生体情報と IC カード学生証を組み合わせた オンライン出欠確認の提案

阿部絢太[1]　古屋保[2]　下園幸一[2]　升屋正人[2]

概要：遠隔講義には，地理的，空間的，時間的制約からの解放という利点がある．しかし，対面講義よりもなりすましが容易であり，既存の出欠管理方法では不正を防止することは難しい．このため，なりすましをさせないオンライン出欠管理システムが求められている．そこで本研究では，学生本人が講義を受講しているかを正しく判定するために，顔や指紋などの生体情報と IC カード学生証の所持情報を組み合わせることで２要素により遠隔で出欠を確認する方法を提案する．

キーワード：教育支援，遠隔学習，組織活動を支える情報システム

Proposal for Online Attendance Confirmation Combining Biometric Data and Student ID Card

KENTA ABE[1]　TAMOTSU FURUYA[2]
KOICHI SHIMOZONO[2]　MASATO MASUYA[2]

Abstract: Remote learnings have the advantage of being free from geographical, spatial, and time constraints. However, it is easier to impersonate a lecturer than a face-to-face lecture, and it is difficult to prevent fraud with existing attendance management methods. Therefore, there is a need for an online attendance management system that does not allow spoofing. In this study, we propose a two-factor remote attendance verification method that combines biometric information (e.g., face and fingerprints) and the possession information of IC card student ID cards to correctly determine whether a student is attending a lecture or not.

Keywords: educational support, remote learning, information systems supporting organizational activities

1. はじめに

遠隔講義は地理的，空間的，時間的制約が小さいという利点があるため，新型コロナウィルスの影響が落ち着いた現在でも広く活用されている．しかし，遠隔講義は対面講義よりもなりすましが容易であり，出欠管理が難しい．例えば，Zoom など Web 会議サービスの参加履歴を出欠確認に用いる場合，端末とアカウントを複数用意すれば他人になりすまして講義に参加できてしまう．また，respon など学習管理システムと連携できるアンケート・出席管理サービスを用いる場合も，学習管理システムの ID・パスワードを共有することでなりすましができる．既存の出欠管理方法ではなりすましを防止することは難しい．

なりすましを防止するには，より信頼性や利便性の高いオンライン出欠確認システムが必要である．志田らは指紋認証を用いることで，オンライン試験のなりすまし不正を防止するシステムを構築した[1]．このシステムは，試験システムへのログイン時に USB 生体セキュリティキーを用いて指紋認証を行い，試験中はカメラとマイクの使用を許可した携帯端末上で Zoom を動作させて監視に利用，試験に用いる PC は試験システムとのみ接続させるというものである．あらかじめ用意した PC においては高い指紋認識率を示したが，個人所有の PC ではセキュリティキーの互換性に問題があり，認識率が低下するという問題があった．また，本人確認に Web 会議サービスのカメラ映像を用いる方法では，携帯端末の設置や設定に時間や労力がかかる．特に，セキュリティキーには費用がかかるため導入は難しい．

三谷らは IC カードリーダーと定点 Web カメラを接続した PC を用いて，IC カード学生証の情報を取得し，画像と組み合わせることで出席確認するシステムを構築した[2]．しかし，設置場所が固定されるこのシステムは遠隔授業への応用が難しい．

一方，新たな機器を導入することなく本人を確認できる方法に，eKYC 技術がある．eKYC（electronic Know Your Customer）とは，オンライン上での本人確認手続きであり，犯罪による収益の移転防止に関する法律施行規則[3]でもさまざまな方法が規定されている．スマートフォンで eKYC を実現するためのサービスの 1 つである Liquid eKYC は銀行・クレジットカード会社・携帯電話事業者など，さまざまな事業者のオンライン本人確認に用いられて

1 鹿児島大学大学院理工学研究科
Graduate School of Science and Engineering, Kagoshima University
2 鹿児島大学情報基盤統括センター
Center for Management of Information Technologies, Kagoshima University

いる．このサービスは，犯罪による収益の移転防止に関する法律施行規則第 6 条第 1 項第 1 号ホに基づき，まず運転免許証・マイナンバーカードなどの写真付き身分証を厚みその他の特徴とともにスマートフォンで撮影し，次に本人の容貌を撮影し，容貌の写真と身分証の本人写真の一致を確認することで本人確認が完了する．しかし，本人確認書類の写真を差し替えることでなりすましが可能であるという欠点がある．

