M-058

セキュアモバイルアクセス基盤の提案
A Proposal of a Secure Mobile Access Platform

梅澤 克之† Katsuyuki Umezawa
礒川 弘実† Hiromi Isokawa
本澤 純† Atsushi Honzawa
川連 嘉晃† Yoshiaki Kawatsura
堀 健太郎† Kentaro Hori
南 幸雄† Sachio Minami
砂田 一茂‡ Kazushige Sunada
手塚 悟†† Satoru Tezuka

1． まえがき

携帯電話を用いたサービスに関して，クラウドコンピューティング時代の到来を考えると，近い将来全ての情報は仮想的な個人用サーバ（以降モバイルフォルダと呼ぶ）に蓄積し，携帯電話通信事業者（以降モバイルキャリアと呼ぶ）に依存しない形でサービス事業者と連携可能であることが望まれる．しかし，現在の携帯電話には，安全に個人毎の情報を格納するアーキテクチャが実現されておらず，また，セキュアにリモート環境からアクセスするための共通的な基盤が存在しない．また，入場チケット，身分証明書等の個人情報を共通的かつ統一的なインタフェースで携帯電話にダウンロードする環境が存在しない．本研究では，セキュアな個人情報の格納技術，セキュアな個人認証，アクセス技術等を実現する，モバイルキャリアに共通な基盤としてのセキュアモバイルアクセス基盤を提案する．さらに，提案に基づいて，システムを開発し機能評価を行う．

図 1 にセキュアモバイルアクセス基盤を用いたサービス例を示す．また，セキュアモバイルアクセス基盤のコンセプトを以下に示す．

【サービス提供者に対するコンセプト】

- 実世界の郵便局会社における私書箱へ郵便物を届けるように，個人に対する電子的な権利を配信する．
- その際に，ユーザがどのモバイルキャリアの携帯電話を持っていても，モバイルキャリアの違いを意識する必要なく，権利の配信が可能となる．
- モバイルアクセス基盤側の仕組みを意識することなく，配信された権利が，サービス提供者に戻ってくることを確認することによって，サービスを提供する．
- ユーザが利用するモバイルキャリアの違いを意識することなく，サービス提供だけに注力できる．

