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）
成果報告書

2012年3月30日

株式会社日立製作所

1. 事業概要：背景と目的

HITACHI
Inspire the Next

背景

政府の動向

✓ 政府目標で国民の50%以上、利用頻度・利便性の高い行政サービスを週7日24時間のオンライン利用を掲げている※1

サービス提供機関の動向

✓ 携帯電話では確実な本人認証手段がないため、サービスメニューは限定的
✓ 一方で、パソコン利用では、場所を問わない24時間のオンラインサービスの提供は困難
✓「携帯アプリ」等の開発・運用に多大なコストが発生

サービス利用者の動向

✓ サービス提供機関ごとの「携帯アプリ」のダウンロード・インストールが面倒で分かりにくい
✓ ブラウザと「携帯アプリ」で提供サービスが異なり、ユーザインタフェースが同一でない

課題認識

①携帯電話による電子行政サービスの適用範囲の拡大

②利用者による設定の簡素化、操作性などの向上

③サービス提供機関の導入・運用負荷の軽減

目的

携帯電話から電子行政サービスなどを簡単かつ安全に利用できる仕組みの実現

※1:“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）

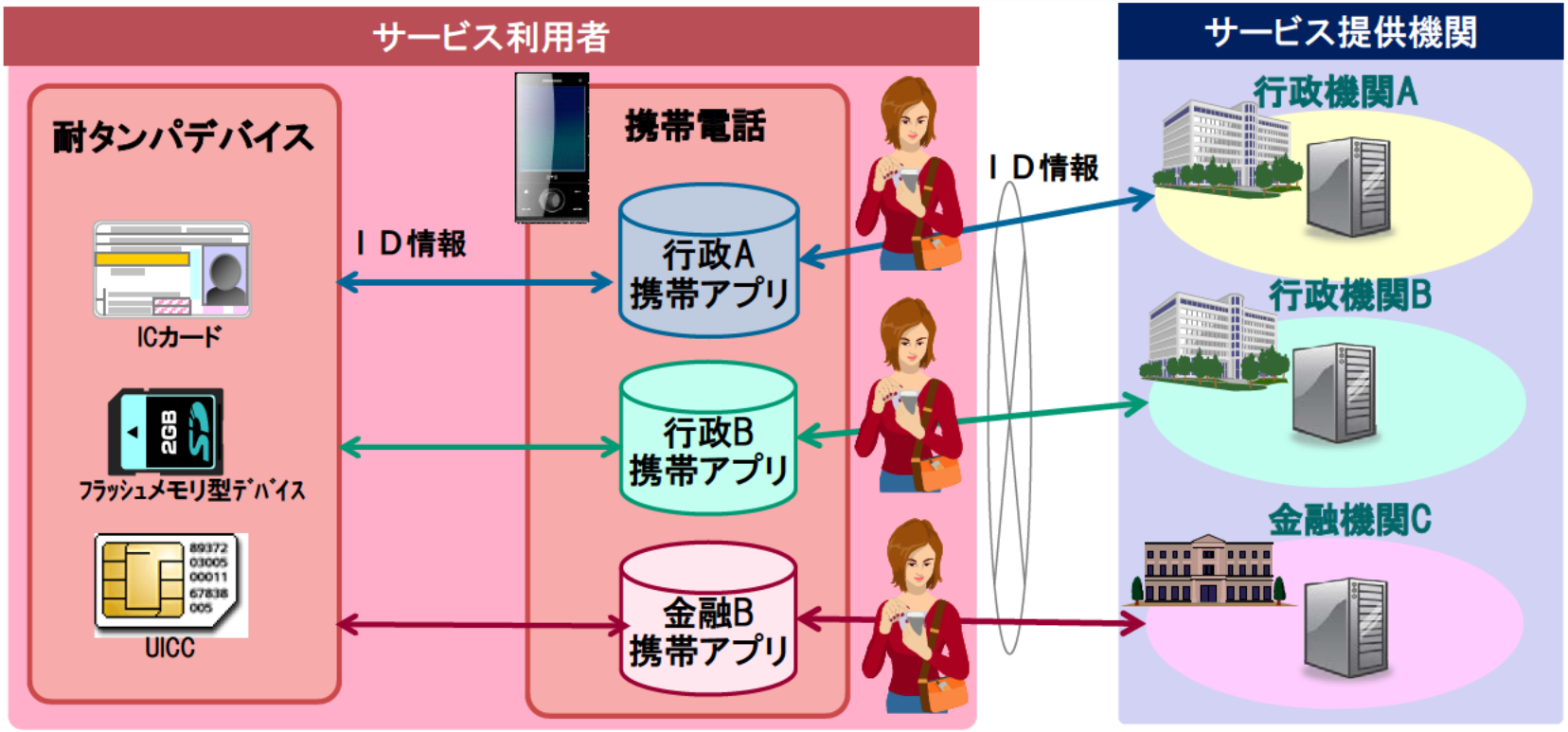
1. 事業概要：現状の課題

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※1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ID情報の安全な格納先として、フルサイズのICカード、ICチップを搭載したフラッシュメモリ型デバイス、UICCの耐タンパデバイスが想定されている。

