トピックス

IoT時代に求められるセキュリティ対策
―IoTセキュリティの考え方と具体的施策―

各産業がIoT（Internet of Things）の本格的なビジネス展開を検討している。しかし、IoTにおけるセキュリティ対策の重要性は理解しているものの、セキュリティを確保するための観点や具体的な施策については不明確な状況ではないか。本稿では、昨今のIoT攻撃の脅威と、技術的観点からのセキュリティ施策について紹介する。

NRIセキュアテクノロジーズ サイバーセキュリティサービス事業本部
サイバーセキュリティサービス二部 主任セキュリティコンサルタント
田篭 照博（たごもり てるひろ）
専門はアプリケーションセキュリティ、セキュアコーディングなど

IoT時代の新たなセキュリティリスク

各業界でIoTビジネスが急速に広がりつつある。一方、ビジネス展開を優先するあまりか、セキュリティ施策が不十分なままリリースした結果、脆弱性を突かれた攻撃を受ける事例も増加しつつある。IoTの世界では、エンドユーザーも含めた不特定多数が保有するIoTデバイスがインターネットに接続される事になる。この結果、個人情報漏えいといった従来のリスクに加え、IoTならではの新たなリスクが生まれることになる。

例えば、自動車のように運転（操作方法）を誤ると人命や財産に直接影響を与えるモノがインターネットにつながり、IoTデバイス化される。それが攻撃者によって侵害可能な状態になった場合、車の「運転」に対する脅威という新たなリスクが加わる事になる。ほかにも介護・育児などのために自宅や施設に取り付けられた見守りカメラやセンサーからプライバシーが侵害されるリスクも増加する。このため、従来のセキュリティ対策に加え、安全面やプライバシーを守るといった新たな観点での対策が必要となり、セキュリティが担保されている事がIoTビジネスの前提となる。このようにIoTビジネスにおいてセキュリティ対策は最重要課題といっても過言ではないだろう。

しかし、具体的にはどういった観点で対策を考え、それを解決するためにはどのような施策が必要かはまだ不明確な状況にある。以降では、IoTにおける攻撃事例とその脅威を考察した上で、現時点で想定されるいくつかの技術的施策について紹介する。

既に始まっているIoTへの攻撃

IoTの脆弱性において最も注目を集めた事例の1つに世界的セキュリティカンファレンス「Black Hat 2015」で発表された自動車関連の報告がある。「Jeep Cherokee」に搭載されていた「Uconnect」という車載システムの脆弱性を突き、遠隔から走行中の自動車のハンドルやエンジンを不正に制御するというデモが行われた。この報告は、IoTへの攻撃

により人体および財産に影響を与える可能性を示唆した極めてショッキングな発表であり、多くのセキュリティ関係者の注目を集めた。

ほかにも国内自動車メーカーの事例として2016年、電気自動車のエアコンなどを遠隔操作できる専用スマートフォンアプリに、ほかの車も操作できてしまう脆弱性がある事が海外のセキュリティ研究者により公表された。注目すべき点はインターネット経由の攻撃が可能で、研究者は豪国から英国の車に対する不正操作に成功したと公表している。本脆弱性を突いても走行制御系の操作はできず、できる事はエアコンの操作といった程度で安全面への影響は少ないが、もし走行制御も可能となった場合は、極めて危険な脆弱性となり得る。

このようにインターネット経由でIoTデバイスが不正なアクセス・攻撃を受け、安全性が脅かされるという脅威がますます増えていくことになる。

安全性に加え、プライバシー侵害の脅威も増加する。事例として、世界中の防犯カメラ映像を誰でも閲覧できるWebサイトが今年話題となった。このサイトではインターネットに接続している防犯カメラに不正にアクセスし、その映像を公開していた。防犯カメラには認証の仕組みがあり本来容易にアクセスできるものではないが、不正アクセスされたカメラはデフォルトIDとパスワードのまま運用されており、容易に不正アクセスが可能な状態であった。

