



スマホで認証！ パスキー入門ガイド



株式会社ムービット

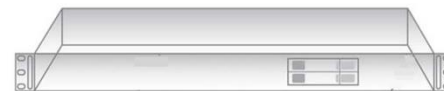
会社の概要

社名 株式会社ムービット

設立 1995年12月8日

所在地 東京都北区王子1-28-6

主な製品 Powered BLUE シリーズ
アプライアンスサーバー (Linux)
ソフトウェア開発



パスワード からの 脱却

① さよなら パスワード



② ようこそ パスキーへ



本日のプレゼンで覚えていただきたいたい事項 は

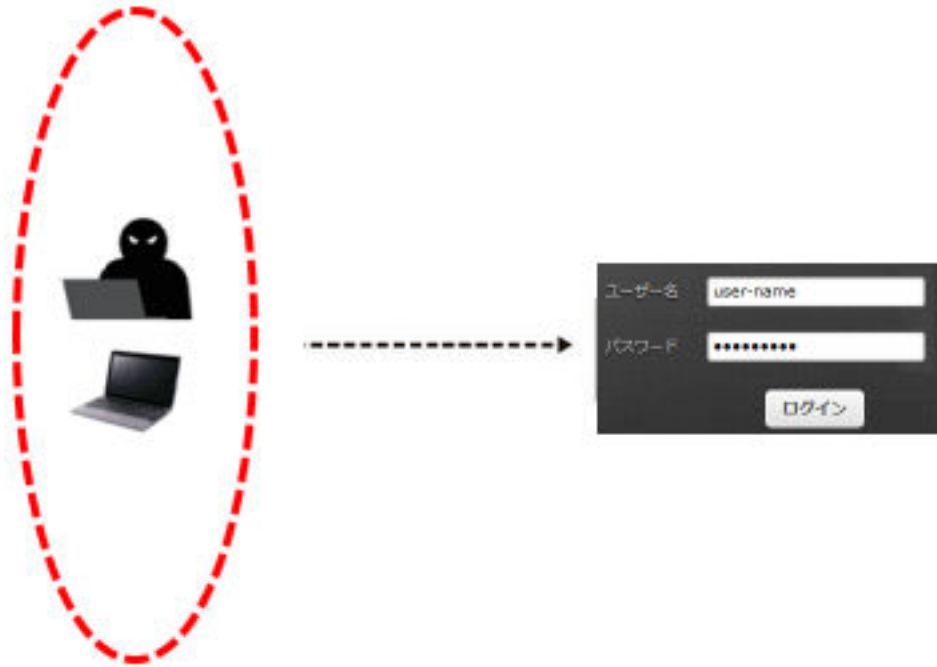


Webサイトへの不正アクセス

- 総当たり攻撃
- パスワードリスト攻撃
- 辞書攻撃

パスワードスプレイ攻撃

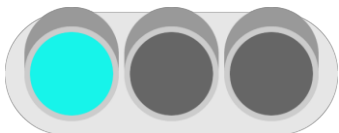
パスワードは固定
ユーザーIDを変更



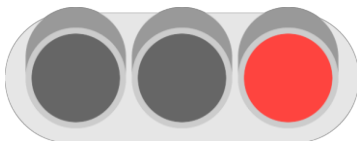
SMS認証は安全か ？



G-123789 があなたの
Google 確認コードです。



Google では SMS認証 は 使用可能



Salesforce では SMS認証 の 利用禁止

生体認証が必要な背景

- ID・パスワードの漏洩対応
- リモートワーク
社員の自宅や出先からのアクセス対応

➡ 安全を担保できる仕組みが生体認証

■ パスワード を 利用 しない 認証方式



➡ 生体認証 の 場合



- 利用者が保有する生体「固有の情報」を利用
- パスキー認証は ①「生体情報」 + ②「端末保有」の2要素認証

FIDO (ファイド) アライアンス 経過

- 2012年 FIDOアライアンス設立
Paypal / Lenovo などで設立
パスワードを解消することを目的として設立

- 2018年 FIDO2の規格



- ① ➡ ■ 2022年 Google / Apple / Microsoft 促進表明

- ② ➡ ■ 2022年 Appleが iPhone のパスキー対応
複数端末での利用



- 2023年 パスキー元年

FIDO2とPasskey認証の相違

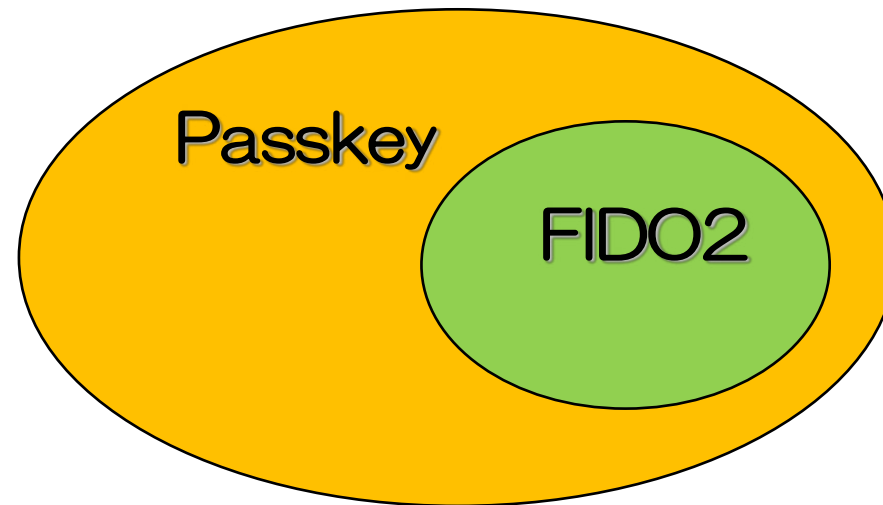
