平成 29 年度

電子情報利活用研究レポート

一般財団法人日本情報経済社会推進協会　電子情報利活用研究部

序文

IoT（Internet of things：モノのインターネット）で様々な機器やデータ等がつながり、業界横断した活用が進むと、ビジネスや社会全般に大きな革新をもたらすと期待されている。欧米では、IoT を第 4 次産業革命として捉え、ドイツの「インダストリー4.0」や、米国の「インダストリアル・インターネット」が生まれており、産業の変革の中で IoT という考え方から実態に変化している。

我が国においては、IoT の考え方が生まれる前から、TQC（Total Quality Control）やカイゼン（トヨタ生産方式）等に代表されるように、データを活用することで一連のプロセスを見える化するとともに、顧客ニーズを吸い上げ、生産や開発にフィードバックするなどして、世界的な競争力を維持しているとともに、IoT を活用したビジネスの事例も創出し始めている 。また、政府においては、2017 年 6 月 9 日に「未来投資戦略 2017」を閣議決定し、第 4 次産業革命の社会実装を通じた「Society5.0・Connected Industries」を提唱し、働き方改革及び人材活用を通じた「生産性の向上」や、イノベーションの促進等により、2020 年までに GDP600 兆円経済の実現が盛り込まれているとともに、2017 年 7 月 6 日には、欧州委員会との間で、日本と EU の間の個人データの保護に関する共同声明を発表し、個人データ保護レベルについての「十分性認定」について、相手国として日本を優先的に検討する方針を確認するなど、データを横断的に活用するにあたっての具体的な動きが出てきている。

以上のような動きを踏まえ、IoT、ビッグデータ、人工知能（AI）などの技術革新によって、データの到達コストが圧縮され、モノ作り、交通、医療、農業など、様々な分野でイノベーションが生まれる機運が高まっている。これは、我が国が世界に先駆けて第 4 次産業革命を実現するチャンスでもある。

当協会電子情報利活用研究部では、IT に関する調査研究を推進していることから、上記のような世界的な潮流について触れる機会が多い。また、事業プログラム制度等産業界と連携した研究会なども実施しており、国内のニーズやシーズに触れる機会も多い。

そこで、今年度より、年度ごとに調査研究した内容を整理し、読みやすいレポートとして公開することとした。

一部、委託調査などの関係もあるため、記載できない内容もあるが、産業界等がイノベーションについて考える場合などの参考にはなれば幸いである

一般財団法人日本情報経済社会推進協会
電子情報利活用研究部　部長
坂下　哲也

目次

序文 i
1. 調査研究１：データ保護と利活用 1
1.1. 調査研究の視点 1
1.1.1. 背景 1
1.1.2. データ保護と利活用のバランス 1
1.2. 調査研究の対象 2
1.3. 国際的な個人情報保護及びデータ流通・活用のための制度整備の最新動向調査結果 3
1.3.1. 欧州におけるデータ保護法制（GDPR）の概要と状況 3
1.3.2. アジア太平洋地域におけるデータ保護法制（APEC プライバシーフレームワーク）の概要と状況 8
1.3.3. 日欧亜の個人情報保護法制の概略比較（概要の比較整理） 10
1.3.4. ISO（国際標準化機構）におけるプライバシー関連の規格 13
1.4. 考察 17
1.4.1. 国際的な法制度への対応と越境移転 17
1.4.2. 越境移転に対する企業の関心 17
1.4.3. 個人データ保護をめぐる今後の動向 21
1.5. 参考文献 23
2. 調査研究２：IoT セキュリティについて 24
2.1. 調査研究の視点 24
2.2. 調査研究の対象 26
2.3. IoT システムにおける ISMS 適用可能性の調査結果 27
2.4. 考察 42
2.5. 参考文献 43
3. 調査研究３：オンライン完結社会の実現に向けて 44
3.1. 調査研究の視点 44
3.2. 調査研究の対象 45
3.3. オンライン完結に向けた電子認証のセキュリティについての調査結果 46
3.3.1. NIST SP800-63-3 について 46
3.3.2. Assurance Level について 47
3.3.3. SP800-63-3 の日本語訳について 50
3.4. 考察 50
3.5. 参考文献 54

1. 調査研究１：データ保護と利活用

1.1. 調査研究の視点

1.1.1. 背景

平成 29 年度は、5 月に改正個人情報保護法が全面施行され、個人情報保護委員会の役割も明確化されるなど、データ保護に関する新たな法制度の運用が本格的にスタートした節目の年となった。また、昨今のクラウドコンピューティング環境の普及により、データを組織内のハードウェアに保有せず、クラウド環境に保管し、共有・活用する手法は一般的になってきている。インターネット環境においては、データの保管・共有・活用が簡便になる一方、データ漏洩や第三者からの攻撃のリスクも高まっており、データを適切に保護しつつ活用するということは企業活動を行ううえで必須の対応と言える。

一方、海外では、欧州における一般データ保護規則（General Data Protection Regulation：通称 GDPR）[1]の施行が 2018 年 5 月に予定されているなど、日本国内同様にデータ保護と利活用のための法制度整備が急速に進められている。また、日本企業も多数の支社や支店を置くアジア太平洋地域においても、各国がデータ保護と利活用のための法制度整備を着々と進めており、企業がグローバルに活動を行う上では、欧米だけでなくアジア諸国を含む国際的な法制度の確認と対応が必要な時代となっている。

1.1.2. データ保護と利活用のバランス

企業活動の中で、顧客情報や従業員情報（所謂、個人データ）の取り扱いは日常的に行われているが、これらは営業秘密情報などと同様、企業内で適切に管理すべき情報である。個人データは個人情報保護法により明確な保護を要求される対象であるのは自明だが、企業活動という視点からすれば、企業秘密に該当する情報などの内部情報も適切な管理が必要であり、個人データだけが特別な存在というわけではない。この視点は、個人情報保護法を正しく理解し対応することを実現する上で重要な視点の一つであろう。個人情報保護法は、その名の通り個人情報の保護に関する法律であるが、その内容は個人情報の保護だけを規定しているわけではなく、「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資する」（同法第一条）とも書かれている。

---

[1] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則（一般データ保護規則）

個人情報保護法　第一条
「この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。」

一方、海外に目を向けると、欧州の GDPR も「個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則」という正式名称が示すとおり、個人情報保護法同様に個人情報の保護だけを目的としてはおらず、データの自由な移転（データフリーフロー）も目的に掲げている点が特徴的である。アジア太平洋地域では、APEC プライバシーフレームワーク[2]があるが、個人情報保護法や GDPR 同様、適切な個人情報の保護を実現しつつ、データフリーフローを促進し、デジタル経済の発展を目的としている。

これら「個人情報を適切に保護し、活用することで経済発展を推進する」という考え方は、OECD プライバシーガイドライン[3]以降の国際的な潮流である。すなわち、国際的な流れとしても、個人情報の保護と利活用のバランスに注意しつつ、新たな産業の創出や活性化を目指した法制度整備が進んでいると言えよう。

1.2. 調査研究の対象

上記「1.1 調査研究の視点」に基づき、平成 29 年度の調査研究テーマの一つとして、主に国際的なデータ保護と利活用に関する法制度の調査を実施し、その内容を概括することとした。

特に、国際的な影響力が大きく、グローバル企業の関心も高い GDPR に関しては、過去に当協会で仮訳を作成して公開[4]するなど、継続的な調査を実施していること、施行が 2018 年 5 月と目前に控えていることなどの理由から、重点的な調査対象と位置づけた。さらに、GDPR だけではなく、アジア太平洋地域におけるデータ保護法制度に関しても概要を調査

[2] APEC Privacy Framework　https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[3] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[4] https://www.jipdec.or.jp/library/archives/gdpr.html

し、特徴を整理することとした。調査のポイントとしては、法制度の特徴、個人情報保護法との差異、企業にとっての影響等を観点とし、国内企業が留意すべき事項として整理を行うこととした。

また、本調査では、ISO における個人情報保護やプライバシー関連の規格についても、その最新動向の調査を実施した。ISO 規格は文字通り国際的な標準規格であり、企業の国籍や活動領域の法制度に依存していない点において、各国や地域の法制度と比較し、よりグローバルな共通言語になりうる存在と言える。当協会は ISO 等の国際標準化団体が策定する国際規格についても随時動向を調査しているが、特に ISO/IEC JTC 1/SC27/WG5（アイデンティティ管理とプライバシー技術）[5] では、個人情報保護やプライバシーに関する各種ガイドラインやデータ保護のためのマネジメント規格等を検討・策定していることから、重要な調査対象と位置づけた。

図表 1　調査対象

調査対象	概要
GDPR	概要と特徴を整理し、個人情報保護法との比較・分析を実施
APEC プライバシーフレームワーク	
ISO/IEC JTC 1 SC27/WG5	規格策定の最新動向を調査・整理

1.3. 国際的な個人情報保護及びデータ流通・活用のための制度整備の最新動向調査結果

国際的な個人情報保護及びデータ流通・活用のための制度整備の最新動向調査として、欧州及びアジア太平洋地域における法制度の状況と、ISO における国際標準化状況の調査を実施した。

1.3.1. 欧州におけるデータ保護法制（GDPR）の概要と状況

GDPR は、2016 年 4 月に欧州議会と理事会により規則案の内容が承認され、2018 年 5 月に施行されることが決定した。以後、欧州でビジネスを行う企業は GDPR 対応が必須とされ、日本国内でも平成 29 年度（2017 年～2018 年）を境に多くの勉強会やセミナー等が開催されている。

[5] ISO/IEC JTC1/SC27（IT Security techniques）内には、WG1 から WG5 までの作業部会が存在し、うち WG5 がアイデンティティ管理とプライバシー技術の検討を行っている。
https://www.iso.org/committee/45306.html

図表 2　GDPR 策定の経緯

時期	対象文書
1995 年	EU 一般データ保護指令　採択
2012 年	EU 一般データ保護規則（案）　公表
2016 年 4 月	EU 一般データ保護規則（GDPR）　承認
2017 年 10 月頃～	GDPR 関連の各種ガイドライン　発行（随時）
2018 年 5 月	EU 一般データ保護規則（GDPR）　施行（予定）
2018 年 5 月	ePrivacy 規則　施行（予定）

当協会では、2016 年 4 月に GDPR 規則案が承認されたことを受け、対応検討のための資料として同年 8 月に当協会の Web サイトを通じて「仮訳」を公開するなど、継続的な調査を行ってきた。ここでは、当協会が作成した仮訳版をもとに、GDPR の概要について整理する。

図表 3　目次構成（仮訳より抜粋）

第 1 章　総則
第 2 章　諸原則
- 個人データの取扱いに関する原則
- 適法な取扱い
- 同意の条件
- 情報社会サービスに関する子どもの同意に対して適用される条件
- 特別な種類の個人データの取扱い
- 有罪判決及び犯罪に係る個人データの取扱い
- 識別を要求しない取扱い

第 3 章　データ主体の権利
- データ主体の権利行使のための透明性のある情報、通知及び手続
- データ主体から個人データを収集する場合に提供される情報
- データ主体から個人データを取得しない場合に提供される情報
- データ主体のアクセス権
- 訂正の権利
- 消去の権利（忘れられる権利）
- 取扱い制限の権利
- 個人データの訂正若しくは消去又は取扱いの制限に関する通知義務
- データポータビリティの権利
- 異議を唱える権利
- プロファイリングを含む自動化された個人意思決定

第 4 章　管理者及び取扱者
- 一般的義務
- 個人データの保護
- データ保護影響評価及び事前協議
- データ保護オフィサー
- 行動規範及び認証

第 5 章　第三国又は国際機関への個人データ移転
- 移転に関する一般原則
- 十分性決定に基づく移転
- 適切な保護措置に従った移転
- 拘束的企業準則
- EU 法によって認められていない移転又は開示
- 特定の状況における例外
- 個人データ保護に関する国際協力

第 6 章　独立監督機関
第 7 章　協力及び一貫性
第 8 章　救済、法的責任及び制裁
第 9 章　特別な取扱い状況に関する条項
第 10 章　委任行為及び実施行為
第 11 章　最終条項

図表 4　GDPR の概要（特徴的なものを抜粋）

特徴	概要
目的	個人データの保護に対する権利という基本的人権の保護を目的とするものであり、第 1 条において、以下の通りに規定されている。 1. 本規則は、個人データの取扱いに係る自然人の保護に関する規定及び個人データの自由な流通に関する規定を定める。 2. 本規則は、自然人の基本的権利及び自由、並びに、特に彼らの個人データ保護の権利を保護する。 3. EU 域内の個人データの自由な移動は、個人データの取扱いに係る自然人の保護に関連する理由によって、制限又は禁止されてはならない。
適用範囲	第 3 条 1 項 EU 域内の管理者又は取扱者の事業所の活動に関連してなされる個人データの取扱いに適用される。この場合、その取扱いが EU 域内又は域外でなされるか否かについては問わない。 第 3 条 2 項 本規則は、EU 域内に拠点のない管理者又は取扱者による EU 在住のデータ主体の個人データの取扱いに適用される。ただし、取扱い活動が次に掲げる項目に関連しているものに限られる。 a) EU 在住のデータ主体に対する商品又はサービスの提供に関する取扱い。この場合、データ主体に支払が要求されるか否かについては問わない。 b) EU 域内で行われるデータ主体の行動の監視に関する取扱い。 第 3 条 3 項 本規則は、EU 域内に拠点を持たない管理者による個人データの取扱いにも適用されるが、国際公法により加盟国の国内法が適用される場所にある管理者による取扱いの場合に限られる。
定義：個人データ	「個人データ」とは、識別された又は識別され得る自然人（以下「データ主体」という。）に関するあらゆる情報を意味する。識別され得る自然人は、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子、又は当該自然人に関する物理的、生理的、遺伝子的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な一つ若しくは複数の要素を参照することによって、直接的に又は間接的に、識別され得る者をいう。
定義：管理者（Controller）	「管理者」とは、単独で又は他と共同して、個人データの取扱いの目的及び手段を決定する自然人、法人、公的機関、行政機関又はその他の団体をいう。当該取扱いの目的及び手段が EU 法又は加盟国の国内法によって決定される場合には、管理者又は管理者の指定に関する特定の基準は、EU 法又は加盟国の国内法をもって定めることができる。
定義：取扱者（Processor）	「取扱者」とは、管理者のために個人データの取扱いを行う自然人、法人、公的機関、行政機 関又はその他の団体をいう。 （※「処理者」と訳される場合もある）
原則：同意取得	データ主体の「同意」とは、強制を受けず、特定的に、情報提供を受けたうえでかつ曖昧でないデータ主体の意思表示であることを意味する。その意思は、当該データ主体が、宣言又は明らかな積極的行為によって、自己に係る個人デ

