Internet of Things (IoT)インシデントの影響評価に関する考察

一般社団法人日本クラウドセキュリティアライアンス　IoT ワーキンググループ

第 1 . 1 版　2016 年 5 月 12 日

目次

変更履歴

2016 年 4 月 4 日　初版

2016 年 5 月 12 日　１．１版

・サービス影響要素の定義を明確化し、保守管理サービスをサービス評価対象から除外した。（保守管理サービスの影響度は機器特性やシステム規模（デバイス数）に依存するため）

・一部の図の表記を改善した。

・デバイス数評価において、連続的な評価方法をあわせて提示した。

・IoT システムのリスク評価における「影響評価」の位置づけの明確化のため記述を追加した。

概要

様々なモノをネットワーク化し、多彩なサービスを提供したり、ビジネスに利用したりするInternet of Things (IoT)の開発、導入、利用は急拡大している。一方で、サイバー攻撃の可能性など、様々な脅威の存在も指摘される中、セキュリティ対策が不十分なデバイスやシステムが侵害を受ける事例も頻発している。

こうしたシステムのセキュリティ対策は、その設計、開発段階から考慮され、適切に実装されることが必要だが、こうした考え方は、システムの開発者や企業にサイバーセキュリティに関する経験や人材が少なく、また対策コスト負担などの問題から、まだまだ浸透していないのが実情である。

この背景には、提供しようとするシステムに不具合が生じたり、サイバー攻撃が発生したりした場合に、利用者や周辺の環境、社会に対してどのような影響をもたらすかという点についての認識の欠如がある。提供するシステムに関するリスク評価が十分に行われていない点が指摘されるが、一方で、詳細なリスク評価については、手順も確立されておらず、個別の努力や今後の研究に依らざるを得ないのが現実だろう。脅威を認識しつつも、「どこまで対策をすればいいのか」という疑問を持つ開発者も多い。ただ、「リスク」の評価は立場によって異なる。システムの提供者が行うリスク評価と利用者が自信で行うリスク評価では内容も異なる上に、利用者個々の事情を事業者側が勘案することも難しい。従って、事業者が（事業者自身へのリスクとしてではなく）利用者へのリスクそのものを厳密に評価することは困難だ。しかし、一方で事業者として、提供するシステムに問題が生じた際、利用者にどのような影響があるのかを明らかにし、それに対して講じている対策を含めて利用者に知らしめることは、極めて重要な責務だろう。このことにより、利用者は、事業者の影響評価に固有の状況を反映させて、自身の「リスク」を正しく把握することができる。

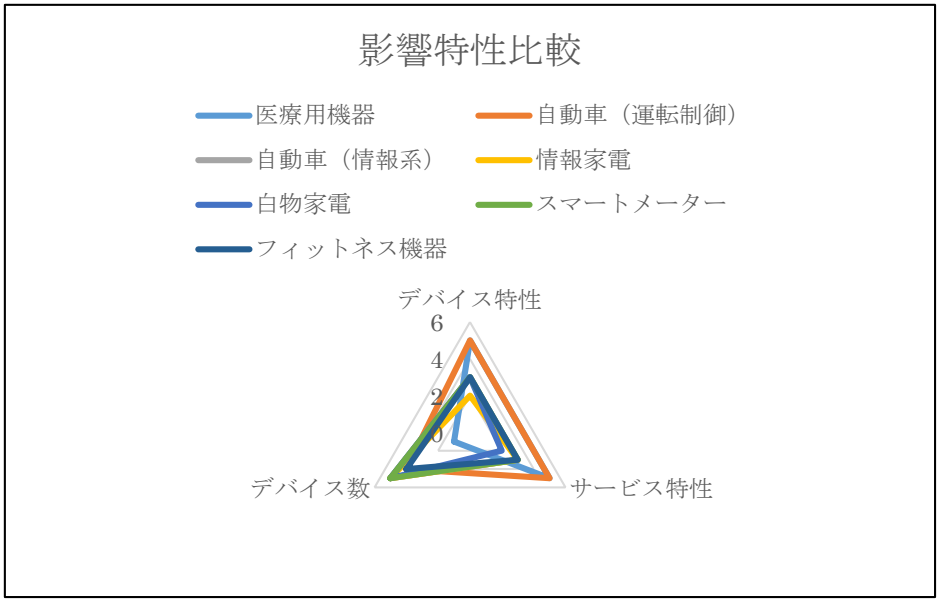
それ故、この考察では、リスク評価の一部分としての「影響評価」を考える。ここでは、なんらかのインシデントが IoT システムで発生した場合に、それが利用者や周辺環境、社会などに与える影響の大きさを考えるため、デバイスの特性、サービスの特性、システムを構成するデバイス数という３つの要素に着目している。前提とする IoT システムは、以下の図のような三階層構造（デバイスレイヤ・サービスレイヤ・BigData/サービスブローカーレイヤ）を持っている。

