Technology Reports（特集）

生体認証　セキュリティ　FIDO認証

パスワード課題を解決するFIDO（ファイド）認証特集

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

プロダクト部　尾崎 友彦　上坂 浩貴　牧野 由樹子　富山 由希子　森山 光一

近年，フィッシングなどで奪取されたパスワードを用いた不正アクセスが問題となっている．また，類推しにくい複雑なパスワードを覚えなければならないなどパスワード管理にも煩わしさがある．このようなパスワード認証の課題を解決しつつ，セキュリティと利便性を両立するため，ドコモは2020年3月にFIDO®*1認証を活用したdアカウント®*2 パスワードレス認証の提供を開始した．スマートフォンの生体認証などを利用し，パスワードを無効化して不要とすることで，利便性を確保しつつ，dアカウントの不正利用を防止する．

1. まえがき

近年，インターネットサービスへのログインや，ネットショッピングにおける決済など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，第三者による不正アクセスや不正決済などのニュースが後を絶たない．特に最近では，巧妙なフィッシングサイト*3でパスワードを奪取し，それらを悪用した不正アクセスが増加している．

ドコモは，スマートフォンやPCなどからdポイントの確認やdマーケット®*4などドコモのサービスを利用する際の共通IDとしてdアカウントを提供しており，ドコモ回線のユーザだけではなく，ドコモ回線以外のユーザにも広く利用されている．このdアカウントのログインや決済時の本人確認などのシーンにおいて，ドコモは2015年からシンプルで堅牢なオンライン認証を可能にするオープンな標準規格，FIDO（Fast IDentity Online）（ファイド）認証を活用したdアカウント生体認証を提供してきた［1］．パスワード入力の代わりにスマートフォンの生体センサに指紋や虹彩をかざすだけのシンプルな動作で認証を可能とし，dアカウント認証の利便性向上を

©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 Allianceの商標または登録商標．
＊2　dアカウント®：㈱NTTドコモの登録商標．
＊3　フィッシングサイト：実在する企業などの公式サイトとそっくりな偽サイト．巧みにIDやパスワードなどの個人情報を入力させて奪取する．
＊4　dマーケット®：㈱NTTドコモの登録商標．

行ったものである．しかし，パスワード認証をユーザが選択できる限り，パスワードを取り巻くセキュリティ課題を常にもち続けることとなる．そのため，FIDO認証導入当初から，将来的にはパスワードを無くすことでdアカウント認証をよりセキュアにすることを構想していた．

今回，dアカウントFIDO生体認証の十分な普及を背景として，パスワード認証をいよいよ無効にする機能を開発し，全面的にFIDO認証に移行可能なオプション機能の提供を開始した．これによりパスワードに起因したdアカウントへの不正アクセスを防止することができる．

本稿では，まずdアカウント パスワードレス認証のベースとなるdアカウント FIDO生体認証の概要について述べる．次にパスワードレス認証の実現にあたっての課題，設計・開発と導入の詳細について解説する．そして，今後の展望について述べる．

2. dアカウント FIDO生体認証の導入背景と概要

ドコモは，スマートフォンやタブレットからユーザがもっと便利にログインしてサービスを使えるようにするため，「あんしんをもっと便利に」をキャッチフレーズとして，2015年5月にdアカウントFIDO生体認証を導入した．ドコモ回線のユーザには，dアカウント（旧docomo ID）とそのパスワードに加えて，spモードパスワードとネットワーク暗証番号（いずれも数字4桁）を提供しており，それらをまとめる便利な認証手段として生体認証の機能を積極的に展開することとした．

生体認証を導入するにあたり，FIDO認証に着目した理由の1つは，ユーザと認証器（例えばスマートフォン）の間の本人照合の部分と，公開鍵暗号方式を活用した認証器とサーバ間の検証部分が完全に分離されていることである．これにより，スマートフォンそれぞれの機種の特徴にあった生体センサを搭載でき，異なる種類の指紋センサを搭載した複数のスマートフォンと世界初の虹彩認証スマートフォンを対象として，dアカウント FIDO生体認証の同時提供を開始するなど，端末ラインアップの魅力を高めることができた．また，機種ごとに生体センサが異なっていても認証サーバ側の個別対応を不要にできた．

