JEITA

情産－19－技標－３

平成30年度情報セキュリティ調査報告書

－サイバーフィジカルシステムの実現に向けた セキュリティ脅威とリスク分析に関する調査－

平成３１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

政府が提唱する Society 5.0 や Connected Industries では、サイバー空間とフィジカル空間が連携する社会の実現に向け、IoT（Internet of Things）や AI の利活用が期待されている。その一方で、サイバー攻撃による人命や社会インフラに与える脅威についても懸念されており、従来の「情報セキュリティ」が主眼としてきた情報資産に加え、人命や社会インフラの安全性の確保を加えた、新たな「サイバー・フィジカル・セキュリティ」の実現が求められるようになってきている。

本調査報告書では、上記のような状況を踏まえ、サイバー空間とフィジカル空間が融合する社会におけるサイバー攻撃の脅威について、今後、利活用が進展していくと考えられる各種 IoT 機器をターゲットとした攻撃や AI を利用した新たなサイバー攻撃について考察するとともに、それらサイバー攻撃のリスクを定量的に把握できるようにするための新たなリスク評価モデルを提案する。

またさらに、このリスク評価モデルに基づいて、さまざまな分野の IoT が抱えるサイバーセキュリティ上のリスクの大きさをアンケート調査により試算した結果について報告する。

本報告書の作成にあたり、ヒアリングにご協力いただいた有識者の方々、及び当専門委員会の関係者の皆様に深く感謝するとともに、本報告書が広く活用され、今後のサイバー・フィジカル・セキュリティ対策の進展に寄与することができれば幸いである。

2019 年 3 月

情報セキュリティ調査専門委員会
委員長　増田　佳弘

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	増田佳弘	富士ゼロックス㈱
副委員長	森安　隆	㈱日立製作所
委員	福島孝文	東芝テック㈱
〃	白石節男	富士通㈱
〃	池田恵一	富士通㈱
〃	佐藤　淳	㈱リコー
〃	船木　靖	㈱リコー
オブザーバ	田中清一	エム・アール・アイ リサーチアソシエイツ㈱
〃	牧野夏葉	エム・アール・アイ リサーチアソシエイツ㈱
〃	江連三香	㈱三菱総合研究所
〃	綿谷謙吾	㈱三菱総合研究所
事務局	長岡　勉	(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

1. サイバー空間とフィジカル空間が融合した社会のセキュリティ上の課題

政府は、現在、第 5 期科学技術基本計画の一環として、サイバー空間とフィジカル空間を高度に融合させることにより、地域、年齢、性別、言語等による格差なく多様なニーズ、潜在的なニーズにきめ細かに対応したモノやサービスを提供することで経済的発展と社会的課題の解決を両立し、人々が快適で活力に満ちた質の高い生活を送ることのできる「超スマート社会」Society 5.0 の実現を目指している（図 1-1）[1]。

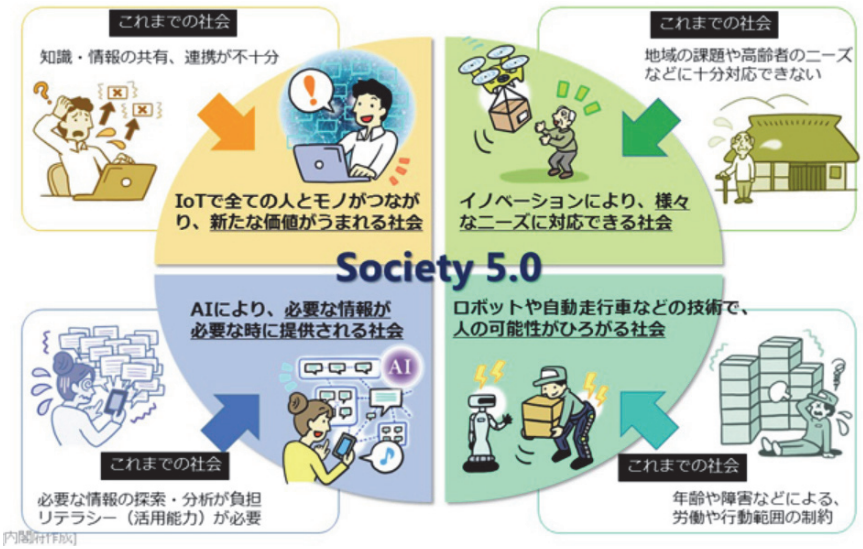


図 1-1 Society 5.0 で実現する社会のイメージ

本章では、この「超スマート社会」Society 5.0 の実現に向けたセキュリティ上の課題を整理する。

1.1 サイバー空間とフィジカル空間が融合する社会

「超スマート社会」Society 5.0 は、サイバー空間とフィジカル空間が連携して、さまざまなニーズに応じた価値を提供するサイバーフィジカルシステム（CPS：Cyber-Physical System）によって実現される。このサイバーフィジカルシステムの中核となる技術は、以下の特徴を備えた IoT（Internet of Things）と人工知能（Artificial Intelligence）であり、図 1-2 に示すような形態でフィジカル空間とサイバー空間を連携する。

- IoT（モノのインターネット）：自動車や家電などの「モノ」がネットワークに接続され、相互に連携することにより新たな価値を創出する
- AI（機械学習や深層学習）：各種 IoT 機器により収集される膨大な情報（ビッグデータ）を分析し、予測や最適解の導出などを可能にする

[1] Society 5.0、内閣府、2019 年 2 月 8 日、https://www8.cao.go.jp/cstp/society5_0/index.html

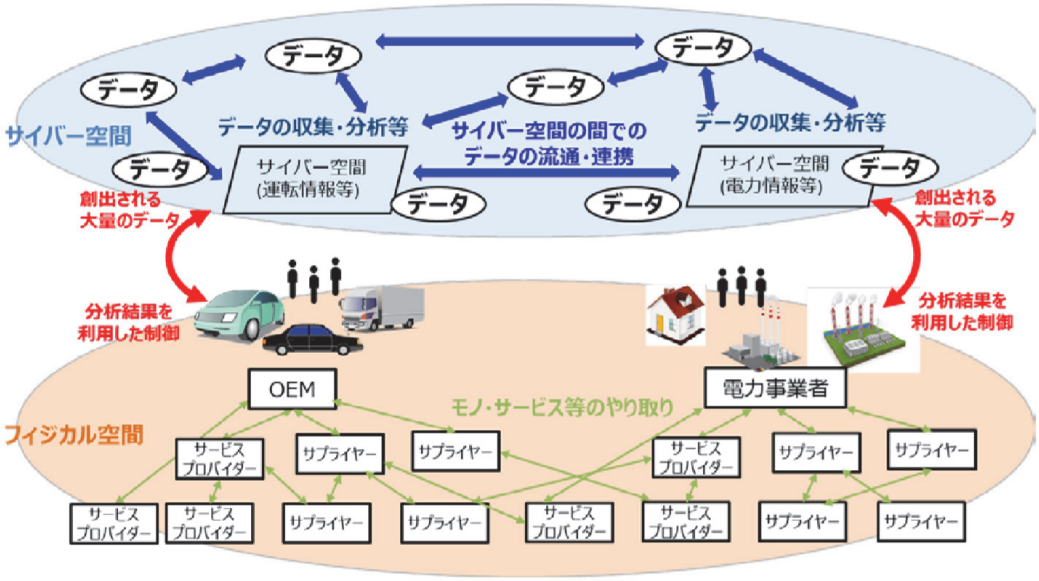


図 1-2　サイバーフィジカルシステムの構成[2]

1.2　サイバーフィジカルシステムの実現に向けた IoT や AI の実用化の現状

本節では、サイバーフィジカルシステムの中核である IoT と AI の実用化の現状について概観する。

1.2.1　IoT の実用化の現状

IoT は、家電製品や自動車、施設、ロボット等のさまざまなモノをインターネットに接続して情報をやり取りすることで、新たな付加価値を生み出そうとする概念である。総務省[3]によると、2000 年代以降、利用されている IoT 機器の数は増加の一途をたどっており、2020 年までに約 530 億個に達すると予想されている。表 1-1 に、IoT の実用化事例を示す。

表 1-1　IoT の実用化事例

IoT の種類	実用化事例
家電製品	炊飯器、給湯器、ドアのシャッター、電子錠等の家電、住宅設備を無線接続し、専用のディスプレイ上で操作する。[4]
病院システム	患者の寝室天井またはベッド下にバイタルセンサを設置し、非接触で心拍・呼吸数を計測、WEB で値の表示・グラフ表示・ログの保存を行う。異常を検知するとメールや警告画面、アラーム音で知らせる。[5]

[2] 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（案）」
[3] 情報通信白書平成 27 年版、総務省、2019 年 2 月 8 日、
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/html/nc254110.html
[4] AI 使い、スマート家電からスマートホームへ、株式会社産業経済新聞社、2019 年 2 月 8 日、
https://www.sankei.com/premium/news/181226/prm1812260003-n2.html
[5] IoT 介護見守りシステム『ミマモリ君ＷＥＢ』、トーカイセキュリティ株式会社、2019 年 2 月 8 日、
http://www.tokaisecurity.net/html/mimamorikun-web.html

IoT の種類	実用化事例
監視カメラシステム	LTE 通信モジュールを内蔵した防犯カメラとインターネットのサービスをセットにした IoT サービス。現地に設置したカメラ等から、ネットワーク環境を通じてクラウドサーバに映像データを収集・保存する。スマートフォンやパソコンから管理用ウェブサイトにアクセスし、ID とパスワードを入力してクラウドサーバ上に保存された映像データの閲覧が可能となる。[6]
ビル・エネルギーマネジメントシステム（BEMS）	ビル設備を集中監視する制御システムがなくても、照明・空調機器から直接、あるいはキュービクルや分電盤の回路等からデータを取得し、電力量の監視・管理等を実施。データの取得は、IP ネットワークや近距離無線等を使用する。[7]
農業工場	栽培ハウス内に設置したセンサーから、環境データを収集し多角的に分析。スマートフォンで撮影した動画データを解析することで、作物の収量・収穫期予測、病害虫リスクの診断をする。[8]
自動車システム	ICT 端末としての機能を有す（コネクテッドカーとなる）ことで、スマートフォン等のほかの情報端末ともフレキシブルにつながるようになる。災害時には、通行可能な道路をその地域での自動車の走行データから瞬時に解析し、インターネットを介して開示する等、道路交通の混乱を避けることに貢献する。[9]
デジタルサイネージ	防犯カメラ画像、店舗の POS、SNS の書き込み、天気予報や施設内の各種センサー情報等をリアルタイムに収集・分析することで、サイネージやスマートフォンの位置・時間に対応したコンテンツを配信する。AI 技術を駆使することで、タイムリーで最適なコンテンツを適切な場へ提供する。[10]
自動販売機	大画面ディスプレイや AR（拡張現実）カメラを備えた IoT 自動販売機。表示は日本語の他、英語、中国語、韓国語に対応している。決済手段も最高 3 万円までの現金高額決済に加え、決済用ユニットの追加により各種電子マネーやクレジットカードによる支払い、QR コード決済にも対応。[11]
遠隔医療機器	X 線写真や MRI 画像等、放射線科で使用される画像を通信で伝送し、遠隔地の専門医が診断を行う「遠隔画像診断」で活用。その他に、情報通信端末で測定した生態情報（体温、血圧、脈拍、尿糖値）や患者の映像・音声等を遠隔地の医師へネットワークを通じ送信することで受けられる在宅医療や、遠隔病理診断、遠隔相談等でも活用。[12]

[6] KDDI IoT クラウド Standard: 監視カメラパッケージ、KDDI 株式会社、2019 年 2 月 8 日、https://www.kddi.com/business/mobile/m2m-solution/iot-cloud-standard/camera/

[7] IoT でビル管理！「BEMS ビジネス」はクラウド型で中小ビルにも拡大へ、株式会社リックテレコム、2019 年 2 月 8 日、https://businessnetwork.jp/Detail/tabid/65/artid/4100/Default.aspx

[8] OPTiM が描く、スマート農業、株式会社オプティム、2019 年 2 月 8 日、https://www.optim.co.jp/agriculture/?gclid=EAIaIQobChMI3-bGxOeo4AIV2qmWCh0TMgeREAAYBCAAEgIUQ_D_BwE

[9] 平成 27 年版 情報通信白書、総務省、2019 年 2 月 8 日、http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/html/nc241210.html

[10] 「まち」の QoL 向上を実現するスマートライフ・ビジネスデジタルサイネージ向け総合情報サービス、株式会社日立製作所、2019 年 2 月 8 日、http://www.hitachihyoron.com/jp/archive/2010s/2018/02/02c01/index.html

[11] “AR 試着”もできる IoT 自動販売機「スマートマート」、ブイシンクが本格展開、アイティメディア株式会社、2019 年 2 月 8 日、http://www.itmedia.co.jp/news/articles/1806/12/news128.html

[12] 医療分野の情報化の推進について、厚生労働省、2019 年 2 月 8 日、https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html

1.2.2 AI の実用化動向

AI（人工知能）に関する研究は 1950 年代後半に始まり、自然言語処理、パターン認識、推論システム等、これまでさまざまな応用が試みられてきた。近年では深層学習（ディープラーニング）に代表される機械学習の進展により、その実用化への可能性が広がり、再び脚光を浴びるようになってきている。以下に、AI 技術の実用化事例を示す。

表 1-2 AI の実用化事例

分野	実用化事例
故障箇所推定	【鉄道設備の故障個所の原因推定】 過去の鉄道設備の点検やトラブルに関する報告書の学習結果から、事象を手がかりに故障原因や発生箇所を推定。[13]
自然言語処理	【AI による顧客窓口対応】 多言語での顧客からの質問や問い合わせに対し、AI による自然言語処理により自動応答するサービスを航空会社が導入。[14]
顔認証	【空港の顔認証ゲート】 深層学習（ディープラーニング）を活用し、従来は認証が困難であった斜め、うつむき、逆光、 経年変化等の条件にも対応可能な顔認証ゲートを導入。[15,16]
行動パターン予測	【在宅確率予測システム】 蓄積されたデータ(エネルギー使用量)から、AI が各家庭の生活パターンを学習、各家庭の未来の在宅確率を予測し、可視化する Web アプリケーションを開発。本アプリケーションの活用により、宅配業者の再配達件数の減少を見込む。[17]
推定・予測	【船舶の燃費性能の予測】 船舶に関連するビッグデータ（気象・海象のセンシングデータ、船舶エンジンのログデータ、船舶の速度や位置のデータ等）から、AI が船舶の実海域における燃料消費や速度等の性能を推定する技術を開発。船舶の性能評価や設計へのフィードバック、燃費改善等に役立てる見込み。[18]
ロボットアームによる自動化	【物流倉庫でのピッキング工程の自動化】 ピッキング対象物の認識画像を元に、AI がロボットアームの軌道や掴み方をプログラムとして自動生成するシステムを物流倉庫にて導入。[19]

[13] JR EAST Technical Review、東日本旅客鉄道株式会社、2019 年 3 月 14 日、https://www.jreast.co.jp/development/tech/pdf_55/tech-55-13-16.pdf

[14] 本邦航空会社初！AI（人工知能）を活用した 7 言語の顧客対応を開始 ～イノベーションでさらなる顧客満足の向上へ～、SCSK サービスウェア株式会社、2019 年 3 月 14 日、https://www.scskserviceware.co.jp/news/144/detail.html

[15] 羽田空港での、日本人の帰国手続の合理化に貢献法務省様がパナソニックの「顔認証ゲート」を採用、パナソニック株式会社、2019 年 3 月 14 日、https://news.panasonic.com/jp/press/data/2017/12/jn171215-1/jn171215-1.html

[16] サングラス姿でも顔照合。ディープラーニング技術とデジタルカメラ「LUMIX」のカメラ技術が高精度の顔認証ソリューションを実現、パナソニック株式会社、2019 年 3 月 14 日、https://news.panasonic.com/jp/stories/2018/55991.html

[17] 次世代 物流オープンデータ活用コンテスト／岡山大学が優秀賞、株式会社ロジスティクス・パートナー、2019 年 3 月 14 日、https://lnews.jp/2017/11/j111310.html

[18] 運航データを活用して船舶の燃費性能を高精度に推定、株式会社富士通研究所、2019 年 3 月 14 日、http://pr.fujitsu.com/jp/news/2016/05/10-2.html

[19] アスクル、最新の技術をもつロボットベンチャーMULIN と業務提携　両社協力してロボティクス技術開発を加速、e コマースの物流現場へロボットを導入、アスクル株式会社、2019 年 3 月 14 日、http://pdf.irpocket.com/C0032/FgNv/MwDt/IK0R.pdf

1.3　セキュリティ上の課題

経済産業省が中心となって策定を進めている「サイバー・フィジカル・セキュリティ対策 フレームワーク（案）[20]」によれば、IoT を通じてサイバー空間ですべての人やモノがつながり、高付加価値が得られるようになる一方で、以下のようなセキュリティ上の課題が示唆されている。

- さまざまな IoT 機器がサイバー空間に接続するため、サイバー攻撃の脅威・感染源が現状より増大
- すべての人とモノがつながっているため、サイバー攻撃を受けた時の被害の影響範囲が広域
- サイバー空間での影響が、フィジカル空間に波及

1.2 節でも述べたとおり、サイバーフィジカルシステムでは、利用者の個人情報や、各種センサーで収集したデータが利用される。サイバー攻撃により、収集したデータの改ざんや、漏洩した時、事業継続への影響が及ぼされるだけでなく、場合によっては IoT 機器が誤動作して人命や社会インフラに影響を及ぼしてしまうなどの可能性がある。

また、人工知能（AI）がサイバー攻撃に利用されることにより、より広範かつ効果的、効率的な攻撃が可能になる可能性がある。

[20] 経済産業省、サイバー・フィジカル・セキュリティ対策 フレームワーク(案)、2019 年 3 月 14 日、http://www.meti.go.jp/press/2018/01/20190109001/20190109001-2.pdf

2. IoT 機器、AI 技術の活用に関するセキュリティ上の脅威

サイバーフィジカルシステムにおけるセキュリティ対策の検討に際し、サイバー攻撃の脅威を把握する必要がある。そこで、本章では IoT 及び AI に関するセキュリティ上の脅威について、実際のインシデントや研究の事例を整理するとともに、IoT サービスの提供者を対象に実施したアンケート調査の結果をまとめる。

2.1 サイバーフィジカルシステムに関するセキュリティ上の脅威に関する事例

本章では、サイバーフィジカルシステムに関するセキュリティ上の脅威について、IoT 及び AI を対象に事例を整理する。

2.1.1 IoT 機器や AI をターゲットにしたサイバー攻撃

(1) IoT 機器をターゲットにしたサイバー攻撃

国立研究開発法人 情報通信研究機構（NICT）の NICTER 観測レポート 2017[21]によると、IoT 機器へのサイバー攻撃は、2016 年頃から急速に増加している。また、2016 年以前は、単純な ID とパスワードで設定された IoT 機器に対して、パスワード設定の脆弱性（telnet や SSH のパスワード脆弱性等）を突いて侵入する攻撃が多くあったが、2017 年には、特定の IoT 機器や IoT 機器を活用したサービスの脆弱性を突いた高度な攻撃へ移行しつつある。表 2-1 に IoT の脆弱性に関する最新の動向を例示する。

なお、NICT では、上記の状況を踏まえ、脆弱な IoT 機器の調査及び、脆弱な IoT 機器を利用する利用者への注意喚起を行う「NOTICE（National Operation Towards IoT Clean Environment）」を 2019 年 2 月より開始した。[22]

[21] NICTER 観測レポート 2017 の公開、国立研究開発法人情報通信研究機構、2019 年 3 月 14 日、http://www.nict.go.jp/press/2018/02/27-1.html

[22] IoT 機器調査及び利用者への注意喚起の取組「NOTICE」の実施、国立研究開発法人 情報通信研究機構、2019 年 3 月 20 日、https://www.nict.go.jp/press/2019/02/01-1.html

表 2-1　IoT の脆弱性に関する最新の動向

名称	脆弱性の概要
Wi-Fi の KRACKs 脆弱性[23]	Wi-Fi のセキュリティプロトコルである WPA2 に脆弱性が発見された。 発見された脆弱性は、KRACKs（Key Reinstallation AttaCKs）と呼ばれ、鍵管理に関する脆弱性である。KRACKs を用いることで、Wi-Fi 端末機器とアクセスポイントの通信傍受や覗き見、通信の乗っ取り、改ざんが可能となる。 影響範囲は、Wi-Fi 端末機器の利用者である。
国際標準規格 IEEE 1149.1 （JTAG）の悪用[24]	JTAG では、バウンダリ・スキャン・アーキテクチャとそれにアクセスするためのシリアル・ポートが規格化されている。シリアル・ポートは、メモリ、CPU レジスタ、I/O レジスタの読み書き、ブレークポイント、実行トレース、データ変化の監視等のデバッグ用にも使用が可能である。そのため、機器の内部が暴露され、プログラムコードの書き換えが可能となる。

また、IoT 機器の脆弱性等を突いてサイバー攻撃が行われた 2017 年以降の事例を表 2-2 にまとめる。これらの被害のほかに、IoT 機器の脆弱性を突いてネットワークや超音波、音波を活用して攻撃コードを送りこみ、IoT 機器を通じて通信傍受や覗き見、通信の乗っ取り、改ざんを行うハッキングの事例も複数ある。具体的には自動車や、ドローン、交通システム（電光掲示板）、スマートスピーカ等が挙げられる。音波では可聴域以外の周波数を用いて、利用者に気づかれずに操作することも可能である。

表 2-2　2017 年以降に発生した IoT 機器をターゲットにしたサイバー攻撃の事例

事例		内容
IoT 機器を悪用した攻撃[25]	攻撃に利用されるマルウエア	IoTroop、IoT_reaper
	対象 IoT 機器	インターネットに接続された監視カメラを含む数百万台規模の IoT 機器
	被害	IoT 機器に搭載されたカメラを通じた覗き見、盗撮
制御系システムへのランサムウェア感染[25]	攻撃に利用されるマルウエア	ランサムウェア、WannaCry
	対象 IoT 機器	医療機関の制御系システム
	被害	患者の診療データベースへのアクセス制限が生じ、レントゲン撮影ができない等の被害が発生
	攻撃に利用されるマルウエア	ランサムウェアや Not Petya
	対象 IoT 機器	交通機関、ATM 等の制御系システム
	被害	システムの機能停止
IoT 機器の破壊[25]	攻撃に利用されるマルウエア	BrickerBot
	対象 IoT 機器	ログイン情報がデフォルトから変更していない IoT 機器
	被害	IoT 機器のファイルを破壊し、機器を使用不能

[23] WPA2 の脆弱性「KRACKs」、ほぼすべての Wi-Fi 通信可能な端末機器に影響、トレンドマイクロ株式会社、2019 年 3 月 14 日、https://blog.trendmicro.co.jp/archives/16162

[24] JTAG とは何か、CQ 出版株式会社、2019 年 3 月 14 日、http://www.cqpub.co.jp/dwm/contents/0027/dwm002700200.pdf

[25] 情報セキュリティ 10 大脅威 2018、情報処理推進機構 2019 年 3 月 14 日、https://www.ipa.go.jp/security/vuln/10threats2018.html

一方、IoT に関するセキュリティ上の脅威として、OWASP（Open Web Application Security Project）がまとめた IoT に関するセキュリティ上の 10 大脅威[26]がある（表 2-3）。

表 2-3　OWASP が提案する IoT に関するセキュリティ上の 10 大脅威

No.	脅威	概要
1	弱い、推測しやすい、またはハードコード化されたパスワード	設定インタフェースに telnet/ssh 等でログインする際のパスワードクラッキング
2	安全でないネットワークサービス	IoT 機器における不要ポートの開放
3	安全でないエコシステムインターフェイス	IoT 機器及び関連するサービスコンポーネントとの連携における通信や認証の安全性
4	サービスのアップデートメカニズムの欠如	パッチの適用状況を最新化しておくことが難しい
5	安全でないまたは古くなったコンポーネントの使用	製造コストを抑えるために、脆弱性のあるサポート切れの古いものを利用している場合がある
6	不十分なプライバシー保護	IoT サービスが保持する個人情報の保護
7	安全でないデータ転送と保存	暗号化されていない通信路でのデータ転送
8	デバイス管理の欠如	市場に展開されているデバイスの把握や監視、更新、サポートが難しい
9	安全でない初期設定	強度の低い初期設定パスワードの使用等
10	物理的強度の欠如	IoT 機器への物理的な攻撃や USB ポート等からの不正アクセス

