行政業務システム連携推進事業
（アクセス手段としての携帯電話の利便性向上方法の検証）
研究成果報告書

研究開発課題名	課題ア：オンラインでの ID 情報の格納・利用を実現するモバイルアクセスシステムの技術仕様の検討 課題イ：実験環境による検証 課題ウ：制度・運用面の課題の検討 課題エ：本事業に基づく成果の普及
研究機関名	株式会社　日立製作所（研究責任者：小野瀬 健太郎）

目次

1. 事業の概要

1.1 事業の背景

総務省「携帯電話エリア整備推進検討会」報告書[1]によれば，国内の携帯電話契約数は，1 億 1200 万件を超え，国民生活及びあらゆる社会経済活動を支える重要なインフラとなっている。人口カバー率においても主要移動体通信事業者に関して 99～100%を達成している。このようにすでに携帯電話は国民にとってなくてはならない社会インフラとなった。また、iPhone や Android 端末などのいわゆるスマートフォンの利用も拡大している。さらに、高度情報通信ネットワーク推進戦略本部（本部長：内閣総理大臣）が公表した「新たな情報通信技術戦略工程表」[2]によれば、携帯電話等からの行政サービスへのアクセス方式に関して、平成 25 年度までに国民の 50%以上が、利用頻度・利便性の高い行政サービスを自宅等からの週 7 日 24 時間のオンライン利用を可能とするという政府目標が掲げられている。

また、平成 24 年度以降、ＮＦＣ（near field communication：短距離無線通信）機能を実装した携帯電話端末の市場投入が予定されている。ＮＦＣ機能を実装した携帯電話端末では、オフライン・オンラインで耐タンパデバイスへ ID/Password 等の認証情報やポイントやクーポン等のサービスに関連した利用者情報を格納し、これらの格納した情報の読込が可能となる。この機能を活用することで政府がかかげる目標を実現するため、携帯電話端末から利用する電子行政サービスに係る利用者の本人認証の利便性を向上させ、世代を問わず、国民目線での行政サービスを実現するための取り組みが必要である。

1.2 事業の目的

背景に述べたように、国民が世代を問わず携帯電話端末から本人認証を含めたサービスを簡単かつセキュアに利用できる仕組みが必要である。平成 21 年度の総務省の調査研究では、携帯電話端末からの電子行政サービス等へのアクセス手段について、サービス提供機関が利用者に対して発行する情報（以下、ID 情報という。）の安全な格納先として、①国が発行する公的 IC カードを携帯電話にかざして利用する公的 IC カード方式、②携帯電話端末に挿入可能なデバイスを国が発行し携帯電話端末に挿入して利用する携帯電話向け公的カード方式、③携帯電話端末内に国が発行する情報を書き込み利用する公的認証情報方式、等の検討を行っている。耐タンパデバイスとしては、公的 IC カード方式の場合は、フルサイズの IC カード、携帯電話向け公的カード方式の場合には、IC チップを搭載したフラッシュメモリ型デバイス、公的認証情報方式の場合には、UICC（Universal Integrated Circuit Card）などが想定できる。

しかしながら、現状では、図 1-1 に示すように、耐タンパデバイスに ID 情報や利用者情

報を格納し利用するためには、サービス提供機関ごとに様々な携帯電話端末上で動作するアプリケーション（以下、携帯アプリ）を個別に開発する必要がある。また、利用者は、利用したいサービス提供機関ごとに携帯アプリをダウンロードする必要がある。

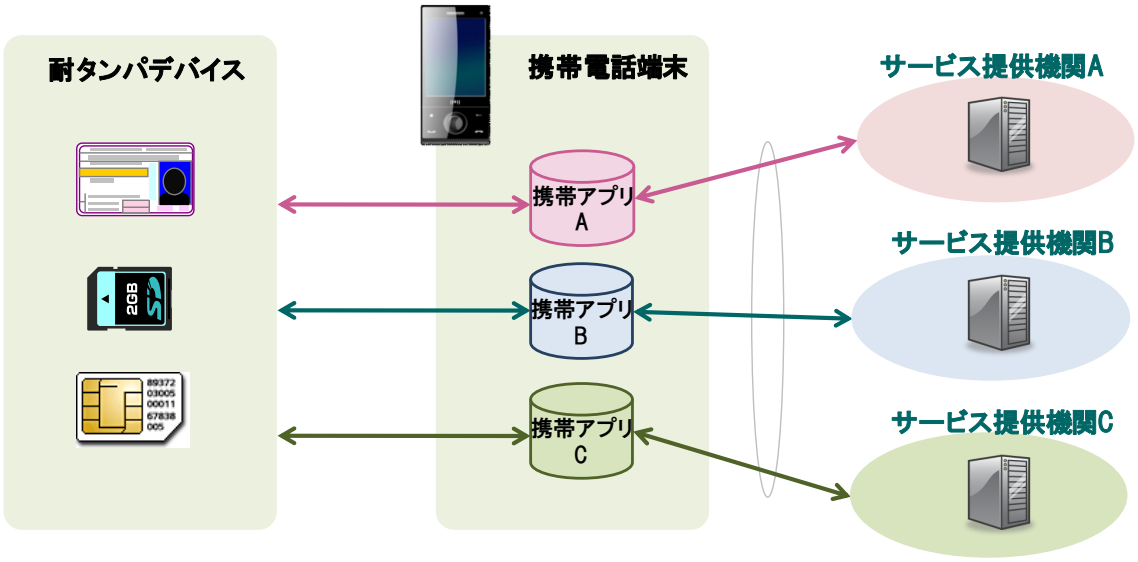


図 1-1 現状の耐タンパデバイスを利用するサービスの問題点

このように、耐タンパデバイスを利用するサービスを実現する際には、サービス提供機関・利用者の双方にとって負担がかかっている。これらの負担を解消するため、サービス提供機関・利用者の双方が共同で利用することのできる基盤システムを検討する。具体的には､個々のサービス提供機関に代わって ID 情報の格納と読み込みを安全に行うサーバと、これに対応して ID 情報を耐タンパデバイスに格納・利用するための複数のサービス提供機関から共通的に利用できる携帯アプリ（以下、共通アプリ）からなるモバイルアクセスシステムの技術仕様の検討及び実証実験による検証、並びに制度・運用面における課題抽出とその解決方策の検討、その検討・開発結果に基づく標準化団体でのガイドライン化を目指すことを目的とする。

1.3 事業の目標

サービス提供機関・利用者の双方にとって負担軽減が可能な ID 情報をオンライン上で安全に耐タンパデバイスに格納・利用するモバイルアクセスサーバと、これに対応する携帯電話端末上の共通アプリからなるモバイルアクセスシステムを検討する（図 1-2 参照)。

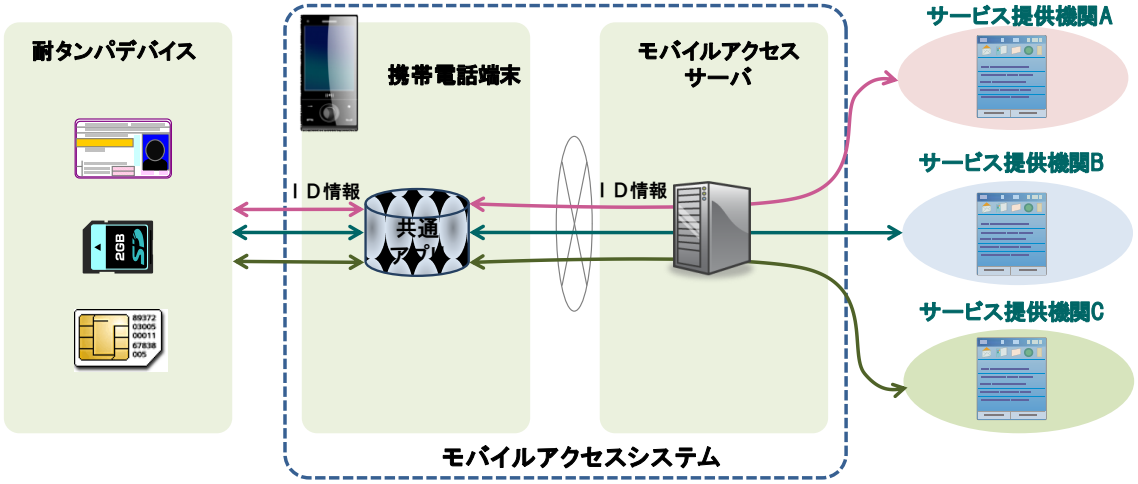


図 1-2 モバイルアクセスシステムの全体構成

具体的には、以下の検討・開発を行い、標準化団体でのガイドライン化を目指とともに、サービス提供機関の携帯アプリの開発、運用負荷の軽減、利用者の利用促進を図る。

(1) 課題ア：以下を実現するモバイルアクセスシステムの技術仕様の策定

- サービス提供機関ごとに携帯アプリを開発することなく、オンライン上で安全に耐タンパデバイスへの ID 情報の格納と、格納した ID 情報を利用するためのモバイルアクセスシステムの技術仕様を策定する。
- ID 情報としては、電子証明書だけでなく、その他の会員 ID やチケット情報などの任意の情報を共通の方式で扱える技術仕様を策定する。
- モバイルアクセスシステムは、サービス提供機関に応じて様々なアクセス方式に対応させるため、「公的 IC カード方式」「携帯電話向け公的カード方式」「公的認証情報方式」のどの方式にも適用できる共通の方式（共通プロトコル/API で実現可能なもの）で扱える技術仕様を策定する。
- 検討にあたっては３方式ともサービス提供機関からみて、共通プロトコル/API で実現可能な技術仕様を策定する。
- ID 情報の提供格納の主体としては、複数のサービス提供機関を想定した技術仕様を策定する。
- 検討にあたっては、委員会にて、今後の想定される技術動向等を十分に考慮し、技術仕様を策定する。

(2) 課題イ：実験環境による検証

- 課題アの検討結果に基づき、実験環境を構築し、サービス提供機関・利用者双方の

観点での運用性、利便性の検証ならびに、技術的検証を行う。

- 検証にあたっては、利用者に普及しつつあり、オープンプラットフォームを採用したAndroid OSを搭載したスマートフォンを用いる。
- 耐タンパデバイスとして、「携帯電話向け公的カード方式」に対応したICチップを搭載したフラッシュメモリ型デバイスを用いた実証実験システムを構築する。
- 実証実験システムのデモシナリオは、課題ウでのユースケースの検討結果に基づいたものとする。
- 委員会にてデモを実施し、応答速度や動作間隔などのユーザビリティについて受容性を検証する。
- 実験環境を課題ウのサービス提供機関（連携自治体）の住民の方に体験していただき、ヒアリングを実施し、ユーザビリティとしての受容性を検証する。

(3) 課題ウ：制度・運用面の課題の検討

- 行政、医療、金融のカテゴリ別に既存サービスの高度化の観点から洗い出しを行い、適用サービスを選定する
- 選定した適用サービスに対するセキュリティレベルの要件を現行の制度・運用を参考に調査・整理する。
- 選定した適用サービスについて各サービス提供機関にヒアリングを実施し、セキュリティレベルと認証強度、現行制度面の制約事項、社会環境、政策動向等より実現性を評価し、カテゴリ別に最適なサービス一つを選定する。
- 現行の制度・運用、システムを整理し、新サービスによる想定運用フローを策定し、対比することで新たに発生する課題を整理し、対策案、方針等を検討する。

(4) 課題エ：本事業に基づく成果の普及

- （株）ＮＴＴドコモ、ＫＤＤＩ（株)、ソフトバンク（株)、イー・アクセス（株)、および有識者として東京工科大学手塚悟教授、行政機関などで構成された委員会を設置する。
- 委員会にて上記①～③での検討・検証結果を議論し、将来性、実現性を考慮した技術仕様及び、制度・運用面における方策案を策定する。
- 本事業の成果となる技術仕様等に関しては一般社団法人 電波産業会（ARIB） 高度無線通信研究委員会 モバイルコマース部会を活用しながらガイドライン化を図る。

図 1-3 に本成果報告書の構成を示す。まず、課題アでサービスに依存しない一般論での仕様の策定を行う。次に課題イで、課題アの仕様を前提とした実証実験について記述する。実証実験で利用する想定サービス提供機関やサービスと対になるICカードアプリケーションなどは課題イに記述する。課題ウでは、課題アの仕様および課題イの実証実験の結果を

もとに、制度・運用面の課題の検討を行う。課題エでは、課題アの部分集合をガイドラインとして規定する。

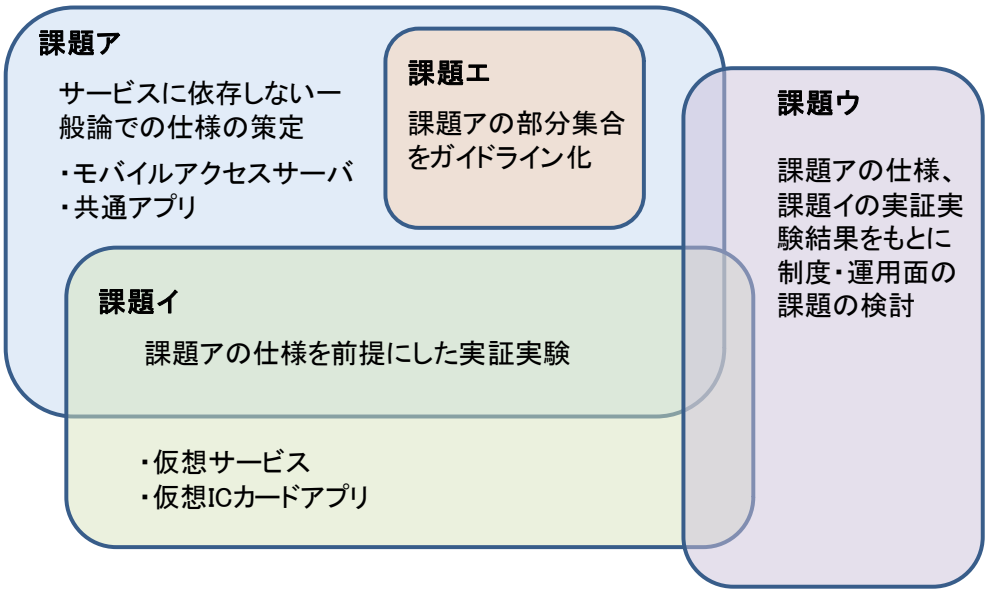


図 1-3 本成果報告書の構成

1.4 事業の実施体制

以下に本事業の実施体制を示す。

(1) 開発・実証担当者

株式会社日立製作所

・セキュリティ・ソリューション事業部

○小野瀬 健太郎（責任者）

長谷川 大造

桑名 利幸

森田 光

川野 隆

山田 知明

佐藤 隆行

荻原 正樹

松井 裕介

池上 隆介

上松 正史
堀　健太郎
・横浜研究所
藤城 孝宏
梅澤 克之
萱島 信
礒川 弘実
森田 伸義

(2) 委員会委員

以下に委員会委員を示す。

手塚 悟 （東京工科大学　教授）
佐藤 一夫（株式会社ＮＴＴドコモ　モバイルデザイン推進室　室長）
安部 孝太郎（(株) ＮＴＴドコモ モバイルデザイン推進室 主査）
阪東 謙一（ＫＤＤＩ株式会社　コンバージェンス推進本部　担当部長）
田中 卓弥（ＫＤＤＩ（株）コンバージェンス推進本部　課長補佐）
小峰 正裕（ソフトバンクモバイル株式会社　海外事業推進本部　室長代行）
立原 彩子（ソフトバンクモバイル（株）海外事業戦略室）
渡辺 芳治（イー・アクセス（株）デバイス開発部　副部長）
宮北 幸典（イー・アクセス（株）デバイス開発部　端末推進Ｇ　課長代理）
小野瀬 健太郎（株式会社日立製作所　セキュリティ・トレーサビリティ事業　部長）
川野 隆（株式会社日立製作所 セキュリティ・トレーサビリティ事業部 技師）
梅澤 克之（株式会社日立製作所 横浜研究所 主任研究員）

以下にオブザーバを示す。

黒瀬 泰平（総務省 情報流通行政局 情報流通振興課 課長）
本橋 充成（総務省 情報流通行政局 情報流通振興課 課長補佐）
古謝 玄太（総務省 情報流通行政局 情報流通振興課 主査）
前原 正男（厚生労働省 政策統括官付社会保障担当参事官室 室長補佐）
浜田 哲 （厚生労働省 政策統括官付社会保障担当参事官室 技術参与）
鈴木 重郎（厚生労働省 政策統括官付社会保障担当参事官室 主査）
安田 浩（東京電機大学 未来科学部 教授）
安井 秀行（ＮＰＯ団体アスコエ 代表）

以下に事務局を示す。

勝家 由樹（株式会社日立製作所 セキュリティ・トレーサビリティ事業部 技師）
川野 隆（株式会社日立製作所 セキュリティ・トレーサビリティ事業部 技師）

（敬称略）

（参考文献）

[1] “携帯電話エリア整備推進検討会報告書,”携帯電話エリア整備推進検討会, 2010 年 5 月,http://www.soumu.go.jp/main_content/000066466.pdf

[2]“新たな情報通信技術戦略工程表” 高度情報通信ネットワーク推進戦略本部（本部長：内閣総理大臣）（平成 22 年 6 月）

2. 課題ア　モバイルアクセスシステムの技術仕様の策定

2.1. 概要

2.1.1. 対象範囲

本研究の対象範囲を図 2-1 に示す。図 2-1 に示すように、複数のサービス提供機関が、携帯電話端末利用者の耐タンパデバイスへの認証情報や個人情報などの ID 情報（※）を書き込こむ。また、書き込んだ ID 情報を読み込んでサービス提供に利用する。このような、耐タンパデバイスへの ID 情報の書き込みと読み込みを安全かつ容易に行うことを本実証事業の対象範囲とする。

※本事業で想定する ID 情報とは、ユーザがサービスを受ける際に使用する、会員 ID などのユーザ識別子と認識情報のようなユーザ本人であることを証明する情報、およびサービス利用時に作成されるユーザ固有の情報を指す。

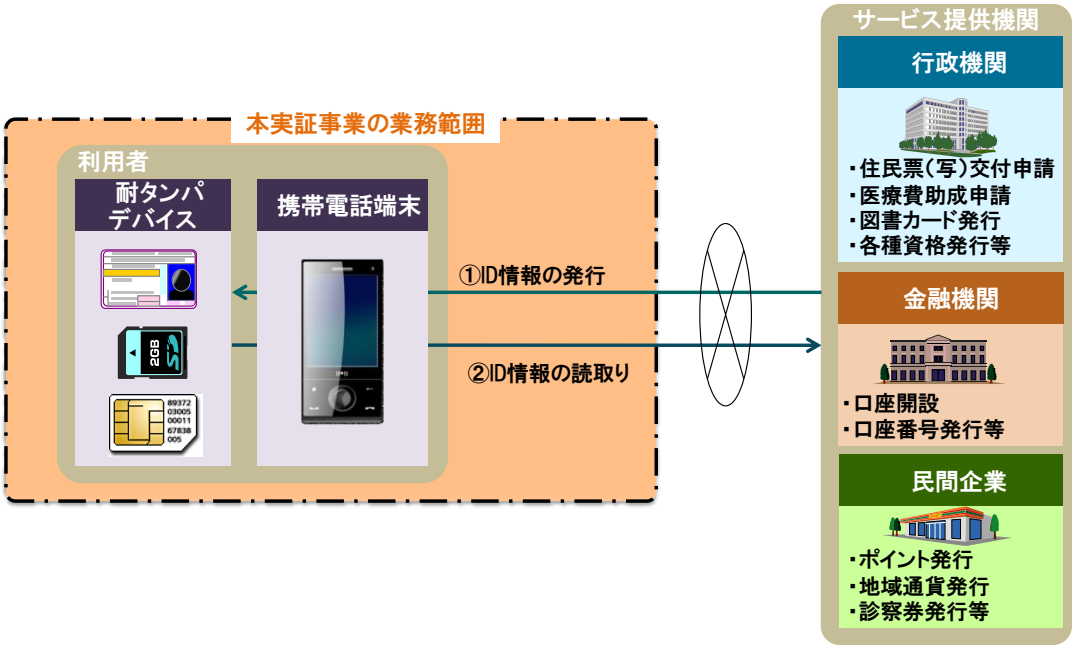


図 2-1 本実証事業の業務範囲

2.1.2. 現状の課題

複数のサービス提供機関が、携帯電話端末利用者の耐タンパデバイスへの ID 情報の書き込みや読み込みを行おうとする場合、現状では図 2-2 に示すように、サービス提供機関ごとに携帯アプリを開発・運用する必要がある。また、利用者は各サービス提供機関が提供

する携帯アプリを個別にダウンロード・インストールする必要がある。さらに今後は携帯電話端末の OS のオープン化が進むことが想定されるため、携帯アプリのセキュリティを確保する仕組みも必要となる。

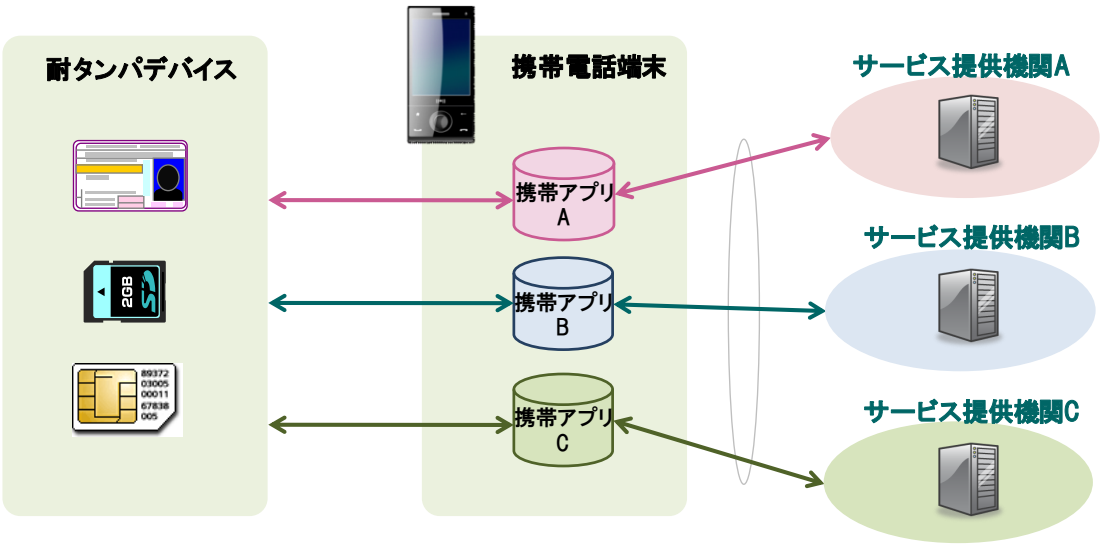


図 2-2 業務範囲の現状と課題

2.1.3. 解決方法

上記現状の課題を解決するために、図 2-3 に示す構成のモバイルアクセスシステムを提案する。具体的には、サービス提供機関が耐タンパデバイスにアクセスする際に共通的に利用できるモバイルアクセスサーバおよび携帯電話端末上の共通アプリからなるモバイルアクセスシステムを提案する。

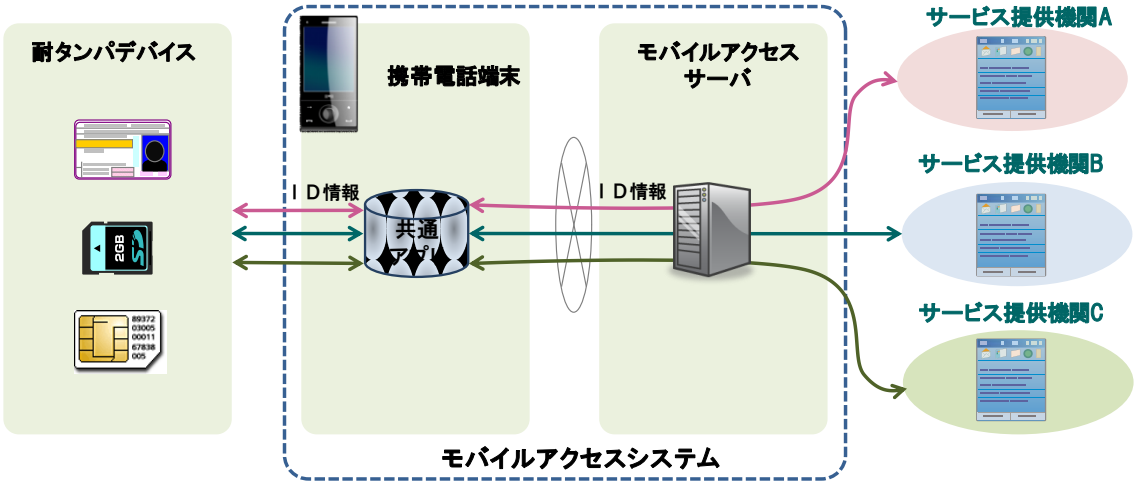


図 2-3 現状課題の解決方法（提案方式）

具体的には、サービス提供機関は、耐タンパデバイスに対する命令（コマンド）を生成し、モバイルアクセスサーバに通知する。モバイルアクセスサーバは、共通アプリを経由して、耐タンパデバイスとのセキュアな通信路を確立する。（具体的には、モバイルアクセスサーバと耐タンパデバイスが共有するセッション鍵を使って安全な通信路（セキュアチャネル）を張る）。モバイルアクセスサーバは、確立された安全な通信路を使ってサービス提供機関から通知されたコマンドを、共通アプリを経由して耐タンパデバイスに送信する。共通アプリは、耐タンパデバイスの複数種類の差異を吸収し、モバイルアクセスサーバからのセキュアチャネル上のコマンドを正しく耐タンパデバイスに届けることを行う。このときに不正なサービス提供機関がコマンドを発行できないような仕組みを組み込む。また、携帯電話端末もオープン端末を想定しているため、共通アプリは不正者の攻撃の対象になるという前提を置き、鍵などの秘密情報を持たせない設計とする。

このようなモバイルアクセスシステムを導入することにより、耐タンパデバイスの ID 情報を格納・参照するための複数サービス提供機関が共通的に利用できる仕組みをシステムとして利用することで、サービス提供機関が個別に携帯アプリを開発しなければならないという負担を減らすことが期待できる。また、サービス提供機関ごとに個別の携帯アプリを開発する方式では、サービスごとに利用者は携帯アプリをダウンロードする必要があるが、共通アプリであればダウンロードの手間は省ける。さらに、共通アプリを用いることによってユーザインタフェースなどが統一化され、利用者の操作性を向上させることが期待できる。

2.2. 前提条件

以下に課題アの仕様の検討におけるシステムの前提条件を示す。なお、ID 体系の仕組みやその管理方法に関する仕様、個別のサービスに関する仕様は、本章の範囲外とする。

(1) 端末に関する前提条件

- データ通信が行える端末を前提とする。音声通話だけしかできない端末は対象としない。
- 今後は携帯電話端末の OS のオープン化が進むことが想定される。そのような OS 上でも安全に耐タンパデバイスへアクセスできるようにするため、携帯電話端末上ではマルウェア等が動作する可能性があり、必ずしも安全性が確保されるとは限らない。つまり耐タンパデバイスへアクセスする鍵などの秘密情報の管理を正しく行うことができない場合があるという前提を置いたうえで仕様の検討を行うものとする。
- ブラウザから携帯電話端末内のアプリを起動できるものとする。
- 逆に、携帯電話端末内のアプリからブラウザを起動できるものとする。
- 耐タンパデバイスにアクセスできる機能を有するものとする。

(2) 耐タンパデバイスに関する前提条件

- 携帯電話端末を使ってデータの送受信ができるものとする。
- 耐タンパデバイス内の処理は、安全に行えるものとする。つまり、耐タンパデバイス上で動作するアプリケーションは、正当なサービス提供機関によって作成され、正当な方法で耐タンパデバイス内へロードされ、その動作も正しく動くものとする。
- 耐タンパデバイスは、マルチアプリケーション対応とし、複数のサービス提供機関が相乗りできるものとする。異なるサービス提供機関の IC カードアプリケーションはファイアウォールで適切に守られているとする。
- 平成 21 年度の総務省の調査研究「携帯電話から電子行政サービス等へのアクセス技術の調査研究」で対象とされた①国が発行する公的 IC カードを携帯電話にかざして利用する公的 IC カード方式におけるフルサイズ IC カード(ISO14443 Type A/Type B)、②携帯電話端末に挿入可能なデバイスを国が発行し携帯電話端末に挿入して利用する携帯電話向け公的カード方式における IC チップを搭載したフラッシュメモリ型デバイス、③携帯電話端末内に国が発行する情報を書き込み利用する公的認証情報方式における UICC (Universal Integrated Circuit Card) を前提とする。
- 携帯電話端末に対して OTA (Over the Air) で耐タンパデバイスへアクセスするための唯一の世界標準である GlobalPlatform に準拠した IC カードを前提とする。

(3) ネットワークに関する前提条件

- サービス提供機関とモバイルアクセスサーバはインターネットに接続されるため、携帯電話端末とサービス提供機関間、携帯電話端末とモバイルアクセスサーバ間は、

モバイル網以外のオープンなネットワークを通ることになる。このため、必ずしも安全性が確保されるとは限らないものとする。 つまり、携帯電話端末とサービス提供機関間、携帯電話端末とモバイルアクセスサーバ間は、ネットワーク上のデータの盗聴や改ざんの恐れがあるものとする。

- サービス提供機関とモバイルアクセスサーバ間の通信は VPN や専用線などで保護されるため安全であるものとする。

(4) サービス提供機関に関する前提条件

- 偽造や改ざん、漏洩などから守るべき何らかの価値を有する情報（ID 情報）を携帯電話端末に接続された耐タンパデバイスに対して付与し、また、耐タンパデバイスから読み込み、その ID 情報を利用することを行うサービス提供機関を対象とする。
- サービス提供機関の動作は、運用も含め正しく安全に行われるものとする。
- サービス提供機関とモバイルアクセスサーバは事前の契約に基づいて鍵の共有などを行っているものとする。

(5) モバイルアクセスサーバに関する前提条件

- モバイルアクセスサーバ内の動作は、運用も含め正しく安全に行われるものとする。
- サービス提供機関とモバイルアクセスサーバは事前の契約に基づいて鍵の共有などを行っているものとする。

2.3. セキュリティ要件

前述の前提条件のもとで、提案システムは、以下に示すセキュリティ要件を満たす必要がある。

(1) 不正な携帯電話端末アプリケーションへの対応

（1-1） 悪意のある携帯電話端末アプリケーションによる耐タンパデバイス内のセキュアデータへのアクセスの防止

(2) 通信路の安全性の確保

（2-1） サービス提供機関―（共通アプリ）―モバイルアクセスサーバ間の通信路の安全性の確保

（2-2） モバイルアクセスサーバー（共通アプリ）－耐タンパデバイス間の通信路の安全性の確保

（2-3） サービス提供機関－モバイルアクセスサーバ間の通信路の安全性の確保

(3) 成りすまし防止

（3-1） サービス提供機関の成りすましの防止

（3-2） モバイルアクセスサーバの成りすましの防止

2.4. 全体システム構成

本実証事業のシステムの全体構成を図 2-4 に示す。行政機関や、金融機関や民間企業なども含めて複数のサービス提供機関が、携帯電話端末を使う利用者に対して種々のサービスを提供することを想定している。今回対象とするサービスは、利用者の ID 情報を利用することを前提とするものである。ID 情報は、利用者の携帯電話端末からアクセスできる耐タンパデバイスに保存するものとする。

耐タンパデバイスへの情報の書き込み、および読み込みには、通常、サービス提供機関が個別に耐タンパデバイスの自身の領域に対してセキュアなチャネルを構築し、そのチャネルを経由してのみ読み書きが可能となる。今回の提案では、複数のサービス提供機関への負担を軽減するために、前記耐タンパデバイスへの情報の読み書きを代行するモバイルアクセスサーバをモバイルアクセスシステム側に用意し、サービス提供機関の負担を軽減する。

また、耐タンパデバイスと直接データの送受信を行う携帯アプリに関しても、従来であれば個々のサービス提供機関が自身のサービスのために携帯アプリを個別に開発する必要があったが、今回の提案では、複数のサービス提供機関が共通的に利用できる共通アプリで処理することとする。

また、耐タンパデバイスへの ID 情報の読み書きに対する結果通知サービスや、耐タンパデバイスからの ID 情報の読み込みを本人認証に利用した後の実際のサービスなどは、Web ベースで提供されることを想定している。よって、携帯電話端末内での共通アプリとブラウザの連携、モバイルアクセスシステム内でのモバイルサイトとモバイルアクセスサーバの連携を実現することで安全なサービス提供の基盤を実現する。

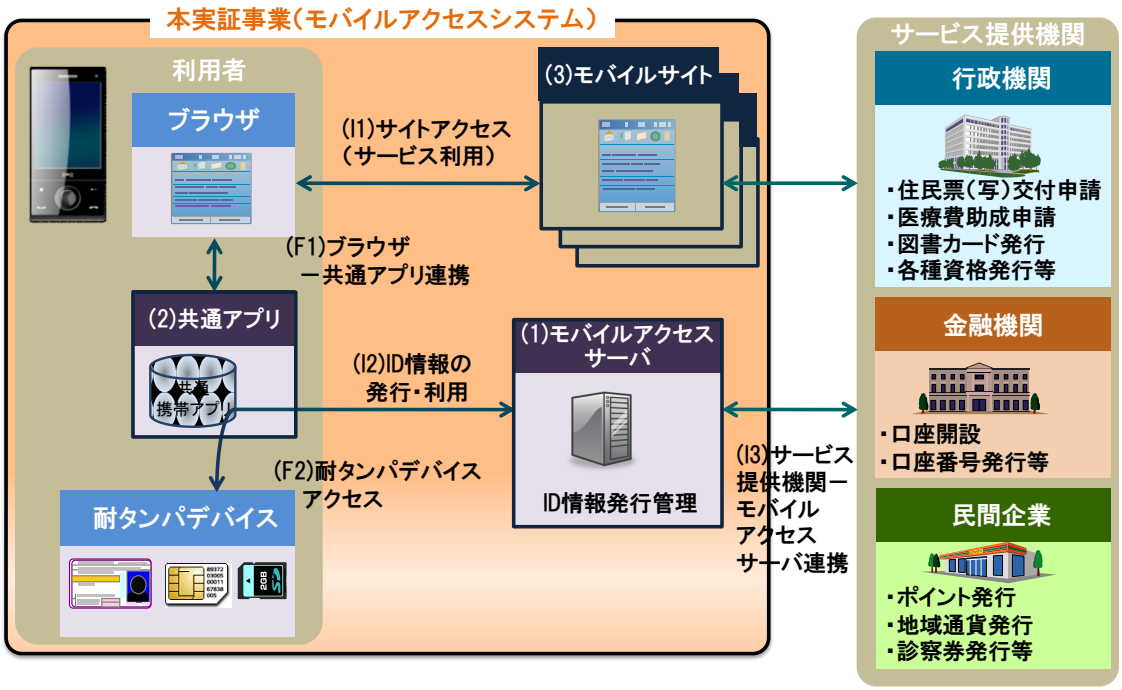


図 2-4 本実証事業のシステムの全体構成

エンティティの説明

- サービス提供機関:行政機関や金融機関、民間企業などの ID 情報を利用者に付与して、その ID 情報を利用することを前提としたサービスを提供する機関
- モバイルサイト：サービス提供機関ごとに構築する携帯電話端末向けサイト
- モバイルアクセスサーバ：サービス提供機関との契約に基づいて、利用者の耐タンパデバイスとセキュアな通信路を確保し、暗号化した IC カードコマンドの送受信を行うサーバ。
- 共通アプリ：モバイルアクセスサーバと通信を行い、受信したデータを耐タンパデバイスに送信し、耐タンパデバイスからのレスポンスをモバイルアクセスサーバに返信する携帯アプリ。共通アプリ自身は秘密情報を保持しない設計とすることでオープンな携帯電話端末においても安全性を確保する。
- 耐タンパデバイス:IC チップを搭載したデバイス。携帯電話端末と非接触 IC 通信(NFC)で通信を行うフルサイズの IC カードや、IC チップを搭載したフラッシュメモリ型のデバイス、UICC (Universal Integrated Circuit Card) などを想定する。

具体的には、以下の流れで処理が実行される。

(1) 利用者が携帯電話端末内のブラウザでモバイルサイトにアクセスする(図 2-5 の(I1))。

(2) モバイルサイトからのレスポンスによってブラウザから共通アプリが起動される (図 2-5 の (F1))。

(3) 共通アプリからモバイルアクセスサーバに接続し、モバイルアクセスサーバから ID 情報の発行を受ける（図 2-5 の（I2））。

(4) 発行する ID 情報の管理はサービス提供機関が行う。当該 ID 情報をサービス提供機関からモバイルアクセスサーバに通知する。（図 2-5 の（I3）のようにサービス提供機関とモバイルアクセスサーバ間で直接通知する方法と、（I1）と（I2）のインタフェースを使って共通アプリを経由して通知する方法がある）。

(5) 上記ステップで発行された ID 情報を共通アプリが耐タンパデバイスに書き込む(図 2-5 の（F2））。

(6) 書き込み後の結果通知は、モバイルアクセスサーバを経由して、さらにブラウザを経由して、モバイルサイトに通知され、最終的にブラウザの画面でユーザに通知される。

課題アでは、図 2-5 の破線で示した範囲を検討範囲とする。破線の矩形が新規に導入されるサブシステム（機能）であり、破線の楕円が、新規に定義するインタフェースである。

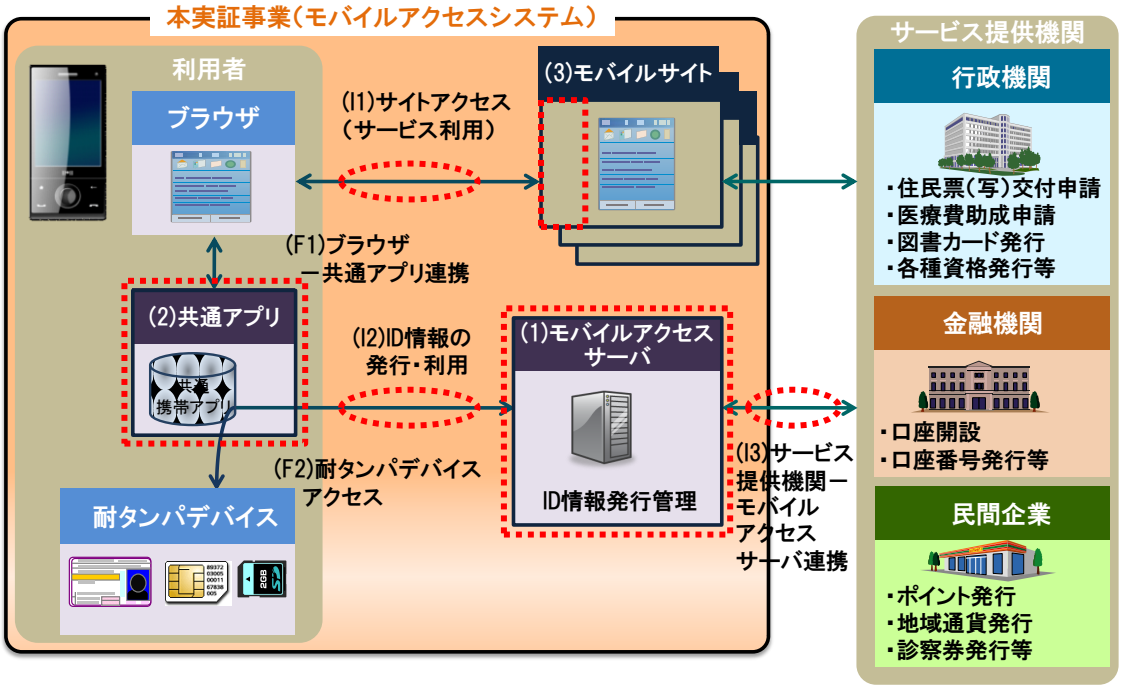


図 2-5 課題アの検討範囲

なお、ブラウザと共通アプリの連携に関しては、現状利用できる携帯電話端末の機能に準ずる。また、耐タンパデバイスと共通アプリのインタフェースに関しては、耐タンパデバイスの種類によって使われるデバイスドライバなどが変わる事が想定されるためハードウェアレベルでの規定は行わない。さらに、モバイルサイトとサービス提供機関は同一機関が運営すると考えられるため、モバイルサイトーサービス提供機関間のインタフェース

の規定は行わない。

2.5. システム概要

2.5.1. 機能の概要

以下に、各エンティティの機能の概要を記述する。

(1) モバイルアクセスサーバ（全機能）（図 2-5 の（1））

- 受付処理機能：
  サービス提供機関から送信された情報（サービス事業者 ID、受付番号、APDU 生成年月日、APDU 実行順序、APDU コマンド）を受け取り、情報が正しい場合は、受け取った情報を DB に登録する。
- 共通アプリアクセス機能：
  サービス提供機関から共通アプリ経由で転送されるデータが本当に正しいサービス提供機関から送信されたデータなのかを確認する。さらに、携帯電話端末内の共通アプリを経由して、耐タンパデバイスとセキュアセッションを確立し、携帯電話端末内の共通アプリに対して暗号化されたコマンドを送受信し、結果をサービス提供機関に返信する。

(2) 共通アプリ（全機能）（図 2-5 の（2））

- APDU 転送機能：
  モバイルアクセスサーバから受信した暗号化されたコマンドを耐タンパデバイスへ送信し、耐タンパデバイスからのレスポンスをモバイルアクセスサーバに返信する。

(3) モバイルサイト（一部機能）（図 2-5 の（3））

- ID 情報発行機能：
  耐タンパデバイスに送信したいコマンドをモバイルアクセスサーバに移譲し、かつ、携帯電話端末のブラウザを経由して、共通アプリを起動させ、耐タンパデバイスに ID 情報を送信する。
- 処理結果受信機能：
  モバイルアクセスサーバから耐タンパデバイス内での処理結果を受信し、返される処理結果が本当に正しいモバイルアクセスサーバから送信されたデータなのかを確認する。

2.5.2. インタフェースの概要

以下に、各インタフェースの概要を記述する。

(1) 共通アプリ起動インタフェース（図 2-5 の I1 および F1）

- JavaScript で共通アプリを起動する。
- 要求元：モバイルサイト（ブラウザ経由）、応答先：共通アプリ
- 通信形式：実行時パラメータ

(2) 共通アプリ連携インタフェース（図 2-5 の I2 および F2）

- 耐タンパデバイスに対してセキュアにアクセスするために、共通アプリとモバイルアクセスサーバが通信する。
- 要求元：共通アプリ、要求先：モバイルアクセスサーバ
- 通信形式：HTTPS（XML）

(3) APDU 移譲インタフェース（図 2-5 の I3）

- 耐タンパデバイスに対して実行する APDU コマンドをサービス提供機関からモバイルアクセスサーバに移譲する。
- 要求元：サービス提供機関、要求先：モバイルアクセスサーバ
- 通信形式：HTTPS（XML）

(4) APDU 実行結果通知インタフェース（図 2-5 の I3）

- 耐タンパデバイスに対して実行した APDU コマンドの結果をモバイルアクセスサーバからサービス提供機関に通知する。
- 要求元：モバイルアクセスサーバ、要求先：サービス提供機関
- 通信形式：HTTPS（XML）

(5) 再アクセスインタフェース（図 2-5 の I1,I2 および F1）

- モバイルアクセスサーバから共通アプリに処理終了を通知し、共通アプリからサービス提供機関へ再アクセスする。
- 要求元：モバイルアクセスサーバ（共通アプリ経由、ブラウザ経由）、要求先：サービス提供機関
- 通信形式：HTTPS

2.5.3. プロトコルの概要

以下に各エンティティ間のデータの流れ（プロトコル）に関して記述する。図 2-6 は、サービス提供機関による耐タンパデバイスとの ID 情報の書き込み、及び読み込みの際のデータの流れを示す簡易的な図である。

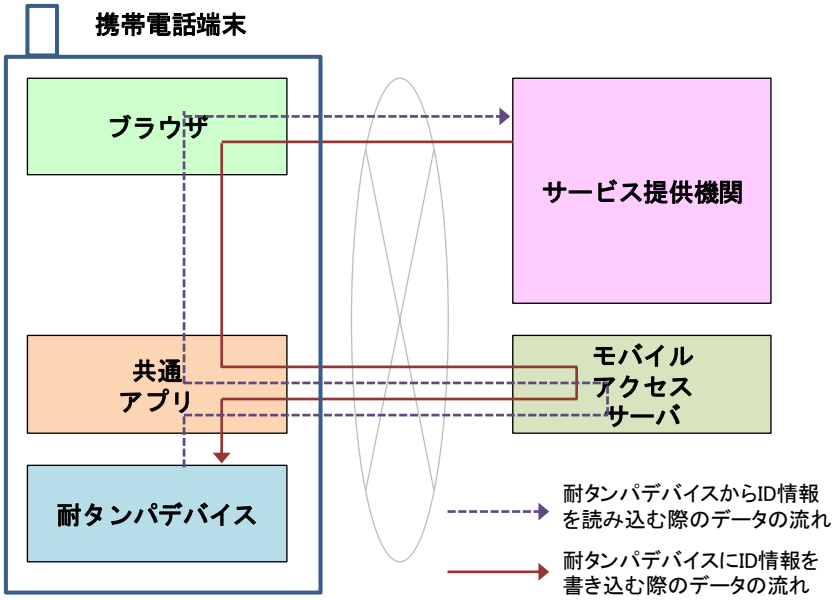


図 2-6 データの流れを示す簡略図

図 2-6 に示す実線の矢印が、サービス提供機関から耐タンパデバイスへ送信する ID 情報の流れである。サービス提供機関はブラウザ経由で共通アプリを起動し、その後、共通アプリからモバイルアクセスサーバに接続され、モバイルアクセスサーバは、共通アプリ経由で耐タンパデバイスに ID 情報を送信する。その際に、モバイルアクセスサーバと耐タンパデバイスはセキュアな通信路を確立する。点線の矢印は、耐タンパデバイスからモバイルアクセスサーバへ送信する ID 情報の流れである。サービス提供機関は、ブラウザ経由で共通アプリを起動し、その後、モバイルアクセスサーバ経由で共通アプリから耐タンパデバイスにアクセスし、ID 情報をモバイルアクセスサーバに送信する。モバイルアクセスサーバは、共通アプリ、ブラウザ経由でサービス提供機関に ID 情報を送信する。

図 2-7 にデータの流れを表す。さらに詳細なフローを示す。

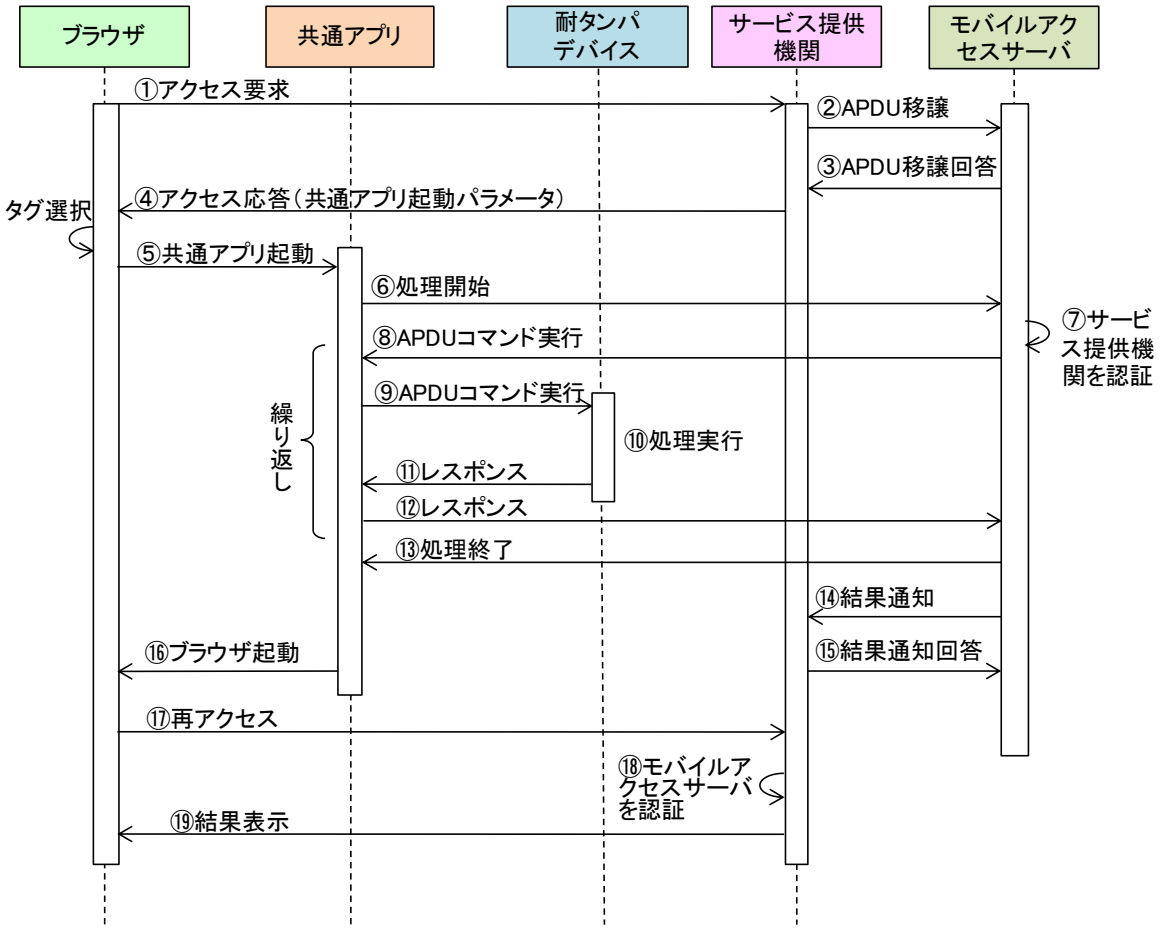


図 2-7 データの流れを示す詳細図

まず、利用者が携帯電話端末のブラウザ経由でサービス提供機関にアクセスする①。サービス提供機関からモバイルアクセスサーバに対して、耐タンパデバイスに送るべき APDU コマンドを送信し②、回答を受信する③。

次にサービス提供機関から、アクセス応答として、ブラウザに対して共通アプリの起動パラメータを送信する④。ブラウザは、共通アプリを起動し、サービス提供機関から受信したデータを共通アプリに渡す⑤。

耐タンパデバイスにアクセスするための秘密情報を保持しない共通アプリは、そのままでは耐タンパデバイスにアクセスできないため、モバイルアクセスサーバに処理開始要求を送信する⑥。④、⑤、⑥でサービス提供機関からモバイルアクセスサーバに送信されるデータは暗号化されている。モバイルアクセスサーバは、共通アプリから転送された処理開始要求データが正しいサービス提供機関から送信された要求データだということを確認する⑦。モバイルアクセスサーバは、耐タンパデバイス内のサービス提供機関の管理下の領域の IC カードアプリケーションに送信するための APDU コマンドを共通アプリに返信する⑧。共通アプリは受信した APDU コマンドを耐タンパデバイスに転送する⑨。耐タンパデ

バイスは、APDU コマンドに従って耐タンパデバイス内で処理を実行し⑩、結果をレスポンスデータとして共通アプリ経由でモバイルアクセスサーバに返す⑪⑫。APDU コマンドは複数回実行されることが想定されるため⑧～⑫が繰り返される。なお、この APDU コマンド送受信の初期の段階で、モバイルアクセスサーバと耐タンパデバイス内のサービス提供機関の管理下の領域の IC カードアプリケーションとの間で、セキュアセッションの確立（暗号通信を行うための鍵共有）が行われ、以降の APDU コマンドは安全な通信路内で送受信される。よって APDU コマンドは共通アプリを経由するが共通アプリはその内容を見ることはできない。

サービス提供機関は耐タンパデバイスでの処理結果をモバイルアクセスサーバから受信し⑬、受信結果をモバイルアクセスサーバに返信する⑭。

モバイルアクセスサーバは、共通アプリに対して処理終了通知を送信し⑮、共通アプリはブラウザを起動する⑯。起動されたブラウザでサービス提供機関に再度アクセスする⑰。⑬、⑯、⑰でモバイルアアクセスサーバからサービス提供機関に送信されるデータは暗号化されている。サービス提供機関は共通アプリからブラウザ経由で転送されたデータが正しいモバイルアクセスサーバからのデータであるか否かを確認する⑱。最後にサービス提供機関からブラウザに対して結果を表示させる⑲。

なお、図 2-7 では、②、③と⑭、⑮のステップにおいて、直接サービス提供機関とモバイルアクセスサーバの間で、APDU コマンドの送信と処理結果の受信を行っているが、②の APDU コマンドの移譲の代わりに、④～⑥のそれぞれの送信データに移譲すべき APDU コマンドを含めることもできる。その場合には、⑬、⑭の処理結果受信の代わりに、⑮～⑰のそれぞれの送信データに処理結果を含める。

また、⑬、⑭の処理結果通知処理は、⑧～⑫の繰り返しが終わった後に一括して行っているが、⑫のレスポンスを受け取る都度、サービス提供機関に処理結果を通知しても良い。

2.6. セキュリティ対策

本節では、2.3 節で示したセキュリティ要件に対する対策を示す。

(1) 不正な携帯電話端末アプリケーションへの対応

(1-1)

【要件】悪意のある携帯電話端末アプリケーションによる耐タンパデバイス内のセキュアデータへのアクセスの防止

【対策】耐タンパデバイスへアクセスするためには、耐タンパデバイスと相互認証を行ったうえで安全な通信路を確保（セキュアセッションの確立）するようにし、共有鍵を持たない携帯電話端末アプリケーションは、耐タンパデバイスにアクセ

スできないようにした。また、共通アプリも共有鍵を持たず、モバイルアクセスサーバ側に共有鍵を持たせることで、共通アプリがマルウェアやウィルスに感染しても共有鍵が漏洩することがないような設計にした。

(2) 通信路の安全性の確保

(2-1)

【要件】サービス提供機関―（共通アプリ）―モバイルアクセスサーバ間の通信路の安全性の確保

【対策】図 2-7 のデータの流れを示す詳細図の④、⑤、⑥のサービス提供機関からモバイルアクセスサーバへ送信されるデータおよび、⑬、⑯、⑰でモバイルアアクセスサーバからサービス提供機関に送信されるデータは暗号化される。よって安全性が確保されるとは限らない共有アプリを経由してもデータは漏えいしない。

(2-2)

【要件】モバイルアクセスサーバー（共通アプリ）－耐タンパデバイス間の通信路の安全性の確保

【対策】モバイルアクセスサーバと耐タンパデバイス間は、GlobalPlatform 仕様に基づく相互認証および暗号通信を行うため安全性は確保される。

(2-3)

【要件】サービス提供機関－モバイルアクセスサーバ間の通信路の安全性の確保

【対策】2.2 節のネットワークに関する前提条件で示したように、サービス提供機関－モバイルアクセスサーバ間の通信路の安全性は確保されているという前提を置いている。

(3) 成りすまし防止

(3-1)

【要件】サービス提供機関の成りすましの防止

【対策】図 2-7 のデータの流れを示す詳細図の⑦で示したように、共通アプリを経由してモバイルアクセスサーバが受信したデータには、サービス提供機関の署名が付与されており、モバイルアクセスサーバはその署名を検証することで、正しいサービス提供機関から送信されたデータだということを確認できる。

(3-2)

【要件】モバイルアクセスサーバの成りすましの防止

【対策】図 2-7 のデータの流れを示す詳細図の⑱で示したように、共通アプリを経由してサービス提供機関が受信したデータには、モバイルアクセスサーバの署名が付与されており、サービス提供機関はその署名を検証することで、正しいモバイルアクセスサーバから送信されたデータだということを確認できる。

2.7. 機能の詳細

本節では、共通アプリ、モバイルアクセスサーバ、サービス提供機関の各エンティティの機能に関して詳細を記述する。なお、図 2-7 に示した全体フローと本節で詳述する機能は下図のような対応関係になっている。

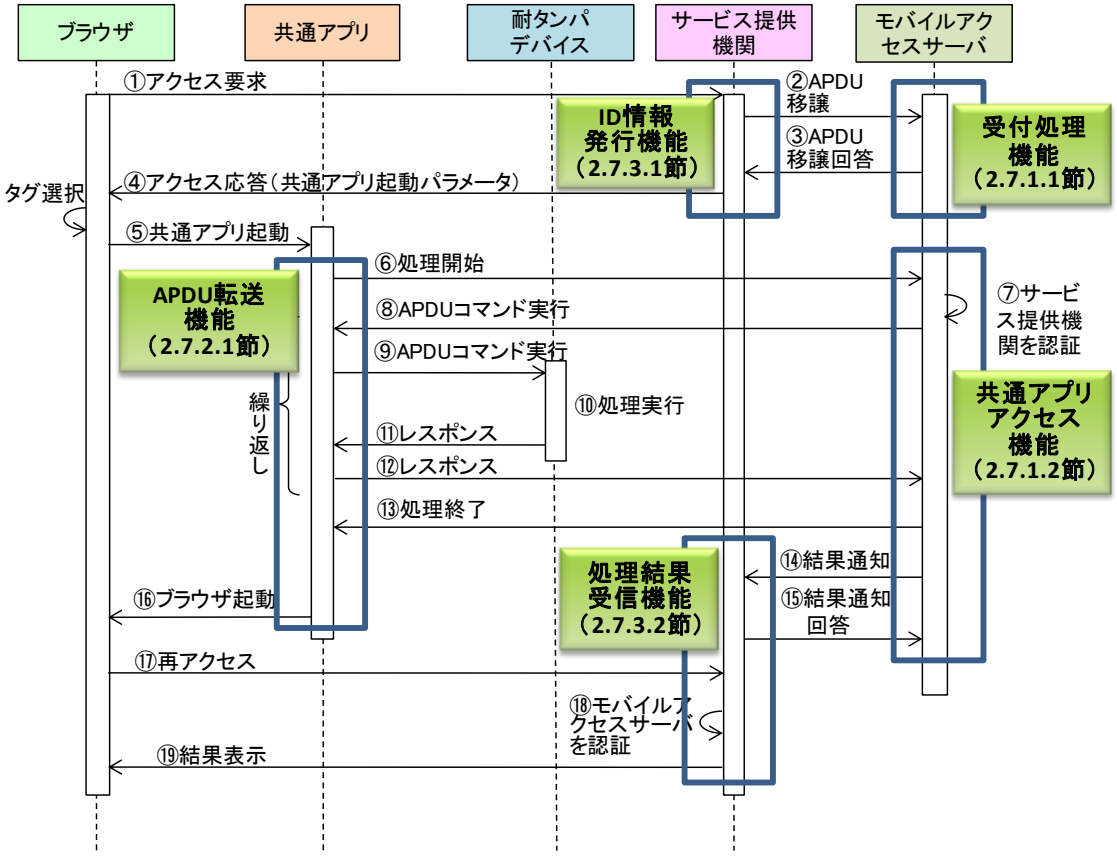


図 2-8 本節の構成と、各機能の対応関係

2.7.1. モバイルアクセスサーバの機能

モバイルアクセスサーバは、サービス提供機関から APDU の移譲を受ける受付処理機能、および、共通アプリに対して、処理開始、セキュアセッション確立、APDU コマンド送信、処理終了を送信する共通アプリアクセス機能を有する。

前提として、モバイルアクセスサーバとサービス提供機関はセキュアな通信が確立されているものとする。

2.7.1.1.　　受付処理機能

サービス提供機関から送信された情報（サービス事業者 ID、受付番号、APDU 生成年月日、APDU 実行順序、APDU コマンド）を受け取り、情報が正しい場合は、受け取った情報を DB に登録する。受付処理機能の処理フローを以下に示す。

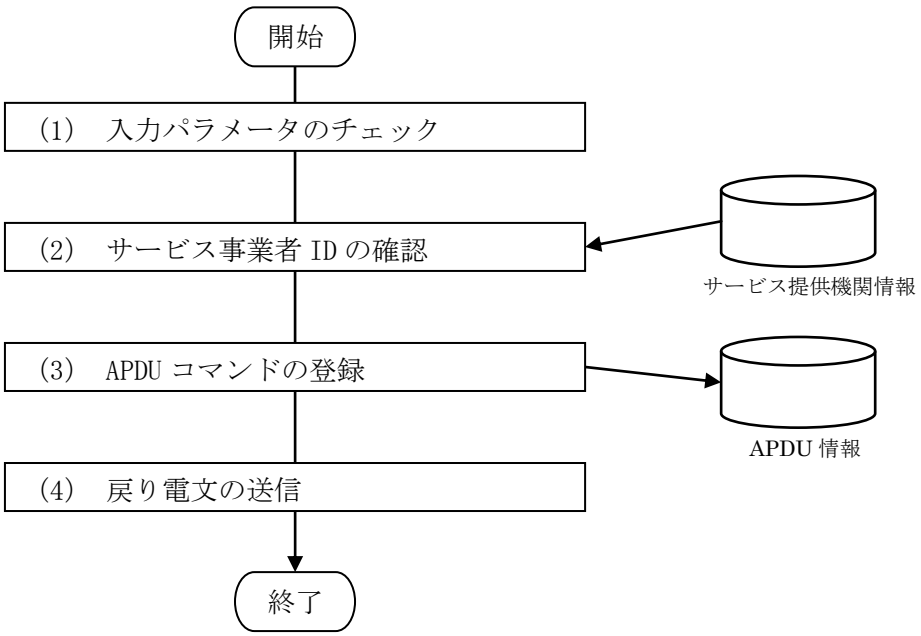


図 2-9 受付処理機能の処理フロー

(1) 入力パラメータのチェック

入力パラメータ（サービス事業者 ID、受付番号、APDU 生成年月日、APDU 実行順序、APDU コマンド）のチェック（文字数などのチェック）を行う。

また、APDU 実行順序と APDU コマンドのペアが 1 つ以上指定されていること、1 番目の APDU コマンドが SELECT であること、APDU 実行順序が 1 からの通番であること等の相関チェックを行う。

入力チェックエラーの場合、処理を中断して（4）の戻り電文の設定処理を実行する。

(2) サービス事業者 ID の確認

受信したサービス提供機関 ID が契約関係にあるサービス提供機関であることを確認する。

(3) APDU コマンドの登録

受信した APDU コマンドを保管する。APDU コマンドが複数ある場合は、その数分登録処理を実行する。

(4) 戻り電文の送信

サービス提供機関に、戻り電文（処理ステータス（00:正常終了、02：アプリエラー)、エラー情報、APDU 受付年月日）を送信する。

2.7.1.2. 共通アプリアクセス機能

共通アプリに対して、処理開始、セキュアセッション確立、APDU コマンド送信、処理終了を送信する。また、共通アプリから実行結果を受信してサービス提供機関に送信する。

