資料7

fido ALLIANCE | simpler stronger authentication

第2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

スマートフォンへの生体認証の搭載・FIDO認証の適用を通じて得られた知見を基にしたご提案

2020年12月4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

本資料の内容

- FIDOアライアンスとFIDO認証のご紹介
  - FIDOアライアンスとFIDO認証の概要
  - 国内外におけるFIDO認証の導入事例と期待感

- ご提案の骨子
  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
  2. マイナンバーカードの機能のクラウド利用、レベルに応じた認証、民間IDとの紐づけ等における**FIDO認証**の利活用について
  3. マイナンバーカードによる公的個人認証サービス等の利用シーンにおける**FIDO認証**の利活用の可能性について

FIDOアライアンスとFIDO認証のご紹介

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**

The **F**ast **ID**entity **O**nline 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

simpler stronger authentication

グローバルでの業界としての取り組みとボードメンバー

+ スポンサーメンバー

+ アソシエイトメンバー

+ 政府系機関メンバー

+ リエゾンメンバー

政府系機関メンバー

Australian Government
Digital Transformation Office

Cabinet Office

CAICT
中国信息通信研究院
China Academy of Information and Communications Technology

ETDA
www.etda.or.th

Federal Office
for Information Security

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

TTA 한국정보통신기술협회
Telecommunications Technology Association

国内から参加しているFIDOアライアンスメンバー企業

ボードメンバー

スポンサーメンバー

アソシエイトメンバー

株式会社アクセル　Capy株式会社　株式会社イードクトル　エクスジェン・ネットワークス株式会社　株式会社アイピーキューブ　日本情報システム株式会社
オープンソース・ソリューション・テクノロジ株式会社　パスロジ株式会社　株式会社Quado　株式会社セシオス　ウィンマジック・ジャパン株式会社　xID株式会社

FIDO Japan WG 参加メンバー

AuthenTrend　株式会社アクセル　Capy株式会社　株式会社イードクトル　エクスジェン・ネットワークス株式会社　株式会社アイピーキューブ　日本情報システム株式会社
オープンソース・ソリューション・テクノロジ株式会社　パスロジ株式会社　株式会社Quado　株式会社セシオス　Singular Key, Inc.　ウィンマジック・ジャパン株式会社　xID株式会社

FIDO認証モデル

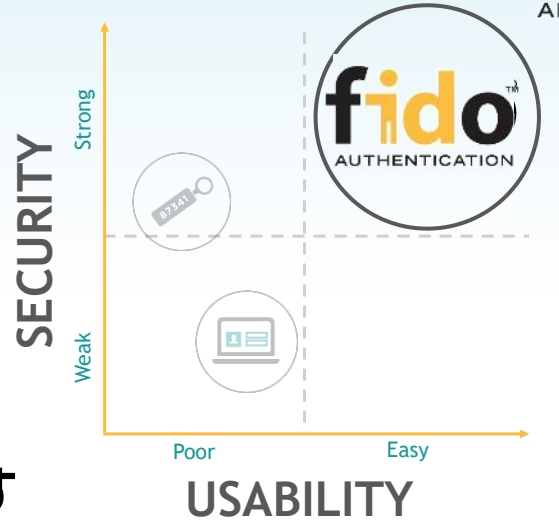
公開鍵暗号方式を活用した
オンライン認証

THE NEW MODEL
Fast IDentity Online

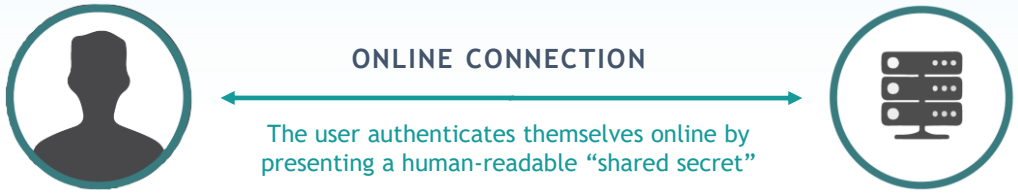
open standards for
simpler, stronger authentication
using public key cryptography

