スマートフォンに顔画像と二次元コードを表示する個人認証方式と評価

金 宰郁 [1)], 立野 貴之 [1),] 舘 秀典 [2)]

1）松蔭大学 観光メディア文化学部

2) 東京福祉大学 社会福祉学部

jaewook@shoin-u.ac.jp

概要

個人認証データ及び二次元コードをスマートフォンの画面に表示して、ID カードに代替して使用できる個人認証方式を提案した。提案方式は、通常の ID カードに比べて、紛失の危険性の最小化、個人認証の精度、確認時間、操作性、及び安全性で優れている。検査者端末がサーバとオフラインの状態でも、ユーザのスマートフォンと検査者端末だけで、個人認証を行える。提案方式を、出席確認、建造物立入り管理、出勤管理、及び投票所入場券などのアプリケーションに拡張できることを示し、既存のアプリケーションである電子チケット等との技術的相違を明確化した。プロトタイプとして、スマートフォン、検査者端末、及び Web サーバを用いる電子学生証システムを試作して評価を行い、有効性を確認した。

1 はじめに

個人認証は様々な情報システムにおいて重要である。携帯電話を個人認証に用いることに関しては、パスワードの安全性向上、並びに、ID カードの機能向上の意味がある。プラスチックカード、磁気カード、及び IC カードが、ID（個人識別）カードとして多く使用されているが、紛失、盗難、及び偽造の危険が大きい。携帯電話を ID カード代わりの個人認証に用いる場合には、携帯電話の画面上に個人認証データをすべて表示することができ、紛失等の危険も少なくなる。提案方式は、スマートフォンを用いる一般的な個人認証として拡張できることを、身分証明証、出勤管理・研究室出席確認の個人認証、企業等の建造物に入る時の個人認証、国や自治体の選挙における投票所入場券の個人認証などのモデルについて考察することによって示す。この提案方式の実現性を確認するためのプロトタイプとして電子学生証システムを試作し、評価することによって、有効性を確認する。

2 過去の知見

過去の研究（金宰郁、ほか 2002）によれば、携帯電話における個人認証データ（顔画像、個人文字データ）及び個人認証データを含む二次元コードをスマートフォンの画面に表示することによって、ID カードのような個人認証を行う方式が提案され、有効性、セキュリティ、及び応用方法を示されている[1]-[4]。スマートフォンに二次元コードを表示する応用は、自動販売機の商品購入のための電子マネー、航空機などの電子チケット、商店の電子クーポン、などに利用されている[5]、[6]。しかし、内部処理やセキュリティについての方式と評価、及び実装内容を詳細に報告している公開文献は、著者が調べた範囲では存在しない。スマートフォンに顔画像、個人文字データ、及び二次元コードを適用して、ID カードに代わる個人認証に有効利用することを詳細に報告している文献は存在しない。

3 提案方式の応用モデルと考察

3.1 提案方式の特徴

提案方式を身分証明証に利用する場合の特長を、以下に示す。

①スマートフォンは、電話及びメール等の使用頻度が多いので、通常の ID カードよりも紛失する危険が少ない。ユーザは、個人認証データを、サーバから、任意の時点でダウンロードできる。

②スマートフォンに表示される顔画像は、通常の ID カードに印刷される顔写真サイズに比べて十分に大きいので、検査担当者がスマートフォンの顔画像と実際の生の顔を比べるときの正確性が向上する。正面顔画像だけでなく、横顔も表示できるので、検査者が目視チェックするときの精度を向上できる。

③個人認証データを直接に二次元コードスキャナで読取って、端末に入力できるので、自動的に処理できる。

④スマートフォンによる個人認証機能に二次元コ

ードを追加することによって、個人認証データの偽造が困難になり、更には個人認証データの内容をチェックする時間を短縮できる。

ID 方式の比較を、表１に示す。これによって、提案方式が優れていることが分かる。

表１　ID 方式の比較

方式 / 項目	一般の ID カードによる ID 方式	スマートフォンの顔画像と個人文字データだけによる ID システム	提案方式
紛失の危険性の極少化	C	B	B
個人認証の精度	C	B	A
確認時間の極小化	B	B	A
操作性	C	B	A
安全性	C	B	A

［備考］：A：優れている、B：良い、C：劣る

3.2 応用モデル

提案方式は身分証明のための ID カードの代替と機能向上以外にも、色々なアプリケーションに拡張できる。以下にそのモデル例を述べる。

(1) 授業の出席確認、研究室出席確認

サーバは、授業の受講者に出席チェック用の二次元コードを送信する。受講者は、受講時にスマートフォンに表示される二次元コードを、検査者端末に接続された二次元コードスキャナに提示する。検査者端末は、二次元コードをデコードし、正当性チェックを行って、出席状況をデータベースで管理する。必要に応じて、顔画像のチェックも行う。同様な方法で、大学の研究室への卒業研究学生の出席確認を行える。

