特集

情報セキュリティ

IoTにおけるサイバーセキュリティの現状と将来の可能性

国立情報学研究所
アーキテクチャ科学研究系教授　高倉　弘喜

1．はじめに

IoT機器へのサイバー攻撃が社会問題化し、世界各国でその対策が検討されています。表１は筆者が責任者を務めるNII Security Operation Collaboration Services (NII-SOCS)においてある１日で観測した、ShodanやRapid7等の調査組織による機器探索の上位14件を示しています。メールやWebの通信に使われる25/tcp、80/tcp、443/tcpよりも、81/tcpなど何に使われるか分からないものを探索する動きの方が活発なことが読み取れます。これらは主にIoT機器の制御に使われていると推定されますが、具体的なメーカや機種が特定できているものは僅かしかありません。このように、インターネットに直結されたIoT機器は高頻度で探査を受けており、見つけられた機器は調査組織がhttps://www.shodan.ioなどで無償・有償で公開しているのです。

IoT機器といっても、家庭にあるブロードバンドルータやWebカメラのように単体で動作が完結するものから、医療機器、自動車や工場の制御システムのようにIoT機器が連携して動作するものまで、様々な利用形態があります。

単体で動作が完結する場合、サイバー攻撃によりIoT機器が利用不能になっても、例えばWebカメラが使えなくなるだけで、その影響は限定的と言えます。

一方、連携するIoT機器の場合はサイバー攻撃による被害が発生すれば、その影響は他のIoT機器に及びます。IoT機器の利用目的によっては、すべての機器が完動し、全体として正常な動作を続けることが求められます。

例えば、Boeing 787は500種類のソフトウェア部品(Loadable Software Airplane Parts: LSAPs)を１機あたり800から900箇所に搭載しています[1]。また、Airbus A380は40社から1,000個のLSAPsを提供されています[2]。個々のLSAPは、インターネットを含む様々な通信回線を通じて製造メーカ、組み立てメーカ、航空会社などの動作検証を常に受け、サイバー攻撃を含めた不具合に対しLSAPsの完全性を確認しています。もちろん、そこにかかる運用コストはとても高くなります。

表１　IoT機器探索の一例

回数	ポート番号/プロトコル
639,317	81/tcp
638,848	102/tcp
637,993	444/tcp
637,040	2222/tcp
636,701	82/tcp
636,534	9000/tcp
636,482	6666/tcp
358,167	80/tcp
351,648	443/tcp
345,561	53/udp
324,982	8080/tcp
320,330	3749/tcp
320,149	25/tcp
320,007	4782/tcp

2．IoT機器の脆弱性

Avast社の報告[3]によると、2018年９月に、全世界のAvastユーザの約1,600万(日本は約23,000)のホームネットワークをスキャンした結果、5,600万のネットワーク接続機器を確認し、その内の40.8%に何らかの脆弱性を発見しています。脆弱性の内訳は、弱いクレデンシャル（69.2%）、ソフトウェアの脆弱性（31.4%）でした。また、59.1%のユーザはルータ機器へのログインやファームウェアの更新を行なったことがなく、そのためルータ機器の59.1%に脆弱性が見つかっています。

脆弱性が見つかった機器の種別では、全世界的にプリンタの割合が高く、日本でも42.3%を占めていました。一方で、諸外国では比較的割合の高

い監視カメラやNASはそれぞれ4.9%と1.4%であり、これらの比率は非常に小さいものとなっています。

この調査はホームネットワークを対象としていましたが、筆者のこれまでの経験やNII-SOCSの運用事例から、NASの比率が高くなるなどの一部の例外はありますが、高等教育機関でもほぼ同じ傾向にあると考えられます。

このことから、Avastの報告で指摘されているように、キャンパスネットワークと研究室LANとの境界に設置されるルータ(大多数はブロードバンドルータ)がサイバー攻撃を受けて乗っ取られ、そこからLAN内のプリンタやNASといったIoT機器が乗っ取られるという事態の発生が懸念されます。また、ルータの設定を変更することで悪意あるDNSサーバを利用させ、偽サイトなどへ誘導するという攻撃も実際に起きています。

