JEITA

IS－16－技標－３

平成27年度情報セキュリティ調査報告書

－IoT時代のデータ利活用と情報セキュリティ対策に関する調査－

平成２８年３月

一般社団法人　電子情報技術産業協会
情報セキュリティ調査専門委員会

はじめに

情報機器の小型化やモバイルネットワークの高速化など、近年の情報処理インフラの急激な変化に伴い、これまでは技術面やコスト面から実現できなかったサービスが次々に実現し始めている。「モノのインターネット」と言われる IoT（Internet of Things）は、様々な機器をネットワーク化し、機器からデータを集めることによって、これまで実現できなかった新しいサービスを創造して提供していこうとする動きである。

IoT をめぐる標準化動向としては、様々なメーカーが製造する様々な機器を接続する必要性から、システムの構成や通信プロトコル、プラットフォームなど各レイヤーで標準化が始まってはいるものの、まだ、関連業界のコンセンサスが得られたとは言えない状況である。特にセキュリティ面では接続機器の認証、通信路の暗号化、収集されたデータの取り扱いなど、注意が必要な事柄が数多くあるが、これまでインターネットに接続しないことを前提として利用されていた既存の機器も多く、慎重な取り組みが必要である。

一方で一部の企業は自社内に閉じた環境で自社での活用を想定したデータ収集を開始したり、IoT に利用できる独自のプラットフォームの提供を開始するなど、活用事例が出始めている状況にある。しかし、収集したデータの所有権の問題や、機密保持の観点、データの分析手法が未確立といった理由から、収集したデータを元に他社にデータやサービスの提供を開始した事例はまだ少ないとみられる。

今年度、情報セキュリティ調査専門委員会においては、これから IoT を応用したシステムを構築・運用・利用したいと考えている組織が参考とするべく、IoT に関わる制度や標準化動向の調査、IoT データの取り扱いに関する消費者や企業の意識調査と、既に IoT データの利活用を行っている企業の事例収集を行った。併せて、IoT を利用する際に注意すべき脅威とリスクを検討した。また、セキュリティ対策の動向についての調査を行った。

今年度の調査・分析にあたり、ヒアリングにご協力いただいた企業・有識者の方々、そして本委員会の関係者の皆様に、深く感謝の意を表すと共に、本報告書が関係の方々に活用され、今後のビジネス拡大の一助となれば幸いである。

平成 28 年 3 月

情報セキュリティ調査専門委員会
委員長　坂上　勉

情報セキュリティ調査専門委員会名簿

（敬称略・順不同）

委員長	坂上　勉	三菱電機（株）
副委員長	福島孝文	東芝テック（株）
委員	水島九十九	日本電気（株）
〃	對馬孝高	（株）日立製作所
〃	池田政弘	富士ゼロックス（株）
〃	増田佳弘	富士ゼロックス（株）
〃	白石節男	富士通（株）
〃	池田恵一	富士通（株）
〃	平木博史	（株）リコー
〃	佐藤　淳	（株）リコー
オブザーバ	川口修司	（株）三菱総合研究所
〃	阪口瀬理奈	（株）三菱総合研究所
事務局	稲垣　宏	（一社）電子情報技術産業協会
〃	内田光則	（一社）電子情報技術産業協会

目　次

第1章　社会環境の変化

近年、モノとインターネットとの融合により新たな付加価値を創造する IoT（Internet of Things：モノのインターネット）への注目が高まっている。これは従来の機械同士がネットワークでつながる M2M（Machine to Machine）が拡大し発展したものである。IoT を利用することで、取り扱うデータが広範囲になり、分析可能なデータ量やその種類が飛躍的に増大することが期待されている。

米国や欧州を中心に様々な産業や企業において、IoT を成長戦略の中心に掲げた取り組みが進められている。ドイツ政府は製造業のイノベーション政策として『インダストリー4.0：第 4 次産業革命』を主導している。工場を中心にインターネットを通じてあらゆるモノやサービスを連携させ、新しい価値やビジネスモデルの創出を目指すものである。日本でも、「『日本再興戦略』改訂 2015－未来への投資・生産性革命－」が閣議決定され、IoT の活用が重要な施策として掲げられた。

様々なモノや製品が相互に接続するような「IoT 時代」＝「つながる世界」が到来し、新たな製品やサービスが創出され、利便性が向上することが見込まれている。このような IoT を取り巻く社会環境変化における顕著なトピックを、以下に概観する。

1.1 IoT への期待

企業は、新たな価値を創造する IoT を活用したビジネスの創出や、我々の生活に役立つソリューションの実現に積極的に取り組んでいる。このような新たなテクノロジーが登場し普及することは、企業の競争環境や産業構造の変革にとどまらず、個人のライフスタイルをも含めた社会全体に大きなインパクトを与えることになる。

インターネットに接続される端末は年々増えており、従来のパソコンやサーバに加え、スマートフォンやタブレットなどのモバイル端末がインターネットデバイスとして広く普及してきている。また、液晶テレビやデジタルビデオレコーダー、デジタルカメラなどネットワーク接続用のインターフェースを持つ情報家電も続々と登場している。これらによりコミュニケーションを円滑にし、必要な情報をリアルタイムに取得し、収集されたデータを分析することにより、今までにないサービスが提供され始めている。

また、ビッグデータ分析が本格化し、ロボットや人工知能が高度化するなど、テクノロジーは加速度的に進化し注目すべき取り組みも次々と登場してきている。医療分野では、インターネットに接続できる医療機器や着用型の生体モニタによる 24 時間モニタリングや、ヘルスケア分野でのバイタルデータ活用による健康管理や生活習慣改善などが可能になる。気象予報についても、今よりも小型で安価な気象センサーが多数設置されることにより、より詳細な観測に基づいた精度の高い予報が可能となると考えられている。

IoT の用途は多様化が進むことにより、離れた場所にあるモノの状態を検知しデータ分

析することで、インターネット経由の遠隔操作による新たなサービスや価値提供が生み出されることになる。インフラの点検業務や高齢者等の見守りサービスなどに IoT を活用したサービスも増えてきている。国内における社会インフラの老朽化や少子高齢化が進む中、そうした社会問題を効率的に解決することが広く求められている。また、将来的には、自動車の自動運転や人工知能を活用したロボティクスなど、これまでにない用途や目的での IoT の利活用が期待されている。

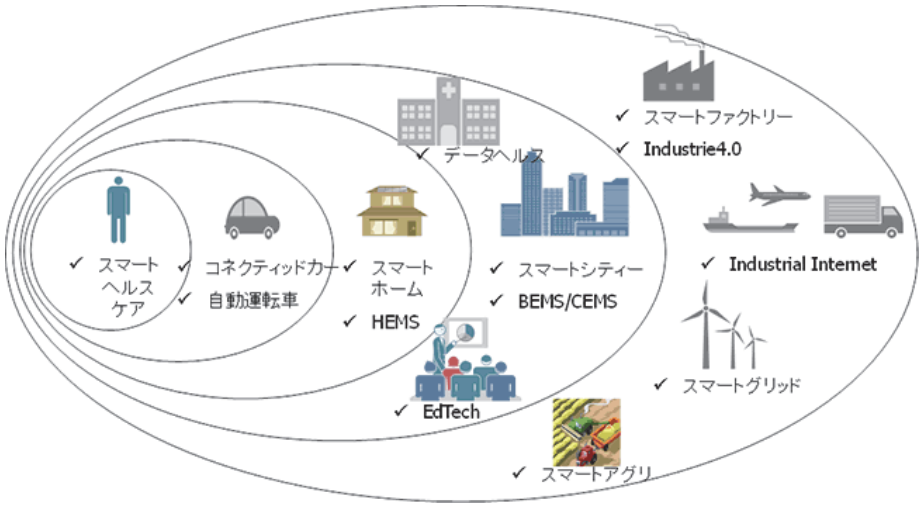

図 1.1-1 社会変革が期待される IoT の活躍分野[1]

1.2 IoT 時代に想定される脅威とセキュリティ対応

IoT がビジネスや生活に様々な価値を生み出す可能性がある一方、対象となるデバイスには多くのセキュリティ問題が発生すると懸念されている。IoT が様々な社会インフラを支えることになり、ますます IoT デバイスや IoT サービスへの脅威が直接的に人命の危機に結びつく恐れがあると考えられている。

Windows や Linux などの従来タイプの OS がよりセキュアになるにつれ、マルウェアやウィルスがシステムに悪影響を与えることが難しくなり、これらの脆弱性を突いた攻撃は減るものと予測されている。逆に IoT が進展することにより、膨大な数の組み込み OS が稼働することになると、これらが新たなターゲットとなりハッカーの目を引くことになるのである。今後は攻撃の対象はスマートフォンなどのモバイル端末や IoT デバイスになっていくと考えられる。コンピュータの乗っ取りを企むハッカーは、悪意あるコードをできるだけ長期間デバイスに常駐させようと考える。しかしながら、ほとんどの IoT デバイス（パソコン、スマートフォン、タブレット、ゲーム機器、家電製品、医療機器、センサー類など）にはローカルストレージがなくリソースもわずかであるため、コードを送り

[1] MRI コラム・レポート「 IoT が拓く未来社会」
http://www.mri.co.jp/opinion/column/trend/trend_20151210.html

込んでファームウェアを書き換える方法が使われると考えられる。今後、ベンダー側はそれらのセキュリティ対策を強化することが重要になる。

また、製品が市場に出てからソフトウェアの脆弱性が発見されることも多く、その脅威をゼロにすることは不可能である。特にセキュリティ対策が難しい原因としては、デバイスが小型であるゆえに技術的な問題や、デバイス数の多さにより人手でのメンテナンスが困難で、社会インフラ自体も老朽化してきていることなどが挙げられる。