特徴	概要
	ータの取扱いに合意(agreement)して表すものとする。
特別な種類の個人データの取扱い	人種若しくは民族的素性、政治的思想、宗教的若しくは哲学的信条、又は労働組合員資格に関する個人データの取扱い、及び遺伝データ、自然人の一意な識別を目的とした生体データ、健康に関するデータ又は自然人の性生活若しくは性的指向に関するデータの取扱いは禁止する。
データ主体の権利	（代表的なものとして、以下を規定　※一部のみ抜粋） 第 7 条 3 項 データ主体は、いつでも同意を撤回する権利があるものとする。また、同意の撤回は撤回前の同意に基づく取扱いの合法性に影響を与えない。データ主体は、同意を与える以前にその旨が通知されていなければならない。同意の撤回は、その付与と同程度に容易なものでなければならない。 第 17 条 消去の権利（忘れられる権利） データ主体は当該データ主体に関する個人データについて管理者に不当に遅滞することなく消去させる権利を持つものとする。 第 20 条 データポータビリティーの権利 データ主体は、当該データ主体が管理者に提供した当該データ主体に関する個人データについて、構造化され、一般的に利用され機械可読性のある形式で受け取る権利があり、当該データを、個人データが提供された管理者の妨害なしに、他の管理者に移行する権利がある。
データ保護影響評価（DPIA）	第 35 条 データ保護影響評価 特に新たな技術を用いるなどのある種の取扱いが、その性質、範囲、文脈及び取扱いの目的を考慮して、自然人の権利や自由に高リスクを生じさせる可能性がある場合、管理者は、取扱いの前に、予定された取扱い作業の個人データ保護への影響評価を実施しなければならない。 データ保護影響評価は、以下の場合に特に必要となる（第 35 条第 3 項)。 ・ プロファイリングを含めた自動処理に基づいて自然人に関する個人的側面が体系的かつ広範囲に評価され、当該評価に基づいて自然人に関して法的効果を発生させまたは類似の重大な影響を及ぼす決定が行われる場合 ・ 特別カテゴリの個人データまたは有罪判決および犯罪に関する個人データを大規模に処理する場合 ・ 一般の人々がアクセス可能な空間において大規模な体系的監視を行う場合 第 36 条 事前協議 管理者は、第 35 条に基づくデータ保護影響評価が管理者によるリスクを軽減する対策の非存在下で取扱いが高リスクを生じさせ得るとことを示す場合、取扱いの前に監督機関と協議しなければならない。
データ保護オフィサー（DPO）	DPO の意義： DPO とは、GDPR の内部における遵守を監視するために、管理者または取扱者を支援するために専任されるデータ保護法およびその実務に関する専門知識を有するものとして専任される者 DPO の任務：

特徴	概要
	少なくとも第 39 条第 1 項に列挙されたタスク、例えば、GDPR およびその他の EU および加盟国の条項に基づく義務について管理者・取扱者および個人データを処理する従業員に対し情報と助言を提供すること、管理者・取扱者の個人データ保護方針の遵守を監視すること等を行うこと DPO の選任： 専門家としての質、特にデータ保護法およびその実務の専門知識ならびに任務を遂行する技量に基づいて選任されるものとする（IAPP（国際プライバシー専門家協会）の CIPP/E は GDPR を含む EU データ保護法の専門知識を有することを示すものであり国際的に認められている資格である）。管理者または取扱者の従業員、または業務委託契約に基づいて任務を遂行するものでもよい。 DPO の地位： ・ 管理者・取扱者は、DPO が個人データ保護に関する一切の事柄について適切、適時に取り組むことを確保。 ・ 管理者・取扱者は DPO が任務の遂行に係わる指示を一切受けないことを確実にしなければならない。DPO は当該任務の遂行について管理者・取扱者から解雇または処罰を課されないものとする。 ・ DPO は、管理者または取扱者の最高経営レベルに直接報告を行なうものとする。 ・ DPO は、その他の任務や義務も遂行できるものとする。管理者または取扱者は、そのような任務や義務が利益相反にならないよう確実にしなければならない。
行動規範及び認証	第 40 条 行動規範 加盟国、監督機関、欧州データ保護会議及び欧州委員会は、様々なデータ取扱い分野の具体的特徴並びに零細及び中小事業の具体的要望を考慮し、本規則の適切な適用に寄与することを意図した行動規範の作成を推奨しなければならない。 第 42 条 認証 加盟国、監督機関、欧州データ保護会議及び欧州委員会は、特に EU 規模において、管理者及び取扱者による取扱い作業に関する本規則の遵守を証明する目的で、データ保護認証メカニズム、データ保護シール及びマークの確立を奨励するものとする。零細及び中小事業に特有の要望は考慮されなければならない。 **※GDPR では、行動規範及び認証について規定されているが、詳細が示されていない。具体的な行動規範や認証のためのプログラム等については、別途ガイドラインにて詳細が提示される見通しである。**
データの越境移転	第 45 条 十分性決定に基づく移転 第三国又は国際機関への個人データの移転は、当該第三国、第三国域内の領域若しくは一つ若しくは複数の特定された部門、又は国際機関が保護に関して十分なレベルを保証していると欧州委員会が決定した場合に行うことができる。 **※平成 30 年 3 月現在において、個人情報保護委員会と欧州委員会間で日本が十分性決定の適用を受けるかどうかについて協議中である。**

特徴	概要
	第 47 条 拘束的企業準則（BCR） 事業体グループ又は共同経済活動に従事する事業者グループ内で、一カ国又は複数の第三国における管理者又は取扱者に対して個人データ移転又は一連の個人データ移転のため、加盟国の領域上にある管理者又は取扱者によって遵守される個人データ保護方針 **※平成 30 年 3 月現在において、楽天株式会社がルクセンブルグの監督当局からBCR承認取得済み。株式会社インターネット・イニシアティブ（IIJ）は英国の監督当局に申請中。その他、2018 年 3 月初め時点で少なくとも数社の BCR 申請が完了。** 標準契約条項（Standard Contractual Clauses：SCC） 上記のほか、SCC を締結することにより、データの越境移転が可能となる。 **※欧州委員会が決定したデータ移転契約のひな型で、個人データの移転を GDPR 上適法化するためのものである。日本の多くの企業は、GDPR 上のデータ移転規制に、SCC を締結することにより対応を行っている。**

1.3.2. アジア太平洋地域におけるデータ保護法制（APEC プライバシーフレームワーク）の概要と状況

欧州における GDPR と同様、アジア太平洋経済圏においても、APEC が定めるデータ保護の枠組みが存在する。ただし、GDPR が EU 加盟国共通の規則として位置づけられているのに対し、APEC プライバシーフレームワークはあくまでも枠組みであり、APEC 加盟国に対する勧告レベルの文書という位置づけである。したがって、国際的な法制度のレベルまでは至っていない。ただし、GDPR 同様、根本的な思想は OECD プライバシーガイドラインに基づいて作成されており、要求内容の大小に差異があるとは言え、データ保護において重要とする事項は概ね同様のことが記されている。また、データ越境移転に関しては CBPR（Cross Border Privacy Rules）というメカニズムを規定し、各加盟エコノミーは CBPR のメカニズムを構築したうえで、個人データの流通を推進しているという点が特徴である。

図表 5　目次構成

第 1 部 序文

第 2 部 適用範囲
定義
その他の定義
適用

第 3 部 APEC 情報プライバシー原則
1.被害の防止
2.通知
3.収集の制限

第 4 部 実施
A.国内における実施の手引き
1.プライバシー保護と情報流通の利益の最大化
2. APEC プライバシーフレームワークの効果
3.プライバシー管理プログラム
4.プライバシー保護のための技術的対策の推進
5.公立の教育とコミュニケーション
6.公的部門と民間部門の協力
7.プライバシー保護侵害に対する適切な救済策の提供
8. APEC プライバシーフレームワークの国内導入の報告メカニズム

4.個人情報の利用	B.国際的な実施
5.選択	1.加盟国間の情報共有
6.個人情報の完全性	2.調査と実施における国境を越えた協力
7.安全保護	3.国境を越えたプライバシーの仕組み
8.アクセスと修正	4.越境移転
9.アカウンタビリティ	5.プライバシーフレームワーク間の相互運用性

図表 6　APEC プライバシーフレームワークの概要（特徴的なものを抜粋）

特徴	概要
目的	APEC 加盟エコノミー[6]における整合性のある個人情報保護への取組を促進し、情報流通に対する不要な障害を取り除くこと。
適用範囲	APEC 加盟エコノミーが対象となる。 APEC 加盟エコノミーに対して適用を推奨。適用に際しては、加盟エコノミーにおける個別事情を考慮すべきであるとされている。
定義：個人データ	個人情報（personal information）とは、識別される、あるいは識別されうる個人に関するあらゆる情報を意味する。
定義：管理者	個人情報管理者（Personal information controller）とは、個人情報の収集、保持、処理、使用、開示、移転を管理する個人または組織を意味する。 これには、他の人や組織に、個人情報を収集、保持、処理、使用、転送または開示するよう指示する人物または組織が含まれるが、他の人や組織が指示したような機能を実行する人物や組織は除く。 **※GDPR とは異なり、明確な処理者（processor）の定義は存在しない。**
フレームワークの適用	原則： 各加盟エコノミーの社会的、文化的、経済的、法的背景の違いを考慮して、これらの原則を柔軟に実施すべきである。 注釈： 電子商取引では、APEC 内のすべての法律や慣行が同一である必要はないが、APEC 諸国間のプライバシー保護との互換性のあるアプローチは、国際商取引とプライバシー執行の協力を大いに促進する。 枠組みは、各エコノミーの社会的、文化的およびその他の相違点を考慮する必要性を認識している。

[6] APEC では、各加盟国のことを”economy”と称すため、そのままエコノミーと表記した。平成 30 年 3 月現在、APEC 加盟エコノミーはアジア太平洋地域の 21 の国と地域である。
http://www.mofa.go.jp/mofaj/gaiko/apec/soshiki/gaiyo.html

特徴	概要
プライバシー保護と情報流通の利益の最大化	（第 35 項） 個人情報は、個人のプライバシーを保護する方法で収集、保持、処理、使用、移転、開示され、個人および経済界が国境を越えた情報の流れの便益を最大にすることを可能にする。 （第 36 項） したがって、APEC プライバシーフレームワークを実現するためのプライバシー保護の確立またはレビューの一環として、各エコノミーは、情報フローへの不必要な障壁を特定し、除去し、そのような障壁の発生を回避するための合理的で適切な措置を講じるべきである。
国境を越えたプライバシーの仕組み	（第 65 項） APEC は、国境を越えた自由な個人情報の流れを維持しながらプライバシーを保護することの重要性を認識し、例えば CBPR システムの使用を通じて情報が安全かつ確実に流れる条件を提供するために、加盟国にフレームワークの準拠を奨励する。 （第 67 項） 各エコノミーは、データの越境移転を実施するための実践的メカニズムを提供する CBPR システムを開発し、CBPR システムに基づき、データの越境移転を実施する組織が個人情報のプライバシーを保護していると自己宣言する方法により、国境を越えて個人情報を保護する。
越境移転	（第 69 項） 各エコノミーは、(a) 他のエコノミーがフレームワークに影響を及ぼす立法上または規制上の手段を備えているか、(b) 十分な保護手段が存在する場合には、それ自体が他のエコノミーとの間で個人情報の越境を制限することを控えるべきである。 （CBPR のような）有効な執行メカニズムと適切な措置を含め、個人情報管理者が実施する枠組みおよびそれを実施する法律や方針と一致した継続的なレベルの保護を保証する。 （第 70 項） 個人情報の越境移転への制限は、情報の機密性と国境を越えた移転の目的と背景を考慮して、譲渡によって提示されるリスクに比例するものでなければならない。

1.3.3. 日欧亜の個人情報保護法制の概略比較（概要の比較整理）

グローバルな企業活動を行う上で企業が最も留意する点は、国内と海外（もしくは特定の外国）において、どのような対応の違いを要求されるのか、という点であろう。ここでは、日本（個人情報保護法）、欧州（GDPR）、アジア太平洋地域（APEC）それぞれの個人データ保護に関する事項を整理し、三者の比較を試みた。

図表 7　日本及び欧州、アジア太平洋地域における個人データ保護法制の概略整理

比較ポイント	日本（個人情報保護法）	欧州（GDPR）	アジア太平洋（APEC プライバシーフレームワーク）
目的	個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護すること	個人データの取扱いに対する自然人の基本的権利及び自由、特にプライバシー権の保護。	APEC 加盟エコノミーにおける整合性のある個人情報保護への取組を促進し、情報流通に対する不要な障害を取り除くこと。
適用範囲	日本国内	EEA[7]域内	APEC 加盟の 21 の国と地域
個人データの定義	GDPR や APEC における定義と比較して、やや限定的	両者ともほぼ同等の定義（識別される、あるいは識別されうる個人に関するあらゆる情報を指す）であり、日本の個人情報保護法での定義よりも広義	
明示的な同意取得	具体的な同意の定義が示されていないが、個人データの収集・利用・第三者提供等において個人の同意が必要である旨が規定されている。	データ主体の「同意」とは、強制を受けず、特定的に、情報提供を受けたうえでかつ曖昧でないデータ主体の意思表示であることを意味する。その意思は、当該データ主体が、宣言又は明らかな積極的行為によって、自己に係る個人データの取扱いに合意(agreement)して表すものとする。	具体的な同意の定義が示されていないが、個人データの収集・利用・第三者提供等において個人の同意が必要である旨が規定されている。
配慮が必要な個人データ	要配慮個人情報として定義 「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するもの」	特別な種類の個人データとして定義 日本の個人情報保護法での定義とほぼ同じ内容が定義されている	特に明示されていない

[7] EEA：European Economic Area（欧州経済領域）。EU 加盟 28 カ国に、アイスランド、リヒテンシュタイン、ノルウェーの三国を加えた国々を指す。

比較 ポイント	日本 （個人情報保護法）	欧州 （GDPR）	アジア太平洋 （APEC プライバシーフレームワーク）
情報主体の権利	個人の権利権益を侵害してはならないとされているが、明確な個人の権利については特に示されていない。 （事業者が個人からの要求には応えなければならないという書き方になっている）	個人の権利を明確に示しており、それらの権利を侵害してはならないとしている。 例：データアクセスの権利、データポータビリティの権利、データ消去の権利（忘れられる権利）等	個人の権利権益を侵害してはならないとされているが、明確な個人の権利については特に示されていない。
データ保護責任者（DPO）	言及されていない。	GDPR によって新たに定義された役職である。ただし、具体的な役割や資格要件等に関してまでは定義されていない。	言及されていない。
データ保護影響評価（DPIA）	言及されていない。 （個人情報保護法では規定されていないが、マイナンバー法においてプライバシー影響評価（PIA）についての規定がある）	特に新たな技術を用いるなどのある種の取扱いが、その性質、範囲、文脈及び取扱いの目的を考慮して、自然人の権利や自由に高リスクを生じさせる可能性がある場合、管理者は、取扱いの前に、予定された取扱い作業の個人データ保護への影響評価を実施しなければならない。独立した評価は同様の高リスクを示す同様の取扱い作業の集合で用いることができる。	言及されていない。
データの越境移転	個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者が可能であるとしている。	1 つの章を割いて規定している。 越境移転が許されるケースとして、十分性認定を受けた国に対する移転と、適切な保護措置に従った移転として、標準契約条項（SCC）に基づくものと拘束的企業準則（BCR）について規定されている。	越境移転のためのメカニズムとして、CBPR システムを規定し、その運用を推奨している。

1.3.4. ISO（国際標準化機構）におけるプライバシー関連の規格

EU や APEC が定める勧告や規則のほか、国際的に企業が注意を払うべき対象として、ISO 等の国際標準規格がある。標準規格は、規格への準拠はそれぞれの企業活動に基づく判断によるものであるが、日本国内では一般的に認知されている ISO9001 品質マネジメントシステムや ISO14001 環境マネジメントシステム等、企業活動を行うにあたり率先して規格への準拠を宣言するケースも少なくない。また、一部の政府調達等では、特定の規格への準拠を調達要件として定めることもあり、企業としてはその対応について検討が必要な場合も生じる。日本においては、個人情報保護のマネジメント規格として JIS Q 15001 が存在しているが、同様に ISO でも、様々なプライバシー関連の国際規格が発行されており、今後の動向が注目される。