共通アプリアクセス機能の処理フローを以下に示す。下図に示すように、共通アプリから受け取った処理 ID を判定して処理を分岐する。

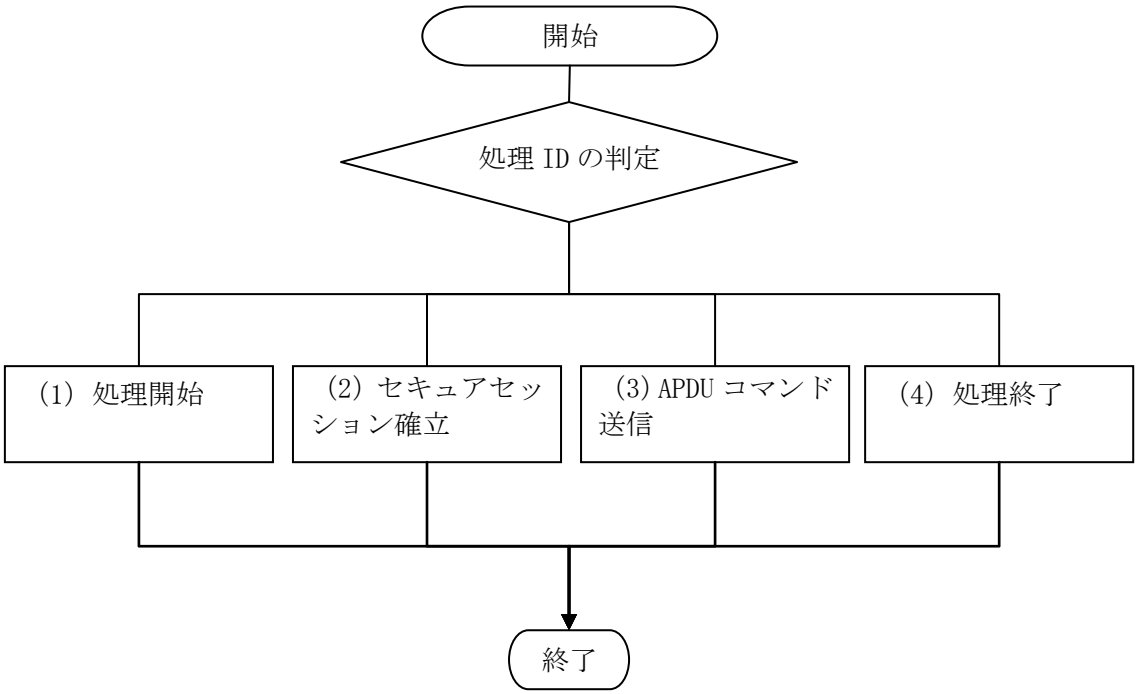


図 2-10 共通アプリアクセス機能の処理フロー

(1) 処理開始

処理 ID が処理開始（001）の場合、初期処理を行い耐タンパデバイスへの接続要求を送信する。処理フロー及び処理詳細を以下に示す。

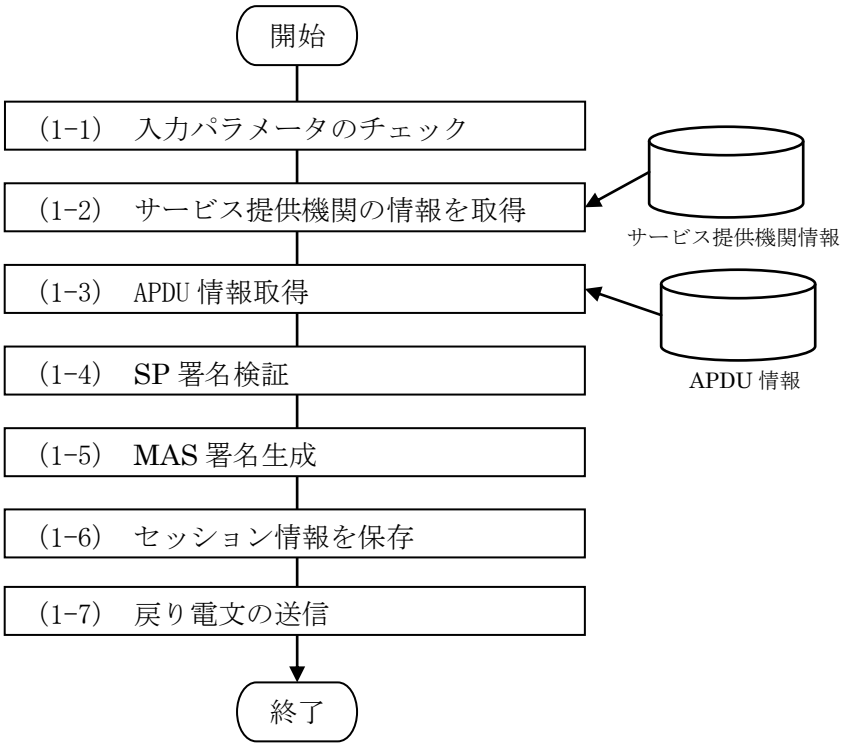


図 2-11 処理開始における処理フロー

(1-1)　入力パラメータのチェック

入力パラメータ（サービス事業者 ID、受付番号、SP 署名）のチェックを行う。

(1-2)　サービス提供機関の情報を取得

サービス事業者 ID から、登録されているサービス提供機関の情報（サービス提供機関のの URI,鍵,鍵のバージョン）を取得する。

(1-3)　APDU 情報取得

サービス事業者 ID と受付番号から APDU 情報（APDU 生成年月日、APDU 受付年月日、処理ステータス）を取得する。

（1-4） SP 署名検証

受信したサービス事業者 ID、受付番号と取得した APDU 生成年月日からハッシュ値を算出する（SHA 方式でハッシュ値を算出する）。

次に、SP 署名の復号を行う。具体的には、受信した SP 署名を秘密鍵で復号する。

最後に、SP 署名の検証を行う。具体的には、算出したハッシュ値と SP 署名を復号した値を比較する。

（1-5） MAS 署名生成

受信したサービス事業者 ID、受付番号と取得した APDU 受付年月日を使用して MAS 署名を生成する（SHA 方式でハッシュ値を取得したものを RSA 方式で暗号化する）。

（1-6） セッション情報を保存

サービス提供機関の情報（サービス提供機関のの URI,鍵,鍵のバージョン）や共通アプリから受け取ったサービス事業者 ID、受付番号と生成した MAS 署名をセッション情報として保存する（これらの情報は以降処理で使用する）。

（1-7） 戻り電文の送信

共通アプリに対して、戻り電文（処理 ID（101：Connect 要求戻り）、104:処理終了（エラー発生時)、MAS 署名（エラー発生時））を送信する。

(2) セキュアセッション確立

処理 ID が Connect 結果（002）の場合、またはレスポンス APDU（003）でかつセキュアセッションの確立前の場合、セキュアセッションの確立処理を行う。また、セッションからセキュアセッション確立状態の情報を取得して処理を分岐する。SELECT コマンド実行後は処理 ID がレスポンス APDU（003）である為、セッションに保持したセキュアセッション確立状態から次に実行する処理を判定する。処理フロー及び処理詳細を以下に示す。

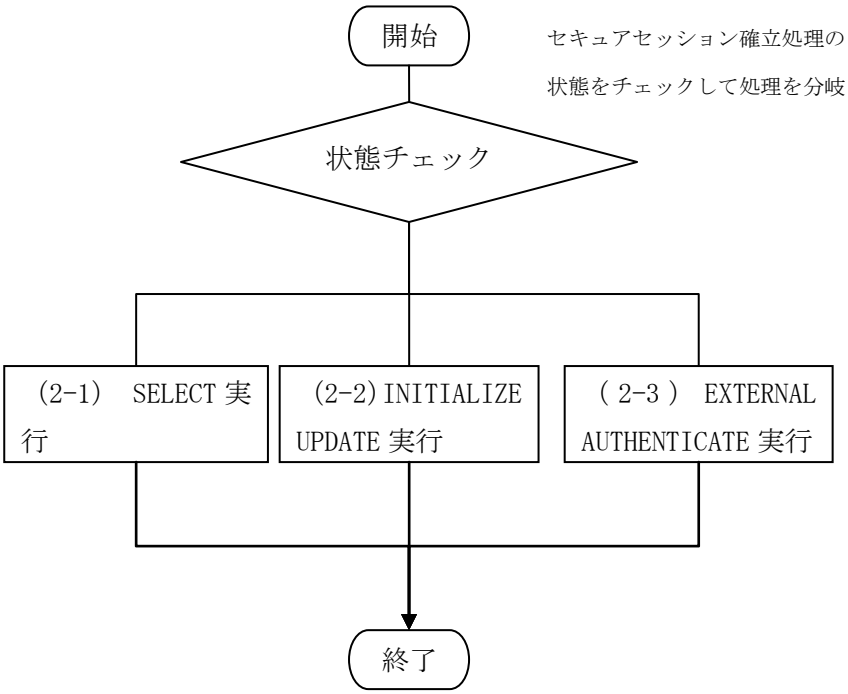


図 2-12 セキュアセッション確立における処理フロー

(2-1) SELECT コマンド処理

セキュアセッションの状態を確認し、セッション確立前であれば、SELECT コマンドを送信する。処理フロー及び処理詳細を以下に示す。

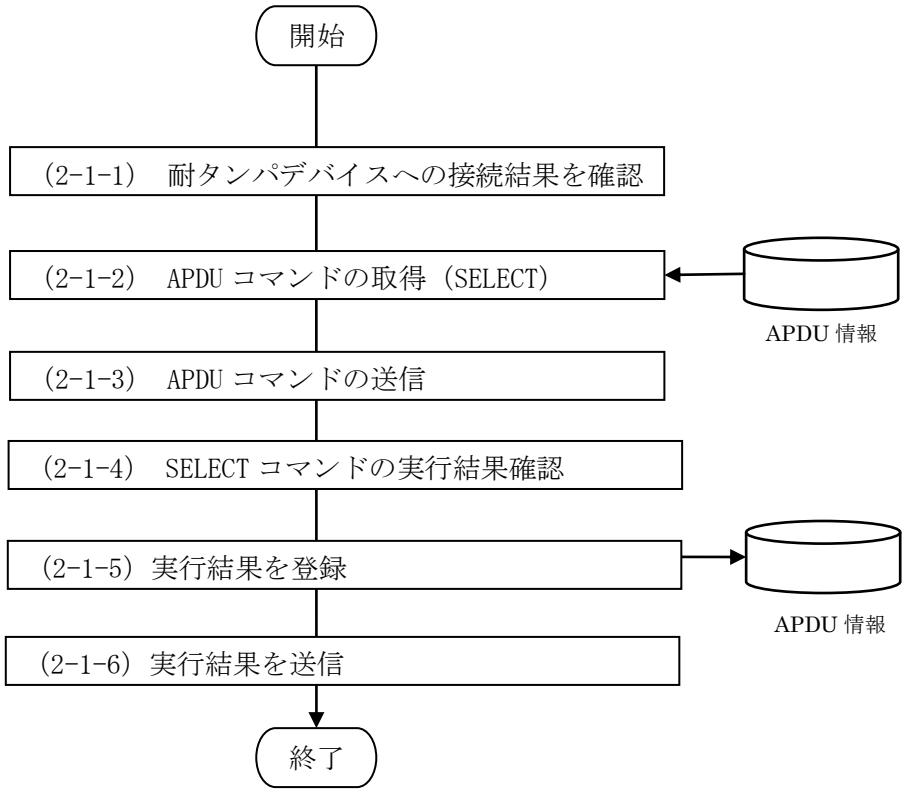


図 2-13 SELECT コマンド処理における処理フロー

(2-1-1) 耐タンパデバイスへの接続結果を確認

耐タンパデバイスへの接続結果が正常であることを確認する。

(2-1-2) APDU コマンドの取得

実行順序が 1 番目の APDU コマンド（SELECT）を取得する。その後、セキュアセッション確立状態を SELECT コマンド実行中に更新する。

(2-1-3) APDU コマンドの送信

耐タンパデバイスに SELECT コマンドを送信する。

(2-1-4) SELECT コマンドの実行結果確認

APDU コマンド実行結果が正常（SW1 が 0x90、SW2 が 0x00）であることを確認する。

(2-1-5) APDU コマンド（SELECT）の実行結果を登録

APDU コマンド(SELECT)の実行結果を保管する。また、現在実行中の APDU コマンド(APDU 実行順）を 1 に設定する。

(2-1-6) APDU コマンド（SELECT）の実行結果を送信

サービス提供機関に APDU コマンドの実行結果（受付番号、APDU 実行順序、APDU レスポンス番号、APDU レスポンス、処理ステータス）を送信する。なお、本ステップで実行結果を送信せず、(4) の終了処理でまとめてサービス提供機関に送信することも可能である。

(2-2) INITIALIZE UPDATE コマンド処理

次に、INITIALIZE UPDATE コマンドを実行する。処理フロー及び処理詳細を以下に示す。

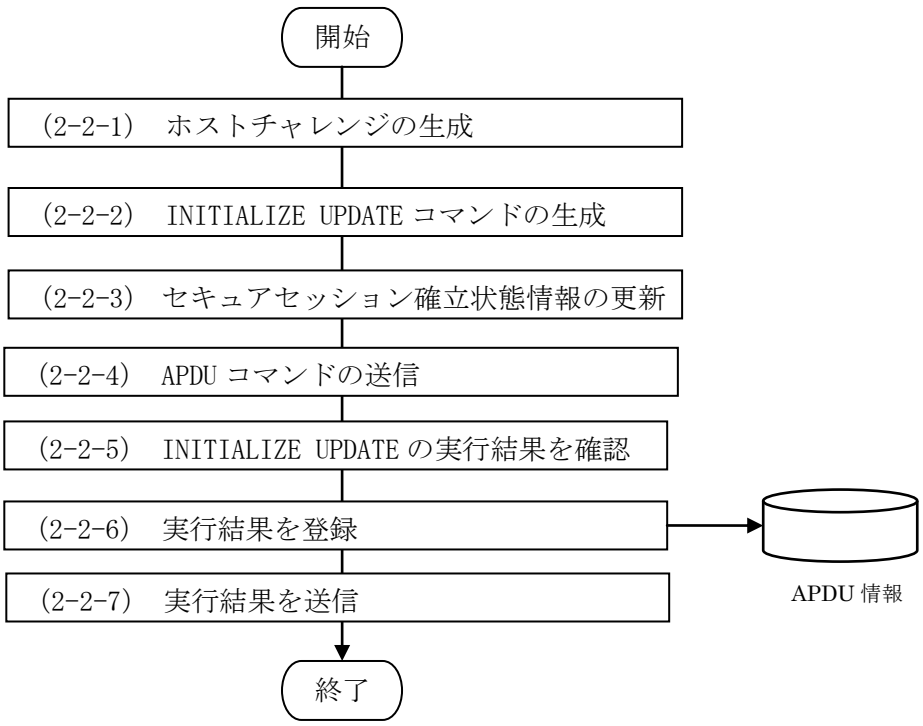


図 2-14 INITIALIZE UPDATE コマンド処理における処理フロー

(2-2-1) ホストチャレンジ（認証乱数）の生成

8バイト長のホストチャレンジを生成する。また、作成したホストチャレンジはセッションに保存する。この値は、カード認証演算（INITIALIZE UPDATE のレスポンス判定）で使用する。

(2-2-2) INITIALIZE UPDATE コマンドの生成

INITIALIZE UPDATE コマンド（GlobalPlatform 仕様に準拠）を生成する。

(2-2-3) セキュアセッション確立状態情報の更新

セッション情報に保持したセキュアセッション確立状態を INITIALIZE UPDATE コマンド実行中に更新する。

(2-2-4) APDU コマンドの送信

耐タンパデバイスに INITIALIZE UPDATE コマンドコマンドを送信する。

(2-2-5) INITIALIZE UPDATE の実行結果を確認

エラー種別が正常（00）、および APDU コマンド実行結果が正常（SW1 が 0x90、SW2 が 0x00）であることを確認する。

SW1 が 0x61 または 0x6C の場合には、レスポンスデータが存在する場合の為、GET RESPONSE コマンドを送信してデータの取得を行う。

(2-2-6) APDU コマンド（INITIALIZE UPDATE）の実行結果を登録

APDU コマンド（INITIALIZE UPDATE）の実行結果を保管する。

(2-2-7) APDU コマンド（INITIALIZE UPDATE）の実行結果を送信

サービス提供機関に APDU コマンドの実行結果（受付番号、APDU 実行順序、APDU レスポンス番号、APDU レスポンス、処理ステータス）を送信する。なお、本ステップで実行結果を送信せず、(4) の終了処理でまとめてサービス提供機関に送信することも可能である。

(2-3) EXTERNAL AUTHENTICATE コマンド処理

INITIALIZE UPDATE コマンドの実行結果を確認する。実行結果が正常の場合、EXTERNAL AUTHENTICATE コマンドを生成する。処理フロー及び処理詳細を以下に示す。

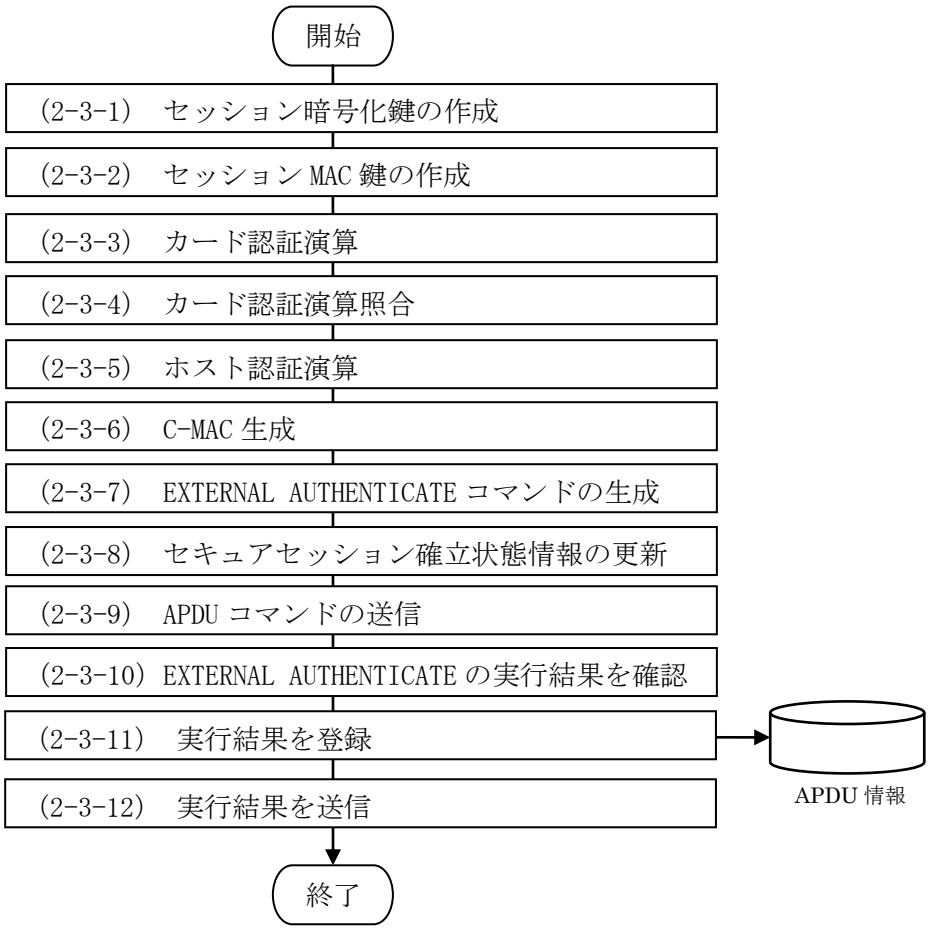


図 2-15 EXTERNAL AUTHENTICATE コマンド処理における処理フロー

(2-3-1) セッション暗号化鍵の作成

セッション情報からベース鍵情報を取得する。ベース鍵からセッション暗号化鍵を作成する。また、作成した鍵はセッション情報に保存する。Data 領域の暗号化と APDU レスポンスの復号化で使用する。

(2-3-2) セッション MAC 鍵の作成

ベース鍵からセッション MAC 鍵を作成する。また、作成した鍵はセッション情報に保存する。C-MAC 作成で使用する。

(2-3-3)　カード認証演算

セッション暗号化鍵、ホストチャレンジ、カードチャレンジの情報からカード認証演算結果を算出する。ホストチャレンジはセッションから取得する。また、カードチャレンジはAPDUレスポンスから取得する。

(2-3-4)　カード認証演算照合

算出したカード認証演算結果と共通アプリから受け取ったカード認証演算結果が正しいことを確認する。

(2-3-5)　ホスト認証演算

セッション暗号化鍵、ホストチャレンジ、カードチャレンジの情報からホスト認証演算結果を算出する。

(2-3-6)　C-MAC生成

セッションMAC鍵とAPDUコマンドからC-MACを生成する。また、作成したC-MACはセッション情報に保存する。次にC-MACを作成する時に使用する。

(2-3-7)　EXTERNAL AUTHENTICATEコマンドの生成

EXTERNAL AUTHENTICATEコマンド（GlobalPlatform仕様に準拠）を生成する。

(2-3-8)　セキュアセッション確立状態情報の更新

セッションに保持したセキュアセッション確立状態を EXTERNAL AUTHENTICATE コマンド実行中に更新する。

(2-3-9)　APDUコマンドの送信

耐タンパデバイスにEXTERNAL AUTHENTICATEコマンド送信する。

(2-3-10)　EXTERNAL AUTHENTICATEコマンドの実行結果を確認

EXTERNAL AUTHENTICATEコマンドの実行結果を確認する。エラー種別が正常（00)、およびAPDUコマンド実行結果が正常（SW1が0x90、SW2が0x00）であることを確認する。

SW1が0x61または0x6Cの場合には、レスポンスデータが存在する場合の為、GET RESPONSEコマンドを送信してデータの取得を行う。

(2-3-11)　APDUコマンド（EXTERNAL AUTHENTICATE）の実行結果を登録

APDUコマンド（EXTERNAL AUTHENTICATE）の実行結果を保管する。

(2-3-12)　APDU コマンド（EXTERNAL AUTHENTICATE）の実行結果を送信

サービス提供機関に APDU コマンドの実行結果（受付番号、APDU 実行順序、APDU レスポンス番号、APDU レスポンス、処理ステータス）を送信する。なお、本ステップで実行結果を送信せず、(4) の終了処理でまとめてサービス提供機関に送信することも可能である。

(3) APDU コマンド送信

処理 ID がレスポンス APDU（003）であり、セキュアセッション確立状態が、EXTERNAL AUTHENTICATE コマンド実行中、またはセキュアセッション確立成功の場合、実行する APDU コマンドを送信する。EXTERNAL AUTHENTICATE コマンド実行中の場合は、その結果を確認する。処理フロー及び処理詳細を以下に示す。

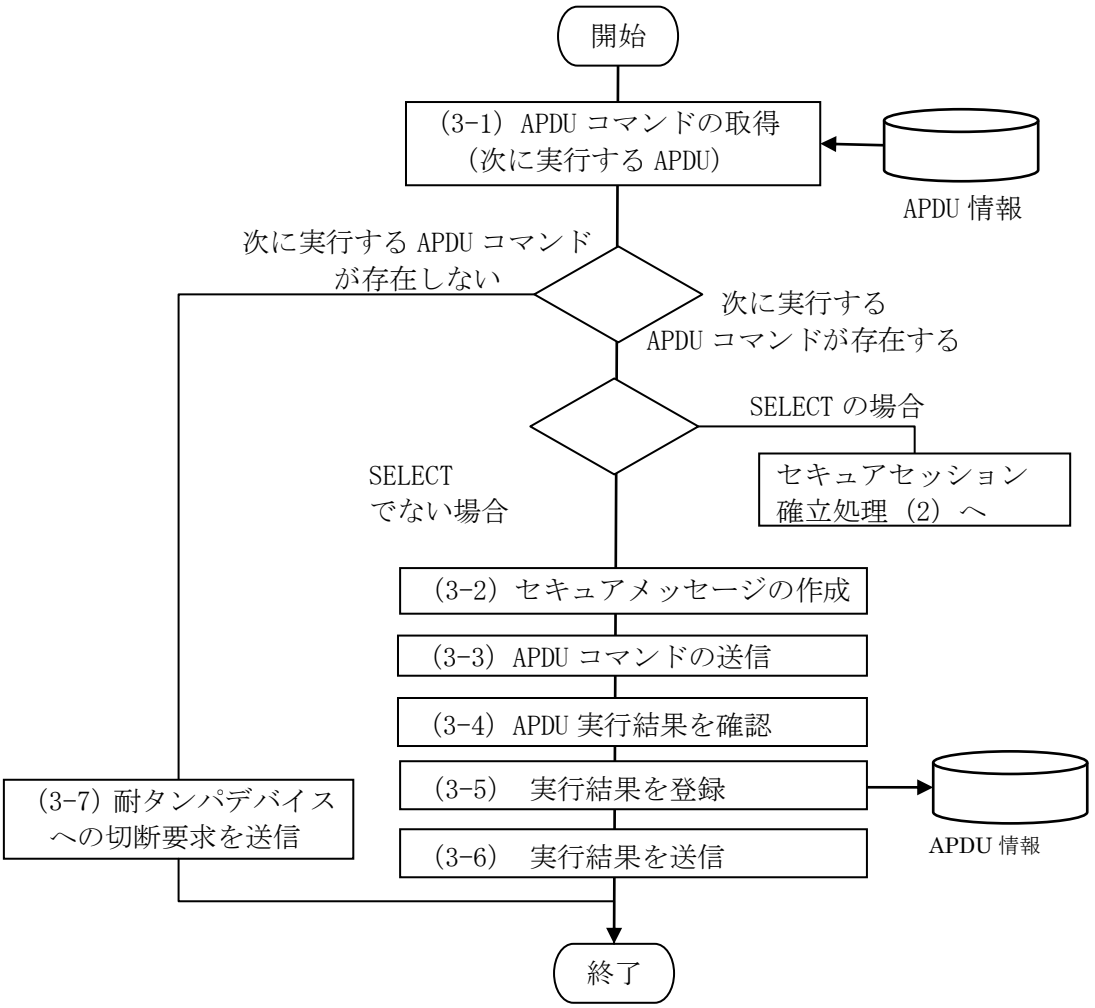


図 2-16 APDU コマンド送信における処理フロー

(3-1) APDU コマンドの取得

次に実行する APDU コマンドを取得する。

(3-2) セキュアメッセージの作成

次に実行する APDU コマンドが存在し、その APDU コマンドが SELECT ではない場合、セキュアメッセージの作成を行う。具体的には、C-MAC の生成と Data 領域の暗号化を行う(SELECT コマンドの場合は、(2) のセキュアセッション確立処理を実行する)。

・C-MAC の作成

セッション MAC 鍵と APDU コマンドから C-MAC を作成する。また、セッションに保持してある C-MAC を作成した C-MAC に更新する。セッション MAC 鍵はセッション情報から取得する。

・Data 領域の暗号化

セッション暗号化鍵で Data 領域を暗号化する。セッション暗号化鍵はセッション情報から取得する。

・セキュアメッセージを作成

セキュアメッセージ（GlobalPlatform 仕様準拠）を作成する。

(3-3) APDU コマンドの送信

耐タンパデバイスに対してセキュアメッセージ化した APDU コマンドを送信する。

(3-4) APDU コマンドの実行結果を確認

APDU コマンドの実行結果を確認する。エラー種別が正常（00)、および APDU コマンド実行結果が正常（SW1 が 0x90、SW2 が 0x00）であることを確認する。

SW1 が 0x61 または 0x6C の場合には、レスポンスデータが存在する場合の為、GET RESPONSE コマンドを送信してデータの取得を行う。

(3-5) APDU コマンドの実行結果を登録

APDU コマンドの実行結果を保管する。

(3-6) APDU コマンドの実行結果を送信

サービス提供機関に APDU コマンドの実行結果（受付番号、APDU 実行順序、APDU レスポンス番号、APDU レスポンス、処理ステータス）を送信する。なお、本ステップで実行結果を送信せず、(4) の終了処理でまとめてサービス提供機関に送信することも可能である。

(3-7) 耐タンパデバイスへの切断要求を送信

ステップ（3-1）で、次に実行する APDU コマンドが存在しない場合（APDU コマンドが全て実行済みの場合)、耐タンパデバイスへ切断の要求を行う。

(4) 処理終了

処理 ID が DisConnect 結果（004）の場合、処理終了のステータスを送信する。処理フロー及び処理詳細を以下に示す。

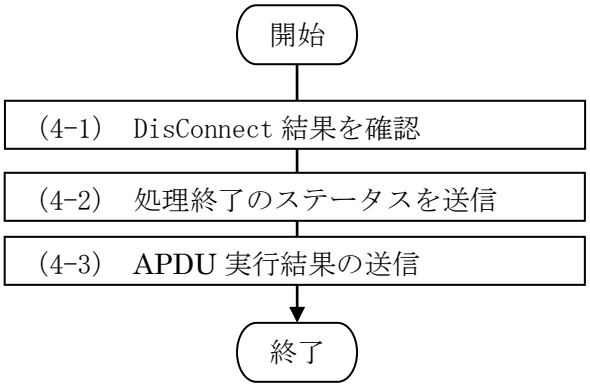


図 2-17 処理終了における処理フロー

(4-1) DisConnect 結果を確認

耐タンパデバイスの切断結果の確認を行う。

(4-2) 処理終了のステータスを送信

共通アプリに対して戻り電文（処理 ID（104：処理終了)、MAS 署名）を送信する。

(4-3) APDU 実行結果の送信

サービス提供機関に対して、APDU 処理の結果（受付番号、APDU 実行順序、APDU レスポンス番号、APDU レスポンス、処理ステータス）を送信する。

2.7.2. 共通アプリの機能

共通アプリは、耐タンパデバイスとの接続、切断を行い、モバイルアクセスサーバから受信したAPDUコマンドを耐タンパデバイスに送信し、また、その結果をモバイルアクセスサーバに送信する機能を有する。

ブラウザから起動され、モバイルアクセスサーバと連動して耐タンパデバイスとの接続、切断を行い、モバイルアクセスサーバから受信したAPDUコマンドを耐タンパデバイスに送信する。モバイルアクセスサーバから処理終了要求を受信すると、ブラウザを立ち上げ処理を終了する。

2.7.2.1.　　APDU 転送機能

共通アプリの APDU 転送機能の処理フローを以下に示す。

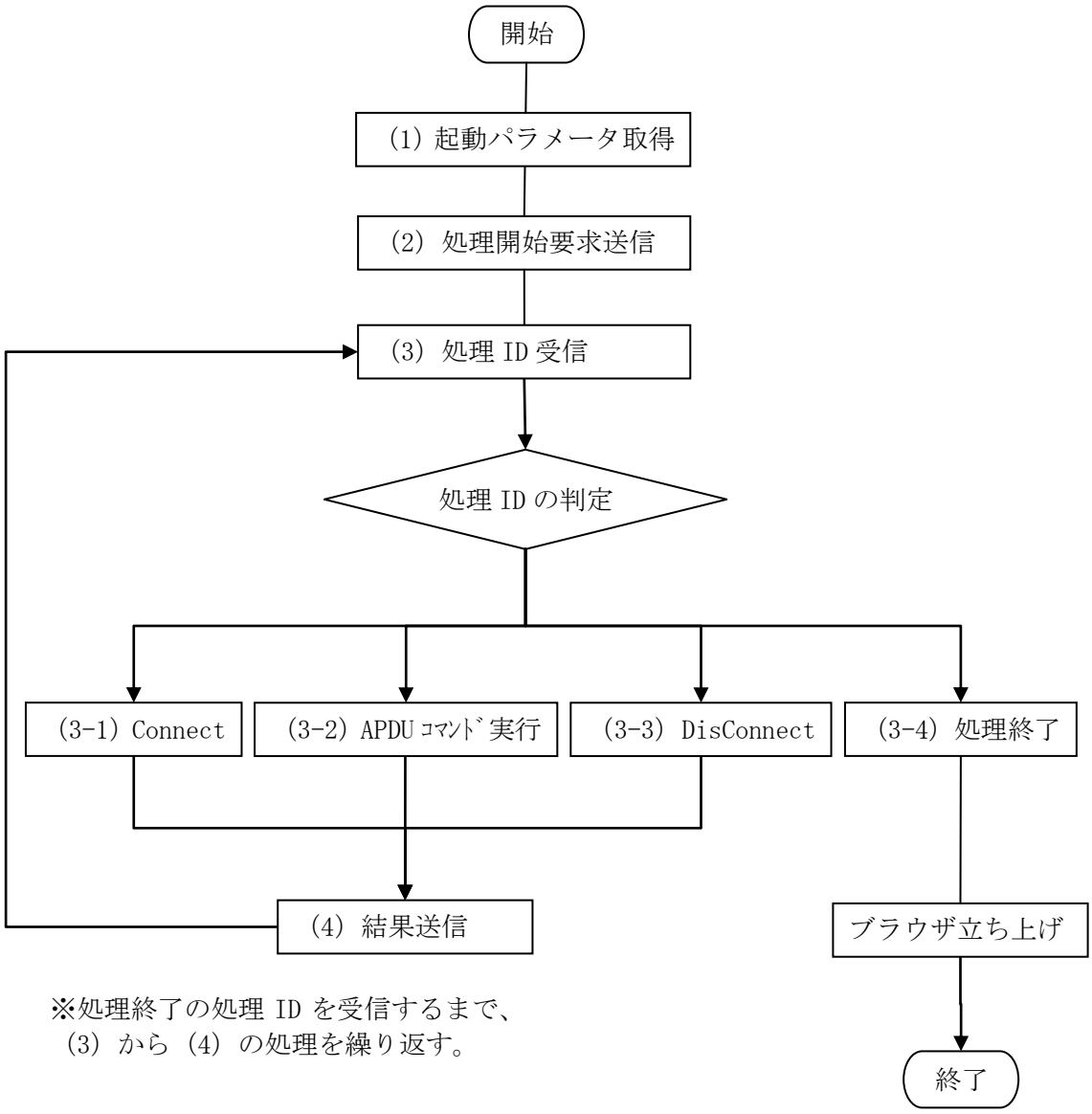


図 2-18 共通アプリの APDU 転送機能の処理フロー

(1) 起動パラメータ取得

共通アプリは、起動パラメータから、サービス事業者 ID、受付番号、戻り URL、モバイルアクセスサーバ URL、SP 署名を取得する。ここで、SP 署名とはサービス提供機関で生成した署名値である。

(2) 処理開始要求送信

モバイルアクセスサーバに、送信電文（処理 ID（001:処理開始)、エラー種別（00:正常)、サービス事業者 ID、受付番号、SP 署名）を送信する。

(3) 処理 ID 受信

モバイルアクセスサーバから処理 ID を受信する。処理 ID の値によって処理を分岐し、処理終了要求を受信するまで処理を繰り返す。

(3-1) Connect（処理 ID：101）の場合

耐タンパデバイスに接続（Connect）する。

モバイルアクセスサーバに Connect 結果（処理 ID（002：Connect 結果)、エラー種別（00：正常)、カード情報（00:SD カード,01:UIM カード,02:非接触 IC カード））を送信する。

(3-2) APDU コマンド実行（処理 ID：102）の場合

APDU が SELECT コマンドの場合には、SELECT 処理を実行し、モバイルアクセスサーバに電文（処理 ID（003：レスポンス APDU)、エラー種別（00：正常)、SW1,SW2（0x9000)、取得したレスポンス APDU）を送信する。

APDU が SELECT コマンド以外の場合には、受信した APDU コマンドをそのまま耐タンパデバイスに送信する。

その後、モバイルアクセスサーバに電文（処理 ID（003：レスポンス APDU)、エラー種別（00：正常)、取得した SW1,SW2、取得したレスポンス APDU）を送信する。

(3-3) DisConnect（処理 ID：103）の場合

耐タンパデバイスとの接続を解除（DisConnect）する。

モバイルアクセスサーバに電文（処理 ID（004：DisConnect 結果)、エラー種別（00：正常））を送信する。

(3-4) 処理終了（処理 ID：104）の場合

「戻り URL + MAS 署名」を指定してブラウザを起動し、処理を終了する。ここで、MAS 署名とはモバイルアクセスサーバで生成した署名値である。

2.7.3. サービス提供機関の機能

サービス提供機関は、耐タンパデバイスに ID 情報を送信する ID 情報発行機能、および、モバイルアクセスサーバから耐タンパデバイスでの処理結果を受信する機能を有する。

なお、前提として、サービス提供機関とモバイルアクセスサーバはセキュアな通信が確立されていることとする。

2.7.3.1. ID 情報発行機能

耐タンパデバイスへ ID 情報を発行する処理フローを以下に示す。ただし「任意」と書かれた処理はサービスに依存する任意の処理である。

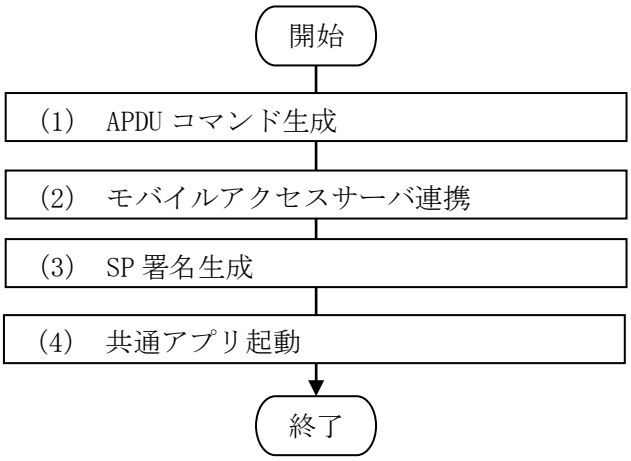


図 2-19 耐タンパデバイスへの ID 情報発行における処理フロー

(1) APDU コマンド生成

任意の APDU コマンドを生成する。

(2) モバイルアクセスサーバ連携

モバイルアクセスサーバに APDU 情報（サービス事業者 ID、受付番号、APDU 生成年月日、APDU 実行順序、APDU コマンド）を送信する。(実行する APDU の数だけ APDU 実行順序と APDU コマンドのペアが存在する)。

(3) SP 署名生成

サービス事業者 ID、受付番号、APDU 生成年月日を使用して SP 署名を生成する。具体的には、SHA 方式でハッシュ値を取得したものを RSA 方式で暗号化する。

(4) 共通アプリ起動

ブラウザに対して共通アプリ起動パラメータ（サービス事業者 ID、受付番号、戻り URL、モバイルアクセスサーバ URL、SP 署名）を送信し、共通アプリを起動する。

2.7.3.2. 処理結果受信機能

耐タンパデバイスから処理結果を受信する処理フローを以下に示す。ただし「任意」と書かれた処理はサービスに依存する任意の処理である。

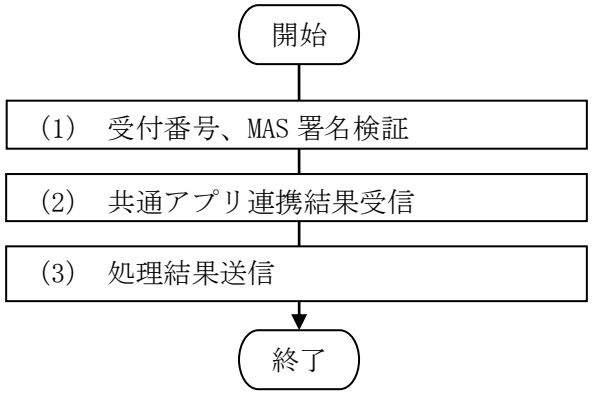


図 2-20 耐タンパデバイスからの処理結果受信における処理フロー

(1) 受付番号、MAS 署名検証

ブラウザから送信された GET パラメータから受付番号、MAS 署名を取得し、検証する。具体的には、まず、サービス事業者 ID、受信した受付番号、APDU 受付年月日からハッシュ値を算出する（SHA 方式でハッシュ値を算出する）。次に、受信した MAS 署名を秘密鍵で復号する。算出したハッシュ値と MAS 署名を復号化した値を比較する。値が異なった場合は、エラー画面を表示する。

(2) 共通アプリ連携結果受信

モバイルアクセスサーバから APDU コマンドの実行結果（受付番号、APDU 実行順序、APDU レスポンス番号、APDU レスポンス、処理ステータス）を受信する。

(3) 処理結果送信

モバイルアクセスサーバに処理結果（成功、失敗）を送信する。

2.8. インタフェースの詳細

本節では、ブラウザ、共通アプリ、耐タンパデバイス、サービス提供機関、モバイルアクセスサーバの各エンティティ間のインタフェースに関して詳細を記述する。なお、図 2-7 に示した全体フローと本節で詳述するインタフェースは下図のような対応関係になっている。

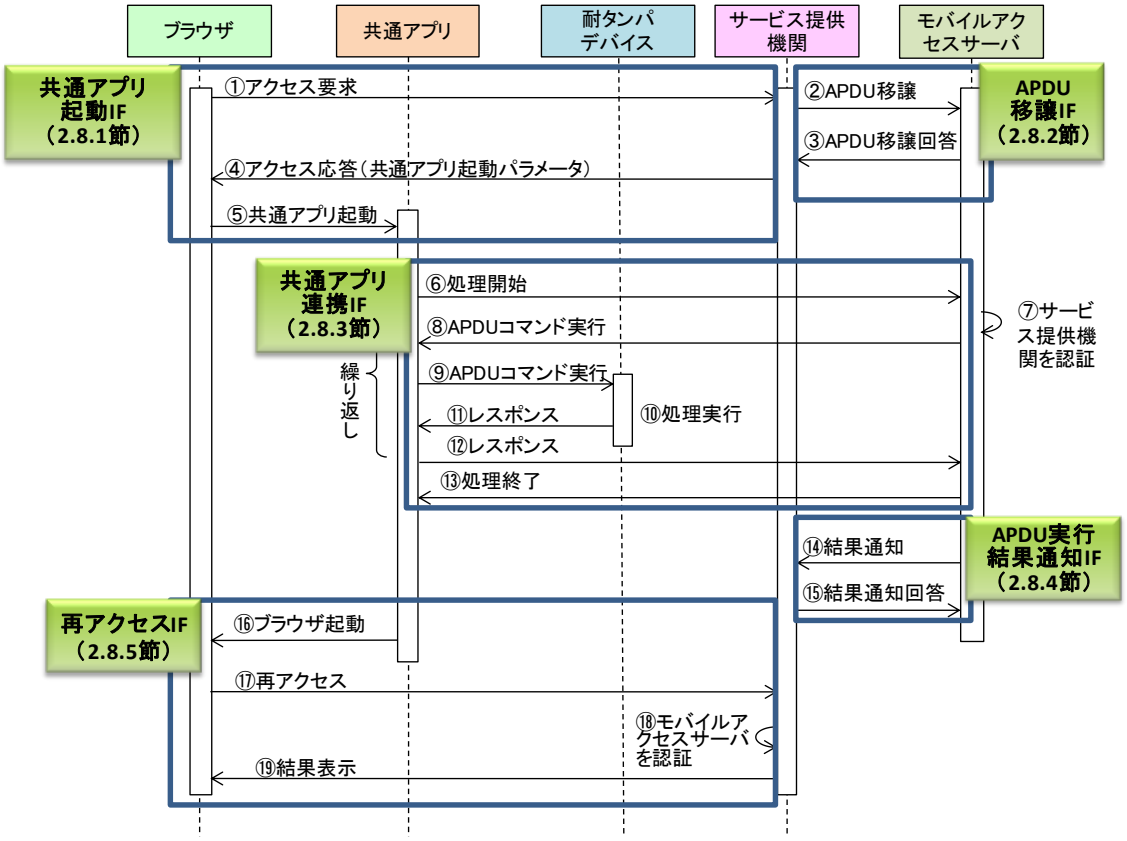


図 2-21 エンティティ間のインタフェース

本システムで使用する通信 IF を下の表に示す。

表 2-1 インタフェース一覧

#	IF 名	概要	要求元	応答先	通信形式
1	共通アプリ起動	JavaScript で共通アプリを起動する。	ブラウザ	共通アプリ	実行時パラメータ
2	APDU 移譲	耐タンパデバイスに対して実行する APDU コマンドをサービス提供機関からモバイルアクセスサーバに移譲する。	サービス提供機関	モバイルアクセスサーバ	HTTPS／※XML
3	共通アプリ連携	耐タンパデバイスに対してセキュアにアクセスするために共通アプリとモバイルアクセスサーバが通信する IF。	共通アプリ	モバイルアクセスサーバ	HTTPS／※XML
4	APDU 実行結果通知	耐タンパデバイスに対して実行した APDU コマンドの結果をモバイルアクセスサーバからサービス提供機関に通知する。	モバイルアクセスサーバ	サービス提供機関	HTTPS／※XML
5	再アクセス	共通アプリからサービス提供機関の処理結果画面へ接続する IF。	共通アプリ	サービス提供機関	HTTPS

2.8.1. 共通アプリ起動インタフェース

共通アプリを起動する際の起動パラメータ（Android OS の場合）を以下に示す。

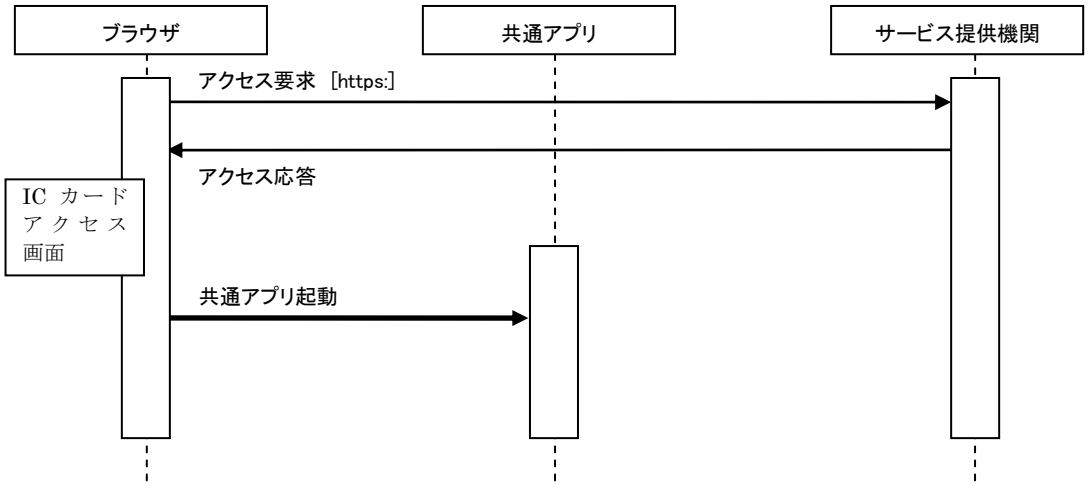


図 2-22 共通アプリ起動シーケンス図

表 2-2 共通アプリ起動時の要求例

```
function startCommonApl(param){
var hrefString="commonApl: " + param;
location.href=hrefString;
}
```

表 2-3 共通アプリ起動時のパラメータ

#	項目名	パラメータ名	属性	桁数	説明
1	起動パラメータ	param	varchar	-	共通アプリの起動パラメータ

表 2-4 起動パラメータの構成

spId=XXXXXXXX&rcptNum=XXXXXXXXXXXXXXXX&rtnUrl=XXXXXXXXXXXXXXX&masUrl=XXX
XXXXXXXXXXXXX&spSign=XXXXXXXXXXXXXXXX

※spId=、&rcptNum=、&rtnUrl=、masUrl、spSign が必ず存在すること。

表 2-5 起動パラメータの構成要素の詳細

#	項目名	パラメータ名	属性	桁数	説明
1	サービス事業者 ID	spId	char	8	サービス事業者 ID
2	受付番号	rcptNum	char	16	サービス提供機関が採番した受付番号（日付+8 桁の番号）
3	戻り URL	rtnUrl	varchar	-	戻り URL
4	モバイルアクセスサーバ URL	masUrl	varchar	-	モバイルアクセスサーバの URL
5	SP 署名	spSign	varchar	256	Base64 エンコードした SP 署名

2.8.2. APDU 移譲インタフェース

耐タンパデバイスに対して実行する APDU コマンドをサービス提供機関からモバイルアクセスサーバに移譲する通信インタフェースを以下に示す。

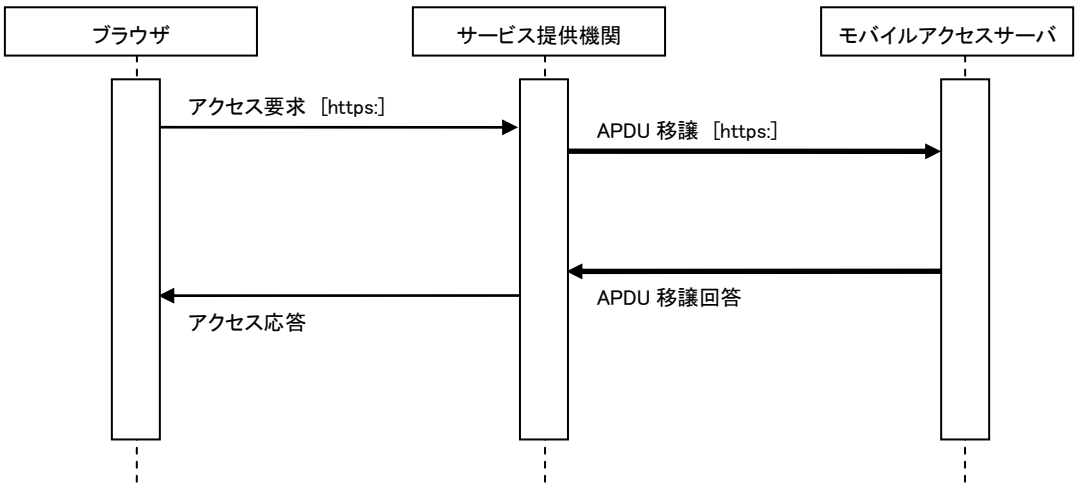


図 2-23 APDU 移譲シーケンス図

表 2-6 APDU 移譲時の要求例

```
POST /xxxxx/xxxx/xxxxx HTTPS/1.1
Host: xxxxx.com
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<request>
  <strSpId>XXXX</strSpId>
  <strRcptNum>XXXX</strRcptNum>
  <strApduGeneDate>XXXX</ strApduGeneDate >
  <apduCmnds>
    <apduCmnd>
      <iApduOrder>XXXX</iApduOrder>
      <byApduCmndAry>XXXX</byApduCmndAry>
    </apduCmnd>
    ・・・<apduCmnd>は実行する APDU の数分定義する
  </apduCmnds>
</request>
```

表 2-7 APDU 移譲時の要求 IF

#	項目名	パラメータ名	属性	桁数	説明
1	サービス事業者 ID	strSpId	char	8	サービス事業者 ID
2	受付番号	strRcptNum	char	16	サービス提供機関が採番した受付番号（日付+8 桁の番号）
3	APDU 生成年月日	strApduGeneDate	char	14	APDU を生成した年月日（YYYYMMDDhhmmss）
4	APDU 実行順序	iApduOrder	varchar	3	APDU コマンドの実行順序
5	APDU コマンド	byApduCmndAry	varchar	※説明参照	Base64 エンコードした APDU コマンド ※桁数は生成した APDU の約 3 分の 4 倍

※実行する APDU の数だけ APDU 実行順序と APDU コマンドのペアが存在する

表 2-8 APDU 移譲時の応答例

```
HTTPS/1.1 200 OK
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<response>
  <strProcStatus>XXXX</strProcStatus>
  <strErrInfo>XXXX</strErrInfo>
  <strApduRcptDate>XXXX</strApduRcptDate>
</response>
```

表 2-9 APDU 移譲時の応答 IF

#	項目名	パラメータ名	属性	桁数	説明
1	処理ステータス	strProcStatus	char	2	処理ステータス
2	エラー情報	strErrInfo	varchar	20	エラー情報
3	APDU 受付年月日	strApduRcptDate	char	14	APDU を受け付けた年月日 (YYYYMMDDhhmmss)

2.8.3. 共通アプリ連携インタフェース

耐タンパデバイスに対してセキュアにアクセスするために共通アプリとモバイルアクセスサーバ間でデータを送受信する通信インタフェースを以下に示す。

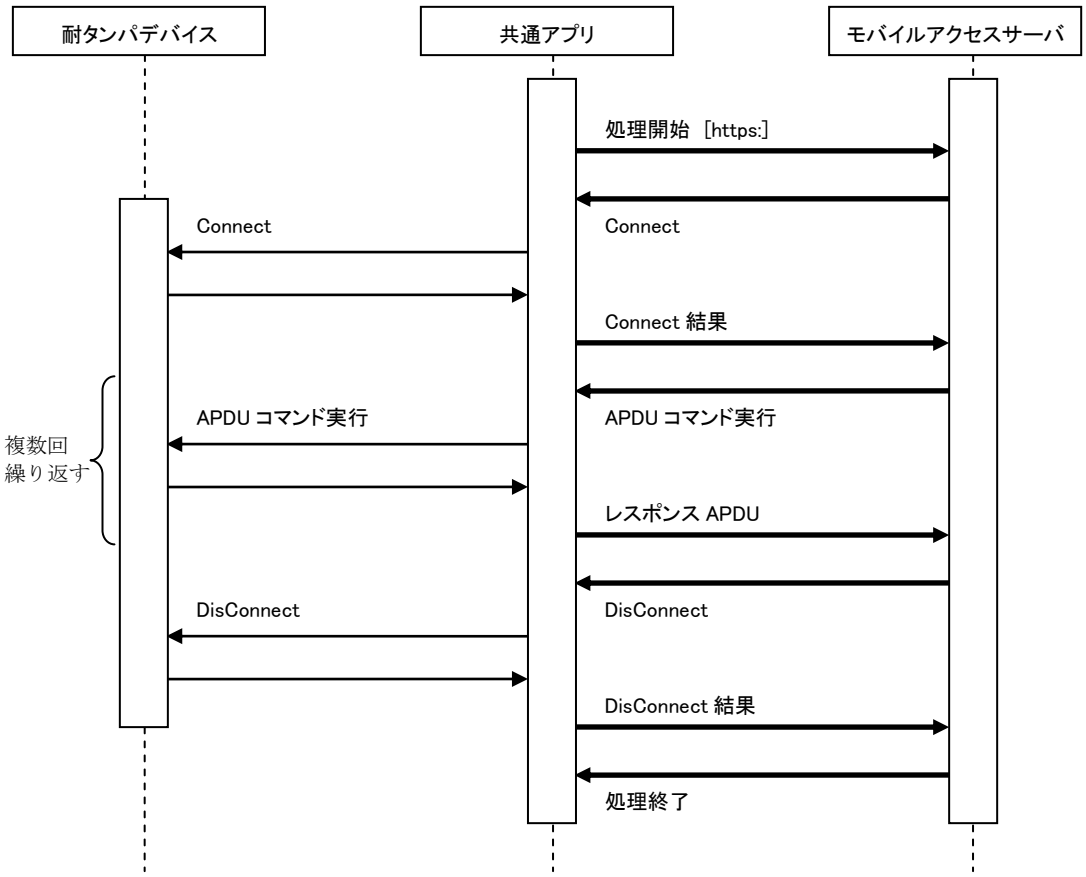


図 2-24 共通アプリ連携シーケンス図

表 2-10 共通アプリ連携時の要求例

```
POST /xxxxx/xxxx/xxxxx HTTPS/1.1
Host: xxxxx.com
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<request>
  <strProcId>XXXX</strProcId>
  <strProcStatus>XXXX</strProcStatus>
  <strSpId>XXXX</strSpId>
  <strRcptNum>XXXX</strRcptNum>
  <byRespSWAry>XXXX</byRespSWAry>
  <byRespApduDataAry>XXXX</byRespApduDataAry>
  <strConnectCard>XXXX</strConnectCard>
  <strErrInfo>XXXX</strErrInfo>
  <strSpSign>XXXX</strSpSign >
</request>
```

表 2-11 共通アプリ連携時の要求 IF

#	項目名	パラメータ名	属性	桁数	説明
1	処理 ID	strProcId	char	3	処理 ID
2	処理ステータス	strProcStatus	char	2	処理ステータス
3	サービス事業者 ID	strSpId	char	8	サービス事業者 ID ※未設定の場合あり
4	受付番号	strRcptNum	char	16	サービス提供機関が採番した受付番号 （日付+8 桁の番号） ※未設定の場合あり
5	SW1,SW2	byRespSWAry	char	3	Base64 エンコードした APDU コマンド実行結果 ※未設定の場合あり
6	レスポンス APDU	byRespApduDataAry	varchar	※説明参照	Base64 エンコードしたレスポンス APDU ※未設定の場合あり ※桁数はレスポンス APDU の約 3 分の 4 倍
7	カード情報	strConnectCard	char	2	Connect したカードの情報 ※未設定の場合あり
8	エラー情報	strErrInfo	varchar	20	エラー情報
9	SP 署名	strSpSign	varchar	256	Base64 エンコードした SP 署名 ※処理 ID：001 の場合のみ設定する

表 2-12 共通アプリ連携時の要求 IF における処理 ID

#	コード	説明
1	001	処理開始
2	002	Connect 結果
3	003	レスポンス APDU
4	004	DisConnect 結果

表 2-13 共通アプリ連携時の要求 IF におけるカード情報

#	コード	説明
1	00	SD カード
2	01	SIM カード

表 2-14 共通アプリ連携時の応答例

```
HTTPS/1.1 200 OK
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<response>
  <strProcIdRtn>XXXX</strProcIdRtn>
  <byApduAry>XXXX</byApduAry>
  <byApduAry>XXXX</byApduAry>
</response>
```

表 2-15 共通アプリ連携時の応答 IF

#	項目名	パラメータ名	属性	桁数	説明
1	処理 ID（戻り）	strProcIdRtn	varchar	3	処理 ID（戻り）
2	APDU コマンド	byApduAry	varchar	※説明参照	Base64 エンコードした APDU コマンド ※桁数は APDU コマンドの 3 分の 4 倍 ※未設定の場合あり
3	MAS 署名	strMasSign	varchar	256	Base64 エンコードした MAS 署名 ※処理 ID（戻り）：104 の場合のみ設定する

表 2-16 共通アプリ連携時の応答 IF における処理 ID（戻り）

#	コード	説明
1	101	Connect
2	102	APDU コマンド実行
3	103	DisConnect
4	104	処理終了

2.8.4. APDU 実行結果通知インタフェース

耐タンパデバイスに対して実行した APDU コマンドの結果をモバイルアクセスサーバからサービス提供機関に通知する通信印インタフェースを以下に示す。

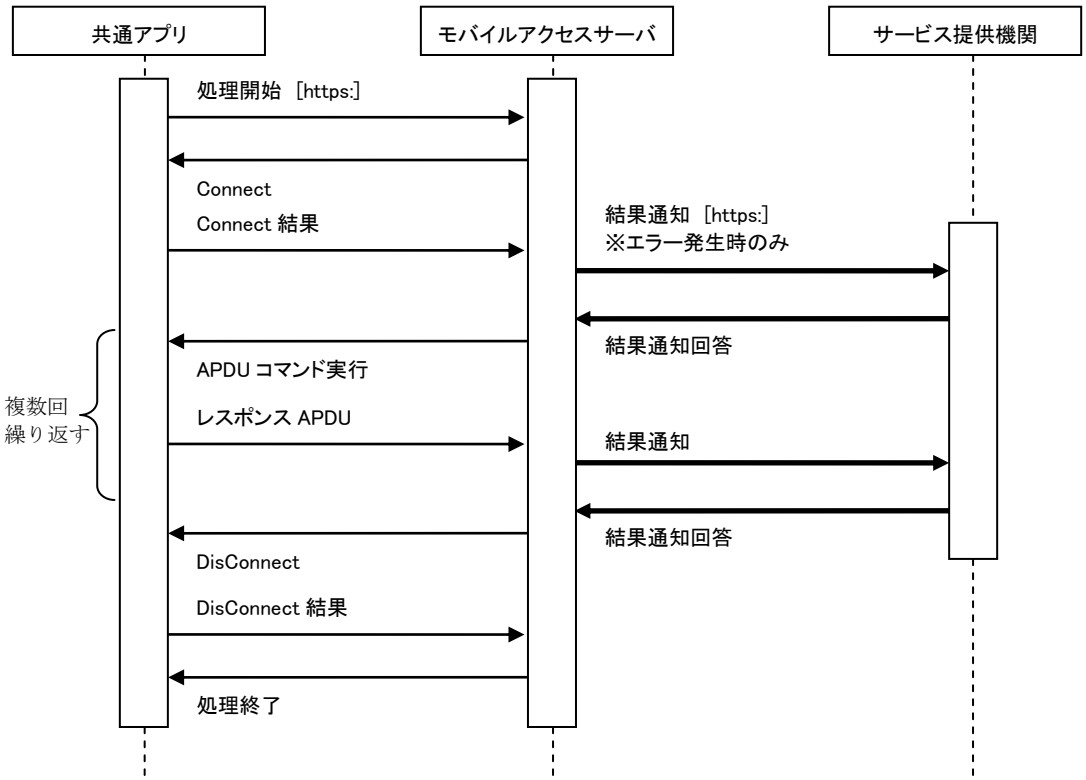


図 2-25 APDU 実行結果通知シーケンス図

表 2-17 APDU 実行結果通知時の要求例

```
POST /xxxxx/xxxx/xxxxx HTTPS/1.1
Host: xxxxx.com
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<request>
   <strRcptNum>XXXX</strRcptNum>
   <iApduOrder>XXXX</iApduOrder>
   <iRespApduNum>XXXX</iRespApduNum>
   <byRespSWAry>XXXX</byRespSWAry>
   <byRespApduDataAry>XXXX</byRespApduDataAry>
   <strProcStatus>XXXX</strProcStatus>
   <strErrInfo>XXXX</strErrInfo>
</request>
```

表 2-18 APDU 実行結果通知時の要求 IF

#	項目名	パラメータ名	属性	桁数	説明
1	受付番号	strRcptNum	char	16	サービス提供機関が採番した受付番号（日付+8 桁の番号）
2	APDU 実行順序	iApduOrder	varchar	3	APDU コマンドの実行順序
3	APDU レスポンス番号	iRespApduNum	varchar	3	APDU レスポンス番号
4	SW1,SW2	byRespSWAry	char	3	Base64 エンコードした APDU コマンド実行結果 ※未設定の場合あり
5	レスポンス APDU	byRespApduDataAry	varchar	※説明参照	Base64 エンコードしたレスポンス APDU ※未設定の場合あり ※桁数はレスポンス APDU の約 3 分の 4 倍
6	処理ステータス	strProcStatus	char	2	処理ステータス
7	エラー情報	strErrInfo	varchar	20	エラー情報 ※未設定の場合あり

