「Shibboleth IdP V5におけるPasskeysの種別による認証可否の判定」による認証保証レベルの厳格化への第一歩

The First Step Toward Strengthening Authentication Assurance Levels Based on "Authentication determination based on the types of Passkeys in Shibboleth IdP V5"

茨城大学情報戦略機構准教授 野口 宏
Hiroshi Noguchi, Associate Professor, Institution for Information Management and Strategy, Ibaraki University
ORCID ID : https://orcid.org/0009-0000-5496-3070

株式会社 DTS 榊原 勇人
Hayato Sakakibara, DTS Corporation
ORCID ID : https://orcid.org/0009-0001-4362-5348

国立情報学研究所 アーキテクチャ科学研究系助教 清水 さや子
Sayako Shimizu, Assistant Professor, Information Systems Architecture Science Research Division, National Institute of Informatics
ORCID ID : https://orcid.org/ 0009-0002-8469-5833

[紹介論文]
Shibboleth IdP V5 における Passkeys の種別による認証可否の判定
榊原 勇人（株式会社 DTS），清水 さや子（国立情報学研究所），野口 宏（茨城大学）
学術情報処理研究，Vol. 29, No. 1, pp. 130-140, 2025.

1. はじめに

このたびは，論文誌「学術情報処理研究」に掲載された我々の論文 [1] について，機関誌「AXIES Trajectory」において紹介の機会を与えて頂き，関係者の皆様に深く感謝申し上げる．

近年，ID とパスワードによる認証は攻撃の対象となることが多く，その対応策としての多要素認証も広く利用されるようになってきた．しかし，すぐに多要素認証も攻撃の対象となり，根本的な対策として Passkeys が注目を浴びている．Passkeys は公開鍵暗号方式を採用しており，自身の秘密鍵の所持形態により，Synced Passkeys と Device-bound Passkeys に分けられる．この区別により認証における強度が異なっている．この強度は NIST SP 800-63B-4 [2] において認証保証レベル（AAL: Authentication Assurance Levels）として定められており，前者のレベルは 2（AAL2），後者は 3（AAL3）となっている．このレベルを区別して認可するサイトが増えてくると思われるため，紹介論文は，認証を行う IdP（Identity Provider）においてそれらを区別できるような仕組みが必要と考え，実装したことを報告したものである．

2. 紹介論文の目的

認証，認可，認証フェデレーションを行うシステムとして，日本の学術界では Shibboleth が広く利用されている．国立情報学研究所（NII）が全国の高等教育機関を取りまとめている認証連携基盤である「学認」では認証情報の交換のために SAML（Security Assertion Markup Language）を採用し，SAML を利用するためのミドルウェアとして Shibboleth を利用している．学認への参加機関が多いことも，Shibboleth が広く利用されている理由と考えられる．Shibboleth 環境下のシステムにおいては，ID 情報を保持し，それら ID に対する認証を行う IdP と，認証された ID に対してサービスを認可・提供する SP（Service Provider）に分けてサービスが利用できるようになっている．更に，複数のサービスが IdP に認証機能を委ねる認証フェデレーションの環境を構築することが可能となっている．認証を行う Shibboleth IdP での Passkeys の対応は，2024 年 12 月に提供が始まった Shibboleth IdP V5 のプラグイン WebAuthn version1.0.0 [3] において行われたばかりであり，Passkeys の機能を部分的に可能とするものである．そのため，Passkeys の区分による認証強度の違いまで区別できておらず，フル実装までの課題は多い．

しかし，NIST SP 800-63B において AAL が定めら

れ，指定された AAL によって認可を決める SP が遠くない将来に数多く出てくることが予想される．その場合は，IdP 側で AAL に従った認証を行う必要がある．そこで，紹介論文では，IdP 側で認証強度に従った認証が可能となるよう Passkeys の区分による認証の区別を行えるようにした．つまり，AAL2 を指定されていれば Synced Passkeys で，AAL3 を指定されていれば Device-bound Passkeys で認証するよう Shibboleth IdP V5 のプラグイン WebAuthn の改良を行い，更に，改良を行った際の現行の Shibboleth IdP への改良点を示唆することが紹介論文の目的である．