しかしながら、現状では耐タンパデバイスにID情報を格納・利用には、**携帯電話上にアプリケーション（以下、「携帯アプリ」）が必要**となり、以下の課題が存在する。

■行政機関等のサービス提供機関ごとに携帯アプリを**個別に開発、運用が必要**。

■利用者は、利用したいサービス提供機関毎に携帯アプリを**ダウンロード・インストールが必要**。

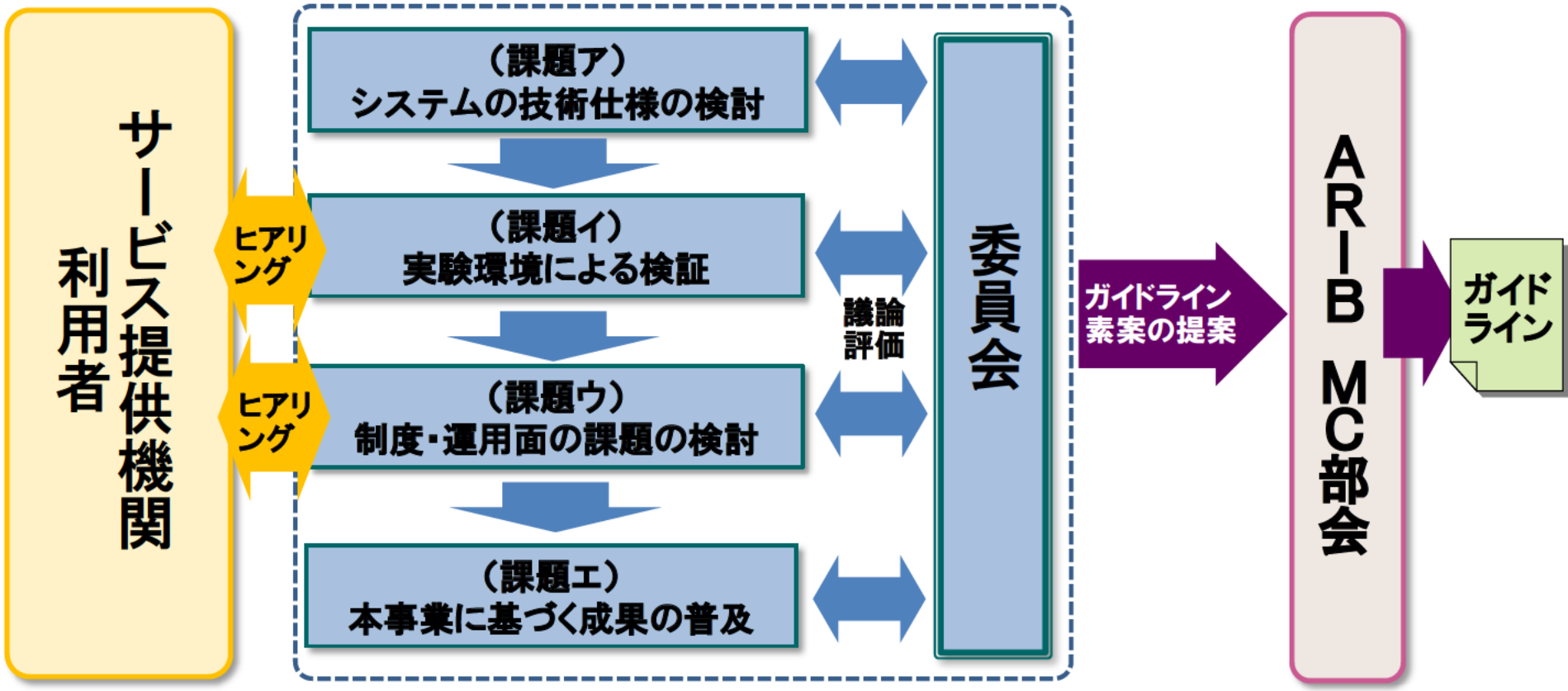


※1：H21年度 「電子行政サービス等によるアクセス手段の多様化に関する調査研究（携帯電話からの電子行政サービス等へのアクセス技術の調査研究）」

1. 事業概要：課題解決のための進め方

HITACHI
Inspire the Next

- 課題アで技術仕様の策定し、その結果に基づき、課題イで実証環境を構築・検証、課題ウで制度・運用面の課題・方策の検討を行う。
- 課題エでは、成果普及のために課題アの技術仕様に基づき、ガイドライン素案を作成し、一般社団法人 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（以下、ARIB MC部会）にて議論・検討を行い、ガイドライン化を推進する。
- 課題ア～エの検討を行う際には、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、議論を行う。