■ FIDO2（ファイド）

利用デバイスは1端末に固定



■ Passkey（パスキー）

複数デバイスからの利用に対応



➡ FIDO2のみに対応の機器もPasskey対応を謳っている

同期パスキーとデバイスバウンドパスキー比較

1.同期パスキー（ Synced passkeys ）

2.デバイスバウンドパスキー（ Device bound passkeys ）

項目	1. 同期パスキー	2. デバイスバウンドパスキー
秘密鍵保存先	クラウドサービスを利用	特定のデバイス内に保存
利用方法	複数のデバイスで利用可能	1つのデバイスのみ利用可能
メリット	スマホ買い替え時の乗換が簡単	より高い安全性
デメリット	セキュリティリスクがやや高い	複数のデバイスで利用できない



- iCloudキーチェーン
- Googleパスワードマネージャー



同期パスキー構成時のWeb





1 かんたん

スマートフォンの認証を利用
Webへパスワードレス・ログイン



2 安全・安心

なりすましログイン防止



3 マルチデバイス

PCに対応



Passkey認証 に対応 の 機器

✓ スマートフォン



✓ ブラウザ



✓ Windows / Mac



✓ 認証器 (USB)



Passkey認証でWebサービス提供 例

Yahoo! JAPAN、安全なパスワードレス認証を、より利便性高く利用できる“パスキー”に対応



① dアカウント 2022年10月から

～ 端末ごとの事前設定が不要になり、
複数端末での利用や端末買い換え時も再設定なく
安全なパスワードレス認証が利用可能に ～

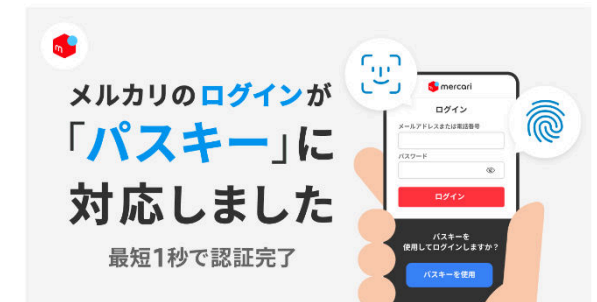
ヤフー株式会社（以下、Yahoo! JAPAN）は、Yahoo! JAPAN IDでの認証において、より安全性・利便性が高いパスワードレス認証技術“パスキー”に対応しました。これにより、現在“パスキー”をサポートしているAppleのiOS、iPadOS、MacOS、GoogleのAndroidなどでは、端末ごとの生体認証利用の設定が不要になり、複数端末での利用や端末買い換え時も再設定なく安全なパスワードレス認証が利用可能になりました。



