デバイスWebコンソーシアム　第４回技術WG

指紋認証と「FIDO」について

2016年6月29日

株式会社　ディー・ディー・エス
事業支援本部　FIDO事業推進部
井上　幸三　inoue_kozo@dds.co.jp

〒103-0028
東京都中央区八重洲1-8-5　新槇町ビル別館第二

弊社ご紹介

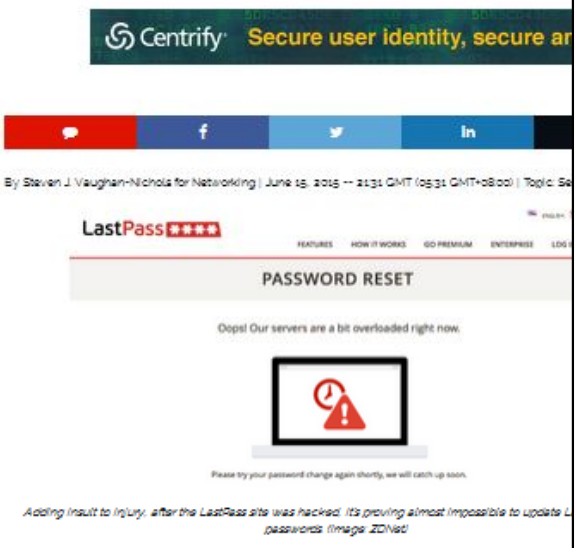
・『誰でも使える』『より使いやすい』指紋認証システムを個人情報の管理するユーザー向けに提供
・「ICカード（ID）」＋「指紋認証（パスワード）」によるアクセスコントロールを提供

・2014年4月、FIDOアライアンスに加入
・2014年10月、FIDO東京セミナー事務局
・NokNokLabs社販売代理店
(https://byebye.pw/)

「不正アクセス」の原因は、パスワード

Password site LastPass warns of data breach

LastPass was successfully attacked last Friday. The company claims that your passwords should be safe. Nevertheless, they are requesting you to update your master passwords.



Adding insult to injury, after the LastPass site was hacked, it's proving almost impossible to update L passwords (Image: ZDNet)

Even LastPass, a cloud-based password security site, isn't immune to data breach

The company's chief executive Joe Siegrist said in a blog post that account email password reminders, server per user salts, and authentication hashes were compr

But, he said, the company has "found no evidence that encrypted user vault data nor that LastPass user accounts were accessed."

As for the stolen data, Siegrist wrote:

日本年金機構の個人情報流出について

1. 事象の内容

日本年金機構において、職員の端末に対する外部からのウイルスメールによる不正アクセスにより、当機構が保有している個人情報の一部が外部に流出したことが、5月28日に判明しました。現時点で流出していると考えられるのは、約125万件です。

流出した情報	件数
二情報（基礎年金番号、氏名）	約3．1万件
三情報（基礎年金番号、氏名、生年月日）	約116．7万件
四情報（基礎年金番号、氏名、生年月日、住所）	約5．2万件
合計	約125．0万件

なお、現在のところ、基幹システム（社会保険オンラインシステム）への不正アクセスは確認されていませんが、さらに精査中。

日本年金機構
Japan Pension Service

2. 事象の原因

電子メールのウイルスが入った添付ファイルを開封したことにより、不正アクセスが行われ、情報が流出したものと認められます。

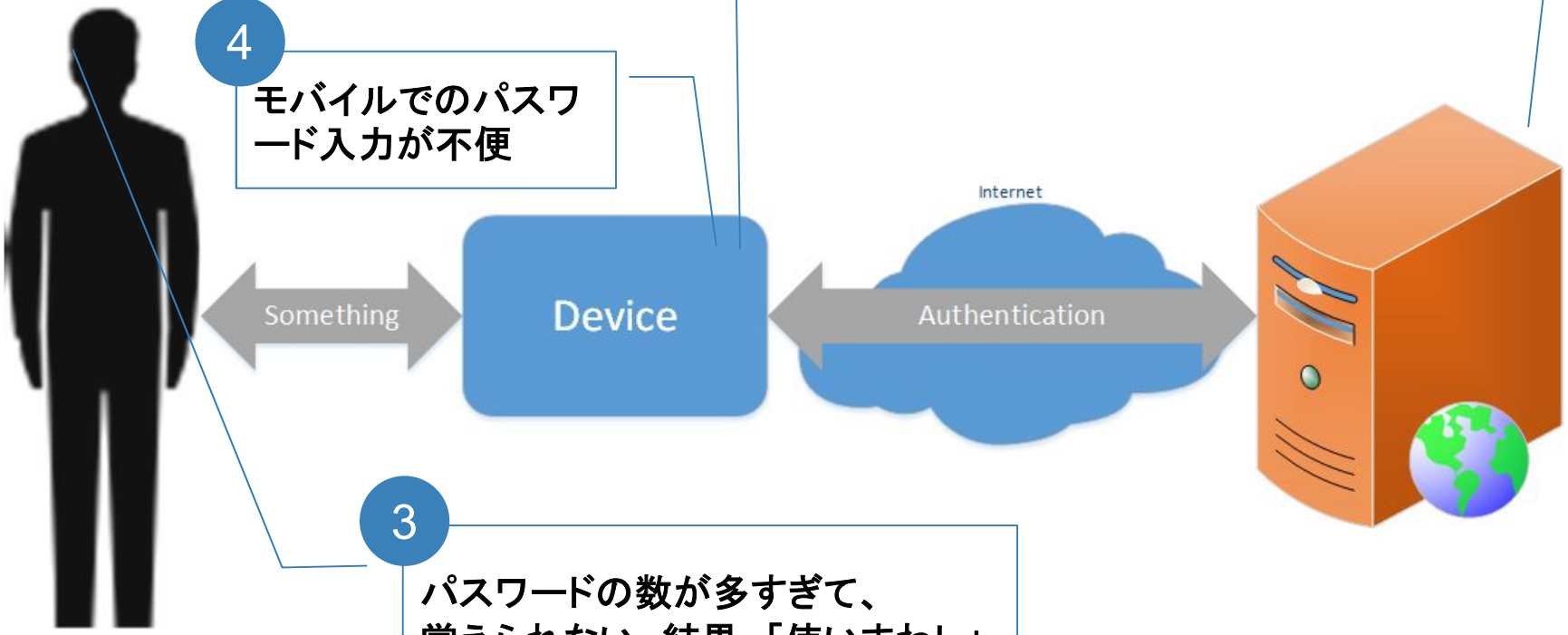
（引用元）　http://www.zdnet.com/article/lastpass-password-security-site-hacked/
http://www.nenkin.go.jp/oshirase/taisetu/2015/201506/20150601.html