そして，FIDO認証に着目したもう1つの大きな理由は，セキュリティにおける優位性である．FIDO認証では，オンライン上に生体情報やパスワードのような秘密情報を流さないため，フィッシング耐性がある．そのため，dアカウント FIDO生体認証を提供開始した当初から，将来的にはパスワード認証を無くし，FIDO認証の特長を活かしてセキュリティ強化につなげたいという構想をもっていた［1］．

一方，提供開始当初はFIDO生体認証対応スマートフォン4機種でスタートしており，多くのサービス・アプリを継続的に提供する必要性から，従来のパスワード認証も併存させる必要があった．生体センサが反応しなかった場合などへの考慮もあった．

2.1 FIDO UAFの採用とアーキテクチャ

dアカウント FIDO生体認証の当初の導入にあたっては，2014年12月に正式に仕様が公開されたFIDO UAF（Universal Authenticator Framework）1.0[*5]を採用した．そして，すでに商用導入していたdアカウント認証サーバと端末のdアカウント設定アプリに対してFIDO UAF 1.0の追加対応を行った．

dアカウント設定アプリは，ドコモのさまざまなサービスからの認証要求に対して一元的に処理を行うアプリである．ドコモのサービスはWebで提供しているもの，ネイティブアプリで提供しているものがあり，合わせて100以上存在する．そして，それらのサービス・アプリを原則としてdアカウント設定アプリと連携させることで，dアカウント認証

＊5 FIDO UAF 1.0：パスワードレス認証のためにデザインされた仕様．2014年12月に策定された．

サーバとの結合インタフェースをシングルポイントにしている．

このdアカウント設定アプリにFIDO UAF 1.0クライアントを内包し，端末メーカにてFIDO認証器として必要な要件を実装することで，dアカウントへのFIDO認証の導入をスムーズに実現することができた．

2.2 dアカウントFIDO生体認証における本人確認方法

dアカウント FIDO生体認証では，ドコモ回線のユーザがスマートフォンなど生体センサを具備する端末をFIDO認証器として設定する際，ネットワーク暗証番号の入力を必須とすることでオンライン認証に使われる生体情報がdアカウント認証の対象である本人のものであることを担保した．すなわち，本人確認できた場合にのみFIDO認証を設定させることで，本人確認の結果をFIDO認証器に括り付けることができる．

⑴ネットワーク暗証番号と本人確認

ネットワーク暗証番号とは，ドコモショップやドコモオンライン手続きでのご注文受付時などにユーザが入力する数字4桁の番号である．

ドコモでは，電気通信事業者として携帯電話不正利用防止法順守のため，従前から回線契約時などの本人確認に必要な事業基盤を確保している．1つはドコモショップなど店頭における対面での身分証明書の提示を受けての本人確認，1つは本人確認書類に記載された住居に，携帯電話などを転送不要郵便や特定事項伝達型本人限定受取郵便などで送付することによる本人確認，そしてもう1つが回線契約時に発行するネットワーク暗証番号による本人確認である．

ネットワーク暗証番号で本人確認を行うには，回線契約済みのSIM（Subscriber Identity Module）[*6]カードを挿入してドコモ回線に接続した端末において4桁の番号を入力する．SIMカードは個体として唯一性があり，かつ契約していないと回線接続できないため，それ自体が強力な所持認証（回線認証）である．また，このとき入力された4桁の番号はインターネットを流れない．すなわち，ネットワーク暗証番号は，一般のオンラインパスワードと異なり，回線認証と契約者本人のみが記憶する知識による認証を組み合わせた強力な多要素認証で，堅牢性の高いオンラインでの本人確認手段である．

⑵キャリアフリーのdアカウント FIDO生体認証

dアカウントはドコモの回線以外のユーザでも利用可能（キャリアフリー）だが，ネットワーク暗証番号は利用できない．そのためFIDO生体認証の設定においては，認証器である端末の画面ロックを必須とし，第三者がその端末を使用できないことを前提に，dアカウントのパスワード入力が必要な設計とした．

2.3 スマホ認証

dアカウント FIDO生体認証を発表したとき，「あんしんをもっと便利に」と合わせて将来構想として発表したのが「スマホが暮らしの鍵になる」である．すなわち，生体センサを具備しない周辺デバイスで提供するサービスを使う場合の認証においても，生体認証対応スマートフォンを使って安心・便利に認証していただきたいという構想である．

