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—

前　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）

【はじめに】

突然ですが、マルウェアを知っていますか。そうです、コンピュータ・ウィルスのことです。インターネットからコンピュータに入り込んで攻撃をするソフトウェアですね。みなさん、対策は十分ですか。パソコンとスマホの OS はちゃんと更新していますか。アンチウィルスソフトも最新バージョンにしていますよね。あやしげなホームページには繋いだことがないですね。でも、パソコンとスマホだけの安全対策では不十分なのだそうです。

今、IoT 機器を狙うマルウェアが猛威を奮っています。

IoT 機器の一つに VPN 装置があります。VPN は、会社と家庭を暗号通信で繋ぐ装置・システムです。在宅勤務に不可欠なので、コロナ禍で急速に数が増えました。中には急拵えでセキュリティの不十分なものがあって、その隙をついた攻撃が増えているのだそうです[1]。ビジネスで使う IoT 機器は、ふつうは会社の情報システム部門が管理しているので、それ以外の社員には滅多に触る機会がありません。しかも、IoT 機器の中にはファームウェアの更新が簡単にはできないものや、無防備な通信プロトコル Telnet が動作しているものなど狙われやすい機器が結構あるのです。ですから、IoT 機器を攻撃から守ることは『言うは易し』の典型です。

いったい、どういうことでしょうか。横浜国立大学の吉岡克成先生に聞いてきました。

吉岡（以下、敬称略）は横浜国立大学先端科学高等研究院サイバー・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の准教授で、大学院環境情報研究院 社会環境と情報部門の准教授でもあります。研究分野は『情報セキュリティ、情報システムセ

キュリティ、ネットワークセキュリティ』です[2]。舌を噛みそうなので勝手に超訳すると、『情報システムとインターネットの安全を守るための研究』と言うことでしょうか。研究内容は、細分化して数えるとたくさんになりますが、その一つに IoT 機器のセキュリティ研究があります。インターネットや情報システムに潜むウィルスの動きを観察して特徴を把握して対策を作り出す研究です。

今回は、さらにその中から『IoT 機器を狙うマルウェア』『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』の三つについての研究を紹介しましょう。それぞれについて『どのような研究をしているのか』『研究で何がわかったのか』『サイバー攻撃を予防するためには何をすればよいのか』を説明していただきました。ここから先は、それを私なりに整理したものです。『研究成果を公表することのジレンマ』についてもお話をいただきましたので、2 回に分けて紹介しましょう。前編は、主に『IoT 機器を狙うマルウェア』、マルウェアから IoT 機器を護るための研究、後編は『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』、外部からの侵入についての研究紹介が中心です

それでは、はじめましょう。

◇

1. IoT 機器を狙うマルウェア

最初に紹介しますのは『IoT 機器を狙うマルウェア』の研究です。この研究には、研究室のハニーポットとサンドボックスが重要な役割を果たしています。聞き慣れない言葉ですが、いったい何のことでしょう。どちらも IoT のセキュリティ研究になくてはならないものです。

ハニーポットは甘い匂いで虫などを誘き寄せる蜜壺という意味です。ここではマルウェアを誘き寄せて捕まえるシステムを指します。サンドボックスは砂場、マルウェアの挙動を観察・解析するシステムです。

インターネットの空間を、無数のソフトウェアやデータが飛び交っている様子を想像してみてください。その中には IoT 機器を狙うマルウェアがたくさん交じっていて、狙った種類の IoT 機器を見つけると即座に取り付きます。取りついた先の IoT 機器にセキュリティ脆弱性が無ければ、(家に例えれば、「鍵が掛かっていれば」) そのまま離れ、脆弱な (鍵がかかっていない) IoT 機器だったら入り込みます。入り込んだ先ではひたすら増殖に励み、分身をどんどん外にばら撒くのです。ばら撒かれたマルウェアは次の獲物を探して飛んで行きます。別の獲物に取り付いて、また同じことを繰り返します。こうしてマルウェアは感染しながら数を増やして行くのです。コロナウィルスと全く同じですね。マルウェアに感染した沢山の機器を操る悪の親分サーバは別にあるのですが、これは後ほど。

ところで、コロナウィルスの実効再生産数が、マスクや手洗いなどの対策で変えられるように、マルウェアの増殖もセキュリティ対策で抑えられることは注意しておいていいでし

ょう。セキュリティ対策こそが自分を守ることであり、社会を守ることに繋がるのですね。これもコロナウィルスとそっくりです。

ある日、悪の親分サーバが突然、ある指令を出します。ばら撒いたマルウェアは実は全て子分で、このとき一斉に反応し、特定のサーバを狙って一斉攻撃を開始します。いわゆるDOS 攻撃、DDOS 攻撃です。どうですか、パソコンとスマホの安全対策だけでは不十分でしょう。

