つながる世界におけるセキュリティ

SECソフトウェアグループリーダー　中尾 昌善　　SEC研究員　宮原 真次

1 はじめに

IoT（Internet of Things）時代には、自動車、家電、ウェアラブル機器、ロボットなど様々な「モノ（things）」がネットワークに接続され、新しいサービスの創出や制御の高度化が期待される。このようなIoT時代のことを、我々は別名で「つながる世界」と呼んでいる。つながる世界では、ますます利便性が高まる一方で、これまで閉じた範囲でしか通信を行っていなかった製品やシステムに、外部からもアクセス可能な通信の入り口が付加されるため、そこからセキュリティ上の攻撃が発生したり、悪影響が他のモノに波及するなどのリスクが懸念される。

そこでIPA/SECは、つながる世界のリスクに対応するために、以下のような分野横断的に活用できる「つながる世界の開発指針」を取りまとめ、2016年３月に公開した。

安全・安心なIoTを実現するために、IoT製品やシステムの開発者が開発時に考慮すべきリスクや対策を17の指針として明確化

http://www.ipa.go.jp/sec/reports/20160324.html

前述の開発指針は、セーフティやリライアビリティについても考慮したものとなっているが、本稿ではとくにセキュリティに着目して、その考え方を解説する。

2 つながる世界とは

つながる世界、あるいはIoTの捉え方はまちまちである。IPA/SECで捉えているつながる世界のイメージを、図１に示す。図の横軸は、異なる分野の製品やシステムがつながって新しいサービスを創出することを表している。例えば、屋外からスマホで屋内の家電を制御するというサービスが考えられる。一方縦軸は、実製品や実システムから得られたデータに対して、ビッグデータ解析したり、AI（人工知能）制御を用いることにより、実製品や実システムの動きにフィードバックすることを表している。CPS（Cyber Physical System）と呼ばれることもある。例えば、電車の車両にセンサを装着し、電車の運行中に線路の保全データを収集し、劣化の予兆解析を行うことで、線路の保全をタイムリーに行うことが考えられる。

