FIDO2 認証サーバーによる退学者防止効果の研究
——出席不良者と退学率相関関係の視点にて——

杉本　理[†a)]　志田　崇[†]　仰木　裕嗣[††]

Research for Dropout Prevention Using FIDO2 Authentication Server: From Aspect of Correlation Between Poor Attendance and Dropout Rate

Osamu SUGIMOTO[†a)], Takashi SHIDA[†], and Yuji OHGI[††]

あらまし　FIDO2 標準は，クレデンシャルをユーザとサーバーで共有しないことから，安心・安全な認証環境を構築できることで知られる．本論文においては，城西大学が独自に実装した FIDO2 アプリケーション・サーバーによるパスワードレス環境において，なりすましのできない出席管理システムが退学者防止効果に与える影響ついて，出席不良者と退学率相関関係の視点にて分析を行った．分析の結果，「1 年生の退学率・退学者数が最も多いこと」「リモート対応の中，退学につながる可能性のある「出席不良者」の確認対応に改善必要性があること」を確認し，FIDO2 サーバーの活用は，こうした学生の退学者防止に一定の効果がある可能性があることを確認した．

キーワード　出席不良者，退学者防止，なりすまし，FIDO2，Web 認証，生体認証

1. まえがき

コロナの影響により，各教育機関においてはリモートアクセスを活用した講義が進められている．一方，リモート環境において，「環境になじめない」「学習についていけない」等の理由からの退学者も発生している．本論文では，なりすましができない FIDO2 認証サーバーと出席管理システムによる退学者防止効果について，出席不良者と退学率相関関係の視点にて分析，考察を行う．

なお，本研究においては生体情報として指紋を扱うが FIDO2 標準に準拠しているため，サーバーに生体情報が保管されたり，収集するものではない．ただし，学生を対象とした実験であることから，城西大学において「人を対象とする研究倫理審査委員会」の審査を受け，承認番号【人倫 2021-03】として承認を受けている．

2. はじめに

学生の退学理由に関する影響分析の研究によれば，退学理由の主な要因としては「学習意欲損失」があり，欠席の増加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ことを指摘している [1].

一方，学生の代理出席という視点でパスワード共有の意識分析の結果，友人からパスワードを聞いてしまう学生もある割合で存在していることを指摘している [2]．また，「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，全体的に友人とのパスワード等の共有に対する問題意識が低い [3]．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．

こうした先行研究の知見を踏まえ，本論文においては出席不良者と退学率の相関関係を実データにより分

† 城西大学経営学部，坂戸市
Faculty of Management, Josai University, 1–1 Keyakidai, Sakado-shi, 350–0295 Japan
†† 慶應義塾大学大学院政策メディア研究科，藤沢市
Graduate School of Media and Governance, Keio University, 5322 Endo, Fujisawa-shi, 252–0882 Japan
a) E-mail: sam@josai.ac.jp
DOI:10.14923/transfunj.2022BAP0005

析するとともに，特にリモート環境において発生懸念されるパスワード共有による代理出席の解決手段の一つとして FIDO2 認証による出席管理を提案し，学生，教員，FIDO2 サーバー間のデータの流れや運用方法について説明する．そして所持と生体情報によるパスワードレス認証がなりすましを防止することで代理出席を実行するきっかけをなくし，出席が必須であるという文化を広めることで，出席不良者そして退学者防止に有効である可能性について考察していく．

3. 分　　析

先行研究の知見である，退学と欠席率の関連性を分析する為，所属する大学学部の学生の出席不良者と退学との関連性について分析を行った．

分析は，1 学年定員 500 名の学生について過去 6 年間分（2016～2021 年度）にわたって行った年 2 回調査の結果であり，この調査における出席不良者データと退学者の関連性分析を行った．

分析データの概要，分析方法を下記に示す．

- 出席不良者の定義
  - ‥年 2 回調査を行っているゼミ，必修科目の出席率の悪い学生のうち，特に 1 年～4 年まで必修講義となっているゼミに焦点をあて，講義開始から 5 回目までで 3 回以上欠席の学生を出席不良者と定義した．

