6ZD-04

家庭用 IoT 機器のセットアップ手順に関する一考察

鈴木松卓　　寺田真敏
東京電機大学

1. はじめに

IoT(Internet of Things)技術の活用やスマートフォンの普及とともに，IoT 家電のような電球やスピーカ，プラグなどの家庭用 IoT 機器が広く流通し，販売され始めている．

IoT 機器のセキュリティ対策不備によるサイバー攻撃事案は 2016 年頃から報告されており，情報セキュリティ視点から IoT 機器を安全に利用するにあたって留意すべき事項を，ユーザや開発者視点から明らかにしていくことが急務であり，これを本研究の目的としている．

本稿では，IoT 家電のセットアップの際，多くはスマートフォンを通じて無線アクセスポイント(以下，AP)に接続しているが，その手順についてはユーザからは見えない部分であり，情報も少ないことに注目し，セットアップ手順に関するガイドラインの状況並びに，スマートプラグを対象にセットアップ時の手順を調査した結果を報告する．

2. IoT 機器開発におけるセキュリティガイドライン

IoT 機器開発に関するガイドラインは，IoT のセキュリティ対策全般に関するガイドラインと IoT 機器のセキュリティ設計に関するガイドラインがある．また，ガイドラインに基づく IoT 機器の認定制度[1]も始まっている．

(1) IoT のセキュリティ対策全般

総務省，経済産業省が作成した IoT セキュリティガイドライン[2]は，IoT 機器やシステム，サービスの関係者が取り組むべき IoT のセキュリティ対策の認識や関係者間の情報共有を促している．米国では，連邦政府機関が IoT 機器を利用する際にベンダに対して何を求めるべきかを NIST SP800-213[3]に記載している．

(2) IoT 機器のセキュリティ設計

IoT 機器セキュリティ要件・適合基準ガイドライン[4][5]は，IoT 機器を設計するうえで最低限守るべき要件と，それに基づいたセキュリティ機能要件の定義や検査手法について具体的に示している．IoT 開発におけるセキュリティ設計の手引き[6]は，セキュリティ設計を担当する開発者向けに，IoT のセキュリティ設計において行う脅威分析・対策検討・脆弱性への対応方法を解説している．米国では，IoT 機器製造企業が，実施すべきセキュリティ関連活動の推奨事項を NISTIR 8259[7]に示している．欧州では，消費者向け IoT 機器を開発・製造する関係者に向けて，製品の安全確保に関する規定を EN 303645[8]に記載している．

3. IoT 家電セットアップ手順の調査

本章では，スマートプラグを対象にセットアップ時の手順を調査した結果を報告する．

3.1 調査目的

IoT 家電のセットアップの際，多くはスマートフォンを通じて AP に接続しているが，手順に関する情報は開示されていないことから，次の視点から手順を明らかにする．

- セットアップフロー
- セットアップ時のセキュリティ対策

3.2 調査内容

(1)調査対象機器

メーカーごとにセットアップ手法が異なるか調査するため，入手しやすく，多様なメーカーが販売しているスマートプラグを対象とした(表 1).

(2)調査方法

スマートプラグとスマートフォン間の通信を調査するため，調査ネットワークを構築した(図 1)，観測 PC とスマートフォンでそれぞれパケットキャプチャし、収集したパケットデータはログサーバとしての役割を果たす観測 PC に集約保存した後，解析をする．

- 観測 PC：ネットワークアナライザソフトウェアの Wireshark を使用し，無線 LAN 通信のパケットキャプチャをする．
- スマートフォン：無線 LAN 通信と Bluetooth 通信のパケットキャプチャをする．無線 LAN 通信の場合，スマートフォン上で tcpdump を利用する．Bluetooth 通信の場合，開発者オプションにある Bluetooth HCI スヌープログを有効化し通信をキャプチャする．

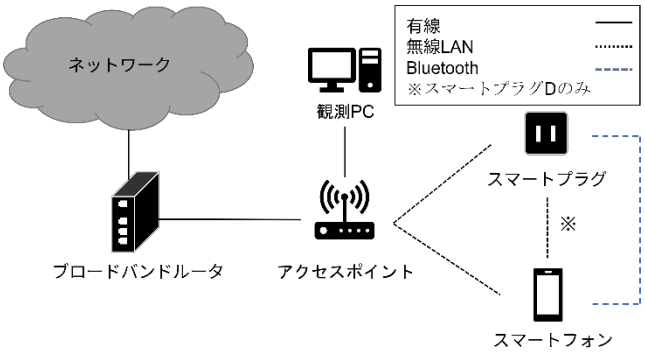

図 1　調査ネットワーク構成

3.3 調査結果

各スマートプラグのセットアップのフローを図 2 に，AP 情報の受け渡し方法と暗号化の有無を表 2 に示す．今回の調査結果から，セットアップの流れはある程度似通ったフローを採用している．その一方，セキュリティ対策については，実装差がみられる．具体的には，スマートプラグ B では接続先 AP 情報と専用アプリをスマートフォンで使用するうえで必須のユーザアカウント情報を Bluetooth 通信で受け渡しており，それぞれの値は Base64 でエンコードしている．スマートプラグ D では，プラグ自身が立てた AP にスマートフォンが接続してセットアップをするが，通信が暗号化されていないため接続先 AP 情報が読み取れる．

