さまざまなユースケースへの FIDO の対応に向けて

（国際版の日本語訳）

2022 年 3 月

エグゼクティブサマリー

FIDO（ファイド）標準は、WebAuthn（以下、Web 認証）仕様とともに重要な新展開を迎えています。このたびの FIDO アライアンスと W3C Web 認証コミュニティによる技術標準への革新的な変更提案は、FIDO 認証のユーザビリティと導入のしやすさをさらに著しく向上させることを目的としています。その結果、安全な FIDO 認証技術はインターネット上における主要な認証方式として、いよいよパスワードにとって代わることができるようになるのです。

本稿ではまずはじめに、FIDO および Web 認証の標準仕様により、これまでも非常に高い認証保証レベルを低コストで実現することができていたことについて説明します。これは従来のスマートカード認証に代わる魅力的な手段であり、コンシューマー領域における高い認証保証レベルへの扉を開くものでしたが、世界レベルの大規模な FIDO 認証の導入はまだ達成できていません。そこで、現在 FIDO アライアンスが取り組んでいる「マルチデバイス対応」FIDO 認証資格情報（マルチデバイス FIDO クレデンシャル）の導入について説明します。これにより、ユーザーがいつでもどこでも、たとえデバイスを機種変更したとしても FIDO 認証資格情報をいつでも利用できるようになるため、多くのコンシューマー領域におけるユースケースで FIDO 認証がパスワードにとって代わり得ることになるのです。

オンライン認証の歴史

認証は、コミュニケーション、ソーシャルネットワーク、金融取引、その他のビジネスなどデジタルネットワークで発生するあらゆることにおいて必要不可欠なものです。私たちにとって、そしてこれまでのインターネットの歴史において、認証とはユーザー名とパスワードを入力することを意味していました。つまり、この歴史の中でほとんどの人がセキュリティとユーザビリティの両面からパスワードが持つ欠点と共存しなければならなかったのです。しかし、すべての人が常にパスワードに頼ってきたわけではありません。20 年も前から政府の特定の部門で働いていた人は、おそらく Personal Identity Verification（PIV：米国連邦政府の職員及び請負業者のための個人識別情報の検証）やその他のスマートカード認証に使っていたはずです。スマートカードはパスワードよりもはるかに安全ですが、スマートカード本体だけでなく、専用の読み取り装置を必要とし、ブラウザなどの Web プラットフォームに統合されることはなかったため、その利用範囲は限定されたままでした。

その後、周期的に変化するコードをユーザーに表示するハードウェア・トークンが登場し、ユーザーが二段階認証のために所持するようになりました。専用の読み取り装置は不要になり、Web でもうまく機能するようになったものの、物理的なトークン自体は依然として必要で、コンシューマー向けの用途で広く採用されるためには乗り越えられないハードルでした。このようなトークンは、タイムベースワンタイムパスワード（TOTP：Time-based One-

time Password）のような標準規格を使用しているか独自方式を採用しているかにかかわらず、ある程度広範囲に利用されていましたが、ほとんどの場合においては多くのユーザーが依然として認証時にパスワードを入力する必要がありました。

スマートフォンの普及に伴い、専用のハードウェアトークンの必要性は薄れました。その代わりに、スマートフォンは TOTP コードを表示したり、SMS で送信されたワンタイムパスワードを表示したり、よりシンプルにスマートフォンに確認メッセージをプッシュ送信するなどして二段階認証を提供することが可能になりました。オンラインバンキングなどのコンシューマー向けユースケースに対して、より安全な認証メカニズムが提供されるようになったのです。しかし、そこには注目すべきトレードオフがあります。TOTP トークンやスマートフォンを使った二段階認証は、単一のパスワードよりは安全ですが、スマートカードと異なり、フィッシング攻撃などを受ける可能性があるのです。

