

Modern Authentication

FIDO2 Web Authentication (WebAuthn) を学ぶ

栗原 淳

兵庫県立大学 大学院応用情報科学研究科
株式会社ゼタント

April 29, 2020

はじめに

認証とは

認証

「何らかの手段」で対象の正当性を確認すること。

- メッセージの正当性を確認 ⇒ メッセージ認証
- サービス利用ユーザの正当性を確認 ⇒ ユーザ認証
- etc.

※このスライドで単純に「認証」と呼んだときは、認証対象を「正規ユーザ本人」としたユーザ認証・本人認証を指すこととする。

本人認証の3つの要素

本人認証において、正当性確認のため検証されるものは大きく3要素に分類。

■ 知識

⇒ 本人しか知らない知識を持っていればOK (ex. パスワード)

■ 所有物

⇒ 本人しか持っていない物を提示できればOK (ex. HWキー)

■ 生体

⇒ 本人の体の一部を提示できればOK (ex. 指紋)



本人しか知らない



本人しか持っていない
(複製できない)



本人の体の一部

オンラインサービスでのパスワード認証

- サービスの利用者の識別子 (ID) と対応するパスワードをサービス事業者に登録、サービス利用時に利用者が自分の ID とパスワードを入力する。
- パスワードは個人の記憶にのみ存在するため、**パスワードを知っている人はそのサービスに登録してある本人と同一人物と考えることができる。**

おそらく、誰にとっても最も馴染み深い認証方式！

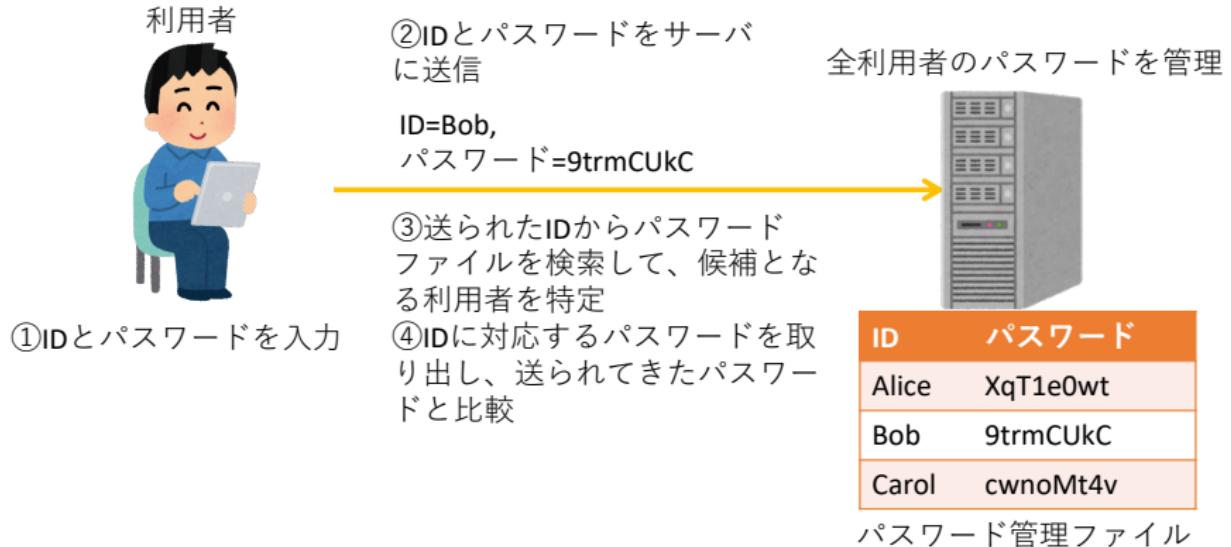


Figure: オンラインでの単純なパスワード認証

オンラインでのパスワード認証の問題

英数字・記号を組み合わせたパスワード:

- 攻撃者にとって比較的予測しやすい¹
- 「強い」 パスワードを使わせるにはユーザ教育が必要²
- 覚えられない
- etc...