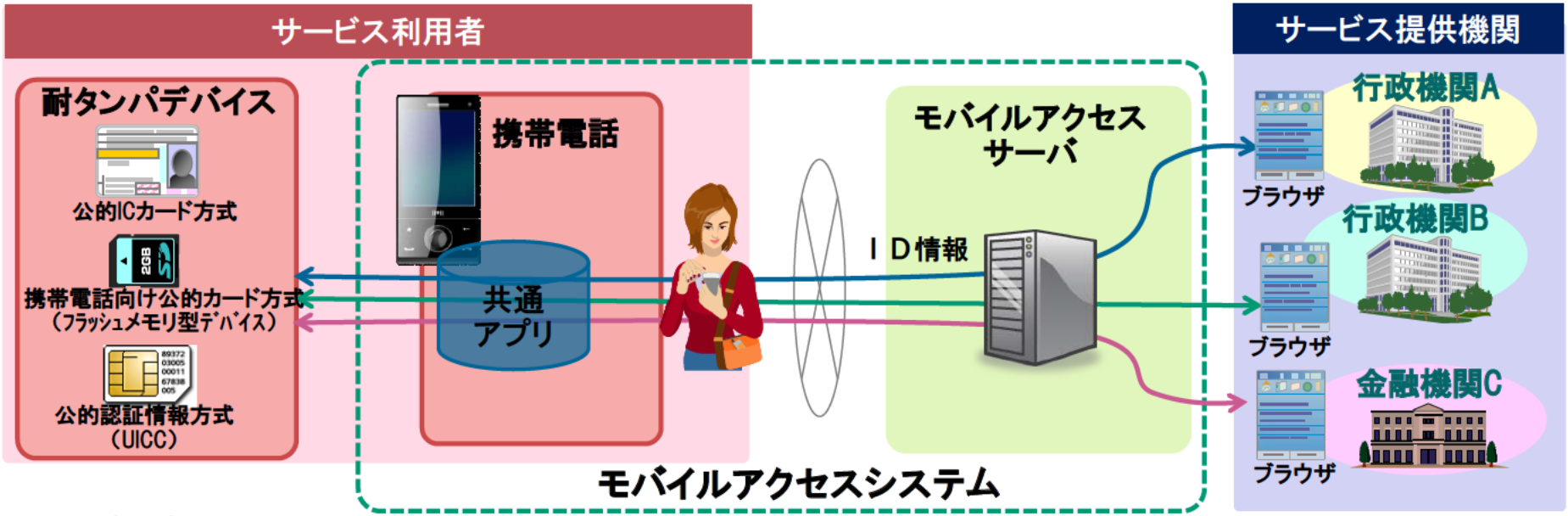


2. 成果目標の達成状況：課題ア(1)

HITACHI
Inspire the Next

成果目標	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策定
実施内容	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。
達成状況	・ID情報のセキュアな送受信を行うモバイルアクセスサーバと、ブラウザ連携し、ID情報の耐タンパデバイスへの書込み・読込みを行う複数のサービス提供機関が共通的に利用できる携帯アプリケーション(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を策定した。 ・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した。 ・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(ICカード)」「携帯電話向け公的カード方式(ﾌﾗｯｼｭﾒﾓﾘ型ﾃﾞﾊﾞｲｽ)」「公的認証情報方式(UICC)」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した。

