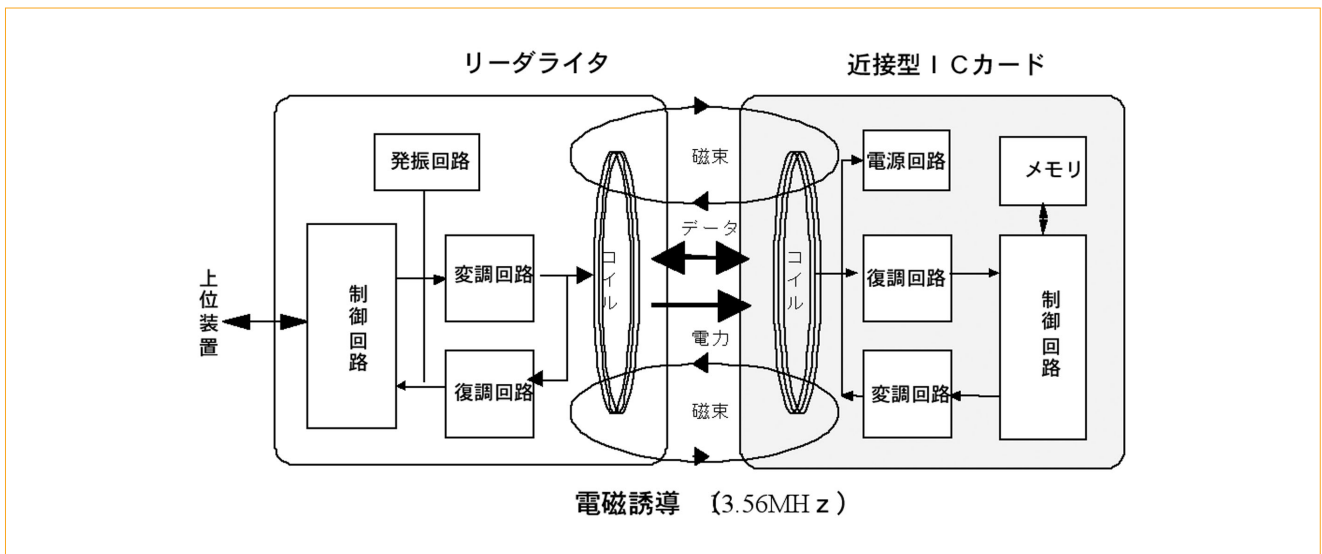


図2 コンタクトレスICカードとリーダ・ライタ間の基本原理

4k-bitのN-MOS・EPROM(12v・紫外線消去型)と個別に販売されており、ICカード用のCPUとMemoryを1チップ化したチップは、入手困難であったこと等、試作も困難であった。そのために、当時フランスから提案された標準作業案(Working Draft)は、専用に開発した独自仕様の8bit-CPUと、4kbit-EPROM(12v・紫外線消去型)を1チップ(他にRAM/98B、ROM/2KB)化したチップを背景として作成されていた。また、IC回路の設計技術も3ミクロン幅であり、チップサイズの制限から、カードのOSも「バイト伝送方式」で金融決済用途等の単一利用目的向けであった。(書替え不可のため、金融用途で150回で使い捨てとなる)

一方、わが国において1985年に試作開発したチップは、8bit-CPUと16kbit-EEPROM(5v・電氣的消去型)を1チップ(他にRAM/128B、ROM/8KB)化し、

カードのOSも「ブロック転送方式」で当初から多目的利用が可能な国際規格を提案した。

SC17では、2方式の国際規格開発の必要性を認めて、外部端子付ICカードでは、カードの初期応答情報にカード識別のためのコードを設け、技術革新に合わせて拡張できる規格となった(参考:タイプT=0(バイト伝送)、タイプT=1(ブロック伝送)、2、3、...)。規格はパート1~6の基本規格と、用途に応じて任意に採用するためのパート7~12、15の応用規格がある。また、高度なセキュリティを必要とする用途に対応するため、1995年にはセキュリティ系のコマンド改訂と共に、暗号計算のための専用コプロセッサを搭載するICチップを開発し、非対称暗号方式(RSA、鍵長-512bit~)の採用を可能にしたICカードが開発された。

さらに、2001年9月11日にUSAで発生した同時多発テロを契機に、本人の真正性を厳格チェックのためバイオメトリクスデータ(指紋、顔写真、虹彩等)をICカードに記載して、個人識別に利用するための標準化も始まった。

外部端子付ICカードの主な用途は、国際クレジットカード(VISA、MasterCard、Europay、JCB等)及び銀行キャッシュカード等の金融決済系に利用されている。

2. 非接触ICカードの開発背景

1989年のISO/IEC JTC1/SC17(識別カードと関連機器と改称)国際総会において、ドイツ標準協会から新しく「コンタクトレスICカード」に対する国際規格開発の必要性が提案され、ISOガイドラインの手続を得て1989年に規格開発グループSC17/WG8として発足した。外部端子付ICカードでは使用が困難な屋外利用、端末保守費用の軽減及びスピード処理を要する鉄道・運輸業務用に、規格開発が始まったが、カードとリーダ/ライタの交信距離で、次の3種類に区分して規格を作成することとなった。ISO/IEC10533(密着型、

~3mm)、ISO/IEC14443(近接型、~10cm)、ISO/IEC15693(近傍型、~70cm)があり、これ等の内で近接型は、利用業務が多く、各国での開発競争が規格開発の提案(タイプA/フィリップス他、タイプB/モトローラ他、タイプC/ソニー日本、等)にも影響して、規格制定までに特許問題を含めて調整に困難を極めた。特にわが国では、タイプCが国際規格に不採用となった後も交通系の統一仕様書にタイプCが採用され、JR東日本旅客鉄道が2001年11月から本格的実用を開始した。このためにわが国ではタイプC案を修正し、国際規格として追補させるため、タイプAの改訂作業に併せて高速処理用(848kb/s~6.78Mb/s)の追加規格としての必要性を付記し、新国際規格開発作業の手続を行った(2002年9月)。

近接型カードの用途は、過酷な環境での使用が可能なこと、カード所持者の使用が容易なこと、保守が殆ど不要なこと等から用途は拡大し、わが国に於いては既に交通定期券が実用を始め、住民基本台帳カードは、2003年8月から実用を予定している。また、運転免許証、パスポート等では、規格開発の進展に合わせて世界各国で導入のための実証計画が具体化しつつある。



ICカードに関する日欧間の技術的整合性等

(出典：研究成果レポート8号 2002.11)

1. はじめに

本稿は、平成13年度に行政系ICカードシステム普及促進事業で実施した「ICカードに関する日欧間の技術的整合性等将来動向に関する調査研究事業」の成果とその内容について報告するものです。

クレジットカードや乗車券等の分野での急速な普及や経済産業省によるIT装備都市研究事業での大規模な実証実験を証左としてICカードが我々の生活に浸透する日も目前に迫っています。その一方で実運用を通じて発見された新たな課題や現在の技術と将来動向から予測される新たな課題が提起されています。代表的な課題の一つとして、国際間におけるICカードの相互運用性の問題が挙げられます。

この課題に対処するために、これまでICカードの先進的利用を行っている欧州と日本との間で、ICカードの相互運用性を実現するための技術及び応用面での協調を図ってきています。

本調査研究事業の狙いは、これまでのICカードに関する日欧連携の研究活動および成果の整理を行うとともに、日欧間の今後の課題、将来動向を探ることにあります。

2. 現在までの日欧共同プロジェクト総括

(1) 日欧共同プロジェクトの歴史

ICカードに関する日欧連携の取り組みは、1995年の先進7ヶ国による情報サミットでの医療・福祉分野を対象とした国際的共同プロジェクト「GLOBAL HEALTH CARE APPLICATION」のサブプロジェクト6(SP6)が発端になっています。SP6におけるヘルスケアカードシステムの相互運用性の議論を受けて、欧州では、欧州各国におけるICカードシステムの相互運用性を実現するためのフィージビリティ調査、我が国は相互運用性を実現するための基盤技術である内容アクセスマネージャを提案してきました。この発展形が日欧間でのICカードに関する共同プロジェクトの取り組みに繋がっています。

平成10年度(1998年)以降、産業・社会情報化基盤整備事業(平成10年度第三次補正予算)において「日欧ICカードシステム相互運用性実現のための基盤技術開発」を実施しました。

平成13年度(2001年)に入り、我が国の次世代ICカードシステム研究会(NICSS)と欧州委員会におけるスマートカード・チャータ・タスクフォース(SCC)との合同会議が開始されるなど、日欧におけるICカードに係る共同事業がより活発になってきています。

