様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ５ 月 １９ 日現在

機関番号：３２７１４
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ０５０１２

研究課題名（和文）免疫的攻撃検知によるスマート公共サービスのレジリエンス強化

研究課題名（英文）Enhancing the Resilience of Smart Public Services by Immunity-Based Attack Detection

研究代表者
岡本　剛（Okamoto, Takeshi）

神奈川工科大学・情報学部・教授

研究者番号：９０３５０６７８

交付決定額（研究期間全体）：（直接経費）　　1,400,000円

研究成果の概要（和文）：本研究では、研究代表者らが提案した免疫的攻撃検知の技術がスマート化された公共サービスの妨害攻撃に対して有効であるかを明らかにするため、公共サービス向けの免疫的攻撃検知の設計・実装・テストを行った。その結果、免疫的攻撃検知は極めて高い検知精度でサービス妨害攻撃を防止できることを示した。また、通信データのサイズを５キロバイトに制限すれば、オーバーヘッドがほとんどないことも示した。最後に、メモリリークやCPUリソース消耗の脆弱性に対する攻撃と機械学習に対する攻撃の対策と課題を示した。

研究成果の学術的意義や社会的意義
研究成果の社会的意義は免疫的攻撃検知の技術がIoTでスマート化された公共サービスのレジリエンスを強化できることを示したことである。本研究のレジリエンスとは、攻撃によって停止したサービスを自動的に回復する能力と二度目以降の類似の攻撃を未然に検知・防止する能力のことを指す。この回復力によって人手を介さずにサービスを持続できるようになる。研究成果の学術的意義は、従来のヒューリスティックな検知技術と機械学習による検知技術を組み合わせることによって、攻撃の検知・防止だけでなくサービスの回復までカバーする技術を実現したことである。

研究成果の概要（英文）：In order to determine the effectiveness of our previously proposed technique of “immunity-based attack detection” against denial-of-service attacks in smart public services with IoT, we redesigned, implemented, and tested immunity-based attack detection for public services. The results showed that immunity-based attack detection can prevent denial-of-service attacks with extremely high detection accuracy. We also showed that there is almost no overhead if the size of the communication data is limited to 5,000 bytes. Finally, we demonstrated the practical issues such as memory leaks and CPU resource exhaustion and the feasibility of attacks against machine learning.

研究分野：情報セキュリティ

キーワード：MQTT　DoS攻撃　機械学習　スマートシティ　IoT　レジリエンス　侵入検知　脆弱性

１．研究開始当初の背景

（1）スマートシティの実現に向けて、社会インフラや公共サービスのスマート化が進められている。スマートシティは従来の社会インフラや公共サービスを効率化し、環境にも配慮しながら、人々の生活の質を高めることが期待されている。その一方で、スマートシティに対するサイバー攻撃が懸念されている。その最大の脅威が未知の脆弱性に対するサイバー攻撃である。なぜなら、未知の脆弱性に対するサイバー攻撃を検知できたとしても、その攻撃を防止する技術が確立されていないからである。

（2）未知の脆弱性に対するサイバー攻撃によって発生したサービス不能の状態からサービスを回復させるにはセキュリティアナリストなど専門家による対応が必要であり、数分から数日のダウンタイムが発生する。機械学習による検知が世界中で研究されているが、検出精度が十分ではないため、専門家によるサポートが不可欠である。特に防災サービスの妨害攻撃は人の生命を脅かすリスクがあるため、ダウンタイムの最小化などレジリエンス（回復力）の強化が喫緊の課題である。

（3）研究代表者は、サービス不能の状態を手がかりにして攻撃データを特定して機械学習でその攻撃データを学習する免疫的攻撃検知という技術（図1）を開発してきた。免疫的攻撃検知は、たとえ最初の攻撃を防止できなくても、二度目以降の類似の攻撃に対してサービスを止めることなく未然に防止するレジリエンス強化技術である。本研究課題では免疫的攻撃検知の技術がスマート化された公共サービスのレジリエンスを強化できるかを明らかにする。

