パスワードレスでの利用資格の共有・委譲技術

吉村 康彦（よしむら やすひこ）/菅 友梨香（すが ゆりか）
大森 芳彦（おおもり よしひこ）/山下 高生（やました たかお）
柴田 哲良（しばた あきら）
NTTネットワークサービスシステム研究所

NTT研究所では，安全性と利便性を両立させた認証基盤の確立をめざし，研究開発を進めています．本稿では，特に近年普及が進むスマートフォンのようなモバイル端末を用いてさまざまなサービスを利用する際に，パスワードを必要としない安全な認証基盤技術について紹介します．今後は本技術をさまざまなサービスに適用し，利便性の向上を図っていきます．

背　景

スマートフォンのようなモバイル端末の急速な普及に伴い，場所を問わずオンラインでさまざまなサービスが利用可能になってきました．個々のサービスを利用する際にはIDとパスワードを用いて認証する方法が一般的に用いられていますが，利用者はサービスごとに異なるパスワードを記憶して入力する必要があり，利便性の観点で課題があります．また，ID・パスワードの流出によるなりすましへの懸念もあります．これらの問題に対処するため，安全かつ便利な認証の実現をめざし，技術検討を進めています．

FIDO関連技術

安全・便利な認証という観点では，FIDO（Fast IDentity Online）アライアンスが，公開鍵暗号化技術を活用した認証方式を提案しています[(1)]（**図1**）．FIDO仕様の1つに，スマートフォンなどのモバイル端末での利用を想定しているUniversal Authentication Framework（UAF）プロトコルがあります．UAFは認証用の秘密鍵をモバイル端末のセキュア領域（SE/TEE領域など）に格納し，モバイル端末を認証トークンとして利用します．また，認証時に公開鍵暗号技術を活用することで，サーバと端末で秘密情報（パスワードなど）を共有することなく高い安全性を提供します．さらに，最近のモバイル端末が一般的に備えている生体認証などの本人確認手段を用いて認証を実現することで，パスワードを必要としない認証を実現します．

利便性向上技術概要

さまざまなサービス事業者がFIDO認定を受けた認証エコシステムを導入し始めており，FIDO技術の普及が進みつつあります．NTT研究所では，FIDO技術を応用して利用者間で物やサービスの利用資格の共有を実現することで，さらなる利便性の向上をめざしています．

FIDOのように公開鍵暗号化方式を用いる場合，モバイル端末にはサービス数分の鍵を登録しますが，機種変更などにより新しい端末を利用する際にはユーザ自身が再登録を実施する必要があります．利便性向上技術では複数の端末間で鍵を安全・簡単に共有する仕組みを提供することにより，再登録の負担を軽減します．

利便性向上技術の核となる鍵共有（委譲）方式の概要を**図2**に示します．鍵コピー方式（図2(a)）ではSE/TEE領域にある秘密鍵を新しい端末に複製します．この際，安全性を確保するために生体認証を用いることや，電子証明書を用いた本人確認を行うこと，NFCやBluetoothなどの近傍通信