今後はIoTデバイス等へのサイバー攻撃により、社会インフラ基盤がダウンしたり、交通事故が引き起こされたり、患者の容態変化が見落とされるなどの社会的な影響や課題が懸念されている。既に、自動車に対するハッキング手法が公開されたため、140万台の自動車がリコール対象となったとのマスコミ報道もされている。また、医療機器についても近年ネット接続する機器の脆弱性に関する情報が増えている。

あらゆるモノがあらゆる地域でつながるような時代においては、従来と比較にならないほどの強固な情報セキュリティ基盤の整備が必要となる。IoTによって企業が扱う情報量が爆発的に増え、センシティブな情報も集まるようになると、従来以上にセキュリティリスクも増大する。様々な攻撃にさらされる危険性が非常に高くなるため、デバイスや関連するアプリケーションのベンダーはセキュリティを強化する必要に迫られることになる。ビジネスや社会にイノベーションを引き起こすためにも、IoTに関連するセキュリティ対策を加速することが重要になる。

1.3 IoTの標準化

IoTの発展に伴い重要となるのが「IoT規格の標準化」である。異なる機器やプラットフォーム間で標準化を進めることが重要なテーマとなっている。これまでに多くの技術が標準化によって普及し定着してきたように、企業が連携することにより業種を超えて新しい製品やサービスを生み出すために非常に重要な要素と考えられている。

IoT関連のコンソーシアムや標準化団体も多数あり、産業分野では150社以上の企業が「Industrial Internet Consortium」に参加している。また、「oneM2M」が欧米やアジアの通信関連の標準化組織7団体によって設立され、200以上の企業が参加して標準化が検討されている。

IoTの標準化技術については、例えば、工場の中の製造機器において、異なるメーカー製の機器同士であっても互換性を持った接続やデータ連携が大変重要と考えられている。大手の産業機器メーカーや半導体メーカーが標準化を推進することで、機器間の相互接続性を高めようとする取り組みが必須となる。また、こうした取り組みにより、世界各国へIoTデバイスを輸出している企業にとっては、グローバルなIoT利用を容易に実現できるインフラ環境の整備も求められている。

2014 年末には、ドイツが提唱する製造業強化戦略『インダストリー4.0：第 4 次産業革命』の国際標準化に向けた議論が始まった。国際電気標準会議は標準化に向けた検討グループの初会合を 2014 年にシンガポールで開催した。最終目標として、工場の完全自動化や、企業グループ間のサプライチェーン全体でのデータ統合を目指している。そのためには産業機械間でのデータ連携が不可欠であり、データ仕様や通信手順を統一化ができないとデータ統合管理も実現することが困難になる。

また、2016 年 4 月、日本とドイツが IoT の共通規格を策定することにおいて、政府間で覚書を交わすことが明らかとなった。覚書では企業や大学で開発中の技術等を可能な範囲で共有し、今後必要となる新しいソフトウェアや通信技術などで共同開発を進めることなどが盛り込まれている。技術的に先行するドイツとの間で共通規格とすることは、企業や国の枠を越えた共通の土台を作り上げ、国際標準化に向けて先行するチャンスになると考えられている。IoT 分野ではアメリカとドイツが開発で大きくリードし、日本の出遅れ感が問題視されていた。しかしながら、ドイツと連携を図ることでキャッチアップする機会を得たと考えられている。

1.4 IoT と法対応

IoT 技術により提供される製品やサービスにより、既存の法律の範囲で十分に対処できないプライバシー侵害などについての課題が表面化してきている。今後は、IoT デバイスを利用したシステムやサービスにおいて法対応や法解釈が大変重要になってくると考えられている。

また、2016 年 4 月には、EU 域内 28 カ国で個人データを保護する法律「EU データ保護規則」が採択された。個人データを扱う企業の域外へのデータの持ち出しを厳しく規制し、違反企業には最高でその企業の世界全体の売上高の 4%という行政上の制裁金を課すものである。IoT では個人が知らぬ間に個人情報を取得してしまうリスクがあり、この法律は IoT 関連サービスにも大きな影響を与えることになる。

IoT ベンダーはデータ転送の安全を確保すると共に、プライバシー保護に配慮することが必要となる。適切なプライバシーやセキュリティを確保するため、製品設計や開発プロセスにおいて十分な評価を行うことや、また、一般市民の個人情報や機微情報などを必要に応じて消去することなどが必要になると考えられている。

IoT によって様々な利便性が得られる反面、従来とは異なるリスク管理が必要となる。今後、IoT ベンダーはこれまでに想定していなかったような法的課題に対処することが求められるのである。

第2章　IoT の利活用動向

本章では、IoT データ利活用に対する消費者及びサービスを提供する企業側の意識調査の結果を概観する。また、企業における IoT データの利活用事例を紹介する。

2.1 IoT データ利活用に対する消費者意識

本項では、IoT データ利活用に対する消費者意識として、トレンドマイクロ社が行った調査結果[2]に対する考察を行った。なお、調査結果の詳細については、付録「IoT 時代のデータ利活用と情報セキュリティ対策調査」の 47 ページ以降を参照いただきたい。

(1) 日本国内の消費者

国内ではスマートフォン・タブレット、スマート TV 以外の IoT（スマートデバイス）の普及はあまり進んでいない。原因の一つとして、セキュリティ・プライバシーへの懸念が挙げられる。自分で情報をコントロールできないことや、提供者（スマートデバイスベンダ）によるセキュリティ・プライバシーに関する情報が開示不足しているため、ユーザが不安を感じていると考えられる。ただし、信頼できる企業に関してはユーザに明確な（とくに金銭的な）メリットがあれば、個人情報の提供への抵抗感は下がると考えられる。

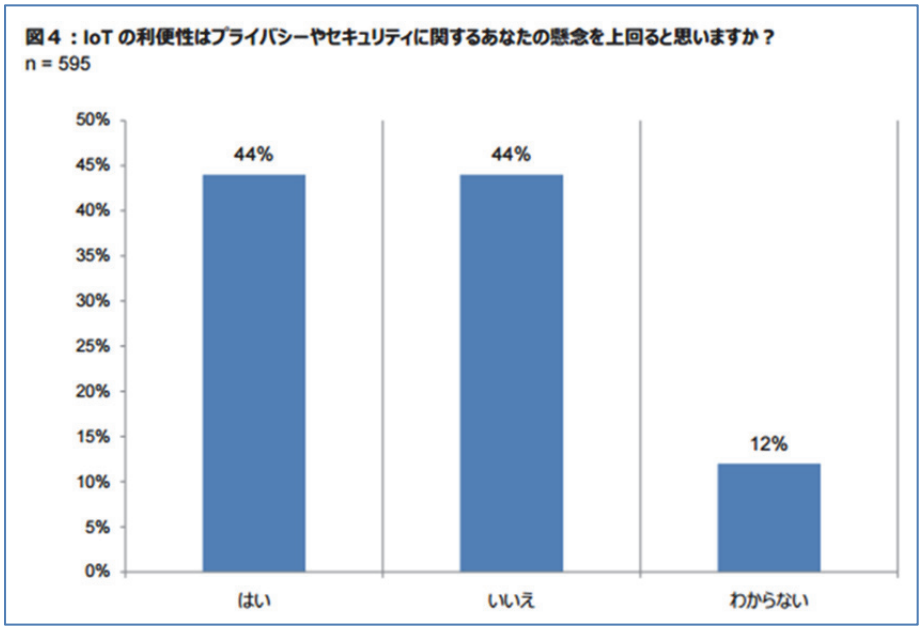

図 2.1-1　IoT の利便性とセキュリティ/プライバシーの懸念 [2]

[2] “IoT 時代のプライバシーとセキュリティ意識（トレンドマイクロ社）”
http://www.go-tm.jp/iot_2015/

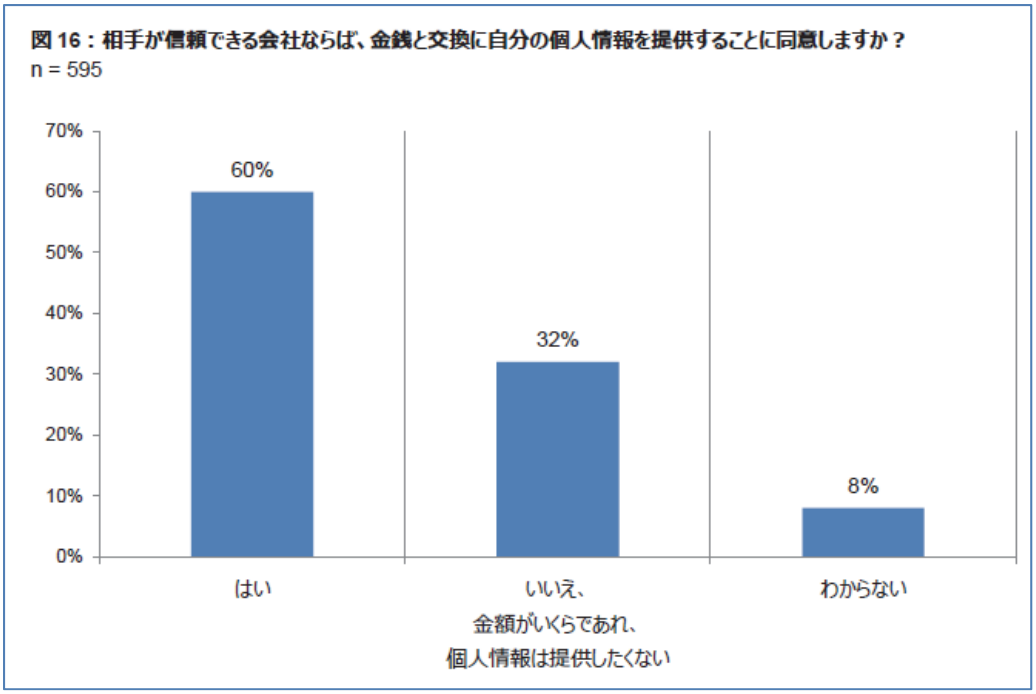

図 2.1-2　金銭と個人情報の交換可否 [2]