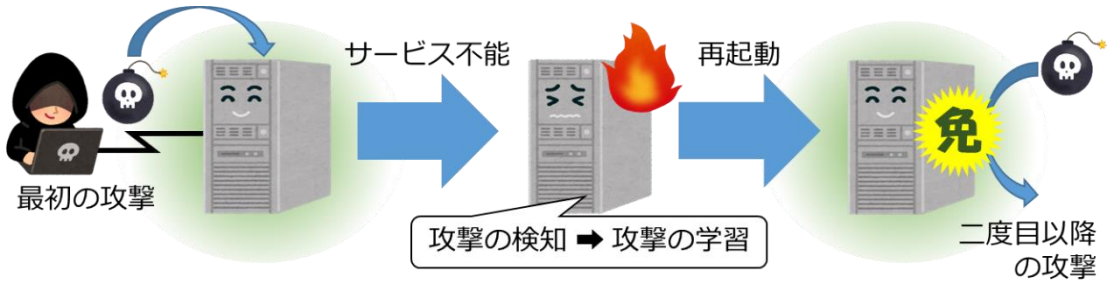

図１　免疫的攻撃検知のイメージ図

２．研究の目的

（1）公共サービスのスマート化において中心的役割を果たす技術が IoT である。IoT を活用したサービスには、IoT 機器の乗っ取りやサーバのサービス妨害など様々な脅威が存在する。本研究は、IoT サービスのサーバに焦点を絞り、サーバのサービス妨害に対するレジリエンスを免疫的攻撃検知によって強化することが目的である。公共サービスには様々なサービスが存在するが、本研究では、高いレジリエンスが求められる防災サービスを対象にする。ただし、DDoS 攻撃のようにサーバのネットワーク帯域を消費させる攻撃は既存の方法で対処することとする。

３．研究の方法

（1）本研究は、研究代表者らが開発してきた免疫的攻撃検知モジュールを防災サービスに応用することによって、免疫的攻撃検知が防災サービスの妨害をどれくらい防止できるかを明らかにする。具体的には水害の予測や警報のための水害対策サービスを想定する。このサービスには、水位を計測する水位センサー、センサーの計測情報を中継する MQTT ブローカーとこれらをつなぐ IoT ゲートウェイが含まれる（図 2）。水位の計測には安価な超音波距離センサーを使う。IoT ゲートウェイには少ない消費電力で広いエリア（半径 2～5Km）をカバーできる LoRaWAN ゲートウェイを使う。MQTT ブローカーにはオープンソースの Eclipse Mosquitto を使う。本研究は免疫的攻撃検知を Mosquitto ブローカーに組み込んで、免疫的攻撃検知がレジリエンスをどれくらい強化できるかを明らかにする。

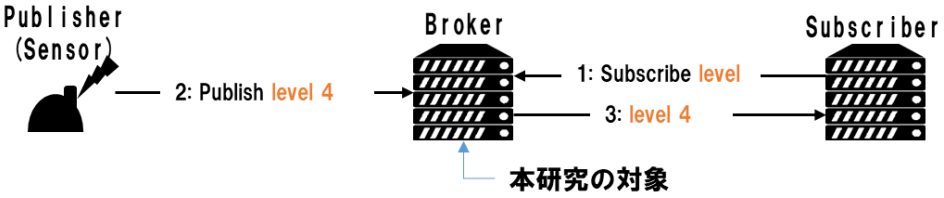

図２ 水害対策サービスのテストベッド

（2）次に MQTT ブローカーの脆弱性を攻撃するモジュールを開発する。検知精度の評価には脆弱性に対する攻撃のテストが不可欠である。既知の脆弱性に関しては Metasploit Framework など既存のペネトレーションツールを使うことが多いが、Metasploit Framework には Mosquitto の脆弱性に対するテストモジュールがなかったため、Mosquitto の公開リポジトリに含まれる脆弱性テストスクリプトを改造して攻撃モジュールを開発する。

