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

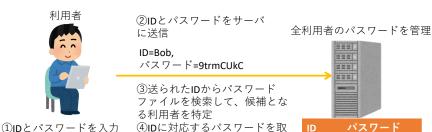
「何らかの手段」で対象の正当性を確認すること。

- 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。

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!



り出し、送られてきたパスワー

ドと比較

cwnoMt4v パスワード管理ファイル

XqT1e0wt

9trmCUkC

Alice

Bob

Carol

Figure: 単純なパスワード認証

パスワード認証の危うさ

FIDO (Fast IDentity Online)

FIDO

業界団体 FIDO Alliance¹ の策定する、生体認証をベースとしたオンライン認証技術。

¹https://fidoalliance.org

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2

²https://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