fido ALLIANCE | simpler stronger authentication

日本銀行決済機構局 ISOパネル（第7回）
生体認証技術の金融サービスへの活用 ―新しい国際標準ISO 19092の概要と活用可能性―

FIDO認証とスマートフォンにおける生体認証技術

2023年3月6日

株式会社NTTドコモ　チーフ セキュリティ アーキテクト（経営企画部 セキュリティイノベーション統括）
FIDOアライアンス　執行評議会・ボードメンバー FIDO Japan WG座長

森山 光一

FIDOアライアンスにおけるIndividual Contributorsのお一人、
新崎 卓様にご協力をいただいて作成しています。

森山 光一（もりやま こういち）

株式会社NTTドコモ　チーフ セキュリティ アーキテクト
経営企画部 セキュリティイノベーション統括担当 コーポレートエバンジェリスト

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
W3C, Inc. 理事（ボードメンバー）

フェリカネットワークス株式会社 社外取締役（非常勤）
日本スマートフォンセキュリティ協会 副会長・理事

情報セキュリティ大学院大学 博士後期課程

慶應義塾大学　理工学研究科　計算機科学専攻　修士課程　修了。ソニー株式会社入社。株式会社NTTドコモ　移動機開発部（出向）、ソニー・エリクソン・モバイルコミュニケーションズ株式会社、ドコモのシリコンバレー拠点を経て、2014年7月からプロダクト部でFIDO認証のプロジェクトに着手。2015年5月からFIDOアライアンスのボードメンバー、2016年10月からFIDO　Japan　WG座長、2019年1月からFIDOアライアンス執行評議会メンバー。進化するソフトウェアとモバイルを軸に経験を重ね、端末を起点にオープンイノベーションを推進。2020年7月からセキュリティサービス・基盤に注力し、2022年7月より現職。

https://www.linkedin.com/in/koichi-moriyama-92669b23/

本日の内容

- FIDO認証について
- スマートフォンにおける生体認証について
- FIDOアライアンスにおける生体認証への取り組みについて
- FIDO認証のさらなる普及に向けて

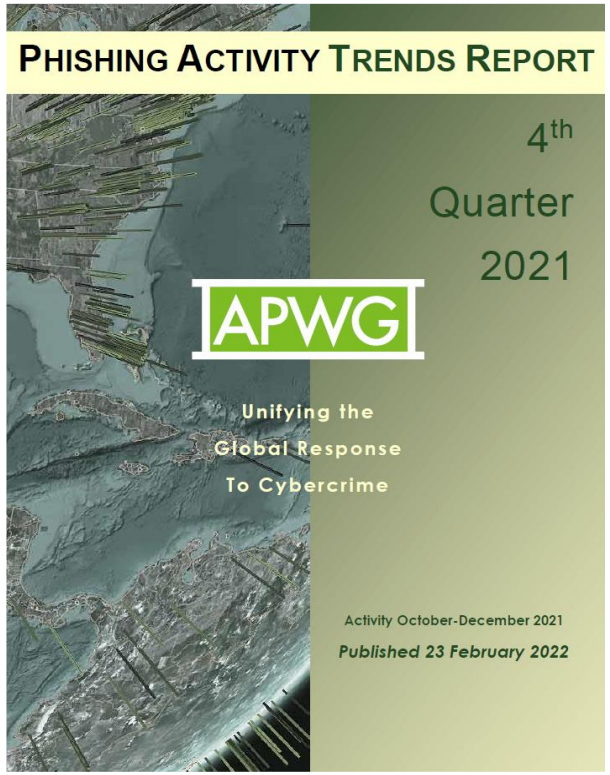
WHY FIDO?

パスワード課題への挑戦

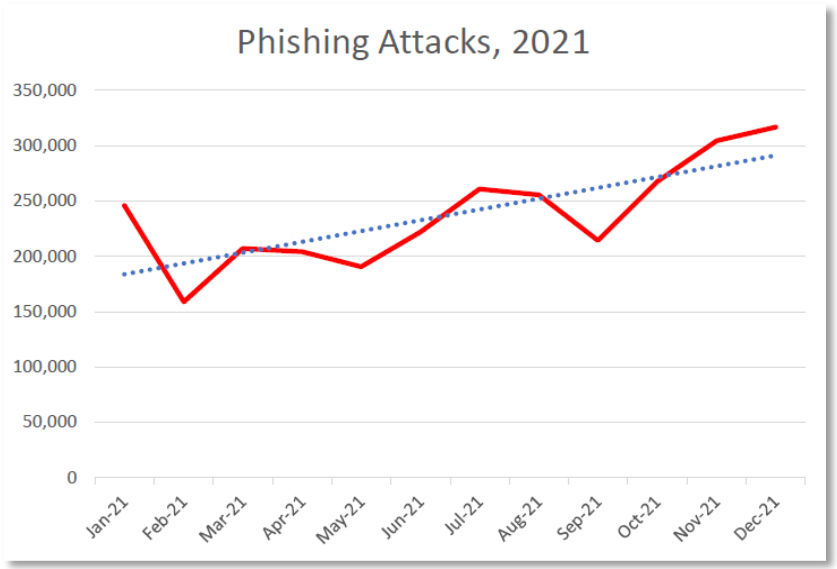
CLUMSY | HARD TO REMEMBER | NEED TO BE CHANGED ALL THE TIME

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/

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

From legacy, **knowledge-based** credentialing

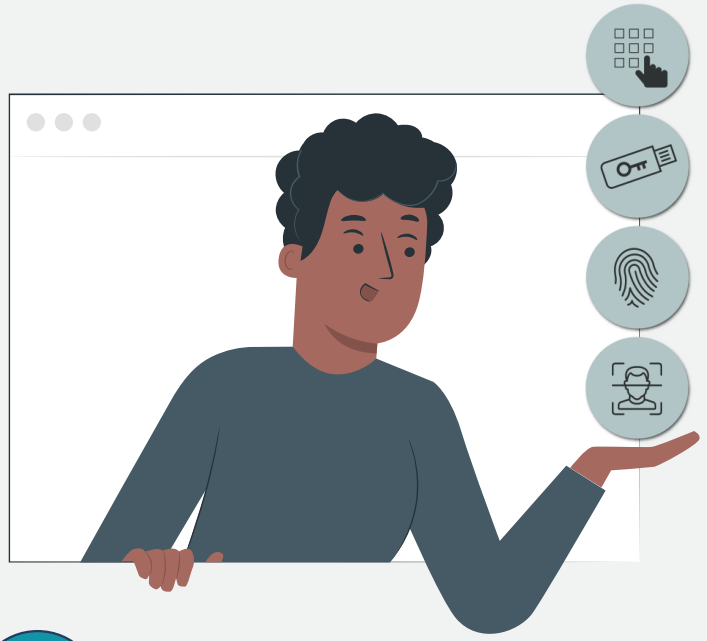
In your head (remembered)