NIST（米国立標準技術研究所、National Institute of Standards and Technology）はこの状況をデジタル・アイデンティティ・ガイドライン、NIST Special Publication 800-63B に反映しています。このガイドラインでは、3 種類のセキュリティレベル（「AAL」、「認証器の保証レベル」）について概説しています。AAL1（最低レベル）はパスワード、AAL2 は（フィッシング耐性を必要としない）多要素認証、AAL3 はハードウェアベースのフィッシング耐性のある認証メカニズムにおよそ対応しています。これらのセキュリティ・レベルに照らし合わせると、大多数のコンシューマーはオンライン認証の際に AAL1 を使用しています。多くのエンドユーザーは、例えばオンラインバンキングの利用時などに AAL2 を求められるようになってきていますが、AAL3 が求められることはほとんどありません。

FIDO：トップダウンのアプローチ

2010 年頃の状況：ハードウェアに紐付いてフィッシング耐性がある認証メカニズム（AAL3）は、高度なセキュリティが求められる政府機関や企業でのニッチなユースケースに限られてました。このような環境では、認証装置（スマートカード）に加えて専用の読み取り装置が必要となり、また、Web プラットフォームとの統合が必要な場合は、その都度開発する必要がありました。その対極に位置するセキュリティ方式がパスワード認証です。圧倒的に多くの（コンシューマー）ユースケースで使用され、Web 上で機能していますが、セキュリティのレベルは低くなります（AAL1）。この中間に二段階認証が位置づけられましたが、これもフィッシング攻撃などを受けやすいものです。

FIDO アライアンスはフィッシング耐性のある認証メカニズムの仕様一式を 2014 年 12 月までに公開しました。のちに、それに対応する W3C Web 認証仕様が公開されました。そして、2010 年代の終わりまでにほとんどの主要なブラウザが Web 認証仕様を実装しました。これにより、世界で初めて、特別な読み取り装置やドライバのインストールなどを必要としない、標準化された Web 統合型のフィッシング耐性のある認証メカニズムをサービス事業者とそのユーザーが広く利用できるようになったのです。さらに、ハードウェアに実装することで、FIDO ベースの認証は AAL3 レベルのスマートカードと同等のセキュリティレベルを達成することもできます。これには、2 つの重要な効果があります。

1. ハードウェアベースの認証器やフィッシング耐性のある認証メカニズムを必要とするセキュリティ強度の高いユースケースを、既製のオペレーティングシステム、スマートフォン、Web ブラウザなどの標準的な Web プラットフォームで実現でき、その導入コストを劇的に削減することができるようになったのです。このような高セキュリティのユースケースでは、しばしば、認証器は暗号鍵[1]を抜き取られないようにすることが要求されます。FIDO は、これらの厳しいハードウェアベースのセキュリティ要件を満たす FIDO セキュリティキーをお客様が選択できるよう、認定プログラムを提供しています。

2. これまでフィッシングのリスクがある二段階認証で対応せざるを得なかったユースケースでも、より堅牢なセキュリティを検討できるようになりました。例えば、Google はフィッシング耐性のある FIDO 認証を中心に Advanced Protection Program（アドバンスド・プロテクション・プログラム）を構築し、標的型攻撃のリスクを抱えるユーザーに、Google の通常の二段階認証製品を超えるセキュリティレベルを提供することができました。このユースケース（フィッシング攻撃が主な懸念事項）にとって、ハードウェアベースの FIDO セキュリティキーが魅力的なのは、暗号鍵の抜き取りに耐性があるということもさることながら、フィッシング耐性のある認証資格情報をユーザーが持ち歩く（あるいは安全な場所に保管する）のに便利なデバイス形状を提供することができるという点も大切です。

まとめると、FIDO は高度なセキュリティが求められる政府機関や企業におけるハードウェアベースの認証メカニズムの導入に革命をもたらし、また、当時はフィッシング耐性のないメカニズム（SMS、TOTP、プッシュ通知など）のみで構成されていたコンシューマー領域における二段階認証に代わるより良い選択肢を可能にしたのです。FIDO ベースの二段階認証はフィッシング耐性があり、多くの場合フィッシング耐性の確保と同時に（耐タンパ性のあるデバイスで暗号鍵を取り出すことのない）ハードウェアベースでもあったのです。

[1] 実際、NIST 800-63B では、少なくとも FIPS-140 レベル 2 の一般セキュリティとレベル 3 の物理セキュリティを提供しない限り、認証器は AAL3 とはみなされない。

