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

NS3 を用いた IoT マルウェア感染拡大・攻撃シミュレータの実装
Implementation of an IoT malware infection spread and attack simulator using NS3

石田 裕貴 * 前田 泰浩 *
Yuki Ishida Yasuhiro Maeda

キーワード IoT マルウェア, Mirai, シミュレーション

あらまし

IoT(Internet of Things) 機器の普及に伴い, 脆弱なパスワードなどを設定された IoT 機器に感染する, Mirai を代表とした IoT マルウェアの活動が活発化している. Mirai は初期設定で運用されている Linux ベースの IoT 機器に対して, Telnet などを介して感染して, ボットネットを構築するマルウェアであり, 2016 年には国内外で複数回の大規模なサービス妨害攻撃が確認されているマルウェアである. Mirai はソースコードが公開されているため, 実環境における評価は積極的に行われているが, 大規模環境での評価している研究は少ない. 大規模環境による実験を実環境で行うには多数の機器が必要となるが, 設置や実験に要するコストの観点から実用的ではない. しかし, マルウェアの感染拡大挙動を把握することは, IoT 機器に迫る脅威を理解するために重要である. そこで本稿では Mirai の公開されているソースコードや動作を解析した論文を元に動作をモデル化し, ネットワークシミュレータ NS-3 を用いて, 多様なネットワーク構成で大規模 IoT 機器環境の再現が可能な感染拡大・攻撃シミュレータを実装した. 本シミュレータの評価では, 中規模から大規模を想定した環境下で, シミュレータの実用性の観点からシミュレーションに要する時間及び攻撃性能の評価を行なった.

* 株式会社セキュアブレイン〒 102-0094 東京都千代田区紀尾井町 3 – 12 紀尾井町ビル 7F. SecureBrain Corporation Kioicho Bldg 7F, 3-12 Kioicho, Chiyoda-ku, Tokyo 102-0094