(2)　AI をターゲットにしたサイバー攻撃

AI（深層学習、機械学習）をターゲットとしたサイバー攻撃には、ルール等を導くのに必要な教師データにノイズを与える攻撃手法と認識データにノイズを与える攻撃手法がある。表 2-4 に具体的な攻撃手法の例を示す。

表 2-4　AI ターゲットにした攻撃手法[27]

攻撃手法	内容
トレーニングセット・ポイズニング	AI がルール等を導くのに必要な教師データに不正なデータを入れ込む。 例えば、AI を利用したマルウエア検出エンジンに誤った教師データを入れ込み、マルウエアを検出できなくさせる手法。
アドバーサリアル・エクザンプル	認識させる画像データ等に誤検出を誘発させるようなノイズを加える。 例えば、交通標識にステッカーを貼り、「停止」を「速度規制」の交通標識に誤認識させて、自動運転等、社会生活に大きな悪影響を及ぼす可能性があると危険性が指摘されている。

[26] OWASP Internet of Things Project、 The OWASP Foundation、 2019 年 3 月 14 日、https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[27] ディープラーニングにもセキュリティ問題、日経 BP 社、2019 年 3 月 14 日、https://business.nikkei.com/atcl/report/15/061700004/111400232/?P=1

2.1.2　IoT 機器や AI 技術を活用したサイバー攻撃

(1)　IoT 機器を活用したサイバー攻撃

IoT 機器を活用したサイバー攻撃の多くは、IoT 機器をマルウエア感染させた後、同じ脆弱性を持つ IoT 機器を探索し、感染を繰り返し行うことで、被害を拡大させる攻撃を行う。表 2-5 に、具体的な事例を紹介する。

表 2-5　近年発生した主な IoT を利用したサイバー攻撃の事例（2017 年）

事例	内容
ボットに感染した IoT 機器による DDoS 攻撃	ボットネット化した IoT 機器からの DDoS（分散型サービス妨害）攻撃。2017 年に、Android アプリに組み込まれたマルウエア「WireX」による、スマートフォンからの大規模な DDoS 攻撃や、IoT 機器に感染するマルウエア「Mirai」による大規模な DDoS 攻撃が発生。
Bluetooth の脆弱性を利用した BlueBorne	Bluetooth の脆弱性を悪用して、ペアリングを実施することなく感染拡大する攻撃。公共の場所に設置されている IoT 機器が感染し、被害を拡大させる可能性がある。

(2)　AI 技術を活用したサイバー攻撃

Cornell University の「The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation」[28]によると、表 2-6 のような、AI（深層学習、機械学習）を利用した攻撃として、以下 3 つの脅威が指摘されている。

- 従来型の脅威の増幅
  攻撃の効率化、攻撃に用いる計算資源のスケーラビリティ増加、拡散の容易化等

- 新たな脅威の出現
  合成顔画像／合成音声を利用した攻撃、ロボットやドローンを利用した攻撃、IoT 機器の脆弱性を利用した攻撃等

- 典型的な攻撃の変容
  マルウエアの自動生成、攻撃対象の絞り込み、攻撃の匿名性の向上等

[28] The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation、Cornel l University、2019 年 3 月 14 日、https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

表 2-6　AI 技術を活用したサイバー攻撃

分類	サイバー攻撃の内容
デジタル	• ソーシャルエンジニアリングの自動化（フィッシングサイトのターゲット向けのカスタム自動生成） • 脆弱性探索の自動化（プログラムの脆弱性のパターン履歴から、未発見の脆弱性を見つけ出す） • ハッキング自動化（行動パターンからの攻撃対象の絞り込み自動化） • 人間になりすました DoS 攻撃 • 攻撃行動の自動化（ランサムウェアでの身代金徴収の自動化） • 機械学習を利用した攻撃ターゲットの優先順位付け
フィジカル	• 商用 AI システムをテロリストが攻撃に転用（ドローンや自動運転の乗り物） • 低スキルの攻撃者に専門的な高いスキルを付与 • 攻撃規模を大規模化する（多数の IoT 機器への攻撃） • 群衆攻撃（Swarming Attack）：分散ネットワークを形成する自律型ロボットが、広域をモニタリングして、協調的な攻撃を実施 • 時間と空間の概念を必要としない攻撃（攻撃を実施する物理システムと直接コミュニケーションしなくても自律的に攻撃を開始できる）
ソーシャル	• 自動化された監視システムが言論の自由を抑圧（画像認識や音声認識による広域監視活動の自動化） • リアリティの高い映像や音声によるフェイクニュース • 特定の個人をターゲットにした誹謗中傷キャンペーンの自動化 • SNS 等を利用した影響キャンペーン • Denial-of-information 攻撃（間違った情報を生成する攻撃） • 利用できる情報の操作

2.2　IoT 機器を用いたビジネス上の脅威と守るべき資産

本章では、IoT サービスの提供者を対象に実施したアンケート調査について述べる。なお、実施したアンケートの詳細は、添付資料に記載する。

2.2.1　IoT ビジネスにおける脅威

(1)　IoT ビジネスの利用者数

IoT ビジネスの利用者数について調査したところ、「1,000 人～10 万人未満」（26.6%）が最も多く、次いで「10 人～100 人未満」（22.8%）となった。また、最大利用者数は 10 億人といった回答があった。

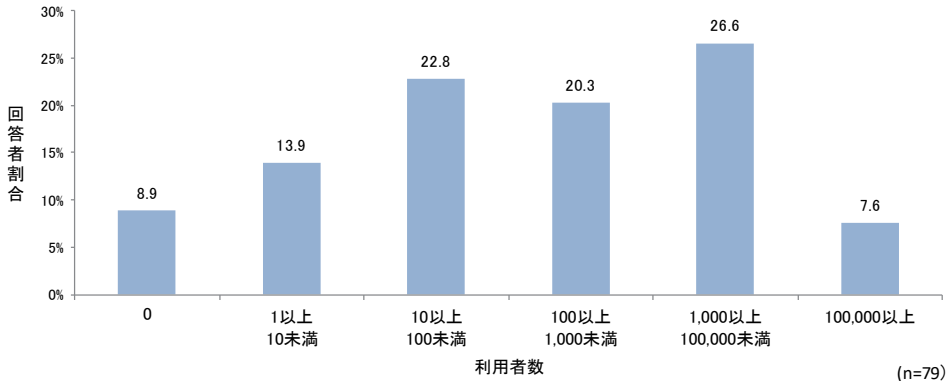


図 2-1　IoT ビジネスの利用者数

(2)　サイバー攻撃者の意図

各社が実施する IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者の意図について、想定される可能性を 5 段階で評価したところ、攻撃が想定されるのは「IoT ビジネスや利用者への業務妨害」（79.7%）、次いで、「個人情報や機密情報の窃取」（77.2%）、「マルウエア拡散」（72.2%）であった。

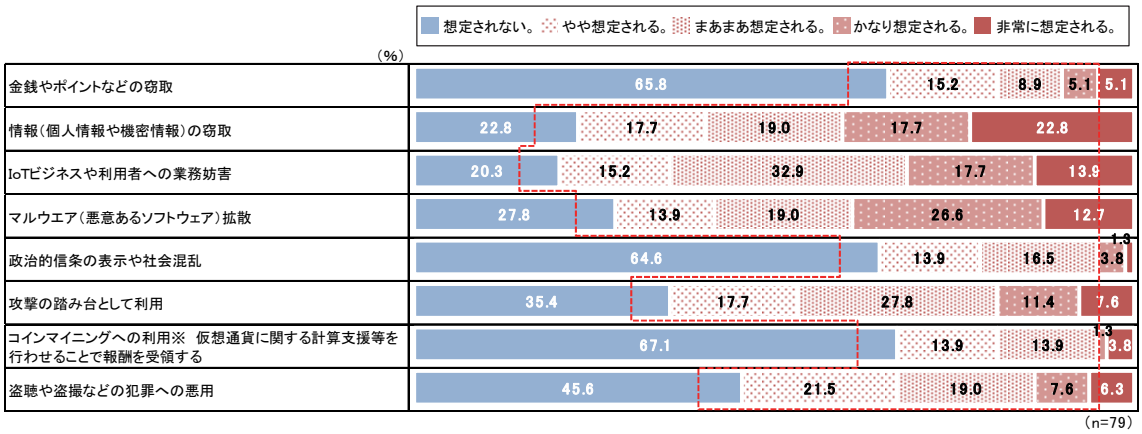


図 2-2　サイバー攻撃者の意図

その他には、以下のような意見があった。

- サービス等の利用権の不正取得
- IoT データの改竄
- 愉快犯
- 私怨
- 生産データの抜き取り及び加工技術の入手
- 個人情報の取得
- 工場、施設の運転データ取得　等

(3)　サイバー攻撃の方法

IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する方法について、想定される可能性を 5 段階で評価したところ、「ユーザアカウントやシステム管理者アカウントの不正利用」（83.5%）の回答が最も多く、次いで「マルウエア感染（遠隔操作）」（75.9%）であった。

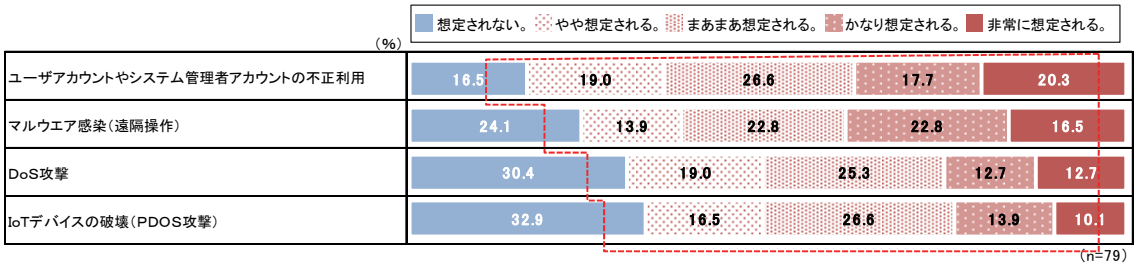


図 2-3　サイバー攻撃の方法

(4)　サイバー攻撃者が利用する界面

IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する界面について、想定される可能性を 5 段階で評価したところ、「センターサーバーとデバイス（あるいはエッジサーバー）との通信の脆弱性」（84.8%）の回答が最も多い結果となったが、他の脆弱性についても想定されるという回答が概ね 8 割以上となった。

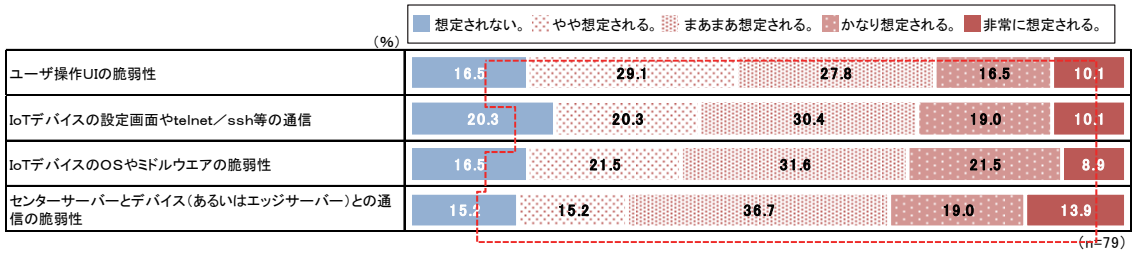


図 2-4　サイバー攻撃者が利用する界面

2.2.2　IoT ビジネスで守るべき資産

IoT ビジネスで守るべき資産をランク分けで調査したところ、最も守るべき資産は「人命」（79.7%）となった。

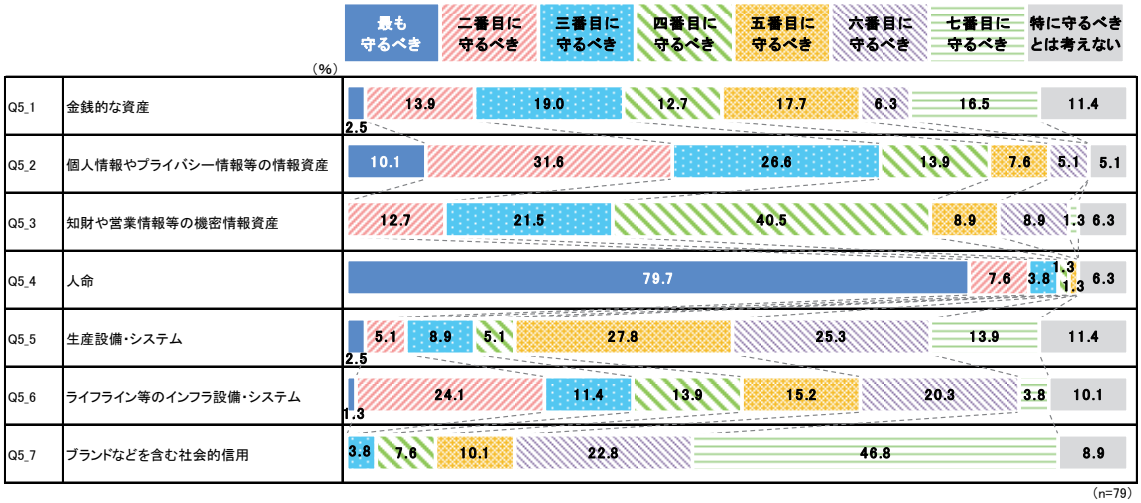


図 2-5　IoT ビジネスで守るべき資産

また、最も守るべき資産を 7 点、二番目に守るべき資産を 6 点、三番目に守るべき資産を 5 点、四番目に守るべき資産を 4 点、五番目に守るべき資産を 3 点、六番目に守るべき資産を 2 点、七番目に守るべき資産を 1 点、特に守るべきとは考えないを 0 点と点数化した結果、「人命」に次ぐものとして「個人情報やプライバシー情報等の情報資産」、「知財や営業情報等の機密情報資産」といった順になった。

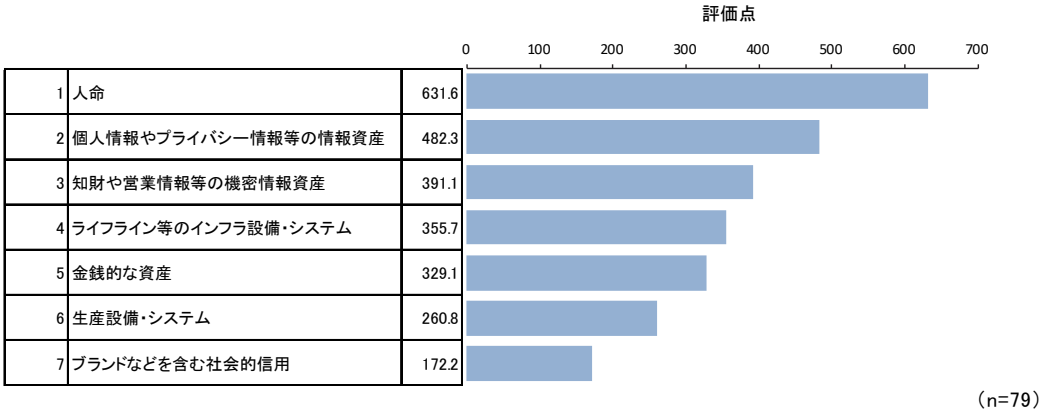


図 2-6　IoT ビジネスで守るべき資産の評価点

3. IoT サービスのリスク評価モデルの検討

1 章では、サイバー空間とフィジカル空間が融合した社会におけるセキュリティ上の課題を整理し、2 章では、サイバー空間とフィジカル空間が融合した社会の実現に向け必要となるツールである IoT 機器や AI 技術等におけるセキュリティ上の脅威や、IoT 機器を用いたビジネスと守るべき資産について調査を行った。

本章では、上記の結果を踏まえ、サイバー空間とフィジカル空間が融合した社会を想定し、IoT 機器をターゲットに、AI 技術を活用して行うサイバー攻撃に対する攻撃シナリオとリスク評価モデルを提案する。

3.1 サイバー空間とフィジカル空間が融合した社会にて想定されるサイバー攻撃

IoT サービスにおけるリスク評価モデルを検討するために、サイバー空間とフィジカル空間が融合した社会にて想定される攻撃シナリオを検討した。具体的には、サイバー空間とフィジカル空間が融合した社会にて想定される攻撃者の行動をサイバー・キル・チェーン[29]の考え方に基づき整理した。

3.1.1 サイバー空間とフィジカル空間が融合した社会にて想定される攻撃者の行動

標的型攻撃の攻撃手法として代表的な、サイバー・キル・チェーン [29] の 7 つのステップ（偵察、武器化、配送、攻撃、インストール、遠隔制御、目的の達成）を参考に、サイバー空間とフィジカル空間が融合した社会にて想定される攻撃者の行動について検討した結果を表 3-1 に示す。

攻撃手段や考えは現状と変化はないが、攻撃の処理速度やターゲットが、現状以上に拡大されることが予想され、IoT サービスを実施するにあたっては、事業者ごとにこれらを防ぐ取り組みがなされているか、評価できるモデルを検討する必要があるものと考えられる。

[29] THE Cyber Kill Chain®、lockheedmartin、2019 年 3 月 14 日、
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
※THE Cyber Kill Chain は、米国 Lockheed Martin Corporation の米国における登録商標または商標です。

表 3-1　攻撃者の行動についての検討結果

ステップ	攻撃者の行動
偵察 （攻撃ターゲットの情報収集）	データ処理速度の向上により、個人サイトを含めた不特定多数のサイトがターゲット対象になる可能性がある。 モニタリング作業の自動化が可能となる。 音声解析による情報収集が可能となる。 攻撃先のリストアップの自動化が可能となる。
武器化 （攻撃コードやマルウエアの作成）	企業側の対策が追い付かないスピードで、個人向けのマルウエア（デバイス固有のマルウエア）、攻撃コードの作成が可能になる。 自己学習により、手動で行うより効率的に行動が可能なマルウエアの作成が可能となる。
配送 （作成した攻撃コードやマルウエアの送付）	ユーザの行動パターンを踏まえ、ユーザがメールを展開させやすいWebサイトへアクセスしたいと思う文章の作成が可能となる。
攻撃（攻撃コードの実行）	従来型の攻撃からの大きな変化は無いものと想定される。
インストール （マルウエアのインストール）	
遠隔制御 （ユーザ端末を遠隔操作）	端末の自動（遠隔）操作が可能となる。
目的の達成 （情報をユーザ端末から窃取）	従来型の攻撃からの大きな変化は無いものと想定される。

3.1.2　攻撃シナリオ

2 章で述べたセキュリティ上の課題を踏まえ、サイバー空間とフィジカル空間が融合した社会にて想定される攻撃シナリオを以下に例示する。

(1)　シナリオ 1: 音声で制御可能な IoT 機器を一斉に誤動作させる攻撃

【シナリオ１】

コネクテッドカー（車種：○○）を製造販売しているある大手自動車会社が、人間の音声でサイドミラーの調整ができる新機能を搭載した自動車を販売したところ、ある日、同社への以下のような脅迫メールがあった。

「3 日以内に****ビットコインを支払わなければ、おたくの会社が製造販売しているクルマを近いうちに一斉に遠隔操作してやる。多くの人命が失われるかもしれない。これは脅しではない。」

1 週間後、政府の運輸安全委員会から、「同社が製造販売しているコネクテッドカー（車種：○○）が、いろいろな地域で同時多発的に遠隔操作されたことが原因で人身事故が発生した」との連絡を受けた。

その後、原因調査を行ったが、コネクテッドカー（車種：○○）からは、攻撃に利用されるような脆弱性やマルウエア感染の痕跡は発見できなかった。また、事故を起こした利用者からは、「サイドミラーがいつのまにか動いていたため、車線変更時に後方確認ができなかった。」という共通した証言が得られた。

1 週間後、攻撃者から、「3 日以内に****ビットコインを支払わなければ、もう一度、同じ攻撃をしてやる。」との脅迫があった。

【攻撃者の目的】
遠隔操作権限を奪取することにより、企業や政府を脅迫し、身代金を得る。

【AI を利用した攻撃の手口】
攻撃者は、偽装した無料スマートフォン用アプリ（コネクテッドカーに超音波による音声コマンドを遠隔から発信する）をアプリケーションダウンロードサイトに公開し、利用者にインストールさせる。

攻撃者は、ある時間帯に、上記のスマートフォン用アプリを経由して超音波によるコマンドを送信。たまたま同社製造のコネクテッドカーに乗車していた利用者のスマートフォン経由で音声認識システムがコマンドを受信し、コネクテッドカーが遠隔操作される。

【攻撃対象、または攻撃に利用される IoT 機器】
音声認識により制御可能な IoT 機器や、スマートスピーカにより操作 IoT 機器。

(2) シナリオ 2: 家電製品からキャプチャした情報に基づく標的型攻撃

【シナリオ２】
A さんは、海外会社が製造販売している安価なスマートスピーカを購入した。
しばらくすると、SNS 上で最近知り合った、日本酒を愛好するグループのひとりから、お勧めの日本酒を紹介するサイトを紹介してもらい、そのサイトにアクセスした。
その後、しばらくしてから、海外のショッピングサイトから届いた明細に、発注していない商品が、身に覚えの無い宛先に送られていることがわかった。

【攻撃者の目的】
金銭の窃取や偽装発注を行う。

【AI を利用した攻撃の手口】
会話内容の音声認識結果をサーバに送信する機能が埋め込まれたスマートスピーカを販売し、購入者（攻撃ターゲット）にオンラインユーザ登録してもらう（メールアドレスを登録してもらう）。

スマートスピーカを購入した攻撃ターゲットの日常会話の内容（音声認識された結果）を自動解析し、攻撃ターゲットに興味を持ってもらえそうなサイトに誘導する内容の標的型攻撃メールの文章が自動生成されて送信される。

上記の標的型攻撃メールに記載されたサイトにアクセスすると、攻撃ターゲットの PC がマルウエアに感染（このマルウエアはウイルス対策ソフトに検知されないようにカスタマイズされている）。保存されているアカウント情報が攻撃者により窃取され、ショッピングサイトから偽装発注が行われる。

【攻撃対象、または攻撃に利用される IoT 機器】
スマートスピーカなどの家電製品（カメラやマイクを内蔵したもの）。

(3)　シナリオ 3: モザイクアプローチによる個人情報収集の自動化

【シナリオ３】
A さんは、行きつけの近所の居酒屋やレストランで食べた料理の写真は、いつも SNS にアップしている。
ある日、高級外車を購入したので、休日に、自宅近くの駐車場にて、購入した車とともに撮影した写真を SNS にアップした。
数日後、購入したばかりの高級外車が何者かにより盗難されていた。

【攻撃者の目的】
金品や高額品の窃取。

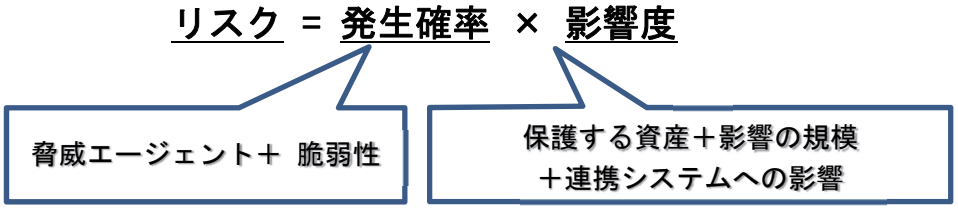
【AI を利用した攻撃の手口】
インターネット上に公開された SNS に投稿された膨大な量の写真データを自動的に画像解析することにより、写真に写り込んだ背景などを手掛かりに投稿者（攻撃ターゲット）の住所や高額な所持品を特定する。
車の所有者の現在の位置情報を SNS の投稿から推測して尾行し、スマートキーから発信されている電波を傍受して他の仲間に転送して車を開錠、エンジンを始動させて盗難する（リレーアタック）。

【攻撃対象、または攻撃に利用される IoT 機器】
スマートフォンや自動車（スマートキー）。

3.2　サイバー攻撃に対するリスク評価モデル案

3.2.1　リスク評価モデル案

OWASP（Open Web Application Security Project）[30]等の公開資料によると、リスクマネジメントにあたっては、「発生確率」、「影響度」毎に評価指標を設定の上で、以下の考え方によりリスクの大きさを把握するものとしている。



[30] OWASP Risk Rating Methodology(Japanese)、The OWASP Foundation、2018 年 12 月 25 日、https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology(Japanese)

本調査においても、上記の算定式を基本として IoT サービスにおけるリスク評価を実施することとし、「発生確率」、「影響度」毎の評価指標、評価基準は、公開資料やアンケート結果を用いて設定した。