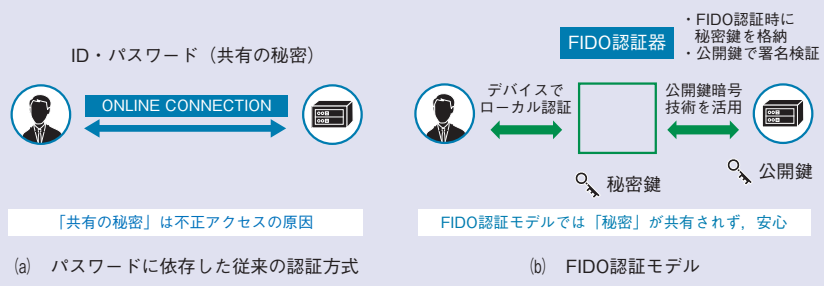


図1　FIDO認証方式の特徴

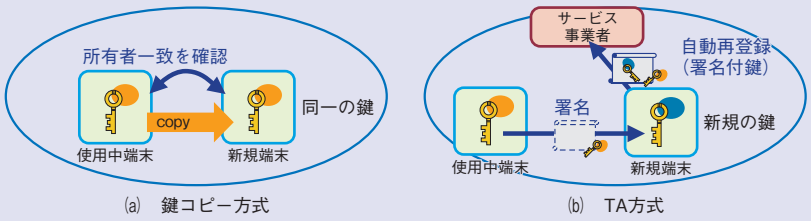


図２　鍵共有（委譲）方式の概要

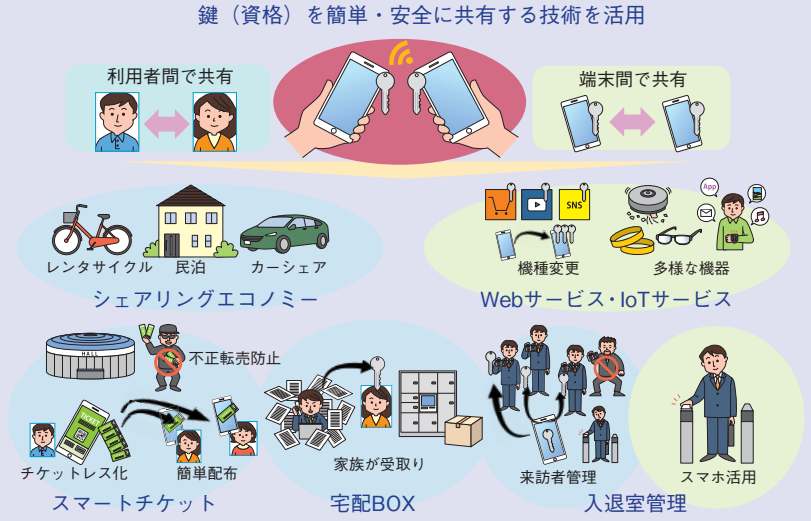


図３　利便性向上技術の適用

を用いることでインターネットを経由させないことなどの工夫をしています[2]．また，端末間の鍵共有はお互いの端末をかざしたうえで，生体認証を行うという簡単な端末操作で実現できます．

また，ワシントン大学が提案しているTransfer Access（TA）方式[3]（図２⒝）は，すでに登録済の利用者の秘密鍵を使い，新しい端末の公開鍵に電子署名を付与することで，サーバ（サービス事業者）に同一の利用者であることの通知を可能にします．この方式は，認証サーバを改造する必要がありますが，サービス事業者が新たな端末で認証を行うことを知りたい場合に有効な方法です．

利便性向上技術の応用

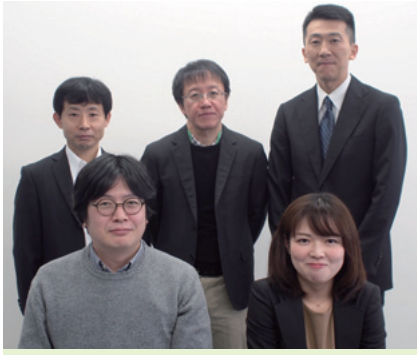
利便性向上技術の端末間で秘密鍵を共有する仕組みを用いて，利用者間でサービスや資源の利用資格を共有（委譲）する仕組みへの応用についても検討を進めています[4]．TA方式において，使用中端末を利用者A，新規端末を利用者Bとすると，利用者Bが公開鍵を登録する際に，サービス事業者にとってはすでに利用資格のある利用者Aが新たに利用者Bに利用資格を与えると考えることができます．利用資格を端末間で共有するだけでなく，利用者間での権限の委譲に用いることでさまざまなサービスへの適用が可能となります（**図３**）．

今後の展開

本稿ではパスワードを必要としない安全かつ便利な利用資格の共有，委譲方法について紹介しました．今後はさまざまなサービスへの適用について具体的な実現方式の検討を進めることで，認証基盤の汎用化，高度化に努め，関連サービスのさらなる付加価値向上に貢献していきます．

■参考文献

⑴ https://fidoalliance.org/
⑵ H. Nishimura, Y. Omori, T. Yamashita, and S. Furukawa: “Secure Authentication Key Sharing between Mobile Devices Based on Owner Identity,” Proc. of MobiSecServ 2018, Miami, U.S.A., Feb. 2018.
⑶ A. Takakuwa, T. Kohno, and A. Czeskis : “The Transfer Access Protocol Moving to New Authenticators in the FIDO Ecosystem,” Technical Report UW-CSE-17-06-01, The University of Washington, 2017.
⑷ 大森・西村・山下：“多数のユーザ端末間でのサービス利用の認可に関する検討，” 2018信学ソ大，2018.



（後列左から）大森　芳彦/ 山下　高生/
柴田　哲良
（前列左から）吉村　康彦/ 菅　友梨香

スマートフォンの普及で，生活のさまざまな場面でオンラインサービスを利用する機会が増えています．さまざまなサービスに対応したパスワードを必要としない簡単かつ安全な認証基盤を確立することで利便性向上に貢献していきたいと考えています．

◆問い合わせ先
NTTネットワークサービスシステム研究所
ネットワーク制御基盤プロジェクト
TEL　0422-59-3449
E-mail　nepud-rv-ml@hco.ntt.co.jp