The Josai Journal of Business Administration (2021), Vol. 17, No. 1, 39−54

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

志田　崇・栗田るみ子・杉本　理

要　旨

2020 年のコロナ禍により，感染対策の面から社会のデジタル化・オンライン化が急速に進んでいる。文部科学省は，GIGA スクール構想として，2023 年度までに義務教育の全課程において児童生徒のひとりひとりに学習用端末を購入することを決定した。これは，高速大容量の通信ネットワークの環境の新しいスクールの実現を推進したものである(1)。

また，大学入試などにおいても文部科学省の「令和 4 年度大学入学者選抜実施要項」（2021 年 6 月 4 日）で，新型コロナウイルス感染症拡大防止の観点から，ICT を活用したオンラインによる入学試験への工夫が要請されている。

以上のことから，城西大学の杉本理，栗田るみ子，志田崇の研究チームはデジタル化・オンライン化へ向けた学習環境の構築のための，研究設備整備費等補助金を獲得した(2)。補助金により，学内にサーバーを設置し，世界初のアカデミア所有の FIDO 2 認証サーバーを完成させた。

「FIDO 2（Fast Identity Online 2）標準を利用したパスワード認証環境による機密性，可能性の高いデジタルクラスルームの運用システムを構築し，JAMS（Josai Attendance Management System）」と名付けた。

本論では，JAMS の活用による，オンライン上での，「なりすまし」による不正防止の可能性に関する検討について述べる。

キーワード：オンライン認証，なりすまし，不正防止，FIDO 2，パスワードレス

1. オンライン授業による学びの変化

2001 年のインターネットを利用したメディア授業が実施されてから 20 年の月日が過ぎ，2020 年のコロナ禍によるキャンパス閉鎖を受け「オンライン授業」という呼称が当然のように展開している。文科省が設置基準で用いてきた「メディア授業」という表現はあまり耳にしないが，同様の意味合いを持っているようである。いずれにしても，これまで行われてきた対面授業と異なる講義や演習をインターネット上で実施することに軸足を置いた新しい授業形態である。

1998 年 3 月までは，我が国の学部通学制において，メディアを利用した授業（以下「メディア授業」）

（1） GIGA スクール構想は（Global and Innovation Gateway for All）の略称で文部科学省が，『安心と成長の未来を拓く総合経済対策』（令和元年 12 月 5 日閣議決定）において，「学校における高速大容量のネットワーク環境（校内 LAN）の整備を推進するとともに，特に，義務教育段階において，令和 5 年度までに，全学年の児童生徒一人ひとりがそれぞれ端末を持ち，十分に活用できる環境の実現を目指すこととし，事業を実施する地方公共団体に対し，国として継続的に財源を確保し，必要な支援を講ずることとする。あわせて，教育人材や教育内容といったソフト面でも対応を行う。」目的で設置。

（2） 2019 年度文部科学省私立大学等研究設備整備費等補助金を獲得。

は認められていなかった。1998 年 3 月～1999 年 3 月の間，メディア授業が 30 単位認められたが，このときは未だインターネットによる授業は認められていない。この時のメディア授業は，同時かつ双方向のもので，例えば衛星通信，テレビ会議システムのみである。以下に示すように，その後，時を経て 2001 年 3 月から，インターネットによるメディア授業が 60 単位まで認められるようになった（大学設置基準第 32 条第 5 項)。

1) 【学部（通学制)】卒業要件 124 単位中，60 単位まで
2) 【学部（通信制)】卒業要件 124 単位すべてをメディア授業により修得可
3) 【大学院】卒業要件 30 単位すべてをメディア授業により修得可
※ただし研究指導は別途必要
4) 【短期大学】(a)修業年限 2 年の場合：卒業要件 62 単位中 30 単位まで；(b)修業年限 3 年※の場合 : 卒業要件 93 単位中 46 単位まで（※修業年限 3 年以上の夜間学科等のうち，短期大学設置基準第 19 条の卒業の要件の特例の対象となるものについては，卒業要件 62 単位中 30 単位まで((a)と同様))

引用　文部科学省　授業時間の縛り→法令「大学設置基準」より

このようなネットワーク時代に 2018 年から 2022 年の 5 年間で実現する予定の，GIGA スクール構想は児童生徒 1 人 1 台の端末と高速通信環境の整備をベースとして，「個別最適化され，創造性を育む教育」を実現させる施策であった。しかし，2019 年の新型コロナウイルスの流行と新たな生活様式への対応を受け 2020 年 5 月に，「GIGA スクール構想の加速による学びの保障」として追補版が発表され，補正予算も 4,610 億円と大きく増額された。その結果，2021 年 3 月には，ほとんどの自治体ですでに 1 人 1 台端末や高速通信ネットワークの実現へ向け動いた。

このような中，文部科学省は，GIGA スクール構想として，2023 年度までに義務教育段階にある小学 1 年から中学 3 年生の児童生徒のひとりひとりに学習用端末購入を進め，1 人あたり最大 4.5 万円の補助，学校へは環境整備費（2 分の 1 補助）を行うことで，高速大容量の通信ネット環境スクールの実現を推進している。現在の取り組みの中心は，「授業や自宅学習での端末の利活用促進」「授業での活用事例の創出・共有」，「教員の指導スキルの向上」，「コンテンツのリッチ化」，「高校の ICT 環境の整備」などの課題解決にシフトしてきている。

現在メディア授業の実施においては，定義や指導法が混在して議論の只中にあり，未確定の状態であるが，文部科学省は 2001 年に告示第 51 号（大学設置基準第二十五条第二項の規定に基づく大学が履修させることができる授業等）において，メディア授業の類型で以下の 2 点を告示している。

メディア授業告示第 1 号
(1)　同時双方向型（テレビ会議方式等）
【形　態】「同時」かつ「双方向」
【履修場所】授業を行う教室等以外の教室，研究室又はこれらに準ずる場所
（科目等履修生の場合，企業の会議室等の職場又は住居に近い場所を含む。）
【その他留意事項】（平成 10 年 3 月 31 日通知より抜粋）
○授業を実施するに当たっては，面接授業に近い環境で行うことが必要であり，各大学においては，以下

のような事項について配慮することが望ましい。
・授業中，教員と学生が，互いに映像・音声等によるやりとりを行うこと。
・学生の教員に対する質問の機会を確保すること。
・メディアを利用して行う授業の受信側の教室等に，必要に応じ，システムの管理・運営を行う補助員を配置すること。また，必ずしも受信側の教室等に教員を配置する必要はないが，必要に応じてティーチング・アシスタントを配置することも有効であること。