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

SUSCEPTIBLE TO COMMON THREATS

To modern, **possession-based** credentialing

In your hand

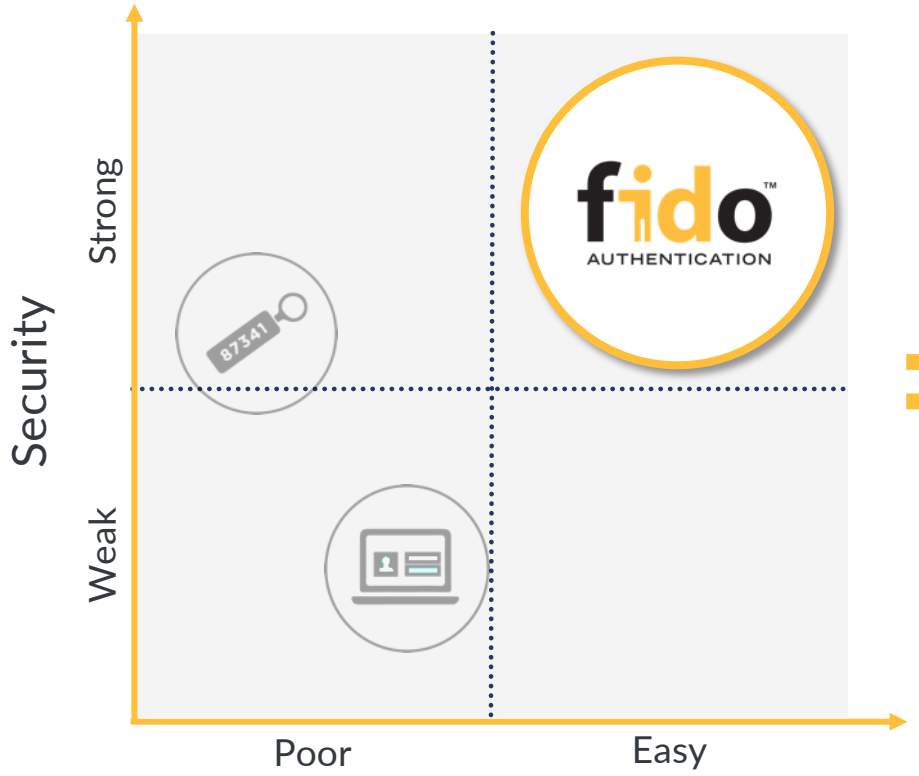


- On-device
- Local Biometric / PIN
- DocAuth
- “Passkeys”

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

=

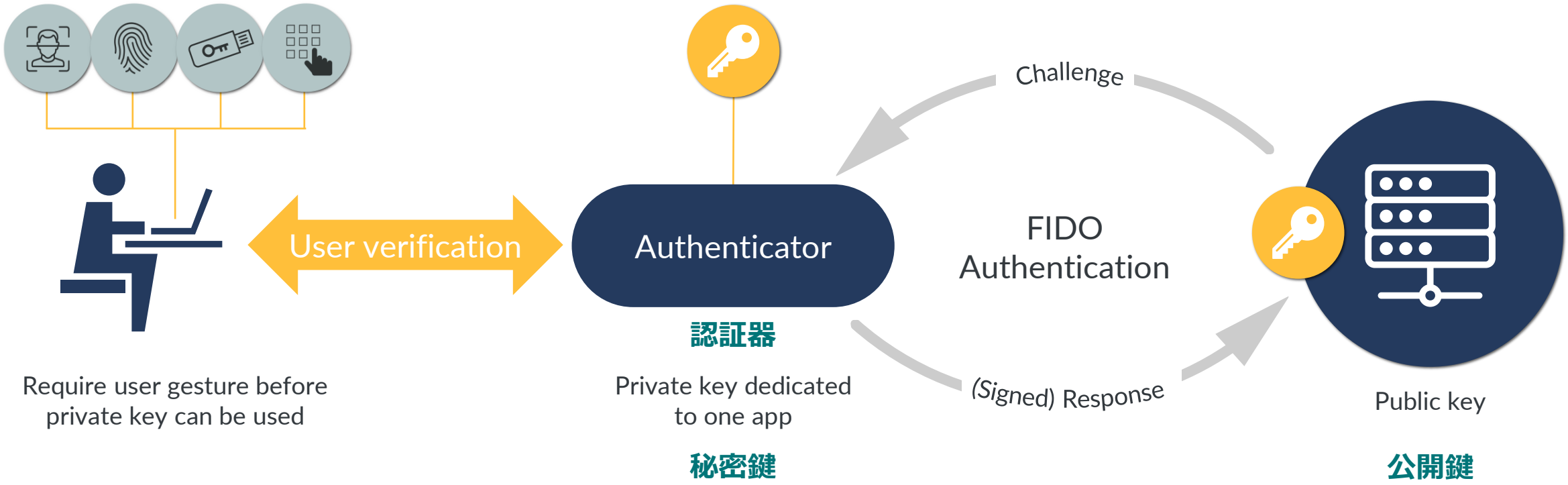
公開鍵暗号方式を活用したオンライン認証

Open standards for simpler, stronger authentication using public key cryptography

