デジタル社会を安心して暮らすために

IC カードを利用した「本人確認」サービスの提言

平成 17 年 12 月 15 日

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

市民カード普及検討委員会

目次

はじめに　「なりすまし」社会の恐怖と対抗策

２１世紀の訪れと共に、我が国の社会では、これまでになかったタイプの市民生活への脅威、犯罪が拡がり始めています。

たとえば、「振り込め詐欺」「オレオレ詐欺」に代表されるなりすまし犯罪。社員名簿や同窓会名簿などを正当な持ち主から買って、転売する名簿業者。金融機関や通信事業者から流出する個人情報。どこからともなく家族宛てに送られてくるダイレクトメール。家族の名前や履歴を電話で語る勧誘業者・・・

今、日本では、「自分が自分であることの証明」や「自分や家族の個人情報の管理」について、今までの常識が通用しなくなりつつあります。

それは、何故か。私達は二つの大きな理由があると考えます。

一つは、戦後数十年の間に進んだ都市化によって、多くの個人の生活の場が、地域のコミュニティーより広い範囲になったこと。市町村単位の地域社会の中で、お互いに「顔の見える」者同士が暮らしているような社会から、隣の人の顔も知らない、通勤先や買い物先も地元ではない遠いところ、そんな暮らしをする人々が多数を占めるような社会になってきました。

二つには、この十年ほどの間に急速に進んだ社会の電子ネットワーク化、デジタル化によって、大量の情報処理が瞬時にできるようになったこと。さらに遠くの人や会社ともネットワークを通じて「自分が誰かを名のらずに」交信できるようになったことなどが、個人情報を脅威にさらすことにつながっています。コンピュータやプリンタの発達で素人でも偽札を刷ることが可能になったように、デジタル社会ではこっそり他人の個人情報を入手し、あるいは複製したり、ネットワーク上を匿名で、あるいは何者かになりすまして活動することがきわめて容易になってきています。

私達ＩＣカードシステム利用促進協議会は、ＩＣカードシステムの普及を願う事業者の集まりです。

私達は、このような社会状況をふまえ、ＩＣカードシステムを活用することによって、これからの社会をより安心で、なおかつ自由な、そんな社会にしていくことを願い、この提言をまとめました。

用語「アプリケーション」について：この提言で言う「アプリケーション」とは「IC カードに搭載される特定の用途と機能を持ったソフトウェア」を意味します。

用語：「市民カード」について：JICSAP 市民カード検討委員会は、主に住民基本台帳カードの現状の見なおしと普及策を中心に検討を進めてきましたが、現在の住民基本台帳カードの制度、運用、技術仕様をすべて前提としているわけではありません。そこで、「市民生活一般に汎用される IC カードを」との願いを込めて、検討の対象を「市民カード」と名付

けました。ここでいう「市民カード」は、現在一部の市町村で住民基本台帳カードの外に発行されている住民証（一部では「市民カード」と呼称されているものもあります）とは別のものです。

第１章　住民基本台帳カードが泣いている

1.1　住民基本台帳カードの始まり

私達のメンバの多くは、平成１５年８月から発行が始まった住民基本台帳カードや関連するシステムの開発になんらかの形で関わってきました。しかし、発行開始後約一年半がすぎても、住民基本台帳カードはあまり普及する兆しが見えず、各市町村での発行枚数は、概ね住民数の百分の一の単位にも届いていないのが実情です。

私達は、後に述べるように、この住民基本台帳カードには、社会のセキュリティを高めるすぐれた可能性が秘められていると考えています。また、このカードシステムの基盤を整備するためには、莫大な国費と民間の開発投資が投じられています。それにもかかわらず、このカードが何故普及しないのか。そのことを考えるためには、まず、住民基本台帳カードがどのようにして生まれたのかを知る必要があります。

住民基本台帳カードの初期の目的は、社会の都市化の流れの中で、日本中どこでも自分の住民票を取得できるようにすることです。このカードは、転居によって市町村を移籍しても住民データを電子的にトレースできるようにする、住民基本台帳ネットワークシステムの副産物として生まれました。「市町村が発行した住民基本台帳カードを持っていれば、自分の住んでいる土地の役場でなくても住民票を取得することができる」という限られた目的から生まれたものです。

しかし、一方でこのカードは、他の公共目的にも利用できる技術特性を持たせ、市町村が様々なアプリケーションを選んで搭載できる拡張性を持っています。

つまり、このカードの発行目的にはそもそも二義性があり、「住民票を取るための機能」と「いろいろ使える機能拡張の可能性」を併せ持っていたことを私達は理解する必要があります。なお、現在の所、全国一律で住民基本台帳カードに搭載可能な拡張機能は、電子ネットワークをつうじて政府に何かの行政申請を行う時に個人の認証を行うための「公的個人認証アプリケーション」だけで、ほかについては、各市町村が独自の判断で開発したり、採用したりすることになっています。

1.2　その位置づけ

前項の位置づけを図に示したものが、下記です。

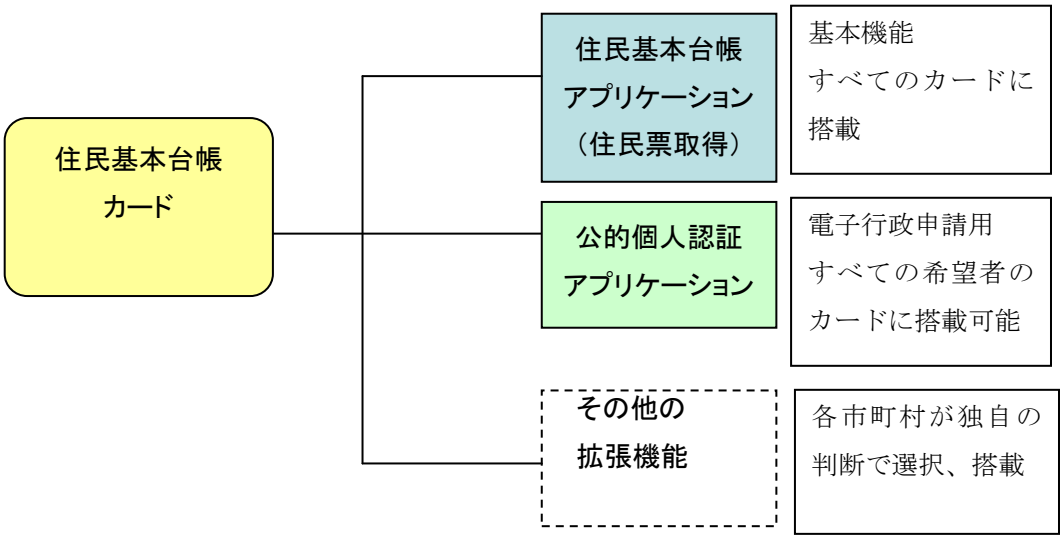


図 1－住民基本台帳カードの位置付け

1.3　現在の二つの主要機能　「住民基本台帳アプリ」と「公的個人認証アプリ」

それでは、次に住民基本台帳カードに搭載される二つの主要な機能「住民基本台帳アプリケーション」「公的個人認証アプリケーション」についてその機能を説明します。

「住民基本台帳アプリケーション」は、住民基本台帳カード内に格納されている住民基本台帳番号（住基コード）を、住民基本台帳ネットワークをつうじて市町村サーバのデータと照合することによって、個人を、基本四情報といわれる「氏名、生年月日、住所、性別」で、識別しています。カード所持者にとって、アプリケーションの機能は、「日本中どこの市町村役場でも、自分の住民票を取得すること」に限られています。このアプリケーションを用いて、カード内の情報を読み出すためには、カード所持者（住民）が自分で暗証番号を入力する必要があります。カード内の情報は、この暗証番号で守られていて、他者が容易に読み出すことはできません。アプリケーション提供者の市町村は、上記の個人情報を住民基本台帳ネットワークシステムの目的以外に利用することを禁じられています。

「公的個人認証アプリケーション」は、国が提供するアプリケーションで、カード所持者が電子ネットワークを用いて行政申請をするとき、申請者が正当な本人であることを認証する機能です。この機能は、きわめて高度で複雑な暗号処理を用いて、「顔の見えない」電子ネットワークを経由しても、申請者が「なりすまし」ではない本人であることを証明するものです。「その人が本人であること」を証明するのは、本人が居住する場所の都道府県知事で、市町村はこのアプリケーションについては、都道府県から委託されて発行等の事務を行っています。「公的個人認証アプリケーション」は電子行政申請にしか用いることができず、この本人確認証明を民間事業者の電子ネットワーク上のアプリケーションに用いることはできません。

1.4　なぜ普及しないのか

住民基本台帳カードが、何故普及しないかについて、私達は昨年の秋以来、議論を重ねてきました。その結論を要約すれば次のとおりとなります。

第一に、現在の二つの主要機能「住民基本台帳アプリ」と「公的個人認証アプリ」のニーズがきわめて少ないこと。私達市民がそもそも住民票を必要とする機会は、多くても年に数回で、人によっては数年間必要としない場合も多いと考えられます。それをさらに自分の住んでいない場所で取得するために、わざわざ市町村役場で住民基本台帳カードを受給しようとする人はきわめて限られています。また、個人がネットワーク経由で電子行政申請を行う機会も、現在の所きわめて限られています。「電子政府でいままでより便利になる」といわれても、そもそも個人は行政申請を行う機会がきわめて少ないので、企業法人ほど「便利さ」を実感するわけではありません。

第二に、多くの市民が「何のためにそのカードを持つのか」について、まったく理解できないこと。つまり、「将来いろいろ便利な機能が搭載されるらしい」といわれても、「そのカードを持っていると何ができるのか」がはっきりわからない限り、「将来のために」現在カードを受給しようとは思わないのではないでしょうか。

1.5　ほかの便利な機能？

それでは、どのような機能が搭載されたら、人々は「住民基本台帳カード」を便利なカードとして認識できるようになるのか、「何のためにこのカードを持つのか」がはっきりわかるような、いわゆる「キラーアプリケーション」の可能性について、私たちは議論を重ねました。

国の機関が、住民基本台帳カードの機能拡張のために用意しているいわゆる標準アプリケーション（証明書の自動交付や申請書の自動作成、公共施設の予約など)、あるいは健康保険番号を格納しておいて医療機関が有効期限などをすぐに確認できる機能、地元だけではなく各地の図書館を連携して利用できる機能などなど。

しかし、容易に導入可能で、現在の運用より飛躍的に便利になるような機能は、すぐにはみつかりません。「その機能があれば少し今より便利になる人がいる」ということと「その機能を使うためにみんながカードを持つ」ということの間には、かなりの距離があります。

また、多くの公共的な機能は、市町村の域を超えて、よそでも利用できなければ意味のないものですが、アプリケーションの採否は各市町村にまかされているので、端末側の機器を市町村が運用するようなアプリケーションの場合には「隣の町では使えない機能」が生じる可能性があることが、もっとも大きな障害となっています。

では、民間用途のアプリケーション、たとえば、電子マネーやクレジットなどの金融機能、電子乗車券、民間事業者が運営する各種のポイントシステムの会員証機能などとの連携をはかっていくという考え方はどうでしょうか？

たしかに金融・交通などとの連携は不可能ではありませんが、金融機関も交通機関もすでに独自のカードシステムの基盤を持っていて、住民基本台帳カードと無理に連携しなくても、成り立っています。住民基本台帳カードの民間アプリケーションとの連携は、住民基本台帳カードの公共的な機能という基盤があって、はじめてその補完的な機能として追加されるべきものなのです。また、もともと住民基本台帳カードがあまり普及していない現状では、民間側からみても連携のメリットは少ないというのが実情ではないでしょうか。

1.6　私たちの提言　あまねく国民がもてる「本人確認カード」に！

一人一人の市民が「何のために住民基本台帳カードを持つのか」がはっきりわかるような用途。「その機能があれば少し今より便利になる人がいる」のではなく「それを使うためにみんながカードを持つ」ような機能。

