Close-Up

パスワードのいらない世界へ

～注目のFIDO（ファイド）技術～

近年、インターネットを利用したサービスの拡大を背景に、IDを乗っ取る「パスワードリスト攻撃」が横行している。そこには、管理の大変さから、ユーザーが複数のサービスでパスワードを使い回す現状がある。こうした現状に対し、セキュリティ上のリスクを軽減するため、生体認証を取り入れる動きが活発化している。特に注目されるのが、「FIDO（ファイド：Fast IDentity Online）」と呼ばれるオープン標準の認証方法。2004年2月、ビル・ゲイツ氏はパスワードの終焉を予言したが、ようやくその時が訪れようとしているかもしれない。

パスワード管理が限界に？

トレンドマイクロの「パスワードの利用実態調査 2014」によると、Webサービスを利用する際、ユーザーの9割以上がパスワードを使い回しているという。理由は「異なるパスワードを設定すると忘れてしまう」「異なるパスワードを考えるのが面倒」など。パスワードを使い回すユーザーが多いことから、「パスワードリスト攻撃」の成功率も高くなっている。これは、何らかの方法で攻撃者が入手したIDとパスワードのリストを用いて、様々なインターネットサービスにログインを試みる攻撃方法である。

また依然として、ありうるパスワードを全パターン試みる「総当たり攻撃」や、利用頻度の高いパスワードを試みる「辞書攻撃」も多い。主に北米や西欧で流出したパスワードのデータを分析した米SplashDataの「2014年最も使われているパスワード」調査の上位3位は、「123456」「password」「12345」だった。

サービス提供者は様々な認証強化に取り組んでいるが、最近は「パスワード疲れ」という言葉もよく聞かれ、ユーザーのパスワード管理は限界になりつつある。

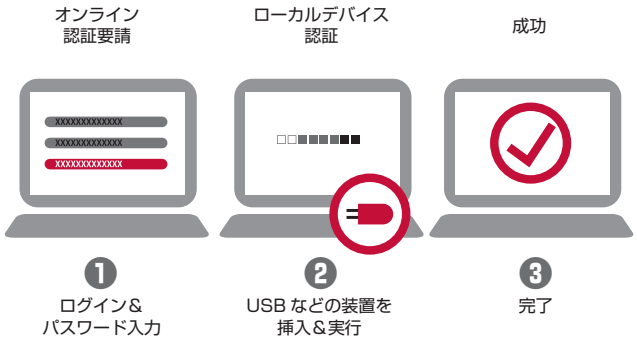
標準化団体「FIDO Alliance」誕生

こうした背景から、より簡単かつ安全なユーザー認証を目指し、本人の身体的特徴（指紋、声紋、てのひら、顔、虹彩、網膜、静脈など）や行動的特徴（筆跡、キーストローク、ジェスチャーなど）を利用した生体（バイオメトリクス）認証に取り組むサービス事業者は多かったが、サービスの基準がばらばらだった。そうした中、「パスワードのいらない世界」の実現を目指し、強固なオンライン認証方式の新標準確立に取り組む非営利の業界団体が現れた。2012年に米国で設立された非営利組織「FIDO Alliance」である。

構想が始まったのは2009年。当時PayPalのCISO（最高情報セキュリティ責任者）であったマイケル・バレット氏の元へ、Validity Sensors（後にSynaptics が買収）のCTO（最高技術責任者）が、PayPal.comに指紋認証を導入しないかと訪問。以前からID／パスワードに代わる認証方法が必要だと感じていたバレット氏はこの時、指紋認証に興味を持ちつつも、複数のベンダー間で利用できる業界標準確立が必要だと語った。

それからPayPalとValidity Sensors、さらにLenovoやセキュリティベンダーら6社で2012年にFIDO Allianceを立ち上げ、その後2013年にはFIDO仕様の策定、業界のア

■図1-1 FIDO UAF標準（パスワード置き換え型）



■図1-2 FIDO U2F標準（パスワード補完型）

FIDO Alliance発表資料を参考に作成（図1-1、1-2）　https://fidoalliance.org/specifications/overview/

ライアンス、対応製品・サービスの認証を行う団体として公式な活動を開始した。間もなく2要素認証の標準化に2011年から取り組んでいたGoogleやスウェーデンのデバイスメーカーYubico、オランダの半導体メーカーNXP Semiconductorsも参加し、2014年12月にオンライン認証のプロトコル仕様「FIDO 1.0」を公開した。

