FIDO2 サーバーの実装とキャンパス ID 型セキュリティキーによるパスワードレス・ネットワークの構築

杉本　理 [1)], 仰木 裕嗣 [2)]

1) 城西大学経営学部
2) 慶應義塾大学大学院政策・メディア研究科

sam@josai.ac.jp

Implementation of FIDO2 Server and Passwordless Network Using Campus ID Type Security key

Osamu Sugimoto [1)], Yuji Ohgi [2)]

1) Department of Management, Josai University
2) Graduate School of Media and Governance, Keio University

概要

本研究はキャンパス・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、パスワードレス・キャンパスネットワークの構築とそれに欠かせない FIDO2 サーバーの実装、そして多要素認証の弱点を補うキャンパス ID 型セキュリティー・キーを用いた出席管理システムの開発について報告する。また本プラットフォームを用いた他の学術的アプリケーションへの応用についても提案する。

1　はじめに

コロナ禍によるオンライン授業や BYOD の急増に伴い、セキュリティー・インシデントの報告件数も急増しており、2020 年度（2020 年 4 月 1 日～2021 年 3 月 31 日）は 2019 年度の約 2.3 倍になった（表 1）[1]。

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

表 1：年度別セキュリティーインシデント数

直近の 2021 年度第一四半期（2021 年 4 月 1 日～6 月 30 日）におけるセキュリティー・インシデントの内訳はフィッシングに分類されるインシデントが 69.4%、スキャンに分類される、システムの弱点を探索するインシデントが 19.9%を占めており、フィッシングを防ぐことができるソリューションが必須となってきている[2]。最近の巧妙なリアルタイム・フィッシングにおいては TOTP などは実際にパスワードをフィッシングサイトに入力してしまうことから役に立たない。また、サイバー攻撃の対象も変化してきており、最近では攻撃の対象が大手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、インフラや教育機関にシフトしてきており攻撃を受けたデバイス数の約 63%が教育機関所有である（図 1）。一方で Microsoft 社や Google 社の研究で多要素認証を導入することで 95%以上のフィッシング攻撃を防御できるという報告がある[3]。さらにランサムウェアによる被害も看過できない。海外の大学では身代金約 5,000 万円を支払って解決した例があるが、ランサムウェアへの感染はフィッシングによるパスワード等アイデンティティ情報の漏洩からメール等によってランサムウェアが配布されていると言われている。

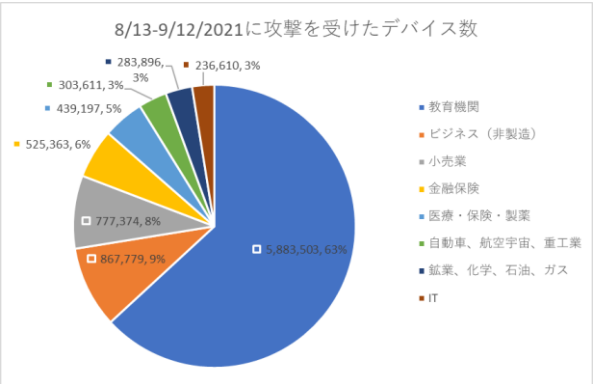

図 1：最近の攻撃対象

2　大学へのサイバー攻撃とその要因

2.1 大学へのサイバー攻撃事例

（1） お茶の水女子大学の例

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） 慶應義塾大学の例

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およ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 およ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） 城西大学の例

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） ユタ大学の例

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る。民間の例では日本においても被害にあった 32%が身代金の支払いに応じており，その金額は平均で約 1 億 2300 万円にのぼる[4]。

2.2 被害の要因

被害の要因となっている背景には次の 3 点がある。

(1)　管理しなければならないパスワードが多い

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。

WiFi 、 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

大きな被害を被った慶應義塾大学でも 7 つ以上のパスワードを管理しているとのことだ。

(2)　パスワードの使いまわしをしている

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以下の様なことがわかっている[5]。

- パソコン利用者の 38.1%が 6 個以上のアカウントを保有いる
- パソコン利用者の 49.8%が使いまわしをしている
- 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いる
- スマートデバイス利用者の 58.5%が使いまわしをしている

