令和 3 年度サイバー・フィジカル・セキュリティ対策促進事業

（サイバー・フィジカル・セキュリティ対策フレームワークの実装・推進に関する調査）

調査報告書

令和 4 年 3 月 31 日

株式会社日立製作所

目次

エクゼクティブサマリー.....1

1　本事業の概要.....3

1.1　目的.....3

1.2　事業内容.....4

1.3　実施スケジュール.....8

1.4　実施体制.....9

1.5　本調査報告書の構成.....9

2　サイバー空間におけるつながりの信頼性及び IOT 機器等の転写機能の信頼性を確保するための対策要件等に関する動向等についての調査.....10

2.1 IoT 機器等の転写機能の信頼性を確保するための対策要件等に関する動向等についての調査.....10

2.2 サイバー空間におけるつながりの信頼性を確保するための対策要件等に関する動向等についての調査.....15

3　CPSF 等に基づく国際規格（TR 等を含む）の推進.....21

3.1　本事業項目の目的.....21

3.2　本事業項目の実施内容.....21

3.3　本事業項目の実施結果.....21

エクゼクティブサマリー

・ 経済産業省では、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、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」の実現へ向けて様々なデータの「つながり」から新たな付加価値を創出していく「Connected Industries」という概念を提唱し、その実現に向けた取り組みを推進している。「つながる」ことによるネットワーク化の進展は、悪意のある者にとって新たな攻撃の機会ともなっていくおそれがあるため、各企業におけるサイバーセキュリティ対策に加えて、サプライチェーン全体としてサイバーセキュリティ確保に向けて取り組む必要がある。また、サイバー攻撃は国境を越えて行われるものであり、米欧各国等との連携を強化し、我が国の取り組みを積極的に国際標準に提案するなど、国際ハーモナイゼーションを確保していくことを常に視野に入れた取り組みを進めていく必要がある。

・ このような背景を踏まえ経済産業省では、平成 29 年 12 月に産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される「産業サイバーセキュリティ研究会」（以下、「研究会」という。）を立ち上げた。サプライチェーンのサイバーセキュリティ強化に向けては、「制度・技術・標準化」WG にて、「Society5.0」における新たな形のサプライチェーンに求められるセキュリティ対策の全体像を整理した「サイバー・フィジカル・セキュリティ対策フレームワーク」（以下、「CPSF」という。）を平成 31 年 4 月に策定した。CPSF では、「Society5.0」における産業社会を3つの層（企業間のつながり（第1層）、フィジカル空間とサイバー空間のつながり（第2層）、サイバー空間におけるつながり（第3層））に整理し、セキュリティ確保のための信頼性の基点の明確化を行った。加えて、産業分野共通の課題を検討する分野横断 SWG、タスクフォース（以下、「TF」という。）等を立ち上げ、それぞれの課題に応じた検討を並行して進めている。

・ CPSF では、サイバー空間とフィジカル空間が高度に融合した産業社会の中で、サイバー空間とフィジカル空間の境界で交換される情報が正確に転換されること、つまり境界上における“転写”という役割に焦点を当て、第 2 層の信頼性の基点を転写機能とした上で、転写機能の信頼性を確保するための対策要件及び対策例を提示しているが、転写機能を担う IoT 機器等の多様性やインシデントが発生した場合の被害の複雑化等も踏まえ、IoT 機器等に求められるセキュリティ対策やリスクアセスメントの考え方等について更なる検討が必要である。そこで、令和 2 年 11 月に、サイバー空間とフィジカル空間をつなぐ新たな仕組みによってもたらされる新たなリスクに着目し、リスク形態及びそうしたリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示する「IoT セキュリティ・セーフティ・フレームワーク」（以下、「IoT-SSF」という。）を策定した。

・ サプライチェーンのサイバーセキュリティ強化に向けては、各国政府においても取り組みが行われている状況下で、日本が国際的なサイバーセキュリティ対策のルールメイキングに主導的な役割を担えるようになるためにも、日本からサイバーセキュリティ対策の枠組みを提案することが重要である。

・ 本事業では、研究会及び各 WG 等の議論を踏まえ、各国政府の取り組みやその他国内外のセキュリティ等に関する文献等を調査し、サイバー空間におけるつながりの信頼性及びIoT機器等の転写機能の信頼性を確保するための対策要件等の検討及び CPSF 等に基づく国際規格（TR等を含む。）の推進を目的として実施した。

・ 本事業項目（1)「サイバー空間におけるつながりの信頼性及び IoT 機器等の転写機能の信頼性を確保するための対策要件等に関する動向等についての調査」では、IoT 機器等の転写機能の信頼性を確保するために求められる標準化団体、業界団体及び外国政府の取り組み等や IoT 機器等のセキュリティ対策、及びそれらの信頼性の確認手法等について、公開情報等を調査し整理した。また、一連の IoT-SSF の適用の流れを複数のユースケースを用いて例示するユースケース集を検討し、事業期間中開催された TF 等の議論の内容を反映して、「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集」としてまとめた。

・ サイバー空間におけるつながりの信頼性を確保するために求められる標準化団体、業界団体及び外国政府の取り組み等やデータのセキュリティ対策及びそれらの信頼性の確認手法等について、公開情報等を調査し整理した。また、事業期間中 2 回実施したパブリックコメントでいただいた意見や、TF 等での議論の内容を反映し、「協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ」としてまとめた。

・ 本事業項目（2)「CPSF 等に基づく国際規格（TR 等を含む。）の推進」においては、CPSF をベースにした国際標準化を推進することを目的として、推進に必要な諸外国の政府又は政府関連機関、業界団体、標準化団体等によるルール形成の取り組み状況等の調査や、ISO/IEC 及びそれに関連する会議等における必要な働きかけの実施、CPSF 等に基づく国際規格（案）の作成等を実施した。

・ 具体的には、国際規格策定に向けた検討のロードマップを策定し、適宜必要な文献調査等を実施しつつ、サイバーセキュリティに関する国際規格の策定や維持管理を担う ISO/IEC JTC 1/SC 27/WG 4（セキュリティコントロールとサービス)の国内エキスパートと連携して本件に係る国際規格策定プロジェクトの提案及び PWI(予備業務項目)、NWIP(新規作業項目提案)としてのプロジェクト推進、その他必要に応じて国内外の関係者との意見交換を行った。CPSF をベースにした国際標準の実現に向けては、2022 年度以降も、本調査を通じて策定されたロードマップや識別された推進上の課題等を参照して、ISO/IEC JTC 1/SC 27/WG 4 におけるプロジェクトを効果的に推進していくことが期待される。

1 本事業の概要

1.1 目的

我が国では、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、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」の実現を提唱している。経済産業省では、「Society5.0」の実現へ向けて様々なデータの「つながり」から新たな付加価値を創出していく「Connected Industries」という概念を提唱し、その実現に向けた取り組みを推進している。

その一方で、「つながる」ことによるネットワーク化の進展は、悪意のある者にとって新たな攻撃の機会ともなっていくおそれがある。サイバー攻撃の起点は急激に拡大し、攻撃の手法も高度化しており、サイバー攻撃の脅威は、あらゆる産業活動に潜むようになっている。このような状況においては、各企業におけるサイバーセキュリティ対策に加えて、関連企業、取引先等、サプライチェーン全体としてサイバーセキュリティ確保に向けて取り組む必要がある。また、サイバー攻撃は国境を越えて行われるものであり、サイバーセキュリティ対策も国内だけの取り組みでは十分ではなく、米欧各国等との連携を強化し、我が国の取り組みを積極的に国際標準に提案するなど、国際ハーモナイゼーションを確保していくことを常に視野に入れた取り組みを進めていく必要がある。

このような背景を踏まえ、経済産業省では、産業におけるサイバーセキュリティ政策を「産業政策と連携した政策展開」、「国際ハーモナイゼーション」、「サイバーセキュリティビジネスの創出支援」及び「基盤の整備」の 4 つの柱で捉え、平成 29 年 12 月に、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される「産業サイバーセキュリティ研究会」（以下、「研究会」という。）を立ち上げた。そして、同研究会の下に専門的な議論を行う3つのワーキンググループ（以下、「WG」という。）を設置し、「制度・技術・標準化」、「経営・人材・国際」及び「サイバーセキュリティビジネス化」のテーマ毎に議論を行い、平成 30 年 5 月に開催した第 2 回研究会にて、「サプライチェーンサイバーセキュリティ強化」、「サイバーセキュリティ経営強化」、「サイバーセキュリティ人材育成・活躍促進」及び「セキュリティビジネスエコシステム創造」の 4 つのパッケージからなるアクションプランを公表し、平成 31 年 4 月に開催した第 3 回研究会にて、上記のアクションプランを深化・拡大するために、「グローバルをリード」、「信頼の価値を創出」及び「中小企業・地域まで展開」の 3 つの加速化指針を示した。更に、令和 2 年 4 月の第 4 回研究会では、セキュリティ対策の徹底と強化をお願いする「産業界へのメッセージ」を示し、同 6 月の第 5 回研究会において、上記アクションプランの持続的発展と新たな課題へのチャレンジとして「アクションプランの高度化」、「For the future infrastructure」を公表した。

特に、サプライチェーンのサイバーセキュリティ強化に向けては、「制度・技術・標準化」WG にて、「Society5.0」における新たな形のサプライチェーンに求められるセキュリティ対策の全体像を整理した「サイバー・フィジカル・セキュリティ対策フレームワーク」（以下、「CPSF」という。）を平成 31 年 4 月に策定した[1]。CPSF では、「Society5.0」における産業社会を 3 つの層（企業間のつながり（第1層）、フィジカル空間とサイバー空間のつながり（第 2 層）、サイバー空間におけるつながり（第3層））に整理し、セキュリティ確保のための信頼性の基点の明確化を行った。加えて、CPSF の考え方を産業活動に実装するために、産業活動の実態に応じて、必要な対策要件や対策水準について検討を行う産業分野別のサブワーキンググループ（ビルサブワーキンググループやスマートホームサブワーキンググループ等。以下、まとめて「産業分野別 SWG」という。）に加えて、産業分野共通の課題を検討する分野横断 SWG、タスクフォース（以下、「TF」という。）等を立ち上げ、それぞれの課題に応じた検討を並行して進めている。

「Society5.0」における産業社会では、様々なモノやサービスがつながる中で、信頼できる主体が生成・加工したとは必ずしもいえないデータによる産業活動が想定されるため、サイバー空間におけるデータの信頼性確保は重要な課題となる。CPSF では、第 3 層の信頼性の基点をデータと

した上で、データの信頼性を確保するための対策要件及び対策例を提示しているが、実際の産業活動への実装に向けて、産業活動におけるデータの区分やデータ利活用の実態を踏まえた上で、より具体的な対策要件やデータの完全性や真正性を確認する仕組みとしてどのような手法やルールが効果的か、その実効性や国際的な動向も踏まえた上で更なる検討が必要である。また、CPSF では、サイバー空間とフィジカル空間が高度に融合した産業社会の中で、サイバー空間とフィジカル空間の境界で交換される情報が正確に転換されること、つまり境界上における“転写”という役割に焦点を当て、第 2 層の信頼性の基点を転写機能とした上で、転写機能の信頼性を確保するための対策要件及び対策例を提示しているが、転写機能を担うIoT機器等の多様性やインシデントが発生した場合の被害の複雑化等も踏まえ、IoT 機器等に求められるセキュリティ対策やリスクアセスメントの考え方等について更なる検討が必要である。

サプライチェーンのサイバーセキュリティ強化に向けては、各国政府においても取り組みが行われている。例えば、米国では国防総省と直接取引をする企業だけでなく、サプライチェーンに連なる全ての企業に対して、Cybersecurity Maturity Model Certification の第三者認証を求めることを検討している。このような状況下で、日本が国際的なサイバーセキュリティ対策のルールメイキングに主導的な役割を担えるようになるためにも、日本からサイバーセキュリティ対策の枠組みを提案することが重要である。

本事業では、研究会及び各 WG 等の議論を踏まえ、各国政府の取り組みやその他国内外のセキュリティ等に関する文献等を調査し、サイバー空間におけるつながりの信頼性及び IoT 機器等の転写機能の信頼性を確保するための対策要件等の検討及び CPSF 等に基づく国際規格（TR 等を含む。）の推進を目的として実施するものである。

1.2 事業内容

本事業ではこの目的を達成するため、大きく分けて 3 つの事業項目を実施した。本事業において実施した事業内容を表 1-1 に示す。また、具体的な実施内容の全体像を図 1-1 に示す。

表 1-1 本事業の事業項目と具体的な実施内容

No	事業項目	仕様書の内容	具体的な実施内容
1	サイバー空間におけるつながりの信頼性及び IoT 機器等の転写機能の信頼性を確保するための対策要件等に関する動向等についての調査	【事業内容】 本事業では、サイバー空間におけるつながりの信頼性及びIoT機器等の転写機能の信頼性を確保するために求められる外国政府の取り組みやその他国内外のデータのセキュリティ対策やIoT機器等のセキュリティ対策及びそれらの信頼性の確認手法等を調査する。 想定する調査項目例を以下に示すが、具体的な調査項目については、商務情報政策局サイバーセキュリティ課の担当者（以下、「担当者」という。）と協議の上で決定する。 なお、3⑥に示すTFでの議論等によって新たな視点での調査の必要性が生じた場合は、追加的に調査を行うこと。 ＜想定する調査項目の例＞ ●産業活動で利活用するデータやIoT機器等のセキュリティ確保に向けた国内外の政策動向 ●既に国内外で策定されているデータやIoT機器等のセキュリティ確保を目的とした制度やガイドライン等の概要（国・地域、適用分野、策定者、対象者、遵守義務、普及状況など） ●データやIoT機器等の差異や区分（カテゴリ）に応じて異なるセキュリティ水準及びセキュリティ対策が求められている場合には、当該セキュリティ水準及びセキュリティ対策の内容 ●データやIoT機器等の信頼性を確認するための技術的又は制度的枠組	IoT 機器等の転写機能の信頼性を確保するために求められる標準化団体、業界団体及び外国政府の取り組み等や IoT 機器等のセキュリティ対策等について、日本、米国、欧州、シンガポールの公開情報等を調査し整理した。 また、一連の IoT-SSF の適用の流れを複数のユースケースを用いて例示するユースケース集を検討し、社内有識者へのヒアリングで得た意見、事業期間中開催された TF 等の議論の内容を反映して「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集」としてまとめた。

No	事業項目	仕様書の内容	具体的な実施内容
		また、上記調査の結果及び3⑥に示すTFでの議論の内容について、サイバー空間におけるつながりの信頼性及びIoT機器等の転写機能の信頼性を確保するための具体的なセキュリティ対策要件等を今後策定していく上での現状と課題等を整理し、調査報告書にまとめる。 なお、調査報告書の具体的な内容については担当者と協議の上で決定するが、例えば、以下に示す論点を含むこととする。 ＜調査報告書における論点の例＞ ●データやIoT機器等の区分（カテゴリ）に関する考え方 ●上記の区分に沿ったセキュリティ対策例 ●上記の区分に沿ったデータやIoT機器等の信頼性の確認方法 ●データマネジメントの考え方 【実施方法】 ・ 公開情報（外国政府・国際標準化団体の報告資料、国内外の専門誌等を含む。）、国内外のニュース記事、商用データベース等の調査により実施する。調査結果の妥当性確認などを目的として、必要に応じてデータやIoT機器等のセキュリティに精通した有識者（国外の有識者を含む3名程度）に対して面談によるヒアリングを実施することが望ましい。ただし、国外の有識者に対しては電話又はテレビ会議によるヒアリングでもよい。 ・ 日本に加えて、少なくとも米国、欧州を調査対象の国・地域に含め、3つ以上の国・地域の調査を行う。また、外国語の調査結果や報告資料は日本語に翻訳する。 ・ 調査の際は、CPSFの関係項目や国際動向とのハーモナイゼーションを常に考慮しながら、データやIoT機器等の区分（カテゴリ）及びそれらに応じたセキュリティ対策例や信頼性の確認方法や、データマネジメントの考え方等について整理を行うこと。	サイバー空間におけるつながりの信頼性を確保するために求められる標準化団体、業界団体及び外国政府の取り組み等やデータのセキュリティ対策等について、日本、米国、欧州、中国の公開情報等を調査し整理した。 また、事業期間中 2 回実施したパブリックコメントでいただいた意見、社内有識者へのヒアリングで得た意見、TF 等での議論の内容を反映し、「協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ」としてまとめた。
2	CPSF 等に基づく国際規格（TR 等を含む。）の推進	【事業内容】 本事業では、日本企業の競争力強化に寄与する国際的なルールを形成していくことを目的とし、ルール形成を構成する一要素になりうるCPSF等をベースにした国際標準化を推進する。具体的には、サプライチェーン全体のサイバーセキュリティ確保に求められるリスク管理、リスク評価、セキュリティ対策に関する、諸外国の政府又は政府関連機関、業界団体のルール形成の取り組み状況や、標準化機関における標準化の動向等を調査しつつ、サイバーセキュリティに関する国際的なフレームワークについて、CPSF等の考え方をベースにしたものが採用されるよう必要な働きかけ・検討を行う。 想定する調査項目例を以下に示すが、具体的な調査項目については、担当者と協議の上で決定する。 なお、有識者等との議論等によって新たな視点での調査の必要性が生じた場合は、追加的に調査を行うこと。 ＜想定する調査項目の例＞ ●CPSF等に基づく国際規格（TR等を含む。）策定に向けた具体的なロードマップの提示 ●上記ロードマップに基づく、国内外の関係機関・関係者の巻き込みやそのために必要な資料の作成等の実施 ●CPSF等に基づく国際規格（TR等を含む。）策定に向けたドラフト文書の作成、及び国内外の関係機関・関係者との意見交換	CPSFをベースにした国際標準化を推進することを目的として、推進に必要な諸外国の政府又は政府関連機関、業界団体、標準化団体等によるルール形成の取り組み状況等の調査や、ISO/IEC及びそれに関連する会議等における必要な働きかけの実施、CPSF等に基づく国際規格（案）の作成等を実施した。具体的には、国際規格策定に向けた検討のロードマップを策定し、適宜必要な文献調査等を実施しつつ、サイバーセキュリティに関する国際規格の策定や維持管理を担うISO/IEC JTC 1/SC27/WG 4(セキュリティコントロールとサービ

No	事業項目	仕様書の内容	具体的な実施内容
		を踏まえたドラフト文書の更新 ●米欧の公的機関又は国際標準化機関において策定された、あるいは策定が進むサプライチェーンのサイバーセキュリティ確保を目的としたリスク評価、リスク管理、セキュリティ対策、セキュリティ評価・認証等に関係する国際規格、ガイドライン、フレームワーク、政策文書等の調査 上記調査は、文献（国内外の公的機関や標準化機関の公表資料、国内外の専門誌等）、インターネット、意見交換等により実施する。意見交換の対象の国内外の公的機関・有識者・組織や意見交換の内容は実施者が提案することし、サイバーセキュリティ課と協議の上、決定する。また、必要に応じて国際会議（ISO Meetings等。対面での会議を2回程度、その他複数回の電話会議等を想定。）に参加し、日本のCPSFに基づくセキュリティ対策の考え方について諸外国の公的機関と意見交換等を行い、CPSF等に基づく国際規格（TR等を含む。）標準化を推進すること。加えて、当該意見交換等については、関連するISO/IECの日本のエキスパート等と協力し、可能な限り効果的な方法で行うこと。 なお、意見交換を英語で行った場合には、議事概要は日本語に翻訳すること。 【実施方法】 ・ 公開情報（外国政府・国際標準化団体の報告資料、国内外の専門誌等を含む。）、国内外のニュース記事、商用データベース等の調査により実施する。調査結果の妥当性確認などを目的として、必要に応じてセキュリティの国際標準に精通した有識者（国外の有識者1名以上を含む、3名以上）に対して面談によるヒアリングを実施することが望ましい。ただし、国外の有識者に対しては電話又はテレビ会議によるヒアリングでもよい。また、必要に応じて国際会議（ISO Meetings等。対面での会議を2回程度、その他複数回の電話会議等を想定。）に参加することが望ましい。 ・ 日本に加えて、少なくとも米国、欧州を調査対象の国・地域に含め、3つ以上の国・地域の調査を行う。また、外国語の調査結果や報告資料は日本語に翻訳する。 ・ CPSF等に基づく国際規格（TR等を含む）策定に向けた活動は、ISO/IECの日本のエキスパート等と協力しながら進める。	ス)の国内エキスパートと連携して本件に係る国際規格策定プロジェクトの提案及びPWI(予備業務項目)、NWIP(新規作業項目提案)としてのプロジェクト推進、その他必要に応じて国内外の関係者との意見交換を行った。
3	研究会、各 WG、分野横断SWG及び TF の運営	【事業内容】 本事業では、上記1の調査及び検討に関連して、専門的な視点からの検討、分析及び助言を得るために、以下①から⑥までに示す研究会、各WG、分野横断SWG及びTF（以下、①から⑥までをまとめて「研究会等」という。）を以下の要領にて運営する。 研究会等の構成及び構成員については、別紙を参照すること。 なお、これまでの開催実績を基に別紙を作成しているため、令和3年度においては肩書きや構成員の変更が生じる可能性があることに留意すること。 ①産業サイバーセキュリティ研究会 大所高所から政策や産業界の取り組みを議論する。研究会の構成員（10名程度）は、産学を代表する有識者とし、担当者が指定する。令和3年度中に3回程度開催する。 ②WG1（制度・技術・標準化）	研究会、WG 及び 2 つの TF（『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース（第 2 層 TF）、『第 3 層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース（第 3 層 TF）、について、構成員との日程調整、開催案内（出欠確認）、資料準備等といっ

No	事業項目	仕様書の内容	具体的な実施内容
		制度、技術、標準化の関連政策を一体的に政策展開する戦略を議論する。WGの構成員（15～20名程度）は、産学の有識者とし、担当者が指定する。令和3年度中に2回程度開催する。 ③WG2（経営・人材・国際） サイバーセキュリティ政策全体の共通基盤となる経営・人材・国際戦略を議論する。WGの構成員（10～15名程度）は、産学の有識者とし、担当者が指定する。令和3年度中に3回程度開催する。 ④WG3（サイバーセキュリティビジネス化） セキュリティサービス品質向上と国際プレイヤー創出に係る政策を議論する。WGの構成員（10～15名程度）は、産学の有識者とし、担当者が指定する。令和3年度中に3回程度開催する。 ⑤分野横断SWG WG1の下に設置し、産業分野に共通する課題について議論する。WGの構成員（15～20名程度）は、産学の有識者とし、担当者が指定する。令和3年度中に2回程度開催する。 ⑥特定課題の検討TF 2つのTFにおいて1の調査結果に基づいて、サイバー空間におけるつながりの信頼性及びIoT機器等の転写機能の信頼性を確保するための対策要件等を議論する。各TFの構成員（15名程度）は、産学の有識者とし、担当者が指定する。令和3年度中に各TF3回程度開催する。 なお、産業分野別 SWG の運営は、他の委託事業や他府省庁、民間団体等において実施されているため、本事業の対象外とする。 【実施方法】 ・ 研究会等の開催に当たっては、構成員との日程調整、開催案内（出欠確認）、会場確保（基本的に経済産業省又は経済産業省近郊で開催する。経済産業省以外の会場は、委託先において確保する。Web開催の場合は、経済産業省が指定するオンライン会議システムにより会議を主催する。）、資料準備（印刷等含む。）、会議の議事録の作成（研究会等の開催後に速やかに作成し、経済産業省に対して提出する。）等といった事務的な業務を全て行う。加えて、令和2年度に開催した研究会等に関する事務的な業務を事後的に実施する必要がある場合、経済産業省担当者の指示に基づき行う。 なお、実施に係る経費については事業費に計上する。 ・ 3⑥のTFのうち、1の調査に基づく議論を行うTFにおいては資料の作成及び報告を行う。 ・ 研究会等の資料のうち、国際ハーモナイゼーション及び我が国の取り組みの海外発信の観点に基づき、経済産業省担当者が指示する資料について英訳を行う。	た事務的な業務を全て行った。 また、第 2 層 TF 及び第 3 層 TF において、資料の作成及び経済産業省担当者への報告を行った。

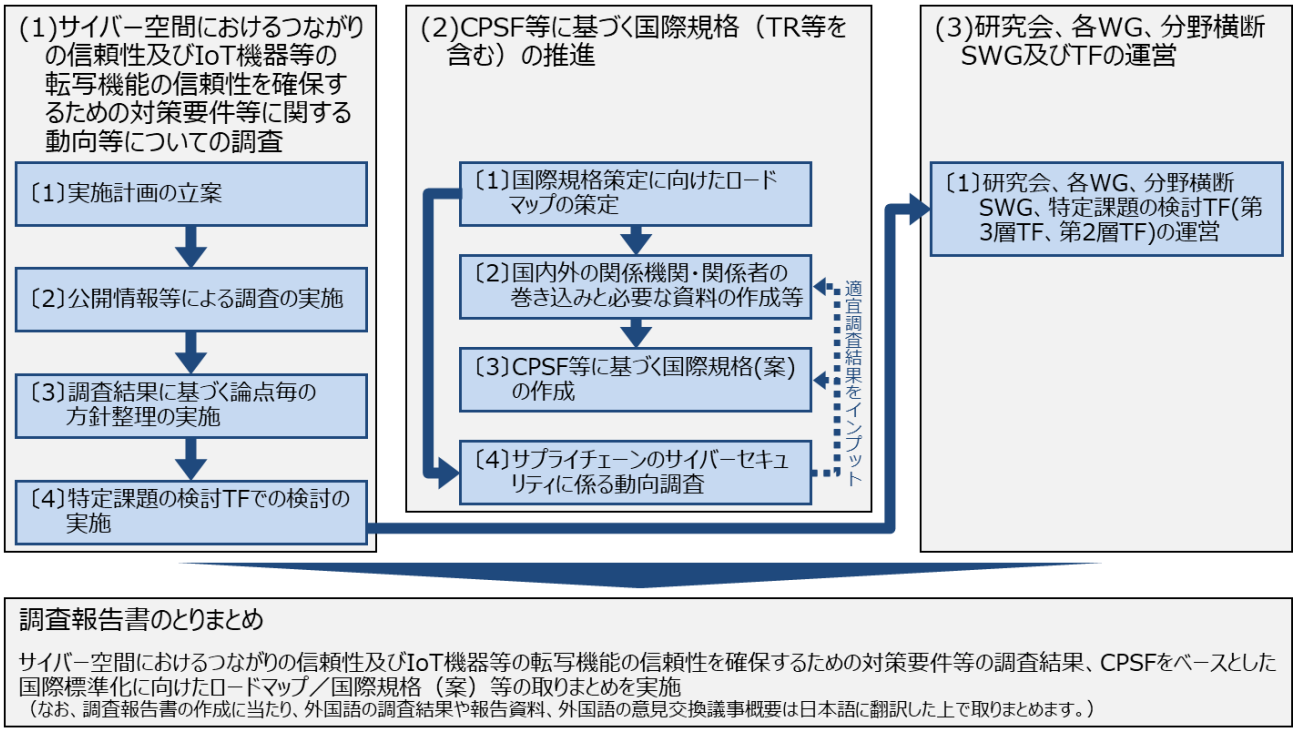


図 1-1 具体的な実施内容の全体像

1.3 実施スケジュール

本事業の実施スケジュールを図 1-2 に示す。「サイバー空間におけるつながりの信頼性を確保するための対策要件及び対策水準に関する動向等についての調査」、「フレームワークの課題整理」について、産業サイバーセキュリティ研究会、WG、検討 TF における検討や助言を踏まえて検討を推進した。

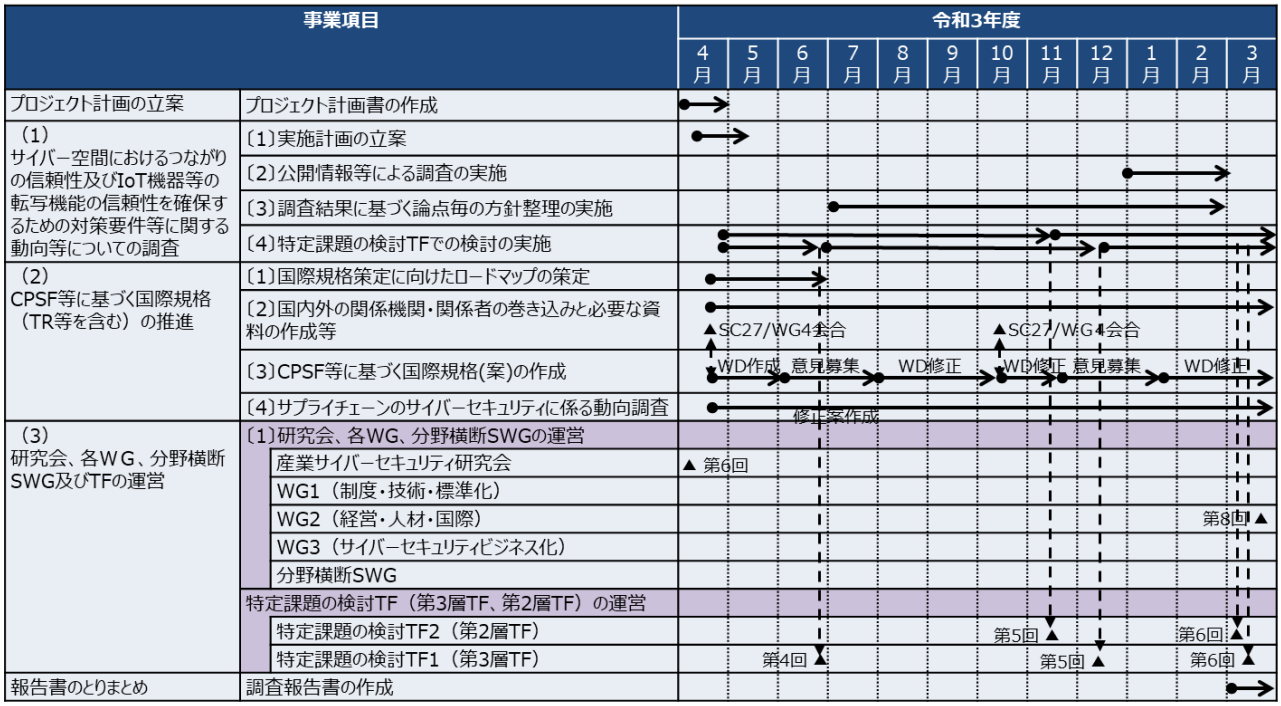


図 1-2 本事業の実施スケジュール

1.4 実施体制

本事業は、プロジェクトオーナーである経済産業省商務情報政策局サイバーセキュリティ課と委託事業者が、事業項目(1)と事業項目(2)について検討・協議を実施するとともに、その内容に関して産業サイバーセキュリティ研究会の研究会等における検討や助言を踏まえながら推進した。本事業の実施体制を図 1-3 に示す。

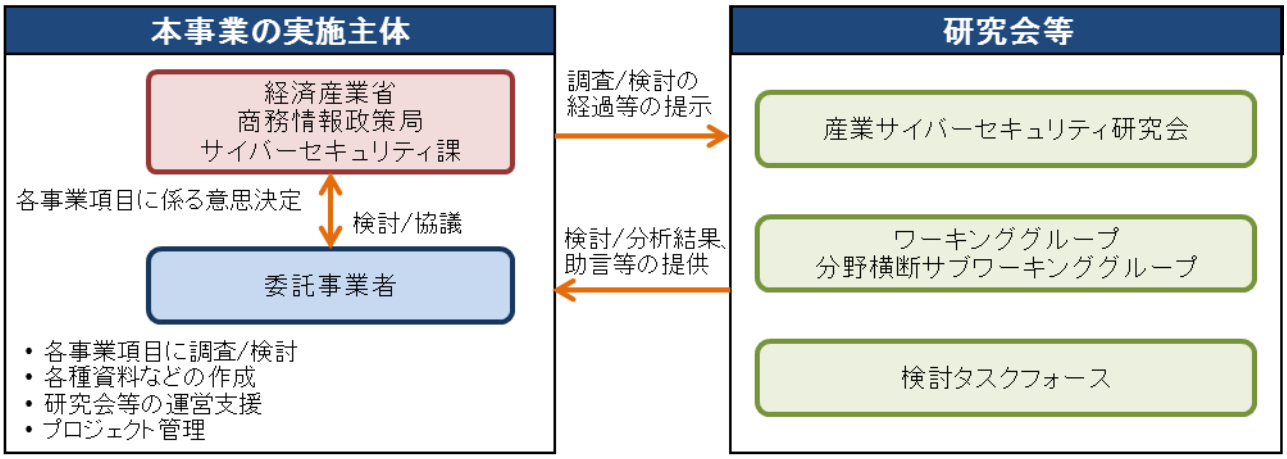


図 1-3 本事業の実施体制

1.5 本調査報告書の構成

本調査報告書では、「サイバー空間におけるつながりの信頼性及び IoT 機器等の転写機能の信頼性を確保するための対策要件等に関する動向等についての調査」と「CPSF 等に基づく国際規格(TR 等を含む。)の推進」について、それぞれ目的、実施内容、実施結果を報告する。

- 第 2 部では、「サイバー空間におけるつながりの信頼性及び IoT 機器等の転写機能の信頼性を確保するための対策要件等に関する動向等についての調査」の目的、実施内容、実施結果を報告する。
- 第 3 部では、「CPSF 等に基づく国際規格(TR 等を含む。)の推進」の目的、実施内容、実施結果を報告する。

2　サイバー空間におけるつながりの信頼性及び IoT 機器等の転写機能の信頼性を確保するための対策要件等に関する動向等についての調査

2.1 IoT 機器等の転写機能の信頼性を確保するための対策要件等に関する動向等についての調査

2.1.1 本事業項目の目的

本事業項目では、IoT 機器等の転写機能の信頼性を確保するため、転写機能を担う IoT 機器等の多様性やインシデントが発生した場合の被害の複雑化等も踏まえて、IoT 機器等に求められるリスクアセスメントの考え方やセキュリティ対策等について整理することを目的とした。

2.1.2 本事業項目の実施内容

上記目的を達成するため、IoT 機器等の転写機能の信頼性を確保するために求められる標準化団体、業界団体及び各国政府の取り組み等や IoT 機器等のセキュリティ対策、及びそれらの信頼性の確認手法等について、公開情報等を調査し整理した。

また、事業期間中に開催された TF や WG 等での議論を踏まえて、IoT 機器等の転写機能の信頼性を確保するための具体的なセキュリティ対策要件等を今後策定していく上での現状と課題等を整理した。

さらに、今後様々な分野/業界のプレイヤーが、IoT-SSF を「基本的共通基盤」として活用するために、既存のリスクマネジメントのプロセスも考慮しつつ、一連の IoT-SSF の適用の流れを複数のユースケースを用いて例示するユースケース集を検討し、事業期間中開催された TF 等の議論の内容を反映して、「IoT セキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集」[2]としてまとめた。

2.1.3 本事業項目の実施結果

(1) 公開情報等の調査

本事業の調査対象を表 2-1 に示す。令和 2 年度事業以前に調査を行っている一部文書を除いて、詳細な調査結果を別紙 1 に示す。

調査結果のサマリについては、地域(欧州、米国、日本及びその他地域)ごとに整理して以下に示す。

- 欧州では、「Cybersecurity Act」(2019 年 6 月)の施行によって、「Cybersecurity Certification: Candidate EUCC Scheme V1.1.1」(2021 年 5 月公表)を含む認証制度の具体化が進められている。2022 年 3 月現在、3 つ(「Cybersecurity Certification: Candidate EUCC Scheme V1.1.1」(2021 年 5 月公表)、「EUCS-CLOUD SERVICE SCHEME」(2020 年 12 月公表)、「candidate European cybersecurity certification scheme for 5G networks[a]」(策定中))の候補スキームが検討されている。また、既に発行されている NLF 関連指令(例:機械製品指令、一般製品安全指令)についても、欧州委員会等にて議論が進められ、サイバーセキュリティの要素を追加した草案が提案されており、機会製品指令は 2021 年 4 月に、一般製品安全指令は 2021 年 6 月に、それぞれ「指令」を域内で直接適用する「規則」に置き換える提案がなされている。

[a] 2021 年 6 月、アドホックワーキンググループの公募を実施し、「candidate European cybersecurity certification scheme for 5G networks」の検討が行われている。

表 2-1 調査対象一覧

No	国	文書名	別紙 1 に調査結果を示した文書
1	欧州	Cybersecurity Act	
2		Cybersecurity Certification: Candidate EUCC Scheme V1.1.1	
3		EUCS – CLOUD SERVICE SCHEME	
4		2018 Code of Practice for Consumer Internet of Things Security	
5		Product Security and Telecommunications Infrastructure Bill	○
6		ETSI EN 303 645 V2.1.1	○
7		ETSI TS 103 701 V1.1.1	○
8		Guidelines for Securing the Internet of Things	○
9		Recommendations for the security of CAM[b]	○
10	米国	Executive Order on Improving the Nation's Cybersecurity	
11		Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products	
12		Recommended Criteria for Cybersecurity Labeling of Consumer Software	
13	日本	電気通信事業法	
14		IT セキュリティ評価及び認証制度（JISEC）	
15		IoT セキュリティ・セーフティ・フレームワーク	
16	中国	サイバーセキュリティ法	
17	シンガポール	Cybersecurity Certification Guide	○

・ 英国では、「2018 Code of Practice for Consumer Internet of Things Security」（2018 年 10 月施行）や「ETSI EN 303 645」（2020 年 6 月公表）等をベースとして、2021 年 11 月より IoT 機器に一定のセキュリティ対策を義務付ける法案である「Product Security and Telecommunications Infrastructure Bill」の審議が行われている。

・ 英国を含む欧州では、認証制度の枠組みに関する検討が進められつつ、それと並行してセキュリティ機能の実装を強制する法案が審議されていることから、IoT 機器・システムのセキュリティに関するルールとして、セキュリティ標準の策定以外の規制や認証といった文脈でも具体化されつつあると言える。

・ 米国では、2021 年 5 月にバイデン大統領が「Executive Order on Improving the Nation's Cybersecurity」に署名し、当該大統領令の第 4 節に規定された商務省及び国立標準技術研究所(National Institute of Standards and Technology: NIST)に対する指示事項に基づいて、「Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products」（2021 年 8 月）や「Recommended Criteria for Cybersecurity Labeling of Consumer Software」（2022 年 2 月）等が公表されている。アプローチに差異はあるが、欧州と同様に米国においても、IoT セキュリティに関する認証/ラベリングやソフトウェアサプライチェーン SBOM 等の IoT セキュリティに関するルールが具体化されつつある。

・ 日本では、IoT セキュリティに関連する既存の制度として、特定の条件下で稼動する IoT 機器等に対してセキュリティ対策の準拠を求める電気通信事業法（2021 年 4 月改正）が施行されている他、IT 機器のセキュリティ認証制度として、IT セキュリティ評価及び認証制度が存在している。一方で、これらの制度には、カバーしている範囲が限定的、IoT 機器を対象とする場合に対応コスト(例：金銭、時間)がかかりすぎる等の課題が想定される。

・ より IoT に特有な事情を広範に勘案したものとしては、本事業に関連して 2020 年 11 月に

[b] CAM: The Connected and Automated Mobility

「IoT セキュリティ・セーフティ・フレームワーク」(以下、「IoT-SSF」という。)を公表し[2]、IoT セキュリティに関するルールの更なる具体化に向けて検討を進めている。

	米国における検討状況 (連邦政府で議論されているもの)	EUにおける検討状況 (EU単位で議論されているもの)	日本政府の検討状況 (主にIoT機器・システムの認定に係るもの)
主な法令等	国家サイバーセキュリティの向上に関する大統領令 (Executive Order 14028)	サイバーセキュリティ法(CSA) NLF関連指令/規則 (例：機械規則案)	電気通信事業法 上記のほか、IT関連製品を対象にした認証制度として、ITセキュリティ評価及び認証制度(JISEC)等が存在する。
適用対象	消費者向けのIoT製品 IoT製品には、IoT機器に加え、機器の利用に必要な製品コンポーネント(ネットワーク機器、モバイルアプリ等)を含み得る。	製品分野等により異なる 機械規則や無線指令等の各NLF関連指令/規則に規定が設けられており、現状は垂直的な規制が議論されている。	インターネット等に接続する端末機器 ルータ、ウェブカメラ等が該当し、IPを使用しない機器やインターネット等に直接接続しない機器は含まれない。
セキュリティ基準	消費者向けIoT製品のサイバーセキュリティ・ラベリングのための推奨基準 現行案はNISTIR 8259シリーズをベースに策定されている。	製品分野等により異なる 機械規則や無線指令等の各NLF関連指令/規則に規定が設けられており、現状は垂直的な規制が議論されている。	端末設備等規則 必ずしも機器・システム等の認定に関わらないものとしては、IoTセキュリティガイドライン、CPSF/IoT-SSF等が存在する。
事業者の義務等	現状では必ずしも議論されていない NISTは、政府主導の認証・ラベリング制度ではなく、今後制度を開発する主体が参照するものを志向している。	NLF関連指令/規則を通じて義務化される見込み	技術基準適合認定が求められる場合等を除けば、必ずしも対策は義務とされていない。
今後の予定	• 2022年5月12日までに、NISTは、上記検討に関する総括報告書を発行する予定。 • 上記報告書の公開後、基準に基づく認証制度の検討が推進される見込み。	• EUCC等、CSAに基づく認証制度の具体化が進む見込み。また、草案が公開されているNLF関連指令/規則は、順次欧州議会等で議論が進められる。 • 2022年下期に、水平的なセキュリティ基準の確立を志向する「サイバーレジリエンス法」公表を予定。	• (IoTを対象にした具体的な認証・ラベリング等の議論はなされていないという認識)

