資料5

fido ALLIANCE | simpler stronger authentication

第5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

マイナンバーカードの機能を利活用した民間IDの認証におけるセキュリティと使い勝手の高いレベルでの両立に向けて

2021年3月3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

w/ FIDO Japan WG アカウントリカバリータスクフォース

はじめに

- マイナンバーカードの機能（公的個人認証サービス）のスマートフォンへの搭載等に関する検討が進み、利用者証明用認証においては、スマホならではの使いやすいUXの実現に向けて、生体認証の利活用についても方向性が確認された。（第4回　検討会）　これにより、耐タンパ性のあるICチップに安全に格納する電子証明書の所持と、その利用者のみがもつ知識情報または利用者であることを表す生体情報を組み合わせた多要素認証で、高いレベルのセキュリティを便利にご利用いただけるようになる。
- 一方、民間では多くの場合において、業種を問わずサービス提供者が提供するIDとパスワード等による認証が広く使われている。（電子証明書等の所持を伴う認証ではない）　最近では、二段階認証や追加認証と呼ばれる手段も広く使われるようになったが、不正アクセスの報告や報道が後を絶たない。
- このような状況下、国内からドコモ、LINE、ヤフーがボードメンバーとして参画しているFIDOアライアンスが推進するFIDO認証に注目していただいている。FIDO認証は、マイナンバーカードの機能のスマホへの搭載のように、一度設定していただければ、認証資格情報の所持と、知識情報または生体情報とを組み合わせた多要素認証で、フィッシング耐性のあるセキュリティを便利にご利用いただける。つまり、不正アクセスの対策に有効である。
- この設定や、端末を紛失したときなどの再設定（復旧）に際して、マイナンバーカードの機能を有効に利活用できる。（民間IDと紐づけ）

第2回検討会でのご提案資料より再掲・加筆

ご提案の骨子

- 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。

本日のご提案

第2回検討会でのご提案資料より再掲

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）
  - 携帯電話事業者は、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。

民間IDにおける認証をとりまく課題～パスワードと二段階認証

- IDとパスワードが流出していると言われる。通信元の特定を困難にする技術などを使って、悪意のある第三者は、匿名性を確保しながらIDとパスワードなどの個人情報をやりとりしていると言われる。そして、それらを使ったいわゆる**リスト型攻撃**により、効率よく不正アクセスが可能になったと言われている。この要因として、多くの利用者が異なるサービスに対して同じIDとパスワードを流用していることなども原因とされている。
- 最近では、**フィッシング型攻撃**による不正アクセスも急増している。悪意のある第三者が本物そっくりの偽サイトを立ち上げてアクセスさせたり、本物そっくりの偽ブラウザアプリをインストールさせたりする。そして、第三者は、利用者がだまされて入力したIDとパスワードやワンタイムパスコードを奪取し、不正アクセスするというものである。これによって、二段階認証も突破されていることが明らかになっている。

  - 二段階認証とは、多要素を二段階で認証することを意味することがあるが、単一要素を二段階で認証することを意味することもある。従来から使われて来た二段階認証は、パスワードに加えて予め紐付けられたデバイスやアプリに表示されるワンタイムパスコード（認証コード）を利用者が入力することで、二段階認証を構成することが多かった。しかし、デバイスに表示された認証コードは、ユーザーの知識として入力されるので、パスワードと認証コードという同じ知識要素を2個使った認証になっている。そのため、フィッシング型攻撃に対して脆弱である。（多要素認証、二要素認証と区別した方が良い）
  - これらの攻撃に対しては、パスワードを複雑にしたり文字数を増やすなどの対策は、効果がない。