(2)海外の消費者との比較

日本は、欧米と比較してセキュリティへの懸念は最も高いが、一方でプライバシーへの懸念は低くなっている。欧州は個人情報・プライバシーデータ提供そのものへの懸念が強くなっている一方で、日本はセキュリティ対策の施された適切な範囲内であれば、プライバシーデータ提供への懸念は比較的強くないと考えられる。

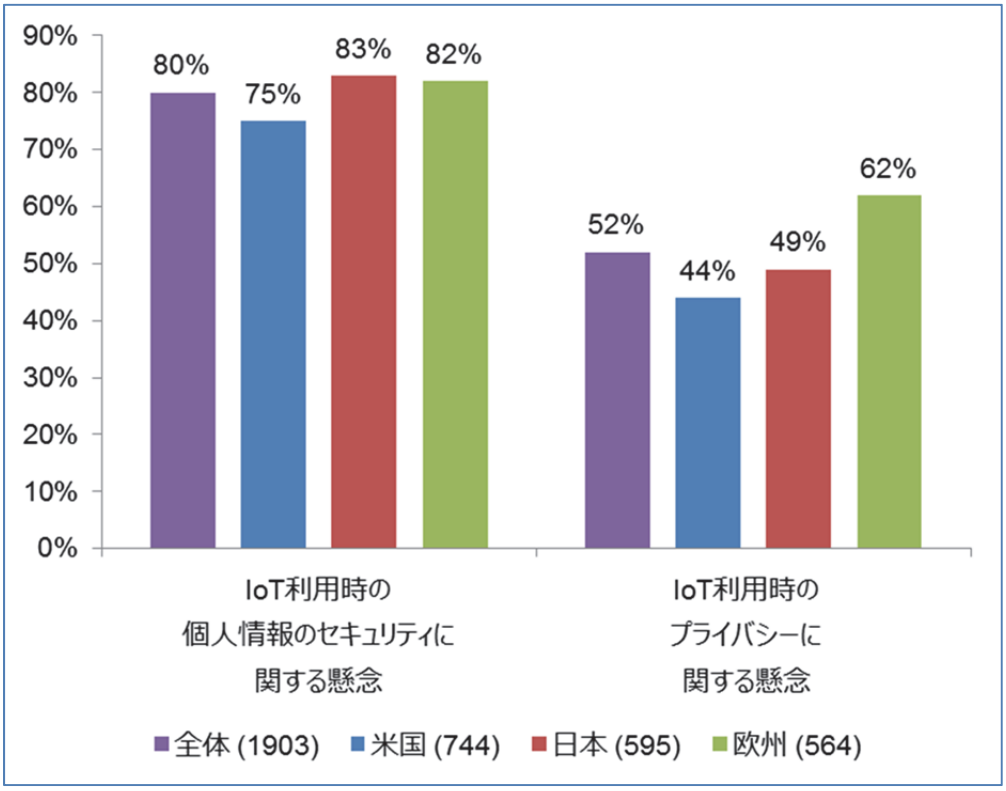

図 2.1-3　地域別 IoT 利用時の懸念事項 [2]

2.2 IoT データ利活用に対する企業意識

今年度の調査活動の一環として、IoT 時代の情報セキュリティ対策に関する企業の意識調査を行った。本項では、調査結果を紹介する。なお、調査結果の詳細については、付録「IoT 時代のデータ利活用と情報セキュリティ対策調査」の 60 ページ以降を参照いただきたい。なお、意識調査の実施概要は以下のとおりである。

調査タイトル　：IoT 時代の情報セキュリティ対策に関する企業意識調査
調査対象　　：国内の従業員数 50 名以上で、IoT 導入済/検討中の企業において IoT 導入について決裁や選択肢を絞り込む立場の方
調査手法　　：WEB アンケート
調査時期　　：2015 年 10 月
回収数　　：500 件

(1) パーソナルデータを収集しているか否かによる特徴

調査にあたり、導入済もしくは導入予定の IoT システムにおいて、パーソナルデータを収集しているか否かによって、異なる特徴があるのではないかという仮説を立てた。結果として、パーソナルデータを収集対象としている企業では、社内で分析を行い、その結果をマーケティング等に活用している割合が高く、セキュリティ対策について、具体的事例

やデバイスの保護に対するニーズが高いといった特徴が現れた。仮説の検証結果を表 2.2-1 に示す。

表 2.2-1　収集対象情報の違いによる特徴

	IoT システムでパーソナルデータを含む情報を収集している	**IoT システムでパーソナルデータを含む情報を収集していない**
業種	BtoC 企業が顧客のパーソナルデータを利用しているケースが多い。	製造業が多い。
IoT 導入背景、目的	・検討、導入が先行。特に 2011～2012 年頃に盛り上がった。 ・マーケティング等への活用される割合が高い。	・機器の遠隔制御の割合が高い。 ・ここ数か月で導入が進んでいる。 ・データ販売ビジネスを IoT 導入目的とする割合が比較的高く、パーソナルデータを含む情報よりも障壁が低いと思われる。そのため今後パーソナルデータを含まない情報を販売するビジネスが広がる可能性あり。
社内体制	大部分がデータ分析を社内で行う。専門部署で分析するケースも多い。	・IoT 導入へ現業部門の関わりが強いケースが多い。 ・社内でも現業部門で分析する割合が多い。
セキュリティ対策ニーズ	具体事例やセキュリティ対策の情報、デバイスの保護へのニーズが比較的高い。	セキュリティ対策ツール、プラットフォーム、人材育成サービスへのニーズが比較的高い。

(2) IoT システムの導入時期による特徴

また、IoT システムの導入時期によって、異なる特徴があるのではないかという仮説も立てた。結果として、IoT システムは、従業員数 10,000 人以上、総売上高 1,000 億円以上の BtoC 分野の大企業で導入が進んでいることが明らかになった。また、未導入の企業でも、1 年以内に導入を予定するなど検討が具体化してくるとシステムの脆弱性や情報漏洩などの懸念事項に対し、センシティブになってくるという特徴が現れた。仮説の検証結果を表 2.2-2 に示す。

表 2.2-2　システム導入時期の違いによる特徴

	時期未定で検討中	一年以内に導入予定	導入済
企業規模	・50 ～300 人規模の企業で導入検討が開始 ・総売上高 1～10 億円の企業で導入検討が開始	小規模～大規模企業の 8～16％が一年以内に導入予定	・導入済み企業の 30％弱は従業員数 10,000 人以上の大企業 ・総売上高 1,000 億円以上の企業で導入が進んでいる ・BtoC 企業での導入が進んでいる
業種・業態	特に建設業で検討を開始する企業の割合が増加	BtoC の企業で IoT の導入・導入検討が進んでいる	
ニーズ	導入事例や技術系人材へのニーズが高い	・導入が具体化する段階ではあらゆる脆弱性や懸念事項に対してセンシティブ ・特に情報漏えいは半数が深刻な懸念事項と考えている ・検討が進み 1 年以内に導入予定の場合、セキュリティ対策関係へのニーズが高くなる	導入済みの企業では人材不足が最も大きな課題

(3) 各セグメントの特徴

(1)、(2)の仮説に対する検証結果のまとめを表 2.2-3 に示す。

表 2.2-3　各セグメントの特徴

	IoT システムでパーソナルデータを含む情報を収集している	IoT システムでパーソナルデータを含む情報を収集していない
時期未定で導入検討中	ここ 1、2 年で製造業以外の業種（情報通信、医療等）でも検討が進んでおり、導入事例、人材育成の提案が求められているセグメントである。	ここ 1、2 年は建設業等が増えてきており、今後も増加傾向のセグメントである。

一年以内に導入予定	導入間近の BtoC 企業で課題意識が高くなっており、セキュリティ対策関連のニーズが最も高いセグメントである。	IoT 導入検討に現業部門も関わっていることが多く、セキュリティ対策ツール、PF、人材育成サービスへのニーズが最も高いセグメントである。
導入済	BtoC 企業がマーケティングのために IoT 導入を進めており、セキュリティ対策、とくにデバイス保護のニーズが高いセグメントである。	大手製造業で機器の遠隔監視等のために導入が進んでいる。データ販売ビジネスに関心をもつ可能性が高い。

2.3 企業の IoT データ利活用事例

本項では、IoT のデータ利活用を進めている企業の事例を紹介する。2.3.1～2.3.3 が、パーソナルデータを含む情報を収集している事例となる。

2.3.1 健康プラットフォーム「WM（わたしムーヴ）」（NTT ドコモ）

WM（わたしムーヴ）は、ヘルスケア関連のプラットフォーム事業として、2013 年に提供が開始された[3]。

様々なアプリケーション（例：ダイエット、睡眠記録、運動記録、体調管理、血圧管理等）と血圧計、体重計、体温計等の測定機器が連携する。例えば、体温計で体温を計測し、スマートフォンをかざすことで、測定データが転送・記録される。

各種測定機器、アプリケーションのデータはプラットフォーム上に蓄積・分析され、一般ユーザに対しよりよいライフスタイルを提案したり、アライアンス企業に対しデータを活用したビジネス機会を提供したりするサービスである。

