Standardization（特集）

FIDO認証　セキュリティ　公開鍵暗号方式

パスワード課題を解決するFIDO（ファイド）認証特集

FIDOアライアンスにおけるオンライン認証の標準化動向とドコモの貢献

プロダクト部　森山（もりやま） 光一（こういち）　富山（とみやま） 由希子（ゆきこ）
牧野（まきの） 由樹子（ゆきこ）

FIDO®＊1（ファイド）アライアンスは，オンライン認証におけるセキュリティと利便性の両立をめざし，ID・パスワードに代わる新しい認証方式を提唱するグローバルな非営利団体である．ドコモは2015年からボードメンバーとして加入し，FIDO仕様策定とエコシステムの発展に貢献している．本稿では，FIDOアライアンスとFIDO認証について解説する．また，ドコモの貢献と国内外におけるFIDO認証の広がりを紹介し，今後を展望する．

1. まえがき

FIDOとはFast IDentity Onlineの略称で，FIDOアライアンスが提唱するオンライン認証方式のモデルとそれに基づく仕様群を指している．この認証モデルの特徴は，ID・パスワードに代わり公開鍵暗号方式＊2を活用することで，「共有の秘密」に依存しない認証方式としていることである．そして，FIDO認証モデルに生体認証などを組み合わせることで，シンプルで堅牢なオンライン認証を実現し，セキュリティと使い勝手の良さの両立をめざしている［1］．

近年，キャッシュレスによる決済やその他さまざまな場面でオンライン認証の必要性が増している一方，不正アクセスや不正決済などに関するニュースが後を絶たず，使い勝手を確保したまま安全に認証できる手段の提供がますます重要になっている．そのような中，ドコモは2020年3月からdアカウント®＊3パスワードレス認証の提供を開始した．これは，2015年5月から提供しているdアカウントFIDO生体認証［2］の十分な広がりをベースとして，全面的にFIDO認証に移行するオプション機能をお客様に提供することで，より安心してオンライン認証を使っていただくものである［3］．

この実現は，単にFIDO認証を技術の1つとして採用したというものではない．まず，商用サービスの提供開始当初から，FIDO認証の特長を最大限活

©2020 NTT DOCOMO, INC.
本誌掲載記事の無断転載を禁じます．
本誌に掲載されている社名，製品およびソフトウエア，サービスなどの名称は，各社の商標または登録商標．

＊1　FIDO®：FIDOおよびFIDO Allianceロゴは FIDO Allianceの商標または登録商標．
＊2　公開鍵暗号方式：秘密鍵と公開鍵のペアを用いる非対称な暗号方式．秘密鍵は安全に保持する必要があるが，公開鍵は秘匿する必要がなく，共通鍵暗号方式と異なる特徴をもつ．
＊3　dアカウント®：㈱NTTドコモの登録商標．

用した．そして，FIDOアライアンスにボードメンバーとして加入した上でその経験をフィードバックし，FIDO認証の可能性をさらに探求し，FIDOアライアンスにおける標準化活動において貢献してきたことで成し遂げることができたものである．また，結果として，国内外においてより広くFIDO認証が使われ始めていることについても注目いただきたい．

本稿では，FIDOアライアンスとFIDO認証について解説し，ドコモの貢献と国内外におけるFIDO認証の広がりを紹介し，今後を展望する．

2. FIDOアライアンスとFIDO認証

2.1 FIDO認証モデル

FIDO認証モデルは，セキュリティと使い勝手の両立を実現するため，公開鍵暗号方式を活用したオンライン認証のための新しいモデルである．FIDO認証モデルでは，FIDO認証器（以下，認証器）によってユーザが認証器の所有者であることをローカル検証する部分と，公開鍵暗号方式に基づく秘密鍵と公開鍵のペアを使った署名検証によってオンライン認証を成立させる部分に分離している（**図1**）．

認証に際しては，あらかじめ設定が必要である．設定では，まず認証に必要な秘密鍵と公開鍵のペアを認証器で生成し，秘密鍵を認証器に格納し，公開鍵を認証サーバ（以下，サーバ）に登録する（**図2**(a)）．登録要求に対しては，まずサーバから認証器にチャレンジコード（ランダムな文字列）が送られる．そして，認証器で鍵ペアを生成して秘密鍵を認証器の安全な領域に格納した上で，秘密鍵で署名したチャレンジコードと公開鍵をサーバに送信する．チャレンジコードを使うのは，サーバと認証器のや