「発生確率」、「影響度」毎の評価指標は、表 3-2 のとおり。評価指標に対する評価基準（パラメータ）は、3.2.2 項に示す。

表 3-2　発生確率と影響度の評価指標

区分	評価指標		
	大分類	中分類	小分類
発生確率	脅威エージェント	攻撃者の動機と意図	想定される攻撃意図や目的
		攻撃方法	利用される攻撃手段
		攻撃機会	IoT 機器の共有有無
	脆弱性	アクセス制御	認証方式
			ポート制御
			設定インタフェース
		パッチ適用タイミング	パッチ適用のタイミング
影響度	事業への影響	保護資産	収集&利用するデータの種類
		影響の規模	市場にあるデバイス数
			利用者数
		連携システムへの影響	連携システムの有無

3.2.2　評価指標毎のパラメータ

(1)　発生確率

「発生確率」は、以下の方法で算定し、IoT サービスが脅威を受ける発生確率を評価する。「脅威エージェント」の評価基準は 1)、「脆弱性」の評価基準は 2)のとおり。

発生確率 ＝ 脅威エージェント ＋ 脆弱性

1)　脅威エージェント

表 3-2 より、脅威エージェントの評価指標は表 3-3 のとおり。

重み付けした評価指標を以下のとおり算出した結果を、脅威エージェントの評価基準値として採用した。

脅威エージェント＝ 10×｛（攻撃者の動機と意図 ＋ 攻撃方法 ＋ 攻撃機会）÷43｝

※正規化のため”43”で除している。

表 3-3　脅威エージェントの評価指標（表 3-2 より一部抜粋）

評価指標		
大分類	中分類	小分類
脅威エージェント	攻撃者の動機と意図	想定される攻撃意図や目的
	攻撃方法	利用される攻撃手段
	攻撃機会	IoT 機器の共有有無

表 3-3 の小分類毎の評価基準は、表 3-4 のとおり。

例えば、「想定される攻撃意図や目的」の場合、アンケートの回答が図 3-4 であれば、5 段階評価のうち最も評価が高い「マルウエア（悪意あるソフトウェア）拡散」を採用し、表 3-4 より、「マルウエア（悪意あるソフトウェア）拡散」の「設問に対する重み」である「2」と「マルウエア（悪意あるソフトウェア）拡散」の「設問に対する評価の重み」である「4」を乗じ、「想定される攻撃意図や目的」の評価基準値を算出する。「利用される攻撃手段」に関しても同様の考えで、評価基準値を算出する。

※図 3-4 の回答にて、5 段階評価のうち最も評価が高い設問が複数ある場合は、「設問に対する重み」が高い順に、採用する。

また、「IoT 機器の共有有無」の場合は、図 3-3 の回答が「共有がある」を選択した場合、「設問に対する重み」である「3」を「IoT 機器の共有有無」の評価基準値として採用する。

さらに、上記の合計値が「22」となった時、10 段階で適正化した「5」を脅威エージェントの評価基準値として採用する。

表 3-4　脅威エージェントのパラメータ

小分類	算出方法	設問		設問に対する評価	
		重み	設問内容	重み	評価
想定される攻撃意図や目的	図 3-1 のアンケート結果を用いる。 「金銭やポイントなどの窃取」等、攻撃者の意図のうち、回答者が選択した設問から最も評価が高い設問を採用。 採用した設問を用い、以下の方法で算出した値を評価基準値とした。 「設問に対する重み」× 「設問に対する評価の重み」	4	金銭やポイントなどの窃取	0	想定されない
				1	やや想定される
				2	まあまあ想定される
				3	かなり想定される
				4	非常に想定される
		3	情報（個人情報や機密情報）の窃取	同上 （「金銭やポイントなどの窃取」と同様）	
		3	IoT ビジネスや利用者への業務妨害		
		2	マルウエア（悪意あるソフトウェア）拡散		
		1	政治的信条の表示や社会混乱		
		3	攻撃の踏み台として利用		
		3	コインマイニングへの利用		
		5	盗聴や盗撮などの犯罪への悪用		
利用される攻撃手段	図 3-2 のアンケート結果を用いる。 「ユーザアカウントやシステム管理者アカウントの不正利用」等、攻撃者の攻撃方法のうち、回答者が選択した設問から最も評価が高い設問を採用。 採用した設問を用い、以下の方法で算出した値を評価基準値とした。 「設問に対する重み」× 「設問に対する評価の重み」	4	ユーザアカウントやシステム管理者アカウントの不正利用	0	想定されない
				1	やや想定される
				2	まあまあ想定される
				3	かなり想定される
				4	非常に想定される
		3	マルウエア感染（遠隔操作）	同上 （「ユーザアカウントやシステム管理者アカウントの不正利用」と同様）	
		5	DoS 攻撃		
		1	IoT 機器の破壊（PDoS 攻撃）		
		3	ユーザ操作 UI の脆弱性		
		4	IoT 機器の設定画面や telnet/ssh 等の通信		
		2	IoT 機器の OS やミドルウエアの脆弱性		
		2	センターサーバーとデバイス（あるいはエッジサーバー）との通信の脆弱性		
IoT 機器の共有有無	図 3-3 のアンケート結果を用いる。 回答者が選択した設問の重みを評価基準値として採用。	3	共有がある	—	
		1	共有がない		

※アンケートにて、1 問でも「未定、わからない、IoT 機器がない」を選択した回答者の結果は、評価対象外とした。

図 3-1　アンケート設問（Q3-1）

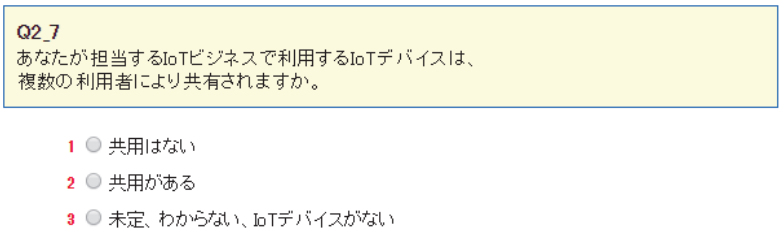
Q3_3
あなたが担当するIoTビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する方法について、
次の項目に関して想定される可能性を5段階で評価してください。
(それぞれひとつずつ)

	回答方向	5 非常に想定される。	4 かなり想定される。	3 まあまあ想定される。	2 やや想定される。	1 想定されない。
1	ユーザアカウントやシステム管理者アカウントの不正利用	5	4	3	2	1
2	マルウエア感染(遠隔操作)	5	4	3	2	1
3	DoS攻撃	5	4	3	2	1
4	IoTデバイスの破壊(PDOS攻撃)	5	4	3	2	1

Q3_5
あなたが担当するIoTビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する界面について、
次の項目に関して想定される可能性を5段階で評価してください。
(それぞれひとつずつ)

	回答方向	5 非常に想定される。	4 かなり想定される。	3 まあまあ想定される。	2 やや想定される。	1 想定されない。
1	ユーザ操作UIの脆弱性	5	4	3	2	1
2	IoTデバイスの設定画面やtelnet/ssh等の通信	5	4	3	2	1
3	IoTデバイスのOSやミドルウエアの脆弱性	5	4	3	2	1
4	センターサーバーとデバイス(あるいはエッジサーバー)との通信の脆弱性	5	4	3	2	1

図 3-2　アンケート設問（Q3-3、Q3-5）



Q2_7
あなたが担当するIoTビジネスで利用するIoTデバイスは、
複数の利用者により共有されますか。

1 共用はない
2 共用がある
3 未定、わからない、IoTデバイスがない

図 3-3　アンケート設問（Q2-7）

Q3_1
あなたが担当するIoTビジネスに対してサイバー攻撃を仕掛けてくる攻撃者の意図について、
次の項目に関して想定される可能性を5段階で評価してください。
(それぞれひとつずつ)

	回答方向	5 非常に想定される。	4 かなり想定される。	3 まあまあ想定される。	2 やや想定される。	1 想定されない。
1	金銭やポイントなどの窃取	5	4●	3	2	1
2	情報(個人情報や機密情報)の窃取	5	4●	3	2	1
3	IoTビジネスや利用者への業務妨害	5	4	3●	2	1
4	マルウエア(悪意あるソフトウェア)拡散	5●	4	3	2	1
5	政治的信条の表示や社会混乱	5	4	3	2	1●
6	攻撃の踏み台として利用	5	4	3	2	1●
7	コインマイニングへの利用 ※仮想通貨に関する計算支援等を行わせることで報酬を受領する	5	4	3	2	1●
8	盗聴や盗撮などの犯罪への悪用	5	4	3	2	1●

図 3-4　アンケート回答例

2)　脆弱性

表 3-2 より、脆弱性の評価指標は表 3-5 のとおり。
重み付けした評価指標を以下のとおり算出した結果を、脆弱性の評価基準値として採用した。

脆弱性 ＝ 10×｛（アクセス制御 ＋パッチ適用タイミング）÷20）｝

※正規化のため"20"で除している。

表 3-5　脆弱性の評価指標（表 3-2 より一部抜粋）

評価指標		
大分類	中分類	小分類
脆弱性	アクセス制御	認証方式
		ポート制御
		設定インタフェース
	パッチ適用タイミング	パッチ適用のタイミング

表 3-5 の小分類毎の評価基準は、表 3-6 のとおり。

例えば、「認証方式」の場合、図 3-5 で「ID とパスワードの利用」を選択し、さらに、図 3-6 より、初期パスワードの設定方法を「個々の IoT 機器で異なる初期パスワードを設定している」と選択、パスワードの変更の有無にて「パスワードは変更することもできる」を選択した時、表 3-6 で設定されている重みから 1.05（＝3×0.5×0.7）を「認証方式」の評価基準値として採用する。
その他の算出方法は、「脅威エージェント」と同様である。

表 3-6　脆弱性のパラメータ

<table>
<tr><th rowspan="2">小分類</th><th rowspan="2">算出方法</th><th colspan="2">設問 1</th><th colspan="2">設問 2</th><th colspan="2">設問 3</th></tr>
<tr><th>重み</th><th>設問 1 内容</th><th>重み</th><th>設問 2 内容</th><th>重み</th><th>設問 3 内容</th></tr>
<tr><td rowspan="6">認証方式</td><td rowspan="6">図 3-5、図 3-6 のアンケート結果を用いる。
回答者が選択した設問の重みを評価基準値として採用。
ただし、「ID とパスワードを利用」と「上記を含む複数（多要素）を利用」の回答があった場合は、設問 1 の重みに設問 2、設問 3 の値を乗じ、算出した値を評価基準値として採用。</td><td rowspan="3">3</td><td rowspan="3">ID とパスワードを利用</td><td>1</td><td>IoT 機器で共通の初期パスワードを設定している</td><td>1</td><td>パスワードの変更はできない</td></tr>
<tr><td>0.5</td><td>個々の IoT 機器で異なる初期パスワードを設定している</td><td>0.7</td><td>パスワードは変更することもできる</td></tr>
<tr><td>0.5</td><td>利用者ごとに異なる初期パスワードを設定している</td><td>0.5</td><td>初期パスワードからの変更を必須としている</td></tr>
<tr><td>1</td><td>電子証明書を利用</td><td colspan="4">—</td></tr>
<tr><td>1</td><td>生体認証を利用</td><td colspan="4">—</td></tr>
<tr><td>1</td><td>上記を含む複数（多要素）を利用</td><td colspan="4">同上
（「ID とパスワードを利用」と同様）</td></tr>
<tr><td>5</td><td>アクセス制御なし</td><td colspan="4">—</td></tr>
<tr><td rowspan="2">ポート制御</td><td rowspan="2">図 3-7 のアンケート結果を用いる。
回答者が選択した設問の重みを評価基準値として採用。</td><td>1</td><td>ポート制御している</td><td colspan="4">—</td></tr>
<tr><td>5</td><td>ポート制御していない</td><td colspan="4">—</td></tr>
<tr><td rowspan="4">設定インタフェース</td><td rowspan="4">図 3-8 のアンケート結果を用いる。
回答者が選択した設問の重みを評価基準値として採用。</td><td>5</td><td>インターネットを介してアクセス</td><td colspan="4">—</td></tr>
<tr><td>1</td><td>ローカルネットワークを介してアクセス</td><td colspan="4">—</td></tr>
<tr><td>1</td><td>ネットワークを介さず直接接続してアクセス</td><td colspan="4">—</td></tr>
<tr><td>1</td><td>設定ユーザーインターフェースはない</td><td colspan="4">—</td></tr>
<tr><td rowspan="6">パッチ適用のタイミング</td><td rowspan="6">図 3-9 のアンケート結果を用いる。
回答者が選択した設問の重みを評価基準値として採用。
ただし、「利用者が適用を行う」、「利用者にかかわらず強制的に適用する」の回答があった場合は、設問 1 の重みに設問 2 の値を乗じ、算出した値を評価基準値として採用。</td><td>0</td><td>パッチの適用は必要がない</td><td colspan="4">—</td></tr>
<tr><td>5</td><td>パッチの適用はしない（できない）</td><td colspan="4">—</td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">利用者が適用を行う</td><td>0.5</td><td>すべてのデバイスを対象とする</td><td colspan="2">—</td></tr>
<tr><td>0.7</td><td>一部を除いた大部分のデバイスを対象とする</td><td colspan="2">—</td></tr>
<tr><td>1</td><td>一部のデバイスのみを対象とする</td><td colspan="2">—</td></tr>
<tr><td>1</td><td>利用者にかかわらず強制的に適用する</td><td colspan="4">同上
（「利用者が適用を行う」と同様）</td></tr>
</table>

※アンケートにて、1 問でも「未定、わからない、IoT 機器がない」を選択した回答者の結果は、評価対象外とした。

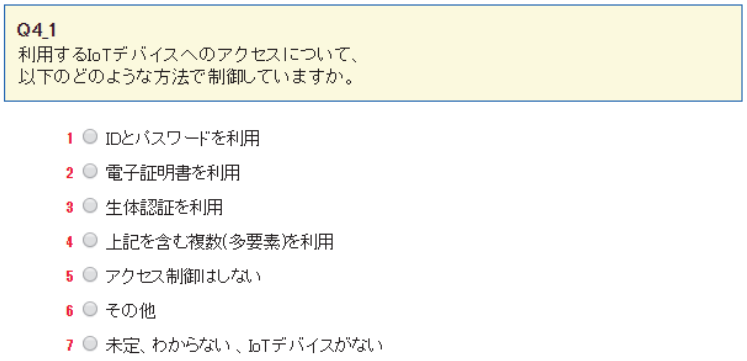


図 3-5　アンケート設問（Q4-1）

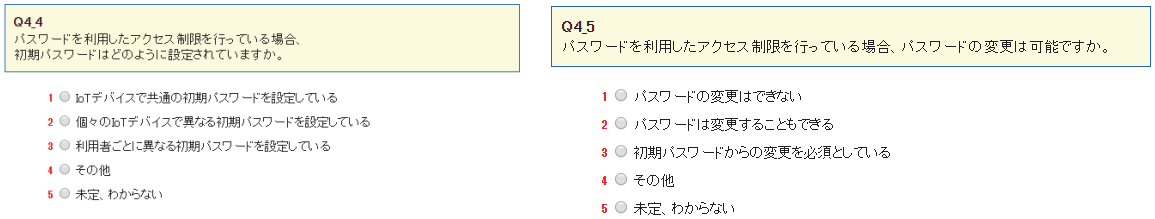


図 3-6　アンケート設問（Q4-4、Q4-5）

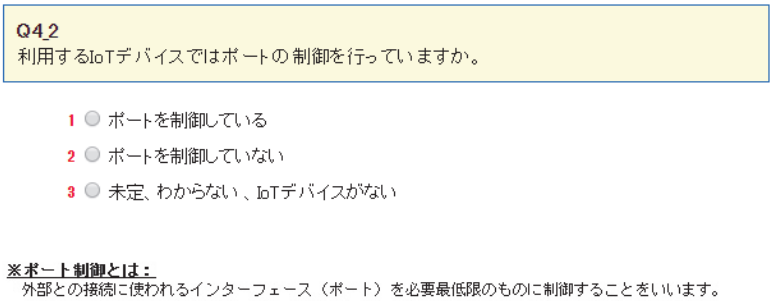


図 3-7　アンケート設問（Q4-2）

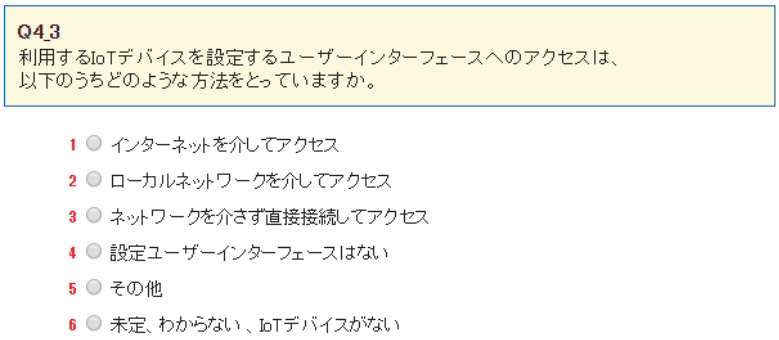


図 3-8　アンケート設問（Q4-3）

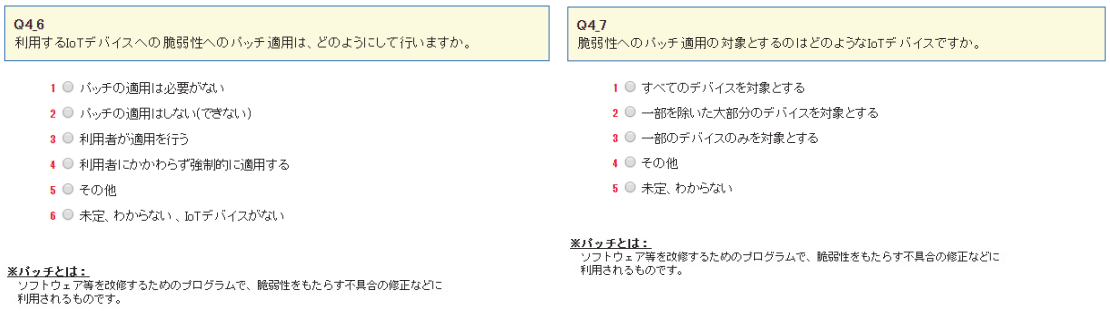


図 3-9　アンケート設問（Q4-6、Q4-7）

(2) 影響度

「影響度」では、事業への影響を評価する。

表 3-2 より、事業への影響の評価指標は表 3-7 のとおり。

重み付けした評価指標を以下のとおり算出した結果を、影響度の評価基準値として採用した。

影響度 ＝ 20×｛（保護資産 ＋ 影響の規模 ＋ 連携システムへの影響）÷20｝

表 3-7 事業への影響の評価指標（表 3-2 より一部抜粋）

評価指標		
大分類	中分類	小分類
事業への影響	保護資産	収集&利用するデータの種類
	影響の規模	市場にあるデバイス数
		利用者数
	連携システムへの影響	連携システムの有無

表 3-7 の小分類毎の評価基準は、表 3-8 のとおり。

例えば、アンケート回答者が図 3-10 で「パーソナルデータ※を含む情報（個人の氏名や画像、位置情報、ヘルスケアデータ等）」、図 3-11 でデバイス数を「1,000 台」、利用者数を「1,000 人」、連携システムの有無を「連携はない」と選択した場合は、表 3-8 で設定した重み付けより、「収集&利用するデータの種類」の評価基準は「4」、「市場にあるデバイス数」の評価基準は「3」、「利用者数」の評価基準は「3」、「連携システムの有無」の評価基準は「1」となり、合計値は「11」となる。これを 20 段階で正規化した値（「11」）を、影響度の評価基準値として採用する。

表 3-8 影響度のパラメータ

小分類	算出方法	設問	
		重み	設問内容
収集&利用するデータの種類	図 3-10 のアンケート結果を用いる。 回答者が選択した設問の重みを評価基準値として採用。	4	パーソナルデータ※を含む情報 （個人の氏名や画像、位置情報、ヘルスケアデータ等）
		2	パーソナルデータ※を含まない情報 （工場のセンサー情報、自社製品につけたセンサー情報等）
		5	上記の両方を含む情報
市場にあるデバイス数	図 3-11 のアンケート結果を用いる。 回答者が選択した設問の重みを評価基準値として採用。	1	0~10 台
		2	11~100 台
		3	101~1,000 台
		4	1,001~100,000 台
		5	100,001 台以上
利用者数	図 3-11 のアンケート結果を用いる。 回答者が選択した設問の重みを評価基準値として採用。	1	0~10 人
		2	11~100 人
		3	101~1,000 人
		4	1,001~100,000 人
		5	100,001 人以上
連携システムの有無	図 3-12 のアンケート結果を用いる。 回答者が選択した設問の重みを評価基準値として採用。	1	連携はない
		5	連携がある

※アンケートにて、1 問でも「未定、わからない、IoT 機器がない」を選択した回答者の結果は、評価対象外とした。

Q2_2
あなたが担当するIoTビジネスで収集、または利用する(購入も含む)データ種類について、
最も当てはまるものをお選びください。

1 パーソナルデータ※を含む情報
（個人の氏名や画像、位置情報、ヘルスケアデータ等）
2 パーソナルデータ※を含まない情報
（工場のセンサー情報、自社製品につけたセンサー情報等）
3 上記の両方を含む情報
4 収集する情報は現在未定、わからない

※パーソナルデータとは：
個人情報（氏名、生年月日等）に加え、
個人を識別することが可能な情報（位置情報や購買履歴等）も含むデータです。

図 3-10　アンケート設問（Q2-2）

Q2_9
あなたが担当するIoTビジネスの利用者数を概数の整数でお答えください。
(おおよその人数で結構です)

[　　] 人

Q2_10
あなたが担当するIoTビジネスで利用するIoTデバイス数を概数の整数でお答えください。
(おおよその台数で結構です。また、IoTデバイスがない場合は、0とお答えください。)

[　　] 台

図 3-11　アンケート設問（Q2-9、Q2-10）

Q2_8
あなたが担当するIoTビジネスのシステムやデータは、
他のサービスやシステムとの連携がありますか。

1 連携はない
2 連携がある
3 未定、わからない

図 3-12　アンケート設問（Q2-8）

3.3　リスク評価モデル案の試行

アンケート結果より、IoT 機器を用いて IoT ビジネスを展開あるいは展開予定の事業者（計 32 事業者）の回答を用いて、3.2 節で提案したリスク評価モデル試行した。

(1)　属性別

1)　属性毎の平均リスク評価結果

業種別の平均値で整理したところ、情報通信業の方が製造業より発生確率・影響度ともに、リスクが低い結果となった。

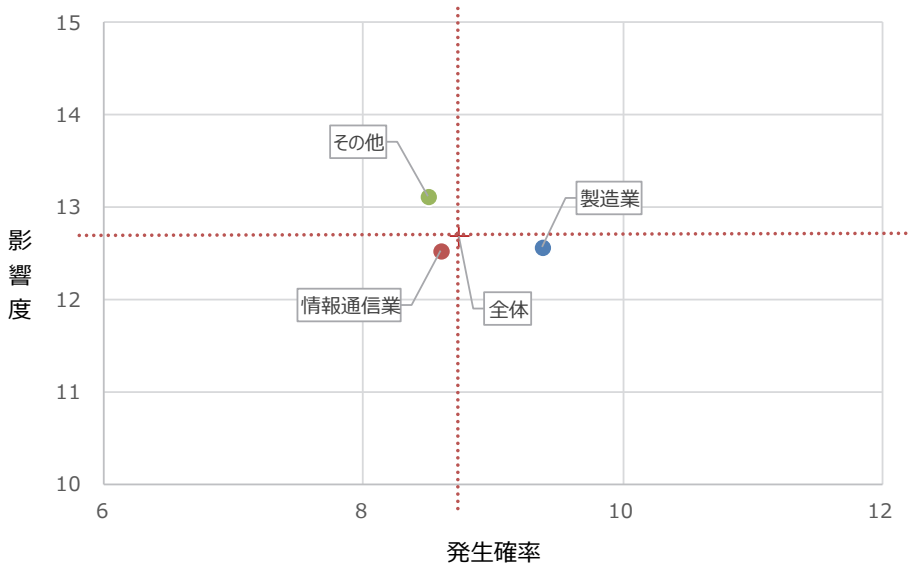


図 3-13　業種別リスク評価結果

※破線は、影響度及び発生確率の全体の平均値

2)　回答者毎のリスク評価結果

業種別の平均値を回答者別に整理した結果、製造業では概ね類似の傾向にあるのに対し、情報通信業は影響度・発生確率がともに低いと回答する事業者がいる一方で、どちらも高いと回答する事業者がいた。情報通信業では取り扱う情報内容が多様であることが伺える。

