スマートフォン時代の個人認証技術

Personal Authentication Technologies in Smartphone Age

大江哲浩*
Akihiro Ooe
山口奈津子*
Natsuko Yamaguchi
小林良輔*
Ryosuke Kobayashi

要　旨

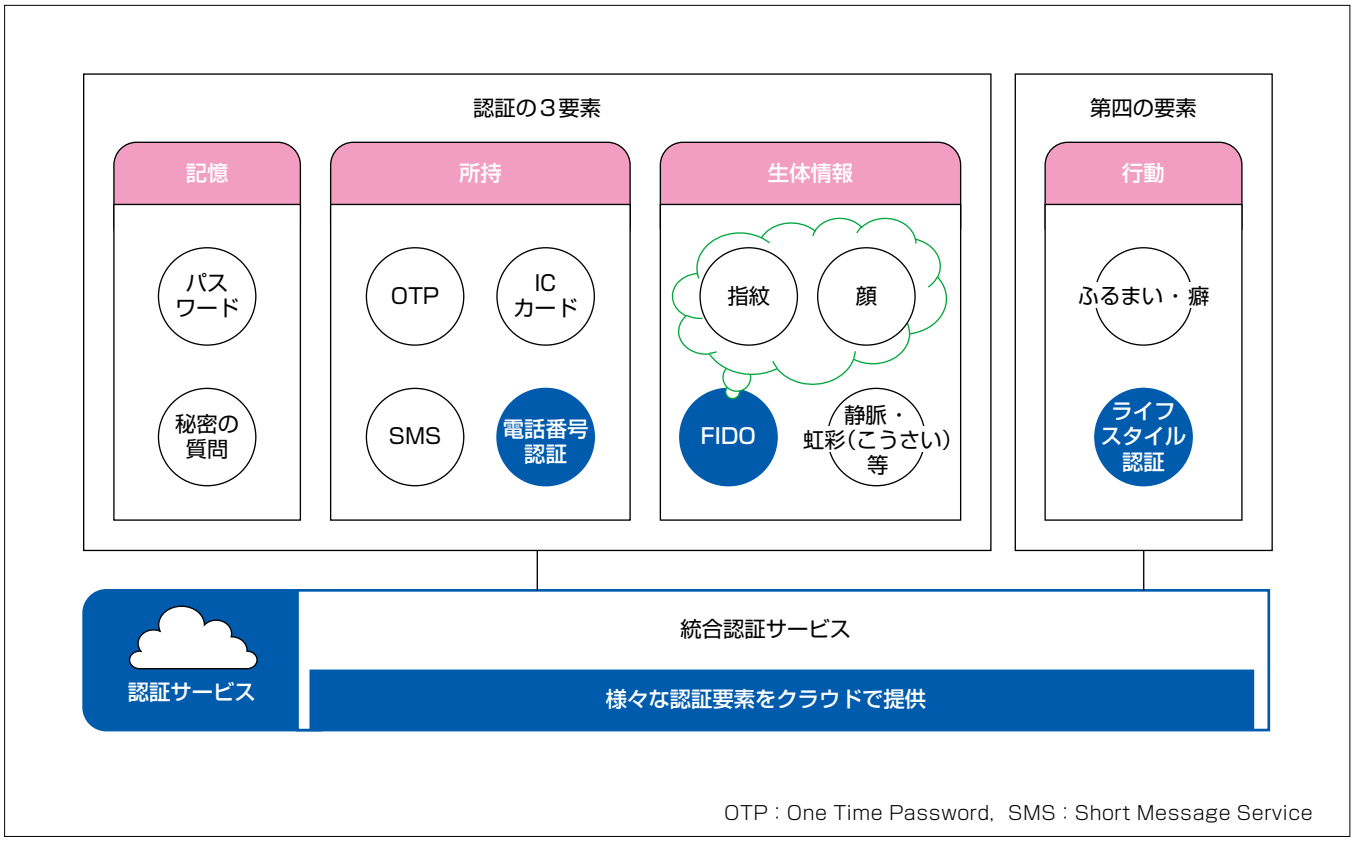
2019年には60歳代のスマートフォン(以下“スマホ”という。)所有率が70％を超えるなど，全世代がスマホを持つ時代になりつつある。全世代に向けたICT(Information and Communication Technology)サービスを提供する際には，ITリテラシーの低い人でも利用できるようなユーザビリティが重要とされている。一方，ICTサービスの利用ではユーザーが本人であることの確認(個人認証)が最重要であるが，個人認証に利用されるパスワードへの攻撃が多発しており，他の認証要素を組み合わせた多要素認証による本人確認が必要になっている。