表 2-19 APDU 実行結果通知時の応答例

```
HTTPS/1.1 200 OK
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<response>
  <strResult>XXXX</strResult>
</response>
```

表 2-20 APDU 実行結果通知時の応答 IF

#	項目名	パラメータ名	属性	桁数	説明
1	処理結果	strResult	varchar	5	処理結果 true：正常、false：異常

2.8.5. 再アクセスインタフェース

共通アプリからサービス提供機関の処理結果画面へ接続するインタフェースを以下に示す。

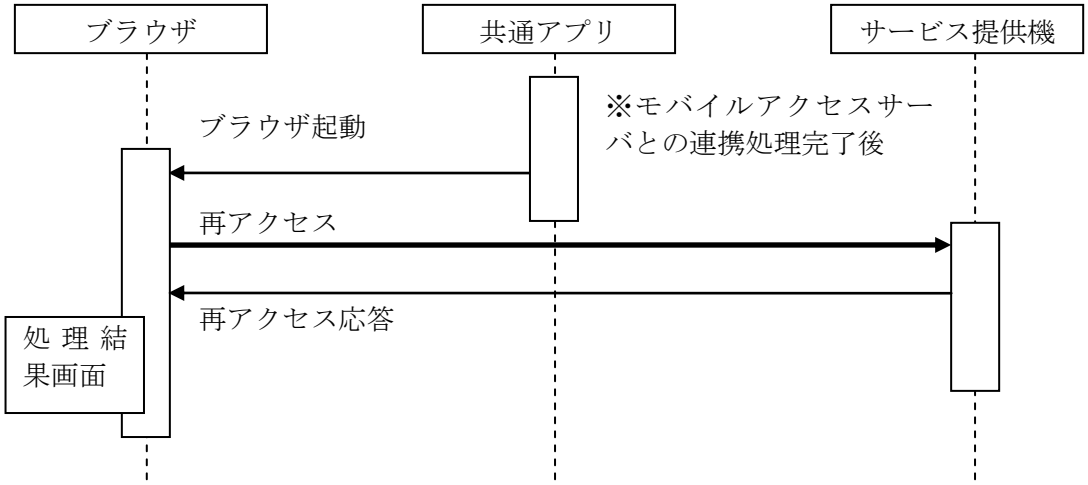


図 2-26 再アクセスシーケンス図

表 2-21 再アクセス時の要求例

https://(戻りURL)?rcptNum=XXXXXXXXXXXXXXX&masSign=XXXXXXXXXXXXXXX

※rcptNum=、masSign=が必ず存在すること。

表 2-22 再アクセス時における要求の構成要素

#	項目名	パラメータ名	属性	桁数	説明
1	戻り URL	-	varchar	-	サービス提供機関の処理結果画面の URL
2	受付番号	rcptNum	char	16	サービス提供機関が採番した受付番号 （日付+8 桁の番号）
3	MAS 署名	masSign	varchar	256	Base64 エンコードした MAS 署名

2.9. まとめ

課題アでは、サービス提供機関が携帯電話端末利用者の耐タンパデバイスへ ID 情報の書き込みと読み込みを安全かつ容易に行うことを対象範囲とした検討を行った。

上記対象範囲に関する現状の課題として、複数のサービス提供機関が、携帯電話端末利用者の耐タンパデバイスへの ID 情報の書き込みや読み込みを行おうとする場合、今まではサービス提供機関ごとに携帯アプリを開発・運用する必要があった。また、利用者は各サービス提供機関が提供する携帯アプリを個別にダウンロード・インストールする必要があった。さらに今後は携帯電話端末の OS のオープン化が進むことが想定されるため、携帯アプリのセキュリティを確保する仕組みも必要となっていた。

このような課題を解決するために、モバイルアクセスシステムを提案した。具体的には、サービス提供機関が耐タンパデバイスにアクセスする際に共通的に利用できるモバイルアクセスサーバおよび携帯電話端末上の共通アプリからなるモバイルアクセスシステムの提案を行った。

課題アで提案したモバイルアクセスシステムを導入することにより、耐タンパデバイスの ID 情報を格納・参照するための複数サービス提供機関が共通的に利用できる仕組みをシステムとして利用することで、サービス提供機関が個別に携帯アプリを開発しなければならないという負担を減らすことが期待できる。また、サービス提供機関ごとに個別の携帯アプリを開発する方式では、サービスごとに利用者は携帯アプリをダウンロードする必要があるが、共通アプリであればダウンロードの手間を省ける。さらに、共通アプリを用いることによってユーザインタフェースなどが統一化され、利用者の操作性を向上させることが期待できる。

表 2-23 応募資格に対する本成果報告書の対応個所

	実施要領に記載される要件	参照先	対応内容
課題ア	NFC 機能を実装したスマートフォンを想定	2.2	2.2 節に示した前提条件において、端末に関する前提条件として、耐タンパデバイスにアクセスできる機能を有する端末としている。さらに、耐タンパデバイスに関する前提条件として公的 IC カード方式におけるフルサイズの IC カードを前提条件としている。このように課題ア全体として NFC 機能を実装したスマートフォンを想定した検討を行った。

		2.2 2.3 2.6	2.2節に示した前提条件において、端末に関する前提条件として、オープンなOSを搭載した携帯電話端末を前提とした。また、耐タンパデバイスにアクセスできる機能を有する端末としている。また、2.3節に、不正な携帯電話端末アプリケーションへの対応をセキュリティ要件として挙げ、2.6節で、その対策について述べている。
課題ア	サービス提供機関ごとに携帯電話端末向けアプリケーションを開発することなく、オンライン上で安全に耐タンパデバイスへのID情報の格納と、格納したID情報を利用するためのモバイルアクセスシステムの技術仕様の検討を行う。	2.4 2.6	2.4節の全体システム構成で示したように、個別の携帯アプリの開発を不要とするため、耐タンパデバイスへアクセスする携帯アプリは、共通アプリとして、様々なサービス提供機関から利用可能な設計とした。また、2.6節のセキュリティ対策で示したように、耐タンパデバイスとモバイルアクセスサーバとの間では、GlobalPlatform仕様に基づくセキュアな通信環境を確立した上で、データのやり取りを行うこととした。
		2.8	2.8節のインタフェースの詳細で示したように、ID情報格納・利用時のサービス提供機関とのインタフェースとしてWebアクセスインタフェース（HTTPS）での利用を可能とした。これにより、サービス展開時の展開コスト、運用コストが低減可能となる。
課題ア	モバイルアクセスシステムは、サービス提供機関に応じて様々なアクセス方式に対応させるため、「公的ICカード方式」「携帯電話向け公的カード方式」「公的認証情報方式」のどの方式にも適用できる共通の方式（共通プロトコル/API で実現可能なもの）を検討する。	2.2 2.7.2	2.2節に耐タンパデバイスに関する前提条件として、「公的ICカード方式」におけるフルサイズICカード、「携帯電話向け公的カード方式」におけるICチップを搭載したフラッシュメモリ型デバイス、「公的認証情報方式」におけるUICCを挙げた。各方式によって、携帯電話端末内のドライバが異なるため、それより上位のプロトコルで、「公的ICカード方式」「携帯電話向け公的カード方式」「公的認証情報方式」のどの方式にも適用できる方式として定義した。また、2.7.2節に共通アプリの機能としてConnect処理の機能を3方式のカードに対応するような仕様にした。
		2.7.1	2.7.1節にモバイルアクセスサーバの機能として、下位のプロトコルに関してもICカードの世界標準であるGlobalPlatform仕様に準拠し、「公的ICカード方式」「携帯電話向け公的カード方式」「公的認証情報方式」のどの方式にも適用できる方式として定義した。GlobalPlatform仕様を使うことで、エンド

			ツーエンドのセキュア通信路の生成、ＩＤ情報の安全な書込、読込を可能とした。
課題ア	ID 情報の提供主体としては、複数のサービス提供機関を想定する。	2.7.3	2.7.3 節に示したように、サービス提供機関は、モバイルアクセスサーバに対して、サービス事業者 ID を通知することで、複数のサービス提供機関がモバイルアクセスサーバと情報の送受信を行えるプロトコルとして設計を行った。
		2.7.1	2.7.1 節に示したように、モバイルアクセスサーバの機能として共通アプリを経由してデータを送信してきたサービス提供機関が、正しいサービス提供機関であることを、認証する SP 認証機能を定義した。
課題ア	検討にあたっては、複数の移動体通信事業者等へのヒアリングを通じて、今後の想定される技術動向等を十分に考慮する。	課題エ	課題エの報告で示すように、複数の移動体通信事業者等へのヒアリングを行い、議論を行いながら、仕様の検討を行った。移動体通信事業者、有識者等から構成する委員会を立ち上げ、委員会において議論を行いながら、仕様の検討を行った。
		課題エ	NTT ドコモ、KDDI、ソフトバンクモバイル、イー・アクセスの４移動体通信事業者のモバイルセキュリティに強い有識者と、東京工科大学の手塚教授等から構成する委員会を立ち上げ、委員会において議論を行いながら、仕様の検討を行った。
課題ア	サービス提供機関、携帯電話端末、耐タンパデバイス間で想定される連携インタフェース仕様の検討・策定を行う。	2.8	2.8 に示したように、サービス提供機関のモバイルサイトとブラウザ間、モバイルアクセスサーバと共通アプリ及び耐タンパデバイス間、モバイルアクセスサーバとサービス提供機関間とのインタフェース仕様の検討・策定を行った。
		課題エ	課題エの報告で示すように、移動体通信事業者、有識者等から構成する委員会を立ち上げ、委員会において議論を行いながら、仕様の検討を行った。 また、社団法人電波産業会　高度無線通信研究委員会　モバイルコマース部会（ARIB　MC 部会）にて連携インタフェース仕様のガイドライン化を推進する。

3. 課題イ　実験環境による検証

3.1. 概要

本章では、課題アの技術仕様の検討に基づいて実施した実証実験による検証結果を示す。

3.1.1. 目的

課題アの仕様検討結果に基づき、実験環境を構築し、技術仕様の検証と、サービス提供機関・利用者双方の観点での有効性を検証することを目的とする。

3.1.2. 検証内容

具体的な検証内容を以下に示す。

(1) 課題アのモバイルアクセスシステムの技術仕様に基づき、実験環境を構築し、機能、インタフェースなどの技術仕様を検証する。
(2) 利用者参加型の実証実験を行うことで、ユーザ意見を収集し、モバイルアクセスシステムの運用性、利便性を検証する。 具体的には、以下の 2 つの観点で運用性、利便性を検証する。
　(2-1)　モバイルアクセスシステムを活用することによる運用性、利便性の検証
　(2-2)　応答速度や動作間隔などの受容性の検証

3.1.3. 実験内容

利用者にモバイルアクセスシステムの実験環境を利用頂き、ヒアリングを実施し、技術検証に加え、有効性を検証する。

3.1.4. 実証実験シナリオ

沖縄県浦添市と連携し、健康増進を目的とした健康診断受診や健康イベントへの参加に応じたポイント付与、そのポイントを利用した地域活性化を実現するシナリオで実証実験を実施した。

3.1.5. 実証実験 1

(1) 日時

2012 年 2 月 15 日（水）14:00－15:00

(2) 場所

沖縄県浦添市役所

(3) ヒアリング対象者

- 65 歳以上の浦添市民　4 名
- 介護に携わっている保護士 3 名及び自治体職員 1 名

3.1.6. 実証実験 2

(1) 日時

2012 年 3 月 9 日（金）15:00－16:00

(2) 場所

台東区　浅草

(3) ヒアリング対象者

- 60 歳以上の台東区民　7 名

3.2. 前提条件

(1) 端末に関する前提条件

- Android2.3 端末（機種名：ｘｘｘｘｘ）を前提とする。

(2) 耐タンパデバイスに関する前提条件

- microSD 型耐タンパデバイス、および UICC を前提とする。

(3) ネットワークに関する前提条件

- 携帯電話端末とサービス提供機関間、携帯電話端末とモバイルアクセスサーバ間は、インターネットを用いるものとする。
- サービス提供機関とモバイルアクセスサーバ間の通信は、同一サーバ内に実装する。

(4) サーバに関する前提条件

- サービス提供機関とモバイルアクセスサーバは、正しく安全に動作するものとする。

3.3. 実証実験システムの概要

3.3.1. 全体システム構成図

図 3-1 に実証実験システムの全体システム構成図を示す。

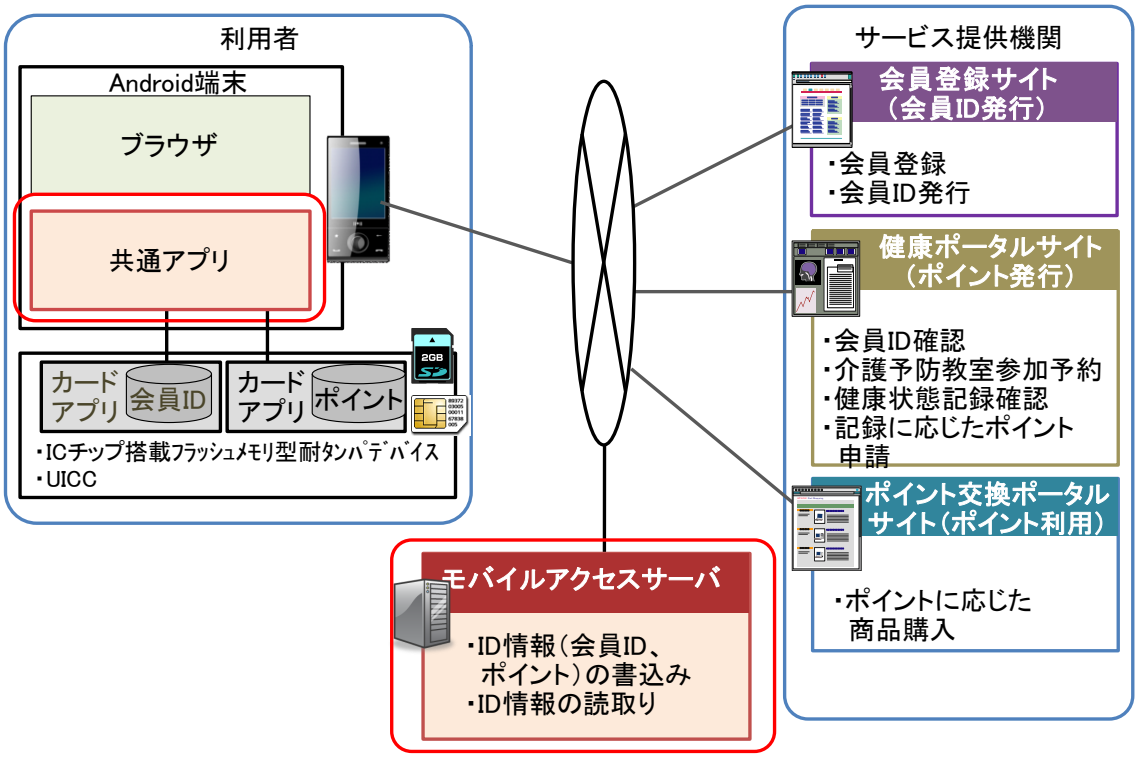


図 3-1 実験システム全体構成

図 3-1 に示すように、モバイルアクセスサーバおよび携帯電話端末内の共通アプリは、課題アでの検討結果に基づき実証システムを構築した。また、仮想的なサービス提供機関として、名前や住所などのユーザ情報を登録して会員 ID を発行する会員登録サイト、会員 ID を確認し、健診の予約などのサービスを行い、サービス実績に応じたポイントを付与する健康ポータルサイト、ポイントを読み込みポイントに応じた商品を購入するポイント交換ポータルサイトの 3 つのサイトを構築した。

また、会員 ID やポイントといった ID 情報を格納する耐タンパデバイスとしては、IC チップを搭載したフラッシュメモリ型のデバイスを用いて、IC チップ内には、会員 ID を格納するカードアプリと、ポイントを格納するカードアプリを構築した。

3.3.2. 実証実験システムの機器構成

3.3.2.1. 全体機器構成

図 3-2 に実証実験環境の全体構成を示す。図 3-2 に示すように、同一サーバ内に、モバイルアクセスサーバ、会員登録サイト、健康ポータルサイト、ポイント交換ポータルサイトを構築した。実証実験では、Android 端末からインターネットを経由して、HTTPS 通信で前記サーバ及び各種サイトにアクセスする。

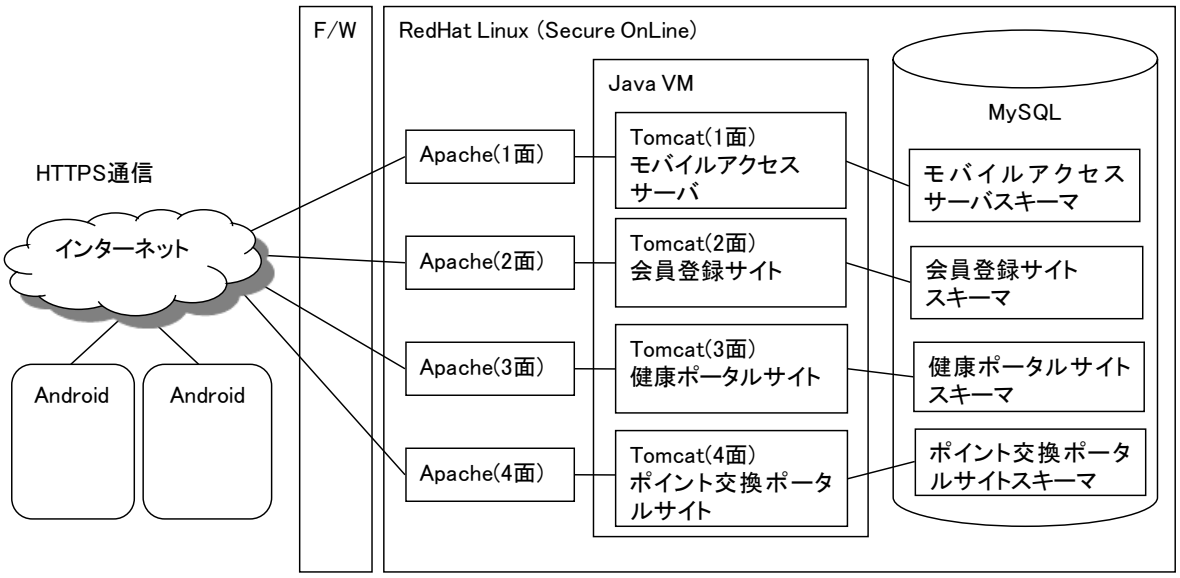


図 3-2 実証実験環境

3.3.3. ハードウェア一覧

表 3-1 に実証実験で用いるハードウェア一覧を示す。

表 3-1 実証実験で用いるハードウェア一覧

#	機器名	HOST 名（ホスト OS）	HW 構成（概要）
1	アクセス多様化サーバ	acsweb001	プロセッサ数 2 コア、メモリ 6GB、ディスク 30GB

3.3.3.1. ソフトウェア一覧

表 3-2 に実証実験で用いるソフトウェア一覧を示す。

表 3-2 実証実験で用いるソフトウェア一覧

#	製品名	数量	インストールホスト名	備考
1	Red Hat Enterprise Linux 5.4	1	acsweb001	前提
2	Apache 2.2.16	3	acsweb001	モバイルアクセスサーバ、会員登録サイト、健康ポータルサイト、ポイント交換ポータルサイトの 4 環境を構築する
3	mod_jk 1.2.30	3	acsweb001	同上
4	Tomcat 6.0.29	3	acsweb001	同上
5	MySQL 5.5.16-1	1	acsweb001	
6	JDK 6.0 Update 27	1	acsweb001	

3.3.4. 実証実験システムの全体サービスフロー

図 3-3 に実証実験システムのおける仮想サービスのフローの概要を示す。

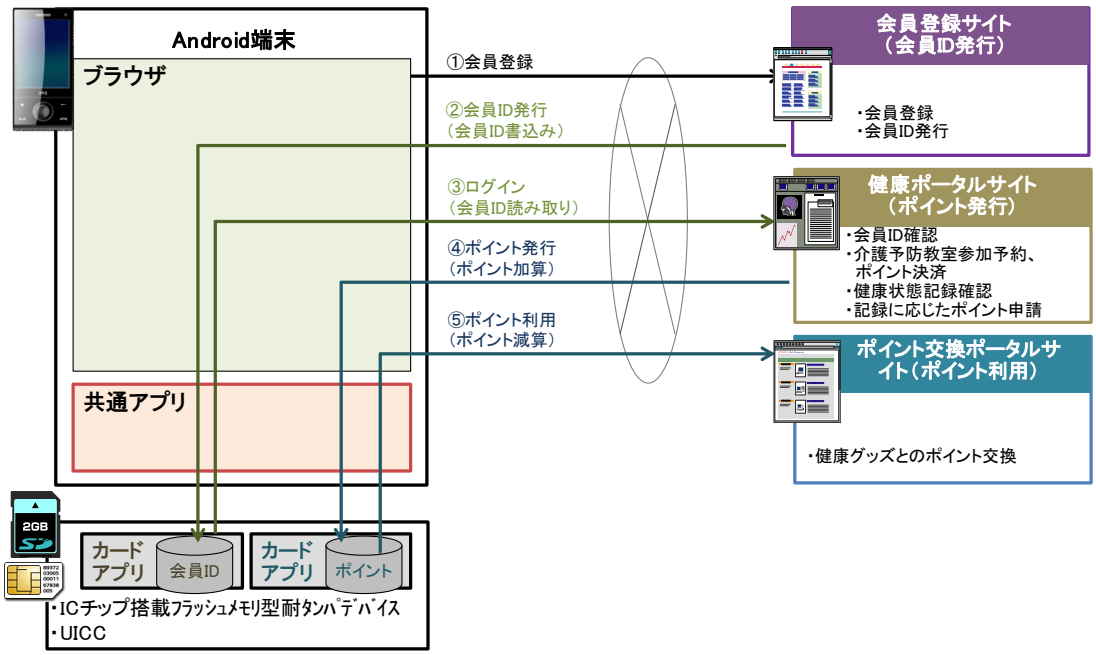


図 3-3 実験システムの仮想サービスフロー

まず実証実験参加者は、Android 端末を用いて会員登録サイトにアクセスする①。ユーザ情報を入力した後、会員登録サイトから、共通アプリを起動し、モバイルアクセスサーバを経由して会員 ID が、会員 ID 管理カードアプリに書き込まれる②。

次に、実証実験参加者は、健康ポータルサイトにアクセスする。その際に、健康ポータルサイトは共通アプリを起動し､前述の会員 ID 管理カードアプリから会員 ID を読み出し、会員 ID を確認することでログイン処理を行う③。健康ポータルサイト内で各種サービスを受け、実績に応じたポイントの発行を受ける。このとき健康ポータルサイトは、共通アプリを起動し、モバイルアクセスサーバ経由で、耐タンパデバイスのポイント管理カードアプリに対してポイントを発行する④。

最後に、実証実験参加者は、ポイント交換ポータルサイトにアクセスし、ポイントの残高を確認する。ポイントに応じた商品を購入する。このときにポイント交換ポータルサイトは、共通アプリを起動し、モバイルアクセスサーバ経由で、耐タンパデバイス内のポイント管理カードアプリが管理しているポイントを減算する⑤。

なお、モバイルアアクセスサーバおよび共通アプリに関しては、課題アで示した機能をそのまま実装したシステムを用いて実証実験を行った。

3.3.5. 仮想サービス提供機関（会員登録サイト）

本節では、実証実験用に構築した仮想的なサービス提供機関としての会員登録サイトについて記述する。特に、耐タンパデバイスにアクセスする機能について詳述する。

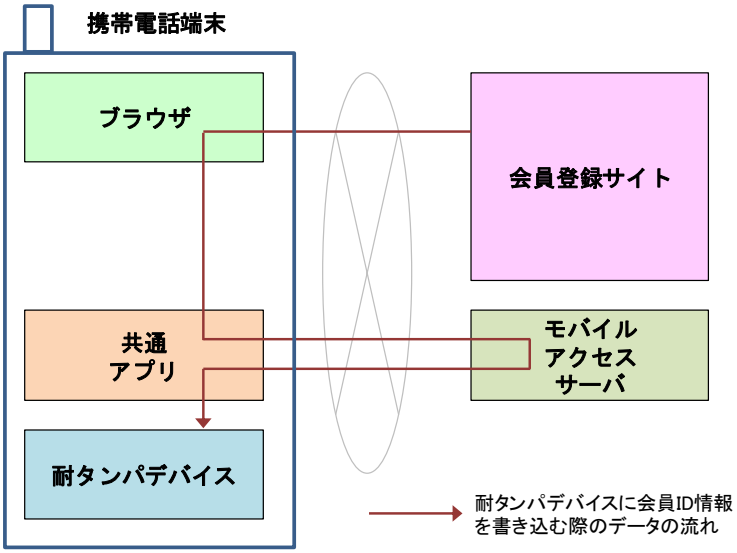


図 3-4 会員 ID 発行時のデータの流れ

図 3-4 に示すように、会員登録サイトでは、耐タンパデバイスに対して会員 ID の書き込みを行う。

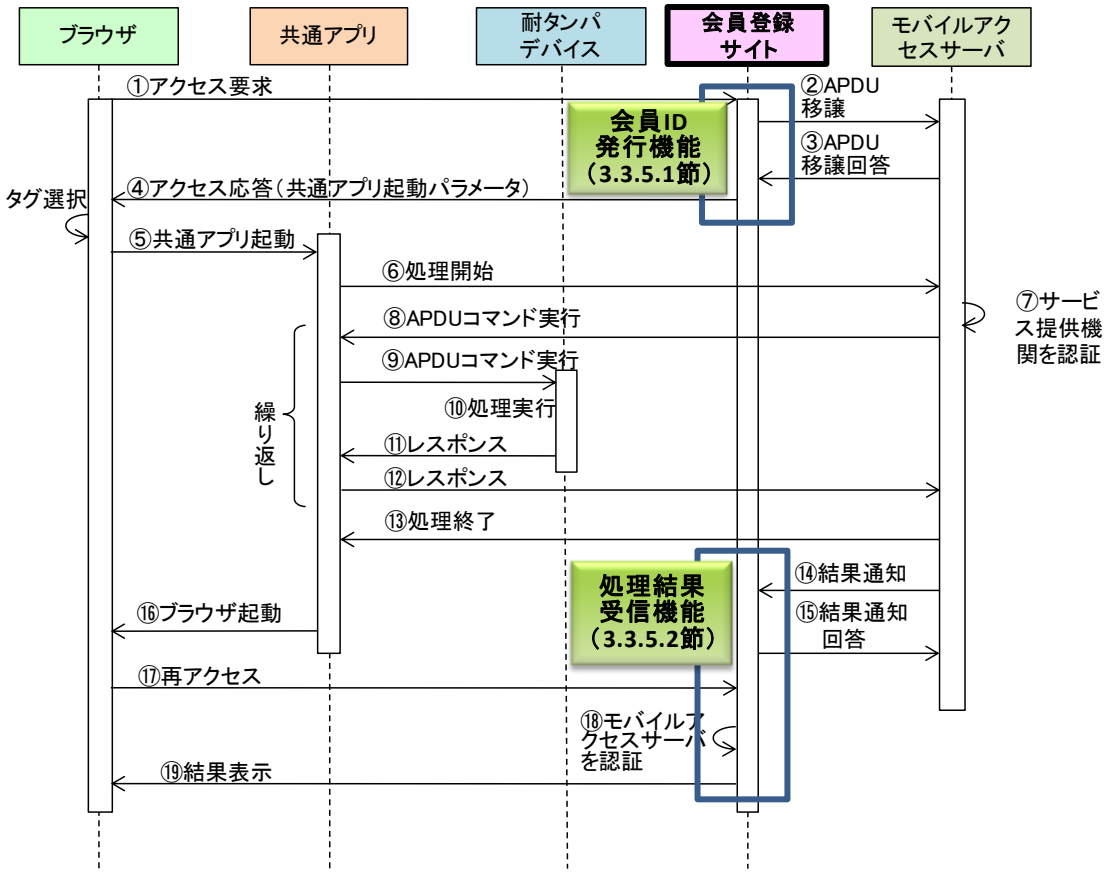


図 3-5　会員 ID 発行時の全体フロー

図 3-5 に示したように、実証実験で利用する会員登録サイトは、以下の機能を有する。

表 3-3 会員登録サイトの機能一覧

#	機能名	説明
1	会員 ID 発行	登録画面から入力されたユーザ情報を DB に登録して、会員 ID を発行する。
2	処理結果受信	モバイルアクセスサーバから受信した耐タンパデバイスへの処理結果を DB に登録する。

3.3.5.1. 会員 ID 発行機能

登録画面から入力されたユーザ情報を DB に登録して、会員 ID を発行する。会員 ID 発行

処理のフローを以下に示す。なお、下図の太線で示した処理は、課題アで示したサービス提供機関に共通の処理である。

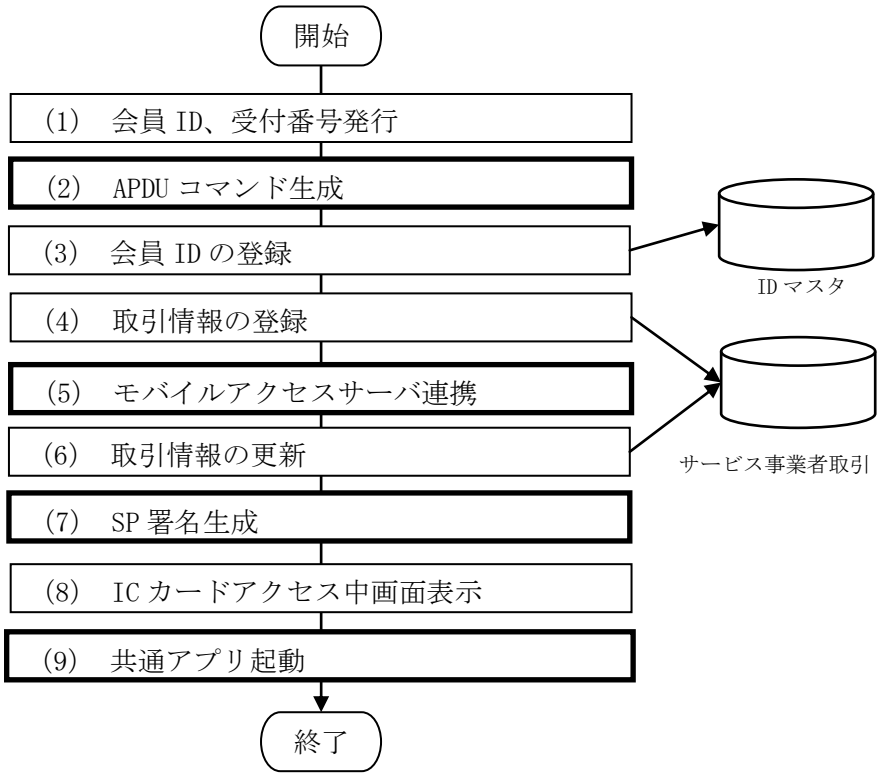


図 3-6 会員 ID 発行時の処理フロー

(1) 会員 ID、受付番号を発行

会員 ID（日付：8 桁+ID 用シーケンス番号：8 桁）と受付番号（日付：8 桁+受付番号用シーケンス番号：8 桁）を発行する。

(2) APDU コマンド生成

APDU コマンドを生成する。生成するコマンドは、Select, Verify, SelectFile, UpdateBinary である。

(3) 会員 ID の登録

DB 接続のオープンし、会員 ID を ID マスタに登録する。

(4) 取引情報の登録

取引情報を DB に登録する。

(5) モバイルアクセスサーバ連携

モバイルアクセスサーバに取引情報を送信する。

(6) 取引情報更新

連携結果が正常な場合は、取引情報を更新する。

(7) SP 署名生成

サービス事業者 ID、受付番号、APDU 生成年月日を使用して SP 署名を生成する。具体的には、SHA 方式でハッシュ値を取得したものを RSA 方式で暗号化する。また、サービス事業者 ID、公開鍵はプロパティファイルで管理する。

(8) IC カードアクセス中画面表示

IC カードアクセス中を表わす画面を表示する。

(9) 共通アプリ起動

JavaScript から共通アプリを起動する。

3.3.5.2.処理結果受信機能

耐タンパデバイスから処理結果を受信する処理フローを以下に示す。なお、下図の太線で示した処理は、課題アで示したサービス提供機関に共通の処理である。

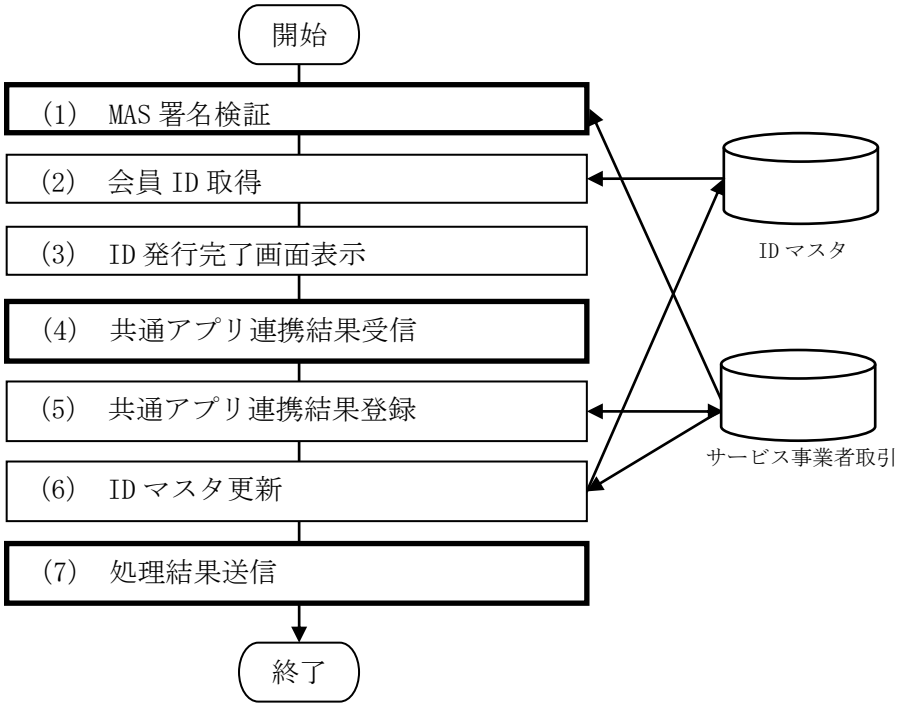


図 3-7 ID 発行完了時の処理フロー

(1) MAS 署名検証

GET パラメータから受付番号、MAS 署名を取得する。次に、サービス事業者取引テーブルから APDU 受付年月日を取得して、サービス事業者 ID、受信した受付番号、APDU 受付年月日からハッシュ値を算出する（SHA 方式でハッシュ値を算出する)。

受信した MAS 署名を秘密鍵で復号化する（秘密鍵はプロパティファイルで管理する)。算出したハッシュ値と MAS 署名を復号化した値を比較する（値が異なった場合は、DB 接続クローズとログ出力をしてエラー画面を表示する)。

(2) 会員 ID 取得

ID マスタから会員 ID を取得する。

(3) ID 発行完了画面を表示

ID 発行完了画面を表示する。

(4) 共通アプリ連携結果受信

モバイルアクセスサーバから共通アプリ連携結果を受信する。次に、受信した受付番号から APDU コマンドを取得する。

(5) 共通アプリ連携結果登録

共通アプリ連携結果を更新する。

(6) ID マスタ更新

サービス事業者取引から受信した受付番号で APDU 実行順序、APDU レスポンス番号の最大値を取得する。サービス事業者取引から取得した APDU 実行順序の APDU 戻り値を取得する。

取得した APDU 戻り値が’9000‘の場合には、受信した受付番号の削除フラグを’0‘に更新する。

(7) 処理結果送信

モバイルアクセスサーバに処理結果を送信する。

3.3.6. 仮想サービス提供機関（健康ポータルサイト）

本節では、実証実験用に構築した仮想的なサービス提供機関としての健康ポータルサイトについて記述する。特に、耐タンパデバイスにアクセスする機能について詳述する。

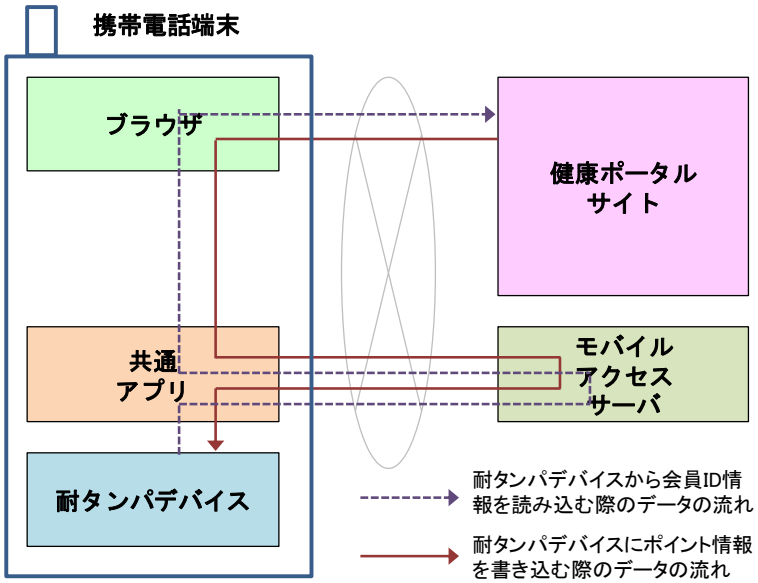


図 3-8 会員 ID 読込・ポイント書込時のデータの流れ

図 3-8 に示すように、健康ポータルサイトでは、耐タンパデバイスから会員 ID の読込みを行う。また、新たに付与されたポイントの書き込みを行う。

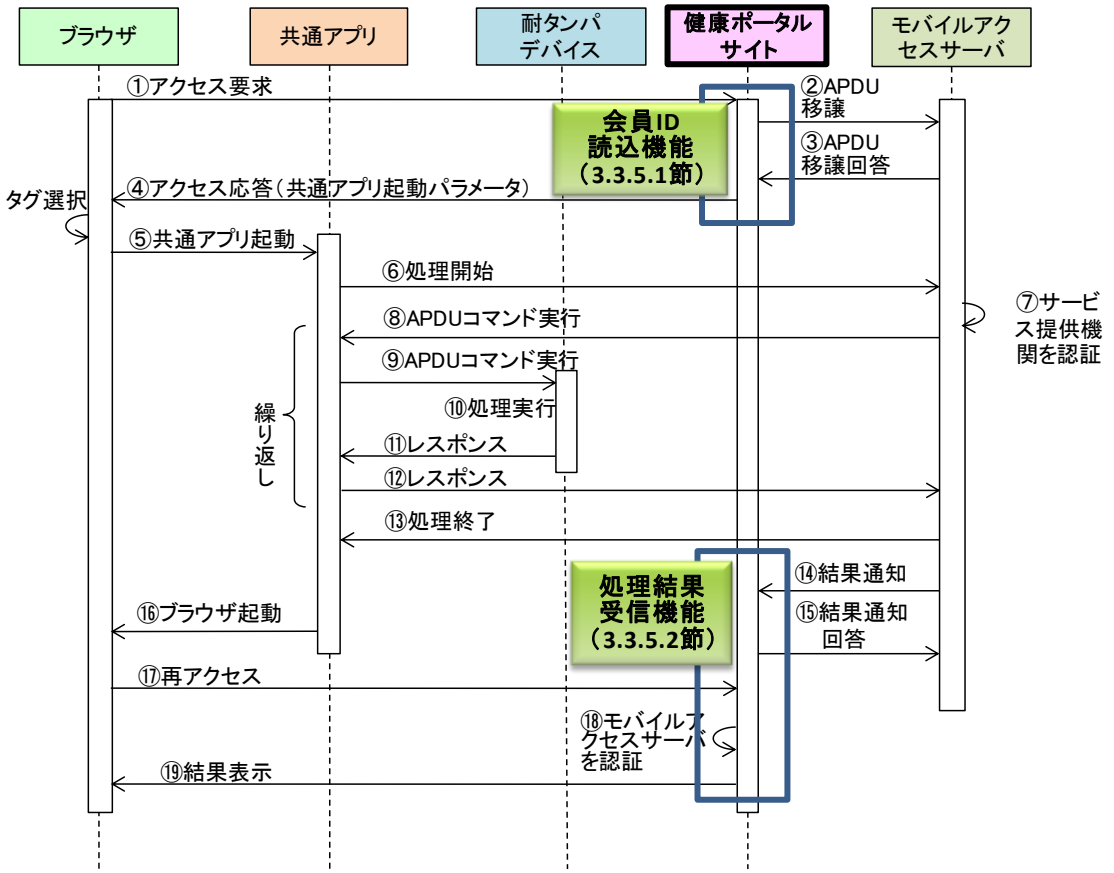


図 3-9　会員 ID 読込・ポイント書込時の全体フロー

図 3-9 に示したように、実証実験で利用する健康ポータルサイトは、以下の機能を有する。

表 3-4 健康ポータルサイトの機能一覧

#	機能名	説明
1	会員 ID 読込（ログイン）	ログイン誘導画面から IC カードアクセス中画面を表示し、共通アプリを起動する。 IC カードから読み込んだ会員 ID で健康ポータルサイトに認証をかけ、正常の場合は、ログイン結果画面を表示する。
2	処理結果受信	モバイルアクセスサーバから受信した耐タンパデバイスへの処理結果を DB に登録する。

なお、健康ポータルサイトは、ポイントの読み込み、およびポイントの書き込み処理もあるが、IC カードへアクセスし、APDU コマンドを送受信し、レスポンスを受け取るという処理の流れは、前述の会員登録サイトの会員 ID の書き込み処理、および本節のログイン機能における会員 ID の読み込み処理と共通のため本節への記述は省略する。

3.3.6.1.会員 ID 読込機能（ログイン機能）

会員登録サイトで登録され、耐タンパデバイスに書き込まれた会員 ID を読み込んでログインを行う。会員 ID 読込処理のフローを以下に示す。なお、下図の太線で示した処理は、課題アで示したサービス提供機関に共通の処理である。

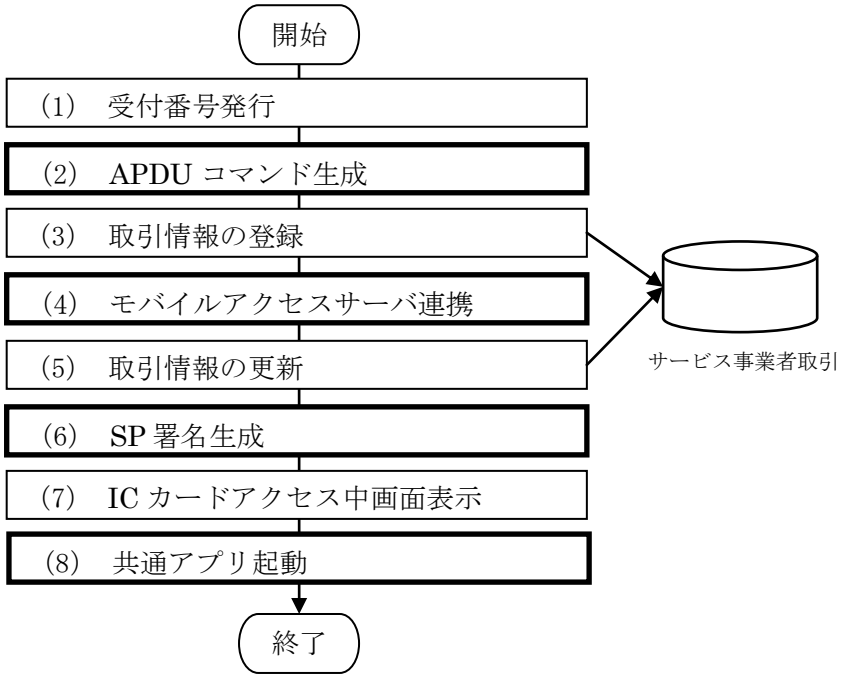


図 3-10 会員 ID 読込時の処理フロー

(1) 受付番号発行

受付番号を発行する。（日付：8 桁+受付番号用シーケンス番号：8 桁）

(2) APDU コマンド生成

APDU コマンドを生成する。生成するコマンドは、Select、Verify、SelectFile、ReadBinary である。

(3) 取引情報の登録

DB 接続をオープンし、取引情報を DB に登録する。

(4) モバイルアクセスサーバ連携

モバイルアクセスサーバに取引情報を送信する。

(5) 取引情報更新

連携結果が正常な場合は、取引情報を更新する。

(6) SP 署名生成

サービス事業者 ID、受付番号、APDU 生成年月日を使用して SP 署名を生成する。具体的には、SHA 方式でハッシュ値を取得したものを RSA 方式で暗号化する（サービス事業者 ID、公開鍵はプロパティファイルで管理する）。

(7) IC カードアクセス中画面表示

IC カードアクセス中画面を表示する。

(8) 共通アプリ起動

JavaScript から共通アプリを起動する。

3.3.6.2. 処理結果受信機能

耐タンパデバイスから処理結果としての会員 ID を受信する処理フローを以下に示す。なお、下図の太線で示した処理は、課題アで示したサービス提供機関に共通の処理である。

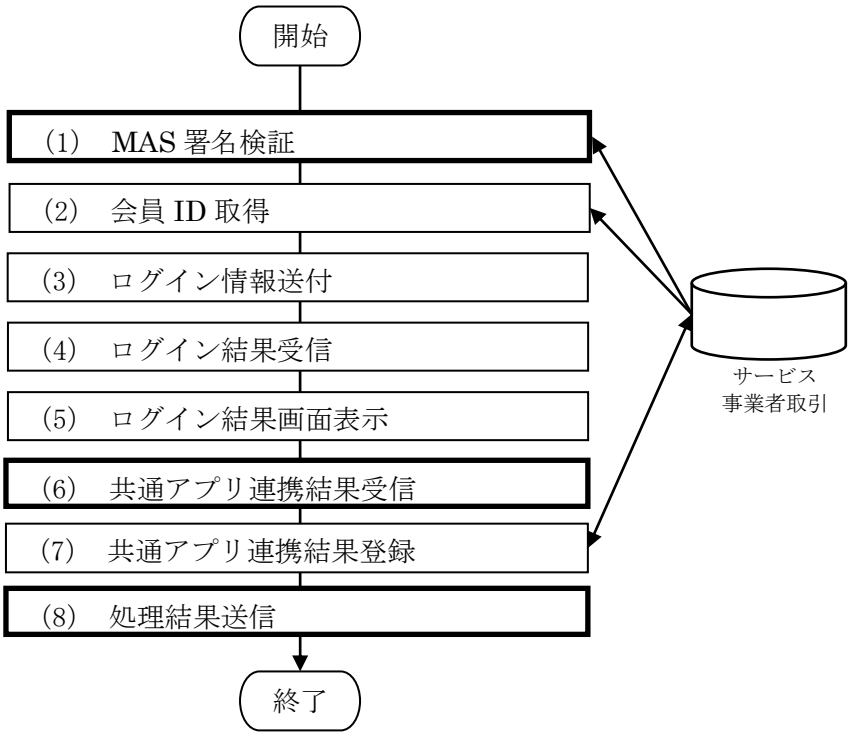


図 3-11 ログイン結果画面表示時の処理フロー

(1) MAS 署名検証

GET パラメータから受付番号を取得する。その後、サービス事業者取引テーブルから APDU 受付年月日を取得して、サービス事業者 ID、受信した受付番号、APDU 受付年月日からハッシュ値を算出する（SHA 方式でハッシュ値を算出する)。その後、受信した MAS 署名を秘密鍵で復号化する（秘密鍵はプロパティファイルで管理する)。最後に、算出したハッシュ値と MAS 署名を復号化した値を比較する。

(2) 会員 ID 取得

受付番号から会員 ID を取得する。APDU レスポンスが複数存在する場合、全てを結合した値を会員 ID とする。

(3) ログイン情報送付

健康ポータルサイトに会員 ID とパスワードを送信する。

(4) ログイン結果受信

認証結果を受信する。

(5) ログイン結果画面表示

ログイン結果画面として、ユーザ情報を表示する。

(6) 共通アプリ連携結果を受信

モバイルアクセスサーバから共通アプリ連携結果を受信する。

(7) 共通アプリ連携結果登録

受付番号から APDU コマンドを取得し、受信したレコードが存在するか確認する。レコードが存在する場合、共通アプリ連携結果を更新する。レコードが存在しない場合（GET RESPONSE の結果)、共通アプリ連携結果を登録する。

(8) 処理結果送信

モバイルアクセスサーバに処理結果を送信する。

3.3.7. 仮想サービス提供機関（ポイント交換ポータルサイト）

本節では、実証実験用に構築した仮想的なサービス提供機関としてのポイント交換ポータルサイトについて記述する。

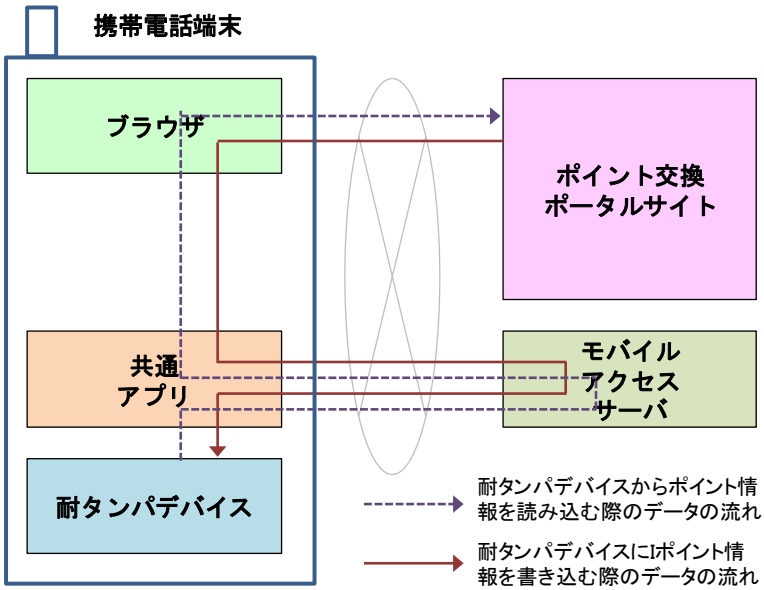


図 3-12 ポイント書込・読込時のデータの流れ

図 3-12 に示すように、ポイント交換ポータルサイトでは、耐タンパデバイスからポイントの読込みを行う。また、更新されたポイントの書き込みを行う。

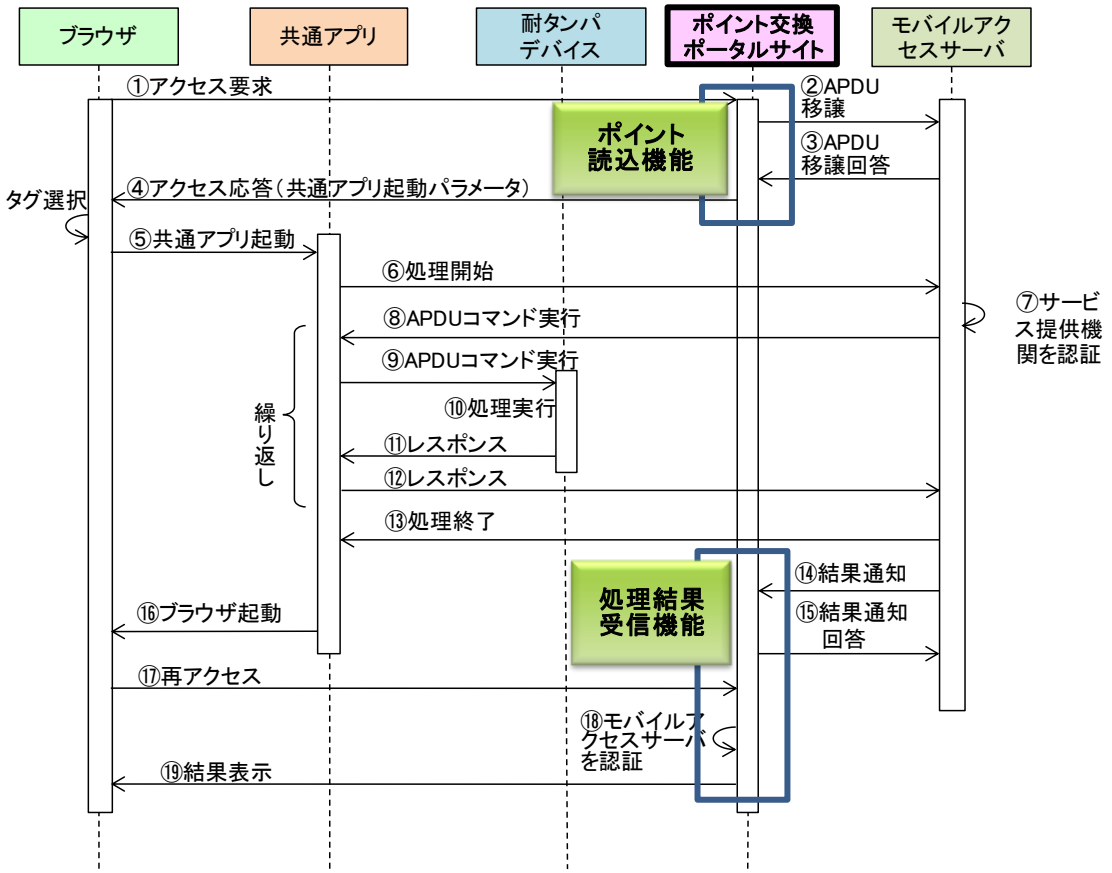


図 3-13　ポイント書込・読込時の全体フロー

ポイント交換ポータルサイトは、ポイントの読み込み、およびポイントの書き込み処理があるが、IC カードへアクセスし、APDU コマンドを送受信し、レスポンスを受け取るという処理の流れは、前述の会員登録サイトの会員 ID の書き込み処理、および前述の健診ポータルサイトのログイン機能における会員 ID の読み込み処理と共通のため本節への記述は省略する。

3.3.8. 仮想 IC カードアプリ（会員 ID 管理アプリ、ポイント管理アプリ）

本節では、IC カードアプリケーションの実装例を示す。会員 ID 管理アプリとポイント管理アプリは、同じ仕様で実現する。

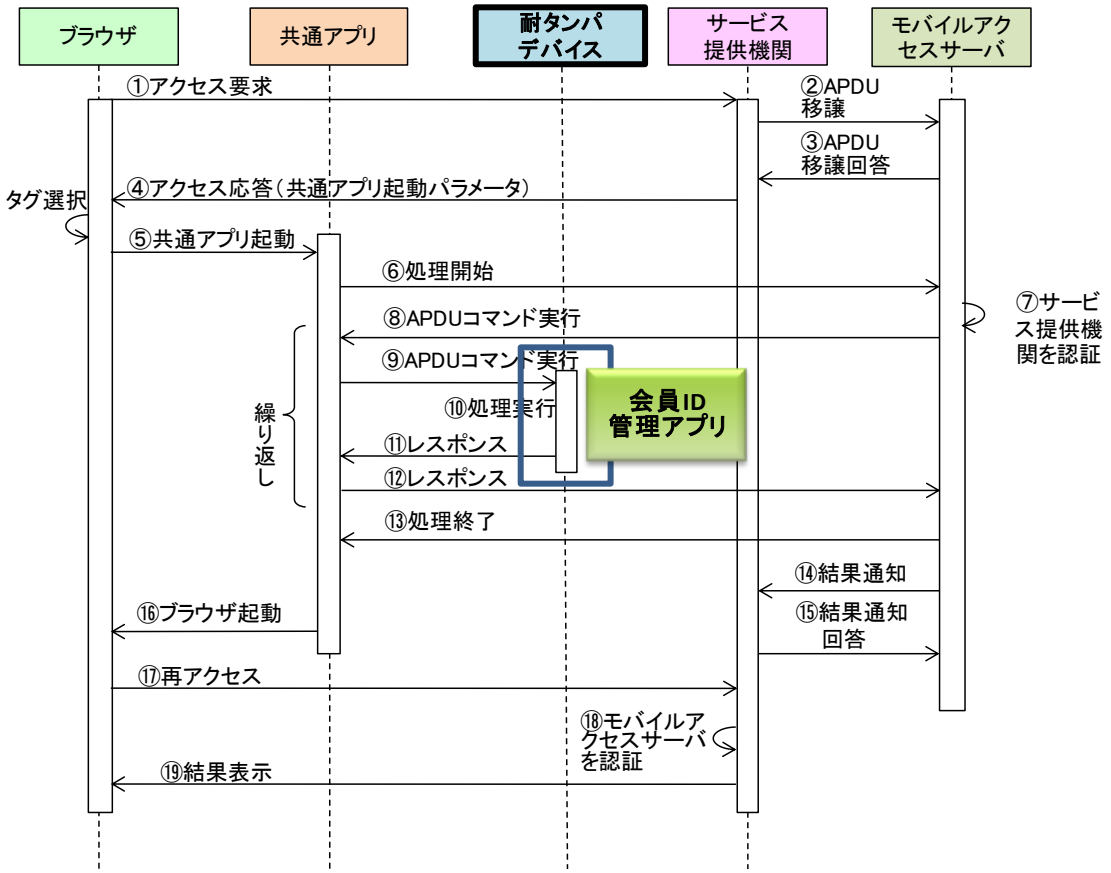


図 3-14　会員 ID 管理アプリ利用時の全体フロー

3.3.8.1. シーケンス

(1) ファイル読み出し時の処理シーケンス

ファイル読み出しを行う場合、Select コマンドの後、Initialize Update コマンドと External Authenticate コマンドによってセキュアチャネルを構築した後、Verify コマンドによって認証を行った後、ReadBinary コマンドでファイルの読み出しを行う。セキュアチャネルの構築の詳細は、「Global Platform Card Specification Version 2.2.1 Public Release」を参照。

(2) ファイル更新時の処理シーケンス

ファイル更新を行う場合、Select コマンドの後、Initialize Update コマンドと External Authenticate コマンドによってセキュアチャネルを構築した後、Verify コマンドによって認証を行った後、UpdateBinary コマンドでファイルの読み出しを行う。セキュアチャンルの構築の詳細は、「Global Platform Card Specification Version 2.2.1 Public Release」を参照。

3.3.8.2.状態遷移

(1) セキュアチャネル認証での状態遷移

アプリケーションが選択された状態のとき、内部状態はセキュアチャネル未初期化を初期状態としている。Initialize Update コマンド、External Authenticate コマンドを実行し、セキュアチャネル認証を行うことで、認証が成功すると、各種機能を実行することが出来る。この状態をセキュアチャネル認証済と呼ぶ。セキュアチャネル認証済はアプリケーションが再選択されると状態がリセットされ、セキュアチャネル未初期化状態となり、各種機能を実行する際には再度セキュアチャネル認証が必要となる。

(2) キー認証での状態遷移

アプリケーションが選択された状態のとき、内部状態はキー未認証を初期状態としている。上記（1）で示すセキュアチャネル認証を行った後、キー認証を実行することで、認証が成功すると各種機能を実行することができる。この状態をキー認証済と呼ぶ。キー認証済はアプリケーションが再選択されると状態がリセットされ、キー未認証状態となり、各種機能を実行する際には再度キー認証が必要となる。

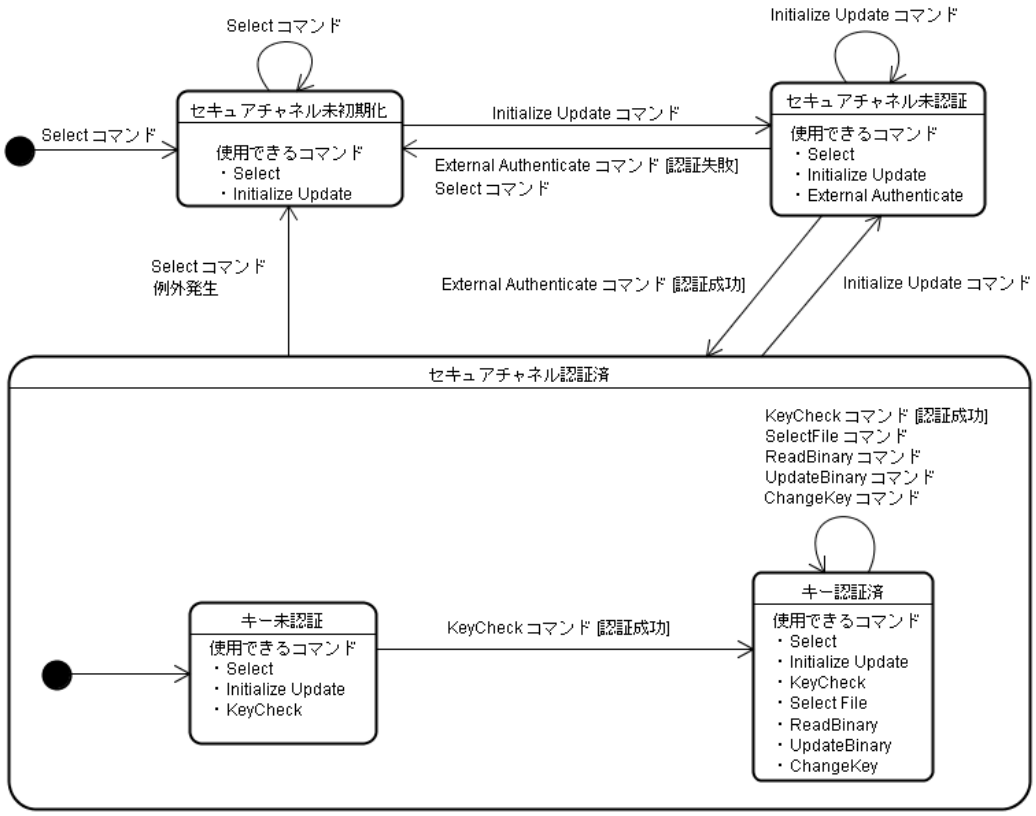


図 3-15 IC カードアプリケーションの状態遷移図

3.3.8.3.データ格納管理方式

本 IC カードアプリケーションは、ファイル名でファイルを管理し、ホストから指定されたファイルについて、データの読み出しと書き込みを行う機能を提供している。

(1) データ管理方式

本 IC カードアプリケーションのデータ構造を図 3-16 に示す。また、エリアの説明を表 3-5 に示す。

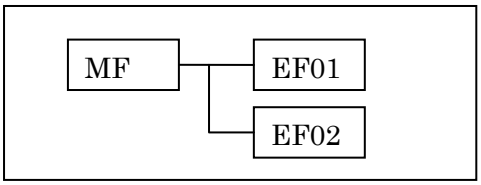


図 3-16 IC カードアプリケーションの構造

表 3-5 IC カードアプリケーションのエリアの説明

#	エリア名称	型	長さ	説明
1	MF	-	-	本 CAP の主ファイルである。本 CAP の AID を指定することで選択状態となる。
2	EF01	byte	2048	2048Byte の大きさを持つデータ領域である。本 EF のファイル名を指定することで選択状態となる。 ファイル名は 0x01。
3	EF02	byte	2048	2048Byte の大きさを持つデータ領域である。本 EF のファイル名を指定することで選択状態となる。 ファイル名は 0x02。

