「マルチメディア，分散，協調とモバイル
(DICOMO2021)シンポジウム」 令和3年6月-7月

大規模災害時の
情報共有のための個人認証についての一検討

周 爽[1] 高井 峰生[2,3] 大和田泰伯[4] 小口 正人[1]

概要：日本は，その位置，地形，地質など様々な条件から，地震，津波，台風，豪雨などの災害が頻繁に発生している．災害が発生する時に，避難勧告，避難指示が発せられた人，また家屋の倒壊，水や食料など物資の不足によって，自宅では生活できない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，災害，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．また，周囲に身元を証明してくれる人が誰もいない状況下での本人確認を考慮しておく必要がある．そのため，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．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が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が利用できるようにする仕組みを検討した．また，仮登録を行った人は第三者からの本人確認を行うことで，本登録になる仕組みを提案した．

A Study on Personal Authentication for Information Sharing in a Large-Scale Disaster

SHUANG ZHOU[1] MINEO TAKAI[2,3] YASUNORI OWADA[4] MASATO OGUCHI[1]

1. はじめに

日本は，その位置，地形，地質など様々な条件から，地震，津波，台風，豪雨などの災害が頻繁に発生している．また，南海トラフ巨大地震や首都直下地震などの大地震が予想されている．特に，南海トラフ巨大地震により，住宅全壊及び焼失棟数は約 95.4 万棟～約 238.2 万棟と想定されている[1].

災害が発生する前に，避難指示が発せられた人や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は避難所に行かなければならない．避難所とは災害の危険性がなくなるまで避難した住民等を一時的に滞在させる場所である．平成 26 年 10 月 1 日時点には 48,014 箇所であったが，令和元年 10 月 1 日時点には 78,234 箇所に増加した[2].

避難者が安全に生活できるためには，水，食料，避難所，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．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が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が利用できるようにする仕組みを検討した．また，仮登録を行った人は第三者からの本人確認を行うことで，本登録になる仕組みを提案した．

2. 研究背景

2.1 認証手段

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 お茶の水女子大学 〒112-8610 東京都文京区大塚 2-1-1
2 大阪大学 〒565-0871 大阪府吹田市山田丘 1-5
3 UCLA Electrical and Computer Engineering Department
420 Westwood Plaza, Los Angeles, CA 90095, USA
4 情報通信研究機構〒980-0812 宮城県仙台市青葉区片平 2-1-3

（1）知識（Something You Know）

知識情報による認証とは，パスワード，暗証番号，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（Something You Have）

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，USB トークン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．改ざんの可能性が低いが，携行しなければならないため，利便性が低い．

（3）バイオメトリクス（Something You are）

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．身体の一部を使い，忘れたり，紛失したりすることがない．また，複製できないため，なりすましが難しくなっている．しかし，生体情報を読み取る等の特別な装置が必要である．

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．多要素認証というのは，前述の三つの要素の内，複数の要素を組み合わせる認証手段である[3]．例として，ATM を利用する際には，自分のキャッシュカードとパスワードが必要となる．

また，近年ではスマートフォンの普及に伴い，多要素認証の一種として，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．

リスクベース認証では，アクセスしてきたユーザの端末やアクセス時間などの行動パターンや，IP アドレス，ブラウザなどの情報が普段と異なっていた場合，なりすましの可能性があると判断し，通常の認証に追加する形で，秘密問題など別の認証を実施する仕組みが使われている．正規のユーザがアクセスする際には，特別な操作が必要ではないため，ユーザの便利性が高いというメリットがある．

ライフスタイル認証[4]は，東京大学で研究開発が進められている技術であり，行動や買い物の履歴などユーザの生活習慣データを解析し，その情報に基づいて個人を認証する．ライフスタイル認証ではユーザに付加的な手間が必要ではないというメリットがある．

2.2 関連研究

Choudhury らはディープラーニングを用いた新しい個人認証手法を提案した．その手法は，指の爪板と指のナックルという 2 つの生体属性を融合させたものである[5]．Mohammed らはユーザのリスクレベルを判断し，適切な認証方法をユーザに求める認証システムを提案した．機械学習アルゴリズムを用いるリスクエンジンはユーザの IP アドレス，モバイル端末型番やログイン時間などデータを入力するデータとし，リスクレベルを判断する．このような適応型認証モデルは，ユーザに高いレベルのセキュリティを提供することができる[6]．鈴木らはライフスタイル認証の有効性を評価するため，スマートフォンやウェアラブル端末のセンサで収集される漫画閲覧履歴データ，電子チラシ履歴と活動量計データを収集した[7]．