このような情勢のもと、平成13年9月(2001年)に新たにニューメディア開発協会(NMDA)と、欧州ICカ

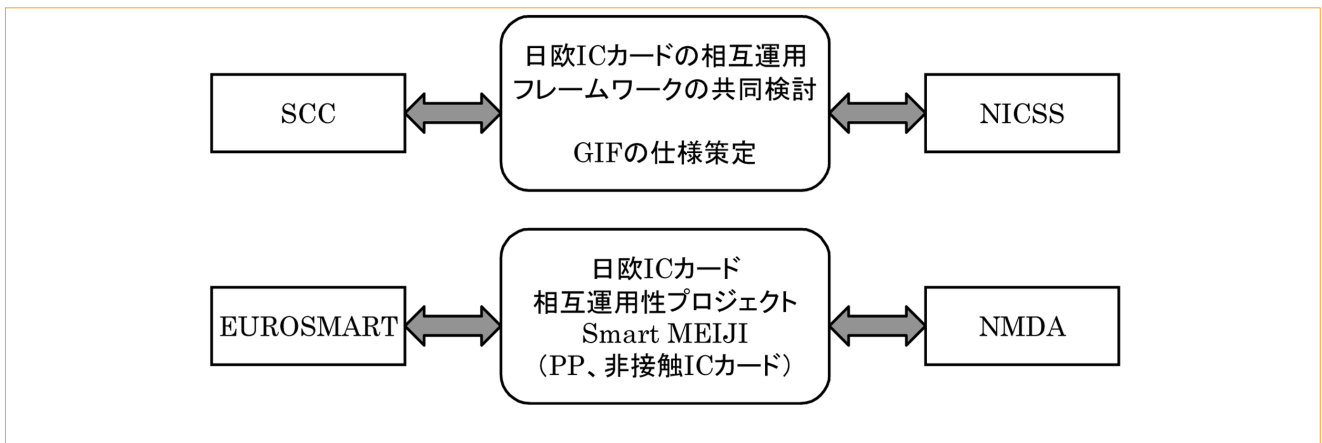


図1 日欧連携のフレームワーク

	概要
次世代ICカードシステム研究会 The Next generation IC Card System Study group, NICSS	公共分野における次世代ICカードシステムの共通プラットフォームの検討と、その普及推進に向けた社会情報基盤の形成に寄与するため、民間企業17社を发起人として、平成10年12月9日に設立
ニューメディア開発協会 New Media Development Association, NMDA	ニューメディアに関する調査開発、普及啓発などを行う経済産業省の認可団体であり、1972年に設立された財団法人映像情報システム開発協会が母体
スマートカード・チャータ・ タスクフォース Smart Card Charter task force, SCC	欧州委員会・社会情報局（DG13、ベリユー総局長）の後押しで、欧州におけるICカードの標準化・普及組織としてスマートカード・チャータのタスクフォースが組織された。350団体1000人登録
欧州ICカード工業会 EUROSMART	欧州のカード関連メーカーの業界団体

表1 各組織の紹介

ード工業会(EUROSMART)との間で近接型非接触ICカード分野における日本と欧州の協力体制を確立するためのジョイントプロジェクトであるSmart MEIJI(Mutual European and Japanese Initiative for Inter-operability)プロジェクトを発足しました。このプロジェクトは、20ヶ月間の活動を予定しており、その間に、セキュリティと非接触カードでワークショップをそれぞれ開催し、平成15年4月に完了する予定です。

(2) ICカードに関する日欧連携のフレームワーク

現在、日欧連携のフレームワークとしては、図1に示すように2つの主要な取り組みが挙げられます。

1つ目は、次世代ICカードシステム研究会(NICSS)と、欧州委員会におけるスマートカード・チャータ・タスクフォース(SCC)との間の共同検討プロジェクトです。ICカードの相互運用フレームワークの策定を目的として、現在、「NICSS推奨方式(NICSSフレームワーク)をベースとして、ICカードによる識別、認証、電子署名のための相互運用フレームワークである、グローバル・インターオペラビリティ・フレームワーク(Global Interoperability Framework, GIF)の仕様策定を行っています。

共同検討の最終目標としては、以下の2つを挙げています。

- ICカードシステムの共通フレームワーク作成
- ICカードシステムの仕様の統一

2つ目は、財団法人ニューメディア開発協会と欧州ICカード工業会の間での共同検討プロジェクトです。現在は、日本と欧州の協力体制を確立するためのジョイントプロジェクトである相互運用プロジェクトSmart MEIJIが進行中です。セキュリティ(Protection Profile, PP)と非接触ICカードの特定技術分野の共同検討を行っています。

