資料2

第4回 マイナンバーカードの機能のスマートフォン搭載等に関する検討会

スマホならではの使いやすいUXの実現に向けて

2021年1月29日

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）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

森山 光一

はじめに

- 第2回検討会で提案させていただいた内容のうち、1．マイナンバーカードの機能のスマートフォン搭載における**生体認証**の利活用 については、「第1次とりまとめ～電子証明書のスマートフォン搭載の実現に向けて～」における「スマホならではの使いやすいUX」の観点も含めて、具体的な実現方法を提案できればと考えております。
- 使いやすいUXの実現に向けては、「生体認証」の利活用に合わせて、スマートフォンエコシステムで標準的になった「画面ロック解除」のために設定するPIN/パスワード/パターンも活用することで、マイナンバーカードの機能のスマートフォンへの搭載で必要となる「ローカルPIN」の導入に際する懸念を軽減できると考えております。（ぜひ、ご議論いただきたい）
- 本資料では、FIDO認証に関する標準化活動とdアカウント認証への適用を通じてお客さまに生体認証とパスワードレス認証を提供してきた知見から、解決策をご提案できればと思います。

指摘事項・議論すべき観点

- スマートフォンに搭載されている生体認証機能の利活用についてどう要求条件を定め、第三者評価等を実施すべきか？
- 万一の問題等発生時に備えて、責任分界点をどのように定めるべきか？
- 生体認証、ローカルPINの導入の懸念などを勘案し、使いやすいUXをどう実現するか？
- 上記コンセプトを踏まえて、Android OSのAPIを利用し、どのようにマイナンバーカードの機能のスマートフォンへの搭載を実現するか？

内容

- スマートフォンに搭載されている機能を利活用する考え方
- ご参考～ドコモにおけるスマートフォンとdアカウント認証への生体認証の導入事例より
  - 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
  - スマートフォンに搭載した生体認証のためのセンサー・部品の取り扱いについて
  - 万一の問題発生時に備えた対策
  - dアカウント規約における生体認証の位置づけ
- 関連する背景情報
  - NIST SP 800-63Bにおける生体認証の位置づけ
  - Google Android CDDにおける生体認証に関する要件、生体認証の性能測定のガイダンス、関連APIs
  - 再掲：Androidスマートフォンにおける生体認証と画面ロック解除の関係について
- 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
- 提案1-2：本検討における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ために設定するPIN/パスワード/パターンの利活用について

スマートフォンに搭載されている機能を利活用する考え方

- スマートフォンに搭載されていない機能を新たに実現し、提供していく場合には、実現・提供する主体者が要件を定め、OS提供者・PFチップ提供者・端末メーカーらに協力を仰ぎ、実現する過程で役割分担を定める。その機能を利用するための条件等も定めていくことができる。
- スマートフォンに搭載されている機能については、既に定められた条件等に従って、その機能を利活用していくことが一般的と思われる。

- 本検討において、スマートフォンに搭載されている生体認証機能を利活用するにあたっては、より多くの利用者にとっての利便性の向上に資するためには、致命的な課題がない限り、GP-SEを搭載するスマートフォン（Android OS 9 or 10～）に搭載されている生体認証をそのまま利活用することが期待されていると考える。（新たな要件等を定めることは現実的ではない）
- 民間においては、スマートフォンに搭載されている生体認証機能が広く使われており、大きな問題は報告されておらず、報告された問題についても速やかな対応が行われていることなどから、本検討と実現においても、そうした経験を参考にして、準備を進めることができると思われる。（以降、数ページに渡ってドコモとして経験してきたことをご紹介します）

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：万一の問題発生時に備えた対策

- dアカウント パスワードレス認証における生体認証の導入に際しては、万一の問題発生時に備えて、下記の対策を準備している。
  - お客さまの申告等に応じて、お客さまのdアカウントをロックする機能を兼ね備えている。
  - 市場で発生した問題に応じて、当該機種ないし当該メーカー製機種のdアカウントのFIDO認証を無効化できる機能（生体認証できないようにする機能）を兼ね備えている。
  - いわゆるFIDO認証の仕様におけるアテステーションの考え方を継承し、FIDO2対応の実装ではSafetyNet APIでAndroid端末が正規のデバイスであるかどうかの判断を実施している。