インターネットやスマートフォンの普及に伴い，個人認証に関する研究が進んでいる．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．前述の参考文献[5]では，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．参考文献[6]の認証方法では，ユーザのモバイル端末型番が必要であるため，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．参考文献[7]の認証方法では，ライフスタイル認証はユーザに付加的な手間が必要ではないというメリットがあり，無人商店やアプリケーションへのログインなどの場合は適用されることが期待されている．しかし，ライフ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．

さらに大規模災害時には，避難者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，避難所の装置の状況は万全ではないということから，適切な個人認証の仕組みを考える必要があると考えられる．

3. 実験環境

3.1 Node.js

本研究では，Node.js を採用する．

Node.js[8]は Chrome V8 エンジンベースの JavaScript 実行環境である．Node.js は，PHP，Python，Perl，Ruby などのサーバサイド言語と同等のスクリプト言語として，JavaScript を動作させることができるサーバサイド開発プラットフォームである．2009 年 5 月に Ryan Dahl により開発された．

3.2 Express Platform

Express フレームワークは柔軟性が高い Node.js の Web アプリケーションフレームワークである．様々な Web アプリケーションの作成に役立つ強力な機能と豊富な HTTP ツールを提供している．Express を使えば，完全に機能的なウェブサイトを素早く構築することができる．また，Express フレームワークをベースにして，MVC（Model，View，Controller）アーキテクチャを構成できる．

モデル（Model）は，アプリケーションのデータロジックを処理するために，使用される．ビュー（View）とは，アプリケーションの中で，データの表示を処理するものであり，モデルデータを元に作成される．コントローラ（Controller）は，ユーザのインタラクションを処理するアプリケーションの部分である．ビューからデータを読み取ったり，ユーザの入力を制御したり，モデルにデータを送信したりする役割を担っている．

MVC の動作は図 1 に示す．

(1) ブラウザはユーザからのリクエストを受け，URL をルーティングに送る．
(2) ルーティングは，URL によって，どのコントローラを呼び出すかを判断する．
(3) 呼び出されたコントローラはモデルと打合せる．
(4) モデルはデータロジックを処理した結果をデータベースに反映する．
(5) モデルはデータベースからのデータを受け取る．
(6) 受け取ったデータをコントローラに渡す．
(7) コントローラは受け取ったデータをビューに引き渡す．
(8) ブラウザに Web ページが表示される．

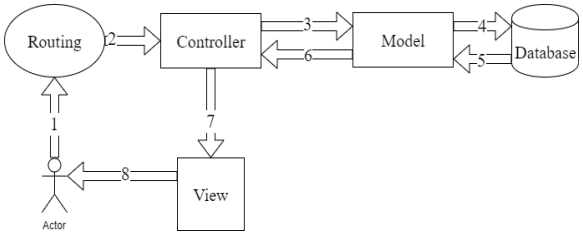

図 1　MVC

3.3 MongoDB

MongoDB は NoSQL のドキュメント指向データベースである[9]．これらのドキュメントは，JSON (JavaScript Object Notation) 形式で MongoDB に保存される．大量のデータを扱うシステムにおいて，リレーショナルデータベースに比べ，MongoDB は比較的簡単にスケールできるような仕組みを持っていることが特徴的である．

災害が発生し，アクセスが多い場合，MongoDB はデータの追加，更新，削除，クエリを高速に行うことで，効率的な対応ができる．

3.4 ウェブアプリケーション

ウェブアプリケーション（Web application）は，ウェブ（World Wide Web）技術を基盤としたアプリケーションソフトウェアである．ウェブアプリケーションは，複数の静的な Web リソースと動的な Web リソースから構成されている．ウェブアプリケーションはダウンロードしてインストールする必要がなくなり，ウェブブラウザ（Web browser）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を利用可能になる．

本研究の目的としては，災害の時に，時間がかからないのみならず，お年寄りでも簡単に使える必要がある．また，ウェブアプリケーションの論理的なトランザクションの大部分はサーバで実現されている．これにより，クライアントコンピュータやスマートフォンなどのマシンの負荷が軽減され，システムのメンテナンスやアップグレードの効率が向上される[10].

