



NIIオープンフォーラム 2019



FIDO認証の技術と 応用展開の最新状況

2019年5月30日

ヤフー株式会社 Yahoo! JAPAN研究所
上席研究員 五味秀仁

本日の内容

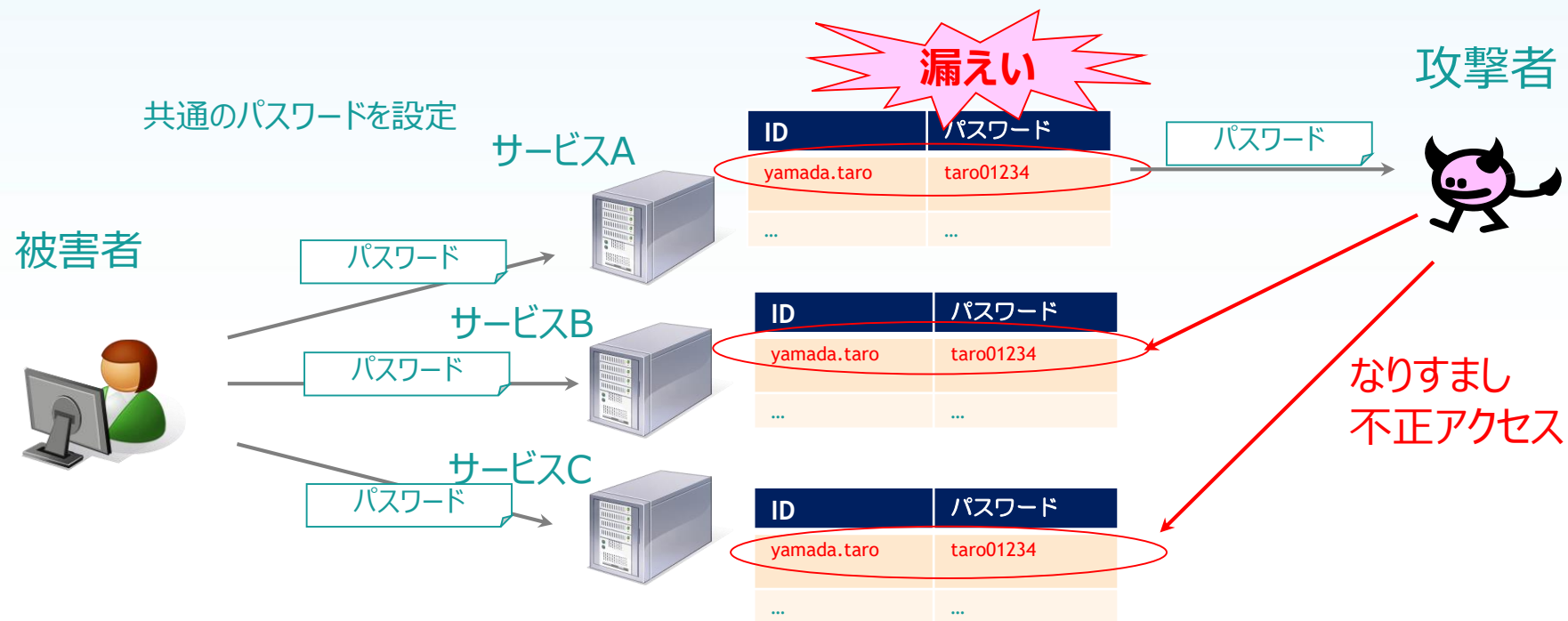
- FIDO認証が出現した背景
- FIDOアライアンス概要
- FIDO認証の考え方
- FIDO認証の技術と適用
- FIDO JAPAN WGの活動と日本での展開状況
- まとめ



FIDO認証が出現した背景

パスワードの問題：リスト型攻撃

- 同じパスワードを使い回すと、漏れた場合、なりすましや不正アクセスが発生

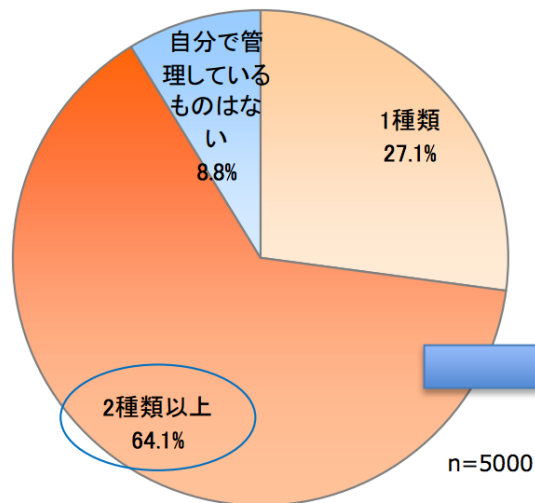


自社サーバーのセキュリティ管理に問題がなくても、利用者のリテラシーや他社サーバーの管理に影響を受け、不正アクセスを受ける可能性あり

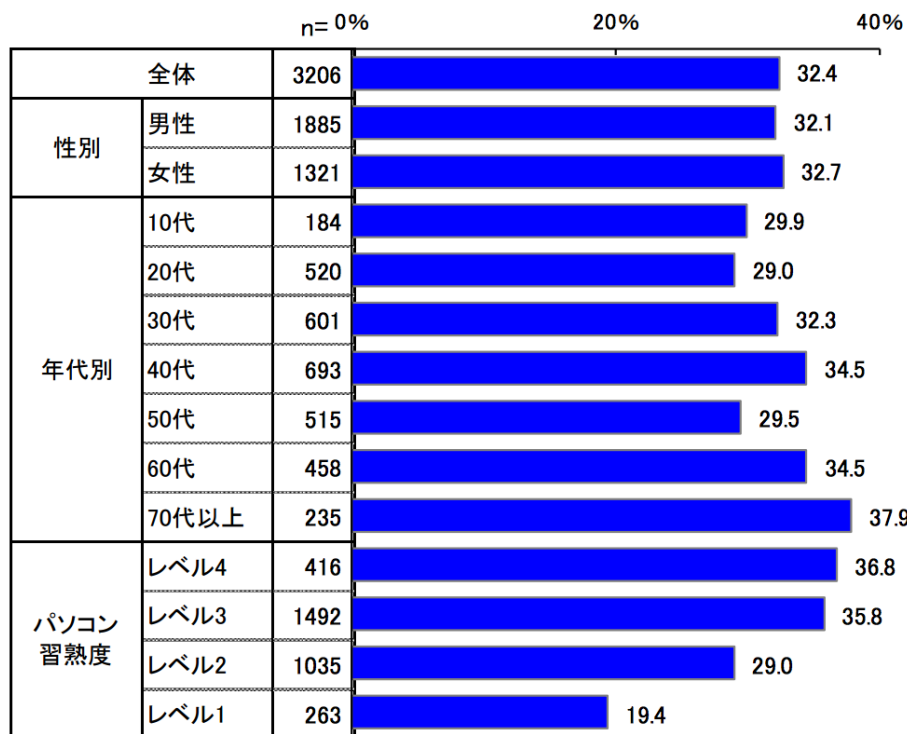
パスワードの使い回し

複数IDを持つ利用者の約7割がパスワードを使い回している
(パスワードをサイトごとに変えているかアンケート)

Q6 あなたがインターネットで利用しているID（アカウント）の内、自分で管理しているものはいくつありますか。あてはまるものを1つだけ選択してください。（お答えは1つ）



n=管理しているID（アカウント）が2種類以上の回答者(Q6)



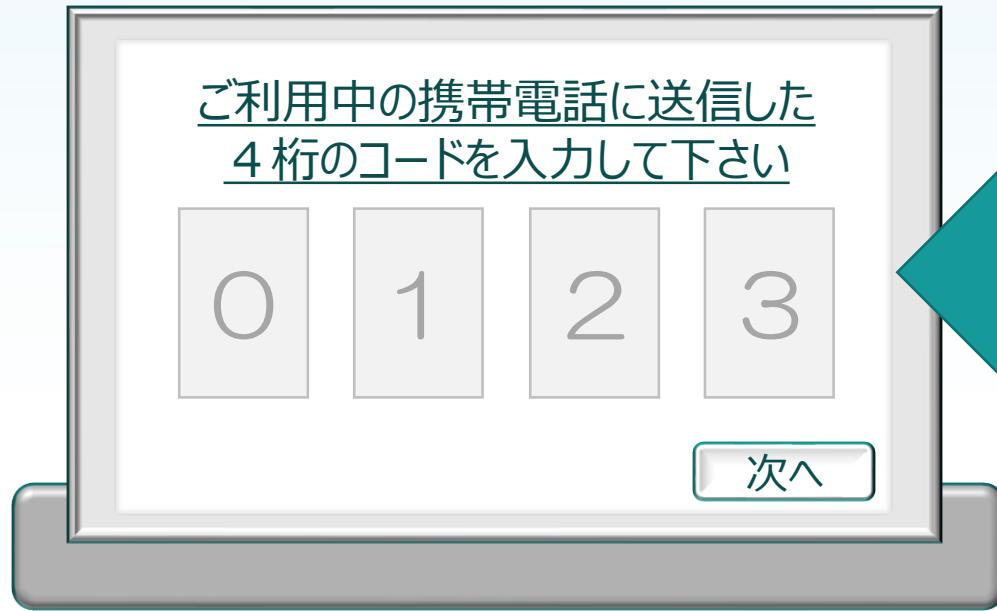
※習熟度を以下のように定義し、分析に使用している。

- レベル4：非常に習熟している（パソコンを組み立てたり、トラブルが起きても自分で解決できるレベルである）
- レベル3：習熟している（必要なソフトウェアをインストールして使ったり、パソコンやソフトウェアの設定を変えて使ったりできるレベルである）
- レベル2：基本操作は習熟（メールを使ったり、ホームページを閲覧したり、文章を書いたりするのに支障がないレベルである）
- レベル1：入門・初心者（パソコンの設定はお店や家族・知人に任せ、メールやホームページの閲覧をする程度で簡単な操作ならできるレベルである）