② Yahoo 2023年3月から

mercari

https://about.mercari.com/press/news/articles/20230414_passkeys/



メルカリは、これまで電話番号認証^{※2}や3Dセキュア2.0^{※3}による認証など、安心・安全なマーケットプレイスの実現に向け複数の本人認証サービスを提供してまいりました。お客さまから端末移行時に「再登録に失敗してしまった」といった声や、「機種変更時に煩雑である」というお声をいただいたことから、2023年4月より「パスキー」を導入しています。

③ メルカリ 2023年4月から

Passkey認証 導入後の効果

メルカリ

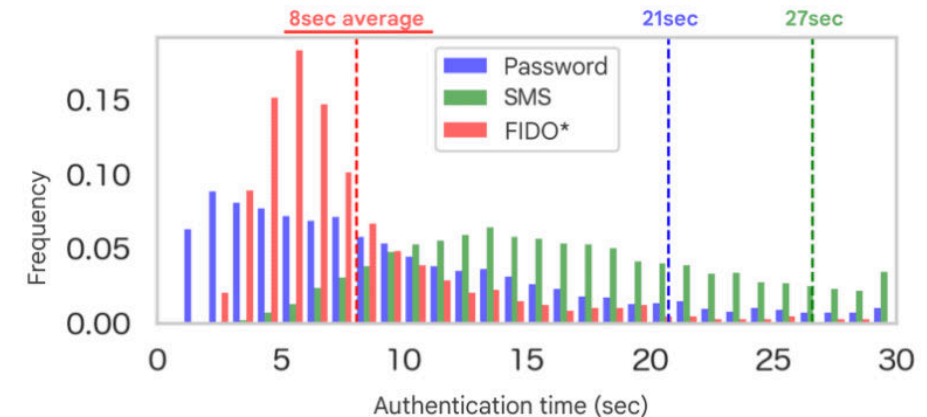
認証方式	ログイン時間	認証成功率
SMS OTP 認証	17 秒	67.7 %
Passkey 認証	4.4 秒	82.5 %