Single Gesture
Possession-based Authentication

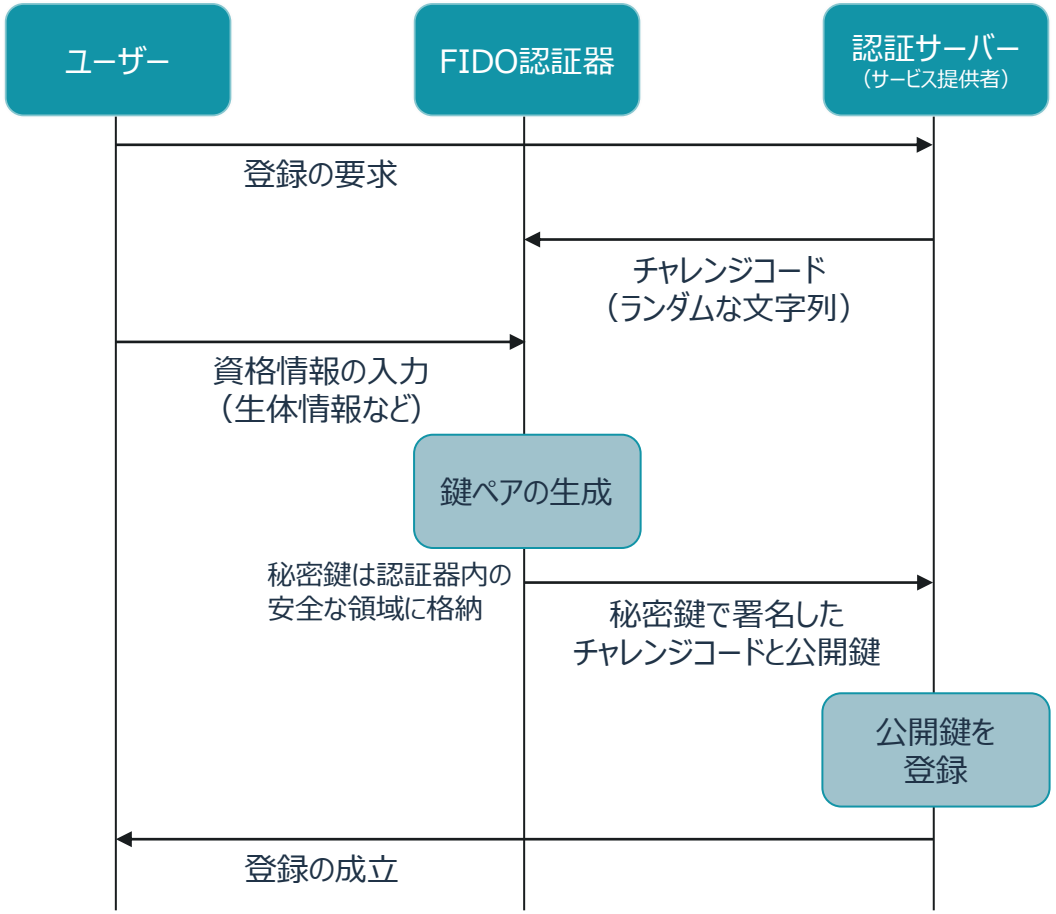
「所持」を伴う多要素認証を「シングルジェスチャー」で

FIDO Authentication: How it works

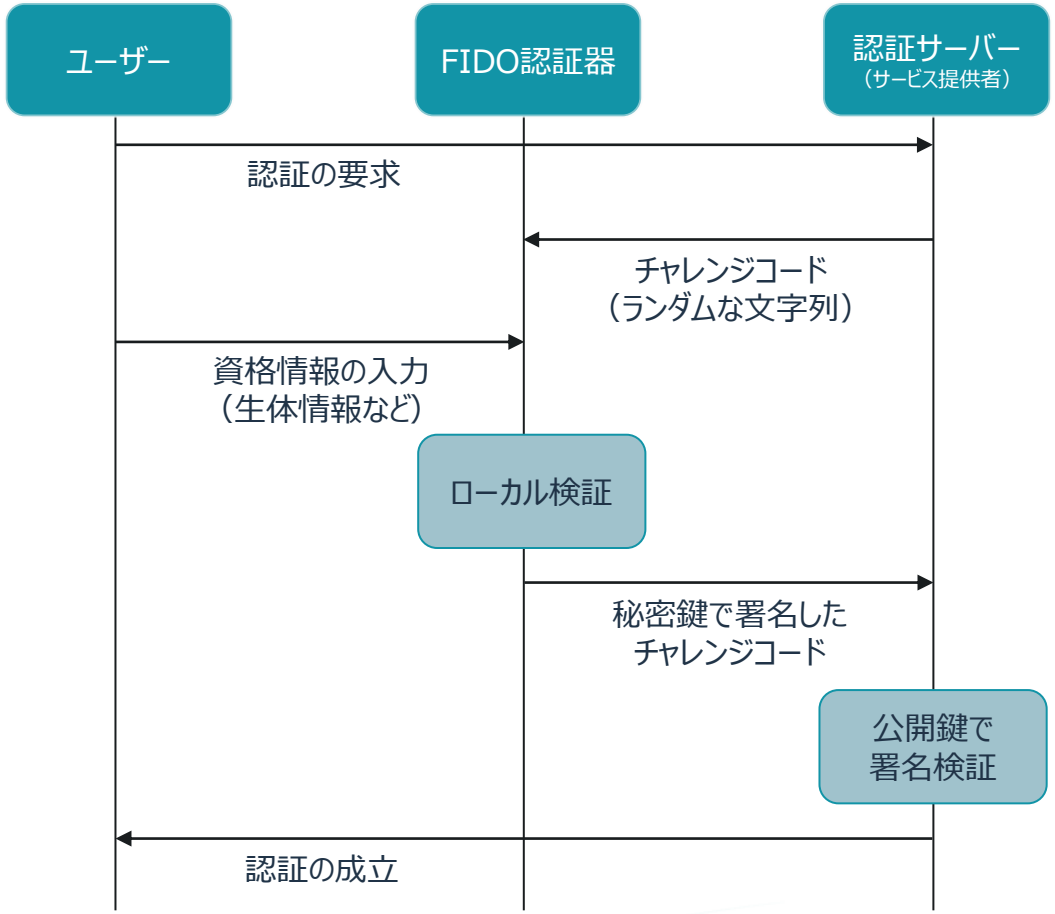


FIDO認証の流れ（「秘密」がインターネットを通過しない）

設定（登録）時



認証時



（出典：ドコモ テクニカルジャーナル Vol.28 No.1 Apr. 2020）

FIDO認証 ≠ 生体認証

それでも親和性がとても良いことにはまちがいがない。
それは「フィッシング耐性」のある認証（≠サーバーマッチング）

FIDO認定プログラム

- 機能認定（エンド・エンド）：（2015年～）
  - 適合性テスト
  - 相互接続性テスト

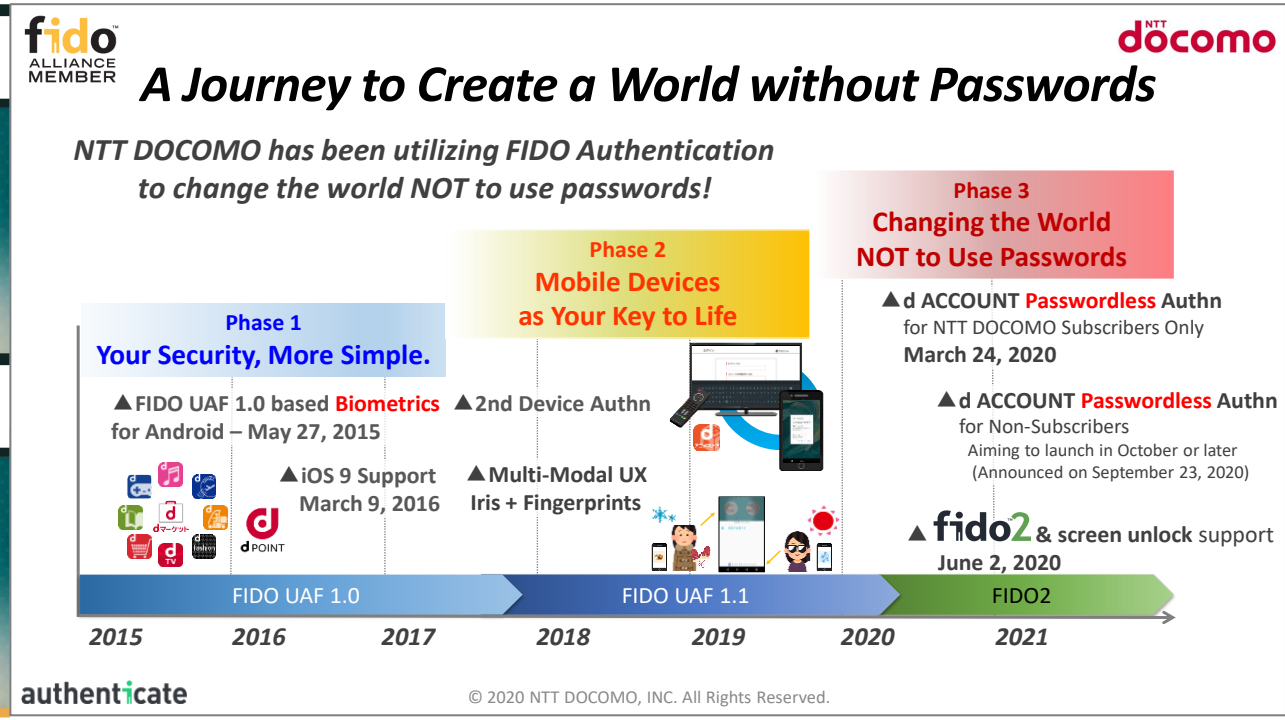
- FIDO認証器のセキュリティ認定：（2016年～）
  - 秘密鍵保護がどれだけ優れているか？
  - 第三者ラボによる検証