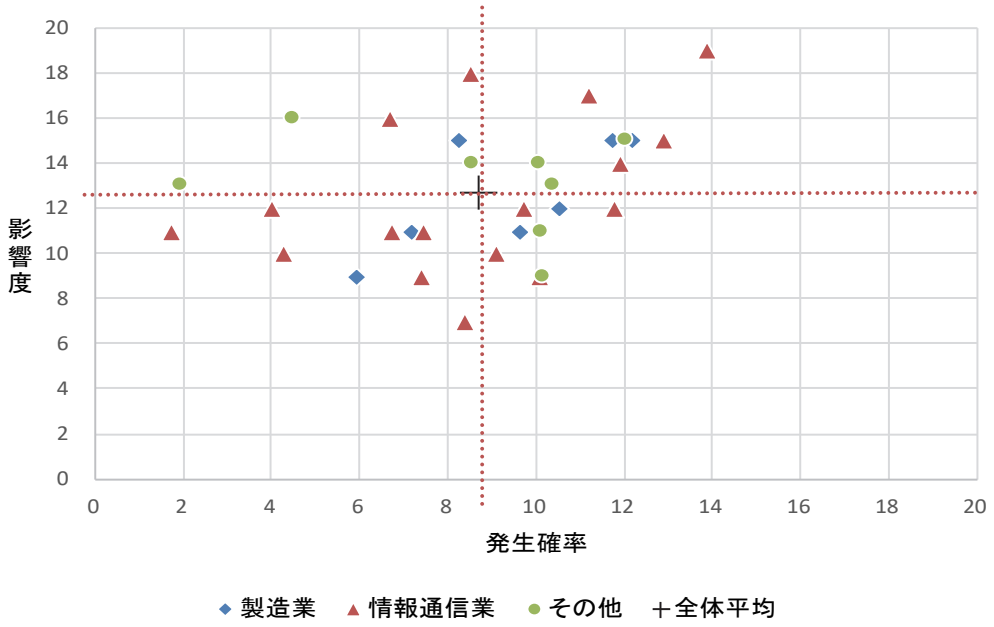


図 3-14　回答別リスク評価結果

※破線は、影響度及び発生確率の全体の平均値

3)　平均別、最大・最小別リスク評価結果

業種別にリスク値を平均値化した結果、大きな差はないといった結果となった。

一方、製造業の最大値・最小値の差は全体平均と比較しても小さく、情報通信業は全体平均と同程度の傾向を示した。

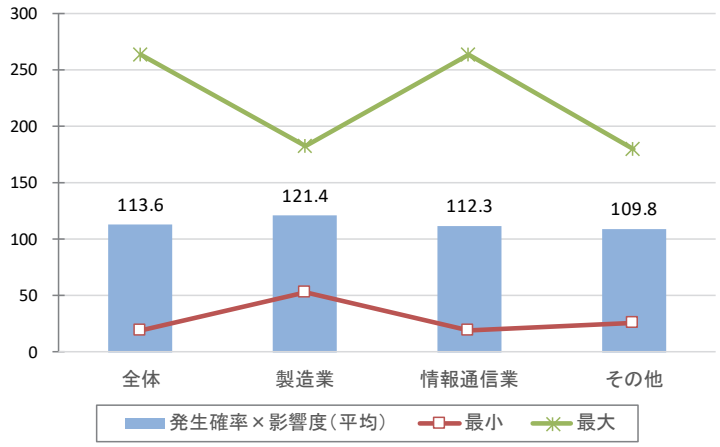


図 3-15　業種別リスク評価結果

4)　パラメータ別リスク評価結果

脅威エージェント（攻撃者の動機と意図、攻撃方法、攻撃機会）、脆弱性（認証方式、ポート制御、設定インタフェース、パッチ適用タイミング）、事業への影響（保護資産、市場にあるデバイス数、利用者数、連携システムへの影響）を 5 段階で正規化した値を用い、各評価指標に対する傾向を整理した。

業種別に整理した結果、情報通信業は全体平均のバランスと概ね一致するといった結果となった。

一方、製造業は「攻撃方法」・「利用者数」・「市場にあるデバイス数」、その他の業種では「保護資産」・「連携システムの影響」が全体平均よりリスク値が高い結果となった。

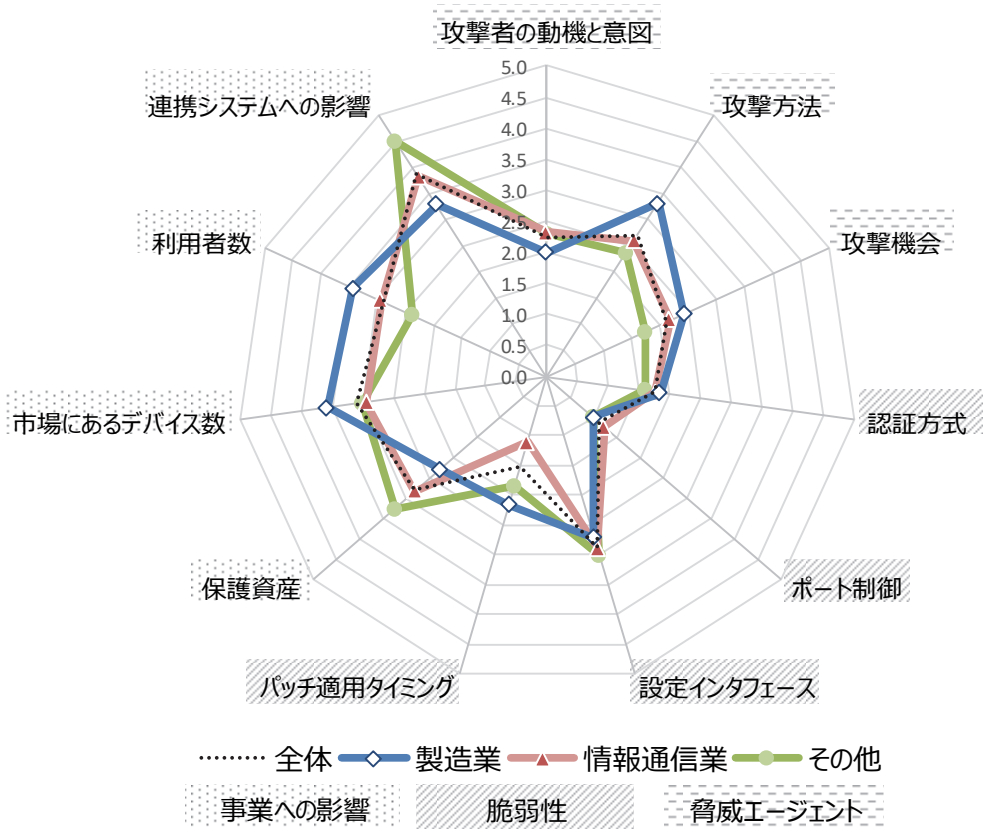


図 3-16　事業への影響、脆弱性、脅威エージェント別結果（属性別）

(2)　収集・利用する IoT データ分野別

1)　収集・利用する IoT データ分野毎の平均リスク評価結果

収集・利用する IoT データ分野別の平均値を整理した結果、「ヘルスケア・生命科学」のデータを利用・収集する事業者のリスクは、他のデータを扱う事業者と比較してサイバー攻撃を受けるリスクが低めの傾向にあるように見える。

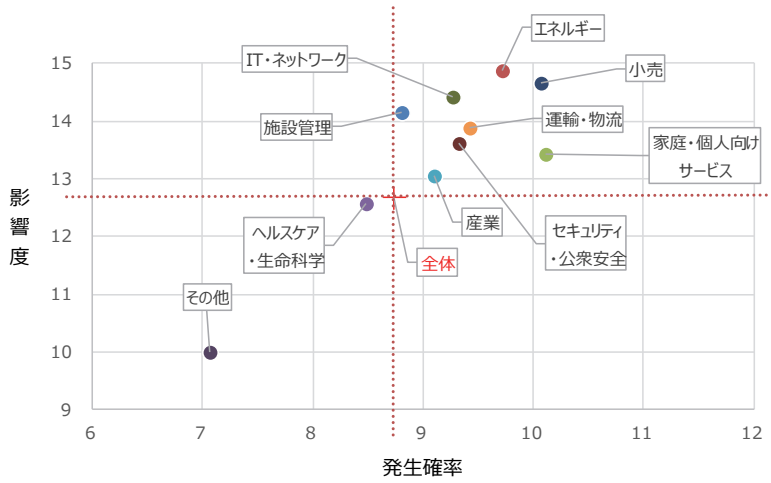


図 3-17　収集・利用する IoT 分野別 リスク評価結果

※破線は、影響度及び発生確率の全体の平均値

2)　回答者毎のリスク評価結果

a. 施設管理（空調や入退室等の自動監視・制御）結果

「施設管理」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、サイバー攻撃を受けた時の影響度が広く、サイバー攻撃が発生する確率も高い事業者が多いという結果となった。

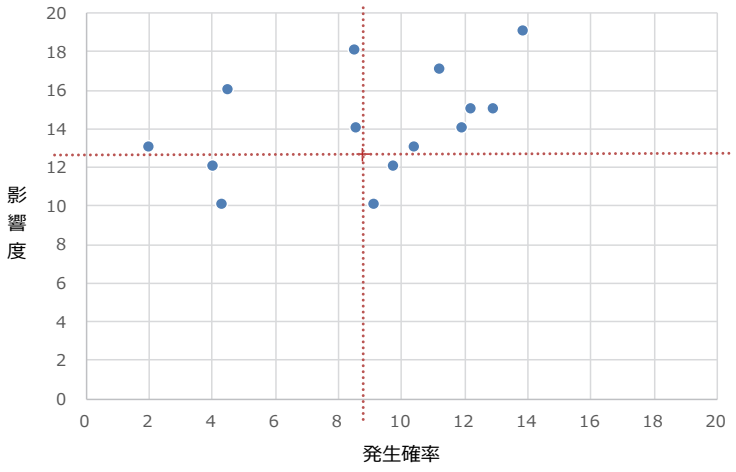


図 3-18　リスク評価結果（施設管理）

※破線は、影響度及び発生確率の全体の平均値

b. エネルギー（施設や地域のエネルギー管理等）結果

「エネルギー」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、サイバー攻撃を受けた時の影響度が広く、サイバー攻撃が発生する確率も高いと回答する事業者が多いという結果となった。また、発生確率・影響度ともに低い事業者は、1 事業者も無いという結果となった。

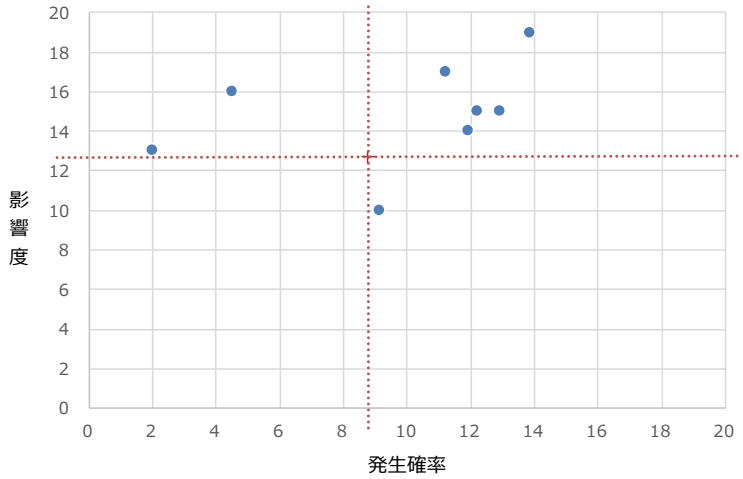


図 3-19　リスク評価結果（エネルギー）

※破線は、影響度及び発生確率の全体の平均値

c. 家庭・個人向けサービス（家庭向け安心、安全サービス、監視サービス等）結果

「家庭・個人向けサービス」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、サイバー攻撃を受けた時の影響度が広く、サイバー攻撃が発生する確率も高い事業者が多いという結果となった。

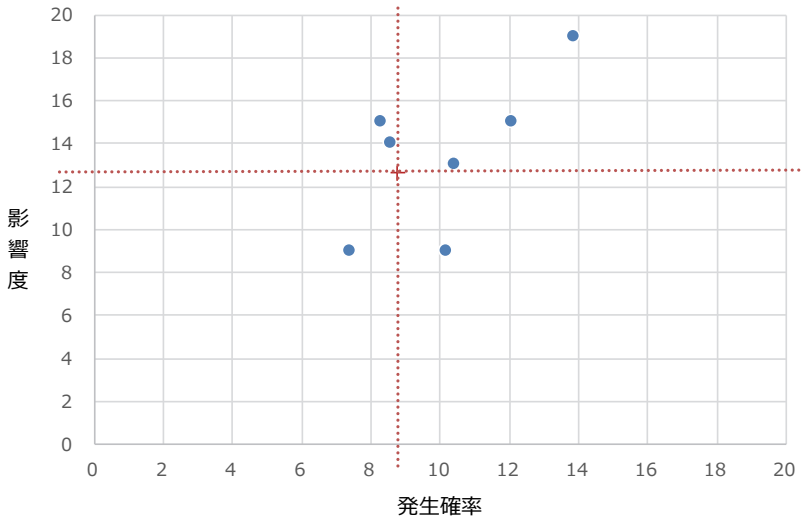


図 3-20　リスク評価結果（家庭・個人向けサービス）

※破線は、影響度及び発生確率の全体の平均値

d. 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等）結果

「ヘルスケア・生命科学」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、サイバー攻撃を受けた時の影響度、サイバー攻撃が発生する確率ともに高い事業者と、ともに低い事業者は同程度いるという結果となった。

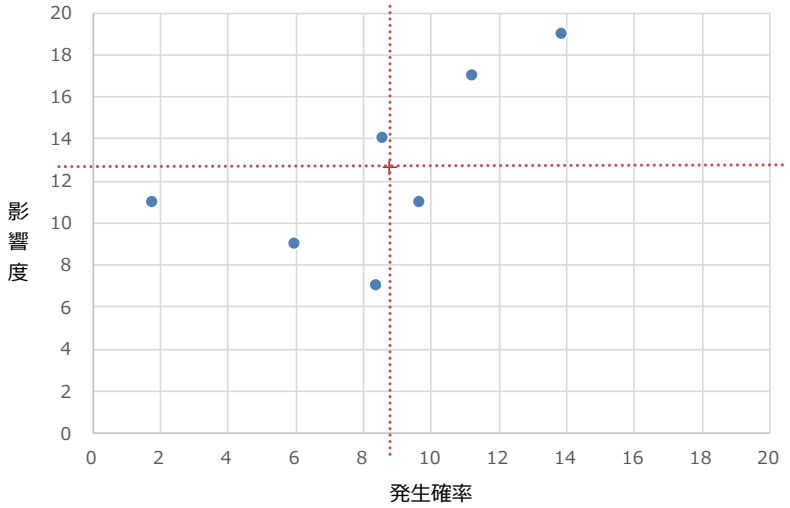


図 3-21　リスク評価結果（ヘルスケア・生命科学）

※破線は、影響度及び発生確率の全体の平均値

e. 産業（生産プロセスの可視化・高度化、生産性向上等）結果

「産業」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、サイバー攻撃を受けた時の影響度は比較的高めであるが、サイバー攻撃が発生する確率は低めから高めまで広く分布する結果となった。

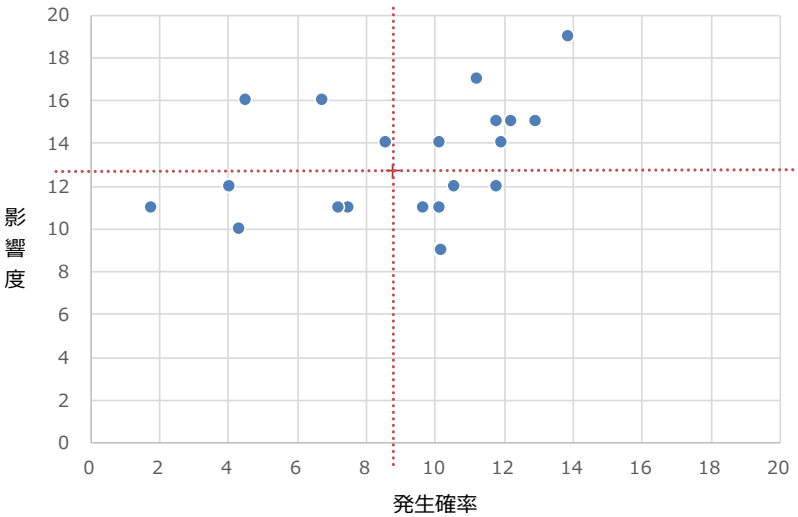


図 3-22　リスク評価結果（産業）

※破線は、影響度及び発生確率の全体の平均値

f. 運輸・物流（輸送管理の高度化、交通システム管理の高度化）結果

「運輸・物流」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、サイバー攻撃を受けた時の影響度は同程度、サイバー攻撃が発生する確率は高い事業者が多いという結果となった。

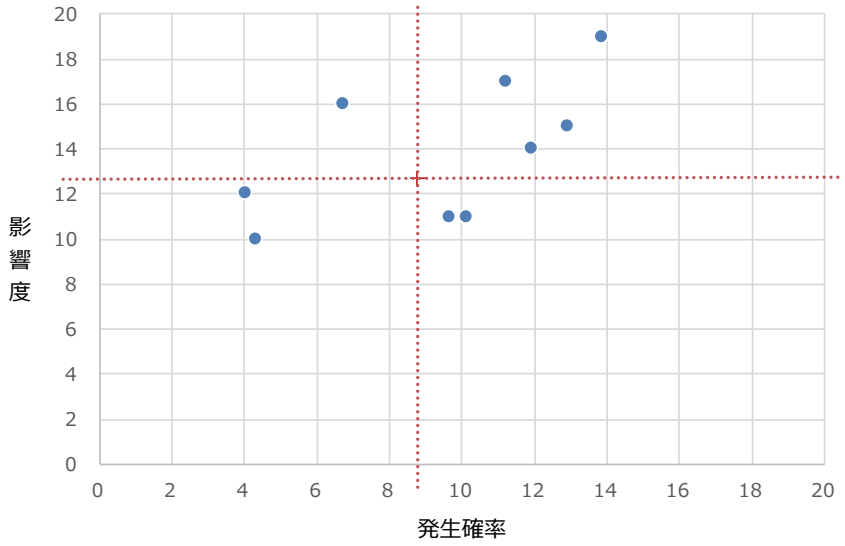


図 3-23　リスク評価結果（運輸・物流）

※破線は、影響度及び発生確率の全体の平均値

g. 小売（サプライチェーンの可視化、顧客・製品情報の収集、在庫管理の改善等）結果

「小売」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、サイバー攻撃を受けた時の影響度が高く、サイバー攻撃が発生する確率も高い事業者が多いという結果となった。

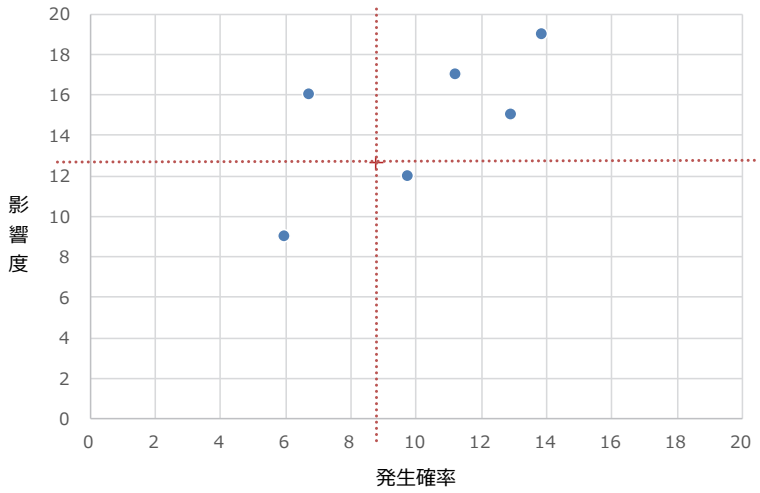


図 3-24　リスク評価結果（小売）

※破線は、影響度及び発生確率の全体の平均値

h. セキュリティ・公衆安全（緊急機関、公共インフラ管理の監視システム等の高度化）結果

「セキュリティ・公衆安全」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、サイバー攻撃を受けた時の影響度は広く、サイバー攻撃が発生する確率は高い事業者とサイバー攻撃を受けた時の影響度は低く、サイバー攻撃が発生する確率は低い事業者が同程度いるという結果となった。

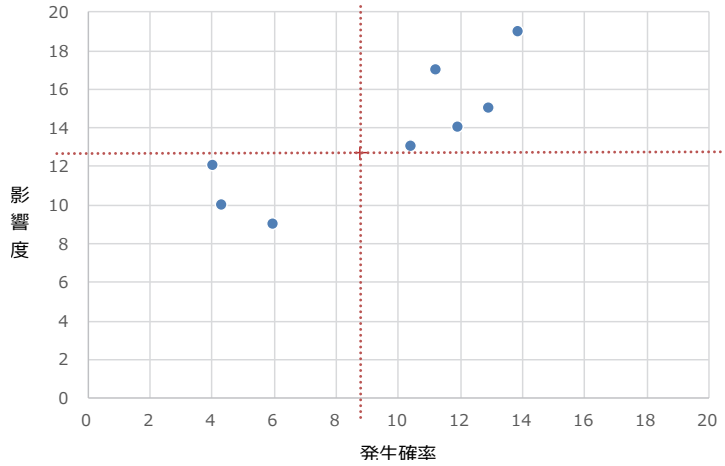


図 3-25　リスク評価結果（セキュリティ・公衆安全）

※破線は、影響度及び発生確率の全体の平均値

i. IT・ネットワーク（オフィス関連機器の監視・管理、通信インフラの監視・管理の高度化等）結果

「セキュリティ・公衆安全」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、サイバー攻撃を受けた時の影響度は高く、サイバー攻撃が発生する確率も高い事業者が多くいるという結果となった。

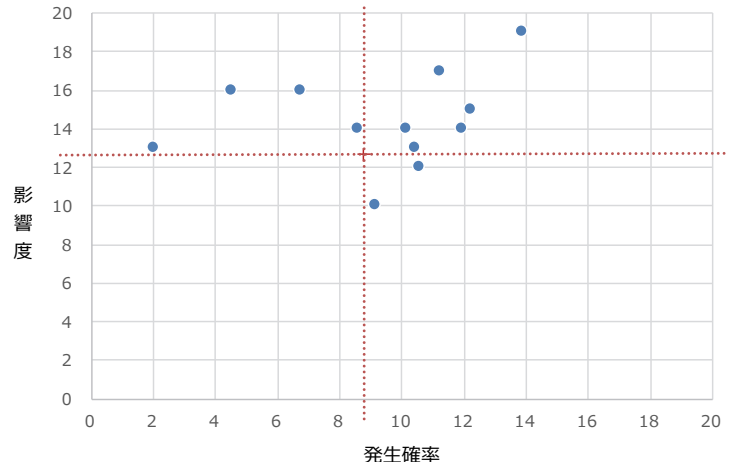
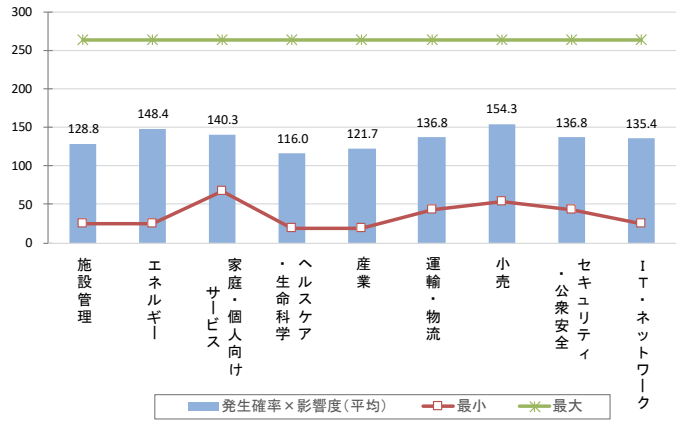


図 3-26　リスク評価結果（IT・ネットワーク）

※破線は、影響度及び発生確率の全体の平均値

3)　平均別、最大・最小別リスク評価結果

収集・利用する IoT データ分野別にリスク値を平均値化した結果、「ヘルスケア・生命科学」と「産業」は、その他の分野と比較してリスク値が低めであるという結果となった。



