インターネット防衛最前線　　—IoT セキュリティ研究の現場から—

後　編

—吉岡克成准教授—
（サイバー・ハードウェアセキュリティ研究群情報・物理セキュリティ研究ユニット）

【後編のはじめに】

いかがでしたか、前編の『IoT 機器を狙うマルウェア』。研究には囮のシステムを使うのですね。後編でご紹介するのは『インターネットカメラの覗き見』『重要施設のセキュリティ不備の発見』が中心ですが、こちらも前編と同様、『囮』が大きな役割を果たします。それではお楽しみください。

◇

1. インターネットカメラの覗き見

次に紹介するのはインターネットに接続したカメラ（これも IoT 機器です）の覗き見です。皆さんの中にも「一人で住んでいるお祖父さんが心配で見守り用に」とか「留守宅のワンちゃんの様子を見たい」とかでインターネットカメラをつけている人がいるかもしれませんね。街頭のカメラや工場や店舗の監視カメラにもインターネットにつながっているものがあります。

研究室には、このようなインターネットカメラが数台並んだ一角があります。レンズに映るのはソファとテーブル、大型テレビ、無造作に服のかかったハンガーラックなどです。こんなところにドラマのセットがあるわけはなく、学生の休憩場所にしては掃除が行き届き過ぎです。実は、このくつろぎコーナーは、インターネットカメラへの攻撃を研究するための囮だったのです。ここのカメラはインターネットに接続され、無防備なものが交じっていて、覗き見されるのをじっと待っています。長く待つ必要はありませんでした。最初の侵入は設置してから 5 日目にドイツからだったといいます。これを皮切りに、覗き見はどんどん増えました。

ところで、「無防備な」インターネットカメラとはどんなカメラでしょうか。簡単に言うと、パスワードが掛かっておらず、だれでも映像が遠隔から見えてしまうものや、掛かっていても容易に推測できてしまうカメラです。取り扱い説明書に初期パスワードが書いてあるものも多く、そのまま変更せずに使っていると、簡単に見破られてしまいます。

覗き見をする側の身になってみれば、いくら試してもヒットしなければ何もできませんから、諦めて次の獲物を探しに行きます。ですから、パスワードをわかりにくいものに変更

すると、たいへん有効に防御することができるのです。

なんとまあ、驚くべきことに無防備なカメラの映像を集めて公開しているサイトがあります。新聞でも話題になったから知っている人もいるでしょう[7]。INSECAM というロシアのサイトで、無防備なカメラの映像を世界中から集め、街頭でも工場でも個人の家でも無断で掲載しています。この囮部屋もすぐに見つかって掲載されました。それからもう、侵入者は千客万来、来るわ来るわの大盛況だったといいますから、大勢の人がこのサイトを覗いているのは間違いありません。ちなみに、大部分は日本からのアクセスだったそうです[8]。一方で、掲載されている無防備なカメラも日本のものが多いそうですよ。侵入した者の中には見るだけでは満足できないのかカメラを動かす者まで出てきて、URL とパスワードを書いたメモを映るところに置いておくと、そこへの侵入も増えたそうです。

ところで、INSECAM は安心して見てもいいのでしょうか。気になりますよね。今のところは「わかりません」としか答えようがありませんが、このようなサイトを開設する人（グループ）が信用できる人（グループ）だと、あなたは思いますか。決してお勧めしませんし、私は絶対にアクセスしません。図 2 に吉岡研究室の囮部屋の写真を載せておきます。右奥の棚に並んでいるのがカメラで、室内の家電はすべて IoT 機器です。

図 2.吉岡研究室の囮部屋（筆者撮影）

家の中にあって危険なのはカメラだけではありません。スマート TV だとかプリンタだとかシーリングライトだとか。他にも FAX 電話機、Blu-ray, DVD レコーダなどインターネットにつながる機器はたくさんあります。このようなものが、カメラと同じように勝手に操作されたらどうなるのでしょう。録画したはずの TV 番組が勝手に消されたり、深夜に突然、照明が点滅したりするのでしょうか。思わず「ホラー映画か！」と突っ込みたくなりませんか。吉岡研究室では家庭内の IoT 機器ネットワーク、ホームネットワークへの攻撃も研究対象にしています[9],[10]。インターネットにつながる家電を実際に繋いだり、仮想的にネットワークを作ったりして攻撃を観察したのですよ[10]。