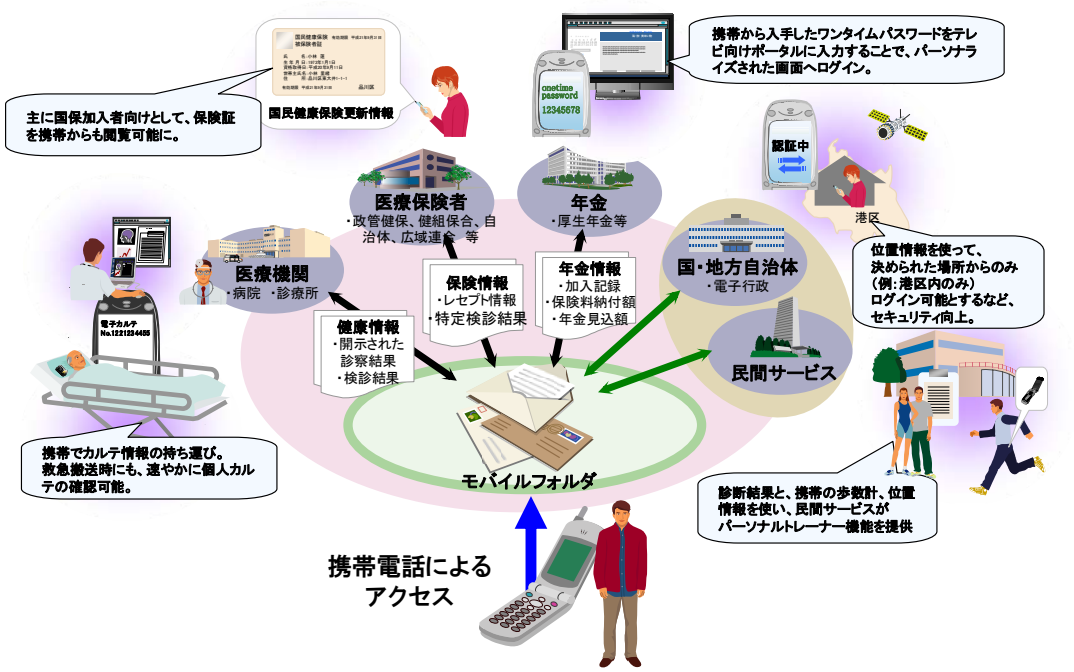

図 1　セキュアモバイルアクセス基盤を用いたサービス例

†（株）日立製作所, Hitachi, Ltd.
‡（株）インデックス沖縄, Index Okinawa Corporation.
†† 東京工科大学, Tokyo University of Technology.

【ユーザに対するコンセプト】

- 自分自身がどのモバイルキャリアの携帯電話を使っていても，共通的なアクセス方法で，自身のモバイルフォルダにアクセスできる．
- 自身宛てに配信された権利を利用したい際に，その権利をダウンロードでき，その権利を利用する際には，かざすという直感的な利用方法で簡便に利用することができる．

我々は，文献[1]～[4]において，ユーザが利用するモバイルキャリアの違いを意識する必要のない認証方式を提案してきた．本研究は，アクセス方式にとどまらず権利情報の配信，携帯電話へのダウンロード，展示会などの現地でのローカル環境での利用まで含めた基盤技術の提案を行う．

2. モバイルアクセス基盤の提案

2.1 モバイルアクセス基盤の要件

本節では，前節で述べたモバイルアクセス基盤を，サービス事業に適用する際の要件を示す．

- サービス事業者へのサービスの登録申し込みの際に，サービス提供者がモバイルフォルダと連携し，モバイルフォルダへチケット等の権利情報を配信できなければならない．
- その際に，モバイルフォルダにユーザ登録がなされていない場合は，モバイルフォルダに対するユーザ登録も合わせて行うことができなければならない．
- サービス利用者は各種モバイルキャリアの携帯電話を所有していることが想定されるため，少なくとも複数モバイルキャリアの携帯電話に対応しなければならない．
- 携帯電話にダウンロードされたチケットは，どのような内容のチケットなのかをユーザが確認できなければならない．
- 読取装置は複数設置されることが想定されるので，どの読取装置で読み取ったチケット情報なのかをサービス提供者が判断できなければならない．
- 携帯電話の中に複数種類のチケットをダウンロードできなければならない．
- 読取装置は，自身で読み取りたいチケット情報を，携帯電話に対して指定できなければならない．
- 配信されたチケットは，どのサービス提供者によって配信されたチケットなのかを，読取装置は認識できなければならない．

2.2 モバイルアクセス基盤の基本構造，基本仕様

モバイルフォルダへの安全なアクセスを実現するためには，アクセス者本人の正しい認証が必要である．モバイル PKI 技術をベースとし，国内モバイルキャリアの現行商用機，試作機を含め，将来出荷が予定される携帯電話での認証方式を整理し，さまざまな，タイプの携帯電話からのセキュアなアクセスを可能とし，コンテンツをダウンロードできるようにする基盤を定義する．