たとえば、航空機、自動車、医療機器、工業用機器などのデバイスは、それ自体が利用者や周辺の環境に深刻な影響を与えうる。一方、フィットネス機器や家電製品へサービスを提供するようなシステムにおいては、デバイスそのものの侵害の影響は比較的低いものの、そのサービスから個人情報の大量漏洩などの被害が懸念される。また、これらのシステムは非常に多くのデバイスから構成されることが多く、このような多数の機器において同時に問題が発生する場合、社会的な影響も懸念される。このように、それぞれの切り口で影響の大きさを検討することで、まず、どこに重点をおいて対策を考えるべきかが明らかになるだろう。

こうした検討は、システムの企画や要求定義の段階で実施することで、システムへのセキュリティや障害対策の方針を立て、それらを開発工程にあらかじめ組み入れることを可能にするだろう。さらに、細部の要件定義の段階では、より影響が大きいと考えられる部分に絞って詳細な検討を行うといった段階的な検討も可能になる。

この考察では、このような影響評価の方法について、デバイスの特性、サービスの特性、システムに接続されるデバイス数、つまりシステムの規模の３つの切り口での評価方法を提案している。

たとえば、デバイス特性、サービス特性、デバイス数のそれぞれの切り口での影響の大きさを５段階程度で評価してグラフ化すると以下のような図が得られる。



この図を見れば、それぞれのシステムにおいて、どの要素の影響が大きいかを視覚的に知ることが出来る。この図では、仮に、各システムに以下のような影響評価値を割り当てた。

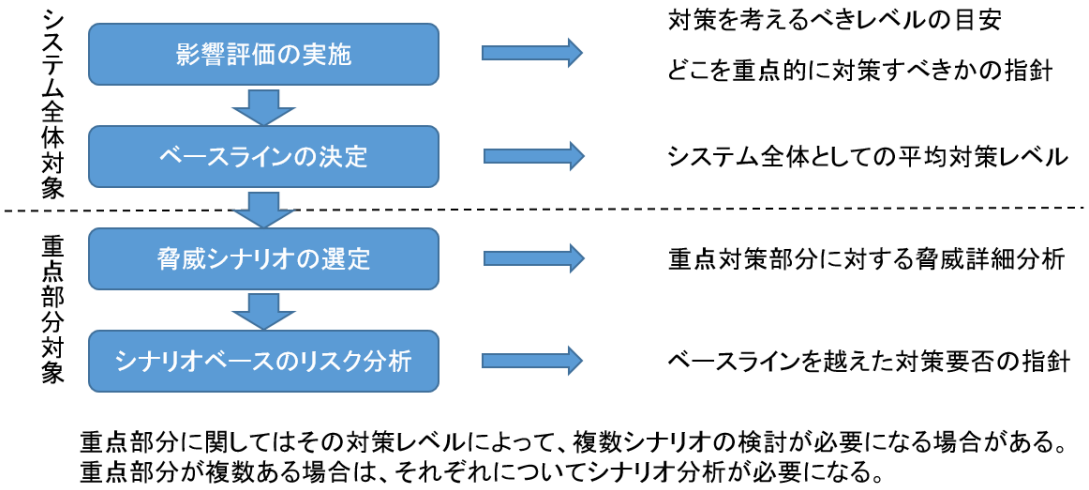
システム例	デバイス特性	サービス特性	デバイス数
医療用機器	5	5	1
自動車(運転制御)	5	5	4
自動車(情報系)	3	3	5
情報家電	2	3	5
白物家電	3	2	5
スマートメーター	3	3	5
フィットネス機器	3	3	4

ここでは、一般的なカテゴリーに対して評価値を割り当てているが、事業者は提供するシステムについて、より厳密な評価を行うことができるだろう。この考察では、こうした評価の方法についても論じている。

IoT システムを開発、提供しようとしている事業者が、こうした方法でシステムが与える影響の特徴を把握することができれば、セキュリティ対策の方向性を定める上で大きな助けになるだろう。

さらに、この考察では。システム全体の影響度スコアとして、３つの評価値を加重平均したものを計算し、システム全体としての対策ベースラインを決めるための指標とすることを

提案している。これを用いて、全体的な対策レベル（ベースライン）を決め、その上で、このスコアを上回る部分に限定して、より高度な対策を考えることで、開発におけるセキュリティ対策のプロセスを効率化することもできるだろう。



