「つながる世界の開発指針」の策定

SEC研究員 宮原 真次　SEC研究員 小崎 光義　SEC研究員 遠山 真
SEC研究員 西尾 桂子　SEC研究員 丸山 秀史

1 はじめに

IoT（Internet of Things）では自動車や家電、ウエアラブル機器など様々な「モノ（Things）」がネットワークに接続されるが、このような「つながる世界」においては利便性は高いものの、遠隔から攻撃されたり故障の影響が他のモノに波及したりするなどのリスクも高い。そこでIPA/SECはIoTならではのリスクに着目し、開発者向けにリスク対策に資する開発指針をとりまとめることとした。

2 つながる世界とは

2.1 System of SystemsとしてのIoT

IoTでは、迅速かつ正確にデータを収集・分析し、ビッグデータとして新しい知見を得たり、リアルタイムに機器やシステムを制御したりすることが可能となる。また、自動車や家電、ヘルスケアなど異なる分野の機器やシステムが相互に連携して新しいサービスを実現することが可能である。

IoTには、複数のシステムが連携することでより大規模なシステムとなり、かつ新たな価値を創造する「System of Systems（SoS）」の考え方が当てはまる。本開発指針の「つながる世界」も単に「モノ」同士がつながるだけではなく、単体でも価値を持つIoTが他のIoTとつながることにより、新たな価値を提供するSoSの世界をイメージしている（図１）。

一方で、異なるIoTがつながることにより、今までにないセーフティやセキュリティ上の問題が発生する可能性もあり、リスクの特定と対策が必要となる。

2.2 IoTのリスクとは

IoTにおいては、IoT同士がつながることにより、故障の影響が広範囲に波及したり、接続点から第三者に侵入されて攻撃されたりするなどのリスクが想定される。それ以外にも、以下の特徴的なリスクが挙げられる。

(1) 想定しないつながりが発生する

IoTを構成する機器やシステムは相互につながりやすく、IoTサービス事業者はもちろん、ユーザが興味本位でつなげてしまうケースもある。その結果、メーカが想定しないつながりにより不具合が発生する危険性がある。