日欧連携の目的として、以下の3つを挙げています。

- 日欧間の協力体制を推進するための基盤構築
- セキュリティにおけるコモンクライテリア(セキュリティ評価基準)の作成
- 非接触カードシステムの進展

3. 日欧共同プロジェクトの将来動向

ICカード分野で日欧の取り組みについて動向調査と有識者へのヒアリング調査を実施し、今後日欧で協調

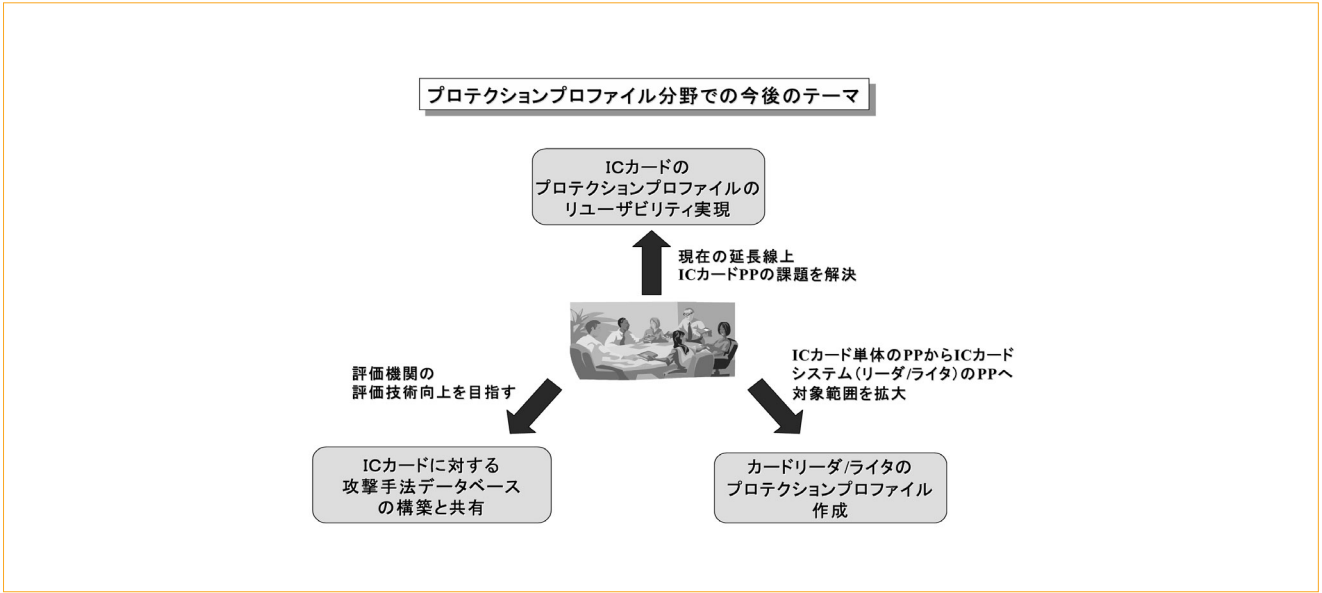


図2 プロテクション・プロファイル分野での将来動向

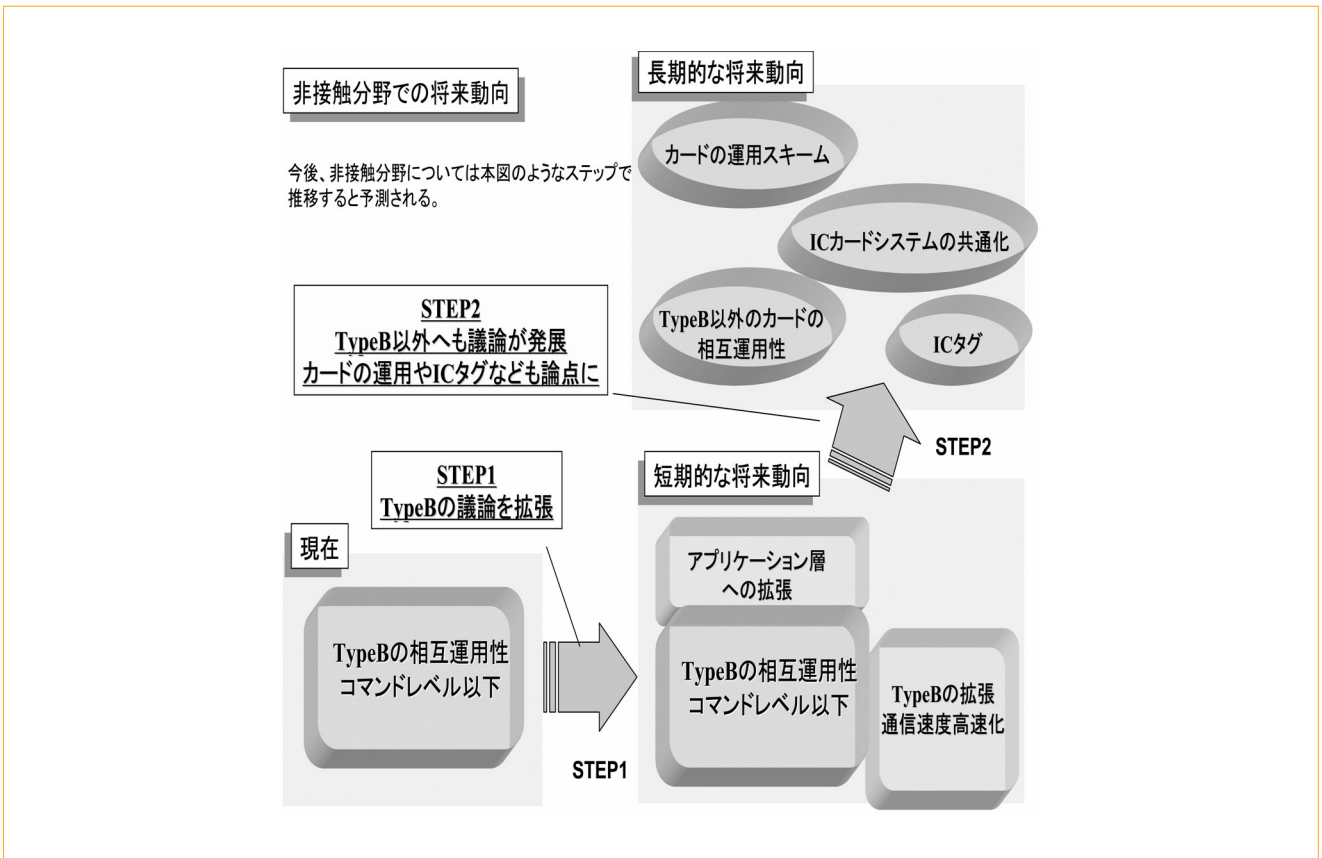


図3 非接触分野での将来動向

して対処すべき課題とテーマを抽出しました。主要なものを以下に紹介します。(図2：プロテクション・プロファイル分野での将来動向、図3：非接触分野での将来動向)

(1) プロテクション・プロファイル (PP) の今後の主なテーマ

PPのリユーザビリティの実現：複数の製造業者が

カード製造に関与している場合の、前工程のセキュリティ評価を次工程の製造業者に引き継ぐなど評価のリユーザビリティの実現

ICカードリーダライタのPP作成：ICカード単体のPPからICカードシステムのPPへ対象範囲拡大を目的としたICカードリーダライタのPP作成

ICカードに対する攻撃手法データベースの構築と共有

(2) 非接触ICカードの今後の主なテーマ

短期的には、TypeBのICカードにおける相互運用性の完全性が高められていくと共に、議論が拡張されてアプリケーション層での相互運用性や通信速度の高速化についても協議されるようになると予測しています。更に長期的には、TypeBのICカードの相互運用性から議論が発展して、TypeB以外のICカー

ド、ICタグ、ICカードシステム、カードの運用スキーム等へ議論が発展していくものと報告しています。

今後の主なテーマとしては以下が考えられます。アプリケーション層での相互運用性の確認カード及びリーダー間通信速度の高速化相互運用性確保のための各社ICカードのノイズ分析

ICカードの普及等によるIT装備都市研究事業

(出典：当事業報告書 2002.3)

1. はじめに

現在、世界的規模で生じている産業・社会構造の変革、いわゆるIT革命に関しては、我が国においても官・民が一体となって戦略的かつ重点的に取り組むことが急務となっている。政府は、世界有数のIT社会を確立すべく、その方向性を具体化するための検討を行い、平成12年度補正予算においてIT革命への対応のための措置を講じた。

「ICカードの普及等によるIT装備都市研究事業」(以下、「本研究事業」という)は、この平成12年度補正予算による事業であり、経済産業省より財団法人ニューメディア開発協会(以下、「当協会」という)が委託を受け実施した。

本研究事業は、特に公的分野において共通的に利用されることを想定し、マルチアプリケーションICカードシステムの研究開発を行うとともに、本システムを行政・民間アプリケーションに組み込んで、全国21の地域(54市町村)において実証実験を行ったものである。

開発事業においては、非接触マルチアプリケーションICカードやリーダー、運用管理システムの共通仕様を策定し、本仕様に基づいて研究開発を行い、その成果の有効性を実証事業において検証した。ICカードを、21地域合計で約120万枚を住民等に配布するなど、非接触マルチアプリケーションICカードの実験としては、世界初の試みとなっている。

また、ICカードシステムの運用ガイドラインや関係者間で取り交す規約の検討など、運用に係る社会的・制度的課題についての検討も併せて行っており、本研究事業の成果は、今後のIT社会の実現において有用なものとする。

2. 開発事業

開発事業では、ICカードシステムの研究開発の

要素として、次のテーマを設定し、マルチアプリケーションICカードシステム(ICカード、リーダー、運用管理システムなど)の研究開発、システムの相互運用性の確保、高度な運用管理機能の実現等の研究開発を実施した。

- テーマ1：IT装備都市研究事業に利用するICカードシステムの機能仕様の研究
- テーマ2：IT装備都市研究事業に利用するICカードシステムの品質仕様の研究
- テーマ3：IT装備都市研究事業に利用するICカードシステムのセキュリティ仕様の研究
- テーマ4：IT装備都市研究事業に利用するICカードの相互運用性の研究
- テーマ5：IT装備都市研究事業に利用するICカードの製造実現性の研究
- テーマ6：IT装備都市研究事業に利用するICカードの発行・運用管理に関する研究
- テーマ7：IT装備都市の将来に有効なICカード技術の研究

テーマ1～6では、3コンソーシアムが、21の実証地域において使用するICカードシステムを研究開発し、当協会を通して実証コンソーシアムへの供給を行った。また、「行政系ICカードシステムの普及促進事業」の実証地域である東京大学・杉並区地域に対しても、研究員企業によるICカード等の大量発行・配布実験を行った。

また、テーマ7では、6つの研究員企業が、将来のICカード社会に有効なICカード技術についての研究開発を行った。

3. 実証事業

実証事業は、開発コンソーシアム(テーマ1～6)から供給されたICカードシステムを活用し、地域において実証実験を行うことを目的としており、21の実証コンソーシアムが実施した。

また、各実証コンソーシアムは、ICカードシステムを組み込んだアプリケーションを開発・導入しているが、実証地域で共通的に利用され、今後

- 1 開発事業（テーマ1～6）及び大規模発行・配布実験
 次世代スマートICカードシステム開発コンソーシアム
 ICカードシステムの共通基盤技術等を研究する開発コンソーシアム
 次世代ICカードシステム基盤開発コンソーシアム
 行政系ICカードシステムの普及促進事業実施地域に対するIT装備都市ICカードの大規模発行・配布実験
- 2 開発事業（テーマ7）
 ISO 14443タイプBカード・タイプCカード共用非接触リーダライタの研究
 オープンプラットフォームによる、新世代ICカードの開発研究
 発行主体の異なるPKIカード、異なる暗号方式へのCA局認証研究
 レーザーエンレーピングを使用したカード発行システムと社会システムモデルの研究
 公共分野における非接触MULTOS OSの適用
 非接触ICカードシステムに有効な、新公開鍵暗号方式適用技術の研究

表1 開発事業一覧

コンソーシアム	実証地域
札幌市IT装備都市実証コンソーシアム 「バーチャルシティやまがた」ICカード推進協議会 「会津若松市民カード構想」推進協議会 上越IT装備コンソーシアム 横須賀・三浦・葉山地域における官民共用ICカードシステム実証コンソーシアム 電縁都市ふじさわIT装備都市研究・実証コンソーシアム 多摩地域ICカード実証実験コンソーシアム	札幌市 山形市 会津若松市 上越市 横須賀市、三浦市、葉山町 藤沢市 多摩地域（稲城市、狛江市、立川市、羽村市、日野市） 大和市 駒ヶ根市、飯島町 豊田市 多治見市、笠原町 津市 池田市、羽曳野市、枚方市（大阪府） 宝塚市、伊丹市、川西市、猪名川町 岡山市 下関市 高知市 北九州市 福岡県介護保険広域連合田川支部（田川市等10市町村） 久留米市…… 沖縄北部地区（名護市等12市町村） 介護保険共通アプリケーション開発コンソーシアム 健保・国保共通アプリケーション開発コンソーシアム
大和市全員参加型E.Community研究会 伊南コミュニティカード・コンソーシアム 豊田市ICカード利用実証実験コンソーシアム 多治見市・笠原町IT装備都市研究・実証コンソーシアム Tsuハイパー・ネットワーク・シティ・コンソーシアム 大阪スマートICカードコンソーシアム 阪神北部TIKIカードコンソーシアム 医療・介護分野におけるICカード活用とスーパー電子自治体構築研究コンソーシアム 下関市IT装備都市推進コンソーシアム こうち2001プラン推進協議会・高知県ICカード普及促進協議会（ICカードWG） 北九州市IT装備都市推進コンソーシアム 介護保険証ICカード化推進協議会	
久留米市統合ICカード研究会 沖縄北部地区医療情報研究会 介護保険共通アプリケーション	
健保・国保共通アプリケーション	