メディア授業告示第２号
(2)　オンデマンド型（インターネット配信方式等）
【形態】「同時」又は「双方向」である必要は無い
【指導方法】①毎回の授業の実施に当たって，指導補助者が教室等以外の場所において学生等に対面することにより，又は②当該授業を行う教員若しくは指導補助者が当該授業の終了後すみやかにインターネットその他の適切な方法を利用することにより，【※MOOC 等】
*設問解答，添削指導，質疑応答等による十分な指導 * を併せ行うことが必要。*
＊学期末などにまとめてではなく，毎回の授業の実施に当たって併せ行う。
→いつまでに質疑応答を行うべきかについては，従来の通知等では必ずしも明示されていないが，①学生が疑問をただちに提出できる環境があること，②当該疑問が次の講義の学修の前提となる場合には，次の講義までに，もしくは次の講義の中で回答を行うこと，③②以外の場合には，講義期間中適切な時期に回答を行うこと，を目安として示してはどうか。
＊「指導」には，設問解答，添削指導，質疑応答のほか，課題提出及びこれに対する助言を電子メールやファックス，郵送等により行うこと，教員が直接対面で指導を行うことなどが含まれる。
→従来の通知等では示されていないが，ICT の活用例として，たとえば，よくある質問とそれに対する答えについて AI に蓄積し，学生からの質問があった場合には AI が回答し，AI が判断に迷う質問については担当教員若しくは指導補助者がフォローする，といった手法も考えられる。

引用　文部科学省は 2001 年に告示第 51 号（大学設置基準第二十五条第二項の規定

2020 年，城西大学では学生へ 5 万円の補助を出し，BYOD[(3)] によるオンライン環境を整えている。我々は，このような背景を基に，セキュリティに注目した BYOD 学習環境の構築を実現すべく，2020 年度設備研究支援費を獲得し，「FIDO 2 標準を利用したパスワード認証環境による機密性，可能性の高いデジタルクラスルームの運用システム（JAMS)」を構築した。本システムに用いている FIDO 2（Fast Identity Online 2）は個人情報をサーバーに残さず高速なオンライン ID 認証を可能としセキュリティ管理上，安心安全を担保している点で特徴といえる。

2. 教育機関におけるオンライン試験の現状

コロナ禍の影響もあり，感染対策の面から社会のデジタル化・オンライン化が急速に進んでいる。教育機関においては講義に加え，その動きは試験・入試にも広がりを見せている。日本英語検定（英検）においては，2013 年度よりコンピューターを利用して英検を受験する英検 CBT（Computer Based Testing）を開始しており，従来型の英検と同じ出題形式を取りつつ，1 日で 4 技能（リーディング，リスニング，ライティング，スピーキング）を測る「英検 S-CBT」の受験者数は増加しており，2020

（3）　BYOD は，Bring your own device の頭文字で「個人が保有しているパソコンなどの端末を活用すること」で教育効果を上げる目的がある。

年７月時点の累計受験者数は６万人を超えている[4]。

こうした受験生増加の背景には，従来型英検が年間３回の実施であったのに対し，「英検 S-CBT」は原則毎週土日に試験日を設定しており，受験生の予定に合わせて柔軟に受験日を選択できることがあげられる。

また，首都圏の私立中高も ICT（情報通信技術）を活用したオンライン入試の導入を進めている。各校のオンライン入試導入の動きに対し，神奈川県私立中高協会は「私学の多様性」を重視すべきとしてこれを前向きに捉え，「公平，公正の担保」を条件に実施に対して，基本的に容認の方針を示した。同様の方針は千葉県，静岡県でも示され，幾つかの学校においてオンライン入試としてプレゼンテーションや面接試験が実施され，海外在住者などが受ける「帰国子女入試」においても，こうしたオンライン面接の活用が進んでいる。

特に，千葉県市川市にある昭和学院においては，オンラインによる筆記試験も実施している。算数１科目で実施しており，実施方法としては Zoom を活用し，受験生は事前に配布された解答用紙を手元に，画面越しに提示される問題を解き，画面越しに回答用紙を提示する。こうした形式により，学校側として Zoom 越しに受験生を監視し，不正防止につとめている。

こうしたオンラインでの入学試験は有効であると評価されており，実施した各校は今後とも継続の方針を示している。

こうした中，文部科学省は 2021 年５月 24 日に「新型コロナウィルス感染症に対応するための個別試験におけるオンラインの活用」の結果を公表した。2021 年度の大学入試で，新型コロナ対応として実施されたオンライン入試の状況を学部ごとに調べ，調査は国公私立の計 775 校に行われ，調査回収率は 100％であった。

調査結果は，図１に示されているように，オンラインを活用した入試実施校の割合は「一般選抜」は 2.9％であったものの，「総合型選抜」で 19.1％，「学校推薦型選抜」で 18.4％，「その他選抜」（帰国生徒，社会人，留学生等）で 20.4％と約二割の大学がオンライン入試を実施している。

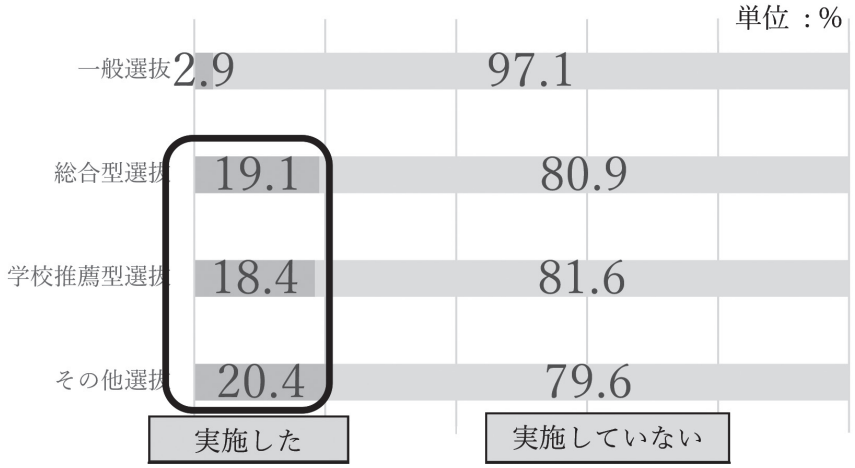

図１　個別選抜においてオンラインを活用した入試の実施状況[5]

出典）　文部科学省　大学入試のあり方に関する検討会議（第 26 回）2021. 5. 24 資料

（４）　日本英語検定協会（英検協会）は 2020 年７月 14 日に７月 12 日時点の英検 S-CBT の累計受験者数は６万 3,190 人にのぼると公表している。