施設管理：空調や入退室等の自動監視・制御
エネルギー：施設や地域のエネルギー管理等
家庭・個人向けサービス：家庭向け安心、安全サービス、監視サービス等
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等
産業：生産プロセスの可視化・高度化、生産性向上等
運輸・物流：輸送管理の高度化、交通システム管理の高度化
小売：サプライチェーンの可視化、顧客・製品情報の収集、在庫管理の改善等
セキュリティ・公衆安全：緊急機関、公共インフラ管理の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、通信インフラの監視・管理の高度化等

図 3-27　収集・利用する IoT データ分野別結果

※当該設問は、マルチアンサーであり、リスク評価値が高い回答者が、収集・利用する IoT データ全データを選択したため、最大値が一定の値を示す結果となった。

4)　パラメータ別リスク評価結果

脅威エージェント（攻撃者の動機と意図、攻撃方法、攻撃機会）、脆弱性（認証方式、ポート制御、設定インタフェース、パッチ適用タイミング）、事業への影響（保護資産、市場にあるデバイス数、利用者数、連携システムへの影響）を 5 段階で正規化した値を用い、各評価指標に対する傾向を整理した。

a. 施設管理（空調や入退室等の自動監視・制御）結果

「施設管理」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、「攻撃機会」・「保護資産」・「連携システムへの影響」のリスクが高い傾向を示した。

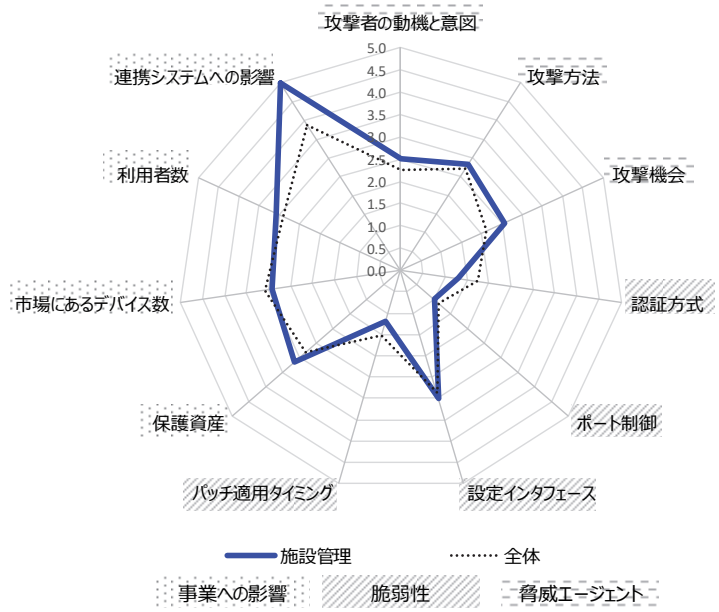


図 3-28　事業への影響、脆弱性、脅威エージェント別結果（施設管理）

b. エネルギー（施設や地域のエネルギー管理等）結果

「エネルギー」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、「脅威エージェント」・「事業への影響」のすべての項目でリスクが高い傾向を示した。

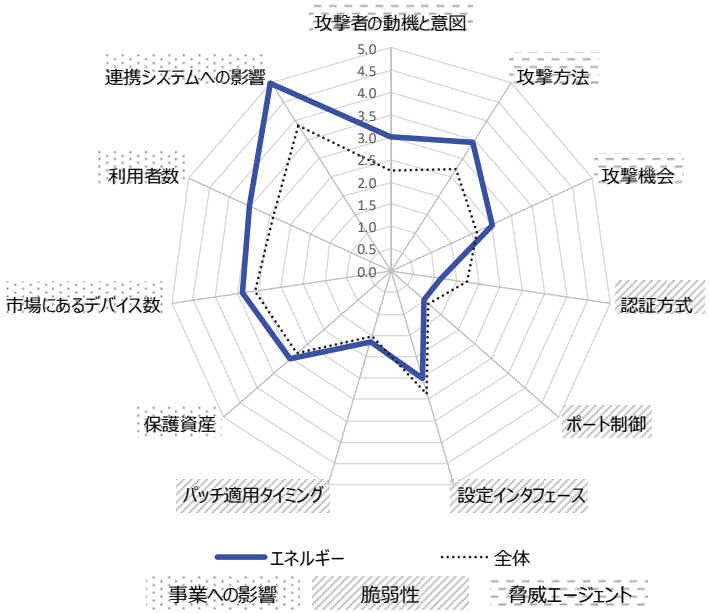


図 3-29　事業への影響、脆弱性、脅威エージェント別結果（エネルギー）

c. 家庭・個人向けサービス（家庭向け安心、安全サービス、監視サービス等）結果

「家庭・個人向けサービス」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、「攻撃者の動機と意図」・「設定インタフェース」・「パッチ適用のタイミング」・「保護資産」でリスクが高い傾向を示した。

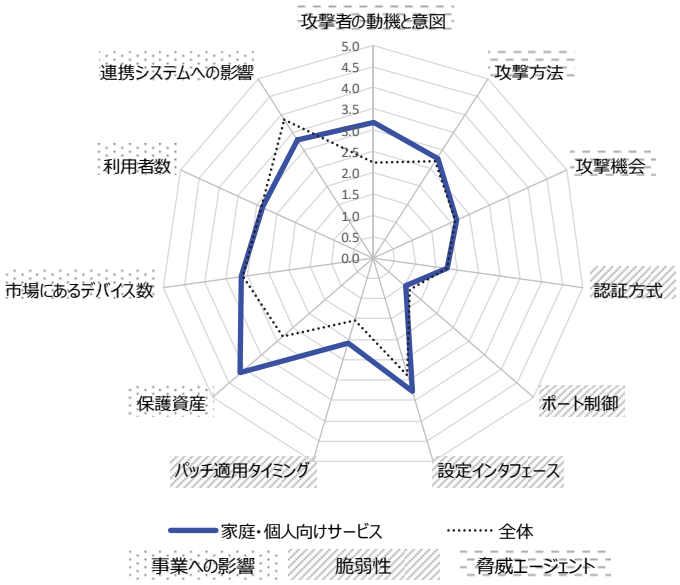


図 3-30　事業への影響、脆弱性、脅威エージェント別結果（家庭・個人向けサービス）

d. 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等）結果

「ヘルスケア・生命科学」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、「設定インタフェース」・「連携システムへの影響」でリスクが低い傾向を示した。

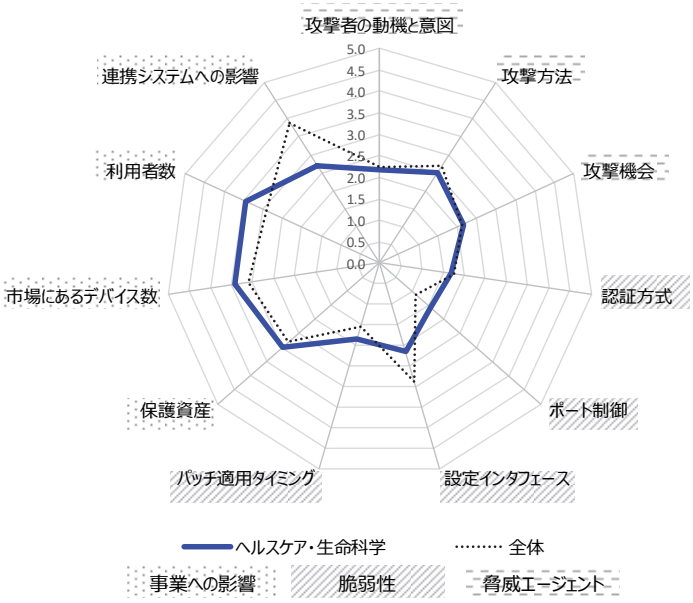


図 3-31　事業への影響、脆弱性、脅威エージェント別結果（ヘルスケア・生命科学）

e. 産業（生産プロセスの可視化・高度化、生産性向上等）結果

「産業」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、概ね同様の傾向を示した。

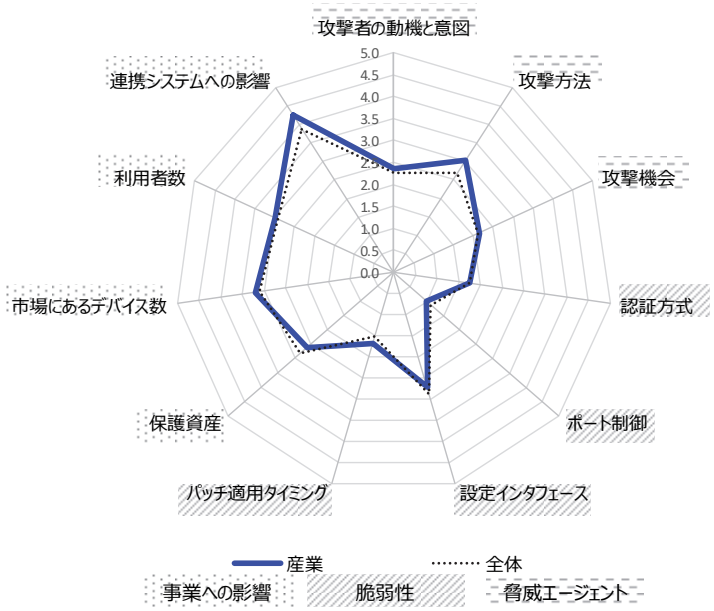


図 3-32　事業への影響、脆弱性、脅威エージェント別結果（産業）

f. 運輸・物流（輸送管理の高度化、交通システム管理の高度化）結果

「運輸・物流」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、「攻撃者の動機と意図」・「攻撃方法」・「連携システムへの影響」でリスクが高く、「認証方式」でリスクが低い傾向を示した。

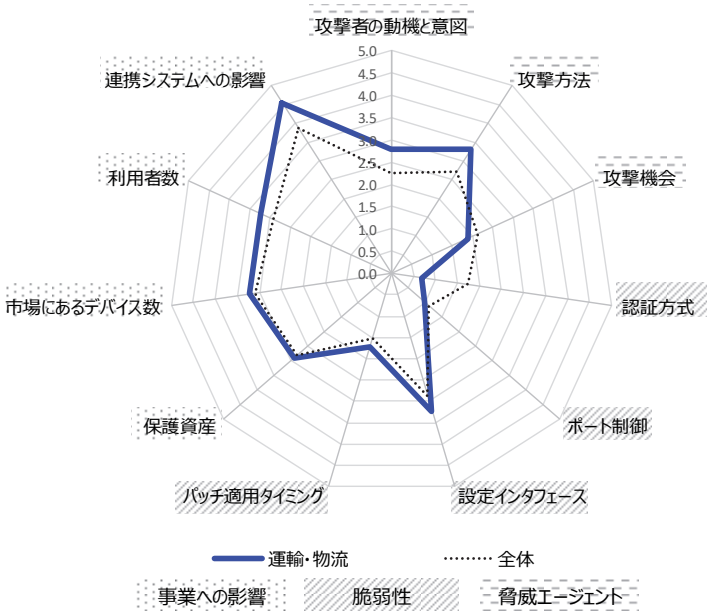


図 3-33　事業への影響、脆弱性、脅威エージェント別結果（運輸・物流）

g. 小売（サプライチェーンの可視化、顧客・製品情報の収集、在庫管理の改善等）結果

「小売」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、「脅威エージェント」・「事業への影響」のすべての項目でリスクが高い傾向を示した。

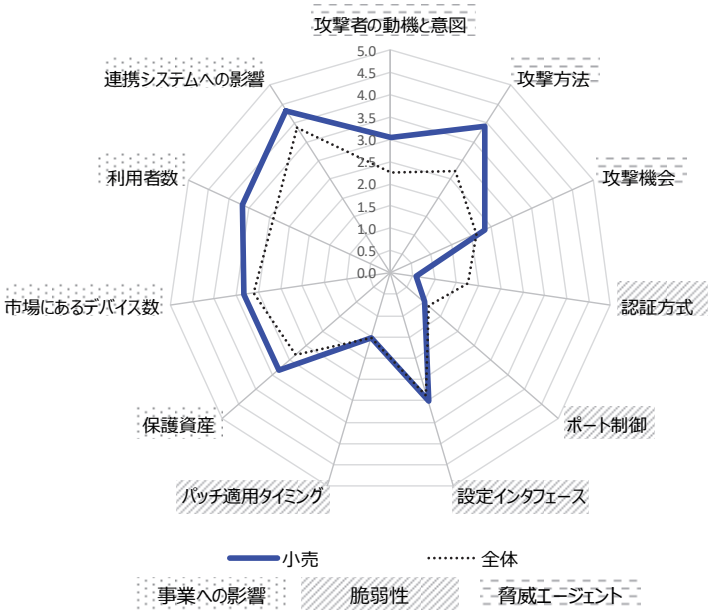


図 3-34　事業への影響、脆弱性、脅威エージェント別結果（小売）

h. セキュリティ・公衆安全（緊急機関、公共インフラ管理の監視システム等の高度化）結果

「セキュリティ・公衆安全」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、「脅威エージェント」の各項目、「連携システムへの影響」の項目でリスクが高く、「認証方式」でリスクが低い傾向を示した。

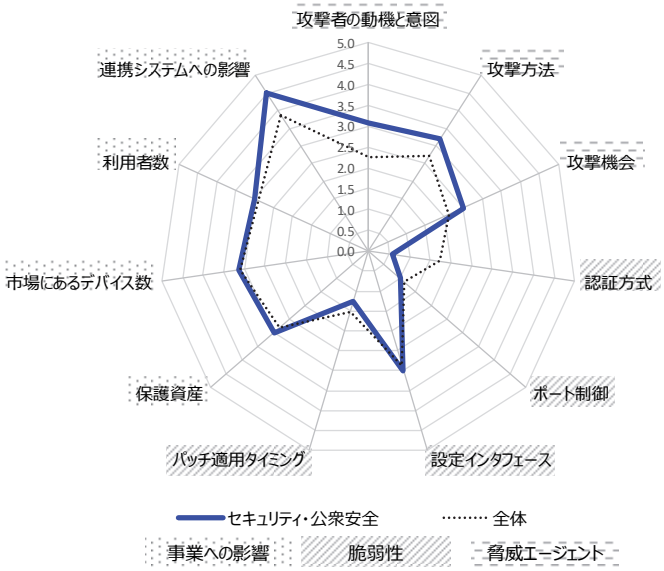


図 3-35　事業への影響、脆弱性、脅威エージェント別結果（セキュリティ・公衆安全）

i. IT・ネットワーク（オフィス関連機器の監視・管理、通信インフラの監視・管理の高度化等）結果

「ネットワーク」用のデータを利用・収集する事業者別に整理した結果、全体平均と比較して、「脅威エージェント」の各項目、「保護資産」・「連携システムへの影響」でリスクが高い傾向を示した。

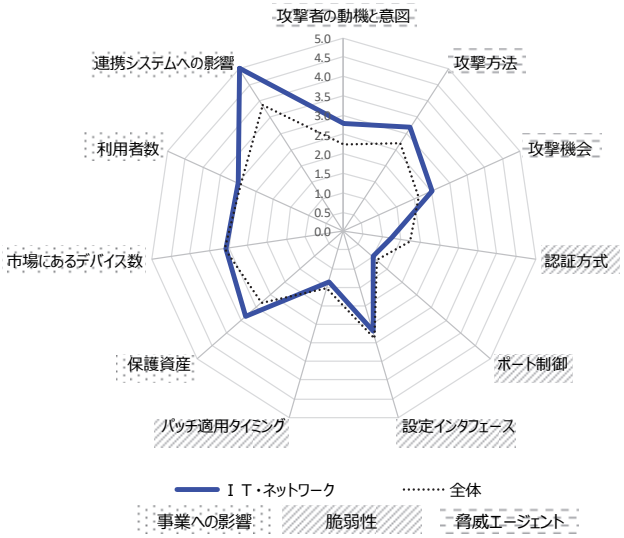


図 3-36　事業への影響、脆弱性、脅威エージェント別結果（IT・ネットワーク）

3.4　試行結果の考察

3.3 節でリスク評価を試行した結果より、「発生確率」の要素である「脅威エージェント（攻撃者の動機と意図、攻撃方法、攻撃機会）」、「脆弱性（認証方式、ポート制御、設定インタフェース、パッチ適用タイミング）」、また「影響度」に関して「事業への影響（保護資産、市場にあるデバイス数、利用者数、連携システムへの影響）」を 5 段階で正規化した値を用い、各評価指標の傾向を考察した。

3.4.1　発生確率

(1)　脅威エージェント

「発生確率」のうち「脅威エージェント」に関しては、「攻撃方法」に関するリスク値が全体平均で 2.7 と比較的高くなっている。想定されている攻撃手段が比較的容易な手法であることによるリスクの高さが表されているものと考えられえる。

「攻撃方法」でのリスクは、業種別では他の業種に比べて製造業で高めである。収集・利用する IoT データ分野別では、小売り分野で高めとなっている。

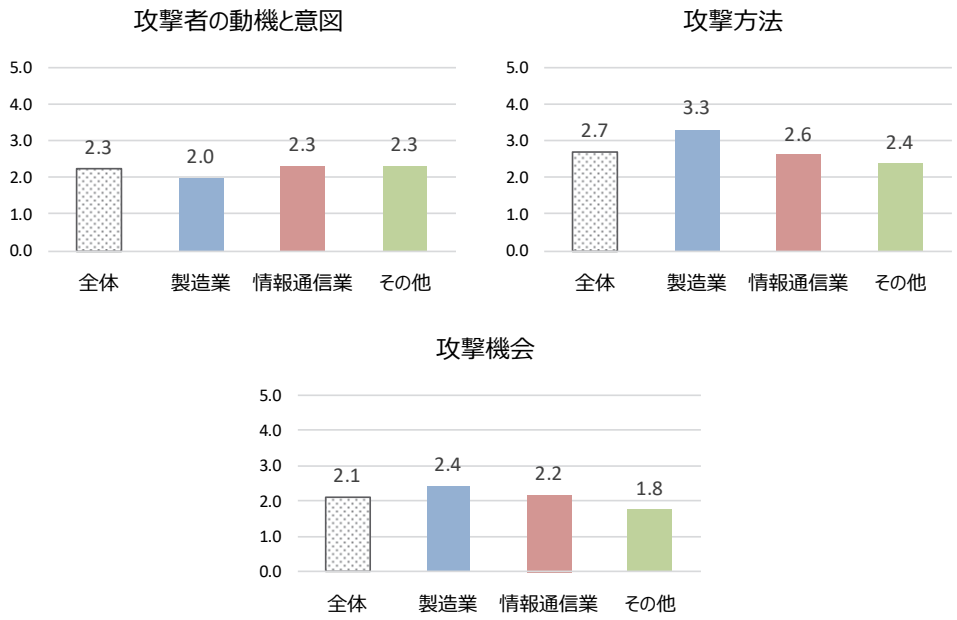


図 3-37　業種別・パラメータ別結果（脅威エージェント）

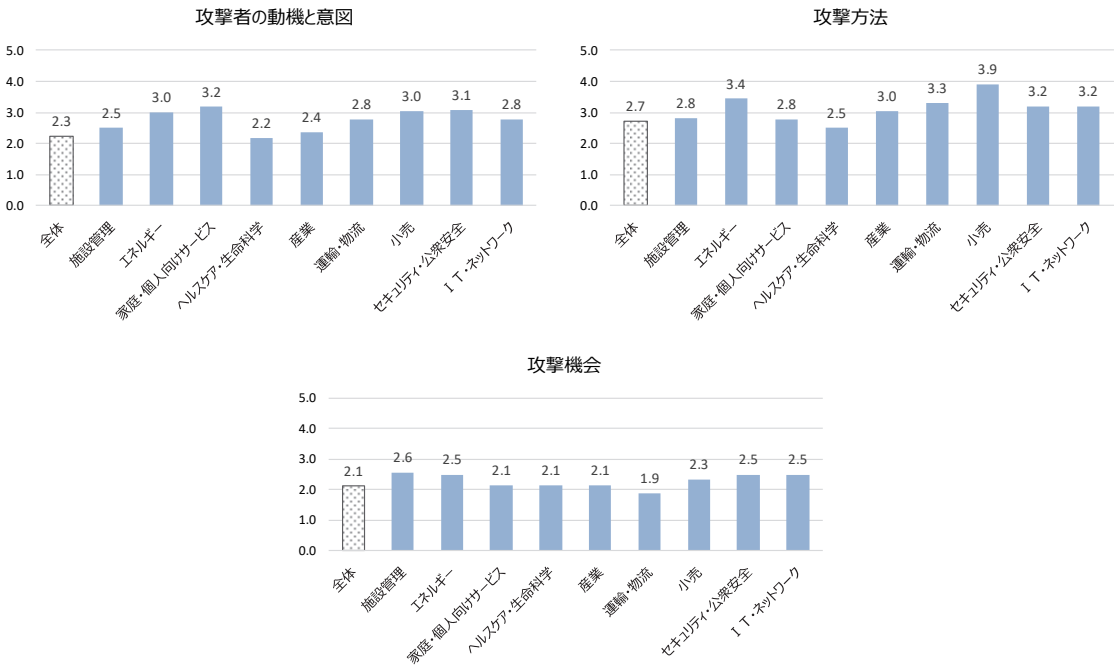


図 3-38　IoT の分野・パラメータ別結果（脅威エージェント）

(2)　脆弱性

「脆弱性」に関しては、「設定インタフェース」におけるリスクが全体平均で 3.9 と高い結果となっている。IoT 機器ではインターネットを介してアクセスするケースが多く、これをリスクとして評価していることによるものと考えられる。IoT データ分野別では、家庭個人向けサービス、運輸・物流分野で特に高くなっている。

「ポート制御」に関するリスク値は全体平均で 1.1 と低くなっており、業種別、IoT データ分野別に見ても差は少ない。

「パッチ適用タイミング」のリスク値は全体平均で 1.5 と中位であるが、情報通信業においてパッチ適用が適宜行われてリスクが低い傾向（1.1）があり、逆に製造業ではリスクが高め（2.2）となっている。

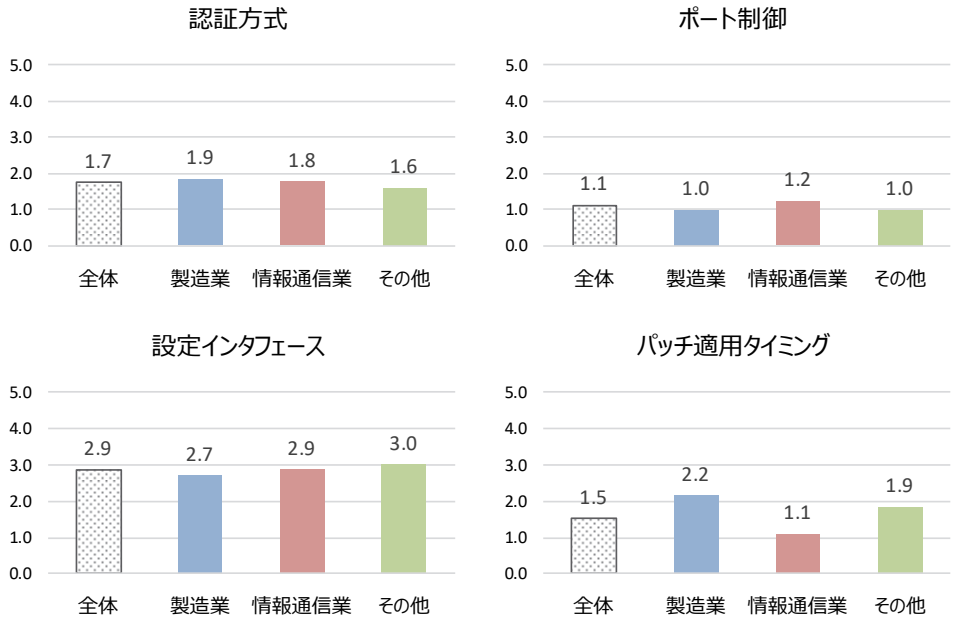


図 3-39　業種別・パラメータ別結果（脆弱性）

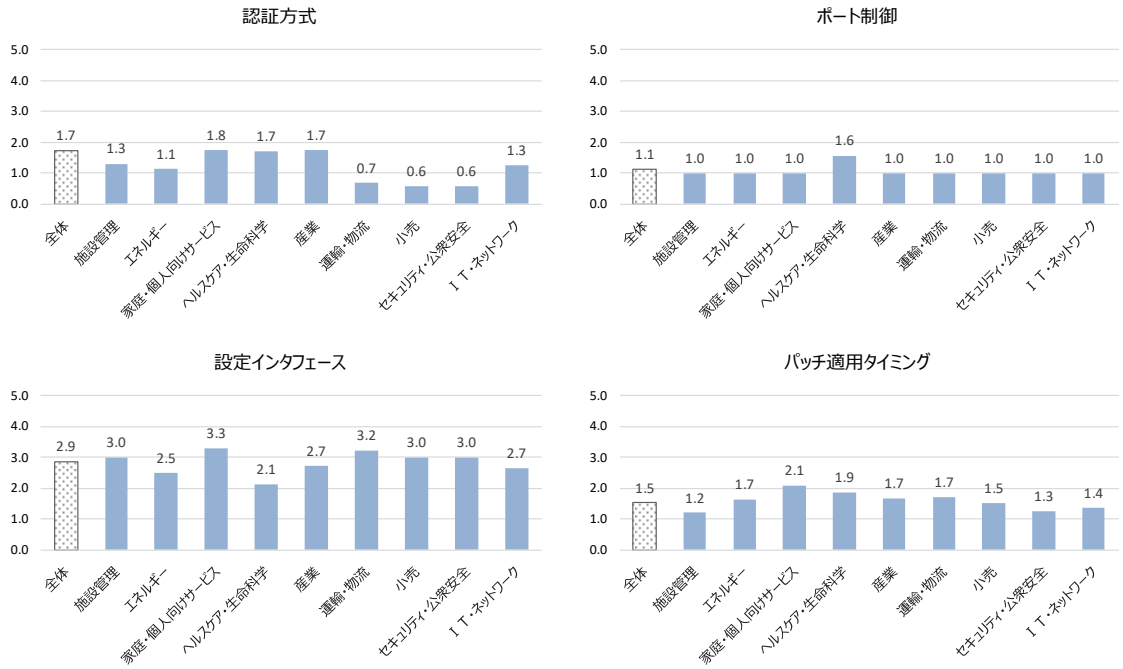


図 3-40　IoT の分野・パラメータ別結果（脆弱性）

3.4.2　影響度

「事業への影響」に関しては、「連携システムへの影響」が全体平均で 3.9 と高くなっている。連携システムがある場合にリスクが高いという評価をしているため、高いリスク値となるのは必然でもある。ただし、IoT データ分野別ではヘルスケア・生命科学分野では比較的低くなっている。

