**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の保護を用いたProvenance AuditingのIoT機器への適用
# Provenance Auditing with TEE Protection Applied to IoT Devices

竹村 太一 *† 須崎 有康 * 山本 嶺 †
Taichi Takemura Kuniyasu Suzaki Ryo Yamamoto

**キーワード** Arm TrustZone，Provenance Auditing，Secure Logging

## あらまし

IoT 機器を対象とした初期の攻撃では，マルウェアである Mirai，BASHLITE を用いて DDoS（Distributed Denial of Service attack）やネットワークのスキャンを行っていた．しかし，最近の攻撃では，ファイルレスマルウェアやシェルコマンドを利用する攻撃といったステルス性の高い攻撃が増加している．さらに，マルウェアを用いた攻撃においても攻撃が洗練されており，検知システムから逃れるための回避行動を積極的に行う．例として，ファイアウォールのプロセスの無効化やアクセスログ，履歴ログの削除やタイムスタンプの変更を行う [1]．そのため，従来の攻撃の検知手法では攻撃をすべて検知することができず，攻撃の見逃しが発生する [2]．ステルス性の高い攻撃を検知するためにも，改竄不可能なログから攻撃の影響範囲を調査するための手法が必要である．従来のコンピュータを対象とした攻撃の影響範囲を調査する手法として PA (Provenance Auditing) [3] が提案されている．PA は，システムで実行されるイベントを記録したログから DAG (Directed Acyclic Graph) を構築し，DAG から攻撃の影響範囲を調査する．しかし，PA を IoT 機器に用いるのには以下の三つの問題がある．(1)IoT 機器は CPU パワーが限られており，高い CPU パワーを要求する PA を実行するのが難しい．(2)IoT 機器はセキュリティの仕組みが備わっていないことが多く，攻撃者によってログの改竄や削除を行われる可能性がある．(3)IoT 機器は管理者がいないため，M2M (Machinet to Machine) で管理するために自律的に復旧できる仕組みが必要になる．

本論文では，クラウド上のサーバと IoT 機器を連携させることにより，リモートで PA を行う手法を提案する．この手法では，クラウド上のサーバで SPADE [3] を用いて PA を行い，エッジで動作する IoT 機器は堅牢化したカーネルと TEE (Trusted Execution Environment) を用いてログの生成や送信を保護する．TEE はハードウェアによって提供される隔離された実行環境である [4]．ログの送信を止めるといった攻撃に対処するため，リモートからの Heart Beat を行うことで問題を検出し，問題が発生した際は TEE で保護された Watchdog Timer からシステムリセットを行う．提案手法のプロトタイプを Raspberry Pi 3B の Arm TrustZone に OP-TEE を用いて実装した．

## 参考文献

[1] Omar Alrawi, Charles Lever, Kevin Valakuzhy, Kevin Snow, Fabian Monrose, Manos Antonakakis, and Others. The circle of life: A Large-Scale study of the IoT malware lifecycle. In *USENIX Security Symposium*, 2021.

[2] Fan Dang, Zhenhua Li, Yunhao Liu, Ennan Zhai, Qi Alfred Chen, Tianyin Xu, Yan Chen, and Jingyu Yang. Understanding fileless attacks on linux-based IoT devices with HoneyCloud. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, pp. 482–493, June 2019.

[3] Ashish Gehani and Dawood Tariq. SPADE: Support for Provenance Auditing in Distributed Environments. In *In Proceedings of the 13th International Middleware Conference*. Springer, 2012.

[4] 須崎有康. Trusted execution environment の実装とそれを支える技術. 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, Vol. 14, No. 2, pp. 107–117, 2020.

* 産業技術総合研究所, 東京都江東区青海 2-3-26, National Institute of Advanced Industrial Science and Technology, 2 Chome-3-26 Aomi, Koto City, Tokyo
† 電気通信大学, 東京都調布市調布ヶ丘 1-5-1, The University of Electro-Communications, 1 Chome − 5 − 1, Chofugaoka, Chofu, Tokyo