電子行政サービス等へのアクセス手段の多様化に関する調査研究（デジタルテレビ等の固定系情報通信機器からの電子行政サービス等へのアクセス技術及び中央サーバに認証機能を一部移行させる方式の調査研究）報告書

平成 22 年 3 月

NTT コミュニケーションズ株式会社

目次

1. 調査研究の概要

1.1 背景

「IT 政策ロードマップ」（平成 20 年 6 月 11 日 IT 戦略本部決定）においては、「IT 基盤や利用環境の整備という点では大きな成果を挙げてきているが、IT が国民生活におけるサービス・付加価値の向上といった質的な面での成果につながっているか、さらにはその成果が国民に実感として伝わっているか、といった点においては、未だ改善の余地がある状況にある。」という現状認識がなされており、「オンライン利用拡大行動計画」（平成 20 年 9 月 12 日 IT 戦略本部決定）においては、「電子行政サービス等に対して、パソコンだけでなく、より普及率が高く多くの国民にとって身近なテレビ放送受信機や携帯電話端末等の情報通信機器を活用したアクセス手段の多様化について検討する」とされたほか、「中央サーバに認証機能を一部移行させることによって、個人がオンライン上で簡易にサービスを受けられる方策(カナダの e-Pass 類似の方式導入)の可否」等の検討に着手することが掲げられている。更には「原口ビジョン」（平成 21 年 12 月 22 日公表）においても、2014 年までに国民本位の電子行政の実現及び 24 時間 365 日のオンライン行政サービスの利用可能化することが目標として掲げられており、国民目線に立った電子行政サービス等の実現の必要性が高まっていることが伺える。

なお、平成 20 年度の総務省委託事業の「電子行政サービス等へのアクセス手段の多様化に関する調査研究」では、電子行政にアクセスする手段について、今後の実証実験のあり方の整理について報告されている。

平成 22 年 2 月からはコンビニエンスストアに設置されたキオスク端末と住民基本台帳カードを使用して、住民票の写しなどの交付が受けられるサービスが開始されるなど、電子行政サービス等の利便性向上が実感できるようになってきている。また、平成 23 年 7 月の地上波放送の完全デジタル放送への移行を迎えようとしている中、デジタルテレビがインターネット接続可能となり、電子行政サービス等へのアクセス手段の１つとして活用する環境が整いつつある。

1.2 目的

上記背景を踏まえ、本調査研究の目的を以下のように設定する。

本調査研究では、電子行政サービス等に対してパソコン以外の固定系情報通信機器（デジタルテレビ及びキオスク端末）が有効なアクセス手段であるか、また、中央サーバに認証機能を一部移行させる方式が実現可能であるかを明らかにするため、将来の実用化に向けて、関連する政府等の検討状況を整理し、各種課題の抽出、対策検討及び一部検証を実施した上で、有効性を確認するための実証実験のあり方の検討を行うことを目的とする。

1.3 概要

本調査研究の目的にしたがい、電子行政サービス等へのアクセス手段の多様化及び中央サーバに認証機能を一部移行させる方式について、検証環境も一部用いて、実用化できるレベルを念頭において進めることとする。図 1-1 に調査研究の進め方及び報告書の章構成を示す。

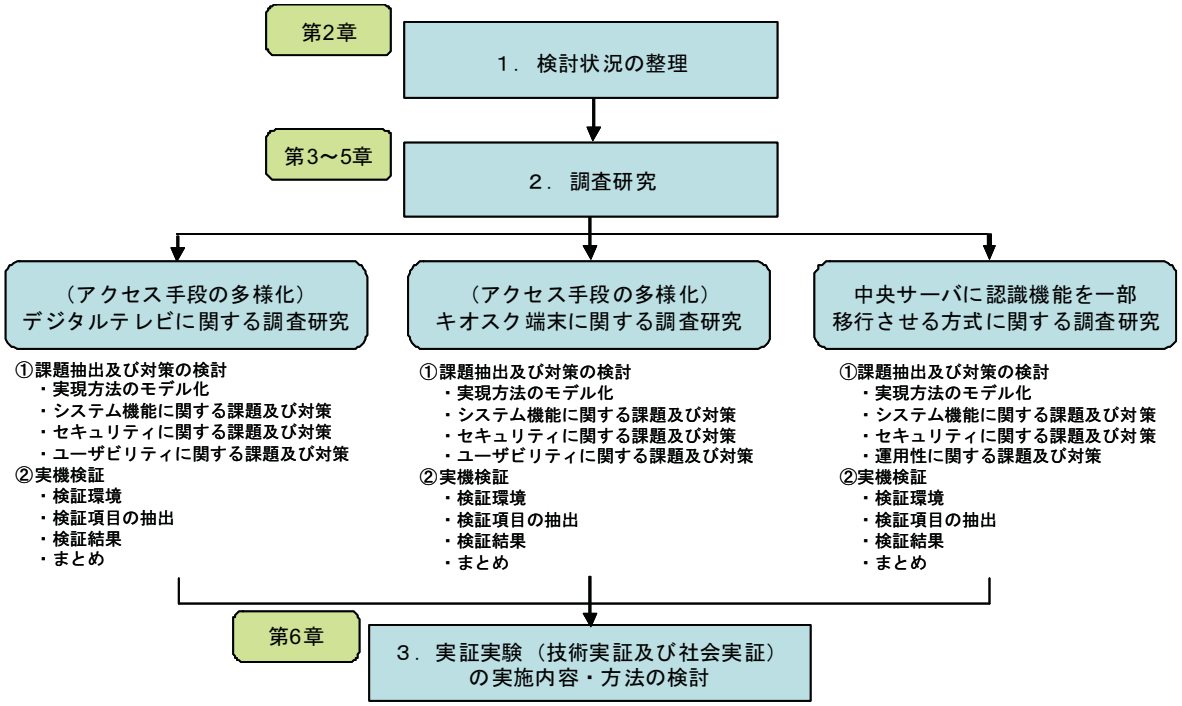


図 1-1 本調査研究の進め方及び報告書の章構成

1.3.1 検討状況の整理

関連する政府の検討動向、調査研究報告書、技術資料等を参考に技術調査を実施し、これまでの検討状況を明らかにする。また、キオスク端末に関しては、最新の動向を調査するため、関係機関へのヒアリングも実施する。

動向調査の参照資料は以下の通りである。

(1) 共通

- IT 政策ロードマップ
- 重点計画－2008
- 電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書（平成 20 年度総務省委託事業）

(2) 固定系情報通信端末機器からのアクセス多様化の検討

① デジタルテレビ

- 社団法人電波産業会(ARIB:Association of Radio Industries and Businesses) 標準規格（放送分野）
- デジタルテレビ情報化研究会機能仕様書
- 各社 最新デジタルテレビ　カタログ及び取扱説明書

② キオスク端末

- 2009 年版 セルフサービス情報端末（KIOSK）市場
- オンライン利用促進ワーキンググループ報告書
- 電気通信アクセス協議会ガイドライン
- 地方公共ネットワークに係る標準仕様
- 高齢者･障がい者等に配慮した電気通信アクセシビリティガイドライン 2 版

(3) 中央サーバに認証機能を一部移行させる方式の検討

- オンライン利用拡大行動計画
- ディペンダブル VLSI ワークショップ 2008 論文
- コンピュータセキュリティシンポジウム 2009 論文

1.3.2 調査研究

調査研究では、後述する電子行政サービス等へアクセスするための具体的な実現モデルをもとに、各構成要素に求められる機能を整理する。想定した実現モデルに対してシステム機能、セキュリティ、ユーザビリティ及び運用性に関して、課題の抽出を行う。課題解決に必要な対応・対策方法を調査・検討し、評価を行う。また、検討した対策の一部については実機検証を行い、検証結果と考察をまとめる。

(1) 課題の抽出及び対策の検討

① 実現方法のモデル化

固定系情報通信端末機器（デジタルテレビ及びキオスク端末）から電子行政サービス等へアクセスするため、及び中央サーバに認証機能を一部移行させる方式の実現に向けた具体的な実現モデルを 図 1-2 に示す。

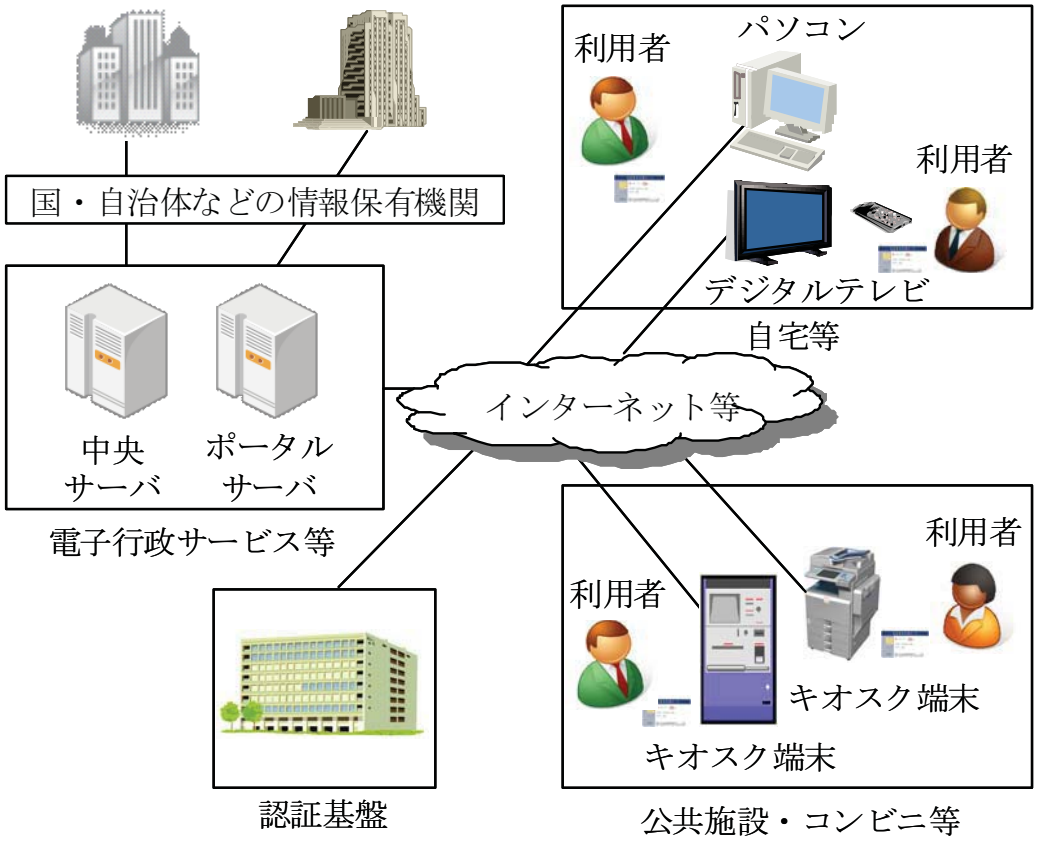


図 1-2 実現モデル

実現モデルを構成する各要素の想定される機能及び要件の詳細については、3～5 章で述べる。

② 課題の抽出及び対策の検討

電子行政サービス等へのアクセスのための実現モデルを踏まえ、実現モデルの各構成要素に対し、調査研究対象毎に以下の観点で課題の抽出及び課題解決のために必要となる対応、対策方法の検討を行う。

(i) (アクセス手段の多様化) デジタルテレビに関する調査研究

- システム機能に関する課題及び対策
- セキュリティに関する課題及び対策
- ユーザビリティに関する課題及び対策

(ii) (アクセス手段の多様化) キオスク端末に関する調査研究

- システム機能に関する課題及び対策
- セキュリティに関する課題及び対策
- ユーザビリティに関する課題及び対策

(iii) 中央サーバに認証機能を一部移行させる方式に関する調査研究

- システム機能に関する課題及び対策
- セキュリティに関する課題及び対策
- 運用性に関する課題及び対策
- 電子署名法による推定効に関する課題及び対策

(2) 実機検証

検討した対策について、一部検証環境を用いて実機で検証を行う。実機検証では、最初に検証環境を説明し、続いて検証項目の抽出及び結果について述べ、最後に検証結果をまとめる。

① (アクセス手段の多様化) デジタルテレビに関する調査研究

電子行政サービス等とデジタルテレビとの接続性や操作性など、ユーザビリティについての検証を行う。(1) IC カードリーダライタ接続形態、(2) リモコンでの操作性、(3) 電子行政サービスポータルへのアクセシビリティ、(4)電子行政サービスポータルサイトにおけ

るユーザビリティの４点について検証を実施する。

② （アクセス手段の多様化）キオスク端末に関する調査研究

電子行政サービス等とキオスク端末との接続性やユーザビリティについての検証を行う。(1) 電子行政サービス等への接続、(2) 認証基盤利用、(3) 紙情報の真正性確保、(4) 閲覧時のプライバシー確保及び端末の長時間占有を防止するための方法、(5) 端末内の個人情報保護、(6) 限定的な表示によるユーザビリティ確保の６点について検証を実施する。

③ 中央サーバに認証機能を一部移行させる方式に関する調査研究

中央サーバに認証機能を一部移行させる方式について実現。(1) HSM へのアクセス制御方式の検証、(2) サーバ連携型多目的 IC カードの構築に関する検証、(3) サービス提供者インタフェースの検証、(4) HSM による鍵管理のスケーラビリティ検証、(5) サーバ連携型多目的 IC カードを用いた基本的なサービスのフィージビリティ(実現可能性)検証の５点について検証を実施する。

1.3.3 実証実験の実施内容・方法の検討

パソコンと同様に自宅のデジタルテレビやコンビニエンスストア等に設置されたキオスク端末から電子行政サービス等へのアクセスを実現するため、及び電子行政サービス等の分野において、中央サーバに認証機能を一部移行させる方式が果たす役割を明確にし、実現するために必要となる実証実験について述べる。

オンライン行政サービスに 24 時間 365 日いつでもどこでも簡単にアクセスすることができる環境の構築に向けた実証実験として、実運用に向けた技術的な対策の検証や更なる課題の抽出を行う技術実証と、運用を想定した課題解決の検証を行う社会実証の内容及び方法について検討する。

2. 検討状況の整理

2.1 （アクセス手段の多様化）デジタルテレビ

2011 年 7 月の、地上波放送の完全デジタル放送への移行に向けて、国内各社からインターネット接続可能デジタルテレビが発売され、「デジタル放送推進のための行動計画（第 10 次）」（総務省 平成 21 年 12 月 1 日）によると、図 2-1 に示すように普及が拡大し、2009 年 9 月時点で、世帯普及率は約 69.5%（3,480 万世帯）となっており、2009 年末には約 77%（約 3,850 万世帯）に到達すると予想されている。

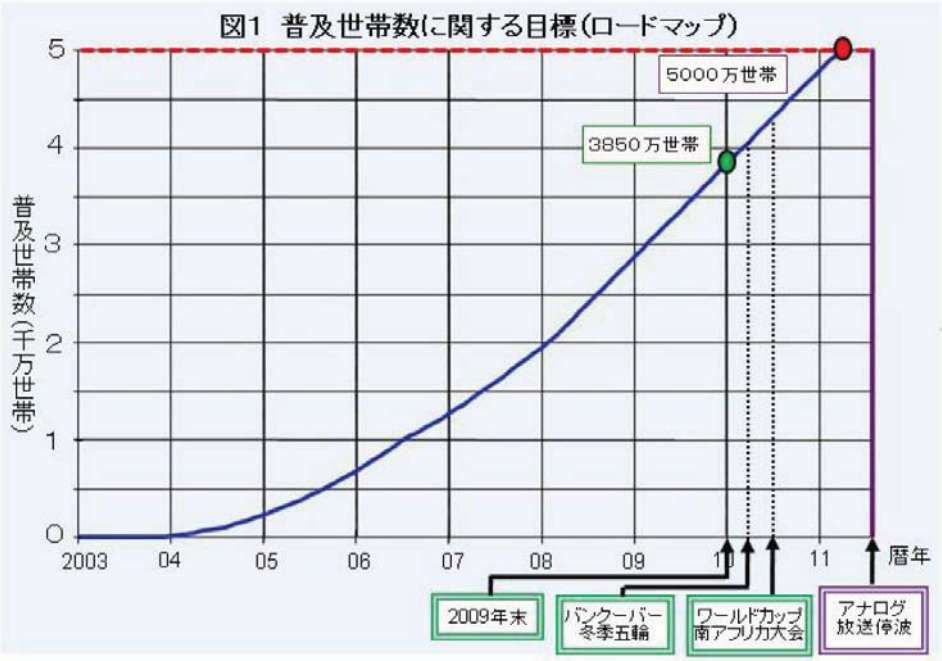


図 2-1 デジタルテレビ普及世帯数の遷移「デジタル放送推進のための行動計画（第 10 次）」より

また、テレビのデジタル化によって、インターネットへの接続ができるようになり、ネット対応テレビ向けのインターネットを介した動画配信サービスが行われるなど、デジタルテレビからのネット接続が普及しつつある。

また、「IT 政策ロードマップ」（IT 戦略本部、平成 20 年 6 月 11 日）においては、

> セキュリティレベルに配慮しつつ利便性の高い ID・パスワード方式の普及拡大に努めるとともに、携帯電話やデジタルテレビなどの活用によるアクセス手段の多様化等についても検討を行う。

とされ、「重点計画-2008」（IT 戦略本部、平成 20 年 8 月 20 日）では、

> 社会保障サービス等に関し、パソコンだけでなく携帯電話やデジタル放送受信機等の情報通信機器による、ネットワークを用いた多様なアクセス手段の確保について、2010 年度までに調査研究及び実証実験を行う。

とされている。

本節では、電子行政サービス等に公的 IC カードを用いてアクセスする手段の多様化として、デジタルテレビを用いて利用者がアクセスする場合について、デジタルテレビの状況や利用者のアクセス環境について、現状を整理する。

2.1.1 デジタルテレビに関する検討背景

「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では、電子行政サービス等へのアクセス手段の多様化にむけて、

> パソコン以外の情報端末も電子行政サービス等の利用に活用できる可能性が高まることが期待される。情報端末としてはパソコンよりインターネット機能の付いたデジタルテレビや携帯電話の方が身近なものとして日常的に利用されている。

とされ、デジタルテレビを用いたサービスの利用について検討が行われている。

前述の調査報告以降、デジタルテレビ本体のハードウェア構成、ネットワークへ接続の仕様についても変化があり、デジタルテレビを用いた電子行政サービス等の利用を検討するにあたり、パソコンとデジタルテレビの機能的な差異について 表 2-1 のとおり整理した。

表 2-1 パソコンとデジタルテレビの機能比較

	パソコン	デジタルテレビ
利用形態	個人利用 画面とは近距離で利用	個人・共用利用 画面とは 2m、3m 離れて利用
性能（処理能力）	起動には時間がかかるが、処理能力そのものは高い	すぐに起動するが、処理能力そのものは、パソコンに比べると低い
画面	10 インチから 27 インチ	16 インチから 65 インチ
IC カードリーダライタの接続	USB もしくは PC カード方式でリーダライタを接続できる	一般的な接続方法は確立していない（1 社のみリーダライタを搭載したリモコンを発売している）
インターネット接続	Windows や Linux などの OS が基本機能として提供している	ネット対応機種では、Linux を採用する機種が増えており、インターネット接続が広く利用できるようになってきている
ソフトウェア更新・追加	ユーザがソフトウェアの更新・追加が容易にでき、新しい機能を追加できる	放送波やインターネットによってソフトウェアの更新は可能であるが、ユーザが新しい機能を追加できない
ブラウザ	ユーザが選択可能である	デジタルテレビに組み込まれており、変更はできない 機能限定されており、パソコン向けのサイトが表示できない場合がある
操作方法	キーボード、マウス、タッチパッド等多様な手段が有る	赤外線を使った専用リモコンが主流で、ブラウザ操作もリモコンで行う
利用者認証	ID、パスワードによるログイン機能がある	視聴年齢制限設定等で暗証番号設定はあるが、個人識別は行っていない

パソコンとデジタルテレビでは、このような機能差があるため、公的IC カードを利用したアクセス多様化に関してこれらの機能差についての検討が重要と考えられ、下記の項目について、現状のデジタルテレビおよび、関連仕様を調査し、現状を整理する。

- 外部インタフェース（IC カードリーダライタの接続）
- インターネット接続
- デジタルテレビに搭載されているブラウザ仕様
- リモコン
- 利用者認証
- 電子行政サービス等への外部接続

2.1.2 外部インタフェース（IC カードリーダライタの接続）

ここでは、市販されているデジタルテレビの外部インタフェース、及び、IC カードリーダライタについて調査する。

デジタルテレビの外部インタフェースとして求められる要件としては、IC カードリーダライタとの接続の観点から、

- 双方向のデータ通信用途で利用できること

また、普及促進の観点から、

- IC カードリーダライタ､デジタルテレビの双方で普及率が高いインタフェースであること
- 高機能・高価なインタフェースではなく、適切な機能で安価に実現できるインタフェースであること

が挙げられる。

上記の観点から、国内大手メーカ 6 社から販売されているデジタルテレビの外部インタフェースについて､2009 年 12 月時点の各社のカタログに掲載されている 153 機種について調査を行った。また、それぞれのインタフェースについて IC カードリーダライタでの採用状況についても併記している。

(1) USB

USB はホストの機器に周辺機器を接続するためのバス規格であり、現在のパソコン周辺機器において、最も普及率の高い双方向の汎用インタ

フェース規格である。デジタルテレビにおいては、国内の主要メーカ 6 社のうち、4 社から USB 端子搭載の機種が発売されており、搭載機種も増加している。基本的には HDD や USB メモリ、デジタルカメラ等との接続を想定して実装されている。

また、市販されている IC カードリーダライタの外部インタフェースとしては、USB が最も一般的なインタフェースである。

(2) IEEE1394

IEEE1394 は AV 機器やパソコンの周辺機器を接続するための高速シリアルバス規格であり、AV 機器では、i.Link の名称で搭載されている。最新のデジタルテレビの中では 3 社が採用しているが、搭載機種が減少傾向にあるのが現状である。規格上、双方向に様々なデータをやり取りすることができるが、AV 機器に搭載されているものは音声映像信号の入出力に用途が限定されており、データ通信単独での利用は見受けられない。

また、外部インタフェースとして IEEE1394 を搭載する IC カードリーダライタは現状見当たらない。

(3) HDMI

HDMI とは、著作権保護機能を持つ、主に AV 機器向けのデジタル映像・音声入出力インタフェースである。国内主要メーカのデジタルテレビについてみると、HDMI の搭載は非常に進んでおり、各社の最新機種では、ほとんどの機種に搭載されている。ただし、AV 伝送とその制御信号の伝送用途のみ利用されており、データ通信単独での利用は見られない。

今後、100Mbps 程度のデータ送受信がサポートされる 次世代の規格 HDMI1.4 に対応する機種が出てくる可能性があるが、対応機種は現状ない。

また、外部インタフェースとして HDMI を搭載する IC カードリーダライタは現状見当たらない。

(4) IrSS

IrSS とは、赤外線通信規格である IrSimple を簡略化した仕様の一つである。片方向通信を行うためのもので、双方向でのデータ通信はできない。IrSS 搭載機種はシャープから発売されており、携帯電話やデジタルカメラからの画像データ受信用途で利用されている。

また、外部インタフェースとして IrSS を搭載する IC カードリーダライタは現状見当たらない。

(5) SD カード

SD カードはメモリカードの一つである。4 社から SD カードのスロットを搭載した商品が発売されており、SD カード内データの再生、SD カードへの録画等の用途に利用されている。

また、SD カードと同じ端子･形状で、データ記録以外の拡張機能を追加することができる SDIO がある。これにより、双方向の無線通信などの機能追加が可能となるが、利用には専用のスロットが必要となる。ただし、デジタルテレビへの搭載製品は現状見受けられない。

また、外部インタフェースとして SDIO を搭載する IC カードリーダライタは現状見当たらない。

(6) Bluetooth

Bluetooth とは、デジタル機器の短距離無線通信技術の一つであり、数 m 程度の機器間での双方向通信に使われる。1 社がリモコンとのインタフェースとして搭載した商品を発売しているのみである。

外部インタフェースとして Bluetooth を搭載する IC カードリーダライタは現状見当たらない。

(7) RS-232C

RS-232C とはシリアル通信方式のなかで最も普及しているインタフェースで、多くのパソコンに標準で搭載されている。しかしながら、デジタルテレビにおける普及率は低く、一部のメーカの製品で、パソコンから制御する目的で利用されているのみである。

外部インタフェースとして RS-232C を搭載する IC カードリーダライタがあるが、該当機種は少ない。

(8) PC カード

PC カードは小型カード型インタフェースである。主にノートパソコン用に利用されており、デジタルテレビへの搭載は見受けられない。

外部インタフェースとして PC カードを搭載する IC カードリーダライタがあるが、該当機種は少ない。

以上の各インタフェースの現状と特性を 表 2-2 にまとめた。表中の普及率は機種数をベースとしており、デジタルテレビについては前述の 153 機種を、ICカードリーダライタについては、国内大手ICカードリーダライタメーカ 9 社から 2010 年 2 月時点で販売されている 17 機種を元に算出している。

表 2-2デジタルテレビ外部インタフェースのICカードリーダライタ接続可能性

	双方向性	普及率（デジタルテレビ）	普及率（ICカードリーダライタ）	接続可能性	
USB	○	○ 37.3%	◎ 88.2%	○	双方向性があり、デジタルテレビ、IC カードリーダの両方で普及している
IEEE1394	○	△ 5.9%	× 0.0%	×	双方向性があるが、デジタルテレビへの普及率は低く、ICカードリーダでの対応機種はない
HDMI	○	◎ 98.7%	× 0.0%	△	双方向性があり、デジタルテレビでは最も普及しているが、IC カードリーダでの対応機種はない
IrSS	×	○ 11.8%	× 0.0%	×	双方向性がなく、要件を満たさない
SD	×	○ 41.2%	× 0.0%	×	双方向性がなく、要件を満たさない
SDIO	○	× 0.0%	× 0.0%	×	双方向性があるが、デジタルテレビ、および、IC カードリーダで対応している機種がない
Bluetooth	○	× 0.0%	× 0.0%	×	双方向性があるが、デジタルテレビでの普及率は低く、ICカードリーダで対応しているものがない
RS-232C	○	○ 22.9%	△ 5.9%	△	双方向性があり、デジタルテレビ、IC カードリーダの両方で対応機種がある
PC カード	○	× 0.0%	△ 5.9%	×	双方向性があり、IC カードリーダでも対応するものがあるが、デジタルテレビで対応しているものがない

「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では、

> 現在の国内有力メーカのデジタルテレビについてみると、USB 端子はデジタルカメラや USB メモリ、HDD との接続を目的として実装されている機種がみられるものの、その実装率は現状ではそれほど高くない模様である。
>
> その他、デジタルテレビに実装されている接続端子としては i-Link も考えられるが、USB 端子より実装されている機種がやや多い程度である。イーサネットはほぼ全てのデジタルテレビに実装されているが、カードリーダーを単独で接続しての利用はできないことから、当面は利用できないものと考えられる。
>
> HDMI についてはデジタルテレビへの実装は進んでおり、複数の HDMI 端子を搭載している機種が一般的である。しかし、現状では画像・音声の伝送用に利用されており、データ通信単独での利用はないものと思われ、カードリーダーも接続はできないものと考えられる。ただし、HDMI は現在次世代の規格が検討されており、2009 年中には制定される模様で、その中ではイーサネット対応がされたり、想定する接続機器の拡充を図る方向にあるものと思われ、今後の動向は留意する必要がある。
>
> また、一部のメーカでは IrSS(高速赤外線通信の規格の 1 つ)をサポートしており、デジタルカメラからのワイヤレスデータ転送等の利用を想定している。いずれにしても、IC カードのリーダーに汎用的に接続できるような端子は現状では見受けられない。

とされていたが、

- USB-HDD 接続可能な機種が増えるなど、USB 搭載メーカが増加している。
- HDMI については、2009 年 5 月に、イーサネット対応の次世代の HDMI 規格である HDMI1.4 の仕様が発表されているが、現状、対応機種は見受けられない。

という変化がある。

2.1.3 インターネット接続

2009 年ではブロードバンド（特に FTTH）の普及や、デジタルテレビ普及機でのネット対応が進むなど、「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では、

> テレビでインターネット閲覧したり、サービスを利用できるようしたりする試みは 10 年以上前から行われてきたがなかなか普及が進まなかった。しかし、ここに来て FTTH を中心としたブロードバンド環境の普及やそれと相まってインターネット上のリッチコンテンツサイトの一般化が進んだことにより、テレビにおけるインターネット接続が実用的なものになりつつあり、利用者の多様なニーズに応えることで、今後、急速に普及していく可能性を秘めている。

とされていたものの実現化が進んでいる。

デジタルテレビからのインターネット接続の現状について、ネットワークインフラ、端末（ハードウェア）、及び、端末（ソフトウェア）の観点からまとめる。

(1) ネットワークインフラ

FTTH（光ファイバー）などの普及により、家庭でも高速なブロードバンド環境を利用することが一般的となってきている。「平成 20 年通信利用動向調査」（総務省）によると、平成 20 年現在では、インターネットの人口普及率が 75.3%、自宅のパソコンを使ってインターネットを利用する人の 86.9%がブロードバンド回線を利用しているなど、高い水準になっている。さらに、国内デジタルテレビメーカからインターネット接続が可能な機種が数多く発売されており、デジタルテレビからのインターネット利用者向けに、様々なポータルサービスも開始されている。

株式会社アクトビラの 2009 年 12 月 22 日のプレスリリースによると、「デジタルテレビ向けネット・サービス『アクトビラ』の累計接続台数が 2009 年 12 月 21 日に 150 万台に達した」としている。2008 年 12 月時点での累計接続台数が 70 万台であったことを考えると、デジタルテレビからのインターネット接続の増加がうかがえる。

(2) 端末（ハードウェア）

デジタルテレビにはデジタルテレビ専用の CPU が搭載されているのが一般的である。近年の高機能化に伴い、CPU の処理能力は向上しているが、パソコンと比べるとまだ低い。

一般的に、パソコン向けに作成されたリッチなコンテンツを視聴する

には相応の CPU のパワーが必要であるが、デジタルテレビは、リッチコンテンツの視聴に十分な処理能力を備えていない。

(3) 端末（ソフトウェア）

最近では、デジタルテレビへの Linux の採用が拡大しており、国内の主要メーカの多くが Linux を採用するようになっている。これにより、TCP/IP などのプロトコルスタックがデジタルテレビにも標準的に組み込まれ、インターネット接続のための基盤が整いつつある。

また、インターネット接続を利用するアプリケーションとしては、ブラウザ、電子メールソフト、Widget などが各社のデジタルテレビに実装されているが、パソコンでは広く普及している、ソフトウェアをダウンロードし、インストールする仕組みは、現状のデジタルテレビでは普及しておらず、アプリケーションの追加は制限されている。

2.1.4 デジタルテレビに搭載されているブラウザ仕様

デジタルテレビに搭載されているブラウザ仕様の現状について、ブラウザのインターネット接続仕様、及び、ブラウザで利用する入力機器の観点からまとめる。

(1) デジタルテレビに搭載されているブラウザのインターネット接続仕様

デジタルテレビに搭載されているブラウザには、インターネット接続を想定した HTML ブラウザ、デジタル放送に含まれるコンテンツの表示を主な目的とする BML ブラウザの 2 つが搭載されている。

国内大手メーカのデジタルテレビに搭載されているHTMLブラウザは、2003 年に設立されたデジタルテレビ情報化研究会[1]において策定、公開（http://nw-dtv.jp/ より入手可能）された、デジタルテレビのインターネット接続機能の共通仕様に準拠しており、共通化が図られてきている。具体的には、HTMLブラウザの共通仕様（デジタルテレビ ネットワ

[1] デジタルテレビ情報化研究会は、家電メーカ 5 社（シャープ株式会社、ソニー株式会社、株式会社東芝、株式会社日立製作所、松下電器産業株式会社（当時、現 パナソニック株式会社））の呼びかけにより、2003 年 4 月 14 日に設立され、現在の会員は 107 社となっている。本研究会は、デジタルテレビをインターネットからの情報収集にも使うことのできる「生活情報ツール」とするために必要な事項について論議し、通信サービスに対応した デジタルテレビが持つべき機能の、デファクト・スタンダードとなりうる技術仕様の策定と、デジタルテレビを活用したサービス全体の充実と普及に貢献する活動をしている。 現在国内で発売されているインターネット接続機能付きデジタルテレビのほとんどは、本研究会で策定された技術仕様に基づいて開発されている。

ーク機能仕様　ネットTVブラウザ仕様書）や、対応コンテンツの制作ガイドライン（デジタルテレビ ネットワーク機能仕様　コンテンツガイドライン、デジタルテレビ ネットワーク機能仕様　サービスガイドライン）などに準拠している。

また、デジタルテレビ情報化研究会では、HTML ブラウザを用いた IC カードへのアクセスに関する仕様（デジタルテレビ ネットワーク機能仕様　IC カードアクセス仕様書）を 2009 年 6 月に公開しており、この仕様に準拠している製品がソニーから発売されている。

この IC カードアクセス仕様では、図 2-2 に示す通り、カードにアクセスするためのカード種別によらない共通部分のみを規定しており、実際に IC カードにアクセスする場合には、カードの種別やサービスごとに、アクセスプラグインや応答フォーマットを規定する必要がある。上記のソニーのリモコンについては、Felica にのみ対応となっている。電子行政サービス等にアクセスするために使用する IC カードの種別や、サービスに応じて、ブラウザで使用するプラグインから IC カードへのコマンドやそれに対する応答のフォーマットについては別途策定する必要がある。

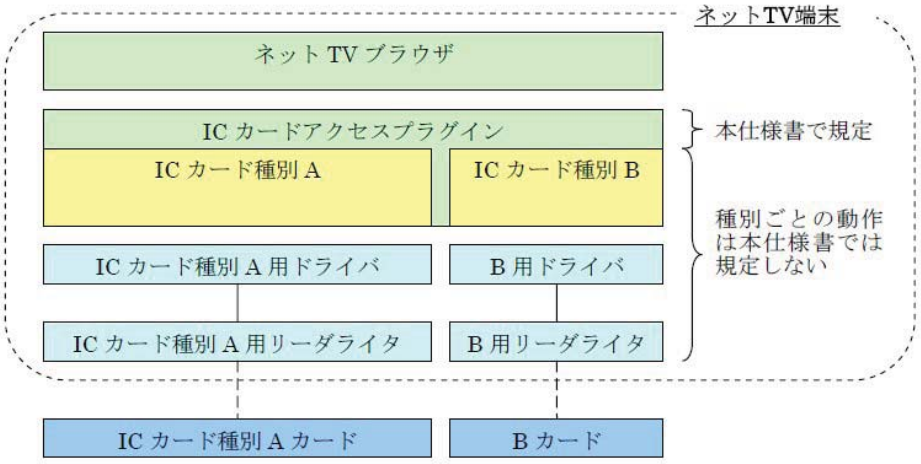


図 6-1　IC カードアクセス機能を実現するための構成要件

図 2-2 IC カードアクセスの構成要件　（デジタルテレビ　ネットワーク機能 IC カードアクセス仕様書　より）

BMLブラウザの仕様はARIB[1] で規定されているが、ARIB仕様（ ARIB仕様はhttp://www.arib.or.jp/　より入手可能）ではICカードへのアクセス規定は現状ない。

[1] ARIB　Association of Radio Industries and Businesses 社団法人 電波産業会

(2) デジタルテレビに搭載されているブラウザで使用する入力機器

デジタルテレビはリモコンでの操作を想定しているため、ブラウザの操作（HTML コンテンツの視聴）に関しても、現状ではリモコンにのみ対応しているのが一般的である。

コンテンツ上では、アンカー要素などへのフォーカス移動やページスクロール、ポインティングカーソルの移動などの操作を行う必要がある。デジタルテレビでは、リモコンの上下左右ボタンによって実現していることが多いが、リモコンでのポインティングカーソル移動は操作性が良くなく、任意の位置に移動させることは、マウスでの操作と比べて困難である。したがって、FLASH などのポインティングデバイスを必要とするコンテンツの視聴は、現状のデジタルテレビには向いていないと言える。

文字入力については、キーボードをサポートしているデジタルテレビは少なく、各メーカ独自のユーザインタフェースを用い文字入力画面を表示することで、リモコンでの文字入力を実現している。一般的なものとして、入力できる文字の一覧を画面上に表示し、所望の文字を選択させるソフトキーボード型や、数字ボタンを複数回押すことで所望の文字を入力する携帯電話型などがあるが、パソコンで用いられているキーボードと比べると、入力が煩雑である。

「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では、デジタルテレビで IC カードリーダライタに HTML ブラウザからアクセスする方法について、具体的に提示されていなかったが、2009 年 6 月に IC カードアクセス仕様がデジタルテレビ情報化研究会にて公開された。

2.1.5 リモコン

ここでは、デジタルテレビのリモコンの主流である赤外線（IR）方式と、最近製品化され始めた無線通信方式のリモコン（RF リモコン）の現状と特徴について述べる。

(1) 現在のリモコンについて

現在のデジタルテレビのリモコンで最も一般的なものが赤外線方式であり、1970 年代後半に登場してから現在に至るまで、ほとんどのテレビでこの方式がとられてきた。特徴としては、部材のコストが低く、簡素で開発が手軽であるという点が挙げられるが、無線方式のものと比べ、

データの通信速度が比較的遅いため、大量のデータ転送には向いていない。また、基本的には単方向の通信方式を採用しており、双方向でのデータの送受信はできない。

最近では、RF リモコンがデジタルテレビにも採用され始めている。無線通信方式としては Bluetooth など 2.4GHz 帯の無線方式を用いたものが一部メーカから発売されている。特徴としては、双方向性があることや、無指向性によりリモコンをテレビの受信部に向けなくても操作が可能であること、また、赤外線リモコンと比べて通信速度が早いことが挙げられる。しかしながら、赤外線方式と比べ、RF 方式では、送受信部の部材コストが高く、テレビ側に接続する受信部の電力によってテレビの待機時電力アップにつながるといった課題もある。

(2) IC カードリーダライタ搭載リモコンについて

2009 年 4 月には、FeliCa カードの開発・販売元であるソニーから、2.4GHz 帯の無線(IEEE 802.15.4)を使ったリモコンに FeliCa のリーダライタを内蔵した「お気楽リモコン」が商品化されている。当該製品は、先述のデジタルテレビ情報化研究会の IC カードアクセス仕様に沿った形で実装されているものの、FeliCa 依存部分については当該会社からのライセンスが必要なことや、リモコンのコストアップに対してニーズが低いため、他のメーカからは搭載商品は発売されていない。

2.1.6 利用者認証

デジタルテレビから電子行政サービス等に接続する際の利用者認証については、どの程度簡便に行えるかが利便性の面から重要である。「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」(平成 20 年度総務省委託事業) では「3.2.2 本人認証と利用者認証」にて、

> サーバ連携型 IC カードシステム(仮称)を活用する場合には、公的カード等内に格納される情報は、電子行政サービス等に共通の本人認証に活用される情報となり、各サービスの利用に必要な利用者認証に必要な情報は中央サーバに格納されることになる。

とサーバ連携型 IC カードを用いた認証の方式について検討されているが、ここでは、テレビを使用する際の利便性の観点から、現在利用されている認証方式について述べる。

デジタルテレビで実現可能な利用者認証方式には以下のような方式が

ある。

(1) IC カード内の利用者の基本情報を利用した認証方式

現状のデジタルテレビで使用されている IC カードである、B-CAS カードについて、「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では、「3.1.1 デジタルテレビの現状」で、

> デジタル放送受信機には固有の ID 番号をもった B-CAS カードが 1 枚付随しており、デジタル放送を視聴するためには B-CAS カードを受信機に挿入する必要がある。これは、デジタルコンテンツの流通における著作権保護等の観点から機器認証において B-CAS 方式が実用化され、事実上唯一の方式となっているためである。

と記載されている。

B-CAS カードの固有 ID 番号の読み出しに際しては、ピンコードなどによるセキュリティ設定が無いため、利用者認証ができる仕組みとはなっていない。

B-CAS カードの持つ固有の ID 番号と利用者を紐付けて利用者認証を行う方式では、カードがあればどのテレビ端末でも認証ができるが、比較的容易に取りはずしできることから、カードの盗難などにより、利用者以外の第三者が簡単に使用できてしまう危険性がある。

また、B-CAS カードの持つ固有の ID 番号は、放送に多重化された BML コンテンツのみで利用できる。放送に多重化された BML コンテンツから、インターネット上のコンテンツに遷移した状態では使用できなくなるという制限がある。また、HTML ブラウザからも利用できない。

(2) テレビ端末内の固有 ID を利用した認証方式

ひかり TV などの IPTV サービスでは、端末内に保存されている固有 ID(DRM-ID)によって認証を行う機器認証も利用されている。

この認証方式では、利用者は決まった端末からしかサービスを利用することができないといったデメリットがある一方、同一端末から利用する場合には利便性が良いといったメリットがある。

DRM-ID は IPTV サービスを提供している事業者の BML コンテンツでのみ使用できるように規定されており、当該事業者以外や、HTML ブラウザからも使用できないという制限がある。

(3) 利用者が設定する ID・パスワードを利用した認証方式

HTML ブラウザから一般的な Web サービスに接続した場合には、利用者がサービス事業者に対して ID やパスワードを事前に登録し、それをもって本人性を確認する方式が一般的であり、既に様々な Web サービスで利用されている。パソコン向けにサービスされている、東京電子自治体共同運営サービスでも、同様の方式が取られている。

ID・パスワードは基本的に利用者しか知り得ないため、上で述べた(1)、(2)と比べると、利用者の認証に向いている。また、ID・パスワードさえ覚えてしまえばどこでも使えるので汎用性が高い。

しかしながら、デジタルテレビのリモコンを用いて、ID やパスワードの文字入力を行うことは、パソコンのキーボードを用いた入力と比べると煩雑となる。

セキュリティの観点からみると、利用者が IC カードを紛失した場合や ID・パスワードが漏洩した場合においても、カード内に保存された利用者の情報、アクセス先の利用者の情報が第三者に漏洩しないようにすることが必要とされるが、一般的に、セキュリティをより強固なものにすると、利便性を損ねてしまうと言われている。たとえば、東京電子自治体共同運営サービスでは、利便性を損なわないように、サービスのセキュリティレベルに合わせ、ID とパスワードのみで受けられるサービス、電子署名が必要なサービスと、認証手段が使い分けされている。

また、サービスにおいて利用者の個人情報を扱う上では、利用目的の公表や、ユーザ登録時にユーザに対して通知が行われている。

2.1.7 電子行政サービス等への外部接続

デジタルテレビから電子行政サービス等への接続についての現状を以下に述べる。

パソコン向けサイトとしては、「電子政府の総合窓口 e-Gov (http://www.e-gov.go.jp) や、東京電子自治体共同運営サービス (http://www.e-tokyo.lg.jp) などのサイトが運営されている。

これらパソコン向けサイトを、デジタルテレビに搭載されている HTML ブラウザでアクセスすることは可能であるが、コンテンツがパソコン向けに作成されているため、サービス側のコンテンツ作成意図通りにデジタルテレビで表示できるとは限らない。

現状では、デジタルテレビ向けを前提とした、電子行政サービス等のポータルサイトは見受けられない。

また、国内大手デジタルテレビメーカ各社のポータルサイトには、電子行政サービス等へのリンクが張られていない。従って、上記のサイトにアクセスするためには､利用者がURLを入力して直接アクセスするか、もしくは、検索サイトで検索文字を入力し、検索結果からアクセスするより他に手段が無い。そのため、ユーザインタフェースがリモコンのみであるデジタルテレビで文字入力を行うこととなり、サイトへのアクセシビリティは低下する。

2.2 （アクセス手段の多様化）キオスク端末

自治体やその出張所等には、各種証明書の発行のための自動発行機が設置されている。さらに、コンビニエンスストア（以下、「コンビニ」と略す）にも様々なコンテンツにアクセスする情報端末が設置され、利用されるシーンが増えてきている（「2009 年版　セルフサービス情報端末（KIOSK）市場」、中日社、2009 年 1 月）。

このような中、電子行政サービス等の実現に向けて、「IT 政策ロードマップ」（IT 戦略本部、平成 20 年 6 月 11 日）には「先進的な地方公共団体におけるコンビニのキオスク端末による住民票の交付を 2009 年中に実現する」、「重点計画-2008」（IT 戦略本部、平成 20 年 8 月 20 日）には「利用者視点に立って利便性の向上及びオンライン利用のメリット拡大を進め、申請・届出等手続のオンライン利用の促進を図るため、2008 年度はインセンティブ付与のあり方、証明書等のペーパーレス化等について調査研究を実施するとともに、コンビニのキオスク端末を利用した証明書等の交付の実現に向けた検討を行う」と明記されている。

本節においては、電子行政サービス等への多様なアクセス手段の提供方法の１つとして、自治体などの公共施設、または、コンビニ等の民間施設に設置されたキオスク端末についてこれまでの取り組み状況を整理する。

2.2.1 キオスク端末に関する検討背景

主として住民の利便性向上を目的に、住民票や印鑑証明等の交付のための自動交付機の導入が進み、市役所等の出張所、駅前等に設置され利用されている。但し、自動発行機は各自治体のシステムの一部となっており、高価であるばかりでなく、他の自治体の証明書の発行はできない仕様となっていた。

これに対して、特定の自治体に限定せず証明書を交付する広域での証明書交付サービス（自動交付機の利用を含む）の検討が進むとともに、安価な自動発行機の導入、あるいは自治体が提供する施設予約等のサービスの申し込みや自治体のWebページを閲覧する機能を備えた自治体サービス向けキオスク端末が導入されるなどの動きもでてきている。また、コンビニに設置されたキオスク端末での先進自治体の住民票交付が 2010 年 2 月より実施された[1]。電子行政サービス等の中で市民から最も要望されていた証明書の交付が実現されただけでなく、将来は証明書の出力に限らず、今後導入が検討されるワンストップサービス等の行政情報サービスにも活用されることが期待されている（付録A参照）。

[1] 総務省報道資料（http://www.soumu.go.jp/menu_news/s-news/22772.html）

キオスク端末における証明書等の交付については、電子自治体の推進に関する懇談会の「オンライン利用促進ワーキンググループ報告書」（総務省「電子自治体の推進に関する懇談会」、平成 20 年 3 月）にも詳細に記述され、以下が課題として挙げられている。

コンビニの従業員等を介さない証明書等の交付の必要性

- 電子交付等に関する住民アンケート結果によると、多くの住民が従業員の人為的なミス（渡し間違い等）に不安を感じている。そのため、コンビニのキオスク端末で印刷された証明書等を住民が直接受け取ること等により、コンビニの従業員等を介さずに証明書等を交付することが重要である。

交付手続の標準化

- コンビニのキオスク端末を利用した証明書等の交付の普及のためには、交付手続の標準化が非常に重要である。各コンビニの交付手続の標準化によって、申請者は全国どこのコンビニでも同じように証明書等を受け取ることができる。また、各地方公共団体の交付手続の標準化によって、コンビニは全国の地方公共団体の証明書等の交付サービスを効率的に提供することができる。
- 標準化すべきものとしては、交付プロセス、本人確認のために利用するカード、キオスク端末の操作方法等が挙げられる。本人確認のために利用するカードの標準化に当たっては、全国共通の住民基本台帳カードを利用することが考えられる。交付手続の標準化が非常に重要である。

普通紙の利用の検討

- 現在、地方公共団体では住民票の写し等に改ざん防止用紙（専用紙）を利用している。しかし、コンビニのキオスク端末を利用した証明書等の交付については、全国のコンビニまで専用紙を運ぶ負担及びキオスク端末において専用紙を盗取されないよう管理する負担は極めて重い。このため、印刷時に普通紙に高度な偽造防止対策を施して利用することにより、専用紙の利用に代えることを検討すべきである。

共通基盤の整備

- 多くの地方公共団体がコンビニのキオスク端末を利用した証明書等の交付を導入する段階においては、各地方公共団体と各コンビニが個別にネットワーク等を整備することは現実的でない。セキュリティを確保しつつ効率的にネットワーク等を整備するため、将来的には LGWAN の活用等による共通基盤の整備について検討する必要がある。

アクセス多様化という視点でキオスク端末を検討した資料である「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度　総務省委託事業）でも課題が検討され、以下が課題として挙げられている。

- 表示されている情報の閲覧時のプライバシーの確保が必要となる
- 届出、申請の際に、端末を長時間に渡って占有するのは望ましくない
- 利用者にキオスク端末の使い方をサポートする必要がある場合がある

2.2.2 電子行政サービス等への接続の現状

現状の電子行政サービス等にアクセスするキオスク端末は以下の２種類に分類される。

- 自治体内あるいは関連施設に設置された自動交付機、及びキオスク端末
- コンビニに設置されたキオスク端末

前者の場合、図 2-3 に示すようにキオスク端末等は地域ポータル等の接続サーバを介して自治体の窓口システムに接続されるか自治体の窓口となるシステムに接続することによって、各自治体が提供するサービスを受けることとなる。

後者の場合には、図 2-4 に示すようにコンビニ事業者と電子行政サービス等の提供システムを専用線で接続して、キオスク端末から電子行政サービス等へ接続して各自治体のサービスを受けることとなる。

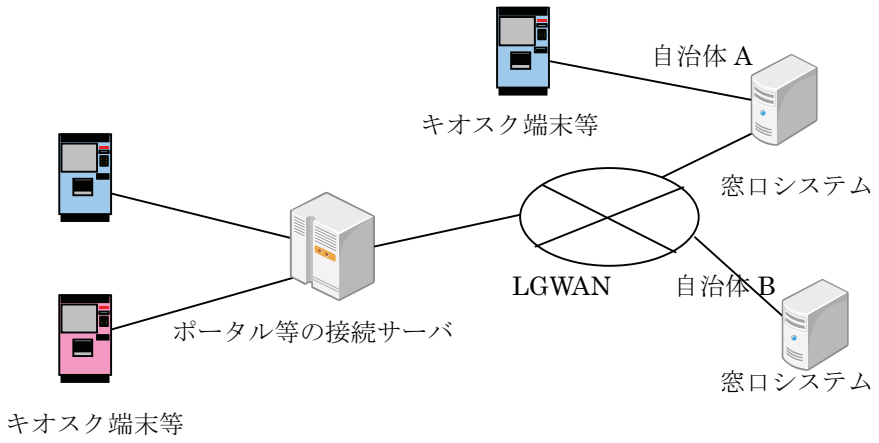


図 2-3 自治体が設置したキオスク端末等の接続

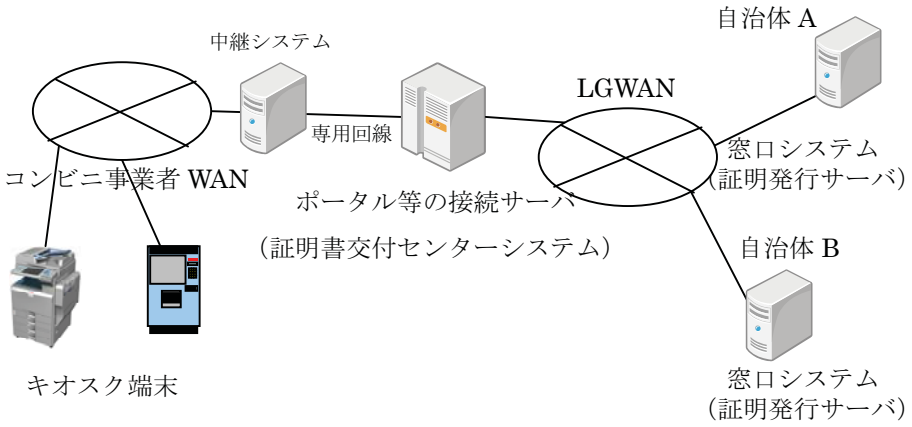


図 2-4 コンビニに設置されたキオスク端末等の接続

2.2.3 利用者認証に関する現状

電子行政サービス等の利用においては、以下の３つの利用シーンが想定される。

(1) 住民票の写しや印鑑証明書等利用者に関する各種証明書を交付する

(2) 電子行政サービス等が保有する利用者に関連する情報（たとえば年金情報）を取得し、表示する

(3) 各種申請を行う

いずれの場合も個人情報を含むため、適切な利用者認証を行う必要がある。現状のキオスク端末の多くは、図 2-5 のような構成をとっている。

（出展：http://www.family.co.jp）

図 2-5 キオスク端末（Fami ポート）の構成例

クレジットカード等に代表される磁気カードだけではなく、接点付きの IC カード、あるいは非接触の IC カードを読み取るカードリーダを持つ端末が導入されているコンビニも出てきており、将来的には磁気カードよりも安全性の高い IC カードを利用した認証を前提としても問題はないと考えられる。

現状の電子行政サービス等においては予め登録された識別番号と対応した暗証番号あるいはパスワード（暗証番号等）によって、利用者の識別・認証を行っている。各自治体が発行した磁気カードあるいは IC カード内に格納された個人識別番号とそれに対応した暗証番号等で利用者の識別・認証を行っている例もあれば、利用者が申請した識別名（例えばメールアドレス）と暗証番号等で行っている例もある。

2.2.4 キオスク端末の機能（入出力インタフェース）に関する現状

キオスク端末は、不特定多数が利用することが前提となる。特に情報機器に慣れていない高齢者等の利用を想定すると、キオスク端末の画面を操作することに戸惑う場面も想定される。また、キオスク端末の表示画面の大きさは限定され、入出力には制限がある。

(1) キオスク端末のユーザインタフェース

現状コンビニ等に設置されているキオスク端末の多くは、図 2-5 のような構成をとっているので、以下の通り入力に制限がある。

表示画面に関しては、普通のパソコンより小さめの 15 インチ程度の表示画面が主流であり、小さい場合には、800x600 程度の画素程度の表示能力を持つ。

入力に関しては、暗証番号を入れるテンキーを別にすると、入力するキーボードを持たない場合がほとんどであり、数字以外の文字を入力する場合には、タッチパネルの画面に表示したソフトキーボードを使用することとなる。文字の入力以外でも、パソコンのマウスのようなポインティングデバイスはないため、タッチスクリーンでの入力によってすべての操作を行う必要がある。

紙への出力に関しては、感熱紙によるレシートを出力するプリンタは装備しているが、普通紙へのプリンタを持たない端末が大部分であり、普通紙に印刷ができる端末は限定されている。

(2) 高齢者や障がい者等への配慮

高齢者や障がい者等も含めた場合には、たとえば「高齢者・障がい者等に配慮した電気通信アクセシビリティガイドライン 2 版」(情報通信アクセス協議会、平成 16 年 5 月)では以下のような要求が説明されている。

- 可能な限り高齢者・障害者が操作又は利用できるように配慮する
- 単独では電気通信アクセシビリティを確保できないときは，オプション製品や他社の製品，高齢者障害者支援技術と組み合わせて電気通信アクセシビリティを確保できるように配慮する

実際の要件としては、

① 視覚による情報入手が困難な状態であっても操作又は利用できる。

② 聴覚による情報入手が困難な状態であっても操作又は利用できる。

③ 発話が困難な状態であっても操作又は利用できる。

④ 力の強弱及びその制御能力にかかわらず操作又は利用できる。

⑤ 下肢が不自由な状態であっても操作又は利用できる。

⑥ 車いすを利用する状態であっても操作又は利用できる。

⑦ 任意の片手で操作又は利用できる。

⑧ 手，足，指又は義肢の限定された動きだけでも操作又は利用できる。

⑨ 触覚の感度が低下している状態であっても操作又は利用できる。

⑩ アレルギー性，及び毒性のある素材との接触を回避する。

⑪ 認知及び記憶への過度な負荷をかけないで，操作又は利用できる。

⑫ 文化の差異及び言語の違いがあっても，操作又は利用できる。

⑬ 初めて操作又は利用する人にとっても，操作又は利用できる

等が挙げられている。一部の端末で設置されたハンドセットによりオペレータへの質問ができるものや点字によるガイドが付けられた端末が出始めているが、個々の利用者の状況に合わせたアクセシビリティを提供する端末は存在しない。

(3) 証明書等の出力の現状

住民票など現在の証明書は、透かしや特殊な文様によって改ざんを防止する対策を施した専用紙に印刷される。専用紙は一般には入手不可能であるため、利用する紙によって証明書の真正性を担保している。しかし、自治体の管理が及ばないコンビニ等に設置された端末で使用する場合には、専用紙の利用は現実的でない。そのため、専用紙の代わりに印

刷技術によって証明書の真正性を担保する必要がある。また、証明書の場合、原本とコピーを識別することも重要となる。コピーした場合には、透かしとして入れた牽制画像が浮き出るなどの方法をとる必要がある。

住民票等の証明書の場合には、氏名に用いられる外字の問題も存在する。現状では登録されている外字のコードは自治体毎に異なっており、統一は実現していない。そのため、外字を使うことを前提とした住民票等の証明書の交付では、外字を印刷可能な状態として端末側に送る必要がある。

(4) 情報閲覧及び電子申請等の状況

パソコンを用いた情報閲覧やパソコン及び携帯電話を用いた電子申請が普及してきているが、キオスク端末を用いた情報閲覧や電子申請は限定的である。以下に代表的なパソコンでのサービスの現状を示す。

現状の電子行政サービス等で、個人の情報を入手・閲覧するサービスは少ない。一例としては、日本年金機構の年金個人情報提供サービスによって年金情報の一部の参照が実現されている。

電子申請等は、e-Taxをはじめ、各自治体などでも様々な施設予約等の申請が電子的に行えるようになってきている。インターネットを通しての申請例を 図 2-6 に示す。

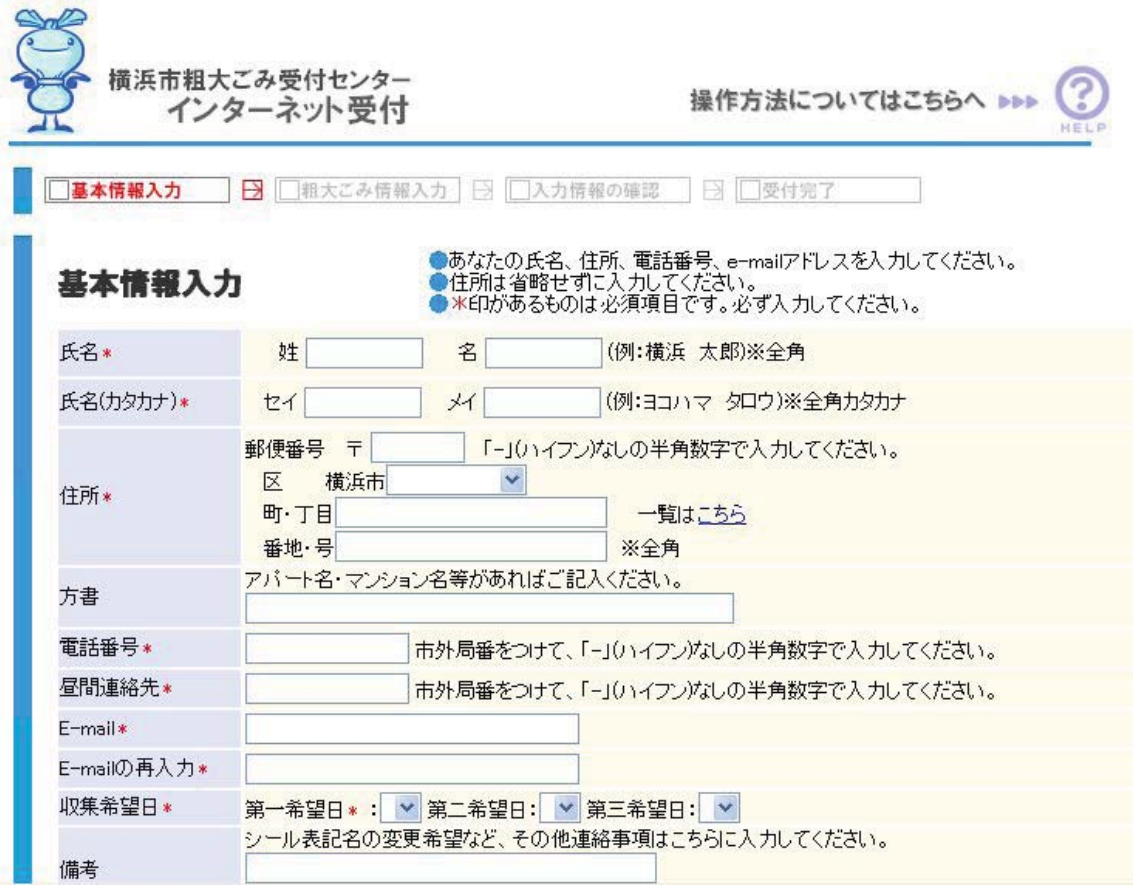


図 2-6 電子申請の一例（横浜市の粗大ごみ申請ページより）

現在の画面は、パソコン上でブラウザを利用して入力することを前提としている。多くの入力項目があるだけでなく、一度に表示できないため、スクロールしながら入力を行う必要がある等、キオスク端末での利用には適していない。

自動交付機を用いたサービスとして市川市が始めているのは、電子交付というサービスである。インターネットで申請した証明書が受け取り可能になるとパソコンあるいは携帯電話へメールによって通知され、最寄りの自動交付機で証明書を受け取ることができる。申請者自身の住民票や印鑑証明の交付は申請者の確認以外の審査が必要ないので即時交付が可能であり、多くの自治体で自動交付機で利用可能なサービスとして実施されてきた。その他何らかの審査が必要となる証明書の交付は実現されていなかったが、今回はそれを実現する新しい試みである。

2.3 中央サーバに認証機能を一部移行させる方式

平成 20 年 9 月 12 日 IT 戦略本部が決定した「オンライン利用拡大行動計画」では、行政手続におけるオンライン利用促進の重点的取組として「中央サーバに認証機能を一部移行させる方式」が掲げられている。

電子行政サービス等の実現に向けては、上記のみならず「重点計画－2008」（IT 戦略本部、平成 20 年 8 月 20 日）をはじめ、政府機関を中心に様々な角度から検討が行われており、平成 21 年 12 月に政府（総務省）が発表した「原口ビジョン」においても、「国民本位の電子行政を実現」することが施策例として掲げられている。この中で、平成 26 年までにすべての申請処理を電子化し、24 時間 365 日オンライン行政サービスを利用可能とすることなどが施策例として示されている。

本節では、「中央サーバに認証機能を一部移行させる方式」に関する、これまでの取り組み状況を整理する。なお、整理にあたっては、平成 20 年度に実施された「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）をはじめとする資料を参考とした。

2.3.1 「中央サーバに認証機能を一部移行させる方式」に関する検討背景

「IT 政策ロードマップ」（IT 戦略本部、平成 20 年 6 月 11 日）に示される「IT 基盤や利用環境の整備という点では大きな成果を挙げてきているが、IT が国民生活におけるサービス・付加価値の向上といった質的な面での成果につながっているか、さらにはその成果が国民に実感として伝わっているか、といった点においては、未だ改善の余地がある状況にある。」という現状認識に基づき、その具体的な改善策の一環として「オンライン利用拡大行動計画」（IT 戦略本部、平成 20 年 9 月 12 日）では、「中央サーバに認証機能を一部移行させることによって、個人がオンライン上で簡易にサービスを受けられる方策（カナダの e-Pass 類似の方式導入）の可否」等の検討に着手することが掲げられている。

利用者の認証については「次世代電子行政サービス（e ワンストップサービス）の実現に向けたグランドデザイン」（次世代電子行政サービス基盤等検討プロジェクトチーム、平成 20 年 6 月 4 日）および「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）の中で以下のような方向性および課題が示されている。

「次世代電子行政サービス（e ワンストップサービス）の実現に向けたグランドデザイン」より

> ポータルにアクセスすれば、複数機関の各サイトにアクセスしなくても、個々の機関の処理状況を確認できるようにし、１つの認証でワンストップサービスを提供できるようにする。また、そのための認証連携の仕組みを検討する。

「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）より

> 一般的な認証機能では、利用者とサービス提供者の間で 1 対 1 の直接認証が行われており、利用者がアクセス開始時にサービス提供者に直接送付した認証情報をもとに利用者の認証が行われ、サービスの利用が許可される。
>
> 関係する複数の手続きのワンストップ化・効率化を図るためには、サービス提供者が提供するサービスへのアクセス方法の連携を図り、利用者側の認証もシングル・サインオンを可能にするような仕組みが必要であるが、サービス提供者が独立に利用者と 1 対 1 の関係で直接認証を求める限り、ワンストップ化・効率化を図るのは難しいと考えられる。

一方、利用者が認証時に使用する認証デバイスについては昨今のセキュリティに対する関心の高まりから IC カードの利用が増加傾向にある。

IC カードを複数のサービスで利用するためには、多目的 IC カードとしてこれらサービスに応じた異なる認証鍵を格納する必要が生じるが、現状の課題として「様々なサービスへの対応を可能とするサーバ連携型 IC カードシステムの実現方式の検討」（コンピュータセキュリティシンポジウム 2009）では以下のような点が挙げられている。

(1) カードの記憶容量の制約により、利用できるサービスの数に制限が生じる。

(2) 電子私書箱が民間サービスを含め将来的にどのようなサービスに利用拡大されているかが明らかでなく、導入時点のカードの仕様によっては利用追加ができないサービスが生じる可能性がある。

(3) カード保有者がサービス追加を行う度に窓口まで赴き新たな認証鍵の書き込みを行う必要がある。

2.3.2 「中央サーバに認証機能を一部移行させる方式」の検討状況の整理

(1) 要求事項

前述の背景を踏まえ、「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では新たな概念として、“認証機能の一部をシステム側に集約することで、利用者側のサービスへのアクセスの利便性を向上させるとともに、複数のサービス毎の独立した認証を維持することにより、従来 IC カード内に搭載した多目的アプリの機能をシステム側で実現する”という考え方に基づき、“IC カードのサービスへの認証機能の一部を中央サーバに集約する”構想の概念が以下のように示されている。

利用者が電子行政サービス等にアクセスするための認証に必要な情報を中央サーバに移して、IC カードや端末など利用者側の仕組みをなるべく簡略化するとともに、中央サーバとサービス提供者間で利用者認証を代理で行うことが可能となる方式

(1) 電子行政サービス等の利用に必要な認証鍵等を中央サーバに格納

“電子行政サービス等の利用を希望する利用者を、サービス提供者側が認証するために使用する情報（以下「認証鍵等」という)”をサーバ連携型 IC カードシステム(仮称)においては、中央サーバに格納する。

(2) 電子行政サービス等の利用者認証に必要な利用者側のプログラム等を中央サーバに格納

電子行政サービス等の利用者認証に利用者側で必要となる認証鍵等以外のサービスへアクセスするための関連情報等をサーバ連携型 IC カードシステム(仮称)においては、可能な限り中央サーバに格納する。

(3) 電子行政サービス等の利用者が希望するサービスに関わる利用者認証の実行

中央サーバは利用者が希望したサービスに関わる利用者認証処理を利用者の代理で行い、認証処理の結果を利用者に通知する。

また、「サーバー連携型多目的 IC カードシステム －耐タンパー技術の重要性－（ディペンダブル VLSI ワークショップ 2008)」においても以下のように類似の概念が提示されている。

・サーバーにおかれる個人アカウントと連携する

・個人アカウントは、データ実体へのアクセスキーを管理

・アカウントに記録される情報（アクセスキーと一部のデータ実体）は必要に応じて暗号化し、アクセスカードでのみ復号化可能とする

・サーバーに置かれる個人アカウントとアクセスキーで、従来の多目的カードを実現

上記、「中央サーバに認証機能を一部移行させる方式」に関して「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では以下の要求事項が示されている。

- サービスの内容
- セキュリティ
- スケーラビリティ
- 利用者インタフェース
- 運用性・可用性
- サービス提供者インタフェース
- 認証の最適化

(2) 実現に向けた課題

前述の要求事項に続いて、同報告書では、「中央サーバに認証機能を一部移行させる方式」の実現に向けた課題として以下が示されている。

① 高いセキュリティレベルを確保する方法

高いセキュリティレベルを HSM (Hardware Security Module)で実現しようとした場合の課題として以下が挙げられている。

- 利用者認証鍵を保護しようとした場合のスケーラビリティの確保

② 可用性とリスクへの対応を可能にするバックアップの方法

運用時のバックアップ等に関する課題として以下が挙げられている。

- 耐タンパー性相当リソースのクラスタリング･レプリケーションやフェイルオーバー
- バックアップ処理の効率化

③ スケーラビリティを確保する方法

スケーラビリティについて､利用者の増加等により発生が予想される課題として以下が挙げられている。

- 中央サーバへのアクセス数の増大

- 管理を必要とする利用者認証鍵等の数の増大
- 全体構成や拠点についての議論
- 認証鍵等の移動

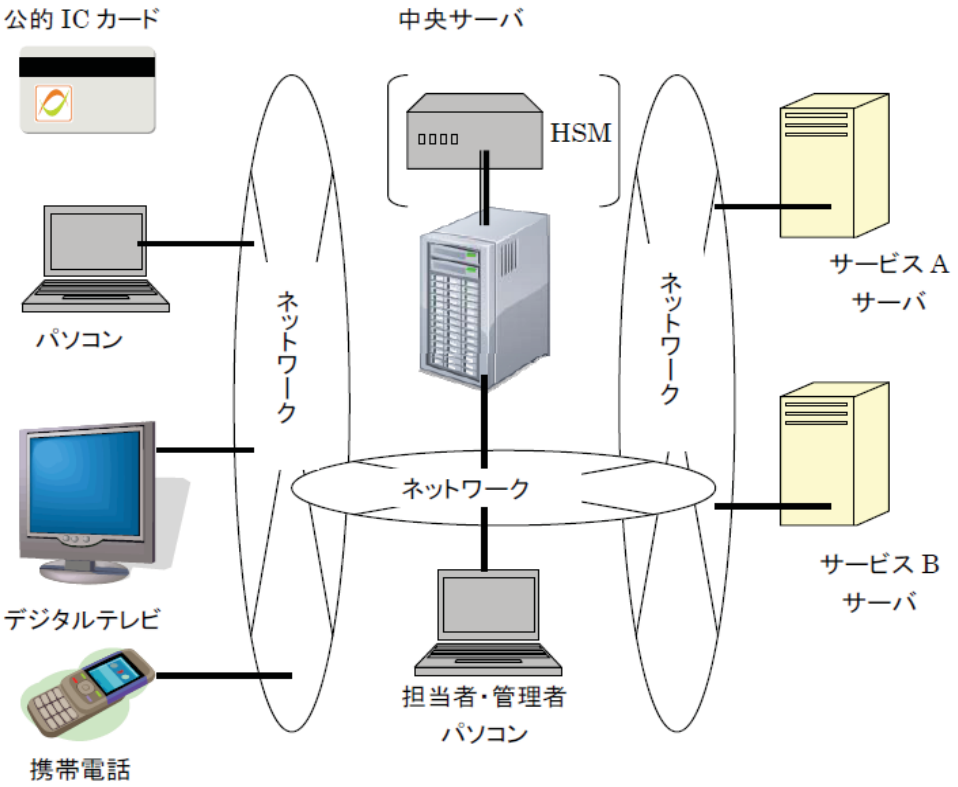
(3) 実証実験の実施内容・方法の検討

これまでの検討を踏まえ、同報告書では、「中央サーバに認証機能を一部移行させる方式」の実装に向けた機能の検討として「耐タンパー性相当を必要とする情報の取扱い（利用者認証鍵の管理方法)」および「基本機能」が示されるとともに、これらの検証を含めた以下の実証実験の方法が挙げられている。