予測できず、誰が使っても強力で、確実に認証できる方法が必要
⇒ ハードウェアセキュリティキーを使った認証が人気に
⇒ FIDO はそのような手法の標準化された方式

¹しかもオンラインだと予測→認証トライを繰り返せる

²教育なしだと覚え易く「弱い」ものを利用しがち

FIDO (Fast IDentity Online)

業界団体 FIDO Alliance³ の策定する、ハードウェアセキュリティキー+生体認証⁴をベースとしたオンラインでの本人認証技術。

現在は FIDO2 (v2.0) が最新の規格。以降、FIDO2 の内容について触れていく。

厳密には、FIDO2 はパスワードレス認証をサポートしつつも、パスワード+デバイス・生体認証の多要素での認証もサポートする。

³<https://fidoalliance.org>

⁴すなわち、「所有物」と「生体」の二要素を同時に使った認証が可能。

FIDO 認証概略

FIDO 認証の特徴:

- 公開鍵暗号を利用した、オンラインでの認証方式の提供
- 認証器によるローカルでの本人認証
- 認証器内部に閉じた署名生成
⇒ 秘密鍵・パスワード等の秘密情報は外部に出ない

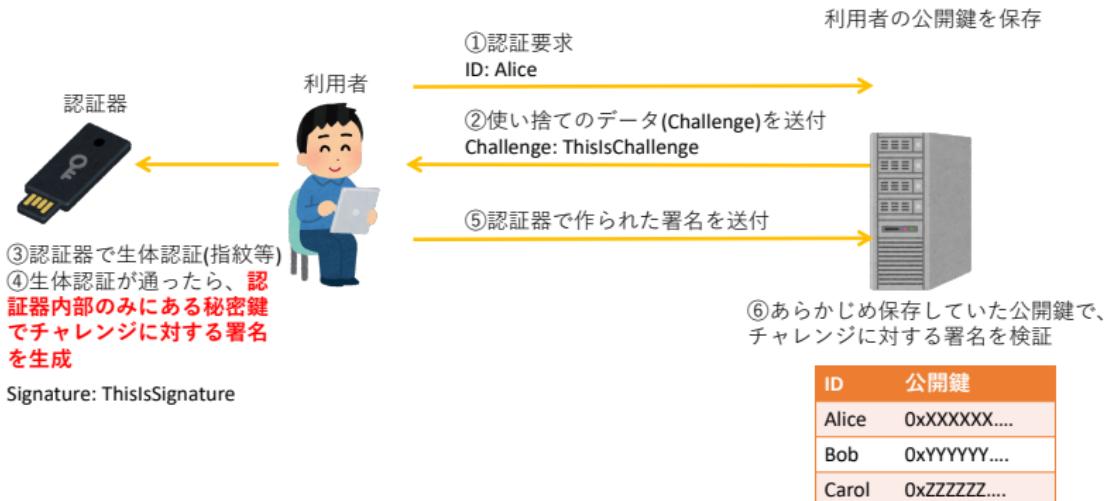
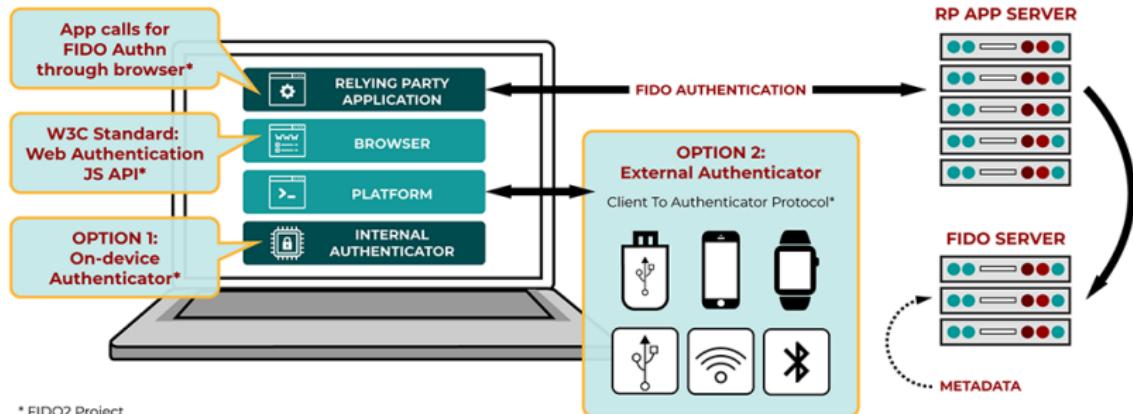


Figure: FIDO 認証概略

FIDO2 の要素

FIDO2 は、WebAuthn (Web Authentication)⁵と、CTAP
(Client-to-Authenticator Protocol)⁶の 2つの要素で構成される。