IoT機器の乗っ取りでは、ホームネットワークで心配される盗撮によるプライバシ侵害やDDoS攻撃への参加などに加え、学生・教職員の個人情報、研究情報の流出を高等教育機関は警戒する必要があります。

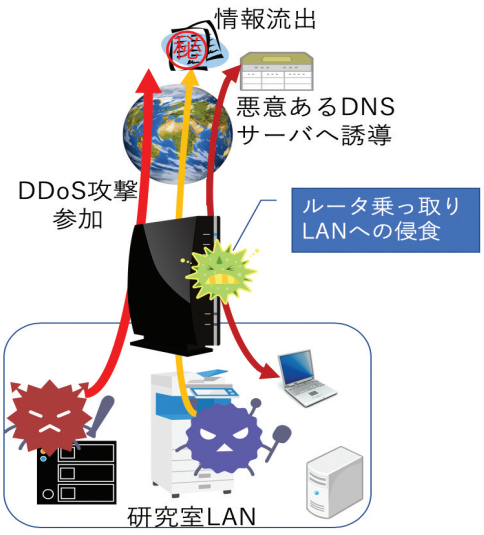

図１　IoT機器乗っ取りによる被害例

３．IoTのセキュリティ対策

IoTのセキュリティ問題に対し、各国で法規制が検討され始めています。本節では、米国の二例をあげます。

（１）カルフォルニア州法

2018年9月28日に州知事が署名し、2020年１月１日に発行予定のSB-327 (Information privacy: connected devices)[4]では、ネットワーク接続可能な装置に以下の要件を課します。

- 装置が適切に機能すること
- 収取・保存・送信される情報を適切に扱うこと
- 不正アクセス・破壊・使用・改変・暴露から機器本体と機器内データを保護する設計であること
- LAN外からの認証手段は以下のいずれかであること
  - パスワードを事前設定する場合は機体ごとに異なること
  - 初期設定でユーザにパスワード設定を求めること

SB-327は抽象的すぎますが、IoT機器に限定せず、インターネットに直接/間接的に接続する機器全てを対象とする点に特徴があります。

（２）米国連邦法案

2017年８月１日に上院て提出され審議継続中の米国連邦法案S.1691(Internet of Things (IoT) Cybersecurity Improvement Act of 2017)[5]では、連邦政府が調達するソフトウェア、ファームウェア、ハードウェアに対して、以下の要件を求めています。

- NISTなどが公開する脆弱性を含まないこと
- 適切に認証・信頼されたソフトウェア・ファームウェア更新がベンダーから提供されること
- 通信プロトコル、暗号、他機器との接続には廃止されていない業界標準プロトコルや技術のみを使用すること
- リモート管理、更新の配信、通信には固定またはハードコードされた認証情報を用いないこと

（３）IoT機器単体での限界

現在、多くのIoT機器でセキュリティレベルが低いことが問題になっていますが、SB-327もS.1691も極めて初歩的な要件であり、一般的な情報機器に求められる現在のセキュリティ要件に比べると不十分なのは明らかです。

例えば、NII-SOCSではLAN内の情報機器に盗聴ソフトウェアを仕掛け、平文通信による認証情報窃取の攻撃を確認しています。この攻撃には暗号通信による防御が最も効果的ですが、一方で、１銭単位で製造・運用コスト削減を求められるIoT機器の現状を踏まえると、最低限の要件のみにとどめざるを得ないのが現状です。

４．困難化するセキュリティ対策の即時適用

2017年４月に発生したWannaCryの事例[6]では、多くの病院や工場で情報機器やIoT機器が被害を受けました。WannaCry対策は、３月にマイクロソフ

ト社が提供したセキュリティパッチをOSに適用するだけで十分でした。しかし、サポートが終了していたOSをベースとした機器、もしくは、パッチ適用を見送っていた機器が多数稼働していたのです。

10年前であれば、パッチ適用やサポート切れ機器の撤去などの対策の即時実施は常識とされていました。万が一、パッチ適用の副作用で情報機器に不具合を生じても、予備機や手動作業に切り替えるなど代替策は存在していました。

しかし、我々の生活は情報機器なしには成り立たなくなりました。情報機器が高性能になり依存度が増すほど、24/365運用は当たり前で、手動での代替作業も不可能となり、運用停止を伴う対策実施のタイミングを計るのが難しくなりました。

