SENSOR

No. 023
2015/10
東京海上研究所ニュースレター

トピックス

IoT 時代のリスクと対策

あらゆるものがネットワークにつながる「モノのインターネット」(Internet of things:IoT)は、生活を便利で快適にする反面、私たちが日常使っている機器がハッカーに乗っ取られる、というような新たなリスクも生まれています。
本SENSORでは、IoT時代の家電や自動車のセキュリティリスクと対策についてご紹介します。

●新たなリスク

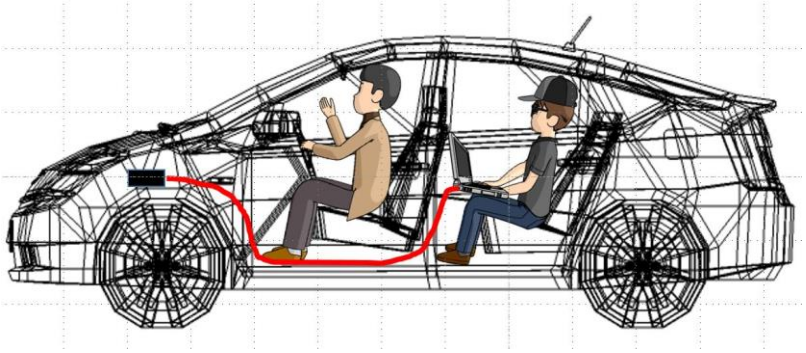
最近ではパソコンやスマホだけでなく、自宅のテレビ、DVD レコーダー、エアコンなど、実に様々なものがネットワークにつながっています。また、常時ネットワークと接続されて情報をやり取りする自動車なども現れました。あらゆるものがネットワークにつながる世界、これは「モノのインターネット」、"Internet of things"(IoT)と呼ばれています。

IoTは生活を便利にする反面、新しいリスクも生んでいます。これまで、家電や自動車は外部と接続されていなかったため、コンピュータウイルスやハッカーの侵入のことを心配する必要がありませんでした。しかし、IoTの時代には、サイバー攻撃によって自動車のハンドルが操作されたり、エアコンや洗濯機が勝手に動き出したり、DVDレコーダーに録画しておいた番組が消されたり、自宅の冷蔵庫が踏み台になってサイバー攻撃に荷担するというようなことも起こり得ます。サイバー攻撃の脅威はもはやパソコンやスマートフォンだけにとどまらず、ネットワークにつながる全てのモノが対象となる時代となっています。

●研究者による警告

幸い、現時点では家電や自動車などに対するサイバー攻撃によって死傷者が出た、という事例は報道されていません。しかし、そのような事故が起こりうるという警告は、ハッカーや研究者によって繰り返しなされています。

2013 年 8 月、米 Forbes 誌は車載システムのハッキング実験に関する記事とビデオを掲載しました1。自動車乗っ取りのデモを行ったのは Twitter のセキュリティ研究者 Charlie Miller 氏と、米セキュリティ企業 IOActive の技術者 Chris Valasek 氏。実験には Forbes 記者が運転するフォード「エスケープ」とトヨタの「プリウス」を利用しました。2人の研究者は車に搭載されているソフトウェアを解析し、後部座席でコンピュータを操作して警笛を勝手に鳴らしたり、高速走行中に急ブレーキをかけたり、ハンドル操作や GPS の誤動作、スピードメータ数値の偽装などができることを実証しました。この実験は自動車の電子回路と攻撃者のパソコンをケーブルで直接接続して行ったものですが、万一無線などで遠隔からハッカーに侵入されれば、外部からでも制御を乗っ取ることが可能であることを示唆しています。



(イメージ図:東京海上研究所にて作成)

また、米国のセキュリティ会社である Trustwave 社は、2013 年 8 月に、日本の住宅設備メーカーが提供する「スマートトイレ」に脆弱性が見つかったと発表しました。このトイレはスマートフォンのアプリから蓋の開閉、水勢、水温の調節などができるのですが、このアプリの脆弱性を利用することにより、攻撃者は自分のスマホから当該のトイレを制御できるようになると Trustwave 社は警告しています[2]。

