日本のコンサルタントの見解
DDoS攻撃 (Distributed Denial-of-Service)

IoTの進展に伴い危険性が拡大

DDoS攻撃によるリスクは以前からあるが、近年のIoT化の進展に伴い脆弱なデバイスがボットに加わるようになり、2016年はMiraiのようなマルウェアによって攻撃規模が飛躍的に拡大した。

Miraiのソースコードは公開され、その亜種も出現している。DDoSプログラムのアンダーグラウンド市場での金銭価値は、攻撃対象の規模とサービスの社会的・経済的重要性に比例する。今後、攻撃者はより多くの脆弱なデバイスをボットネットに組み込むために、DVR、CCTV（IPカメラ）、ルーターの更に内側にあるデバイスにも感染を拡大させようと、マルウェアを改悪する可能性が高いと考えられる。本章にも解説されているとおり、デバイスのセキュリティ対策は総じて不十分であるため、攻撃者にとっては格好のターゲットとなる。

諸外国における規制強化

米国では2013年の大統領令で国家安全保障省（DHS）がサイバーセキュリティを主管することになり、16の重要インフラセクターはサイバーセキュリティ対策の底上げを始めた*12。デバイスにおいても医療、自動車セクターでは米国内の医療機器や自動車を対象にガイドラインやベストプラクティスの制定・施行を進めている。医療機器に至っては2016年末に市販後、つまり病院等で稼働しメーカーの手を離れたデバイスの脆弱性管理までをメーカーに求めるようになった*13。また、DHSは2016年11月に各セクターの取り組みを紹介しながらIoTセキュリティに関する指針*14を提示し、全セクターに対して更なる取り組みを促している。

連邦取引委員会（FTC）はIoTのセキュリティとプライバシーを対象としたレポートを発行する一方、2017年1月には、ドイツテレコムをターゲットとしたDDoS攻撃に利用された、Miraiに感染したルーターの生産元である台湾のデバイスメーカーD-Linkを「消費者をリスクに晒した」として提訴している*15。

EUおよび加盟国は米国の政策・規制に協調路線を取りながら推進している状況である。まずEUでは2016年4月にGDPR（一般データ保護規則）が制定され、個人データを収集、処理を行う事業者に対して多くの義務を課す一方、違反に対しては2,000万ユーロ、又は前年度の全世界売上の4%のいずれか高い方が制裁金として課すことが決められた*16。また、2016年8月にネットワーク・情報セキュリティ指令（NIS Directive）が施行され、各国は重要インフラ事業者に対するサイバーセキュリティ法整備を進めている*17。

これらの規制強化は、組織のセキュリティ・プライバシーを保護するため、インターネットの治安を守るためといった大義名分を掲げてはいるが、そこには外国企業・製品を排除しようとする保護主義的な思惑も透けて見えるようだ。

特に2017年1月のFTCによるD-Linkの提訴のケースは、同社も製品をアピールしていたコンシューマー・エレクトロニクス・ショー（CES）の開催期間中に発表されており、一種の「見せしめ」のようにも見受けられる。

法整備で遅れをとる日本

翻って日本ではデバイスのサイバーセキュリティ対策に対する法規制が不十分な状況にある。2016年7月に、IoT 推進コンソーシアムおよび経済産業省・総務省がIoT機器やサービスを提供する関係者が取り組むべき「IoTセキュリティガイドライン」を発表したが、これは法規制のような強制力を持たない*18。また、主務官庁はデバイスを対象とした規制やベストプラクティスを打ち出しておらず、諸外国と比較すると質、量ともに不足している。

現在は民間団体*19が主導し製品分野別のセキュリティガイドを発行するなどの活動をしているが、デバイスメーカー・サービス提供事業者の責任なども含めた形での、政府レベルによる法整備にはまだまだ時間がかかるだろう。

デバイスに組み込まれたソフトウエアに脆弱性があり、それを悪用されたサイバー攻撃により、利用者が被害を受けた場合の補償についてはどうだろうか。消費者保護の観点においては、消費者庁管轄の製造物責任（PL）法は1995年の立法時の考え方により、民法上の有体物、つまり動産であるデバイスのハードウエアを対象とし、無体物であるソフトウエアそのものは対象外としている。ただしソフトウエアが組み込まれたデバイスが、そのソフトウエアの不具合が原因で製品に欠陥があるとみなされた場合は、そのデバイスの製造業者には損害賠償責任が発生するとの解釈もある。しかし条文はなく、都度の状況の判断となるため、曖昧さが残る*20。製造物責任法を適用出来ない場合、消費者は民法の不法行為責任などに基づきメーカーに損害賠償を請求することが可能である。しかし、原告となる消費者はメーカー側の故意または過失などについて証明する責任を負っており、製造物責任法の認定要件と比較しハードルは高い。米国FTCのように法執行機関が消費者保護のために訴訟を自ら起こすことがベストであるとは思わないが、IoT化が進展する今後を見据え、組み込みソフトウエアに対するメーカーの責任認定に関してはガイドラインがあっても良いのではないか*21。