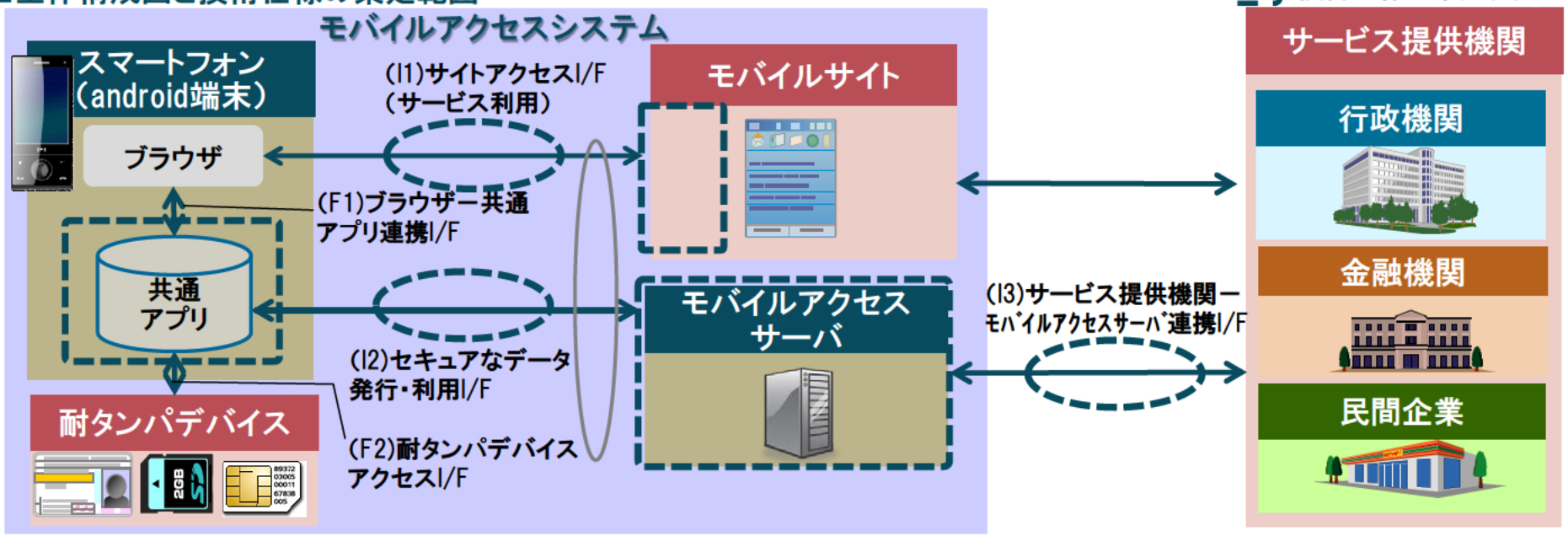
■技術仕様概要図



2. 成果目標の達成状況：課題ア(2)

HITACHI
Inspire the Next

■全体構成図と技術仕様の策定範囲



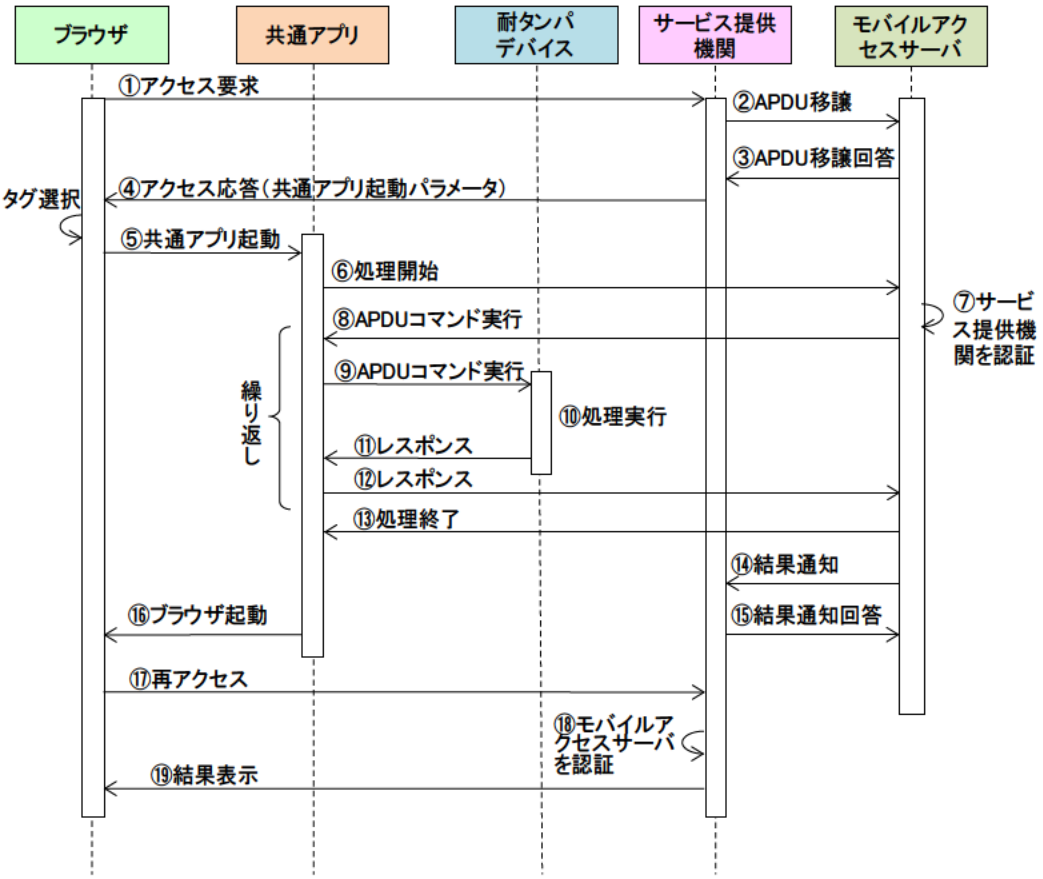
■機能概要

項目	機能概要
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。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。また、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。
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。サービス提供機関から送信された情報(APDUコマンド等)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。また、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。
共通アプリ	モバイルアクセスサーバと通信を行い、受信した暗号データ(コマンド)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し、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)を想定する。

2. 成果目標の達成状況：課題ア(3)