① 実験室レベルでの基本機能検証

前述で検討された中央サーバの基本機能を利用者情報端末、管理者端末、サービス提供者サーバを接続した構成で機能検証を行う。

本検証における機器構成イメージを 図 2-7 に示す。



「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」
（平成 20 年度総務省委託事業）より

図 2-7 実験室レベルでの基本機能検証における機器構成イメージ

② モニタによる利便性等の検証

実験室レベルのシステムを数十から数百人規模のモニタが同時に利用する環境・構成へと拡張して、拡張した機能の動作と基本機能の利用における利便性等を検証する。

③ 一定規模のフィールドによる実用性の検証

最終段階として実用システムを構築して、数千人から数万人規模の利用者が確保できる地域での実用システムの試験運用を行う。

これらの検討状況を踏まえて、5 章にて本調査研究で取り組む課題を整理し、対策について検討を行うこととする。

3. （アクセス手段の多様化）デジタルテレビに関する調査研究

2章で述べた現状を踏まえ、デジタルテレビから電子行政サービス等へアクセスするための具体的な実現モデルを設定し、モデルの各構成要素に求められる機能を整理する。また、想定した実現モデルに対する課題への対策方法を調査するとともに、実証環境にて実現性の評価を行う。

3.1 課題の抽出及び対策の検討

本節では、デジタルテレビから電子行政サービス等へアクセスするための具体的な実現モデルを示すとともに、課題への対策方法を検討する。

3.1.1 実現方法のモデル化

「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では、実証実験の検討の中で、そのモデルが示されてはいるが、電子行政サービス等へのアクセスのための具体的なモデルについては考察されていない。本項では、デジタルテレビからの電子行政サービス等へのアクセスについて、実現に向けた具体的なモデル化を行う。

図 3-1 は、デジタルテレビ、及び、IC カードリーダライタを利用して、電子行政サービス等へアクセスするための実現モデルのイメージである。

実現モデルを想定するにあたり、利用者が、インターネット等に接続可能なデジタルテレビを通して電子行政サービス等にアクセスし、IC カード認証等の手段によって認証を受け、国や自治体が提供する電子行政サービス等、例えば、情報提供サービスや申請サービスなど、の一連の手続が完結できることを想定している。

さらに、本項で設定した実現モデルを構成する各要素（情報保有機関、電子行政サービス等、ネットワーク対応デジタルテレビ、IC カードリーダライタ、メーカポータルサービス、認証基盤、及び、その他インターネットサービス等）について、2.1 節で述べた現状を踏まえた上で、想定される機能、要件について述べる。

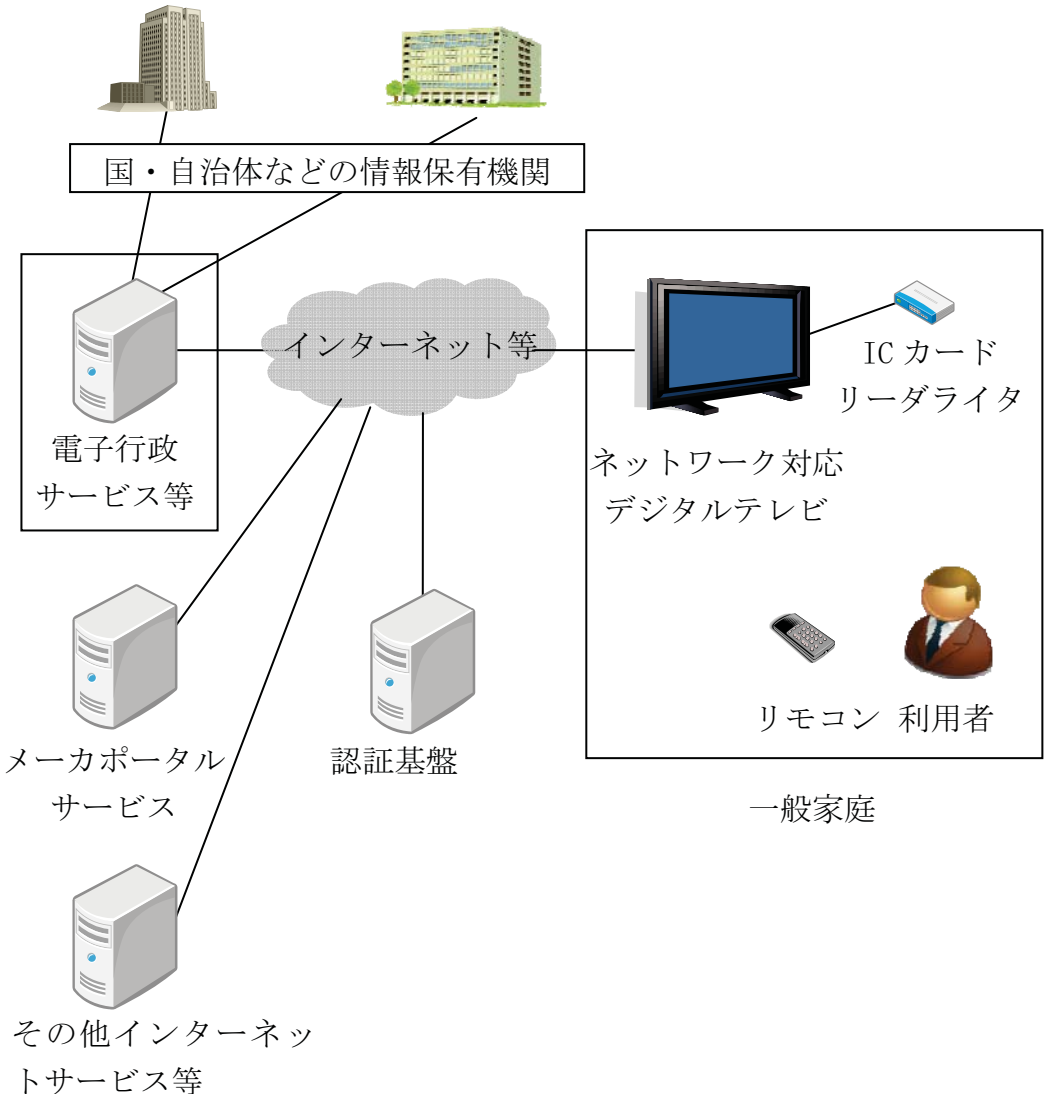


図 3-1 実現モデル

(1) 情報保有機関

利用者の情報を保有し、電子行政サービス等からの要求に応じて、電子的に蓄積された情報を利用者に提供する情報提供サービスや、利用者から国や自治体への申請を受け付ける申請サービス等を、電子行政サービス等を通じて利用者に提供する。

(2) 電子行政サービス等

情報保有機関と、利用者が操作するデジタルテレビ端末との間に位置し、インターネット等を通じて両者を接続する機能を有する。電子行政サービス等を提供するためのサーバもしくはサーバ群から構成され、ポ

ータルなどの機能を有する。

(3) 認証基盤

個人を識別、認証するための情報基盤。公的個人認証基盤のように、PKI にて個人を認証する個人認証基盤を想定する。

(4) インターネット等

デジタルテレビと電子行政サービス等を接続するネットワークで、一般的に利用されているインターネット等接続サービスの回線を想定する。一般家庭の場合には、FTTH もしくは ADSL によるブロードバンド回線で、24 時間接続可能な回線を想定する。

(5) ネットワーク対応デジタルテレビ

デジタル放送対応テレビのうち、インターネット等を通じて電子行政サービス等にアクセスすることが可能なテレビ。ブラウザが搭載され、電子行政サービス等から提供される情報を利用者に提示したり、自治体が行っている講演会等のサービスへの参加申し込み等が行える機能を有する。

(6) IC カードリーダライタ

デジタルテレビに接続可能、もしくは内蔵可能な IC カードリーダライタ。電子行政サービス等では、個人認証や、デジタル署名に対応していることが想定されるため、Type-B カードの読み書き機能を有する。また、申請手数料の納付までを完結させるためには、何らかの方法で決済機能を有することが望ましい。

(7) メーカポータルサービス

インターネット等接続機能を持つデジタルテレビを販売している各メーカが、自社のテレビ向けに提供している、テレビの特性を活かした専用のポータルサイトを有するサービス。

(8) その他インターネットサービス等

パソコンやネットワーク対応デジタルテレビからアクセス可能なインターネット等上のサービス。デジタルテレビメーカ 5 社が設立した、（株）アクトビラによる、「アクトビラ」のようなテレビ向けのサイトがここに含まれる。

3.1.2 システム機能に関する課題及び対策

2章での現状調査の結果、及び、3.1.1でモデル化を行った電子行政サービス等の実現モデルに基づいて、デジタルテレビから電子行政サービス等へアクセスするための実現方法を検討し、電子行政サービス等への接続に関する課題、デジタルテレビに関する課題の抽出と対策方法の検討を行う。

(1) 電子行政サービス等への接続

デジタルテレビがインターネット等回線を通じ電子行政サービス等へ接続されることからすると、2.1.3(1)で整理した通り、ネットワークインフラは整備されつつあると考えられる。むしろ、2.1.4で示したように、デジタルテレビに関しては、従来のインターネットブラウザと比べ制限された仕様となっている。このため、アクセス多様化の実現に当たっては、電子行政サービス等でもデジタルテレビを意識したサービスの提供が必要となる。

① デジタルテレビ向けコンテンツの提供

デジタルテレビ向けコンテンツとは、デジタルテレビのHTMLブラウザ上で視聴、実行が可能なコンテンツ(HTML文書やスクリプト等、インターネット等を通して提供される、映像、静止画、音声、文字などのデータ)であり、デジタルテレビ向けに最適化されたものを提供することが求められる。

現行のコンテンツは、パソコン向けに作成されており、デジタルテレビでは、意図通りに動作しないことがあげられる。この具体例としては、

- デジタルテレビでは、プラグイン機能で実現されているFlash Playerなどが搭載されていない機種が多数で、また、ダウンロードする機能も搭載されていないため、プラグイン機能によるレンダリング(情報の画像化)が行われず、意図通りの表示がされない。
- 大きなイメージデータが利用されている場合や、1ページの記載量が多い場合には、メモリ不足となりレンダリングできず、意図通りの表示がされない。
- スクリプト処理で検索などの複雑な処理を行うと、その処理に時間がかかり、応答が遅くなる。
- スクリプトによる動的なコンテンツ生成が行われていると、レンダリングが遅れたり、メモリ不足によりレンダリングできず、

意図通りの表示がされない。

- カスケードスタイルシート（CSS）で対応していないものがあると意図通りの配置ができない。

といった不具合が発生する可能性がある。

これらの解決には、サーバ側の負荷となってしまうが、デジタルテレビ情報化研究会仕様に準拠してコンテンツを作成することが、当面の解決方法である。また、できるだけスクリプト処理を減らし、検索処理やコンテンツ動的作成処理などの高負荷の処理を電子行政サービス等のサーバ上で行い、結果のみを表示するなど対策を行うことで、デジタルテレビにかかる負荷を抑制することが可能となる。

② コンテンツからの IC カードへのアクセス機能

電子行政サービス等で、IC カードの情報を利用するためには、電子行政サービス等が提供するコンテンツに、デジタルテレビの IC カードアクセスプラグインを呼び出す JavaScript が記載されていることが必要である。コンテンツに含まれるスクリプトと、デジタルテレビの IC カードアクセスプラグインとの間の制御データの送受信手段については、デジタルテレビ情報化研究会策定の、IC カードへのアクセスに関する仕様（デジタルテレビ ネットワーク機能仕様　IC カードアクセス仕様書）に準拠することが必要である。

加えて、2.1.4 で示したとおり、電子行政サービス等で使用するカードの種別やサービスの内容について技術検証や社会検証を行い、アクセスプラグインや応答フォーマットを策定する必要がある。

③ メーカポータル等からの接続性

パソコンに比べてデジタルテレビでは文字入力が煩雑であり、ユーザが都度、リモコンを使って電子行政サービス等のポータルサイトの URL を入力するのは手間がかかってしまうという課題がある。

デジタルテレビメーカでは、自社のテレビ向けにポータルサイトを運用していたり、アクトビラのようなデジタルテレビ向けのサイトも運用されている。これらのサイトは、ブラウザ起動時に表示されるなど、リモコンボタンの 1 回から数回の操作で接続できるようになっている。これらのサイトから電子行政サービス等のポータルへのリンクがあれば、接続性の向上に繋がる。

(2) ネットワーク対応デジタルテレビの機能

利用者がどのメーカのデジタルテレビを使用しても、同質の電子行政サービス等が受けられることが必要であり、これに求められる要件を以

下で述べる。

① インターネット等への接続機能

HTML ブラウザによるインターネット等への接続機能を有する。利用者が、どのデジタルテレビからでも同様に閲覧、操作できるよう、デジタルテレビ情報化研究会が策定するネットワーク機能仕様（デジタルテレビ ネットワーク機能仕様ネット TV ブラウザ仕様書）に準拠することが必要である。現在発売されているインターネット等への接続機能を持つデジタルテレビのほとんどは本仕様に対応している。

② IC カードへのアクセス機能

電子行政サービス等から取得したコンテンツの記載に従って、デジタルテレビに搭載されている HTML ブラウザが、デジタルテレビに接続・内蔵された IC カードリーダライタを介して、IC カード情報の読み書き、状態取得などの処理が適切に行うことができる機能を有する。コンテンツに含まれるスクリプトと、デジタルテレビの IC カードアクセスプラグイン間の制御データの送受信手段については、先述の IC カードアクセス仕様に準拠している必要がある。

また、デジタルテレビのSoC[1]やOSは、各社で異なったものが用いられており、電子行政サービス等に対応する部分のドライバについては、各社がそれぞれ組み込みを行う必要がある。

③ 文字入力機能

ID・パスワード、PIN コードなどの文字列を入力するための入力機能を備えていることが求められる。

また、パソコン向けに提供されている電子行政サービス等において申請等を行う際には、漢字入力を求められる場合もあり、仮名漢字変換に対応していることが求められる。

④ リモコンに求められる機能

リモコンに求められる機能は、IC カードリーダライタの接続形態によって異なる。リモコンに IC カードリーダライタを接続・内蔵する場合には、リモコン-テレビ本体間での双方向の通信が求められるため、この場合のリモコンの通信方式には、現行用いられている赤外線方式ではなく、無線方式であることが要求される。IC カードリーダライタがデジタルテレビ本体に接続・内蔵される場合は、リモ

[1] System on Chip: 1 つの半導体チップ上に必要とされる一連の機能を集積した半導体。ここでは、デジタルテレビに必要とされる CPU やデコーダ機能等を集積した半導体をいう。

コンには新たな機能は必要なく、現行の赤外線通信方式のリモコンが使用できる。

⑤ セキュリティ

利用者の個人情報の送受信が想定されるため、IC カードリーダライタとの接続経路上、及び、デジタルテレビ本体（もしくはリモコン内部）において、通信するデータが傍受されることが無いよう、セキュリティの確保が要求される。

(3) IC カードリーダライタ

現状のデジタルテレビには、デジタル放送のコンテンツ保護のためにIC チップを内蔵した B-CAS カードを用いている。しかしながら、このカードを抜くとデジタル放送が視聴できなくなることや、地上デジタル放送専用ではあるが、Plugin-SIM 形状の miniB-CAS カードに対応しているデジタルテレビには、IC カード対応だった従来の B-CAS カードリーダが無いため、IC カードを読み込むことが出来ない。このため、IC カードリーダ接続・搭載が、デジタルテレビのコストアップ要因となることが課題である。本システムを実現するためには必須の機能となるためメーカサイドでのコストダウン対策が求められる。具体的には、USB や RS-232C など、デジタルテレビが備えている一般的で安価なインタフェースを実装するといった対策が必要である。

3.1.3 セキュリティに関する課題及び対策

「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では、デジタルテレビによる電子行政サービス等の使用におけるセキュリティ上の課題として、IC カードリーダライタをリモコンに搭載する場合の通信のセキュリティレベルについて言及がある。

本項では、3.1.1 でモデル化を行った電子行政サービス等へのアクセスのための実現モデルを踏まえて、セキュリティ上の課題の抽出と対策方法の検討を行う。

デジタルテレビは、通常、家庭での使用が前提となっている。まず、一般家庭から電子行政サービス等へのアクセスについて、現在行われているパソコンからのアクセスと対比することで、課題と対策を検討する。

次に、デジタルテレビが公共の場所に設置された場合についての課題と対策について検討する。

(1) 一般家庭からデジタルテレビでアクセスする場合の課題と対策

一般家庭からデジタルテレビでアクセスする場合のモデルを図 3-2 に、同様に、パソコンからアクセスする場合のモデルを図 3-3 に示す。

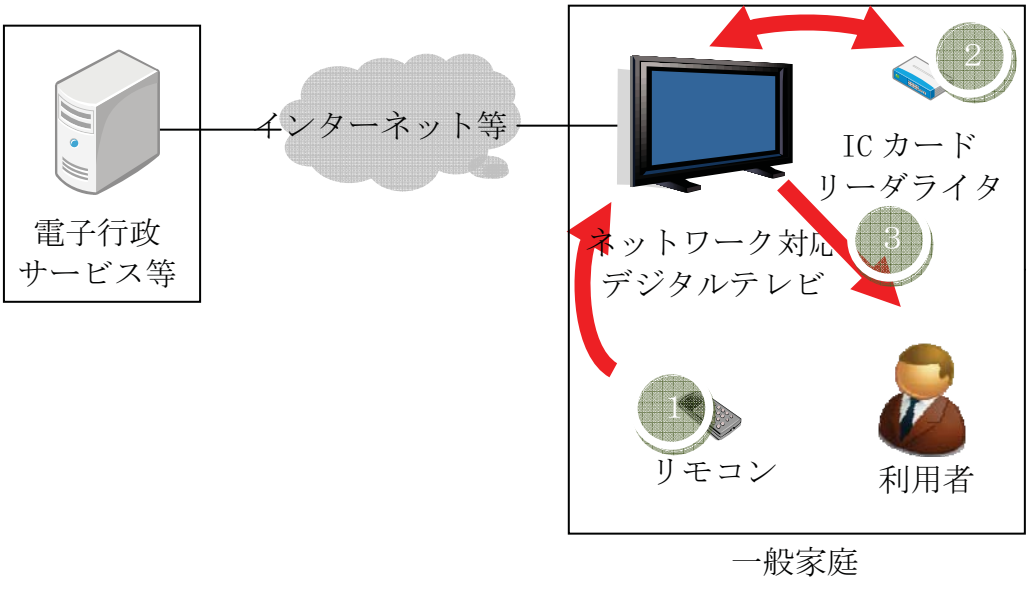


図 3-2　デジタルテレビに特徴的な構成要素

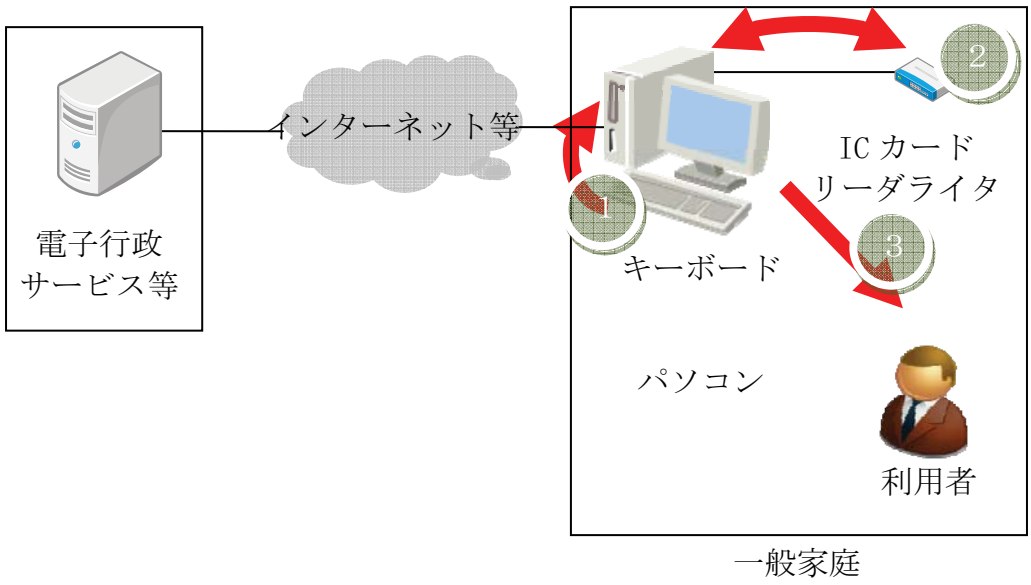


図 3-3 パソコン環境

① パソコンおよびデジタルテレビから電子行政サービス等にアクセスする場合に共通するセキュリティ上の脅威

現状のパソコン向けサービスでのセキュリティ上の脅威について示す。これらについては、デジタルテレビでも同様に発生すると考えられることから、新たな問題として今回の分析の対象とはしない。

- OS やブラウザの脆弱性。
- パソコンと電子行政サービス等との間で暗号化通信が行われている場合の通信路の盗聴。
- 機器に対する盗聴器等の設置。
- IC カードの盗難によるなりすまし。
- 画面に表示される内容の盗聴。
- 家族による、ID・パスワードを使ったなりすまし。

② パソコンとデジタルテレビの差異

図 3-2、図 3-3 の比較で分かるように、パソコンとデジタルテレビでは、入力装置（図 3-2①、図 3-3①）と IC カードリーダライタ（図 3-2②、図 3-3②）の接続方法に差異がある。IC カードリーダライタ

の接続方法については、有線接続のほか、リモコンに内蔵する方式や、独立して無線接続を行う方式が想定される。

デジタルテレビにおける装置間の脅威について表 3-1 にまとめる。

表 3-1 デジタルテレビにおける装置間の脅威分析

<table>
<tr><th></th><th>情報の流れ</th><th colspan="2">脅威分析</th></tr>
<tr><td rowspan="3">デジタルテレビへ</td><td>図 3-2①
リモコン
↓
デジタルテレビ</td><td>赤外線接続については対象外。</td><td rowspan="3">無線接続の場合は屋外から盗聴可能であり、暗号化が必要。</td></tr>
<tr><td>図 3-2②
IC カードリーダライタ
↓
デジタルテレビ</td><td rowspan="2">有線接続の場合はパソコンと同様で問題なし。</td></tr>
<tr><td rowspan="2">デジタルテレビから</td><td>図 3-2②
デジタルテレビ
↓
IC カードリーダライタ</td></tr>
<tr><td>図 3-2③
デジタルテレビ
↓
利用者への情報表示</td><td colspan="2">PIN 等の盗み見が想定されるが、家庭内では対象外とする。</td></tr>
</table>

表 3-1 に示す通り、パソコンと比較した場合に、デジタルテレビでは、リモコン、IC カードリーダライタの接続形態によって、セキュリティ上の脅威が異なることが分かる。

また、デジタルテレビと IC カードリーダライタ間が無線接続されている場合には脅威が存在するが、情報により脅威が異なることが考えられるため、情報別の脅威分析を行った。(表 3-2、表 3-3)

なお、脅威が存在する通信路を通る情報についてのみ分析を行った。

表 3-2 電子行政サービス等と IC カードリーダライタ間で授受する情報

情報	脅威分析
電子証明書 申請書類にデジタル署名を行った際、本人であることを証明するために IC カードリーダライタにより IC カードから読み出し、デジタルテレビのブラウザを通じて電子行政サービス等へ送付する。	なりすまし・盗聴の場合、基本的に公開するもの（公開鍵証明書）であり、問題ない。 改ざんの場合、証明書として成り立たない。
申請書類 （Digest、デジタル署名等を含む） 各種申請を行う際、記入の上、必要に応じて電子署名を行い提出する。 申請書類の Digest はブラウザから IC カードリーダライタを通して IC カードに送られ、IC カード内でデジタル署名され返される。	なりすまし・盗聴の場合、不正使用される可能性がある。 改ざんの場合、正規の利用者が正常にサービスを利用できない可能性がある。

表 3-3 IC カードのコントロールやアクセスするための情報

情報	脅威分析
PIN 電子証明書等を読み出す際、所有者認証のため入力装置（リモコン等）から、デジタルテレビ、IC カードリーダライタを通じて IC カードに入力する。	なりすまし・盗聴の場合、不正使用される可能性がある。 改ざんの場合、正規の利用者が正常に IC カードにアクセスできない。
コマンド IC カードの読み書きや電子署名などを実行する為の命令。 デジタルテレビと IC カードリーダライタ間で送受する。	なりすまし・盗聴の場合、不正使用される可能性がある。 改ざんの場合、正規の利用者が正常に IC カードにアクセスできない。

表 3-2、表 3-3 に示す通り、情報による脅威の差異はないことが分かる。

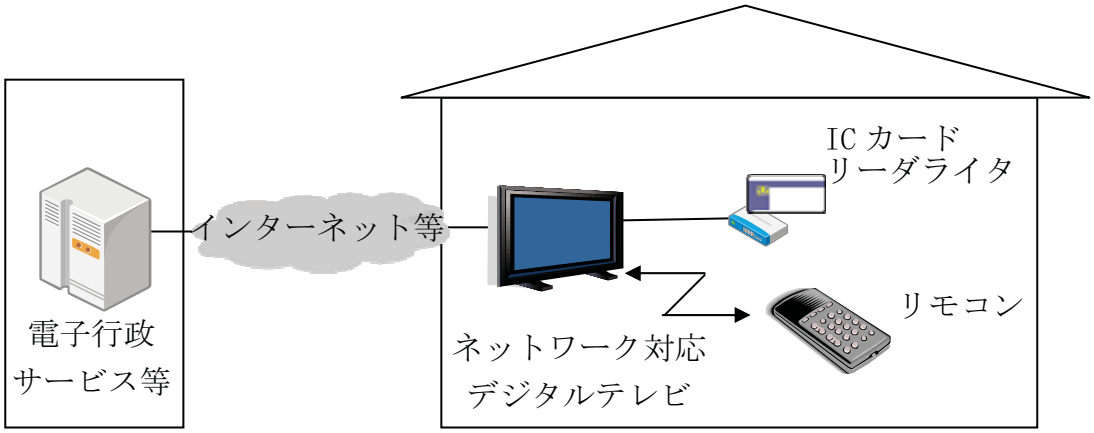
③ デジタルテレビとリモコン、およびデジタルテレビと IC カードリーダライタの接続形態（図 3-2①、②）

表 3-1 で、デジタルテレビとリモコンの接続形態として、赤外線接続と無線接続があることを示した。このうち赤外線接続の場合は、見通し環境での利用に制限されるため、セキュリティ上は問題とならない。

以下に、リモコンおよび IC カードリーダライタの接続に想定される 3 つの方式を示す。

i）リモコンは赤外線で、IC カードリーダライタは有線で接続される場合

この場合は、パソコンと同等の接続であり、セキュアな通信路が確立されている電子行政サービス等へのアクセス方式として、早期に実現可能なモデルである。

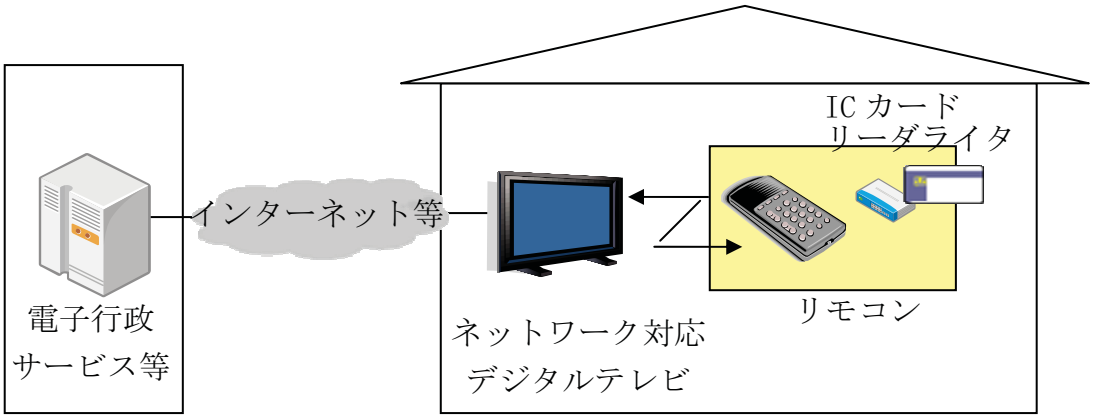


（注）折れ線の矢印で示した箇所は無線、実線は有線であることを示す。

図 3-4 リモコンは赤外線で、IC カードリーダライタは有線で接続される場合

ii）リモコンと IC カードリーダライタが一体の場合

この場合は、リモコンと IC カードリーダライタがともにデジタルテレビと無線で接続されおり、 通信経路を暗号化するほかに、デジタルテレビとの紐付け（ペアリング）をどのようにして行うかという課題がある。

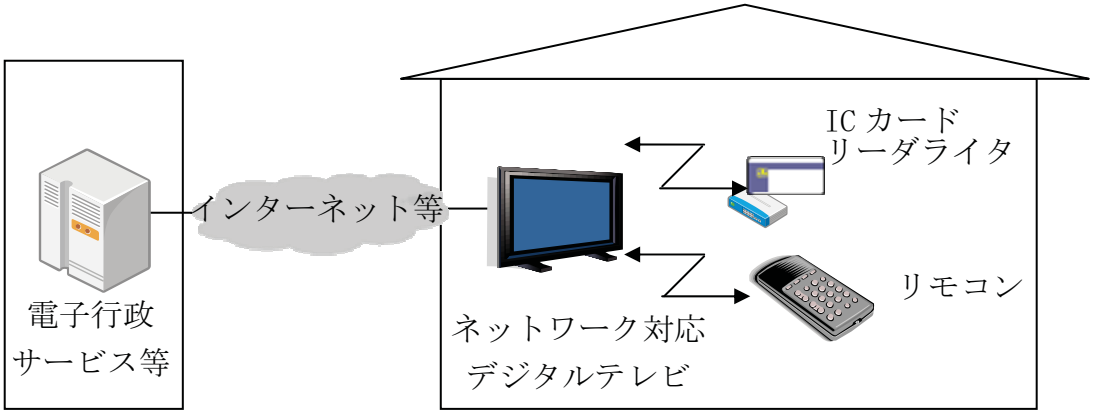


（注）折れ線の矢印で示した箇所は無線、実線は有線であることを示す。

図 3-5　リモコンと IC カードリーダライタが一体の場合

iii）リモコンおよび IC カードリーダライタが無線でそれぞれ接続される場合

この場合は、通信経路を暗号化するほかに、デジタルテレビとの紐付け（ペアリング）をどのようにして行うかという課題がある。



（注）折れ線の矢印で示した箇所は無線、実線は有線であることを示す。

図 3-6　リモコンおよび IC カードリーダライタが無線でそれぞれ接続される場合

④ リモコンおよびICカードリーダライタの無線通信方式の検討

上記の接続形態を踏まえて、デジタルテレビとリモコンおよびICカードリーダライタの通信方式について、広く普及している無線通信で候補となる3つの方式についてセキュリティの観点から比較する。(表3-4)

表3-4 無線通信方式のセキュリティ面の比較

名称	無線LAN	Bluetooth	ZigBee
規格	IEEE 802.11	IEEE 802.15.1	IEEE 802.15.4
暗号アルゴリズム	ストリーム暗号 RC4(WPAではAES)	ストリーム暗号 E0	ブロック暗号 AES
鍵長	128～256ビット	8～128ビット	128ビット
電子政府推奨暗号[1]	○	×	○
用途	LAN向け	モバイル機器向け	家電向け 業界標準で検討中

まず、十分なセキュリティが確保できるという観点では、電子政府推奨暗号に対応していることが必要である。また、ZigBeeについては、家電向け無線通信の業界標準として検討されていること、他の方式に比較して、消費電力が小さく、リモコンへの内蔵に適することから、リモコンおよびICカードリーダライタに適用する無線通信方式として、有力な候補と考えられる。

⑤ 一般家庭からのアクセスについてのまとめ

以上のように、現在行われているパソコンからの電子行政サービス等へのアクセスと比較すると、デジタルテレビとICカードリーダライタ間・デジタルテレビとリモコン間が無線接続になった場合の暗号化が担保できれば、同様のセキュリティが確保できるといえる。

[1]総務省及び経済産業省が共同で開催する暗号技術検討会等において、暗号を公募の上、客観的に評価し、平成15年2月20日に、「電子政府」における調達のための 推奨すべき暗号（電子政府推奨暗号）のリストを決定し、公表した。
電子政府システム一般における暗号技術要件は、共通鍵128ビットブロック暗号、共通鍵64ビットブロック暗号、共通鍵ストリーム暗号のいずれかで、鍵長は128ビット以上である。

(2) 公共の場に設置したデジタルテレビからのアクセスする場合のセキュリティ

公民館や病院、その他公共の場に設置されているデジタルテレビから電子行政サービス等へアクセスする場合のセキュリティについて検討する。

公共の場という特性から、一般家庭からのアクセスと比べ、セキュリティ上の対策がより必要となる。具体的には、複数人での機器の使用、機器の入れ替えなどや盗聴器の設置の可能性、盗み見による情報の漏洩やなりすましなどがあげられる。

① 複数人での利用を想定したセキュリティ上の対策

複数人での利用を想定した場合には、使用した人の履歴が全く残らないように配慮しなければならない。具体的には

- サービスではCookieを使用しない
- ブラウザの閲覧履歴を残さない
- 手続の途中で応答が無くなった場合に、初期に戻ること

という対応が必要となる

② 盗聴器等の取り付けに対する対策

公共に場に設置する場合には、IC カードリーダライタ、デジタルテレビ本体やリモコンに盗聴機能が仕掛けられる可能性がある。このため、ICカードリーダライタについては、デジタルテレビ本体に内蔵されることが望ましい。

デジタルテレビやリモコンについては、取り外して改造等が出来ないように固定したり、裏蓋が開けられたなど、改造されたことが分かるようにしたりするなどの対策が必要となる。

③ 盗み見に対する対策

公共の場に設置する以上、個人の情報を第3者に盗み見されることを完全に回避することは不可能であるが、パーティションを設置して見られにくくする、ミラーを設置して盗み見されているかどうかの確認ができるようにすることが最低限必要である。

IC カードの PIN 入力や、パスワード入力に関しては、画面上にそれが表示されないように配慮しなければならない。

このように、公共の場に設置されたデジタルテレビから電子行政サービス等にアクセスする場合には、市販のテレビに加えてセキュリティ対策が必要となる。

3.1.4 ユーザビリティに関する課題及び対策

3.1.2 で述べたように、デジタルテレビでは入力手段が限定されていることや、使用されているブラウザがパソコンでのブラウザの仕様とは異なることなどの制約事項がある。本項では、ユーザビリティの観点から課題の抽出と対策方法の検討を行う。

(1) デジタルテレビの使用環境とブラウザ仕様について

現行のデジタルテレビでは、数字キー、カーソルキー、テレビとしての機能キーで構成されるリモコンが入力デバイスとなっており、パソコンのようにキーボードやマウスによる入力が行えない。このため、ユーザビリティを向上させるためには、「デジタルテレビ情報化研究会　デジタルテレビネットワーク機能仕様 コンテンツガイドライン」に準拠したコンテンツ作成が望ましい。この仕様では、ユーザビリティに関して、下記が規定されている。

- 2、3 メートル離れて操作していることを考慮すること。
- 文字サイズは 16 ポイント以上を推奨する。
- アンカーは縦 1 列に並べる等、カーソルキーで選択しやすくする。
- スクロールに関して、横スクロールするコンテンツは望ましくない。縦スクロールする場合は、ページ内の上端や下端などに、そのページ内の区切り位置にジャンプするリンクを設けることを推奨する。
- イメージマップを使用する場合は、カーソルキーによるフォーカス移動で到達できない領域が出ないよう、複雑な配置は行わない。
- フレームは、フレーム間の移動が発生するため仕様外とする。
- 文字入力補助　カスケードスタイルシート (CSS) の拡張として、character-type を追加し、INPUT 要素に対して文字の種別を指定することが望ましい。

また、電子行政サービス等では、申請、閲覧等において、ID やユーザ名、住所などの情報の入力が求められる。リモコンを使って文字を入

力することは煩雑であるため、IC カードリーダライタが接続されている場合には、IC カードから読み込む、または、サーバからダウンロードするようなコンテンツとすることで、ユーザビリティが向上できる。

(2) デジタルテレビの入力手段

デジタルテレビでは、入力手段がリモコンに限定されているなどの制約がある、その制限下でもストレス無くサービスを利用できる機能を持つ必要がある。

① 入力手段の制限

入力手段がリモコンに限定されているため、特に、文字入力が煩雑となったり、ポインティングデバイスが無いために位置指定が不可能であったりすることがある。この直接的な解決は、キーボードやマウスをデジタルテレビに接続できるようにすることであるが、コストの面から採用されていないのが現状である。2009 年 12 月に東芝から発売された CELL レグザ（55X1）では、パソコンのブラウザと同等の機能のブラウザを搭載しており、ポインタ操作可能なタッチパッドがリモコンに搭載されている。また、デジタルテレビでの USB の採用が広まると、パソコン用の USB キーボードや USB マウスが使用できるようになる可能性もある。

文字入力の煩雑さにより、

- 電子行政サービス等へのアクセシビリティが悪いこと。
- 申請等での文字入力に手間がかかる。

の 2 つが課題となる。

前者の解決方法としては、

- デジタルテレビ向けポータルサイトにリンクを置く。デジタルテレビメーカでは、少ない操作で自社のポータルサイトに遷移できるようになっており、メーカポータルサイトに電子行政サービス等へのリンクがあれば、容易にアクセス可能になる。
- デジタルテレビの初期設定のブックマークに電子行政サービス等へのリンクを組み込んでおく。
- 携帯電話等のメール機能などとデジタルテレビと連携する機能によって、電子行政サービス等へアクセスする。シャープのデジタルテレビでは、IrSS を用いて携帯電話からメールに添付されている URL 情報を含む JPEG 画像を受け取り、その URL にジャンプする機能がある。（フォトリモ機能）。

・ デジタル放送の放送波に含まれるBMLコンテンツに、電子行政サービス等のURLを多重化し、ユーザ操作によって、HTMLブラウザを起動する。

が考えられる。

後者の解決方法としては、

・ リモコンやデジタルテレビ本体に使用頻度の高い文字列を登録し、リモコン操作で入力できるようにする。

・ 電子行政サービス等のコンテンツで、一度入力した情報を、Cookieとして、デジタルテレビに保存し、再利用する。

・ 電子行政サービス等で用いるICカードにID・パスワード、名前住所などを記録してコンテンツからその情報を取り込む。

・ 電子行政サービス等のサーバから、名前、住所等の情報をダウンロードして取り込む。

などがある。一般家庭でデジタルテレビが共用されていることから、IDやパスワードをCookieとして保存し、自動ログインを行うことや、ユーザを特定せずにCookieを使用することは、セキュリティ上、望ましくない。

② ICカードリーダライタの操作性

ICカードリーダライタを用いる場合、ICカードリーダライタをどこに取り付けるかという課題がある。コストダウンやセキュリティの面から、ICカードリーダライタはデジタルテレビに内蔵することが望ましいと考えられる。

しかしながら、大画面テレビでの利用では、利用者がテレビ本体と離れた場所から操作することが想定され、ICカードリーダライタが本体に内蔵もしくは、本体近くに有線接続されていると、ICカードを挿入したり、所定の位置にかざす操作の際に手間がかかる可能性があり、ユーザビリティが低下する。大型テレビでは、リモコンへICカードリーダライタを接続・内蔵することでユーザビリティの向上を図れるが、デジタルテレビ本体との通信においては、暗号化された通信方法とすることが必要となる。セキュリティに関しては、3.1.3で詳しく検討している。

デジタルテレビ本体や、リモコンにICカードリーダライタを搭載する場合に、読み書きを確実に行えるようにするという課題がある。特に、リモコンで操作しながら、ICカードの読み書き動作を行うこととなり、読み書き中に位置がずれたりしないように、リーダライ

タの位置を分かりやすく示したり、ガイドを設けたり、非接触であっても挿入型とするなど形状を考慮することが必要となる。

3.2 実機検証

具体化したモデルの実現性を検討するに当たり、電子行政サービス等とデジタルテレビとの接続性や操作性など、特にユーザビリティについての検証が重要となる。そのため、ユーザビリティに関して、(1) IC カードリーダライタ接続、(2) リモコンでの操作性、(3) 電子行政サービス等のポータルへのアクセシビリティ、(4) 電子行政サービス等のポータルサイトにおけるユーザビリティの 4 点について、実際の検証環境にて検証を行う。本節では、それぞれの検証環境について説明し、続いて検証項目と検証内容、検証結果について述べる。

今回の検証を行うために、電子行政サービス等の例を想定する必要があった。できるだけ実例に即したものとするために、総合行政ネットワーク運営協議会が発表している、認定済行政サービスリストの中で、複数の市町村区にまたがって実際にサービスされており、パソコンからのアクセスが可能であった、東京電子自治体共同運営サービスを参考としている。

3.2.1 検証環境

検証のために準備した環境を以下に示す。本検証で用いた機材を表 3-5 でまとめ、検証環境を図 3-7 に示す。

表 3-5 検証構成

構成要素	説明	備考
デジタルテレビ	市販のデジタルテレビ	シャープ LC-40LX1 検証項目 3-1、3-2、3-3、4-1 で使用
	IC カードリーダライタ接続対応試作品	シャープ LC-40LX1 をベースとした IC カードリーダライタ対応の試作品 検証項目 1-1、1-2、2-1、2-2、2-3、2-4 で使用
リモコン	デジタルテレビの付属品	
サーバ 1	ローカルネットワーク上のローカルサーバ Microsoft Windows XP CPU : Pentium(R) 4 CPU 3.60GHz RAM : 2.00GB HDD : 300GB	電子行政サービス等を想定
コンテンツ 1	IC カードリーダライタ接続を想定したテスト用コンテンツ	電子行政サービス等のコンテンツを想定
サーバ 2	インターネット等上のメーカポータルサイト	シャープのメーカポータルサイトのテストサーバ
コンテンツ 2	サーバ 1 に設置するコンテンツ	コンテンツ 3 へのリンクを設置
サーバ 3	PC 向け電子行政サービス等のサーバ	http://www.e-tokyo.lg.jp
コンテンツ 3	PC 向け電子行政サービス等に含まれるコンテンツ	
IC カード	Type-B 準拠の試作品	
IC カードリーダライタ	USB 接続、Type-B 対応の試作品	

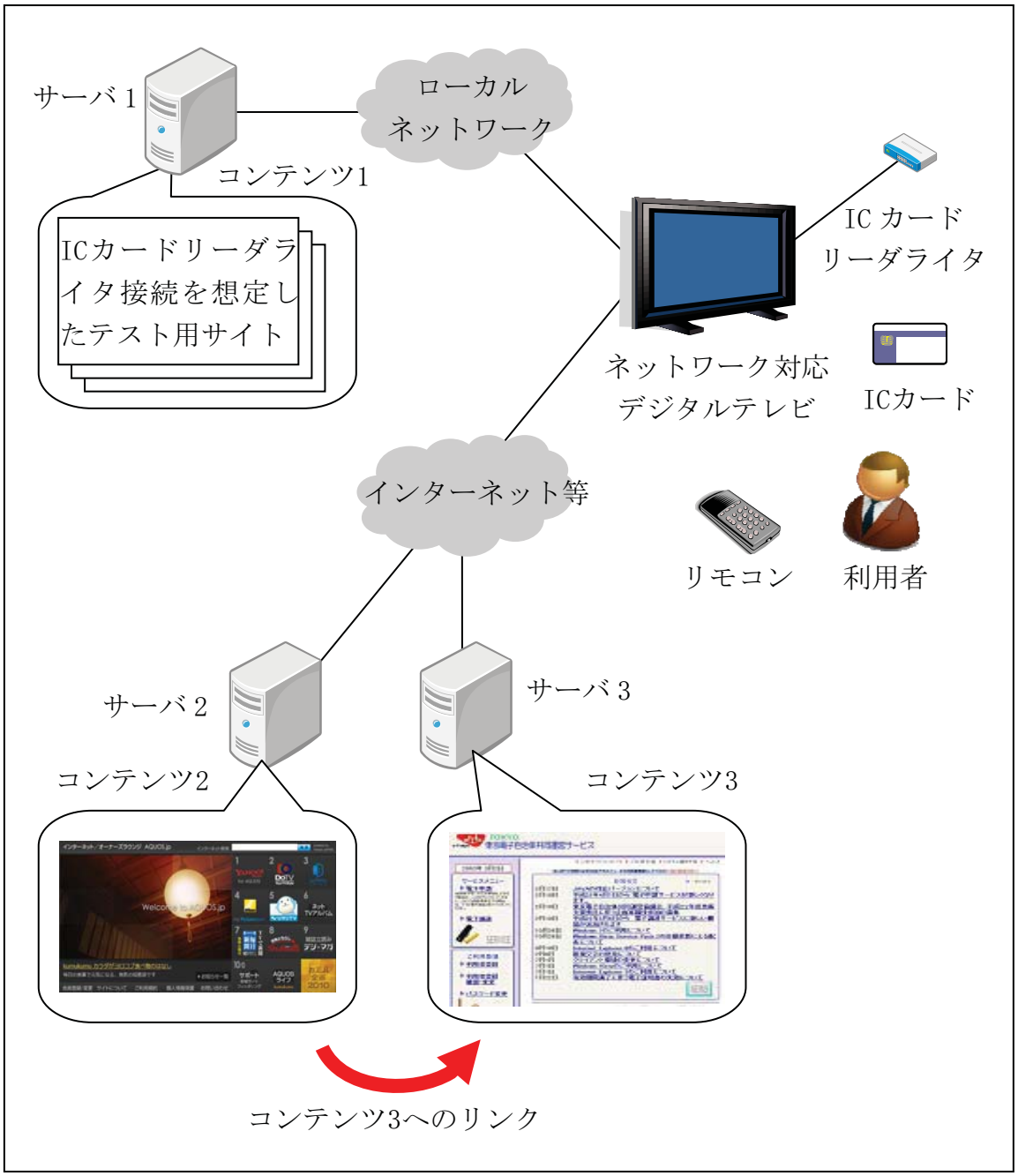


図 3-7 検証環境

(1) IC カードリーダライタの接続に関する検証環境

IC カードリーダライタの接続性の検証を行うために、IC カード試作品（Type-B）と、デジタルテレビ情報化研究会の IC カードへのアクセスに関する仕様（デジタルテレビ ネットワーク機能仕様　IC カードアクセス仕様書）に準拠した HTML ブラウザを搭載するデジタルテレビ試作品とによって、IC カードへのアクセスの実証検証を行う。本検証では、

シャープ LC-40LX1 をベースとした IC カードリーダライタ接続対応試作品を用いる。また、表 3-5 のサーバ 1、コンテンツ 1 を使用して検証を行う。

(2) リモコンでの操作性に関する検証環境

デジタルテレビとリモコンを用いて電子行政サービス等を受ける際のリモコン操作におけるユーザビリティと IC カードを用いた場合のユーザビリティの検証を行う。リモコン操作の検証には図 3-8 で示す現行のデジタルテレビと、その付属品のリモコンを用いる。また、表 3-5 のサーバ 1、コンテンツ 1 を使用する。

図 3-8 検証で使用したデジタルテレビとリモコン
（シャープ製 LC-40LX1）

(3) 電子行政サービス等のポータルへのアクセシビリティに関する検証環境

仮想的に準備したインターネット等上の電子行政ポータルサイトへのアクセス方法について検証を行う。本検証では、図 3-8 で示した現行のデジタルテレビとリモコン、及び、表 3-5 のサーバ 2、サーバ 3、コンテンツ 2、コンテンツ 3 を使用する。

(4) 電子行政サービス等のポータルサイトにおけるユーザビリティに

関する検証環境

市販されているデジタルテレビから現状の電子行政サービス等へアクセスすることで、電子行政サービス等を利用する上でのユーザビリティについて検証を行う。本検証では、図 3-8 で示した現行のデジタルテレビとリモコン、及び、表 3-5 のサーバ 3、コンテンツ 3 を使用する。

3.2.2 検証項目の抽出

3.2.1 で述べた検証環境において、3.1 で挙げた課題と対策の実現性について、以下の検討を行う。

(1) IC カードリーダライタの接続に関する検証

電子行政サービス等へのアクセスに関しては、IC カードリーダライタの接続・搭載が必須の機能となるため、ここでは IC カードリーダライタの接続形態、接続性について以下の検証を行う。

① 検証項目 1-1：IC カードリーダライタの接続形態の検証

IC カードリーダライタの接続形態について、3.1.3 で検討した 3 つの構成、すなわち、リモコン・IC カードリーダライタが一体となっている場合、リモコンと無線接続 IC カードリーダライタが分離している場合、リモコンと有線接続 IC カードリーダライタが分離している場合、のそれぞれについて、ユーザビリティの検証を行い、実利用を想定した場合のユーザビリティ上の課題を抽出する。

② 検証項目 1-2：コンテンツから IC カードへのアクセス検証

コンテンツから IC カード内に保存された情報の読み込みについて、実際に読み出しを行えることを実証する。本検証では USB 接続可能な試作 IC カードリーダライタをデジタルテレビ試作機に有線接続し、次項で説明するコンテンツを用いて、IC カードの情報が読み出せることの確認を行う。

(2) リモコンでの操作性に関する検証

2.1.4 (2) や 3.1.4 (2) でも述べたように、リモコンからの文字入力はパソコンにおけるキーボードからの入力と比較すると煩雑である。デジタルテレビから電子行政サービス等を受ける際のユーザビリティを考えた場合、文字入力の手間を如何に軽減するかが課題となる。実際に、パソコン向けに電子行政サービス等を提供している、東京電子自治体共同運営サービスにおいて利用できるサービスのほとんどが、利用時に ID やパスワードの入力を要求される。特に電子申請を利用する際には、住所、氏名など利用者情報の入力を要求するものが多く見られ、入力項目が多いほど、申請時の手間、所要時間が増大する。図 3-9 は前述の東京電子自治体共同運営サービスのサービス画面の一例である。

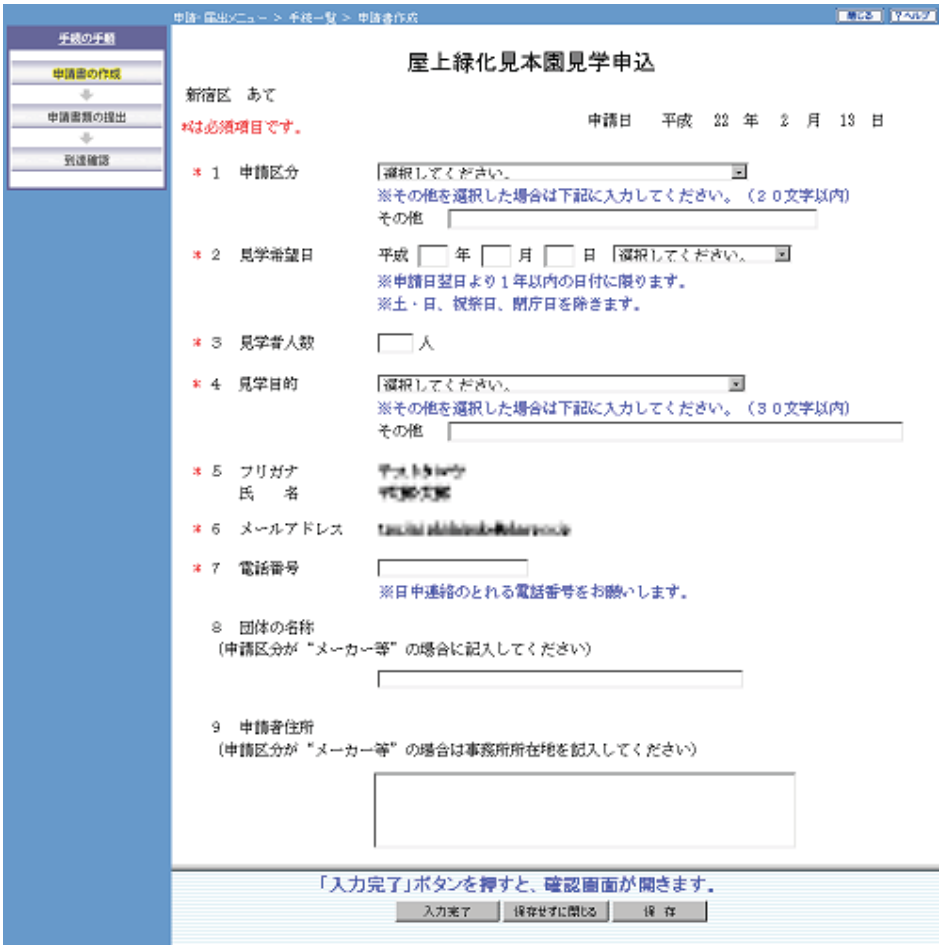


図 3-9　東京電子自治体共同運営サービス申請画面一例

ID・パスワードの設定時に入力した利用者情報が、申請時に自動入力される項目があるが、ID・パスワード設定時に登録が可能な情報としては、ID、氏名、連絡先メールアドレスのみであり、一般的にサービス申請時に必要とされる、住所、生年月日などの追加情報については、利用者が手動で入力する必要がある。

以上の調査結果を鑑み、本検証では、仮想的な住民が一連の申請手続を完結するまでを想定し、すべての入力項目を手動入力する場合と、IC カードを利用し入力項目の自動入力を行う場合とで、手続完了までのリモコンのボタン押下数、及び操作ステップ数を計測し、比較を行う。検証には、3.2.1（2）で述べた検証環境を用いる。

IC カード内には、以下で想定する申請画面で入力が必要なすべての利用者情報が保存されており、PIN コードを入力することで、利用者情報が自動的に入力項目に反映されるものとする。手動入力の場合は、検証に用いるデジタルテレビに搭載されている、図 3-10 のようなソフト

ウェアキーボードを利用し、リモコンによる文字入力を行う。

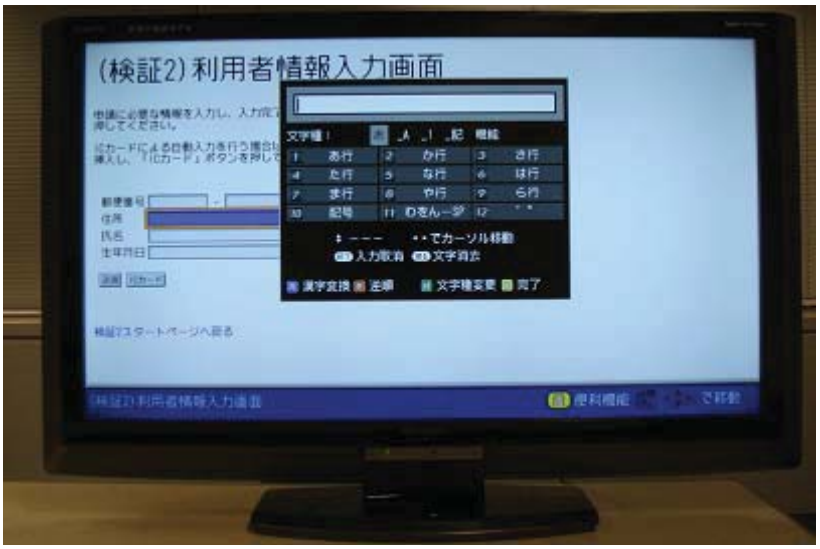


図 3-10　検証に使用したデジタルテレビのソフトウェアキーボード

検証項目としては、①閲覧サービスを利用する場合、②申請サービスを利用する場合、③申請サービスで決済が必要なサービスを利用する場合、④数回の認証が必要なサービスを利用する場合における、リモコンでの操作性の検証を行う。以下でそれぞれの検証項目について述べ、表 3-6、および、表 3-7 にこれらの検証における設定条件をまとめる。なお、検証のフローと検証に用いたコンテンツ仕様については、付録Bに記載している。

① 検証項目 2-1：閲覧サービスを利用する場合

電子行政サービス等の一例として、ID・パスワード入力が必要な情報の閲覧サービスを想定した擬似コンテンツを作成し、市販のデジタルテレビのブラウザからアクセスして、IC カードを利用しない場合と、利用する場合とでサービス完了までの操作を比較する。

IC カードを利用する場合には、4 桁の PIN コードを手動入力することにより、ID・パスワードを自動入力できるものとする。

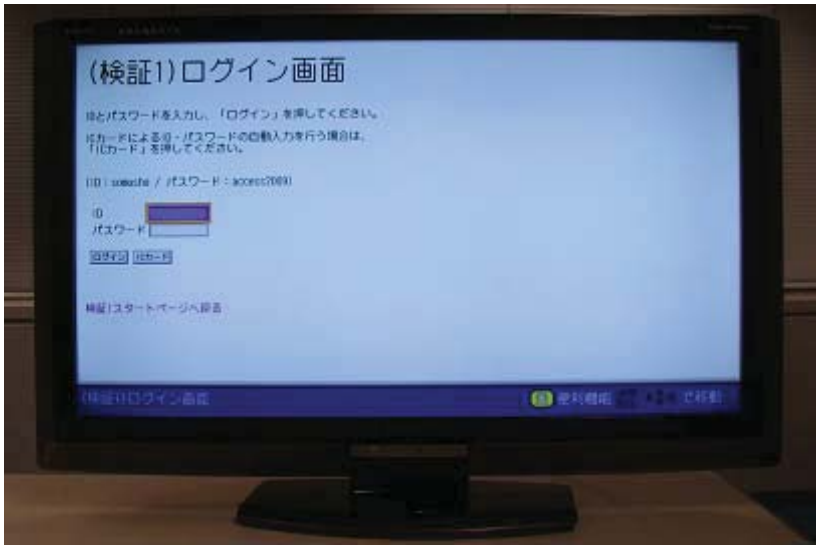


図 3-11　検証 2-1 に用いたテスト用画面（ログイン画面）

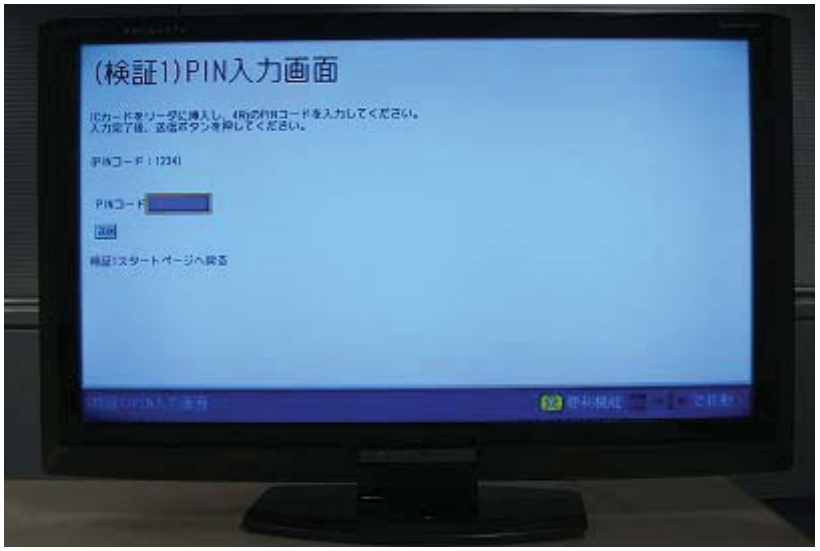


図 3-12　検証 2-1 に用いたテスト用画面（PIN コード入力画面）

上の図 3-11、および、図 3-12 は、検証に用いた画面の一例である。

② 検証項目 2-2：申請サービスを利用する場合

電子行政サービス等の一例として、ID・パスワード入力に加え、利用者情報の入力が必要な電子申請サービスを想定した擬似コンテンツを作成し、市販のデジタルテレビのブラウザからアクセスして、

IC カードを利用する場合と、しない場合とでサービス完了までの操作を比較する。

検証において、申請時の入力項目として、電子申請サービスで入力が必要となることが想定される、郵便番号、住所、氏名、生年月日を設定している。IC カードを利用する場合には、これらの値は、PIN コードを入力することで自動的に入力枠に反映されるものとする。

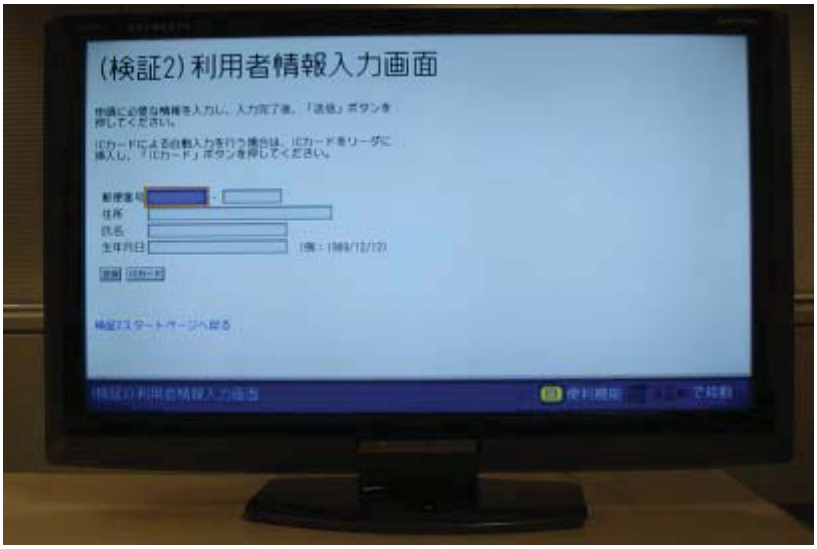


図 3-13 検証 2-2 に用いたテスト用画面
（利用者情報の入力画面）

上図 3-13 は本検証に用いた画面の一例である。

③ 検証項目 2-3：申請サービスで決済が必要なサービスを利用する場合

電子行政サービス等の一例として、ID・パスワード入力、利用者情報の入力に加え、決済情報の入力が必要な電子申請サービスを想定した擬似コンテンツを作成し、市販のデジタルテレビのブラウザから接続して、IC カードを利用する場合と、しない場合とでサービス完了までの操作を比較する。

なお、IC カードを利用しない場合は、クレジットカードよる決済を行うものとし、クレジットカードの情報の入力が要求される。入力項目としては、決済時に一般的に入力が要求される、クレジットカード番号、セキュリティコード、有効期限の 3 項目を設定した。IC カードを利用する場合は、IC カード内にクレジットカード番号等が保持されている、もしくは IC カードとクレジットカード番号が紐

付けられていると想定し、決済画面での文字入力項目は無い。

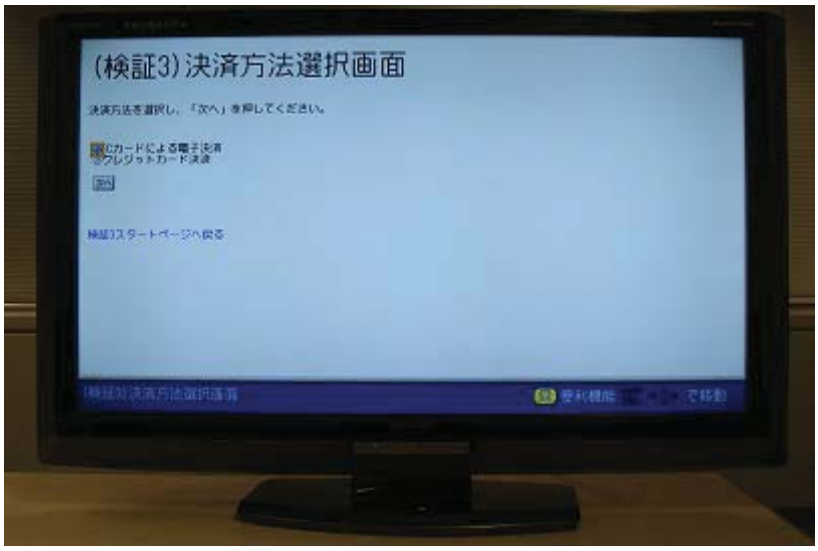


図 3-14　検証 2-3 に用いたテスト用画面
（決済方法選択画面）

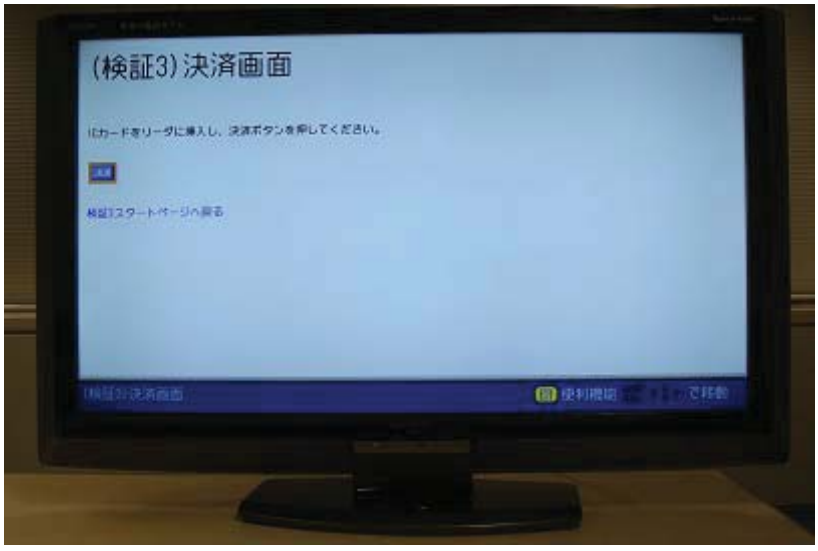


図 3-15　検証 2-3 に用いたテスト用画面
（IC カード決済画面）

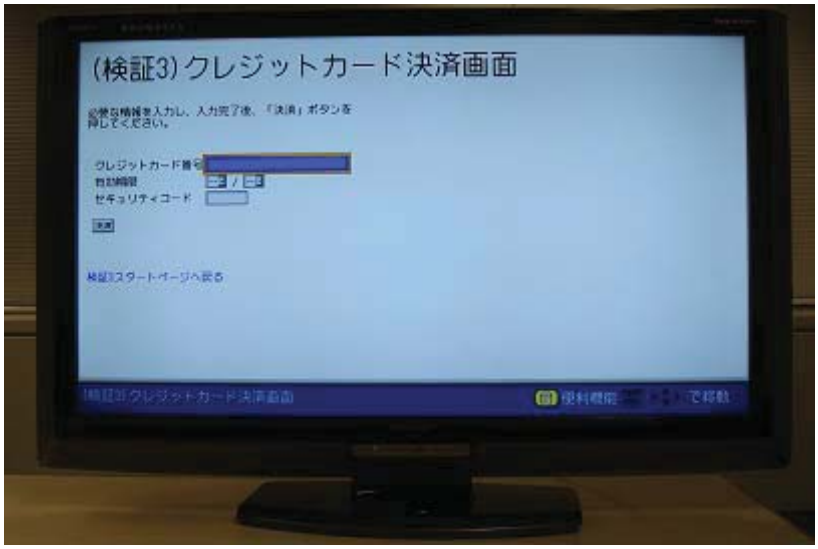


図 3-16　検証 2-3 に用いたテスト用画面
（クレジットカード決済画面）

図 3-14、図 3-15、および、図 3-16 は、検証に用いた画面の一例である。

④ 検証項目 2-4：数回の認証が必要なサービスを利用する場合

擬似サービスコンテンツを用いて、サービス選択、とくに選択先で再度認証が必要となるコンテンツを用いて、都度認証を行うケースと、ワンストップ化するケースでの操作について、IC カードを利用する場合と、しない場合とで比較を行う。

なお、検証項目 2-1 から検証項目 2-4 で用いた入力項目と入力値は 表 3-6 と 表 3-7 の通りである。

表 3-6　入力項目

検証項目	画面遷移数	入力項目数	入力項目	総入力文字数
2-1	4	2	ID,パスワード	17
2-2	5	7	ID,パスワード,郵便番号上 3 桁,郵便番号下 4 桁,住所,氏名,生年月日	56
2-3	7	10	ID,パスワード,郵便番号上 3 桁,郵便番号下 4 桁,住所,氏名,生年月日,クレジットカード番号,セキュリティコード,有効期限	75
2-4	6	4	ID,パスワード	34

表 3-7　各項目の入力値

入力項目	入力値	入力文字数	IC カードからの入力
ID	jikkenR	7	○
パスワード	access2009	10	○
PIN コード	1234	4	×
郵便番号 上 3 桁	261	3	○
郵便番号 下 3 桁	8520	4	○
住所	千葉県千葉市美浜区中瀬 1 丁目 9 番 2 号	18	○
氏名	千葉太郎	4	○
生年月日	1980/01/01	10	○
クレジットカード番号	0123456789012345	16	○
セキュリティコード	123	3	○
有効期限	04/12	-	○

(3) 電子行政サービス等のポータルサイトへのアクセシビリティに関する検証

本検証では、電子行政サービス等へのアクセシビリティ向上のためのアクセス手段を用意し、実際にアクセスし、比較実験を行うことで、そ

れぞれの効果について検証する。アクセス手段としては、現状の手段、ポータルへのリンク設置、ブックマーク機能利用、携帯電話からの画像転送、の 4 つを検証する。前述の東京電子自治体共同運営サービスに市販のデジタルテレビの HTML ブラウザから実際にアクセスすることを想定し、それぞれの手段を用いて、電子行政サービス等へのアクセスが完了するまでに要する操作ステップの計測を行う。

① 検証項目 3-1：現状の手段

HTMLブラウザの「アドレス入力機能」を用いて、リモコンから東京電子自治体共同運営サービスのアドレス（www.e-tokyo.lg.jp）を直接入力し、該当サービスへアクセスする。図 3-17 に検証で用いたデジタルテレビのアドレス入力画面を示す。

図 3-17　検証に使用したデジタルテレビのアドレス入力画面

② 検証項目 3-2：テレビ向けポータルにリンクを設置

テレビ向けポータルサイトの一部を改変して、テレビ向けポータルページに東京電子自治体共同運営サービスへのリンクを設置する。そのリンクを利用して、該当サービスへアクセスする。検証において使用したテレビ向けポータルサイトを図 3-18 に示す。

図 3-18　テレビ向けポータルサイトにリンクを追加した画面

③ 検証項目 3-3：HTML ブラウザのブックマーク機能を利用

デジタルテレビの HTML ブラウザに搭載されている「ブックマーク機能」に東京電子自治体共同運営サービスへのブックマークを事前登録しておく。検証では、ブックマーク選択画面を開き、上記のブックマークを選択することにより、該当サービスへアクセスする。図 3-19 に検証で用いたデジタルテレビのブックマーク選択画面を示す。

図 3-19　検証に使用したデジタルテレビのブックマーク選択画面

④ 検証項目 3-4：携帯電話からの画像転送を利用

シャープ製LC-40LX1 に標準搭載されているフォトリモ [1]機能を利用し、東京電子自治体共同運営サービスのアドレス（www.e-tokyo.lg.jp）を付加したフォトリモ画像を携帯電話からデジタルテレビへ送信することで、該当サービスへアクセスする。

図 3-20 はフォトリモ利用のイメージ図である。

図 3-20　フォトリモ利用のイメージ図

電子行政サービス等からのメールやダウンロードにより、機器制御情報や指定 URL を含んだ画像を取得する。取得した画像を、IrSS 機能を利用して携帯電話からデジタルテレビに送信し、デジタルテレビ側では、その情報を読み取って、自動的に指定された URL へアクセスする。

(4) 電子行政サービス等のポータルサイトにおけるユーザビリティに関する検証

本検証では、パソコン向けに電子行政サービスを提供している、東京電子自治体共同運営サービス（www.e-tokyo.lg.jp）にアクセスし、市販のデジタルテレビのブラウザで表示させた場合の、現状の課題を抽出する。具体的には、東京電子自治体共同運営サービスのトップページから、新宿区の「屋上緑化見本園見学申込」の申請サービスの申請書作成