そうした用途として、私達は、住民基本台帳カードを公式の「本人確認証」として用いることを提言します。

その理由は、次のとおりです。

- 「なりすましの防止」は、現在社会で求められているきわめて重要な課題であること
- 「なりすましの防止」のためには、現在社会で行われている「運転免許証」「健康保険証」などの目的外利用による本人確認では不十分であること
- 誰でも持つことができ、本人を確認するのに十分な情報が搭載（記載）されている「本人確認証」が求められていること。そして住民基本台帳カード（B タイプ）の券面は現在でもその条件をみたしていること
- 住民基本台帳カードは IC カードなので、従来の紙カードや証明書の視認による本人確認よりも精度の高い電子的な本人確認ができること
- 生体情報処理による電子的本人確認など高度な技術的拡張に対応可能であること
- 電子ネットワーク上の本人確認機能も拡張可能であること

私達は、社会のどこかで「本人であることの確認」を求められたときに、住民基本台帳カードを示せばよいような、そんな「自治体による住民証明書」としてこのカードを用いることを提案します。

第２章　「本人確認カード」

2.1　いまの社会で本人確認はどのように行われているか？

一昔前の日本では、たとえば預金通帳と印鑑を持っていけば、預金者本人でなくてもかなりの金額を現金化することができました。また家族のために住民票や印鑑証明書を取得するような場合、本人の認印を捺した委任状があれば、その委任状の真偽は特に確認されずとも通用しました。

しかし、現在の社会では、「本人になりすました者」が横行しているので、社会の様々な場面で「本人であることの証明」が求められるようになってきています。

では、「本人確認」は通常どのように行われているでしょうか。

もっとも通常行われているのは、運転免許証、旅券、健康保険証などの公共用途の証明書の目的外利用です。しかし・・

- 運転免許証は、自動車を運転しない人、運転できない人には発行されません。
- 旅券は、海外渡航しない人には発行されませんし、住所は所持人が自署するようになっています。
- 健康保険証は、券面に通常顔写真がなく、借りたり拾ったり盗んだりした保険証を、本人でない者が使うことは容易です。

つまり、いわゆる「公共用途証明書類の目的外利用」では、広く一般の人のための十分な本人確認ができないことが明らかです。

2.2　「なりすまし」に対抗できる本人確認

私達は、次のような要件を満たす「本人確認証」が必要と考えます。

- そもそもの用途が「本人であることの証明」のためのものであること
- 券面に、少なくとも基本四情報（氏名、生年月日、性別、住所）が記載され、かつ必ず生体情報（顔画像）が掲載されていること
- 偽造改竄を防止するため十分な処置がとられていること（改竄や偽変造が著しく困難な IC チップに基本四情報と生体情報が格納され、券面との照合が可能であること）
- 暗証番号のような「本人しか知らない」情報によって、所持者の真正性を証明できること
- 市町村などの公的機関が発行する、公式の信用できる証明であること

2.3　誰でも「証明される」権利がある

私達は、上記のような「本人確認証」を受給することにより、当該市町村に居住するすべての住民が「本人であることを証明される」権利があると考えます。

2.4　誰でも「証明を使わない」権利がある

ただし、いかに「なりすまし社会」の恐怖があると言っても、社会生活のすべての局面で「本人確認」が必要であるとは、私達は思いません。人間は時として「無名」でありたい存在であることは十分理解しています。また、「本人であることを証明されない」不便（たとえば金融機関で口座を開けない）をしのげば、そのような「本人確認証」を行使せずとも何とか暮らせる社会であってほしいとも考えています。

ですから、私達の提案する「本人確認証」は、あくまでも持つことを希望する人のためのもので、「本人確認証」を「持たない」「使わない」自由はあるべきとも考えています。

2.5　個人情報保護と本人確認

「なりすまし」が横行し、社会生活の様々な場面で「本人確認」が必要になると、もう一方の問題、「個人情報の保護」にも影響が及びます。

最近ではなんらかの本人確認のために「確認する側」が証明書類をコピーして保管するケースは増えてきていますし、カードによる電子的な本人確認の場合には、「確認」の都度、カード所持者の個人情報が「確認する側」に移転します。もし「本人確認する側」が偽者であったり、適正な個人情報の管理を怠ったりすれば、「本人確認」という行為自体が徒となって、セキュリティが破られることになりかねません。

そこで、私たちは社会の中で適正な「本人確認」が行われるために、次の提案をします。

- 「本人確認をする側」が個人情報保護法の定めを守り、適正な個人情報保護の措置をとること。そのことを促す「本人確認システム」を構築すること
- 「本人確認システム」において、「本人確認をする側」の「なりすまし」を防ぐ技術的措置をとること
- 「本人確認システム」においては、本人確認のために必要十分な個人情報以外は、「本人確認をする側」に移転しないような技術的措置をとること
- 「本人確認システム」においては、「いつ、誰が、どこで、何の用途で」本人確認をしたかの記録が（紙または、電子データで）「本人確認をされる側」に残るような技術的措置をとること
- 公的証明書類（運転免許等）の目的外利用による本人確認の場合、本人確認用途以外の個人情報が「本人確認をする側」にわたる可能性が高いので、適正な「本人確認システム」の普及とともに、こうした目的外利用を漸次やめること

2.6　住民基本台帳カードの拡張機能としての「本人確認」

以上私たちが提案する住民基本台帳カードの「本人確認証」としての利用のためには、カードに「本人確認アプリケーション」が搭載される必要があります。

このアプリケーションの主な機能は、「個人の基本四情報（氏名、生年月日、性別、住所）の暗証番号による読み出し」機能になるでしょうから、技術的には現在すでにカードに搭

載されている「住民基本台帳アプリケーション」に近いものになるでしょう。

が、「住民基本台帳アプリケーション」は、市町村などの公的機関しか読み出すことができず、また、目的外利用を禁じられています。そして住民基本台帳ネットワークのセキュリティを守るためには、前記の目的外利用の禁止は不可欠と考えられます。また世間で言われている「目的外利用の禁止が守られないのではないか」との懸念を払拭するためにも、「住民基本台帳アプリケーション」はその運用において、ISMS の活用によるセキュリティ監査の導入等現行より厳しい措置がとられるべきものと考えます。

そこで私達は、住民基本台帳ネットワークと直結する「住民基本台帳アプリケーション」の運用をゆるめるのではなく、これとは別にあたらしく、広く一般用途に開放される「本人確認アプリケーション」を住民基本台帳カードの拡張機能として全国共通で提供し、それを各市町村が採用する形で普及していくことを提案します。

次章では、その「本人確認アプリケーション」の要件について、提案することにします。

表 本人確認カードの用途

No	本人確認として利用するシーン	関連する規定
1	銀行、証券会社での口座開設	「金融機関等による顧客等の本人確認等に関する法律（本人確認法）」 http://www.fsa.go.jp/honninkakunin/honninkakunin.html
2	リサイクルショップへの持込み	古物営業法 http://www.npa.go.jp/safetylife/seiankis7/tutatu.pdf
3	プリペイド携帯における本人確認	ルール化の動き http://keitaiphsjyouhou.hp.infoseek.co.jp/000.html
4	青少年の社会環境 (ゲームセンター、カラオケ等)	青少年保護育成条例 における本人確認
5	医薬品等の販売 ・農薬等の販売。 ・薬局の販売	各種商品における販売jに関わる規定 http://www.pref.yamanashi.jp/download/6-6-1.html
6	レンタル事業者における本人確認 ・レンタカー ・レンタルビデオ、CD店 等	事業者ごとに独自に規定
7	匿名で行える各種サービス ・オークションにおける本人確認 ・インターネット喫茶	事業者ごとに独自に規定 ルール化の動き http://www.shugiin.go.jp/itdb_kaigiroku.nsf/html/kaigiroku/00021552 0021108005.htm

第３章　「本人確認アプリケーション」の基本機能仕様案

私達が想定する「本人確認アプリケーション」の構造は下記の通りです。

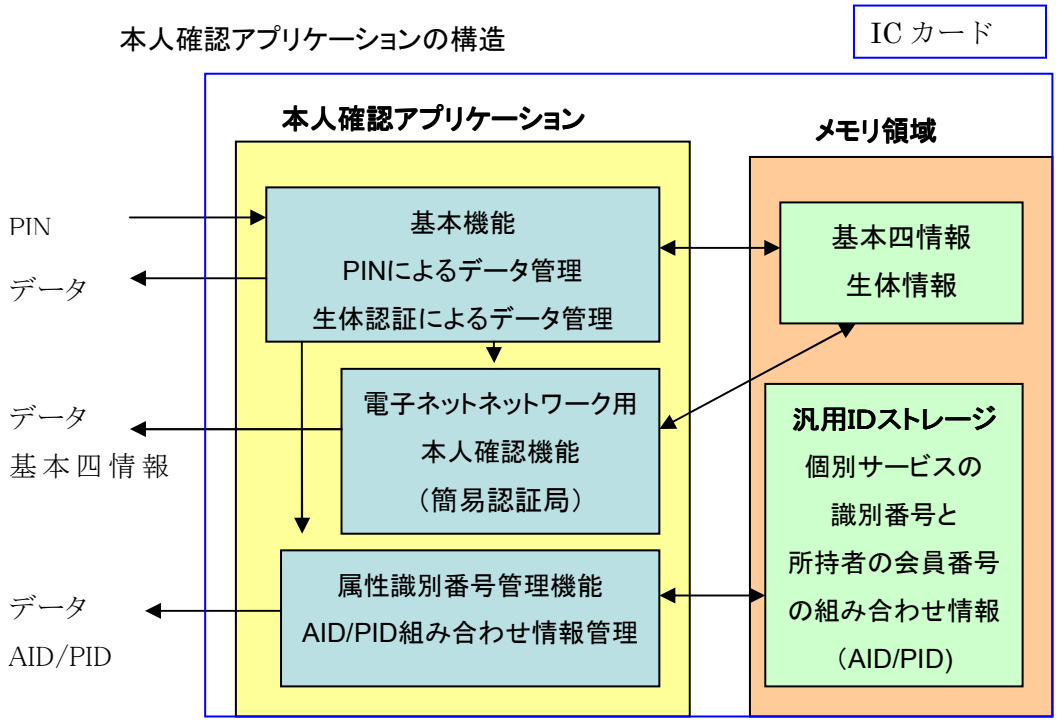


図 2－本人確認アプリケーションの構造

本章では、このうち基本機能の仕様について提案します。

3.1　住民基本台帳カード B タイプへの搭載

まず、現在発行されている「住民基本台帳カード」には、券面に市町村名と所持者の氏名だけが記載されている A タイプと、券面に発行市町村名、所持者の基本四情報（氏名、生年月日、性別、住所）及び生体情報（顔画像）が記載されている B タイプがあります。

A タイプの所持者は、顔画像などの個人情報の掲載を忌避し、住民基本台帳カードに搭載されるアプリケーション（現在の所、主には「住民票の取得」と「電子行政申請のための個人認証」）を利用することだけを目的にカードを取得する方ですから、いわゆる「本人確認用途」を放棄していると考えられます。

したがって、「本人確認アプリケーション」を搭載する住民基本台帳カードは、券面でも視認による本人確認が可能な B タイプだけとすることを提案します。

3.2　住民基本台帳カード視認による本人確認

「本人確認アプリケーション」を搭載する住民基本台帳カードは、カード内の電子的機

能より前に、まず「券面視認による本人確認」が可能なものである必要があります。

現在の住民基本台帳カードBタイプは、券面に発行市町村名、所持者の基本四情報（氏名、生年月日、性別、住所）及び生体情報（顔画像）が記載されており、たとえば金融機関の口座開設など民間の本人確認用途に利用可能であり、この条件を満たしていると考えます。