このような図１の横軸と縦軸の組み合わせによって形成されるのが、つながる世界であると捉えている。

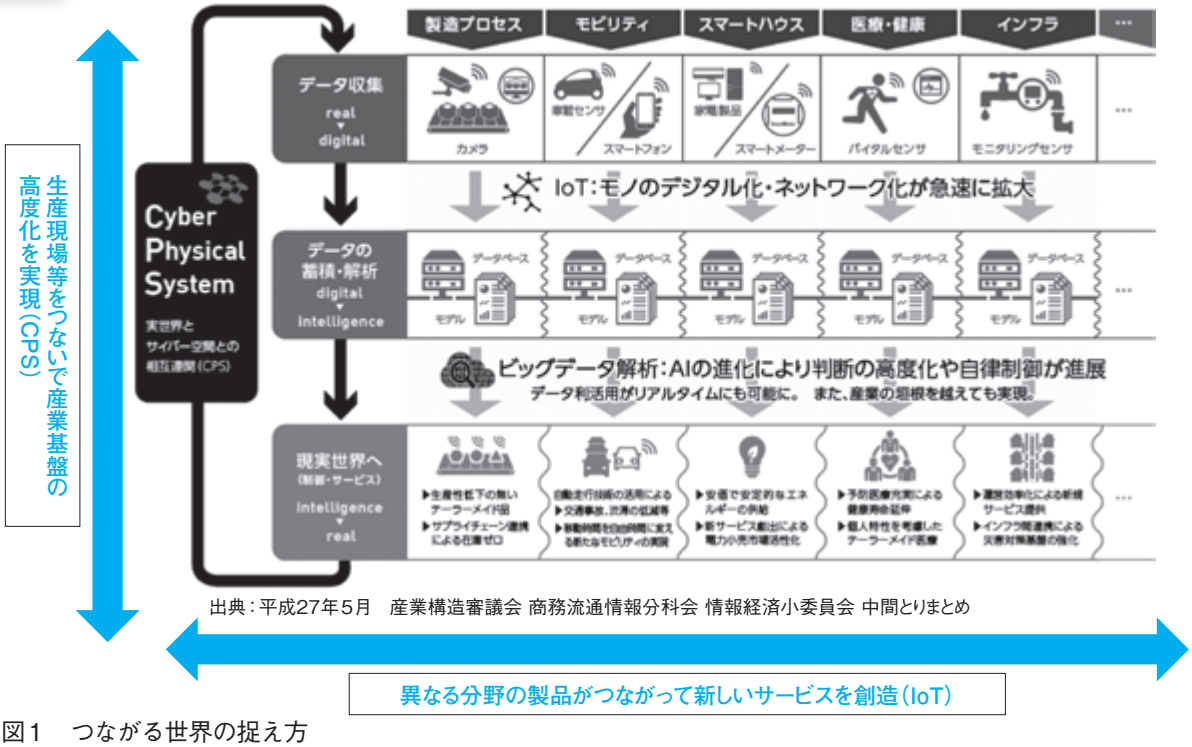

図１　つながる世界の捉え方

3 つながる世界のセキュリティリスク

3.1 つながる世界の特性

つながる世界のセキュリティリスクを考える前に、つながる世界の特性を考えてみたい。経済産業省と総務省が主導して設立した民間団体であるIoT推進コンソーシアムが、「IoTセキュリティガイドライン」※1を2016年７月に発行している。そこでは、IoTの特性は次のように整理されている。

① 脅威の影響範囲・影響度合いが大きいこと
② IoT機器のライフサイクルが長いこと
③ IoT機器に対する監視が行き届きにくいこと
④ IoT機器側とネットワーク側の環境や特性の相互理解が不十分であること
⑤ IoT機器の機能・性能が限られていること
⑥ 開発者が想定していなかった接続が行われる可能性があること

3.2 つながる世界のセキュリティリスクの特徴

つながる世界では、IoT機器やシステム同士がつながることにより、接続点から第三者に侵入され攻撃されるリスクが想定される。その対策を考える際には、次のようなつながる世界特有の課題、あるいはそこで顕著になると想定される課題を認識しておく必要がある。

(1) 想定しないつながりが発生する

IoT機器やシステムの開発者は、それがどういう場面でどのような使われ方をするかを想定し、設計条件を決める。しかし、IoT機器やシステムは、想定しない使われ方や接続が行われる可能性がある。例えば、工場、医療機関、家庭内のようなクローズドな環境でしか利用されないと想定していたIoT機器が、オープンな環境で利用されてしまうケースも出てくるであろう。更に、ユーザが興味本位でつなげてしまうケースがあるかもしれない。その結果、メーカが想定しないつながりによるリスクが高まる危険性がある。

(2) 管理されていないモノもつながる

IoT機器は、絶えずメーカや利用者の監視下にあるとは言えない。例えば、落とし物のスマホ、駐車場に放置された自動車、廃棄されたIoT機器などである。これらのIoT機器を悪意を持った第三者が手にすると、不正なソフトウェアを埋め込んだり、データを盗み出したりすることも可能である（図２）。

図２　物理的に管理されないIoT機器のイメージ

(3) 身体や財産への危害が波及する

自動車、家電、ヘルスケア製品、金融端末のようなIoT機器は、物理的な動作を伴うため、身体や財産への危害を与える危険性がある。被害が発生したとき、単体であれば範囲も限定的であるが、つながる世界では被害が波及し、より深刻な問題を招く可能性があると言っても過言ではない。

(4) 問題が発生してもユーザにはわかりにくい

故障や破損など物理的な異常は分かりやすいが、ウイルス感染や無線経由での不正アクセスなど、つながりに起因するセキュリティ上の問題は目に見えないため、利用者が気づかない可能性が高い。これは、もちろん既存のコンピュータシステムでも起こる事象であるが、IoT機器はアドレス管理などが弱いため原因を見つけにくく、より潜伏しやすいリスクとして捉える必要がある。