[1]フォトリモ機能とは、携帯電話などの携帯端末から、機器制御情報を付加した「フォト（画像データ）」を送信することで、ネットワーク対応 TV など、様々なデジタル家電製品を制御・利用する仕組み。シャープ製のインターネット対応デジタルテレビに搭載の機能。

までを行い、その過程で課題点の抽出を行う。(検証項目 4-1)

3.2.3 検証結果

以下に、各検証項目についての検証結果を示す。

(1) IC カードリーダライタの接続に関する検証結果

以下で、3.2.2 (1) で述べた検証 1-1、1-2 の結果についてまとめる。

① 検証項目 1-1：IC カードリーダライタの接続形態の検証

IC カードリーダライタの接続形態は、ユーザとデジタルテレビとの距離と関連性が高い。パソコンの場合では、ユーザはディスプレイの至近距離で操作するため、カードリーダライタもパソコン本体やディスプレイのそばにあってもユーザビリティ的に問題は無い。

デジタルテレビの場合、2～3 メートル程度本体から離れて視聴・操作しているのが通例である。特に近年の大画面デジタルテレビではそれ以上離れて視聴・操作していることも想定される。そのような状況で、デジタルテレビ本体に IC カードリーダライタが内蔵されている場合や、有線接続されている場合では、都度、カードを持ってデジタルテレビ本体に近づかなくてはならないため、ユーザビリティは低下してしまう。

これらを、3.1.3 項で示した各接続形態について検討を行った結果をまとめると、表 3-8 の通りとなる。

IC カードリーダライタを無線接続する形態がもっとも自由度が高いが、実際に使用面から見ると IC カードリーダライタの場所が分からなくなることが想定されることや、電源供給の課題から、現実的では無いと想定される。リモコン一体型の場合は、特に大画面デジタルテレビでも、手元にあるリモコンで操作可能となることから、ユーザビリティの面からは推奨できるものである。

しかしながら、多くのユーザが IC カードリーダライタを用いたサービスを利用するようにならなければ、利用しないユーザに対して不要なコストを強いることとなるので、パソコンで利用されている IC カードリーダライタをデジタルテレビで使用できるようにすることも、普及の一助と考える。

表 3-8　IC カードリーダライタの接続形態ごとのユーザビリティ

	リモコンと IC カードリーダライタが一体型の場合	IC カードリーダライタが無線接続の場合	IC カードリーダライタが有線接続の場合
リモコンの操作性	課題有り IC カードへのアクセス時にも、リモコンの操作性が損なわれない形状が必要	課題無し 別筐体となるので、リモコン操作への影響は少ない	課題無し 別筐体となるため、リモコン操作への影響は少ない
大型テレビでのユーザビリティ	良 ユーザの手元で IC カードの操作が可能	良 ただし、カードリーダライタそのものが紛失する可能性あり	課題有り IC カード読書き時に、移動しなければならない可能性が高い
小型テレビでのユーザビリティ	良 ユーザの手元で IC カードの操作が可能	良 ただし、カードリーダライタそのものが紛失する可能性あり	良 距離が短いため大きな問題とはならない
ペアリング操作	必要 ただし、出荷時に設定可能	必要 ただし、出荷時に設定可能	不要
IC カードリーダライタへの電力供給	課題有り リモコンの電池と共用となるため、電池寿命を延ばすための工夫が必要	課題有り IC カードリーダライタとして使用のたびに電源 ON/OFF を行う必要あり	課題無し デジタルテレビ本体から供給されるため、ユーザビリティの課題はない。もちろん、省電力であることは求められる

② 検証項目 1-2：コンテンツから IC カードへのアクセス検証

電子行政サービス等から、デジタルテレビに接続された IC カードリーダライタを通して、IC カードの情報が読み書きできるかについては、IC カードリーダライタを有線でデジタルテレビに接続する形態で検証を行った。

一般に市販されている IC カードリーダライタでは、論理的にはシリアルで物理的には USB で接続する形態のものが多いため、一般に市販されているデジタルテレビのファームウェアに対して、USB シリアル変換をサポートするカーネルに入れ替えたファームウェアを搭載したデジタルテレビ試作機で検証を行った。USB シリアル変換をサポートするための修正は、カーネルのコンフィグレーションパラメータのみを変更し、再コンパイルするのみであり、Linux OS を採用しているデジタルテレビでは容易に対応できるもとの想定できる。

今回の検証において、USB 接続可能な Type-B 試作カードリーダライタをデジタルテレビ試作機に接続して、Type-B IC カードの情報が読み出せることが確認できた。今回の検証では、カード情報の読み出しのみであったが、デジタルテレビ試作機からコマンドを送出していることから、書き込みも同様にできるものと推測できる。

検証項目 1-1 の検証結果で示したように、IC カードを有線接続する方式は、ユーザビリティ上の課題はあるが、デジタルテレビとしては、対応の敷居が低く、アクセス多様化に関しては、有望な選択肢と考える。

一方、IC カードリーダライタがリモコンと一体となっている場合については、ユーザビリティとしても、今後、下記の検討が必要である。

- リモコン操作の妨げとならないような場所に IC カードリーダライタを取り付ける必要がある。
- IC カードの情報が確実に読み書きできるように、IC カードの読み書き中であることをユーザに通知したり、読み書き中に IC カードの位置がずれないような形状にする、などの対応が求められる。
- リモコンと電源を共通化することから、必要なときのみに IC カードリーダライタの電源を入れるなどの工夫が必要となる。ソニーのリモコンでは、ユーザが明示的に電源を入れる工夫を行っているが、自動的に制御できる工夫が必要である。
- 双方向通信が必要となることから、リモコン信号を含め、無線通

信となる可能性が高い。この場合に、

・家庭内で使用している無線機器、例えば、携帯電話や無線 LAN 装置と競合しても、確実に通信が行えること

・無線通信路上で十分なセキュリティが保たれること

・リモコンのみとして使用しても、従来リモコンと同等の電池寿命となるような省電力方式であること

が求められる。

(2) リモコンでの操作性に関する検証結果

3.2.2(2)で述べたリモコンでの操作性の検証 2-1 から 2-4 について、結果を 表 3-9 にまとめる。

表 3-9　リモコンでの操作性の検証の結果

検証項目	条件	画面遷移数	入力項目数	総入力文字数	クリック数（内 文字入力）		操作ステップ数（内 文字入力）	
2-1	IC カードなし	4	2	17	54	(47)	7	(2)
	IC カードあり	6	1	4	16	(5)	7	(1)
2-2	IC カードなし	5	7	56	210	(192)	18	(7)
	IC カードあり	7	1	4	23	(5)	9	(1)
2-3	IC カードなし	7	10	75	254	(214)	29	(10)
	IC カードあり	9	1	4	27	(5)	11	(1)
2-4	IC カードなし	6	4	34	107	(94)	13	(4)
	IC カードあり	10	2	8	31	(10)	13	(2)

表 3-9 で、クリック数の内、文字入力でのクリック数をカッコ内に記載している。また、入力項目数と関連を見るため、操作ステップ数につい

ても計数した。操作ステップとは、意味のある一連の操作をまとめたものと定義する。本検証では、以下の操作ステップを定義する。

- 選択決定操作:選択したいコンテンツ上のリンクやボタンにカーソルを移動し、決定ボタンを押す操作
- 文字入力操作:文字入力パネル上で所望の文字列を入力し、コンテンツへ反映させる操作
- ラジオボタン選択操作:Form 要素のラジオボタンで所望の項目を選択する操作
- セレクトボックス選択操作:Form 要素のセレクトボックスで所望の項目を選択する操作
- 機能呼び出し操作:ブラウザの機能を呼び出すための操作

検証項目 2-1 から検証 2-4 全てで、IC カード内の情報を文字入力に利用し、文字入力の手間を低減する事により、一連の手続完了までに要するボタンのクリック数、操作ステップ数は、IC カードを利用しない場合と比べて低減された。検証項目 2-1 のように、ID とパスワードの入力のみでも、PIN コードより長い ID やパスワードが設定されている場合は、効果があることが分かる。

特に、検証 2-2 と検証 2-3 のように、個人情報を入力する電子申請を想定した検証では、そのクリック数のほとんどが文字列の入力となっており、これらの情報を IC カードから読み込むことにより、PIN コードの入力分を加味しても、クリック数が約 90%低減され、効果が大きいことが分かる。

また、操作ステップ数の観点から見ると、入力項目が多くなると項目間の移動などのための操作ステップ多くなるが、IC カードに保持されている情報の項目が多いほど、IC カードからの読み込みよって操作ステップ数が削減（今回では 1 回となる）されている。

(3) 電子行政サービス等のポータルへのアクセシビリティに関する検証結果

3.2.2(3)で述べたリモコンでの操作性の検証 3-1 から 3-4 について、結果を 表 3-10 にまとめる。

表 3-10　電子行政ポータルへのアクセシビリティの検証結果

検証項目	画面遷移数	クリック数	操作ステップ
3-1	3	57	5
3-2	1	2	2
3-3	3	6	3
3-4	1	0	0

リモコンから東京電子自治体共同運営サービスのアドレス（www.e-tokyo.lg.jp）を直接入力してアクセスを行う場合と比べ、テレビ向けポータルやデジタルテレビ端末側でなんらかの対策を行った場合は、クリック数、操作ステップともに低減することができる。

しかしながら、メーカポータルサイトは、通常、メーカ側の管理下となっており、リンクを置くことで費用の発生が想定され、電子行政サービス等へのリンクを置くには困難なことが想定される。また、ブックマークを利用するにしても、操作が必要となってしまう。

たとえば、メーカポータルサイトにおいて、ユーザの使用している機器に保存されている特定ブックマークへのリンクを追加できるような機能があれば、課題解決の１つとなる。

(4) 電子行政サービス等のポータルサイトにおけるユーザビリティに関する検証結果

3.2.2 (4) で述べたユーザビリティに関する検証 4-1 について、市販のデジタルテレビを用いて、パソコン向け電子行政サービス等にアクセスを行った検証項目 4-1 の結果と、抽出した課題点を列挙する。

① イメージマップの利用

電子申請トップ画面の申請先自治体選択では、東京都の地図画像の中に複数のリンクが設定されており（イメージマップ）、その中から申請先の自治体を選択できるようになっている（図 3-21 を参照）。これを現行のデジタルテレビで操作を行ったところ、千代田区にフォーカス移動をすることができなかった。

パソコンであれば、マウスを用いて、所望の位置にポインティングカーソルを移動させることは容易であるが、現状のデジタルテレビは、ポインティングカーソルをサポートしていないものが一般的であるため、リモコンの上下左右ボタンを用いて所望の位置にフォーカスを移動せねばならず、複雑な配置になると、ユーザの意図した移動とならないだけでなく、到達できない場合が発生する。

図 3-21　東京電子自治体共同運営サービスの申請先自治体選択画面

② フレームの使用

申請・届出手続ナビゲーション、申請書作成ページなどでは、デジタルテレビ情報化研究会のガイドラインで仕様外とされているフレームが使用されていた。

リモコンでフォーカスを移動する場合、フレームが利用されていると、操作対象となるフレームがわかりにくい、カーソルの挙動が不自然になる、といった問題がある。

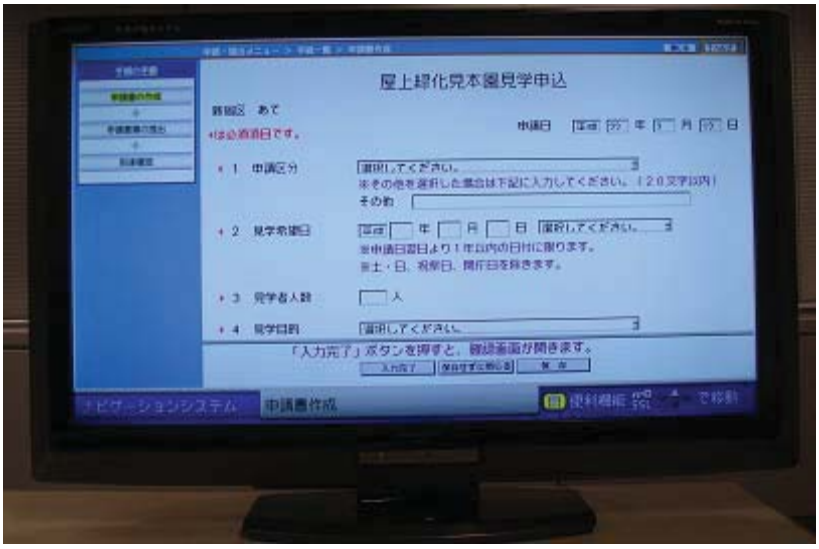


図 3-22　東京電子自治体共同運営サービスでのフレームの利用

③ JavaScript の使用

電子申請サービスで利用している JavaScript がデジタルテレビで対応しておらず、正しく視聴できない可能性がある。今回の検証においては、申請書作成ページへ遷移する際、図 3-23、図 3-24 に示すような JavaScript の警告が出た。

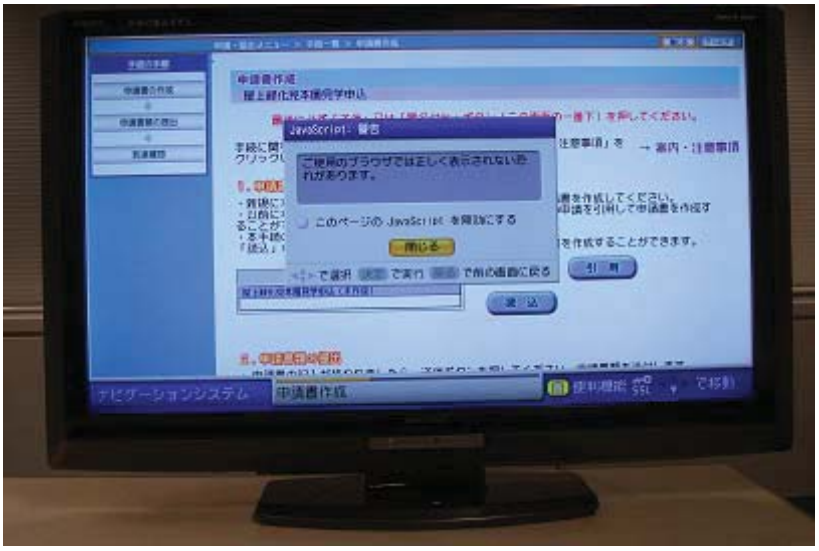


図 3-23　東京電子自治体共同運営サービス での
JavaScript 警告

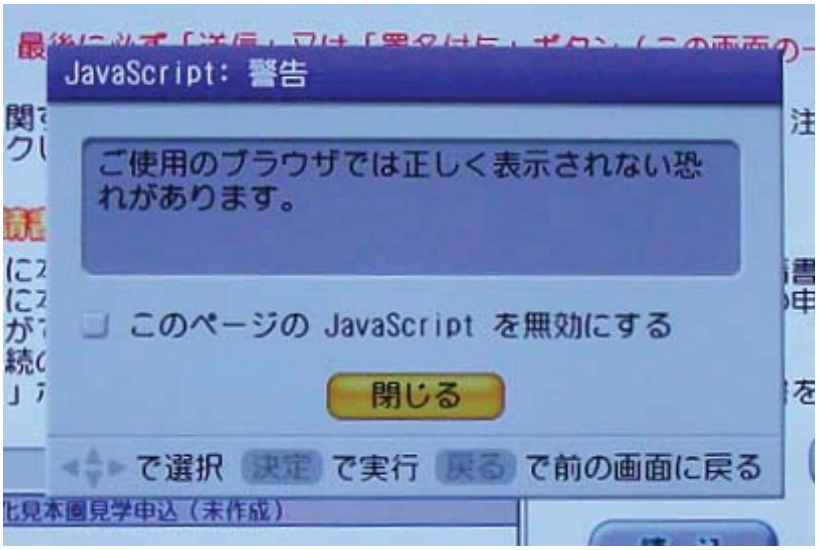


図 3-24　東京電子自治体共同運営サービス での
JavaScript 警告詳細

パソコンの場合であれば、使用するブラウザを変更したり、ブラウ

ザのアップデートを行ったりすることで対応が可能な場合が多い。しかしながら、デジタルテレビの場合、デジタルテレビ情報化研究会のネットTVブラウザ仕様において、実装が必須と規定されているもの以外のオブジェクト、属性、メソッド、イベントハンドラ、命令文、演算子については、サポートできない場合がある。今回の実験では、上記の警告が出たものの、表示できたが、使用するブラウザによっては、表示できない可能性がある。

④ 入力要素のcharacter-type特性

デジタルテレビ情報化研究会のガイドラインでは、文字入力を行うINPUT要素に対して、入力する文字種別を指定するcharacter-type特性を追加している。東京電子自治体共同運営サービスはパソコン向けのサービスであるため、この特性は指定されていなかった。

デジタルテレビでの文字入力において、入力する文字種を変更するためには、リモコンの機能キー押下や、ソフトウェアキーボード上に用意された文字種変更ボタンの押下といった、操作が必要となるのが一般的である。要求される文字種と、ソフトウェアキーボードの文字種の初期値が異なる場合、INPUT要素にこの特性が指定されていなければ、利用者側で所望の文字種に変更してから文字を入力する必要があり、その分入力効率が悪くなる。

3.2.4 まとめ

本項では今回行った実機での検証結果のまとめと考察を行う。

(1) IC カードリーダライタ接続形態の検証結果について

試作品レベルではあるが、Type-B の IC カードリーダライタをデジタルテレビに接続し、HTML コンテンツを用いてパラメータの読み込みができることを確認した。

今回の検証作業では、IC カードへの書き込みについては検証を行っていないが、デジタルテレビから、IC カードリーダライタへのコマンド送受信ができていることから、IC カードへの書き込みについても読み込みと同じ通信線を使うことから、IC カードリーダライタへの書き込みについても問題なく行えると想定できる。

IC カードリーダライタの形状については、確実に読み込むことができるように、デジタルテレビへの内蔵、デジタルテレビと有線接続、リモコンへの内蔵のそれぞれの場合について、引き続き検討が必要である。特にデジタルテレビの場合には、その大きさに幅があり、それぞれの大きさについて、より多くのユーザの意見を求めることが必要である。

IC カードリーダライタをリモコンに内蔵した場合については、デジタルテレビ本体との通信において無線方式が想定されるが、既存の無線機器との干渉に強く、十分なセキュリティが保たれる通信方式の選択が必要である。

また、電子行政サービス等へのアクセス多様化の観点では、IC カードリーダライタが内蔵、もしくは、同梱されていることが望ましいが、USB 接続などで必要なユーザが後付けできると、テレビのコストアップが抑えることができ、対応機器を増やすことが可能となる。

(2) リモコンでの操作性の検証結果について

デジタルテレビでの課題となっている文字入力に関して、IC カードから読み込むことによって、簡便に行えることが確認できた。東京電子自治体共同運営サービスで、個人向けサービス登録数の多い葛飾区と中野区を調査したところ、98%で個人情報の入力が必要であり、葛飾区では、イベント等申し込み手続の 70%が個人情報の入力のみで申し込みが可能となっている。このことから、電子行政サービス等の申請や閲覧時、住所、氏名等の個人情報の入力が簡略できるとユーザビリティを向上できるものと考えられる。調査の詳細については、付録 C を参照。

IC カードリーダライタを有線でデジタルテレビに接続した場合について操作性の検証を実施したが、IC カードリーダライタをリモコンに内

蔵した場合についても、操作として問題ないかの確認は必要と考える。

また、本検証では、テスト用のコンテンツ、テスト用のカードを使用したが、実際のサービスに向けては、

- 電子行政サービス等との連携を前提としたカード仕様として、どこまでの情報を IC カードに保持するか
- ID、パスワードがオンライン発行された場合に、これらをどのように IC カードに書き込むか、もしくは電子行政サービス等との連携を行うか
- デジタルテレビで、電子署名を行う場合の技術的な仕様と操作性の検討

などについて、引き続き検討が必要と考える。

カードの仕様に関しては、IC カード内に個人情報が保持されている場合について検証を行ったが、サーバに個人情報が保持されている場合についても検証が必要である。

サービスを完結するとの観点では、決済についてはクレジットカードによる決済について検討を実施したが、電子マネーなどの小額決済への対応についても検討が必要である。また、証明書発行については、デジタルテレビからの印刷や、キオスク端末との連携などの検討が必要である。

今回の検証では、リモコンでの操作に限定して、その操作数を基準にユーザビリティの検証を行ったが、今後、デジタルテレビの性能向上や、インターネット等のアクセスが一般化すれば、キーボードやマウスなどの接続も想定され、これらを用いた場合の検証も必要である。

(3) 電子行政サービス等のポータルへのアクセシビリティの検証結果について

電子行政サービス等のポータルサイトへのアクセシビリティについては、メーカポータルサイト、ブックマーク機能等を用いて、より容易にアクセスできることが検証できた。

しかしながら、デジタルテレビを使っている多くのユーザは、デジタルテレビ放送を視聴しており、受動的な操作を行っているのが現状である。例えば、放送波に多重化されているデータ放送から、ユーザへのお知らせができれば、行政サービスから個人に合わせた情報提供が可能となる。デジタル放送の BML ブラウザから、HTML ブラウザを起動する仕様については、既に規定されており、技術的には可能となっている。

(4) 電子行政サービス等のポータルサイトにおけるユーザビリティの検証結果について

パソコン向けに行われている電子行政サービス等を一例として、パソコンでアクセスする状況では、非常に良くできているサイトであったとしても、デジタルテレビでサービスを受ける場合について、3.2.4 (2)で示したように、デジタルテレビ情報化研究会仕様のガイドラインにて留意すべき点の内、下記の3点には対応できていないことが確認できた。

- イメージマップで到達できない領域があった
- 仕様外とされているフレームが使用されていた
- INPUT 要素に対して文字種別が設定されていなかった

電子行政サービス等へのアクセス多様化では、デジタルテレビ、キオスク端末、携帯電話などの様々な種別の端末からのアクセスが想定されるため、それぞれの端末種別にあったコンテンツ配信が必要となる。現行のデジタルテレビに対してサービスを行う場合については、ガイドライン従ったコンテンツ作成が望まれる。

デジタルテレビも、年々能力・機能が向上してゆくことが期待でき、例えば、2009 年 12 月に発売された東芝の CELL REGZA 55X1 では、タッチパッドや一般のインターネット等サイトの視聴が可能なブラウザ（フルブラウザ）が搭載されるなど、ネット機能についてパソコンと同様の機能が実現されつつある。このように、フルブラウザが搭載されたり、キーボードやマウスなどのデバイスが接続されるような次世代のデジタルテレビに対して、その能力を十分にサービス側から使えるようにするための仕様検討も必要と考えられる。

4. （アクセス手段の多様化）キオスク端末に関する調査研究

2章で述べた現状を踏まえ、キオスク端末から電子行政サービス等へアクセスするための具体的な実現モデルを設定し、モデルの各構成要素に求められる機能を整理する。また、想定した実現モデルに対する課題への対策方法を調査するとともに、実証環境にて実現性の評価を行う。

4.1 課題の抽出及び対策の検討

本節では、キオスク端末から電子行政サービス等へアクセスするためのモデルを示すとともに、具体的な課題とその解決策について検討する。

4.1.1 実現方法のモデル化

図 4-1 は、キオスク端末を利用して電子行政サービス等にアクセスするための実現モデルである。利用者は、インターネット等によって電子行政サービス等と接続されたキオスク端末を利用することによってアクセスする。ICカード認証等の手段によって利用者の特定・認証・利用許可を受け、証明書の交付、個人情報を含む情報提供、申請などの様々な行政側が提供する電子行政サービス等を受けることになる。

図 4-1 の各構成要素は以下の通りとなる。

(1) 情報保有機関

利用者の情報を保有し、利用者に対して、証明書の交付サービス、電子的に蓄積された利用者等の情報を提供する情報提供サービス、利用者から行政サービスへの申請を受け付ける申請サービス等を提供する国・自治体の機関等であり、これらの各種サービスを電子行政サービス等を通じて提供する

(2) 電子行政サービス等

国・自治体などの情報保有機関と、利用者が操作する端末を接続する機能を有するシステムで、認証基盤を利用した個人の識別・認証や、各サービスを提供するためのポータルなどの機能を持つ。

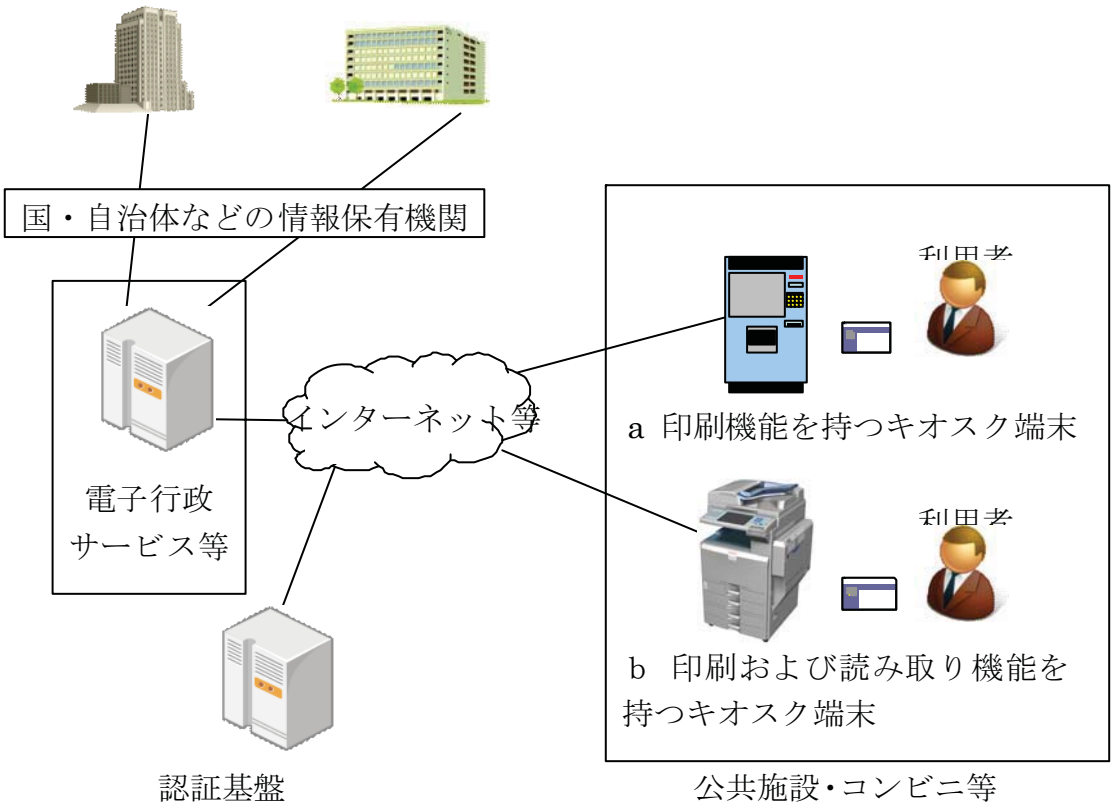


図 4-1　実現モデル

(3) 認証基盤

個人を識別、認証するための情報基盤。公的個人認証基盤のように、PKI にて個人を認証する個人認証基盤を想定する。

(4) インターネット等

キオスク端末と電子行政サービス等を接続するネットワークは、2.2.2 で述べたとおり、自治体等が設置したネットワーク、コンビニ事業者等の民間事業者のネットワーク及びインターネット等の公衆網などのいずれかあるいは組み合わせの可能性がある。

(5) 印刷機能を持つキオスク端末

電子行政サービス等に接続される情報端末の１つで、自治体の関連施設やコンビニ等に設置され、不特定多数の利用者から利用される端末。電子行政サービス等を通じて各情報保有機関が保有する情報に接続するとともに、電子行政サービス等から提供された情報を利用者の指示によって表示あるいは紙に印刷する機能を有する。

(6) 印刷及び読み取り機能を持つキオスク端末

電子行政サービス等に接続される情報端末の１つで、自治体の関連施設やコンビニ等に設置され、不特定多数の利用者から利用される端末。電子行政サービス等を通じて各情報保有機関が保有する情報に接続するとともに、電子行政サービス等から提供された情報を利用者の指示によって表示あるいは紙に印刷する機能と、利用者が紙で用意した情報を電子化して電子行政サービス等を通じて情報保有機関等に送信する機能を提供する。申請自体は電子化されているが、添付書類が紙で残っているものも多い。スキャンによって紙情報を電子化して電子文書として取り扱うことによって、電子文書が適応可能なサービスが広がる可能性がある。

4.1.2 システム機能に関する課題及び対策

本項では、4.1.1 で述べた実現モデルに基づいて、キオスク端末から電子行政サービス等へアクセスするための実現方法を検討し、電子行政サービス等への接続に関する課題、キオスク端末に関する課題についての考察を行う。

(1) 電子行政サービス等への接続

2.2.2 の電子行政サービス等への接続の課題で挙げた通り、キオスク端末の設置環境等により異なる接続構成を取る可能性がある。本研究では、ネットワーク基盤の安全性が確保されているという前提で、電子行政サービス等を共通に提供するという視点からの課題と解決策について検討する。

① 多様な接続構成に対応した情報提供

キオスク端末の接続構成は複数想定されるが、電子行政サービス等で接続経路の異なる端末毎に異なったサービスの提供を行うことは非常に効率が悪い。つまり、同じキオスク端末であれば、接続の形態によらず、基本的には同じサービスが利用できる必要がある。また利用者は、キオスク端末に限らず、パソコン、デジタルテレビ、携帯電話等、多様な端末から電子行政システム等にアクセスする可能性がある。その際電子行政サービス等が考慮しなくてはならないのは、どのような端末からも同じようにサービスが利用できる必要がある点である。そのためには、以下が必要となる。

(i) ネットワーク接続手段

標準的なネットワーク接続手段で接続できること（例えば、TCP/IP 等）が必要となる。キオスク端末の場合、オプションでネットワー

ク接続手段を設けることができるので、ハードウェアは標準的な接続手段を具備していることを前提として問題ないと考えられる。

（ii）利用手順

同じ手順で電子行政サービス等が利用可能なこと。例えば端末や接続経路によらない利用者毎のポータルを用意するのも一案である。どのようなアクセス手段を利用しても同じポータルからスタートし、同じ手順で利用できるようにすることによって、利用者はアクセス手段を意識することなく電子行政サービス等を利用できるようになる。サービス毎に利用の手順を標準化する必要も生じる。

（iii）記述様式

一度導入すると端末が入れ替わるまで一定期間（数年～5 年程度）必要であるため、新しい記述様式に対応するのは難しい。そのため、例えば、印刷を前提とした場合には、PDF、その他の場合には HTML あるいは XML 等を利用するなど、標準的に使用されているあるいは標準が存在する記述様式を採用する必要がある。

② 多様な能力の端末に対応した情報提供

利用者が電子行政サービス等にアクセスする入り口は、同じであるほうが利用しやすい。但し、端末によっては表示能力、操作性等が大きく異なるので、その点を考慮しつつ情報を提供しなければならない。現在多くのホームページが、パソコンと携帯電話からのアクセスの２種類のコンテンツを用意している。これは、両者の間に表示能力に大きな差があることと、ユーザインタフェースが大きく異なっているためである。キオスク端末においては、ユーザインタフェースにタッチパネルが採用され、マウスのような操作性の高いポインティングデバイスや通常のキーボードは利用できないので、それに配慮した入力や画面遷移で必要な情報の入手等ができる必要がある。具体的には

・スクロールを極力避けた画面作り

・キーボードの利用を極力避ける入力

・単純なボタンによる選択及び画面遷移

等に配慮した形で情報を提供する必要がある。

(2) キオスク端末の機能

想定される電子行政サービス等は、証明書交付、情報参照、申請の３種類である。これらのサービスを提供するためには、キオスク端末とし

て、以下のような機能が必要となる。

① 安全に電子行政サービス等に接続する機能

キオスク端末は、電子行政サービス等の標準的なネットワーク接続手段によるサービス提供に対応したものである必要がある。特に、利用者個人の情報がネットワーク上を流れることになるので、SSL あるいは VPN などの機能によって安全な通信路を確立した上でそのサービスが利用できる必要がある。

② 提供されるサービスを受けるための機能

(i) 証明書交付

紙への出力を前提としているので、証明書の内容の画面への表示は必須とはならない。むしろ印刷に適したフォーマットで情報の提供が行えることが重要であって、PDF はその候補の１つである。尚、最近のオフィス向けのプリンタや多機能プリンタは、PDF ファイルをプリンタドライバを介さずに直接受取り、受け取った PDF ファイルを内部で印刷画像に変換して印刷する機能を持った機種も増えており、PDF での配布は現実的な方法の１つである。

(ii) 情報参照

情報の参照は、端末での表示を前提とする。但し、キオスク端末では印刷の可能性があるので、表示・印刷の両方の機能を持つ必要がある。

(iii) 申請

キオスク端末の場合には、標準的な入力がタッチパネルと数字入力用のテンキーのみとなっているのが普通である。その他の場合には、画面に表示されたソフトキーボードからの文字入力が必要となる。ソフトキーボードは、通常のキーボードより操作性が劣り、入力にも時間がかかる。そのため、入力情報を氏名等から自動的に挿入する等、ソフトキーボードからの入力を極力必要としない方法を検討する必要がある。

利用者がキオスク端末で申請の結果を受け取る場合、情報参照と同様に結果を表示・印刷する機能が必要となる。

(3) 認証基盤の利用

本項では、4.1.1 で述べた実現モデルに基づいて、キオスク端末から利用者認証に利用される認証基盤を利用するための実現方法を検討する。対象として公的個人認証基盤相当のPKIの電子認証用基盤を利用するこ

とを想定した。

他にも ID とパスワードを組み合わせる認証方式等もあるが、キオスク端末においては ID を手で入力する必要のない IC カード等個人識別番号を機械的に読み取れる媒体を利用した認証のほうが利用者にとって利便性が高いと考えられる。

① 電子行政サービス等に対する検討

公的な個人認証サービスの利用を前提とすると、証明書の有効性の確認を行えるのは、公的サービスを提供する電子行政サービス等となる。キオスク端末から電子行政サービス等に安全な経路で送られた電子証明書によって証明書の有効性を確認し、利用者の識別を行い、暗証番号等の照合と秘密鍵の確認による利用者認証を行うものとする。

② キオスク端末の機能

キオスク端末はコンビニ等の民間施設に設置する可能性もあるので、電子証明書の有効性確認を含めた認証手順そのものは電子行政サービス等が制御することになる。キオスク端末では以下の機能を提供すればよいことになる。

（i）カードアクセスソフトウェア

PKIを用いる場合、一般にはPKCS#11[1]インタフェースを利用したカードアクセスソフトウェアを通じて対象となるICカードにアクセスすることになる。通常はICカードを使ったシステムを提供する提供者が対応したソフトウェアも一緒に提供することになるが、Windowsなど一般的なOSに対してはソフトウェアが提供されている。しかしながら多機能プリンタの場合にはWindows以外の組み込み型OSを採用している場合も多く、カードサービスの提供者が対応したソフトウェアを提供できない場合も起こりうる点に注意が必要となる。キオスク端末に限らず、組み込み型OSを採用した環境でも広く使えるようにするためには、仕様を公開して、各社が対応ソフトウェアを開発可能にするか、公開されている仕様に基づいて構築された基盤を採用することが必要である。

（ii）暗証番号入力

利用者が暗証番号を入力する機能を持つ必要がある。英数字・記号

[1] PKCS#11 とは、公開鍵基盤（PKI）の技術仕様をまとめたデファクトスタンダードである PKCS シリーズで規定されるもので、PKI の演算などで使用する暗号鍵、公開鍵証明書等を格納しているトークン（媒体）を利用するためのソフトウェアのインタフェース仕様を規定している。

等を組み合わせたパスワードとする場合には、ソフトキーボードから入力することとなるので、キーボードあるいはテンキーを利用する場合に比べて操作性が劣ることと第三者から覗き見られる可能性が高くなる点に注意する必要がある。

4.1.3 セキュリティに関する課題及び対策

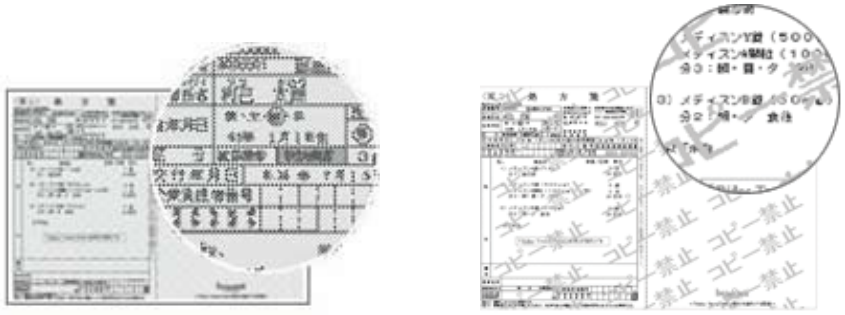
本項ではキオスク端末で電子行政サービス等を実現するために要求されるセキュリティに関する事項に対する検討を行う。

(1) 証明書の交付に関連する安全性確保

証明書の有効性を担保するために、コピーされたものでないこと、偽造されていないことを確認することが重要となる。特殊な紙でなく、普通の紙を使った技術としては以下のような実現方法がある。

① コピーの防止・検出

紙幣で使われているようなコピーを防止する技術を一般のプリンタで実現することは難しいので、コピーされたことがわかる技術を使うのが一般的である。典型的な技術は、図 4-2 に示すようなコピーすると背面に禁止文字が浮き出る技術である。



オリジナル　　コピー

図 4-2　コピー禁止文字が背景に浮き出る例

② 偽造防止・真正性の確保

証明書自体が偽造されたものではなく、正しいものであることを確認する方法には、オフラインで確認する方法及びオンラインで確認する方法がある。

(i) 隠れた画像の埋め込み技術（オフライン）

肉眼では識別できない画像を埋め込んでおき、それを確認すること

で正当性を確認する方法である。国立印刷局の ImageSwitch が典型的な例で、特殊な観察装置の元では、肉眼では見えなかった画像が浮き出る。問題点としては、検証に観察装置が必要となる点である。

（ii）コードの埋め込み技術による内容確認（オフライン）

画像の中に特定の情報を埋め込む技術や、文書（画像）の特徴量を抽出する方法などが応用可能である。

電子透かしと呼ばれる画像や映像、音声の中に人間には感知できない情報を埋め込む技術がある。画像に限ってみても、画像の背景となる地の部分にコードを埋め込む方法、色の階調を変化させて埋め込む方法、文字などの境界線の部分を変形させる方法など多様な方法が提案されている。手法によっては数 KB から数十 KB の情報を埋め込むことができるので、電子透かしの中に検証用のコードを埋め込み、埋め込まれた検証コードの正当性を確認することで証明書の正当性を確認する方法がある。一例としては、証明書の証明内容あるいはその一部と検証コードの中に埋め込まれた情報が一致するか否かによって判断することができる。たとえば、証明書の内容に対応する情報（住所・氏名等）を埋め込んでおけば、印刷されている証明書の情報とコードから再現した証明書の情報を目視にて比較し、一致するか否かによって情報が正しいかどうかを判別することができる。問題点としては、画像を取り込む装置と解析ソフトが必要となる点と、印鑑証明のようなデータ量の多くなる証明書には向かない点である。

（iii）画像情報確認（オンライン）

証明書の内容を暗号化したコードとして印刷しておき、オンラインでその内容を確認する方法である（図 4-3①）。

（iv）内容確認（オンライン）

（ii）のコード埋め込み技術の応用で、証明書そのものを埋め込むのではなく、交付する証明書を識別する証明書番号を埋め込んでおき、その番号によって検証サーバに問い合わせて証明書の内容を確認する方法である（図 4-3②）。

現状ではコピーの防止と真正性の確保を同時に実現する技術はないため、両者を組み合わせて証明書としての機能を実現する必要がある。また、証明する内容によって、適応可能な技術が限定される場合があるため、内容に合わせた選択が必要となる。技術が進歩してコピーを作られたり、偽造されたりする危険性は常に存在するため、常に新しい技術が適応可能なように入れ替え可能な設計にしておく必要がある。また、

真正性の確認においては、何らかの検証装置・システムが別途必要となるので、検証を行う側によって導入しやすい技術を選択することも重要である。

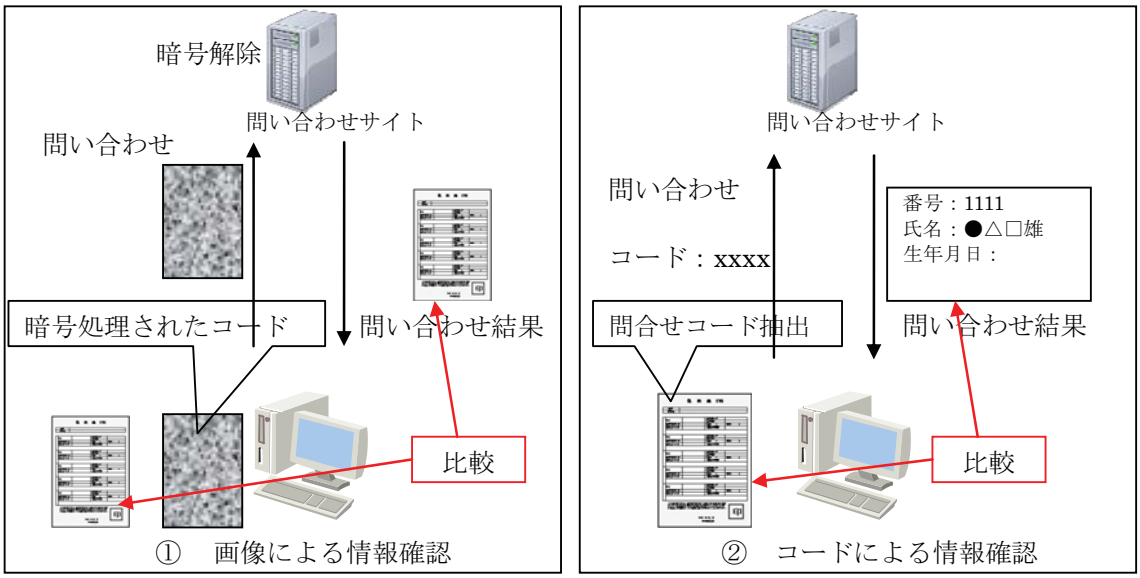


図 4-3 オンラインでの画像情報確認と内容確認

(2) 情報表示の閲覧時のプライバシー配慮

キオスク端末は、自治体の施設内やコンビニ等第三者が立ち入ることのできる場所に設置される。そのため、個人情報を表示する際には利用者以外の第三者に表示された情報を覗き見されないような配慮が必要となる。

① 物理的対策

考慮すべき対策としては、以下の対策が挙げられる

(i) 設置場所

キオスク端末を操作する利用者の後ろに、第三者が入りこみにくい場所に設置すべきである。コンビニの場合には、キオスク端末の後ろに商品を置けないスペースに設置する、あるいは後ろに商品棚を置かない、入り口近くに設置しないなどの対策が必要となる。また、第三者が端末に近づいてきたことを利用者にわかりやすくさせる対策も必要となる。簡単な方法としては、後ろを確認できる鏡を設置するなどの方法がある。

（ii）画面の設定

キオスク端末を操作する画面が覗き込まれる可能性を減らすために、表示画面を傾けて操作者以外には見難くする、覗き見防止のフィルタを画面の表面に付ける（但し、タッチパネルとの共存が難しくなる恐れがある）、画面に覗き見が難しいように枠を付けるなどの対策を考慮する必要がある。

（iii）印刷紙の横取り防止

近づいた第三者が横から印刷された情報を持ち去る可能性も否定できない。証明書や参照情報が印刷された紙が操作者以外の第三者によって取り難いような構造とすることを考慮する必要がある。

物理的対策の中には利便性やユーザビリティと反する対策も存在するので、利用者の許容限度と安全性の面で評価する必要がある。

② 技術的対策

物理的な対策を施していたとしても、長時間表示していると覗き見られる可能性は高くなる。技術的な対策としては、利用者が意識しなくとも表示時間を極力短くする対策を考慮する必要がある。

（i）表示レベルの変化

長時間表示している場合に、徐々に表示の明るさを減らしてフェードアウトする（表示部分を暗く）、一定時間後は情報を表示する前の画面やメニューに戻る、あるいは再表示と遷移画面を選択するダイアログを表示させるなどの方法によって、長時間同じ情報が表示されるのを防ぐことができる。

（ii）表示の禁止

表示すべき情報が多い場合には、端末を占有する時間も長くなるので、覗き見られる可能性も高くなる。表示が何画面にも渡る場合には、画面の表示を禁止し、紙への出力だけに限定する方法もある。

(3) 端末内の個人情報取り扱い

キオスク端末は、自治体の施設内やコンビニ等第三者が立ち入ることのできる場所に設置される。電子行政サービス等から送られた情報は、一時的にキオスク端末内部のハードディスクやメモリ上に保持されているので、端末がハッキングや盗難に遭った場合に個人情報が漏洩しないための対策が必要となる。

① 一時情報の上書き消去

一時的なファイルを上書きによって消去する方法による対策である。パソコンなどでも商品が出始めているが、多機能プリンタでもオプションで内部データ消去の機能を実現するモデルが出ている。個人情報を含む情報を一時的に内部ファイルとして保存した場合に、ファイルを出力（表示・印刷）した後には規定された方法に従って上書き消去する。

② ハードディスク等保存装置の暗号化

一時的なファイルを保持するハードディスク等の保存装置全体を暗号化する方法である。ハードディスクが持ち出されたとしても、内容を判別することは難しくなる。

③ データ暗号化

ハードディスク全体ではなく、一時ファイルのみ暗号化しておく方法である。

④ 揮発性メモリだけへの個人情報の展開

一時的なファイルを電源供給が止まると内容が失われるメモリ上に保存する方法である。電源が落とされた場合には、確実に消去されることと、一般にはハードディスク等の不揮発性メモリよりも少ない容量しか搭載されないため、メモリ上から削除した場合に上書きされる頻度が高くなる。更に、暗号化等の技術を組み合わせる方法もある。

(4) 電子行政サービスへの接続に関する安全性

接続の構成によっては、キオスク端末もインターネットに直接接続する可能性もある。その場合、機器自体が安全に動作するための保護、接続される電子行政サービス等からの機器の確認が必要となる。

① 機器の保護

接続されたキオスク端末は、インターネットからの攻撃の脅威にさらされるので、そのため以下のような一般的な保護対策を導入する必要がある。

- ウィルス対策
- ファイアウォール
- オペレーティングシステムの更新　　等

② 機器の確認（機器認証）

接続サーバは、個別の機器を確認することにより安全な端末からのアクセスを保障する必要がある。一方で、ネットワークに接続されたプリンタには、プリントする情報を暗号化するために機器が保持する PKI の秘密鍵と証明書によって SSL のサーバ機能を持った製品も出てきている。機器を特定するための認証基盤ができてキオスク端末に設定できれば、各端末で生成した鍵ペアに対して公開鍵証明書を発行して識別することが可能となる。

キオスク端末を識別するために機器が PKI の秘密鍵と証明書を保持する技術的な仕組みは存在するので、構築コスト、接続サーバ及びキオスク端末の安全性に対するリスク、利用者の利便性等を総合的に検討して導入を検討する必要がある。

4.1.4 ユーザビリティに関する課題及び対策

4.1.2 で述べたように、キオスク端末ではパソコンと比較して表示画面が小さい、入力手段が限定されている等の制約事項がある。また、多数の人が利用する可能性のあるキオスク端末を長時間に渡って占有するのには問題がある。本項では、ユーザビリティの視点から課題の抽出とその対策について述べる。

(1) 限定的な表示機能・入力機能を持った場合のユーザビリティ機能

キオスク端末は、表示画面の大きさ（物理的な表示デバイスの大きさ及び表示できる画面の大きさ）、入力デバイス（タッチパネルとテンキー）に制限があるため、その条件の下で、利用者がストレスなく利用できる機能を持つ必要がある。

① 表示における制限

表示画面の大きさは、小さい場合には 800x600 画素程度となる。多くの情報を表示する場合には、1 画面に収まらずにスクロールが必要になる。しかし、タッチパネルによる位置の指定はパソコンのマウスなどのポインティングデバイスに比較すると細かい位置の指定を伴う操作が難しい場合が多い。そのため、タッチパネルを用いる場合には、スクロールバーを用いたスクロールを極力避ける必要がある。

画面は表示されるページ単位で区切る。表示する情報が多くて 1 画面に収まらず複数ページに渡る場合には、ページ移動のボタンの表示によるページ切り替えか、タブによるページ切り替えによって表示が切り替わるなど、スクロールしなくとも情報が全て表示でき

る画面設計にする必要がある（図 4-4)。

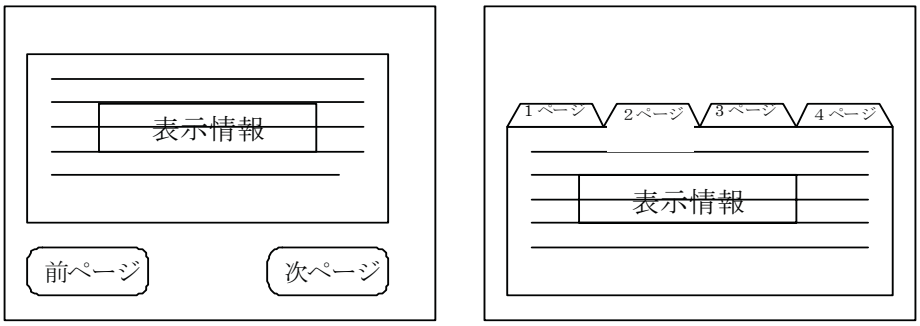


図 4-4　スクロールを避けるユーザインタフェース

また、プルダウンメニューについても、スクロールが伴う可能性があるので、避けるべきである。選択項目を全て表示した上で指定項目を選択するようなインタフェースを用いる必要がある。

キオスク端末からアクセスするコンテンツは、予め用意されたメニュー画面から選択するのが一般的であるため、一般のホームページ等にアクセスする必要はない。限定された電子行政サービス等や民間サービスで利用できれば十分と考えられるので、上記に従ったキオスク端末向けの画面によって各サービスが提供されることが望ましい。

② 入力における制限

テンキー以外の入力は、ソフトキーボードになる。なるべく文字の入力を避けたインタフェースとする必要がある。利用者を識別するユーザIDはICカードから読み出すことが望ましい。利用者の基本情報や属性情報が予めICカードや電子行政サービス等に登録可能で、活用できる可能性があるのであれば、それらの情報を入力情報に活用することによって、必要な入力を最低限にすることが可能である。東京電子自治体共同運営サービスから利用することのできる東京都渋谷区の電子申請の例では、電子申請が可能な 18 種類のサービスのうち、本人情報以外は項目の選択によって文字入力が必要のないサービスが 5 種類、予め個人の属性情報として登録した子ども、パートナー（配偶者)、介護保険関連基本情報などが利用できれば文字入

力が不要となるサービスが７種類ある。[1]

以上の理由により、キオスク端末では多くの文字入力が必要となる電子行政サービス等での利用を避けるか、本項 (2) で示す方法など別の手段によって文字入力することを考慮すべきである。

(2) 紙を用いたユーザインタフェースのユーザビリティ

情報機器に慣れていない人でも、これまでと同様に紙による申請であれば、問題が生じる可能性は低い。しかし、行政の電子化では電子行政システムは電子化して行政の業務効率を上げる必要があるので、なるべく電子的な方法で申請を受け付けられたほうがよい。相容れない課題を解決する方法の１つとして、パーソナライズした申請書を用いる方法がある。以下に実現の手順を示す（図 4-5)。

[1] http://www.e-tokyo.lg.jp を通じての平成 22 年 2 月時点での調査結果による(付録 D 表 D-1 参照)。

① 申請者が特定の申請を選択すると、行政システムは申請者の基本情報と申請書類を識別するための識別番号を付与した申請書を作成する。

② キオスク端末では、その申請書を印刷して出力する。

③ 利用者は追加すべき部分の情報を紙に記入する。

④ 利用者は、記入した申請書（及び添付書類）をキオスク端末でスキャンすることで、申請を行う。

⑤ 電子行政サービス等は、スキャンした画像情報によって申請を受け入れる。画像内から申請の識別番号を読み出して該当する申請者の基本情報を取得し、申請に応じたサービスを提供する。

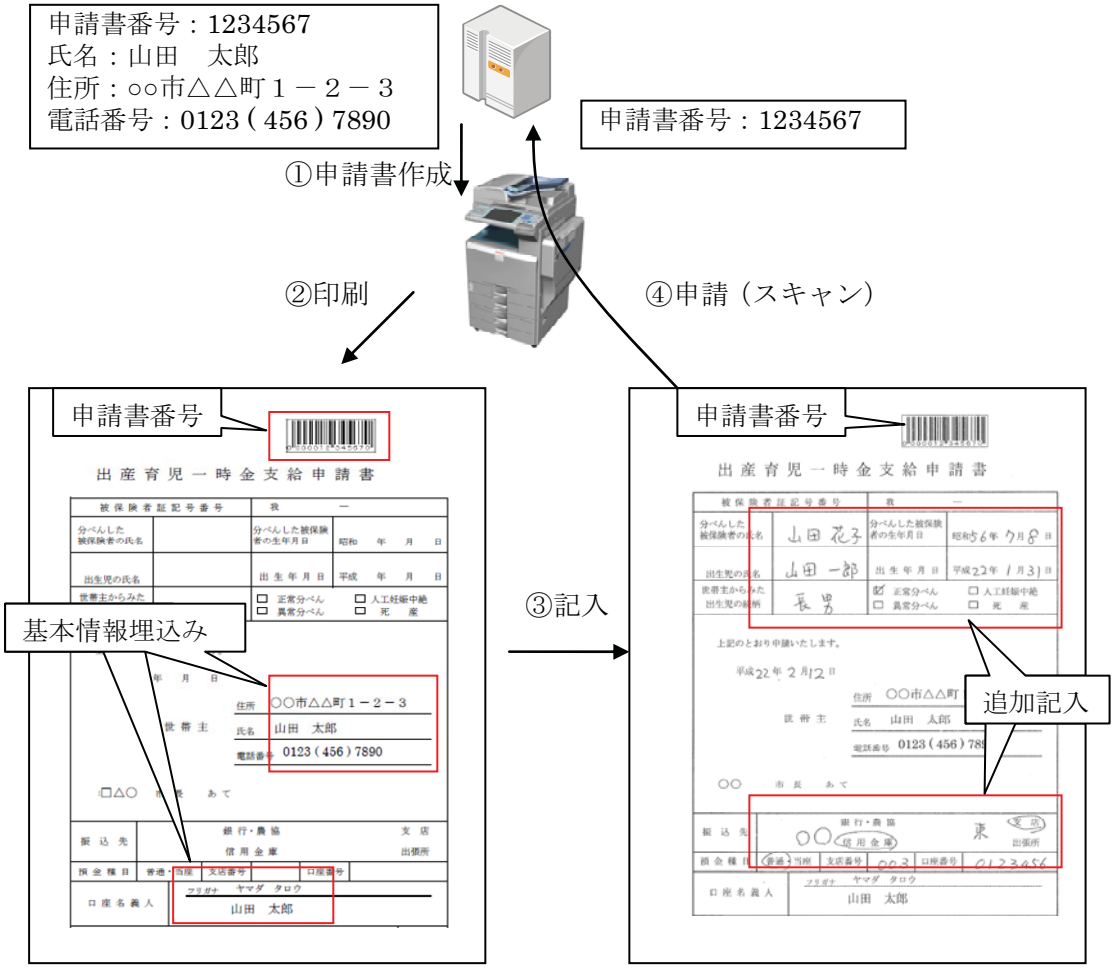


図 4-5　紙を用いた電子的申請

以上の方法を取ると、

- 電子行政サービス等では基本情報は電子的に保持できるので、追加記入部分のみの情報を電子化すればよい
- 利用者は慣れた紙に記入して申請ができる
- 申請書に記入する間、端末は利用者が占有する必要はないので、他の人が端末を利用できる
- 申請書が手元に残るので、後で利用者が申請内容を確認がしやすい

などの効果が期待できる。

(3) 端末を長時間占有せずに情報アクセス利用するための方法

第三者が立ち入ることのできる場所に設置されたキオスク端末を長時間に渡って一人の利用者が占有することは、個人の情報が覗き見られる可能性が高くなる、他の利用者の利用の妨げになるなどの観点から好ましくない。長時間の占有を防ぐには、以下の点に配慮する必要がある。

① 入力における対策

対象となる電子行政サービス等が簡単に見つけられるように配慮する必要がある。わかりやすいカテゴリに分類して選択できるようにする、選択のサブメニューなどに入る際には、その深さが視覚的にわかるようにすることも重要である。

なるべく短い操作で目的の情報にたどりつくように配慮することが必要である。たとえば、個人あるいは利用者全体の統計的な情報からよく利用される電子行政サービス等を選択しやすく表示するなどはその例である。

提供されるサービス全体にわたって統一的な手順で操作ができるように工夫して、利用者が戸惑わないための配慮が必要である。たとえば、入力を確認するための画面の設置、必ず１つ前の画面に戻れるようにする、操作ミスのエラーの表示、入力の不足を示して入力を促す場合の提示方法などが統一されていれば、初めてサービスを利用する場合であっても、これまでに経験しているサービスでの操作を応用することによって利用者が戸惑うことなく利用することが可能となる。

(2) で示したように、入力が必要な場合に予めICカードや電子行政サービス等に登録されている個人の属性情報を活用して埋め込んで

表示するなども効果的である。但し個人の情報の保護との兼ね合いで、属性情報の登録と利用範囲に対する同意を取るなどの配慮も必要である。

② 表示・出力における対策

なるべく長時間の表示を避けるように、例えば同じ画面を長時間表示している場合には警告を与える等、短時間で利用を終えるよう促す表示を行うなど、表示側を工夫する対策が必要となる。画面の変化によって、利用者が画面を変更する気付きを与えることとなり、画面あたりの表示時間を減らす効果が期待できる。4.1.3（2）②の場合と同様、１情報あたりの表示時間を短くすることで、全体としての端末の占有時間を短縮することが可能となる。

(4) 個人の状況に合わせたインタフェース提供によるユーザビリティ向上

公共の場におかれたキオスク端末は、障がい者あるいは高齢者等が利用することも想定する必要がある。その場合、画一的なユーザインタフェースでは提供される電子行政サービス等を十分に利用できない可能性がある。近年の動向として、個人の特性に合わせてユーザインタフェースを提供するという方法が提案されている。

- 端末使用時に利用者が必要とするアシスト機能、例えばディスプレイの文字を大きくすることや白黒反転やガイド用の音量を大きくする等の情報（好ましい設定及び避けるべき設定）をカード内に記録しておく。
- 利用時にカードが端末に挿入されると、端末はアプリケーション処理の始めに、利用者が必要とするアシスト情報を読み取る。
- 端末は、これらのカード情報から端末が持っている機能を使用して、その人に必要なユーザインタフェースを実現する。

カード等の媒体への記録方法としては、日本提案の国際標準[1]として審議が進んでおり、国内はもとより国際間でも相互に利用できる統一的なアシスト情報の内容及び形式として制定される予定である。主な設定可能な情報は以下の通りである。

[1] ISO/IEC CD 12905 Integrated circuit cards — Enhanced Terminal Accessibility using cardholder preference interface

- 追加のタイムアウト時間
- タッチパネルスクリーンの利用（ボタンの大きさ「大」あるいは「特大」）
- 表示するソフトキーボードの種類設定
- 音声入力（文字単位、単語単位、自然言語）
- 入力位置の高さ
- 表示スクリーンの高さ及び角度
- 表示画面のテキスト及び背景の表示色（好む色、避ける色）
- 表示テキストの大きさ
- 点字表示の有無
- アイコン（コントラストを上げる、あるいはテキストの併記）
- 警告をあたえる画面の種類（全体、アクティブウィンドウ、タイトルバー）
- 画面の部分拡大の有無と倍率
- 音声によるガイドの場合の音量
- 表示画面の音声読み上げ機能の利用
- 表示言語

これらを可能な限り端末側でサポートすることで、2.2.4(2)の高齢者や障がい者等への配慮で示した要件に対応した対策を部分的に実現できるので、利用者にとって使いやすい利用環境を構築する１つの方法となる。

(5) 人による補助

IT 機器に慣れていない人の場合には、これまでにあげた補助手段を適応したとしてもキオスク端末を十分に使いこなせない場合も想定される。その場合には、コールセンターで対応する、あるいは補助員を配置するなどの対策も考慮すべきである。

4.2 実機検証

4.1 で検討した対策の実現性を検討するに当たっては、キオスク端末からの電子行政サービス等への接続性、ユーザビリティなどの検証が重要となる。そのため、検討した対策の一部は実際の検証環境にて検証する。本節では、検証環境について説明し、引き続いて検証項目とその結果について述べる。

4.2.1 検証環境

検証のために準備した環境は、以下の通りである。

(1) キオスク端末の構成

現在コンビニ等に設置されているキオスク端末は、以下の 2 種類に大別することができる。

① パソコンをベースとしたキオスク端末

多くのキオスク端末が採用している構成で、内部にパソコン相当の機能を持ち、表示画面がタッチパネルの入力を供えている。金融系のカードやICカードを利用する際の暗証番号等を入力するために、数字を入力するためのテンキーが別途用意されているのが一般的である。自治体が設置した証明書等の自動交付機は証明書を印刷するためのプリンタを内蔵しているが、その他の場合には、レシートを印刷するためのプリンタを持っている場合が多い。典型的なものが、図 2-5 及び図 4-6 である。

（出展：http://www.lawson.co.jp/）

図 4-6 キオスク端末（Loppi）の構成例

② 多機能プリンタをベースとしたキオスク端末

一部のキオスク端末が採用している構成で、多機能プリンタによって端末を構成している。多機能プリンタのオペレーションパネルが表示及び入力デバイスになっているとともに、暗証番号や数字を入力するテンキーを備えているのが一般的である。多機能プリンタには、多機能プリンタ単体で構成するタイプのものと、筐体内に多機能プリンタのコントロールとは別にパソコン相当の機能を内蔵したタイプのものが存在する。前者のタイプは通常のオフィスなどに置かれているほとんどの多機能プリンタで、現在コンビニ等に設置されて証明書交付に用いられているキオスク端末として稼動しているは、後者のタイプである。

パソコンをベースにした場合と多機能プリンタにした場合の機能等の比較を 表 4-1 に示す。

設置される場所や利用されるサービスや環境によって、適切な構成のものが選択される必要がある。本調査研究では、紙を入力に活用する等の多様な可能性を検討するため多機能プリンタをベースとしたキオスク端末によって検証を行う。

表 4-1　パソコンベースと多機能プリンタベースの場合の機能の違い

項目	パソコンベース	多機能プリンタベース
OS	Windows 等	Windows/Unix 等組み込み型 OS（パソコン組み込み型は＋Windows）
CPU	最新のものが利用可能である可能性あり	一般にパソコンより設計から製品化されるまでの期間が長いため最新のものを利用するのは難しい
メモリ	パソコンとほぼ同じ	制限あり
表示	15 インチ程度のモニタがつけられている場合が大部分	プリンタの操作パネル（10-12 インチ程度）
入力	モニタ上のタッチパネル及び暗証番号等の入力のためのテンキー	モニタ（操作パネル）上のタッチパネル及び暗証番号等の入力のためのテンキー
プリンタ	USB 等で外付けになる。一体にするためには別途筐体が必要	組み込み
スキャナ	USB 等で外付けになる。入力が必要でない場合は不要	組み込み
汎用パソコンアプリケーション利用	パソコンベースなので可能	OS や環境に依存する。移植が必要な場合もあり、すべてが利用可能ではない。

(2) 多機能プリンタを用いた検証環境

多機能プリンタを用いたキオスク端末の評価環境は 図 4-7 のようになる。既に述べたとおり、多機能プリンタには 2 種類が存在するが、今回の評価環境では、追加のパソコンを持たない多機能プリンタで実現した。多機能プリンタ内で実現できない機能は、外部に設置したアクセスサーバによって追加する。実際の利用を考えると、アクセスサーバは複数の多機能プリンタを制御可能であるため、たとえばコンビニ事業者内

に 1 台設置して運用するなどの構成も想定できる。パソコン搭載の多機能プリンタを用いるのか、今回の検証環境のようにアクセスサーバを介した接続になるのかは、全体のパフォーマンス、コスト等を考慮する必要がある。

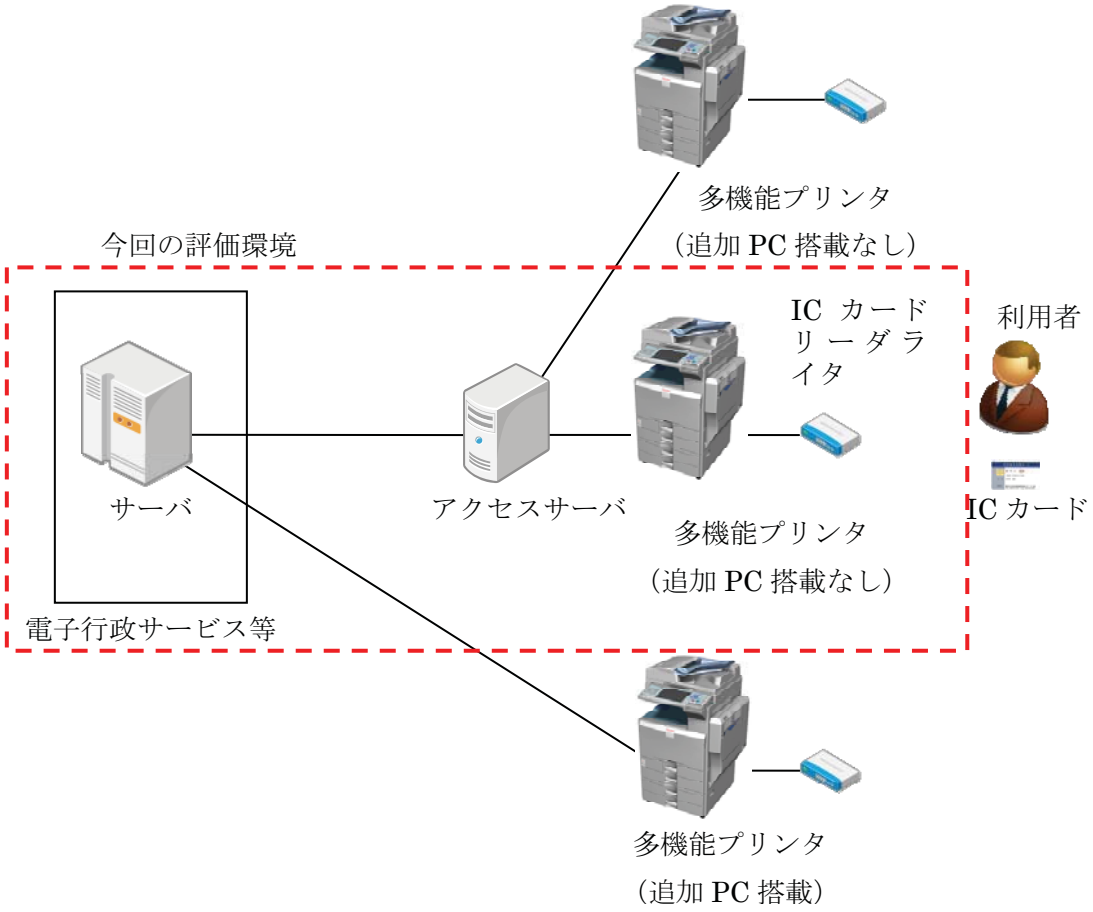


図 4-7　多機能プリンタを用いた検証環境

図 4-7 に基づいた検証環境を構成するそれぞれの構成要素の概略を 表 4-2 に示す。

表 4-2　検証環境の構成

構成要素	説明	備考
電子行政サービス等	PC/AT 互換サーバ （日立 Flora370W）	Windows XP Apache Tomcat:5.0.23 DB(PostgreSQL):8.1 JAVA: J2SDK1.4.2_11
インターネット等	LAN にて代用する	
多機能プリンタ	多機能プリンタ MPC 4500	ブラウザ Type B カードアクセスライブラリ 周辺機器接続用 USB ボード
アクセスサーバ	PC/AT 互換サーバ （Lenovo ThinkCentre S50）	Windows XP Apache:4.03 JAVA: J2SDK1.4.0 1
IC カードリーダライタ	ISO/IEC 14443 Type B 準拠のカードに対応したもの （デンソーウェーブ PR-400UDMM）	
IC カード	ISO/IEC 14443 Type B 準拠のカード （NTT コミュニケーションズ社 eLWIZE）	認証基盤を利用するための PKI アプリケーション（Security Keeper）搭載

各構成要素は以下の機能を持っている

① 電子行政サービス等

- 利用者毎の情報を保持
  年金及び特定検診相当の個人情報を XML にて保持
  利用者毎の暗号鍵で暗号化
- 利用者識別、及び認証
- アクセスサーバに対して表示・印刷情報の提供
- アクセスサーバを通じてスキャンした情報の保持

② アクセスサーバ

- 多機能プリンタ制御
- 電子行政サービス等との接続（情報の入出力）
- 利用者毎の暗号鍵で暗号化・復号
- 認証（IC カード制御）制御
- セキュリティコード解析

③ 多機能プリンタ

- 表示：操作パネル
- ユーザインタフェース、：操作パネル上のタッチパネル及びテンキー
- IC カード入出力
- 印刷（出力）
- スキャン（入力）

4.2.2 検証項目の抽出

検証環境において、4.1 で挙げた課題と対策の実現性について以下の検証を行う。

(1) システム機能に関する検証

システム機能に関する検証においては、4.1.2 で挙げた機能のうち、電子行政サービス等への接続及び認証基盤の利用について検証する。

① 電子行政サービス等への接続に関する検証

電子行政サービス等への接続に際しては、複数のサービスとの接続が前提となる。電子行政サービス等の提供方法は明確になっていないが、本調査研究においては、標準的な接続手段と標準的な記述様式で接続することを前提に、接続には Web サービスを用い、提供する情報の記述を XML で行うこととした（付録 E 参照）。これは、e-Tax の利用者向けのメッセージの配信、特定検診情報の提供など、XML を前提として既に稼動あるいは計画されているサービスを参考とした。複数の情報（年金の情報と特定検診情報）を用意し、認証、情報の選択後出力を行うまでの一連の流れを検証する情報参照に関しては、電子行政サービス等から受け取った情報を想定した書式に従って出力することを確認することとした。情報の種類に応じてスタイルシートを合わせることによって出力イメージに変換したのちに出力することとした。

検証項目 1：電子行政サービス等への接続

汎用的なインタフェース、汎用的なデータフォーマットでの電子行政サービス等アクセスを確認するとともに、現在サービスが始まっている方式との比較検討を行う。

② 認証基盤の利用に関する検証

利用者の認証及び暗号化された個人情報の復号、アップロードする個人情報の暗号化に PKI を用いることで認証基盤の利用を確認することとした。検証環境で用いた多機能プリンタは Windows 環境ではないため、提供された PKI を利用するカードアクセスソフトウェアがプリンタ内で利用できない条件での検証となった。そのため、アクセスサーバ側で IC カードにアクセスする部分を多機能プリンタの IC カードを呼び出す形で実現することとした。