- こと生体認証の導入当初は、お客さまからのお問い合わせに対しての想定応対フローを準備し、万全を期した。
  - dアカウントのためのFIDO認証に起因するものか、スマートフォンに具備された生体認証の装置に起因するかを切り分ける。
    - 生体認証の装置に問題がない場合、その機種のみで発生するものかどうかを切り分ける。
    - 生体認証の装置に関係がありそうだとわかった場合、その原因を見極める。（生体情報の登録の設定、センサーの汚れ、生体情報を登録しなおしてどうか、端末状態・リセットしてどうか、など）

ご参考：dアカウント規約における生体認証の位置づけ

- dアカウント規約では、ID/パスワードと生体認証について、現時点で下記のように定めている。
  - お客さまは、dアカウントのID/パスワードを第三者に知られないように管理し、dアカウントのID/パスワードとそれらを入力したことがある端末の管理と利用について一切の責任を負っていただいている。
  - お客さまの生体情報または画面ロック解除情報を利用した認証に対応する端末において、dアカウントのID/パスワード（やspモードパスワード等）の代わりに予め登録したお客さまの生体情報または画面ロック解除の情報を入力する方式の認証機能を使うことができる。生体認証等サービス等において生体情報または画面ロック解除情報が端末に入力された場合、ドコモは対応するパスワード等が入力されたものとみなすことができる。
  - ドコモは、生体認証機能による予め登録された生体情報と入力された生体情報の照合の確実性等を保証するものではない、としている。万一、生体認証等機能により、第三者の生体情報等が一致すると判定された場合であっても、ドコモは入力された情報を予め登録された情報とみなして認証し、本規約の各条項が適用されるとしている。

上記はdアカウント規約の抜粋またはその要約で、正式には https://id.smt.docomo.ne.jp/src/utility/rules.html をご参照ください。

NIST SP 800-63Bにおける生体認証の位置づけ

- NISTのデジタルアイデンティティガイドラインにおける認証に関する文書SP 800-63Bでは、生体認証について、主に下記のようにガイドされている。（本検討で重要と思われる点をサマリーします）
  - 5章2節 “General Authenticator Requirements” にある10項のうちの5.2.3項 “User of Biometrics” で生体認証の特性とガイダンスが述べられている。
    - 生体認証は、その特徴から、物理的な認証器における多要素の一要素として使用されるべきであること。その特徴とは、生体認証が他の認証手段と比較して決定性によらず蓋然性（確率論的）に基づくこと、生体情報がカメラ付き携帯などでキャプチャされ得るなど秘密と言い切れない特性を持っていることなど。
    - システムとしてPAD（Presentation Attack Detection）を実装すべきであること。攻撃に対して少なくとも90%の耐性を確保し、そのテストはISO/IEC 30107-3に準拠すること。
    - 連続して5回生体認証に失敗した場合（またはPADを実装している場合10回）、次の試行前に30秒（さらにその次は1分、2分のように）待ち時間を設けること、または生体認証の代替手段を提供すること。
  - 10章 “Usability Considerations” にある4節のうちの10.4節 “Biometrics Usability Considerations” に生体認証の使い勝手に関して考慮すべき事項が述べられている。
    - 生体認証の利用についてわかりやすい手順を示すこと、生体認証の1回の失敗後の残る試行可能数や次に生体認証が可能になるまでの待ち時間をわかりやすく示すことが大切であることなど。
    - 生体認証が動作しないときに備えて、多要素認証における一要素としての生体認証の代替手段が提供が求められていることなど。