そこで本研究では，新たなデバイスを必要とせず，なりすましによる不正を防止するための，遠隔から利用できる出欠確認の方法を提案することにした．用いるのは個人のスマートフォンである．提案システムはスマートフォンのアプリケーションとして開発する．まず，アプリケーションに IC カード学生証を登録し，アプリケーションの使用者が特定の学生であることを保証する．その上で，当該アプリケーションを使用するために，スマートフォンの生体情報による認証機能を必須として，本人であることを保証する．この 2 要素 2 段階の認証により，遠隔であるかどうかにかかわらず，アプリケーションの利用者が特定の学生であることが保証される．

2. 提案システムの実証

提案するシステムでは，IC カード学生証と関連付けられたスマートフォンのアプリケーションにより本人確認を行うことで出欠確認を行う．動作の流れを図 1 に示す．受講前の初期設定時に IC カード学生証をスマートフォンの NFC リーダーで読み込み，学籍番号と氏名を登録する．出席登録時にはアプリの起動時に顔または指紋を認証し，講義の識別コードを入力することで出席データが出欠管理側に送信される．関連付けの段階で学生証とスマートフォンの紐付けが行われ，スマートフォンの保持と学生証の保持が同義となる．スマートフォンを手もとから離すことは少ないため，関連付けは 1 回のみ行うことでよい．学生証紛失時には再登録を行う．関連付け後は，スマートフォンの顔認証機能や指紋認証機能を用いることで，指示した時点で学生証を紐付けた本人がスマートフォンを保持していることを確認できる．

この提案を実証するため，Android 上で動作するプロトタイプアプリケーションを開発した（図 2）．学生や講義の情報，出席データは全てアプリケーションに接続したクラウド上のデータベースである Firebase Realtime Database 上で管理する．

