生体認証によるモバイルサービスのセキュリティと利便性の両立

中司 豊　池谷 亮平　手塚 由起子　天野 信一　青柳 亨　岩佐 綾香

要 旨

オンラインサービスにおける本人認証で使われているIDとパスワードでの不正アクセスがあとを絶たない状況が続くなか、NECが得意とする顔認証をはじめとする生体認証技術により「忘れない、無くさない、盗まれない」セキュアなオンライン認証を、「生体情報などの認証に必要な秘匿すべき情報」をサーバ側に送信・保持することなくモバイル端末上で実現するFIDOの取り組み、更に、FIDOとAPI-GWを活用した金融サービスの高度化について紹介します。

KeyWords

FIDO／NC7000-3A／認証／認可／ID連携／生体認証／顔認証

1. はじめに

インターネット上のオンラインサービスにおけるユーザー認証の仕組みとして、従来IDとパスワードが一般的に使われてきていますが、不正アクセスなどのセキュリティ面での課題が以前から指摘されています。特に金融機関では不正送金被害があとを絶たず、このようなパスワード認証への依存度を減らすため、生体認証技術を活用した新しいオンライン認証であるFIDO(Fast IDentity Online)が注目されています。

FIDOは2012年にFIDO Allianceが設立されて以降、強固なセキュリティと利用者の使いやすさという両面を備えた認証標準の確立というスタンスのもと、オンラインサービス利用時のパスワードレス認証の標準化を目指し、各技術仕様の策定が進められており、金融事業者、通信事業者、セキュリティベンダーなど各事業分野における大手プレイヤーが参画し、デファクト標準の仕様となりつつあります[1)]。

金融機関においても、海外においてFIDOを利用したインターネットバンキングを既に提供しているところもあり[2)]、今後は国内の金融機関においても、インターネットバンキングなどの各種コンシューマ向けサービスにおいて、生体認証の安全性と利便性を考慮したうえでFIDOの活用が進んでいくものと思われます。

本稿では、FIDO生体認証の活用による金融サービスの高度化について紹介します。

2. 生体認証活用の背景

オンラインサービスにおける本人認証ではIDとパスワードが約8割を占めるといわれており[3)]、平成27年度中のなりすましなどによる不正アクセス行為による認知件数は2,051件で、不正アクセス後の行為は「インターネットバンキングの不正送金」が認知件数の74.6%を占めてい

図1　生体認証のメリット

※顔認証・指紋認証・指ハイブリッド認証以外にも、DNA・話者・掌紋、虹彩などさまざまな生体認証技術の研究開発に取り組んでいます

図2　NECの生体認証の取り組み

ます（不正アクセス行為の発生状況（警視庁・総務省・経済産業省））。

また、IPA（オンライン本人認証方式の実態調査報告書）によると、約70%の利用者が安全なパスワードが何かを概ね知っている一方で、安全なパスワードを設定しているのは僅か13%であり、事業者側でもID・パスワード以外の認証方式の提供は約10%以下となっています。これは、認証デバイスを用いた認証は専用装置の所持が前提であることへの懸念や、パスワードポリシーを厳しくすることによるサービスの利用率の低下を危惧していることが背景にあります。

このような従来の知識認証（パスワードや暗証番号など）や所有物認証（ICカードや鍵など）に潜むセキュリティリスクを解決する手段として、**図1**に示すように生体認証が注目されています。

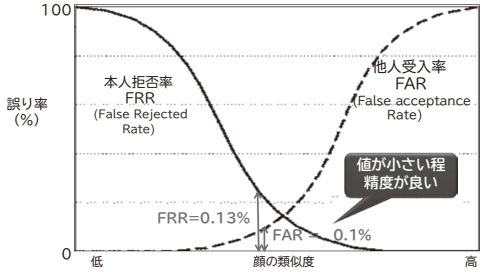
3. NECでの生体認証の取り組み

NECでは40年以上にわたり、生体認証の研究開発及びビジネスを実施してきており（**図2**）、世界一[4) 5)]の指紋認証・顔認証技術を保有しています。

一方サービスを提供するデバイスは、PCからモバイル端末（スマートフォンやタブレット）に大きく変り、モバイル端末上のアプリで認証をすることが一般的になってきています。これらモバイル端末には、カメラや指紋センサーなどが標準で具備されており、顔認証や指紋認証、更には声紋認証といった生体認証を活用することが容易になってきています。