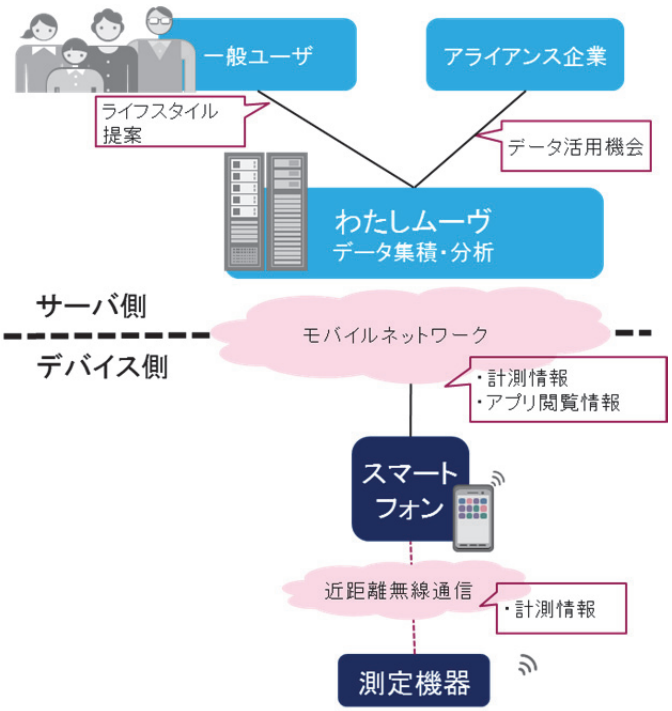

図 2.3-1　わたしムーヴのアーキテクチャ

[3] “健康プラットフォーム「WM（わたしムーヴ）」の提供開始”
https://www.nttdocomo.co.jp/info/news_release/2013/03/06_00.html

2.3.2 高齢者見守りシステム（クオリカ）

高齢者見守りシステムは、クオリカと岐阜県群上市 NPO 法人つくしん棒との共同実証実験が 2014 年に開始された[4]。

水道の流量計へ通信装置を設置し、モバイルネットワークにてデータサーバへデータを送信し、水道利用パターンから生活における事象を推測するシステムである。以下のような事象例が推測可能となると考えられている。

①トイレ回数増加→糖尿病の可能性

②入浴回数の不自然な増加→認知症可能性　等

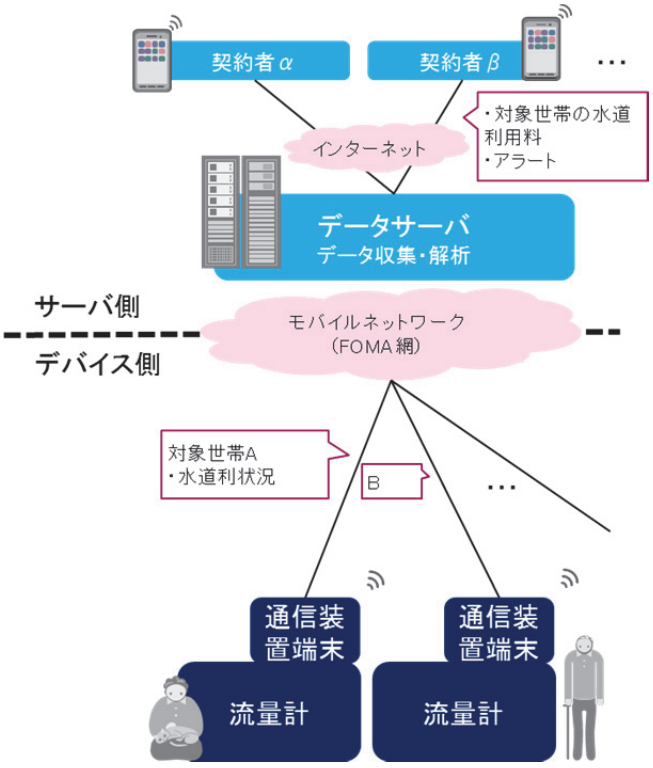

図 2.3-2　高齢者見守りシステムのアーキテクチャ

[4] “クオリカ、NPO 法人つくしん棒と共同し、水道メーター情報を活用した高齢者見守りシステムの実証実験を開始”
https://www.qualica.co.jp/news/140127_2.html

2.3.3 車番認識システム「PMO パーキング・アナライザー」（駐車場綜合研究所）

PMO パーキング・アナライザーは、駐車場ゲート部に入場する車輌のナンバープレートをカメラで撮影し、その情報をデータ化して分析するシステムである。2014 年 4 月に提供が開始された[5]。

リアルタイム帳票出力機能に併せ、ナンバープレート情報から町名まで地図化する機能を持つ。自動車検査登録情報協会等と連携し、ナンバーから登録検査情報を収集している。分析結果から以下を実現している。

①来店車両の駐車場利用時間

②車利用者の商圏把握

③特定ナンバーに対するアラート

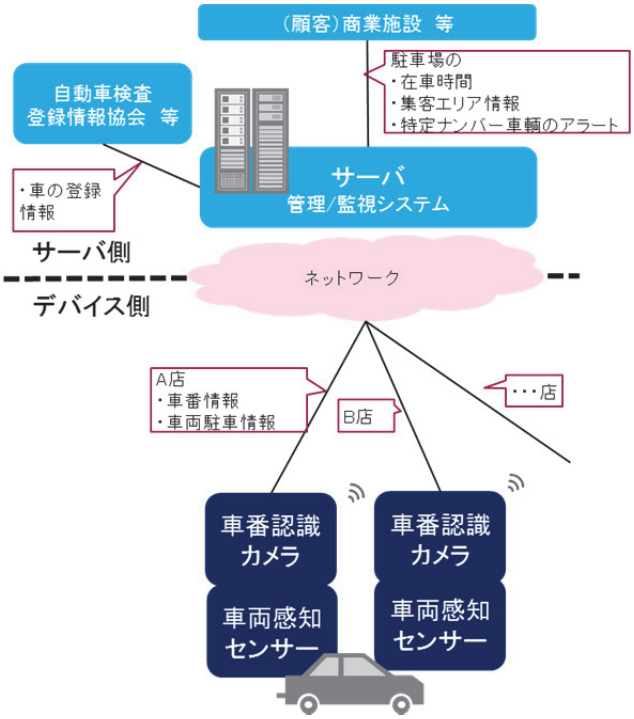

図 2.3-3　PMO パーキング・アナライザーのアーキテクチャ

[5] “車番認識システム「PMO パーキング・アナライザー」販売開始のお知らせ”
http://prtimes.jp/main/html/rd/p/000000003.000007474.html

2.3.4 KOMTRAX（コマツ）

KOMTRAX は、建設機械に装備された GPS やセンサーから建設機械の所在地、車両状態、稼働状況等の情報をモバイルネットワーク経由で収集し、分析を行うシステムである[6]。2001 年からすべての建設機械に GPS やセンサーを標準装備している。収集したビッグデータの分析結果から以下を実現している。

①建設機械の稼働データを元に配車計画や作業計画の作成支援、最適時期の点検や部品交換など顧客ごとの「カスタマイズ化」により保守・運用サービスを向上

②建設機械の盗難防止

③建設機械の稼働状況で製品の需要動向予測

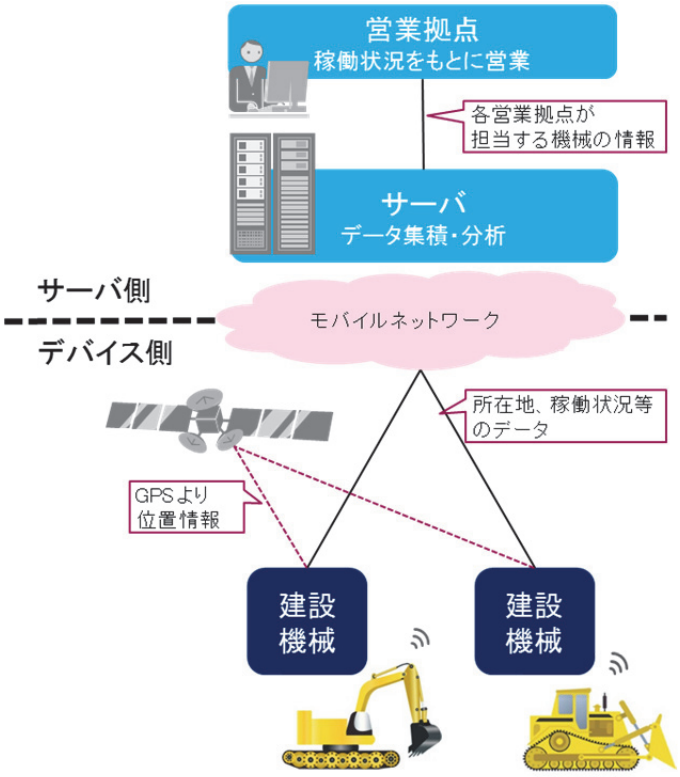

図 2.3-4　KOMTRAX のアーキテクチャ

6 “ビッグデータ活用でビジネスはどう変わったか～コマツにおけるモノのインターネット事例から考える～”
https://www.salesforce.com/jp/socialenterprise/social-media/vol3-bigdata.jsp

2.3.5 「精算客数予測システム」（ベイシア）

ベイシアでは、イギリスのシステム開発会社の製品である精算客数予測システムを 5 年前に導入した[7]。

入口とレジの近くに 50 台近くのセンサーを設置。店内の客数（組数）やレジ待ち客数（組数）をカウントし、客数情報、レジ待ち客数情報と過去の実績データをもとに数十分以内に必要となるレジの台数を予測する。予測結果をレジ前係の PDA へ送信することで、以下を実現している。