THE FIDO PARADIGM

セキュリティと
使い勝手の両立をめざす



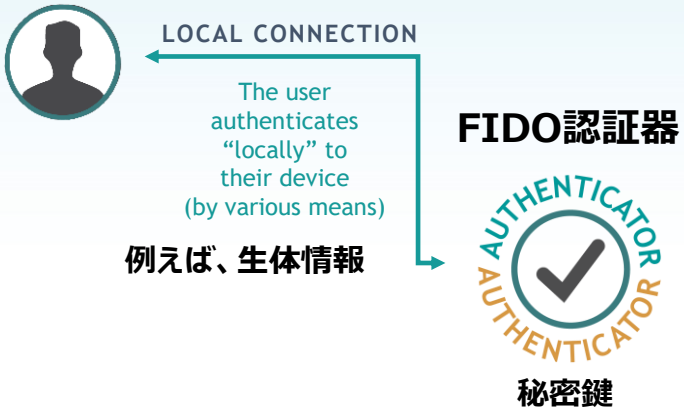
HOW OLD AUTHENTICATION WORKS



ID・パスワード（“Shared Secret”）

「共有の秘密」は不正アクセスの原因

HOW FIDO AUTHENTICATION WORKS



例えば、生体情報

FIDO認証器

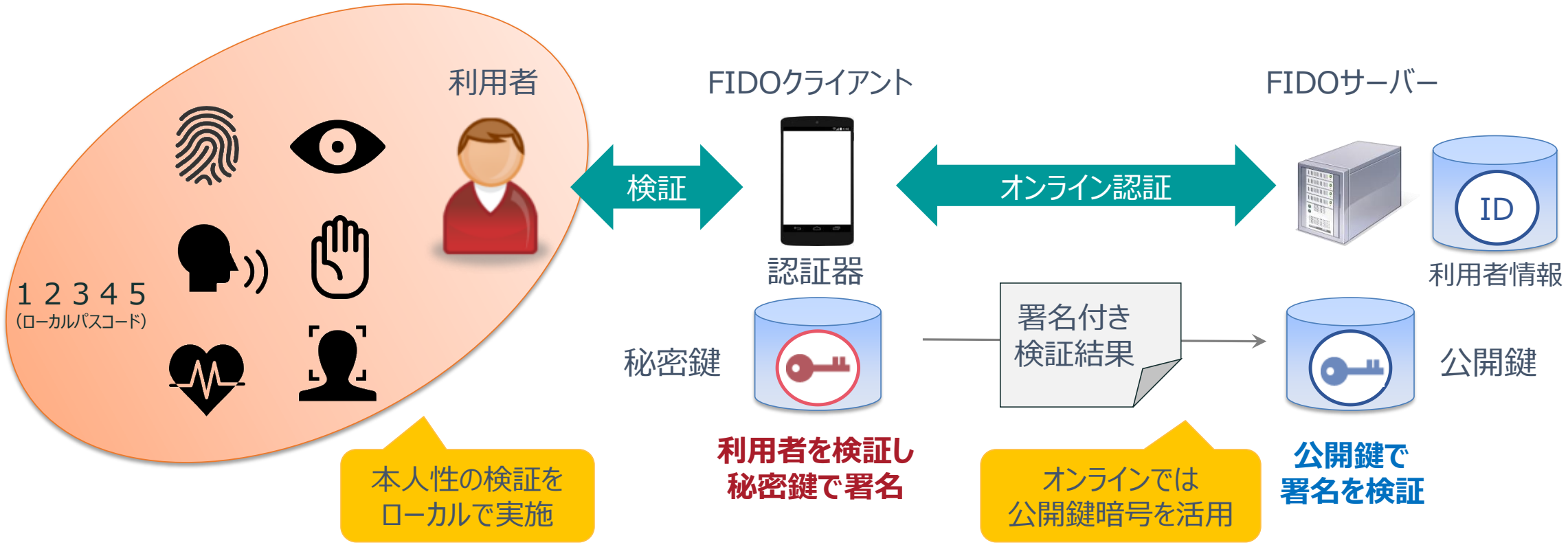
秘密鍵

公開鍵

FIDO認証器に
秘密鍵を格納
公開鍵で署名検証

FIDO認証モデルでは
「秘密」が共有されず、安心

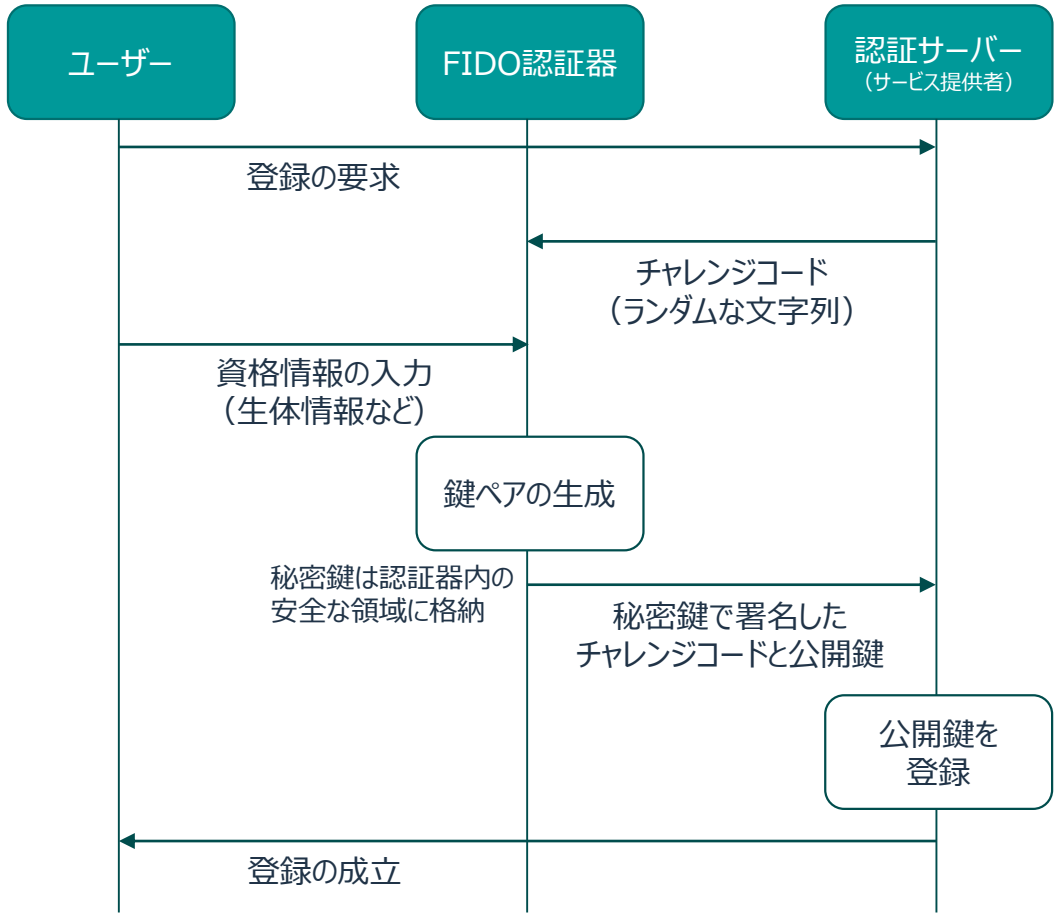
FIDO認証モデル（端末とサーバーで秘密を共有しない）



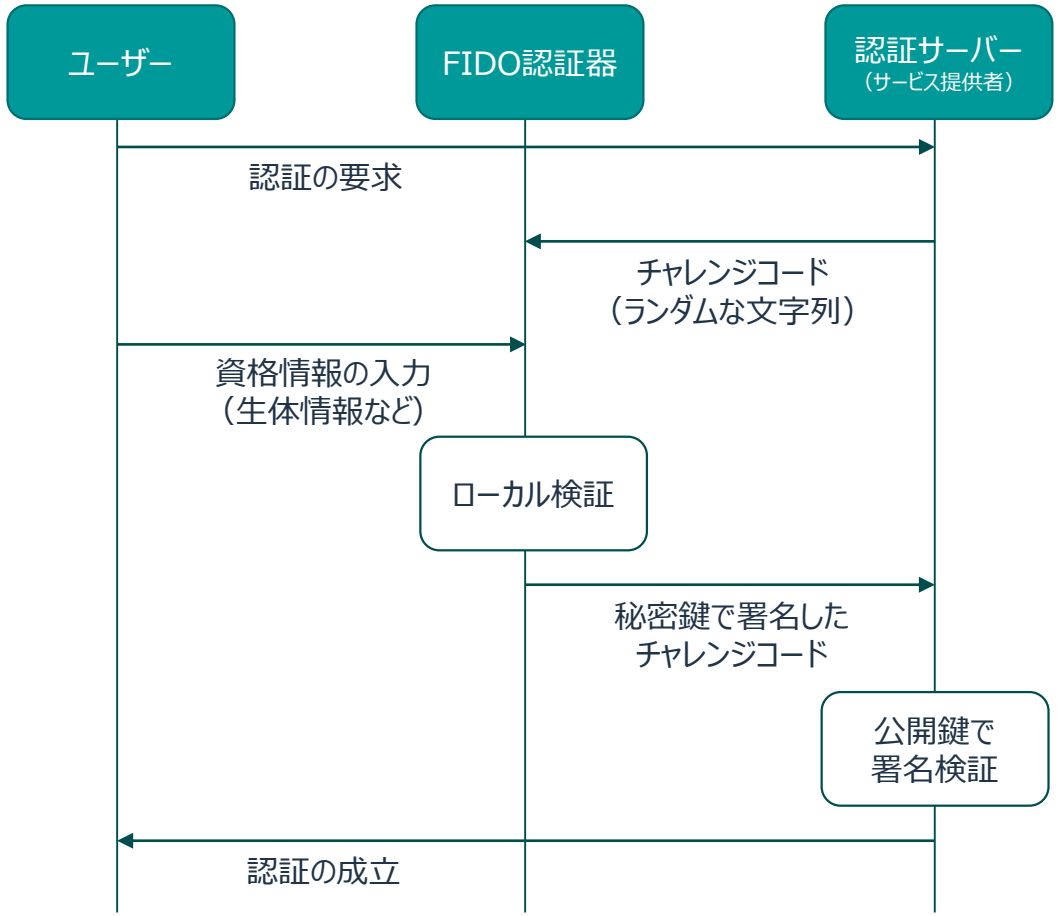
利用者が「認証器」（Authenticator）に適切な秘密鍵を保有することを検証することによって認証を実現しており、認証器の簡単な操作だけで（動的な）多要素認証

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 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

iOSおよびMacOSにおいてFIDO認証をサポート

Andrew Shikiar, Executive Director & CMO, FIDO Alliance

AppleはWWDCで、iOSとMacOS 14に搭載されるSafariの今後のリリースで、ユーザーがWebログインにTouch IDとFace IDを利用できるようになると詳細な発表を行いました。これは、パスワードを超えて、FIDO標準に基づく暗号学的に安全な認証に移行しようとする業界の取り組みにおいて、大きな一歩を踏み出したことを示しています。

