JEITA

情産－17－技標－３

平成28年度情報セキュリティ調査報告書

－IoT社会の将来像とセキュリティリスクに関する調査－

平成２９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

本調査報告書は、情報セキュリティ調査専門委員会が、「IoT（Internet of Things）社会の将来像とセキュリティリスク」に関する調査のため、IoT の市場動向や活用事例、そして IoT 政策動向の調査・整理、IoT ビジネスを展開する企業に対するデータ利活用・流通・セキュリティに関するアンケートを実施し、今後の IoT 社会の将来像を検討し、IoT 社会の実現に向けたセキュリティリスク等の課題を分析し、課題解決のための提言を報告するものである。

近年、IT 関連機器以外の機器のインターネットへの接続する IoT や、機器同士の通信 M2M（Machine to Machine）が増加し、これを活用したビジネスが国内外で登場している。IoT 社会は実世界とサイバー空間とが相互に連携した社会であり、パソコンやスマートフォンといった端末にとどまらず、自動車や生活空間にある家電やセンサーなど多くの機器がインターネットに接続されるようになってきた。これらの機器から収集されたデータ（IoT データ）を分析し有効活用することで、社会的な課題である少子高齢化、生産性向上、エネルギー問題などの解決につながっていくと考えられる。多様な IoT データには、個人情報やプライバシー情報、営業秘密情報などが含まれることが多いため、サイバー攻撃が常態化している昨今は、IoT データの活用範囲や取扱い方法においてリスクを考慮した対策を施すことが必要である。IoT では多くの機器や関係者がつながる可能性が増えている。このため、機器やシステムそしてサービスが、他のシステムやサービスともつながることを前提としたセキュリティ機能を検討することが望まれる。

本年度の活動として当専門委員会は、国内外で数多くの取組が進められている IoT について、国内外企業や自治体の取組や政策を整理し、IoT 社会の将来像を検討し、検討した将来像を基に、IoT 社会の実現に向けたセキュリティリスク等の課題を検討し、JEITA 会員企業のビジネスや事業戦略の策定に役立ててもらうことを目的として調査した。その結果を報告書として取りまとめた。

本調査報告書の作成にあたり、視察およびヒアリングにご協力いただいた企業・自治体や有識者の方々、そして当専門委員会の関係の皆様に深く感謝の意を表すとともに、本報告書が関係の方々に活用され、今後のセキュリティビジネスのさらなる発展に寄与できれば幸いである。

2017 年 3 月

情報セキュリティ調査専門委員会
福島　孝文

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	福島 孝文	東芝テック（株）
副委員長	佐藤 淳	（株）リコー
委員	水島 九十九	日本電気（株）
〃	對馬 孝高	（株）日立製作所
〃	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）
〃	坂上 勉	三菱電機（株）
〃	平木 博史	（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
〃	綿谷 謙吾	（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　社会動向

1.1 IoT の市場動向

IoT の市場動向については、様々な企業・調査会社から予測が提供されている。CISCO は、インターネットに接続されるモノの数について、2013 年の 100 億個から 2020 年には、500 億個に増加すると予測している（図 1-1）。Gartner は、インターネットに接続される機器の数について、「一般消費者向け製品」「産業分野」「自動車分野」に分類した予測を提供している。その予測によると特に自動車分野での伸びが顕著で、2014 年から 2020 年にかけて 18.5 倍になると推定している（図 1-2）。

IoT を活用する世界の市場規模については、IDC が、2014 年の 6,558 億ドルから 2020 年には 1 兆 7,000 億ドルに拡大（年平均成長率：16.9%）すると予測している。日本国内の市場規模については、IDC Japan が、2015 年の 6 兆 2,332 億円（見込み値）から、2020 年に 13.8 兆円に拡大（年平均成長率：16.9%）すると予測している。（図 1-3）

いずれの予測においても、インターネットに接続される機器やそれに関連する市場については、今後大きく拡大していくものとなっている。

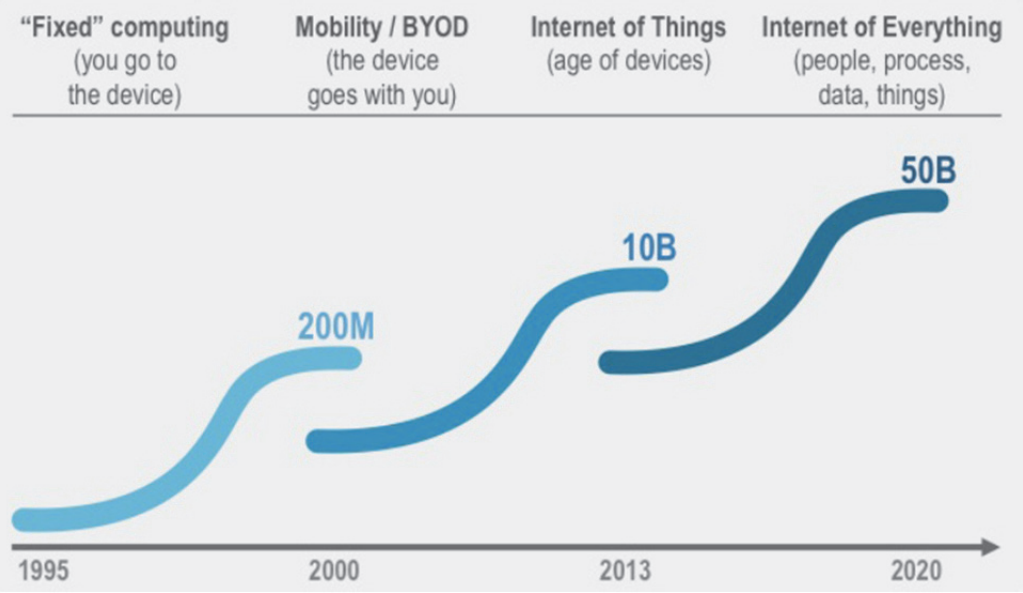

図 1-1　インターネットに接続されるモノの数[1)]

[1)] Cisco Systems, Inc, "Embracing the Internet of Everything To Capture Your Share of $14.4 Trilion", (http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf)

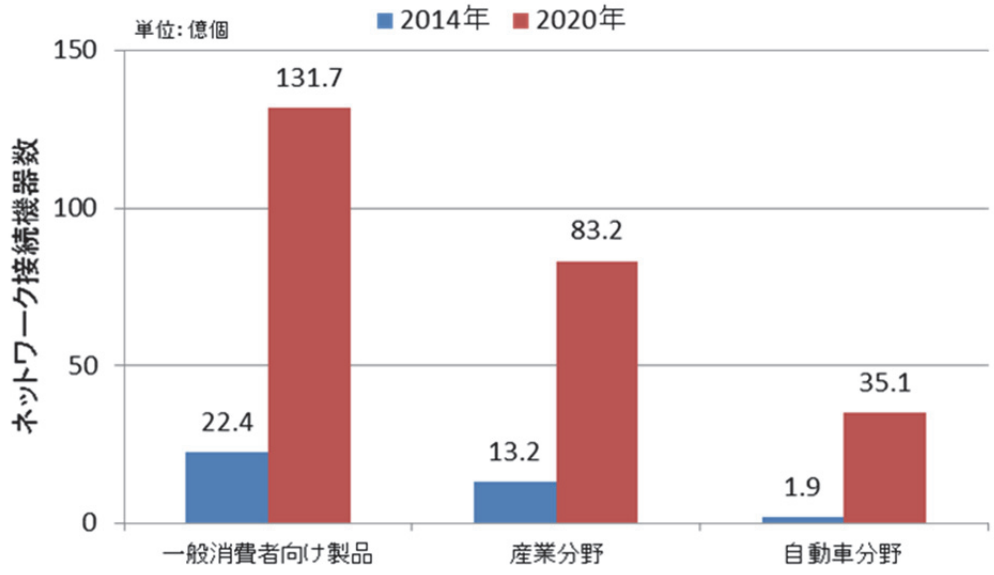

図 1-2　分野別インターネットに接続されるモノの数[2)]

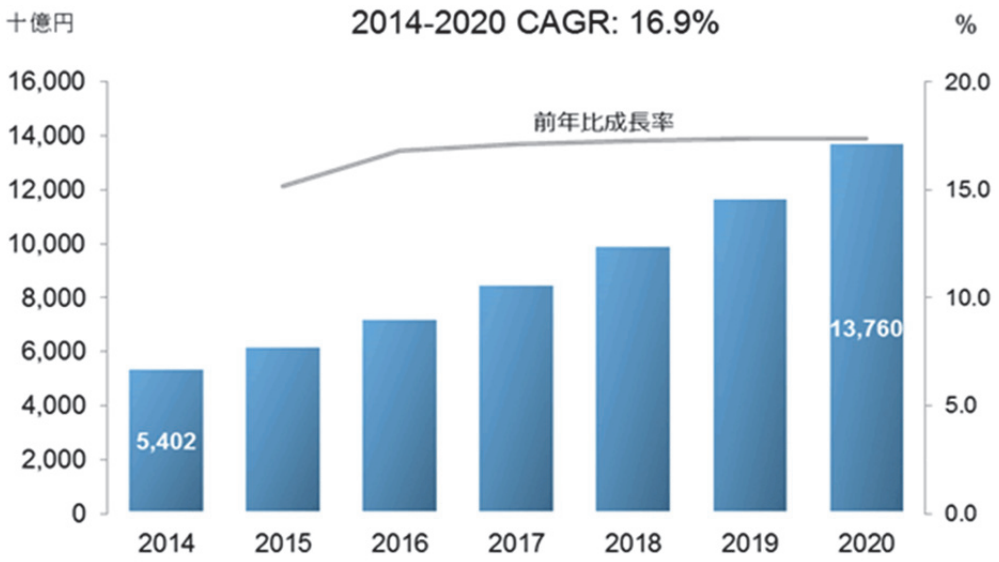

図 1-3　国内 IoT 市場 支出額予測： 2014 年～2020 年[3)]

[2)] Gartner Inc, “Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015”を基にグラフを作成, (http://www.gartner.com/newsroom/id/2905717)
[3)] IDC Japan 株式会社, “国内 IoT 市場 ユースケース（用途）別／産業分野別予測を発表”, (http://www.idcjapan.co.jp/Press/Current/20160223Apr.html)

1.2 IoT の利活用事例

将来的に大きく拡大していくことが見込まれている IoT の利活用であるが、現在様々な分野で個別の取組が進められている。本項では、自治体における取組として、豊田市エコフルタウンと民間企業の取組としてエブリセンスの事例を紹介する。

1.2.1 自治体の取組「とよたエコフルタウン」

「とよたエコフルタウン」は、愛知県豊田市が推進するスマートシティプロジェクトである。同市は、平成 21 年に「環境モデル都市」として国からの指定を受け、「ハイブリッドシティ」をキーワードとして、「民生」「交通」「森林」「産業」「都心」の 5 分野を中心にした取組を進めている。エコフルタウンでは、スマートハウスや ITS、植物工場などの ICT を活用した展示を行っており、主に環境面に着目した取組が進められている。都市機能を集約するコンパクトシティではなく、現在住んでいる所で、いかに利便性を高めて住んでもらうかを目標としている。また、取得する情報の利活用について、これまでは交通情報や電気利用情報が中心であったが、住民からの同意を得た上で、交通情報の見守りへの活用や電気利用情報と健康情報の連携など、ヘルスケア情報なども加えた形での分野を横断した取組も検討されている。