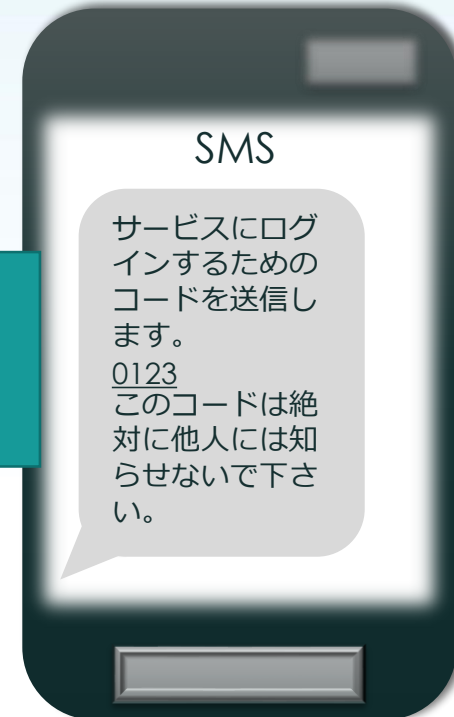
(出典) IPA 「2016年度情報セキュリティの脅威に対する意識調査」報告書
<https://www.ipa.go.jp/files/000056568.pdf>

パスワードの強化と課題

帯域外認証(Out of Bound認証)の一例



PC上のログイン画面



携帯電話に送信されたコード

その他の手段



コード生成器 (HW/SW)



登録電話番号への音声案内通知

パスワードとは異なり携帯などのデバイスを所持していなければログインできない
→パスワードの安全性を強化しつつも (※)、利便性に課題が残っている

(※)近年では米国NISTより「SMSを利用した帯域外認証については非推奨」というアナウンスもされてきている (悪意のあるアプリケーションや攻撃者から比較的容易に参照可能な情報であるため、と推測される)



FIDOアライアンス概要

The Fast IDentity Online Alliance

- FIDO ALLIANCE, INC. (A NONPROFIT MUTUAL BENEFIT CORPORATION) -

FIDO (ファイド) アライアンス

2012年に設立されて以来、現在約250社で構成される
米国カリフォルニア州法に基づくグローバルな非営利団体（相互利益法人）
パスワードと認証にまつわる課題解決のため、

- 「FIDO認証モデル」に基づく技術仕様の策定
- 技術仕様を導入展開するためのプログラム運営
- 各標準化団体との協業などを通じたさらなる導入展開を推進

The logo for FIDO Alliance, featuring the word "fido" in a lowercase, sans-serif font with a yellow dot above the 'i', and "ALLIANCE" in a smaller, uppercase, sans-serif font below it.

simpler
stronger
authentication

250+のメンバーでグローバルに運営



グローバルなブランドとテクノロジー企業を中心に構成するFIDOボードメンバー 40社



+ スポンサーメンバー

+ アソシエイトメンバー

+ リエゾンメンバー

FIDO Alliance is the global industry collaboration dedicated to solving the password problem

...with no dependency on “shared secrets”

FIDOアライアンスは、パスワード課題の解決に注力するグローバルな業界の連携であり、その特徴は「共有の秘密」に依存しないことです。



FIDO認証の考え方

FIDOアライアンスの目指す認証とは

パスワードの課題

利便性 (Usability)

覚えられない

入力不便

安全性 (Security)

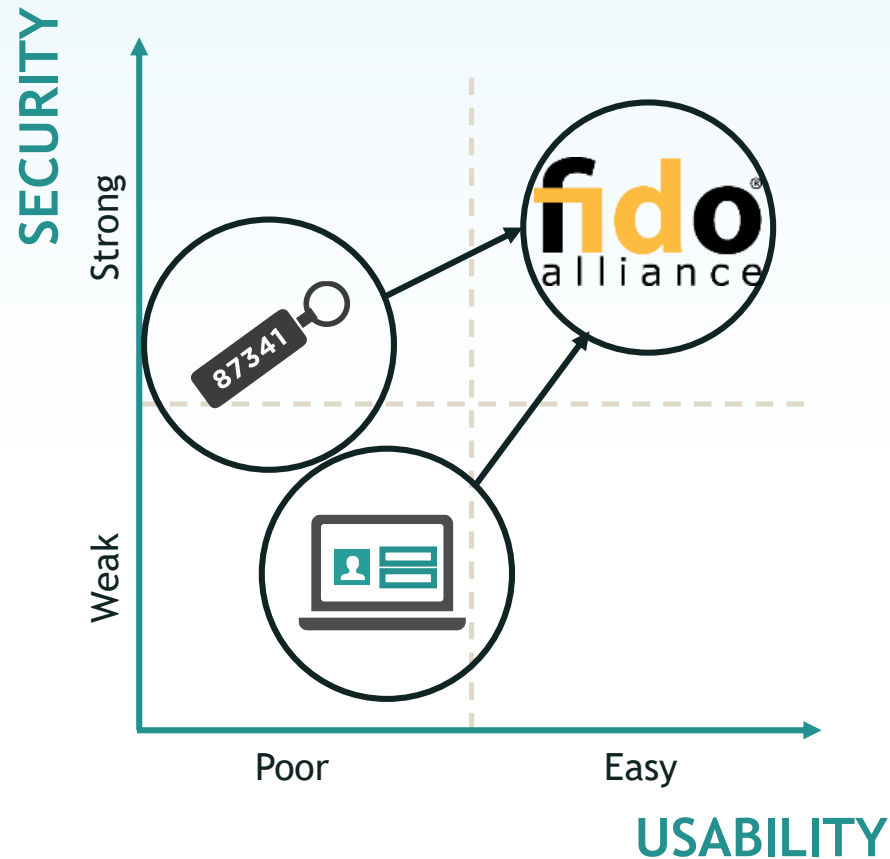
再利用可能

漏えいしやすい



パスワードへの依存度を減らしつつ、利便性と安全性の両面を向上させる

FIDO認証のビジョン

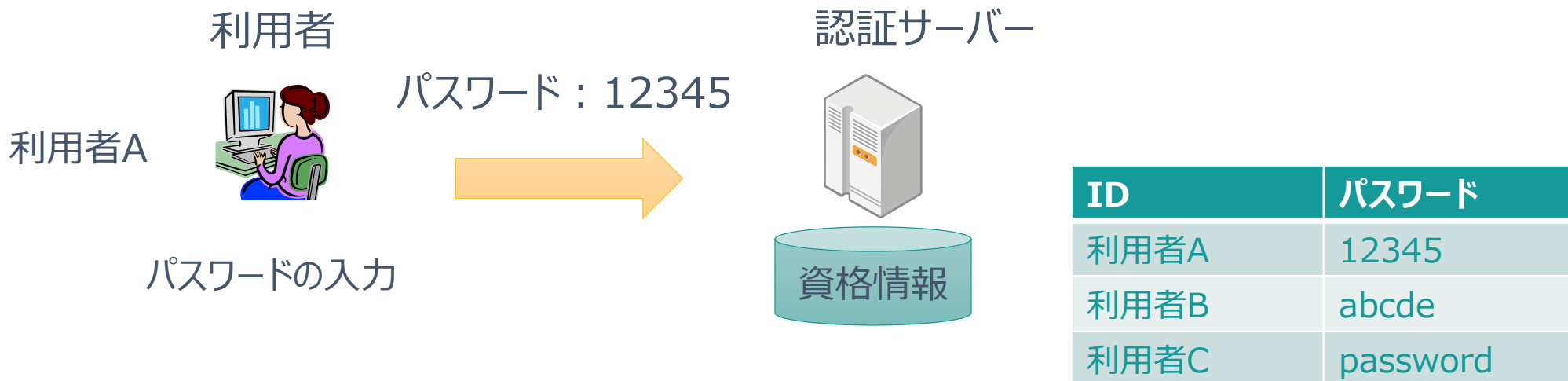


(出所 : FIDOアライアンス)