検証項目 2：認証基盤利用

IC カードを利用する PKI インフラにて個人の認証や暗号化を行う機能を確認するとともに、実現における課題を明らかにする。

(2) セキュリティに関する検証

セキュリティに関する検証においては、システム機能に関する検証においては、4.1.3 で挙げた機能のうち、証明書の交付に関連する安全性確保、閲覧時のプライバシー確保及び端末内の個人情報取り扱いについて検証する。

① 情報閲覧時のプライバシー確保及び端末を長時間占有せずに情報アクセス利用するための方法に関する検証

検証環境においては、筐体を含む物理的なハードウェアの変更は行わない範囲で検証を行うものとした。閲覧時の表示を制限する機能として、表示画面に収まらないと判断する情報に関しては、印刷のみを許可するという形での実現を行う。

検証項目 3：閲覧時のプライバシー確保及び端末の長時間占有を防止するための方法

情報の表示と印刷を組み合わせることにより、覗き見から個人情報の漏えいを防止可能であることと、表示時間が短くなるため、端末の占有時間を短縮することが可能となることを検証する。

② 端末内の個人情報取り扱いに関する検証

今回の試験環境においては、電子行政サービス等から送られるデー

タは全て個人毎の暗号鍵で暗号化するとともに、復号したデータはハードディスクには保存せず揮発性メモリ上にのみ保持し、出力後はメモリ上から消去するという方法で対応した。プリンタ内に一時的に保持される印刷用及びスキャン後の画像データに関しては、処理後の上書きによって消去し、全体として個人情報の保護に対する機能を確認するものとする。

検証項目 4：端末内の個人情報保護

端末内に個人情報がアクセス可能な生の状態で残留しないで利用可能であることを検証する。

(3) ユーザビリティに関する検証

ユーザビリティに関する検証においては､4.1.4 で挙げた機能のうち、限定的な表示機能・入力機能を持った場合のユーザビリティについて検証する。検証環境においては、暗証番号の入力以外は、タッチパネル上のボタンによる操作だけで基本動作が行えることを前提に画面を設計し、十分な情報提供が行えることを確認する。

検証項目 5：限定的な表示によるユーザビリティ確保

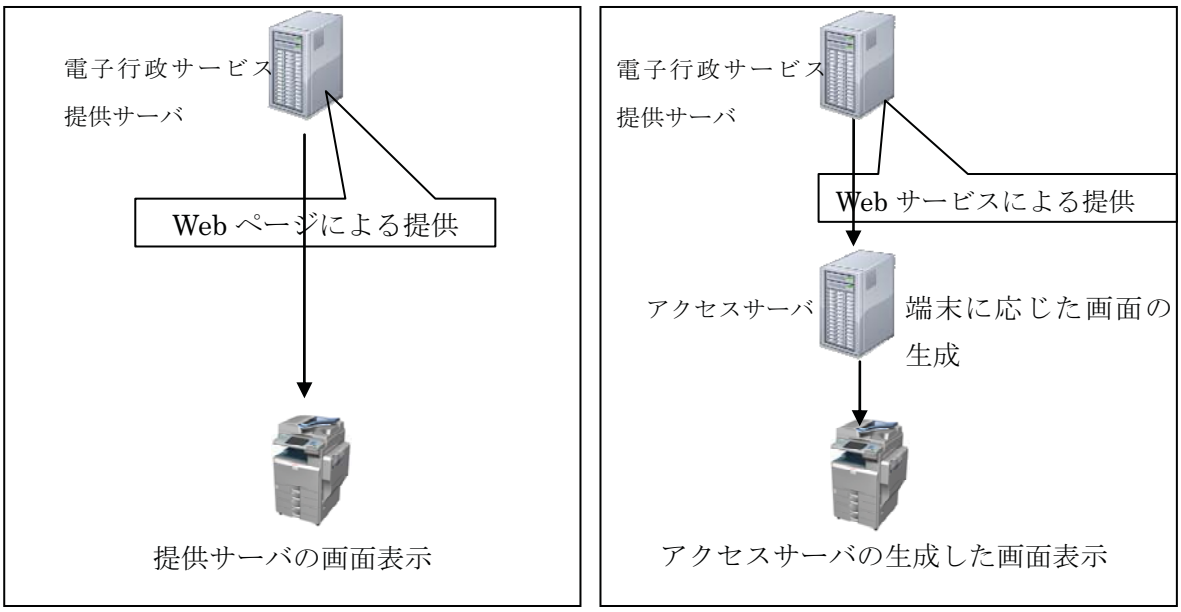
大きさの制限された表示機能及びタッチパネルによる入力という限定されたユーザインタフェースを利用し、利用者認証から情報利用までの画面遷移で情報提供可能できることを検証する。

4.2.3 検証結果

4.2.2 で挙げた検証項目の検証環境における検証結果を示す。

(1) 検証項目 1：電子行政サービス等への接続に関する検証結果

電子行政サービス等とキオスク端末を接続する汎用的なインタフェースとして、Web サービスとして実現した。またやり取りする情報については、XML にて記述することで汎用性を確保した(付録 E 参照)。表示及び印刷に関しては、XML とスタイルシートを組み合わせる方法で実現可能性を確認した。データ本体は XML で送り、表示あるいは印刷に必要な書式の情報をスタイルシートの形で別に取り扱うことで対応した。印刷時には印刷に最適となるスタイルシートを合わせることによって印刷イメージに変換したのちに出力することとした。ただし、今回利用した多機能プリンタは、簡単な表形式であれば問題なく出力できたが、複雑な表現を取る組み合わせの場合には内部のメモリリソースが不足して出力が難しかった。実証実験に当たっては十分なリソースを持ったハードウェアを利用する必要がある。



① Web ページによる提供　　② Web サービスによる提供

図 4-8　キオスク端末と電子行政サービス等の接続

電子行政サービス等とキオスク端末の接続方式としては、図 4-8①に示すように、電子行政サービス等側でユーザインタフェースを含めた画面を生成しキオスク端末ではその画面を表示するだけで実現する方法と、図 4-8②に示すように中間のアクセスサーバと電子行政サービス等はWebサービスで接続し、ユーザインタフェースは端末の機能に合わせてアクセスサーバが生成し、キオスク端末ではアクセスサーバが生成した画面を表示することによって実現する方法が考えられる。

表 4-3　接続方式の比較

方式	メリット	デメリット
Web ページによる提供	・キオスク端末やデジタルテレビ等端末の種類毎のユーザインタフェースを統一するのは容易	・個々の端末の機能や利用者に合わせた細かなインタフェースの調整は難しい
Web サービスによる提供	・端末の特性やユーザのニーズに合わせた細かなインタフェースの調整ができる（2.2.4(2)参照）	・ユーザインタフェースの統一するためにはガイドライン等が別途必要 ・端末側あるいは中間に入るアクセスサーバに負荷がかかる

提供側で端末の条件に合ったアクセス方式を提供する方式か、今回検証したように、端末と電子行政サービス等の中間で端末の特性や利用者の要件に合わせたインタフェースを提供する方式のどちらかを選択する必要がある。

(2) 検証項目 2：認証基盤利用に関する検証結果

検証環境で用いた多機能プリンタは Windows 環境ではないため、提供された PKI 利用のカードアクセスソフトウェアが利用できない条件での検証となった。そのため、アクセスサーバ側に新規のカードアクセスモジュールを用意するとともに多機能プリンタ側にそのモジュールからの要求を受けてカードの入出力を行う機能を追加して実現可能であることを確認した。但し、アクセスサーバと多機能プリンタの通信上に利用者のパスワードやカードへのコマンドなどが流れることになるので、別途安全性を確保する対策が必要となる。本来であればパスワードは多機能プリンタ内で処理をしてカードにアクセスできるほうがパスワードの漏洩の危険性を減らすことができるので、将来的にはカードへのアクセス制御は全て端末側で行われることが望ましい。

公的個人認証サービスの場合には、利用するカードアクセスソフト

ウェアのアプリケーションインタフェース仕様は公開されているが[1]、独自仕様になっているカードアプリケーションの仕様は公開されていない。キオスク端末に限らず、デジタルテレビなど組み込み系OSの環境でこのような基盤を利用する場合には、それぞれの環境で動作する独自のカードアクセスソフトウェアが提供される必要がある。多くの環境に対応したカードアクセスソフトウェアを提供するのが難しいのであれば、カードアプリケーションの仕様を公開し、それぞれの環境で動作する独自のモジュールを各メーカーが開発可能とする必要がある。

HPKI 等の場合には、国際標準に準拠した PKI カードアプリケーションとなっている。将来的には国際標準に準拠したカードアプリケーションも想定し、カード提供者あるいは認証サービス事業者に依存しない共通の認証の仕組みも利用可能にして開発の負担を減らすとともに、複数の PKI インフラを利用する際のカードアクセスソフトウェアの競合等の問題を避ける方法も検討する必要がある。

(3) 検証項目 3：閲覧時のプライバシー確保及び端末を長時間占有せずに情報アクセス利用するための方法に関する検証結果

情報の選択までは画面で行い、出力は表示せずに印刷することにより覗き見できないことを確認した。表示によって何ページにもわたる情報をその場でページを送りながら確認しなくとも済むため、印刷された出力を受け取ることで端末の利用時間が短縮される可能性があることを確認した[2]。但し、将来の実施に当たっては、事前に利用者に出力枚数を通知するなど、利用者の不安を取り除くことが好ましい。印刷にかかるコストの負担方法も課題となる。また、出力された紙の横取り防止などの物理的な対策が別途必要となる。

印刷によって出力する場合には、プリンタのハードウェア上のトラブルによって紙詰まりを起こした場合の対応をどのようにするかも検討の必要がある。知識のある利用者であれば、詰まった紙を取り除いて復旧することが可能であるが、プリンタの機種ごとに復旧方法は異なるので、トラブルに遭遇した利用者が戸惑わないような対応を検討する必要がある。出力された個人情報の保護に注意を払いつつ補助員による援助を行うなど、運用を含めて対策を検討する必要がある。

---

[1] (財)自治体衛星機構のホームページ（http://www.lascom.or.jp/jinfo/software.html）にて公開されている

[2]印刷で 1 ページに収まる情報でも、画面に表示すると複数ページにわたる場合がある。その場合にはページを送りながら閲覧することになるので、それぞれのページを閲覧した時間の和が全体の閲覧時間となる。例えば、1 ページの情報が 3 画面に展開された場合、1 ページを印刷するのに必要な時間が今回の検証環境では約 5 秒であったが、1 画面あたり 3 秒の閲覧時間を必要とすると少なくとも全体を閲覧するのに 9 秒必要となる。

(4) 検証項目 4：端末内の個人情報保護に関する検証結果

今回の試験環境においては、電子行政サービス等から送られるデータは全て個人毎の暗号鍵で暗号化するとともに、復号したデータはハードディスクには保存せず揮発性メモリ上にのみ保持し、出力後はメモリ上から消去するという方法で対応した。プリンタ内の画像データに関しては、上書きによって消去した。以上の対策により個人情報が認識できる状態で残留していないことを確認した。一連の印刷処理においてもっとも処理時間を要したのは、印刷画像へのコードの埋め込みであり、上書きによる消去は印刷の空き時間などに実行可能であり、利用者への影響は回避できる。

プリンタ内のハードディスクに保存された一時データの消去に関しては、各社がオプションで提供しているが、情報の消去のタイミングに関しては、統一されているものではない。上記空き時間に消去するもの、利用後直ちに消去するもの、次回の起動時に消去するものなど様々であるので、端末の運用も含めて考慮する必要がある。

(5) 検証項目 5：限定的な表示によるユーザビリティ確保に関する検証結果

大きさの制限された表示機能及びタッチパネルによる入力という限定されたユーザインタフェースを利用し、利用者認証から情報利用までの画面遷移で情報提供可能であることを確認した。

- サービス選択（電子行政サービス等、真正性検証）
- ユーザ認証（PIN 入力）
- 対象情報サービス選択（情報取得、情報登録）
- 情報選択（一覧からの選択）

同じページを表示モニタの大きさが異なる端末で利用した場合には、表示画面の小さな端末では表示が想定よりも小さくなる可能性があるので、画面の設計においては、表示する可能性のある最も小さな画面サイズを意識して画面設計をする必要がある。

現状の画面の大きさでは、メニューに出す項目、提供する情報の数が少ないために大きな影響を感じなかったが、今後利用できるサービスが増え、メニューや利用可能な情報が増えた場合には、影響が出る可能性がある。実際の普及時期を想定すると、ハードウェアの価格低下も期待できるため、画面表示に関しては画面の大きさ（例えば 10 インチ以上）及び画素数 XGA(1024x768)を最低限度の要件として定めるとともに、実際に表示される文字の実寸等も含めてガイドライン等を作成することを検討する必要がある。

入力方法に関しては、金融機関の ATM や乗車券の自動販売機、公共

端末でタッチパネル方式がようやく普及してきている状況である。最近携帯電話や携帯端末で普及してきているマルチタッチ等の新しい入力技術を導入するためには、社会的な導入状況も考慮して判断する必要がある。

4.2.4 まとめ

本項では、今回行った実機での検証結果のまとめと考察、キオスク端末を前提とした場合の電子行政サービス等の課題に関する考察を行う。

(1) キオスク端末に対する検証結果のまとめと考察

① システム機能に関する検証結果について

本調査研究では、4.1.2 で挙げた課題のうち、電子行政サービス等への接続に関する検証、認証基盤の利用に関する検証を行った。

電子行政サービス等を模したサーバへのアクセスによって、基本的なネットワーク接続と Web サービスによる組み合わせで接続を確認し、多機能プリンタをベースにしたキオスク端末が接続可能であることを確認にした。今回の検証の中では、機器内のリソースの問題が発生したが、十分なメモリ等を追加する等対応した構成にすれば問題は解決すると考えられる。但し、キオスク端末を導入すると一定期間は導入した端末が使い続けられるため、電子行政サービス等と接続するための仕様は長期にわたって利用可能にすることと、最低限の端末仕様を明確にして、その中でも行政サービスが確実に提供できるようにする必要がある。サービスの提供が開始された後は、仕様が変更されることによって既存の端末が利用できなくなることは避けなければならないので、仕様の変更をする場合には、端末のライフサイクルを考慮して十分な猶予期間を設ける等の考慮が必要である。

実際に情報保有機関から利用者の個人情報を参照する場合、利用する端末がキオスク端末だけでなく家庭のパソコンであっても参照した情報を手元で印刷するニーズが出てくるものと予想されるので、電子行政サービス等として表示だけでなく印刷に適した情報提供を行うことも検討の余地がある。

認証基盤の利用に関しては、PKI をベースにした認証基盤を利用可能であることを確認した。しかし、カードのアクセスソフトウェアが利用できない環境が存在することが明らかになったので、個人認証基盤を用いる場合には対応したソフトウェアの提供を求めるか、仕様の公開を求める、必要がある。

本調査研究の検証では、申請に関する検証、実際の公的個人認証基

盤の利用等は行っていないので、引き続き検討及び検証が必要である。

② セキュリティに関する検証結果について

本調査研究では、4.1.3 で挙げた課題のうち、閲覧時のプライバシー保護及び端末内の個人情報取り扱いに関する検証を行った。

プライバシー保護に関しては、提示した技術的な対応で十分であるかを利用者の観点で評価する必要がある。そのため、利用者の意見を求めるなど、社会的な検証が必要となる。キオスク端末においては、高齢者や障がい者に対する対応も重要である。そのため、高齢者や障がい者が利用した場合を想定し、全体の運用の中でプライバシー保護に対して十分配慮がなされているかについては、引き続き検討及び検証が必要である。

今回検証を行わなかった、筐体の変更を伴う評価、画面の表示を変化させることによって利用者に気付きを与える方法、接続する機器の識別と認証についても、引き続き検討及び検証が必要である。

③ ユーザビリティに関する検証結果について

本調査研究では、4.1.4 で挙げた課題のうち、限定的な表示機能・入力機能を持った場合のユーザビリティに関する検証を行った。今回の検証は、限定された種類・数のサービス（コンテンツ）での検証に限定されているため、問題は発生しなかったが、サービスが増えた場合に問題が生じないかどうかを検証する必要がある。

キオスク端末の場合には、一般の Web ページに自由にアクセスするというのではなく、あくまで用意されたメニューの中からサービスを選択して利用するという形になると考えられる。しかし、マウスや通常のキーボードが接続されていない環境であるため、文字入力に様々な入力に対する制限を設けた上でのサービス提供が必要となる。サービス共通となるユーザインタフェース等サービス提供についてのガイドラインを作成する等の方法によって一定の基準を作成し、それに従ったサービス提供をする必要がある。

キオスク端末においては、デジタルデバイドとなる高齢者や障がい者に対する対応も重要である。そのため、利用者が使いやすいユーザインタフェースの実現については技術的な検証を行う必要がある。また、実際のユーザの意見を求めるなど、社会的な検証も必要となる。

本調査研究で検証できなかった、申請における紙を用いたインタフェースの検証は、電子申請の対象を広げる可能性もあるので、引き

続き検討及び検証が必要である。

(2) 電子行政サービス等の課題に関する考察

電子行政サービス等の提供の方法が定まっていないが、以下の点に注意すべきである。

① アクセス多様化を目指した場合の課題

キオスク端末に限らず､デジタルテレビや携帯電話等様々なアクセス手段が想定されているが、利用される端末によって、表示能力や操作性が異なることを指摘した。利用者の立場から見ると、どの端末を用いても同じサービスが利用できることが理想であるデジタルテレビ、キオスク端末、携帯電話などの大まかな端末のグループ毎に端末の機能には共通項があると考えられるので、その中での基本的な仕様を合わせることと、それに合わせてサービスが提供される必要がある。端末に依存する機能の切り分けを電子行政サービス等側で行うのか、中継するポータルサイトあるいはすべて端末側（含アクセスサーバ）側で行うのかは課題として検討する必要がある。

サービスによらず共通の利用を実現するためには､サービスによらず共通な部分となる情報の提供方法や画面設計、ユーザインタフェース等、それぞれの端末種別に応じたガイドラインの作成も必要である。

② 情報参照

情報の提供の方法として､利用者が要求してオンラインで情報を取得するPULL型の情報参照と、申請結果のように、電子行政サービス等側でPUSHされる情報を参照する場合の2つのケースが考えられる。また、キオスク端末の場合には表示と印刷という2種類の提示方法があることは既に述べた。単純な表などの情報の場合には問題がないが、複雑な表示である場合には表示に適した画面と、印刷に適した画面を別々に生成する必要がある。情報参照の場合には、キオスク端末だけではなく家庭のパソコンからの参照などでも同様に印刷の可能性がある。印刷に適した情報提示を行政情報システム側で行うのか、あるいは中継するアクセスサーバやポータルサイト側で行うのか、機能の分担を明確にする必要がある。

③ 個人の属性情報利用

申請においては、個人の属性情報が有効であることを述べた。ICカードに個人情報を格納して利用するのか、電子行政サービス等側で利用者の個人情報の管理が可能であるのか、利用者の同意をどのような形で得るのか、利用の範囲をどのように考えるのかなど利便

性を考慮したうえで電子行政サービス等側、利用者側の合意を得て進める必要がある。

④ 外字

証明書においては、氏名、住所等に利用される外字の問題がある。標準的な文字コードにない文字をイメージとして各自治体それぞれが管理・利用しており、現状で全国共通な文字セットやコードが定まっていない。全国的な電子行政サービス等を展開する場合には、必ず問題となるので、標準を定めることが望ましい。

⑤ 認証基盤

PKI 認証基盤において、現在利用可能である公的個人認証基盤は、電子署名の基盤であって、本来は今回想定したオンライン利用の際の電子認証に用いるのにはそぐわない。電子認証の基盤が構築されることが望ましい。

5. 中央サーバに認証機能を一部移行させる方式に関する調査研究

2章で述べた現状を踏まえ、中央サーバに認証機能を一部移行させるための具体的な実現モデルを設定し、モデルの各構成要素に求められる機能を整理する。また、想定した実現モデルに対する課題への対策方法を調査・検討するとともに、実証環境にて実現性の評価を行う。

5.1 課題の抽出及び対策の検討

本節では 2.3 で挙げた検討状況に基づき課題の抽出及び対策の検討を行う。

5.1.1 実現方法のモデル化

本項では課題の抽出及び対策の検討に先立ち、前提とする中央サーバの実現モデルについて検討する。実用化を見据えた検討を行うため、本調査研究では中央サーバ単体ではなくその利用形態も考慮したモデルを想定する。実現モデルを 図 5-1 に示す。

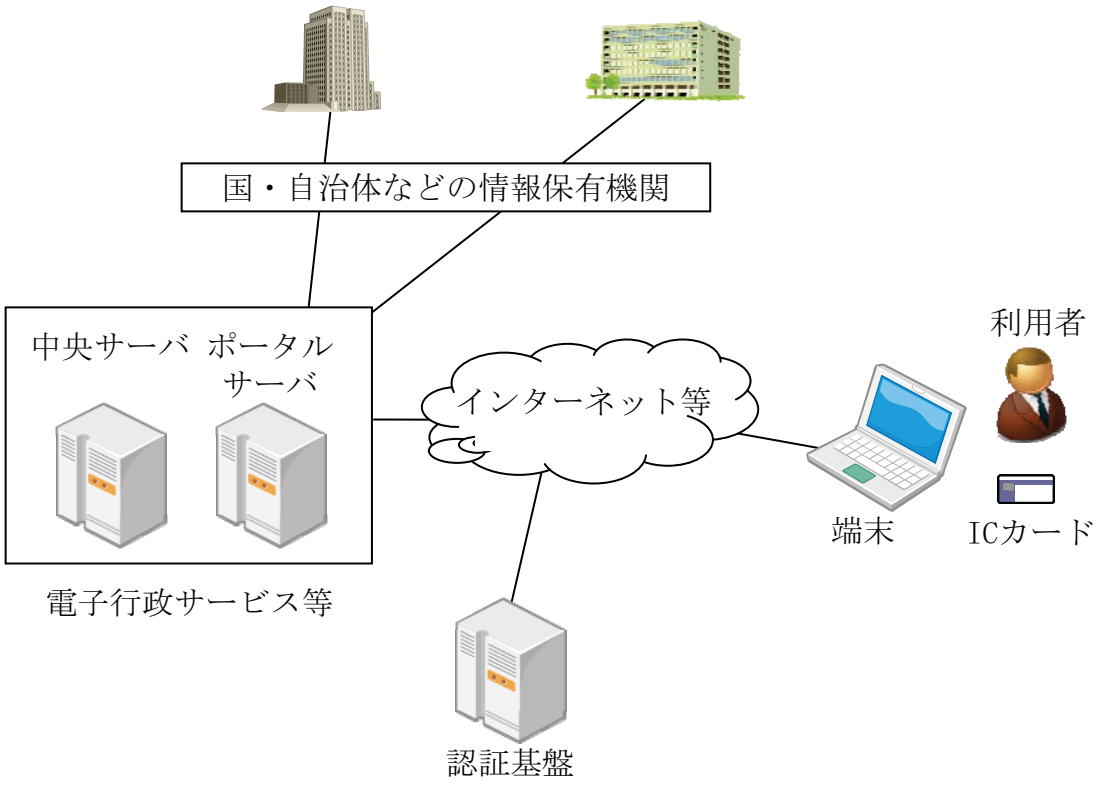


図 5-1 実現モデル

図 5-1 の各構成要素は以下の通りとなる。

(1) 情報保有機関

利用者の情報を保有し、利用者に対して、住民票や印鑑証明書のような証明書の交付サービス、電子的に蓄積された利用者等の情報を提供する情報提供サービス、利用者から行政サービスへの申請を受け付ける申請サービス等を提供する国・自治体の機関等であり、これらの各種サービスを電子行政サービス等を通じて提供する。

(2) 電子行政サービス等

以下に示す「ポータルサーバ」および「中央サーバ」により構成され、国・自治体などの情報保有機関や利用者に対して認証機能や各サービスを提供するためのポータル等の機能を提供する。

(3) ポータルサーバ[1]

国・自治体などの情報保有機関と、利用者が操作する端末を接続する機能を有するシステム。利用者に対するサービスの入口として、中央サーバでの認証に基づき利用可能なサービスメニューをWeb画面等として提供する。

(4) 中央サーバ

利用者からの要求に応じた本人認証の実施や認証状態の管理および、サービスの実行に必要な認証情報の管理や情報保有機関との間での利用者認証の実施等を行うシステム。

(5) 認証基盤

個人を識別、認証するための情報基盤。認証局による電子証明書の発行や失効情報の管理等を行い、電子証明書の有効性の検証を行う。公的個人認証基盤等を想定。

(6) インターネット等

端末と電子行政サービス等を接続するネットワークは、自治体等が設置したLGWAN等のネットワーク、及びインターネット等の公衆網などの可能性がある。

(7) 端末

利用者がサービスへアクセスするために操作する端末。本人認証時にはICカードとの通信も行う。

[1] 「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」(平成20年度総務省委託事業) では実証実験での中央サーバへのアクセスイメージとしてポータル等が記述されており、利用者に対する各種サービスの窓口を担う構成要素として想定されている。

(8) ICカード[1]

利用者が中央サーバにアクセスし、本人確認を行うために用いるデバイス。

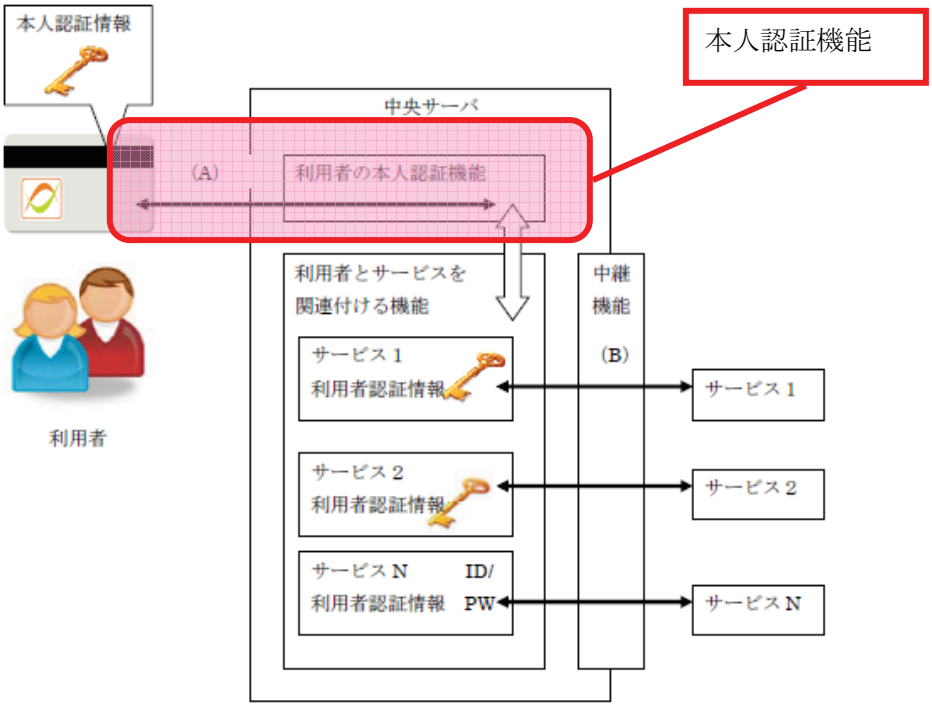
5.1.2 システム機能に関する課題及び対策

本項では 5.1.1 で述べた実現モデルに基づいたシステム機能の検討を行う。

(1) 認証サーバの分離

「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」(平成 20 年度総務省委託事業) には中央サーバの利用イメージとして「利用者は端末とIC カード内の情報等(本人認証鍵等)を用いてネットワーク上の中央サーバにアクセスし、本人確認を行う」と記述されており、中央サーバの機能として本人認証機能が必要であることが示されている。本人認証機能の位置付けを 図 5-2 に示す。

[1] 「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」(平成 20 年度総務省委託事業) では「利用者は端末と IC カード内の情報等(本人認証鍵等)を用いてネットワーク上の中央サーバにアクセスし、本人確認を行う。」としており、利用者側のアクセス手段として IC カードの利用が想定されている。



「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」
（平成 20 年度総務省委託事業）より

図 5-2 本人認証機能の位置付け

本人認証は、個人が利用する電子行政サービス等のシステムでは従来から一般的に実施されているサービスであり、実績のある既存システムが多数存在している。今後「中央サーバに認証機能を一部移行させる方式」を導入するにあたり、本人認証機能を新規で開発・運用することはコスト負担も大きく、実用化を阻害する要因となる可能性もある。このため既存の技術やシステムを活用することでシステム全体の開発・運用コストを軽減することが重要であると考えられる。

そこで本調査研究ではシステム機能の構成の一例として、本人認証を行う「認証サーバ」と耐タンパー相当による情報管理など新規性の高い機能を実現する「サーバ連携型多目的 IC カード」に分離する構成を提案する。本人認証機能は既存システムにおいて、ID/パスワードによる方法や、IC カードを利用した方法および外部認証機関と連携する方法など、複数の方法が従来から提供されている。本人認証を行う既存システムとの連携により、様々な認証方法に対応できる柔軟性の高いシステムを構築することが可能となる。

(2) 耐タンパー装置(HSM)[1]の利用

前述の調査研究報告書では従来の IC カードと同様に耐タンパー相当による情報管理が中央サーバに求められる可能性を示している。

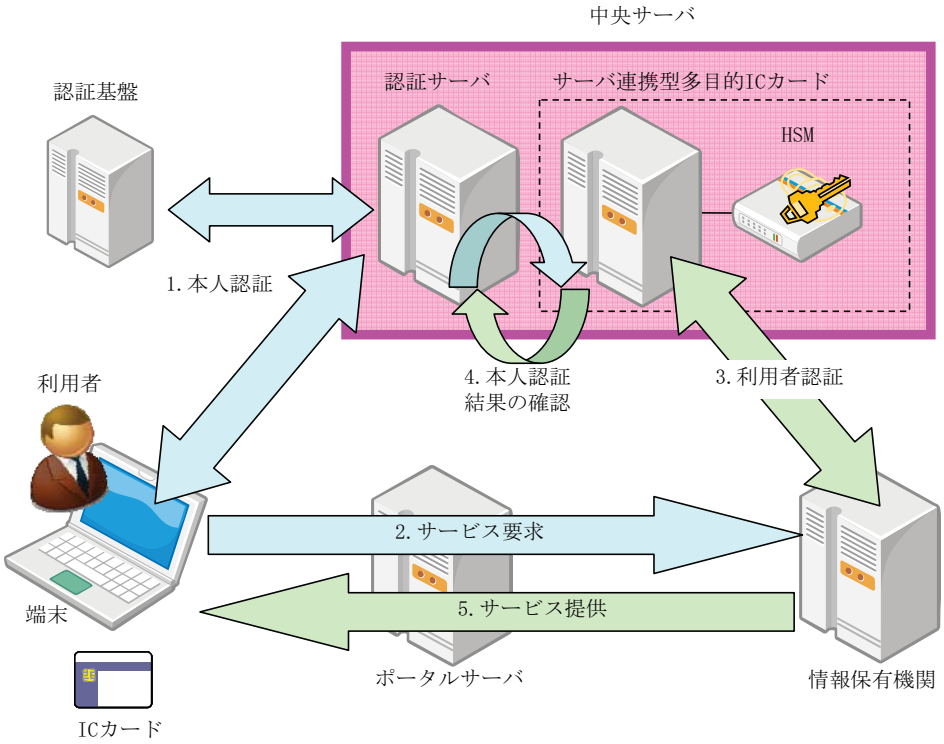
耐タンパー性の実現には大きくハードウェアにより実現する方式と、ソフトウェアにより実現する方式が考えられる。ハードウェアによる方式としてはHSM (Hardware Security Module)、TPM[2] (Trusted Platform Module) などによる方法が知られており、ソフトウェアによる方式としては仮想化技術等による方法が知られている。そこで本調査研究ではシステム機能の構成の一例として、HSMを利用した方式 (「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」(平成 20 年度総務省委託事業) において「5.1.1 耐タンパー性相当を必要とする情報の取扱い」として記述されている利用者認証鍵の間接保護 (方法 2) に該当) を前提として検討を行うこととする。

(3) 実現モデルのシステム構成に基づくサービスフロー

これらを背景として、前述の調査研究報告書で利用者のメリットとして示される「電子行政サービス等の利用における利用者認証は、サービス共通の本人認証を最初に 1 度行うことを原則とし、それ以降、複数のサービスを連続して利用する場合も、サービス毎に複雑な個別の操作を要求されることはなくなる。」という内容について本実現モデルのシステム構成におけるサービスフローを 図 5-3 に示す。

1 非正規な手段による機密データの読取を防止する機能。「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」(平成 20 年度総務省委託事業)「参考資料 1：耐タンパー性」参照

2 ハードウェア耐タンパー性をもつセキュリティチップ。利用者端末であるパソコンなどのマザーボードに取付けられているのが一般的である。TPM の仕様は TCG (= Trusted Computing Group)という国際的な業界団体で策定されている。



1. 利用者は認証サーバに対して本人認証を実施
2. 利用者はポータルサーバを介して希望するサービスを要求
3. 情報保有機関はサーバ連携型多目的 IC カードに対して利用者認証を要求
4. サーバ連携型多目的 IC カードは本人認証結果を確認し利用者認証を制御
5. 情報保有機関は認証結果に応じて利用者にサービスを提供

図 5-3 実現モデルのシステム構成に基づくサービスフロー

(4) 実現モデルのシステム構成に基づく検討の進め方

以降では、上記で検討した実現モデルのシステム構成に基づき 2.3.2 (1) で述べた「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」(平成 20 年度総務省委託事業) で示される要求事項について検討を行う。

上記報告書では中央サーバへの 7 つの要求事項として以下が示されている。

- サービスの内容

- セキュリティ
- スケーラビリティ
- 利用者インタフェース
- 運用性・可用性
- サービス提供者インタフェース
- 認証の最適化

上記要求事項についてそれぞれ以下のように検討を行う。

5.1.3 では、「セキュリティ」、「サービス提供者インタフェース」、「認証の最適化」について検討を行う。

5.1.4 では、「スケーラビリティ」、「運用性・可用性」について検討を行う。

「サービスの内容」および「利用者インタフェース」については具体的なサービスでの検討が必要と考え、本調査研究では、5.2 で電子行政サービス等での基本的なサービスにサーバ連携型多目的ICカードを適用する処理フローを検討し、フィージビリティについて検証を行うこととする。

5.1.3 セキュリティに関する課題及び対策

本項では 2.3.2（1）で挙げた「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）で示される中央サーバへの要求事項のうちセキュリティに関する以下の内容について課題の抽出及び対策の検討を行う。

①セキュリティ

②サービス提供者インタフェース

③認証の最適化

以降ではまずこれらの要求事項を具体化し、それらを実現するために解決すべき課題について整理する。続いて整理された各課題の対策について検討を行う。

課題の抽出及び対策の検討フローを 図 5-4 に示す。

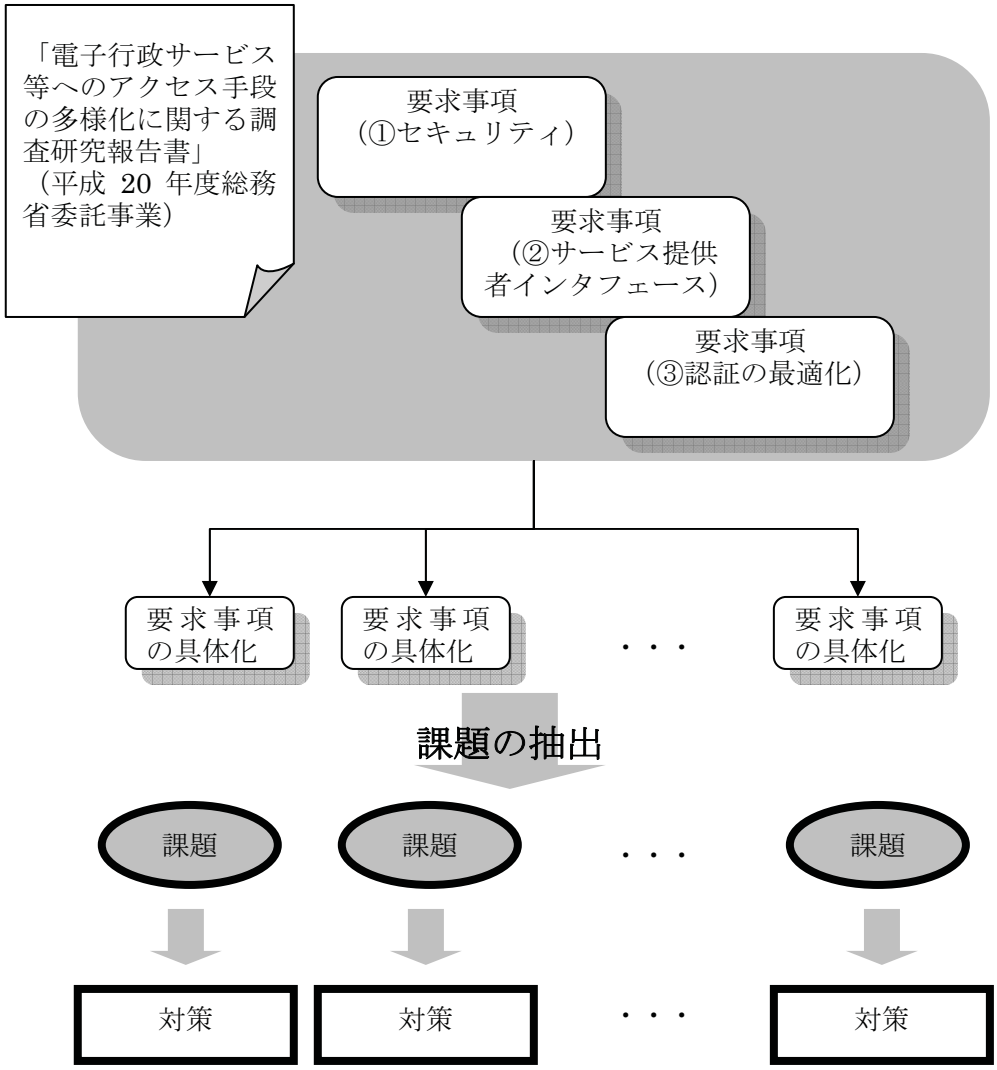


図 5-4 課題の抽出及び対策の検討フロー

(1) 課題の抽出

① セキュリティ

前述の調査研究報告書ではセキュリティに関して以下のように要求事項が示されている。

現在使用されている IC カードを用いた主要なサービスと同等のセキュリティが確保可能であること。IC カード内の情報は暗号等で耐タンパーに保護されていることから、中央サーバに格納される情報も、運用上、同様の保護が要求される可能性もある。

本調査研究では、耐タンパー相当に保護されるべき情報を格納し、それを活用する処理を担うサーバを「耐タンパー相当サーバ(仮称)」と表記する。

上記要求事項に基づき従来の IC カードが有するセキュリティ機能と同等の機能が必要となる。

本調査研究では、前述の要求事項を以下のように具体化することとする。

- [R1-1] 認証情報など機密性の高いデータを耐タンパー相当の領域に格納できること
- [R1-2] 認証情報などの各種データへのアクセスは適切な権限を持つ者以外は実施できないことを保証する機能、手段を有すること
- [R1-3] 本人の認証情報を用いた認証により本人性を確認する機能、手段を有すること

また、従来 IC カードで行われていた認証機能等の一部がサーバ側で実施されることにより、悪意の利用者から自身の実行したサービス結果が否認される可能性を考慮し、以下のように否認防止の要求事項を設定することとする。

- [R1-4] 利用者によるサービス実行結果の否認を防止する機能、手段を有すること

なおこの他、従来 IC カードで実現していた機能の一部をサーバ側へ移行するためサーバに求められる一般的なセキュリティ対策にも留意が必要であるが、各種ファイアウォール製品などにより既知の技術が広く普及していることから、本調査研究ではサーバ連携型多

目的 IC カードの特徴である認証情報の管理に主眼を置いた検討を行うこととする。

次に上記要求事項の実現方法について検討し、要求事項を満たすために解決すべき課題を抽出する。

[R1-1] 認証情報など機密性の高いデータを耐タンパー相当の領域に格納できること

耐タンパー相当の領域としては 5.1.2 (2) に示す通りHSMによる実現方法が考えられる。

これに関して前述の調査研究報告書では HSM を用いた場合の課題として利用者認証鍵を保護しようとした場合のスケーラビリティの確保が示されており、本要求事項を実現するために解決すべき課題と考えられる。

[R1-2] 認証情報などの各種データへのアクセスは適切な権限を持つ者以外は実施できないことを保証する機能、手段を有すること

認証情報など機密性の高い情報の管理を前述の HSM を用いて行う場合、HSM へのアクセス制御が必要となる。利用者の認証情報は基本的に利用者本人のみがアクセスできるような制御が必要であり、管理者であっても任意に HSM へアクセスできないような仕組みが必要となるため「HSM へのアクセス制御方式」が本要求事項を実現するために解決すべき課題と考えられる。

[R1-3] 本人の認証情報を用いた認証により本人性を確認する機能、手段を有すること

本人認証は、従来から一般的に実施されているサービスであり、実績のある既存システムが多数存在している。5.1.2 (1) に示すように、これら既存の技術やシステムを活用することで本人認証を実現しシステム全体の開発・運用コストを軽減することが可能であると考えられる。

[R1-4] 利用者によるサービス実行結果の否認を防止する機能、手段を有すること

一般的にサービスの否認防止対策としては、サービス利用時のメッセージに対して、利用者が所有する鍵を用いてデジタル署名を利用する方法が挙げられる。今回はこれに加え、認証機能等の一部がサーバ側で実施されることに配慮した防止策の検討が必要であるため「認証機能等の一部がサーバ側で実施されることに配慮したサービスの否認防止」が本要求事項を実現するために解決すべき課題と考えられる。

② サービス提供者インタフェース

前述の調査研究報告書ではサービス提供者インタフェースに関して以下のように要求事項が示されている。

サーバ連携型 IC カードシステム(仮称) が提供する認証機能を各サービス提供者の業務アプリケーションサーバが利用可能とする Web サービスなど標準的なインタフェースを有すること。

上記要求事項に加え従来の IC カードを用いた主要なサービスと同等のサービスを提供するため、認証機能以外の機能についても考慮が必要となる。

本調査研究では、前述の要求事項を以下のように具体化することとする。

・[R2-1] 外部システム向けにサービス利用に必要な機能を標準的なインタフェースとして提供すること

次に上記要求事項の実現方法について検討する。

[R2-1] 外部システム向けにサービス利用に必要な機能を標準的なインタフェースとして提供すること

従来の IC カードを用いた主要なサービスと同等のサービスを提供するためサーバ連携型多目的 IC カードには、サービスの利用開始から廃止までのライフサイクルイベントを考慮した上でどのような機能を提供すべきかが課題となる。また、従来の IC カードサービスにおいて課題となっていた、新たなサービスの追加を実現するためのインタフェースについても考慮が必要となるため「標準的なインタ

フェースで提供する機能の種類」が本要求事項を実現するために解決すべき課題と考えられる。

③ 認証の最適化

前述の調査研究報告書では認証の最適化に関して以下のように要求事項が示されている。

本人認証レベルの異なった業務サービスへの仲介を情報の重要性やセキュリティ等を考慮した上で最適化可能であること。

この要求事項は前述の調査研究報告書の中で利用者のメリットとして挙げられる、「電子行政サービス等の利用における利用者認証は、サービス共通の本人認証を最初に 1 度行うことを原則とし、それ以降、複数のサービスを連続して利用する場合も、サービス毎に複雑な個別の操作を要求されることはなくなる。」という内容を実現するためのものと考えられる。

また本人認証レベルとして、PKI 認証や ID／パスワード認証などセキュリティのレベルが異なる複数の認証方式を扱えるようにし、このレベルに応じたアクセス制御が求められる。

本調査研究では、前述の要求事項を以下のように具体化することとする。

- [R3-1] 本人の認証情報を用いた認証により本人性を確認する機能、手段を有すること
- [R3-2] 利用者とサービスを関連付ける機能、手段を有すること
- [R3-3] 各サービスの利用者認証処理を利用者の代理で行う機能、手段を有すること
- [R3-4] 複数の本人認証手段をサポートすること
- [R3-5] 本人認証レベルに応じたアクセスコントロールを行う機能、手段を有すること

認証の最適化に関する要求事項を 図 5-5 に示す。

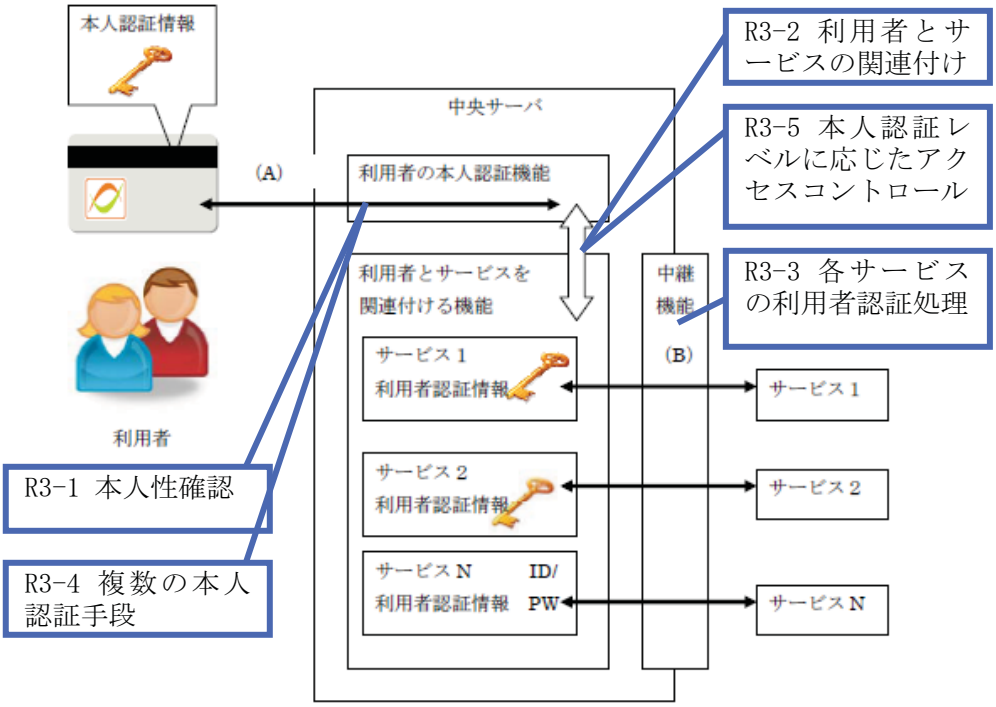


図 5-5 認証の最適化に関する要求事項

次に上記要求事項の実現方法について検討する。

[R3-1] 本人の認証情報を用いた認証により本人性を確認する機能、手段を有すること

本要求事項は 5.1.3 (1) ①に示す通り、既存の技術やシステムを活用することで本人認証を実現しシステム全体の開発・運用コストを軽減することが可能であると考えられる。

[R3-2] 利用者とサービスを関連付ける機能、手段を有すること

利用者とサービスを関連付けるために必要となる識別情報の管理や各システムからアクセスされる際に用いられる本人識別情報等について検討が必要となる。このため「利用者とサービスの関連付けに用いる識別情報の管理」が本要求事項を実現するために解決すべき課題と考えられる。

[R3-3] 各サービスの利用者認証処理を利用者の代理で行う機能、手段を有すること

情報保有機関等から利用者認証の要求を受け付けるような仕組みが必要となる。5.1.3 (1) ②に示す通り情報保有機関等からの要求は当該インタフェースを介して実現される。

[R3-4] 複数の本人認証手段をサポートすること

本要求事項は 5.1.2 (1) に示すように、既存の技術やシステムを活用することでID/パスワードによる方法や、ICカードを利用した方法など既存より利用される複数の方法に対応可能となる。

[R3-5] 本人認証レベルに応じたアクセスコントロールを行う機能、手段を有すること

認証レベルは、サービス毎のセキュリティポリシに依存することが想定されるため、本人認証における認証レベルとこれらの認証レベルを連携させるための対応方法の管理について検討が必要となる。このため「認証レベルの対応管理」が本要求事項を実現するために解決すべき課題と考えられる。

(2) 課題の整理

これまでの内容を踏まえ 表 5-1 に具体化された各要求事項を整理する。またこれら要求事項を実現する上での課題を 表 5-2 に整理する。

表 5-1　要求事項の整理

項番	要求事項
－	セキュリティ
R1-1	認証情報など機密性の高いデータを耐タンパー相当の領域に格納できること
R1-2	認証情報などの各種データへのアクセスは適切な権限を持つ者以外は実施できないことを保証する機能、手段を有すること
R1-3	本人の認証情報を用いた認証により本人性を確認する機能、手段を有すること
R1-4	利用者によるサービス実行結果の否認を防止する機能、手段を有すること
－	サービス提供者インタフェース
R2-1	外部システム向けにサービス利用に必要な機能を標準的なインタフェースとして提供すること
－	認証の最適化
R3-1	本人の認証情報を用いた認証により本人性を確認する機能、手段を有すること
R3-2	利用者とサービスを関連付ける機能、手段を有すること
R3-3	各サービスの利用者認証処理を利用者の代理で行う機能、手段を有すること
R3-4	複数の本人認証手段をサポートすること
R3-5	本人認証レベルに応じたアクセスコントロールを行う機能、手段を有すること

表 5-2　課題の整理

項番	課題	対応 要求事項	内容
－	セキュリティ	－	－
P1-1	HSM を用いて利用者認証鍵を保護しようとした場合のスケーラビリティの確保	R1-1	HSM を用いて利用者認証鍵を保護しようとした場合のスケーラビリティの確保 ※本課題は 5.1.4 に示すスケーラビリティに関する課題と関連するため 5.1.4 (3) ① (i) にて検討する。
P1-2	HSM へのアクセス制御方式	R1-2	HSM で管理する鍵へのアクセス制御に関する実現方法
P1-3	認証機能等の一部がサーバ側で実施されることに配慮したサービスの否認防止	R1-4	認証機能等の一部がサーバ側で実施されることに配慮した防止策
－	サービス提供者インタフェース	－	－
P2-1	標準的なインタフェースで提供する機能の種類	R2-1	サービスの利用開始から廃止までのライフサイクルイベントを考慮した提供すべきインタフェースの種類
－	認証の最適化	－	－
P3-1	利用者とサービスの関連付けに用いる識別情報の管理	R3-2	本人認証を行った利用者とサービス側で管理する利用者との対応に用いる識別情報の管理
P3-2	認証レベルの対応管理	R3-5	各サービスに要求される認証レベルと本人認証レベルの管理、およびこれらの連携

なお、前述の調査報告書ではシステムの実現に向けた今後の取組みとして実証実験による実用性の検証が挙げられているが、「中央サーバに認証機能を一部移行させる方式」の構想については検討が開始されたばかりであり実装手段や方式は十分な検討がなされていない状況である。

そのため本調査研究では、表 5-2 で整理した課題への対策を検討し、その内容も踏まえて今後必要となる実証実験について、6.3 および 6.4 で提案を行うこととする。

(3) 対策の検討

① セキュリティ

(i) HSM へのアクセス制御方式

HSM は製品の有する耐タンパー特性により HSM への物理的な不正アクセスから鍵を保護する。一方で、HSM へのログイン情報の流出等による不正なアプリケーションからのアクセス制御についても考慮が必要となる。一般的に HSM は標準的なアプリケーションインタフェースを有するため HSM へのログイン情報を有する任意のアプリケーションからアクセスが可能となる。このため、特定のアプリケーション以外は HSM へのアクセスを拒否するような仕組みが必要となる。

一例として、セキュア OS の有する強制アクセス制御機能により特定のアプリケーションからのみ HSM へのアクセスを許可するよう制御することができる。強制アクセス制御は OS レベルでアクセス制御を行う仕組みであり全てのユーザやプロセスに対してアクセス制御が可能となる。これにより不正なアプリケーションによる HSM へのアクセスは行えなくなる。

上記により HSM による物理的な鍵保護に加えセキュア OS による HSM へのアクセス制御を併用することでセキュリティの確保が可能となる。

本方式による実現方法を 図 5-6 に示す。

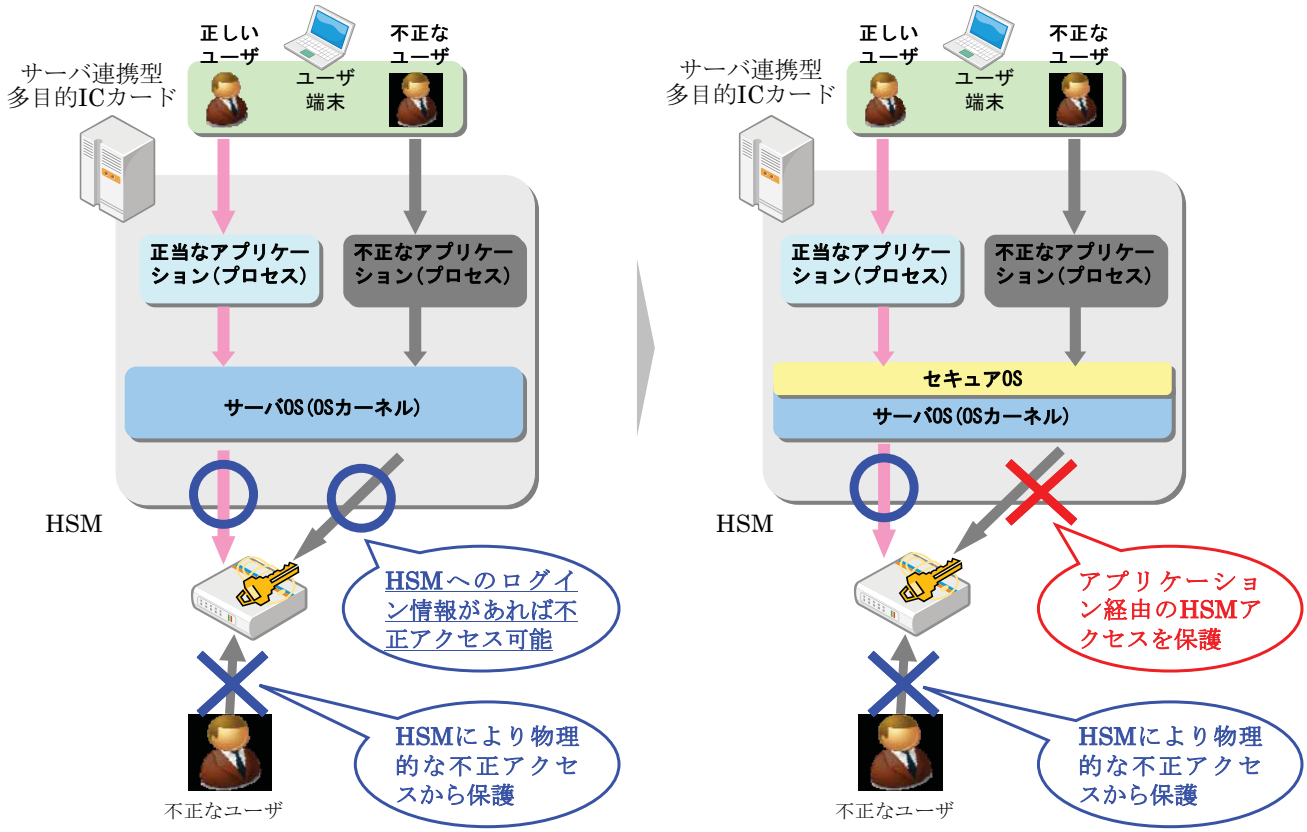


図 5-6 セキュア OS によるアクセス制御方法

上記については、5.2 にてセキュアOSの設定によりHSMへのアクセス制御が可能であることを実機を用いて検証することとする。

（ii）認証機能等の一部がサーバ側で実施されることに配慮したサービスの否認防止

前述したように、サービスの否認防止対策としては利用者の所有する鍵を用いたデジタル署名を利用する方法が考えられるが、認証機能等の一部がサーバ側で実施されることを考慮するとこれだけでは十分ではないと考えられる。一例としてこれに加え、サーバ連携型多目的 IC カードへのアクセス履歴を管理しこれを検証可能とすることで、サービスの否認防止に活用することができる。

サーバ連携型多目的 IC カードでは認証情報等をサーバ側で管理するため、これらが利用者により使用されたことをシステムのアクセス履歴として残すことでサービスの利用証跡としサービスの否認防止に活用する。なおアクセス履歴としては最低限「どのリソースに」、「いつ」、「誰が」、「どこから」、「どのようにアクセスしたか」といった情報が必要となる。

またアクセス履歴は、利用者に対し自身の情報へのアクセス履歴を参照できるようにするとともに、適切な権限を有する第三者がアクセス履歴を参照できるようにすることで、サービスの利用有無を客観的に検証できるような仕組みが必要である。

一方これらのアクセス履歴は証跡として安全な管理が求められる。具体的な管理方法としてはログの暗号化や電子署名、外部媒体や外部サーバでのログ管理および管理者権限の分割によるログファイルへのアクセス制御等により情報の改ざんを防止し信頼性を確保することが可能である。

② サービス提供者インタフェース

（i）標準的なインタフェースで提供する機能の種類

サーバ連携型多目的 IC カードで必要となる処理としては、アカウント開設やアカウント閉鎖などサービスに依存しないシステム共通的なものと、サービスの利用登録、サービス利用といったサービス内容に依存するものに分類されるがサービス提供者インタフェースとしてサービス提供者に提供すべき機能は後者となる。

従来のICカードサービスを考慮した場合、表 5-3 に示すような機能が最低限必要となる。

表 5-3 サービス提供者に提供すべき機能の例

項番	機能	説明
1	サービス利用開始	新規サービス利用に伴うサービス情報の登録(サービスで利用する認証情報、業務データの登録含む)
2	サービス利用停止	サービスの利用規約違反等に伴う一時的な利用停止
3	サービス利用再開	サービス利用停止後のサービス利用再開
4	サービス削除	サービスの利用終了に伴う永続的な利用停止
5	サービス変更	認証情報や業務データの変更/更新に伴うサービス情報の変更
6	利用者認証	サービスで提供する利用者の認証処理
7	サービス利用	署名/暗号処理など各業務で提供するサービスのために必要となる処理

なおこれらの機能は基本的にネットワークを介してアクセスされることが想定されるため、開発言語やプラットフォームへの依存性が低く一般的にも広く利用される SOAP や REST 等の Web インタフェースとして提供することで利用システム側へのコスト負荷を軽減できる。

またサービス提供者が上記インタフェースを利用することで、利用者は新たなサービスの追加利用が可能となる。

利用者は端末のブラウザ等によりサービス提供者が提供するサービス利用開始用の画面にアクセスし必要事項等を入力すると、前述のインタフェースによりサーバ連携型多目的 IC カードへ利用者の認証鍵等が登録され、新たなサービスが利用可能となる。

サービス利用開始のフローを 図 5-7 に示す。

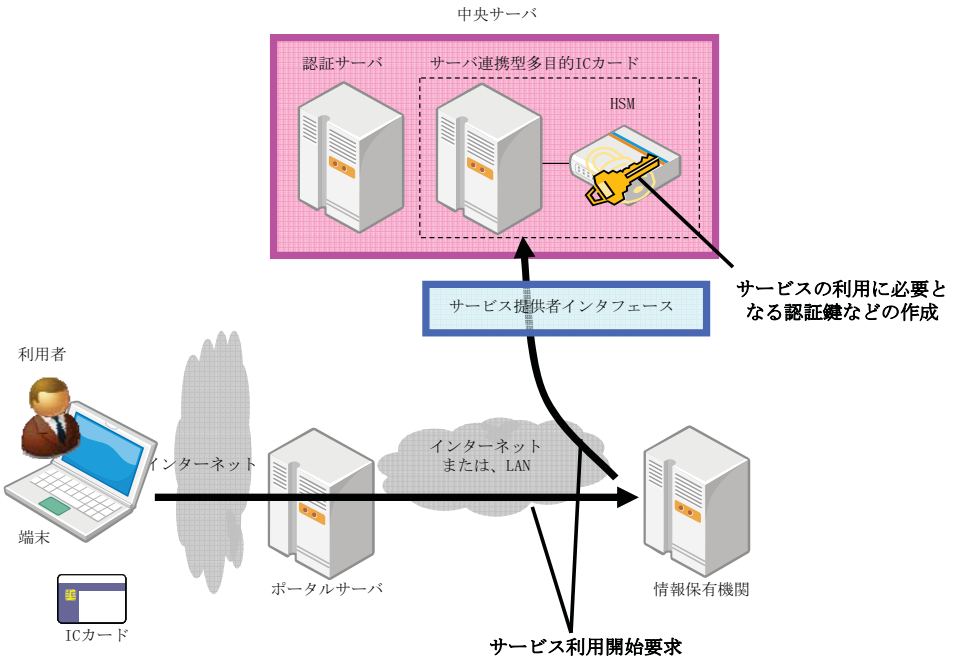


図 5-7 サービス利用開始フロー

上記については、5.2 にて前述のインタフェースにより利用者が新たなサービスを追加利用できることを実機を用いて検証することとする。

なお、利用者によるサービスの利用開始に先立ち、サービス提供者は認証情報等の生成や実際のサービス利用に伴う処理を行う従来 IC カード内に搭載していたアプリケーションに相当するモジュールをサーバ連携型多目的 IC カードに登録する必要がある。また、サーバ連携型多目的 IC カードはサービス提供者インタフェースを介してこれらのモジュールを実行するような仕組みが必要となる。

③ 認証の最適化

(i) 利用者とサービスの関連付けに用いる識別情報の管理

サーバ連携型多目的ICカードは各情報保有機関から 5.1.3 (3) ②に示すインタフェースを介して各サービスの認証要求を受け付け、本人の代理として認証処理を行うような方法が想定される。

各サービス提供者における利用者の管理は各サービス毎の ID 体系

で行われるものと考えられ、情報保有機関からのアクセスには各サービスで管理されるこれらの ID を利用できるようにすることが望ましいと思われる。このためにはサーバ連携型多目的 IC カードではこれらサービス毎に管理される ID により利用者とサービスの連携を可能とする必要がある。

また、これと合わせてサービス固有の ID を規定する等により、情報保有機関からのアクセス時にサービスの種類を一意に特定できるようにする必要がある。

なお各サービスで管理される ID は各サービス事業者のセキュリティポリシにより他システムへの ID の流通が制限されるケースも考えられるため、個人が特定できないような匿名性のある ID に既存 ID を置き換えて利用するようなケースにも留意すべきと考えられる。

ID対応管理によるサービス連携方法を 図 5-8 に示す。

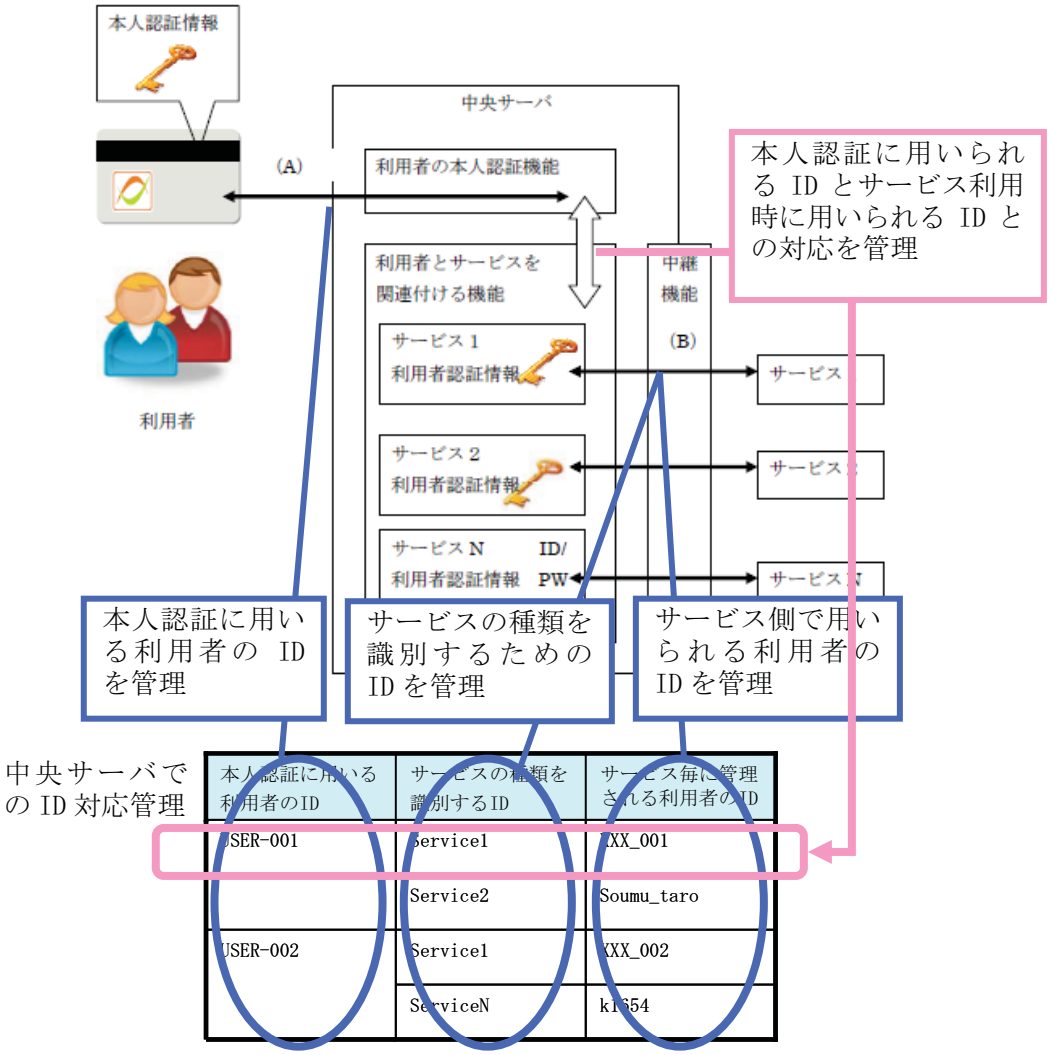


図 5-8 ID 対応管理によるサービス連携方法

（ii）認証レベルの対応管理

認証レベルは、情報保有機関が提供するサービス毎に設定されるセキュリティポリシに依存することが想定される。このため、一例としてサーバ連携型多目的 IC カードでサービス毎に規定される認証レベルを管理することで、サービスの認証に先立ち実施される本人認証の認証レベルに応じてサービスの認証処理の実行可否を制御したり、必要に応じて対応する認証を追加実施することなどが可能となる。

また、認証レベルは IC カード認証や ID／パスワード認証などサーバ連携型多目的 IC カードおよび各サービスの間で共通のレベルを

規定することで、本人認証とサービスの認証の認証レベルを対応付けられるようにする。

各サービスの認証レベルと本人認証レベルの対応管理方法を 図 5-9 に示す。

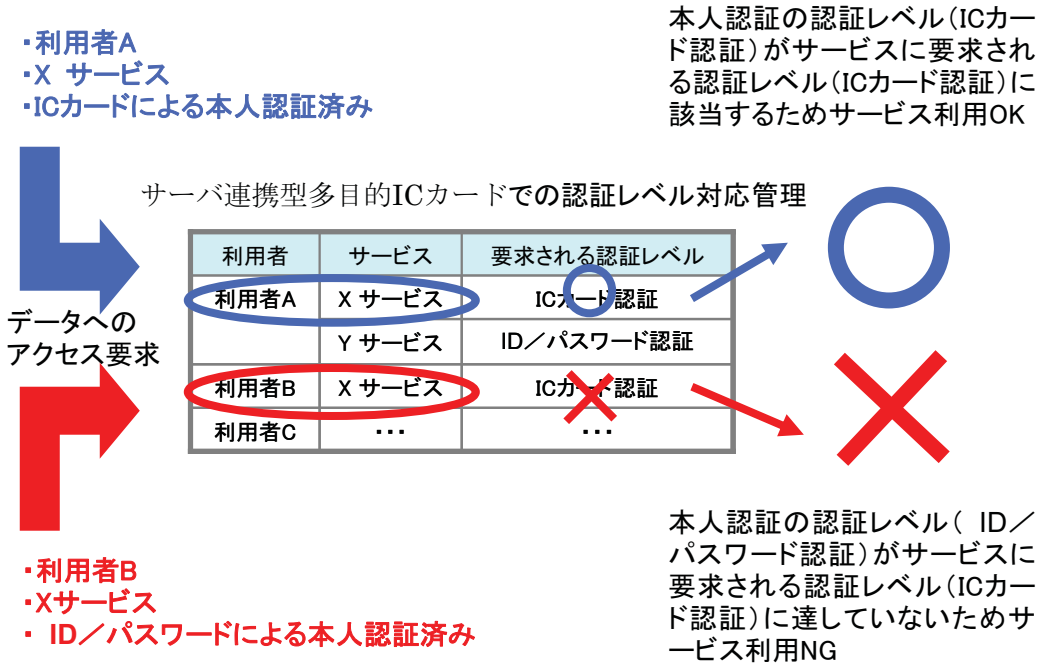
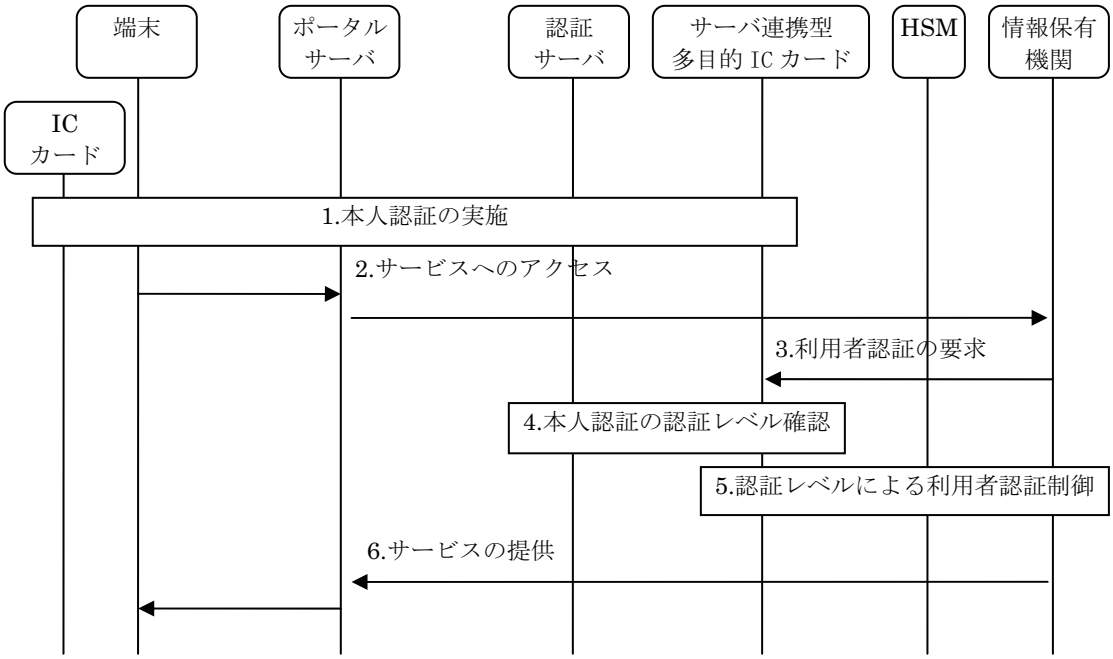


図 5-9 各サービスの認証レベルと本人認証レベルの対応管理方法

上記に示す内容に基づき認証の最適化を実現した場合のサービスフローを 図 5-10 に示す。



1. 本人認証の実施
   利用者は認証サーバへアクセスし本人認証を実施する。認証サーバへのアクセスには認証サーバで個人の識別に使用する本人固有の ID(以下、本人 ID とする)を利用する。また認証サーバでの本人認証処理時にサーバ連携型多目的 IC カードと連携し、サーバ連携型多目的 IC カードを利用する意思確認を行う。