（3）ここから次に述べる 3 つの実験を繰り返し、免疫的攻撃検知の機能と性能の改善を行う。まず、免疫的攻撃検知で使用する機械学習アルゴリズムの検知精度をシミュレーション評価により比較して、最適なアルゴリズムを選ぶ。次に、Mosquitto ブローカーの免疫的攻撃検知の機能を設計してプロトタイプを実装する。最後に、開発した攻撃モジュールで実機の Mosquitto ブローカーを攻撃してプロトタイプの検知精度がシミュレーション評価と同等になることを確認する。検知精度を落とさずにプロトタイプのオーバーヘッドを抑える方法も検討する。

4．研究成果

（1）Mosquitto ブローカーに対する免疫的攻撃検知の有効性を確認するため、免疫攻撃検知が対象とする Mosquitto ブローカーの脆弱性を洗い出した。その結果、2021 年 3 月時点で該当する脆弱性（リモートからブローカーの可用性を侵害できる脆弱性）は 4 件あった。ここで、2013 年リリースの MQTT のバージョン 3 の機能に含まれる脆弱性と 2019 年リリースのバージョン 5 に含まれる脆弱性に分けて、プロトタイプの実装では、まず最も広く普及していると予想されるバージョン 3 系の脆弱性を対象にした。これをプロトタイプⅠとする。プロトタイプⅠの性能を評価した結果、検知精度と検知速度のバランスが最もよい機械学習アルゴリムは LightGBM であることを確認した（図 3）。CVE-2018-12543 と CVE-2019-11779 の脆弱性への攻撃に対して、免疫的攻撃検知の検知精度は平均で 99.72%（真陰性率＝99.77%、真陽性率＝99.67%）であった。また、MQTT の最大メッセージサイズを 5,000 バイト未満に制限すれば、プロトタイプⅠのオーバーヘッドはほとんどなかった（図 4）。これらの結果は、当初の想定よりも優れた結果である。

