fido ALLIANCE | simpler stronger authentication

NII Open Forum 2022 AXIES認証技術部会・学認合同企画セッション

FIDO認証～「パスワードレス」に向けたさらなる推進

2022年6月2日

森山 光一

FIDOアライアンス 執行評議会メンバー・ボードメンバー・FIDO Japan WG座長
株式会社NTTドコモ マーケティングプラットフォーム推進部 セキュリティサービス担当部長 兼 経営企画部 経営企画担当部長

はじめに

- 本年もAXIES認証基盤部会の皆様と共に、このような機会をいただき、ありがとうございます。
- NII Open From 2019における認証トラック「新しい認証技術標準FIDO」をきっかけとして、大学ICT推進協議会 年次大会2019に向けて大学ICT環境ならではのさまざまな要件と身元確認、当人認証の関係について集中的な議論を重ねました。
- さらにNII Open Forum 2020でパネルディスカッションを開催、昨年はFIDOアライアンスから当時の最新ニュースをお届けしました。（デベロッパーチャレンジなど）
- 本年は、パスワードレス認証をさらに推進するための最新の取り組みについてご紹介します。

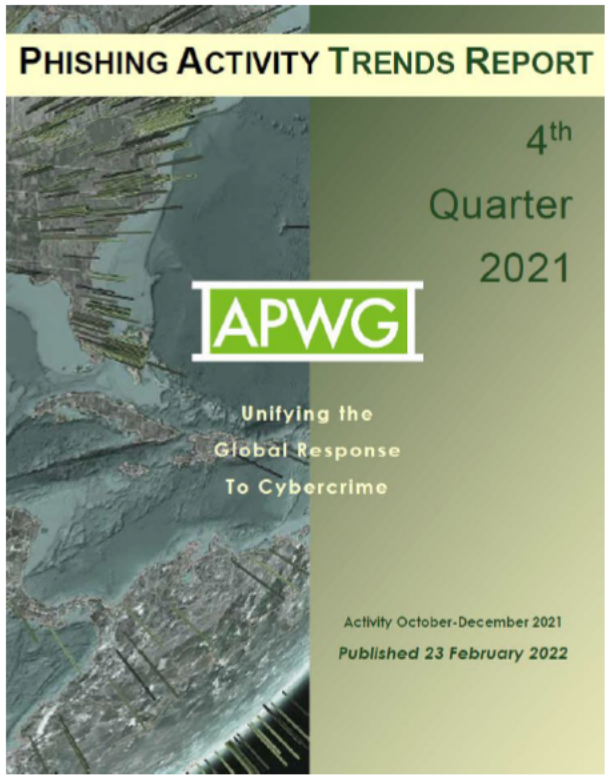
WHY FIDO?

パスワード課題への挑戦

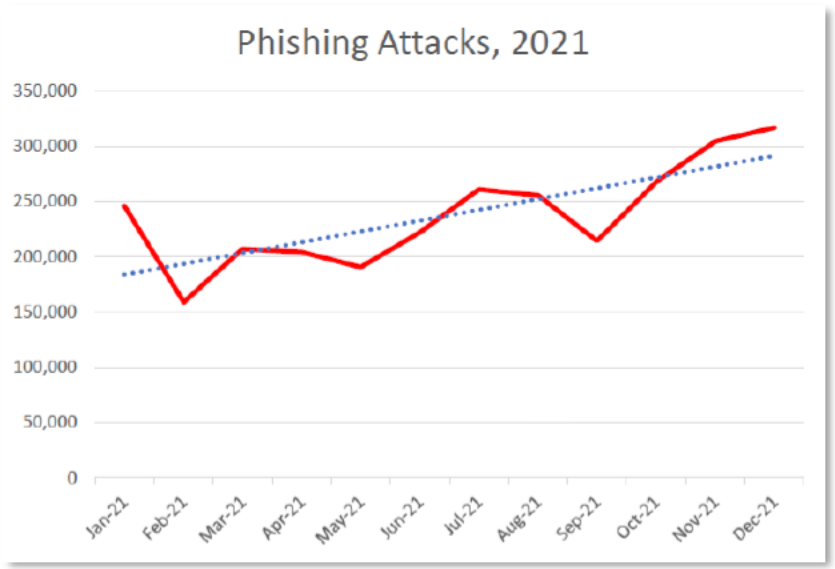
CLUMSY | HARD TO REMEMBER | NEED TO BE CHANGED ALL THE TIME

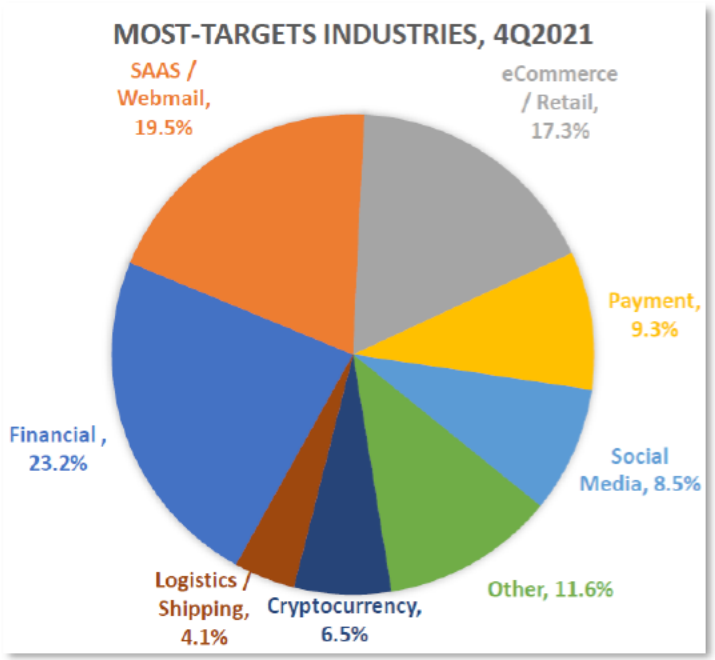
煩雑　覚えるのが大変　日々パスワードの変更も求められる

APWG (Anti-Phishing Working Group) の報告より



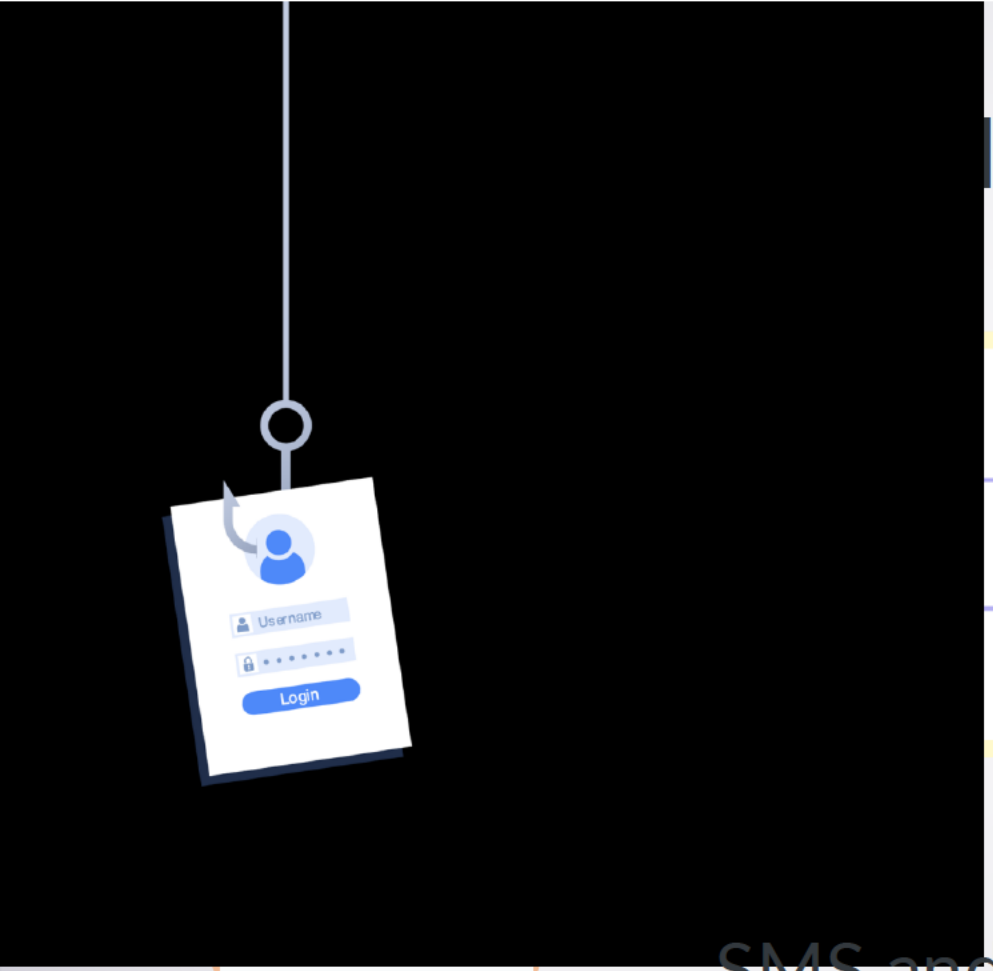
Phishing Hits All-Time High in December 2021; Attacks Triple Since Early 2020