HITACHI
Inspire the Next

■データの流れ図



■セキュリティ対策

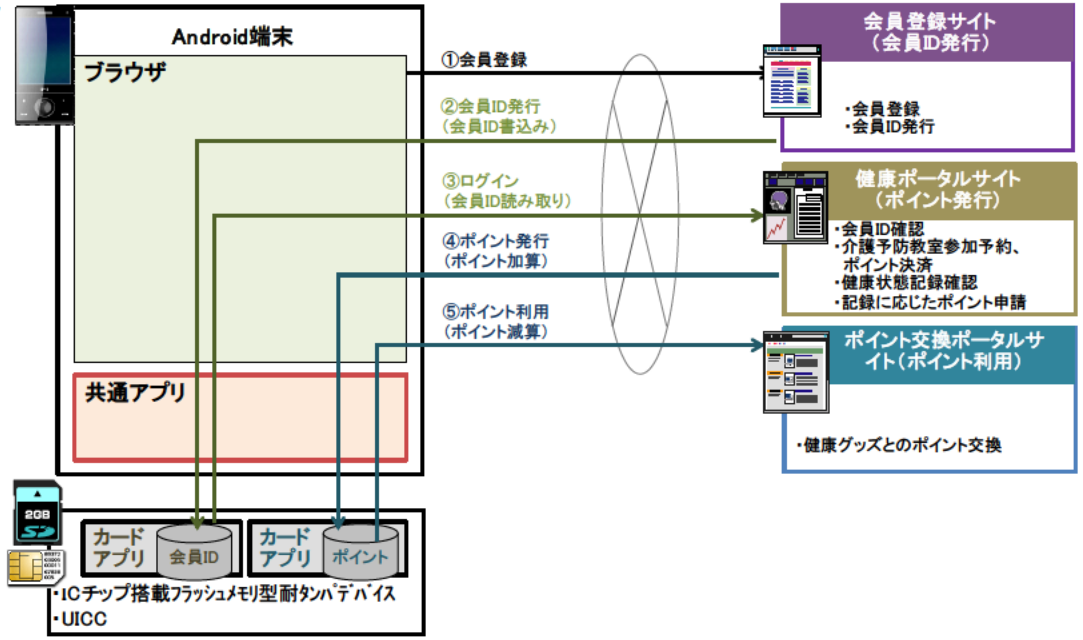
要件	対策
悪意のある携帯電話端末アプリケーションによる耐タンパデバイス内のセキュアデータへのアクセスの防止	耐タンパデバイスへアクセスするためには、耐タンパデバイスと相互認証を行ったうえで安全な通信路を確保（セキュアセッションの確立）するようにし、共有鍵を持たない携帯電話端末アプリケーションは、耐タンパデバイスにアクセスできないようにした。また、共通アプリも共有鍵を持たず、モバイルアクセスサーバ側に共有鍵を持たせることで、共通アプリがマルウェアやウィルスに感染しても共有鍵が漏洩することがないような設計にした。
サービス提供機関―（共通アプリ）―モバイルアクセスサーバ間の通信路の安全性の確保	④、⑤、⑥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。
モバイルアクセスサーバー（共通アプリ）ー耐タンパデバイス間の通信路の安全性の確保	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。
サービス提供機関ーモバイルアクセスサーバ間の通信路の安全性の確保	前提条件として、サービス提供機関ーモバイルアクセスサーバ間の通信路は、VPNや専用線などで保護されており、安全性は確保されているものとする。
サービス提供機関の成りすましの防止	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。
モバイルアクセスサーバの成りすましの防止	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. 成果目標の達成状況：課題イ(1)

HITACHI
Inspire the Next

成果目標	課題アの技術仕様に基づく実験環境の構築・検証
実施内容	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。
達成状況	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からなる実証環境を構築し、機能評価、性能評価、ヒアリング評価を行った。 ・機能評価では、課題アで検討したシステムが、十分な機能を備えていることを確認した。 ・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、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。 ・ヒアリング評価では、サービス提供機関及び利用者、移動体通信事業者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、ユーザビリティを確認した。

■実証環境



2. 成果目標の達成状況：課題イ(2)