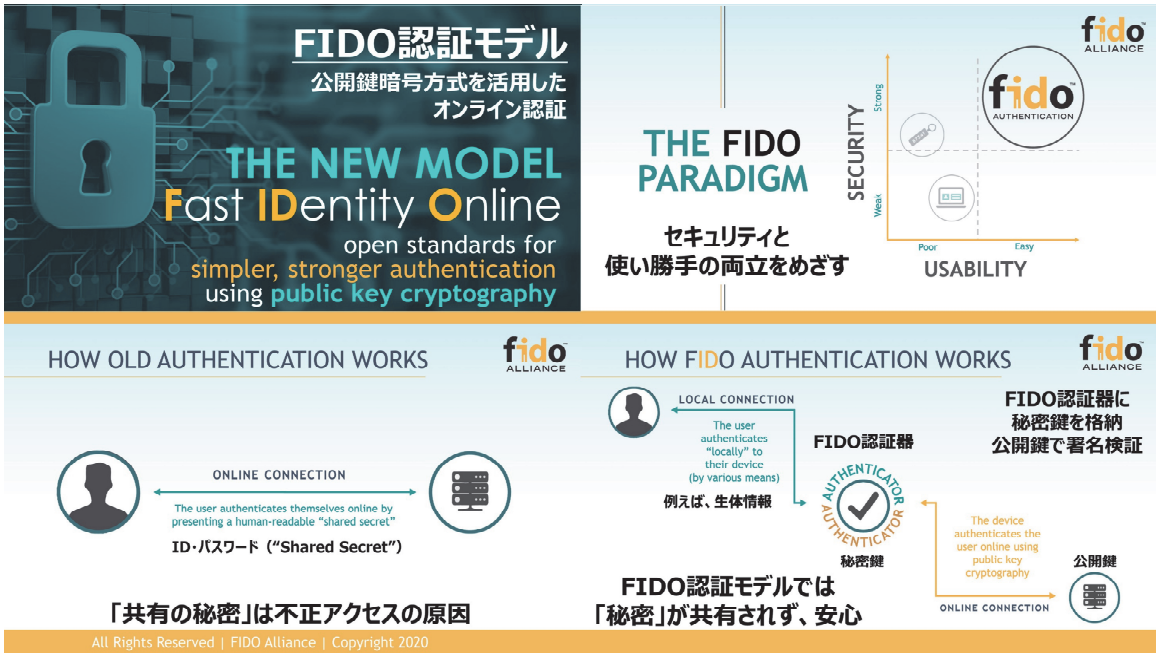

図1　FIDOアライアンスの目標とFIDO認証モデル

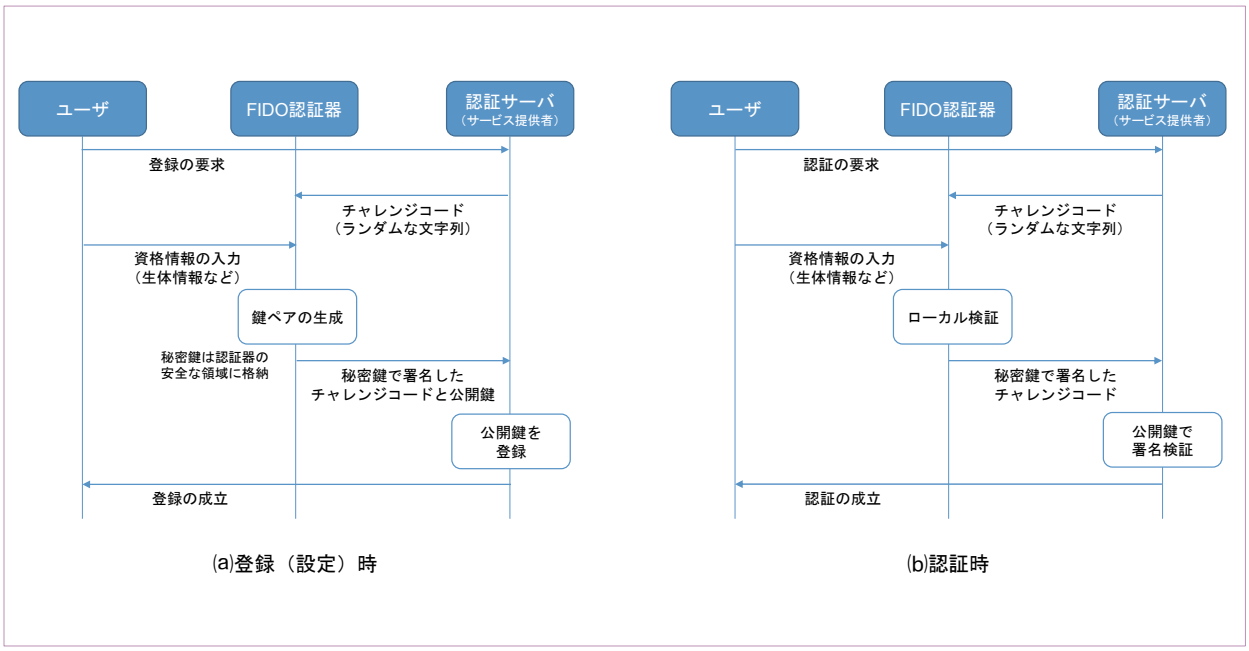

図2　FIDO認証の流れ（「秘密」がインターネットを通過しない）

りとりが対になっていることを担保するためである．

ユーザからの認証要求に対しては，まずサーバから認証器にチャレンジコードが送られる．次に，生体情報や端末ローカルでのみ有効な知識情報（例えば，パスコード）などの資格情報で認証器のユーザを検証する．検証できた場合には，秘密鍵でチャレンジコードに署名し，サーバに返却する．そして，サーバでは署名されたチャレンジコードをペアとなる公開鍵で署名検証し，検証できた場合にオンライン認証が成立する（図2(b)）．

このように，FIDO認証モデルでは従前のID・パスワードを使った認証と異なり，ユーザ・認証器とサーバとで「秘密」が共有されず，パスワードのような「共有の秘密」がインターネットを通過することもない．そのため，フィッシング耐性があり，異なるサービス提供者に対する認証のための操作も，指紋をかざすなどの動作のみで同一にできるという特長がある．すなわち，シンプルで堅牢なオンライン認証を実現することが可能である．

2.2　FIDOアライアンス

FIDOアライアンスは，2012年に設立されたパスワード課題の解決に注力するグローバルな非営利団体である．FIDO認証モデルに基づく技術仕様の策定，相互運用性を確保するための認定プログラムの運営，そして各標準化団体との協業などを通じたFIDO認証の導入推進を行っている．さまざまな業界から現在約250社が参画し，業界の垣根を超えるコンソーシアムとなっている（**図3**）．

(1)メンバーシップ

FIDOアライアンスには，年会費とベネフィットの違いに応じて，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，ガバメントメンバーと4つのメンバーシップのレベルと区別がある．これらのうち，FIDOアライアンスで特にリーダーシップを発揮できるのがボードメンバーである．

ボードメンバーは，FIDOアライアンスにおける意思決定に参加する権利をもつ．すなわち，ボード会議への参加，新たな戦略やその遂行に必要な作業

