AXIES認証基盤部会・学認合同企画セッション

パスキーのすべて：
- なぜパスキーが最強の認証なのか -

小岩井航介

自己紹介

小岩井 航介

ID・認証に関することを中心に、
新しい技術を調べて、それを発表したり、
仕様を書いたり、広めたりしています。

GitHub: kkoiwai
Qiita: kkoiwai
sizu.me/kkoiwai
↑パスキーに関するブログ記事を公開して
おります。よろしければご覧ください。

パスキーを使って便利で安全なログイン体験

パスワードに代わる次世代認証技術「パスキー」を徹底解説！

最新WebAuthn Level 3仕様をカバーし、
実装の解説はもちろんのこと、
皆さんの疑問にお応えするコラムも充実。

パスキーとアプリの生体認証の違いは？
パスキーは多要素認証なのか？

ぜひ本書で確認してください。

パスキーとは何か

パスキーとはなにか

- **セキュリティ**と**ユーザビリティ**を**両立**する、優れた認証方式

- 強力な**フィッシング攻撃 への耐性**

なぜパスキーなのか

- これまでの認証と課題の振り返り -

パスワード

パスワード

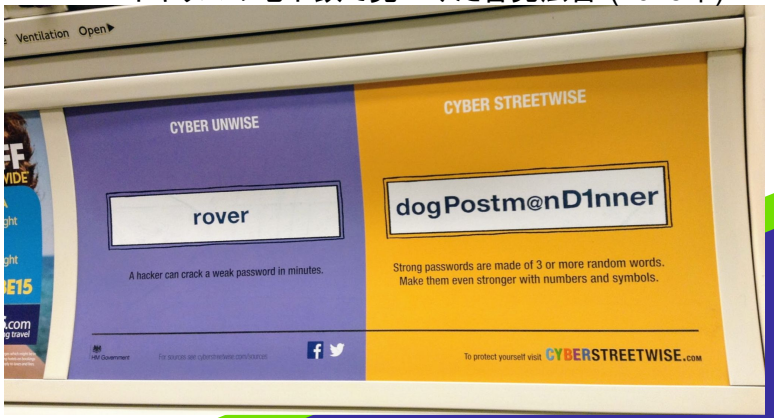
しくみ

- ユーザー名とパスワードが、事前に登録したものと一致するかを確認する
- 機種や端末依存はなく、どこからでも利用可能

課題

- 弱いパスワードを作ってしまう
- 同じパスワードを使い回してしまう
- フィッシングサイトに入力してしまう

イギリスの地下鉄で見つけた啓発広告 (2015年)



パスワードマネージャー

しくみ

- サイトごとに強力なパスワードを自動生成してくれ、保存・管理してくれる
- ドメインの一致するサイトでのみパスワードを自動入力してくれる
- 異なるデバイスでも保存したパスワードを同期してくれる