認証の要素には“記憶”，“所持”，“生体情報”の三つがある。セキュリティとユーザビリティを両立させたスマホ時代の個人認証として三菱電機インフォメーションシステムズ㈱(MDIS)は，“生体情報”として使われることの多いFIDO(Fast IDentity Online)，“所持”要素である電話番号認証，第四の要素として研究されている“行動”を利用したライフスタイル認証(注1)の三つに取り組んでいる。

認証の要素には新旧様々な方式があり，各サービス提供企業が利用情報の重要性とユーザビリティを比較検討して適切な認証要素を選択していくことが必要である。

MDISは複数の認証要素から選択して採用できる統合認証サービスの開発を検討している。MDISは，セキュリティとユーザビリティを両立させた個人認証を提供することによって，安全と便利さが両立した社会の実現に貢献していく。

(注1)　ライフスタイル認証は，東京大学の登録商標である。



OTP：One Time Password，SMS：Short Message Service

多要素認証の要素とそれぞれの要素に使われる認証技術

多要素認証とは，認証の３要素のうち二つ以上の要素を利用した認証のことをいう。スマホ向きの認証技術としては電話番号認証，FIDO，ライフスタイル認証が挙げられる。なお，FIDOは生体認証そのものではなく，生体認証を扱いやすくするための規格である。MDISでは様々な認証要素をクラウドで提供する統合認証サービスの開発を検討中である。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

近年のスマホの普及によって，日本では2019年の60代のスマホ所持率は70％超，70代でも40％超になっており(NTTドコモ モバイル社会研究所調べ)，国民のほとんどがスマホを所持し，民間・行政問わずサービスの提供形態がICT及びスマホ前提になりつつある。

ICTサービスの利用にはユーザーが本人であることの確認が最重要であるが，最も普及している個人認証手段であるパスワードについては，フィッシングやリスト型攻撃によってパスワードが破られ，2019年の7pay事件のような不正アクセス被害が頻発している。不正アクセスの対策として，パスワードだけではなく他の認証要素を組み合わせた多要素認証が必要になっている。

一般に個人認証のセキュリティ強度とユーザビリティはトレードオフの関係にあるが[(1)]，高齢者を含めたITリテラシーの低いユーザーがスマホを扱うことや，ユーザーの快適性への要求レベルも高くなっていること[(2)]等から，多要素認証にはセキュリティ強度とユーザビリティの高さを両立させた認証が求められている。

2. 新たな個人認証技術が必要とされる背景

内閣サイバーセキュリティセンターの情報セキュリティハンドブックV.4ではICTサービスの利用時には多要素認証が推奨されており，国際ペイメントブランド５社が共同で策定して2016年に発効したPCI DSS(決済カード業界データセキュリティ基準)3.2では多要素認証が必須になっている。また，欧州での法的枠組みとして2017年に発効されたPSD2(欧州決済指令第２版)の技術基準ガイドラインで多要素認証，経路外認証等を要求している。

多要素認証での認証の要素としては“記憶(Something you know)”，“所持(Something you have)”，“生体情報(Something you are)”の３要素がある。それらの要素のうち二つ以上を含む認証方法を多要素認証といい，“記憶”に加えて“所持”と“生体情報”のどちらかの組合せが採用される事例が多い。現在，メジャーな認証要素としては“記憶”にはパスワードや秘密の質問，“所持”にはICカードを含むPKI(公開鍵認証基盤)，OTP，SMS等があり，“生体情報”には顔，指紋等による認証がある。

しかし，近年採用事例の多いSMSについてはフィッシング，なりすまし等による攻撃が発生しており，2016年にアメリカ国立標準技術研究所(NIST)から危険性が勧告されている。OTPについてもフィッシングやマルウェアによるリアルタイムでの認証コード詐取が多発している。