図3　FIDOアライアンスのボードメンバー

部会（WG：Working Group）の設置など各種提案のボード会議への付議，そして意思決定のための投票権をもつ．また，FIDOアライアンスとボード会議を代表する執行評議会（Executive Council）のメンバー，および作業部会の座長・共同座長として選出され，定められた任期を務めることを権利としてもつ．さらに，マーケティング活動に優先的に参加できる権利などをもつ．

ドコモは，FIDOアライアンスに加入した2015年5月からボードメンバーである．

⑵作業部会

FIDOアライアンスの日々の活動は，主にそれぞれの役割を担った作業部会によって推進されている．現在，FIDOアライアンスには15の作業部会がある．作業部会の種類には，FIDO認証の技術仕様，セキュリティ要件，認定プログラム仕様などを定める技術作業部会（Technical WGs），FIDO認証の導入・展開を推進する作業部会（Adoption WGs），そしてFIDOアライアンスのミッションを国・地域ごとに効果的に実行することを目的とした作業部会（Regional WGs）の3つがある．

ドコモが座長・共同座長を務めている，または務めてきた作業部会は下記の通りである．

・コンシューマー・デプロイメント作業部会（Consumer Deployment WG）
・セキュリティ・プライバシー要件作業部会（Security and Privacy Requirement WG）
・日本作業部会（FIDO Japan WG）

2.3　FIDO仕様

FIDO認証モデルを実装可能にするFIDO仕様には，2014年12月にそれぞれバージョン1.0として仕

様を公開したFIDO UAF（Universal Authenticator Framework）とFIDO U2F（Universal Second Factor），そして2018年から積極的に展開しているFIDO2がある（**図4**）．

- FIDO UAF：パスワードレス認証のために設計した仕様
- FIDO U2F：2段階認証の2要素目のために設計した仕様
- FIDO2：FIDO UAFとFIDO U2Fのそれぞれの特長を活かし，FIDO認証をより広く展開するため，OS・ブラウザなどのプラットフォームに組み込みやすくするために設計した仕様