2. サービスへのアクセス
   利用者はサービス利用のため、ポータルサーバを介して情報保有機関へアクセスする。

3. 利用者認証の要求
   情報保有機関はサービスの利用に必要となる利用者の認証をサーバ連携型多目的 IC カードへ要求する。サーバ連携型多目的 IC カードへのアクセスには各サービスで使用される利用者の ID(以下、サービス利用者 ID とする)およびサービスの種類を一意に特定するためのサービス固有の ID(以下、サービス ID)を利用する。

4. 本人認証の認証レベル確認
   サーバ連携型多目的 IC カードは、サービス ID およびサービス利用者 ID から本人 ID を特定し、事前に行われた本人認証の認証レベルを認証サーバと連携し確認する。

5. 認証レベルによる利用者認証制御
   サーバ連携型多目的 IC カードは、本人認証の認証レベルがサービスの要求する認証レベルを満たす場合、本人に代わりサービスの利用者認証処理を情報保有機関との間で行う。本人認証の認証レベルがサービスの要求する認証レベルに達していない場合は利用者の認証処理を拒否する。

6. サービスの提供
   情報保有機関は利用者認証が正常に行われた場合、利用者に対して要求されたサービスを提供する。

図 5-10 認証の最適化を実現した場合のサービスフロー

5.1.4 運用性に関する課題及び対策

本項では 2.3.2（1）で挙げた「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）で示される中央サーバへの要求事項のうち運用性に関する以下の内容について課題の抽出及び対策の検討を行う。

①スケーラビリティ

②運用性・可用性

以降ではまずこれらの要求事項を具体化し、それらを実現するために解決すべき課題について整理する。続いて整理された各課題の対策について検討を行う。

課題の抽出及び対策の検討フローを 図 5-11 に示す。

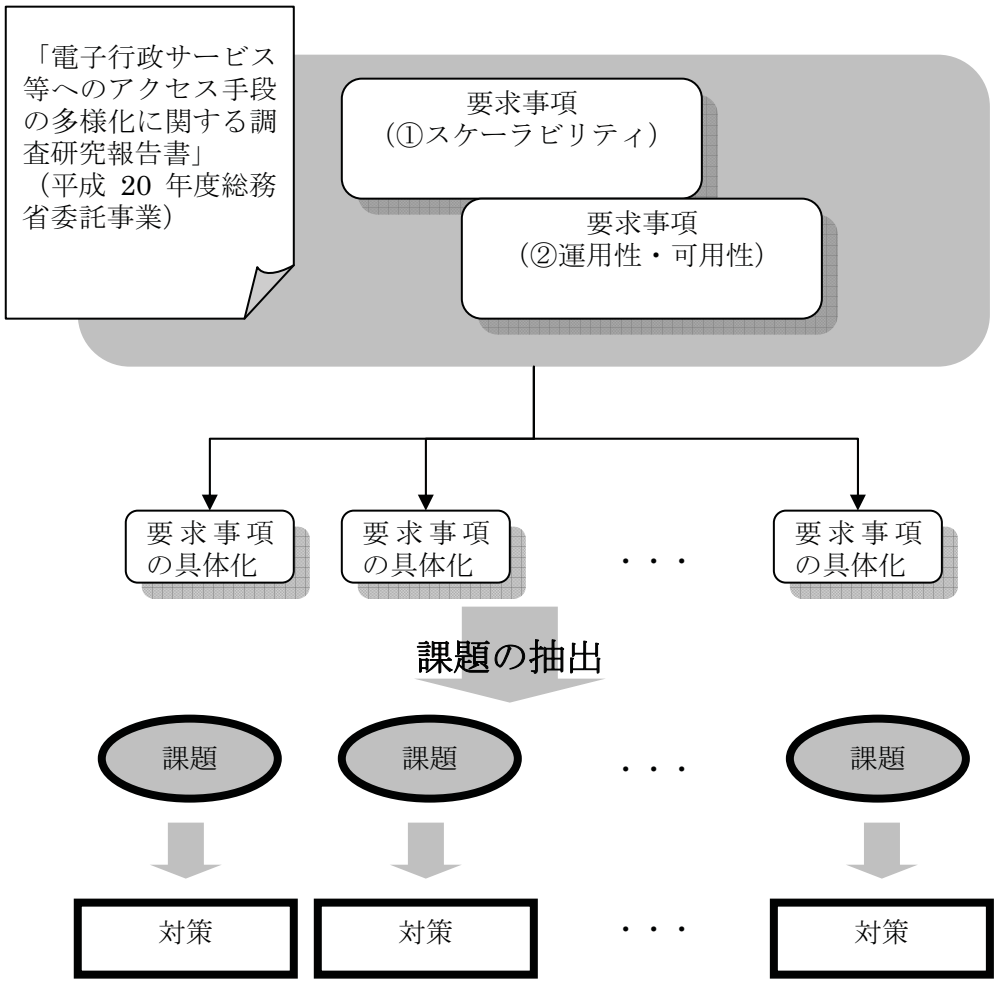


図 5-11 課題の抽出及び対策の検討フロー

(1) 課題の抽出

① スケーラビリティ

前述の調査研究報告書ではスケーラビリティに関して以下のように要求事項が示されている。

現在使用されている IC カードを用いた主要なサービスと同等の規模のサービスを提供可能であること。例えば利用者一人が複数のサービスへの認証鍵を中央サーバに置くとすると、認証鍵数×人口数をサーバに搭載しなければならない。

中央サーバを利用するサービスとして電子行政サービス等を想定した場合、主なエンドユーザは一般市民となるため仮にシステムを自治体など特定の単位に分散して管理したとしても各システムでは相当量のデータ管理が求められる。また、提供するサービスについても段階的にサービス数の増加や範囲の拡大が考えられる。このため、利用者数やサービス数の増加に柔軟に対応できる構成が望まれる。

また､利用者が多数となることを考慮すると大量アクセスに伴うシステム負荷への対策も必要となる。利用者数やサービス数などのサービス規模や通信回線などのサービス環境に応じて処理能力を拡張可能な構成とすることが望まれる。

本調査研究では､前述の要求事項を以下のように具体化することとする。

- ［R4-1］利用者数やサービス数に応じて、認証情報などの管理データの増加に対応可能な構成であること
- ［R4-2］サービスの規模や環境に応じて処理能力が拡張可能な構成であること

次に上記要求事項の実現方法について検討し､要求事項を満たすために解決すべき課題を抽出する。

［R4-1］利用者数やサービス数に応じて、認証情報などの管理データの増加に対応可能な構成であること

前述の調査研究報告書では利用者が増加することで予想される課題として、管理を必要とする利用者認証鍵等の数の増大、全体構成や拠点の整理および認証鍵等の移動が示されている。

利用者認証鍵等の数の増大に関してサーバやデータベース等についてはデータの増加に伴う管理リソースの拡張等に関する既知の技術が広く普及しているが、HSM での鍵管理については製品の特性を踏まえた対策の検討が必要となる。

上記より本要求事項を実現するために解決すべき課題として｢鍵件数増大への対応｣、｢全体構成や拠点の整理｣、｢認証鍵等の移動｣ が考えられる。

［R4-2］サービスの規模や環境に応じて処理能力が拡張可能な構成であること

前述の調査研究報告書では利用者の増加等により発生が予想される課題として、中央サーバへのアクセス数の増大が示されている。

サーバやデータベース等についてはクラスタ構成等の負荷分散に関する既知の技術が広く普及しているが、HSM を考慮した負荷分散については製品の特性を踏まえた対策の検討が必要となるため「HSM を考慮したアクセス数増大への対応」が本要求事項を実現するために解決すべき課題と考えられる。

② 運用性・可用性

前述の調査研究報告書では運用性･可用性に関して以下のように要求事項が示されている。

現在運用されている IC カードを用いた主要なサービスと同等の運用性・可用性が確保可能であること。原則 24 時間連続運用が要求される。但し、計画的なメンテナンスのための最小限のサービス停止は必要である。

上記要求事項に基づき、機器の故障・破壊・紛失等による情報逸失への対策としては定期的なデータのバックアップやリストアの運用整備が必要となる。

また事故や災害等によるサーバやネットワークの停止への対策として 24 時間 365 日の利用が求められる。

本調査研究では､前述の要求事項を以下のように具体化することとする。

- ［R5-1］システム障害やデータ紛失時の復旧に備え、データのバックアップ/リストアの機能、手段を有すること。
- ［R5-2］ネットワーク、ハードウェアなどの障害発生時にもサービスを継続する機能、手段を有すること。

次に上記要求事項の実現方法について検討する。

[R5-1] システム障害やデータ紛失時の復旧に備え、データのバックアップ/リストアの機能、手段を有すること

前述の調査研究報告書では運用時のバックアップ等に関する課題として、バックアップ処理の効率化が示されている。

サーバやデータベース等についてはバックアップに関する既知の技術が広く普及しているが、HSM で管理する鍵のバックアップ/リストア方式について製品の特性を踏まえた対策の検討が必要となるため「HSM で管理する鍵のバックアップ/リストア方式」が本要求事項を実現するために解決すべき課題と考えられる。

[R5-2] ネットワーク、ハードウェアなどの障害発生時にもサービスを継続する機能、手段を有すること

前述の調査研究報告書では運用時のバックアップ等に関する課題として、耐タンパー性相当リソースのクラスタリング・レプリケーションやフェイルオーバーが示されている。

サーバやデータベース等についてはクラスタ構成など冗長化に関する既知の技術が広く普及しているが、HSM を考慮した冗長化について製品の特性を踏まえた対策の検討が必要となるため「HSM を考慮した障害対策」が本要求事項を実現するために解決すべき課題と考えられる。

(2) 課題の整理

これまでの内容を踏まえ 表 5-4 に具体化された各要求事項を整理する。またこれら要求事項を実現する上での課題を 表 5-5 に整理する。

表 5-4　要求事項の整理

項番	要求事項
－	スケーラビリティ
R4-1	利用者数やサービス数に応じて、認証情報などの管理データの増加に対応可能な構成であること
R4-2	サービスの規模や環境に応じて処理能力が拡張可能な構成であること
－	運用性・可用性
R5-1	システム障害やデータ紛失時の復旧に備え、データのバックアップ/リストアの機能、手段を有すること
R5-2	ネットワーク、ハードウェアなどの障害発生時にもサービスを継続する機能、手段を有すること

表 5-5　課題の整理

項番	課題	対応要求事項	内容
－	スケーラビリティ	－	－
P4-1	鍵件数増大への対応	R4-1	HSM による鍵管理のデータ増大への対策
P4-2	全体構成や拠点の整理	R4-1	鍵等の分散管理の要否およびシステムの拠点
P4-3	認証鍵等の移動	R4-1	鍵の分散管理における利用者の移転等に伴う運用管理
P4-4	HSM を考慮したアクセス数増大への対応	R4-2	アクセス数増大への対策として、HSM を考慮したシステム全体の処理能力の向上
－	運用性・可用性	－	－
P5-1	HSM で管理する鍵のバックアップ/リストア方法	R5-1	HSM で管理する鍵のバックアップ/リストア方法
P5-2	HSM を考慮した障害対策	R5-2	HSM を考慮した障害対策

なお、前述の調査報告書ではシステムの実現に向けた今後の取組みとして実証実験による実用性の検証が挙げられているが、「中央サーバに認証機能を一部移行させる方式」の構想については検討が開始されたばかりであり実装手段や方式は十分な検討がなされていない状況である。そのため本調査研究では、表 5-5 で整理した課題への対策を検討し、その内容も踏まえて今後必要となる実証実験について、6.3 および 6.4 で提案を行うこととする。

またスケーラビリティに関する課題「全体構成や拠点の整理」および「認証鍵等の移動」については、サービス内容やサービス環境がより具体的になった段階でシステム全体の運用とあわせて検討されるべき内容であるため本調査研究では課題の整理に留める。(前述の 表 5-5 のハッチング部分)

(3) 対策の検討

① スケーラビリティ

(i) 鍵件数増大への対応

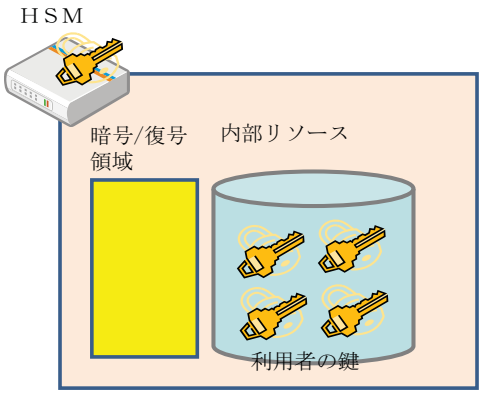
一般的にHSMにおける鍵管理ではHSMの内部に鍵を管理するタイプ(以下、内部管理型と呼ぶ)と外部で管理するタイプ(以下、外部管理型と呼ぶ)が存在する。前者は文字通り管理対象の鍵を HSM 内部のディスク等にて管理する方法である。

後者はマスターとなる鍵のみを HSM 内部のディスクやスマートカード等にて管理し、管理対象の鍵はこのマスターとなる鍵で暗号化された状態で HSM を利用するシステムの外部ディスク等、HSM の外部リソースにて管理される。鍵の生成およびマスター鍵での暗号化や鍵の利用時におけるマスター鍵での復号は全て HSM の内部で行われるため、管理対象の鍵が非暗号化の状態で外部に出力されることはない。この方式は「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」(平成 20 年度総務省委託事業)において「利用者認証鍵の間接保護 (方法 2) 」としても挙げられる方式をHSMの製品としてサポートするものである。

大量のデータ管理を想定した場合、内部管理型は管理可能なデータ量が HSM 内部のリソースに依存してしまうため、本調査研究では一般の外部記憶装置の活用が見込める外部管理型を提案することとする。

HSMにおける鍵管理方法を 図 5-12 に示す。

【内部管理型】
・利用者の鍵は全てHSM内に管理する。
・管理可能なデータ量はリソースの容量に依存する。



【外部管理型】
・HSM内部にはマスターとなる鍵のみ管理する。
・利用者の鍵はマスターとなる鍵で暗号化し、外部リソースで管理する。
・管理可能なデータ量は外部リソースの容量に応じて拡張可能
・暗号化/復号化などはＨＳＭ内部で行われるので鍵が非暗号化のまま外に出ることはない。

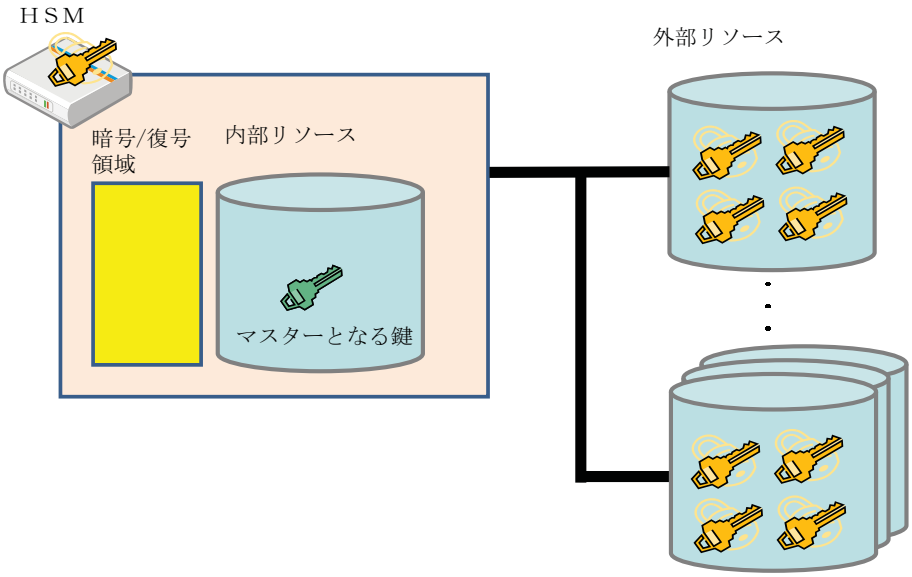


図 5-12 HSM における鍵管理方法

上記については、5.2 にて外部管理型のHSMで管理可能な鍵件数および処理性能への影響等について実機を用いて検証することとする。

(ii) HSM を考慮したアクセス数増大への対応

HSM の接続形態としては大きく PCI 接続等により HSM を利用するサーバに直接接続させるタイプ(以下、直結型と呼ぶ)と、ネットワー

クを介して接続させるタイプ(以下、ネットワーク型と呼ぶ)が存在する。アクセス数増大への対策として、処理能力向上のためサーバや HSM の増設を想定した場合、直結型の HSM は複数サーバから共有することができないためサーバを増設するとこれと併せて HSM も増設が必要となる。HSM は一般的に高価な製品であるためコスト面が課題となる。一方、ネットワーク型は複数のサーバで共有することができるため、HSM の台数に依存せずサーバの増設が可能となるとともに、クラスタ構成をサポートする HSM も存在するため HSM のみ増設させるような構成も可能となる。ただし通信速度に関して直結型と比較した場合、ネットワーク通信によるオーバーヘッドが発生することを考慮する必要がある。

HSMの接続方法を 図 5-13 に示す。

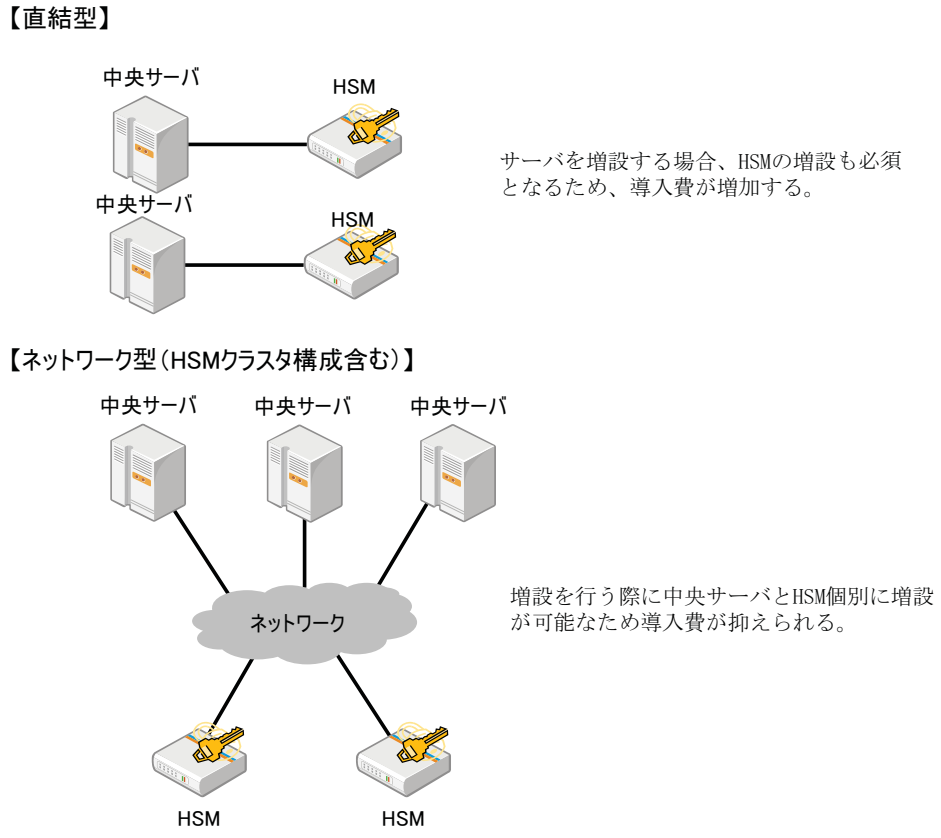


図 5-13 HSM の接続方法

上記については、5.2 にてネットワーク型のHSMを複数台設置し、HSM間で鍵情報を安全に共有できることを実機を用いて検証することとする。

② 運用性・可用性

（i）HSM で管理する鍵のバックアップ/リストア方式

5.1.4 (3) ①でも述べたように、HSMにおける鍵管理では内部管理型と外部管理型が存在する。内部管理型では一般的に鍵のバックアップ方法は各HSM製品に依存した方法となる。一方外部管理型では保存先が外部記憶装置となり、通常のファイルに関するバックアップ技術が活用できる製品も存在する。

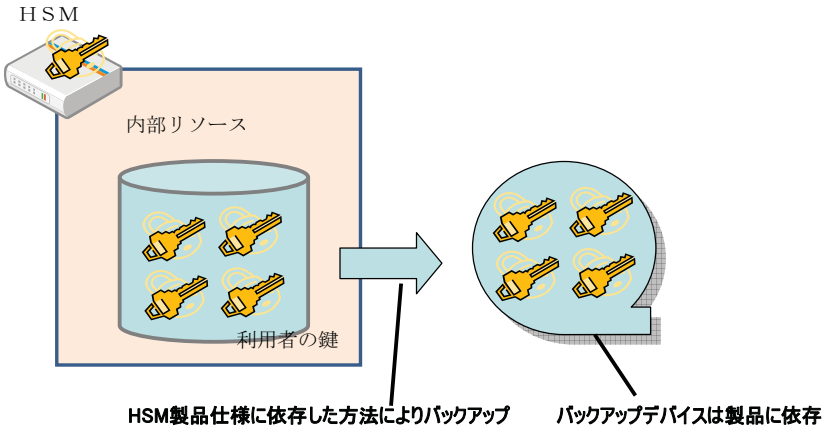
バックアップ作業は一般的に自動化による作業も見込まれるため、HSM 製品に依存した方法の場合個別のバックアップ計画が必要となる可能性がある。また大量の鍵管理を行う場合、差分バックアップ等の手法が取れない場合は毎回フルバックアップが必要となるためバックアップ時間についても課題となる。一方、HSM 外部で鍵管理を行う場合は差分バックアップやデータ重複排除などの既存の技術により効率的なバックアップが見込める。これらのことから本調査研究では既存技術の活用が見込める外部管理型を提案することとする。

なお外部管理型の場合、管理対象の鍵を暗号化するマスター鍵のバックアップも必要となる。この鍵は HSM 内部のディスクやスマートカード等により管理されるためバックアップは HSM 製品に依存した方法となるが、この鍵は通常運用中に変更されることはないため初期構築時にバックアップを取得することとなり、定期的に実施される通常のバックアップ計画への影響はないと考えられる。

また、製品によっては前述のマスター鍵のバックアップを複数の IC カードに分割してバックアップすることが可能であり、管理対象の鍵およびマスターとなる鍵が格納された一部の IC カードが万一紛失したとしてもデータを保護する仕組みを有するものも存在する。

鍵のバックアップ方法を 図 5-14 に示す。

【内部管理型】
・バックアップ方法は製品仕様に依存
・バックアップ方法が独自の場合、個別のバックアップ計画が必要となる可能性がある。
・差分バックアップ等の手法が取れない場合は毎回フルバックアップが必要となり、
大量の鍵管理を行う場合、バックアップ時間の考慮が必要となる。



【外部管理型】
・利用者の鍵は一般のバックアップ技術が活用可能
・マスターとなる鍵のバックアップはHSM製品に依存した方法となるが、通常マスターとなる鍵は
変更されないため定期的なバックアップは不要

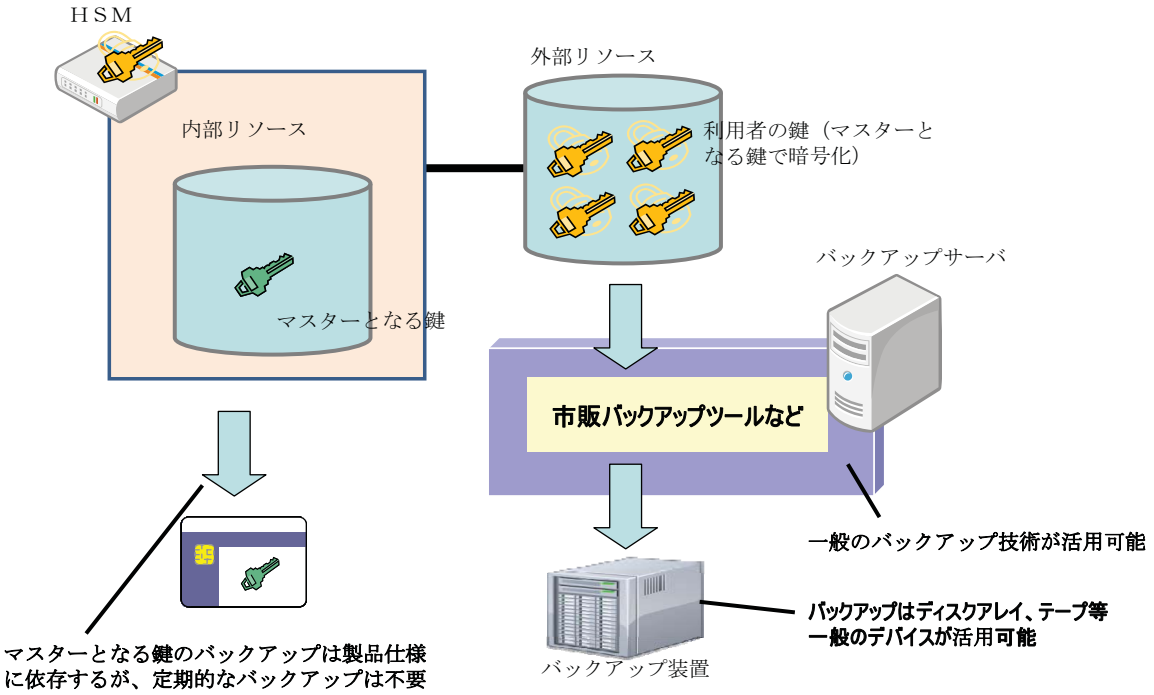


図 5-14 鍵のバックアップ方法

（ii）HSM を考慮した障害対策

HSMに関する可用性確保のためにはHSMを利用するサーバも考慮した検討が必要となる。5.1.4（3）①でも述べたように、HSMの接続形態としては直結型と、ネットワーク型が存在するが、前述したように直結型のHSMは複数サーバから共有することができないため、サーバの可用性確保のため冗長化構成をとる場合、サーバの増設に併せてHSMの増設も必要となる。

なお現状 HSM 自身の可用性確保については製品自身の有するフェイルオーバー機能の有無に依存するため注意が必要である。

5.1.5 電子署名法による推定効に関する課題及び対策

本項では電子署名法の「電磁的記録の真正な成立の推定」で示される要求事項から導かれる課題及び対策の検討を行う。

(1) 課題の抽出

電子署名及び認証業務に関する法律(平成十二年五月三十一日法律第百二号)(以降「電子署名法」と記述) 第二章(電磁的記録の真正な成立の推定)第三条「電磁的記録であって情報を表すために作成されたもの(公務員が職務上作成したものを除く。)は、当該電磁的記録に記録された情報について本人による電子署名(これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。)が行われているときは、真正に成立したものと推定する。」(このような推定が可能となることを「推定効」と呼ぶ)に示されるように、電子署名の要件として、「これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。」との条件が示されている。

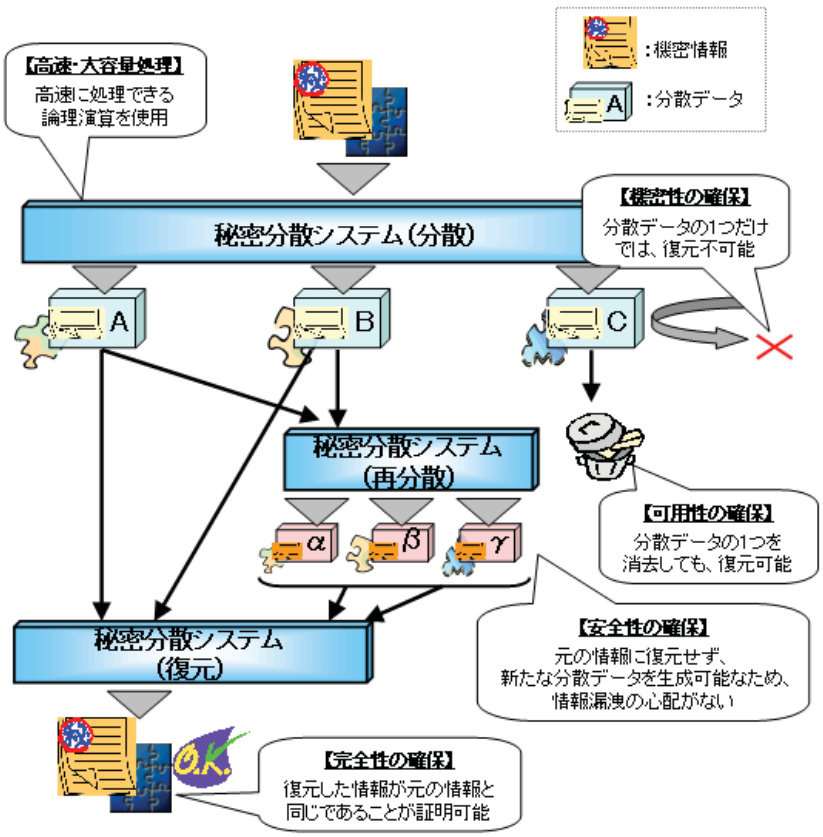
一方で、公的個人認証サービスにおいては、電子署名に係る地方公共団体の認証業務に関する法律施行規則(平成十五年九月二十九日総務省令第百二十号)第八条(利用者署名符号及び利用者署名検証符号を記録する電磁的記録媒体)において、「電磁的記録媒体は、住民基本台帳カードその他の半導体集積回路を一体として組み込んだカード(住所地市町村長の使用に係る電子計算機の操作により利用者署名符号及び利用者署名検証符号を安全かつ確実に記録できるものに限る。)であって、総務大臣が定める技術的基準を満たすものとする。」とされ、事実上、住民基本台帳カードに格納されていることを条件としている。

これらを勘案すると、「電子署名」に用いる秘密鍵は、個人のICカードに格納されていることが求められていると考えられる。サーバ連携型多目的 IC カードでサーバ側に配置した秘密鍵を用いた「電子署名」サービスを実施する場合、この前提を満足しないため、電子署名法で示される「推定効」が成り立たないことが指摘されている。

(2) 対策の検討

① 秘密分散技術について

NTTコミュニケーションズでは、機密情報を安全に保管するための技術として、秘密分散技術を開発した。本技術の概要を 図 5-15 に示す。



出典:http://www.ntt.com/release/2005NEWS/0004/0415a.html

・機密情報を 3 つのデータに分散する。

・分散された 3 つのデータのうち、2 つを組み合わせなければ、元の情報の復元は不可能。単独の分散データを紛失しても情報漏えいとはならないため、安心して持ち運ぶことができる。

・ハッシュ値*の照合により、復元した情報と元の情報が同じであることを証明できる。

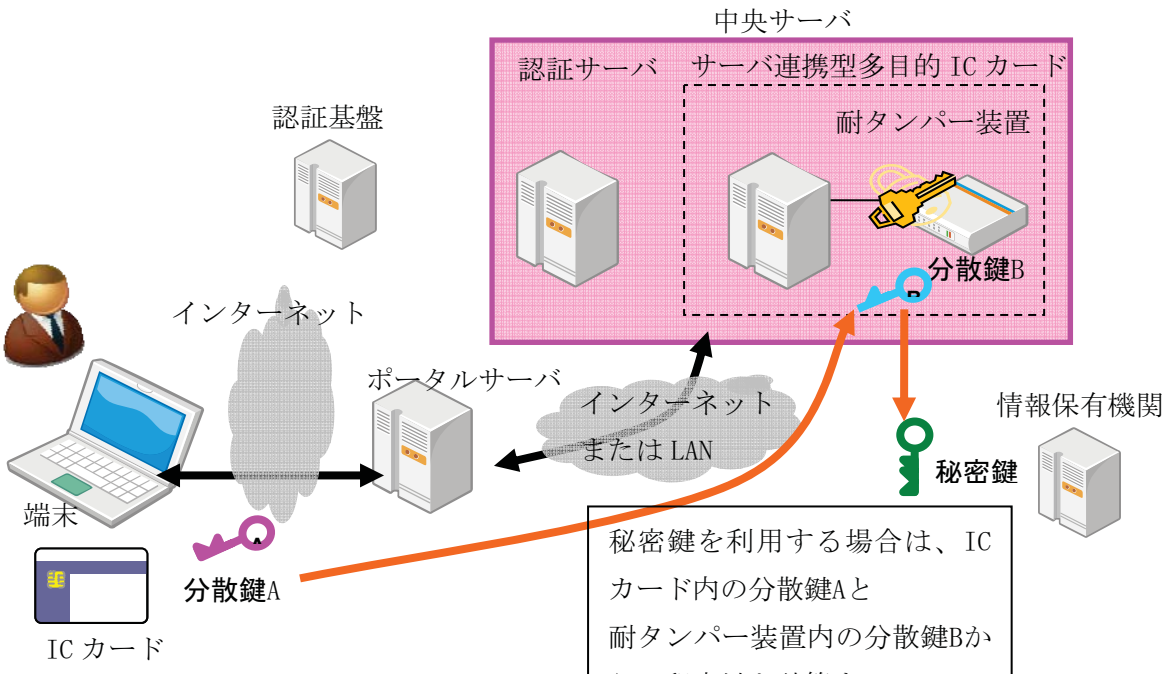
・NTT コミュニケーションズが独自開発した論理演算を使用することで、従来の秘密分散法では困難とされていた大容量のデータを高速に処理することができるため、スムーズな情報の分散、復元が可能。

*ハッシュ値：一方向関数により割り出されたファイル固有の識別番号。同じハッシュ値をもつファイルを複製することは極めて困難であるため、ファイルの真偽を判別することが可能。

図 5-15 NTT コミュニケーションズが開発した秘密分散技術の概要

② サーバ連携型多目的 IC カードを使い、かつ、「推定効」を満足する方式の提案

「推定効」を得るための方式として、サーバ上の秘密鍵の利用にあたり、従来と同様に、利用者が持つICカード内の情報を必要とする方式を考えることができる。本方式の概要を 図 5-16 に示す。



（準備）

(1) IC カード内に、対応する秘密鍵と同じ長さの乱数列 A を格納する。

(2) サーバ上で本乱数列 A を用いて、秘密鍵を秘密分散する。（分散鍵を B,C とする）

(3) 分散鍵 B（または C）を耐タンパー装置(HSM)に記憶する。

（署名実施）

(4) IC カードを挿入し、署名を指示する。

(5) IC カードと耐タンパー装置間に秘密通信路を設定し、耐タンパー装置に乱数列を送信する。

(6) 耐タンパー装置内で、秘密鍵を計算し、署名を実施する。

(7) 秘密鍵を削除する。

図 5-16「推定効」に関する課題に対応する方式の概要

③ 本方式の特徴

本方式の特徴を以下に示す。

- 署名を実施するタイミングで、IC カードの挿入が確認されるため、「推定効」の観点からは、IC カード内に秘密鍵を配置することと同様と見なせる。
- IC カード内の乱数列は、サーバ上の複数の秘密鍵に対して共通的に利用可能であり、また、秘密鍵の更新の際にも必ずしも、同期して変更する必要はない。
- IC カードを紛失した場合に秘密鍵を復旧させるためには、分散鍵 B,C の双方を保存しておく必要があるが、復旧の手順を慎重に設計するとともに、利用者に手順を明示する必要がある。

④ 本方式に特徴的なセキュリティおよび運用面の評価

(i) セキュリティ評価

ここでは、「推定効」を無効化する攻撃について検討する。

(a) 乱数列の盗難、耐タンパー装置(HSM)内の秘密鍵の盗難

(分散鍵生成時、秘密鍵計算時)

1. プログラム：HSM 内に存在するためロジックの改ざんは不可能。

2. 通信路：IC カード、HSM の双方を確認の上、秘密通信を行うことから盗聴の危険は無い。

3. HSM

3-1. 保守者：保守者については、CP などで運用を規定する必要がある。

3-2. 悪意のあるユーザ:HSMの権限管理により防御が可能と考えられる。(5.1.3 (3) ① (i) 参照)

4. IC カード：サーバ通信時以外での乱数列読み出しを禁止とすることで漏洩を防御できる。

(ii) 運用面の評価

秘密分散を利用した場合に特徴的な課題について評価する。

(a) スケーラビリティ

1. 分散鍵 B,C の保存：秘密分散を利用しない場合に比較すると、2 つの分散鍵を保存する場合には、保存容量が 2 倍必要となる。

2. HSM 処理性能：秘密分散では、HSM 内で秘密鍵計算処理が増加する。

(b) 保守性

1. 乱数列の発生：秘密分散には真正乱数が必要であり、発生装置が必要になる。

2. 乱数列の IC カードへの格納：乱数列について、(秘密鍵とは異なる) ライフサイクルを考慮し、定期的な置換が必要と考えられる。

⑤ 性能面の評価

(i) 性能評価の機器構成

本方式では、本報告書の他の方式と検証環境の構成が異なることから、「5.2実機検証」に示す検証環境とは別に 図 5-17 に示す環境を用いて評価を行った。

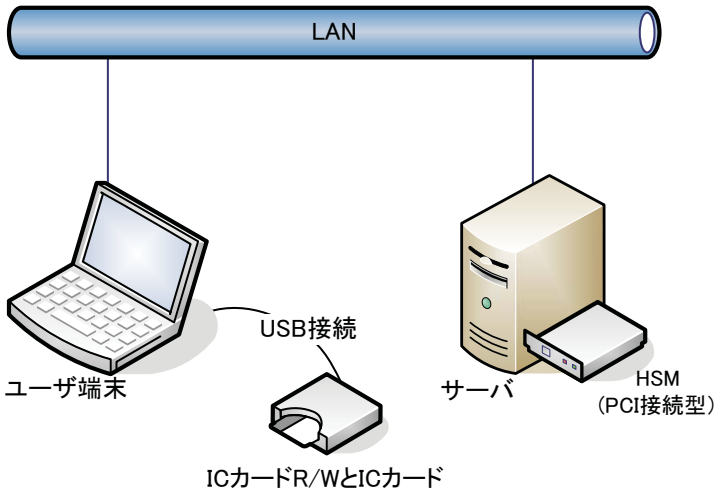


図 5-17 性能評価で使用した環境

(ii) 性能評価の処理シーケンス

本評価で使用したシーケンスを 図 5-18 及び 図 5-19 に示す。

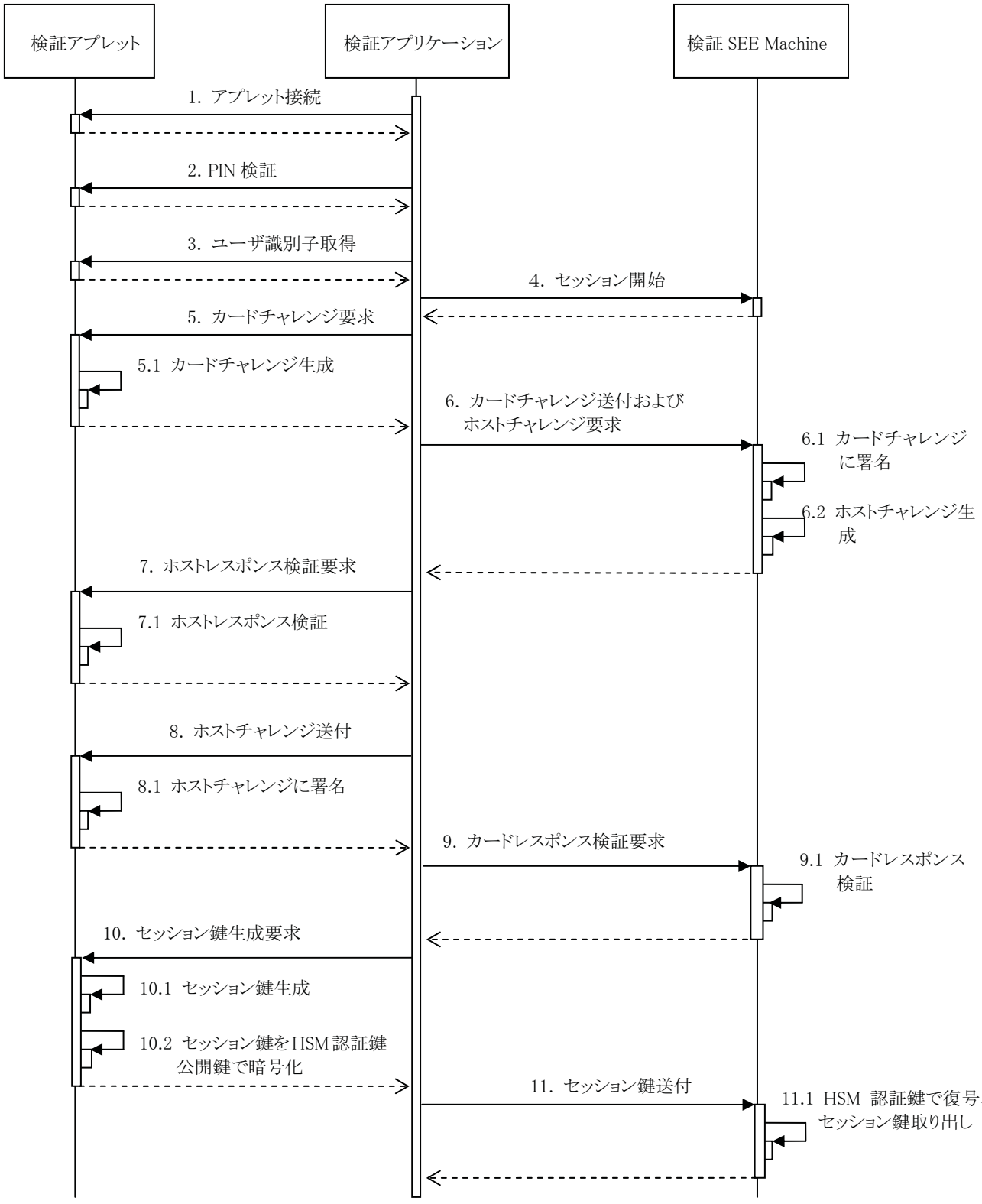


図 5-18 性能評価で使用したシーケンス図（１／２）

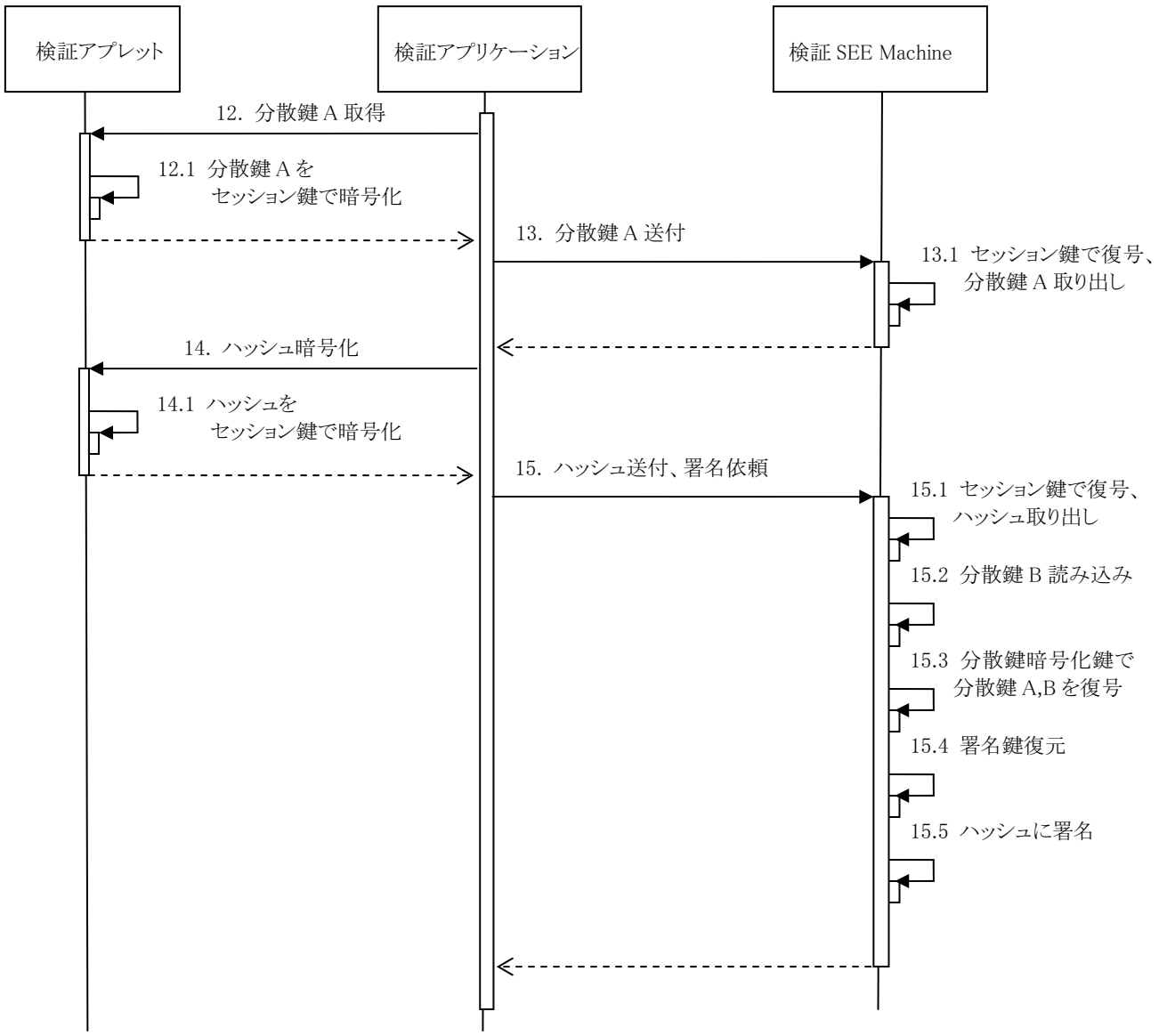


図 5-19 性能評価で使用したシーケンス図（２／２）

（iii）性能評価結果のポイント

秘密分散を使用する場合、乱数列を IC カードからサーバに安全に送るための処理に要する時間が必要となるため、通常の IC カードでの署名に比較すると、約 1.5 倍の時間を要することがわかった。

（評価結果の詳細）

・IC カード内署名時間を約 1 秒と想定する。

・ 図 5-19 で示した実証環境で、秘密分散を使用して電子署名を行

った結果、平均で約 1.5 秒を要した。

- IC カードの処理は、HSM の処理に比較すると遅いため、本処理時間（1.5 秒）のおよそ 90%が IC カード内の処理だった。
- 本実証実験では、IC カードと HSM 間の通信路として LAN を用いたが、実運用時に WAN を使うことを想定した場合、1 回の通信毎に 0.1 秒オーダーの時間がかかり、今回の処理シーケンスでは、0.5 秒以上の増加が想定される。

5.2 実機検証

本節では 5.1 で挙げた課題及び対策について、実機による検証を行う。

5.2.1 検証環境

検証のために準備した環境について以下に示す。

(1) サーバ連携型多目的 IC カードを用いた検証環境

検証環境は 5.1.1 を考慮し、図 5-20 に示す環境とする。

利用者からのアクセスは、インターネット等の公衆回線を想定した検証を行うため、DMZ にプロキシサーバを設置し、ポータルサーバや認証サーバへの中継を行う構成とした。また、複数のサービスを用いた検証を行うため情報保有機関を複数配置する構成とした。

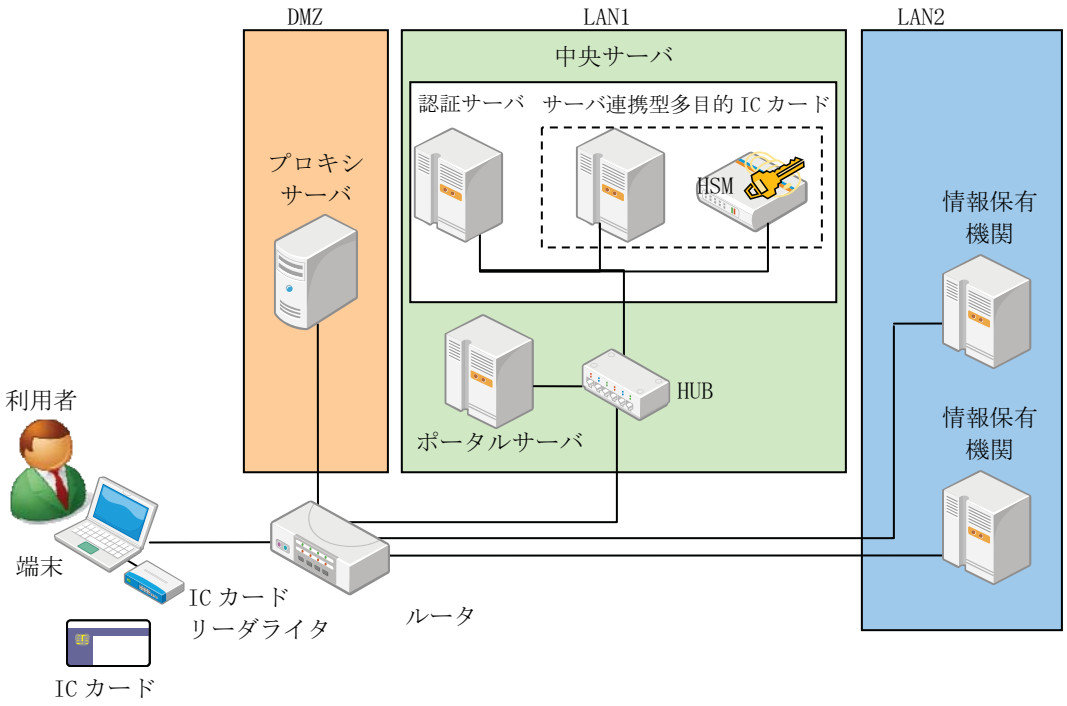


図 5-20　サーバ連携型多目的 IC カードを用いた検証環境

(2) 検証環境の構成

検証環境で使用するサーバ機や端末は、一般的なスペックのものを市販製品から選定した。IC カードについては、公的個人認証等の公的 IC

カードとして幅広く利用されている type-B カードを適用した。

検証環境の構成を 表 5-6 および 表 5-7 に示す。

表 5-6 検証環境の構成(ハードウェア)

分類	種別	説明	備考
サーバ（共通）	機種	PC/AT 互換機	
	CPU	Intel Xeon 相当以上	
	メモリ	4GB 以上	
	HDD	300GB 以上	
	ネットワーク	100Base-T 以上	
HSM	－	nCipher Corporation 製 NC4333N-500 netHSM 500 SEE Ready	
端末	機種	PC/AT 互換機	
	CPU	Intel Celeron 相当以上	
	メモリ	2GB 以上	
	HDD	5GB 以上	
	ネットワーク	100Base-T 以上	
	USB ポート	空き USB2.0 ポート 1 つ以上	
	モニタ	解像度 1024×768 以上	
IC カードリーダライタ	－	SCR331DI-NTTCom	
IC カード	－	Type-B カード（eLWISE）	
ネットワーク装置	ルータ	WAN ポート：100Base-T×1 以上 LAN ポート：100Base-T×3 以上	
	HUB	100Base-T×4 以上	

表 5-7 検証環境の構成(ソフトウェア)

分類	種別	説明	備考
サーバ連携型多目的ICカード	OS	Red Hat Enterprise Linux 5.1	
	セキュアOS	TOMOYO Linux	
	Webサーバ	Apache2.2	
	APサーバ	Tomcat6	
	DBサーバ	PostgreSQL8	
	Java	JRE1.6	
	認証局	OpenSSL	
認証サーバ／ポータルサーバ	OS	Red Hat Enterprise Linux 5.1	
	Webサーバ	Apache2.2	
	APサーバ	Tomcat6	
	DBサーバ	PostgreSQL8	
	Java	JRE1.6	
	ID連携製品	TrustBindFederation Manager	
情報保有機関	OS	Red Hat Enterprise Linux 5.1	
	Webサーバ	Apache2.2	
	APサーバ	Tomcat6	
	DBサーバ	PostgreSQL8	
	Java	JRE1.6	
プロキシサーバ	OS	Red Hat Enterprise Linux 5.1	
	Webサーバ	Apache2.2	
	メールサーバ	Postfix (SMTP) Dovecot (POP)	
HSM	ドライバ	netHSMドライバ	
端末	OS	WindowsVista	
	ブラウザ	Internet Explorer 8	
	ドライバ	ICカードリーダライタドライバ (SCR331DI-NTTCom)	

(3) 設定

利用者が検証環境を使用するためのアカウント開設を 図 5-21 のフローで設定した。

本処理では利用者が認証サーバやサーバ連携多目的 IC カードを利用するために必要な情報を登録する。また、利用者が利用できるサービスの登録およびサービス利用時に必要となる鍵ペア生成、認証局と連動した証明書の発行と登録を行う。

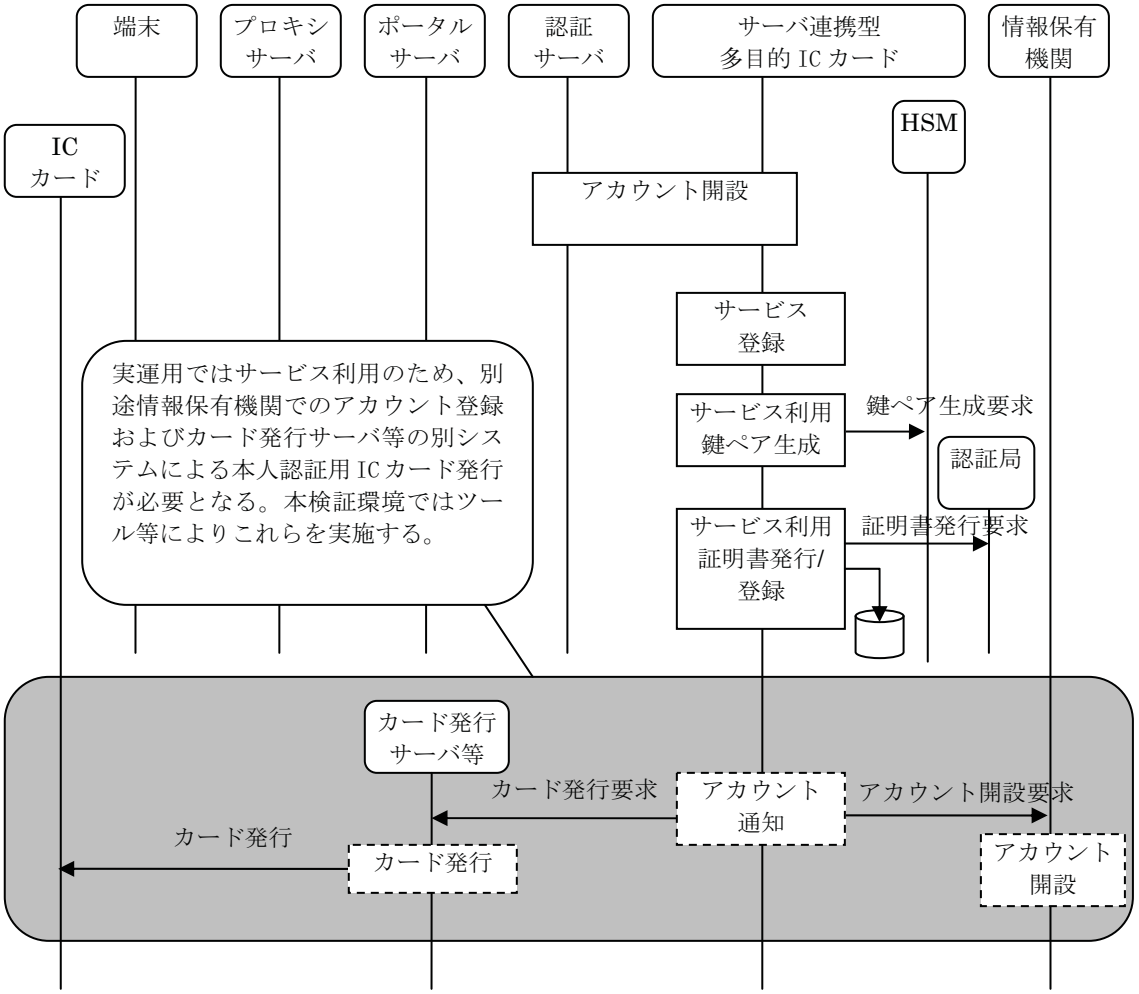


図 5-21 アカウント開設フロー

5.2.2 検証項目の抽出

前述の検証環境による実機検証項目を以下に示す。

(1) HSM へのアクセス制御方式の検証

5.1.3 で検討した「(P1-2) HSMへのアクセス制御方式」に関する対策に

ついて検証を行う。本検証では、セキュアOSの設定によりHSMに格納されている利用者の鍵への鍵の所有者以外からの不正なアクセスを防止する方法について検証する。

(2) サーバ連携型多目的 IC カードの構築に関する検証

5.1.4 で検討した「(P4-4) HSMを考慮したアクセス数増大への対応」に関する対策について検証を行う。本検証では、アクセス数増大を考慮してHSMを複数台設置する場合に、複数のHSM間で鍵情報を安全に共有する方法について検証する。

(3) サービス提供者インタフェースの検証

5.1.3 で検討した「(P2-1) 標準的なインタフェースで提供する機能の種類」に関する対策について検証する。本検証では、従来のICカードでICカード内にサービス追加が可能であったように、提案したインタフェースにより、サービス提供者がサーバ連携型多目的ICカードにサービスを追加できることを検証する。

(4) HSM による鍵管理のスケーラビリティ検証

5.1.4 で検討した「(P4-1) 鍵件数増大への対応」に関する対策について検証する。HSMによる鍵管理のスケーラビリティについては、「一般的には管理できる鍵の数は多くなく、高々数百のオーダーである」と「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では報告されている。HSMで管理可能な鍵件数および処理性能への影響等について検証を行う。

(5) サーバ連携型多目的 IC カードを用いた基本的なサービスのフィージビリティ検証

本検証では、利用者向けの基本的なサービスとして、親展サービスや申請サービスを検証環境として準備し、個人情報の安全な流通方法としてサーバ連携型多目的 IC カードを適用した場合のフローについてフィージビリティ検証を行う。

5.2.3 検証結果

前述の各検証項目の結果を以下に示す。

(1) HSM へのアクセス制御方式の検証

HSM へのアクセス制御について、HSM へアクセス可能なアプリケーションの制限を検証するため前述の検証環境を以下のように準備した。

- HSM へアクセスするアプリケーションとして、サーバ連携型多目的 IC カードアプリケーションを準備する。また、HSM で管理する任意の鍵の削除および参照を行う擬似攻撃用のテストプログラムを準備する。
- セキュア OS(TOMOYO Linux)の機能を用いて、HSM はサーバ連携型多目的 IC カードアプリケーションからのみアクセス可能とするよう制御する。(HSM へアクセス可能なアプリケーションの制限)

検証環境によるアクセス制御実現方法を 図 5-22 に示す。

なお 5.2.1 (1) に示す通り本環境はインターネット等の公衆回線からの外部アクセスを想定して、DMZにプロキシサーバを設置しまた通信プロトコルにSSLを用いることでDOS攻撃や盗聴やなりすましといった脅威への対策を行っている。

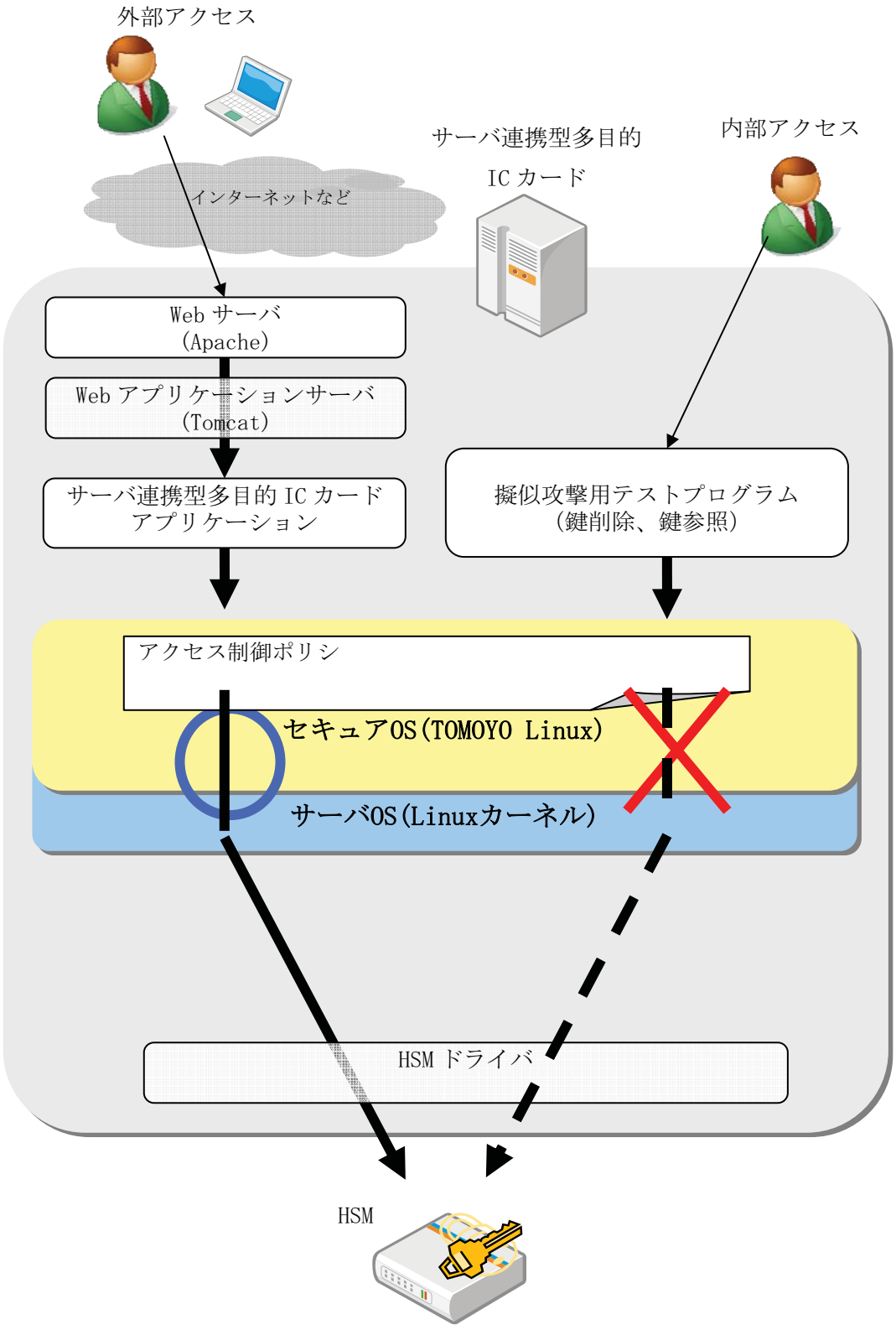


図 5-22 検証環境によるアクセス制御実現方法

本検証により以下の確認を実施した。

① セキュア OS のアクセス制御ポリシ設定

TOMOYO Linux のアクセス制御機能を用い、HSM へアクセス可能なアプリケーションを制限するようなポリシ設定が行えることを確認した。

TOMOYO Linux では「学習モード」と呼ばれる動作モードにてアプリケーションを動作させ、当該アプリケーションがアクセス可能なリソースを OS に記録させることでアクセス制御ポリシを設定することが可能である。続いて「学習モード」を「強制モード」と呼ばれる動作モードに変えると前述で設定したアクセス制御が有効となり、学習した動作以外は OS によりアクセスが拒否されるような制御が行われる。

TOMOYO Linuxのアクセス制御ポリシ設定方法を 図 5-23 に示す。

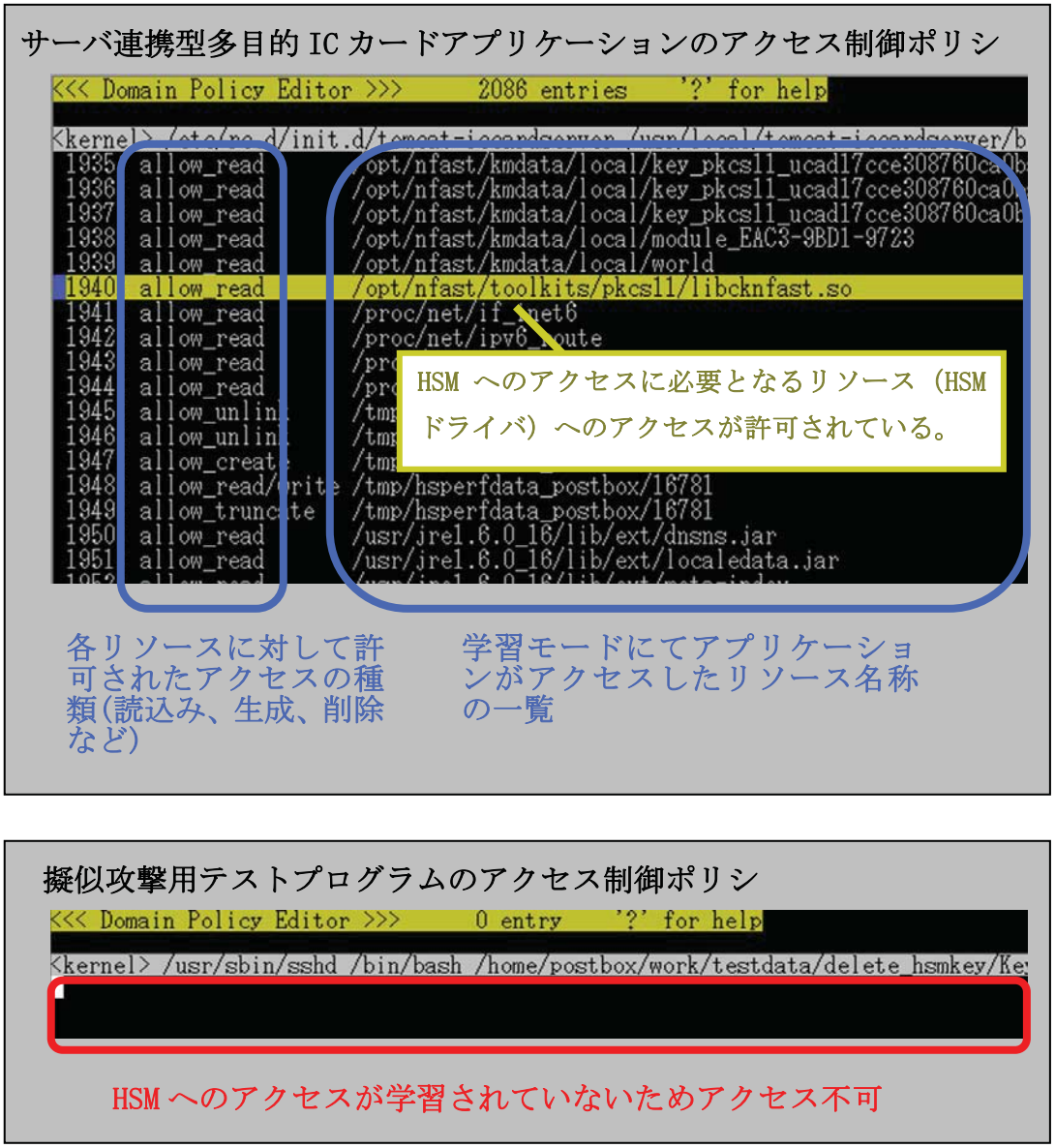


図 5-23 TOMOYO Linux のアクセス制御ポリシ設定方法

また、上記の擬似攻撃用テストプログラムのように直接 HSM へアクセスするのではなく、HSM へのアクセスが許可された「サーバ連携型多目的 IC カードアプリケーション」を不正に実行することにより、間接的に HSM へアクセスするようなケースも考えられる。

通常 Web サーバ経由でアクセスされた場合は本人認証により正しい利用者かどうかの確認が要求される。この本人認証を不正に回避する目的で直接「サーバ連携型多目的 IC カードアプリケーション」へアクセスする不正なプログラムが実行された場合も、本検証で用

いた TOMOYO Linux によるアクセス制御により、「サーバ連携型多目的 IC カードアプリケーション」へアクセスできるアプリケーションを制限できるため、このような間接的な HSM への不正アクセスも防ぐことが可能となる。

図 5-24 に間接的なHSMへの不正アクセス制御方法を示す。

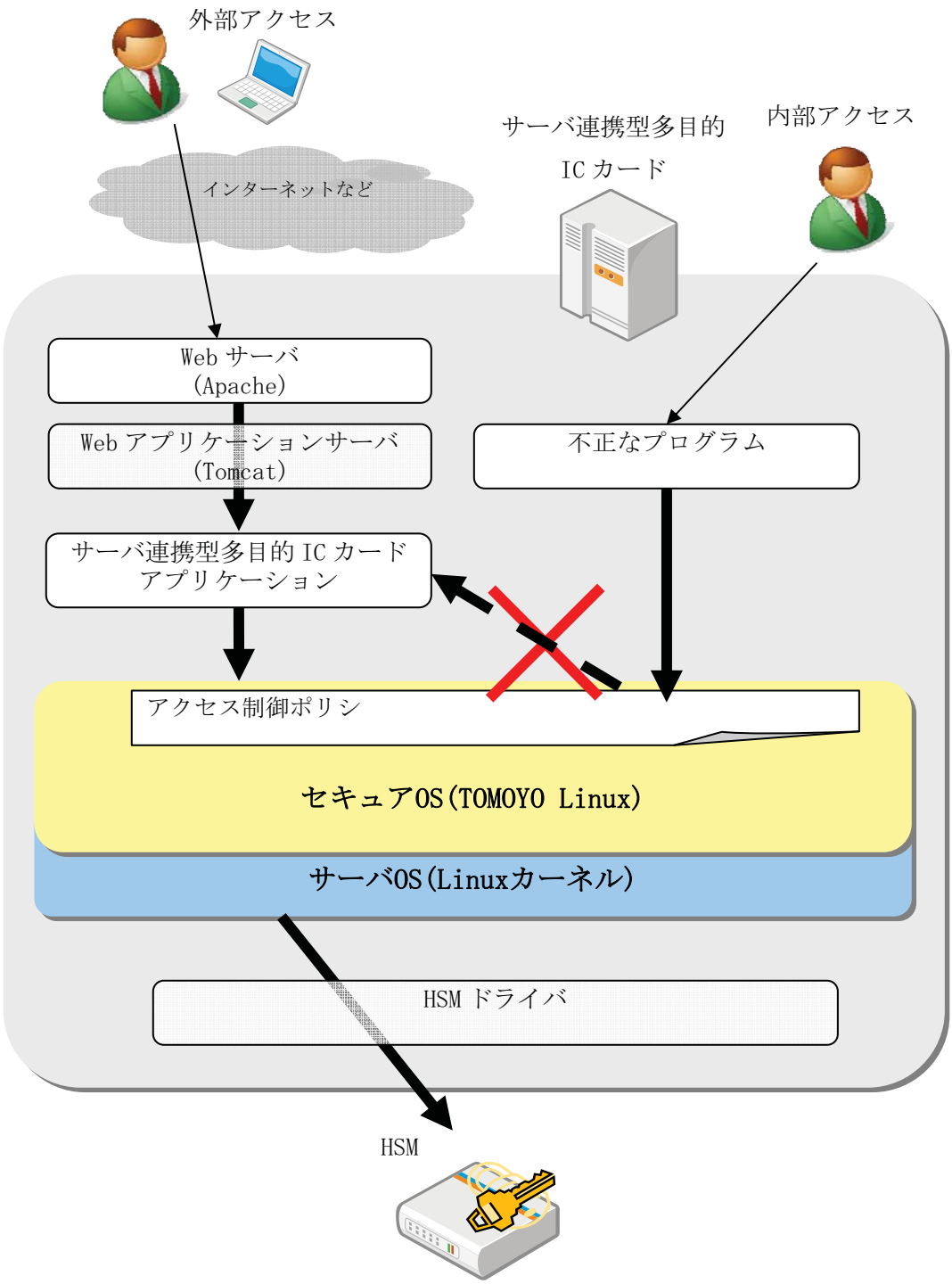


図 5-24 HSM への間接的な不正アクセス制御方法

(2) サーバ連携型多目的 IC カードの構築に関する検証

アクセス数増大への対策として、サーバ連携型多目的 IC カードを構築する際に、複数台の HSM を用意した環境を構築した。

本検証で用いた HSM は、「セキュリティワールド」という仕組みを用いて、HSM で生成した利用者の鍵情報を管理する。セキュリティワールドを新規で作成すると、「modulekey」と呼ばれるマスター鍵が HSM 内に生成される。HSM で利用者の鍵生成を行うと、このマスター鍵により利用者の鍵情報が暗号化され、HSM にアクセスしているサーバ上のディスクに暗号化された利用者の鍵情報が保管される。また上記鍵を用いて演算を行う場合は、HSM 内部でマスター鍵により利用者の鍵情報を復号し演算を行うことで、鍵の実体が HSM 外部に出力されることがないような仕組みになっている。