重点部分に関してはその対策レベルによって、複数シナリオの検討が必要になる場合がある。
重点部分が複数ある場合は、それぞれについてシナリオ分析が必要になる。

CSA ジャパン IoT ワーキンググループでは、今後、これを最初のステップとして、事業者側と利用者側の両面から IoT システムのリスク（影響）評価のありかたについて掘り下げ、提案していく予定である。

CSA ジャパン IoT ワーキンググループリーダー　二木真明

はじめに

Internet of Things (IoT)は、様々なデバイスをネットワーク化し、クラウド上のサービスなどと結合したシステムを構成する。（図１）こうしたシステムが内包する情報セキュリティ上のリスクは、デバイスやサービスの種類、システムの規模などにより大きく変化する。こうしたリスクを変化させる要素を明らかにし、適切なリスク評価を実施することは、IoT に関する様々な脅威に対抗するために極めて重要である。とりわけ、システムを構築し、サービスを提供する側の事業者においては、そのシステムで発生した情報セキュリティ上のインシデントが、個別の利用者や利用者全体、また社会などに、どのような影響を与えるかを評価することが極めて重要である。しかし、その影響が個々の利用者にどのようなリスクをもたらすかは、利用者固有の事情に左右されるため、事業者として厳密に評価することは困難だ。一方、事業者側での対策は、影響評価の結果をもとに決めることができる。事業者が、こうした影響評価とそれに応じて講じた対策について利用者に対して明らかにすることで、利用者は、それに自身の事情を反映させたリスク評価を行うことが可能になる。一方で、事業者は自らのビジネスに対するリスクについて、この影響評価をもとに詳しく評価することが可能だ。この考察では、まず、事業者側で、IoT システムインシデントの影響の概観を評価する方法について考え、さらにシステム開発における対策検討への反映や、より詳細なリスク分析に至る流れについて考える。

図 1　IoT システムのイメージ

1. リスク評価の方法論とこの考察の位置づけ

一般にリスク評価を行う場合、リスクを生じさせる原因について、それが生じさせる影響（主に損失や被害）と、それが現実化する可能性（確率）を考慮する。すなわち、それは被害（損失）の期待値という位置づけになる。ISO 0073:2009/JISQ 0073:2010 では、リスクは、ある目的に対する「不確実性」と定義されるが、これを受けて改定された ISO/IEC27000:2013 でも、セキュリティの目的である「ビジネス目標の達成」に対する不確実性という形で再定義された。従来、ISO/IEC27000 において、リスクは脅威の大きさと脆弱性、そして情報資産の価値の積として定義されてきたが、脅威の大きさと脆弱性は、リスクを現実化させる可能性を導くための要素として、情報資産の価値は、あるビジネス目的が損なわれることで生じうる結果（主に損失）の大きさを導く要素として再定義されることになる。IoT システム、すなわち Things（「モノ」）にあたるデバイスとそれを管理、統括するサービスや、さらにそのデバイス群によって成り立つところの付加価値サービスなどをすべて含めた全体のリスク評価を考える場合、その目的が損なわれることによって生じる結果は多岐にわたる。脅威が直接、間接に情報やシステム（情報資産）に与えた影響は、そのビジネス価値もしくは、利用者にとってのサービス価値や効果の減少、消滅に、場合によっては社会的な影響に繋がり、それが損失を生むと考えられる。一方、リスクを現実化させる可能性（確率）は、主に、IoT システムに対する情報セキュリティ上の脅威の大きさや特性に依存する。脅威にはその主体となるもの（組織、人、その他、脅威を引き起こすもの）があり、さらに、その目的や動機が存在する。脅威の強さは主体の特性と動機の強さ、目的に対して、標的とする対象がどの程度効果的かといった要素に左右されることになる。脆弱性や脅威への対抗措置となる予防的なセキュリティ対策は、こうした脅威の強さを増幅または低減する要素として働くことになる。