①レジ待ち時間の減少による顧客満足度（CS）の向上

②レジ人員の効率化によるコスト削減

③混雑前に準備可能となり心理的負担が下がることによる従業員満足度の向上

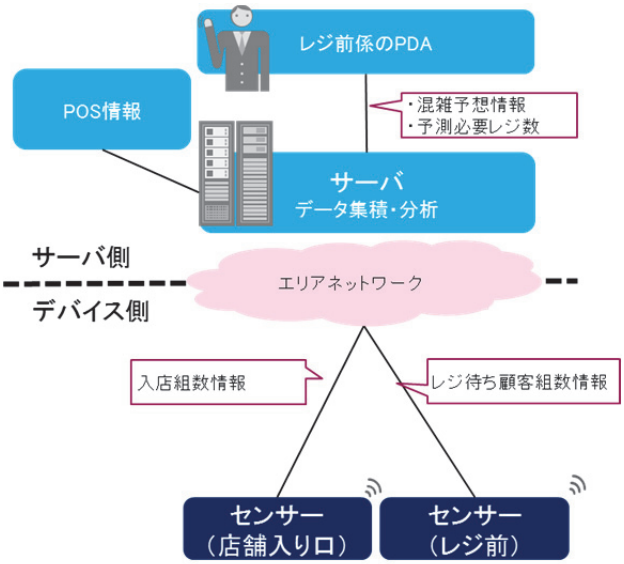

図 2.3-5　精算客数予測システムのアーキテクチャ

[7] “激安スーパーを支える IoT、30 分後の混雑予測（日経情報ストラテジー、2015/1/6）”

第3章　IoT の脅威とリスク

本章では、IoT において想定される脅威とリスクを例示した上で、実際に IoT に関連して発生したインシデントの事例を記載する。

3.1 想定される IoT の脅威とリスク

本節では、IoT において想定される脅威を整理する。

3.1.1 脅威を想定する際の IoT モデル

下図の IoT モデルに従って、レイヤー毎に想定される脅威を検討する。

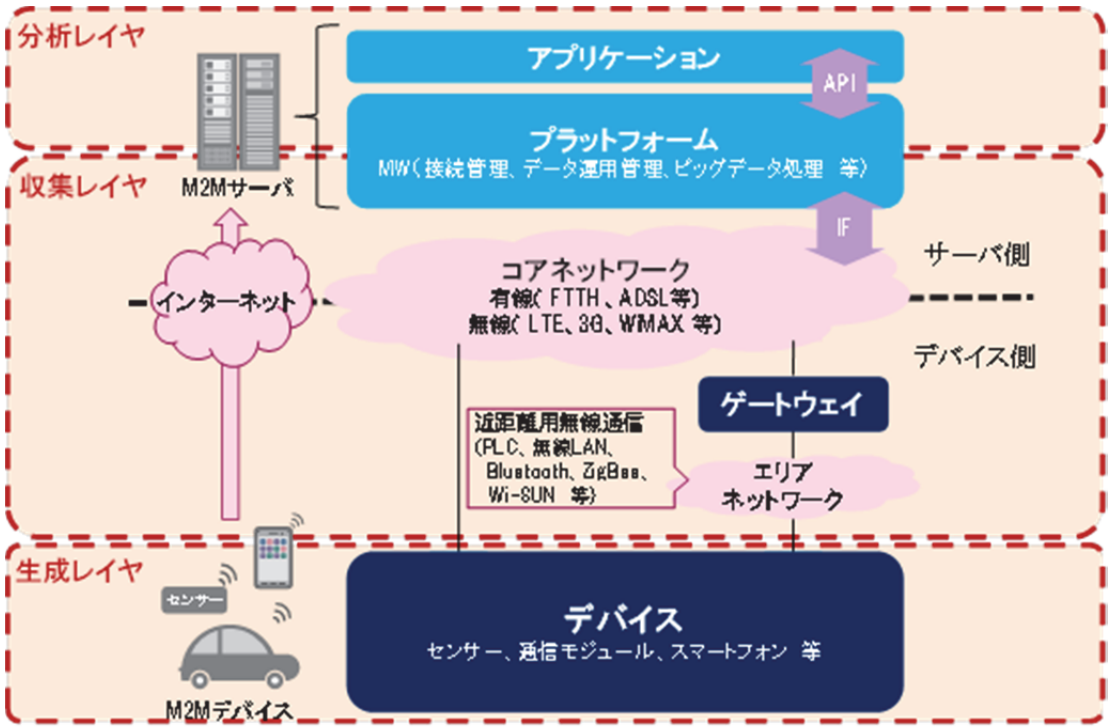

図 3.1-1　IoT/M2M のアーキテクチャ

各々のレイヤーの概要を次に記す。

(1) 生成レイヤー

本来の機能に加えて情報収集・通信機能を持ち、データを生成するデバイスが生成レイヤーに相当する。このレイヤーは収集レイヤーとネットワークを介して接続され、デバイスが生成したデータの送信を行ったり、遠隔からデバイスの操作・制御を受けたりする。

なお、生成されるデータには業務データやパーソナルデータといった機微な情報が含ま

れる場合がある。

(2)収集レイヤー

収集レイヤーでは、生成レイヤーのデバイス類からネットワークを介して自動的にデータを収集する。加えて、デバイス類の接続管理や収集したデータの管理も行う。

(3)分析レイヤー

分析レイヤーでは、収集された大規模データを分析し、サービス提供や業務効率化につながるような情報提供を行う。加えて、データの分析だけではなく、分析結果に基づいてデバイスの制御を行う場合や、サービスを提供する場合もある。

3.1.2 生成レイヤーで想定される脅威と特徴

生成レイヤーで想定される脅威を次に示す。

(1)デバイス内の情報に対する脅威

デバイスが生成したデータや、収集レイヤーに接続するための認証情報（パスワードや暗号鍵等)の漏洩が脅威として考えられる。デバイスに対して不正アクセスされる場合や、収集レイヤーにアクセスする際に通信の保護が不十分なために漏えいする場合などが想定される。

生成したデータは機微な情報を含む場合もあり、そのような場合にはプライバシー面での被害が生じ得る。

(2)デバイスの不正操作や動作妨害に関する脅威

正当なユーザやサービス以外からデバイスが不正に操作されたり、正常な動作を阻害されたりすることが脅威として考えられる。

一般的なITシステムへの攻撃と異なり、IoTではデバイスが不正操作された場合に物理面での影響が生じ得る。例えば、自動車で運転を第三者に制御されれば、最悪の場合には人命への影響も生じる。また、セキュリティシステムが不正に操作されてドアロックが解除され、物理的なセキュリティが無効化される状況も想定される。このように、IoTデバイスへのセキュリティ侵害は、実世界のセーフティへの影響につながる。

(3)踏み台として悪用される脅威

デバイスが攻撃者に踏み台として悪用され、第三者への攻撃に加担することが脅威として想定される。

踏み台として悪用されることは一般的なITシステムでも想定されるが、生成レイヤー

のデバイスは数が多く管理の徹底が困難なこと、ライフサイクルが長いことなどから、脆弱性発覚時の対策に課題があり、悪用されるリスクは高いと考えられる。

(4)生成レイヤーで想定される脅威の特徴

生成レイヤーのデバイスは、これまでインターネットへの接続が想定されていなかったものもある。このため、一般的な IT システムでは常識的に行われているようなセキュリティ対策が漏れていたり、不十分であったりする場合がある。

例えば、セキュリティに関する設定のデフォルト値が不適切である、設定が正しくされないために脆弱な状態で運用されている、といった場合がある。具体的には、パスワードが設定されない、マニュアルに記載されたパスワードが変更されずそのまま利用される、とった状況がある。

また、これまで閉じたネットワーク環境での利用を前提としていたものをインターネットに接続したために、認証や通信の保護が不十分で、なりすましや情報漏洩のリスクが高い場合もある。

加えて、前述の通り運用開始後の脆弱性への対処に課題がある。

生成レイヤーのデバイスにおいても、一般的な IT システムと同様に設計段階からのセキュリティの検討と作り込み、及びセキュリティを維持するための継続的な脆弱性対策などの運用が必要であろう。

3.1.3 収集レイヤーで想定される脅威

収集レイヤーで想定される脅威を次に示す。

(1)不正な情報を受け取る脅威

生成レイヤーからのものではない不正な情報を、あたかも正当なデバイスからのものとして受け取る脅威が想定される。

結果としてデータ分析に悪影響が生じたり、場合によってはデータを元にしたデバイスに対する操作や制御が不適切なものとなり、実世界に悪影響を生じることも想定される。

(2)保持する情報に対する脅威

生成レイヤーから受領し、保存している情報が漏洩したり、改ざんされたりするような脅威が想定される。

漏えいの場合にはプライバシー面での被害につながる恐れがあり、また、改ざんの場合には前項と同様の結果につながることが想定される。

(3)収集レイヤーで想定される脅威の特徴

収集レイヤーで想定される攻撃は、一般的な IT システムに想定されるものと同様であるが、取り扱う情報が機微なものである場合があること、また、そのような情報を大量に取り扱うことから、プライバシー面でのリスクはこれまで以上に高いと言える。

また、大量となる生成レイヤーのデバイスを安全に運用するためには、収集レイヤーでの管理機能が重要になるだろう。

3.1.4 分析レイヤーで想定される脅威

分析レイヤーで想定される脅威を次に示す。

(1)プライバシー面での脅威

分析されるデータにはパーソナルデータなど機微な情報を含む場合があり、取扱いによってはプライバシーを侵害する場合もある。

(2)デバイスに不正な操作・制御を指示する脅威

分析結果をデバイスにフィードバックして制御する場合に、分析ロジックに誤りがあったりして予期せぬ制御を行う脅威が想定される。

(3)分析レイヤーで想定される脅威の特徴

分析レイヤーで想定される攻撃も一般的な IT システムに想定されるものと同様である。

しかし、取り扱う情報が機微なものである場合があったり、収集したデータ自体は機微な情報を含まなくともビッグデータ解析の結果、プライバシー情報になる場合が想定されるので、一般的な IT システムと比してプライバシーを侵害するリスクは高いと言える。

また、IoT で収集する情報の利活用に関する法制度の整備は途上であり、その面でのリスクも未知数である。

3.2 IoT のインシデント事例

前述で示したように、IoT で様々な脅威が想定されている。本節では、実際に発生した IoT のインシデントの主な事例を記載する。なお、より詳細を知りたい場合は、付録「IoT 時代のデータ利活用と情報セキュリティ対策調査」の 56 ページ以降を参照頂きたい。

