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

カメレオン署名を用いたFIDO認証の権限移譲機能の検討
Account Dalegation of FIDO using Chameleon Signature

成松 怜央 * 岡田 怜士 * 満永 拓邦 *
Reo Narimatsu Satoshi Okada Takuho Mitsunaga

キーワード 公開鍵暗号, デジタル署名, FIDO, カメレオン署名, カメレオンハッシュ関数

あらまし

今日，パスワード認証に代わる認証方法として Fast IDentity Online (FIDO) 認証が注目されている．FIDO 認証はパスワードによる認証を必要とせず，公開鍵暗号方式を用いてユーザの認証を行うため，利用者と Web サーバの間で秘密情報を事前に共有する必要がない．そのため，フィッシング攻撃や辞書型攻撃への耐性を持っており，Google Chrome をはじめとする主要なブラウザが対応している．FIDO 認証が普及することで，パスワードの使いまわしや複雑なパスワードの暗記の必要がなくなり，今後，リモートワーク環境でのセキュアな認証の普及していくことが期待されている．また，利用者を認証するという主たる機能に加えて，FIDO 認証にアカウント権限の移譲などの追加的な機能を持たせる研究が行われている [1]．リモートワークの拡大に伴い，ネットワークを介した安全なアカウント権限の移譲機能は必要性が増えると考えられる．本論文では，カメレオン署名を FIDO 認証のプロトコルに適用することにより，アカウント権限の委譲を実現する方法について考察する．

参考文献

[1] F. Alqubaisi, A. S. Wazan, L. Ahmad and D. W. Chadwick,“”Should We Rush to Implement Password-less Single Factor FIDO2 based Authentication?,”2020 12th Annual Undergraduate Research Conference on Applied Computing (URC), 2020,pp. 5-6,

* 東洋大学，115-8650 東京都北区赤羽台１丁目７－１１，Toyo University, 1-7-11, Akabanedai, Kita-ku, Tokyo 115-8650
s1f101802904@iniad.org