この機能は、FIDO2標準のWebAuthn（以下：Web認証）APIに基づいており、生体認証を使ってiPhoneやiPadの画面ロックを解除するのと同様の簡単な操作でWebサイトにログインできるようになります。Appleの純正Webブラウザに組み込まれているということは、すべての最新のデバイスプラットフォームがFIDOをサポートしていることを意味しており、FIDO認証を他の重要なインターネットプロトコルと同様にどこででも利用可能なものにするという私たちの目標を後押ししています。

そのために、私たちは最近、ブラウザやプラットフォーム全体でのFIDOサポートの最新の進捗状況を示す情報を提供しました。この画像（下の画像）は、Web認証に関する情報が記載されたFIDOアライアンスのWebページで閲覧可能です。

AppleがFIDOのサポートを強化して以来、過去12ヶ月ほどの間に、この図が（Appleのオペレーティングシステムが追加され）より広く、よりグリーンの部分が多くなっているのを見るのは、とても素晴らしいことでした。今日のブラウザの85%以上がFIDO認証をサポートしており、多くのサービスプロバイダーが世界中の顧客にFIDOを導入しようと積極的に取り組んでいます。

FIDOアライアンスは、たった一つのミッションに基づいて設立されました。それは、シンプルで堅牢なユーザー認証のためのオープンスタンダードを作成し、その採用を促進することで、パスワードへの依存をなくすことです。今日、私たちは、FIDOエコシステムが過去数年間取り組んできたこの大胆な目標の達成に近づいています。ありがとう、Apple!

