SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

WebAuthnを基にしたWebサービスにおける端末追加のためのプロトコルの評価

An Evaluation of a Protocol on Addition of New Devices Based on WebAuthn

網川 澪 * 福光 正幸 *
Mio AMIKAWA Masayuki FUKUMITSU

キーワード WebAuthn，FIDO，端末追加

あらまし

「WebAuthn[1]」とは，W3CとFIDO（Fast IDentity Online） Allianceによって策定された次世代認証Web APIである．この認証は，公開鍵認証をベースとする「オンライン認証」と，オンライン認証で使用する秘密鍵を使用可能にするためのユーザ端末内認証「オフライン認証」の2つのフェーズに分けられる．この秘密鍵は，Secure Elementのような耐タンパ性を備えたハードウェアや，Trusted Execution Environmentなどの通常の動作領域から独立したセキュア領域に保管される前提となっている．すなわち，秘密鍵を端末外に持ち出すことが困難であるため，Webサービス利用の際，アカウント登録時に使用した端末とは異なる端末でログインするには，新たにその端末を用いた登録作業を行う必要がある．これに対し，従来研究では，Webサービス利用の際に通信キャリアのサーバを経由することで，複数端末に対応した認証方式を提案していた．

我々[2]は，WebAuthnの仕組みとQRコードを応用することにより，仲介サーバなしの新規端末追加プロトコルを検討し，プロトタイプを実装した．このプロトコルでは既にWebサービスに登録済みの端末（以降，既存端末）が，オンライン認証の際に生成するレスポンスから，新規に登録する端末（以降，新規端末）が登録する際に用いるチャレンジを生成し，これをQRコードを介して新規端末に送り登録作業を行うことで，既存端末と新規端末の紐づけを行っていた．しかし，文献[2]のプロトコルでは，プロトコルの動作途中で既存端末のレスポンスをインターネット通信を介してサーバに送信していた．

本研究では，文献[2]のプロトコルについてさらに検討を行い評価する．具体的にはまず，新規端末のチャレンジ生成の際にサーバを介さず，既存端末上でチャレンジの生成とそのQRコード化を行い，オフラインで新規端末にチャレンジを送信できる改良プロトコルを検討し，このプロトタイプを実装する．

また，文献[2]のプロトコルと改良プロトコルに対し，次の2つの評価を行う．1つ目は，文献[3]を基にした，利便性，安全性，導入容易性に関する定性的評価である．2つ目は，定性的評価にて評価しきれなかった項目に対するユーザ実験を介した定量的評価である．

参考文献

[1] FIDO Alliance, “FIDO2: Web Authentication (WebAuthn),” FIDO Alliance, `https://fidoalliance.org`, 参照 Dec. 3, 2021.

[2] 網川 澪, 福光 正幸, “WebAuthnを基にした端末追加と権限付与のためのプロトコルの実装,” 電子情報通信学会総合大会講演論文集, No.A-7-10, p.59, 2021.

[3] J. Bonneau, C. Herley, P.C. van Oorschot, F. Stajano, “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,” IEEE Symposium on Security and Privacy, pp. 553–567, 2012.

* 北海道情報大学 大学院経営情報学研究科, 〒069-8585 北海道江別市西野幌59番2, Graduate School of Business Administration and Information Science, Hokkaido Information University, Nishi Nopporo 59-2, Ebetsu, Hokkaido. 069-8585