したがって，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。

(3)　大学特有の事情

大学では特に学生のユーザ ID 及びメールアドレスをあるパターン化した法則によって割り当てていることが多く、推測によって大量に有効なメールアドレスが生成可能である。また、学生間でユーザ ID やパスワードを共有し、授業の代理出席を行うなど問題意識が低い。プライベートな通信は SNS などで済ませるため、大学のメールを友人と共有してもプライバシー侵害にならないとの考え方があるようだ[6]。

3 多要素認証とパスワードレス

筆頭著者らは人的及び金銭的リソースが限られる大学等教育機関においてフィッシングやランサムウェアから情報資産を守るキャンパス・ネットワーク・セキュリティのベストプラクティスが多要素認証及びパスワードレス認証であるとの仮

定を証明する実証実験を行っており、キャンパス ID 型の FIDO2 セキュリティキーを作成し(図 2)、パスワードを使わないキャンパスネットワークの実装を行った[7]。

図 2：キャンパス ID 型 FIDO2 セキュリティキー（多要素認証の弱点となっていた複数デバイス認証による利便性の棄損をシングルデバイス認証として実現・解決した：所持＋生体）

多要素認証においては以下の 3 つのうちから 2 つを選んで認証を行う。

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）

パスワード＋トークン（ワンタイムパスワード）やパスワード＋スマホ（Authenticator など）が一般的であるが、前述のリアルタイムフィッシングを防ぐことはできない。パスワード漏洩が被害の要因になっていることから②所持＋③生体を組合わせたパスワードレス認証が必要不可欠である。図 2 に示したキャンパス ID は単独のシングルデバイスで所持と生体（指紋）の 2 要素認証を実現しており、従来の 2 要素認証の弱点とされた、スマホやトークンなどの複数デバイスの所持とそれに伴う利便性の棄損を解決するに至った。またキャンパス ID であれば普段持ち歩いているものであり、Extra item として負担になりにくい。さらにキャンパス ID であれば紛失時に届けられることが多く、実際に一人の学生が紛失した時は本人が気づく前に学部事務室に届け出があった。また、自宅などに忘れた場合も仮キャンパス ID の形で貸出すことが可能であり、運用上もあまり負担にならないと考えられる。

城西大学は Microsoft 社との包括契約があることから Azure AD によるパスワードレス認証（FIDO2 認証）が無料で利用でき、教員や学生が図 2 の身分証を使ってパスワードを使わずにキャンパスネットワークと Office などのオンラインアプリにアクセスできる環境の構築に成功した[7]。現在 75 人の学生と 3 人の教員で実験を続けている。一方で Microsoft 社との包括契約がない例えば慶応義塾大学湘南藤沢キャンパスでは利用できない。一般化のためには先行研究でも考察されているように FIDO2 認証サーバーを独自に実装し、パスワードレス認証の環境を構築する必要がある[6]。本研究ではキャンパス・ネットワーク・セキュリティのベストプラクティスの一般化ソリューションとして FIDO2 認証サーバーを独自に実装し、すべての教育機関が享受できるパスワードレス・キャンパスネットワークの一般化ソリューションを実装した。

4 FIDO2 サーバーの実装と応用

城西大学ではキャンパス・ネットワーク・セキュリティのベストプラクティスの一般化ソリューションとして FIDO2 認証サーバーを独自に実装し、さらに RP として出席管理システムを実装することで「なりすましができない」というパスワードレス認証の特徴を生かしたプラットフォーム、Josai Attendance Management System (JAMS)を開発した。