表2 実証事業一覧

- ・東京工業大学・ニューメディア開発協会共同研究
- ・プロテクション・プロファイルの作成
- ・実証実験向け近接型ICカード及びリーダライタの互換性検証
- ・都市部におけるCDCを活用したICカードシステム等の運用に関する検討・研究
- ・ICカード利用動向海外調査
- ・IT装備都市の推進方策に関する調査研究

表3 調査研究事業一覧

も普及が見込まれる健保・国保及び介護保険のアプリケーションに関しては、「共通アプリケーション」として別途、開発を行い実証地域に供給した。

4. 調査研究事業

開発事業、実証事業を円滑に推進するために、

■ 非接触ICカードの互換性確保への取り組み

(出典：研究成果レポート11号 2004.1)

1. はじめに

(財)ニューメディア開発協会では、長年にわたり公的分野を中心としたICカードの普及促進に向けた取り組みを進めてきました。

特に、平成10年度以降、国際標準化機関での非接触ICカード(ISO/IEC14443タイプB)の審議の進展もあり、「新世代ICカード共通システム」(平成10年度第三次補正事業)においてプロトタイプ開発による検証を行うと共に、その成果を基礎に「IT装備都市研究事業」(平成12年度補正事業)を通して、住民基本台帳カードの交付に先駆け、全国21地域(54市町村)において非接触、マルチアプリケーションの搭載可能な、公開鍵暗号方式をサポートした高機能なICカードによる実証実験を実施しました。平成15年8月25日からは、市区町村による非接触インタフェース仕様をベースとした住民基本台帳カード(以下住基カード)の交付が開始され、当協会の非接触ICカード普及センター(CLIC)においても、地方自治体の外部委託を受けて住基カードの発行業務を開始したところです。

本稿では、非接触ICカードの技術面での普及促進を支える重要な要素の一つである、互換性確保への取り組みについて報告するものです。

2. 取り組みの経過

我が国では、安価で簡易な磁気ストライプカードの普及が進んでいたことから、高機能、高セキュリティのICカードの普及がなかなか進まないという状況にありました。また、ICカードには、業界毎に異なる仕様が存在し、異なるICカードシステム間でICカードの相互利用が困難となり、多品種少量生産によるコスト負担が増大し、普及を阻害するという課題がありました。そのような側面から、業界横断的に利用可能な新世代ICカードの

各種の調査研究を行った。

詳細については、当協会のウェブサイト(<http://www.itcity.jp>)を参照のこと。

出現が望まれ、平成10年度末から新世代ICカードの共通利用を可能とするためのシステムアーキテクチャの検討、及びそれに基づく基盤システムの開発を目的に、「新世代ICカード共通システム」プロジェクトが開始され、非接触ICカードによる～Interoperability(相互運用性)の確保～を主要なテーマとして開発を進めました。

「新世代ICカード共通システム」プロジェクトでは、2種類のカード(標準、ミニ、後に大容量タイプも追加)と1種類のリーダライタ(接触カードの非接触カードへの置き換えを想定し、ICカードをリーダライタに挿入する利用形態、これをスロットイン型と呼ぶ)とをISO/IEC14443に準拠した仕様で異なるベンダで開発を進めました。並行して関係企業が参加した非接触ICカードの相互運用性、互換性の向上を目的に、互換性作業グループを立ち上げ、ICカードとリーダライタの互換性を確保するための実装仕様の検討を進め、成果をフィードバックし近接型通信インタフェース実装規約書としてまとめました。

開発当初は、ICカードやリーダライタの電磁波特性が悪く、電波法規上の微弱電波内ではICカードとリーダライタ間を非接触インタフェースでありながら接触させないと動作しないという、厳しい状況もありました。カード内のLSIチップの動作が不安定で、試験中に何度か動作不能に落ち入るといったこともありました。そのような試行錯誤の中で開発し、標準カードとミニカードを使用し互換性の検証を積み重ね、異なるベンダの2枚のカードを一度に重ねてリーダライタで読ませる、いわゆる2枚読みも可能であることを検証しました。これは当時としては画期的なことであり、非接触ICカードの普及に向けた大きな一歩となりました。それらの成果は、「近接型通信インタフェース実装規約書」第1.0版としてとりまとめ、平成12年12月に技術開示しました。

その後、平成12年度末から「新世代ICカード共通システム」の開発成果をより発展させ、住民基本台帳カード交付の先駆的な役割も担って、「IT装備都市研究事業」が開始され、実証地域で使用するICカードやリーダライタ、運用管理システムを開発

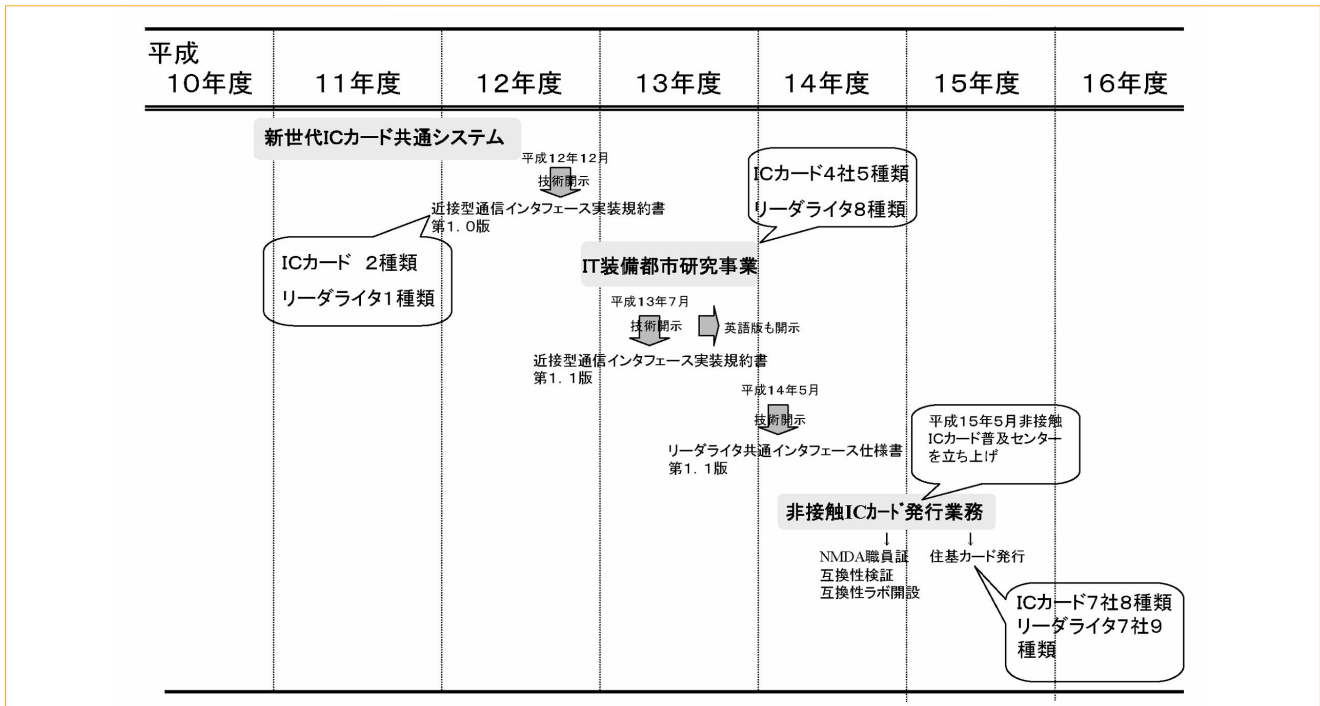


表1 非接触ICカードの互換性向上への取り組みの経過

コンソーシアムで仕様化し、共通システムとして供給することとし、「近接型通信インタフェース実装規約書」についても最新化を図ることとなりました。実装規約の改訂は、ISOでの審議の進展や、公的分野で利用するICカードでも、バスや鉄道等で利用する際の改札機にカードを置く、あるいは添える形で利用するためのリーダライタ(これを開放(オープン)型リーダライタと呼ぶ)を想定した仕様の追加要望が高まり、それらへの対応を図ることとしました。

また、このプロジェクトでは、上位インタフェースでの相互運用性向上の観点から、アプリケーション開発の効率化や可用性を高めるため、各社固有のリーダライタドライバの上位にリーダライタ共通インタフェース仕様を策定し、各社のリーダライタドライバ仕様の差異を吸収し、上位で開発されるアプリケーションインタフェースの共通化を図りました。

IT装備都市研究事業では、4社5種類のICカードと、8(社)種類のリーダライタの互換性検証を行ない、21の実証地域に動作確認されたICカード約120万枚、リーダライタ8000台の供給を行いました。実証地域での利用形態として、据置型のリーダライタにICカードを挿入して利用する形態に加え、バス乗車時の改札機(横須賀地域)や地下鉄乗車時の改札機(札幌地域)での開放型リーダライタを使用した、いわゆるタッチ・アンド・ゴーでの高速利用の実証実験も行ない、行政系の非接触ICカード(タイプB)においてもストレスなく利用出来ることを確認しました。