https://apwg.org/

ls are not fit for purpose



- Clumsy 煩雑
- Hard to remember 覚えるのが大変
- Easy to phish, harvest, replay

攻撃も受けやすい

SMS and OTPs add security,
but are inconvenient and still phishable

SMS OTPが普及しつつあるが、依然としてフィッシング耐性がない

フィッシング詐欺により二段階認証は突破されている

- 二段階認証を突破する方法は2019年10月に図解でわかりやすく示されるに至り、2020年2月に新聞紙上でも記事として報道された。

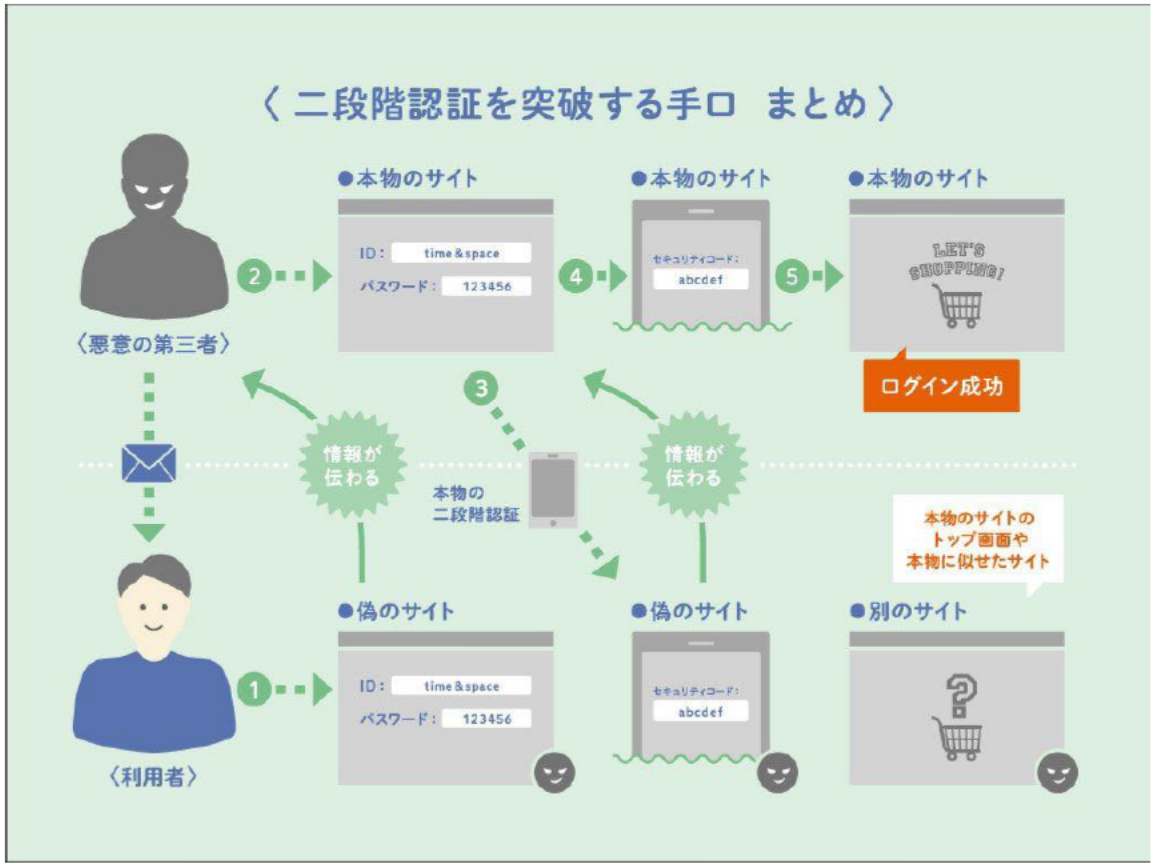
① 利用者が偽サイトにアクセスする。悪意のある第三者に情報が伝わる

② 悪意ある第三者が本物のサイトにIDとパスワードを入力する

③ 本物のサイトへ正しいIDとパスワードが入力されたので、本物の二段階認証が機能する。利用者は、受信したワンタイムパスワードを（この時点ではまだ偽サイトと気が付かずに）入力する。この情報も悪意のある第三者に伝わる

④ 悪意のある第三者は、そのワンタイムパスワードを本物のサイトに入力する

⑤ そして、悪意ある第三者がログイン・決済等に成功する。（利用者は、この時点で何かおかしいと気が付くこともあるだろうし、気が付かないこともあるかもしれない）



https://time-space.kddi.com/it-technology/20191021/2761

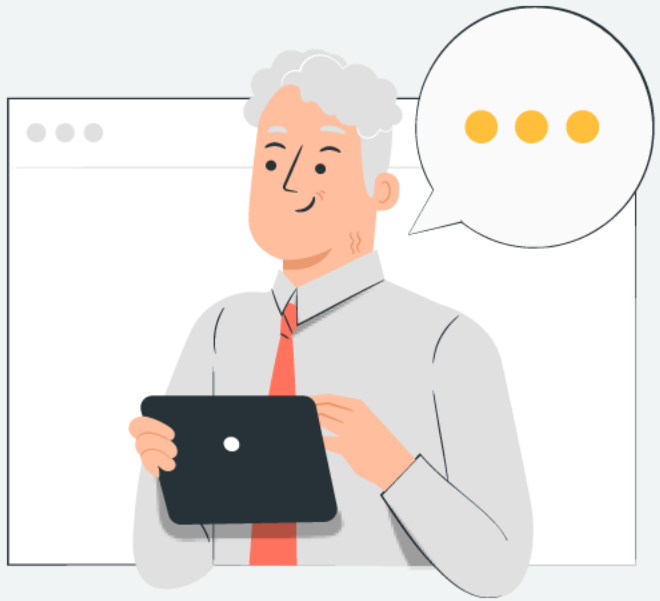
民間IDにおける認証をとりまく課題～パスワードと二段階認証

- IDとパスワードが流出していると言われる。通信元の特定を困難にする技術などを使って、悪意のある第三者は、匿名性を確保しながらIDとパスワードなどの個人情報をやりとりしていると言われる。そして、それらを使ったいわゆる**リスト型攻撃**により、効率よく不正アクセスが可能になったと言われている。この要因として、多くの利用者が異なるサービスに対して同じIDとパスワードを流用していることなども原因とされている。
- 最近では、**フィッシング型攻撃**による不正アクセスも急増している。悪意のある第三者が本物そっくりの偽サイトを立ち上げてアクセスさせたり、本物そっくりの偽ブラウザアプリをインストールさせたりする。そして、第三者は、利用者がだまされて入力したIDとパスワードやワンタイムパスコードを奪取し、不正アクセスするというものである。これによって、二段階認証も突破されていることが明らかになっている。

