1D-03

FIDO2 サーバーによるなりすまし防止効果の研究 ー退学者防止効果の視点にて

杉本　理[†1]　　志田　崇[†2]　仰木裕嗣[†3]
城西大学[†1†2]　慶應義塾大学[†3]

1. 概要

オンライン授業やハイブリッド授業における受講者のなりすまし，すなわち代理出席は大人数授業であれば避けるすべがない．本研究では FIDO2 標準を使うことで生体情報による個人認証を行いながらかつ大学が生体情報を収集せず，サイバー攻撃に対しても耐性のある，安心安全な出席管理システムを提案する．また，なりすましを防止することが学生の出席を促し，退学者防止につながるという仮説をデータから実証を試みる．

2. はじめに

大学で使用するパスワードだけでなく，ネットショッピングや SNS など複数のアカウントに対するパスワードを管理しなければならない時代が来ている．IPA の調査では 2 つ～5 つのパスワードを管理するユーザーのうち，SNS 使用者の約 40%，金銭を伴うオンラインサービスの利用者の約 45%がパスワードを使いまわしていると答えている[1]．6 つ以上のパスワードを管理している場合はさらに使いまわす傾向が強い．また大学には特有の環境があり，友人間でアカウント情報を共有することで授業の代理出席を行うという目的にも起因する．慶應義塾大学の研究によれば，「友人の ID とパスワードを使ってログインした」と答えた学生のうち「問題がある」と回答した割合はパソコン利用の場合で 10 代が 55.8%，20 代が 45.0%，スマートフォン利用の場合は 10 代が 45.7%，20 代が 42.3%となっており，全体的に問題意識が低い[2]．この代理出席が勉学への意欲低下を招き，最終的に退学へつながってしまうという可能性がある．FIDO2 の最大の特徴でもある「なりすまし防止」が「代理出席防止」に直結することからこれらの取り組みによって大学が防止につなげたいと考えている．

3. 代理出席の実態

コロナ禍の状態が現在も続く中，各教育機関においてはリモートを活用した講義が進められている．そうした中，学生が友人になりすまして行う「代理出席」がある．

「なりすまし」実態の可能性確認ということで，講義における ICT を活用した出席確認の実データにより分析を実施した．具体的には出席管理システムの設定にて各学生の出欠確認に使用する携帯電話の MAC アドレスが確認できる設定にすることにより，同じアドレスであった場合は同一携帯を使用した「代理出席」であったものと仮定した．

履修講義 247 人の講義にて出席確認を実施したところ，初回講義においては，出席者数 161 人の内，10 人，6.2%の ID 重複がデータにより確認された．以降，この ID 重複者割合は講義における説明・注意喚起の効果もあり，徐々に減少していった．

本数値の意味するところは，「同じ携帯端末での出席登録」であり，学生間の携帯端末貸し借りの可能性もあり，ID・パスワードを学生間で共有していた不正出席登録に直結するものではないが，「なりすまし」の可能性を示唆する一つの参考データになるものと思われる．

4. 「なりすまし」の就学への影響

続いて，こうした代理出席学生の成績・進級面への影響について分析を下記条件により実施した．

【分析方法】

① 講義の ID 重複による代理出席可能性学生を抽出する（総数 24 名）

② 上記学生の最終的な GPA を確認する

③ ID 重複は 2 名 1 組となっており，GPA 下位者が上位者に依頼して，「なりすまし」を実施していたものと仮定する．

④ 総数 24 名の内，GPA 下位者 12 名の最終的な進級状態（卒業・退学）について調査する．

分析の結果は図 1 に示すように，25%の学生が最終的には退学となっていた．学部全体の平均した退学率が約 5%であることからすると，かなり高い数値を示しており，本数値の意味するところは，「代理出席」により講義に参加しない学生はその場対応として出席となったとしても学力は見につかず，講義についていけなくなることで，最終的には退学にもつながる可能性があることとなる．

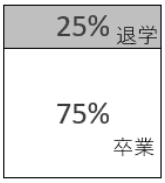


図 1　代理出席可能性
学生の卒業・退学区分

Research on Anti-spoofing Using FIDO2 Server - From the Perspective of Dropout Prevention -
†1 OSAMU SUGIMOTO, Josai University
†2 TAKASHI SHIDA, Josai University
†3 YUJI OHGI, Keio University

中途退学理由の調査研究における大学の主なものとして，日本中退予防研究所の調査があるが，図 2 で示されるように，「学習意欲損失」がある．代理出席により，学習についていけなくなることがこの主要な要因につながる可能性がある[3].