4 「つながる世界の開発指針」作成の背景

4.1 当初の課題認識

例えば、スマホで車を自動駐車することを考える。

図３に示すように、車は人の命を預かるレベルの厳しい設計条件で開発されており、一方スマホは通信やエンターテイメントで利用されることを想定した設計条件になっている。セキュリティの設計条件もおのずとこれに準じたものになっており、両者には違いがあるものと想定される。両者をつないだ製品やサービスを開発する際には、それぞれがつなぐ相手の設計条件を考慮した上で、対策を考える必要がある。このような課題認識のもとに、設計時に考慮すべき事項を指針としてまとめたのが「つながる世界の開発指針」である。

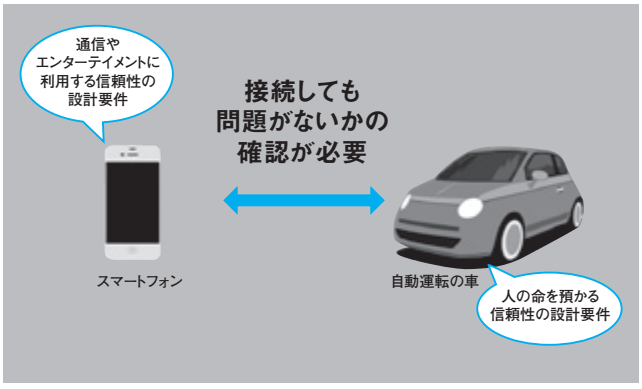

図３　異なる製品接続時の課題認識

4.2 課題認識に関する調査結果

つながる世界における課題認識を、セミナーなどの参加者にアンケート調査した結果を図４に示す。接続相手の信頼性が不明であることが、最も懸念される事項として指摘されており、上述の課題認識と一致している。

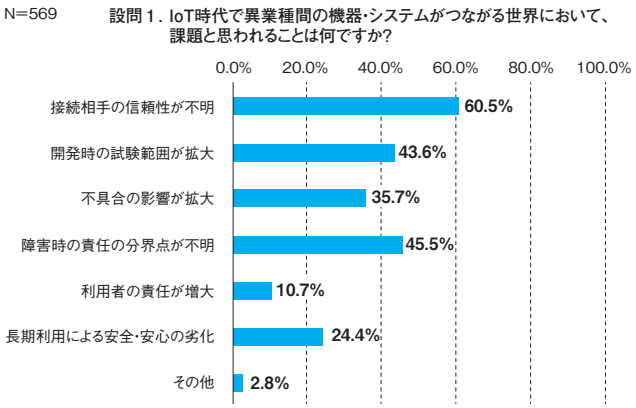

図４　IoT時代に向けての課題認識アンケート結果

5　つながる世界の開発指針

5.1　開発指針の導出方針

開発指針の策定においては、広く知見を集めるために学術研究者及び自動車、家電、住宅、ATM、産業機械など多様な産業の識者からなる「つながる世界の開発指針検討WG」を立ち上げ、WGメンバーのコンセンサスをとりながら検討を進めた。また、過去に発行した「つながる世界のソフトウェア品質ガイド」、「つながる世界のセーフティ &セキュリティ設計入門」など※2の作成において得られたセキュリティとセーフティの関係の整理などの知見も活用した。

(1)「IoTコンポーネント」に着目

IoTは、あらゆるモノがネットワークにつながり、新しい価値を生むが、新たなリスクの発生が懸念される。また、IoT同士がつながって拡大していく性質を有するため、IoTのシステム構成が刻々、変化し、リスク分析が難しいという課題がある。そこで、本開発指針では、IoTを「System of Systems（SoS）」と捉え、IoTを構成する機器やシステムのうち単独で目的や機能を果たす「IoTコンポーネント」に着目した。この「IoTコンポーネント」のリスクを想定し、対策を検討することで、IoTの安全・安心を実現することが可能と考えた。

(2) IoTコンポーネントのリスク分析

IoTコンポーネントのリスクを分析するために、IoTコンポーネントをモノ本来の機能や情報にIoT機能（通信機能など）を付加したものと仮定してモデル化し、守るべきものとリスク箇所を整理した。図５に示す。