  - 二段階認証とは、多要素を二段階で認証することを意味することがあるが、単一要素を二段階で認証することを意味することもある。従来から使われて来た二段階認証は、パスワードに加えて予め紐付けられたデバイスやアプリに表示されるワンタイムパスコード（認証コード）を利用者が入力することで、二段階認証を構成することが多かった。しかし、デバイスに表示された認証コードは、ユーザーの知識として入力されるので、パスワードと認証コードという同じ知識要素を2個使った認証になっている。そのため、フィッシング型攻撃に対して脆弱である。（多要素認証、二要素認証と区別した方が良い）
  - これらの攻撃に対しては、パスワードを複雑にしたり文字数を増やすなどの対策は、効果がない。

A fundamental shift is required – 「所持」を伴う多要素認証

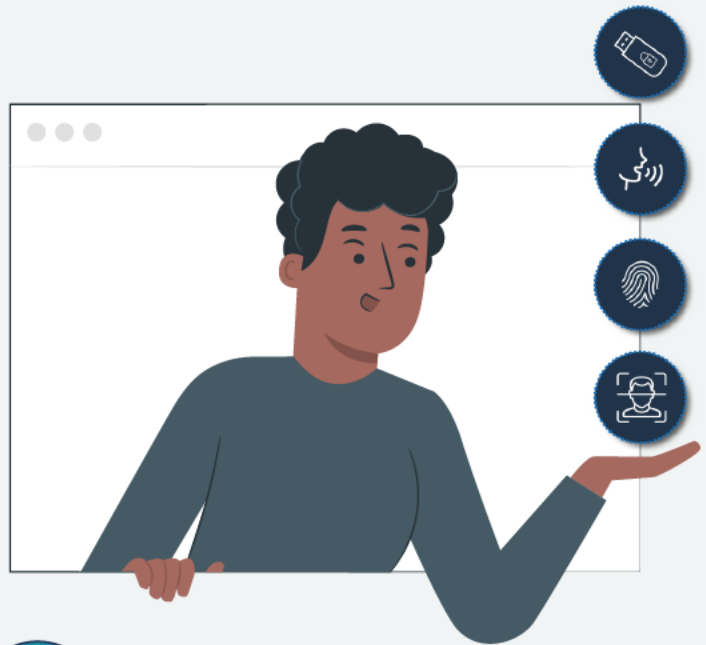
From legacy, **knowledge-based** credentialing
In your head (remembered)



- Stored on a server
- SMS OTP
- KBA
- Passwords

SUSCEPTIBLE TO COMMON THREATS

To modern, **possession-based** credentialing
In your hand

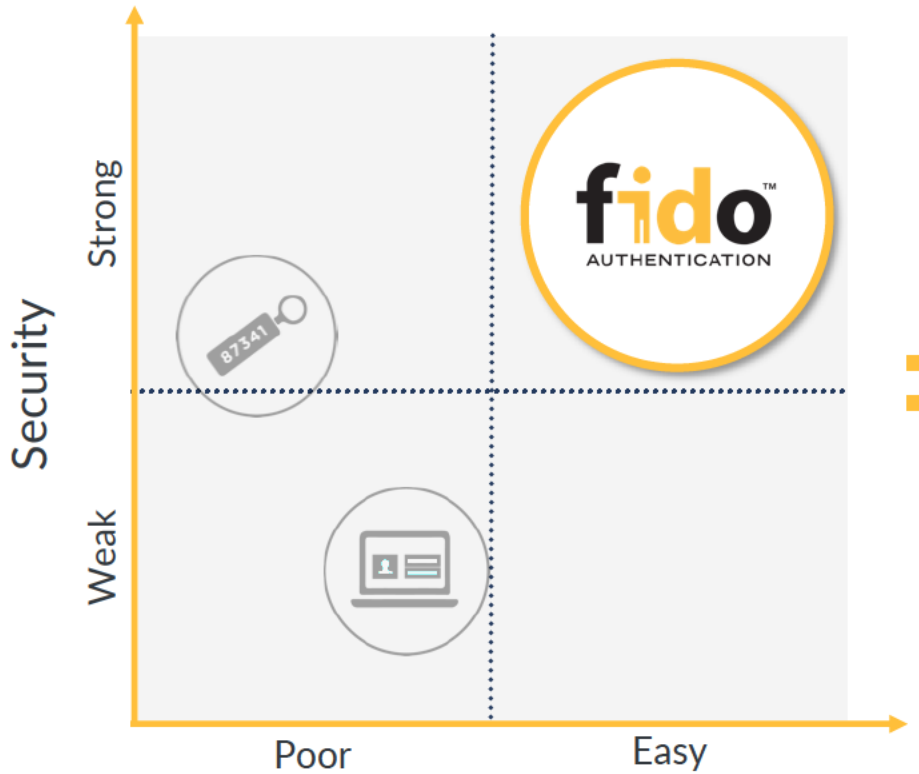


- On-device
(never on a server)
- Local Biometric / PIN
- DocAuth
- “Passkeys”

PHISHING RESISTANT

フィッシング耐性のある認証

Industry imperative: Simpler and stronger（シンプルで堅牢に）



セキュリティと
使い勝手の両立をめざす

=

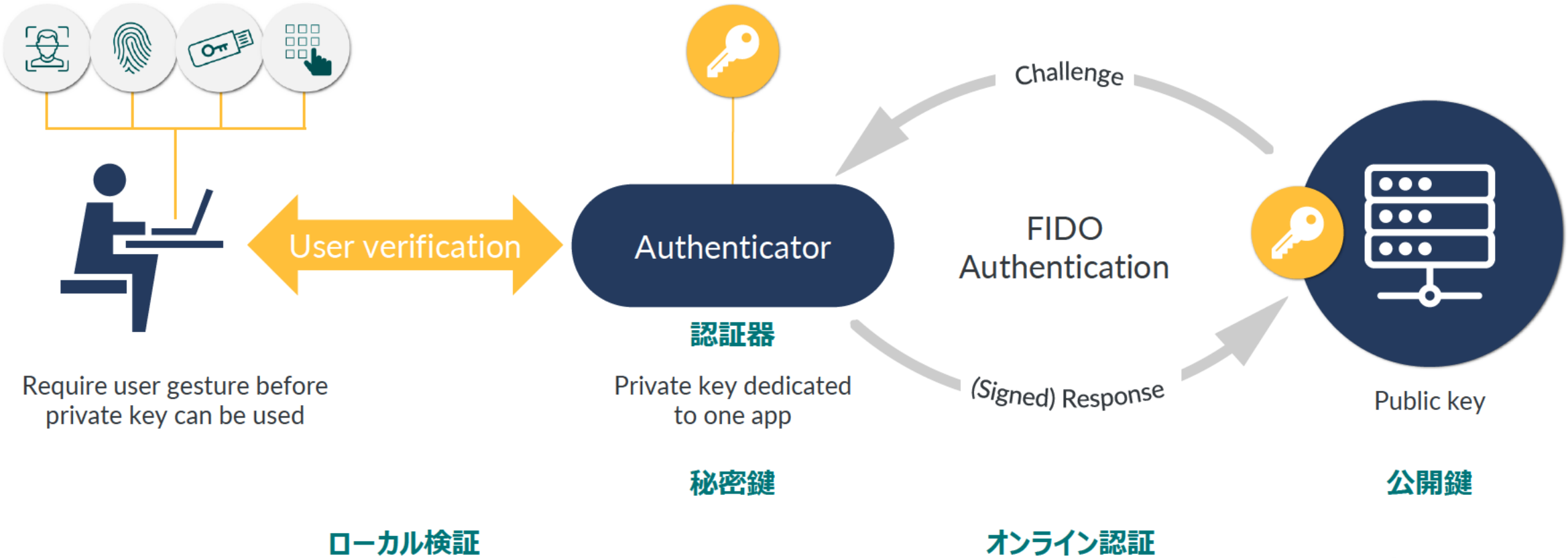
公開鍵暗号方式を活用したオンライン認証

Open standards for simpler, stronger authentication using public key cryptography