当時のPCは現在と比較して，生体センサを具備しているものは大変少なかった．また，テレビやセットトップボックスにリモコンでカーソルを何度も移動させてパスワードを毎回入力するのは面倒である．2017年1月に提供開始したスマホ認証では，あらかじめPCやセットトップボックスなどの周辺デバイスを登録しておくことで，それらのデバイスで提供するサービス・アプリにおいて「スマホで認証」ボタンを選択するだけで，パスワードを入力することなく，dアカウント FIDO生体認証対応のスマートフォンで簡単に認証することができる．

＊6 SIM：携帯電話会社と契約した電話番号などを記録しているICカード．

2.4 対応機種の拡大

dアカウント認証における「あんしんをもっと便利に」をより多くのユーザに提供するため，dアカウントFIDO生体認証の提供開始以降，対応機種の速やかな拡大を図った．

まず，いち早くiOS*7に対応する取組みを行った．iPhone®*8・iPadでは，すでにTouch IDを搭載している機種が普及し始めていたことから，2016年3月からTouch ID搭載機種への対応を行った［2］．また，2017年12月からFace ID搭載機種へも正式対応を開始した．

さらに，Android™*9においてもさらなる対応機種増に向けた取組みを行った．当初は，端末メーカへのFIDO UAF 1.0対応について積極的な働きかけを行った．また，ドコモがFIDOアライアンスに加入してから［3］並行して，FIDO UAF対応端末が普及するための仕組みづくりとその採用を推進した［4］．すなわち，Android OSの新しい機能を活用することで，端末メーカがFIDO認証器として必要な要件を実装するためにAndroid OSを特別にカスタマイズする必要がないFIDO UAF 1.1*10［5］の仕様化で貢献し，2017年11月から対応端末を提供開始した［6］．これにより端末メーカの開発負担を低減でき，dアカウント FIDO生体認証対応機種の継続的な提供を確実にした．

結果として，2019年末時点で，FIDO生体認証対応機種はAndroid，iOS搭載端末合計で93機種にまで広がっている（Android FIDO UAF 1.0：36機種，Android FIDO UAF 1.1：32機種，iOS：25機種）．

3. dアカウント パスワードレス認証の実現に向けた課題

ドコモが販売するほぼすべてのスマートフォンとタブレットで，dアカウント FIDO生体認証が利用できる土台を整えることができた背景を踏まえ，dアカウントのパスワード認証を無効化し，FIDO認証に全面的に移行するパスワードレス認証の導入が現実的となった．

dアカウント パスワードレス認証により，第三者によるパスワードの不正奪取やリスト型攻撃*11などを防ぐとともに，パスワード管理の煩雑さからも解放され，安全かつ快適なオンライン認証を提供することができる．しかし，パスワードレス認証の実現に向けては，下記のような検討すべき多くの課題があった．

・パスワードレス認証への移行方法
・生体認証の代替手段
・アカウント再設定と端末紛失時などの復旧手段の提供
・多様なデバイスへの対応
・多数のドコモサービス・アプリへの影響

⑴パスワードレス認証への移行方法

セキュリティを考慮すると，すべてのユーザがパスワードレス認証を利用することが望ましい．しかし，日々使い慣れたパスワードが使えなくなったときのユーザへの影響やサービスの継続性などを踏まえて，移行可能な対象範囲と移行方法を丁寧に検討する必要があった．

⑵生体認証の代替手段

パスワードが無効化されると，指の怪我などで生体センサが利用できない場合の代替手段として従来のパスワード認証が利用できないため，これに代わる手段を確保する必要があった．また，生体認証対応端末を持っていても生体センサを利用しないユーザが約3割いるため（ドコモ調べ），そのようなユーザもパスワードレス認証を利用できる手段を検討する必要があった．

