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

IoT 環境における動的セキュリティ管理システム
Dynamic Security Management System in IoT Environment

竹内　佑樹 * 金井　敦 * 谷本　茂明 † 佐藤　周行 ‡
Yuki Takeuchi Atsushi Kanai Shigeaki Tanimoto Hiroyuki Sato

キーワード IoT, 動的セキュリティ, ネットワークセキュリティ

あらまし

IoT デバイスが普及し，より様々な分野で使用されている一方で，IoT デバイスに対するサイバー攻撃への対策が急務である． 実際，IoT デバイス群をターゲットとしたサイバー攻撃は増加しているとされている．そのため，必要なセキュリティ対策をしっかりと講じることが肝要であるが，IoT デバイスはハードウェアの特性上，セキュリティ対策に大きくリソースを割くことは難しく，従来の PC のようなセキュリティ対策ソフトをインストールする方法は向いていない．また，IoT デバイスでは可用性が最重要視されており，いかに稼働状態を維持しながら状況に応じたセキュリティ対策を行えるかが重要である．先行研究では，ネットワークルータに通信内容を監視する機能を持たせ，必要によっては通信をすべて遮断して疑似的に隔離したり，あるいは通信内容から相手がボットかどうかを判別したりする [?] ものや，機械学習を使って SDN でボットネットを検知する手法 [?] などがあげられる．

本研究では，SDN の技術を利用しつつ，IoT のサービス可用性に重点を置き，より軽量で動作するプロトコルを使用することでネットワークへの負荷軽減を図った IoT セキュリティモデルとして動的セキュリティ管理システムを提案する．このシステムでは，物理環境・ネットワーク環境の変化を検知し，動的にセキュリティレベルを変化させることによってサービス稼働状態を維持しつつもネットワーク上のデバイスをサイバー攻撃から防御することを目的とし，図 1 に示すようなプロトタイプを作成した．物理環境・ネットワーク環境双方の変化に応じて警戒度を動的に変更する．警戒度が上がった際には，SDN の技術を使用して，あらかじめ登録された通信先以外にデータを渡したり，アクセスを許可したりできなくし，よりセキュアなネットワーク環境を作ることができるモデルである．当該モデルについて，動作実験を行い，警戒レベルの反応速度や処置が正しく適用されているかなどの性能について評価する．

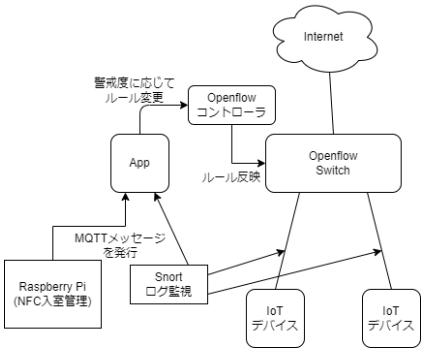

図 1 プロトタイプ環境図

参考文献

[1] C.Dietz et al., “IoT-botnet detection and isolation by access routers”, in *Proceedings of 9th International Conference on Network of the Future (NOF)*, 2018, pp.88-95.

[2] Shogo M, et al.,“A Botnet Detection Method on SDN using Deep Learning”, in *Proceedings of 2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019, pp.1-6.

* 法政大学理工学研究科, 東京都小金井市梶野町 3-7-2, Graduate School of Science and Engineering of Hosei University , Koganei City, Tokyo
† 千葉工業大学社会システム科学部, 千葉県習志野市津田沼 2-17-1, Social Systems Svience of Chiba Institute of Technology, Narashino City, Chiba
‡ 東京大学情報基盤センター, 千葉県柏市柏の葉 6-2-3, Information Technology Center, the University of Tokyo, Kashiwa City, Chiba