図 2-1 IoT 機器・システムのセキュリティに係る日米欧の制度化動向

日本以外のアジア地域においても、中国ではネットワーク事業者などの法的義務と責任等を規定するサイバーセキュリティ法(2017 年 6 月)が施行されたことによって、IoT 機器事業者へ影響が懸念されている。また、シンガポールではサイバーセキュリティ・ラベル制度に関する文書である「Cybersecurity Certification Guide」が公表されており、IoT 機器のラベリングに関する議論が進められている。したがって、欧州や米国以外のアジア地域においても、IoT 機器・システムのセキュリティを強化するための強制を伴う、もしくは事業者の自発的な取り組みを促すルール形成が進められており、IoT セキュリティに関する技術要件だけでなく、それらを活用した適合性評価やラベリングに関する議論が欧州や米国に留まらず、広く進められている。

(2) IoT セキュリティ・セーフティ・フレームワーク実践に向けたユースケース集の作成

2020 年 11 月に公表された IoT-SSF は、サイバー空間とフィジカル空間をつなぐ新たな仕組みによってもたらされる新たなリスクに着目し、リスク形態及びそうしたリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示するものである。

昨年度開催された第 4 回第 2 層 TF[3]では図 2-3 に示す通り、IoT-SSF には抽象度が高い部分が含まれており、読者にとって理解が難しい部分がある可能性があるとの声が寄せられた。そのため、具体的な事例を IoT-SSF に当てはめた「IoT セキュリティ・セーフティ・フレームワーク実践に向けたユースケース集」(以下、「ユースケース集」という。)を作成することとなった。

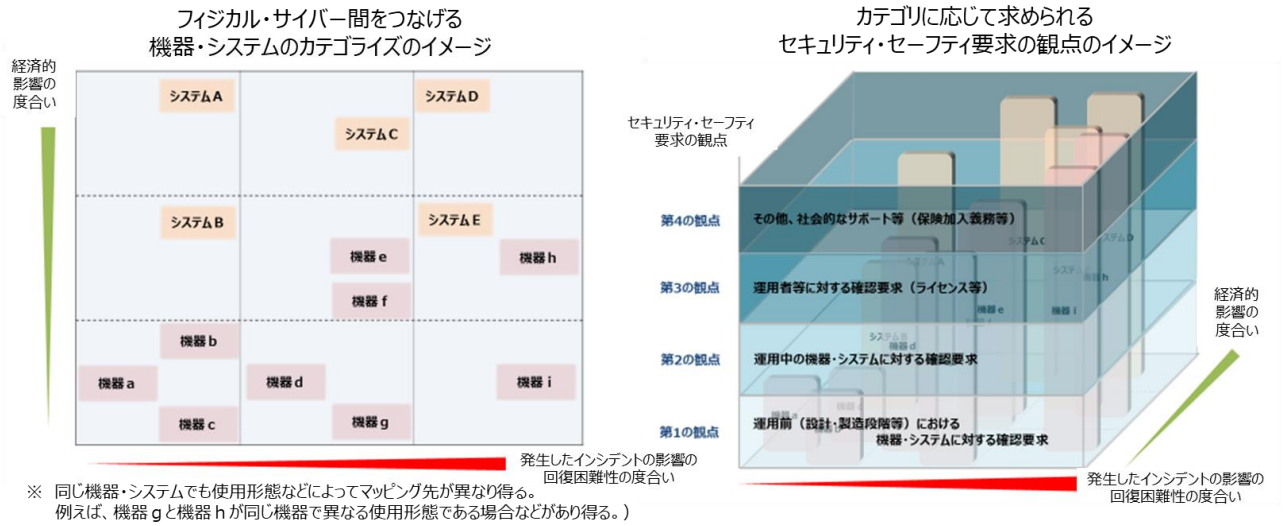


図 2-2 IoT-SSF の概要

<寄せられたご意見>

- IoT-SSFがIoT機器・システムのセキュリティに係る様々な主体に適用可能な「基本的共通基盤」を提供していることを評価する。
- 一方で、IoT-SSFには抽象度が高い部分も含まれているため、読者にとって理解が難しい部分がある可能性がある。
- IoT-SSFにて示されたリスクのマッピング手法やカテゴライズ手法に関する指針もしくはガイドラインの整備が必要ではないか。

<本文での記載>

- 今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースとして整理していくことで、IoTが広く活用されるサイバー空間とフィジカル空間が高度に融合した社会におけるセキュリティ・セーフティ対策を適切に実施していく制度的対応の整備を進めていくための基礎的条件を整えて行く必要がある。

図 2-3 第 4 回第 2 層 TF にて寄せられたご意見

ユースケース集では、今後様々な分野/業界のプレイヤーが、IoT-SSF を「基本的共通基盤」として活用するために、既存のリスクマネジメントのプロセスも考慮しつつ、一連の IoT-SSF の適用の流れを複数のユースケースを用いて例示した。なお、本ユースケース集の想定読者は以下に示すものとし、IoT 機器・システム及び関連サービスに係る様々な主体（事業者）により活用されることを想定した。

- IoT 機器・システムを通じて提供されるサービスのユーザー（IoT 利用者）
- IoT 機器・システムを通じて提供されるサービスの開発者（IoT サービス開発者）
- IoT 機器・システムを通じて提供されるサービスの提供者（IoT サービス提供者）
- IoT 機器・システム及び関連サービスを適切に管理する制度・環境を検討する者

ユースケース集では、1 章を導入として、2 章ではユースケース選定の考え方、各ユースケースに共通する記載項目、6 件の具体的なユースケースを記述している。IoT-SSF のユースケース集にて詳述するユースケースは、以下に示す通りである。詳細については、別紙 3 及び別紙 4 を参照されたい。

① 家庭用ガス給湯器の遠隔操作
② ドローンを活用した個人による写真撮影
③ 物流倉庫内の AGV による自動ピッキング
④ 化学プラント施設内の蒸留工程の自動制御
⑤ 工場内のロボットによる部材加工作業(溶接工程)の自動化
⑥ 金属製造現場の温度センサ等による製造設備の状態監視

本事業期間中に令和 3 年 11 月に第 5 回第 2 層 TF、令和 4 年 3 月に第 6 回第 2 層 TF が開催され[4,5]、ユースケース集について各委員からコメントを頂戴した。表 2-2 に第 2 層 TF にて頂戴した主な意見を示す。

表 2-2 第 2 層 TF にて頂戴した主なご意見

No	TF	主なご意見
1	第 5 回 (令和 3 年 11 月 29 日開催)	ユースケースの記述様式について、誰の視点のリスクかを明確にしていく必要がある。
2		事業者個別に実施すべき発展的なレベルの取り組みに関する示唆も必要である。
3		十分なコミュニケーションが図られておらず、責任の所在が曖昧となっているケースがあるため、ステークホルダー間でコミュニケーションを十分に行う必要がある旨を記載してはいかがか。
4	第 6 回 (令和 4 年 3 月 9 日開催)	自分事に感じてもらうには、どの部署の人がリスクを感じないといけないのかがわかるようになっているとよいと感じる
5		第 3 軸について、第 3 の観点、第 4 の観点を踏まえたユースケースの拡充を期待する。
6		メーカーとしてどこまで対策を実装すべきか、どこから免責されるのかという点を切り分けていかないといけない。最低限どこまで実装すればよいかの基準を示していただきたい。
7		民間事業者自身がアセスメント等を実施することは非常に重要なため、何らかのインセンティブがあるとよい

(3) 今後の方向性について

- 欧米もしくは一部のアジア諸国では IoT セキュリティに関する技術要件の策定だけでなく、それらを活用した適合性評価やラベリングに関する議論が進められており、これらの流れは今後更に加速する可能性がある。日本においても IoT セキュリティに関する制度やルールに関する議論を深化させ、例えば、IoT 機器・システムに関する検証サービスの仕組みや、IoT 機器・システムを検証するための基準を具体化させていくことが望まれる。
- IoT-SSF のユースケース集の今後の取り組みとしては、第 2 層 TF に参画している委員が所属する団体や業界への紹介や経済産業省主催の講演会等での紹介等、IoT-SSF 及びユースケース集の普及啓発活動を進めていく等、普及啓発活動を行うにあたっての方策を検討することが有効と考える。
- 事業者による IoT-SSF の自立的な活用に向けて、第 6 回第 2 層 TF にて寄せられたご意見の通り、IoT 機器・システムの更なるセキュリティ強化に向けては、事業者の自発性に依拠する施策のみならず、インセンティブ付与や規制化等の措置を実施することも有効であると考えられる。
- その際、全ての IoT 機器を同一の制度の対象とすることは現実的ではないとも考えられるため、まずは、対象となる IoT 機器の重要度やそれらを対象にし得る既存の法制度(例:電気用品安全法、消費生活用製品安全法、医療品医療機器等法)における分類等に応じて機器やそれらを含んだシステムを分類し、各々の枠組みにおいて必要な措置及び、それら複数の枠組みにおいて共通に必要とされる措置を検討することも有効であると考えられる。

2.2 サイバー空間におけるつながりの信頼性を確保するための対策要件等に関する動向等についての調査

2.2.1 本事業項目の目的

本事業項目では、サイバー空間におけるつながりの信頼性を確保するため、産業活動におけるデータの区分やデータ利活用の実態を踏まえた上で、より具体的な対策要件やデータの完全性や真正性を確認する仕組みとしてどのような手法やルールが効果的か、その実効性や国際的な動向も踏まえた上で更なる検討が必要となっているため、データマネジメントにおけるモデルの具体化にあたり、必要となる情報を整理することを目的とした。

2.2.2 本事業項目の実施内容

上記目的を達成するため、サイバー空間におけるつながりの信頼性を確保するために求められる標準化団体、業界団体及び各国政府の取り組み等やデータのセキュリティ対策及びそれらの信頼性の確認手法等について、公開情報等を調査し整理した。

また、事業期間中に開催された TF や WG 等での議論を踏まえて、データのセキュリティ対策要件等を今後策定していく上での現状と課題等を整理した。

さらに、事業期間中 2 回実施したパブリックコメントでいただいた意見や、TF 等での議論の内容を反映し、「協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ」としてまとめた。

2.2.3 本事業項目の実施結果

(1) 公開情報等の調査

本事業の調査対象を表 2-3 に示す。令和 2 年度事業以前に調査を行っている一部文書を除いて、詳細な調査結果は別紙 2 に示す。

表 2-3 調査対象一覧

No	国	文書名	別紙 2 に調査結果を示した文書
1	欧州	General Data Protection Regulation	
2		The regulation for the free flow of non-personal data in the European Union	
3		Technical Overview: Secure cross-company communication	○
4	米国	Electronic Communications Privacy Act of 1986	
5		Gramm Leach Bliley Act	
6		Health Insurance Portability and Accounting Act	
7		California Consumer Privacy Act of 2018	
8		Consumer Data Protection Act21	
9		Colorado Privacy Act22	
10		Export Control Reform Act of 2018	
11		CLOUD SECURITY TECHNICAL REFERENCE ARCHITECTURE	○
12		SP 800-47 Rev.1 Managing the Security of Information Exchanges	○
13		Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward	○
14	日本	協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ (旧　データによる価値創造(Value Creation)を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク(仮))	
15	中国	サイバーセキュリティ法	○
16		データセキュリティ法	○
17		データ域外移転のセキュリティ評価に関する弁法	○
18		個人情報保護法	○

No	国	文書名	別紙 2 に調査結果を示した文書
19	国際機関	Data Protection Best Practices	○

調査結果のサマリについては、地域（欧州、米国、日本及びその他地域）ごとに整理して以下に示す。

・ 欧州では、2018 年 5 月に施行された General Data Protection Regulation（GDPR）によって個人情報の保護に関するルールが EU 域内で統一された。GDPR においては、個人データを管理者又は処理者が取扱う際の原則や個々の規則に加え、第三国に対する European Economic Area（EEA）域外への個人データの移転及び第三国から別の第三国への個人データの移転を規律しており、GDPR を遵守したデータ(越境)移転のみが許容された。また、一般データ保護規則（GDPR）の対象外である非個人データについても、域内における自由流通を促進することを目的として、2018 年 11 月に「The regulation for the free flow of non-personal data in the European Union」が施行されているが、欧州としては、個人のデータ保護を目的としたルール形成に重点が置かれている。

・ 米国では、個人データ保護に関する包括的な連邦法は存在しないものの、個別法として 1986 年 10 月に通信分野を対象とした「Electronic Communications Privacy Act of 1986（ECPA）」、1999 年 11 月に金融分野を対象とした「Gramm Leach Bliley Act（GLBA）」及び 1996 年 8 月に医療分野を対象とした「Health Insurance Portability and Accounting Act（HIPAA）」が施行されている。また、カリフォルニア州（California Consumer Privacy Act of 2018（2020 年 1 月））及びコロラド州（Colorado Privacy Act22（2021 年 7 月））等プライバシーの保護を目的とした個別の州法が施行されている。

・ 個人データの保護を目的としたもの以外では、国家安全保障の観点から、「Export Control Reform Act of 2018」（2018 年 8 月）が定めてられている。下位規則である輸出管理規則では、製品の「開発」、「製造」又は「使用」に必要となる特定の情報等が米国人から非米国人に対して米国内で開示される場合に、みなし輸出と判断し、これらを輸出管理の対象としている。輸出管理の対象とされた場合には、例えば、米国内であっても輸出許可が必要となる。

・ 米国において、個人データ保護に関する連邦レベルでの包括的なルールは存在していないものの、分野や州単位でルール形成が進んでいる。また、国家安全保障の観点から非個人情報に関するルールも整備されている。

・ 日本では、2019 年 1 月のダボス会議及び同年 6 月の G20 大阪サミットにて、新たな価値の源泉であるデータが自由で信頼性が担保された枠組みで流通することが経済成長をもたらすとの考えの下、信頼性のある情報の自由かつ安全な流通の確保を図ることを目的として、Data Free Flow with Trust（DFFT）が提唱されている。DFFT は上記会合後もデータ戦略に考え方が盛り込まれる等、様々な機関により取り組みが推進されている。その中のひとつとして、後述の「協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ」（以下、「フレームワーク」という。）の作成や「データの越境移転に関する研究会」での検討が進められている。

・ 日本以外のアジア地域では、中国において、2017 年 6 月に「中国サイバーセキュリティ法」、2021 年 9 月に「データセキュリティ法」、2021 年 11 月に「個人情報保護法」が施行されている。また、これらの法律に関連して、2021 年 9 月に「重要情報インフラセキュリティ保護条例」や 2021 年 10 月に「自動車データセキュリティ管理若干規定」が施行されている。

・　中国においては個人を含めた権利の保護に加えて、国家安全保障の観点から、個人データや重要データを含むデータ保護に関するルール形成が、枠組み作りのみならず詳細な要求事項等のレベルに至るまで急速に進められている。

対象や個別の規定の違いはあるものの、データ保護に関する規定を含むルール形成が欧州、米国及びアジア地域で進んでいると言える。ただし、欧州では個人情報保護に重点を置いていることに対して、米国や中国においては、個人の権利の保護に加えて、国家安全保障の観点からルール形成が進められている。

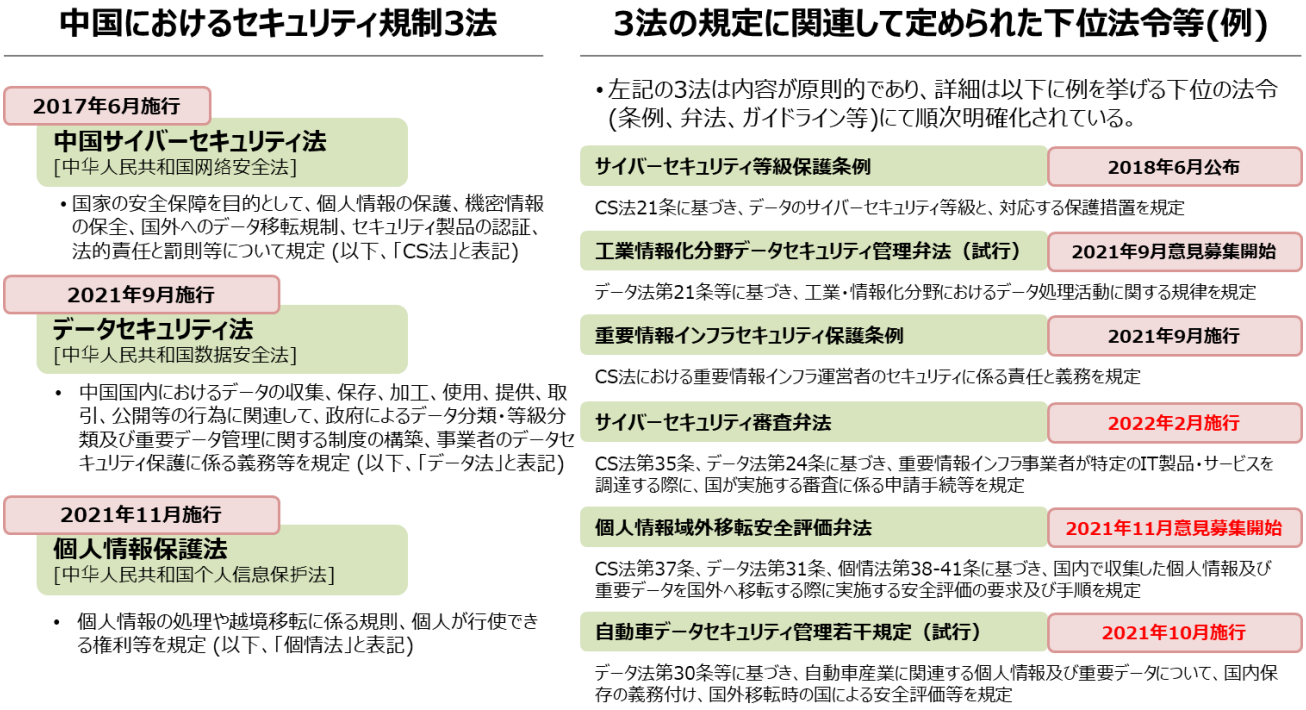


図 2-4　中国におけるセキュリティ規制法等

(2)「協調的なデータ利活用に向けたデータマネジメント・フレームワーク～データによる価値創造の信頼性確保に向けた新たなアプローチ」の作成

主体間を転々流通するデータの信頼性を確保することで、バリュークリエイションプロセスが付加価値を生み出していくために、データを軸に置き、データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し、そのセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することを目的として、フレームワークを作成した[6,10]。フレームワークの想定読者は下記に示す。

- バリュークリエイションプロセスに参加する者
- データ利活用に関するサービスを提供する者
- データ利活用に関するサービスを提供するシステムの設計・構築・運用に関わる者
- トラストサービスを提供しようとする者
- データセキュリティに関わるガイドライン等のルール設定に関わる者

フレームワークでは、1 章を導入として、2 章では本フレームワークにおけるデータマネジメントのモデルを紹介し、3 章ではこれらのモデルの活用方法を記述している。また、添付資料では、モデルを個別の事例に当てはめたユースケース(添付 A)やイベントごとのリスクの洗い出しのイメージ(添付 B)を記述している。詳細については、別紙 5 及び別紙 6 を参照されたい。

2 章では、データマネジメントを「データの属性が場におけるイベントにより変化する過程を、ライフサイクルを踏まえて管理すること」と定義し、「場」、「属性」、「イベント」からなるモデルで説明している。フレームワークでは、この 3 つの要素を使ってデータの置かれた状態を可視化することにより、データに対してどのようなリスクが存在し、それに対してどう対処すべきか、ということを明確にすることができるとした。

フレームワークでは、下記に示す 4 つのステップに沿ってバリュークリエイションプロセスにおけるデータの状態を可視化することで、データに関わるリスクの洗い出しと対応策の整理を実施することが可能となるとした。

- STEP 1:データ処理フロー(「イベント」)の可視化
- STEP 2:必要な制度的な保護措置(「場」)の整理
- STEP 3:「属性」の具体化
- STEP 4:「イベント」ごとのリスクポイントの洗い出し

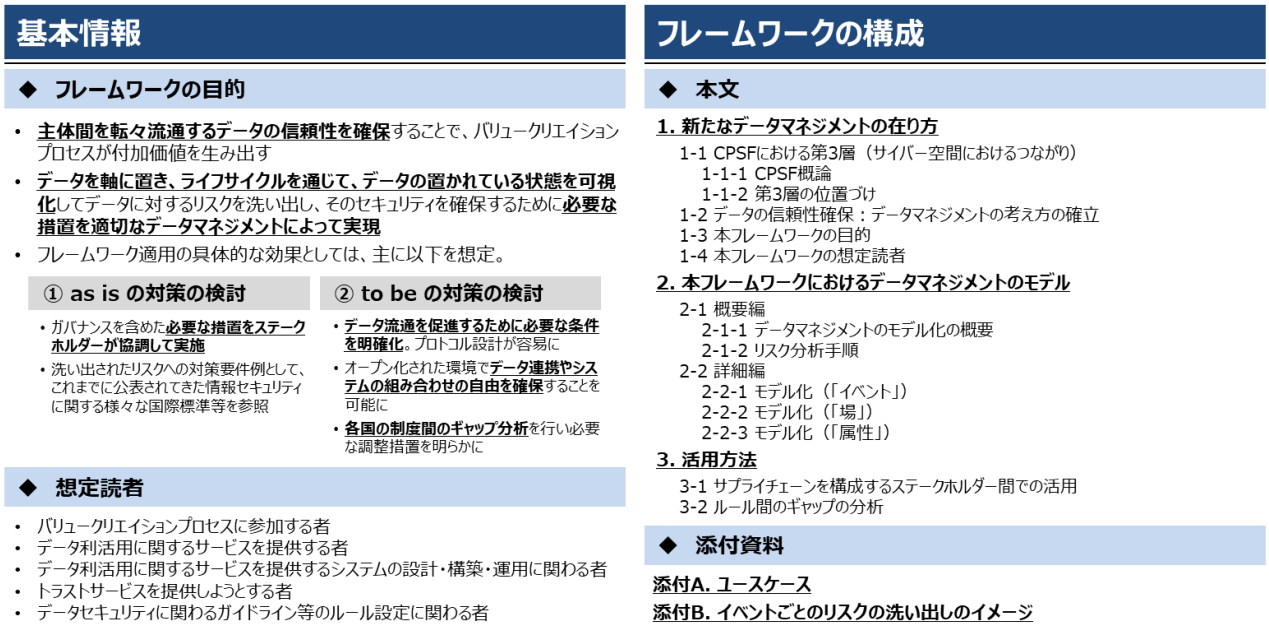


図 2-5 フレームワークの概要

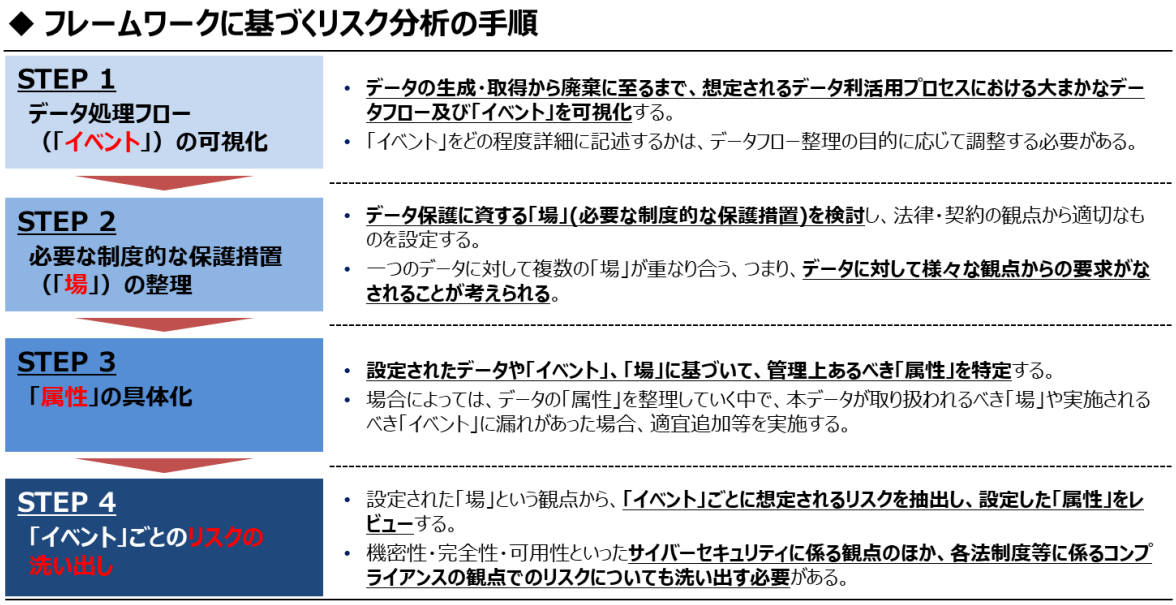


図 2-6 フレームワークに基づくリスク分析の手順

本事業では令和 3 年 7 月 15 日～10 月 11 日に第 1 回パブリックコメントを、令和 4 年 2 月 2 日～3 月 9 日に第 2 回パブリックコメントを実施し[6,10]、ユースケース集について、コメントを頂戴した。表 2-4 にパブリックコメントにて頂戴した主なコメントを示す。

表 2-4　パブリックコメントにて頂戴した主なコメント

No	パブリックコメント	主なご意見
1	第 1 回	「異なるデータ管理のルール」を「跨いでデータが流通した場合」のセキュリティ確保に必要な調整を図るため、「本フレームワークを活用してデータマネジメントに関する共通理解を得る」という考え方に賛同する。
2		3 つの要素（「場」、「属性」、「イベント」）が変化することでリスクが新たに出現したり、変化したりすることが考えられるため、「場」「属性」「イベント」が時間の経過とともに変化することを前提に Step4 の記載を修正すべき。
3		「イベント」における「保管」については、オンプレミス環境を想定しているように読み取れるが、利活用の進むクラウドサービスプロバイダ等が提供するクラウドストレージの例示を加えてはいかがか。
4	第 2 回	個人情報保護法のガイドラインとの整合性を保つために、「現にデータが所在する国を把握できるようにしておくことが望ましい。」という部分は「現にデータが所在する国や地域を把握し、保有個人データの本人には合理的に認識できると考えられる形で情報提供を行う必要がある」と修正した方がよい。
5		4 つの単位（国・地域・組織・人、システム・サービス、機器）の単位でリスクを整理するとあるが、添付 A に示されたユースケースでは、この観点が抜けているため、例示すべき。

(3) 今後の方向性について

- 欧州、米国及びアジア地域にて、ルール形成に当たっての目標や背景は異なるものの、データ保護に関する規定を含むルール形成が進んでいる。グローバルに事業展開を行う企業の各国法令への対応コストは、近年ますます大きくなってきているため、日本においても DFFT に関する検討をより具体化させ、例えば、今年度作成したフレームワークを比較分析の枠組みとして機能させることが望ましい。
- 第 4 回から第 6 回の第 3 層 TF 及び 2 回のパブリックコメントを経てフレームワークが具体化されたものの、内容が抽象的であり、読者にとって理解が難しいものとなっているとのご意見が第 3 層TFの委員より寄せられた(表 2-5)。フレームワークに関するヒアリングを事業者に対して実施することで、使いやすさ等を検証し、改善点を洗い出すことも有効であると考えられる。
- 国内（他省や他課）における議論を踏まえて、フレームワークの改善・普及やルールの具体化を進めた上で、例えば、データ移転に関する各国間の法令ギャップを調整するための体制構築を国際的な会合で提唱することが望ましい。

表 2-5 第 3 層 TF にて頂戴した主なご意見

No	TF	主なご意見
1	第 4 回 （令和 3 年 6 月 30 日）	抽象的な表現が多く具体的なイメージを持ちづらいため、具体的な説明で補完することが良いと思う。一方で、あまり細かく示しすぎると、それが独り歩きして深く考えずにその例をそのまま使ってしまうということも起こり得るので注意が必要である。
2		「場」が曖昧な場合も世の中には多く、例えばオープンソースのコミュニティや研究コミュニティなどは、暗黙知に基づいてルールが形成、運用されていることがある。そのようなものも「場」として扱うのか否かわかるようになっていると良い。
3		時間軸の表現の仕方について、ある瞬間、最後のスナップショットで見ているのか、それとも時間軸が移り変わっていく様子を見ているのかを考えた方が良い。クラウドサービスを利用する例で考えれば、複数の権利者や管理主体が出てくる場合というのは、「場」毎に管理者と権利主体は異なるが、同時に発生し得る、という表現になるのではないか。
4		データを流通させていく中で次に伝えるべき情報（属性）としては、少なくとも客観的な情報と主観的な情報を分けておくべき。
5	第 5 回 （令和 3 年 12 月 13 日）	特にユーケースが典型的な例として理解しやすい例としてまとめているところは素晴らしいと思っている一方で、チャレンジングなことをやっているというところもあり、このフレームワークが公開されたときに読み手が本文の記述だけで、読み取ることは難しい可能性がある。
6		クラウド事業に関するユースケースにて、IaaS の層では「保管」だが、上のレイヤーでは「保管」ではなく色々な処理が入り、発生するリスクがある。ポータルサイトと顧客管理システムの間では、「移転」のみ表現されているが、SaaS、PaaS、IaaS がサプライチェーンを構成しており、その間のイベントの絵があった方がわかりやすい。
7		高齢者事業に関するユースケースにて、「場」の適用を受けるのが誰かが明確化されていない。
8	第 6 回 （令和 4 年 3 月 17 日）	フレームワークの名称案は少々長い。「信頼」という用語が主題と副題で被っているため、主題から削除する等の措置が考えられる。
9		デジタル庁の重点取り組み対象である教育や防災、介護のいずれも基礎自治体が関与するが、その点で様々な制約が生じていると聞いている。可能であれば自治体を巻き込んでケーススタディができると望ましい

3　CPSF 等に基づく国際規格（TR 等を含む）の推進

3.1 本事業項目の目的

本事業では、日本企業の競争力強化に寄与する国際的なルールを形成していくことを目的とし、ルール形成を構成する一要素になりうる CPSF 等をベースにした国際標準化を推進した。

3.2 本事業項目の実施内容

上記目的を達成するため、以下の(1)～(4)を実施内容として整理したうえで、まず、国際規格策定に向けたロードマップを策定した。その後、サプライチェーン全体のサイバーセキュリティ確保に求められるリスク管理に関する国際的なルール形成の状況を調査しつつ、サイバーセキュリティに関する国際的なフレームワークについて、CPSF の考え方をベースにしたものが採用されるよう必要な働きかけ・検討を行った。

＜本事業項目の実施内容＞
(1) 国際規格策定に向けた具体的なロードマップの提示
(2) 国内外の関係機関・関係者の巻き込みや必要な資料の作成等の実施
(3) 国際規格ドラフト文書の作成及び(2)を踏まえた同文書の更新
(4) サプライチェーンのサイバーセキュリティに係る動向調査

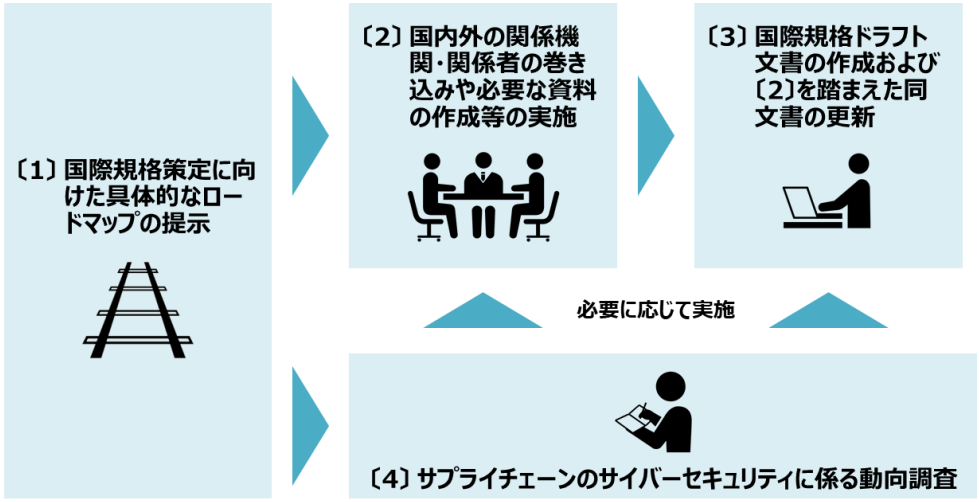


図 3-1 本事業項目の実施プロセス(概要)

3.3 本事業項目の実施結果

3.3.1　国際規格策定に向けたロードマップの策定

(1) 前提：主要な国際標準化機関とその標準策定プロセス

一般に国際規格は、ISO（国際標準化機構）や IEC（国際電気標準会議）等の機関が規定した標準的なプロセスに則り策定される。当該プロセスは主体となる国際標準化機関や策定される文書の種別(例：IS/TS/TR)によって異なるため、具体的なロードマップの策定にあたっては CPSF 等に基づく国際規格の策定を行う機関や委員会、策定する文書の種別を特定し、参照されている標準的な規格策定プロセスを確認する必要がある。

■ CPSF 等に基づく国際規格の策定を行う機関や委員会

国際規格の開発及び保守等を実施している代表的な国際標準化機関及び、当該機関においてサイバーセキュリティ関連の規格化を担当している技術委員会(TC: Technical Committee)又は研究委員会(SG: Study Group)として、以下が挙げられる。

- **ISO(国際標準化機構)**
  電気・電子・通信分野を除く幅広い分野の国際規格を制定している。

- **IEC(国際電気標準会議)**
  電気・電子分野の国際規格を制定している機関である。IEC 内では、TC 65 (Industrial-process measurement, control and automation)が、セーフティ及びセキュリティの側面を含めた、産業プロセスの測定、制御、自動化に使用されるシステムやその構成要素に関する国際規格を開発している。TC 65 は 50 以上の作業部会(WG)を擁する非常に大規模な組織だが、中でも WG 10(Net & System Security)にてセキュリティに係る標準の開発、維持を行っている。TC 65/WG 10 にて開発されている代表的な規格としては産業用自動制御システム(IACS: Industrial Automation Control System)のセキュリティ技術仕様を提供する IEC 62443 シリーズがある。

- **ISO/IEC JTC 1(ISO/IEC 第一合同技術委員会)**
  ISO と IEC が共同設立した技術委員会で、情報技術に関する国際規格を制定している委員会である。中でも JTC 1/SC 27 (Information security, cybersecurity and privacy protection)は、JTC 1 の分科委員会(Sub-Committee)のひとつであり、セキュリティとプライバシーの両側面に対処する一般的な手法、技術、ガイドラインを開発している。JTC 1/SC 27 にて開発、維持される代表的な標準として、情報セキュリティマネジメントに関する規格群である ISO/IEC 27000 シリーズがある。

- **ITU(国際電気通信連合)**
  通信分野、放送・情報技術分野の国際規格を制定している機関である。中でも、ITU-T SG17(Security)は、ITU-T(ITU 電気通信標準化部門)におけるセキュリティの取り組みをほぼ集約して活動し、「セキュリティ」、「ID 管理」、「言語と形式記述技術」 について、Lead Study Group として、ITU-T 全体を取りまとめる立場として活動を行っている。ITU-T/SG17 にて開発、維持される代表的な標準として、CSIRT が必要とするサイバーセキュリティ情報を交換するための標準化された手段を提示する ITU-T X.1500 がある。

CPSF 等に基づく国際規格策定の推進にあたっては、昨年度の事業において、上記のうち JTC 1/SC 27 にて規格化のプロジェクトを立ち上げたところである。図 2-2 に示すように、SC 27 には以下 5 つの作業部会(WG)が存在する。

- **WG 1 (Information security management systems)**
  情報セキュリティマネジメントシステム(ISMS)実装における要求事項や、セクター毎のガイドライン等を策定している。

- **WG 2 (Cryptography and security mechanisms)**
  暗号アルゴリズム、エンティティ認証等のセキュリティ基盤技術の標準化を進めている。

- **WG 3 (Security evaluation, testing and specification)**
  IT 製品や情報システムのセキュリティ評価に関連した規格の開発・保守を行っている。

- WG 4 (Security controls and services)
  ISMS を組織内で実装するための補助となる規格の開発・保守を行っている。

- WG 5 (Identity management and privacy technologies)
  ID 管理、生体認証、プライバシーに関する規格の開発・保守を行っている。

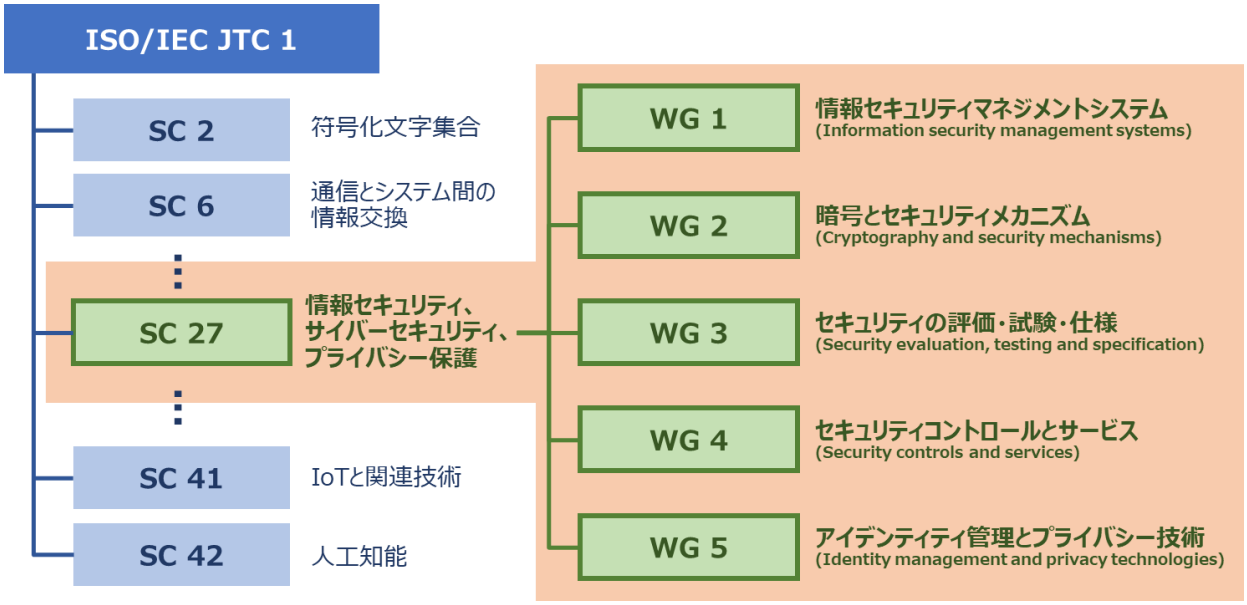


図 3-2 JTC 1/SC 27 の構成

なお、CPSF 等に基づく規格策定に係る具体的なプロジェクトは、ISO/IEC 5689 とナンバリングされ、上記のうち WG 4 (セキュリティコントロールとサービス)で推進されている。

■ 策定する文書の種別と規格策定プロセス

国際規格策定に向けたロードマップを策定する上では、JTC 1/SC 27/WG 4 を含む、ISO/IEC における国際標準策定プロジェクトが、一般的に、表 2-1 のようなプロセスで推進される点 [11] を考慮する必要がある。

No.1.「予備段階」は、目標期日を確定できない業務項目について適用するもので、新業務項目提案(NP)の推敲や初回原案の作成に用いられる段階である。
No.2.「提案段階」では、NP に対して投票を実施し、提案先の委員会(TC、SC 又は WG)の投票 P メンバー の過半数による承認を通じて新プロジェクトを登録する。
No.3「作成段階」では、当該プロジェクトを担当する委員会の指名するエキスパートが作業原案(WD)を作成する。規格を技術仕様書(TS: Technical Specification)[4] 又は技術報告書(TR: Technical Report)[5] として提案する場合、「作成段階」の最後に規定された割合の投票 P メンバーからの承認 を得て、No.6「承認段階」へと移行することができる。
規格を国際規格(International Standard)として提案する場合、No.3「作成段階」に続いて、技術的内容について合意に達するよう、各国代表団体からのコメントを検討する No.4「委員会段階」を実施する。
すべての技術的問題が解決し、委員会原案(CD)を照会原案(DIS)として回付することが承認され、中央事務局によって登録された時点で、「委員会段階」は終了する。
No.5「照会段階」では、中央事務局から 4 週間以内に、すべての国代表団体に原案が回付され、5 か月投票にかけられる。
続く No.6「承認段階」では、中央事務局は、2 か月投票のために最終国際規格案(FDIS)をすべ

ての国代表団体に回付する。FDIS は、投票 P メンバーの 3 分の 2 以上が賛成で、反対が投票総数の 4 分の 1 以下の場合に承認され、No.7「発行段階」にて国際標準として発行される。

表 3-1 ISO/IEC におけるプロジェクトの各段階と関連文書

プロジェクトの段階		関連文書	
		名称	略語
1	予備段階	予備業務項目(Preliminary work item)	PWI
2	提案段階	新業務項目提案(New work item proposal)	NP
3	作成段階	作業原案(Working draft(s))	WD
4	委員会段階	委員会原案(Committee draft(s))	CD
5	照会段階	照会原案(Enquiry draft)	DIS
6	承認段階	最終国際規格案(Final draft international standard)	FDIS
7	発行段階	国際規格(International standard)	ISO/IEC