現在、FIDO Alliance には220社以上が加盟し、ボードメンバーには、Alibaba、Google、Intel、Microsoft、Qualcomm、Samsung、VISA、NTTドコモなど、世界的な企業が名を連ねている。2015年6月には、米国の国立標準技術研究所（NSTIC）や、英国の首相官邸からもメンバーが参加。政府機関も他の民間企業と共にFIDOの仕様策定に携わることになった。

FIDOの認証プロセス

一般に認証要素には次の3つがある。

- **本人しか知り得ない知識**（something you know）
  例：パスワード
- **本人の持ち物**（something you have）
  例：ICカード、トークン
- **本人と識別できる特徴**（something you are）
  例：生体情報

この中でFIDOは、特徴（生体情報またはPINと呼ばれる暗証番号）を使って認証する「UAF」（Universal Authentication Framework：パスワード置き換え型）と、UAFへの移行期の対応として既存のパスワード（知識）に2つめの要素（持ち物）を追加する「U2F」（Universal Second Factor：2要素認証によるパスワード補完型）の2つを標準化している。それぞれのユーザー操作は次のようになる。

○UAF

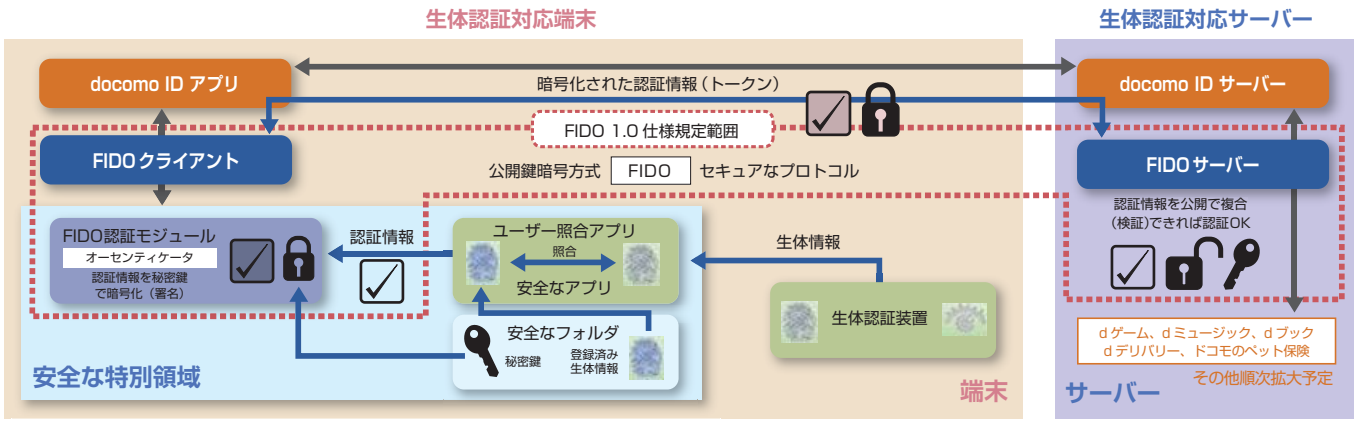
ユーザーは、UAFを搭載した端末に自分の生体情報（またはPIN）を保存。利用するオンラインサービスで生体認証を使うように一度設定しておけば、以降はID／パスワードを入力する必要がない。例えば指紋認証であれば読み取り画面で指をあてるだけでサービスにログインできる（図1-1）。

○U2F

U2F対応のWebブラウザをインストールした端末で、USBなどのU2F対応セキュリティキーを登録しておく。そして利用するU2F対応のオンラインサービスで一度認証しておけば、ID／パスワードの入力に加え、セキュリティキーによる2つめの認証を追加できる。これにより、何者かが他の端末から同じID／パスワードを使ってログインするなりすましを防ぐことに加え、アクセスしているサイトがフィッシングサイトではないことも保証される（図1-2）。

FIDOは、従来のパスワード認証のように生体情報やセキュリティキー情報をサーバへ送信・保管せず、また端末内ではOSから隔離されたセキュアな領域に格納する。オンラインサービスのサーバとのやり取りには公開鍵暗号を採用しており、オンラインサービスに登録する際に秘密鍵と公開鍵のペアを生成し、サーバへは公開鍵のみ送信・保管。サーバとデバイス間のリンク付けがないためプライバシーも保護される。