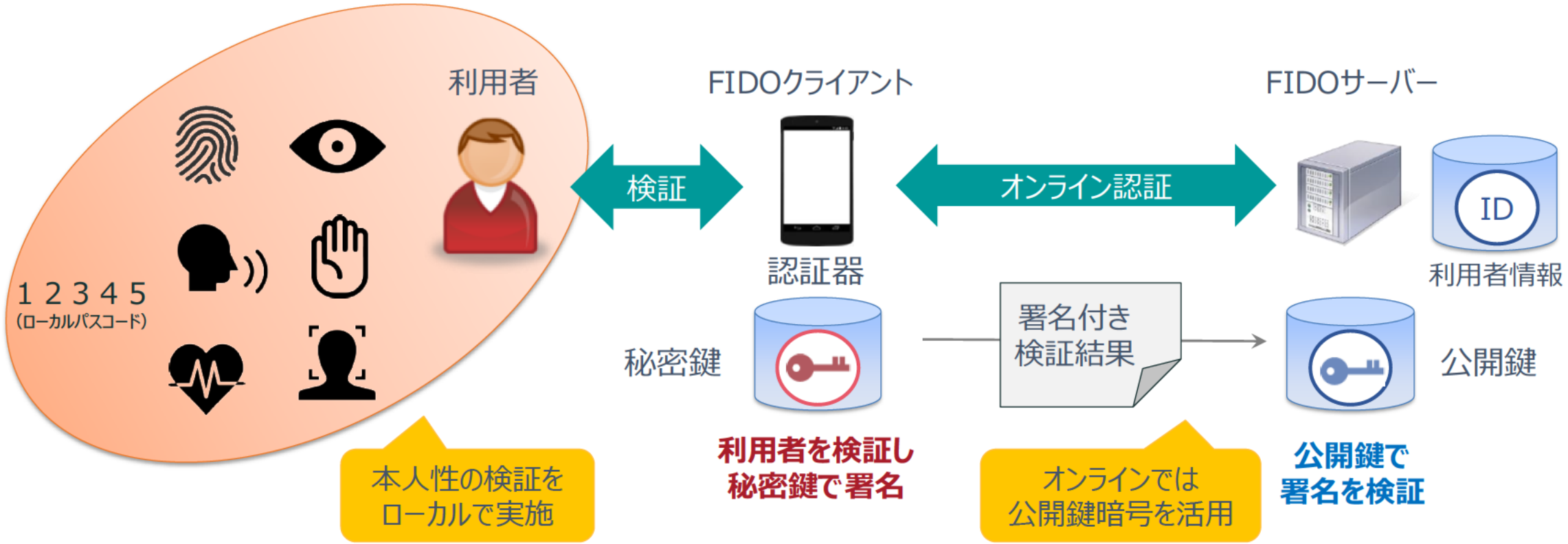
Single Gesture
Possession-based Authentication

「所持」を伴う多要素認証を「シングルジェスチャー」で

FIDO Authentication: How it works



FIDO認証モデル（端末とサーバーで秘密を共有しない）



利用者が「認証器」（Authenticator）に適切な秘密鍵を保有することを検証することによって
認証を実現しており、認証器の簡単な操作だけで（動的な）多要素認証

FIDO認証・パスワードレス認証の利用者を増やす

止まらないフィッシング詐欺被害への対策として、パスワードレス認証をおすすめします！

「ドコモからのお知らせ」による注意喚起

- 【お客さまへの注意喚起】「NTTセキュリティ」などを装ったフィッシングSMSや不正なアプリによるドコモオンラインショップでのApp Store & iTunesギフトカード等の不正購入発生について（2021年10月2日）
- 【お客さまへの注意喚起】通信事業者などを装うフィッシング詐欺にご注意ください（2021年7月21日）
- 【注意喚起】ドコモを装った「dアカウントの一時的な利用停止」に関するフィッシングメールにご注意ください（2021年7月8日）
- 【注意喚起】「あんしんセキュリティ」の偽アプリにご注意ください（2021年6月11日）
- 【注意喚起】「NTT」「NTTセキュリティ」「NTT docomo」を装ったフィッシングSMSやアプリにご注意ください（2021年5月21日）
- 【注意喚起】身に覚えのない不審なSMS（宅配事業者や銀行等）にご注意ください（2021年1月23日）

2021年10月18日、ドコモでは生体認証非対象機種についても dアカウント パスワードレス認証提供開始を発表（10月22日以降、順次提供開始）

2021年9月15日、コンシューマー向け「Microsoftアカウント」にパスワードレスで運用するオプションを導入と発表

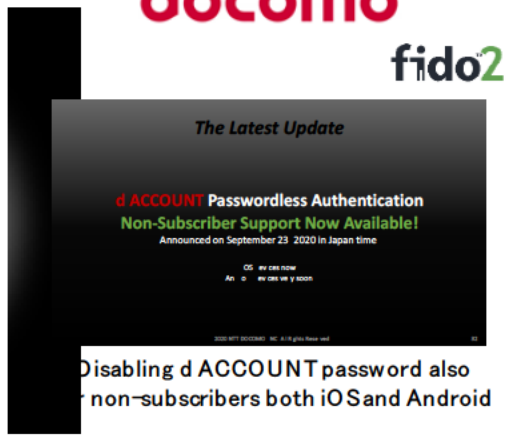
FIDO認証の国内導入事例～最新動向

LINE fido2

LINE desktop app supporting Passwordless on iPad and Windows PC

November, 2020

NTT docomo fido2



Disabling d ACCOUNT password also for non-subscribers both iOS and Android

January, 2021

YAHOO! JAPAN

ヤフー、Yahoo! JAPANアプリなどのアプリやスマートフォンブラウザーで指紋・顔認証を利用したログインに対応

コンシューマ向け商用サービスとしてiOS「Safari」でFIDO2に対応した認証方法の導入は世界初。パスワードを使わない認証方法を推進し、利便性と安全性の向上を目指す

2021年2月8日 発表

2021年12月9日 発表

Rakuten

「楽天ウォレット」のログインや出金・出庫、「楽天キャッシュ」へのチャージをより簡単・安全に利用できる「かんたんログイン」を導入

パスワード入力と外部認証アプリによる確認コード入力の2段階認証からFIDO2対応へ。パスワードを使わない認証方式でより便利に！

Rakuten Wallet

2021年12月13日 提供開始

- 本検討会の発足以降も、ボードメンバー企業による取り組みを中心に、FIDO認証の導入が進んでいる。
  - ヤフーが2021年2月8日に、iOS「Safari」対応に加えてアプリでもFIDO2認証を導入し、アプリとスマートフォンブラウザで生体認証の導入完了を発表。2021年12月9日にはパソコンでもFIDO2認証による生体認証を利用したログインに対応
  - 楽天が2021年12月13日、「楽天ウォレット」のiOS、引き続きAndroidで、FIDO2認証を導入し、かんたんログイン対応
- さらに多くの民間企業が提供するID・アカウントへの認証シーンで、フィッシング型攻撃に耐性のあるFIDO認証がより活用され、その設定・再設定に必要な身元確認や一意性確保手段としてマイナンバーカードの機能に期待。

早稲田大学 NTT寄付講座 サイバー攻撃対策技術の基礎 ～ パスワード課題とフィッシング対策（2022年1月7日）より
（第5回 総務省 マイナンバーカードの機能のスマートフォンへの搭載等に関する検討会（2021年3月3日）に最新状況を加筆）