(2) CPSF 等に基づく国際規格策定に向けたロードマップ

ISO/IEC における規格策定プロセスや実際に策定される文書の種別、JTC 1/SC 27/WG 4 における実際の議論の状況等を踏まえ、CPSF 等に基づく国際規格策定に向けたロードマップを以下の通り作成した。なお、ここでは、策定する文書の種別が「技術仕様」(TS)である場合を想定し、2022 年 3 月時点での議論の状況も加味したうえでロードマップの具体化を行った。

A. 2022 年 3 月時点までの経過

CPSF 等に基づく国際規格策定に向けては、2020 年 4 月の SC 27/WG 4 会合において、日本から CPSF 等に基づく国際規格に係るプロジェクト提案を実施し、PWI(Preliminary Work Item)として「予備段階」の検討が開始された。

その後、約 1 年半をかけて PWI としての検討を実施した後、2021 年 11 月に新規作業項目提案(NWIP)を行い、3 月 5 日までの約 3 か月間投票を実施した。

承認条件が、棄権票を除く 2/3 以上の賛成及び、5 か国以上からの積極的な貢献の表明となる中、賛成 19 票、反対 2 票、棄権 29 票、賛成票を投じた国の中で積極的な貢献の表明を行ったのが 2 か国(日本、ベルギー)ということで、賛成多数となったものの結果は否決となった。プロジェクトは PWI の段階に戻り、4 月の会合以降に再度スコープ等の議論を実施していくこととなる。

今後は、再度の NWIP の実施及び、当該投票における合意形成に向け、スコープの再整理及び、関係者への働きかけ(具体的な貢献を実施するエキスパートの指定、賛成票の増加、棄権票の減少に向けた対外的なコミュニケーション等)を強化していく必要がある。

B. 今後の見通し

本規格(案)を技術仕様書(TS)又は技術報告書(TR)として策定する場合、現在位置している「予備段階」の後で実施される「作成段階」の最後に規定された割合の投票 P メンバーからの承認を得て、「承認段階」及び「発行段階」へと移行することができる。

前述したように 3 月初旬まで実施した NWIP 投票で本件プロジェクトの「作成段階」への進捗は否決されたことから、2022 年 4 月に予定されている SC 27/WG 4 会合では再度 PWI としての審議を継続したうえ、2022 年 9 月または 10 月に実施される SC 27/WG 4 会合以降での再提案実施が想定される。当該投票を通じて、予備段階から作成段階への移行が承認されること、作成段階が 1 年半程度で終了し 2024 年 10 月以降に投票を行い、承認段階へ移行することを仮定すると、図 3-3 に示す形で国際規格(案)の策定が進んでいくものと考えられる。

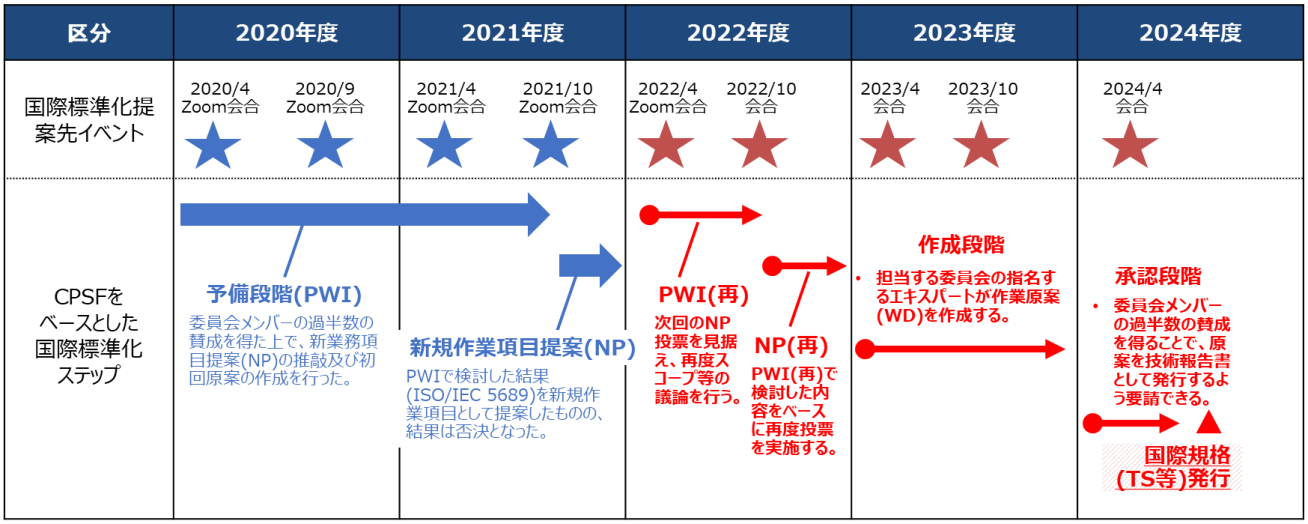


図 3-3 CPSF等に基づく国際規格策定に向けたロードマップ

3.3.2 国内外の関係機関・関係者の巻き込み

前節で検討したロードマップ等を踏まえ、CPSF 等に基づく国際規格(案)の策定を目指し、JTC 1/SC 27/WG 4、JTC 1 内の他の委員会及び国内外のその他の関係機関・関係者に対して実施した巻き込みについて詳述する。

本節以下では、今年度事業にて実施した国内外の関係機関・関係者との議論の状況について、図 3-4 にて示すように、(1) JTC 1/SC 27/WG 4、(2)JTC 1 内の他の SC、(3) その他という 3 つの観点から整理した。

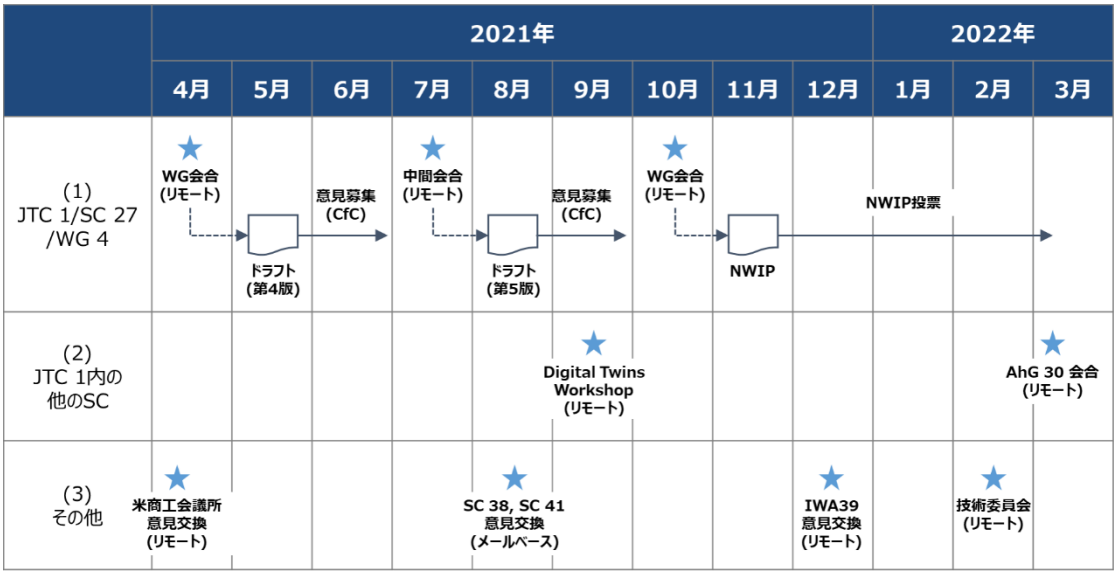


図 3-4 国内外の関係機関・関係者との意見交換の状況

(1) JTC 1/SC 27/WG 4 における国際的な議論の状況

前述したように、JTC 1/SC 27/WG 4 では、2020 年 4 月に日本からの提案を受け、CPSF 等に基づく国際規格に係るプロジェクト(ISO/IEC 5689 Security frameworks based on the conceptual model of cyber-physical systems)を現に推進している。以下にて、同 WG における議論の経過について概要を述べていく。

同委員会における審議のプロセスとしては、半年に一度の WG 会合(SC 27/WG 4 においては通常、4 月と 9 月又は 10 月に開催される)、WG 会合の合間にエディタ等の判断で適宜実施される中間会合(Interim meeting)、会合後に修正されたドラフト文書等に基づいて実施されるエキスパートへの意見募集(CfC: Call for Contribution)が設定されており、それらを通じて、エキスパート間で規格案のスコープや内容等について合意形成を図ることとなっている。

上記の通り、本件についても 2021 年 4 月、10 月の定期会合、エディタの判断により 7 月に中間会合を設け、スコープや内容に関する議論を行った。PWI における議論では、他の既存又は策定中の規格とのスコープの棲み分けや用語定義の明確化(特に、サイバー・フィジカル・システム(CPS)と IoT、デジタルツイン等の類似概念との差異)、規格の構成等がしばしば議論された。

10 月の会合では、用語定義等について関係する委員会(特に IoT やデジタルツインに関する標準化を実施する SC 41)を含めて継続的に議論を行っていくことを前提に、本件プロジェクトを次の段階である NWIP(新規作業項目提案)を実施することが合意され、翌 11 月から 2022 年 3 月 5 日までの期間で投票が行われた。

ドラフト文書の最新版は、11 月の NWIP 向けに作成した準備ドラフト(Preliminary draft)となっており、その概要については次節にて述べる。

(2) JTC 1 の他の SC における国際的な議論の状況

一般に、本規格案の表題にある CPS のような広いスコープを有する概念について議論を行う際、リエゾン・パートナー[12]として関連組織や関係者を規格策定プロセスに巻き込み、合意形成を図る必要がある。

(1) にて述べた SC 27/WG 4 での議論と並行して、JTC 1 の他の関連する SC との議論も行っている。2022 年 3 月現在、SC 41(Internet of Things and related technologies)との連携が明確に認識され、実際に意見交換等が実施されている。具体的には、2021 年 9 月に SC 41 で開催されたデジタルツインに関するワークショップに本件プロジェクトから複数名の関係者が参加する、10 月の SC 27/WG 4 会合にて、SC 41 を兼務するフランス(AFNOR)のエキスパートが窓口となり、SC 27/WG 4 からもエキスパートが参画する形でアドホック・グループを設ける旨が決定される等の連携が行われている。同アドホック・グループは、3 月 9 日に初回会合を開催し、その後も CPS とデジタルツイン等の関係について検討を実施することが予定されている。

(3) 国内の会議体における議論の状況

前述した ISO/IEC JTC 1 内での国外の関係機関・関係者の巻き込みに加え、本事業ではその他の国外関係機関及び、国内の関係機関・関係者の巻き込みを実施した。

4 月には、経済産業省の仲介を通じ、米商工会議所(US Chamber of Commerce)との打合せを実施し、本件プロジェクトの概要を紹介した後、彼らがコネクションを有する米国エキスパートへの協力要請を行った。

また、国内の関係者等の巻き込みとしては、昨年度に引き続き、SC 38 専門委員会、SC 41 専門委員会の代表者との情報共有及び、意見募集等を行った。意見募集の過程で提示された意見等に基づき、各回の CfC における日本(JISC)からのコメントを作成した。

12 月には、SC 41 専門委員会の代表者からの紹介により、情報共有等を目的として、Society 5.0 に関する国際標準化を推進する IWA 39 (Gap analysis for standardization on sustainable and human-centered societies enabled with cyber physical systems)関係者との打合せを実施し、相互の情報共有、意見交換等を行った。

3.3.3 CPSF 等に基づく国際規格(案)の作成

前節で述べたように、本事業項目に係る ISO/IEC における標準策定プロジェクトは、JTC 1/SC 27/WG 4 を中心に、JTC 1/SC 41 やその他の関連する委員会と議論をしながら推進されている。本事業では、国際的な会合の都度、それらの会合における議論の状況をインプットとしてドラフト文書の作成等を実施した。本節では、2022 年 3 月現在の最新版の文書である 11 月に発行された準備ドラフトの内容について概要等を記載する。

当該準備ドラフト文書では、以下のように章節を設けて内容を記載している。

序文［Introduction］
1　適用範囲［Scope］
2　引用規格［Normative references］
3　用語及び定義［Terms and definitions］
4　略語［Abbreviated terms］
5　サイバー・フィジカル・システム(CPS)の概念モデル及び一般的性質［Conceptual cyber-physical systems (CPS) model and its general features］
　5.1　CPS 概念モデル［Conceptual cyber-physical systems (CPS) model］
　5.2　CPS の一般的性質［General features of cyber-physical systems (CPS)］
　5.3　CPS と関連する概念、文書との関係［The relationship of CPS to other related concepts and documents］

6　CPS におけるセキュリティ及びその他の懸念[Security concerns and other concerns in cyber-physical systems］
7　CPS 概念モデルに基づくセキュリティ・フレームワーク［Security frameworks based on the conceptual model of cyber-physical systems］
　7.1　概要［Overview］
　7.2　CPS 概念モデルに基づくセキュリティ・フレームワーク - CPSF［Security framework based on the conceptual model of CPS - CPSF］
　7.3　CPS 概念モデルに基づく OT/IT フレームワーク［OT/IT framework based on the conceptual model of CPS］
Annex A　ユースケース［Use cases for 7.2 (CPSF) (informative)］
Annex B　特定のユースケースを対象にしたフレームワークの利用方法［How to utilize the framework for specific business cases for 7.2 (CPSF) (informative)］

文章の全体的な構成としては、まず、5 章にて CPS の概念モデルと一般的な性質を導入し、IoT やデジタルツイン、エッジ・コンピューティング等の関連概念との差異を示すことを通じて基礎を確立している。ここで、CPS は、「デジタル、アナログ、物理、人の各構成要素が相互に作用し、物理と論理を統合して機能するように設計されたシステム」(system with digital, analogue, physical, and human components interacting with each other engineered to function through integrated physics and logic)と定義されている。この定義は、前述した IWA 39 において Society 5.0 に関する標準化を進める際に用いられているものであり、検討を実施する委員会間で定義の調和を図るため、本件プロジェクトにおいて従来用いていたものから変更した。他の概念との差異については、SC 41 と SC 27/WG 4 の間で設置されたアドホック・グループにおいて今後も検討がなされる。

次に 6 章では、5 章で定義した CPS においていかなる懸念が生じ得るのかという点を整理している。かかる整理は、セキュリティだけでなく、セーフティ、プライバシー、レジリエンス等、広義の「信頼性」(trustworthiness)を構成する観点を踏まえて実施される。本章で示される懸念は、後にセキュリティ・フレームワークを導入する際の基礎となるものとなっている。

7 章では、5 章及び 6 章の内容を踏まえ、組織が自らのセキュリティ課題を解決しようとする際に

「参照」として機能するものとして、セキュリティ・フレームワークを提示している。提示するフレームワークについては、各国・各機関からインプットを得つつ内容の検討を行っているが、日本からはCPSF にて提示されている「三層構造モデル」、「6 つの構成要素」を提案している。加えて、ドイツ(DIN)からの提案に基づき、OT/IT フレームワークも掲載しており、合計で 2 種類が提示されている。

CPS やそのセキュリティ・フレームワークのような抽象度の高い概念に関して共通の理解を醸成するためには、Annex A にあるように、ユースケースを記述し、共有することが有用である。CPSF では、添付 A においてビル分野、スマートホーム分野、自動車分野等、「三層構造モデル」及び「6 つの構成要素」に係る分野別のユースケースが整備されていることから、本検討においてもビル分野、スマートホーム分野等に関してそれらを拡張したユースケースの提案を行っている。

3.3.4 サプライチェーンのサイバーセキュリティに係る動向調査

本事業項目では、これまでに述べた国際標準を直接的に推進する活動に加え、それを補助する目的で、米欧の公的機関又は国際標準化機関において策定された、あるいは策定が進むサプライチェーンのサイバーセキュリティ確保を目的としたリスク評価、リスク管理、セキュリティ対策、セキュリティ評価・認証等に関係する国際規格、ガイドライン、フレームワーク、政策文書等の調査を行った。今回の調査にて対象とした文献の一覧を以下に示す。

表 3-2 調査対象文献一覧

No.	対象文献	発行/審議団体
1	ISO/IEC 27002:2022	ISO/IEC JTC 1
2	ISO/IEC FDIS 27400	ISO/IEC JTC 1
3	ISO/IEC 2nd CD 27402	ISO/IEC JTC 1
4	ISO/IEC PWI 27404	ISO/IEC JTC 1
5	IEC 62443 シリーズ	IEC TC 65

(1) ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ、プライバシー保護- 情報セキュリティ管理策 [Information security, cybersecurity and privacy protection ー Information security controls]

ISO/IEC 27002 は、情報セキュリティマネジメントシステム(ISMS)に関する要求事項を規定する ISO/IEC 27001 の Annex A にて示されたセキュリティ管理策の実施方法を具体的に記載したガイドラインとして位置づけられる。同規格は、2013 年に出版されたものがこれまで活用されていたが、ISO/IEC JTC /SC 27/WG 1 における審議を経て、2022 年 2 月に最新版が公開されている[13]。

最新版では、主に図 3-5 に示す 3 つのポイントについて改定がなされている[14]。

① 章構成の見直し
従来は、ISO/IEC 27001:2013 Annex A の構成にならって 14 に分かれていた章構成を、「組織的管理策」、「人的管理策」、「物理的管理策」、「技術的管理策」の 4 つに再編している。

② 新規管理策の追加
前回改定時からの環境変化等を勘案し、11 の新規管理策を追加している。
(脅威インテリジェンス、クラウドサービス利用のための情報セキュリティ、ビジネス継続のための ICT の備え、物理的セキュリティ監視、設定管理、情報削除、データマスキング、データ漏えいの防止、監視活動、ウェブフィルタリング、セキュアコーディング)

③ 管理策に対する属性の設定

各管理策を様々な観点から見ることができるようにするため、管理策ごとに管理策タイプ(予防/検知/是正)、情報セキュリティプロパティ(機密性/完全性/可用性)、サイバーセキュリティコンセプト(識別/防御/検知/対応/復旧)等の「属性」(attribute)を設定している。

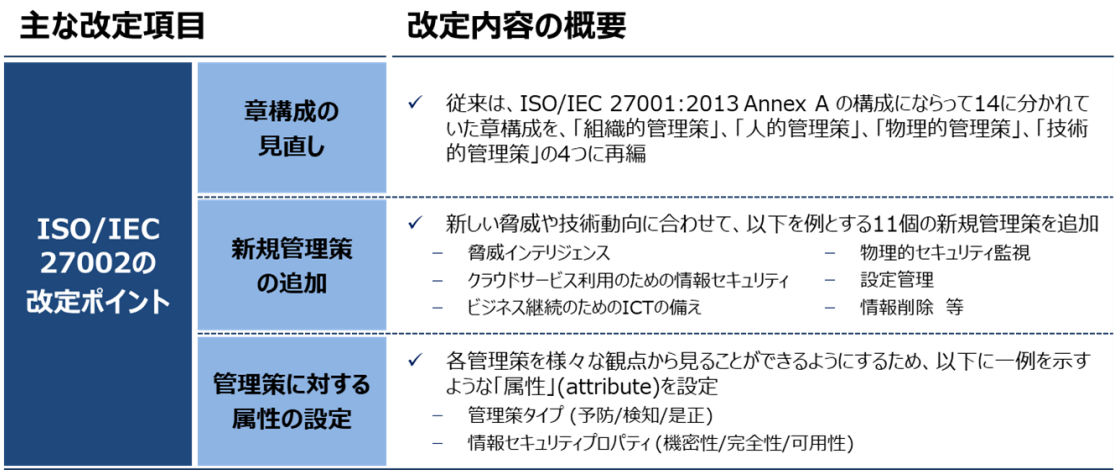


図 3-5 ISO/IEC 27002 の改定ポイント

また、本改定に伴い、ISO/IEC 27001 の動向についても変化が生じる見込みである。具体的には、ISO/IEC 27002:2022 の発行を受けて、短期的には Annex A のみを改定することを目指す。また、中長期的な目標としては、Annex A の改定と並行して、本格的な改定プロジェクトを立ち上げるとされている。

(2) ISO/IEC FDIS 27400 サイバーセキュリティ - IoT セキュリティ及びプライバシー -ガイドライン [Cybersecurity ー IoT security and privacy ー Guidelines]

図 6 にて示すように、JTC 1/SC 27/WG 4 では、近年、IoT セキュリティ関連標準の開発が盛んに実施されている。中でも、ISO/IEC FDIS 27400 は、はじめに日本から提案されたものであり、策定状況でも最も発行に近いものとなっている。

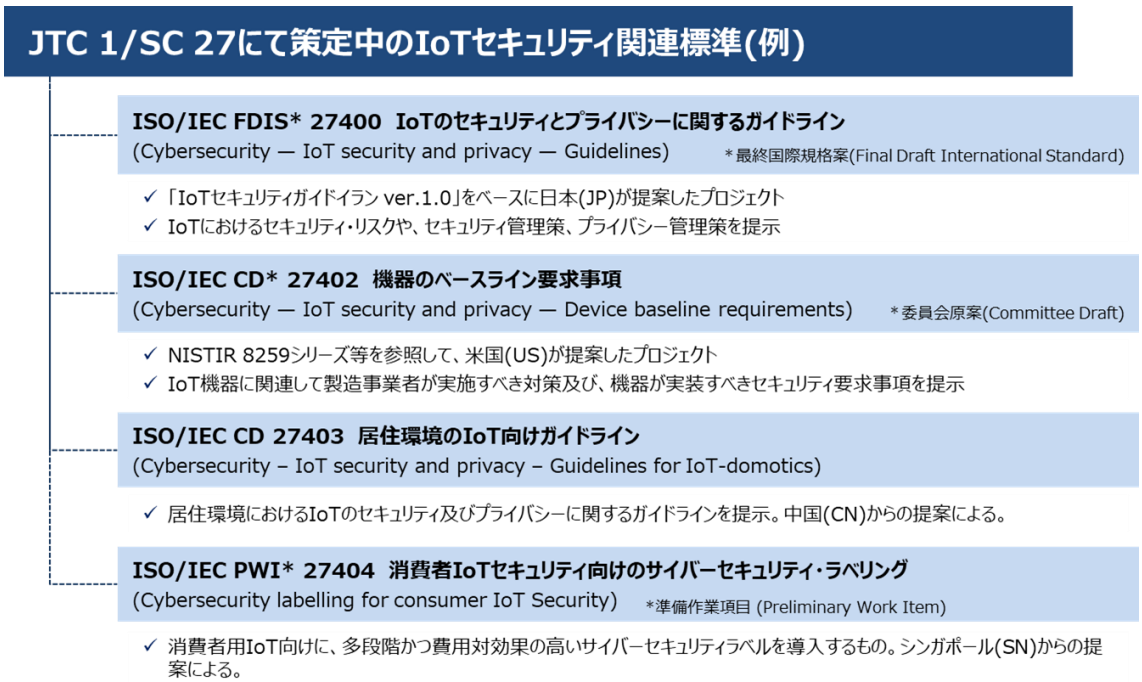


図 3-6 JTC 1/SC 27 にて策定中の IoT セキュリティ関連標準(例)

規格の構成としては、5 章において IoT の特性、IoT システムに関連するステークホルダー(IoT サービス提供者/IoT サービス開発者/IoT 利用者)、IoT サービスのライフサイクル、参照モデル等の前提となる枠組みを提示し、6 章にて IoT において想定されるリスク源を整理している。その後の 7 章は、IoT におけるセキュリティ管理策及びプライバシー管理策を提示しており、ガイドライン規格としての中核を担っていると捉えられる。

本規格では、参照モデルとして、図 3-7 に示す ISO/IEC 30141:2019 (IoT 参照アーキテクチャ)において示されるドメインベースのものが利用されている。

参照モデルにおける各ドメインは、以下のように位置づけられる。

- ユーザドメインは、ヒトとデジタルユーザーを含む
- 物理エンティティドメインは、IoT システムの物理エンティティを含む。
- センシング＆コントロールドメインは、IoT 機器及び IoT ゲートウェイを含む。
- 運用＆管理ドメインは、運用支援システムやビジネス支援システムを含む。
- リソースアクセス＆相互作用ドメインは、外部エンティティが IoT システムの機能にアクセスするメカニズムを提供する。
- アプリケーション＆サービスドメインは、IoT サービス提供者が提供するアプリケーションやサービスを含む。

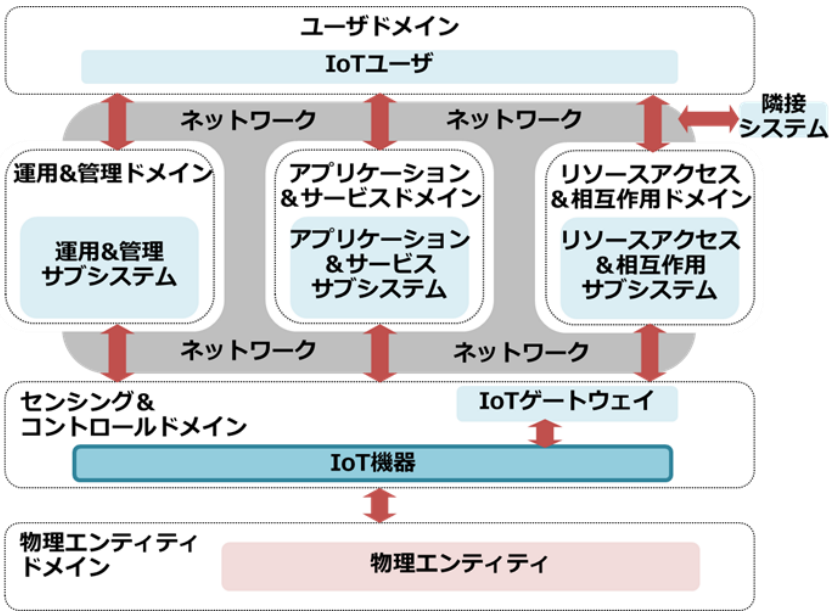


図 3-7 ドメインベースの参照モデル

6 章では、図 3-7 に示すドメインごとにリスク源が示され、7 章では対策ごとにそれらが適用されるドメインが明示される。その他、詳細は割愛するが、7 章にてセキュリティ管理策及びプライバシー管理策は、目的、想定読者(ステークホルダーの分類に準じる)、追加のガイダンスとともに提示される。

ISO/IEC FDIS 27400 は、2022 年 3 月現在、FDIS の投票期間にあり、4 月 25 日の締め切り後、発行に向かうと想定される。

(3) ISO/IEC CD 27402 サイバーセキュリティ - IoT セキュリティ及びプライバシー - 機器ベースライン要求事項［Cybersecurity ー IoT security and privacy ー Device baseline requirements］

ISO/IEC CD 27402 は、ISO/IEC FDIS 27400 と同様に IoT に関連する規格であるが、特にセンシング＆コントロールドメインに属する IoT 機器(センサー又はアクチュエータ)及びその開発者が、(ISO/IEC 27400 等で規定される)セキュリティ管理策及びプライバシー管理策をサポートするために実装すべきベースライン要求事項を規定する。

ここでベースライン要求事項とは、ヘルスケアや金融、産業、家電、輸送等の様々な垂直市場(vertical markets)に共通する水平方向(horizontal)の要求事項を意図したものである。特定のセクター及び垂直市場固有の要求事項は、本規格に上乗せする形で構築されることが期待されている。

現時点で、要求事項は、IoT 機器開発者向けのもの(3 件)と、IoT 機器向けのもの(7 件)に分けられる。前者には、①リスクマネジメントの実施、②IoT 機器提供者やユーザーとのコミュニケーション、③脆弱性の開示・対処プロセスの確立が含まれ、後者には、①IoT 機器固有の識別子、②構成機能、③安全なリセット機能、④ユーザーデータの消去機能、⑤データ保護機能、⑥インターフェースへのアクセス制御機能、⑦ソフトウェア及びファームウェアの更新機能が含まれている。

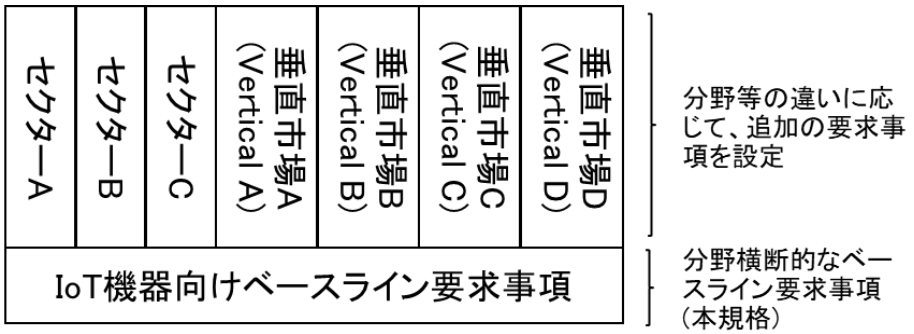


図 3-8 ベースライン要求事項(本規格)の位置づけ

(4) ISO/IEC PWI 27404 情報技術 - セキュリティ技術 - 消費者 IoT 向けのサイバーセキュリティ・ラベリング [Information technology − Security techniques − Cybersecurity labelling for consumer IoT]

ISO/IEC PWI 27404 は、消費者向け IoT に多段階で費用対効果の高いサイバーセキュリティ・ラベルを導入するものとされている。2021 年にシンガポールから提案された新規のプロジェクトである。

現時点で提示されているドラフト文書では、シンガポール国内で運用されるサイバーセキュリティ・ラベリング制度[15]を参照しつつ、ラベリングの原則やステークホルダーの役割と責任(4 章)、ラベリングのレベル(6 章)、ラベル取得プロセス(8 章)等が扱われている。

ドラフト文書では、以下に示す 4 つのラベリングに係るレベルとアセスメント・ティアが示されている。ラベリングに係る 4 つのレベルの含意は以下の通り。

- レベル 1: 基本的な要求事項に適合している
- レベル 2: セキュリティ・バイ・デザイン原則に基づいて開発されている
- レベル 3: 既知の脆弱性がない
- レベル 4: 一般的な攻撃に対するレジリエンスがある

上記 4 つのレベルは、それぞれ 4 つのアセスメント・ティアに対応している。

- ティア 1: セキュリティ・ベースライン要求事項への適合を自己宣言する
- ティア 2: ベースライン要求事項に加えて、ライフサイクル要求事項への適合を自己宣言する

- ティア 3: ベースライン要求事項及びライフサイクル要求事項への適合に関して第三者機関がバイナリ解析を実施する
- ティア 4: ベースライン要求事項及びライフサイクル要求事項への適合に関して第三者機関がペネトレーションテストを実施する

本文中には、ベースライン要求事項やライフサイクル要求事項に相当する対策は明示されていないが、附属書 B において ETSI EN 303 645 をベースにした適合性チェックリストが整備されている。一方で、ISO/IEC の文脈では必ずしも同欧州規格がベースライン要求事項等の形で公式に受容されているわけではないことを踏まえれば、今後何らかの形で規格のスコープや内容に対して修正がなされている可能性が高いと考えられる。

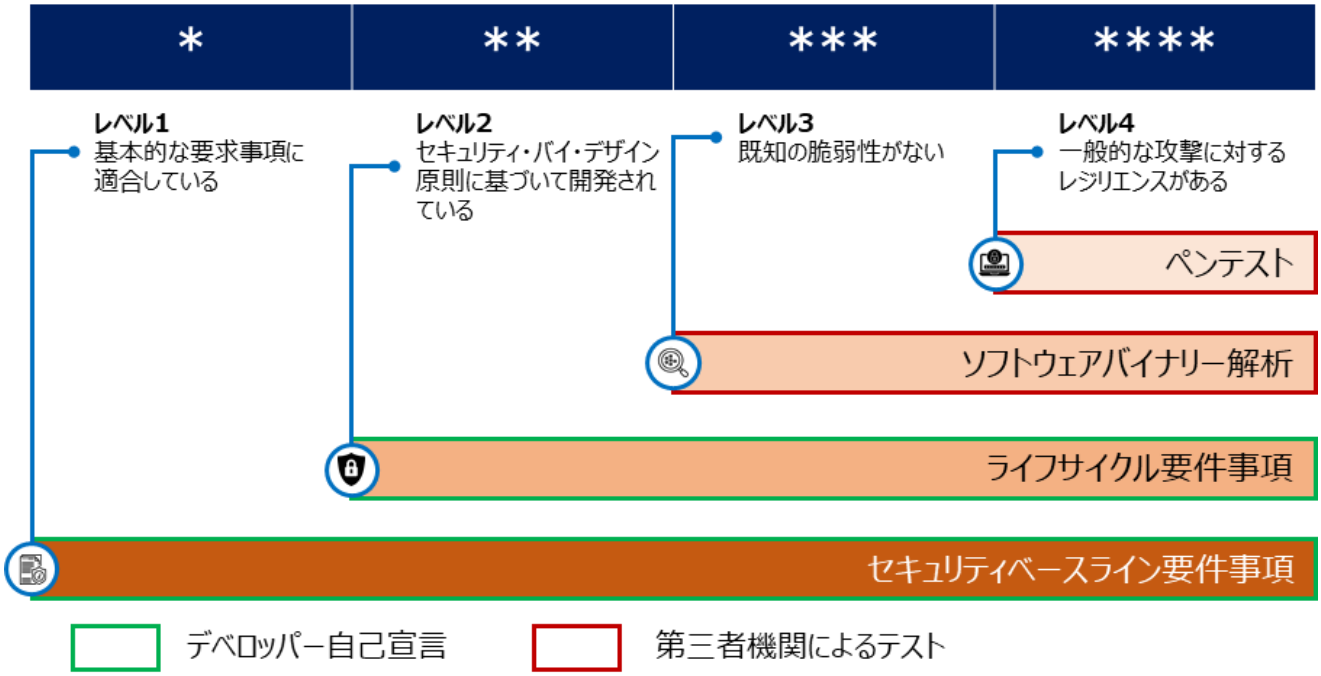


図 3-9 消費者 IoT ラベリングにおけるレベルとアセスメント・ティア

(5) IEC 62443 産業用オートメーション及び制御システムのセキュリティ［Security for industrial automation and control systems］

IEC 62443 シリーズは、IEC TC 65(工業用プロセス制御)の WG 10 で開発、保守されている一連の規格群であり、産業用オートメーション及び制御システム(IACS:Industrial Automation and Control System)を対象としたサイバーセキュリティ規格である。同シリーズは、以下の規格グループを構成している。

- IEC 62443-1: 全体に共通する一般的な事項を規定
- IEC 62443-2: 主に工場オーナ向けにポリシー、プロシージャレベルの要求事項等を規定
- IEC 62443-3: 主にシステムインテグレータ向けにシステムレベルの要求事項等を規定
- IEC 62443-4: 主に装置ベンダー向けにコンポーネントレベルの要求事項等を規定
- IEC 62443-6: IEC 62443 シリーズに係るセキュリティ評価手法を規定

適合性評価及び認証に係るものとしては、IACS 分野のセキュリティマネジメントシステムを対象に、IEC 62443-2-1 を認証基準として、CSMS(Cyber Security Management System)適合性評価制度[16]が第三者認証制度として運用されている。

また、IEC 62443-4-1/2 を認証基準として、IACS を構成する各コンポーネントを対象とした

EDSA 認証(Embedded Device Security Assurance)が運用されている。

IEC 62443 シリーズに関連して、昨今議論されているのが、水平規格化(Horizontal standardization)である。現在は、FA(Factory Automation)、PA(Process Automation)、BA(Building Automation)等の分野で同シリーズの活用が実施されているが、その裾野を広げるべく、まずは TC 65 内で規格の調査等を開始した段階になる。

さらに、IEC 62443 シリーズと、JTC 1/SC 27 で開発される ISO/IEC 27000 シリーズとの整合性確保についても議論がなされている。特に、ISO/IEC 27400 シリーズ (IoT security and privacy)、ISO/IEC 24392 (Security reference model for Industrial Internet Platform)との整合が課題視されており、JTC 1/SC 27 と共同で今後何らかの検討がなされる可能性がある。

参考文献

1 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(CPSF)を策定しました”，2019 年 4 月 18 日 (https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html)

2 経済産業省，“IoT セキュリティ・セーフティ・フレームワーク(IoT-SSF)を策定しました”,2020 年 11 月 5 日 (https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html)

3 経済産業省，“第 4 回『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース”，2020 年 8 月 6 日 (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/WG_seido/WG_bunyaodan/dainiso/004.html)

4 経済産業省，“第 5 回『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース”，2021 年 11 月 29 日 (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/005.html)

5 経済産業省，“第 6 回『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース”，2022 年 3 月 9 日 (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/dainiso/006.html)

6 経済産業省，“データによる価値創造(Value Creation)を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク(仮)」案の意見公募手続(パブリックコメント)を開始しました”，2022 年 2 月 2 日 (https://www.meti.go.jp/press/2021/02/20220202001/20220202001.html)

7 経済産業省，“第 4 回『第 3 層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース”，2021 年 6 月 30 日 (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/004.html)

8 経済産業省，“第 5 回『第 3 層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース”，2021 年 12 月 13 日 (https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/daisanso/005.html)

9 経済産業省，“第 6 回『第 3 層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース”，2022 年 3 月 17 日 (未定)

10 経済産業省，”データによる価値創造(Value Creation)を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク(仮)」骨子案の意見公募手続(パブリックコメント)を開始しました”，2021 年 7 月 15 日 (https://www.meti.go.jp/press/2021/07/20210715005/20210715005.html)

11 規格開発プロセス等の詳細については、「ISO/IEC 専門業務用指針 第1部」 (https://webdesk.jsa.or.jp/pdf/dev/md_4917.pdf)を参照されたい。

12 ISO/IEC における基本原則の一つである「ステークホルダーの関与」を達成するため、すべての関連するステークホルダーが規格開発プロセスに加われる機会を提供するメカニズムであり、ISO/IEC 委員会間での連携や、その他の機関との連携等が含まれる。詳細については、ISO が発行する委員会リエゾン向けの文書を参照されたい。(https://webdesk.jsa.or.jp/pdf/dev/md_4908.pdf)

13 ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection − Information security controls (https://www.iso.org/standard/75652.html)

14 土屋直子(NTT テクノクロス株式会社), “改定版 ISO/IEC 27002 の概要及び ISO/IEC 27001 最新動向”, https://www.jnsa.org/seminar/2021/isms2021/kouen1.pdf

15 Cybersecurity Labelling Scheme (CLS) (https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls)

16 CSMS 適合性評価制度 (https://isms.jp/csms.html)

17 IEC 62443 CONFORMANCE CERTIFICATION – Certifying Industrial Control System Devices and Systems (https://www.isasecure.org/ja-JP/)

別紙1

公開情報等の調査
IoT関連文献

対象文献

調査対象リスト

項番	国・地域	文献等の名称	対象分野	作成機関	作成時期	文書種別
1	欧州	Product Security and Telecommunications Infrastructure Bill	消費生活用製品	英国DCMS	2021年	政策
2		ETSI EN 303 645 V2.1.1	消費生活用製品	ETSI	2020年	ガイドライン
3		ETSI TS 103 701 V1.1.1	消費生活用製品	ETSI	2021年	ガイドライン
4		Guidelines for Securing the Internet of Things	全般	ENISA	2020年	ガイドライン
5		Recommendations for the security of CAM	全般	ENISA	2021年	ガイドライン
6	その他	Cybersecurity Certification Guide	消費生活用製品	The Cyber Security Agency of Singapore (CSA)	2021年	ガイドライン

(1) Product Security and Telecommunications Infrastructure Bill
概要

文献概要	名称	Product Security and Telecommunications Infrastructure Bill（製品セキュリティ及び電気通信インフラストラクチャ法案）		
	主旨	英国内で販売されるスマートデバイスを対象として、IoTデバイスに一定のセキュリティ対策を義務付ける法案。		
	国・地域	英国	適用分野	IoTデバイス
	策定者	英国デジタル・文化・メディア・スポーツ省	対象者	IoTデバイスを製造するメーカー、輸入業者、ディストリビューター、小売店など
	遵守義務	違反には罰金が課せられる。		
	普及状況	下院で法案審議が開始されており、第二読会が終了した段階。		
	策定年	2021年	ページ数	72ページ

カテゴリ	カテゴライズ	パート1の「製品セキュリティー」ではセキュリティ要件、関係者義務など、エンフォースメント、補足規定、そしてパート2の「電気通信インフラストラクチャ」で構成されている。
	カテゴリ評価	IoTデバイスに関しては、メーカーと輸入業者、ディストリビューターに対する要求事項が示されている。
	カテゴリ確認要求	消費者向け接続可能製品がサイバー攻撃に対してより安全で、個人のプライバシーとセキュリティを保護するための規定が示されている。違反に対しては罰金が課せられる。
	制度的枠組み	セキュリティー要件は「2018 Code of Practice for Consumer Internet of Things Security」と「European Standard on Internet of Things Security, ETSI EN 303 645」に基づいている。

関連URL	https://bills.parliament.uk/bills/3069 https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets https://www.gov.uk/government/news/new-smart-devices-cyber-security-laws-one-step-closer

(1) Product Security and Telecommunications Infrastructure Bill
詳細

法案構成

パート1：製品セキュリティ
第1章：セキュリティ要件
　製品に関連するセキュリティ要件
　　セクション1. セキュリティ要件を指定する権限
　　セクション2. セクション1に基づく規制に関する追加規定
　　セクション3. セキュリティ要件事項への適合性を判断する権限

　セキュリティ要件が関係する可能性のある製品
　　セクション4. 関連する接続可能な製品
　　セクション5. 関連する接続可能な製品となる可能性のある製品の種類
　　セクション6. 除外製品