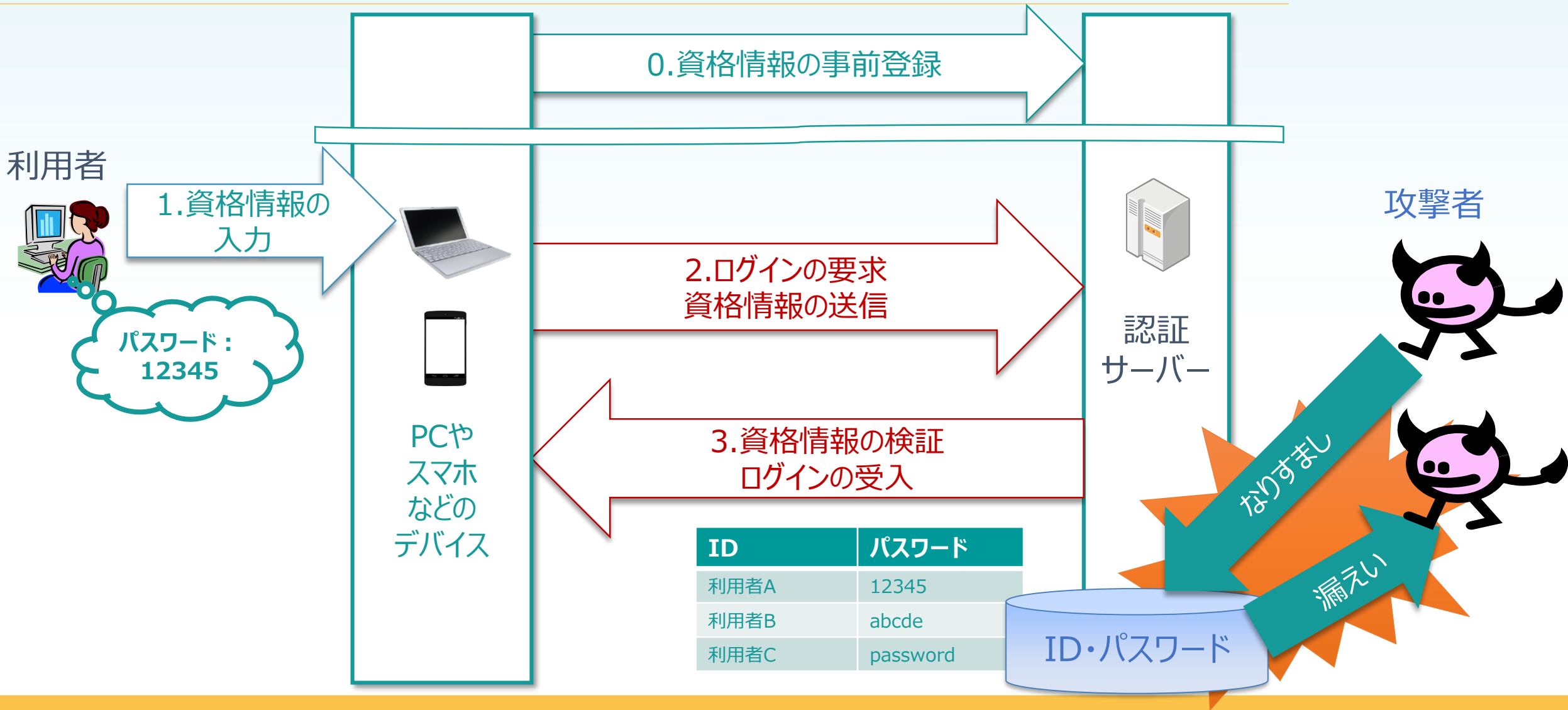
FIDOアライアンスは、安全性と利便性の両立を目指している

従来の認証モデル（リモート認証）

- 利用者はIDとクレデンシャル＝資格情報（認証情報：パスワードなど）を通信路を介して認証サーバーに対して送付する。認証サーバーは受け取ったIDを識別し、資格情報がIDに紐付いた適切な情報であるか否かを検証する。
- この場合、利用者の資格情報はあらかじめ認証サーバーが保管し、識別と検証の処理は認証サーバーで行う。（利用者・端末とサーバーで「秘密」を共有する）

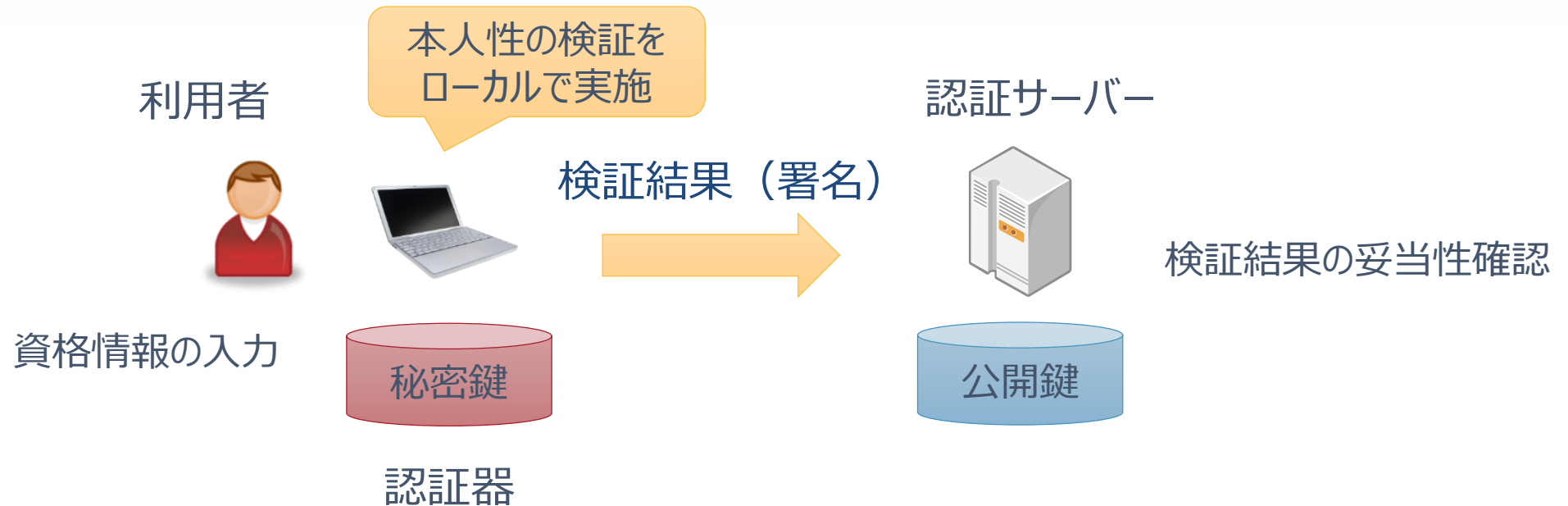


リモート認証の流れ

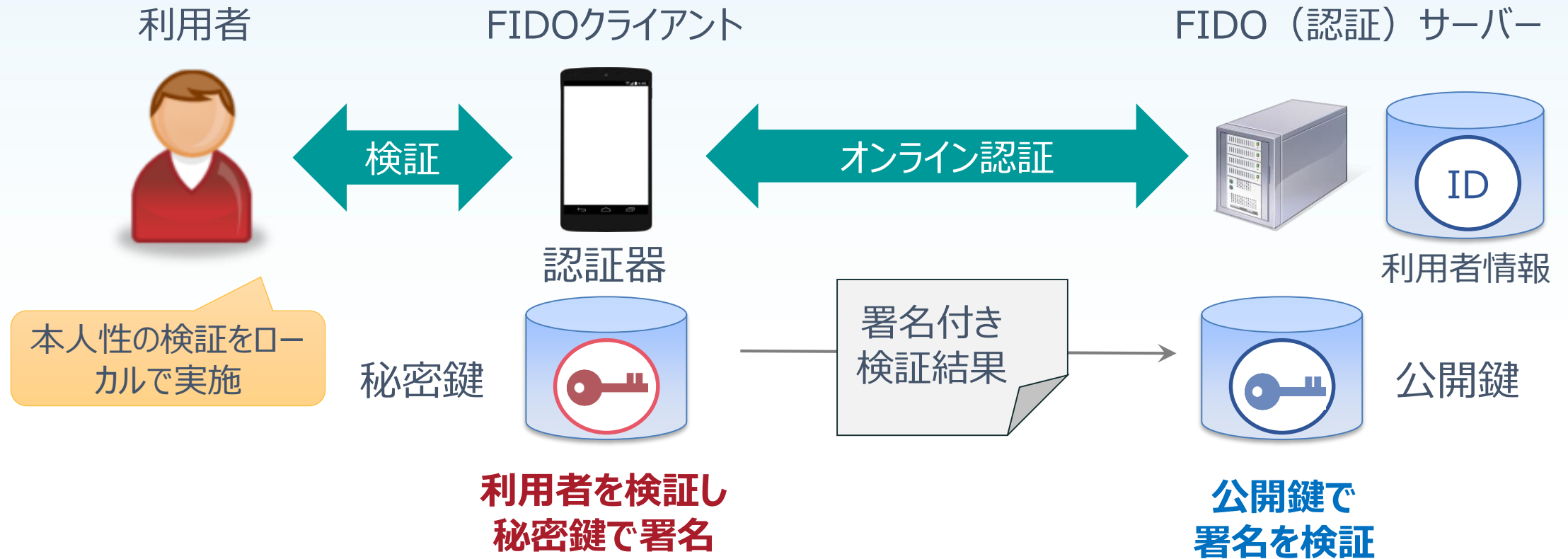


FIDO認証モデル（端末とサーバーで秘密を共有しない）

- 利用者のデバイスなど手元にある**「認証器」 (Authenticator)** が利用者の本人性を検証する機能を持つ。本人性の検証結果は認証サーバーに送付され、認証サーバーは検証結果の妥当性を確認し、認証が完結する。
- すなわち、FIDO認証ではネットワーク上に資格情報が流れることはない。
（不正アクセスの原因となる「共有の秘密」を用いない認証）