図 2 脅威とリスク

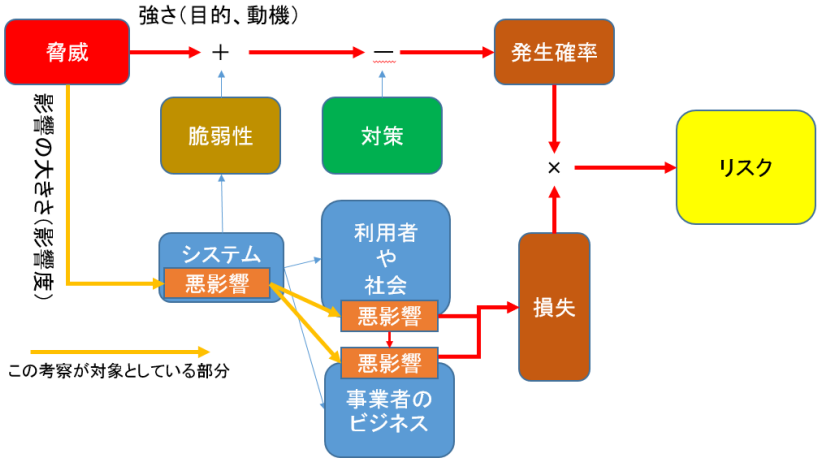


図２では、これらの関係を表している。最終的なリスク評価は、インシデントによって生じる「(悪) 影響」が、そのような「損失」をもたらすかで決まるが、利用者の損失を事業者が個々に評価することは困難である。一方で、事業者自身のリスクは事業者自身が詳しく評価できる。ここで重要となるのは、利用者がその IoT システムを利用する上でのリスクを正しく評価できるかどうかという点だ。利用者側のリスクは利用者自身が評価するにしても、システムが利用者にどのような影響を与える可能性があるのか、また、事業者側でそれに対してどのような対策がとられているのか、といった情報がなければ評価ができない。つまり、こうした影響評価や対策状況を利用者に対して明らかにすることは事業者の責務として極めて重要なのである。

この考察では、まず脅威をその主体と IoT を標的とする場合の動機や目的で分類する。これは、脅威が、IoT の何を標的とするかを考え、詳細なシナリオ分析を行う上で重要である。その後、IoT システムの特性をデバイス、サービス、規模（デバイス数）の観点から分類し、それらと脅威の目的とを対応づけて評価するための前提を明らかにすることを考える。

2. IoT への脅威

影響評価を考える前に、これらの影響（悪影響）を利用する可能性がある脅威について考えてみる。ここでは、脅威の種類やその目的などを整理し、それらがどのような切り口で、システムを悪用しようとするかを考える。

IoT にとって、最大の危機は、システム全体が停止、誤動作したり、そのシステムの制御を奪われたりするような事態である。こうした事態は、サイバー攻撃や、内部犯罪その他不正行為、不注意など、様々な原因で発生し、その結果は、システムの乗っ取り、サービスの停止や妨害、改変、情報の漏洩、改ざん、破壊など多岐にわたる。こうしたサイバー攻撃や不正行為を行う可能性がある主体は複数あるが、より影響が深刻なものを例として挙げれば以下のようなものがある。

① （過激な）ハクティビスト
② 犯罪組織
③ 産業スパイ
④ テロリスト
⑤ 国家機関または国家が支援するグループ（サイバースパイ、サイバー軍）
⑥ 悪意ある内部者

これらの脅威主体が、どのような目的を持つかによって、IoT システムに対する攻撃方法は変化する。

たとえば、目的の分類として、

A) 特定の、もしくは少数のデバイスを掌握できればよい目的
B) 一定数のデバイス群を掌握することが必要な目的
C) デバイス自体ではなく、関連するサービスへのアクセスが必要な目的
D) システム全体もしくは大部分を掌握することが必要な目的

のような分け方が可能だろう。これらについて、その例を挙げれば、

A) 特定のデバイス所有者に対して、デバイスを通じて危害を加えたい場合
B) デバイスを攻撃やスパムなど、他の行為の道具（踏み台）として悪用したい場合
C) 収集された情報やその派生情報を盗む、もしくは改ざん、破壊したい場合
D) 多くの利用者を混乱させたい（社会的混乱の発生など）場合

というようなケースが考えられる。このため、影響の評価は、目的に対して、攻撃者がどのような IoT システムの、どの部分に対して影響を与えれば最も効率がいいのかを考える必要がある。IoT システムが取り扱うデバイスやサービスの特性、規模など複数の切り口から影響評価を行うことで、脅威がどの部分を狙う可能性が高いかを知ることができる。また、こうした悪意を持った脅威に加え、開発や運用上のミス、事故などのインシデントについても、こうした影響評価によって、最も影響が大きな部分を知ることができるだろう。

このような影響評価の使い方については、後に詳しく述べるが、影響評価の結果として、脅威に狙われやすい部分を特定し、その部分に対して、可能性の高い脅威を選んで、より詳細なシナリオを作り、対策内容を決めるというような流れが考えられる。

3. 影響の大きさを決める要素

IoT をデバイスとサービスから構成されるシステムと考えれば、脅威の対象となりうる主な影響要素は以下のようなものと考えられる。

・デバイス自体の特性（用途や機能）に依存する要素

たとえば、医療機器、自動車や列車、飛行機の制御用デバイスなどは、それ自体が利用者の安全や健康、生命に大きな影響を与える可能性があるため、単独のデバイスへの攻撃が深刻な結果をもたらす可能性が高い。また、機器単独でも利用者に関する機微な情報が得られる可能性もある。