課題

- ユーザーに利用を強制することはできない
- コピー&ペーストでフィッシングサイトに手動入力できてしまう

AppleのPasswordsアプリ

二要素認証

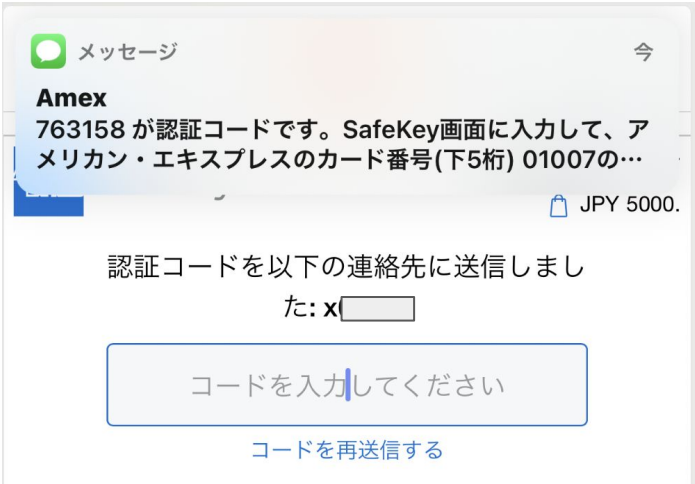
SMS OTP

しくみ

- パスワードに加えて、SMSに送信した6桁程度の短い有効期限のOTP（One-Time Password）を入力し一致を検証する

課題

- SMSが受信できないといけない
- 送信コストがかかってしまう
- OTPが有効である間にリアルタイムフィッシングされてしまう
- 携帯電話の店頭やサポートを欺くSIMスワップのリスク



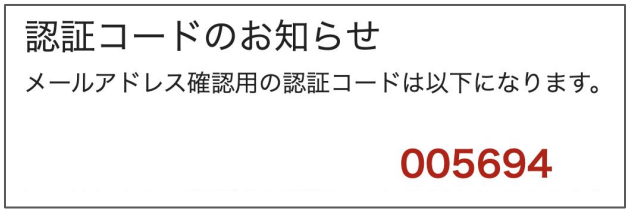
メールOTP

しくみ

- パスワードに加えて、メールアドレスに送信した6桁程度の
  短い有効期限のOTPを入力し一致を検証する

課題

- メールアカウントの乗っ取りのリスクあり
  ユーザがメールアカウントと同じパスワードを使っていたら意味が無い
- OTPが有効である間にリアルタイムフィッシングされてしまう



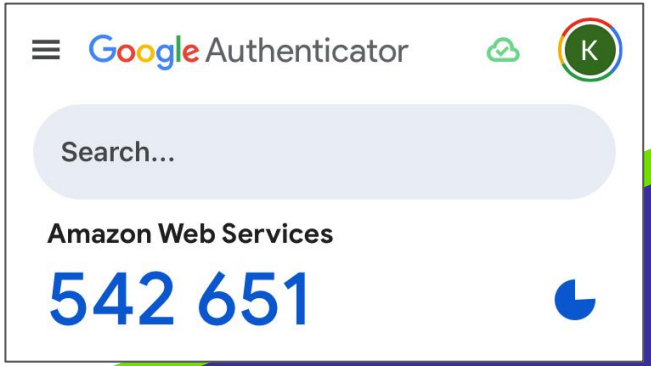
TOTP（Time-Based One-Time Password）

しくみ

- パスワードに加えて、専用アプリに表示された30秒程度で変わる通常6桁の数字からなるOTPを入力し検証する
- サービスごとにシークレットを登録しておく

課題

- OTPが有効である間にリアルタイムフィッシングされてしまう
- デバイスの乗り換え時に再設定が必要となる
- 専用アプリのインストールが必要になる



プッシュ通知

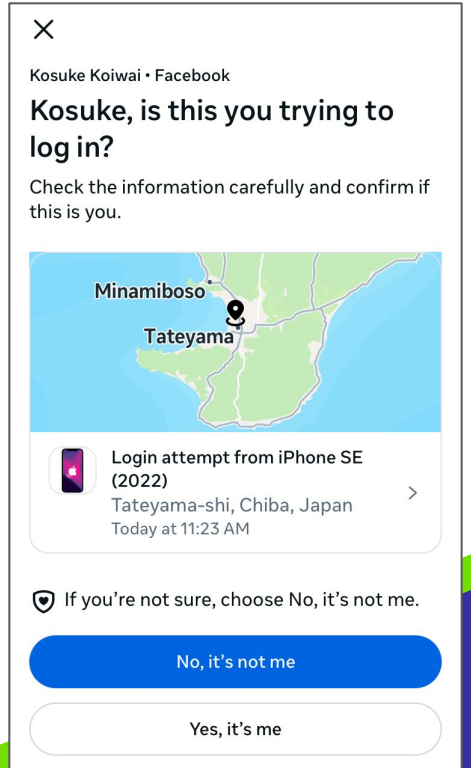
しくみ

- パスワードに加えて、ログイン済みアプリにプッシュ通知を送信し、ログインを承認する

課題

- アプリを提供する必要がある
- 多要素認証疲労攻撃（MFA Fatigue Attack）されてしまう

Facebookアプリのプッシュ通知



セキュリティキー

しくみ

- USB、BLE、NFCなどで公開暗号方式による電子署名を検証する
- 生体やPINを利用したパスワードレスな二要素認証をすることもできる
- **フィッシング耐性がある**