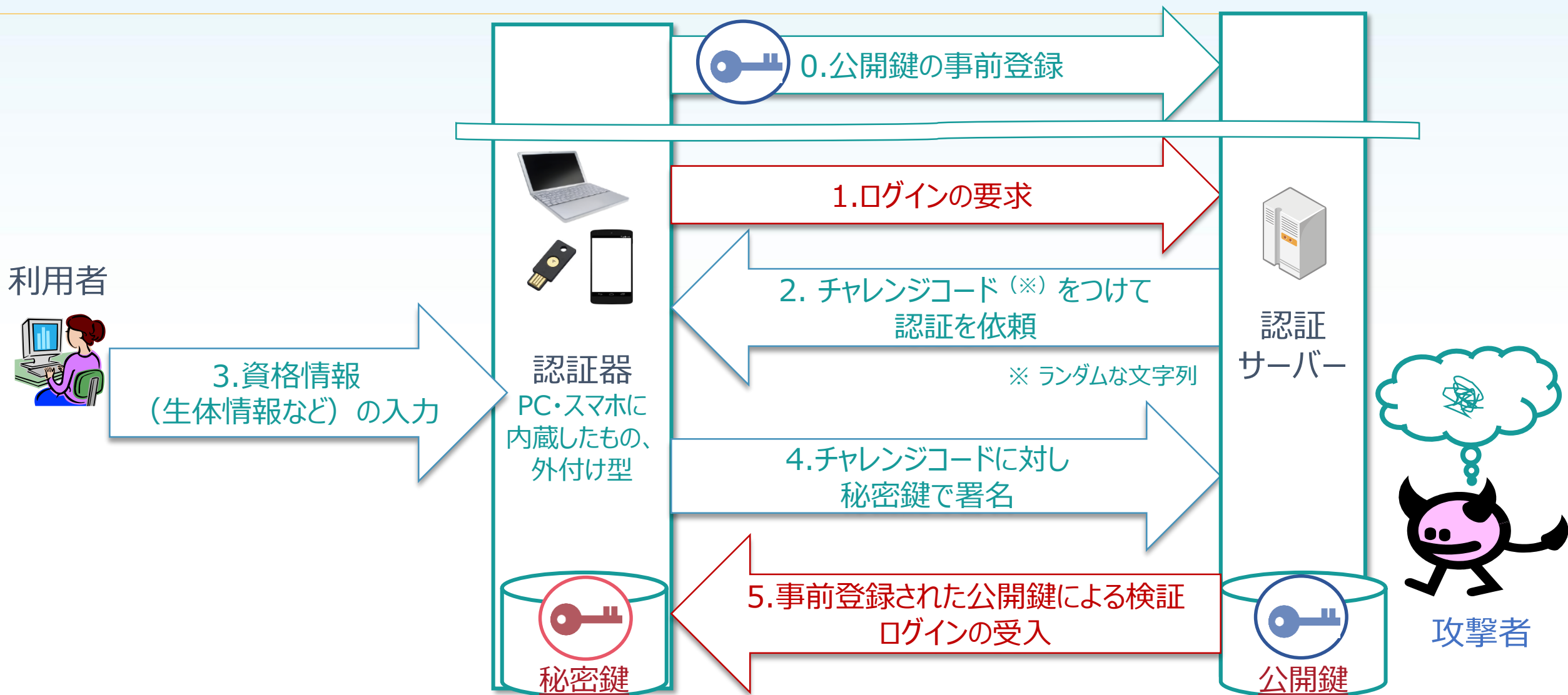


公開鍵暗号方式の活用と「認証器」の導入



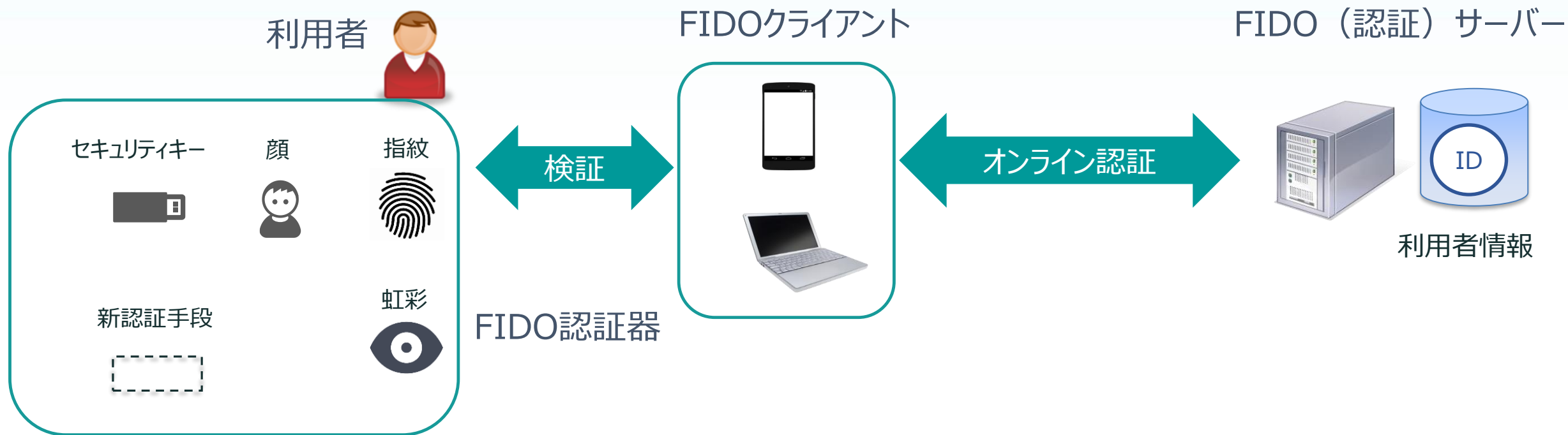
利用者が適切な秘密鍵を保有することを確認（検証）することによって認証を実現（利用者・端末とサーバーが「秘密」を共有しない）

FIDO認証の流れ



FIDO認証のバリエーション

- FIDO認証に対応している生体認証の方式や装置の種類を問わない。
(ローカルパスコードでも良い)



FIDO認証の特徴と “プライバシーポリシー”



No 3rd Party in the Protocol

- ✓ FIDO認証プロトコルはend-endであり、第三者の介在はない



No Secrets generated/stored on the Server side

- ✓ サーバー側で秘密情報が生成されたり保存されることはない
(FIDO認証の鍵ペアのうち、秘密鍵はFIDO認証器の外に出ない)



Biometric Data (if used) Never Leaves Device

- ✓ 生体情報はFIDO認証器に保存され、外に出ない



No Link-ability Between Services and Accounts

- ✓ 異なるサービス・アカウントに対して、FIDO認証の鍵ペアは独立



FIDO認証の技術と適用

FIDO Specifications

FIDO認証モデルに基づくFIDO仕様群

FIDO UAF



FIDO U2F



FIDO2



WebAuthn*
(W3C)

CTAP

UAF : Universal Authentication Framework (パスワードレス認証)

U2F : Universal Second Factor (2段階認証)

WebAuthn : Web Authentication (ウェブ認証)

CTAP : Client to Authenticator Protocol (デバイス間連携仕様)

* FIDOアライアンスから仕様 (案) を開示し、W3Cとして仕様化

FIDO認証の仕様化 (2014 - 2018)

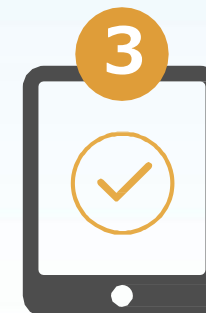
パスワードレスの体験 (UAF : Universal Authentication Framework)



認証開始 (チャレンジ)



生体情報によるユーザーの検証*



認証成功 (オンライン)

2段階認証の体験 (U2F : Universal Second Factor)



2要素目の認証開始 (チャレンジ)



セキュリティキーを挿入* /
ボタンを押す



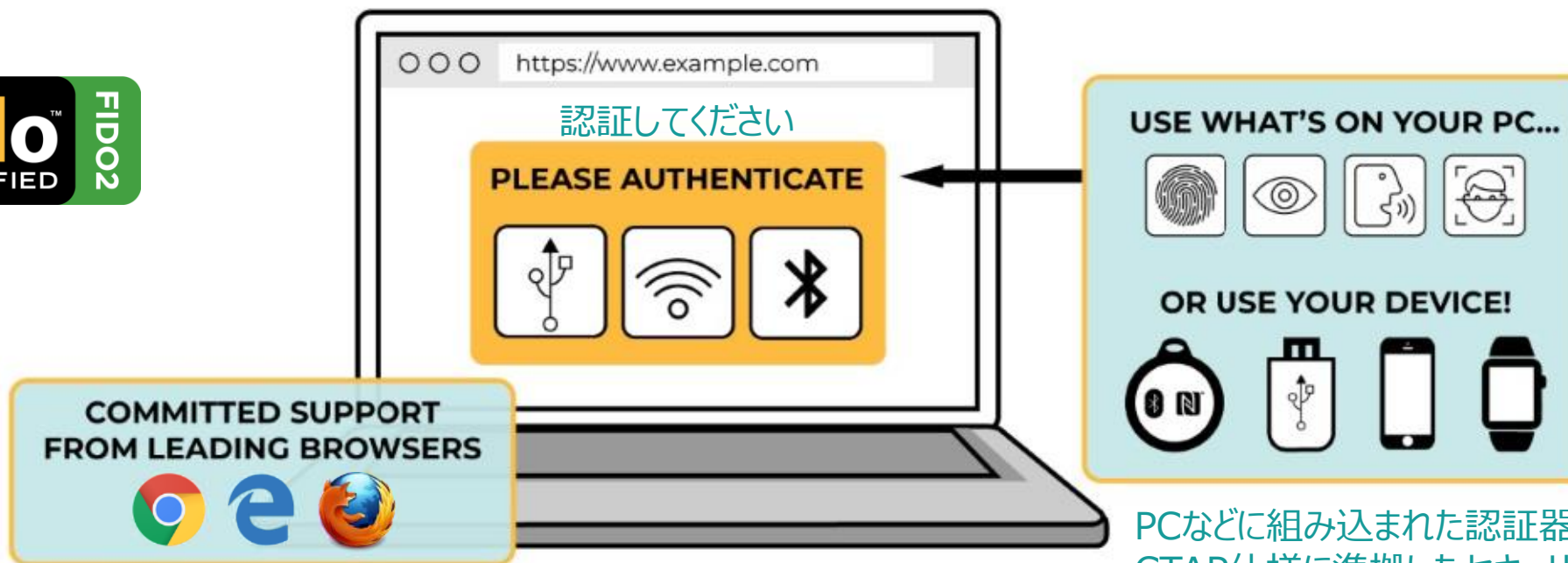
認証成功 (オンライン)

*他タイプの認証器もある

FIDO2 : さらなる普及をめざしプラットフォーム化

FIDO2 : WebAuthn (Web認証) & CTAP

- 2016年11月 FIDOアライアンスからW3CにWeb認証 (案) を提出
- 2018年4月 Web認証 発表 (勧告候補) 、2019年3月 Web認証 正式勧告