(1)事例：サーモスタットを踏み台としたホームネットワークへの侵入可能性

2014 年 8 月、米国では Nest 社のサーモスタットのセキュリティ対策について、TrapX

Labs がそのセキュリティ対策を回避する方法を提示したという報告があった[8]。TrapX Labs によればサーモスタットを踏み台としてホームネットワークへの侵入が可能で、最終的にはルート権限を奪取することが可能としていることから、スマート家電の分野において、すべての機器を自由に操作される危険性があることが示唆された。

(2) 事例：ネットワークカメラの脆弱性

2014 年 11 月に、日本に設置された約 1300 箇所の防犯カメラ情報が流出したという報告があった[9]。Web サイト「Insecam」において、世界各国に設置されている防犯カメラのうち、デフォルトのユーザ名とパスワードを変更せずに使用している防犯カメラ映像を取得しており、情報流出が生じているということがわかった。流出の主な理由は、パスワードの設定不備、アクセス制限設定の問題であるとされている。ネットワークにつながるカメラは、2007 年に「カメラにおける重要な情報を取得される脆弱性（JVNDB-2007-002641）」、2008 年に「複数のネットワークカメラにおけるクロスサイト・スクリプティングの脆弱性（JVNDB-2008-000037）」等が公表され、2014 年には「複数の IP カメラにおける認証回避の脆弱性（JVNDB-2014-000087）」が公表され、攻撃者が認証回避して外部から自由に映像が見られる危険性が報告される等、脆弱性の報告が続いている。

(3) 事例：電光掲示板のハッキング

2015 年 1 月には、ロサンゼルスのダウンタウンにおいて、交通情報を表示する電光掲示板がハッキングされたとの報道があった[10]。掲示板の所有者の Traffic Management Incorporated 社によれば、手口は不明だが、装置のある場所に侵入して書き換えたか、Wi-Fi が使えるタイプなのでリモートから書き換えられた可能性もあったと報告されている。

(4) 事例：医療機器及び自動車の脅威

2015 年 4 月には、医療分野における遠隔手術ロボットに対してリモートハッキングできたという初の事例報告があった[11]。医師からロボットに送る信号を遅延させたり改ざんしたりして、遠隔手術ロボットの動作を不安定にすることができた。独自の通信規格を使用しているが公開されているため、乗っ取ることが容易としている。

---

[8] “米国 net-security 記事”
https://www.helpnetsecurity.com/2015/03/10/hacking-nest-thermostat/

[9] “日本 techcrunch 記事”
http://jp.techcrunch.com/2014/11/08/20141107insecam-displays-insecure-webcams-from-around-the-world/

[10] “米国 LA Weekly 記事”
http://www.laweekly.com/news/read-a-f-ing-book-street-sign-was-likely-a-hack-photos-5332229

[11] “米国 MIT Technology Review”
https://www.technologyreview.com/s/537001/security-experts-hack-teleoperated-surgical-robot/

2015 年 7 月には、自動車の遠隔操作問題で 140 万台リコール対象になるという報告があった[12]。携帯電話ネットワークにもつながる車内インターネット/エンターテインメントシステム「Uconnect」における脆弱性があると報告され、セキュリティ研究者により発見されたこのセキュリティホールを突くと、遠隔からアクセスし自動車の制御を奪えるという事例報告であった。すなわち、Uconnect 搭載車を半ばラジコン化することができ、自動車のブレーキやステアリング操作、エンジンのオン/オフに至るまでを勝手に操作される可能性があると報じられた。対策として、遠隔操作の標的となりうる車種はリコール対象とすると共に、Uconnect の修正プログラムの配布が実施された。

[12] “日本 engadget 記事”
http://japanese.engadget.com/2015/07/27/140-1-500/

第4章　IoT セキュリティ対策の動向

前章までで、IoT に関する脅威とリスクについて述べたように、IoT ではこれまで想定されることのなかったデバイスとの接続が増大しており、想像以上に多くの IoT デバイスがネットワークを介してプラットフォームやアプリケーション（サービス含む）と連携され始めている。一般の消費者にとっては、どのような IoT デバイスがどのようなプラットフォームやアプリケーションとつながっているかは解らない。ましてや本当にそのプラットフォームやアプリケーションが安全で安心できるものかなど解らない状態である。更に、IoT デバイスはライフサイクルが長く人手によるデバイス自身の監視が行き届かないなどの管理面でも難しい。

そこで本章では、これらの IoT に関する脅威とリスクをできる限り最小とするために必要となる IoT セキュリティ対策を述べる。

4.1 IoT セキュリティ対策の方向性

IoT デバイスはモビリティ機能と標準的な通信機能（オープンプロトコルによる通信）を前提として構成されており、不特定多数の人間やデバイス、システムが容易に接続可能となっている。そして、接続されるデバイスやプラットフォームのアーキテクチャは異なり、安心・安全のレベル（セキュリティレベル）も異なっていることがある。この場合、システムの接続性や可用性を重視し、サービスを稼働させるために、セキュリティレベルは低いレベルに合わされるのが常である。

このような状態でセキュリティを高めるためには、利用者が使う IoT デバイスと、最終的にサービスを提供するアプリケーションの間のセキュリティを強固なものにして、その間にあるネットワークやプラットフォームのセキュリティの強度に依存しないシステムを採用することが望ましい。そのためには、IoT デバイスやアプリケーションが予期したとおりの動作（正しい動作）が得られることが必要である。

IoT デバイスを長期に渡って利用することを想定するのであれば、世の中の進展に合わせたセキュリティレベルを確保するために、IoT デバイスのセキュリティ機能の維持が必要となってくる。一般的にセキュリティ機能を維持するためには、脆弱性への対応とセキュリティ機能の陳腐化に伴う更新などが必要となってくる。脆弱性対応やセキュリティ機能の更新などの IoT デバイスの管理は、IoT デバイスの増大に従い人手による管理は困難となってきているので、リモートによる IoT デバイスの管理が今後必要となってくると言える。

また、IoT システムを提供する側は企画・開発段階での「プライバシー・バイ・デザイン」を考慮した設計を行い、そして利用する側も、どのようなデータが収集されており、どのように利用されているのかに注意を払うことが必要である。

4.2 IoT セキュリティの技術対策

IoT システムの階層は、デバイス、ネットワーク、プラットフォーム、アプリケーション（サービス含む）の４階層からできている。また、その利用の仕方から分類する IoT モデルの階層は、分析レイヤー、収集レイヤー、生成レイヤーから構成されている。

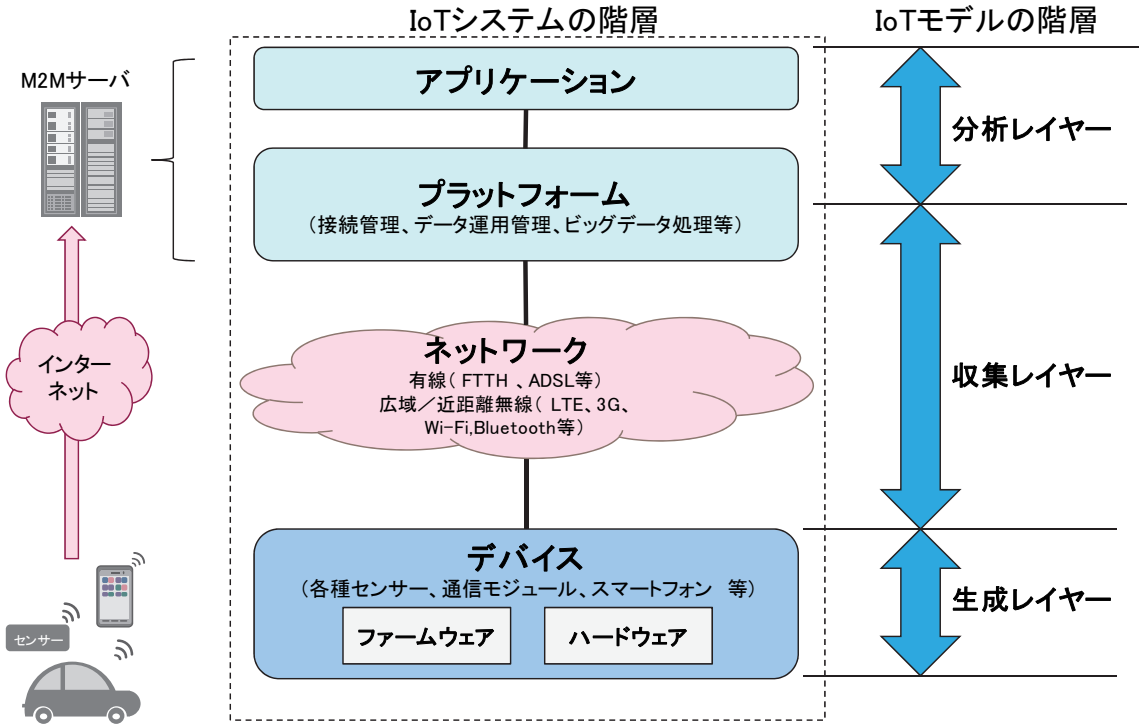

図 4.2-1　IoT システム及び IoT モデルの階層

デバイスは各種センサー、通信モジュール、スマートフォン等とそれらの機能を搭載した装置のことでハードウェアとファームウェアから構成されていることが一般的である。

これらの階層でのセキュリティ対策として次のようなものが挙げられる。

(1)デバイスのセキュリティ対策

脅威の具体例：　マルウェアによる情報漏えい、デバイスの乗っ取り、物理的な破壊

対策技術：
- 機器認証
- ユーザ認証
- デバイス内のデータ暗号化
- サービスとデバイス間のエンドポイント暗号化
- デバイスの真正性の確認
- マルウェア感染検出と感染からの回復