このような背景から、サーバサイドの生体認証技術をモバイル端末へ展開することが必要であり、NECは、世界一[5)]の精度・性能を持ち、更にモバイル認証向けに改良した顔認証エンジン（**図3**）を提供します。

■FAR=　0.1% 時の FRR=0.13%, FAR=　0.01% 時の FRR=0.26%
■FAR=0.001% 時の FRR=0.64%, FAR=0.0001% 時の FRR=1.8%



* 上記は NEC 内での精度評価値です。
* 相関曲線図はイメージ図であり、モバイル向け顔認証エンジンの実データの相関曲線図ではありません。

図3　モバイル認証向け顔認証の精度見込み

4. モバイルコンシューマ向け認証の取り組み

NECでは、大手キャリアのコンシューマ向けの統合認証基盤として、NC7000-3Aシリーズでサービスを提供しており、SAML2.0/OAuth2.0/OpenID Connect/OTP(ワンタイムパスワード)/証明書認証などの各種認証サービスをトータルで提供しています。

今回、このNC7000-3A認証基盤に、新たにFIDO生体認証をラインアップに加えます（**図4**）。

4.1 NC7000-3A

～セキュリティと利便性を両立する認証技術への取り組み～

従来、モバイル端末のサービスでは、ID・パスワードを

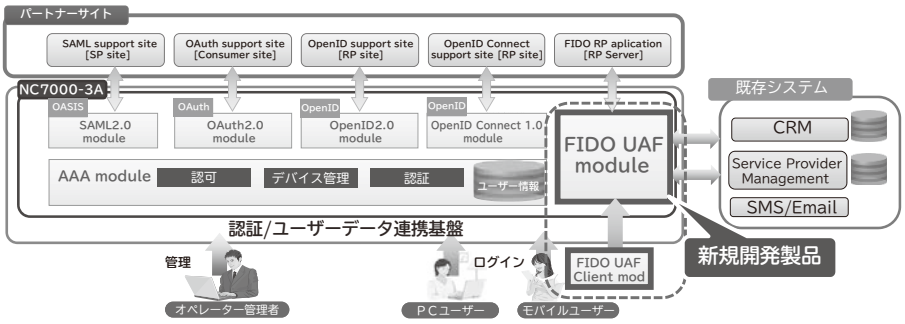


図4　NC7000-3A全体イメージ

使わず利用者を認証する仕組みとして、通信事業者が提供する回線認証を用いることで、モバイル端末の限られたUIの環境でも煩わしさを感じることなくサービスを利用することができました。

スマートフォンの普及により、通信事業者が提供するネットワークを介さないモバイルアクセスが広まると、そこでは回線認証によるユーザー認証が適用できず、サービス利用者は安心したサービス利用のためID・パスワードや、その他煩わしい操作が必要となるユーザー認証を行う必要がありました。

それに対し、NECは2012年の高セキュリティの証明書技術を活用した、セキュリティと利便性を両立する認証・セキュリティソリューションを発表しました。また2016年には独自のデバイス認証機能を提供するなど、この分野における取り組みを推進してきました。

4.2 FIDOの概要

FIDOには大きく分けて(1)UAF、(2)U2Fという2種類の規格があります。

(1) UAFは"Universal Authentication Framework"の略であり、FIDO対応のデバイスを用いてパスワードを使わずに行う認証の規格を定めています。

(2) U2Fは"Universal Second Factor"の略であり、二要素認証を標準化した規格です。

本項では生体認証である(1)のUAFの取り組みについて説明します。

FIDOの最大の特徴は、すべての手続きにおいて生体情報などの個人に紐づく情報がいっさい端末の外部へ送信されないことです。これにより、例えば顔の特徴点など

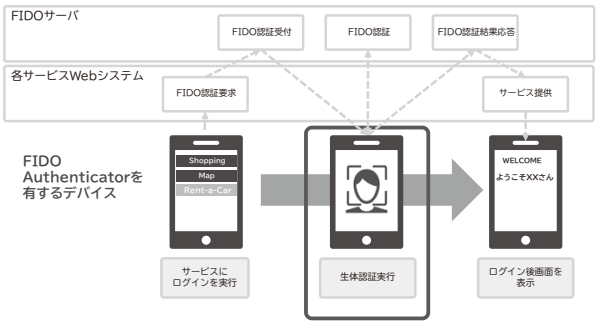


図5　FIDOを利用したログインイメージ

どの生体情報がネットワーク上を流れることはなく、またサービス事業者のサーバに保管されることもないため、万が一の場合にサーバから漏えいするといったこともなく、非常に安全性が高まります。