    尚，本定義は大学学則における講義の 1/3 欠席により単位不可となることから，15 回講義においては 5 回欠席となると単位不可となり，最初の 5 回で 3 回欠席者は単位不可となる可能性が高い学生であるとして設定されている．
- 出席不良者総数
  - ‥上記定義のもと，抽出された出席不良者は過去 6 年間で 1,028 名
- 退学者総数
  - ‥過去 6 年間（2016～2021 年度）での 2021 年 12 月時点での退学者総数は 415 名
- 分析方法
  - ‥上記データについて，「出席不良者」と「退学者」の相関関係について

    ①学年別

    ②年度別

    の傾向分析を実施した．

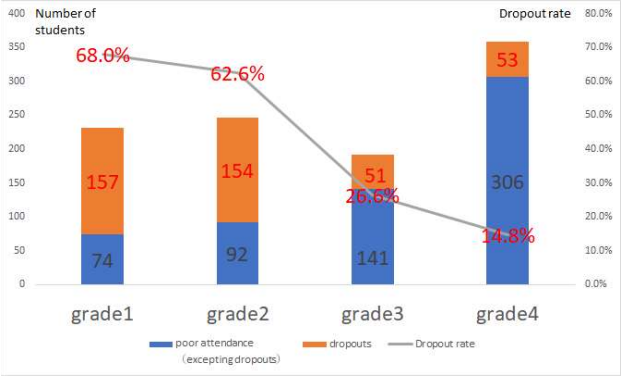


図 1　出席不良者及び退学者数並びにその割合（学年別）
Fig. 1　Number of Poor Attendance and Dropouts, and its ratio (By Grade).

3.1　学年別分析

上記定義の出席不良者と退学者の相関関係における学年別分析結果を図 1 に示す．

この分析結果より 1 年生においては出席不良者は 74 名（出席不良者にリストアップされたものの退学とはならない学生）+ 157 名（出席不良者にリストアップされ，最終的に退学となった学生）の 231 名となり，退学率は

157 名（退学者）÷ 231 名（出席不良者）= 68.0%

であり，出席良好者の退学率が約 5% であることと比較するとかなり高い数値であることがわかる．

同様な見方を学年ごとに見ていくと，下記傾向があることが見て取れる．

(1) 退学率は 1 年生が最も高く，学年があがるごとに減少傾向となる．（1 年（68.0%），2 年（62.6%），3 年（26.6%），4 年（14.8%））
(2) 退学者は 1 年生が多く，次に 2 年生，4 年生，3 年生と続く．（1 年（157 名），2 年（154 名），4 年（53 名），3 年（51 名））
(3) 出席不良者は 4 年生が多く，次に 2 年生，1 年生，3 年生と続く．（4 年（306 + 53 = 359 名），2 年（92 + 154 = 246 名），1 年（74 + 157 = 231 名），3 年（141 + 51 = 192 名））

ここから言えることは，退学率，退学者ともに 1 年生が最も高い為，1 年次の出席不良者への面談等によるフォローが重要であることが示唆されるとともに，出席不良者とならないよう，適切な出席管理が重要となってくることがわかる．

また，4 年生に出席不良者が多いものの，退学率が低いことについては，就職活動が佳境となっているこ

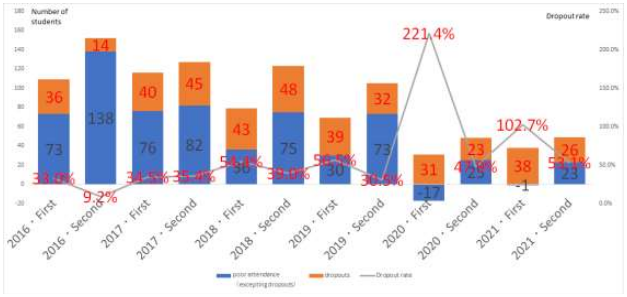


図 2　出席不良者と退学者の相関関係（年度別）
Fig. 2　Correlations Between Poor Attendance and Dropouts (By Year).