課題

- セキュリティキーの購入と持ち歩く必要あり
  - 紛失や破損も想定しないといけない

セキュリティキーも広義の「 パスキー 」です。
拙著では「 デバイス固定パスキー 」と呼んでいます。

パスワードレス

マジックリンク

しくみ

- メールを送信し記載されたリンク先にアクセスしたことを確認する

課題

- Webサイトとメールクライアントを切り替えなければならない
  - リンクの遷移先でログイン状態となるため、異なる端末でメールを開いてしまうとログイン体験が損なわれる
- メールアカウントの乗っ取りのリスクあり

下記URLをクリックして、メールアドレス認証を完了してください。

認証用URL：https://menu.onelink.me/qm5m/57e941f9?type=mailAuth&code=

SMS認証

しくみ

- SMSに送信した6桁程度の短い有効期限のOTPを入力し一致を検証する
- WebOTP APIやautocompleteで対象ドメインへの自動入力も可能

課題

- SMSが受信できないといけない（利用環境に制約がある）
- 送信コストがかかってしまう
- 携帯電話の店頭やサポートを欺きなりすますSIMスワップのリスクあり
- OTPが有効である間にリアルタイムフィッシングがされてしまう

ID連携

ID連携

しくみ

- 認証機能（OpenID ConnectやSAML）を提供する第三者のサービス（アイデンティティ・プロバイダ / IdP）と連携する

課題

- アイデンティティ・プロバイダの影響を受けてしまう（垢バン問題）
- サービスをIdPに把握されてしまったり、サードパーティCookieでトラッキングが可能になる場合がある
- 複数IdPのログインボタンの表示で混乱につながる（NASCAR問題）