平成15年5月からは、非接触ICカードシステムの普及をさらに加速させていくことを目的に、当協会内に「非接触ICカード普及センター」(略称: CLIC、Contact-Less IC card Deployment Center)が設立され、長年にわたり開発実証してきた公的分野を中心とする非接触ICカードの成果を基に、住民基本台帳カードを含む各種の非接触ICカードの発行やICカードとリーダライタの互換性の検証、ICカードに関連した各種技術コンサルティングなどを、継続的な事業として実施していくこととなりました。

表1に前述した非接触ICカードの互換性向上への取り組みの経過を示します。

3. 互換性確保のためのプロセス

非接触ICカードとリーダライタの互換性を確保するためのプロセスを図1に、互換性確保のイメージを図2に示します。

各ベンダは、基本となるISOドキュメントを元にICカードやリーダライタを開発しますが、ISO標準だけでは、アンテナの形状や、磁界強度等の違いにより、異なるベンダの製品間の互換性を確保することが困難となることから、当協会では、前述したISO標準を補完する仕様を「近接型通信インタフェース実装規約書」として実際に試作評価し、結果をフィードバックしてとりまとめ、日本語版だけでなく英語版も用意し、広く技術開示し製品開発に役立てていただけるようにしています。

各ベンダは、ISOと実装規約書の2つのドキュメ

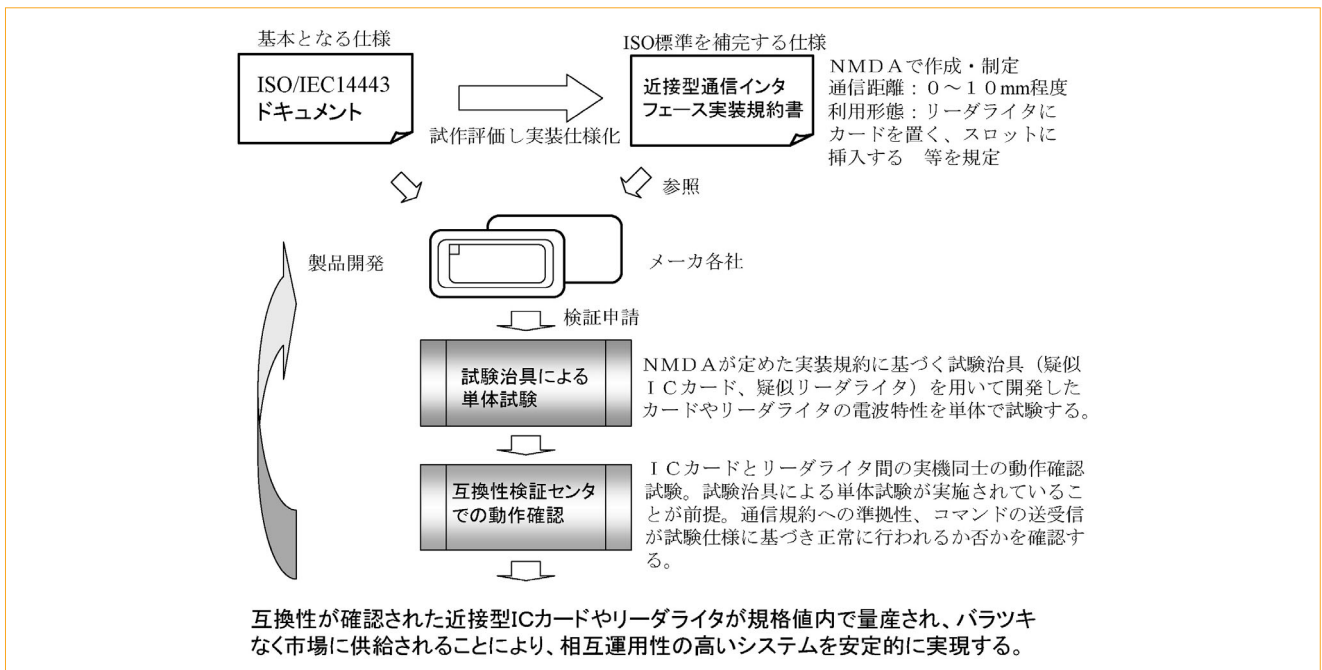


図1 互換性確保のためのプロセス

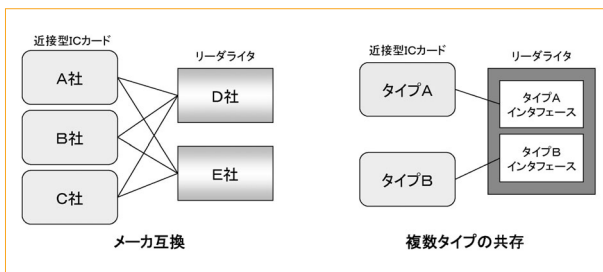


図2 非接触ICカードとリーダライタの互換性の確保

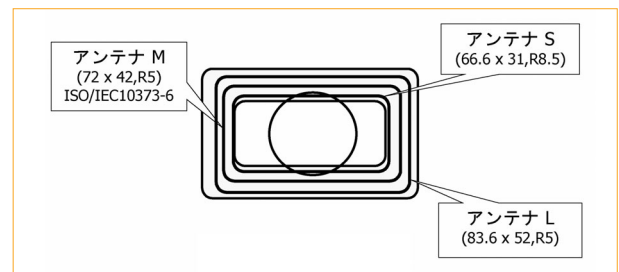


図3 実装規約に基づく試験器具の規定例（アンテナのサイズの規定）

ントを参照して開発することで、互換性を確保するための基本的な要件を満たす事になりますが、現実には、更にもその製品と他社製品との組合せによる動作確認（これを互換性検証と称する）を行うことで初めて互換性が確保されていることが確認されます。そうしないと、ICチップ内の暗号ソフトのロジック変更だけでチップの消費電力が変化し、互換性がとれなくなる等の恐れがあります。量産される場合には、特に、製造ロットのバラツキや製品バージョンの改変等による規格値のズレが互換性に影響を与える要素となります。互換性の検証は、このような様々なケースを想定し、CLICにおいては継続的に実施していくこととしています。各ベンダにとっては、いかに互換性が確保された製品を、規格値内でバラツキなく量産し、提供していくかが大きな鍵となります。

互換性検証試験は、実装規約に基づく試験器具を使用し電波特性を中心として行う単体試験と、カードとリーダライタによる実機同士の組合せで機能確認を行うクロステストから構成されます。

CLICでは、各社からの申請に基づき互換性の検

証を行います。互換性が確認されたICカード及びリーダライタは、該当企業宛に確認書を発行すると共に、当センターのホームページ上に型番を含めどのような組合せにおいて互換性が確認されたかを広く公表し、自治体や団体、企業等の調達検討時の参考としていただけるようにしています。

開発ベンダは、互換性が確保された同等仕様の製品を量産出荷することにより相互運用性の高いシステムの構築を安定的に実現していくことが可能となります。

4. 近接型通信インタフェース実装規約書

近接型通信インタフェース実装規約書は、先に述べた通り、ISO/IEC14443の規定だけでは、ベンダ製品間の互換、タイプAとタイプB等の複数タイプ共存等の互換性確保が困難であることから、補完的な仕様及び試験方法を規定したものです。例えば、ICカードのアンテナ範囲を規定することで、想定するリーダライタとICカード間のアンテナ特性のチューニングを図ると共に、図3のように互

