脆弱機器を模擬した囮（おとり）システムによるIoTのセキュリティ現状把握

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

1. はじめに

ネットワークを通じて様々なモノが接続し、それらから得られる情報が新たな価値を生み出す新しい情報社会の形としてIoT（Internet of Things）が注目されている。既に、時計やメガネといったウェアラブル機器、情報家電やスマートメーター、ビル制御システム、自動車や交通インフラ、各種センサ、監視カメラ、工業制御システム、医療機器、放送システム、その他多種多様な機器や情報通信インフラがネットワーク接続されており、いわばIoTの黎明期とも言える状況となっている。一方、これまでのインターネットの発展とそれに伴うサイバー攻撃の増大の歴史が示すとおり、高い価値の創出は、それを奪取したり、操作したり、破壊しようとする不正な試みを誘引する。今後、IoTが生み出す新たな価値が高まるにつれて、このような脅威はさらに増大していくと予想される。

本稿では、既にインターネットに接続されている多種多様なIoT機器のセキュリティの現状を把握するための観測技術と、それらの技術を用いた観測結果について解説する。次章では、まずIoTの現状とIoT機器のセキュリティに関するこれまでの先端研究や報告事例について紹介する。次に3章では、脆弱なIoT機器を模擬した囮システムであるハニーポットによるサイバー攻撃の観測技術とその観測結果について説明する。

2. IoTの現状とIoT機器のセキュリティに関する研究事例

IHS社の試算[1]では、2015年の時点でインターネットにつながるモノ（IoT機器）の数は既に約154億個であり、2025年までに約754億個まで増大すると推定されている。一方、シスコ社[2]によると、99%以上のモノは未だにインターネットに接続されていないとされており、IoTの潜在的な裾野の広さを示している。例えば、製造業等の産業分野では、生産ラインにおける各機器からのログ収集分析による効率化が進んでいる。また、エネルギー、交通、物流等の社会インフラ分野でも、センサやモニタによる施設管理、物流管理、故障予測などが行われている。家庭用としても、照明の操作、火災報知器や情報家電との連動から、歯ブラシ、コンタクトレンズからデータ収集を行うものまで広く開発が進められている。これらの機器が連動することにより利便性の向上や省エネ、災害検知を実現するスマートホーム、社会インフラとも連携したスマートシティ構想などが世界中で進められている。

このようにIoTの実現形態としてとらえることができるシステム、サービス、取組みは既に様々なものがあるが、以下では、これまでに発生しているセキュリティ問題の事例や機器の脆弱性に関する先行研究について説明する。

近年の自動車は、内部の多数のECU（Electronic Control Unit）が車載ネットワークを通じて通信することで走行や車内装置の制御を行っており、自動車に対するサイバー攻撃は長い間懸念されてきた。2011年には実車に対して携帯電話回線等を用いて遠隔から侵入しこれを制御できることが発表され[3]、2015年には同様に実車に対して完全に制御を奪えることが実証され[4]、140万台のリコールへと発展した。

産業制御システムへのサイバー攻撃として2010年に発見されたスタクスネット[5]がイランの核燃料施設に侵入し被害を与えた事例が特に知られている。その後もドイツの製鉄所制御システムが不正侵入により損傷を受けたり、2015年末には電力会社の関連設備への侵入によりウクライナ西部において大規模な停電が発生するなど[6]、サイバー攻撃を原因とする産業制御システムの事故が発生している。

ドローンは様々な応用が期待される無人航空機であるが、既に多くのハッキング事例が存在する。一例として、RSAカンファレンス2016で発表された事例[7]では、オランダ警察が使用する監視用ドローンの制御を乗っ取ることに成功している。

医療機器の中には病院内のネットワークに接続するものも多く存在する。これらの機器がマルウェア感染した事例が複数存在する。例えば、米国ボストンの病院において胎児モニタ装置にマルウェア感染した事例や、国内でも金沢大学付属病院においてUSBメモリ経由で多くの医療機器がマルウェア感染した事例がある[8]。また、インスリンポンプやペースメーカーといったインプラント型医療機器についても不正に操作を行うことができる脆弱性が複数発見されている[8]。