　セキュリティ要件が適用される可能性のある人物
　　セクション7. 関係者

第2章：関係者義務など
　製造者の義務
　　セクション8. セキュリティ要件を遵守する義務
　　セクション9. コンプライアンスステートメント
　　セクション10. コンプライアンス違反の可能性を調査する義務
　　セクション11. コンプライアンス違反に関連する措置を講じる義務
　　セクション12. 記録保持の義務

　販売代理店
　　セクション13. 製造者のコンプライアンス違反に関連する措置を 講じる義務

　輸入業者の義務
　　セクション14. セキュリティ要件を遵守する義務
　　セクション15. コンプライアンスステートメント
　　セクション16. 製造者によるコンプライアンス違反があった場合、製品を供給しない義務
　　セクション17. 輸入業者又は製造業者のコンプライアンス違反の可能性を調査する義務
　　セクション18. 輸入者のコンプライアンス違反に関する措置を講じる義務
　　セクション19. 製造者のコンプライアンス違反に関連する措置を講じる義務
　　セクション20. 記録保持の義務

　ディストリビューターの義務
　　セクション21. セキュリティ要件遵守の義務
　　セクション22. コンプライアンスステートメント
　　セクション23. 製造者によるコンプライアンス違反があった場合、製品を供給しない義務
　　セクション24. ディストリビューターのコンプライアンス違反に関連する措置を講じる義務
　　セクション25. 製造者のコンプライアンス違反に関連する措置を講じる義務

第3章：エンフォースメント（強制執行）
　一般
　　セクション26. パート1のエンフォースメント
　　セクション27. エンフォースメント機能の委任

　エンフォースメント通知
　　セクション28. コンプライアンス通知
　　セクション29. 停止通知
　　セクション30. リコール通知
　　セクション31. エンフォースメント通知を変更又は取り消す権限
　　セクション32. エンフォースメント通告に従わない場合
　　セクション33. エンフォースメント通知に対する不服申し立て
　　セクション34. 不当になされた通知に対する補償
　　セクション35. セクション34に基づく決定に対する不服申し立て

　罰金
　　セクション36. 罰金
　　セクション37. 罰金の金額決定
　　セクション38. 最大金額
　　セクション39. 罰金通知：追加規定
　　セクション40. 罰則通告のエンフォースメント
　　セクション41. 罰金通知に対する不服申し立て

　没収
　　セクション42. 没収
　　セクション43. 没収に関する追加規定
　　セクション44. セクション42に基づく決定に対する不服申し立て

(1)Product Security and Telecommunications Infrastructure Bill 詳細

その他のエンフォースメント権限
セクション45．コンプライアンス違反について一般公表する権限
セクション46．関連人物に対して取られたエンフォースメント措置の詳細を公表する権限
セクション47．製品リコール権限

情報開示
セクション48．情報開示

その他・補足
セクション49．エンフォースメント機能を行使する権限を有すると称する罪
セクション50．通知手段
セクション51．販売代理店の責任
セクション52．取締役、パートナー等による犯罪

第4章：補足規定
ガイダンス
セクション53．ガイダンス
解釈
セクション54．「英国消費者向け接続製品」の意味
セクション55．「供給」の意味
セクション56．パート1で使用される他の表現の意味

パート2：通信インフラストラクチャ
コードの権利を付与できる人
セクション57．事業者が占有している土地に関する「占有者」の意味

機器のアップグレードと共有の権利
セクション58．機器を共有するための電子通信法上の権利
セクション59．機器のアップグレードと共有：既存の契約
セクション60．2003年12月29日以前に設置された機器のアップグレードと共有
規約上の権利を付与された事業用借地権の更新
セクション61．規約上の権利を付与された賃借権に基づく賃貸料：イングランドとウェールズ
セクション62．規約上の権利を付与された賃借権に基づく賃貸料：北アイルランド
セクション63．規約上の権利に関する補償：イングランドとウェールズ
セクション64．規約上の権利に関する補償：北アイルランド
セクション65．イングランドとウェールズにおける借地権に関する裁判所の管轄権

応答のない占有者
セクション66．応答のない占有者

暫定的措置
セクション67．　規約に基づく特定の申請に対する決定保留の取り決め

電子通信規約に基づく紛争
セクション68．裁判外紛争解決手続の使用
セクション69．事業者の行動に関する苦情

手続き制限時間
セクション70．　規約手続の決定に期限を設ける権限

インフラストラクチャに関連するネットワークプロバイダーの権利
セクション71．インフラストラクチャに関連するネットワーク事業者の権利

附則
セクション72．　改正を行う権限
セクション73．「電子通信規約」の意味

パート3：最終規定
セクション74．経過措置又は保存規定を設ける権限
セクション75．規則
セクション76．範囲
セクション77．開始
セクション78．ショートタイトル

(1)Product Security and Telecommunications Infrastructure Bill 詳細

IoT関連の法案内容

製品のセキュリティ対策（法案のパート1）で示されている内容は以下の通り。
【目的】
消費者向け接続可能製品がサイバー攻撃に対してより安全で、個人のプライバシーとセキュリティを保護することを保証。
接続可能製品例：スマートフォン、スマートTV、ゲームコンソール、セキュリティカメラ、アラームシステム、スマートトイレ、スマート家電といったインターネットにアクセスできるすべてのデバイス。
スマート電球、スマートサーモスタット、ウェアラブルフィットネストラッカーなど、他の複数のデバイスに接続できるがインターネットに直接接続できない製品にも適用される。
これらの製品に関して遵守しなければならない製造業者、輸入業者、ディストリビューターの義務を規定。義務に違反した場合、強制執行ができる権限を与える。
安全でない製品が英国市場で販売されるのを防ぐことを目的とした、民事及び刑事制裁を伴うエンフォースメント体制を構築する。
消費者向け接続可能製品に関する最低限のセキュリティ要件を規定し、修正する権限を大臣に付与する。
【具体策】
本法案では、デジタル機器に組み込まれ、サイバー犯罪者の標的となる推測しやすいデフォルトパスワードが禁止される。
機器にあらかじめ設定され、サイバー犯罪の標的となりやすい「password」や「admin」などのユニバーサルデフォルトパスワードの禁止。製品にあらかじめ設定されているパスワードは、ユニークなものでなければならず、工場出荷時にリセットできないようにする必要がある。
製造者は、接続可能な製品のセキュリティアップデートを受け取る期間について顧客に対してより透明性を高め、これらの製品で見つかった脆弱性についてのより良い公開報告システムを構築する必要がある。
デバイス製造者が製品のセキュリティアップデートを提供する期間について消費者に透明性を持たせ、人々が購入する際に明確になるようにする。製品がセキュリティアップデートを受け取らない場合、顧客に通知する必要がある。
ソフトウェアの欠陥やバグを報告しやすくするために製造者が容易に利用できる公的な窓口を確保すること。
この措置を守らなかった場合、最高1,000万ポンド又は世界全体での売上高の4%、さらに継続的な違反の場合は1日あたり最高2万ポンドの罰金を科される可能性がある。

(2) ETSI EN 303 645 V2.1.1
概要

文献概要	名称	ETSI EN 303 645 V2.1.1 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements		
	主旨	ネットワークに接続されている消費者向けIoT機器のセキュリティと、関連するサービスとの関係における上位レベルの要求を規定している。		
	国・地域	欧州	適用分野	消費者向けIoT機器
	策定者	ETSI	対象者	消費者向けIoTの開発と製造に携わるすべての関係者向け
	遵守義務	消費者向けIoT機器のサイバーセキュリティについての欧州規格。		
	普及状況	EUローカルのIoTセキュリティ規格。民生用IoT製品の安全性が高まるにつれ、将来の改訂では本文献で推奨されている規定が義務付けられることが想定される。英国では、「Product Security and Telecommunications Infrastructure Bill」の基礎となっている。		
	策定年	2020年	ページ数	34ページ

カテゴリ	カテゴライズ	消費者向けIoTのサイバーセキュリティ対策規定と、消費者向けIoTのデータ保護規定で構成。
	カテゴリ評価	製品が本規格に適合するかどうかの判定を各規定で紹介。そのため、本規定をどのように実装するかについて、事例と解説文により基本的な指針を示している。
	カテゴリ確認要求	インターネットに接続された民生機器のセキュリティについて広く考えられているグッドプラクティスを、成果に焦点を当てた一連の上位レベルの規定としてまとめたものとなっている。また、消費者向けIoTの開発及び製造に携わるすべての関係者に、製品の安全確保に関するガイダンスを提供することを目的としている。
	制度的枠組み	本文献の規定は、IoTのセキュリティとプライバシーに関する公表された規格、勧告、ガイダンスの検討を経て策定されており、ETSI TR 103 305-3、ETSI TR 103 309、ENISA Baseline Security Recommendations, 英国デジタル・文化・メディア・スポーツ省セキュア・バイ・デザイン・レポート、IoT Security Foundation Compliance Framework、GSMA IoT Security Guidelines and Assessment、ETSI TR 103 533、DIN SPEC 27072、OWASP Internet of Thingsなどが含まれている。

関連URL	https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard

(2) ETSI EN 303 645 V2.1.1
詳細

対象

ネットワークインフラ（インターネットやホームネットワークなど）に接続される消費者向けIoT機器と、その関連サービスとの相互作用に関するハイレベルなセキュリティ及びデータ保護規定を規定。関連サービスは対象外。消費者向けIoT機器の例は以下の通り。
コネクテッド・キッズ・トイ、ベビーモニター
コネクテッド煙探知機、ドアロック、窓センサー
複数機器が接続するIoTゲートウェイ、基地局、ハブ
スマートカメラ、テレビ、スピーカー
ウェアラブル・ヘルス・トラッカー
コネクテッドホームオートメーション、アラームシステム（特にそのゲートウェイとハブ）
洗濯機や冷蔵庫などのコネクテッド家電
スマートホームアシスタント
本文献では、以下のような制約のある機器に特有のセキュリティの考慮事項にも言及。
窓用コネクトセンサー、浸水センサー、エネルギースイッチは一般的に制約のある機器。
消費者向けIoT機器でない機器、例えば製造業、ヘルスケア、その他の産業用アプリケーションでの使用を主目的とする機器は本文献の範囲外。

5 コンシューマー向けIoTのためのサイバーセキュリティ規定

5.1 ユニバーサルデフォルトパスワードの廃止	
規定番号	規定
5.1-1	パスワードが使用され、工場出荷時以外の状態にある場合、すべての民生用IoT機器のパスワードは機器ごとに一意であるか、又はユーザーによって定義されるものとする。
5.1-2	プリインストールされた機器ごとの固有のパスワードが使用される場合、これらは機器のクラス又はタイプに対する自動的な攻撃のリスクを低減するメカニズムで生成されること。
5.1-3	機器に対してユーザーを認証するために使用される認証メカニズムは、技術の特性、リスク及び用途に適したベストプラクティスの暗号を使用するものとする。
5.1-4	ユーザーが機器に対して認証を行うことができる場合、機器はユーザー又は管理者に使用する認証値を変更するための簡単なメカニズムを提供しなければならない。
5.1-5	機器が制約を受けない機器の場合、ネットワークインタフェース経由の認証機構に対する総当たり攻撃を実行不可能にする機構が利用可能でなければならない。

5.2 脆弱性の報告を管理する手段の導入	
規定番号	規定
5.2-1	製造者は、脆弱性開示の方針を公開するものとする。この方針には、最低限問題を報告するための連絡先とタイムラインに関する情報を含むものとする。
5.2-2	開示された脆弱性には、適時に対処する必要がある。
5-2.3	製造者は、定められたサポート期間中に販売、生産、生産された製品及びサービス内のセキュリティの脆弱性を継続的に監視し、特定し、是正する必要がある。

5.3 ソフトウェアを最新の状態に保つ	
規定番号	規定
5.3-1	消費者向けIoT機器に含まれるすべてのソフトウェアコンポーネントは、安全にアップデート可能とすること。
5.3-2	制約のない機器である場合、アップデートを安全にインストールするための機構を有すること。
5.3-3	アップデートは、ユーザが簡単に適用できるものでなければならない。簡単さの程度は、機器設計と意図された使用方法に依存する。（自動アップデート、関連サービス（モバイルアプリケーションなど）を使用して開始、機器のウェブインターフェースを介する）
5.3-4	ソフトウェアのアップデートは自動的なメカニズムを使用する必要がある。自動アップデートに失敗した場合、状況によってはユーザーが機器を使用できなくなる。 ウォッチドッグやデュアルバンクフラッシュ、リカバリーパーティションなどの検出メカニズムにより、機器が正常であったバージョン、又は工場出荷状態に戻すことが保証される。

(2) ETSI EN 303 645 V2.1.1
詳細

規定番号	規定
5.3-5	機器は初期化後、定期的にセキュリティアップデートが利用可能かどうかを確認する必要がある。
5.3-6	機器が自動アップデートやアップデート通知をサポートする場合、初期化状態でこれらを有効にし、ユーザーがセキュリティアップデートやアップデート通知のインストールを有効、無効、又は延期できるように設定可能とする必要がある。
5.3-7	機器は安全なアップデートメカニズムを促進するため、ベストプラクティス暗号を使用するものとする。
5.3-8	セキュリティアップデートは適時に行うこと。
5.3-9	機器は、ソフトウェアアップデートの真正性と整合性を検証すること。
5.3-10	アップデートがネットワークインターフェースを介して配信される場合、機器は信頼関係（Trust relationship）を介して各更新の真正性と整合性を検証すること。
5.3-11	製造者は、セキュリティアップデートが必要であることを、そのアップデートによって軽減されるリスクに関する情報とともに、認識可能で明白な方法でユーザーに通知すること。
5.3-12	ソフトウェアアップデートの適用によって機器の基本的な機能が停止する場合、機器はユーザーに通知する必要がある。
5.3-13	製造者は、定められたサポート期間をユーザーにとって明確かつ透明性のある方法で公表すること。
5.3-14	ソフトウェアアップデートができない制約のある機器については、ソフトウェアアップデートができない根拠、ハードウェアの交換サポート期間と方法、定められたサポート期間について、製造者がユーザーに分かりやすい形で公表すること。
5.3-15	ソフトウェアアップデートができない制約のある機器については、製品の分離とハードウェアの交換が可能であること。
5.3-16	消費者向けIoT機器のモデル名は、機器上のラベル又は物理的なインターフェースを介して、明確に認識可能とすること。

5.4 機密性の高いセキュリティパラメータを安全に保存	
規定番号	規定
5.4-1	永続的なストレージにある機密性の高いセキュリティパラメータは、機器によって安全に保管されること。
5.4-2	セキュリティ目的のため、機器ごとにハードコードされた固有の識別子が機器に使用される場合、物理的、電気的又はソフトウェアなどの手段による改ざんに耐えるように実装されなければならない。
5.4-3	機器ソフトウェアのソースコードに、ハードコードされた重要なセキュリティパラメータは使用してはならない。
5.4-4	ソフトウェアアップデートの整合性及び真正性チェック、並びに機器ソフトウェアにおける関連サービスとの通信保護に使用される重要なセキュリティパラメータは、機器ごとに固有でなければならず、機器クラスに対する自動攻撃のリスクを低減するメカニズムで生成されるものとする。

5.5 セキュアな通信	
規定番号	規定
5.5-1	消費者向けIoT機器は、ベストプラクティスの暗号を使用して安全に通信するものとする。
5.5-2	消費者向けIoT機器は、ネットワーク及びセキュリティ機能、特に暗号の分野において、審査又は評価済みの実装を使用する必要がある。
5.5-3	暗号化アルゴリズムとプリミティブは、アップデート可能とする必要がある。
5.5-4	初期化された状態のネットワークインターフェイスを介した機器機能へのアクセスは、そのインターフェイスでの認証後にのみ可能とする。
5.5-5	ネットワークインタフェースを介してセキュリティに関連する設定の変更を可能にする機器機能は、認証後にのみアクセスできるものとする。ただし、機器が依存するネットワークサービスプロトコルにおいて、機器の動作に必要な設定を製造者が保証できない場合は例外とする。
5.5-6	重要なセキュリティパラメータは転送中に暗号化されるべきであり、その暗号化は技術の特性、リスク、用途に応じた適切なものでなければならない。

(2) ETSI EN 303 645 V2.1.1
詳細

規定番号	規定
5.5-7	消費者向けIoT機器は、遠隔からアクセス可能なネットワークインターフェースを介して通信される重要なセキュリティパラメータの機密性を保護しなければならない。
5.5-8	製造者は、機器に関連する重要なセキュリティパラメータについて、安全な管理プロセスに従わなければならない。 重要なセキュリティパラメータ（一般に「キー・マネジメント」と呼ばれる）については、オープンで査読された標準を使用することが強く推奨される。

5.6 外部に晒される攻撃対象領域を最小限とすること	
規定番号	規定
5.6-1	未使用のネットワーク及び論理インターフェースはすべて無効にすること。
5.6-2	初期化状態において、機器のネットワークインタフェースは、セキュリティ関連情報の未認証の開示を最小にしなければならない。
5.6-3	機器ハードウェアは、物理的なインターフェイスを不必要に攻撃に晒すべきではない。
5.6-4	デバッグインタフェースが物理的にアクセス可能な場合は、ソフトウェアで無効化すること。
5.6-5	製造者は、機器の使用目的又は操作に使用又は必要とされるソフトウェアサービスのみを有効にする必要がある。
5.6-6	コードはサービス／機器の動作に必要な機能に限定する。
5.6-7	ソフトウェアはセキュリティと機能性の両方を考慮し、必要最小限の権限で実行されること。
5.6-8	機器はメモリに対するハードウェアレベルのアクセス制御機構を含むこと。
5.6-9	製造者は、機器に展開されるソフトウェアについて、安全な開発プロセスに従うこと。

5.7 ソフトウェアの整合性を確保	
規定番号	規定
5.7-1	消費者向けIoT機器は、セキュアブートメカニズムを使用してソフトウェアを検証する必要がある。
5.7-2	ソフトウェアに不正な変更が検出された場合、機器はユーザー及び／又は管理者に問題を警告し、警告を行うために必要な範囲以上のネットワークに接続してはならない。

5.8 個人情報の安全性を確保	
規定番号	規定
5.8-1	機器とサービス、特に関連するサービスとの間でやり取りされる個人情報の機密性は、ベストプラクティスの暗号化により保護されること。
5.8-2	機器と関連サービス間で通信される機密性の高い個人データの機密性は、技術の特性や使用方法に適した暗号を使用して保護されること。
5.8-3	機器のすべての外部感知能力は、ユーザーにとって明確で透明性のあるアクセス可能な方法で文書化されなければならない。

5.9 停止から回復力のあるシステム	
規定番号	規定
5.9-1	消費者向けIoT機器やサービスには、データネットワークや電力が停止する可能性を考慮し、レジリエンスを組み込む必要がある。
5.9-2	消費者向けIoT機器は、ネットワークアクセスが失われた場合でも、動作とローカル機能を維持し、電力損失が回復した場合には正常に回復する必要がある。
5.9-3	消費者向けIoT機器は、イインフラストラクチャの能力を考慮した上で、期待される稼働状態、安定した状態で、秩序正しくネットワークに接続する必要がある。

(2) ETSI EN 303 645 V2.1.1
詳細

5.10 システムテレメトリーデータの検証	
規定番号	規定
5.10-1	消費者向けIoT機器やサービスから、利用状況や計測データなどのテレメトリーデータを収集する場合、セキュリティ上の異常がないかを調べる必要がある。

5.11 ユーザーが簡単にユーザーデータを削除できるようにすること	
規定番号	規定
5.11-1	ユーザーデータを簡単な操作で機器から消去できる機能を提供すること。
5.11-2	ユーザーが簡単な方法で関連するサービスから個人データを削除できるような機能を機器に提供すること。
5.11-3	ユーザーは、個人データを削除する方法について明確な指示を受ける必要がある。
5.11-4	サービス、機器、アプリケーションから個人データが削除されたことを、ユーザーが明確に確認できるようにすること。

5.12 機器のインストールとメンテナンスを容易にすること	
規定番号	規定
5.12-1	消費者向けIoTのインストールとメンテナンスは、ユーザーによる判断を最小限にとどめ、ユーザビリティに関するセキュリティのベストプラクティスに従う必要がある。
5.12-2	製造者は、ユーザーに機器の安全な設定方法に関するガイダンスを提供する必要がある。
5.12-3	製造者は、機器が安全に設定されているかどうかを確認する方法について、ユーザーにガイダンスを提供する必要がある。

5.13 入力データの検証	
規定番号	規定
5.13-1	消費者向けIoT機器ソフトウェアは、ユーザーインターフェースを介して入力されたデータ、アプリケーションプログラミングインターフェース（API）を介して転送されたデータ、又はサービスや機器内のネットワーク間で転送されたデータを検証する必要がある。

6. 民生用IoT機器のデータ保護規定

規定番号	規定
6.1	製造者は、消費者に対し、機器やサービスごとに、どのような個人データが、誰によって、どのような目的で処理されているかについての明確かつ透明性のある情報を提供するものとする。これは、広告主を含む関与しうる第三者にも適用される。
6.2	個人データが消費者の同意に基づいて処理される場合、この同意は有効な方法で取得されるものとする。
6.3	個人データの処理に同意した消費者は、いつでもそれを撤回することができるものとする。
6.4	消費者向けIoT機器やサービスからテレメトリーデータを収集する場合、個人データの処理は意図した機能に必要な最小限のものにとどめるべき。
6.5	消費者向けIoT機器やサービスから遠隔測定データを収集する場合、消費者はどのような遠隔測定データが収集され、それが誰によって、どのような目的で使用されているかについての情報を提供されるものとする。

(3) ETSI TS 103 701 V1.1.1
概要

文献概要	名称	ETSI TS 103 701 V1.1.1 CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements		
	主旨	ETSI EN 303 645のテスト仕様に位置づけられる規格。これにより、製造業者、ベンダー、販売業者などのサプライヤー組織は、自己評価又はテストラボを介して、ETSI EN 303 645に対する自社機器の適合性を評価することができる。		
	国・地域	欧州	適用分野	消費者向けIoT製品
	策定者	ETSI	対象者	消費者向けIoT製品のセキュリティを保証するテストラボや認証機関、及び自己評価の実施を希望する製造業者
	遵守義務	IoT製品がEN 303 645に適合しているかどうかを判定するときの判断基準を示しており、遵守義務といった内容ではない。		
	普及状況	普及状況に関する情報はないが、BMW, ANEC, Huawei Tech.(UK) Co.. Ltd, KAT, NCSC, CIS, DCMS, Eurosmart AISBLが支援団体となっている。		
	策定年	2021年	ページ数	135ページ

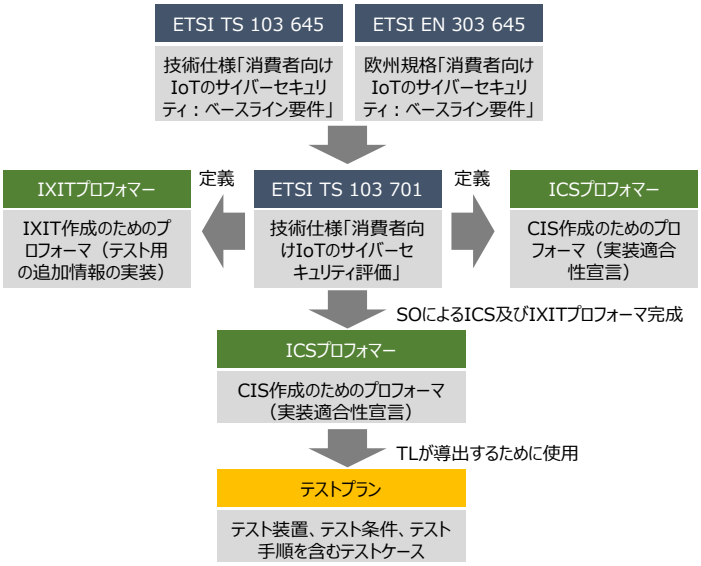
カテゴリ	カテゴライズ	消費者向けけIoTのテストシナリオとして、「レポートの実装」と「ユニバーサルデフォルトパスワードの廃止」、「脆弱性の報告管理手段の導入」、「ソフトウェアを最新の状態に保つ」、「機密性の高いセキュリティパラメータを安全に保存」、「セキュアなコミュニケーション 」、「攻撃面の露出を最小化」、「ソフトウェアの整合性を確保」、「個人データが安全であることを確認」、「停電に強いシステムの構築 」、「システムテレメトリーデータの検証」、「ユーザーが簡単にユーザーデータを削除できるようにする」、「デバイスのインストールとメンテナンスを容易に」、「入力データ検証」、「消費者向けIoTのデータ保護」で構成。
	カテゴリ評価	テストケース（概念）とテストケース（機能）において、各カテゴリーの「PASS」と「FAIL」を示す。
	カテゴリ確認要求	消費者向けIoT製品の供給者・実装者が第1者評価（自己評価）を行う場合、利用者組織が第2者評価を行う場合、独立試験機関が第3者評価を行う場合、及び認証・適合性宣言スキーム所有者が調和されたスキームを運用する場合での使用となっている。
	制度的枠組み	ETSI TS 103 645（技術仕様「消費者向けIoTのサイバーセキュリティ：ベースライン要件」）とETSI EN 303 645（欧州規格「消費者向けIoTのサイバーセキュリティ：ベースライン要件」）に対する適合性評価の基礎の位置づけ。

関連URL	https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

(3) ETSI TS 103 701 V1.1.1
詳細

4 適合性評価プロセスに関する本書の関係

本文献は、ETSI TS 103 645 /ETSI EN 303 645に対する適合性評価の基礎となるもので、ICS（Implementation Conformance Statement、実装適合性宣言）とIXIT（Implementation eXtra Information for Testing、試験用プロトコル実装補助情報）のプロフォーマが定義されている。ICSとIXITは、ICSとIXITのプロフォーマに基づき、SO（Supplier Organization、DUT（Device Under Test）のサプライチェーンの重要な部分を担当する事業者）からTL（Test Laboratory、DUTの適合性評価を実行する独立テスト組織など）に提供される。TLは、これらの文書を用いて、テスト計画を導き出す。



5 コンシューマーIoTのテストシナリオ（TSO）

TSO 4：レポートの実装

テスト	テストグループ目的
テストグループ4-1	
テストケース 4-1-1（概念）	本テストケースの目的は、DUTに適用できない、又はDUTが満たさないと考えられる推奨事項の正当性を概念的に評価すること。

TSO 5.1：ユニバーサルデフォルトパスワードの廃止

テスト	テストグループ目的
テストグループ5.1-1：本テストグループは、工場出荷時を除くDUTの全状態に対応。	
テストケース 5.1-1-1（概念）	本テストケースの目的は、パスワードベースの認証機構の概念評価。
テストケース 5.1-1-2（機能）	本テストケースの目的は、IXITの文書、ユーザー定義パスワード、生成メカニズムの完全性に関するパスワードベースの認証メカニズムの機能評価。
テストグループ5.1-2	
テストケース 5.1-2-1（概念）	本テストケースの目的は、プリインストールされているパスワードの生成メカニズムの概念評価。
テストケース 5.1-2-2（機能）	本テストケースの目的は、プリインストールされたパスワードの生成メカニズムの機能評価。
テストグループ5.1-3：本テストグループの目的は、第一に暗号方式が認証機構に必要なセキュリティ保証を提供しているかどうか、第二に暗号方式が実現可能な攻撃に対して脆弱であることが知られていないかどうかを評価。	
テストケース 5.1-3-1（概念）	本テストケースの目的は、認証機構に使用される暗号について、ベストプラクティス暗号の使用と実現可能な攻撃に対する脆弱性に関する概念評価。
テストケース 5.1-3-2（機能）	本テストケースの目的は、認証機構に使用される暗号の機能評価。

(3) ETSI TS 103 701 V1.1.1
詳細

テスト	テストグループ目的
テストグループ5.1-4	
テストケース 5.1-4-1（概念）	本テストケースの目的は、認証値を変更する仕組みの概念評価。
テストケース 5.1-4-2（機能）	本テストケースの目的は、認証値を変更するメカニズムの機能評価。
テストグループ5.1-5	
テストケース 5.1-5-1（概念）	本テストケースの目的は、ネットワークインターフェースを介したブルートフォースアタックを実行不可能にするためのメカニズムの概念評価。
テストケース 5.1-5-2（機能）	本テストケースの目的は、IXITのドキュメントと対応するメカニズムの完全性に関して、ネットワークインターフェースを介したブルートフォース攻撃を実行不可能にするメカニズムの機能評価。

TSO 5.2：脆弱性の報告管理手段の導入

テスト	テストグループ目的
テストグループ5.2-1	
テストケース 5.2-1-1（概念）	本テストケースの目的は、脆弱性開示ポリシーの公開に関する概念評価。
テストケース 5.2-1-2（機能）	本テストケースの目的は、脆弱性開示ポリシーの公開に関する機能評価。
テストグループ5.2-2	
テストケース 5.2-2-1（概念）	本テストケースの目的は、脆弱性への対処方法の概念評価と、実施の前提条件が確保されていることの確認。
テストグループ5.2-3	
テストケース 5.2-3-1（概念）	本テストケースの目的は、記載された手順に関して、継続的な監視、セキュリティ脆弱性の特定と是正、及び実施の前提条件が確保されていることの確認を概念的に評価。

TSO 5.3：ソフトウェアを最新の状態に保つ

テスト	テストグループ目的
テストグループ5.3-1：本テストグループは、ソフトウェアのアップデートが現実的でない場合や、セキュリティ上の理由でアップデートがない場合を除き、各ソフトウェアコンポーネントのアップデート可能性を取り扱う。	
テストケース 5.3-1-1（概念）	本テストケースの目的は、ソフトウェアのアップデートの有無とアップデート機構に関するソフトウェアコンポーネントのアップデート可能性を概念的に評価。
テストケース 5.3-1-2（機能）	本テストケースの目的は、誤用を避けるためのアップデート機構の有効性を機能的に評価。
テストグループ5.3-2：本テストグループでは、ソフトウェアアップデートを安全にインストールするためのアップデート機構が少なくとも1つ存在することを検証。	
テストケース 5.3-2-1（概念）	本テストケースの目的は、DUTへのアップデートインストールを攻撃者が悪用することを防ぐための適切な対策に関するアップデートインストール機構の概念評価。
テストケース 5.3-2-2（機能）	本テストケースの目的は、誤使用を避けるためのアップデート機構の有効性を機能的に評価。
テストグループ5.3-3：本規定の焦点は、ユーザーの視点からアップデートのトリガーとなり、すべてのソフトウェアコンポーネントを簡単な方法でアップデートできる機能が提供されているかどうかを検証すること。	
テストケース 5.3-3-1（概念）	本テストケースの目的は、ユーザーがアップデートを適用する際の簡便性に関するアップデート機構の概念評価。
テストグループ5.3-4：本規定の焦点は、ユーザー視点でのアップデートのトリガーと、すべてのソフトウェアコンポーネントを自動的にアップデートする機能がユーザーに提供されているかどうかを検証すること。	
テストケース 5.3-4-1（概念）	本テストケースの目的は、自動化機構に関するアップデート機構の概念評価。
テストグループ5.3-5：本規定の焦点は、DUTのソフトウェアのセキュリティアップデートを確認する機能。	
テストケース 5.3-5-1（概念）	本テストケースの目的は、利用可能なセキュリティアップデートのチェックに関するアップデート機構の概念評価。

(3) ETSI TS 103 701 V1.1.1
詳細

テスト	テストグループ目的
テストグループ5.3-6	
テストケース 5.3-6-1（概念）	本テストケースの目的は、自動アップデートとアップデート通知の構成の概念評価。
テストケース 5.3-6-2（機能）	本テストケースの目的は、自動アップデート及びアップデート通知設定の機能評価。
テストグループ5.3-7：本テストグループの目的は、第一に暗号方式が安全なアップデート機構に必要なセキュリティ保証を提供するかどうか、第二に暗号方式が実現可能な攻撃に対して脆弱であることが知られていないかどうかを評価すること。	
テストケース 5.3-7-1（概念）	本テストケースの目的は、ベストプラクティス暗号の使用に関するアップデート機構に使用される暗号と、実現可能な攻撃に対する脆弱性の概念評価。
テストグループ5.3-8：本評価では、セキュリティアップデートをタイムリーに展開するために必要な管理手続きに焦点を当てている。	
テストケース 5.3-8-1（概念）	本テストケースの目的は、セキュリティアップデートの導入方法に関する概念評価と、導入のための前提条件が確保されていることの確認。
テストグループ5.3-9：本評価では、ソフトウェアアップデートのインストール前にDUT自身が行う真正性と整合性の検証に焦点を当てている。	
テストケース 5.3-9-1（概念）	本テストケースの目的は、真正性、整合性、実行主体に関するソフトウェアアップデートの検証の概念評価。
テストグループ5.3-10：信頼関係の検証。	
テストケース 5.3-10-1 （概念/機能）	本テストケースの目的は、真正性・整合性に関する信頼関係と実行主体によるソフトウェアアップデート検証の概念評価と、IXITドキュメントの完全性の機能評価。
テストグループ5.3-11	
テストケース 5.3-11-1（概念）	本テストケースの目的は、必要なセキュリティアップデートについて、ユーザーへの情報提供の方法と内容を概念的に評価。

テスト	テストグループ目的
テストグループ5.3-12	
テストケース 5.3-12-1（概念）	本テストケースの目的は、破壊的なソフトウェアアップデートが行われた場合のユーザー通知に関する概念的な評価。
テストグループ5.3-13：サポート期間。	
テストケース 5.3-13-1（概念）	本テストケースの目的は、定義されたサポート期間の公開を概念的に評価すること。
テストケース 5.3-13-2 (機能)	本テストケースの目的は、定義されたサポート期間の公開の機能評価。
テストグループ5.3-14	
テストケース 5.3-14-1（概念）	本テストケースの目的は、アップデートやハードウェア交換のサポートがない根拠を公表する概念評価。
テストケース 5.3-14-2（機能）	本テストケースの目的は、アップデートやハードウェア交換のサポートがない根拠を公表する機能評価。
テストグループ5.3-15	
テストケース 5.3-15-1（概念）	本テストケースの目的は、DUTの分離機能とハードウェア交換対応の概念評価。
テストケース 5.3-15-2（機能）	本テストケースの目的は、DUTの分離機能とハードウェア交換対応の機能評価。
テストグループ5.3-16	
テストケース 5.3-16-1（概念）	本テストケースの目的は、モデル指定の概念評価。
テストケース 5.3-16-2（機能）	本テストケースの目的は、モデル指定の機能評価。

(3) ETSI TS 103 701 V1.1.1
詳細

TSO 5.4：機密性の高いセキュリティパラメータを安全に保存

テスト	テストグループ目的
テストグループ5.4-1：本テストグループは、機密性の高いセキュリティパラメータが、主張する保護スキームを用いてそのタイプに応じて安全に保管されているかどうかを評価。	
テストケース 5.4-1-1（概念）	本テストケースの目的は、セキュリティクレームとIXIT文書の完全性に関する機密セキュリティパラメータの安全な保管の概念評価。
テストケース 5.4-1-2（機能）	本テストケースの目的は、機密性の高いセキュリティパラメータの安全な保管の機能評価。
テストグループ5.4-2：本テストグループは、ハードコード化されたデバイスの識別と、適切な保護ニーズが特定されているかどうかを取り上げている。	
テストケース 5.4-2-1（概念）	本テストケースの目的は、ハードコード化されたIDの耐タンパ性ストレージの概念評価。
テストケース 5.4-2-2（機能）	本テストケースの目的は、ハードコード化されたIDの耐タンパ性保存の機能評価
テストグループ5.4-3：本テストグループは、提供された重要なセキュリティパラメータのプロビジョニング機構において、デバイスソフトウェアのソースコードにハードコードされた重要なセキュリティパラメータが文書化されていないことを示すものがあるかどうかを評価。	
テストケース 5.4-3-1（概念）	本テストケースの目的は、ハードコード化された重要なセキュリティパラメータの概念評価。
テストケース 5.4-3-2（機能）	本テストケースの目的は、ハードコード化された重要なセキュリティパラメータの機能評価。
テストグループ5.4-4：本テストグループは、基本的な規定によって対処されるすべての重要なセキュリティパラメータが特定され、その生成メカニズムが対応する要件を満たしているかどうかを文書によって評価。	
テストケース 5.4-4-1（概念）	本テストケースの目的は、ソフトウェアアップデートの整合性と信頼性のチェック、及び生成メカニズムに関する関連サービスとの通信保護に使用される重要なセキュリティパラメータの概念評価。

TSO 5.5：セキュアなコミュニケーション

テスト	テストグループ目的
テストグループ5.5-1：本テストグループの目的は、第一に暗号方式が通信のユースケースに必要なセキュリティ保証を提供しているかどうか、第二に暗号方式が実現可能な攻撃に対して脆弱であることが知られていないかどうかを評価すること。	
テストケース 5.5-1-1（概念）	本テストケースの目的は、通信機構に使用される暗号について、ベストプラクティス暗号の使用と、実現可能な攻撃に対する脆弱性に関する概念的評価を行うこと。
テストケース 5.5-1-2（機能）	本テストケースの目的は、通信機構に使用される暗号の機能評価。
テストグループ5.5-2：本テストグループの目的は、第一にネットワークとセキュリティの機能性が対応する範囲に基づいて審査又は評価されているかどうか、第二に報告書がDUT実装の識別（バージョンと名前）と一致しているかどうかを評価すること。	
テストケース 5.5-2-1（概念）	本テストケースの目的は、審査と評価に関するネットワークとセキュリティ機能の実装の概念な評価。
テストケース 5.5-2-2（機能）	本テストケースの目的は、審査と評価に関するネットワークとセキュリティ機能の実装の機能評価。
テストグループ5.5-3：本テストグループの目的は、第一にその実装を示すソフトウェア部品ごとのアップデート機構があるかどうか、第二に暗号アルゴリズムやプリミティブを提供する実装の置き換えが可能かどうか、アップデートによる副作用が製造者によって考慮されているかどうかを評価すること。	
テストケース 5.5-3-1（概念）	本テストケースの目的は、暗号アルゴリズムやプリミティブを提供する実装の更新性に関する概念な評価。
テストグループ5.5-4：本テストグループの目的は、第一に認証後にのみ機器の機能にアクセスできるかどうか、第二に認証方法が異なるサブジェクトを識別できるかどうか、第三にそれが有効で敵に強いかどうか、最後に認証ステップが有効であるかどうかを評価すること。	
テストケース 5.5-4-1（概念）	本テストケースの目的は、認証と承認に関する初期化された状態でのネットワークインターフェイスを介した機器機能の概念評価。
テストケース5.5-4-2 （機能）	本テストケースの目的は、認証と承認に関する初期化された状態でのネットワークインターフェイスを介した機器機能の機能評価。

(3) ETSI TS 103 701 V1.1.1
詳細

テスト	テストグループ目的
テストグループ5.5-5：本テストグループの目的は、第一にセキュリティに関連する変更を可能にするデバイス機能が認証後にのみアクセス可能かどうか、第二に認証方法が異なるサブジェクトを識別できるかどうか、第三にそれが有効で敵に強いかどうか、最後に認証ステップが有効かどうかを評価すること。	
テストケース 5.5-5-1（概念）	本テストケースの目的は、認証と承認に関するネットワークインターフェイスを介したセキュリティ関連の変更を可能にするデバイス機能の概念評価。
テストケース 5.5-5-2（機能）	本テストケースの目的は、認証と承認及びIXIT文書の完全性に関して、ネットワークインターフェースを介してセキュリティ関連の変更を可能にするデバイスの機能評価。
テストグループ5.5-6：本テストグループの目的は、第一に暗号方式が重要なセキュリティパラメータの通信というユースケースに必要なセキュリティ保証を提供するかどうか、第二に暗号方式が実現可能な攻撃に対して脆弱であることが知られていないかどうかを評価すること。	
テストケース 5.5-6-1（概念）	本テストケースの目的は、重要なセキュリティパラメータの通信に使用される暗号の概念評価。
テストケース 5.5-6-2（機能）	本テストケースの目的は、重要なセキュリティパラメータの通信に使用される暗号の機能評価。
テストグループ5.5-7：本テストグループの目的は、第一に暗号方式が重要なセキュリティパラメータの通信というユースケースに必要なセキュリティ保証を提供するかどうか、第二に暗号方式が実現可能な攻撃に対して脆弱であることが知られていないかどうかを評価すること。	
テストケース 5.5-7-1（概念）	本テストケースの目的は、リモートアクセス可能なネットワークインターフェースを介して重要なセキュリティパラメータを通信するために使用される暗号の概念評価。
テストケース 5.5-7-2（機能）	本テストケースの目的は、リモートアクセス可能なネットワークインターフェースを介して重要なセキュリティパラメータを通信するために使用される暗号の機能評価。
テストグループ5.5-8	
テストケース 5.5-8-1（概念）	本テストケースの目的は、パラメータのライフサイクルの網羅性に関する安全管理プロセスの概念評価と、実施の前提条件が確保されていることの確認。