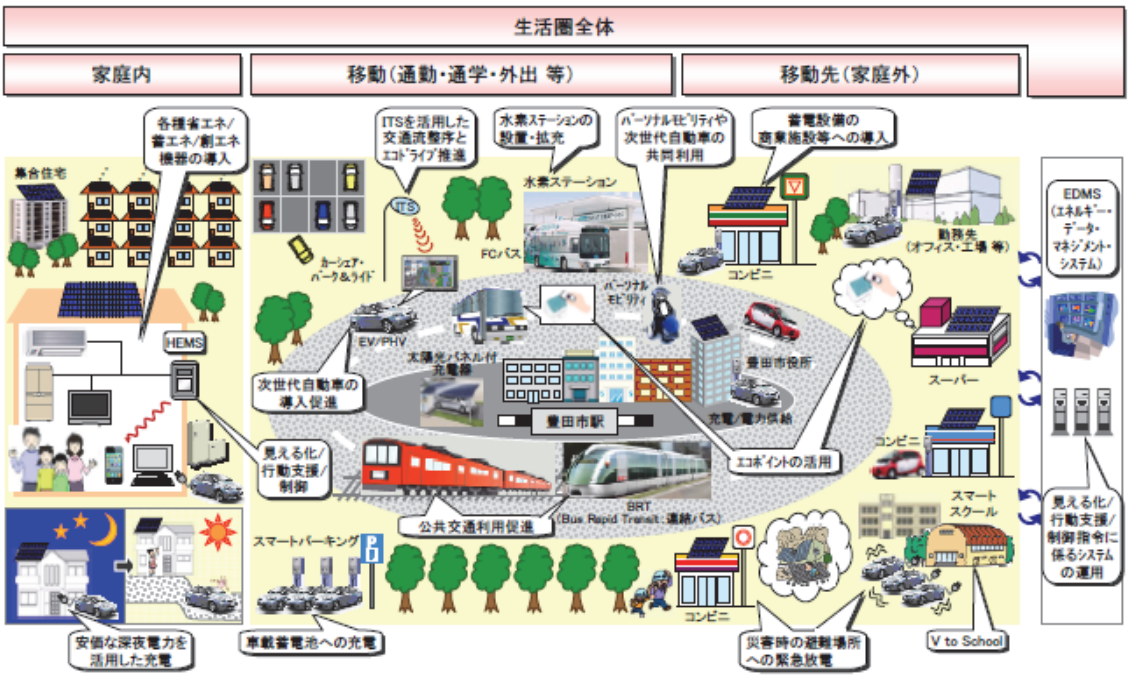

図 1-4　実証が目指す低炭素なまちのイメージ[4)]

4) 経済産業省，“愛知県豊田市における「家庭・コミュニティ型」低炭素都市構築実証プロジェクトマスタープラン”，（http://www.meti.go.jp/committee/summary/0004633/masterplan002.pdf）

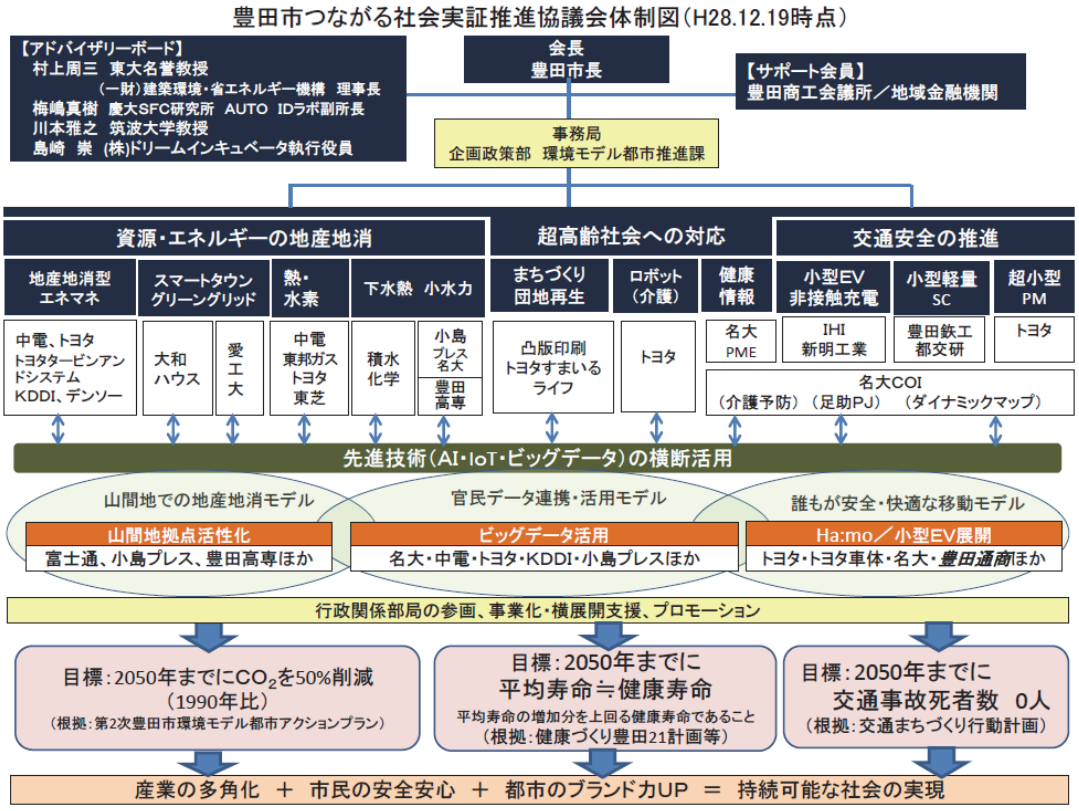

図 1-5　豊田市つながる社会実証推進協議会体制図[5)]

1.2.2 民間企業の取組「EverySense」

エブリセンスジャパン株式会社が提供するサービス「EverySense」は、IoT 情報を流通させるためのプラットフォームである。情報提供者の IoT 機器が持つデータとそのデータを利用して新規事業や新しいサービスの開発に取り組む企業などが求めるデータをマッチングさせ、データの売買を仲介するサービスである。

情報を収集したい企業などは、条件を設定し入手したいデータをリクエストする。情報提供者は、その条件を確認し、データ提供の可否、データが利用される範囲、匿名か実名かなどを決定する。情報提供者は、提供するデータの質と量によって、対価（ポイント）を得ることができる。

「EverySense」のサービスは、データを仲介するプラットフォームの提供のみに専念し、データの売買や保持は行わず、価格決定権も持たない。サービスの概要を図 1-6 に示す。

5) 豊田市報道発表資料（2017 年 3 月）“豊田市つながる社会実証協議会が、県内市町村で初めて「地方版 IoT 推進ラボ」に選定されました”　（http://www.city.toyota.aichi.jp/pressrelease/201703/1018183.html）

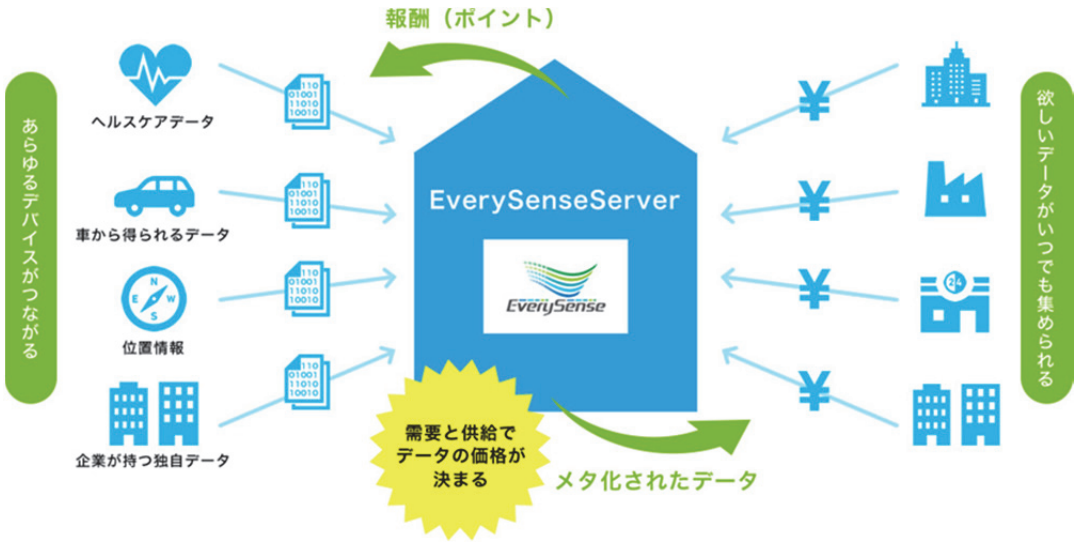

図 1-6　IoT プラットフォームサービス「EverySense」[6)]

1.3 IoT の政策動向

国内外ともに IoT を、今後の政策・産業の重点分野と位置付け、国を挙げた取組を進めている。本項では、国内の取組として IoT 推進コンソーシアム、海外の取組としてドイツの Industrie4.0 を紹介する。

1.3.1 IoT 推進コンソーシアム

2015 年に、産官学が参画・連携し、IoT 推進に関する技術の開発・実証や新たなビジネスモデルの創出・推進のための体制構築を目的として、総務省と経済産業省の協力の下、「IoT 推進コンソーシアム」が設立された。フォーラムの法人会員数は、2,812 社（2017 年 1 月 31 日現在）となっている。IoT 推進コンソーシアムの推進体制を図 1-7 に示す。

コンソーシアムでは、IoT に関する技術の開発・実証および標準化等の推進、IoT に関する各種プロジェクトの創出および当該プロジェクトの実施に必要となる規制改革等の提言等を推進するとしている。

ワーキンググループとして、技術開発 WG（スマート IoT 推進フォーラム）・先進的モデル事業推進 WG（IoT 推進ラボ）・IoT セキュリティ WG・データ流通促進 WG が設置されており、Iot セキュリティ WG からは、2016 年 7 月に「IoT セキュリティガイドライン ver.1.0」が提供されている。IoT セキュリティガイドラインについては、1.4.1 にて後述する。

[6)] EcerySense, Inc, “IoT プラットフォームサービス「EvurySense」”,
（https://every-sense.com/services/everysense/）

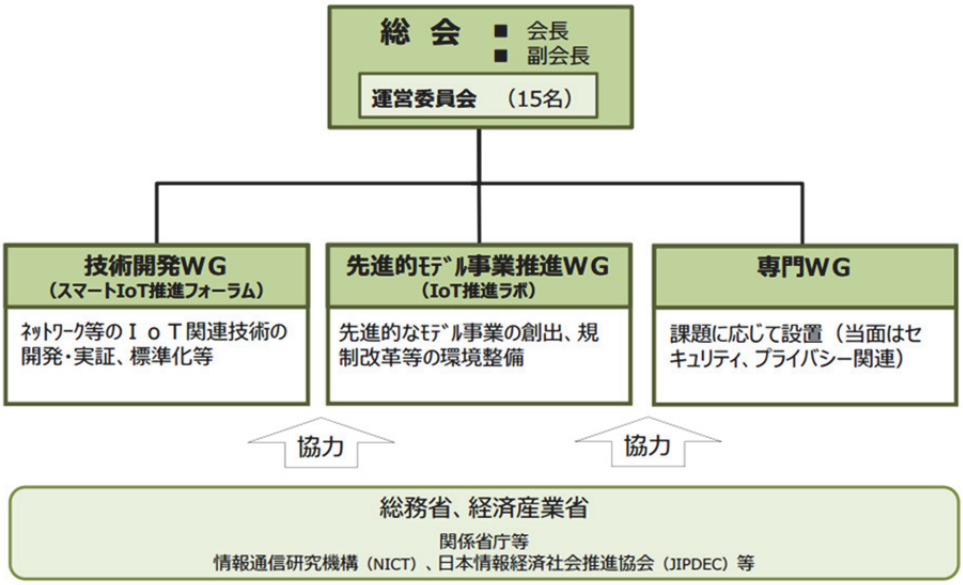

図 1-7　IoT 推進コンソーシアム体制図[7)]