パスキーの登場

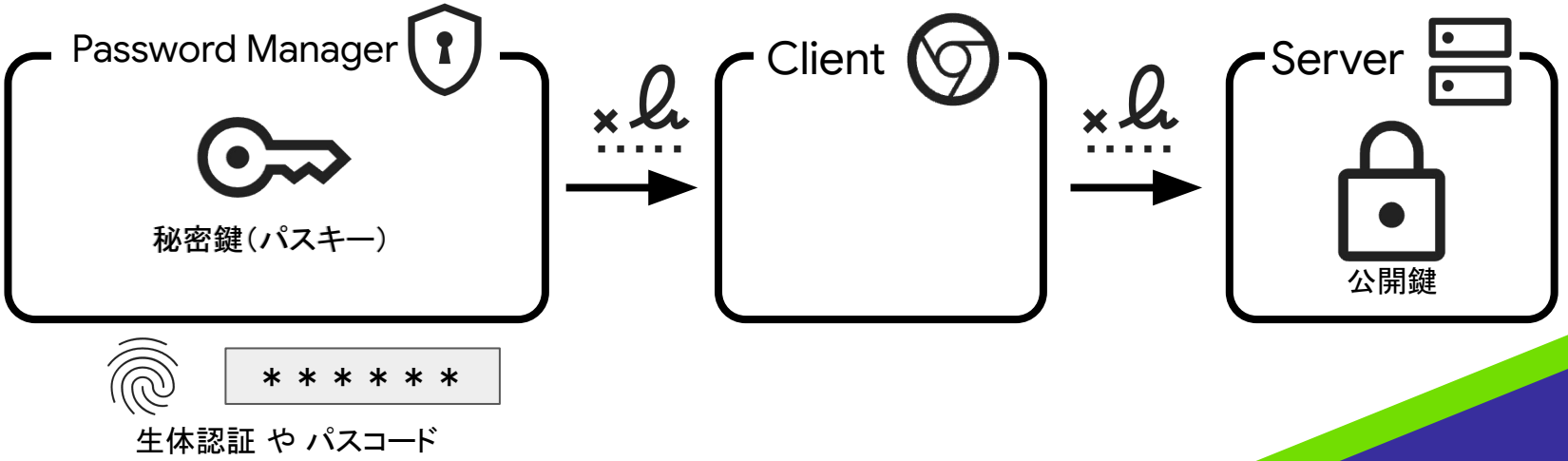
パスキーの登場

- **安全かつ簡単に利用できる認証**
  - デバイスの生体認証を実行するだけ
  - パスワード単体やOTPベースの二要素認証よりも安全

- **パスキーはパスワードマネージャに保存される**
  - **パスキープロバイダとも呼ばれる**

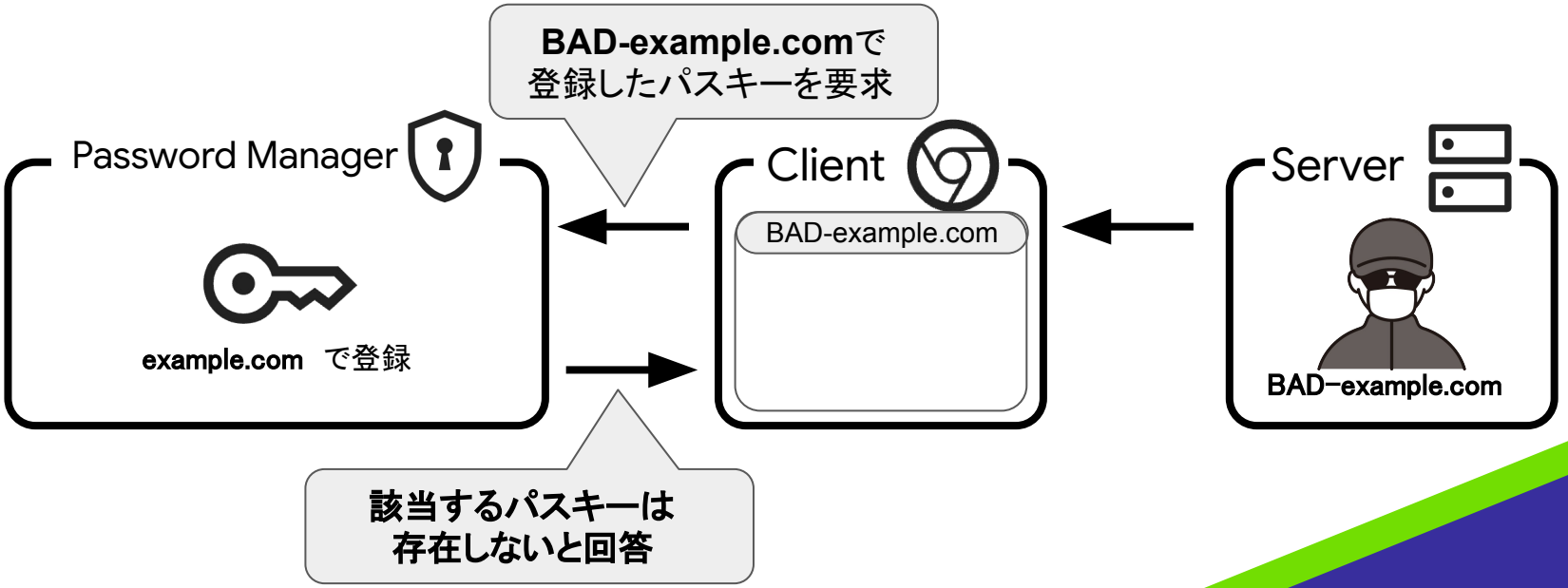
公開鍵暗号方式

- アカウントに紐づける形で公開鍵ペアを作成
  - デバイスのアンロック機構がトリガー
  - 公開鍵をサーバーに登録、秘密鍵はデバイスに保存
- ログイン時はその秘密鍵（パスキー）を使って署名を行う



