桑名レポート：サイバーセキュリティの現場から（4）

IoT機器のセキュリティ対策

NTT アドバンステクノロジ株式会社
常務取締役　セキュリティ事業本部
本部長　桑名 栄二
博士（工学）、CISSP

本稿では、IoT 機器やシステムへの攻撃事案を報告するとともにそのセキュリティ対策について述べる。

急増するIoT機器

米カリフォルニア州知事は本年 9 月 28 日、IoT（Internet of Things）機器（Connected Device）を対象とするセキュリティ法案（SB-327）に署名し、米国で初めて IoT セキュリティ法が成立した [1]。2020 年 1 月に施行されると、IoT 機器の製造業者は、その機器に適切なセキュリティ機能を装備しなければならないことなる。

IoT は近年その市場の成長性で注目されている分野であり、IoT 機器は 2020 年には約 300 億個となる見通しという報告もある [2]。IoT 機器は、我々の身近にあるウエアラブル機器、スマートスピーカ、監視カメラ、HEMS（Home Energy Management System）等に加え、電力・ガス・水道設備、工場、化学プラント、交通制御など古くから利用されてきた産業用制御システム（ICS:Industrial Control System）や監視制御システム（SCADA:Supervisory Control and Data Acquisition）、さらに今後も拡大する「自動車」や「医療機器」なども含まれる。爆発的に増加する IoT 機器の弱点を突いたサイバー攻撃は増加傾向にあり [3]、カリフォルニア州の IoT セキュリティ法の成立が示すようにセキュリティ対策の重要度が増している。

IoT攻撃事案

①重要インフラ攻撃事案

2016 年のウクライナの電力システムが大規模停電に至った CrashOverride マルウェア [4] や、2017 年 12 月に報告された産業制御システムの安全装置（安全計装システム）を不正操作する HatMan マルウェア（TRITON、TRISIS）[5] など多くの事案がある。また、2016 年に米国 ICS-CERT が対応したインシデント件数は 290 件で、その内 63 件は製造業、62 件は通信インフラ、59 件はエネルギー関係であったとの報告もある [6]。その主な攻撃の手口はスピアフィッシング、認証基盤の脆弱性をついた攻撃、ネットワークスキャン等で、290 件のインシデントのうち 6 件はビジネスやサービスに重要な影響を与えたようである。

②DDoS攻撃事案

2016 年 9 月に米国の著名なセキュリティブログ「krebsonsecurity.com」は 620Gbps 以上の大規模な DDoS 攻撃を受けた [7]。幸いにもサイトダウンには至らなかったようであるが、これは約 38 万台の乗っ取られた IoT 等の機器で構成される超巨大ボットネットを使った攻撃と見られている。また同年 10 月には、DNS を提供する米企業「Dyn」を狙ったサイバー攻撃が発生し、Twitter、Netflix、Spotify などのサイトに接続できない状態が断続的に続いた [8]。原因は krebsonsecurity.com への DDoS 攻撃と同じで、マルウェア「Mirai」の辞書攻撃によって乗っ取られた監視カメラなど数十万台の IoT 機器からの大規模な DDoS 攻撃であり、DNS システムが影響を受けた。

③情報漏洩と乗っ取り事案

MQTT（MQ Telemetry Transport）は、M2M や IoT などで広く採用されているメッセージプロトコルで、ブローカーと呼ばれる仲介サーバを介して通信を行う。IOActive 社の Lucas Lundgren 氏は Black Hat 2017 で、デフォルトで暗号化されていないポート 1883 番を使うブローカーがインターネット上に 8.7 万台以上あり、多くの MQTT 通信は暗号化されていない状況でかつ、なかには ID/ パスワードも十分に設定されていない状況であることを発表した [9]。Lundgren 氏は、情報閲覧以外にリモート操作も可能で、監房ドアのロック解除や計測器のデータ改ざん、鉄道の運行情報の改ざんなど、大事件・大事故

に繋がる問題への警鐘を鳴らした。

また、2017年7月IoTセキュリティ企業Senrio社は、OSSのWebサービスライブラリ「gSOAP」にスタックバッファオーバーフローの脆弱性（Devil's Ivy）を発見した。この脆弱性により監視カメラなどIoT端末がリモート攻撃の脅威に晒された[10]。

