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

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、<u>認証対象を「正</u> 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!

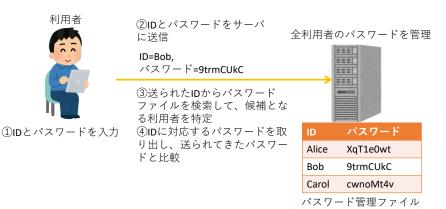


Figure: オンラインでの単純なパスワード認証

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は、

- 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

 $^{^1}$ 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)

FIDO

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+牛体認証⁴ をベースとしたオンラインでの本人認証技術。

³https://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。

FIDO1からFIDO2へ

- FID2 CTAP: ITU-T で勧告として国際標準化
- FIDO2 WebAuthnP: W3C で勧告として国際標準化5

⁵https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.ja

FIDO2 デバイス

Security Key by Yubico



FIDO2 webauthn/U2F 専用のデバイス

FIDO2 標準化状況