検証環境におけるHSMの鍵管理方法を 図 5-25 に示す。

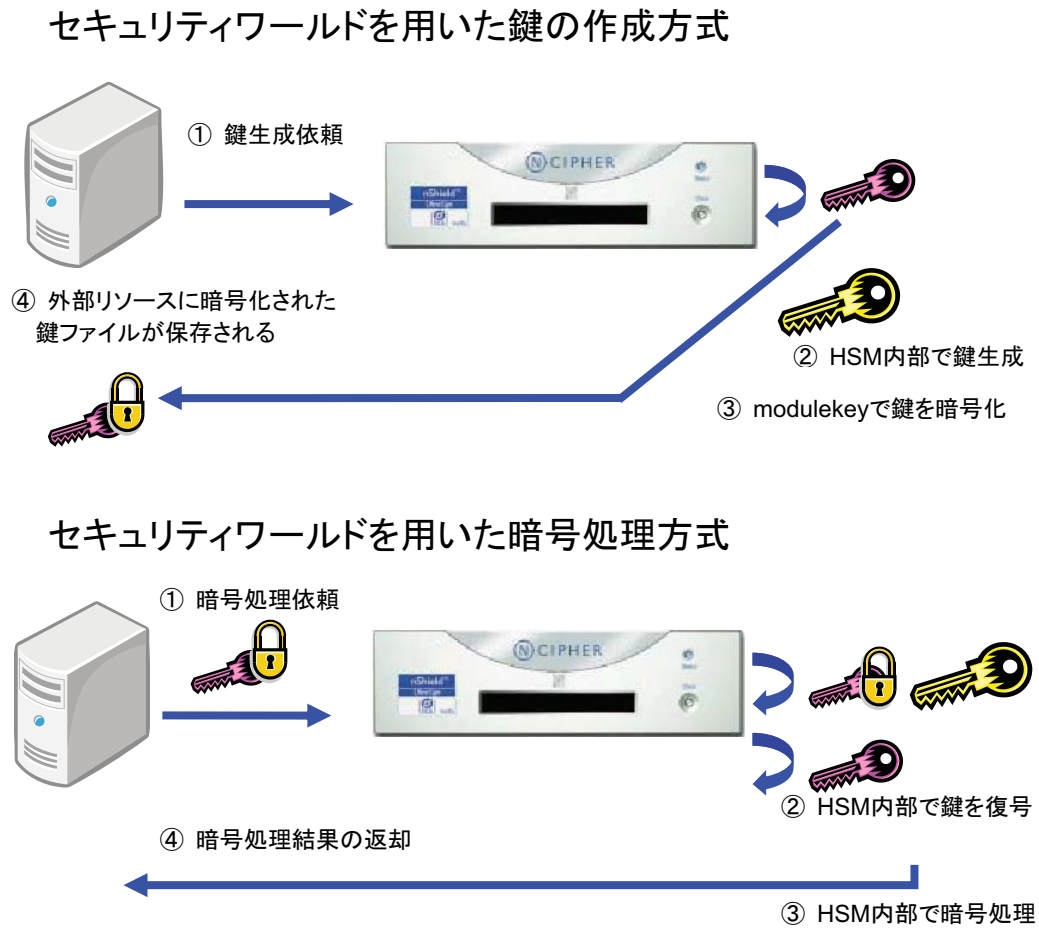


図 5-25 検証環境における HSM の鍵管理方法

また上記マスター鍵はセキュリティワールドを新規作成した際に ACS(Administrator Card Set)と呼ばれるカードのセットに格納される。HSM を増設する際はこのカードを用いることにより、マスター鍵を増設した HSM へインポートすることが可能となり 1 台のサーバで複数台の HSM をクラスタ構成として使用することができる。なお

ACS は複数の IC カードに分割することが可能でありこれらのカードを複数の管理者により管理することで、特定の管理者のみで HSM の増設が行えないようセキュアな運用管理を実現している。

またこの仕組みにより、運用中にアクセス数がさらに増大した場合においても、HSM を容易に追加することが可能である。

検証環境における複数台のHSMの構築方法を 図 5-26 に示す。

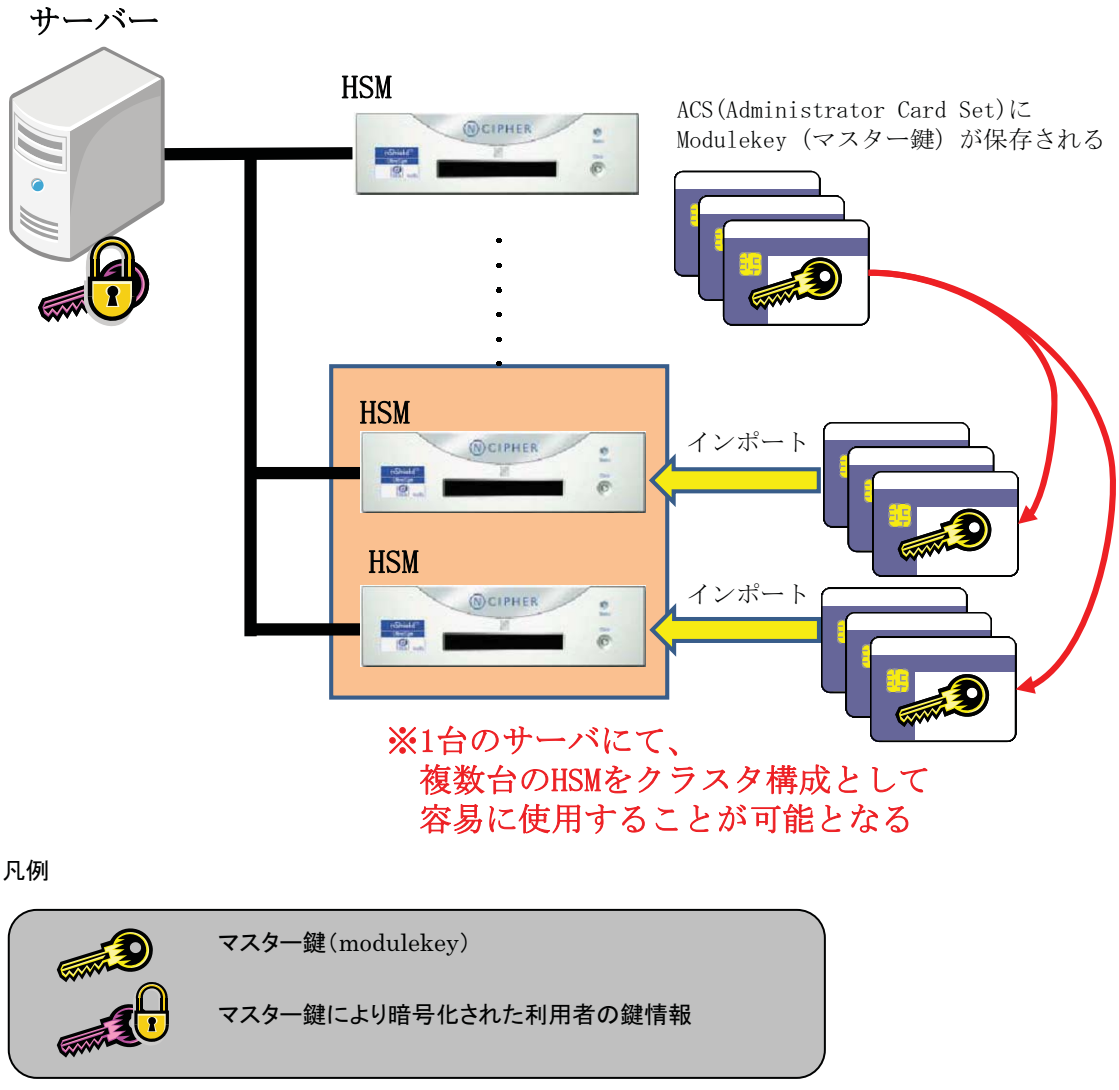


図 5-26 検証環境における複数台の HSM の構築方法

なお、製品の仕様を調査した結果以下のような制約が確認された。

・（クラスタ構成の台数制限）クラスタ構成において 1 台のサーバで認識できる HSM の台数に制限があるため、負荷分散における HSM の増設時の制約となる。

・（負荷分散処理の制限）鍵生成など一部の処理は負荷分散の対象外となるため、アプリケーション側や運用での対策が必要となる。

(3) サービス提供者インタフェースの検証

サービス提供者インタフェースについて 5.1.3 (3) ②に基づき、提案したインタフェースにより、サービス提供者がサーバ連携型多目的ICカードにサービスを追加できることを検証するため、前述の検証環境を以下のような構成で準備した。

- サービス提供者インタフェースとして「サービス利用開始」、「サービス利用」を準備
- HTTP/SOAP プロトコルによる Web インタフェースにより機能を提供
- サービス利用開始用のサンプルサービスとして、鍵ペアを用いて利用者から送信された情報に署名を行うサービスを準備
- 上記サンプルサービスの実行に伴う鍵ペア生成や署名といったサービスに依存した処理を行うモジュール(java アプリケーション)をサーバ連携型多目的 IC カードへ登録し、サービス提供者インタフェースを介してこのモジュールが実行されるようにする。

検証環境によるサービス提供者インタフェースを 図 5-27 に示す。

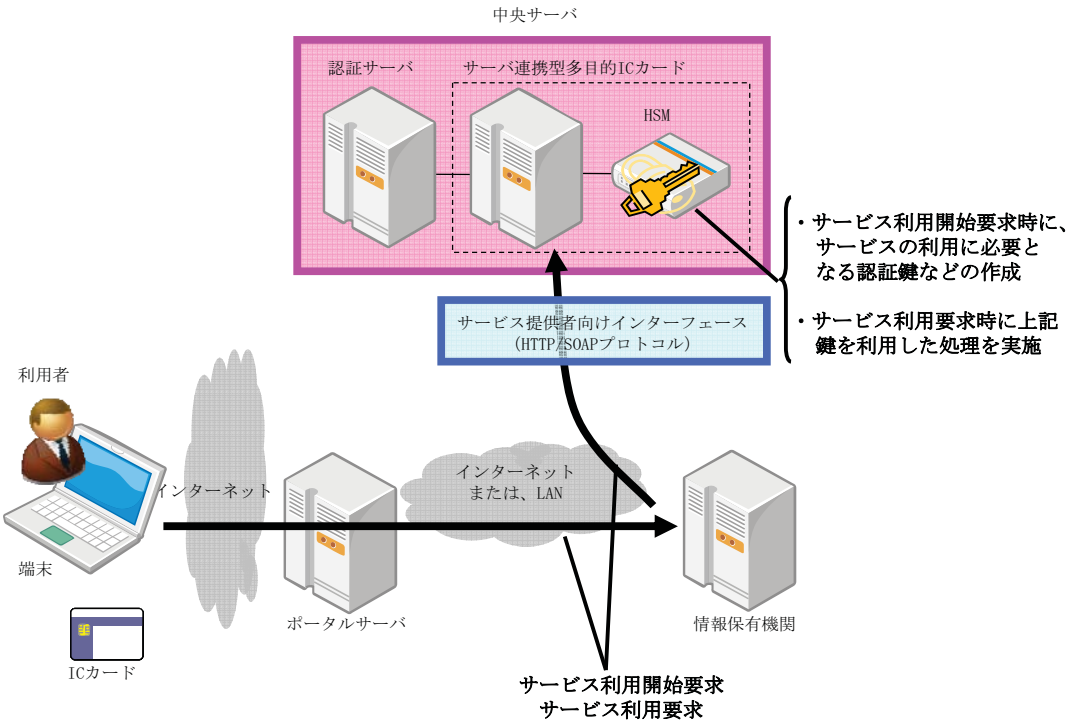


図 5-27 検証環境によるサービス提供者インタフェース

本検証により以下の確認を実施した。

① 利用者の簡易な操作によるサービス利用開始の検証

前述の「サービス提供者インタフェース」を用いて、情報保有機関がサーバ連携型多目的 IC カードと連携することにより利用者が新たなサービスの追加をブラウザの操作のみで簡易に行えることを確認した。

(i) サービス利用開始

利用者が、サーバ連携型多目的 IC カードで実行可能なサービスを追加するサービス。利用者の簡易な操作によるサービス利用開始を検証するため本サービスを準備する。

利用者はポータルを経由して新たに追加したいサービスの情報保有機関へアクセスしサービスの利用に必要な申請情報等を入力する。情報保有機関は入力された情報を元に、サーバ連携型多目的ICカードのインタフェースを用いサービスの追加要求を行い、サービスの利用登録を行うとともにサービスの実行に必要な鍵ペアを生成する。サービス利用開始のフローを 図 5-28 に示す。

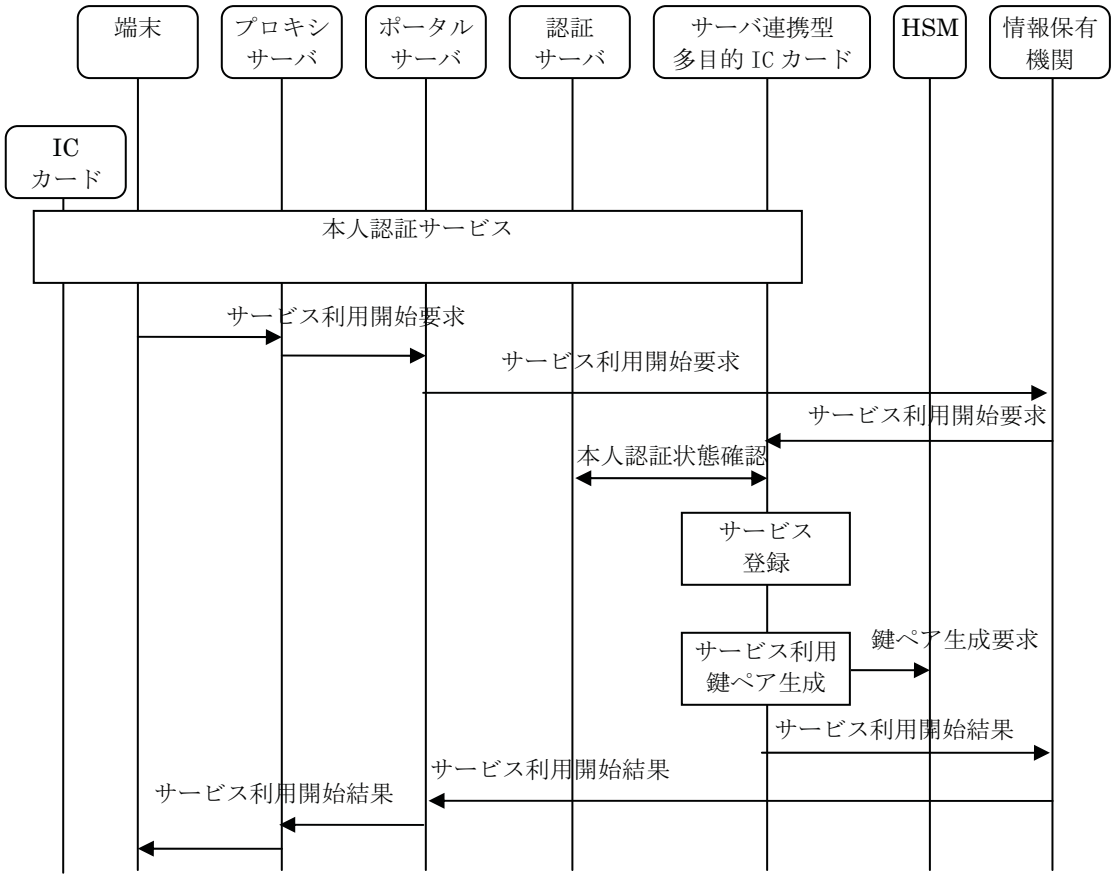


図 5-28 サービス利用開始フロー

（ii）サービス利用

利用者が、サーバ連携型多目的 IC カードに追加したサービスを利用するサービス。前述の「サービス利用開始」により開始したサービスの利用を検証するため本サービスを準備する。

利用者はポータルを経由し情報保有機関へアクセスしサービスの実行を要求する。情報保有機関は要求に基づきサーバ連携型多目的ICカードのインタフェースを用いてサービスの実行を行う。サービス利用のフローを 図 5-29 に示す。

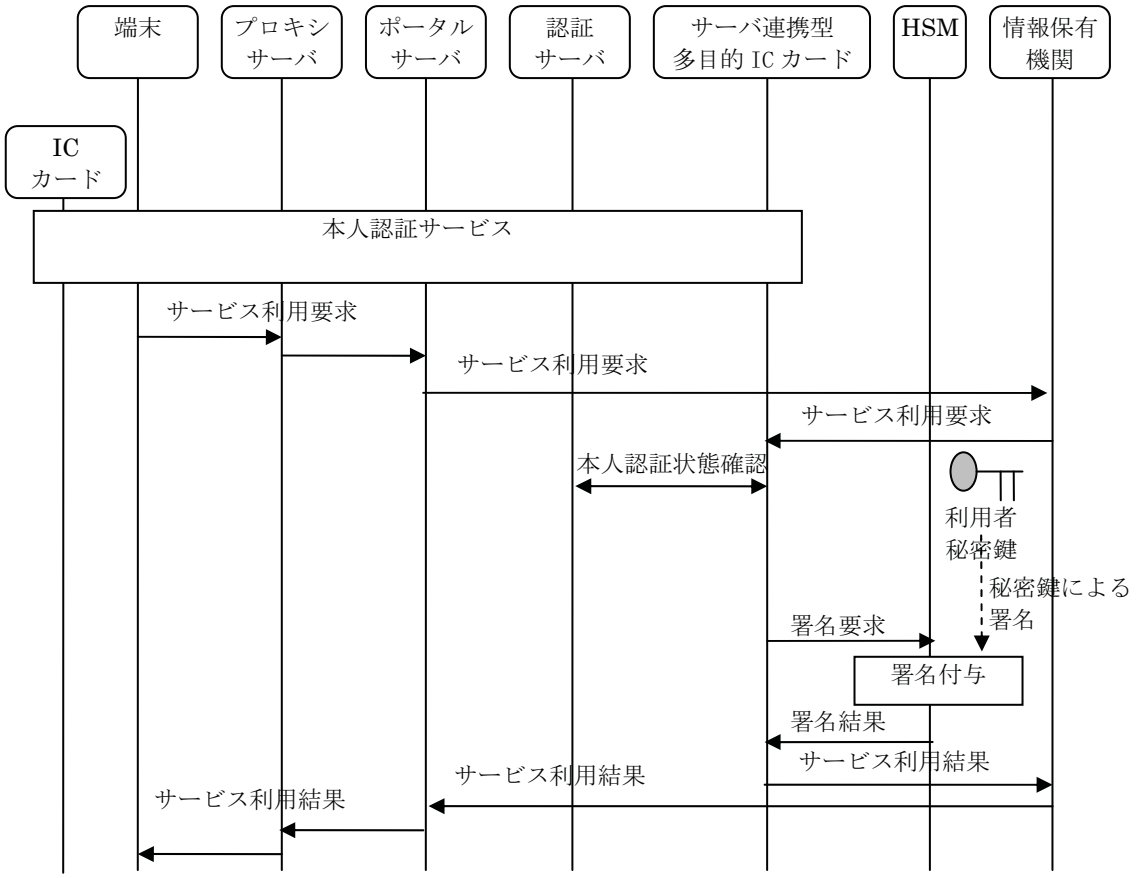


図 5-29 サービス利用フロー

上記検証結果により、IC カードではなくサーバ連携型多目的 IC カードへサービスの追加を行うことで、従来 IC カードの課題であったカードの記憶容量の制約によらず様々なサービスの利用が可能となるため、利用者はサービスの組合せを自由に選択できるようになる。また、本人認証機能のみでサービス追加の機能を持たない既存 IC カードを持つ利用者についてもサーバ連携型多目的 IC カードを利用した新たなサービスの利用が可能となる。

さらに自身の端末からのアクセスによりサーバ連携型多目的 IC カードへ新たなサービスの利用開始が可能となるため、従来 IC カードへのサービス追加で課題となっていたサービス追加の度に利用者が窓口へ赴く必要があるといった運用も解消され利用者の利便性を高めることができる。

上記により 2.3.1 でも示した現状のICカードの課題への対策としてサーバ連携型多目的ICカードの活用が有効であることを確認する

ことができた。

② インタフェースの検証

「サービス利用開始」インタフェースで実施される鍵ペア生成や、「サービス利用」インタフェースで実施される署名付与などは本来提供されるサービスの内容に依存したものとなる。

本検証では、サービスの内容に応じて任意のデータが利用できるような項目を設けることで、サービスに依存しない汎用的なインタフェースを準備することができた。具体的な項目について以下に説明する。

「サービス利用開始」インタフェースではサービスの内容に依存したデータを利用可能とするため「サービス利用開始情報」および、「サービス利用開始レスポンス情報」という項目を準備した。本インタフェースでは新たなサービスの利用登録を行うとともに、本項目を用いてサービスを利用するために必要な各種データの生成や登録を行う。例として、鍵ペアを用いて利用者宛のメッセージを暗号化して送信し、利用者がサーバ連携型多目的 IC カードを用いてこのメッセージを復号するようなサービスを想定する場合、鍵ペアの生成に必要となる鍵のアルゴリズムや鍵サイズに関する情報を「サービス利用開始情報」として設定し、生成された鍵ペアのうち公開鍵を「サービス利用開始レスポンス情報」として返却する利用が考えられる。(情報保有機関はこの公開鍵を用いてメッセージを暗号化する)

また、「サービス利用」インタフェースではサービスの内容に依存したデータを利用可能とするため「サービス利用情報」および、「サービス利用レスポンス情報」という項目を準備した。本インタフェースでは本項目を用いてサービスに依存した各業務を行う。例として前述のサービスを想定する場合、復号対象のデータを「サービス利用情報」として設定し、復号されたデータを「サービス利用レスポンス情報」として返却する利用が考えられる。

表 5-8、表 5-9 に各インタフェースの詳細を示す。

表 5-8 サービス利用開始インタフェース

分類	パラメータ	必須 ※	用途
リクエスト	サービス提供者 ID	○	リクエスト元のサービス提供者を識別するための ID
	サービス提供者パスフレーズ	○	リクエスト元のサービス提供者を認証するためのパスフレーズ
	サービス ID	○	サービス提供者の提供するサービスを識別する ID
	本人識別 ID	○	サーバ連携型多目的 IC カードが管理する本人を識別するための ID。本人との関連付けに利用。
	サービス利用者 ID	○	サービス提供者が利用者を識別するための ID
	サービス利用開始情報		各サービスの利用に必要となる情報。サービスの内容に依存した任意の情報が設定できる。
レスポンス	処理結果	○	リクエストした処理の結果を示す結果コード
	処理結果メッセージ		リクエストした処理の結果の内容を示すメッセージ
	サービス利用開始レスポンス情報		各サービス利用開始の際の結果として返却する情報。サービスの内容に依存した任意の情報が返却できる。

※○印は必須パラメータを示す。

表 5-9 サービス利用インタフェース

分類	パラメータ	必須 ※	用途
リクエスト	サービス提供者 ID	○	リクエスト元のサービス提供者を識別するための ID
	サービス提供者パスフレーズ	○	リクエスト元のサービス提供者を認証するためのパスフレーズ
	サービス ID	○	サービス提供者の提供するサービスを識別する ID
	業務種別 ID	○	サービスで実施する各業務内容を識別するための ID。サービスの内容として署名処理、情報復号処理など複数の業務が存在する場合、それらを識別するための用途を想定。サービスの内容に依存した任意の情報が設定できる。
	サービス利用者 ID	○	サービス提供者が利用者を識別するための ID
	サービス利用情報		各サービスの利用に必要となる情報。サービスの内容に依存した任意の情報が設定できる。
レスポンス	処理結果	○	リクエストした処理の結果を示す結果コード
	処理結果メッセージ		リクエストした処理の結果の内容を示すメッセージ
	サービス利用レスポンス情報		各サービス利用の際の結果として返却する情報。サービスの内容に依存した任意の情報が返却できる。

※○印は必須パラメータを示す。

③ 従来 IC カードと比較したサービス提供者のメリット

サービス提供者は前述の「サービス提供者インタフェース」を利用することによりサービスの利用開始や認証情報等の利用をサーバ側で実施することが可能となる。これにより 表 5-10 に示すメリットを享受することができる。

表 5-10 従来 IC カードと比較したサービス提供者のメリット

項目	従来 IC カード	サーバ連携型多目的 IC カード
アプリケーションやデータのサイズ管理	IC カード内で情報が管理されるため、容量の制約から IC カードに搭載可能なアプリケーションやデータについて厳格なサイズ管理が必要。	サーバ側で情報が管理されることで、容量の制約が緩和されるため、サービス提供者はサービス開発時のプログラム設計やデータ設計の負担が軽減される。
アプリケーション開発	IC カードの種類に応じたアプリケーション開発が必要。	IC カードの種類に依存しない開発が可能となるため開発コストが軽減される。
アプリケーションの更新	IC カードの配布(新規の場合)や個々の IC カードへのアプリケーションや認証情報等の書き込み(既存カード更新の場合)を行う必要がある。 また、IC カード毎にアプリケーションのバージョン管理が必要。	サーバ側で一括登録、一括更新が可能となるため、更新やバージョン管理のコストが軽減される。

項目	従来 IC カード	サーバ連携型多目的 IC カード
クライアント端末への専用アプリケーションの配布	サービス利用時の IC カードへのアクセスのために、専用のアプリケーションの開発および各クライアント端末へ配布が必要	サーバ側で処理が可能となるためクライアント端末へのアプリケーションの配布は不要

(4) HSM による鍵管理のスケーラビリティ検証

鍵管理について 5.1.4 (3) ①に基づきHSMで管理可能な鍵件数および処理性能への影響等について検証するため前述の検証環境を用い、HSMで鍵管理を行う環境を準備した。本検証で用いたHSMはHSM内部で管理されるマスター鍵により利用者の鍵情報が暗号化され、HSMにアクセスしているサーバ上のディスクに暗号化された利用者の鍵情報が保管される。

検証環境によるHSMでの鍵管理方法を 図 5-30 に示す。

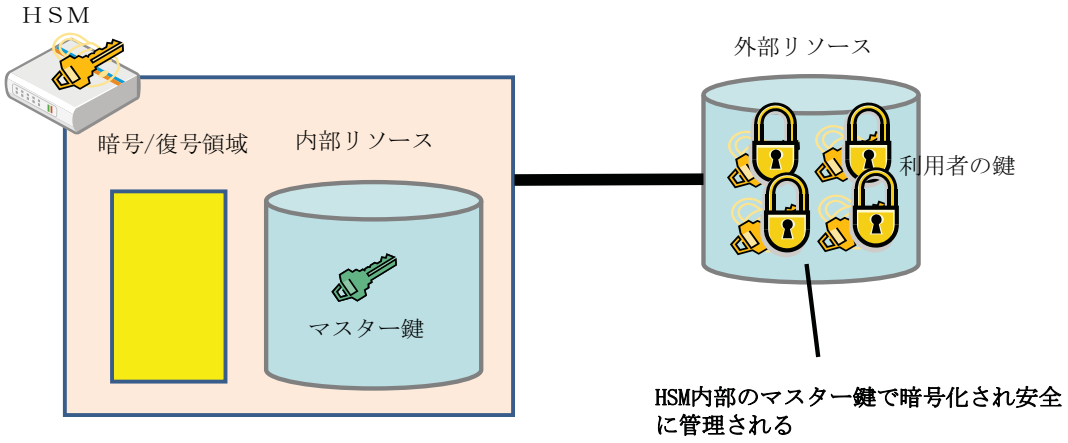


図 5-30 検証環境による HSM 鍵管理方法

本検証により以下の確認を実施した。

① 一般的なHSMで管理可能とされる数[1]を超える件数の鍵管理の実現可否

以下の条件の下、4 万件の鍵生成が実施できることを確認した。

- 各利用者につき、各サービスでの異なる用途を想定し 4 つの鍵ペア生成を実施
- 鍵ペアは RSA 1024bit 長の鍵ペア×2、RSA 2048bit 長の鍵ペア×2 を使用（サービス毎に異なるセキュリティレベルを想定し 1024bit と 2048bit の 2 種類の鍵長を使用）

また上記検証により以下の制限事項が検出された。

- 鍵生成を連続して行う場合、鍵件数が約 12,000 件程度で HSM 内部のメモリの枯渇によりエラーが発生する。（アプリケーションの再起動によるメモリのクリアが必要となる。）
- HSM へのログイン処理時に管理する鍵情報を HSM 内部のメモリにロードするため、管理できる鍵件数は HSM 内部のメモリサイズに依存する。今回 4 万件の鍵生成を行った際 1 件あたり約 1,500 バイト程度のメモリ消費が見られたこと、および製品の利用可能メモリサイズが約 63MB であることから約 42,000 件程度が上限と考えられる。

② 4 万件の鍵管理時における処理性能結果

以下の条件の下、鍵管理件数を 40 件(利用者 10 人分に相当)から 4 万件(利用者 1 万人分に相当)まで増加させた場合の処理時間を比較したところ特に HSM へのログイン処理で所要時間の増加が見られた。

- 鍵ペアは RSA 1024bit 長の鍵ペア×2、RSA 2048bit 長の鍵ペア×2 を使用(前述①と同様)
- 署名処理の鍵は RSA 1024bit を使用
- 測定対象はサーバ連携から HSM へのログイン、鍵の検索要求、署

[1] 「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）では「一般的には管理できる鍵の数は多くなく、高々数百のオーダーである」とされている

名要求に要した処理とする。

- 鍵管理件数は 40 件、1 万件、2 万件、3 万件、4 万件の場合それぞれについて測定する。

上記検証結果を 図 5-31 および図 5-32 に示す。

HSM へのログイン処理では、鍵管理件数が 40 件の場合、約 0.5 秒なのに対して、鍵管理件数が増加するにつれて処理時間も増加し 4 万件の場合は約 7 分 20 秒を要している。

また、鍵の利用(鍵検索＋署名処理)では、署名処理は鍵管理件数が増加しても一定なのに対し、鍵検索処理では鍵管理件数が増加するにつれて処理時間も増加し、40 件の場合、0.006 秒なのに対し、4 万件の場合 0.037 秒となっている。

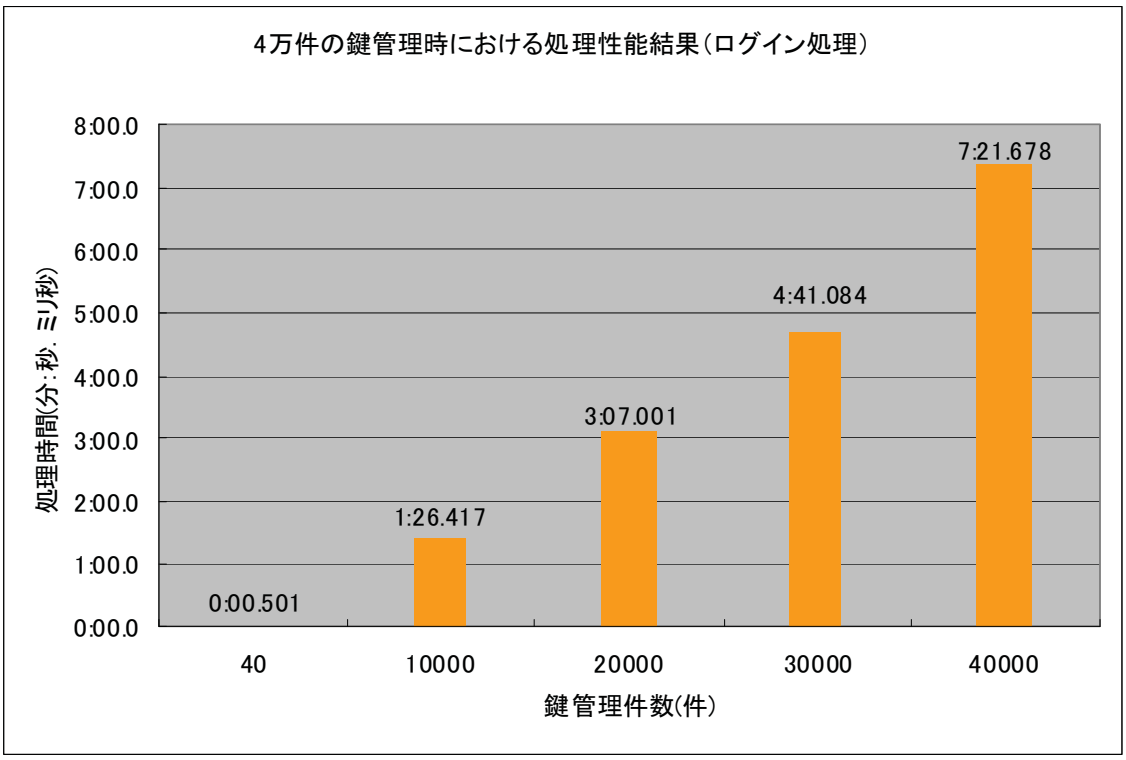


図 5-31 検証環境における鍵管理検証結果（ログイン処理）

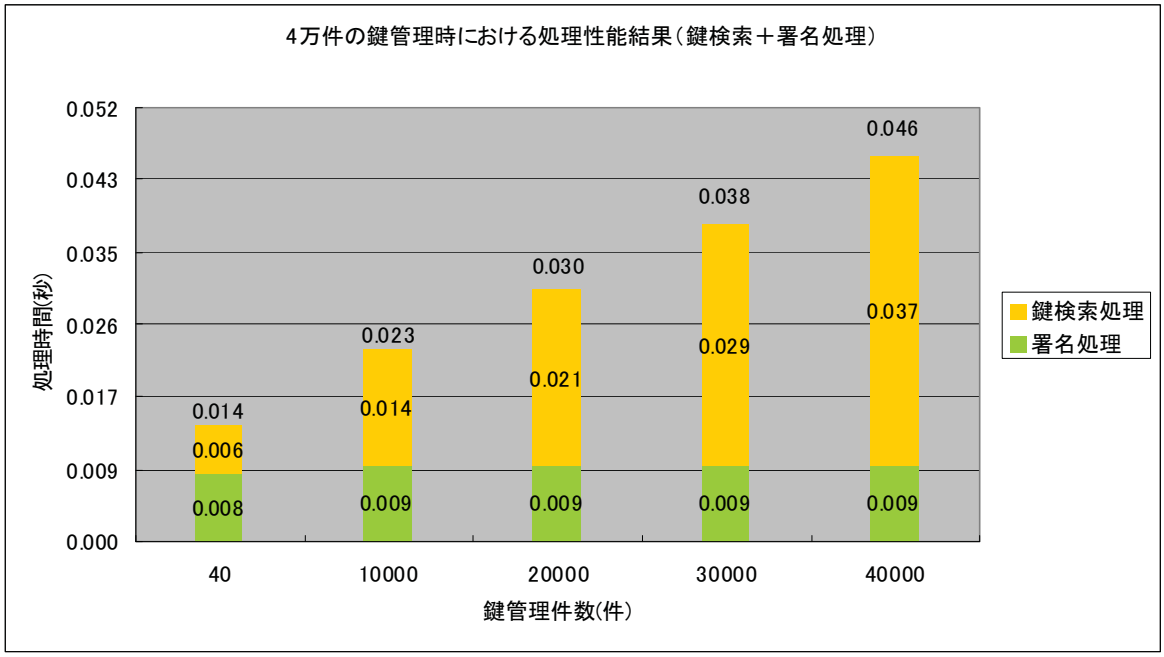


図 5-32 検証環境における鍵管理検証結果（鍵検索＋署名処理）

(5) サーバ連携型多目的 IC カードを用いた基本的なサービスのフィージビリティ検証

サーバ連携型多目的 IC カードを用いたサービスについては、「電子行政サービス等へのアクセス手段の多様化に関する調査研究報告書」（平成 20 年度総務省委託事業）で要求事項として「サービスの内容」が記述されているが具体的な検討までは行われていない。検証環境では、3 つの基本的なサービスを準備しサーバ連携型多目的 IC カードの適用について検証した。なお、従来の IC カードによるサービスと比較した場合の各機能の対応は付録 F で説明する。

① 本人認証サービス

利用者がポータルサーバにログインするために、本人認証を行うサービス。検証環境で準備した本人認証サービスのフローを 図 5-33 に示す。

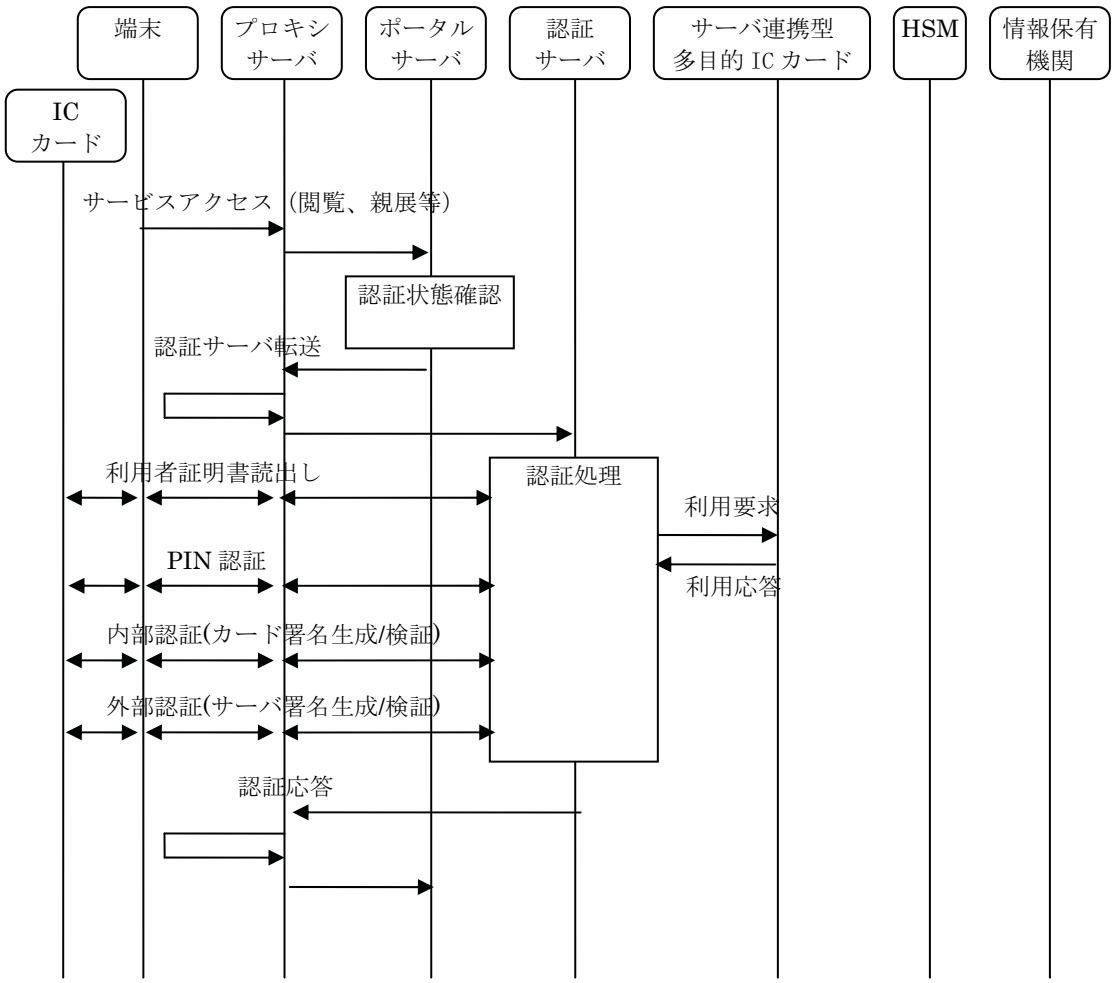


図 5-33 本人認証サービスフロー

認証サーバでの本人認証処理時にサーバ連携型多目的 IC カードと連携し、サーバ連携型多目的 IC カードを利用する意思確認を一度のログイン処理で行うことが可能となる。

また、ログイン後はポータルサーバが提供するメニューで暗号関連の処理を行う場合に、サーバ連携型多目的 IC カードが提供するインタフェースを使用して処理を行うことができる。サービス提供者が暗号関連の処理を独自に作りこむ必要がなく、以下の②申請サービスや③情報通知サービスのような、個人情報の安全な流通を必要とするサービスでの利用に適用できることを確認した。

なお利用者インタフェースに関して、前述の調査研究報告書では「現在使用されている IC カードを用いた主要なサービスと同等の利用者インターフェースが確保可能であること。例えば、電子行政

サービス等の利用時のアクセスカードである IC カードをリーダーライターのスロットに挿入する、リーダーライターにかざすなどの簡易な操作で本人認証が可能なことが要求される。」という要求事項が記述されている。本人認証については認証サーバにより従来の認証方式が利用可能であるため、従来と同等の利用者インタフェースを確保することが可能である。また、ログイン後は従来の IC カードの代わりにサーバ連携型多目的 IC カードが利用可能となるため、IC カード関する利用者の操作が不要となる。

② 申請サービス

利用者が、情報保有機関に対して申請情報を送信するサービス。本検証では「e-Tax」等のように利用者からオンラインで申請を受付ける申請受付サービスと、「公的個人認証サービス」のように、申請書等に対して利用者の秘密鍵により署名を行う署名付与サービスという 2 種類のサービスを想定する。検証環境で準備した申請サービスのフローを 図 5-34 に示す。

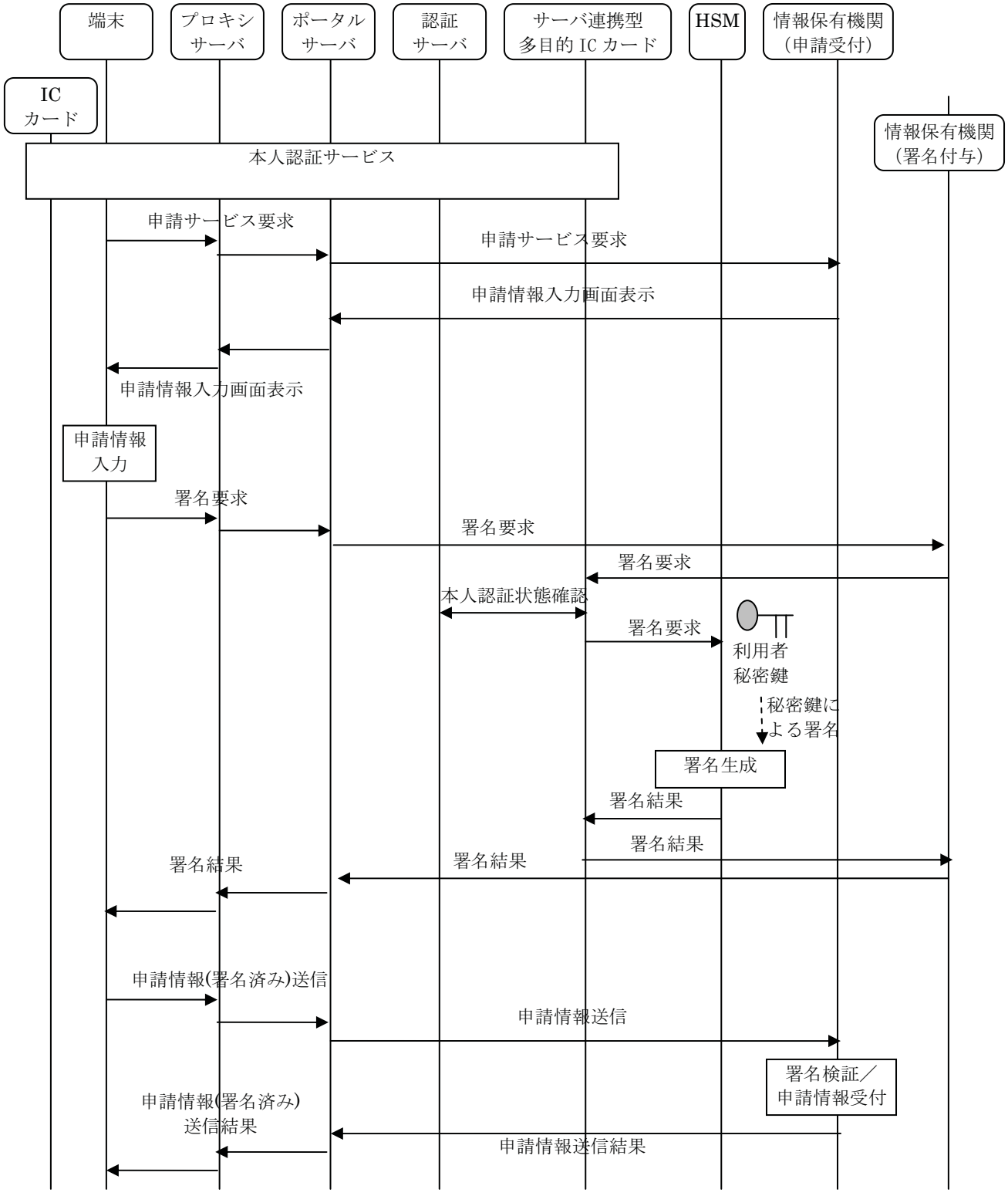


図 5-34 申請サービスフロー

利用者は本人認証サービスでログインした後に、サーバ連携型多目的 IC カードが提供するインタフェースを利用して、HSM で管理されている利用者の秘密鍵を使用した電子署名を付加することが可能である。

付加された電子署名は情報保有機関(申請受付)で検証され、もし申請情報に相違があれば検知することができる。

以上のように、利用者の申請情報送付にサーバ連携型多目的 IC カードを適用することで、利用者の申請情報に改ざんが無いかどうかを検証することができる。

③ 親展サービス

情報保有機関がある特定の利用者に対して個人に関連する情報を提供するサービス。本検証では親展情報を個人宛に配信する親展情報配信サービスと、個人宛に配信された各種親展情報を管理し、利用者に対して親展情報の閲覧を提供する親展情報管理サービスという 2 種類のサービスを想定する。検証環境で準備した親展サービスのフローを 図 5-35 および 図 5-36 に示す。

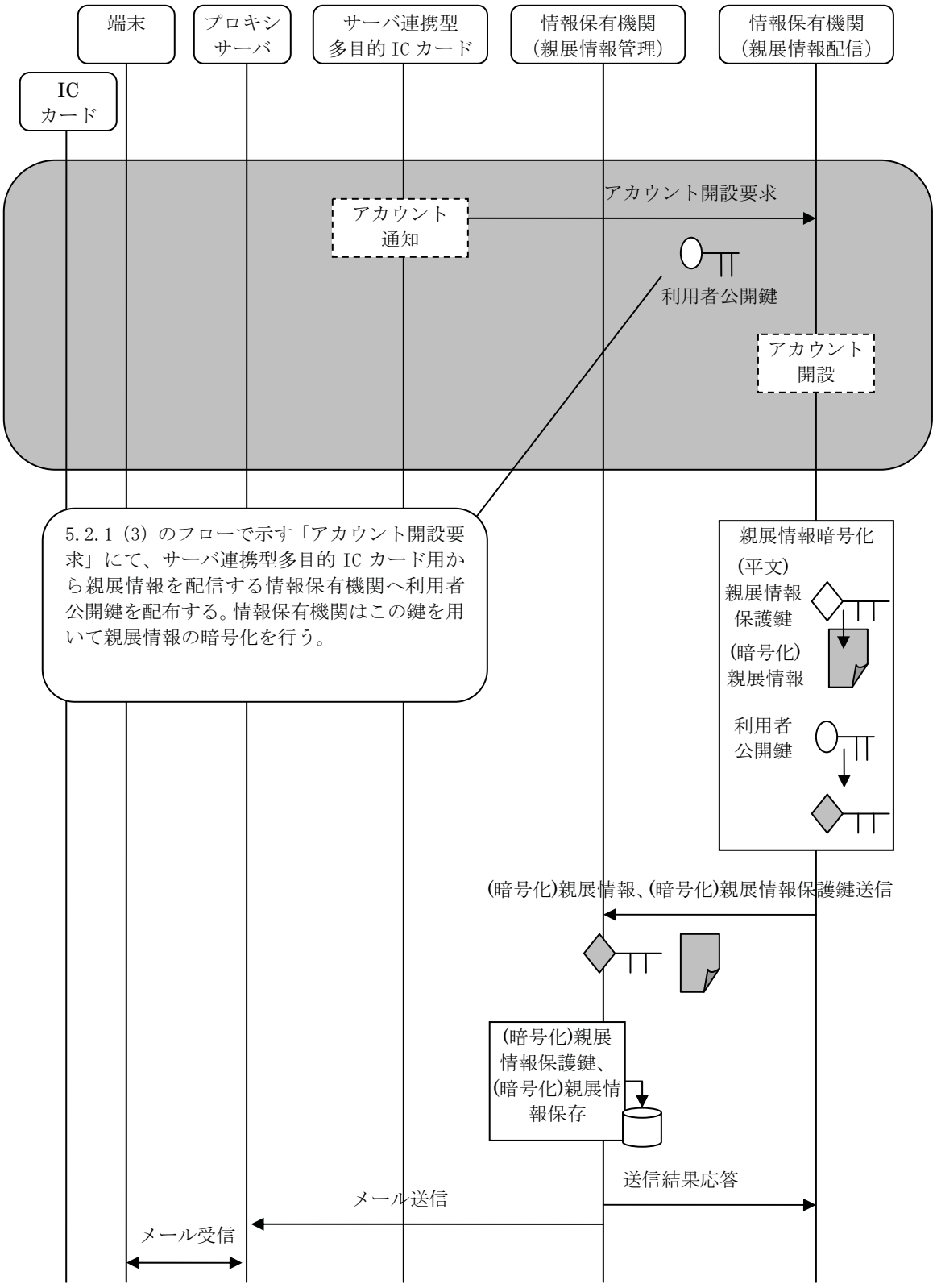


図 5-35 親展サービスフロー（親展情報の配信）

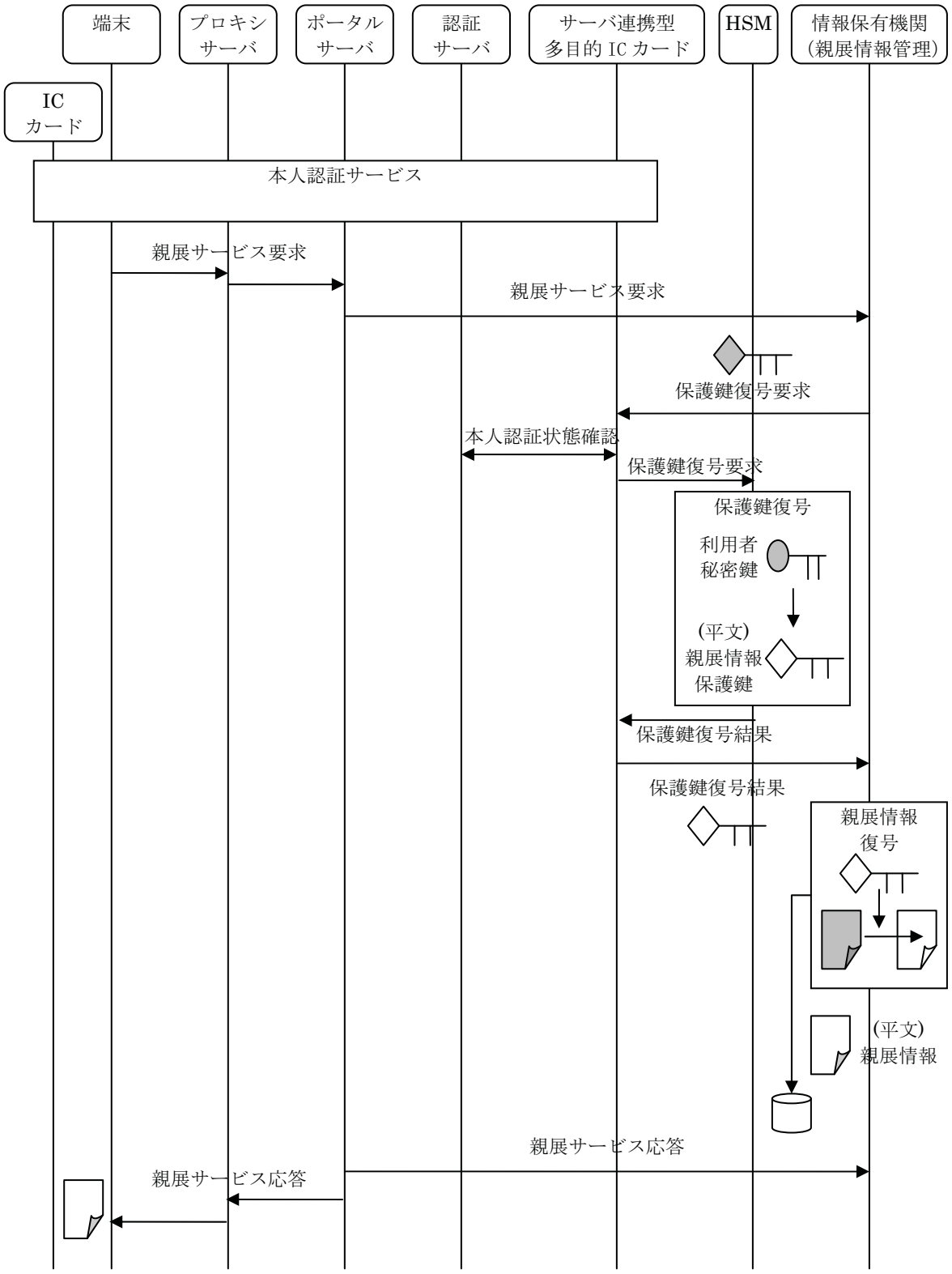


図 5-36 親展サービスフロー（親展情報の表示）

情報保有機関(親展情報配信)は、利用者の公開鍵を用いて親展情報を暗号化し、情報保有機関(親展情報管理)に送信する。

親展情報は利用者によって表示されるまで情報保有機関(親展情報管理)に暗号化された状態で保存されるが、親展情報を開封するのに必要な秘密鍵はサーバ連携型多目的 IC カードに保持されているため、親展情報の暗号が解読されて第三者に漏洩する危険を大幅に低減することができる。

以上のように、親展サービスにサーバ連携型多目的 IC カードを適用することにより、情報保有機関(親展情報管理)に安全に情報を送付・保管することが可能となる。利用者はポータルサーバにログイン後、サーバ連携型多目的 IC カードが提供するインタフェースを利用して、HSM で管理されている利用者の秘密鍵を利用して復号し、情報を安全に閲覧することが可能となる。

5.2.4 まとめ

本検証により、セキュアOSを用いたHSMへのアクセス制御を始め「5.1 課題の抽出及び対策の検討」にて検討した対策の有効性を確認するとともに、サーバ連携型多目的ICカードを用いた基本的なサービスのフィージビリティを確認することができた。

また、今回使用した HSM での鍵管理に関する以下の制約および制限事項が検出された。

① 管理可能な鍵件数に関する制限

今回使用した HSM では管理する鍵件数に応じて、HSM 内部で使用するメモリ量が増加するため、HSM で管理可能な鍵件数は HSM のメモリサイズに依存する。本検証では約 42,000 件程度が管理可能な鍵件数の上限となる結果となった。

また、連続して鍵生成を行う場合、HSM のメモリが枯渇し約 12,000 件でアプリケーションの再起動が必要となった。(HSM のメモリクリアのため)

② 所要時間の増加

今回使用した HSM では管理する鍵件数に応じて、処理に要する時間の増加が見られた。本検証では鍵管理件数が 4 万件の場合、鍵検索処理で 0.037 秒(40 件の場合 0.006 秒)、HSM へのログイン処理に約

7 分 20 秒(40 件の場合約 0.5 秒)の処理時間を要する結果となった。本結果について鍵検索処理は所要時間の増加は見られるものの、0.037 秒という処理時間は Web サービス等での利用を想定するとそれほど重大な制約とはならないと考えられる。HSM へのログイン処理に関しても、本処理は初期化や故障回復時等に必要となる処理であるため、運用するサービスにも依存するが通常の運用では問題にはならないと考えられる。

③ 運用に関する制約

今回使用した HSM のクラスタ構成では、1 台のサーバで認識できる HSM の台数に制限があるため、負荷分散における HSM の増設時の制約となる。また、 鍵生成など一部の処理は負荷分散の対象外となるため、アプリケーション側や運用での対策が必要となる。

処理性能の劣化や運用に関する制約については今後、具体的なサービスへの適用を検討する際にサービスに求められる運用条件や性能条件を踏まえ、これらの制約を考慮したアプリケーションの性能設計やシステム構成の検討が必要となる。

また管理可能な鍵件数に関する制限について、今回使用した HSM では鍵へのアクセスを即時に行うことや HSM の標準的な機能による実現を考慮して、全ての鍵を HSM 内部のメモリ上に展開して使用する方式により検証を行った。今回の検証では管理可能な鍵件数の上限は約 42,000 件程度という結果となった。昨年度の調査研究報告書では、管理可能な鍵は数百件程度となっていたが、今回の検証結果により小規模な自治体(人口 1 万人程度)であれば、すべての鍵をメモリ上に展開する方式であっても収容可能であることが分かった。しかし、中規模以上の自治体ないし、国レベルでの電子行政サービス等における利用者数を考慮した場合は、さらに大量件数の鍵を管理する必要があるため、鍵管理の方式を工夫する必要がある。大量件数の鍵管理を行う場合は、全ての鍵を HSM 内部のメモリ上に展開するのではなく、鍵へのアクセスが必要となる度に対象となる鍵のみを HSM 内部に取り込み使用するような方式も考えられる。このような方式を実現するための HSM は市中製品でも存在するが、HSM の標準的な機能ではないことや、製品個別の仕様となっていることなどから、製品動向については今後も注目しておくべきである。鍵管理の方式については、サーバ連携型多目的 IC カードを利用するサービスに求められる性能や規模、収容利用者数、同時アクセス数などを勘案し、適用する方式を検討する必要がある。

6. 実証実験(技術実証及び社会実証)の実施内容・方法の検討

国民がICTの利便性を真に実感できる国民本位の電子行政サービス等の実現のためには、あらゆる国民が、自宅のデジタルテレビやコンビニエンスストア等に設置されたキオスク端末など多様な端末からパソコンと同様に、24 時間 365 日・全国どこからでも、自らの健康・医療をはじめとする様々な情報を容易に閲覧・入手でき、かつ、活用できる環境が整備されることが望ましい。国民本位の電子行政サービス等の実現イメージを 図 6-1 に示す。

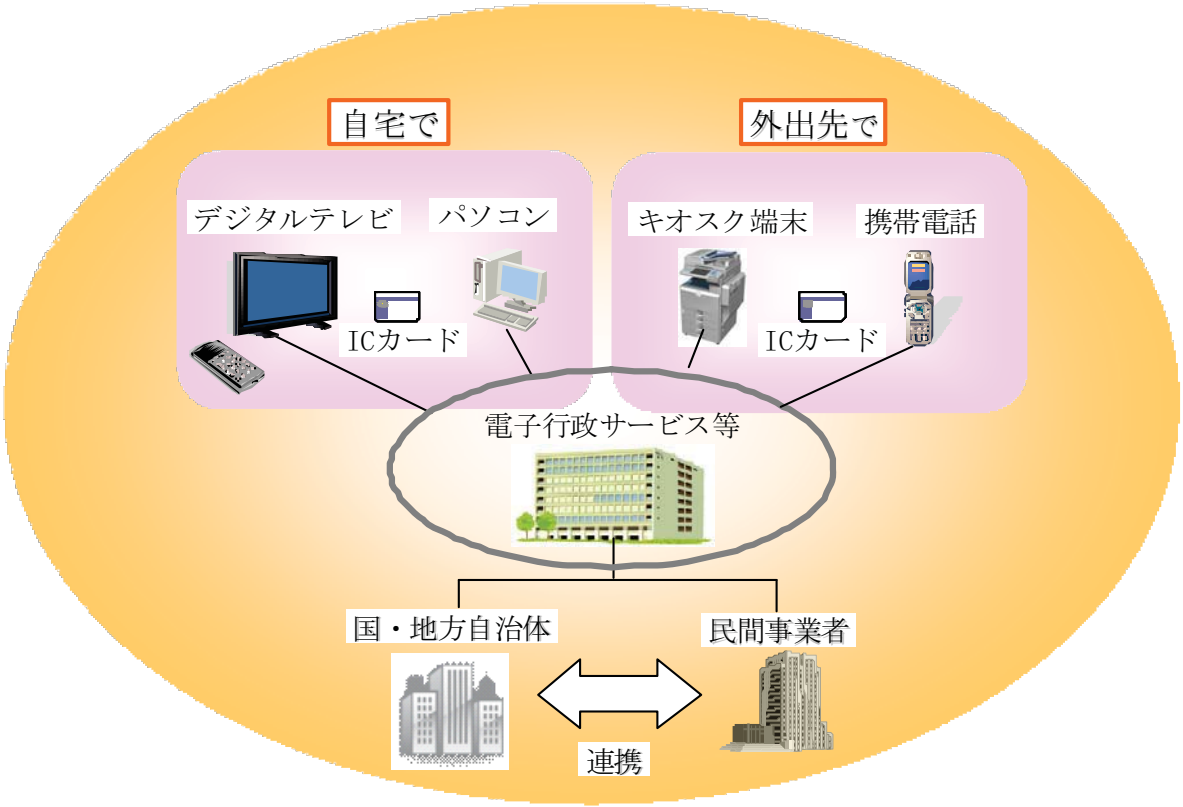


図 6-1 国民本位の電子行政サービス等の実現イメージ

本章では、上述のような、国民が ICT の利便性を真に実感できる国民本位の電子行政サービス等の実現に向けて、これまでの検討で抽出した課題の解決に向けた技術的実証実験及び一般利用者(モニタ)によるフィールド実証も含めた社会実証の実施内容及び方法について検討し、具体的に述べることとする。

6.1 （アクセス手段の多様化）デジタルテレビ

本節では、デジタルテレビから電子行政サービス等へのアクセスの実現に向け、そのステップとして必要と考えられる実証実験について述べる。

まず、本調査で明らかとなった、実証に向けて解決しなければならない課題に対し、技術的対策を検討し、その対策方法の妥当性を検証するための技術実証が必要と考えられる。

また、社会実証として、技術実証での検討結果を踏まえた上で、現状広く行われているパソコン向けサービスと同等の機能を、デジタルテレビに適したコンテンツとした擬似電子行政サービス等を構築する。この擬似電子行政サービス等を用い、一般利用者による基本機能の検証、ユーザビリティの検証を行うことで、本調査での対策の有効性の確認と、本調査では明らかにできなかった、デジタルテレビから電子行政サービス等へのアクセス多様化の実現にむけた課題の抽出が期待できる。

6.1.1 技術実証

本項では、本調査で明らかとなった課題に対して、必要と考えられる技術実証について述べる。今回行った調査結果から、電子行政サービス等へのアクセス多様化の実現に向けて、解決すべき課題や、さらなる検討が必要な項目をまとめる。続いて、その課題の解決のために必要と考えられる技術実証について述べる。

(1) 電子行政サービス等で想定される IC カードに関する検証

デジタルテレビから電子行政サービス等へのアクセスを実現するにあたって、どのような IC カードを利用するかについて、現在、公的に利用されている IC カードとしては、住民基本台帳カードや運転免許証、また IC チップが内蔵されているという点ではパスポートなどが挙げられる。本調査で行った実機検証では、IC カードに利用者の個人情報を保存し、それを利用することで、申請サービス等を受ける際のユーザビリティが向上することが明らかになった。本調査では、テスト用のカードを使用したが、サービスの実現化に向けて、電子行政サービス等との連携を前提とするカード仕様として、IC カード側、電子行政サービス等のサーバ側のそれぞれで、どのような情報を保持するかという棲み分けについても重要となる。また、現在発行されている公的 IC カードに保持されている情報をどのように利用できるかについての検討も、利用者の利便性から重要である。

このため、以下の技術検証が必要である。

・ 電子行政サービス等との連携を前提とした IC カードでの個人情報の保持方法の検討。ユーザビリティの観点からの利便性とセキュリティの観点も加え、IC カードでの保持の方法、サーバとの連携による保持方法の検討。また、どのような項目をどのようなセキュリティレベルで使用可能かの検討。

・ 運転免許証やパスポートなど、既存の公的 IC カードの利用可能性の検討。ユーザビリティの観点から見た場合では、カードの種別による自動判別が行えるか、また、今後発行されるカードについての互換性の可能性の検討。

(2) IC カードリーダライタ内蔵型リモコンの検証

IC カードリーダライタの接続形態について、リモコンに IC カードリーダライタを組み込んだ場合の検討が必要である。今回の IC カードリーダライタの接続形態に関する検証の中では、IC カードリーダライタを有線でデジタルテレビ本体に接続した場合について、試作機を用いて実際に IC カード情報の読み出し実験を行った。さらに、リモコンに IC カードリーダライタを内蔵することについても検討を行い、特に大画面デジタルテレビ利用時において、手元にあるリモコンで操作可能となることから、ユーザビリティの面からは、IC カードリードライタをリモコンに内蔵することを推奨する、と結論付けている。

しかしながら、リモコンに IC カードリーダライタを内蔵した場合における、リモコン操作をしながら IC カードをかざすなど、確実に読み書きできるための形状や通信方式の検討、省電力性の向上などについてはさらに検討する必要がある。

このため、以下の技術検証が必要である。

・ 無線機器との干渉に強い通信方式、および、省電力性の向上についての机上検討を行った上で、実際に IC カードリーダライタを内蔵した無線リモコンを試作し、基本的な動作確認、無線干渉についての評価。

・ 複数のリモコンのモックアップを作成し、IC カード利用時のリモコン操作とカードの読み取りの確実性の検討を行う。

(3) デジタルテレビ向けコンテンツの検証

現状の電子行政サービス等がパソコンからの利用を想定したコンテンツ配信を行っており、デジタルテレビからの操作では、操作性が悪いという課題がある。電子行政サービス等へのアクセス多様化では、様々な端末からのアクセスが想定されるため、それぞれの端末にあったコンテンツが必要となる。そのため、現行のデジタルテレビからのアクセス

を実現するには、デジタルテレビ向けのコンテンツ作成ガイドラインに従ったコンテンツの作成が課題となる。

このため、以下の技術検証が必要である。

- パソコン向けに作成された、現行の電子行政サービス等の一部をデジタルテレビ向けに作成し直し、デジタルテレビからの申請操作が確実かつ容易に行えることを確認する。
- パソコン向けサービスコンテンツからデジタルテレビ向けサービスコンテンツの変換を行い、必要となる工数の調査、自動変換の実現可能性の検討を行い、技術的なノウハウを検討する。

(4) デジタルテレビの入力デバイスの検討

今回の検証においては、デジタルテレビに付属するリモコンを用いて実際の文字入力を行うことで、操作性の検証を行った。デジタルテレビではUSB接続端子が搭載されるようになっており、パソコン向けに販売されている各種周辺機器が使用できる可能性が出てきている。このように、パソコン向けの周辺機器などを使用して、デジタルテレビのユーザビリティを高めることが課題である。

このため、以下の技術検証が必要である。

- 現状のリモコンを用いる範囲でも、良く使用する文字列を、リモコンやデジタルテレビ本体に登録し文字入力を行う検討
- パソコン向けに販売されている周辺機器、キーボード、マウス、タブレット等を、入力手段として使用できるかの検証。
- 現在、USB 接続が主な接続方法となっているが、Bluetooth などの無線による接続の検証。
- 携帯電話等外部のデバイスからの入力の検討
- このほか、ユーザの視線や、音声、ジェスチャなどの、多様な入力方式の検討。

(5) ワンストップ化に向けた検証

デジタルテレビからの電子行政サービス等の利用を拡大させるためには、一連の手続のワンストップ化を検討する必要がある。電子行政サービス等で想定されるサービスの一連の流れとしては、ユーザ認証、サービス選択、申請、電子署名、決済できる機能が求められる。現状デジタルテレビでは、電子署名の機能が搭載できていないことや、今回調査を行った東京電子自治体共同運営サービスにおいては、申請料などの決済の仕組みは見受けられないことから、デジタルテレビでのワンストッ

プ化についての検証が必要となる。

このため、以下の技術検証が必要である。

- デジタルテレビでの電子署名対応の機能検証
- デジタルテレビでの小額電子決済が利用できるか、またその際のユーザビリティに関する検証
- デジタルテレビでの証明書の交付の可能性について必要な機器と要件の検討とその検証

(6) 放送との連携によるアクセシビリティの検証

住民からの電子行政サービス等へのアクセスをより簡便にするために、さらに検討が必要である。本調査では、デジタルテレビ向けポータルサイトから電子行政サービス等へのリンクを張るなどによって、アクセシビリティの向上が行えることを確認しているが、いずれもユーザの能動的な動作が必要となっている。

デジタルテレビ本来の放送を受信する機能と連動させて、テレビ視聴中に個人個人に対するお知らせを出せるようにするなど、放送との連携により、より広く、もれなくアクセスが可能になることが想定される。

このため、以下の技術検証が必要である。

- デジタル放送に多重化されているコンテンツに電子行政サービス等へのリンクを含むことにより、電子行政サービス等へのアクセスが可能になること。
- 2.1.6 の現状を踏まえ、B-CAS カードや DRM-ID を用いて個人とデジタルテレビの紐付け方法の検討を行い、ユーザビリティが向上できるかの検証
- デジタルテレビは共用されることを前提とし、放送事業者や IPTV サービス事業者と連携し、放送を用いて個人への情報更新通知を行う方法を検討し、個人に向けた情報発信が可能かの検証