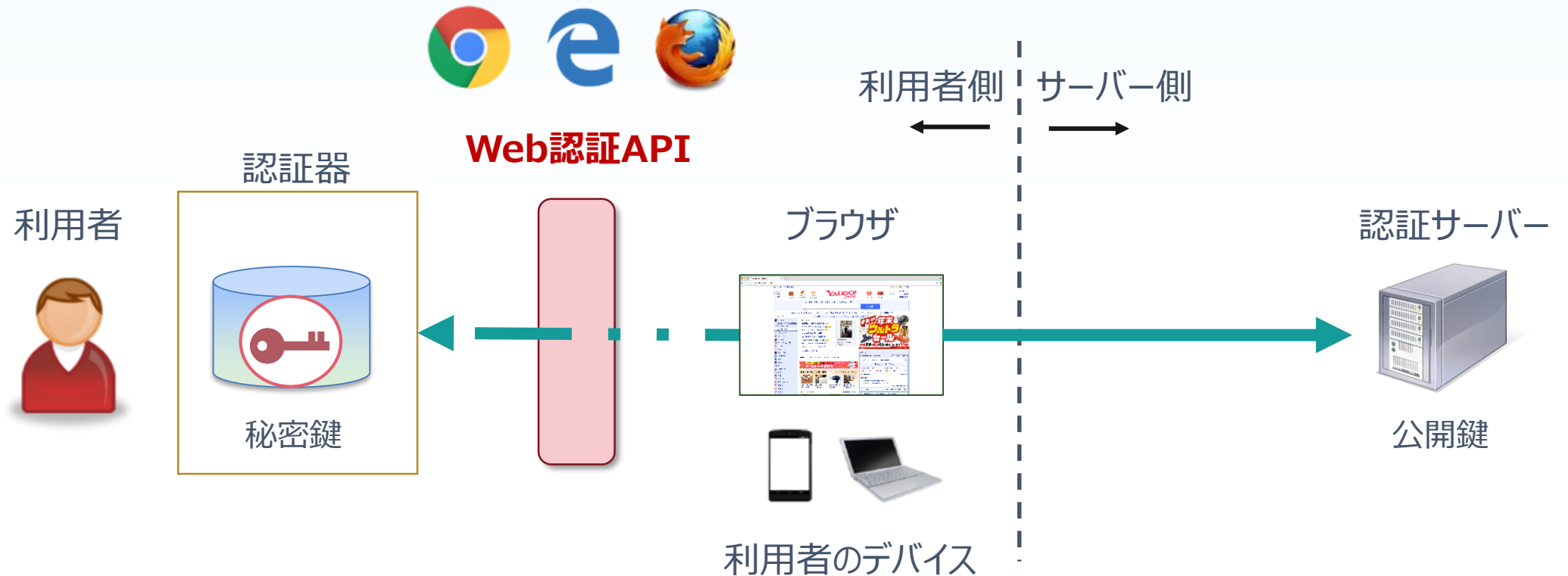


主要なブラウザが対応 (Safariもプレビュー版にて対応済)

PCなどに組み込まれた認証器、またはCTAP仕様に準拠したセキュリティキーを利用して認証可能

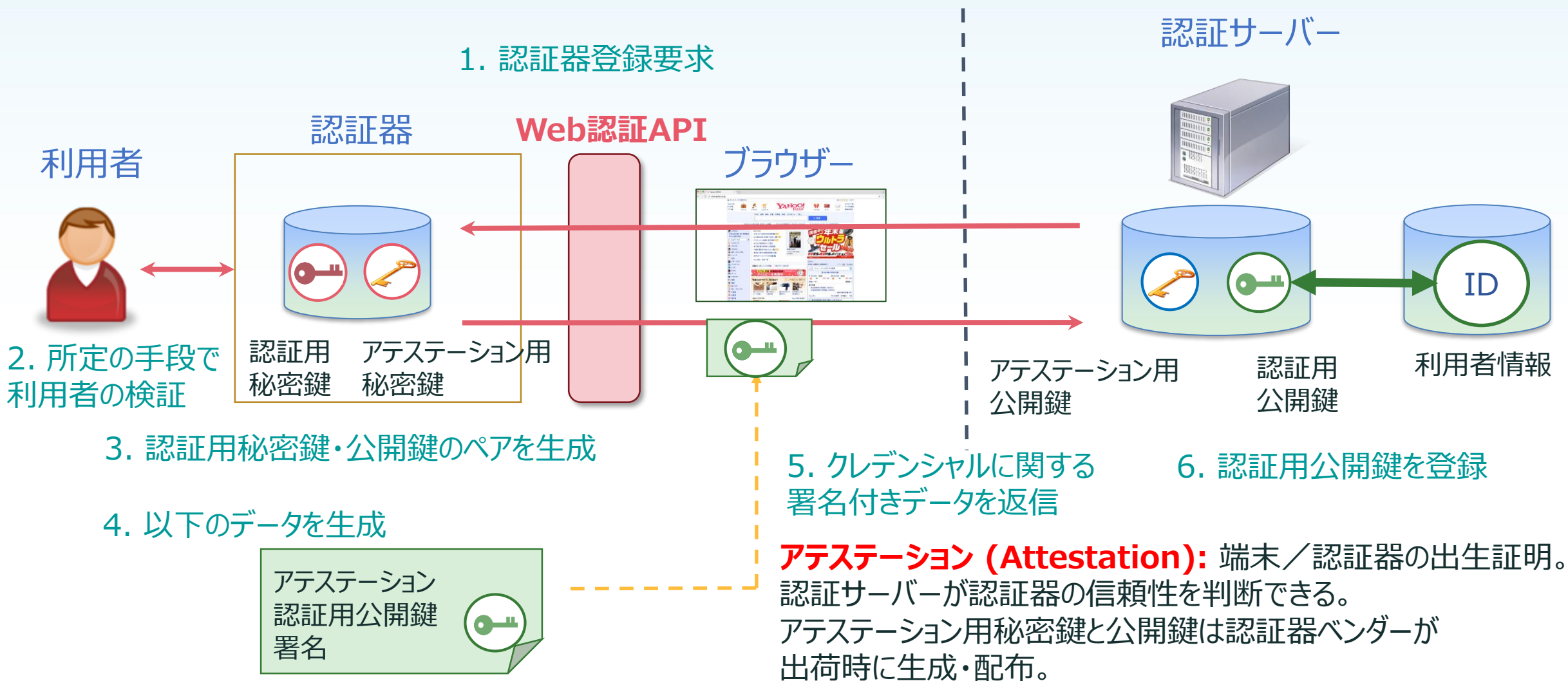
Web認証API

- Webブラウザに表示されるウェブコンテンツからJavaScriptでFIDO認証器を呼び出し、認証サーバーとのやり取りでFIDO認証を可能にするためのWeb API



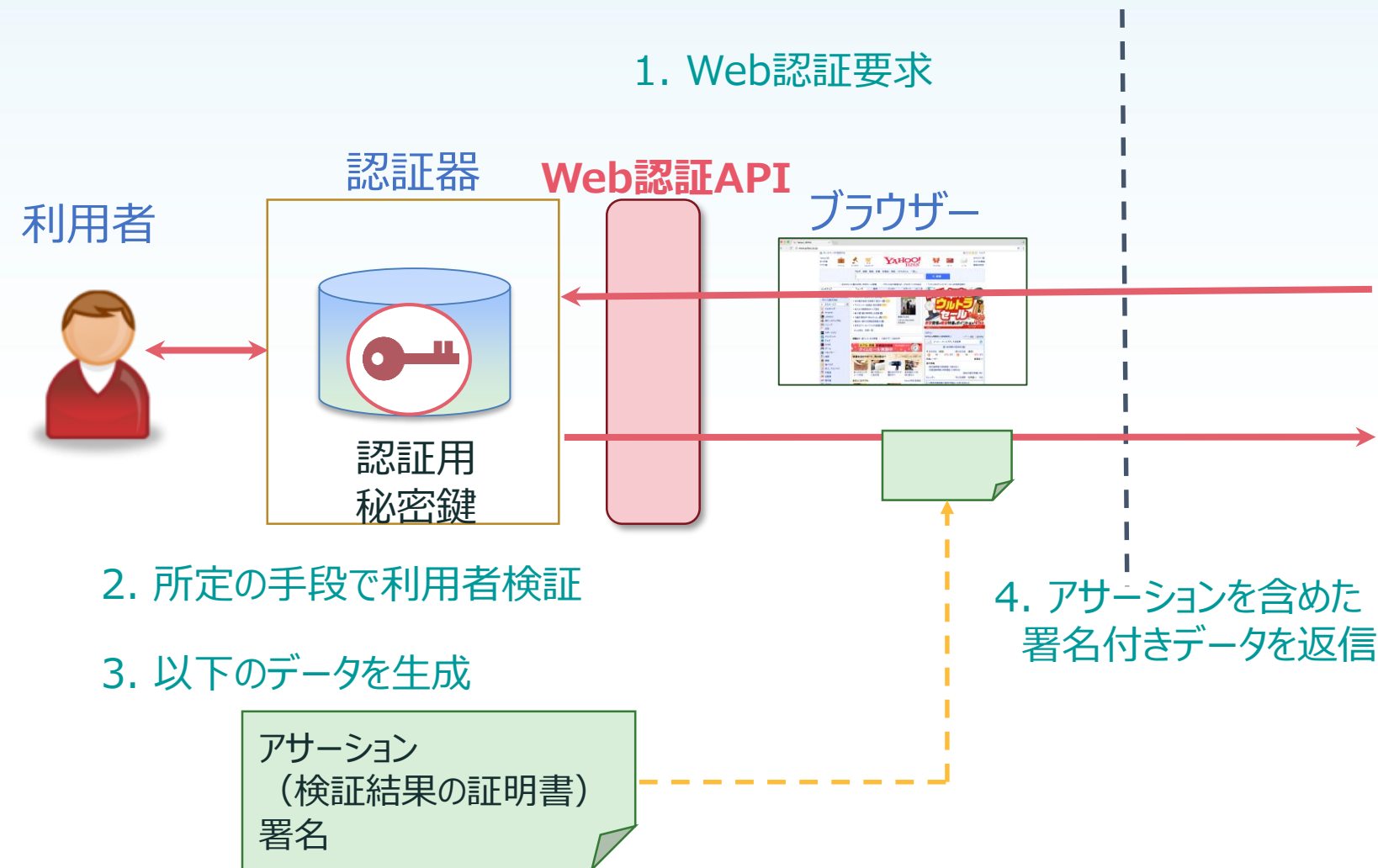
*API (Application Programming Interface)