HITACHI
Inspire the Next

■ヒアリング評価

a.実施概要(1):浦添市

項目	内容
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

a.実施概要(2):台東区

項目	内容
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

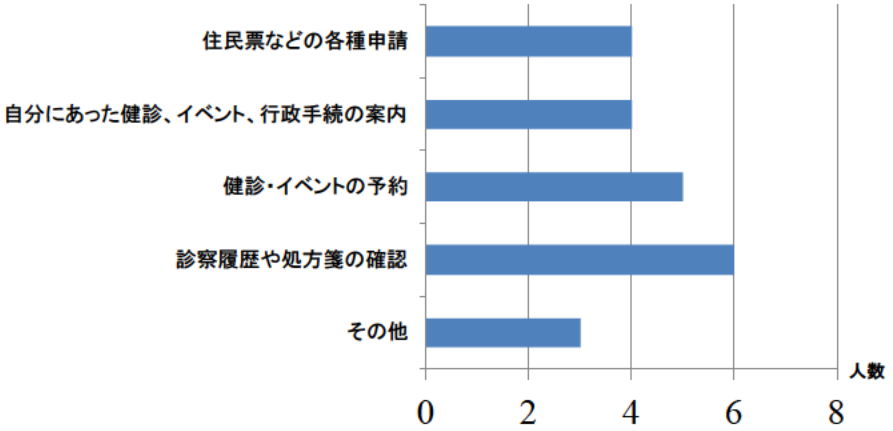
b.実施手順

以下の①から④の手順で説明、ヒアリング等を実施した。

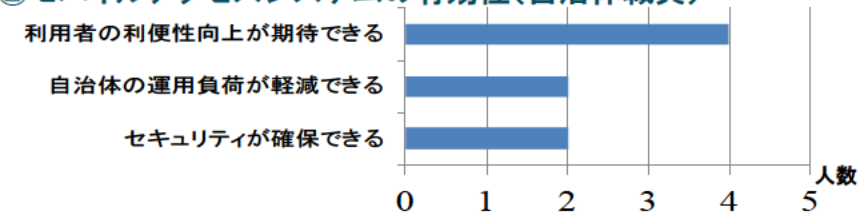
①モバイルアクセスシステムを活用した想定される自治体提供サービスの概要説明
②デモ内容の説明
③利用者によるスマートフォンからのモバイルアクセスシステム利用
④その結果を係員がヒアリングし、ヒアリングシートに記載

c.ヒアリング結果

①モバイルアクセスシステムで実現してほしい行政サービス(利用者)



②モバイルアクセスシステムの有効性(自治体職員)



③数字の入力に関する操作性について(利用者)

※「文字、画面、入力スペースが小さい」との意見が多かった。

2. 成果目標の達成状況：課題ウ

HITACHI
Inspire the Next

成果目標	モバイルアクセスシステムを導入する際の制度・運用面の課題の検討
実施内容	課題アおよび課題イでの検討・検証結果に基づき、実際に導入するにあたって想定される制度・運用・技術面での課題抽出と、その対応案を策定する。
達成状況	・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適用サービスを選定した。 ・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・整理した。 ・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、制度、環境、政策動向等より実現性を評価した。 ・適用サービスによる想定業務フローを策定。現行の制度・運用と対比し、課題を抽出した。 ・抽出した課題を整理し、対策案、方針等を検討した。

■モバイルアクセスシステムを検討する上での主な課題

	主な課題
運用	ID情報をスマートフォンに格納する際の本人確認方法
	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）
	スマートフォンの契約者が異なる場合や複数台での利用可否の検討と運用方法
	端末所有者確認を行う際の運用方法
	スマートフォンの利用一時停止や紛失、故障、契約解除等のライフサイクルに応じた手続き及び、証明書の処理方法
	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
	圏外、電池切れ、アプリ障害における代替策の用意
	公共施設等でスマートフォンを読み取るための環境の整備
	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
制度	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
	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
技術	電子証明書等のID情報を格納する際の発行端末の認証方法
	スマートフォンと外部端末とのローカル通信でのID情報のやり取りを考慮したモバイルアクセスサーバの仕組み

2. 成果目標の達成状況：課題エ

HITACHI
Inspire the Next

成果目標	本事業に基づく成果の普及
実施内容	本事業の成果となる技術仕様に関してはARIB MC部会を活用しながらガイドライン化を図る。
達成状況	・関連する業界の代表的な企業として、(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からなる検討委員会を設置し、計4回開催した。 ・検討委員会にて課題ア～課題ウでの検討・検証結果に対して、議論した。 ・ガイドライン化を目指し、ガイドラインの素案をARIB　MC部会にインプットした。

■委員会構成(敬称略)

手塚 悟 (東京工科大学)
佐藤 一夫、安部 孝太郎((株)NTTドコモ)
阪東 謙一、田中 卓弥(KDDI(株))
小峰 正裕、立原 彩子(ソフトバンクモバイル(株))
渡辺 芳治、宮北 幸典(イー・アクセス(株))
小野瀬 健太郎、川野 隆、梅澤 克之((株)日立製作所)
以下にオブザーバを示す。
黒瀬 泰平、本橋 充成、古謝 玄太(総務省)
前原 正男、浜田 哲、鈴木 重郎(厚生労働省)
安田 浩(東京電機大学)
安井 秀行(NPO団体アスコエ)
以下に事務局を示す。
勝家 由樹、川野 隆((株)日立製作所)

■ガイドライン化の状況

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)
・状況：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等を議論中。