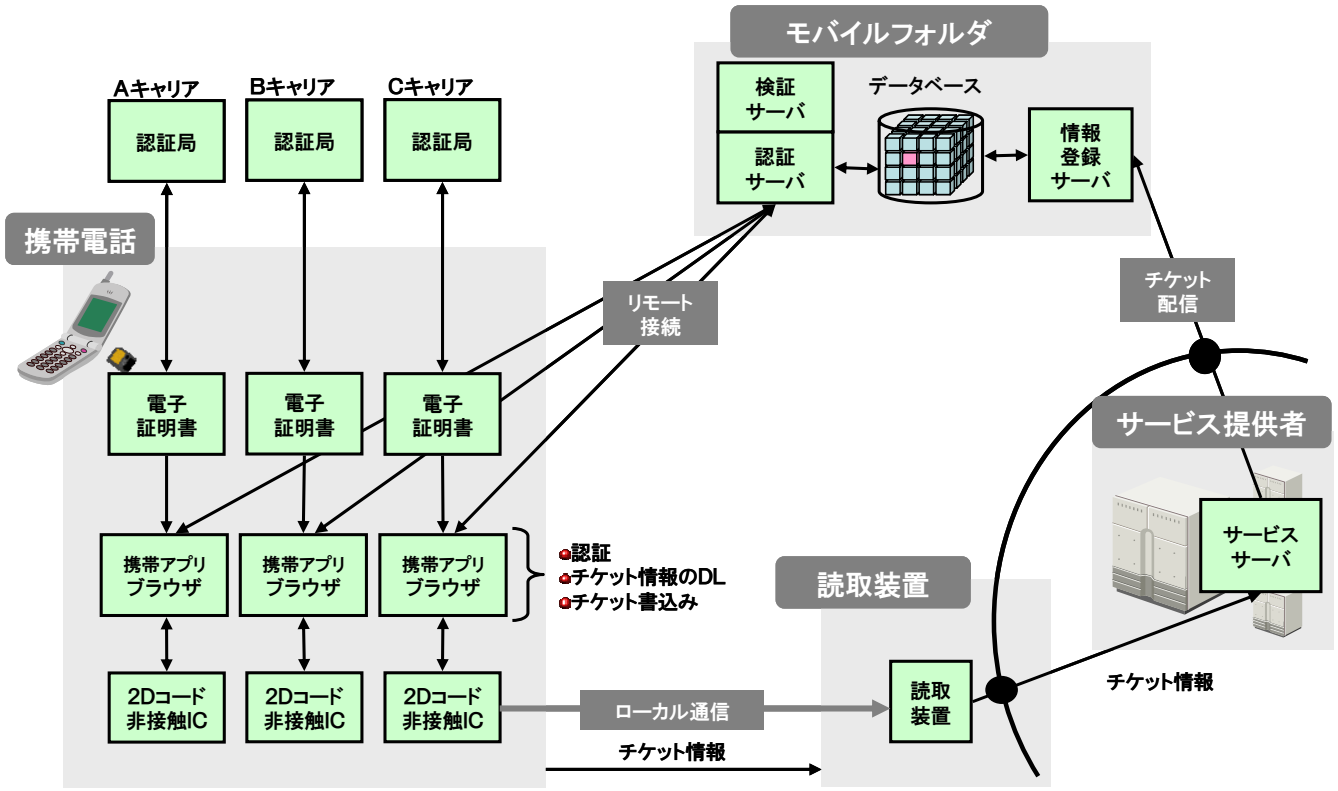

図 2　モバイルアクセス基盤の基本構造

図 2 にモバイルアクセス基盤の基本構造を示す．モバイルアクセス基盤は，図に示したように，ユーザのデータを管理・蓄積するモバイルフォルダ，ユーザが所有する携帯電話，展示会の入場ゲートやセミナ会場入り口に設置しユーザの携帯電話からチケット情報などを読み取る読取装置，ユーザへのチケット配信やチケット読み取り後の実際のサービスの提供を行うサービス提供者の 4 つのエンティティから構成する．なお，携帯電話での認証方式を整理すると，商用サービスで PKI 機能を提供しているモバイルキャリアと提供していないモバイルキャリアが存在する．提供しているモバイルキャリアに関しては商用 PKI 機能を利用し，提供していないモバイルキャリアに関しては，仮想的な認証局を構築し同等の PKI 機能を実装することとする．

以降の節では，モバイルフォルダ，携帯電話，読取装置，サービス提供者の各エンティティ間のインタフェースおよび，各エンティティの機能について記述する．

2.3 モバイルアクセス基盤のインタフェース

本節では，モバイルフォルダ，携帯電話，読取装置，サービス提供者の各エンティティ間のインタフェースについて記述する．

① サービス提供者－モバイルフォルダ間インタフェース

- モバイルフォルダ確認 IF：参加希望者が申し込み依頼を行った際に，対象ユーザのモバイルフォルダが存在をチェックする．通信形式は HTTPS 等の安全な通信方式とする．
- チケット情報送付 IF：モバイルフォルダにチケット詳細情報を送付する．通信形式は HTTPS 等の安全な通信方式とする．