ご参考：二段階認証は突破される

- 二段階認証を突破する方法は2019年10月に図解でわかりやすく示されるに至り、2020年2月に新聞紙上でも記事として報道された。

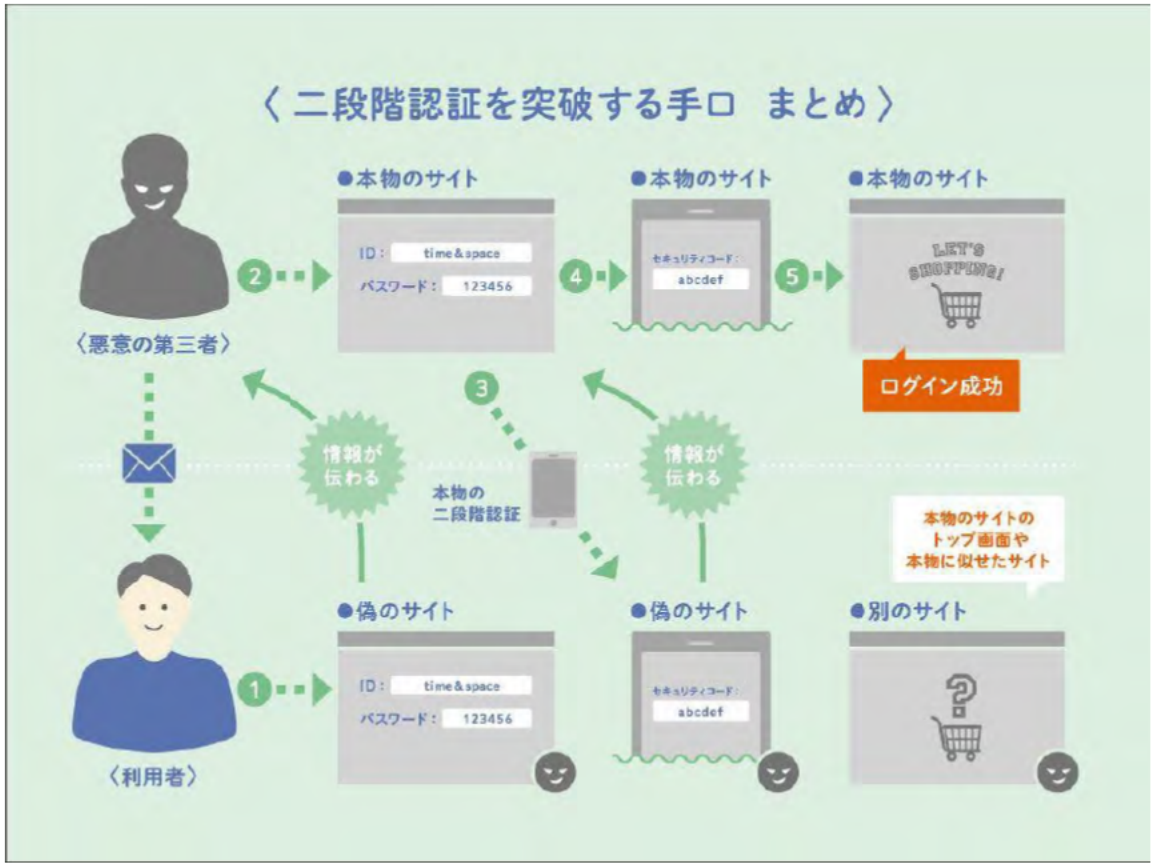
① 利用者が偽サイトにアクセスする。悪意のある第三者に情報が伝わる

② 悪意ある第三者が本物のサイトにIDとパスワードを入力する

③ 本物のサイトへ正しいIDとパスワードが入力されたので、本物の二段階認証が機能する。利用者は、受信したワンタイムパスワードを（この時点ではまだ偽サイトと気が付かずに）入力する。この情報も悪意のある第三者に伝わる

④ 悪意のある第三者は、そのワンタイムパスワードを本物のサイトに入力する

⑤ そして、悪意ある第三者がログイン・決済等に成功する。（利用者は、この時点で何かおかしいと気が付くこともあるだろうし、気が付かないこともあるかもしれない）



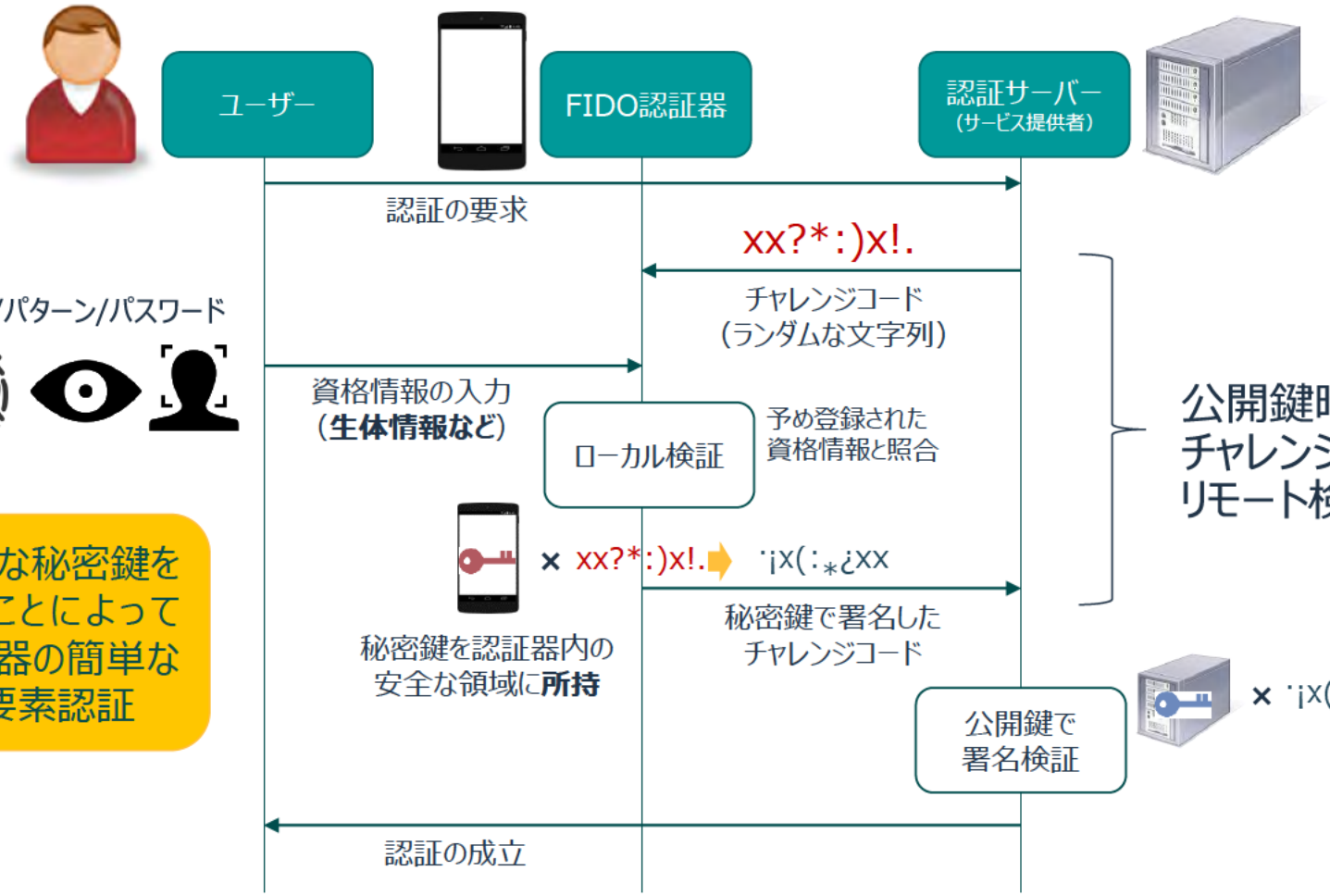
https://time-space.kddi.com/it-technology/20191021/2761

GoogleによるFIDO Japanセミナーでの報告（2020年12月1～4日）

https://youtu.be/BKqTt0HF6-U

FIDO認証の流れ（認証～「秘密」がインターネットを通過しない）

認証時



利用者が「認証器」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（設定（登録））

設定（登録）時

登録するユーザーの
本人確認
または、その本人と
保証できる手段

この手段として、マイナンバーカードの機能（公的個人認証サービス）を利用可能。

マイナンバーカードの機能がスマホに搭載されれば、さらに便利に利用可能！

マイナンバーカードを持ち歩かなくても、スマホだけでFIDO認証の設定、再設定ができる！

ユーザー

FIDO認証器

認証サーバー
（サービス提供者）

身元確認の保証が重要
（レベルよりも一意性）

PIN/パターン/パスワード

登録の要求

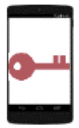
xx?*:)x!.