■委員会実施実績

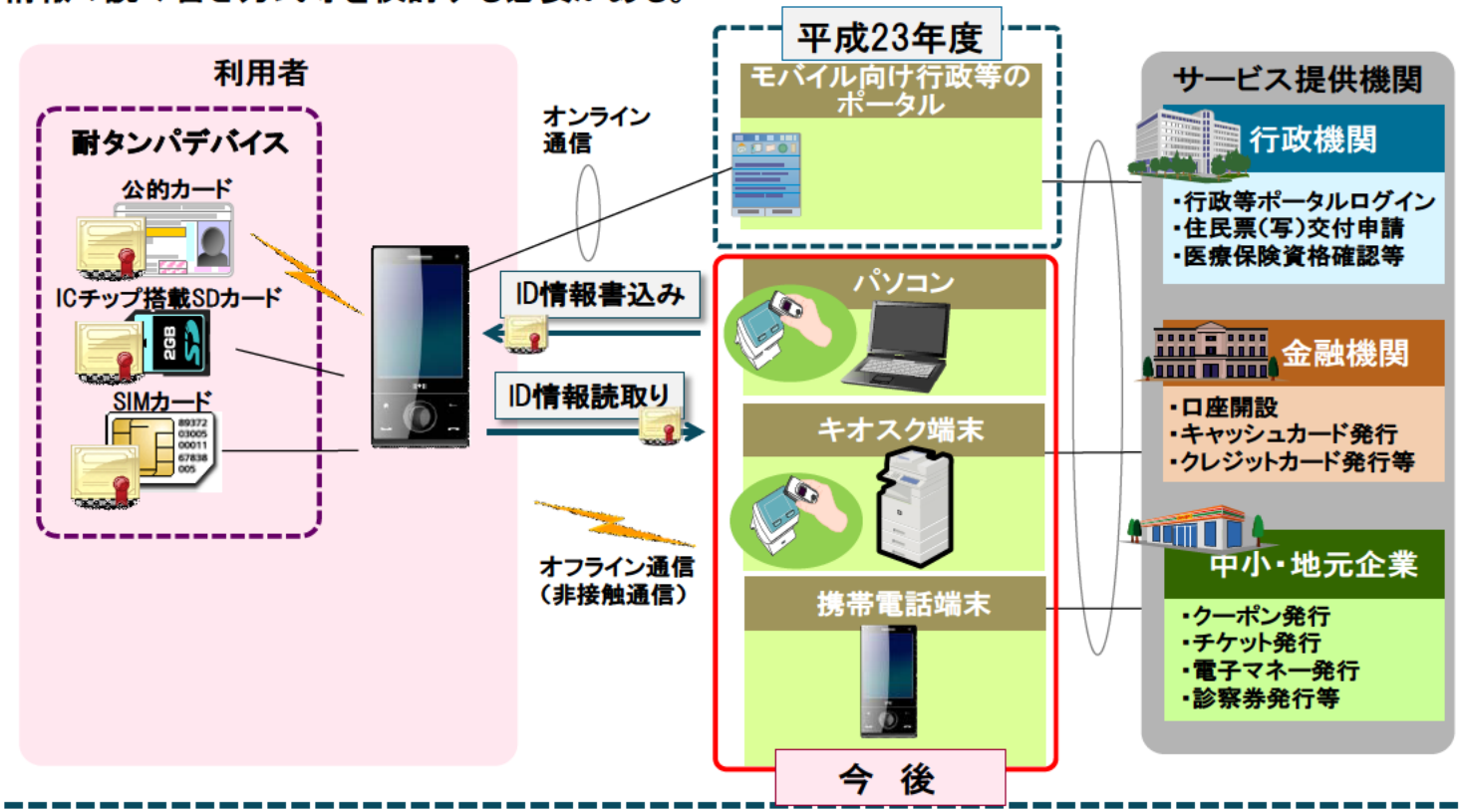
●第一回委員会
・日時：平成23年12月19日(月)13時00分～14時30分
・場所：秋葉原UDXビル20F　Conference Room3
●第二回委員会
・日時：平成24年1月23日(月)15時00分～17時00分
・場所：日本生命丸の内ビル23F　Conference Room5
●第三回委員会
・日時：平成24年2月20日(月)15時00分～17時00分
・場所：日本生命丸の内ビル23F　Conference Room4
●第四回委員会
・日時：平成24年3月16日(金)10時00分～12時00分
・場所：秋葉原ダイビル18F　Conference Room3

■学会・論文発表

●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
・日時：2012年5月10日～11日
・タイトル：モバイルアクセス基盤の検討
・著者名：梅澤 克之、川野 隆、森田 伸義、礒川 弘実、萱島 信(日立)
・場所：秋田大学　手形キャンパス
●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
・日時：2012年5月21日～22日
・タイトル：モバイルアクセス基盤システムの開発
・著者名：梅澤 克之、川野 隆、森田 伸義、礒川 弘実、萱島 信(日立)
・場所：沖縄県青年会館

3. 今後の検討課題

本事業ではAndroid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、非接触通信機能を活用したオフライン通信に関し、証明書等のID情報の読み書きを検討する必要がある。
具体的には、利用者のAndroid端末とサービス提供機関のパソコン、キオスク端末(マルチコピー機等)、Android端末とのセキュアな情報の読み書き方式等を検討する必要がある。