②サービス提供者－読取装置間インタフェース

- 読取装置 ID 認証 IF：読取装置に設定された読取装置 ID を認証する．通信形式は HTTPS 等の安全な通信方式とする．
- サービスリクエスト IF：読取装置にて読み取ったチケット ID を送受信する．通信形式は HTTPS 等の安全な通信方式とする．

③携帯電話－モバイルフォルダ間インタフェース

- モバイルフォルダへのアクセス IF：ユーザが携帯電話を使ってモバイルフォルダにアクセスする．通信形式は HTTPS 等の安全な通信方式とする．

④ 携帯電話－読取装置間インタフェース

- 権利情報（チケット情報）の提示 IF：モバイルフォルダからダウンロードした権利情報（チケット情報）を入場ゲート等で提示する．通信形式は 2D バーコードや非接触 IC 通信などのローカル通信とする．

2.3 モバイルアクセス基盤の機能

本節では，モバイルフォルダ，携帯電話，読取装置，サービス提供者の各エンティティの機能について記述する．

① モバイルフォルダの機能

【ユーザ向け機能】

- ユーザ認証機能
  モバイルフォルダにアクセスしてきた携帯電話を認証する．
- 会員初期登録機能
  モバイルフォルダにユーザ登録されていない場合に新規アカウントを登録する．
- 会員再登録機能（PKI 証明書登録機能）
  携帯電話からアクセスし，モバイルフォルダのアカウントと携帯電話の PKI 証明書を紐づける．
- 登録情報変更機能
  登録情報を変更する．
- チケットダウンロード機能
  携帯電話からの要求に基づき，チケットをダウンロードする．

【サービス提供者向け機能】

- 会員登録存在チェック機能
  サービス提供者にアクセスしてきたユーザ（携帯電話）が，既にモバイルフォルダに既にアカウントを持っているか否かを確認する．
- オブジェクト（チケット）登録機能
  サービス提供者が発行したオブジェクト（チケット）をモバイルフォルダに登録する．

②. 携帯電話の機能

- モバイルフォルダアクセス機能
  モバイルフォルダへセキュアにアクセスする．
- チケットダウンロード機能
  モバイルフォルダのチケットのうち 1 枚を選択し，携帯電話へダウンロードする．
- チケット利用機能
  ダウンロードしたチケットを読取措置にかざして利用する．

③サービス提供者の機能

- アカウント存在確認要求機能
  モバイルフォルダに既にユーザのアカウントが存在するか否かを確認する．
- チケット発券機能
  モバイルフォルダの特定ユーザのアカウントに対して，チケットを発行する．
- チケット判定機能
  読取装置から送信されたチケット情報の正当性を確認し，結果を読取装置に送信する．

- ユーザ認証機能
  サービス提供者にアクセスするユーザを認証する．

④ 読取装置の機能

- 認証要求機能
  読取装置に設定された ID を基に，サービス提供者に認証処理を要求する．
- チケット読み取り機能
  2 次元コードあるいは非接触通信より，チケットを読み取り，サービス提供者に判定処理を要求する．
- 判定結果出力機能
  サービス提供者の判定処理結果に従い，ログ出力，画面表示，音声の再生を行う．

3．提案システムの構築

前章までは，提案するセキュアモバイルアクセス基盤の基本構造，基本インタフェース，基本機能について述べた．本章では，提案方式に基づいて開発したシステムについて詳述する．