4. 個人認証についての提案

4.1 全体の仕組み

個人認証の仕組みについては登録時と利用時の二つの場合に分けて検討する．まず図 2 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．本人確認というのは，本人が自分の身分証明書を持っていることが認められることである．

ユーザがシステムを利用する時は，自分の手元のデバイスによって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．

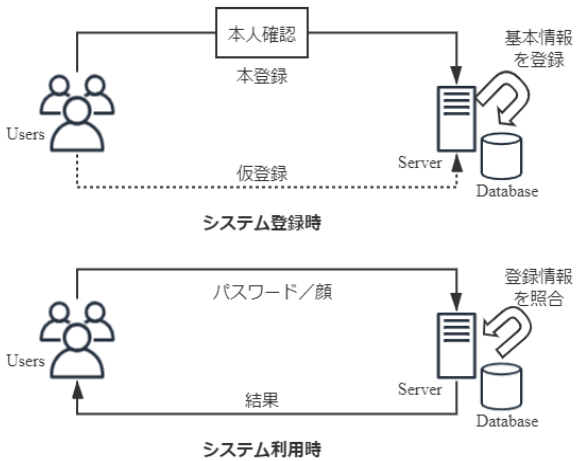

図 2　個人認証の全体の仕組み

システムを利用する前に，必要な登録情報は以下である．

- 氏名
- 性別
- 生年月日
- 住所
- パスワード
- 顔画像の特徴量

ユーザの登録状態は以下である．

- 本登録
- 仮登録

4.2 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 3 に示す．

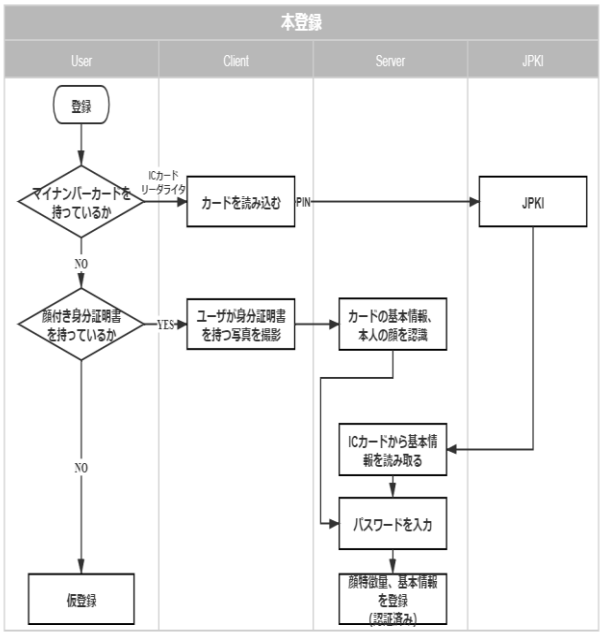

図 3　本登録のフローチャート

（1）マイナンバーカードによる本人確認を行う際に，カードリーダライタで読み込んで PIN を入力して JPKI（Japanese Public Key Infrastructure）に問い合わせる．JPKI は公的個人認証サービスである[11]．JPKI で本人確認ができた後，カードからデータ(氏名，生年月日，性別，住所，顔画像)読み取る．そして顔画像の特徴量を抽出する．パスワードを設置して顔特徴量と基本情報（氏名，生年月日，性別，住所）をシステムに登録する．

（2）　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．その写真からカードの基本情報（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（図 4）．本人の顔特徴量と身分証明書の顔写真の特徴量との類似度を計算する．類似度により，本人の身分証明書と認められる場合，パスワードを設定し，基本情報をシステムに登録する．