Google Android CDDにおける生体認証に関する要件

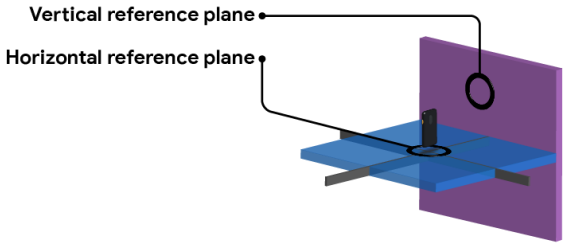
- Android CDDの7章 “Hardware Compatibility” 7.3節 “Sensors” 7.3.10項 “Biometric Sensors” で生体認証装置（センサー）について要件が定められている。ここで、冒頭「端末がセキュアな画面ロック解除（Secure Lock Screen）を実装するのであれば※、生体認証装置を具備することが望ましい [SHOULD]」と位置付けられている。※ 後述の9.11.1項で STRONGLY RECOMMENDED として強く実装が求められている。
  - 生体認証装置は、その性能によってClass 3（強）、Class 2（弱）、Class 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

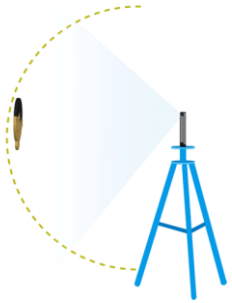
- Android CDDから参照されている生体認証の要件に対する測定・評価に関して公開されている文書で、生体認証の実装に関するセキュリティの評価についてのガイダンスが示されている。
- （GP-SEが搭載されるようになった）Android 9のCDDから導入されたSpoof Acceptance Rate（SAR）について、顔・虹彩認証、指紋認証それぞれについて、測定・評価に先立つ「調整フェーズ」と実際の測定・評価を行う「テストフェーズ」について、具体的なガイダンスが示されている。

【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）

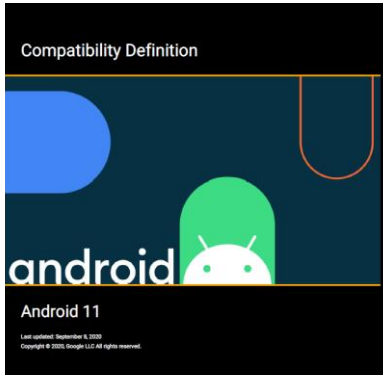
※ 端末メーカーはより詳細に定められた手順に従って測定・評価した結果をGoogleに提出し、CDD準拠の端末として出荷承認を得ている。

再掲・一部加筆・修正

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: Imposer 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。

Android OSにおける生体認証に関するAPIs

- マイナンバーカードの機能のAndroidスマートフォンへの搭載に際し、利用者がGoogle Playからダウンロードして使うJPKIアプリからは、下記のAPIsを活用して実装することになる。

- Androidスマートフォンに具備された生体認証の機能を利活用するために、Android 9から導入されたBiometricPrompt APIを使う。Authenticatorsとして強・Strong/Class 3を使用するため“BIOMETRIC_STRONG” を指定する。（弱・Weak/Class 2の生体認証を使わないようにする）
- Androidスマートフォンが正規の端末であることを確認するためには、SafetyNet APIを利用する。（Android標準のFIDO2実装でも使われている）
- Androidスマートフォンに具備されたセキュアな画面ロック解除を生体認証と組み合わせて使うには、Keyguard APIを利用する。（Android標準のFIDO2実装でもこの画面ロック解除が使われている）

- 状況によりJPKIアプリの動作を変更する一つの方法として、Firebase Remote Configを活用できると考える。（バージョンアップ版のアプリをダウンロードして再インストールしていただかなくても、全ユーザーまたは特定セグメントユーザーに対してアプリ内のデフォルト値を上書きでき、アプリの振る舞いを変更できる）