3.1 開発コンポーネント

先に定義した要件を実証する試作システムを構築し，有用性を実証する．図 3 に開発したコンポーネントを示す．

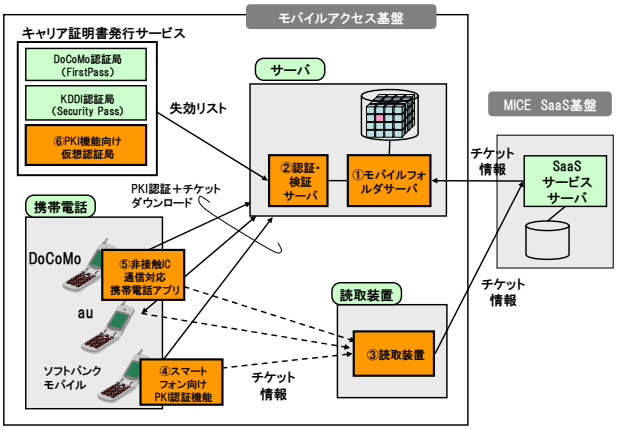

図 3　開発コンポーネント

具体的には以下のコンポーネントの試作を行った．

①モバイルフォルダサーバ
　モバイルフォルダは，サービス提供者およびユーザの携帯電話の 2 つのエンティティに対して，機能を提供する．モバイルフォルダの概要を図 4.5 に示す．

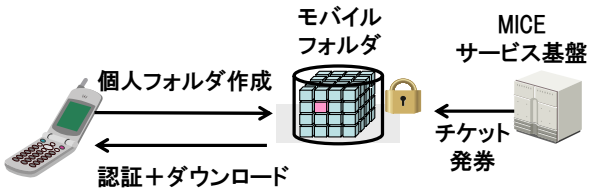

図 4　モバイルフォルダの概要

　モバイルフォルダは，ユーザ（携帯電話）に対して，会員初期登録機能，再登録機能（PKI 証明書登録機能），登録情報変更機能，チケットダウンロード機能を提供する．また，サービス提供者に対して，会員登録存在チェック機能，オブジェクト（今回はチケットに限定）の登録機能を提供する．個人毎に格納する情報は，携帯メールアドレス，チケットデータ（チケット ID とチケット Description と有効期限），携帯電話 PKI 証明書との紐付け情報，機種変更用 ID，PW 情報とする．なお，モバイルフォルダは，個人毎の情報を格納することを主な機能とし，サービス提供者のサービス内容に依存するビジネスロジックはもたない．

②認証・検証サーバ
　認証・検証サーバは，携帯電話からのモバイルフォルダへのアクセスに対して，各モバイルキャリア所定の認証機能（SSL 認証/CRL 検証）を提供することにより，安全かつモバイルキャリアに依らない統一的なアクセス手段を実現する．また，CRL ファイル自動/手動取得機能および環境設定機能を提供する．下図に認証・検証サーバの概要を示す．

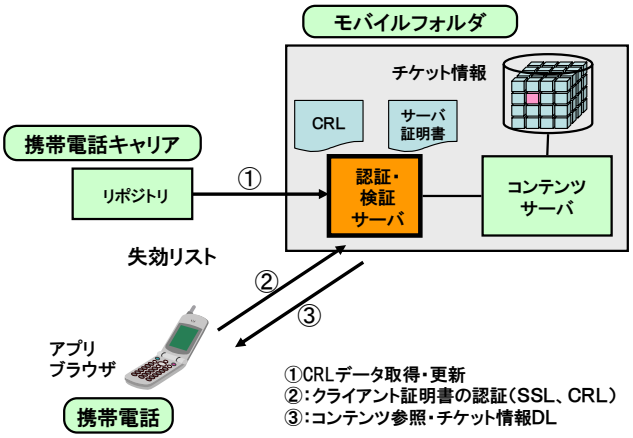

図 5　認証・検証サーバの概要

③読取装置
　ユーザの携帯端末の FeliCa や 2 次元コードをリーダライタ端末で読み取ることにより情報を取得し，その情報をサービス事業者側サーバへ送信することを主な目的とする．また，サービス事業者側サーバから受信した応答伝文を解析し，画面表示を行う．