（3）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．

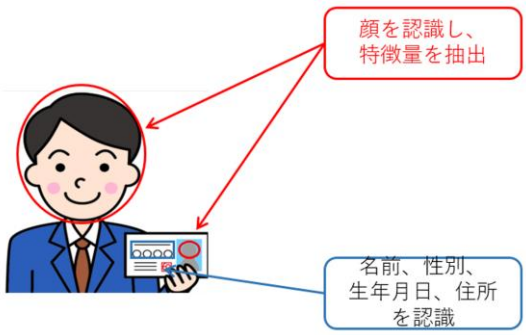

図 4　他の顔付き身分証明書の場合

4.3 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 5 に示す．

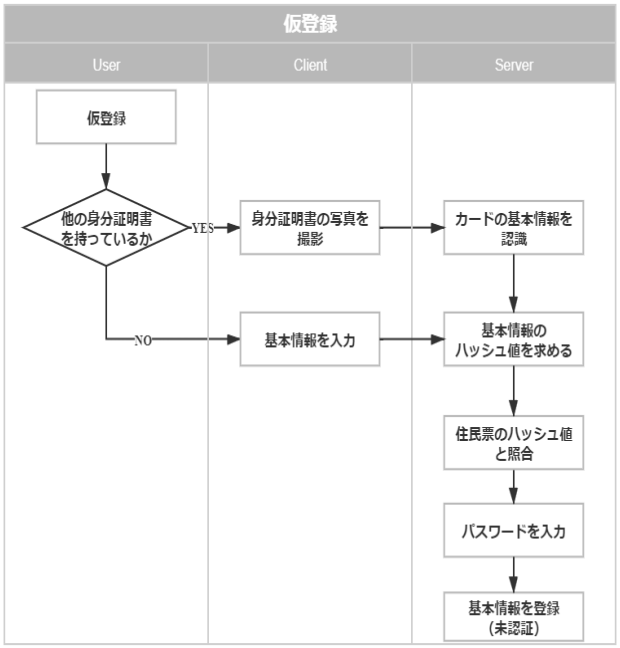

図 5　仮登録のフローチャート

（1）他の身分証明書（顔が付かない身分証明書）を持っているかを判断する．持っている場合は，身分証明

書の写真を撮影する．身分証明書の基本情報を認識する．また，ハッシュ値を求める．

(2) 他の身分証明書を持っていない場合は，ユーザが基本情報を入力する．また，基本情報のハッシュ値を求める．

(3) 基本情報のハッシュ値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．

仮登録の時，システムに登録した情報は以下である．

- 氏名
- 性別
- 生年月日
- 住所
- パスワード

4.4 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 6 に示す．

(1) 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．

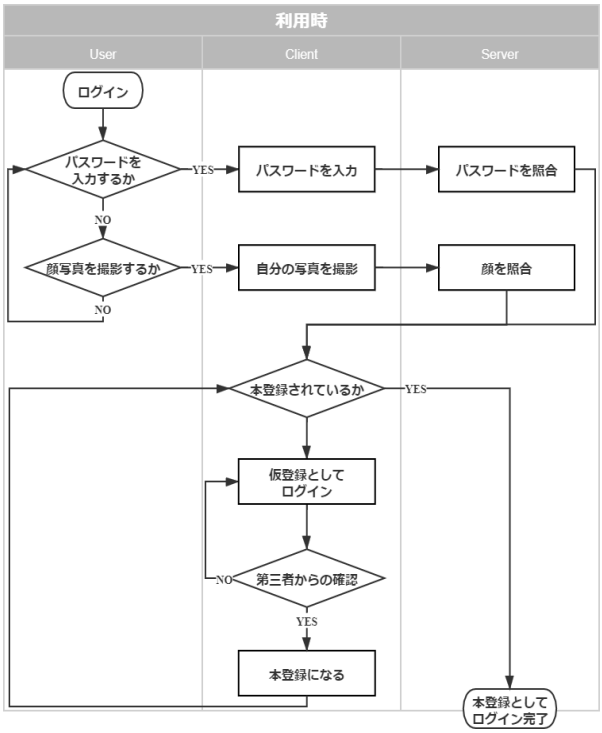

図 6 利用時のフローチャート

(2) 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．

登録状態と対応する機能は表 1 に示す．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．

表 1 登録状態と対応する機能範囲

登録状態	機能	情報
本登録	すべての機能	すべての情報
仮登録	一部の機能	公開情報

4.5 第三者からの本人確認

偽者としての不正行為を防ぐため，本人確認が必要である．但し，災害の時，身分証明書を避難所に持って来ないこともあるため，本人確認ができなくなる．そこでシステム登録時に本人確認が完了したユーザと本人確認が出来ていないユーザを分けることで，セキュリティを強化することができると考えられる．しかし，災害時に本人確認ができていないユーザが多い状況になると，システムの利用率が低くなる．そこで，本人確認が出来ていないユーザはすべての機能を利用できるために，第三者からの本人確認を行う仕組みを提案する．