⑶アカウント再設定と端末紛失時などの復旧手段の提供

パスワードを無効化した後に機種変更をするときの再設定や，端末紛失・故障した場合のFIDO認証

＊7 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．
＊8 iPhone®：「iPhone」「iPad」はApple Inc．の商標．ただし，「iPhone」商標は日本国内では，アイホン株式会社のライセンスに基づき使用されている．
＊9 Android™：Google LLCの商標または登録商標．
＊10 FIDO UAF 1.1：FIDO UAF 1.0の拡張版で2016年12月に策定された．「キーの構成証明機能（Key Attestation）」を利用可能で，これにより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・搭載が可能となる．
＊11 リスト型攻撃：不正に入手したIDとパスワードの一覧を用い，アカウントへの不正アクセスを試みる攻撃手法．

器としての端末の復旧について，ユーザや応対部門にも分かりやすい手段を提供する必要があった．

⑷多様なデバイスへの対応

生体センサを具備しないPCやセットトップボックスなどのデバイスや，2台目のスマートフォンなどからログインや認証を利用するシーンも想定されるため，それらのデバイスからパスワードレス認証を使ってもらうための手段の検討が必要であった．

⑸多数のドコモサービス・アプリへの影響

現在，dアカウントを利用しているすべてのサービス・アプリがFIDO生体認証に対応しているわけではない．また，店頭などの装置でdアカウントのIDとパスワードを入力することを求めるサービスや，dアカウント設定アプリとシングルポイントで連携していないサービス・アプリも存在する．そのため，パスワードを無効化した場合のあらゆる場面での影響を考慮し，認証手段の提供を確保する必要があった．

4. 設計・開発と導入

dアカウント パスワードレス認証の実現にあたっては，セキュリティ強化を目的とし，前述した複数の課題を解決しながら，利便性を損なわず，ユーザが簡単に利用できることを念頭に設計した．

4.1 全体構想とアーキテクチャ

dアカウント パスワードレス認証は，dアカウントFIDO生体認証のアーキテクチャをベースとして実現することとした．dアカウント設定アプリに新たな設定項目の1つとして，dアカウントのパスワードを無効化できる機能を設ける．ユーザがこの機能を選択することで，dアカウントのオンラインパスワードをサーバ側で一切無効化する．また，合わせてdアカウント設定アプリと連携するサービス・アプリのdアカウント認証画面のすべてでパスワード入力欄を削除することでパスワードレス認証を実現する（**図1**）．

図1　パスワードレス認証の概要

dアカウント パスワードレス認証は，最初はドコモ回線のユーザを対象にスタートした．ドコモ回線のユーザはネットワーク暗証番号が利用できるため，本人確認した結果をFIDO認証器（スマートフォンなど）に括り付けることができる．パスワード認証を無効化することで，適切に設定されたFIDO認証器のみを使ってパスワードレスでのログインや本人確認のためのオンライン認証ができることになるため，パスワードを取り巻くセキュリティ課題を解決できる．

4.2 パスワードレス認証への移行設定

セキュリティ強化という目的を考慮すると，できるだけ多くのユーザがパスワードの無効化の設定をすることが望ましい．一方，日々使い慣れたパスワードが使えなくなったときのユーザの懸念を考慮し，まずはオプション機能としてオプトイン*12で提供を開始した．

dアカウント パスワードレス認証へ移行するには，dアカウント FIDO生体認証対応機種にプリインストールしてあるdアカウント設定アプリをバージョンアップし，新たに設けたメニュー「パスワード無効化設定」からユーザ自身の操作によってパスワードの無効化をONに設定する．

その際，すでにdアカウント 生体認証を設定しているユーザについては，「パスワード無効化設定」をONにする際に1回だけ生体認証を行えば完了するようにした．また，生体認証を設定していないユーザについては，ネットワーク暗証番号の入力で設定を完了するようにした．このように簡単な操作でdアカウントのパスワードを無効化することができる（**図2**）．

なお，必要に応じてパスワードの無効化をOFFに戻すときには，ONに設定するときと同様にdアカウント設定アプリから切替え可能な仕様とした．

図2　dアカウント設定アプリの「パスワード無効化設定」と設定時の画面遷移

*12 オプトイン：ユーザの選択により利用や設定を許可すること．

4.3 生体認証が使えない場合への対応

⑴画面ロック解除の活用

生体認証対応端末を持っていても生体センサを利用しないユーザがいること，また指の怪我などで生体センサが利用できない場合を考慮し，生体以外の手段でもパスワードレス認証の実現を検討する必要があった．FIDO認証の特徴はユーザと認証器（スマートフォンなど）の間の本人照合の部分と，公開鍵暗号方式を活用した認証器とサーバ間の検証部分が完全に分離していることである．つまり，FIDO認証器ローカルでの本人照合には生体認証に加えて，本人のみがもつ知識，例えば端末の画面ロック解除で使われるローカルPINなどもFIDO認証に活用することができる．