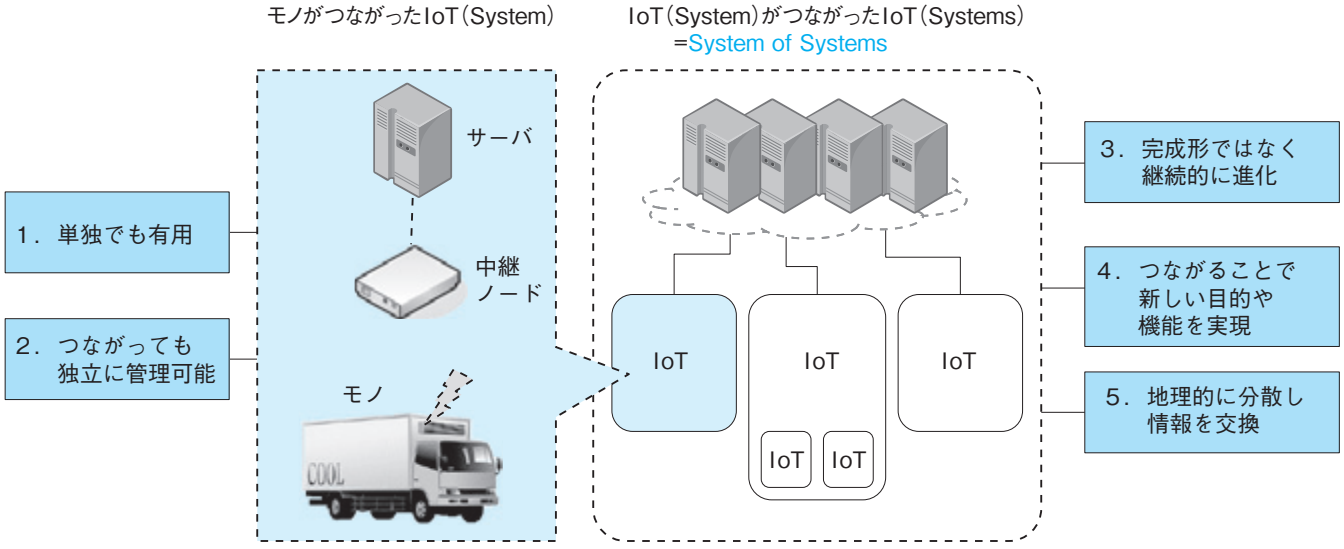

図1　System of SystemsとしてのIoT

(2) 管理されていないモノもつながる

IoTにつながる自動車や家電などは管理されていないものも多く、第三者が隙を見て不正なソフトウェアを埋め込むことも可能である。

(3) 身体や財産への危害がつながりにより波及する

生活に利用する機器は不具合によりユーザの身体や生命、財産に危害を及ぼす可能性がある。つながることで誤動作が引き起こされたり、被害が他の機器やシステムに波及したりすることが懸念される。

図2　つながりにより波及する危害

(4) 問題が発生してもユーザには分かりにくい

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問題は目に見えないため、問題が発生してもユーザが気づかない可能性が高い。

以上のように、IoTは社会全体に広がる重要なインフラであり、ユーザの身体や財産に危害を与える危険性もある。しかし、IoTは日々拡大し、変化するため、リスクの特定が難しいという問題がある。

3 欧米におけるIoT関連規格と本開発指針の位置付け

3.1 海外のIoT関連規格

IoTについては様々な団体で規格化が進められており、大まかには業界・分野に共通的な「共通・汎用規格」と特定の業界や分野に依存する「業界別・特定規格」とに分類できる。前者としてはIEEE、ISO/IEC、NIST、oneM2Mなどがあり、後者としてIndustrie 4.0やIICがある。Industrie 4.0とはドイツ政府が推進する製造業の高度化を目指すプロジェクトであり、第４次産業革命と称されている。その特徴はCyber Physical System (CPS)をベースとした製造業の高度化である。

IICは、米国企業中心に産業市場におけるIoTの推進を目指して設立された団体である。IICはエネルギー、医療、製造、運輸、行政などの領域を対象としている。IICではIoT向け規格の標準化団体に会員企業の要望を伝えることにより、相互運用性を実現し、テストベッドによる検証環境構築の推進を行っている。

Industrie 4.0はドイツの機械産業の国際市場拡大、IICは参加企業によるIoTプラットフォームビジネスの市場創生が主要な目的と想定される。

主要な関連規格の動向を表１に示す。

3.2 開発指針の位置付け

表１の「業界別・特定規格」については、前述のIndustrie 4.0やIICのように各国産業の活性化やIoTビジネス創造を狙いとしたものが多く、開発者が参考とするには具体化されていない。表１の「共通･汎用規格」についても、安全･安心に関する事項は分野共通・汎用的な内容となっており、個別の産業の開発者が参照するには実践的な内容にはなっていない。

そこでIPAでは、我が国の産業の安全・安心への取り組みの現状や各企業が抱える課題を踏まえて実用的な対策を整理する必要があると判断した。それに基づき、本開発指針では、各業界別の実際のリスク例をベースに安全・安心に関して実践的なレベルにまで踏み込みつつ、各業界で利用できるよう共通的・業界横断的なものとしてまとめることを目指した。

表１　海外におけるIoT関連規格の動向

	規格/団体	概要	主要参加メンバー等
共通・汎用規格	IEEE　P2413	IoTにおいてドメイン横断のプラットフォームを検討	－
	ISO/IEC 30141	JTC1 SWG5の後を受けてWG10でリファレンスアーキテクチャを検討	－
	NIST CPS PWG	CPSのFramework検討のためのPublic WG	－
	oneM2M	世界の主要７標準化団体の共同プロジェクト。 従来の垂直統合型M2Mサービスを共通PFで水平統合型に展開	Continua、HGI、OMA等業界団体等、約200社
代表的な業界別・特定規格	Industrie 4.0	ドイツ政府が製造業のイノベーション政策として主導	Siemens、Bosch、SAP等
	IIC	エネルギー、医療、製造、運輸、行政に焦点	GE、AT&T、IBM、Cisco、Intel等、約150社
	AllSeen Alliance	家電製品、モバイル端末向け規格	Qualcomm、LG、MS等、約50社
	OCF	家庭、企業における多様なデバイス間の相互運用のための規格	Intel、サムスン電子、Cisco、MS等
	HomeKit	iOSと機器をつなぐ規格	Apple等、約20社