(2)ネットワークのセキュリティ対策

脅威の具体例：　ネットワーク上の通信暗号化の欠如による情報漏えい

対策技術：　・通信データの暗号化、電子署名

・ネットワークの監視

・ネットワークの物理的隔離

(3)プラットフォームのセキュリティ対策

脅威の具体例：　プラットフォームのデータ改ざん、情報漏えい、サービス障害

対策技術：　・プラットフォームへのアクセス制御（機器認証）

・プラットフォームのデータ暗号化

・IoT デバイスのログ管理、監視

・プラットフォームの保護、回復

・脆弱性への対応

(4)アプリケーションのセキュリティ対策

脅威の具体例：　なりすまし、脆弱性攻撃による不正利用、情報漏えい、サービス停止

対策技術：　・アプリケーション（サービス含む）へのアクセス制御（ユーザ認証）

・アプリケーションとデバイス間のエンドポイント暗号化

・アプリケーションの真正性の確認

・脆弱性への対応

IoT システム要素に必要となる主なセキュリティ対策を一覧にしたものが表 4.2-1 である。

表 4.2-1　システムの主なセキュリティ対策

	機器認証	ユーザ認証	データ暗号化	エンドポイント暗号化	真正性の確認	マルウェア感染検出と感染からの回復	ログ・監視	物理的隔離	脆弱性への対応
IoTデバイス	●	●	●	●	●	●			●
ネットワーク			●				●	●	
プラットフォーム	●		●		●	●	●		●
アプリケーション		●		●	●	●			●

この表からも判るように、IoT デバイスのセキュリティ対策が最も多くなると共に、IoT デバイスは広く配布、そして長期に渡って設置されるものであるから、これらのセキュリティ機能は IoT デバイスの開発・設計時点から考慮する必要がある。

特に、IoT デバイスとアプリケーション間のエンドポイント暗号化については、データの安全な取り扱いのために必須と言える。

4.3 IoT デバイスのセキュリティ機能

IoT デバイスは、そのリソース環境により対策の仕方は異なるが、次のような機能を持つことが望ましい。表 4.3-1 にこれからの IoT デバイスに必要なセキュリティ機能を掲げる。

表 4.3-1　IoT デバイスに必要な機能

これから必要な機能	説明
デバイス・アイデンティティの確立と保護	IoT デバイスは、アプリケーション、または他の IoT デバイスと伴に相互認証を実行する能力を持つべきである。なお、IoT デバイスにはユーニークな ID が付与されていることが条件となる。これにより、未許可の IoT デバイスを防止すると共に、不正なアプリケーション（なりすまし）を防止することができる。
デバイスとアプリケーション間のエンドポイント暗号化	IoT デバイスとアプリケーションの間でデータの暗号化を行い、指定されたアプリケーション以外にはデータが復号化出来ないようにする。
マルウェア感染に対する保護（セキュアブート）	IoT デバイスは、セキュアブートを実施して、起動時に IoT デバイスが正しい動作をするか否かを検査する。正しくないと判断された場合にはマルウェア感染と考えて、不正な動作を制限する。
感染からの回復（安全な回復）	マルウェアに感染した IoT デバイスは、安全に機能回復が実行できることが望ましい。（回復できるべきである） これは、感染したデバイスを検出して、健全状態に回復して、正しい機能化をリスタートするようにする。ただし、この回復プロセスはプラットフォームで管理される必要がある。
デバイス・ヘルスの保護（アップデート）	IoT デバイスは、ファームウェアのアップデートを安全にする機能を持つべきである。これは、デバイスが既知の脆弱性に対してアップデートのインストールを素早く、そして、安全に行われることによってマルウェアの一歩先を行く状態を保つのに役立つ。

これから必要な機能	説明
感染後の機密保持	IoT デバイスがマルウェアに感染している場合、マルウェアがそれらにアクセスすることができないようにし、ユーザデータとロングターム鍵のような重要な機密情報を保護する。
ハードウェア改ざんに対しての保護	IoT デバイスは、ハードウェア改ざんに対して自身を保護する必要がある。例えば、耐タンパ機能などを内蔵して、改ざんされた場合にはプラットフォームやアプリケーションに通知して、早急な対応が取れるようにする。
データの秘匿性の保護	データの無許可の暴露からの保護。例えば、秘密鍵を IoT デバイスからコピーして、そのデバイスになりすまして、ユーザデータを取得するなど。
データの完全性の保護	データの無許可の変更からの保護。例えば、電気メーター上で記録を修正する。
プログラム実行の保護	プログラム実行が干渉できる場合、セキュリティ検査をスキップすることができ、IoT デバイスの信頼性は危うくされる。
保存データの秘匿性、完全性、可用性	IoT デバイスで保存される秘密データを保護する。
デバイスのリユースまたは破棄	IoT デバイスがリユースされるか廃棄される前には、以前のオーナーが所有しているセンシティブなデータを安全に消去する方法を提供する必要がある。そして、IoT デバイスが安全に新しいオーナーが利用できるようにするか、または分解とリサイクルのための安全な方法を用意する。
暗号プロトコル要件の適合	IoT デバイスは信頼性の低いネットワークにつながる可能性がある。このため暗号プロトコルの実装は不可欠である。セキュアな鍵ストレージと暗号アクセラレーションの適切な実装を行う。暗号アルゴリズムは最終的に弱体化されるので、暗号プロトコルの更新が可能となる実装を考慮しておく必要がある。
監査ログを保持	アカウンタビリティを保持して、ログはセキュアに保存する必要がある。これは、フォレンジックとして必要不可欠である。
リモート管理	IoT デバイスは、セキュアなリモート管理を実装する必要がある。これらは、プラットフォームやサービスで管理されており、IoT デバイスの状況を確認できるようにする必要がある。

これから必要な機能	説明
レガシーハードウェアの接続	IoT デバイスとしてのセキュリティ機能やファームウェアのアップデート機能などを装備していないレガシーハードウェアは、データの出入口に対してセキュリティ対策を実施する。 また、物理的セキュリティの有る場所に設置するなども検討する。

IoT デバイスの中には、コスト削減のためにあえてレガシーハードウェアとしてファームウェアのアップデートをしないデバイスもある。更に、今後 IoT デバイスの活用が進み、データ量が増大するとデータ処理の効率化等のために、IoT/M2M サーバを経由しない IoT デバイス同士の通信や連携が増えることも予測される。このような場合には、IoT ゲートウェイを設置して、IoT デバイスと M2M サーバ間のセキュリティ機能の維持や、デバイス間通信の保護、外部からの不正アクセスの防止などを実施するのが良い。

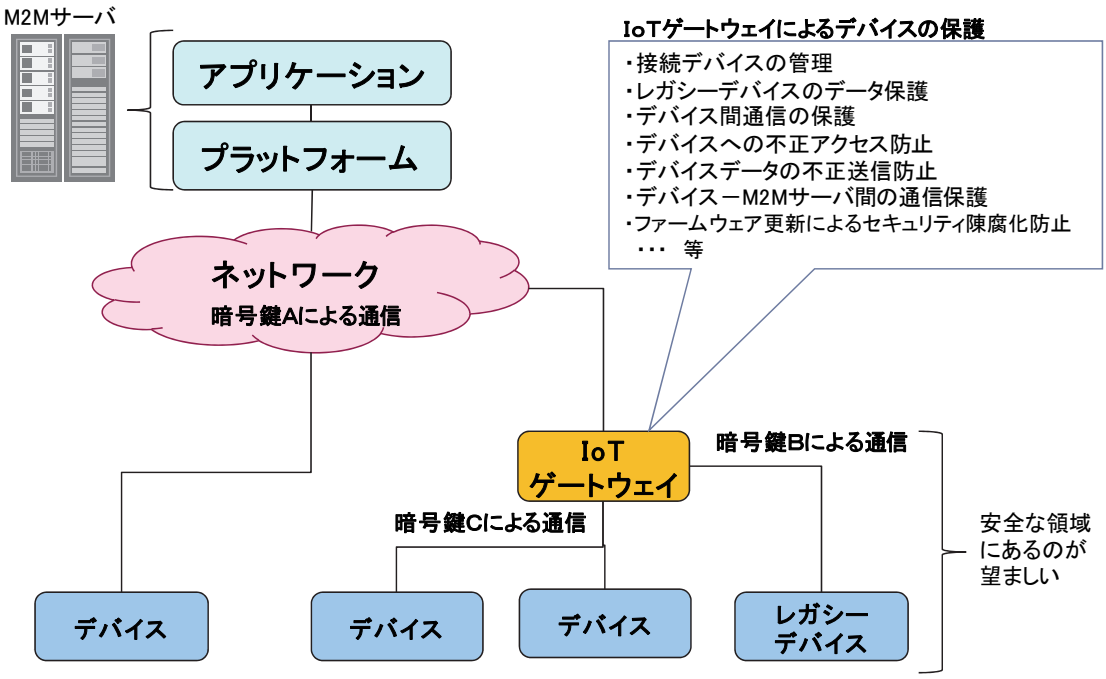

図 4.3- 1　IoT ゲートウェイによる IoT デバイスの保護

4.4 IoT セキュリティのその他対策

IoT システムのプラットフォーム、アプリケーションは、IoT モデルの分析レイヤーに相当し、ここに存在するデータはパーソナルデータなど機微な情報を含んでいる事が多い。

このため、分析レイヤーのセキュリティ対策としては、サーバやアプリケーションに施す技術的セキュリティ対策だけでなく、組織的、物理的、人的なセキュリティ対策を施す

必要がある。

分析レイヤーでは、IoT デバイスからのデータを守るべき重要情報資産と位置付け、機密性、完全性、可用性に対する様々な脅威から守るため、系統立てたバランスのよい現実的なセキュリティ対策を施していく必要がある。これらのニーズに現実的な対処をするものとして情報セキュリティマネジメントシステム（ISMS: Information Security Management System）がある。ISMS とは、情報セキュリティを確保、維持するための、人的、物理的、技術的、組織的な対策を含む、経営者を頂点とした組織的な取り組みのことであり、ISMS の要求事項の基準は、国際規格 ISO/IEC 27001／日本工業規格 JIS Q 27001「情報セキュリティマネジメントシステムー要求事項」に記載されている。