(2) EF のデータ格納方式

本 IC カードアプリケーションの EF は透過形式のファイル構造を持つ。データの読み出しと書き込みを実行するアドレスとデータ長を指定することにより読み書きを実現する。

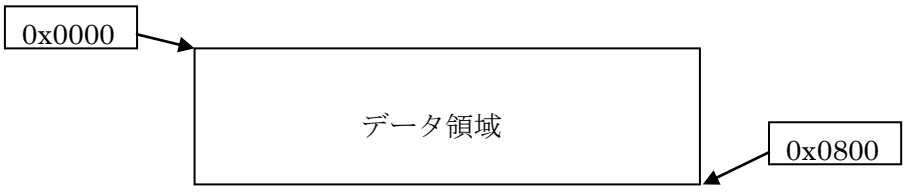


図 3-17 EF のデータ格納方式

3.3.8.4. コマンド

本 IC カードアプリケーションが備えるコマンドを以下に示す。

(1) Select

本 IC カードアプリケーションの AID を指定することで、本 IC カードアプリケーションを選択状態にすることができるコマンドである。

(2) Initialize Update

カードとホスト間でカードとセッションのデータを送信するために使用される、セキュアチャネルを開始することができるコマンドである。このコマンドはアプリケーションが選択された後、いつでも、新しいセキュアチャネルセッションを開始するために実行することができる。本コマンドを実行し、成功すると「セキュアチャネル未認証」状態となる。

(3) External Authenticate

ホストの認証と後続のコマンドのセキュリティレベルを設定することができるコマンドである。本コマンドを実行し、成功すると「セキュアチャネル認証済」状態となる。

(4) Verify

キーの状態を「キー認証済」にすることができるコマンドである。キーの状態が「キー認証済」のとき、本コマンドを実行し、認証が失敗した場合は、キーの状態は「キー未認証」に変更される。

(5) Select File

本カード AP が持つ EF のファイル名を指定することで、該当 EF を選択状態にすることができるコマンドである。

(6) ReadBinary

現在選択状態のファイル（EF01 または EF02）からデータを読み出すことができるコマンドである。本コマンドで一度に読み出せるデータ長は 255Byte である。

(7) UpdateBinary

現在選択状態のファイル（EF01 または EF02）にデータを書き込むことができるコマンドである。該当アドレスにデータが存在している場合には、上書き更新をする。本コマンドで一度に書き込めるデータ長は 255Byte である。

(8) ChangeKey

キー格納テーブルのキーの値を変更することができるコマンドである。

3.4. 実証実験方法

3.4.1. 会員登録サイトへの会員登録

会員登録サイトでは、会員登録を行う。会員 ID が、耐タンパデバイスにダウンロードされる。

図 3-18 に画面遷移を示す。

(1) まず、ユーザは会員登録情報を入力する。

(2) 登録内容を確認して登録ボタンを押す。

(3) モバイルアクセスサーバを経由して IC カードにアクセスし、会員 ID を書き込む。

(4) 登録完了画面が表示される。

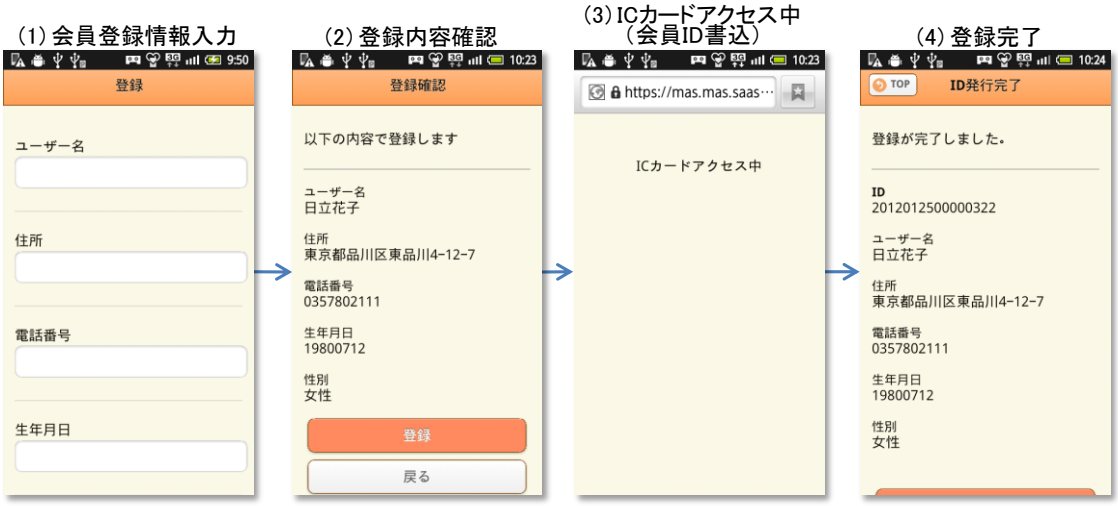


図 3-18 会員登録サイトへの会員登録の手順

3.4.2. 健康ポータルサイトでのポイント発行

会員 ID で健康ポータルサイトにログインし、日々の健康状態を記録することでポイントを貯めたり、健康状態を確認する。ポイントは、耐タンパデバイスに貯まる。

図 3-19 に画面遷移を示す。

(1) まず、ログインボタンを押す。

(2) モバイルアクセスサーバを経由して IC カードにアクセスし、会員 ID を読み込んで会員の確認を行う。

(3) 健康ポータルサイトのトップページが表示される。

(4) 健康ポータルサイトのトップページの「健康状態記録確認」ボタンを押すことで、健康状態記録を確認することができる。

(5) 健康ポータルサイトのトップページの「健康状態記録」ボタンを押すことで、血圧値、体重等の登録を行う。この登録を行うとポイントが付与される。

(6) IC カードにアクセスするためのパスワードを入力する。

(7) モバイルアクセスサーバを経由して IC カードにアクセスし、ポイント残高を読み込む。

(8) ポイントチャージ確認画面を表示する。

(9) モバイルアクセスサーバを経由して IC カードにアクセスし、ポイント残高を更新する。

(10) ポイントチャージ完了画面を表示する。

図 3-19 健康ポータルサイトでのポイント発行の手順

3.4.3. 健康ポータルサイトでのポイント利用

健康ポータルサイトにて、介護予防教室の申込みを行う。このときの参加費は、日々の健康状態記録で貯めたポイントを使うことができる。

図 3-20 に画面遷移を示す。

(1) まず、ログインボタンを押す。

(2) モバイルアクセスサーバを経由して IC カードにアクセスし、会員 ID を読み込んで会員の確認を行う。

(3) 健康ポータルサイトのトップページが表示される。

(4) 健康ポータルサイトのトップページの「介護予防教室参加者募集」ボタンを押すことで、介護予防教室への参加日を選択する。

(5) 教室の場所、時間を選択する。

(6) 予約状況を確認する。参加料金は、日々の健康状態記録で貯めたポイントを使うことができる。

(7) IC カードにアクセスするためのパスワードを入力する。

(8) モバイルアクセスサーバを経由して IC カードにアクセスし、ポイント残高を読み込む。

(9) ポイント利用後のポイントを確認する。

(10) モバイルアクセスサーバを経由して IC カードにアクセスし、ポイント残高を更新する。

(11) 受付完了画面を表示する。

図 3-20 健康ポータルサイトでのポイント利用の手順

3.4.4. ポイント交換ポータルサイトでのポイント利用

ポイント交換ポータルサイト（地域の仮想商店街）にて、日々の健康状態記録等で貯めたポイントと健康グッズ等を交換する。

図 3-21 に画面遷移を示す。

(1) ポイント交換ポータルサイトにアクセスする。

(2) IC カードにアクセスするためのパスワードを入力する。

(3) モバイルアクセスサーバを経由して IC カードにアクセスし、ポイント残高を読み込む。

(4) 現在のポイントおよびポイント利用後のポイントを確認する。

(5) モバイルアクセスサーバを経由して IC カードにアクセスし、ポイント残高を更新する。

(6) ポイント交換完了画面を表示する。

図 3-21 ポイント交換ポータルサイトでのポイント利用の手順

3.5. 実証実験による評価

本節で、実証実験に基づくモバイルアクセスシステムの評価を記述する。

3.5.1. 機能評価

本節では、実証実験システムにおける機能評価を示す。表 3-6 に機能評価の結果一覧を示す。表 3-6 は、2.5.1 節で示したモバイルアクセスサーバ、共通アプリ、サービス提供機関の機能に対する実証実験システムにおける対応個所を示し、それぞれの機能が実証実験において正しく動作したことを示している。

表 3-6 機能評価結果一覧

エンティティ	機能	説明	実証実験システム対応個所	評価結果
モバイルアクセスサーバ	受付処理機能	サービス提供機関から送信された情報を受け取る。	会員登録サイトの会員 ID 発行時の APDU 受け付け	○
			健康ポータルサイトの会員 ID 読込時の APDU 受け付け	○
			健康ポータルサイトのポイント書込時の APDU 受け付け	○
			健康ポータルサイトのポイント読込時の APDU 受け付け	○
			ポイント交換ポータルサイトのポイント読込時の APDU 受け付け	○
			ポイント交換ポータルサイトのポイント書込時の APDU 受け付け	○
	共通アプリアクセス機能	サービス提供機関から共通アプリ経由で転送されるデータが本当に正しいサービス提供機関から送信されたデータなのかを確認し、耐タンパデバイスとセキュアセッションを確立し、携帯電話端末内の共通アプリに対して暗号化されたコマンドを送受信し、結果をサービス提供機関に返信する。	会員登録サイトの会員 ID 発行時の共通アプリアクセス	○
			健康ポータルサイトの会員 ID 読込時の共通アプリアクセス	○
			健康ポータルサイトのポイント書込時の共通アプリアクセス	○
			健康ポータルサイトのポイント読込時の共通アプリアクセス	○
			ポイント交換ポータルサイトのポイント読込時の共通アプリアクセス	○
			ポイント交換ポータルサイトのポイント書込時の共通アプリアクセス	○

共通アプリ	APDU 転送機能	モバイルアクセスサーバから受信した暗号化されたコマンドを耐タンパデバイスへ送信し、耐タンパデバイスからのレスポンスをモバイルアクセスサーバに返信する。	会員登録サイトの会員 ID 発行時の APDU 転送	○
			健康ポータルサイトの会員 ID 読込時の APDU 転送	○
			健康ポータルサイトのポイント書込時の APDU 転送	○
			健康ポータルサイトのポイント読込時の APDU 転送	○
			ポイント交換ポータルサイトのポイント読込時の APDU 転送	○
			ポイント交換ポータルサイトのポイント書込時の APDU 転送	○
			会員登録サイトの会員 ID 発行時の APDU 転送	○
サービス提供機関サイト	ID 情報発行機能	耐タンパデバイスに送信したいコマンドをモバイルアクセスサーバに移譲し、かつ、携帯電話端末のブラウザを経由して、共通アプリを起動させ、耐タンパデバイスに ID 情報を送信する。	会員登録サイトの会員 ID 発行	○
			健康ポータルサイトの会員 ID 読込	○
			健康ポータルサイトのポイント書込	○
			健康ポータルサイトのポイント読込	○
			ポイント交換ポータルサイトのポイント読込	○
			ポイント交換ポータルサイトのポイント書込	○
	処理結果受信機能	モバイルアクセスサーバから耐タンパデバイス内での処理結果を受信し、返される処理結果が本当に正しいモバイルアクセスサーバから送信されたデータなのかを確認する。	会員登録サイトの会員 ID 発行の結果受信	○
			健康ポータルサイトの会員 ID 読込の結果受信	○
			健康ポータルサイトのポイント書込の結果受信	○
			健康ポータルサイトのポイント読込の結果受信	○
			ポイント交換ポータルサイトのポイント読込の結果受信	○
			ポイント交換ポータルサイトのポイント書込	○

3.5.2. 性能評価

3.5.2.1.性能評価に用いた機器

本節では、性能測定に用いた機器について述べる。性能測定で用いたモバイルアクセスサーバの機器仕様を表 3-7 に示す。なお、サービス提供機関の機能も同様のサーバ上に構築した。また、耐タンパデバイスとしては、IC チップを搭載した microSD 型の耐タンパデバイスを用いた。

表 3-7 モバイルアクセスサーバの機器仕様

OS	Red Hat Enterprise Linux ES 5 64bit
CPU	Intel Core 2 Duo P8700 (2.53GHz)
Memory	6GB
HDD	30GB

また、表 3-8 および表 3-9 に性能測定に用いた携帯端末の機器仕様を示す。

表 3-8 携帯電話端末 1 の機器仕様

OS	Android™ 2.3.5
CPU	Qualcomm Snapdragon MSM8655 1.4GHz
データ通信方式	WIN HIGH SPEED (CDMA2000 1xEV-DO MC-Rev.A)
通信速度	下り最大 9.2Mbps/上り最大 5.5Mbps

表 3-9 携帯電話端末 2 の機器仕様

OS	Android™ 2.3
CPU	OMAP4430 1GHz (デュアルコア)
データ通信方式	ULTRA SPEED (HSPA+)
通信速度	下り最大 21Mbps、上り最大 5.7Mbps

3.5.2.2.性能測定項目

本節では、性能測定を行う項目を示す。

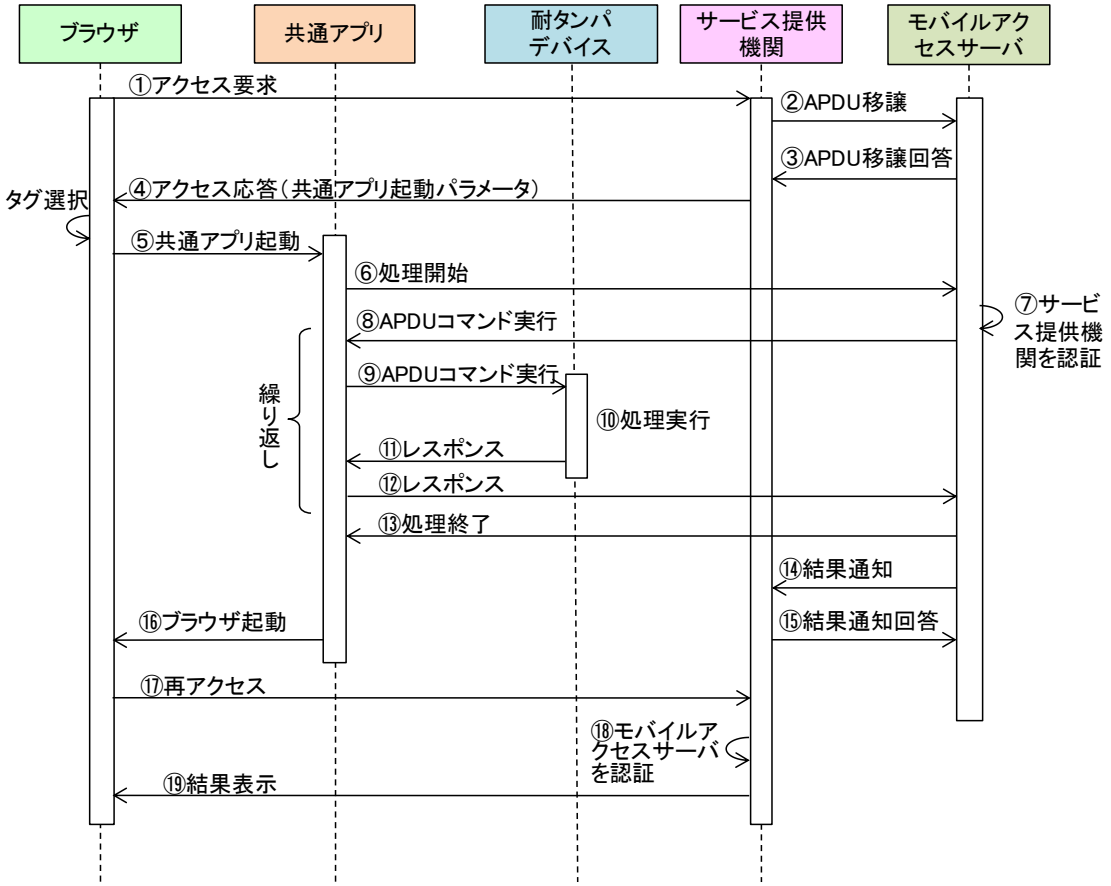


図 3-22 データの流れを示す詳細図（再掲）

表 3-10　性能測定項目

#	性能計測項目	詳細説明	図 3-22 の対応番号
1	サービス提供機関内の処理＋サーバ間通信	①を受信→内部処理→②③APDU 移譲連携（サーバ通信含む）→内部処理→④の開始まで、⑰を受信→内部処理→⑱モバイルアクセスサーバ認証→⑲の開始まで	②－③、⑱
2	携帯電話端末－モバイルアクセスサーバ間の通信	⑥の通信、⑧の通信、⑫の通信、⑬の通信	⑥、⑧、⑫、⑬
3	携帯電話端末内の処理	⑨APDU コマンド実行→⑩処理実行→⑪レスポンス＋その他内部処理	⑨－⑩－⑪
4	モバイルアクセスサーバ内の処理＋サーバ間通信	⑦サービス提供機関認証、⑭⑮結果連携（サーバ通信含む＋その他内部処理	⑦、⑭－⑮
5	携帯電話端末－サービス提供機関間の通信＋携帯電話端末内の処理（共通アプリ起動＋ブラウザ起動）	④の通信→⑤の共通アプリ起動時間、⑯のブラウザ起動→⑰の通信	④－⑤、⑯－⑰

3.5.2.3.性能測定結果

本節では、性能測定結果を示す。実証実験で行った仮想サービスの内、会員 ID の書き込み処理とポイントの書き込み処理の性能を測定した。また、携帯電話端末は、表 3-8 および表 3-9 に示した性能の異なる 2 種類の機器を用いた。性能評価結果を表 3-11 および表 3-12 に示す。なお、表 3-11 および表 3-12 に示した測定値は、5 回計測した平均値を示している。

表 3-11　会員 ID 書込処理の性能測定結果

#	性能計測項目	端末 1（ms）	端末 2　（ms）
1	サービス提供機関内の処理＋サーバ間通信	91	103
2	携帯電話端末－モバイルアクセスサーバ間の通信（8 往復）	3751	2951
3	携帯電話端末内の処理（Connect＋APDU（5 回）＋DisConnect＋その他処理）	1193	1234
4	モバイルアクセスサーバ内の処理＋サーバ間通信（3 往復））	343	217
5	携帯電話端末－サービス提供機関間の通信＋携帯電話端末内の処理	1291	792
6	全体	6669	5296

表 3-12　ポイント書込処理の性能測定結果

#	性能計測項目	端末 1　（ms）	端末 2　（ms）
1	サービス提供機関内の処理＋サーバ間通信	126	63
2	携帯電話端末－モバイルアクセスサーバ間の通信（9 往復）	3760	3526
3	携帯電話端末内の処理（Connect＋APDU（6 回）＋DisConnect＋その他処理）	1173	1424
4	モバイルアクセスサーバ内の処理＋サーバ間通信（4 往復））	317	216
5	携帯電話端末－サービス提供機関間の通信＋携帯電話端末内の処理	908	833
6	全体	6283	6063

3.5.2.4. 性能測定結果に対する考察

表 3-11 および表 3-12 に示したように、耐タンパデバイスに対する会員 ID の書込みおよびポイントの書き込みに関して、約 6 秒で行えることが分かった。

処理速度および通信速度の異なる 2 つの携帯電話端末で会員 ID 書き込み処理とポイント書き込み処理について性能測定を行った結果では携帯電話端末の違いでの性能差はほとんどみられなかった。

但し、処理別にみるとサーバと携帯電話端末間の通信（項目 No.2 と No.5）がそれぞれ 7 割以上と大きな割合を占めていた。それに対してサーバ間通信（項目 No.4）は数往復のデータ送受信を行っているが 350ms 以内とほとんどかかっていないことから、この結果はネットワーク上の処理性能差と判断できる。

また、今回の性能測定では、会員 ID の書き込み（APDU 送信回数 5 回）と、ポイントの書き込み（APDU 送信回数 6 回）の測定を行ったが、送受信するデータの大きさによって、あるいは、同時アクセス数によって性能は異なる。導入の際は、上記観点を考慮する必要がある。

3.5.3. ヒアリング評価

本節では、モバイルアクセスシステムの有効性を確認するため、利用者参加型の実証実験を実施し、利用者の意見を収集した。

3.5.3.1. 実施概要

(1) 目的

利用者がモバイルアクセスシステムの実験環境を実際に利用し、その結果をヒアリング、分析することで、モバイルアクセスシステムの運用性、利便性を検証する。

(2) 概要

モバイルアクセスシステムの運用性、有効性を確認するため、以下の通り、沖縄県浦添市民と市職員、台東区民にヒアリングを実施した。

①浦添市

- 日時
  2012 年 2 月 15 日（水）14:00－15:00
- 場所
  沖縄県浦添市役所　会議室
- ヒアリング対象者
  ・65 歳以上の浦添市民　4 名
  ・介護に携わっている保護士 3 名及び自治体職員 1 名

②台東区

- 日時
  2012 年 3 月 9 日（金）15:00－16:00
- 場所
  台東区　浅草
- ヒアリング対象者
  60 歳以上の台東区民　7 名

3.5.3.2. 実施内容

(1) 実施手順

以下の①から④の手順で説明、ヒアリング等を実施した。

①モバイルアクセスシステムを活用した想定される自治体提供サービスの概要説明
②デモ内容の説明
③利用者によるスマートフォンからのモバイルアクセスシステムの利用
④その結果を係員がヒアリングし、ヒアリングシートに記載

(2) 実施内容

①モバイルアクセスシステムを活用した自治体提供サービス（想定）の概要説明

モバイルアクセスシステムを活用した想定される自治体提供サービスとして、健康支援サービス向上のための地域通貨（ポイント）活用と行政手続きの電子化の概要について説明を実施した。具体的には、以下のサービス内容である。

- 健康支援サービス向上のための地域通貨（ポイント）活用サービス

  高齢者が安心・安全で便利な生活を行うことができ、かつ健康維持を図るためのサービスを想定している。具体的には、以下のサービス内容である。

  - 携帯（スマートフォン）を利用して、いつでも、どこでも、情報（生活状態・健康状態・教室参加等）の記録と確認を行う。
  - 情報をスマートフォンから自治体に提供すると、地域の商店や自治体等で利用できる地域ポイントを付与する。
  - 病気など緊急時には予め登録した方（家族、病院、自治体、近隣のボランティア、友人など）に通知する。
  - ボランティア活動に参加すると、地域の商店や自治体等で利用できる地域ポイントを付与する。

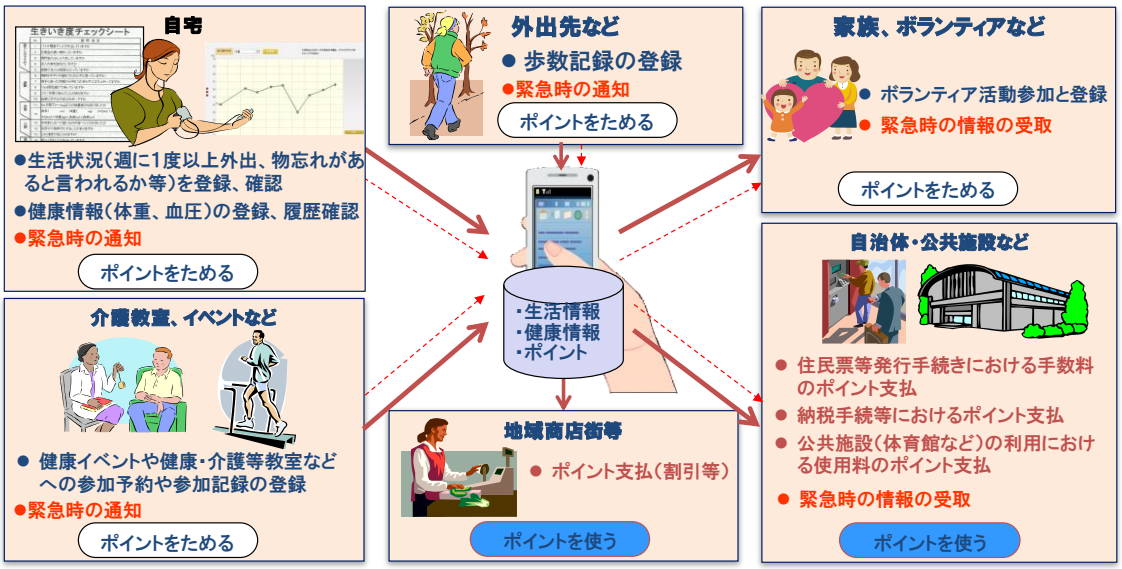


図 3-23 健康支援サービス向上のための地域通貨（ポイント）活用イメージ

● スマートフォンによる行政の各種申請サービス

スマートフォンで行政の各種申請を事前に登録し、スマートフォンをかざすと用紙への記入なしで申請できるサービスを想定している。具体的には、以下のサービス内容である。

・ スマートフォン上で予め登録した申請書により、住民票の写し、戸籍などの証明書の発行を行う。

・ スマートフォン上で予め登録した申請書により、住民登録（転出、転入）などの各種申請手続きを行う。

図 3-24 スマートフォンでの各種申請手続きイメージ

● スマートフォンによる税金、保険料等の支払いサービス

税金、各種保険料等の支払いにおいて支払情報をスマートフォンに通知し、クレジットなどオンラインで支払を行うサービスを想定している。

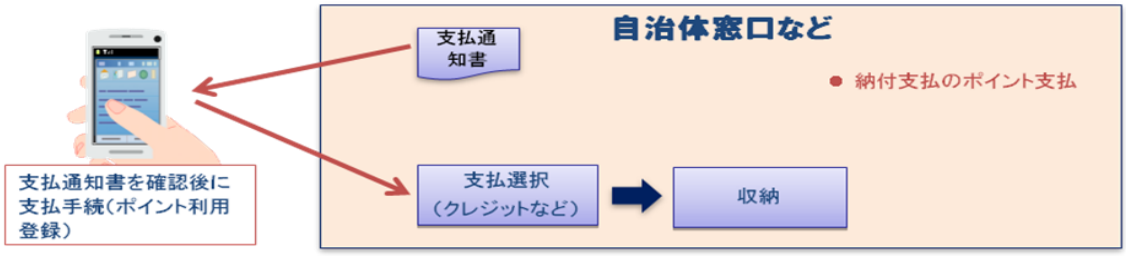


図 3-25 スマートフォンでの税金等の支払いイメージ

②デモ内容の説明

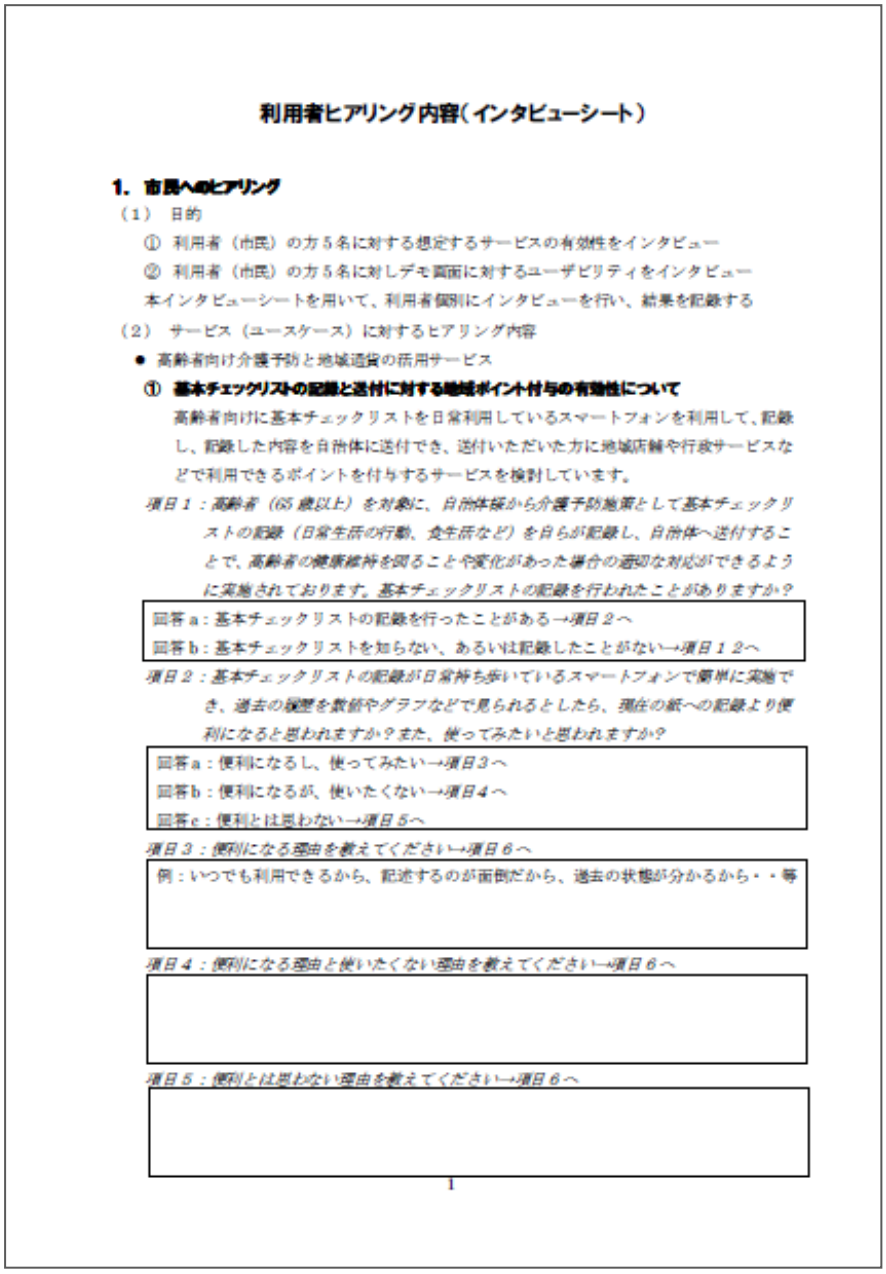
利用者に 3.3. 節の実証実験システムの概要と、3.4. 節の実証実験方法について説明を実施した。

③利用者によるスマートフォンからのモバイルアクセスシステムの利用

利用者は、②のデモ内容に従い、スマートフォンを操作し、モバイルアクセスシステムを利用した。

④係員によるヒアリングし、ヒアリングシートに記載

係員が利用者にヒアリングを行いながら、以下のヒアリングシート（サンプル）に記載した。



利用者ヒアリング内容（インタビューシート）

1. 市民へのヒアリング

（1） 目的

① 利用者（市民）の方５名に対する想定するサービスの有効性をインタビュー

② 利用者（市民）の方５名に対しデモ画面に対するユーザビリティをインタビュー

本インタビューシートを用いて、利用者個別にインタビューを行い、結果を記録する

（2） サービス（ユースケース）に対するヒアリング内容

● 高齢者向け介護予防と地域通貨の活用サービス

① 基本チェックリストの記録と送付に対する地域ポイント付与の有効性について

高齢者向けに基本チェックリストを日常利用しているスマートフォンを利用して、記録し、記録した内容を自治体に送付でき、送付いただいた方に地域店舗や行政サービスなどで利用できるポイントを付与するサービスを検討しています。

項目１：高齢者（65 歳以上）を対象に、自治体様から介護予防施策として基本チェックリストの記録（日常生活の行動、食生活など）を自らが記録し、自治体へ送付することで、高齢者の健康維持を図ることや変化があった場合の適切な対応ができるように実施されております。基本チェックリストの記録を行われたことがありますか？

回答ａ：基本チェックリストの記録を行ったことがある→項目２へ
回答ｂ：基本チェックリストを知らない、あるいは記録したことがない→項目１２へ

項目２：基本チェックリストの記録が日常持ち歩いているスマートフォンで簡単に実施でき、過去の履歴を数値やグラフなどで見られるとしたら、現在の紙への記録より便利になると思われますか？また、使ってみたいと思われますか？

回答ａ：便利になるし、使ってみたい→項目３へ
回答ｂ：便利になるが、使いたくない→項目４へ
回答ｃ：便利とは思わない→項目５へ

項目３：便利になる理由を教えてください→項目６へ

例：いつでも利用できるから、記述するのが面倒だから、過去の状態が分かるから・・等

項目４：便利になる理由と使いたくない理由を教えてください→項目６へ

項目５：便利とは思わない理由を教えてください→項目６へ

1

図 3-26 ヒアリングシート（サンプル）

3.5.3.3. 利用者へのヒアリング結果

図 3-26 のヒアリングシートに基づき、利用者にヒアリングを行った。以下にヒアリングの結果を示す。

(1) モバイルアクセスシステムを活用した自治体提供サービス内容の有効性についてのヒアリング

①日常生活の行動、食生活等の記録と送付に対する地域ポイント付与の有効性について

高齢者向けに日常利用しているスマートフォンを利用して、日常生活の行動、食生活等の情報を記録し、記録した内容を自治体に送付でき、送付いただいた方に地域店舗や行政サービスなどで利用できるポイントを付与するサービスの有効性に関するヒアリング結果は以下となる。

【結果】サービスの有効性についてヒアリングした結果、11 人中 7 人（64%）が「使いたい」という意見であった。主な理由は以下であった。

- メールなどで通知されれば電話にでられないときに便利、いつでも確認ができる
- 郵送する手間がなくなるから
- データで見ることが出来、自己管理ができる
- お薬手帳のように利用し、緊急時等で使いたい
- 病院や先生が変わったときに便利

一方、以下のコメントがあった。

- 仕事、趣味以外に携帯電話端末を使いたくない

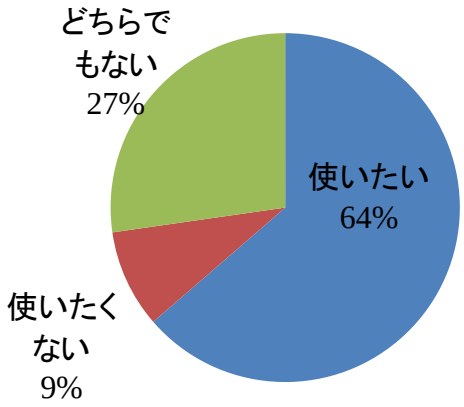


図 3-27 日常生活の行動、食生活などの情報の記録と送付に対する地域ポイント付与

②個人バイタルデータ（健康状態登録）や歩行の記録と自治体への送付、送付された方への地域ポイント付与の有効性について

高齢者向けに血圧、体重、歩数記録を日常利用しているスマートフォンを利用して、記録し、記録した内容を自治体に送付でき、送付いただいた方に地域店舗や行政サービスなどで利用できるポイントを付与するサービスの有効性に関するヒアリング結果は以下となる。

【結果】サービスの有効性についてヒアリングした結果、11 人中 7 人（64%）が「使いたい」という意見であった。主な理由は以下であった。

- 現在は毎日紙媒体に結果を記録しているが、スマートフォンになると紙で管理する必要がなく、また自分が記録した結果がグラフで見れ、管理できるのでよい

一方、以下のコメントがあった。

- 毎週の通院の際に検査を受けているから不要

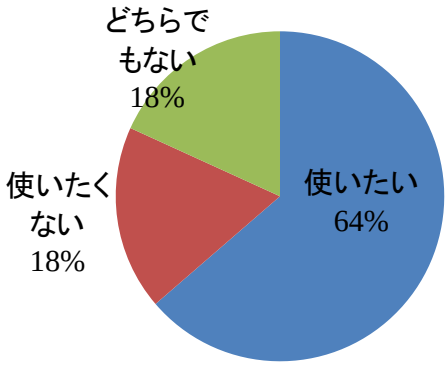


図 3-28 個人バイタルデータ（健康状態登録）や歩行の記録と自治体への送付、送付された方への地域ポイント付与

③介護教室への参加等高齢者自らが介護予防活動への参加と活動結果の自治体への送信に対する地域ポイント付与の有効性について

高齢者向けに自治体にて実施している介護予防教室、予防相談、介護サークル等の活動に参加している方に日常利用しているスマートフォンを利用して、参加記録し、記録した内容を自治体に送付いただいた方に地域店舗や行政サービスなどで利用できるポイントを付与するサービスの有効性に関するヒアリング結果は以下となる。

【結果】サービスの有効性についてヒアリングした結果、11 人中 6 人（55%）が「便利になるし、使ってみたい」という意見であった。主な理由は以下であった。

- スマートフォンが使えれば、簡単に登録ができそうだから
- 参加した記録がすぐに確認でき、他人に見せることができるから

一方、以下のコメントがあった。

- 書くシーンが減るので、脳が老化しないか心配
- 病院で十分
- 教室に参加するのが大変

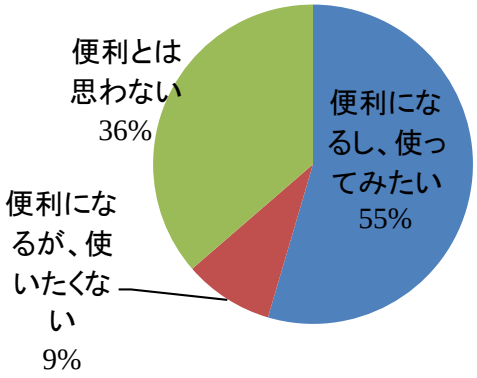


図 3-29 介護予防活動への参加と活動結果の
自治体への送信に対する地域ポイント付与

④高齢者の見守りに対する有効性について

高齢者の方（特に独居の方）を対象として、緊急時に予め通報対象者として登録した方（親類、ボランティア、自治体、医療機関など）に対して緊急通報ができるサービスの有効性に関するヒアリング結果は以下となる。

【結果】サービスの有効性についてヒアリングした結果、11 人いずれも「便利になるし、使ってみたい」という意見であった。主な理由は以下であった。

- 命に関わることなので常に持っている携帯電話端末で緊急時に病院等にすぐに連絡が取れるから
- 1 人暮らしの老人や、1 人で出かけるときに、これがあると安心
- このサービスは、今回のサービス案の中で、一番効果があると思う
- 持病があるので便利

一方、以下のコメントがあった。

- 最初の初期登録が面倒そう

⑤介護ボランティアの活動に対する地域ポイント付与の有効性について

高齢者向けにボランティア活動（健康教室、介護サークル、高齢者見守りなど）に参加している方に日常利用しているスマートフォンを利用して、参加記録し、記録した内容を自治体に報告いただいた方に地域店舗や行政サービスなどで利用できるポイントを付与するサービスの有効性に関するヒアリング結果は以下となる。

【結果】サービスの有効性についてヒアリングした結果、11 人中 9 人より回答があり、9 人中 4 人（45%）が「便利になるし、使ってみたい」という意見であった。主な理由は以下であった。

- 自分の参加記録をわざわざ紙に記入する必要がなくなるから

一方、以下のコメントがあった。

- ポイントのためにやっているわけではない

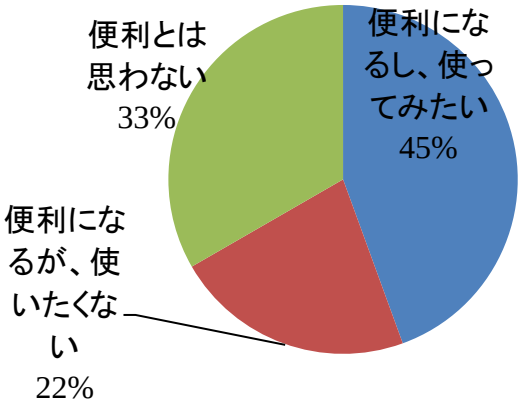


図 3-30 介護ボランティアの活動に対する地域ポイント付与

⑥地域ポイント利用に対する有効性について

上記①から⑤の活動に対して、高齢者やボランティアの方に付与されたポイントの活用として、地域店舗での利用に加えて、住民票等の発行手数料、介護教室や運動教室など有料イベントへの参加料、公共施設（体育館、テニスコートなど）の利用料など行政サービスで利用できるサービスに関するヒアリング結果は以下となる。

【結果】サービスの有効性についてヒアリングした結果、11 人中 8 人（73%）が「便利になるし、使ってみたい」という意見であった。主な理由は以下であった。

- 公共施設やサービスはよく使っているので便利
- ポイントの利用分野が増え便利
- 病院、映画館、コンビニで使えると便利

一方、以下のコメントがあった。

- ポイントを利用できる範囲が狭そう
- 施設・役所の利用が頻繁にはないため、不要
- 使い方を調べるのが面倒

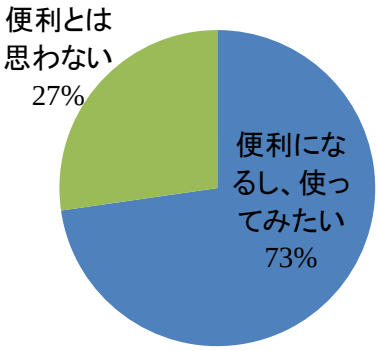


図 3-31 ボランティアの活動に対する
地域ポイント付与

⑦住民票等の発行手続きの電子化に対する有効性について

住民票や戸籍などの各種証明書の発行を自治体窓口、コンビニ等でスマートフォンをかざすことで、申請が行えるサービスに関するヒアリング結果は以下となる。

【結果】サービスの有効性についてヒアリングした結果、11 人中 9 人（82%）が「便利になるし、使ってみたい」という意見であった。主な理由は以下であった。

- 時間短縮になる

一方で、以下のコメントがあった。

- 手が不自由な為、利用が難しい

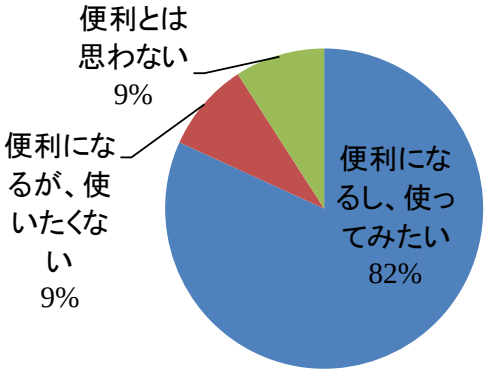


図 3-32 住民票等の発行手続きの電子化

⑧公金収納の電子化に対する有効性について

市民税や固定資産税などの納税を市民の保有するスマートフォンに通知し、スマートフォン上からクレジットなどで支払を行うサービスに関するヒアリング結果は以下となる。

【結果】サービスの有効性についてヒアリングした結果、11 人中 8 人（73%）が「便利になるし、使ってみたい」という意見であったが、一方で、以下ような意見もあった。

- 公金納付等が電子化されることは望ましいことだが、浦添市のサービスだけが電子化されても、国・県・第三セクタ等が紙だと、住民にとっては逆に管理が面倒になる。やるなら、まとめてスマホで出来るようにならないと、利便性は向上しない

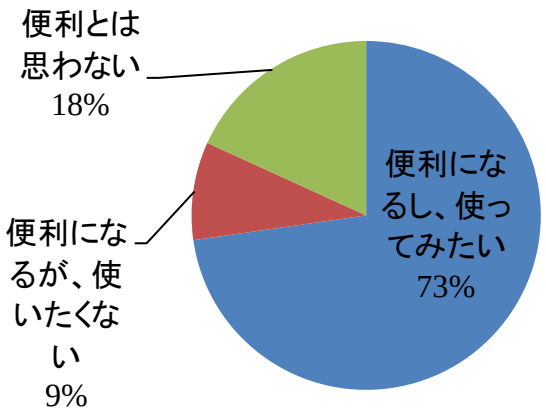


図 3-33 公金収納の電子化

(2) スマートフォンのユーザビリティについて

①携帯電話端末の利用状況について

【結果】携帯電話端末の利用状況についてヒアリングした結果、11 人中 9 人が携帯電話端末を持っており、そのうち 8 人がメールのやり取りした経験がある。

一方、インターネット接続、無料・有料のアプリケーションをダウンロードした経験がある方は少数であった。

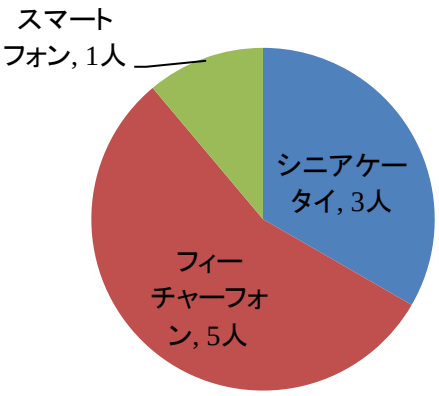


図 3-34 使用している携帯電話端末

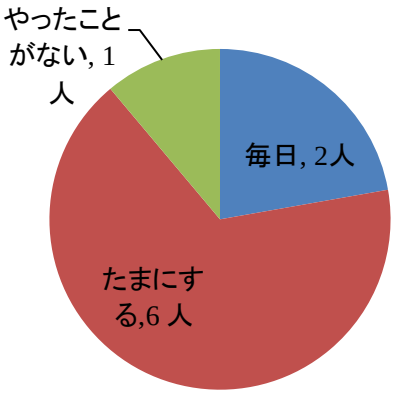


図 3-35 携帯電話端末でメールのやり取り

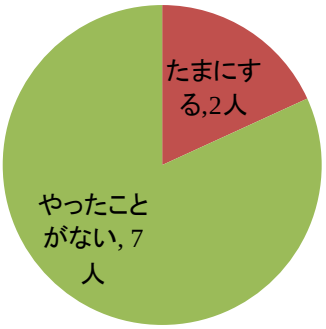


図 3-36 携帯電話端末でインターネット接続

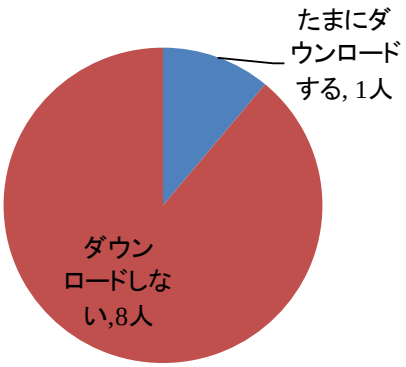


図 3-37 携帯電話端末で無料・有料のアプリケーションのダウンロード

②介護予防教室の予約に関する操作性について

選択方式で介護予防教室の予約ができる操作性についてのヒアリング結果は、以下となる。

【結果】選択方式による入力方法に関する操作性をヒアリングした結果、ヒアリング対象者 11 人中 4 人が「簡単にできた」または、「まあまあ簡単にできた」という意見であった。

一方、「できない」と回答した 2 人から、以下の意見があった。

- 楽しい、でも一生懸命だったので評価が難しい
- 手が震えるため、ボタンの方がよい

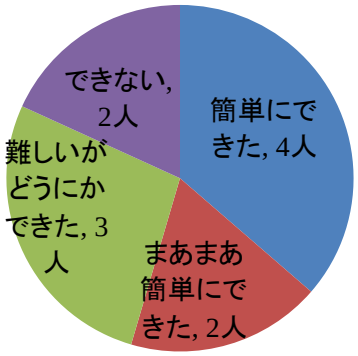


図 3-38 介護予防教室の予約

③タッチパネル血圧や体重等の入力に関する操作性について

血圧や体重をタッチパネルで入力する方式で登録できる操作性についてのヒアリング結果は、以下となる。

【結果】数字の入力方式に関する操作性をヒアリングした結果、ヒアリング対象者 11 人中 4 人が「簡単にできた」または、「まあまあ簡単にできた」という意見であった。

一方、「できない」と回答した 2 人から、以下の意見があった。

- 文字、画面、入力スペースが小さい
- 手が震えるため、ボタンの方がよい

図 3-39 タッチパネル血圧や体重等の入力

④操作した際の反応速度、動作間隔について

操作した際の反応速度、動作間隔に関する操作性についてのヒアリング結果は、以下となる。

【結果】モバイルアクセスシステムの反応速度、動作間隔に関する操作性をヒアリングした結果、ヒアリング対象者 11 人中 7 人が「気にならなかった」または、「ほとんど気にならなかった」という意見であった。

一方、「気になった」「少し気になった」と回答した 4 人から、以下の意見があった。

- そもそもテキパキ操作できない
- そもそもどこを押して良いのかわからない
- 入力した後の画面遷移が遅い
- 直ぐに画面が暗くなる（端末の設定の問題）

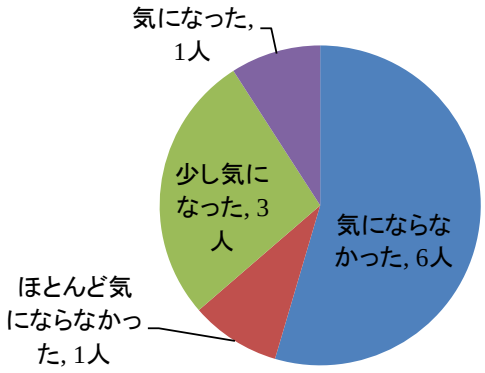


図 3-40 操作した際の反応速度、動作間隔

⑤今回、デモンストレーションしたサービスが実現したとの利用意向について

デモンストレーションしたサービスが実現したときには、利用意向についてのヒア

リング結果は、以下となる。

【結果】デモンストレーションしたサービスの利用意向に関するヒアリング結果は、ヒアリング対象者 11 人中 8 人が「使ってみたい」という意見であった。
一方、「使いたきない」と回答した 2 人から、以下の意見があった。

- スマートフォンにしないでほしい
- 操作が難しい。一人で操作できない

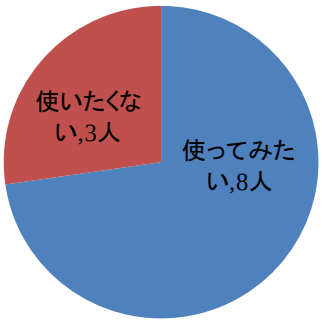


図 3-41 デモンストレーションしたサービスの利用意向

⑥今回のデモンストレーションを通じて、スマートフォンで実現してほしい行政サービスについて

スマートフォンで実現してほしい行政サービスについてのヒアリング結果は、以下となる。

【結果】もっとも実現してほしいサービスとして、「診察履歴や処方箋の確認」で次いで「健診・イベントの予約」となった。それ以外に以下のサービスを実現してほしいという意見であった。

- 役所等からの案内（郵送）をスマートフォンに集約してほしい
- 税金の支払い、買い物
- 自分の位置を家族等に知らせる
- 緊急時の連絡サービス
- 自治体、病院、周辺の方に不調を伝える緊急速報

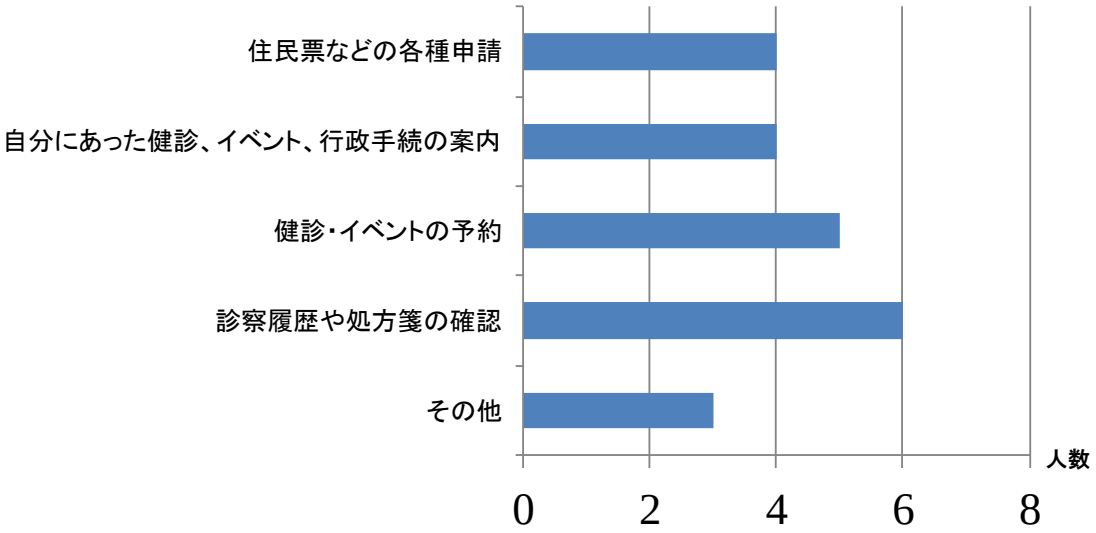


図 3-42 スマートフォンで実現してほしい行政サービス（複数回答可）

3.5.3.4. 自治体職員（浦添市）へのヒアリング結果

図 3-26 のヒアリングシートに基づき、サービスを提供する側の自治体職員にヒアリングを行った。以下にヒアリングの結果を示す。

(1) 生きいきチェックリスト（日常生活の行動、食生活など）の記録と送付に対する地域ポイント付与の運用性について

【結果】サービスの有効性についてヒアリングした結果、ヒアリング対象者 4 人いずれも業務の効率化になるという意見であった。主な理由は以下であった。

- 紙を回収し、パソコンの専用ソフトに入力する作業が不要になる
- 郵送費の負担が軽減される
- 電子化することでチェックリストの回収率が上がる

(2) 住民票等の発行手続きの電子化に対する運用性について

【結果】サービスの有効性についてヒアリングした結果、ヒアリング対象者 4 人中 3 人については業務の効率化になるという意見であった（4 人中 1 人は業務を担当していないため意見を頂けていない)。主な理由は以下であった。

- 混雑の緩和につながる
- 窓口での用紙への記入方法などの説明員が必要なくなる

(3) 住民登録等の申請手続きの電子化に対する運用性について

【結果】サービスの有効性についてヒアリングした結果、ヒアリング対象者 4 人中 3 人については業務の効率化になるという意見であった（4 人中 1 人は業務を担当していないため意見を頂けていない)。主な理由は以下であった。

- 窓口での用紙への記入方法などの説明員が必要なくなる

(4) 公金収納の電子化に対する運用性について

【結果】サービスの有効性についてヒアリングした結果、ヒアリング対象者 4 人中 2 人については業務の効率化になるという意見であった（4 人中 2 人については業務を担当していないので意見を頂けていない)。主な理由は以下であった。

- 督促が容易である

(5) 携帯電話端末（スマートフォン）で電子行政サービスを提供する際に重視する点について

【結果】携帯電話端末で電子行政サービスを提供する際に重視する点についてヒアリングした結果、ヒアリング対象者４人のほとんだから利用者の利便性の向上と業務効率化という意見であった。

(6) 携帯電話端末（スマートフォン）で電子行政サービスを提供する際の課題について

【結果】携帯電話端末で電子行政サービスを提供する際の課題についてヒアリングした結果、ヒアリング対象者４人から以下の意見があった。

- 字が小さく、言葉（ログイン、パスワードなど）がわかり難い。ソフトキーが押しにくい
- スマートフォンのみだと利用者が限られる
- 個人情報の取扱いが気になる
- 書く作業が減ったり外出が減ったりすることにつながり、脳に良くないのではないかと心配
- 広め方（利用者獲得）が難しそう
- スマートフォンに機種変更した際の料金増が心配

(7) モバイルアクセスシステム（スマートフォン）による自治体提供サービスの有効性について（複数回答可）

モバイルアクセスシステム（スマートフォン）を活用し、自治体サービスを提供する際に有効だと思うかについてヒアリングした結果、ヒアリング対象者４人いずれも有効だという意見であった。主な理由は図 3-43 の通りであった。

一方、モバイルアクセスシステムを活用する上で、想定される課題について目の悪い人には使い難い、実際は利用するための説明会の実施や、利用に関する問い合わせが予想されるという意見であった。

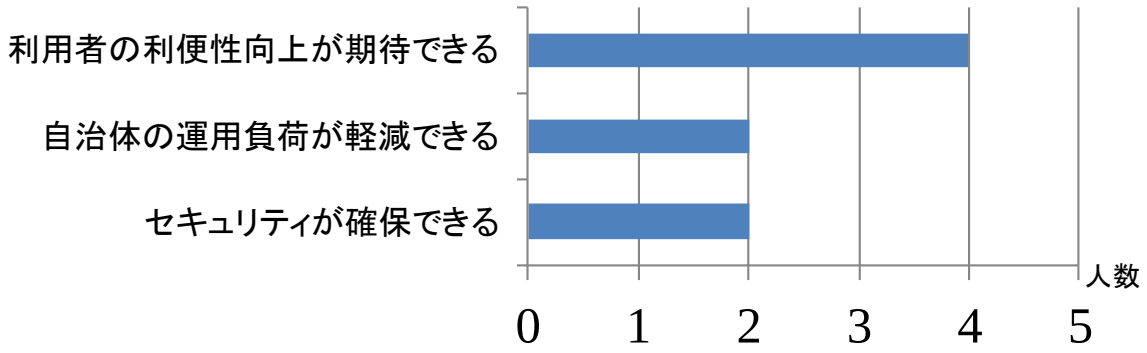


図 3-43 自治体におけるモバイルアクセスシステムの有効性

(8) その他の意見

サービス全体に関わる懸念事項として以下のコメントがあった。

- 本サービスの対象者には、最初に操作性についてマンツーマンでの説明が必要。説明書や説明会だけでは不十分。また、利用者を広めるためには、高齢者に操作を教えることが出来る若い利用者を増やすことも大切。そうしないと、サービスが広まらない。
- 問合せ窓口は必須であり、問合せが増加することが懸念される。
- サービスが実現したら使いたいとは思うが、値段との兼ね合い。スマートフォンは高いと聞くが、私１人だけがスマートフォンに変えるのは、家族に申し訳なくてできない。変えるとすると、家族まとめてとなるが、そうなると家計に響くので難しい。そのあたりもサービス普及の足かせになりかねない。
- セキュリティ面の確保が心配。利用する際に、セキュリティ対策について、しっかりとした説明が欲しい。「説明書に書いている」のような対応は困る。事例も交えて、教えて欲しい。
- 携帯電話端末にポイントを入れるとなると、お金が入っているようなものなので、今まで以上に端末の扱いを大切にしなくてはいけない。利用にあたっては、注意が必要である。

3.5.3.5. 民間サービス（観光分野）に関するヒアリング

本節では、スマートフォンによる民間提供サービスの有効性を確認するため、利用者にサービスを提供するサービス事業者にヒアリングを実施した。その結果を示す。

(1) 実施概要

①目的

モバイルアクセスシステムの民間活用に関して、民間のサービス事業者の意見を収集し、モバイルアクセスシステムの運用性、利便性を検証する。

②概要

モバイルアクセスシステムの運用性、有効性を確認するため、以下の通り、沖縄県の観光関連の民間サービス事業者にヒアリングを実施した。

- 株式会社エー･イー･シー
  - 日時
    2012 年 2 月 16 日（木）9:00－10:30

- 株式会社カヌチャリゾート及びニッポンレンタカー沖縄株式会社
  - 日時
    2012 年 2 月 16 日（木）11:00－12:00

(2) 実施内容

以下のモバイルアクセスシステムを活用した民間提供サービスの概要を説明後、ヒアリング等を実施した。

①モバイルアクセスシステムを活用した地域活性化及び販促サービス

モバイルアクセスシステムを活用した民間提供サービスとして、観光による地域活性及び販促サービスの説明を実施した。具体的には、以下のサービス内容である。

- 低価格な IC タグをタクシー、レンタカー、宣伝ポスター、充電器、観光地の看板、コンシェルジュのネームプレート、レストラン等のテーブルに設置。利用者は、IC タグに携帯電話端末をかざすことで、非接触通信（NFC 等）による観光・ショッピング情報（地図等）や割引クーポンを取得する。
- 利用者は、例えば、取得した地図情報に基づき、携帯電話端末の GPS 機能を使い、観光・ショッピングにでかけ、でかけた先の店舗の端末に携帯電話端末をかざすことで割引が受けられる。

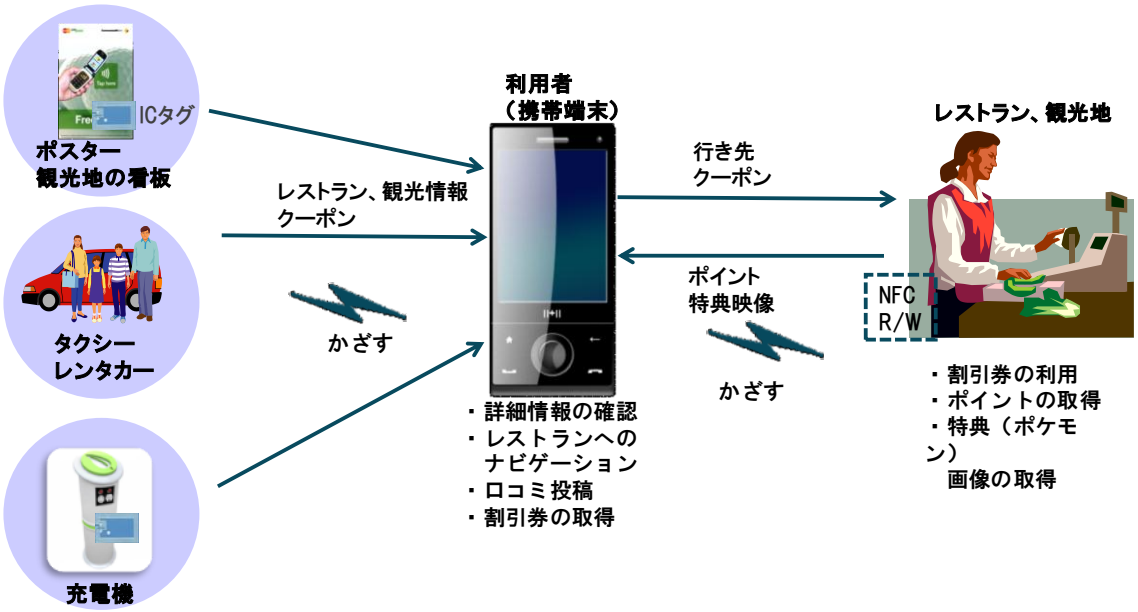


図 3-44 地域活性化及び販促サービスイメージ

②コンシェルジュ、レンタカー窓口等による観光案内サービス

モバイルアクセスシステムを活用した想定される民間提供サービスとして、ホテルのコンシェルジュやレンタカーの窓口等による観光案内サービスの説明を実施した。具体的には、以下のサービス内容である。

- コンシェルジュは、例えば、宿泊者からの「この近くにおすすめのレストランありませんか」等の質問を受けた際に、タブレット端末でおすすめのレストランを検索し、紹介する。 利用者は、気に入ったレストランがあった場合は、利用者の携帯電話端末をタブレット端末にかざすことで、非接触通信によるレストラン情報（地図、連絡先等）を取得する。
- 利用者は、携帯電話端末のナビケーション機能を使い、目的地に向かうことや、車で移動する際は、携帯電話端末をカーナビにかざすことで、地図情報をカーナビに非接触通信で送信する。

