6ZE-06

大規模災害時における個人認証手法についての検討

周　爽[†]　　高井　峰生[††, †††]　　大和田泰伯[††††]　　小口　正人[†]

†お茶の水女子大学　††大阪大学　†††UCLA　††††情報通信研究機構

1. はじめに

近年，日本各地で地震や台風などの災害が連続して発生している．災害発生時に長時間の停電による被害や暴風による屋根の被害により，自宅で生活できない人や避難指示が発せられた人は避難所に行かなければならない．避難者が安全に生活できるためには，水，食料，家族や友人の安否確認などの情報共有を行うシステムの利用が必要である．しかし，システム利用時に，偽者としてシステムに登録したり，アクセスしたりすることが可能であると，個人情報の漏えいや改ざんなどが起こり，大きな問題になる．加えて，災害時，身分証明書を避難所に持って来ないこともあるため，身分証明書のみに基づく個人認証では，本人確認ができなくなる．その人たちのためにも，本人確認の手法を考えなければならない．

そこで本研究では，本人確認ができるものを持つ状況により，システムへの登録時とシステム利用時の個人認証についての仕組みを検討した．

2. 研究背景

人が主体となる認証は，知識，所有物，生体情報の三つの手段がある．

(1)　知識情報による認証とは，パスワード，秘密の質問など，本人のみが知っている秘密の知識情報によって本人確認をすることであり，特別な装置が必要とされないため，認証の基本方法として広く使用されている．しかしながら，パスワードが漏れてしまう可能性が高いため，複雑なパスワードを設置することや定期的に変更することが求められる．その結果，ユーザに対して利便性は低くなる．

(2) 所持情報による認証とは，身分証明書，ワンタイムパスワードなど本人しか持ち得ない情報が記録された媒体によって本人確認をすることである．

(3) バイオメトリクス情報による認証とは，指紋，顔，筆跡，静脈パターン，虹彩など本人の身体，行動が持つ固有情報によって本人確認をすることである．

個人認証への関心度が高くなると共に，多要素認証（MFA：Multi-Factor Authentication）がよく使われるようになった．また，近年ではスマートフォンの普及に伴い，多要素認証の一つとして，リスクベース認証，ライフスタイル認証など行動情報を活用した認証手段が提案された．

但し，大規模災害時における個人認証についての研究が少ない．筆跡，静脈パターンなどによる認証は生体情報を読み取るための特別な装置が必要であるため，災害時の避難所での利用は難しい．リスクベース認証では，災害時の状況を考えると，避難所に携帯電話やスマートフォンなどを持ってこない場合は付加的な認識の手間がかかってしまう．また，子どもやお年寄りなどは携帯電話やスマートフォンを持っていない場合もある．ライススタイル認証は事前に一定期間のデータを収集しなければならない．災害時の混乱状態では，避難者の移動軌跡が普段通りではない可能性が高い．

3. 個人認証についての提案

ユーザはシステムに基本情報を登録し，登録された情報によってシステムを利用できる．そのため，登録時に本人が正しい情報を登録することと利用時に本人であることを確認できる必要がある．また，災害時には，ユーザが必ずしも本人確認できるものをもっているとは限らず，そのユーザに対しては仮登録を行い，システムを利用できるようにする必要がある．

個人認証の仕組みについては登録時と利用時二つの場合に分けて検討する．まず図 1 に示すように，登録に関しては，顔付き身分証明書をもっているか否かによって2種類に分けられる．持っている場合は本人確認が完了している本登録に，持っていない場合は本人確認が完了していない仮登録になる．一方，ユーザがシステムを利用する時は，パスワードあるいは顔画像を入力することでログインできる．登録状態によりログイン状態も違う．

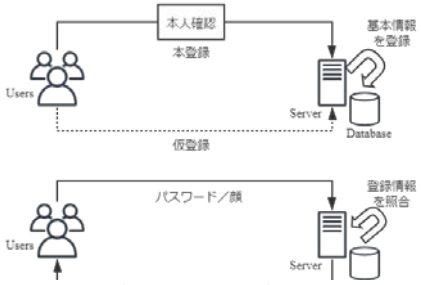

図 1　個人認証の全体の仕組み

3.1 本登録

本登録はユーザがシステムに登録する際に，要求された本人確認の手続きが完了した状態である．本登録のフローチャートを図 2 に示す．

マイナンバーカードによる本人確認を行う場合，JPKI（Japanese Public Key Infrastructure）で本人確認ができた後，パスワードを設定し，カードから読み取ったデータをシステムに登録する．他の顔付き身分証明書を持っている場合，ユーザが身分証明書を持って写真を撮影する．カードの基本情報（氏名，性別，生年月日，住所，顔画像の特徴量）と本人の顔画像の特徴量を抽出する．また，パスワードを設定し，基本情報をシステムに登録する．

顔付き身分証明書を持っていない場合，本人確認ができないため，仮登録を行う．

A Study of Personal Authentication Methods in A Large Scale Disaster

†Shuang ZHOU　Ochanomizu University

††, †††Mineo TAKAI　Osaka University, UCLA

†††† Yasunori OWADA　National Institute of Information and Communications Technology

†Masato OGUCHI Ochanomizu University

Copyright ©2021 Information Processing Society of Japan.
All Rights Reserved.