FIDO仕様策定におけるドコモの貢献の1つに，FIDO UAF 1.1がある．これは，ドコモがdアカウント認証にFIDO UAF 1.0をいち早く採用して商用導入した経験をフィードバックし，Android™＊4 OS 8.0以降に搭載された「キーの構成証明機能（Key Attestation）」を活用することで，端末メーカによる機種ごとのカスタム実装なしに，FIDO UAFアプリの開発・搭載を可能にしたものである．2017年11月に商用導入を開始し，同年12月に発表した．これは，FIDO2の離陸を待たずにFIDO認証を普及させる一助となった．

(1)FIDO2とWeb認証

FIDOアライアンスは，FIDO認証のさらなる展開に向けて，OS・ブラウザなどのプラットフォーム対応が不可欠と判断した．そこで，ブラウザでの対応のためにはW3C®（The World Wide Web Consortium）＊5での標準化が必須であることから，2015年11月にFIDOアライアンスからW3CにWeb部分の基本仕様（案）を提供し，リエゾンパートナーとして連携して標準化することに貢献した．そして，W3CとしてFIDO認証モデルをWebブラウザで提供

図4　FIDO認証モデルに基づくFIDO仕様群

＊4　Android™：米国Google LLCの商標または登録商標．

＊5　W3C®：Web技術の標準化を進める国際機関．The World Wide Web Consortiumの略称であり，商標または登録商標．

するためのJavaScript*6 API（Application Programming Interface）*7（Web認証）を標準化し，2019年3月にLevel 1として正式勧告とした．現在，主要なブラウザがWeb認証Level 1に対応し，W3CではLevel 2の策定が進んでいる［4］［5］．

ブラウザでWeb認証を提供する場合にも，ユーザは認証器の利用が必要になる．この認証器としてはブラウザが動作する端末に組み込まれたプラットフォーム認証器，またはUSBなどを介して接続する外部認証器（いわゆるセキュリティキーなど）を使うことができる．後者を実装可能とするためFIDOアライアンスとして策定したのがCTAP（Client to Authenticator Protocol）（デバイス間連携仕様）である．このCTAPはFIDO U2F仕様の該当部分を継承して策定された．

⑵国際標準化

FIDOアライアンスでは国際標準化団体との連携も進めており，その成果の1つとして，認証器の実装に必要なFIDO UAFとCTAPは，2018年12月に国際電気通信連合（ITU：International Telecommunication Union）の電気通信標準化部門（ITU-T：ITU Telecommunication Standardization Sector）によって，国際標準として以下の通り採択された．

・ITU-T勧告X.1277 - FIDO UAF 1.1
・ITU-T勧告X.1278 - FIDO2 CTAP（U2F CTAP1含む）

2.4 認定プログラム

FIDOアライアンスは，FIDO認証に対応する製品のFIDO仕様への適合性を検証し，主に製品とサービス間で相互運用性を確保するための認定プログラム制度を設けている．認定を受けた企業は，FIDO認定ロゴを製品に付与することができる．FIDO認定プログラムは，FIDOアライアンスに加入していない企業・団体でも参加することが可能である．

相互運用性を確保するための認定プログラムには，認証器とサーバの機能に関して開発者が自ら実施する適合性（Conformance）テスト，FIDOアライアンス主催としてFIDOアライアンスメンバー企業がホストとして実施する相互接続性（Interoperability）テスト，そして第三者ラボによって検証する認証器のセキュリティ認定がある．

認証器のセキュリティ認定では，後述するセキュリティ・プライバシー要件作業部会が定めるセキュリティ要件（L1，L1＋，L2，L2＋，L3，L3＋の6段階）の適合性を検証しており，L1認定の取得は必須，L1＋～L3＋認定の取得はオプションである．2018年からは生体センサの性能に関するバイオメトリック部品認定プログラム（オプション）も開始している．

ドコモは，2015年4月にカリフォルニア州サンノゼで開催された第1回相互接続性テストに参加し，2015年5月のFIDO UAF 1.0を採用したdアカウントFIDO認証の提供開始当初からFIDO認定を取得した端末で商用サービスに対応することができた．また，その経験を踏まえ，カリフォルニア州パロアルトに拠点を持つDOCOMO Innovations, Inc. でFIDO認定プログラム黎明期の相互接続性テストをホストし，そのフィードバックで貢献している．

2019年11月には，国内で初めて相互接続性テストが開催され，10の国・地域から14の企業が参加し，国内から新たに3製品がFIDO認定を取得した．

3. ドコモのFIDOアライアンスにおける貢献

現在，ドコモはFIDOアライアンスにおいて複数の役割を果たしている．1つはボードメンバー企業としての役割である．FIDOアライアンスにおけるボード会議はその意思決定を担っており，ドコモはその一員である．

＊6 JavaScript：Webブラウザなどでの利用に適したスクリプト言語．JavaScriptは，Oracle Corp. およびその子会社，関連会社の米国およびその他の国における登録商標または商標．
＊7 API：OSやミドルウェアなどが提供する機能を，他のアプリケーションソフトウェアが利用するためのインタフェース．