Considerations on Configuration Methodology for Home IoT Devices
Matsutaka Suzuki and Masato Terada, Tokyo Denki University

表 1　調査対象のスマートプラグ一覧

	スマートプラグ A	スマートプラグ B	スマートプラグ C	スマートプラグ D
販売開始年	2020 年	2020 年	2021 年	2021 年
使用通信規格	IEEE 802.11 b/g/n, Bluetooth Low Energy	IEEE 802.11 b/g/n, Bluetooth 4.2	IEEE 802.11 b/g/n	IEEE 802.11 b/g/n
接続可能 AP 暗号化方式	記載なし	WPA/WPA2	記載なし	WPA/WPA2
操作方法	専用アプリ，本体操作	専用アプリ，本体操作	専用アプリ，本体操作	専用アプリ，本体操作

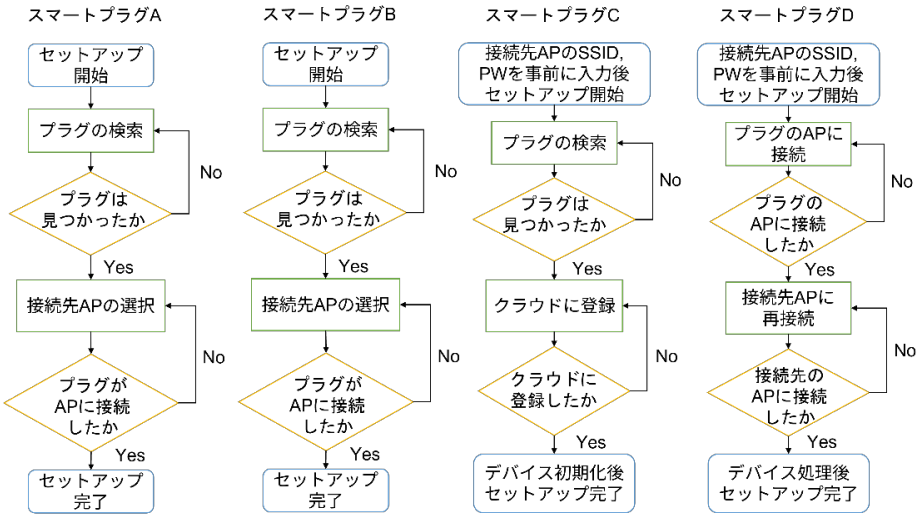

図 2　各スマートプラグのセットアップフロー

表 2　各スマートプラグの AP 情報受け渡し手法

	AP 情報の受け渡し方法	暗号化
スマートプラグ A	Bluetooth	あり
スマートプラグ B	Bluetooth	なし
スマートプラグ C	無線 LAN	あり
スマートプラグ D	無線 LAN	なし

4. 考察

(1)各スマートプラグのセットアップ手順について

- 図 2, 表 2 から Bluetooth 通信を利用した AP 情報の受け渡し方法はメーカーによって差異はほとんど無いため, 設計方針として通信暗号化の有無に焦点が当たる.
- Bluetooth，無線 LAN 通信など，IoT 家電のセットアップの通信方法が異なるだけではなく，セキュリティ対策についてもばらつきがある.
- IoT 家電のセットアップの工程は，限られた環境かつ限られた時間で実施することが大部分を占めるため，悪用される危険性は低いものの，ユーザが安心して使うために，セキュリティ対策を実施すべきである.

(2)ガイドラインの整備について

- 図 2，表 2 から無線 LAN 通信を利用した AP 情報の受け渡し方法はメーカーの設計方針に依存している. 発行済の IoT 機器開発におけるセキュリティガイドラインでは，設計や実装時点でのセキュリティ対策の考え方について触れられていることから，実装上で考慮する点についても開発手引きとして整備していくと良いと考えている.

5. まとめ

本稿では，IoT 家電のうち，それぞれメーカーが異なるスマートプラグ 4 種類を対象に，セットアップ時の手順を調査した. 調査の結果，メーカーによって異なるセットアップ手順を採用しており，具体的なセットアップ手順に関するセキュリティ面での改善点があることを確認した. 今後は IoT 家電を情報セキュリティ視点から安全に利用するために，調査対象機器の拡大，セットアップ手順だけではなく，IoT 家電運用フェーズでのセキュリティ対策についての調査を通して，IoT 家電のセキュリティ対策の改善をしていく.

参考文献

[1] CCDS，”CCDS サーティフィケーションプログラム実施概要”， https://ccds.or.jp/certification/index.html
[2] 総務省，”IoT セキュリティガイドライン ver 1.0”, https://www.soumu.go.jp/main_content/000428393.pdf
[3] NIST，” SP800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements”, https://csrc.nist.gov/publications/detail/sp/800-213/final
[4] CCDS, ”IoT 機器セキュリティ要件ガイドライン 2023 年版_ver1.0”, https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2023_v1.0_jpn.pdf
[5] CCDS，” IoT 機器セキュリティ要件_適合基準ガイドライン 2023 年版_ver1.0”, https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_Criteria_2023_v1.0_jpn.pdf
[6] IPA，”IoT 開発におけるセキュリティ設計の手引き”, https://www.ipa.go.jp/files/000052459.pdf
[7] NIST，” NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers”, https://csrc.nist.gov/publications/detail/sp/800-213/final
[8] ESTI，” EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements”, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf