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

Implementation of Password-less Campus Network and its Application

杉本　理[*1]，仰木　裕嗣[*2]
Osamu SUGIMOTO[*1], Yuji OHGI[*2]
[*1] 城西大学経営学部
[*1]Department of Management, Josai University
Email: sam@josai.ac.jp
[*2] 慶應義塾大学大学院政策・メディア研究科
[*2]Keio University, Graduate School of Media and Governance

あらまし：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後を絶たず，海外の例では身代金約 5000 万円を支払った例も報告されている．これらの攻撃のほとんどがフィッシングなど標的型攻撃によるパスワードの漏洩に起因する．本論文ではサイバー攻撃の被害実態とその要因、高度なセキュリティと利便性を両立するパスワードレス・キャンパスネットワークの具体的な導入プロセスとその応用について報告する．
キーワード：FIDO2，パスワードレス，セキュリティ，キャンパスネットワーク，フィッシング

1. はじめに

大学キャンパスネットワークの環境では，毎年多くの大学で実施されている「情報セキュリティテスト」によってセキュリティに関するリテラシーが向上していると考えられる一方で，パスワードの管理等アイデンティティに関する意識や責任に対して無頓着な教員が一定数存在していたり、入学から卒業までパスワードを変更しない学生がいることも否定できない．コロナ禍におけるテレワークやオンライン授業によって，セキュリティ・インシデントの報告数は飛躍的に伸びており，従来のセキュリティ対策だけでなく，すべての端末がインターネット上に晒されていると考えなければならない時代がやってきた（ゼロトラスト）．本論文では内外の大学に対するサイバー攻撃による被害の実態とその要因，被害の軽減や防御のための多要素認証（Multi Factor Authentication，以後 MFA）とパスワードレス認証，そしてパスワードレス認証を用いた学術的アプリへの応用について報告する．

2. サイバー攻撃の動向と大学への攻撃

JPCERT/CC によれば，セキュリティ・インシデントの報告件数は 2016 年度以降毎年増加しており，特に 2020 年度（2020 年 4 月～2021 年 3 月）における報告数は 2019 年度の約 2.3 倍になった[(1)]（表 1）．

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

表 1:各年度の報告件数

2020 年度の飛躍的な増加はコロナ禍によるテレワークやオンライン授業（会議）によって多くのコンピュータ端末がインターネット上に晒されることになったことが原因と考えられる。

大学におけるセキュリティ・インシデントも枚挙にいとまがないが，主な事例を以下に掲げる．

（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 5000 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(2)．

また，セキュリティ・インシデントの約 67.5%が巧妙化するフィッシングによるパスワード漏洩に起因する(1)．最近のリアルタイム・フィッシングでは TTOP（Time-Based One Time Password）も役に立たない．以下に述べる MFA そしてパスワードレス認証によるキャンパス・ネットワークの構築が急務と考えられる．

3.　MFA とパスワードレス認証

MFA は以下の 3 つの要素の中から 2 つ以上を選択して認証に利用することを意味する．

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）

このうち②と③を用いて MFA を実現する場合に「パスワードレス認証」と呼ぶ．MFA は高いセキュリティを実現するが利便性を損なう場合が多い。しかしパスワードレス認証では 1 デバイスで MFA を実現でき高いセキュリティと利便性を兼ね揃えた認証システムが構築可能である．城西大学では試験的に図 1 のような身分証を用意し、パスワードレス認証の実証実験を行っている．

図 1　1 デバイスによる MFA（カード：Something you have，指紋（カード右上）：Something you are）

4.　MFA・パスワードレス認証の構築

ほとんどの大学で Microsoft のライセンスを所有していると考えられることから，本章では安価な Office365 ライセンスを所有している場合について簡単に説明する。

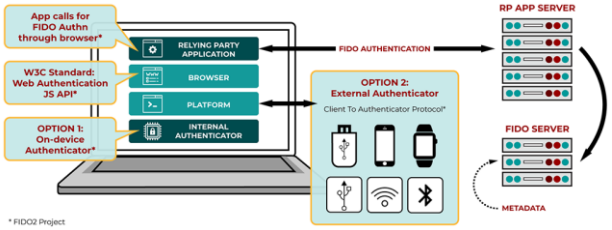
1: Azure Portal において MFA を有効にする．
2: ユーザーを選択
3: セキュリティを選択
4: 認証方法からセキュリティ・キーを選択

画面の指示に従えば例えば図 1 のような FIDO2 標準のセキュリティ・キーを登録できる．これにより，Windows や Mac のログインに対してパスワードレスによる認証が実現できる．

5.　FIDO2 パスワードレス認証の応用

城西大学では学術機関としては世界初となる FIDO2 サーバーを独自に構築し，RP App として出席管理システムをインプリした（Josai Attendance Management System: JAMS）．構成図を以下に示す．

同様の実証実験に興味のある学術機関には FIDO2 サーバーを無償でお貸しすることも可能であることからお声をかけていただきたい．



6.　結論

大学におけるキャンパス・ネットワークにおいては MFA もしくはパスワードレス認証の構築が急務である．学生が安心・安全な環境で学べることは学びの質だけでなく，例えば出席管理をパスワードレス認証によって行うことで代返などのなりすまし防止となり，授業に出るという行動を促すことから退学者防止につながる可能性もある．この課題については現在データを取っているところである．同様のパスワードレス認証の実験を試みたい大学があればご連絡いただきたい．

参考文献

(1) 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”, JPCERT/CC（2021）
(2) CrowdStrike：“2020 CrowdStrike Global Security Attitude Survey”，CrowdStrike（2020）