1.3.2 Industrie 4.0

ドイツでは、「Industrie4.0 戦略」が進められている。官民が連携した活動で、製造業の IoT 化を通じ、産業機械・設備や生産プロセス自体をネットワーク化し、注文から出荷までをリアルタイムで管理することでバリューチェーンを結ぶ「第 4 次産業革命」の実装を目指している。この活動には、ドイツ機械業界主要 3 団体を始め、Bosch・Siemens・Deutsche Telekom・Volkswagen 等の多くの企業や大学機関が参加している。

組織の運営については、「運営委員会（Steering Committee）」が中心となって全体的な運営を担い、戦略の決定や下部組織であるワーキンググループの設立およびその作業の進捗確認を行う。「理事会（Governing Board）」は、運営委員会メンバー企業の代表者により構成され、戦略的アドバイスや政策担当者・メディア等との調整を実施する。また、「科学諮問委員会（Scientific Advisory Committee）」では、製造や IT 等の関連する技術分野の大学教授や技術分野の専門家がメンバーとなり、科学的観点からアドバイスを行っている。推進体制を図 1-8 に示す。

7) IoT 推進コンソーシアム，（http://www.iotac.jp/）

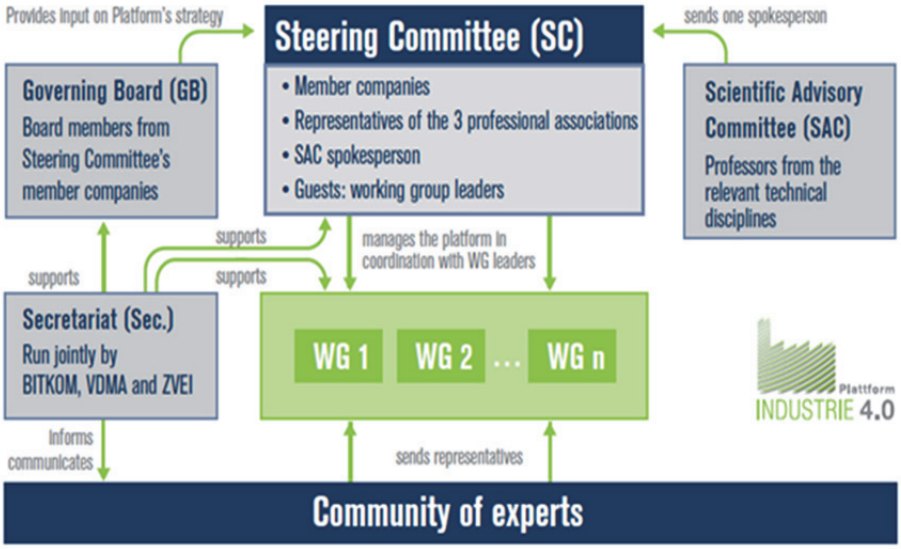

図 1-8 “Industry 4.0” プラットフォームの暫定組織図[8)]

1.4 IoT セキュリティに関するガイドライン

IoT セキュリティに関し、国内外でガイドラインが提供されている。主なガイドラインを表 1-1 に示す。これらガイドラインが提供されることで、トラブルが発生し、民事で紛争になった場合、ガイドラインに準拠していないと過失が指摘される可能性が出てくることも考えられる。本項では、国内のガイドラインとして、「IoT セキュリティガイドライン」と「IoT 開発におけるセキュリティ設計の手引き」、海外のガイドラインとして、「IoT Security Guidance」を紹介する。

表 1-1 主な IoT セキュリティに関するガイドライン

ガイドライン名	発行団体（発行年）	概要
IoT セキュリティガイドライン	IoT 推進コンソーシアム・総務省・経済産業省（2016 年 7 月）	・IoT 機器やシステム、サービスに提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）の各段階における指針を示したもの ・一般利用者が IoT 機器等を利用する際のルールも示している
IoT 開発におけるセキュリティ設計の手引き	情報処理推進機構（IPA）（2016 年 5 月）	・今後の IoT の普及に備え、IoT 機器およびその使用環境で想定されるセキュリティ脅威と対策を整理したもの ・対策例として、デジタルテレビ・ヘルスケア機器・クラウドサービス・スマートハウス・コネクテッドカーの分野について解説

8) acatech, “Recommendations for implementing the strategic initiative INDUSTRIE 4.0”, (http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf)

ガイドライン名	発行団体（発行年）	概要
コンシューマ向け IoT セキュリティガイド	日本ネットワークセキュリティ協会（JNSA）（2016 年 6 月）	・JNSA IoT Security WG が作成したガイド。単にユーザが利便性を得るだけではなく、無用のサイバーセキュリティリスクにさらされることのない製品やサービスを提供するために作り手が考慮すべき事柄をまとめたもの。
IoT Security Guidance	Open Web Application Security Project(OWASP)（最終更新は 2016 年 5 月）	・IoT 製品開発者・アプリ開発者・利用者別のガイダンス ・IoT セキュリティに関する 10 の項目別に、考慮すべき事項・推奨事項をまとめている
IoT Trust Framework	Online Trust Alliance (OTA)（2016 年 7 月）	・データセキュリティやプライバシー関連事業を実施する非営利団体である OTA が策定した IoT に関するフレームワーク ・プライバシー・セキュリティ・持続性に関する要求事項として 31 原則を提示
Framework for Cyber-Physical Systems (CPS) Release 1.0	National Institute of Standards and Technology (NIST)（2016 年 5 月）	・NIST の CPS Public Working Group がまとめた CPS に関するフレームワーク ・CPS の開発段階で考慮すべき 3 つの Facet とシステムに関連するステークホルダーが考慮すべき 7 つの Aspects で整理

1.4.1 IoT セキュリィティガイドライン

IoT セキュリティガイドラインは、IoT 機器やシステム、サービスに提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針、一般利用者が IoT 機器等を利用する際のルールを示したものである。

セキュリティ確保の観点から求められる基本的な取組を、セキュリティ・バイ・デザインを基本原則とし、明確化することにより、産業界における積極的な開発等の取組を促し、利用者が安心して IoT 機器やシステム、サービスを利用できる環境を生み出すことを目的としている。ガイドラインに示されている要点を表 1-2 に示す。

表 1-2　セキュリティ対策指針一覧[9)]

大項目	指針	要点
方針	IoT の性質を考慮した基本方針を定める	経営者が IoT セキュリティにコミットする
		内部不正やミスに備える
分析	IoT のリスクを認識する	守るべきものを特定する
		つながることによるリスクを想定する
		つながりで波及するリスクを想定する
		物理的なリスクを認識する
		過去の事例に学ぶ
設計	守るべきものを守る設計を考える	個々でも全体でも守れる設計をする
		つながる相手に迷惑をかけない設計をする
		安全安心を実現する設計の整合性をとる
		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
		安全安心を実現する設計の検証・評価を行う
構築・接続	ネットワーク上での対策を考える	機器等がどのような状態かを把握し、記録する機能を設ける
		機能および用途に応じて適切にネットワーク接続する
		初期設定に留意する
		認証機能を導入する
運用・保守	安全安心な状態を維持し、情報発信・共有を行う	出荷・リリース後も安全安心な状態を維持する
		出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える
		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
		IoT システム・サービスにおける関係者の役割を認識する
		脆弱な機器を把握し、適切に注意喚起を行う

1.4.2 IoT 開発におけるセキュリティ設計の手引き

情報処理推進機構から公開されている「IoT 開発におけるセキュリティ設計の手引き」は、IoT のセキュリティ設計を担当する開発者向けに、今後の IoT の普及に備え、IoT 機器およびその使用環境で想定されるセキュリティ脅威と対策を整理したものである。2016 年 3 月に IPA ソフトウェア高信頼化センターから公開された「つながる世界の開発指針[10)]」に対する、具体的なセキュリティ設計と実装を実現するための手引書として位置付けられる。IoT システムにおける具体的な脅威分析や対策検討の実施例として、デジタルテレビ・ヘルスケア機器・クラウドサービス・スマートハウス・コネクテッドカーの分野別に紹介している。手引きにおいてモデル化された IoT の全体像を図 1-9 に示す。

9) IoT 推進コンソーシアム，“IoT セキュリティガイドライン ver.1.0”,
（http://www.iotac.jp/wp-content/uploads/2016/01/03-IoT セキュリティガイドライン ver1.0 別紙 1 .pdf）

10) 情報処理推進機構，“「つながる世界の開発指針」を公開”,
（https://www.ipa.go.jp/sec/reports/20160324.html）

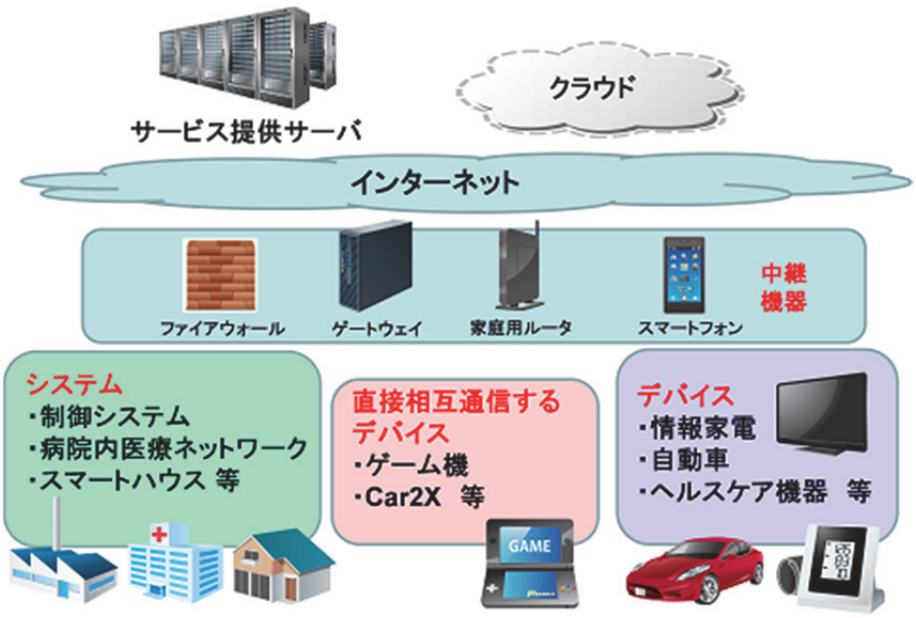

図 1-9 「IoT 開発におけるセキュリティ設計の手引き」の IoT 全体像[11)]