- AppleはWWDCで、iOSとMacOS 14に搭載されるSafariの今後のリリースで、ユーザーがWebログインにTouch IDとFace IDを利用できるようになると詳細な発表を行いました。（左記ブログは日本語で2020年7月1日に発信）

  FIDO2標準のWebAuthn（Web認証）APIに基づいており、生体認証を使ってiPhoneやiPadの画面ロックを解除するのと同様の簡単な操作でWebサイトにログインできるようになります。

Safari 14 Beta Release Notes より

Authentication and Passwords New Features – Added a Web Authentication platform authenticator using Face ID or Touch ID, depending on which capability is present.

https://developer.apple.com/documentation/safari-release-notes/safari-14-release-notes#Authentication-and-Passwords

WebAuthn fido2

FIDO2 / WebAuthn（Web認証）のプラットフォーム認証器として
Android、Windowsに加えて、iOS・MacOSも正式に対応

国内におけるFIDO認証の導入状況

fido ALLIANCE

NTT docomo
YAHOO! JAPAN
LINE
isr International Systems Research Co.
KDDI
SoftBank
DDS DIGITAL DEVELOPMENT SYSTEMS
yubico
OneSpan
softgiken
Quado
nok nok
Capy Security for All
egis Technology
FEITIAN WE BUILD SECURITY
FUJITSU
MUFG MUFG Bank
JP BANK ゆうちょ銀行
住信SBIネット銀行
Lenovo
NEC
Aflac
NRI SECURE
NTT Communications Transform. Transcend.
NTT DATA

※ 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を提供済、またはそれらを導入済の主な企業

グローバルにおけるFIDO認証の導入事例と期待感

海外では特に韓国・台湾で実際の利用が進んでいる他、“Authenticate 2020”（FIDOアライアンスが主催する「認証」に関するオンラインセミナー。11月9日～20日開催）や “FIDOセミナー in Japan”（12月1日～4日）でも数々の事例が報告されている。FIDO認証への期待感があり、政府系機関・民間での利用が進んでいる。

- 韓国 – 2016年からKISA（Korea Internet Security Agency）が定めるK-FIDO（韓国の国民IDをFIDO UAFと組み合わせた認証仕様）が使われている。2018年からFIDOベースで電子署名が可能となり、最近はコロナ禍にあって、法令の改正があり、モバイルベースの身分証等にシフトしていくであろうとの報告あり。

- 台湾 – 2019年からPKIベースのMOICAと呼ばれる台湾市民IDにTAIWAN FidOとして、FIDO認証に対応。従前はMOICAのスマートカードをPCに接続したICカードリーダーに挿入して使う方式であったが（2003年～）、セキュリティと使い勝手のバランスを考慮して、スマートフォンでFIDO認証を使う方式が新たに提供されたとのこと。

- 米国 – コロナ禍によって連邦政府がリモートワークに関するガイダンスを発出、従来から使用されてきたPIV（Personal Identity Verification）やCAC（Common Access Card）という認証方式に加えて、FIDOが代替認証として採用され始めている。他の多くの認証方式と異なりFIDO認証はフィッシング耐性があると認識され、また、SP800-63-3の改訂に先立って、最近のセキュリティキーがAAL2/3として認められてきている。

- 欧州 – eIDAS、PSD2（Payment Service Directive 2）等に対してFIDO認証を適用する機運があり、チェコではeIDASの認証に適合するかたちでFIDOの導入が試行されているとのこと。

NIST SP800-63-3とFIDO認証の関係

- NIST SP800-63-3が改訂のさなかにあり、FIDO認証の位置づけについても議論がある。
- NIST SP800-63-3BにおけるAAL（Authenticator Assurance Level）の定義で、その最高ランクに位置付けられるAAL3は、連邦政府の調達に関する基準であるため、パスワード認証の脆弱性への対処レベルのみならず、装置の実装レベルなどについても規定がある。（例：FIPS 140等）
- NISTへは、FIDOアライアンスとしてコメントを申し入れており、多くのAAL2相当の認証器と異なり、フィッシング耐性に有効である方式であるということについてご理解いただいている認識。ただし、改訂で最終的にどのように扱われるかは未定。
- なお、FIDOアライアンスにおいても、秘密鍵などをセキュリティ実装上どのように守るかについてのレベル定義と認定プログラムを提供している。（レベル1～3+）　認証器として単機能のセキュリティキーについては、装置の実装レベルを全体として認定取得できる状況になりつつある。