カメラの類いのデバイスはプライバシー侵害に直結する分かりやすい例だが、ほかにも同様のデバイスは多いだろう。例えば、インターネット経由で操作・監視できるような自宅のLEDライトが不正アクセスされた場合、その状態を監視する事で住人の在宅や外出状態が露呈されるといった事が予測できる。

これらの脆弱性は一例ではあるが、さまざまな「モノ」がユーザーが意識しないままインターネットにつながるIoT時代において、ユーザーの安全性やプライバシーが常にリスクにさらされる危険がある事を認識する必要がある。

また、攻撃はIoTデバイスへの直接的なものにとどまらない。例えば、家庭内の電化製品を制御できるスマートホームデバイスなどはスマートフォンアプリケーション経由で遠隔操作する方法が一般的になるだろう。スマートフォンアプリは、悪意のあるWebサイトやアプリから不正な操作をされるといった脆弱性が生み出される事もあり、脆弱なアプリケーション経由で間接的に不正操作を許してしまうリスクがある。このようにIoTデバイスが接続するバックエンドのシステムだけではなく、それを操作する端末も含め「つながる」事で相互に発生する脅威も考えられる。

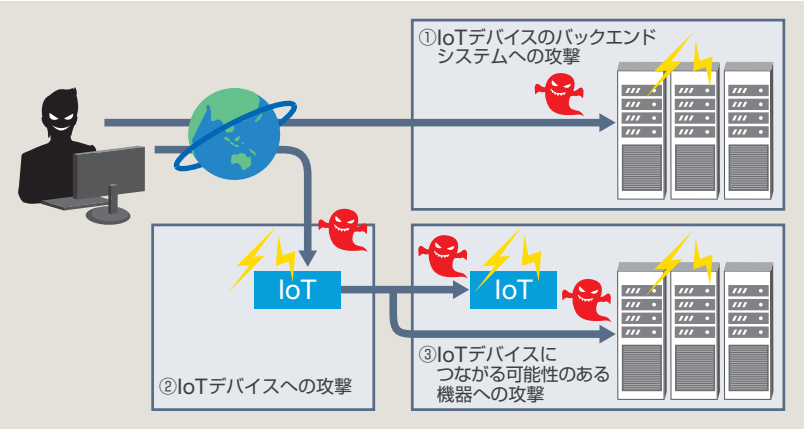
3つの攻撃対象に対する技術的観点での施策

では、どういった技術的施策が考えられるだろうか。まず、検討すべき対象を

①IoTデバイスのバックエンドシステム
②IoTデバイス
③IoTにつながる可能性のある機器

に分解して考察してみる。（次ページ図1参照）

図1　IoTシステムにおける攻撃対象



①IoTデバイスのバックエンドについてはネットワーク監視・遮断、Webアプリケーションのセキュリティ対策といった従来のシステムセキュリティの考え方がそのまま流用できる点も多い。ただし不特定多数からのアクセスを考慮すると、接続相手が想定している機器であるか否かを検証する強固なクライアント検証の仕組みが必要である。

②IoTデバイス自体への攻撃については出荷時にデバイスへファイアウォール、IPS（侵入防止システム）、ウイルス対策ソフトのような侵入防止機能を自己防衛的に搭載する事が必要だと考えられる。独自性が高いプラットフォームやプロトコルを利用する場合、既知の脆弱性を検知するシグネチャベースのものより、未知の脅威に対する対策として昨今進化が著しい「機械学習」による異常・予兆検知が有効ではないかと考える。しかし、リソースの制約上、この機能をIoTデバイス上に実装させる事は困難であるため、サーバーと相互に連携してサーバー側で機械学習を行わせるなどの工夫は必要だろう。また、出荷して終わりではなく、脆弱性発見時はオンラインでのソフトウェアアップデート機能を搭載するなど、出荷後の保守・運用スキームの構築も必要である。ただし、アップデートプログラムについては、そのプログラム自体を悪用され、不正なアップデートが行われる懸念もあり、IoTデバイス側でアップデートプログラムの署名検証をするなどの考慮も必要である。

