平成28年度 情報工学コース卒業研究報告要旨

村瀬勉 研究室	氏　　名	伊 藤　克 恭
卒業研究題目	IoT向けプロトコルのためのハニーポットシステム	

近年あらゆる機器をインターネットに繋げる思想であるIoTが急速に普及しており，総務省の推測では，2020年には530億台ものIoT端末が利用されるようになる．そのような状況のもと，IoTシステムに対する攻撃の発生が懸念される．IoT端末には，低消費電力や低オーバヘッドを求めて軽量プロトコルを使うものがある．IoTシステムの動作に関わるような攻撃を防ぐためには，IoT向けのプロトコルを用いた攻撃の手段や狙いを観測し，知る必要がある．

そこで本研究では，IoT向けプロトコルを利用した攻撃を観測するためのハニーポットシステムについて提案する．本研究では，IoT向けプロトコルの例として公共交通の位置情報サービスや心臓ペースメーカーのモニタリングなどで使われるMQTTに着目してハニーポットを構築し，攻撃を観測・収集するシステムを構築した．MQTTは，ブローカと複数のクライアントが通信を行うメッセージプロトコルである．クライアントはブローカに対してトピックを指定してメッセージの送信（パブリッシュ）と，欲しいトピックについてメッセージの要求（サブスクライブ要求）を行う．トピックは内容ごとにまとめられ，文字列の階層構造を用いて表される．MQTTを用いて，各地のセンサデータを遠隔で監視するIoTシステムの一例を図1に示す．

本システムでは，長期間IPアドレスが固定して運用され，攻撃が集まると考えられるブローカを外部に接続する．また，本物のIoTシステムが動作しているように見せかけるために本物の温度・湿度・気圧の値を登録し，遠隔で監視できるIoTを模擬したシステムとした（図2）．ハニーポットは，攻撃を受けても他のネットワークに影響を与えないように工夫する必要がある．本研究では，MQTTブローカとしてオープンソースのmosquittoを利用し，ソースコードに変更を加えることでハニーポットが攻撃を受けても外部に攻撃が及ばない構成とした．また外部ネットワークだけでなく，ハニーポットシステムの繋がる管理用ネットワークにも配慮し，仮想環境を上手く使うことで攻撃が侵入しないようにした．また，解析を容易に行うために，1日ごとのpcapファイルからMQTT接続とpingの送信元を列挙する解析プログラムも作成した。

構築したMQTT用ハニーポットをグローバルアドレス空間に設置し，ブローカの通信を2ヶ月間収集・解析を行った．2ヶ月間観測した結果，TCPの通信を用いて攻撃とみられるものを観測できたのは4件，pingを用いて動作を確認されたのは437件であった．

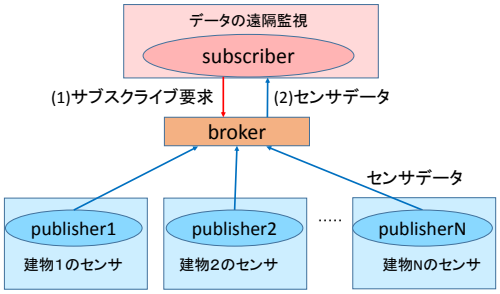

図1 MQTTを用いたセンサの遠隔監視

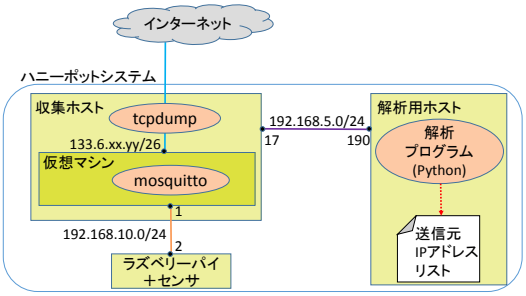

図2 MQTT向けハニーポット