チャレンジコード
（ランダムな文字列）

資格情報の入力
（生体情報など）

鍵ペアの生成

秘密鍵は認証器内の
安全な領域に格納



× xx?*:)x!. ➡ ¨¡x(:⁎¿xx

秘密鍵で署名した
チャレンジコードと公開鍵

公開鍵を
登録

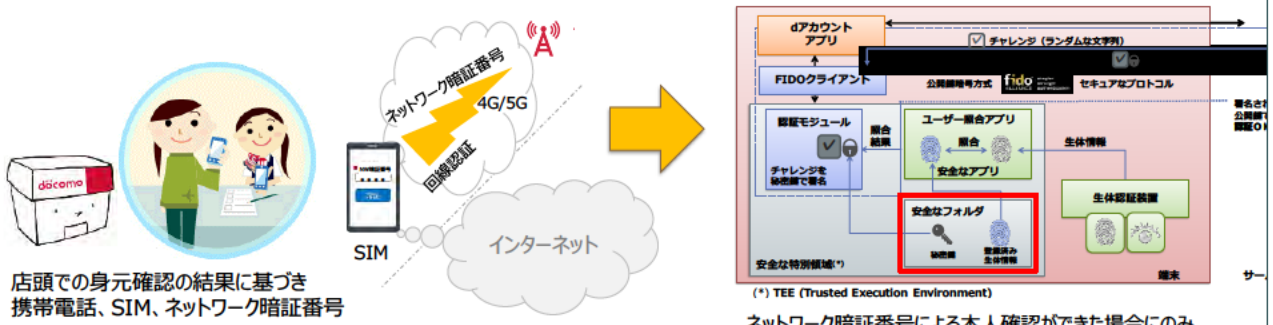
× ¨¡x(:⁎¿xx ➡ xx?*:)x!.

登録の成立

FIDO登録時の身元保証手段#1: 携帯電話事業者の例

端末紛失時などの再設定（アカウントリカバリー）
～ネットワーク暗証番号による本人確認で解決～

- ドコモの回線をお持ちのお客さまにご利用いただくことができるネットワーク暗証番号は、複製困難な契約中のSIMの所持とそのお客さまだけがご存じの知識（ドコモ回線を通過する4桁の暗証番号）を組み合わせた本人確認手段 – FIDO認証の設定・再設定に有効



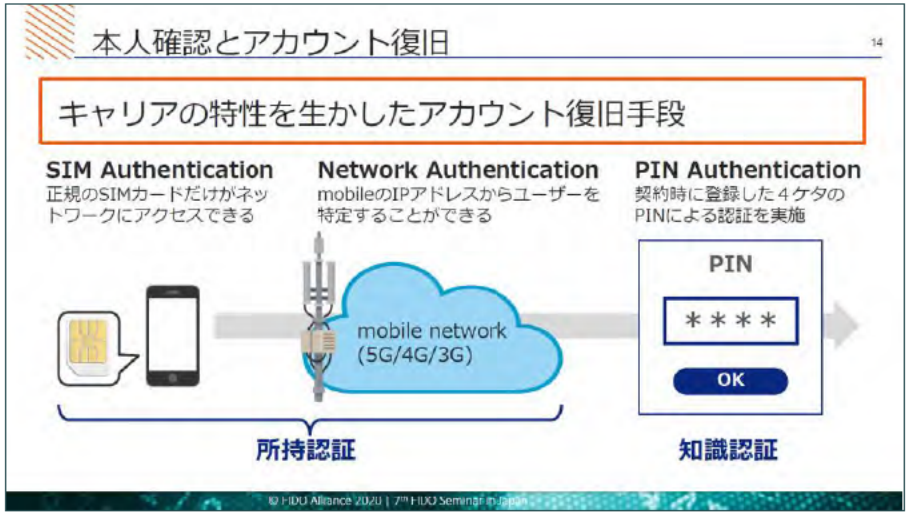
ネットワーク暗証番号による本人確認は、ドコモの回線をお持ちのお客さまのSIMによる回線認証と、そのお客さまだけがご存じの暗証番号を組み合わせた多要素認証