幸い近年のスマートフォンOSでは端末の画面ロック解除は端末の所有者のみが知る情報としてセキュアに実装されており，かつアプリケーションからも活用可能である．そこで，dアカウント パスワードレス認証では生体認証に加えて，画面ロック解除のためのローカルなPIN／パスコード／パターンでもdアカウントのログインや決済時の本人確認をできるようにする．

なお，dアカウント パスワードレス認証は，前述したようにドコモ回線のユーザへの対応から始めるため，生体認証ができない場合の代替手段としてネットワーク暗証番号を入力して本人確認を行うこともできる．こうした状況から，画面ロック解除によるdアカウント パスワードレス認証は段階的に提供を開始する方針とした．

⑵FIDO UAFからFIDO2[*13]［7］への移行

画面ロック解除を活用した認証を実現するため，Android OS端末向けに提供しているdアカウント設定アプリは，FIDO UAF 1.1からFIDO2へ移行することとした．Android OS 7.0以降のバージョンで標準的に利用できるようになったFIDO2の実装を活用することで，端末の画面ロック解除で用いるローカルなPIN／パスコード／パターンを本人照合の手段として利用することが可能となる（**図3**）．また

図3　画面ロック解除を用いたdアカウント パスワードレス認証（Android OS端末におけるFIDO2の活用事例）

＊13 FIDO2：FIDO認証のさらなる普及のため，FIDO認証モデルをプラットフォーム対応させた仕様群．FIDOアライアンスとして策定した機器間連携仕様（CTAP：Client to Authenticator Protocol）とFIDOアライアンスが提案し，W3Cとして策定したWeb認証APIで構成されている．Web認証APIの最初のバージョンは2019年3月に正式に勧告化された．

将来，ドコモの回線契約を持っていないユーザに対しdアカウント パスワードレス認証を提供する場合にも，より多くの端末でFIDO認証が提供可能になる．

Android OSの画面ロック解除でdアカウントによるログインや本人確認をするためには，dアカウント設定アプリをバージョンアップし，FIDO UAF 1.1からFIDO2へ移行する．

移行の操作は単純で，dアカウント認証の動線の1画面で，生体認証に加えて画面ロック解除でもdアカウント認証が可能になることを案内した上で，FIDO2への登録のための操作として指紋センサなどにタッチする．つまり，ユーザはFIDO仕様の違いを意識する必要がない（**図4**）．本機能は2020年5月以降，提供開始予定である．

なお，端末メーカにFIDO認証器として必要な要件を実装するためにAndroid OSを特別にカスタマイズする必要があったFIDO UAF 1.0対応端末については，FIDO2への移行対象外とした．

4.4 アカウント再設定と端末紛失時の復旧手段

機種変更をする場合，新しい端末でdアカウントの再設定が必要になる．dアカウント パスワードレス認証を設定済みのユーザはパスワードが無効化された状態であるが，設定のときと同様にネットワーク暗証番号を利用して本人確認を行うことで，再設定を完了することができる．

端末を紛失した場合には，dアカウント FIDO生体認証でも実績がある通り，ドコモの端末紛失時の手続きに従う．すなわち，SIMカードを再発行して新たな端末を準備すれば，上記の再設定と同様にネットワーク暗証番号で本人確認を行ってdアカウントパスワードレス認証を再設定することで復旧できる．

なお，ユーザがドコモ回線を解約した場合には，パスワード無効化設定は自動的にOFFに戻る仕様とした．

FIDO2登録時画面
（ユーザがFIDO仕様の違いを意識する必要はない）

図4　FIDO UAF 1.1からFIDO2への移行時の画面遷移

4.5 多様なデバイスへの対応

FIDO UAFからFIDO2へ移行することにより，生体認証を使えない場合の代替手段としてだけではなく，生体センサをもたない機種でも画面ロック解除を利用することでdアカウント パスワードレス認証を利用できるようにした．