とから出席率は一時的に下がってしまうものの，就職が決まった後はきちんと履修がなされ，退学には至っていないことが推察される．

3.2　年度別分析

次に，出席不良者と退学者の相関関係における年度別分析結果を図 2 に示す．

この分析結果で特に顕著な傾向としては 2020 年度前期において退学率が 221.4% となっているが，これはコロナウイルス禍（以下，コロナ禍による顕著な影響が発生したのが 2020 年度からであるということである．

2020 年度前期で「出席不良者にリストアップされたものの退学とはならない学生」が −17 名という数値となっているが，これは退学者が 31 名発生したにもかかわらず，出席不良者調査においては 14 名しかリストアップできていなかったことを示す．退学者自体は 31 名ということで，例年並みの人数であったことから，退学者が激増したということではなく，コロナ禍によるリモート対応という前例のない状況の中，大学・学生間で出欠確認・集計において例年通りの対応が難しかったことを示している．

2021 年度前期においても退学率は 102.7%，「出席不良者にリストアップされたものの退学とはならない学生」は −1 名，退学者自体は 38 名の例年並みとなっていることから，数値的には改善されているものの，まだ大学・学生間で出欠確認・集計において例年通りまでの対応とはなっていないことを示している．

3.3　欠席率と退学者，なりすまし出席の関連性

これまで出席不良者と退学者の相関関係を学年別・年度別に見てきたが，欠席率と退学者の関連性については，見かけ上は出席となっているものの，いわゆる学生による「なりすまし出席」による事実上の欠席者の問題もある．

「なりすまし」の実態分析では杉本などにより大人数講義での実態調査がなされているが，履修講義 247 人の講義にての出席確認で出席者数 161 人の内，10 人，6.2% の ID 重複がデータにより確認されている．そして，こうした「なりすまし」出席学生の成績・進級面への影響についての分析では，「なりすまし」出席可能性学生（総数 24 名）の内，ID 重複 2 名 1 組の内，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と GPA 下位者 12 名の最終的な進級状態（卒業・退学）では 25% の学生が最終的には退学となっており，学部全体の平均した退学率，約 5% と比較して 5 倍の高い数値を示していた [4]．

以上の分析結果による示唆として，

- 1 年生が退学率・退学者数ともに最も多い
- コロナ禍によるリモート対応の中，退学につながる可能性のある「出席不良者」の確認対応に改善の必要性がある
- 出席者の中には「なりすまし」出席学生が発生している可能性がある
- 「なりすまし」による欠席者の退学率は全体平均の約 5 倍

があげられる．

以上のことからなりすまし（代理出席）をなくすことが退学者防止に一定の効果がある可能性が仮定できる．次章ではなりすまし（代理出席）をなくす方法として FIDO2 認証サーバーを活用することを提案する．

4.　FIDO2 認証による出席管理

前章ではなりすましができない出席管理システムが提案できれば代理出席が減り，結果的に退学者防止につながる可能性があることが指摘された．本章では FIDO2 認証がなぜなりすまし防止となるのか，FIDO2 標準の概要，FIDO2 認証サーバーと統合された出席管理システムの実装，運用の方法及び FIDO2 認証フローについて詳述する．

4.1　FIDO2 標準の意義

FIDO2 標準は 2019 年 3 月 4 日に World Wide Web Consortium（W3C）と FIDO Alliance によって策定された世界標準である．FIDO2 は W3C 勧告である，Web Authentication: An API for accessing Public Key Credentials（WebAuthn）[5] と FIDO Alliance におけるデバイス間連携仕様である，Client-to-Authenticator Protocol（CTAP）から構成される [6]．FIDO2 ではバイオメトリクスなどがバインドされた認証器または FIDO セ

表 1　カテゴリーごとのセキュリティインシデント
Table 1　Security Incident by Category.

