Vol.2012-DPS-151 No.18
Vol.2012-MBL-62 No.18
2012/5/22

モバイルアクセス基盤システムの開発

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．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開発する．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，サービスを提供するサービス提供機関，耐タンパデバイス内の IC カードアプリからなるモバイルアクセス基盤システムを開発し，性能評価を行う．

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

Development of Mobile Access Infrastructure System

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 develop a mobile access infrastructure system to solve such a problem and evaluate the developed system.

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

1. はじめに

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た．また，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．このような携帯電話端末を使ってサービスを安全に受けるには，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．しかしながら，現状では，耐タンパデバイスに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．

[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

Vol.2012-DPS-151 No.18
Vol.2012-MBL-62 No.18
2012/5/22

文献 [2] では，これらの負担を解消するため，図 1 に示すようなサービス提供機関・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した．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った．

本研究では，上記の検討に基づいたモバイルアクセス基盤システムを開発し，評価を行う．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，サービスを提供する仮想的なサービス提供機関，耐タンパデバイス内の仮想的な IC カードアプリからなるモバイルアクセス基盤システムを開発し，性能評価を行う．

以下では，まず，2 章で概要を述べ，3 章で提案システムについて記述する．4 章で実証実験システムについて示し，5 章で性能評価を行う．最後に 6 章でまとめと今後の課題を示す．

2. 概要

2.1 対象業務

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．

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，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．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．

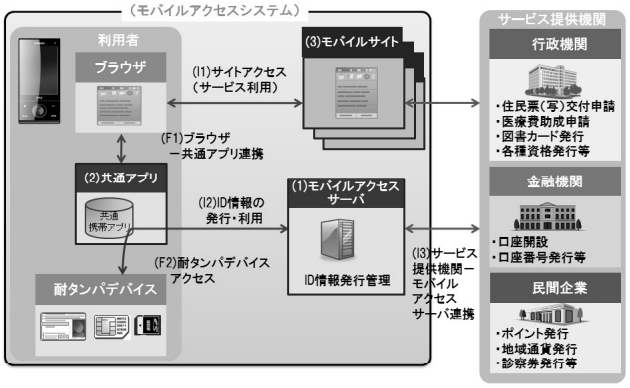

図 1 提案システムの全体構成

3. 提案システム

3.1 全体システム構成

提案システムの全体構成を図 1 に示す．図 1 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．

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のちの実際のサービスな

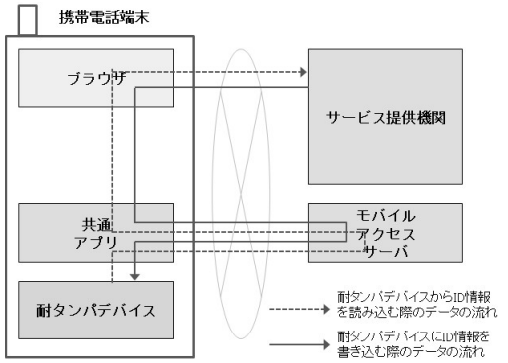

図 2 データの流れを示す簡略図

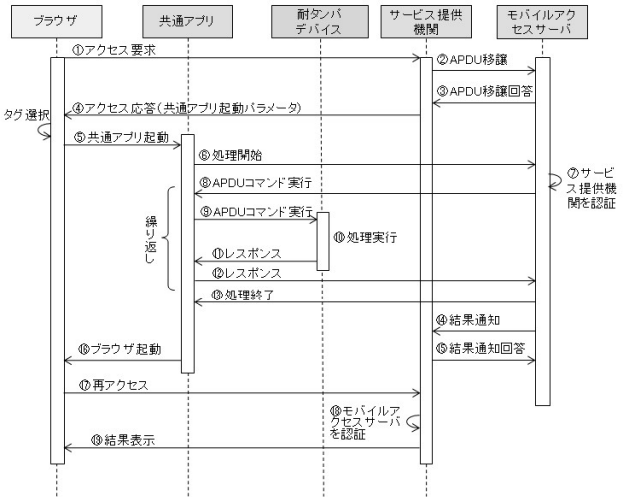

図 3 データの流れを示す詳細図

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．

3.2 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 2 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 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 3 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 ．

共通アプリは，モバイルアクセスサーバに処理開始要求をを送信する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，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，処理を実行し⑩ ，結果を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．

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 ．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 ．

4. 実証実験システム

4.1 全体システム構成図

図 4 に実証実験システムの全体システム構成図を示す．図 4 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，文献 [2] 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，会員情報を登録して会員 ID を耐タンパデバイスに対して発行する会員登録サイト，会員 ID 情報を耐タンパデバイスから読み込んで確認し，検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耐タンパデバイスに付与する健康ポータルサイト，耐タンパデバイスからポイント情報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，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，ID 情報を格納するカードアプリと，ポイント情報を格納するカードアプリを構築した．