しかし、FIDO アライアンスの目標はより一層高いところにありました。その使命（ミッション）は「世界中のパスワードへの過度な依存を減らすことに貢献する」ことです。言い換えれば、二段階認証やスマートカードを使っていない（まだ使っていない）ユーザーのセキュリティを向上させることが目的です。しかし、現在の FIDO/Web 認証の仕様とそれに対応する主要なブラウザやオペレーティングシステムでの実装では一筋縄ではいかなかったのです。FIDO はプラットフォーム認証器、つまりユーザーが既に所持しているスマートフォンやラップトップ PC などに組み込まれた認証機能をサポートしていますが、ユーザーがラップトップを買い換えたりスマートフォンを失くしたりすると、それらのプラットフォーム認証器で管理されている認証資格情報は失われてしまいます。その結果、ユーザーはサインインが必要なときにプラットフォーム認証器に頼ることができない場合があります。例えば、ユーザーが新しいスマートフォンからオンラインバンキングシステムに初めてサインインしようとする場合を考えてみてください。このため、ユーザーはセキュリティキーを購入するか、新しいデバイスからサインインするたびに、安全性の低い FIDO 以外の認証に戻るかのどちらかを選択することになりました。

たとえセキュリティが強化されたとしても、オンラインサービスの利用者全員がインターネット上でのサインインのために専用のハードウェア機器を購入し、携帯することを期待するのは非現実的です。私たちはこのことを経験から知っています。TOTP（または類似の）トークンといった特殊なハードウェアの時代は、コンシューマーの世界に大規模に浸透することはありませんでした。（セキュリティキーを必要とする）Google の Advanced Protection Program（アドバンスド・プロテクション・プログラム）のようなサービスは、より高いセキュリティのために追加料金を支払うことをいとわないユーザーの間では人気があり、またハードウェアウォレットは暗号通貨のアーリーアダプターの間で人気があります。しかし、こうした事例はコンシューマーの世界にはあてはまらないのです。認証のため（だけ）に追加のデバイスを必要とせず、不便なく簡単に使えなければならないのです。

Web 認証レベル 3：ボトムアップのアプローチ

現在、FIDO 認証は、フィッシング耐性を備えたハードウェアベースの認証器によるもので、従来の AAL3 スタイルのスマートカード認証に代わる素晴らしい選択肢となっています。FIDO は、安全な二要素認証として使用でき、フィッシング耐性のある多要素認証を単一のデバイス（認証器）で提供することができるため、従来の高セキュリティのユースケースでパスワードを無くす手段を提供することができるのです。企業内でパスワードへの依存を減らし、フィッシングを無くすことで、最も顕著な 2 つの攻撃ベクトルを排除することができます。

FIDO 認証はフィッシング耐性を提供することができ、コンシューマーが必要とする認証におけるセキュリティを向上させることができます。しかし、物理的なセキュリティキーの不便さ（購入、登録、携行、紛失時の対応）や、プラットフォーム認証の非継続性（例えば、新しいデバイスごとに再登録する必要がある）により、この後者のカテ

ゴリ、特にコンシューマー領域における導入に限界があることが確認されてきました。これらの欠点は、物理セキュリティキーまたはプラットフォーム認証器に基づく FIDO ベースのソリューションをすでに二要素認証に慣れているユーザーにとって面倒なものにするだけでなく、二要素認証をまったく使用せず、パスワードにこだわるユーザーにとって FIDO 認証を提供する上でのさらに高い障壁とする可能性すらありました。

FIDO アライアンスと W3C の Web 認証作業部会は、Web 認証仕様の新バージョン（「Level 3」）でこれらのギャップに対処することを提案しています。特に 2 つの改善提案は特筆に値します。