PCやテレビ，セットトップボックスなど生体センサの搭載されていないデバイスでログインするユースケースには，既述のスマホ認証の仕組みをdアカウント パスワードレス認証にも応用した．すなわち，あらかじめ設定をしておくことで，PCやセットトップボックスなどの周辺デバイスで提供するサービス・アプリでdアカウント認証ボタンを選択すると，パスワードレス認証設定済みのスマートフォンに認証要求を通知するようにした．そして，そのスマートフォンでパスワードを入力することなく，生体認証や画面ロック解除で簡単に認証することができる（**図5**）．あらかじめ必要な設定においては，第三者のなりすましによる認証要求を防ぐための工夫をしている．

パスワードレス認証（パスワード無効化）設定済みのdアカウントは，マルチデバイスでの認証にも対応する．つまり，ユーザが複数の回線を持つ場合，それらに1つのdアカウントを紐づけることができる．そのため，ユーザが所持する回線数に応じたFIDO認証器を設定可能であり，どちらの端末でもdアカウント パスワードレス認証をすることができる．

4.6 多数のドコモサービス・アプリへの対応

dアカウント パスワードレス認証の企画に際して網羅的な確認を行った結果，dアカウント設定アプリとシングルポイントで連携していないサービ

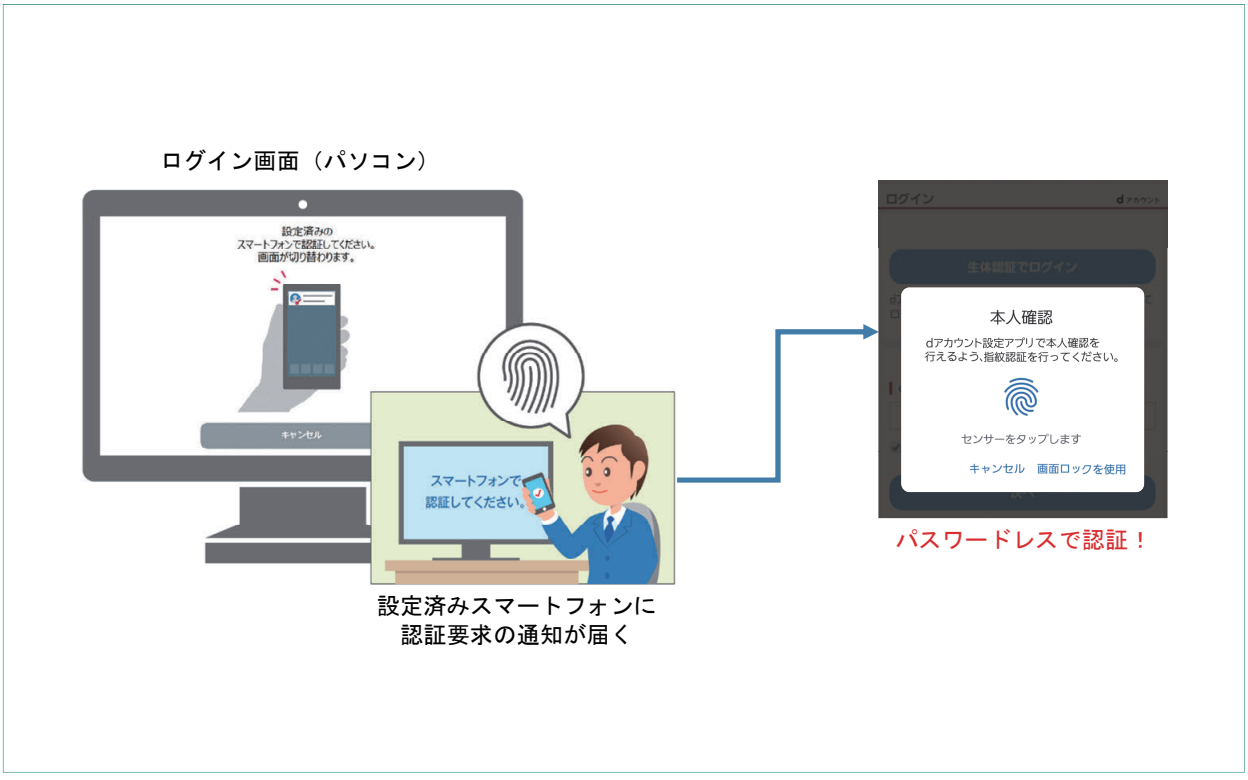

図5 パソコンからdアカウント パスワードレス認証

ス・アプリが一定数あることが分かった．この解決のため，スマホ認証の仕組みを応用した．

すなわち，それらのサービス・アプリでパスワードレス認証が必要なシーンを生体センサが搭載されていないデバイスで認証が必要なユースケースと捉える．そして，それらのサービス・アプリでdアカウント認証ボタンを選択すると，dアカウントパスワードレス認証を設定済みであるそのスマートフォンに認証要求を通知することで，スマートフォンにパスワードを入力することなく，認証することができる．

いくつかの特定の装置でdアカウントのID・パスワードを入力して認証している場面があることも分かったが，この新しいスマホ認証の仕組みで同様に解決を図った．

5. 今後の展望

今回，提供を開始したdアカウント パスワードレス認証は，FIDO認証の特長を活かしてセキュリティ強化につなげる取組みの第一歩である．

現在のdアカウント パスワードレス認証は，dアカウントをより安心して利用するためのオプション機能であり，dアカウントのパスワードが存在する状態からパスワードを無効化する仕様となっている．将来的には，dアカウントを新規作成する段階からパスワードレスとする機能を提供し，オプション機能としての提供ではなく，デフォルトでの提供も視野に入れている．

また，ドコモのサービスの多くはドコモの回線契約を持たないユーザにも提供している．このようないわゆるキャリアフリーのユーザもdアカウントをさまざまな用途で利用しているため，dアカウントパスワードレス認証のキャリアフリー対応についても検討している．

このような複数のアプローチで，より多くのユーザにあんしんでもっと便利なdアカウント パスワードレス認証を提供する取組みを継続していく予定である．

6. あとがき