さらに券面には、発行年月日、有効期限、発行市町村長の「住民であることを証明する」旨の文言などが加えられることが望ましいと考えます。

3.3 端末機による本人確認（PINと生体情報）

上記の前提で、私達は次のような「本人確認アプリケーション」仕様を提案します。

- 「本人確認アプリケーション」には、所持者の基本四情報（氏名、生年月日、性別、住所）及び生体情報（顔画像）の電子データが格納されます。
- 「本人確認アプリケーション」には、発行市町村長による住民であることを証明、証明の発行年月日、証明の有効期限が電子データで格納されます。
- 「本人確認アプリケーション」は所持者自身しか知らない暗証番号（PIN）が入力されなければ、中のデータを読み出せない仕様とします。
- 「本人確認アプリケーション」を用いて、中の生体情報を読み出し、端末機上で撮影した所持者の画像と照合することが可能な仕様とします。
- 上記により、「券面の視認」「暗証番号による基本四情報の読み出し」「生体情報と実画像の照合」の三段階での本人確認が可能になります。利用者は、自己に必要なセキュリティの程度に応じて、段階を選ぶことができます。
- 「本人確認アプリケーション」のため「暗証番号による基本四情報の読み出し」「生体情報と実画像の照合」の電子的な処理を行う端末機は、何らかの公的な登録機関に登録され、「本人確認」を行う都度登録機関に認証される必要があると考えます。
- 「本人確認アプリケーション」を用いて「本人確認」を行う場合、必ず端末機側のアクセスデータ（端末機のID、アクセス時刻等）がカード内及び登録機関に電子データとして残るような仕様とします
- 「本人確認アプリケーション」を用いて読み出された情報は、所持者の同意がなければ、端末機側に記録されない仕様とします。

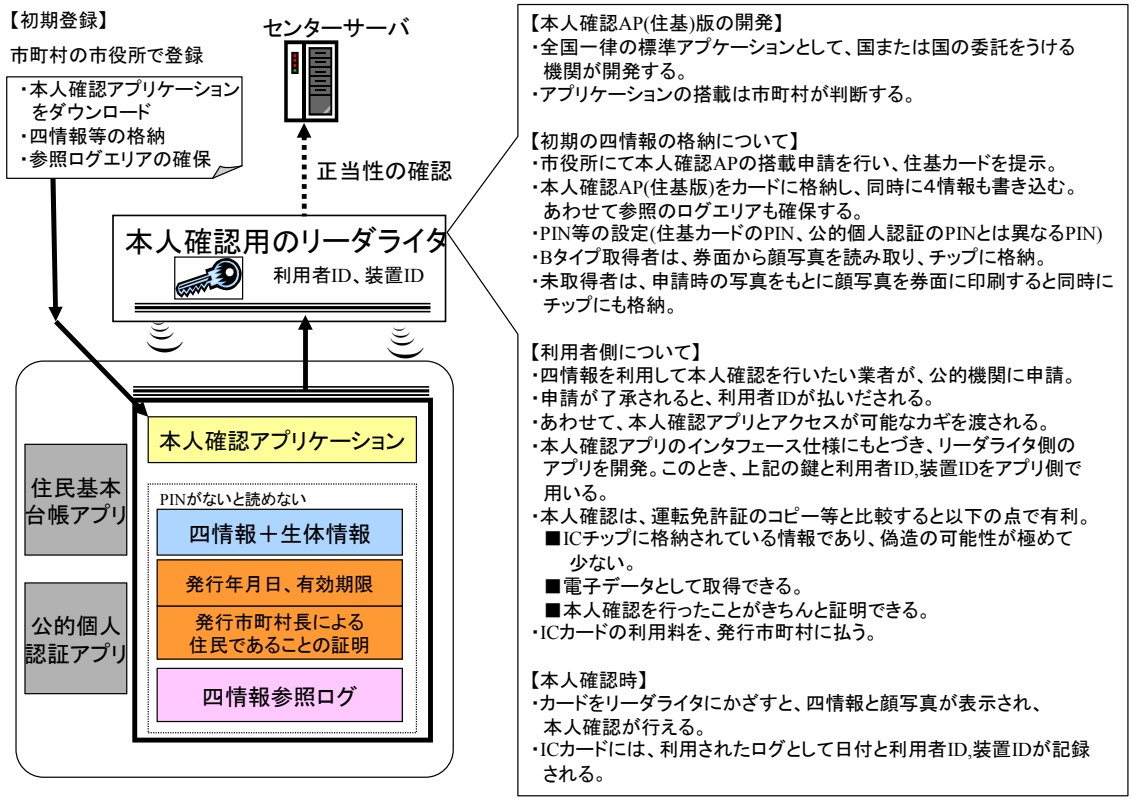


図 3－本人確認アプリケーション

3.4　「住民基本台帳アプリケーション」とどこがちがうか

「住民基本台帳アプリケーション」は、住民基本台帳ネットワークに直結し、全国の市町村の管理する端末機以外では、データを読み出すことができません。また、アプリケーション用途は、住民票の取得に限られています。

一方、私達が提案する「本人確認アプリケーション」は、このアプリケーションを管理する公的機関に「個人情報保護法に基づく適正な個人情報管理」を誓約して、端末機 ID を登録すれば、広く一般に端末機の使用を希望する者が端末機を持つことができ、カード所持者の許諾を得て端末機からカード内の情報を読み出したり、記録したりすることができることを意図しています。

来訪者に「本人確認」をもとめる相当の理由のある者は、誰でもこのアプリケーションを利用できるというのが、「住民基本台帳アプリケーション」と最も違う点です。

3.5　By whom 「証明する」主体は自治体首長

「本人確認アプリケーション」の発行者は、カード所持者が居住する市町村とします。

「本人確認アプリケーション」において、所持者が発行市町村の住民であることの証明は、当該市町村の首長の責任で行います。証明の発行年月日、証明の有効期限（本人が死亡または住所を移転したとき、または発行後一定時日後まで）が付加されます。

3.6　What 「証明する」対象は基本四情報と生体情報（顔画像）

「本人確認アプリケーション」において、発行市町村の首長が証明するのは、所持者の基本四情報（氏名、生年月日、性別、住所）及び生体情報（顔画像）です。

「本人確認アプリケーション」を発行する市町村は、発行時になんらかの別の手段で所持者の本人確認を行った上で、券面と同じ本人の顔画像を基本四情報と共に入力します。

3.7　To whom「証明する」相手は民間も含む多様な利用者

「本人確認アプリケーション」においては、発行市町村の首長は、特定の対象ではなく、広く一般に「本人確認を求める者」対して所持者の基本四情報（氏名、生年月日、性別、住所）及び生体情報（顔画像）を証明します。

3.8　Where and How 「証明する」場面はリアル社会、対面

「本人確認アプリケーション」は広く公開の場に設置される、IC カード専用の端末機（リーダライタ）を用いて、「本人確認を求める者」が「カード所持者」と対面で、カード所持者の同意を得て、カード内のデータを読み出すことを想定します。

「本人確認アプリケーション」では、カード所持者が家庭のコンピュータ端末にカードリーダライタを接続し、電子ネットワークをつうじて「本人確認を求める者」にアクセスすることは想定しません。

3.9　運用のイメージ

「本人確認アプリケーション」は、全国一律のアプリケーションとして、国または国の委託を受ける機関によって市町村に提供されるべきものと考えます。実際には、アプリケーション開発業者が製造したアプリケーション・ソフトウェアを、国の委託を受ける機関が相互運用性を確認した上で「正しい本人確認アプリケーション」として認定し、認定を受けたものを各市町村がアプリケーション発行システムと一緒に調達する方式が考えられます。

上記の機関は、同時に「本人確認アプリケーション」用の端末機の登録・認証を行うことを想定します。当該機関の経常的な運営費用は、「本人確認アプリケーション」を用いて「本人確認を求める側」の端末機使用者が負担すべきものと考えます。

3.10 どんなセキュリティが必要か

「本人確認アプリケーション」には、たとえば次のようなセキュリティ機能が必要と考えます。

- 所持者の同意をあらわす暗証番号の入力がなければ、なかの個人情報を読み出し、または端末機側に個人情報を記録させることができないこと
- 端末機が、登録された正当な使用者のものであることが確認されなければ、なかの個

人情報を読み出し、または端末機側に個人情報を記録させることができないこと
- 「本人確認アプリケーション」を用いた本人確認が行われる都度、端末機の正当性が、なんらかの公的機関が運用するセンターサーバによって認証されること
- 何時、どの端末機が、所持者の本人確認を行ったかを示すデータが所持者側のカードに残されること
- 端末機に搭載される、端末機の認証用データや「本人確認アプリケーション」読み出し用のアプリケーションソフトが偽変造されない措置がとられている（アプリケーションが封止され使用者が自由に取り出したり入れ替えたりできない）こと
- カード内に格納される市町村長の証明の偽造改竄、個人情報・生体情報の偽造改竄を防ぐ措置がとられていること
- 正当なアプリケーション発行者（市町村）以外には、「本人確認アプリケーション」を住民基本台帳カードにダウンロードできない措置がとられていること

3.11 アプリケーション運用上のセキュリティ課題

「本人確認アプリケーション」においては、「確認される」カード所持者と「確認する」端末機使用者の双方が「真正な者であること」つまり「なりすましでない、ほんとうの相手」であることが求められます。

そのためには、アプリケーション・システムの技術仕様だけではカバーできない管理運用上の問題も検討する必要があります。

そもそも、市町村は住民基本台帳カードを発行する際に、どのような「本人確認」をしているのか。

「本人確認アプリケーション」を住民基本台帳カードにダウンロードする際には、どのような「本人確認」をするのか。

端末機が正当な使用者によって登録された後に、持ち去られたり盗まれたりした場合、すみやかに登録を抹消するための業務フロー。

などが、アプリケーション運用上のセキュリティ課題となるでしょう。

3.12 住民基本台帳カード以外のメディアでも・・

本章で提案した、「本人確認アプリケーション」は、技術的には住民基本台帳カードではない、別のＩＣカードにももちろん搭載可能です。

一般の市民生活では、「本人であること」をだれかが証明してくれればよいので、必ずしも市町村長だけが「証明の主体」であると考える必要はないかもしれません。

「本人確認を求める者」にとって、証明の主体が市町村長ではなくとも、社会的に信用のある第三者のものであってもよいのであれば、たとえば、このアプリケーションソフトをそのまま、ある私立学校の発行するＩＣカード学生証として使うこともおそらく可能でしょう。

端末機側でこれを読むときに、「証明の主体」が誰であるかを識別し、「証明主体」を信用できると判断すれば、ＩＣカード学生証でも「本人確認」の役割を果たすことはあり得ます。