・デバイスの数に依存する要素

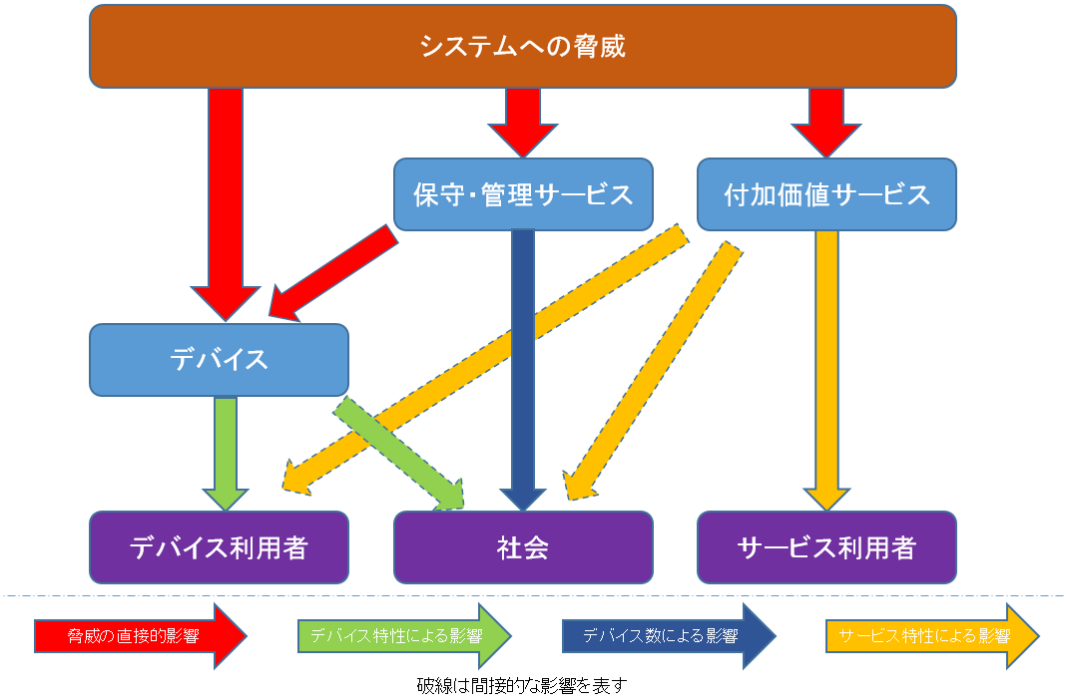
たとえば、ネットワーク家電、コンシューマ向けの IoT 機器の場合、デバイス数は非常に大きくなる。こうした多数のデバイス全体に影響するような攻撃は、社会的に大きな影響をもたらす可能性がある。たとえば、偽情報を拡散することによる社会混乱の発生といった目的で利用される可能性がある。

・サービスの特性に依存する要素

デバイスを統括するサービスには、デバイスから収集した様々な情報が集積する。さらには、集積された情報から派生する様々な情報も存在する。さらに、こうした情報がデバイスにフィードバックされるケースもあり、こうした情報に対する侵害が大きな影響をもたらす可能性がある。サービスには、多くのデバイスを集中制御したり、更新したりする機能を持つ保守管理サービスと情報を活用して付加価値を生む付加価値サービスの両方が考えられるが、保守・管理サービスの影響度は、機器特性とシステム規模の両方に依存するため、これらに含め、ここでは、付加価値サービス（もしくはデータ処理サービス）を対象とする。

IoT システムにおけるインシデントの影響評価では、少なくとも、これらの要素を考慮する必要があるだろう。この３つの要素（影響要素）は、１．で述べた脅威の主体が抱く「目的」と密接にかかわっている。詳細なリスク分析においては、影響度と目的の関連性から、どの要素に主眼を置いて評価するかを考える必要がある。図３に、脅威が機器やサービスを経由して利用者や社会に影響をもたらす経路を示した。脅威がシステムの各部に影響した場合に、どのような経路でその影響が波及するかを示している。その経路において、前述した 3 つの要素が、その影響を評価する上で重要となる。この図を逆にたどれば、脅威がその目的を達成するために最も効率が良い経路が明らかになる。つまり、その経路への対策が最も優先度が高いことになる。

図 3　脅威の影響経路



この図では、実線の矢印が直接的な影響、破線の矢印が間接的な影響を示している。デバイスやサービスから、デバイス利用者やサービス利用者、社会に向かう影響の矢印は、それがどの影響要素によるものかで色分けしてある。

たとえば、脅威がデバイス利用者を標的にしたものであれば、デバイスを直接狙うか、保守・管理サービスを狙うのが効率的だろう。また、それを考えれば、利用者が深刻なダメージを受けるようなデバイスでは、デバイス自体に加え、保守、管理サービスへの対策も重要となることがわかる。一方、社会に対して大きな影響を与えるためには、デバイス数の影響を最大限に利用できる、保守。管理サービスが第一目標になると考えられる。