Security Incident by Category(4Q2021)		
Phishing Site	6,311	**71.8%**
Website Defacement	579	6.6%
Malware Site	119	1.4%
Scan	1,291	14.7%
DoS/DDoS	7	0.1%
ICS Related	0	0.0%
Targeted attack	4	0.0%
Other	475	5.4%

キュリティキー，モバイルデバイス，ウェアラブルなどの外部認証器が利用できる多要素認証を提供できる．FIDO2 標準における CTAP を特に CTAP2 と呼び，従来 FIDO U2F と呼んでいた CTAP1 と区別している．技術仕様の解説は五味（2018）などを参考にされたい [7]．多要素認証は通常，① Something You Know（知識：パスワード，PIN，画像など）② Something You Have（所持：トークン，スマートカード，USB トークンなど）③ Something You Are（生体：生物学的な特徴，行動特性，指紋，顔など）から二つを選んで認証することを意味するが，パスワード＋スマホアプリ，パスワード＋トークンなどが一般的であり，「パスワードのみ」での認証に比べてセキュリティレベルは上がるものの利便性は劣る．FIDO2 ではパスワードを使わない，「パスワードレス認証」が特徴の一つであり，堅牢なフィッシング耐性を有している．

JPCERT/CC の報告によれば，フィッシングはセキュリティ・インシデントの約 72% を占めており [8]，フィッシング耐性をもった環境の構築は極めて重要である（表 1 参照）．

また，警察庁によれば近年自動車業界などに大きな影響を与えているランサムウェアへの感染は，フィッシングなどによってパスワードが盗まれ，リモートデスクトップサービスや VPN などのネットワーク機器を経由して被害にあったという報告がされている [9] ことからも，パスワードのない「パスワードレス」を実現できる FIDO2 は企業に限らずコンピュータネットワーク・セキュリティのベストプラクティスの一つであると言うことができる．

図 3　キャンパス ID 型 FIDO2 セキュリティキー
Fig. 3　Campus ID Type FIDO2 Security Key.

4.2　キャンパス ID 型セキュリティキーと FIDO2 認証サーバーの実装

4.2.1　セキュリティキーの選択

学生や教職員が所持する FIDO2 セキュリティキーは，①所持＋生体の 2 要素認証がワンデバイスで実現できること，②セキュリティキーを出席管理のためだけに携帯するのでは利便性を損ね，紛失や遺失につながる．普段もち歩いているキャンパス ID と兼用できるようにカード型とした．③USB，NFC，BLE で認証が可能なこと．④運用において IT センターなどが仮セキュリティキーの貸出しが容易なこと．を条件に調査し，Authentrend 社の ATKey.Card を選択した．身分証風のシールを貼ってキャンパス ID のように実装した [10]（図 3 参照）．なお，学生用のカードはファームウェアを改変して自身では指紋を登録できないようになっている（友人の指紋を登録できないようにするため）．教員のパソコン若しくは IT センターや事務室でのみ指紋登録が行える．この実装方法は FIDO2 を利用するにあたり，Binding Assurance Level を強化するための手段として重要であると考えた．

4.2.2　FIDO2 サーバー（JAMS）の実装

前述のように FIDO2 の仕様は W3C や FIDO アライアンスによって公開されており，それに準拠することで実装が可能である [5], [6]．また，StrongKey 社のように github 上でサーバーのソースコードを公開して商用利用を許可しているケースもある [11]．城西大学では，OS に Ubuntu，開発言語に Node.js，データベースに Mongo DB，Web サーバー・リバースプロキシに NGINX を用いて FIDO2 認証サーバー及び出席管理アプリケーションを実装し，Josai Attendance Management System（JAMS）とした．図 4 にログイン

図 4　JAMS ログイン画面
Fig. 4　JAMS Login Screen.