「パスワード」の問題

2
パスワードを、知らないアプリや
Webサイトへ入力
（フィッシング）

1
サーバーから認証情報の
漏洩の可能性

4
モバイルでのパスワ
ード入力が不便

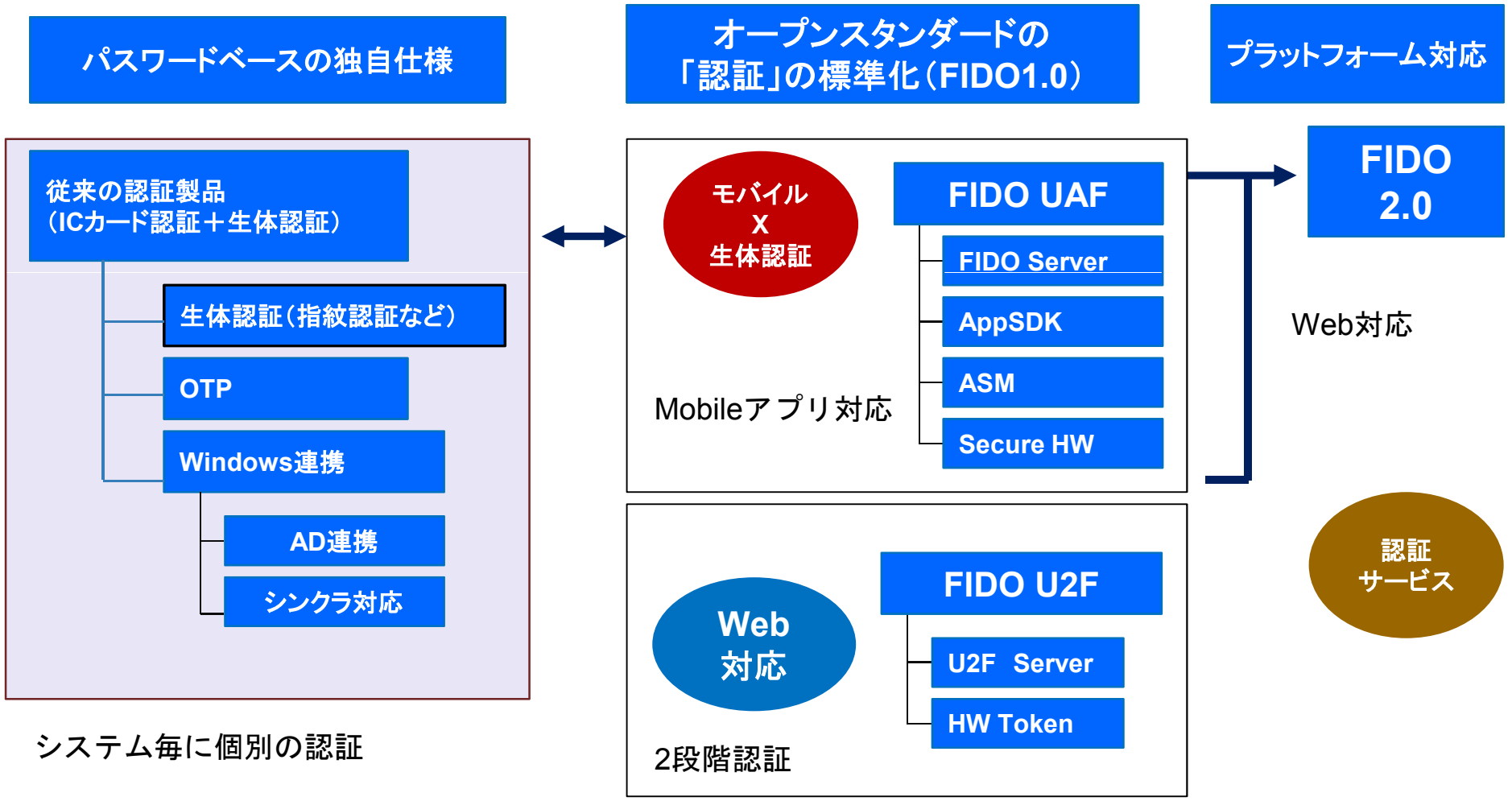


3
パスワードの数が多すぎて、
覚えられない。結果、「使いまわし」
リスクの増大や、利用の中止

（参考：FIDO UAFチュートリアルを元に邦訳）

従来の認証システムとFIDOとの関係性

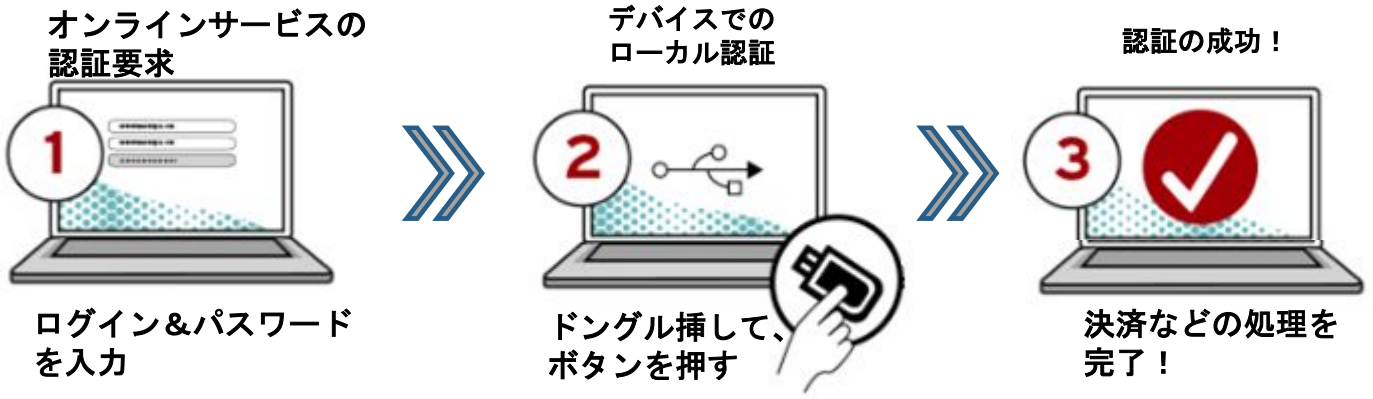
・従来の「生体認証」とFIDOとは、何が違うのでしょうか。
・特定の製品の機能ではなく、オープンスタンダードの規格
→　生体情報の管理を「デバイスから出さない」