TSO 5.6：攻撃面の露出を最小化

テスト	テストグループ目的
テストグループ5.6-1：論理インターフェースは、原則として複数のネットワークインターフェースを経由してアクセスすることができるため、製造者は論理インターフェースへのすべてのアクセス経路が特定されていることを確認。	
テストケース 5.6-1-1（概念）	本テストケースの目的は、DUTのネットワークと論理インターフェイスの概念評価。
テストケース 5.6-1-2（機能）	本テストケースの目的は、DUTのネットワーク及び論理インターフェイスの機能評価と、IXIT文書の完全性。
テストグループ5.6-2	
テストケース 5.6-2-1（概念）	本テストケースの目的は、初期化された状態で認証を行わないネットワークインタフェースが開示する情報の概念評価。
テストケース 5.6-2-2（機能）	本テストケースの目的は、初期化された状態で認証を行わないネットワークインタフェースが開示される情報の機能評価。
テストグループ5.6-3：本テストグループの目的は、一方では露出を必要としない物理ポートインターフェイスがデバイスの筐体によって保護されているかどうかを評価すること。一方では、露出を必要としないエアインターフェイスが無効化されているかどうかを評価。	
テストケース 5.6-3-1（概念）	本テストケースの目的は、一般的に暴露を必要としないインタフェースと恒久的暴露を必要としないインタフェースに関するDUTの物理的インタフェースの概念評価。
テストケース 5.6-3-2（機能）	本テストケースの目的は、IXIT文書の完全性と、DUTの物理インターフェースの機能評価。
テストグループ5.6-4：デバッグインターフェイスを無効にするソフトウェアメカニズムが必須であることを除いて、テストグループ5.6-3と同様の考慮事項が適用される。	
テストケース 5.6-4-1（概念）	本テストケースの目的は、DUTの物理的にアクセス可能なデバッグインターフェイスの概念評価。
テストケース 5.6-4-2（機能）	本テストケースの目的は、DUTの物理的にアクセス可能なデバッグインターフェイスの機能評価と、IXIT文書の完全性。

(3) ETSI TS 103 701 V1.1.1
詳細

テスト	テストグループ目的
テストグループ5.6-5：本規定を満たすには、主に3つのアプローチがある。1.消費者向けIoTデバイスの動作に必要なソフトウェアサービスのみを起動・管理するサービス管理フレームワークが設定されている場合。2. これらのソフトウェアサービスへのアクセスは、たとえそのサービスがアクティブであっても、パケットフィルタ（ファイアウォール）などのフィルタリングメカニズムによって防止される。3. デバイスの動作に必要でないソフトウェアサービスはインストールされない。	
テストケース 5.6-5-1（概念）	本テストケースの目的は、DUTの使用目的又は操作に関する有効なサービスの概念評価。
テストグループ5.6-6：コードの最小化は、選択した手法が実際にコードの最小化に役立っているか、どの程度役立っているか、コードの最小化の努力とセキュリティリスクの低減が比例しているかという観点から評価。	
テストケース 5.6-6-1（概念）	本テストケースの目的は、コード最小化手法の概念評価。
テストグループ5.6-7：IoT向けのOSの多くは、あるソフトウェアの実行に必要な権限を減らすことができる。このアプローチは、職務の分離、知る必要性、特権の最小化という3つの原則に依存している。権限を最小化できるかどうかは、最初の2つの原則の適用と、ハードウェア及びソフトウェア・プラットフォームが提供する機能の両方に依存する。	
テストケース 5.6-7-1（概念）	本テストケースの目的は、DUTの権限制御機構の概念評価。
テストグループ5.6-8：メモリのハードウェアレベルのアクセス制御機構を提供するために組み合わせることができる多くのオプションが存在する。グレーボックステストのレベルでは、メーカーから提供された文書、又は基板の目視検査及びハードウェア部品サプライヤーから提供された文書に基づいて評価することができる。	
テストケース 5.6-8-1（概念）	本テストケースの目的は、DUTのメモリへのアクセス制御のためのハードウェアレベルのメカニズムを概念的に評価。
テストグループ5.6-9	
テストケース 5.6-9-1（概念）	本テストケースの目的は、セキュア開発プロセスの概念評価と、実装の前提条件が確保されていることを確認すること。

TSO 5.7：ソフトウェアの整合性を確保

テスト	テストグループ目的
テストグループ5.7-1：本テストグループは、提供されたセキュリティ保証に基づき、検証メカニズムがソフトウェアを検証するのに適しているかどうかを評価し、その実装に関する証拠を提供するもの。本テストグループでは、耐タンパ性を実現するために、少なくとも整合性と信頼性を保証することが必要である。	
テストケース 5.7-1-1（概念）	本テストケースの目的は、DUTのセキュアブート機構の概念評価。
テストケース 5.7-1-2（機能）	本テストケースの目的は、DUTのセキュアブート機構の機能評価。
テストグループ5.7-2：本テストグループは、ソフトウェアの不正な変更が検出された場合に、指定されたエンティティにアラートが送信され、DUTの通信がアラート機能に絶対に必要なものに制限されているかどうかを評価。	
テストケース 5.7-2-1（概念）	本テストケースの目的は、警告メカニズムと、許可されていないソフトウェアの変更を検出した場合に通信を制限するメカニズムの概念評価。
テストケース 5.7-2-2（機能）	本テストケースの目的は、警告メカニズムと、許可されていないソフトウェアの変更を検出した場合に通信を制限するメカニズムの機能評価。

TSO 5.8：個人データが安全であることを確認

テスト	テストグループ目的
テストグループ5.8-1：本テストグループの目的は、第一に暗号方式が個人データの通信というユースケースに必要なセキュリティ保証を提供しているかどうか、第二に暗号方式が実現可能な攻撃に対して脆弱であることが知られていないかどうかを評価すること。	
テストケース 5.8-1-1（概念）	本テストケースの目的は、デバイスとサービス間で個人データを通信するために使用される暗号化の概念評価。
テストケース 5.8-1-2（機能）	本テストケースの目的は、デバイスとサービス間で個人データを通信するために使用される暗号化の機能評価。

(3) ETSI TS 103 701 V1.1.1
詳細

テスト	テストグループ目的
テストグループ5.8-2：本テストグループの目的は、第一に暗号方式が個人データの通信というユースケースに必要なセキュリティ保証を提供しているかどうか、第二に暗号方式が実現可能な攻撃に対して脆弱であることが知られていないかどうかを評価すること。	
テストケース 5.8-2-1（概念）	本テストケースの目的は、デバイスと関連サービスの間で機密性の高い個人データを通信するために使用される暗号化の概念評価。
テストケース 5.8-2-2（機能）	本テストケースの目的は、デバイスと関連サービスの間で機密性の高い個人データを通信するために使用される暗号化の機能評価。
テストグループ5.8-3：本テストグループでは、光学、音響、生体又は位置センサーなど、その周囲に関する情報を感知するDUTのあらゆる能力を明らかにすることを目的としている。	
テストケース 5.8-3-1（機能）	本テストケースの目的は、外部センシング能力の文書化とIXIT文書の完全性の機能評価。

TSO 5.9：停電に強いシステムの構築

テスト	テストグループ目的
テストグループ5.9-1	
テストケース 5.9-1-1（概念）	本テストケースの目的は、ネットワークと電力の供給停止に関する回復力機構の概念評価。
テストケース 5.9-1-2（機能）	本テストケースの目的は、ネットワークと電力の供給停止に関する回復力機構の機能評価。
テストグループ5.9-2	
テストケース 5.9-2-1（概念）	本テストケースの目的は、ネットワークや電力の供給停止、ネットワーク停止時のオペレーション、停電後の復旧に関するレジリエンスメカニズムの概念評価。
テストケース 5.9-2-2（機能）	本テストケースの目的は、ネットワークや電力の供給停止、ネットワーク停止時のオペレーション、停電後の復旧に関するレジリエンスメカニズムの機能評価。

テスト	テストグループ目的
テストグループ5.9-3：本テストグループの目的は、標準化された接続確立、及び大量の再接続から保護する機能について検討。	
テストケース 5.9-3-1（概念）	本テストケースの目的は、通信機構の耐障害性対策の概念評価。
テストケース 5.9-3-2（機能）	本テストケースの目的は、通信機構の耐障害性対策の機能評価。

TSO 5.10： システムテレメトリーデータの検証

テスト	テストグループ目的
テストグループ5.10-1：ETSI TS 103 645/ETSI EN 303 645によると、テレメトリーデータは製造者がDUTの使用に関連する問題、又は情報を特定するのに役立つ情報を提供することができる。	
テストケース 5.10-1-1（概念）	本テストケースの目的は、セキュリティ異常の検査の概念評価。

TSO 5.11：ユーザーが簡単にユーザーデータを削除できるようにす

テスト	テストグループ目的
テストグループ5.11-1	
テストケース 5.11-1-1（概念）	本テストケースの目的は、DUTのユーザーデータ消去機能の概念評価。
テストケース 5.11-1-2（機能）	本テストケースの目的は、DUTのユーザーデータ消去機能の機能評価。
テストグループ5.11-2：本規定は、個人データの削除のための機能が明確に特定され、容易に実行できることを意味する。	
テストケース 5.11-2-1（概念）	本テストケースの目的は、DUTの個人データ削除機能の概念評価。
テストケース 5.11-2-2（機能）	本テストケースの目的は、DUTの個人データ削除機能の機能評価。

(3) ETSI TS 103 701 V1.1.1
詳細

テスト	テストグループ目的
テストグループ5.11-3：ユーザーが期待する明確な指示の特徴として、簡潔さと正確さが挙げられる。	
テストケース 5.11-3-1（機能）	本テストケースの目的は、DUTの個人データ削除機能に関するユーザードキュメントの機能評価。
テストグループ5.11-4：明確な確認とは、要求された操作が正常に完了した場合に、肯定的なステートメントを伝える透明なメッセージを意味する。本テストグループの目的は、確認の設計を評価すること。	
テストケース 5.11-4-1（機能）	本テストケースの目的は、削除機能に関するユーザーの確認の機能評価。

TSO 5.12：デバイスのインストールとメンテナンスを容易に

テスト	テストグループ目的
テストグループ5.12-1：ユーザーによる最小限の決定を伴うということは、一部の決定手順がDUTにより自動化されることを意味する。ユーザビリティに関するセキュリティベストプラクティスは、決定手順が使用者に対して顕著に表示され（隠されない）、構成パラメータが安全な初期値を有することを必要とする。	
テストケース 5.12-1-1（概念）	本テストケースの目的は、ユーザーが行うインストールとメンテナンスの決定の概念評価。
テストケース 5.12-1-2（機能）	本テストケースの目的は、ユーザーが行うインストールとメンテナンスの決定の機能評価。
テストグループ5.12-2：ガイダンスとは、セキュリティに影響を与える設定パラメータを説明し、安全な設定を実現するためのパラメータの設定方法を推奨すること。	
テストケース 5.12-2-1（機能）	本テストケースの目的は、DUTを安全にセットアップするためのユーザーガイダンスの機能評価。
テストグループ5.13-1：デバイスが安全にセットアップされているかどうかを確認する方法は製品によって異なるため、テストグループはガイダンス文書の存在と、その主要な特徴である「アクセス可能、トピックが明確、簡潔、正確、検証基準が明確、ユーザーが再現可能」を確認することに焦点を合わせている。	
テストケース 5.12-3-1（機能）	本テストケースの目的は、DUTが安全にセットアップされているかどうかを確認するためのユーザーガイダンスの機能評価。

TSO 5.13：入力データ検証

テスト	テストグループ目的
テストグループ5.13-1：入力データの検証は、受信側が予期せぬ動作を起こすことなくデータを処理できることを保証する。これには、提供されたデータが正しいタイプ（許容されるデータ形式とデータ構造）であり、許容される値であり、許容される基数及び順序であることを検証することが必要である。	
テストケース 5.13-1-1（概念）	本テストケースの目的は、DUTのデータ入力検証方法の概念評価。
テストケース 5.13-1-2（機能）	本テストケースの目的は、DUTのデータ入力検証方法の機能評価と、IXIT文書の完全性。

TSO 6：消費者向けIoTのデータ保護

テスト	テストグループ目的
テストグループ6-1	
テストケース 6-1-1（概念）	本テストケースの目的は、個人データの処理に関するユーザー情報の概念評価。
テストケース 6-1-2（機能）	本テストケースの目的は、個人データの処理に関するユーザー情報の機能評価。
テストグループ6-2：ETSI TS 103 645/ETSI EN 303 645によると、「有効な方法で」同意を得るには、通常、消費者が自分の個人データを特定の目的で使用するかどうかを自由かつ明白に選択できるようにすることが必要。	
テストケース 6-2-1（概念）	本テストケースの目的は、個人データの処理に対する消費者の同意の概念評価。
テストケース 6-2-2（機能）	本テストケースの目的は、個人データの処理に対する消費者の同意の機能評価。

(3) ETSI TS 103 701 V1.1.1
詳細

テスト	テストグループ目的
テストグループ6-3：ETSI TS 103 645/ETSI EN 303 645によると、いつでも同意を撤回するには、通常、IoTデバイスとサービスの機能を適切に設定することが必要。	
テストケース 6-3-1（概念）	本テストケースの目的は、個人データの処理に対する消費者の同意を撤回する概念評価。
テストケース 6-3-2（機能）	本テストケースの目的は、個人データの処理に対する消費者の同意を撤回する機能評価。
テストグループ6-4	
テストケース 6-4-1（概念）	本テストケースの目的は、テレメトリーデータの処理の概念評価。
テストグループ6-5	
テストケース 6-5-1（概念）	本テストケースの目的は、テレメトリーデータの処理に関するユーザー情報の概念評価。
テストケース 6-5-2（機能）	本テストケースの目的は、テレメトリーデータの処理に関するユーザー情報の機能評価。

(4) Guidelines for Securing the Internet of Things
概要

文献概要	名称	Guidelines for Securing the Internet of Things		
	主旨	IoTのサプライチェーンのセキュリティを確保するためのガイドラインを定義し、IoTの専門家の意見を取り入れながら、要件や設計から、最終用途での納品やメンテナンス、廃棄に至るまでの全ライフサイクルを対象としたセキュリティガイドライン。		
	国・地域	欧州	適用分野	IoTサプライチェーン
	策定者	ENISA	対象者	IoTソフトウェア開発者とメーカー、情報セキュリティの専門家、IT・セキュリティソリューションアーキテクト、最高情報セキュリティ責任者、重要情報基盤保護専門家、プロジェクトマネージャー、調達チーム
	遵守義務	IoTサプライチェーンのセキュリティーに関するグッドプラクティスを示しいる内容であり、遵守義務はない。つまり、接続されたモノを構築する際に生じ得る脆弱性から組織を保護するために、IoTサプライチェーン全体における推奨事項を定めている。		
	普及状況	普及状況に関する情報はなかったが、IoTメーカー、開発者、インテグレーター、及びIoTのサプライチェーンに関与するすべての利害関係者を対象としている。		
	策定年	2020年	ページ数	52ページ

カテゴリ	カテゴライズ	「アクター」（サプライチェーンのアクターとしては、業界の専門家（マネージャー、エンジニアなど）、エンドユーザー、組織など）、「プロセス」（IoTプロジェクトの設計、開発、導入、保守に関わるプロセス）、「テクノロジー」（脆弱性や脅威を予測、検出、低減するために適用できる潜在的な技術的手段や要素）の3項目に分類。
	カテゴリ評価	上記3項目のグッドプラクティスについての記述となっている。
	カテゴリ確認要求	「アクター間のより良い関係の構築」、「サイバーセキュリティの専門性をさらに高めるべき」、「設計によるセキュリティ」、「セキュリティに対する包括的かつ明確なアプローチをとる 」、「既存の標準とグッドプラクティスを活用」という項目において、最も適切な基準を示している。
	制度的枠組み	2019年にENISAがリリースした「Good Practices for Security of IoT - Secure Software Development Lifecycle 」に基づき、IoT製品の開発に活用されるサプライチェーンの実際のプロセスに焦点を当てている。また、ENISAの「Baseline Security Recommendations for IoT」も引用している。

関連URL	https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

(4) Guidelines for Securing the Internet of Things 詳細

【セキュリティ向上のためのグッドプラクティス】

本文献では、アクター、プロセス、テクノロジーの3つの主要グループに分類してベストプラクティスを提言。

- **アクター：**サプライチェーンのアクターとしては、業界の専門家（マネージャー、エンジニアなど）、エンドユーザー、組織などを挙げることができる。
- **プロセス：**IoTプロジェクトの設計、開発、導入、保守に関わるプロセスにおけるセキュリティを扱う。
- **テクノロジー：**脆弱性や脅威を予測、検出、低減するために適用できる潜在的な技術的手段や要素。

アクター

番号	内容
ACT-01	**セキュリティ保証のあるサプライヤーとの取引を優先** この脅威は、ISO 27036やISO 28000などの規格、あるいはNISTIR 8259などの勧告を実施している企業を優遇することで最小化することができる。
ACT-02	**透明性の向上に向けた取り組み** ステークホルダー、特にサプライヤーは透明性を保ち、供給される製品の動作や正常な動作について明確で詳細な情報を提供する必要がある。
ACT-03	**革新的な信頼モデルを開発** 各ステークホルダーは、それぞれのニーズと専門性に応じて最低限の信頼性を確立し、データの流れを分析し、自社のサービスや製品におけるセキュリティとプライバシーを保証する必要がある。
ACT-04	**サプライチェーンにおけるセキュリティを継続的なプロセスとする** セキュリティは継続的かつ反復的なプロセスとして、サプライチェーンのすべての段階に含める必要がある。
ACT-05	**有能で熟練した労働力を維持・育成** ほとんどの組織には、セキュリティのみを専門とする専門家チームが存在する必要がある。
ACT-06	**リスクベースアプローチに重点を置いた開発者ワークカルチャーの推進** リソースを配分する際にリスクを考慮し、セキュリティに適切な注意を払うような開発プロセスを推進することは、サプライチェーンのセキュリティに大きな影響を与える。
ACT-07	**ユーザーへのIoTセキュリティ啓発推進** 適切なセキュリティの重要性を認識させるためのキャンペーンやアクションにリソースを投資することは、組織にとって有益なこととなる。
ACT-08	**顧客にセキュリティの約束を提供** 顧客は、セキュリティに関する包括的な情報を明確かつ明示的に提供されるべきである。

プロセス

番号	内容
PRO-01	**設計原則によるセキュリティの採用** セキュリティモジュールは優先順位の高いコンポーネントと考え、サプライチェーン全体を通して最初の段階から設計プロセスに組み入れるべきである。
PRO-02	**データ収集、計測技術、データマネジメントの確立と改善** すべてのステークホルダーがセキュリティ監査や分析を行うリソースを持っているわけではないので、大半はある時点で信頼仮定を実行する。エンドユーザーのプライバシーを保証しつつ、実行可能な限りこれらの仮定を最小化することが望ましい。
PRO-03	**サプライチェーンの整合性指標作成** サプライチェーンの状態を可視化するために指標を作成し、継続的に監視することができる。これらの指標は現在のサプライチェーンに特化したものであっても、より水平的なものであってもよい。
PRO-04	**サプライチェーンの脅威モデルを開発** 脅威モデルは、サイバーフィジカルシステムに内在する物理的安全性とデジタルセキュリティの両方の概念を融合する必要がある。
PRO-05	**サードパーティソフトウェアの特定** サードパーティソフトウェアの使用は、サプライチェーンのセキュリティにとって脅威となる不確実性をもたらす。これらのソフトウェア・コンポーネントは、サプライチェーンのセキュリティ・プロセスの一部として、その選択に従った基準を含めて文書化されなければならない。
PRO-06	**包括的なテストプランを確立** すべてのIoTソリューションには、製品がソフトウェアとハードウェアの両方で期待される機能を表示することを検証するための包括的なテストプランが含まれている必要がある。

(4) Guidelines for Securing the Internet of Things 詳細

番号	内容
PRO-07	**デフォルトでセキュリティを使用する工場出荷時設定の実装** デフォルトでのセキュリティは、製造者やサプライヤーのアプローチであるべきで、セキュリティを無効にする必要がある顧客は、意識的かつ明確な方法でそれを行う必要がある。
PRO-08	**一定期間、セキュリティパッチを提供することを約束** IoT製品の設計や計画には、延長サポートやセキュリティパッチのタイムリーな提供を考慮する必要がある。 製造者にはセキュリティ配信の義務があり、少なくとも保証期間終了まで、できればサポート期間終了までパッチを適用する。
PRO-09	**安全なスクラップ管理プロセスを統合** 製造・加工段階で発生した材料や部品で品質検査に不合格となったもの、又は何らかの理由で生産に適さないと判断されたものは、安全な方法で処理・廃棄されること。
PRO-10	**安全なデータ削除技術を使用** デバイスは通常、工場出荷時の設定に戻され、廃棄・復旧の段階で全ての個人ユーザーデータが消去される。全ての個人ユーザーデータと構成データが安全な方法で効果的に削除されることを保証するために、安全なデータ消去技術をこれらの段階に統合する必要がある。
PRO-11	**包括的なドキュメントリソース作成** ヒューマンエラーに対処するための包括的な文書リソースを構築し、特に構成管理と障害後の復旧の側面について、各成果物で実施すべき明確なガイドライン又はアクションポイントを含める。
PRO-12	**IoT向けサプライチェーンの標準を開発・適応** 現状では、あらゆる業界のIoTのサプライチェーンを保護するという目的に完全に合致する規格はない。ISO 27001やNERC CIP-013-1のような一部の規格は、かなりオープン又は汎用的であると考えられる。 新たな標準の開発や既存標準の適応は、IoTのグローバルサプライチェーンのセキュリティ管理に一貫性を与え、すべてのアクター間のセキュリティ情報の統合を改善することに寄与する。
PRO-13	**IoTデバイスのソフトウェア部品表（SBOMS）の提供** SBOMは、理想的には商業的に流通されているか否かにかかわらず、あらゆる組織のすべてのIoT製品で利用可能であるべきである。

テクノロジー

番号	内容
TEC-01	**デバイスのアップグレード可能性と陳腐化の計画・管理を確立・改善** 通常、IoTソリューションでは数世代のデバイスやソフトウェアが共存し、陳腐化しないよう、また異なるレベルのセキュリティや安全性に対処しないよう更新する必要がある。サプライチェーンの範囲は、特にOTAアップデートが含まれる場合、接続されたデバイスの寿命が尽きるまで拡張される必要がある。
TEC-02	**セキュリティ管理と監査に新しいテクノロジーを活用** 新技術は、IoTサプライチェーンの可視化に役立つ可能性があり、少なくとも評価する必要がある。組織はアプリケーションにコミットする前に、まずセキュリティの観点からその実行可能性を評価する必要がある。
TEC-03	**ハードウェアメカニズムによる内部検証** リバースエンジニアリングや過剰生産などの脅威から保護するために、回路設計プロセスにハードウェア難読化技術を統合する。
TEC-04	**ソフトウェア・インテグリティ対策の存在を要求するSLAの採用を支持** セキュアブートとファームウェア署名は、改ざんに対する一定の保護を提供するセキュリティ対策である。
TEC-05	**IoTデバイス用の統合ID管理システム** すべてのIoTデバイスを一意に識別する機能は非常に重要であり、サプライチェーンの可視性と説明責任に大きな影響を及ぼす。そのため、ID管理システムをサプライチェーンに統合して、これらの一意の識別子を提供する必要がある。
TEC-06	**信頼の強力なルートを統合** ルート・オブ・トラストは、デバイスの信頼の連鎖における最初の項目であり、一般的には、デバイスが信頼できると仮定できる一連の暗号機能及びプリミティブを提供する専用のハードウェアコンポーネントを使用して実装される。IoTサプライチェーンにおけるアクター（OSプロバイダ、アプリケーション開発者等）は、可能な限りこのセキュリティ基盤をベースに貢献することが望まれる。

(4) Guidelines for Securing the Internet of Things 詳細

番号	内容
TEC-07	**リモートアップデートを実現** サプライチェーンのセキュリティプロセスにおいて、現場のデバイスに遠隔地から自動でアップデートを適用する機能は非常に重要となる。環境の変化に迅速に対応し、リモートデバイスのアップデートを展開する能力は、設計の初期段階から含まれ、考慮されなければならない。さらに、これらメカニズムは誤用やマルウェアの侵入を防ぐために安全でなければならない。
TEC-08	**認証メカニズムを回路に統合** トレーサビリティと保守性をサポートするために、機器認証は必須である。PUF（Physical Unclonable Functions）は、最も重要なオプションの一つである。
TEC-09	**ハードウェアとソフトウェアの協調がもたらすサイバーセキュリティの可能性を考慮** ハード・ソフト協調方式は、ハードウェアやソフトウェア層のみで動作するセキュリティ対策で生じるサイバーセキュリティ上のギャップをカバーすることに重点を置いたアプローチである。

【ガイドラインと結論】

以下では、グッドプラクティスとスタンダードの分析から抽出された一般的な結論を反映させている。

	考慮すべきグッドプラクティス	最も適切な基準
アクター間のより良い関係の構築	• サイバーセキュリティを保証するサプライヤーとの取引を優先 • 透明性の向上に努力 • 革新的な信頼モデルを開発 • サプライチェーンのセキュリティは継続的なプロセスであるという考え方を採用 • ソフトウェアのインテグリティ確保を義務付けるSLAの採用支持 • 顧客にセキュリティに関する約束をする	• ISO/IEC 27001：情報セキュリティマネジメントシステムに対する要求事項 • ISO 27036：サプライヤー関係の情報セキュリティ
サイバーセキュリティの専門性をさらに高めるべき	• 有能で熟練した労働力を維持・育成 • リスクベースのアプローチに焦点を当てた開発者のワークカルチャーを促進 • ユーザーに対するIoTセキュリティの啓発を推進	• NIST8276：サイバーサプライチェーンリスクマネジメントのキープラクティス
設計によるセキュリティ	• セキュリティ・バイ・デザインの原則を採用 • データ収集、測定技術、データ管理の確立・改善 • サプライチェーンの整合性に関する指標作成 • セキュリティ管理及び監査のための新技術活用 • デバイスのアップグレード可能性と陳腐化に関する計画と管理を確立・改善 • リモートアップデートのメカニズムを実装 • IoTサプライチェーンの脅威モデル開発	• ISO 20243：悪意を持って汚染された製品や偽造品に関連する脅威に対する規格
セキュリティに対する包括的かつ明確なアプローチをとる	• サードパーティソフトウェアを特定 • 包括的なテスト計画立案 • デフォルトでセキュリティを使用する工場出荷時設定を実施 • セキュリティパッチを一定期間提供 • 安全なスクラップ管理プロセス導入 • 安全なデータ削除技術の使用 • ハードウェアメカニズムによる内部検証 • IoTデバイスのID管理システムを統合 • 強力なルート・オブ・トラスト導入 • 回路に認証機構組み込み • ハード・ソフト協調方式 • IoTデバイスのソフトウェア部品表提供 • 包括的なドキュメントリソース作成	• ISO 11889：信頼できるプラットフォームモジュール • IETF RFC 8520: 製造者使用説明書 • IEEE 802.1AR-2018: ローカル及びメトロポリタンエリアネットワーク向けのセキュアなデバイスID • ISO 20243：悪意を持って汚染された製品や偽造品に関連する脅威に対する規格

(4) Guidelines for Securing the Internet of Things 詳細

	考慮すべきグッドプラクティス	最も適切な基準
既存の標準とグッドプラクティスを活用	• IoTのためのサプライチェーンの標準を開発・適応	• GSMA SAS-UP:UICC製造のセキュリティ認定スキーム • CMU SPL：セキュリティ＆プライバシー・ラベル

(5)Recommendations for the security of CAM
概要

文献概要	名称	Recommendations for the security of CAM（コネクテッド及びモビリティのセキュリティに関する推奨事項）		
	主旨	CAM（コネクテッド及びモビリティ）分野におけるサイバーセキュリティの課題をハイレベルで概観し、CAMに関わる関係者と関連する推奨事項を紹介。本文献は、現状における主な課題を明らかにし、欧州におけるCAMのインフラやシステムのセキュリティレベルと回復力を高めるために、CAMのエコシステムに関わる様々な関係者に対して実行可能な推奨を提示している。		
	国・地域	欧州	適用分野	オートモーティブ業界
	策定者	ENISA	対象者	オートモーティブ製造者及び関係者
	遵守義務	コネクテッド・モビリティとオートメーション・モビリティのセキュリティに関する様々な推奨事項についての言及。		
	普及状況	欧州連合では、2022年7月からサイバーセキュリティに関する新規制が義務付けられ、2024年7月から生産されるすべての新型車両にCAMが義務付けられる予定。さらに、UNECE規則と関連するISO規格は、自社の製品やサービスがサイバーセキュリティの目標に適合していることを保証しなければならないすべてのCAM関係者に適用される。		
	策定年	2021年	ページ数	23ページ

カテゴリ	カテゴライズ	「ガバナンスとサイバーセキュリティの企業活動への統合 」、「トップマネジメントのサポートとサイバーセキュリティの優先度欠如 」、「CAMエコシステムの技術的複雑性」、「CAMへのセキュリティ実装のための技術的制約 」、「断片的な規制環境」、「CAMサイバーセキュリティのための専門知識と熟練したリソースの不足」、「CAM関係者間のセキュリティ問題に関する情報共有と協調の欠如」で構成。
	カテゴリ評価	各々のカテゴリーについての現状の課題と共に、ENISAの推奨事項、及び関連する企業・機関・団体を明示。
	カテゴリ確認要求	オートモーティブ製造者及び関係者に対する推奨事項となっており、企業内における体制整備などが要求されている。
	制度的枠組み	「断片的な規制環境」において、オートモーティブ業界に関連するISO 27035、ISO/SAE 21434, ISO 26262, SAEJ 3061, ISO 21177, ISO 21184、ISO 21185、ETSI TC ITS、IEEE802.11bd、ISO/IEC 15408、ISO 27001、ISO/SAE 21434、ISO 21434、ISO 26262などが挙げられている。ただ、本文献はこうした断片化した規制環境を整理することを目的の一つにしている。

関連URL	https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam

(5)Recommendations for the security of CAM
詳細

本書CAMエコシステムの関係者

- 協会
- オートモーティブ・アフターマーケット事業者
- モビリティサービスプロバイダー
- 国家機関
- 高度道路交通システム事業者
- OEM企業
- 政策立案者
- 規制機関
- 道路管理者
- 道路機器メーカー
- スマートシティ事業者
- 標準化団体
- システムインテグレーター
- システムプロバイダー
- Tier1及びTier2サプライヤー

CAM領域におけるサイバーセキュリティの課題と推奨事項

章番号	内容
2.1	ガバナンスとサイバーセキュリティの企業活動への統合
2.1.1	推奨事項 • サイバーセキュリティとテクノロジーがCAMエコシステムのライフサイクルに与える影響について、適切な場合には組織のトップマネジメントレベルまで意識を向上させる。 • サイバーセキュリティとテクノロジーがCAMエコシステムのライフサイクルに与える影響について、組織全体、特に企業やグループ内の適切な意思決定レベルにおいて認識を高める。 • 組織内の役員レベルにおいて、デジタルトランスフォーメーションと共にサイバーセキュリティの統合を推進。 • 組織の役員レベルで、サイバーセキュリティなど、変化の激しいビジネスや技術に関するトピックを恒常的にアドバイスする。 • サイバーセキュリティの発展に対応するため、CAM技術の研究開発費におけるサイバーセキュリティの加速を推進。 • サイバーセキュリティのリスク指向の要件を統合するための調達プロセスを推進。 • サイバーセキュリティのスキル育成に対処。 • サイバーセキュリティ部門以外の関連する組織内部門においても、サイバーセキュリティに関する明確な役割と責任を定義。 • ビジネスプロセスとサポートプロセスの両方について、資産のサイバーセキュリティの必要性を考慮。
2.1.1 続き	• 製品・サービスのライフサイクルを通じたリスク評価、処置の決定、及び所有権を可能にするリスク管理プロセスを定義。 • 異なるチーム間の協力体制を確立し、プロジェクトやビジネスプランニングにおいてサイバーセキュリティの活動を考慮。

章番号	内容
2.2	トップマネジメントのサポートとサイバーセキュリティの優先度欠如
2.2.1	企業トップによるサイバーセキュリティの優先順位の向上、サイバーセキュリティの資金調達と予算配分の改善を促進するため、以下を推奨事項とする。 • 経営トップ層がサイバーセキュリティの専門家やCISO（最高情報セキュリティ責任者）と議論し、意見交換するための管理体制を確立。 • IT及びCAM環境、コンポーネント、システム、サービスを保護するための技術革新と研究開発活動にインセンティブを付与。 • 自動車業界の慣行から学ぶことで、企業の事業戦略におけるセキュリティの側面を促進。 • 市場の調和を図り、消費者の信頼を高め、新しいビジネスチャンスを開拓するために、自動車業界のセキュリティに関する認証制度の開発を検討。 • サイバーセキュリティを経営委員会に直接参加させ、企業のセキュリティ文化を醸成。 • サイバーセキュリティの法的要件、想定される脅威、リスク、セキュリティ対策に関する認識を高めるために、トップマネジメントを含む企業の様々な階層に対して、定期的なトレーニングプログラムを確立。 • 自動車アフターマーケットとサービス部門の中小企業を対象としたサイバーセキュリティ情報と認証スキームを開発。CAMエコシステムに関与するすべての利害関係者のための共通の要件と責任を定義。 推奨事項の対象は以下の通り。 • オートモーティブ・アフターマーケット事業者 • 高度道路交通システム事業者 • OEM企業 • 道路機器メーカー • スマートシティオペレーター • Tier1及びTier2サプライヤー

(5)Recommendations for the security of CAM
詳細

章番号	内容
2.3	CAMエコシステムの技術的複雑性
2.3.1	技術的な複雑さを克服するため、以下を推奨事項とする。 • サイバーセキュリティの最低レベルを遵守し、適切なセキュリティレベルを確保するため、コンポーネントやサービス間で共通のセキュリティ対策の利用を促進。 • 適切な認証制度の利用を推進。 • オンボードとオフボードの両方のソリューションに対するセキュリティ評価を推進し、製品のライフタイムにおける脆弱性の発見と是正を標準化。 • 組織が一貫性のある最新の資産目録を維持することを確実化。 追加推奨事項 • 脅威情報の共有、監視結果やサイバーセキュリティインシデントの報告、CAMを標的としたサイバー犯罪行為に関するエコシステム関係者間の協力を可能にするための業界標準の定義を検討。 • データセキュリティ戦略（プライバシー遵守メカニズム）の適用を検討し、CAMのエコシステム全体に対して最低レベルのセキュリティ対策を要求。 • CAMエコシステムの組織に固有資産を自動的に発見、識別、列挙できる資産管理支援ツールを使用。 • ハードウェア、ソフトウェア、又は構成に適用される変更がサイバーセキュリティに与える潜在的な影響について評価され、検証されることを確認するため、CAMエコシステムに変更管理プロセスが実装されることを確実化。 • 新製品開発のコンセプト段階から、OEMやサプライヤーの開発プロセスに標準的な成果物として組み込まれるサイバーセキュリティの要件と検証方法を確立。 • より高いセキュリティレベルを実現するため、サイバーセキュリティ認証を受けたコンポーネントが存在する場合は、その使用にインセンティブを付与。 推奨事項の対象は以下の通り。 • オートモーティブ・アフターマーケット事業者 • OEM企業 • 道路機器メーカー • スマートシティオペレーター

章番号	内容
2.3.1 (続き)	• システムインテグレーター • システムプロバイダー • Tier1及びTier2サプライヤー
2.4	CAMへのセキュリティ実装のための技術的制約
2.4.1	CAMのセキュリティを確保し、技術的な制約を緩和するための対策を適用する推奨事項。 • 方法論的なリスク評価に基づき、CAM製品・サービスのセキュリティモデルを定義。 • 標準部品及び／又は共通部品の使用へのコミットメントを確保。 • CAM製品及びサービスのライフサイクルを通じて、リスク評価後に関連するセキュリティ対策を適切に実施し、リスク評価を最新の状態に保つようにすること。 • リスク評価方法、設計原則、セキュリティ対策一式、情報セキュリティポリシーなど、すべての関係者に共通するルールを導入。 • CAMのすべてのコンポーネント、デバイス、サービス、プロトコル、通信、プロセスに対して、デフォルトでセキュリティバイデザインの原則を適用。 • リスクアセスメントに基づき、CAM製品及びサービスのセキュリティ目標が満たされていることを確認するために、検証テスト及び侵入テストを実施。 • 導入されたサイバーセキュリティソリューションの成熟度を定期的に評価。 • 現在進行中の脅威や新たに発生する脅威に対処し、監視するために、サイバーセキュリティのインシデント対応構造を全体的に構築。 • CAM製品及びサービスのライフサイクルにおける中心的なセキュリティメカニズムとして、継続的かつ安全な更新及びアップグレードの可能性を確立。 • 自動車の運行開始後に後付けで追加される可能性のあるソフトウェア機能を開発するOEMやISPが講じるセキュリティ対策の互換性を確保。 • フェイルセーフを原則とするCAM製品・サービスにおいて、フェイルセーフ機構を用いたインシデントレスポンスを可能とする。 • CAMエコシステムのサイバーセキュリティ標準とベストプラクティスの開発を追跡。

(5)Recommendations for the security of CAM
詳細

章番号	内容
2.4.1	• 相互信頼を確立し、最先端技術を実証するために、適切な認証スキームを使用。 • 新しい脅威が発見された場合、脅威モデルを定期的に更新。 推奨事項の対象は以下の通り。 • オートモーティブ・アフターマーケット事業者 • 高度道路交通システム事業者 • OEM企業 • システムインテグレーター • システムプロバイダー • Tier1及びTier2サプライヤー
2.5	断片的な規制環境
2.5.1	規制環境に関する取り組みを調和させ、完全なCAMエコシステムに対する責任と要件を定義するため、以下を推奨事項とする。 • CAMのサイバーセキュリティに関するEUの法的環境を均質、詳細、安定的なものとし、すべての関係者がセキュリティの側面を含み、長期的で持続的な事業戦略を計画できるようにする。 • 政策決定のすべてのレベルに渡って国の基準及び責任を明確にし、安全な製品及びサービスの開発を促進しながらイノベーションへの障壁を減らすために、新しい調和のとれた法律及びガイダンスの開発に参加。 • オートモーティブ関連の現行規制を分析し、潜在的なギャップを検証。 • 関連する技術基準及び規制の開発におけるコンセンサスを獲得するため、オートモーティブ業界の利害関係者間との対話を促進。 • 相互運用性を含む、オートモーティブ業界のセキュリティに総合的に取り組む標準化活動への取り組みを促進。 • オートモーティブ関連の現行規格の分析を実施し、潜在的なギャップを調査。 • 標準化活動間のマッピングスキーム（ENISAとUNECE によるものなど）を開発・維持し、標準間の共通性と相乗効果を探る。 • CAMエコシステムにおけるサイバーセキュリティの取り組みを支援するため、標準化活動などの協力活動に対する財政支援を含む資金調達スキームを立ち上げる。 • 基準や要求事項の適切な実施を確保するための方策を検討。

章番号	内容
2.5.1 (続き)	• オートモーティブ・アフターマーケット事業者のアクセス権、情報要件、認可スキームを定義。 • コンポーネントの装着を可能にする標準化に基づき、サイバーセキュリティに関する明確な要件を定義し、それによってエコシステム全体の相互運用性を促進。 • 調和モデル候補の評価基準の確立を検討。 推奨事項の対象は以下の通り。 • 国家機関 • 政策立案者 • 規制機関 • 道路管理者
2.6	CAMサイバーセキュリティのための専門知識と熟練したリソースの不足
2.6.1	セキュリティの専門知識やガイダンスに関する部門横断的な知識を促進するため、以下を推奨事項とする。 • IT/OT（オペレーショナルテクノロジー）とモビリティのそれぞれの専門家の間で、部門横断的なセキュリティと安全に関する知識交換を促進。 • IT/OTとモビリティシステムを安全に融合するための最先端技術、ベストプラクティス、方法論、ツールに関する知識を含む、モビリティ産業におけるセキュリティ教育・訓練を開始。 • モビリティ業界のセキュリティに特化したオーダーメイドのトレーニングコースを確立し、トレーニングの効果を高め、モビリティとIT/OTのセキュリティ専門家が関連するサイバーセキュリティの問題をより効率的に解決できるように支援。 • 全職員を対象としたモビリティ業界特有の意識・教育トレーニングを提供するため、能力プロファイルを開発。 • 業界全体のセキュリティと安全に関する知識の不足に対処するため、学校や大学でプログラムを導入する。 • 職員向けのサイバーカルチャーとサイバー衛生の紹介コースを編成。 • コースをサプライチェーン全体に拡張、又はサプライチェーンのすべての部分でサイバーセキュリティのトレーニングを含むことを企業に義務付け。 • 職業プロファイルにサイバーセキュリティを含め、企業文化を強化。 • 情報共有・分析センターなどの情報交換プログラムに参加し、情報知識とグッドプラクティスの交換をさらに高める。

(5)Recommendations for the security of CAM

詳細

章番号	内容
2.6.1 (続き)	推奨事項の対象は以下の通り。 • オートモーティブ・ アフターマーケット事業者 • 国家機関 • 高度道路交通システム事業者 • OEM企業 • 政策立案者 • 規制機関 • 道路管理者 • 道路機器メーカー • スマートシティ事業者 • システムインテグレーター • システムプロバイダー • Tier1及びTier2サプライヤ
2.7	CAM関係者間のセキュリティ問題に関する情報共有と協調の欠如
2.7.1	CAMエコシステムの関係者間の情報共有を確実とするため、以下を推奨事項とする。 • 既存及び今後設立される可能性のあるEUのISAC（情報共有分析センター）の内部、及び相互間で分析能力を開発することを検討。 • 今後設立される可能性のあるISACでの協力を模索し、開始する。 • 欧州CSIRTネットワークを含む、コンピュータセキュリティインシデント対応チーム（CSIRT）のコミュニティとの協力関係模索を検討。 • EUの機関や団体、法執行機関、他の業界団体、さらに協会や通信事業者に限定せず、適切なステークホルダーのISACへの参加を検討。 • 情報共有のためのグッドプラクティスや、CAM業界（特にオートモーティブのサプライチェーン）に関連する可能性のある攻撃や脅威に関する知識を交換するため、他のセクターの関係者やEU全体のISACとの協力インターフェース作成を検討。 • 関連するCAMステークホルダーからのサイバーセキュリティ互換性情報が、要求に応じて権限を有するすべてのCAMステークホルダーに提供されることを法的に確保。