（５）　文部科学省　大学入試のあり方に関する検討会議（第 26 回）2021. 5. 24 資料。

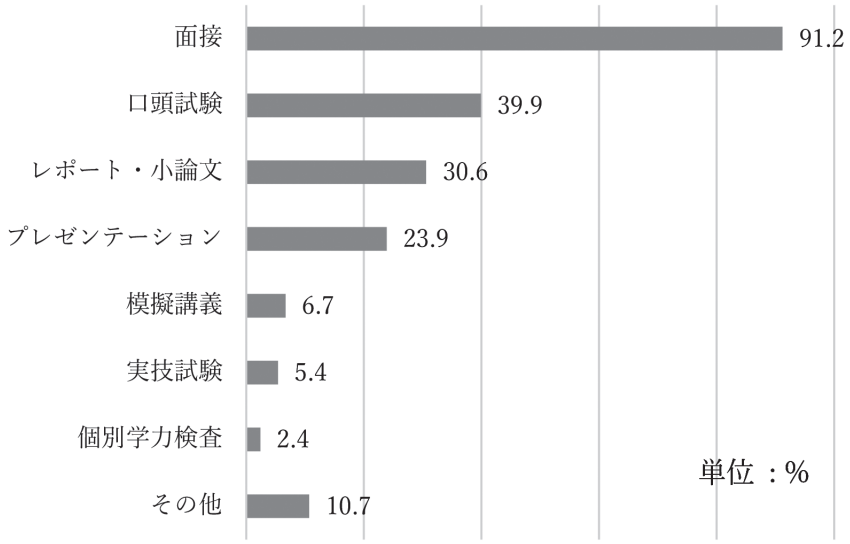

図２　オンラインを活用した入試の実施内容
出典）　文部科学省　大学入試のあり方に関する検討会議（第 26 回）2021.5.24 資料

「総合型選抜」を例として，オンライン入試の実施内容を見てみると，図２の如く「面接試験」が91.2%と最も多く，次いで「口頭試験」「レポート・小論文」「プレゼンテーション」の実施割合が多くなっている。「その他」の試験内容としてはグループディスカッションや自己 PR 動画，演奏動画の提出など多岐にわたっている。

また，文部科学省は 2021 年 6 月 4 日には「令和 4 年度大学入学者選抜実施要項」を通知し，新型コロナウイルス感染症の拡大防止の観点から，ICT を活用したオンラインによる選抜の工夫要請を行っている。具体的には，特に総合型選抜及び学校推薦型選抜において，ICT を活用したオンラインによる個別面接やプレゼンテーション，大学授業へのオンライン参加とレポートの作成，実技動画の提出，小論文等や入学後の学修計画書，大学入学希望理由書等の提出などを取り入れた選抜実施の工夫をうたっている。

在外教育施設やその他外国の学校の生徒についても，水際対策の影響により，容易に帰国できないことから，同様の工夫に配慮することを要請している。

このように，実施が広まっており，今後ますます拡大が予想されるオンライン入試だが，各校とも「不正防止対策」への取り組みが必要になっている。現状の主な不正防止対策は，選抜要項や学生募集要項での「注意事項の周知」であり，次いで「写真付き身分証明書を投影させることによる本人確認や，受験場所の全体を撮影させることによる環境の確認」が多くなっている。それ以外には「出願書類の写真と本人を照合」「誓約書の提出」「試験実施者による録画」などにより「不正防止対策」を実施している。

「遠方居住者（海外含む）の移動を伴わない受験機会確保」「交通費・宿泊費等の経済的負担の軽減」など受験生にとってメリットのある，こうしたオンライン入試はコロナ禍以降も単なる一時期の感染対策ということではなく，入学志願者拡大に向けた大学としての重点取り組み事項の一つになる可能性があると考えられる。

一方，「不正防止対策」という点では，現状上記のような対策で対応しているものの，いわゆる「なりすまし」の防止など更なる対策が必要になってくると思われる。

こうした中，「なりすまし」発生の可能性について，講義における出席データでの実証分析とあわせ，その防止策として，指紋認証による FIDO 2（Fast Identity Online 2）を利用した JAMS（Josai Attendance Management System）システムの可能性について考察する。

3. なりすまし不正の可能性 ── 講義での出席データによる ID 重複者確認

オンライン入試においては，様々に「不正対策」の実施が必要になってくるが，その一つに本人確認がある。本人確認の不正対策として，写真と本人との照合や ID・パスワードの設定などがあげられるが，いわゆる「なりすまし」の可能性について考察する。

「なりすまし」の可能性という観点から講義における 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。履修講義 247 人の講義にて Webclass[(6)] による出席確認において，「なりすまし」による代返防止の為，表 1 の条件設定にて出席確認を行った。

表 1　Webclass による出席確認　設定方法

	携帯端末 個別アドレス 確認	備　考
通常設定 （IP アドレス制限無し）	×	携帯キャリア通信経由にて出席登録が可能な為，個別アドレス確認不可
IP アドレス制限有り	○	大学の WiFi 経由での出席登録のみとなり，携帯端末の個別アドレス確認が可能

こうした条件設定により，大学の WiFi 経由での出席登録のみが可能となり，WiFi 経由した各学生の携帯端末の個別アドレス確認が可能となる。この出席データの分析結果を図 3 に示す。

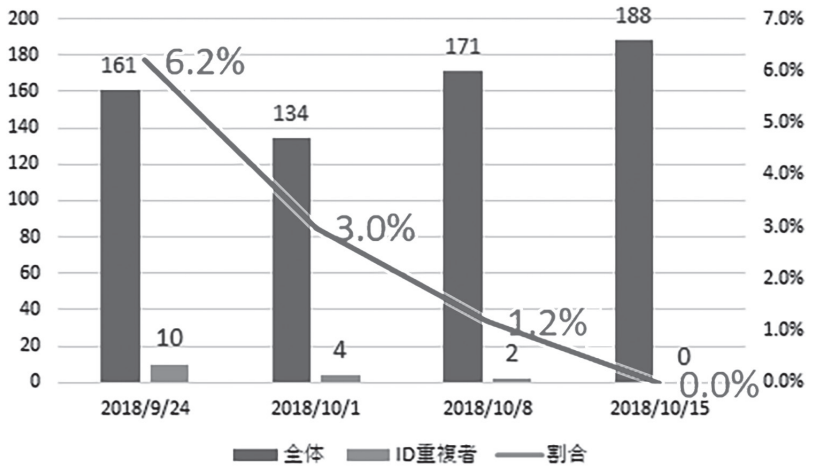

図 3　講義（247 名履修）における ID 重複者割合推移

（6）　Webclass（ウェブクラス）は，経営学部設立時の 2004 年から学部教育及び事務作業に利活用し教員及び学生に馴染みのある LMS（ラーニングマネジメントシステム）で，大学教育に必要な教材やテストの作成，レポート提出や成績データの集計が行える。