Backed by global tech leaders – ボードメンバー

amazon
AMERICAN EXPRESS
arm
Bank of America.
CVSHealth.
egis Technology
FEITIAN WE BUILD SECURITY
Google
HYPR
IDEMIA
Infineon
ING
intel.
JUMIO
Lenovo
LINE
LogMeIn
mastercard.
Meta
Microsoft
nok nok
NTT docomo
OneSpan Be bold. Be secure.
onfido
PayPal
Qualcomm
RAON
RSA
SAMSUNG
Synaptics
THALES
transmit security
TRUSONA
TRUSTKEY SOLUTIONS
USAA
VISA
vmware
WELLS FARGO
YAHOO! JAPAN
yubico

+ スポンサーメンバー | + アソシエイトメンバー | + リエゾンパートナー | + 政府系機関メンバー

fido ALLIANCE

Global market validation (partial list)

政府系機関を含めたグローバル市場におけるFIDO認証の広がり～その一部

Browser and OS Support = Endpoint Ubiquity

ブラウザ・OSサポート = あらゆるデバイス（エンドポイント）でFIDO認証を使えるようにするために

Platformization has enabled passwordless deployment…

FIDO認証のプラットフォーム対応と共に「パスワードレス認証」の導入も進んでいます！

https://fidoalliance.org/yahoo-japan-turns-to-fido-authentication-for-enhanced-login/

https://fidoalliance.org/ebays-journey-to-passwordless-with-fido/

https://fidoalliance.org/ntt-docomo-deployment-case-study-your-security-more-simple-2/

…but some challenges persist

しかし、課題もまだ残っていました

Next Steps for Reaching Mass Adoption:

さらなるコンシューマー市場へのFIDO認証の利用推進のために…

Furthering usability while keeping security in mind

利用シーンを見据えて、セキュリティを確保しつつ、
使い勝手の改善をさらに探求する

Core usability initiatives

- **2021:** First FIDO UX guidelines (platform authenticators): published June 2021
- **2022:** UX Committee launched this year
- **Upcoming:** Plans for future UX research (e.g., Security key guidelines)
- **Upcoming:** Multi-device FIDO credentials
  マルチデバイス対応FIDO認証資格情報

New: Multi-device FIDO credentials

マルチデバイス対応FIDO認証資格情報

- Enables deployment of FIDO at scale to consumers moving between devices and upgrading to new ones

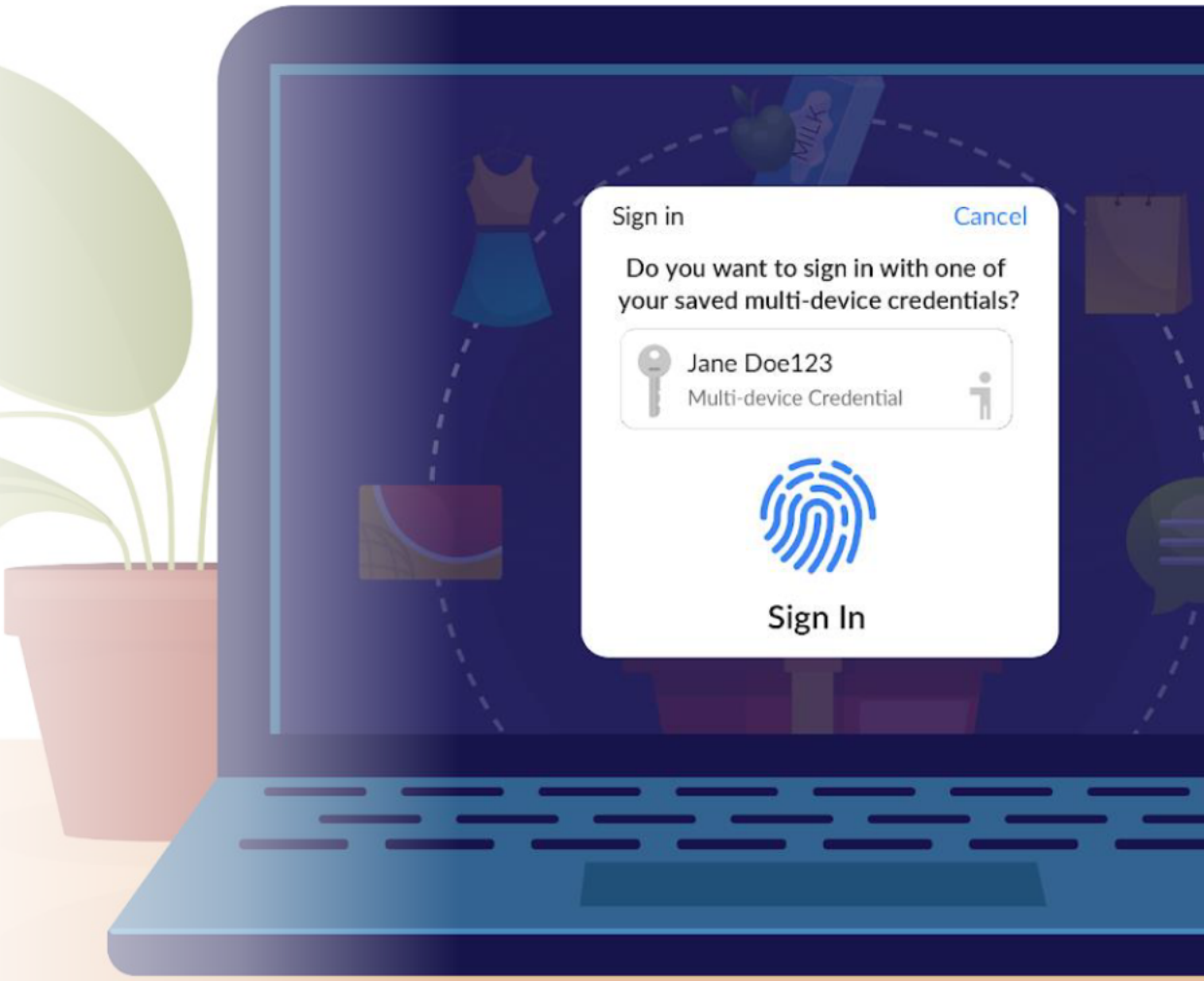
  端末買い換え時の初期設定

- Addresses usability AND security challenges with account recovery

  いわゆるアカウントリカバリーへの対処

- Anticipate support in leading device platforms starting this year

  OSベンダーによる年内の対応開始に期待



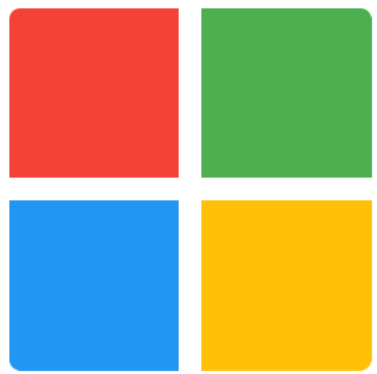
マルチデバイス対応FIDO認証資格情報（クレデンシャル）

- より一層FIDO認証、そしてパスワードレス認証の普及を見据えたとき、機種変更の際に必要となるサービス提供者毎の再登録（FIDO認証資格情報の再設定）などに懸念が示されていた。これを解決するため、マルチデバイス対応FIDO認証資格情報をOSプラットフォーム提供者のクラウドに保存し、（最近のスマートフォンの機種変更の際にはクラウドを経由して多くの設定が移行するように）FIDO認証に関する設定も移行するようにするもの。
  - 従前の考え方を継承し、FIDO認証資格情報があくまでもデバイスに紐づいているようにする方法として、「デバイスに紐づいた暗号鍵」を使うオプションも残される。

ホワイトペーパー「さまざまなユースケースへのFIDOの対応について」より（国際版（英語） 2022年3月17日、国際版の日本語訳 4月22日）

Platform Commitments

New capabilities expected to become available in 2022 and 2023



FIDOアライアンスとしてのパスワードレス認証のさらなる推進

Apple、Google、MicrosoftがFIDO標準のサポート拡大にコミット、パスワードレス認証の普及を促進

FIDOアライアンスと各社からグローバルで同時にニュースリリース

2022年5月5日、カリフォルニア州マウンテンビュー – すべての人にとってウェブをより安全で使いやすいものにするための共同の取り組みとして、Apple、Google、Microsoftは本日、FIDOアライアンスとWorld Wide Web Consortium（以下、W3C）が策定した共通のパスワードレス認証のサポートを拡大する計画を発表しました。この新機能により、ウェブサイトやアプリケーションは、コンシューマーに対してデバイスやプラットフォームを問わず一貫して、安全かつ容易なパスワードレス認証を提供できるようになります。