ネットワーク暗証番号による本人確認ができた場合にのみ、FIDO認証に必要な認証資格情報（鍵ペア）を生成し、秘密鍵をそのまま端末の安全な特別領域に格納する。

docomo Open House 2021 © 2020 NTT DOCOMO, INC. All Rights Reserved. 35

ネットワーク暗証番号による本人確認とアカウントリカバリー @ docomo Open House 2021（2021.2.4-7）

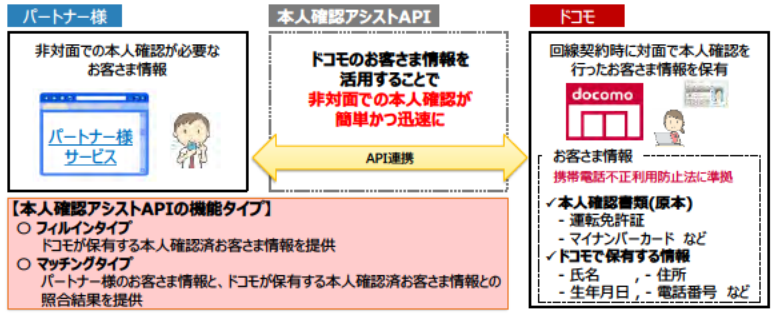
- 携帯電話事業者では、携帯電話不正利用防止法に基づく本人確認を実施しており、回線認証（強力な所持認証）と知識認証の組み合わせによる多要素認証で再設定（復旧）可能
- この基盤を利用して、ビジネスパートナーに本人確認をアシスト・支援するAPIを提供する携帯電話事業者もある。



KDDIによるFIDO2導入とアカウント復旧 @ FIDO Japanセミナー（2021.12.1）

本人確認アシストAPI

- 携帯電話を利用されるお客さまの情報を活用し、お客さまから個別同意をいただいた上で、パートナー様における本人確認を支援する有償サービス（2017年6月提供開始）



LINE x Intertrust Security Summit 2019 © 2019 NTT DOCOMO, INC. All Rights Reserved. 9

ドコモによる本人確認アシストAPIのご紹介 @ LINE x Intertrustセキュリティサミット（2019.5.29）

FIDO登録時の身元保証手段#2: eKYC、SMS認証

- **eKYC**: スマホのカメラ等を用い、オンライン越しに公的身分証明書の顔写真との一致を確認するなどして、対面の本人確認に代えて、オンラインで法令等が求める本人確認が可能になるソリューションがある。現在、eKYCがFIDO登録時の身元確認の保証手段として広く使われているとはまだ言えないが、今後の有効な手段の一つとして、2019年6月に作業部会（IDWG: Identity Verification and Binding WG）を設置して検討を続けている。
- **SMS認証**: IDにSMSを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ある。IDとSMSを受信できる電話番号を1:1に紐づけることで、いわゆる本人確認に必要な属性情報を確認できないが、利用者の一意性を一定のレベルで担保できる※。電話番号は、解約後に一定の期間を経て再利用されるため、新たな利用者が登録するときに、既にその電話番号が紐づけられたIDが他に存在すると衝突する問題が知られ、その他にも理由があって、決定的な方法になっていない。

  ※携帯電話のSIMは、携帯電話不正利用防止法に基づく本人確認をした結果として利用されているが、本人確認なしに入手できるデータ通信用のSIMでSMSを受信できるなど例もあるため、SIMの利用者はすべて本人確認済とは言えない。