画面を示す．

JAMS には三つの権限を用意した．以下にそれぞれの権限と可能な作業を示す．

【アドミン】：キャンパス（学部），時間割，授業，教員・学生の登録

【教員】：教員及び学生のセキュリティーキーの登録及び指紋の登録・修正，授業の詳細登録（遅刻限界時間，受講者など）

【学生】：自身の受講科目への出席登録・出席状況の閲覧など

現在，教員 3 名，学生 66 名で運用している．

4.3　JAMS による FIDO2 認証と出席管理

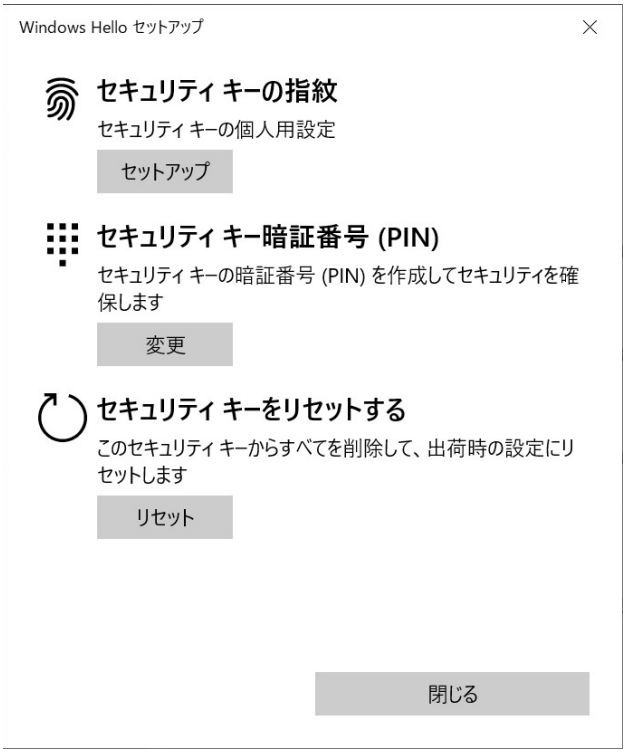
実際の出席管理システムの運用工程と FIDO2 認証フローは以下のようになる．

(1) アドミンは担当教員及び学生にセキュリティキーを配布する

(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．IT センター等が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ても構わない．上述のように学生自身のパソコンでは指紋の登録ができない仕様になっている．

指紋の登録は Windows 環境では【設定】⇒【アカウント】⇒【サインインオプション】⇒【セキュリティキー】⇒【管理】と進むと図 5 の画面となり，指紋が登録できる．MacOS などの環境ではベンダーが供給するアプリケーションによって指紋を登録する．

(3) 教員は JAMS に自身と受講する学生の名前，ID（学籍番号など），種別を登録する．学生を JAMS に登録した画面を図 6 に示す．



供給するアプリケーションによって指紋を登録する．

図 5　指紋登録画面
Fig. 5　Fingerprint Registration.

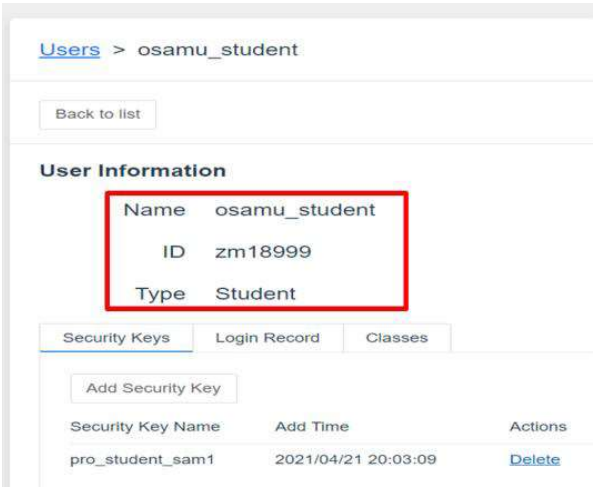


図 6　JAMS に学生を登録した様子
Fig. 6　Registered Student in JAMS.

(4) 教員は JAMS において自身と各学生が使用するセキュリティキーを登録する（図 7 参照）

【FIDO2 フロー】この際，JAMS 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

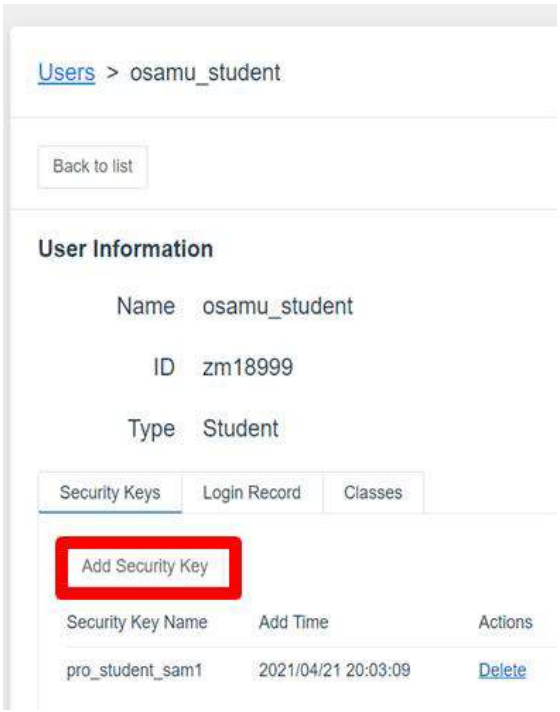


図 7　セキュリティキーの登録画面
Fig. 7　Registering a Security Key.