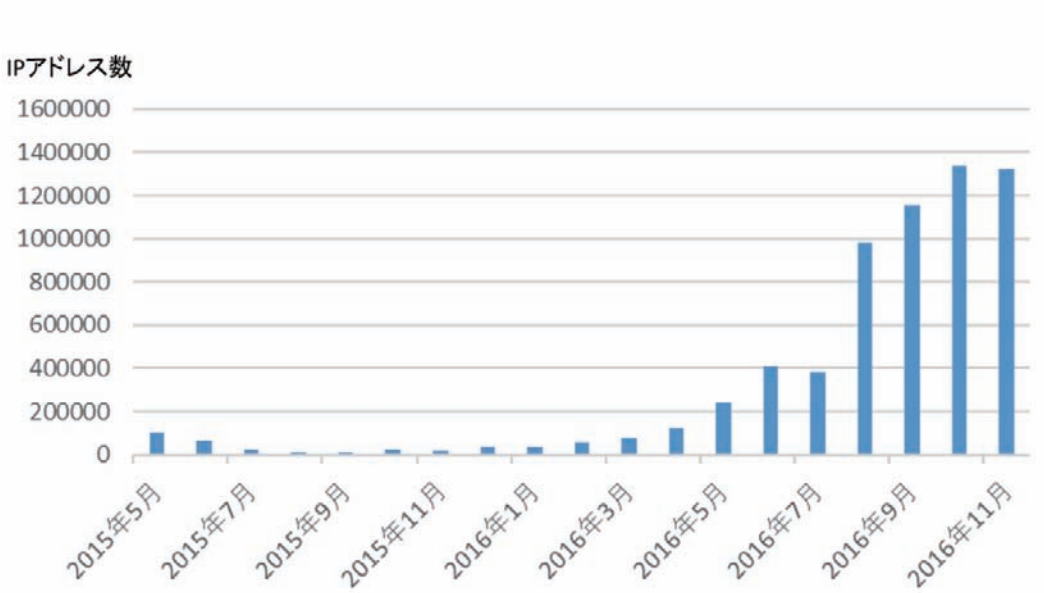
国内の大学等教育機関においてインターネットとつながる複合機やプリンタの内部データ（印刷物等のデータ）が、外部からアクセス可能な状態となっているケースが多数発見されている[9]。また、監視カメラ、Webカメラの中には適切にパスワード等のアクセス制御が設定されておらず、任意のユーザから閲覧可能となってしまっているものが多数存在していることが知られている[10]。

3. 脆弱機器を模擬した囮システムによるIoTにおけるサイバー攻撃の観測

インターネットに接続されている機器の中には、これらの機器上で動作する遠隔操作用のプログラムであるTelnet経由で、容易に推定可能なパスワードを用いてログインできるものが多数存在する。2012年には、匿名の自称セキュリティ研究者により上記を含む脆弱な機器を大量に乗っ取り操作することで、インターネット上で動作するホストの大規模探索実験[11]が行われ問題となった。これらのサイバー攻撃を調査するため、横浜国立大学情報・物理セキュリティ研究拠点では、2015年よりサイバー攻撃に対して脆弱なIoT機器を模擬した囮システムであるハニーポットを用いた観測を実施している[12]。ハニーポットは、脆弱な機器において動作していることが多いネットワークサービス、例えば、前述のTelnetや機器の設定を行うためのWebインタフェースなどを模擬する通信プログラム群（フロントエンド）と、フロントエンドが応答する内容を学習するための脆弱機器（バックエンド）からなる。フロントエンドに割り当てるIPアドレスは、国内外のものを用いることで様々な地域におけるサイバー攻撃を観測する。バックエンドは実際に脆弱な機器群（実機）と仮想マシンを組み合わせて実現している。攻撃者が遠隔からハニーポットが設置されたIPアドレスにアクセスすると、これらのフロントエンド及びバックエンドが連動して応答し、あたかも脆弱なIoT機器が動作しているかのように振舞うことで攻撃の詳細を観測し、攻撃元となっている不正プログラム（マルウェア）を収集する。ハニーポット技術の詳細については文献（12）を参照いただきたい。