(2) 建造物の立入り管理

重要な施設のあるビルや工場等への立入りに際しては、入口で建物検査者に社員証の提示を求められることが行われているが、この方法では、社員証の写真が小さいので、個人認証が不十分である。社員証の代わりに、スマートフォン画面を提示し、二次元コードを検査担当者が読取ることによって、個人認証チェックを、高精度に行うことができ、且つ、建造物への立入り者をサーバで管理できる。

(3) 企業における出勤管理

サーバは、定期的に社員に出勤チェック用の二次元コードを文字情報と共に送信する。社員は、出勤時にスマートフォンに表示される二次元コードを、出勤チェック用端末に接続された二次元コードスキャナに提示する。出勤チェック用端末は二次元コードをデコードし、正当性チェックを行って、サーバに送信する。サーバでは、出勤状況をデータベースで管理する。

(4) 国や自治体の選挙時の投票所入場券

現在の国や自治体の選挙では、投票所入場券が有権者に郵送される。有権者は、投票所入場券を持って指定された投票所に行き、生年月日を尋ねられて、回答できたら投票所における個人認証が終了する。この方法の問題点は、①有権者数が膨大なために、投票所入場券を印刷・郵送するためのコスト（印刷費＋郵送費）が膨大であり、更には、②投票日よりも数週間前に投票所入場券が郵送されるために紛失しやすいということがある。提案の個人認証方式に基づく改善方法を以下に示す。

【スマートフォンを用いる改善方法】: 選挙の有権者は、事前に選挙管理委員会に電子メールアドレスを届け出ておく。選挙管理サーバは、投票所入場券の情報（ユーザ名、住所、投票場所）の文字データと地図、及び認証データを含む二次元コードをユーザのスマートフォンに送信する。有権者は、そのスマートフォンを投票所の受付に提示する。受付では、二次元コードを読取って、投票所入場券の正当性をチェックし、サーバからダウンロードして端末に表示した個人認証情報（生年月日（年齢）、性別）との一致性および有権者の風貌によって個人認証する。この場合、顔写真の確認は現在の選挙時には行われていないので、オプションの機能になる。

3.3 応用モデルの考察

表２に、スマートフォンと二次元コードを利用する応用モデルによる技術の相違を示す。

電子メール配送を主とする場合でも、ユーザが電子メールを紛失又は消去した場合には、サーバからの二次元コード等の入手も必要である。電子チケットや電子マネーは、実用化されていても、詳細情報が公開されていない場合が多いので、次のような方法を仮定する。電子チケットでは、チケット情報を二次元コードに書込み、

表 2　携帯電話機と二次元コードを利用する応用モデルによる技術の相違

比較事項 / 応用モデル		顔の画像	サーバからスマートフォンへの配送		サーバと検査者端末の通信		個人認証情報の安全性
			電子メール	Web ブラウザ	オンライン	オフライン	
新規提案	身分証明証（ID）	○	○	○	○	△	○
	出席確認	△	○	△	○	△	△
	建造物の立入り管理	○	×	○	○	△	○
	投票所入場券	△	○	○	△	○	○
従来	電子チケット	×	△	○	○	×	○
	電子クーポン	×	△	○	○	×	○
	電子マネー	×	×	○	○	×	○

[備考]　○：必須　　△：必要な場合もある　×：不要

その二次元コードをスマートフォンに表示し、二次元コードスキャナで読取ったデータについて、サーバで処理を行う。電子クーポンも電子チケットと同様である。電子マネーでは、個人識別情報と使用可能金額などを二次元コードに書込み、二次元コードをスマートフォンに表示し、二次元コードスキャナで読取ったデータをサーバに送信し、サーバに登録されている決済方法で使用金額の決済を行う。

4 プロトタイプの開発

4.1 スマートフォンによる個人情報の表示

提案方式の実現性と有効性を検証するために、スマートフォンと二次元コードを用いる電子学生証システムをプロトタイプとして開発した。

図 1 に、ユーザのスマートフォンのディスプレイ表示例を示す。

図 1　スマートフォンによる個人情報の表示例

検査者はサーバに学生証データを入力する。サーバは学生証データから二次元コードを作成する。サーバは、Web ソフト及びスクリプトで実現する。二次元コードスキャナは、パソコンに接続する USB インターフェース及び二次元コードのデコーダを実装している市販品であり、検査担当者が手に持って撮像するハンドヘルド型と、机上等に置く据置型を比較評価する。このプロトタイプを授業の出席確認に応用する場合には、学生証データと二次元コードは、電子メールとして、サーバで設定した時刻に受講者のスマートフォンにサーバから送信される。授業開始時に、受講者はスマートフォンに表示される二次元コードのデータを二次元コードスキャナに提示する。出席者の氏名等は二次元コードに含まれた学生証データによって、確認できる。そのとき、氏名及び学籍番号が出席者名簿ファイルに記録され、検査担当者の端末（ノートパソコン等のコンピュータ）に表示される。