でも「自分のうちの IoT 機器にセキュリティ対策がきちんとされているかどうかなんてわかりません、どうやってするのですか。そもそも、ウチの家に IoT 機器があるのかどうかさえ分かりません」と言うのが普通でしょう。

IoT 機器とは何でしょうか。IoT は『モノのインターネット』、モノどうし、機械どうしがデータをやりとりして仕事をするシステムです。よくある IoT はセンサから周囲の状況を読み取って、それに合わせた働きをします。例えば「住宅への不審者侵入を感知して遠くにあるセキュリティ会社の警報盤を鳴動させる」とか「カメラでダムの水位を観察して遠くの監視センターのモニターに送る」とかいう働きです。IoT 機器は IoT システムに使われる機器、ここではセンサやカメラがそれに当たります。家にある家電ではプリンタ（複合機）、無線 LAN ルータ、スマートスピーカ、テレビ、ＴＶチューナ、ＤＶＤデッキ、固定電話・FAX なんかでインターネットに繋がる物は IoT 機器ですね。ビジネスの現場、例えばオフィスや工場、倉庫などにもたくさんありますよ。

さて、話をハニーポットに戻しましょう。先ほど言いましたようにハニーポットは脆弱な（無防備な）IoT 機器に擬態した振る舞いをして、気づかずに侵入してくるマルウェアを騙して捕まえます。こういう話を聞くと食虫植物とか、ゴキブリを捕える例の紙箱とかを連想してしまいがちですが、ここは可愛らしく『蜂蜜の壺』を思い浮かべましょう。

囚われの身となったマルウェアはどうなるのか。ハニーポットは、捕まったことを知らないマルウェアを『サンドボックス』に護送します。『サンドボックス』は、公園で子どもたちが遊ぶ砂場です。仕切りで囲った狭い所で、子どもが好き勝手に遊び回るのを大人たちが見守るように、マルウェアはサンドボックスの中では自由に動くことができます。それを周囲から研究者が見守るのです。

小学生の頃、蟻の観察をしたことのある人は覚えているでしょう。砂糖に集まった蟻を掬い上げて捕まえ、土を入れた透明容器に入れますと、蟻は巣作りをしたり、与えた餌を取りに出かけたりします。蟻は普段通りに活動して生活の様子を見せてくれますが、容器から出ることはできませんでしたね。しっかり観察してノートをとれば、自由研究の一丁上がりです。サンドボックスは、これと同じような使い方をすると思えばよいのではないでしょうか。

何はともあれ、吉岡研究室の心臓はこの『ハニーポット』と『サンドボックス』と言っても間違いではないでしょう。今、この瞬間にもマルウェア捕まえているかもしれませんね。

ところで、この『ハニーポット』は欧米やアジアなど２２か国に置いてあります[3]。そして、世界で捕まえたマルウェアは、ここ横浜の吉岡研究室の『サンドボックス』に護送さ

れ、そこで分析されます。まさに、国際共同研究のハブ、要と言ってもいいでしょう。

吉岡研究室では、オランダのインターネットサービスプロバイダに感染状況を伝え、共同研究のパートナーを通じて警告してもらったことがあるそうです。他にもハニーポットを使って、さまざまなIoT機器が感染していることを解明し、世の中に知らせてきました[4]。捕まえたマルウェアの検体や解明した特徴の情報は、すでに 150 を越える研究組織やウイルス対策ソフトを作るセキュリティベンダーに提供しています[4]。他の大学や研究所での研究にも役立ち、ウィルス対策の向上にも役立っているのです。私たちがインストールするセキュリティソフトの更新にも、吉岡研究室の成果が使われているかもしれませんね。

マルウェアは、コンピュータや社会にどのような被害を与えるのでしょうか。IoT を狙うマルウェアで有名なものに Mirai というものがあります。Mirai は守りの弱い IoT 機器を探してインターネット上を飛び回っています。先に述べましたように、取り付いたデバイスを一台感染させると、そこでたくさんの分身をばら撒きます。ばら撒かれた分身は次の犠牲者を求めて二次感染、三次感染を繰り返して増殖し、あっという間に蔓延するのです。コロナウィルスにそっくりですね。Mirai は 2016 年に急増して大きな被害を与え、IoT 機器のメーカ 2 社が製品を回収する事態になりました[5],[6]。図 1 にハニーポットとサンドボックスの中心となるサーバの写真を載せておきましょう、見た目は変わり映えしませんが、マルウェアに取っては出会いたくない強敵です。

図 1.ハニーポット・サンドボックスの
中心となるサーバ（筆者撮影）

文　献　（前後編）

[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）