6.1.2 社会実証

以上で述べたそれぞれの技術実証の結果を踏まえ、デジタルテレビから電子行政サービス等へのアクセスの実用に向け、一般利用者による社会実証が必要と考える。

社会実証の検証環境例を以下の 図 6-2 に示し、その構成の例を 表 6-1 に示す。

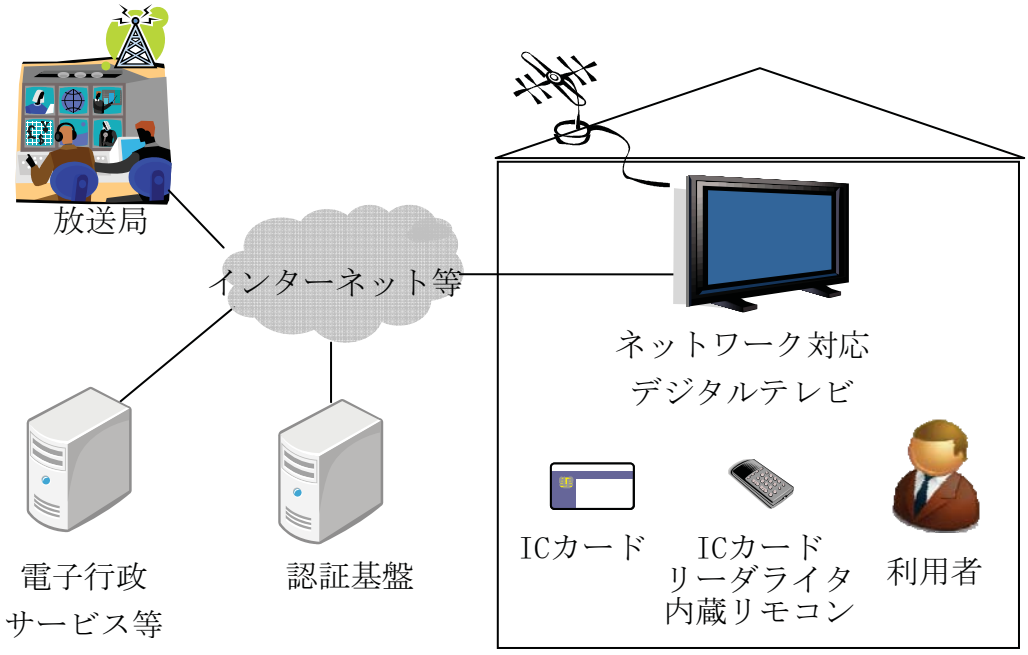


図 6-2 社会実証のイメージ図

表 6-1 社会実証の構成例

構成要素	説明
電子行政サービス等	国や自治体が蓄積している個人情報の提供や、電子申請を受けるサービス
放送局	電子行政サービス等からの情報を放送に多重化して放送を行う
認証基盤	IC カードを用いて個人認証を行うための認証基盤
ネットワーク対応デジタルテレビ	IC カードリーダライタへのアクセスに対応したネットワーク対応のデジタルテレビ
リモコン	IC カードリーダライタを内蔵したリモコン
IC カード	Type-B 準拠の電子行政サービス等との連携を前提とした IC カード

社会実証においては、技術検証を踏まえ、一般利用者が、電子行政サービス等へアクセスし、ユーザ認証、サービス選択、申請、電子署名、決済までの一連の手続を含む申請サービスを行う場合について、下記の観点での検証を行う必要がある。

- 一般家庭におけるデジタルテレビの設置場所について、リビングに設定されている場合や、個部屋に設置されている場合において、そのユーザビリティについて問題なく行えること。
- デジタルテレビは、その大きさの範囲が広いため、大型テレビから小型テレビまで、どのテレビのサイズにおいても、問題なく手続が行えること。
- IC カードリーダライタを内蔵したリモコンにおいて、確実に操作が行えるか。
- 入力デバイスとしてどのようなものが利用しやすいか

また、デジタルテレビからの電子行政サービス等の利用に関しても、ユーザの意識調査が必要である。具体的には、

- デジタルテレビでは、どのような電子行政サービス等を利用したいか
- デジタルテレビで利用する場合に、どのような機能があれば便利か
- パブリックスペースでの利用の可能性、その場合の制限事項

など、ユーザの意識なり要望をサービスの実現に向けて反映してゆくことが必要である。

6.2 （アクセス手段の多様化）キオスク端末

本節では、キオスク端末から電子行政サービス等へのアクセスを実現するために必要となる実証実験について述べる。

実証実験においては、4 章で明らかになった課題のうち机上検討となっている技術的対応策の検証を行うとともに、電子申請を含む電子行政サービス等へのアクセスを想定した実証システムを構築し小規模なモニタによる評価を行う。これによって、実運用に向けた技術的対策の妥当性や利用者及び行政側許容性の検証が可能となり、更なる課題の抽出、解決を図ることが期待される。

原口ビジョンで示されている 24 時間 365 日いつでもどこでも簡単に電子行政サービス等を受け付けられる姿を想定すると、キオスク端末の場合には自宅にパソコンを持たない人の利用が見込まれるため、その前提に立った実証実験が重要となる。

6.2.1 技術実証

技術実証においては、主として 4 章で検討した技術課題に対する解決策の実現性等検証すべき項目と、さらに検討が必要となる技術的な項目について述べる。

(1) キオスク端末の電子行政サービス等へのアクセス方法

将来の姿を見据えると、多くの電子行政サービス等がキオスク端末を通じて簡単に利用できることが必要となる。そのためには、

- 認証基盤及び IC カードを利用して統一的な電子認証基盤に基づいて電子行政サービス等が受けられること
- 現在行われている証明書の交付については交付対象となる証明書の範囲を広げること
- 電子申請が可能となること
- 情報参照が可能となること

が必要となる。

① 電子認証基盤との連携の検証

現在は証明書の交付を前提とした認証が行われているが、広く電子

行政サービス等で利用するためには、公的な個人認証サービスを用いて電子行政サービス等が利用可能であることが必要となる。本研究では PKI を前提として同等の認証基盤を利用可能であることを検証したが、実際の公的な電子認証基盤に基づいた認証によるサービス提供が実現できることを確認する必要がある。

② 様々な証明書の交付の検証

現在実施されているコンビニに設置されたキオスク端末において可能な証明書の交付は、住民票と印鑑証明である。個別の自治体では実現している、税に関する証明、戸籍に関する証明など様々な証明書に広げる必要がある。また、将来の紙の証明書から電子の証明書の証明書への移行も見据えた形での技術検証を行う必要がある。そのため、様々な現状の紙の証明書をキオスク端末で交付するための検証と、将来の電子証明書との共存を前提とした検証の２つの観点から検討を行い、実現性を検証する必要がある。

- 多種の証明書交付に必要な要件の整理と、紙による多種の証明書交付が可能であることの検証
- 将来の電子的証明書との共存を前提とした場合の紙の証明書のあり方の整理と、それに基づいた証明書交付の検証

これらの検証においては、制度的な検討に合わせた技術検証が必要となる。

③ 電子申請の検証

本調査研究の調査結果によると、2.2.4(4)に示したように、現在の電子申請はパソコンを前提としている。一部携帯電話での電子交付が始まっているが、いつでもどこでも電子行政サービス等を利用できるという観点からは、限定的なユーザインタフェースという条件の下でキオスク端末を利用した申請を実現することが重要である。そのため、本研究では個人の属性情報の活用と、紙を合わせて活用する方法を 4.1.4 で示した。

（i）利用者情報を活用した申請

4.1.4(1)で示したように多くの電子申請で、本人の氏名、性別、住所、生年月日、連絡先（電話番号やメールアドレス）等の属性情報の入力が必要になっている。これらの情報を電子行政サービス等で安全に保持し、申請の際に活用できれば申請の効率が上がると考えられる。このような方法を実現するに当たって必要となる、セキュリティ上の要件、運用上の要件を明確にし、実現性を検証する必要がある。

（ii）紙を活用した申請

4.1.4(2)で示したように、個人の基本的属性以外にも入力が必要となる申請の場合、電子情報と関連付けられた紙を活用して申請を行う方法について説明した。（i）の方法も合わせて実現すると電子的な機器の入力に慣れない人に効果を発揮すると予想されるので、電子申請の仕組み自体も含めて検証する必要がある。

現在電子申請が行われていない申請について検討すると、第三者が作成した添付書類が必要である申請が多く見受けられる。これらを含めた電子申請を実現する手段として、前述の個人属性情報を印刷した申請書本体と紙の添付書類を合わせてスキャンすることにより申請を行う方法が考えられる。電子申請の範囲を広げる観点で、その実現性を検証する必要がある。

（iii）他の電子メディアを活用した申請

申請によっては、デジタルカメラなどの電子ファイルを添付する申請も想定される。キオスク端末でこのような申請を行う際の実現方法について検証する必要がある。

④ 情報参照の検証

本調査研究の調査結果によると、2.2.4(4)に示したように、現在個人の情報参照は限定されており、パソコンで参照することを前提としている。キオスク端末での情報参照に当たっては、限定されたユーザインタフェースに表示を行う場合と、印刷を行う場合とが想定されるので、両者に対応した情報提供の方法の実現性を検証する必要がある。

(2) セキュリティの検証

キオスク端末の場合には第三者が立ち入ることのできる場所に設置されるため、個人の情報を参照する場合には、キオスク端末内の情報の取り扱い、表示の際の配慮などプライバシー情報を様々な形で保護する必要がある。特に利用者の不安を取り除くためには、表示されている情報の閲覧時のプライバシー保護の検証が重要となる。表示される情報が第三者に見られにくい配置にキオスク端末を設置するだけでなく、4.1.3(2)②に情報表示における技術的な対策として表示を変化させて警告を与える方法や表示せずに直接印刷する方法等を示したが、その検証が必要となる。

(3) ユーザビリティの検証

特に高齢者はパソコン等のデジタル機器を使い慣れないだけでなく、

身体的な問題により表示が見にくかったり入力がしにくいという状況が想定される。そのような場合にも、利用者がなるべく抵抗なく端末操作を行える必要がある。紙を活用するインタフェースについては（ii）に述べたとおりである。さらに、高齢者や障がい者等の利用者の身体的な特徴を配慮して個人にあったユーザインタフェースを提供できる可能性を 4.1.4(4)に示している。利用者が必要とするユーザインタフェース情報をカードあるいは電子行政サービス等に保持し、その情報に合わせたユーザインタフェースを実現することにより、利用者の利便性が向上することを検証する必要がある。

(4) 耐久性の検証

現在のキオスク端末は、画面での利用と印刷が中心となっている。上記で示した申請に使った場合には紙をスキャンして入力する操作も入るため、スキャンを含めた耐久性について検証する必要がある。コンビニ等の第三者が立ち入ることのできる環境における印刷、スキャンを含めた端末の耐久性に関し、評価方法の検討とそれに従った検証を行い、評価法の妥当性を検証する必要がある。

6.2.2 社会実証

社会実証おいては、6.2.1 で述べた技術的な検証を踏まえ、利用者の許容性、運用上の課題に対する課題の確認と解決を行う。利用者の観点からの許容度評価などの事項については、将来の実施を模した環境で、小規模なモニタによる評価を行う。また、本研究の中では、単一の電子行政サービス等をキオスク端末で利用する際の検証を限定的な検証環境で行っているが、社会実証においては、複数の電子行政サービス等を想定するとともに、実際の利用シーンに近い環境でデジタルテレビやキオスク端末など複数の種類の端末にて実証を行うことが望ましい。

(1) 交付手続等電子行政サービス等の標準化

多様なアクセス手段を用いて多種の電子行政サービス等を提供する場合には、利用者の利便性を意識する必要がある。特に提供される各サービスで統一性のない表示や手順が採用されると、利用者の操作性を損なうことになる。現在都道府県単位で電子行政サービス等用のポータルを準備する自治体が増えており、都道府県単位では電子行政サービス等の提供方法が統一されつつある。それを 1 歩進め、全体として同じ形で多様なアクセス手段に対応した電子行政サービス等を提供するのに必要な要件手順を示す必要がある。

- 電子行政サービス等間の統一性確保のためのガイドライン

(2) セキュリティ

自治体の設置する自動交付機に関しては、「自動交付機の安全対策等に係る通知」が出されている。キオスク端末においてもその通知との整合性を検証する必要がある。またプライバシー保護に関しては、モニタによる評価を実施し、実現方法の有効性を検証する必要がある。

- 「自動交付機の安全対策等に係る通知」との整合性検証
- プライバシー対策に対する利用者の評価及び許容度の検証

(3) ユーザビリティ

普及のためには、利用者の利便性確保が重要な項目となる。コンビニでの証明書交付が注目を浴びているので、申請と情報参照を含めた電子行政サービス等全体としてのユーザビリティを検証する必要がある。ユーザビリティの検証においては、実際の利用者による評価が重要であるため、モニタによる評価を実施し、実現方法の有効性を検証する。

- 限定的な表示機能・入力機能を持った場合のユーザビリティに関して、モニタによる評価を行い、検証する。
- 紙を活用した入出力を利用する場合のユーザビリティに関して、モニタによる評価を行い、検証する。
- モニタによるキオスク端末の利用時間（占有時間）に関する評価を行い、想定した端末機能の有効性を検証する。
- 利用者の特性に合わせたユーザインタフェース提供によるユーザビリティ向上に関して、モニタによる評価を行い、検証する。

(4) コスト負担のモデル

印刷が関連する場合には、紙やインク・トナー等消耗品コスト負担が課題の一つになる。証明書等は一部利用者の負担となることで受け入れられるが、情報参照の際に印刷した場合のコスト負担のモデルを検討し、その許容度を含めた実現性を評価する必要がある。

6.3 中央サーバに認証機能を一部移行させる方式

本節では中央サーバに認証機能を一部移行させる方式の実用化に向けて、今後必要と考えられる実証実験について述べる。

実証実験においては、まず 5 章で明らかになった課題のうち机上検討となっている対策の検証および実機検証により抽出された制約や制限に対する対策の検討および検証等の技術実証が必要となる。

また社会実証として、技術実証での検討結果を踏まえた上で、中央サーバに認証機能を一部移行させる方式を活用した電子行政サービス等を想定した実証システムを構築し、一般利用者によるユーザビリティや全体運用の検証を始めシステムのスケーラビリティ、サービス提供者への影響等について検証を行うことで本調査研究や技術実証で検討した対策の有効性の確認と実現に向けた更なる課題の抽出、解決を図ることが期待できる。

6.3.1 技術実証

本項では、実験室レベル等による技術的な検証、評価が必要と考えられる内容について整理する。

(1) 認証サーバでの認証結果を用いて情報保有機関と利用者認証を行う方式

一度の本人認証で複数のサービスを利用可能とするため、実際に複数の検証用サービスを用意し 5.1.3 (3) ③で示した方式の活用等により、情報保有機関とサーバ連携型多目的ICカードとの間での利用者認証の検証を行う。

また、要求されるセキュリティレベルがサービス毎に異なることを想定し、本人認証に使用した認証方式のセキュリティレベルに応じてサービスの利用可否が制御できることの検証も必要となる。

(2) 各サーバ間のセキュリティ・信頼性の確保方式

今回の実証実験は 5.2.1 の 図 5-1 で示したシステム構成で実施したが、将来の実運用の段階では、ポータルサーバと情報保有機関を結ぶネットワーク、及び、情報保有機関同士を結ぶネットワークについては、専用線のようにセキュリティと信頼性が確保された回線だけではなく、信頼性の劣る公衆のネットワーク上で運用される可能性も考慮してお

く必要がある。そこで、各サーバ間でやりとりされるメッセージについて、より強固なセキュリティとトランザクション性の確保を検討・検証しておく必要がある。

(3) 大規模な認証情報の管理方式

利用者の認証情報の管理は高いセキュリティによる保護が求められるが、セキュリティを確保した上で大規模な利用者数を想定した管理方式の検討が必要となる。HSM を効率的に活用する方法等の検討を踏まえ大規模な鍵管理の検証が必要となる。また認証情報の管理方式に応じて、冗長構成や負荷分散構成への適用および処理性能についてもあわせて検証しておく必要がある。

(4) 認証情報のバックアップ方式

機器の故障・破壊・紛失等による情報逸失への対策としては定期的なデータのバックアップやリストアの運用整備が必要となる。特に利用者の認証情報については耐タンパー装置等による高いセキュリティにより保護されているため、5.1.4 (3) ②で示したHSMで管理する鍵のバックアップ方式の活用等により安全なデータの保管を考慮したバックアップ方法の検証が必要となる。

またフルバックアップ、差分バックアップ、増分バックアップなど適用可能なバックアップの形式を検証するとともに、バックアップやリストアに要する処理時間を測定し、実運用におけるバックアップ/リストア計画策定の基礎データとして活用できるようにする必要がある。

6.3.2 社会実証

本項では、小規模なモニタ形式や一定規模のフィールド等により検証、評価が必要と考えられる内容について整理する。

(1) アカウントのライフサイクル管理

サーバ連携型多目的 IC カードのアカウント開設からアカウント廃止に至る各ライフサイクルに伴う一連の処理フローを検討する。具体的にはアカウント開設に伴う利用開始申請、IC カードの発行・交付や、本人認証に用いる IC カード紛失時に伴う通知、認証情報等の一時利用停止、

およびICカード内の証明書失効時に伴う証明書更新手続などを考慮し、利用者やサービス窓口担当者等の運用や関連機関とのインタフェースを検証する。

(2) ICカード利用におけるユーザビリティ

小規模なモニタ形式にて、従来のICカードを用いたサービスとサーバ連携型多目的ICカードを用いたサービスのユーザビリティを比較検証する。検証の際は操作性だけでなく、各種ネットワークの相互接続等に伴う処理時間(体感)の考慮も必要となる。またこれに伴いサーバ連携型多目的ICカードの活用に適したサービスの検討を行う。

(3) サービス提供者への影響

既存サービスをサーバ連携型多目的ICカードを利用する方式に移行する場合の既存システムへの影響を検証するとともに、インタフェースの整備など導入に伴うシステムへの負担を軽減する方法を検討する。またサービスの開始や利用停止、廃止など運用への影響も検証が必要と考えられる。

(4) スケーラビリティ

電子行政サービス等の本格稼動に向け、一定規模のフィールドにより管理データやアクセス数の増加に伴うシステムの処理能力等の検証が必要となる。また本検証に伴いサーバやストレージの分散等を考慮したシステム全体の構成についての検討も合わせて行う必要がある。

6.4 アクセス手段の多様化と、中央サーバに認証機能を一部移行させる方式の連携

アクセス手段の多様化と、中央サーバに認証機能を一部移行させる方式は、独立な技術要素であるが、両者を連携して利用できることが、電子行政サービス等の利便性向上にとって重要と考える。

中央サーバに認証機能を一部移行させる方式（サーバ連携型多目的ICカード）を用いると、従来、ID／パスワードやICカードのように利用者と直接行っていた利用者認証を、中央サーバに対して実施することとなるため、デジタルテレビやキオスク端末における認証方式に係るユーザビリティの

課題を解決することができる。

また、6.1 節や 6.2 節では、デジタルテレビやキオスク端末の限定的なユーザインタフェースという条件から、個人属性（氏名、住所等）を、IC カードまたは電子行政サービス等の情報から引用することが提案されている。サーバ連携型多目的 IC カードでは、IC カードと同様に利用者に係る情報を耐タンパー領域に格納することが可能であるため、このような目的に使用される場合の保守・運用性を評価することが重要である。

本節では、このようなアクセス手段の多様化と中央サーバに認証機能を一部移行させる方式の連携に関する検証について、具体的な検証項目を提案する。

6.4.1 技術実証

技術実証では、テレビ局またはコンビニ事業者等と協力し、システム間を接続した環境を構築する。（図 6-3）

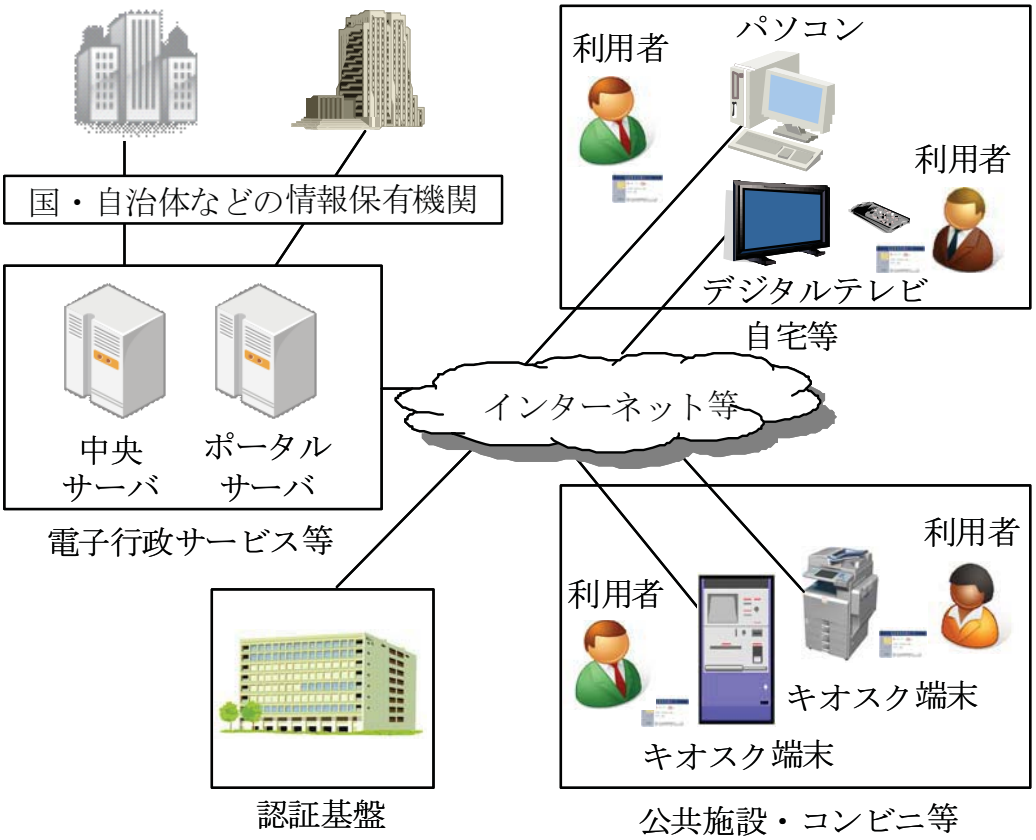


図 6-3 実証実験で使用する環境

本環境は、6.1 節や 6.2 節で構築する環境に、中央サーバを追加したものである。本環境で実施できる実証試験について、サーバ連携型多目的 IC カードを利用することに特徴的な検証課題を以下に示す。

(1) 認証連携に関する検証

本報告書の中では、デジタルテレビやキオスク端末から、利用者を認証する場合の ID／パスワードの入力や IC カードの利用に対するユーザビリティの検討を行っているが、サーバ連携型多目的 IC カードでは、ここに対応する部分は、中央サーバで実施されることになる。中央サーバにある認証要素（ID／パスワード、IC カード内の情報）の使用を許可するためには、結局、何らかの利用者認証が必要となるが、その方式は、従来のようにサービス提供者が決定するのではなく、サーバ連携型多目的 IC カード側で決定することになる。この場合は、デジタルテレビやキオスク端末の特徴を勘案した適切な方式を選択することができるため、このような認証連携方式に関して検証を行う。

(2) サーバ連携型多目的 IC カード技術を活用した入力補助検証

デジタルテレビやキオスク端末では、リモコンやタッチパッドのように限定的なユーザインタフェースという条件があるため、申請等での文字入力に手間がかかるといった課題がある。そこで、サーバ連携型多目的 IC カードに利用者の属性情報を保存し、これらの情報を画面に予め表示する等による文字入力補助への活用が考えられる。本検証では、ユーザビリティの確認を行うとともに、利用者の属性情報として管理すべき項目および、これらの情報を外部システムが利用する際のアクセス制御やインタフェース等について検証を行う。

6.4.2 社会実証

6.3 節では、中央サーバに認証機能を一部移行させる方式の実用化に向けて、各種課題解決のために必要となる実証実験の具体的な内容について検討した。アクセス多様化とサーバ連携型多目的 IC カードの連携では、認証基盤の代わりに、中央サーバが放送局等の民間事業者側のサーバと接続されることになる。社会実証では、以下のことを検証することが考えられる。

(1) サービス登録手順

サービスの登録およびサービスへの利用者の登録には、多くの関係者が存在する。一括登録機能のような技術的な課題の他、各関係者への事

前の承認（テレビ局等からの認証情報の通過、中央サーバへの利用者の登録、認証基盤との紐付け、ポータルサーバへの利用者の登録など）の手順などを明確化する必要がある。

(2) 利用者からのクレーム受付と切り分け

利用者認証や情報提供の途中にあるネットワークの断線、中央サーバのダウン、などが発生した場合、利用者には、故障箇所が特定できない場合が考えられる。アクセス多様化とサーバ連携型多目的 IC カードを組み合わせた場合に発生する故障毎の切り分け手順や利用者からのクレーム受付窓口など、サービス性に係る課題を明確化する必要がある。

(3) 民間事業者との連携

提案方式では、アクセス多様化に対しては、サービス提供者におけるコンテンツの対応、サーバ連携型多目的 IC カードに対しては、認証方式の対応が求められる。これらの対応は、多様なアクセス手段から、多様な認証方式を使って国民がサービスを享受することが目的であり、同じ方式で、民間サービスを受けられることが、国民サービスの向上につながる。したがって、民間事業者との連携を可能とするために、コンテンツや認証方式の標準化の材料を提案するとともに、協力いただける民間事業者を募集し、サービス性や安全性の評価を行う。

6.4.3 将来展望

サーバ連携型多目的 IC カードを使用すると、サービス提供者毎にばらばらとなっている端末側の認証方式を簡略化(例えば、１種類の IC カードに１本化する等)することにより、アクセス端末に要求される認証方式を絞り込むことができる。また、アクセス端末の種別を意識して中央サーバのシステムを作成することで、テレビ局やコンビニ事業者等において、アクセス端末毎の対応が不要となることも考えられる。これらのことから、端末ベンダだけでなく、テレビ局やコンビニ事業者等における設備投資が抑制され、新しい（認証を要求する）サービスに簡単に対応することができる。一方、利用者から見ると、IC カード１枚で、自治体窓口はもちろん、パソコン、デジタルテレビ、キオスク端末などの多くのアクセス手段を用い、アクセス手段にマッチしたユーザインタフェースで、行政サービスを受けることができるようになる。

付録 A （財）地方自治情報センターへのヒアリング調査

A-1 調査の概要

コンビニエンスストア（コンビニ）での住民票等の証明書交付について、その概要と技術的ポイントを把握するために、実証事業を行っている（財）地方自治情報センターを訪問し、公開可能な範囲での情報の提供をいただいた。

A-2 調査の内容

主な質疑は以下の通り。

(1) コンビニに設置されているキオスク端末について

質問：現在のコンビニ側の端末ですが、印刷を行う多機能プリンタに IC カードの読み取り装置が設置されていなかったように記憶している。今後、カード（非接触）に対応した読み取り装置が設置されていくのか?

回答：セブン-イレブンの店舗内のマルチコピー機が、非接触Ｒ／Ｗ付きの機器にリプレースされているところである。

(2) 認証に利用される IC カードについて

質問：利用者の認証に住民基本台帳カードを利用するのか？

回答：その通り

(3) 住民票の対象について

質問：画面遷移の中で、本人の情報を確認する画面があるが、そこで申請内容の修正が可能となっている。今回のシステムでは、本人及びその属性情報のみ（世帯主、本籍、等）の証明書が取得できるもので、家族全体や他の家族の分の住民票は発行できないという理解でよいか?

回答：すべて交付対象となる。「住民票の写し」を選択すると、「本人のみ」「世帯全員」「世帯員の一部」のボタンが出る。「世帯員の一部」を選択すると、市町村のシステムから、ボタンのキャプションとして、世帯員の情報がもらえる。

(4) 住民票の真正性について

質問：住民票の真正性を担保するために、印刷技術が使われているが、どのような技術か？

回答：両面印刷にして、表面でこれまでの住民票の情報と、透かしによるコピー識別、裏面で真正性の確認ができるようにしている。真正性の確認には 2 つの技術を使っている。１つはオフラインで検証が可能な印刷技術で、もう 1 つは暗号化されて印刷されている情報を検証サーバに送って、記載内容そのものを確認する方法である。

(5) キオスク端末と証明書交付サーバ接続の安全性

質問：キオスク端末と証明書交付サーバの間では、通信の安全性確保が必要となる。ブラウザを利用しているように見受けられるので、SSL を利用しているのか?

回答：SSL を利用している。

(6) 証明書交付サーバのインタフェースについて

質問：キオスク端末と証明書交付サーバの間では、ブラウザを利用しているように見受けられるので、HTTP をベースにした通信を行っていると思われるが正しいか？

回答：キオスク端末と証明書交付サーバ HTTPS にて通信を行っている。印刷用データをダウンロードする際も HTTPS での通信となる。

(7) 証明書交付センターのインタフェースについて

質問：キオスク端末のユーザインタフェースは固定になっているが、利用者の特性に応じたインタフェースを提供する可能性はあるか？

回答：現状の交付シーケンス制御は証明書交付センターで行っている。ユーザインタフェースを利用者ごとに変えるという要望が強いのであれば、今後検討する可能性はある。

(9) ほかのサービスへの展開について

質問：住民票、印鑑証明の交付以外のサービスへの展開はどうか？

回答：展開は可能であるが、今後検討する必要がある。

付録 B リモコンでの操作性に関する検証の仕様

本章では本検証の各項目についての詳細、及び、使用した検証用コンテンツの仕様について記述する。まず初めに、各検証項目の概要、および、検証フローについて説明する。

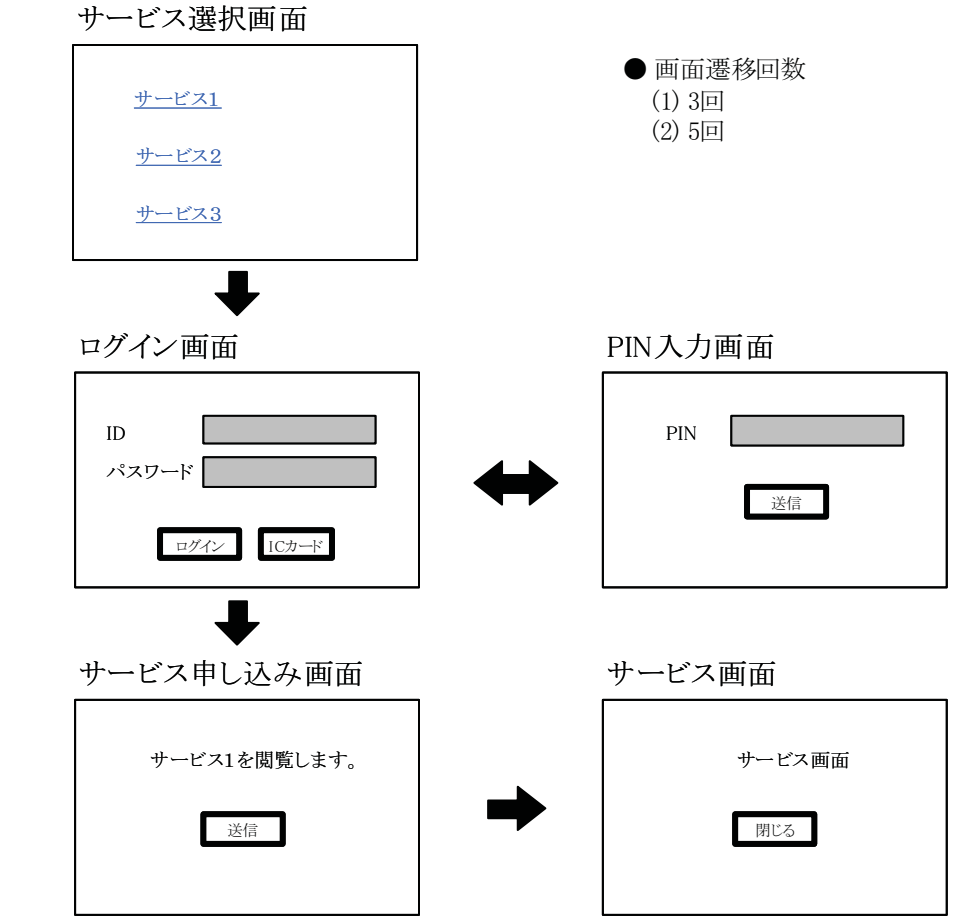
【検証項目 2-1 閲覧サービスを利用する場合の検証】

概要

(1) 擬似サービスコンテンツを用いて、IC カードを全く用いずに、ユーザ ID とパスワード入力を行なう場合の、申請完了までのクリック数、操作ステップ数を計測する

(2) 擬似サービスコンテンツを用いて、IC カードから、ユーザ ID とパスワード入力を行なう場合の、申請完了までのクリック数、操作ステップ数を計測する（TV 本体にリーダライタを接続）

画面遷移

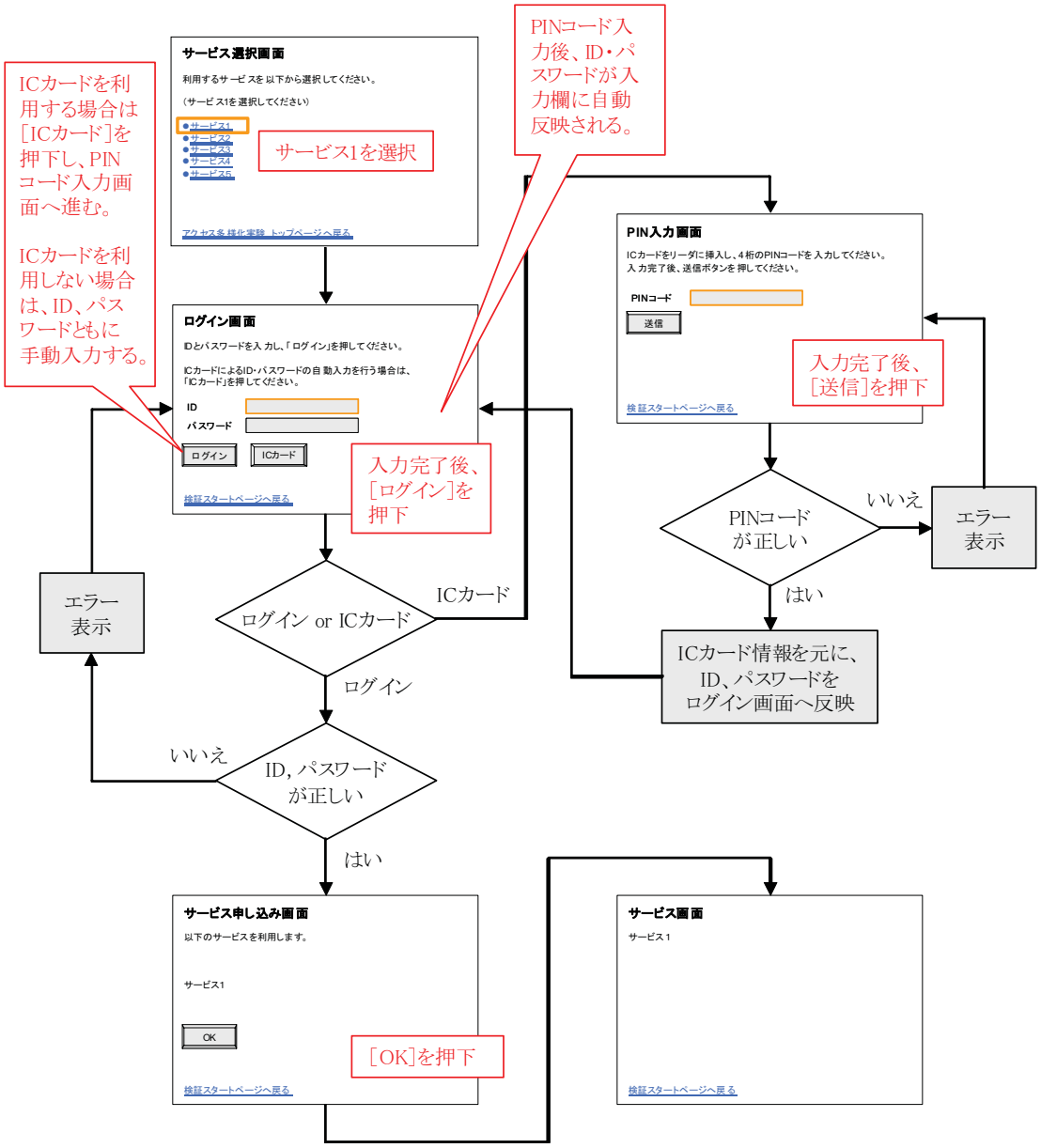


● 画面遷移回数
(1) 3回
(2) 5回

●入力項目数
(1) 2項目 (ID, パスワード)
(2) 1項目 (PINコード)

各項目への設定値については、後述の検証コンテンツ仕様 を参照のこと

検証フロー


サービス選択画面
利用するサービスを以下から選択してください。
（サービス1を選択してください）
サービス1
サービス2
サービス3
サービス4
サービス5
アクセス多様化実験 トップページへ戻る
サービス1を選択
ICカードを利用する場合は［ICカード］を押下し、PINコード入力画面へ進む。
ICカードを利用しない場合は、ID、パスワードともに手動入力する。
PINコード入力後、ID・パスワードが入力欄に自動反映される。
ログイン画面
IDとパスワードを入力し、「ログイン」を押してください。
ICカードによるID・パスワードの自動入力を行う場合は、「ICカード」を押してください。
ID
パスワード
ログイン
ICカード
検証スタートページへ戻る
入力完了後、［ログイン］を押下
PIN入力画面
ICカードをリーダに挿入し、4桁のPINコードを入力してください。
入力完了後、送信ボタンを押してください。
PINコード
送信
検証スタートページへ戻る
入力完了後、［送信］を押下
PINコードが正しい
いいえ
エラー表示
はい
ICカード情報を元に、ID、パスワードをログイン画面へ反映
エラー表示
ログイン or ICカード
ICカード
ログイン
ID, パスワードが正しい
いいえ
はい
サービス申し込み画面
以下のサービスを利用します。
サービス1
OK
検証スタートページへ戻る
［OK］を押下
サービス画面
サービス1
検証スタートページへ戻る

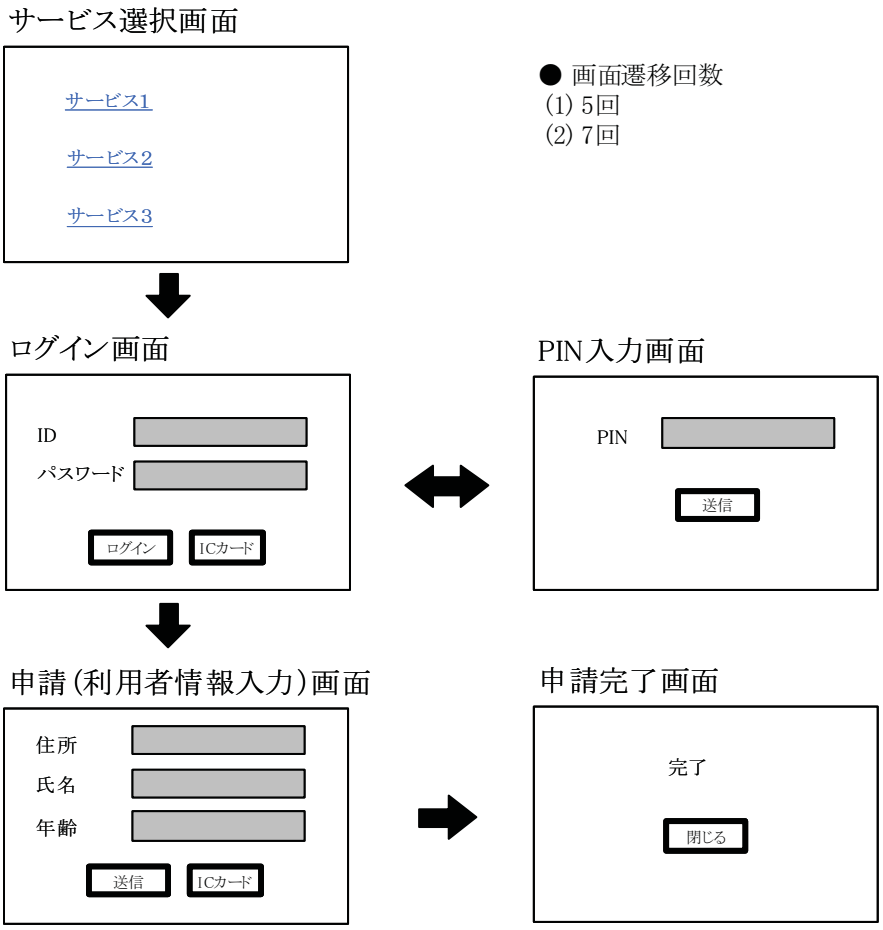
【検証項目 2-2 申請サービスを利用する場合の検証】

概要

(1) 擬似サービスコンテンツを用いて、IC カードを全く用いずにユーザ ID とパスワード、住所等を入力する場合の申請完了までの操作ステップ数を計測する

(2) 擬似サービスコンテンツを用いて、IC カードからユーザ ID とパスワード、住所等を入力する場合の申請完了までの操作ステップ数を計測する（TV 本体にリーダライタを接続）

画面遷移

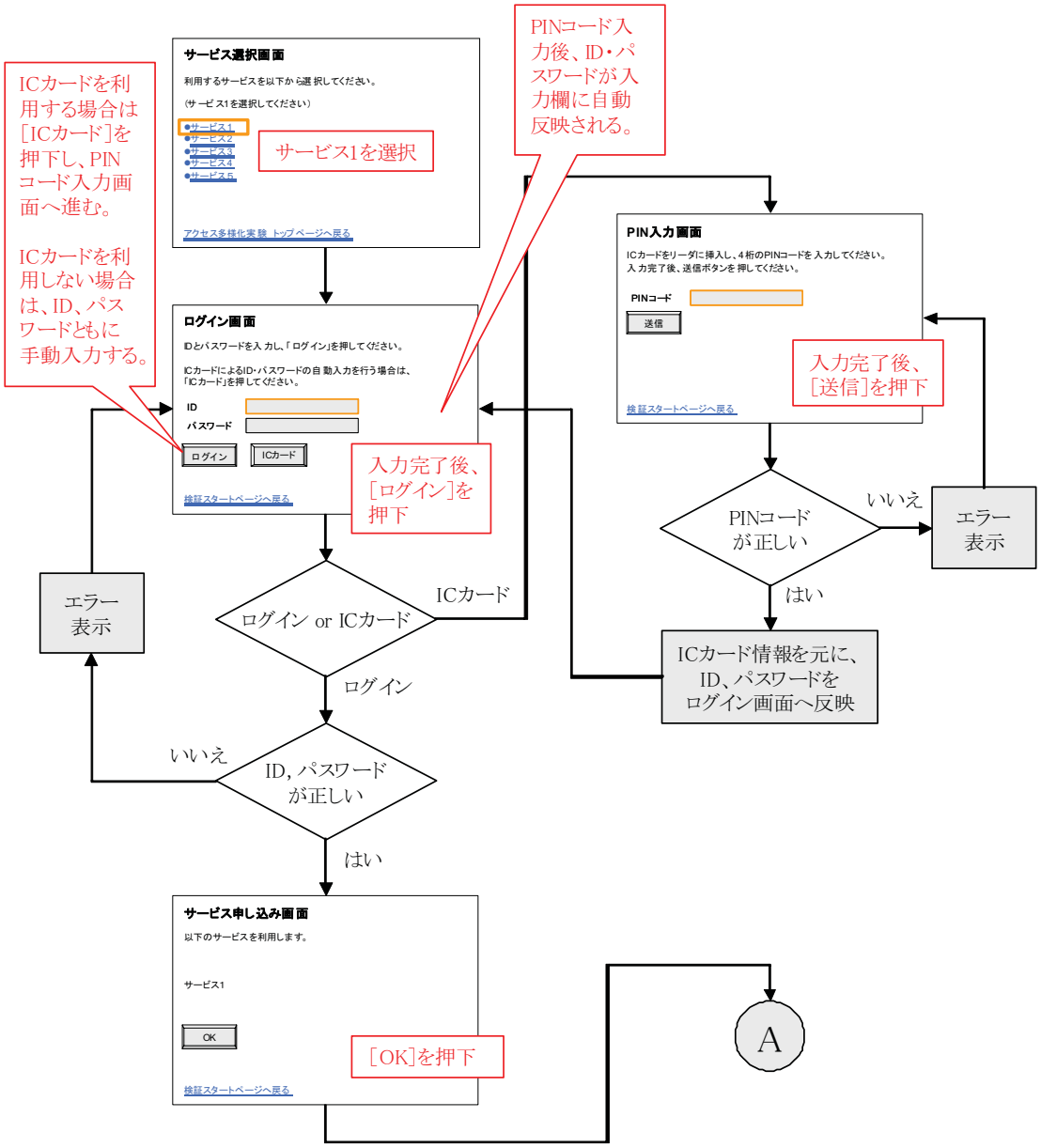


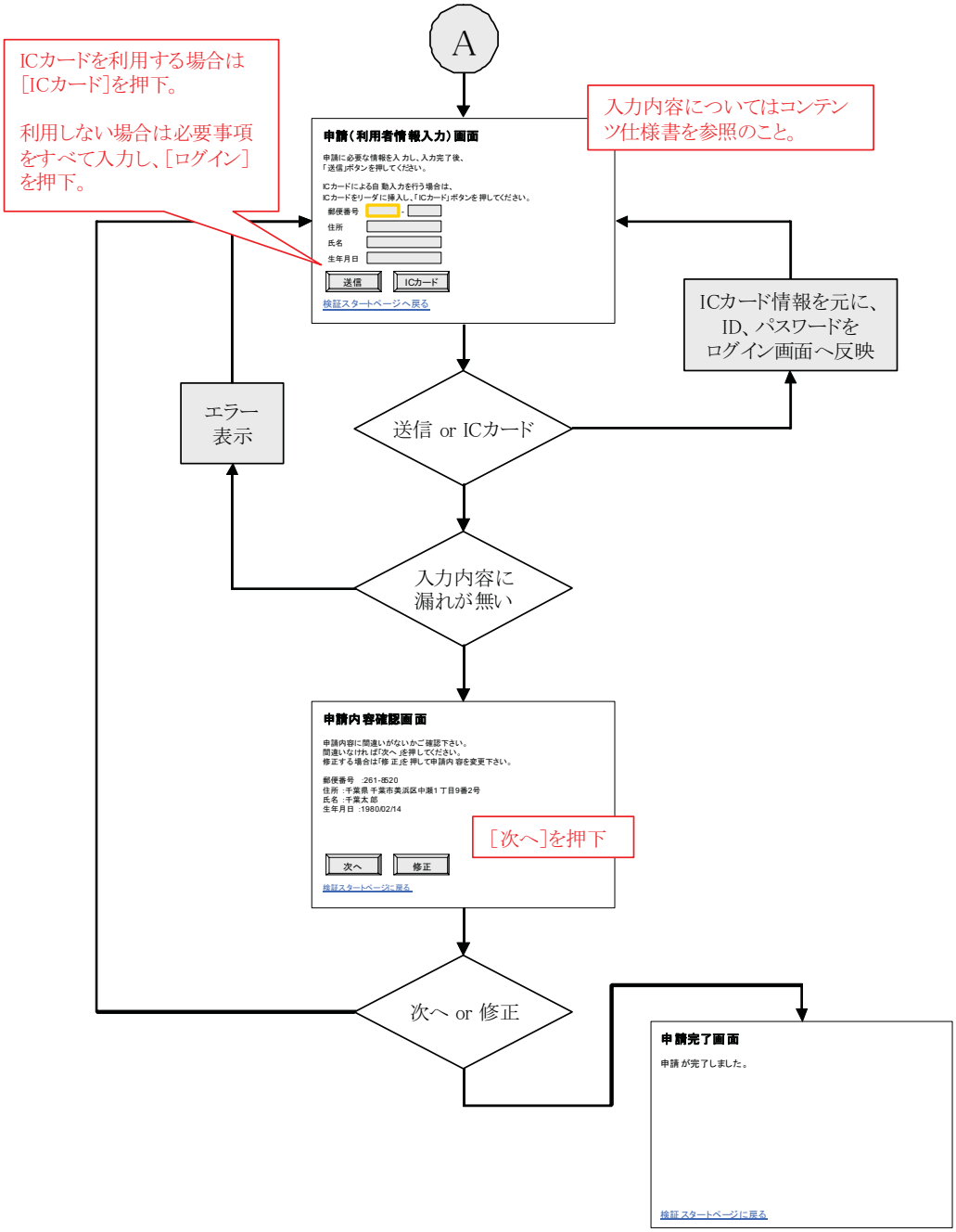
● 画面遷移回数
(1) 5回
(2) 7回

●入力項目数
(1) 7項目(ID, パスワード, 郵便番号 上3桁, 下4桁, 住所, 氏名, 生年月日)
(2) 1項目(PINコード)

各項目への設定値については、後述の検証コンテンツ仕様 を参照のこと

検証フロー


サービス選択画面
利用するサービスを以下から選択してください。
(サービス1を選択してください)
サービス1
サービス2
サービス3
サービス4
サービス5
アクセス多様化実験 トップページへ戻る
サービス1を選択
ICカードを利用する場合は[ICカード]を押下し、PINコード入力画面へ進む。
ICカードを利用しない場合は、ID、パスワードともに手動入力する。
PINコード入力後、ID・パスワードが入力欄に自動反映される。
ログイン画面
IDとパスワードを入力し、「ログイン」を押してください。
ICカードによるID・パスワードの自動入力を行う場合は、「ICカード」を押してください。
ID
パスワード
ログイン
ICカード
検証スタートページへ戻る
入力完了後、[ログイン]を押下
PIN入力画面
ICカードをリーダに挿入し、4桁のPINコードを入力してください。
入力完了後、送信ボタンを押してください。
PINコード
送信
検証スタートページへ戻る
入力完了後、[送信]を押下
PINコードが正しい
いいえ
エラー表示
はい
ICカード情報を元に、ID、パスワードをログイン画面へ反映
エラー表示
ログイン or ICカード
ICカード
ログイン
ID, パスワードが正しい
いいえ
はい
サービス申し込み画面
以下のサービスを利用します。
サービス1
OK
検証スタートページへ戻る
[OK]を押下
A


A
ICカードを利用する場合は
[ICカード]を押下。
利用しない場合は必要事項
をすべて入力し、[ログイン]
を押下。
入力内容についてはコンテン
ツ仕様書を参照のこと。
申請（利用者情報入力）画面
申請に必要な情報を入 力し、入力完了後、
「送信」ボタンを押してください。
ICカードによる自 動入力を行う場合は、
ICカードをリーダに挿入し、「ICカード」ボタンを 押してください。
郵便番号
住所
氏名
生年月日
送信
ICカード
検証スタートページへ戻る
ICカード情報を元に、
ID、パスワードを
ログイン画面へ反映
エラー
表示
送信 or ICカード
入力内容に
漏れが無い
申請内容確認画面
申請内容に間違いがないかご確認下さい。
間違いなければ「次へ」を押してください。
修正する場合は「修正」を 押して申請内 容を変更下さい。
郵便番号 :261-8520
住所 :千葉県 千葉市美浜区中瀬1 丁目9番2号
氏名 :千葉太 郎
生年月日 :1980/02/14
次へ
修正
検証スタートページに戻る
[次へ]を押下
次へ or 修正
申請完了画面
申請 が完了しました。
検証 スタートページに戻る

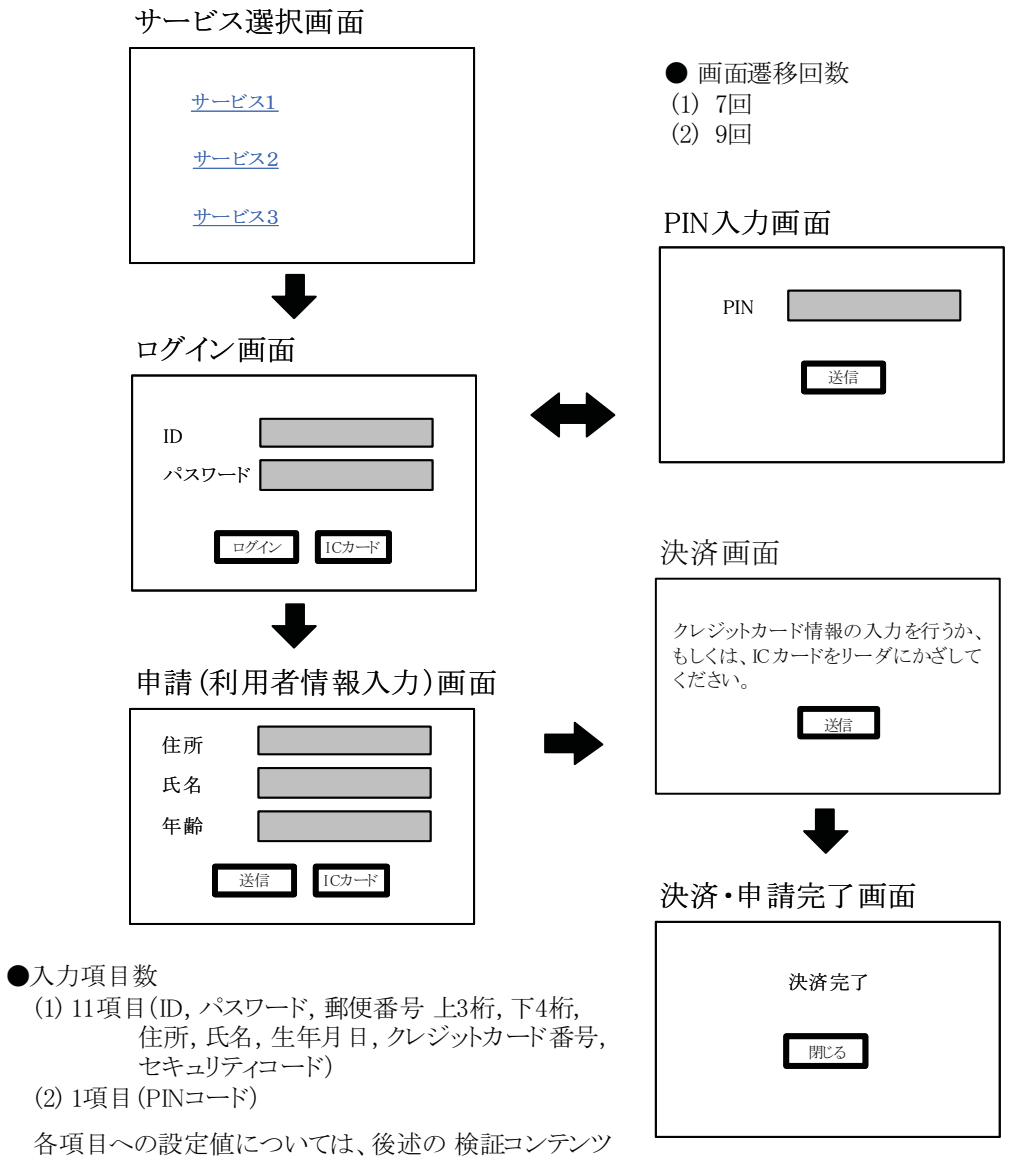
【検証項目 2-3 申請サービス（決済）を利用する場合の検証】

概要

(1) 擬似サービスコンテンツを用いて、IC カードを全く用いずに、ユーザ ID とパスワード、住所等を入力し、決済が完了するまでの操作ステップ数を計測する

(2) 擬似サービスコンテンツを用いて、IC カードからユーザ ID とパスワード、住所等を入力し、決済が完了するまでの操作ステップ数を計測する（TV 本体にリーダライタを接続）

画面遷移

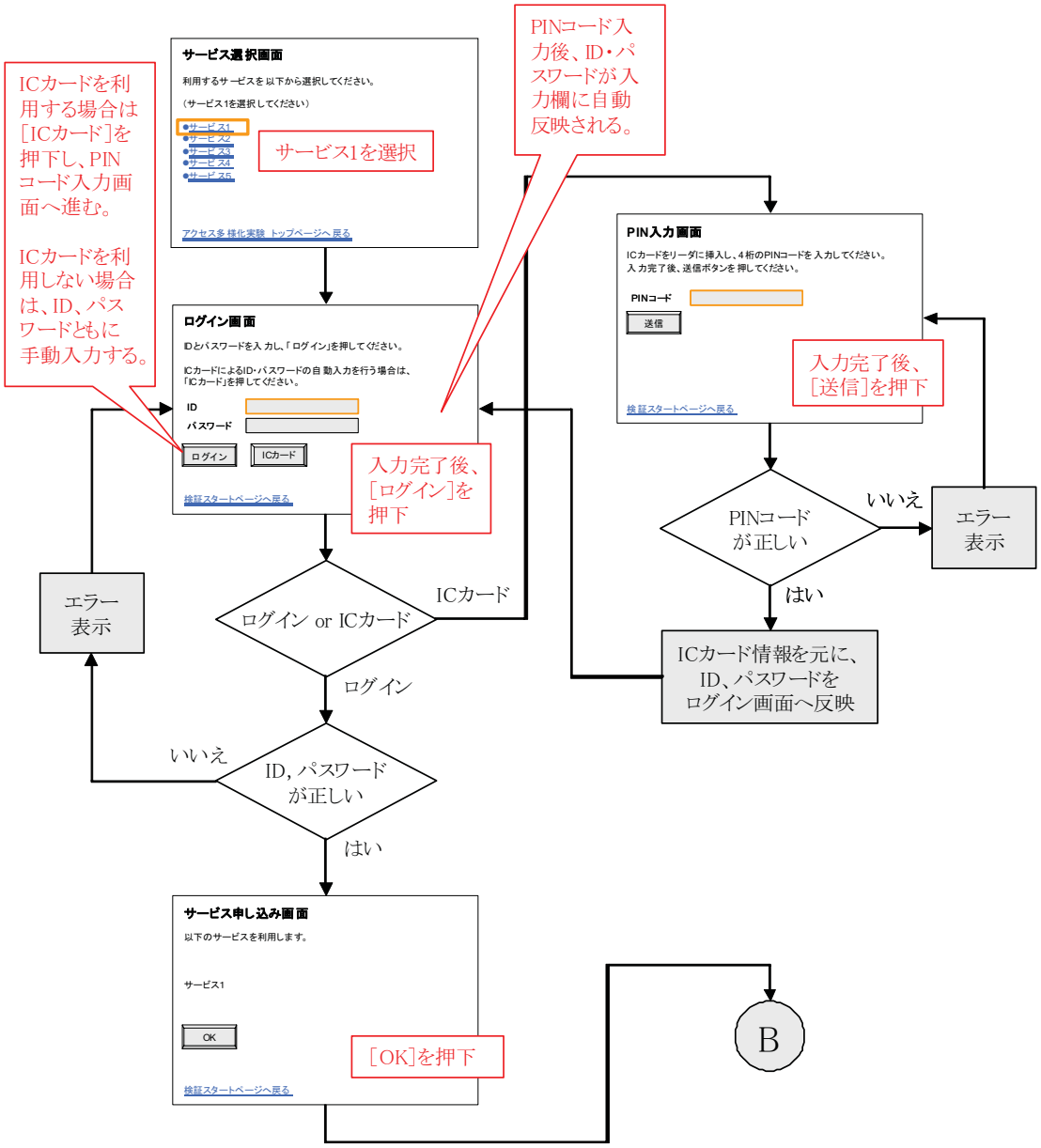


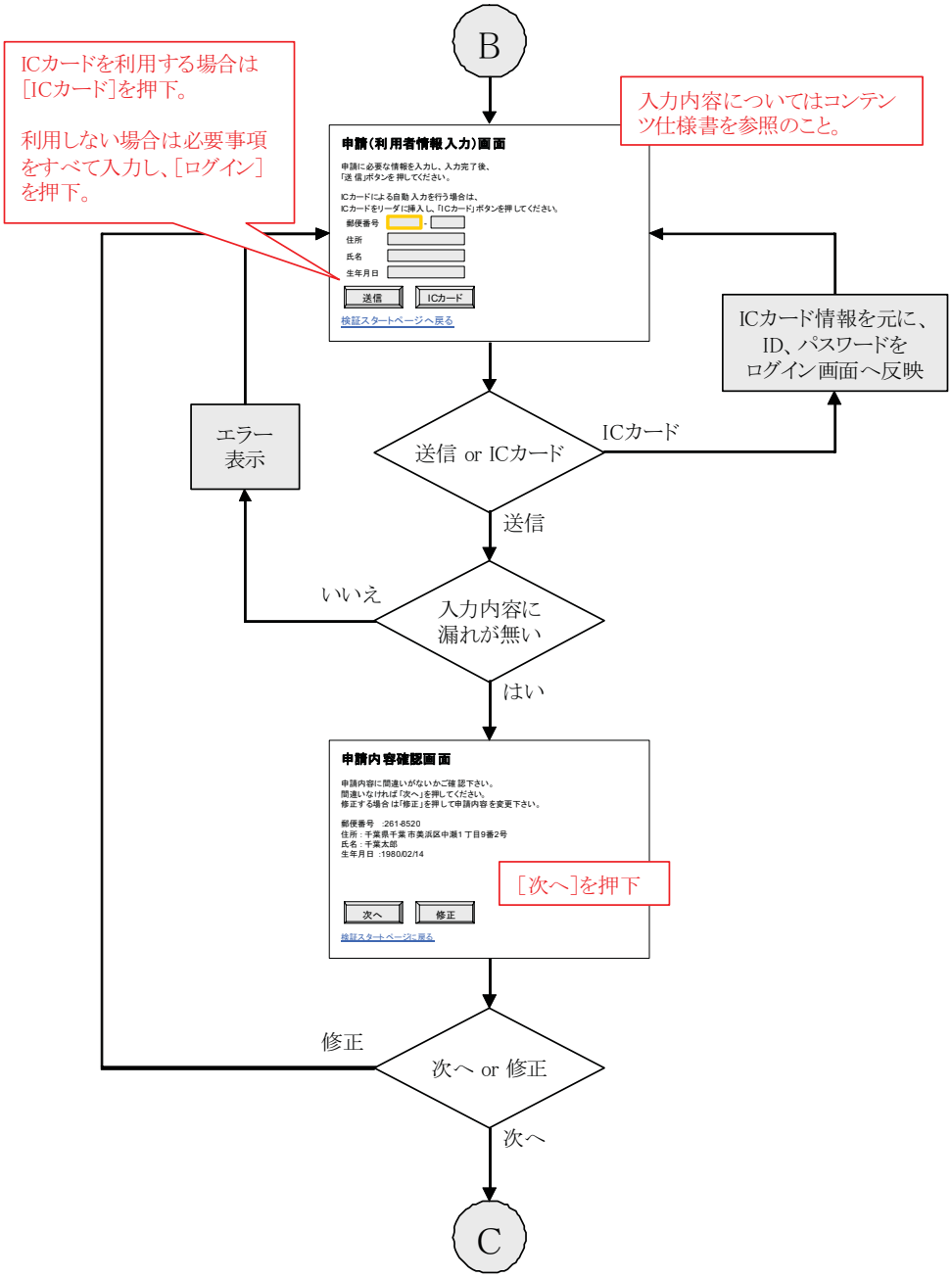
● 画面遷移回数
(1) 7回
(2) 9回

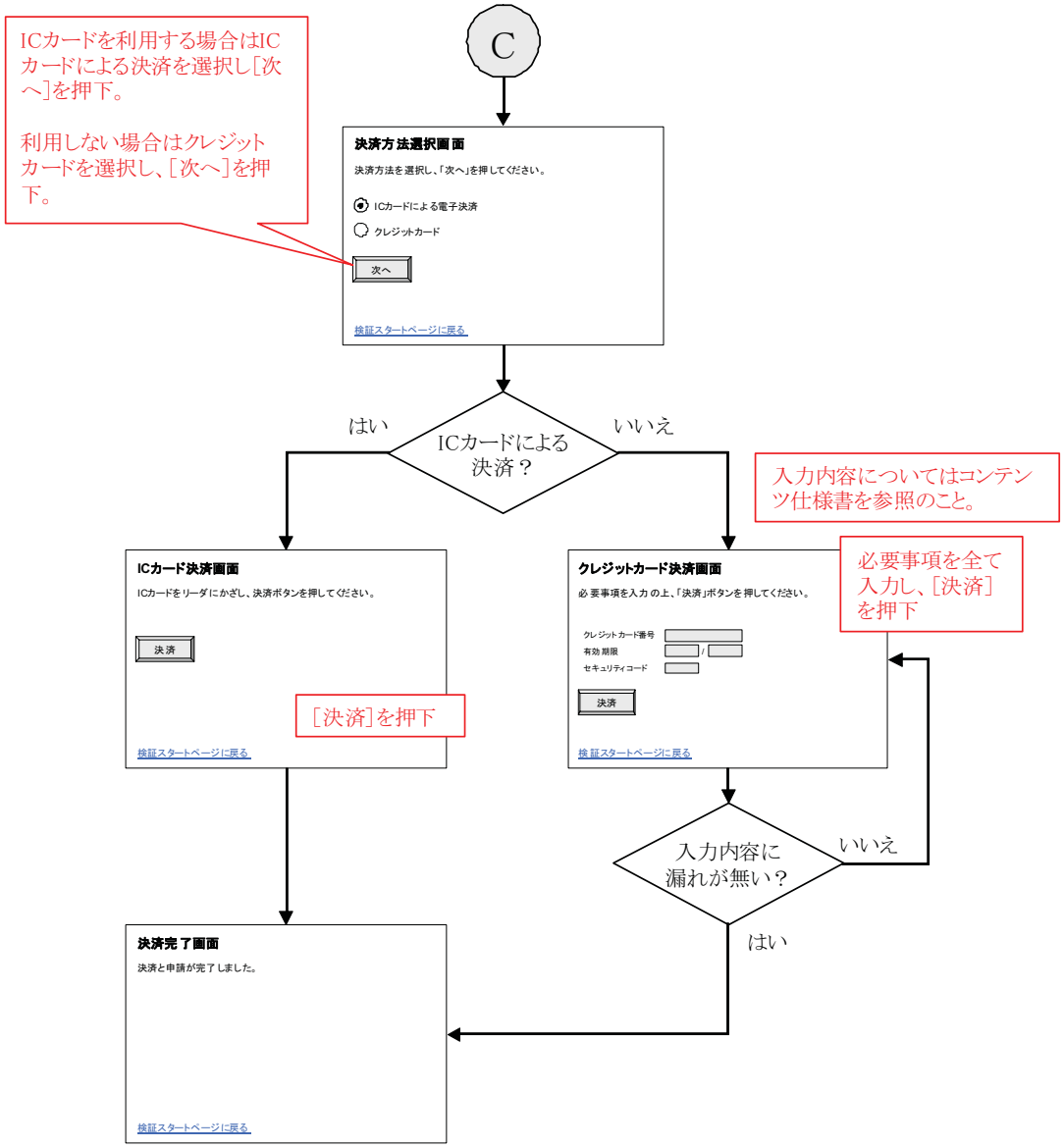
●入力項目数
(1) 11項目(ID, パスワード, 郵便番号 上3桁, 下4桁, 住所, 氏名, 生年月日, クレジットカード番号, セキュリティコード)
(2) 1項目(PINコード)

各項目への設定値については、後述の 検証コンテンツ仕様書 を参照のこと

検証フロー


サービス選択画面
利用するサービスを以下から選択してください。
（サービス1を選択してください）
サービス1
サービス2
サービス3
サービス4
サービス5
アクセス多様化実験 トップページへ戻る
サービス1を選択
ICカードを利用する場合は［ICカード］を押下し、PINコード入力画面へ進む。
ICカードを利用しない場合は、ID、パスワードともに手動入力する。
PINコード入力後、ID・パスワードが入力欄に自動反映される。
ログイン画面
IDとパスワードを入力し、「ログイン」を押してください。
ICカードによるID・パスワードの自動入力を行う場合は、「ICカード」を押してください。
ID
パスワード
ログイン
ICカード
検証スタートページへ戻る
入力完了後、［ログイン］を押下
PIN入力画面
ICカードをリーダに挿入し、4桁のPINコードを入力してください。
入力完了後、送信ボタンを押してください。
PINコード
送信
検証スタートページへ戻る
入力完了後、［送信］を押下
PINコードが正しい
いいえ
エラー表示
はい
ICカード情報を元に、ID、パスワードをログイン画面へ反映
エラー表示
ログイン or ICカード
ICカード
ログイン
いいえ
ID, パスワードが正しい
はい
サービス申し込み画面
以下のサービスを利用します。
サービス1
OK
検証スタートページへ戻る
［OK］を押下
B


B
ICカードを利用する場合は
[ICカード]を押下。
利用しない場合は必要事項
をすべて入力し、[ログイン]
を押下。
入力内容についてはコンテン
ツ仕様書を参照のこと。
申請(利用者情報入力)画面
申請に必要な情報を入力し、入力完了後、
「送信」ボタンを押してください。
ICカードによる自動入力を行う場合は、
ICカードをリーダに挿入し、「ICカード」ボタンを押してください。
郵便番号
住所
氏名
生年月日
送信
ICカード
検証スタートページへ戻る
ICカード情報を元に、
ID、パスワードを
ログイン画面へ反映
エラー
表示
送信 or ICカード
ICカード
送信
いいえ
入力内容に
漏れが無い
はい
申請内容確認画面
申請内容に間違いがないかご確認下さい。
間違いなければ「次へ」を押してください。
修正する場合は「修正」を押して申請内容を変更下さい。
郵便番号 :261-8520
住所 : 千葉県千葉 市美浜区中瀬1丁目9番2号
氏名 : 千葉太郎
生年月日 :1980/02/14
次へ
修正
検証スタートページに戻る
[次へ]を押下
修正
次へ or 修正
次へ
C


C
ICカードを利用する場合はICカードによる決済を選択し[次へ]を押下。
利用しない場合はクレジットカードを選択し、[次へ]を押下。
決済方法選択画面
決済方法を選択し、「次へ」を押してください。
ICカードによる電子決済
クレジットカード
次へ
検証スタートページに戻る
はい
ICカードによる決済？
いいえ
入力内容についてはコンテンツ仕様書を参照のこと。
ICカード決済画面
ICカードをリーダにかざし、決済ボタンを押してください。
決済
[決済]を押下
検証スタートページに戻る
クレジットカード決済画面
必要事項を入力の上、「決済」ボタンを押してください。
クレジットカード番号
有効期限
セキュリティコード
決済
必要事項を全て入力し、[決済]を押下
検証スタートページに戻る
入力内容に漏れが無い？
いいえ
はい
決済完了画面
決済と申請が完了しました。
検証スタートページに戻る