ただし、このような「本人確認アプリケーションの民間利用」の場合、「証明主体のなりすましを防ぐ」という別の措置をとる必要が生じます。

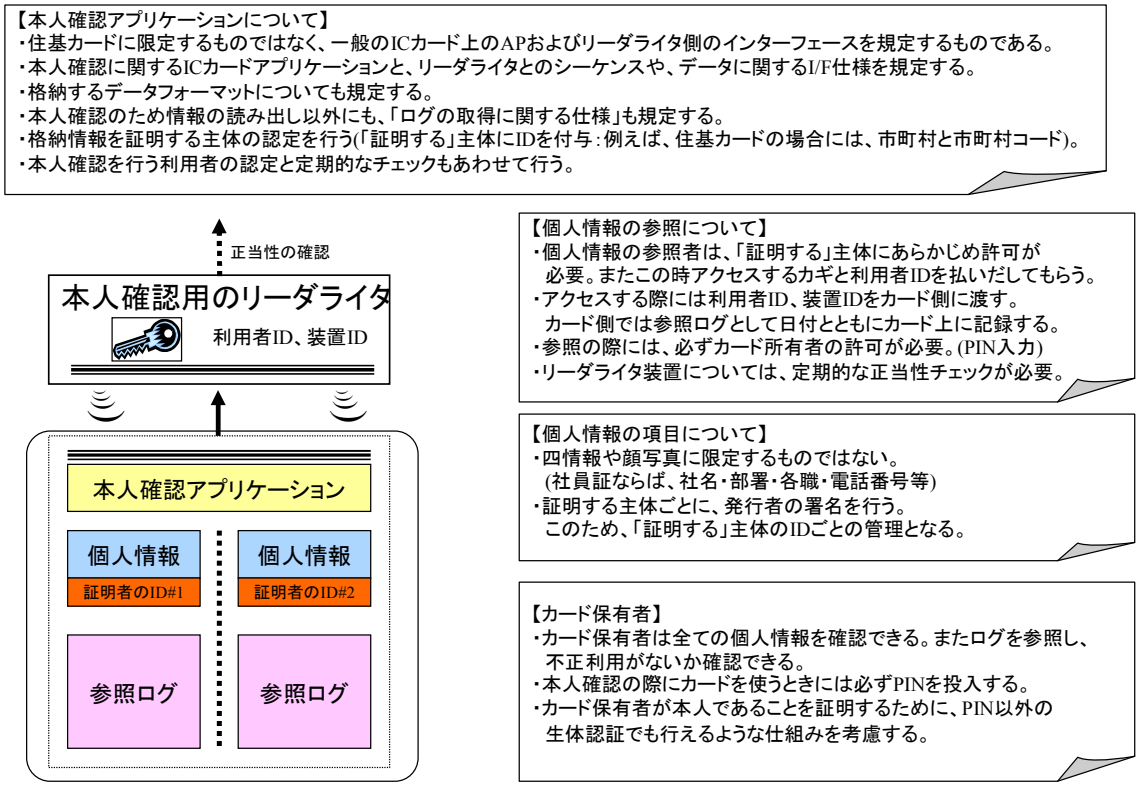


図 4－本人確認アプリケーションのインタフェース仕様

第４章　「本人確認アプリケーション」の属性識別番号管理機能仕様案（一般用途への機能拡張）

本章では、「本人確認アプリケーション」の「属性識別番号管理機能」を用いて、住民基本台帳カードの用途を拡張し、社会一般に使われている様々なＩＣカードアプリケーションとの併用をはかることを提案します。

4.1　住民基本台帳カードのジレンマ（全国共通アプリケーションの困難性）

住民基本台帳カードに、便利な新しいアプリケーションを搭載し、普及させていこうとする場合、基本的な障害がひとつあることを、私達は第 2 章で指摘しました。それは、機能拡張の選択が住民基本台帳カードの発行者である市町村にまかされていることです。

都会では、個人の生活域は特別区や市町村の域をはるかに超えています。自分が居住する地域の住民基本台帳カードに、ある便利な機能が搭載されていても、他の地域でそれを使えないのでは、意味がないことが多いのです。もちろんそうした便利なアプリケーションが、ある特定の市町村で発行され、全国の市町村ではない窓口、たとえば郵便局とか国立病院とかで使われるような場合には、隣の市町村がそのアプリケーションを採用しなくても、「隣の住民が不便」なだけでカード所持者の自分の利便性は損なわれません。しかし、そのアプリケーションが、全国の市町村の施設、たとえば市町村営の図書館などを対象にする場合には、「隣町で使えないのでは不便だ」ということになります。

また、民間事業者が広域で社会一般に提供しているサービス（たとえばチェーンストアのポイントシステムなど）のアプリケーションを住民基本台帳カードに搭載しようとする場合でも、市町村によって採否が分かれるのでは、民間事業者側にとっては住民基本台帳カードと連携する上で、いろいろな不都合が生じることになります。

一方で、市町村には住民基本台帳カードの発行者としての責任があるわけですから、発行者の関知しないところで、住民基本台帳カードに新しいアプリケーションが搭載されてしまうようなことは、セキュリティ上の観点からも、問題があると言わざるを得ません。

4.2　ジレンマを超える方法

私達は、上記のジレンマを超える方法を議論しました。その結果、「本人確認アプリケーション」の一部分として、様々な IC カードアプリケーションの ID（識別番号）だけを管理する一種のメタ（上位）・アプリケーションである「属性識別番号管理機能」を提案します。

この「属性識別番号管理機能」の考え方は、住民基本台帳カードに、発行市町村が採用する新しいアプリケーション・ソフトウェアを追加しなくても、「IC カードアプリケーションのアプリケーション識別番号と個別メンバ-の識別番号」の組み合わせデータを住民基本台帳カード内のメモリ領域（「汎用ＩＤストレージ」と呼びます）に書き込み、そのデータを上手に管理する機能だけを持てば、一般に普及しているかなりのＩＣカードアプリケーションに応用できる、と言うものです。

IC カードのアプリケーションには、「ソフトウェアのような論理構造をもって、端末機側との交信を通じてカード内でかなりの演算処理を行う」タイプと、「IC カード内に一定のデータを格納して、それを端末機側が読み出すことだけをカード-端末機間で行い、主要なアプリケーション機能はネットワークを通じてセンターサーバと交信することによって行う」タイプのものがあります。

4.1 項で「発行者である市町村の関知しないところで、住民基本台帳カードに新しいアプリケーションが搭載されてしまうようなことは、セキュリティ上の観点からも、問題がある」と述べた対象は、主に前者のアプリケーションであって、後者についてはカード内のアプリケーション・ソフトウェアによって適正な識別番号管理が行われれば、カード発行者の責任に帰するようなセキュリティ上の問題が生じることはないと考えられます。

但し、「本人確認アプリケーション」のダウンロード自体については、住民基本台帳カードの発行者である市町村による適正な運用管理が行われることが前提となります。

（注） IC カードアプリケーションを識別する ID は、国際標準規格や日本工業規格などでは「アプリケーション識別子」と呼ばれています。が、ここでは、一般的な言い方である「アプリケーション識別番号」を採ることにしました。ただし、厳密に言えば、この ID は番号だけではなく記号も含むものであることを注記します。

4.3 「属性識別番号管理機能」の仕様案

私達が本項で提案する「上位アプリケーション」＝「本人確認アプリケーションの属性識別番号管理機能」の考え方は、前者の IC カードアプリケーションには使用できませんが、後者のタイプについてはどんなものにでも対応可能なものとして、次の仕様を想定します。

- この機能は、住民基本台帳カードの所持者が、「任意の IC カードアプリケーション（公共民間を問わない）を識別する番号（AID）とそのアプリケーション下で個人を識別する番号（PID）の組み合わせ」を任意の個数書き込み記録し、自らの責任で使用することが出来るようにするものです。
- どのような「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」を当該住民基本台帳カードに書き込むかは、カード所持者にまかされるものとします。
- 「属性識別番号管理機能」自体は「本人確認アプリケーション」の一部として、全国共通の仕様で個別の市町村によって採用されるものですが、アプリケーションの保証する機能は、「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」を、カード所持者の同意があったときにだけセキュアに取り出して使うことができること」に限定され、その後に取り出された一組の「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」をどう使うかは、下位の IC カードアプリケーションにまかされます。

- 「本人確認（上位）アプリケーション」を発行する市町村は、どんな「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」がカードの中に書き込まれるかについては関知しないわけですから、個別（下位）アプリケーションの使用上の責任は、カード所持者と個別アプリケーション発行者が負うことになります。
- 個別のＩＣカードにどんな「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」データが、いつどの端末機によって書き込まれたかの記録は、端末機を登録・認証する公的機関のサーバに記録され、カード所持者が自分で参照したり、有償で定期的に自己のカード内に書き込まれたデータの連絡を受けたりすることが可能な仕様とします。
- 前記の「カード所持者の同意」のためには同意をあらわす暗証番号の入力などが必要で、その暗証番号自体を「なりすました端末機」に盗まれたりすることのないように、所要のセキュリティ対策が措置されることを前提とします。
- また、任意の利用者がカード所持者の同意の下に「上位アプリケーション」内のファイルに個別の「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」を書き込む際のセキュリティ確保についても十分な技術的措置が行われるものとします。

アプリケーション識別番号と個人識別番号

No	分類	アプリケーション識別番号(AID)	個人識別番号(PID)
1	会員証	A社ポイントカード （D392111111ABC11111111111）	A社の会員番号 (1234567)
2		B社レンタルショップ会員カード (D392222222123456789ABCDE)	B社の会員番号 (11111)
3		C社スポーツ倶楽部会員カード (D392333333000000000ABCFAD99881122)	C社の会員番号 (000111222)
4	口座番号	D銀行の口座番号 (D3924444441111111111111111111111)	D銀行の口座番号 (111-1234567)
5		E証券の口座番号 (D392555555000000000000000000000AA)	E証券の口座番号 (222-8899001)
6	サービス	F生命保険の保険番号 (D3926666661111111111111111111)	F生命保険の保険番号 (100-12345678)
7		G社ソフトのライセンス番号 (D392777777000000000000ABC)	G社のAAソフトのラインセンスID (AA-0132364)
8	ユーザID	H社サイト[http://www.**.abc.com] (D392888888111111222222222)	H社サイトのユーザID (entry_name01)
9		I社のWebメール[http://www.**.mail.com] (D392999999111122222222333)	I社サイトのメールアドレス (mail_add001)

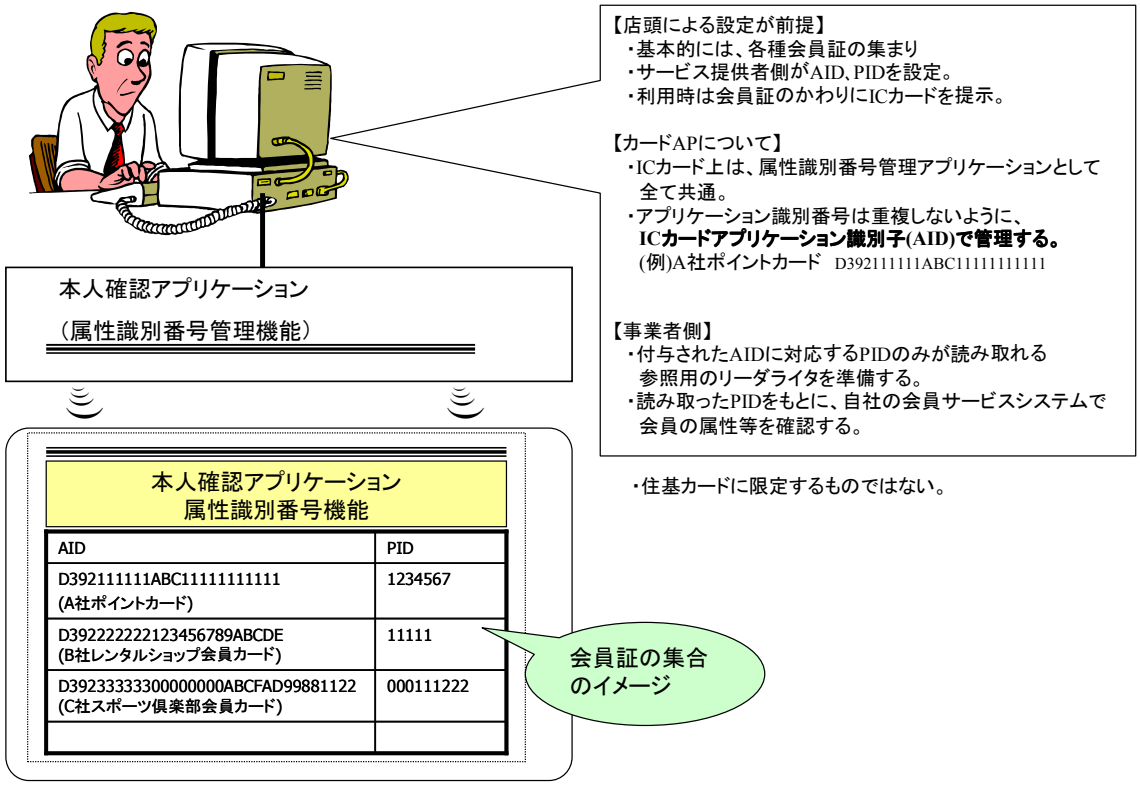


図 5－属性識別番号管理機能（店頭・窓口）

4.4　様々なアプリケーションに使える「属性識別番号管理機能」

私達は、様々な IC カードアプリケーションに使える「属性識別番号管理機能」の普及によって、現在の制度運用のままで、公共民間を問わず多数の IC カードアプリケーションに住民基本台帳カードを使用できるようにすることを提案します。