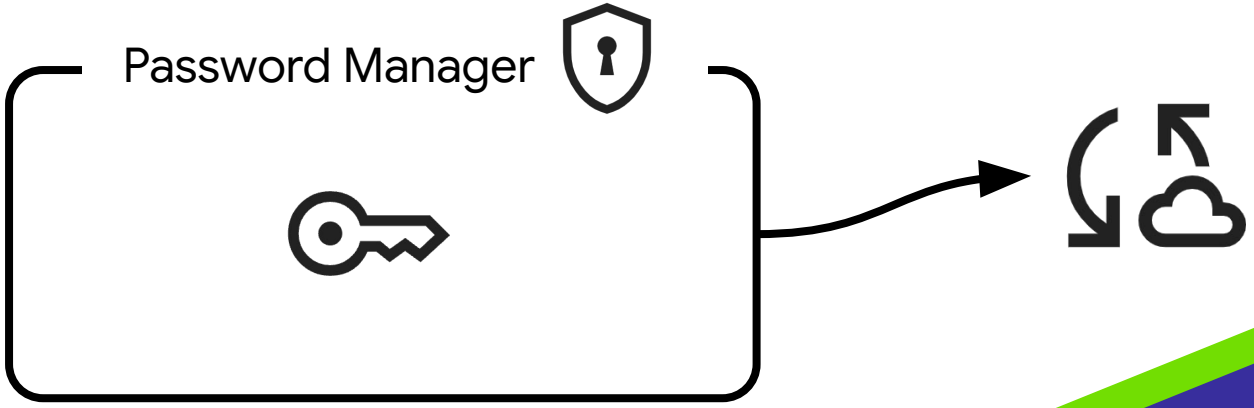
フィッシング耐性

- 登録したサイト以外では、パスキーを利用することができない。
  - パスワードのようにコピーペーストも不可能。



パスワードマネージャーで管理

- 秘密鍵（パスキー）はパスワードマネージャーを介して
  デバイス間で同期される
- 複数端末を持っている場合や、端末紛失時も利用し続けることが
  可能



パスキーの安全性

- 公開鍵はパスワードのように漏洩しても署名を偽造されにくい
- 公開鍵ペアはユニークなので、盗まれても別サイトで再利用できない
- パスワードマネージャーに管理されるので、フィッシングに引っかかりにくい
- そもそも登録したドメインと違うWebサイトやサービスでは
  利用できない

パスキーのまとめ

- パスワードに代わる、新しい認証方法
- パスワードの危険性を大きく改善
  - 覚える必要がない
  - 使い回しできない
  - **フィッシング攻撃を受けない！**（これ重要）
- 既存の２要素認証に比べてもメリットが大きい
  - SMS認証のように送信コストがかからない
  - メール認証のようにアプリを切り替えたり、コードをコピペしなくて良い
  - TOTPのように特殊なアプリが不要（OSやブラウザがデフォルトで提供）
  - **リアルタイムフィッシングの危険がない！**（大事なことなので2回）
- 端末を紛失してもリカバリが可能
  - ただしパスワードマネージャーにアクセスができる場合に限る

もちろん課題もあります。

パスキーの利用環境

- ユーザの環境によって、パスキーが使えない場合もある
  -

	Windows	macOS	iOS/iPadOS	Android	Linux	ChromeOS
Googleパスワードマネージャー	🔄*1*2	🔄*1	🔄	🔄	🔄*1	🔄*1
Appleパスワード		🔄	🔄			
Windows Hello	✅					
3Pパスワードマネージャー	🔄*3	🔄*3	🔄	🔄	🔄*3	🔄*3