1. **スマートフォンをローミング認証器として利用：**スマートフォンは、エンドユーザーが一般的に既に所持しているものです。今日、コンシューマー領域における二段階認証はユーザーのスマートフォンを利用しています。ここでの問題点は、以下に述べるようなフィッシングが可能な方法で認証を行うことです。すなわち、フィッシングサイトで誤って OTP（ワンタイムパスワード、1 回のログイン試行またはトランザクションでユーザーを認証する文字列）を入力してしまったり、ブラウザがフィッシングサイトを表示していることに気づかずスマートフォンでログイン確認画面を承認してしまったりする可能性があります。FIDO/Web 認証仕様への追加提案は、Bluetooth を使用して、FIDO 認証器となるユーザーのスマートフォンとユーザーが認証を行おうとしているデバイスの間で通信するためのプロトコルを定義しています。Bluetooth は物理的な近傍性を必要とするため、認証時にユーザーのスマートフォンを活用したフィッシング耐性のある認証手段を手に入れたことになります。この FIDO/Web 認証仕様への追加提案により、ユーザーが専用の認証ハードウェア（セキュリティキー）を携帯することなく、ユーザーのスマートフォンを第 2 要素として利用している現状の 2 要素認証の仕組みを、より高いセキュリティレベル（耐フィッシング性）へアップグレードすることが可能になります。

2. **マルチデバイス対応 FIDO 認証資格情報（マルチデバイス FIDO クレデンシャル）：**

   私たちは、スマートフォンや PC を紛失しても、FIDO 認証器ベンダー（特に OS プラットフォームに組み込まれた認証器）が FIDO 認証資格情報（クレデンシャル）を引き続き有効とするような実装が行われることを期待します。言い換えれば、ユーザーが自分のスマートフォンで異なるサービス事業者を利用するために多数の FIDO 認証資格情報をセットアップしていた場合、その後新しいスマートフォンを入手すると、そのユーザーはすべての FIDO 認証資格情報が新しいスマートフォンで利用可能になるべきです。これは、ユーザーがもはやパスワードを必要としなくなることを意味します。ユーザーがデバイスから他のデバイスへ移動する際、FIDO 認証資格情報はすでに（移行されて）存在し、フィッシング耐性のある認証器として使用できる状態になっているのです。この変更は FIDO 標準の変更ということではなく、認証器ベンダーによる実装に関することであるということに留意してください。現在提案されているこ

の Web 認証および FIDO 仕様への変更案は、特にパスワード認証 FIDO 認証を同時に提供する必要があるサービス事業者にとって、FIDO クレデンシャル（マルチデバイス対応 FIDO 認証資格情報を含む）周辺のより良いユーザー体験を可能にするものになっています。FIDO 認証資格情報に関する新しいユーザー体験は、パスワードマネージャーを使用する場合と非常に似ているものになりますが、セキュリティレベルは従来の FIDO 認証を使わない二段階認証よりもはるかに優れているにもかかわらず、認証時に新たなデバイスや追加の認証ステップを必要としません。新しいユーザー体験では、通常、ユーザーが新しいデバイスでサービス事業者にサインインする時でも、デバイスに組み込まれた生体認証[2]を使えるようになります（以下でさらに詳しく説明します）。

これらのマルチデバイス対応 FIDO 認証資格情報については、ユーザーが必要とする場所でクレデンシャル（認証資格情報）が利用できることを担保するのは OS プラットフォームの責務であるということです。（FIDO 認証資格情報がマルチデバイス対応資格情報である場合、一部の企業は製品の実装において FIDO 認証資格情報を「パスキー」[3]と呼んでいます。）パスワードマネージャがパスワードに対して行うのと同様に、基盤となる OS プラットフォームは、FIDO 認証資格情報に属する暗号鍵をデバイス間で「同期」させます。つまり、ユーザーの同期された資格情報のセキュリティと可用性は、基盤となる OS プラットフォーム（Google、Apple、Microsoft など）のオンラインアカウントの認証メカニズムのセキュリティと、すべての（古い）デバイスが失われたときにアクセスを復活させるためのセキュリティ方法に依存することになります。これは、例えば AAL3 を必要とするユースケースの基準を必ずしも満たしていないかもしれませんが、パスワードと比較するとセキュリティのレベルは大きく向上しています。前述の各プラットフォームは、高度なリスク分析を適用し、認証時に暗黙的または明示的な第二要素を使用し、これによって多くのユーザーに AAL2 相当の保護を与えています。このように、世の中のあらゆるサービスが独自のパスワードベースの認証システムで自活することから、プラットフォームの認証メカニズムの高いセキュリティに依拠することへのシフトによって、インターネットの過度なパスワードへの依存を大規模に有意義に削減することができるのです。

例えば、ユーザーが、あるベンダーのデバイスで FIDO 認証資格情報を有していた場合、そのユーザーが異なるベンダーの新しいデバイスでその暗号鍵を同期させることは、必ずしも可能でない場合があります。このような場合、上記の標準化された Bluetooth プロトコルの存在が便利で安全な代替手段を可能にします。ユーザーが

---

[2] WebAuthn Level 3 仕様の提案はいずれも、現在の生体認証の使われ方が変わることを想定していないことに注意してください。従来通り、あるデバイスでユーザーを認証するための生体認証テンプレートはそのデバイスから外部に出ないことを想定しています。

[3] なお、本書において「passkey」という用語を使用する場合は、第三者が使用していることを例示するものであり、FIDO アライアンスまたはその仕様の正式な用語ではありません。

認証しようとしているデバイス上で FIDO 認証資格情報が容易に利用できない場合も、ユーザーは資格情報を持つデバイス（スマートフォンなど）を近くに持っている可能性が高いのです。それによって、ユーザーは既存のデバイスを使用して、新しいデバイスからの認証を容易にすることができます。

FIDO 認証資格情報の同期と Bluetooth の利用により、FIDO 認証は既存の二段階認証の代替となるだけでなく、二段階認証の導入が困難で、その結果コンシューマーがパスワードに縛られているユースケースに対して初めて有効なソリューションになると考えています。このアプローチは、FIDO エコシステムの進化を反映したものであり、パスワード認証に匹敵する規模でフィッシング耐性のある認証を実現します。

先に述べたように、同期された FIDO 認証資格情報のセキュリティは、基礎となる OS プラットフォームのアカウント・セキュリティに依存します。サービス事業者は、この依存性に依拠することを望むかもしれないし、望まないかもしれません。しかし、少なくとも、同期された FIDO 認証資格情報の検証は、サービス事業者にとってユーザーの本人性を示す非常に強いシグナルとなります。実際、多くのサービス事業者にとって、これだけでユーザーにサインインすることが可能となると予想されます。しかし、追加のセキュリティ要件または規制上の理由から、サービス事事者は新しいデバイス上で同期された FIDO 認証資格情報を信頼する以上のことを選択することができ、ユーザーが新しいデバイスからサインインするときは常に追加のユーザー検証ステップを実行することが可能です。これを実現するために、新たな拡張仕様を提案しています。この拡張仕様では、ユーザーが新しいデバイスから既存の FIDO 認証資格情報を提示したときに、サービス事業者がそれを認識できその新しいデバイス上に追加の当該デバイスに紐ついた暗号鍵を作成できるようにすることができます。このデバイスに紐づいた暗号鍵は、後でこのデバイス上でユーザーを（再）認証するために、余分な検証ステップなしに、また基礎となる OS プラットフォームのアカウントのセキュリティ機構に依存せずに使用することができます。