- バイオメトリクス部品認定：（2018年～）

- 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

FIDO認証～最初のエコシステム、そして発展

（2015年5月27日）



（2020年9月23日）

2015年当初からのさまざまな世界初～エコシステムの営みの中でFIDO認証が「あたりまえになる」ことをめざした8年半

ご参考：スマートフォンの生体認証機能に関連した指摘等と対応事例

- スマートフォンに生体認証機能が搭載されるようになって以来、その黎明期から最近にかけて、まったく指摘等がなかったわけではない。適宜、指摘を受け止め、対応してきた。
  - セキュリティに関するイベントBlack Hat USA 2015で、ドコモでは採用していない企業によるグローバル仕向けスマートフォンで、生体情報が暗号化されないまま第三者アプリが読み出し可能な方法で格納されていることが発表され、警鐘が鳴らされた。（ドコモでは、当時から安全な特別領域に格納）
  - 2016年3月、粘土に自分の指紋の形を作り、指紋センサーに押し当てることで指紋認証できるというビデオクリップが広く出回り、話題になった。粘土で作った型で登録したパターンはその型で認証できることがあるが、本来あるべき手続きで登録された指紋の認証は難しいことが知られつつ、それ以前からのセンサーベンダーの尽力によってスプーフィング攻撃への耐性向上が進んだため、近年は問題として指摘されることは少なくなった。
  - 2016年10月、生体認証に関するウルフパターン関連技術と攻撃可能性について指摘を受けた。FAR 1/50,000以下の指紋センサーを攻撃して突破できる確率はきわめて低いと確認できた。
  - 2017年4月、スマホで撮ったピース写真から指紋が盗み取られ、勝手に進入される危険があるとの報道が広くなされた。FIDO Japan WGとして記者説明会・記者発表会する際も指紋がみえるポーズを止めた。実際のところ、市場から写真から指紋が盗み取られて認証されたと疑われるご指摘は届いていない。
  - 2019年10月、Samsung Galaxy S10に搭載されたディスプレイ埋め込み型指紋センサーについて、特定の画面保護フィルムを張り付けた場合に誰でも指紋認証を突破できるとの指摘・報道がなされ、Samsung社が速やかに生体認証のソフトウェア更新を発表した。一時的に当該機種による生体認証の利用制限を行ったサービス提供者もあった。

ご参考：生体認証のためのセンサー・部品の取り扱いについて

- スマートフォンへ生体認証機能を積極的に搭載することとした当時、Android OSに標準的な生体認証APIがなく、Android OSの最新バージョン毎にリリースされる互換性定義ドキュメント（CDD）にも生体認証のための要求条件が示されていなかったため、ドコモとして積極的にセンサー・部品ベンダーとも情報・意見交換を行った。また、原則として端末メーカーから採用部品と端末装置としての性能について開示を受け、信頼性の確保に努めた。
  - スマホに搭載されている生体認証装置は、センサー部分に注力しているベンダー、そのセンサーを使ってモジュールとして端末メーカーに提供しているベンダーなどに役割が分担されている場合がある。また、端末装置全体として複数の部品と技術を組み合わせて実現するケースもある。営業上の秘密として情報開示を受けられない場合もある。
- その後、市場と業界の両方から、なりすまし攻撃への耐性の重要性が強く認識されるようになり、動向を注視した。また、引き続き、性能が確保されていない部品や生体情報がアプリケーション領域を通過するなどなりすまし攻撃に脆弱性のある実装は、dアカウントのFIDO認証に使えないように区別した。
- 回線契約をお持ちではないお客さまを含めて広くご利用いただくため、ドコモ以外の端末についても便利にあんしんしてご利用いただける方策を模索し、ドコモ以外の端末も個別に確認する手続きを開始した。
- 現在では、CDDで生体認証のための要求条件が整備され、また、Googleから出荷承認のある端末にのみ搭載されるGoogle Play開発者サービスを搭載していない端末でFIDO認定を取得したFIDO2の標準実装が動作しないなど環境が整ったため、すべての端末の個別確認は実施しない運用に移行した。

ご参考：Android OSの「ロック解除」で利用できる認証方法

～CDD（Compatibility Definition Document）における生体認証の位置づけ～

認証レベル	概要
プライマリ認証	• 知識認証ベース（端末ローカルのPIN/パスワード/パターン） • 最もセキュア
セカンダリ認証 生体認証 （強・Strong/Class 3）	• **生体認証**（FAR: 0.002%以下、SAR/IAR: 7%以下（※）） ※ Android Biometrics Test Protocols https://source.android.com/security/biometric/measure に準じて測定する。 • 72時間毎に1度はプライマリ認証が求められる • FIDO2 APIで利用可能
生体認証 （弱・Weak/Class 2）	• 生体認証（SAR: 7%超で「弱・Weak」、20%超で「便利・Convenient」） • 4時間以上利用しない場合、1度はプライマリ認証が求められる • FIDO2 APIでは利用できない
ターシャリ認証	• 操作を必要としないパッシブ認証など • 上記より弱い

https://source.android.com/compatibility/10/android-10-cdd
https://source.android.com/compatibility/11/android-11-cdd

FAR: False Accept Rate – 他人受入率。ランダムな他人の生体情報を誤って認識してしまう率
SAR: Spoof Accept Rate – スプーフィング攻撃への耐性。録音した音声での攻撃など
IAR: Imposter Accept Rate – なりすまし攻撃への耐性の指標　上記の強・弱はこれら3つの率の組み合わせで定められている。