２つのFIDOプロトコル

１． UAF standards：パスワードレス・エクスペリエンス

２． U2F standards：セカンド・ファクタ・エクスペリエンス



（参考：FIDO 1.0 Specリリース資料）

FIDO （UAF）のサービス実装

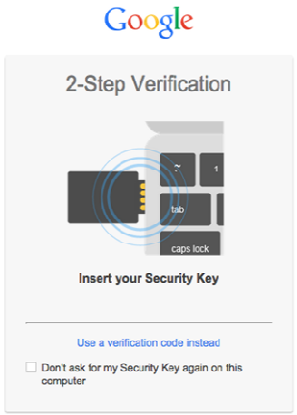
2014年4月、PayPal社は、指紋センサー搭載のサムソンGalaxy S5で、オンライン決済サービスを提供。端末に搭載されているFIDO Ready™のソフトウェアを利用。指紋センサーとPayPal社のクラウドサービスとの安全な通信を行っています。2014年7月、アリババ社も、Samsung Galaxy S5を利用した、FIDO仕様のオンライン決済サービスを開始。

（参考： FIDO101資料）

FIDO （U2F）のサービス実装

2014年10月、Googleは ChromeブラウザでのU2Fサポートを発表。同時に、Yubico社とPlug-Up社は、公開鍵ハードウェアデバイスのFIDO U2F セキュリティキーを紹介。セキュリティキーを利用して、FIDO U2Fプロトコルベースの強力な認証方式による、高いセキュリティを実現。

- グーグルアカウントの利用ユーザー向けの強力な2段階確認
- サービスの拡大が簡単
- ウィンドウズやOSX、Linux上で、シームレスに動作する。
- セキュリティキーは、パスワードなどの暗号化する機能を持つ。
- 各アプリケーション毎に、ユニークな公開鍵と秘密鍵のキーペアを作成する。



fido U2F Ready

yubico

（参考： FIDO101資料）

- 動画紹介

- PayPal（UAF）
- Yubico（U2F）

（引用元）PayPal　https://www.youtube.com/watch?v=c1aYFjHVFA8
Yubico　https://www.yubico.com/why-yubico/for-businesses/authentication-solutions/gov-uk-verify-digidentity/

FIDOボードメンバー

・メンバーは、「ボード」「スポンサー」「アソシエイト」の3種類
→　スポンサー以上で、ワーキンググループの参加が可能。
・テクニカルやマーケティングワーキンググループの活動を行っている。

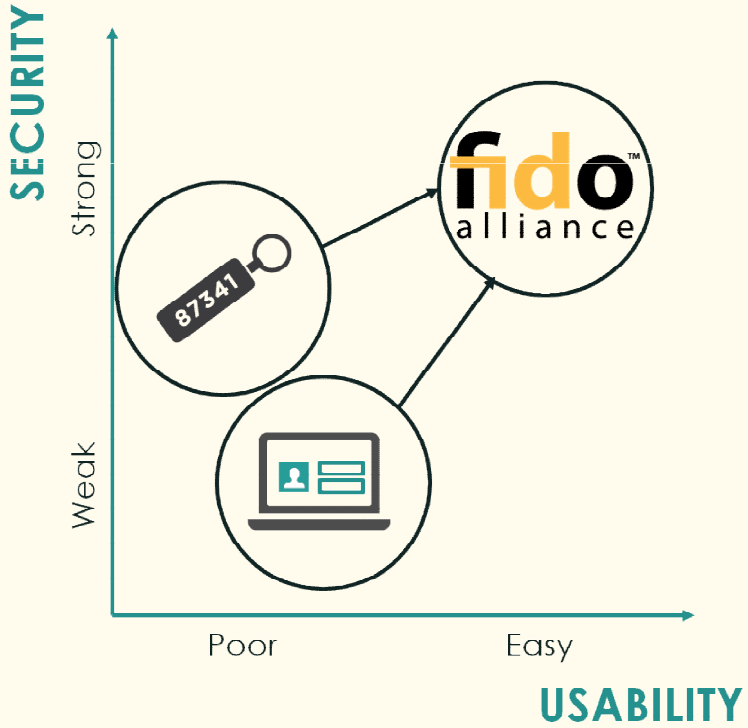
（参考：FIDO アライアンス説明資料より抜粋）

FIDO101 ：東京セミナー@東京電機大学（第1回）

・FIDO創設のきっかけ：PayPalサービスへの指紋認証の提案から
・家族からの意見で、他のサイトでも使いたい。→　「スタンダードベース」の認証が必要

パスワードに取って代わる「FIDO認証」

・「Password 」は、「bearer token」（知っているトークン）・・・盗まれる
・「user-binding token」（ユーザーに紐づいたトークン）を採用し、
使い易さとサービスの信頼性を両立。
→　初期登録で利用した認証情報が一致しないと、認証しない。（フィッシング防止）

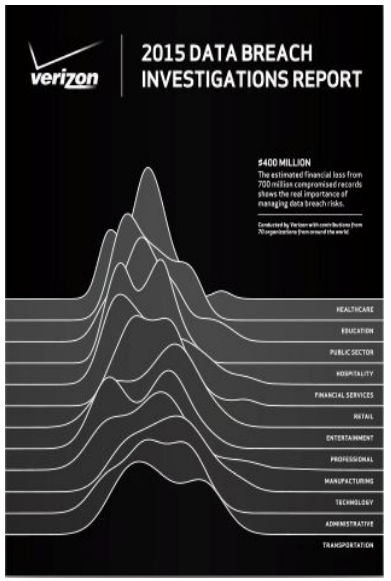


（参考：FIDO アライアンス説明資料を元に作成）

パスワード認証の限界

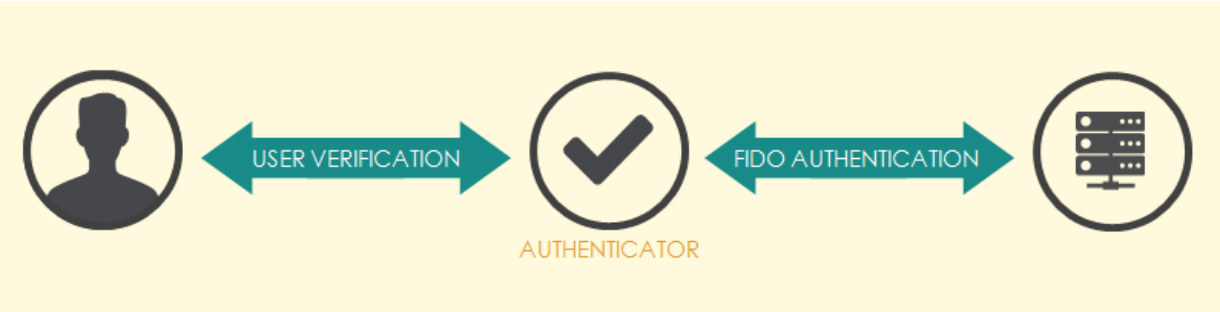
“情報漏洩の95%は、顧客のデバイスからクレデンシャル（認証情報）を入手し、ウェブアプリにログイン。”
Verizon DBIR, 2015

“情報漏洩の61%は、クレデンシャルの紛失・盗難が原因。”
Javelin Research, The Consumer Data Insecurity Report.