個人情報保護やプライバシーに関する国際標準規格は、ISO/IEC JTC 1 SC27/WG5 Identity Management and Privacy Technologies（アイデンティティ管理とプライバシー技術）[8]において複数の規格が発行・検討されている。

[8] https://www.iso.org/committee/45306.html

図表 8　ISO/IEC JTC 1/SC27/WG5 が発行・検討中のプライバシー関連規格

規格番号	タイトル	概要
ISO/IEC 29100:2011	Privacy framework	国際規格として発行済（2011 年）。 JIS X 9250:2017 プライバシーフレームワーク（プライバシー保護の枠組み及び原則）として JIS 化済。
ISO/IEC 29191:2012	Requirements for partially anonymous, partially unlinkable authentication	国際規格として発行済（2012 年）。 部分的匿名化及びリンク不可能な認証のための要求事項
ISO/IEC 29101:2013	Privacy architecture framework	国際規格として発行済（2013 年）。 プライバシーアーキテクチャフレームワーク
ISO/IEC 29115:2013	Entity authentication assurance framework (ITU-T X.1254)	国際規格として発行済（2013 年）。 エンティティ認証保証フレームワーク
ISO/IEC 27018:2014	Code of practice for PII protection in public clouds acting as PII processors	国際規格として発行済（2014 年）。 PII プロセッサとして動作するパブリッククラウドにおける PII 保護の行動規範
ISO/IEC 29190:2015	Privacy capability assessment model	国際規格として発行済（2015 年）。 プライバシー能力評価モデル
ISO/IEC PDTS 19608	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408 (WG3 project:　formerly Privacy seal programs)	PDTS：技術仕様書原案段階 ISO/IEC 15408 に基づくセキュリティとプライバシーの機能要件の開発のためのガイダンス （WG3 のプロジェクト：所謂プライバシーシールプログラム）
ISO/IEC 29134:2017	Guidelines for privacy impact assessment	国際規格として発行済（2017 年）。 プライバシー影響評価のガイドライン
ISO/IEC 29151:2017	Code of practice for personally identifiable information protection	国際規格として発行済（2017 年）。 PII（Personally Identifiable Information）保護のための行動規範

規格番号	タイトル	概要
SD2	Privacy references list	プライバシー参照リスト
SD4	Standards privacy assessment(SPA)	プライバシー評価基準
SD5	Guidelines on the application of ISMS in the area of privacy	プライバシー分野における ISMS の応用のためのガイドライン
ISO/IEC TS 29003:2018	Identity proofing	国際規格（TS：技術仕様書）として発行済（2018 年)。 アイデンティティプルーフィング
ISO/IEC NP 29115	Entity authentication assurance framework	NP：新作業項目提案段階 ISO/IEC 29115:2013 に対する追補の内容を含めた改訂プロジェクトとして提案
ISO/IEC DIS 20889	Privacy enhancing data de-identification techniques	DIS：国際規格案段階 データの非識別化（匿名化）技術
ISO/IEC CD 29184	Guidelines for online privacy notice and consent	CD：委員会原案段階 オンラインサービスにおける通知と同意のガイドライン （日本提案のプロジェクト）
ISO/IEC AWI 20547-4	Big data reference architecture – Part 4: Security and privacy fabric (WG4 project)	AWI：プロジェクト活動が開始された段階 ビッグデータ参照アーキテクチャ Part4 セキュリティとプライバシーの構造 （WG4 のプロジェクト）
ISO/IEC CD 27550	Privacy engineering	CD：委員会原案段階 プライバシーエンジニアリング
ISO/IEC AWI 27551	Requirements for attribute-based unlinkable entity authentication	AWI：プロジェクト活動が開始された段階 属性ベースのリンク不可能なエンティティ認証の要求事項

規格番号	タイトル	概要
ISO/IEC CD 27552	Enhancement to ISO/IEC 27001 for privacy management – Requirements	CD：委員会原案段階 プライバシーマネジメントのための ISO/IEC27001 の拡張 – 要求事項

NP　：New Proposal（新規提案）
AWI　：Approved Work Item（承認済み作業項目）
WD　：Working Draft（作業原案）
CD　：Committee Draft（委員会原案）
DIS　：Draft International Standard（国際規格原案）
IS　：International Standard（国際規格）

PDTS　：Proposed Draft Technical Specification（技術仕様書提案）
TS　：Technical Specification（技術仕様書）

PDTR　：Proposed Draft Technical Report（技術報告書提案）
TR　：Technical Report（技術報告書）

1.4. 考察

1.4.1. 国際的な法制度への対応と越境移転

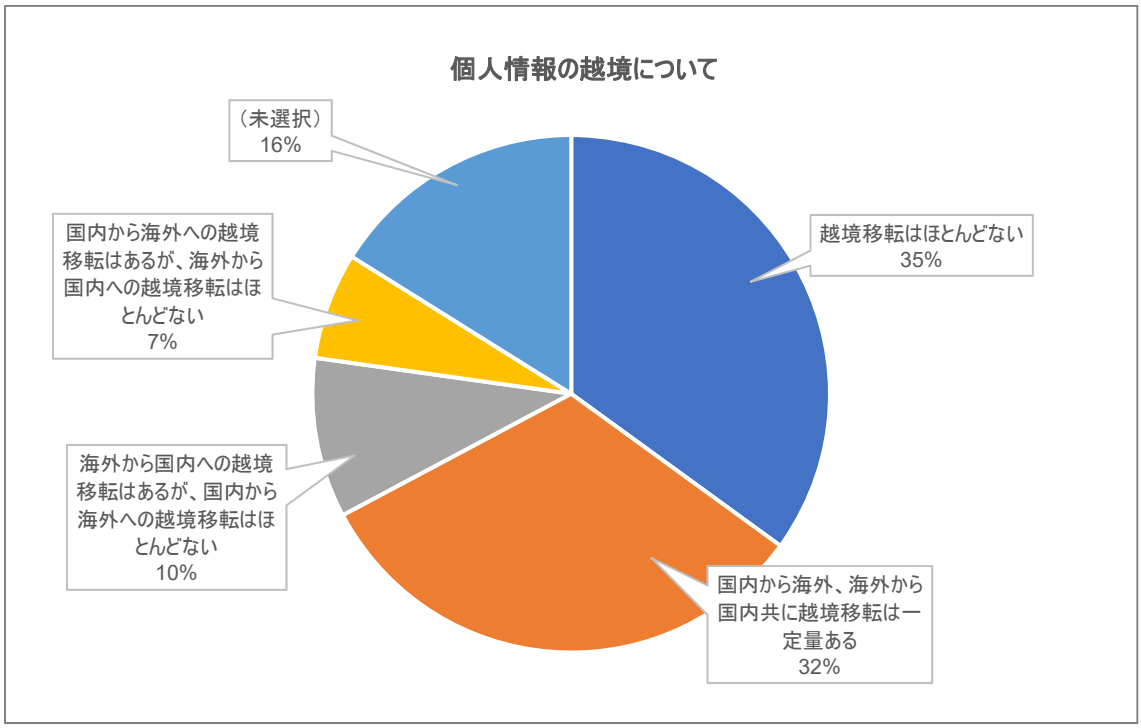
国内だけでなく海外展開も行うグローバル企業にとって、各国のデータ保護法制などの規制を理解し、対応していくということはコンプライアンス上避けて通れない道である。残念ながら、データ保護に関する万国共通の国際法は存在していないのが現状であるため、企業は都度各国・各地域の法制度に従わざるを得ない。しかしながら、EEA と APEC という世界の二大経済圏において、それぞれの経済圏内で各国共通のルール整備を進めているという事実から、将来的にデータ保護に関する万国共通のルールが策定されることへの期待は大きいのではないだろうか。

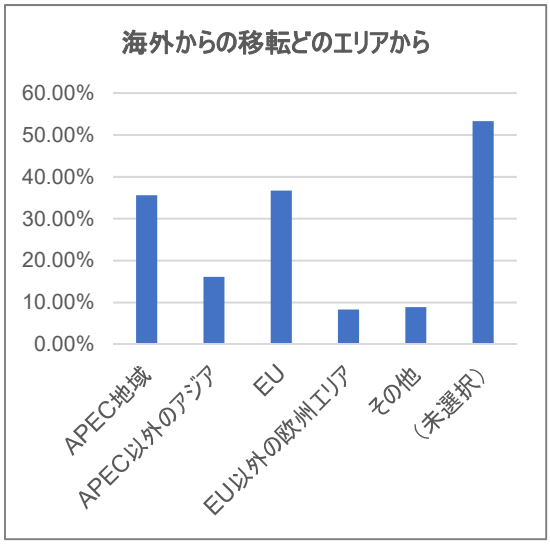
また、グローバルな企業活動を行う上で、個人データの越境移転における各国法制度への対応は特に留意すべき事項と考えられる。各国や地域における法制度では、データフリーフローの実現による経済発展に期待すると謳いつつも、企業に対して要求するデータ保護対策のレベルは高い。クラウド環境におけるデータ管理が一般的な昨今、データをどこに保管し、どのように管理し、どのように流通させるか、という組織内のデータマネジメントルールの策定や一般化が望まれるところである。マネジメントシステムの構築に関しては、ISO 規格や JIS 規格を活用することが一般的である。事実、ISMS（情報セキュリティマネジメントシステム）や品質マネジメントシステム、環境マネジメントシステム等の日本企業の採用率は世界的に見ても高いと言われている。このことは、組織内にマネジメントシステムを導入することでコンプライアンスの証明や担保を実現するという手法が、日本企業にとって一般的になりつつあるということを示唆しているのかもしれない。法制度へのコンプライアンスはいわば当然の義務であるが、義務を果たしていることの証明をマネジメントシステムの導入により担保するというモデルは、引き続き検討に値するアプローチなのではないだろうか。

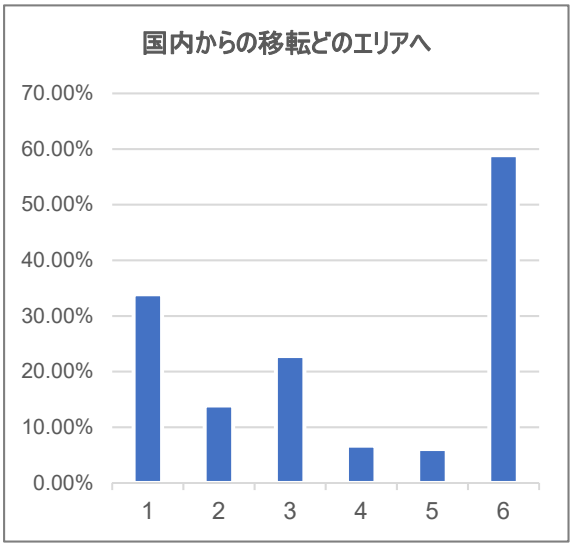
1.4.2. 越境移転に対する企業の関心

GDPR に関しては、2018 年 5 月の施行を目前に控え、平成 29 年度は国内でも数多くの関連セミナーや対策講座等が開催されていた。当協会でも、平成 30 年 3 月 13 日に「個人情報の域外移転セミナー〜グローバル・ビジネスにおける域外移転対策の具体的アプローチ〜」と題するセミナーを開催し、180 名の聴講者の来場があった。以下、来場者アンケートをもとに、国内企業における GDPR 対応や越境移転に関する状況をまとめる。

（1）　越境移転の状況





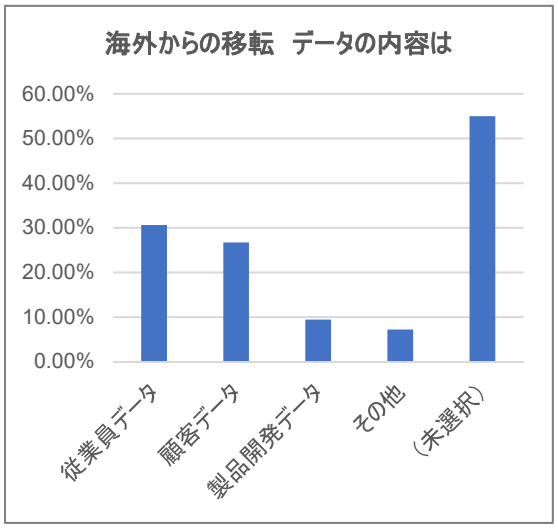


（有効回答数：151/180）

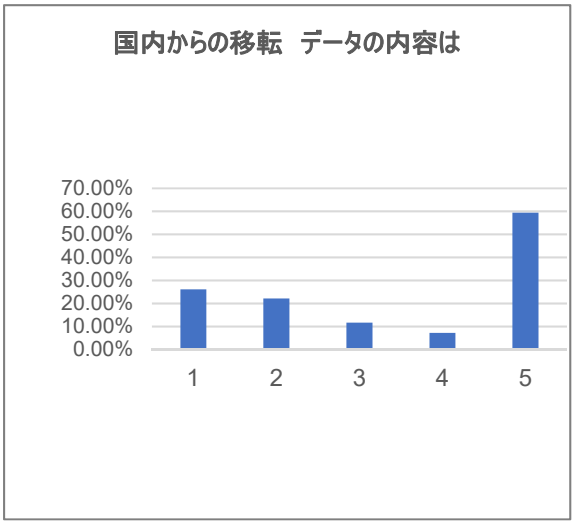
全体の約 3 割強については、越境移転はほとんどないという回答であったが、約半数が、何らかの形で越境移転がある、という回答であった。何らかの越境移転があると回答があった半数以上が、国内外双方向での越境移転があり、全体のうちそれぞれ 1 割前後が、国内から国外へ、もしくは国外から国内への一方向の移転があるという状況である。

また、越境移転の地域別にみると、やはり北米を含むアジア太平洋地域が最も多く、次いで EU 圏という結果であった。この結果は、グローバルに企業活動を行っている日本企業の活動地域と密接に関連があると思われる。