Google Android CDDにおける生体認証に関する要件

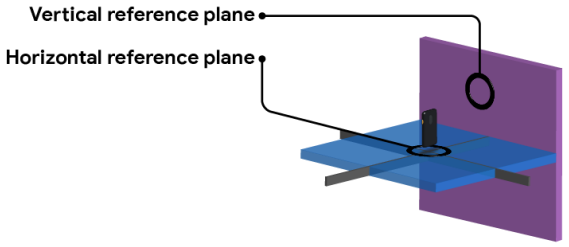
- Android CDDの7章 “Hardware Compatibility” 7.3節 “Sensors” 7.3.10項 “Biometric Sensors” で生体認証装置（センサー）について要件が定められている。ここで、冒頭「端末がセキュアな画面ロック解除（Secure Lock Screen）を実装するのであれば※、生体認証装置を具備することが望ましい [SHOULD]」と位置付けられている。※ 後述の9.11.1項で STRONGLY RECOMMENDED として強く実装が求められている。
  - 生体認証装置は、その性能によってClass 3（強）、Class 2（弱）、Class 1（便利）に分類されている。
  - 端末に搭載するアプリ（サードパーティアプリ）が生体認証を使えるようにするためにはClass 3またはClass 2の要件を満たすことが必須 [MUST]。
  - 端末の実装がアプリにkeystore keysへのアクセスを許可するのであれば、Class 3の要件を満たすのが必須。そして、アプリが “BIOMETRIC STRONG”（強）を要求したらClass 3のセンサーを動作させることが必須。
  - 一定以上使われていない場合、一定時間経過後、あるいは3回生体認証に失敗した場合、推奨されているプライマリー認証による代替えの認証手段を求めることが必須。
- また、同項で、生体認証の要件に対する測定・評価については、別の文書 “Measuring Biometric Security documentation” https://source.android.com/security/biometric/measure を参照するよう指示されている。
- 9章 “Security Model Compatibility” 9.11節 “Keys and Credentials” 9.11.1項 “Secure Lock Screen and Authentication” において、PIN/パスワード/パターン（または同等）によるセキュアな画面ロック解除をプライマリー認証、生体認証をセカンダリー認証とできることが定められている。

Googleによる生体認証のセキュリティ測定のガイダンス

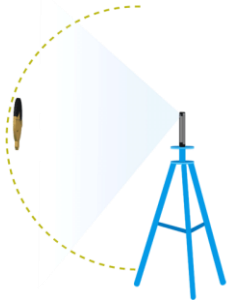
- Android CDDから参照されている生体認証の要件に対する測定・評価に関して公開されている文書で、生体認証の実装に関するセキュリティの評価についてのガイダンスが示されている。
- （GP-SEが搭載されるようになった）Android 9のCDDから導入されたSpoof Acceptance Rate（SAR）について、顔・虹彩認証、指紋認証それぞれについて、測定・評価に先立つ「調整フェーズ」と実際の測定・評価を行う「テストフェーズ」について、具体的なガイダンスが示されている。

【顔・虹彩認証の例】

調整フェーズ：顔の写真や3Dプリントされた仮面、目の写真や義眼を準備し、測定・評価環境を整える。



基準位置の準備



垂直弧と水平弧に沿ったテスト
デバイスの左右と上下で 10 度ずつ位置を変えて繰り返す

テストフェーズ：SAR算出方法、試行回数などがガイドされている。

調整フェーズを終えると、2D と 3D のスプーフィング可能性をテストするための 2 つの調整位置（2D と 3D を合わせて）が得られます。調整位置を決定できない場合は、基準位置を使用します。テスト方法は 2D と 3D で共通で、非常に単純です。

- 登録する顔の総数を E >= 10 とし、異なる顔を少なくとも 5 つ含めます（つまり、最小のテストでは、5 つの異なる顔を 2 回ずつ繰り返すことになります）。
  - 顔または虹彩の登録
  - 前のフェーズで得られた**調整位置**を使用して、ロック解除を U 回試行します。前のセクションで説明した方法で試行回数をカウントし、U >= 10 になるようにします。成功したロック解除数（S）を記録します。
  - 以上により、（2D と 3D で別々に）SAR の測定値を以下のように算出できます。

$$SAR = \frac{\sum_{i=1}^{E} S_i * 100}{U * E}$$

ここで

- E = 登録数
- U = 登録ごとのロック解除試行回数
- Si = 登録 i の成功したロック解除の数

（出所：https://source.android.com/security/biometric/measure）

※ 端末メーカーはより詳細に定められた手順に従って測定・評価した結果をGoogleに提出し、CDD準拠の端末として出荷承認を得ている。

スマートフォンに搭載されている生体認証装置の利用について

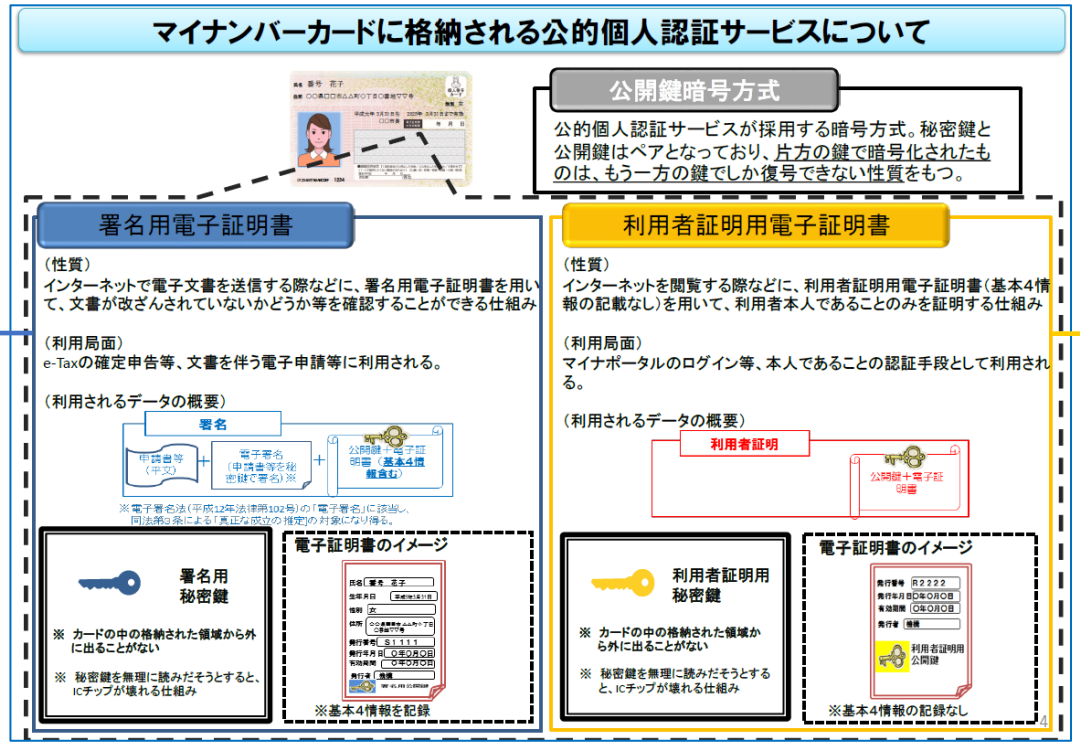
- スマートフォンにおける生体認証装置の搭載が一般的になった。いわゆるサーバーマッチング方式ではなく、端末の安全なところに生体情報を保管してローカルで照合する方式が国内外を問わず広く普及したことから、プライバシー保護の観点などを踏まえても、安心してお使いいただける状況になって来たものと考える。
- 生体認証は、暗証番号やパスワードなど知識とのマッチングと異なり、生体認証装置から入力された情報から特徴点を抽出し、数学・統計的に処理して照合するため、その結果が絶対に同じになることは保証できないと言われている。そのため、生体認証の利用に際しては、利用者へ丁寧な説明が必要になる。
  - ドコモでは、サービス・機能の一つとして、生体認証に関する情報発信をしている。また、dアカウント規約では第5条 dアカウントによる生体認証等の利用 を定めている。また、試行回数によってロックを掛けるなども要件化してきた。
- ドコモは、生体認証装置をスマートフォンに積極的に搭載を進めた当初、Googleとして定めるものがない時期は、ドコモとして要件を定め、端末メーカーに実装を要請し、ドコモとして品質確保に努めた。その後、スマートフォンのエコシステムに貢献しながら、エコシステムが定めるAPIと要件に合わせるようにシフトした。現在、スマートフォンに搭載されている生体認証装置は、プラットフォームOSを問わず、端末メーカーによる製品の一部として具備されている。Androidの場合には、Googleが定めるCDD（Compatibility Definition Document）に記載される要件を満たした実装が提供されている。
- マイナンバーカードの利用者がスマートフォンに搭載される生体認証装置を利用することについては、万一意図せぬ動作をした場合などの考え方について、事前に整理・整頓しておく必要があると思われる。