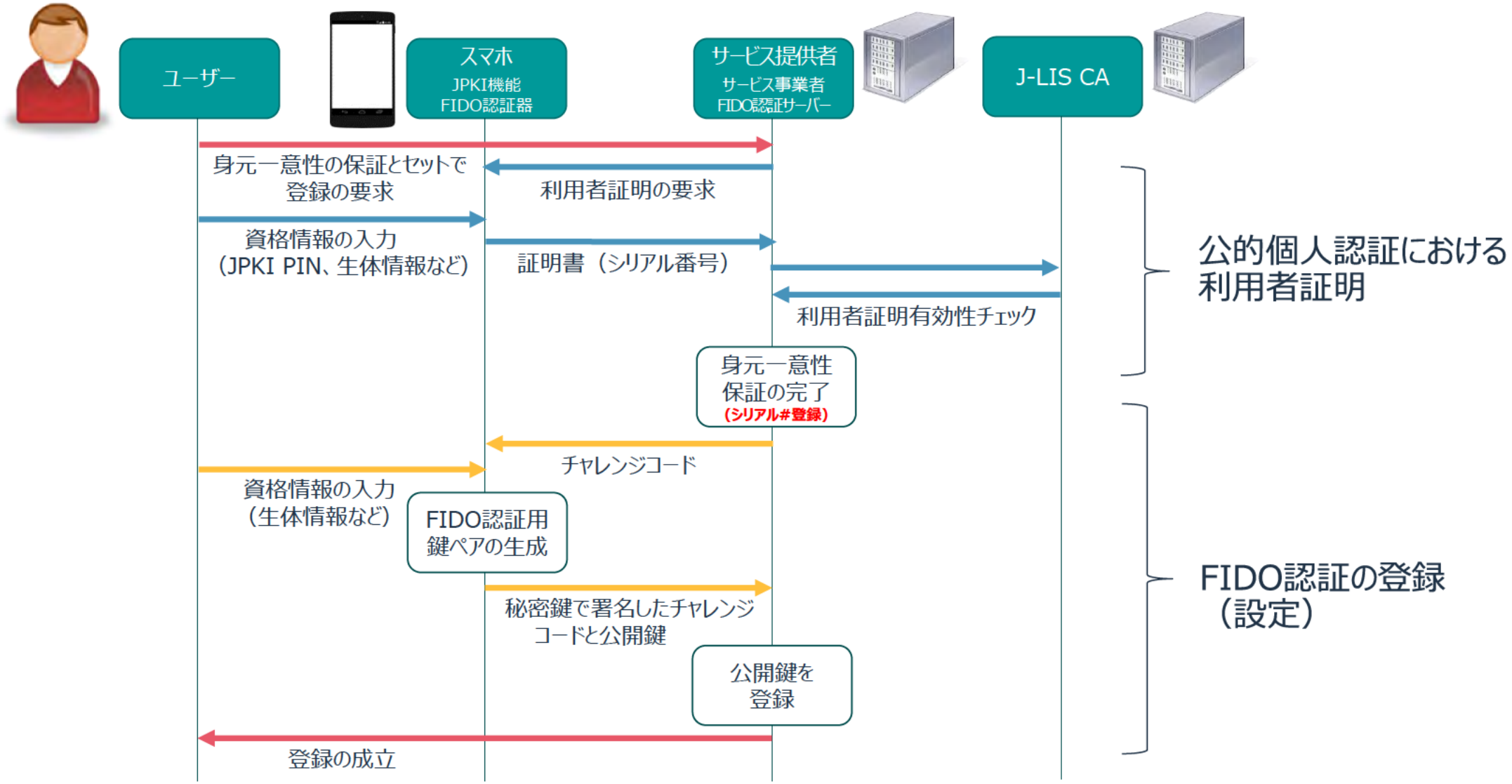
  - 身元確認の保証（レベルより一意性）が重要な点として、NIST SP 800-63-3 FAQ Q-1/A-1に触れられていることがある。Q-1: Why were identity proofing, authentication, and federation separated into distinct categories? A-1: （略） This flexibility also asks agencies to think innovatively about their system's privacy requirements. This includes pseudonymous interactions even when strong, multi-factor authenticators are used. In a nutshell, the new version gives agencies the flexibility to deploy strong authentication while avoiding unnecessary proofing of users' identities that would require collecting (and then protecting) sensitive information. This was not possible in previous versions of the document, where proofing and authentication requirements were bound together in a single assurance level. すなわち、サービス提供者が本人確認に必要な属性情報を集めなくても、堅牢な多要素認証を提供することで、利用者のプライバシーをより容易に保護できる可能性が言及されている。この点は、民間IDと認証をとりまく課題を解決していく際に重要な観点の一つと考えられる。（多要素認証の堅牢性を活かすのに、本人確認性または利用者の一意性を確保することが重要）

FIDO登録時の身元保証手段#3: 公的個人認証（JPKI）

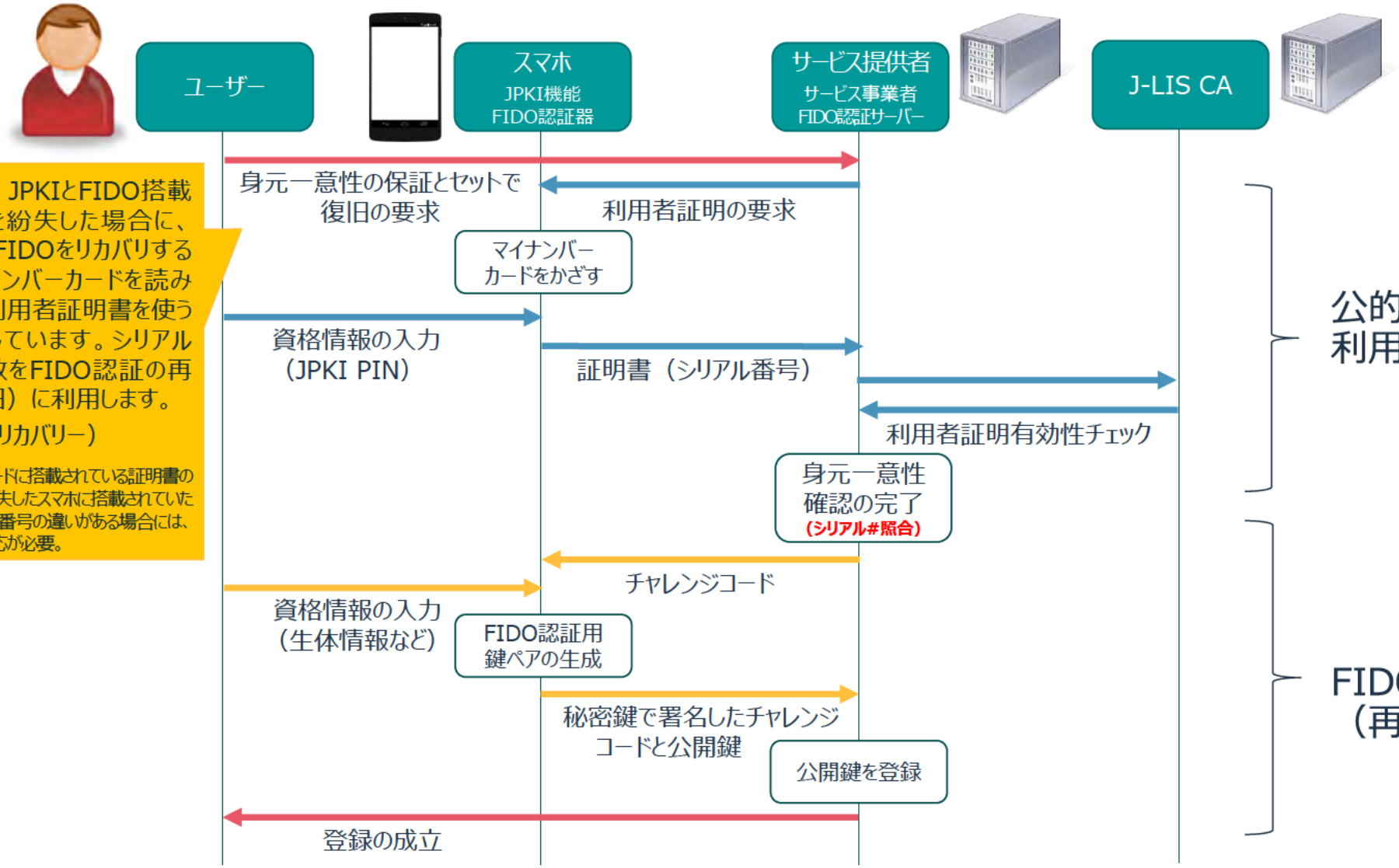
- **署名用証明書の利用**：基本4情報による本人確認が可能。数字とアルファベット混在で半角文字6文字から16文字までの署名用パスワードが必要。4情報が変更になると証明書の再発行が必要。より厳格な本人確認。1回あたりの費用はやや高価。
- **利用者証明用証明書の利用**：数字4桁の利用者証明用パスワード（暗証番号）が必要。4情報が変更になっても証明書は有効だが、5年に一度更新が必要。利用者証明の結果として、証明書との一意性を表現する符号としてシリアル番号を利用できる。1回あたりの費用はやや安価。スマホでは生体認証も使えるようになる。

  - シリアル番号は少なくとも一世代前にさかのぼることができるとのことであり、利用者証明ができるようになっている限り、一定期間はサービス提供者にとってもFIDO認証の適切な復旧を提供可能になる。
  - スマホを紛失してしまったときなどは、マイナンバーカードの機能（公的個人認証）のスマホへの搭載（設定）も再度行う必要があるため、この場合は先にマイナンバーカードの機能をスマホに搭載した上で、生体認証などを使ってFIDO認証も復旧するか、マイナンバーカードをスマホにかざして利用者証明用パスワード（暗証番号）を入力してFIDO認証を復旧することになる。
  - サービス提供者がシリアル番号を利用することになるが、ここにはいわゆるlinkabilityが存在する。すなわち、万一にもIDと紐づいたシリアル番号が漏洩してしまった場合の他サービス提供者へ波及リスクがある。そのため、NIST SP 800-63-3が触れているpairwise pseudonymous identity（サービス提供者毎に限定できる仮名性を確保したID）をシリアル番号に代えて利用できれば、サービス提供者にとってはより一層利活用しやすいアカウントリカバリーの基盤になる。