講義は履修人数 247 人の大人数講義となるが，本講義において Webclass による上記設定の出席確認を実施したところ，9/24 の出席確認においては，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，3.0%（10/1），1.25%（10/8），0%（10/15）と減少していった。

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. サイバー攻撃の実態と要因

4-1. 概　要

これまで，ICT 機器を活用した出席確認において，ID・パスワードを学生間で共有するような「なりすまし」発生の可能性が否定できないことを見てきた。こうした「なりすまし」発生の可能性は講義における出席確認に加え，入試における対応においても範囲を日本全国，しいては世界各国に拡大するにあたっては何らかの対策を講じていく必要がある。

一方，セキュリティの観点からサイバー攻撃の実態とその要因についての考察を行う。

コロナ禍によるリモートワークやオンライン授業の影響でフィッシングによるパスワードの流出やランサムウェアによる機密情報の漏洩が急増している。大学キャンパスのネットワークをターゲットにしたサイバー攻撃は全体の 60% を超え，海外の例では身代金約 5,000 万円を支払った例も報告されている。巧妙なリアルタイムフィッシングにより，TOTP（Time-based One Time Password）であってもパスワードの流出は一定数不可避であり，解決法の一つはパスワードを使わないパスワードレスの環境を構築することである。大手 IT 企業の研究によればアイデンティティ（パスワード等）を狙った攻撃は多要素認証を導入することで 90% 以上防ぐことができるという[(7)]。また高いセキュリティは利便性を損なうのが通常であるが，多要素認証をパスワードレス認証とすることで高いセキュリティと利便性の両方を実現することができる。ここではサイバー攻撃の実態と被害の要因，FIDO 2 標準を使った，パスワードレス・キャンパスネットワークによるセキュリティについて論じる。

4-2. サイバー攻撃の実態

コロナ禍によりテレワークやオンライン授業が急増し，インターネットを介したコンピューターの利用が通常になりつつある。これに伴ってサイバー攻撃も急増しており，2020 年度は前年比約 2.3 倍になった（表 1）。VPN（Virtual Private Network）を利用した外部からのネットワークアクセスや組織の中での利用は安全という「境界型」のセキュリティ対策では防御できず，VPN や組織内に居ても外

表 1　サイバー攻撃の推移

年　度	2016	2017	2018	2019	2020
報告件数	15,954	18,141	16,398	20,147	46,942

出典）JPCERT/CC, インシデント報告対応レポート 2021 年 1 月 1 日～2021 年 3 月 31 日

（7）ZDNet（https://www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/）

部にいるのと同様のセキュリティ対策が必要になってきている（ゼロトラスト）。

また 2020 年 11 月に Crowdstrike 社が発表したデータによると世界の 56％の組織が過去 12 カ月にランサムウェアによる被害を受けたという（図 4）。

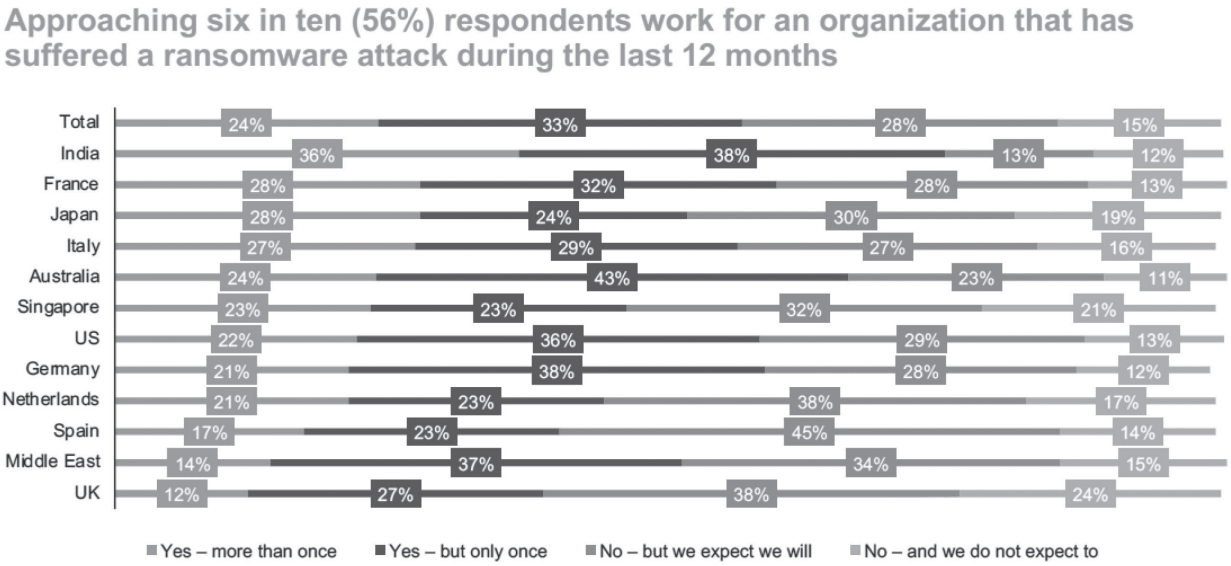

図 4　主要国におけるランサムウェア攻撃の実態

出典）　Crowdstrike 社

同社の 2020 CrowdStrike Global Security Attitude Survey によると日本の組織の 52％が過去 12 カ月以内にランサムウェアの攻撃を受けているほか，ランサムウェアの被害に遭った日本企業の 32％が身代金の支払いに応じているという。またその平均額は 117 万ドル（約 1 億 2,300 万円）にのぼる[(8)]。これらはメディアで紹介されることがほとんどないがインシデントの性格上，公開すると組織自らのブランドを傷つける可能性があるからと考えられる。

最近では攻撃の対象が対策を行っている大企業から身代金を払わざるを得ない中小の組織である地方自治体，ライフライン，インフラ，NGO，そして教育機関にシフトしてきている。世界的なニュースとなった米国で最大の精製石油製品のパイプラインシステムであるコロニアルパイプラインの事件は攻撃対象の変化を代表しており，同社は解決金約 5 億円を払った。図 5 に 2021 年 8 月 13 日～9 月 12 日に攻撃されたデバイス数の業界別割合を示す。教育機関が全体の 63％で他業界とは違う次元で攻撃を受けていることがわかる。

大学に対するセキュリティ・インシデントも枚挙にいとまがないが，規模的にインパクトがあり，ランサムウェア対応において金額含め他大学対応の規範となった事例として，各大学のホームページで公開されている，個人情報の漏洩だけでなくスパムメールの配信や身代金の支払いなど二次被害が起きた大規模な事例を以下に掲げる[(9)]。

（8）　CrowdStrike,（2020）, 2020 CrowdStrike Global Security Attitude Survey

（9）　杉本理，仰木裕嗣，（2021），FIDO 2 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とその応用，教育システム情報学会 2021 年度全国大会。