万が一サーバで情報漏洩があっても、公開鍵から個人を特定されることはなく、再び公開鍵を生成し直せばよい。FIDOは、指紋や虹彩、音声、PIN、セキュリティキーといった複数の認証要素に対応し、プロトコルについては規定しているが、どの認証要素を採用するかはオンラインサービ



■図2 FIDOプロトコルを実装したNTTドコモの新しい認証方式

NTTドコモのプレスリリース（2015年5月26日）を参考に作成
https://www.nttdocomo.co.jp/info/news_release/2015/05/26_00.html

ス側で決定できる柔軟性もある。

標準化によって、PCやタブレット、スマートフォンのメーカーやオンラインサービスのプロバイダーは、低コストで認証手段を提供でき、ユーザーの認証強化につながる。またユーザーにとっても、従来のようなWebサイトごとに異なるセキュリティキーを持ったり、セキュリティコードを毎回入力するといった必要がなくなる。

日本でも普及が進む FIDO認定製品

FIDOではUAF、U2Fのそれぞれに、サーバとクライアント（オーセンティケーター）の仕様を定めており、認証テストに合格した製品は「FIDO Certified」とされ、2014年12月に公開されたFIDO 1.0認定製品の中にはすでに日本で利用されているものもある。

FIDO Allianceの設立メンバーである米Nok Nok Labsからは、UAF準拠のモバイルアプリのSDKや認証サーバなどが、またYubicoからはU2F準拠のセキュリティキーが、それぞれ販売されている。Googleは、Chrome 38からU2Fに対応し、ログイン時のセキュリティを強化している。

Yahoo! Japanは、自社の「Yahoo! ID連携」サービスにFIDOを採用することで認証強度を強化している。同サービスは認証機能のオープン標準である「OpenID Connect」※1で構築されているが、FIDOはこうした既存のオープン標準を補完するものとして組み合わせて使うことができる。

2015年5月にキャリアとして世界で初めてFIDO Allianceに加盟したNTTドコモは、2015年春に発表したスマートフォンの4機種をFIDOに対応。前述のNok Nok Labsのソリューションを採用し、ドコモが提供するゲームやトラベルなどのオンラインサービスで、UAFに準拠した指紋や虹彩によるログインや決済ができるようにした。今後もこのFIDO対応の順次拡大を予定している。

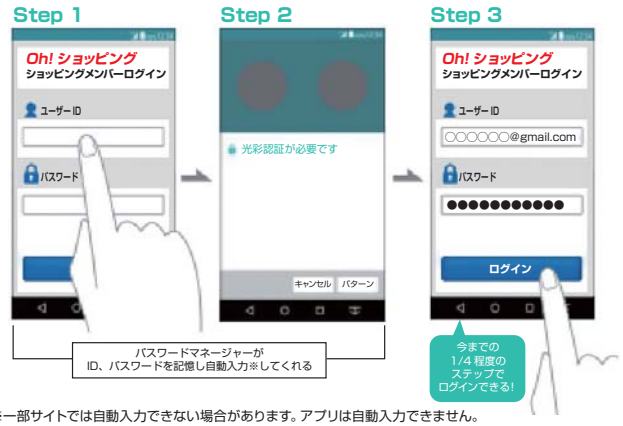
NTTドコモにおけるオンライン認証の内部的な流れは次のようになる（図2）。まず、指紋や虹彩の情報を端末に登録する。そして「docomo ID設定」で生体認証を使うように指定すると秘密鍵と公開鍵のペアが作成される。秘密鍵は端末内の安全な領域に格納され、公開鍵は「docomo IDサーバ」を経由して「FIDOサーバ」へ送信され、設定が完了する。ユーザーがオンラインサービスにログインする際に指紋や虹彩を読み取ると端末内の情報と照合され、合致すれば認証情報が秘密鍵で暗号化された後、docomo IDサーバを経由してFIDOサーバへ送信される。そして認証情報を受け取ったFIDOサーバーが登録時の公開鍵で認証情報を復号できれば、オンライン認証が完了となる。

MicrosoftはFIDO 2.0の仕様策定に参加しており、2015年7月に提供開始した「Windows 10」はこれから策定される2.0仕様に準拠する予定。Windows 10の新たな認証機能は、指紋・顔・虹彩の3つの生体認証が可能なサインイン機能「Windows Hello」と、そのWindows Hello（またはPIN）にデバイス認証を加えた2要素認証を行う「Microsoft Passport」※2である。これは、個人用のMicrosoftアカウントのほか、企業用のActive DirectoryやAzure Active Directoryでも設定できる。