4. 各要素の評価

個々のシステムについてのリスク評価を行う前に、IoT システム特性を加味した影響評価を行って、ベースラインを決めておくことが出来るだろう。こうしたベースラインは、個々のシステムのリスク評価を行うための基礎的なデータとして利用することができる。

情報セキュリティにおけるリスク評価は、相対的な大きさの評価にとどまることが多い。従って、この考察では、厳密な影響の数値化は将来的な課題として、まず、その性質と相対的な大きさを評価することを主眼におく。そのため、各要素は 5 段階程度のレベル分けされた評価尺度を使用して行うことを前提とした。

各要素の評価は、デバイス特性、サービス特性の面からは、侵害が発生した際の影響の大きさを結果の重大さや影響範囲の広さで評価し、デバイス数については、その規模を評価する。たとえば、以下のようなクラス分けを行うとよいだろう。

デバイス特性としての影響度評価では単体デバイスの機能侵害を前提に表 1 のような評価が考えられる。

表 1　デバイス特性の評価

レベル	尺度
1	ほとんど影響なし （利用者、システムに対してほとんど問題を生じない）
2	軽微な影響 （利用者に不便が生じるが、比較的容易に代替手段を利用できる。システム全体への影響は軽微）
3	事前対処が必要な影響 （利用者が非常に気にするもしくは困る状況で、代替手段が非常に限られる。利用者の情報への侵害。またはシステム運用に一部支障が生じるなど）
4	大きな影響 （利用者に直接的被害、損害、傷害などを発生または、間接的にそうした被害に結びつく機微な情報の侵害など。またはシステムを介して全体もしくは他に同様の悪影響を与えるなど）

5	重大もしくは破壊的影響 （直接、間接に利用者の甚大な被害、生命、健康に対する重大な影響を生じる。社会に対して大きな混乱をもたらすなど。またはシステム全体の機能が損なわれたり、重大な副作用が生じたりするなど）

というような尺度を用いる。

サービス特性としては、サービス自体の機能や取り扱う情報などへの侵害により、集積した情報等への影響が生じることを前提に

表 2　サービス特性の評価

レベル	尺度
1	ほとんど影響なし （デバイスや利用者、サービス情報への影響はほとんどない）
2	軽微な影響 （サービスを原因とするデバイスへの深刻でない影響、サービスが有する重要度が低い情報への侵害。また、サービスから提供する情報が失われる、もしくは誤った情報を提供することで、利用者に比較的軽微な影響がある）
3	事前対処が必要な影響 (サービスを原因とするデバイス機能障害の発生や個別デバイスの誤動作の可能性、サービスが有する非公開情報（一般個人情報、サービスに関する構成情報など）への侵害。サービスから提供する情報が失われたり誤った情報を提供することで、利用者に無視できない影響を生じる)
4	大きな影響 （サービスが原因で多くの機器が悪影響を受ける可能性、サービスが有する機微な情報（個人の機微情報、その他秘密情報）への侵害、サービスが外部に提供する重要情報の改ざん。サービスから提供する情報が失われたり、誤った情報を提供することで、多数の利用者に大きな影響を与え、場合によっては社会的な影響も懸念される）

5	重大もしくは破壊的影響 （高度な秘密情報への侵害が発生する可能性が高い。誤った、もしくは意図的な情報により広範囲の利用者もしくは社会的な混乱をもたらす可能性が高い。生命や公共の安全に関わる判断、処理を誤らせる可能性が高いなど）

のような尺度を用いる。

デバイス数については、デバイス数のオーダー（桁数）でクラス分けすることが考えられ、たとえば以下のような尺度を用いることができる。

表 3　デバイス数の評価

レベル	尺度
1	100 デバイス未満
2	1000 デバイス未満
3	10000 デバイス未満
4	100000 デバイス未満
5	100000 デバイス以上

それぞれの尺度は、評価対象によって、さらに検討が必要だが、いずれも、レベルの数値に対して影響度は指数関数的に増加する。（レベル値は対数的なスケールであると考えられる）こうしたレベル設定では各レベルの境界付近で、大きな違いが生じる。それが気になるようであれば、以下のような連続的な評価式を使ってもいいだろう。