1.4.3 OWASP IoT Security Guidance

OWASP IoT Security Guidance は、OWASP Internet of Things (IoT) Project の一環で作成されたガイダンスである。同プロジェクトは、IoT 製品の開発者や IoT に関連したアプリケーション開発者および利用者が、安全な IoT 製品を開発・構築・利用できることを目的として、活動を進めている。ガイダンスにおいて示されている IoT セキュリティの考慮事項を表 1-3 に示す。

11) 情報処理推進機構, “IoT 開発におけるセキュリティ設計の手引き”, (https://www.ipa.go.jp/files/000052459.pdf)

表 1-3　IoT セキュリティの考慮事項[12)]

分類	IoT セキュリティの考慮事項(一部抜粋)
安全ではない Web インタフェース	・弱いパスワードの設定を許可しない、アカウントのロックアウトメカニズムの導入 ・XSS や SQL インジェクション等の脆弱性対策
不十分な認可/認証	・ユーザの権限の適切な設定（マルチユーザ環境の場合） ・二要素認証の導入（可能であれば）
安全ではないネットワークサービス	・必要最小限のネットワークポートのみをアクティブにする ・バッファオーバーフローや DoS 攻撃等の脆弱性がないか確認
伝送経路の暗号化の欠如	・システム間、ネットワーク間等のデータ伝送は暗号化する ・SSL/TLS の実装は適宜更新し、適切な設定をする
プライバシー	・利用者からの個人情報の収集は必要最小限とする ・認可された個人のみが個人情報にアクセスできるようにする
安全ではないクラウドインターフェース	・クラウドインターフェースにセキュリティ上の脆弱性が存在しないか確認する ・弱いパスワードの設定を許可しない、アカウントのロックアウトメカニズムの導入
安全ではないモバイルインタフェース	・弱いパスワードの設定を許可しない、アカウントのロックアウトメカニズムの導入 ・二要素認証を実装する
不十分なセキュリティ設定	・パスワードの使用可能文字、最低文字数等を設定する ・セキュリティイベント発生時に利用者にアラートが届く設定とする
安全ではないソフトウェア/ファームウェア	・脆弱性が明らかになった場合は迅速にアップデートする ・アップデートファイルは暗号化し、ファイル転送時も暗号化する
貧弱な物理セキュリティ	・物理的な外部のポート（USB ポート等）は必要最低限な数とする ・製品は耐タンパー性を満たすこと

[12)] OWASP, “Manufacturer IoT Security Guidance”をもとに作成,
（https://www.owasp.org/index.php/IoT_Security_Guidance）

第2章　IoT に関連する法制度

第 4 次産業革命により IoT や AI に関する市場は、世界規模で大きく拡大すると考えられている。特に IoT 関連のデータではその取り扱いが重要となり、大きな可能性が期待されているのと同時に、個人情報保護法やプライバシーへの配慮が必要となってくる。社会的に受容される仕組みにおいて、消費者の信頼を得てデータを利活用することにより、中長期的に新しいイノベーションが促進されると考えられている。このような取り巻く社会環境変化において、IoT に関連する法制度を以下に概観する。

2.1 グローバルでの個人データ法制の動向

急速な ICT 技術の進歩やグローバル化の進展に伴い、個人の権利利益を侵害するリスクの拡大が懸念されている。IoT デバイスについては、センサー等から消費者が把握していない形で勝手に個人情報が収集され、利用される危険性が指摘されている。欧米を中心に IoT のデータ保護に関する議論がなされており、EU、OECD、欧州評議会、米国などで、世界的にデータ保護制度の見直しが進められている。

2.1.1 日本の改正個人情報保護法

個人情報保護法は平成 15 年に制定され（平成 17 年に全面施行)、その後 10 年余りが経過し消費者や事業者を取り巻く環境が大きく変化してきている。

(1)個人情報を含むビッグデータにおいて、適正な利活用をするための環境整備が必須

(2)個人情報かどうかの判断が困難ないわゆる「グレーゾーン」が拡大

(3)事業活動が国際化し、国境を越えて多くの個人情報が流通

これらの環境変化に対応するため、消費者の個人情報の保護を図りつつ円滑な利活用を促進させ新事業等を創出することを目的として、平成 27 年 9 月に個人情報保護法が改正された。個人情報保護法の改正の主なポイントは下記の通りである。

(1)個人情報保護委員会の新設

・個人情報の保護に関する独立機関として、個人情報保護委員会を新設。現行の主務大臣の有する権限を個人情報保護委員会に集約し、立入検査の権限等を追加。

(2)個人情報の定義の明確化

・特定の個人の身体的特徴をデータ変換した情報を、個人識別符号として新設。

・要配慮個人情報を新設し、人種・信条・病歴等が含まれる個人情報については、本人同意を得て取得することを原則義務化し、本人の同意を得ない第三者提供を禁止。

(3)適切な規律の下で個人情報等の有用性を確保

・匿名加工情報として、特定の個人を識別することができないように個人情報を加工したものを匿名加工情報とし新設。その加工方法および事業者による公表等の規律を規定。

(4)適正な個人情報の流通を確保

・事業者はオプトアウト手続によって個人データを第三者に提供する際、データの項目等を個人情報保護委員会へ届出を行う。また、個人情報保護委員会はその内容を公表。

・個人データを提供した事業者は、受領者の氏名等の記録を保存することを義務化。

・個人情報データベース等不正提供罪として、データ盗用行為を処罰する規定を新設。

(5)個人情報の取扱いのグローバル化対応

・日本に居住する本人から個人情報を直接取得した外国の事業者についても個人情報保護法を原則適用。

・外国事業者への第三者提供では、個人情報保護委員会が規定する方法以外は原則不可。

(6)その他の改正事項

・小規模取扱事業者（5000 人分以下の個人情報を取り扱う事業者）も新たに対象者。

・開示等請求権として、本人の開示、訂正、利用停止等の求めも請求権であると明確化。

次に、IoT と改正個人情報保護法の関係において課題を考察する。以下のような課題があると考えられる。

(1)本人関与の明確化（第三者提供における同意等）

IoT デバイスが個人情報を取得している場合には、その概要を明らかにし消費者が理解できるようことが必要となる。個人情報保護法においては、①外国にある第三者への提供（第 24 条)、②トレーサビリティ義務（第 25 条・26 条）が義務化される。どのように本人が関与していることを周知するかが大きな課題となっている。

(2)利用目的の明確化

個人情報保護法においては、利用目的に関して可能な限り特定し（15 条)、②利用目的の範囲で取り扱い（16 条)、利用目的を通知、公表する（18 条）ことが義務化されている。通知、公表の方法は、個人情報取扱事業者が選択することなる。個人情報取扱事業者は事業内容等に合わせて、消費者が常識的な努力の範囲内でそれを知ることができるように適切な方法で通知、公表する。カメラ等の IoT デバイスではどのように通知、公表すれば良いかが大きな課題となっている。

また、解決策としては下記のような内容が考えられる。

(1)「個人情報を取得していない」と認められる範囲を規定する。カメラにて顔画像を取得する際に、一時的に取得して直ぐに廃棄する際には短時間であれば個人情報を取得していないと容認する等を明確化する。

(2)「取得の状況からみて利用目的が明らか」であることを規定化する。監視カメラによる窃盗防止からどこまで拡大できるかが重要となる。

(3)IoT のサービス提供者が限定されれば，本人による情報コントロールが容易になる。

2.1.2 ＥＵの一般データ保護規則（GDPR）他

2016 年 4 月、EU は「EU 一般データ保護規則」、GDPR（General Data Protection Regulation）を制定した。GDPR は 2018 年 5 月 25 日に施行される予定であり、個人データを収集し処理を行う事業者に多くの義務を課せている。また、個人データの収集処理についての説明責任を要求しており、事業者は GDPR に遵守した個人データの保管と運用が求められる。事業者がこれらの義務に違反した場合には、最大で 2,000 万ユーロまたは前年度の全世界売上の 4%のいずれか高い方が制裁金として課せられ、事業に重大な影響を及ぼすリスクが生じる。日本企業には必要に応じて下記の対応が求められることになる。

(1)処理対象の個人データおよびその処理プロセスを特定し､適切な安全管理措置を実施
(2)EU 域外へのデータ移転にあたり、適切な方法を選択し確実なる運用を実施
(3)インシデントが発生した際は、データ主体および監督機関に通知
(4)データ保護責任者（Data Protection Officer）を選任
(5)データ保護影響評価（DPIA）を実施し、必要に応じて監督機関への報告　等

次に、IoT と EU の GDPR の関係において、課題は以下の通りと考えられる。

(1)セキュリティ違反

IoT デバイスはセキュリティ侵害の影響を受けやすい。GDPR では個人データ漏洩の場合、事業者は GDPR の要件に従いリスクを特定し対処することが求められる。

(2)本人同意

GDPR はデータ主体の同意を要件としている｡そのためデータ主体の積極的な同意が得られない場合などでは、事業者は自由にパーソナルデータを利用することができない。

(3)プライバシー・バイ・デザイン等

技術的・組織的な安全管理措置として Privacy by Design 等が規定された。また、データ保護に多大な影響を及ぼす可能性がある場合には、データ保護影響評価（DPIA）を実施することが規定されている。

(4)データ権利の強化

GDPR は個人データについて、データ主体に新しい実質的な権利を付与され、忘れられる権利の明示、データ可搬性の権利、自動意思決定に反対する権利が含まれる。特にデータの移植性に関して IoT デバイス等のシステムの設計において､GDPR に準拠したデータ主体の権利行使を容易にするための機能が要求される。

(5)プロファイリング

IoT デバイスを通じて蓄積された個人データは、個人の嗜好や政治的傾向、事故や犯罪の可能性、特定の疾患リスクなどについて、相当程度高い精度での推測が可能になる。個人データの管理者や処理者は、個人の尊厳や自由などに十分配慮したシステムなどの設計と運用が要求される。

また、包括的なサイバーセキュリティに関する EU 指令（ネットワークおよび情報システム指令）である「NIS 指令」が 2016 年 8 月に施行された。これは、重要インフラ提供者だけでなく、クラウドサービス等のデジタルサービス提供者にも、セキュリティ上の義務が課されるというものである。NIS 指令と一般データ保護規則（GDPR）の違いは、NIS 指令がすべてのデータを対象とするのに対して、GDPR では個人データに限定されるということである。NIS 指令はデータ取扱いの違反行為だけでなく、セキュリティやサービスの提供に影響があるインシデントも対象となる。日本企業が EU 域内で重要インフラサービス等を提供している際には、サイバーセキュリティ上の義務を負う可能性があり適切な対応が必要となる。

2.1.3 米国のプライバシー保護法制

米国には、いわゆる個人情報保護法のような包括的に個人情報を保護する法律がない。全体としては自主規制をもとに、規制する必要性が高い分野について分野ごとに個別法を定めて規制している。例えば、迷惑メール（スパム・メール）防止法や児童オンライン・プライバシー保護法などである。

米国では、個人情報を取り扱う企業が自ら個人情報をどのように取り扱うのかをプライバシーポリシーなどで公表する。このプライバシーポリシーは、基本的には各企業が自由に規定することになる。そして、企業が自ら公表しているプライバシーポリシーに反して運用をした場合には、連邦取引委員会（FTC）法 5 条の「不公正・欺瞞的行為または慣行」に該当するとして、FTC から課徴金を課されるなどのペナルティを受ける可能性がある。