同じく米国のセキュリティ会社、Proofpoint社が、2013 年の 12 月 23 日から 2014 年 1 月 6 日の間に世界規模で起こった迷惑メール攻撃を調査したところ、迷惑メールのうちの 75 万通はウイルスに乗っ取られた 10 万台の家庭用機器によって送られたものであると発表しました。家庭用機器とはルーターやマルチメディアシステム、テレビなどで、この中には「少なくとも一台の冷蔵庫も含まれている」として話題を呼びました。同社は「インターネットに接続する家庭用機器は侵入が容易で、ユーザーはセキュリティ対策に関心がなく、急速に増加するこれらの機器は脅威である」と警告しています[3]。

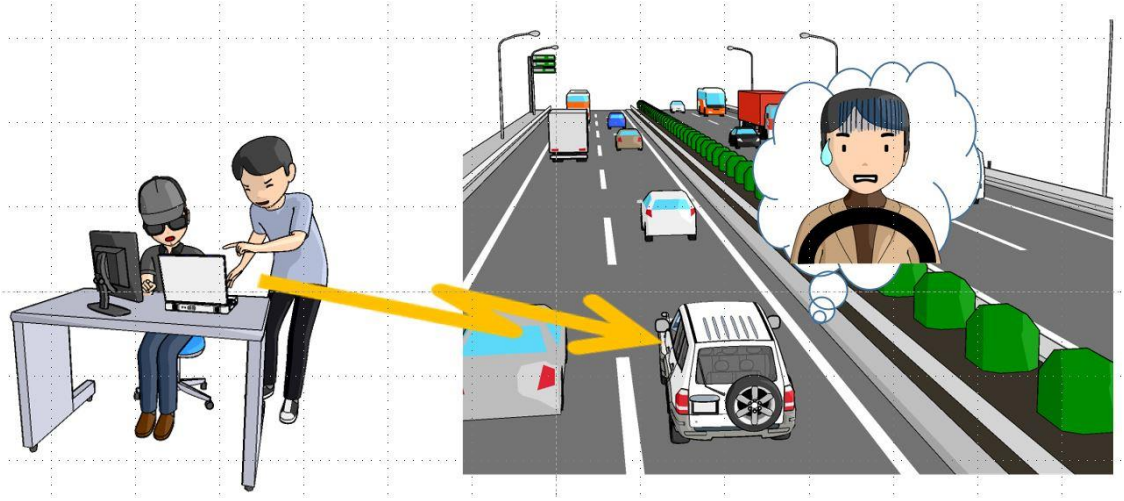
自動照準機能付きライフルをハッキングして、本来の意図とは異なる別のターゲットに照準を合わせるという衝撃的な実験結果も、今年の 8 月に開催された米国の大規模セキュリティカンファレンス“Black Hat”で発表されました[4]。この実験を行ったのはセキュリティ研究者の Runa Sandvik 氏と、夫の Michael Auger 氏。夫妻は TrackingPoint 社の TP750 ライフルを購入し、中身を解析して、WiFi 回線から侵入して照準を別のターゲットに合わせることが可能であることを発見しました。その様子はデモムービーで公開されています[5]。

（イメージ図：東京海上研究所にて作成）

●乗用車 140 万台のリコールも

今年の 7 月 24 日、米国のフィアット・クライスラー・オートモビル社（FCA）は、ハッキング対策のために同社の乗用車 140 万台をリコールすると発表しました[6]。これは、前述の研究者、Charlie Miller 氏と Chris Valasek 氏が米専門誌“WIRED”と共同でクライスラー車を乗っ取る実験を行い、ネット上で公開したことを受けたものです。今回の実験では、車載コンピュータにパソコンを直接接続するのではなく、外部から無線を経由して侵入し、ハイウエイを走行中の車のエアコンやラジオ、ワイパーを操作したり、車載ディスプレイにハッカーの姿を映したり、トランスミッションを切ったりするというデモンストレーションを行いました。さらに、低速度で走行中にエンジンを切ったりブレーキをかけたり、逆にブレーキを効かなくするという実験も行いました[7]。

これを受けて、FCA 社はハッキング対策のために無償で改訂版のソフトウェアを提供し、希望者はディーラーに持ち込めば無償でソフトウェアのアップデートをする対応をしたと発表しました[8]。