本稿では，dアカウント FIDO生体認証の導入背景と概要を述べ，パスワードレス認証の実現にあたっての課題，設計・開発と導入の詳細について解説し，今後の展望について述べた．

dアカウント パスワードレス認証の導入により，ドコモはこれまで当り前であったIDとパスワードのあり方を根本から変える．既存のアセット＊14を十分に活用することで，利便性を損なうことなく，幅広いユーザがより安心してdアカウントを利用するための機能を提供開始することができた．第三者による不正アクセスや不正決済などのニュースが後を絶たない昨今，FIDO認証への注目度も年々増してきている．ドコモは今後もFIDO認証を積極的に活用した先進的な端末の提供とサービス展開を通じて，「パスワードのいらない世界」の実現をめざしていく．

文　献

[1] 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.

[2] NTTドコモ：“dアカウントログイン等のオンライン認証にTouch IDが対応．”
https://www.nttdocomo.co.jp/info/notice/pages/160307_00.html

[3] 森山，ほか：“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，”本誌，Vol.28，No.1，pp.22-32，Apr. 2020.

[4] M.Hata and R.Lindemann：“FIDO Alliance White Paper：Hardware-backed Keystore Authenticators (HKA) on Android 8.0 or Later Mobile Devices，”Jun. 2018.
https://fidoalliance.org/wp-content/uploads/Hardware-

＊14 アセット：保有する有用な資産や資材，利点のこと．

backed_Keystore_White_Paper_June2018.pdf
［5］ FIDO Alliance：“First FIDO UAF 1.1 Implementations Ease Deployment of Advanced Biometric Authentication on Android Devices,” Dec. 2017.
https://fidoalliance.org/first-fido-uaf-1-1-implementations-ease-deployment-advanced-biometric-authentication-android-devices/
［6］ FIDOアライアンス：“FIDO（ファイド）UAF 1.1の初実装が登場，Androidデバイスへの先進的生体認証の導入が容易に ～ドコモ スマートフォン Xperia™の二機種が市場初の対応デバイスに～,” Dec. 2018.
https://prtimes.jp/main/html/rd/p/000000006.000029122.html
［7］ W3C：“W3CとFIDO Alliance - パスワード不要の安全なログインが勧告化に,” Mar. 2019.
https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.ja