また，ボードメンバー企業であることから可能な役割として，ドコモは複数の作業部会の設立に貢献するとともに，座長・共同座長を務め，リーダーシップを発揮している．また，ボード内に設置されている複数の委員会（Board Committees）で委員も務めている．そして，ボードメンバー企業の代表者から選出された7名のメンバーで構成される執行評議会メンバーの一員としても2019年から推挙され，大切な役割を果たしている．

さらに，特筆すべきは，FIDO認証の特長を積極的に活かしたドコモにおける導入と，さまざまなチャネルを通じたFIDOエコシステム[*8]へのフィードバックと考える．

3.1 座長・共同座長を務める作業部会での貢献

⑴コンシューマー・デプロイメント作業部会（Consumer Deployment WG）

ドコモは，FIDOアライアンスに加入後2度めのボード会議（2015年6月）にて，ドコモにおけるFIDO導入事例の紹介とそれを通じて認識した主な課題に関するプレゼンテーションを行った．その結果，FIDO認証をより広く導入推進していくための作業部会の設置について機運が高まり，FIDOアライアンスにとって初めてのAdoption WGとなるD@S WG（Deployment-at-Scale WG）の設置を提案し，ボード会議での議論と承認の結果，起案者のドコモが座長を務めることになった．

設置当初においては，FIDO認証の導入事例がまだ少なく，並行して検討が進む当時のFIDO2の将来性を支持しつつ，認証モデルは同一ながらも，異なる複数のFIDO仕様間の差異とは独立する課題の解決とFIDO UAF・U2Fのさらなる展開の可能性を模索した．その1つとして，D@S WG座長として，韓国で進みつつあった導入事例をホワイトペーパーとしてまとめる作業を推進した［6］．また，のちに国内大手銀行でFIDO認証の採用につながる活動を行った．さらに，前述したFIDO UAF 1.1の基礎となる考えをまとめ，FIDOアライアンスのボードメンバーでもあるパートナー企業とともにホワイトペーパーを執筆し，公開した［7］．

こうした活動を通じて，現在では一般消費者向け，法人ビジネス向け，そして政府系機関向けにそれぞれ作業部会を分化して活動することがより効果的との段階に至り，ドコモはコンシューマー・デプロイメント作業部会での活動に注力している．

・アカウントリカバリー

近年取り組んでいるテーマの1つに，アカウントリカバリーと呼ばれる課題がある．これは，ユーザが認証器を紛失したとき，「共有の秘密」をもたない条件下で，どのように新しい認証器に秘密鍵を再設定することができるのかという課題である．

この課題に対してドコモは，dアカウントのFIDO生体認証の導入に際して，電気通信（携帯電話）事業者として，携帯電話不正利用防止法への順守などのため従前から保持していた「本人確認」に必要な事業基盤を活用し，初期設定と端末紛失時の対応を当初から確保している．また，dアカウント パスワードレス認証においてもその基盤を活用している．しかし，ドコモとして回線契約の有無にかかわらない「会員基盤」を軸とした事業運営を推進するにあたり，回線契約の無いお客様に対しても適切なアカウントリカバリーの手段を提供することが重要であり，業界とFIDOエコシステム共通の課題として，解決に向けて取り組んでいる．

ドコモはコンシューマー・デプロイメント作業部会での活動を通じて，アカウントリカバリーに関するホワイトペーパーのとりまとめで貢献し，引き続き活動をリードしている．

⑵セキュリティ・プライバシー要件作業部会（Security and Privacy Requirements WG）

セキュリティ・プライバシー要件作業部会は，ク

＊8 エコシステム：複数の企業が連携して，お互いの技術や資産を活かし，社会を巻き込んで，技術開発から導入へと普及にいたる一連の流れを形作る共存共栄の仕組み．

レジットカード事業を営むボードメンバー企業の提案でセキュリティ要件作業部会として発足し，共同座長にプラットフォームチップセットベンダのセキュリティ専門家が加わって運営されてきた．

ドコモは，dアカウント FIDO認証の提供開始当初からドコモ スマートフォン（Android）における生体情報と秘密鍵の格納および生体情報の照合動作に端末上の安全な特別領域，例えばTEE（Trusted Execution Environment）を活用し，プライバシー情報の漏洩対策を重視した実装を要件化していた．この要件には，生体センサから安全な特別領域までの生体情報の伝送に関することも含まれる．

そのため，FIDOアライアンスにおけるセキュリティとプライバシー保護に関する認定プログラム強化に向けた正式な要件化に際しては，その経験を積極的にフィードバックした．そして，関係者で議論を深め，現在の6段階に分類されたセキュリティ要件の骨子が固まった．