第三者からの本人確認を行う前にまず友達になる必要がある．

図 7 に示すようにシステムにログインしているユーザが友達になる機能が利用できる．user0 は user1 と user 2 から友達になる申請リクエストを受け，拒否あるいは応諾をする．user0 と user 1 は家族や近隣の関係の場合，同じ避難所にいる可能性があるため，その際対面でのリクエストを受けることができ，なりすましの被害を受ける可能性が低いと考えられる．同じ避難所ではない場合，リクエストと共に送ったメッセージとその時に user2 が撮影した写真により，user2 が本人であるかを判断し，拒否あるいは応諾をする．二人しか知らない情報のようなプライバシー情報と自分と周囲の環境の写真を本人の判断要素として，非常時にある程度，本人確認ができると考えられる．

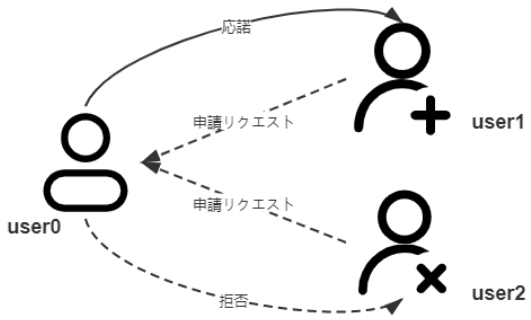

図 7 友達になるリクエスト

友達になったうえで本人確認を行う．また，本人確認を完了したユーザだけ他人の本人確認を行うことができる．三人以上の友達が本人だと認める場合，登録の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（図 8）．

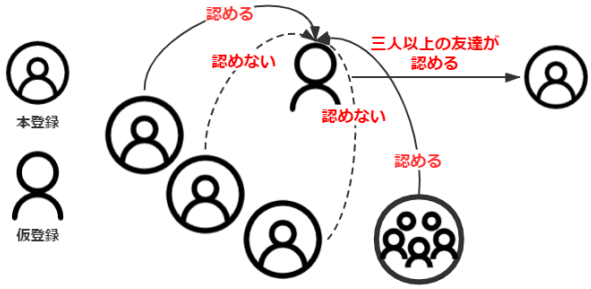

図 8 仮登録から本登録への移行

5. 実装

本システムの一部として第三者からの本人確認の仕組みを実装した．

図 9 に示すように，電話番号または名前によってユーザを検索できる．

図 9 ユーザを検索するページ

追加ボタンを押して友達申請ページが表示される（図 10, user2 が user0 に友達リクエストを送る）．

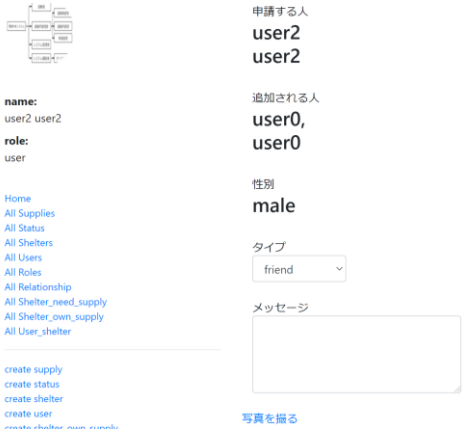

図 10 友達申請ページ

図 10 に示すページでメッセージと写真を入力することができる．写真を撮るボタンを押すとカメラを読み出して写真を撮影する（図 11，左側はカメラ画面，右側は撮った写真）．