また、IoTコンポーネントのつながりに着目し、誰がどのようにIoTコンポーネントをつなぐのかを洗い出し、つながり方のパターンを整理した。図６に示す。

IoTにおけるリスクの分析手法は、まだ、確立した手法がないため、我々は、上記の「守るべきものとリスク箇所」及び「つながり方のパターン」を横軸、IoTに関するリスク事例を縦軸としてリスク分析を行った。（詳細は本開発指針の付録Aを参照いただきたい）。

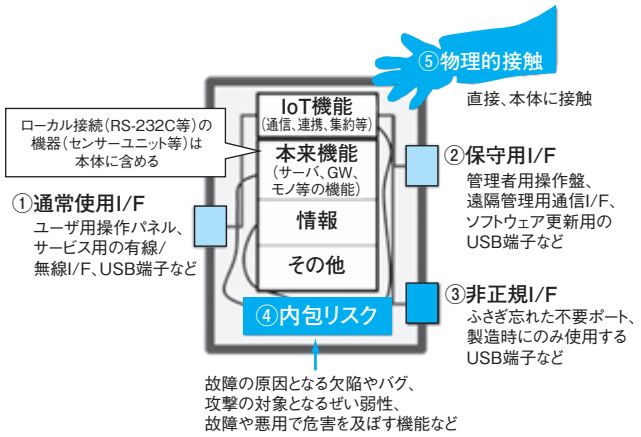

図５　IoTコンポーネントの守るべきものとリスク箇所

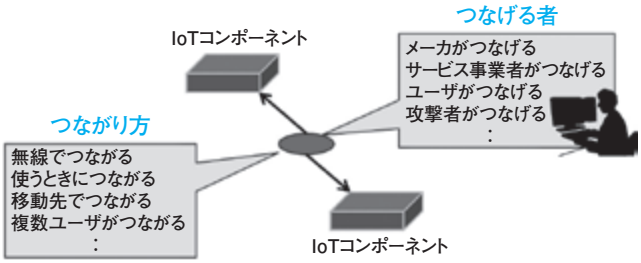

図６　IoTコンポーネントのつながりの捉え方（イメージ）

(3) 開発指針の導出

今回のリスク分析では、横軸の事項を６W1Hの視点で、誰がどのようにつないで、どこの箇所でどのような問題が発生したか。また、どの段階で発生したか、結果的にどのような被害になり、原因は何だったか、について分析した。この分析をもとに、発生要因を分類し、そこから本質的な課題を抽出し、IoT機器やシステムのライフサイクルの観点で整理することで、開発時に考慮すべき指針を導出した。

5.2　開発指針の概要

開発指針をまとめるにあたり、以下を考慮した。

- 分野横断的に活用できる抽象度の高い表現を採用
- IoTは利用期間が長いのでライフサイクルを意識
- 指針を具体的に検討するためのポイントを明示

開発指針は、表１の通り、ライフサイクルに合わせて、「方針」「分析」「設計」「保守」及び「運用」の５つのフェーズに分類し、17の指針としてまとめた。各指針は、指針／ポイント／解説／対策例により構成されている。実際の開発においては、ハードウェアの性能、開発コストなどの制約により各指針で例示した対策を実装できないケースも想定されるが、少なくとも各指針のポイントは、必ず検討していただきたいと考えている。

本開発指針は開発者を主たる対象としているが、「方針」に含まれる３つの指針はメーカ等の経営者にIoTのリスクに気づいていただくために有用である。また、「保守」「運用」に含まれる５つの指針は、開発者と保守者が連携してIoTコンポーネントの安全・安心を実現するために活用していただきたいと考えている。

