Vol.2012-CSEC-57 No.17
Vol.2012-IOT17 No.17
2012/5/11

モバイルアクセス基盤の検討

梅澤 克之[1]　川野 隆[2]　森田 伸義[3]　礒川 弘実[3]　萱島 信[3]

概要：国内の携帯電話契約数は 1 億 1200 万件を超え，重要なインフラとなった．また，ポイントや電子マネー，会員 ID 情報などの秘匿性の高い情報（以降，ID 情報と呼ぶ）を扱うサービス提供機関も増えてきた．このようなサービス提供機関が携帯電話端末の耐タンパデバイスへの ID 情報の読み書きを行おうとする場合，現状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．本研究では，上記のような現状の課題を解決するためのモバイルアクセス基盤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基盤システムを提案する．

キーワード：モバイル，携帯電話，スマートフォン，耐タンパデバイス，IC カード

A Study on Mobile Access Infrastructure

Katsuyuki Umezawa[1]　Takashi Kawano[2]　Nobuyoshi Morita[3]　Hiromi Isokawa[3]
Makoto Kayashima[3]

Abstract: The number of the domestic cellphone contracts was beyond 112 million. The cellphone became the important infrastructure. In addition, the service provider who treated secure information such as a point and electronic money, the subscriber ID information (we call it ID information) increased. Such a service provider reads and writes ID information to the tampa-resistant device of the cellphone. When service provider reads and writes the ID information to tampa-resistant device, it is necessary to develop application for cell-phones every service provider under the present conditions. In addition, it is necessary for the user to download and install application for the cell-phones which each service provider offers individually. The security mechanism of the application of the cellphone is necessary. In this study, We propose a mobile access infrastructure system to solve such a problem.

Keywords: Mobile, Cellular Phone, Smart Phone, Tamper Resistant Device, Smart Card

1. はじめに

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．

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

[1] 日立製作所 情報システム事業部
Hitachi, Ltd. Information Technology Division
[2] 日立製作所 セキュリティ・トレーサビリティ事業部
Hitachi, Ltd. Security & SmartID Solutions Division
[3] 日立製作所 横浜研究所
Hitachi, Ltd. Yokohama Research Laboratory

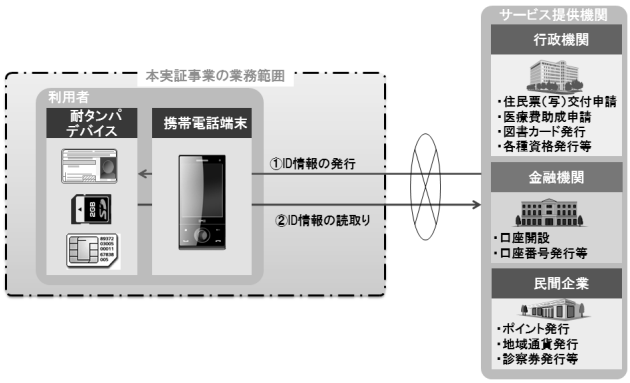

図 1 本研究の対象業務

府目標が掲げられている．

これらの目標を実現するためには，携帯電話端末の耐タンパデバイスを活用することが重要である．耐タンパデバイスへ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（以降，ID 情報と呼ぶ）を格納し，これらの格納した情報を読み書きすることで，安全，便利に電子行政サービスを受けることが可能となる．

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（以降，携帯アプリと呼ぶ）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．

本研究では，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して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を行う．

以下では，まず，2 章で概要を述べ，3 章に前提条件を記述する．4 章にセキュリティ要件を列挙し，5 章で提案システムについて記述する．6 章でセキュリティ要件に対する対策を示し，最後に 7 章でまとめと今後の課題を示す．

2. 概要

2.1 対象業務

本研究の対象業務を図 1 に示す．図 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 情報の書き込こむ．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．

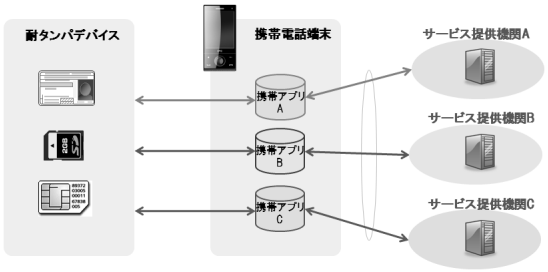

図 2 現状の課題

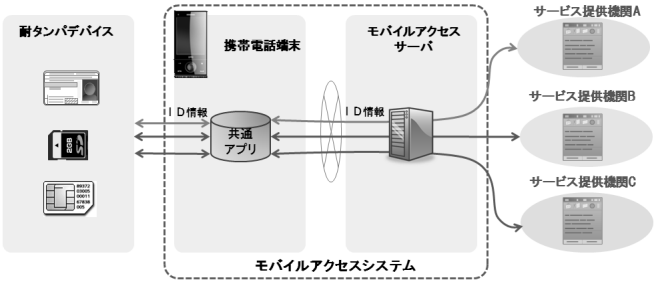

図 3 解決方法

2.2 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 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．