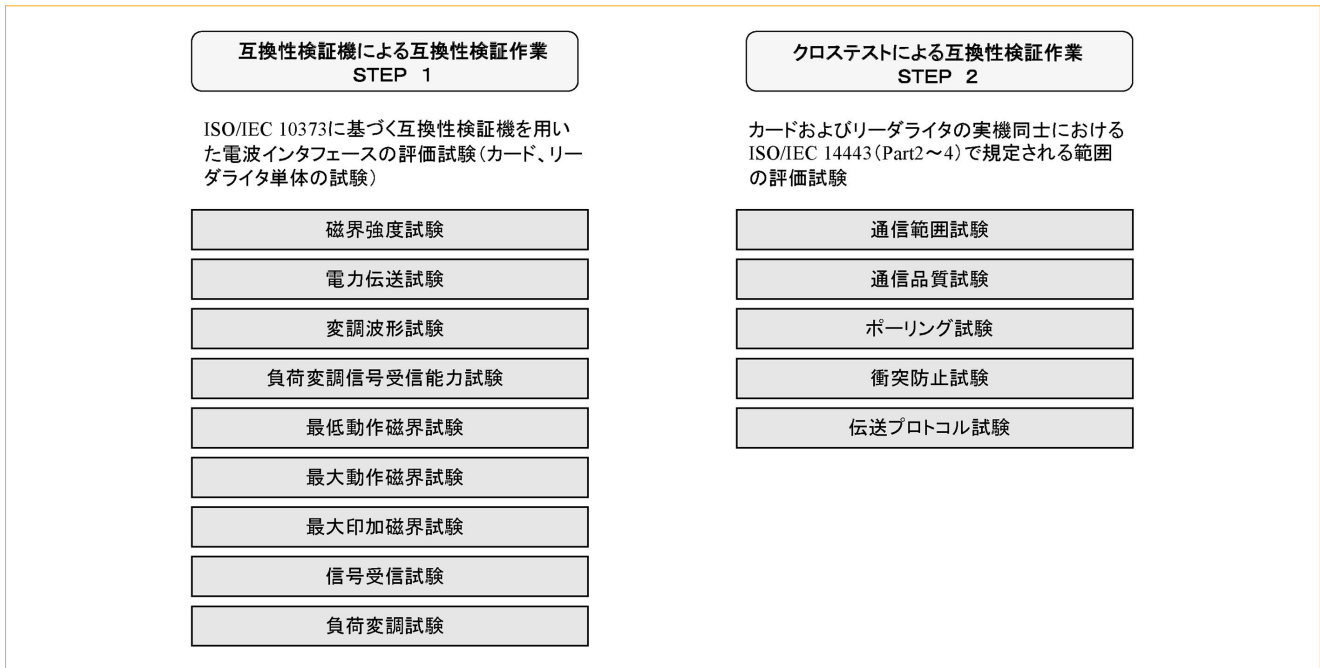


図4 互換性検証試験の概要

換性検証用の試験治具についても、アンテナサイズが大きい場合(L)、小さい場合(S)を含め、ISO標準の規定(M)に追加し、バリエーションのある試験を可能にしています。

実装規約で想定する近接型ICカードの使用条件は、

- ・通信距離 0~10mm程度
- ・操作形態 リーダライタにカードを置く、あるいは、スロットに挿入する
カードの方向、表裏には依存させない
- ・同時アクセス 2枚のカードの同時アクセスを可能とする

であり、規定項目としては、カードやリーダーライタのアンテナ特性やカード用IC特性、電力伝送、信号伝送、伝送プロトコル、ポーリング、衝突防止、ICカードやリーダーライタの試験方法、外部通信プロトコル、互換性試験方法等を規定しています。記述の仕方としては、ISO標準の規定を「基本仕様」とし、互換性を確保するために実装規約書において付加した仕様を「拡張仕様」として規定し、さらに「参考」として補足的な情報があれば付記し、設計者が参照して理解し易いように考慮しています。

現在「近接型通信インタフェース実証規約書」第1.1版については、関係各社の参加する作業グループにおいて本年度末を目標にバージョンアップすべく作業を進めています。主な検討項目としては、ISO標準のその後の進展への対応、高速化(n倍速通信)や、ICカードやリーダーライタの温度規定、アンテナ結合度と共振周波数、試験方法、リトライプロトコルの規定等、今まで十分な規定がなかった部分を補強し、より明確化することで、互換性確保の精度をより高

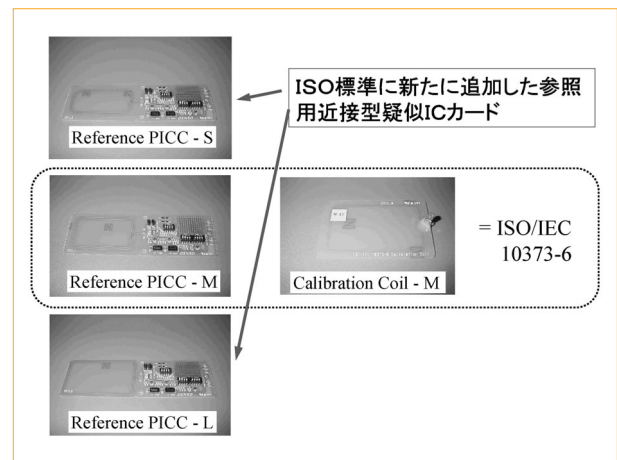


図5 互換性検証試験用治具例 (STEP1試験用)

める方向で検討を進めています。

5. 互換性検証試験の構成と内容

非接触ICカードとリーダーライタの互換性検証試験は、図4に示す通り、STEP1とSTEP2の2段階で構成しています。

STEP1は、実装規約に基づく試験治具(疑似ICカード、疑似リーダーライター)を使用した電波特性試験であり、各ベンダが自社製品単体に対して行う試験です。この試験を通して開発した製品が実装規約の規定値内に入っているか否かを試験します。図5にSTEP1で使用する試験治具(疑似ICカード)の例を示します。

STEP2は、STEP1の確認を終えた製品を前提に、各社で開発したICカードとリーダーライターを用いた

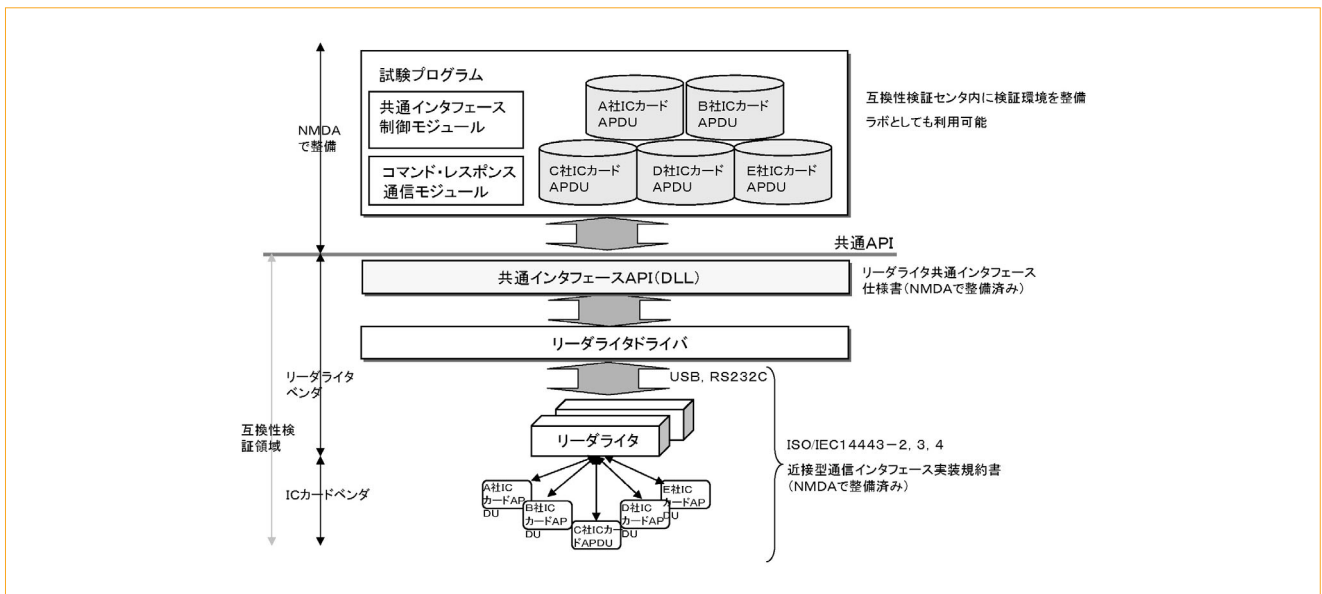


図6 互換性検証試験（クロステスト）の構成

全ての実機同士の組合せによる機能の確認（これをクロステストと呼んでいます）を行うものです。STEP1で確認済みの製品をSTEP2で試験するのは、いきなりSTEP2での試験を行った場合、組合せによっては電磁波の共振条件等によりチップが異常発熱し高温となる恐れがあるからです。STEP2試験では、互換性を確保する動作条件として最も厳しいICカードの消費電力が最大となるコマンドを含む選択されたコマンドを実行して確認します。図6にクロステストの試験構成を示します。

互換性検証試験は、先に述べた通り、実装規約書で規定した規格値に準拠しているか否かを検証するものですが、実際の試験作業の方法（何回繰り返し試験するか、判定基準は等）については、前もって互換性検証試験仕様を別途定め、それに従い作業を実施し公平性を保つようにしています。

当協会では、関係各社の協力を得て互換性検証済みのICカードとリーダーライタを含む試験環境を常時整備し、新たなベンダを含む新製品開発による互換性検証の申請があり次第、対応していくこととしています。また、そのような試験環境を「ラボ」として要請があればオープンに使用出来るようにし、公式な互換性検証試験だけでなく、希望する試作品を各社が持ち込み他社製品とのローカルな検証が出来るようにもしています。

6. 非接触ICカード普及センターの取り組み

- 「非接触ICカード普及センター」(略称CLIC)は、
- ・住基カードをはじめとする非接触ICカードの発行
 - ・異なるメーカー、異なる機種同士の利用を促進するための互換性検証の実施
 - ・ICカードシステムの円滑な導入に向けた各種技

術コンサルティング

等を、国内のカードベンダ、リーダーライタベンダ、カード発行機ベンダなどの協力の下で運営されています。

非接触ICカードの発行は、ICカードとリーダーライタの互換性検証を行ない、確認がとれたカードを発行対象とし、住基カードや、国や自治体への電子申請や電子入札等で利用するICカード等各種の発行を行います。