(2)　越境データの内容



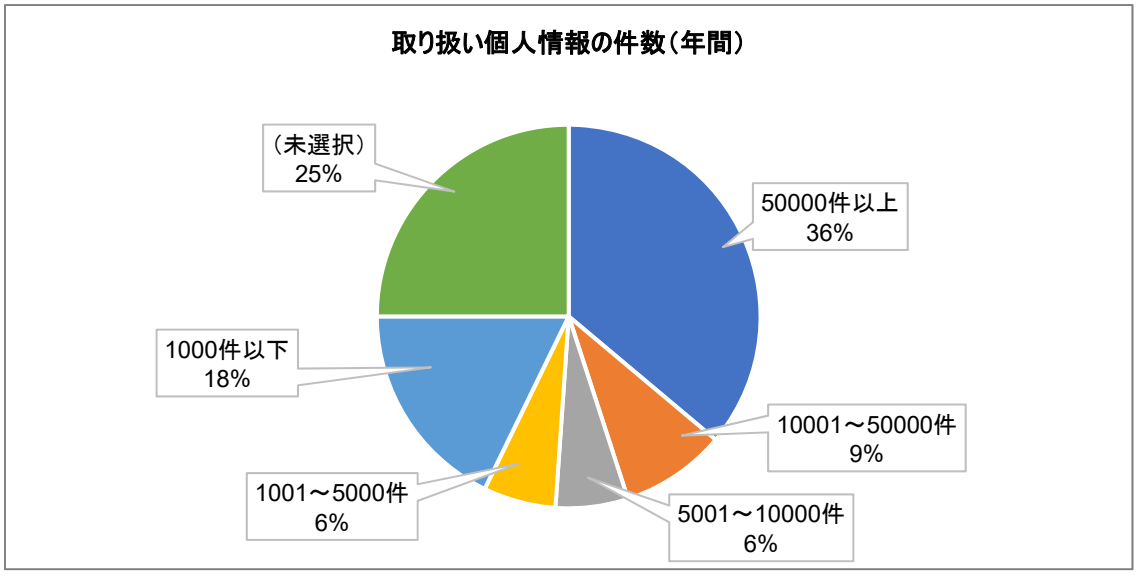
（有効回答数：81/180）



（有効回答数：74/180）

越境データの内容については、従業員データ、顧客データ、製品開発データの順であった。

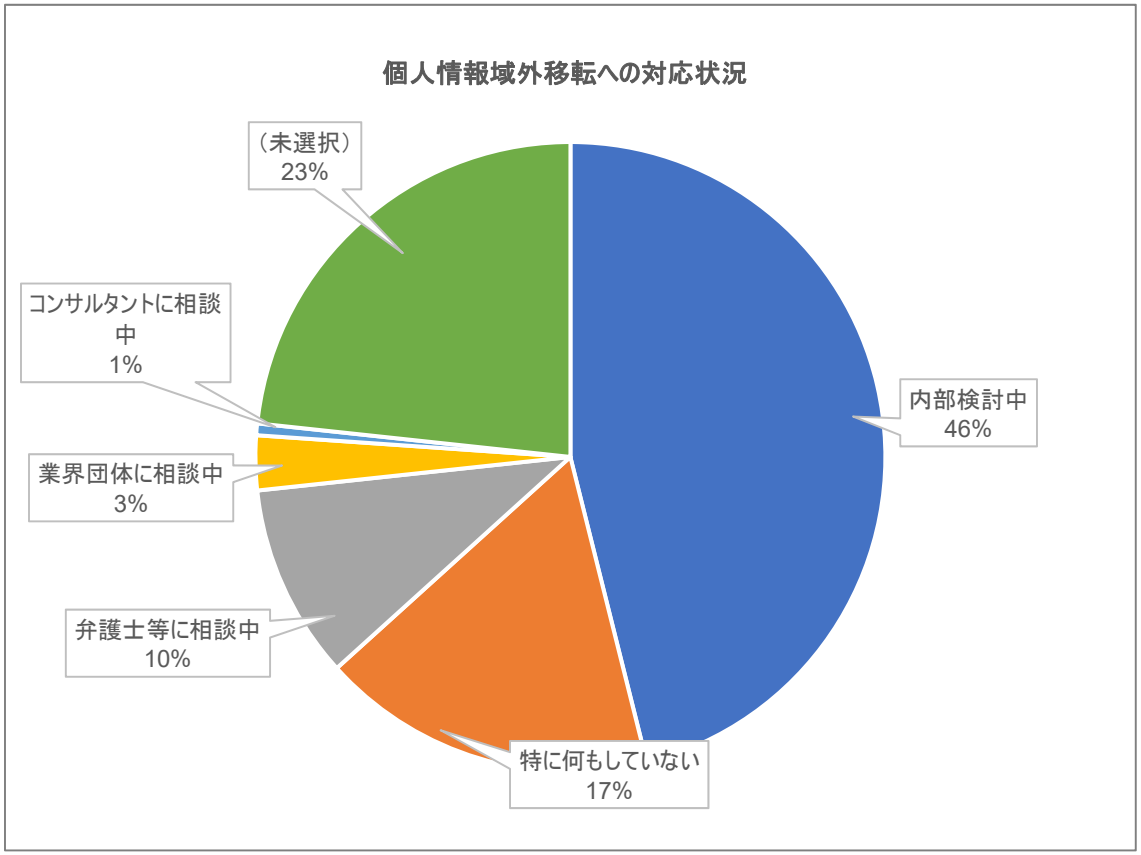
(3)　取り扱い個人情報の件数



（有効回答数：135/180）

取り扱い個人情報の件数に関しては、50,000 件以上という結果が 3 割強と最も多く、次いで 1,000 件以下、10,000～50,000 件、1,000～5,000 件、5,000～10,000 件と続く。上記「(2) 越境データの内容」の結果と合わせると、国内外で多数の従業員を抱える大手企業による越境が最も多いのではないかと分析できる。次いで多いのが逆に最も件数が少ない回答であることから、大企業と従業員規模の小さい企業の 2 極化が進んでいることが覗える。

（4）　越境移転の対応状況



（有効回答数：138/180）

越境移転の対応状況であるが、GDPR 施行直前であることもあり、何らかの対応を実施予定あるいは実施中の企業が全体の約 6 割を占める結果となった。内部検討中という回答が最も多く、半数近くにのぼるが、弁護士やコンサルタント等に具体的に相談中という企業も 1 割強存在している。今後、GDPR 施行が迫るにつれ、この割合は高まるのではないかと予想される。

1.4.3. 個人データ保護をめぐる今後の動向

平成 29 年度から 30 年度にかけて、国内外でデータ保護に関する法制度が相次いで施行されたことで、データ保護の重要性はより一層クローズアップされることとなった。特に、GDPR 施行に際しては、平成 29 年 10 月頃を境にして各種ガイドライン等の文書が順次公開されてきており（図表 9 参照)、各国もその動向を注視しているところである。

また、平成 29 年から我が国の個人情報保護委員会が正式なメンバーとなった、国際プライバシーコミッショナー会議などでは、各国からデータ保護法制に関する報告があるなど、データ保護に関して国際的に様々な議論が行われている。

当協会では、引き続き国際的なデータ保護についての動向を調査し、Web サイト等を通じて紹介していく予定である。

図表 9　WP29 が発行している GDPR 関連のガイドライン

発行日	タイトル	概要
2017/10/13	Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)	データ保護影響評価（DPIA）のガイドライン
2017/10/27	Guidelines on the right to "data portability" (wp242rev.01)	データポータビリティのためのガイドライン
2017/10/30	Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)	データ保護管理者（DPO）のガイドライン
2017/10/31	Guidelines on the Lead Supervisory Authority (wp244rev.01)	監督を行う当局に関するガイドライン
2018/01/24	[adopted, but still to be finalized] Guidelines on Consent under Regulation 2016/679 (wp259)	（作業中）GDPR に基づく同意に関するガイドライン
2018/02/13	Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)	GDPR における自動化された個人意思決定とプロファイリングに関するガイドライン
2018/02/13	Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)	GDPR に基づくデータ漏洩時の通知に関するガイドライン
2018/02/13	Guidelines on the application and setting of administrative fines (wp253). Now including available language versions.	制裁金の適用と設定に関するガイドライン
2018/04/13	Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)	GDPR に基づく透明性に関するガイドライン
2018/04/16	Guidelines on Consent under Regulation 2016/679 (wp259rev.01)	GDPR に基づく同意に関するガイドライン

1.5. 参考文献

- 個人情報の保護に関する法律（平成 15 年 5 月 30 日　法律第 57 号）
  平成 28 年 5 月 27 日公布（平成 28 年法律第 51 号）改正　平成 29 年 5 月 30 日施行
  https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf
- REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
  個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則（一般データ保護規則）
  （原文）http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC
  （当協会仮訳）http://www.jipdec.or.jp/archives/publications/J0005075
- APEC Privacy Framework
  （原文）https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)
- Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)
  プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告（OECD プライバシーガイドライン）
  （原文）http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
  （当協会仮訳）https://www.jipdec.or.jp/library/archives/u71kba0000002fym-att/01.pdf

2. 調査研究２：IoT セキュリティについて

2.1. 調査研究の視点

高度な情報活用による世界に先駆けた「超スマート社会（Society5.0）」の実現に向けて、IoT などの技術革新によって、データの到達コストが圧縮され、業界横断した活用が進むと、モノづくり、交通、医療、農業など、様々な分野でイノベーションが生まれ、ビジネスや社会全般に大きな革新をもたらすと期待されている。他方、これを具体的に進めるためには、機器・サービスの信頼性確保等から、IoT のサイバーセキュリティ対策[9]は最も重要な観点の一つである。例えば、2016 年以降、重大な攻撃がいくつも発生しているが、その一つにボットネットの「Mirai」がある。このボットネットは多くの IoT デバイス（主に古いルータと IP カメラ等）に感染し、それらを使って Dyn[10]に大規模な DDoS（分散型サービス拒否）攻撃を仕掛けた。この攻撃では、古いバージョンの Linux カーネルを使用しているデバイスで、ユーザーID とパスワードがデフォルトのまま利用されているものが標的とされた。このように、攻撃対象が PC のみならず、ネットワークにつながる全ての機器に拡大しているとともに、攻撃手法も多様化しており、その影響度も深刻になりつつある。

このような状況を踏まえ、我が国では、サイバーセキュリティ戦略（平成 27 年 9 月 4 日閣議決定）において、IoT システムのセキュリティが確保された形での新規事業の進行やガイドラインの策定などの制度整備、技術開発等を進めることとしている。

本調査研究では、IoT 機器が用いられるシステムに対するサイバーセキュリティ対策について検討する。IoT のセキュリティについては、我が国をはじめとして、米国（NIST[11]等）、EU（ENISA[12]等）、ドイツ（PI4[13]等）など、様々な国と地域で検討がなされているところである。

他方で、企業の情報セキュリティ対策については、様々な標準規格が策定されてきており、その適用事例も増えてきている。例えば、主に企業や組織内の情報を扱う情報システム分野（IT）の管理・運用に関する一つの例として、ISO/IEC27001[14]において国際標準化されており、我が国においても、同規格に対応した JIS Q 27001 を活用した情報セキュリティマネ

---

[9] 「CSMS 認証基準（IEC62443-1）」によると、サイバーセキュリティ対策とは、「重要なシステム又は情報資産に対する無許可での使用、サービス不能攻撃、改変、開示、収益の逸失、又は破壊を防止するために要求されるアクション」である。

[10] DNS サービスを提供する米国企業

[11] アメリカ国立標準技術研究所：https://www.nist.gov/

[12] 欧州ネットワーク・情報セキュリティ機関：https://www.enisa.europa.eu/

[13] Platform Industrie4.0：http://www.plattform-i40.de/I40/Navigation/DE/Home/home.html

[14] https://www.iso.org/isoiec-27001-information-security.html　参照。

ジメントシステム（ISMS）適合性評価制度があり、2002 年 4 月より本格運用を開始している。また、主に企業や組織内の物理的なデバイス、プロセス、イベントの直接監視及び/または制御を行う産業システム分野（OT）では、サイバーセキュリティ対策の一つの例として、ISMS をベースにしたセキュリティマネジメントシステムが IEC62443-2-1 として規格化されており、この IEC62443-2-1 に基づき、産業システム分野のセキュリティマネジメントシステム認証基準として「CSMS 認証基準（IEC62443-2-1）(JIP-CSCC100 2.0)」が策定されている。

IEC62443-2-1（CSMS）は、ISO/IEC27001（ISMS）を加味して策定されたことから、両者には数多くの共通点がある。具体的には、両規格とも継続的改善（PDCA）を念頭においた仕組みであること、守りたい情報資産を基にリスクアセスメントを実施すること、そこに機密性・可用性・完全性という観点を持つこと、リスクに対する管理策を規格に列挙された詳細管理策から選択すること等である。

IoT 機器が用いられるシステムに対するサイバーセキュリティ対策についても、前述のような既存規格をベースとした標準規格が今後設定されてくると思われる。IoT システムの定義・範囲は、本来は複雑に絡み合う要素を一つ一つ丁寧に整理する必要があるが、ここでは「センサーが取り扱う情報のみ」に着目し、以下のように整理した。

① 取得時・利用時共に機密情報が含まれるセンサー（ウェアラブルセンサー等）を利用するケース
② 取得時は機密情報が含まれるが利用時には機密情報が含まれないセンサー（画像センサー等）を、利用するケース
③ 取得時・利用時共に、機密情報が含まれないセンサー（環境センサー等）を利用するケース

上記①のケースについては、セキュリティの優先順位に着目すると、「継続的な安定稼働」よりも「機密情報の漏洩防止」のほうが、優先順位が高くなる場合も少なくなく、その場合には、情報システム分野（IT）のセキュリティマネジメントで用いられる ISMS が適用しやすいケースもあると想定される（但し、事例毎に検証する必要があるため、必ずしもこの限りではない）。

また、上記②や③のケースにおいても、工場生産ラインのように「継続的な安定稼働が求められるもの」でない場合では、産業システム分野（OT）と同様のマネジメントを適用すると、要求事項が異なる（もしくは適さない）場合もあり、むしろ、ISMS のほうが適用しやすい場合もあるのではないかと考えられる。

そこで、上記②と③のケースにおいて、企業が保護すべき資産として、物理的資産（IoT 機器）に着目し、具体的な事例をベースとして、ISMS を構築し、現状の情報セキュリティマネジメントの範囲において、リスク分析できること/できないことなどを明らかにする。

2.2. 調査研究の対象

利用時に機密情報が含まれない IoT システムの具体的な事例をベースにするにあたり、当協会が事務局を運営している「データ流通促進 WG[15]」では、「新たなデータ流通取引に関する検討事例集[16]」を作成・公表しているが、その中で取り扱った事例から、「気象データ等の活用」を対象とする。

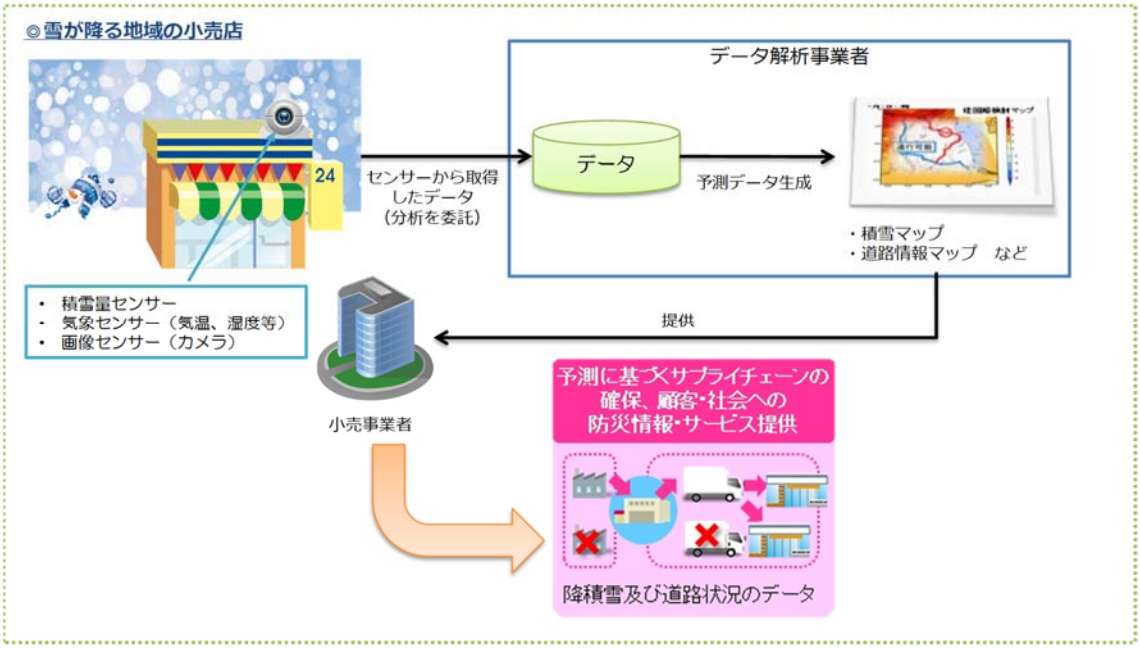
【気象データ等の活用モデルの概要】

- 降雪地域に展開する日常品、食料品等を扱う小売店舗に環境センサー（積雪量センサー、気象センサー、画像センサー）を設置し、得られた情報から降雪量や通行可能な道路などの予測データを生成する
- 小売事業者が生成された予測データを基に、自社の最適なサプライチェーンの確保（通行可能な配送ルートなど）を行う
- 本事例は委託モデルである（小売事業者からデータ解析事業者に対して、センサーの設置及び予測データ生成について委託する）
- 生成された予測データは、小売事業者の自社内のみで活用する（第三者提供等は行わない）