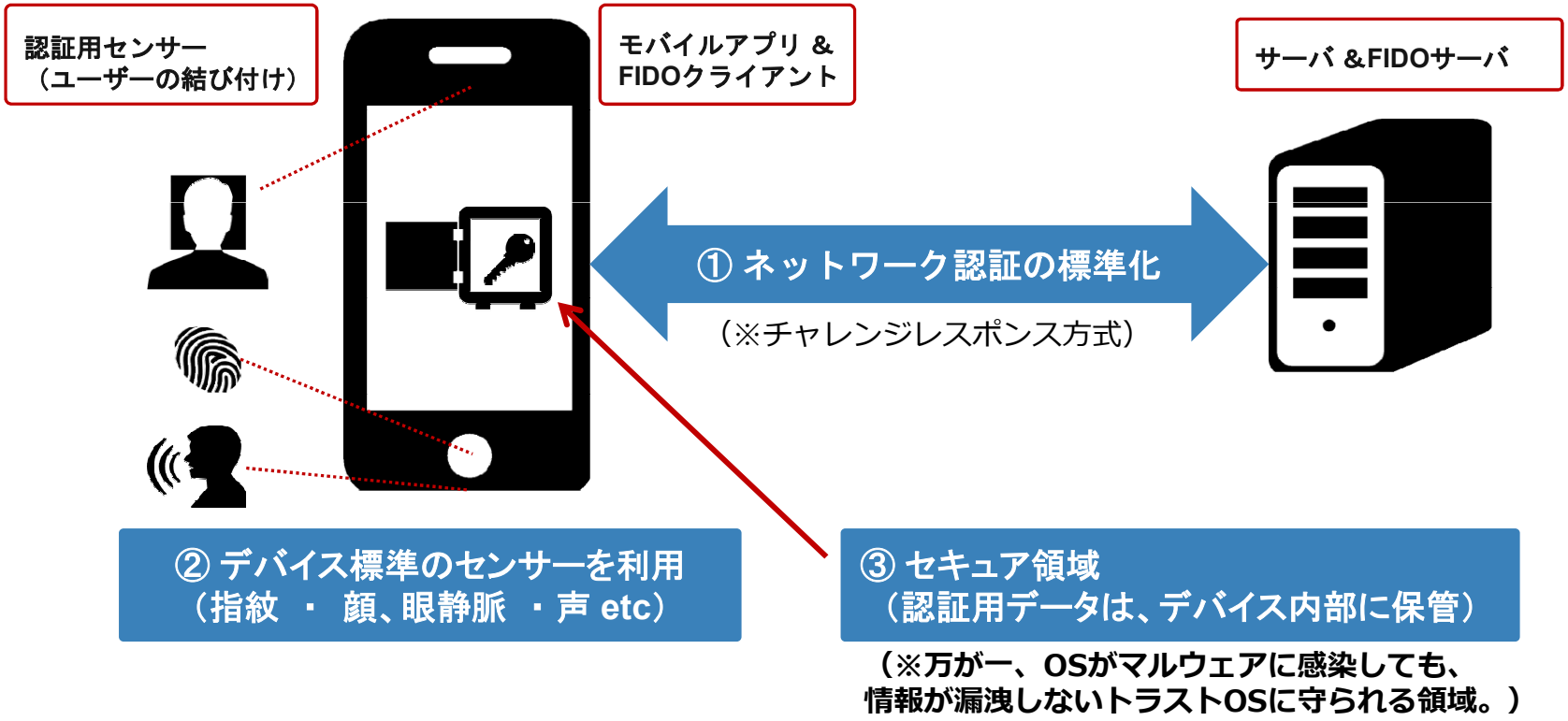
FIDOのコンセプト

・パスワード認証に代わる認証のスタンダードを提唱。
・特定のデバイスに限定しない、標準仕様化を行う。
・「モバイル機器のローカル認証」と「デバイスのサーバ認証」を分離し、サーバ認証にパスワードを利用しない。
→　中間者攻撃への対応