FIDOではこれを、(1)端末内部での本人認証と、(2)PKIベースで「本人を認証した結果」をサーバサイドへ送信する、という2つのフェーズで実現しています。

具体的には、ユーザーのデバイス内にある「Authenticator」と呼ばれる認証器が、生体情報などを使って本人認証を行った後、認証器が本人確認結果に秘密鍵を使って署名してサーバサイドへ送信、サーバサイドでは事前登録された公開鍵を使って署名を検証し、認証を完了します。なお、秘密鍵と公開鍵のペアは初回のユーザー登録時に生成、登録されるものを利用します。

4.3 利用イメージ

ユーザーがFIDOによりログインする手続きは非常に簡単です。典型的な利用イメージは**図5**に示すとおり、ログインボタンを押下したあとに、スマートフォン上の指紋セン

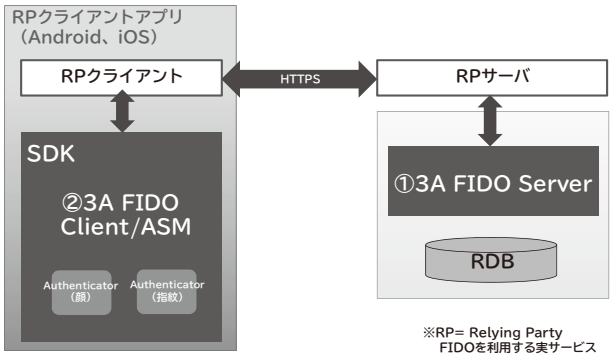


図6　NC7000-3A-FS構成

サーに指をかざしたり、カメラに顔をかざすことで認証が行われます。

4.4 NC7000-3A-FS（FIDOサービス）

3A-FSは、FIDO UAF 1.0に準拠した認証ソフトウェア製品で、生体認証による高いユーザー利便性と安全性を実現します。

3A-FSは、**図6**の構成で、(1)FIDO Server、(2)FIDO Client/ASM/Authenticator（指紋、顔認証）を提供します。

サーバのみ・クライアントのみの利用も可能で、FIDO仕様準拠を示すFIDO Allianceのcertified products*として認定が完了しています[6)]。

サーバ、及びクライアント両方の認定を受けるのは国内メーカーとしては初（弊社調べ2016/12）であり、FIDO生体認証のサービスをワンストップで提供します。

今後、静脈認証や声紋認証などの技術を随時本製品に取り入れることで、複数の生体情報を用いて本人認証を行う「マルチモーダル認証」を実現します。マルチモーダル認証は複数の生体情報を用いてユーザーを判定する生体認証技術であり、世界の金融機関における本人確認技術の1つとしても注目されており、利用拡大が見込まれるソリューションの1つです。ID・パスワードよりも確実で使いやすい次世代の認証方式として検討が進められています。

4.5 NEC独自のセキュリティ実装

近年のモバイルアプリケーション開発においては、サーバだけでなく端末への攻撃も増加しています。FIDOのように、端末内で認証情報保管や暗号計算を行う仕組みの場合には、端末内のセキュリティが重要となります。3A-FSのFIDO Authenticatorでは端末側の情報をもとにした独自のセキュリティモジュールを搭載しています。更にセキュリティモジュールには、強固な難読化を施しています。これらによって、マルウェアや外部の悪意のあるアプリケーションからの不正利用、ハッキングを防止しています。

またNECでは長年、中央研究所のセキュリティ研究所において暗号方式などの研究を行っています。高速秘密計算による認証情報の強固な漏えい防止など、NECの最新の独自暗号技術についても随時取り入れていくことを今後予定しています。

5. オープンAPIへの対応

全国銀行協会では「オープンAPIのあり方に関する検討会」を設置し、銀行システムへの接続仕様をFinTech企業などに公開（オープンAPI）し、金融機関とFinTech企業などとの連携を通じた金融サービスの高度化を検討しています。