4 開発指針の策定プロセス

開発指針の策定においては、学術研究者及び自動車、住宅、ATM、産業機械など多様な産業の識者から成る「つながる世界の開発指針検討WG」を立ち上げ、WGメンバのコンセンサスを取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。

その上で、以下のプロセスにて策定した。

(1)「IoTコンポーネント」に重点を置いた検討

IoTは２節で示したように異なる分野のIoT同士がつながって拡大していくため、新たなリスクの発生やリスクの影響範囲の変化によりリスク分析が難しい。そこで本開発指針では、２節で示したSoSの最小単位、すなわち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ものを「IoTコンポーネント」と呼び、IoTは「IoTコンポーネント」と「つながり（ネットワークや情報通信など）」から構成されるものと想定した。その上で、「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・安心を実現する指針を策定した。単体でも、つながっても安全・安心なIoTコンポーネントを実現できれば、日々、拡大・変化するIoTにおいても安全・安心を維持することが期待される。

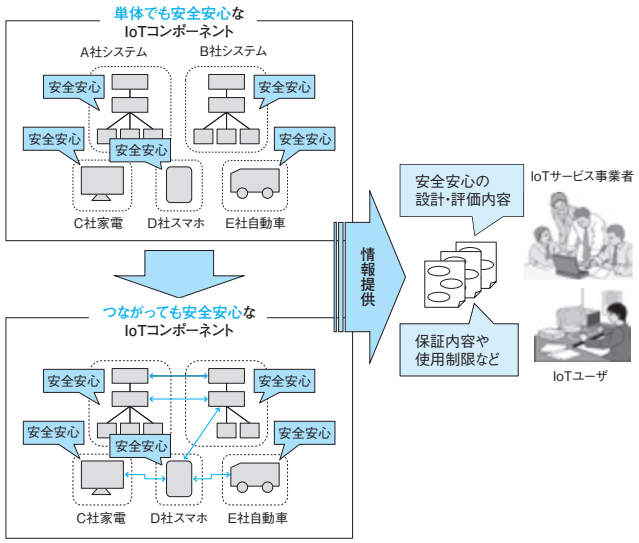

図３　単体でもつながっても安全・安心な「IoTコンポーネント」

(2)「IoTコンポーネント」のリスク分析

次に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）」を付加したモデルとして想定し、「守るべきもの」を整理した。また、IoTコンポーネントのつながり方のパターン、つなげた者、攻撃の発生個所などを整理し、これらを横軸、リスク事例を縦軸としてリスク分析表を作成した（詳細は本開発指針を参照いただきたい）。IoTのリスク事例はまだ少ないため、リスクの想定例を追加した。最後に、このリスク分析表を基に、開発指針を導出した。フローを図４に示す。

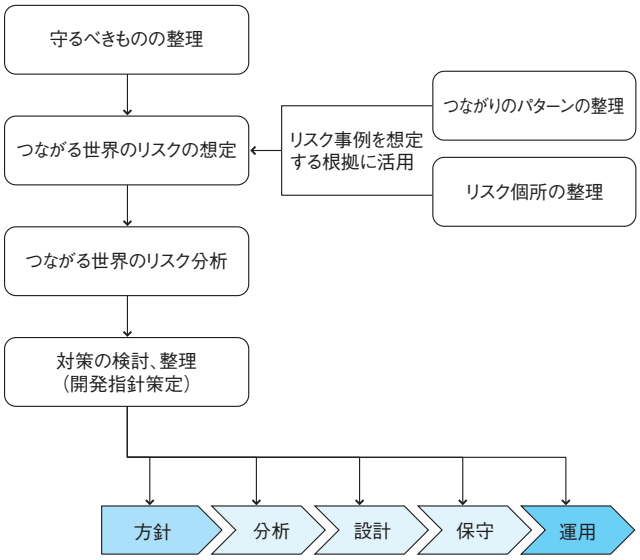

図４　開発指針の策定フロー

5 つながる世界の開発指針

(1) 開発指針の概要

図４の通り、「方針」「分析」「設計」「保守」及び「運用」のライフサイクルに合わせて17の開発指針を策定した。実情としてはハードウェアの性能、開発コストなどの制約など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着眼点での検討は必ず実施いただきたいと考えている。開発指針の一覧を表２に示す。