$$\mathrm{L} = \log_{10} N \quad （\mathrm{N} \text{ は機器数}）$$

L を整数値としたければ、小数点以下を適切な基準で丸めてもよい。

5. 影響度スコアの算出と特性の可視化

こうした要素を反映させた影響度スコアを求める最も簡単な方法は、特性要素の評価値の積をとることだが、実際、レベル値が対数的スケールであることを考慮すれば、

影響度スコアを I、デバイス特性値を Ld、サービス特性値を Ls、デバイス数レベルを Ln として、

$$I = a \times Ld + b \times Ls + c \times Ln$$

で表される。（各指標は対数的なスケールなので、積の計算は加算に置き換わる）なお、a, b, c はそれぞれの要素の重み付けである。I を 5 段階の範囲に正規化するならば、

$$i = \frac{I}{a + b + c}$$

この場合の i は１～５の範囲に正規化される。仮に、いくつかのシステムで各要素の指標値を決め、計算結果がどのようになるかを見てみる。（表４）

表 4　システム種類ごとの評価例

システム例	デバイス特性	サービス特性	デバイス数	I	i
医療用機器	5	5	1	26	4.3
自動車（運転制御）	5	5	4	29	4.8
自動車（情報系）	3	3	5	20	3.3
情報家電	2	3	5	17	2.8
白物家電	3	2	5	18	3.0
スマートメーター	3	3	5	20	3.3
フィットネス機器	3	3	4	19	3.2

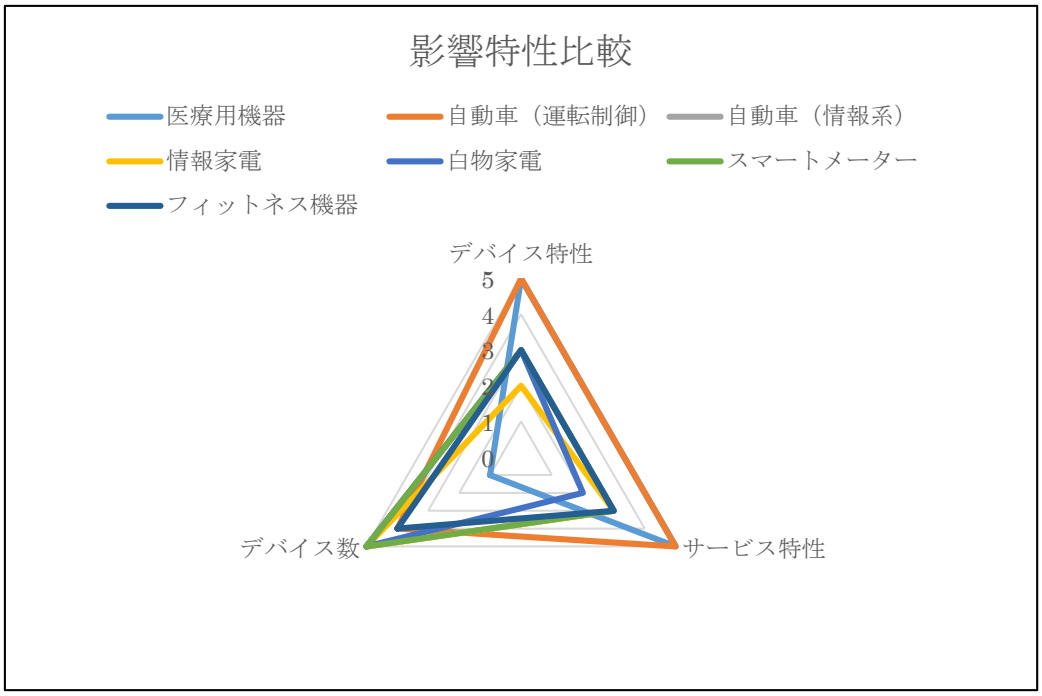
但し　以下の条件で計算した場合の数値。

a	b	c
3	2	1

ここで、各システムの評価値は仮に決めたもので、実際の適用時には、より細部を評価した上で決める必要がある。また、各数値の傾向を図にしてみると、そのシステムの特性が

よくわかる。係数 a, b, c の選択は脅威の目的、手段などの性質や、デバイスやサービスの特性によって異なる可能性がある。この計算式の目的は、異なる種類の脅威による影響の相対的な大きさを尺度を揃えた形で評価をできるようにする事である。一方、特性要素ごとの影響度分布は、その特性を狙った脅威に対してシステムがどの程度敏感かという特性（影響特性）を表すために用いる。

図 4　影響特性のレーダーチャート



こうした評価により、評価値からは、必要な対策の大きさ（強度）に対する目安が得られ、影響特性からは、対策によってどの影響要素を低減すべきかという点が見えてくる。これにより厳密なリスク評価を行わなくても、対策の方向性や優先度をある程度明らかにすることができる。