次に、IoT と米国のプライバシー保護法制の関係は下記の通りである。

2015 年 1 月、FTC は IoT のプライバシーとセキュリティに関するレポートを公表した。この中で IoT 関連の企業に対して、セキュリティとプライバシーへ取り組むように強く要請し対応策について指針を示している。

・セキュリティは後付けするのではなく、当初よりデバイスに組み込むべき
・製品ライフサイクルの終了まで、IoT デバイスの監視と修正パッチを提供すべき
・権限のないユーザは、ネットワーク上に保存された個人情報にアクセス不可
・委託先企業等がどのように個人情報を扱っているかを把握すべき

また、同レポートでは、企業はどの情報をどのような目的で収集するのかを消費者に知らせるべきであり、また、消費者は企業による情報の収集を拒否する機会が与えられるべきであると記載している。さらに、企業に対して収集するデータを制限すること、一定期間が経過すればデータを廃棄すること等が勧告されている。

2.2 その他 グローバルな潮流

IoT やビッグデータの利活用においては、データが生み出す利便性とプライバシー侵害のバランスをどのように取るかという点が大きな課題となっている。IoT は社会全体から様々な情報を集め、ビッグデータを利用し様々な分析を行うことができるが、ビッグデータに個人情報が含まれている場合にはプライバシー侵害のリスクを高めることになる。

2014 年 10 月に開催された個人情報保護に関する監視機関や専門家が集まる国際会議「第 36 回 データ保護プライバシー・コミッショナー国際会議」では、IoT とビッグデータの利用により起こりうるプライバシー侵害のリスクが議論のメインテーマとなった。そして、IoT とビッグデータに関する宣言と決議が採択された。これらの技術が個人の自由意思を脅かす可能性と合わせて、インターネット接続された機器から収集されたデータには個人情報が含まれ、データ転送されるリスクについて述べられている。また、ビッグデータによるプライバシー侵害を防ぐため、事業者はデータ保護原則を守るべきと記載されている。

公表された「IoT におけるモーリシャス宣言」では、以下のような提言がなされている。

・IoT デバイスから収取されたデータには、個人情報が含まれることを認識すべき
・消費者が IoT デバイスを利用する際、情報の取扱い方法を十分理解できるようにすべき
・プライバシーは設計時点から配慮されるべきである（Privacy by Design）
・データ処理をデバイス内で行うことがセキュリティリスクの低減につながる
・IoT の価値はデバイスだけでなく、データから提供されるサービスにも影響を与える

2.3 国境を越えるデータやサービス提供

企業の活動がグローバル化していく中、母国以外で事業展開され様々なビジネスが経済活動や社会活動に重大な影響を及ぼす機会が増加している。国境を越えて行われるデジタルコンテンツのやり取りなどデータ関連サービスの課題が議論されている。

外国からの越境サービスに対する各国法の域外適用について、また、国際的な執行協力について、グローバルな見地から積極的に議論や検討がなされる必要がある。域外適用による執行のためには、外国の執行当局との執行協力が必要となり、執行協力を実効的に行うには、根拠規定（条約、経済連携協定等の国際協定など）が必要になる。また、執行協力が円滑に行われ実効的な執行を担保するためには、外国当局との情報の相互提供が重要である。そのための根拠規定の整備も必要になり、各国法の域外適用により管轄権が重複や抵触しうることにも考慮し、国際的ハーモナイゼーションに向けて取り組むべきと考える。

2.4 データオーナーシップに関わる法的課題

IoT やビッグデータの利活用を進める上での大きな課題に「データのオーナーシップ」がある。データの保有権を持つデータ主体は、「設置された場所やものの所有者」なのか「センサーの設置人」なのかが不明確なのである。そうした法整備をきちんと進めていくことが、IoT やビッグデータの利活用を加速させる前提条件となる。

一般的にはオーナーシップとは、ある所有の対象物について他人や法人に対して行使できる権利と負っている責任のことである。オーナーシップを明らかにするということは、「その対象物は誰に帰属するか」「どのような権利・責任があるのか」という２点について明確化することである。オーナーシップの権利面として、アクセス権や削除権、修正権といったものがあり、一方で責任面ではデータの品質管理責任や管理責任などが考えられる。また、データに関するオーナーシップの強さは、基本的にはそのデータの利用から生み出される価値の大きさに依存し、様々な活動への貢献度によりオーナーシップを主張しうるものになる。

IoT やビッグデータのオーナーシップに関しては、法制度上も多層的で複雑であり不明確な点が多い。そのため共通認識が欠如するからコンフリクトが起きるため、オーナーシップの共通認識を醸成するための考え方が必要になる。データの収集や保管について、様々な関係者が複雑に関与していることから、関係者がデータに対してどのような権限を有しているのかも不透明になる。今後、データの経済的価値がますます増大し、複数の関係者によりデータ利活用の権限が整理されないと、データ利活用による便益を巡っての争いが生じるリスクがある。

また、データ主体のプライバシー権がどのようなデータまで及ぶかは、個別の事例に応じて結論が大きく異なることが想定される。現行の法制度を超えたプライバシー保護については、データの保護と利活用のバランスに十分配慮した上で進める必要がある。

第3章　IoT 社会のセキュリティ上の脅威

本章では、IoT 社会の現状と将来像を概観した上で、想定される脅威について考察する。

3.1 IoT 社会の将来像

ICT はこれまでも様々な事業分野で利用されてきたが、多くの事業分野では主にデータの集計や統計処理など事務作業の効率化の観点での利用にとどまっていた。しかし、高性能なデバイスの小型化やネットワークの高度化などが実現したことにより、幅広い産業分野で IoT 的な取組が行われている。

産業分野での IoT 導入事例として、国内では株式会社小松製作所の「KOMTRAX」での建築機械の稼働状況収集・分析や、三菱電機株式会社の「e-F@ctory」での生産現場での情報収集・解析による生産の効率化の取組がある。海外でも米 GE 社の提唱する「インダストリアル・インターネット」や独の「Industrie 4.0」プロジェクト等があり、製造業分野：第二次産業での IoT の適用、開発が進んでいる。

また、それ以外の分野でも IoT の適用が進んでおり、一次産業では農業分野での省力化、生育環境制御による品質向上、ニーズに応じた精算・出荷管理や、水産分野での海洋情報収集、魚群情報提供等への適用が行われている。第三次産業でも医療・ヘルスケア分野での情報収集、予防医療への活用や小売業での商品管理やプロモーションへの活用等、適用が行われつつある。

このように、既に多分野での IoT 導入が始まっており、また、国レベル、産業レベルで取組が進められていることから、今後も様々な分野において IoT の利活用が拡大すると想定される。

表 3-1　IoT の利活用分野・利用例[13)]

分野	IoT の利用例
施設	・施設内設備管理の高度化（自動監視・制御等）
エネルギー	・需給関係設備の管理を通じた電力需給管理 ・資源採掘や運搬等に係る管理の高度化
家庭・個人	・宅内基盤設備管理の高度化 ・宅内向け安心・安全等サービスの高度化
ヘルスケア・生命科学	・医療機関/診察管理の高度化 ・患者や高齢者のバイタル管理 ・治療オプションの最適化 ・創薬や診断支援等の研究活動の高度化
産業	・工場プロセスの広範囲に適用可能な産業用設備の管理・追跡の高度化 ・鉱業、灌漑、農林業等における資源の自動化
運輸・物流	・車両テレマティクス・追跡システムや非車両を対象とした輸送管理の高度化 ・交通システム管理の高度化
小売	・サプライチェーンに係る高度な可視化 ・顧客・製品情報の収集 ・在庫管理の改善 ・エネルギー消費の低減
セキュリティ・公衆安全	・緊急機関、公共インフラ（環境モニタリング等）、追跡・監視システム等の高度化
IT・ネットワーク	・オフィス関連機器の監視・管理の高度化 ・通信インフラの監視・管理の高度化

現在は主にデータ収集が取組の中心であるが、今後収集したデータの活用と分析が進むことにより、ビジネスの仕組みの変革や効率化が進展するものと考えられる。IoT を有効に活用するには収集したデータの利活用が重要であると考えられるが、現状の IoT の取組では単一企業のサービス内で閉じている事例が多く、IoT で収集したデータを流通させるような取組はまだ少ない。

しかし、企業間・産業間でのデータ流通により新たなサービスの開発につながり、イノベーションをもたらす可能性が考えられる。経済産業省新産業構造審議会の中間整理でも、今後「データ利活用が付加価値の源泉」になるとされており、データ利活用促進に向けた環境整備を行うことが我が国の戦略の筆頭にあげられていることから、企業間の連携やデータ流通が拡大していくものと考えられる。新産業構造審議会の中間整理で予想されているデータ利活用により起こる変革は以下のとおりである。

13) 総務省「平成 27 年度情報通信白書」（http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/pdf/）

表 3-2　有力分野変革の方向性[14)]

分野	変革の方向性
ものづくり革新・産業保安・流通・小売	• 大量生産工場を用いて即時対応・オーダーメイド生産が可能に。 • 製造・物流・販売をデータで連携させることでムダゼロ・リードタイムゼロが可能に。 • ドローンを用いた物流も本格化。 • プラントの常時監視により、異常・予兆の早期検知、適切なアラームが可能。
自動走行・モビリティ	• 隊列走行の実現により、物流業の効率性向上。 • 様々な産業での完全自動走行技術の活用が進展。運転中の広告や車内時間活用サービス等が立ち上がる。 • 交通弱者や交通事故、渋滞や環境問題の解消。
金融（FinTech）	• ネット上での少額の決済・送金や、データに基づく迅速な与信審査が可能となり、従来困難だった決済・送金や資金調達等が可能に。 • 会社の経営状況や企業会計、家計のリアルタイムでの見える化により、効率的な企業のバックオフィス業務や家計管理が可能に。
健康・医療・介護	• 健康/医療関連データの利活用により、各個人に見合った健康・予防サービスを提供する事が可能に。 • 人工知能により認識・制御機能を向上させた医療・介護ロボットの実装が進み、医療・介護現場の負担を軽減。
スマートハウス・スマートコミュニティ・エネルギー	• 地域の特性に応じて需要側も含めた総合的なエネルギー需給管理を行うスマートコミュニティが実現。 • エネルギーデータにとどまらず、家庭内・コミュニティ内の多様なデータを取得・利活用することで多様なサービスが可能に。
教育	• アダプティブ・ラーニング等の進展により、子供一人一人の習熟度や学習上の困難さ、得意分野など、個に応じた学習が可能に。 • 教育コンテンツのオープン化とネット授業を活用しつつ、個別のニーズに応じて、いつでも誰でも職業に必要な能力や知識へ容易にアクセス可能に。
農業	• ロボットや自動走行システム等の導入による省力化や人工知能による生産現場の暗黙知の形式知化を通じたさらなる生産性の向上。 • ICT の活用により、生産・加工・物流・販売の連携が可能になり、トレーサビリティの確保等を通じた高度な品質管理が実現。 • 販売実績等のデータの利活用等を通じ、多様な消費者ニーズ対応した農作物の提供が可能に。
観光	• 観光客の行動データを収集・活用し、個々人の趣味・嗜好に合致するカスタマイズされた観光体験を提供。 • シェアリングやマッチングサービスの広がりにより、宿泊先や移動における観光客の選択肢が拡大するとともに、個人もサービス提供者として観光産業に参画。