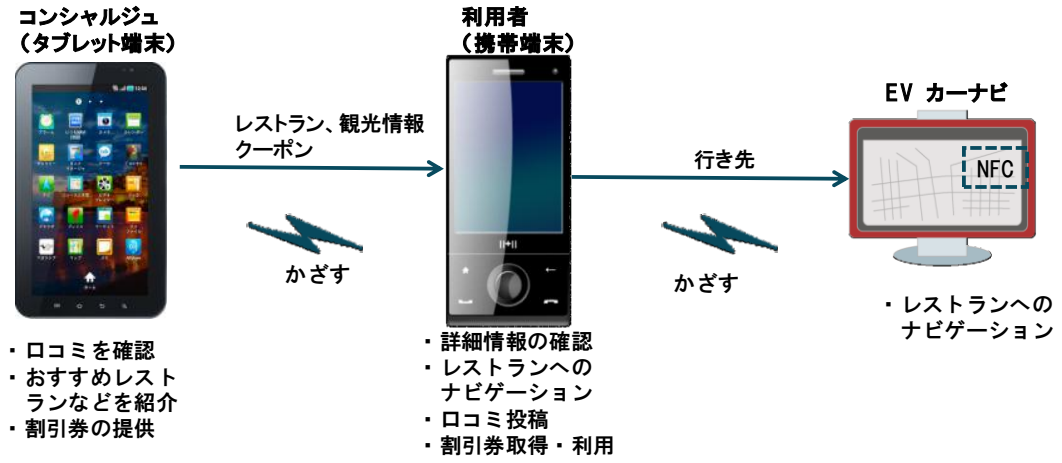


図 3-45 コンシェルジュ、レンタカー窓口等による観光案内サービスイメージ

(3) ヒアリング結果

①スマートフォンを活用したクーポンの取得・利用

現在、ある企業が電気自動車（EV）とタブレット端末を連動させ、沖縄県内で開催される“プロ野球沖縄春季キャンプ”の期間中、球団別最新キャンプ情報の配信、期間限定キャンプ情報番組を配信している。

GPS を使い、例えば施設、店舗に近づくとポップアップで画面に施設、店舗情報が表示され、クーポンの取得を可能とし、その施設、店舗に行くことで割引を受けられるサービスができるのではないかと思っている。

また、NFC を使うことで、クーポンの利用実績も取れるのでよい。

②電気自動車の充電スタンドでの支払い

充電スタンドに大掛かりな決済端末が無くても、NFC 対応携帯電話端末を使って簡単に決済することもできるのではないかと思っている。

③たくさんのカードを一台のスマートフォンで管理

行政カード以外にキュッシュカード、クレジットカード、ポイントカードなど多くのカードを持っているがスマートフォン一台で管理できるようになれば、楽だし、便利だと思う。

④免許証のスマートフォンへの格納

スマートフォンに免許証情報を格納できないか。予約は、スマートフォンで行いコンビニ等で借りられれば、便利だし、コスト低減になるのではないか。

ただし、レンタカーを借りるときは、窓口で免許証の確認が義務付けられているようなので確認が必要となる。

3.5.3.6. ヒアリング結果による考察

(1) モバイルアクセスシステムを活用した自治体提供サービス内容の有効性について

①高齢者向け支援サービスついて

今回、浦添市、台東区のシニアの方々にヒアリングを実施した結果、地域特性がみられた。例えば、台東区のシニアの方は日常の健康状況の把握は近所のかかりつけ医が行っているケースが多かった。一方、浦添市民は、浦添市役所がその役割をある程度になっている。そのため、浦添市民の方が日常から生活状況や健康状況をスマートフォンにて登録するサービス等に関して、関心が高かった。

スマートフォンによる高齢者向け支援サービス等を検討する際は、地域特性等を考慮する必要がある。

②行政手続の電子化について

行政の申請手続きの際に窓口に出向く必要がなく、待たされないサービスであれば、利用意向は高い。例えば、スマートフォンで事前申請し、近所のコンビニでそのまま受け取れる仕組みが構築されれば、利用される可能性が非常に高いと想定される。

(2) スマートフォンのユーザビリティについて

シニアの方々のほとんどがスマートフォンの操作は、はじめての経験となったが説明しながら、操作することで8割の人が利用できた。近い将来、スマートフォンがシニアケータイになる可能性を感じた。

一方、携帯電話端末からのインターネットアクセスに慣れていないことから、「どこを押せばよいか分からない」、「文字が小さい」等の意見が多くあった。シニアでも容易に操作が可能な画面デザインを考慮する必要がある。

また、ブラウザ連携する共通アプリを使うことで反応速度、動作間隔に心配はあったが画面遷移が遅いとの指摘は一人に留まり、利用上の支障はないと想定される。

(3) 自治体職員（浦添市）へのヒアリングについて

浦添市の職員からは、スマートフォン導入により、利用者の利便性、業務効率化が期待されるが一方で使い方を教える説明会の開催や問い合わせが増加することを懸念していた。導入の際は、ボランティア等の連携による支援体制の構築が重要である。

(4) 民間サービス（観光分野）での利用について

観光分野による地域活性化の効果として、ＮＦＣ機能等を活用することで、人と

人との連携やリアルとサイバーの連携が簡単にできるようになる。NFC 機能と組み合わせることでモバイルアクセスシステムの有効性を高めることが確認できた。

3.6. まとめ

課題イでは、課題アで検討した、モバイルアクセスサーバ、携帯電話端末内の共通アプリを基盤として用いて、そのうえで動く仮想的なサービス提供機関および仮想的な IC カードアプリケーションを開発した。そして、開発したシステムを用いて、実証実験を行った。実証実験の結果として、機能評価、性能評価、ヒアリング評価を行った。機能評価により、課題アで検討したシステムが、適切に機能していることを確認できた。さらに、性能評価では、2 種類の携帯電話端末を使ったシステムの動作について性能測定を実施し、約 6 秒という時間で、ID 情報の書込み、およびポイント情報の書き込みが行えることを確認した。さらに、ヒアリング評価では利用者及びサービス提供機関にヒアリングを実施し、モバイルアクセスシステムの運用性、有効性を確認できた。また、導入にあたっては、利用者への支援体制が重要であることや、NFC 等の非接触でのローカル通信を活用することでさらに、利便性の向上ができることが確認できた。

表 3-13 に応募資格に対する本成果報告書の対応個所を示す。

表 3-13　応募資格に対する本成果報告書の対応個所

	実施要領に記載される要件	参照先	対応内容
課題イ	課題アの検討結果に基づき、実験環境を構築し、サービス提供機関・利用者双方の観点での運用性、利便性の検証ならびに、技術的検証を行う。	3.5	3.5 節で示したように、課題アで検討した技術仕様にもとづき、十分な機能を備えているかの評価を行った。また、実験環境において、サービス提供機関、及び利用者双方の観点で、ユーザビリティを検証した。また、移動体通信事業者などに対し、実証環境でデモを実施し、実サービス時の業務・運用を想定し、現行の業務･運用と対比することで運用負荷、経済性などの有効性の検証を行った。
		3.5	3.5 節で示したように、移動体通信事業者、サービス提供 ･関の協力を得て ･実際に実サービス時を想定した際の運用負荷、経済性などの有効性の検証を行った。

4. 課題ウ　制度・運用面の課題の検討

4.1. 概要

4.1.1.　背景と目的

政府の IT 戦略に示された「国民本位の電子行政」の実現手段の一つとして、電子自治体サービスへのアクセス手段の多様化により、より使いやすい電子行政へのアクセスが検討されている。

アクセス手段としては、これまでのパソコン中心から携帯電話やデジタルテレビなどの日常個人が利用する端末へ範囲を拡大することが期待される。

しかし、行政の情報や医療の情報、金融機関の情報などの個人情報保護の観点からセキュリティレベルの高いものと、民間で保有している情報などの比較的セキュリティレベルが低いものとがあり、それぞれの情報へのアクセスに対するセキュリティ対策（本人認証のレベル）も異なり、最適な対策が望まれている。

本検討では、利便性を重視しつつ、情報の機微度に応じたセキュリティレベル（本人認証のレベル）を確保したアクセス手段について、携帯電話端末での活用を前提に具体的なサービスを抽出し、モバイルアクセスシステムを導入した際の認証等セキュリティ対策やサービスに対する運用の課題、情報のアクセスや活用に対する制度面の課題などを抽出し、課題に対する対策を明らかにすることを目的とする。

4.1.2.　検討の進め方

制度・運用面の課題の検討に当たっては、まず、検討対象となる適用サービスを洗い出し、洗い出されたサービスに求められるセキュリティレベル等の検討後、ヒアリング結果を基に最適なサービスを選定し、選定した最適なサービスに対して課題と対策の検討を行う。以下、検討の進め方の概要を示す。

(1) 適用サービスの洗い出し

① 行政、医療、健康、福祉、金融分野のカテゴリ別にサービス案を検討し、サービス提供機関へのヒアリングを行って、適用サービスを洗い出す。

② 洗い出したサービスから想定されるサービス案を策定し、効果、有効性の観点からサービスの絞り込みを行う。

③ 絞り込んだサービスの概要（ユースケース）を検討する。

(2) セキュリティレベル等の検討

① （1）で整理した適用サービスの取扱う情報を基に、各サービスに対するセキュリティレベル要件を整理する。

② 適用サービスに対する認証のレベルについて、各種ガイドラインを参考に検討する。その際、取扱情報と認証レベルを 4 段階に分類し、マッピングする。

(3) 最適なサービスの選定

① 適用サービスに対するヒアリングを実施し、セキュリティレベル、制度、環境、政策動向等のコメントと実現評価を実施する。

② （1）の適用サービス概要からユースケースをヒアリングにより具体化し、業務フローとして整理する。

③ サービスに対する現行の政策課題、制度課題、運用課題をヒアリングにより具体化する。

(4) 最適なサービスの課題と対策の検討

最適サービスについて、実現フローにおける実現課題を抽出し、対応策を検討する。

4.2. 適用サービスの洗い出し

4.2.1.　適用サービスの検討の考え方

制度・運用面の課題の検討の対象となる適用サービスの洗い出しを行う。

サービスの洗い出しは、行政、医療、健康、福祉、金融などのサービス領域（カテゴリ）から、カテゴリ別に既存サービスの高度化の観点から適用サービス（案）を想定サービスとして検討する。

検討した想定サービス（案）は、サービス提供機関へのヒアリングを基に、制度・運用面の課題の検討対象として適切かどうかの評価を行い、モバイルアクセスシステムにおける適用サービスとして絞り込みを行う。

4.2.2.　想定サービス概要

行政、医療、健康、福祉、金融分野のサービス領域から想定サービスを検討するに当たり、携帯電話の活用性や利用者、サービス提供機関の観点から、次のような方針を立て、この方針に基づいてサービス（ユースケース）案を検討した。

＜サービス選定のための基本方針＞

① アクセス手段として、携帯電話（スマートフォン）を活用できるサービスを選定
② 利用者個人が活用しつつ、情報に対するアクセスの際に本人確認（認証）が必要なサービスを選定
③ 利用者にとって利便性や効果の高いサービスを選定
④ サービス提供機関が保有する利用者の情報を活用したサービスを選定
⑤ サービス提供機関が抱える課題の解決につながると想定されるサービスを選定

行政、医療、健康、福祉、金融分野のサービス領域（カテゴリ別）に、基本方針に基づき、8 件のサービス（ユースケース）を洗い出した。

洗い出したサービスの概要と利用者、サービス提供者に対する想定効果を表 4-1 に示す。また、洗い出したサービス（ユースケース）のサービスの概要を図 4-1～ 図 4-8 に示す。

表 4-1 想定サービス一覧

項番	分野カテゴリ	ユースケース概要	想定効果	
			利用者	サービス提供者
①	医療・健康	● 健康情報の記録と管理、健康維持のための地域通貨（ポイント）活用 ※国保加入者向けに自治体が有する健診情報とレセプト情報を開示し、健康度に応じてポイントを付与 ※民間のフィットネスクラブでの運動履歴や歩数履歴などの情報を加入者向けに開示し特定健診結果の判定により、健康増進度に応じたポイント付与	簡易な自己管理 健康意欲向上	健康増進
②	福祉	● 高齢者向け支援サービス（介護予防等）向上のための地域通貨（ポイント）活用	安心安全な見守 健康意欲向上	健康増進
③	福祉	● 介護者向けに介護事業者が提供する各種サービス（介護用品、介護タクシーなど）の予約、申請	介護サービスの充実	業務効率化
④	地域活性化・観光	● 観光情報や地域情報の発信などによる地域通貨（ポイント）活用	情報価値の向上	地域産業活性化
⑤	行政	● スマートフォンでの公的カードの一元化 ● 住民票・戸籍・税関係証明等の発行手続き ● 住民登録・印鑑登録・戸籍などの届け	待ち時間解消	円滑な窓口業務
⑥	行政	● 税金・保険料・年金保険料等の支払い	時間・場所の制約解消	業務コスト削減 収納率向上
⑦	金融	● 国保加入者向けに自治体が保有するレセプト情報等を元に既往歴等の情報を開示し保険加入時の告知や申請に活用	健診情報等の提出削減	業務コスト削減
⑧	金融	● 保険契約情報を閲覧、保険加入の申請、事故情報の申告に活用	時間・場所・書類の制約解消	業務コスト削減

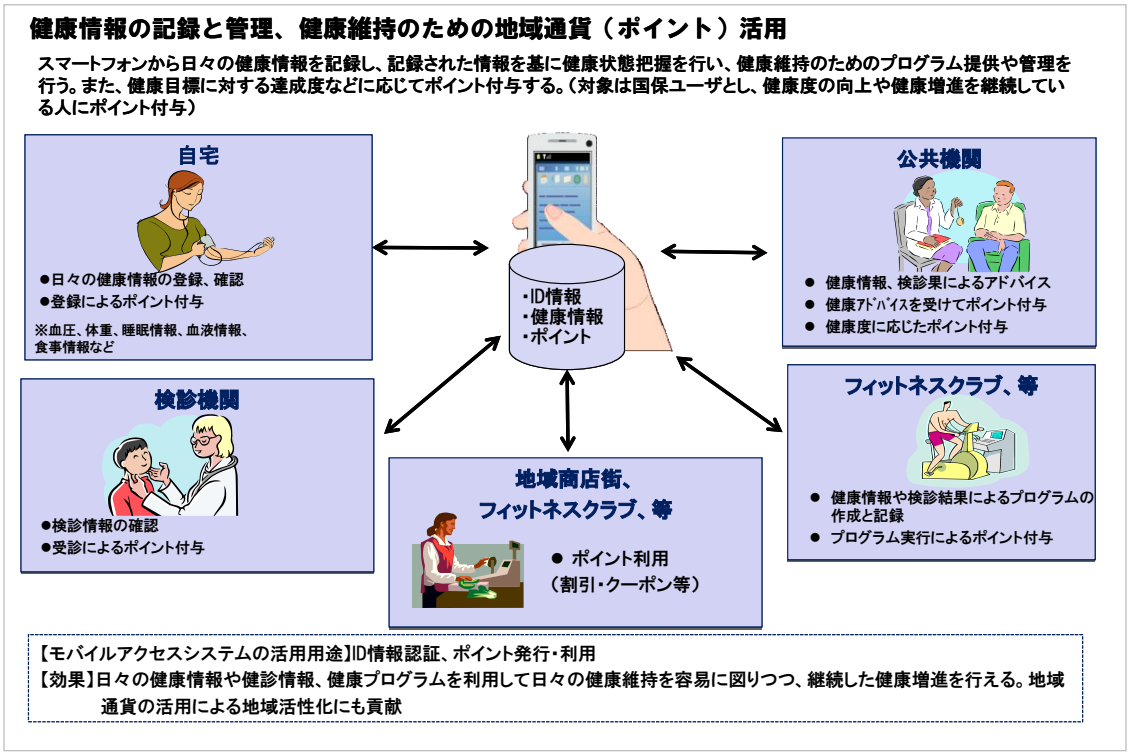


図 4-1　健康情報の記録と管理、健康維持のための
地域通貨（ポイント）活用（医療・健康）

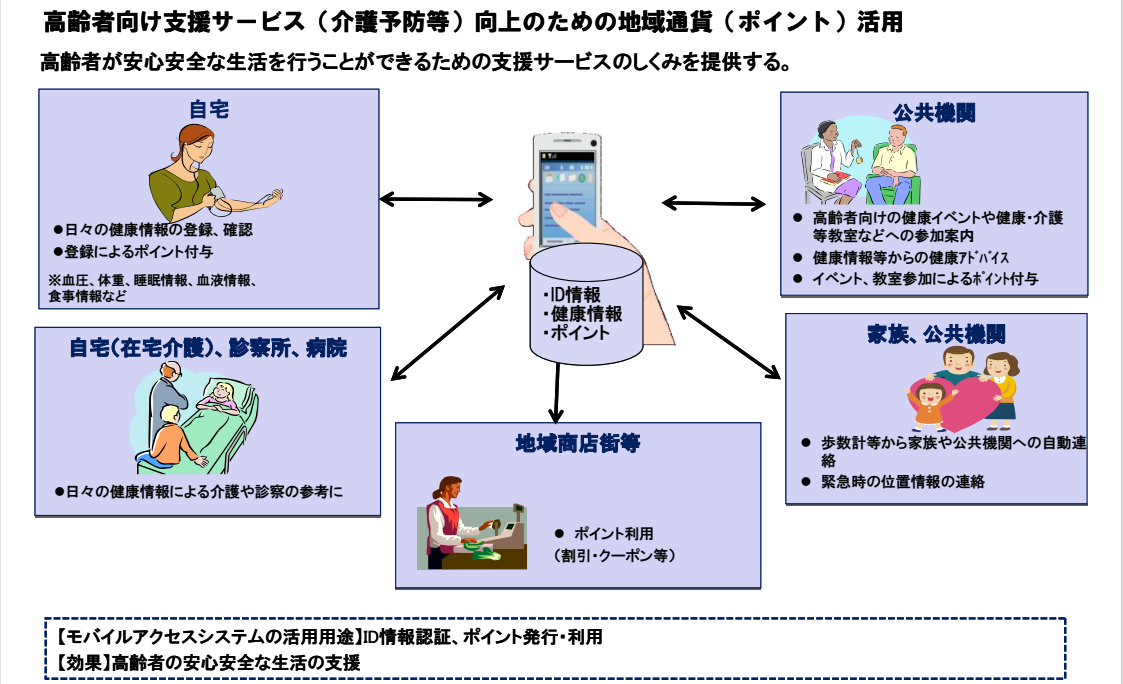
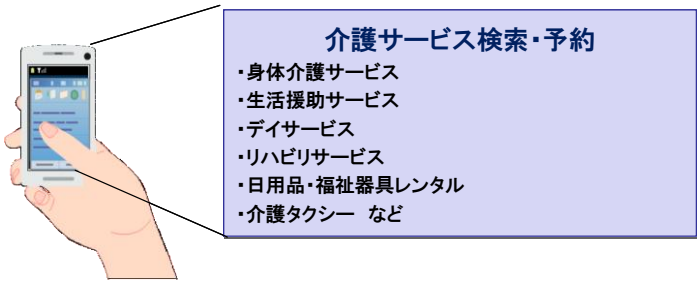


図 4-2　高齢者向け支援サービス（介護予防等）向上のための
地域通貨（ポイント）活用（福祉）

介護者向け介護事業者が提供する各種サービス(介護用品、介護タクシー等)の予約、申請
いつでもどこでも介護サービスの利用が行えることで、介護サービスの向上を図る。

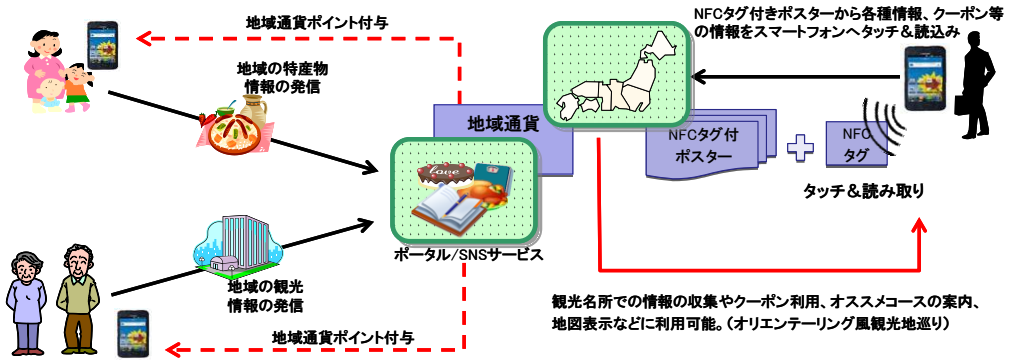


【モバイルアクセスシステムの活用用途】ID情報認証
【効果】
・利用者のニーズに即したタイムリーな介護サービスの提供と介護サービスの品質・サービス拡大
・介護サービスの的確な提供(サービス提供誤りなどの防止)

図 4-3　介護者向け介護事業者が提供する各種サービス（介護用品、介護タクシー等）の予約、申請（福祉）

観光情報や地域情報の発信などによる地域通貨（ポイント）活用

・観光客や住民に対してポスターなどから観光情報等をスマートフォンで読込みと同時にポイントを付与する。
・地域の特産物の紹介や観光名所等をSNSやポータルを利用して情報発信した住民へのインセンティブとしてポイントを付与する。

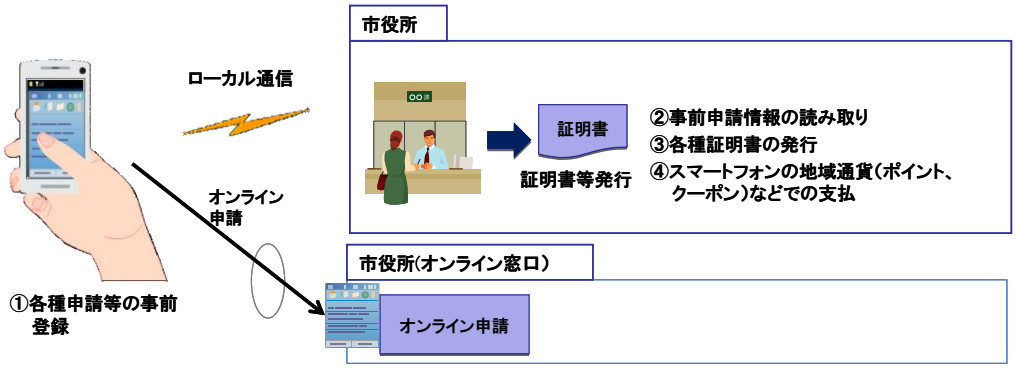


【モバイルアクセスシステムの活用用途】ID情報認証、ポイント発行・利用
【効果】
・利用者は、必要情報をタッチするだけで収集でき、スマートフォン上(Web、地図など)で活用できると同時に付与されるポイントを商品購入等に利用できる。
・地元住民からの発信する情報にポイントを付与することで、住民参加型の情報発信モデルとして、観光客の集客とともに、地元の地域活性化につながる可能性がある。

図 4-4　観光情報や地域情報の発信などによる地域通貨（ポイント）活用（地域活性化・観光）

スマートフォンでの各種申請の事前手続き

・スマートフォン上で、あらかじめ住民票の写し、戸籍、税関係の証明書等の事前申請手続きを行う
・スマートフォン上で住民票・戸籍・税関係証明書等の届出情報を事前登録を行う

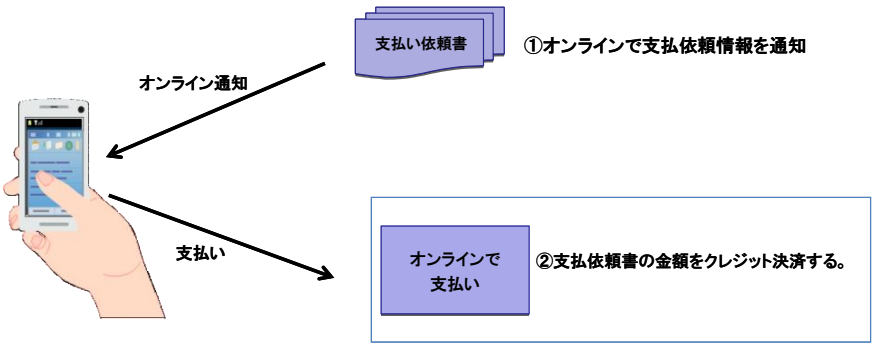


【モバイルアクセスシステムの活用用途】ID情報認証
【効果】
・各種手続きの簡略化。スマートフォン上で申請登録を行うことで、窓口での処理を短縮化することができる。支払いも地域通貨等により迅速に処理できる。
・効果：利用者の利便性向上(時間や場所にとらわれないサービス利用)、円滑な市役所(窓口)業務

図 4-5　スマートフォンでの公的カードの一元化、
住民票・戸籍・税関係証明等の発行手続き（行政）

税金・保険料・年金保険料等の支払い

税金・保険料・年金保険料等の支払いの簡略化。支払い依頼情報をスマートフォンにオンラインで通知し、オンラインで支払を行う。



【モバイルアクセスシステムの活用用途】ID情報認証
【効果】
・利用者の利便性向上(時間や場所にとらわれない支払いや支払通知書紛失防止)
・市役所業務のコスト削減(支払通知や督促コストの削減)、徴収率の向上

図 4-6　税金・保険料・年金保険料等の支払い（行政）

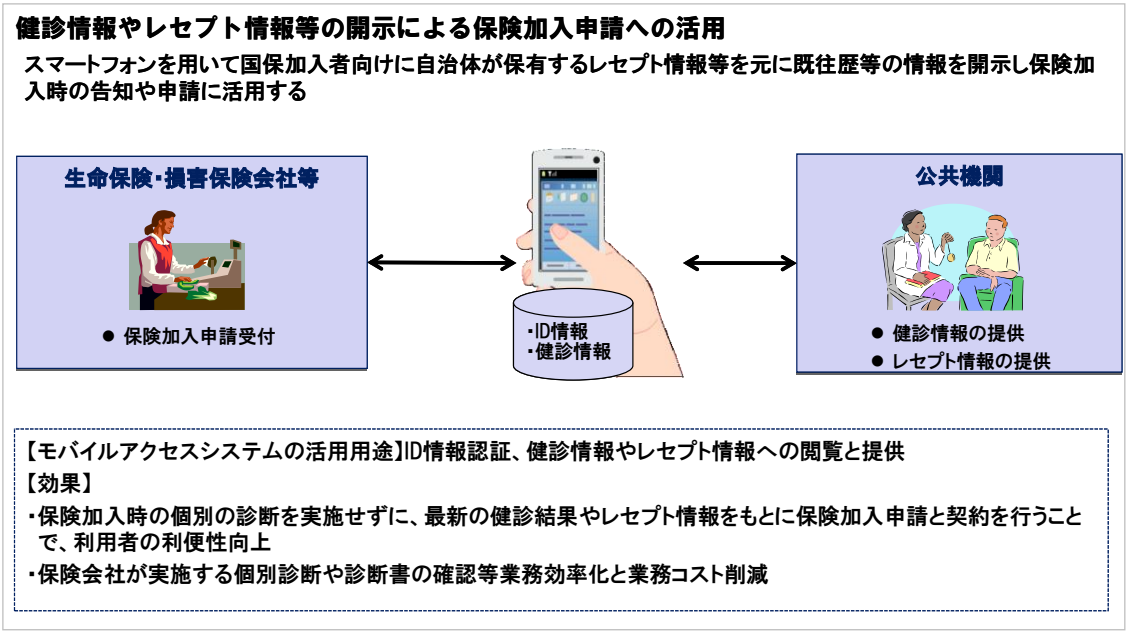


図 4-7　保険加入申請への活用（金融）

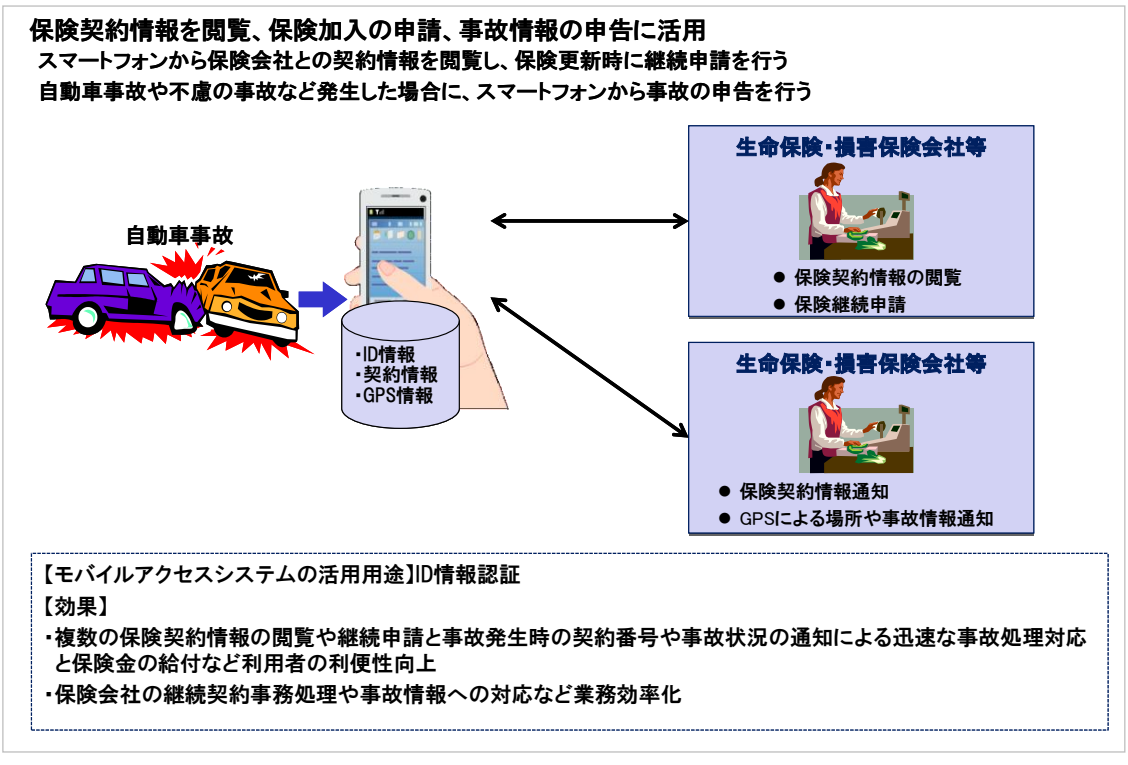


図 4-8　保険契約情報の閲覧（金融）

4.2.3.　適用サービスの洗い出しにおけるヒアリング結果と絞り込み

4.2.2 節で検討したサービス（案）をサービス提供機関の視点からサービスの効果や有効性を評価し、制度・運用面の課題の検討対象サービスとして絞り込みを行う。

サービスの効果や有効性を評価するため、サービス提供機関に対するヒアリングを実施し、その結果を基に、サービス提供機関が協力可能な対象範囲のサービスに対して、サービス提供機関の課題解決、検討の具体性、利用者の利便性の観点（検討対象サービスの選定に当たっての観点）から、効果や有効性が高いサービスを選定する。

検討対象サービスの選定に当たっての観点を以下に示す。

＜検討対象サービスの選定に当たっての観点＞

① サービス提供機関が解決すべき課題であること

② サービス提供機関が実現に向けた検討を具体化できること

③ サービス提供機関として利用者の利便性の向上が図れること

表 4-1 に示す先に洗い出した 8 件のサービス（ユースケース）に対し、サービス提供機関のヒアリングを実施した。ヒアリングによる主なコメントと総合判断の結果を表 4-2 に示す。

各サービス（ユースケース）を上記の選定に当たっての観点から評価し、福祉、行政、金融の各分野から計 4 件のサービスを適用サービスとして絞り込んだ。絞り込んだ適用サービスを以下に示す。

なお、以降の検討では、下記に示すサービス名を用いる。

＜選定した適用サービス＞

- （福祉：項番②）サービス 1：高齢者向け支援サービス
- （行政：項番⑤）サービス 2：行政手続きの申請手段の電子化サービス
  （スマートフォンでの公的カードの一元化と住民票・戸籍・税関係証明等の発行手続き、住民登録・印鑑登録・戸籍などの届け）
- （行政：項番⑥）サービス 3：公金収納の電子化サービス
  （税金・保険料・年金保険料等の支払い）
- （金融：項番⑧）サービス 4：保険契約情報の閲覧、保険加入の申請、事故情報の申告

なお、今回のヒアリング対象として、表 4-2 のうちサービス①～⑥は自治体（浦添市企画部情報政策課、企画課、健康部地域支援課）、⑦・⑧は損害保険会社（株式会社損害保険ジャパン）にご協力いただいた。

表 4-2　検討対象サービス一覧

項番	カテゴリ	ユースケース概要	サービス提供機関ヒアリング結果	
			主なコメント	総合
①	医療･健康	● 健康情報の記録と管理、健康維持のための地域通貨（ポイント）活用	※成人病対策など健康増進への取組みに有効であるが医療は自治体が持っている情報と民間の医療機関との連携等の兼ね合いもあるため、福祉分野に注力する。	－
②	福祉	● 高齢者向け支援サービス（予防介護等）向上のための地域通貨（ポイント）活用	（１）介護予防対策やボランティア参加者増加などに有効 （２）実現に向けて具体的に検討実施可能だが、介護事業者サービスは対象外（経済産業省の高齢者介護見守り事業にて検討） （３）高齢者 70 歳以上の操作性が懸念	検討対象
③	福祉	● 介護者向けに介護事業者が提供する各種サービス(介護用品、介護タクシーなど）の予約、申請	※課題というより利便性向上が中心 ※介護事業者サービスは対象外（経済産業省の高齢者介護見守り事業にて検討）	－
④	地域活性化･観光	● 観光情報や地域情報の発信などによる地域通貨（ポイント）活用	※観光は評価指標の具体的な検討が困難なため、今回は対象外	－
⑤	行政	● スマートフォンでの公的カードの一元化 ● 住民票・戸籍・税関係証明等の発行手続き ● 住民登録・印鑑登録・戸籍などの届け	（１）繁忙時業務効率化に有効 （２）税などは検討が困難（問合せも含まれるため）　⑤と⑥は合わせて申請書での活用で検討 （３）繁忙時の待ち時間削減に有効	検討対象
⑥	行政	● 税金・保険料・年金保険料等の支払い	（１）収納率向上やコスト削減に有効 （２）他自治体の取組の踏まえ将来的に検討 （３）時間や場所の制約撤廃に効果	検討対象
⑦	金融	● 国保加入者向けに自治体が保有するレセプト情報等を元に既往歴等の情報を開示し保険加入時の告知や申請に活用	※実現ハードル（制度等）が高く、官民の連携した検討が必要であり検討困難	－
⑧	金融	● 保険契約情報を閲覧、保険加入の申請、事故情報の申告に活用	（１）事故処理の迅速化、効率化に有効 （２）実現に向けて具体的な検討実施可能	検討対象

4.2.4. まとめ

電子自治体サービスを利用するに当たってのアクセス手段の多様化検討を行うに当たっての対象サービスを行政、医療、健康、福祉、金融の各サービス分野から、携帯電話端末の活用性や本人認証の必要性、利用者にとっての利便性とサービス提供機関の保有する情報の活用の観点から、計8件の適用サービスを洗い出した。

洗い出した適用サービスは、サービス提供機関から、ヒアリングを行い、その結果を基に、サービス提供機関の解決すべき課題であることやサービス提供機関が実現に向けた検討の具体化ができること、サービス提供機関として利用者の利便性の向上が図れることの3項目の観点から評価し、検討対象サービスとして福祉、行政、金融の各サービス分野から次に示す4件の適用サービスを選定した。

＜選定した適用サービス＞

- （福祉）サービス1：高齢者向け支援サービス（介護予防等）
- （行政）サービス2：行政手続きの申請手段の電子化
  （スマートフォンでの公的カードの一元化と住民票・戸籍・税関係証明等の発行手続き、住民登録・印鑑登録・戸籍などの届け）
- （行政）サービス3：公金収納の電子化
  （税金・保険料・年金保険料等の支払い）
- （金融）サービス4：保険契約情報の閲覧、保険加入の申請、事故情報の申告

4.3. セキュリティレベル等の検討

4.2 節で選定した適用サービスに対して必要となるセキュリティレベル（保証レベル）と認証方式についての要件を検討する。

検討対象サービスである、高齢者支援サービス、および、行政手続きの申請手段の電子化サービス、公金収納の電子化サービス、保険契約情報の閲覧、保険加入の申請、事故情報の申告サービスで取扱う情報を基に、リスク影響度の分析を行い、それぞれのサービスで必要となる認証レベルを検討し、4 段階ある認証レベルにマッピングを行う。

リスク影響度分析と認証レベルの検討に当たっては、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日)」（以下、「ガイドライン」という）を基に検討を進めた。検討に当たっての考え方や検討手順については、4.7 節に示す。

以下、各サービスでセキュリティの観点から必要となる保証レベルの検討結果を示す。なお、保証レベルの定義を表 4-3 に示す。

表 4-3 保証レベルの定義

保証レベル	レベル定義
レベル 4（かなり高い保証）	特定される身元識別情報の信用度が非常に高い
レベル 3（高い保証）	特定される身元識別情報の信用度が相当程度ある
レベル 2（中程度の保証）	特定される身元識別情報の信用度がある程度ある
レベル 1（低い保証）	特定される身元識別情報の信用度がほとんどない

（出典）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）

4.3.1. 選定した各適用サービスでの対応する保証レベル

適用サービスでの対応する保証レベルを以下に示す。

（1） 高齢者向け支援サービス（介護予防等）

高齢者向け支援サービス（介護予防等）は、健康状態の記録と管理、介護予防活動記録の統計分析への利用サービスとボランティア活動の継続的な促進サービスの 2 つのサービスからなる。

健康状態の記録と管理、介護予防活動記録の統計分析への利用サービスと保証レベルを表 4-4 に、ボランティア活動の継続的な促進サービスと保証レベルを表 4-5 に示す。

表 4-4　健康状態の記録と管理、介護予防活動記録の統計分析への利用に係る保証レベル

ユース ケース	取扱う情報	情報の 利用形態 (※)	保証 レベル
生活状況等の登録と閲覧、チェックリストの送信	氏名、住所、生年月日、性別、実施日、生活状況のチェック結果	・本体記録 ・ﾛｰｶﾙ通信 ・オンライン	レベル 3
健康状態の記録と閲覧	氏名、住所、生年月日、性別、バイタル情報（血圧、体重）の履歴	・本体記録	レベル 2
運動情報の登録と閲覧	氏名、住所、生年月日、性別、運動記録（歩行記録）や体力測定結果の履歴	・本体記録	レベル 2
介護予防プログラムへの参加記録と閲覧	氏名、住所、生年月日、性別、介護予防プログラムやボランティア活動の参加記録（日時、プログラム名、活動内容、活動結果、報告事項、指導内容等）	・本体記録	レベル 3
健康状態や介護予防プログラムの参加状況等の自治体への提供	氏名、住所、生年月日、性別、バイタル情報や運動記録や体力測定結果、介護予防プログラムやボランティア活動の参加記録（日時、プログラム名、活動内容、活動結果、報告事項、指導内容等）	・ﾛｰｶﾙ通信 ・オンライン	レベル 3
ポイントの付与	ポイント数	・本体記録 ・ﾛｰｶﾙ通信 ・オンライン	レベル 2

（※）取り扱う情報の利用形態を記載する。

本体記録・・・スマートフォン等の機器本体に情報を記録し取り扱うもの

ﾛｰｶﾙ通信・・・NFC 機能等を利用してローカルでのデータを送受信するもの

オンライン・・・ネットワークを通じてデータを送受信するもの

表 4-5　ボランティア活動の継続的な促進に係る保証レベル

ユース ケース	取扱う情報	情報の 利用形態	保証 レベル
ボランティア活動の実施記録と送信	氏名、住所、生年月日、性別、ボランティア活動の記録（日時、プログラム名、活動内容、活動結果、報告事項、実施確認、等）	・本体記録 ・ローカル通信 ・オンライン	レベル 3
一人暮らし高齢者の現況報告の記録と送信	氏名、住所、生年月日、性別、一人暮らし高齢者の現況報告内容（訪問先高齢者の氏名、住所、生年月日、性別、前回訪問時の状況、今回の訪問時の状況等）	・本体記録 ・オンライン	レベル 4
ポイントの付与	ポイント数	・本体記録 ・ローカル通信 ・オンライン	レベル 2

（2）　行政手続きの申請手段の電子化サービスと保証レベルを表 4-6 に示す。

表 4-6　行政手続きの申請手段の電子化に係る保証レベル

ユース ケース	取扱う情報	情報の 利用形態	保証 レベル
住民票等の交付申請情報の登録と交付申請	申請者の情報（氏名、住所、生年月日、性別、連絡先）、必要な人の情報（氏名、住所、生年月日、請求者との関係、使用目的）、必要な住民票の写しの種類と必要数	・本体記録 ・ローカル通信	レベル 2
住民票等の交付時のポイント利用	ポイント利用数	・ローカル通信	レベル 2
住民登録（転入届）等の申請情報の登録と申請	新住所と世帯主氏名、住み始めた日、今までの住所と世帯主氏名、転入者の生年月日と新世帯主との続柄、転入者の本籍と戸籍の筆頭者、申請者（住所、氏名、連絡先電話番号）	・本体記録 ・ローカル通信	レベル 3

（３） 公金収納の電子化

公金収納の電子化サービスと保証レベルを表 4-7 に示す。

表 4-7　公金収納の電子化に係る保証レベル

ユース ケース	取扱う情報	情報の 利用形態	保証 レベル
納付書の送付	氏名、住所、生年月日、納付情報（納付種目、金額、納付時期、納付金額の根拠の説明）	・メール	レベル 3
ホームページでの納付情報の閲覧	氏名、住所、生年月日、納付情報（納付種目、金額、納付時期、納付金額の根拠の説明）	・Web	レベル 3
納付情報支払い	氏名、住所、生年月日、納付情報（納付種目、金額、納付時期、納付金額の根拠の説明）	・Web	レベル 3

（４） 保険契約情報の閲覧、保険加入の申請、事故情報の申告

保険契約情報の閲覧、保険加入の申請、事故情報の申告サービスと保証レベルを表 4-8 に示す

表 4-8 保険契約情報の閲覧、保険加入の申請、事故情報の申告に係る保証レベル

ユース ケース	取扱う情報	情報の 利用形態	保証 レベル
複数の保険契約情報の名寄せ登録	契約者氏名、複数の他種目契約番号	・本体記録 ・Web	レベル 4
契約情報の閲覧権限付与	契約者氏名、契約番号、権限情報（閲覧、申請等） 運転者氏名（付与対象）、運転者年齢、続柄など	・ﾛｰｶﾙ通信 ・本体記録	レベル 3
事故発生時に契約情報を通知	契約者氏名、契約者住所、運転者氏名、運手者住所、運転者の続柄、契約情報（契約番号、車両番号、車種、登録番号、給付金額、給付種別など）、位置情報など	・本体記録 ・Web	レベル 3

4.3.2.　リスク評価に基づく認証方式

各サービスで取り扱う情報を基に、必要な保証レベルの検討を行った。その結果から、各サービスのリスク影響度分析により対応する保証レベルは、ユースケースにより異なるが、保証レベル 3、または、保証レベル４が必要となることがわかる。

保証レベル 3 は、“特定される身元識別情報の信用度が相当程度ある”と定義され、また、保証レベル４は、“特定される身元識別情報の信用度が非常に高い”と定義される。本サービスにおける、レベル 3、レベル４の対策基準を、「登録」、「発行・管理」、「トークン」の観点から整理結果を以下に示す。

ｉ）登録の対策基準

認証方式の「登録」における対策基準を表 4-9 に示す。

表 4-9　「登録」の対策基準

保証レベル	対策基準
レベル 4	重複登録でないことを確認する。（対面）
レベル 3	申請者の氏名や住所等の公的な台帳を照合または申請書に添付された公的証明書によりチェックする。（対面・遠隔）
	申請者の氏名と住所等が記載された申請書に本人の電子署名（郵送は署名、捺印）を付与して申請する。（遠隔）

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）を基に作成した。

ⅱ）発行・管理の対策基準

認証方式の「発行・管理」における対策基準を表 4-10 に示す。

表 4-10　「発行・管理」の対策基準

保証レベル	対策基準			
	発行	管理	更新/再発行	失効
レベル 4	認証情報及びトークンが窓口にて直接手渡される。 （本人限定受取郵便基本型等の手段による身元確認は対面）	レベル 3 と同等以上	レベル 3 と同等以上	レベル 3 と同等以上
レベル 3	認証情報及びトークンが以下のいずれかの方法により本人に送付される。 ・窓口にて直接手渡される ・本人住所に書留郵送または本人限定受取郵便により送付される。 ・本人住所に書留郵便または本人限定受取郵便にてパスワードが送付され、本人が当該パスワードによる認証の上で認証情報及びトークンをダウンロードする。 ・申請者が電子署名を付与した申請を行い、検証された上で認証情報及びトークンをダウンロードする。	検証者が使用する秘密情報はアクセス制御によって保護され、パスワードのような秘密情報を平分のまま含まない。	・認証情報及びトークンの更新、再発行に関する運用ポリシーが策定され周知されている。 ・上記同等以上の対策基準に加え特にオンラインによる手続の場合には、既存の認証情報及びトークンを用いた認証の上で通信を暗号化して行う。	認証情報及びトークンが有効でなくなった、または危殆化されたことを通知された時から認証情報及びトークンを延滞なく失効する。

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）を基に作成した。

ⅲ）トークンの対策種類

認証方式の「トークン」における対策種類と実現例を表 4-11 に示す。

表 4-11　「トークン」の対策種類と実現例

保証レベル	対策種類	実現例
レベル 4	耐タンパ性を有するパスワード付ハードウェアトークン	・IC カード、・USB
レベル 3	ソフトウェアトークンとパスワードなどの複数のトークンの組み合わせ	・パスワード付ソフトウェアワンタイムパスワード、・パスワード付ソフトウェア ・パスワード付ハードウェアワンタイムパスワード

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）を基に作成した。

4.3.3.　まとめ

適用サービスをスマートフォンで利用する際に必要とされるセキュリティ、特に認証方式の保証レベルについて検討を行った。

検討に当たっては、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）」（以下、「ガイドライン」という）に示されているガイドに従い、各サービス適用時に、スマートフォンで取り扱う情報からリスク評価レベルを分析し、その評価レベルからスマートフォン利用時に求められる保証レベルを分析した。

分析の結果、各々のサービスで取り扱う情報の利用ケースによって、レベル 2 からレベル 4 の保証レベルが必要となることが明らかになり、サービスによって、上位のレベル３、または、レベル 4 の保証をスマートフォン上で満たせば、すべての適用サービスのセキュリティ要求を満たすことが明確になった。

また、保証レベル 3 は、“特定される身元識別情報の信用度が相当程度ある”と定義され、保証レベル４は、“特定される身元識別情報の信用度が非常に高い”と定義される。レベル３、レベル 4 での具体的な対策基準を「登録」、「発行・管理」、「トークン」の観点から整理した。

＜保証レベル３＞

- 「登録」においては、対面・遠隔で、申請者の氏名や住所等の公的な台帳を照合または申請書に添付された公的証明書によりチェックすること
- 「発行・管理」においては、認証情報及びトークンが窓口にて直接手渡すことや、本人住所に書留郵送されること、など
- 「トークン」においては、ソフトウェアトークンとパスワードなどの複数のトークンの組み合わせを用いること

＜保証レベル４＞

- 「登録」においては、「対面」を基本とし、申請者の氏名や住所等の公的な台帳を照合または申請書に添付された公的証明書によりチェックすること、さらに重複登録がないこと
- 「発行・管理」においては、認証情報及びトークンが窓口にて直接手渡されること、など
- 「トークン」においては、IC カードや USB など耐タンパ性を有するパスワード付ハードウェアトークンを用いること

保証レベル４の「トークン」の要件を満たすためには、耐タンパデバイスの情報を読み書きできるモバイルアクセスシステムが必要となる。また、携帯電話端末（特に今回対象

としたスマートフォン）は、IC カードのインタフェースと SIM 領域に情報を格納することで、耐タンパ性を有するハードウェアトークンを有するため、保証レベル 4 を満たしていることが言える。

4.4. 最適なサービスの選定

4.4.1. 検討の考え方

4.2 節で検討した適用サービスについて、サービス提供機関からのヒアリングを実施し、セキュリティレベル、制度、環境、政策動向等のコメントと実現評価を実施する。

また、適用サービス概要からユースケースをヒアリングにより具体化し、業務フローとして整理するとともに、サービスに対する現行の政策課題、制度課題、運用課題をヒアリングにより具体化する。

検討対象とするサービスは以下の 4 サービスである。

- サービス 1：高齢者向け支援サービス
- サービス 2：行政手続の申請手段の電子化
- サービス 3：公金収納の電子化
- サービス４：保険契約情報の閲覧、保険加入の申請、事故情報の申告

以下、これらのサービスごとに、サービスの目的、ヒアリングによる有効性評価、サービス概要とサービスの流れ、サービスの効果と課題について検討結果を示す。

また、あわせてスマートフォンでの運用について、地域通貨を利用したポイントの活用に係る運用も含めた検討を行う。

4.4.2. サービス 1 概要：高齢者向け支援サービス

（1） サービスの目的

高齢者の生活機能低下を防ぎ、また、生活機能が低下した高齢者（生活機能低下者）の機能向上を目的とする介護予防事業（一次予防、二次予防）の課題解決を図るため、高齢者向け支援サービスを検討する。

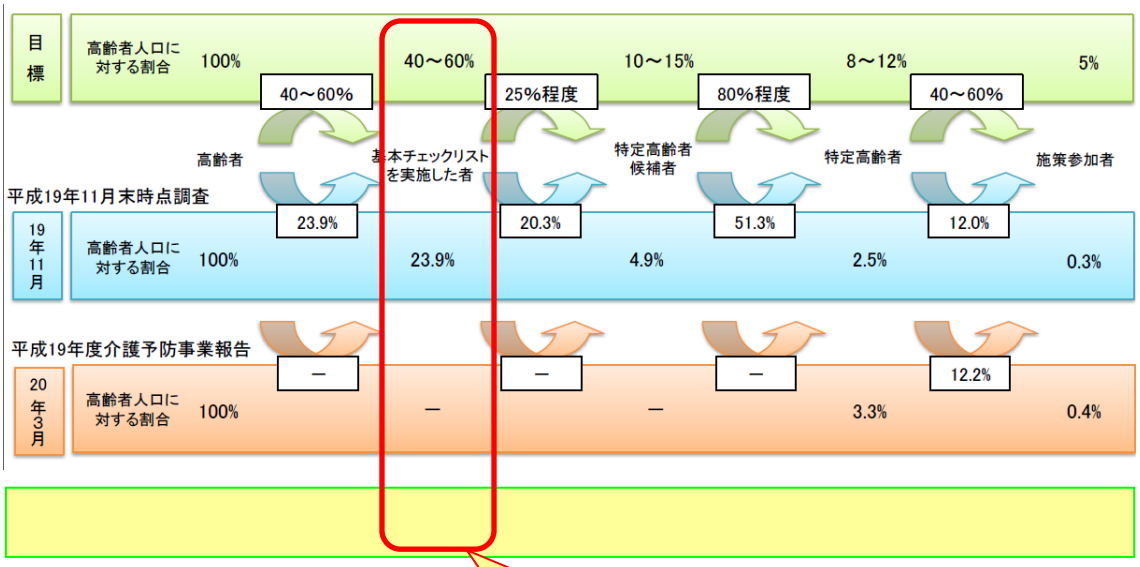
課題解決の手段として、地域ポイント（以下、ポイントという）を活用したサービスを検討する。

① 介護予防事業における施策課題（図 4-9）である生活機能低下者の早期発見に対応するため、基本チェックリスト（※）の効率的な回収と回収率の向上
② 一次予防事業である介護予防ボランティアの活動活性化と継続的な活動の促進
③ 高齢者自身の介護予防活動への取組活性化と継続的な取組みの促進
④ 高齢者からの情報収集による自治体における統計分析への活用

（※）基本チェックリスト・・・厚生労働省のガイドラインにもとづき、６５歳以上の高齢者の方を対象に実施する介護予防のチェックリスト。チェックリストの回答を集計し、

項目別の合計点が一定以上となった場合、必要に応じて介護予防活動や健康診断や生活機能チェックなどを個別に実施し、その結果、要支援・要介護状態となる可能性があり、生活機能の向上が必要と判定された対象者（「特定高齢者」）に対しては、個別の「介護予防プラン」が実施される。

なお、上記①で示す介護予防事業における施策課題は図 4-9 示すように、現状の介護予防事業（特定高齢者）の施策課題として、課題 1～課題 3 の 3 件の課題が挙げられている。本検討での高齢者向け支援サービスとしては、課題 1 の解決を目的とする。



出典：第８２回市町村職員を対象とするセミナー「今後の介護予防に　　21.12.11）「介護保険制度と介護予防の役割について（厚生省課長、宇都宮啓）

基本チェックリストを実施した人数が不十分

【施策課題】

・課題１：①ハイリスク者の把握が不十分
（基本チェックリストによる把握と回収率の向上や未回収者への対応方策など）
②健診による把握に要する費用負担大

・課題２：ケアプランに係る業務負担が大きい

・課題３：①魅力あるプログラムの不足、②特定高齢者施策への参加率が低い

出典：第５期介護保険事業（支援）計画の策定準備及び地域支援事業の見直しに係る会議資料<<介護予防事業関係>>（H22.10.27）（厚生労働省老健局老人保健課）

図 4-9　介護予防事業（特定高齢者施策）の現状と課題

（2） 高齢者向け支援サービスのヒアリングによる有効性評価

高齢者向け支援サービスの目的を実現する手段としてポイント付与に関するサービス案を表 4-12 に示すように 8 項目抽出し検討した。

サービス提供機関へのヒアリングであげられた意見や評価を基に、サービス提供機関の施策や業務上のメリットの有無の観点から 4 項目のポイント付与サービスを選定した。

項番 4、項番 7 はサービス提供機関の施策上の課題がなく、かつ、二重投資になる観点から選定候補から外した。

選定したポイント付与サービスの内、項番 1 と項番 8 を、高齢者の健康状態の記録と管理、健康状態と介護予防活動記録の統計分析への利用サービスとして、項番 2 と項番 3 をボランティア活動の継続的な促進サービスとしてまとめた。

表 4-12　高齢者向け支援サービスのヒアリングによる有効性評価

項番	検討サービス		ヒアリング内容				評価結果
	目的	ポイント付与サービス（案）	ヒアリング時の評価	ポイント付与による期待効果（注）			ポイント付与サービスとして選定候補
				施策課題の解決	活動の奨励	業務の効率化	
1	基本チェックリストの効率的な回収と回収率の向上	基本チェックリスト実施時にポイント付与	・一般自治体については施策課題である介護予防の生活機能低下者の早期発見のための基本チェックリストの回収率の向上に有効である。 ・浦添市においては回収目標を達成しており課題認識をしていない。 ・一般自治体や浦添市において、発送や回収に郵送等でのコストがかかっている。	○（浦添市以外）	—	○	○
2	ボランティア活動の継続的な活動の促進	ボランティア実施にポイント付与	・ボランティアの動機づけになり、ボランティア活動の活発化や継続的な活動の促進に有効である。	—	○	—	○
3		見守り実施時にポイント付与		—	○	—	○
4	高齢者自身の介護予防活動への取組活性化と継続的な取組み	健康目標の達成時にポイント付与	・自治体主催のプログラムへの参加に対して、さらにポイントを付与することは自治体からは二重投資になり、好ましくない。 ・民間業者（フィットネスクラブなど）にお願いして、入会金を免除するなど、行政が投資しないインセンティブは実施している。	—	○	—	×
5		運動目標の達成時にポイント付与					×
6		介護利用時にポイント付与					×
7		健康イベント等への参加時にポイント付与					×
8	自治体での統計分析の利用	健康状態と実態状況の情報収集	・実態状況の調査にコストをかけており、ポイント付与による情報収集の奨励やコスト削減、業務効率化、介護施策の分析に有効である。	—	○	○	○

（注）ポイント付与の期待効果の定義：
・施策課題の効果　：　介護予防事業の施策上の課題のうち「ハイリスク者の把握」に関する課題に対する期待効果
・活動の奨励　　：　ポイント付与が高齢者やボランティアの方の動機づけに対する期待効果
・業務の効率性　　：　自治体業務でのコスト削減や業務の効率化に対する期待効果

（３） 高齢者の健康状態の記録と管理、健康状態と介護予防活動記録の統計分析への利用

本サービスのサービス概要とサービスの流れ、サービスの効果と課題を整理する。

ｉ）サービス概要

本サービスは高齢者の方の介護予防活動を継続的に行うための支援を行うサービスであり、高齢者自身の健康状態や介護予防活動への参加状況の記録と閲覧、自らの健康状態や生活状態をチェックするための基本チェックリストの入力と送信、高齢者の介護予防活動の取り組み情報の収集と統計分析への利用に関する、サービスから構成される。

本サービスの概要を以下に示す。

- 高齢者自身の健康状態や介護予防活動への参加状況をスマートフォンに記録し、情報を閲覧することで介護予防活動を継続的に行う。
- 統計分析に活用する基本チェックリストや各プログラムの参加状況等を、スマートフォンを用いて高齢者個人からの情報収集を図る。自治体に情報提供する時にポイントを付与することで情報提供率の向上を図る。

ⅱ）サービスの流れ

本サービスの流れを図 4-10 に示す。

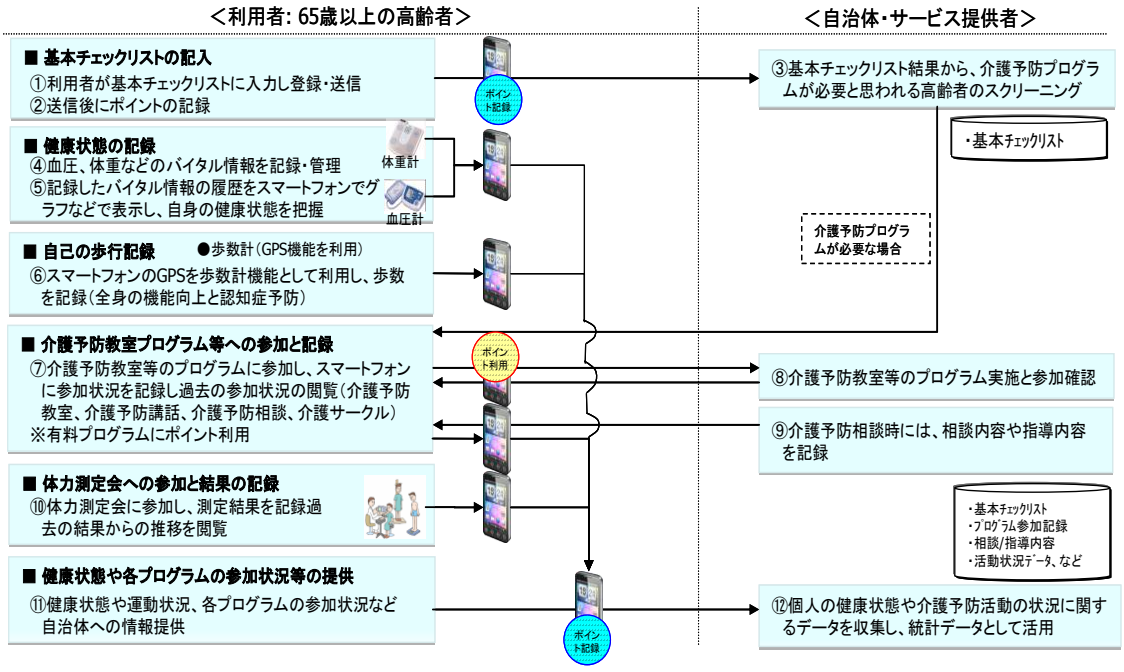


図 4-10　サービスの流れ

ⅲ）サービスの効果と課題

本サービスの想定効果と課題を整理する。

本サービスの利用者（65 歳以上の高齢者）とサービス提供機関である自治体に対する想定効果を表 4-13 に示す。

また、本サービスを実現する際の運用上の課題と制度上の課題を表 4-14 に示す。

表 4-13　サービスの想定効果

利用者（65 歳以上高齢者）	自治体
• （浦添市を除く自治体）ポイント付与により、基本チェックリストに対する高齢者自身の取り組みを活性化でき、自己の健康状態を経年的かつ簡易に把握することができる。 • 高齢者の健康状態（基本チェックリストや健康状態の記録など）の記録から自己の介護予防の目標が明確になり、介護予防活動の意識向上と継続的な推進ができる。 • 高齢者の健康状態と介護予防プログラムやサークル活動等への参加状況が記録され、過去の活動履歴の閲覧など健康状態や活動の経過が可視化され、継続へのモチベーションを維持・向上することができる。 • スマートフォンの活用により、いつでも場所を問わず入力や参照が可能となり、利便性向上によるモチベーション向上につながる。	• ポイント付与により、基本チェックリストの回収率が向上し、国の目標を達成することができる。 （浦添市を除く自治体） • スマートフォンを利用することにより、基本チェックリストの回収コストや回収業務を削減することができる。 • スマートフォンの利用により、効率的に、高齢者の健康状態や介護予防プログラムやサークル活動等への参加状況の収集・蓄積ができ、傾向把握のための統計分析を行うことができる。ポイント付与により情報収集が促進され、タイムリーに情報を収集することができる。 • 介護予防事業への参加状況や運動の活動状況を簡易に把握でき、施策効果を把握することができる。 • 本人の取組状況や生活状態が把握できるため、適切なアクションやアドバイスが可能となる。

表 4-14　サービスの実現課題

運用上の課題	制度上の課題
• IT 機器に不慣れな高齢者でも、簡単に操作できるようなスマートフォン上の操作性や運用性（サービス機能やサービスの流れ）の検討 • ポイント付与を行う場合の確認方法の検討 • 収集データの保管期限や利用方法等に関する問合せ対応 • 情報提供に対し付与する地域通貨（ポイント）の原資（自治体負担）と既存の地域通貨　（ポイント）の原資（事業者負担）を統合して管理するための管理主体 • 介護予防プログラムへの参加記録や介護予防相談時の相談内容や指導内容の記録の運用（従来の介護予防手帳への手書き記入からスマートフォン上への入力に変わることによるサービス提供者側の運用負荷） • 介護教室などスマートフォン上に参加記録とポイントを付与する場合の環境(PC と IC カードリーダ、NW 環境など) • 高齢者による基本チェックリストの登録や健康状態等の情報提供時に、オンラインで地域通貨（ポイント）を付与する仕組みの検討 • 外部端末とスマートフォンがお互いに通信する機能（NFC 等）の実装	• 自治体での統計利用時の個人情報の管理や匿名化方法の検討