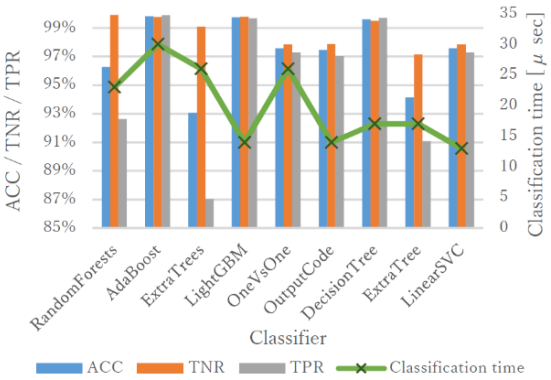

図 3　機械学習アルゴリズムの比較

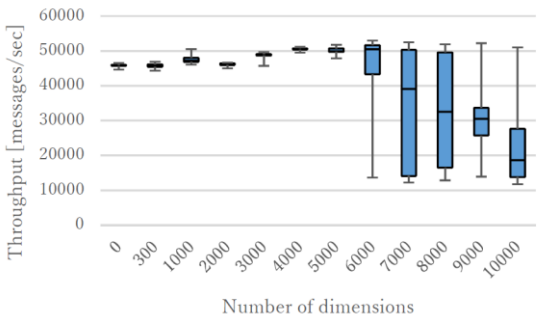

図 4　メッセージサイズとスループット（プロトタイプⅠ）

（2）次にプロトタイプⅠが MQTT バージョン 5 系の脆弱性に対する攻撃を検知できるかを検証した結果、攻撃を検知できるが検知するタイミングが実際に攻撃を受けたタイミングではないため、攻撃メッセージを正しく学習できなかった。この問題は Use-After-Free（UAF）の脆弱性が原因であり、この脆弱性を正確に検知することによって解決できる。そこで、UAF などメモリアクセスのバグを高精度で検知できる AddressSanitizer をブローカーに組み込み、UAF を正確に検知できるようにした。さらに、AddressSanitizer が UAF を検知したとき、攻撃メッセージを特定する仕組みを導入した。これをプロトタイプⅡとする。プロトタイプⅡを実機で動作確認した結果、想定通り、正しく攻撃メッセージを特定できることを確認した。検知精度に関しては、CVE-2019-11778 への攻撃は 99.33%の精度で、Issue-1244 のバグへの攻撃は 97.28%の精度で検知・防止できることを確認した。オーバーヘッドに関しては、プロトタイプⅠと比べて最大メッセージサイズの限界値が 3,000 バイトまで低下した（図 5）。これは攻撃メッセージの探索処理が原因と考えられる。

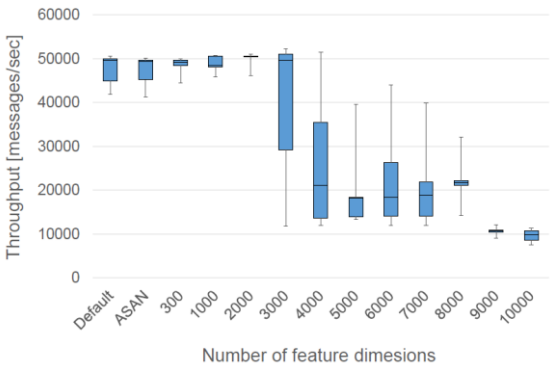

図 5　メッセージサイズとスループット（プロトタイプⅡ）

（3）本研究の総まとめとして、2022 年 11 月時点でリモートから Mosquitto ブローカーの可用性を侵害できる脆弱性を洗い出した。2021 年に 4 件の脆弱性が新しく公開されたため、プロトタイプⅡで検知できるかを検証した。その結果、CVE-2021-28166 を 99.99%の精度で、CVE-2021-34432 を 99.88%の精度で検知できることを示した。残り 2 件の脆弱性（CVE-2021-34431 と CVE-2021-41039）に関しては研究成果（5）で述べる。研究成果（1）と（2）で評価した脆弱性と 2021 年の 2 件の脆弱性への攻撃に対しては、99.37%の精度で検知できることを示した。免疫的攻撃検知のオーバーヘッドに関しては、MQTT メッセージの大きさが 5,000 バイト未満なら、ほとんど影響ないことを確認した（図 6）。研究成果（2）では 3,000 バイトが限界値であったが、MQTT メッセージサイズの限界値を 5,000 バイトまで引き上げることができた要因は CPU のアップグレード（AMD Ryzen Threadripper 2960X → 3960X）である。CPU を 1 世代新しくするだけでもオーバーヘッドの問題を大幅に緩和できることを示した。

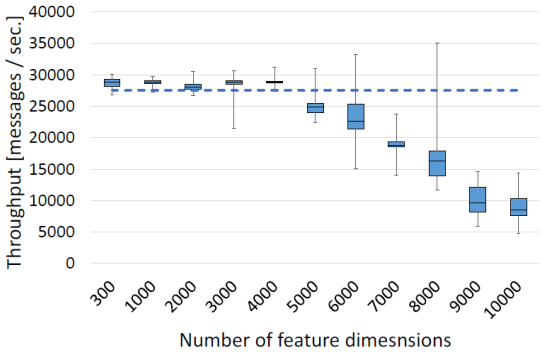

図 6　メッセージサイズとスループット
（プロトタイプⅡ＋Ryzen Threadripper 3960X）

（4）これらの研究成果から、免疫的攻撃検知の機能を備えた Mosquitto ブローカーは、次の原因によって引き起こされる可用性侵害の脆弱性に対して 99.37%以上の精度で攻撃を検知してレジリエンスを強化できることを明らかにした。括弧内の数字は 2022 年 11 月時点の Mosquitto ブローカーの CVE ID の件数である。
①アサーションエラー（1 件）
②Use-After-Free（2 件）
③スタックオーバーフロー（1 件）
④NULL ポインター参照（2 件）