図1にハニーポットにより観測された攻撃元ホスト群のIPアドレス数の月ごとの推移を示す。

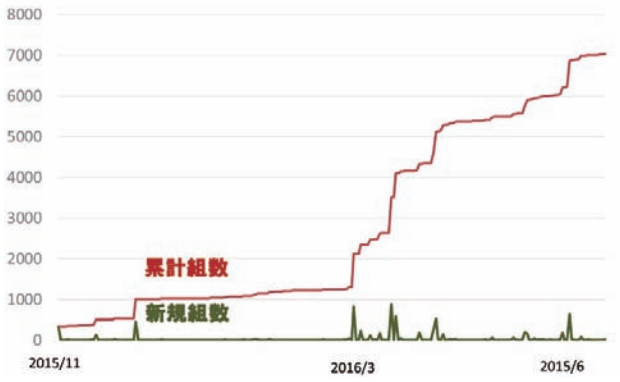
ハニーポットにアクセスしてくる攻撃元ホストは2015年から既に高い水準であったが、特に2016年の3月以降に急増し、その5か月後にはさらに倍増し、130万IPアドレスを超えている。ハニーポットは正規ユーザが存在しない囮のサービスであり、もしサイバー攻撃等の不正なアクセスがなければ本来的にはアクセス数はゼロになるはずであることを考えると、いかに多くの攻撃元ホストが脆弱なIoT機器を狙って攻撃を行っているかが分かる。詳しくは後述するが、これらの攻撃元ホスト群の実体は、攻撃者に乗っ取られて操られている脆弱なIoT機器群であり、これらの機器は他の機器に攻撃を行っている点で加害者である一方、真の攻撃者によって侵入を受けて不正に操られているとい



■図1. ハニーポットにより観測された攻撃元ホストの月別IPアドレス数の推移

う意味で被害者でもある。したがって、ハニーポットへの攻撃ホスト数の増加は、マルウェア感染した機器の増加を意味する。詳細は割愛するが、2016年8月以降の攻撃ホストの急増はMiraiと呼ばれるIoTマルウェアによる活動が活発化したことが関係している。Miraiのソースコードが公開され、多くの攻撃者がこれを利用できる状況となったことから、本原稿執筆時点でもMiraiに派生したマルウェアに感染した機器からの攻撃が特に多くなっている。

IoT機器への攻撃は多様化を見せているものの、現時点では前述のTelnetを狙った攻撃が最も多い。Telnetはアクセス時にIDとパスワードによる認証が必要であるが、多くのIoT機器は推測が容易なIDとパスワードが設定されており、機器使用者はTelnetの存在すら気付かずに機器を使用しているため、攻撃者やマルウェアはこの不備をついて機器に侵入し、様々な不正活動を行う。図2にハニーポットにより観測された攻撃者が用いるIDとパスワードの組の種類数の推移を示す。図2から分かるとおり、攻撃に使われるIDとパスワードの推計組数は2016年の3月以降増加傾向が顕著であり、この時期以降により多くの機器がサイバー攻撃の対象となっていることが分かる。また、図1と比較すると、攻撃元IPアドレス数の増加、すなわち、感染機器数増加の時期と一致していることが分かる。



■図2. 攻撃に使用されるIDとパスワードの組の種類数の推移

上記の観測は、IoT機器を狙った攻撃の増減傾向や攻撃内容を把握する上で有益であるが、ハニーポットに対するアクセス元、つまりマルウェア感染機器の種類を特定することはできない。そこで、ハニーポットにアクセスしてきた攻撃元ホスト（感染機器）上で動作するサービスに対してハニーポット側から通信を行い、その応答から感染機器を推定する。特にTelnetやWebインタフェース（機器の管理画面）の応答には機器を特定するための情報が含まれている場合があるため、これらの情報をシグネチャとして登録し機器推定を行う。図3はハニーポットに攻撃をして

- 監視カメラ等
  - IP カメラ
  - デジタルビデオレコーダ
- ネットワーク機器
  - ルータ・ゲートウェイ
  - モデム、ブリッジ
  - 無線ルータ
  - ネットワークストレージ
  - セキュリティアプライアンス
- 電話関連機器
  - VoIPゲートウェイ
  - IP電話
  - GSMルータ
  - アナログ電話アダプタ
- インフラ
  - 駐車管理システム
  - LEDディスプレイ制御システム
- 制御システム
  - ソリッドステートレコーダ
  - インターネット接続モジュール
  - センサ監視装置
  - ビル制御システム
- 家庭・個人向け
  - Webカメラ、ビデオレコーダ
  - ホームオートメーションGW
  - 太陽光発電管理システム
  - 電力需要監視システム
- 放送関連機器
  - 映像配信システム
  - デジタル音声レコーダ
  - ビデオエンコーダ/デコーダ
  - セットトップボックス・アンテナ
- その他
  - ヒートポンプ
  - 火災報知システム
  - ディスク型記憶装置
  - 医療機器（MRI）
  - 指紋スキャナ