2. 重要施設のセキュリティ不備の発見

ダムや水門などの治水施設や太陽光や風力発電所の監視や操作にも IoT 機器が使われています。インターネットに繋がっているといっても設定は非公開（のつもり）、組織や会社の外から見えない（はずです）。ところが実際には外から見えるものが沢山あるというのです。

こんな例があります。2017 年に、鹿児島県のダムがインターネットから丸見えになっていることが記事になりました[11]。この記事で吉岡は「ダムの水門や排水ポンプなどの管理

画面がネット上で丸見えになっている事象を 50 件以上発見した」と発言しています。また、吉岡はその都度関係者に情報提供していると言います[11]。東京オリンピック開催前には総務省の調査に協力し、その結果、200 件以上の注意喚起が行われました[https://www.ict-isac.jp/news/news20210901.html]また、インターネットカメラへの侵入から類推すると、攻撃した者が見るだけで満足してくれると期待するのは、ちょっと甘すぎるような気がします。実際、吉岡が設置した“おとりの”重要施設の遠隔監視制御システムにも不審なアクセスは多く、機器を制御しようとする試みが観測されているそうです。

さて、ここで、最近増えている身代金ウィルス『ランサムウェア』について述べておきましょう。ランサムウェアを使う攻撃者は企業や団体などのシステムを暗号化して使えなくしたり、秘密データを盗み出したりして「復旧して欲しければ金を出せ」「秘密を晒されたくなければ金を出せ」という脅迫を行います。最近の事件を 2 件紹介しましょう。どちらも報道されたので、知っている人も多いかと思います。

最初に紹介するのは日本での事件です。2021 年 11 月、日本の主要新聞、ニュースがランサム攻撃の記事を相次いで報道しました。記事によると、10 月 31 日、徳島県西部のつるぎ町の町立半田病院がランサムウェアの攻撃を受け、電子カルテや会計システムが使えなくなって混乱が続いているということです。病院は身代金を払わず、2 億円かけてシステムを作り直すことにしたそうです[12],[13],[14],[15],[16]。

次は米国での例です。半田病院の事件に先立つ 5 月、米国の燃料パイプラインがサイバー攻撃で停止し、米国東海岸の燃料パイプラインが約 1 週間停止しました。この事件で被害を受けたコロニアル・パイプライン社はビットコインで 440 万ドル（約 4 億 8000 万円）を支払ったと証言しています[17]。

僅かな隙が億単位の損害につながるとは、本当に「恐ろしい」としか言いようがありません。なお、NAS と呼ばれるネットワーク接続した記憶装置（これも IoT 機器）もランサム攻撃の対象になっており、吉岡研究室ではこの調査、分析を行っているそうです。

3. 研究成果を公表することのジレンマ

ここで仮定の問題を一つ出しますので、答えを考えてみてください。あなたならどうしますか。

仮にあなたがセキュリティの研究者だったとして、ある機器の脆弱性、攻撃に弱いところを見つけたとしましょう。あなたはすぐに発表しますか、それとも発表しませんか。

「これは放っておくと大変危険な欠陥だ。すぐに発表して皆で対策を立てなければ」と言うのは一つの考え方です。でも、そんなことをすれば悪い奴らにも教えることになって、かえって危ないことにならないでしょうか。

それなら反対に、「悪い奴らに知られて攻撃されたら困る」と考えて隠しておく方が良いのでしょうか。でも、他の誰かが見つけるのは時間の問題かもしれません。そして見つけた

「誰か」が同じように隠しておくとは限りません。その「誰か」に悪意があれば、他人に知られる前に攻撃を始めるでしょう。そのときになって「あのとき発表しておけばよかった」と臍を噛んでも取り返しはつきません。

このように、公開と秘匿のメリットとデメリットは表裏一体です。どちらに光を当てても反対側に影ができます。

このジレンマに対して研究者がたどり着いた一つの答えは、研究倫理のイシューとして扱い、公開のルールを作ることでした。研究倫理については生命科学が先行していて「ベルモント・レポート」と言う規範を公開しています。情報科学の研究者は、この「ベルモント・レポート」をベースにして情報科学の規範を作りました。それが「メンロ・レポート」(2012年)です。ベルモントレポートで謳われた人格の尊重、恩恵、正義の上に法と公益の尊重が追加されているということです。その後、学術国際会議や学会でも議論が進められ、現在は論文誌、学会発表に投稿、応募するためには研究倫理を明記すること、自組織での研究倫理委員会で承認を受けることが求められています[18]。