図 2 のキャンパス ID 型 FIDO2 セキュリティキーは指紋認証型であることから学生が友人と共有することはできない。ただし、学生が自身で指紋の登録ができないようにセキュリティキーベンダーである、Authentrend 社と協力してファームウェアを書き換えてある。図 3 に JAMS のログイン画面を示す。

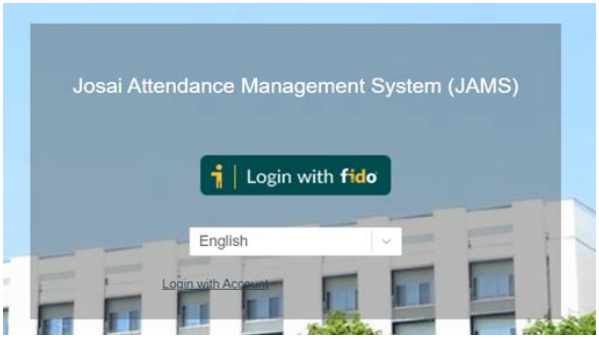

図 3：JAMS のログイン画面

JAMS には 3 つのレベルの権限を用意した。

1. アドミン：キャンパス（学部）、時間割、授業、教員・学生の登録
2. 教員：教員及び学生のセキュリティーキーの登録、授業の詳細登録（遅刻限界時間、受講者など）
3. 学生：自身の受講科目への出席・出席状況の閲覧など

実際の流れは以下の様になる。

1. アドミンは時間割やキャンパスの設定を行い、該当する全学生を登録する
2. 学生は教員のパソコン（もしくはITセンターや学部事務室など）で自身のキャンパスID型FIDO2セキュリティキーに指紋を登録する
3. 教員はキャンパスID型FIDO2セキュリティキーを使って学生を自身の授業に登録する
4. 学生はセキュリティーキーでJAMSにログイン後、当該授業のページにアクセスし、出席処理を行う

言うまでもなくJAMSはFIDO2準拠であり、学生・教員の個人情報や生体情報、パスワードはサーバー上に存在しない。

FIDO2認証サーバーであるJAMSと図2のキャンパスID型セキュリティキーの組み合わせによってパスワードレス認証が実現できると同時に「なりすまし」が一切できなくなる。現在のべ1,000人の学生が出席を入力しているが代理出席はゼロである。この特徴を使って様々な学術的アプリケーションに応用できる。現時点では以下の様なアプリケーションへの応用を検討しており、各部署や外部団体と調整している。

1. 入退室管理：薬学部の薬剤室への入退室管理をデジタル化でき、正確な管理が可能となる
2. 面接入試：リモートで行ってもカメラで本人確認はできるが、さらに生体認証を使って「なりすまし」を防止できる
3. 検定試験：学内で行っている日本商工会議所の検定試験が、カメラとの組み合わせで自身のパソコンや自宅で受験できるようになる

4 結論

本研究ではフィッシングおよびそれが原因で感染するランサムウェアから情報資産を守るキャンパス・ネットワーク・セキュリティのベストプラクティスがパスワードレス認証であることを実証実験によって確かめることができた。そして学生はキャンパスID型FIDO2セキュリティキーを使ってキャンパスネットワークにログインでき、大学提供のアプリが使えること、FIDO2サーバーを実装したJAMSによって学術的アプリケーションの一つである、出席管理システムが利用でき「代理出席」が無くなることがわかった。次の展開としてなりすましができないという特徴を生かした、薬剤室の入退室管理のデジタル化や面接入試、検定試験のオンライン化などに貢献できることが期待できる。

参考文献

[1] 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.

[2] JPCERT/CC インシデント報告対応レポート 2021 年 4 月 1 日 ～ 2021 年 6 月 30 日.

[3] Microsoft. (2021). Most affected industries Reported enterprise malware encounters in the last 30 days.

[4] CrowdStrike : “2020 CrowdStrike Global Security Attitude Survey”, CrowdStrike（2020）

[5] 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

[6] 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. 2019

[7] 杉本理, 仰木裕嗣, FIDO2 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, 2021