また，PKIについては，セキュリティレベルは維持されているものの，秘密鍵の配布・管理等の運用面での煩雑さという課題がある。2019年にiOS13で非接触ICカード通信に対応したことによって，スマホ上でマイナンバーカード等の非接触ICカード内の秘密鍵を利用したPKI認証も可能になって運用面での負荷は軽減されたが，認証時は毎回カードをかざしてPIN(Personal Identification Number)を打ち込む形になり，日々利用するサービスの利用用途としてはユーザビリティ上の問題がある。

生体認証については各社独自の技術を利用しているため個別実装が必要であり，また生体情報の流出の危険性というプライバシーの問題もある。この問題を解決するために考案された標準規格がFIDOである。

MDISでは標準規格への対応だけでなく，ベンチャーの技術を利用した着信電話番号による個人認証(以下“電話番号認証”という。)や，東京大学との共同研究によるライフスタイル認証といった独自の個人認証サービスの研究開発も進めており，今後展開予定である。

3. スマホ時代の認証技術

この章では，セキュリティとユーザビリティを両立させたスマホ時代の認証技術としてFIDO，電話番号認証，ライフスタイル認証について述べる。

3.1 FIDO

FIDOとはFIDO Allianceで策定されている標準規格であり，端末内で生体認証やセキュリティトークン等を利用したオフライン本人確認を実施した後，端末内の秘密鍵によってPKIでのオンライン認証を行うという形式の認証方式である。生体認証自体はオフラインで行われるため，生体情報が外部に流出することがなく，オンライン認証部分も従来のPKIのノウハウが流用できるという利点がある。

2019年にはFIDO2.0の機能であるWebAuthnがW3C(World Wide Web Consortium)に正式に勧告されたことによって，様々なWebブラウザでFIDO2.0による認証が利用可能になっている。

FIDOではスマホの内蔵生体認証センサを利用する場合が多いため，認証の３要素のうち“生体情報”に分類されることが多いが，FIDOの規格では生体認証の認証精度に対しては認定制度がなく，生体認証が十分な精度を保持しているかの保証は行わないため，認証の３要素のうち“所持”に当たるとされることもある。また，オフライン本人確認には“生体情報”だけでなくセキュリティトークン等も利用可能である。

3.2　電話番号認証

電話番号認証では，ユーザーの所持物である電話から認証システムに対して電話を掛け，着信した電話番号と顧客データベース上の電話番号の照合によってICTサービスのログイン認証を行う。固定電話からの利用も可能であるが，個人認証としては携帯電話での利用を想定している。

3.2.1　認証要素としての電話番号の特徴

⑴　国内での携帯電話の契約数は2020年３月時点で１億8,000万件を超える[3]。携帯電話はその性質上，個人利用を前提にしており，個人を識別するための認証装置としての適性を持つ。

⑵　新規の電話番号契約時には必ず本人確認が行われており，不正に取得される可能性が低く，有事の際はキャリアによるユーザーの追跡も可能である。MNP(携帯電話番号ポータビリティ)の普及によって，同じ電話番号が継続的に利用される傾向も高く，長期的に認証装置として利用できる。

⑶　ユーザー自身の所持物を認証装置として利用しているため，OTPやICカードと異なり，配布や管理といった企業側の負荷が少ない。

3.2.2　電話番号認証の特長

⑴　ユーザーは自身の所有する電話から認証用電話番号へ発信するだけで認証完了となり，操作が簡易である。特にスマホの場合はブラウザやアプリケーションに記載された電話番号をタップするだけで電話発信されるため，ITリテラシーの低い子供や高齢者でも利用できる。

⑵　認証システム側では着信のあった電話番号情報を一時的にハッシュ化して登録するが，認証完了後に瞬時に削除されるか，又は数分間保持の後に削除される。また，電話番号以外の，例えばユーザーID(IDentification)等の情報は取得しないため，個人情報の取り扱いが発生しない。

⑶　電話網はキャリア間での安全な専用線になっており，通信の盗聴・改ざんは困難である。携帯電話の電話番号はセキュアエレメントであるSIM(Subscriber Identity Module)に格納され改ざんは不可能である。電話番号の詐称については国内ではキャリア側で排除される。

3.2.3　電話番号認証のシステム構成

⑴　電話番号認証の構成要素

電話番号認証は次の要素で構成される(**図１**)。

①電話を利用して認証を行うユーザー(以下“ユーザー”という。)