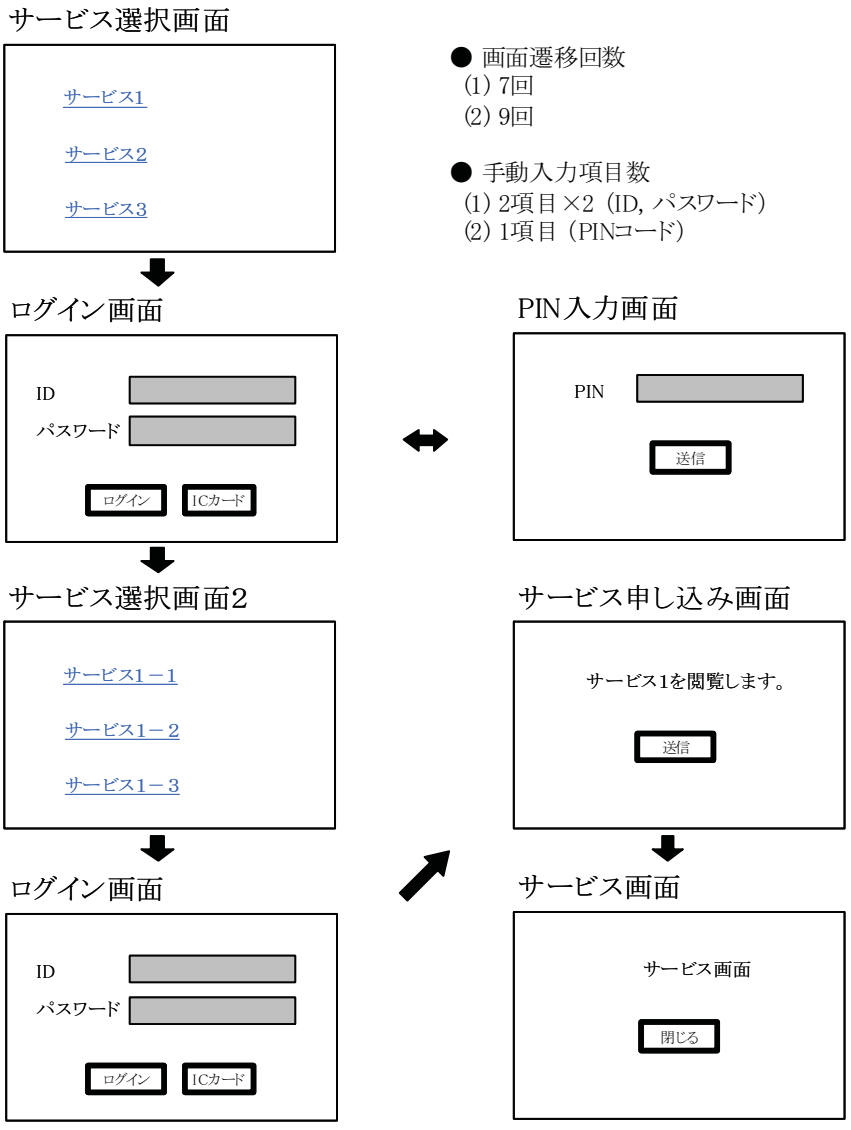
【検証項目 2-4 数回の認証が必要なサービスを利用する場合の検証】

概要

(1) 擬似サービスコンテンツを用いて、サービス選択、特に選択先で再度認証が必要となるコンテンツを用いて、都度認証を行なう場合と、ワンストップ化する場合とでの操作ステップ数を計測する

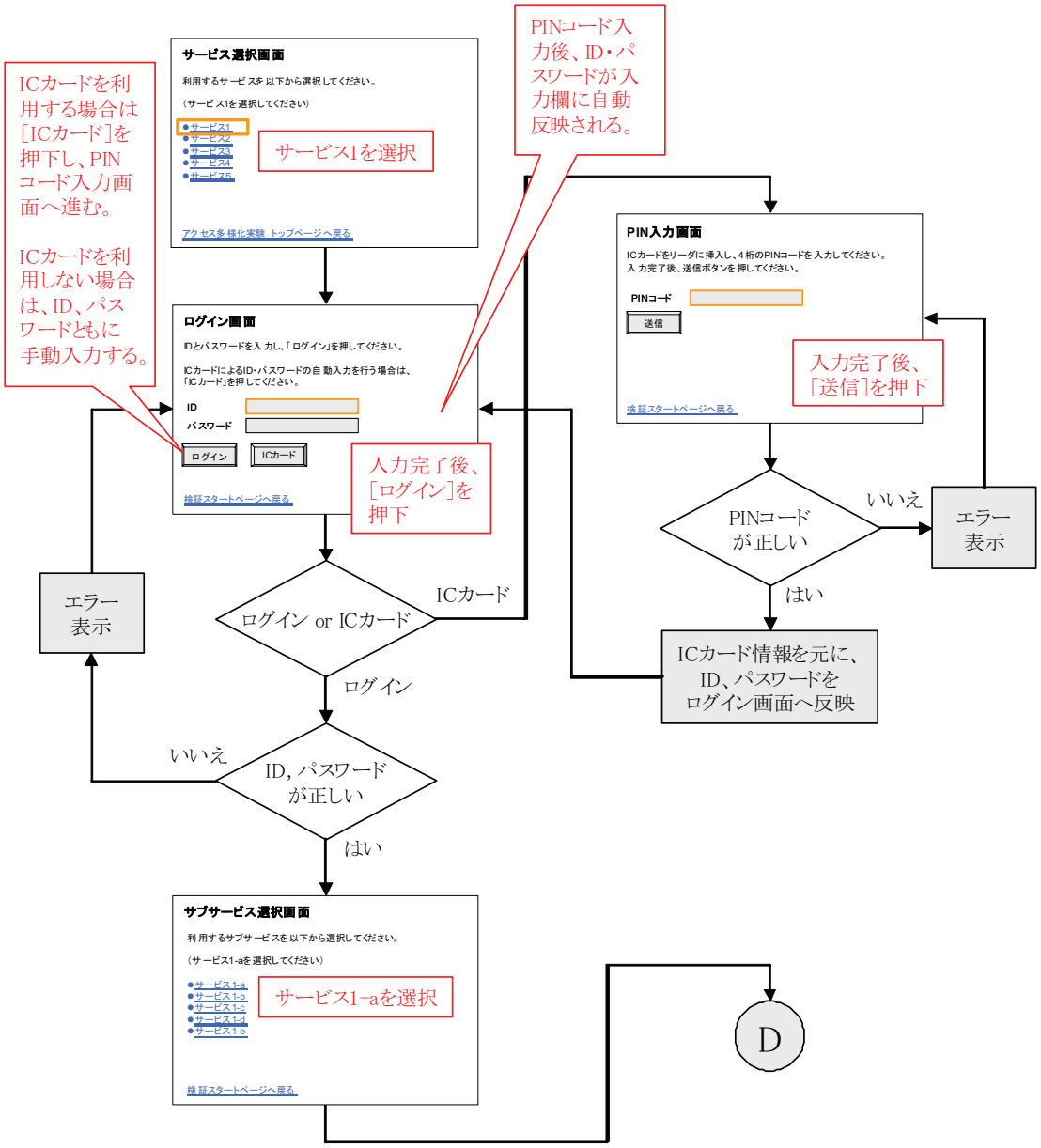
(2) 擬似サービスコンテンツを用いて、サービス選択、とくに選択先で再度認証が必要となるコンテンツで IC カードを用いて認証を行う場合での、都度認証を行う場合と、ワンストップ化する場合とでのクリック数、操作ステップ数を計測する（TV 本体にリーダライタを接続）

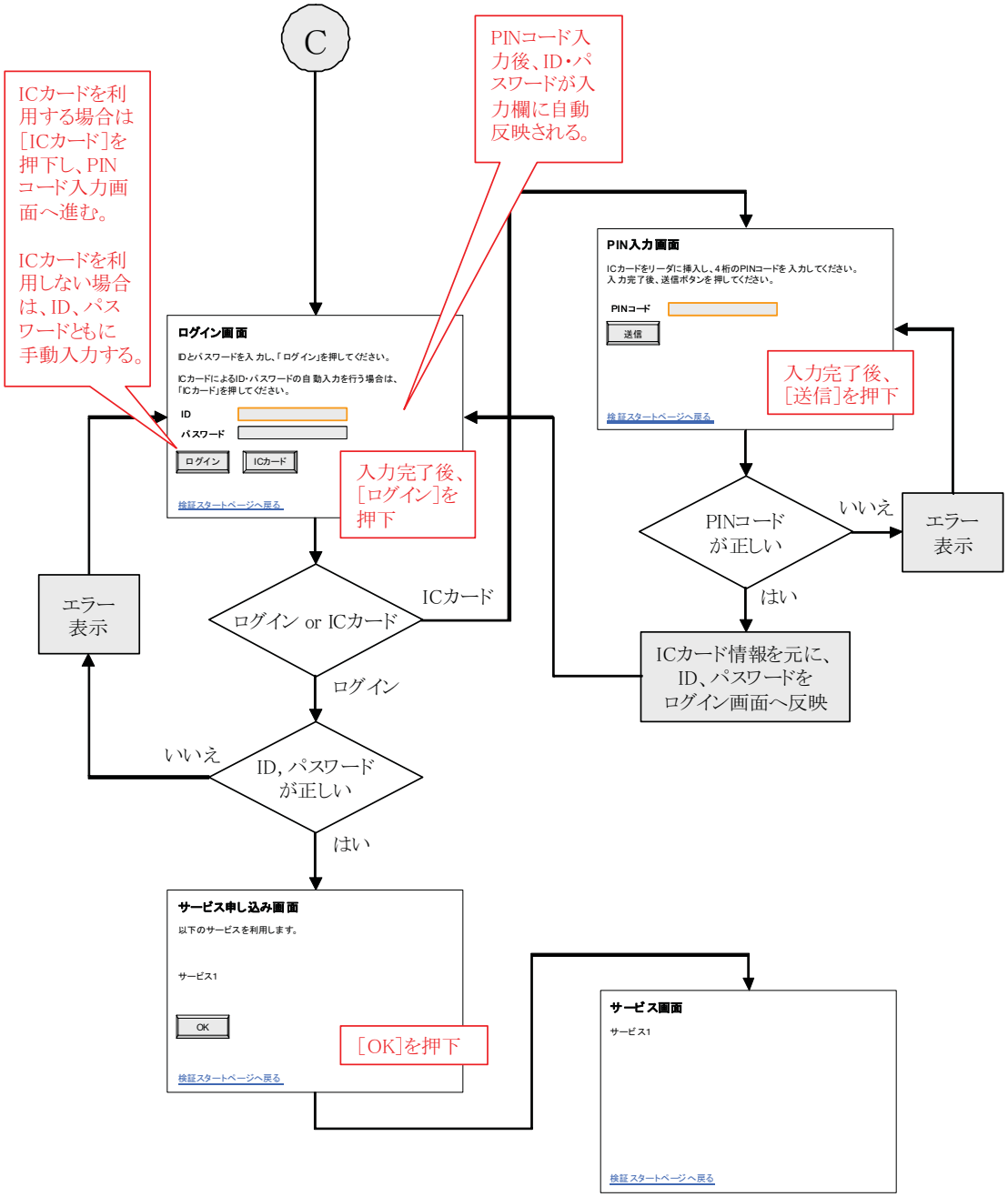
画面遷移



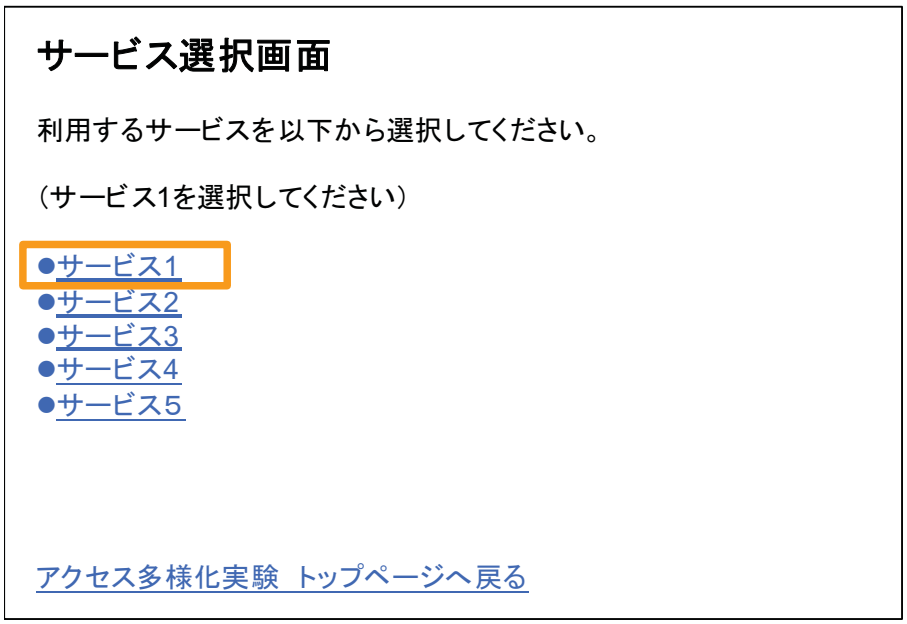
各項目への設定値については 後述の検証コンテンツ仕様書 を参照のこと

検証フロー


サービス選択画面
利用するサービスを以下から選択してください。
（サービス1を選択してください）
サービス1
サービス2
サービス3
サービス4
サービス5
アクセス多様化実験 トップページへ戻る
サービス1を選択
ICカードを利用する場合は［ICカード］を押下し、PINコード入力画面へ進む。
ICカードを利用しない場合は、ID、パスワードともに手動入力する。
PINコード入力後、ID・パスワードが入力欄に自動反映される。
ログイン画面
IDとパスワードを入力し、「ログイン」を押してください。
ICカードによるID・パスワードの自動入力を行う場合は、「ICカード」を押してください。
ID
パスワード
ログイン
ICカード
検証スタートページへ戻る
入力完了後、［ログイン］を押下
PIN入力画面
ICカードをリーダに挿入し、4桁のPINコードを入力してください。
入力完了後、送信ボタンを押してください。
PINコード
送信
検証スタートページへ戻る
入力完了後、［送信］を押下
PINコードが正しい
いいえ
はい
エラー表示
ICカード情報を元に、ID、パスワードをログイン画面へ反映
ログイン or ICカード
ICカード
ログイン
エラー表示
ID, パスワードが正しい
いいえ
はい
サブサービス選択画面
利用するサブサービスを以下から選択してください。
（サービス1-aを選択してください）
サービス1-a
サービス1-b
サービス1-c
サービス1-d
サービス1-e
検証スタートページへ戻る
サービス1-aを選択
D


C
ICカードを利用する場合は［ICカード］を押下し、PINコード入力画面へ進む。
ICカードを利用しない場合は、ID、パスワードともに手動入力する。
PINコード入力後、ID・パスワードが入力欄に自動反映される。
ログイン画面
IDとパスワードを入力し、「ログイン」を押してください。
ICカードによるID・パスワードの自動入力を行う場合は、「ICカード」を押してください。
ID
パスワード
ログイン
ICカード
検証スタートページへ戻る
入力完了後、［ログイン］を押下
PIN入力画面
ICカードをリーダに挿入し、4桁のPINコードを入力してください。
入力完了後、送信ボタンを押してください。
PINコード
送信
検証スタートページへ戻る
入力完了後、［送信］を押下
PINコードが正しい
いいえ
エラー表示
はい
ICカード情報を元に、ID、パスワードをログイン画面へ反映
ログイン or ICカード
ICカード
エラー表示
ログイン
ID, パスワードが正しい
いいえ
はい
サービス申し込み画面
以下のサービスを利用します。
サービス1
OK
検証スタートページへ戻る
［OK］を押下
サービス画面
サービス1
検証スタートページへ戻る

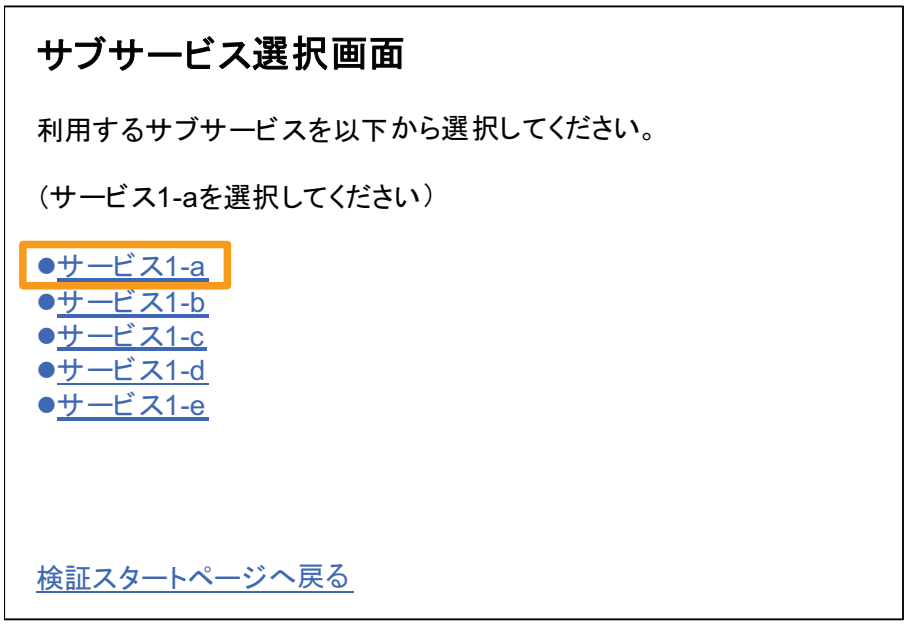
【コンテンツ仕様：サービス選択画面】



コンテンツ概要

・ デフォルトフォーカスは「サービス 1」

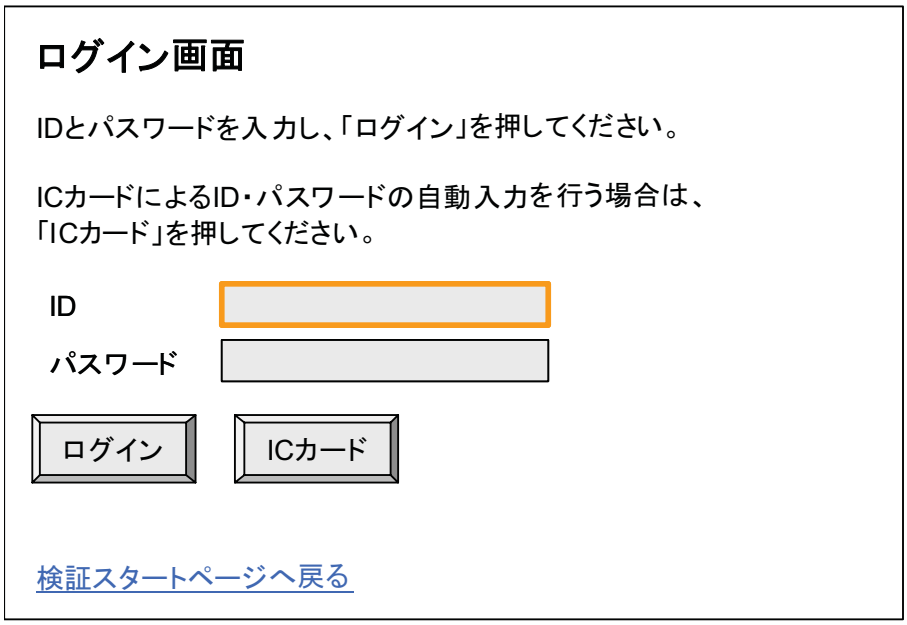
【コンテンツ仕様：サブサービス選択画面】



コンテンツ概要

・デフォルトフォーカスは「サービス 1-a」

【コンテンツ仕様：ログイン画面】

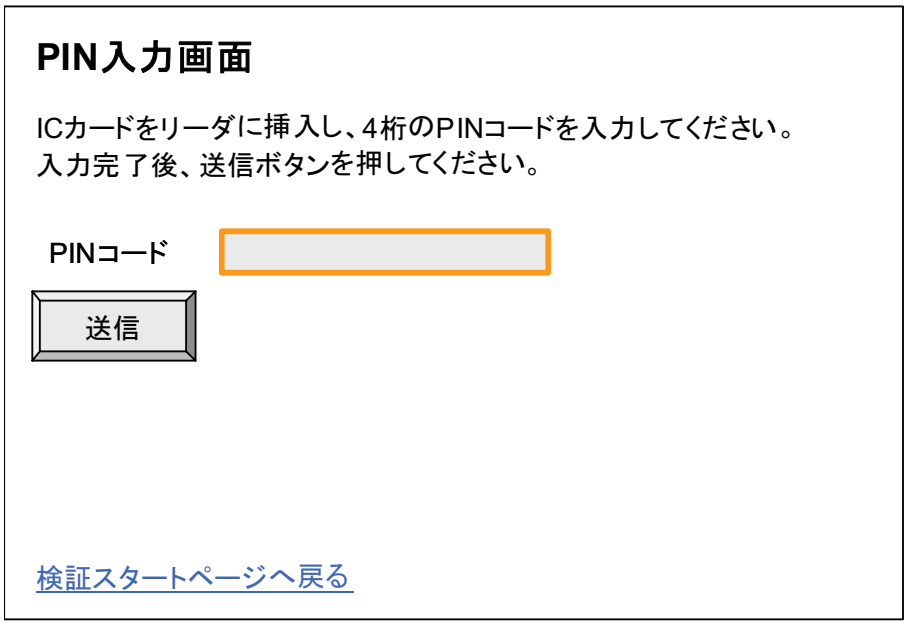


コンテンツ概要

- ID、パスワードに正しい値を入力した後、ログインボタンを押すと次の画面へ遷移する
- デフォルトフォーカスは ID 入力欄
- 入力内容が間違っている場合は、エラーダイアログが表示され、次の画面へ遷移しない
- IC カードボタンを押下すると、PIN 入力画面に遷移する
- PIN 入力画面で正しい PIN コードが入力されると、本画面の入力欄に、自動的に ID、パスワードが入力される
- ID 入力欄の charactertype 属性は hankaku
- パスワード入力欄の type 属性は password
- 各入力項目へ入力する値を以下のように設定する

要素	入力値	文字数
ID	jikkenR	7文字
パスワード	access2009	10文字

【コンテンツ仕様：PIN 入力画面】

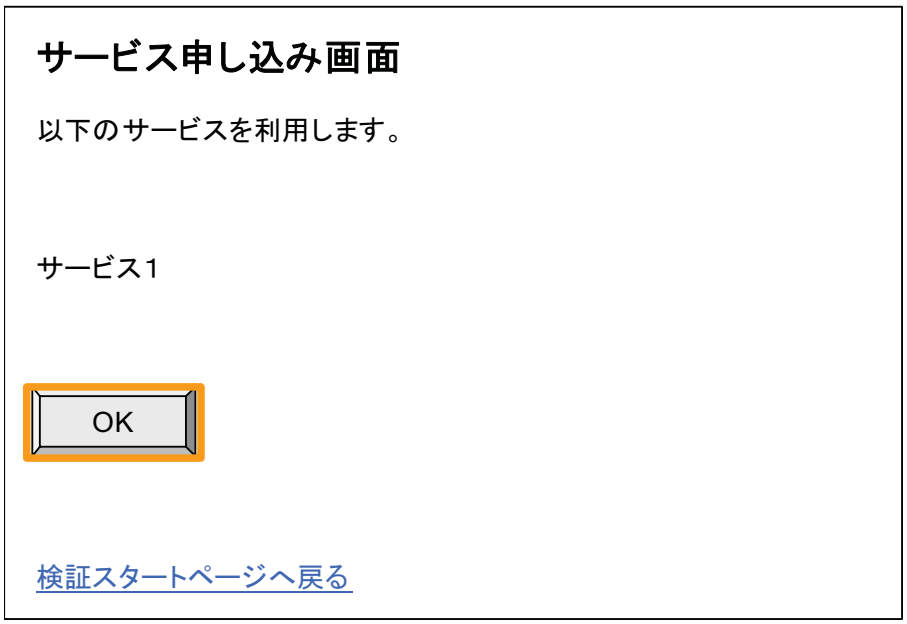


コンテンツ概要

- PIN コード入力欄に正しい値を入力し、送信ボタンを押下すると、元の画面（ログイン画面）へ遷移する
- デフォルトフォーカスは PIN コード入力欄
- 入力内容が間違っている場合は、エラーダイアログが表示され、画面遷移はしない
- PIN コード入力欄の charactertype 属性は number
- 各入力項目へ入力する値を以下のように設定する

要素	入力値	文字数
PIN	1234	4文字

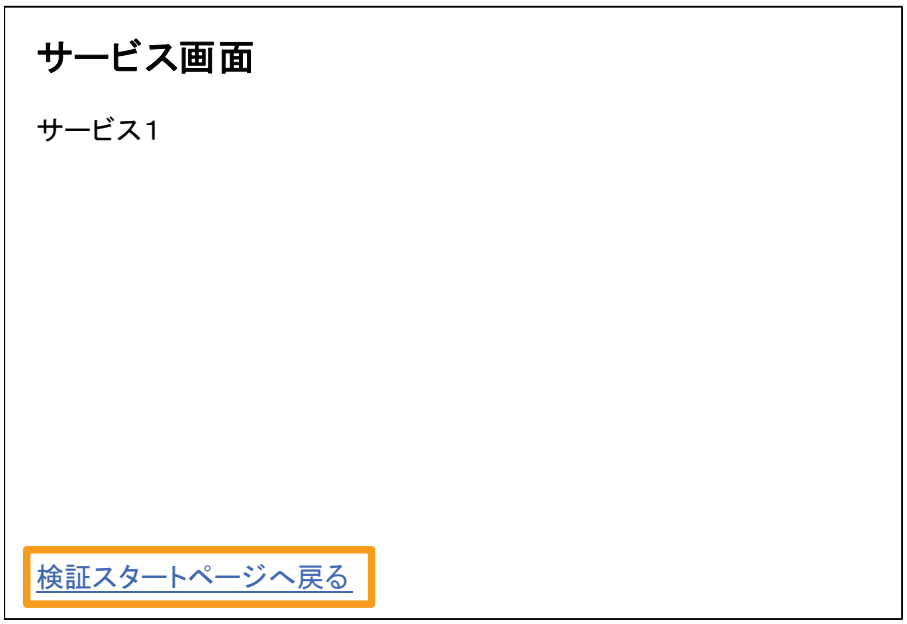
【コンテンツ仕様：サービス申し込み画面】



コンテンツ概要

- サービス 1 利用前の確認画面
- デフォルトフォーカスは OK ボタン
- OK を押下するとサービス画面（サービス 1）へ遷移する

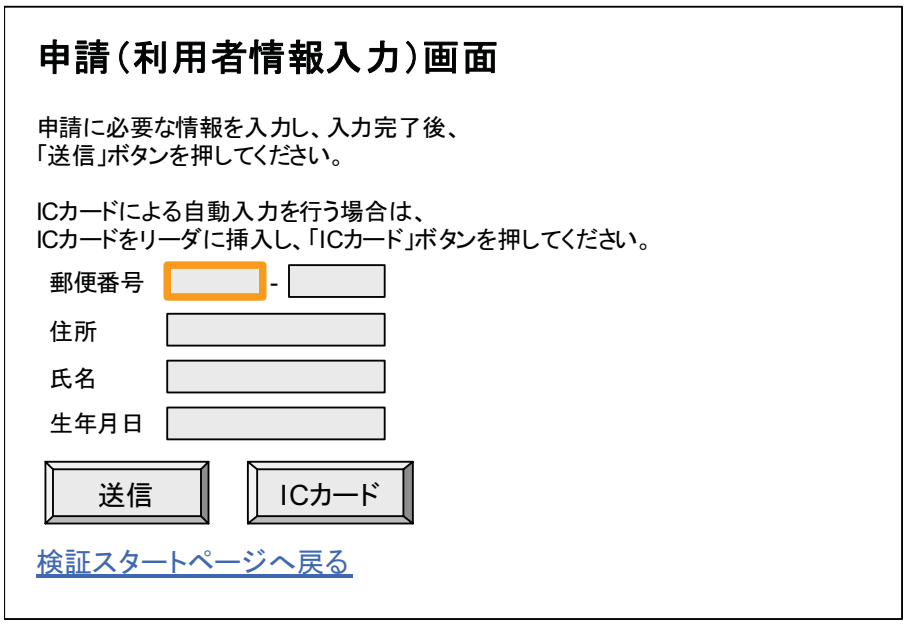
【コンテンツ仕様：サービス画面】



コンテンツ概要

・ 実際のサービス画面に相当。情報閲覧サービスを想定

【コンテンツ仕様：申請（利用者情報入力）画面】

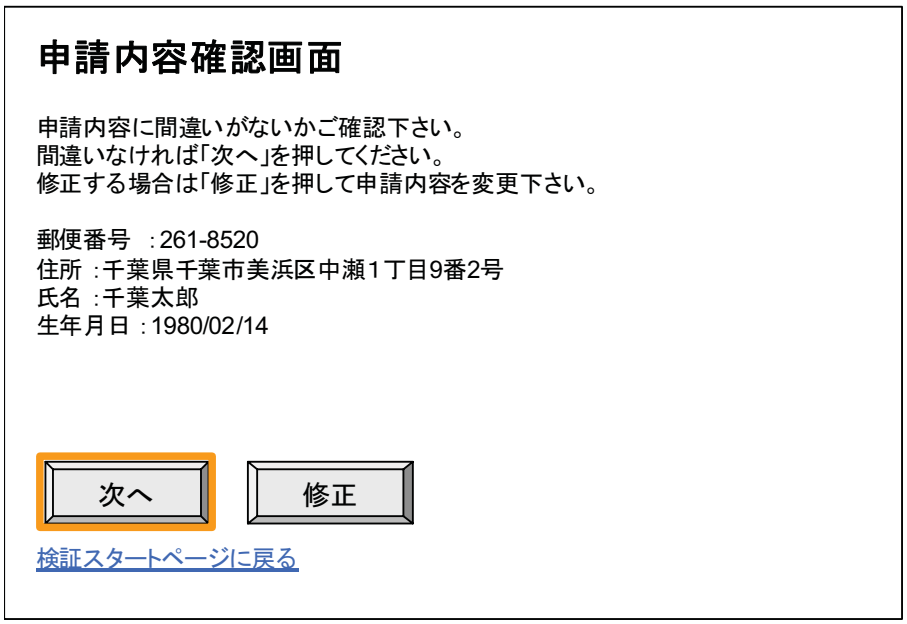


コンテンツ概要

- 利用者の情報を入力する画面
- 入力項目にすべて入力した後、送信ボタンを押下すると、（入力情報を POST し、）申請内容確認画面へ遷移する
- 入力内容は、郵便番号上 3 桁、郵便番号下 4 桁、住所、氏名、生年月日
- デフォルトフォーカスは、郵便番号上 3 桁 入力枠
- 入力に漏れがある場合は、エラーダイアログを表示し、画面遷移はしない
- IC カード を押下すると、すべての入力欄に自動的にあらかじめ（カードに）設定した情報が入力される
- 各入力項目へ入力する値を以下のように設定する

要素	入力値	文字数
郵便番号上3桁	261	3文字
郵便番号下3桁	8520	4文字
住所	千葉県千葉市美浜区中瀬 1 丁目 9 番 2 号	18文字
氏名	千葉太郎	4文字
生年月日	1980/01/01	10文字

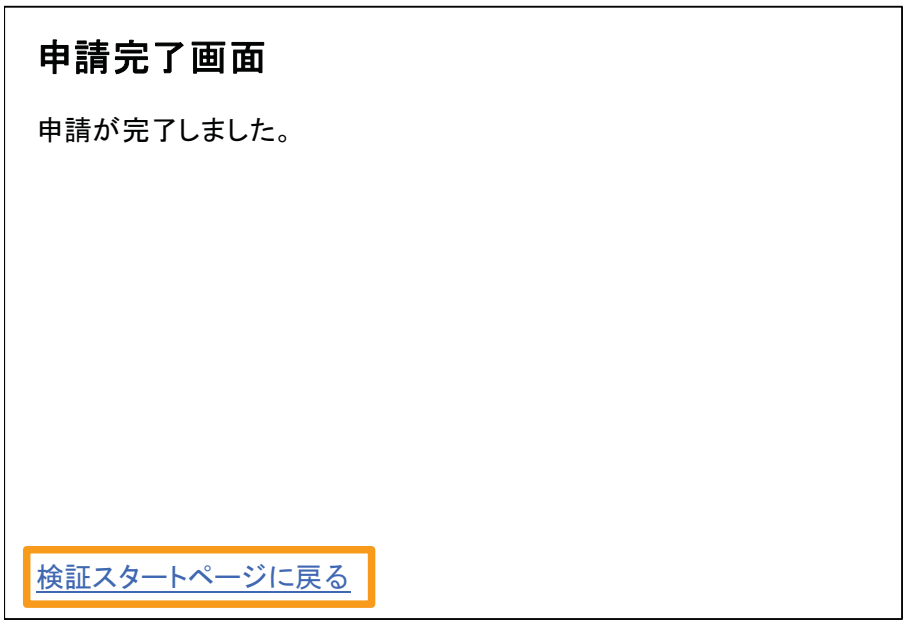
【コンテンツ仕様：申請内容確認画面】



コンテンツ概要

- 申請（利用者情報入力）画面で入力した利用者情報を表示し確認を促す画面
- 次へボタンを押すと次の画面へ遷移、修正を押すと、申請（利用者情報入力）画面へ戻る
- 確認内容は、郵便番号上 3 桁、郵便番号下 4 桁、住所、氏名、生年月日
- デフォルトフォーカスは、次へボタン

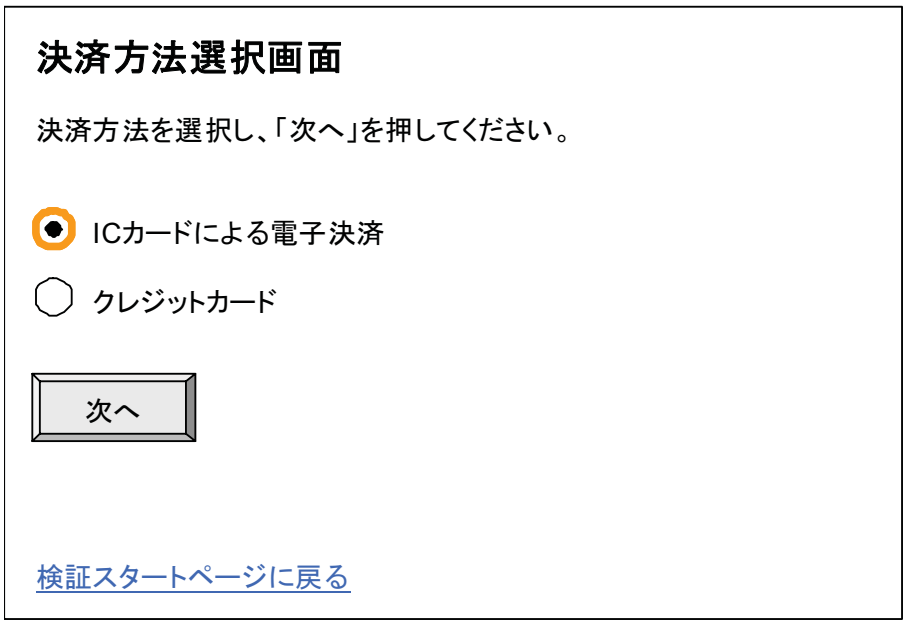
【コンテンツ仕様：申請完了画面】



コンテンツ概要

・申請完了通知画面。サービス終了

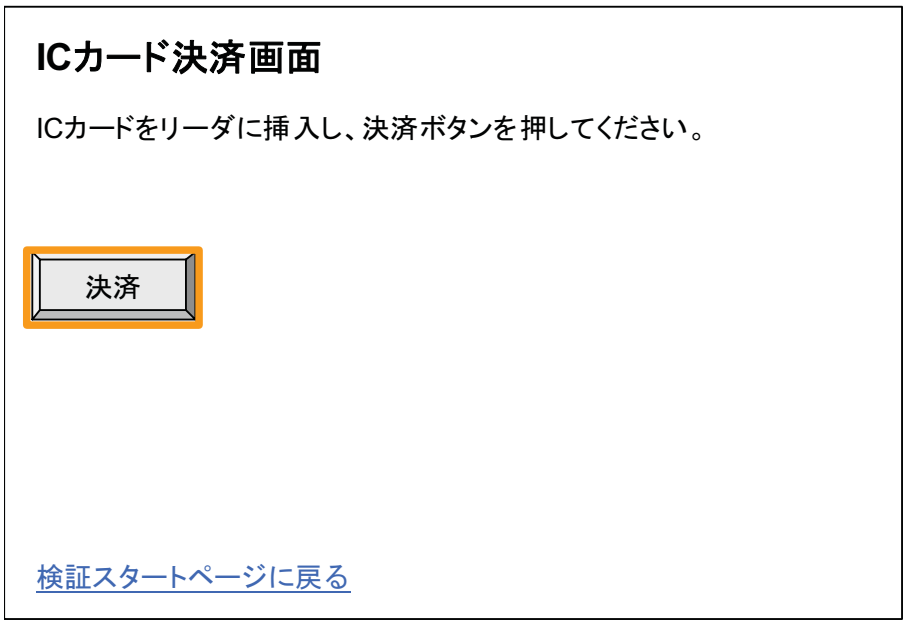
【コンテンツ仕様：決済方法選択画面】



コンテンツ概要

- 決済方法を利用者に選択させる画面
- ラジオボックス（排他）により、IC カードによる決済 か クレジットカード決済 のどちらかを選択させる
- デフォルトフォーカスは IC カードによる電子決済のラジオボタン
- ラジオボタンのデフォルト値は IC カードによる電子決済
- 次へ を押すと、ラジオボタンの設定値に応じて別ページへ遷移する
- 設定値が IC カードによる電子決済 の場合は、IC カード決済画面へ遷移
- 設定値が クレジットカードによる決済 の場合は、クレジットカード決済画面へ遷移

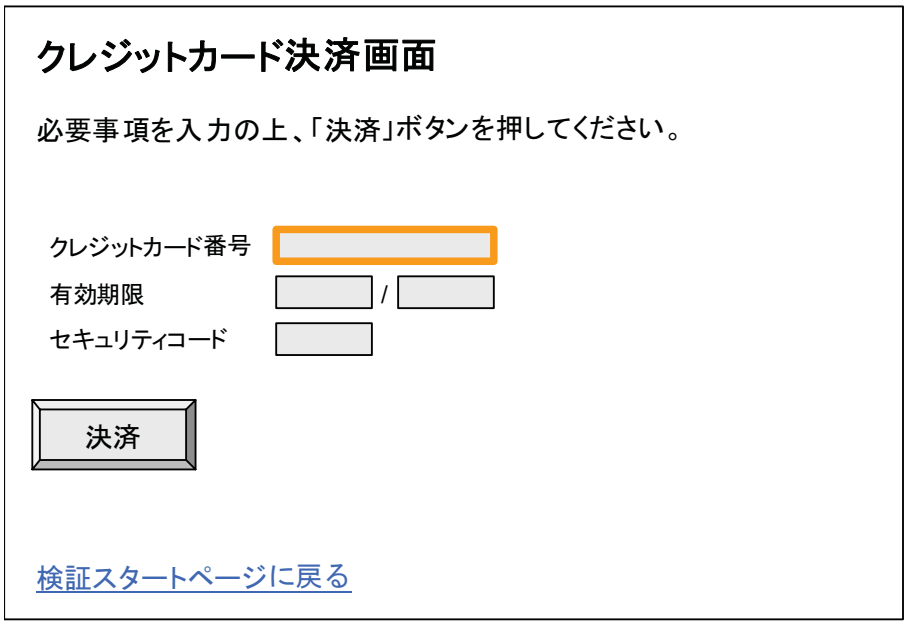
【コンテンツ仕様：IC カード決済画面】



コンテンツ概要

- IC カード決済時に、IC カードのリーダへの挿入を促す
- （IC カードをリーダへ挿入し、）決済ボタンを押すと、次の画面へ遷移する

【コンテンツ仕様：クレジットカード決済画面】

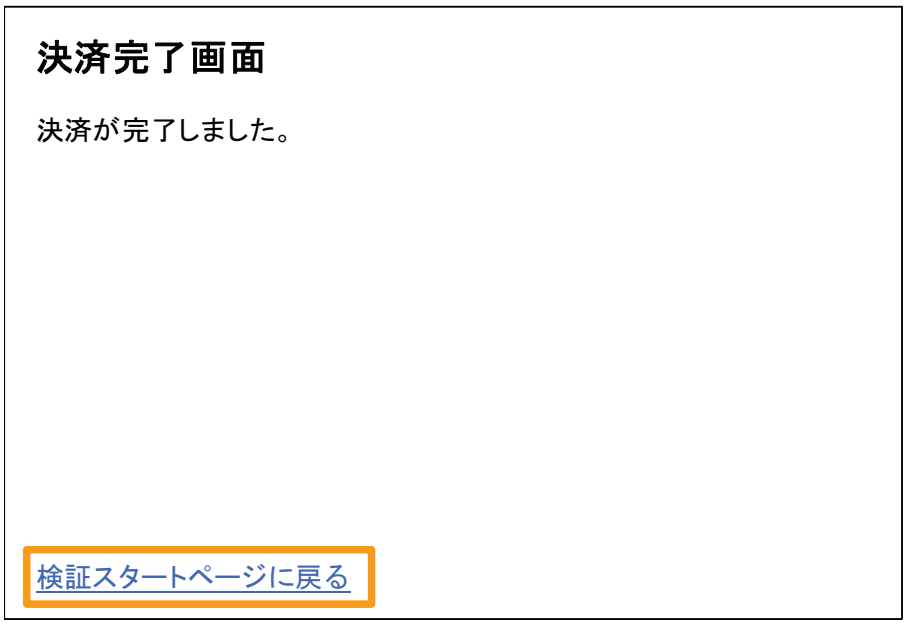


コンテンツ概要

- 利用者のクレジットカード情報を入力する画面
- 入力項目にすべて入力した後、決済ボタンを押下すると、決済完了画面へ遷移する
- 入力内容は、クレジットカード番号、有効期限、セキュリティコード
- デフォルトフォーカスは、クレジットカード番号
- 入力に漏れがある場合は、エラーダイアログを表示し、画面遷移しない
- クレジットカード番号、セキュリティコード入力欄の charactertype 属性は number
- 各入力項目へ入力する値を以下のように設定する

要素	入力値	文字数
クレジットカード番号	0123456789012345	16文字
セキュリティコード	123	3文字
有効期限	04/12	ドロップダウンリストから選択

【コンテンツ仕様：決済完了画面】



コンテンツ概要

・決済完了通知画面。サービス終了

付録 C 東京電子自治体共同運営サービス調査

東京電子自治体共同運営サービスが、個人向けに提供されているサービスに対し、文字入力項目の数や入力内容の分析を行うことで、個人情報等の自動入力の有効性についての検討材料とする。

調査内容

IC カードを用いて情報の自動入力を行うことによるユーザビリティ向上の効果を考察するために、サービスの内容と、必要となる文字入力項目の内容について調査を行った。

具体的には、提供されるサービスを「イベント等申し込み手続」と「公的申請手続」に、また、サービスに含まれる文字入力項目を「申請者個人情報入力項目」と「サービス特有の情報入力項目」にそれぞれ分類して、集計した。

サービスの分類方法

東京電子自治体共同運営サービスが提供する個人向けサービスを以下のように分類した。

- イベント等申し込み手続

  自治体が提供する、講習会への参加申し込みなどの、定期的に更新が行われ、利用者が日々利用することが想定される手続。

- 公的申請手続

  イベント申し込み手続以外の手続。自治体が提供する、各種公的書類の交付申請や、申告手続など、ライフイベント毎に必要な手続。

文字入力項目の分類方法

東京電子自治体共同運営サービスが提供する個人向けサービスに含まれる文字入力項目以下のように分類し、調査に用いた。

- 申請者個人情報入力項目

サービス全体を通して必要と考えられる、申請者の個人情報。今回の調査では、以下の 14 の情報を申請者個人情報として設定した。

氏名フリガナ，氏名，生年月日，郵便番号，住所，電話番号，メールアドレス，緊急連絡先氏名，緊急連絡先電話番号，年齢，住所フリガナ，職業，性別，本籍地

・ サービスに特有な情報入力項目

サービスに含まれる入力項目のうち、申請者個人情報入力項目以外の入力項目。各サービスを受ける際に必要な入力項目のうち、サービス実施希望日、申請事由といった、受けるサービス、タイミングによって入力内容が変わる情報、及び、家族の情報、勤務地の情報など、特定のサービスで必要となるような情報

調査対象

2010 年 2 月 2 日時点で東京電子自治体共同運営サービスにおいて 54 の自治体から提供されている電子申請届出サービス総数は、2,548 件であり、内、個人向けに提供されているサービスは、2,156 件（全体の 84.6%）であった。

また、表 C-1 は、全 54 自治体のうち、個人向けに提供されているサービスの総数が多かった上位 10 の自治体をまとめたものである。サービス総数は、東京電子自治体共同運営サービスの各申請先（自治体）の手続一覧画面で表示されるサービスの総数を集計したものであり、括弧内の数字は、提供総サービス数（2,156 件）に対する割合を表している。

本調査では、東京電子自治体共同運営サービスの中で、個人向けサービスの提供数が多かった、葛飾区と中野区を調査対象とした。

表 C-1 2010 年 2 月 2 日時点での個人向けサービス提供数上位 10 自治体

順位	自治体	個人向けサービス数
1	葛飾区	431 (20.0%)
2	中野区	134 (6.2%)
3	東村山市	133 (6.2%)
4	東京都	129 (6.0%)
5	渋谷区	111 (5.1%)
6	日野市	107 (5.0%)
7	新宿区	85 (3.9%)
8	墨田区	80 (3.7%)
9	中央区	79 (3.7%)
10	荒川区	70 (3.2%)

調査結果

2010 年 3 月 4 日時点での、葛飾区、中野区の個人向けサービスにおける入力項目に関する調査結果は以下の通りである。

表 C-2 各サービスでの文字入力の調査結果

葛飾区		サービス数	申請者個人情報入力項目を含むサービス	サービスに特有な情報入力項目を含むサービス
サービス有効数		61	60 (98%)	47 (77%)
	イベント等申し込み関連	20	20 (100%)	6 (30%)
	公的申請関連	41	40 (98%)	41 (100%)
中野区		サービス数	申請者個人情報入力項目を含むサービス	サービスに特有な情報入力項目を含むサービス
サービス有効数		105	102 (97%)	98 (93%)
	イベント等申し込み関連	9	9 (100%)	8 (89%)
	公的申請関連	96	93 (97%)	90 (94%)
葛飾区・中野区 合計		サービス数	申請者個人情報入力項目を含むサービス	サービスに特有な情報入力項目を含むサービス
サービス有効数		166	162 (98%)	145 (87%)
	イベント等申し込み関連	29	29 (100%)	14 (48%)
	公的申請関連	137	133 (97%)	131 (96%)

集計結果より、以下のことが考察できる。

- イベント等申し込みサービスについて、登録されている個数に対して有効なサービスが少なくなっているが、これはその性質上期間が限定されるためである。見方を変えると、利用者にとっては、イベント等のサービスは、利用する頻度が高いと想定できる
- サービスの 98%と、ほぼ全てで申請者個人情報項目の入力が必要であり、申請者個人情報入力項目の自動入力を実現することにより、ほぼ全てのサービスで入力の手間の低減効果が得られると考えられる
- イベント等申し込みサービスでは、2 区合計で 52%、葛飾区では 70%が個

人情報のみで申し込み可能となっており、使用頻度の高いサービスで、文字入力の手間が省ける可能性がある

- 中野区では、バスケットボール大会の申し込みや、フリーマーケット申し込みなどがあり、純粋に個人の申し込みが少ないため、サービス特有の情報が必要となっていた

付録 D 現在の電子申請の状況調査（渋谷区の例）

表 D-1 渋谷区における電子申請の状況

	申請等の種類	基本情報以外で必要になる入力（数字、選択）	基本情報以外で必要になる入力（キーボード必要）	属性情報の可能性
1	育児学級	参加希望日（選択）	子供の情報(名前、生年月日）	○（子どもの情報）
2	飼い犬の死亡届		飼い犬情報（所在地、種類、経路、性別、名前）	
3	ケアプラン作成依頼	被保険者番号	サービスを依頼する事業者	一部○ （介護保険、更新の場合の事業者）
4	家具転倒防止金具の取り付け申し込み	世帯の対象区分（選択）		
5	家庭用消火器購入申し込み	本数、古い消火器の引取りの有無	配送先（オプション）	
6	家庭用消火器詰め替え申し込み	本数	配送先（オプション） 器種・形式、メーカー名、	
7	カラスよけネット（防鳥ネット）の貸出し	仕様世帯数（数字） ネット数量(大、中、小、箱型　の数を記入）	使用者（申請者と同じ場合には選択のみ） 使用場所（使用者住所と同じ場合には選択のみ）	
8	軽自動車税納税証明書交付申請	用途（選択） 必要年度と枚数（車検用は不要）→年度と枚数の数字入力	標識番号（番号とかな入力）	
9	子ども医療費助成受給資格消滅届	消滅理由（選択、その他の場合に事由記述あり）	子どもの情報（名前、生年月日）	○（子どもの情報）
10	就労支援セミナー			
11	児童手当額改定申請	増額又は減額の理由（選択だが、その他の場合に文字記入）	子どもの情報（名前、生年月日）	○（子どもの情報）
12	児童手当消滅届		子ども名前、理由	○（子どもの情報）
13	住居表示変更証明書交付申請	変更　年月日 申請枚数	氏名、名称又は施設の名称 住所　旧住所（記入）、新住所（記入） 用途（記入）	
14	住宅用火災警報器購入申し込み	購入製品個数（個数入力） 取り付けの希望の有無（選択）	配送先（オプション）	
15	情報公開請求	請求の区分（閲覧、市長、写しの交付）	請求の区分（選択＋記述） 選択理由 選択（＋その他の記述） 公文書を特定するために必要な事項（記述）	
16	課税・納税・非課税証明書交付申請	必要とする証明書（3種類まで） 年度、枚数、証明書（選択） 使い道 選択（＋その他記入）	請求の区分（選択＋記述） 窓口に受け取りに来る人（本人以外は記入：住所、氏名、電話番号、証明する人との関係）	
17	乳幼児・子ども医療証再交付申請	医療の種類（選択） 負担者番号、受給者番号 申請理由：選択（＋その他記入）	こども1：氏名、生年月日　（Max 3）	○（子どもの情報）
18	パパ・ママ入門学級	参加希望（3つのコース、複数の日付）	パートナーの参加 参加希望（選択） パートナー（氏名、年齢）	○（パートナーの情報）

2010年2月の時点の調査による

現状で文字の入力不要(オプションを除く)

属性情報が活用できれば、文字入力不要

付録 E 検証環境で利用したデータの一例

E-1　住民票（証明書）

```
<?xml version="1.0" encoding="Shift_JIS" ?>
<xsl:stylesheet      xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
version="1.0">
  <xsl:output method="html" encoding="Shift_JIS" />
  <xsl:template match="/">
    <html>
    <head>
    <title><xsl:value-of select="books/@title" /></title>
    </head>
    <H1><DIV ALIGN="center"><FONT SIZE="3">
        <xsl:value-of select="books/@title" /></FONT></DIV></H1>

<body>
    <table width="597" border="1" bordercolor="black" CELLSPACING="0"
        CELLPADDING="0" FRAME="box">
        <tr>
            <th colspan="5"><DIV ALIGN="center">住所</DIV></th>
            <th colspan="5"><DIV ALIGN="left">
                 <xsl:value-of select="books/jyuusho" /></DIV></th>
        </tr>
         <tr>
            <th colspan="5"><DIV ALIGN="center">世帯主</DIV></th>
            <th colspan="5"><DIV ALIGN="left">
                <xsl:value-of select="books/setainushi" /></DIV></th>
        </tr>
        </table>
    <table  width="597" border="1" bordercolor="black" CELLSPACING="0"
        CELLPADDING="0" FRAME="box">
        <tr>
            <th rowspan="5" colspan="5">
               <DIV ALIGN="center">1</DIV></th>
            <th rowspan="2"><DIV ALIGN="left">氏名</DIV></th>
            <th rowspan="2"><DIV ALIGN="left">
               <xsl:value-of select="books/name" /></DIV></th>
            <th colspan="2"><DIV ALIGN="left">住民票コード</DIV></th>
            <th colspan="2"><DIV ALIGN="left">
              <xsl:value-of select="books/jyuminhyocode" /></DIV></th>

           <tr>
            <th colspan="2"><DIV ALIGN="left">生年月日</DIV></th>
            <th colspan="2"><DIV ALIGN="left">
              <xsl:value-of select="books/born" /></DIV></th>
           </tr>
        </tr>
         <tr>
            <th><DIV ALIGN="left">住所を定めた日</DIV></th>
            <th><DIV ALIGN="left">
                  <xsl:value-of select="books/jyusyo" /></DIV></th>
             <th><DIV ALIGN="left">性別</DIV></th>
```

```
            <th><DIV ALIGN="left">
                  <xsl:value-of select="books/sex" /></DIV></th>
            <th><DIV ALIGN="left">続柄</DIV></th>
            <th><DIV ALIGN="left">
                 <xsl:value-of select="books/zokugara" /></DIV></th>
         </tr>
          <tr>
            <th><DIV ALIGN="left">住民となった日</DIV></th>
            <th><DIV ALIGN="left"><xsl:value-of select="books/jyumin"
/></DIV></th>
       <th colspan="2"><DIV ALIGN="left">届出の年月日</DIV></th>
            <th colspan="2"><DIV ALIGN="left">
                 <xsl:value-of select="books/todokede" /></DIV></th>
         </tr>
          <tr>
            <th  height="30" colspan="6"><DIV ALIGN="left">
                 <xsl:value-of select="books/sonota" /></DIV></th>
         </tr>
         <tr>
            <th              rowspan="5"              colspan="5"><DIV
ALIGN="center">2</DIV></th>
            <th rowspan="2"><DIV ALIGN="left">氏名</DIV></th>
            <th rowspan="2"><DIV ALIGN="left"></DIV></th>
            <th colspan="2"><DIV ALIGN="left">住民票コード</DIV></th>
            <th colspan="2"><DIV ALIGN="left"></DIV></th>
           <tr>
            <th colspan="2"><DIV ALIGN="left">生年月日</DIV></th>
            <th colspan="2"><DIV ALIGN="left"></DIV></th>
           </tr>
         </tr>
          <tr>
            <th><DIV ALIGN="left">住所を定めた日</DIV></th>
            <th><DIV ALIGN="left"></DIV></th>
             <th><DIV ALIGN="left">性別</DIV></th>
            <th><DIV ALIGN="left"></DIV></th>
            <th><DIV ALIGN="left">続柄</DIV></th>
            <th><DIV ALIGN="left"></DIV></th>
         </tr>
          <tr>
            <th><DIV ALIGN="left">住民となった日</DIV></th>
            <th><DIV ALIGN="left"></DIV></th>
       <th colspan="2"><DIV ALIGN="left">届出の年月日</DIV></th>
            <th colspan="2"><DIV ALIGN="left"></DIV></th>
         </tr>
          <tr>
            <th height="30" colspan="6"><DIV ALIGN="left"></DIV></th>
         </tr>
         </table>
</body>
         <div ALIGN="right"><FONT SIZE="2">1 枚中     1 枚目</FONT></div>
         <P></P>
     <div><FONT SIZE="2">
        <xsl:value-of select="books/owner" /></FONT></div>
         <div ALIGN="left"><FONT SIZE="2">    </FONT></div>
```

```
        <PRE><FONT SIZE="2">      平成      年      月      日</FONT></PRE>

    <PRE><FONT SIZE="2">                                横浜市都筑区長</FONT></PRE>
    </html>
  </xsl:template>
</xsl:stylesheet>
```

E-2　特定検診情報相当（健康情報）

```
<?xml version="1.0" encoding="Shift_JIS" ?>
<?xml-stylesheet type="text/xsl" href="metabo.xsl" ?>
<books title="特定検診情報 ">
  <book isbn="検査結果">
    <保険者氏名>谷内田益義 01</保険者氏名>
    <保険者番号>123456789</保険者番号>
    <被保険者証等記号>ABCDEFGHI</被保険者証等記号>
    <被保険者証等番号>abcdefghi</被保険者証等番号>
    <住所>東京都中央区 1-1-1</住所>
    <郵便番号>123-4567</郵便番号>
    <性別>男</性別>
    <生年月日>1988 年 12 月 31 日</生年月日>

    <血液型 ABO>A</血液型 ABO>
    <血液型 Rh>Rh+</血液型 Rh>
    <身長>206</身長>
    <体重>145</体重>
    <BMI>22</BMI>
    <腹囲>85</腹囲>
    <既往歴>無し</既往歴>
    <自覚症状>無し</自覚症状>
    <自覚症状特記事項>無し</自覚症状特記事項>
    <他覚症状>無し</他覚症状>
    <血圧収縮期>120</血圧収縮期>
    <血圧拡張期>80</血圧拡張期>
    <中性脂肪>150</中性脂肪>
    <HDL コレステロール>40</HDL コレステロール>
    <LDL コレステロール>120</LDL コレステロール>
    <AST>68</AST>
    <ALT>74</ALT>
    <γ-GT>30</γ-GT>
    <空腹時血糖>100</空腹時血糖>
    <尿蛋白>-</尿蛋白>
    <ヘマトクリット>40</ヘマトクリット>
    <血色素量>14.5</血色素量>
```

<赤血球数>450</赤血球数>
<心電図>異常なし</心電図>
<眼底所見>異常なし</眼底所見>

<メタボリックシンドローム判定>異常なし</メタボリックシンドローム判定>
</book>
</books>

E-3　年金記録相当（年金情報）

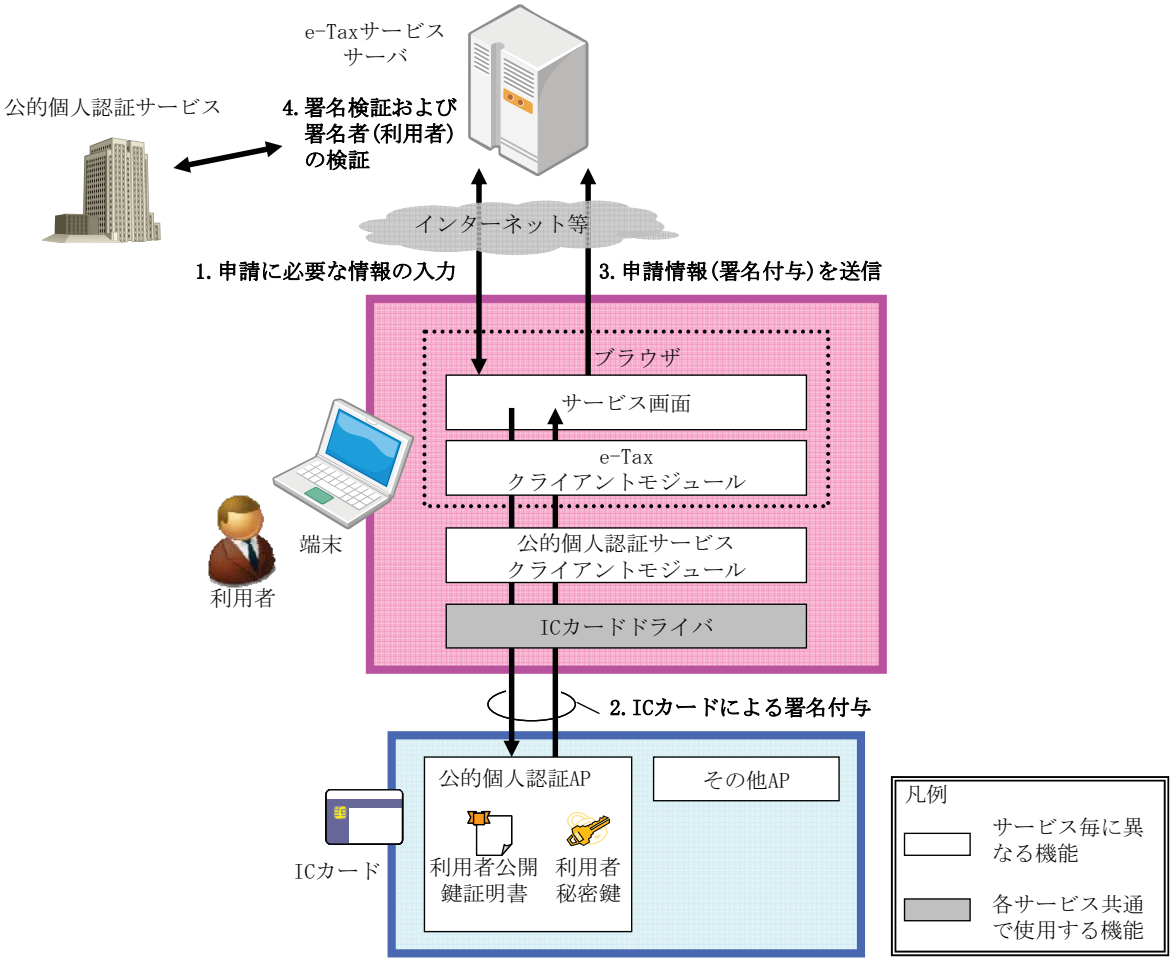
```
<?xml version="1.0" encoding="Shift_JIS"?>
<?xml-stylesheet type="text/xsl" href="nenkin.xsl" ?>
<books title="年金加入記録">
  <book isbn="検査結果">
    <保険者氏名>リコー太郎</保険者氏名>
    <保険者番号>123456789</保険者番号>
    <被保険者証等記号>ABCDEFGHI</被保険者証等記号>
    <被保険者証等番号>abcdefghi</被保険者証等番号>
    <住所>東京都中央区 1-1-1</住所>
    <郵便番号>123-4567</郵便番号>
    <性別>男</性別>
    <生年月日>1988 年 12 月 31 日</生年月日>
    <加入 1>ABC 船舶（船舶）</加入 1>
    <加入 1 開始>平成 4 年 4 月 1 日</加入 1 開始>
                <加入 1 終了>平成 5 年 10 月 1 日</加入 1 終了>
    <加入 2>国民年金（国民）</加入 2>
    <加入 2 開始>平成 5 年 10 月 1 日</加入 2 開始>
                <加入 2 終了>平成 7 年 5 月 1 日</加入 2 終了>
    <加入 3>東京株式会社（厚生）</加入 3>
                <加入 3 開始>平成 7 年 4 月 1 日</加入 3 開始>
                <加入 3 終了>平成 8 年 4 月 1 日</加入 3 終了>
    <加入 4>RSI 共済組合（共済）</加入 4>
    <加入 4 開始>平成 8 年 10 月 1 日</加入 4 開始>
    <加入 4 終了>平成 12 年 4 月 1 日</加入 4 終了>
    <加入 5>高井戸社会保険（厚生）</加入 5>
    <加入 5 開始>平成 16 年 4 月 1 日</加入 5 開始>
    <加入 5 終了>平成**年**月**日</加入 5 終了>
  </book>
</books>
```

・

付録 F（中央サーバに認証機能を一部移行させる方式)従来のICカードとの対応

本章ではサーバ連携型多目的ICカードを活用したサービスの利用イメージについて、従来のICカードによるサービスと比較した場合の各機能の対応を説明する。なおサービスとしては「国税電子申告・納税システム(e-Tax)[1]」を例に説明を行う。

従来のICカードによるサービスとして想定されるフローを 図 F-1 に示す。



※e-Taxサービスへのアクセスに際しては事前にID/パスワード等による本人認証が別途必要となるが本図では省略している。

図 F-1 従来の IC カードによるサービスフロー(想定)

[1] http://www.e-tax.nta.go.jp/

【図 F-1 のサービスフロー説明】

1. 利用者は e-Tax のサービスを提供するサーバへアクセスしブラウザにより申請に必要な情報を入力する。

2. 画面上のボタンを押下することにより、e-Tax クライアントモジュール、公的個人認証サービスクライアントモジュール、IC カードドライバ等を経由して IC カード内の公的個人認証 AP により申請情報に対して署名が付与される。署名には公的個人認証 AP が管理する利用者秘密鍵および利用者公開鍵証明書が利用される。

3. 署名が付与された申請情報が e-Tax のサービスを提供するサーバへ送信される。

4. サーバは送信された申請情報の正当性を確認するため、公的個人認証サービスと連携して、申請情報に付与された署名および署名者(利用者)の検証を行う。

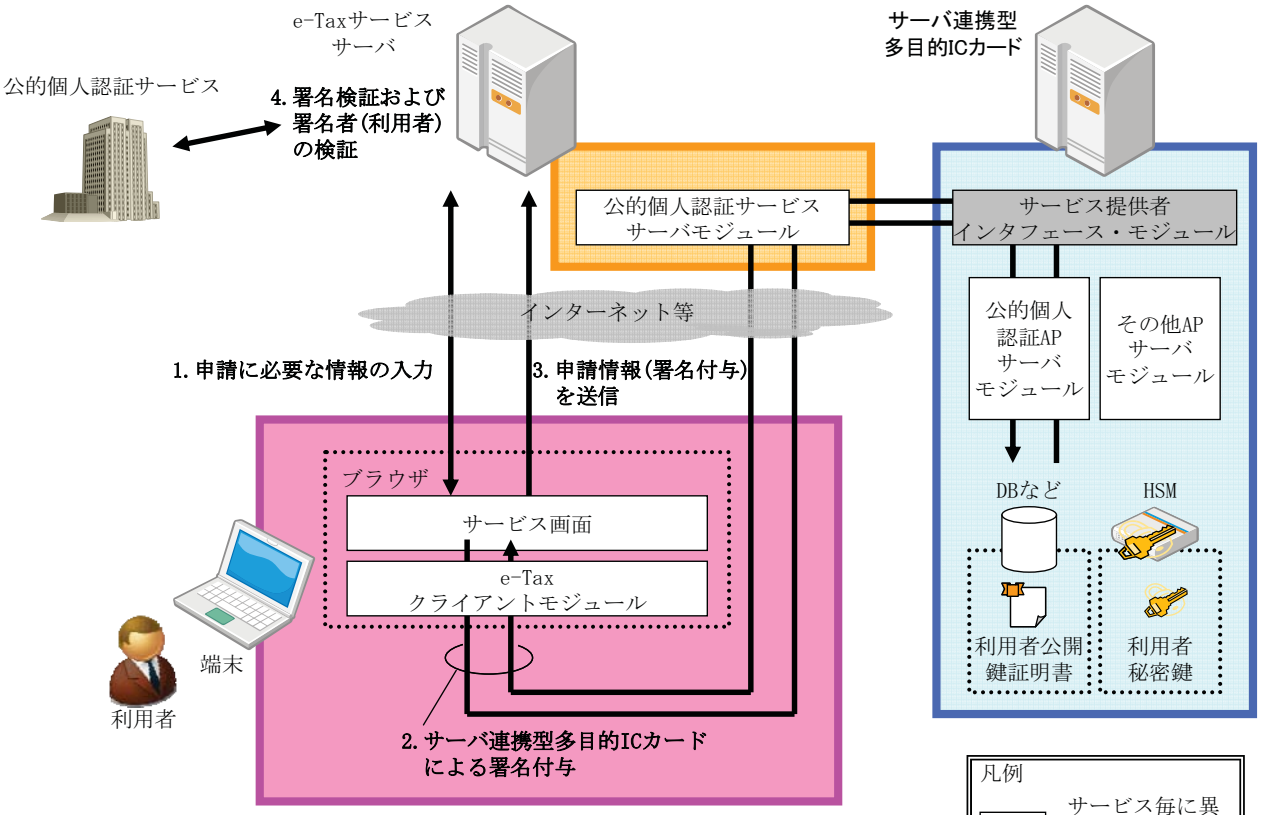
【図 F-1 の構成要素の説明】

各構成要素の説明を 表 F-1 に示す。

表 F-1 構成要素の説明(図 F-1)

項番	構成要素	説明
1	サービス画面	e-Tax サービスが提供する申請に必要な情報の入力等を行う画面。
2	e-Tax クライアントモジュール	IC カードへのアクセスを行うため e-Tax サービスが提供するクライアント用のモジュール。
3	公的個人認証サービスクライアントモジュール	公的個人認証サービスが提供する IC カード内の公的個人認証 AP へアクセスするためのモジュール。
4	IC カードドライバ	IC カードリーダライタ製品付属のドライバ。ドライバのインタフェース仕様としてはメーカ各社が製造する IC カードリーダライタを、端末上で相互利用できるようにするための仕様である「PC/SC(Personal Computer/Smart Card)」や「IT 装備都市研究事業 リーダライタ共通インターフェース」等が存在する。
5	公的個人認証 AP	IC カードに格納される公的個人認証サービスが提供するアプリケーション。利用者秘密鍵や利用者公開鍵証明書を利用した署名等、サービスに依存した処理を行う。利用者秘密鍵や利用者公開鍵証明書は IC カード内の公的個人認証 AP にて管理される。
6	その他 AP	IC カードに格納される「公的個人認証 AP」以外のアプリケーション（「住基ネット AP」等)。

次に、サーバ連携型多目的ICカードを用いたサービスフローを 図 F-2 に示す。なお本図は従来のICカードによるサービスとの機能比較を目的とするため、ポータルサーバや認証サーバといったサービスに依存しない共通的なシステムは省略している。



※e-Taxサービスへのアクセスに際しては事前にICカード等による本人認証が別途必要となるが本図では省略している。

※本図のサービスイメージはサーバ連携型多目的ICカードを活用したサービスの一例として 示すものである。

図 F-2 サーバ連携型多目的 IC カードを用いたサービスフロー

【図 F-2 のサービスフロー説明】

1. 利用者は e-Tax のサービスを提供するサーバへアクセスしブラウザにより申請に必要な情報を入力する。

2. 画面上のボタンを押下することにより、e-Tax クライアントモジュールは e-Tax のサービスを提供するサーバに対し申請情報に対する署名付与を要求する。サーバは公的個人認証サービスサーバモジュールおよびサーバ連携型多目的 IC カードの提供するサービス提供者インタフェース・モジュールを介して、サーバ連携型多目的 IC カード内に存在する公的個人認証 AP サーバモジュールを実行し、利用者秘密鍵および利用者公開鍵

証明書により署名を付与する。

3. 署名が付与された申請情報が e-Tax のサービスを提供するサーバへ送信される。

4. サーバは送信された申請情報の正当性を確認するため、公的個人認証サービスと連携して、申請情報に付与された署名および署名者(利用者)の検証を行う。

【図 F-2 の構成要素の説明】

各構成要素の説明を 表 F-2 に示す。

表 F-2 構成要素の説明(図 F-2)

項番	構成要素	説明
1	サービス画面	e-Tax サービスが提供する申請に必要な情報の入力等を行う画面。
2	e-Tax クライアントモジュール	公的個人認証サービスサーバモジュールへアクセスするため e-Tax サービスが提供するクライアント用のモジュール。
3	公的個人認証サービスサーバモジュール	公的個人認証サービスが提供するサーバ連携型多目的ICカード内の公的個人認証APサーバモジュールへアクセスするためのモジュール。
4	サービス提供者インタフェース・モジュール	サーバ連携型多目的 IC カードが提供するサービス提供者向けのインタフェース・モジュール。各サービス提供者は本インタフェースを通じてサーバ連携型多目的 IC カードが利用する各種機能を利用する。
5	公的個人認証 AP サーバモジュール	サーバ連携型多目的 IC カードに格納される公的個人認証サービスが提供するアプリケーション。利用者秘密鍵や利用者公開鍵証明書を利用した署名等、サービスに依存した処理を行う。利用者秘密鍵や利用者公開鍵証明書はサーバ連携型多目的 IC カード内の DB および HSM にて管理される。
6	その他 AP サーバモジュール	サーバ連携型多目的 IC カードに格納される「公的個人認証 AP サーバモジュール」以外のモジュール。

各機能の対応を 表 F-3 に示す。

表 F-3 機能の対応

項番	従来ICカードを用いたサービスでの機能	サーバ連携型多目的ICカードを用いたサービスでの機能	機能単位	機能提供者の例
1	サービス画面	サービス画面	サービス	e-Tax サービス提供者
2	e-Tax クライアントモジュール	e-Tax クライアントモジュール	サービス	e-Tax サービス提供者
3	公的個人認証サービスクライアントモジュール	公的個人認証サービスサーバモジュール	サービス	公的個人認証サービス提供者
4	ICカードドライバ*1	サービス提供者インタフェース・モジュール*2	共通	*1 IC カード RW 製品ベンダ *2 サーバ連携型多目的ICカード
5	公的個人認証AP	公的個人認証APサーバモジュール	サービス	公的個人認証サービス提供者
6	その他AP	その他APサーバモジュール	サービス	その他サービス提供者など

※サービス毎に異なる機能として提供されるものを「サービス」、各サービス共通で使用する機能として提供されるものを「共通」としている。