章番号	内容
2.7.1 (続き)	すべての関係者が最低限のセキュリティレベルを確保できるよう、サイバーセキュリティ情報の相互運用性をカバーする業界標準又は最低要件を適応させる。 推奨事項の対象は以下の通り。 • オートモーティブ・アフターマーケット事業者 • 高度道路交通システム事業者 • OEM企業 • 道路機器メーカー • スマートシティ事業者 • システムインテグレーター • システムプロバイダー • Tier1及びTier2サプライヤー

(6)Cybersecurity Certification Guide

概要

文献概要	名称	Cybersecurity Certification Guide		
	主旨	シンガポールのサイバーセキュリティ庁が推進する「サイバーセキュリティラベル制度」などに関する文書。本制度では、スマートデバイスがサイバーセキュリティ対策のレベルに応じて評価される。		
	国・地域	シンガポール	適用分野	消費者向けIoTデバイス
	策定者	The Cyber Security Agency of Singapore (CSA)	対象者	製造者
	遵守義務	国内向けガイドラインであり、遵守義務はない。ただ、競合他社との差別化において有利に働く。特に、国家IT評価スキームは政府調達で必須。		
	普及状況	シンガポールのサイバーセキュリティ庁とフィンランドの運輸通信庁が発行するサイバーセキュリティラベルを相互に承認する覚書を締結。このMoUに基づき、フィンランドのサイバーセキュリティラベルの要件を満たしたコンシューマーIoT製品は、シンガポールのサイバーセキュリティラベル制度のレベル3の要件を満たしているとされている。シンガポール国内では、まずWi-Fiルーターとスマートホームハブにサイバーセキュリティ・ラベリングスキームを導入する計画。2022年2月12日時点で、56の製品が同スキームの認証を受けている。		
	策定年	2021年	ページ数	11ページ

カテゴリ	カテゴライズ	「シンガポールのコモンクライテリアスキーム」と「サイバーセキュリティ・ラベリングスキーム」、「国家IT評価スキーム」で構成。
	カテゴリ評価	サイバーセキュリティ・ラベリングスキームでは、4つのレベル（セキュリティ・ベースライン要件、ライフサイクル要件、ソフトウエア・バイナリ分析、ペネトレーションテスト）で評価。
	カテゴリ確認要求	国家IT評価スキームは、シンガポール政府調達において求められる。サイバーセキュリティ・ラベリングスキームは、対象製品にセキュリティレベルのラベルが貼られ、セキュリティー性を消費者が認知できる。
	制度的枠組み	コモンクライテリアスキームはISO / IEC 15408、ISO/IEC 17025など、サイバーセキュリティ・ラベリングスキームではレベル1においてETSI EN 303 645に基づくセキュリティ・ベースライン要件、国家IT評価スキームはISO / IEC15408やコモンクライテリアといった枠組みを基礎としている。

関連URL	https://www.csa.gov.sg/-/media/Csa/Documents/CLS/CSA-Cybersecurity-Certification-Guide.pdf https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-certification-centre

(6)Cybersecurity Certification Guide
詳細

シンガポールのコモンクライテリアスキーム
（SCCS：Singapore Common Criteria Scheme）

SCCS概要とベネフィット
SCCSは、国際市場を対象とした商用IT製品の認証制度。

ユーザー向けベネフィット：
デジタル資産とサービスの安全性向上
製品のセキュリティ評価が一貫して公平、かつ国際標準に従って行われていることを保証

開発者向けベネフィット：
規制要件に対応
重複した評価の負担なく市場参入が可能
より安全な製品を開発し、差別化を図る

資料#1：スキーム概要（https://bit.ly/3GdKusq）
スキームの目的
- IT製品の評価が高い水準で一貫して行われ、これらの製品のセキュリティに対する信頼に大きく貢献すると見なされるようにすること。
- 評価され、セキュリティが強化されたIT製品の利用可能性を向上させること。
- IT製品の評価を重複して行う負担をなくす。
- IT製品の評価・認証プロセスの効率と費用対効果を継続的に向上させる。
- 設置目的
- IT 製品の開発者又はIT製品の評価を希望する者が、関連するST（セキュリティ・ターゲット）に規定される製品のセキュリティに関する主張について独立した確認を得ること。
- 消費者が自らの特定のIT環境で使用するために適切なセキュリティ製品を選択すること。
- 評価者がCCRAとCCに従ってITセキュリティの評価結果を独立に確認すること。

TOE（ターゲット・オブ・エバリュエーション）評価
- STは、まずその内部整合性、TOEが提供すると主張する対策の十分性、及び運用環境を判断するために評価される。STの評価は、CC CEMに定義されたセキュリティターゲット評価活動（ASE：Assurance class for Security Target Evaluation）に従い、CC Part 3 に定義されたセキュリティターゲット評価基準を用いて実施される。
- 次に、TOEの設計文書や開発者の試験結果などのTOE評価エビデンスに保証クラスの要件（SARs：Security Assurance Requirements）を適用し、TOEの正しさを評価する（詳細はCC Part 3を参照）。

資料#2：テストラボ承認要件（https://bit.ly/3AX6GWZ）
仮承認・承認されたCCTL（Common Criteria Test Laboratory）の資格基準と義務

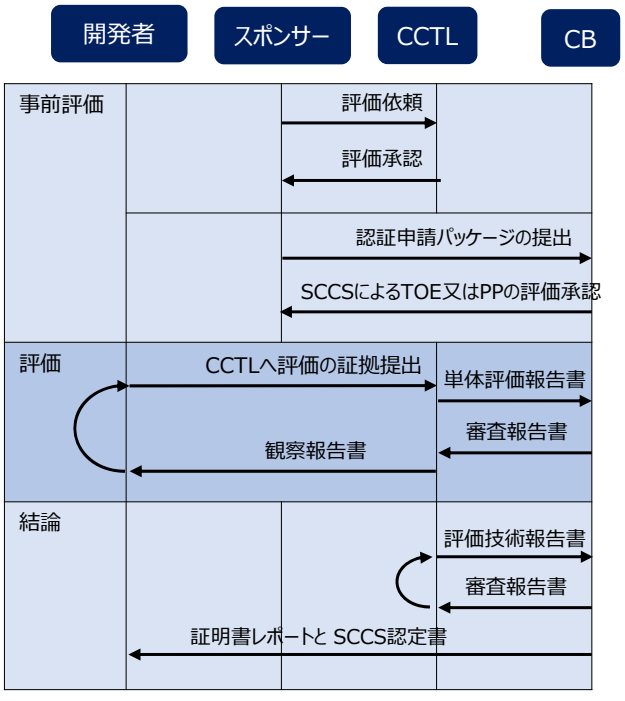
- 評価ラボはITセキュリティ評価のコモンクライテリアに従い、ITセキュリティ分野の試験所として、シンガポール認定評議会、又は他の認定機関によりISO/IEC 17025に従って認定あるいは認定中（ローカルラボにのみ適用）であること。公認認定機関は、国際認定機関フォーラム及び国際試験所認定協力機構のメンバーでなければならない
- 評価ラボは、可能であればISO/IEC 27001に準拠した適切なセキュリティポリシーを有すること。情報セキュリティ管理の実施に関するガイダンスとしては、評価ラボはISO/IEC 27002を参照。
- 評価ラボは、CC Part 3で定義されたAVA_VAN.5及びALC_FLR.2を用いて、評価保証レベル4までのITセキュリティ評価を実施すること。
- 他に公平性、品質システム、スタッフ、環境条件、メソッド、セキュリティー方針について規定。
- 仮承認・承認されたCCTLのその他義務
- CCTLは常にISO/IEC 17025の認定資格を維持し、本文書に定めるCCTLの承認に関す る要求事項の遵守を続けること。
- CCTLは、SCCSの資料#1～#3に記載されたCSA（サイバーセキュリティエージェンシー認証機関）の手順、規則及び方針に従ってITセキュリティ評価を実施することを保証するものとする。

(6)Cybersecurity Certification Guide
詳細

シンガポールのコモンクライテリアスキーム
（SCCS：Singapore Common Criteria Scheme）

資料#3：評価と認証（https://bit.ly/3Hg42xw）
ITセキュリティ評価・認証
1. 事前評価フェーズ
   ① フィジビリティースタディ（国家保護プロファイルへの適合主張、承認されたCCプロファイルへの適合主張、CSAによって認識/承認された認定保護プロファイルへの適合主張 など）
   ② 認証取得の申請
   ③ 新規認定申請の審査（当事者による申請書記入・署名など）
   ④ タスクキックオフミーティング（TKM）
2. 評価フェーズ
   ① 評価タスク（TKMが成功裏に終了し、適用される認証料がすべて支払われた場合にのみ開始）
   ② 単体評価報告書（各評価タスクの最後に、CCTLによって提出される）
   ③ 評価技術報告書（CCTLはすべての評価作業を完了した後、評価技術報告書を作成する）
3. 結論フェーズ
4. STサニテーション（CCRAに基づくTOEの国際認証のためには、認証書とともにSTを公開）
5. 情報サニテーション（CCTL、OR、ETRなどの評価情報・結果には、開発者に属する機密情報や専有情報が含まれる可能性があり、サニタイズ処理を実施する）
6. 認定証の授与
7. ナショナルスキームコミュニケーション（認証機関はナショナルスキームコミュニケーションを活用し、認証プロジェクトに必要な更なる情報、ガイダンス、明確化、規則を提供）

代表的な評価・認証プロセス



備考
スポンサー：IT製品の開発者、又はIT製品の評価を希望するその他の関係者
PP：保護プロファイル、CB：認証機関（Certification Body）

(6)Cybersecurity Certification Guide
詳細

サイバーセキュリティ・ラベリングスキーム
（CLS：Cybersecurity Labelling Scheme）

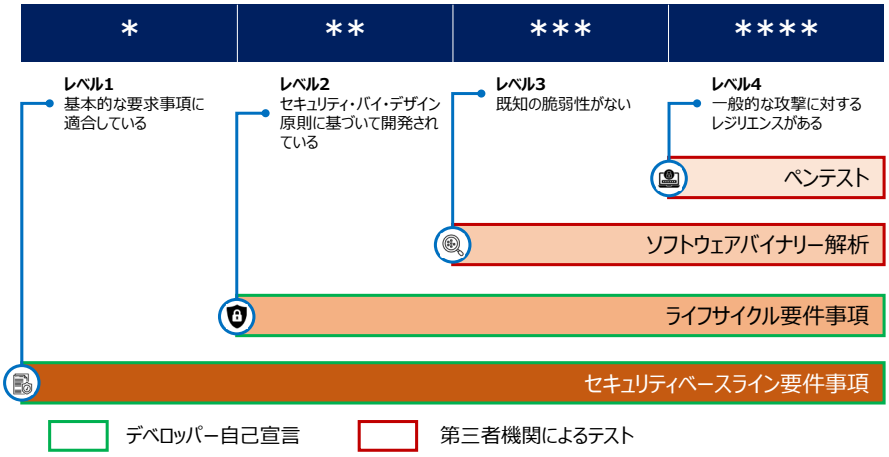
CLS概要とベネフィット
アジア太平洋地域で初めて、ネットワーク接続されたスマートデバイス向けサイバーセキュリティ・ラベリングスキームを導入。

消費者ベネフィット：
サイバーセキュリティのリスクからより安全に保護するために、セキュリティ情報に基づいた購入の意思決定が可能に

開発者ベネフィット：
より優れたサイバーセキュリティ対策で製品を差別化

サイバーセキュリティレベル
CLSは4段階評価で、消費者が製品のセキュリティレベルを見極め、購入時にセキュリティ意識を持たせることができるようになっている。

レベル1： 基本的な要求事項に適合している 本製品は、固有のデフォルトパスワードの確保やソフトウェアアップデートの提供など、基本的なセキュリティ要件を満たしている。	**レベル2：** セキュリティ・バイ・デザイン原則に基づいて開発されている 脅威のリスク評価、重要な設計レビュー、受け入れテストなど、セキュリティ・バイ・デザインの原則に則って開発され、レベル1の要求事項を満たしている製品。
レベル3： 既知の脆弱性がない 本製品は、ソフトウェアバイナリについて、認定された第三者機関による評価を受け、レベル2の要件を満たしている。	**レベル4：** 一般的な攻撃に対するレジリエンスがある 本製品は、認定された第三者機関によるペネトレーションテストを受け、レベル3の要件を満たしている。



(6)Cybersecurity Certification Guide
詳細

サイバーセキュリティ・ラベリングスキーム
（CLS：Cybersecurity Labelling Scheme）

資料#1：スキーム概要（https://bit.ly/35oA0cX）

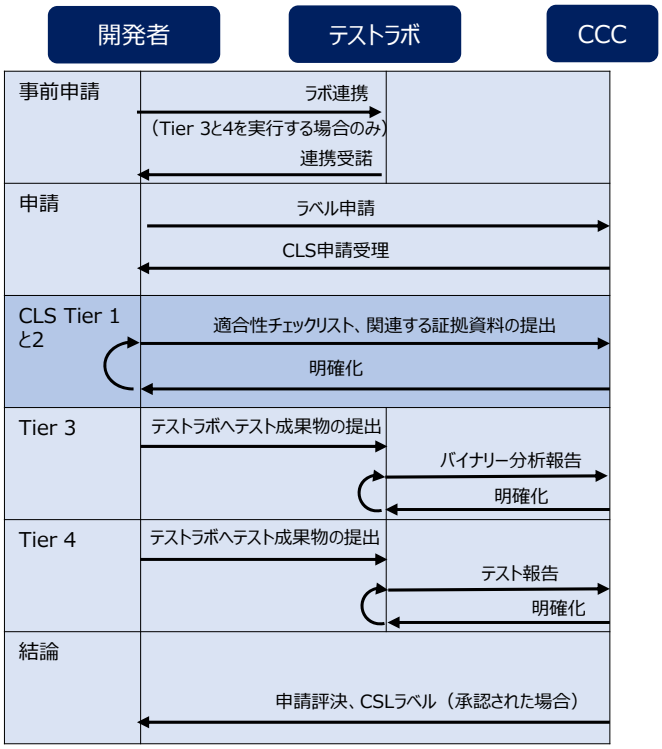
- 評価層（Assessment Tiers）の概要

#	評価層	フォーマット
1	セキュリティ・ベースライン要件	開発者が適合を宣言 テストラボによる独自チェックなし
2	ライフサイクル要件	
3	ソフトウエア・バイナリ分析	テストラボによる第三者評価
4	ペネトレーションテスト	

- Tier #1は、ETSI EN 303 645のセキュリティ基本要件に準拠することを開発者に求める。
- Tier #2は、「IMDA IoTサイバー・セキュリティー・ガイド」（https://go.shr.lc/3KSCGQp）で指定されているライフサイクル要件を参照。
- Tier #3は、機器のソフトウェア（機器のファームウェアとコンパニオンモバイルアプリケーション）に対して、マルウェア、使用されているサードパーティライブラリの既知の脆弱性、バッファオーバーフローなどのソフトウェアの脆弱性を分析。
- Tier #4は、インターネットに接続された機器のペネトレーションテストが前提。開発者はテストを容易にするため、十分な機器サンプルと関連するユーザーガイダンスドキュメントをテストラボに提供する必要がある。
- 下記、その他の関連書類。

資料#2：スキーム仕様（https://bit.ly/3Hdpqn3）
- Tier #4の最小限のテスト仕様と方法論（https://bit.ly/3AH1TIM）
- コンタクトトレーシング機器に関する補足的な最小試験仕様（https://bit.ly/3GcSF8t）
- 適合性チェックリスト・テンプレート（https://bit.ly/3IRBWsO）
- 料金体系（https://bit.ly/3IJxQmw）

ラベリングのプロセス全体は、主に4つのフェーズに分かれる。



備考
CCC：サイバー・セキュリティー・センター

(6)Cybersecurity Certification Guide
詳細

国家IT評価スキーム
（NITES：National IT Evaluation Scheme ）

SCCS概要とベネフィット
政府の機密データを扱う製品は、NITESに準拠した評価を受ける必要がある。シンガポールの国益を守るためには、最も厳しい要件が必要であり、NITESは国家的な追加要件とは別に、製品を高い保証水準で評価するコモンクライテリア（CC）の手法をほぼ採用している。

ユーザー向けベネフィット：
製品が提供するセキュリティ対策が、機密性の高い情報を保護できることを保証
開発者向けベネフィット：
政府調達のポリシー要件を満足

概要
NITESは2009年11月に発足し、 IT製品を評価・認証し、政府評価済みセキュリティ製品リスト（GESPL：Government Evaluated Security Product List）に掲載するためのプラットフォームを提供している。
NITESは、CCなどの国際標準を参照することで、高いセキュリティ保証を実現。
国家IT評価スキームが承認したラボは以下の通り。

An Security Pte Ltd
atsec information security GmbH
SGS Brightsight
Riscure BV
T-Systems International GmbH
TUV Informationstechnik GmbH
UL Verification Services Pte Ltd

別紙2

公開情報等の調査
データ関連文献

対象文献

調査対象リスト

項番	国・地域	文献等の名称	対象分野	作成機関	作成時期	文書種別
1	米国	CLOUD SECURITY TECHNICAL REFERENCE ARCHITECTURE	全般	CISA	2021年	政策
2		SP 800-47 Rev. 1 Managing the Security of Information Exchanges		NIST	2021年	ガイドライン
3		Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward	防衛	DoD	2021年	政策
4	欧州	Technical Overview: Secure cross-company communication	産業IoT	PI4.0	2016年	ガイドライン
5	中国	サイバーセキュリティー法	全般	サイバー空間管理局	2017年	政策
6		データセキュリティー法	全般	サイバー空間管理局	2021年	政策
7		データ域外移転のセキュリティ評価に関する弁法	策定中	サイバー空間管理局	2021年	政策
8		個人情報保護法	全般	サイバー空間管理局	2021年	政策
9	国際	Data Protection Best Practices	産業IoT	IIC	2019年	ガイドライン

(1)Cloud Security Technical Reference Architecture
概要

文献概要	名称	CLOUD SECURITY TECHNICAL REFERENCE ARCHITECTURE		
	主旨	TRAは、共有サービス、クラウド移行やクラウドセキュリティの状態管理に関する注意事項を説明することで、組織のクラウドへの安全な移行を導くことを目的としている。CISAのゼロトラスト成熟度モデルは組織のゼロトラスト戦略と実施計画の策定をサポートし、さまざまなCISAサービス支援を提供する同時に、組織間のゼロトラストソリューション策定も可能できる。		
	国・地域	米国	適用分野	サイバーセキュリティ
	策定者	CISA(Cybersecurity and Infrastructure Security Agency)	対象者	クラウドテクノロジを使用する機関
	遵守義務	連邦政府がネットワークトラブルを防止、検出、評価、又は修復できるように、クラウドテクノロジを使用する機関は、クラウドテクノロジを協調的かつ慎重に使用する必要がある。		
	普及状況	CISA は、このガイドラインが安全なクラウド移行に関する注意事項に適切に対処できるように、組織・業界・学界からの重要なフィードバックを収集し、パブリックコメントを求めている。		
	策定年	2021年	ページ数	46

カテゴリ	カテゴライズ	CLOUD SECURITY　TRAは、CISA、US digital services agency (USDS)やFederal risk and authorization Management Program (FedRAMP) の共同努力により開発された。
	カテゴリ評価	TRAの目的は、推奨されるクラウド移行とデータ保護方法を説明する。Exective Order 14028の第 3 (c) (ii) で説明されたように、連邦政府がクラウドへの移行を続ける中、TRAは各組織がクラウドに安全に移行する際に使用するガイドラインとなる。 また、共有サービス、クラウド移行やクラウドセキュリティの状態管理に関する注意事項についても説明している。
	カテゴリ確認要求	TRAは、クラウドコンピューティングソフトウェアを設計するにはDevSecOpsアプローチを採用する必要があること、及びセキュリティテストなどの分野で自動化を使用して移行を促進することを主張する。 ゼロトラスト・APIの利点・セキュリティ制御の継承の最大化などのソフトウェアをクラウドに移行する必要がある理由を強力に説明し、承認操作(ATO) プロセスを通じてシステム承認を加速する。
	制度的枠組み	クラウドセキュリティTRA は、クラウドサービスで使用される共有リスクモデルに関するガイダンス(FedRAMPによって作成)、クラウド環境の構築方法 (USDS によって作成)、及びどのように堅牢なクラウドセキュリティ状態管理を通じてこの環境を監視するか(CISA によって記述)について、組織にガイダンスを提供する。

関連URL	https://www.cisa.gov/sites/default/files/publications/CISA%20Cloud%20Security%20Technical%20Reference%20Architecture_Version%201.pdf

(1)Cloud Security Technical Reference Architecture
詳細

TRAは主に以下の3つのセクションに分けられる:

- **共有サービス**：このセクションではクラウドサービスの安全性を評価するための標準化されたベースラインについて説明する。
- **クラウド移行**：このセクションでは、一般的な移行シナリオの説明等を含む、クラウド移行の戦略と考慮事項の概要について説明する。
- **クラウドセキュリティの状態管理**：クラウドセキュリティの状態管理であるCSPM (Cloud Security Posture Management) を定義し、クラウド環境での監視、開発、統合、リスク評価及びインシデント対応のための関連セキュリティツールを列挙する。

特徴	番号		コンテンツ	説明
table	1		イントロダクション	クラウドセキュリティTRAは、急速に進化するテクノロジー環境で連邦政府機関のサポートを提供する。
	2		目的	組織がクラウドサービス継続して利用するためのガイドとなること。
	3		**共有サービス**	このセクションではクラウドサービスの安全性を評価するための標準化されたベースラインについての説明。
		1	クラウドサービスモデルの概要	米国国立標準技術研究所(NIST)が定義した3つの基本的なクラウドサービスモデル：SaaS、PaaS、IaaSについての説明。
		2	FedRAMPの説明	FedRAMPは、連邦政府がクラウドサービスを採用するための経済的な方法を提供する。
		3	FedRAMPのセキュリティ	FedRAMPでのセキュリティに関する考慮事項を説明する。
	4		**クラウド移行**	一般的な移行シナリオの説明等を含む、クラウド移行の戦略と考慮事項の概要について説明する。
		1	ソフトウェア	クラウド向けソフトウェアの設計について説明する。
		2	戦略	クラウドに移行することを決定した組織は、クラウドサービスを採用することの利点とリスクの説明。
		3	データ移行の説明	3つの主要なデータ移行が想定され、対応する方法SaaS、PaaS、IaaSに関する詳細な説明を提供する。
		4	ソフトウェアの開発	DevSecOpsソフトウェ開発、セキュリティ、運営の組み合わせについて説明する。
		5	アーキテクチャの構築	組織がクラウドサービスの採用を拡大する際にいくつアドバイスを提供する。
	5		**クラウドセキュリティの状態管理(CSPM)**	クラウドセキュリティの状態管理であるCSPM (Cloud Security Posture Management) を定義し、クラウド環境での監視、開発、統合、リスク評価及びインシデント対応のための関連セキュリティツールを列挙する。
		1	CSPM状態管理の定義	クラウドセキュリティの状態管理であるCSPM (Cloud Security Posture Management) を定義
		2	CSPMの結果	クラウド環境での監視、開発、統合について説明する。
		3	リスク評価とツール	リスク評価及びインシデント対応のための関連セキュリティツールを説明する。

(1)Cloud Security Technical Reference Architecture
詳細

➢ **背景**
- 新しいリーダーシップ、進化するテクノロジー、変化するニーズにより、既存の戦略とシステムの強化が急務となった。 特に、クラウドコンピューティング環境へのサイバー侵入による大きな影響についても国からの対応が必要となる。
- サイバー脅威から国を保護するために、従来のビジネス手段はもはや受け入れられない。
- 更に、クラウド移行には、組織全体に受け入れられ、推進され、サポートされるべき文化的変化、優先順位、及び設計アプローチが必要である。

➢ **目的**
- TRAの目的は、組織がクラウドテクノロジを引き続き採用している間に、協調的かつ慎重な方法でそれらを指導すること。
- このアプローチにより、連邦政府は企業全体のサイバーセキュリティを向上させながら、サーバーインシデントを特定、検出、保護、対応及び回復できる。
- 行政命令で概説されているように、このドキュメントは、クラウドサービスがゼロトラストアーキテクチャに近づくにつれて、クラウドサービスを採用する利点とリスクを組織に通知することを目的としている。
- また、クラウド移行及びデータ保護機関のデータ収集とレポート作成の推奨方法についても説明する。

➢ **結論**
- CLOUD SECURITY TRAは、クラウド移行及びデータ保護に対する推奨されるアプローチを説明するために設計されている。
- 主な内容は、クラウドサービス採用の共有リスクモデル、クラウド環境の構築方法、及びクラウドセキュリティポスチャ確認と管理を通じてそのような環境を監視ツールの説明である。
- 共有サービス、クラウド移行、クラウドセキュリティの状態管理(CSPM)を含む3つの主要なテーマについて説明する。
- 米国連邦政府がクラウドに移行するにつれて、TRAは、政府機関や組織が安全にクラウドに移行する際に活用できるガイドになる。

(2)SP 800-47 Rev. 1 Managing the Security of Information Exchanges
概要

文献概要	名称	SP 800-47 Rev. 1 Managing the Security of Information Exchanges		
	主旨	情報交換における関連事項に関するガイダンスを提供し、交換前・交換中・交換後又はアクセスされた情報の保護と管理に焦点を当て、情報交換のための特定の、交換された情報の保護に関する考慮事項、及び交換された情報の保護の管理に必要な契約上の事項に関するガイダンスを提供する。		
	国・地域	米国	適用分野	サイバーセキュリティ
	策定者	NIST(National Institute of Standards and Technology)	対象者	情報交換に関わる各組織
	遵守義務	組織は、リスクに見合った情報の機密性・完全性・可用性を保護する特定の組織のニーズと要件を満たすために、情報交換事項に関するガイダンスを調整する必要がある。		
	普及状況	組織は通常自身のタスクとビジネスのニーズに基づいて、さまざまな情報交換ルートを通じて1つ又は1つ以上の内部/外部組織と情報を交換 (共有) する必要がある。しかし、交換される情報は、ある組織から別の組織へ移行する際に、同じ又は類似のレベルの保護(リスクに見合った保護)が必要となることが認識されている。したがって、この文献は、情報を交換する様々な組織のための関連ガイダンスを提供する。		
	策定年	2021年	ページ数	59

カテゴリ	カテゴライズ	このガイドラインは、連邦政府機関の推奨ガイドとして、又は非連邦組織で使用することができる。連邦政府機関は、適用される法律、規制、ポリシーを使用して、機密データの保存、処理、配布に使用されるシステム間で情報を交換する。
	カテゴリ評価	テクノロジーベースの情報アクセスから逸脱し、再開発された情報交換の範囲を与え、データ共有活動における潜在的なセキュリティリスクに対処することに重点を置いている。
	カテゴリ確認要求	あらゆる特定種類のテクノロジーベースの接続や情報アクセスに重点が置かれず、情報交換の範囲が更新され、情報交換のセキュリティ管理の利点が説明され、情報交換の種類が特定され、情報交換に関連する潜在的なセキュリティ リスクが議論され、セキュリティ管理システム及び組織間の情報交換に使用される 4 つのステージのアプローチが詳しく説明される。また、そのアプローチの各ステージの手順が推奨され、共有データの保護に必要な安全対策が強調される。
	制度的枠組み	このアプローチの重点は交換前、交換中、交換後に交換される又はアクセスされる情報の保護を管理することであり、特定の種類のテクノロジーベースの接続又は情報アクセス又は交換方法ではないため、基本的な構造には情報交換の識別、保護の考慮事項に関するガイダンスの交換、及び交換情報の保護の管理に必要なプロトコルが含まれる。 組織は、情報交換に関する特定の組織のニーズと要件を満たすようにガイダンスを調整することが期待される。

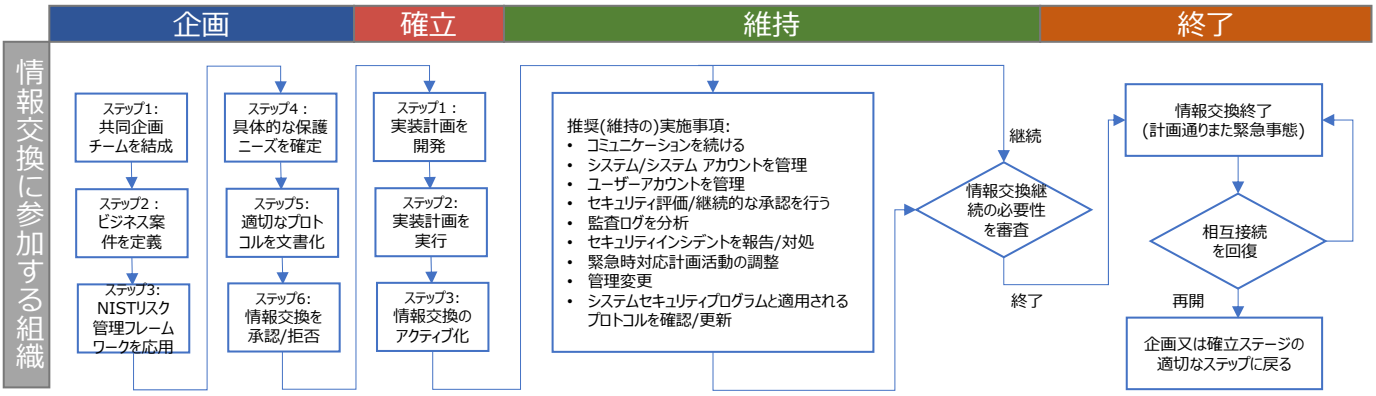
関連URL	https://csrc.nist.gov/publications/detail/sp/800-47/rev-1/archive/2021-01-26

(2)SP 800-47 Rev. 1 Managing the Security of Information Exchanges 詳細

情報交換管理の4つのフェーズを以下に示す。

番号	コンテンツ	説明
1	**情報交換の企画**	• 関係組織は事前活動を展開する。関連する全ての技術、安全及び管理上の問題をチェックする。 • 適切なプロトコルを作成し署名し、情報の管理・使用及び情報の交換方法 (相互接続、ファイル転送、データベース共有、Webベースのサービス、電子メールによる簡単なファイル交換など) を規制する。
2	**情報交換の確立**	• 組織は情報交換を確立するための計画を作成し、実施する。 • その中には、適切なセキュリティ制御の実装又は実現、組織のポリシー・プロセス・署名されたプロトコルに基づいた交換のアクティブ化などが含まれる。
3	**交換及び関連するプロトコルの維持**	• 情報交換が確立されると、組織は情報交換の安全性を積極的に維持し、関連する契約の条項が満たされ、関連性が維持されるようにする。
4	**情報交換の終了**	• ある時点で、組織は情報交換を終了する必要がある。情報交換を中断する方法は、組織のシステムの破壊を避ける必要がある。 • インシデントやその他の緊急事態に対応する際、組織は情報交換を直ちに終了することを決定できる。

情報交換管理ステージのプロセス図



(3)Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward 概要

文献概要	名称	Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward		
	主旨	CMMC は、DIB部門企業がFCIとCUIを保護する能力を測定する国防総省認定プロセスである。CMMC2.0は当初のCMMCフレームワークに基づいており、進化する脅威に対応するために、防衛産業基盤企業 (DIB)サイバーセキュリティを動的に強化できる。		
	国・地域	米国	適用分野	サイバーセキュリティ
	策定者	DoD(Department of Defense)	対象者	敏感的な非機密情報を国防総省と共有する請負業者や下請け業者など
	遵守義務	必要に応じて、相応のサイバーセキュリティ標準に準拠する。		
	普及状況	2021年3月、米国商務省はDFARS暫定規則に関するCMMC 1.0の内部評価を開始し、850件以上のパブリックコメントを受けた。CMMC のこの包括的で手続き的な評価は、国防総省内のサイバーセキュリティや調達のリーダーを巻き込み、ポリシーとプログラムの実施を改善した。このレビューで「CMMC 2.0」を生成した。		
	策定年	2021年	ページ数	1(ヘッドページよりリンク)

カテゴリ	カテゴライズ	CMMC は、既存の規制、特に48連邦規制 (CFR)、52.204-21、及び DFARS 252.204-7012 に基づいており、NIST SP 800-171 rev 1、NIST SP 800-171B ドラフト、英国の Cyber Essentials、オーストラリアの Essential Eight など、さまざまなソースからのプラクティスを組み合わせたものである。
	カテゴリ評価	CMMC2.0は、CMMCプログラムの実装を簡素化及び改善するために、プログラムの構造と要件を更新した。
	カテゴリ確認要求	国防総省は、「連邦規則」第32条と第48条の2つの分野においてCMMC2.0手続き要件を確立する。更に、その計画内容のあらゆる必要な変更を行う。
	制度的枠組み	CMMCフレームワークは、国防総省が請負業者や下請け業者と共有する敏感的な非機密情報を保護し、FCI(Federal Contract Information : 連邦契約情報)とCUI(Controlled Unclassified Information : 管理対象非機密情報が、高度な継続的な脅威を含むサイバーセキュリティリスクに見合ったレベルで保護されるように設計されている。

関連URL	https://www.acq.osd.mil/cmmc/ https://www.acq.osd.mil/cmmc/documentation.html https://www.federalregister.gov/documents/2021/11/17/2021-24880/cybersecurity-maturity-model-certification-cmmc-20-updates-and-way-forward

(3)Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward 詳細

- **CMMC2.0は、CMMC1.0の5つのレベルモデルを3つの高度なサイバーセキュリティ要件レベルに置き換え、それぞれが個別に確立された標準 (連邦調達規則 (FAR) 要件、NIST 要件など)を中心としている。**
- **また、新しいモデルは第三者のエバリュエーターへの監督を強化し、全ての「成熟度」要件とCMMC固有の慣行を排除する。**
- **3つのレベルのそれぞれの要件は以下の通り:**

ロレベル1「基礎知識」
- レベル1は以前のモデルと基本的に同じである。
- 毎年、企業のリーダーシップによって自己評価し、認証する。レベル1では、FAR 52.204-21 が連邦契約情報を保護するために必要な「基本」実施事項から派生した同じ15の実施事項が必要である。

ロレベル2「アドバンス」
- CMMC2.0のレベル2は、古いCMMCの「レベル3」に基づいており、管理対象非機密情報 (CUI) の敏感性に関連し、「優先調達」と「非優先調達」の選択がある。
- 例えば、優先調達には武器システムに関連するCUIが含まれ、非優先調達には軍服関連のCUIが含まれる場合がある。優先順位の詳細は将来の規則策定で提供されることが期待される。
- 優先調達は、認定された第三者評価認定機関 (C3PAO) が3年ごとに個別のサードパーティ評価を行う必要があるが、非優先調達は年1回の自己評価と認証のみを必要とする。
- CMMC の新しい Level 2は、NIST SP 800-171 Rev 2 (NIST SP 800-171) の 110 の実施事項を要求する。CMMC 1.0 Level 3 の20の実施事項が排除される。

ロレベル3「エキスパート」
- 新しいレベル3は、既存のレベル4とレベル5を代替する。 最も注目すべきは、このレベルの調達には3年ごとに政府主導の評価(すなわち、C3PAOsではない)が必要となる。
- 更に、新しいLevel 2で要求する110の実施事項に加えて、Level 3認証はNIST SP 800-172の実施事項の遵守を要求する。レベル2やレベル3の実施事項をNIST標準と同等にする決定は、バイデン政権が連邦サイバーセキュリティにあるNISTの役割をさらに集中させるためにした他の努力と関係がある。Exective Order 14028も含まれる。

CMC Model 2.0	MODEL	ASSESSMENT
LEVEL 3 Expert	**110+** Practices based on NIST SP 800-172	Triannual government-led assessments
LEVEL 2 Advanced	110 Practices aligned with NIST SP 800-171	Triannual third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 Practices	Annual self-assessment

(3)Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward 詳細

コンテンツ	説明
背景	• CMMCプログラムは変化する脅威に対応するために DIBサイバーセキュリティを動的に強化し、米国の戦闘員をサポートし支援する情報を保護することを目的とした国防総省の最優先事項である。 • 2020年11月30 日より、DF ARS 条項 252.204-7021 の請負業者のためのサイバーセキュリティ成熟度モデル認定レベル要件が施行された。この条項は、CMMCプログラムの初期バージョン (以下「CMMC 1.0」) を実現した。 • CMMC1.0は、国防総省が請負業者や下請け業者と非連邦請負業者情報システムで共有又は処理するFCIやCUIの保護を目的とする。CMMC1.0には5つのサイバーセキュリティレベルが含まれる。DIB請負業者は特定のレベルでCMMCサイバーセキュリティ標準への準拠を証明するために認定プロセスを受けるように要求されている。 • 2021年3月、米国商務省はDFARS暫定規則に関してCMMC 1.0の内部評価を開始し、850件以上のパブリックコメントを受けた。 • CMMC についてのこの包括的で手続き的な評価は、国防総省内のサイバーセキュリティや調達リーダーを巻き込み、ポリシーとプログラムの実施を改善した。このレビューは、CMMCプログラムの実施を簡素化し改善するために、プログラム構造と要件を更新する「CMMC 2.0」を生成した。
CMMC1.0 から CMMC2.0への各変更事項	◘ レベル2とレベル4を削除し、CMMC 2.0で3つのレベルを下記のように再定義する: • レベル1「基礎知識」はCMMC 1.0 のレベル1と基本的に同じである。 • レベル2「アドバンスト」はCMMC 1.0 のレベル3と類似する。 • レベル3「Expert」はCMMC 1.0のレベル5と類似する。 ◘ 全てレベルから「成熟度」要件とCMMC固有の慣行を排除する。 ◘ CMMCレベル1「基礎知識」については、毎年の自己評価とDIBのリーダーシップによっての認証を可能とする。 ◘ 2択となるCMMC レベル2「アドバンスト」についての評価要件: • CUIに関わる優先調達は第三者認証を必要となる。 • CUIに関わる非優先調達は毎年の自己評価とDIBのリーダーシップによっての認証を可能とする。 ◘ CMMC レベル3「Expert」については、政府主導の認証を必要とする。 ◘ 時間制限と実施可能な行動計画とマイルストーンプロセスを策定する。 ◘ 必要に応じて、承認された上で、対象限定で時間制限のある免除手順を確立する。
Way Forward	• CMMC 2.0フレームワークに反映される変更は、規則作成プロセスを通じて実施される。 • 国防総省は、「連邦規則CFR」第32条と第48条の2つの分野において規則を策定していく。 • CMMC2.0手続き要件を確立する上に、CFR第48条にあるCMMC内容のあらゆる必要な変更を行う。どちらの規則もパブリックコメント期間を設ける。 • リリースされるCFRの第32条と第48条では、更新されたCMMC2.0 に対する国防総省の要件が実施される。中には、CMMC1.0 からの各種変更も含まれる。

(4)Technical Overview: Secure cross-company communication
詳細

文献概要	名称	Technical Overview: Secure cross-company communication		
	主旨	インダストリー4.0環境における企業間バリューネットワークのニーズに対応する安全な通信の基本的な要件、セキュリティ上の課題、及びさまざまなアプローチに関する共通の立場を記載。		
	国・地域	ドイツ	適用分野	製造業
	策定者	Platform Industrie 4.0	対象者	Industrie 4.0(原文のまま)のコンテクストにおける意思決定者とユーザーを対象
	遵守義務	保護が必要な企業資産に基づき、企業間の安全なコミュニケーションリンクを提示し、行動のための初期推奨事項を提示しているものであり、遵守義務はない。Platform Industrie 4.0自体が、学者や企業、政治家に具体的な推奨事項の提供を目指している。		
	普及状況	本文献の具体的な普及状況は紹介されていなかったが、Platform Industrie 4.0のユースケースとしてシーメンス、ファーウェイ、ABB、フォルクスワーゲン、横河電機、ファイザーなどが紹介されている。		
	策定年	2016年	ページ数	26ページ

カテゴリ	カテゴライズ	「コミュニケーション」、「セキュアコミュニケーションの目的と効果」、「セキュアコミュニケーションチャンネル」、「コミュニケーションパートナー」、「法律上の留意点」、「推奨されるアクション」に分類されている。
	カテゴリ評価	インダストリー4.0の要件とソリューションの評価を支援するためのガイドラインを提案している。
	カテゴリ確認要求	保護が必要な企業資産に基づき、企業間の安全な通信リンクを提示し、アクションのための初期推奨事項を提案している。
	制度的枠組み	本文献は、Platform Industrie 4.0「ネットワークシステムのセキュリティ」ワーキンググループが、ハノーバートレードフェア2016に向けてまとめた中間結果を反映したものとなっている。また、同タスクにおいては、情報の流れの監視や、セキュリティインシデント発生時の緊急対策など、新たなテーマにも取り組んでいる。

関連URL	https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/secure-cross-company-communication.pdf?__blob=publicationFile&v=6