[15] http://www.iotac.jp/wg/data/　参照。

[16] http://www.meti.go.jp/press/2016/03/20170310002/20170310002-1.pdf　参照。

図表 10　本調査研究で扱う事例



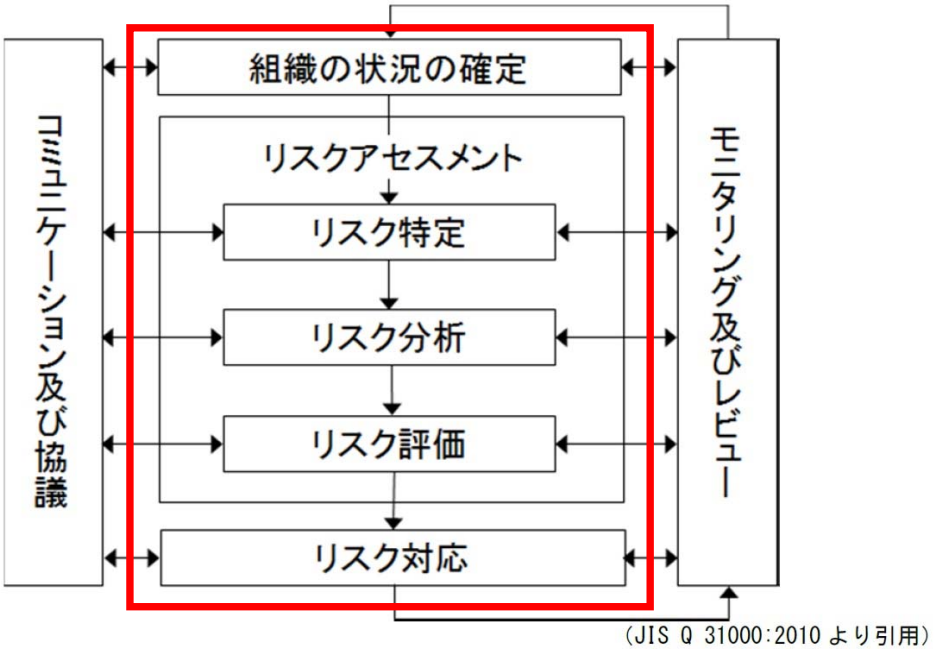
2.3.　IoT システムにおける ISMS 適用可能性の調査結果

「2.2 調査研究の対象」で示した事例について、JIS Q 27001:2014（ISO/IEC 27001:2013）に対応した「ISMS ユーザーズガイド」、及び「ISMS ユーザーズガイド（リスクマネジメント編）」（以降、まとめて ISMS ユーザーズガイドという）に基づいて構築する。ISMS ユーザーズガイドでは、情報セキュリティに関わるリスクを明確にするために、情報セキュリティの主たる 3 要素（機密性、完全性、可用性）のそれぞれの観点から分析を行った。

ISMS の目的は、リスクマネジメントプロセスを適用することによって、情報の機密性、完全性、可用性を保護し、かつ、リスクを適切に管理しているという信頼を利害関係者に与えることにある。

リスクマネジメントのプロセス間の情報の流れを図表 11 に示す。

図表 11　リスクマネジメントのプロセス間の情報の流れ



今回は、上図表の実施作業のうち、赤枠で示した「組織の状況の確定」、「リスク特定」、「リスク分析」、「リスク評価」、「リスク対応」を対象とする。

また、上記のリスクアセスメントを実施するにあたっての基準[17]として、「詳細リスクアセスメント[18]」に沿って評価を行った。

なお、今回はあくまでも ISMS をベースにした簡易的な分析を通じて、利用時に機密情報が含まれない IoT システムでは、ISMS の範囲でどこまでセキュリティマネジメントを実施できるか、また、情報システム分野（IT）と比較して、守るべき資産などの違いは何かを明らかにすることが目的であり、本書で示した内容を実施すれば、実際に ISMS を構築できるというものではなく、ISMS を取得するためには、ユーザーズガイドに基づいたきめ細やかな対応が必須となる。

◎組織の状況を確定する

ISMS ユーザーズガイドでは、組織をとりまく内外の状況や利害関係者のニーズ及び期待を理解、決定し、それらを考慮に入れたうえで ISMS の適用範囲を定めることとしている[19]。

本事例の日常品や食料品を扱う小売業は、生活者の日々の暮らしに密着しており、言わば

[17] ISMS ユーザーズガイドでは他に「ベースラインアプローチ」、「非形式アプローチ」、「組合せアプローチ」が紹介されている。

[18] システムについて詳細なリスクアセスメントを行うアプローチで、資産に対し「資産価値」、「脅威」、「ぜい弱性」や「セキュリティ要件」を識別し、リスク評価する方法。

[19] 分析手法の一つに SWOT 分析等がある。

生活インフラの位置づけであることから、降雪等により仕入れがストップしてしまうことは、安定的な経営の観点からも、最優先して対応すべきインシデントである。このような組織状況を加味し、リスク分析を行った。

◎リスクを特定する

（1）資産の特定（リスト化）

ここでは、組織の ISMS 適用範囲における資産の保有状況を確認する。資産の対象は、主要資産（事業プロセス及び事業活動、情報）、及び支援資産（ハードウェア、ソフトウェア、ネットワーク、要員、サイト、組織の構成）であるが、ここでは、「4.2.調査研究の視点」で述べた通り、ハードウェアのみを対象として下図表の通りリスト化した。

図表 12　資産の洗い出し

IoT 機器	概要
積雪センサー（深さ・重さ）	ポール上に設けた測定部と雪面との間の距離及び積もった雪の重さを測る装置
気象センサー（気温・湿度）	外気温と湿度を測る装置
画像センサー	気象状況及び路面状況を映像で把握する（リアルタイム、録画）ための屋外設置型カメラ

（2）脅威・脆弱性の明確化

リスクの発生のしやすさは、個別の資産がさらされるであろう脅威と管理上の問題などによる脆弱性の組み合わせで表現される。

①脅威の識別

「脅威」とは、情報システムや組織に損失や損害をもたらすセキュリティ事故の潜在的な原因である。脅威は後述する「脆弱性」によって誘引され、顕在化することにより組織及び業務に影響を与える。脅威の大きさは、その要因や対象となる資産ごとに、その発生の可能性を評価して決定する[20]。

ISO/IEC27005:2011 では、図表 13 の通りに大別している。

図表 13　脅威の分類

故意によるもの	偶発的なもの	環境的なもの
deliberate⇒D	accidental⇒A	environmental⇒E

[20] ISMS ユーザーズガイドでは、自身の業務と関連する他部門と協力して整理することとしている。

図表 13 をもとに、自らが管理する資産がさらされる脅威を識別し、分類した（図表 14）[21]。故意によるものは、攻撃者の動機、攻撃に必要とされるスキル、利用できるリソースを考慮に入れ、資産の特性、魅力、脆弱性からどのような要因が脅威であるかを識別した。偶発的なものは、立地条件、極端な気候条件の可能性及び要員によるミスや誤作動などから影響を及ぼす可能性を識別した。

図表 14　脅威の認識とその分類

類型	脅威	原因
環境的（自然現象）	地震、火災	A,D,E
	異常気象（大雨・暴風・豪雪など）	E
	気候（高温による熱暴走、低温による凍結など）	E
	粉塵（ダスト）、腐食	E
技術的	電力供給の停止（停電など）	A,D,E
	機器の故障	A
	機器の誤動作	A
意図的（故意）	機器の盗難・破壊	A,D,E
	盗聴・漏洩	D
	遠隔攻撃（DDoS 攻撃など）	D
	侵入/乗っ取り（データ改竄・破壊）	D
過失	使用時のミス	A
	権限の詐称・乱用	A,D
	権限の詐称	D

本事例で用いられる環境センサーは、屋内のみならず、屋外にも設置されることから、図表 14 の通り、ISMS のメインターゲットである情報システム分野と比較した際の特徴として、自然現象や人間や動物等による機器や媒体の破壊などの脅威をより注意深く見る必要がある。また、遠隔攻撃（DDoS 攻撃など）への対策については情報システム分野でも指摘されているが、IoT 機器が乗っ取られた場合、その種類が多様であるため、DDoS 攻撃側に加担してしまう機器が格段に増え、結果、甚大な被害をもたらす可能性がある。

②脆弱性の識別

脆弱性とは、脅威の発生を誘引する資産固有の弱点やセキュリティホールのことである。

[21] 本来は洗い出した資産ごとに作成するものであるが、ここでは積雪センサー、気象センサー、画像センサーに共通化したものを作成した。

脆弱性はそれだけでは障害とはならないが、脅威を顕在化させ、損害や損傷を導く可能性がある[22]。

脆弱性の分類について、脅威と関連付けて整理したものを下図表に示す。

図表 15　脆弱性の識別

類型	脅威	脆弱性
環境的（自然現象）	地震、火災	機器を設置した建物の耐震･耐火工事の未実施 耐火設計されてない機器の利用
	異常気象（大雨・暴風・豪雪など）	過酷な気象状況では動作できない機器の利用
	気候（高温による熱暴走、低温による凍結など）	温度変化に対する影響の受けやすさ
	粉塵（ダスト）、腐食	湿気、埃、汚れに対する影響の受けやすさ
技術的	電力供給の停止	予備電源、UPS 等の未確保 現地での対応が必要になった時に、遠方にある場合はすぐに駆け付けられない
	機器の故障	初期不良 定期的な交換計画の欠如
	機器の誤動作	初期不良 不適切な設定
意図的（故意）	機器の盗難・破壊	悪意あるユーザーによる実行 設置時、廃棄時の注意の欠如
	盗聴・漏洩	悪意あるユーザーによる実行 適切な ID/PW の未設定 最新の機器への交換やセキュリティパッチの未適用
	遠隔攻撃（DDoS 攻撃など）	悪意あるユーザーによる実行 最新の機器への交換やセキュリティパッチの未適用
	侵入/乗っ取り（データ改竄・破壊）	悪意あるユーザーによる実行 適切な ID/PW の未設定 最新の機器への交換やセキュリティパッチの未適用

[22] 換言すると、脅威が存在しない脆弱性は対応の優先度が低くなる。

類型	脅威	脆弱性
過失	使用時のミス	複雑なユーザーI/F 不正確なパラメータ設定
	権限の詐称・乱用	ユーザーの識別及び認証メカニズムの欠如 誤ったアクセス権の割当て 不十分なパスワード管理

上図表の通り、脅威に対する脆弱性については、機器の不適切な設定（類推が容易なパスワードの設定、誤ったパラメータの設定など)、セキュリティパッチの未適用など、項目としては情報システム分野と大差ないが、IoT 機器は PC 等と比較してライフサイクルが長いので、可用性の確保等の観点から、これらの管理をより難しくさせることが予想される。

◎リスクを分析する

（1）起こり得る結果のアセスメント

前記で特定した資産及びリスクに基づき、資産ごとに機密性、完全性、可用性が損なわれた時の事実上の影響（損害）を評価した。

図表 16　影響度の評価

#	機密性	完全性	可用性
積雪センサー	中長期的な経営には影響が少ない（限定された人に対して悪い風評が及ぶ可能性はある）	当期経営に多少の影響を及ぼす	当期経営に多少の影響を及ぼす
気象センサー			
画像センサー	中長期的な経営に重大な影響を及ぼす（多くの人に対し悪いイメージが残る）	当期経営に多少の影響を及ぼす	当期経営に多少の影響を及ぼす

上図表の通り、機密性の観点においては、積雪センサー、気象センサーは自然現象の様子を可視化するものであり、かつ機密情報等は含まれないので、漏洩した場合でも中長期的な経営には影響が少ないと評価したが、画像センサーについては、不特定多数の往来者が映り込む可能性が高く、撮影条件（カメラの性能、設置角度など）によっては、個人を特定できる場合もあるため、漏洩した場合は、個人情報取扱事業者に求められる安全管理措置義務の違反にあたるとともに、多くの人に対して悪いイメージが残る（信用・ブランドの損失）ものであることから、中長期的な経営に重大な影響を及ぼすと評価した。

他方、完全性、可用性の観点からは、全ての環境センサーにおいて、当期経営がストップ

してしまうほどではないが、当期経営に多少の影響を及ぼすものと評価した。理由は、通行可能な配送ルートを予測・確保するにあたっては、各種センサーから取得したデータを解析するだけでなく、他の情報（天気予報、実際の天候状況の目視、ドライバーが持っている過去の経験など）を組み合わせて、総合的に判断するものであり、センサーから取得したデータが改竄されたり、センサー自身がダウンしてデータを取得・利用できなくなった場合、予測精度が下がることはあっても、経営自体がストップしてしまうような重大な影響を及ぼすものではないと判断した[23]。また、センサー固有の影響度にも違いは見られなかった[24]。

（２）起こりやすさのアセスメント

ここでは、起こり得るセキュリティ障害などの現実的な発生可能性を評価するために、認識されている脅威及び脆弱性を評価する。その際、資産に影響を及ぼす脅威や連動して起こり得る脅威などを洗い出し、現在実施されている管理策から脆弱性を考慮する。

①脅威の評価

脅威の評価は、対象とする資産の影響度の評価に基づき、意図的（故意によるもの）、偶発的（不注意によるもの）、環境的（自然現象など）な側面から評価することとした[25]。

②脆弱性の評価

脆弱性の評価は、その資産が持つ弱点がどの程度であるかを評価する。十分な管理策が実施されている場合は、脆弱性は少なくなり、管理策を実施しておらず、その弱点が剥き出しであるような場合は、脆弱性が高いと判断することとした。

以上を基にして、資産（積雪センサー、気象センサー、画像センサー）に対して実施している管理策を、機密性、完全性、可用性の観点から脆弱性を分析した[26]。また、評価基準として、現在実施している対策を基にした５段階の基準を用いた。（図表１７）

---

[23] 予測データを、自社内での活用のみならず他者に販売（第三者提供など）する場合は、この限りではない。

[24] 各センサーの特性等を詳細に分析し、影響度のランクが付けられる場合はこの限りではない。

[25] ISMS ユーザーズガイドでは、脅威の評価は脅威の識別と同様に自身の業務と関連する他部門と協力して整理するとともに、作成した脅威一覧に基づき、業務上の経験や過去に収集した統計的なデータに基づいて検討し、自らのマネジメントシステムにおいて、最も適切な評価方法を確立することが重要としている。

[26] ISMS ユーザーズガイドでは、脅威や脆弱性の評価は、作業を専門家に依頼して実施した方が客観性や効率性の確保の面から良い場合があるとともに、情報セキュリティ監査制度を利用し、外部の専門家が脆弱性評価の支援をすることも考えられるとしている。

図表 17　リスク判定基準

リスクレベル	リスク判定基準
1	最高程度の対策を実施している状況
2	一般的な対策＋αを実施しており、通常の利用状況では殆どリスクが顕在化する恐れがない状況
3	一般的な対策を実施している状況
4	対策が不十分であり、リスクが顕在化する恐れがある状況
5	特段の対策を実施しておらず、リスクが顕在化している状況

