IoT セキュリティ研究開発最前線

横浜国立大学　環境情報研究院/先端科学高等研究院 准教授　吉岡 克成（よしおか かつなり）

日本電信電話株式会社　塩治 榮太朗（しおじ えいたろう）

国立研究開発法人情報通信研究機構　サイバーセキュリティ研究室 研究マネージャー　笠間 貴弘（かさま たかひろ）

横浜国立大学　先端科学高等研究院 特任教員（准教授）　田辺 瑠偉（たなべ るい）

日本電信電話株式会社　秋山 満昭（あきやま みつあき）

国立研究開発法人情報通信研究機構　サイバーセキュリティネクサス ネクサス長　井上 大介（いのうえ だいすけ）

1. IoTにおけるサイバー攻撃と対策技術

パソコンやスマートフォンだけでなく、センサやカメラ、家電や自動車、ビルや工場など、様々なモノがネットワークに接続されるIoT（Internet of Things）、モノのインターネットが現実となっている。今後も医療、産業、コンシューマ、自動車・宇宙航空などの分野での市場拡大が見込まれており[1]、IoTはSociety5.0を実現する重要な構成要素となっている。一方で、これらのモノがサイバー攻撃の標的となることも指摘されており、実際に産業分野やコンシューマ分野においてその脅威が顕在化している。特に、ホームルータやIPカメラなどのコンシューマ機器を狙ったサイバー攻撃は2015年頃から顕著となり、2016年にはMiraiと呼ばれるマルウェアに数十万台の機器が感染し、それらの機器を悪用した大規模サービス妨害攻撃が発生した。IoT機器を狙ったマルウェアは、その後も次々と出現している。インターネット上では、このようなマルウェアによる脆弱な機器を狙う攻撃や、セキュリティ調査のためのネットワークスキャンが急増している。NICTER観測レポート2020によると、NICTの観測網では2020年の1年間で5001億パケットもの不審な通信が観測されており、この中にはIoT機器を探索する通信が多数含まれている[2]。前述の観測パケット数は、2014年の19.4倍、Miraiが登場した2016年と比べても3.9倍に上り、年を追うごとにIoT機器が外部からのアクセスを受けやすくなっている実態が分かる。

本稿では、IoTセキュリティ研究開発の最前線を、主にコンシューマ機器に関するセキュリティ情報の収集、サイバー攻撃の観測・解析・対策、そして、研究開発を行う上で注意すべき研究倫理の観点から当該分野の第一線で活躍する研究者によって解説する。複雑なサプライチェーンにより製造され、流通するIoT機器はセキュリティ上の課題も多い。本稿が多様化・高度化するサイバー攻撃の対策を検討する上での一助となれば幸いである。

2. 情報収集

IoT機器に対する脅威の実態を分析する上で、機器に関する様々な情報を収集することが必要となる。例えば、機器自体に関する情報や、機器のインターネット上での観測情報などが挙げられる。また、IoT機器は多種多様であるため、そのような情報を網羅的かつ効率よく収集できることが望ましい。本章では、一般に公開されている情報のうち実際の研究活動でよく利用されているものをいくつか紹介する。このような情報は、研究者のみでなく、機器をセキュアに運用したい一般ユーザや自社製品に関する脅威情報を把握したいベンダにとっても有用となり得る。

機器情報：IoT機器自体に関する情報は、脆弱性の発見などの機器自体の脅威を分析する上で重要であるが、実機の調達は様々な観点からスケールしないという問題がある。そのような情報を取得する方法の一つとして、機器ベンダのサイトから機器に関する情報を取得できる。例えば、ユーザによる手動更新の実施を促すことを目的として提供されている機器のファームウェアを入手できたり、機器に関する様々なメタデータのほか、ドライバなどの付属ソフトウェア、マニュアルなども入手できる場合がある。また、ファームウェ