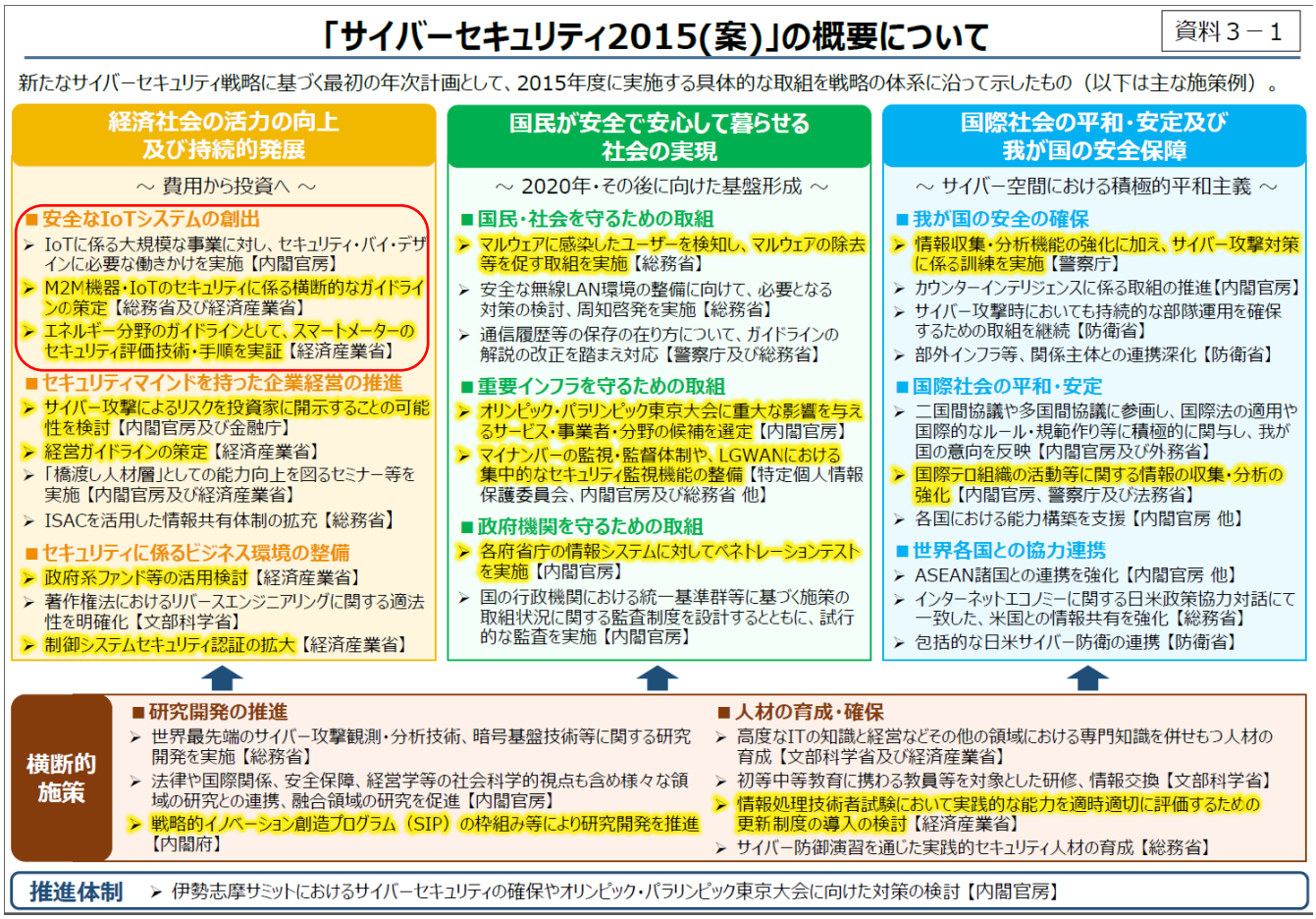
（イメージ図：東京海上研究所にて作成）

●強化される対策

増大するサイバーセキュリティのリスクに対し、国や業界団体も対策を強化しています。

内閣サイバーセキュリティセンター（NISC）は、本年９月４日に、新たなサイバーセキュリティ戦略を閣議決定しました[9]。これは2013年６月に国の情報セキュリティ政策会議で決定された「サイバーセキュリティ」のアップデート版です。