②電話番号を含むユーザー情報を管理し，電話番号による認証結果を利用するシステム(以下“サービスシステム”という。)

③ユーザーからの着信情報とサービスシステムから送信された認証対象となる電話番号を紐(ひも)づける認証システム(以下“電話番号認証システム”という。)

⑵　電話番号認証の認証フロー

電話番号認証での認証は次のフローで行われる。

①サービスシステムはユーザーから認証リクエストを受ける。

②サービスシステムはユーザーを特定し，そのユーザーの電話番号情報を取得する。取得した電話番号情報をハッシュ化し，電話番号認証システムに登録する。

③サービスシステムはユーザーに対して，認証用電話番号情報を表示する。

④ユーザーは認証用電話番号に対して，自分の所持する電話番号から発信を行う。

⑤電話番号認証システムは着信のあった電話番号情報を取得し，②でサービスシステムから登録された電話番号と一致するものが存在するか確認する。

⑥登録された電話番号が存在した場合は認証成功の結果を，認証が成功せず一定時間経過した場合は認証失敗の結果をサービスシステムに返す。

⑦サービスシステムはユーザーに対し，認証結果に対応する処理を行う。

3.2.4　電話番号認証の利用用途

⑴　ログイン認証時のパスワードの代替

セキュリティを確保しつつ，煩雑なパスワード管理から解放され，ユーザーの利便性を向上させる。

⑵　SMS認証とOTP認証の代替

SMS認証とOTP認証はマルウェアやフィッシングによるリアルタイムでの認証コードの詐取のおそれがあるが，電話番号認証では認証コードの授受は行わない。

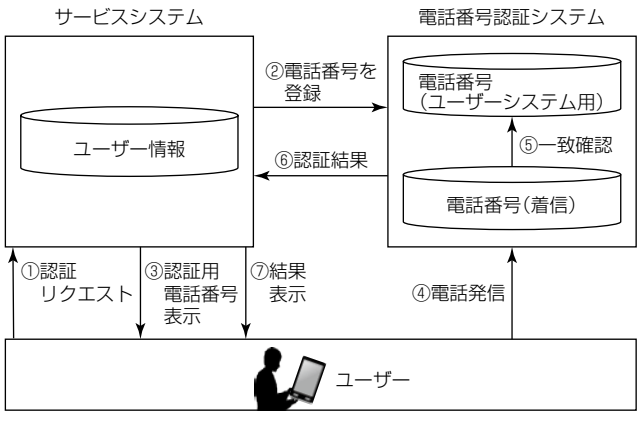


図１．電話番号認証のシステム構成と認証フロー

⑶　チャットを利用したサービス提供時の個人認証

チャット上で使える認証要素はパスワードやOTP等テキストベースのものに限られるが，チャット上のテキストとして，認証用電話番号を記載し，その電話番号にユーザーから電話させることでチャット内での個人認証が可能である。

⑷　簡易本人確認

顧客データベースに電話番号を事前に登録している場合，電話番号認証システムに着信した番号と顧客データベース上の電話番号を照合することで，少なくとも同一電話番号を所持している人であることが確認できる。また，顧客データベースに電話番号の登録がない場合でも，チケット購入時等に同一人物による複数申し込みを抑止し，不正転売等を防止すること等に利用可能である。

3.3　ライフスタイル認証

この節では新たな個人認証技術であるライフスタイル認証の概要と，2019年にMDISで実施した実証実験及び実用化に向けた今後の展開について述べる。

3.3.1　ライフスタイル認証の概要

三つの認証要素に加えて“行動”が第四の認証要素として活用できることが指摘されている[4]。ライフスタイル認証は“行動”のうち特に生活習慣から見いだされる個人の特性に着目したものであり，東京大学が2016年にその構想を発表したものである[5]。

IoT(Internet of Things)技術の発展によって，人の行動は様々なセンサによってリアルタイムかつ自動的に収集されるようになった。特にスマホの普及は，その搭載されているセンサによって個人の行動を電磁的データとして活用することを容易にした。ライフスタイル認証ではこのような行動情報を個人認証に活用する。行動情報はユーザーが意識せずに自動的に収集されるため，認証時に意識的な入力を必要としない。パスワードや指紋認証等の煩わしい入力を省き，水面下での認証を可能にするこの手法は，なりすましを防ぐだけでなく利便性も向上させる手法として期待されている。