図表 18　リスク分析結果（積雪センサー、気象センサー、画像センサー共通）

類型	脅威	脆弱性	実施している対策	リスク値		
				機密性	完全性	可用性
環境的（自然現象）	地震、火災	・機器を設置した建物の耐震・耐火工事の未実施 ・耐火設計されてない機器の利用	・機器を設置した建物の耐震・耐火工事を実施している ・機器が故障した際の対応マニュアルを作成している	1	2	4
	異常気象（大雨・暴風・豪雪など）	・過酷な気象状況では動作できない機器の利用	・機器が故障した際の対応マニュアルを作成している	1	2	4
	気候（高温による熱暴走、低温による凍結など）	・温度変化に対する影響の受けやすさ	・機器が故障した際の対応マニュアルを作成している	1	2	4
	粉塵（ダスト）、浸食	・湿気、埃、汚れに対する影響の受けやすさ	・機器が故障した際の対応マニュアルを作成している	1	2	4
技術的	電力供給の停止（停電など）	・予備電源、UPS等の未確保 ・現地での対応が必要になった時に、遠方にある場合はすぐに駆け付けられない	–	1	2	4
	機器の故障	・初期不良 ・定期的な交換計画の欠如	・保守サービスに加入している	1	3	4
	機器の誤動作	・初期不良 ・不適切な設定	–	1	3	4
意図的（故意）	機器の盗難・破壊	・悪意あるユーザーによる実行 ・設置時、廃棄時の注意の欠如	・人間や動物等が近寄れない場所に設置する	2	2	3
	盗聴・漏洩	・悪意あるユーザーによる実行 ・適切なID/PWの未設定 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	2	2	4
	遠隔攻撃（DDos攻撃など）	・悪意あるユーザーによる実行 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	1	2	4
	侵入/乗っ取り（データ改竄・破壊）	・悪意あるユーザーによる実行 ・適切なID/PWの未設定 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	2	3	4
過失	使用時のミス	・複雑なI/F ・不正確なパラメータ設定	・運用マニュアルを作成している	2	2	4
	権限の詐称・乱用	・ユーザーの識別及び認証メカニズムの欠如 ・誤ったアクセス権の割り当て ・不十分なパスワード管理	・ID/PWを適切に管理している	2	2	3

（3）リスクレベルの決定

リスクレベルは、その資産の重要度を検証するため、ISMS ユーザーズガイドでは、例として、「リスクレベル＝『資産の価値』×『脅威』×『脆弱性』」が挙げられているが、ここでは、資産（積雪センサー、気象センサー、画像センサー）毎に、機密性、完全性、可用性それぞれの観点から、図表 17 に示したリスクレベルのどこまでを担保する必要があるかについて、図表 16 で示した影響度の評価を基にして、図表 19 の通り算出した。

図表 19　資産ごとに担保すべきリスクレベルの決定

#	機密性	完全性	可用性
積雪センサー	2	2	3
気象センサー			
画像センサー	1	2	3

◎リスクを評価する

図表 18 で示したリスク分析結果に対して、図表 19 に示した資産毎に担保すべきリスクレベルを比較した。具体的には、「積雪センサーと気象センサー」及び「画像センサー」に対し、『担保すべきリスクレベル』－『リスク値』を算出した。結果が 0 以上になっている部分は、担保すべきリスクレベルを満たしていると評価し、マイナス数値になっている部分は、担保すべきリスクレベルを満たしていないと評価した。

図表 20　リスク評価結果（積雪センサーと気象センサー）

類型	脅威	脆弱性	実施している対策	リスク値			リスク評価		
				機密性	完全性	可用性	機密性	完全性	可用性
環境的（自然現象）	地震、火災	・機器を設置した建物の耐震・耐火工事の未実施 ・耐火設計されてない機器の利用	・機器を設置した建物の耐震・耐火工事を実施している ・機器が故障した際の対応マニュアルを作成している	1	2	4	1	0	-1
	異常気象（大雨・暴風・豪雪など）	・過酷な気象状況では動作できない機器の利用	・機器が故障した際の対応マニュアルを作成している	1	2	4	1	0	-1
	気候（高温による熱暴走、低温による凍結など）	・温度変化に対する影響の受けやすさ	・機器が故障した際の対応マニュアルを作成している	1	2	4	1	0	-1
	粉塵（ダスト）、浸食	・湿気、埃、汚れに対する影響の受けやすさ	・機器が故障した際の対応マニュアルを作成している	1	2	4	1	0	-1
技術的	電力供給の停止（停電など）	・予備電源、UPS等の未確保 ・現地での対応が必要になった時に、遠方にある場合はすぐに駆け付けられない	−	1	2	4	1	0	-1
	機器の故障	・初期不良 ・定期的な交換計画の欠如	・保守サービスに加入している	1	3	4	1	-1	-1
	機器の誤動作	・初期不良 ・不適切な設定	−	1	3	4	1	-1	-1
意図的（故意）	機器の盗難・破壊	・悪意あるユーザーによる実行 ・設置時、廃棄時の注意の欠如	・人間や動物等が近寄れない場所に設置する	2	2	3	0	0	0
	盗聴・漏洩	・悪意あるユーザーによる実行 ・適切なID/PWの未設定 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	2	2	4	0	0	-1
	遠隔攻撃（DDos攻撃など）	・悪意あるユーザーによる実行 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	1	2	4	1	0	-1
	侵入/乗っ取り（データ改竄・破壊）	・悪意あるユーザーによる実行 ・適切なID/PWの未設定 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	2	3	4	0	-1	-1
過失	使用時のミス	・複雑なI/F ・不正確なパラメータ設定	・運用マニュアルを作成している	2	2	4	0	0	-1
	権限の詐称・乱用	・ユーザーの識別及び認証メカニズムの欠如 ・誤ったアクセス権の割り当て ・不十分なパスワード管理	・ID/PWを適切に管理している	2	2	3	0	0	0

図表 21　リスク評価結果（画像センサー）

類型	脅威	脆弱性	実施している対策	リスク値			リスク評価		
				機密性	完全性	可用性	機密性	完全性	可用性
環境的（自然現象）	地震、火災	・機器を設置した建物の耐震・耐火工事の未実施 ・耐火設計されてない機器の利用	・機器を設置した建物の耐震・耐火工事を実施している ・機器が故障した際の対応マニュアルを作成している	1	2	4	0	0	-1
	異常気象（大雨・暴風・豪雪など）	・過酷な気象状況では動作できない機器の利用	・機器が故障した際の対応マニュアルを作成している	1	2	4	0	0	-1
	気候（高温による熱暴走、低温による凍結など）	・温度変化に対する影響の受けやすさ	・機器が故障した際の対応マニュアルを作成している	1	2	4	0	0	-1
	粉塵（ダスト）、浸食	・湿気、埃、汚れに対する影響の受けやすさ	・機器が故障した際の対応マニュアルを作成している	1	2	4	0	0	-1
技術的	電力供給の停止（停電など）	・予備電源、UPS等の未確保 ・現地での対応が必要になった時に、遠方にある場合はすぐに駆け付けられない	−	1	2	4	0	0	-1
	機器の故障	・初期不良 ・定期的な交換計画の欠如	・保守サービスに加入している	1	3	4	0	-1	-1
	機器の誤動作	・初期不良 ・不適切な設定	−	1	3	4	0	-1	-1
意図的（故意）	機器の盗難・破壊	・悪意あるユーザーによる実行 ・設置時、廃棄時の注意の欠如	・人間や動物等が近寄れない場所に設置する	2	2	3	-1	0	0
	盗聴・漏洩	・悪意あるユーザーによる実行 ・適切なID/PWの未設定 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	2	2	4	-1	0	-1
	遠隔攻撃（DDos攻撃など）	・悪意あるユーザーによる実行 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	1	2	4	0	0	-1
	侵入/乗っ取り（データ改竄・破壊）	・悪意あるユーザーによる実行 ・適切なID/PWの未設定 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	2	3	4	-1	-1	-1
過失	使用時のミス	・複雑なI/F ・不正確なパラメータ設定	・運用マニュアルを作成している	2	2	4	-1	0	-1
	権限の詐称・乱用	・ユーザーの識別及び認証メカニズムの欠如 ・誤ったアクセス権の割り当て ・不十分なパスワード管理	・ID/PWを適切に管理している	2	2	3	-1	0	0

◎リスク対応を行う

リスクアセスメントで明確になった管理対象となるリスクに対して、リスクマネジメントの枠組みの中でどのような対応を実施するかを決定し、リスクを組織が受容できる水準に修正するプロセスである。

本来であれば、分析したリスクの優先順位を決定する必要があるが、ここでは、前述のリスク評価結果（図表 20 及び図表 21）で、リスク評価がマイナス数値になっている部分（赤枠セル部分）について、担保すべきリスクレベルを達成するようなリスク対応策を検討した。

図表 22　リスク基準を満たすために実施すべき対応策（積雪センサーと気象センサー）

類型	脅威	脆弱性	実施している対策	リスク値			リスク評価			リスク対応策
				機密性	完全性	可用性	機密性	完全性	可用性	
環境的（自然現象）	地震、火災	・機器を設置した建物の耐震・耐火工事の未実施 ・耐火設計されてない機器の利用	・機器を設置した建物の耐震・耐火工事を実施している ・機器が故障した際の対応マニュアルを作成している	1	2	4	1	0	-1	・複数名の責任者を配置し、そのうち1名を現地スタッフとして常駐する ・保険に加入する
	異常気象（大雨・暴風・豪雪など）	・過酷な気象状況では動作できない機器の利用	・機器が故障した際の対応マニュアルを作成している	1	2	4	1	0	-1	・防水対応センサーを用いる ・複数名の責任者を配置し、そのうち1名を現地スタッフとして常駐する ・保険に加入する
	気候（高温による熱暴走、低温による凍結など）	・温度変化に対する影響の受けやすさ	・機器が故障した際の対応マニュアルを作成している	1	2	4	1	0	-1	・複数名の責任者を配置し、そのうち1名を現地スタッフとして常駐する ・保険に加入する
	粉塵（ダスト）、浸食	・湿気、埃、汚れに対する影響の受けやすさ	・機器が故障した際の対応マニュアルを作成している	1	2	4	1	0	-1	・防塵対応センサーを用いる ・複数名の責任者を配置し、そのうち1名を現地スタッフとして常駐する ・保険に加入する
技術的	電力供給の停止（停電など）	・予備電源、UPS等の未確保 ・現地での対応が必要になった時に、遠方にある場合はすぐに駆け付けられない	−	1	2	4	1	0	-1	・予備電源、UPSを確保する
	機器の故障	・初期不良 ・定期的な交換計画の欠如	・保守サービスに加入している	1	3	4	1	-1	-1	・定期的な機器の交換計画を立て、実施する ・定期的なバックアップを実施する
	機器の誤動作	・初期不良 ・不適切な設定	−	1	3	4	1	-1	-1	・機器監視の強化
意図的（故意）	機器の盗難・破壊	・悪意あるユーザーによる実行 ・設置時、廃棄時の注意の欠如	・人間や動物等が近寄れない場所に設置する	2	2	3	0	0	0	
	盗聴・漏洩	・悪意あるユーザーによる実行 ・適切なID/PWの未設定 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	2	2	4	0	0	-1	・問題が発生した場合の対応マニュアルを作成する（早急にネットワークから取り外して初期化する、新型にリプレースするなど）
	遠隔攻撃（DDos攻撃など）	・悪意あるユーザーによる実行 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	1	2	4	1	0	-1	・DDos攻撃対策ソリューションを導入する ・問題が発生した場合の対応マニュアルを作成する（早急にネットワークから取り外して初期化する、新型にリプレースするなど）
	侵入/乗っ取り（データ改竄・破壊）	・悪意あるユーザーによる実行 ・適切なID/PWの未設定 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	2	3	4	0	-1	-1	・ネットワーク監視を強化する（侵入検知システムを導入するなど） ・定期的なバックアップの実施する ・問題が発生した場合の対応マニュアルを作成する（早急にネットワークから取り外して初期化する、新型にリプレースするなど）
過失	使用時のミス	・複雑なI/F ・不正確なパラメータ設定	・運用マニュアルを作成している	2	2	4	0	0	-1	・運用マニュアルを常に最新版にするように徹底する
	権限の詐称・乱用	・ユーザーの識別及び認証メカニズムの欠如 ・誤ったアクセス権の割り当て ・不十分なパスワード管理	・ID/PWを適切に管理している	2	2	3	0	0	0	

図表 23　リスク基準を満たすために実施すべき対応策（画像センサー）

類型	脅威	脆弱性	実施している対策	リスク値			リスク評価			リスク対応策
				機密性	完全性	可用性	機密性	完全性	可用性	
環境的（自然現象）	地震、火災	・機器を設置した建物の耐震・耐火工事の未実施 ・耐火設計されてない機器の利用	・機器を設置した建物の耐震・耐火工事を実施している ・機器が故障した際の対応マニュアルを作成している	1	2	4	0	0	-1	・複数名の責任者を配置し、そのうち1名を現地スタッフとして常駐する ・保険に加入する
	異常気象（大雨・暴風・豪雪など）	・過酷な気象状況では動作できない機器の利用	・機器が故障した際の対応マニュアルを作成している	1	2	4	0	0	-1	・防水対応センサーを用いる ・複数名の責任者を配置し、そのうち1名を現地スタッフとして常駐する ・保険に加入する
	気候（高温による熱暴走、低温による凍結など）	・温度変化に対する影響の受けやすさ	・機器が故障した際の対応マニュアルを作成している	1	2	4	0	0	-1	・複数名の責任者を配置し、そのうち1名を現地スタッフとして常駐する ・保険に加入する
	粉塵（ダスト）、浸食	・湿気、埃、汚れに対する影響の受けやすさ	・機器が故障した際の対応マニュアルを作成している	1	2	4	0	0	-1	・防塵対応センサーを用いる ・複数名の責任者を配置し、そのうち1名を現地スタッフとして常駐する ・保険に加入する
技術的	電力供給の停止（停電など）	・予備電源、UPS等の未確保 ・現地での対応が必要になった時に、遠方にある場合はすぐに駆け付けられない	−	1	2	4	0	0	-1	・予備電源、UPSを確保する
	機器の故障	・初期不良 ・定期的な交換計画の欠如	・保守サービスに加入している	1	3	4	0	-1	-1	・定期的な機器の交換計画を立て、実施する ・定期的なバックアップを実施する
	機器の誤動作	・初期不良 ・不適切な設定	−	1	3	4	0	-1	-1	・機器監視の強化
意図的（故意）	機器の盗難・破壊	・悪意あるユーザーによる実行 ・設置時、廃棄時の注意の欠如	・人間や動物等が近寄れない場所に設置する	2	2	3	-1	0	0	・人間や動物等が直接触れられないように柵を設置する ・不特定多数の者に拾われた場合の対策として、連絡先を記載しておく ・廃棄時においては、専門業者に委託する
	盗聴・漏洩	・悪意あるユーザーによる実行 ・適切なID/PWの未設定 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	2	2	4	-1	0	-1	・問題が発生した場合の対応マニュアルを作成する（早急にネットワークから取り外して初期化する、新型にリプレースするなど） ・可能な限り、人が映り込まない角度で撮影する
	遠隔攻撃（DDos攻撃など）	・悪意あるユーザーによる実行 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	1	2	4	0	0	-1	・DDos攻撃対策ソリューションを導入する ・問題が発生した場合の対応マニュアルを作成する（早急にネットワークから取り外して初期化する、新型にリプレースするなど）
	侵入/乗っ取り（データ改竄・破壊）	・悪意あるユーザーによる実行 ・適切なID/PWの未設定 ・最新の機器への交換やセキュリティパッチの未適用	・ID/PWを適切に設定している ・常に最新のファームウェアを適用している ・ファイアウォールを導入している	2	3	4	-1	-1	-1	・ネットワーク監視を強化する（侵入検知システムを導入するなど） ・定期的なバックアップの実施する ・問題が発生した場合の対応マニュアルを作成する（早急にネットワークから取り外して初期化する、新型にリプレースするなど） ・telnet等、不要なサービスを停止する（ポートを閉じる） ・電子証明書を導入する
過失	使用時のミス	・複雑なI/F ・不正確なパラメータ設定	・運用マニュアルを作成している	2	2	4	-1	0	-1	・運用マニュアルを常に最新版にするように徹底する ・運用者への教育を徹底する ・運用者が変更になった場合の適切な引継ぎを徹底する
	権限の詐称・乱用	・ユーザーの識別及び認証メカニズムの欠如 ・誤ったアクセス権の割り当て ・不十分なパスワード管理	・ID/PWを適切に管理している	2	2	3	-1	0	0	・運用担当者毎に適切な権限を割り当てる

