YNU 横浜国立大学 YOKOHAMA National University

Press Release
2024 年 4 月 19 日

〒240-8501 横浜市保土ケ谷区常盤台 79-1

遠隔からの IoT 機器制御用セキュアシステムを国際標準化

本学から提案した Technical Report を国連標準化機関 ITU-T が正式発行

本研究のポイント

- 一つの制御サーバから多数の任意の IoT 機器をセキュアに制御可能な基盤技術「放送型認証方式」を開発し、国際標準（Technical Report）として成立した。
- 上記の放送型認証方式を活用し、多数の機器から構成されるネットワークにおいて、不具合のある機器や寿命に到達した機器を一括で選択的に停止や再起動させる制御が可能。
- 上記の停止・再起動以外の様々な制御コマンドにも適用可能。

【研究概要】

- 横浜国立大学大学院環境情報研究院・先端科学高等研究院 四方順司教授らの研究グループが国連専門機関の国際電気通信連合（ITU）における国際標準化部門（ITU-T）に提案していた“Broadcast authentication schemes for IoT system” が 2023 年 9 月 5 日 Technical Report として承認され、2024 年 2 月に発行されました。
  (https://www.itu.int/pub/T-TUT-ICTSI-2023-1)
- 本研究成果およびその国際標準化により、今後ますます活用が広がる IoT 機器の安全かつ効率的な制御および管理の実現に貢献することが期待されます。
- 本研究およびその国際標準化は、総務省委託研究・電波資源拡大のための研究開発「電波の有効利用のための IoT マルウェア無害化/無機能化技術等に関する研究開発（研究代表者 横浜国立大学先端科学高等研究院 IAS 客員教授 中尾康二)」(令和 2 年～4 年)の成果です。

【研究成果】

今後、多種多様で多くの IoT 機器がさらにネットワークにつながる時代となります。これら多くの IoT 機器を遠隔から安全かつ迅速に一括で制御するための暗号技術として、放送型認証方式を開発しました。本方式では、制御を行うエンティティ（サーバ等）が、ネットワークにつながる多くの IoT 機器に対して、ブロードキャスト通信を介して、任意の複数個の IoT 機器を一括で効率的に制御することが可能となります。例えば、マルウェアに感染した IoT 機器や、寿命が尽きても放置されている IoT 機器に対して、それらの電源を切ってネットワークから隔離するための制御に応用できます。

本開発技術において、多数の IoT 機器を一斉に制御するため、制御する送信者（サーバ等）と各 IoT 機器の間の個別通信を考えるのでなく、ブロードキャスト通信による 1 対多通信を取り入れたシステム設計になっています。放送型認証方式では、送信者がネットワ

ーク上のすべての IoT 機器に制御コマンドをブロードキャスト通信により一斉送信し、指定された機器のみがそのコマンドを実行可能になります。このような遠隔制御システムの設計は、IoT 時代のニーズと(Beyond) 5G の多数同時接続通信のニーズに応える技術となっています。

【標準化に至る道筋】
本研究成果である放送型認証技術の提案を柱として、そのユースケース分析を含めた国際標準化提案を行い、2022 年 5 月に ITU-T SG17 会合において新規課題 TR.ba-iot（技術レポート）として承認されました。そして 2022 年 8 月、2023 年 2 月に開催された ITU-T SG17 課題６会合において、
TR.ba-iot(Broadcast authentication schemes for IoT system)の草案とその改善に関する寄書を提出し、2023 年 9 月に提案が Technical Report として承認され、2024 年 2 月に正式に発行されました。

【今後の展開】
本研究成果は、多くの多種多様な IoT 機器を安全・簡便・瞬時に制御することが必要なシーンで利活用できることが期待でき、例えば、スマートファクトリー、スマートホーム、重要インフラ監視システム等で利活用が期待できます。

【謝辞】
本研究成果は、総務省の電波資源拡大のための研究開発(JPJ000254)「電波の有効利用のための IoT マルウェア無害化/無機能化技術等に関する研究開発（研究代表者　横浜国立大学先端科学高等研究院　IAS 客員教授 中尾康二)」(令和 2 年～4 年)において実施した成果です。この場をお借りして関係者の皆様に深く感謝申し上げます。

（参考文献）今回の国際標準化技術の基盤となる放送型認証方式（Broadcast Authentication）の技術開発に関わる学術論文は以下の通りです。

- Yoshinori Aono and Junji Shikata, “Anonymous Broadcast Authentication with Logarithmic-order Ciphertexts from LWE”, Cryptology and Network Security, The 22nd International Conference on Cryptology and Network Security (CANS 2023), LNCS 14342, pp.28-50, Springer, 2023. DOI: 10.1007/978-981-99-7563-1_2
- Yohei Watanabe, Naoto Yanai, and Junji Shikata, “IoT-REX: A Secure Remote-Control System for IoT Devices from Centralized Multi-Designated Verifier Signatures”, Information Security Practice and Experience, The 18th International Conference on Information Security Practice and Experience (ISPEC 2023), LNCS 14341, pp. 105-122, Springer, 2023. DOI: 10.1007/978-981-99-7032-2_7

- Kazuhiko Minematsu, Junji Shikata, Yohei Watanabe, and Naoto Yanai, “Anonymous Broadcast Authentication with One-to-Many Transmission to Control IoT Devices,” IEEE Access, Volume 11, pp. 62955-62969, 2023. DOI: 10.1109/ACCESS.2023.3288337
- Hirokazu Kobayashi, Yohei Watanabe, Kazuhiko Minematsu, and Junji Shikata, “Tight Lower Bounds and Optimal Constructions of Anonymous Broadcast Encryption and Authentication”, Designs, Codes and Cryptography, Volume 91, pp. 2523-2562, 2023. DOI: 10.1007/s10623-023-01211-x
- Yohei. Watanabe, Naoto Yanai, and Junji Shikata, “Anonymous Broadcast Authentication for Securely Remote-Controlling IoT Devices”, The 35th International Conference on Advanced Information Networking and Applications (AINA 2021), pp. 679-690, Springer, 2021. DOI: 10.1007/978-3-030-75075-6_56

本件に関するお問い合わせ先
横浜国立大学 大学院環境情報研究院，先端科学高等研究院
教授　四方 順司
e-mail： shikata-junji-rb@ynu.ac.jp