*1 Chromeのみ
*2 要TPM
*3 拡張機能として

パスキーの利用環境

- ユーザの環境によって、パスキーが使えない場合もある
  - Windows8以下の場合
  - Windows Hello で作成したパスキーは現状クラウド同期されない。
  - iOSの場合、MDMなどでiCloudアカウントにログインできないと使えない
  - AppleのPasswordsアプリで作成したパスキーはWindows, Androidと同期できない

生体認証への不安

サービス事業者に自分の生体情報（指紋・顔など）が送られるのではないかという不安を持つユーザも存在する

パスキーの仕組み上、それはありえないが、周知・啓蒙が必要かもしれない

パスキーを導入すればセキュリティは完璧なのか？

パスキーはあくまで **ログイン時のセキュリティ** を高めるモノ

ログイン後のセッションを守るには、別の対策が必要です。

例えば、重要な取引前には、パスキーによる再認証を行うことで
リスクを軽減できます。

パスキーについて
もっと詳しく知りたい時は？

パスキーを使って便利で安全なログイン体験

パスワードに代わる次世代認証技術「パスキー」を徹底解説！

最新WebAuthn Level 3仕様をカバーし、
実装の解説はもちろんのこと、
皆さんの疑問にお応えするコラムも充実。

パスキーとアプリの生体認証の違いは？
パスキーは多要素認証なのか？

ぜひ本書で確認してください。

「パスキーのすべて」の概要

2025年1月28日発売
紙版・電子版　絶賛発売中

「パスキー」はパスワードレス認証を実現する認証技術です。

本書では、開発者はもちろん、企画職やデザイン職、セキュリティ担当などの認証に携わる方々に向けた内容になっています。

- 従来の認証技術の課題と比較して何が優れているのか
- パスキーの導入で知っておくべき特性
- パスキーの登録・認証・管理画面などのUX設計
- WebサイトだけでなくiOSやAndroidの具体的な実装
- パスキーが登場する以前の歴史から最新の仕様までの解説
- 読者の疑問や質問に答えるコラムも充実

本書についての詳細はこちら

本書の構成

第1章　パスキー導入が求められる背景
── 既存の認証方法とパスキーの背景を知ろう

第2章　パスキーを理解する
── パスキーの特徴や利点を理解しよう

第3章　パスキーのユーザー体験
── パスキーの体験をイメージしよう

第4章　サポート環境
── ユーザーの環境ごとに利用できる機能を確認しよう

第5章　パスキーの UXを実装する
── UXの実現に必要なメソッドやパラメータを知ろう

第6章　WebAuthn APIリファレンス
── クライアントとサーバの実装の詳細を確認しよう

第7章　スマホアプリ向けの実装
── AndroidとiOSにおける実装を確認しよう

第8章　パスキーのより高度な使い方
── より効果的な活用とUX向上方法を知ろう

第9章　パスキー周辺のエコシステム
── 標準化の流れや開発者向け情報を確認しよう

付録A　クライアント用 Extensionの解説
── 後方互換や先進的な活用のための拡張機能をみてみよう

付録B　iOS実装サンプル
── サンプルアプリを動かしてみよう

本書についての詳細はこちら

コラム一覧

第1章

- ❑ NIST SP 800-63
- ❑ 公開鍵暗号をざっくりと理解する

第2章

- ❑ ディスカバラブルでないクレデンシャル
- ❑ パスキーは多要素認証ではない場合もあるのでは？
- ❑ アカウントのライフサイクルとパスキーの関係性

第3章

- ❑ パスキーの他人との共有
- ❑ クロスデバイス認証のしくみ

第5章

- ❑ PINを使わず，生体認証だけでパスキーを利用できるようにすることはできますか？

第6章

- ❑ パスキーの同期を禁止する方法はある？

第7章

- ❑ アプリで利用している生体認証とパスキーは何が違うの？

本書についての詳細はこちら

パスキーのすべて
導入・UX設計・実装

ぜひお買い求めください！