例えば、制限時間内の処理完了というリアルタイム制御が求められるシステム制御分野では、対策実施により制御のタイミングが数ミリ秒ずれただけでシステム全体が機能停止に陥ることあります。他社でのWannaCry被害を聞き、慌ててパッチを適用した所、製造ラインが制御不能になり破損したという事例まであります。

対策実施そのものが業務全体を止めかねない程のリスク要因となった現在、実施前の十分な動作検証が必須となり、対策の即時実施は非現実的となったのです。つまり、人命に関わるシステムなどでは、後述する多層防御なしにIoT機器を含めた情報機器は使ってはならないのです。

5．実施可能な暫定策

IoT機器に比べ遥かに強固なセキュリティ要件を課されるパソコンやサーバ機器ですら、サイバー攻撃による被害が現在も発生しているのが現状です。IoT機器単体で取りうるセキュリティ対策は限られていますが、本節では、その幾つかをあげます。

（1）強度の高いパスワードや多要素認証

MIRAI[7]などIoT機器を標的としたマルウェアはメーカが工場出荷時に設定した初期IDとパスワードなどのリストを用いて辞書攻撃を行います。したがって、最低限のセキュリティ対策として、強度の高いパスワードへの変更が必須となります。特に、初期IDを変更できないIoT機器の場合、パスワードだけが唯一の防御となり、機器毎に異なるパスワードが理想となります。パスワードの強度については、パスワード強度チェックサイト[8]などで確認することができます（簡単なパスワードがどの程度で破られるかを確認するに留め、実際に使用するパスワードは入力しないことをお勧めします。）。

ただし、NII-SOCSでは、管理パソコンにマルウェアを感染させ、IDとパスワードの入力を盗み出す事例も確認していますので、強固なパスワードの過信は禁物です。

理想としては、多要素認証の導入となりますが、多要素認証に対応しているIoT機器が少ないのが現状です。

（2）閉域網による防御

数万台のIoT機器が接続されるような大規模ネットワークの場合、全ての機器で高い強度かつ個々に異なるパスワードを設定することは非現実的です。また、パッチの即時適用が困難な場合、機器単体でサイバー攻撃を防ぐことはできません。この場合、インターネットから隔離されたネットワークにIoT機器と管理コンピュータだけを収容する閉域網の使用が推奨されます。

しかし、2015年、blackhat USAにおいて、クライスラー社製自動車へのハッキング[9]が発表されました。閉域網のはずのネットワークへの侵入経路が見つかり、140万台の自動車がサイバー攻撃でステアリングやブレーキなどの制御を奪われる状況にありました。前述のWannaCryでも、WannaCryに感染したが発症していなかった保守PCを閉域網に持ち込んだため、爆発的に被害が広がったという事例もあります。

閉域網はサイバー攻撃による被害発生を緩和することはできますが、攻撃（マルウェア）の侵入を許せば一瞬にしてその防御能力を失うことを理解しておく必要があります。

（3）多層防御の採用

そもそもIoTの主要な用途であるシステム制御では、機器単体での障害対策はあり得ません。設計ミス、施工ミス、運用手順の想定漏れ、人為的ミスなど様々な要因により故障や異常動作が起きることを想定し、それらを前提とした保安計装を採用しています。次ページ図２は、それぞれ各層の問題をスイスチーズの穴に見立て、ある層の穴を他の層でカバーすることで、事故に至らないようにする多層防御の概念を示しています。言い換えると、全ての穴が繋がると事故に至ってしまうことになります。

不具合が人命に危害を及ぼす可能性があるシステムなどでIoT機器を使用する場合、IoT機器の異常動作を想定した対策が必要となります。この時、異常動作がサイバー攻撃によるのか、故障によるのかを区別して考える必要はありません。