～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）

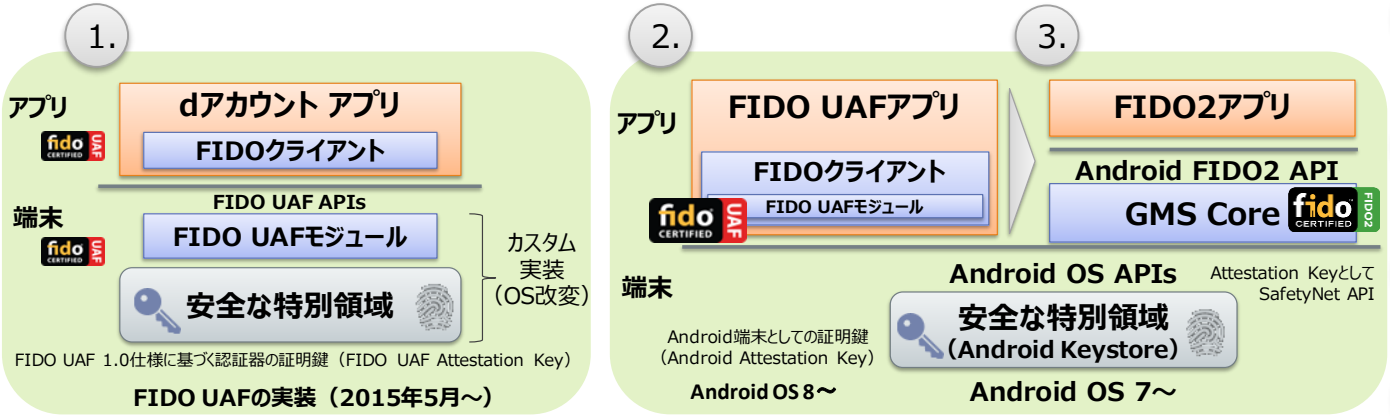
▲fido2 対応（画面ロック解除にも対応）
（2020年6月2日）

FIDO UAF 1.0 | FIDO UAF 1.1 | FIDO2

FY 2015 2016 2017 2018 2019 2020 2021～

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

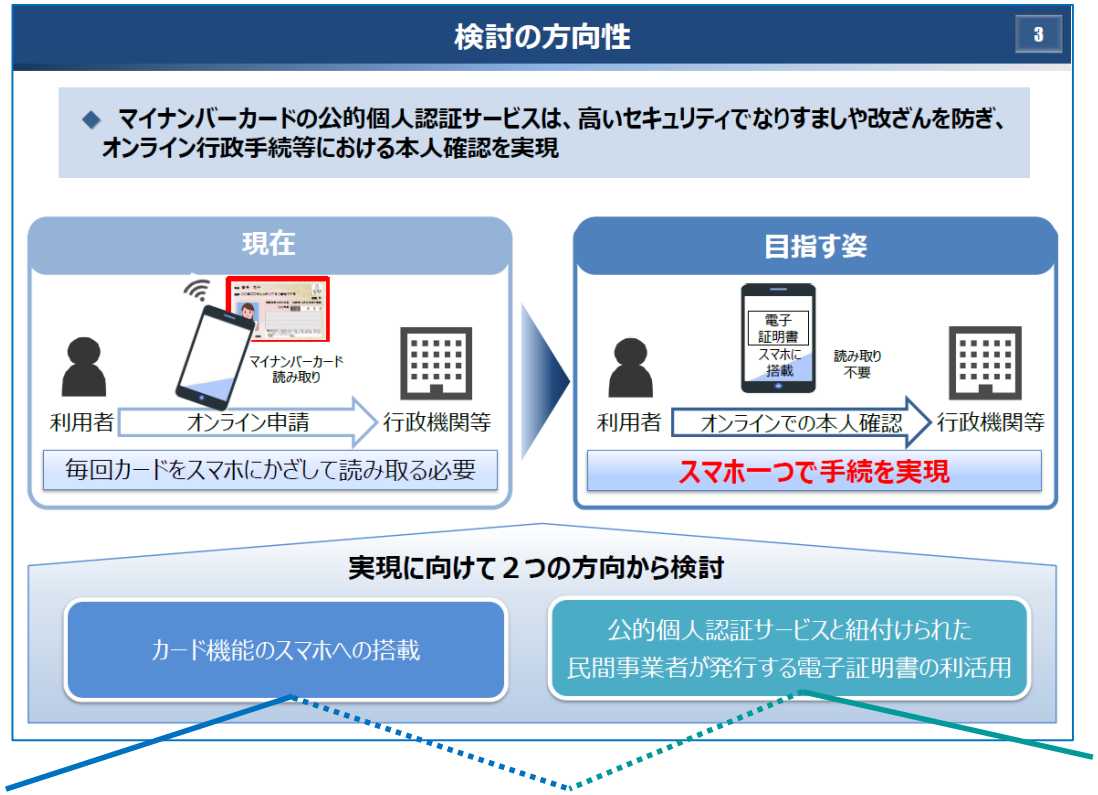
ご提案の骨子

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
2. マイナンバーカードの機能のクラウド利用、民間IDとの紐づけ等における**FIDO認証**の利活用について
3. マイナンバーカードによる公的個人認証サービス等の利用シーンにおける**FIDO認証**の利活用の可能性について





ご提案の骨子（イメージ）



1. カード機能のスマホへの搭載

3. 公的個人認証サービス等での利用シーン

2. 公的個人認証サービスと紐づけられた民間事業者が発行する電子証明書の利活用

ご提案の骨子（1/2）

- マイナンバーカードのセキュリティレベルを維持しつつ利便性の抜本的向上に資するため、生体認証とFIDO認証をそれぞれ下記のように利活用するというご提案についてご議論いただけると幸いです。

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

- マイナンバーカードのエコシステム自体がFIDO認証のしくみと似ているため、マイナンバーカードの機能をFeliCa-SEを利用してスマートフォンに搭載する際、積極的にFIDO認証を統合する必然性は少ない。しかし、生体認証を組み合わせて、利便性を向上させることについては検討の価値があると考える。
- FIDO認証は生体認証と親和性が良く、スマートフォンにおけるオンライン認証で生体認証を使うアプローチとしてFIDO認証が普及しつつある。FIDO認証の実用化を通じてスマートフォンで生体認証をどのように扱ってきたかを振り返ることで、本検討における生体認証の利活用について、そのアプローチが見えてくるものと考える。

2. マイナンバーカードの機能の民間IDとの紐づけ等における**FIDO認証**の利活用

- パスワードが漏洩・類推・奪取されることでの不正アクセスは社会的な問題となっており、FIDO認証は有力な解決手段である。一方、その設定・再設定時に必要な身元確認の手段はまだ限定的と思われる。このため、マイナンバーカードを活用した民間ID等と紐づけには期待が大きく、検討の価値があると考える。