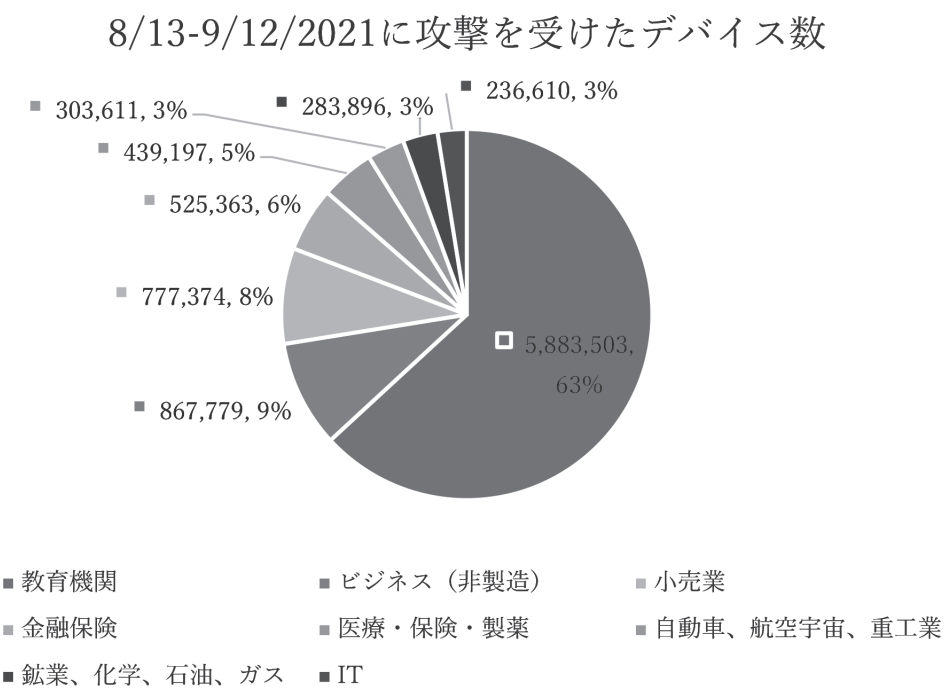

図 5　2021 年 8 月 13 日～9 月 12 日に攻撃されたデバイス数
出典）　マイクロソフト社データより筆者作成

(1)　A 大学の例

2019 年 7 月，お茶の水女子大学は所属教員 1 名のメールアカウントが何者かの不正アクセスを受け，ID・パスワードが盗まれたことでアカウントが乗っ取られた。犯人は奪ったメールアカウントを利用し，合計 2,215 件のスパムメールを送信。さらにメールボックス内を閲覧されたことで教職員 62 件，学生 88 件，学外者 77 件の氏名・所属・メールアドレス・電話番号などの機密情報が漏洩した。

(2)　B 大学の例

2020 年 9 月湘南藤沢キャンパスの情報ネットワークシステム及び授業支援システム（SFC-SFS）において，何らかの方法でシステムの利用者 19 名（教職員）の ID 及びパスワードが窃取され，それを用いた外部からの不正アクセスと授業支援システムの脆弱性をついた攻撃により，同システムから利用者の個人情報が漏洩した可能性があることが判明した。これにより学生情報 5,088 件，同顔写真 18,636 件，単位取得情報 4,493 件，教員情報 2,276 件などが漏洩し，学術機関における被害としては過去最大規模となった。

(3)　C 大学の例

同大学の情報科学研究センターによると 2019 年 2 月に学生のメールアカウントが 19 件乗っ取られ，踏み台となったため 9,800 通以上の迷惑メールが送信された他，2019 年 6 月「教室コントロールシステム」に対する不正アクセスによって登録している利用者情報が外部に漏洩した。

(4)　D 大学の例

2020 年 7 月サーバー上の約 0.02％のデータが漏洩したが，その後学生の機密情報がブラックマーケッ

トに晒されたことで解決金約 5,000 万円を支払った。

日本の大学では漏洩した学生の個人情報など機密情報を「人質」に金銭を要求された例は報告されていないが，一旦機密情報が漏洩すれば後日身代金を要求される可能性があり対策が急務である。

4–3. 被害の要因

被害の要因となっている背景には次の 2 点がある。一つ目に「管理しなければならないパスワードが多い」ことがあげられる。城西大学の場合は筆者の立場であっても，以下の 11 個以上のパスワードを管理する必要があり，当然違うパスワードと予測されない複雑さ，定期的な変更が求められている。

・Wi-Fi，共有 PC，Web 財務，JUNavi（Campusmate），WebClass，Cypochi（CMS），給与明細システム，DataBrain，VPN，図書館システム，科研費，各種学会

尚，大きな被害を被った慶應大学でも 7 つ以上のパスワードを管理している。

もう一つが，「パスワードの使いまわし」である。IPA（独立行政法人 情報処理推進機構）の 2019 年度情報セキュリティの脅威に対する意識調査によるとパソコン利用者の 38.1％が 6 個以上のアカウントを保有しており，49.8％が使いまわしをしているという。また，スマートデバイス利用者の 31.8％が 6 個以上のアカウントを保有しており，58.5％が使いまわしをしている。このように，ネット利用者の約半数が「パスワードの使いまわし」をしており，特にリスト攻撃や辞書攻撃の対象になりやすい環境にあることがわかる。

4–4. 対　策

大学のような研究機関は金銭的・人的リソースが限られている。このような組織にふさわしいベストプラクティスの一つに多要素認証がある。多要素認証とは①Something You Know（知識：パスワード，PIN，画像など），②Something You Have（所持：トークン，スマートカード，USB トークンなど），③Something You Are（生体：生物学的な特徴，行動特性，指紋，顔など）の中から 2 つを組み合わせて認証を行う仕組みである。特に①のパスワードを使わない多要素認証をパスワードレス認証と呼び，WebAuthn/FIDO 2 標準として世界的に認知されている。

城西大学では FIDO 2 標準に準拠したセキュリティキーを「身分証」の形で実現し，FIDO 2 サーバーと出席管理システムを統合した，JAMS（Josai Attendance Management System）を開発した。

5. JAMS システムの検証状況

今回開発した指紋認証による FIDO 2（Fast Identity Online 2）を利用した JAMS（Josai Attendance Management System）システムの検証状況について報告を行う。

指紋認証による FIDO 2（Fast Identity Online 2）認証とは，図 6 のようにカードまたは USB メモリに学生各個人の指紋を登録し，認証においてはパソコンに接続するカードまたは USB メモリにタッチし，指紋がマッチしたら FIDO 2 サーバーとの間で認証を行うものとなる。