ライフサイクルに合わせた理由は、自動車や家電などの機器は10年以上も利用されることがあるため、廃棄の段階まで安全・安心の対策が必要なためである。

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つの指針はメーカなどの経営者にIoTのリスクに気づいていただくために有用であると考えている。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いただきたいと考えている。

表2　検討してほしい開発指針一覧

大項目	指　針	ポイント
方針	指針1　安全安心の基本方針を策定する	① 経営者は、つながる世界の安全安心の基本方針を企業として策定し、社内に周知すると共に、継続的に実現状況を把握し、見直していく。
	指針2　安全安心のための体制・人材を見直す	① つながる世界における安全安心上の問題を統合的に検討できる体制や環境を整える。 ② そのための人材（開発担当者や保守担当者など）を確保・育成する。
	指針3　内部不正やミスに備える	① つながる世界の安全安心を脅かす内部不正の潜在可能性を認識し、対策を検討する。 ② 関係者のミスを防ぐと共に、ミスがあっても安全安心を守る対策を検討する。
分析	指針4　守るべきものを特定する	① つながる世界の安全安心の観点で、守るべき本来機能や情報などを特定する。 ② つなげるための機能（IoT機能）についても、本来機能や情報の安全安心のために、守るべきものとして特定する。
	指針5　つながることによるリスクを想定する	①クローズドなネットワーク向けの機器やシステムであっても、IoTコンポーネントとして使われる前提でリスクを想定する。 ② 保守時のリスク、保守用ツールの悪用によるリスクも想定する。
	指針6　つながりで波及するリスクを想定する	①セキュリティ上の脅威や機器の故障の影響が、他の機器とつながることにより波及するリスクを想定する。 ② とくに、安全安心対策のレベルが低い機器やシステムがつながると、影響が波及するリスクが高まることを想定する。
	指針7　物理的なリスクを認識する	① 盗まれたり紛失した機器の不正操作や管理者のいない場所での物理的な攻撃に対するリスクを想定する。 ② 中古や廃棄された機器の情報などの読み出しやソフトウェアの書き換え・再販売などのリスクを想定する。
設計	指針8　個々でも全体でも守れる設計をする	① 外部インターフェース経由／内包／物理的接触によるリスクに対して個々のIoTコンポーネントで対策を検討する。 ② 個々のIoTコンポーネントで対応しきれない場合は、それらを含む上位のIoTコンポーネントで対策を検討する。
	指針9　つながる相手に迷惑をかけない設計をする	① IoTコンポーネントの異常を検知できる設計を検討する。 ② 異常を検知したときの適切な振る舞いを検討する。
	指針10　安全安心を実現する設計の整合性を取る	① 安全安心を実現するための設計を見える化する。 ② 安全安心を実現するための設計の相互の影響を確認する。
	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	① IoTコンポーネントがつながる相手やつながる状況に応じてつなぎ方を判断できる設計を検討する。
	指針12　安全安心を実現する設計の検証・評価を行う	① つながる機器やシステムは、IoTならではのリスクも考慮して安全安心の設計の検証・評価を行う。
保守	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	① 自身の状態や他機器との通信状況を把握して記録する機能を検討する。 ② 記録を不正に消去・改ざんされないようにする機能を検討する。
	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	① 経年で増大するリスクに対し、アップデートなどで安全安心を維持する機能を検討する。
運用	指針15　出荷後もIoTリスクを把握し、情報発信する	① 欠陥や脆弱性、事故やインシデントの最新情報を常に収集・分析する。 ② 必要に応じて社内や関係事業者、情報提供サイトなどへリスクの情報を発信し共有する。
	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	① 導入、運用、保守、廃棄で守ってもらいたいことを直接それらの業務にかかわっている担当者や外部の事業者に伝える。
	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	① 不用意なつなぎ方や不正な使い方をすると、自分だけでなく、他人に被害を与えたり、環境に悪影響を与えたりするリスクがあることを一般利用者に伝える。 ② 安全安心を維持していくために一般利用者に守ってもらいたいことを伝える。

(2) 指針の例

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。言葉ではイメージが掴みにくい場合にはイラストや表も活用している。以下に特徴的な２つの指針について、意図を説明する。