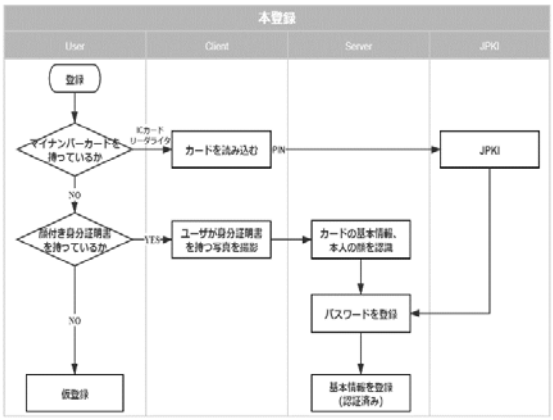

図 2　本登録のフローチャート

3.2 仮登録

仮登録は，ユーザがシステムに登録する際に，本登録で要求された本人確認がなされていない状態である．仮登録のフローチャートを図 3 に示す．

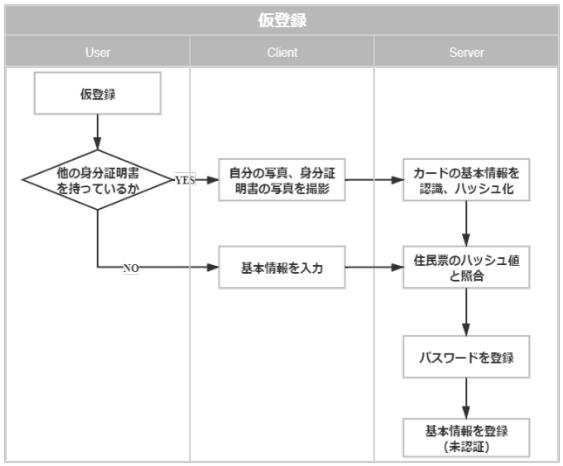

図 3　仮登録のフローチャート

他の身分証明書（顔が付かない身分証明書）を持っている場合，本人の顔写真と身分証明書の写真を撮影する．顔の特徴量を抽出し，身分証明書の基本情報を認識してハッシュ化する．他の身分証明書も持っていない場合は，ユーザが基本情報を入力してハッシュ化する．ハッシュ化したデータを自治体から取得した住民票の基本情報データのハッシュ値と照合し，一致する場合はパスワードを入力して基本情報をシステムに登録する．

3.3 利用時

利用時に，ユーザは端末デバイスによってパスワードと顔写真でどちらでもログインできる．フローチャートを図 4 に示す．

まずユーザがパスワードあるいは顔写真を入力してデータベースに登録したデータと照合する．ログインの際にはユーザの登録状態を確認し，仮登録あるいは本登録としてログインする．登録状態によってアクセス権を設定し，アクセス権に合ったページの表示やサービスの提供を行う．本登録のユーザはすべての機能が使えるが，仮登録のユーザは一部の機能が制限され，災害情報など公開情報を受信する機能だけを利用できる．

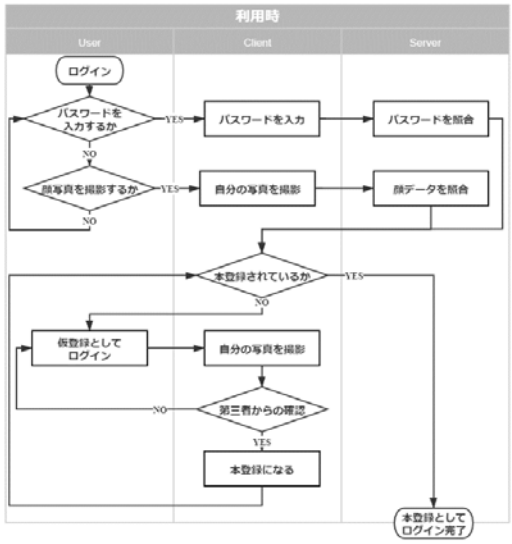

図 4　利用時のフローチャート

3.4 第三者からの本人確認

仮登録の状態において，友達として追加した第三者からの本人確認ができたら，登録の状態が本登録になる．第三者の登録状態や被認証者との関係により信頼度が異なる．認証者の信頼度の総和が友達の信頼度の総和の 70%以上の場合は本人確認が完了し，登録状態が本登録になる．第三者からの本人確認が行われていない場合は，そのまま仮登録の状態でシステムを使い続ける．

4.　まとめと今後の課題

本研究では，大規模災害時に個人の本人確認ができるものを持つ状況により異なるシステムへの登録時とシステム利用時の個人認証についての仕組みを検討した．また，本人確認が完了していない人はシステムのすべての機能を利用できない状況を避けるために，仮登録を行うことによって一部の機能を利用でき，第三者からの本人確認ができたら本登録の状態になる仕組みを提案した．

今後は提案した仕組みをウェブアプリケーションとして実装していく．ウェブアプリケーションは Web ブラウザが搭載されているデバイスからインターネット環境に接続するだけで，システムの利用が可能になる．災害時に時間の短縮化が可能となり，お年寄りでも簡単に利用できるのではないかと考えられる．第三者からの本人確認の仕組みについての信頼度に関する要素は登録状態と被認証者との関係であり，本人確認の完了標準は例えば 70%と考えられる．しかし，要素の妥当性や基準の合理性についての検討が必要である．最後に，全体的に個人認証についての仕組みを更に考えていく必要がある．

謝辞

本研究は一部， JST CREST JPMJCR1503 の支援を受けたものです．ここに感謝の意を表します．

参考文献

[1] 内閣府：防災情報のページ，“南海トラフの巨大地震被害想定（第一次報告および第二次報告概要）”，平成 25 年度．

[2] 内閣府：防災情報のページ，“ 防災白書”，令和 2 年．

Copyright ©2021 Information Processing Society of Japan.
All Rights Reserved.