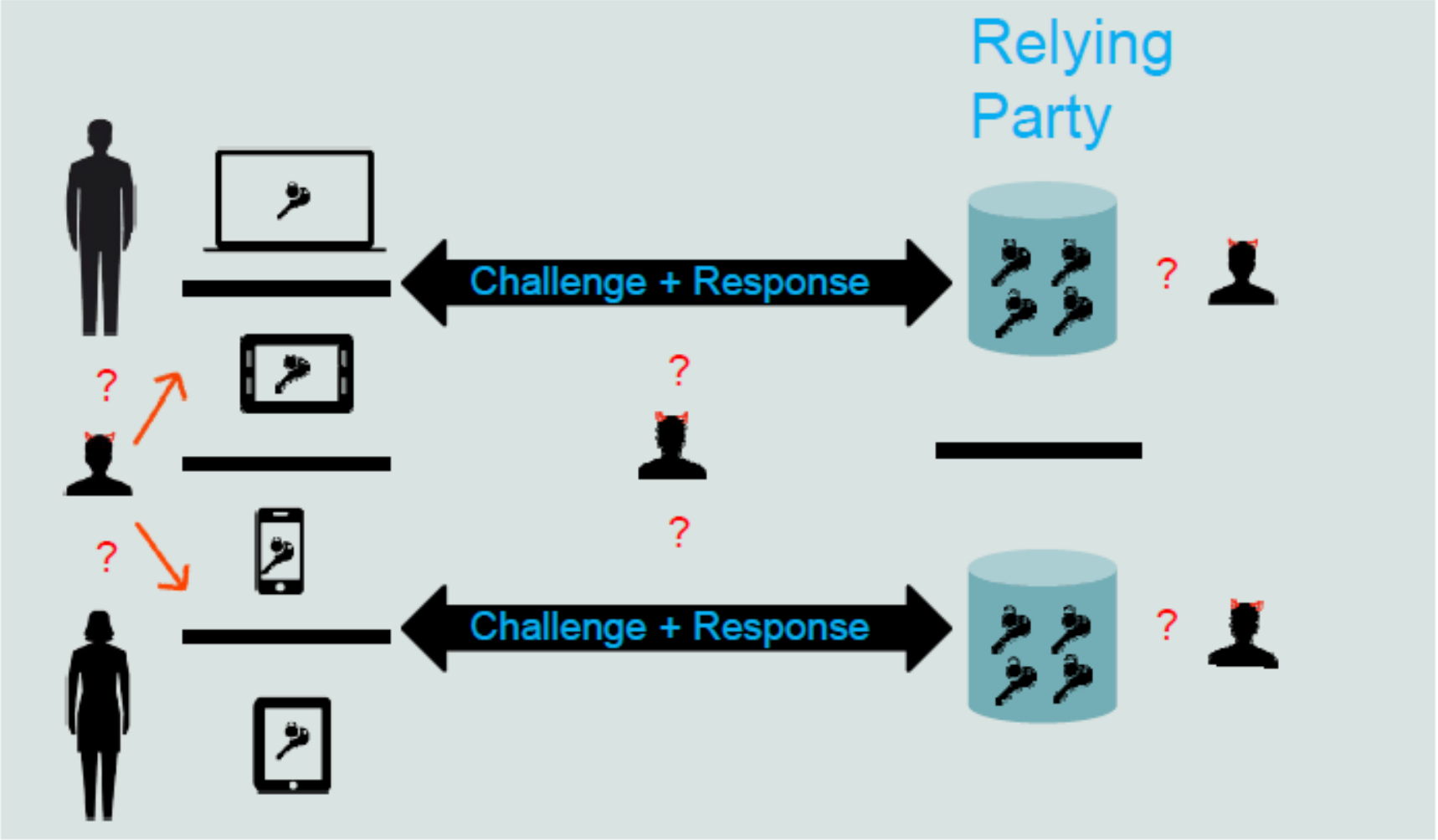
FIDO認証のコンセプト

・各ベンダーは、FIDO仕様書にのっとり、「FIDOサーバ」「クライアント」「認証ツール」を作成。認証精度、セキュリティ強度は、仕様に含みません。
・FIDOアライアンスは、各カテゴリの相互通信テストを行い、製品認定を行う。



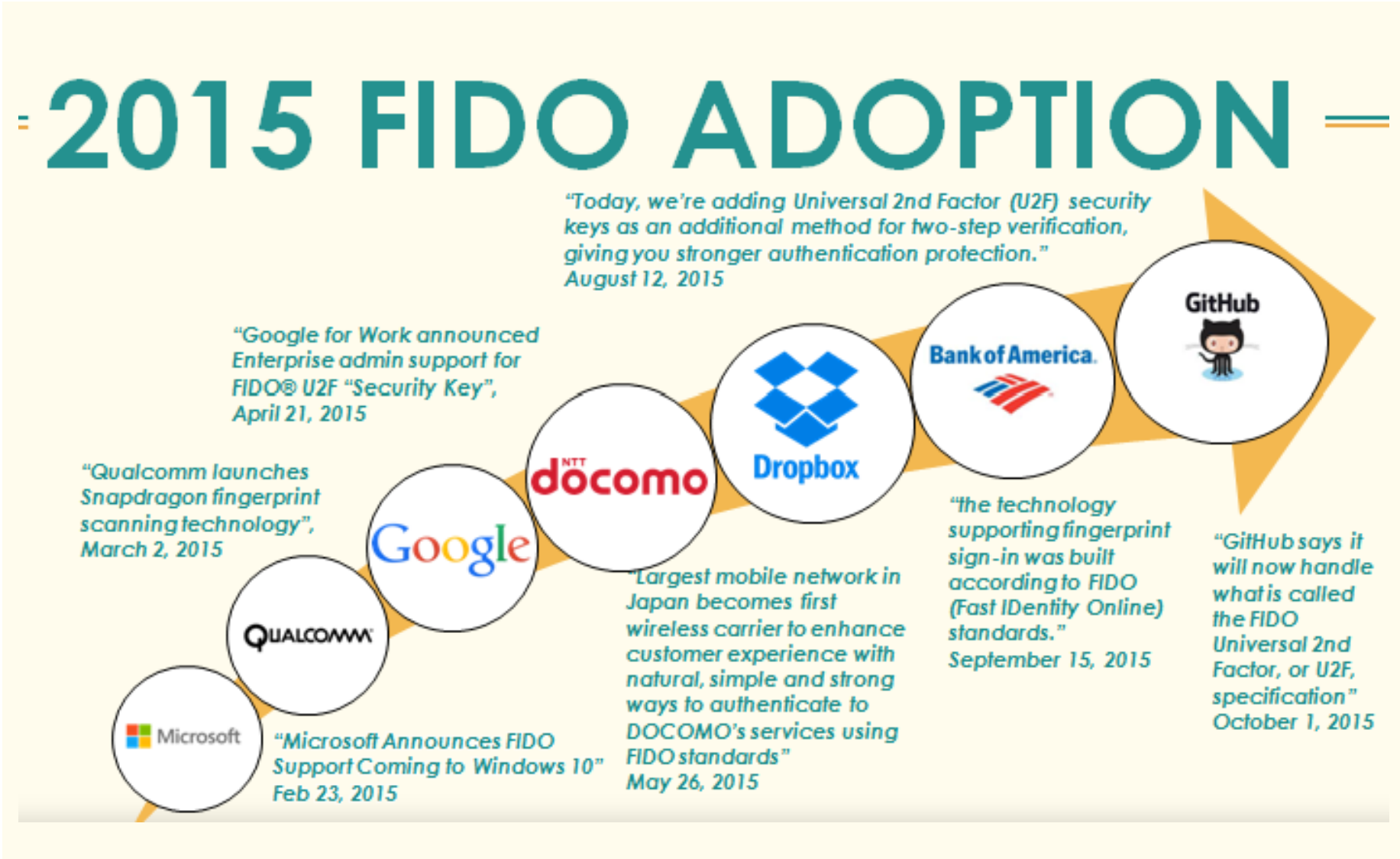
（参考：NNL社FIDO 説明資料より）

FIDO認証の効果



（参考：NNL社FIDO 説明資料より）

FIDO採用サービスの拡大（2015年）



（参考：FIDO アライアンス説明資料）

FIDO対応デバイス（OEMs）

Samsung

S5, Mini

Alpha

Note 4, 5

Note Edge

Tab S, Tab S2

S6/S7, S6/S7 Edge

Sharp
Aquos Zeta

Sony
Experia Z5

Fujitsu
Arrows
(Iris Biometrics)