（4） ボランティア活動の継続的な促進

本サービスのサービス概要とサービスの流れ、サービスの効果と課題を整理する。

ｉ）サービス概要

本サービスは、ボランティアの方がボランティア活動や高齢者の見守り活動を行う際の支援サービスとして、また、民生委員の方が一人暮らしの高齢者の現状把握調査の支援サービスを行うものである。

本サービスの概要を以下に示す。

- スマートフォンを用いてボランティアの登録やボランティア活動の案内など、ボランティアに対する支援サービスを提供するとともに、ポイント付与による高齢者向けボランティア活動への継続的な参加を促進し、地域コミュニティの活性化を図る。
- 民生委員等による一人暮らし高齢者の現状把握調査などをスマートフォンによって記録するなどの支援サービスを提供し、民生委員等へのポイント付与による高齢者の現況情報の質や見守り体制の向上を図る。
- スマートフォンを用いて、緊急時に高齢者からいつでも、どこでも関係者への通報により、高齢者の事故防止を図る見守りボランティア活動の支援を行う。

ii）サービスの流れ

本サービスの流れを図 4-11 に示す。

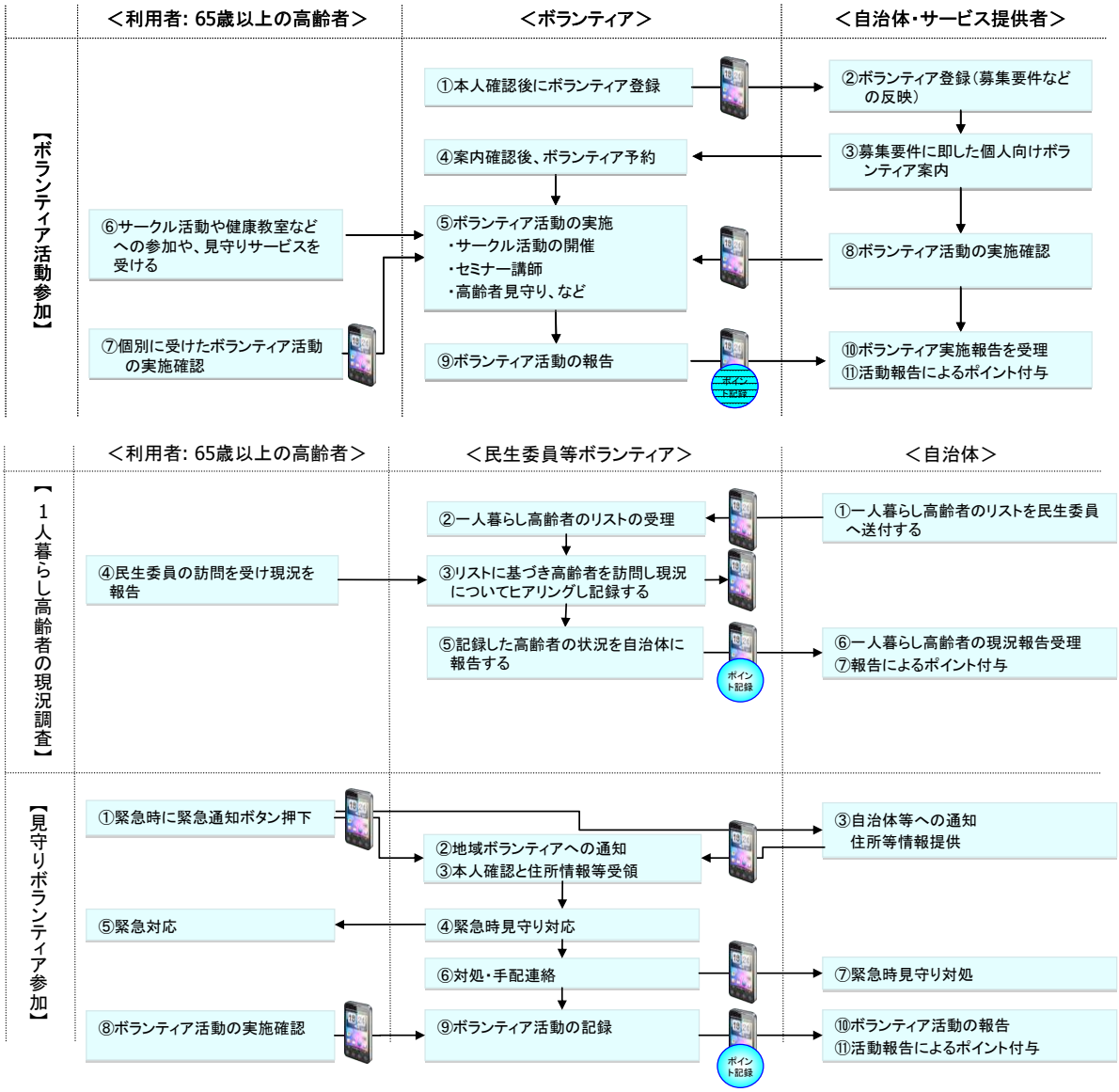


図 4-11　サービスの流れ

iii）サービスの効果と課題

本サービスの想定効果と課題を整理する。

本サービスの利用者（高齢者）、ボランティアとサービス提供機関である自治体に対する想定効果を表 4-15 に示す。

また、本サービスを実現する際の運用上の課題と制度上の課題を表 4-16 に示す。

表 4-15　サービスの想定効果

利用者（高齢者）	ボランティア	自治体
• 一人暮らしの高齢者が安心して暮らせる • コミュニケーションによる不安解消 • 緊急時の迅速な対応	• ポイント付与により、高齢者を支えるボランティアの活動意識を高めることができ、ボランティア活動を継続的に推進することができる。	• ポイント付与によるボランティア活動への動機づけにより、ボランティアの自立的な活動が進み、活動の場の拡大やボランティア人員の確保などによるボランティア事業の推進を図ることができる。

表 4-16　サービスの実現課題

運用上の課題	制度上の課題
• ボランティアの意識づけに有効なポイントの付与基準やポイントの用途（利用範囲）の検討 • ボランティアへの利用登録方法と権限の付与方法（権限によって厳密な本人確認が必要な場合の確認方法） • 見守りなどの緊急対応時のエスカレーション方法（見守り者が対応できない場合などの緊急措置など） • ボランティアの活動報告を自治体へ報告する、運用ルールの規定化 • ボランティア活動を実施した際の第三者（ボランティア本人以外の自治体など）による実施確認の方法	• ボランティアへの付与ポイントの財源を確保する必要がある。 • 見守りボランティア時のボランティア等への高齢者個人情報の提供に対する個人情報保護の制約 • 見守りボランティア時に見守り情報を第三者（自治体）に報告する場合の本人同意

4.4.3.　サービス 2 概要：行政手続の申請手段の電子化サービス

(1) サービスの目的

行政手続きの申請手段の電子化サービスは、自治体窓口での行政手続きの申請手段の電子化サービスとして、スマートフォンによる簡便な操作性や迅速な情報伝達の特徴を活かし、行政手続きの待ち時間の短縮や煩雑な申請手続きを簡略化することにより住民サービスの向上を図る

(2) 行政手続きの申請手段の電子化のヒアリングによる有効性の検証

行政手続きの申請手段の電子化サービスの目的を実現するために下表の３項目のサービス（案）を検討し、サービス提供機関である自治体へのヒアリングを実施し、その際のご意見や評価を基に、住民サービスの向上につながる施策であるかどうかの観点から検討サービス（案）を評価し、項番 1～3 のサービスを選定した。

ヒアリングによる有効性の検証結果を表 4-17 に示す。

また、選定したサービスの内、項番 1 と項番 3 を、住民票等の交付サービス、項番 2 を住民登録サービスとしてまとめた。

表 4-17　ヒアリングによる有効性の検証

項番	検討サービス（案）		ヒアリング内容	評価結果
	目的	サービス	ヒアリング時の評価	サービスとして選定候補
1	行政手続きの待ち時間の短縮や煩雑な申請手続きをなくすことによる住民サービスの向上	住民票等の電子手続きによる交付	• 行政手続きの申請･登録時の窓口での待ち時間の短縮が期待できることや、複数の申請を同時に行う際､同じような申請情報の記入がなくなることにより､申請の煩雑さがすくなることから、住民サービスの向上に有効である。 • ただし､納税証明や戸籍などは困難かもしれない。	○
2		住所等の電子手続きによる登録・申請		○

(3) 住民票等の交付

住民票等の交付サービスのサービス概要とサービスの流れ、サービスの効果と課題について示す。

ⅰ）サービス概要

本サービスは、住民がスマートフォンを利用し、住民票などの交付証明書の申請情報を事前に入力し、自治体窓口での申請情報の入力の煩雑や待ち時間の短縮を図るサービスである。

本サービスの概要を以下に示す。

- 住民がスマートフォンを利用し、住民票などの交付証明書の申請情報を事前に入力し、自治体窓口での申請用紙への記入の煩雑さや待ち時間の短縮を図る。
- 窓口業務での記入漏れチェックや二重入力の排除などによる業務効率化と待ち時間の短縮、業務コストの削減を図る。
- 浦添市においては、「てだカード（市民カード)」と「察度」カード（地域通貨カード）を所有する利用者に対し、1 台のスマートフォンに統合することで利用者の利便性向上を図る。
- スマートフォンに記録されたポイントを利用し、交付手数料を支払う。

ⅱ）サービスの流れ

本サービスの流れを図 4-12 に示す。

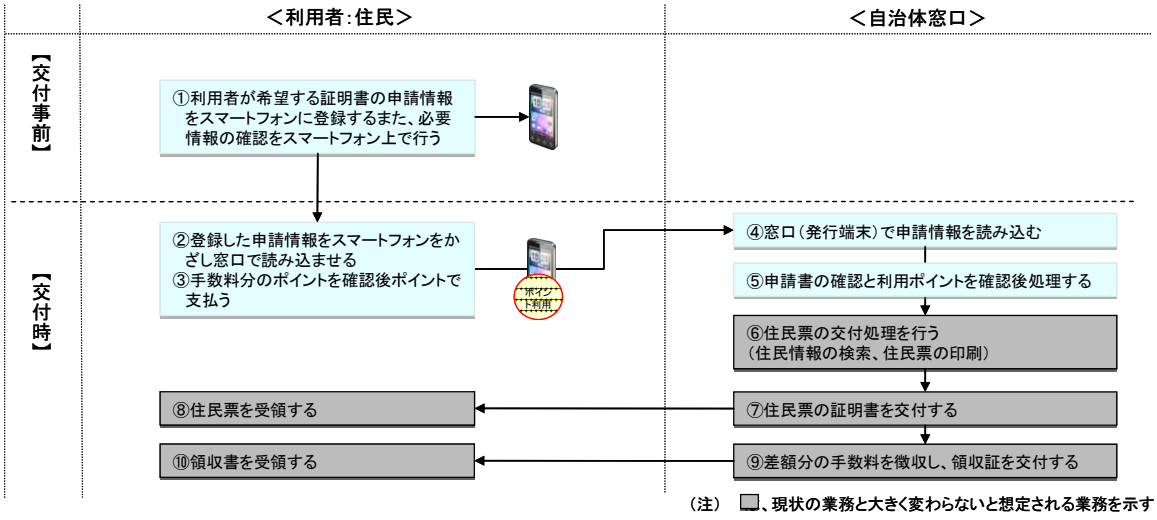


図 4-12　サービスの流れ

ⅲ）サービスの効果と課題

本サービスの想定効果と課題を整理する、

本サービスの利用者（住民）とサービス提供機関である自治体に対する想定効果を表 4-18 に示す。

また、本サービスを実現する際の運用上の課題と制度上の課題を表 4-19 に示す。

表 4-18　サービスの想定効果

利用者（住民）	自治体
• 窓口での申請書記入の煩雑さがなくなり、また、待ち時間の短縮など証明書交付申請時の利便性を向上することができる。 • 行政の手数料へのポイント利用範囲が広がることにより、地域通貨の利便性が向上する。 • 浦添市では、既存カード所有者に対し、「てだカード」と「察度」カードの統合により、2 枚のカードを保持する煩雑さがなくなる。	• 窓口業務での交付処理が簡略化と迅速化によって、住民の待ち時間が短縮され、サービス性が向上する（通常 30 分、混雑時 3 時間かかる待ち時間を短縮することができる）。 • 窓口業務での記入漏れチェックや二重入力の排除などによる業務効率化と業務コストの削減が図れる。

表 4-19　サービスの実現課題

運用上の課題	制度上の課題
• 交付対象の行政手続きとして、住民票、印鑑証明、税関連証明書等を想定しており、これらの証明書発行を電子化手続きで行う際の本人性の確認方法 • 複数の証明書を 1 回の申請処理で交付するワンストップ処理を行う際、税務などの専門性が必要となる業務処理との連携方法 • 現状、本人確認の記録として免許証番号を記録しているが、スマートフォンでの本人確認を行う際の記録対象情報 • スマートフォンと通信するための設備（PC、IC カードリーダ等）の整備	• 現状、複数のカードで実施しているサービスを、一つのスマートフォンに統合する場合の統合方法（浦添市の場合、「てだカード」（市民カード）と「察度」カード（地域通貨）を１台のスマートフォンに統合する） • 現状、複数のカードで実施しているサービスを、一つのスマートフォンに統合する場合、既存のサービスで認めている代理申請への対応方法

(4)　住民登録等その他利用

ⅰ）サービス概要

本サービスは、住民がスマートフォンを利用して、住民登録の手続きに必要な情報を事前に一括入力し、窓口での登録申請時の手続きの煩雑さや待ち時間の短縮を図るものである。

本サービスの概要を以下に示す。

- 住民がスマートフォンを利用して住民登録の手続きに必要な情報を事前に一括入力し、窓口では、事前登録した情報を取り込みさせることにより、登録申請時の記入の煩雑さや待ち時間の短縮を図る。
- 窓口業務での記入漏れチェックや二重入力の排除などによる業務効率化と待ち時間の短縮、業務コストの削減を図る。

ⅱ）サービスの流れ

本サービスの流れを図 4-13 に示す。

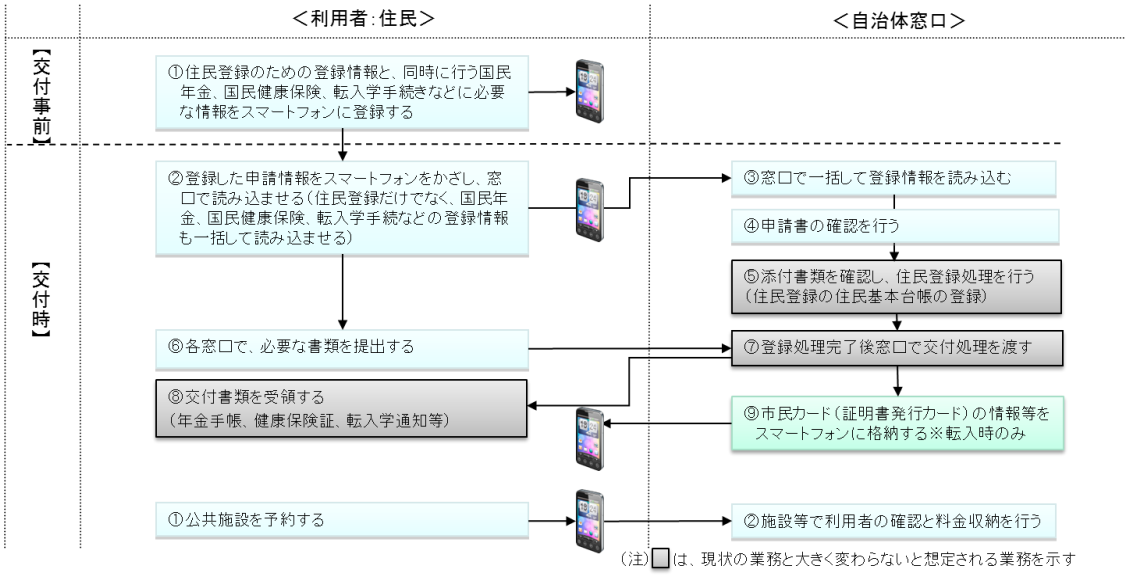


図 4-13　サービスの流れ

ⅲ）サービスの効果と課題

本サービスの想定効果と課題を整理する。

本サービスの利用者（住民）とサービス提供機関である自治体に対する想定効果を表 4-20 に示す。

また、本サービスを実現する際の運用上の課題と制度上の課題を表 4-21 に示す。

表 4-20　サービスの想定効果

利用者（住民）	自治体
• 複数の登録手続きに必要な情報を一括して入力することにより、複数の登録申し込みの記入の煩雑さがなくなり、住民登録手続きと関連の手続きの利便性が向上する。 •	• 窓口業務での二重入力の排除など交付処理が簡略化し、処理待ち時間の短縮による住民サービスが向上する（通常 30 分～混雑時 3 時間かかる待ち時間を短縮することができる）。 • 窓口業務での記入漏れチェックや二重入力の排除などによる業務効率化と業務コストの削減が図れる。

表 4-21　サービスの実現課題

運用上の課題	制度上の課題
• 交付の際の対象とする行政手続きとして、住民登録、印鑑登録、住所変更などの各種届出を想定しており、これらの登録手続き申請の電子化を行う場合の本人性の確認方法 • 氏名等の外字処理に関連して、スマートフォンと自治体システムの外字コード体系の共通化 • 公共施設等でスマートフォンを読み取るための設備（PC、IC カードリーダ等）の整備	• 既存の登録手続き申請方法について、市の条例で規定している場合、カードだけでなくスマートフォンを用いて申請可能となるよう改正する必要がある。

4.4.4.　サービス 3 概要：公金収納の電子化サービス

（1）　サービスの目的

公金収納の電子化サービスは、スマートフォンによるいつでもどこでもタイムリーに操作できるモバイル性を活かし、公金収納に関する収納率の向上を図る。

（2）　公金収納の電子化サービスのヒアリングによるサービス性の検証

公金収納の電子化サービスの目的を実現するために表 4-22 の 2 項目のサービス（案）を検討し、サービス提供機関である自治体へのヒアリングを実施し、その際のご意見や評価を基に、公金収納に関する収納率の向上に有効かどうかの観点から検討サービス（案）を評価し選定した。

検討サービスに対するヒアリング時の評価と評価結果を表 4-22 に示す。

表 4-22　ヒアリングによるサービス性の検証

項番	検討サービス（案）		ヒアリング内容	評価結果
	目的	サービス	ヒアリング時の評価	サービスとして選定候補
1	公金収納に関する収納率の向上	市民税等の通知書（納付書）送付と支払い(注)	• スマートフォンのモバイル性から、納付者が納付内容の確認や支払いをその場で行うなど支払い手続きの簡便化により収納率の向上に有効となる	○

（注）本資料では、通知書（納付書）は、通知書に納付書を含むことを示す。各々の書類を個別に言及する場合は、通知書、納付書と個別に記す。

（3）　市民税等の通知書（納付書）送付と支払いサービス

本サービスのサービス概要とサービスの流れ、サービスの効果と課題を検討し、結果を以下に示す。

ｉ）サービス概要

通知書（納付書）を利用者のスマートフォンに直接通知することにより支払いの忘れや支払いの迅速化を図るとともに、通知書（納付書）配送時の印刷・郵送にかかるコストの

削減や処理時間の短縮、及び収納率の向上を図る。

ⅱ）サービスの流れ

サービスの流れを図 4-14 に示す。

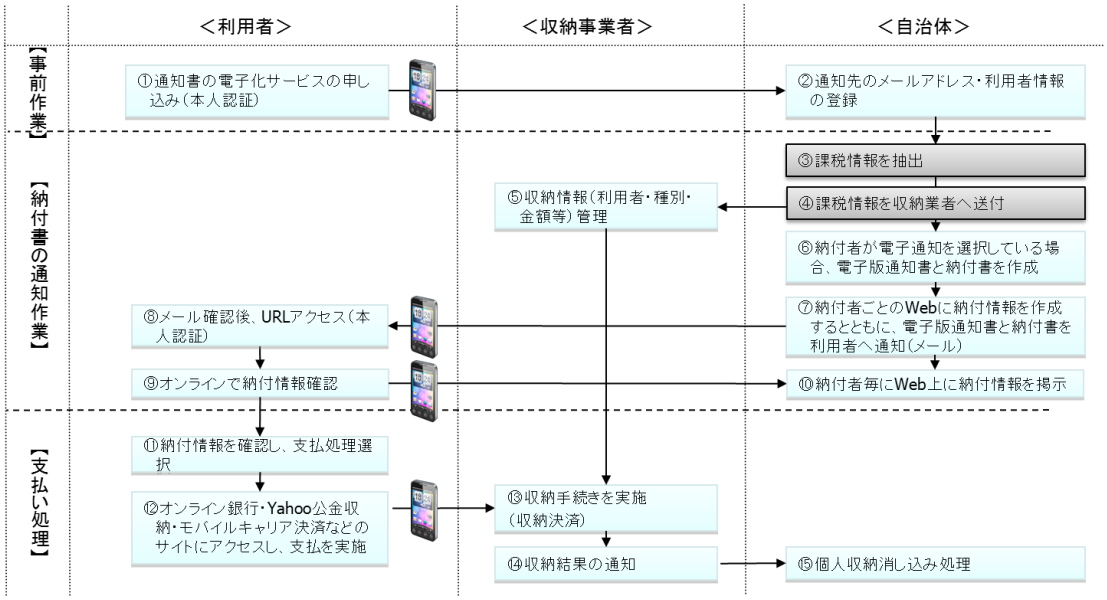


図 4-14　サービスの流れ

ⅲ）サービスの効果と課題

本サービスの想定効果と課題を整理する。

本サービスの利用者（住民）とサービス提供機関である自治体に対する想定効果を表 4-23 に示す。

本サービスを実現する際の運用上の課題と制度上の課題を表 4-24 に示す。

表 4-23　サービスの想定効果

利用者（住民）	自治体
• 納付者のスマートフォンに直接通知されることにより、スマートフォン上で納付内容の確認や支払いをその場で行うことができ、支払いを忘れることなく迅速に行うことができる。	• 課税計算後の通知書（納付書）の印刷や配送までの処理時間の短縮と配送コストの削減し、また、収納率の向上を図る。（浦添市の場合通知書（納付書）の印刷から配送までの処理期間（２週間）の短縮と年間約 2,000 万円のコストの削減）

表 4-24　サービスの実現課題

運用上の課題	制度上の課題
• 紙の通知書（納付書）と電子通知が併存する場合の通知運用の負荷（紙での納付と電子通知の選択方法、課税処理後の処理の流れなど） • 通知書（納付書）の電子通知時のメールアドレス変更手続きとメール不達時の再送処理時の通知運用の負荷（従来の督促処理を行うなど） • スマートフォンへ、メールにより通知書を送付する場合、その通知の到達確認の技術的要件の明確化	• 通知書の送付に関する、地方税法 第 20 条（書類の送達）で規定されている郵送または信書便による送達と到達時の規程の電子通知手段に対する拡張と改定 • メールにより通知書を送付する場合、その通知の到達確認の条件が制度上、明確でない

4.4.5. サービス 4 概要：保険契約情報閲覧、保険加入申請、事故情報申告

(1) サービスの目的

保険契約に対する既存契約情報の一括表示や保険継続加入申請などの電子化による業務効率化を図るとともに、スマートフォンによる事故発生時の迅速な対応と利用者（契約者）への事故処理の効果的な誘導による顧客サービスの向上を図ることを目的とする。

(2) 保険契約情報閲覧、保険加入申請、事故情報申告のヒアリングによるサービス性の検証

保険の電子化サービスの目的を実現するために下表の 2 項目のサービス（案）を検討し、サービス提供機関である保険会社様へのヒアリング時のご意見や評価を基に、保険情報の電子化に関する業務効率化や顧客サービスの向上に有効かどうかの観点から検討サービス（案）を評価し選定した。

なお、項番 1 については、利用者から日々アクセスしたい情報がないと利用者拡大につながらない点と契約情報の閲覧は事故等が発生しない限り効果が薄いとの観点から選定候補から外した。

検討サービスに対するヒアリング時の評価と評価結果を表 4-25 に示す。

表 4-25　ヒアリングによるサービス性の検証

項番	検討サービス（案）		ヒアリング内容	評価結果
	目的	サービス	ヒアリング時の評価	サービスとして選定候補
1	契約情報の閲覧や加入申請の電子化による効率化	会員専用ページの活用	• 利用者が手間なく確実な認証ができれば将来的に有効だと考える • 会員専用ページの利用が少ないため、利用促進となる情報が必要であり、既存情報のみでは利用が広がらない • IC カードも利用するとなると利用者の操作性や IC カード運用などのコストが懸念され、保険会社が持つというより公的な機関が発行したカードを利用できればメリットがある	×
2	事故発生時の効果的な誘導による顧客サービス向上	事故発生時のスマートフォン利用	• 事故発生時の電話対応での契約確認や状況把握などの効率化や、事故対応の迅速化につながる • 全ての事故申告をスマートフォンアプリで実施するのは現実的ではなく、電話対応も必要である	○

(3) 事故発生時のスマートフォン利用

本サービスのサービス概要とサービスの流れ、サービスの効果と課題を検討し、結果を以下に示す。

ⅰ）サービス概要

事故発生時の連絡において、スマートフォンに登録した情報の送信により、サービスセンターからの様々な確認事項の削減による事故処理の迅速化を図るとともに、保険契約における他種目保険契約の名寄せによる適切な保険給付を行う。契約者以外（運転者、家族等）が事故発生時にサービスセンターの連絡先や契約内容を確認できる。

ⅱ）サービスの流れ

サービスの流れを図 4-15 に示す。

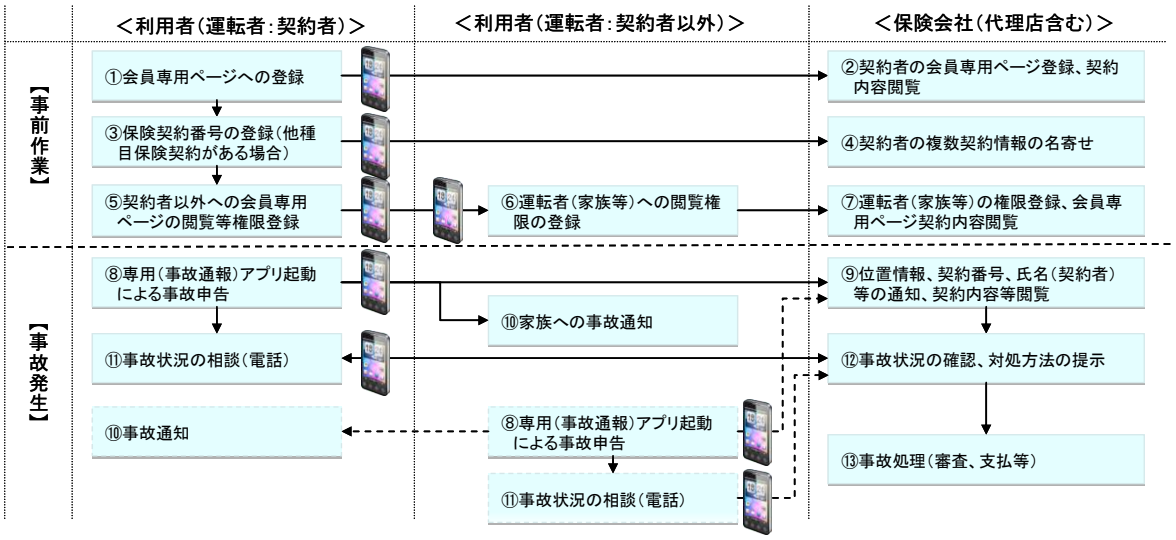


図 4-15　サービスの流れ

ⅲ）サービスの効果と課題

本サービスの想定効果と課題を整理する。

本サービスの利用者（契約者）とサービス提供機関である保険会社に対する想定効果を表 4-26 に示す。

また、本サービスを実現する際の運用上の課題と制度上の課題を表 4-27 に示す。

表 4-26　サービスの想定効果

利用者（契約者）	保険会社
• 事故発生時に必要な基本情報を本人と保険会社の間で迅速に送受信が可能となることで、気が動転した状態での長時間のヒアリングを受けることなく、事故時の適切な行動や保険金請求へ対処できる。 • 本人や家族を含め、もはや手放せず常に携帯しているスマートフォンへ、保険情報や保険会社連絡先が簡易に登録出来ることで、緊急時保険会社といつでも連絡が取れるようになり、日常生活への安心感が高まる。	• 緊急時の受付処理が効率化され、運営コストを軽減出来る可能性があると共に顧客満足度向上が期待できる。 • 普及の推進のため、協力代理店には活用者数等により、軽減されたコストを手数料等へ還元できる可能性もある。

表 4-27　サービスの実現課題

運用上の課題	制度上の課題
• 事故専用アプリへの情報登録や保険会社への発信など運転者による事前の情報入力・操作を実施する仕組みの検討 • 他種目保険番号の誤入力とその際の本人連絡等の保険会社の負荷への対応（本人であることの一意の特定が必要） • 携帯電話圏外、電池切れ、故障、紛失、アプリ障害における代替策の用意 • 紛失した場合や情報を送信する際の情報漏洩防止策 • 緊急時にスマートフォン AP が直ぐに利用できる仕組みの検討（AP 起動時に本人確認ためのパスワード入力は実行上不可能） • スマートフォンの機種変更、キャリア変更時の再登録 • スマートフォンアプリ対応と電話応対の効果的な運用	• 保険業法や金融商取引法、保険法、個人情報保護法などに対する金融庁確認 • 本人を特定し認証するための公的情報を活用する場合の民間活用に対する制度見直し（自動車保険に必要な免許証情報などをスマートフォンに格納する場合、免許情報の利用について警察庁への確認、公的個人認証の民間利用への制度改正など）

4.4.6. スマートフォンでの運用検討

(1) 目的

スマートフォンでのサービスを実現するに当たり、サービス提供事業者である自治体と金融機関（保険会社）での運用を検討し上で、モバイルアクセスシステムの適用範囲を明らかにする。

その際、これまでの運用上の課題と、セキュリティレベル等の検討によって評価した認証方式にそって検討を行う。

(2) 自治体におけるスマートフォン、モバイルアクセスシステムを利用したサービスの運用

自治体でのスマートフォンでのサービスの利用開始時の登録や発行・管理における運用と各サービス時の運用を以下に示す。

適用サービスにおけるセキュリティ保証レベルの検討から必要な保証レベルはレベル 3 以上であるが、運用の検討に当たっては、IC カード（PKI）による認証をスマートフォンにて実現することを前提にトークンを PKI 証明書とし、レベル 4 として運用を検討した。

① サービス開始時の登録（窓口での交付処理）

利用者は、共通アプリケーションをインストールし、モバイルアクセスサーバからカード AP をインストール。自治体窓口にて本人確認およびスマートフォンの所有者であることを確認し、モバイルアクセスサーバからスマートフォンの耐タンパデバイスに利用者情報（証明書等）を登録する。