（5）免疫的攻撃検知の技術は「1 つの攻撃メッセージによってプロセスが強制的に停止させられること」を前提としているため、複数の攻撃メッセージを組み合わせることによってプロセスを停止させる攻撃を検知できない。具体的には、メモリリークや CPU リソース消耗など攻撃メッセージを繰り返し送り続けられることによって少しずつリソースが消費され、サービスが停止する攻撃を検知できない。Mosquitto ブローカーにおいて、これに該当する脆弱性はメモリリークの脆弱性（CVE-2017-7654 と CVE-2021-34431）と CPU リソース消費の脆弱性（CVE-2021-41039）の計 3 件であることを確認した。当初はこれらの脆弱性に対する攻撃は免疫的攻撃検知の対象外として捉えていたが、プロトタイプⅡで実装した UAF に対する攻撃検知の仕組みを利用すれば、メモリリークによる攻撃も検知できると考えられる。また、CPU リソース消耗に関しては、異常検知の仕組みにより対処可能であると考えられる。具体的には各メッセージの処理に必要な時間を設定して、事前に設定した時間を超える場合に攻撃として検知して学習させる方法である。

（6）今後に想定されるリスクとして機械学習に対する攻撃（転移攻撃、回避攻撃、汚染攻撃）を考察して、各攻撃の対策と課題を示した。転移攻撃に関しては、免疫的攻撃検知の仕組みを論文で公開しているため、代替モデルの生成が可能である。回避攻撃に関しては、免疫的攻撃検知の機能は動的に攻撃データと正常なデータを学習するので、一定の耐性があることを研究成果（1）から（3）において確認している。汚染攻撃に関しては、偽陰性と偽陽性を引き起こす攻撃が考えられるが、免疫的攻撃検知には類似の攻撃を動的に学習する仕組みがあるため、偽陰性を引き起こす攻撃に対して、もともと耐性がある。一方、偽陽性を引き起こす攻撃に関しては事前学習データ（事前に学習させることができる正常なデータ）を増やすことによって、偽陽性を減らせることを確認している。なお、耐性に関する性能は定量的な評価を必要とする。

＜引用文献＞

① 岡本　剛、MQTT ブローカーのための免疫的攻撃検知の試作、情報処理学会研究報告、2021(CSEC-92)、2021、1－8
② 岡本　剛、免疫的攻撃検知による MQTT ブローカーのレジリエンス強化 ～ Use-After-Free の脆弱性に対する DoS 攻撃の検知と防止 ～、信学技報、121(433)、2022、212－217
③ Takeshi Okamoto, Prevention of DoS Attacks on Use-After-Free Vulnerabilities in Mosquitto, Procedia Computer Science, 207, 2022, 1763－1772
④ 岡本 剛、機械学習による適応的サイバー攻撃検知の性能評価、JSAI 合同研究会 2022 第 1 回安全性とセキュリティ研究会予稿集、SIG-SEC-01-05、2022、33－40

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Okamoto Takeshi	４．巻 207
２．論文標題 Prevention of DoS Attacks on Use-After-Free Vulnerabilities in Mosquitto	５．発行年 2022年
３．雑誌名 Procedia Computer Science	６．最初と最後の頁 1763～1772
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.procs.2022.09.234	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 岡本　剛
２．発表標題 機械学習による適応的サイバー攻撃検知の性能評価
３．学会等名 JSAI合同研究会2022第1回安全性とセキュリティ研究会
４．発表年 2022年

１．発表者名 岡本　剛
２．発表標題 免疫的攻撃検知によるMQTTブローカーのレジリエンス強化 ～ Use-After-Freeの脆弱性に対するDoS攻撃の検知と防止 ～
３．学会等名 電子情報通信学会　ネットワークシステム研究会
４．発表年 2022年

１．発表者名 岡本　剛
２．発表標題 MQTTブローカーのための免疫的攻撃検知の試作
３．学会等名 情報処理学会　第92回コンピュータセキュリティ研究会（CSEC）
４．発表年 2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関