また、このニュースリリースに先立って3月17日、ホワイトペーパー「さまざまなユースケースへのFIDOの対応について」も発表

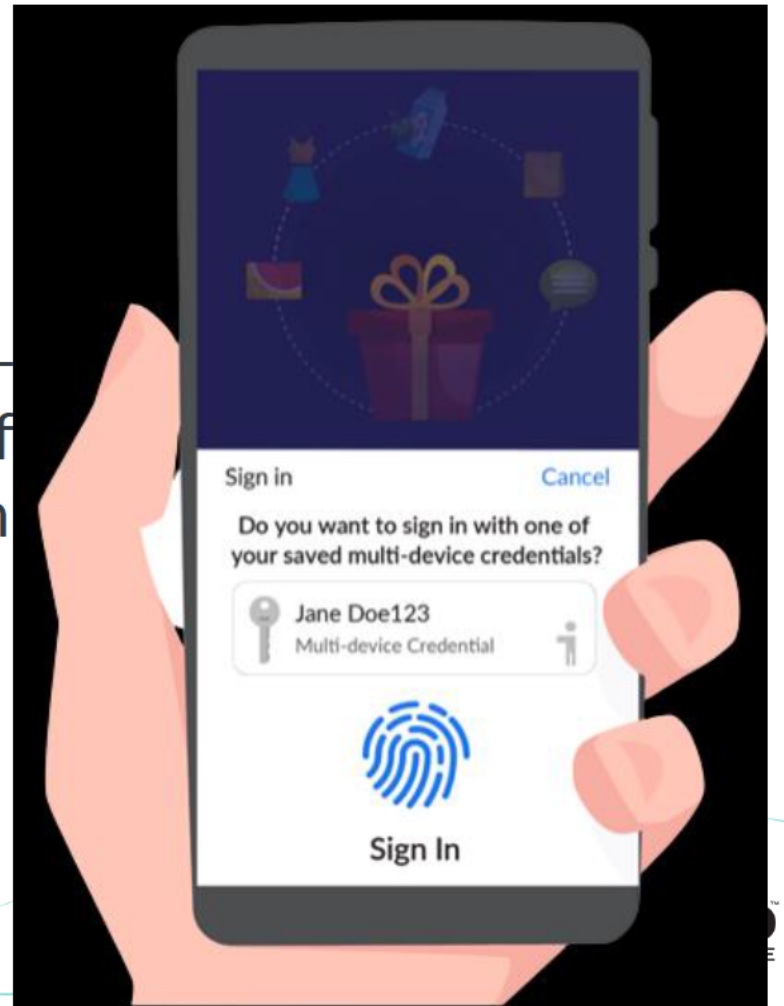
https://fidoalliance.org/charting-an-accelerated-path-forward-for-passwordless-authentication-adoption-jp/?lang=ja

New capabilities enabling passwordless sign-ins

パスワードレス認証の推進を加速するさらなる新機能

- Allow users to automatically access their FIDO sign-in credentials (referred to by some as a “passkey”) on all their devices, even new ones, on a single platform without having to enroll for every account.
  利用者のすべての端末でFIDO認証できる（“Passkey”と呼ばれる場合もある）

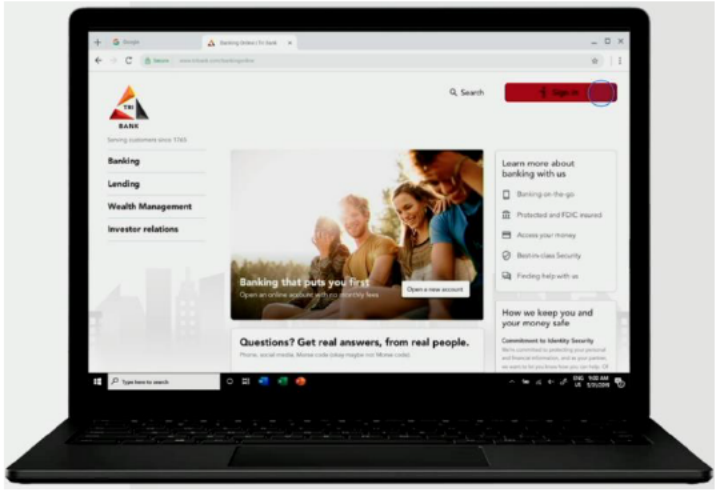
- Enable users to use FIDO on their mobile device to sign-in to an app or website on a nearby device, regardless of the OS platforms and browsers that the two devices run
  - e.g., sign-in on the Google Chrome browser on Microsoft Windows using FIDO keys stored on an Apple phone.
    利用者のモバイルデバイスで近くにある利用者のその他のデバイスにログインできる（例えば、iPhoneでWindows PCにログインできる）



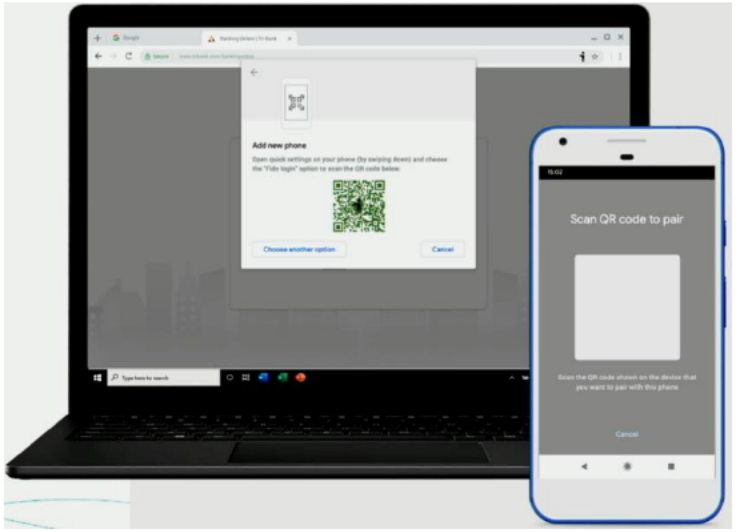
caBLE（cloud assisted Bluetooth Low Energy）