窓口での交付処理フローを図 4-16 に示す。

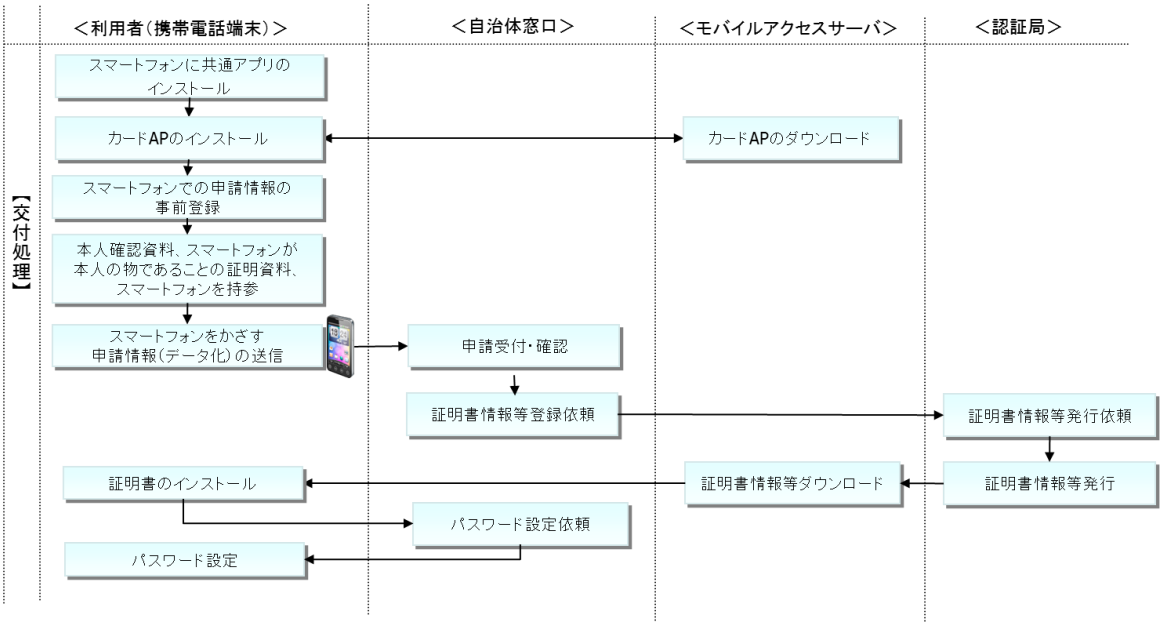


図 4-16　窓口での交付処理フロー

サービス開始時の登録（オンラインでの交付処理）

利用開始時オンラインにて申請を受け付け、書留郵便等で本人宛にパスワードを送付し、スマートフォンへのアプリケーションおよび利用者情報を登録する。

オンラインでの交付処理フローを図 4-17 に示す。

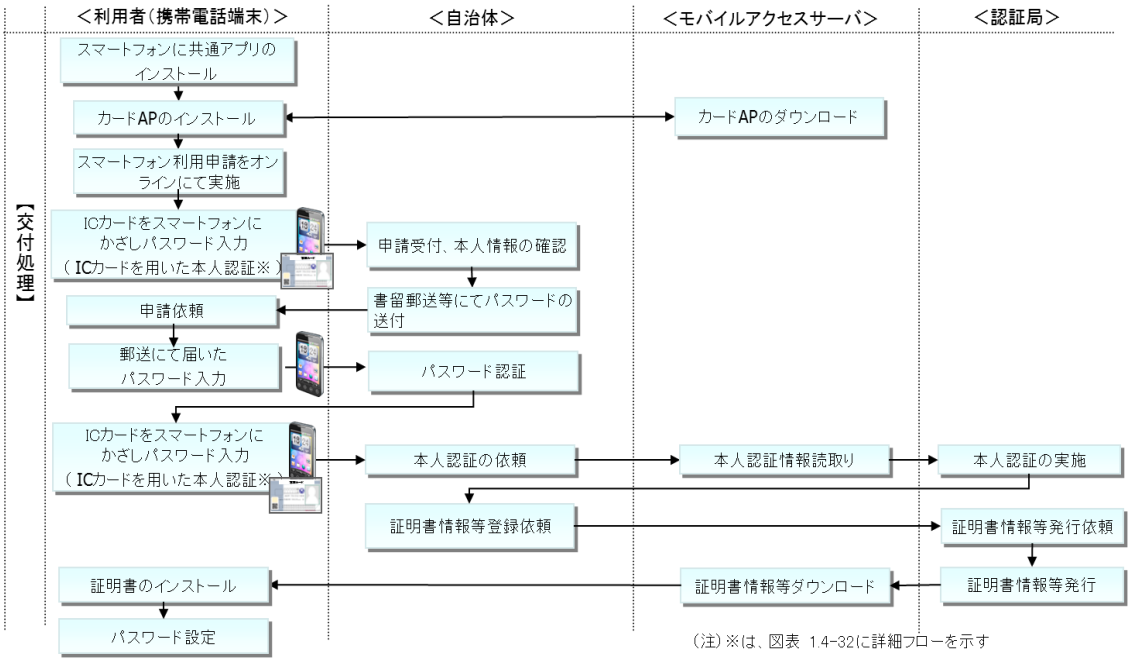


図 4-17　オンラインでの交付処理フロー

② 発行・管理（一時停止処理）

利用者からの電話連絡にて一時停止処理を行うことを想定した場合の一時停止処理フローを図 4-18 に示す。

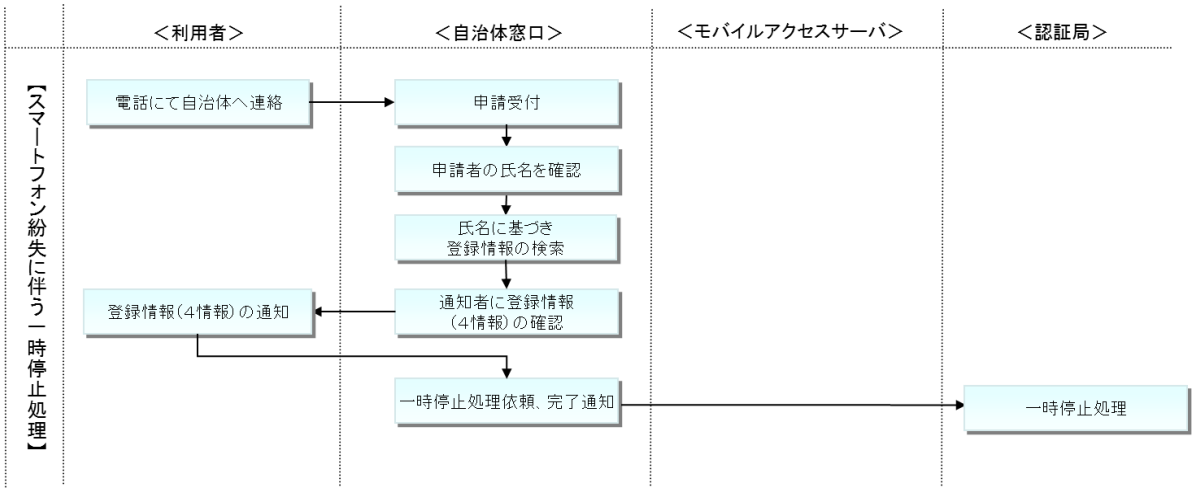


図 4-18　一時停止処理フロー

③ 発行・管理（更新処理）

自治体様窓口にて更新処理を行うことを想定した場合の更新処理フローを図 4-19 に示す。

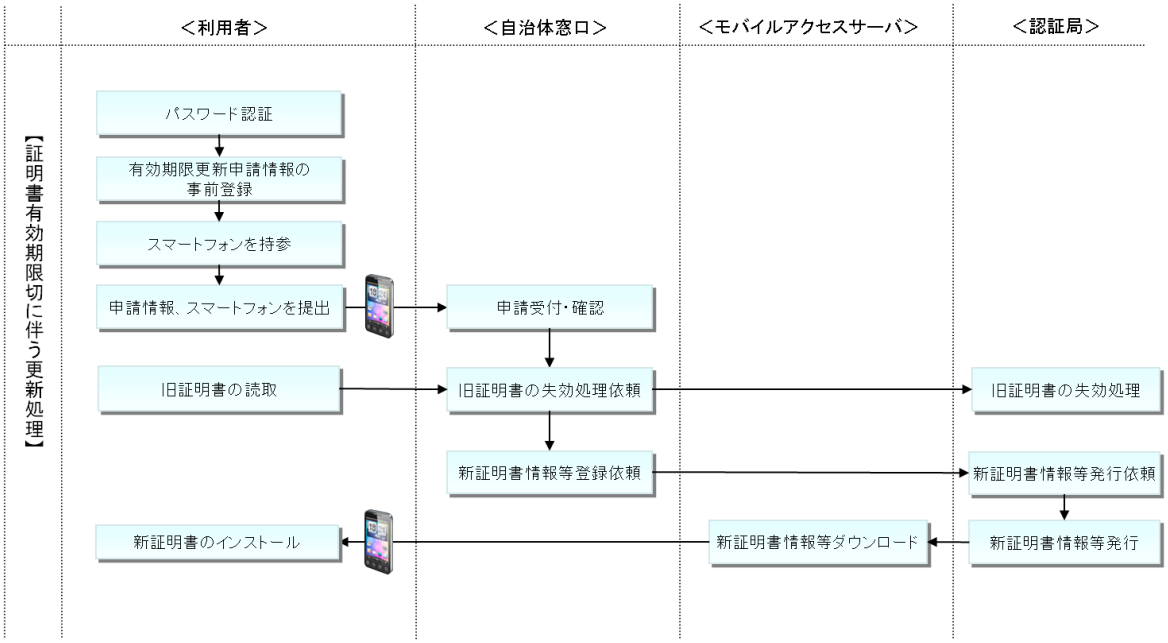


図 4-19　更新処理フロー

④ 失効（失効処理）

自治体窓口にて失効処理を行うことを想定した場合の失効処理フローを図 4-20 に示す。

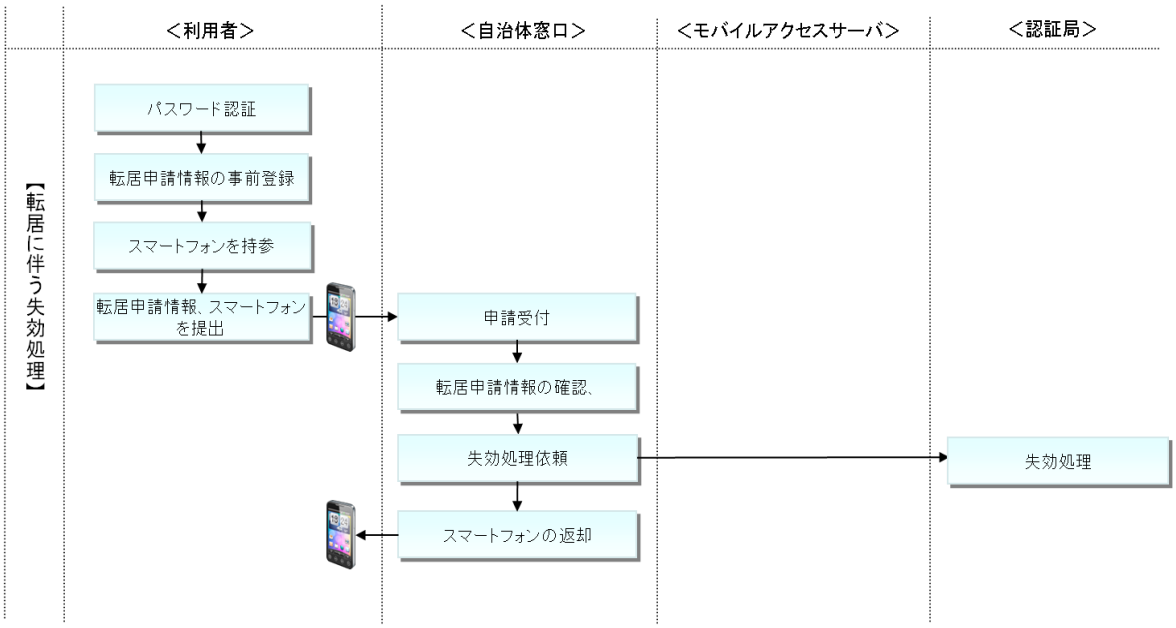


図 4-20　失効処理フロー

⑥健康状態の記録と管理、介護予防活動記録の統計分析への利用

i）基本チェックリストの入力（保証レベル 2）および自治体への提供（保証レベル 3）

基本チェックリストの入力と入力された情報の自治体への提供時の運用フローを図 4-21 に示す。

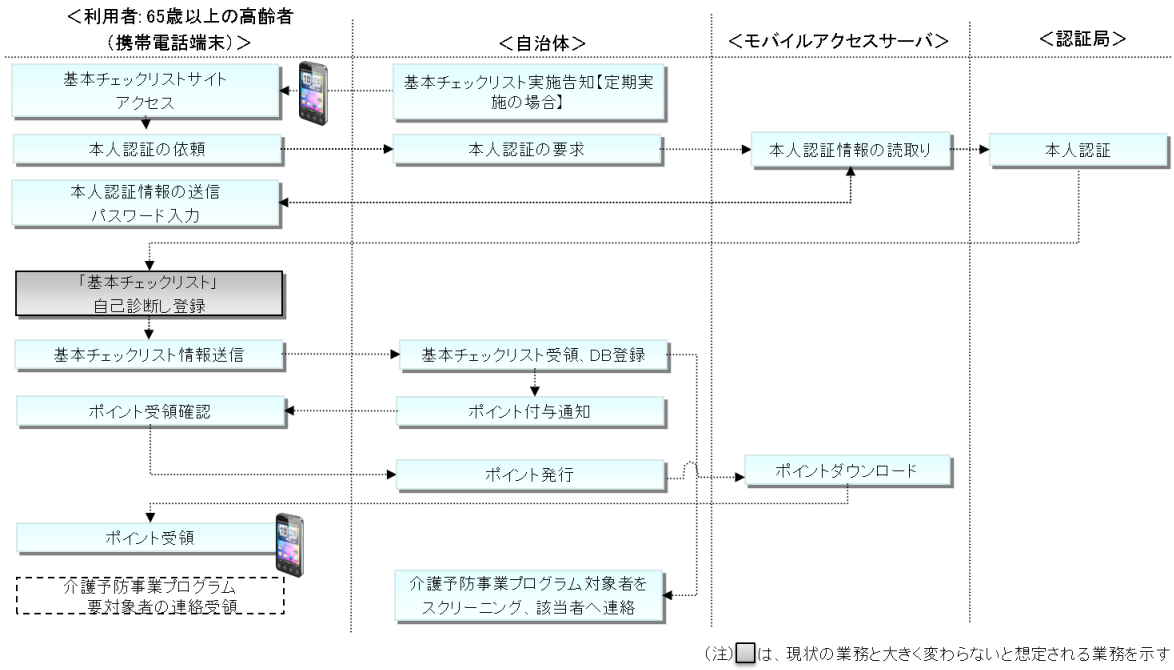


図 4-21　基本チェックリストの入力（保証レベル２）および自治体への提供（保証レベル３）

ii）介護予防プログラム等への参加登録（保証レベル２）

介護予防プログラム等への参加登録時の運用フローを図 4-22 に示す。

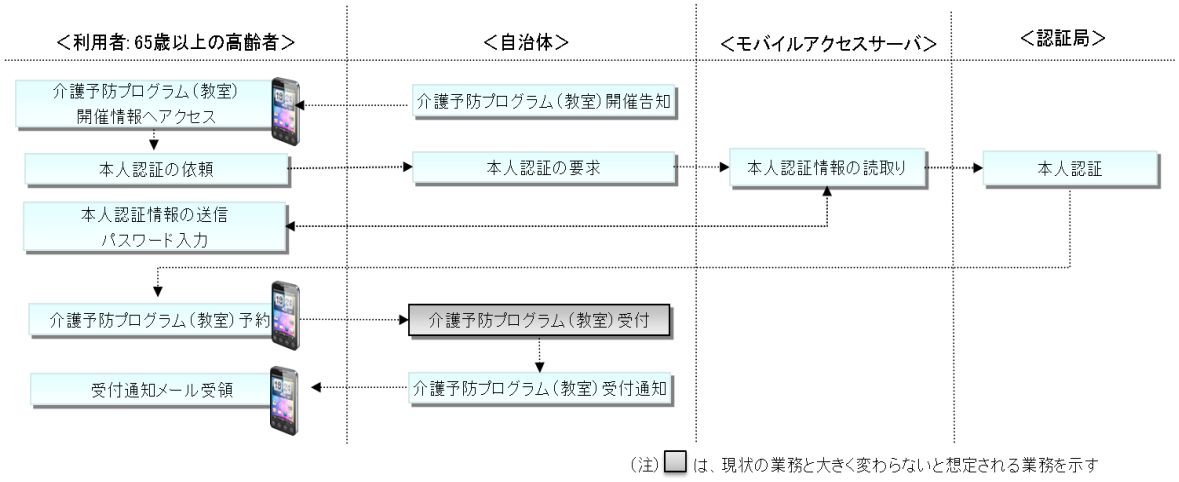


図 4-22　介護予防プログラム等への参加登録（保証レベル２）

iii）介護予防プログラム等の参加、受講の記録（保証レベル３）および自治体への提供（保証レベル３）

介護予防プログラム等の参加、受講の記録と記録した情報の自治体への提供時の運用フローを図 4-23 に示す。

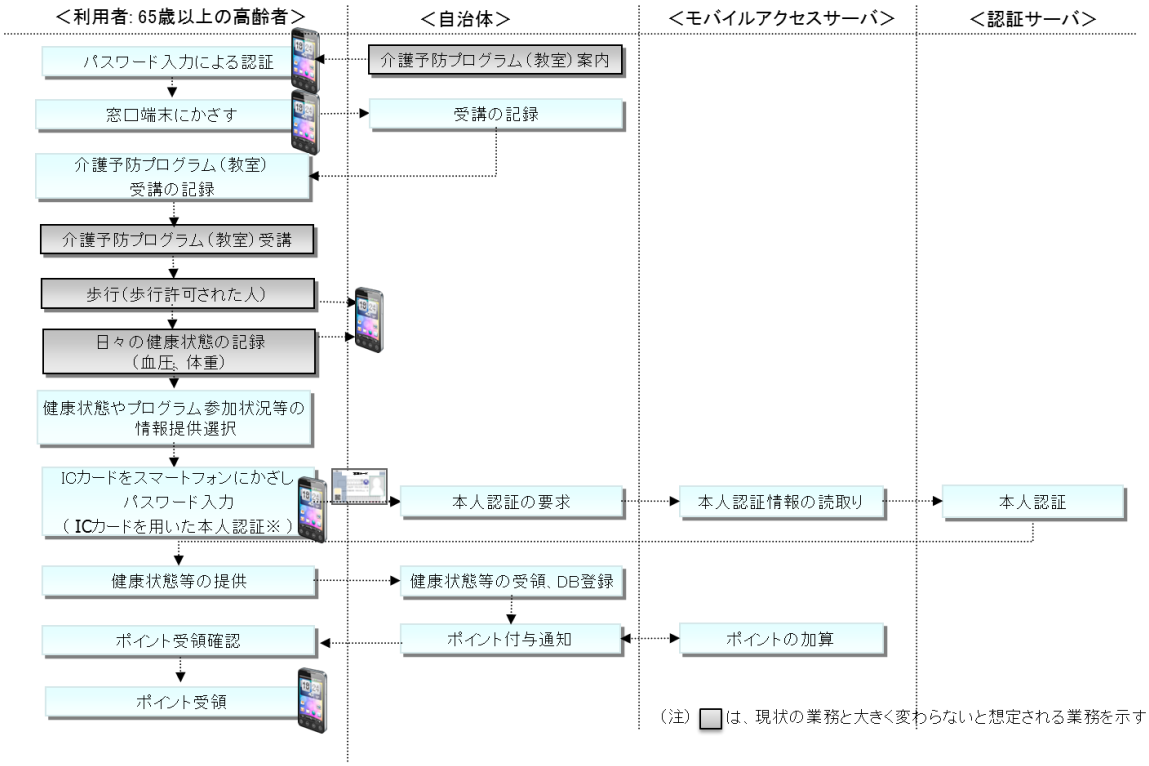


図 4-23　介護予防プログラム等の参加、受講の記録（保証レベル３）および自治体への提供（保証レベル３）

⑦IC カードを用いた本人認証

IC カードを用いた本人認証の運用フローを図 4-24 に示す。

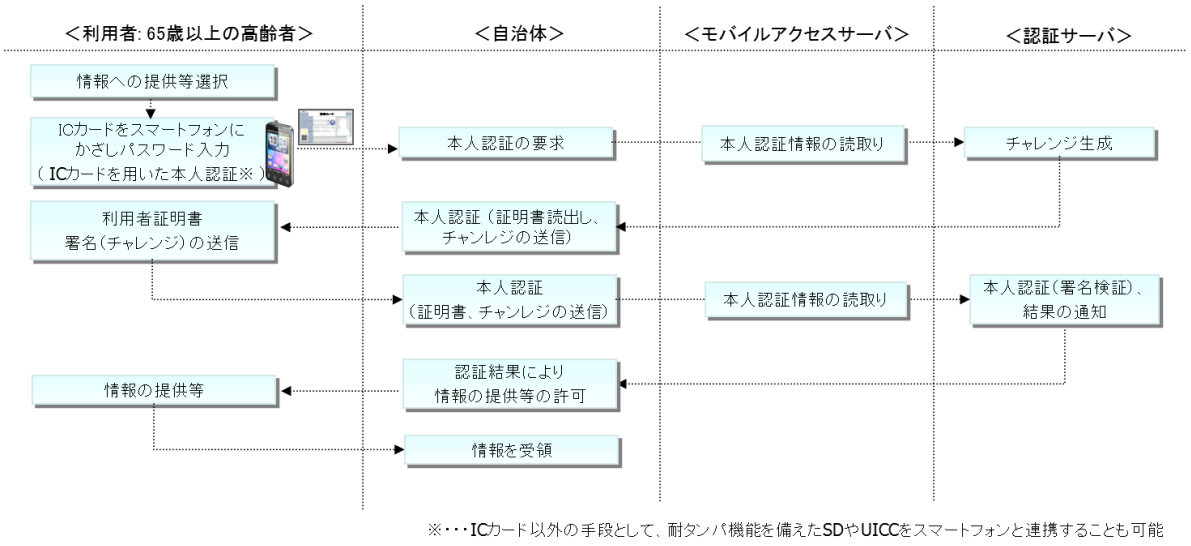


図 4-24　IC カードを用いた本人認証

⑧ボランティア活動の継続的な促進

i）ボランティア登録（保証レベル３）の運用フローを図 4-25 に示す。

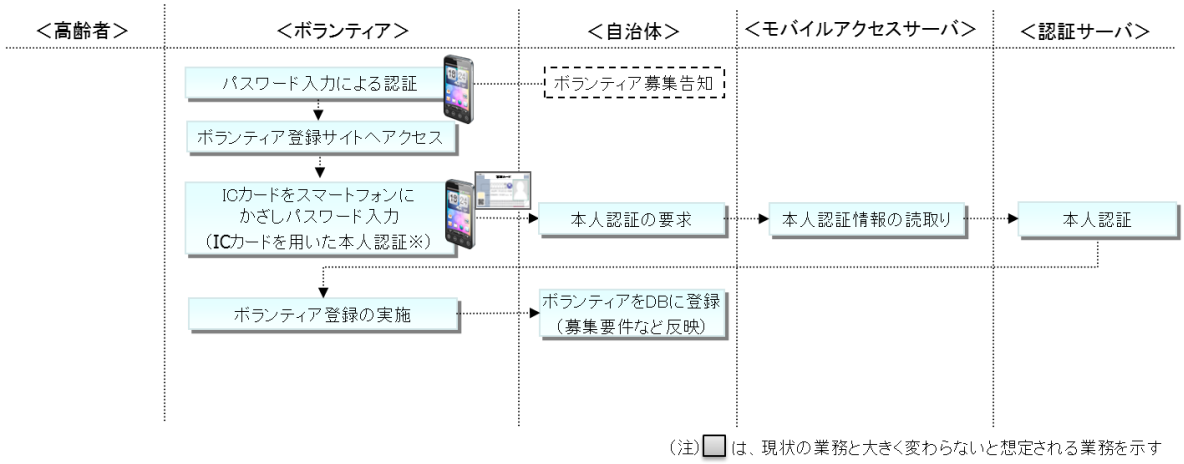


図 4-25　ボランティア登録（保証レベル３）

ii）ボランティア活動の実施と活動情報の提供（保証レベル３）の運用フローを図 4-26 に示す。

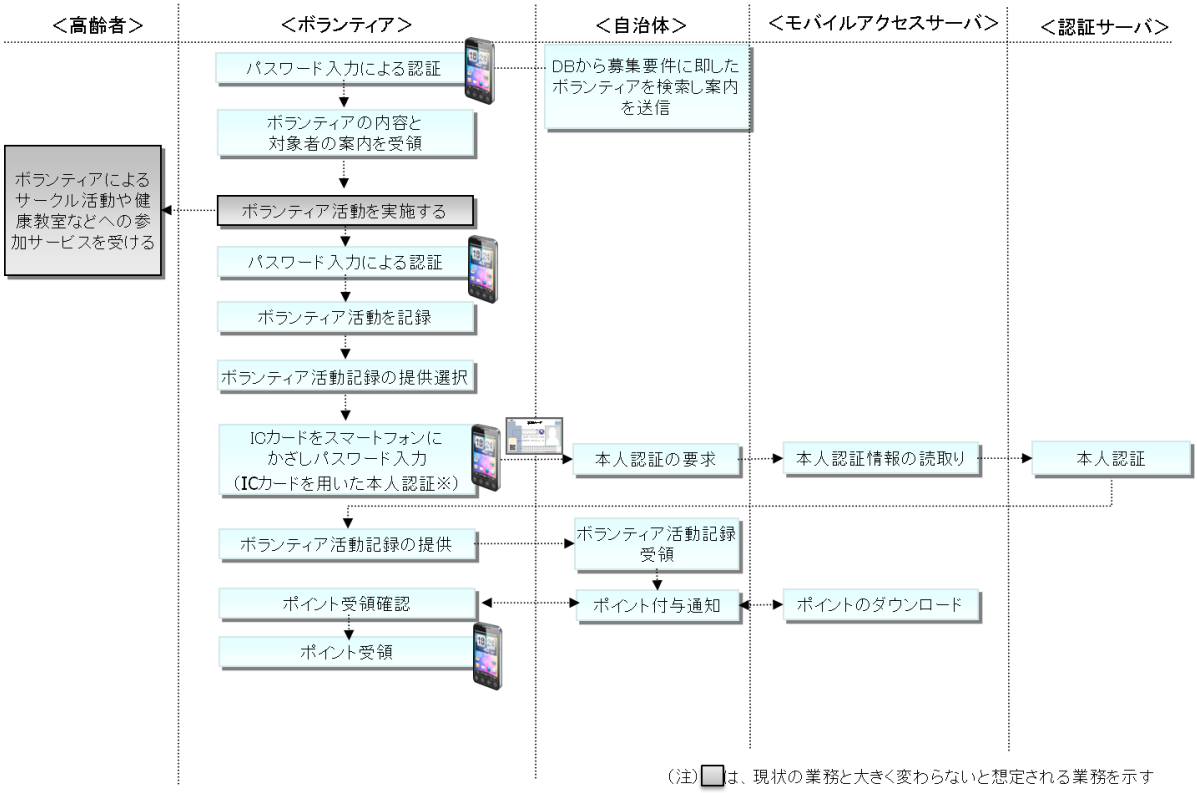


図 4-26　ボランティア活動の実施と活動情報の提供（保証レベル３）

iii）見守り（緊急通知）ボランティア活動の実施と活動情報の提供（保証レベル３）の運用フローを図 4-27 に示す。

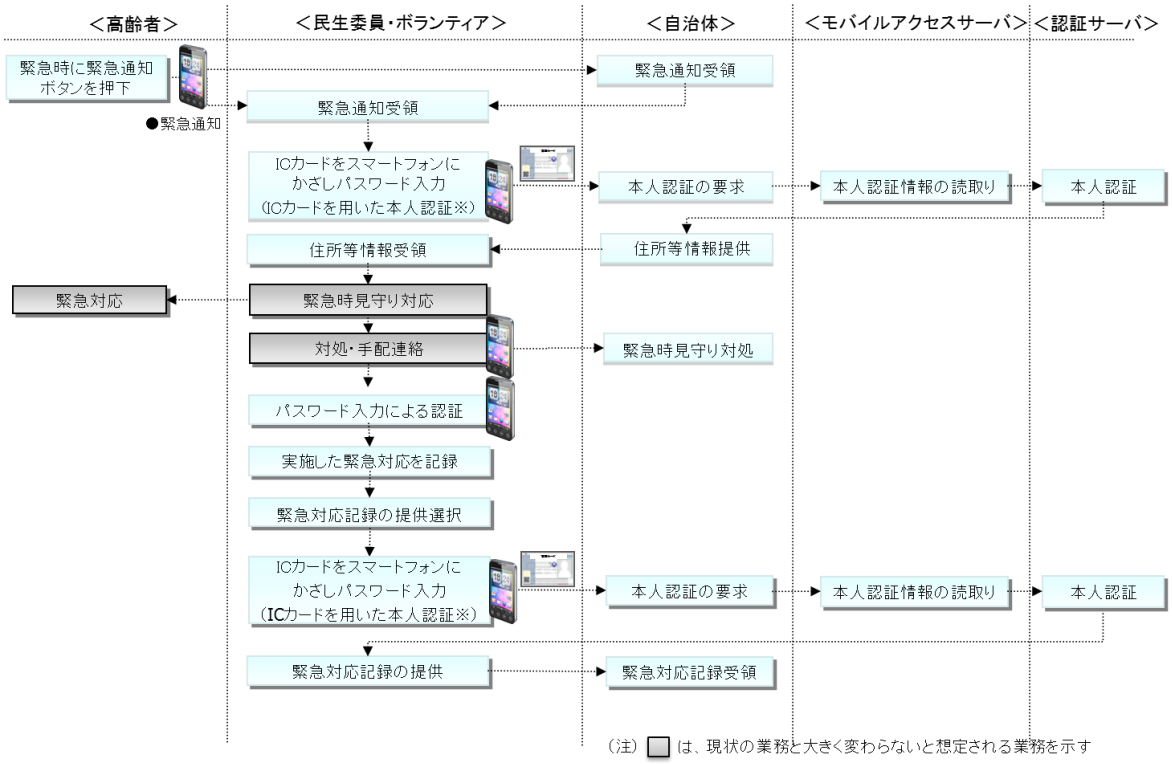


図 4-27　見守り（緊急通知）ボランティア活動の実施と活動情報の提供
（保証レベル３）

iv）民生委員への一人暮らし高齢者のリスト提供と現況報告（保証レベル４）の運用フローを図 4-28 に示す。

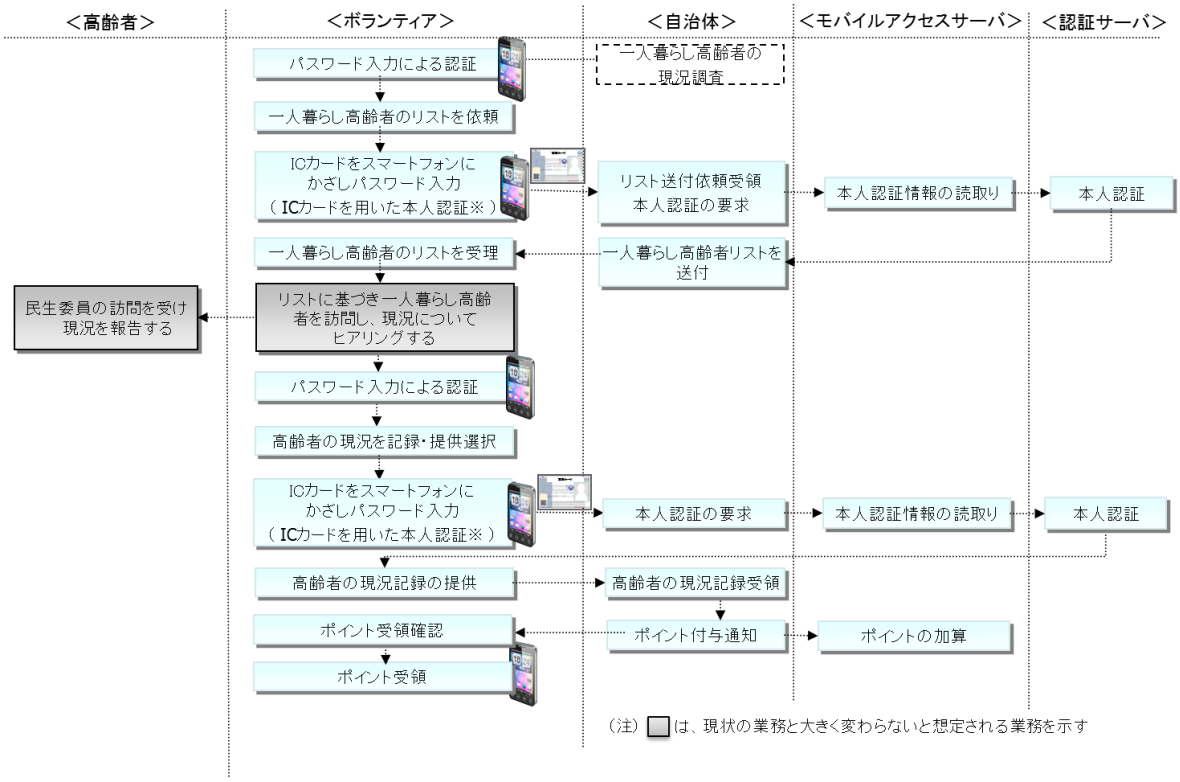


図 4-28　民生委員への一人暮らし高齢者のリスト提供と現況報告（保証レベル４）

⑨行政手続きの電子化：住民票等の交付

i）住民票等の交付（保証レベル２）の運用フローを図 4-29 に示す。

事前にスマートフォンで電子申請し、窓口端末にスマートフォンをかざし、住民登録することも可能。

図 4-29　住民票等の交付（保証レベル２）

ii）住民登録その他利用（保証レベル３）の運用フローを図 4-30 に示す。

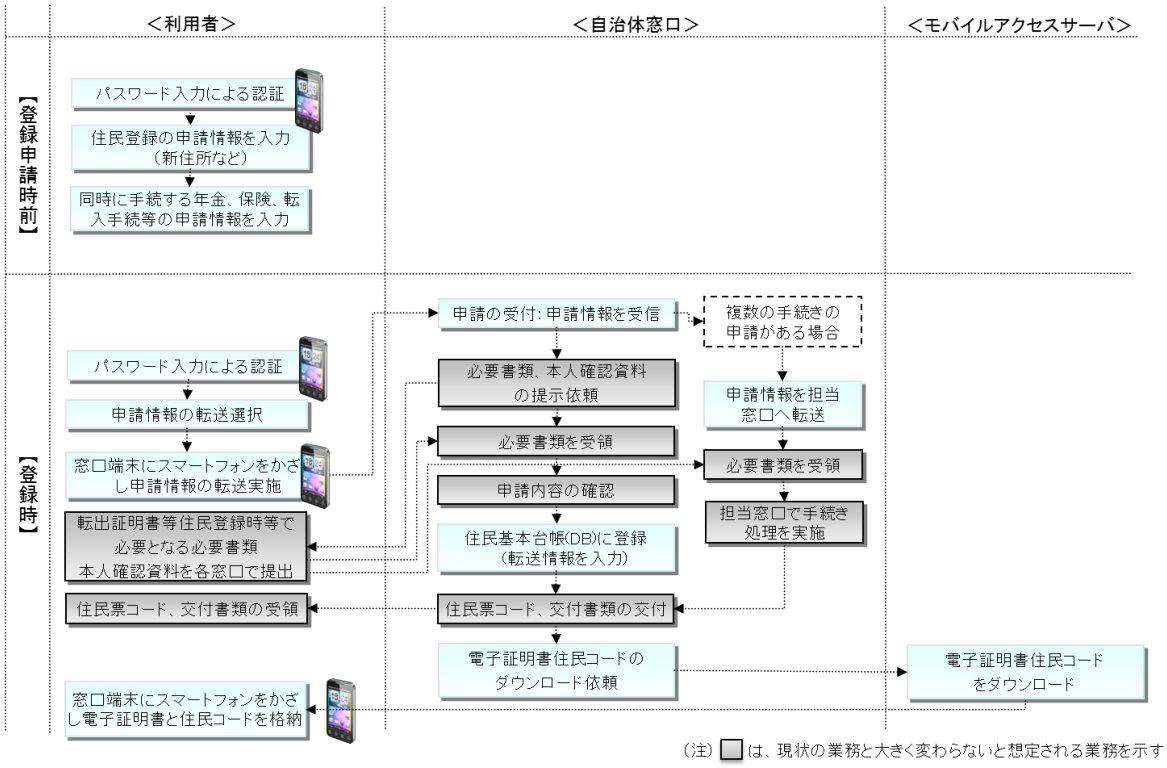


図 4-30　住民登録その他利用（保証レベル３）

⑩公金収納の電子化

i）公金収納の電子化（保証レベル３）の運用フローを図 4-31 に示す。

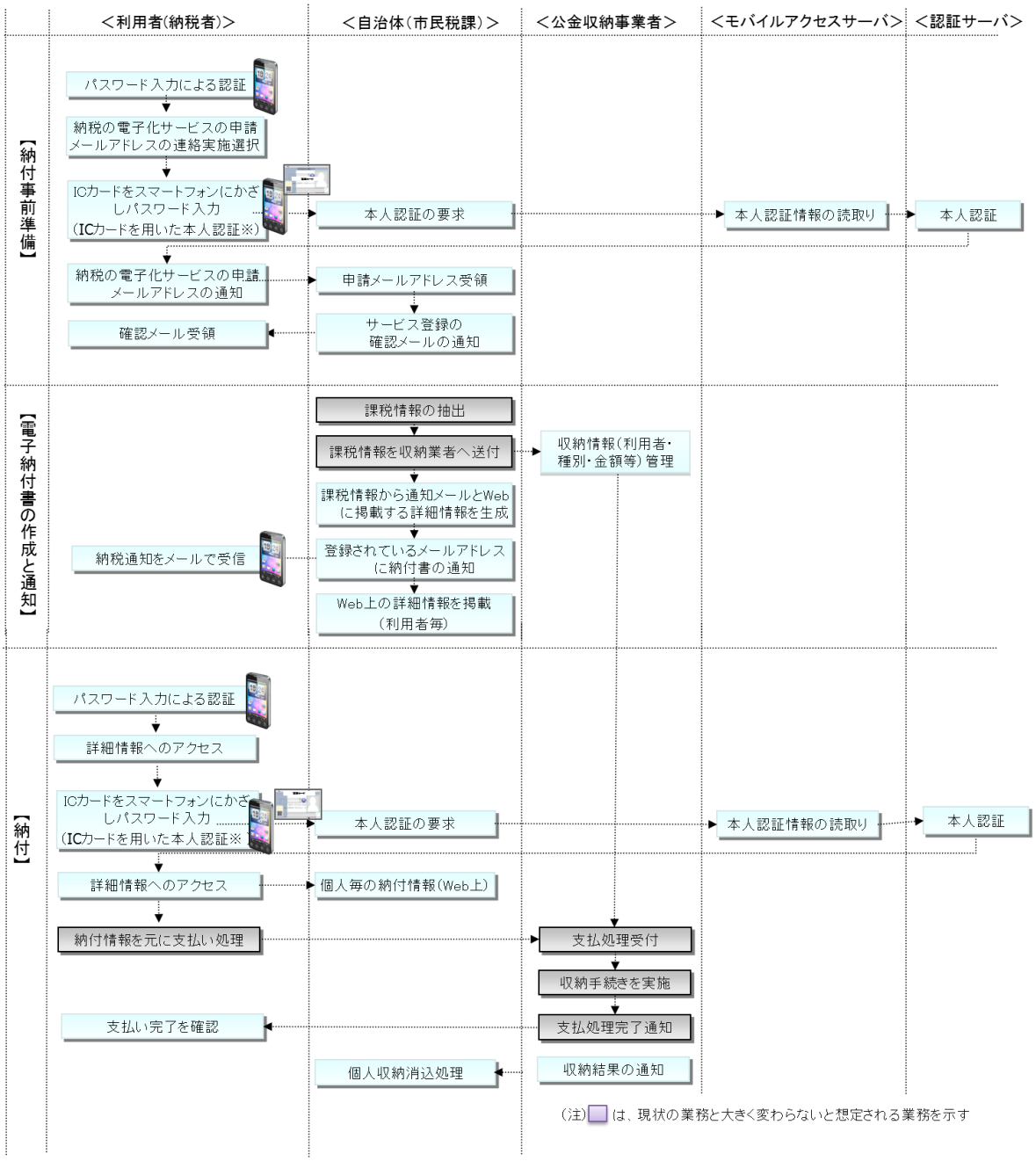


図 4-31　公金収納の電子化（保証レベル３）

(3) 自治体におけるスマートフォンを活用した場合の地域通貨利用での運用

スマートフォンによる地域通貨での利用許可、ポイント付与、ポイント確認の運用フローを図 4-32 に示す。

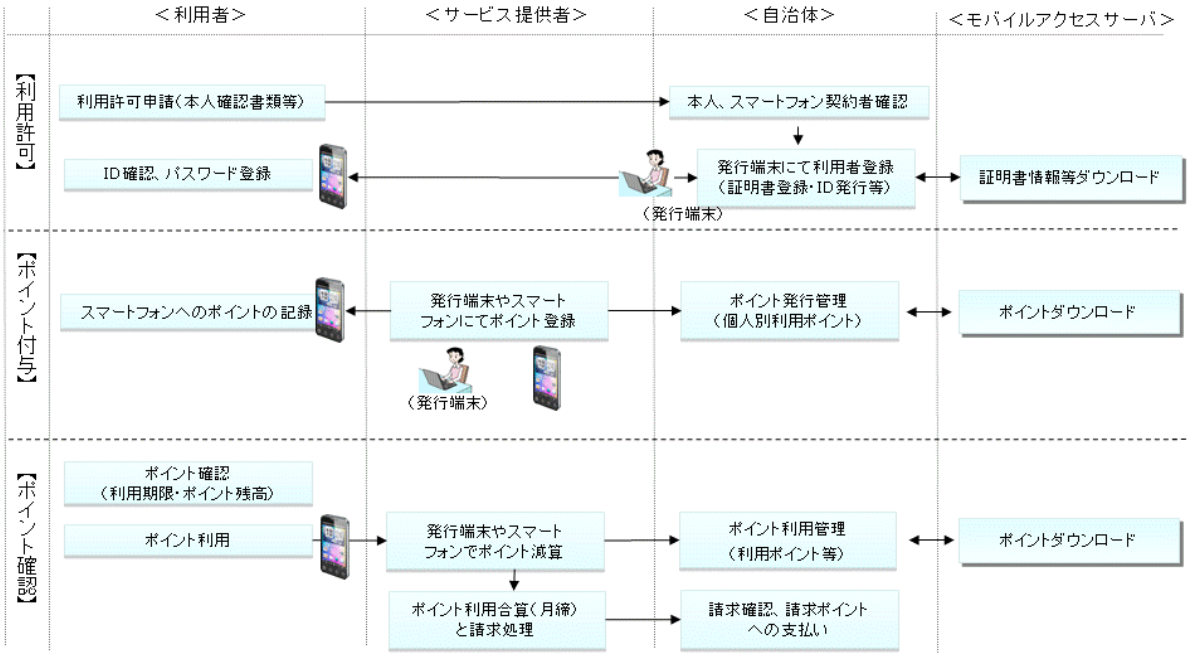


図 4-32　利用許可、ポイント付与、ポイント確認の運用フロー

また、スマートフォンによる地域通貨でのポイント利用の運用フローを図 4-33 に示す。

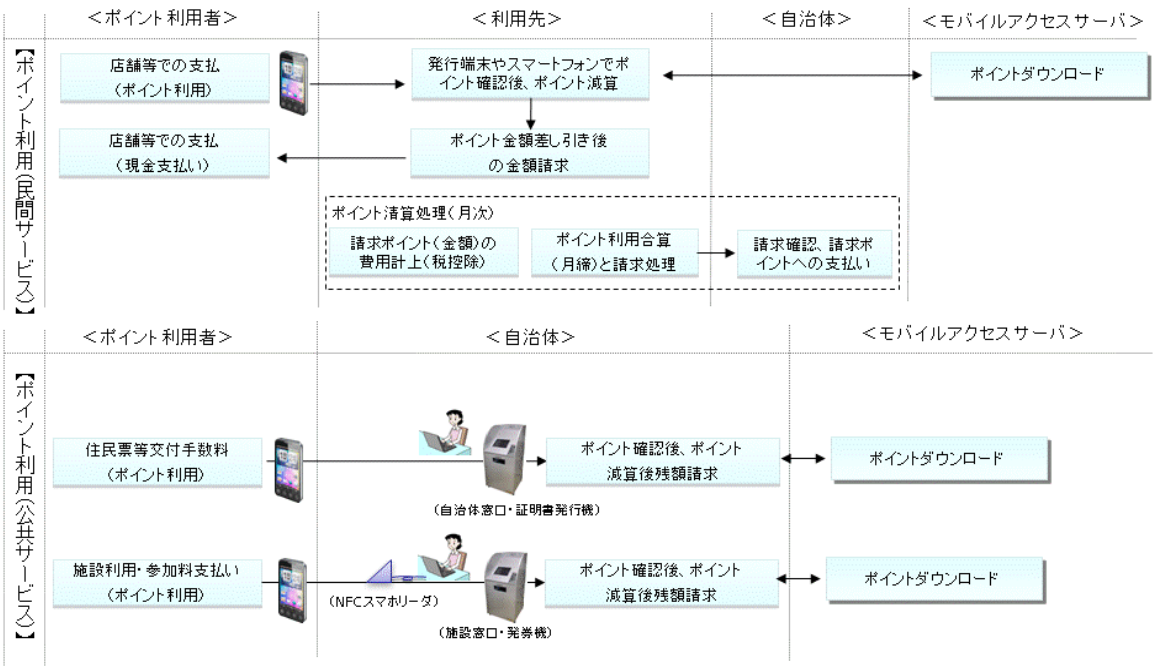


図 4-33　ポイント利用の運用フロー

(4) 金融機関（保険会社）におけるスマートフォンを活用した場合の運用

金融機関（保険会社）におけるスマートフォンを活用した場合の運用フローを図 4-34 に示す。

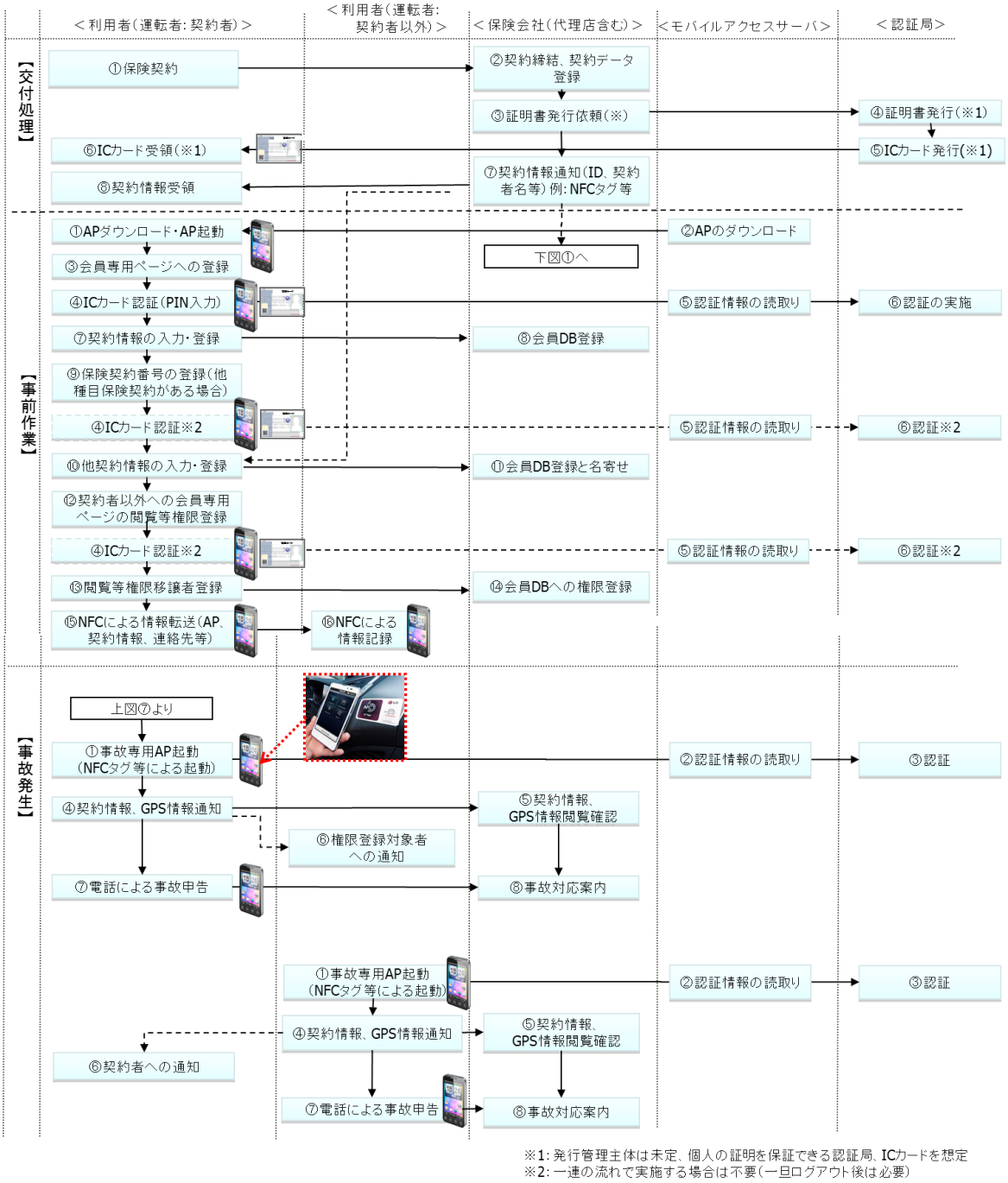


図 4-34　運用フロー

4.4.7. まとめ

適用サービスである、高齢者向け支援サービス、行政手続きの申請手段の電子化、公金収納の電子化サービス、保険契約情報の閲覧・保険加入の申請・事故情報の申告サービスの具体的なサービスの流れや想定効果と実現課題を明らかにするため、サービス提供機関（自治体と金融機関）からのヒアリングを実施し、セキュリティレベルや、運用や制度などに関するコメントを基に検討を行った。

高齢者支援サービスの高齢者の健康状態の記録と管理、健康状態と介護予防活動記録の統計分析への利用では、高齢者個人の管理による介護予防への意識向上と自治体の統計分析による施策立案の効果が期待されるが、高齢者の IT 機器への不慣れなどからスマートフォンでの操作性に関する課題やスマートフォンへのキータッチによる入力、スマートフォンと情報を転送するために機器に関する課題や統計情報活用における個人情報管理等制度面の課題を明らかになった。

また、高齢者支援サービスのもう一つのサービスである、ボランティア活動の継続的な促進では、インセンティブによるボランティア活動への活性化が期待されるが、ボランティア活動の実施確認のスマートフォンへの記録に関する方法やボランティアの運用ルール化、見守りにおける高齢者の個人情報の扱い等、制度面の課題が明らかになった。

行政手続きの申請手段の電子化では、住民の待ち時間解消など利便性向上の効果が期待されるが、スマートフォンを利用して本人確認を行う際の記録情報の扱いに関する課題を明らかにするとともに、証明書発行と住民登録等の申請では住民基本台帳法など制度的に自治体のみで解決できない課題があることが明らかになった。

公金収納の電子化では、住民の支払い方法の多様化による収納率向上や業務コスト削減の効果が期待されるが、スマートフォンへのメール通知の不達に関する技術的要件や制度面で電子的手段への適用がないなどの課題が明らかになった。

保険契約情報閲覧、保険加入申請、事故情報申告では、緊急時に必要な基本情報の本人と金融機関（保険会社）との間での迅速な送受信など効果が期待されるが、緊急時のスマートフォンで直ぐに利用できることとパスワード入力の操作性との背反する課題などが明らかになった。

地域ポイントの運用面では、スマートフォン等でいつでもポイント管理や利用ができるなどの効果が期待されるが、行政サービス（特に納税）にポイントを利用することに対する制度課題が明らかになった。

また、スマートフォンにおける運用の検討について、保証レベル 3 以上のセキュリティレベルでの認証方式に基づく運用の検討を行い、運用フローを明確にした。スマートフォン利用時の本人認証や証明書情報、情報の格納媒体などの課題が明らかになるとともに、モバイルアクセスシステムの適用範囲が明確になった。

4.5. 最適なサービスの課題と対策案の検討

4.5.1. 検討の考え方

最適なサービスに対する運用、制度の課題から想定される対応策を検討する。
検討に当たっては、以下の具体化したサービスから抽出した運用、制度の課題に対する対応策を案として整理する。

＜対象サービス＞

① 高齢者向け支援サービス：介護予防における高齢者やボランティア向けポイント活用
② 行政手続きの電子化：各種証明書発行、住民登録、その他施設利用の手続き電子化
③ 公金収納の電子化：納税等の納付書の電子化と支払いの電子化
④ 保険契約情報閲覧、保険加入申請、事故情報申告

4.5.2.　高齢者向け支援サービス

(1) 高齢者の健康状態の記録と管理、健康状態と介護予防活動記録の統計分析への利用に関する課題と対応策（案）

本サービスのスマートフォンにおける共通基盤関連の課題と対応策を表 4-28 に、運用上の課題と対応策を表 4-29 に、また制度上の課題と対応策を表 4-30 に示す。

表 4-28　スマートフォンにおける共通基盤関連の課題と対応策

No	スマートフォンに関する課題	対処策（案）
1	IT 機器に不慣れな高齢者でも、容易にサービスを受けられるような、スマートフォン上の操作も含めたサービス運用性（サービス機能やサービスの流れ）の検討	高齢者でも抵抗感なく直感的に操作できるよう、以下の点を考慮してサービス運用も含めた操作性を実現する。 • 容易に利用環境の設定ができるようにする • タッチ操作を前提とする • 表示上の文字フォントやアイコンを大きく表示し押し間違いがないようにする • 画面上に表示するサービスはよく使われる機能に限定し、また、必要処理手順をあらかじめ一つのアイコンで操作できるよう工夫する • キーボードでの入力をできる限り排除し、選択的な入力方法を採用する • できる限り画面が分岐しないような流れとする　など
2	介護予防プログラムへの参加記録や介護予防相談時の相談内容や指導内容を記録する際に、従来の介護予防手帳への手書き記入からスマートフォン上への入力に変わることによるサービス提供者側の運用負荷	• プログラム実施会場に参加記録用の端末を用意し、そこにスマートフォンをかざすことにより、参加記録をスマートフォン上に記録することにより人的負荷を軽減する。 • 相談内容や指導内容の記入（記録）は、相談員が PC 等に入力した内容を一括してスマートフォンに読むことや手書き入力等により運用負荷を軽減する。
3	介護教室などスマートフォン上に参加記録とポイントを付与する場合の環境（PC と IC カードリーダ、NW 環境など）	教室の管理者保有のスマートフォンにより、参加者のスマートフォンにポイント書き込みを行う仕組みを実現する。
4	外部端末とスマートフォンがお互いに通信する機能（NFC 等）の実装	オンライン接続以外に、対象サービスシステムの外部端末とお互いに通信するための通信機能として、NFC のような短時間かつ非接触で必要な情報を転送できる通信機能を実装する。

表 4-29　運用上の課題と対応策

No	運用上の課題	対処策（案）
1	ポイント付与を行う場合の確認方法（ポイント付与対象行為の確認方法）の検討	会場にて職員が参加者の確認をスマートフォンのリーダモードで実施し、利用者のスマートフォンにポイントに書き込む仕組みを実現する。
2	収集データの保管期限や利用状況の問合せ対応	統計分析に必要な保管期限を本人の同意の元に策定する。 利用状況の問い合わせに活用可能な証跡管理の仕組みの実現
3	情報提供に対し、付与する察度ポイントの原資（自治体負担）と既存の察度ポイントの原資（事業者負担）を統合して管理する必要があるが、そのための管理主体や運用方法	行政が準備した原資の内容によってポイント利用範囲が異なることも想定され、ポイントやその原資と利用状況を管理するための管理組織を第三者機関として独立させ、民間だけでなく、行政でのポイント利用に当たっての運用管理体制を構築する。
4	高齢者による基本チェックリストの登録や健康状態等の情報提供時に、オンラインで地域通貨（ポイント）を付与する仕組みの検討	情報提供を受けた際に、サーバから付与するポイント数をスマートフォン上のアプリケーションに送付し、スマートフォン上のポイント数を更新するような方式を実現する。

表 4-30　制度上の課題と対応策

No	制度上の課題	対処策（案）
1	自治体での統計利用時の個人情報の管理や匿名化方法の検討	統計利用時にはガイドラインに沿って管理・運用規定を設け、個人情報保護条例に即した制度を構築する。 匿名化は個人が特定できる情報を纏めて蓄積しないなど、分散管理を実施する。

(2) ボランティア活動の継続的な促進に関する課題と対応策（案）

本サービスのスマートフォンにおける共通基盤関連の課題と対応策を表 4-31 に、運用上の課題と対応策を表 4-32 に、また制度上の課題と対応策を表 4-33 に示す。

表 4-31　スマートフォンにおける共通基盤関連の課題と対応策

No	スマートフォンに関する課題	対処策（案）
1	ボランティア活動を実施した際の第三者（ボランティア本人以外の自治体など）による実施確認の方法	• 個別に行うボランティア活動については、ボランティア実施者の実施確認を相手のスマートフォンより電子署名を付加した情報を受け取ることで実施確認とする • 事前に計画されて実施されるプログラムの実施結果については、ボランティア活動の実施報告内容によって実施したことを確認する

表 4-32　運用上の課題と対応策

No	運用上の課題	対処策（案）
1	ボランティアの意識づけに有効なポイントの付与基準やポイント位置づけ（利用の範囲）の検討	＜ボランティアへのポイント付与基準＞ ボランティアのスキルと作業量（時間数）が効果的に反映できるようなポイント付与基準が望ましい。ボランティア活動を必要なスキルレベルで分類し、その分類のレベルと作業時間との積によってポイントを付与する。 ポイント数 = 基準ポイント/単位時間当たり×ボランティア活動の分類による係数×作業時間数 ＜ポイントの利用範囲＞ 介護予防ボランティアに付与するポイントの財源を特別会計とすれば、ポイントの利用は介護予防事業の範囲となるが、一般財源を原資とする場合、利用範囲を定めない察度ポイントと同様の位置づけで運用することができ、利便性が高く望ましい。
2	ボランティアへの利用登録方法と権限の付与方法（権限によって厳密な本人確認が必要な場合の確認方法）	ボランティアにもランク付けを事前に行い、個人情報を閲覧受診、可能な権限などを規定する。
3	ボランティアの活動報告を自治体へ報告する、運用ルールの規定化	ボランティア不在の場合には、予め登録（緊急対応に同意あるは指定した）された近隣のボランティアへのエスカレーションを行う仕組みを用意する。
4	ボランティアの活動報告を自治体へ報告するに当たり、運用ルールの規定化	報告内容の定型化（日時、プログラム名、活動内容、活動結果、報告事項、等）や、報告時期（月次等）などの運用を定める。

表 4-33　制度上の課題と対応策

No	制度上の課題	対処策（案）
1	ボランティアへの付与ポイントの財源を確保する必要がある。	特別会計予算の利用が難しいため、一般財源の利用を図る必要がある。ただし、介護予防ボランティアのポイント利用については、地域支援事業交付金の利用の可能性がある（「介護保険制度を活用した高齢者のボランティア活動の支援（厚生労働省、平成 19 年 5 月 11 日）」）
2	見守りボランティア時のボランティア等への高齢者個人情報の提供に対する個人情報保護の制約	見守り時の個人情報の提供に当っては、個人情報提供の運用に関する申請書を提出することにより実現する。 個人情報の提供先は「ボランティア」とし、ボランティア個人を特定しない。
3	見守りボランティア時に見守り情報を第三者（自治体）に報告する場合の本人同意	事前に申請した個人情報の運用に基づき、本人の同意を求める。

4.5.3. 行政手続きの申請手段の電子化サービス

(1) 住民票等の交付に関する課題と対応策（案）

本サービスのスマートフォンにおける共通基盤関連の課題と対応策を表 4-34 に、運用上の課題と対応策を表 4-35 に、また制度上の課題と対応策を表 4-36 に示す。

表 4-34　スマートフォンにおける共通基盤関連の課題と対応策

No	スマートフォンに関する課題	対処策（案）
1	交付の際の対象とする行政手続きとして、住民票、印鑑証明、税関連証明書等を想定しており、これらの証明書発行を電子化手続きで行う際の本人性の確認方法	サービス開始前のサービス利用申請の段階で、自治体窓口にて本人確認のために必要な電子証明書をスマートフォンに格納する。この手続きの本人確認は、本人確認書類に基づき行う。
2	スマートフォンと通信するための設備（PC、IC カードリーダ等）の整備	NW や PC 等環境がない施設の場合、施設管理者保有の NFC 機能を実装したスマートフォンにより、参加者の NFC 機能を実装したスマートフォンと読み書きを行う仕組みを実現する。

表 4-35　運用上の課題と対応策

No	運用上の課題	対処策（案）
1	現状、本人確認の記録として免許証番号を記録しているが、スマートフォンでの本人確認を行う際の記録対象情報	申請手続きの本人確認の記録として、原本性が求められるため、スマートフォンの電子的な仕組みでは、公的個人認証情報とする。
2	複数の証明書が存在し、1回の申請処理で交付するワンストップ処理を行う際、税務などの専門性が必要となる業務処理との連携方法	行政窓口でのワンストップ窓口として、必要書類の申請手続きに必要な情報を一括入力し、窓口で一括して入力することで、申請手続き時のワンストップ化を実現する個々の事務手続きは、各課の窓口にて行う。

表 4-36　制度上の課題と対応策

No	制度上の課題	対処策（案）
1	現状、複数のカードで実施しているサービスを、一つのスマートフォンに統合する場合の統合方法（浦添市の場合、「てだカード」（市民カード）と「察度」カード（地域通貨）を1台のスマートフォンに統合する）	複数のカードで実施しているサービスを、一つのスマートフォンに統合する場合には、NFC 準拠のインタフェースでカード情報を規定する。てだカードのような磁気カードの場合は、磁気カードから IC カードへの技術的な変更を行う。
2	現状、複数のカードで実施しているサービスを、一つのスマートフォンに統合する場合、既存のサービスで認めている代理申請への対応方法	複数のカードを1枚に統合するのではなく、それぞれのカードを独立して一つのスマートフォンに統合することにより、既存サービスで認めていた代理申請の扱いを可能とする。

(2) 住民登録等その他利用に関する課題と対応策（案）

本サービスのスマートフォンにおける共通基盤関連の課題と対応策を表 4-37 に、運用上の課題と対応策を表 4-38 に、また制度上の課題と対応策を表 4-39 に示す。

表 4-37　スマートフォンにおける共通基盤関連の課題と対応策

No	スマートフォンに関する課題	対処策（案）
1	交付の際の対象とする行政手続きとして、住民登録、印鑑登録、住所変更などの各種届出を想定しており、これらの登録手続き申請の電子化を行う場合の本人性の確認法	サービス開始前のサービス利用申請の段階で、自治体窓口にて本人確認のために必要な電子証明書をスマートフォンに格納する。この手続きの本人確認は、本人確認書類に基づき行う。
2	公共施設等でスマートフォンを読み取るための環境（PC と IC カードリーダ等）の整備	NW や PC 等環境がない施設の場合、施設管理者保有の NFC 機能を実装したスマートフォンにより、参加者の NFC 機能を実装したスマートフォンと読み書きを行う仕組みを実現する。
3	氏名等の外字処理に関連して、スマートフォンと自治体システムの外字コード体系の共通化	スマートフォン上で、住民基本台帳ネットワーク統一文字をサポートし、最低限、住民基本台帳ネットワーク同等レベルの文字のサポートする案が考えられるが、登録文字種が自治体間で統一されていないため、スマートフォン上では新字での扱いとし、自治体システムで外字に変換する。

表 4-38　運用上の課題と対応策

No	運用上の課題	対処策（案）
1	現状、本人確認の記録として免許証番号を記録しているが、スマートフォンでの本人確認を行う際の記録対象情報	申請手続きの本人確認の記録として、原本性が求められるため、スマートフォンの電子的な仕組みでは、公的個人認証情報とする。

表 4-39　制度上の課題と対応策

No	制度上の課題	対処策（案）
1	既存の登録手続き申請方法について、市の条例で規程している場合、カードだけでなくスマートフォンを用いて申請可能となるよう改正する必要がある。	市の条例で規程される、既存サービスで利用するカードについて、スマートフォンに格納されたカードも該当サービスで使用するカードとして利用できるよう、条例の改定を行う。

4.5.4.　公金収納の電子化サービス

(1) 市民税等の納付書送付と支払いサービスに関する課題と対応策（案）

本サービスのスマートフォンにおける共通基盤関連の課題と対応策を表 4-40 に、運用上の課題と対応策を表 4-41 に、また制度上の課題と対応策を表 4-42 に示す。

表 4-40　スマートフォンにおける共通基盤関連の課題と対応策

No	スマートフォンに関する課題	対処策（案）
1	スマートフォンへ、メールにより通知書を送付する場合、その通知の到達確認の技術的要件の明確化	スマートフォンにメールによる通知書を送付する場合、メール通知の不達状況を発信者側、または、利用者に通知する次のような技術的な対策（案）を用意する。 ・プロバイダのメールサーバでの送信エラーの発信者側への通知（メールアドレスの誤り等） ・スマートフォンの電源 OFF などで受診できない場合にセンターに蓄積されたメールが一定期間読み出されなかった時の発信者側への不達通知 ・スマートフォン側で正常にメールを受信できなかった場合に、受信エラー状態を管理し、発信者、並びに、利用者への通知

表 4-41　運用上の課題と対応策

No	運用上の課題	対処策（案）
1	紙の通知書（納付書）と電子通知が併存する場合の通知運用の負荷（紙での納付と電子通知の選択方法、課税処理後の処理の流れなど）	紙による通知書（納付書）と電子通知が併存する場合の運用処理を以下のように行うことにより、紙による送付と電子通知が併存する場合の運用負荷の軽減を図る。 ・通知書（納付書）の配信方法の選択：住民は納付書の通知方法を選択出来ることとし、デフォルトは紙での配信方法とする。電子通知を希望する住民は、事前に電子通知の申請と配信先のメールアドレスの登録を行う登録先の誤りがないことを確認するため、登録したメールアドレスに電子通知の設定の完了通知を送付する。 ・通知書（納付書）の送付処理：課税計算後、納付方法によって郵送配布による納付情報と電子通知による納付情報に分け、それぞれの通知書（納付書）の送付処理を行う。
2	通知書（納付書）の電子通知時のメールアドレス変更手続きとメール不達時の再送処理時の通知運用の負荷（従来の督促処理を行うなど）	・電子通知を選択している住民のメールアドレスに変更があった場合は、電子通知の申請と同等の手続き処理を行い、メールアドレスの変更を行う等の運用により、運用負荷が負担にならないよう配慮する。 処理の時間差によって旧メールアドレスに納付情報を送付し、不達となった場合は、紙による督促処理を行う。 ・電子通知の不達時の運用処理：電子通知が不達になった場合は、再度、同メールアドレスに電子通知を行う再度不達になった場合は、通知書（納付書）の通知方法を紙による方法に変更し、郵送による督促処理を行う。

表 4-42　制度上の課題と対応策

No	制度上の課題	対処策（案）
1	通知書の送付に関する、地方税法 第20条(書類の送達)で規定されている郵送または信書便による送達と到達時の規程の電子通知手段に対する拡張と改定	①　納税告知書等の電子的方法による通知については、政府の情報通信技術利活用のための規制・制度改革に関する専門調査会報告書(平成23年度3月）にて、以下のように検討されている。 • 民法 97 条において、隔地者に対する意思表示が有効となるのは通知が相手方に到達した時と規定されており、行政手続オンライン化法第 4 条第 3 項は、この民法の一般原則に基づき、オンライン手続においては「処分通知等を受ける者の使用に係る電子計算機に備えられたファイルへの記録がされた時」を「到達」とすることを定めたものと、されている。 • 本件の対処方針：総務省は、行政手続オンライン化法第 4 条第 3 項に基づく行政処分の電子的な方法による通知について、具体的にどのような方法が可能であるかを示すガイドライン等を作成し、公表する。＜平成 23 年度中措置＞ 納税告知書等の送付に関する手続を所管する財務省、総務省は、上記ガイドライン等を踏まえ、納税告知書等の電子的な方法による通知の実施について、費用対効果の面も含めて検討する。＜平成 23 年度以降検討開始＞ ②　①の状況より、スマートフォン内へのメールによる通知書の通知を上記、使用者の電子計算機へのファイルの記録としてみなすよう提案するが、ガイドラインが示されるまで、郵送による通知と併用する。
2	メールにより通知書を送付する場合、その通知の到達確認の条件が制度上、明確でない	・制度的には、上記の示すように、今後作成されるガイドラインによるが、電子的な通知をメールによって行う際の到達条件を以下の案のように明確にする。 ・到達条件（案）：　電子通知としてのメールがスマートフォン内のメールが格納されるファイル（フォルダ）に格納された状態で、メール読み出し時に、人が読める状態になっていること（文字化け等していないこと)。 ・上記条件を想定する場合、技術的な対策として、スマートフォン側で正常にメールを受信できなかった場合に、受信エラー状態を管理し、送信者、並びに、利用者に通知する仕組みを用意する。

4.5.5.　事故申告におけるスマートフォンの利用

(1) 事故申告におけるスマートフォンの利用に関する課題と対応策（案）

本サービスのスマートフォンにおける共通基盤関連の課題と対応策を表 4-43 に、運用上の課題と対応策を表 4-44 に、また制度上の課題と対応策を表 4-45 に示す。

表 4-43　スマートフォンにおける共通基盤関連の課題と対応策

No	スマートフォンに関する課題	対処策（案）
1	緊急時にスマートフォン AP が直ぐに利用できる仕組みの検討（AP 起動時に本人確認ためのパスワード入力は実行上不可能）	• NFC タグを常備しておくことで、スマートフォンを近づけると AP が起動して、自動的に事故情報の発信を行う（スマートフォンには契約者情報が登録されており、NFC タグとスマートフォンの契約者情報：ID 等がマッチした場合、パスワード等の入力を不要とする）
2	スマートフォンの機種変更、キャリア変更時の再登録	• 契約者 ID 等の情報管理や AP 配布のプラットフォームにより、通信キャリアや機種に依存しない配布管理の仕組みによる対処 • NFC タグと IC カードがあれば､機種等の変更時に設定等が登録できる仕組み
3	事故専用アプリへの情報登録や保険会社への発信など運転者による事前の情報入力・操作を実施する仕組みの検討	• 保険契約時に代理店などが専用アプリのダウンロードと情報入力を補助する仕組み 情報登録のための契約者向けの IC カードと NFC タグを配布し、ﾛｰｶﾙ通信により、AP ダウンロードや設定までの実施を行う（事前に契約者情報を NFC タグに記録しておき、設定時には IC カードにて本人認証を行うことで NFC タグと IC カードによる契約者情報がマッチした場合にのみ情報設定を可能とする）
4	他種目保険番号の誤入力とその際の本人連絡等の保険会社の負荷への対応（本人であることの一意の特定が必要）	• 保険契約毎に契約者向けの NFC タグを配布し、契約者情報を登録したスマートフォンを近づけ､IC カードの認証を経て契約番号の登録を可能とする 公的な IC カードと認証情報の活用
5	携帯電話圏外、電池切れ、故障、紛失、アプリ障害における代替策の用意	通話圏外、電池切れ、その他障害等は従来の通話による問合せ対応とし、配布した NFC タグに IC カードやスマートフォンの登録情報とは別の問合せ ID の表示による対処
6	紛失した場合や情報を送信する際の情報漏洩防止策	• スマートフォンの紛失時には IC カードや NFC タグがないと閲覧や情報登録ができない仕組み • 情報送信時は SSL 等による暗号化対策

表 4-44　運用上の課題と対応策

No	運用上の課題	対処策（案）
1	スマートフォンアプリ対応と電話応対の効果的な運用	• 専用 AP には登録情報を送信する機能とインターネット電話のキャリアフリーの番号による発信機能を搭載し、AP 起動で両方の機能を実現する

表 4-45　制度上の課題と対応策

No	制度上の課題	対処策（案）
1	保険業法や金融商取引法、保険法などに対する金融庁確認	• 現行の法制度上は、電子的な記録や申請に対する明確な規定はないが、本人が権限を委譲したことを証跡として残すための規制が必要である
2	本人を特定し認証するための公的情報を活用する場合の民間活用に対する制度見直し（自動車保険に必要な免許証情報などをスマートフォンに格納する場合、免許情報の利用について警察庁への確認、公的個人認証の民間利用への制度改正など）	• IC 免許証など公的機関が発行する IC カードを利用した限定的な認証サービスの活用 • 公的個人認証サービスの法律（電子署名及び認証業務に関する法律）に対する認証用途の証明書を制度的に付加し、特定民間認証事業者の認証業務を許可する

4.5.6. モバイルアクセスシステムを検討する上での課題と対応策（案）

本事業におけるモバイルアクセスシステムを検討する上での技術上の課題と対応策を表 4-46 に示す。また、運用上の課題と対応策を表 4-47 に、制度上の課題と対応策を表 4-48 に示す。

表 4-46　技術上の課題と対応策

No	技術上のの課題	対処策（案）
1	本人確認の手段として、本人用電子証明書をスマートフォンに格納する場合の安全な初期設定手段 ①運用案１：自治体窓口で証明書を格納し利用可能とする。 ②運用案２：ネットワーク経由でスマートフォンに証明書を発行し利用可能とする。	①安全性、確実性の観点から、自治体窓口で本人用電子証明書の格納を行う際、本人確認書類にて本人確認を行う。また、この作業は住民からの申請時に行うだけでなく、転入時に行うことにより、スムーズな導入を行うことができる。なお、電子証明書の格納と同時に、本人の住所、氏名、生年月日、性別に加え、各サービス機関固有の情報（例えば、自治体の個人コードなど）を格納し、以後の行政手続きなどの電子化サービスで利用することができる。 ②ネットワーク経由での発行は、公的 IC カードをスマートフォンにかざし、本人認証後、ID、PW を登録住所に書留郵便で送付。公的 IC カードと ID、PW を元に証明書を発行する
2	電子証明書等の証明書情報としての必要情報（例、4 情報等）	本人確認のため、証明書情報として、氏名、住所、性別、生年月日の 4 情報を基本情報として格納することが望ましい。
3	電子証明書等の証明書情報のセキュリティレベルに応じた格納媒体（例、耐タンパデバイス等）	適用サービスの実施の際に、レベル 4 の保証レベルが必要であるため、証明書情報は、耐タンパデバイスに格納する必要がある。
4	複数カードをひとつのスマートフォンで安全に利用可能とする格納媒体の検討	GP に準拠した方式にすることで各サービス提供機関が提供した耐タンパデバイス内各カードアプリレットを安全に格納することが可能となる。
5	スマートフォンの契約者が異なる場合の利用許可の運用方法	スマートフォンの契約者が異なる場合でも、そのスマートフォンの実質的な利用者の意思により、本人確認のための電子証明書の格納を行うことによりサービス利用を可能とする。
6	厳密な本人確認や端末所有者確認を行う際の運用方法	スマートフォンへの証明書等の交付業務、ならびに、失効に伴う業務は、自治体窓口にて実施する。その際の本人確認は現行の住基カードの発行時と同レベルが望ましい。
7	サービスを受ける際に、複数台のスマートフォン（耐タンパデバイス）でも利用可否	必ずしも不可ではないが管理上、不正が見抜けない可能性が想定される。
8	電子証明書等の証明書情報を格納する際の発行端末の認証方法	利用者端末と発行端末にて相互認証を実施する。

9	スマートフォンの利用一時停止申込みの方法と本人確認方法（電話による停止受付の本人確認）、また、その際の証明書情報の処理方法	スマートフォンの利用一時停止申込は、利用停止手続きを準用し、本人による申請書による手続きを行う。紛失等による緊急時の利用停止は、サービス提供機関への連絡を行うことにより停止し、その際の本人確認は、住所、電話番号、生年月日の確認によって行う。
10	スマートフォン紛失時等の再利用申請時の証明書情報の処理方法	再利用時には、初期登録と同様に証明書情報を再度登録する。ただし、すでに発行している登録情報を使用時に無効とする。
11	スマートフォンとのローカル通信での情報のやり取りを考慮したモバイルアクセスサーバの設置と仕組みの実現	モバイルアクセスサーバは、個人認証情報やサービス提供時の情報のやり取りなどのゲートウェイ機能として提供される。 スマートフォン利用時の情報のやり取りには、オンラインでの情報のやり取りとローカル通信経由での情報のやり取りがあり、それぞれの情報のやり取りに際してモバイルアクセスサーバとの効率的、かつ運用も考慮したモバイルアクセスサーバムの設置とそれに対応したシステム仕様であることが必要となる。
12	IT 機器に不慣れな高齢者でも、容易にサービスを受けられるような、スマートフォン上の操作も含めたサービス運用性（サービス機能やサービスの流れ）の検討	高齢者でも抵抗感なく直感的に操作できるよう、以下を考慮してサービス運用も含めた操作性を実現する。 • 容易に利用環境の設定ができるようにする • 表示上の文字フォントやアイコンを大きく表示し押し間違いがないようにする • 画面上に表示するサービスはよく使われる機能に限定し、また、必要処理手順をあらかじめ一つのアイコンで操作できるよう工夫する • キーボードでの入力をできる限り排除し、選択的な入力方法を採用する • できる限り画面が分岐しないような流れとするなど
13	圏外、電池切れ、アプリ障害における代替策の用意	電池切れ、携帯電話圏外の際もローカル通信は可能とし、情報のやり取りを可能とする。
14	スマートフォンの機種変更、契約変更、故障、盗難・紛失といったイベントに応じたスマートフォンに対する処理をどうするか	機種変更時は失効処理を実施した上で新規機種への交付処理、故障および盗難・紛失時は一時停止処理を実施するなど、イベントに応じた処理を実施する。
15	公共施設等でスマートフォンを読み取るための環境（PC と IC カードリーダ等）の整備	NW や PC 等環境がない施設の場合、NFC 機能を実装したスマートフォンにより、利用者の NFC 機能を実装したスマートフォンと読み書きを行う仕組みを実現する。
16	氏名等の外字処理に関連して、スマートフォンと自治体システムの外字コード体系の共通化	スマートフォン上で、住民基本台帳ネットワーク統一文字をサポートし、最低限、住民基本台帳ネットワーク同等レベルの文字のサポートする案が考えられるが、登録文字種が自治体間で統一されていないため、スマートフォン上では新字での扱いとし、自治体システムで外字に変換する。

表 4-47　運用上の課題と対応策

No	運用上の課題	対処策（案）
1	スマートフォンにインストールする共通アプリ、モバイルアクセスサーバ等モバイルアクセスシステムに関わる運用主体をどうするか	モバイルアクセスシステムの運用は、サービスシステムも含めてサービス提供機関が行うことが考えられるが、サービス提供機関がスマートフォンを用いたサービスを迅速に提供するためには、運用負荷を抑えることが重要であり、そのためには、モバイルアクセスシステムを第三者のサービスベンダが提供することも考えられる。
2	携帯電話圏外、電池切れ、アプリ障害における代替策の用意	通話圏外、電池切れ、その他障害等は従来の通話による問合せ対応とし、配布されている IC カードやスマートフォンの登録情報とは別の問合せ ID の表示による対処。

表 4-48　制度上の課題と対応策

No	制度上の課題	対処策（案）
1	本人確認の方法として電子証明書を利用する場合の電子署名法への対応	スマートフォンに格納される電子証明書による本人確認は、通常の IC カード等で用いられる電子署名と同等の機能を有しており、電子署名法で定義される「電子署名」に該当すると想定される。
2	既存の登録手続き申請方法について、市の条例で規程している場合がある。	市の条例で規程される、既存サービスで利用するカードについて、スマートフォンに格納されたカードも該当サービスで使用するカードとして利用できるよう、条例の改定を行う。

4.5.7. まとめ

最適なサービスとして選定した、高齢者向け支援サービス、行政手続きの電子化、公金収納の電子化の各サービス、および、地域通貨をスマートフォンで利用する場合の運用、制度の課題について、想定される対応策を検討した。

対応策には、主にスマートフォンでの利用に関して、スマートフォンの操作性やサービス性、スマートフォンと情報のやり取りを行うための設備等の環境の対応策、行政手続きの電子化では、スマートフォンでのサービス利用時の本人確認の方法、公金収納の電子化では、スマートフォンへのメール通知の不達に関する技術要件などの対応策を示した。

サービスの運用や制度面の観点では、高齢者福祉サービスにおける、ポイント付与のための原資やポイント付与の運用、ボランティア活動での個人情報の扱いやボランティア活動の記録の運用などの課題に対する対応策を示した。

また、行政手続きの電子化では、スマートフォンへの複数カードの統合等の課題対応策や公金収納の電子化での、電子通知時の運用や電子通知の到達に関する制度上の課題等について対応策を示したが、住民基本台帳法で決められている住基カードの取得に関する資格者の要件や、メール通知の制度面での到達の解釈など自治体のみで解決でない課題もありこれらの制約を回避する策もあわせて示している。

モバイルアクセスシステムについては、本人確認を含めた申請時や一時停止、本人確認情報の処理などの運用、各サービス利用等の課題対応策を示した。また、ローカル通信時での情報のやり取りを行うことから運用負荷を軽減する方法についての対応策も示した。

本検討により、スマートフォンをアクセス手段として最適サービスを利用する際の、スマートフォンに関する課題やサービスの制度面・運用面の課題に対してそれぞれ課題対応策を明らかにすることができた。

4.6. まとめ

アクセス手段としての携帯電話の利便性向上方法の検証として、制度・運用面の検討を行った。

検討は、行政、医療、健康、福祉、金融の各サービス領域から、携帯電話（スマートフォン）が活用でき、情報へのアクセスの際に本人確認（認証）が必要なサービスで、利用者の利便性が高く、サービス提供機関の抱える課題解決につながる観点からサービスを洗い出し、サービス提供機関へのヒアリング結果などを基に、検討対象として、福祉、行政の観点から高齢者支援サービス、行政手続きの申請手段の電子化、公金収納の電子化のサービスを適用サービスとして選定した。

スマートフォンを利用して、これらの適用サービスで取扱う情報には、セキュリティレベルの高い情報もあり、各サービスで求められるセキュリティレベルと認証レベルについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）」に基づいて、各サービスで取扱う情報のリスク影響度分析の方法を定義し、その定義に基づいて分析を行った。分析の結果、必要なセキュリティの保証レベルとしてレベル 4（特定される身元識別情報の信用度が非常に高い）が必要であることが明確になった。あわせて、レベル 4 を実現する上での認証の対策基準について、「登録」、「発行・管理」、「トークン」の観点から整理した。

セキュリティレベルの検討結果も踏まえ、適用サービスの実現評価を行うため、制度や環境、政策動向などの観点に対し、サービス提供機関に対するヒアリングを実施し、その評価などを基にサービスの有効性について評価を行ったが、スマートフォンの活用と本人認証の仕組みを基にして、福祉、行政、金融の各適用サービスの検討から、それぞれのサービスについて、利用者並びに自治体や金融機関などのサービス提供機関に対し効果がありサービスの有効性を明らかにすることができた。

また、その際に、スマートフォンでの操作性やサービス性などスマートフォンを活用する際の課題やスマートフォン利用時の各適用サービスの運用や制度面の課題、モバイルアクセスサーバの運用設置に関する課題が明らかになった。

最後に、これらの課題ごとに対応策（案）を示したが、対応策に関しては今後さらなる検討が必要と考える。

本検討により、福祉、行政、金融の各サービス分野での、携帯電話（スマートフォン）を活用した各サービスへのアクセス手段について、運用、制度上の課題と対応策（案）を検討することで、実現に向け解決すべき事項を明確化したが、今後は実際の環境下で住民やサービス提供機関などでの評価が必要と考える。

表 4-49 に応募資格に対する本成果報告書の対応個所を示す。

表 4-49 応募資格に対する本成果報告書の対応個所

	実施要領に記載される要件	参照先	対応内容
課題ウ	課題ア～イでの検討・検証結果に基づき、実際に導入するにあたって考えられる制度・運用面での課題抽出と、その対応案を検討する。	4.5.6	モバイルアクセスシステムで、新たに生まれる好適なサービスを検討した上で、制度・運用面での課題を抽出し、重要な課題については、対応方策の検討を行った。
		4.5	応募資格では「平成２１年度　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（携帯電話からの電子行政サービス等へのアクセス技術の調査研究)」での好適サービスの検討結果や制度、運用の調査結果を踏まえた検討を行う」こととした。だだい、提案評価会より「直近の動向を踏まえた調査・検討を行うこと」と指摘があり、今回、改めてサービス提供機関にヒアリングを実施し、現状を踏まえた調査・検討行った。

4.7. 参考：セキュリティレベルの検討

4.7.1. 検討の考え方

制度・運用面の課題検討の対象適用サービスに対して必要となるセキュリティレベル（保証レベル）と認証方式についての要件の検討に当たっての考え方を示す。

検討対象サービスである、高齢者支援サービス、および、行政手続きの申請手段の電子化サービス、公金収納の電子化サービス、保険契約情報の閲覧、保険加入の申請、事故情報の申告サービスで取扱う情報を基に、リスク影響度の分析を行い、それぞれのサービスで必要となる認証レベルを検討し、4 段階ある認証レベルにマッピングを行う。

リスク影響度分析と認証レベルの検討に当たっては、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日)」（以下、「ガイドライン」という）を基に、以下の手順で検討を進める。

(1) リスク影響度の分析と保証レベルの決定方法の定義
ガイドラインに従い、各サービスで取扱う情報に対して、金銭的損害に係るリスク評価と機微情報の漏えいに係るリスク評価の分析と必要となる保証レベルの決定方法を定義する。

(2) 各サービスでのリスク影響度と対応する保証レベルの決定
高齢者向け支援サービス（介護予防等）向上のための地域通貨(ポイント)活用、行政手続の申請手段の電子化、公金収納の電子化の 3 つのサービス毎に、定義したリスク評価の分析と保証レベルの決定方法に基づき検討を行い、対応するリスク影響度と保証レベルを決定する。

(3) リスク評価に基づく認証方式の検討
決定した保証レベルから、各サービスに必要な認証方式（登録、発行・管理、トークン）について検討する。

4.7.2. リスク影響度の分析と保証レベルの決定方法の定義

リスク影響度の分析と保証レベルの決定は、ガイドラインに基づき、各サービスで取り扱う情報を基に、金銭的損害に係るリスク評価と機微情報の漏えいに係るリスク評価を行い、その結果から必要な保証レベルを求め、その保証レベルを満たす認証方式を明確にする。本節ではそのためのリスク影響度分析と保証レベルの決定方法の定義を明確にする。

ガイドラインに基づき保証レベルの検討方法を以下の 3 段階の手順で実施する。

- ステップ 1：金銭的損害に係るリスク評価と機微情報の漏えいに係るリスク評価の分析
- ステップ 2：ステップ 1 の分析結果を基に、その組み合わせによる総合的リスク評価の導出
- ステップ 3：導出した総合的リスク評価による、必要な認証方式の決定

ステップ 1、ステップ 2、ステップ 3 でのリスク評価方法の定義ついて以下に示す。

【ステップ 1】金銭的損害に係るリスク評価と機微情報の漏えいに係るリスク評価の分析

各サービスで取扱う情報のリスク影響度をガイドラインに基づき、情報の金銭的損害に関する観点と機微情報の漏えいの観点から評価を行い、両者の結果を基に該当情報に対する総合的なリスク評価分析を行う。

① 金銭的損害に係るリスクの影響度の評価方法と評価基準

金銭的損害に係るリスク影響度の評価方法と評価基準の定義についてガイドラインに基づき定義する。

金銭的損害に係るリスクの影響度は、各サービスで取扱う情報を金銭的損害の観点からリスク影響度を分析するもので、ⅰ）金銭的損害の程度とⅱ）申請等に係る厳格さの２つの評価軸から評価する。

金銭的損害に係るリスク影響度のレベル定義を表 4-50 に示す。

表 4-50　金銭的損害に係るリスクの影響度のレベル定義

レベル	ⅰ）金銭的損害の程度	ⅱ）申請等に係る厳格さの程度
特高	1000 万円以上の金銭的損害	当該手続の申請等に当たり、本人確認又は申請書等の真正性確保のため、当該手続を所管する主体が保有するデータベースに加え、主体以外が保有するデータベースとの照合を実施している、もしくは厳格な公的証明書等注による確認を実施している。
高	100 万円以上、1000 万円未満の金銭的損害	当該手続の申請等に当たり、本人確認又は申請書等の真正性確保のため、当該手続を所管する主体が保有するデータベースとの照合、もしくは公的証明書等による確認を実施している。
中	100 万円未満の金銭的損害	当該手続の申請等に当たり、本人確認又は申請書等の真正性確保のため、上記の方法ほどの厳格さはないが、何らかの確認を実施している。
低	金銭的損害なし	当該手続の申請等に当たり、特に確認を実施していない。

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）を基に作成した。

② 金銭的損害に係るリスクの影響度の評価パターン

金銭的損害に係るリスクの影響度は、表 4-50 に示す金銭的損害の程度と申請等に係る厳格さの 2 軸での評価を行った後、各々の評価結果を点数化し、その合計値から金銭的損害に係るリスクとしての評価レベルを求める。

レベル評価の点数は、特高：4 点、高：3 点、中：2 点、低：1 点とし、各軸の評価レベルの合計点から、7 点以上：特高、5 点以上：高、3 点以上：中として、金銭的損害に係るリスクとしての評価レベルとする。

金銭的損害に係るリスクのレベルと申請等に係る厳格さに係るリスクのレベルの組み合わせによって金銭的損害に係るリスク影響度が求められるが、その組み合わせ結果を評価パターンとして表 4-51 に示す。

表 4-51　金銭的損害に係るリスクの影響度の評価パターン

レベル	金銭的損害に係るリスク	申請等に係る厳格さに係るリスク
特高(8)	特高	特高
特高(7)	特高	高
特高(7)	高	特高
高(6)	特高	中
高(6)	高	高
高(6)	中	特高
高(5)	特高	低
高(5)	高	中
中(4)	中	中
中(4)	低	特高
中(4)	低	高
中(3)	中	低
中(3)	低	中

（注）（　）内は評価点数を示す

③ 機微情報の漏えいに係るリスク影響度の定義

機微情報の漏えいに係るリスク影響度は、各サービスで取扱う情報の機微の度合いから表 4-52 に示す基準で評価を行う。

表 4-52　機微情報の漏えいに係るリスク影響度の定義

レベル	情報に含まれる機微（センシティブ）の度合い
特高	生命の危険または差別や名誉毀損等の社会的不利益につながるもののうち、回復が困難なもの（「個人情報保護マネジメントシステム－要求事項（JIS Q 15001）」で収集禁止の個人情報として定義されているものなど）
高	特高と中の中間に位置するもの
中	公知のもの
低	機微情報ではないもの

（出典）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）

【ステップ2】ステップ1の分析結果を基にその組み合わせによる総合的リスク評価の導出

ステップ 1 で分析された金銭的損害に係るリスクの影響度と機微情報の漏洩に係るリスクの影響度の分析結果から、総合的なリスク評価の分析を行い、その評価レベルから対応する保証レベルを決定する。

① 金銭的損害に係るリスクの影響度と機微情報の漏洩に係るリスクの評価パターン

ステップ 1 での分析結果から、金銭的損害に係るリスクの影響度と機微情報の漏洩に係るリスクの評価レベルを、特高：4 点、高：3 点、中：2 点、低：1 点と数値化し、その合計点として、7 点以上：特高、5 点以上：高、3 点以上：中として、総合的リスク評価を行う。

金銭的損害に係るリスクのレベルと機微情報の漏洩に係るリスクのレベルの組み合わせから総合リスク評価を求められるが、その評価パターンを表 4-53 に示す。

表 4-53　総合リスク評価のパターン

レベル	金銭的損害に係るリスク	機微情報の漏洩に係るリスク
特高(8)	特高	特高
特高(7)	特高	高
特高(7)	高	特高
高(6)	特高	中
高(6)	高	高
高(6)	中	特高
高(5)	特高	低
高(5)	高	中
中(4)	中	中
中(4)	低	特高
中(4)	低	高
中(3)	中	低
中(3)	低	中

（注）（ ）内は評価点数を示す

② 総合的なリスクの影響度と対応する保証レベル

総合的なリスクの影響度の評価レベルから、各サービスで求められる保証レベル決定する。

保証レベルは、総合的なリスク影響度の評価レベルから決定され、リスク影響度の特高、高、中、低の各々のリスク影響度を保証するレベルとしてそれぞれ、レベル 4、レベル 3、レベル 2、レベル 1 が対応している。総合的なリスクの影響度のレベルとその

定義、対応する必要な保証レベルの関係を表 4-54 に示す。

表 4-54　総合的なリスクの影響度と対応する保証レベル

リスク影響度	定義	保証レベル
特高	当該リスクの影響による損失が、組織の運営、組織の資産、または個人に致命的または壊滅的な悪影響を及ぼすと予想される。	レベル 4
高	当該リスクの影響による損失が、組織の運営、組織の資産、または個人に重大な悪影響を及ぼすと予想される。	レベル 3
中	当該リスクの影響による損失が、組織の運営、組織の資産、または個人に限定的な悪影響を及ぼすと予想される。	レベル 2
低	当該リスクの影響が、測定可能な結果をもたらさない。	レベル 1