表1　検討して欲しい開発指針一覧

大項目		指針
方針	つながる世界の安全安心に企業として取り組む	指針１　安全安心の基本方針を策定する
		指針２　安全安心のための体制・人材を見直す
		指針３　内部不正やミスに備える
分析	つながる世界のリスクを認識する	指針４　守るべきものを特定する
		指針５　つながることによるリスクを想定する
		指針６　つながりで波及するリスクを想定する
		指針７　物理的なリスクを認識する
設計	守るべきものを守る設計を考える	指針８　個々でも全体でも守れる設計をする
		指針９　つながる相手に迷惑をかけない設計をする
		指針10　安全安心を実現する設計の整合性をとる
		指針11　不特定の相手とつなげられても安全安心を確保できる設計をする
		指針12　安全安心を実現する設計の検証・評価を行う
保守	市場に出た後も守る設計を考える	指針13　自身がどのような状態かを把握し、記録する機能を設ける
		指針14　時間が経っても安全安心を維持する機能を設ける
運用	関係者と一緒に守る	指針15　出荷後もIoTリスクを把握し、情報発信する
		指針16　出荷後の関係事業者に守ってもらいたいことを伝える
		指針17　つながることによるリスクを一般利用者に知ってもらう

5.3　指針の例の解説

以下では特徴的な２つの指針について、その意図を説明する。

［指針５］つながることによるリスクを想定する

今までネットワークにつながっていなかった家電や生活機器などがつながるIoTの世界では、つながることによるリスクを想定することが大変重要になる。また、クローズドなネットワークでつながっていた機器やシステムが広域ネットワークにつながる場合も、想定していないことが起こる可能性があり、リスク対策が必要である。

具体例としては、2013年にプリンター複合機でパスワード未設定のまま、直接インターネットにつないだことによるデータ漏えいの危険性が指摘された。また、2016年にインターネットで閲覧可能となっている監視カメラが国内だけでも6000台あることがニュースとなった。

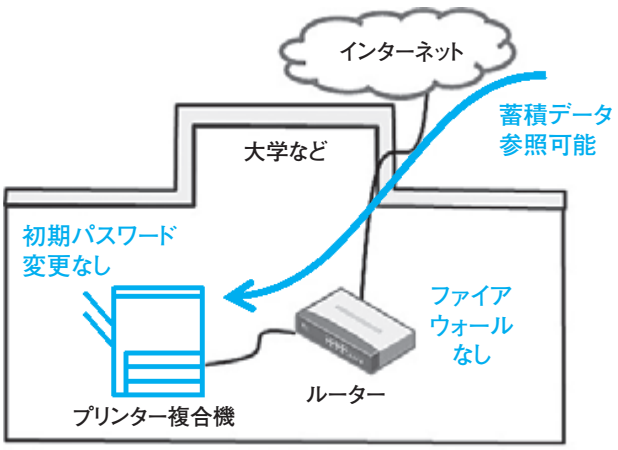

図7　インターネット接続によるリスクのイメージ

このような問題を防ぐには、利用される状況や環境などあらゆる場面におけるインターネット接続によるリスクを想定して、IoT機器・システムを開発すると共に、その危険性や対策機能について、利用者や設置事業者などに伝えることが重要となる。

［指針14］時間が経っても安全安心を維持する機能を設ける

IoTの特徴の一つに、ライフサイクルが長いことが挙げられる。10年以上にわたり利用されることを想定し、出荷後も安全・安心を維持する仕組みが求められる。とくに、製品サービスの重大な欠陥や脆弱性問題が起きたときは、速やかにかつ、長期にわたり改修するための機能が必要となる。また、屋外や人手が届かない場所に設置されるIoT機器などは、遠隔で改修できるリモートアップデートなどの仕組みが必須となる。

図8　経年で増大するリスク

一方で、このリモートアップデートの機能を具備することによるリスクの想定も必要である。アップデート実行中にIoTコンポーネントの性能が劣化することや多数のIoTコンポーネントの同時アップデートによるネットワーク帯域不足の影響など、運用を考慮する必要がある。

6　おわりに

本開発指針の内容は、IoT推進コンソーシアムが策定している「IoTセキュリティガイドライン」に採用された。現在、IoTにかかわる企業や業界団体などに対して、開発指針の普及活動を行っている。具体的には、開発現場で活用可能なチェックリストの整備や特定分野でのセキュリティガイドライン作成などの支援活動を行っている。また、今後は、開発指針の拡充や国際標準化に向けて、海外の関連団体との協調も進めていく。

脚注

※1　http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html
※2　http://www.ipa.go.jp/sec/our_activities/iot.html