1. スマートフォン搭載における生体認証の利活用について

ドコモにおける世界初の虹彩認証搭載スマートフォンを含む生体認証対応Androidスマートフォンの FIDO対応（2015年5月）を基点とし、業界の連携で、スマートフォンにおける生体認証の搭載と利用が一般的となりました。これを実現しているしくみ等を勘案し、GP-SEを搭載するスマートフォンでは、利用者証明用電子証明書の利用シーンからスマートフォンに搭載している生体認証を活用することを提案します。

署名用パスワード 半角文字
6文字から16文字まで、かつ、
数字とアルファベット の混在

市場のスマートフォンに搭載の
生体認証装置で証明書の
所持者であることを検証可能か、
要継続検討



利用者証明用パスワード
（暗証番号）4桁の数字

市場のスマートフォンに搭載の
生体認証装置で証明書の
所持者であることを検証可能

提案1-1: Android OSが提供するAPIとマイナンバーカードの機能のスマートフォンへの搭載における生体認証の利活用に向けた実現方法について

- Androidスマートフォンに具備されている生体認証の機能は、アプリケーション開発者にBiometricPrompt APIが提供されようになったAndroid 9以降は特に以前と比較して成熟している。CDDによって要件が明確になり、性能測定・評価についても定められている。そこで、マイナンバーカードの機能のスマートフォンへの搭載にあたっては、生体認証の性能について強・Strong/Class 3を使用するため“BIOMETRIC_STRONG”を指定することを前提に、既に議論して来た「ローカルPIN」による認証に加えて、生体認証（BiometricPrompt API）の結果を使えるようにしてはいかがでしょうか？
  - この場合、Androidに標準で搭載されているFIDO2実装と同様にSafetyNet APIを使ってAndroid端末が正規の端末であるかをチェックするなどのしくみも導入することが望ましいと考える。
  - NISTのガイドライン、CDDなどに準じて、生体認証が動作しないときに備えて、あるいは生体認証が一定回数失敗したときには、「ローカルPIN」を利用可能にしておく必要があると考える。
  - Android端末として出荷承認を受けている端末は、ガイダンスにしたがって性能測定・評価された結果が確認されていることから、追加の第三者評価等を実施する必要はないものと考える。ただし、疑義が生じたときには関係者に確認を求める手段を確保しておくことが望ましい。
  - いずれにしても、万一の問題発生時に備えて、ドコモが実施しているように、問題発生時には対象端末等から機能を無効化する手段などについても準備をしておくことが必要と考える。

提案1-2: 生体認証の利活用に際し、ローカルPIN導入の課題と使い勝手の改善に資する画面ロック解除の利活用について

- マイナンバーカードの機能のスマートフォンへの搭載にあたっては、マイナンバーカードに設定する署名用パスワード、利用者証明用パスワード（暗証番号）に加えて、GP-SEに「ローカルPIN」を設定する必要があると認識している。この「ローカルPIN」を利用者に別途覚えていただくことについて、使い勝手の観点から懸念が指摘されている。この解決のため、スマートフォンにおける生体認証が「セキュアな画面ロック解除（Secure Lock Screen）」におけるセカンダリー認証の位置づけであることを勘案し、プライマリー認証である画面ロック解除のために設定するPIN/パスワード/パターンも利活用できるようにしてはいかがでしょうか？（生体情報を登録するには、利用者はPIN/パスワード/パターンの登録が必須・前提となっている）
  - この場合、Androidに標準で搭載されているFIDO2実装と同様に、設定済の利用者には生体認証を促し、利用者が選択した場合または生体認証に一定回数失敗した場合には、画面ロック解除のために設定されたPIN/パスワード/パターンでもスマートフォンに搭載したマイナンバーカードの機能を利用できるようにする。
  - 画面ロック解除のために設定されたPIN/パスワード/パターンは、利用者が毎日スマートフォンを使うためのものであるため、基本的には忘れることがない。利用者にはご自身のスマートフォンを守るためにも画面ロックの設定を促す。そして、他者に類推されないようなPIN/パスワード/パターンの設定を促す。また、見られないように促す。
  - スマートフォンに搭載された生体認証の設定率は100%に至っておらず、至ることはないと考えられ、その性能もすべてが強・Strong/Class 3なるとは限らないことからも、効果的なアイデアと考える。
  - 万一の問題発生時には、生体認証（または画面ロック解除）を使えないようにして、この場合には「ローカルPIN」で引き続きスマートフォンに搭載したマイナンバーカードの機能を利用できるようにする。

提案1-2に対する補足: SP 800-63Bにおける スマートフォンに搭載されたPINに関する記述について

- NIST SP 800-63Bの4章2節 “Authenticator Assurance Level 2” にある5項のうち4.2.2項 “Authenticator and Verifier Requirements” に下記の記載がある。

  “When a device such as a smartphone is used in the authentication process, the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors. Generally, it is not possible for a verifier to know that the device had been locked or if the unlock process met the requirements for the relevant authenticator type.”