LG
V10 & G5

Huawei
Mate 8

Lenovo
P1

Lenovo
K52

Lenovo
ThinkPad

Supported iOS Fingerprint Devices

NTT docomo

Bank of America

iPhone 5s

iPhone 6, 6+

iPhone 6s, 6s+

iPad Air 2, Mini 3

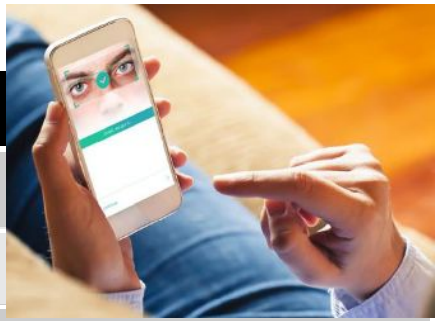
iPad Mini 4

iPad Pro

（参考：FIDO アライアンス説明資料）

FIDO対応製品（認証ツール）

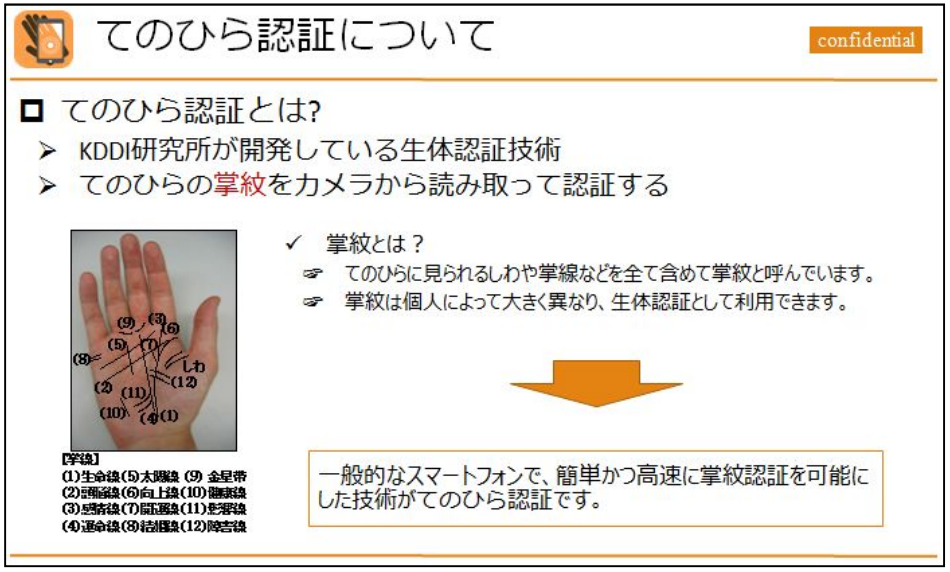
・スマートフォンに指紋センサが付いていない場合、何を利用するか。
→カメラやスピーチ（ボイス）を利用した認証ツール



方式	ベンダー	環境	対応ハードウェア	その他
ソフトピン	NokNokLabs社	Android	不要	
顔＆声	センサリー社	Android	フロントカメラ、マイク	マルチモード
眼の静脈	EyeVerify社	Android	フロントカメラ	

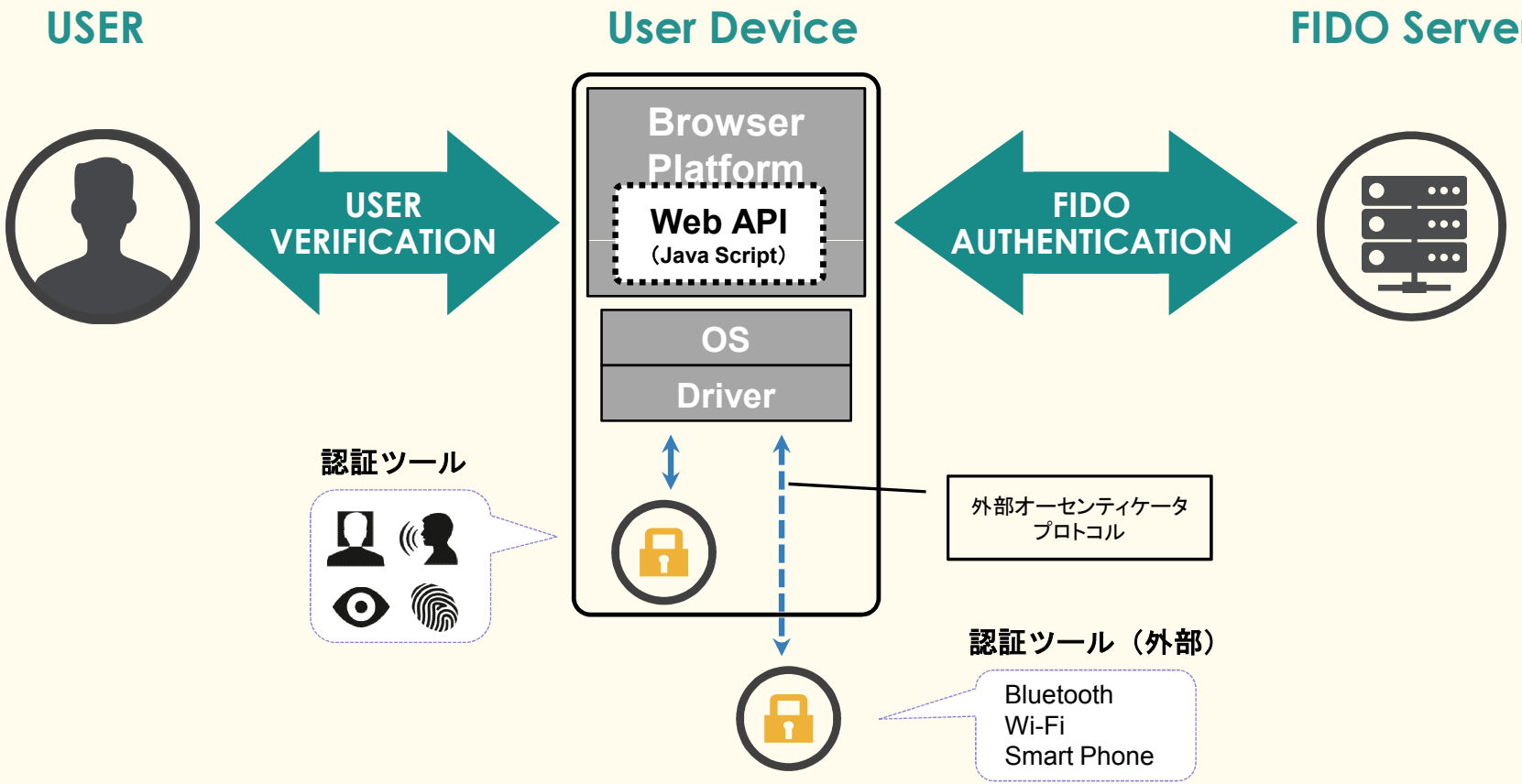
（認定製品一覧）https://fidoalliance.org/certification/fido-certified/