なお，2018年7月から2020年3月までは，ドコモが共同座長としてそのファシリテーションでも貢献した．

⑶日本作業部会（FIDO Japan WG）

2015年に日本でFIDOアライアンスに参画する企業が集まり，FIDOアライアンスとしてのFIDO認証の普及活動を開始した．翌年の2016年12月には，FIDOアライアンスのミッションである，「パスワードに代わるシンプルで堅牢なFIDO認証モデルの展開・推進」を日本国内でより効果的に実践することをミッションとして，11社で日本作業部会を発足することを発表した．現在では45社が参加し，FIDOアライアンスで最も多くのメンバーが参加する作業部会となっている．

ドコモは発足時から座長を務めており，国内におけるFIDO認証のプレゼンス向上と普及に微力ながら貢献している．国内に事業拠点をもつ国内外のFIDOアライアンスメンバー企業ならびに関係者の方々の多くのご協力によって活動を推進できており，グローバルなアライアンスにおいて日本から世界に向けて貢献する1つのかたちとして成り立ちつつある．ご協力をいただいているすべての方々にこの場を借りて深くお礼を申し上げたい．

なお，日本作業部会としての活動とその成果は，プレスリリースや発表資料で公開しており，発足以来，毎年記者説明会・記者発表会の開催を通じて多く記事にしていただいているので，ここではその活動の詳細は，割愛する［8］［9］．

3.2 FIDO認証を活用しての貢献

FIDOアライアンスにおける活動を通じての貢献に加えて，ドコモでは端末からサービスまでトータルでFIDO認証の特長を積極的に活用し，その経験をフィードバックすることでFIDOアライアンスとそのエコシステムに貢献している．

⑴さまざまな生体センサの活用

ドコモにおいて，FIDO認証を採用したきっかけの1つは，お客様により魅力的な端末を提案するところにあった．当時，ドコモではdアカウント（当時のdocomo ID）以外にも多くのパスワードをお客様にご利用いただいており，より便利な認証手段として生体認証について検討を進めていた．そのような中，世界初の虹彩認証搭載スマートフォンARROWS NX（F-04G）（製造：富士通株式会社）を含む2015年夏モデルの企画において，FIDO認証はユーザ検証のための生体センサの種類を問わないという特長を活かし，メーカ・機種ごとに異なる種類の生体センサを搭載することができた．なお，搭載にあたっては，生体センサに求める性能とセキュリティ＆プライバシー保護の要件定義とその実現，そして継続性の確保には万全を期した．

その後，複数の端末メーカから装置として虹彩・指紋と複数のセンサを搭載可能なスマートフォンの提案を受け，FIDO UAF仕様を改めて振り返り，

その解釈と実装上の工夫により，ドコモとして新しいdアカウント設定アプリを開発し，お客様が意識することなく虹彩と指紋のどちらでも認証できる機能の提供も行った．

⑵オープンな標準技術であることの活用

オープンな標準技術である特長を活かし，異なる認証器の実装を受け入れた．これにより，（FIDO UAF 1.1に移行する前の）FIDO UAF 1.0準拠のドコモ スマートフォン（Android）全36機種を製造した7メーカで5つの異なる実装に分かれたが，いずれもFIDO認定を取得することにより相互運用性があることを確認しており，機能・サービス提供上も問題は発生していない．もちろん，その後のFIDO UAF 1.1に基づく実装においても相互運用性を確保している．今後導入予定のFIDO2についても，問題ないものと考えている．

⑶ID連携との親和性の良さの活用

FIDO認証は，OpenID® Connect*9などのID連携技術と親和性が良い．そこで，ドコモではdアカウントのOpenID Connect対応により，ドコモのパートナー企業におけるIDと連携し，パートナー企業が提供するサービスサイトへのログインなどにおいても，dアカウント FIDO生体認証が利用可能となっている．

⑷「共有の秘密」に依存しない認証方式の最大活用

ドコモとしてFIDO認証の採用当初からその実現を構想していたのが，FIDO認証への全面的な移行を見据えた機能提供である［2］．すなわち，dアカウントパスワードレス認証は「共有の秘密」に依存しないFIDO認証方式の特長を最大限に活用するものである．詳細は本特集の別記事を参照されたい［3］．

4. 国内外におけるFIDO認証の導入状況と広がり

dアカウント FIDO生体認証の提供開始は，通信事業者として，また虹彩認証を含む複数のメーカによるFIDO認定端末によるものとして世界初であった．当時は，FIDO認証が商用導入された事例は世界的にみても，FIDO UAF 1.0に先立つFIDO Ready仕様*10に基づくSamsungとPayPalによる事例などに限られ，決して多くはなかった．しかし，現在では国内外を問わず，広くFIDO認証が使われるようになってきている．