アは最新版のみでなく、過去のバージョンも含めて公開されている場合もあり、時系列的な分析も実施できる。さらに、機器でGPLライセンスのソフトウェアが利用されている場合は、ソースコードも入手できる場合もある。機器の脆弱性に関する情報は、従来のソフトウェアと同様にCVEやJVNなどの脆弱性データベースから取得できたり、ベンダサイト上のリリースノートに記載されている場合もある。このような情報を活用し様々な観点から分析することで機器の脅威を発見する研究が多く行われている。例えば、ファームウェアを解析することによる幅広い機器におけるセキュリティ機構の実装の時系列的な分析や[3]、脆弱性の公開日と対応する脆弱性の修正ファームウェアのリリース日の関係の分析[4]などから、IoTのセキュアな開発における課題が明らかにされている。また、一般ユーザや機器ベンダも、このような情報に基づいて所有する機器の脅威情報を把握することで、適切な対策の実施に役立てることができる。

観測情報：インターネット上で観測可能なIoT機器についての情報は、脅威に晒されている機器の実情を把握する上で重要であるが、自ら大規模なインターネットスキャンを継続的に実施することは容易ではない。そのような情報を取得する方法の一つとして、インターネット上のホストをスキャンした結果を蓄積したデータベースを閲覧・検索することができるサービスを利用できる。このようなサービスは、無料・有料のもの含めて多く存在し、最も古くから存在するShodanや、学術研究がベースとなっているCensysなどが有名である。このようなサービスでは、スキャンに対する応答や、応答元ホストに関する情報、応答から推測される機器種別や脆弱性など、様々な情報が取得できる。このような情報に基づいて脆弱な機器の実態を解明する研究が盛んに行われている[5]。また、一般ユーザも自宅や自社ネットワークレンジに脆弱な機器が意図せずに公開されていないか、ベンダも自社の機器が利用をされていないかを把握する用途などで利用できる。

3. 観測技術

IoT機器に対する攻撃活動を観測することは正しい状況認識につながり、適切な対策導出に役立つ。観測技術は大別すると、未使用のIPアドレス宛てのトラフィックを観測するダークネット観測や、脆弱な囮サーバを用いて攻撃活動を観測するハニーポットに代表される攻撃側からのアクセスを待ち受ける受動的な観測手法と、ネットワークスキャンやクライアントハニーポットに代表される観測対象に対して観測側から能動的にアクセスを行う観測手法に分けることができる。また、それらを適切に組み合わせることで、より複雑な攻撃の一連の流れを捉えることも可能になる。

受動的な観測：Miraiをはじめとするネットワーク感染型（ワーム型）マルウェアがコンシューマ向けIoT機器へ感染を広げる事例が多発している。ダークネットでは、ワーム型マルウェアの感染活動が観測できる。ワーム型マルウェアが多数のIoT機器に感染を広める場合、攻撃活動と新たな感染が連鎖的に発生するため、当該マルウェアが感染時に用いるサービス（宛先ポート番号）への攻撃元IPアドレス数が急増することがダークネット観測によって確認できる。さらに、感染手法の詳細を観測するためには、応答を返さないダークネット観測ではなく、ハニーポットを用いて攻撃側と適切なインタラクションを行う必要がある。例えば、TelnetやSSHに対して容易に推測可能なID／パスワードを用いることで感染を広げるマルウェアに対しては、TelnetやSSHに対応したハニーポットを構築することで感染に用いるID／パスワードや感染後の挙動を把握することができる。Mirai亜種を含むマルウェアの中にはリスト型攻撃ではなく、個別の機器の脆弱性を悪用して感染を広めるものも存在するため、観測したいマルウェアが攻撃対象とするサービスに合わせたハニーポット構築が必要である。また、感染後の挙動についても実行環境や用意されているライブラリ等が異なることで、マルウェアにハニーポットだと検知されるケースやマルウェアが適切に動作しないことがあるため、ハニーポットを実環境に近付けたり実機をハニーポットとして用いたりといった工夫が必要である。特に実機を用いる場合は、観測を行う中で外部に攻撃通信が発生して二次被害を引き起こさない対策も重要となる。

