

家庭を模した IoT 家電ハニーポットを用いた 攻撃者の行動の観測および検証 Analyzing attacker's behavior using IoT home appliances honeypot

大塚瑠莉*
Ruri Otsuka

吉岡克成††
Katsunari Yoshioka

岡田晃市郎‡
Koichiro Okada

キーワード ハニーポット, IoT

あらまし

社会全体における IoT 機器の増加に伴い、一般家庭においても IoT 家電の普及が広がっている。IoT 家電は、部屋に設置したカメラの映像を外出先から確認したり、外出先から室内のエアコンの電源を入れるなど、遠隔操作を用いることで外出先から室内の機器に対する制御ができるものが多い。遠隔操作には主にクラウドネットワークが利用され、クラウドネットワークを通じた操作は利便性が高い一方、攻撃者に乗っ取られて操作をされてしまう危険性がある。しかし乗っ取られた場合どのような意図で何をされるかは、現在不明な部分も多い。そこで本研究では、家庭で使用される IoT 家電は直接クラウドネットワークに接続されるのではなく、必ず市販の無線ルータを経由することに着目し、無線ルータを乗っ取った攻撃者がローカルネットワーク内の家電に対してどのような攻撃をするのか知ることを目的とする。そのため、攻撃者の行動順序の仮説を立て検証を行うこととした。検証は、家庭を模した IoT 家電ハニーポットを構築し、運用観測することで得られた攻撃パケットを分析することで行う。なお、本ハニーポットの特徴として、応答機能として実際の市販されている家電を使用してい

る。

本講演では、攻撃者の攻撃順序が、(1) 無線ルータを乗っ取る、(2) ローカルネットワークに対し探索行為を行う、(3) 応答が返ってきたものに対して攻撃をする、という3段階で行われると仮説を立て、それらについての検証を行う。この検証により、IoT 家電使用に伴った家庭内のルータのセキュリティレベルを上げる重要性を主張する。

* 三菱電機株式会社, 神奈川県鎌倉市大船 5-1-1, Mitsubishi Electric Corporation, 5-1-1, Ofuna, Kamakura, Kanagawa

† 横浜国立大学大学院環境情報研究院, 神奈川県横浜市保土ヶ谷区常盤台 79-7, Graduate School of Environment and Information Sciences, Yokohama National University, 79-7, Tokiwadai, Hodogaya, Yokohama, Kanagawa

†† 横浜国立大学先端科学高等研究院, 神奈川県横浜市保土ヶ谷区常盤台 79-5, Institute of Advanced Sciences, Yokohama National University, 79-5, Tokiwadai, Hodogaya, Yokohama, Kanagawa

‡ 株式会社レインフォレスト, 東京都杉並区成田西 2-8-10, Rainforest Corporation, 2-8-10, Naritanishi, Suginami, Tokyo