下図は、マルチデバイス対応 FIDO 認証資格情報（デバイスに紐づいた暗号鍵ー付属）の考え方と、従来の FIDO 認証資格情報との相違点をまとめたものです。

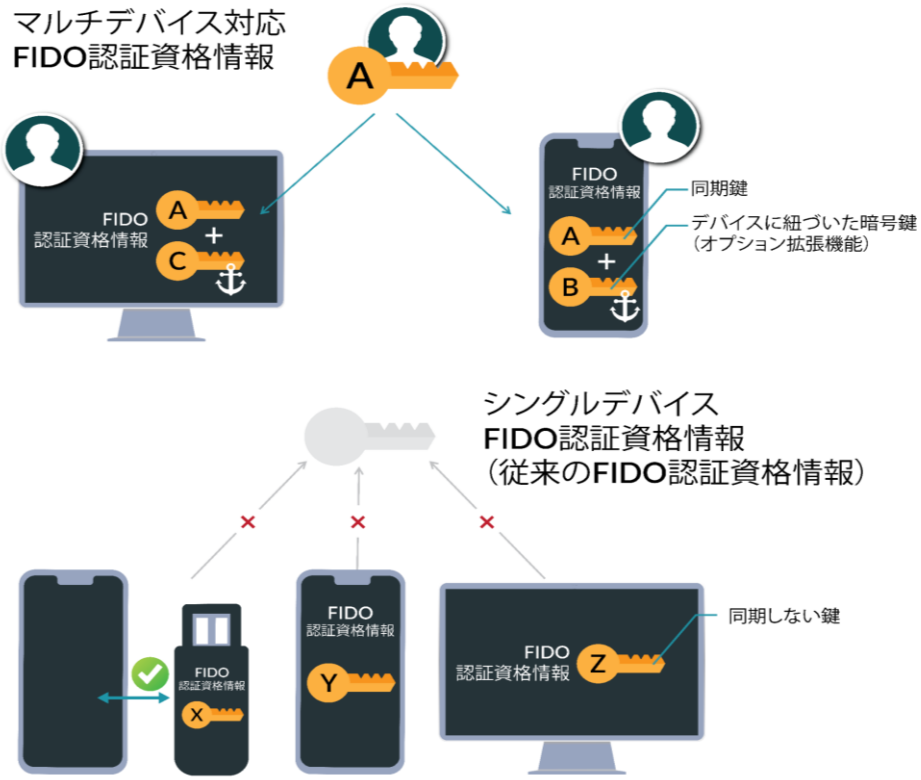

図 *1*：マルチデバイス *vs* シングルデバイス *FIDO* 認証資格情報の比較

マルチデバイス vs シングルデバイス・資格情報：認証機能の実装の際は、同じユーザー（キーA）に属する複数デバイス間で FIDO 認証資格情報の暗号鍵を同期するかどうかを選択できる。同期をサポートする認証器は、デバイス間で同期されないことが保証される追加のデバイスに紐づいた暗号鍵（キーB およびキーC）を作成し、資格情報が新しいデバイスから来たのか、既受入デバイスから来たのかを検出するために使用できる拡張機能もサポートできる（上に示す）。実装によっては、同期がサポートされていなかったり、キーの同期が他の理由、たとえばユーザーの設定によってオフにされている可能性がある（以下に示す）。このような単一デバイスの資格情報であっても、たとえばユーザー認証時にスマートフォンでセキュリティキーを使用する場合（上図左下）など、デバイス間で使用可能である場合もある。

Web 認証/FIDO 仕様は、策定当初より認証資格情報を同期させることを決して排除してはいませんでした。また、今回の仕様変更は認証資格情報の同期の可否を変更するものではありません。むしろ、提案された Web 認証/FIDO 仕様への変更は FIDO 認証資格情報がデバイスをまたいで同期できる世界でより良いユーザー体験を提供すべく設計されているのです。

まとめ

現在の FIDO と Web 認証の仕様は、非常に高い認証の保証レベル（ハードウェアベースの FIDO 認証器を使用する場合は AAL3 と同等）を、従来のスマートカードの展開と比較してはるかに低い展開コストで優れたユーザビリティを提供しています。

しかし、セキュリティレベルが低いユースケース（パスワードのみやフィッシング可能な二段階認証など）では、FIDO を検討する際にセキュリティと利便性のトレードオフという従来からある問題に直面しています。FIDO はより高いセキュリティを提供できますが、その高いセキュリティには、ユーザーが専用の認証デバイス（セキュリティキー）を採用しなければならないという代償を伴います。その結果、多くのサービス事業者はユーザーにパスワード認証のみを提供しているかフィッシング耐性のない二段階認証の提供に留まっていました。

Web 認証の変更案は、この状況を次のように改善するものです

1. ユーザーの既存のスマートフォンをローミング認証器にすること、および
2. ユーザーのデバイス間で FIDO 認証情報を同期させる認証器の実装（特にプラットフォーム認証器）に対してより良いサポートを提供すること

これにより FIDO 認証は、パスワード認証にフィッシング耐性がないなどのリスクを排除し、現時点のパスワードにおけるユビキタス性（現時点の広がり）に匹敵する初めての認証技術となるのです。

Web 認証の変更案には、サービス事業者がローミング認証器やプラットフォーム認証器で（デバイス間で同期されることはない）デバイスに紐づいた暗号鍵を要求できるようにする新しい拡張機能も含まれており、デバイスに紐づいた鍵情報を必要とするユースケースのサポートをさらに向上させることができます。

