IoTの導入とセキュリティー対策はセットで考える

～知らぬ間にサイバー攻撃の被害者・加害者にならないために～

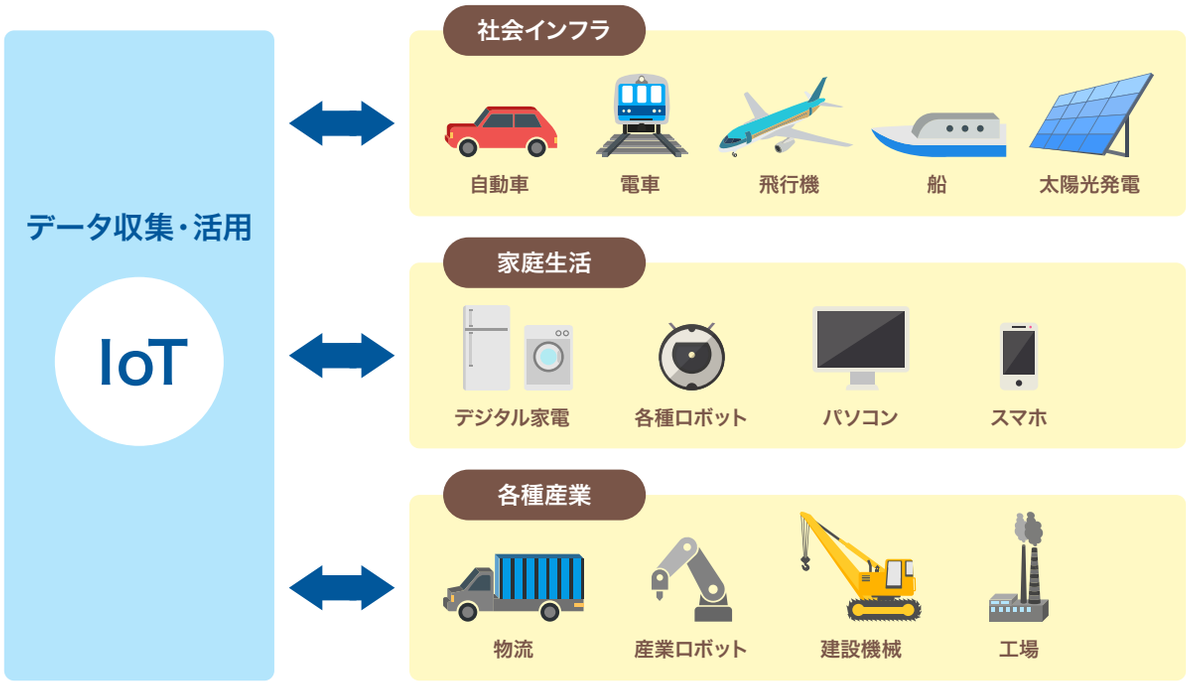
IoTデバイスの利用が増えています。しかし、CPUパワーが弱い、ストレージが少ない、パスワード（PW）が初期設定のままで使われてしまうことが多いなど正しく運用されていない、もともとセキュリティーを考慮して作られていない、といったIoTデバイスも存在し、「セキュリティー対策が置き去りにされている」という声さえ聞かれます。セキュリティー対策が十分でないIoTデバイスは、サイバー攻撃の標的になりやすいばかりでなく、攻撃を受けたときの影響が大きくなることも十分に考えられます。今後、ますます広がっていくであろうIoTを安全に活用するには、セキュリティーについてどのように考え、対策を施していけばよいのでしょうか。

家庭やビジネスを変える、急拡大するIoTとその裏側

2018年6月、「Society 5.0」、「データ駆動型社会」への変革に向けて、「未来投資戦略2018」が閣議決定されました。その中では、IoT、ビッグデータ、AI（人工知能）、ロボットなど先端テクノロジーを活用することの重要性が明記されています。