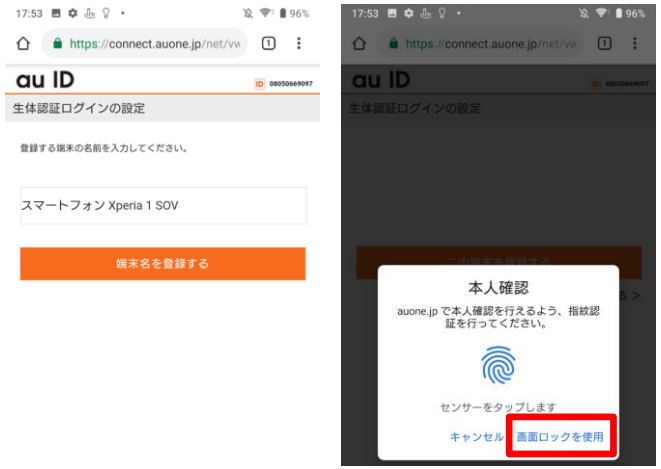
ご参考：各社FIDO2導入における生体認証失敗時の対応

多くの場合、AndroidのFIDO2機能をそのまま活用し、生体認証を一定数失敗したときは画面ロック解除のために設定されたPIN/パスワード/パターンによる対応を可能としている

ヤフー

ドコモ

KDDI



ヤフー、KDDI、ドコモはAndroidのFIDO2 APIを使い、生体認証の替わりに、または生体認証に失敗したときに画面ロック解除のためのPIN/パスワード/パターンを使うことを可能にしている。