「デバイス数」、「利用者数」は、数が多いほどリスクが高いと評価していることから、双方とも多い製造業で高いリスク値となっている。

「保護資産」については、個人情報等を含む場合が多いと考えらえる家庭個人向けサービスでのリスク値が高い結果となった。

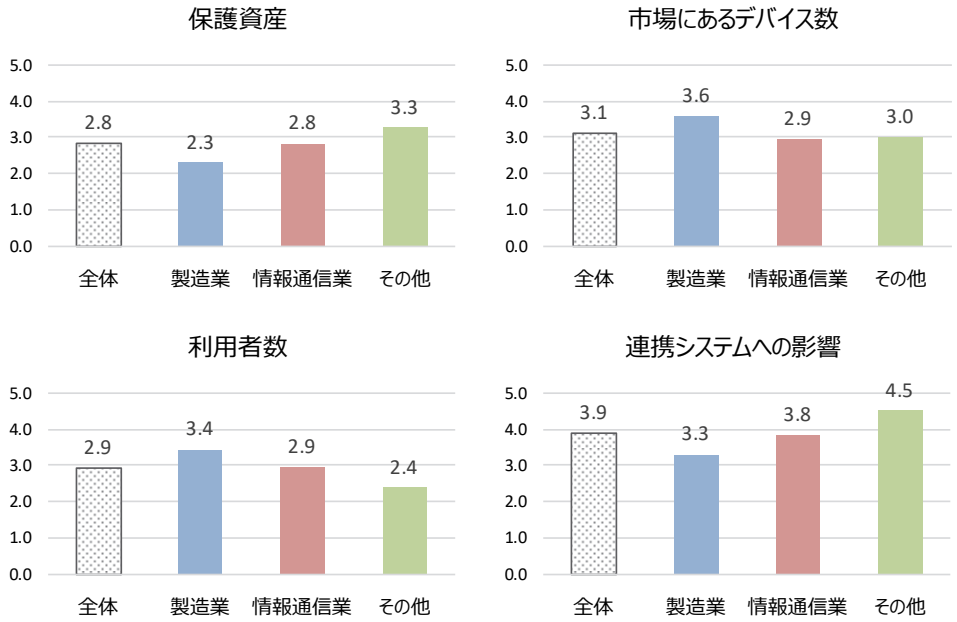


図 3-41　業種別・パラメータ別結果（事業への影響）

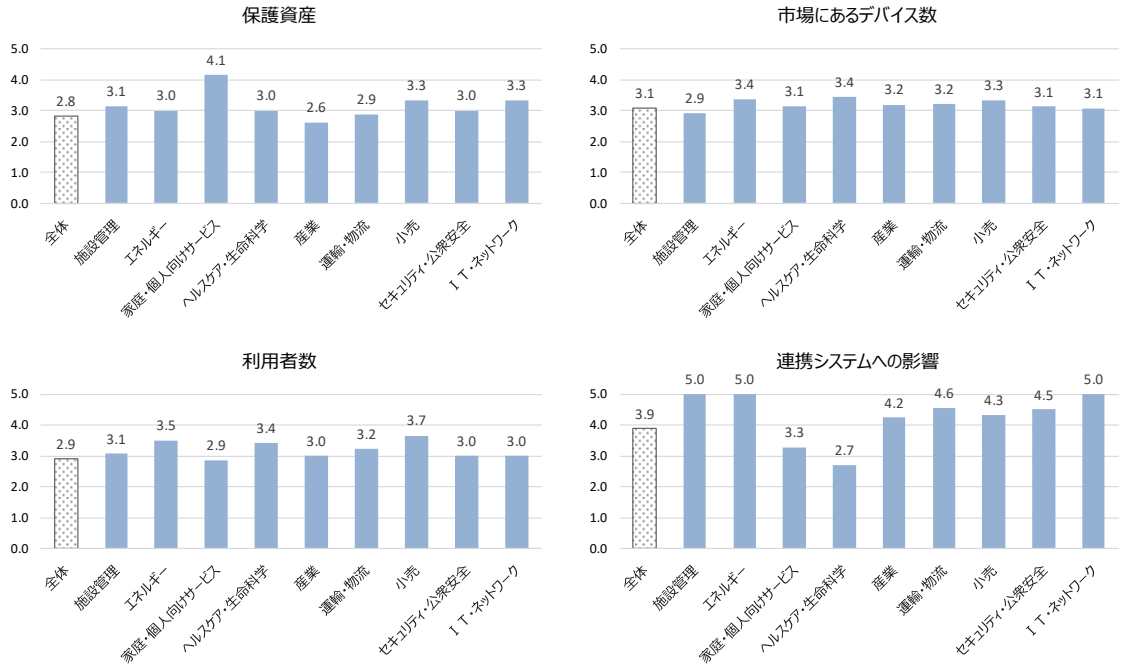


図 3-42　IoT の分野・パラメータ別結果（事業への影響）

3.4.3　まとめ

IoT サービスに関する脅威をモデリングし、アンケート結果を利用してリスク算定の試行を行った。

リスクに関する大まかなパラメータを設定し、パラメータごとの評価値（重み）を仮置きして試算を行い、リスク値を算出したが、モデルや評価値の検証までは至らなかった。特に、各パラメータのリスク値について、それぞれの尺度が異なり、横並びで比較してリスクの多寡が評価しきれないという点は今後の課題であると考えられる。

おわりに

本報告書では、Society5.0、Connected Industries などのサイバー空間とフィジカル空間が融合する社会の実現に向けたセキュリティ上の脅威と新たなサイバー攻撃のシナリオについて、IoT 及び AI の利活用の観点から考察した。

また、フィジカル・サイバー・セキュリティに関する新たなリスク算出モデルを提唱し、IoT サービスを提供している事業者を対象にアンケート調査を実施し、セキュリティ上の脅威の大きさを試算した。なお、今回提案するリスク算出モデルの計算方法は、初版であり、今後、フィードバック等を得ながら改良を加えていく予定である。

情報セキュリティ調査専門委員会では、情報セキュリティ技術とビジネスの方向に関する調査を行い、これまでの情報セキュリティ技術とビジネス環境や社会制度の変化を整理し、情報セキュリティに関する今後の技術開発やビジネス展開の方向について分析を行うことを目的として活動している。本委員会としては、今後の日本における、IT の活用を通じた産業界の発展と国際競争力強化のために、本書が活用されることを期待する。

添付資料１：
IoT ビジネスにおけるセキュリティに対する考え方についてのアンケート調査

(1)　概要

各企業が提供する IoT サービス・システム概況とセキュリティの考え方について調査した。

表 3-9　アンケート実施概要

調査期間	2019 年 1 月 9 日（水）～2019 年 1 月 25 日（金）
調査対象	IoT 推進コンソーシアム 法人会員 (1)IoT を活用した製品・システムやサービスを提供する担当者 【製品・サービス企画・設計・開発・運用部門】 (2)IoT データを収集・分析・提供(あるいはその一部)を行う企業担当者 【サービス企画・設計・開発・運用部門】 【データ収集・分析・提供部門】 (3)自社内で IoT システムを利用している担当者 【システム企画・設計・開発・運用部門】及び 【データ収集・分析・提供部門】
調査方法	Web アンケート
回答状況	回答数：96 件

(2)　アンケート結果

回答結果を以下にまとめる。

1)　回答者企業属性

Q1_1　御社では IoT ビジネス（IoT を活用した製品やサービス、データ利活用等）を展開していますか。当てはまるものを 1 つお選びください。（n=96）

IoT ビジネスの展開状況について調査した結果、「IoT ビジネスを展開している（42.7%）」が最も多く、次いで、「今後 IoT ビジネスを展開予定である（39.6%）」であった。

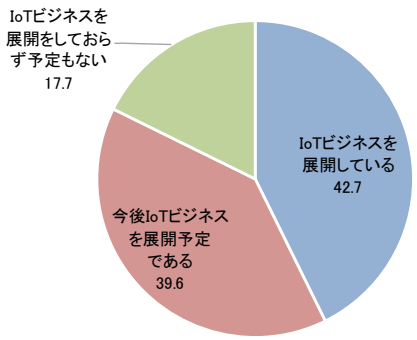


図 3-43　事業展開している IoT ビジネス

Q1_2　御社の総従業員数（有給役員，正社員・正職員，準社員・準職員，アルバイト等を含む）について、直近の会計年度の人数（概算で結構です）をお選びください。(n=79)

総従業員数について調査した結果、「50 名未満（38.0%）」が最も多く、次いで「1,001 名～5,000 名（19.0%）」「101 名～300 名（12.7%）」となった。

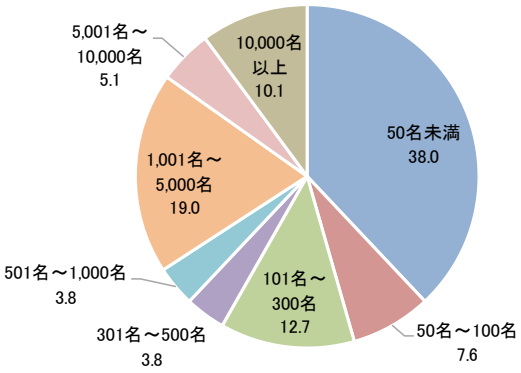
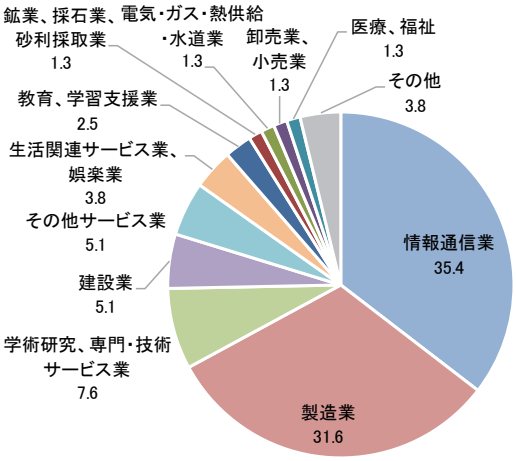


図 3-44　会社の総従業員数

Q1_3　御社の主な業種をお選びください。（n=79）

会社の主な業種について調査した結果、「情報通信業（35.4%）」が最も多く、次いで「製造業（31.6%）」となっており、情報通信業と製造業が 7 割近くを占めた。



情報通信業	製造業	学術研究、専門・技術サービス業	建設業	その他サービス業	生活関連サービス業、娯楽業	その他	教育、学習支援業	鉱業、採石業、砂利採取業	電気・ガス・熱供給・水道業	卸売業、小売業	医療、福祉	農業、林業	漁業	運輸業、郵便業	金融業、保険業	不動産業、物品賃貸業	宿泊業、飲食サービス業
35.4	31.6	7.6	5.1	5.1	3.8	3.8	2.5	1.3	1.3	1.3	1.3	0.0	0.0	0.0	0.0	0.0	0.0

（%）

図 3-45　会社の主な業種

Q1_4　御社の総売上高について、直近の会計年度の金額（概算で結構です）をお選びください。（n=79）

会社の総売上高について調査した結果、「1 億円未満（31.6%）」が最も多く、次いで「1,000億円以上（25.3%）」となった。

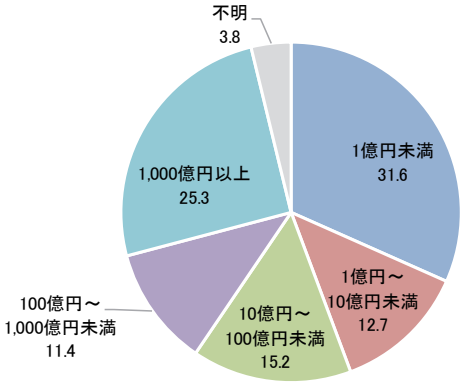


図 3-46　会社の総売上高

Q1_5　あなたの所属部署として最も近いものをお選びください。（n=79）

所属部署について調査した結果、「企画部門（29.1%）」が最も多く、次いで「設計開発部門（26.6%）」、「情報システム部門（24.1%）」となっており、この 3 部門で約 8 割を占めた。

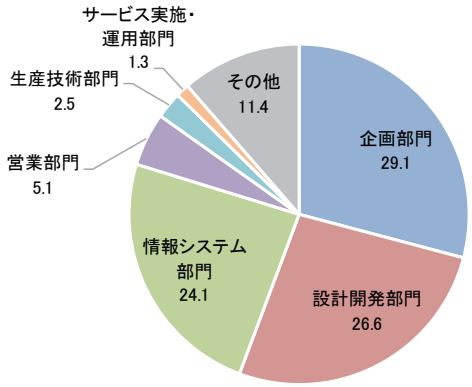


図 3-47　回答者の所属部署

【その他回答】

- 経営管理兼 CIO
- 役員
- 技術
- 教育部門
- 経営企画
- 全社部門
- 知的財産管理
- 調査

2)　担当する IoT ビジネスについて

Q2_1	あなたが担当する IoT ビジネスの主要な形態はどのようなものでしょうか。最も近いものをお選びください。（n=79）

IoT ビジネスの主要な形態を調査した結果、「IoT を活用した製品提供（45.6%）」と約半数を占めており、次いで「IoT データを収集・分析・提供（あるいはその一部）を行うサービス（30.4%）」となった。

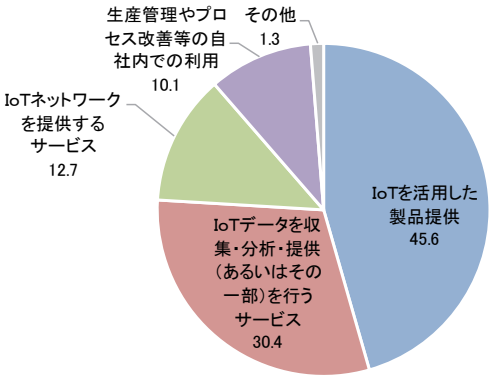


図 3-48　回答者の担当する IoT ビジネスの主要形態

【その他回答】・技術

Q2_2	あなたが担当する IoT ビジネスで収集、または利用する（購入も含む）データ種類について、最も当てはまるものをお選びください。(n=79)

IoT ビジネスで収集、または利用する（購入も含む）データの種類について調査した結果、「パーソナルデータを含まない情報（工場のセンサー情報、自社製品につけたセンサー情報等）（51.9%）」が半数を占めた。

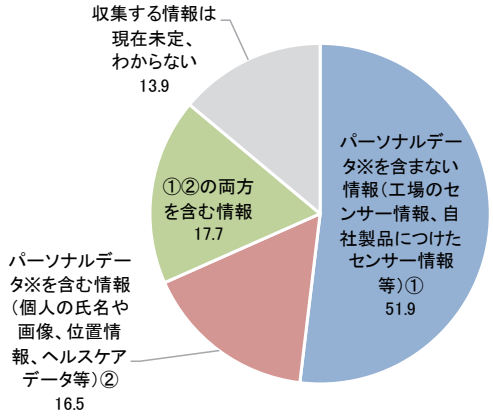


図 3-49　IoT ビジネスで収集、利用するデータ種類

Q2_3	あなたが担当する IoT ビジネスで収集または利用する（購入も含む）IoT データは、どのような分野のものでしょうか。当てはまるものを全てお選びください。（複数回答可）（n=68）

IoT ビジネスで収集または利用する（購入も含む）IoT データの分野について調査した結果、「産業（生産プロセスの可視化・高度化、生産性向上等）（47.1%）」が最も多く、次いで「IT・ネットワーク（オフィス関連機器の監視・管理、通信インフラの監視・管理の高度化等）（36.8%）」となった。

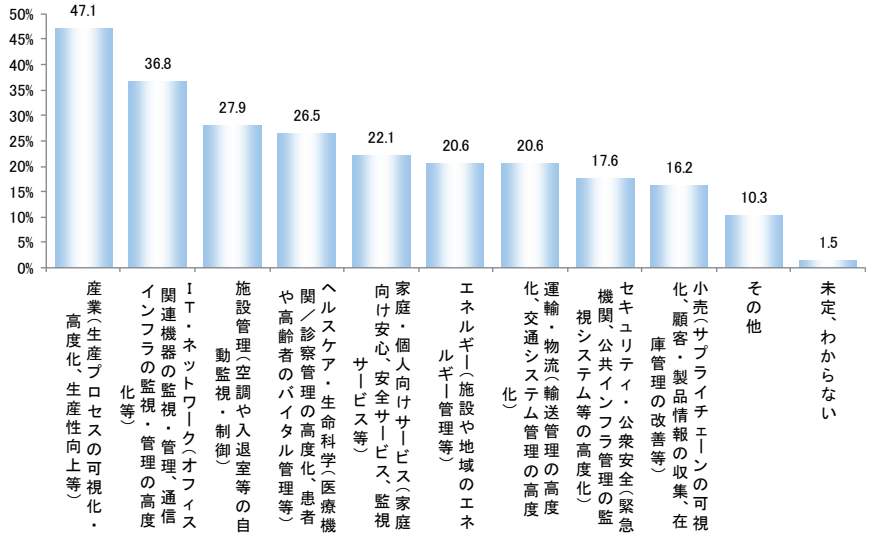


図 3-50　IoT ビジネスで収集、利用するデータの分野

【その他回答】

- 環境データ
- 産業機械の予知保全
- 娯楽
- 地惑
- 社会課題
- 気候、自然
- 行政関連

Q2_4　あなたが担当する IoT ビジネスではデータをどのように収集しますか。収集方法として中心的な手段を 1 つお選びください。（n=68）

データの収集方法について調査した結果、「自社が販売・提供した製品（センサー内蔵）からデータを収集（55.9%）」が過半数を超えており、次いで「自社が社外に設置した IoT 機器（例　監視カメラ等）から収集（11.8%）」「自社内（例　工場等）に設置した IoT 機器から収集（11.8%）」となった。

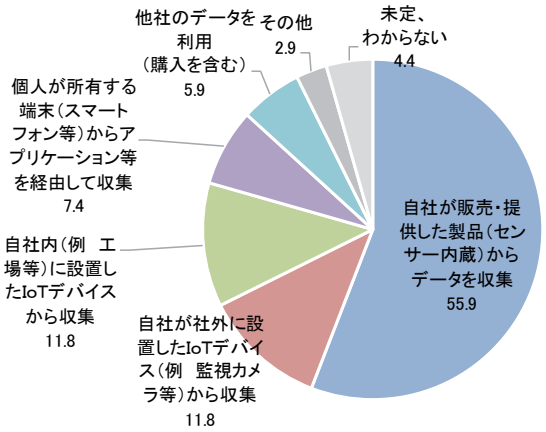
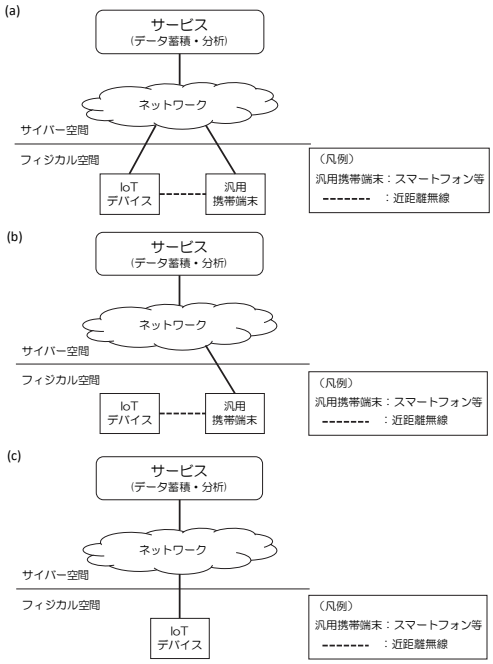


図 3-51　IoT ビジネスでのデータ収集方法

【その他回答】上記の混在，実地

Q2_5　あなたが担当する IoT ビジネスのシステム構成は、図の（ａ）、（ｂ）、（ｃ）に当てはめるとすると、どれに最も近いですか。（n=79）



IoT ビジネスのシステム構成について調査した結果、IoT 機器のみをネットワークに接続する「c に当てはまる（c に近い）（48.1%）」が半数を占める結果となった。

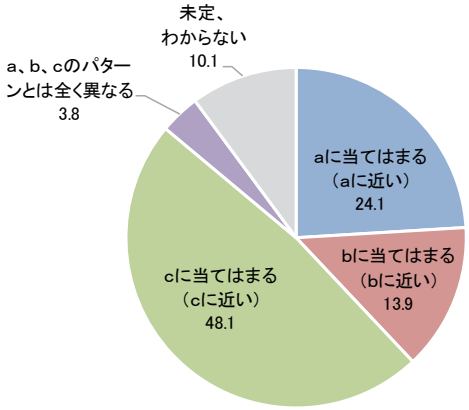


図 3-52　IoT ビジネスのシステム構成

Q2_6　あなたが担当する IoT ビジネスで利用する IoT 機器は、主にどのようなものでしょうか。（n=79）

IoT ビジネスで利用する IoT 機器について調査した結果、「専用デバイス（49.4%）」が最も多く、次いで「機器組み込み（家電製品、複合機、カメラ、自動車等）（19.0%）」となった。

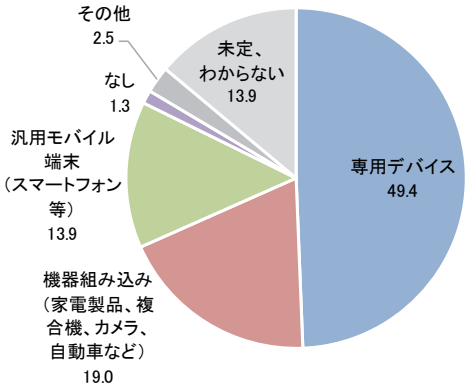


図 3-53　IoT ビジネスで利用する IoT 機器

Q2_7　あなたが担当する IoT ビジネスで利用する IoT 機器は、複数の利用者により共有されますか。（n=79）

IoT ビジネスで利用する IoT 機器の複数利用について調査した結果、「共用がある（50.6%）」が半数を超えた。

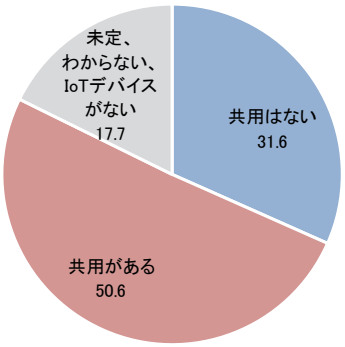


図 3-54　IoT ビジネスで利用する IoT 機器の共有の有無

Q2_8　あなたが担当する IoT ビジネスのシステムやデータは、他のサービスやシステムとの連携がありますか。（n=79）

IoT ビジネスのシステムやデータが、他のサービスやシステムとの連携可能性について調査した結果、「連携がある（48.1%）」が約半数となった。

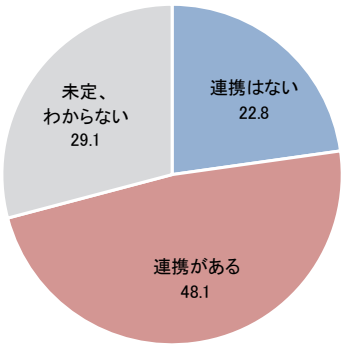


図 3-55　IoT ビジネスの他サービス、システムとの連携の有無

Q2_9　あなたが担当する IoT ビジネスの利用者数を概数の整数でお答えください。（おおよその人数で結構です）（n=79)