認証器の登録



認証器を用いたWEB認証

1. Web認証要求



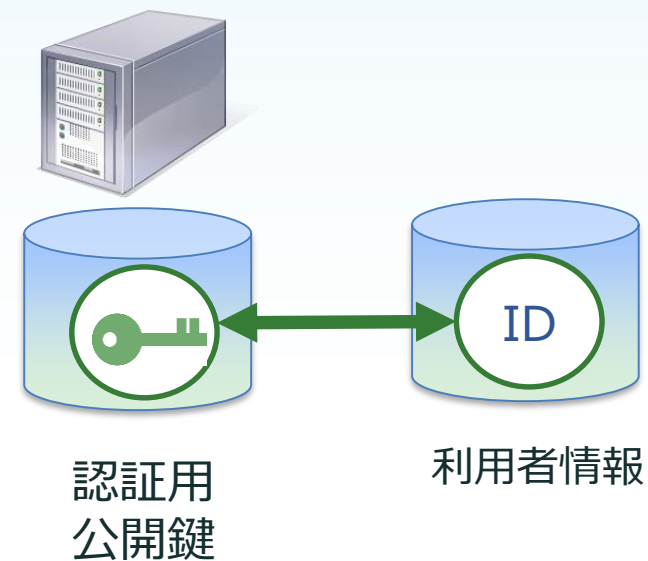
2. 所定の手段で利用者検証

3. 以下のデータを生成

アサーション
(検証結果の証明書)
署名

4. アサーションを含めた
署名付きデータを返信

認証サーバー



5. 署名検証

6. 利用者IDの抽出

(注) アステーション用鍵ペアは図中では省略。

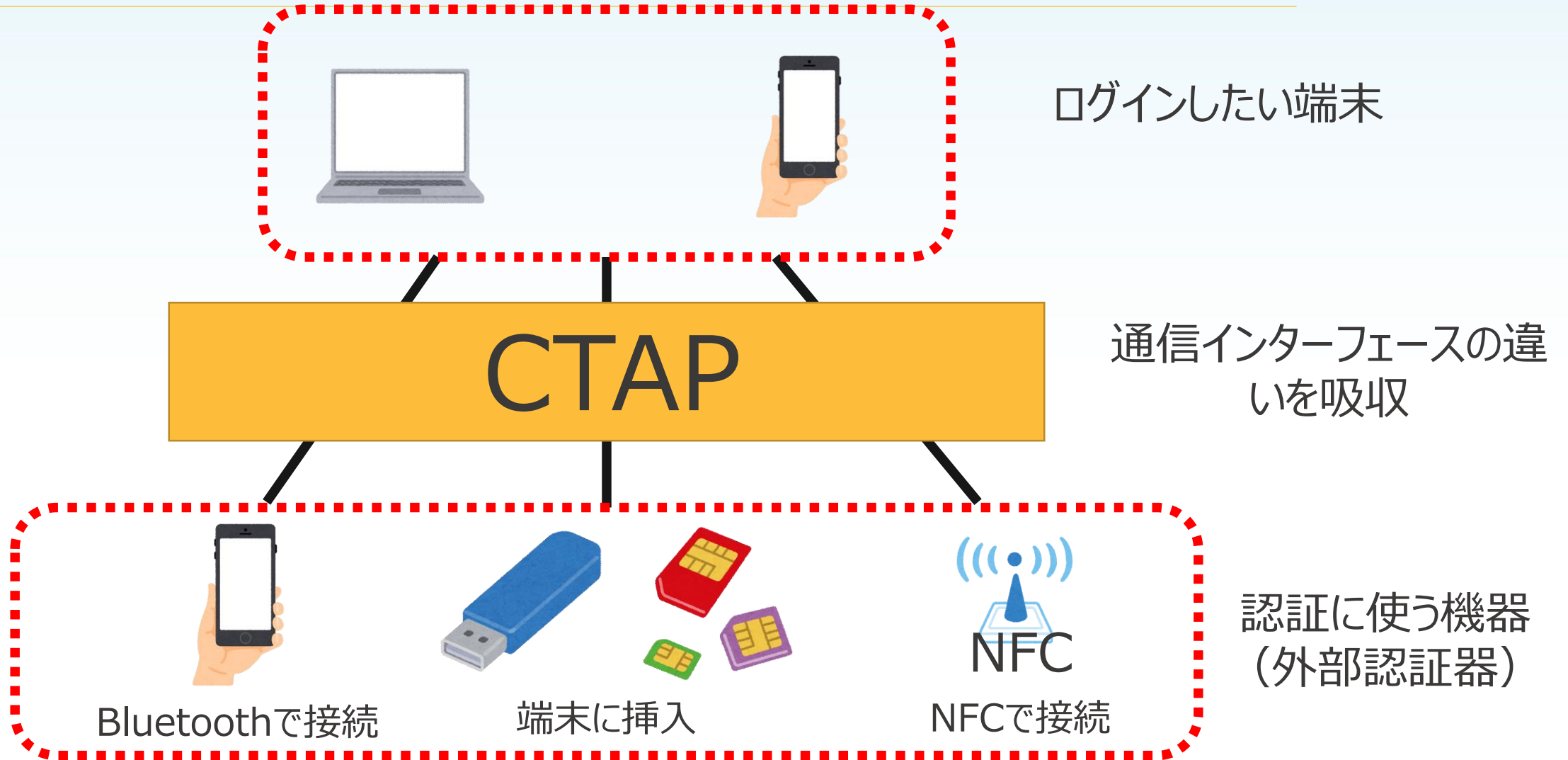
CTAP: デバイス間連携仕様

- Client To Authenticator Protocol - Web認証APIを呼び出すブラウザが動作するデバイスと外部認証器をBluetooth/NFC/USBを通じて安全に通信するための仕様

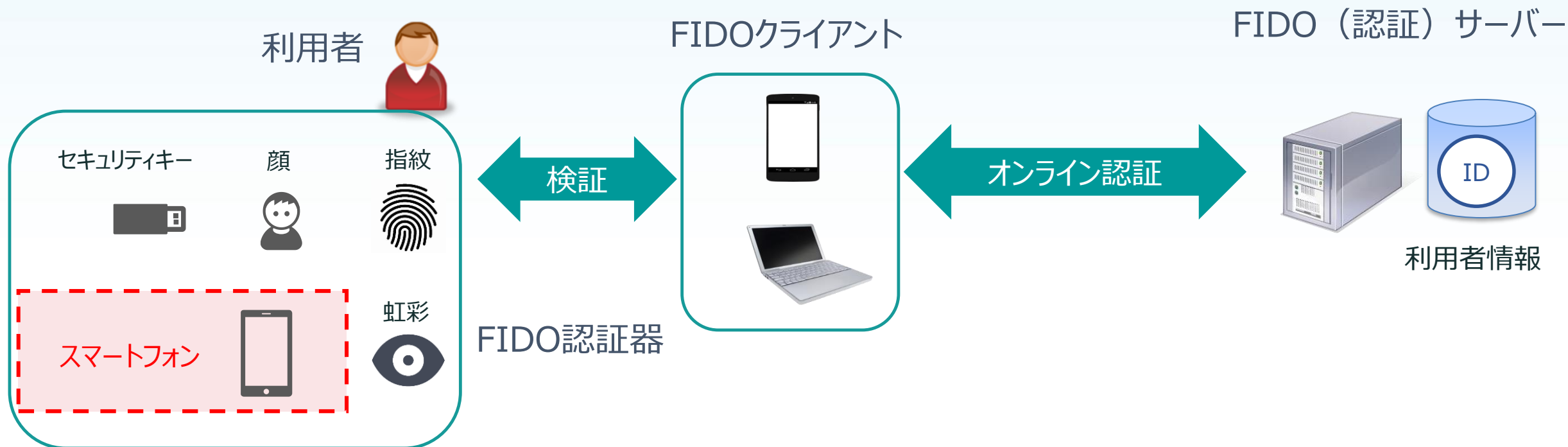


CTAP: U2F仕様の一部であるCTAP1とFIDO2のために拡張したCTAP2を総称する。

CTAP: デバイス間連携仕様 (2)



スマホも一つの認証器に



「スマホ認証器」により、さらに認証のスケラビリティ（拡張性）が向上

FIDO仕様はITU標準の一つ

- 2018年12月、FIDO仕様が国際電気通信連合（ITU）の電気通信標準化部門（ITU-T）によって国際標準として承認された。



ITU-T勧告X.1277 - FIDO UAF 1.1

ITU-T勧告X.1278 - FIDO2 CTAP（U2F CTAP1含む）

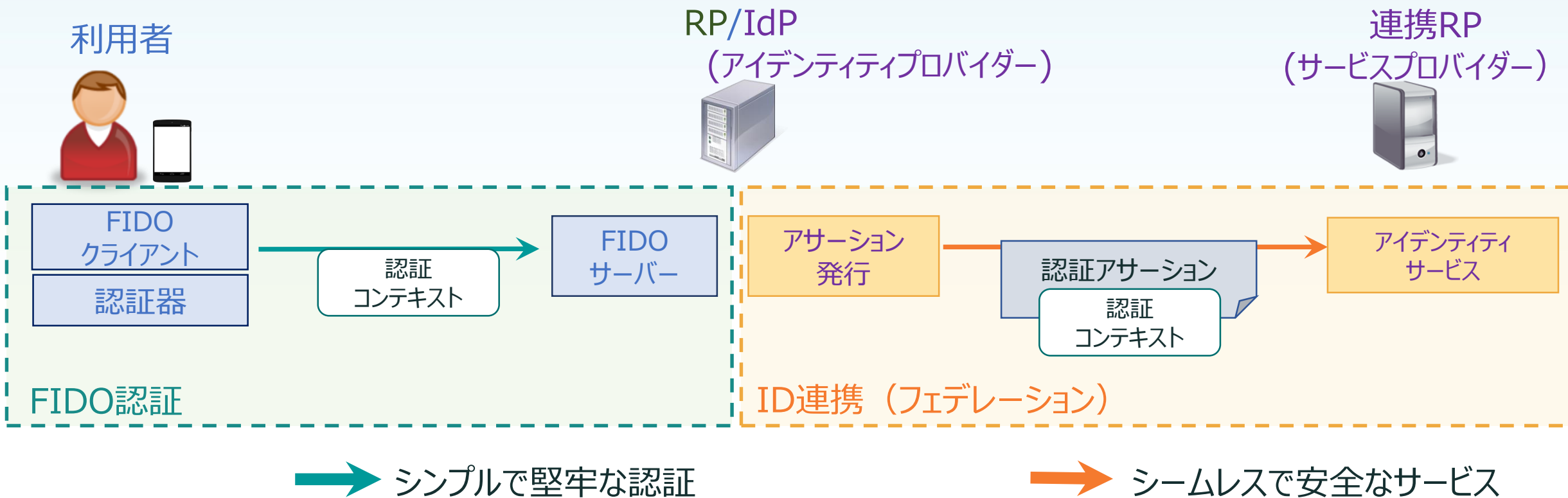
認証：セキュア・トラストアプリケーションのための基盤

一般的なアクセス制限つきシステム



認証が起点になり、様々なオンライン上の行動につながる。

FIDO認証とID連携



FIDO認証とID連携を組み合わせると、認証コンテキストは認証器から連携RPへと伝搬。

*RP: Relying Party



FIDO認定プログラム

FIDO認定プログラム

- 機能認定（エンド・エンド）：
 - 適合性テスト
 - 相互接続性テスト



- FIDO認証器のセキュリティ認定：
 - 秘密鍵保護がどれだけ優れているか？
 - 第三者ラボによる検証
 - 新設されたバイオメトリクス部品認定でさらに充実