ご提案の骨子（2/2）

3. マイナンバーカードによる公的個人認証サービス等の利用シーンにおける**FIDO認証**の利活用の可能性

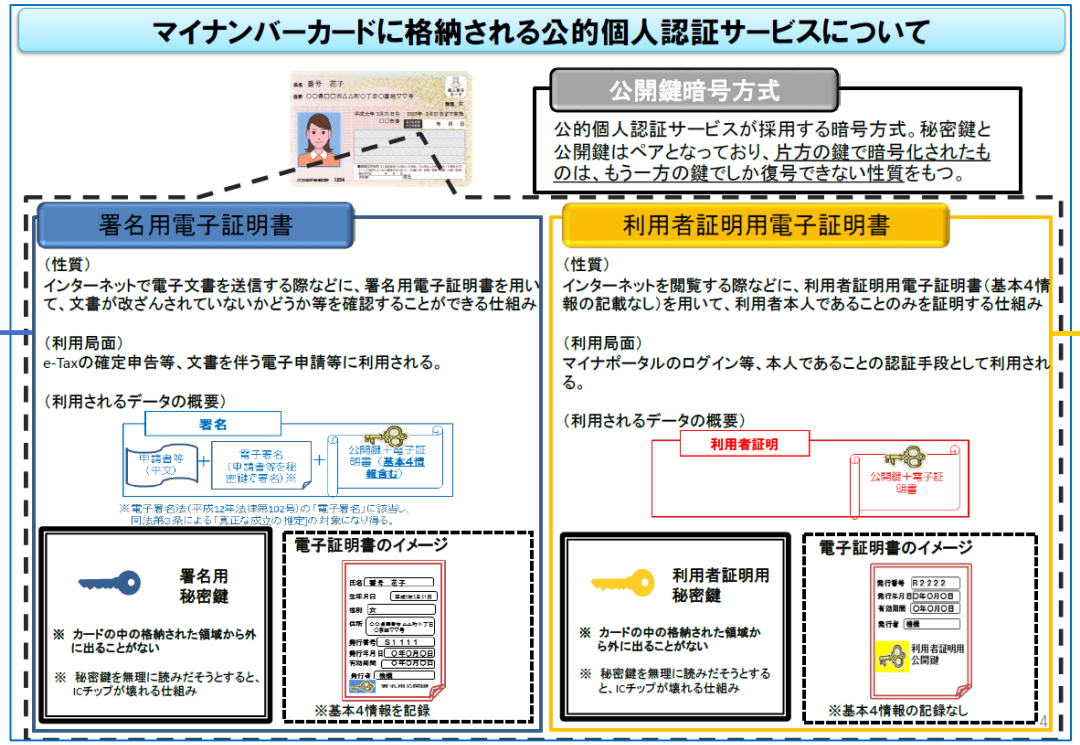
- FeliCa-SEを搭載していないスマートフォンでも公的個人認証サービス等をスマートフォンで安心・便利に利用する方法として、既存のマイナンバーカードに格納された証明書を読み取ることなどができるスマートフォンであれば、FIDO認証と組み合わせることで利便性を向上させることができる可能性について、検討の価値があると考える。
- また、公的個人認証サービスに限らず、マイナンバーカードと組み合わせて提供されるサービスなどにおいて、パスワードに替えて（2段階認証などでもパスワード・OTPを奪取されることがなく、フィッシング耐性のある）FIDO認証を導入することで、利用者が安心して認証サービスをご利用いただけるようになるものと考える。

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、FeliCa-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

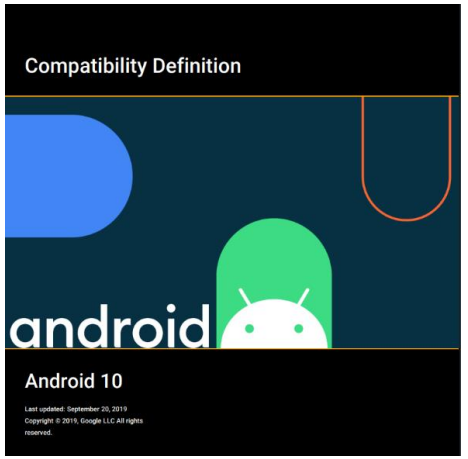
スマートフォンに搭載されている生体認証装置の利用について

- 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。

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/パターン/パスコード） • 最もセキュア
セカンダリ認証 生体認証（強）	• **生体認証**（SAR: 7%以下、FAR: 0.002%以下） • 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・便利）	• 生体認証（SAR: 7%以上で「弱」、20%以上で「便利」） • 2時間以上利用しない場合、および24時間ごとに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



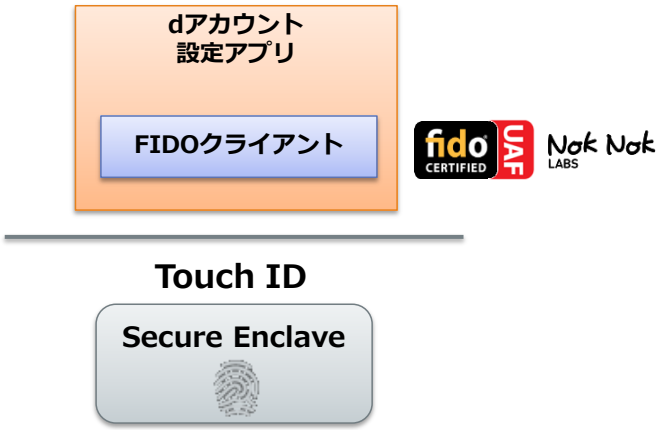
https://source.android.com/compatibility/10/android-10-cdd