またこのようにして収集される行動情報は，認証用途だけでなく，生活習慣に基づくパーソナライズドサービスの提供に応用することも期待されている。

3.3.2　ライフスタイル認証の仕組み

ライフスタイル認証に使用される行動情報として，将来的にはスマートホームや公共施設，店舗等，様々な場所に設置されているセンサ情報を活用することが検討されている。現状では，個人が持つスマホのセンサ情報のうち，GPS(Global Positioning System)による位置情報と電波センサによるWi-Fi(注2)情報を活用した仕組みが実装されている。この項ではこれらの情報を活用したライフスタイル認証の仕組みについて述べる。

位置情報とWi-Fi情報の収集はスマホの専用アプリケーションによって行われ，定期的に情報を認証サーバにアップロードする。一般的に個人認証のフローは登録フェーズと検証フェーズの二つから構成され，ライフスタイル認証も同様の構成になっている。登録フェーズでは，個人の特徴をモデル化したテンプレートが，認証サーバにアップロードされた3週間程度の情報を基に作成される。検証フェーズでは，認証時から過去1時間，及び24時間の行動パターンを認証サーバの情報から抽出し，その行動パターンをテンプレートと比較して行動類似スコアを算出する。そのスコアが設定されたしきい値よりも大きければ正しく本人だと判断し，認証成功となる(**図2**)。しきい値はサービスによって変更可能で，決済のような安全性が求められるものには大きく，一方で照会のような決済ほど安全性を求められないものは小さく設定することが可能である。

人の生活習慣での行動は，繰り返されはするものの常に同じではなく，ゆらぎが存在するため，そのゆらぎを吸収する処理が行われている。人の行動は生体情報と比較すると一定でないが，認証精度については過去の研究では平均で本人受入れ率93%，他人受入れ率は0%に近い数字になることが発表されている[6]。

(注2)　Wi-Fiは，Wi-Fi Allianceの登録商標である。

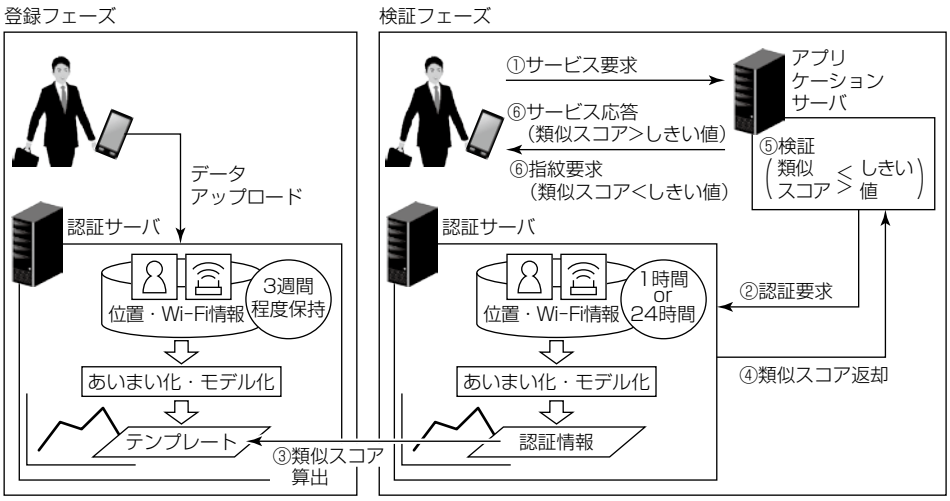


図2．ライフスタイル認証の仕組み

3.3.3　ライフスタイル認証実証実験

三菱UFJニコス㈱(以下“ニコス”という。)とMDISは東京大学山口研究室の協力の下，ライフスタイル認証を他サービスとリアルタイムで連携することを目的にした実証実験を2019年に実施した[7]。

⑴　実験内容

この実験は無人コンビニでの決済を想定したもので，専用アプリケーションをインストールしたスマホを所持して，この実験用にニコス及びMDIS社内に設置した無人販売ボックスに接近すると，ライフスタイル認証によって本人かどうかを自動で検証し，本人であれば扉を開錠する。無人販売ボックスから取り出した商品はRFID(Radio Frequency IDentification)で自動的に特定され，専用アプリケーションにあらかじめ登録されたクレジットカードで決済される。これによって商品を取り出すこと以外，操作なしで商品の購入が可能になる(**図３**)。