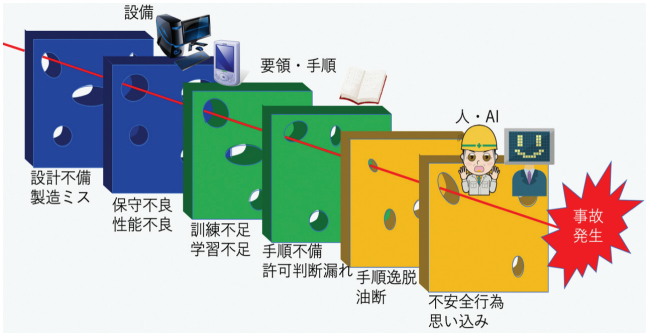

図２　多層防御の概念

６．可用性を重視したレジリエントな設計

従来の情報セキュリティでは、機密性（Confidentiality）が最優先とされ、次は完全性（Integrity）で、可用性（Availability）の最下位であるとする考え方が一般的であり、マルウェアに感染したパソコンは即座にネットワークから切り離すものとされてきました。しかし、IoT機器の停止や隔離を行なっても制御対象のシステムの安全性が確保できるかを検証する必要があります。

IoT機器の停止・隔離で被害箇所を局所的に抑え込みつつ、システムの安全性を維持するダメージコントロールという考え方が鍵となります。また、停止・隔離したIoT機器が担っていた機能を他のIoT機器、もしくは、手動により補う必要があれば、その分システムの機能は低下することになります。安全維持に必要な機能を優先しつつ運用を続けるデグレーデッドオペレーショイン（縮退運転）が必須となります。

このようにシステム全体の安全性を維持して運用を続けるレジリエントな設計が必須となります。

７．次世代サイバー攻撃対策技術

これまでに述べた対策は、暫定的なものであり、IoT機器の防御力は限定的と言わざるを得ません。この説では、現在、研究開発が急速に進みつつある次世代対策技術について説明します。

（１）セキュリティパッチ自動生成

2016年、米国DARPAが主催したセキュリティチャレンジ[10]では、チャレンジ当日に公開されたカスタムのOSやアプリケーションに対し、

- 脆弱性調査
- 攻撃プログラム生成
- 防御用セキュリティパッチ生成
- 攻撃の観測によるセキュリティパッチ生成
- セキュリティパッチの検証
- 攻撃と防御の選択

を人手を一切介さずに自動で行う機能を競い合いました。

当時は、小型IoTを想定した自動攻撃・防御システムでしたが、2018年にAndroid OS程度のバグ検知、パッチ生成、パッチ検証をAI技術を活用し自動で行う技術（Infer, Sapienz, Sapifx）が発表されました[11]。ただし、パッチは100％の完全性を保証できないため、その適用は人が判断する必要があります。

（２）不正機器自動検知

IoT機器本体に強固なセキュリティ機構を搭載することはコスト面からみて非現実的であるとして、2016年、米国MITREが次の条件下で、

- 大量のIoT機器が存在するネットワーク
- IoT機器への機能追加は認めない

不正なIoT機器を特定する技術を競うチャレンジを開催しました[12]。

８．まとめ

IoT機器はサイバー攻撃耐性が未成熟のまま急速に利用が広がっています。現在、我々が採りうる対策は暫定的なものですが、数年後には新たな対策技術の実用化が期待されます。一方、攻撃側も技術は向上し続けています。したがって、サイバー攻撃による個々のIoT機器での被害発生を前提とした、レジリエントなシステムの運用が必須になると考えます。

参考文献および関連URL

[1] Jonathan Ray, “Field Loadable Software,” Avionics, Nov. 2010, https://www.aviationtoday.com/2010/11/01/field-loadable-software/
[2] Exostar, “Identity Assurance in Commercial Aviation,” Oct. 2017.
[3] Avast Smart Home Security Report 2019, https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf
[4] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327
[5] https://www.congress.gov/bill/115th-congress/senate-bill/1691
[6] https://ja.wikipedia.org/wiki/WannaCry
[7] https://ja.wikipedia.org/wiki/Mirai_(マルウェア)
[8] https://password.kaspersky.com/jp/
[9] Charlie Miller, Chris Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” Aug. 2015, http://illmatics.com/Remote%20Car%20Hacking.pdf
[10] https://www.darpa.mil/program/cyber-grand-challenge
[11] Yue Jia, Ke Mao, Mark Harman, “Finding and fixing software bugs automatically with SapFix and Sapienz,” https://code.fb.com/developer-tools/finding-and-fixing-software-bugs-automatically-with-sapfix-and-sapienz/
[12] https://www.mitre.org/research/mitre-challenge/mitre-challenge-iot