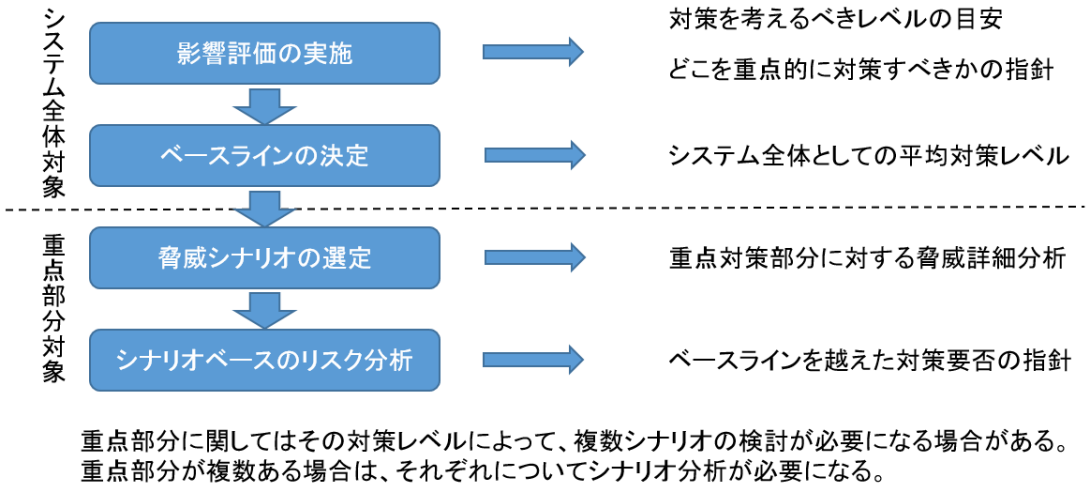
6. 影響評価の利用法

ここまでに述べた影響評価をシステム提供者が実施し、それをもとにどのようなステップでセキュリティ対策を考えていくかについて、以下にひとつの形を提案する。

影響評価によって得られる影響度スコアは、セキュリティ対策のレベル（実装強度）と相関する。一方で、影響要素ごとのスコアは、その影響要素に関わるシステムの各部分、たとえばデバイスや、その制御を統括する管理サービス、データを利用する付加価値的なサ

ービスのそれぞれについて、どこを重点的に対策すべきかと、そのレベル感を示唆する指標となる。したがって、この評価のみでも、ある程度の対策の方向性や優先順位を決めることが可能だろう。システム開発の初期段階では、こうしたおおまかな評価に基づいて、セキュリティ対策方針を定め、より脅威の高いと思われる切り口について、詳細なシナリオベースのリスク分析を実施するというステップが現実的かもしれない。

図 5　リスク分析と対策検討のステップ



比較的、影響の小さい（たとえば影響要素の評価値がすべて 3 以下など）場合は、影響評価のみでリスク評価に代える判断もあるだろう。一方、評価値が 4 を越える影響要素については、ベースラインを上回る対策の必要性を検討すべきであり、5 に至っては詳細なリスク分析が必要だろうと考える。

各影響要素とシステムとの対応では、図 3 を参考に、デバイス特性の影響が大きな場合は、デバイスへの対策を最重点に、管理サービスがデバイスに直接影響する可能性を併せて評価する。サービス特性の影響が大きな場合は、付加価値（データ処理・分析関連など）サービス部分を最重点に、管理サービスが間接的に影響する可能性を考慮する。デバイス数の影響が大きい場合は、管理サービスを最重点に、デバイスが相互に影響を与える可能性などを考慮することが必要となる。

一方、利用者は、事業者側の評価により、インシデントがどのような影響をもたらすかを把握できる。たとえば、その影響が具体的に、自分たちの何に被害をもたらす可能性があるのかを特定できれば、この影響評価を自らのリスク評価に活かすことができるだろう。

7. 結論

IoT システムのリスク評価には、この考察で挙げたような影響要素を少なくとも検討する必要がある。従来のシステムリスク評価同様に、個々のシステムへの適用は、より詳細な分析と、慎重なパラメータの選択が必要だが、この考察で挙げた方法を大きな枠組みとして使用することで、比較的単純な方法で、一般的な影響の大きさや特性を知ることができる。影響評価は、とりわけ、機器やサービスを提供する事業者にとって、製品やサービスのリスクを考えるための最初の一歩となるだろう。IoT の導入、応用が加速している現在、システム開発、運用におけるセキュリティ対策を考える前提として、こうした議論を深めていくことは極めて重要であると考える。

執筆者

二木　真明

レビュアー

一般社団法人日本クラウドセキュリティアライアンス　IoT ワーキンググループ

新宮　貢
斎藤　知明
山下　亮一
鶴田　浩司
上村　竜也
諸角　昌宏
（順不同）

第 1 版　　2016 年 4 月 4 日
改訂（1.1 版）　2016 年 5 月 12 日