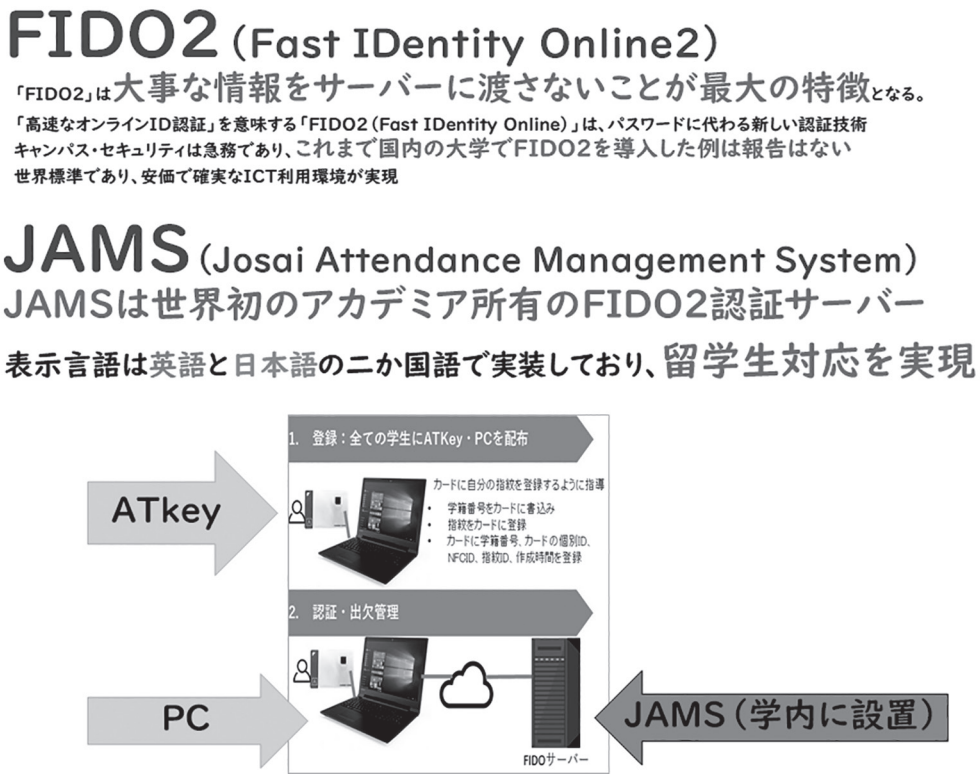

図6　指紋認証による FIDO（Fast Identity Online）認証イメージ(10)

この認証された学生各個人のデータを出席管理として使用するシステムが，JAMS（Josai Attendance Management System）システムとなり，図7にその概略イメージを示す。各学生は事前に指紋を登録したカードまたは USB メモリにタッチしてパソコンと接続させることにより，本システムにログインし，本システムに登録している講義に出席登録を行うこととなる。

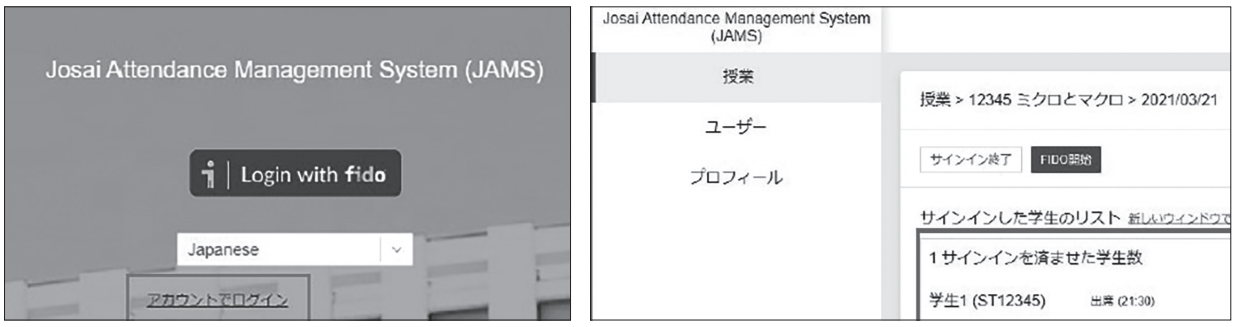

図7　JAMS（Josai Attendance Management System）システムイメージ

ID・パスワードによるログインは前述のように，「なりすまし」の発生を完全に防げるものとはならないが，本システムにおいては指紋は各個人に必ず紐づく為，「なりすまし」発生を防ぐことが可能となる。

(10)　杉本理，栗田るみ子，志田崇「FIDO 標準を利用したパスワードレス認証環境による機密性，可用性の高いデジタルクラスルームの運用実験」，令和 2 年度城西大学研究設備研究報告書，2021 年 3 月 10 日。

① 実証 1　ゼミ及び SPI 試験

本システムによる，実際に出席確認を行った実証データを図 8 に示す。確認方法としてはゼミ（19 名）にて実施し，グラフ左側は教室において，大学側から支給するパソコン（SurFaceGo 2）にて実施したもの，グラフ右側は SPI 試験をオンラインにて各自のパソコンにて実施したものとなる。

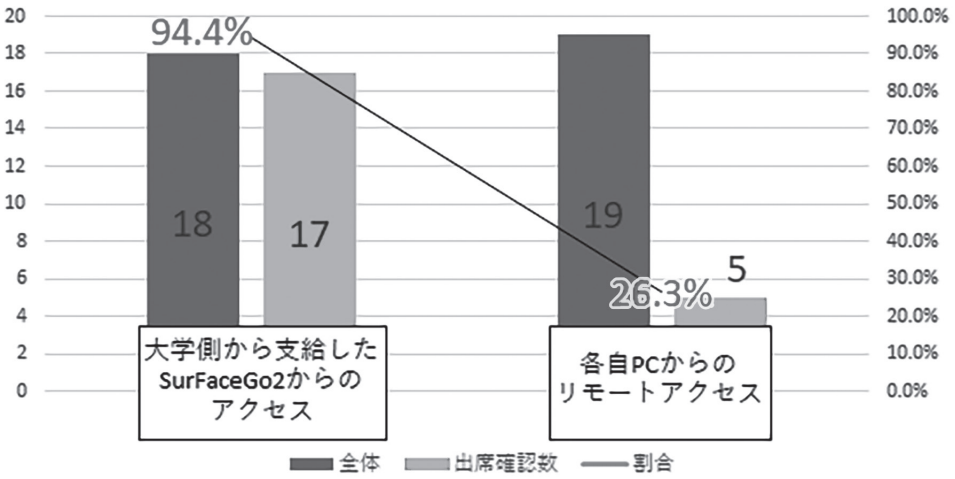

図 8　JAMS（Josai Attendance Management System）システムによる出席確認データ

グラフ左側（大学側支給パソコンにて実施）においては当日の出席者 18 名のうち，17 名が問題なく指紋認証による出席登録がなされ，認識率は 94.4％であった。

一方のグラフ右側（オンライン試験にて各自パソコンにて実施）においては当日出席者 19 名のうち，5 名のみの出席登録となり，認識率は 26.3％であった。この原因として，各自パソコンの OS・ブラウザーのバージョンの問題，各自パソコンにおける共有設定の可能性など，今後原因究明とその対策を進めていきたい。