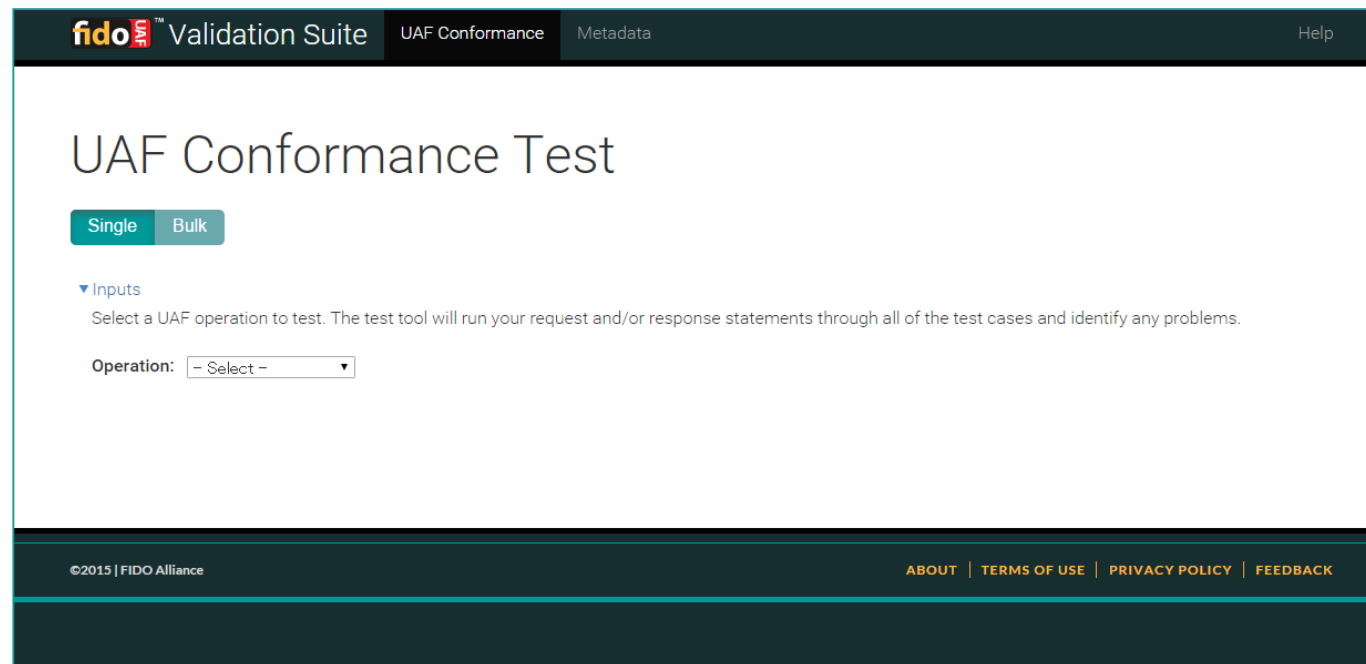


- ユニバーサルサーバー：
 - FIDO認定された全ての認証器との適合性を確保



適合性テスト

認定テストの参加者はまずはFIDOアライアンスの提供する専用の自己診断ツールで、技術仕様への適合性を検証する。



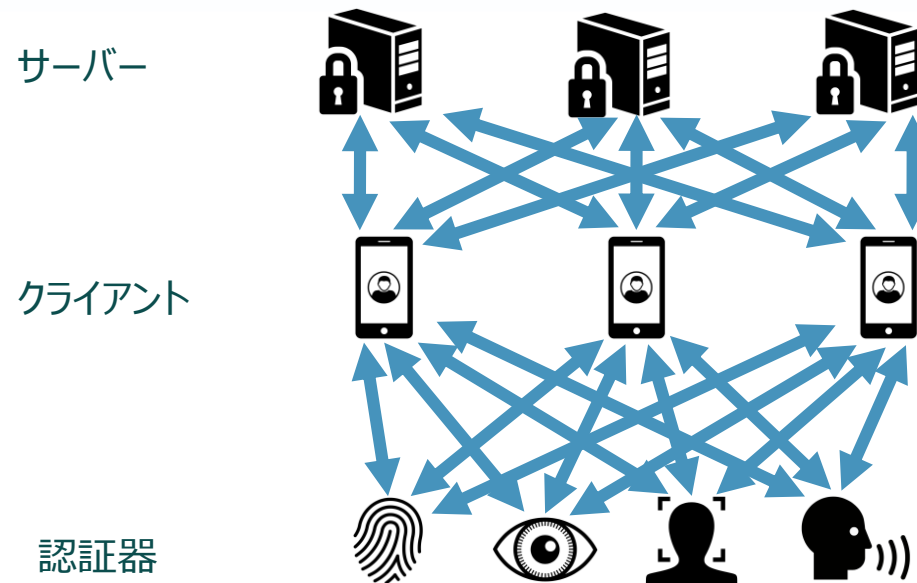
The screenshot shows the 'UAF Conformance Test' interface within the 'fido UAF Validation Suite'. The navigation bar includes 'UAF Conformance', 'Metadata', and 'Help'. The main content area features a title 'UAF Conformance Test' and two tabs: 'Single' (selected) and 'Bulk'. Below the tabs, there is a section for 'Inputs' with a description: 'Select a UAF operation to test. The test tool will run your request and/or response statements through all of the test cases and identify any problems.' A dropdown menu labeled 'Operation:' is currently set to '- Select -'. The footer contains the copyright notice '©2015 | FIDO Alliance' and links for 'ABOUT | TERMS OF USE | PRIVACY POLICY | FEEDBACK'.

相互接続性テスト

各参加者がFIDO認証の実装を持ち寄って集まる試験イベントを開催。

各参加者の3つのロールからなる組み合わせの元で、所定の認証シナリオに応じて接続し、その動作の適切性を逐一確認する。

製品例としてはクライアントと認証器が1つのデバイスに実装されているような場合も含む。



FIDO認証器のセキュリティ認定

認証器はセキュリティのコア

- プライバシー情報（鍵と生体情報）を守る

サードパーティラボにて小規模で認定実施可能

認定されている他のコンポーネント上に構築可能

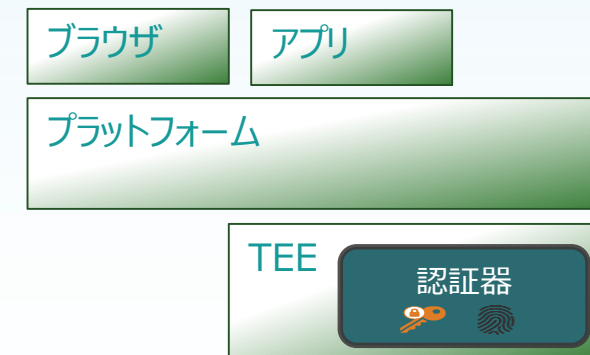
- TEE（Trusted Execution Environment）、Secure Element...

プラットフォーム自体のセキュリティも認定対象
（認証器部分のみが対象）

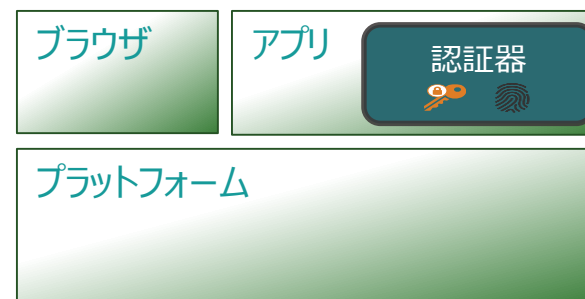
1. プラットフォーム組み込み



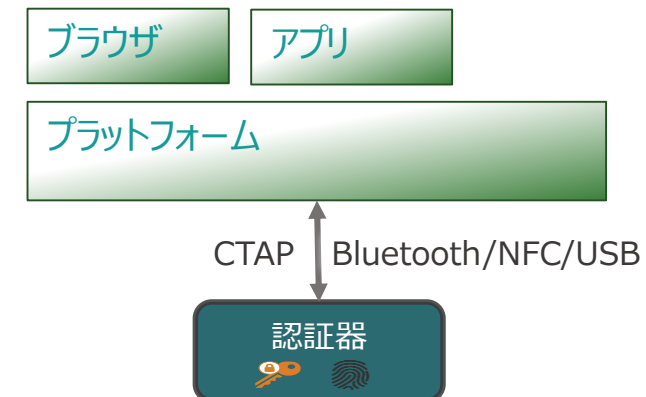
2. TEE内



3. アプリ内



4. セキュリティキー



FIDO認証器のセキュリティ認証：さまざまなユースケースに対応するセキュリティレベル

ハード・ソフトの要求条件の例		防衛の対象
チップへの故障利用攻撃と侵入型攻撃に対する保護機能等	L3+	捕捉されたデバイス (チップレベルの攻撃)
基板のポッティング、パッケージ・オン・パッケージ (PoP)、RAM暗号化等	L3	捕捉されたデバイス (基板レベルの攻撃)
デバイスは機密動作環境 (ROE: TEE、Secure Element等) が必須、 或は、本質的に機密動作環境のデバイス (USB トークン、スマートカード等)	L2+	デバイスのOSの危殆化 (きたいか) (ROEで防衛)
	L2	
どんなHWやSWでもよい	L1+	デバイスのOSの危殆化 (きたいか) (ホワイト・ボックス暗号化で防衛)
	L1	フィッシング、サーバーのクレデンシャル流失、中間者攻撃 (パスワードよりベター)