社会の電子ネットワークが高速化され、ネットワーク使用の通信コストが低減されるにつれて、カード内に複雑な論理構造を持たない後者のタイプのアプリケーションが多く使用されるようになっています。そこで、この「属性識別番号管理機能」を用いれば、発行者の市町村が特定のアプリケーションを採用しなくても、現在一般に普及されている IC カードアプリケーションの内、かなりの（おそらく半分以上の）ものが、当該個別アプリケーションの発行者が望む場合、住民基本台帳カードに搭載された「本人確認アプリケーション」でも実質的に使えるようになるのではないでしょうか。

前項で述べたように、この「属性識別番号管理機能」は、おそらく世間ですでに普及されている様々な IC カード登録証と併用することができ、その IC カード登録証をつうじて実現されるアプリケーションが、住民基本台帳カードでも実現可能になります。

「属性識別番号管理機能」は、学校・会社など法人団体の構成員の識別、各種のビジネスの会員識別などに汎用することができます。が、一方で登録証そのものではありませんか

ら、特定の市町村が「本人確認アプリケーション」の搭載を拒否しても、その地域の住民が社員証・学生証・会員証などの登録証をもらえないということにはなりません。

また、この「識別番号管理機能」とリンクする「汎用 ID ストレージ」内に記録されたすべての「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」をカード所持者だけが読み出せるようなソフトウェアと併せて用いれば、一種の ID 備忘録としても機能します。電子ネットワークの普及とともに、個人が保持する識別番号（PID）の種類は飛躍的に増大しており、現在は大多数のひとが何らかのメモ帳にそれを記録しなければならなくなっています。「汎用 ID ストレージ」はセキュアな電子メモ帳として個人が保持する識別番号（PID）を安全に管理するのにも役立ちます。

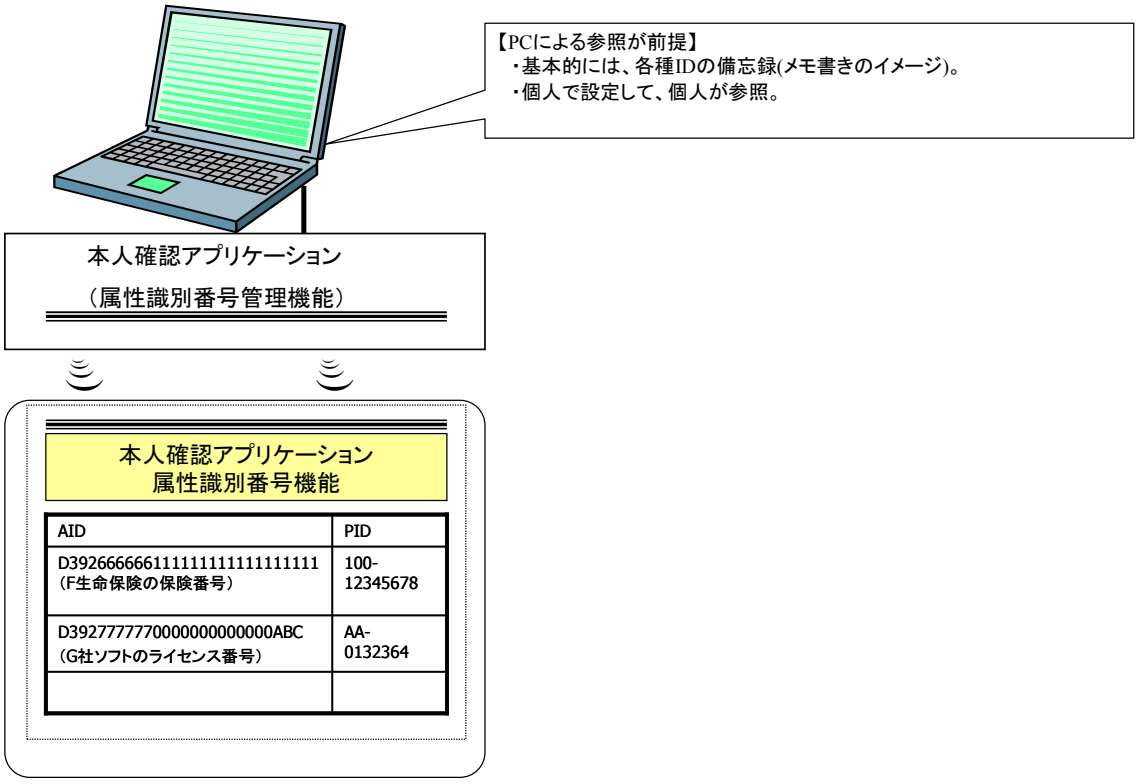


図 6－電子 ID 備忘録

なお、個別 IC アプリケーションの識別番号（AID）については、すでに数年前から国の登録制度が実施され、財団法人日本規格協会の管理下で、法人・団体が任意にこれを取得できるようになっていることを付記します。

4.5　中小規模の事業者に IC カードシステム活用の基盤を提供

私達が提案する住民基本台帳カードの「本人確認アプリケーションの属性識別番号管理機能」を用いれば、これまで自分で IC カードシステムを構築するには、規模が小さすぎて投

資に耐えられなかった、中小規模の事業者も、住民基本台帳カードを基盤として自己の IC カードシステムを構築することが可能になります。

その場合、当該事業者は、自分で IC カードを発行しなくとも、顧客やメンバーの住民基本台帳カードに自己の「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」を書き込むだけで、パソコン、端末機、「本人確認アプリケーション-属性識別番号管理機能」を用いるためのパソコン用ソフトウェア、既成の顧客管理ソフトなどを購入し、公的機関に自己の端末機を登録すれば、たとえば、「○○商店の顧客優待会員システム」とか「○○専門学校の学生証・受講履歴管理システム」とかを実現することができるようになります。

4.2 項で既に述べたように、このような場合、住民基本台帳カードの発行者である市町村は、どんな「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」がその中に書き込まれるかについては関知しないわけですから、個別アプリケーションの使用・運用上の責任は、カード所持者と個別アプリケーション発行者が負うことになります。

4.6 アプリケーションの例外（ゲート通過管理など）

この章で述べてきたいわゆる「属性識別番号管理機能」は、原則としてカード所持者本人の同意をあらわす暗証番号（PIN）の入力がなければ内部の情報を読み出せない仕様を想定しています。内部の個人情報が不当に端末機側に移転することを防ぐためです。

しかし、建物のゲート通過管理など、「カード所持者がかざすだけで通過する」利便性が求められる場合には、暗証番号の入力がなくても端末機側が特定アプリケーションの個人識別番号（PID）だけを読み出せるような、例外的な仕様を設けることも提案します。

この場合は、「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」を書き込む際に、「この組み合わせについては暗証番号を入力しなくても読み出してよい」という、カード所持者側の同意に基づいて書き込み設定をする仕様とします。

4.7 他のカードやメディアとの相互運用（インタフェースの仕様統一）

これまで述べてきた「属性識別番号管理機能」の概念は、必ずしも住民基本台帳カードに限るものではありません。

セキュアなメモリ領域である「ID ストレージ」から「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」を読み出すようなアプリケーションについて、機能の概要とインターフェースの仕様を全国共通で統一しておけば、このような「属性識別番号管理機能」を住民基本台帳カードとは別のカード内にもつことも可能ですし、住民基本台帳カード内に「本人確認アプリケーション」から「属性識別番号管理機能」だけを独立させたアプリケーションをもって運用することも可能です。また、前項で述べたような、学校、企業などが自分の団体の IC カード登録証を発行し、その内部に同じインターフェー

ス仕様を持つ「専用 ID ストレージ」をもつようにすれば、「専用 ID ストレージ」を持つカードでも「汎用 ID ストレージ」を持つカードでも同じ「IC アプリケーション識別番号（AID）と個人識別番号（PID）の組み合わせ」を読み出すことができ、両者の併用が可能となります。

要すれば、この「汎用 ID ストレージ」のインターフェースの仕様と機能概要を統一さえしておけば、民間の複数の事業者が「ID ストレージ」のソフトウェアを開発販売し、たとえばセキュリティと相互運用性について第三者機関の評価認証・確認を受けた「汎用 ID ストレージソフトウェア」を、個別の市町村が住民基本台帳カードに採用する。一方で、様々な個別アプリケーション発行者・利用者も自らの専用「ID ストレージ」ソフトウェアを採用購入するといった運用を想定することができます。

このようにして、セキュアな「本人確認」の場をさらに広げいくような、社会的なシステム基盤を構築することが可能になります。

また、電子ネットワーク上でこの「属性識別番号管理機能」と次章で提案する「簡易認証局機能」による本人確認とを併用すれば、電子ネットワークを通じた様々なビジネスをセキュアに行うための基盤を構築することも容易となることでしょう。

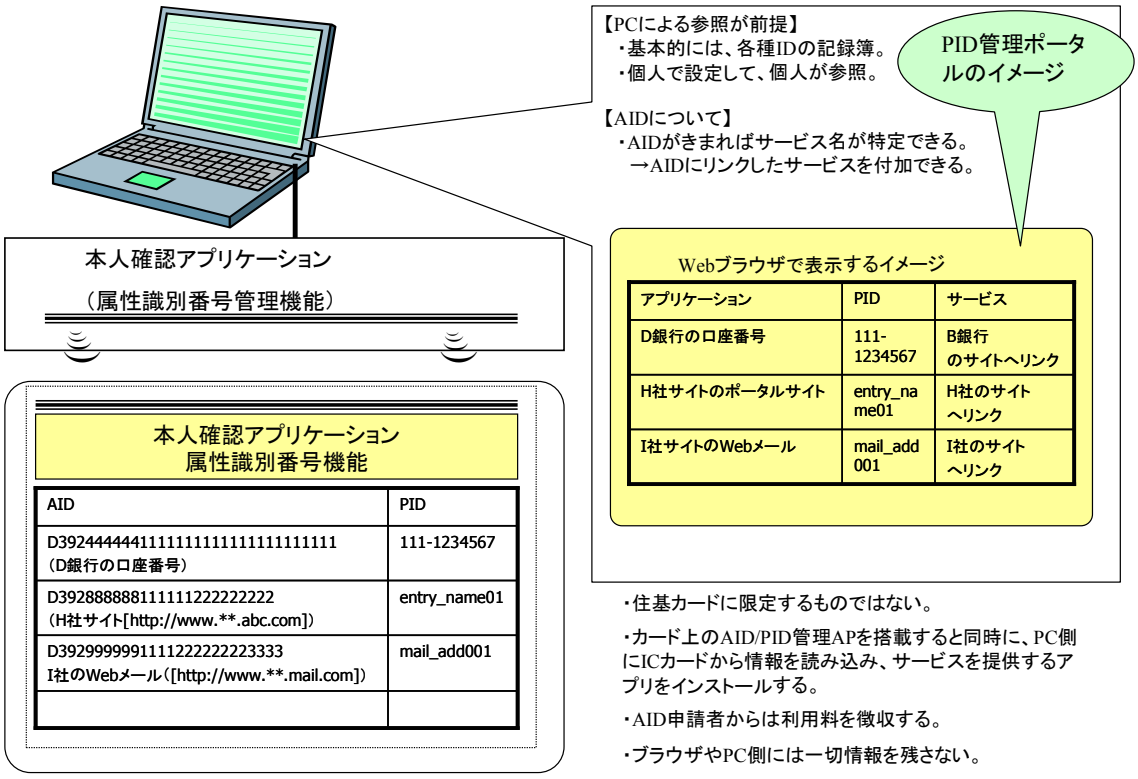


図 7－属性識別番号管理機能（電子ネットワーク）

第５章　電子ネットワーク上の本人確認

5.1　電子ネットワーク上の本人確認

「なりすまし社会」のもう一つの場面、「電子ネットワーク上のなりすまし」を防ぐ対策として、IC カード上に搭載され、「顔の見えない」ネットワークの向うの相手に、交信者が本人であることを証明する電子認証のアプリケーションが有効です。