内閣府も、「Society 5.0」で実現する社会は、「IoTで全ての人とモノがつながり」、さまざまな知識や情報が共有され、今までにない新たな価値を生み出すことで、さまざまな社会的な課題や困難が克服されるとしています。IoTは、現在、そして未来の社会を実現するのに不可欠なテクノロジーです。

ある試算によれば、2020年には全世界で約260億個ものデバイスがIPネットワークに接続されるとされ、IoTは今後、ますます普及していくと考えられています。例えば、家の中のさまざまなモノにセンサーが付けば、インターネット経由で遠隔操作が可能になり、帰宅の少し前からエアコンを起動させたり、テレビ番組を録画したりできます。スマートスピーカーに家中のモノや家電がつながれば、声だけでさまざまなモノや家電を動かせるようにもなります。家中のモノをIoTで遠隔操作できるようにしたスマートホームは、今後ますます増えていくでしょう。



2020年には全世界で約260億個ものデバイスがIPネットワークに接続されるという

IoT特有のサイバー攻撃リスクとは

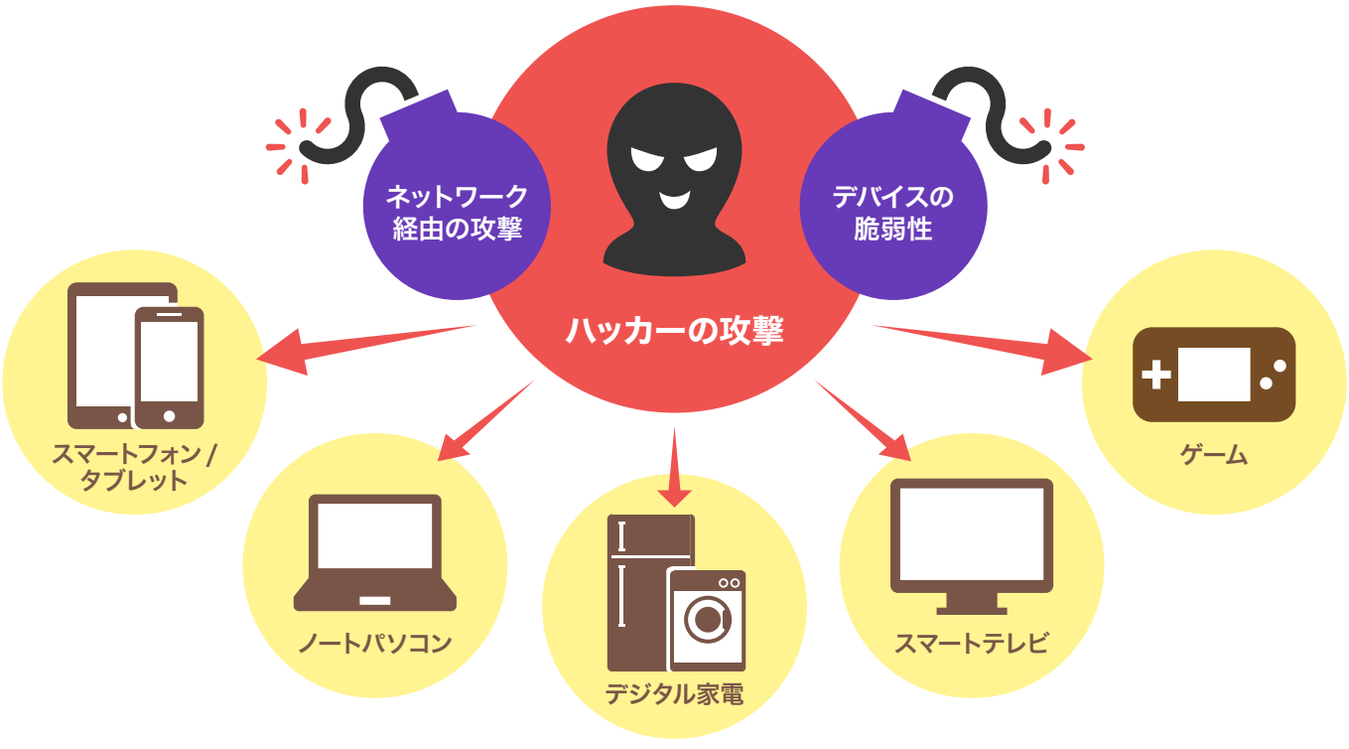
ネットワークにつながることで人々の生活や活動を便利にしてくれるIoT。離れた場所から操作できるようになるということは、ネットワークを経由して、外部からの攻撃が可能になるということでもあります。