- スマートフォンを認証器として活用する取り組みの議論も（名称含めて）進行中
  利用者が所持するデバイスの近傍にもう一つの対象デバイスが存在していることが重要

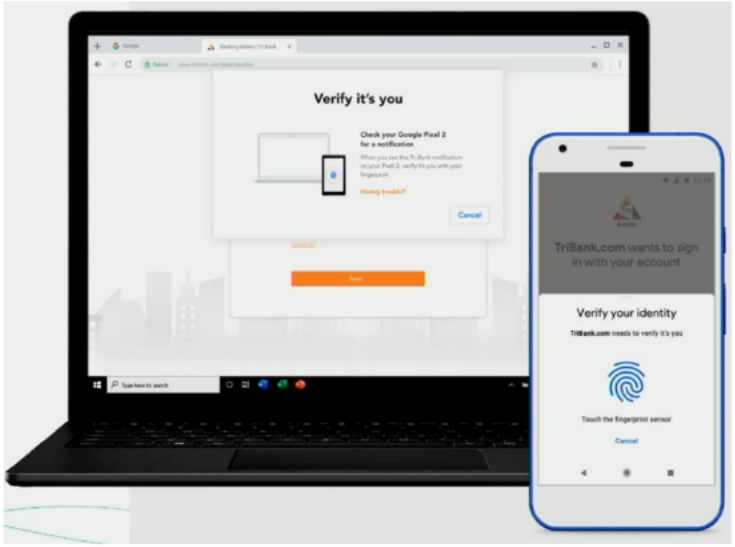
→ デスクトップPCでサインイン



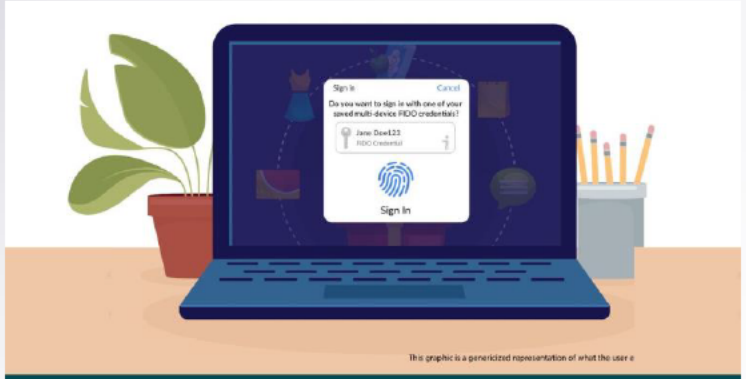
→ 認証用QRコードをスマートフォンで読み取り



→ スマートフォンで本人確認を行い、認証成功



https://github.com/w3c/webauthn/pull/909



This graphic is a genericized representation of what the user e

Multi-device FIDO Credentials
noun

1. *FIDO credentials that are backed up, allowing users to restore the credential to, and use it from, another device.*

Scalability
FIDO credentials are available to users whenever they need them—even if they replace their device.

User Experience
The user experience will be familiar and consistent across many of the user's devices using the same simple action that consumers take multiple times each day to unlock their devices.

Security
Proven resistance to threats of phishing, credential stuffing and other remote attacks. No need for passwords as an alternative sign-in or account recovery method.

This graphic is a genericized representation of what the user experience may be.

Introducing Multi-device FIDO Credentials

Accelerating the Availability of Simpler, Stronger Passwordless Sign-Ins

This graphic is a genericized representation of what the user experience may be.

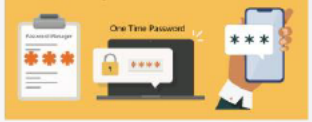
Passwords are a problem.

Knowledge-based | Hassle to use and remember | Easy to phish, harvest, replay

89% of organizations experienced a phishing attack in the past year.*

*HYPR, 2022 State of Passwordless Security Report

Common solutions don't address the security problem and/or are not usable enough to change consumer behavior.

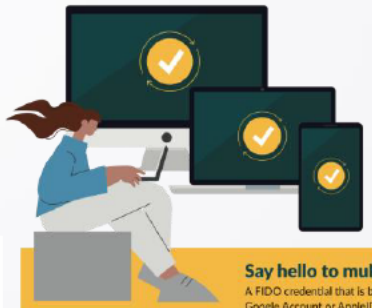


THE SOLUTION NEEDS TO BE STRONGER AND EASIER THAN USING A PASSWORD.

FIDO AUTHENTICATION IS THE WORLD'S ANSWER TO THE PASSWORD PROBLEM.

FIDO Provides A Simpler User Experience With Phishing-Resistant Security.

WHAT IS FIDO? | HOW FIDO WORKS | FIDO SPECIFICATIONS



But how do users sign-in with fido across all of their different devices?

Typically, users have to enroll with FIDO on every device. With the introduction of multi-device FIDO credentials (referred to by some as a "passkey"), there's a new option for users to access their FIDO sign-in credentials on many of their devices, even new ones, without having to re-enroll every account.

Say hello to multi-device FIDO credentials!

A FIDO credential that is backed up (usually to the user's platform account; e.g., Google Account or AppleID), allowing users to restore the credential to, and use it from, another device. From a user experience standpoint, this will be very similar to how one interacts with a password manager today to help them securely enroll and sign into websites – only it will be far more secure.

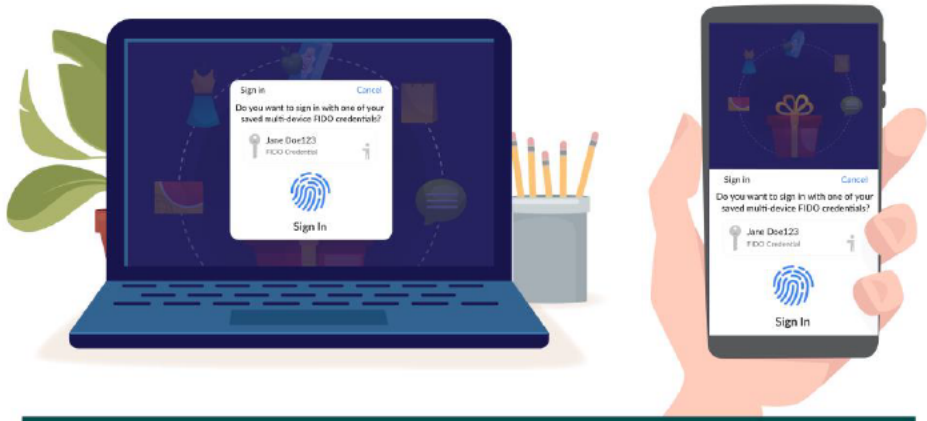
Here's what this means for...

User Experience
The user experience of signing in will become consistent across many of the user's devices – a simple verification of their fingerprint or face, or a device PIN, the same simple action that consumers take multiple times each day to unlock their devices.

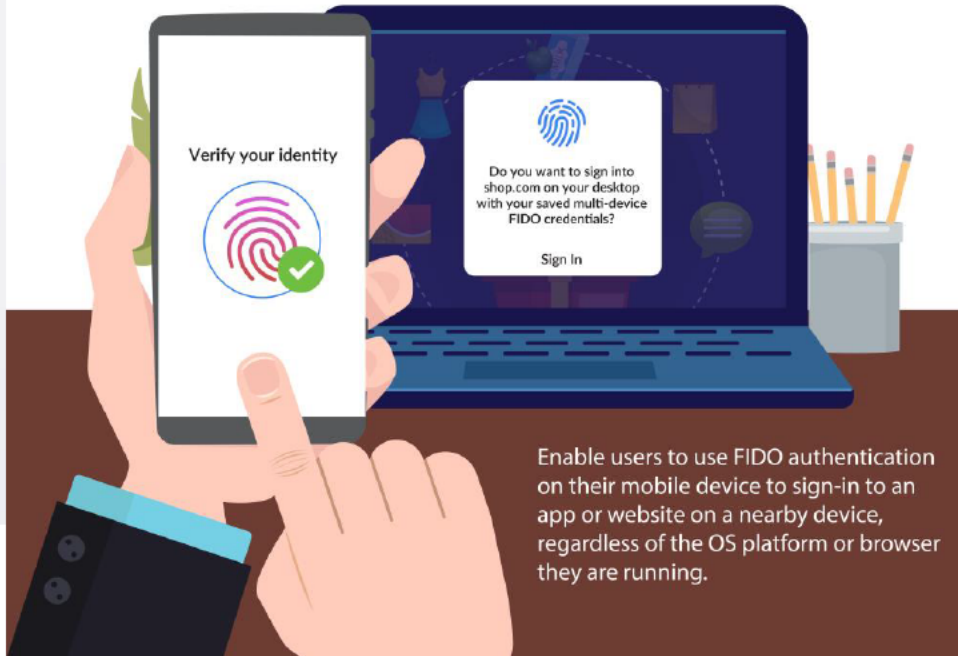
Security
Multi-device credentials are based on FIDO Authentication, which is proven to be resistant to threats of phishing, credential stuffing and other remote attacks. Also, service providers can offer FIDO credentials without needing passwords as an alternative sign-in or account recovery method.

Scalability
Until now, users were required to enroll their FIDO credentials for each service on each new device, typically with a password for that first sign-in. With multi-device FIDO credentials, the credentials are available to users whenever they need them—even if they replace their device.

User Experiences with Multi-device FIDO Credentials



Allow users to automatically access their FIDO sign-in credentials (referred to by some as a "passkey") on many of their devices, even new ones, without having to re-enroll every account.