*12 Improving Critical Infrastructure Cybersecurity, U.S.Government, 2013/2/19: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
*13 NH-ISAC: http://www.nhisac.org/
*14 DHS Releases Strategic Principles For Securing The Internet Of Things, US Department of the Homeland Security, 2016/11/15:
https://www.dhs.gov/news/2016/11/15/dhs-releases-strategic-principles-securing-internet-things
https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
*15 FTC Says D-Link Routers and Cameras Are Vulnerable to Hackers, Fortune,2017/1/5: http://fortune.com/2017/01/05/ftc-d-link-hackers/
*16 Repealing Directive 95/46/EC (General Data Protection Regulation): http://eur-lex.europa.eu/eli/reg/2016/679/oj
*17 The Directive on security of network and information systems (NIS Directive): https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
*18 IoTセキュリティガイドライン, 経済産業省, 2016/7: http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html
*19 一般社団法人 重要生活機器連携セキュリティ協議会: https://www.ccds.or.jp/index.html
https://www.ccds.or.jp/public_document/index.html
*20 組込みソフトウエアを用いた機器におけるセキュリティ, 独立行政法人情報処理推進機構（IPA）,2006/4: https://www.ipa.go.jp/files/000003116.pdf
*21 製造物責任法とは,消費者庁: http://www.consumer.go.jp/kankeihourei/seizoubutsu/pl-j.html
製造物責任にかかわる法律, 国民生活センター, 2012/8: http://www.kokusen.go.jp/wko/pdf/wko-201208_12.pdf

日本企業に求められる対応

IoTデバイスを輸出する日本の機器メーカーは、諸外国の法規制に基づくサイバーセキュリティ・プライバシーの要求水準が国内とは異なるため、その差分を把握する必要がある。また、米国においてMirai等がターゲットにしているDVR、CCTV（IPカメラ）、ルーターなどを生産/販売している事業者は、D-Link社の場合と同様の訴訟とそれに伴うレピュテーションリスクが生じる可能性に留意することが必要だ。ちなみに、2017年2月現在、このD-Linkの訴訟について取り上げた日本国内のメディアはほとんどないが、企業側は今後、そうした情報への感度を上げていく必要がある。

IoTデバイスに関してはサイバーセキュリティが輸出戦略上のリスクであり、海外での売上比率を伸ばしたい日本企業にとって無視出来ないものである。製品のライフサイクル全般にわたりセキュリティ・プライバシー機能を具備していく「Security by Design*22」「Privacy by Design」を意識した製品開発が求められる。

またSecurity by Designの観点においては、市販後の自社製品に脆弱性が発見され、DDoS攻撃に巻き込まれた場合を想定した検討も実施すべきである。2012年に国内でホームルーターが数万台規模でサイバー攻撃の踏み台として悪用された*23。このケースでは、ルーターの製造メーカーがファームウエア更新をリリースするも、セキュリティを意識していない一般ユーザーは対応せず、複数のISPが直接ユーザーに電話なども駆使して連絡し、更新を促すという対応まで取っている。しかし、全ユーザーがファームウエアを更新するまでには相当な時間がかかるようである。

IoTの進展により、IT導入においてはデバイスの売り切りからサービス提供（従量課金）へのシフトが進みつつある*24。今後は法規制要求やDDoS攻撃への対応コストを踏まえ、メーカーが適切なタイミングでファームウエアを更新出来ることが重要になるため、セキュリティがIT-as-a-Service（ITaaS）へのシフトを加速させるドライバの一つに加わる可能性がある。既にITaaS型に切り替えたメーカーは、製品販売後の運用フェーズでサイバー攻撃を監視する等の対策を採っている。将来、サービス提供における運用業務の一環としてセキュリティリスクを管理出来るデバイスが増え、そのような方式が一般的になるだろう。その場合インターネットの治安維持という名目で、攻撃者に乗っ取られた、もしくは基準を満たさない脆弱なデバイスは通信キャリアから強制的に接続を遮断される、“繋がる世界の繋がせない仕組み”が作られる日が来るかもしれない。

日本担当者

小野寺　正
Onodera, Tadashi
デロイト トーマツ リスクサービス株式会社
マネジャー

システムエンジニアを経て、情報セキュリティ専業サービス企業で中央官庁からの調査研究の請負および政策提言をはじめ、セキュリティ戦略策定から技術的対策の導入まで幅広くプロジェクトに従事。また、業務プロセス改革、IT戦略立案/導入などにも従事。
現職では、デロイト トーマツ リスクサービスのIoTセキュリティ担当マネジャーとして、日本のみならずDeloitte海外事務所が実施するプロジェクトにも関与している。

*22 Security by Design の概要については以下を参照; 安全なIoT システムのためのセキュリティに関する一般的枠組、内閣サイバーセキュリティセンター（NISC）,2016/8/26: http://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf,
セキュリティ・バイ・デザイン入門, 独立行政法人情報処理推進機構（IPA）, 2016/11/17-18: https://www.ipa.go.jp/files/000055823.pdf

*23 IoT時代のセーフティ・セキュリティ確保に向けた課題と取組み, 独立行政法人情報処理推進機構（IPA）, 2015/12/7:http://sec.ipa.go.jp/users/seminar/seminar_tokyo_20151207-01.pdf

*24 「IT-as-a-Service」の章を参照（P55）