この新しい戦略は、サイバー空間を「無限の価値を産むフロンティア」と位置づけると同時に、サイバー攻撃の被害規模や社会的影響の拡大、脅威の更なる深刻化を予想しています。これに対し、ネットワークにつながる家電や自動車については、製品の企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進するよう経済界に要請しています。



（出典：内閣サイバーセキュリティセンター。赤枠は研究所にて追加）

民間の業界団体では、家電については一般社団法人重要生活機器連携セキュリティ協議会（Connected Consumer Device Security council：CCDS）[10]など、自動車については一般社団法人 JASPAR（Japan Automotive Software Platform and Architecture）[11]などが、セキュリティに関する調査・研究および企業を横断した安全対策、安全基準作りを行っています。

●個人としてできる対策

個人としても、これまでパソコンやスマホに対して行ってきたセキュリティ対策と同様の考え方で、家電や自動車のセキュリティ対策にも留意する必要があると言えるでしょう。

例えば自動車の場合は、

- 自動車にスマートフォンと連動させる機能がある場合は、スマートフォンにアンチウイルスソフトを導入するなど、スマートフォン側にも十分なセキュリティ対策を施し、信頼できないソフトウェアはスマートフォンに入れない。また、パスワードを設定する場合は 0000、9999、1234、誕生日など、推測されやすいものは避ける。

・ 車の電子回路に直接接続するような外付けのアクセサリは、製造元を確認し、インターネット等で当該機種に関するセキュリティ問題が発生していないかをチェックする。

家電の場合は、

・ 前述の自動車と同様、家電にスマートフォンと連動する機能がある場合は、スマートフォンに適切なセキュリティ対策を施す。
・ 家電に USB メモリや SD カードを挿入する場合は、当該メモリ、カードがウイルスに感染していないかをパソコン等でチェックする。
・ 家電を Wi-Fi 経由でインターネットにつなぐ場合、Wi-Fi ルーターにパスワードを設定する、通信を暗号化するなどのセキュリティ対策を行う。

などが挙げられます。

2012 年のロンドンオリンピックの時には2億件を超えるサイバー攻撃があったと報道されていますが、2020 年の東京オリンピックの際はそれを遥かに上回るサイバー攻撃が予想されています。企業も個人も、サイバーセキュリティに対してより関心を高め、対策を行っていく必要があるでしょう。

---

[1] Hackers Reveal Nasty New Car Attacks--With me Behind The Wheel. 2013/8/12 Forbes
http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

[2] Smart toilet vulnerable to Bluetooth flushing hack 2013/8/5 WIRED UK
http://www.wired.co.uk/news/archive/2013-08/05/toilet-hack-attack

[3] Proofpoint Uncovers Internet of Things (IoT) Cyberattack 2014/1/16 Proofpoint,Inc,
http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799

[4] When IoT Attacks:Hacking A Linux-Powered Rifle 2015/8 Runa A. Sandvik & Michael Auger
https://www.blackhat.com/us-15/briefings.html#when-iot-attacks-hacking-a-linux-powered-rifle

[5] TrackingPoint: a comparison between normal operation and a hacked rifle. - YouTube
https://www.youtube.com/watch?v=eq2lhEAALNI

[6] クライスラー、ハッキング対策で 140 万台リコール ソフト更新し遠隔操作防ぐ 2015/7/25 日本経済新聞
http://www.nikkei.com/article/DGXLASGM25H19_V20C15A7MM0000/

[7] Hackers Remotely Kill a Jeep on the Highway - With me in it. WIRED 2015/7/21
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[8] FCA US LLC Releases Software Update to Improve Vehicle Electronic Security and Communications System Enhancements 2015/7/16 FCA
http://media.fcanorthamerica.com/newsrelease.do;jsessionid=FF4340ED5AE68B556FD30BD3BFBD78E3?&id=16827

[9] サイバーセキュリティ戦略(閣議決定) 2015/9/4 内閣官房サイバーセキュリティセンター
http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf

[10] 一般社団法人重要生活機器連携セキュリティ協議会(Connected Consumer Device Security council:CCDS)
https://www.ccds.or.jp/index.html

[11] 一般社団法人 JASPAR(Japan Automotive Software Platform and Architecture)
https://www.jaspar.jp/guide/index.html