KDDI

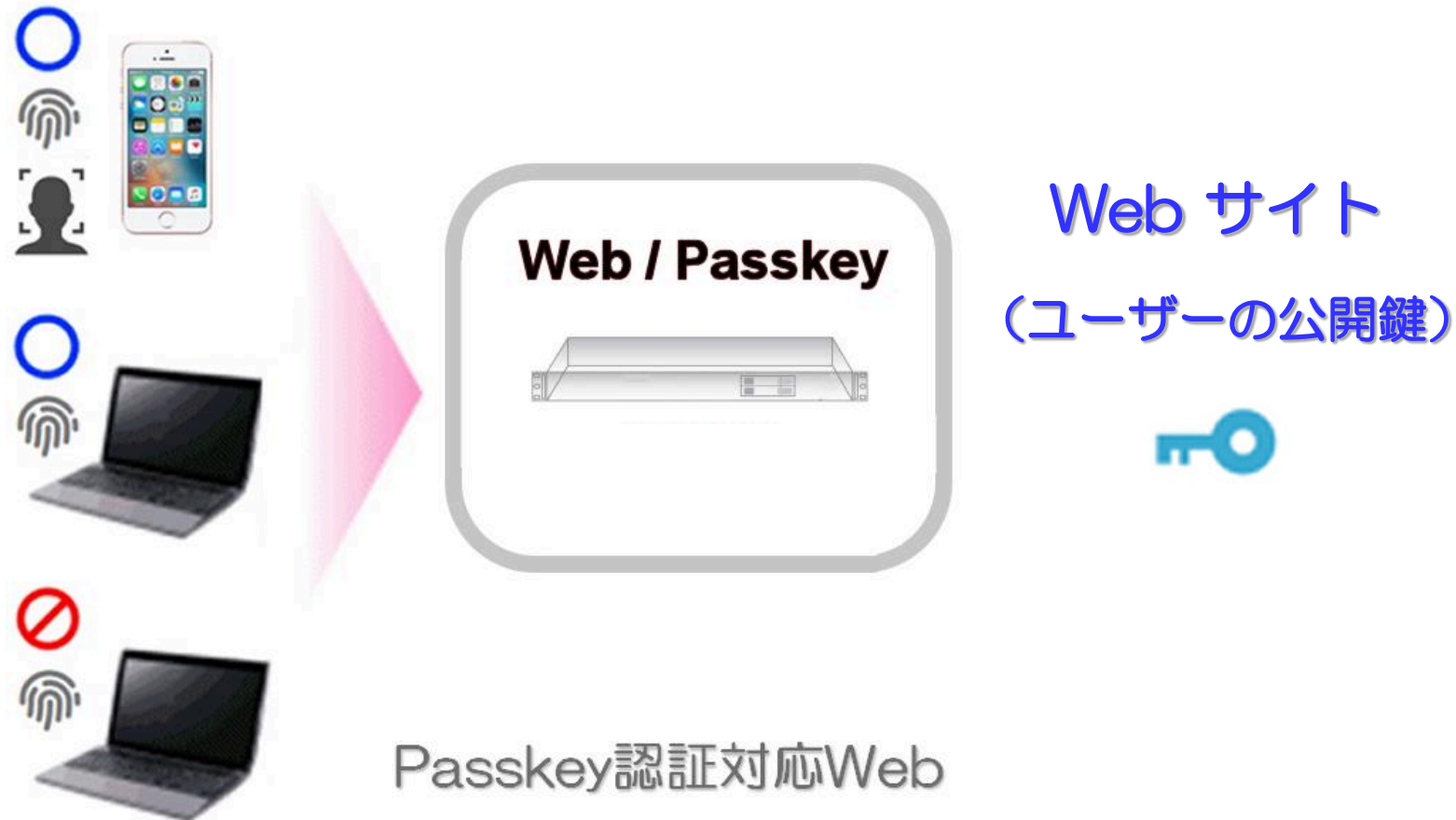
パスワード再設定 不要	✓
コールセンター 負荷低下	✓

ヤフー

認証方式	ログイン時間
SMS OTP 認証	27 秒
パスワード 認証	21 秒
Passkey 認証	8 秒



Passkey 認証対応 の Web



Web サイトに生体情報は「送信&保存」されません

フィッシング・サイト防止

パスキー認証

Webサイトに紐付いた公開鍵 & なりすましログイン防止



Web サイト

(ユーザーの公開鍵)



