平成28年度 情報工学コース卒業研究報告要旨

高田・本田 研究室	氏　　名	長 柄　啓 悟
卒業研究題目	組込みシステム向けマルウェアMiraiの攻撃性能評価	

近年IoT機器が注目され，多種多様な組込みシステムがネットワークに繋がるようになり，それら機器の脆弱性が明らかになっている．このような組込み機器は，製品の規模やアーキテクチャの多様性，資源の乏しさ，使用期間の長さ，コストの制約からセキュリティが十分に考慮されていないことがある．また，LinuxやTCP/IPといった既存技術の流用と共に既存の脆弱性も引き継がれる．脆弱性を悪用される具体例として，IoTマルウェアであるMiraiが挙げられる．Miraiとは，組込みLinuxが動作する，デジタルビデオレコーダーやネットワークカメラ，家庭用ルータなどのIoT機器を対象にボットを感染させ，DDoS攻撃を行うマルウェアである．2016年9月のセキュリティブログへの攻撃や同年10月のDNSサーバープロバイダであるDyn社への攻撃では，史上最大規模である620 Gbpsの攻撃が観測された．この規模の攻撃を防ぐのにかかるコストは莫大であり，DNSサーバが攻撃にあうとそれを利用する多くのサービスも同時に使用できなくなってしまう．また，同年9月にMiraiの作者がソースコードを公開したことにより，これを利用した亜種が確認され，今後も脆弱なIoT機器を対象としたマルウェアの増加が懸念される．

このような被害をなくすためには，組込みシステムに関する脆弱性がどのようなものかを明らかにする必要がある．組込みシステムに関する脅威は数多く報告されているが，実際にその量や種類を把握することは難しい．組込みセキュリティの第一歩として，既存の脅威や脆弱性を把握する必要がある．また，IoTマルウェアの猛威を防ぐためには，主たるMiraiがどのように動作するのか解析する必要がある．Miraiが悪用する脆弱性や，その攻撃手法を調査し，MiraiによるDDoS攻撃の危険性を把握し対策しなければならない．

本研究では，組込みシステムにどのような脆弱性があるかを知るために，世界最大規模のCVEや，日本を中心にしたJVN iPediaといった脆弱性データベースを対象として調査を行なった．脆弱性データベースのエントリ情報から組込みシステムに関する脆弱性の情報について抽出と分類を行なった．さらに，具体的な脆弱性の調査として，公開されているMiraiのソースコードを元に攻撃性能を評価した．予備実験としてVM環境上でMiraiの動作環境を構築し，実際の通信の様子や攻撃の流れを確認し，攻撃の性能を計測した．次に，ローカルネットワーク下での実機実験として複数の組込みボード（odroid-c2）を用いて，VMと同様にMiraiの動作環境を構築し，攻撃の性能や影響の調査を行なった．攻撃性能の調査では，攻撃対象に対して送られてくるパケット総数を，Wiresharkで観察するという手法を用いた．他にも，リアルタイムOS（TOPPERS/ASP）や組込みシステム向けTCP/IPスタック（LwIP）からなるhttpサーバが動作する静的な組込みシステムのプロトタイプを対象に攻撃を行い，その影響を調査した．ボットが動作している実機のCPUやメモリ，帯域の様子についても調べ，これらの調査情報を元にMiraiの感染や攻撃を防ぐ対策を検討した．

脆弱性データベースの調査では，年々組込みシステムに関する脆弱性の登録数が増加していることが判明した．Miraiの攻撃性能は，攻撃を行うボットである組込みボードが1台で最大約248 Mbpsのパケットを送信していることや，台数に応じて攻撃量が比例して増加することが確認でき，約2500台のボットがあれば，前述した実際の620 Gbpsの大規模攻撃が十分に可能であると考えられることを確認した．プロトタイプを対象に攻撃を行った場合，httpサーバの可用性が損なわれることを確認した．これらにより，組込みシステムにおける脅威や脆弱性に対するセキュリティの重要性が再確認された．