4.1 国内におけるFIDO認証の導入状況

国内では，2017年10月の大手銀行におけるFIDO認証による生体認証でのログイン機能提供開始をきっかけとして，金融機関，通信事業者，インターネットサービス事業者，そしてエンタープライズ向けと，FIDO認証の実際の活用が急速に増えている．

具体的には，FIDO UAFについてはその利用・提供開始時期の順にNTTデータ（社内向けモバイルアプリ），みずほ銀行，ソフトバンク，三菱UFJ銀行，アフラック，NTTコミュニケーションズ（SSO（Single Sign On）サービス*11），テプコシステムズ（社内向けシステム），ゆうちょ銀行などに導入された事例がある．また，FIDO2についてはヤフー（Yahoo! JAPAN ID），インターナショナルシステムリサーチ（SSOサービス），LINE Payなどに導入された事例がある．その他，FIDO U2Fの活用事例も含めると，国内でFIDO認証が実際に活用されている事例は多数に及ぶ．

これらの中には，FIDO2の活用で世界初の事例も複数含まれ，日本はFIDOエコシステムの発展でリーダーシップを発揮している国と地域の1つと言える．

4.2 海外におけるFIDO認証の導入状況

海外では，ドコモのFIDO認証提供開始からまもなく北米でBank of AmericaがFIDO UAFを活用したサービスを提供開始した．ドコモとBank of Americaは早い時期からAndroidとiOS*12の両方に

*9 OpenID® Connect：OpenID Foundationが策定するID連携のためのプロトコル．OpenIDはOpenID Foundationの商標または登録商標．

*10 FIDO Ready仕様：FIDO UAF 1.0が公開される前に，FIDO認証の先行商用を可能とするために策定された仕様．

*11 SSOサービス：あらかじめID連携しておくことで，あるIDにログインすることで複数のIDにログインできるサービス．

対応したFIDOアライアンスのボードメンバー企業である．また，韓国ではFIDO Korea WGの共同座長を務めるSamsung，BC Cardらがリーダーシップを発揮し，日本と同様に早い時期からFIDO認証が広く使われてきた．

⑴北　米

Google社内で，FIDO認証に基づくTitan Security Keyを活用することで不正ログインを防止できたことが広く知られるようになった．

また，先ごろ，米Intuit社がSMS OTP（One Time Password）＊13からFIDO認証に移行したことによる効果をFIDOアライアンスメンバーとしてケーススタディとして発表した［10］．これによれば，FIDO認証はユーザ体験の観点からログインに掛かる時間を約20％にまで短縮し，認証の成功率の改善も図っている．

さらに，米国連邦調達庁（GSA：General Services Administration），すなわち米国の公務員，連邦政府職員向けのSSOサービスのためのWebサイトがWindows Hello＊14とセキュリティキーを使ったFIDO認証に対応したとのことである．

このように，北米でFIDO認証の利用シーンが広がっている．

⑵欧　州

欧州では，欧州一般データ保護規則（GDPR：General Data Protection Regulation）＊15が施行された．GDPRにおいて，生体情報はもっとも高レベルなプライバシー情報であるため，生体情報を認証器の安全な領域に格納するFIDO認証に期待がある．また，金融・決済の領域で近く施行されるとみられる欧州決済サービス指令（PSD2：Payment Services Directive II）＊16で2要素認証が必須となり，その対応でFIDO認証の採用が検討されている．

一方，英国の国民保健サービス（NHS：National Health Service）で，開発者がアプリのログインにFIDO生体認証を使えるようにするためのオープンソースをリリースしたとのニュースもある．

欧州で，FIDO認証の利用に期待が高まっている．

⑶アジア・パシフィック

アジア・パシフィックは，世界の中でもFIDO認証の活用が先行している地域であり，日本と並び，韓国と台湾でFIDO認証が広く利用されている．

韓国では，銀行などの金融機関で広くFIDO認証が使われている他，国民IDに対応するK-FIDO［6］の対応により，さまざまなシーンでFIDO認証が使われている．また，台湾ではPKI（Public Key Infrastructure）＊17ベースのMOICAと呼ばれる市民IDにTAIWAN FidOとしてFIDO認証に対応した．

FIDOアライアンスはAPKIC（Asia PKI Consortium）とリエゾンパートナーとして連携もしており，アジア・パシフィックでは国民・市民IDへのFIDO認証の対応事例が特徴的である．