Android – FIDO2認定を取得



Android が FIDO2 認定を取得、
これによりパスワードからの移行がグローバルで加速
(国際版の日本語訳)

グローバルで 10 億台を超える Android 7.0 以降のデバイスでモバイルアプリと
ウェブサイトからシンプルで安全な生体認証によるログインを提供する FIDO 標準を活用可能

2019年2月25日、バルセロナ - FIDO アライアンスは本日、Android が FIDO2 認定を取得し、このプラットフォームが搭載されている 10 億台以上のデバイス上で、シンプルで堅牢な認証機能が利用可能となったことを発表しました。このニュースを受け、Android 7.0 以降を搭載している互換性のあるデバイスは、デバイスを箱から取り出したその時点で、もしくは Google Play 開発者サービスの自動更新後に FIDO2 認定を取得している状態となります。これにより、ユーザーはデバイスに内蔵された指紋センサーを利用して、FIDO2 プロトコルをサポートする Web サイトで安全なパスワードレスでのアクセスが可能になりました。

Web およびアプリ開発者は、既に対象となる Android デバイスを利用しているユーザーと将来新型デバイスにアップグレードする予定があるユーザーの両方を含めて急速に拡大しているエンドユーザーの基盤に対し、シンプルで API の呼び出しを通して Android アプリや Web サイトに堅牢な FIDO 認証を追加することで、パスワードレスとフィッシング耐性を有するセキュリティを提供することができます。

Google のプロダクトマネージャーであるクリスチャン・ブランドは、「Google は、FIDO アライアンスおよび W3C と長い間連携して FIDO2 プロトコルを標準化してきました。これにより、あらゆるアプリケーションがフィッシング攻撃に対する保護を提供しながら、パスワード認証から移行することができます。Android の FIDO2 認定取得に関する本日の発表は、我々のパートナーおよび開発者に対して既に市販されているモデルと今後発売されるモデルの両方のデバイスにわたり、安全なキーストアにアクセスするための標準的な方法を提供することで、ユー

- Android 7.0以降のAndroid OS端末 FIDO2認定
特別な生体認証装置を組み込む、またはさらにセキュリティ強度を高める等追加の差異化要素を盛り込まない限り、端末メーカーは個別にFIDO認定を受ける必要がなくなり、今後のさらなるFIDO認証の普及に弾みがつきました。(2019年2月25日)



Windows Hello – FIDO2認定を取得



Microsoft Windows Hello が FIDO2 認定を取得
(国際版の日本語訳)

グローバルで 8 億台を超えるアクティブな Windows 10 デバイスに安全なパスワードレス認証をもたらします

2019 年 5 月 6 日、カリフォルニア州マウントビュー - FIDO アライアンスは本日、Microsoft Windows Hello が FIDO2 認定を取得したことを発表しました。このニュースにより、Windows 10 を実行している互換性のあるすべてのデバイスは、2019 年 5 月 10 日の Windows 10 更新の後、直ちに FIDO2 認定を取得している状態となります。Windows 10 ユーザーは、集中管理されているパスワードの代わりに、Windows Hello 生体認証または PIN を利用することにより、デバイス、アプリ、オンラインサービス、およびネットワークに FIDO 認定を受けたセキュリティでアクセスできます。

FIDO2¹ は、モバイル機器のバイオメトリクスや FIDO セキュリティキーなどを使って Web サイトおよびアプリケーションへの簡単な安全なログインを可能にする標準規格です。FIDO2 のシンプルなログイン体験は、パスワードよりはるかに優れた堅牢な暗号学的セキュリティによって担保されており、ユーザーをフィッシング、あらゆる形式のパスワード盗難、およびリプレイ攻撃から保護しています。FIDO2 の詳細については、次の URL を参照してください。 <https://fidoalliance.org/fido2/>

Microsoft のプリンシパル・グループマネージャーであるヨゲッシュ・メヘターは、「FIDO アライアンス、W3C との共同作業、および FIDO2 標準への貢献は、パスワードのない世界への Microsoft の取り組みの重要な部分です。Windows Hello は FIDO2 標準に準拠するように構築されているため、Microsoft クラウドサービスおよび異種混在環境内で動作します。本日の FIDO2 認定に関する発表で、組織や Web サイトは 8 億台を超えるアクティブな Windows 10 デバイスを正式に認定された FIDO 認証のためのデバイスとして使うことができるようになりました」と述べています。

パスワードのない未来への責任を率いる Microsoft は、ユーザーにシームレスでパスワードなしのログイン体験を

Microsoft Windows 10デバイスがFIDO2認定

グローバルで8億台を超えるアクティブなWindows 10デバイスに安全なパスワードレス認証をもたらします。Windows HelloはFIDO2標準に準拠するように構築されているため、Windows 10デバイスを正式に認定されたFIDO認証のためのデバイスとして使うことができるようになりました。(2019年5月6日)





FIDO JAPAN WGGの活動と 日本での展開状況

FIDO Japan WGのミッションと主な活動

ミッション

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

2016年11月発足発表時の体制

座長・副座長
プログラムマネジャー

翻訳SWG

マーケティングSWG

デプロイメント @
スケール SWG

技術SWG

FIDO Japan WG活動の一つ～東京セミナー



- 第5回FIDO東京セミナー（2018年12月7日開催）には国内外から11名による講演に300名超の聴衆を集め、FIDO2の最新状況、FIDOセキュリティ認定、GDPR（EU一般データ保護規則）とFIDO標準について、そして実際のFIDO導入事例を広く紹介しました。

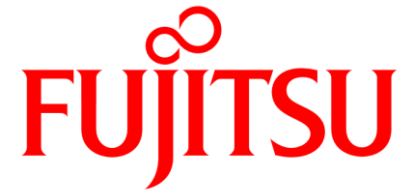


国内から参加しているFIDOアライアンスメンバー

ボードメンバー



スポンサーメンバー



アソシエートメンバー

- Copy, Inc.
- e Doktor Co, Ltd.
- Passlogy Co., Ltd
- Quado, Inc.
- SECIOSS, Inc.

FIDO Japan WG参加メンバー



国内におけるFIDO認証の導入状況



※ FIDO認定製品またはFIDO認定製品を活用するソリューション製品の提供企業、またはそれらを導入済または導入予定時期公表済の企業

NTTドコモによるFIDO UAFの商用導入事例

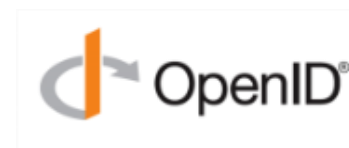


2015年5月にdアカウント認証にFIDO標準を適用以来、2018年にはプラットフォームベースの新しい実装に移行



Step-1: FIDO® UAF 1.0 Certified (認定) 36機種 (2015年5月~2017年)

Step-2: 全Touch ID・Face ID搭載iOS端末~UAF 1.0アプリ対応 (2016年3月~)



Step-3: UAF 1.1アプリでドコモスマートフォン (Android) 以外にも対応 (2018年~)



国内における主なFIDO UAFの商用導入



東京電力パワーグリッド



2017年9月



2018年2月



2018年11月



2018年12月



2019年3月

NTTドコモ・NTTデータ以外での主なFIDO UAFの商用導入事例

国内メンバー企業によるFIDO2認定製品



2018年9月27日



2018年12月7日



2019年3月11日

※ グローバル全体での認定取得製品は順次発表予定

サービス提供者として世界初のFIDO2商用導入



シンプルで堅牢な認証を実現



2018年10月23日



The Upcoming Deployment in 2019

LINE



最近の主なFIDO認証 商用導入事例



ソフトバンク「My SoftBankプラス」をFIDO認証を使ったログインに対応（2018/2/1）

ヤフー サービス提供者として世界初となるFIDO2（Web認証）の商用導入を開始
Yahoo! JAPAN IDのパスワードレス認証に適用（2018/10/23）

三菱UFJ銀行 インターネットバンキングのスマートフォンアプリに指紋や顔でログインできる生体認証機能をリリース（2018/11/21）

富士通 保険とITを融合させたインシュアテック向けソリューションにFIDO認証を導入、
アプリの新しい「即時支払いサービス」に提供開始予定（2018/12/17）

富士通 テプコシステムズが開発した電柱保守業務を効率化する新システムにFIDO認証を導入し、
東京電力パワーグリッドで運用開始（2019/3/4）

LINE、FIDO認証を導入予定と発表。FIDO2対応を含むユニバーサルサーバーを活用して
の対応を表明（2019年予定）



FIDO認定プログラム

FIDO認証に関する刊行物

- “FIDO認証の概要説明”, FIDO Japan WG.
 - <https://www.slideshare.net/FIDOAlliance/fido-83445442>
- “FIDO（ファイド）認証とその技術”, 電子情報通信学会論文誌 Fundamental Review, 2018.
 - https://www.jstage.jst.go.jp/article/essfr/12/2/12_115/_pdf/-char/ja
- “FIDO認証”, 日経FinTech年鑑, 2019.

- FIDO認証モデル
 - パスワードへの依存度を軽減する公開鍵暗号を用いた認証。
- FIDO認証の技術仕様
 - FIDO2 (Web認証 + CTAP) リリース。認定開始。
 - ブラウザー・プラットフォームがFIDO認証へ対応。
- FIDO認証の応用
 - UAF・FIDO2への商用導入、パスワードレス認証の事例が増加。
 - Android/Windows HelloのFIDO2認定取得、エコシステム拡大。
- 日本での活動と商用展開
 - 東京セミナーや説明会・講演、記事寄稿など幅広く活動、商用展開を推進。

ご静聴ありがとうございました。

お問い合わせ先

- info@fidoalliance.org
FIDOアライアンスへの参加などに関するお問い合わせ先
- press@fidoalliance.org
FIDOアライアンスへの取材に関するお問い合わせ先