名し，署名したチャレンジと公開鍵を JAMS に送る．そして公開鍵のみが JAMS に登録される．

(5) 教員と学生は JAMS を立ち上げ，ログインする．登録したセキュリティキーによる認証を要求されるので NFC ポートにかざしたり，USB ポートに挿入する．

【FIDO2 フロー】この際，JAMS からチャレンジがセキュリティキーに送られ認証を促されるので自身の指紋で認証する．署名されたチャレンジは JAMS に送られ，JAMS において保管されている公開鍵を使ってチャレンジを検証する．

(6) セキュリティキーのグリーンのライトが点灯することで認証が成功したことがわかる．これにより所持しているセキュリティキーが自身のものであることが証明され，JAMS へのログインが許可される．

(7) 担当教員が授業開始ボタンを JAMS 上でクリックし，学生は当該授業選択し，セキュリティキーを指紋認証することで出席を登録する．

なお，(4) (5) のプロセスにおいてネット上にチャレンジや公開鍵が流れるがインターセプトされたとしても何らセキュリティに対する脅威とはならないことが FIDO2 認証の大きな利点となる．

これにより，なりすましのできない出席管理システムが実現され，代理出席ができないことから退学者防止につながる可能性がある．

図 8　JAMS デモ動画
Fig. 8　JAMS Demo Movie.

JAMS のデモ動画は以下から閲覧できる（https://www.youtube.com/watch?v=CUnOLJYKftc）（図 8）．

5. む　す　び

本論文においては，FIDO2 サーバーによる退学者防止効果について，出席不良者と退学率相関関係の視点にて分析を行った．分析結果，「1 年生の退学率・退学者数が最も多いこと」「リモート対応の中，退学につながる可能性のある「出席不良者」の確認対応に改善必要性があること」が確認された．

出席者の中には「なりすまし」出席学生が発生している可能性があり，これらの学生の退学率は高いことが指摘されている中，FIDO2 サーバーの活用は，こうした学生の退学者防止に一定の効果がある可能性があることが確認された．

サンプル数（FIDO2 セキュリティキーによる出席管理を行っている学生数）66 名，期間 1 年間においては平均出席率 92.6% で退学者はゼロである．今後学生数を増やし，継続していくことで FIDO2 サーバーによるなりすまし防止が欠席をするきっかけをなくし，授業への参画を促すと同時に勉学意欲の喪失を抑制し，結果的に退学者防止につながっているというデータを蓄積したい．

また，今回開発した JAMS は他大学も利用できるよう設計してあり，広く使っていただきたいと考えている．退学者防止は全ての大学における課題であり，データを集めてシステムの改善につなげていきたい．

同時に JAMS はパスワードレス・キャンパスネット

ワークを実現でき多くのサイバー攻撃からキャンパス資産を守ることができる．執筆の時点では Android スマホの一部のみが FIDO2 セキュリティキーに対応しており，上述のキャンパス ID 型セキュリティキーの代替にもなる．iOS スマホが FIDO2 対応になるのが待ち遠しいが，FIDO2 セキュリティキーとしてのスマホ利用も今後検証していきたい．

文　献

[1] 志田秀史，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，法政大学博士論文，pp.5–7, 2017.
H. Shida, Research on Risk Factor of Dropout and Method for School Retention, Hosei University, Ph.D Dissertation, pp.5–7, 2017

[2] 澤　信吾，菊地拓翔，熊谷匠純，関　良明，“大学生の情報セキュリティ意識に関する調査分析，”信学総大・情報・システム講演論文集 1，p.100, 2018.
S. Sawa, T. Kikuchi, T. Kumagai, and Y. Seki, “Investigation Analysis of Information Security Consciousness in University Students – Passwords Sharing on Spoofing Attendance,” IEICE, Proc. Annual Conference#1, p.100, 2018

[3] 加藤大弥，藤原正和，林　達也，砂原秀樹，“学内サービスパスワードレス化の実現性の検討，”IPSJ，マルチメディア，分散，協調とモバイル (DICOMO2019) シンポジウム，2019
D. Kato, M. Fujio, T. Hayashi, and H. Sunahara, “Feasibility of password-less authentication in campus services,” IPSJ, DICOMO2019, 2019.