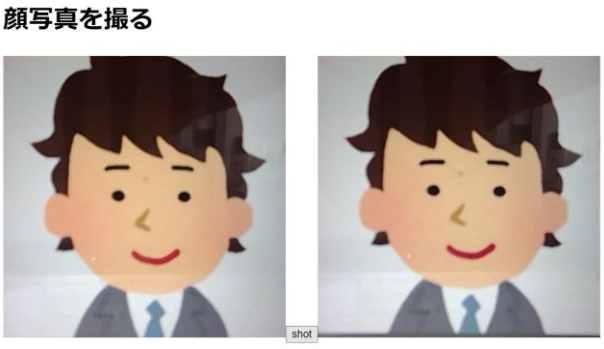

図 11 カメラを読み出して写真を撮影

user0 は友達追加リクエストを受け，メッセージと写真を確認して拒否あるいは応諾をする（図 12）．

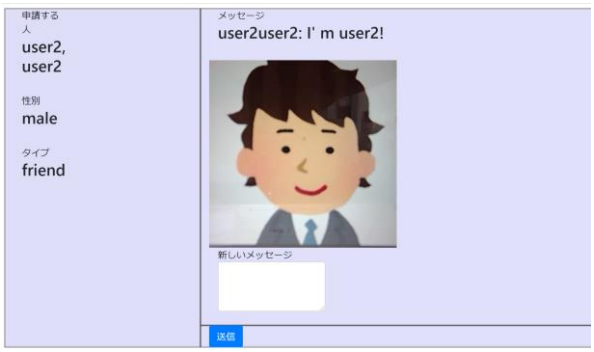

図 12 友達リクエストを確認

ユーザはシステム登録時に本人確認を完了しているか

どうかを判断する is_authenticated と本人確認をしてもらった人数 auth_number 属性がある．本人確認が完了した場合，is_authenticated は real_name_auth になる（図 13）．本人確認が完了していない場合は temp_auth になる（図 14）．

図 13　user0 属性値

図 14　user2 属性値

仮登録のユーザの auth_number は 3 になる時に is_authenticated は real_name_auth になる（図 15）．

図 15　user2 は本登録になる

6. 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，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．システムの一部として第三者からの本人確認の仕組みをウェブアプリケーションとして実装した．

今後は提案した仕組みを続けて実装していく．また，災害時の個人認証システムを提案したが，安全性や妥当性などまだ万全ではないため，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.
[3] 山口利恵，鈴木宏哉，小林良輔．認証精度の違う多要素・段階認証．コンピュータセキュリティシンポジウム 2015 論文集，2015(3)，795-802.
[4] 小林良輔，疋田敏朗，鈴木宏哉，山口利恵．行動センシングログを元にしたライフスタイル認証の提案．コンピュータセキュリティシンポジウム 2016 論文集，2016(2)，1284-1290.
[5] S. H. Choudhury，A. Kumar，S. H. Laskar．Biometric Authentication through Unification of Finger Dorsal Biometric Traits．Information Sciences，2019，497 : 202-218.
[6] M. Mohammed, B. S. Bindhumadhava, B. DHEEPTHA. Design of a risk based authentication system using machine learning techniques．In : 2017 IEEE SmartWorld，Ubiquitous Intelligence & Computing，Advanced & Trusted Computed，Scalable Computing & Communications，Cloud & Big Data Computing，Internet of People and Smart City Innovation(SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)．IEEE，2017，p.1-6.
[7] 鈴木宏哉，小林良輔，佐治信之，山口利恵．ライフスタイル認証実証実験レポート-MITHRA データセット．マルチメディア，分散協調とモバイルシンポジウム 2017 論文集, 2017, 223-230Lidan Mao．“Application of Browser/Server Architecture in College English Online Learning System Design”，Vol.13, No.03，p.129-140，2018
[8] Node.js 入手先 https://nodejs.org/zh-cn/
[9] Madison, Michael．“NoSQL Database Technologies”，No. 6150282，2015.
[10] Kyung-Hwan Ahn，Sung-Kwang Kim，Kwan-Pyo Hong and Ki-Jun Han．“Design and implementation of browser/server environment-based hospital information search system (BS-HISS)”， IEEE，Vol.2，p.1569-1572，1999
[11] 公的個人認証サービス（JPKI）総合ポータルサイト．https://www.kojinbango-card.go.jp/jpki/