CLICでは、本年8月25日から市区町村で交付が開始された住基カードについても同様に互換性検証試験を実施し対象カードを選定しています。

図7に住基カード向け互換性検証試験の実施状況を、表2にCLICで互換性検証済みの住基カードの一覧を示します。

CLICでは、本年10月末時点で7社8種類のICカードと、7社9種類のリーダーライタとの互換性を検証しており、市区町村からの発注（外部委託契約）を受けて、マルチベンダの発行環境を使用し、住基カードの発行を行っています。

住基カードは、全国どこの自治体からでも住民票の広域交付が受けられることが売りの一つになっていますが、これを実現するには、各自治体が独自に調達し設置するリーダーライタと、異なる地域で発行された異なるベンダの住基カードとの間で、互換性が確保されていることが必須となります。

CLICには、互換性検証センター機能と、非公式に試作品等の互換性の検証が可能な「ラボ」機能の2つを備えており、いずれも希望するベンダの要請を受けて実施しています。

技術コンサルティング業務は、当協会がこれまで蓄積してきたICカード関連の技術、ノウハウ等を中心に、地方自治体等が抱えるICカードシステ

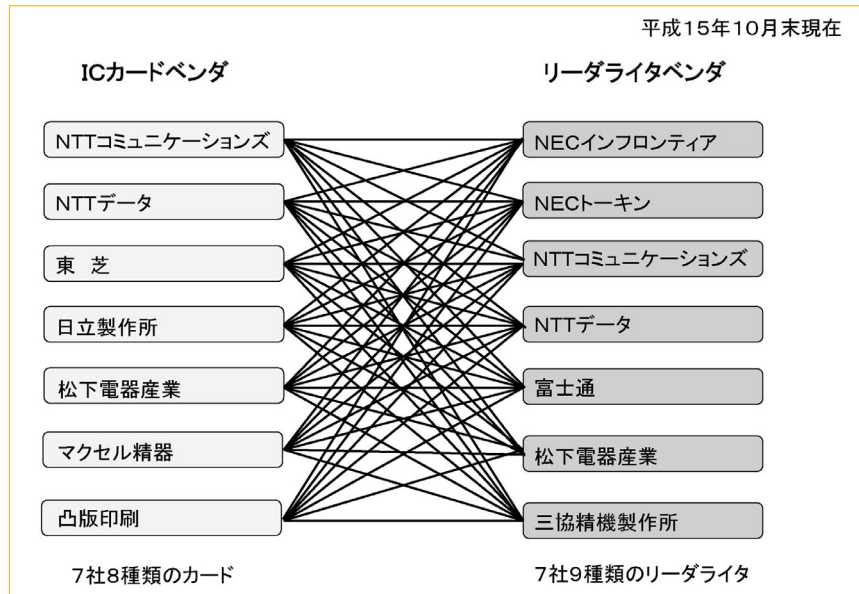


図7 住基カード向け互換性検証試験の実施状況

平成15年10月末現在

カード製造メーカー	ICカード型番	カードプラットフォーム	メモリ容量	メモリタイプ	インタフェース
NTTコミュニケーションズ	E16R10N	ネイティブ	1MB	FLASH	コンビ型
	E16R05N	ネイティブ	512KB	FLASH	コンビ型
NTTデータ	Xaica-α	ネイティブ	32KB	EEPROM	コンビ型
東芝	CQ-3006	Java Card	32KB	EEPROM	非接触
日立製作所	HT-2998-H1B3DJ	MULTOS	32KB	EEPROM	コンビ型
松下電器産業	BN-1M2N004A1	Java Card	32KB	EEPROM	非接触
マクセル精器	IE-32(MU2)JUKI	MULTOS	32KB	EEPROM	コンビ型
凸版印刷	Smartics-AD	ネイティブ	32KB	EEPROM	コンビ型

表2 CLICで互換性検証済み住基カード一覧

ムの導入や運用への課題解決に向けた総合的なコンサルティングを実施するものです。特に、住基カードの交付開始に向けては、周辺自治体が導入するリーダライタと住基カードとの互換性の確保が重要な課題であったため、札幌市様が第1号ユーザとなられ、住基カード関連システムに対する互換性検証サービスを提供しました。

7. 今後の取り組み

非接触ICカードは、ICチップのデジタル系の技術とアンテナを用いた電波インタフェースのようなアナログ系の技術とを複合した技術であり、かつリーダライタとの組合せで利用されることから、ICカード側だけで決められない未確立な技術要素もあり複雑で、組合せで「相性が良い組合せ」、「相

性が悪い組合せ」といった数値ではきちんと表せない微妙な課題が現在も残っています。

現在、各社の独創性を伸ばしながら、より互換性の精度を高めていくために、「近接型通信インタフェース実装規約書」第1.1版の改訂作業を進めています。

今後、自動車運転免許証の非接触ICカード化(平成16年度)や電子パスポート(平成17年度頃)の導入等が予定されており、従来国内だけでとらえられていたカードとリーダライタの互換性確保の課題が、全世界的な規模で解決していく必要が出てきています。

このような動きに対して、我々が蓄積してきた技術やノウハウが生かせるように検討を進めています。

電源地域情報化推進モデル事業

(出典：研究成果レポート12号 2004.7)

電源地域の振興は、我が国の経済成長、国民生活の質的向上の基礎となっているエネルギーの安定供給のために、国をあげて取り組まなければならない課題です。平成15年7月に決定されたe-Japan戦略で、これまで推進されてきたIT基盤の整備の段階から、IT利活用の段階へと移行する必要があることが示され、電源地域の振興を考える上で、ITの利活用による地域の情報化は、地域振興策として重要になってきています。

経済産業省が平成15年度からの3ヵ年計画で実施している「電源地域情報化推進モデル事業」は、今後のIT社会にとって重要なインフラともなる多目的ICカードシステム等の技術をベースとした各種のサービスシステムを構築し、地域のニーズに即したサービスの提供を行うことで、電源地域の活性化及び振興を図ると共に成果及び手法を他地域のモデルにすることを目的とした事業です。

当協会では、経済産業省より委託を受けて「平成15年度電源地域情報化推進モデル事業」を、地元企業である株式会社柏崎情報開発センター（以下、KASIXという）と共に実施しました。

サービス	概要	スケジュール		
		H16年度	H17年度	
健康 (健康増進・予防分野)	(1) 履歴サービス	電子健康手帳に登録した基本健康診断結果や健康相談履歴を、利用者が参照できる	開発・導入	運用
	(2) 相談サービス	電子健康手帳上の健康情報等を利用して、テレビ電話のように映像と音声で相談を行う	開発・導入	運用
	(3) 健康情報サービス	公共施設について、施設紹介やイベント等の情報を健康ボックスやウェブサイトを提供する	開発・導入	運用
	(4) 施設予約・申請サービス	公共施設で行われている教室やつどい等のイベントの予約を行う	開発・導入	運用
	(5) 施設予約・申請決済サービス	運動施設の料金を、金融機関からの口座振替等によりオンライン決済を行う	継続調査	導入・運用(予定)
健康 (医療・介護分野)	(6) 国民健康保険資格確認サービス	医療機関の受付で住基カードを用いて国民健康保険の資格確認を行う	開発・導入	運用
	(7) 介護認定情報照会サービス	ケアマネージャが電子健康手帳から介護認定情報を参照できる	開発・導入	運用
	(8) 検査機関予約サービス	各検査機関にて実施している検査の空き情報を確認し、予約を行う	継続調査	導入・運用(予定)
	(9) 医療決済サービス	医療機関等での会計を口座振替等によりオンライン決済する	継続調査	導入・運用(予定)
	(10) 医療・介護情報連携サービス	複数の医療機関や介護・福祉施設において、患者の診療・介護情報を共有する	継続調査	導入・運用(予定)

表1 健康サービスと導入時期

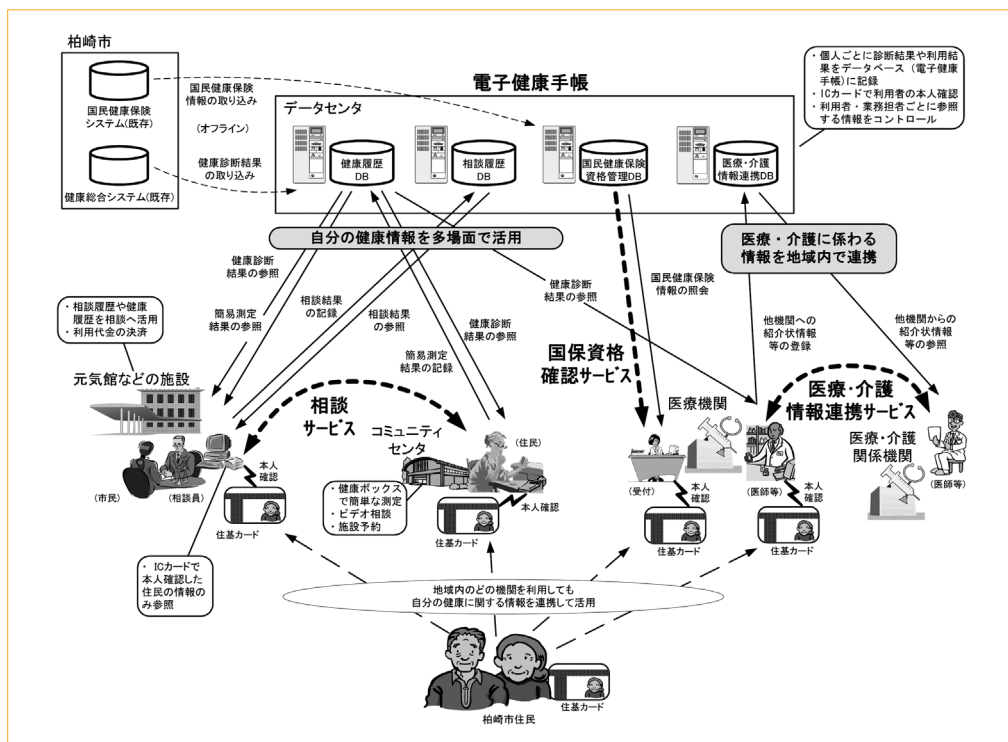


図1 健康サービスのイメージ

バイオメトリクスとは

(出典：研究成果レポート12号 2004.7)