退学理由	学習意欲損失	人間関係	関心の移行	不本意入学	学業不信	精神・身体疾患	経済的理由	妊娠
割合	65.3%	40.6%	34.7%	15.8%	11.9%	6.9%	6.9%	2.0%

図 2 日本中退予防研究所の大学中途退学理由の内訳
（N=101）

一方，高等学校に関する退学者に関する調査としては，内閣府にて実施された若者の意識に関する調査があるが，図 3 で示されるように，退学理由の割合の多くを占めるものに，「欠席・欠時」の増加があげられている[3].

退学理由	欠席・欠時の増加	校則・校風の不適応	勉強の習得不全	人間関係不全
割合	54.9%	52.0%	48.6%	46.3%

図 3　内閣府 ： 若者の意識に関する調査
（高等学校中途退学者の意識に関する調査）

5. FIDO2 サーバーによる「なりすまし」防止

城西大学では学術機関としては初めて独自の FIDO2 アプリケーション・サーバーを構築し，「なりすましのできない出席管理システム」として運用を始めた．

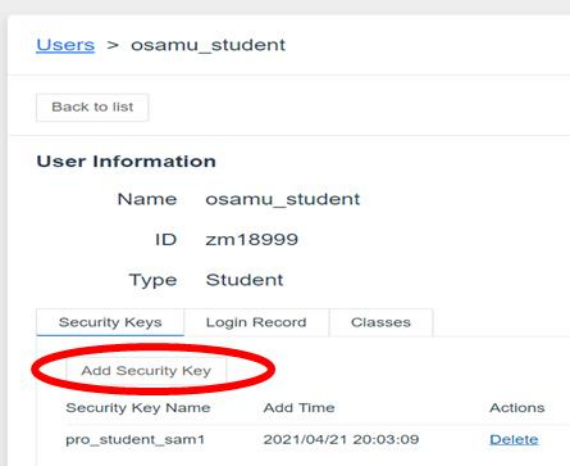
運用の手順は以下のとおりである．

①FIDO2 セキュリティキーを準備する．下図のような FIDO2 セキュリティキーをユーザー数に合わせて担当教員に配布する．下図は USB 型であるが NFC 型，BLE 型，それのハイブリッド型がある．FIDO2 準拠であればどこのベンダーでも構わない（多数選択肢がある）．

②担当教員は自身のパソコンを使って学生一人一人に FIDO2 セキュリティキーを配布するのと同時にそれぞれの学生のセキュリティキーにそれぞれの学生の指紋を登録させる．学生の指紋情報は学生が所持するセキュリティキーにのみ登録される．FIDO2 標準ではセキュリティキーに登録された指紋情報は TEE(Trusted Execution Environment)や SE(Secure Element)と呼ばれる領域に格納され，アプリケーションや OS から完全に独立するため，何人たりとも取り出すことはできない．

③FIDO2 サーバーにユーザー（教職員・学生）を登録する．この際，名前，ID，種別（学生・教員）のみを登録する．

④それぞれのユーザーごとに使用するセキュリティキーを登録する（下図参照）．この際，サーバーからセキュリティキーにチャレンジ（ランダムに生成された文字列）が送られ，ユーザー認証を求められる．上記で登録した自身の指紋で認証することでセキュリティキー内部で秘密鍵と公開鍵が生成される．チャレンジに秘密鍵で署名し，署名したチャレンジと公開鍵をサーバーに送る．そして公開鍵のみがサーバーに登録される．



⑤参加学生はアプリを立ち上げ，セキュリティキーを（例えば）USB ポートに挿入する．

⑥担当教員が授業開始ボタンをクリックし，ユーザー（学生）は，当該授業を選択し，出席を登録する．

6. おわりに

今回導入する，FIDO2 サーバーを活用することにより，なりすましができなくなる．これにより学生の「代理出席」が防止でき，退学者防止に一定の効果があるのではないかと思われる．授業を一定割合以上欠席した学生を出席不良者とするならばそれらの学生が無事卒業したかの統計をさらに集め，出席を促すことが退学防止への一つのアプローチであるとわかれば「なりすまし防止」はさらに意味を帯びる．次の機会にはさらにサンプル数を増やした結果が報告できるようにチャレンジしたい．

参考文献

[1] IPA（独立行政法人　情報処理推進機構）. (2021). 2020 年度情報セキュリティの脅威に対する意識調査.
[2] 加藤大弥　藤原正和　林達也　砂原秀樹. (2019). 学内サービスパスワードレス化の実現性の検討. マルチメディア，分散，協調とモバイル(DICOMO2019)シンポジウム
[3] 志田 秀史(2017). 専門学校における中途退学危険因子と学業定着施策の研究. 法政大学審査学位論文.