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）を基に作成した。

【ステップ 3】導出した総合的リスク評価による、必要な認証方式の決定

ステップまでの分析によって導出された総合的リスク評価を基に必要な保証レベルが決まり、それによって対応する認証方式を決定する。

① リスク影響度と保証レベルの定義

ステップ 2 で分析評価された総合的なリスク影響度から必要となる保証レベルを決定する。

リスク影響度とから定義される保証レベルとその定義を表 4-55 に示す。

表 4-55　リスク影響度と保証レベル定義

リスク影響度	保証レベル	レベル定義
特高	レベル 4（かなり高い保証）	特定される身元識別情報の信用度が非常に高い
高	レベル 3（高い保証）	特定される身元識別情報の信用度が相当程度ある
中	レベル 2（中程度の保証）	特定される身元識別情報の信用度がある程度ある
低	レベル 1（低い保証）	特定される身元識別情報の信用度がほとんどない

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）を基に作成した。

② 保証レベルと認証方式

必要とする保証レベルから実現する認証方式を決定する。

保証レベルを実現する認証方式の基準は、評価軸として「登録」「発行・管理」「トークン」「認証/署名等プロセス」の４つの評価軸からなり、それぞれの評価軸毎のレベルが異なる場合には最も低いレベルが当該認証方式の総合的な保証レベルであると定義されている。

以下、これらの評価軸のうち「登録」、「発行・管理」、「トークン」の保証レベルの対策基準を以下に示す。

ｉ）「登録」の保証レベル

認証方式の「登録」では対面の場合と遠隔の場合で保証レベルと対策基準が異なり、遠隔の場合はレベル 4 の対策はない。登録の対策基準を対面、遠隔の別に表 4-56、表 4-57 に示す。

表 4-56　登録の保証レベル（対面の場合）

対策基準	保証レベル			
	1	2	3	4
電子メールアドレスが申請された場合、有効性（到達性）を確認する	◎	○	○	○
申請者は、公的な写真つきの身分証明書を 1 種類、またはその他の身分証明を 2 種類提示する		◎	◎	◎
申請者の氏名や住所等の公的な台帳の照合または申請書に添付された公的証明書によりチェックする			◎	◎
重複登録でないことを確認する				◎

（出典）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）

表 4-57　登録の対策基準（遠隔の場合）

対策基準	保証レベル			
	1	2	3	4
電子メールアドレスが申請された場合、有効性（到達性）を確認する	◎	○	○	
申請者の氏名と住所等及び身分確認に有効な他機関の登録情報が記載された申請書により申請する		◎	◎	
申請者の氏名や住所等の公的な台帳を照合または申請書に添付された公的証明書によりチェックする			◎	
申請者の氏名と住所等が記載された申請書に本人の電子署名（郵送は署名、捺印）を付与して申請する			◎	

（出典）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）

ⅱ）「発行・管理」の保証レベル

認証方式の「発行・管理」では、発行、管理、更新/再発行、失効、記録保管のそれぞれについて、保証レベル別に対策基準が定義されている。

定義されている「発行・管理」の対策基準を表 4-58 に示す。

表 4-58 「発行・管理」の対策基準

保証レベル	対策基準				
	発行	管理	更新/再発行	失効	記録保管
レベル4	認証情報及びトークンが窓口にて直接手渡される。（本人限定受取郵便基本型及び同サービスと同等の手段による身元確認は対面で行う）。	レベル3と同等以上	レベル3と同等以上	レベル3と同等以上	レベル3と同等以上
レベル3	認証情報及びトークンが以下のいずれかの方法により本人に送付される。 ・窓口にて直接手渡される。 ・本人住所に書留郵送または本人限定受取郵便により送付される。 ・本人住所に書留郵便または本人限定受取郵便にてパスワードが送付され、本人が当該パスワードによる認証の上で認証情報及びトークンをダウンロードする。 ・申請者が電子署名を付与した申請を行い、検証された上で認証情報及びトークンをダウンロードする。	レベル2と同等以上	レベル2と同等以上の対策基準に加え特にオンラインによる手続の場合には、既存の認証情報及びトークンを用いた認証の上で通信を暗号化して行う。	認証情報及びトークンが有効でなくなった、または危殆化されたことを通知された時から認証情報及びトークンを延滞なく失効する。	レベル2と同等以上の対策基準に加え記録を定期的に分析、評価する。
レベル2	認証情報及びトークンが以下のいずれかの方法により本人に送付される。 ・窓口にて直接手渡される。 ・2つに分割され、少なくともその1つが本人住所に普通郵送により送付される。 ・本人の電子メールアドレスに対して入手サイト先の情報とパスワードが通知され、本人が該当パスワードによる認証の上サイトからダウンロードする。	レベル1と同等以上	認証情報及びトークンの更新、再発行に関する運用ポリシーが策定され周知されている。	－	認証情報及びトークンの発行・管理に関する記録を当該認証情報の有効期限または失効時期の遅い方の時期から一定期間保管する。
レベル1	認証情報及びトークンが本人の電子メールアドレスに対して送付される、またはオンラインでの登録手続の過程で本人が認証情報及びトークンをダウンロードする。	検証者が使用する秘密情報はアクセス制御によって保護され、パスワードのような秘密情報を平分のまま含まない。	－	－	－

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成22年8月31日）を基に作成した。

ⅲ）「トークン」の保証レベル

認証方式の「トークン」には、ハードウェアトークン、ソフトウェアトークン、ワンタイムパスワードトークン、パスワードトークンなどの種類があり、求められる保証レベルに応じて使い分けが必要となる。

保証レベルに対応するトークンの対策種類と実現例を表 4-59 に示す。

表 4-59　保証レベルと「トークン」の対策種類

保証レベル	対策種類	実現例
レベル4	耐タンパ性を有するパスワード付ハードウェアトークン	・IC カード ・USB トークン
レベル3	ソフトウェアトークンとパスワードなどの複数のトークンの組み合わせ	・パスワード付ソフトウェアワンタイムパスワードトークン ・パスワード付ソフトウェアトークン ・パスワード付ハードウェアワンタイムパスワードトークン
レベル2	パスワード、事前登録知識の確認など	・アルファベット、数字、記号による 5 桁以上の無作為のパスワード、かつ 3 回連続失敗時は 1 日間パスワード入力不可、かつ有効期限 10 年以内 ・アルファベット、数字、記号による 8 桁以上のユーザ選択によるパスワード、かつ 3 回連続失敗時は 1 日間パスワード入力不可、かつ有効期限 10 年以内 ・数字による 9 桁以上の無作為のパスワード、かつ 3 回連続失敗時は 1 日間パスワード入力不可、かつ有効期限 10 年以内 ・数字による 12 桁以上のユーザ選択によるパスワード、かつ 5 回連続失敗時はパスワード変更を強制
レベル1	パスワード、事前登録知識の確認など	・アルファベット、数字、記号による 4 桁以上の無作為のパスワード、かつ 3 回連続失敗時は 1 日間パスワード入力不可、かつ有効期限 10 年以内 ・アルファベット、数字、記号による 7 桁以上のユーザ選択によるパスワード、かつアルファベット・数字・記号の全てを用い、かつ辞書に記載された単語ではない、かつ 3 回連続失敗時は 1 日間パスワード入力不可、かつ有効期限 10 年以内 ・数字による 8 桁以上の無作為のパスワード、かつ 3 回連続失敗時は 1 日間パスワード入力不可、かつ有効期限 10 年以内 ・数字による 8 桁以上のユーザ選択によるパスワード、かつ 5 回連続失敗時はパスワード変更を強制

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）を基に作成した。

4.7.3.　各サービスでのリスク影響度と対応する保証レベル

適用サービスとして検討対象とした、高齢者向け支援サービス、行政手続きの申請手段の電子化、公金収納の電子化の各サービスでのリスク影響度と対応する保証レベルを 4.7.2 節のステップ 1 からステップ 3 までの分析の定義に基づき分析し、各サービスの実現に必要な保証レベルを求める。

検討に当たっては、各サービスで利用される情報を各サービス内の利用ケースを想定して整理し、その情報ごとにリスク影響度を分析し、その結果から総合的なリスク影響度を求め、必要な保証レベルを決定する。

以下、各サービスの分析結果を示す。

(1) 高齢者向け支援サービス

高齢者向け支援サービスは、健康状態の記録と管理、介護予防活動記録の統計分析への利用サービスとボランティア活動の継続的な促進サービスの 2 つのサービスからなる。

以下、これらのサービス別にリスク影響度と対応する保証レベルを検討する。

① 健康状態の記録と管理、介護予防活動記録の統計分析への利用

リスク影響度分析と保証レベルの検討に当たり、本サービスで取扱う情報を整理する。

このサービスでは、次に示す 5 つの利用ケースを想定し、これらの利用ケースで用いられる情報を検討対象とする。

- 高齢者が自らの日常の行動などを基本チェックリストに記録し、記録した情報を自治体への送信を行うケース
- 高齢者が自ら健康状態や運動、体力測定などを記録し、自己の経年履歴を閲覧するケース
- 介護予防プログラムへの参加を記録し、自己の参加状況や指導状況などを閲覧するケース
- 記録した情報を自治体への送信を行うケース
- 記録した情報を自治体へ送信時に地域ポイントを付与されるケース

これらの利用ケースごとの取扱う情報とその情報の利用形態、リスク影響度の分析結果、および、必要な保証レベルを表 4-60 に示す。

表 4-60　健康状態の記録と管理、介護予防活動記録の統計分析への利用の保証レベル

ユースケース	取扱う情報	情報の利用形態	リスクの影響度			保証レベル
			金銭的損害に係るリスクの影響度	機微情報の漏洩に係るリスクの影響度	総合的なリスクの影響度	
基本チェックリストの登録と閲覧、チェックリストの送信	氏名、住所、生年月日、性別、実施日、基本チェックリストのチェック結果	・本体記録 ・ローカル通信 ・オンライン	中（低/中）	高	高	レベル3
健康状態の記録と閲覧	氏名、住所、生年月日、性別、バイタル情報（血圧、体重）の履歴	・本体記録	低（低/低）	高	中	レベル2
運動情報の登録と閲覧	氏名、住所、生年月日、性別、運動記録（歩行記録）や体力測定結果の履歴	・本体記録	低（低/低）	中	中	レベル2
介護予防プログラムへの参加記録と閲覧	氏名、住所、生年月日、性別、介護予防プログラムやボランティア活動の参加記録（日時、プログラム名、活動内容、活動結果、報告事項、指導内容等）	・本体記録	中（低/中）	高	高	レベル3
健康状態や介護予防プログラムの参加状況等の自治体への提供	氏名、住所、生年月日、性別、バイタル情報や運動記録や体力測定結果、介護予防プログラムやボランティア活動の参加記録（日時、プログラム名、活動内容、活動結果、報告事項、指導内容等）	・ローカル通信 ・オンライン	中（低/中）	高	高	レベル3
ポイントの付与	ポイント数	・本体記録 ・ローカル通信 ・オンライン	中（中/低）	低	中	レベル2

（注）金銭的損害に係るリスクの影響度のカッコ内の表記(A/B)は、A が金銭的損害の程度、B が申請等に係る厳格さの程度を示す。

② ボランティア活動の継続的な促進

リスク影響度分析と保証レベルの検討に当たり、本サービスで取扱う情報を整理する。

このサービスでは、次に示す 3 つの利用ケースを想定し、これらの利用ケースで用いられる情報を検討対象とする。

- ボランティア参加者がボランティア活動を記録し、自治体へ送信するケース
- ボランティア参加者が一人暮らしの高齢者の現況確認を行い、自治体へ送信するケース
- ボランティア参加へポイントを付与するケース

これらの利用ケースごとの取扱う情報とその情報の利用形態、リスク影響度の分析結果、および、必要な保証レベルを表 4-61 に示す。

表 4-61 ボランティア活動の継続的な促進の保証レベル

ユースケース	取扱う情報	情報の利用形態	リスクの影響度			保証レベル
			金銭的損害に係るリスクの影響度	機微情報の漏洩に係るリスクの影響度	総合的なリスクの影響度	
ボランティア活動の実施記録と送信	氏名、住所、生年月日、性別、ボランティア活動の記録(日時、プログラム名、活動内容、活動結果、報告事項、実施確認、等)	・本体記録 ・ﾛｰｶﾙ通信 ・オンライン	中（低/中）	高	高	レベル３
一人暮らし高齢者の現況報告の記録と送信	氏名、住所、生年月日、性別、一人暮らし高齢者の現況報告内容（訪問先高齢者の氏名、住所、生年月日、性別、前回訪問時の状況、今回の訪問時の状況等)	・本体記録 ・オンライン	特高（低/特高）	特高	特高	レベル４
ポイントの付与	ポイント数	・本体記録 ・ﾛｰｶﾙ通信 ・オンライン	中（中/低）	低	中	レベル２

（注）金銭的損害に係るリスクの影響度のカッコ内の表記（A/B）は、A が金銭的損害の程度、B が申請等に係る厳格さの程度を示す

(2) 行政手続きの申請手段の電子化

リスク影響度分析と保証レベルの検討に当たり、本サービスで取扱う情報を整理する。

このサービスでは、次に示す 3 つの利用ケースを想定し、これらの利用ケースで用いられる情報を検討対象とする。

- 住民票等の申請情報を記録し、自治体に申請するケース
- 住民票等の交付手数料を記録したポイントで支払うケース
- 住民登録等の申請情報を記録し、自治体に申請するケース

これらの利用ケースごとの取扱う情報とその情報の利用形態、リスク影響度の分析結果、および、必要な保証レベルを表 4-62 に示す。

表 4-62　行政手続きの申請手段の電子化の保証レベル

ユースケース	取扱う情報	情報の利用形態	リスクの影響度			保証レベル
			金銭的損害に係るリスクの影響度	機微情報の漏洩に係るリスクの影響度	総合的なリスクの影響度	
住民票等の交付申請情報の登録と交付申請	申請者の情報（氏名、住所、生年月日、性別、連絡先)、必要な人の情報（氏名、住所、生年月日、請求者との関係、使用目的)、必要な住民票の写しの種類と必要数	・本体記録 ・ﾛｰｶﾙ通信	中 (低/高)	中	中	レベル 2
住民票等の交付時のポイント利用	ポイント利用数	・ﾛｰｶﾙ通信	中 (中/低)	低	中	レベル 2
住民登録（転入届）等の申請情報の登録と申請	新住所と世帯主氏名、住み始めた日、今までの住所と世帯主氏名、転入者の生年月日と新世帯主との続柄、転入者の本籍と戸籍の筆頭者、申請者（住所、氏名、連絡先電話番号)	・本体記録 ・ﾛｰｶﾙ通信	中 (低/高)	特高	高	レベル 3

（注）金銭的損害に係るリスクの影響度のカッコ内の表記（A/B）は、A が金銭的損害の程度、B が申請等に係る厳格さの程度を示す

(3)　公金収納の電子化

リスク影響度分析と保証レベルの検討に当たり、本サービスで取扱う情報を整理する。

このサービスでは、次に示す 3 つの利用ケースを想定し、これらの利用ケースで用いられる情報を検討対象とする。

- 自治体から納付者に納付書を送信するケース
- 納付書をホームページから確認するケース
- 確認した納付書に基づき、支払うケース

これらの利用ケースごとの取扱う情報とその情報の利用形態、リスク影響度の分析結果、および、必要な保証レベルを表 4-63 に示す。

表 4-63　公金収納の電子化の保証レベル

ユースケース	取扱う情報	情報の利用形態	リスクの影響度			保証レベル
			金銭的損害に係るリスクの影響度	機微情報の漏洩に係るリスクの影響度	総合的なリスクの影響度	
納付書の送付	氏名、住所、生年月日、納付情報（納付種目、金額、納付時期、納付金額の根拠の説明）	メール	高（中/特高）	中	高	レベル 3
ホームページでの納付情報の閲覧	氏名、住所、生年月日、納付情報（納付種目、金額、納付時期、納付金額の根拠の説明）	Web	高（中/高）	中	高	レベル 3
納付情報支払い	氏名、住所、生年月日、納付情報（納付種目、金額、納付時期、納付金額の根拠の説明）	Web	高（高/特高）	高	高	レベル 3

（注）金銭的損害に係るリスクの影響度のカッコ内の表記（A/B）は、A が金銭的損害の程度、B が申請等に係る厳格さの程度を示す

(4)　保険契約情報閲覧、保険加入申請、事故情報申告

リスク影響度分析と保証レベルの検討に当たり、本サービスで取扱う情報を整理する。

このサービスでは、次に示す 3 つの利用ケースを想定し、これらの利用ケースで用いられる情報を検討対象とする。

- 複数の保険契約の名寄せを登録するケース
- 契約情報を家族等運転者に対して閲覧等権限を付与するケース
- 契約者もしくは運転者（家族等）が事故発生時に申告するケース

これらの利用ケースごとの取扱う情報とその情報の利用形態、リスク影響度の分析結果、および、必要な保証レベルを表 4-64 に示す。

表 4-64　事故申告でのスマートフォン利用の保証レベル

ユースケース	取扱う情報	情報の利用形態	リスクの影響度			保証レベル
			金銭的損害に係るリスクの影響度	機微情報の漏洩に係るリスクの影響度	総合的なリスクの影響度	
複数の保険契約情報の名寄せ登録	契約者氏名、複数の他種目契約番号	・本体記録 ・Web	特高 (特高/高)	高	特高	レベル 4
契約情報の閲覧権限付与	契約者氏名、契約番号、権限情報（閲覧、申請等） 運転者氏名（付与対象）、運転者年齢、続柄など	・ローカル通信 ・本体記録	高 (特高/中)	高	高	レベル 3
事故発生時に契約情報を通知	契約者氏名、契約者住所、運転者氏名、運手者住所、運転者の続柄、契約情報（契約番号、車両番号、車種、登録番号、給付金額、給付種別など）、位置情報など	・本体記録 ・Web	高 (特高/中)	高	高	レベル 3

（注）金銭的損害に係るリスクの影響度のカッコ内の表記（A/B）は、A が金銭的損害の程度、B が申請等に係る厳格さの程度を示す

4.7.4.　リスク評価に基づく認証方式

各サービスで取り扱う情報を基に、リスク影響度と必要な保証レベルの検討を行った。その結果から、各サービスのリスク影響度分析により対応する保証レベルはユースケースにより異なるが、保証レベル3以上が必要となることがわかる。

保証レベル3は、“特定される身元識別情報の信用度が相当程度ある”と定義され、また、保証レベル４は、“特定される身元識別情報の信用度が非常に高い”定義される。本サービスにおける、レベル 3、レベル４の対策基準を、「登録」、「発行・管理」、「トークン」の観点から整理すると下記のとおりである。

ｉ）登録の対策基準

認証方式の「登録」における対策基準を表 4-65 に示す。

表 4-65　「登録」の対策基準

保証 レベル	対策基準
レベル 4	重複登録でないことを確認する。（対面）
レベル 3	申請者の氏名や住所等の公的な台帳を照合または申請書に添付された公的証明書によりチェックする。（対面・遠隔）
レベル 3	申請者の氏名と住所等が記載された申請書に本人の電子署名（郵送は署名、捺印）を付与して申請する。（遠隔）

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）を基に作成した。

ⅱ）発行・管理の対策基準

認証方式の「発行・管理」における対策基準を表 4-66 に示す。

表 4-66　「発行・管理」の対策基準

保証レベル	対策基準			
	発行	管理	更新/再発行	失効
レベル 4	認証情報及びトークンが窓口にて直接手渡される。 （本人限定受取郵便基本型等の手段による身元確認は対面）。	レベル 3 と同等以上	レベル 3 と同等以上	レベル 3 と同等以上
レベル 3	認証情報及びトークンが以下のいずれかの方法により本人に送付される。 ・窓口にて直接手渡される。 ・本人住所に書留郵送または本人限定受取郵便により送付される。 ・本人住所に書留郵便または本人限定受取郵便にてパスワードが送付され、本人が当該パスワードによる認証の上で認証情報及びトークンをダウンロードする。 ・申請者が電子署名を付与した申請を行い、検証された上で認証情報及びトークンをダウンロードする。	検証者が使用する秘密情報はアクセス制御によって保護され、パスワードのような秘密情報を平分のまま含まない。	・認証情報及びトークンの更新、再発行に関する運用ポリシーが策定され周知されている。 ・上記同等以上の対策基準に加え特にオンラインによる手続の場合には、既存の認証情報及びトークンを用いた認証の上で通信を暗号化して行う。	認証情報及びトークンが有効でなくなった、または危殆化されたことを通知された時から認証情報及びトークンを延滞なく失効する。

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）を基に作成した。

ⅲ）トークンの対策種類

認証方式の「トークン」における対策種類と実現例を表 4-67 に示す。

表 4-67　「トークン」の対策種類と実現例

保証 レベル	対策種類	実現例
レベル 4	耐タンパ性を有するパスワード付ハードウェアトークン	・IC カード、・USB
レベル 3	ソフトウェアトークンとパスワードなどの複数のトークンの組み合わせ	・パスワード付ソフトウェアワンタイムパスワード、・パスワード付ソフトウェア ・パスワード付ハードウェアワンタイムパスワード

（注）オンライン手続におけるリスク評価及び電子署名・認証ガイドライン（各府省情報化統括責任者（CIO）連絡会議決定、平成 22 年 8 月 31 日）を基に作成した。

5. 課題エ　本事業に基づく成果の普及

5.1. 概要

本節では、検討委員会およびARIB高度無線通信研究員会へインプットするガイドライン案について記述する。

5.2. 委員会について

5.2.1. 委員会構成

以下に委員会委員を示す。

手塚 悟 （東京工科大学　教授）
佐藤 一夫（株式会社ＮＴＴドコモ　モバイルデザイン推進室　室長）
安部 孝太郎（(株）ＮＴＴドコモ モバイルデザイン推進室 主査）
阪東 謙一（ＫＤＤＩ株式会社　コンバージェンス推進本部　担当部長）
田中 卓弥（ＫＤＤＩ（株）コンバージェンス推進本部　課長補佐）
小峰 正裕（ソフトバンクモバイル株式会社　海外事業推進本部　室長代行）
立原 彩子（ソフトバンクモバイル（株）海外事業戦略室）
渡辺 芳治（イー・アクセス（株）デバイス開発部　副部長）
宮北 幸典（イー・アクセス（株）デバイス開発部　端末推進Ｇ　課長代理）
小野瀬 健太郎（株式会社日立製作所　セキュリティ・トレーサビリティ事業　部長）
川野 隆（株式会社日立製作所 セキュリティ・トレーサビリティ事業部 技師）
梅澤 克之（株式会社日立製作所 横浜研究所 主任研究員）

以下にオブザーバを示す。

黒瀬 泰平（総務省 情報流通行政局 情報流通振興課 課長）
本橋 充成（総務省 情報流通行政局 情報流通振興課 課長補佐）
古謝 玄太（総務省 情報流通行政局 情報流通振興課 主査）
前原 正男（厚生労働省 政策統括官付社会保障担当参事官室 室長補佐）
浜田 哲 （厚生労働省 政策統括官付社会保障担当参事官室 技術参与）
鈴木 重郎（厚生労働省 政策統括官付社会保障担当参事官室 主査）
安田 浩（東京電機大学 未来科学部 教授）
安井 秀行（ＮＰＯ団体アスコエ 代表）

以下に事務局を示す。

勝家 由樹（株式会社日立製作所 セキュリティ・トレーサビリティ事業部 技師）
川野 隆（株式会社日立製作所 セキュリティ・トレーサビリティ事業部 技師）

（敬称略）

5.2.2.　委員会実施実績

以下に本委員会の実績を記す。

(1) 第一回委員会：平成２３年１２月１９日（月）【5.2.2.1を参照】

(2) 第二回委員会：平成２４年　１月２３日（月）【5.2.2.2を参照】

(3) 第三回委員会：平成２４年　２月２０日（月）【5.2.2.3を参照】

(4) 第四回委員会：平成２４年　３月１６日（金）【5.2.2.4を参照】

5.2.2.1.　第一回委員会

(1) 日時：平成２３年１２月１９日（月）１３時００分～１４時３０分

(2) 場所：秋葉原ＵＤＸビル　２０Ｆ　Conference Room３

(3) 出席者：

①構成員

手塚構成員（座長)、佐藤構成員、安部構成員、阪東構成員、田中構成員、
小峰構成員、松村構成員、小野瀬構成員、川野構成員、梅澤構成員

②オブザーバ

総務省 情報流通行政局 情報流通振興課　黒瀬課長、本橋課長補佐、古謝主査
厚生労働省 政策統括官付社会保障担当参事官室　前原室長補佐、浜田技術参与、
鈴木主査
東京電機大学 未来科学部　安田教授
ＮＰＯ団体アスコエ　安井代表

③事務局

勝家事務局員
川野事務局員

(4) 議事次第

①開会
②黒瀬課長　ご挨拶
③安田先生　ご挨拶
④構成員、オブザーバのご紹介
⑤事業概要について
⑥検討委員会について
⑦質疑応答
⑧今後の検討委員会の進め方について
⑨閉会

(5) 配布資料

資料１：構成員、オブザーバ

資料２：行政業務システム連携推進事業
（アクセス手段としての携帯電話の利便性向上方法の検証）概要
資料３：検討委員会について
資料４：今後のスケジュール
参考資料１： 実施計画書

5.2.2.2. 第二回委員会

(1) 日時：平成２４年１月２３日（月）１５時００分～１７時００分

(2) 場所：日本生命丸の内ビル２３Ｆ　Conference Room５

(3) 出席者：

①構成員

手塚構成員（座長)、佐藤構成員、安部構成員、阪東構成員、田中構成員、
小峰構成員、渡辺構成員、宮北構成員、小野瀬構成員、川野構成員、梅澤構成員

②オブザーバ

総務省 情報流通行政局 情報流通振興課　黒瀬課長、本橋課長補佐、古謝主査
厚生労働省 政策統括官付社会保障担当参事官室　前原室長補佐、浜田技術参与、
鈴木主査
東京電機大学 未来科学部　安田教授
ＮＰＯ団体アスコエ　安井代表

③日立製作所

勝田部長代理、真下技師

④事務局

勝家事務局員、川野事務局員

(4) 議事次第

①開会
②課題ア：技術仕様の検討状況のご報告
③課題イ：実験に向けた検討状況のご報告
④課題ウ：運用・制度における課題の検討状況のご報告
⑤厚生労働省様　社会保障分野での情報連携のための携帯電話端末の活用に関する検討状況のご報告
⑥閉会

(5) 配布資料

資料１：検討委員会構成員及びオブザーバ
資料２：検討委員会（第１回）議事録（案）
資料３：研究成果報告書（課題ア部分のみ抜粋）
資料４：実験環境による検証（課題イ）について

資料５：運用・制度における課題の検討について
資料６：社会保障分野での情報連携のための携帯電話端末の活用に関する検討業務のプロジェクト計画
資料７：検討委員会メーリングリスト登録者名簿

5.2.2.3. 第三回委員会

(1) 日時：平成２４年２月２０日（月）１５時００分～１７時００分
(2) 場所：日本生命丸の内ビル２３Ｆ　Conference Room４
(3) 出席者：
①構成員
手塚構成員（座長）、佐藤構成員、安部構成員、阪東構成員、田中構成員、
小峰構成員、宮北構成員、小野瀬構成員、川野構成員、梅澤構成員
②オブザーバ
総務省 情報流通行政局 情報流通振興課　黒瀬課長、本橋課長補佐、古謝主査
厚生労働省 政策統括官付社会保障担当参事官室　浜田技術参与、鈴木主査
東京電機大学 未来科学部　安田教授
ＮＰＯ団体アスコエ　安井代表
③日立製作所
勝田部長代理、真下技師
④事務局
勝家事務局員、川野事務局員
(4) 議事次第
①開会
②課題ア：研究成果報告書のレビュー
③課題イ：浦添市 ヒアリング結果のご報告
④厚生労働省様
社会保障分野での情報連携のための携帯電話端末の活用に関する検討状況のご報告
⑤課題エ：ガイドライン化の進め方及びガイドライン（案）のレビュー
⑥閉会
(5) 配布資料
資料１：検討委員会（第２回）議事録（案）
資料２：研究成果報告書（一部抜粋）
資料３：浦添市　ヒアリング結果のご報告
資料４：社会保障分野での情報連携のための携帯電話端末の活用に関する検討状況
資料５：別紙：社会保障分野での情報連携のための携帯電話端末の活用に関する想定業務フロー

資料６：ガイドライン化の進め方
資料７：ガイドライン（案）
資料８：学会発表（予定）について

5.2.2.4. 第四回委員会

(1) 日時：平成２４年3月１６日（金）１０時００分～１２時００分
(2) 場所：秋葉原ダイビル　１８Ｆ　Conference Room３
(3) 出席者：
①構成員
手塚構成員（座長)、佐藤構成員、小峰構成員、川野構成員、梅澤構成員
②オブザーバ
総務省 情報流通行政局 情報流通振興課　黒瀬課長、本橋課長補佐、古謝主査
厚生労働省 政策統括官付社会保障担当参事官室　前原室長補佐、浜田技術参与、鈴木主査
内閣官房　情報通信技術（IT）担当　恩田主幹
東京電機大学 未来科学部　安田教授
③日立製作所
勝田部長代理、真下技師
④事務局
勝家事務局員、川野事務局員
(4) 議事次第
①開会
②課題イ：ヒアリング結果のご報告
③議題ウ：制度・運用面の課題の検討結果のご報告
④課題イ：実験環境における機能評価、性能評価のご報告
⑤厚生労働省様
社会保障分野での情報連携のための携帯電話端末の活用に関する検討状況のご報告
⑥閉会
(5) 配布資料
資料１：検討委員会（第３回）議事録（案）
資料２：研究成果報告書（一部抜粋）
資料３：ヒアリング結果のご報告
資料４：制度・運用面の課題のご報告
資料５：社会保障分野での情報連携のための携帯電話端末の活用に関する検討状況

5.3. ガイドライン（案）

電波産業会高度無線通信研究委員会モバイルコマース部会技術専門委員会へインプットするガイドライン案は、検討委員会での議論に基づき、本成果報告書の課題アに記述した内容の全てとする。

下記の ARIB の会合にて、ガイドライン案のインプットを行った。

・会合名：第 23 回モバイルコマース部会技術専門委員会
・日時：平成 24 年 3 月 15 日（木）午後 3 時 30 分～午後 5 時 10 分
・場所：(社) 電波産業会　第 3 会議室
・出席者： NTT ドコモ)、KDDI 研究所、日立製作所、NEC、
NTT コミュニケーションズ、NTT データ等から合計９名（事務局含む）

上記会合での結論としては、各モバイルオペレータのフィージビリティを検討しながら、ガイドラインの位置づけ（誰に向けてのガイドラインか）や、ガイドラインの範囲を今後の ARIB 技術専門委員会で議論していくことなった。

5.4. まとめ

課題エでは、実施計画どおりに検討委員会を設置し、計 4 回の検討委員会を実施した。さらに電波産業会　高度無線通信研究員会　モバイルコマース部会　技術専門委員会へガイドライン（案）をインプットし、本技術の普及促進に努めた。表 5-1 に応募資格に対する本成果報告書の対応個所を示す。

表 5-1 応募資格に対する本成果報告書の対応個所

	実施要領に記載される要件	参照先	対応内容
課題エ	課題ア～ウでの検討・検証結果にあたっては、最適な標準化団体と連携して普及を図る。	5.3	5.3 節で示したように、本事業で検討した結果は、移動体通信事業者、サービス提供機関などがメンバーである ARIB MC 部会において、意見交換、および議論を行うために、ガイドライン案をまとめた。
		5.2 5.3	5.2 節で示したように、NTT ドコモ、KDDI、ソフトバンクモバイル、イー・アクセスの４移動体通信事業者のモバイルセキュリティに強い有識者と、東京工科大学の手塚教授等から構成する委員会で議論を行った。その上で、5.3 節で示したガイドライン案の ARIB MC 部会へのインプットを行った。

6. まとめと今後の課題

6.1. 厚生労働省　「社会保障分野での情報連携のための携帯電話端末の活用事業」との連携による成果と今後の技術課題

本節では、これまで検討委員会等で連携を深めてきた「社会保障分野での情報連携のための携帯電話端末の活用事業（以下、社会保障分野での携帯電話端末活用事業）について、検討状況を整理する。その上で今回、連携したことによる成果と今後、社会保障分野での携帯電話端末活用事業にて求められる技術課題を明らかにする。

6.1.1. 本事業と社会保障分野での携帯電話端末活用事業との連携の目的

社会保障分野での携帯電話端末活用事業では、社会保障分野の情報連携を実現するにあたり、携帯電話を利用した際の活用イメージを検討し、その上で運用面、技術面での課題の検討を進めている。

図 6-1 に示す通り、本事業は厚生労働省と連携することで、厚生労働省等の各省庁、行政機関等のサービス提供機関で横断的に活用可能な携帯電話端末の共通基盤技術の確立を目指すことである。

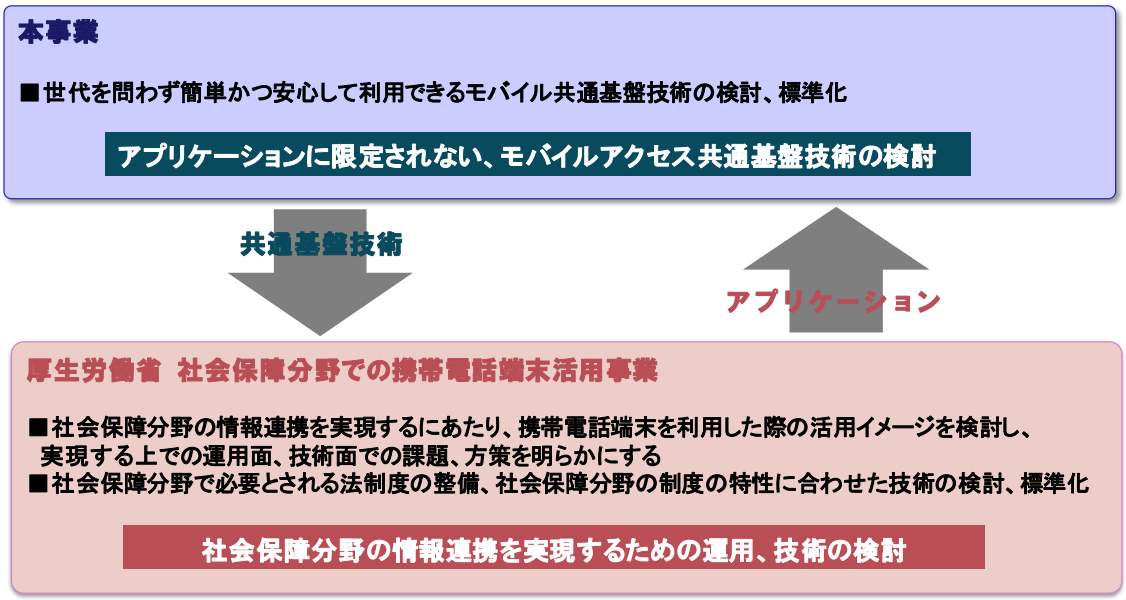


図 6-1 本事業と社会保障分野での携帯電話端末活用事業との連携イメージ

6.1.2.　社会保障分野での携帯電話端末活用事業での検討内容

6.1.2.1.　　概要

(1) 概要

社会保障分野での携帯電話端末活用事業では、「医療分野等における利便性と可用性、および情報の機微性を確保するための情報連携手段として、携帯電話端末の活用技術を確立すること」を目的としている。社会保障分野の情報連携を実現するにあたり、携帯電話端末を活用することが有用だと考えられる活用イメージの検討、取り扱う情報の機微性が高く特段の措置が必要な医療分野での携帯電話端末の代替利用の検討を行った。具体的には、表 6-1 の活用イメージを実現するための携帯電話端末及び認証基盤の要件・課題の検討を行った。

表 6-1 携帯電話端末の活用イメージ一覧

No	活用イメージ
1	医療機関での医療保険の資格確認において、患者（被保険者・被扶養者）が提示する IC カードの代替として携帯電話端末を活用
2	医療機関での医療保険の資格確認において、医療機関の PC 端末やネットワークの障害、あるいは災害等によって一時的にインフラが利用できなくなった場合に医療機関側の端末（PC）の代替として携帯電話端末を活用
3	在宅医療（訪問診療、訪問看護など）での医療保険の資格確認において、医療機関側の端末として携帯電話端末を活用
4	在宅における医療・介護連携として、医者、ケアマネジャー、家族、行政等との連絡掲示板兼在宅介護実施状況を確認するために携帯電話端末を活用
5	同月において複数医療機関を受診した際の高額療養費の窓口現物給付化の際の携帯電話端末の活用（医療機関での自己負担額情報の携帯電話端末への保存など）
6	災害現場での診療等、医療機関外での医療保険資格確認、患者の診療情報等（医療レセプト、調剤レセプト、カルテ（診療簿））を閲覧するために携帯電話端末を活用
7	災害現場での診療等、医療機関外での医療保険資格確認、患者の診療情報等（医療レセプト、調剤レセプト、カルテ（診療簿））を閲覧するために第三者の携帯電話端末を活用

● 活用イメージ例（表 6-1 の No3）

代表的な活用イメージとして、表 6-1 の活用イメージ 3 を図 6-2 に例として示す。

在宅医療（訪問診療、訪問看護など）において、看護師が患者の医療保険の資格確認を行う際に、患者が保有している IC カード（又は携帯電話端末）を看護師の携帯電話端末にかざすことにより、医療保険者のシステムにアクセスし、最新の保険資格を確認するものである。

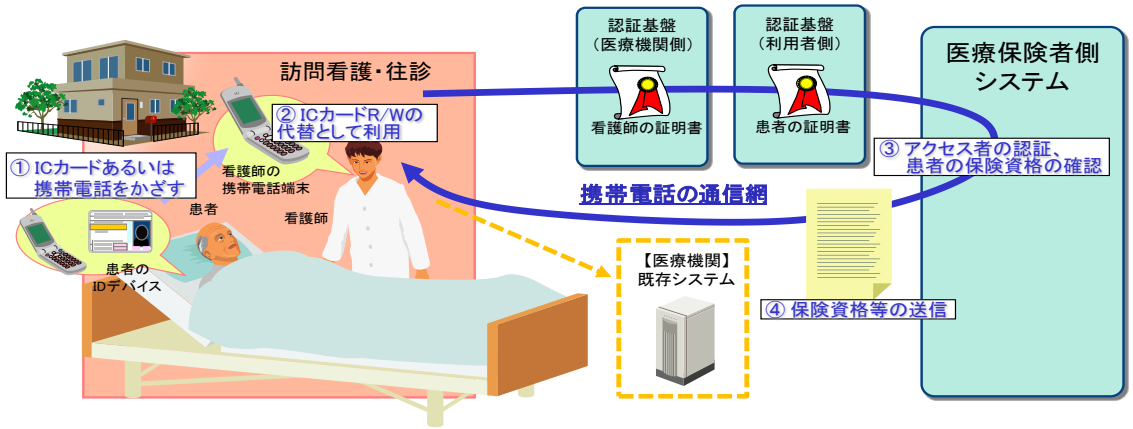


図 6-2 活用イメージ

(2) 検討範囲

図 6-3 に検討範囲を示す。利用者には、IC カードが発行されている前提をおいて、携帯電話端末に IC カードに対するサブキーを格納し、そのサブキーを使うことで携帯電話端末向け社会保障分野のサービス利用を可能する。検討範囲は、サブキー発行の申請からサブキーの発行を検討対象とした。サービス利用の検討においては、携帯電話端末を活用するサービスを検討対象とし、利用者と医療機関間、利用者又は医療機関と、社会保障分野における情報連携基盤間の情報のやりとり部分、医療機関の認証局、利用者の認証局を検討対象とした。

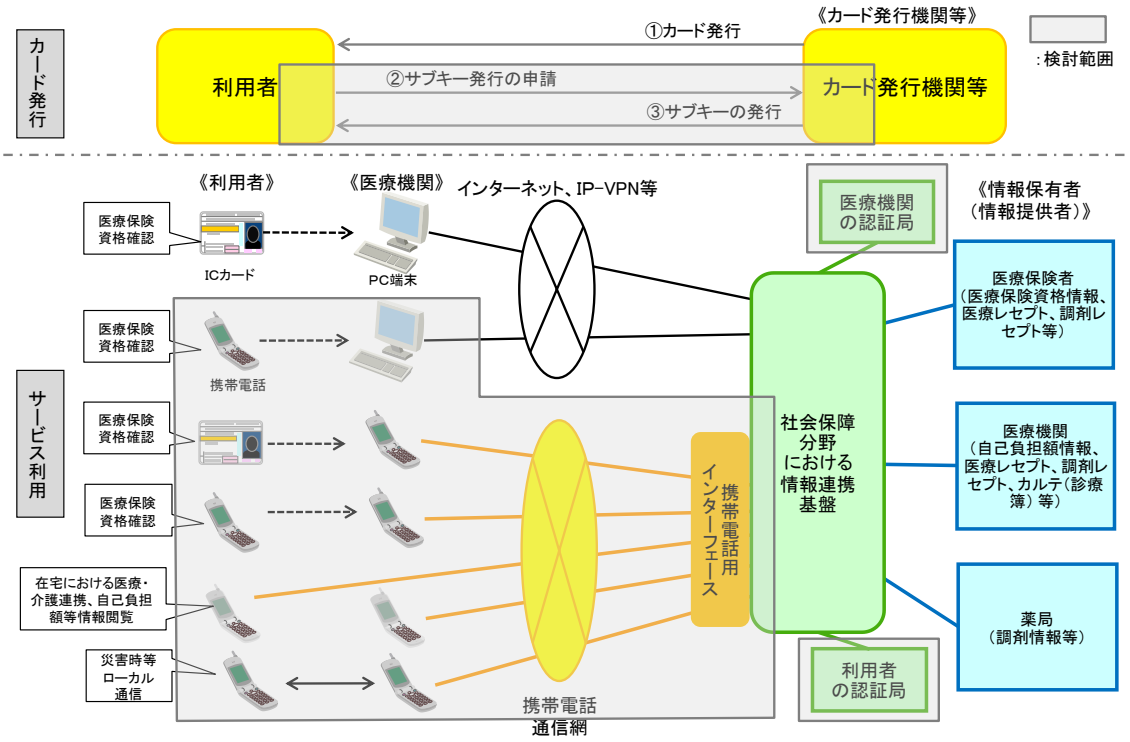


図 6-3 検討範囲

6.1.2.2. 本事業での適用範囲と今後の技術課題

社会保障分野での携帯電話端末活用事業における検討課題に対する本事業で検討した範囲と、今後、検討が必要となる技術課題を明らかにする。

(1) 利用に関する適用範囲と今後の技術課題

本事業では、携帯電話端末の耐タンパデバイスに格納された ID 情報を直接、読み書き可能な方式を検討してきた。

今後の技術課題としては、オフラインでの読み書き可能な方式の検討が必要となる。また、オンライン、オフライン通信を問わず携帯電話端末の認証、証明書による利用者認証及び医療等関連従事者認証の検討が必要となる。

表 6-2 利用に関する検討課題一覧

No	分類	項目	技術課題
1	オンライン利用	携帯電話端末の認証	・携帯電話識別番号の登録・管理・認証の検討 ・携帯電話端末内にあらかじめ格納されている第三者証明書による認証の検討
2		利用者（患者）の PIN 認証	・PIN 有り無しの運用・技術の検討
3		利用者（患者）の認証	・サブキー用証明書の CRL 等によるサブキー用証明書の有効性確認方法の検討
4		医療等関連従事者の認証	・サブキー用証明書の CRL 等によるサブキー用証明書の有効性確認方法の検討
5			・医師、薬剤師、ケアマネジャー等に応じた認証・管理方法の検討
6	オフライン利用	携帯電話端末の認証	・ローカルでの情報のやり取りとなるため、携帯電話端末の契約（通信）状況等による有効性をリアルタイムでの確認は困難である。オフライン時の携帯電話端末の必要可否含め検討
7		利用者（患者）の PIN 認証	・PIN 有り無しの運用に合わせた技術の検討
8		利用者（患者）の認証	・医療等関連従事者の携帯電話端末で利用者のサブキー用証明書の有効性確認方法の検討
10		医療等関連従事者の認証	・利用者の携帯電話端末で医療等関連従事者のサブキー用証明書の有効性確認方法の検討
			・医師、薬剤師、ケアマネジャー等に応じた認証・管理方法の検討

(2) サブキー用証明書のライサイクルに関する適用範囲と今後の技術課題

本事業では、サブキー用証明書の発行や更新時に携帯電話網から携帯電話端末に ID 情報をダウンロードする機能を検討した。

今後の技術課題として、証明書の発行、更新等のライフサイクルに合わせたモバイルアクセスシステムの検討と共に、サブキーとメインキーの紐付けを含めた認証基盤の検討が必要となる。

また、発行端末経由で携帯電話端末にサブキーをダウンロードするモバイルアクセスシステムの検討が必要となる。

表 6-3 サブキー用証明書のライサイクルに関する検討課題一覧

No	分類	項目	検討課題
1	サブキー用証明書のライフサイクル	サブキー用発行端末の正当性の確認	・サブキー、証明書を書き込み可能な端末の限定方法の検討
2		サブキー生成	・鍵ペアの取扱い、生成装置等の検討
3		発行	・窓口での PC 経由での発行方法の検討 ・ネットワーク経由でのオンライン発行方法検討 ・メインキー用証明書の CRL の取得と、メインキー用証明書の有効性確認方法の検討 ・サブキー用証明書のリポジトリ管理方法の検討 ・サブキー用証明書への記載事項の検討 ・UICC の場合、格納領域へのアクセス権、オンラインでのカード AP の発行方法の検討
4		失効 更新 一時停止・解除	・メインキー用証明書のライフサイクルに応じたサブキー用証明書の運用方法の検討 ・携帯電話端末のライフサイクルに応じたサブキー用証明書の運用方法の検討 ・公的ＩＣカードのライフサイクルに応じたサブキー用証明書の運用方法の検討
5		メインキー用証明書との紐付け	・サブキーの用証明書のライフサイクルに応じたメインキー用証明書との紐付け方法の検討 ・メインキー用証明書のライフサイクルに応じたサブキー用証明書との紐付け方法の検討 ・携帯電話端末のライフサイクルに応じたサブキー用証明書の紐付け方法の検討 ・公的ＩＣカードのライフサイクルに応じたサブキー用証明書の紐付け方法の検討 ・サービスを受ける際に複数台の携帯電話端末（耐タンパデバイス）の利用・紐付け方法の検討

(3) 携帯電話端末、公的 IC カード、メインキー用証明書のライフサイクルに関する適用範囲と今後の技術課題

今後の技術課題として、表 6-3 のサブキー用証明書のライフサイクルに対応した認証基盤の検討の際に、携帯電話端末、公的 IC カード、メインキー用証明書のライフサイクルを含めた検討が必要になる。

表 6-4 携帯電話端末の
ライフサイクルに関する検討課題一覧

No	分類	項目	検討課題
1	携帯電話端末ライフサイクル	機種変更	・携帯電話端末本体の携帯電話識別番号による携帯電話端末の認証を行っている際は携帯電話識別番号の変更方法の検討 ・携帯電話端末メモリ内に証明書を格納している際の利用者による移行と失効等の方法の検討
2		契約内容変更	・携帯電話端末の契約者情報を活用している場合は、同期方法の検討
3		契約	・契約者が異なる携帯電話端末の利用許可含め運用方法の検討
4		携帯電話端末の故障	・携帯電話端末本体の携帯電話識別番号による携帯電話端末の認証を行っている際は携帯電話識別番号の変更方法の検討 ・携帯電話端末メモリ内に証明書を格納している際の利用者による一時停止又は、失効等の方法の検討
5		盗難・紛失	・携帯電話端末本体の携帯電話識別番号による携帯電話端末の認証を行っている際は携帯電話識別番号の変更方法の検討 ・利用者による証明書の一時停止、失効等の方法の検討 ・オフラインでの利用不可方法の検討
6		MNP （移動体通信事業者間移動）	・携帯電話端末本体の携帯電話識別番号による携帯電話端末の認証を行っている際は携帯電話識別番号の変更方法の検討 （但し、SIM ロック解除された携帯電話端末をそのまま利用する場合は除く） ・利用者による証明書の移行と失効等の方法の検討
7		解約	・利用者による証明書の失効方法の検討

表 6-5 公的 IC カード、メインキー用証明書の
ライフサイクルに関する検討課題一覧

No	分類	項目	検討課題
1	公的 IC カード ライフサイクル	氏名・住所の変更	・メインキー用認証基盤の登録情報が変更された際のサブキー用認証基盤の登録情報の整合性方法の検討 ・サブキー用証明書へ基本４情報を格納する場合の更新の検討
2		盗難・紛失	・メインキー用証明書が一時停止、失効された場合、サブキー用証明書の一時停止、失効方法の検討
3		故障（IC カード再発行）	・サブキー用証明書の再発行又は、メインキーとサブキーの紐付け変更方法の検討
4		有効期限到来	・サブキー用証明書の有効期限の設定と再交付方法の検討
5		再交付	・サブキー用証明書の再発行又は、メインキーとサブキーの紐付け変更方法の検討
6		回収	・メインキー用証明書の失効時のサブキー用証明書の失効方法の検討
7	メインキー用証明書 ライフサイクル	氏名・住所の変更	・サブキー用証明書へ基本４情報を格納する場合の更新方法の検討
8		盗難・紛失	・メインキー用証明書格納媒体の盗難・紛失時のサブキーの一時停止、失効方法の検討
9		機能損失	・サブキー用証明書の再発行又は、メインキーとサブキーの紐付け変更方法の検討
10		有効期限到来	・サブキー用証明書の有効期限の設定と再交付

(4) サービス特性に関する適用範囲と今後の技術課題

ここでは、社会保障分野での携帯電話端末活用事業における活用イメージ5、6、7において、サービス特性上の検討課題を示す。

今後の技術課題としては、表6-5の活用イメージ6にて示すとおり、オフラインでの読み書き及びローカル保存が一時的に必要となるため、携帯電話端末同士が非接触通信する際のセキュリティ確保や携帯電話端末内でのセキュリティ確保の検討が必要となる。

表 6-6 サービス特性に関する検討課題一覧

No	分類	項目	検討課題
1	サービス特性	活用イメージ5 高額療養費の窓口現物給付化	・利用者と取得した医療保険資格情報の被保険者とが、同一人物であることの確認方法の検討
2			・医療分野において携帯電話端末を活用した場合の、請求・支払方法等に関する事務手続きの検討
3			・携帯電話端末内の情報の完全性の確保方法の検討（要否を含む）
4		活用イメージ6 災害現場での診察等	・携帯電話端末への情報の保存等に関する仕組み・格納場所の検討
5			・書き込む情報が機微な情報である場合に、平常時に持ち歩くことについての想定リスクの検討
6			・違う利用者の情報を読み込んでしまい、誤った診察や処方をしてしまわないための対策の検討(利用者の意識がない場合の携帯電話端末の取り違え防止等)
7			・医師、薬剤師にて参照できる情報の検討（薬剤師は処方箋の情報は読めるが診察結果は読めない等)
8			・携帯電話端末を用いてオフラインの環境下で診察等を実施した場合に、診察結果等を通信復旧後にアップデートする方法の検討
9		活用イメージ7 第三者の携帯電話端末活用	・医療等関連従事者以外の携帯電話端末を活用する場合の、第三者の携帯電話端末に関する取扱方法の検討
10			・医療等関連従事者以外の携帯電話端末を活用する場合の、第三者の携帯電話端末のアプリケーションの配布方法に関する検討
11			・医療等関連従事者以外の携帯電話端末を活用する場合の、第三者の携帯電話端末で読み込んだ患者の情報の取扱の検討

(5) ハードウェア他に関する適用範囲と今後の技術課題

本事業では、サブキーの格納媒体として、複数のサービス提供機関が提供するサービスをセキュアに格納可能なUICCやセキュアSD等の耐タンパデバイスを検討した。

今後の技術課題としては、医療機関、調剤薬局等のサービス提供事業者が連携し、情報の共有、サービス提供できる耐タンパデバイス内のカードAPを検討する必要がある。

また、本事業では、利用者の初期設定、利用する際の負荷軽減として共通アプリを検討した。

表 6-7 ハードウェア他に関する検討課題一覧

No	分類	項目	検討課題
1	ハードウェア	携帯電話端末	・非接触通信機能を有していない携帯電話の場合の通信方法の検討 ・非接触通信可能な媒体を有していない携帯電話の場合の通信方法の検討 携帯電話端末を活用して診療等を実施した場合の、携帯電話端末から既存システムへの転送方法の検討 ・フィーチャーフォンへのセキュア情報格納方法検討
2		格納媒体	・複数事業者の複数サービスの格納 ・サービスレベルに応じた格納媒体の選定
3	その他	操作性	・IT 機器に不慣れな人でも、容易にサービスを受けられるような、携帯電話端末上の操作も含めたサービス運用性（サービス機能やサービスの流れ）の検討
4		証跡管理	・操作やイベントの実行ログの取得方法の検討 ・記録し、保管したログの分析方法の検討 ・それに基づく、認証方法、セキュリティ対策の見直し方法の検討
5	運用	運用体制	・運用主体と運用方法の検討 ・公的機関と移動体通信事業者との連携内容や方法および責任分解点の検討
6		サポート体制	・圏外、電池切れ、アプリ障害等における代替策の検討
7		本人確認方法	・本人確認や端末所有者確認を行う際の運用方法の検討
8		携帯電話端末管理	・医療機関側の携帯電話端末の取り扱い、運用方法の検討

6.1.3. まとめ

社会保障分野での携帯電話端末活用事業における検討課題に対し、本事業での提供可能な範囲を示した。

また、社会保障分野での携帯電話端末活用する際に、必要となる技術課題を表 6-7 に示す。

表 6-8 社会保障分野での携帯電話端末活用事業での技術課題一覧

No	社会保障分野での携帯電話端末活用事業の技術課題
1	オンライン通信での携帯電話端末の認証の検討
2	オフライン通信での携帯電話端末の認証の検討
3	オンライン通信での証明書による利用者認証の検討
4	PIN なしの運用・技術の検討
5	証明書の発行、更新等のライフサイクルを検討した上でサブキーとメインキーの紐付けを含めた認証基盤の検討
6	発行端末経由での携帯電話端末へのサブキーのダウンロードの検討
7	携帯電話端末、公的 IC カード、メインキー用証明書のライフサイクルの検討
8	携帯電話端末同士が非接触通信する際のセキュリティ確保方法の検討
9	携帯電話端末内でのセキュリティ確保の検討
10	医療機関、調剤薬局等のサービス提供事業者が連携し、情報の共有、サービス提供できる耐タンパデバイス内のカード AP の検討
11	携帯電話端末同士が非接触（NFC 等）通信で証明書の認証等を行う方法の検討

6.2. まとめ

課題アでは、サービス提供機関が携帯電話端末利用者の耐タンパデバイスへ ID 情報の書き込みと読み込みを安全かつ容易に行うことを目的に検討を進めた。具体的には、サービス提供機関が耐タンパデバイスにアクセスする際に共通的に利用できるモバイルアクセスサーバおよび携帯電話端末上の共通アプリからなるモバイルアクセスシステムの提案を行った。その結果、サービス提供機関は、個別に携帯アプリを開発しなければならないという負担を減らすことが期待できる。また、利用者は、これまでサービスごとに携帯アプリをダウンロードする必要があったが、共通アプリであれば、ダウンロードの手間が省ける。

さらに、共通アプリを用いることによってユーザインタフェースがブラウザに統一化され、利用者の操作性、利便性を向上させることが期待できる。

課題イでは、課題アで検討した、モバイルアクセスシステムを基盤として、その上で動くデモアプリケーションを開発し、機能評価、性能評価、ヒアリング評価を行った。機能評価により、課題アで検討したシステムが、適切に機能していることを確認できた。性能評価では、2 種類の携帯電話端末を使ったシステムの動作について性能測定を実施し、目標とする約 6 秒で、ID 情報の書込み、およびポイント情報の書き込みが行えることを確認した。ヒアリング評価では利用者及びサービス提供機関にヒアリングを実施し、モバイルアクセスシステムの運用性、有効性を確認できた。また、導入にあたっては、利用者への支援体制が重要であることや、NFC 等の非接触ローカル通信を活用することでさらに、利便性の向上ができることが確認できた。

課題ウでは、モバイルアクセスシステムを適用する際の制度、運用面の課題の検討を行った。具体的は、サービス提供機関へのヒアリングを通して適用サービスを洗い出し、モバイルアクセスシステムを導入する上での課題と対応策案を明らかにした。

課題エでは、実施計画どおりに計 4 回の検討委員会を実施し、モバイルアクセスシステムの議論にとどまらず、行政サービス等への携帯電話端末の適用に向けた活発な議論がなされた。さらに電波産業会　高度無線通信研究員会　モバイルコマース部会　技術専門委員会へガイドライン（案）をインプットし、本技術の普及促進に努めた。

また、本章で、述べた厚生労働省の社会保障分野での携帯電話端末活用事業に関しては、検討委員会等を通じて連携を図り、本事業の適用可能な範囲と、今後の技術課題を共有することができた。

6.3. 今後の検討課題

本節では、1 章から本節までの検討結果を受け、今後、取り組むべき共通基盤技術に関する課題について考察する。

以下に、本事業及び社会保障分野での携帯電話端末活用事業で上がった主な技術課題と、今後、検討を進める上で考慮すべき観点を示す。

表 6-9 主な技術課題と検討の観点一覧

No	技術課題	検討の観点
1	オンライン通信での携帯電話端末所有者の認証の検討 【表 6-7,No.1】	・携帯電話端末の認証については、その要否を含めて検討が必要となる。 例えば、サービス提供機関が、取扱う情報の機微性等を考慮した場合、携帯電話端末の所有者によってアクセス制限を行う必要があるかどうか等。 ・携帯電話端末の認証を行う場合は、認証方法(認証に使用するデータ)の検討が必要となる。
2	オフライン通信での携帯電話端末所有者の認証の検討 【表 6-7,No.2】	
3	オンライン通信での証明書による利用者認証の検討 【表 6-7,No.3,No8】【表 4-46,No1】	・医療分野での活用を想定した場合には、アクセス可能な情報の機微性が高いため、強固な認証基盤が必要となる。 ・耐タンパデバイスに証明書等を格納することでスマートフォンでも安全な認証基盤の確立が必要となる。
4	通信の圏外、災害等の対応として、オフライン通信（NFC 等）での携帯電話端末間の認証方法の検討 【表 6-7,No.9,No11】【表 4-46,No12,16】	・利用者の IC カードまたは携帯電話端末とサービス提供機関の携帯電話端末間の認証方法の検討が必要となる。 例えば、サービス事業者の証明書を利用者が確認する方法の場合には、サービス提供機関の証明書の有効性の確認方法について検討が必要となる。
5	利用者の緊急性や利便性を考慮した PIN なしの運用・技術の検討 【表 6-7,No.4】	・PIN 入力を省略した場合の運用の検討が必要となる。 (PIN あり時と PIN なし時の使い分け、証跡管理を含めたシステム全体でのセキュリティ確保方法の検討等)

6	窓口 PC から携帯電話端末に証明書を格納する方法の検討 【表 6-7,№6】【表 4-46,No1,No9】	・窓口端末を使い携帯電話端末に証明書を発行する際の安全な発行方法の検討が必要となる。
7	証明書の失効、更新等のライフサイクルを検討した上でサブキーとメインキーの紐付けを含めた認証基盤の検討 【表 6-7,No5,No7】 【表 4-46,No10,No11,No15】	・携帯電話、IC カード等のライフサイクルを考慮した上でサブキー用の認証基盤の検討が必要となる。
8	医療機関、調剤薬局等のサービス提供事業者が連携し、情報の共有、サービス提供できる耐タンパデバイス内のカード AP の検討 【表 6-7,№10】【表 4-46,No3,No4】	・各サービス事業者がカード AP を開発することは、非効率な開発と手数料が発生する。利用者には、サービス毎にカード AP をダウンロードする必要があるため、普及の妨げになるため、共通で利用できるカード AP の検討が必要となる。

※【　】は、表 6-7 の社会保障分野での携帯電話端末活用事業での技術課題一覧と、表 4-46　技術上の課題と対応策の対応状況を示す。

以上から、今後検討すべき共通基盤技術の課題を以下に示す。

(1) 利用に関する共通基盤技術の課題

利用に関しては、本事業では携帯電話端末の耐タンパデバイスに、オンラインで ID 情報を読み書き可能な方式を検討してきた。

今後は、オンラインでの携帯電話端末の認証、証明書による認証の検討が必要となる(表 6-8,No1,No3)。

また、オフライン通信に関しても携帯電話端末の認証、証明書等を含んだ ID 情報による利用者認証の検討する必要がある(表 6-8,No2,No4)。

具体的には、携帯電話端末間、携帯電話端末とサービス提供機関等のサーバ間でのセキュアな読み書き方式等を検討する必要がある。

(2) 発行等のライフサイクルに関する共通基盤技術の課題

発行等のライフサイクルに関しては、本事業では様々なサービス提供機関が共通的に携帯電話端末から耐タンパデバイスへ ID 情報を書き込み(発行)可能な方式を検討してきた。今後は、モバイルアクセスシステムを用いて、証明書のライフサイクルを考慮した書き込み方式を検討する必要がある(表 6-8,No7)。

また、携帯電話端末へ直接、証明書等を書き込むだけでなく、その延長線上で窓口端末を使い、証明書を安全に書き込む仕組みも検討する必要がある(表 6-7,No6)。

(3) 共通利用可能な耐タンパデバイス内のカードAPの検討

医療機関、調剤薬局等のサービス提供事業者が連携し、情報の共有、サービス提供できる耐タンパデバイス内のカードAPを検討する必要がある。また、オフラインでのPIN認証も含め検討する必要がある(表6-8,No5,No8)。

今後は、これら課題の解決に向け引き続き、厚生労働省の社会保障分野での携帯電話端末活用事業と連携し、社会保障分野での実運用に適した共通基盤技術の検討を進めると共に、自治体等と連携し、電子行政サービス分野等での活用を目指した共通基盤技術の検討が重要である。

7. 学会発表等

7.1. 論文

(1)一般社団法人情報処理学会　第 57 回 CSEC・第 17 回 IOT 合同研究発表会
①タイトル：モバイルアクセス基盤の検討
②著者名：梅澤 克之、川野 隆、森田 伸義、礒川 弘実、萱島 信（日立）
③発表者名：梅澤 克之
④場所：秋田大学　手形キャンパス
④日時：2012 年 5 月 10 日～11 日

(2)一般社団法人情報処理学会　第 151 回 DPS・第 62 回 MBL 合同研究発表会
①タイトル：モバイルアクセス基盤システムの開発
②著者名：梅澤 克之、川野 隆、森田 伸義、礒川 弘実、萱島 信（日立）
③発表者名：梅澤 克之
④場所：沖縄県青年会館
⑤日時： 2012 年 5 月 21 日～22 日