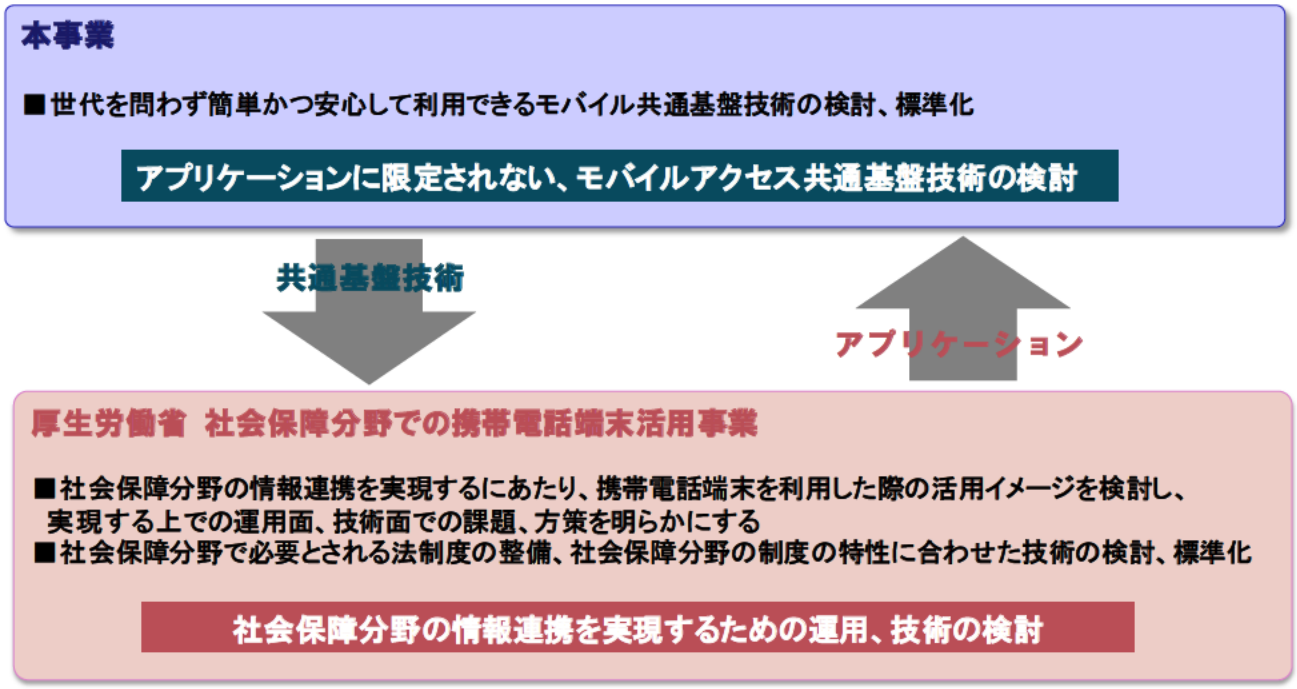


【アプリケーション例】
・行政窓口端末(パソコン)にてAndroid端末の耐タンパデバイスに証明省等のID情報を書込み
・Android端末にてオンラインで証明書等の申請を行い、コンビニ、行政機関に設置されている行政キオスク端末(マルチコピー機等)にAndroid端末をかざし、申請した証明書を印刷・受取
・利用者のAndroid端末と行政職員又は、医療従事者のAndroid端末同士をかざし、認証後に行政職員又は、医療従事者のAndroid端末に利用者情報(診察・投薬履歴情報等)を表示

■本事業との連携の目的

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（以下、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た。

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。



連携イメージ

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」概要

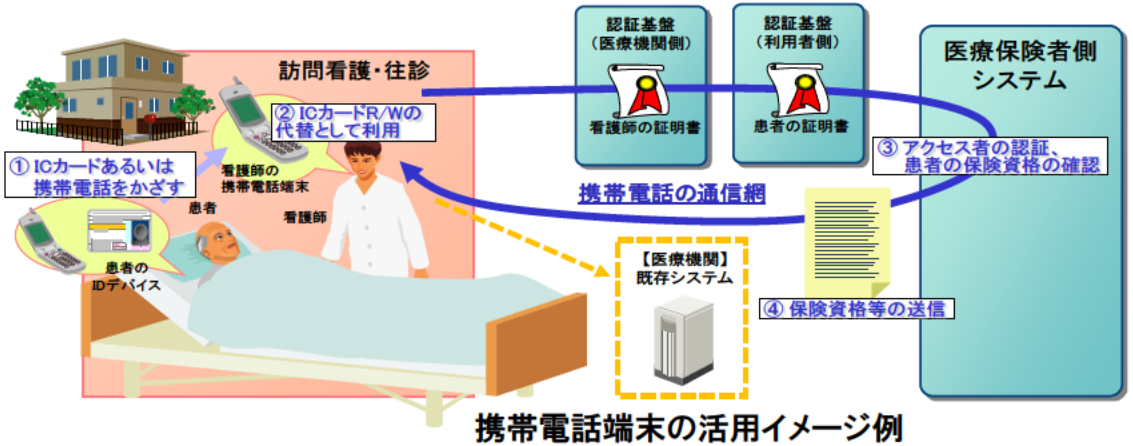
HITACHI
Inspire the Next

■活用サービス

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。

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 ※「携帯電話端末の活用イメージ例」参照
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



携帯電話端末の活用イメージ例

HITACHI
Inspire the Next

■社会保障分野での携帯電話端末活用事業の技術課題

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の検討を行った。

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