  これについて、SP 800-63Bが執筆された時期（2017年6月発行）当時の一般論としての記述として尊重されるべきものだが、現在のスマートフォンOSにおける画面ロックは、より安全な実装が行われている。

  – Android OS 5.0（CDD 2015年1月発行）で画面ロックの実装を伴う場合のストレージの暗号化が必須要件化された。
  – Android OS 6.0（CDD 2015年10月発行）で9章 “Security Model Compatibility” 9.11節 “Keys and Credentials” に「セキュアな画面ロック解除（Secure Lock Screen）」が定義され、セキュアハードウェアを使った実装が要件化された。
  – Android OS 7.0（CDD 2017年4月発行）で9.11.1項 “Secure Lock Screen” が起こされ、セキュアな画面ロックとセキュアハードウェアを使った実装について複数の項目が必須要件化された。以降、毎年、見直しと更新が行われている。

  また、今回の提案はスマートフォンの画面ロックが解除されていること自体を多要素認証の一要素とするのでなく、画面ロック解除のために設定されたPIN/パスワード/パターンを一要素とするもの。これらを勘案し、提案1-2は合理的にその妥当性を確保しているものと考える。（セキュリティと利便性の両立）

FIDOバイオメトリクス部品認定

- バイオメトリクスサブシステムの客観的な性能評価を可能とするため2018年から提供開始。改訂を重ね、バージョン3.0を策定（2022年12月）
- 「ラボテスト」と「テスト文書の提出による自己証明」で構成、ラボテストで偽造受入率を評価
  - 「設定（登録）」で登録したテンプレートと入力とマッチング。マッチングソフトウェアは運用上の実装と同等であることを検証
  - 被験者は複数の偽造物に対して各5トランザクションを実行する。それぞれ複数回の生体入力試行を含む
  - 被験者の多様性（年齢、性別）を必要とする

FIDOバイオメトリクス部品認定3.0

- 低コストの評価をサポート
- プラットフォームが定める閾値と評価手法との間の整合性を向上
- ISO規格との整合性を更新（性能試験、PAD、用語定義）（2022年12月）

参照しているISO/IEC JTC1/SC37の国際標準規格

- ISO/IEC 19795-1:2021 バイオメトリック性能試験及び報告
- ISO/IEC 19795-9:2019 モバイルデバイスの性能試験
- ISO/IEC 30107-3:2023 バイオメトリックPADテストとレポート
- ISO/IEC 30107-4:202（改版中）モバイルデバイスのPADテストプロファイル
- ISO/IEC 2382-37:2022 バイオメトリクスの用語定義

FIDOバイオメトリクス部品認定3.0の主な要件

認定レベル	FIDO Bio 1	FIDO Bio 1+ （v2.2のレベル1）	FIDO Bio 2	FIDO Bio 2+ （v2.2のレベル2）
ラボテスト				
サンプル数（FRR/FAR）	25	245	25	245
FAR（他人受入率）	1%	0.01%	1%	0.01%
FRR（本人拒否率）	7%	5%	7%	5%
偽造物の種類 （レベルBの方が精緻）	レベルA：6 レベルB：8	レベルA：6 レベルB：8	レベルA：6 レベルB：8	レベルA：6 レベルB：8
偽造物の種類毎のサンプル数	15	15	15	15
IAPAR（偽造受入率）	15%	15%	7%	7%
テスト文書の提出による自己証明				
FAR	必須：0.01% オプション：0.004%、0.002%、0.001%	オプション：0.004%、0.002%、0.001%	必須：0.01% オプション：0.004%、0.002%、0.001%	オプション：0.004%、0.002%、0.001%
FRR	必須：5%	オプション：5%	必須：5%	オプション：5%

FIDOバイオメトリクス部品認定3.0におけるPAD要件

- 低レベルのなりすまし攻撃をテストするためのガイドラインを新たに提供
  - 低レベルのなりすまし攻撃：偽造物の作成で最小限の専門知識を必要とするもの。より少ない時間・知識・装備で攻撃可能なもの
- IAPAR（Imposter Attack Presentation Accept Rate。偽造受入率）を測定
  - プレゼンテーション・アタックの成功率をスプーフィングの種類毎に測定
- ベンダーが提供する生体認証サブシステムでテストすることを想定
  - 「既知」の攻撃のみを対象。将来の認証のために “Unknown” な攻撃の定義を予約
- 評価プロセス
  - 非人工物（生体）として登録された被験者1人あたり少なくとも14種類のPAI* を用いた試験を15人、各10トランザクション

(*) Presentation Attack Instrument (PAI) – プレゼンテーション・アタックに使用される生体特性または物体。共通の製造方法を用いて作成され、異なる生体特性に基づく提示攻撃機器の種類（ISO/IEC 30107-3）

FIDO PAD要件3.0における偽造物の種類とレベル

		指紋	顔	虹彩	音声
レベルA	**時間**： ＜ 1日 **専門分野**：素人 **装備**：標準	紙へのプリントアウト、スキャナでの潜像印刷の直接利用	顔写真の紙面プリントアウト、携帯電話による顔写真の表示	虹彩画像の紙への印刷、虹彩写真の携帯電話への表示	録音音声の再生
	バイオメトリクスのソース： 入手は容易	携帯電話の遺留指紋採取	ソーシャルメディアの写真	ソーシャルメディアの写真	音声の録音
レベルB	**時間**：＜ 7日間 **専門知識**：熟練 **装備**：標準装備、専用装備	ゼラチン、シリコンなどの人工素材から作られた指紋	ペーパーマスク、ビデオによる顔面表示（動き・まばたきあり）	虹彩の動画表示（動きあり・点滅あり）／紙のプリントアウト／コンタクトレンズ／人形の眼	特定のパスフレーズを録音した音声の再生、声帯模写、音声合成（簡単なもの）
	バイオメトリクスのソース： 中程度	遺留指紋の採取、盗難指紋画像（協力的な型の作成は対象外）	被写体の動画、高画質写真	被写体の動画、高画質写真	特定フレーズの音声の録音
レベルC	**時間**： ＞ 7日間 **専門家**：専門家（複数） **装備**：特注品	3Dプリンターによるスプーフィング	シリコンマスク、演劇用マスク	コンタクトレンズまたは義眼	ボイスシンセサイザ
	バイオメトリクスのソース： 入手困難	被験者からの3D指紋情報	被写体からの3次元顔情報	近赤外高画質写真	複数録音音声による シンセサイザの学習