これまで外部との通信が行われることなどなかったようなモノや家電までがネットワークにつながることで、今までは考えられなかったようなサイバー攻撃のリスクが生じます。家電や自動車、工場の設備・機器など、インターネットにつながったデバイスが、外部からコントロールされてしまうことで、例えば、工場であれば操業停止を余儀なくされるなど、甚大な被害や影響及ぼす危険性も考えられます。

また、生活に密着しているIoTデバイスは、利用者のバイタルデータなどパーソナルな情報も取得しています。そのため、サイバー攻撃によってさまざまな個人情報が盗まれてしまうリスクも考慮しなければなりません。

具体的なサイバー攻撃を考えてみると、次のようなことが指摘されています。

・外部からエアコンやネットワークカメラ（監視カメラ）などが不正に操作される
・ネットワークにつながったデバイスが外部からコントロールされ、サイバー攻撃の踏み台にされる（DDoS攻撃のボットネットに利用される）
・迷惑メール送信の踏み台にされる
・自動車が遠隔操作されて暴走する
・工場の生産ラインが止まる
・水道や電気などの社会インフラが止まる



IoTの進展に伴いサイバーリスクの拡大も指摘されている

IoTデバイスが抱えるセキュリティーの課題とは

このうち、サイバー攻撃の踏み台にされるという例では、「Mirai」や「BrickerBot」といったマルウェアによる被害が広く知られています。

Miraiは、感染したIoTデバイスを、「DDoS攻撃を実行するロボット」として、狙ったサーバーに攻撃を仕掛けるためのマシン群（ボットネット）に組み込みます。自分のIoTデバイスが、Miraiに感染したことを気がつかないでいると、知らぬ間にサイバー攻撃の加害者になってしまうこともありえます。

「BrickerBot」もMiraiと似た感染方法で拡大していきます。BrickerBotの狙いは感染したIoTデバイスを使用不能にすることとされています。

こうしたIoTデバイスを狙ったマルウェアが登場してきたことからも、利用者はIoTにおけるリスクを認識し、サイバー攻撃への対策を行っていく必要があります。

ただし、IoTデバイスでセキュリティーを強化していくには、さまざまな課題が指摘されています。IoTデバイスのように、基本的に機能が限定されているデバイスはCPUパワーが弱かったり、情報を記録するストレージの容量が少なかったりと、デバイスの単価を低く抑えることもあって、最低限の機能しか搭載されていないことが多いのです。

そのため、セキュリティー対策に関する機能が脆弱なこともあります。パソコンやタブレット端末、スマートフォンであれば、セキュリティー対策ソフトをインストールするといった対策も有効ですが、IoTデバイスでは、そうしたソフトウェアをそもそもインストールできない、できたとしてもCPUパワーが弱くて、安定的に起動させられないといった問題があります。

IoTデバイスの中には、そもそもセキュリティーを意識せずに開発された製品も少なくないのが実情です。結果として、悪意のある攻撃者にしてみれば、パソコンやスマートフォンへの攻撃で蓄積されたノウハウを流用して比較的容易にIoTデバイスへの攻撃ができてしまうのです。

また、セキュリティー対策を考えたIoTデバイスであっても、そのデバイスを管理する利用者が、定期的に基本ソフトのアップデートを実行できるかどうかも問題になります。パソコンやスマートフォンであれば、システム担当者が、従業員が使用するデバイスを管理していることもあって、OS（基本ソフト）の定期的なアップデートや、脆弱性を修正するプログラムの適用などを管理しています。