実例として吉岡が著者に含まれている論文を一本紹介しましょう。この論文は、そのうちの一節が「研究倫理的考察」に割かれています。引用は次の斜体字部分です。

◇

当該研究はメンロレポート[33]に規定される研究倫理原則に基づき実施した.IoT マルウェアの持続的感染の有無は対策を検討する上で重要な要素であるにもかかわらず，これまで十分な研究が実施されておらず，正確な情報が提供されていないのが現状である.特に 2016 年に大流行した Mirai やその亜種が持続的感染機能を有していないことから，一般に IoT マルウェアが持続的感染しないという誤った認識に基づき対策が検討される恐れがある.本研究は，IoT マルウェアの持続的感染の可能性について，機器の性質をふまえて体系的に検討するとともに複数の具体的対策方法を示すものであり，今後出現する可能性がある持続的感染型の IoT マルウェアへの対策に資すると考える.一方，本研究成果の悪用の影響を最小化するため，具体的な機器の情報の匿名化を行うことで直接的な悪用を防ぐとともに，情報処理推進機構・JPCERT/CC に当該研究成果に関する情報提供の実施，及び本論文の執筆にあたり新たに持続的感染の可能性が明らかとなった機器のメーカーへの情報提供を実施する予定である.1 機器に関しては情報処理推進機構を窓口として JPCERT/CC 及び機器のメーカーへ情報提供済である.残る 5 機器に関しても，本論文の公表の 90 日前までに情報提供を実施する予定である.このように本研究により得られる恩恵は，その悪用による潜在的な危害を大きく上回ると考える. [19]

◇

お分かりいただけましたでしょうか。この一節では、この研究がメンロレポートに準拠した研究であることを最初に述べ、その上で(1)論文発表することが IoT 機器の安全性向

上に役立つ理由と、(2)論文発表の悪影響を最小限に止めるために採った措置を書いた上で、発表による社会の利益が不利益を大きく上回ると主張しています。このようにセキュリティ研究者は自らの研究がもたらす恩恵を最大化し、危害を最小化する努力を継続し、社会に役立ち、公開に値する研究になっているか自問を続けているとのことです。

最後に、これからのサイバーセキュリティについて筆者の私見を述べさせてもらいましょう。

コロナ禍以前から、日本のデジタル化は遅れていると指摘されてきましたが、コロナ禍で、この遅れが目に見える形で噴出しました。保健所の感染者報告が手書きとＦＡＸで行われていて大混乱に陥り、それに代わって作られた”HER-SYS”というシステムが使いにくい物であったとか[20],[21]、在宅勤務は進んだものの押印のために出社するハンコ出勤が残ったとか[22]、遅れを示す事例には事欠きません。もちろん、ハンコ出勤はボクもしました、ブツブツ言いながらですけど。このほかにも自嘲というか自虐というか、笑えない笑い話は枚挙にいとまがありません。

さすがにこれでは……、と思ったか、デジタル庁を発足させるなど、日本もようやく重い腰を上げそうな気配が見えてきました。これが束の間の蜃気楼で終わるのか、それとも昔とったキャッチアップの杵柄でデジタル大国が実現するのか、まだまだ見通せませんが、少なくともインターネット、IoT を利用する機会は確実に増えるでしょう。そして、それに合わせてサイバー攻撃の刃は研ぎ澄まされて行くことでしょう。

セキュリティ研究のネタが尽きることは、どうやらなさそうです。そして、吉岡研究室はこれからも戦い続くのです。喜んでいいのか悲しんでいいのか分かりませんけど。

文　献

[1] “在宅勤務に 3 つの脅威　サイバー攻撃にどう備える” 日本経済新聞 2020,7,27,2:00. https://www.nikkei.com/article/DGXMZO61875010S0A720C2X11000/）

[2]横浜国立大学 H P>研究者総覧>吉岡　克成>研究分野・キーワード https://er-web.ynu.ac.jp/html/YOSHIOKA_Katsunari/ja.html(2021,11,18 検索)

[3] Tsutomu Matsumoto “Challenges for IoT Cyber Physical Society “ IoT Security Forum in Bangkok 2020, (2020) Bangkok.