データ流通を促進するためには、データ流通によるステークホルダーへのメリットの提示や、データ流通をやりやすくするための仕組みづくり、例えば、データの標準化やデー

14) 経済産業省産業構造審議会新産業構造部会（第 8 回）資料 5-1
（http://www.meti.go.jp/committee/sankoushin/shin_sangyoukouzou/pdf/008_05_01.pdf）をもとに作成

タ流通プラットフォームの整備が必要となるだろう。

一方、IoT が普及・浸透し収集されたデータの価値が理解されるに伴って、データを収集する際やデータを利活用（蓄積・分析・流通）する際の課題が顕在化すると想定される。中でも、セキュリティ上の課題について取り上げ、次節にて論ずる。

3.2 IoT 社会のセキュリティ上の脅威

IoT の特徴として、ネットワークに接続される IoT 機器の多さ、IoT 機器のライフサイクルの長さ、各機器に対する管理徹底の困難さが挙げられる。このように、これまでの情報システム分野とは特性が異なる点があるため、一般的な情報システムに想定される脅威に加えて、IoT 固有の脅威についても配慮が必要と考えられる。

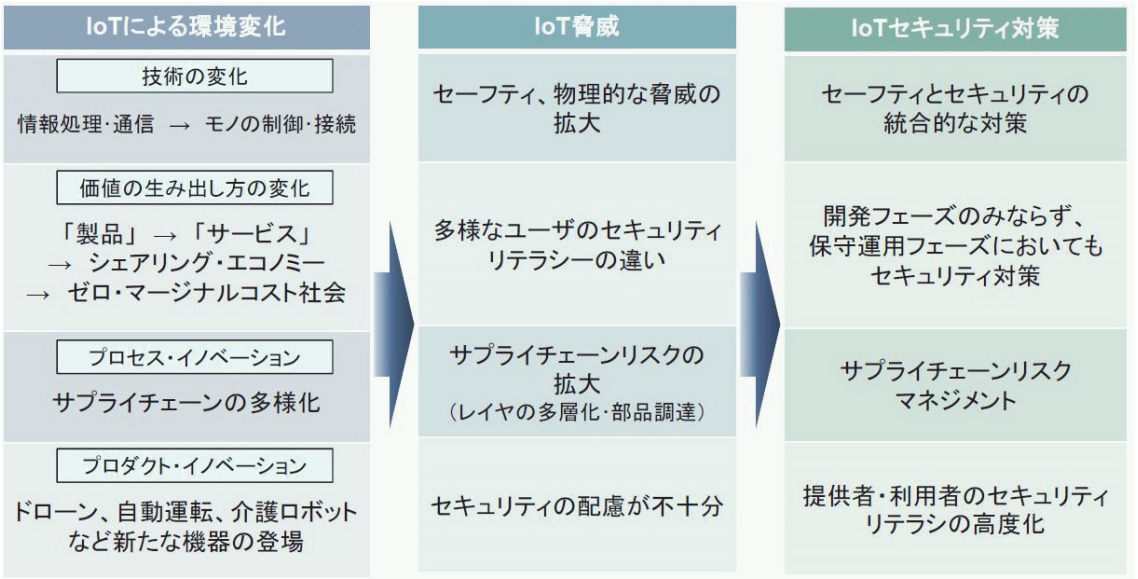

図 3-1　IoT 時代の新たなセキュリティ上の脅威[15)]

3.2.1 IoT において考慮すべき IT システムへの脅威と物理的な脅威の拡大

現在、様々な団体で将来到来する IoT 社会におけるセキュリティ上の課題が議論されているが、このうち「重要生活機器連携セキュリティ研究会[16)]」、「Cloud Security Alliance[17)]」、「Open Web Application Security Project[18)]」で議論されている IoT において考慮するべきセキュリティ上の脅威や課題をまとめると表 3-3 のようになる。

15) IoT 推進コンソーシアム　第 1 回 IoT セキュリティ WG 資料 3-1（http://www.iotac.jp/wg/security/）
16) 重要生活機器連携セキュリティ研究会(https://www.ccds.or.jp/)
17) 日本クラウドセキュリティアライアンス(https://www.cloudsecurityalliance.jp/)
18) Open Web Application Security Project(https://www.owasp.org/)

表 3-3　IoT で想定される脅威と課題

No	想定される脅威・課題	重要生活機器連携セキュリティ研究会	Cloud Security Alliance	OWASP
1	外部からサービスに対する DDoS などの攻撃によるサービス停止	・多くの生活機器がサーバと通信 ・生活機器を遠隔から監視、操作するサービスが増加	1.サービスの妨害、停止 2.謝った情報の流布 3.不正なデータによる機器の乗っ取りや妨害 5. スクリプト、アプリケーションコードの改ざん	・安全ではない Web インタフェース ・安全ではないネットワークサービス ・安全ではないクラウドインターフェース ・安全ではないソフトウェア/ファームウェア
2	クラウドサービスの S/W に存在する脆弱性			
3	クラウドサービスの乗っ取り			
4	クラウドサービスのマルウェアやウィルスに対する感染			
5	機器に対する DDoS などの攻撃による機器の機能停止や制御不能な状態の発生	・いたる所で生活機器とモバイルデバイスが接続 ・多くの生活機器がサーバと通信 ・生活機器を遠隔から監視、操作するサービスが増加	―	・安全ではないネットワークサービス
6	機器の S/W や F/W に存在する脆弱性		7. 不正なデバイスもしくは個別に乗っ取られたデバイスからのサーバ侵害	・安全ではないソフトウェア/ファームウェア
7	機器の乗っ取り			
8	機器のマルウェアやウィルスに対する感染		6. デバイスに配布するシステムソフトウェア改ざん	
9	機器の物理インタフェースからのシステムへの侵入や情報漏えい	―	―	・貧弱な物理セキュリティ
10	設定やパスワードが脆弱であることによるシステムへの侵入や情報漏えい	―	4. 収集された様々な情報の漏えいや悪用	・安全ではないモバイルインタフェース ・不十分なセキュリティ設定 ・不十分な認可/認証 ・伝送経路の暗号化の欠如 ・プライバシー
11	異なるセキュリティレベルの機器やネットワークの相互接続による情報漏えいなど	・今何がつながっているか、これから何がつながるか、分からない ・異なる分野のネットワークが意図せずつながる	―	―
12	収集データの流通経路に対する攻撃によるデータ漏えい	―	8. 他サービスとのデータ授受インタフェースに対する侵害	―

多くの脅威は通常の ICT システムで想定されるものと同様であるが、新たな分野であるために対策が不十分な傾向が見られる。

3.2.2 IoT 固有のセキュリティ上の脅威

前節では、IoT において考慮すべきセキュリティ上の脅威を全般的に整理したが、本節では IoT 固有のセキュリティ上の脅威について考察する。

(1)セーフティ、物理的な脅威の拡大

これまでの一般的な情報システムとは異なり、IoT の場合にはインシデントによる影響がサイバーの世界に留まらず、現実世界に物理的な影響を与える機会が増大する。つまり、情報セキュリティだけではなく、人命、財産、環境への悪影響ーセーフティの面での被害が想定される。

また、情報セキュリティは機密性、完全性、可用性の三要素を維持すること、と定義されるが、これまでの情報システムでは機密性が最重要視され、インシデントへの対策としてシステムの機能停止が選択される場合もあった。それに対して、IoT では制御を止めるわけにはいかず、可用性が最重要視される場合も想定される。

IoT では情報セキュリティに加え、セーフティの観点からも脅威を想定する必要がある。

(2)多様なユーザのセキュリティリテラシーの違い

IoT が社会に普及するにつれて、利用者の層も幅広いものになり、すべての利用者にセキュリティリテラシーを期待する事は困難である。セキュリティリテラシーを欠いた IoT の利用によって生じる悪影響が脅威として想定される。

このような状況下では、IoT 機器の機能が正しく理解されないまま使用されたり、設定変更が適切に行われずに使用されたりすることも想定され、IoT 機器の初期設定がセキュリティ上の問題があった場合、そのままの状態で使用され脅威となり得る。

利用者のセキュリティリテラシー向上、および IoT 機器が初期状態でセキュアな設定とする（デフォルトセキュア）等、セキュリティを確保するための工夫が必要だろう。

(3)サプライチェーンリスクの拡大

昨今の状況下、システムを構成する機器をすべて自前で設計・製作することはほぼありえず、第三者から調達する場合が大半である。このような場合に機器に不良があったり、あるいは悪意を持って不正な機能を埋め込まれたりすると、IoT システムのセキュリティ脅威となる。調達品に不正が行われることも脅威として想定が必要である。

また、IoT の普及に伴い、異種 IoT 間の相互接続やデータ連携も進展すると想定される。そのような状況下では、不正な通信相手が接続することは、関連する全システムに悪影響を生じる。システムやデータが連携するゆえの脅威についても想定が必要である。

(4)セキュリティの配慮が不十分

IoT は、これまでインターネット接続されていなかったような機器がネットワーク接

続される場合もあり、設計者側がセキュリティ脅威を十分認識しておらず、配慮が不足している傾向が見られる。一般の情報システムで常識的に行われているセキュリティ対策が漏れていて脆弱性を内包している場合もあり、脅威となり得る。

また、セキュリティに関する状況は刻々と変化しており、日々新たな攻撃手法が開発されている。このため、開発時点ではセキュリティに問題が無かったとしても、経時とともに脆弱性が発見されることが想定される。ネットワークに接続された機器は攻撃を受けるリスクが高く、リリース後適切なメンテナンスがなされず、長期間経った機器は多くの脆弱性を持つと想定され、脅威となり得る。

設計･製造時のセキュリティを意識した設計・製造、および運用開始後のセキュリティを維持するための継続的な保守はセキュリティを確保するために欠かせないものであり、その点の配慮が欠けたIoT機器はそれ自体が脅威といえるだろう。

(5)データオーナーシップに関わる脅威

「2.4 データオーナーシップに関わる法的課題」に記載したように、IoTによって収集したデータのオーナーシップが曖昧になっている場合がある。オーナーシップが明確に規定されていない場合、データの発生源となるセンサーやデバイスの所有者などからデータの利用に関して訴訟等を提起されるリスクがある。

収集したデータの利用や再販に際しては、単にデータオーナーシップを明確にするだけではなく、データの匿名化など所有者のプライバシーや機密情報に配慮した利用方法を検討する必要がある。

第4章　セキュアな IoT 社会実現に向けた課題

本章では、前章で述べた IoT 社会におけるセキュリティ上の脅威に対応し、セキュアな IoT 社会を実現する上での技術的課題、事業展開上の課題、制度的課題について考察する。

4.1 セキュアな IoT 社会実現に向けた技術的課題

第 3 章では、IoT 社会のセキュリティ上の脅威について述べた。ここでは、これらセキュリティ上の脅威に対応していく上での技術的な課題についてまとめる。

4.1.1 IoT 機器への不正アクセスやマルウェア感染への対応

昨年、制御用アカウントが初期設定まま使用されていた大量の IoT 機器がマルウエア（Mirai）に感染し、大規模な DDoS 攻撃の踏み台として利用されるというサイバー攻撃が発生した。このような攻撃を予防するためには、IoT 機器が初期設定のまま使用されないようにするための対策や、汎用のウィルス対策ソフトウェア等の導入が難しい IoT 機器に対するマルウェア感染から守るための対策が必要になる。

