脱パスワードに向けた次世代認証方式 FIDO の取り組み

ヤフー株式会社
Yahoo! JAPAN 研究所
上席研究員　五味　秀仁氏

近年、パスワードリスト型攻撃が多発しており、業界全体での取り組みが必要とされている。

パスワードは再利用可能であり、漏えいすると不正利用されてしまうが、一方で、ネットサービスの利用が日常化し、多い人で 50 個ものパスワードを利用すると言われている現在、パスワードを記憶に頼って利用することはもはや現実的ではない。

このような状況の解決策の一つが、FIDO（ファイド：Fast Identity Online）である。

■FIDO とは

FIDO とは、技術仕様名であり、2012 年に設立された非営利団体の名称でもある。パスワード認証に代わる認証仕様の策定や普及推進を目的としており、現在 200 団体が参加している。

団体としての主な役割は、

- 技術仕様の策定と標準化に向けた取り組み
- 適合性テストの実施
- 商標ライセンスの登録
- オピニオンリーダーとしてのエコシステム構築牽引

であり、メンバーには Google や VISA、yubico、lenovo、Alibaba、Yahoo! JAPAN 等様々なプレイヤーが名前を連ねている。

FIDO では、認証の三要素（記憶、所持、生体情報）のうち、所持（本人のみが所持しているものによる認証：ワンタイムパスワードのトークン、IC カード等）、生体情報（本人の特徴を表すデータによる認証：指紋、音声、虹彩等）を主な対象としており、現在、パスワード置き換え型（UAF：Universal Authentication Framework）とパスワード補完型（U2F：Universal 2nd Factor）についての技術仕様を FIDO 仕様 1.0 として公開している。

適合性テストでは、FIDO 仕様を実装した各社の製品どうしで検証テストを実施し、合格したものを FIDO-Ready 認定製品としてロゴ使用を認めている。FIDO では、セキュリティ／アプリベンダーによるセキュリティの向上、コンピュータ／携帯端末ベンダーによる強固なセキュリティの組み込みなどを行い、セキュリティ／アプリベンダーには開発コストの低減、ユーザーには使い勝手の向上といったメリットを提供し、コンピュータ／携帯端末ベンダー、セキュリティ／アプリベンダー、認証器メーカー、ユーザーそれぞれがメリットを享受できる FIDO エコシステムとして構築していく。

■各社の取り組み

FIDO-Ready 製品としては、Lenovo の指紋センサー付 ThinkPads や Samsung Galaxy S5 などが挙げられ、Microsoft では Windows10 に FIDO を採用している。PayPal 等ではすでに指紋認証による支

払手続きが利用可能となっており、Alibaba でも FIDO ベースの支払いを開始している。

また、Google では二段階認証（U2F）を採用しており、Yahoo! JAPAN でも U2F 対応サーバーの開発を行い、FIDO-Ready の認定を受けている。

■FIDO の概念

FIDO の概念の 1 つとして、認証の部品化が挙げられる。

従来の認証では、各サービスに特化した認証手段が必要であり、それぞれにコスト負担がかかり柔軟性も低かった。しかし、FIDO の認証では、プロトコルの標準化によりクライアントの認証手段が縛られることがなくなるため、プラグイン的に認証手段を追加することで多要素認証が装備可能となる。これにより、開発ベンダーは新たな認証手段を低コストで公開・配布でき、認証事業者は、多要素認証を取り入れやすくなることで認証強化につながる。また、利用者にとっても、認証手段が選択可能となるなど、それぞれにメリットが生まれる。

また、従来の認証では、認証サーバー側で識別・検証を行っていたが、FIDO では認証機能を分解し、検証はユーザー側端末で行い識別のみを認証サーバーで行うため、検証に必要な生体情報などがネットワーク上に流通することがなく漏えいリスクが低減する。

次に、トラスト（信頼性）の課題として、ユーザー側のクライアント端末に怪しい認証器が入った時などに、認証サーバー側ではクライアントの認証結果情報を受け入れてよいか識別が必要となる。FIDO システムでは公開鍵方式を用いており、あらかじめ認証器を登録し、登録された認証器の秘密鍵によって暗号化された認証情報を FIDO サーバーの公開鍵を使って確認し、改ざんがないことを以てユーザー認証を行う。