[4]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　吉岡克成　ホームページ http://yoshioka.ynu.ac.jp/research.html (2021,11,18 検索)

[5] 吉岡” IoT 機器から 600Gbps を超える DDoS 攻撃” 日経 XTECH （2016,12,12） https://xtech.nikkei.com/it/atcl/column/16/112900283/112900001/

[6] 清嶋” DDoS 攻撃招く IoT 機器に回収騒ぎ、マルウエア「mirai」の脅威が深刻に” 日経 XTECH 2017,01,25）

https://xtech.nikkei.com/it/atcl/column/14/346926/012300784/
[7] “防犯映像、世界丸見え　事務所／美容室／街頭…　国内１５００台、専用サイトで閲覧　露から発信” 毎日新聞 2019,12,20.
https://mainichi.jp/articles/20191220/ddp/041/040/012000c
[8]”IoT マルウェア大量感染の現状と対策　最終回　国内外研究機関と連携し観測網拡大おとりにネットワークカメラも採用” 日経コンピュータ 2016,09,01. pp74-77.
[9] 横浜国立大学 × BBSS “2018 年度 IoT サイバーセキュリティ共同研究プロジェクト” BB ソフトサービス H. P. 2018,07,05. https://www.bbss.co.jp/news/iot_lab.html
[10] “「バーチャル IoT ホームハニーポット」で IoT サイバーセキュリティ脅威を観測
横浜国立大学と BB ソフトサービスが 2018 年度の共同研究を開始 “ BB ソフトサービス H .P. 2018,07,05. https://www.bbss.co.jp/news/2018/news_20180705.html
[11] 清嶋 “鹿児島県　ダムの管理画面がネットで丸見えに 「非公開」の誤解が事態招く” 日経 XTECH 2017,11,20.
https://xtech.nikkei.com/it/atcl/ncd/14/379244/111600080/
[12]“カルテ暗号化、病院まひ ランサム攻撃で 徳島・つるぎ町「災害と同じ事態」 復旧めど立たず” 日経新聞 2021,11,12,14:30
https://www.nikkei.com/article/DGKKZO77500100S1A111C2CE0000/
[13] “病院にサイバー攻撃、新規患者受け入れ２か月停止…身代金払わず２億円で新システム” 読売新聞オンライン 2021,11,26,22:29.
https://www.yomiuri.co.jp/national/20211126-OYT1T50244/
[14] “病院がサイバー攻撃を受けたとき　消えた電子カルテの衝撃” NHK 2021.11.19.
https://www3.nhk.or.jp/news/special/sci_cul/2021/11/special/story_20211119/
[15] “徳島の町立病院にサイバー攻撃　新規患者受け入れ停止　復旧は未定” 毎日新聞 2021,l1,10 .10:23
https://mainichi.jp/articles/20211110/k00/00m/040/028000c
[16] “病院プリンター、一斉に犯行声明　身代金ウイルス、町の医療脅かす” 朝日新聞デジタル 2021,11,28,5:00
https://digital.asahi.com/articles/DA3S15125921.html?iref=pc_ss_date_article
[17] “米コロニアル CEO が証言　身代金支払い「苦渋の選択」” 日本経済新聞電子版 2021,6,9, 2:28 (2021, 6,9, 7:52 更新)
https://www.nikkei.com/article/DGXZQOGN08ENB0Y1A600C2000000/
[18] 秋山、吉岡 ”サイバーセキュリティ研究倫理と日本における活動” ITU ジャーナル 48-5, 21-24, (2018,05)
[19] 原、田宮、鉄、渡辺、吉岡、松本 ”感染持続型 IoT マルウェアの実態調査と実機による概念検証” 電子情報通信学会論文誌 B J102-B, 8, 524-535 (2019)
[20] “社説　コロナ情報共有　現場が使いやすいシステムを” 読売新聞オンライン

2020,10,08 05:00　https://www.yomiuri.co.jp/editorial/20201007-OYT1T50253/
[21] “紙とファクスで混乱した感染状況　国のデータ戦略どこに”　朝日新聞デジタル版
2020,7,2, 19:47
https://digital.asahi.com/articles/ASN72659BN6NULBJ009.html
[22] “在宅勤務なのにハンコを押すために出社…” NHK 2020,4,11,3:47
https://www3.nhk.or.jp/news/html/20200411/k10012381401000.html

（先端科学高等研究院　研究戦略企画マネージャー　中川正広）