さいごにまとめると、サービス事業者には次のような選択があります。同期された FIDO 認証資格情報に依存する（そして事実上、プラットフォーム提供者の認証セキュリティとアカウント回復手順に依存する）、もしくは、新たな FIDO 拡張機能であるデバイスに紐づいた暗号鍵と共に FIDO を使用する（そしてサービス事業者固有のアカウント回復メカニズムを実装する）ことです。その結果、FIDO と Web 認証の仕様変更案とともに、資格情報の同期を可能にする FIDO 認証器の実装が予想され、単一のパスワード認証や二段階認証だけが実装されたコンシューマー向けシステム（FIDO により利便性や導入のしやすさを犠牲にすることなく、セキュリティを大幅に向上させる）から、高度なセキュリティが要求される政府機関や企業内システム（FIDO をシンプルに実装

することにより NIST-AAL3 水準の厳しいセキュリティ要件を満たす）までの全範囲にわたるユースケースに対して初めて現状にとって変わる魅力的な選択肢を提供できる状態になっています。これを図にまとめると、以下のようになります。

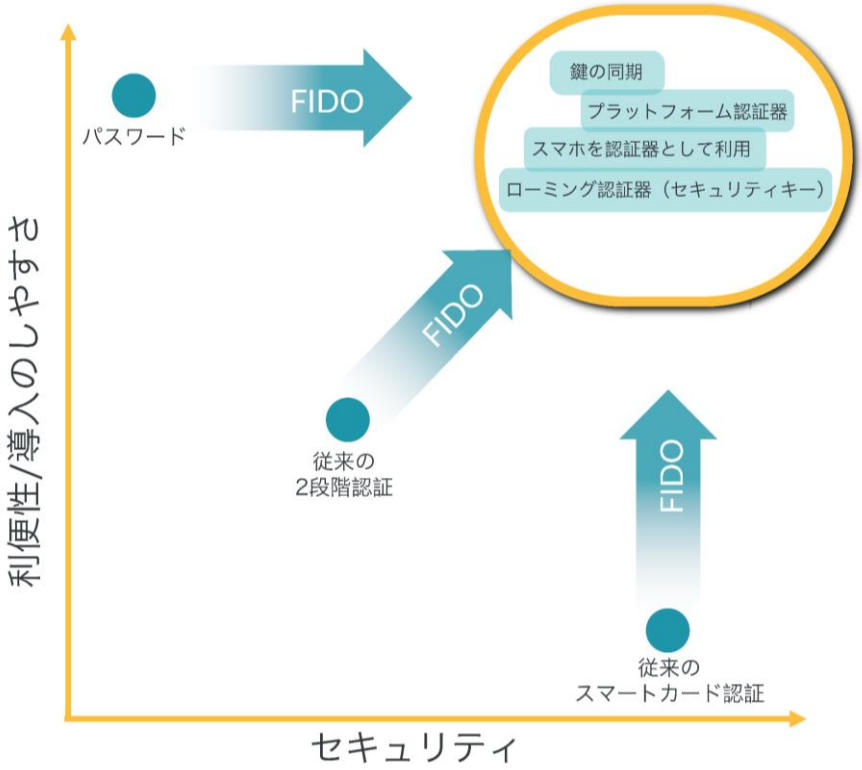

図 *2*：*FIDO* 認証器の実装の方向性

FIDO アライアンスについて

「高速なオンライン ID 認証」を意味する FIDO（Fast IDentity Online）アライアンス www.fidoalliance.org は、セキュリティと利便性の両立をめざすため、2012 年 7 月に設立されたグローバルな非営利団体です。堅牢な認証技術に相互運用性が確保されていない状況を改善し、ユーザーが多くの ID とパスワードを覚えなければならないという煩わしさを解消することを目的としています。FIDO アライアンスは、認証におけるパスワード依存を軽減するために、オープンで拡張性と相互運用性のあるシンプルで堅牢な「FIDO 認証」を標準化することで、オンラインサービスの本質に変革をもたらします。FIDO 認証はオンラインサービスの利用時に、堅牢でプライバシーが確保された便利な認証を提供します。

参照

- FIDO2: WebAuthn & CTAP
- Explainer: broadening the user base of WebAuthn
- FIDO Alliance White Papers & Public Documents