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

# TEE を活用した ID ベース認証付き鍵交換の実装に関する考察
# On the Implementation of Identity-Based Authenticated Key Exchange using TEE

工藤 史堯 * 飯島 悠介 * 永井 彰 *
Fumiaki Kudo Yusuke Iijima Akira Nagai

**キーワード** IoT, TEE, ID ベース暗号, 認証付き鍵交換

## あらまし

本論文では, ID ベース認証付き鍵交換プロトコルを IoT デバイス上でセキュアに実装することを目的として, Trusted Execution Environment(TEE)[1] の活用について考察した結果を報告する.

IoT ではその利用用途の拡大に伴い, 情報漏えいや機器の不正制御の脅威が高まっており, 通信相手が正当な相手であることを相互に確認する相互認証の重要性が増している. IoT にはしばしば LPWA（Low Power Wide Area）のような狭帯域ネットワークが使われるため, 狭帯域なネットワークでも活用可能な IoT 向けの認証技術として, 通信量の少ない ID ベース暗号を活用した認証方式が提案されている [2]. 一方で昨今は末端の IoT デバイスに対する攻撃が増加しており, IoT デバイス上での認証技術の実装においては認証プロトコル自体の安全性もさることながら, IoT デバイスでの実行環境や秘密鍵の管理などセキュアな実装も重要な課題となる.

そこで本稿では, ID ベース暗号を活用した認証付き鍵交換プロトコルを, アプリケーションの安全な実行環境を実現するための技術である TEE を用いてセキュアに実装するための考察を行う. 今回は TEE の実装技術のひとつである, Arm Cortex-M の TrustZone[3][4] を例として取り上げ, TrustZone を ID ベース認証付き鍵交換プロトコルへ適用した場合に期待される効果について議論する. その上で, 期待される適用効果を実現するための, モジュールの適切な配置構成や鍵管理方法に関して具体的に検討し, 認証付き鍵交換を IoT デバイス上でセキュアに実装するための方式を示す.

* NTT 社会情報研究所, 〒 180-8585 東京都武蔵野市緑町 3-9-11, NTT Social Informatics Laboratories, 3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585, Japan

## 参考文献

[1] GlobalPlatform,「The Trusted Execution Environment:Delivering Enhanced Security at a Lower Cost to the Mobile Market White Paper」, June 2015

[2] Junichi Tomida, Atsushi Fujioka, Akira Nagai, and Koutarou Suzuki,“Strongly Secure Identity-Based Key Exchange with Single Pairing Operation,”ESORICS 2019, LNCS 11736, pp. 484–503, 2019.

[3] Arm,「TrustZone Technology for the Armv8-M Architecture」, October 2018

[4] Arm,「Armv8-M Architecture Reference Manual」, September 2021