住民基本台帳カードには、現在のところ、民間も含めて誰でも利用可能な電子認証のアプリケーションは搭載されていません。

私達は、住民基本台帳カードに、こうした「電子ネットワークをつうじて本人であることを確認する」アプリケーションが搭載されることが、普及のための有力な手段のひとつと考えます。

5.2　公的個人認証アプリケーション

既にこれまで述べたように、住民基本台帳カードには、電子行政申請をするときに申請者が本人であることを確認するための全国共通の「公的個人認証アプリケーション」が搭載可能で、既に発行済みの多数の住民基本台帳カードに搭載されています。

この「公的個人認証アプリケーション」は、セキュリティ技術的にもかなり精度が高く、行政事務上の申請者の本人確認を行うのにも十分な機能を持っていますが、残念ながら民間の使用には開放されていません。

「公的個人認証アプリケーション」を民間で使用して本人確認をすることが禁じられている理由としては、次の二つが想像されます。

- 民間を含む多数の利用者にこのアプリケーションが広まることによって、不正な者がこのアプリケーションを利用する利益が増大し、その結果セキュリティ上の脅威が増大して、技術的に精度の高いアプリケーションであっても「破られる」可能性が高まること
- 公的機関が発行する「電子的な本人確認の証明」が広く使われるようになれば、民間の電子認証局事業が利用されなくなり、いわゆる「民業圧迫」につながること

この内第一の理由についていえば、もし現在の「公的個人認証アプリケーション」が、民間で使用されても容易に「破られない」ものであるなら、その使用を一般に開放しても問題はないはずです。が、もしセキュリティ上の懸念が払拭できないのであれば、似たような機能を持つ別のアプリケーションソフトを広く一般用途に普及させるのも一案と考えます。

第二の理由についていえば、民間認証局事業が認証するのは、主に個人や法人の属性（ある個人は○○の資格を持つこととか○○団体に所属していること、ある法人が医療機関であることとか）です。「個人が本人であることを確認すること」は直接民間認証局事業の対象となってはいないので、「公的個人認証アプリケーション」を「本人確認」に用いることは、

「民業圧迫」には当たらないのではないかとも考えられます。

5.3　公的個人認証アプリケーションと民間認証局事業者との連携

公的な機関による電子ネットワーク上の本人確認が、民間でいま事業化される途上にある電子認証局事業と競合するという問題については、次のようにも考えられます。

まず電子認証局事業の事業とは、いわゆる「電子署名」を発行する事業ですが、そもそもこの事業を利用する者の本人確認自体は、通常直接対面で行われているわけではなく、利用者の申請住所になんらかの暗証番号もしくは暗号鍵が郵送されてくるなどのやり方で、間接的に行われています。

そこでたとえば、「公的に認定された電子認証局を運営する民間の事業者」に対してだけ、「公的個人認証アプリケーション」サービスを拡張開放し、「利用者が本人であることを確認する」ような、いわば「電子認証局事業の信用の源泉」を提供するやり方であれば、民業圧迫や競合の問題は発生しないと考えられます。「特定の認定された電子認証局」に対する「本人確認」を行うアプリケーションであれば、それほどセキュリティ上の脅威が拡大するとは考えられません。

また、「公的個人認証アプリケーション」を民間認証局事業の顧客の「本人確認」に用いることは、民間認証局事業のコストを引き下げることにつながりますので、むしろこのことは、民間認証局事業の普及促進につながるものと考えられます。

5.4　「本人確認アプリケーション」の「簡易認証局機能」

前記した「特定の認定された民間電子認証局」に対する「公的個人認証アプリケーション」サービスの開放であれば、それほどセキュリティ上の脅威が拡大するとは考えられませんが、「公的個人認証アプリケーション」サービスを民間一般に開放することには、セキュリティ上の懸念が払拭しきれないとも考えられます。

そこで、上記のほかに、私達は、住民基本台帳カードの「本人確認アプリケーション」の一部として、市町村のサーバが「個人の基本四情報」に限って直接「本人確認を求める」一般の利用者に、住民基本台帳カード所持者が「本人」であることを確認する「簡易認証局」のような機能を提案します。

5.5　「簡易認証局機能」のアプリケーション仕様

前記の「簡易認証局機能」の仕様は、カード保持者が自己のパーソナルコンピュータにカード端末機をつなぎ、センターサーバと交信してなんらかの暗証番号などを入力するようなやりかたの、一種の電子認証局型のものになると考えられます。

- 「簡易認証局機能」は「本人確認アプリケーション」の一部分として、民間のアプリケーション開発業者によって開発され、第三者のセキュリティ評価・認証、公的機関の相互運用性の確認を受けたソフトウェアを市町村が採用し、発行します。

- 「簡易認証局機能」は「カード所持者」「この機能を利用して電子ネットワーク経由で本人確認を求める事業者」「簡易認証局機能を管理する公的機関」の間で、いわゆる公開鍵暗号方式によってカード所持者の本人確認を行う機能とします。
- 「簡易認証局機能」の発行に際して、市町村は住民基本台帳カード内に、カード所持者の基本四情報（氏名・生年月日、性別、住所）と当該個人が住民であることの証明を暗号電文で書き込みます。
- 市町村は、「簡易認証局機能を管理する公的機関」に、カード所持者を登録します。
- 「簡易認証局機能を利用して電子ネットワーク経由で本人確認を求める事業者」は、「個人情報保護法に基づく適正な個人情報管理」を誓約し、「簡易認証局機能を管理する公的機関」に自らを登録します。この事業者は登録及び個人の認証の都度、公的機関のコストを負担し、利用料を支払います。
- カード所持者は、電子ネットワークを通じて本人確認を求められたとき、カード内に書き込まれた暗号電文を、「本人確認を求める者」に送信します。
- 「簡易認証局機能を利用して電子ネットワーク経由で本人確認を求める事業者＝本人確認を求める者」は、受信した暗号電文をカード所持者の「簡易認証局機能を管理する公的機関」と交信することによって、復号します。その際自らが真正な登録済み事業者であり、暗号電文が真正なカード所持者によって送信された者でなければ、前記の復号が成功しないような仕様とします。
- アプリケーションの発行、利用者の登録認証等の管理・運用、については、第 3 章の「本人確認アプリケーション基本機能の仕様」に準じるものが考えられます。

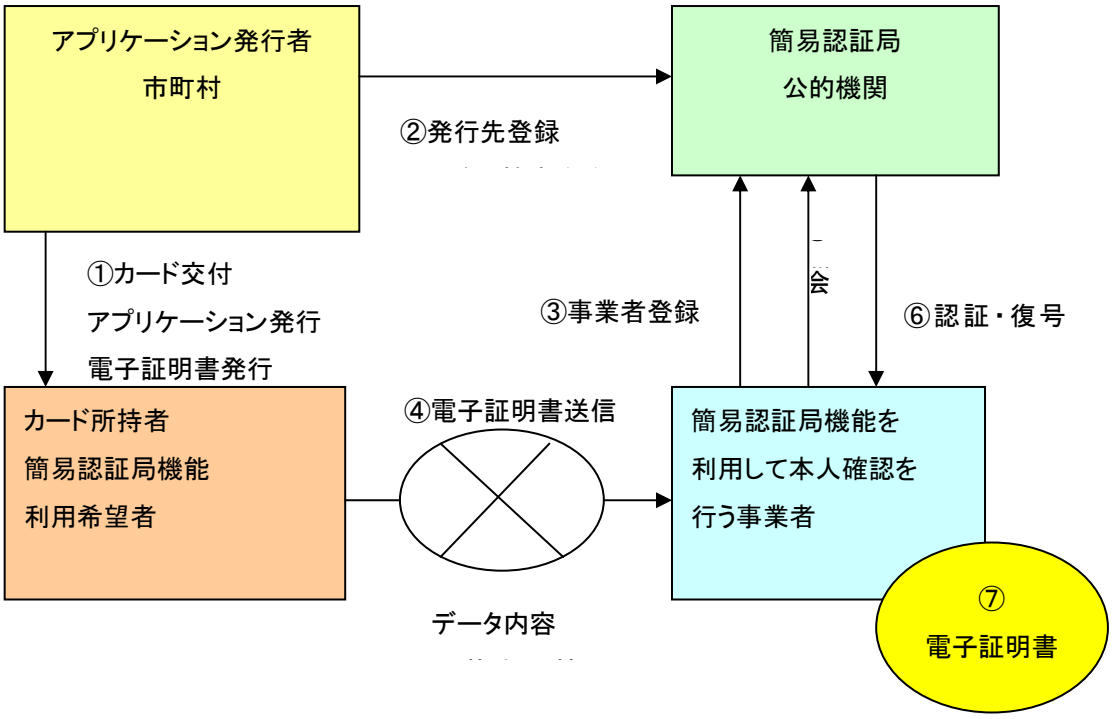


図 8－簡易認証局機能のフローイメージ

第６章　その他の機能

6.1　金融決済アプリケーション

住民基本台帳カードをもっと使いやすい便利なものにするという観点で、私達の間で話題になった多数のアプリケーションについては、第 5 章で述べた方法によって、「どのアプリケーションか」を問題にすることなく解決可能と考えられます。

が、「汎用 ID ストレージ」では搭載できない「ソフトウェアのような論理構造をもって、端末機側との交信を通じてカード内でかなりの演算処理を行う」タイプのアプリケーションを用いるものとして、金融決済のアプリケーションをあげることができます。

住民基本台帳カードに望まれる拡張機能として、行政機関への手数料の支払い等のためのペイメント機能は重要なもので、住民基本台帳カード普及の拡大に資することは確実と思われます。

ただし、このためには、非接触式カードである住民基本台帳カードと、従来金融機関側で接触式カードを前提に開発されてきたシステム基盤やセキュリティ仕様との相互運用性を確保するために、多岐に渡る技術的な調整をはかることが必要であり、実現のためには、解決すべき問題がきわめて多くあることを申し添えます。

6.2　「何でも書けるセキュアな電子メモ帳」アプリケーション

上記の他に、住民基本台帳カードメモリ領域の一定部分を、カード所持者がテキストで秘密の電子メモやパスワードを書けるようなアプリケーションも提案します。

このアプリケーションは、カード所持者の暗証番号入力だけでなく、パソコンに付属した、またはパソコンに連結した携帯電話などの CCD カメラによって所持者の生体情報（顔画像）を撮影し、これを「本人確認機能アプリケーション」を用いてカード所持者の生体情報と照合することによって、カード所持者本人でなければメモリ領域のデータをパソコン上で開披できないようにするような仕様とし、万一カードを落としても、盗まれても、データのセキュリティを確保できるようにすることを提案します。

第７章　市民カードセンター運用のイメージ

本章では、この提言の原案を作成後に委員会内の技術 TF、政策 TF の内部で提起された様々な意見を受けて、この提言を実現していく際に必要になると考えられるアプリケーションの実質的な運用主体と、運用のイメージの概要を述べることとします。

7.1　　市民カードセンター

民間のセクターによって設立され、なんらかの公的な承認とこの方式を採用する全市町村からの委託を受けて、「本人確認アプリケーション」運用のための業務を行う機関を、ここでは、「市民カードセンタ」と仮称することにします。市民カードセンタは、全国で単一の組織を持ち、広範な事業所（たとえば、民営化後の郵便局や鉄道駅、コンビニエンスストアなど）をもつ事業体と連携して、次の業務を行うものとします。