FIDOバイオメトリクス部品認定3.0とAndroid CDD 13との関係

認定レベル	FIDO Bio 1+	Android CDD Class 2	FIDO Bio 2	FIDO Bio 2+	Android CDD Class 3
ラボテスト					
サンプル（FRR/FAR）	245	N/A	25	245	N/A
FAR	0.01%	N/A	1%	0.01%	N/A
FRR	5%	N/A	7%	5%	N/A
偽造物の種類 （レベルBの方が精緻）	レベルA：6 レベルB：8	レベルA、B 認証方式別	レベルA：6 レベルB：8	レベルA：6 レベルB：8	レベルA、B 認証方式別
偽造物の種類毎のサンプル数	15	10	15	15	10
IAPAR（偽造受入率）	15%	レベルA：20% レベルB：30%	7%	7%	レベルA：7% レベルB：20%
テスト文書の提出による自己証明					
FAR	オプション：0.004%、0.002%、0.001%	0.002%	必須：0.01% オプション：0.004%、0.002%、0.001%	オプション：0.004%、0.002%、0.001%	0.002%
FRR	オプション：5%	10%	必須：5%	オプション：5%	10%

FIDOバイオメトリクス部品認定3.0、Android CDD 13と NIST SP800-63-4（Draft）との関係

認定レベル	FIDO Bio 1+	Android CDD Class 2	FIDO Bio 2+	Android CDD Class 3	NIST SP800-63-4（Draft）
ラボテスト					
サンプル（FRR/FAR）	245	N/A	245	N/A	N/A
FAR	0.01%	N/A	0.01%	N/A	0.01%（FMR）
FRR	5%	N/A	5%	N/A	N/A
偽造物の種類 （レベルBの方が精緻）	レベルA：6 レベルB：8	レベルA、B 認証方式別	レベルA：6 レベルB：8	レベルA、B 認証方式別	N/A
偽造物の種類毎のサンプル数	15	10	15	10	N/A
IAPAR（偽造受入率）	15%	レベルA：20% レベルB：30%	7%	レベルA：7% レベルB：20%	10%
テスト文書の提出による自己証明					
FAR	オプション：0.004%、0.002%、0.001%	0.002%	オプション：0.004%、0.002%、0.001%	0.002%	N/A
FRR	オプション：5%	10%	オプション：5%	10%	N/A

FIDOバイオメトリクス部品認定3.0と国際標準規格との関係

FIDOアライアンス

バイオメトリクス部品認定

整合性の確保

規格参照

規格作成貢献
（リエゾン関係）

Google Android Compatibility Definition Document

- バイオメトリクスの性能要件
- 生体認証を用いたロック解除のセキュリティ測定

ISO/IEC JTC1/SC37 バイオメトリクス

- バイオメトリクスの性能評価と報告
  （ISO/IEC 19795シリーズ）
- PAD（偽造弁別）技術の評価と報告
  （ISO/IEC 30107シリーズ）
- バイオメトリクスの用語定義
  （ISO/IEC 2382-37:2022）

生体認証のバイアス評価への取り組み

・顔認証への人種等の影響を評価する仕組みの整備に向けた取り組み

ISO/IEC JTC1/SC37 バイオメトリクス

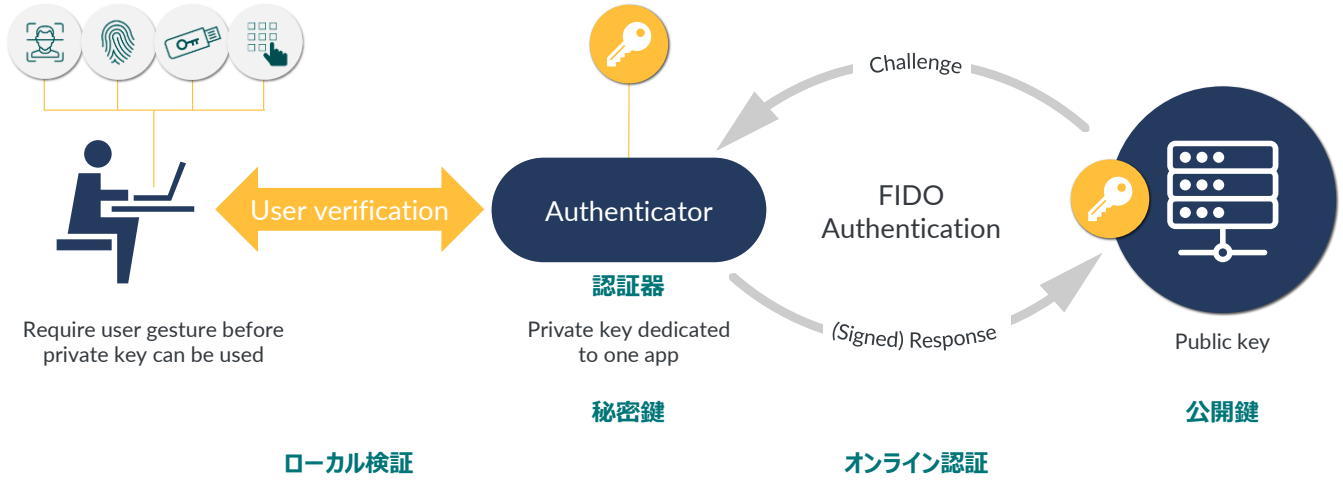
- 生体認証システムの性能の人口統計学的なばらつきを定量化するISO/IEC 19795-10の規格策定

FIDOアライアンス Biometrics Working Group

- ISO/IEC 19795-10のWDを参考に具体的なバイアスの評価方法を検討中

フィッシング耐性のあるFIDO認証をより多くの利用者へ

公開鍵暗号方式を活用したオンライン認証



「所持」を伴う多要素認証を「シングルジェスチャー」で セキュリティと使い勝手の両立をめざす

FIDO = Phishing-Resistant MFA (Multi-Factor Authentication)

マルチデバイス対応FIDO認証資格情報

- FIDO認証・パスワードレス認証の普及に向けて、機種変更などで必要となるサービス提供者毎のFIDO認証資格情報（クレデンシャル）の再登録（再設定）に懸念あり
  ⇒ FIDOクレデンシャルをOSクラウドに保存し、FIDO認証に関する設定も移行
  - 従前の考え方を継承し、FIDOクレデンシャル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。（生体情報は引き続き端末内で管理）

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）

パスワードから「パスキー」へ

1 2 3 4 5 6 7 8 ??

＊ ＊ ＊ ＊ ＊ ＊ ＊ ＊

a password or passwords

（英語）

a passkey or passkeys

（英語）

FIDO認証はフィッシング対策の要～ドコモも「パスキー」

d ACCOUNT

ご清聴、ありがとうございました！

2022年3月6日

FIDOアライアンス　執行評議会・ボードメンバー FIDO Japan WG座長
株式会社NTTドコモ　チーフ セキュリティ アーキテクト（経営企画部 セキュリティイノベーション統括）

森山 光一

FIDOアライアンスにおけるIndividual Contributorsのお一人、
新崎 卓様にご協力をいただいて作成しました。