能動的な観測：インターネットの広域に対してネットワークスキャンを実施し、IoT機器が意図せずまたは不適切にインターネットに対して公開しているサービスを観測する取組みが様々な組織で実施されている。前述したShodanやCensysなどはその代表的なサービスである。ネットワークスキャン自体はサイバー攻撃そのものの観測とは異なるが、各サービスでアクセス可能な機器数や動作するサービスのバージョン情報などが把握でき、サイバー攻撃の潜在的な被害対象を把握するのに役立つ。その他にも、マルウェアの多くは感染後に指令サーバと接続し攻撃者の制御下に置かれる

ことから、マルウェア感染機器の挙動を模倣して指令サーバへ接続し攻撃者からの指令を観測する手法や、マルウェア感染機器同士が構築するP2Pネットワークに参加することで感染機器数やP2Pネットワーク上でやり取りされる指令やアップデートファイルを観測する手法なども存在し、受動的な観測手法のみでは得られない情報を得ることができる。しかし、これらのマルウェア間や攻撃者との情報のやり取りに介在する観測手法を実行するためには、マルウェアが用いる通信プロトコルやフォーマットを事前に把握しておく必要があるため、マルウェア解析技術による解析が必要になるケースが多い。

このような観測手法を適切に組み合わせていく（加えて、情報収集やマルウェア解析の結果とも横断分析する）ことで、サイバー攻撃全体のエコシステムを明らかにする研究が行われている。論文［6］ではMiraiボットネットについて、論文［7］では同じくIoTマルウェアの一種であるHajimeボットネットについての分析が行われており、興味のある読者はぜひ参考にするとよいだろう。

4. 解析技術

IoT機器を解析することはセキュリティ上の欠陥の発見につながり、IoT機器を狙ったサイバー攻撃への対策に役立つ。また、これらの機器に感染するIoTマルウェアを解析することは潜在的な脅威の発見につながり、マルウェア感染の被害を抑制するための対策に役立つ。IoT機器を解析する技術は多岐にわたるが、本章では機器のソフトウェアやネットワークサービスを解析する方法をいくつか紹介する。また、IoTマルウェアを解析する技術として、動的解析と静的解析を紹介する。

IoT機器の解析：IoT機器の中にはLinuxをはじめとする汎用的なソフトウェアを活用するものが存在する。しかし、脆弱性が発見された場合には多数の機器がサイバー攻撃の標的となり得る。また、近年は機器ごとに異なるファイルやプログラムを活用する事例が確認されており、機器固有の脆弱性を狙ったマルウェアが増加している。そのため、IoT機器を解析する研究が盛んに行われている。例えば、高度なエミュレーションによりファームウェアを再現することで、その脆弱性についての分析が行われている[8]。さらに、解析ツールを利用することでIoT機器で使用されるソフトウェアを解析することができる。これらのツールは無料・有料のもの含めて数多く存在し、ファームウェアを抽出するツールであるBinwalkなどが有名である。IoT機器の中にはTelnetやSSHなどのネットワークサービスによりインターネット上からリモートアクセスできるものが存在する。しかし、これらのサービスに容易に推測可能なID／パスワードが設定されている場合や、脆弱性が存在するバージョンが用いられている場合には、サイバー攻撃の標的となり得る。このような機器の情報を取得する方法の一つとして、Nmapをはじめとした検査対象ホストをスキャンするツールを利用することができる。