さらに、プライバシー保護の観点では、FIDO ではクライアント端末で検証が行われるため、生体情報がサーバー上に保管されることはなく、サーバー間、アカウント間でのリンク付けもない。公開鍵は公開情報なので、洩れても生成しなおせばよいだけで問題がないため、サーバー側の管理体制の負担は軽減される。

■FIDO と ID 連携の関係

FIDO が対象として注力している認証は、ID 管理機能における階層構造で ID 連携やシングルサインオンよりも下のレイヤーにある認証を補完するものである。

ID 連携では、Yahoo! JAPAN のような IdP が認証した後、アサーション（認証結果・個人属性）をサービスプロバイダーに渡すことによりユーザーのサービス利用が可能となる。FIDO は IdP-ユーザー間の認証を強固にするための仕様であり、ID 連携を補完、強化するものである。

FIDO は多要素認証を実現するので、NIST の『電子認証ガイドライン』でレベル 3「高」とされる水準まで認証の信頼レベルを上げることができ、METI が推進する ID 連携トラストフレームワークの基盤の一部にできる可能性が期待できる。

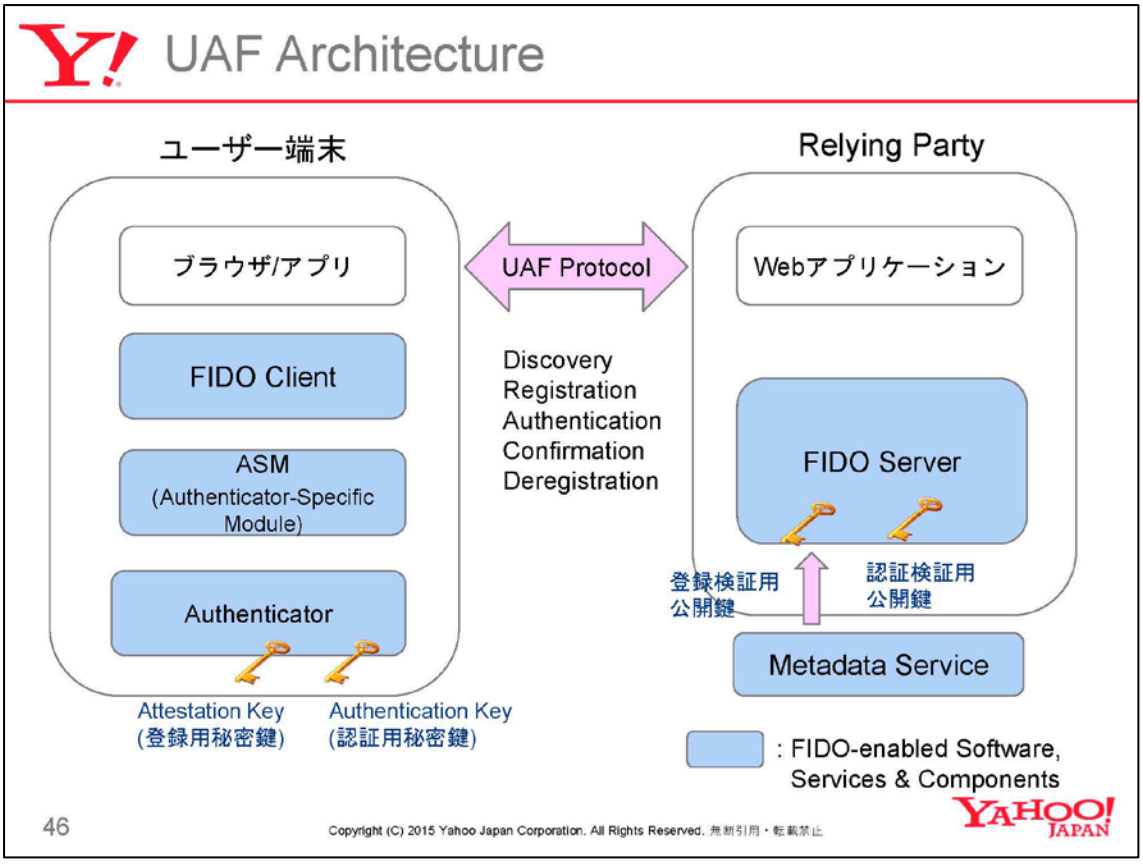

図 1　FIDO の技術仕様　UAF アーキテクチャ