1D-02

FIDO2 サーバーと身分証型セキュリティー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

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

1. 概要

キャンパスネットワーク・セキュリティにおいては多要素認証の先にあるパスワードレス認証が利便性と安全性を兼ね揃えたベストプラクティスであるという仮定を立て，独自の FIDO2 認証サーバーおよび身分証型セキュリティーキーを実装した．また RP サーバーとして出席管理システムを開発し，FIDO2 サーバーと連携させプラットフォーム化した．本論文では学術機関としては初めてとなる FIDO2 統合型システム（Josai Attendance Management System:JAMS）について報告する．また JAMS を利用したアカデミアへの貢献及び応用可能性についても言及する．

2. はじめに

多要素認証はパスワードに加えて何か別の要素の 2 段階認証であるためパスワードのみによる認証に比べて利便性に劣る．より安全であってもユーザーエクスペリエンスが棄損するためユーザーや顧客に勧めにくく，爆発的に普及が進まない原因とも考えられる．また最近の巧妙なリアルタイムフィッシングにおいてはフィッシングサイトにパスワードを入力してしまうため，ハードウェアトークンなどによる TOTP(Time -Based One Time Password)は役に立たない．

多要素認証の弱点である利便性の低下はパスワードレス認証とすることで解決可能である．城西大学では身分証そのものを FIDO2 セキュリティーキーとして作成し（図 1），利便性をさらに追及したパスワードレス・キャンパスネットワークの構築を行っている．独自に実装した FIDO2 サーバーと RP サーバーとして出席管理システムを開発し，FIDO2 統合型システムである，Josai Attendance Management System（JAMS）として 100 人規模で運用を始めた．本論文では開発の背景や過程及び成果の一部を報告する．

3. FIDO 標準によるパスワードレス認証

FIDO 標準の主な特徴は指紋などの大切な情報をサーバーに渡さないことと生体認証などの様々な認証方式を使えることにある．

インターネットを含む通信経路には公開鍵と署名（本人であることを証明する文字列）のみが送信されどちらも誰に見られても問題ない．秘密鍵はスマートフォンや認証器の TEE や SE 領域などに保管されるため OS やアプリの影響を受けないことも大きなメリットである[1].

4. 身分証型 FIDO2 セキュリティーキー

FIDO2 セキュリティキーは，様々なベンダーから販売されているが，多くの学生や教職員に配布することを前提に以下の様な条件を優先した．

1. 次世代の身分証と代替えできるようにカード型であること
2. NFC/USB/BLE にて認証が可能であること
3. 他人のセキュリティーキーでは認証ができない（なりすましができない）仕様であること

図 1　身分証型 FIDO2 セキュリティキー
（シングルデバイスで多要素認証：所持＋生体を実現）

以上から指紋認証器が装備されていることでシングルデバイスでありながら 2 要素認証が実現でき（所持＋生体），他人のセキュリティーキーでは認証ができない製品（Authentrend 社製 ATKey.Card）を選択した．また，安全性のためとは言え携行品を増やすことは利便性を損ない，さらに紛失や忘れ物につながる．通常持ち歩くことになっている身分証をセキュリティーキーと共通化できるように教職員身分証および学生証風のシールを作り，身分証型 FIDO2 セキュリティキーを作成した（図 1）．セキュリティーキーへの指紋登録は Windows10 環境では「設定」⇒「アカウント」⇒「サインイン・オプション」⇒「セキュリティーキー」から設定できるほか，専用のソフトでも設定が可能である．ただし本研究においては学生の「代理出席防

Implementation of Password-less Campus Network Using Josai FIDO2 Server and Campus ID Type Security Key
†1 OSAMU SUGIMOTO, Josai University
†2 YUJI OHGI, Keio University

止」を目的とした，出席管理システムの開発も目的としているため，Authentrend 社にご協力いただき，学生用のセキュリティーキーにおいては自身で指紋の登録ができないようファームウェアを変更してある．

5. FIDO2 サーバーの実装

FIDO2 は世界標準であり，2019 年に World Web Consortium (W3C)と FIDO アライアンスによって策定され，スペックは公開されている[2]．W3C における標準は Web Authentication (Web Authn)と呼ばれる[3]．FIDO2 サーバーのソースコードも github に公開されており，開発可能である[4]．筆頭著者は W3C において Asia Region Business Development Leader として従事していた経験があり知見があることもこの研究の背景にある．

FIDO2 認証サーバーは所属組織が Microsoft 社との包括契約を結んでいれば Azure AD を無償で利用できることから Azure AD を FIDO2 認証サーバーとして利用可能である．例えば慶應義塾大学 SFC キャンパスでは Microsoft 社との包括契約がなく，一般化ソリューションとして FIDO2 認証サーバーの開発が重要と考えた[5].

FIDO2 認証サーバーと上記の身分証型セキュリティーキーを利用したアプリケーションとして「なりすましができない」という特徴を生かした「出席管理システム」を開発し，統合したプラットフォームである Josai Attendance Management System (JAMS)の運用を始めた．

JAMS では 3 つのレベルの権限を設定した．

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）

3.【学生】: 自身の受講科目への出席・出席状況の閲覧など

6. 運用・認証の手順と仕組み

① JAMS 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．

② 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．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，ユーザー認証を求められる．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 JAMS に送る．そして公開鍵のみが JAMS に登録される

③ 学生は JAMS 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．この時，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．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．なお，これまでのプロセスの際，ネット上に流れるチャレンジや公開鍵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．

④ 担当教員が授業開始ボタンを JAMS 上でクリックし，ユーザー（学生）は，当該授業を選択し，出席していることを登録する．担当教員はこれをもって対象ユーザーの存在を確認・認証し，授業を実行する

7. 結論

本論文ではキャンパスネットワーク・セキュリティにおいては多要素認証の先にあるパスワードレス認証が利便性と安全性を兼ね揃えたベストプラクティスであるという仮定を独自の FIDO2 認証サーバーおよび身分証型セキュリティーキー，アプリケーション・サーバーとしての出席管理システムを開発し運用することで証明した．学術機関としては初めてとなる FIDO2 統合型システム（Josai Attendance Management System）は今後他キャンパスへの展開や他大学へ無償で貸し出すことで実験データを積み重ねていきたい．またオンライン面接入試など厳密な生体認証が必要な他のアプリケーションについてもチャレンジしていく予定である．

参考文献

[1] 五味秀仁，大神渉．FIDO 認証とその技術．電気情報通信学会，2018
[2] “FIDO2: WebAuthn & CTAP”， https://fidoalliance.org/fido2/, (参照 2021-10-01)
[3] “Web Authentication Working Group”, https://www.w3.org/Webauthn/, (参照 2021-10-01)
[4] “StrongKey/FIDO2”, https://github.com/StrongKey/fido2, (参照 2021-10-01).
[5] 杉本理，仰木裕嗣. FIDO2 セキュリティー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，教育情報システム学会, 2021