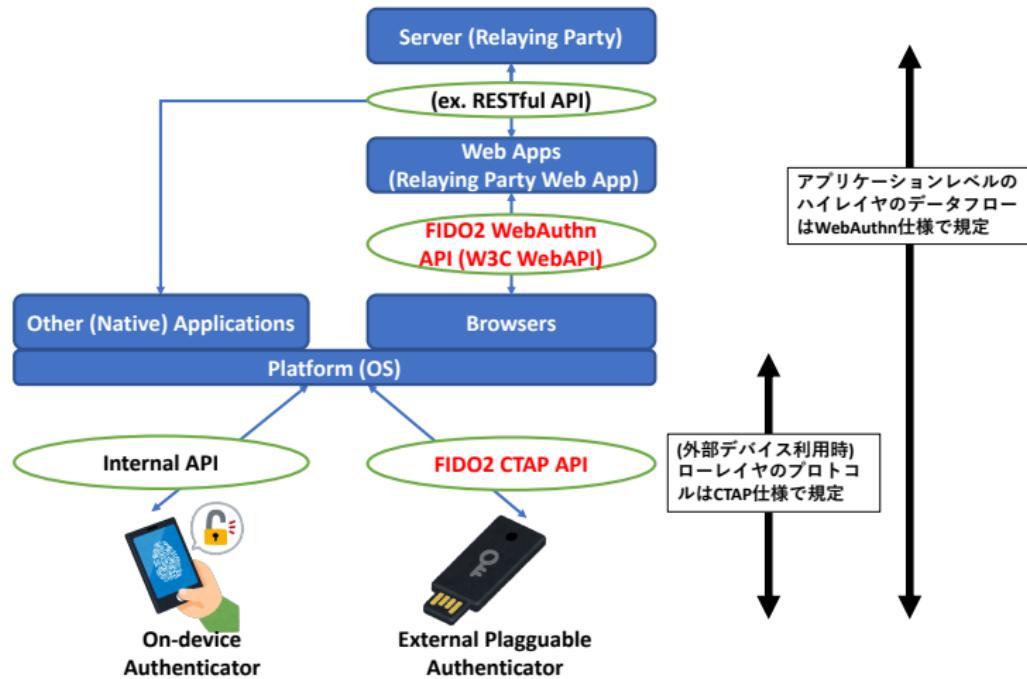
* FIDO2 Project

Figure: ©FIDO Alliance, from <https://fidoalliance.org/specifications/>

⁵Spec: <https://www.w3.org/TR/webauthn-1/>

⁶Spec: <https://fidoalliance.org/specs/fido2/fido-client-to-authenticator-protocol-v2.1-rd-20191217.html>

- **WebAuthn**: WebAPI と、(端末付属 or 外部の) 認証器・WebApp・サーバ間のハイレイヤのデータフローを規定。
- **CTAP**: ブラウザ・ネイティブ App と外部デバイスの認証器間のローレイヤのプロトコルと API を規定。



FIDO2 WebAuthn

FIDO2 CTAP

補足: FIDO1

FIDO1 (v1.x) は、以下の 2 つの要素で構成されている。

- UAF (Universal Authentication Framework): 生体認証機能を持つ FIDO 対応端末 (スマートフォン等) でパスワードレス認証を行う機構。USB 接続などの外部 HW セキュリティキーは利用できない。
- U2F (Universal 2nd Factor)⁷: ID・パスワード認証に加えた 2 要素認証を行うのに、外部 HW セキュリティキーを利用可能とする機構。

FIDO2 は、UAF と U2F を統合し、さらに外部 HW キーを用いてもパスワードレス認証可能な、より利便性の高い規格と見做せる。

⁷U2F は FIDO2 規格では CTAP1 と改称。FIDO2 で追加された仕様は CTAP2 と呼ばれる。

FIDO2 対応デバイス

Security Key by Yubico



FIDO2 専用⁸のデバイス

⁸FIDO2 CTAP1=FIDO1 U2F には対応

FIDO2 標準化状況

FIDO は業界団体の策定した規格ではあるが、

- FIDO2 CTAP: ITU-T で勧告として国際標準化⁹
- FIDO2 WebAuthn: W3C で勧告として国際標準化¹⁰

と、認証器とブラウザ間の通信プロトコル、ハイレイヤの認証プロトコルの両者共に国際標準として策定済。

⁹<https://fidoalliance.org/>

fido-alliance-specifications-now-adopted-as-itu-international-standards/

¹⁰<https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.ja>

この後、FIDO2 WebAuthn の内容に実際に触れ、最新の認証技術について理解を深めてみよう。¹¹

¹¹ 今回は Web 技術から学ぶセキュリティに注力するため、ローレイヤの FIDO2 CTAP については別の機会で。

FIDO2 WebAuthn の構造

FIDO2 WebAuthn の中身を解析

まとめ