［指針６］つながりで波及するリスクを想定する

つながる世界では、機器やシステムに故障が発生したり、ウイルスに感染したりした場合に、つながりを通じて影響が伝播する危険性がある。そこで本指針では、このようなつながりによるリスクの想定を推奨している。

具体例としては、つながりを介して他の機器やシステムの異常やウイルスの影響を受けるケースだけでなく、自分の異常やウイルス感染により加害者となるケースも挙げている。また、安全・安心のための対策レベルが異なるIoTコンポーネントがつながることで、対策レベルが低いIoTコンポーネントが攻撃の入口になるリスクも例として挙げている。

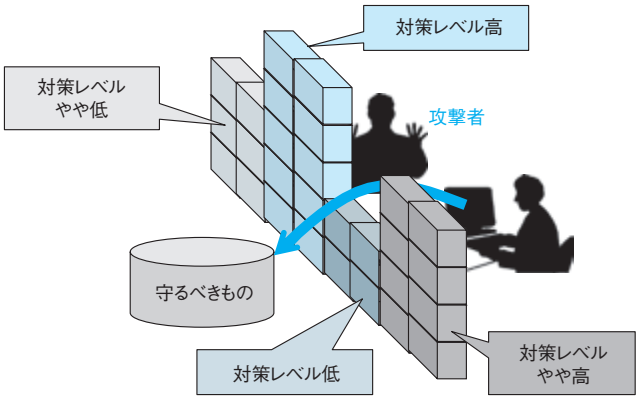

図５　弱い部分からリスクが発生するイメージ

IoTは前述の通りSystem of Systemsであるため、IoT同士が接続してより大きなIoTとなる中で、個々のIoTコンポーネントのリスクがIoT全体に波及する可能性を想定する必要がある。

［指針８］個々でも全体でも守れる設計をする

前述の指針６では、つながることによるリスクの想定を推奨しているが、本指針ではつながりをリスク対策に活用する設計を対象としている。まず、IoTコンポーネントの外部インターフェース、内包する要因、物理的接触によるリスクに対して対策を検討すると共に、IoTコンポーネントのリソース（CPUやメモリなどの能力）が不足している場合には、それらを含む上位のIoTコンポーネントで対策を検討することを推奨している。

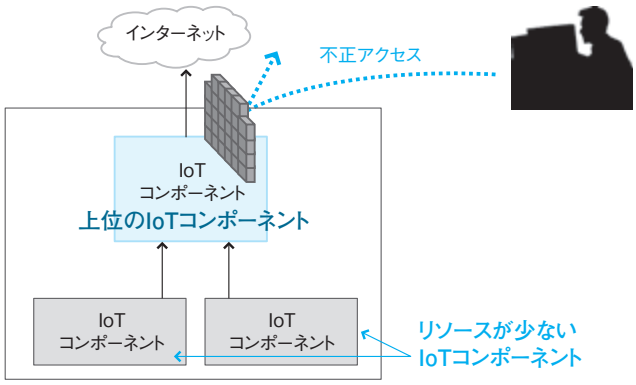

図６　上位のIoTコンポーネントで守るイメージ

更に、このIoTコンポーネントのつながりを利用して遠隔から監視し、異常検知や原因推定を行うことも例として挙げている。このようにリスクの要因となり得るつながりをリスク対策に活用することで安全・安心なつながる世界の実現が期待される。

(3) 指針の活用

開発指針については、IoTを構成する機器やシステムの安全･安心の実現に向けた検討に活用いただきたい。また、業界の実情に合わせて内容を整理することでリスク対策の実施状況のチェックリストとしても活用いただきたいと考えている。

6 おわりに

IPAは現在、多数のIoT関連の民間事業者が参画する「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」に対し、本開発指針の内容を反映させるべく提案を行っているところである。本ガイドラインは国のサイバーセキュリティ戦略で要求されているものであり、本開発指針を反映することによりIoTの安全・安心に寄与できると考えている。また、IoTに関連する各企業、業界団体、業界横断的団体に対して、開発指針の普及展開を依頼しているところである。具体的な現場での活用状況や課題を踏まえ、開発指針を適宜見直していくと共に、将来的には国際標準化や海外の関連団体との協調も視野に入れて進めていく予定である。

本開発指針は以下のWebサイトで公開しているので、積極的に活用いただきたい。

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