IoT ビジネスの利用者数について調査したところ、「1,000 人～10 万人未満（26.6%）」が最も多く、次いで「10 人～100 人未満（22.87%）」となった。1~100 人未満で約半数を占めている。また、最大利用者数は 10 億人といった回答があった。

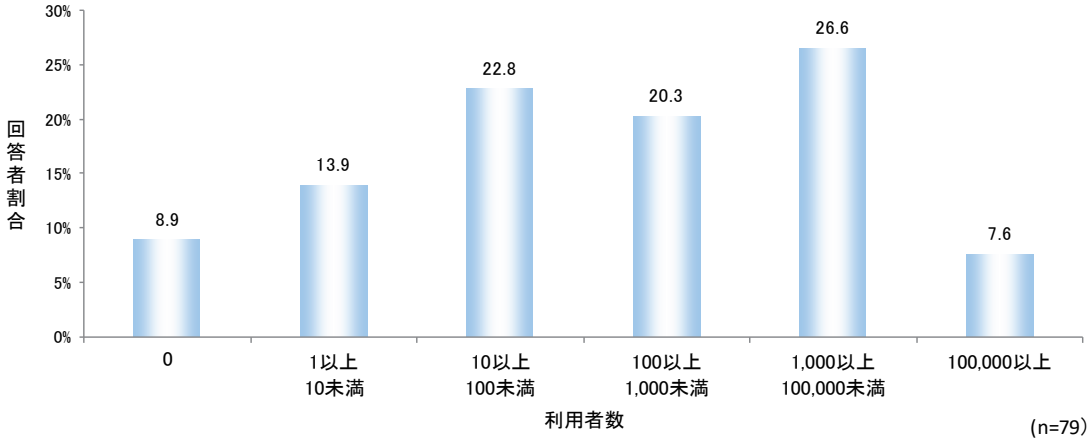


図 3-56　IoT ビジネスの利用者数

Q2_10　あなたが担当する IoT ビジネスで利用する IoT 機器数を概数の整数でお答えください。（おおよその台数で結構です。また、IoT 機器がない場合は、0 とお答えください。）（n=79）

IoT ビジネスで利用する IoT 機器数について、調査したところ「100～1,000 台未満（21.5%）」が最も多く、「10 万台以上（17.7%）」も多くなっている。最大デバイス数は 100 億台であった。

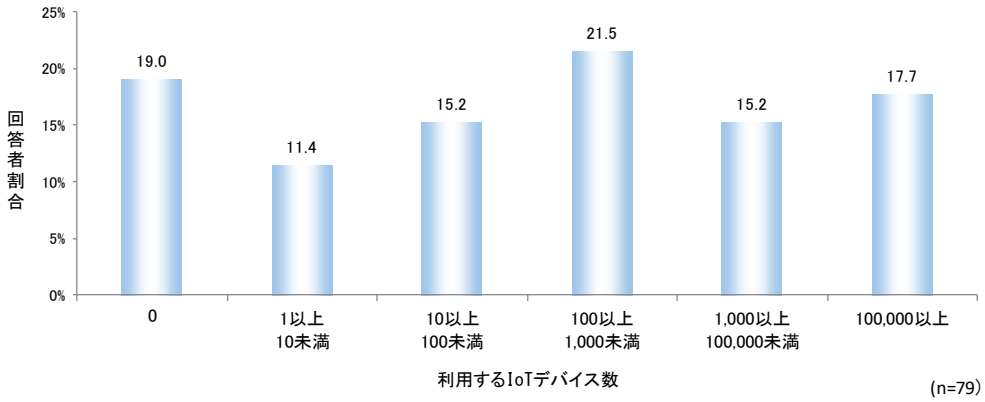


図 3-57　IoT ビジネスで利用する IoT 機器数

Q2_11　あなたが担当する IoT ビジネスで、1 年間でユーザが支払う必要のある金額（機器費用やサービス費用等の合計）を概算の整数でお答えください。
（おおよその金額で結構です）

Q2_12　その金額の課金単位は以下のうちどれにあたりますか。（n=79）

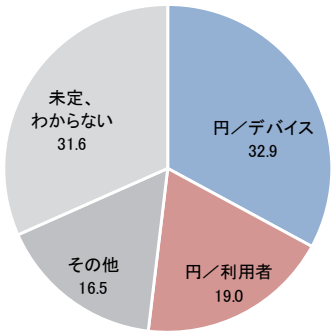


図 3-58　年間支払い金額の課金単位

1 年間でユーザが支払う必要のある金額については、1 デバイスあたりの回答では、最も多かったのは、「100 万円（11.5%）」次いで「5 万円（7.7%）」「30 万円（7.7%）」「50 万円（7.7%）」となった。ユーザあたりの金額をみると、「1 万円（20%）」が最も多く、次いで「100 万円（13.3%）」となった。その他の金額では 13 件の回答があった。

【デバイス】26 件

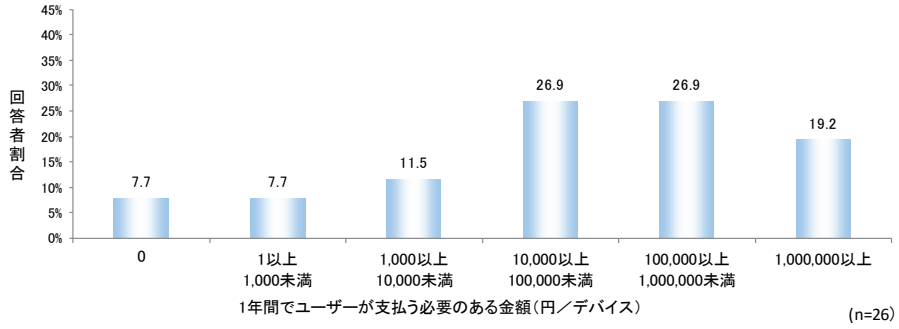


図 3-59　IoT ビジネスの 1 デバイス当たりの支払金額

【利用者】15 件

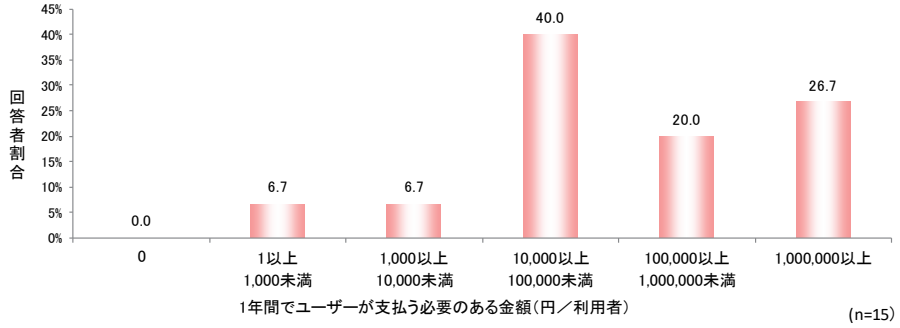


図 3-60　IoT ビジネスの 1 ユーザ当たりの支払金額

【その他の回答】13 件

50,000,000 円	（システム総額）
30,000,000 円	（サービス利用料）
10,000,000 円	（業務単位ごと）
10,000,000 円	（デバイス及び提供サービス）
5,000,000 円	（1 機械）
1,200,000 円	（円/所）
1,000,000 円	（１システム/社）
1,000,000 円	（全体）
20,000 円	（デバイスグループ）
17,000 円	（円/世帯）
200 円	（初期費用以外は利用量に基づく月額課金）
0 円	（決済金額による）
0 円	（販売会社により異なる）

【未定、わからない】25 件

3)　IoT ビジネスに対する脅威について

Q3_1_1_MT	あなたが担当する IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者の意図について、次の項目に関して想定される可能性を 5 段階で評価してください。（n=79）

IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者の意図について、想定される可能性を 5 段階で評価した結果、「非常に想定される」のは「個人情報や機密情報の窃取（22.8%）」、次いで「IOT ビジネスや利用者への業務妨害（13.9%）」「マルウエア拡散（12.7%）」となった。

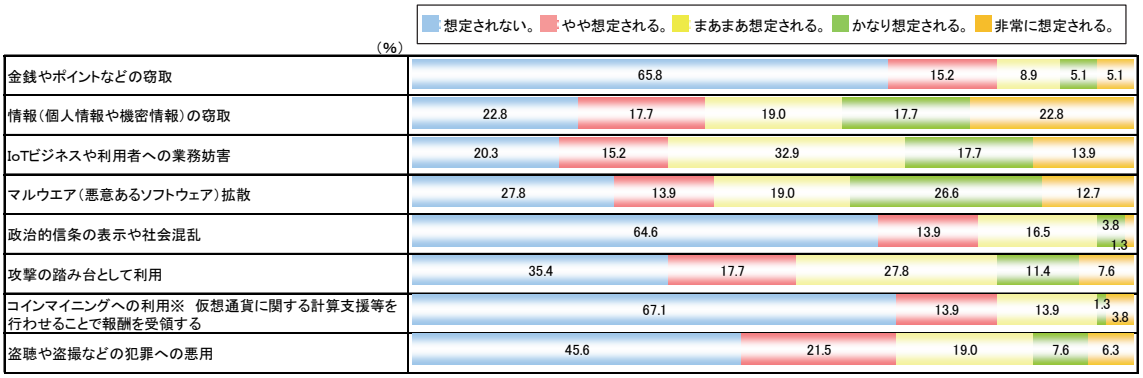


図 3-61　サイバー攻撃の意図についての想定度

Q3_2　あなたが担当する IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者の意図について、上記の項目以外に想定される事項があれば具体的に記入ください。

以下の回答が得られた。

- サービス等の利用権の不正取得
- IoT データの改竄
- 愉快犯
- 私怨
- 生産データの抜き取り及び加工技術の入手
- 個人情報の取得
- 工場、施設の運転データ取得
- 家庭内に IoT 機器を設置することを想定しておりますが、玄関のオートロック解除や自動で電灯、お風呂を沸かす、クーラーの ONOFF 等簡単にできてしまう懸念があります。そのため、設定する際は、スマホでの顔認証や指紋認証等の組み合わせを想定する構想を考えています。

Q3_3_1_MT　あなたが担当する IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する方法について、次の項目に関して想定される可能性を５段階で評価してください。（n=79）

IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する方法について、想定される可能性を５段階で評価したところ、想定されるのは「ユーザアカウントやシステム管理者アカウントの不正利用（83.5%）」が最も多く、次いで「マルウエア感染（遠隔操作）（75.9%）」となった。

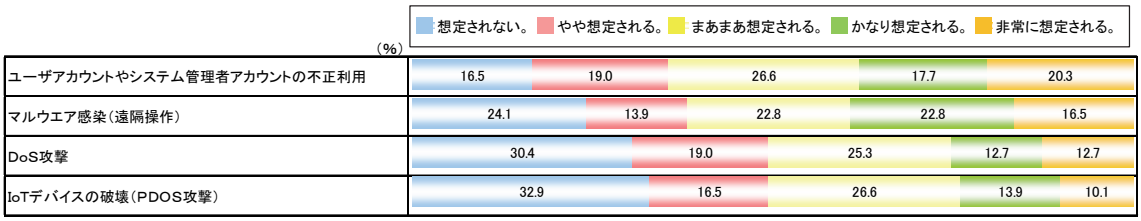


図 3-62　サイバー攻撃方法の想定度

Q3_4	あなたが担当する IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する方法について、上記の項目以外に想定される事項があれば具体的に記入ください。

以下の回答が得られた。

- 生体情報のコピーによるなりすまし
- IoT 機器の乗っ取り
- 内部利用者やゲスト等が、別途バックドアの端末を用意し、物理的にパスワードを奪取する可能性もあるため、2 段階認証は必須と考えられる。また、ブロックチェーンを利用し、IoT 機器の相互認証を行うことを考慮した方が良いと考えております。
- 現時点では分からない新たな手法
- 携帯ネットワークからの不正侵入からのデバイスプログラムの書き換え

Q3_5_1_MT	あなたが担当する IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する界面について、次の項目に関して想定される可能性を 5 段階で評価してください。（n=79）

IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する界面について、想定される可能性を 5 段階で評価した結果、「センターサーバーとデバイス（あるいはエッジサーバー）との通信の脆弱性」の回答が最も多い結果となった。

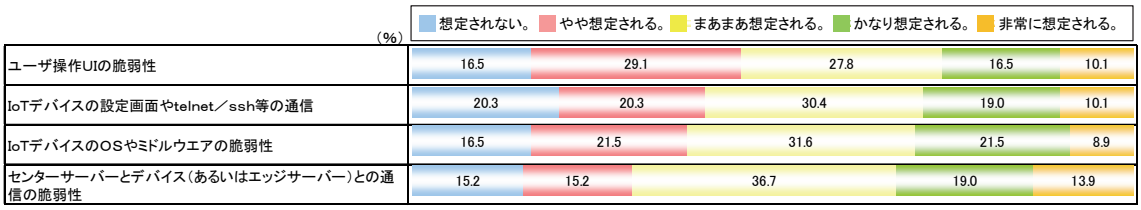


図 3-63　サイバー攻撃者が利用する界面の想定度

Q3_6	あなたが担当する IoT ビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する界面について、上記の項目以外に想定される事項があれば具体的に記入ください。

以下の回答が得られた。

- IoT システムが発展していくとデファクトスタンダードなものが出てくるため、操作端末、アプリを利用し、オレオレ詐欺の進化版が横行すると考えます。基本的なセキュリティ（ファイアウォール、ウイルス、プロキシによる証跡取り、IDs 等）を施し、人的ミスを IT リテラシーの向上により防ぐことができれば、簡単に突破されないと考えます。その人的ミスを AI 化できないかが課題と考えます。
- Gateway のプログラム書き換え及び通信情報の抜き取り Web アプリへの不正アクセス

4)　利用する IoT 機器に関して

Q4_1　利用する IoT 機器へのアクセスについて、以下のどのような方法で制御していますか。（n=79）

IoT 機器へのアクセスについて調査した結果、どのような方法で制御しているかをみると、「ID とパスワードを利用（39.2%）」が最も多く、「電子証明書、生体認証を含む複数（多要素）を利用（12.7%）」が 1 割強、「アクセス制御はしない（8.9%）」も 1 割弱存在した。

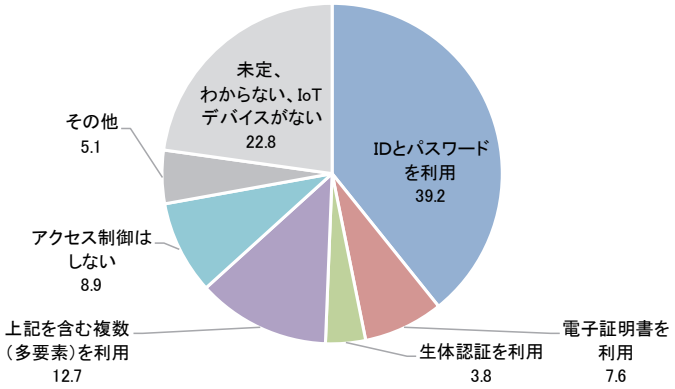


図 3-64　IoT 機器へのアクセス制御方法

Q4_2　利用する IoT 機器ではポートの制御を行っていますか。（n=79）

IoT 機器のポートの制御について調査した結果、「ポートを制御している（53.2%）」のが半数以上を占めている一方、「ポートを制御していない（6.3%）」もわずかながら存在した。

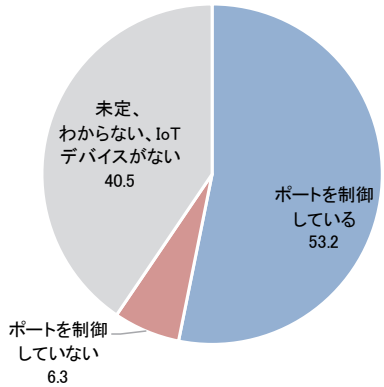


図 3-65　IoT 機器のポート制御方法

Q4_3　利用する IoT 機器を設定するユーザーインターフェースへのアクセスは、以下のうちどのような方法をとっていますか。（n=79）

IoT 機器を設定するユーザーインターフェースへのアクセス方法について調査した結果、「インターネットを介してアクセス（34.2%）」と最も多くあった。

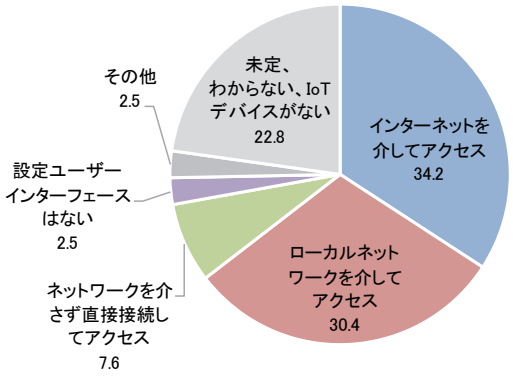


図 3-66　IoT 機器を設定するユーザーインターフェースへのアクセス方法

Q4_4　パスワードを利用したアクセス制限を行っている場合、初期パスワードはどのように設定されていますか。（n=41）

パスワードを利用したアクセス制限を行っている場合の、初期パスワードの設定方法について調査した結果、「利用者ごとに異なる初期パスワードを設定している（46.3%）」が最も多く、次いで、「個々の IoT 機器で異なる初期パスワードを設定している（17.1%）」となった。

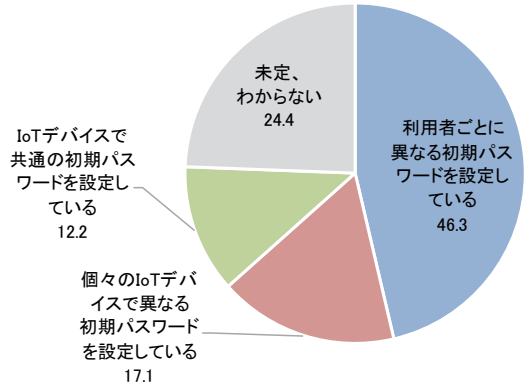


図 3-67　パスワードによるアクセス制限の際の初期パスワード

Q4_5　パスワードを利用したアクセス制限を行っている場合、パスワードの変更は可能ですか。（n=41）

パスワードを利用したアクセス制限を行っている場合の、パスワード変更について調査した結果、「パスワードは変更することもできる（58.5%）」「初期パスワードからの変更を必須としている（22.0%）」となっており、「パスワードの変更ができない」は 0%であった。

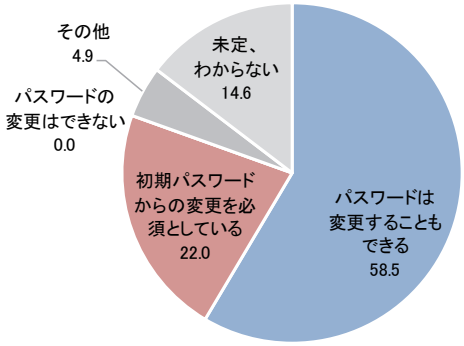


図 3-68　パスワードによるアクセス制限の際のパスワード変更の可否

Q4_6　利用する IoT 機器への脆弱性へのパッチ適用は、どのようにして行いますか。(n=79)

利用する IoT 機器への脆弱性へのパッチ適用について調査した結果、「利用者にかかわらず強制的に適用する（20.3%）」次いで「利用者が適用を行う（17.7%）」となっており、約 4 割が適用を行うという回答となった。

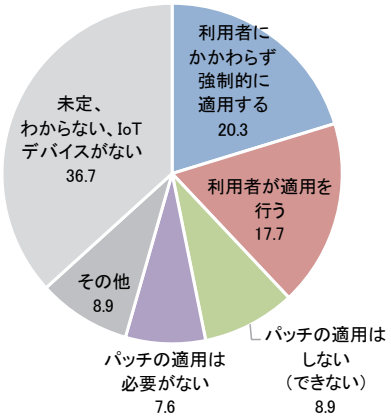


図 3-69　利用する IoT 機器への脆弱性へのパッチ適用

Q4_7　脆弱性へのパッチ適用の対象とするのはどのような IoT 機器ですか。（n=37）

パッチ適用の対象とする IoT 機器について調査した結果、「すべてのデバイスを対象とする（56.8%）」が約 6 割となった。

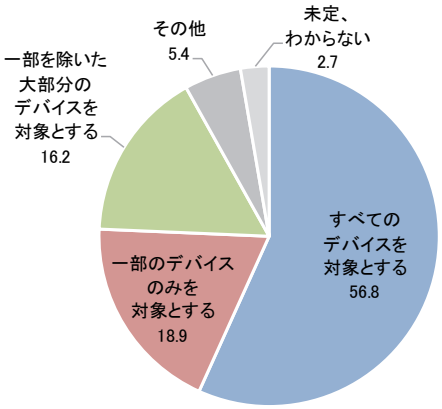


図 3-70　脆弱性へのパッチ適用の対象となる IoT 機器

5)　IoT ビジネスにおいて守るべきと考える資産について

Q5_1_MT　以下の資産のうち、守るべきと考える資産の順に、１つずつお選びください。（n=79）

守るべき資産について優先順位を評価した結果、最も守るべき資産は「人命（79.7%）」となった。二番目に守るべきは、最も守るべき回答を加算し、「個人情報やプライバシー情報等の情報資産（41.7%）」、同様に、三番目に守るべきは「金銭的な資産（35.4%）」次いで、「知財や営業情報等の機密情報資産」「ライフライン等のインフラ設備・システム」「生産設備・システム」「ブランド等を含む社会的信用ブランド等を含む社会的信用」となった。

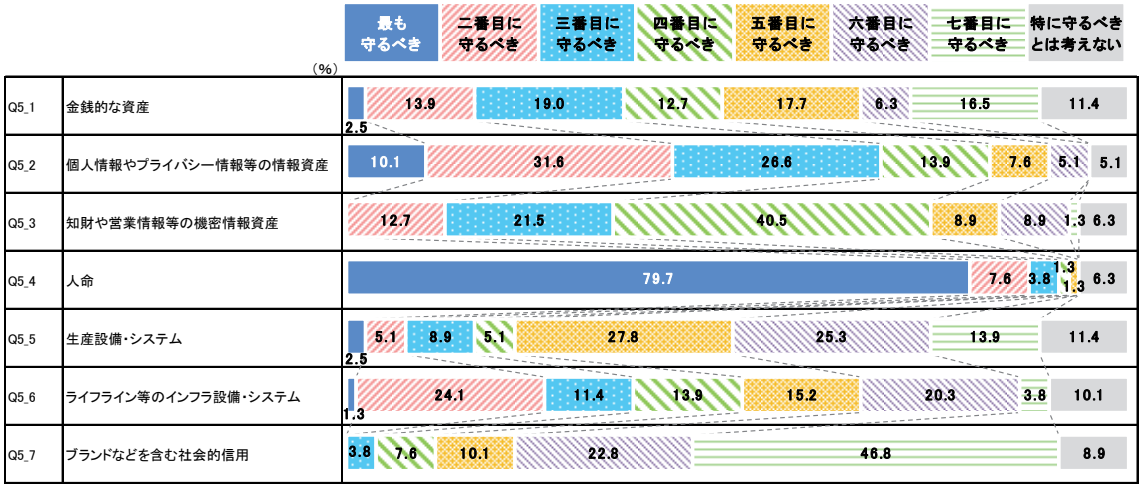


図 3-71　守るべきと考える資産

Q5_2　その他に守るべき重要な資産と考えるものがありましたらご記入ください。

以下の回答が得られた。

- センサーデータそのものから読み取れる顧客の製造技術
- Q5_1 の意図が不明。一般論を問うているのか、特定のシステムについて問うているのか、特定のシステムであったとしても複数の製品・システムでそれぞれ重要性・対象が異なる。