JAMS を使ったオンライン試験実施手順

1）受験者はそれぞれ各地の自宅から携帯またはタブレットから Zoom で監督者とつながり，カメラと音声を常に ON にして本人確認をする
2）PC では試験システムのみ接続
3）PC に指紋認証にてログインし確実に本人が試験システムに接続
4）受験者は，監督者が指定した ID で試験システムにログインし試験を開始
5）試験終了と同時に終了

② 実証 2　日商 PC 検定への運用

2020 年度は前段階として，城西大学では，日本商工会議所の許可を得て，オンライン検定試験を JAMS は使わない形で，10 月と 2 月の 2 回実施した。

2021 年度は，JAMS を利用したオンライン検定の実験を行い，実用化を目指す予定である。以下，2020 年度に行ったオンライン検定の状況を示す。

受験者は長野県，栃木県，静岡県，群馬県，埼玉県，大学 PC 室から参加し，合計 37 名の学生が受験しトラブルなく終了することができた。試験結果は 100％の合格率であった。

この実績から日本商工会議所では城西大学でのオンライン検定の実施の許可を頂くことができた。2021 年度はオンライン検定の実施と共に，JAMS を使った検定試験の実施における実験を積極的に実施し，システムの安定，合理化を検証する。

受験生はこのようなシステムを利活用するにあたり，情報セキュリティに関して，「ソフトウェアの更新」「ウイルス対策ソフトの導入」「パスワードの管理」が重要であるが，JAMS を利用することにより，「パスワードの管理」は不要となる。

2020 年度の実施手順

1） 受験者はそれぞれ各地の自宅から携帯またはタブレットから Zoom で監督者とつながり，カメラと音声を常に ON にして本人確認をする
2） PC では検定試験システムのみ接続
3） 受験者は，監督者が指定した ID で検定試験システムにログインし試験を開始
4） 試験終了と同時に受験者の PC 画面に合否が表示され終了
5） 監督者側の試験システムに受験者リストとその結果表示
6） 終了

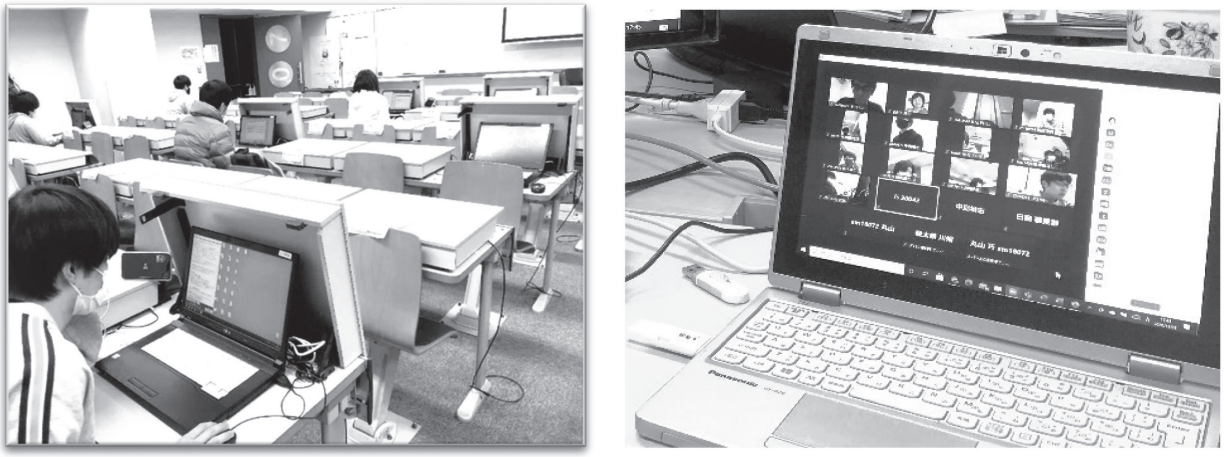

図 9　2020 年度オンライン検定大学 PC 室受験・自宅受験
※携帯電話で個人を映し試験の様子を送信している

以上，見てきたように文部科学省の「GIGA スクール構想」により，１人１台コンピューター端末配備の環境が確立されていく中，オンラインにおける試験は拡大していくものと思われる。こうしたオンライン試験，特に学生がリモートにより自宅から受験を実施するにあたっては，「不正防止対策」が重要になってくる。

こうした「不正防止対策」の観点においては，現状の ID・パスワード設定だけでは，いわゆる「なりすまし」の可能性もあり，今回検証した指紋認証による FIDO 2（Fast Identity Online 2）を利用した JAMS（Josai Attendance Management System）システム確立が有効である可能性があるものと思われる。