Enable users to use FIDO authentication on their mobile device to sign-in to an app or website on a nearby device, regardless of the OS platform or browser they are running.

This graphic is a genericized representation of what the user experience may be.

FIDO Japan WGは7年目を迎えました！

※ 国内外を問わず、FIDOアライアンスメンバーの参加数

10社 (※) → **25社** → **55社**

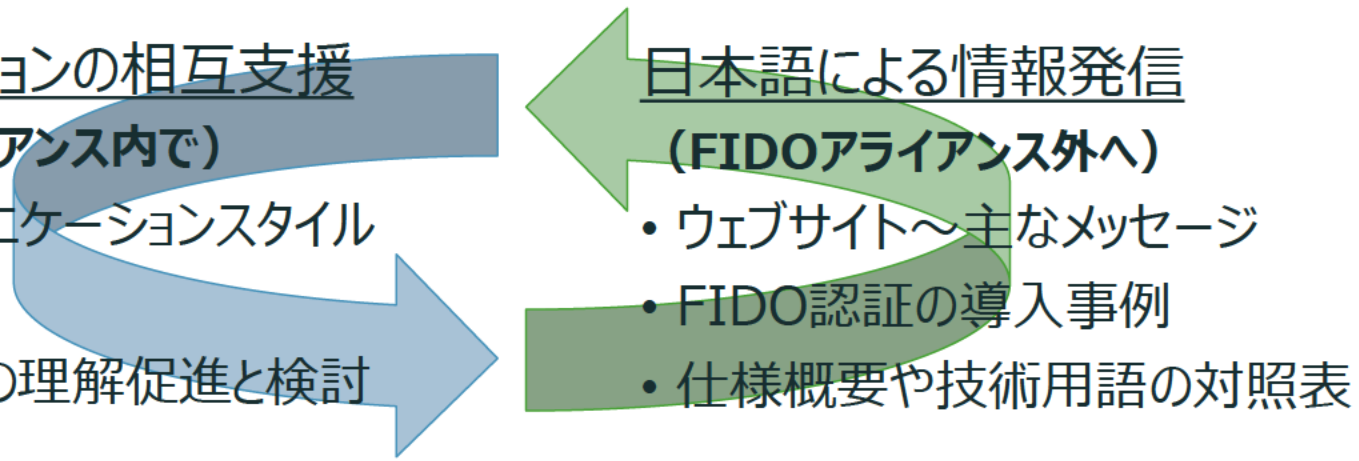
2016.10　　2017-2018　　2022.5

海外企業で国内に拠点を持つメンバー企業の積極的な参加、
スタートアップをはじめとするアソシエイトメンバー企業の参加などによる

※ 発足・運営開始時 10社、発足発表時 11社

FIDO Japan WG ミッションと主な活動

FIDOアライアンスのミッション～パスワードに代わるシンプルで堅牢なFIDO認証モデルの展開・推進～を日本国内でより効果的に実践する（2016年10月～）



コミュニケーションの相互支援

（FIDOアライアンス内で）

- 言語とコミュニケーションスタイル
- 時差
- FIDO認証の理解促進と検討

日本語による情報発信

（FIDOアライアンス外へ）

- ウェブサイト～主なメッセージ
- FIDO認証の導入事例
- 仕様概要や技術用語の対照表

座長　森山　光一（NTTドコモ）
副座長　伊藤　雄哉（ヤフー）
板倉　景子（楽天グループ）

FIDO Japan WG リーダーシップ

座長・副座長・各SWG・TFのリードを担当

APACマーケット開発マネジャー 土屋 敦裕

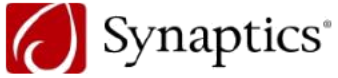
マーケティングSWG

技術・導入SWG

アカウントリカバリTF

翻訳TF

FIDO Japan WGメンバー



AuthenTrend　株式会社アクセル　Capy株式会社　株式会社イードクト　エクスジェン・ネットワークス株式会社　Fingerprint Cards AB
株式会社アイピーキューブ　株式会社インターナショナルシステムリサーチ　ジェイズ・コミュニケーション株式会社　日本情報システム株式会社
株式会社ヌーラボ　OSS Tech株式会社　株式会社Quad　株式会社セシオス　WiSECURE Technologies Corporation　WinMagic, Inc.　xID株式会社

The Future of User Authentication

FIDO認証は
パスワード課題を解決します

FIDO Authentication is the industry's answer to the password problem

STRONGER
Phishing resistance prevents account takeover

FASTER
Reduces sign in times and increases login success rates

PRIVATE
Credentials and biometrics never leave device

CONVENIENT
Leverages technologies built into everyday consumer devices

SUPPORTED
Built-in support on leading browsers and platforms

FITS ALL USE CASES
Native app and web support allows scalable deployments

INDUSTRY BACKED
FIDO represents the efforts of the world's largest companies

IN MARKET
Leading service providers are using FIDO today

EDIX関西に出展します　6月15日(水)～17日(金)

EDIX関西（6/15-17）@インテックス大阪
FIDOブース：４－２６

EDIX東京（5/11-13）のFIDOブース

おわりに

- パスワード課題を解決するFIDO（ファイド）認証～パスワードレス認証
- あらゆるオンライン認証シーンでフィッシング詐欺対策に待ったなし
- 「所持」を基本としたFIDO認証に基づく「パスワードレス認証」は
  利用者の目線に立って、セキュリティと使い勝手の高いレベルでの両立を
  可能にする業界の切り札
  - ✓ さまざまな懸念も“業界の連携”で解決を図ってきました！
- ぜひ、業界をあげて、パスワード課題の対策を進めて参りましょう！！

fido ALLIANCE | simpler stronger authentication

ご清聴、ありがとうございました！

2022年6月2日

森山 光一

FIDOアライアンス 執行評議会メンバー・ボードメンバー・FIDO Japan WG座長
株式会社NTTドコモ マーケティングプラットフォーム推進部 セキュリティサービス担当部長 兼 経営企画部 経営企画担当部長

fido ALLIANCE

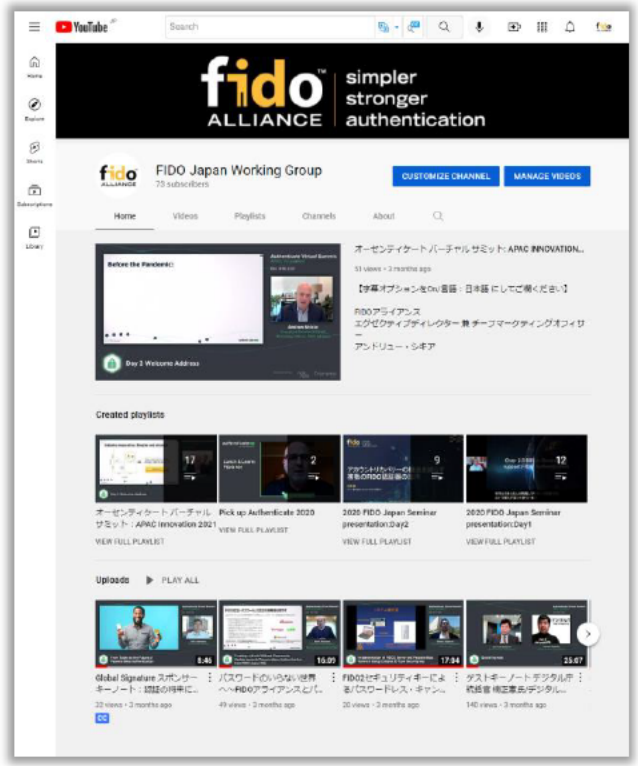
ご参考：日本語による情報発信

ウェブサイト

https://fidoalliance.org/?lang=ja

ニュースレター

YouTube
FIDO Japan Working Group



https://www.youtube.com/channel/UCFEBSesA5GSi9Vz-ESTopiQ

お問い合わせ先：info@fidoalliance.org