④スマートフォン向け PKI 認証機能
　携帯電話からモバイルフォルダへの PKI ベースでアクセ

ス制御を実現するために，モバイルセキュリティカードを用いた PKI 機能を実装する．具体的には，スマートフォン端末向けの PKI 機能を有するプログラム（Crypto Provider for Embedded）を実装した．本プログラムは，CSP（Cryptographic Service Provider）関数の API を持ち，上位アプリケーションが本プログラムの API に連携した CryptoAPI の関数を呼び出すことによって PKI の処理を実現する機能を提供する．

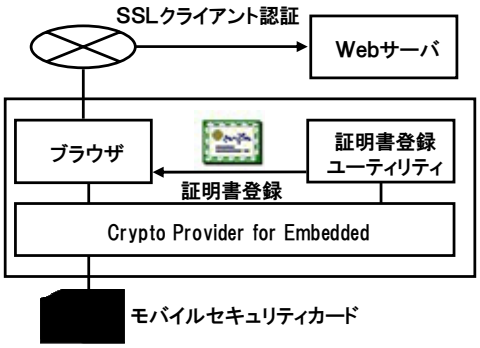

図 6 スマートフォン向け PKI 認証機能概要図

⑤非接触 IC 通信対応携帯電話アプリケーション

モバイルフォルダへの認証・アクセス制御，チケット情報等のダウンロード，携帯電話への格納処理を行う携帯電話アプリケーションを開発する．なお，2 次元コード方式に関しては，ブラウザベースで行うため個別のアプリケーション開発は行わないこととした．

本アプリケーションはサーバから取得したイベント・セミナ情報を携帯電話内の IC チップ領域およびスクラッチパッドに保存し，本アプリケーションを起動することにより，取得した情報を表示する．

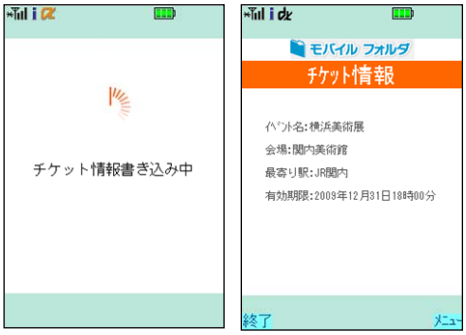

図 7 携帯電話アプリケーション画面イメージ

⑥仮想認証局

④の PKI 機能を実現するための電子証明書を発行する仮想認証局を立ち上げた．

3.2 サブシステム間インタフェース

本節では，モバイルフォルダ，携帯電話，読取装置，サービス提供者の各エンティティ間のインタフェースについて記述する．

①サービス提供者－モバイルフォルダ間インタフェース

モバイルフォルダ確認 IF を通じて，参加希望者が申し込み依頼を行った際に，対象ユーザのモバイルフォルダが存在をチェックする．通信形式は HTTPS とした．また，チケット情報送付 IF を通じて，モバイルフォルダにチケット詳細情報を送付する．通信形式は HTTPS とした．

②サービス提供者－読取装置間インタフェース

読取装置 ID 認証 IF を通じて，読取装置に設定された読取装置 ID を認証する．通信形式は HTTPS とした． サービスリクエスト IF を通じて，読取装置にて読み取ったチケット ID を送受信する．通信形式は HTTPS とした．

③携帯電話－モバイルフォルダ間インタフェース

モバイルフォルダへのアクセス IF を通じて，ユーザが携帯電話を使ってモバイルフォルダにアクセスする．通信形式は HTTPS とした．基本的には上記の HTTPS 方式による Web アクセスによって実現する．NTT ドコモ携帯電話端末で実現する場合には，携帯電話内アプリケーションとの連携が必要である．

④携帯電話－読取装置間インタフェース

権利情報（チケット情報）の提示 IF を通じて，モバイルフォルダからダウンロードした権利情報（チケット情報）を入場ゲート等で提示する．通信形式は 2 次元コードおよび非接触 IC 通信とした．