3. 認証保証レベル（AAL）

NIST SP 800-63B では，従来の認証で利用されていた ID とパスワードの組という知識情報は認証における必要最低限のものという観点から認証保証レベルを 1（AAL1）としている．知識情報は狙われやすく，また漏洩してしまうこともあるため，知識情報要素に加えて，所持情報や生体情報という要素を利用して認証を行う多要素認証が普及している．認証保証レベルという観点からは ID とパスワードの組よりも高いものと考えられるため，レベル 2（AAL2）と考える．また，Passkeys は，公開鍵暗号方式を活用し，パスワードを利用しない．秘密鍵をユーザの手元の認証器に置き，公開鍵をサービス提供者側に置いた上で認証を行う．サービス提供者側に置いた鍵は公開鍵であるため，パスワードと異なり漏洩したとしてもそれを利用して認証を成功させることはできない．これらのことから，Passkeys の認証保証レベルはレベル 2 以上と考えられる．Passkeys はユーザ自身が複数の認証器を所有することを想定し複数の認証器で秘密鍵を同期して利用できる Synced Passkeys と，認証器から秘密鍵を取り出すことができない Device-bound Passkeys に分けられる．前者は ID とパスワードの組より認証においての保証レベルが高いためレベル 2 と考えられ，後者は認証器から秘密鍵を取り出すことが出来ないという点で前者よりもレベルの高いレベル 3（AAL3）と考えられる．

学認では次世代認証連携への取り組み [4] を進めており，ID とパスワードの組による認証から一段高い認証基準である AAL2 の運用を進めている．基本方針としては「多要素認証器 1 個またはパスワード認証に所持要素に基づく認証器を組み合わせたもの」という要件を採用している．また，現在 AAL2 の認証に利用できる認証器を登録した学認認証器レジストリを構築し，順次更新すると共に公開している [5]．AAL2 と AAL3 は特に区別はしていないが，AAL3 となる Device-bound Passkeys を利用するためには耐タンパ性を持ったハードウェアトークンの利用や，Windows Hello のように TPM2.0 を利用する必要があるため，いずれのレベルかは容易に弁別できる．

現時点では AAL2 と AAL3 を区別している事例は少ないが，今後多くの SP においてレベル区別の需要が出てくると予想できる．そのため，まずは IdP において AAL2 と AAL3 を区別した認証可否の判定ができることが必要となる．

4. 認証の可否

Passkeys を利用した際に認証保証レベルに対応しようとする場合，認証器がいずれのレベルに対応したものか，つまりいずれの Passkeys に対応したものかを知る必要がある．全ての認証器には AAGUID（Authenticator Attestation Global Unique IDentifier）が割り当てられており，これをキーとして基本的には図 1 のように，個々の認証器に関するメタデータが Passkeys Developer から提供されている aaguid.json [6] に登録されている．紹介論文では，これを利用し認証器がいずれに対応しているかを判断している．なお，FIDO Alliance から提供されているメタデータサービス（MDS）は提供されているメタデータが少ないため，aaguid.json を利用した．

Shibboleth IdP 上での認証は，図 2 に示した通り，通常の FIDO 認証に加えて認証器から得られた情報を Web ブラウザ経由で Shibboleth IdP に提供（フロー 10 ～ 11）し，それを受けた Shibboleth IdP では AAGUID を取得，aaguid.json から Passkeys の種別を取得した後に認証等による検証を行なう（フロー 12

```
1:"ea9b8d66-4d01-1d21-3ce4-b6b48cb575d4": {
2:  "name": "Google Password Manager",
3:  "icon_dark": "data:image/svg+xml;
      base64,PHN2ZyB4bWxucz0iaHR0cDov...",
4:  "icon_light": "data:image/svg+xml;
       base64,PHN2ZyB4bWxucz0iaHR0cDov...",
5:  "type": "synced"
6:}
```

図 1　認証器のメタデータの例

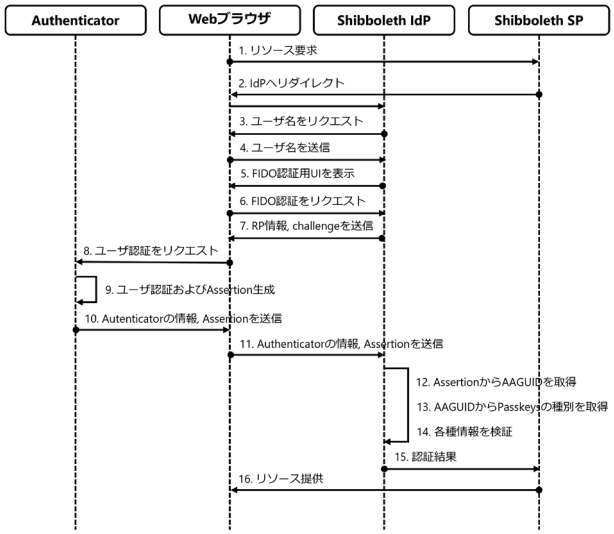

図 2　認証フロー

～ 14）ことにより認証保証レベルへの対応を確認している．

5. 実装

実行環境を構築するにあたり，動作の軽量かつ高速性および再生成が容易であることから Docker コンテナを利用した．システム構成は図 3 に示した通りであり，閉じた環境下で実行が可能なようにまずはリバースプロキシを用意し，加えて Shibboleth IdP, LDAP, Shibboleth SP をコンテナとして用意した．これらのコンテナは，全て同一の Docker Network に属している．また，実行するにあたっては，表 1 に示した 5 つの認証器を利用して検証を行っている．