5. あとがき

本稿では，FIDOアライアンスとFIDO認証について解説し，ドコモの貢献と国内外におけるFIDO認証の広がりを紹介した．

ドコモにおけるFIDO認証の取組みの第一歩は，米Nok Nok Labs社との2014年6月のシリコンバレーでの打合せにさかのぼる．Nok Nok Labsは，FIDOアライアンスの創設メンバー6社のうちの1社である．ドコモは，dアカウント FIDO認証の提供開始当初からFIDO認証サーバの提供を受けており，2015年5月の運用開始以来一度も障害なく運転を続けている．

パスワード課題はデジタルトランスフォーメーション＊18時代において解決すべき社会的な問題の1つであり，ドコモ1社のみで解決できることではない．「共有の秘密」に依存しない認証方式を提唱するFIDOアライアンスは，Nok Nok Labsのような認証とセキュリティ技術に特化した企業も，Google

＊12 iOS：「IOS」は米国およびその他の国におけるCisco社の商標または登録商標であり，ライセンスに基づき使用されている．

＊13 SMS OTP：SMS（ショートメッセージサービス）で配信されるワンタイムパスワード．

＊14 Windows Hello：米国Microsoft Corp．の米国およびその他の国における登録商標または商標．

＊15 欧州一般データ保護規則（GDPR）：EU加盟国および欧州経済領域で適用される個人情報の取扱いに関する保護規則．個人情報の取得や移動にも適用される．

＊16 欧州決済サービス指令（PSD2）：EU域内における安全で便利な電子決済を実現するための規則．インターネットやモバイルでの新しい決済サービスが考慮されている．

やMicrosoftのような大手のOS・プラットフォーム企業も集まる，企業の規模を問わず，ビジネス領域の垣根を超えて，まさにダイバーシティ＆インクルージョンを体現する業界の連携であり，ドコモがその中で役割の一端を微力ながらも担うことができていることは望外の喜びである．

引き続き，ドコモにおけるdアカウント パスワードレス認証の取組みを進めながら，FIDO認証とそのエコシステムの発展に貢献できればと考えている．

文　献

［1］ FIDOアライアンス ホームページ．
https://fidoalliance.org/

［2］ 森山 光一：“パスワードのいらない世界へ：NTTドコモにおけるFIDO（ファイド）標準を活用したdアカウント生体認証の取組みと将来展望，” 電気通信，Vol.80，No.840，pp.13-19，Jan. 2017.

［3］ 尾崎，ほか：“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，” 本誌，Vol.28，No.1，pp.11-21，Apr. 2020.

［4］ W3C Recommendation：“Web Authentication：An API for accessing Public Key Credentials Level 1,” Mar. 2019.
https://www.w3.org/TR/webauthn/

［5］ 松浦 由美子，田中 清，藤村 滋，森山 光一：“W3C TPAC2019@FUKUOKAでの活動，” NTT技術ジャーナル，Vol.32，No.1，pp.72-74，Jan. 2020.

［6］ FIDO Alliance：“FIDO Alliance White Paper：Korean FIDO Deployment Case Study Accredited Certification System for Safe Usage of Accredited Certificate using FIDO in Smartphone in Korea (K-FIDO),” Sep. 2017.
https://fidoalliance.org/white-paper-korean-fido-deployment-case-study-accredited-certification-system-for-safe-usage-of-accredited-certificate-using-fido-in-smartphone-in-korea-k-fido/

［7］ FIDO Alliance：“FIDO Alliance White Paper：Hardware-backed Keystore Authenticators (HKA) on Android 8.0 or Later Mobile Devices,” Jun. 2018.
https://fidoalliance.org/white-paper-hardware-backed-keystore-authenticators-hka-on-android-8-0-or-later-mobile-devices/

［8］ FIDOアライアンス：“パスワードに代わる新たなオンライン認証を推進するFIDO（ファイド）アライアンスの記者説明会，” Jul. 2019.
https://fidoalliance.org/パスワードに代わる新たなオンライン認証を推進/?lang=ja

［9］ FIDOアライアンス：“パスワードに代わる新たなオンライン認証を推進するFIDO（ファイド）アライアンスの記者発表会，” Dec. 2019.
https://fidoalliance.org/パスワードに代わる新たなオンライン認証を推進-2/?lang=ja

［10］ FIDO Alliance：“The Right Mix：Intuit’s Journey with FIDO Authentication,” Oct. 2019.
https://fidoalliance.org/the-right-mix-intuits-journey-with-fido-authentication/

＊17 PKI：公開鍵暗号方式で用いる公開鍵の所有者を保証し，安全な通信を行うようにするための基盤．

＊18 デジタルトランスフォーメーション：IT技術を活用してサービスやビジネスモデルを変革させ，事業を促進するとともに人々の生活をあらゆる面で良い方向に変化させること．