3.3 チケット ID

本節では，チケット ID の構造および変換について示す．

① チケット ID の全体構造

チケット ID 情報は，16 バイトの長さとする．1 バイト目，2～5 バイト目，6～16 バイト目にそれぞれ意味を持たせる．全体構造を下図に示す．

図 8 チケット ID の全体構造

② チケット ID の 1 バイト目

チケット ID の 1 バイト目は，チケット ID のバージョン（1 ビット目～3 ビット目），サービス提供者のクラス（4 ビット目～5 ビット目），チェックサムの種別（6 ビット目～8 ビット目）で構成する．

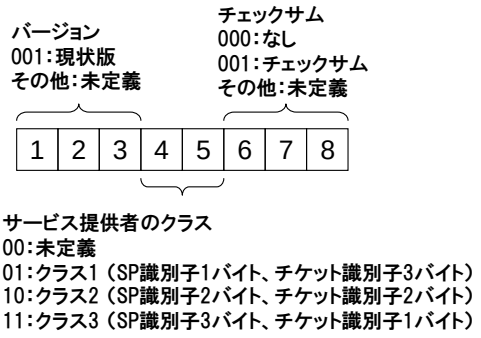

図 9　チケット ID の 1 バイト目の構造

③　チケットの 2～5 バイト目

チケット ID の 2～5 バイト目は，SP 識別子とチケット識別子を表す．2～5 バイト目の構造は，サービス提供者のクラス（1 バイト目の 4～5 ビット目）によって，下図に示すように，3 種類の構造をとる．

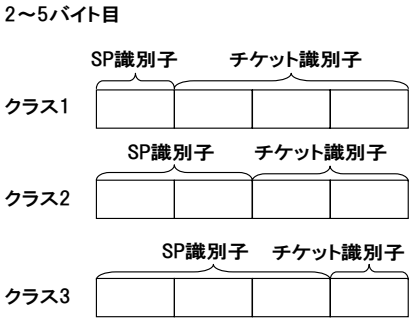

図 10　チケット ID の 2～5 バイト目の構造

④　チケットの 6～16 バイト目

チケット ID の 6 バイト目以降がチケット情報を表す．チェックサムの種別（チケット ID の 1 バイト目の 6 ビット目～8 ビット目）が 000 のときは，16 バイト目までの 11 バイトがチケット情報となる．チェックサムの種別が 001 のときは，15 バイト目までの 10 バイトがチケット情報となり，16 バイト目はチェックサムとなる．チェックサムは，6 バイト目から 16 バイト目までをバイト単位で加算した結果の下位 1 バイトとする．また，強度の高い誤り検出符号が今後定義された場合には，その定義にしたがって最終バイトから何バイトがチェック用に使われるかが決定されることとする．

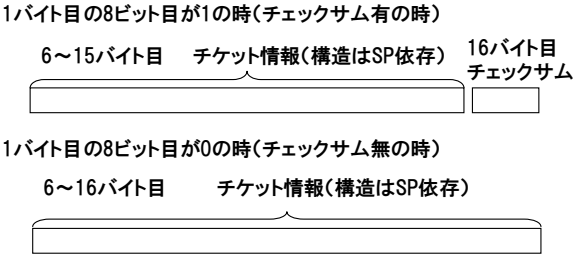

図 11　チケット ID の 6～16 バイト目の構造

⑤　チケット ID の変換について

（1）Base64 エンコード

Base64 とは，バイナリーデータを文字列データにエンコード（置換）する方式の一つである．Base64 では，24 ビットを 1 つの集まりとして扱う．この集まりを 6 ビットごとに 4 つに分けて，それらを決められた変換規則によって，4 個の ASCII に変換する．従って，元サイズの 3 分の 4 倍（約 1.3 倍）のサイズになる．チケット ID は 16 バイトのため，Base64 エンコード後のサイズは 24 バイトになる．