今後の認証サービスの動向

前述のWindows 10で生体情報を登録しない場合は、4桁のPINを設定することでID／パスワードを入力しなくてよくなる。初期セットアップ画面では「パスワードは時代遅れです」というメッセージとともに「PINはパスワード

※1 2005年に米Six Apartが開発した認証技術で、同一IDで様々なWebサイトやアプリへのログインを可能にするAPI標準仕様。
米国の非営利組織OpenID Foundationによって標準化が進められており、日本にも2008年に支部が設立されている。
※2 1999年に発表した「Microsoft Passport」と同名であるが、これはシングルサインオンのためのものであり、現在は「Microsoftアカウント」に引き継がれている機能である。



※一部サイトでは自動入力できない場合があります。アプリは自動入力できません。

■図3 スマートフォン「ARROWS NX F-04G」の虹彩認証

を使用するよりも早くて安全です。ぜひご利用ください」と表示される。これは、デバイスと組み合わせた2要素認証によってセキュリティが強化されるからである。

スマートフォンやタブレットの世界では、煩雑な文字入力が難しいこともあり、例えばiPhoneが4桁のPINまたは指紋認証でアクセスでき、Android端末では画面に表示される点をスワイプする「パターンロック」が使われるなど、パスワードレスが主流である。パソコンの世界でも、Windows 10のFIDO採用で本格的なパスワードレスが進むと見られ、FIDOがオンライン認証の事実上の世界標準だという声も聞かれる。Google ChromeがFIDO対応したことで、他のブラウザの追随も予想され、Webアプリケーションの提供側もFIDOを組み込む動きが出てきそうである。

AmazonやAppleはFIDO Allianceに現時点では加盟していないが、今後の動向が注目されるところだ。またマイナンバー制度の導入が決定した日本では、2015年8月の参議院内閣委員会において、普及の課題となる個人情報保護の観点からパスワード管理の話になった際、生体認証が急速に普及している背景からFIDOに言及しており、こちらの動向も注目される。パスワードレスが進めばユーザーの利便性も向上し、モバイル決済を始め、新たなビジネスモデルの出現が予想される。

一方、生体認証の技術も進化を遂げている。PayPalの開発部門幹部のジョナサン・ルブラン氏は2015年4月、皮膚にチップを埋め込んだり、口から飲み込むカプセルによって認証のためのツールを体内に取り込んだりといった、体内データを利用する時代が来ていると語った。生体認証の技術における進展も注目される。

富士通の取り組み

富士通では、NTTドコモのFIDO実装にいち早く対応。FIDO UAFに準拠し、世界で初めて虹彩認証を搭載したスマートフォン「ARROWS NX F-04G」を2015年5月に発売した。利用者は、読み取り画面に目を映すだけで虹彩の登録が完了し、画面のロック解除に使えるほか、ネットショッピングの決済では画面を見るだけでID／パスワードが自動入力されるので今までの4分の1程度の手間でログインできる（図3）。

なお、富士通の「虹彩認証技術」は、スペインで開催された「Mobile World Congress2015」にて、AndroidPITの「Best innovation award」を受賞。従来からある虹彩認証機能をスマートフォン用に小型・最適化し、桁違いの速度・精度に加え、パスワードを忘れても平気といった利便性などが評価された。これからも富士通は同技術をセキュリティソリューションへの適用など幅広い分野への応用をすすめていく。

AndroidPIT
「Best innovation award」の盾

● 富士通関連サイト
ARROWS NX F-04G
http://www.fmworld.net/product/phone/f-04g/

<参考資料>
○相戸浩志『図解入門よくわかる最新情報セキュリティの基本と仕組み』
秀和システム
○FIDO Alliance　https://fidoalliance.org/
○トレンドマイクロ：ーパスワードの利用実態調査 2014ー
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20140609010140.html
○Windows 10時代の新認証
「Windows Hello／Microsoft Passport」と「FIDO」を理解する
http://www.itmedia.co.jp/enterprise/articles/1507/29/news036.html
○ヤフー株式会社 五味秀仁
「脱パスワードに向けた次世代認証方式FIDOの取り組み」
http://www.jipdec.or.jp/library/report/u71kba0000001uka-att/summary4702.pdf

〈監修〉編集委員　山上浩司　パシフィックシステム㈱