スマートフォンの画面は、顔画像、個人文字基本情報、及び二次元コードを表示する。顔画像は、一般の学生証では正面画像だけであるが、スマートフォンの電子学生証では、正面画像に加えて、横顔も表示できる。二次元コードは、学生証データの一部分を含んでいる。二次元コード機能の使用によって、学生証データを素早く二次元コードスキャナによって読取ることが可能であり、学生証データの安全性も向上できる。

4.2 検査者端末の表示

図 2　オンライン個人認証における検査者端末の表示例

査者の端末は、二次元コードスキャナから、二次元コード内容がデコードされたテキストデータを受取り、個人認証詳細データを表示する。図 2 にオフライン個人認証における検査者端末の表示例を示す。

4.3 オンライン個人認証とオフライン個人認証

オンライン個人認証では、検査者端末に十分に大きなカラーの顔画像を表示できる。個人ごとに画像サイズが若干異なっている。その原画像サイズの平均は、360,054 バイトであり、通常圧縮顔画像サイズの平均は、4,493 バイトである。

オフライン個人認証で使用する極小圧縮顔画像は、圧縮し過ぎると、検査担当者が、本人を高精度に判定できなくなる。圧縮の度合いと目視による識別の度合いの関係を調べるために、色々な圧縮率の顔画像を、被験者に見せて、判定可否を記述する実験を行った。被験者は 14 人である。

識別度は、被験者が、顔画像を見たときにどの程度まで個人認証可能であるかの度合いを表す数値であり、識別不可が 0、識別困難が 10～40、概ね識別可能が 50、識別可能が 60～90、完全に識別可能が 100 としている。図 3 に、極小圧縮顔画像の相対圧縮率（＝（1－（極小圧縮顔画像サイズ／通常圧縮顔画像サイズ））×100　（%））の平均値と、顔画像の識別可能性の度合いである識別度の平均値の関係を示す。図３から、圧縮率が約 80%以下であれば識別可能である。実験に使用したスマートフォンでは、極小圧縮顔画像サイズが 1、760 バイト以下であればスマートフォンに二次元コードを最大表示可能であり、且つ、検査者が本人を極小圧縮顔画像によって識別可能である。

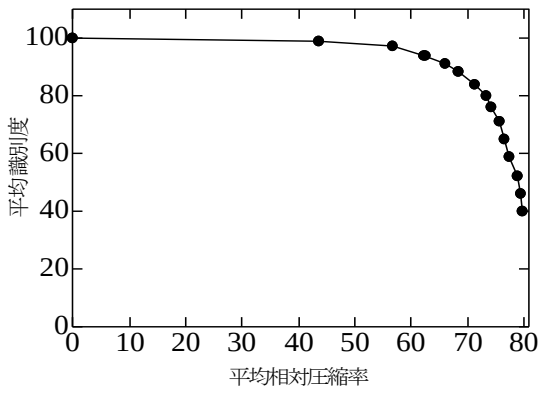

図 3　極小圧縮顔画像の平均圧縮率と被験者による平均識別度の関係

5 まとめと今後の課題

個人認証データ及び二次元コードをスマートフォンの画面に表示して、ID カードに代替して使用できる個人認証方式を提案した。提案方式は、通常の ID カードに比べて、紛失の危険性の最小化、個人認証の精度、確認時間、操作性、及び安全性で優れている。検査者端末がサーバとオフラインの状態でも、ユーザのスマートフォンと検査者端末だけで、個人認証を行える。提案方式を、出席確認、建造物立入り管理、出勤管理、及び投票所入場券などのアプリケーションに拡張できることを示し、既存のアプリケーションである電子チケット等との技術的相違を明確化した。プロトタイプとして、スマートフォン、検査者端末、及び Web サーバを用いる電子学生証システムを試作して評価を行い、有効性を確認した。残された課題には、次世代スマートフォン能の有効利用などがある。

参考文献

[1] J. Kim and T. Kobayashi: A Method for Securing a Web Sever and Its Application to an ID Card, Proceedings of the First International Conference on Information Technology & Applications, Paper No. 227-21, pp. 1-5, IEEE, Australia, Nov. (2002).

[2] T. Kobayashi and J. Kim: Improving the Web Application Security using a Face Image with Watermarking, Proceedings of the Sixth LASTED International Conference on Internet and Multimedia Systems and Applications (IMSA2002), pp.108-112, USA, Aug. (2002).

[3] T. Kobayashi and J. Kim: Security considerations on Two-dimensional Symbols, Proceedings of the First International Conference on Information Technology & Applications, Paper No. 223-21, pp. 1-4, IEEE, Australia, Nov. (2002).

[4] J. Kim and T. Kobayashi: An Electronic ID System using a Cell phone, Proceedings of the Second LASTED International Conference on Communications, Internet and Information Technology (CIIT2003), USA, IASTED, ACTA press, pp.259-263 (2003).

[5] モバイルバーコードの新しい可能性，Mobile RF magazine, Vol. 87, pp.18-25, シーメディア，東京，(2003).

[6] モバイル・インターネット徹底解剖，日経 BP 社，pp.164-232 (2002).