例1: 公的個人認証（JPKI）を利用したFIDO設定（登録）



例2: 公的個人認証（JPKI）を利用したFIDO再設定（復旧）



この例では、JPKIとFIDO搭載したスマホを紛失した場合に、新スマホでFIDOをリカバリするため、マイナンバーカードを読み取ってその利用者証明書を使う方式を示しています。シリアル番号の一致をFIDO認証の再設定（復旧）に利用します。
（アカウントリカバリー）

※マイナンバーカードに搭載されている証明書のシリアル番号と紛失したスマホに搭載されていた証明書のシリアル番号の違いがある場合には、さらなる検討と対応が必要。

公的個人認証における
利用者証明

FIDO認証の復旧のための登録
（再設定）

FIDO認証の最新動向

LINE fido2

LINE desktop app supporting Passwordless on iPad and Windows PC

November, 2020

YAHOO! JAPAN fido2 WebAuthn

Additionally Safari support on iOS devices

December, 2020

NTT docomo fido2

Disabling d ACCOUNT password also for non-subscribers both iOS and Android

January, 2021

YAHOO! JAPAN

ヤフー、Yahoo! JAPANアプリなどのアプリやスマートフォンブラウザーで指紋・顔認証を利用したログインに対応

コンシューマ向け商用サービスとしてiOS「Safari」でFIDO2に対応した認証方法の導入は世界初。パスワードを使わない認証方法を推進し、利便性と安全性の向上を目指す

2021年2月8日 発表（ヤフー）

- 本検討会の発足以降も、ボードメンバー企業による取り組みを中心に、FIDO認証の導入が進んでいる。
  - ドコモが1月27日にパスワードレス認証（パスワード無効化設定）のキャリアフリーユーザー対応を完了（提供開始）
  - ヤフーが2月8日に、iOS「Safari」対応に加えてアプリでもFIDO2認証の導入し、アプリおよびスマートフォンブラウザーへの生体認証の導入完了を発表
- さらに多くの民間企業が提供するID・アカウントへの認証シーンで、フィッシング型攻撃に耐性のあるFIDO認証がより活用され、その設定・再設定に必要な身元確認や一意性確保手段としてマイナンバーカードの機能に期待。

fido ALLIANCE | simpler stronger authentication

ご確認いただきありがとうございます！

2021年3月3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

w/ FIDO Japan WG アカウントリカバリータスクフォース

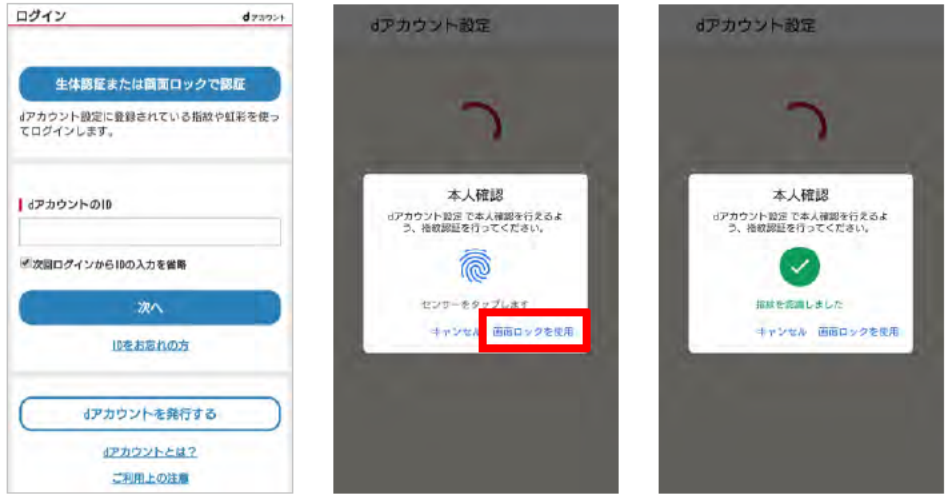
再掲

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）

再掲

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。