(4)Technical Overview: Secure cross-company communication
詳細

コミュニケーション

項目	ガイドライン
セキュアな通信をコアな課題に	将来のシナリオでは、会社の垣根を越えてデータや情報を直接やり取りすることで、新たな可能性が開かれる。このようなシナリオでは、人間も機械もコミュニケーションパートナーとして考える必要がある。また、企業の境界を越えたコミュニケーションは、もはや経営レベル(MES/ERP)だけでなく、下位のレベルでも行われるようになるだろう。例えば、特定の機械や部品からそのサプライヤーに直接連絡するような場合が該当する。さらに、IPv6への移行により、エンド・ツー・エンドの接続性が拡張可能になることも考慮しなければならない。 セキュリティの観点からは、専門知識やデータ、企業秘密の保護など、多くの分野からの要求が適用される。これらは常に、以下のような伝統的なセキュリティ目標によって示される。 1. 機密保持 2. 整合性 3. 可用性 また、次のような二次的な下位のセキュリティ目標も含める必要がある。 1. 真正性 2. 否認防止 3. 拘束力 4. アカウンタビリティ
視点と定義	企業横断的なバリューネットワークに参加したい企業は、ビジネスモデルに沿った組織的なプロセスをさらに適応させる必要があり、ITセキュリティの技術的なソリューションを導入するだけでは十分ではない。信頼を築くためには、例えばCMMI(Capability Maturity Model Integration)に基づくITセキュリティの成熟度によって、セキュリティ基準を評価する必要がある。 中小企業は、この目標を達成するために適切な標準によってサポートされなければならず、大企業ではそれに応じて情報セキュリティマネジメントシステム(ISMS)を構築する必要がある。
その他	「視点と定義」、「組織への影響」についての言及。

セキュアコミュニケーションの目的と効果

項目	ガイドライン
はじめに	Industrie 4.0環境では、企業をつなぐ多様なバリューネットワークにより、新しい事業分野や生産プロセスの出現が促進される。また、企業間のデータ交換はインターネット経由で行われることが多く、Industrie 4.0のプロセスは攻撃に対してより脆弱になっている。そのため、特に企業の垣根を越えたセキュアなコミュニケーションに注目する必要がある。
企業の重要資産保護	Industrie 4.0では、既存の会社の枠を超えた電子的なコミュニケーションの必要性が高まっており、セキュリティへの投資目標を達成するためには、保護が必要な企業資産(例えば数式、手順パラメーター、プロセス関連の品質保証方法など)を特定する必要がある。すべての価値ある情報には、いわゆる「保護要件」があり、それぞれのケースで適切な対策を講じなければならない。この保護要件は、他社とのコミュニケーションプロセスにおいて、各企業が自社の資産の機密扱いと保護を信頼できるようにするために、タスク共有の計画方法によって、Industrie 4.0のプロセス全体を通して確実に保護されなければならない。

(4)Technical Overview: Secure cross-company communication 詳細

セキュアコミュニケーションチャンネル

項目	ガイドライン
はじめに	原則として、安全なコミュニケーションチャネルを導入する場合は、次のセキュリティ上の考慮事項を遵守する必要がある。 1. 可用性：インフラは障害から保護されなければならない。 2. 整合性：データは不正な変更から保護されなければならない。 3. 機密性：データは不正アクセスから保護されなければならない。 認証メカニズムは、コミュニケーションパートナーの真正性やデータソースのオリジナリティを保証するために使用される。認証チェックは、機密性と整合性を確保するために不可欠である。また、エラーや攻撃が発生した場合にプロセスを追跡できるようにするためには、コミュニケーションパートナーとの間で交わされるメッセージが否認されないこと(否認防止)が重要となる。 エラーや攻撃があった場合に、プロセス全体を遡及的に分析できるようにするためには、説明責任の証明を確実に行う必要がある。 一般的に、機密性と整合性を確保するための従来の予防的なセキュリティ対策は以下の通り。 • ユーザーとIDの管理(認証、承認) • データの暗号化と署名
コミュニケーションデザイン	Industrie 4.0のネットワーク化された世界において、機密性と整合性、可用性の原則を守りながら人と機械との企業間のつながりを維持するには、コミュニケーションデザインという形で全体的なアプローチが必要。 この点で、コミュニケーションデザインは情報交換に必要な様々な接続を特定し、文書化し、保護対策を通じてビジネスプロセスの重要性要件を満たすのに役立つ。この場合、通常運転、緊急運転、メンテナンスモード、分析モードなど、さまざまなネットワーク状態を区別することが有効となる。
可用性・信頼性	Industrie 4.0の「注文管理生産」のアプリケーションシナリオは、柔軟な生産構成を提示し、生産能力について企業間及び工場間のネットワーク化を展開し、変化する市場と注文状況に迅速に対応できるようにする。既存の生産設備が持つ能力やキャパシティの最適な活用には、安全なコミュニケーションが不可欠である。 コミュニケーションプロセスの可用性と信頼性を確保するための重要な設計要素を設計段階の早い段階で規定し、その有効性を継続的にチェックすることが重要である。
可用性・信頼性(続き)	また、コミュニケーションプロセスの参加者の重要度やプロセスチェーンへの依存度に応じて、コミュニケーションインフラの可用性と回復力を確保するための技術的、組織的な側面も考慮する必要がある。
セーフガード	会社の重要な資産(システム、データシート、計画書、フォーミュラ、マーケティングデータ)を分類することは、リスクを評価する上で有効であり、不可欠である。 この分類では、これらの資産がどの程度まで他者(例えばパートナー企業)と交換可能なのか、あるいは内部アクセスのみであるのかを特定する必要がある。 以下に、シンプルで一貫性のある分類体系を提案する。 • 保護措置なし：公開 • 中レベルの保護：機密、ビジネスパートナー向け(Industrie 4.0シナリオの新機能) • 高レベルの保護：機密、内部使用 Industrie 4.0ではレジリエンスが重要な役割を担っており、関係するコンポーネンツはヒューマンエラー(無差別)や妨害行為(標的型)に対するレジリエンスを示さなければならない。
重要な会社資産の保護要件と分類	保護レベルの決定が基本的な対策となり、リスクアセスメントを実施することで可能となる。重要なのは、どのようなセキュリティインシデントが起こりうるか、セキュリティ要件が規定されていて適用できるか、適用できるとしたらどの要件かを確定すること。保護範囲の評価には担当部署とデータ及びサービスの所有者が関与する必要がある。 セキュリティ対策が効果的に機能するためには、リスクを考慮した情報の取扱いが必要。保護対策の範囲は、特定のデータやサービスに保護が必要か否かに基づいて決定されるべきである。 機密・内部使用：最高の保護カテゴリで、データ又はサービスは会社内でのみ共有でき、会社外に出てはならない(例：機密の公式や未公開の特許など) 機密、ビジネスパートナー向け：中程度の保護カテゴリで、企業間での情報交換は、Industrie 4.0の基本的な部分。ビジネス情報の適切な取扱いと、関連する正しいプロセスの文書化が不可欠(例：生産情報や合金の自動交換など) 公開：機密保持は要求されない(例：機械の動作データやセンサーデータなど)

(4)Technical Overview: Secure cross-company communication 詳細

コミュニケーションパートナー

項目	ガイドライン
セキュリティ間のコミュニケーションを円滑にするドメイン	コミュニケーションパートナー(生産工場)の識別と認証は、セキュリティ・ドメインの基本要件である。コミュニケーションは、制御とプラントデータの交換に必要な信頼を得るために、識別されたユーザー／プラント／コンポーネントとのみ確立されるべきである。コミュニケーションには、論理的にグループ化されたコミュニケーションチャネル(コンジット)が使用される。これらのコンジットは、ITセキュリティ要件を共有する2つ以上のゾーン又はドメインを接続する。
識別	Industrie 4.0では、関係者の安全な識別が不可欠であり、このプロセスはセキュリティ要件を満たすように設計されなければならない。 接続ネゴシエーションにおいて、IDチェックの安全な統合を提供する必要がある。 • アドレス指定は、管理シェルによって行われ、これにより、希望するIDがエンティティに格納されている安全なIDにマッピングされる。 • アドレス指定は管理用シェルを使って行われ、それによって希望するIDもエンティティに安全に保存される。 これらの要件は、コミュニケーション機構の設計段階から考慮されるべきである。 すべての関連するプロパティとIDを確認するためのデジタル証明書などの必要なデータは、Industrie 4.0コンポーネントの機能であり、したがって管理シェルで表示される。 Industrie 4.0の一部である企業横断的でダイナミックなバリューネットワークでは、権利と役割の理解を深めることが必要。 Industrie 4.0のコンポーネントが企業の境界を越えて自律的にビジネス取引を行うためには、これらのコンポーネントの標準的な仕様も合意する必要がある。企業間のコンテクストでは、例えば完全な商業的権限によって人に適用できる法的拘束力が、機械にも適用できるかどうかを明らかにする必要がある。 Industrie 4.0のコンポーネントは、そのライフサイクルの中で変化する機能を持っており、その結果、例えばIDやセキュリティプロファイルが変更される。初期設定やパラメータ設定などのコミッショニングに加え、交換やデコミッショニングなどの通常運用もサポートする必要がある。 Industrie 4.0の生産的なシナリオは、継続的に変化していく。例えば、新しい生産工程が機械の追加によって導入されたり、生産機械の故障や償却で一時的な交換が必要になったりする。
識別(続き)	生産工程は、必要なセキュリティ上の配慮にもかかわらず、継続的に、あるいは短期間の中断にとどめる必要があり、そのため、生産設備の迅速な交換には、セキュリティ属性の設定と、これらの属性の関連シナリオへの統合を完全に自動化することが必要となる。

法律上の留意点

項目	ガイドライン
データ保護	2018年まで有効なドイツデータ保護法は、たとえ機械間通信「だけ」が実行されるとしても、Industrie 4.0の領域で適用することができる。機械間の個人データの自律的な交換の間、機密保持などの関連する保護要件は引き続き遵守されなければならない。 国境を越えたIndustrie 4.0の生産工程には、欧州の一般データ保護規則に加えて、各国の関連する改正が適用される。
競争法	現在のセクター別ベストプラクティス・ソリューションは、成熟した信頼モデルに焦点を当てており、これらは将来のIndustrie 4.0の信頼モデルに無差別に実装されるべきものである。
サボタージュ保護	一般に破壊的な技術は意図的な競争制限を行うために使用され、このような技術を認識し、防止することが重要である。

推奨されるアクション

項目	ガイドライン
信頼性の高いコミュニケーションチャンネル	Industrie 4.0では、プライベート及びパブリッククラウドインフラを活用したバリューネットワークの機動的な構築とサービスの実現が不可欠な要素となっており、参加する企業は、信頼できるインターネット回線を利用できることが必要である。
安全なID	すべての安全なコミュニケーションプロセスの基本は、コミュニケーションパートナーを安全に識別し、セキュリティプロファイルを安全にネゴシエートすることである。
セキュリティプロファイルのネゴシエーション	情報交換において、情報セキュリティの確保は重要な要素である。コミュニケーションパートナーは、コミュニケーションリンクが確立されている間、この目的のためにセキュリティプロファイルを交換できる必要がある。セキュリティプロファイルは、Industrie 4.0コンポーネントに不可欠な機能である。
情報分類のテクニカルサポート	コミュニケーションパートナーとの間でやり取りされる情報は、分類体系に従って分類されなければならない。Industrie 4.0環境における自動的な情報交換では、情報そのものだけでなく、関連する管理シェルでも表現する必要がある。

(5)中国サイバーセキュリティー法
詳細

文献概要	名称	中国サイバーセキュリティー法		
	主旨	「サイバーセキュリティー法」はサイバーセキュリティの義務と責任を改善する。 「サイバーセキュリティー法」は様々な規制の規定を全国人民代表大会の法的レベルまで引き上げ、ネットワーク事業者などの法的義務と責任を完全に規定する。		
	国・地域	中国	適用分野	ネットワークの構築、運用、保守、使用、監督と管理
	策定者	全国人民代表大会常任委員会	対象者	非政府ネットワーク要素の参加者
	遵守義務	サイバーセキュリティの義務を履行し、政府や社会の監督を受け、社会的責任を果たす。		
	普及状況	「サイバーセキュリティー法」は中国国内におけるあらゆるインターネット関連施設、ハードウエア、ソフトウエア及びサービスに適用する。		
	策定年	2017年	ページ数	12

カテゴリ	カテゴライズ	サイバースペースセキュリティ法制度の不可欠な部分であり、7つの章と79のセクションで構成されており、非常に広い範囲をカバーする。
	カテゴリ評価	画期的な意味を持ち、国家安全保障法制度におけるもう1つの重要な法律であある。 サイバーセキュリティの分野における基本的な法律であり、国家安全保障法やテロ対策法などと同じレベルにあり、その基本原則の確立は、サイバーセキュリティ構築を導く上で重要な役割を果たす。
	カテゴリ確認要求	「サイバーセキュリティー法」は、サイバーセキュリティの規制、個人のプライバシーと機密情報の保護、及び国家サイバースペースの主権・セキュリティの維持を目的とする。
	制度的枠組み	米国国立標準技術研究所(NIST)のサイバーセキュリティフレームワークやISO 27000-27001など、最も一般的に使用されるサイバーセキュリティ規格と類似しており、ネットワーク製品、サービス、運用、情報セキュリティ、監視、早期診断、緊急対応、報告の要件を強調する。 データのプライバシー保護に関して、他の国のデータプライバシー法や規制にも類似する。しかし、国家サイバースペースの主権と国家安全保障には、より特別な要件がある。

関連URL	http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/node_27975.htm

(5)中国サイバーセキュリティー法
詳細

「サイバーセキュリティー法」の全文は、一般規則、サイバーセキュリティ支援と促進、ネットワーク運用セキュリティ、ネットワーク情報セキュリティ、早期警戒と緊急対応の監視、法的責任、及び関連規則を含む7章79条で構成される。 対象の観点から、各条項を10のカテゴリーに分類できる。

番号	カテゴリ	規制	コンテンツ
1	目的と範囲	第一条、第二条	「サイバーセキュリティ法の目的」及び「サイバーセキュリティ法の管轄」の2つの規定
2	国家	第三条、第四条、第五条、第六条、第七条、第八条、第十二条、第十三条、第十四条、第十五条、第十六条、第十七条、第十八条、第十九条、第二十条	「サイバーセキュリティ法の原則、方針、実現経路」など15の規定
3	ネットワーク ユーザー	第十一条、第十二条、第十四条、第二十六条、第二十七条、第二十九条、第四十六条	「業界団体の規範と自主規制」、「権利と義務」など7つの規定
4	ネットワーク オペレータ	第九条、第二十一条、第二十四条、第二十五条、第二十八条、第四十条、第四十一条、第四十二条、第四十三条、第四十四条、第四十七条、第四十九条、第五十六条	「サイバーセキュリティレベル保護制度の導入」、「実名制要件」など13の規定
5	重要な情報インフラストラクチャの運用者	第三十一条、第三十二条、第三十三条、第三十四条、第三十五条、第三十六条、第三十七条、第三十八条	「作業計画、安全対策実施」など8つの規定
6	ネットワーク製品及びサービス プロバイダー	第十条、第十六条、第十七条、第十八条、第二十一条、第二十二条、第二十三条、第三十五条、第三十六条、第三十七条、第三十八条、第四十八条	「サイバーセキュリティとデータセキュリティの要件」など12の規定
7	国家ネットワーク情報部	第八条、第十四条、第二十三条、第三十条、第三十五条、第三十七条、第三十九条、第五十条、第五十一条、第五十三条、第七十三条	「サイバーセキュリティ業務及び関連監督管理業務のコーディネート」など11の規定
8	関連部門	第八条、第十四条、第十五条、第十九条、第二十三条、第三十条、第三十五条、第三十七条、第三十九条、第四十九条、第五十条、第五十一条、第五十三条、第五十四条、第五十六条、第六十九条、第七十三条	「サイバーセキュリティ監視早期警戒・情報伝達体制の整備」17の規定
9	公安部門	第八条、第十四条、第二十八条、第六十三条、第六十四条、第六十七条、第六十九条、第七十四条	「通報処分権」、「調査支援制度」など8つの規定
10	個人情報	第二十二条、第三十七条、第四十一条、第四十二条、第四十三条、第四十四条、第四十五条、第六十四条	「個人が情報を享受するデータ主権」など8つの規定

(5)中国サイバーセキュリティー法

詳細

- 中国のサイバーセキュリティの分野における基本的な法律であり、我が国最初のサイバーセキュリティ法であり、サイバーセキュリティを保護する中国初の基本法である。
- 特徴は、3つの基本原則、6つの顕著な特徴、及び9タイプのサイバーセキュリティシステムに分けることができる。

特徴	番号	コンテンツ	説明
3つの基本原則	1	サイバースペース主権	中国のサイバースペース主権の最高管轄権の具体的な現れである
	2	サイバーセキュリティ・情報化の発展	セキュリティは開発の前提条件であり、開発は安全であり、セキュリティと開発は同時に推進する必要がある
	3	共同ガバナンス	政府、企業、社会組織、技術コミュニティ、市民などのネットワーク関係者の参加
6つの特徴	1	サイバースペースの主権の原則の明確	サイバー主権の原則は、国連憲章と国家法の基本的な規範に基づく
	2	ネットワーク製品・サービス プロバイダーのセキュリティ義務の明確	ネットワーク製品・サービスは、関連する国家規制を満たす必要がある
	3	ネットワーク オペレータのセキュリティ義務の明確	ネットワーク事業者などの法的義務と責任は、完全に規定される
	4	個人情報保護規程をさらに充実させる	個人情報の取引のための特定の法的スペースを初めて与える
	5	重要な情報インフラストラクチャのセキュリティ体制の確立	重要な情報インフラストラクチャのセキュリティ体制が初めて立法形式で保護される
	6	重要な情報インフラストラクチャにおける重要なデータの国境を越えた転送に関するルールの確立	データのローカライズストレージとは、主権国家が法律や規則を制定することにより、自国のデータの海外への流れを制限する
9タイプのサイバーセキュリティシステム	1	サイバーセキュリティレベルの保護システム	サイバーセキュリティレベルの保護システムの実施が国の法律に引き上げされた
	2	ネットワーク製品・サービスのセキュリティ システム	サイバーセキュリティ製品・サービスに関連するセキュリティシステムは、主に市場アクセス、必須セキュリティ検査、必須セキュリティ認証を含む
	3	重要な情報インフラストラクチャは、セキュリティ システムの実行	重要な情報インフラストラクチャの概念と重点的保護の範囲を法的レベルで提案する
	4	サイバーセキュリティリスク評価システム	重要な情報インフラストラクチャの運用者は、少なくとも年1回、関連機関にリスク検出評価を委託する必要がある
	5	ユーザーの実名システム	ネットワーク運用者は、ユーザーに関連サービスを提供する場合、ユーザーに ID 情報を提供する
	6	サイバーセキュリティインシデントの緊急計画システム	ネットワーク運用者は、ネットワーク セキュリティ インシデントの緊急時対応計画を作成し、タイムリーに対処する
	7	サイバーセキュリティ監視早期警戒と情報伝達システム	国家レベルでは、セキュリティ状況認識と情報伝達システムを確立する必要がある
	8	ユーザー情報保護システム	ネットワーク事業者は、収集したユーザー情報を厳重に秘密にし、ユーザー情報保護体制を改善する
	9	重要な情報インフラストラクチャの重要なデータの保持システム	重要な情報インフラストラクチャの運用者は、国内に個人情報及び重要なデータを国内に保管する必要がある

(6)中国データセキュリティー法

概要

文献概要	名称	中国データセキュリティー法		
	主旨	「データセキュリティ法」は、データ処理活動を規制し、データセキュリティを保護し、データ開発と利用を促進し、個人又は組織の正当な権利、国家の主権、セキュリティ、開発の利益を保護する法律である。		
	国・地域	中国	適用分野	データ処理活動、データセキュリティ、データ開発・利用などの分野
	策定者	全国人民代表大会常任委員会	対象者	データを処理する可能性のあるすべての政府、企業、及び組織
	遵守義務	法律、規制、社会倫理、企業・職業倫理、誠実さ、信頼、データセキュリティ義務の履行、社会的責任の遵守、国家の安全と公共の利益を危険にさらさないこと、個人や組織の正当な権利と利益を害しない。		
	普及状況	「データセキュリティ」中国国内におけるデータの保存、移転、修正等行為、及びデータの域外移転関連行為に適用する。		
	策定年	2021年	ページ数	8

カテゴリ	カテゴライズ	「データセキュリティ法」は、データ分野における基本的な法律で、中国の国家安全保障分野に属する重要な法律である。 発効後、「データセキュリティ法」は、「サイバーセキュリティ法」及び立法プロセス中の「個人情報保護法」とともに、中国の情報及びデータセキュリティの分野における法的枠組みを包括的に構築する。
	カテゴリ評価	データセキュリティの全体的な意思決定を中央国家安全保障のリーダーシップに初めて強化し、「国家安全保障法」と整合し、国家安全保障システムにおけるデータ セキュリティの重要性を強化する。
	カテゴリ確認要求	「データセキュリティ法」は、データセキュリティを保護し、データ開発と利用を促進し、市民や組織の正当な権利と利益を保護し、国家の主権、安全及び開発の利益を保護するために制定された。 「データセキュリティ法」の制定は、国家の安全を守るための必然的な要件であり、人々の正当な権利と利益を保護する客観的な必要性であり、デジタル経済の健全な発展を促進するための重要な措置である。
	制度的枠組み	「データセキュリティ法」は、「データセキュリティ法」と「国家安全保障法」と「サイバーセキュリティ法」の関係を整理する。 まず、「データセキュリティ法」と「サイバーセキュリティ法」は、いずれも「国家安全保障法」の下位法であり、平等に「国家安全保障」の下に統合される。 次に、両者の不適切な交差を回避し、相補的な効果を発揮するため、「サイバーセキュリティ法」(サイバーセキュリティ法第76条第2項の後段)を前提に、「データ自律制御」と「データマクロセキュリティ」を規制の焦点とすべきである。

関連URL	http://www.npc.gov.cn/npc/sjaqfca/sjaqfca.shtml

(6)中国データセキュリティー法

詳細

一般規則、法的責任、及び附則に加えて、「データセキュリティ法」には、主に「データ セキュリティ・開発、システム、義務、政府データセキュリティ・オープン」の4つの章がある。

第一章 一般規則

第二章 データセキュリティ・開発(セキュリティと開発の重視)

- ビッグデータ戦略の実装
- データセキュリティ標準システムの構築
- データ取引管理システムの改善
- データ開発・セキュリティ技術の研究の強化
- データセキュリティ検出評価、認証サービスの推進

第三章 データセキュリティシステム(重要なデータの保護)

- データ分類の階層的保護システム(重要なデータ保護ディレクトリ)
- データセキュリティレビューシステム
- リスク評価
- リスク レポート
- 情報共有
- アラーム監視
- データ輸出管理
- データ セキュリティの緊急対応メカニズム
- 外国に対する差別的行動に対する対抗措置

第四章 データセキュリティ義務

データ セキュリティ ガバナンス

- データセキュリティ管理システム
- データ セキュリティ リスクの監視
- データ セキュリティ教育トレーニング
- データ セキュリティ リスクの処分
- データ セキュリティ テクノロジ対策
- データ セキュリティリスク評価(種類/数量/リスク)
- データ セキュリティ管理機関
- 合理・適切なデータ収集

データ処理とサービス

- データ ソースの監査・記録
- データ処理サービス ライセンス
- 法律に従ってデータ使用
- データのアウトバウンド/クロスボーダーストレージ

第五章 政府データのセキュリティ・オープン

- 法令・行政規則に従ってデータを収集・利用
- データセキュリティ管理システムの改善、保護責任の確認
- 委託先のデータ セキュリティ義務の履行を監視
- 政府データ開発カタログとオープンプラットフォーム

第六章 法的責任

第七章 附則

(7)データ域外移転のセキュリティ評価に関する弁法(コメント草案)」(まだ正式決定ではない)

概要

文献概要	名称	データ域外移転のセキュリティ評価に関する弁法(コメント草案)		
	主旨	「データ域外移転のセキュリティ評価に関する弁法(コメント草案)」は、事前評価と継続的な監督の組み合わせ、リスクの自己評価とセキュリティ評価の組み合わせ、データ出国のセキュリティリスクの防止、法律に基づくデータの秩序ある自由な流れの確保など、「国境を越えたデータの安全性と自由な流れの促進」を提案する。		
	国・地域	中国	適用分野	サイバー情報セキュリティとデータのクロスボーダーセキュリティの分野
	策定者	国立インターネット情報局	対象者	データ処理者は、中国国内での事業において収集した重要なデータ及び法律に従って安全評価を行うべき個人情報を海外に提供するときは、これらの措置の規定に従って安全評価を行うものとする。
	遵守義務	データの出国活動を規制し、個人情報の権利・利益、国家の安全・公共の利益を保護し、国境を越えたデータの安全かつ自由な移動を促進する。		
	普及状況	「データ域外移転のセキュリティ評価に関する弁法(コメント草案)」は中国国内におけるデータ処理に関わる行為、及びデータの域外移転に関わる行為に適用される。		
	策定年	2021年	ページ数	3

カテゴリ	カテゴライズ	データ域外移転のセキュリティ評価に関する弁法(コメント草案)は、ネットワーク情報セキュリティの分野における規制の1つ。 CIIO、重要なデータ処理者、個人情報処理者をカバーするデータ出国評価システムは、最終的に法的レベルで確立され、データ出国評価の具体的なルールのギャップを埋め、データアウトバウンドセキュリティ評価のためのルールと基礎を提供し、データアウトバウンドセキュリティの運用性を向上させる。
	カテゴリ評価	データアウトバウンドセキュリティ評価の適用基準、評価内容・プロセスなどの問題が明確になり、企業がデータアウトバウンドプロセスをより明確にする
	カテゴリ確認要求	このアプローチは、データの自由な流れを規制し、データの自由で整然とした流れを確保するために、セキュリティを確保することを目的とする。
	制度的枠組み	「中国サイバーセキュリティー法」、「中国データセキュリティー法」「中国個人情報保護法」などの法令に基づき、「データ域外移転のセキュリティ評価に関する弁法」(コメント草案)起草する

関連URL	http://www.moj.gov.cn/pub/sfbgw/zlk/202110/t20211029_440266.html

(7)データ域外移転のセキュリティ評価に関する弁法(コメント草案)」(まだ正式決定ではない

詳細

- データ域外移転のセキュリティ評価と管理は、データコンプライアンスにおいて重要な課題。
- 以下は、「データ域外移転のセキュリティ評価に関する弁法(コメント草案)」の対象者の具体的な範囲、自己評価・評価内容、評価申告機関、資料及び受理期限、評価審査の重点、期間及び有効期間に関する内容を示す。

データアウトバウンド安全評価図(評価申請の流れ)

規制対象となるデータ範囲

データ保有者

- **CIIO(重要な情報インフラストラクチャの運用者)**
- **100M+(個人情報の取扱いは100万人に達する)**

域外出国データ

- **重要なデータ(出国には重要なデータが含まれる)**
- **PI:100K+(データ量は10万以上)**
- **SPI:10K+(データ量は1万以上)**

データ移転申告

保有者による自己評価

評価項目

・合法性、正当性、必要性の評価
・感度とリスク評価
・セキュリティ評価(経営・技術)
・責任能力評価
・権利救済のアクセシビリティ評価
・契約仕様評価

評価申告機関

受付機関: **地方のインターネット通信局**

申告資料: 申告書、自己評価レポート、契約内容

審査項目:
・自己評価項目
・受信場所の法的・安全な環境
・中国の法律や規制の遵守

審査期間: 45+15営業日

有効期間: 2年

評価を通過したデータ域外移転活動が実際の処理過程でデータ域外移転安全管理の要求に合致しないことが発覚した場合、評価結果を取り消し、書面にてデータ処理者に通知する。
一方、データ処理者はデータ域外移転活動を中止しなければならない。

(8)個人情報保護法

概要

文献概要	名称	個人情報保護法		
	主旨	2021年8月20日、第13回全国人民代表大会常任委員会第30回会議において、2021年11月1日から施行される「中国個人情報保護法」(以下「個人情報保護法」という)が正式に可決された。「個人情報保護法」は、個人情報保護の分野における基本法であり、個人情報の権利と利益の保護と取扱いの標準化を中核とし、個人情報の適正利用とのバランスを図る。		
	国・地域	中国	適用分野	個人情報保護の分野
	策定者	全国人民代表大会常任委員会	対象者	中華人民共和国の領土内で個人情報を処理する活動の自然人
	遵守義務	適法性、正当性、必要性、誠実さの原則を遵守し、誤解、詐欺、強要等によって個人情報を取り扱わないものとする。		
	普及状況	「個人情報保護法」は中国国内における個人情報の収集、保存、使用、加工、転送、提供、公開、削除等情報処理行為、及び国外で国内における個人に製品やサービスの提供を目的とする個人行動の分析、評価等個人情報の処理行為に適用される。		
	策定年	2021年	ページ数	10

カテゴリ	カテゴライズ	「個人情報保護法」及び規制は、「中華人民共和国民法」第1,034条 [個人情報の定義] 自然人の個人情報は法律で保護される。
	カテゴリ評価	「個人情報保護法」は、ネットワークデータ法制度我が国「サイバーセキュリティ法」と「データセキュリティ法」を中継した後、画期的な意義をマークする。
	カテゴリ確認要求	「個人情報保護法」の正式施行により、市民の個人情報保護に関する法令の制定ニーズが明確化された。この法律は、民法、サイバーセキュリティ法、データセキュリティ法、電子商取引法などの法律とともに、市民の個人情報の「保護ネットワーク」として織り込まれる。
	制度的枠組み	この法律は8章74条で構成されて、個人情報の取扱いに関する規則・権利、国境を越えた提供に関する規則、取扱者の義務・保護責任を果たす部門、関連規定に違反する法的責任など、基本的な法的枠組みを構築し、個人情報保護分野我が国における立法トップの設計を完成する。

関連URL	http://www.gov.cn/xinwen/2021-08/20/content_5632486.htm

(8)個人情報保護法
詳細

「個人情報保護法」は、個人情報保護における重要な問題を解決するための強力な法的保護手段を提供し、以下に個人情報保護法の主な内容について説明する。

個人情報の明確な定義	個人情報は、匿名化処理後の情報を除き、識別又は識別可能な自然人に関する電子的又はその他の方法で記録されるさまざまな情報である。 個人情報の取扱いには、個人情報の収集、保管、利用、加工、送信、提供、開示、削除等が含まれる。
個人情報の過剰収集の抑制	個人情報の取扱いは、個人の権利及び利益に最小限の影響を与える明確かつ合理的な目的を有するものとする。 個人情報の収集は、取扱いの目的の達成に最低限とし、過度に収集してはならないものとする。 いかなる組織又は個人も、他人の個人情報を違法に収集、使用、処理、又は送信したり、他人の個人情報を違法に売買、提供、又は公開したりすることはできない。
差別的待遇の禁止	個人情報の取扱い者は、個人情報を利用して意思決定を自動化し、意思決定の透明性と結果の公平性を確保し、取引価格等の取引条件に不合理な差別的待遇を課さない。
パーソナライズの通知を強化ない	自動意思決定を通じて個人に情報をプッシュし、商業マーケティングを行う場合は、個人の特性に合わないオプションを提供するか、個人に簡単な拒否方法を提供する必要がある。 個人の権利と利益に重大な影響を及ぼす決定を自動化された意思決定を通じて行われる場合、個人は、個人情報の取扱者に説明を求める権利を有し、個人情報の取扱いを拒否する権利を有する。
公共の場での画像取得の標準化	公共の場に画像取得及び個人識別装置を設置するには、公共の安全を維持するために、国の関連規定を遵守し、重要なプロンプトマークを設定する必要がある。 収集された個人画像及び識別情報は、公共の安全を維持するためにのみ使用され、他の目的のためにのみ使用することはできない。個人の個別の同意を得た場合を除く。
機密性の高い個人情報の処理	機密性の高い個人情報とは、生体認証、宗教的信念、特定の身元、医療、金融口座、所在の軌跡、14歳未満の未成年者の個人情報など、人の尊厳や人や財産の安全を危険にさらすおそれのある個人情報である。 個人情報の取扱い者は、特定の目的と十分な必要がある場合、かつ厳重な保護措置を講じた場合にのみ、機密性の高い個人情報を取り扱う。
個人情報のクロスボーダー提供を厳格に行う	重要な情報インフラ事業者及び国家ネット情報部門が定める数の個人情報を取り扱う者は、中華人民共和国の領土内で収集・生成された個人情報を国内に保管しなければならない。 海外に提供する必要がある場合は、国家ネットワーク通信部門が主催するセキュリティ評価に合格する必要がある。
個人権利の規定	個人は、個人情報の取扱いについて知る権利、決定する権利、又は他者による個人情報の取扱いを制限又は拒否する権利を有する。 法令・行政規則に別段の定めがある場合を除く。
訴訟は法律に従って提起する	個人情報の取扱者がこの法律の規定に違反して個人情報を処理し、多数の個人の権利と利益を侵害した場合、人民検察院、法律で定められた消費者団体、及び国家ネットワーク通信部門が定める組織は、法律に従って人民裁判所に訴訟を起こすことができる。

(8)個人情報保護法
詳細

- 個人情報保護法の第8章第74条によると、関連法律の上で、当該法規は個人情報の保護が従うべき原則と個人情報の処理規則をさらに細分化し、改善し、個人情報処理活動における権利・義務の境界を明確にし、個人情報保護活動の体制とメカニズムを健全にする。
- 個人情報保護法は広範な国民のネットスペースの合法的権益を確実に維持し、保障し、発展させ、デジタル経済の進化におけるより多くの獲得感、幸福感、安心感を享受できるようにする。

ハイライト1	個人情報保護原則の確立	個人情報保護の原則は個人情報の収集、使用の基本的なルールであり、個人情報保護の具体的な規則を構築する制度の基礎となる。
ハイライト2	活動の規範化、権益の保障	個人情報保護法は個人情報処理活動の規範化、個人情報権益の保障をめぐり、「告知-同意」を核心とする個人情報処理規則を構築した。
ハイライト3	「ビッグデータの利用でリピーターの権益を侵害する」行為を禁止、自動的な意思決定の規範化	個人情報処理者が個人情報を利用して自動化意思決定を行う場合、意思決定の透明性と結果の公平、公正を保証し、個人が取引価格などの取引条件に対して不合理な差別待遇を実施してはならないことを明確に定めた。
ハイライト4	敏感な個人情報の厳格な保護	個人情報保護法が生物識別、宗教信仰、特定身分、医療健康、金融口座、行動軌跡などの情報を敏感な個人情報と定めている。 個人情報保護法は、特定の目的と十分な必要性を有し、厳格な保護措置を講じた場合にのみ、敏感な個人情報を処理することができるとともに、事前に影響評価を行い、処理の必要性及び個人権益への影響を個人に通知しなければならないことを要求する。
ハイライト5	国家機関活動の規範化	個人情報保護法は国家機関が個人情報を処理する活動に対して専門的な規定を行う。 特に国家機関が個人情報を処理する活動に本法を適用することを強調し、しかも個人情報を処理するには法律、行政法規に規定された権限と手順に従って行わなければならず、法定職責を履行するために必要な範囲と限度を超えてはならない。
ハイライト6	個人に十分は権利を与える	個人情報処理活動における個人の各権利を、個人情報処理規則と処理事項の知覚、同意と撤回同意、及び個人情報の照会、複製、訂正、削除などの総括を知る権利、決定権に昇格させ、個人が個人情報の処理を制限する権利を明確にする。
ハイライト7	個人情報処理者の義務の強化	個人情報保護法は専門のセクションを設けて個人情報処理者のコンプライアンス管理と個人情報安全保障などの義務を明確にし、個人情報処理者に規定に従って内部管理制度と操作規程を制定し、相応の安全技術措置をとり、責任者を指定して個人情報処理活動を監督し、定期的に個人情報活動をコンプライアンス監査することを要求する。 敏感な個人情報の処理、個人を利用した自動化意思決定、個人情報の対外提供又は公開などの高リスク処理活動に対して事前影響評価を行い、個人情報漏洩通知と救済義務などを履行する。
ハイライト8	大型インターネットプラットフォームの特別義務	大型インターネットプラットフォームに対して特別な個人情報保護義務を設定し、国家の規定に基づいて個人情報保護コンプライアンス制度体系を確立し、健全化し、主に外部メンバーからなる独立機構を設立し、個人情報保護状況を監督する。
ハイライト9	個人情報域外移転の規範化	個人情報の権益と安全を保障する客観的な要求を満たし、国際経済貿易の往来の現実的な需要に適応するために、明確で系統的な個人情報の越境流動規則を構築した。
ハイライト10	個人情報保護体制の健全化	個人情報保護の監督・管理・司法の協業を強化するため、国家ネット情報部門の個人情報保護の監督管理における統一的協調役割をさらに明確にし、その統一的協調職責を具体的に規定した。

(9)Data Protection Best Practices
概要

文献概要	名称	Data Protection Best Practices		
	主旨	産業IoT(IIoT)におけるデータ保護のベストプラクティスを記載。		
	国・地域	国・地域の特定はしていない	適用分野	産業向け
	策定者	Industry IoT Consortium	対象者	サイバーセキュリティ、プライバシー、IIoTの信頼性に関わる関係者向け
	遵守義務	データ保護の下にあるさまざまなドメインやサブドメインに関するベストプラクティスを提示するものであり、強制力はない。ただ、保存データや移動中のデータ、使用中のデータに本ベストプラクティスの対策を適用しなければ、サービスの中断や重大な労働災害、IPの喪失、**規制上の罰金**、ブランドの評判への悪影響など、IIoTシステムに深刻な結果をもたらす可能性がある。		
	普及状況	普及状況に関する情報はなかったが、同コンソーシアムのメンバーにはファーウェイ、デル・テクノロジーズ、ジョンソン&ジョンソン、カスペルスキー・ラボ、韓国インダストリー4.0協会、マイクロソフト、三菱電機、NEC、東芝などが名を連ねている。		
	策定年	2019年	ページ数	38ページ

カテゴリ	カテゴライズ	データセキュリティー(キー管理とRoT、認証、アクセスコントロール、監査・監視)、データ整合性、IoTインフラストラクチャ保護、データ保護とIoT信頼性、その他のデータ保護に関する考慮事項(データプライバシー、データの機密性、データ レジデンシー、データの電子情報開示とリーガルホールド、データライフサイクル管理)に分類されている。
	カテゴリ評価	各カテゴリーにおいて、保存データ(ライフサイクル中のさまざまな時点で保存されるデータ)、移動中のデータ(ある場所から別の場所に共有又は送信されるデータ)、又は使用中のデータ(処理中のデータ)におけるベストプラクティスを示している。
	カテゴリ確認要求	IoT環境におけるデータに対して、望ましいレベルのセキュリティを実現するために必要な対策とベストプラクティスの明示であり、要求事項ではない。
	制度的枠組み	IoTセキュリティ成熟度モデルを補完し、インダストリアル・インターネット参照アーキテクチャ(IIRA)とインダストリアル・インターネット・セキュリティ・フレームワーク(IISF)の概念に基づき構築されている。

関連URL	https://www.iiconsortium.org/pdf/Data_Protection_Best_Practices_Whitepaper_2019-07-22.pdf

(9)Data Protection Best Practices
詳細

データセキュリティー：キー管理

項目	ベストプラクティス
生成	キー生成プロセスの強さは、予測不可能なキーを生成する乱数供給能力に依存する。強化・重要なセキュリティレベルの場合、承認された暗号化ハードウェアの乱数のみを使用する必要がある。
登録	キーとそれを使用するユーザー、デバイス、システム、又はアプリケーションを関連付け。
ストレージ	キーは許可されたユーザー、又はアプリケーションのみがアクセスできるような方法で保管されなければならない。可能であれば、TPM(Trusted Platform Modules)のような専用の承認されたハードウェアに保管されるべきである。
キー作成	デバイスは以下のいずれか。 1. 内部でキーを生成 2. ある程度デバイス間でユニークな内部物理特性に基づいてキーを計算(Physical Unclonable Functions) 3. 外部から制御された方法でキーを受け取る
キー使用	使用中のキーの露出を最小限にするために最善の努力(最小特権の原則に基づきキーへのアクセスを制御、キーを単一目的にのみ使用、暗号操作終了後にワーキングメモリからキーを削除など)
キーローテーション	キーは定期的に更新し、漏洩のリスクをコントロールする必要がある。
キーバックアップ	適切なキーのバックアップ戦略により、必要最小限のキーのコピーのみ作成し、保管が適切に保護されることを保証。
キー回復	キーが漏洩することなく、また許可された者のみが復元できるような方針と手順を策定。
キー失効	漏洩又は漏洩の疑いのあるキーは失効させ、交換しなければならない。
キーサスペンション	キーが暗号化に使用されなくなった場合でも、新しいキーに更新されていない運用データを復号する必要がある場合に適用。
キー破壊	すべてのバックアップコピーを含め、使用されなくなったキーは破棄する必要がある。

データセキュリティー： RoT(Root-of-Trust)

項目	ベストプラクティス
保存 (At rest)	HRoTは、保存データの重要なセキュアストレージの完全性を検証することを目的とした、不変の秘密を提供する。暗号化キーや重要な認証、又はID機能からの信頼を必要とするその他の秘密キー、又は公開キーを保存するために使用できる。
移動時 (In motion)	HRoTは、移動中のデータを保護するための安全な通信路を確立するために必要な認証・検証・測定を提供する。
使用時 (In use)	HRoTは、認証されたセキュアブートプロセッサーや保存データの構成保護を通じて、使用中のデータを保護し、使用中のデータの整合性をサポートする。
例 (Example)	ARM Trust Zoneは、ARMプロセッサが実現するセキュアパーティションにセキュリティ証明書やソフトウェア認証署名を保存するためのセキュアストレージとして使用することができる。