2.3 解決方法

上記現状の課題を解決するために，図 3 に示すような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．

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・参照の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．

3. 前提条件

以下に本研究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，本研究の範囲外とする．

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が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のもとする．

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　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)，　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，　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[3] に準拠した IC カードを前提とする．

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．用いるため，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とする．

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おこな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．

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．

4. 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

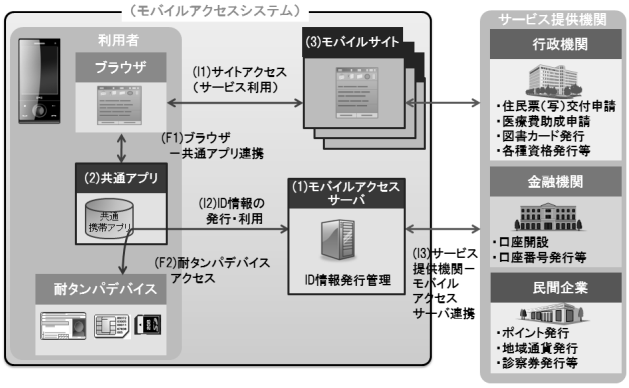

図 4 提案システムの全体構成

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が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)** サービス提供機関ー(共通アプリ)ー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) ー耐タンパデバイス間の通信路の安全性の確保
- **(2-3)** サービス提供機関ー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

5. 提案システム

5.1 全体システム構成

提案システムの全体構成を図 4 に示す．図 4 に示すように，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，何らかの価値を有する情報（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対象とする．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．

表 1 図 4 の各エンティティの説明

No.	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．

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のち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．

5.2 システム概要

5.2.1 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 4 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

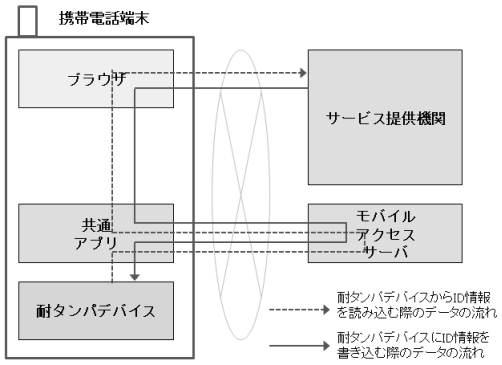

図 5 データの流れを示す簡略図

に返信する．

(2) 共通アプリ（全機能）（図 4 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 4 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．

5.2.2 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 5 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 5 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 情報の流れであり，点線の矢印が，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．

図 6 にデータの流れを表わすさらに詳細なフローを示す．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

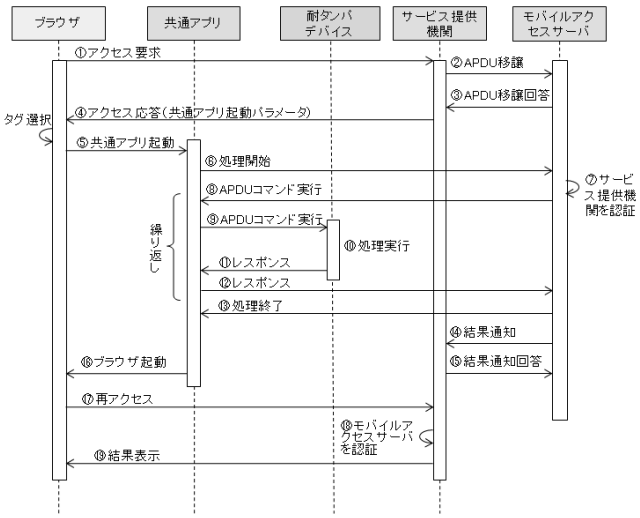

図 6 データの流れを示す詳細図

要求をを送信する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⑪ ⑫ ．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 6 では，② ，③ と⑬ ，⑭ 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．

6. セキュリティ対策に関する考察

本節では，4 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

【要件 (1-1)】悪意のある携帯電話端末アプリケーションが耐タンパデバイス内のセキュアデータへのアクセス防止

【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

【要件 (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

【対策】図 6 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．

【要件 (2-2)】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

【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 [3] 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．

【要件 (2-3)】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

【対策】3 節のネットワークに関する前提条件で示したように，サービス提供機関ー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

【要件 (3-1)】サービス提供機関の成りすましの防止

【対策】図 6 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．

【要件 (3-2)】モバイルアクセスサーバの成りすまし防止

【対策】図 6 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．

7. まとめ

本研究では，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，いま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．

謝辞 本研究は，総務省の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) の成果の一部である．

商標等に関する表示

- JavaScript は，Oracle Corporation 及びその子会社，関連会社の米国及びその他の国における登録商標または商標です．

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）
[3] GlobalPlatform Card Specification Version 2.1.1 March 2003.