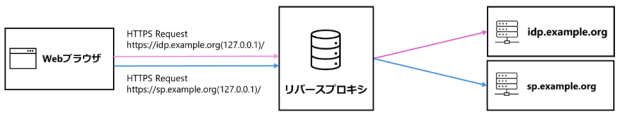

図 3　検証用システム構成

表 1　使用した認証器

Name	Provider	Key Type
YubiKey 5C	Yubiko	Device-bound
Titan Security Key	Google	Device-bound
Windows Hello	Mcrosoft	Device-bound
Google Password Manager	Google	Synced
Proton Pass	Proton	Synced

以上の環境を実現し，認証強度レベルに従った認証を行うことの実証を行なった．加えて，Shibboleth IdP への Passkeys の登録の際も認証強度レベルを意識できるものとしており，利用者にとって分かりやすく認証強度レベルにあった認証が可能となっている．

6. おわりに

紹介論文により認証強度レベルに合った認証が可能となったが，Shibboleth IdP にとどまった認証である．国立情報学研究所では AAL2 の運用に係る実証実験を行うことを計画 [7] しており，そこでは認可の際に SP から IdP に対して認証強度レベルを要求し，IdP ではそのレベルにあった認証を行うようにすることも計画の一部となっている．このように認証強度レベルに対応した認証フェデレーション環境を構築する必要があると考えている．また，認証器のメタデータとして，今回は aaguid.json を利用した．登録されていない認証器もあり，必要な場合は各 Shibboleth IdP の管理者に依頼して登録を行う必要がある．しかし，各管理者の負荷と人的な登録ミス等を避ける必要があると考えるため，一箇所で管理を行い，そのデータを共有する仕組みが必要と考える．

本稿で紹介した研究をさらに進めることにより，状況に応じたより安全な認証環境を提供できるようになり，Shibboleth IdP の管理の負荷が少しでも軽減されることを期待する．

2025 年 12 月 22 日

参考文献

[1] 榊原勇人他：Shibboleth IdP V5 における Passkeys の種別による認証可否の判定，学術情報処理研究，Vol.29, No.1，pp.130-140（2025）
[2] NIST: NIST SP 800-63B-4, 2025, https://doi.org/10.6028/NIST.SP.800-63b-4,（閲覧日 2025 年 12 月 15 日）
[3] Shibboleth Atlassian: Identity Provider Plugins/WebAuthn, https://shibboleth.atlassian.net/wiki/spaces/IDPPLUGINS/pages/3395125387/WebAuthn,（閲覧日 2025 年 1 月 27 日）
[4] 国立情報学研究所 学術認証運営員会 次世代認証連携検討作業部会：AAL2 の新学認での運用に当たって（案），https://www.gakunin.jp/document/661，2022 年 6 月 9 日
[5] 学認：学認 AAL2 認証器レジストリ，https://level2.gakunin.jp/，（閲覧日 2025 年 1 月 29 日）
[6] Passkeys Developer: passkeydeveloper/passkey-authenticator-aaguids, https://github.com/passkeydeveloper/passkey-authenticator-aaguids/blob/main/aaguid.json,（閲覧日 2025 年 1 月 27 日）
[7] 国立情報学研究所：次世代認証基盤における IAL2・AAL2

の運用に係る中規模実証実験のご案内，
https://www.gakunin.jp/news/20251208/，（閲覧日 2025 年 12 月 15 日）

【著者略歴】

野口 宏

1986 年中央大学理工学部数学科卒業．1988 年筑波大学大学院経営・政策科学研究科修了．1988 年茨城大学工学部情報工学科助手．2005 年 12 月茨城大学 IT 基盤センター講師．2018 年 4 月茨城大学 IT 基盤センター准教授．2022 年 4 月より茨城大学情報戦略機構准教授．博士（工学）．コンピュータ及びネットワークシステム構成，認証基盤，ID 管理，情報セキュリティなどの教育・研究に従事．情報処理学会，日本データベース学会，各会員

榊原 勇人

2023 年茨城大学工学部情報工学科卒業．2025 年茨城大学大学院理工学研究科博士前記課程修了．2025 年 4 月より株式会社 DTS．認証基盤，ID 管理などの研究に従事．情報処理学会 会員

清水 さや子

2015 年京都大学大学院情報学研究科博士後期課程単位取得退学．2018 年同学位取得．博士（情報学）．立命館大学文学部卒業後，民間企業でシステムエンジニアを経て，2005 年東京海洋大学情報処理センター（現，総合情報基盤センター）技術職員．2011 年同技術専門職員．2021 年より国立情報学研究所助教．認証認可，教育研究 DX 基盤の研究に従事．電子情報通信学会，情報処理学会，各会員