添付資料２：アンケート画面

1)　回答者企業属性

アンケート画面開始

Page 1

※回答中にブラウザの「戻る」を使用しないでください。（それまでの回答が無効になりますのでご注意ください）

0　50　100(%)

Q1　御社の企業属性についてお答えください。

Q1_1
御社ではIoTビジネス(IoTを活用した製品やサービス、データ利活用等)を展開していますか。
当てはまるものを1つお選びください。
なお、本調査におけるIoTビジネスの定義と事例は以下の通りです。

1 ○ IoTビジネスを展開している
2 ○ 今後IoTビジネスを展開予定である
3 ○ IoTビジネスを展開をしておらず予定もない

※IoTとは：
Internet of Thingsの略で、パソコンやスマートフォンに限らず、センサや家電、
車など様々なものがインターネットにつながる、モノのインターネットのことです。
ここで、IoTビジネスとは、IoTの技術を活用した製品やサービス、IoTにより収集したデータを
分析・活用する事業と定義します。
IoTビジネスには以下のようなものがあります。

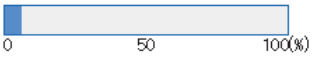
IoTビジネスの例

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
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	顧客・製品情報の収集 在庫管理の改善
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

次へ

Page 2

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)



Q1_2
御社の総従業員数(有給役員,正社員・正職員,準社員・準職員,アルバイト等を含む)について、直近の会計年度の人数(概算で結構です)をお選びください。

1 ○ 50名未満
2 ○ 50名～100名
3 ○ 101名～300名
4 ○ 301名～500名
5 ○ 501名～1,000名
6 ○ 1,001名～5,000名
7 ○ 5,001名～10,000名
8 ○ 10,001名以上

Q1_3
御社の主な業種をお選びください。

1 ○ 農業、林業
2 ○ 漁業
3 ○ 鉱業、採石業、砂利採取業
4 ○ 建設業
5 ○ 製造業
6 ○ 電気・ガス・熱供給・水道業
7 ○ 情報通信業
8 ○ 運輸業、郵便業
9 ○ 卸売業、小売業
10 ○ 金融業、保険業
11 ○ 不動産業、物品賃貸業
12 ○ 学術研究、専門・技術サービス業
13 ○ 宿泊業、飲食サービス業
14 ○ 生活関連サービス業、娯楽業
15 ○ 教育、学習支援業
16 ○ 医療、福祉
17 ○ その他サービス業
18 ○ その他

Q1_4
御社の総売上高について、直近の会計年度の金額(概算で結構です)をお選びください。

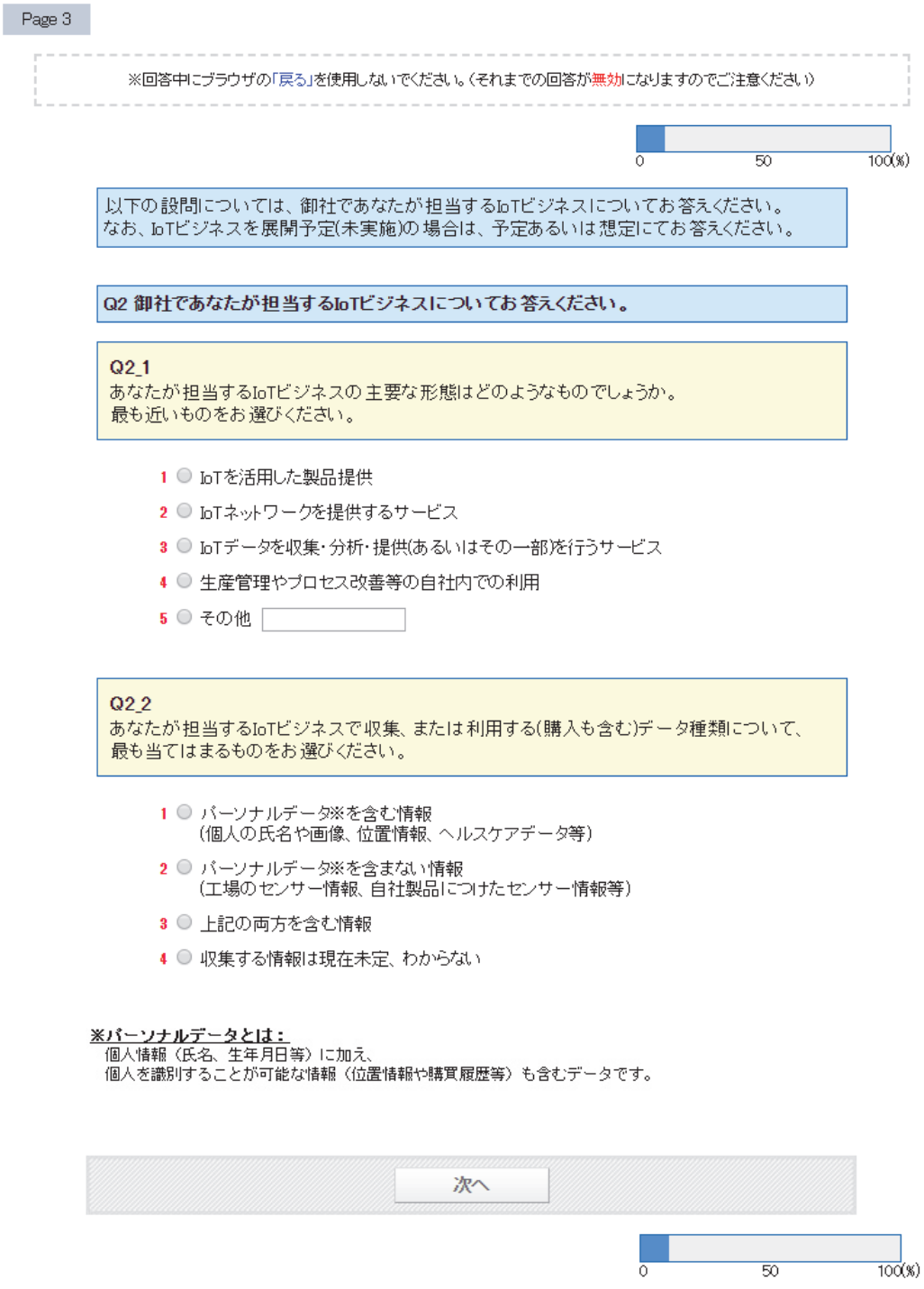
1 ○ 1億円未満
2 ○ 1億円～10億円未満
3 ○ 10億円～100億円未満
4 ○ 100億円～1,000億円未満
5 ○ 1,000億円以上
6 ○ 不明

Q1_5
あなたの所属部署として最も近いものをお選びください。

1 ○ 企画部門
2 ○ 設計開発部門
3 ○ 生産技術部門
4 ○ 品質管理部門
5 ○ 情報システム部門
6 ○ 情報セキュリティ部門
7 ○ アフターサービス部門
8 ○ サービス実施・運用部門
9 ○ 営業部門
10 ○ その他 [ ]

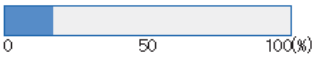
次へ

2)　担当する IoT ビジネスについて



Page 4

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)



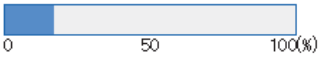
Q2_3
あなたが担当するIoTビジネスで収集または利用する(購入も含む)IoTデータは、
どのような分野のものでしょうか。
当てはまるものを全てお選びください。(いくつでも)

1 ☐ 施設管理(空調や入退室等の自動監視・制御)
2 ☐ エネルギー(施設や地域のエネルギー管理等)
3 ☐ 家庭・個人向けサービス(家庭向け安心、安全サービス、監視サービス等)
4 ☐ 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等)
5 ☐ 産業(生産プロセスの可視化・高度化、生産性向上等)
6 ☐ 運輸・物流(輸送管理の高度化、交通システム管理の高度化)
7 ☐ 小売(サプライチェーンの可視化、顧客・製品情報の収集、在庫管理の改善等)
8 ☐ セキュリティ・公衆安全(緊急機関、公共インフラ管理の監視システム等の高度化)
9 ☐ IT・ネットワーク(オフィス関連機器の監視・管理、通信インフラの監視・管理の高度化等)
10 ☐ その他 [ ]
11 ☐ 未定、わからない

Q2_4
あなたが担当するIoTビジネスではデータをどのように収集しますか。
収集方法として中心的な手段を1つお選びください。

1 ○ 自社が販売・提供した製品(センサー内蔵)からデータを収集
2 ○ 自社が社外に設置したIoTデバイス(例 監視カメラ等)から収集
3 ○ 自社内(例 工場等)に設置したIoTデバイスから収集
4 ○ 個人が所有する端末(スマートフォン等)からアプリケーション等を経由して収集
5 ○ 他社のデータを利用(購入を含む)
6 ○ その他 [ ]
7 ○ 未定、わからない

次へ



Page 5

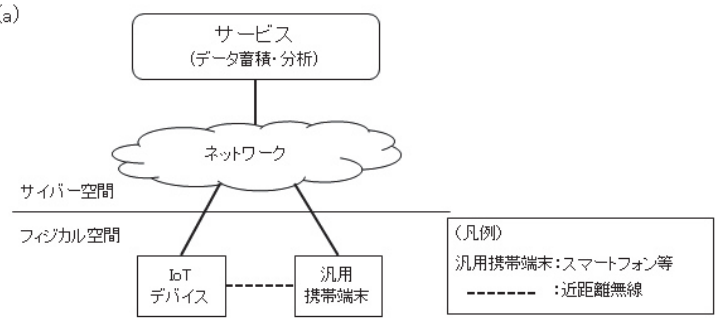
※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

0 50 100(%)

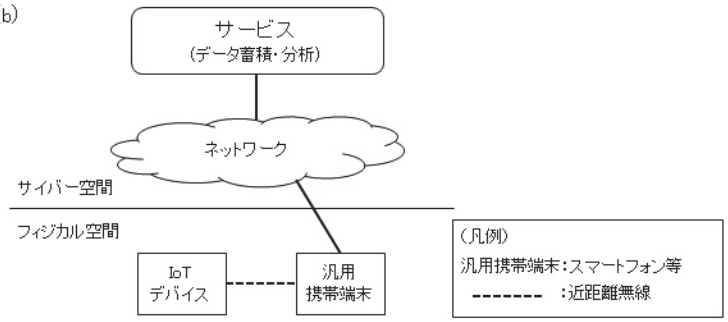
Q2_5
あなたが担当するIoTビジネスのシステム構成は、
図の(a)、(b)、(c)に当てはめるとすると、どれに最も近いですか。

1 aに当てはまる(aに近い)
2 bに当てはまる(bに近い)
3 cに当てはまる(cに近い)
4 a、b、cのパターンとは全く異なる
5 未定、わからない

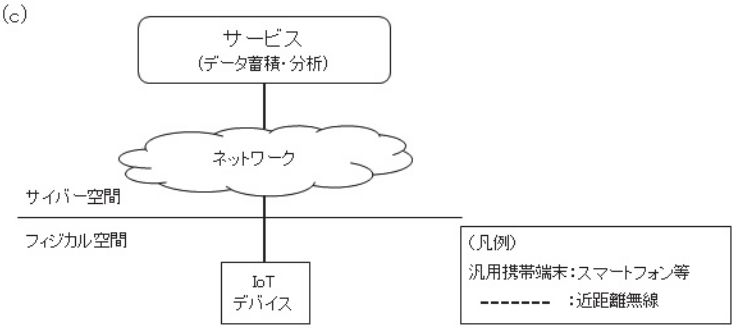
(a)



(b)



(c)



次へ

0 50 100(%)

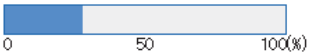
Page 6

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

Q2_6
あなたが担当するIoTビジネスで利用するIoTデバイスは、
主にどのようなものでしょうか。

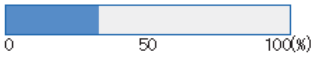
1 専用デバイス
2 機器組み込み(家電製品、複合機、カメラ、自動車など)
3 汎用モバイル端末(スマートフォン等)
4 なし
5 その他
6 未定、わからない

次へ



Page 7

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)



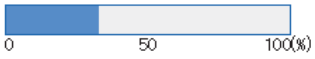
Q2_7
あなたが担当するIoTビジネスで利用するIoTデバイスは、
複数の利用者により共有されますか。

1 共用はない
2 共用がある
3 未定、わからない、IoTデバイスがない

Q2_8
あなたが担当するIoTビジネスのシステムやデータは、
他のサービスやシステムとの連携がありますか。

1 連携はない
2 連携がある
3 未定、わからない

次へ



Page 8

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

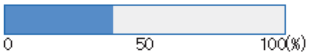
Q2_9
あなたが担当するIoTビジネスの利用者数を概数の整数でお答えください。
(おおよその人数で結構です)

[ ] 人

Q2_10
あなたが担当するIoTビジネスで利用するIoTデバイス数を概数の整数でお答えください。
(おおよその台数で結構です。また、IoTデバイスがない場合は、0とお答えください。)

[ ] 台

次へ



Page 9

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

Q2_11
あなたが担当するIoTビジネスで、
1年間でユーザーが支払う必要のある金額(機器費用やサービス費用等の合計)を
概算の整数でお答えください。
(おおよその金額で結構です)

[ ]

Q2_12
その金額の課金単位は以下のうちどれにあたりますか。

1 ○ 円/デバイス
2 ○ 円/利用者
3 ○ その他 [ ]
4 ○ 未定、わからない

次へ

3) IoT ビジネスに対する脅威について

Page 10

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

0 50 100(%)

Q3 御社のIoTビジネスに対する脅威についてお答えください。

Q3_1
あなたが担当するIoTビジネスに対してサイバー攻撃を仕掛けてくる攻撃者の意図について、次の項目に関して想定される可能性を5段階で評価してください。
(それぞれひとつずつ)

		5	4	3	2	1
	回答方向	非常に想定される。	かなり想定される。	まあまあ想定される。	やや想定される。	想定されない。
1	金銭やポイントなどの窃取	5	4	3	2	1
2	情報(個人情報や機密情報)の窃取	5	4	3	2	1
3	IoTビジネスや利用者への業務妨害	5	4	3	2	1
4	マルウエア(悪意あるソフトウェア)拡散	5	4	3	2	1
5	政治的信条の表示や社会混乱	5	4	3	2	1
6	攻撃の踏み台として利用	5	4	3	2	1
7	コインマイニングへの利用 ※仮想通貨に関する計算支援等を行わせることで報酬を受領する	5	4	3	2	1
8	盗聴や盗撮などの犯罪への悪用	5	4	3	2	1

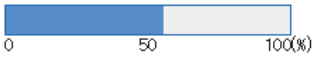
Q3_2
あなたが担当するIoTビジネスに対してサイバー攻撃を仕掛けてくる攻撃者の意図について、上記の項目以外に想定される事項があれば具体的に記入ください。

次へ

0 50 100(%)

Page 11

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

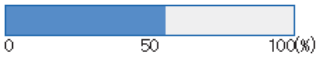


Q3_3
あなたが担当するIoTビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する方法について、
次の項目に関して想定される可能性を5段階で評価してください。
(それぞれひとつずつ)

		5 非常に想定される。	4 かなり想定される。	3 まあまあ想定される。	2 やや想定される。	1 想定されない。
	回答方向					
1	ユーザアカウントやシステム管理者アカウントの不正利用	5○	4○	3○	2○	1○
2	マルウエア感染(遠隔操作)	5○	4○	3○	2○	1○
3	DoS攻撃	5○	4○	3○	2○	1○
4	IoTデバイスの破壊(PDOS攻撃)	5○	4○	3○	2○	1○

Q3_4
あなたが担当するIoTビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する方法について、
上記の項目以外に想定される事項があれば具体的に記入ください。

次へ



Page 12

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

0 50 100(%)

Q3_5
あなたが担当するIoTビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する界面について、
次の項目に関して想定される可能性を5段階で評価してください。
(それぞれひとつずつ)

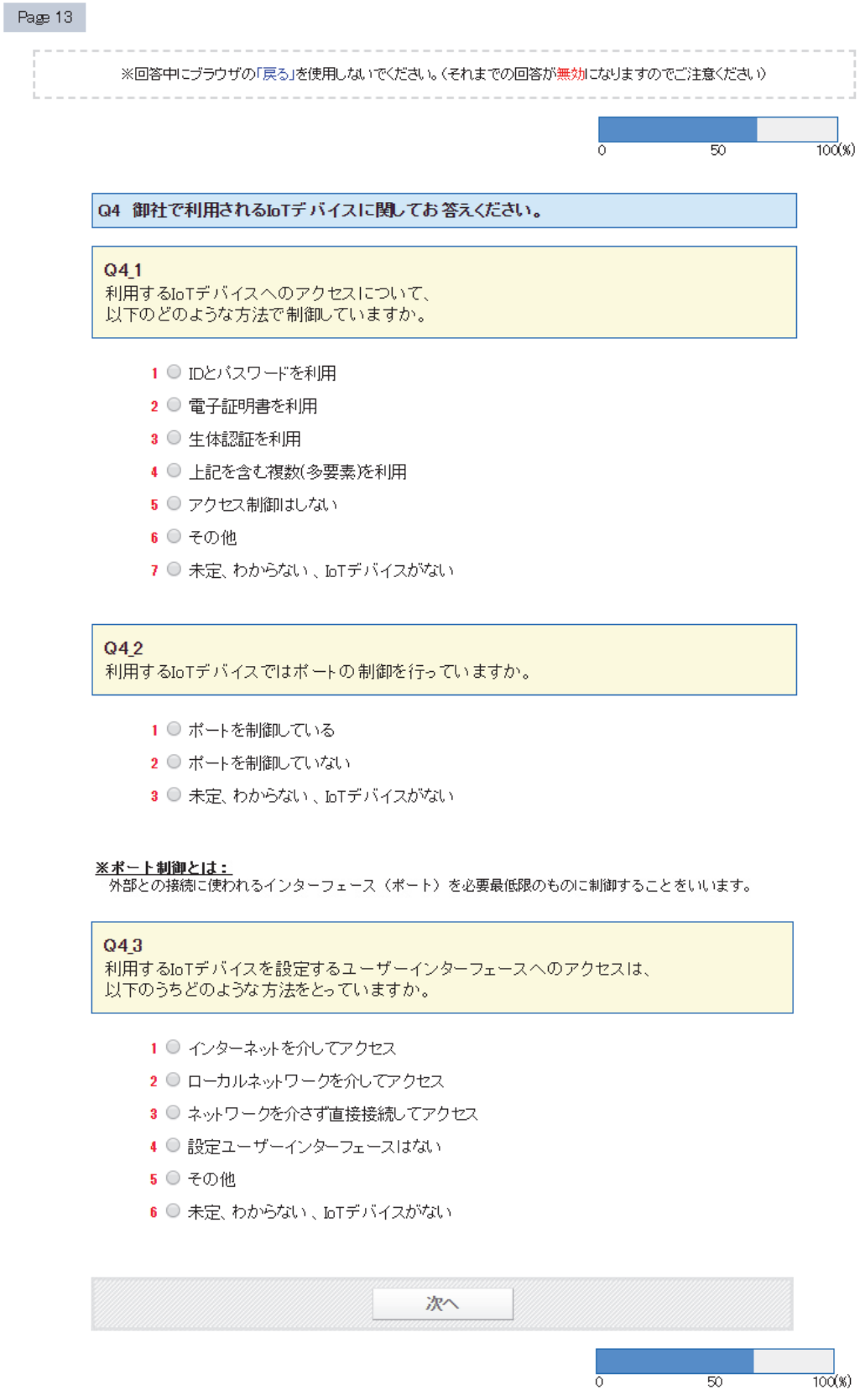
	回答方向	5 非常に想定される。	4 かなり想定される。	3 まあまあ想定される。	2 やや想定される。	1 想定されない。
1	ユーザ操作UIの脆弱性	5	4	3	2	1
2	IoTデバイスの設定画面やtelnet/ssh等の通信	5	4	3	2	1
3	IoTデバイスのOSやミドルウエアの脆弱性	5	4	3	2	1
4	センターサーバーとデバイス(あるいはエッジサーバー)との通信の脆弱性	5	4	3	2	1

Q3_6
あなたが担当するIoTビジネスに対してサイバー攻撃を仕掛けてくる攻撃者が利用する界面について、
上記の項目以外に想定される事項があれば具体的に記入ください。

次へ

0 50 100(%)

4)　利用する IoT 機器に関して



Page 13

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

0　50　100(%)

Q4　御社で利用されるIoTデバイスに関してお答えください。

Q4_1
利用するIoTデバイスへのアクセスについて、
以下のどのような方法で制御していますか。

1 IDとパスワードを利用
2 電子証明書を利用
3 生体認証を利用
4 上記を含む複数(多要素)を利用
5 アクセス制御はしない
6 その他
7 未定、わからない 、IoTデバイスがない

Q4_2
利用するIoTデバイスではポートの制御を行っていますか。

1 ポートを制御している
2 ポートを制御していない
3 未定、わからない 、IoTデバイスがない

※ポート制御とは：
外部との接続に使われるインターフェース（ポート）を必要最低限のものに制御することをいいます。

Q4_3
利用するIoTデバイスを設定するユーザーインターフェースへのアクセスは、
以下のうちどのような方法をとっていますか。

1 インターネットを介してアクセス
2 ローカルネットワークを介してアクセス
3 ネットワークを介さず直接接続してアクセス
4 設定ユーザーインターフェースはない
5 その他
6 未定、わからない 、IoTデバイスがない

次へ

0　50　100(%)

Page 14

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

Q4_4
パスワードを利用したアクセス制限を行っている場合、
初期パスワードはどのように設定されていますか。

1 ○ IoTデバイスで共通の初期パスワードを設定している
2 ○ 個々のIoTデバイスで異なる初期パスワードを設定している
3 ○ 利用者ごとに異なる初期パスワードを設定している
4 ○ その他
5 ○ 未定、わからない

Q4_5
パスワードを利用したアクセス制限を行っている場合、パスワードの変更は可能ですか。

1 ○ パスワードの変更はできない
2 ○ パスワードは変更することもできる
3 ○ 初期パスワードからの変更を必須としている
4 ○ その他
5 ○ 未定、わからない

次へ

Page 15

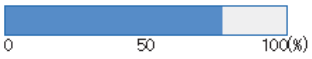
※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

Q4_6
利用するIoTデバイスへの脆弱性へのパッチ適用は、どのようにして行いますか。

1 ○ パッチの適用は必要がない
2 ○ パッチの適用はしない(できない)
3 ○ 利用者が適用を行う
4 ○ 利用者にかかわらず強制的に適用する
5 ○ その他
6 ○ 未定、わからない 、IoTデバイスがない

※パッチとは：
ソフトウェア等を改修するためのプログラムで、脆弱性をもたらす不具合の修正などに利用されるものです。

次へ



Page 16

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

Q4_7
脆弱性へのパッチ適用の対象とするのはどのようなIoTデバイスですか。

1 ○ すべてのデバイスを対象とする
2 ○ 一部を除いた大部分のデバイスを対象とする
3 ○ 一部のデバイスのみを対象とする
4 ○ その他
5 ○ 未定、わからない

※パッチとは：
ソフトウェア等を改修するためのプログラムで、脆弱性をもたらす不具合の修正などに利用されるものです。

次へ

5) IoT ビジネスにおいて守るべきと考える資産について

Page 17

※回答中にブラウザの「戻る」を使用しないでください。(それまでの回答が無効になりますのでご注意ください)

0 50 100(%)

Q5 IoTビジネスにおいて守るべきと考える資産についてお答えください。

Q5_1
以下の資産のうち、守るべきと考える資産の順に、1つずつお選びください。
(それぞれひとつずつ)

	回答方向	最も守るべき	二番目に守るべき	三番目に守るべき	四番目に守るべき	五番目に守るべき	六番目に守るべき	七番目に守るべき	特に守るべきとは考えない
1	金銭的な資産	1	2	3	4	5	6	7	8
2	個人情報やプライバシー情報等の情報資産	1	2	3	4	5	6	7	8
3	知財や営業情報等の機密情報資産	1	2	3	4	5	6	7	8
4	人命	1	2	3	4	5	6	7	8
5	生産設備・システム	1	2	3	4	5	6	7	8
6	ライフライン等のインフラ設備・システム	1	2	3	4	5	6	7	8
7	ブランドなどを含む社会的信用	1	2	3	4	5	6	7	8

Q5_2
その他に守るべき重要な資産と考えるものがありましたらご記入ください。

次へ

0 50 100(%)

平成 30 年度情報セキュリティ調査報告書
ーサイバーフィジカルシステムの実現に向けた
セキュリティ脅威とリスク分析に関する調査ー

発　行　日　　平成31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