LINEアプリも同様である。

LINE Payアプリでは、独自のPINを求めている。（生体認証失敗時に画面ロック解除のためのPIN/パスワード/パターンを使っていない事例）

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）

参考（バックアップ）

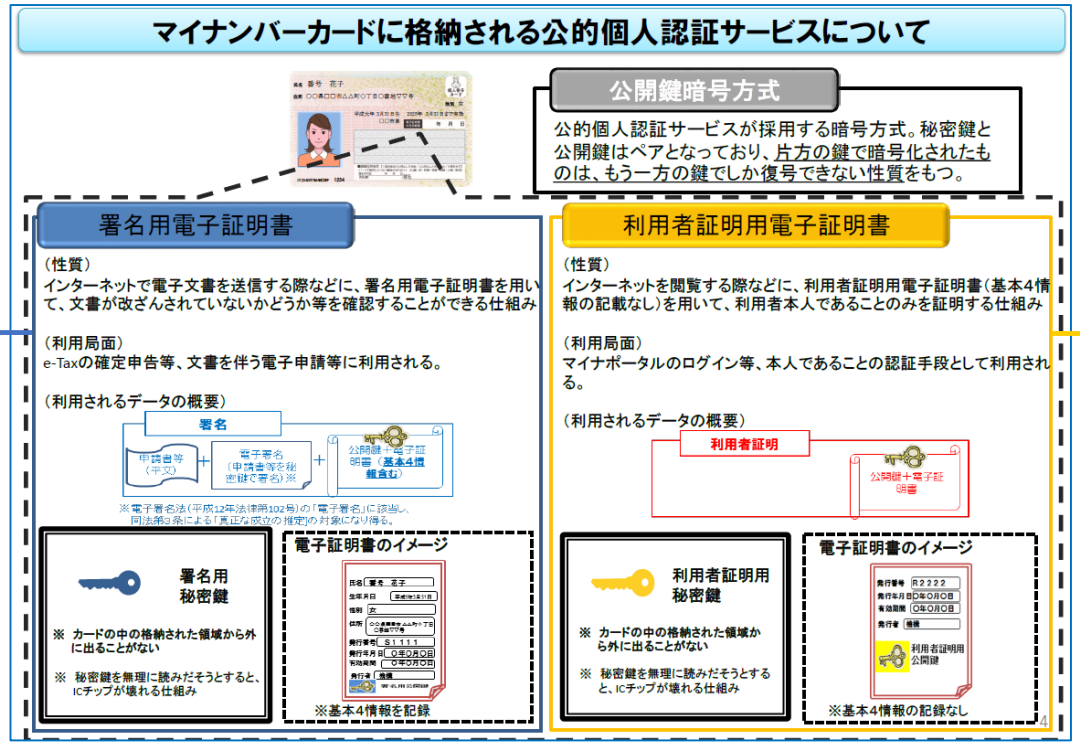
再掲

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

再掲

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。

再掲

～パスワードのいらない世界へ～ の歩み

▼FIDOアライアンスへボードメンバーとして加盟

▼FIDO Deployment at Scale WGを設立

▼FIDO Japan WGを設立・発表

▼執行評議会メンバーとして選出していただく

Phase 1
あんしんをもっと便利に

▲UAF 1.0準拠端末で
FIDO生体認証を導入

▲iOS対応

Phase 2
スマホが暮らしの鍵になる

▲パソコンやSTBから
「スマホ認証」

▲虹彩・指紋
同時認証待受け対応

Phase 3
ID・パスワードのあり方を変える

▲dアカウントパスワードレス認証
（ドコモ回線契約者）（2020年3月24日）

▲ドコモ回線契約者以外へ
パスワードレス認証提供
（2020年11月11日）

▲fido2 対応（画面ロック解除にも対応）
（2020年6月2日）

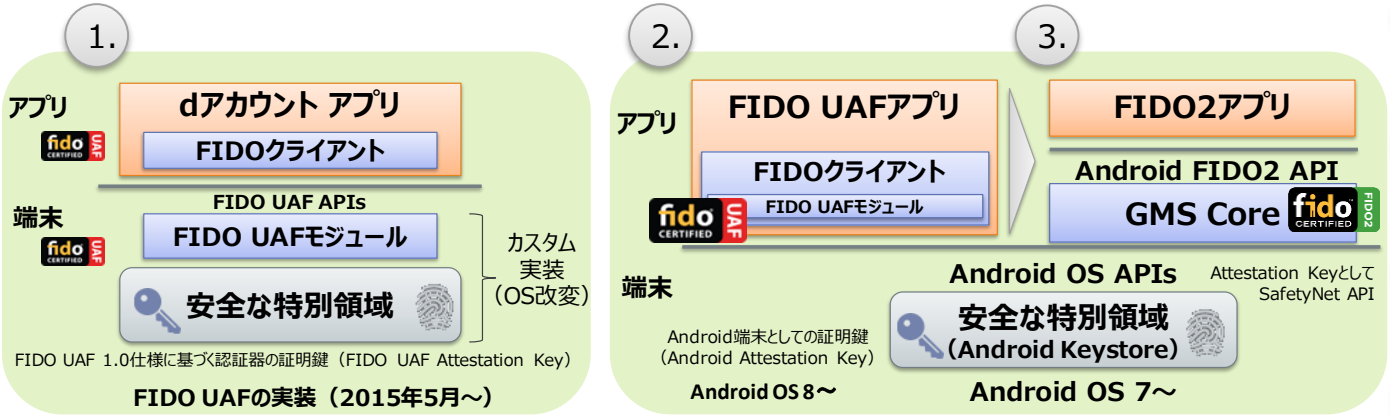
FIDO UAF 1.0 | FIDO UAF 1.1 | FIDO2

FY 2015 2016 2017 2018 2019 2020 2021～

再掲

Android OSセキュリティ実装とFIDO2への移行

dアカウントにおけるUAF 1.1からFIDO2へのシンプルな移行導線



- FIDO UAFの良さを活かしたFIDO認証の商用導入（「あんしんをもっと便利に」）
- 端末メーカーの開発負担を減らし、さらなる普及をめざしたプラットフォーム化の検討
- 先行するOS・PFチップセットのセキュリティ実装を活かしたFIDO UAF 1.1としての普及促進
- 並行して進めたWebAuthn/FIDO2の積極的な導入推進
- パスワードレス化によるセキュリティ強化と出荷済UAF端末のFIDO2移行サポート
- さらに広いカバレッジを確保する大きな進捗（1社のみ、1社としての活動ではない）

1. 生体認証導入当初は端末メーカーと共同開発でFIDO認証の実装して提供
2. Android OS生体認証・セキュリティ対応と歩調を合わせて、FIDOアプリ対応
3. 1つのゴールとして、Android OSのFIDO認定（FIDO2）でより幅広い対応

※ いずれも当初から生体情報と秘密鍵は安全な特別領域（TEE/SE）に格納

標準化活動に貢献しつつビジネス展開して実証、また標準化活動にフィードバックする循環の一事例