金融機関で自社のサービスをAPIとして公開し、ユーザーと銀行及びFinTech企業などを安全に利便性よく結ぶためには、生体認証で認証し認証情報（トークン）を連

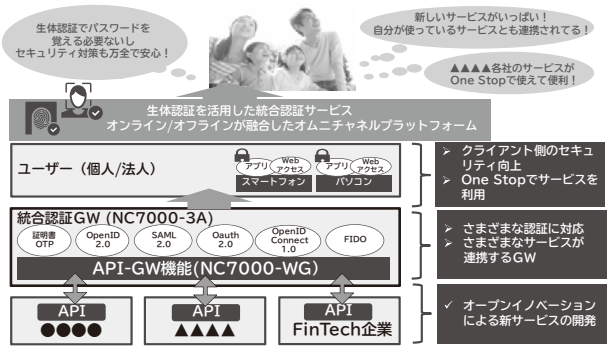


図7　Connected Economy/Open API時代のプラットフォーム

* 2017年2月現在、Server、Client及びAuthenticator(iOS向け指紋認証)の認定が完了。Authneticator(Android向け指紋認証、iOS/Android向け顔認証)の認定も今後予定されています。

携する仕組みが必要となります。

NC7000シリーズであるNC7000-WGにおいてAPI-GWを既に提供しており、生体認証基盤であるNC7000-3Aと連携したアクセス制御などにより、オープンAPIが要求するセキュリティ対策に迅速に対応することが可能です。

このAPI-GWと統合認証基盤の組み合わせにより、Connected Economy/Open API時代の新プラットフォーム（**図7**）を提供していきます。

6. むすび

本稿では、モバイル生体認証の取り組みについて紹介しました。金融機関でのFIDO活用による金融サービスの高度化を進めるとともに、独自のセキュリティ技術も組み合わせながら、将来的にさまざまな領域でインターネットにつながるデジタル端末、家電などIoTセキュリティソリューションへの展開も見据え、技術開発、製品化を進めています。

参考文献

1) FIDO Alliance
https://fidoalliance.org/
2) Bank of America
http://newsroom.bankofamerica.com/press-releases/consumer-banking/bank-america-introduces-fingerprint-and-touch-id-sign-its-mobile-ban
3) シマンテック、個人・企業のパスワード管理に関する意識調査
http://internet.watch.impress.co.jp/docs/news/621665.html
4) NECプレスリリース：NEC、米国国立標準技術研究所(NIST)の指紋認証技術のベンチマークテストにおいて第1位の評価を獲得，2014.8.21
http://jpn.nec.com/press/201408/20140821_02.html
5) NECプレスリリース：NEC、米国国立機関による動画顔認証の性能評価で第1位を獲得，2017.3.16
http://jpn.nec.com/press/201703/20170316_01.html
6) FIDO Certified
https://fidoalliance.org/certification/fido-certified-products/

執筆者プロフィール

中司 豊
SDN/NFV事業部
マネージャー

池谷 亮平
SDN/NFV事業部
主任

手塚 由起子
SDN/NFV事業部
主任

天野 信一
SDN/NFV事業部
主任

青柳 亨
金融システム開発本部
システム主幹

岩佐 綾香
TCI事業部
グローバル第一システム部
マネージャー

関連URL

NC7000-3A（AAA & ID Federation）ID活用基盤ソフトウェア
http://jpn.nec.com/netsoft/nc7000/3a/

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.69 No.2　デジタルトランスフォーメーションを加速するFinTech特集

デジタルトランスフォーメーションを加速するFinTech特集によせて
NECが目指すFinTechの全体像

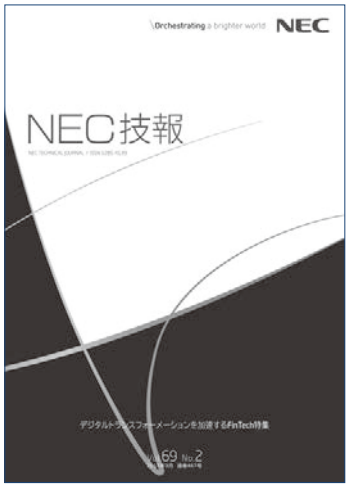
◇ 特集論文

FinTech時代の新しい金融と技術の関係
AIがもたらす金融サービスの変革
ブロックチェーンによる企業間連携の実用化に向けた取り組み
ロボットとAIの組み合わせによる顧客コミュニケーションの高度化
ウェアラブルデバイスを用いた安全・安心・便利な見守りサービス
生体認証によるモバイルサービスのセキュリティと利便性の両立
新たなサービスのスピーディな提供を可能にするモバイルアプリ高速開発
サイバーセキュリティ対策推進による金融サービスの安全性向上
FinTechのセキュリティ強化に貢献するマルチパーティ計算技術

◇ NEC Information

C&Cユーザーフォーラム&iEXPO2016　Orchestrating a brighter world
基調講演
展示会報告

NEWS
2016年度C&C賞表彰式開催



Vol.69 No.2
（2017年3月）

特集TOP