■ KDDI手のひら認証がFIDO認定取得



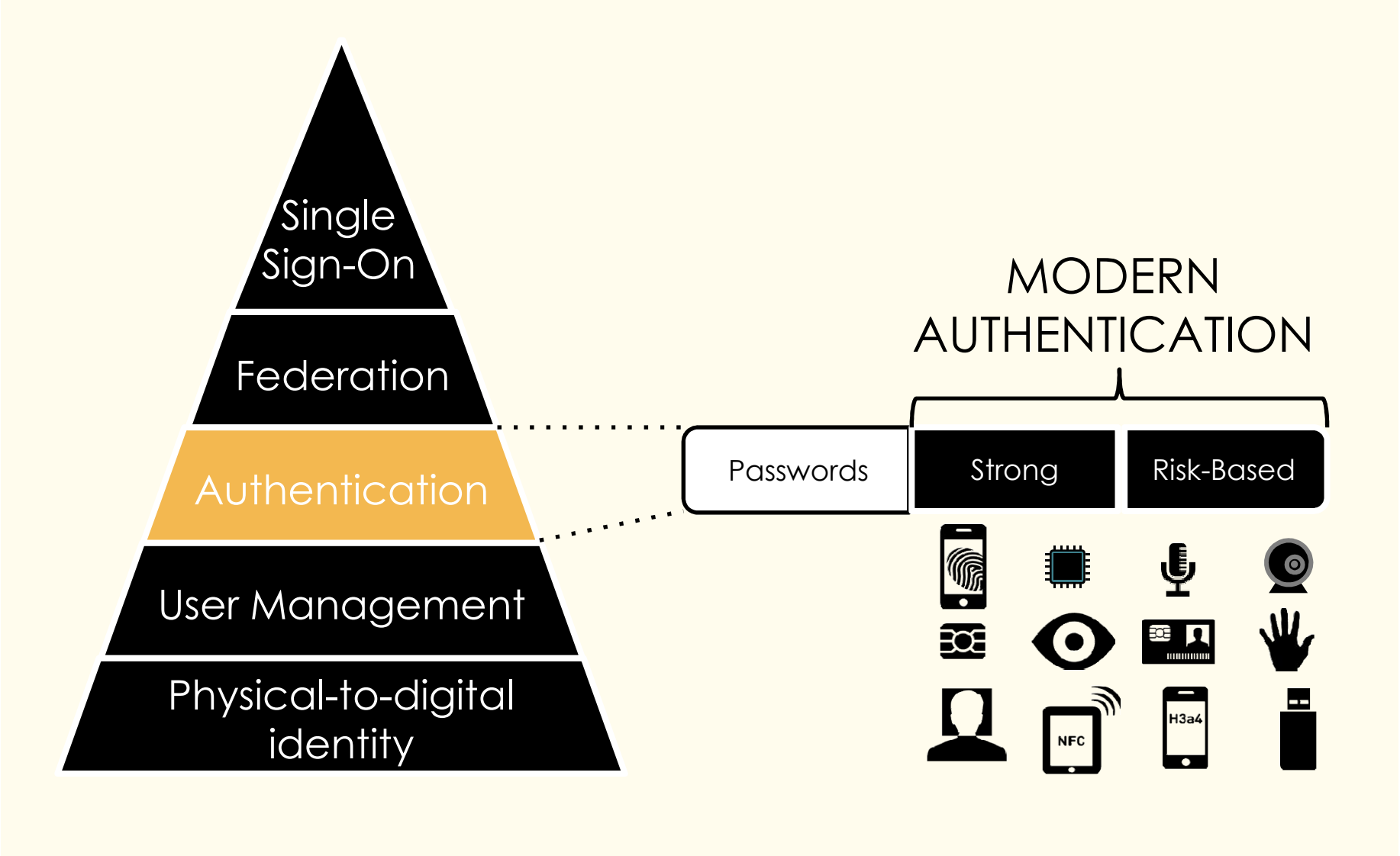
Web プラットフォームの標準へ（FIDO 2.0）

・FIDOアライアンスより、WebAPIの仕様をW3Cに提供。Web認証標準の仕様策定中。
・仕様化され、各ブラウザの標準機能に搭載されれば、各認定デバイスが利用可能に。