2.4. 考察

今回対象としたIoTシステムの事例では、ISMSの範囲内で、セキュリティマネジメントを実施できると評価した（但し、詳細なISMS構築までは行っていないため、部分的にとどまる可能性は残る）。ISMSは情報セキュリティの3要素（機密性、完全性、可用性）のみならず、組織を取り巻く状況等を鑑みてセキュリティ方針を決定し、守るべき資産の抽出、抽出した資産に対するリスク分析、評価、対応を行うプロセスを適用範囲としている。そのため、一般的な情報システムにおける資産（PCや顧客台帳等）に限らず、多様なIoT機器を含むIoTシステムにおける資産に対しても、資産の特徴（IoT機器の場合は、ライフサイクルが長い、物理的な盗難リスクが高いなど）を踏まえたISMSを構築できることが、今回の調査結果から明らかとなったためである。

今回の調査対象としたIoTシステムの事例のように、多様なセンサー等のIoT機器を対象とする場合には、リスクの特定方法（脅威の特徴）に留意する必要がある。

具体的には、環境的脅威（自然現象）を想定した場合、IoTシステムでは、設置場所が屋外にある場合や、遠方にある場合もあるため、高温・低温・風雨など過酷な環境でも安定稼働できるような対策、動物等による接触への対策（柵を設定するなど）、システムが故障した際に迅速に対応できる体制（現地にスタッフを常駐させるなど）を整えることで、可用性を高めることが必要になるケースが出てくるであろう。

また、意図的脅威（盗聴、DDoS攻撃、データ改竄など）については、IoTシステムの場合もPCと同様にリスクを特定する必要がある。例えば、IDやパスワードを適切に設定し、不要なサービスを停止し、常に最新のファームウェアを適用するなどを行い、ネットワークを常に監視しておくことで、ある程度は防ぐことができると考えられる。特に、IoT機器にデフォルトのパスワードを設定し続けることは、INSECAM[27]の事例のようなことを引き起こしかねない。更に、不正アクセス行為の禁止等に関する法律があるが、初期状態のIDとパスワードでログインできる状態では取り締まることができないため、ユーザー自身による自衛が重要となる。

他の脅威としては、IoTシステムでは専用OSを用いていることも多く、十分なセキュリティ機能が搭載されなかったり、複雑な操作性に起因するパラメータの設定ミス等が起こりやすかったりすることが挙げられる。更に、IoT機器の場合は、機器自体の配慮事項、機器からデータを取得・加工する際の配慮事項、加工されたデータを扱う際の配慮事項等が想定され、今回の事例の画像センサーから取得されたデータは、エッジ側で処理するのか、クラウド側で処理されるのか等によってもリスクが異なる可能性がある（例えば、クラウド側で処理する場合、エッジ側で取得した画像データをクラウドへ送信する間の盗聴など）。ま

[27] https://www.insecam.org/en/bycountry/JP/

た、工場生産ラインと同様に「継続的な安定稼働が求められるもの」である IoT システムの場合は、「停止しないこと（＝停止すると損害額が大きくなる）」が最優先であり、セキュリティの多層化や冗長化等を検討する必要があるなど、可用性をより重視する必要があると考えられる。IoT システムにおいては、これらのように IoT 機器に特有のリスクがあることから、それらに留意することで ISMS を構築し、最適なセキュリティマネジメントを実施することが可能になると考えられる。

今回の調査では、IoT システム事例について簡易的な ISMS 構築にとどめている。今後は ISMS 適用可能性を詳細に検討することや CSMS 等の他の標準規格への適用可能性を試行することが必要であろう。引き続き、海外の検討状況等も鑑みて、IoT システムのセキュリティ向上に資するマジメントシステム適用について調査していく。

2.5. 参考文献

- ISMS ユーザーズガイド -JIS Q 27001:2014(ISO/IEC 27001:2013 対応）
- ISMS ユーザーズガイド -JIS Q 27001:2014(ISO/IEC 27001:2013 対応） -リスクマネジメント編-
- CSMS ユーザーズガイド -CSMS 認証基準（IEC62443-2-1）対応-
- IoT セキュリティガイドライン ver1.0（IoT 推進コンソーシアム）

3. 調査研究３：オンライン完結社会の実現に向けて

3.1. 調査研究の視点

インターネットの普及に伴い、様々なサービスが開発・提供され、利用者もスマートフォンやパソコン等でサービスを享受している。サービスを利用する際には、誰が使っているか識別する必要があり、ID・パスワードを用いてログインすることが一般的になっている。

しかしながら、人間の記憶は限界があり、ID・パスワードの組み合わせを覚えきれないという問題もある。記憶可能な ID・パスワードの組み合わせは、平均 3.15 組と言われている一方で、ID・パスワードを用いてログインするサイトの数は一人当たり平均 19.4 個[28]であると言われている。このため、複数のサイトで同じ ID・パスワードの使いまわしが行われ、一度どこかのサイトで ID・パスワードが漏洩すると、その情報が悪用され他のサイトでも不正にアクセスされてしまうという現象が発生しており、問題が深刻化している。

従来、セキュリティ対策の 1 つとして、パスワードの定期的な変更が求められてきた。これは、パスワード文字列が 4 文字であった時代に、パスワードの総当たり攻撃(ブルートフォースアタック)の対策として実施したきたことが起源と言われている。しかし、システム的にパスワード変更を一定周期で行うように設定すると、利用者はどこか 1 文字だけを変更する等新しいパスワードをいい加減に作る傾向があることがわかった。

そもそもパスワードに文字種や長さによる「複雑さ」が求められる理由は、攻撃者が制限のない状態でパスワードの文字列を総当たりで試すと、時間はかかるにせよ「必ず探り当てることが可能」であることを前提としているためである。つまり、攻撃者がパスワードの総当たり攻撃によって解読されるまでの時間を、パスワードの「複雑さ」によって確保している。

「ログインパスワード」は、ウェブサービスのログインページや、パソコンや IoT 機器のログイン画面に入力するもので、こういった入力画面ではネットワーク経由でログインを試みる場合どう頑張っても 1 秒に数回～数十回程度しか入力することが出来ず、これだけで実質的に高速な攻撃を防いでいることになる。また、PIN（Personal Identification Number）と呼ばれるキャッシュカード等の暗証番号などは、一定回数間違えるとログインが制限される仕様とすることで総当たり攻撃の対策がなされている。

一般的に推奨されている、英大文字・小文字、数字、記号（26 種）の合計 88 種類の文字を使い、10 桁のパスワードを作ったとすると、その組合せは約 2785 京個となる。仮に 1 秒 あたり 5 回の「総当たり攻撃」が可能であった場合、全組合せ試すまでに約 1760 億年かかる計算になる。

これならばすぐにパスワードが割り出される可能性は限りなく低く、事実上は不可能と

[28] 『ID とパスワードに関する意識調査 分析レポート』（野村総合研究所、2011 年）

いうことができる。

このような背景を踏まえ、本調査研究では、ID・パスワードの安全性について議論されてきたパスワードの定期的な変更などの論点について、フォーカスを当て検討する。

3.2. 調査研究の対象

実際に、2017 年以降に政府及び関係機関が出している方針では、パスワードの定期的な変更が推奨されなくなってきている。

例えば、NISC（内閣サイバーセキュリティセンター）が、2017 年 12 月 18 日に発行した「ネットワークビギナーのための情報セキュリティハンドブック[29]」では、以下のような記載となっている。

> *『7 パスワードの定期変更は必要なし。流出時は速やかに変更する』*
>
> *利用するサービスによっては、パスワードを定期的に変更することを求められることがあります。しかし、実際にパスワードを破られアカウントを乗っ取られたり、サービス側から流出したりした事実がないのならば、パスワードを変更する必要はありません。*
>
> *むしろ定期的な変更を要求することで、パスワードの作り方がワンパターン化し簡単なものになることや、使い回しするようになることの方が問題となります。定期的に変更をするよりも、機器やサービスの間で使い回しのない、固有のパスワードを設定しましょう。*
>
> *パスワードを破られウェブサービスなどが不正利用されたら、速やかにパスワードを変更し、その原因も特定しましょう。*
>
> *マルウェアなどでパソコン側から情報が流出し続けている場合、原因を特定しないまま放置しているなら、パスワードを変更しても意味がありません。*
>
> *アカウントが完全に乗っ取られてしまった場合はサービス側に連絡して復旧しましょう。*
>
> *一方、自分の使用機器からではなく、ウェブサービスなどの側からパスワード流出が起きた場合は、速やかにパスワードを変更の上、流出の原因となった点の対策が行われたかを確認します。*

また、総務省が公開している「安心してインターネットを使うために国民のための情報セ

[29] 『ネットワークビギナーのための情報セキュリティハンドブック Ver3.00』（NISC、2017 年）
https://www.nisc.go.jp/security-site/handbook/index.html

キュリティサイト[30]」においても、NISC と同様に以下の記載へと変更された。

『パスワードを複数のサービスで使い回さない（定期的な変更は不要)』

またパスワードはできる限り、複数のサービスで使い回さないようにしましょう。あるサービスから流出したアカウント情報を使って、他のサービスへの不正ログインを試す攻撃の手口が知られています。もし重要情報を利用しているサービスで、他のサービスからの使い回しのパスワードを利用していた場合、他のサービスから何らかの原因でパスワードが漏洩してしまえば、第三者に重要情報にアクセスされてしまう可能性があります。

なお、利用するサービスによっては、パスワードを定期的に変更することを求められることもありますが、実際にパスワードを破られアカウントが乗っ取られたり、サービス側から流出した事実がなければ、パスワードを変更する必要はありません。むしろ定期的な変更をすることで、パスワードの作り方がパターン化し簡単なものになることや、使い回しをするようになることの方が問題となります。定期的に変更するよりも、機器やサービスの間で使い回しのない、固有のパスワードを設定することが求められます。

これまでは、パスワードの定期的な変更が推奨されていましたが、2017 年に、米国国立標準技術研究所（NIST）からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示されたところです（※１)。また、日本においても、内閣サイバーセキュリティセンター（NISC）から、パスワードを定期変更する必要はなく、流出時に速やかに変更する旨が示されています（※２)。

（※1）NIST SP800-63B（電子的認証に関するガイドライン）

（※2）https://www.nisc.go.jp/security-site/handbook/index.html

これらの考え方の起点になっている「NIST SP 800-63-3」について、次章で解説するとともに、事業者がとるべき対応について考察する。

3.3. オンライン完結に向けた電子認証のセキュリティについての調査結果

3.3.1. NIST SP800-63-3 について

米国立標準技術研究所（NIST）の認証に関するガイドライン「Electronic Authentication Guideline（電子的認証に関するガイドライン)」が改定され、その第 3 版（NIST SP 800-63-3）が 2017 年 6 月に正式に「Digital Identity Guideline（デジタル・アイデンティティ・ガイドライン)」として発表された。

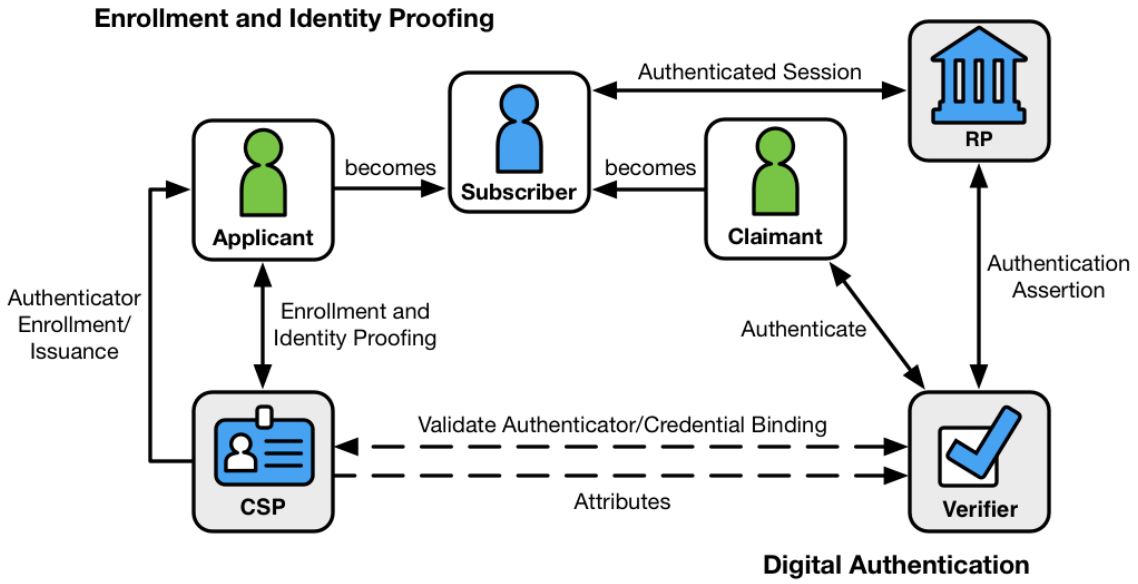
[30] 総務省　安心してインターネットを使うために国民のための情報セキュリティサイト
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01-2.html

このガイドラインは 米国政府のセキュリティ対策での利用を前提にしているが、政府系システムとの接続要件等にも関係してくるため、世界的にも大きな影響を与える可能性がある。既に、ID 管理技術に関する業界団体 Kantara Initiative では、新しいガイドラインに合わせた認証スキームの更新が進められている[31]。

NIST SP 800-63 は、アメリカ政府機関がユーザー認証やユーザーの Identity Proofing を行うシステムを構築する際の実装ガイドラインである。そのため、日本の制度と異なる部分や民間サービスに合わない部分もあるが、参考にすべき点も多い。

これまでの第 2 版では、米国の政府システムで認証を行う際の指標（LoA：Level of Assurance）に基づいた要件を定めており、これは日本でも広く参考にされている。第 3 版では、LoA という考え方に代わり、Digital Identity Model の 3 フェーズについて Assurance Level を定義し、Assurance Level ごとにサブドキュメント化することで、サービスの内容に合わせて各フェーズの Assurance Level をより実際のニーズ（仮名性は確保しつつ認証レベルは強化したい等）に合わせて組み合わせることが可能となっている。

図表 24　Digital Identity Model（出典：NIST Special Publication 800-63-3 Digital Identity Guidelines）