IoTマルウェアの解析：マルウェア解析の手法は大別すると、動的解析と静的解析の2つのアプローチに分けることができる。動的解析は、実際にマルウェア検体を解析環境（サンドボックス）と呼ばれるマシン上で実行して、ネットワークアクセスやファイル操作といった挙動を解析するものである。従来のIoTマルウェアの多くは様々な機器に共通する機能を悪用していたため、解析環境にはVirtualBoxやQEMUなどにより構築した汎用的なサンドボックスが用いられる。また、IoTマルウェアの多くはTelnetなどのネットワークサービスを経由して感染を拡大するため、動的解析の多くにおいてもリモートコマンドを用いて解析環境にマルウェア検体が転送・実行される。そして、あらかじめ用意したtcpdumpやstraceなどの観測ツールを用いて挙動を観測し、動的解析終了後に解析環境がマルウェア感染前の状態に復元される。IoTマルウェアを動的解析した研究が盛んに行われており、例えば、マルウェア感染によって発生する通信を解析し、攻撃者が設置した指令サーバとの接続性についての分析が行われている[9]。しかし、近年は特定の機器の機能に依存したマルウェアが観測されはじめており、解析環境に実機のIoT機器が用いられる場合がある。例えば、IoTマルウェアが特定の機器で持続的感染を引き起こす可能性についての分析が行われている[10]。一方、静的解析は、マルウェアの実行コードを逆アセンブルして、マルウェアの持つ機能や特徴を詳細に解析するものである。Windows PCを狙ったマルウェアの多くは、パッキング（圧縮もしくは暗号化）によりその本来のコードを隠蔽して解析を妨害することが知られているが、IoTマルウェアの中にはパッキングが行われておらず、本来のコードを読み解くことができる場合がある。一般に、静的解析では大量のコードを読み解く必要があり、高度な技術を持つ解析者による手動解析が主流である。また、解析には多くの時間を要するため、解析の目的、ポイントを絞って行われる。

5. IoTセキュリティ研究開発における倫理的配慮

サイバーセキュリティは、その研究行為が社会に対して直接的な影響を与え得るために、十分に前例のない領域を研究対象として取り扱う場合には倫理的な問題にも直面しやすい。本章では、IoTセキュリティの研究開発における情報収集/観測・解析・対策を題材として、世の中で議論・実践されている研究者がとるべき行動や技術的側面・社会的状況・法令などの典型的な観点について説明する。

情報収集/観測：ZmapやMasscanなどのツールが2013年に公開された後、ネットワークスキャンは世界中で大々的に実施されるようになった。これはネットワークスキャンのセキュリティとしての有用性が世の中に受容されたことが一つの要因だと考えられる。ただし、スキャンパケットがネットワークやスキャン対象デバイスに与える影響を十分に考慮する必要がある。特定のネットワークに短時間に大量のスキャンパケットを送信すると、ネットワークが高負荷になることや、ネットワーク管理者にDoS攻撃を受けていると誤解させてしまう可能性がある。また、スキャンパケットがデバイスの動作に悪影響を与えた場合にも、デバイス所有者が攻撃を受けていると誤解させてしまう可能性がある。また、ネットワーク管理者やデバイス所有者が執行機関へ通報した場合、当該スキャン行為が不正アクセス禁止法やその他の法令で禁止されている行為の疑いがかけられる可能性がある。よって、ネットワーク管理者やデバイス保有者などのステークホルダに対するリスクの最小化を実践しなければならない。例えば、単位時間当たりの送信パケット数の制限や、調査目的の提示、非破壊的なパケットの送信、などが考えられる。

解析：セキュリティ上の欠陥を発見するためにIoTの解析が行われている。この過程においてよく行われるリバースエンジニアリング（RE）は、解析対象の著作権を侵害する場合があることが指摘されているが、国内外でその状況は異なる。米国では、古くからフェアユースという法律の原則があり、相互運用性確保のための製品やプログラムのREは権利侵害に当たらないとされてきた。また、日本でも著作物を含むビッグデータを利活用して付加価値を生むことが期待されている社会的背景に基づいて、2019年1月1日著作権法改正により柔軟な権利制限規定が導入されており、第30条の4でプログラムのRE（調査・解析）は著作権侵害とならないとされた[11]。なお、利用規約等でREを禁止する規約がある場合は注意する必要がある。