（2）変換の必要性

チケット ID は 2 次元コードへの変換や SPーモバイルフォルダ間にて XML を使用してデータの受け渡しを行うため文字コードが必須となる．先頭 1 バイトについてはバイナリ形式であるがデータパターンにあてはめると必ず文字コードとなるため問題ないが，最終 1 バイトのチェックサムについては文字コードが保証されないため，Base64 にて文字コードへの変換が必要である．

4．機能評価

本章では，前節で開発したシステムの機能評価を行う．一般ユーザに提案システムのサービスを利用してもらうことにより，構築したモバイルアクセス基盤の各機能が正しく動作することを確認した．具体的には下表に示す機能が正しく動作することを確認した（実証実験の詳細およびユーザの利便性の評価に関しては文献[5]を参照）．

表 1　提案システムの評価内容と確認内容

項番	評価内容	確認内容
1	会場入場	会場入場が完了することを確認
2	会場入場(二重入場)	会場入場でワーニングが発生することを確認
3	イベントアンケートメール受信	イベントアンケートメールの受信が完了することを確認
4	イベントアンケート回答	イベントアンケートの回答が完了することを確認
5	セミナ入場	セミナ入場が完了することを確認
6	セミナ入場（二重入場）	セミナ入場でワーニングが発生することを確認
7	セミナアンケートメール受信	セミナアンケートメールの受信が完了することを確認
8	セミナアンケート回答	セミナアンケートの回答が完了することを確認
9	ブース資料請求	ブース資料請求が完了することを確認
10	ブース資料請求(二重請求)	ブース資料請求でワーニングが発生することを確認
11	抽選	抽選が完了することを確認
12	抽選(二重抽選)	抽選でワーニングが発生することを確認

会場入場から，セミナ会場や展示会場，抽選会場に至るまで，実フィールドにおける評価を実施した結果，構築したモバイルアクセス基盤の各機能が問題なく正しく動作し，入場完了，入場後のアンケートメール送信，資料請求を実現可能とすることが確認できた．

6．まとめと今後の課題

本研究では，サービス提供者が，入場チケット，身分証明書等の個人情報をユーザが利用する携帯電話に違いに依らず安全に配信し，格納する技術，携帯電話ユーザの統一的な認証およびアクセス技術，ダウロードされたチケットの統一的な利用技術を提案した．提案に基づき，モバイルキャリアに依らない共通な基盤としてのセキュアモバイルアクセス基盤を構築し，機能評価を行った．今後は，様々な実事業への適用を推進する．

謝辞

本研究は，総務省『ICT 経済・地域活性化基盤確立事業(「ユビキタス特区」事業)』における「コンベンションビジネス向けモバイルサービスの実証」プロジェクトの成果の一部である．

商標等に関する表示

参考文献

[1] 梅澤克之，笈川光浩，洲崎誠一，手塚悟，平澤茂一，“モバイル向け証明書検証システムの開発，” 情報処理学会論文誌，Vol.48，no.2，pp.625-634，Feb. 2007.

[2] 梅澤克之，笈川光浩，洲崎誠一，手塚悟，平澤茂一，“モバイル環境での証明書検証方式の評価，” 電子情報通信学会論文誌(D)，vol.J90-D，no.2，pp.384-398，Feb. 2007.

[3] 梅澤克之，坂崎尚生，佐藤一夫，松木彰，曽我健二，片山透，清本晋作，田中俊昭，平澤茂一，“モバイルサービス向け認証基盤の検討，” 電子情報通信学会論文誌(D)(研究速報)，vol.J90-D，no.2，pp.596-599，Feb. 2007.

[4] 梅澤克之，手塚悟，佐藤一夫，松木彰，曽我健二，片山透，清本晋作，田中俊昭，“モバイルサービス向け認証基盤の開発，”電子情報通信学会論文誌(D) Vol.J91-D，no.3，pp.744-756，Mar. 2008.

[5] 礒川弘実，梅澤克之，本澤純，川連嘉晃，堀健太郎，南 幸雄，砂田一茂，手塚悟，“セキュアモバイルアクセス基盤の MICE 事業への適用と評価，”第 9 回情報科学技術フォーラム(FIT2010)予稿集，Sep. 2010