[4] 杉本　理，志田　崇，仰木裕嗣，“FIDO2 サーバーによるなりすまし防止効果の研究，”情報処理学会全国大会論文集 3，pp.5–6, 2021.
O. Sugimoto, T. Shida, and Y. Ohgi, “Research on anti-spoofing using FIDO2 server – From the perspective of dropout prevention –,” IPSJ, Proc. Annual Conference#3, pp.5–6, 2021.

[5] W3C, “Web Authentication: An API for accessing Public Key Credentials,” https://www.w3.org/TR/webauthn-1/, ref. March 1, 2022.

[6] FIDO Alliance, “FIDO authentication specifications,” https://fidoalliance.org/specifications/download/, ref March 1, 2022.

[7] 五味秀仁，大神　渉，“FIDO 認証とその技術，”IEICE, Fundamentals Review, vol.12, no.2, pp.115–125, Oct. 2018.
H. Gomi and W. Oogami, “FIDO Authentication and Its Technology: Technical Specifications and Standardization Activities,” IEICE, Fundamentals Review, vol.12, no.2, pp.115–125, Oct. 2018.

[8] JPCERT/CC, “Incident handling report,” https://www.jpcert.or.jp/english/doc/IR_Report2021Q3_en.pdf, ref March 1, 2022.

[9] 警察庁，“サイバー犯罪対策プロジェクト：ランサムウェア被害防止対策，” https://www.npa.go.jp/cyber/ransom/index.html, ref March 1, 2022.

[10] 杉本　理，仰木裕嗣，“FIDO2 サーバーと身分証型セキュリティキーによるパスワードレス・キャンパスネットワークの構築，”情報処理学会全国大会論文集 3，pp.7–8, 2021.
O. Sugimoto and Y. Ohgi, “Implementation of Password-less Campus Network Using Josai FIDO2 Server and Campus ID Type Security Key,” pp.7–8, IPSJ, Proc. Annual Conference#3, 2021.

[11] StrongKey, “FIDO2,” https://github.com/StrongKey/fido2, ref Oct. 1, 2021.

（2022 年 3 月 16 日受付，7 月 6 日再受付，9 月 5 日早期公開）

杉本　理　（正員）

東北大学情報科学研究科博士課程単位取得退学．スタンフォード大学客員研究員，日米での起業などを経て 2013 W3C アジア地区事業開発リーダー兼慶應義塾大学大学院政策メディア研究科特任准教授．2018 より城西大学経営学部教授．認証技術，経営と AI などの研究に従事．

志田　崇

1993 慶應義塾大学経済学部卒業，2006 多摩大学大学院経営情報学研究科修士課程（MBA）修了，2012 中央大学総合政策研究科博士後期課程修了．2018 より城西大学経営学部准教授．

仰木　裕嗣　（正員）

慶應義塾大学大学院政策・メディア研究科兼環境情報学部教授，慶應義塾大学 SFC 研究所スポーツ・アンド・ヘルスイノベーションコンソーシアム代表，専門分野はスポーツ工学，スポーツバイオメカニクス，センサ計測．

Abstract FIDO2 standard is known as a safe and secure authentication protocol since it does not share users' credentials between server and user. In this paper passwordless environment achieved by the FIDO2 application server Josai University implemented is effective for non-spoofing attendance management, and leads to dropout prevention. An analysis was made to find correlation between poor attendance and dropout rate. We found poor attendance management should be improved since freshmen's dropout rate is higher than others and poor attendance rate is higher at hybrid classes. .

Keywords Poor attendance, Dropout prevention, Spoofing, FIDO2, Web Authentication, Biometric Authentication