さらに人命に影響を与えかねないような脅威が顕在化した場合は、少し大げさかもしれないがサービス提供側が能動的に発動できる緊急停止ボタンのような仕組みも必要になるかもしれない。

③については、IoTデバイスは不特定多数の機器と「つながる」可能性があるという前提でセキュリティを考慮すべきである。例えば、前述した例のようにスマートホームデバイスを操作するスマートフォンアプリケーションに脆弱性があった場合、脆弱性が修正されたバージョンからしか操作を受け付けないといった自己防衛機能を働かせる必要がある。万が一ウイルス感染した場合にも、つながっている機器に影響を与えないようにする施策も求められる。例えば、昨今話題になっている攻撃としてDDoS攻撃と呼ばれるものがある。ウイルス感染し、外部から遠隔操作可能な状態（ボット化）となった多数のコンピュータを使い、攻撃対象のサーバーに一斉に大量のパケットを送りつけてサービス不能状態に陥れるという攻撃である。これまでボット化される対象はPCやサーバーといったコンピュータであったが、IoT時代においては膨大な数となるIoTデバイスにまで対象

が広がる事が予測される。自分のデバイスが攻撃側にならないように発信する通信の宛先、量、内容が異常な場合に通信を制限するなど、ほかのデバイスとのアクセス配慮も必要となるであろう。

そうはいったもののこれら個別の対策は、デバイスのリソース制約などの理由で実施できない事もある。最近ではMVNO（仮想移動体通信事業者）であるソラコムが、IoTデバイスにかかる暗号化などの高負荷処理をクラウド上で行うサービスを提供している。このようなサービスを組み合わせる事も有効であろう。また、どの対策においても従来のIT機器と同様に階層型のセキュリティ施策を適用し、多層防御でアーキテクチャー全体としてセキュリティを向上させるという基本的な考え方は重要である。IoTデバイスでは脆弱性が発見されても容易にアップデートできない事も想定し、その観点からも多層防御は検討すべき事項である。

企画・開発段階からの施策が重要

技術的な施策とは少し異なるが、開発者のセキュリティスキルという側面にも目を向ける必要がある。IoTの普及に伴い開発者の業界大移動が予測される。この結果、これまでセキュリティとは無縁だったデバイス系の開発者や、デバイス開発経験のないWeb系の開発者などが畑違いの領域を担当する事になり、高いセキュリティが担保できないといった状況も考えられる。このため、適切なエンジニアの配置、教育に加え、企画・設計・開発工程でセキュリティ対策を考慮する「Secure By Design」という考え方も重要である。

また、米国では開発プロセスに継続的なセキュリティ検査を組み込む「DevSecOps」というアプローチに注目が集まっている。IoTデバイスの検査としては、ソースコードチェックによるセキュリティ検査、異常パケットを大量に送信し、その応答や挙動により脆弱性を検出するセキュリティ検査などが考えられるが、この検査をIoTデバイスのソースコードが更新されたタイミングで自動実行する仕組みを作り、共通ルールの下での作りこみによって属人性を極力排除するといった手法も有効だろう。

記載した施策は完全ではなく現時点で考えられる一例にすぎないが提供するサービス、業界、リスク、デバイスの特性などに合わせて取捨選択やそのほかの策を講じる必要がある。

ここまで、具体的なセキュリティ施策について述べたが、IoTビジネス展開にあたり、コストやユーザーエクスペリエンス（顧客経験価値）など、さまざまな要素とのバランスを考えてセキュリティレベルの落とし所を探っていくことが現実的であろう。そういったバランス感覚も考慮しつつ、エンドユーザーにいかに安心してIoTを利用してもらえるかがIoTビジネス成功の鍵となる。これからIoTビジネスを考えている経営者の方々には設計や実装フェーズでのセキュリティ検討ではなく、企画、開発段階からセキュリティを意識する必要がある事を提言する。これからのIoT時代、日本が世界に誇る高品質に加え、高セキュリティでもIoTビジネスをけん引していく事を楽しみにしたい。 ■