デバイスはWeb及びTelnetの応答から判断

■図3. ハニーポットに攻撃をしてきた感染機器一覧

きたと推定される感染機器の一覧である。特に件数が多い機器は、ネットワークカメラ、ルータ、デジタルビデオレコーダである。また件数は少ないものの、ビルの空調や照明の制御機器、医療機器（MRI）、火災報知システム、太陽光パネル制御機器、電力需要監視装置といったように不具合が発生すると重大な損害が発生し得る重要な機器も観測されている。

マルウェアに感染した機器は、攻撃者に操作され様々なサイバー攻撃に悪用される。我々はハニーポットにより収集したマルウェア検体を実際のIoT機器や疑似解析環境において実行し、その動作を観測することで感染機器の悪用の実態についても分析を行っている。最も頻繁に観測される悪用の事例としては、他の機器に無作為に接続を試み、さらに感染を広げる「感染活動」と、企業等のWebサイト等に対して大量の感染機器で同時にアクセスし、サイトを閲覧しにくくするといった「サービス妨害攻撃」の実施である。特に後者については過去最大規模の分散サービス妨害攻撃がIoT機器を悪用することで行われている[13]。

4. おわりに

本稿では、IoT機器のセキュリティに関するこれまでの先端研究や報告事例について紹介するとともに、脆弱なIoT機器を模擬した囮システムであるハニーポットによるサイバー攻撃の観測技術とその観測結果について説明した。黎明期と言えるIoTにおいて既に大量のサイバー攻撃が発生しており、マルウェア感染事例が多数発生している根本的な原因としてIoT機器のセキュリティレベルが低いことが挙げられる。Telnetのように不必要な通信プログラムが残存していたり、脆弱な認証により容易に管理者権限でアクセスが可能であるといったような初歩的なセキュリティの問題を多くの機器が有している。また、このような現状が明らかとなっても、IoT機器の製造者が業種地域共に多様であることから、問題の周知や対策が徹底しにくいという問題もある。サイバー攻撃を行う攻撃者にとってIoTは格好の標的となっており、これを悪用した攻撃は今後も増加、多様化することが予想されるため、IoTの様々な領域において個々の製造者、利用者を超えた連携による対策が必要と言える。

文献

[1] IHS Technology, “IoT platform：enabling the Internet of Things,” White Paper, 2016. https://technology.ihs.com/576272/iot-platforms-enabling-the-internet-of-things

[2] Cisco, “Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion,” White Paper, 2013.

[3] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” USENIX Security Symposium 2011.

[4] Charlie Miller, Chris Valasek, “REMOTE EXPLOITATION OF AN UNALTERED PASSENGER VEHICLE,” Blackhat USA 2015.

[5] 小熊信孝、“Stuxnet-制御システムを狙った初のマルウェア” JPCERT/CC, http://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf

[6] “電力分野のサイバーセキュリティ対策について” 資源エネルギー庁、2016。http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/kihonseisaku/pdf/004_06_00.pdf

[7] Nils Roddy, “Hacking a Professional Drone,” RSA Conference 2016, https://www.rsaconference.com/writable/presentations/file_upload/ht-w03-hacking_a_professional_police_drone.pdf

[8] 医療機器における情報セキュリティに関する調査、情報処理推進機構、2014。https://www.ipa.go.jp/files/000038223.pdf

[9] “ネット接続の複合機など、データ丸見え　大学など26校,” 朝日新聞、2016。

[10] “IoTマルウェア大量感染の現状と対策,” 日経コンピュータ、2016。https://bizboard.nikkeibp.co.jp/kijiken/summary/20160901/NC0920H_3454979a.html

[11] Internet Census 2012, http://internetcensus2012.bitbucket.org/paper.html

[12] IoTPOT：Analysing the Rise of IoT Compromises、横浜国立大学情報・物理セキュリティ研究拠点、http://ipsr.ynu.ac.jp/iot/

[13] BIT DIFFENDER, “DDoS attack by massive IoT botnet takes down Krebs on Security” HOT FOR SECURITY By BIT DIFFENDER, 2016. https://www.hotforsecurity.com/blog/ddos-attack-by-massive-iot-botnet-takes-down-krebs-on-security-16742.html