また、自動車などの比較的長期間利用される IoT 機器の場合、IoT 機器の譲渡・転売等により所有者が変化していくことが予想されるため、所有者が変更した後に、前の所有者のアカウントが不正利用されないようにするなどの対応も必要になる。

4.1.2 IoT 機器連携におけるセキュリティ上の弱点を狙った攻撃への対応

様々な IoT 機器が連携して動作する IoT 社会において、攻撃者は、最もセキュリティの弱い部分を攻撃してくることが予想される。このため、IoT 機器間の通信路やそれぞれの IoT 機器が保持する認証情報をすべて暗号化する必要がある。また、IoT 機器間で交換されるデータについても、改ざんや否認等を防止するため、データを受信する IoT 機器側で、送信元の IoT 機器の真正性をチェックするなどの対応が必要になる。

さらに、複数の IoT 機器が自律的に接続するような環境においては、IoT 機器同士が相互認証することで、脆弱性のある IoT 機器や攻撃者の管理下にある IoT 機器などの信頼できない IoT 機器との接続を防止するような対策が必要になる。

4.1.3 IoT 機器の脆弱性対応の難しさを利用したゼロデイ攻撃への対応

IoT 機器に脆弱性が発見された場合、利用されているすべての IoT 機器に対して即座にパッチ適用をすることが難しいことなどから、一部の IoT 機器が脆弱性のある状態のまま放置される可能性が高い。このため IoT 機器に対して定期的に脆弱性検査を実施して脆弱性の有無を監視したり、重大な脆弱性が発見された場合は、一時的に他の機器との通信を停止し、自動的にパッチ適用を実施した上で動作を再開できるようにするなど、自律的な脆弱性対策の仕組みが必要になる。

4.1.4 セキュリティ障害の伝搬による被害拡大への対応

複数の IoT 機器が連携して動作する環境においては、一部の IoT 機器のセキュリティ障害が伝播して大規模障害に拡大しないよう、IoT 機器が停止した場合や、ネットワークの利用が困難になった場合でも、セキュリティ上の安全性が保たれるよう、フェイルセキュアな設計をする必要がある。

また、障害から復旧する際など、パスワードリセット等の初期化作業の過程においても脆弱な状態が発生しないようにする必要がある。

4.1.5 IoT 機器への物理的な攻撃への対応

IoT 機器などのエッジコンポーネントは誰でも入手することが可能であり、物理的な攻撃によりネットワークへの侵入等が試みられることが懸念される。このため、耐タンパー性を高めたり、物理的な多層防御を図ることが、従来に比べて、より重要になると考えられる。

4.2 セキュアな IoT 社会実現に向けた事業展開上の課題

本節では、今年度の調査活動（アンケート調査、有識者ヒアリング）から IoT 機器や IoT サービスを普及させる上で必要とされる事業展開上の課題についてまとめる。

4.2.1 セキュアなデータ利活用を支えるプラットフォーム基盤の整備

今回のアンケート調査の結果[19)]から、パーソナルデータを収集する企業（主に非製造業）では、データ収集・利活用プラットフォーム（IoT プラットフォーム）上で「自社のデータを提供し、他社のデータの利活用もしたい」と回答する割合が予想以上に高くいことがわかった（図 4-1）。

19) 付録）三菱総合研究所「IoT 社会の将来像とセキュリティリスクに関する調査」

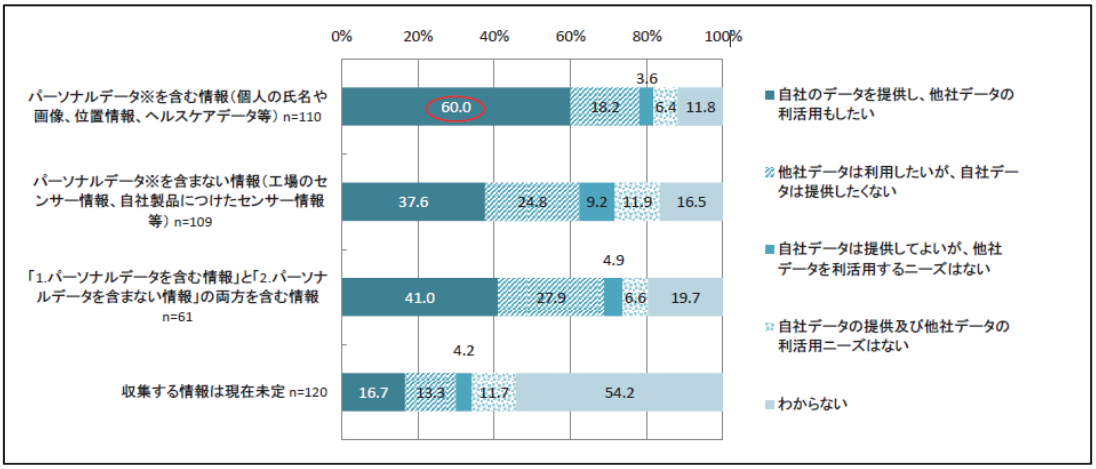

図 4-1　データ収集・利活用プラットフォーム上でのデータ利活用のニーズ

このため、データ利用・流通のための IoT プラットフォームを実現する上では、流通するデータの適切な管理が課題になると考えられる。

また、EverySense などの、一般消費者向けのデータ利活用を促進する IoT プラットフォームでは、IoT サービスベンダ、IoT プラットフォーム、利用者の間で、図 4-2 のような価値連鎖が形成され、データのオープンな利活用が進展していくことが予想される。

このような状況においては、データ利用・流通のための IoT プラットフォームを介して、利用者から収集したデータを IoT サービスベンダに提供する際には、他で収集したデータと照合するなどして利用者個人が特定されないようにするなどのセキュリティ上の安全性を保障できるようにすることが課題となる。

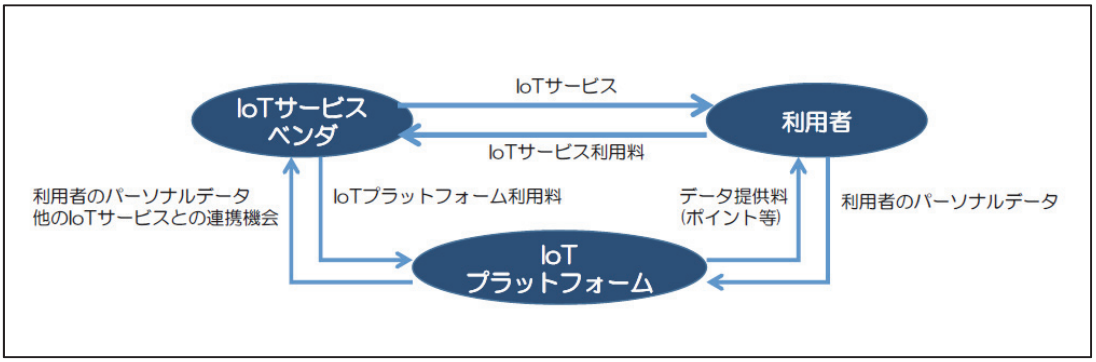

図 4-2　IoT における価値連鎖モデル

4.2.2 IoT 利用者の情報セキュリティに関するリテラシー向上

一般消費者向けのサービス想定した場合、IoT 機器は利用者本人が気付かないうちにつながってしまう場合や安易に接続に同意してしまう場合が想定される。このため、情報窃取

や不正操作が行われる脅威についての教育が必要になると考えられる。

また、今回の活動で実施したアンケート調査の結果から、製造業では、社内利用を想定したIoTを導入しているケースが多いため、十分なセキュリティ対策がとられていない傾向があることがわかった。このため、IoTサービス提供者側のリテラシー向上、特に、つながることへのリスクの認識や、IoTへのサイバー攻撃が発生した場合の対応能力の向上が必要とされる。

4.2.3 情報セキュリティに関するポリシーの利用者への提示と同意確認

IoT機器の中には、表示画面を持たないものも存在する。このため、表示画面を持たない場合であっても、利用者の携帯端末等を利用して、プライバシーポリシー、セキュリティ・ポリシー、サポート・ポリシー等の利用ポリシーの提示と同意確認が利用者に適切に行えるようにする必要がある。

4.3 セキュアなIoT社会実現に向けた制度的課題

本節では、セキュアなIoT社会を実現するための制度的課題として、データ利活用、およびサーバ攻撃に関する法整備上の課題について述べる。

4.3.1 IoT社会におけるセキュアなデータ利活用を支える法整備

第2章では、個人情報保護法を中心とするセキュアなデータの利活用を支える法整備の現状について述べた。ここで述べたように、現行の個人情報保護法においては、利用者への利用目的の提示や、第三者提供に関する同意を行う方法などが大きな課題になると考えられる。また、個人情報の取得、取扱い、第三者提供の観点からは、現行の個人情報保護法に関して図 4-3に示すようなIoT特有の課題があることが指摘されている。

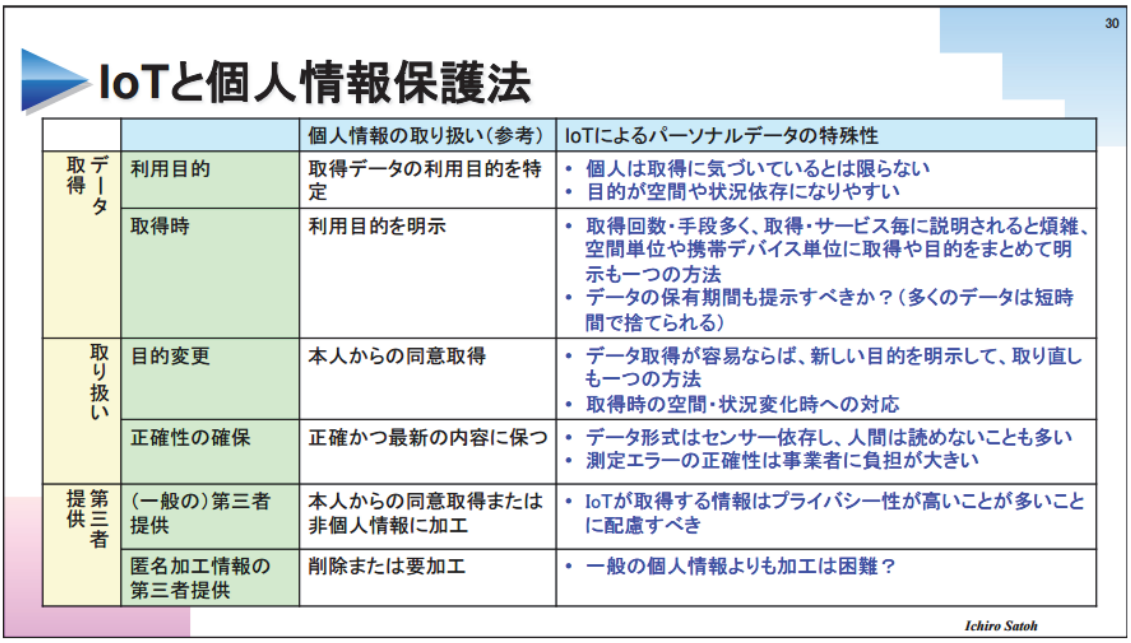

図 4-3　IoT と個人情報保護法[20)]

4.3.2 IoT 社会におけるサイバー犯罪を防止するための法整備

IoT の普及により、遠隔からの自動車の不正操作、ホームネットワークへの侵入による家電製品や防犯機能の不正操作、ペースメーカー等の医療機器の不正操作など、身体や生命に危険を与えるようなサイバー犯罪の発生が予想される。