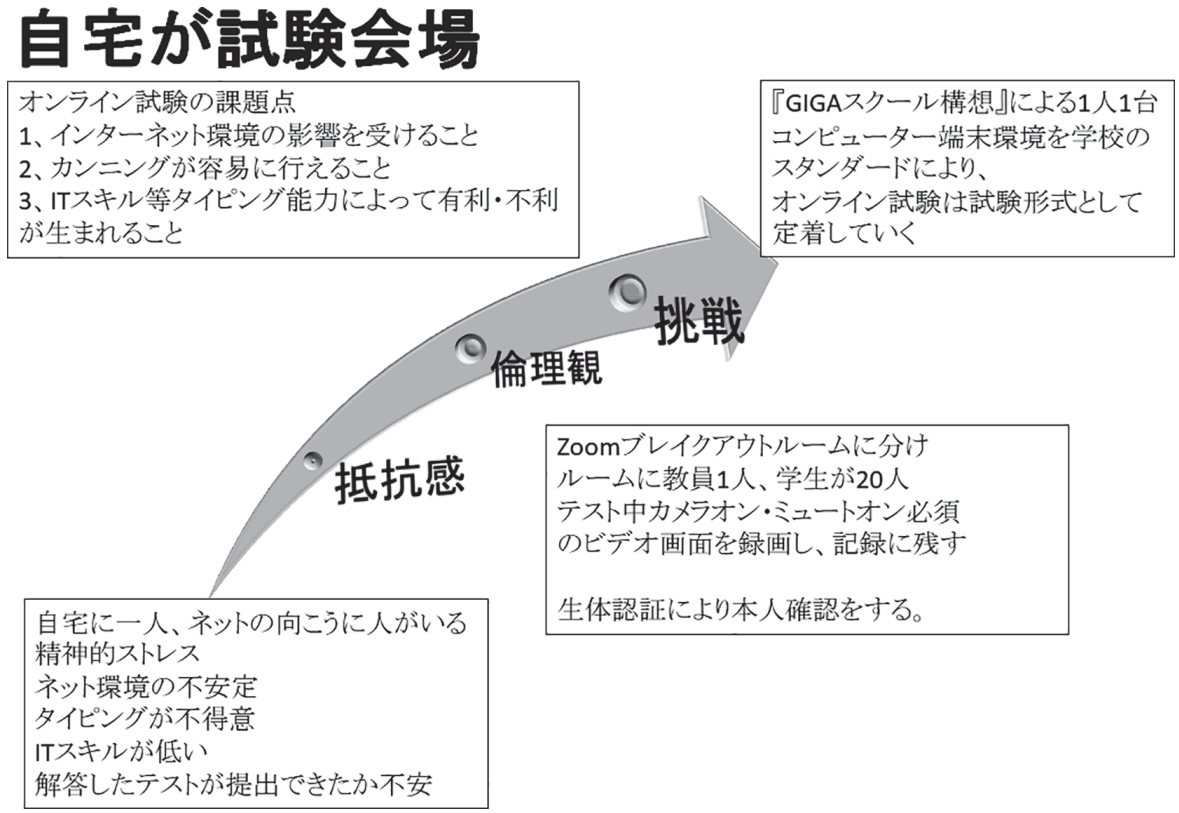

図 10　オンライン入試及び検定受験の成果と課題

6. 総　括

大学において，進化し続ける IT 活用やスキルの育成は使命の一つであるが，変化の激しい IT 機器を利用したシステムの安定運用は苦慮するところが現実である。我々は JAMS（指紋認証システム）の運用を試みつつ安定的に運用することにより，オンラインの場の提供を進め，オンライン教育の拡大を検討する。

また，コロナ禍により，感染対策の面から社会のデジタル化・オンライン化が急速に進んでおり，教育現場においても，資格試験団体や中学・高校・大学など，その動きは拡大している。こうした動きは現在のコロナ禍での一過性のものではなく，「遠方居住者（海外含む）の移動を伴わない受験機会確保」や「交通費・宿泊費等の経済的負担の軽減」など受験生にとってのメリットがあることから，オンライン試験の活用は今後の入学志願者拡大に向けた大学としての重点取り組み事項の一つになる可能性があると考えられる。

一方，「不正防止対策」という点では，今回の講義での出席データによる ID 重複者分析の結果，いわゆる「なりすまし」の発生の可能性も確認され，今後更なる対策が必要になってくると思われる。こうした中，「なりすまし」による不正防止として，指紋認証による FIDO 2（Fast Identity Online 2）を利用した JAMS（Josai Attendance Management System）システムの可能性について考察してきた。

本システムにおいては，事前に設定した大学支給のパソコンにおいては高い認識率を達成しているものの，各自のパソコンでの実施においては，OS・ブラウザー，共有設定等の個別条件に影響するものと思われる認識エラーが現状見受けられ，今後その原因究明と改善策の実施が必要であることが確認さ

れた。

今回の検証結果を踏まえ，更に実証確認を進め，オンライン講義・試験での不正防止対策に活用できるシステム構築を進めていきたい。

参考文献

赤堀侃司他，(2021)，GIGA スクールで実現する新しい学び，東京書籍，2021. 1

川又泰介他，(2017)，e-Testing における不正防止のための顔認証と筆記認証の精度分析，FIT 2017 情報科学技術フォーラム，pp. 471-472

月刊先端教育 2021 年 6 月号，(2021)，学校法人先端教育機構　2021. 5

時通信ドットコム，(2021)，時事通信社 jiji.com，2021. 7. 30 access

杉本理・栗田るみ子・志田崇，(2019)，FIDO 2 標準を利用したパスワードレス認証環境による機密性可用性の高いデジタルクラスルームの運用実験，2019 年城西大学研究設備研究報告書

杉本理，仰木裕嗣，(2021)，FIDO 2 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とその応用，教育システム情報学会 2021 年度全国大会

始まったオンライン入試，(2021)，週刊東洋経済，29 号

文部科学省，(2021)，大学入試のあり方に関する検討会議（第 26 回） 2021. 5. 24 資料

文部科学省，(2021)，「令和 4 年度大学入学者選抜実施要項」 2021. 6. 4

CrowdStrike，(2020)，2020 CrowdStrike Global Security Attitude Survey

IPA（独立行政法人　情報処理推進機構），(2020)，2019 年度情報セキュリティの脅威に対する意識調査。

JPCERT/CC，(2021)。インシデント報告対応レポート　2021 年 1 月 1 日～2021 年 3 月 31 日

Microsoft，(2021)，Microsoft Security Intelligence

Examination of Fraud Prevention Possibility by Online Authentication Using Fingerprint Recognition System Named JAMS (Josai Attendance Management System)

Takashi SHIDA・Rumiko KURITA・Osamu SUGIMOTO

Abstract

Due to the corona epidemic in 2020, the digitization and onlineization of society has been rapidly progressing from the aspect of infection control. The Ministry of Education, Culture, Sports, Science and Technology has decided to purchase learning terminals for each child and student in all courses of compulsory education by 2023 as the 'Global and Innovation Gateway for All'. This aims to promote the realization of a new style school with an environment for high-speed, large-capacity communication networks.

In addition, as indicated by the Ministry of Education, Culture, Sports, Science and Technology's "Guidelines of the Selection of University Admissions for the 4th year of Reiwa (announced on June 4, 2021), universities are required to utilize ICT for their entrance examination, from the perspective of preventing the spread of new coronavirus infections.

Under such circumstances, the research teams of Osamu Sugimoto, Rumiko Kurita, and Takeshi Shida of Josai University planned a project to build a learning environment for digitization and onlineization, and obtained the subsidies for research equipment maintenance costs, etc. Using this subsidy, a server was set up on campus, and complete the world's first academia-owned FIDO 2 (Fast Identity Online 2) authentication server.

The research team has built an operation system for digital class rooms with high possibility of confidentiality by password authentication environment using FIDO 2 (Fast Identity Online 2) standard, and named it JAMS (Josai Attendance Management System). This paper describes the examination of possibility preventing fraud caused by spoof on online, with utilizing JAMS.

Keywords: online authentication, spoof, prevention of fraud, FIDO 2, Passwordless