対策：世界的にも例を見ない先進的な取組みとして、国立研究開発法人情報通信研究機構（NICT）、インターネットプロバイダ（ISP）、総務省が連携するプロジェクトであるNOTICE（2019年開始）がある。NOTICEは、(1) 容易に推測されやすいパスワードを利用しているIoTをインターネット上から発見し、(2) そのIoTの利用者に対してISP経由で注意喚起、する取組みである。これを実施するために、(1) の調査のために国立研究開発法人情報通信研究機構法の一部改正、(2) の情報共有のために電気通信事業法の一部改正が実施された[12]。

社会的コンセンサスや法制度によって受容されるサイバーセキュリティの活動は、時代とともに変化するものである。サイバーセキュリティの研究開発に取り組む際には、これらを念頭に置いて倫理的な配慮をして実施する必要がある。

6. まとめと今後の展望

本稿では、IoTセキュリティに関する研究開発の最前線として、情報収集、観測技術、解析技術、そして倫理的配慮について概観した。このような研究開発に加え、IoTセキュリティを向上させるためには、IoT機器の設計・開発段階、構築段階、運用・保守段階と、様々な段階での対策が求められ、また法的な整備の検討も必要であり、引き続き産学官が連携して取り組むべき重要な課題となっている。

参考文献

[1] 総務省. 令和2年版情報通信白書5Gが促すデジタル変革と新たな日常の構築. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf

[2] 情報通信研究機構. Nicter観測レポート2020の公開. https://www.nict.go.jp/press/2021/02/16- 1.html.

[3] 白石周碁, 福本淳文, 吉元亮太, 塩治榮太朗, 秋山満昭, 山内利宏. ソフトウェア解析とベンダインタビューによるIoT機器のセキュリティに関する大規模実態調査. Inコンピューターセキュリティシンポジウム, 2020.

[4] Asuka Nakajima, Takuya Watanabe, Eitaro Shioji, Mitsuaki Akiyama, and Maverick Woo. 1-day, 2 Countries—A Study on Consumer IoT Device Vulnerability Disclosure and Patch Release in Japan and the United States. *IEICE TRANSACTIONS on Information and Systems*, 103 (7) : 1524-1540, 2020.

[5] Deepak Kumar, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, Rajarshi

Gupta, and Zakir Durumeric. All Things Considered: An Analysis of IoT Devices on Home Networks. In *28th USENIX Security Symposium (USENIX Security 19)*, 2019.

[6] Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the Mirai Botnet. In *Proceedings of the 26th USENIX Conference on Security Symposium*, page 1093-1110, 2017.

[7] Stephen Herwig, Katura Harvey, George Hughey, Richard Roberts, and Dave Levin. Measurement and Analysis of Hajime, A Peer-to-peer IoT Botnet. In *Proceedings of the 26th Annual Network and Distributed System Security Symposium*, 2019.

[8] Abraham Clements, Eric Gustafson, Tobias Scharnowski, Paul Grosen, David Fritz, Christopher Kruegel, Giovanni Vigna, Saurabh Bagchi, and Mathias Payer. HALucinator: Firmware Rehosting through Abstraction Layer Emulation. In *Proceedings of the 29th USENIX Security Symposium (USENIX'20)*, 2020.

[9] Rui Tanabe, Tatsuya Tamai, Akira Fujita, Ryoichi Isawa, Katsunari Yoshioka, Tsutomu Matsumoto, Carlos Gañán, and Michel van Eeten. Disposable Botnets: Examining the Anatomy of IoT Botnet Infrastructure. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020.

[10] 原悟史, 田宮和樹, 鉄穎, 渡辺露文, 吉岡克成, 松本勉. 感染持続型IoTマルウェアの実態調査と実機による概念実証. In電子情報処理学会論文誌, *Vol. J102-B, No. 8, pp. 524-535*, 2019.

[11] 文化庁. デジタル化・ネットワーク化の進展に対応した柔軟な権利制限規定に関する基本的な考え方. https://www.bunka.go.jp/seisaku/chosakuken/hokaisei/h30_hokaisei/pdf/r1406693_17.pdf

[12] 総務省. 電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律. https://www.soumu.go.jp/main_content/000567073.pdf