その他、Kaspersky Labは2018年上半期に発見されたIoTマルウェア数は、2017年の総検出数の3倍以上の12万個に増加していると報告している[11]。

IoT機器のセキュリティ対策

電力・ガス・水道、工場など社会インフラは、その影響範囲・影響度合いが大きいから狙われるが、そもそもID/パスワードを工場出荷時のままで設置・運用している、不要なポートを開けたままにしている、SSL通信を利用していないなど、IoT機器やシステムを安全に実装・利用していないケースも多い。つまり利用する人間側の問題も攻撃者から狙われてしまう大きな原因である。サイバー衛生（Cyber Hygience）含め、下記に示すようなセキュリティ対策が急務である。

①基本的なセキュリティ対策

パスワード等の認証設定は初期設定のまま利用せず変更する、IoT機器のファームウェア最新版への更新等、常に最新の状態に保つことが必要である。またトランスポート層の対策としてTLSの利用、ネットワーク層ではIPSec、WPA3の利用、さらにはHIP等の新しい技術を利用したネットワーク分離[12]も有効と考える。

②情報収集・共有

インターネットに接続されているIoT機器の情報（OS、オープンポート、バナー情報等）を検索できるサービス（SHODAN[13]、censys[14]等）やインターネット上の攻撃トラフィックを可視化するNICTのNICTER等を利用し、最新の脅威、脆弱性情報を収集し、対策を講ずることも有効である。これらは収集したデータを研究用や脆弱性の確認目的として活用することを想定しているが、一方で攻撃者がサイバー攻撃の標的を探すために悪用される危険性もあり、またオープンにすべきでない情報等も存在するので、目的を絞った独自の情報収集システムの構築も必要である。

③脆弱性検査やIoTセキュリティサービスの利用

IoT機器の脆弱性をチェックするセキュリティ診断サービスを活用し、IoT機器の脆弱性を把握し、セキュリティ対策を講ずる。例えば、2018年9月にSPIRENT社のSecurity LabsのIoT診断サービスは米国CITAのIoTサーバーセキュリティプログラムに認定された[15]。その他、IoT機器のモニタリングサービスを提供するarmis社[16]や、ICSを主ターゲットとして監視サービスを提供するCyberX社[17]、医療機器の可視化、異常検出、セキュリティ防御を得意とするMEDIGATE社[18]などもある。

④各種ガイドライン活用

IEC-62443、NISTサイバーセキュリティフレームワーク、OWAPS IoT Security Guidance等を活用し、セキュリティチェックを行ったり、社内基準を制定し運用することも重要である。

⑤法整備

IoTを狙ったサイバー攻撃の対策強化は各国で進められている。冒頭の米カリフォルニア州以外にも、米下院は「DHS産業用制御システム機能強化法2018」を本年8月に承認した。国内でも、総務省は2018年度の通常国会に電気通信事業法と国立研究開発法人情報通信機構（NICT）法の一部改正を提出、可決・成立した。

これらの総合的な対策の継続的な取り組みが今後さらに重要である。

[1]https://www.cnet.com/news/california-governor-signs-countrys-first-iot-security-law/
[2]http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc133100.html
[3]http://www.nict.go.jp/press/2018/02/27-1.html
[4]https://www.us-cert.gov/ncas/alerts/TA17-163A
[5]https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF
[6]https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf
[7]https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[8]https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[9]https://www.blackhat.com/docs/us-17/thursday/us-17-Lundgren-Taking-Over-The-World-Through-Mqtt-Aftermath.pdf
[10]https://japan.zdnet.com/article/35104643/
[11]https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018
[12]https://www.temperednetworks.com/
[13]https://www.shodan.io/
[14]https://censys.io/
[15]https://www.spirent.com/Newsroom/Press_Releases/Releases/2018/September/09-18_Spirent-Approved-as-Authorized-Test-Lab-for-New-CTIA-IoT-Cybersecurity-Certification
[16]https://www.armis.com/
[17]https://cyberx-labs.com/en/
[18]https://www.medigate.io/