近年、サイバー攻撃に対応するために改訂/制定された法律（ウィルス作成罪、不正アクセス禁止法、プロバイダ責任制限法など）があるが、安全な IoT 社会を実現する上では、さらなる法整備の拡張が必要になると考えられる。表 4-1 に、現行のサイバー攻撃関連の法律とその課題についてまとめる。

[20)] 佐藤一郎、IoT が抱えるプライバシーリスクとパーソナルデータの利活用、CEATEC Japan 2016（http://ichiro-satoh.jp/download/presentation/ceatec.pdf）

表 4-1　現行のサイバー攻撃関連の法律の IoT への適用上の課題

法律	セキュアな IoT 社会実現に向けた課題
ウィルス作成罪 （刑法 168 条）	現行法では、コンピュータウィルスの作成・提供・取得・保管について禁止しているが､ウィルスと同等の利用者の意図に沿わない動作を行う IoT 機器を不正に接続させる行為を禁止するなどの拡張も必要になると考えられる。
不正アクセス 禁止法	現行法では､他人のアカウントの窃取やそれを利用した不正アクセスについて禁じられているが､初期設定のアカウントの不正利用や IoT 機器に残存していた他人のアカウントの不正利用などへの拡張、さらには、複数の IoT 機器が連携している状況下における認証回避による不正アクセスなどについても禁止するような拡張も必要になると考えられる。
刑事訴訟法	現行法では、サイバー犯罪捜査のための差押え対象として、サーバや電磁的記録媒体が可能とされているが、今後は、IoT 利用犯罪を想定し、IoT 機器についても差押え可能とするような拡張が必要になると考えられる。
不正競争防止法	現行法では、大規模な個人情報漏洩事件を契機に、事業者が保有する個人情報等の営業秘密の窃取・不正転売などを禁止する改正が行われているが、IoT 機器で収集される複数のセンサーデータ等を突合することで個人情報化するような行為についても禁止するような拡張が必要になると考えられる。
プロバイダ 責任制限法	現行法では、インターネット上の情報流通によって権利侵害が発生した場合、情報を発信した者を特定するために必要な発信者情報の開示請求において､プロバイダ等に対する民事上の責任（損害賠償責任）が制限される。ここでの発信者情報については、権利侵害を行った者の氏名、住所、メールアドレス、IP アドレス、ユーザ ID、SIM カード ID などであるが、IoT 機器を特定する識別情報についても含めるよう拡張が今後は必要になると考えられる。

第5章　提言

本章では、IoT 機器や IoT プラットフォームの提供を進めている組織、およびそれらの組織を支援するビジネスに対し、IoT 社会の実現に向けた課題を解決するために必要な方策を検討し提言する。

5.1 IoT 機器のセキュリティレベル確保

IoT により機器のデータ収集や制御を行うということは機器をネットワークに接続することである。これまで、ネットワークに接続していなかったり、イントラネットにしか接続したことがない機器をインターネットに接続する際には、

- データの不正窃取
- データの改ざん
- 乗っ取り

などのリスクがあるため、十分な注意が必要である。対策として、ICT システムでこれまで当然のこととして行われているセキュリティ対策も含まれるが、

- 機器-クラウド間の通信路は暗号化し相互に認証を行うこと
- 直接機器をインターネットに接続するのではなく、セキュリティ面の配慮をした G/W を経由してデータの収集や制御を行う構成とすること
- 機器に内在する脆弱性について情報を収集し、脆弱性が見つかった場合には速やかに修正すること
- 機器のつながるネットワークに、ネットワーク接続の必要がない機器が接続されていない様にすること

などに留意する必要がある。

制御システムで利用する IoT 機器を新たに開発する際には、例えば、EDSA 認証（Embedded Device Security Assurance）という製品認証制度があるので、こうしたフレームを活用してセキュリティ機能を確認する方法もある。

5.2 セキュリティリスクを低減する管理方策

自社・他社が設置した機器の管理・保守・把握のために、システム全体の挙動やデータの流れを外部から診るセンサーやプローブを用意して、システム外からの情報をもとにして、システムの健康状態を診ること（ヘルスチェック）は有効である。この時、可用性が重要なシステムの場合には、許容範囲内の異常であれば通知は行うがシステムを止めずに経過観察措置とする。経過観察中に対策を策定しておき、異常が許容範囲を越えた場合にはいつでも対処できるように準備をしておく。システム外の情報源としては、データの異

常な振る舞いを検出するために、仮想的なサンドボックスシステムやクラウドにおかれた脅威収集して分析された知識ベースデータなどが有効である。

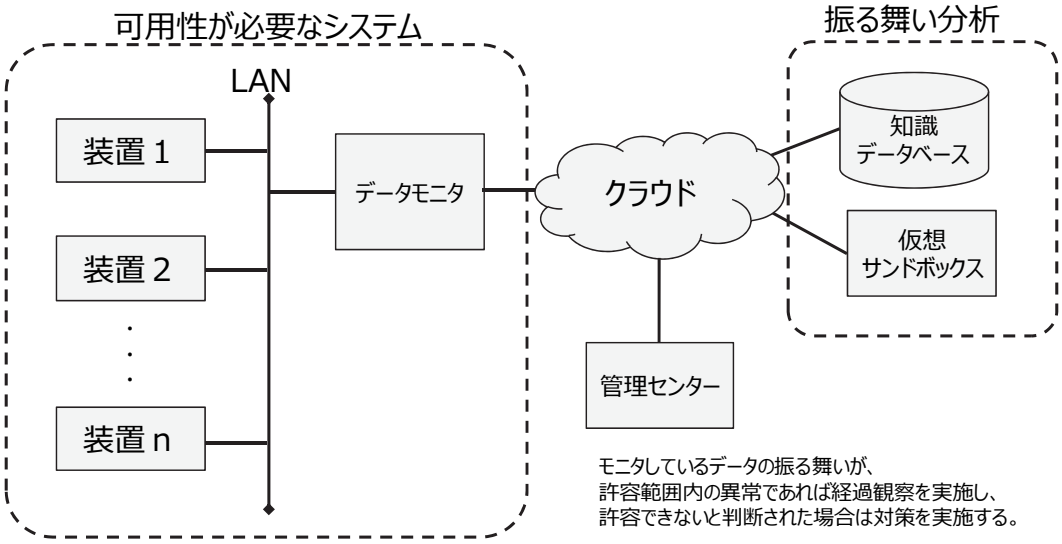

図 5-1　可用性の高いシステムの機能チェック

可用性を重視する装置やシステムの場合には、マルウェアの削除等を実施するのではなく、正しく動作している時の状態を復元することが必要である。既にマルウェアなどの攻撃から装置やシステムを強固に守るのは限界であり守り切れない。したがって、異常な動作を早期に検出して装置やシステムを復元することに注力することがよいと考えられる。なお、復元するための方法は、セキュリティが高いことが必要不可欠である。

IoT 機器のセキュリティ管理では、IoT 機器の長いライフサイクルに渡ってのセキュリティ機能の維持管理も重要になる。IoT 機器は設置や利用の仕方によっては、利用者や管理者からも存在がわからなくなることがある。このような場合、セキュリティ機能の陳腐化が進んでいても気が付かないこともある。このようなことに対応するために、IoT 機器からのセキュリティ情報やセキュリティ機能の有効期間などの管理情報を発信するなどの方法をとる必要がある。IoT 機器が各々勝手に管理情報を発信すると、その IoT 機器を利用しているシステムに影響を及ぼす事が考えられるので、IoT 機器の管理情報や発信ルールなどを業界で標準化することも重要である。

5.3 経営課題でもあるセキュリティ対策

今後さらに IoT が経営資源の一部として大きな比重を占めてくることを踏まえると、セキュリティの確保・維持には基本的なサイバーセキュリティが分かる人材、対策ができる人材が不可欠であり、経営者もセキュリティの重要性を認識し実践する覚悟が必要となる。

IoT 機器の管理・保守・把握では異常が許容範囲を越えた場合にはいつでも対処できるよ

うに準備が必要であるが、問題が発生してから判断するのではなく、どのように判断し、どのように事業を継続するかを前もって想定しておくことが重要である。例えば、システムを止めるか止めないかの判断には、責任能力と決断能力が必要となる。システムを止めるとビジネスに大きなインパクトがあり、経営者にとってもどう判断するか難しい決断を迫られることもある。

経営者が踏み出すべき最初のステップは、すべて現場任せにするのではなく、まずはどこまで対応できていて何ができていないのかの現状を把握することである。これにより、自社でやるべきこと、セキュリティベンダ等の専門家に任せた方がいいことを切り分け、対策が不十分な部分は強化することが必要である。システムや製品のセキュリティ対策に関しても経営者が理解しておくことが重要である。例えば、企画・設計段階から考慮する「セキュリティ・バイ・デザイン」の考え方を採用し、企画・設計から運用・保守までのライフサイクル全体でのセキュリティ対策を向上させる取組を推進しなければならない。

IoT 機器の脆弱性関連情報を収集・分析して、脆弱性の影響を予測して重大なインシデントを未然に防ぐ体制を構築することは経営者の役割である。

5.4 IoT 社会でのセキュアなデータ利活用に向けて

セキュアな IoT 社会実現に向けて商品/サービスを提供していく上では、技術的なセキュリティ対策のみならず、セキュアなデータ利活用を可能にするための情報保護対策、エンドユーザのリテラシー向上のための教育、障害発生時の対応体制などの整備を業界横断的にすすめていく必要がある。特に、サービスの提供形態については、従来のようなエンドユーザ-サービス提供者という 2 者の関係から、エンドユーザ-IoT プラットフォーム-サービス提供者という 3 者の関係に移行していくことが予想されることから、これら 3 者間でセキュリティ対策を考えていく必要がある。

また、IoT 機器を不正利用したサイバー犯罪は、人命等に関わる問題に発展する可能性がある一方、現行法では網羅されないと思われる部分があることから、今後の法整備が期待される。

おわりに

本年度の調査にて、IoT 社会の将来像を検討するとともにセキュリティリスクなどの課題を明らかにし、課題を解決するために必要な方策を検討し提言することができた。

IoT 機器のセキュリティレベルの確保の仕方、IoT 機器のセキュリティ機能の陳腐化を防ぐための方策、経営者が行うべきセキュリティ対策などの提言を通じて、IoT 社会でセキュリティを確保するために必要となる事柄を明確にした。そして、セキュアな IoT 社会を構築、様々な IoT データから得られる情報を活用して行くことで、少子高齢化が一層進んだ時代になっても、生産性の効率化、生活の品質向上、エネルギーの最適化などが実現できると考える。また、提言した方策を提供することはビジネスチャンスにもつながる。

IoT の適用範囲は益々拡大して行くことは紛れもない。したがって、提言したセキュリティリスクを低減するための方策を実施することが望まれる。これらの方策により、JEITA 会員企業のみならず多くの企業において、より安全・安心な IoT 社会の構築につながるとともに、IoT 社会および情報セキュリティ産業が発展していくことを期待する。

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 28 年度情報セキュリティ調査報告書
ーIoT 社会の将来像とセキュリティリスクに関する調査ー

発　行　日　　平成29年3月
編集・発行　　一般社団法人 電子情報技術産業協会
情報・産業システム部
〒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