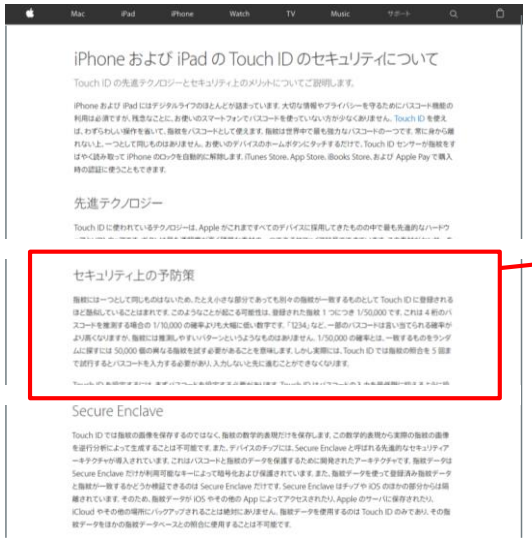
SAR: Spoof Accept Rate – スプーフィング攻撃への耐性。録音した音声での攻撃など
FAR: False Accept Rate – 他人受入率。ランダムな他人の生体情報を誤って認識してしまう率
（最近では、FARに代えて、IAR: Imposer Accept Rate – なりすまし攻撃の指標も導入されつつある）

ご参考：スマートフォン搭載生体認証装置のFAR（他人受入率）

iOS 9端末におけるFIDO UAFの実装

- iOS 9端末用「dアカウント設定」アプリを開発。Nok Nok Labs社FIDO Certified™ SDKでFIDO UAFプロトコルを実装し、さらにTouch IDのセキュリティを活用
  - 「iPhoneおよびiPadのTouch IDのセキュリティについて」により、Touch IDではSecure Enclaveによって指紋データ（数学的表現）をiOS端末内に保持し、また端末の外に出ることがないなど、FIDOプライバシーポリシーと同等と判断
  - iOS 9からの新仕様なども活用し、dアカウント認証に必要な要件を達成





- ドコモが2015年春夏モデル向けにメーカー様に要望した生体認証装置の性能はFAR 1/50,000 (0.002%) 以下でした。
- アップル社による2016年2月当時のTouchIDのセキュリティに関する説明文によれば、FARは1/50,000と言えます。

指紋には一つとして同じものはないため、たとえ小さな部分であっても別々の指紋が一致するものとしてTouchIDに登録されるほど酷似していることはまれです。このようなことが起こる可能性は、登録された指紋1つにつき1/50,000です。これは4桁のパスコードを憶測する場合の1/10,000の確率よりも大変低い数字です。「1234」など、一部のパスコードは言い当てられる確率がより高くなりますが、指紋には推測しやすいパターンというものはありません。1/50,000の確率とは、一致するものをランダムに探すには50,000個の異なる指紋を試す必要があることを意味します。しかし実際には、TouchIDでは指紋の照合を5個まで試行するとパスコードを入力する必要があり、入力しないと先に進むことができなくなります。

2016年2月当時のアップル社による開発者向けサイトの説明文より

2. 民間IDとの紐づけ等におけるFIDO認証の利活用について

- 「検討の背景」として、カード機能（公的個人認証サービス）の抜本的改善（スマートフォンへの搭載、クラウド利用、レベルに応じた認証、民間IDとの紐づけ等）があり、マイナンバーカードの機能のスマホ搭載に加えて、マイナンバーカードのより多くのシーンでの利活用に期待があるとのことであり、社会的に問題になっているパスワード課題の解決のため、民間IDの利用などにおいても、マイナンバーカードの機能を活かした本人性の確認レベル向上に適用できるようになることに期待しています。

  - FIDO認証は、認証のしくみとしては、実績も出て来て、フィッシング耐性があることが認知されてきた。
  - 普及の課題として、FIDO認証を設定（登録）するときの本人性の確認レベルの確保と、再設定時の手段提供などが議論されている。（アカウントリカバリーの問題）
  - 携帯通信事業者は、その手段を提供しやすい環境にある。利用者が安心してオンライン認証できる環境を整えるために、マイナンバーカードの民間IDとの紐づけ等への利用促進にも期待している。