4.2 実証実験システムの機器構成

図 5 に実証実験環境の全体構成を示す．図 5 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

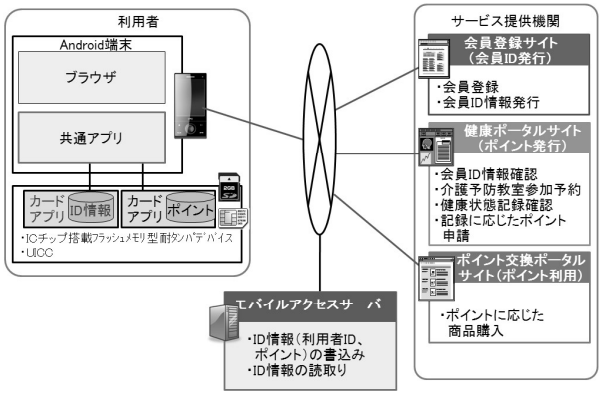

図 4 実証実験システム全体構成

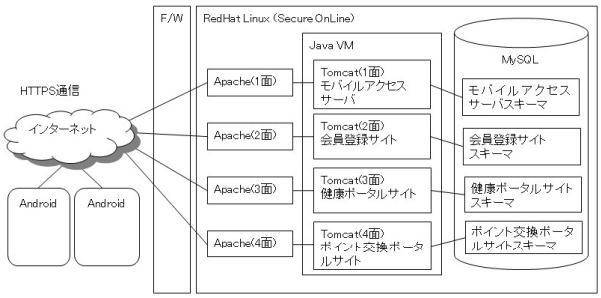

図 5 実証実験環境

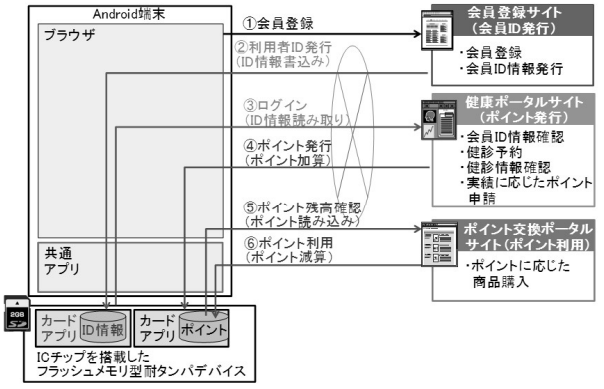

図 6 実証実験システムの仮想サービスフロー

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．

4.3 実証実験システムの全体サービスフロー

図 6 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．

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．会員情報を入力した後，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 ID 情報が，ID 情報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 ID 情報管理カードアプリから ID 情報を読み出し，ID 情報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．

図 7 会員登録サイトへの会員登録の手順

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⑤．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⑥．

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，参考文献 [2] で検討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．

4.4 実証実験の方法

4.4.1 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 7 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 情報を書き込む．
(4) 登録完了画面が表示される．

4.4.2 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 8 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 情報を読み込に会員の確認を行う．
(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．

図 8 健康ポータルサイトでのポイント発行の手順

(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．

4.4.3 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 9 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) ポイント利用完了画面を表示する．

図 9 ポイント交換ポータルサイトでのポイント利用の手順

表 1 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

表 2 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 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

5. 実証実験による性能評価

5.1 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 1 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．

また，表 2 および表 3 に性能測定に用いた携帯端末の機器仕様を示す．

5.2 性能測定結果

実証実験で行った仮想サービスの内，ID 情報の書き込

表 4　性能測定項目

No.	性能計測項目	詳細説明 (図 3 との対応)
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→② ③ APDU 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	携帯電話端末ー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
3	携帯電話端末内の処理	⑨ APDU コマンド実行→⑩ 処理実行→⑪ レスポンス＋その他内部処理
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，⑭ ⑮ 結果連携 (サーバ通信含む＋その他内部処理
5	携帯電話端末ーサービス提供機関間の通信＋携帯電話端末内の処理	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

表 5　ID 情報書き込処理の性能測定結果

No.	端末 1 (ms)	端末 2 (ms)	備考
1	91	103	
2	3751	2951	8 往復の通信
3	1193	1234	5 回の APDU 送信
4	343	217	3 往復の通信
5	1291	792	
全体	6669	5296	

表 6　ポイント情報書込み処理の性能測定結果

No.	端末 1 (ms)	端末 2 (ms)	備考
1	126	63	
2	3760	3526	9 往復の通信
3	1173	1424	6 回の APDU 送信
4	317	216	4 往復の通信
5	908	833	
全体	6283	6063	

み処理とポイント情報の書き込み処理の性能を測定した．性能測定を行った項目を表 4 に示す．また，携帯電話端末は，表 2 および表 2 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 5 および表 6 に示す．なお，表 5 および表 6 に示した測定値は，5 回計測した平均値を示している．また，表 5 および表 6 の No. は，表 4 に示した項番に対応する．

5.3　性能測定結果に対する考察

表 5 および表 6 に示したように，耐タンパデバイスに対する ID 情報の書込みおよびポイント情報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 ID 情報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約 500ms 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．

6.　まとめ

本研究では，文献 [2] 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性能評価を行った．その結果，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，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．

今後は，具体的なサービスに適用し，運用も含めたシステム全体の評価を行う必要がある．

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．

参考文献

[1] GlobalPlatform Card Specification Version 2.1.1 March 2003. http://www.globalplatform.org
[2] 梅澤克之，森田 伸義，礒川 弘実，萱島 信, “モバイルアクセス基盤の検討,” 情報処理学会コンピュータセキュリティ研究会 (CSEC) 予稿集, May. 2012.(予定)