■ スマートフォンの認証をWebサイトの認証に利用



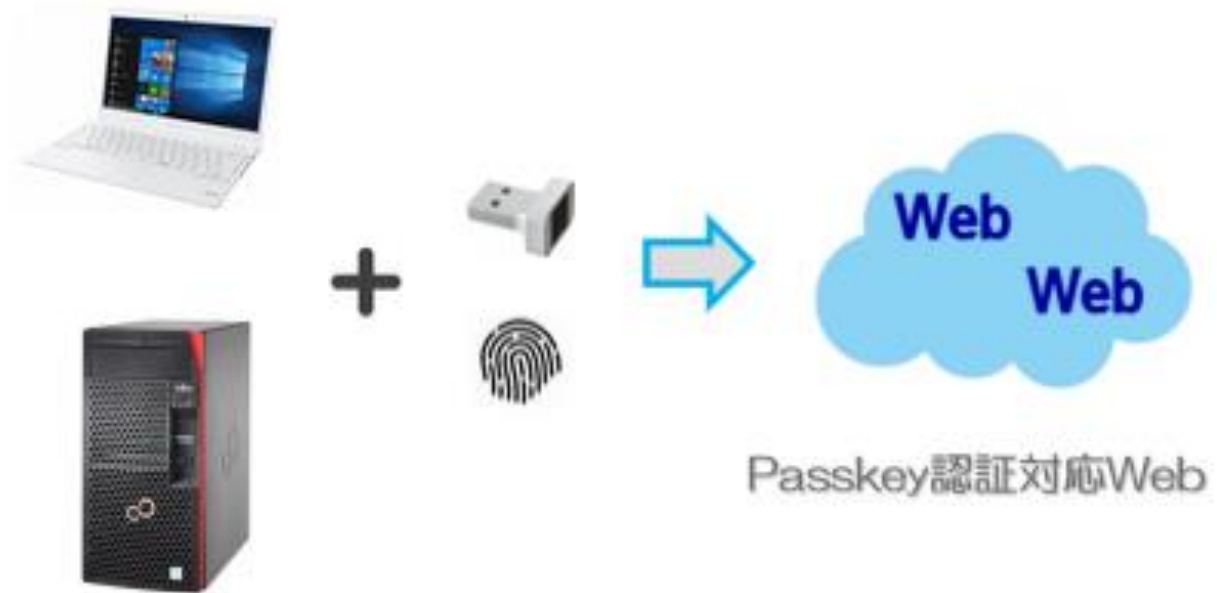
■ PCからのアクセスにスマートフォンの認証を利用

クロスデバイス認証



■ USB認証器をPCからのアクセスに利用

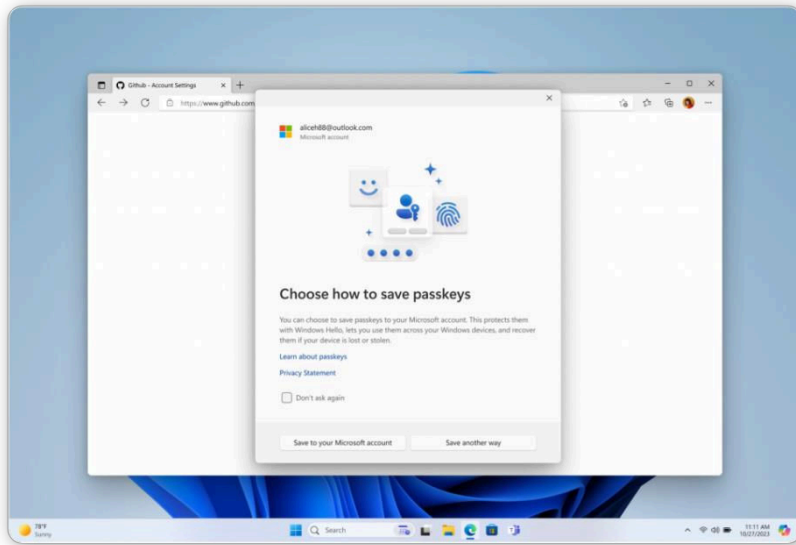
デバイスバウンドパスキー認証



Microsoft / Windows11 も Passkey認証 に対応

Microsoftは、Windows11におけるパスキー認証の新機能を発表

2024年10月8日



パスキーの同期機能：

一度作成したパスキーを
他のWindows 11デバイスでも 使用できるように
Microsoftアカウントを通じて同期が可能に

同期Passkey認証の対応状況

	Apple	Google	Microsoft
同期パスキー対応	✓	✓	✓
クロスデバイス認証	iOS 17 以降	Android 14 以降	Windows11



Passkey生体認証を導入する環境



インフラ	内容
✓	顔認証や指紋認証対応のスマートフォン（すでに保有）
✓	ブラウザ（対応済）
✓	PC（クロスデバイス認証 / USBの認証器を接続）
✓	Apple / Google / Microsoft

ユーザー環境は整っている

「Passkey対応のWebサイトを簡単に導入するには」

■ 生体認証の端末

Passkey のユーザー環境



+

■ Passkey認証対応のWeb

Web / Passkey



Passkey認証のWeb導入方法

■ Passkey認証対応 Powered BLUE アプライアンス



✓ Passkey認証 Webサイト構築

✓ 自社運用

Passkey認証のWeb導入方法



リバースプロキシでWebへアクセス



Passkey認証対応のリバースプロキシ



Powered BLUE アプライアンス の 位置

自社運用 = オールインワンのアプライアンス

Powered BLUE (OS+アプリ+GUI)



Pass

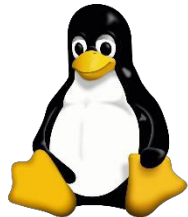
IaaS

OS まで

IaaS

PaaS

SaaS



自社で運用

パスキー認証



Webやリバースプロキシへパスワードレス・ログイン



なりすましサイト & なりすましログイン防止



Web サイト側 に生体情報は「送信&保存」されません



パスキー認証対応Webやリバースプロキシ製品のWebサイトのWebサイト



<https://www.mubit.co.jp/>

問い合わせ先

お問い合わせ

お問い合わせ

購入先

お問い合わせ

お問い合わせフォーム

下記のフォームにご記入後、下のボタンを押してください。

会社名
(会社または組織名。個人の方は省略可)

ご担当者

ご連絡先 郵便番号:

ご住所

<https://www.mubit.co.jp/sub/contact/call.html>



<https://www.mubit.co.jp/sub/contact/call.html>