1. 本人確認の手段

我々人間は、社会生活において常に他人と接する機会があり、必要があればその人が誰であるかを何らかの手段で確認している。同様に、自分が誰であるかを、何らかの手段で他人に証明する必要を迫られる。つまり、本人確認という作業は、監視やセキュリティに限ることなく、日常生活において当たり前のように行われている行為である。本人を確認する手段としては、次の三種類が存在する。

第一の手段は、本人の知識を用いるものである(What you KNOW)。パスワードや暗証番号、さらには母親の旧姓や過去の記憶など、本人しか知りえない情報をもとに本人を確認する方法である。例えばパスワードは、一般的な本人認証手段とし

て最もよく使われているもので、システムへの実装も容易に行える。しかし、適切なセキュリティレベルを保持するためには、利用者にある程度の負荷を強いることになる。もともとパスワードは、キーボード入力を前提としたコンピュータシステム向けの本人確認手段であるため、キーボードに不慣れな人には使いにくい。無意味な文字列を覚えることは容易でなく、忘失の恐れがある。また、忘れないように記録した紙などを見られて盗用される恐れもある。さらに言えば、高いセキュリティレベルを保持するために、定期的にパスワードを更新させるという運用は、利用者にとってはより一層使いにくいものとなる。

第二の手段は、本人の所有物を用いるものである(What you HAVE)。IDを記録した磁気カードや運転免許証など、他人が持ち得ない物をもとに本人を確認する方法である。これらは、認証に用いられる媒体の偽造が難しければ難しいほどセキュリティレベルが高まるとされており、ホログラムやICチップの組み込みなどの工夫が施されてい

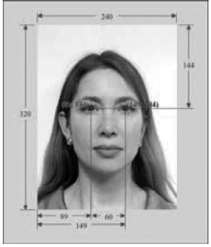


	符号化方式	ヘッダ情報	備考
顔画像データ  画像タイプ毎に撮影条件や顔向きなどの要件を規定	JPEG JPEG2000	必須：画像数、画像タイプ、画像サイズなど オプション：色空間、性別、顔向き、表情、顔特徴点、目の色・髪の色など	同一人物の複数の画像を一つのファイルフォーマットに収容可能
指紋画像データ 	RAW, WSQ, JPEG, JPEG2000, PNG	解像度、階調、画像サイズ、部位(親指-小指、左・右)など	複数の指の登録、一指あたり複数の画像を一つのファイルフォーマットに収容可能
虹彩画像データ  直交座標系と極座標系の画像表現形式	RAW, JPEG, ロスレス JPEG, JPEG2000	画像サイズ、画像向き、撮像波長、虹彩直径、傾きなど	一つのフォーマットに一つの虹彩画像を収容

表1 主要なバイオメトリクスデータ

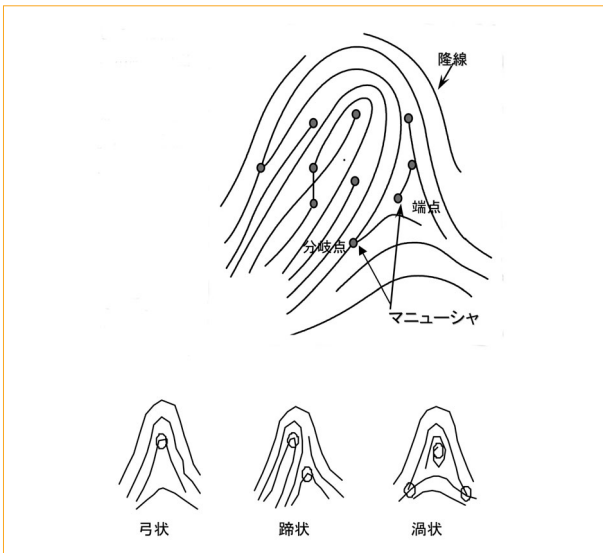


図1 指紋パターンの構造と指紋分類

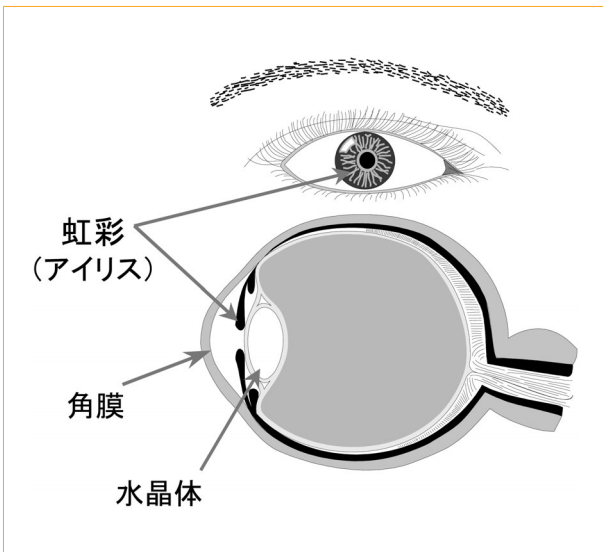


図2 虹彩について

る。しかし、物であるため盗用される危険性が高く、パスワードなど物以外の情報と併用しないと高いセキュリティレベルは保てない。また、媒体の低価格化が進んでも、破損や紛失によるメンテナンスコストが発生し、利用者には媒体の適切な管理が求められる。さらに、知識による認証手段も同様であるが、本人が協力した場合のなりすましに対しては、セキュリティ強度が保てないという弱点を有している。

第三の手段は、生体認証と呼ばれる本人の生体情報を用いるものである（What you ARE）。生体情報は、指紋や顔などの身体的特徴と、署名や音声などの行動的特徴に大別される。また、入力形態は、センサに身体の一部を直接接触する接触型と、何も触れる必要がない非接触型に分けられる。認証に用いる媒体が本人から切り離せないという特

性から、紛失や盗難の危険がないという点で他の手段より優位である。認証に使われる媒体が常に本人の管理下であり、しかも特別なメンテナンスは必要ないことから、利用者に対する負担は少ない。認証システムを管理する側からみれば、媒体の破損や紛失がないため再発行などの手間を必要とせず、ランニングコストを低く抑えられるメリットもある。

しかし、生体認証が持つセキュリティ上の脆弱性については注意すべき点がある。一つは、生体情報の複製の可能性である。例えば指紋を例にとると、指自体を奪われることは通常では考えられないものの、本人の残留指紋から指紋を複製される危険性が指摘されている。顔については、顔写真を使って本人に成りすますことが容易に考えられる。このような成りすましについては、運用に応じてそのセキュリティレベルに合った対策を講じる必要がある。もう一つは、生体情報は本質的にノイズを含むアナログ量である点である。つまり、各試行によって得られる値が必ずしも一致するわけではなく、本人を拒否する誤りや、他人を受理する誤りが常に発生する。また、信号がノイズに埋もれてしまい、生体情報が取得できない場合もある。例えば、指先をよく使う職業の人は指紋が磨耗してしまい、きれいな指紋画像を得ることができない。生体認証では、このような未対応となる人が存在する点にも注意すべきである。

社会的受容性の点から言えば、取得された生体情報が2次利用される危険性やプライバシーの問題から、指紋や顔写真などの生体情報を取られることに抵抗を感じる人が少なくない。磁気カードなどが盗難された場合は再発行が可能だが、個人の身体的特徴や行動的特徴は変えることができないため、生体情報が悪用されてしまうと、その生体情報を使った本人認証は二度と行えなくなる危険性がある点にも注意すべきである。

このような運用上の課題は残されているものの、生体認証による利便性が周知されれば、第三の本人認証手段として市場は急速に広がると予想されている。（表1参照）

バイOMETRICS関連事業最近の成果

1. バイOMETRICSを可搬型メディア（近接型非接触ICカード）に応用するための技術調査
2. 電子パスポート実装規約書日本語版・英語版
3. Personal ID Documents用各種顔画像の品質と顔認証精度に関する調査レポート