（参考：FIDO アライアンス説明資料を元に作成）

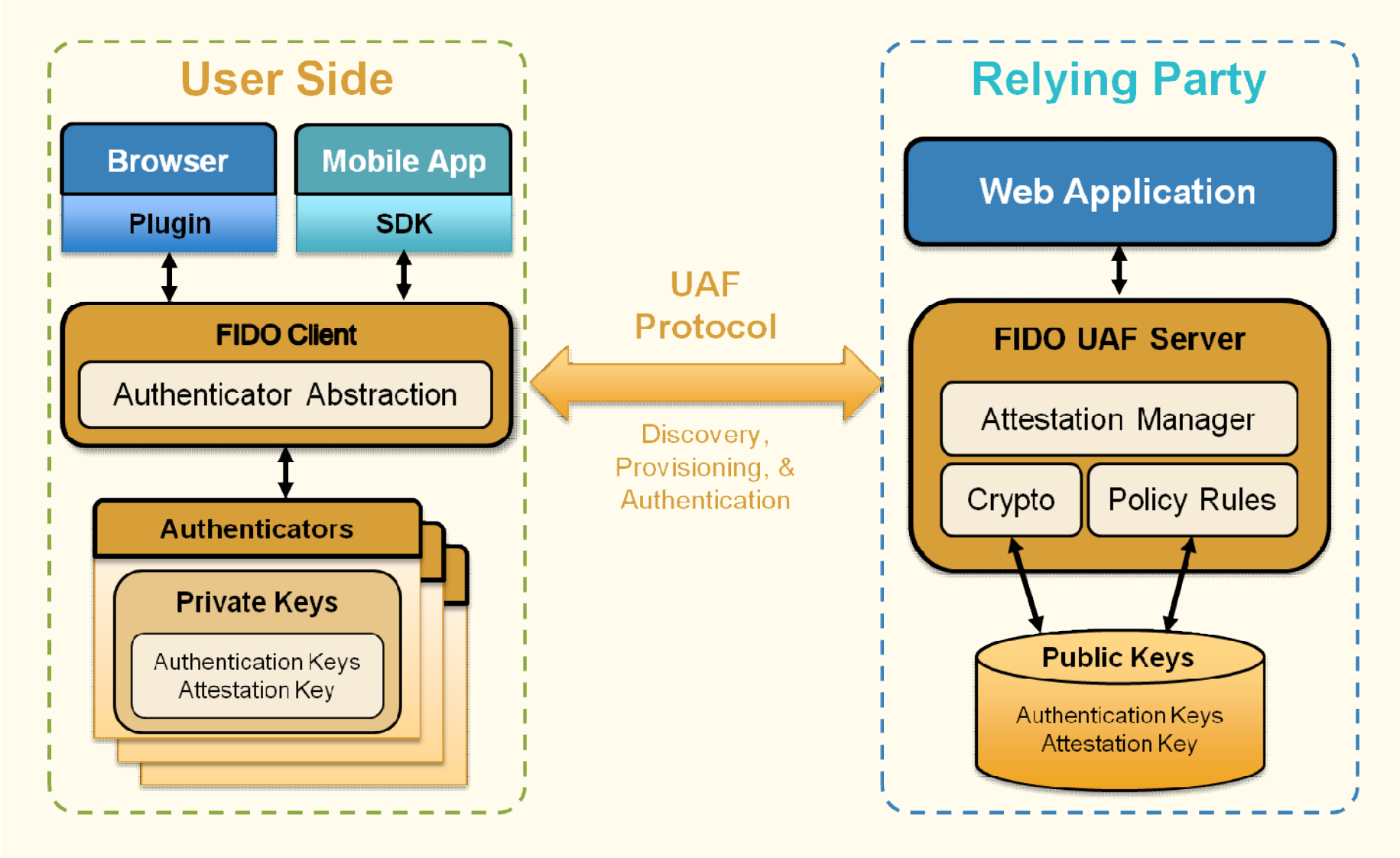
最後に　：　FIDO は、「オーセンティケーション」にフォーカス



（参考：FIDO アライアンス説明資料）

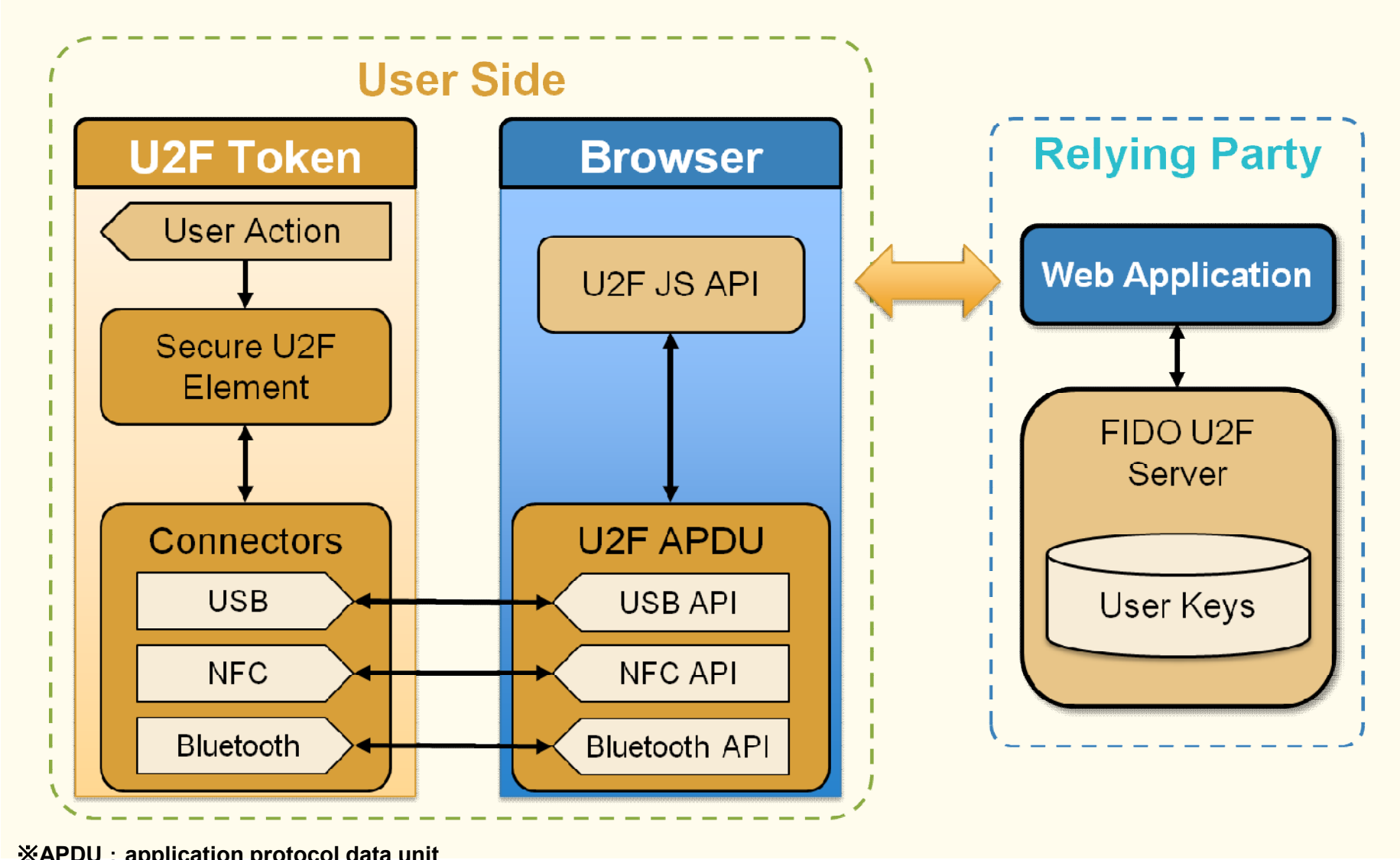
（補足）フローダイアグラム

FIDO UAF フローダイアグラム



（引用元：FIDO Alliance FIDO Overviewより）

FIDO U2F フローダイアグラム



※APDU：application protocol data unit
コマンドやレスポンスといったカードと送受信されるデータ

（引用元：FIDO Alliance FIDO Overview_March2014.ppt）