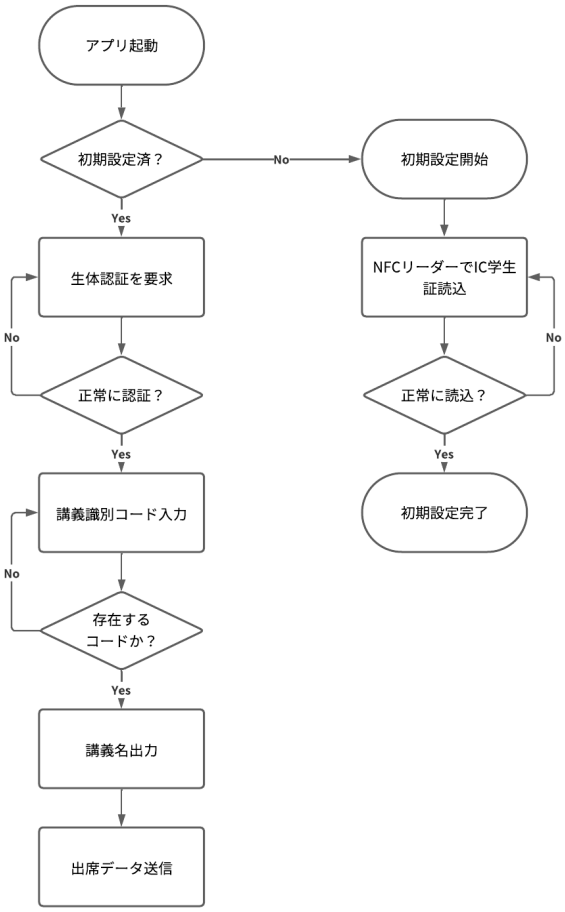

図 1　システム動作フロー

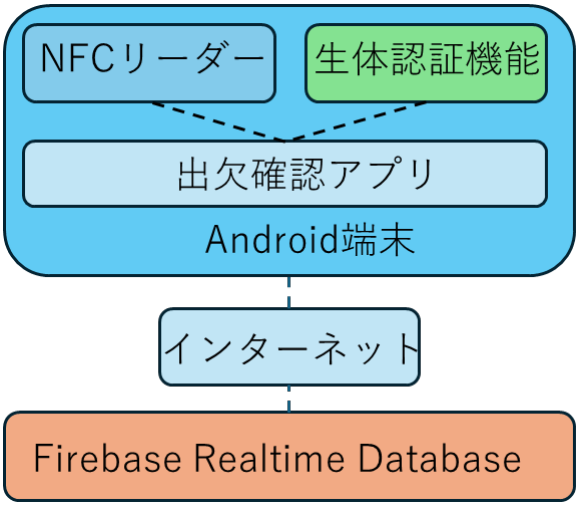

図 2　プロトタイプシステムの構成図

本システムで用いるスマートフォンには IC カード学生証を読み込むことができる NFC リーダーと顔または指紋認証機能が搭載されている必要がある．いずれも一般的なスマートフォンに搭載されているため追加の費用が必要となるケースは多くない．

2.1 受講前の初期設定

初期設定時に学生は IC カード学生証をスマートフォンの NFC リーダーで読み込み，内部に格納されている半角カ

ナ氏名・学籍番号をアプリケーションからデータベースに登録する（図 3）．このとき他人のスマートフォンと紐付けるのを防止するため，学籍番号 1 つにつき 1 台のスマートフォンのみ登録できるよう制限する．学生証を出席確認の度に認証することでより信頼性が高まるが，前述のようにスマートフォンを手放す機会は少ないことから，プロトタイプアプリケーションでは初回登録のみとした．

出欠管理側は受講前に学生がどの講義に出席したのかを識別するための識別コードを発行する．識別コードは前述の respon 等類似のシステムで用いられている 9 桁の数字など，任意の文字列を利用できる．識別コードと講義名は紐付けて，データベースに登録しておく．

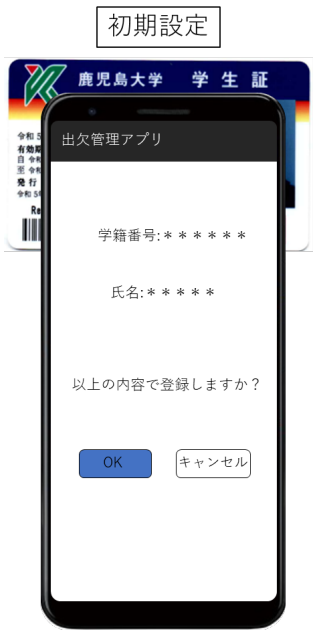

図 3　初期設定画面イメージ図

図 4　学生証読込のテスト

2.2　出席登録時

出席登録時に学生がアプリケーションを起動すると，生体認証を要求するダイアログが表示される（図 4）．顔または指紋認証でアプリケーションのロックを解除することで次に進むことができる．この段階で，学生本人が自身の IC 学生証データを登録した端末を所持し，出席の登録を試みていることを確認できる．最後に講義の識別コードを入力して出席データをデータベースに登録する．

出欠管理側はアプリケーションから送信されてきたデータを集計し，出席データとして保存する．

図 5　出席確認画面イメージ図

図 6　データベースサンプル

3.　まとめ

遠隔講義におけるなりすましを防止することを目的と

して,生体情報と IC カード学生証を組み合わせたシステムを提案し，プロトタイプアプリケーションを開発した．本システムはまず IC カード学生証の所持情報を端末の NFC リーダーで確認し，出席時には生体情報をスマートフォン標準搭載の顔または指紋認証機能で確認した後サーバに出席データを送信する．この 2 要素 2 段階の認証により，なりすましができない遠隔出欠確認が可能である．
今後，実際の講義で使用して有用性を確認するとともに，学生が多く利用している iPhone で動作するアプリケーションの開発を進めることにしている．

参考文献

［1］志田崇，栗田るみ子，杉本理，“JAMS（指紋認証システム）を利用したオンライン認証による不正防止可能性の検討”， The Josai Journal of Business Administration 17 (1), 39-54, 2021-09
［2］三谷素弘，堀幸雄，今井慈郎，“学生証 IC カードを用いた出席者情報取得・表示システム”，教育システム情報学会 2013 年度学生研究発表会
［3］e-Gov 法令検索．「犯罪による収益の移転防止に関する法律施行規則」第 6 条第 1 項第 1 号ホ．https://elaws.e-gov.go.jp/document?lawid=420M60000f5a001．2023/11/27