3.3.2.　Assurance Level について

各 Assurance Level とフェーズ、対応するドキュメントは以下の通りである。

[31] https://kantarainitiative.org/trustoperations/800-63-3/

- Identity Assurance Level（IAL）（SP 800-63A）

ユーザーが、申請者（Applicant）として新規登録（SignUp）する際に、CSP（Credential Service Provider）が行う身元確認（Identity Proofing）の厳密さ、強度を示す。

図表 25　身元情報保証レベル

レベル	条件
IAL1	身元確認は不要、自己申告での登録でよい
IAL2	サービス内容により識別に用いられる属性をリモートまたは対面で確認する必要あり
IAL3	識別に用いられる属性を対面で確認する必要があり、確認書類の検証担当者は有資格者

- Authenticator Assurance Level（AAL）（SP 800-63B）

登録済みユーザー（Claimant）が、ログインする際の認証プロセス（単要素認証 or 多要素認証、認証手段）の強度を示す。

図表 26　認証コード保証レベル

レベル	条件
AAL1	単要素認証で OK
AAL2	2 要素認証が必要。 2 要素目の認証手段はソフトウェアベースのもので OK
AAL3	2 要素認証が必要。 かつ 2 要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）

- Federation Assurance Level（FAL）（SP 800-63C）

ID トークンや SAML Assertion 等、Assertion のフォーマットやデータやり取りの仕方の強度を示す

図表 27　連携保証レベル

レベル	条件
FAL1	Assertion（RP に送る IdP での認証結果データ）への電子署名
FAL2	電子署名に加え、対象 RP のみが復号可能な暗号化
FAL3	FAL2 に加え、Holder-of-Key Assertion の利用（ユーザーごとの鍵と IdP が発行した Assertion を紐づけて RP に送り、RP はユーザーがその Assertion に紐づいた鍵を持っているか（ユーザーの正当性）を確認）

SP 800-63-3 では、各機関はリスクアセスメントを行った後に IAL、AAL、FAL のレベルを選定するためのチャートが提供されており、該当したレベルの要件をサブドキュメントで確認したうえで、要件を満たすサービス実装を行うことになる。

第 3 版では、「セキュリティが統制されている」、「リスク評価がなされている」など、SP800-53 や SP800-30 を前提として、各プロセスにレベル分けした要件が定められている。政府機関は独自の体制が出来上がっているが、専門部署を持たない民間企業が実際にリスク評価を行うことができるかが、本ガイドラインを参考にするうえでの今後の課題となる。

今回の改定で最も注目しているのは、SP 800-63B「Authentication and Lifecycle Management（認証とライフサイクル管理）」である。

SP 800-63B は、登録済みアカウントを利用してデジタル世界でのユーザー認証を行い、その結果の正しさを確認するプロセスについて記述されており、Authenticator タイプや AAL（Authenticator Assurance Level）が定義されている。

今回の改訂で、ユーザー認証に使われる技術に関する NIST の見解が示されており、米国政府向けとは言いつつも、今後一般的なサービスにも影響が及ぶ可能性が一番高い部分になる。特にパスワードや PIN 等ユーザーが記憶するものについては、今後パスワードからパスフレーズへの移行が意図されており、パスワードの定期変更の非推奨、秘密の質問の排除等が盛り込まれている。

このほかにも、乱数表の使用方法が制限されていたり、現時点では生体認証は利便性提供のための補助的な認証要素と位置づけられている、など、ID 管理を含むサービス構築の際に考慮すべきポイントが見られる。

図表 28　各 AAL の要件のまとめ

要件	AAL1	AAL2	AAL3
許可されている Authenticator タイプ	記憶シークレット; ルックアップシークレット; アウトオブバンド; 単一要素 OTP デバイス; 多要素 OTP デバイス; 単一要素暗号化ソフトウェア; 単一要素暗号化デバイス; 多要素暗号化ソフトウェア; 多要素暗号化デバイス	多要素 OTP デバイス; 多要素暗号化ソフトウェア; 単一要素暗号化デバイス; または 記憶シークレット および: • ルックアップシークレット • アウトオブバンド • 単一要素 OTP デバイス • 単一要素暗号化ソフトウェア • 単一要素暗号化デバイス	多要素暗号化デバイス; 単一要素暗号化デバイス および記憶シークレット; 単一要素 OTP デバイス および多要素暗号化デバイスまたはソフトウェア; 単一要素 OTP デバイス および単一要素暗号化ソフトウェアおよび記憶シークレット
FIPS 140 確認	Level 1（政府機関の Verifier）	Level 1（政府機関の Authenticator 及び Verifier）	レベル 2 全体（マルチファクタ認証コード） レベル 1 全体（検証者と単一ファクタ暗号化デバイス） レベル 3 物理セキュリティ (すべての認証コード)
Reauthentication	30 日	12 時間 または 30 分 の非活動; 1 つの Authentication 要素でもよい(MAY)	12 時間 または 15 分 の非活動；両方の Authentication 要素をつかうものとする(SHALL)

要件	AAL1	AAL2	AAL3
セキュリティ管理策	SP 800-53 低度のベースライン(または等価)	SP 800-53 中度のベースライン(または等価)	SP 800-53 高度のベースライン(または等価)
中間者攻撃耐性	必須	必須	必須
Verifier なりすまし耐性	不要	不要	必須
Verifier 危殆化耐性	不要	不要	必須
リプレイ耐性	不要	必須	必須
認証意図	不要	推奨	必須
記録保持ポリシ	必須	必須	必須
プライバシー管理策	必須	必須	必須

3.3.3. SP800-63-3 の日本語訳について

JIPDEC が主催する ID 連携トラストフレームワーク推進コンソーシアム[32]と OpenID Foundation Japan[33]と共同で、NIST SP 800-63-3 の日本語訳ならびに 2 回の勉強会[34]を実施した。NIST SP 800-63-3 の日本語訳については、勉強会の開催報告を参照されたい。

3.4. 考察

パスワードの定期変更については、旧来から実施の意味について議論があったが、NIST SP 800-63-3 が発行されたことで、世の中のパスワードの定期変更に関する考え方が 180 度変わった。徐々にではあるが、日本でも追従する動きが出てきている。

JIPDEC においても、プライバシーマーク推進センターではこれらの検討状況を踏まえ「JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン－第 2 版－」の「Ⅱ．技術的安全管理措置として講じなければならない事項と望ましい手法の例示」において、望ましい手法の例示で、「パスワード有効期限を設定している」の削除ならびに、「漏洩した、または漏洩のおそれがあるパスワードは速やかに変更することを求めている」の追加の対応を行った。

一方で、実際に現場でこのルールが適用されたときに発生する問題や課題について整理して対応策を検討した。

パスワードの取り扱いなどを含む、認証コード（Authenticator）の詳細については、SP 800-63B「5 章　認証コードと検証者の要件」を参照されたい。

ここでは、重要と思われる点について検討したい。

---

[32] https://idftf.jipdec.or.jp/idftf_c.html

[33] http://www.openid.or.jp/

[34] https://www.jipdec.or.jp/topics/event/20171013.html

図表 29　認証要素の概要

#	原文	和訳	認証要素	暗号プロトコル（鍵の所持証明）として認められるか	HW（ハードウェア）として認められるか	例
1	Memorized Secret	記憶シークレット	知識	No	No	パスワード、PIN
2	Look-up Secret	ルックアップシークレット	所有	No	No	乱数表（銀行のログインなどで使用）
3	Out of Band Device	アウトオブバンドデバイス	所有	No	No	モバイル端末での SMS コード送信、QR、バーコード。e メールは×
4	SF OTP Deveice	単一ファクタ OTP デバイス	所有	No	Yes/No	パスフレーズ入力不要な OTP デバイス（スマホインストールソフトも OK）
5	MF OTP Device	マルチファクタ OTP デバイス	所有・知識/生体	No	Yes/No	TouchID やマスタ PW でアクティベートし利用する OPT アプリ
6	SF Cryptographic Software	単一ファクタ暗号化ソフトウェア	所有	Yes	No	端末毎のクライアント証明書（パスワード保護なし）
7	SF Cryptographic Device	単一ファクタ暗号化デバイス	所有	Yes	Yes	FIDO U2F の USB ドングル
8	MF Cryptographic Software	マルチファクタ暗号化ソフトウェア	所有・知識/生体	Yes	No	指紋認証を行うことで有効化されるクライアント証明書
9	MF Cryptographic Device	マルチファクタ暗号化デバイス	所有・知識/生体	Yes	Yes	パスワードまたはバイオメトリクスでアクティベートしなければ利用できないようになっている USB トークン、TouchID 等

参考）勉強会時の説明資料より

https://www.slideshare.net/kthrtty/20171027-nist-sp80063bkthrtty-81333156

●パスワード（認証記憶シークレット）に関する事項
・加入者（利用者）が設定する場合、最低 8 文字以上にしなければならない
・管理者（CSP か検証者）がランダムに設定する場合は、最低 6 文字以上にしなければならない（すべて数字でもよい）
・文字列の繰り返しの禁止など、複雑性に関するほかの要件を強要すべきではない
・定期的に変更するように要求すべきでない
・ただし、パスワード漏洩のある恐れがある時には、変更を強制しなければならない
・貼り付け機能を利用すべきである（現状は禁止しているサイトが多い）
※パスワードマネージャの使用を促進することで、利用者がパスワードを記憶する必要をなくし、複雑性の高い強力なパスワード用いるようにするという考え
・パスワードの入力をアスタリスクなどで表示せずに入力が終わるまで表示するオプションを提供すべきである。
※盗み見られない場所での利用時に、入力確認できるようにする。また、モバイルの場合は入力後の短時間表示を行う機能なども許可してもよい
・パスワードはハッシュ化して保存しなければならない（変わらず）

●パスフレーズ導入に向けた変更
・管理者はパスワードの上限として、最低 64 文字を許可すべきである
・スペースも使えるようにすべきである

このようにパスワードに関する考え方は、従来の考えと真逆になっている部分も多く存在するので注意が必要である。従来の考え方に基づいた現状のシステムでは、文字数を 8 文字以上 16 文字未満のように、レンジに幅を持たせた設定をしているサイトが多く、上限値があまり高くないという問題がある。

今回の改定のコンセプトは自分にとっては覚えやすい、長めの文章（パスフレーズ）を作成し、漏洩時を除き、むやみに変更しないという考えである。このため、パスフレーズ対応が 1 つのポイントになる。パスフレーズ対応に関して、システム側で抱えるであろう課題は 2 つある。1 つは、スペースをパスワード内の利用可能文字列に含めること。もう 1 つは、文字数の上限設定を大幅に拡大することである。

SP 800-63B では、最低 64 文字にすべきであるなどのように、長いフレーズが使えるようにする変更を必要としている。また、文字種の制限は不要であるが、脆弱なパスワードを設定されないように管理者（認証者）側で制限する仕組みを入れることを推奨している。

例えば、
•過去に漏洩した語彙集から得られるパスワード
•辞書に含まれる言葉

•繰り返しや連続文字（例：‘aaaaaa’、’1234abcd’）
•サービス名、ユーザー名、そこから派生するような、文脈で特定可能な単語
などである。

また、パスワード強度については、SP 800-63B の付録 A の記述が興味深い。前提として、ユーザーは複雑で恣意的なシークレットを記憶する能力は限られているため、容易に推測できるパスワードを選ぶことが多い。

パスワードの長さは、パスワードの強度を特徴付ける主要因であることがわかっている。短すぎるパスワードは、単語や一般的に選択されたパスワードを利用する辞書攻撃と同様に総当たり攻撃を受けた時に脆弱である。

最低でも「どの程度の長さのパスワードが必要となるか」は、想定する脅威モデルによって大きく左右される。

ユーザーには、理に適った範囲内で望みどおりの長さのパスワードを使うことを奨励すべきである。

研究では、ユーザーが構成ルールで課せられた要件に対して非常に安易な方法で対応することが明らかになった。例えば、パスワードとして”password”を選択したユーザーは、大文字と数字を含む要件を与えると、比較的高い確率で”Password1”を選択し、記号を要件に追加すると”Password1!”を選択している。

複雑なパスワードを作成しようとしてもオンラインサービスで拒否されることにもユーザーは不満を抱いている。多くのサービスではスペースや特殊文字を含むパスワードが拒否される。特殊文字が受け入れられないケースには、特殊文字を用いる SQL インジェクションのような攻撃を回避する目的がある。しかし、システム側で特殊文字のエンコーディングや適切にハッシュ化を行えばよく、そのような予防策を講じるべきではない。また、自由にフレーズを設定できるようにスペース文字の使用を許可すべきである。

ユーザーのパスワードの選択は、非常に簡単に予想でき、攻撃者は過去に成功した正しいパスワードを推測する可能性がある。こうしたパスワードには、辞書にある単語や上記の例の”Password1!”のように過去に漏洩したパスワードがある。この理由から、ユーザーが選択したパスワードを許容できないパスワードのブラックリストと比較することを推奨する。

極端に複雑な記憶シークレットは新たな脆弱性を生み出す。シークレットを記憶できる可能性が減り、書き留めたり安全でない方法で電子的に記録したりする可能性が高まる。これらの慣例は必ずしも脆弱であるわけではないが、統計的に見るとそのような記録方法の中には脆弱なものがある。これは極端に長いか極端に複雑な記憶シークレットを要求しないということの補足的な理由である。

当然ながら、各システムにパスワード管理の仕組みを導入する際には、守るべき情報の重要性を十分に検討し、認証の強度を使い分けることが大事である。単純に強度をあげればよ

いというものでなく、適切な強度を採用しないと、認証用のハードウェアを持ち歩かなければならなくなるなど、認証の手間がかかりすぎて利便性が低下したり、ユーザーに負荷がかかるケースが想定される。最終的には利便性とセキュリティのバランスを両面から考えて決定する必要がある。

また、同じパスワード（パスフレーズ）を各サイトで使いまわすと、脆弱な 1 つのサイトから漏洩した情報を用いて他のサイトが攻撃されるインシデントに発展する可能性がある。パスワードの使いまわしを抑止するには、パスワードマネージャの使用も有効である。しかし、昨今普及しているクラウドサービス型のパスワードマネージャの全てが安全性の高いサービスを提供しているかは分からない。また、各サイトに安全性の高い認証システムの実装を求める状況は変わらない。

公開された基準に準拠し、高い透明性のもとで監査された認証基盤を実装する CSP と ID 連携によりあらゆるサービスが享受できる ID 連携トラストフレームワークの早期実現に向けて、JIPDEC として継続して活動していきたい。

3.5. 参考文献

- ID 連携トラストフレームワーク
  http://www.meti.go.jp/policy/it_policy/id_renkei/
- NIST SP 800-63-3
  https://pages.nist.gov/800-63-3/
- NIST SP 800-63-3（日本語訳）
  https://www.jipdec.or.jp/sp/topics/event/u71kba0000009o56-att/nist_sp_800-63-3.pdf
- NSIT SP 800-63A（日本語訳）
  https://www.jipdec.or.jp/sp/topics/event/u71kba0000009o56-att/nist_sp_800-63a.pdf
- NSIT SP 800-63B（日本語訳）
  https://www.jipdec.or.jp/sp/topics/event/u71kba0000009o56-att/nist_sp_800-63b.pdf
- NSIT SP 800-63C（日本語訳）
  https://www.jipdec.or.jp/sp/topics/event/u71kba0000009o56-att/nist_sp_800-63C.pdf

電子情報利活用研究レポート

平成 30 年 6 月 29 日

一般財団法人日本情報経済社会推進協会 電子情報利活用研究部

〒106-0032
東京都港区六本木一丁目 9 番 9 号　六本木ファーストビル内
TEL　03-5860-7558
URL　https://www.jipdec.or.jp/