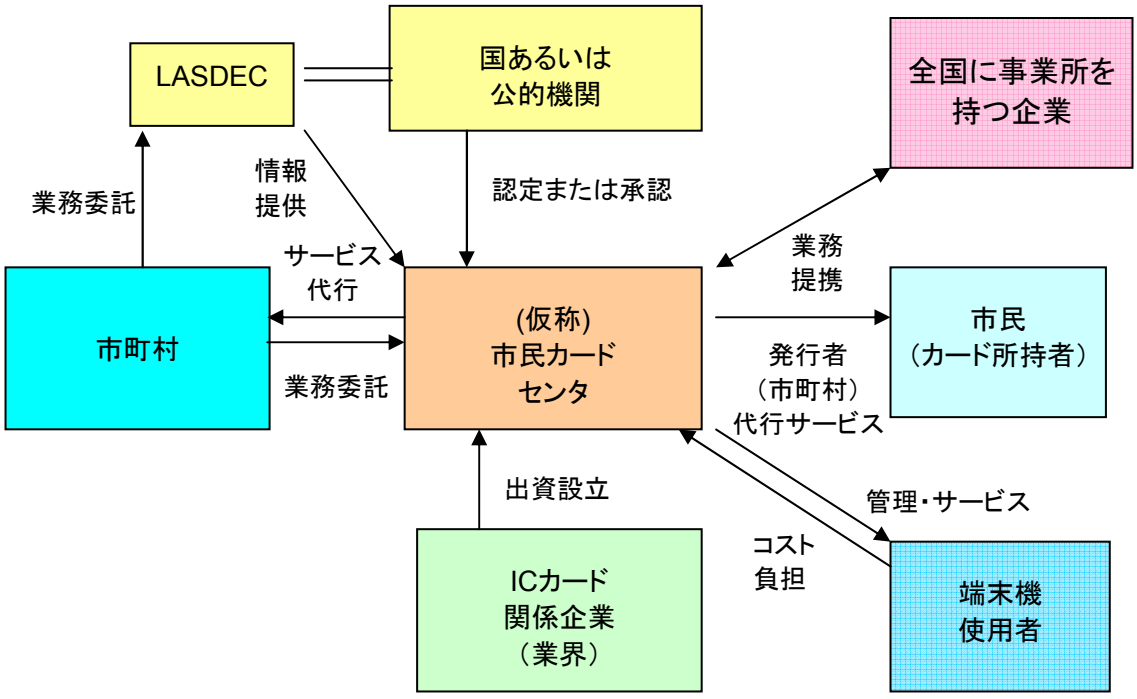


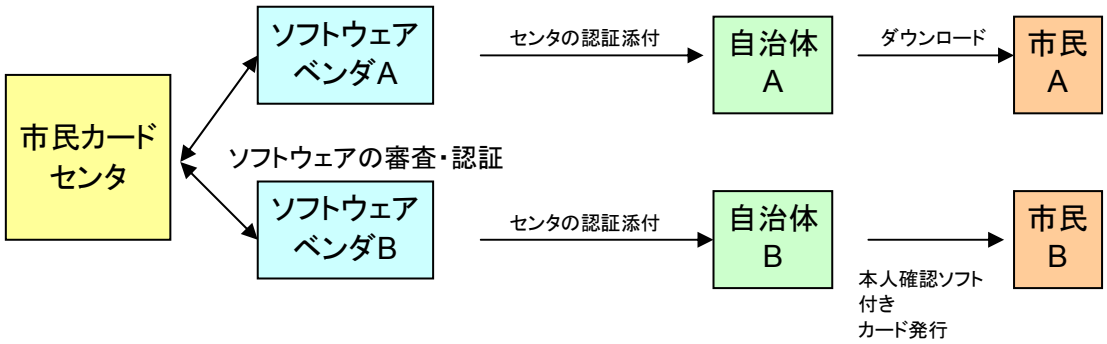
図 9－(仮称)市民カードセンタの設立イメージ

7.2　　本人確認アプリケーションの認証・ダウンロード（インストール）業務

市民カードセンターは、標準化された仕様に基づいて、複数の製造者が開発製造する「本人確認アプリケーション」ソフトウェアが、セキュリティ要求仕様を満たすか、互換性を持つか、どのカード媒体と適合するか等について、試験・認証を行います。

市町村は、市民カードセンターの試験・認証に合格した上記本人確認アプリケーション（ソフトウェア）を調達するものとします。（カードは、住基カードでも、そうでなくてもよい。）

また、市民カードセンタは、市町村が「本人確認アプリケーション」を、発行済みの住民基本台帳カードにインストールする業務を支援または代行します。



ソフトウェア審査の内容:
全タイプ端末機との互換性試験、セキュリティ評価、ダウンロード試験・・・

図 10－本人確認アプリケーションの認証・ダウンロード業務

7.3　　端末機の認証・配布業務

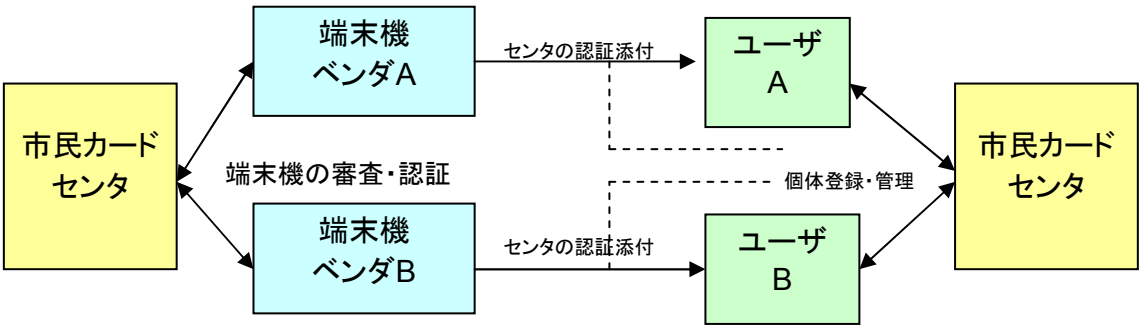
市民カードセンタは、本人確認アプリケーションの運用に掛かる IC カード端末機が、耐タンパー（侵入）性を持つか、端末機の使用者も含めて権限のない者によって偽変造されない仕様になっているか等について試験・認証を行います。

市民カードセンタは、この試験・認証に合格した製品のみが、本人確認アプリケーションの端末機として使用されるように次項（オーソリゼーション業務）の運用を行います。

＜注＞

私たちは、IC カードシステムにおいては、広く一般の人々によって、殊更に厳しい管理を行わない環境下で端末機が使用されても、セキュリティを保てることが望ましいと考えます。そのためには、端末機器の耐タンパー性、偽変造耐性が求められます。本人確認アプリケーションという社会のセキュリティの基本を司るようなシステムにおいては、カードだけではなく端末機器やセンタサーバ側のセキュリティ要求仕様を標準化し、これを試験・認証していくことが望まれます。

このような方向をめざす動きとしては、例えば、欧州から国際標準規格化が提唱されている Secure and interoperable smart card reader (ISO/IEC 24727：ISO/IEC SC 17/WG 4/TF 10 にて審議中) などが参考になります。



端末機審査の内容:
全タイプのソフトウェアとの互換性試験、セキュリティ評価、耐タンパー性試験
改造不能性確認、データ送受信試験・・・

個体登録・管理の内容:
ベンダ販売時の個体特定、ユーザ登録、ユーザとの契約、IDの発行、「怪しい」
個体振る舞いの検出、契約違反個体の機能停止・・・

図 11－端末機の認証・配布業務

7.4 オーソリゼーション業務

本人確認アプリケーションは、基本的にはカードと端末機間の交信によって、本人を確認する仕組みですが、偽変造されたカードや端末機によるシステムの悪用を防ぐこと、個人情報の授受記録を電子的に残すこと等を目的として、ほぼリアルタイムに近いオーソリゼーションの仕組みを持つことが望まれます。

市民カードセンタはこのようなオーソリゼーション業務を行います。具体的には、住民基本台帳カードの「標準アプリケーション」運用者として、無効カード情報を市町村から受取りカードのオーソリゼーションに用いること、端末機の登録管理を行って、権限のない端末機によってトランザクションが行われるのを防止すること等が業務内容となります。

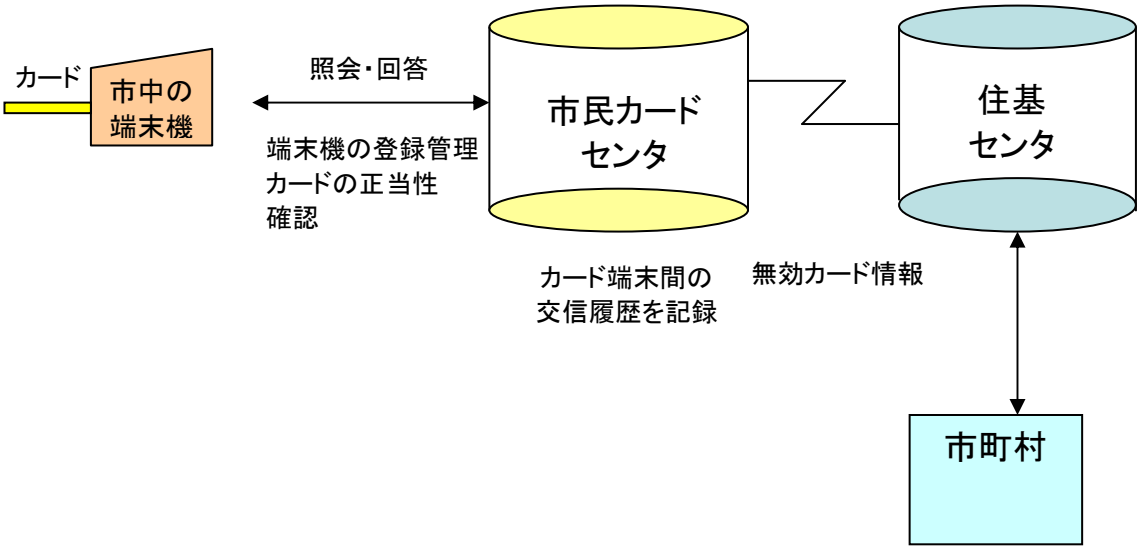


図 12－オーソリゼーション業務

7.5　　簡易認証局サーバの運用管理

市民カードセンタは、第 5 章で述べた本人確認アプリケーションの「電子ネットワーク用本人確認機能」において、市町村から電子証明書の登録情報を得て、市町村の代行者として簡易認証局業務を行います。（**図 8** 参照）

7.6　　データトランスファセンタ業務

市民カードセンタは、転居、有効期限切れなどによる住民基本台帳カードの更新時に、本人確認アプリケーションを用いてカード内に記録されている情報の一部または全部を、新しいカードに安全に（個人情報を守ることができる状態で）移転、再書き込みする業務を行います。このような業務を行う拠点をデータトランスファセンタと呼び、市町村窓口ばかりでなく、（たとえば、民営化後の郵便局や鉄道駅、コンビニエンスストアなど）広く住民が利用しやすい任意の場所で、安全な運用管理の下で情報の移転、再書き込みが行われることをめざします。

＜注＞

冒頭において述べた、この提言原案作成後の検討において、「本人確認アプリケーション」を利用する各種の民間事業者などが各々設定するデータの有効期限と、住民基本台帳カードの有効期限が必ずしも一致しない場合が多いという指摘がありました。討議の結果、転居、有効期限切れなどによる住民基本台帳カードの更新時には、このような情報の移転・再書き込みが必要な場合があるとの観点から、データトランスファセンタ業務の機能を追補することにしました。