⑵　実験結果と課題

この実験では目的であったライフスタイル認証と決済サービスとをリアルタイムで連携することに成功し，ライフスタイル認証技術が実サービスで利用可能であることが実証できた。また，この実験を基に，利用者端末，認証装置，サービス提供装置間の認証情報の連携についての特許を東京大学，ニコスと共同出願している(特願2020-052332)。一方，次のような課題も判明した。

①出張後や休暇明け等で行動が変化した直後は認証が通らないことがあるが，その場合の追加認証をパスワードにしたため，ユーザビリティの評価が低く，追加認証には利便性の高い認証技術の採用が必要である。

②被験者アンケートでは，行動情報収集に関するプライバシーへの不安感といった回答もあり，情報の利用用途や保護の仕組みを周知した上での本人同意の仕組みの整備が必要である。

③この実験は110名強の規模で実施したため，今後，更に大規模展開時のスケーラビリティ評価が必要である。

3.3.4　ライフスタイル認証の今後の展開

実証実験での課題解決に加え，次の対応を行うことでライフスタイル認証の早期実用化と普及を目指している。

⑴　ライフログ取得元のセンサ類の追加と認証アルゴリズムのブラッシュアップ

⑵　FIDO等の標準規格への対応。FIDOは個人情報が端末外に出ないという特徴があるため，プライバシー問題の解決策としても期待されている。

⑶　ライフログ解析技術の生活習慣に基づくパーソナライズドサービスの提供への応用

図３．無人販売ボックスでの実証実験の様子

4. むすび

セキュリティとユーザビリティを両立させた個人認証技術について述べたが，基本的には認証のユーザビリティとセキュリティ強度はトレードオフの関係にあり，公的サービスを利用する際のJPKI(公的個人認証サービス)や医師が医療システムを扱う際のHPKI等，高セキュリティだが導入障壁の高いPKI認証が必要になるケースもある。

各サービス提供企業又はユーザー個人が利用情報の重大性を比較して適切な認証要素を選択していくことが必要であるが，MDISはPKIを含めた複数の従来型認証要素及び本稿で述べた新認証要素を選択又は組み合わせて採用できる統合認証サービスの開発を検討している。

Society5.0(サイバー空間とフィジカル空間の融合による超スマート社会)での個人認証は，“安全で確実であること”に加え“誰でも手軽に負担感なく使えること”が必要とされている[1]。スマホを全世代が持つ時代でMDISは，セキュリティとユーザビリティを両立させた個人認証を提供することによって安全と便利さが両立した社会の発展に貢献していく。

参考文献

⑴　総務省：Society5.0を見据えた個人認証基盤のあり方について(報告)(2018)
https://www.soumu.go.jp/main_content/000560721.pdf

⑵　google：Find Out How You Stack Up to New Industry Benchmarks for Mobile Page Speed
https://www.thinkwithgoogle.com/intl/en-cee/insights-trends/research-data/find-out-how-you-stack-new-industry-benchmarks-mobile-page-speed/

⑶　電気通信事業者協会：携帯電話・PHS契約数(事業者別契約数)
https://www.tca.or.jp/database/index.html

⑷　Yamaguchi，R. S.，et al.：Redefine and Organize，4th Authentication Factor，Behavior，CANDARW 2019，412～415 (2019)

⑸　東京大学ソーシャルICT研究センター：ソーシャルICT研究センター 第４回シンポジウム「ビッグデータを活用した社会基盤の変革と実践」(2016)
http://www.sict.i.u-tokyo.ac.jp/news/sympo20160607/

⑹　Kobayashi，R.，et al.：Large Scale PoC Experiment with 57,000 people to Accumulate Patterns for Lifestyle Authentication. Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy，161～163 (2019)

⑺　日本経済新聞：三菱UFJニコスと三菱電機インフォメーションシステムズ，次世代個人認証技術「ライフスタイル認証」活用の購買実証実験を開始 (2019)
https://r.nikkei.com/article/DGXLRSP513200_Y9A620C1000000