一方、IoTデバイスは種類や数が多く、屋外の遠隔地に設置されたりすることも多いため、全てのIoTデバイスを一元的に管理し、基本ソフトのアップデートなどを定期的に実行するのが難しいといったことが指摘されています。アップデートがなされずに、脆弱性が放置されたままになっていたことや、パスワードが初期設定のままで使われていた点を突かれたサイバー攻撃の事例もあります。各デバイスの初期パスワードを知るのは容易です、その為、IoT機器での初期パスワード使用を禁じる法案が成立した例もあります。

また、数年で買い替えるパソコンやスマートフォンとは異なり、IoTデバイスの中にはつながるモノや家電の利用期間と同様に長期間継続して使用するケースもあるでしょう。使用年数の長さもセキュリティーの課題になります。数の多さや使用年数の長さから、アップデートや運用の監視から漏れてしまうデバイスがでてきてしまのです。

このようにさまざまな課題があるため、利用する際にはIoTデバイスに適したセキュリティーを考えなくてはいけません。

IoTの導入とセキュリティー対策はセットで考える

IoTデバイスに有効なセキュリティー対策とは

IoTにおけるセキュリティー対策について、政府や業界による検討も進められています。2016年7月に、総務省・経済産業省などが中心になって設立した「IoT推進コンソーシアム」が「IoTセキュリティーガイドライン」を公表しました。本ガイドラインでは「方針、分析、設計、構築・接続、運用・保守」それぞれの段階でのセキュリティー指針と具体的な対策の要点を定めています。

セキュリティー対策としては、次のような具体例が考えられます。

・IoTデバイスを管理するシステムを構築する

万が一サイバー攻撃を受けてしまった場合、いかに素早く当該部分を特定して対応できるかが重要です。迅速な対処のためには、IoTのネットワークがどのようになっているのか、どういうデバイスが存在しているのかを把握（可視化）でき、異常があった場合には迅速に検知できるようなシステムを構築する必要があります。

実際、インターネットとIoTデバイスとの間にゲートウェイを設けて故障やサイバー攻撃の発生箇所を検出するネットワーク制御技術が登場しています。

・IoTデバイスの脆弱性対策を施す

IoTデバイスにおいても攻撃時には脆弱性が狙われます。すでに導入済みのIoTデバイスがある場合は十分なセキュリティーが担保できるかを検討し、必要があればアップデートを施す等の対応を行わなければなりません。そもそも導入する際に、脆弱性対策のための定期的なアップデートが行われるのかを確認しておくのも良いでしょう。IoTデバイスは稼働する数が多く、5年10年と長期的に使用する場合もあるため、すべてを把握しておくのが困難です。そこで、自動でアップデートしてくれたり、アップデートが必要なときに通知してくれたりといった、アップデートを行う上でのユーザー側の負担を減らす工夫がなされているIoTデバイスを選ぶのも良いでしょう。
いずれにせよ、既知の脆弱性が放置されることのないように、定期的なアップデートを施すことが重要です。

どうしてもデバイス側での対応が難しい場合は、ゲートウェイや仮想化による通信の監視や認証の設定、暗号化といった対策で補う必要があります。

一方、IoTデバイスのユーザ側においては、上記のようなセキュリティー対策がとられている製品やサービスなのか確認する意識も必要かもしれません。そうした一人ひとりの意識の高さが、安心・安全なIoT社会実現のためにも重要な意味をもつでしょう。
IoTデバイスへの攻撃は自社、個人だけの話にとどまらず、顧客や社会への影響も大きい問題です。セキュリティー上のリスクや課題、取りうる対策についてしっかりと検討した上で導入することが大切になります。

【制作／コンテンツブレイン】

NTTコムウェア株式会社
URL：https://www.nttcom.co.jp/
WEB掲載：2019.1