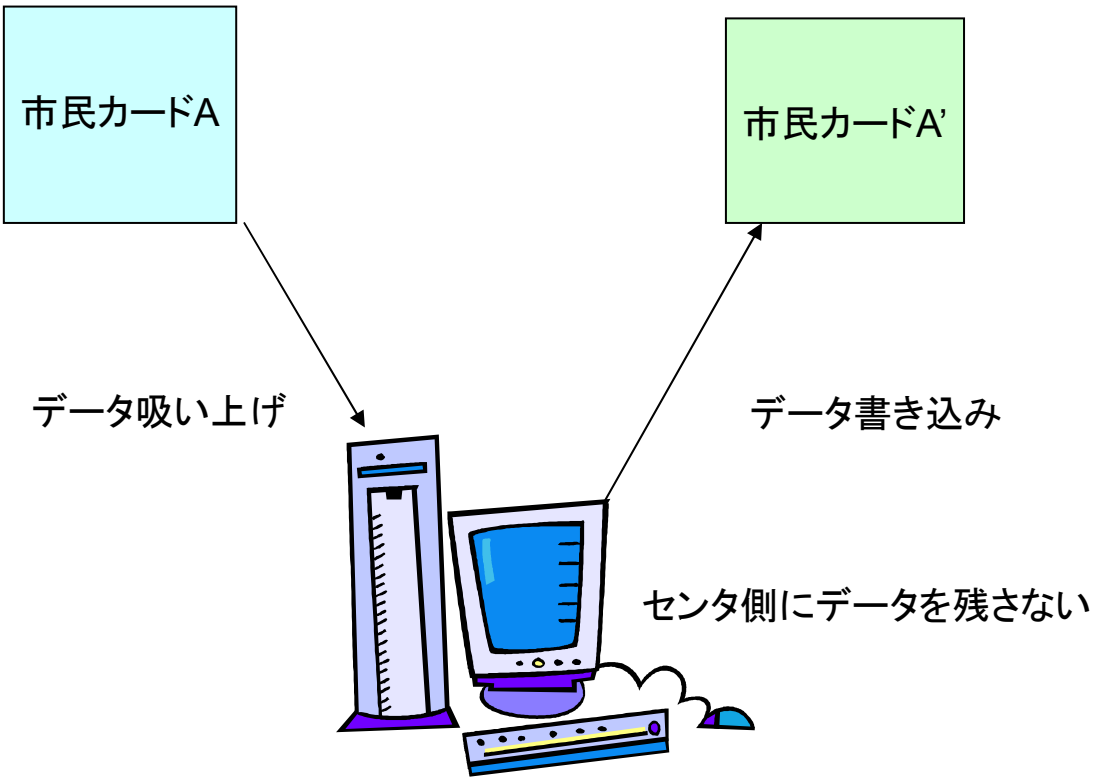


図 13－データトランスファセンタ業務

7.7　　市民カードセンタの運営コスト

市民カードセンタの運営コストは、「本人確認アプリケーション」を用いて、業務を行う事業者が応分に負担すべきものと考えます。

直接には、端末機の利用者からの利用料の徴収などが現実的と考えられます。

- 端末機の認証に対して手数料を徴収する方式
- トランザクションに比例した利用料を受け取る方式
- 端末機自体を市民カードセンタが保有しレンタル料を利用者から受け取る方式

等が考えられます。

市民カードセンタ業務マトリクス

業務名	業務の内容	委託者	業務主体	サービス対象先	コスト負担	提携先
本人確認アプリケーションの認証	IC カードに搭載する本人確認アプリケーション・ソフトのセキュリティ・互換性等を審査し認証する	製造者	市民カードセンタ	市町村	製造者	－
本人確認アプリケーションのダウンロード	認証された本人確認アプリケーション・ソフトを発行済み使用中の住民基本台帳カードにダウンロードする	市町村（カード発行者）	市民カードセンタ	市民	市町村	全国に事業所を持つ企業とセンターが提携
本人確認アプリケーション付きカードの新規発行	認証された本人確認アプリケーション・ソフトを搭載した住民基本台帳カードを新たに発行する		市町村	市民	市町村	市民カードセンターが業務支援する場合も・・・
端末機の認証	本人確認サービスに使用する端末機のセキュリティ・耐タンパー性・互換性等を審査認証する	製造者	市民カードセンタ	端末機使用者	製造者	－
端末機の登録	認証された端末機とその使用者を個体登録する	端末機使用者	市民カードセンタ	端末機使用者	端末機使用者	全国に事業所を持つ企業とセンタが提携
端末機の配布・管理	認証された端末機をその使用者に送付し使用中も管理する	端末機使用者	市民カードセンタ	端末機使用者	端末機使用者	全国に事業所を持つ企業とセンタが提携
オーソリゼーション	市民カードが有効であり正当な使用者によって使用されていることを端末機使用者に認証する	端末機使用者	市民カードセンタ	端末機使用者	端末機使用者	－
トランザクションの記録	カード端末間の交信記録を保持し管理する 不正使用の疑いがあるときは適切に処理する	端末機使用者	市民カードセンタ	市民	端末機使用者	－
トランザクション記録の発信	カード端末間の交信記録を定期的にカード所持者に連絡する	市民	市民カードセンタ	市民	市民の自己負担	－
簡易認証局業務	ネットワーク上の電子証明書の発行	市町村（カード発行者）	市民カードセンタ	市民・アプリケーションユーザ	市町村及びアプリケーションユーザ	－
データトランスファセンタ	カード更新時に本人確認アプリケーションのファイルに記録された有効な情報データを新規カードにセキュアに移転する	市町村（カード発行者）	市民カードセンタ	市民	市町村（カード発行者）	全国に事業所を持つ企業とセンタが提携

むすび　セキュアな 21 世紀社会のために-今こそ IC カードの活用を！

住民基本台帳ネットワークの運用については、いまもかなり激しい賛否の論議があります。

ひとことで言えば、「国民総背番号制」によって官庁に自分の生活のすべての情報（住所、電話、履歴、家族名等だけでなく、海外渡航歴、運転履歴、医療機関の利用歴、納税履歴から、民間機関でのクレジットの利用歴、預金の引き出しに至るすべての情報）が管理されてしまうのではないかという本能的な疑いが一部の国民の側にあり、一方国の側では、住民基本台帳ネットワークとはそのような機能を持つものではないことを弁明するというのが、これまでの論争の焦点であったか思われます。

今、私達はその賛否について議論しようとするものではありません。

しかし、この論議の結果、住民基本台帳ネットワークの副産物として生まれた住民基本台帳カードが、厳しい「目的外利用制限」を課され、さらに「機能拡張は市町村まかせ」とされてきたことが、莫大な国費と民間投資を投じ、社会のセキュリティを高める役割を秘めている、このカードシステムの普及の阻害要因となっているものと私達は考えます。

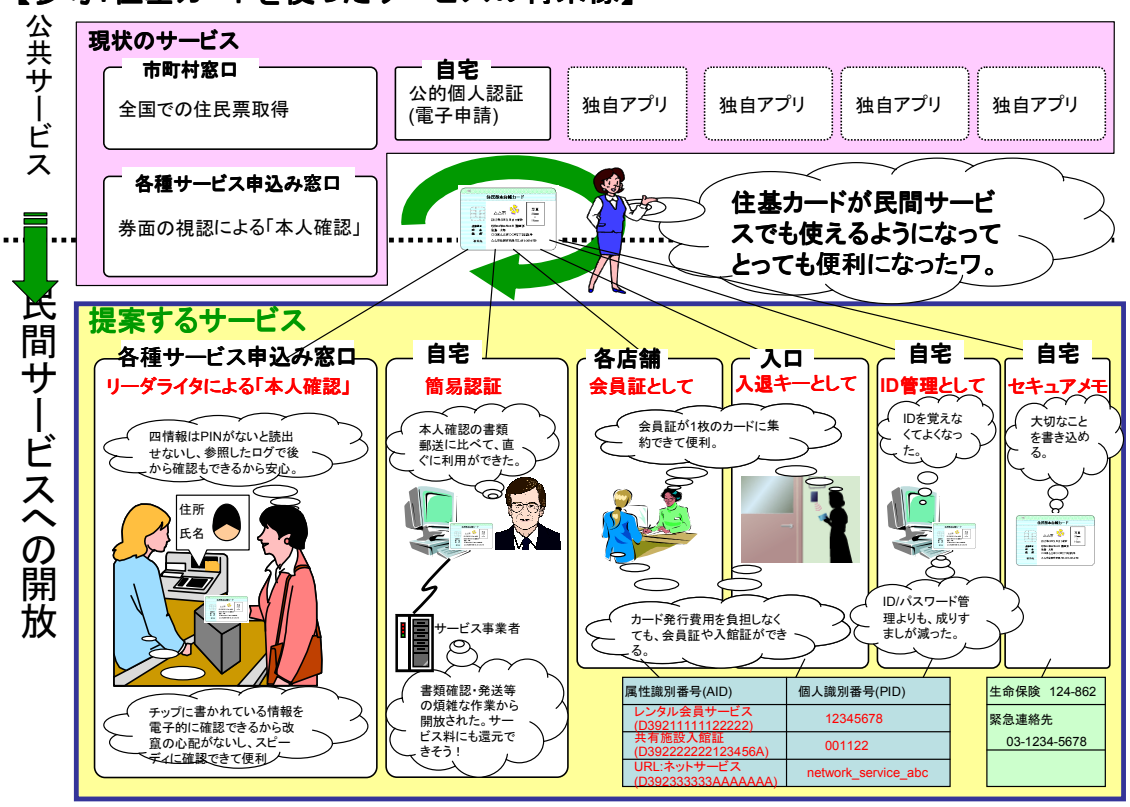
今回の私達の提言は、これまでの住民基本台帳ネットワークの制度運用をあまり大きく替えずに、ひろく「本人確認用途」に使えるようにすることを企図しています。

それと同時に、国民の間に潜在する「すべての個人情報を国家に管理されるのではないか」という危惧に対して、「こうした個人情報のファイルは、自分が所持する IC カードの中で自分だけがきちんと管理する」ということを提案するものです。

21 世紀の社会を、「なりすまし」犯罪や「個人情報漏洩」から防ぎ、より安全で暮らしやすいものにするために、今こそ住民基本台帳カードをはじめとする IC カードを、もっと活用していこう！

それが私達の願いであり、提言です。

【参考：住基カードを使ったサービスの将来像】



市民カード普及検討委員会 委員名簿

担当	委　員　名	所　属
委員長	家木　俊温	武蔵工業大学　環境情報学部 教授
政策 TF 主査	平松　雄一	電子商取引安全技術研究組合
政策 TF 主査代行	植村　泰佳	電子商取引安全技術研究組合
政策 TF 副主査	松澤　寿典	日本電信電話(株)
技術 TF 主査	松本　　勉	富士通(株)
委員	細田　泰弘 宮保　克明	エヌ･ティ･ティ･コミュニケーションズ(株)
	田中　武 安達　陽介	(株)エヌ･ティ･ティ・データ
	坂口　昌平	(株)エヌ･ティ･ティ･ドコモ
	劉　　維正	共同印刷(株)
	小川　竜一 中園　孝順	シャープ(株)
	森田　　直 高山　佳久	ソニー(株)
	酒井　正仁 姉川　武彦	大日本印刷(株)
	吉松　健三 鴨井　　誠	(株)東芝
	寄本　義一	凸版印刷(株)
	伊藤　恭之 今井達二己	日本信号(株)
	竹内　商陛	日本電信電話(株)
	朝倉　　久 林　　太郎	(株)日立製作所
	河瀬　恭一	松下電器産業(株)

委員	苅部　浩 吉岡　勉	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
アドバイザ	廣川　勝久	(株)ジーピーネット
事務局	竹内　眞人 中島　憲慈	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

【開催状況】

市民カード普及検討委員会：第 1 回 7/20/2004、第 2 回 3/25/2005、第 3 回 12/15

政策 TF：　第 1 回 9/3/2004、第 2 回 9/17、第 3 回 10/8、第 4 回 10/22、第 5 回 11/12、第 6 回 11/26、第 7 回 12/10、第 8 回 1/14/2005、第 9 回 1/28、第 10 回 2/10、第 11 回 2/25、第 12 回 10/7、第 13 回 10/28、第 14 回 11/11、第 15 回 12/1

技術 TF: 第 1 回 4/22/2005、第 2 回 5/13、第 3 回 5/27、第 4 回(合同) 6/17、第 5 回 6/24、第 6 回 7/8、第 7 回(合同) 7/22、第 8 回 8/24、第 9 回 9/9、第 10 回 9/22