情報セキュリティ対策は一度行なったら終わりではなく､新たな脅威に対応するために、環境の変化に合わせて絶えず、見直しと改善が求められる。このために、Plan（計画）-Do（実施）-Check（点検・監査）-Act（見直し・改善）という PDCA サイクルをまわす必要がある。このためには、経営層の理解が必要不可欠である。経済産業省と独立行政法人 情報処理推進機構は経営層に向けて、セキュリティ対策は経営問題とする「サイバーセキュリティ経営ガイドライン」[13] を発行して、セキュリティ意識の向上をはかっている。

4.5 標準化に向けた取り組み

安全な IoT デバイスが適切な状態でネットワークにつながるための取り組みとして標準化がある。IoT デバイスの種類や使い方は様々であるので、業界毎に標準化や基準の作成が必要となってくる。

現在、IoT 関連では多くのコンソーシアム、標準化団体がある[14] が、IoT セキュリティに関する基準は整備段階であり、現時点では次のような基準がある。

(1) Security Guidance for Early Adopters of the Internet of Things

米国 Cloud Security Alliance（CSA）[15]

IoT 早期導入者向けのセキュリティの手引き書であり、IoT システムのセキュアな実装を目的としたセキュリティ対策を示している。

---

[13] サイバーセキュリティ経営ガイドライン：
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

[14] 添付 MRI 報告書「IoT 時代のデータ利活用と情報セキュリティ対策の調査」2.1 節全体動向⑤標準化を参照

[15] Cloud Security Alliance
https://cloudsecurityalliance.org/

(2) Security and Resilience of Smart Home Environments: Good practices and recommendations

欧州 European Network and Information Security Agency（ENISA）[16]

スマートホームに限定したセキュリティの実践方法と勧告文書であり、スマートホーム環境における、リモート攻撃の可能性と全体的なセキュリティへの取り組みの必要性を勧告している。

(3) IoT Trust Framework

米国 Online Trust Alliannce（OTA）[17]

IoT 製品及びサービスのセキュリティ、プライバシー、持続可能性に対応するためのトラストフレームワーク。スマートホームと接続された家庭用製品やウェアラブル製品について提案している。

(4) IEEE P2413 –Standard for an Architectural Framework[18]（策定中）

米国 IEEE STANDARDS ASSOCIATION

IEEE は「IEEE P2413 –Standard for an Architectural Framework」として、「共通要素間及び領域をまたがったレファレンスモデル」、「プライバシー、安全性を考慮したデータ取り扱い」などのフレームワークを策定している。

IoT の分野では、IoT の正式な定義はどこにもなく、それぞれの業界や組織が IoT についての定義を作ろうとしている。しかし、それでは接続性やセキュリティレベルが異なるものが出来てきて課題解決には至らない。そのため、IEEE では「マーケットの観点」を導入して、共通となる IoT の定義と、共通の課題の解決を図るために、フレームワークを策定している。

IEEE P2413 では、先ず８つのアプリケーション領域を定めて、その相互運用性、４つの信頼（防御、セキュリティ、プライバシー、セーフティ）、アーキテクチャとリファレンスモデルなどを検討している。IEEE P2413 がターゲットとしているアプリケーション領域は、ヘルスケア、ホーム＆ビルディング、小売、エネルギー、製造、運輸／交通、ロジスティックス、メディアの８領域である（順不同）。

[16] European Network and Information Security Agency
https://www.enisa.europa.eu/

[17] Online Trust Alliannce
https://otalliance.org/）

[18] Standard for an Architectural Framework for the Internet of Things (IoT)
http://grouper.ieee.org/groups/2413/

第5章　提言

本章では、IoT デバイスや IoT プラットフォームの提供を進めている組織、及びそれらの組織を支援するビジネスへの提言を記す。

IoT は急速に規模を拡大し普及し始めているが、IoT アーキテクチャにおける「生成レイヤー」に目を向けると、セキュリティに対する配慮が十分でない IoT デバイスが数多く存在することが懸念される。今後、IoT デバイスの相互接続を可能にするオープンプラットフォームの普及が進むにつれ、分野の異なる多様な機器がつながることでセキュリティレベルの差異から脆弱な部分が顕在化し、セキュリティレベルの低いエンドポイントが攻撃者に狙われることが予想される。

また、IoT デバイスの耐用年数の違いなどから新旧の機器が混在する状況が生まれ、そのことがセキュリティレベルの統一化を難しくしていくと共に、IoT デバイスの開発者、利用者、サービス運用者など責任範囲が不明確なことが、インシデント発生時の対応を困難にすることも予想される。このようなセキュリティレベルの不統一は IoT における大きな課題となると考えられる。

上記のような課題に対応し、IoT の普及を加速するためには、IoT デバイスへのセキュリティ機能の搭載のみならず、セキュリティレベルを維持管理することが重要になると共に、それらを評価・格付けする指標が必要になると考える。これまで、複合機をはじめとした各種 IT 製品の分野では、IT セキュリティ評価及び認証制度など、共通の表現で示された仕様によりセキュリティ機能を比較することを可能としていた[19]。IoT デバイスに対しても、IoT デバイスを活用する業界毎に、安全な機器が適切な状態でネットワークにつながるためのセキュリティ要件を定義して、機器のセキュリティレベルを評価・格付けする指標を定義することが必要であり、指標に基づき機器のセキュリティ評価や安全性の認証を行うためのルール/ガイドライン作りが求められる。

特に、重要なインフラの一部となる IoT デバイスについては、第三者評価・第三者認証の仕組みが整備されることが望まれる。しかしながら、IoT デバイスの数は膨大でありそのすべてに第三者評価・第三者認証の仕組みを使うことも現実的ではない。そこで、重要インフラの一部にならない一般的な IoT デバイスであれば、ガイドライン等で定められた指標に基づいて各社でチェックすることを可能とし、開発や運用のフェーズでもセキュリティ対策がタイムリーに実施できるようになることが望まれる。こうしたルールやガイドライン作りは、機器の製造開発を行う企業だけでなく、サービス提供者や業界団体、行政が連携し、官民一体となった取り組みが IoT の発展に不可欠である。

[19] IT セキュリティ評価及び認証制度
https://www.ipa.go.jp/security/jisec/scheme/index.html

また、IoT の効果的な利活用を促進する上で、「収集レイヤー」や「分析レイヤー」においては、パーソナルデータを安全に取扱う必要がある。このため、IoT システムの設計開発においては、従来の RFID システムや監視カメラなどにも利用されている「プライバシー・バイ・デザイン」[20] の手法などに基づき、プライバシー要件に基づいたシステムの設計開発を行い、IoT デバイスの認証、通信路暗号化、保持するプライバシー情報の選別や暗号化・匿名化などによりプライバシーデータの保護を図ると共に、利用者への安心感を高めることが重要になると考えられる。

また、それと同時に、プライバシーデータの取り扱いに関する法的側面からの要請に対応していくことも重要である。平成 27 年 4 月に成立した改正個人情報保護法では、個人情報と紐付く移動履歴、個人情報と紐付く購買履歴など、他の情報と照合することで容易に個人を識別できる情報も個人情報として取り扱われることになった。今後、様々な IoT デバイスが相互に接続するようになると、個々の IoT デバイスとしては個人情報とは紐付かない形で取得されたセンサデータであったとしても、他の IoT デバイスとの接続により容易に個人情報と紐付けることが可能となる場合は、個人情報としての取り扱いが必要となる可能性がある。また、同法では、特定の個人を識別することができないように加工した匿名加工情報を第三者に公表する際には、個人情報保護委員会に届け出ることが義務付けられている。このため IoT プラットフォームの提供者などが、IoT デバイスを通じて得られた個人情報を匿名加工化して第三者に提供するような場合は、このような点への配慮も必要になると考えられる。

[20] Privacy by design.
https://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/

おわりに

本報告書では、IoT の利活用に関して動向や利用者の意識調査を行い、IoT システムの開発・構築・運用の際に留意するべきルール作りと、プライバシー保護の必要性について提言を行った。

IoT により「モノ」をネットワークに接続し、「モノ」のデータを集めたり、「モノ」の動作を制御したりすることによって、新しい価値を創造できる可能性がある。しかし、これまでネットワークに接続することを前提として作られてこなかった「モノ」が多いうえ、「モノ」の制御を悪意を持った第三者に乗っ取られた場合には、第三者による物理的な攻撃を可能としてしまう可能性があるため、ネットワーク接続する「モノ」に対するセキュリティ対策が重要であることが分かった。また、「モノ」から集めたデータの所有権の考え方や、「モノ」が利用者個人に属するものである場合には、データに含まれる利用者のプライバシー保護の考え方、データを収集した組織でのデータ利活用の考え方についての整理が必要なことが分かった。

今後、IoT が普及していくためには、これら課題を克服したうえで、データの利活用について、データを収集する組織と利用者の間の共通コンセンサスの醸成が必要と考える。

本報告書が IoT による新たな価値の創造を目指す組織に活用されることを期待する。

ー 禁無断転載 ー

本報告書に掲載されている会社名および製品名は、各社の登録商標または商標です。注記がない場合もこれを十分尊重します。

平成 27 年度情報セキュリティ調査報告書
ーIoT 時代のデータ利活用と情報セキュリティ対策に関する調査ー

発　行　日　　平成28年3月
編集・発行　　一般社団法人 電子情報技術産業協会
　　インダストリ・システム部
　　〒100-0004　東京都千代田区大手町1丁目1番3号
　　大手センタービル
　　TEL　(03)5218-1057
印　　刷　　株式会社 オガタ印刷