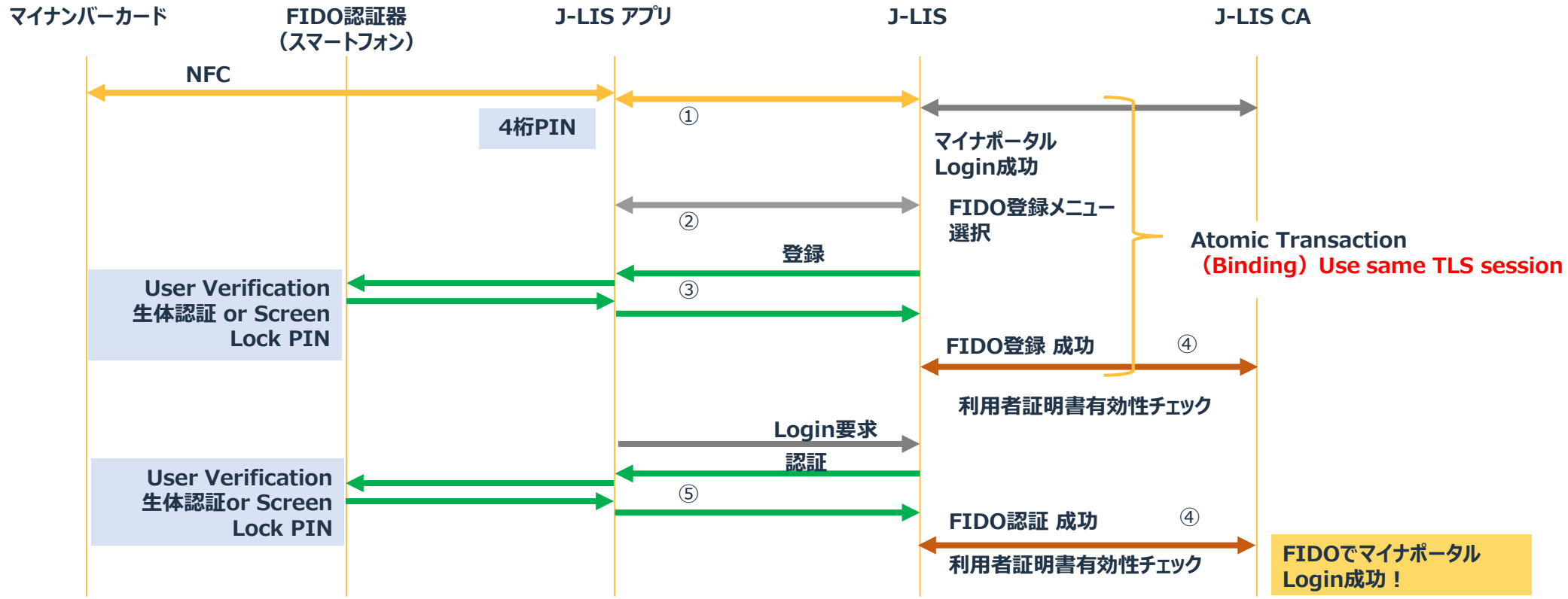
2-1. より具体的に検討すべき点（案）

- 民間サービスにおいては、不正アクセスを防止するための手段として、IDにSMS受信可能な携帯電話番号を紐づけて、利用者を一意に特定する手法が使われています。この方法は、加入者の解約後、一定期間経過したとき、再び電話番号が再利用されたときに発生する問題が知られています。既に提供されているマイナンバー制度対応本人確認サービスよりも軽量で、利用者を一意に特定できるサービスが実現されると、不正アクセスを防止するための手段として有効と考えます。このとき、サービス提供者が利用者を一意に特定する値はNIST SP800-63-3で表現されているpseudonymous identity（仮名性を確保したID）として利用できることを期待します。
- また、既に提供可能な本人確認サービスについても、サービス提供者・サービス利用者にとって、さらに利便性を向上していける可能性があると推察します。（要継続確認・検討）

3. マイナンバーカードによる公的個人認証サービス等の利用シーンにおけるFIDO認証の利活用

- FeliCa-SEを搭載していないスマートフォンでも公的個人認証サービスをスマートフォンであんしん便利に利用する方法として、既存のマイナンバーカードに格納された証明書を読み取ることなどができるスマートフォンも対象として、FIDO認証と組み合わせて利便性を向上できる可能性があります。

【FIDO認証を利活用する事例～既存のマイナンバーカードに対応したNFCスマートフォンで動作する方式（案）】



公的個人認証サービス等の利用シーンにおけるFIDO認証の利活用（補１）

- 既存のマイナンバーカードを使って利用者認証した結果に依拠する形で、FIDO認証を設定（登録）することで、フィッシング耐性のあるシンプルで堅牢な認証でマイナポータルにログインする体験等を提供可能と考えらます。

（シーケンス～FIDOアライアンス内での議論より）

1. J-LISアプリからマイナンバーカードを使ってマイナポータルにログインする。利用者認証を使用する。利用者は4桁の暗証番号を入れる。
2. ログインした状態で利用者が（例えば）「FIDO登録」メニューを選択する。
3. FIDO認証に必要なRegistration（登録）。これでFIDO Credential（鍵ペア。認証資格情報）が登録される。同時にJ-LISサーバー内でこのFIDO Credentialと利用者のアカウントが紐付けられる。すなわち、マイナンバーの証明書とFIDO Credentialがバインドされる。
4. サーバーにてマイナンバーカードの証明書の有効性の検証をする。
5. マイナンバーカードをスマートフォンにかざして暗証番号を入力する代わりに、FIDO認証を使って、利用者の操作として（カードをかざさずに）生体認証や暗証番号を入力することで、よりシンプルにマイナポータルにログインできる。

公的個人認証サービス等の利用シーンにおけるFIDO認証の利活用（補２）

- 先の提案は、マイナンバーカードの機能をスマートフォンに搭載するわけではないので、場合よってはその利便性が限定的になる可能性もあります。病院やコンビニエンスストアなどに設置されている端末での利用は、例えばQRコードを表示してオンライン認証に置換して対応できそうです。

（アイデア～FIDOアライアンス内での議論より）

  - 現在、コンビニエンスストアなどに設置されている端末で住民票や戸籍などを取得する利用シーンでは、端末にカードをかざしてNFC認証する必要がある。
  - QRコードを利用して、オンライン認証に置換することで、対応できる可能性が十分にある。
    - スマートフォンにQRコードを表示して、それを端末に読み込んで、FIDO認証する方式
    - コンビニエンスストアなどに設置されている端末にQRコード表示して、それを読み込んで、FIDO認証する方式

QRコード方式に対しては、よく知られた攻撃としてMITM（Man-In-The-Middle）があるが、コンビニの特定端末に紐ついたQRコードであり、Proximity(*) であるので、悪用される心配はないと思われる。
(*) 利用者と端末の近傍を担保することで、リモートからの不正アクセスを防ぐ

QRコード表示して、コンビニ窓口で支払いをするなどの方式は一般的なので、利用者から見ても使いやすいと思われる。

fido ALLIANCE | simpler stronger authentication

ご確認いただきありがとうございます！

2020年12月4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