データセキュリティー：認証付き暗号化

項目	ベストプラクティス
保存 (At rest)	1. 保存しているデータには暗号化されたコンテナを使用。 2. NSA Suite B、又はその他の広く承認された暗号化アルゴリズムを使用。
移動時 (In motion)	1. 保護する必要のあるデータフローとその方法(デジタル署名、パケット暗号化、ユーザーペイロード暗号化)を決定 2. 要件を満たす対応技術を統合(TLS、DTLS、DDS Securityなど) 3. NSA Suite B、又はその他の広く承認された暗号化アルゴリズムを使用
使用時 (In use)	1. RoTとキー管理を参照 2. メモリの完全暗号化の実践検討
例 (Example)	分散制御システムのすべてのデータを暗号化することは、コスト、時間、性能の制約から実現不可能な場合がある。ヘルスケア環境では、重要なデータは暗号化と認証の両方を考慮する必要があるが、環境温度のような他の方法で決定される可能性がある非重要データは、CPUとネットワーク帯域幅を最適化するためにHMACによる署名、又は認証のみを行うことができる。

(9)Data Protection Best Practices
詳細

データセキュリティー：相互認証によるセッションキーの確立

項目	ベストプラクティス
移動時 (In motion)	1. 信頼できる証明書と PKI を使用して、ネットワーク参加者(ユーザー、アプリケーションなど)のIDを確立 2. 楕円曲線ディフィー・ヘルマン鍵共有など、完全な前方秘匿を実現する推奨暗号スイートを使用 3. セキュリティポリシーに基づき、証明書の失効と更新を行うことで、ネットワーク参加者間の信頼関係を継続的に見直し、確立する。
使用時 (In use)	運用データの場合： 1. 保護する機密データを特定 2. キーマテリアルはTPMなどのハードウェアに保存 3. 機密データを暗号化しても、CPUで処理したり、CPUキャッシュに平文で保存したりできるセキュアエンクレーブを構成
例 (Example)	移動時のデータについては、病院の臨床環境にあるデバイスを検討。すべての機器が通信を必要とするわけではないが、血圧計や心電図、パルスオキシメーターなどインテリジェント・ヘルスケアに必要な機器は、お互いを信頼できるものでなければならない。

データセキュリティー：アクセスコントロール

項目	ベストプラクティス
保存 (At rest)	1. アクセス制御ポリシー定義 2. 読み取り／書き込みのアクセスは、データエンティティ(ファイルなど)又はコンテナ(データベースやストレージコンテナなど)ごとに定義 3. 自動化されたメカニズムは、アクセスポリシーを適用する必要あり
移動時 (In motion)	保存と同じ
使用時 (In use)	保存と同じ
例 (Example)	ネットワーク上のすべてのデバイスが、データに関して同じ動作をするわけではない。ヘルスケア環境では、輸液ポンプアプリケーションは投薬コマンドに対する読み取りアクセス権を持つべきだが、他のデバイスが取得する心拍数や体温などの患者データに対する書き込みアクセスは拒否されるべき。

データセキュリティー：監査・監視

項目	ベストプラクティス
保存 (At rest)	保存データはアクセスポリシーに違反していないか監視し、セキュリティ監査のためにログを作成する。
移動時 (In motion)	移動データは、イングレス及びイグレスポリシーを監視し、セキュリティ監査のためにログを作成する必要がある。
使用時 (In use)	使用中のデータは、不正アクセス又はプライバシー要求がないか監視する必要がある。
例 (Example)	産業用IoTデバイスの監視の例として、OT(Operations Technology)環境におけるICSやSCADAデバイスの監視が挙げられる。これらのデバイスは、複雑で高価値のミッションクリティカルなシステムを制御している。

(9)Data Protection Best Practices
詳細

データ整合性

項目	ベストプラクティス
保存 (At rest)	保存データの整合性は、バックアップやレプリケーションなどの標準ベースのメカニズムによって保証される。システムの設定データを監視し、不正な変更を検出したり、重要なデータを不正な変更(悪意又は偶発的)から直接保護する仕組みが必要。
移動時 (In motion)	移動データの整合性は、標準ベースの暗号化アルゴリズムを使用するプロトコルによって変更、又は改変が確実に検出されるようにすることで保証する必要がある。
使用時 (In use)	使用データの整合性は、ユーザーやアプリケーションに対するポリシーベースの認可とアクセス制御、及び実行用の信頼された安全なメモリなどのメカニズムによって保証されること。IoTデータを生成し、操作するシステムへの不正なソフトウェア(ウイルス、マルウェアなど)の侵入を防止・検出するメカニズムを提供する必要がある。
例 (Example)	TLS 1.2以上を用いた標準的なセキュア通信により、ネットワークレベルで機密性と整合性を保護し、移動データの整合性が保証される。

IoTインフラストラクチャの保護

項目	セキュリティの詳細な戦略
IoTハードウェアメーカー/インテグレーター	• ハードウェアのスコープを最小限の要件とする • ハードウェアの改ざん防止 • 安全なハードウェアを中心に構築 • アップグレードの安全性
IoTソリューションデベロッパー	• 安全なソフトウェア開発方法論に従う • オープンソースソフトウェアを慎重に選択 • 慎重な統合
IoTソリューションデプロイヤー	• ハードウェアを安全に展開(デプロイ) • 認証キーの安全な保管
IoTソリューションオペレーター	• システムを常に最新に保つ • 悪意のあるアクティビティからの保護 • 頻繁な監査 • IoTインフラを物理的に保護 • クラウドクレデンシャルの保護

システムの安全性に関するデータセキュリティの役割

項目	ベストプラクティス
保存 (At rest)	下記の移動時と同じ。
移動時 (In motion)	エンドポイントの相互認証を確保。システムの適切な安全機能を確保するために、IoTデータの整合性を保護。
使用時 (In use)	移動時と同じ。セーフティクリティカルシステムが、安全パラメータの範囲外に変更されたデータを処理する場合、システムの整合性が損なわれる可能性がある。
例 (Example)	IEC 61508に基づき制御システムと安全システムを分離する必要があるIoTユースケースでは、安全に影響を与えるIoTデータに対して、特定のデータ保護対策を適用する必要がある。

その他のデータ保護に関する考慮事項：データの最小化

項目	ベストプラクティス
保存 (At rest)	1. 収集する個人情報の範囲を特定 2. その範囲を個人情報保護法の要件に照らして検証 3. 個人情報の収集が最小限になるように設計されたデータ収集方法を導入 4. ユースケースの要件に基づき、個人データの収集を最小限に抑える 5. 保管中(処理完了後)の個人データを暗号化
移動時 (In motion)	収集から処理までの移動中に個人データを暗号化。
使用時 (In use)	IoTソリューション内、及びそれ以外での個人情報の利用制限を課す。
例 (Example)	GDPRは、特定のユースケースの範囲を満たすため、データ対象者から個人データを収集する必要がある場合があり、これらのユースケースの範囲と個人データは分析・検証・文書化されなければならない。個人データの収集には、データ対象者の同意プロセスが組み込まれていなければならない。データ侵害が発生した場合、特定の期間内に特定の侵害プロトコル(通知を含む)を制定すること。

(9)Data Protection Best Practices
詳細

その他のデータ保護に関する考慮事項：データの匿名化

項目	ベストプラクティス
保存 (At rest)	匿名化されたデータは、定義上、プライバシー保護の対象とはならない。決定を下すのは、組織の法務部門又はデータ保護責任者(DPO)である。
移動時 (In motion)	保存と同じ。
使用時 (In use)	保存と同じ。
例 (Example)	適切に匿名化された個人データがGDPRの管理対象から外れるかどうかを判断するのは、組織のデータ保護責任者。

その他のデータ保護に関する考慮事項：データの仮名化(Pseudonymization)

項目	セキュリティの詳細な戦略
保存 (At rest)	1. 仮名化する個人データの範囲を特定 2. 仮名化戦略を定義(汎用のコードに置き換えるか、データ型ごとに特定のコードに置き換える) 3. 前記データに仮名化プロセスを実装 4. 匿名化アクションが、物理ストレージ層(必要な場合)に至るまで、アーキテクチャスタックのすべての層で実装されていることを確認 5. 元の個人データと仮名化コードの対応付けを安全な環境で保管(個人データにおける制限と同じ制限を受ける)
移動時 (In motion)	機密データにも同様のセキュリティ管理を適用。
使用時 (In use)	機密データにも同様のセキュリティ管理を適用。
例 (Example)	GDPRでは、仮名化データは個人データと仮名化コードの対応付けにアクセスすることで元の個人データを復元することができるため、プライバシー管理及び制限の対象とされている。

その他のデータ保護に関する考慮事項：データの機密性

項目	ベストプラクティス
保存 (At rest)	• 本質的に機密であると見なされるデータの範囲を特定 • データへのアクセスに対する制限のレベルを決定 • データに機密であることを表示する方法を実装 • データセキュリティのセクションで説明したセキュリティ方法とメカニズムを実装
移動時 (In motion)	収集から処理への移動中に機密データを暗号化。
使用時 (In use)	データセキュリティのセクションで説明したセキュリティ方法とメカニズム(例えば、暗号化、認証、アクセスコントロールなど)を実装。
例 (Example)	データの暗号化、データの最小化、データの匿名化、データの仮名化など、データプライバシーと同様のメカニズムや技術をデータの機密保持に使用することができる。

その他のデータ保護に関する考慮事項： データレジデンシー

項目	ベストプラクティス
保存 (At rest)	1. 法律や規制によっては、特定のデータタイプのデータを管轄区域外に保存することを許可しない場合がある。 2. データタイプの分類を作成 3. データレジデンシー要件があるデータタイプを特定 4. データをソースとデータタイプで分類 5. データレジデンシー要件があるデータを、物理的に管轄内に位置する場所に保存するIoTシステムを設計 6. 法務・コンプライアンス部門は、暗号化されていれば管轄外でも保存可能とする可能性あり
移動時 (In motion)	上記の制約事項は、移動データにも同様に適用される。
使用時 (In use)	上記の制約事項は、使用データにも同様に適用される。
例 (Example)	米国のHIPAAやHITECH、英国のNHSなどは、個人健康情報を国の管轄区域内に置かなければならないと定めている。

(9)Data Protection Best Practices
詳細

その他のデータ保護に関する考慮事項：データのeDiscoveryとリーガルホールド

項目	ベストプラクティス
保存 (At rest)	1. 調査や訴訟の範囲に「対応する」と判断されたデータの範囲を定義 2. スコープに「対応する」IoTデータを検索して見つける 3. 真正性の検証を行った上で、IoTデータ及びメタデータを収集 4. 収集したデータを法務チームと調査チームに配信 5. IoTデータを保留(本データの編集又は削除する全ての権利を取り消す) 6. 必要な場合は、不変性を確立するために、定期的な整合性チェックを実施 7. IoTデータが調査や訴訟のために不要と判断された場合、当該データの保留を解除 8. 上記に関する監査証跡を保持
移動時 (In motion)	上記のデータは、個人情報又は機密情報である可能性がある。移動データは、個人情報及び機密情報に対して実施されているデータ保護方法を適用する必要がある。
使用時 (In use)	移動時と同様の制約。
例 (Example)	EDRM.netは、電子証拠開示のフレームワークとして広く受け入れられている。

その他のデータ保護に関する考慮事項：データライフサイクル管理

項目	ベストプラクティス
保存 (At rest)	• システムで生成・消費される固有のデータタイプの分類を定義 • データタイプに応じた法的・規制上のライフサイクル及び処分の要件を特定 • データタイプのライフサイクルポリシーを定義(EoLアクションを含む) • データのライフサイクル中にデータに整合性と不変性を適用する方法を実装 • ライフサイクルが終了したデータに対してEoLアクションをトリガーし、実施する方法を実装 • 上記について、法的な証拠となる監査証跡を作成
移動時 (In motion)	IoTシステム・アーキテクチャ・スタックの設計では、IoTデータがいつ、どこで動いて存在できるのか、そのアーキテクチャのセグメントを特定する必要がある。また、このデータがこれらのセグメントに恒久的に保持されないことを保証しなければならない。
使用時 (In use)	移動時要件と同様に、システム・アーキテクチャ・スタックの設計では、IoTデータを使用できるセグメントを特定する必要がある。
例 (Example)	EUのGDPRでは、データ対象者が要求した場合、特定の個人データを削除することが義務付けられている。

別紙 3

IoT セキュリティ・セーフティ・フレームワーク Version 1.0
実践に向けたユースケース集

目次

1. 本稿の位置づけと構成 2
1-1 「IoT セキュリティ・セーフティ・フレームワーク」の概要 2
1-2 本稿の位置づけと構成 2
1-3 想定読者と利用用途 3
2. 「IoT セキュリティ・セーフティ・フレームワーク」実践に係るユースケース集 4
2-1 対象となるユースケース 4
2-2 ユースケースにおける記載事項 5
2-2-1 リスクアセスメント、リスク対応に向けた事前準備 7
2-2-2 リスクアセスメント 8
2-2-3 リスク対応 13
2-3 具体的なユースケース 19
2-3-1 家庭用ガス給湯器の遠隔操作 19
2-3-2 ドローンを活用した個人による写真撮影 37
2-3-3 物流倉庫内の AGV による自動ピッキング 50
2-3-4 化学プラント施設内の蒸留工程の自動制御 67
2-3-5 工場内のロボットによる部材加工作業（溶接工程）の自動化 84
2-3-6 金属製造現場の温度センサ等による製造設備の状態監視 101
添付 A 対策要件 1
添付 B 実際に講じる対策の例 1

1. 本稿の位置づけと構成

1-1 「IoT セキュリティ・セーフティ・フレームワーク」の概要

「IoT セキュリティ・セーフティ・フレームワーク」（以下、「IoT-SSF」という。）は、サイバー空間とフィジカル空間をつなぐ新たな仕組みによってもたらされる新たなリスクに着目し、リスク形態及びそうしたリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示するものである。

IoT 機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するための「基本的共通基盤」を提供し、IoT という新たな仕組みを社会として効果的に受容できるにすることを目的として、IoT-SSF では IoT 機器・システムについて、リスクの捉え方とその対応に係る基本的な考え方を集約した 3 つの軸を活用し、機器・システムをカテゴライズするとともに、適切な対策の内容を整理して比較・検討することを提案している。

1-2 本稿の位置づけと構成

本稿では、今後様々な分野/業界のプレーヤーが、IoT-SSF を「基本的共通基盤」として活用するために、既存のリスクマネジメントのプロセスも考慮しつつ、一連の IoT-SSF の適用の流れを複数のユースケースを用いて例示するものである。

本章を導入として、2 章ではユースケース選定の考え方(2-1)、各ユースケースに共通する記載項目(2-2)、6 件の具体的なユースケース(2-3)を記述する。なお、個別のユースケースに記載される対策としてはセキュリティに関連した対策を記述し、セキュリティに直接関連しない対策（例：機器・システムの経年劣化による欠陥や故障に対する対策）については本稿の対象外とした上で、これらを含む対策の整理については本稿の改訂時における課題とする。本稿にて詳述するユースケースは、以下に示す通りである。

- 家庭用ガス給湯器の遠隔操作 (2-3-1)
- ドローンを活用した個人による写真撮影 (2-3-2)
- 物流倉庫内の AGV[1]による自動ピッキング (2-3-3)
- 化学プラント施設内の蒸留工程の自動制御 (2-3-4)
- 工場内のロボットによる部材加工作業（溶接工程）の自動化 (2-3-5)
- 金属製造現場の温度センサ等による製造設備の状態監視 (2-3-6)

添付としては、本編でも参照されるセキュリティ、セーフティの確保に資する対策要件（添付 A）、添付 A に示された対策要件ごとに実際に講じる対策の例（添付 B）を整理している。これらは各ユースケース固有の事情に依存しない一般的に適用し得る内容を示しているため、想定読者において具体的な対策を検討する際に適宜参照されたい。

本稿における用語法は、「サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0」（以下、「CPSF」という。）及び IoT-SSF に準じることとする。各種用語定義については、それらを参照されたい。

[1] AGV（Automatic Guided Vehicle）は、人間が運転操作を行わなくとも自動で走行可能な搬送車である。

1-3　想定読者と利用用途

本稿の具体的な想定読者と利用用途は以下に示す通りである。想定読者のうち、本稿は主にIoT機器・システム及び関連サービスに係る様々な主体（事業者）により活用されることを想定する。本稿における記述はあくまで一例であり、事業者等による実際の適用に当たっては、本稿に記述されていないリスクや対策等が新たに抽出され得ることに留意されたい。

- **IoT機器・システムを通じて提供されるサービスのユーザ（IoT利用者）**
  IoT 機器・システム及び関連サービスの利用を計画したり、現に利用しているものの、状況をレビューしたりする際に、セキュリティやそれと関連するセーフティの観点で自身が考慮すべき事項や、IoT サービス提供事業者等に対応を依頼する事項を整理する参考として本稿を参照することができる。

- **IoT機器・システムを通じて提供されるサービスの開発者（IoTサービス開発者）**
  自社製品として IoT 機器・システム又は関連サービスを企画・設計する際、あるいはそのような機器・システムの設計や開発に係る委託を他社から受けた際に、対象機器・システムの運用開始より以前にセキュリティやそれと関連するセーフティの観点で考慮すべき事項や、IoT 利用者や関連事業者（例：業務委託先）等に対応を依頼する事項を整理する参考として本稿を参照することができる。

- **IoT機器・システムを通じて提供されるサービスの提供者（IoTサービス提供者）**
  IoT 機器・システム又は関連サービス[2]を、新たに IoT 利用者に提供する際、あるいは既に提供しているものをレビューし、品質等の改善を図ろうとする際に、対象機器・システムの運用中又は運用終了時にセキュリティやそれと関連するセーフティの観点で考慮すべき事項や、IoT 利用者や関連事業者（例：業務委託先）等に対応を依頼する事項を整理する参考として本稿を参照することができる。

- **IoT機器・システム及び関連サービスを適切に管理する制度・環境を検討する者**
  IoT 機器・システムに関連するセキュリティ及びそれと関連するセーフティの観点から、今後より具体的な制度・環境を検討しようとする際の参考として本書を参照することができる。

[2] ここで、IoT サービス提供者に係る「IoT 機器・システムまたは関連サービス」には、利用者に提供されるサービスのみならず、それに付随して発生し得る役務（例：機器・システムの保守業務）の提供等が含まれ得る。

2. 「IoT セキュリティ・セーフティ・フレームワーク」実践に係るユースケース集

2-1 対象となるユースケース

IoT-SSF にて既に述べられているように、第 2 層におけるセキュリティ対策には、様々な IoT 機器・システムに共通する課題への対応だけでなく、利用者の区分や利用環境の多様性も十分に踏まえた対応が必要となる。全体としての網羅性を意識しつつ、想定読者が IoT 機器・システム（関連するサービスを含む）を提供又は利用する際に、ユースケースがセキュリティ確保を目指した取組みの助けとなるよう、選定にあたっては以下の観点を考慮した。

- **IoT 機器・システムの利用者の区分**
  IoT 機器・システムの利用者の区分を、「個人又は家庭」と「事業者（主に産業）」」に分類し、双方からユースケースを選定する。

- **利用環境の多様性**
  IoT 機器・システムが現に利用される環境には非常に多様なものが想定され得るが、本稿では、消費者用途として消費者現場（家庭、公共空間）、産業用途として製造現場と物流現場を取扱う。また、製造現場としては、網羅性を確保する観点から、原料製造（プラント）、製品製造（工場）という 2 つの業態からユースケースを選定する。

- **IoT 機器・システムの汎用性及び普及率の高さ**
  より幅広い読者にとって参考となるよう、選定する IoT 機器・システムは、利用や提供が特定の事業者等に限定されない汎用的なものであり、広く普及もしくはこれから普及が見込まれるものが望ましい。したがって、以下の 2 点を考慮してユースケースを選定する。
  - 利用が特定の事業者等に限定されない、汎用的な機器・システム
  - 現時点で普及している、もしくは、これから普及が見込まれる機器・システム

- **想定されるリスクと対策の多様性**
  各 IoT 機器・システムは上記の通り、利用者や利用環境が異なるため、使用上のリスクもそれぞれ異なる。加えて、想定されるリスクの差異は、優先的に講じるべき対策の差異にもつながる。読者にとって具体的な検討に参考となるよう IoT 機器・システムに係る使用上のリスク及び当該リスクへの対処方法において、他のユースケースと比較して、特徴的な考慮事項があるようなユースケースを選定する。

上記に示したユースケース選定の考え方を踏まえ、本稿では以下に示す 6 件のユースケースを取扱う。

なお、IoT-SSF を参照した上で IoT 機器・システム及び関連サービスにおけるリスクマネジメントを実行する主体を IoT-SSF の「適用主体」と定めた上で、ユースケースごとにこれらを定めるものとする。

表 1 本稿で取扱うユースケースの一覧

No	利用者の区分	利用環境	ユースケース	想定する適用主体	選定理由
1	個人又は家庭	家庭	家庭用ガス給湯器の遠隔操作	IoT サービス開発者、IoT サービス提供者	・家庭用ガス給湯器は現状多くの住宅等に備えられており、その遠隔操作についても、今後利用の拡大が見込まれるため。 ・インシデントが利用者の負傷につながりやすく、セーフティの側面がより重要となるケースであるため。
2		公共空間	ドローンを活用した個人による写真撮影	IoT サービス開発者、IoT サービス提供者	・多種多様な活用方法が想定されるドローンは、ビジネス用途を含めて、今後様々な業界で利用の拡大が見込まれるため。 ・利用者に限らず周囲のヒトやモノへ被害を及ぼす可能性があり、利用者のスキルや社会的な制度等が要求事項として含まれ得るため。
3	事業者（主に産業）	物流現場	物流倉庫内の AGV による自動ピッキング	IoT 利用者	・AGV は様々な利用シーンでの活用が想定される機器であり、物流業界や製造業界等において今後利用の拡大が見込まれるため。 ・機器・システムの停止等が、サプライチェーンにおける多くのステークホルダーに影響しやすいケースであるため。
4		製造現場（原料製造）	化学プラント施設内の蒸留工程の自動制御	IoT 利用者	・自動制御システムは既に多くの現場で採用されており、特に PA(Process Automation)技術を活用する事業者にとって参考になると考えられるため。 ・自動制御システムの停止等、可用性の損失が課題になるケースであるため。
5		製造現場（製品製造）	工場における部材加工作業（溶接工程）の自動化	IoT 利用者	・製造現場におけるロボットは引き続き利用の拡大が見込まれており、特に FA(Factory Automation)技術を活用する多くの事業者にとって参考になると考えられるため。 ・制御データの改ざんによる異常動作及びそれに伴う品質劣化等が課題になるケースであるため。
6			金属製造現場の温度センサ等による製造設備の状態監視	IoT サービス開発者、IoT サービス提供者	・温度センサ等による設備の状態監視は産業用途（例：原料製造、製品製造）における共通的な要素であり、多様な現場にて参考になると考えられるため。 ・状態監視は品質管理上、重要な要素であり、これらに関連するセキュリティインシデントが事業者にとっての大規模な経済影響等につながりやすいため。 ・遠隔にて設備の状況を監視する点は各種サービス業においても参考になると考えられるため

2-2 ユースケースにおける記載事項

前述したように、IoT-SSF は、IoT 機器・システムを対象に、リスクの捉え方とその対応に係る基本的な考え方を集約した 3 つの軸を提示するものである。以下に示すリスクマネジメントの一般的なプロセスと関連付けて言うならば、提案されている 3 軸のうち、「第 1 軸：発生したインシデントの影響の回復困難性の度合い」（以下、「回復困難性の度合い」という。）と「第 2 軸：発生したインシデントの経済的影響の度合い」（以下、「経済的影響の度合い」という。）は「リスクアセスメント」において IoT 機器・システムに潜むリスクの整理に用いられるものであり、第 3 軸「求められるセキュリティ・セーフティ要求の観点」（以下、「求められるセキュリティ・セーフティ要求」という。）は「リスク対応」の方策をカテゴライズしたものと捉えることができる。

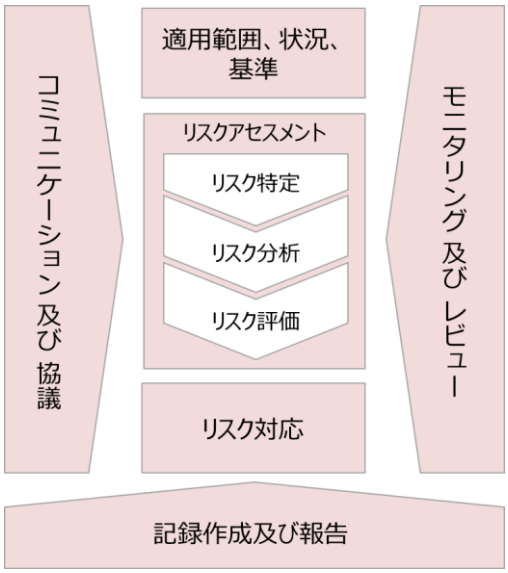


図 1 リスクマネジメントの一般的なプロセス[3]

CPSF では、上記プロセスを参照しつつ、国内外の関連文献の記載内容も加味して、「分析対象の明確化」、「想定されるセキュリティインシデント及び事業被害レベルの設定」、「リスク分析の実施」及び「リスク対応」のステップでセキュリティリスクマネジメントの流れを整理している。

これらを踏まえ、本稿では、前述した 6 つの具体的なケースを対象に、以下のステップからなる一連のリスクマネジメントプロセスを取扱う[4]。

- リスクアセスメント、リスク対応に向けた事前準備[5]（2-2-1）
- リスクアセスメント（2-2-2）
- リスク対応（2-2-3）

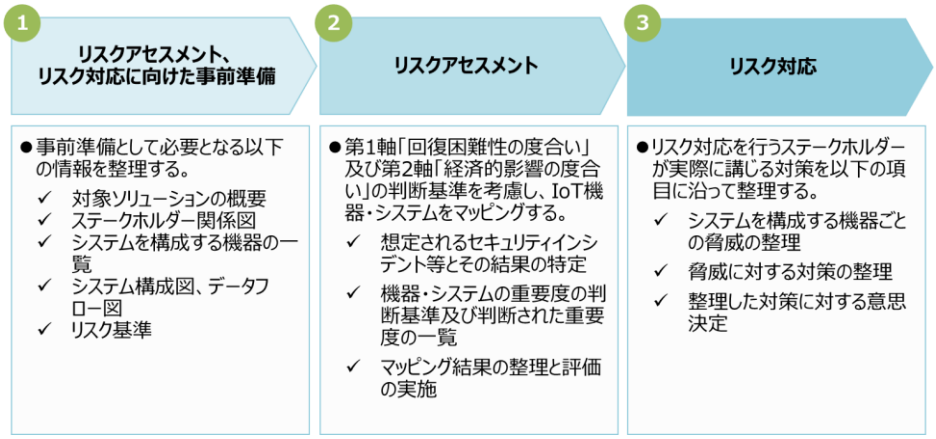


図 2 本稿におけるリスクマネジメントのステップ

[3] JIS Q 31000:2019 リスクマネジメント―原則及び指針を基に作成

[4] 「想定されるセキュリティインシデント及び事業被害レベルの設定」における事業被害レベル（セキュリティインシデントによりもたらされ得る被害の程度。）は、本稿では「第 1 軸：発生したインシデントの影響の回復困難性の度合い」と「第 2 軸：発生したインシデントの経済的影響の度合い」により評価される。

[5] JIS Q 31000:2019 における「適用範囲、状況、基準」に相当する内容を想定する。

想定読者に示した IoT 利用者、IoT サービス開発者、IoT サービス提供者において、リスクマネジメントに関連する部門は多岐にわたると想定される。したがって、適用主体においては対応部署の特定は慎重に行うことが望ましい。また、社内の情報システム部門や情報システムの担当者、製品の開発者、工場の生産技術担当者等の現場の担当者だけではなく、それらを管理する経営層やリスク管理部門等も一体となって全社的にリスクに対応することが望ましい。具体的には、経営層において、サイバーセキュリティに関する方針の設定や体制の整備、適切な経営資源の配分を行った上で、現場の担当者においてリスクマネジメントに関わる活動を行い、経営層に実施結果を共有した上で、必要に応じて内容を更新することが考えられる。本稿では、上記のプロセスにおける現場の担当者のリスクマネジメントに関連する活動に焦点を当て、一連の記述を行っている。

2-2-1 リスクアセスメント、リスク対応に向けた事前準備

IoT 機器・システムを対象にリスクアセスメント及びリスク対応を行う場合には、まず対象となる IoT 機器・システムの置かれている状況の整理ができていなければ、詳細で信頼性のあるリスクアセスメント及びリスク対応を行うことができない。したがって、事前準備として必要となる情報を整理するために、以下の内容を明確にする必要がある。

(1) 対象となる機器・システムの概要と目的

リスクアセスメント及びリスク対応の実施にあたり、対象となる IoT 機器・システム及び関連サービスの概要を特定する。その際、どのような目的で(why)、誰が(who)、何を(what)、いつ(when)、どこで(where)、どのように(how)利用するのかという点等を明確にすることが望ましい。

(2) ステークホルダー関連図

対象機器・システムの提供又は利用における自身の役割と責任を特定する。IoT 機器・システムの提供又は利用には、複数のステークホルダーが関与することが多いため、対象の機器・システムにおけるセキュリティ上のリスクを特定し対応する場合、自身に加えて、サプライヤや顧客のセキュリティ対策実装に係る役割や責任を考慮することが重要である。IoT 機器・システムの提供又は利用に関連して、典型的には以下の役割が特定され得る。

- IoT サービス提供者:IoT 機器・システム及び関連するサービスの運用や管理に係る者
- IoT サービス開発者:IoT 機器・システム及び関連するサービスの設計や開発に係る者(システムインテグレータや IoT 機器の製造者、部品サプライヤを含む)
- IoT 利用者:IoT 機器・システム及び関連するサービスのエンドユーザ

(3) システムを構成する機器の一覧

リスク分析実施範囲内に存在する機器、及び分析に必要となるシステムを構成する機器の一覧を作成する。IoT の典型的な構成要素としてかかる一覧には、IoT 機器(センサ、アクチュエータ)、ネットワーク、ネットワーク機器(ルータ、IoT ゲートウェイ等)、サーバ等が含まれ得る。

(4) システム構成図、データフロー図

対象となる機器・システムの構成図やデータフロー図を特定する。論理構成を示すネットワーク構成

図等を作成した後、分析用のシステム構成図及びデータフロー図を整理する。また、その際、各機器とそれらの操作や保守に係る組織やヒトとの関係性が明確化されていることが望ましい。本稿で示すユースケースでは、データフローのうち抜粋したデータフローを示す。

(5) リスク基準

機器・システムに関連する自身の目的に対して、受容できるリスク、又は相対的に受容しがたいリスクの大きさ及び種類をリスク基準として特定する。リスク基準を検討する際、一般的には、セキュリティインシデントにより生じ得る被害の大きさや、セキュリティインシデントの起こりやすさ、対象となる資産の重要度等が考慮され得る。

本稿では、2-2-2 にて述べるように、セキュリティインシデントにより生じ得る被害の大きさという観点に着目し、かかる基準を「目標とするリスクの水準」として、「回復困難性の度合い」と「経済的影響の度合い」に関連付けて整理する。特定されるリスク基準は、適用主体となる組織内部の上位のセキュリティやセーフティ等に関する基本方針や目標と整合したものとなっていることが望ましい。2-2-2 におけるアセスメントの結果をリスク基準と比較し、分析することを通じて、リスク対応を重点的に行う機器・システム等を特定したり、リスク対応の方針や内容等を検討したりすることが可能となる。

2-2-2 リスクアセスメント

(1) 想定されるセキュリティインシデント等とその結果の特定

2-2-1 で明確化した適用範囲において、想定され得るセキュリティインシデント等とその結果(影響)を特定する。2-3 では想定され得るセキュリティインシデントの例を示すが、機器・システム及びそれに関連するステークホルダーに対して重大な影響を及ぼし得るものについては、漏れ等がないよう取り組むことが望ましい。生じ得る具体的なインシデントや影響は、対象となる IoT 機器・システムの種類や利用環境、適用主体の役割等により様々なものが考えられるが、参考までに、IoT 機器・システムの提供又は利用に際して典型的に想定されるセキュリティインシデントやその結果には以下が挙げられる。

＜想定されるセキュリティインシデント(例)＞

- センサ機能の異常(誤計測、計測機能の停止等)
- アクチュエータ機能の異常(誤動作、稼働停止等)
- ネットワーク機器(ルータ、ゲートウェイ等)の異常(誤動作、設定の不正変更、稼働停止等)
- ネットワーク上における通信データの漏えい、改ざん、ネットワーク機能の停止
- 各種サービスを提供するサーバ等にて保管、活用されるデータの漏えい、改ざん、サービスの停止

＜セキュリティインシデント等により生じ得る結果(例)＞

- 事業の停止、劣化(例:機器・システム及び関連する業務の停止、製造物・供給物の品質低下等)
- 自社に対する信頼の低下 (例:顧客情報の漏えいに伴うサービスへの信頼の低下)
- 人的被害 (例:機器・システムの停止や誤動作等による人的損傷、健康被害の発生)
- システム破壊 (例:機器・システムの停止や誤動作等による周辺設備の損傷、環境への悪影響)
- 法令順守抵触事象の発生 (例:各業法、又はデータ保護法等に定められた報告事案等の発生)

(2) 機器・システムの重要度の判断基準及び判断された重要度の一覧

(1)にて特定されたセキュリティインシデント等とその結果を考慮し、想定される被害(リスク)の程度に応じて重要度を割り当てる。

IoT-SSF は、適用主体が「回復困難性の度合い」及び「経済的影響の度合い」を 2 つの軸として設定した上で、フィジカル・サイバー間をつなぐ機器・システムを、(1)にて特定される当該機器・システムに潜むリスク(インシデント及びその結果)に基づいてカテゴライズし、マッピングすると記述している。

以下では、上記の 2 つの軸に基づきリスクの大きさを評価する際の判断基準や留意すべき点等について、IoT-SSF を参照しつつ考え方を示す。

IoT-SSF では、「インシデント発生によって影響を受ける事象ごとに整理を行うことは、フィジカル・サイバー間をつなげる機器・システムのセキュリティ対策を検討する上で、その考え方を逆に複雑なものにしてしまう」とされている。本来守るべきものは IoT を用いて利用者に提供する付加価値であることから本稿では、付加価値ひいては「機器・システム」に着目し、機器・システムに潜むリスクをシンプルな形で整理する。

また、リスクの大きさを評価する際の判断基準は、本来適用主体やその他の関係者における個別の事情等を勘案して作成されるものだが、IoT-SSF にて示された共通の尺度に基づいて複数のユースケースを評価するという本稿の性質上、評価が取扱うユースケース間で相対的なものとなっている点に留意されたい。

なお、同一のインシデントを想定するとしても、それにより受ける影響の内容やその程度は主体や役割により異なり得るが、IoT-SSF を「基本的共通基盤」として活用しようとする際には、対象の機器・システムが提供主体のみならず、利用者やその他の関係者にとって十分に信頼できるものとなるよう取組みを行うべきである。よって、適用主体は自身のみならず、関係し得る各主体(例:適用主体が IoT サービス提供者の場合、IoT 利用者、IoT サービス開発者、その他の関係者)が機器・システムの利用又は提供を通じて被り得るリスクを十分に明確化したうえで、その程度に関する評価(マッピング)を行い、後の対策の検討等に活用することが望ましい。

① 第 1 軸:発生したインシデントの影響の回復困難性の度合い

IoT-SSF では、人命/身体にかかわるセーフティ側面の影響に加え、個人のプライバシー/名誉に関する影響も第 1 軸「回復困難性の度合い」にて考慮すべきとしている。

人命/身体にかかわる影響の観点では、資産が攻撃された場合に、利用者又は関係者の人命が失われるおそれがある場合は「致命的なダメージ」、重症を負うおそれがある場合には「重大なダメージ」、軽傷を負うおそれがある場合は「限定的なダメージ」と判断できる。資産が悪意のある者により攻撃された場合や、機器・システムを製造する事業者が当初想定していなかった方法で機器・システムが利用される場合に、機器・システムの種類や利用環境等によっては利用者又は関係者の人命が失われる可能性も想定される。なお、人命が失われるおそれがある場合であっても、そのような状態に至る条件等が成立する可能性が高くない場合(例:機器の利用状況が製造者側の想定と著しく異なっている)は、「重大なダメージ」と位置付けることも考えられる。

個人のプライバシー/名誉に関する影響の観点では、個人情報等が流出した際に軽度なプライバシーの侵害が認められる場合は「限定的なダメージ」とした上で、重要度の高い個人情報等が漏えいした際に重大なプライバシーの侵害が認められる場合は「重大なダメージ」とする。より具体的に、プライ

241 バシーの侵害等に関連して、想定されるリスクの深刻度を判断するにあたっては、既に公開されている
242 文献[6]を参考にされたい。
243 以下に、上記の議論を踏まえて特定した第 1 軸「回復困難性の度合い」の判断基準を示す。

レベル	判断基準	（参考）IoT-SSFにおける判断基準
致命的なダメージ	• 資産が攻撃された場合、利用者または関係者の人命が失われるおそれがある。	• 人命が失われる
重大なダメージ	• 資産が攻撃された場合、重症を負うおそれがある。 • 資産が攻撃された際の利用状況が適切でない場合(例：想定利用方法と異なる)、人命が失われるおそれがある。 • 重要度が高い個人情報が漏洩する。	• 重症を負う • 重要な個人情報の漏洩
限定的なダメージ	• 資産が攻撃された場合、軽傷を負うおそれがある。 • 個人情報が漏洩する。	• 軽傷を負う • メールアドレスのみの漏洩

244
245 図 3 発生したインシデントの影響の回復困難性の度合いの判断基準

246 ② 第 2 軸：発生したインシデントの経済的影響の度合い
247 IoT-SSF によると、第 2 軸「経済的影響の度合い」はインシデントによる影響の大きさを金銭的価値に
248 換算した場合の大きさ・度合いを基準としたものであるとしている。ここでは、例えば、IoT 機器・システム
249 の停止等により事業者に生じる逸失利益や、個人の生活や社会への影響等（例：サプライチェーンにお
250 ける遅延、ライフラインの停止等）が評価の対象となり得る。
251 金銭的価値に係る評価の尺度は個別の分野や企業の規模によって異なるものである。例えば、企業
252 や事業部門の規模や財務状況等によって、インシデントにより発生する 1,000 万円程度の経済的影響
253 が、「限定的な経済影響」となる場合も、「壊滅的な経済影響」となる場合もあり得る。そのため、具体的
254 な金銭的価値に換算された経済的影響の評価基準は各々の企業や事業部門等において検討されるこ
255 とが望ましい。本稿では、リスクが大きいにも関わらずリスクが過少評価される可能性を低減するため、
256 レベルごとに具体的な金額を示さず、各レベルを判断するための考え方を示している。定量的な金銭的
257 価値へ換算方法については、既存の文献[7]などを参考にされたい。
258 「経済的影響の度合い」を評価する際、「直接的な経済影響」及び「間接的な経済影響」に分けて検討

[6] 特定非営利法人 日本ネットワークセキュリティ協会(JNSA)「情報セキュリティインシデントに関する調査報告書 別紙」（第 1 版）では、漏洩個人情報の価値を EP 図（Economic-Privacy Map）にマッピングしている。
[7] 既存の文献として、特定非営利法人 日本ネットワークセキュリティ協会(JNSA)「インシデント損害額調査レポート 2021 年版」（2021 年 9 月）、一般社団法人 日本サイバーセキュリティ・イノベーション委員会(JCIC)「取締役会で議論するためのサイバーリスクの数値化モデル」（2018 年 9 月）等が挙げられる。

259 を行うことができる[8]。「直接的な経済影響」とは、インシデントによりもたらされる逸失利益、復旧に要し
260 たコスト、営業継続費用、喪失情報資産額、機会損失額等、直接的に生じる被害の金額をいう。また、
261 「間接的な経済影響」とは、製品回収等の間接的に生じる被害の金額をいう。
262 また、「直接的な経済影響」を評価する際には、「内外への直接影響」、「直接影響の継続時間」及び
263 「代替可能性」に分けて評価を行うこととしている[9]。単に影響の規模が大きなものだけでなく、影響が長
264 期間継続するものや、影響のリカバリーが困難なものに対して、「直接的な経済影響」が大きいと評価さ
265 れ得る点に留意する必要がある。
266 「内外への直接影響」では、直接的な影響が及ぶ範囲として当事者内部と、当事者外部（顧客、取引
267 先等）の双方を考慮する必要がある。また、影響範囲が当事者内部に限定される場合においても、その
268 被害影響が当事者にとって重要な位置づけかを考慮する。
269 「直接影響の継続時間」では、経済的影響を及ぼす事象が長時間に渡って継続するかを考慮する。
270 「代替可能性」では、経済的影響を代替的な手段（例：DR サイト[10]への切り替え）により軽減できるか
271 を考慮する。
272 「間接的な経済影響」では、間接被害の規模として、大規模な製品等の回収が想定されるかを考慮す
273 る。
274 これらの基準を踏まえ、本稿における第 2 軸「経済的影響の度合い」の判断基準を以下に示す。

レベル	判断基準	（参考） IoT-SSFにおける 判断基準
壊滅的な 経済影響	• 影響の範囲が内部に限定されず、取引先やその他の関係者に及び、長期間影響が続くことが想定される。 • 影響を受ける機器・システムの機能を他の製品・サービスで補うことができない。 • 大規模な製品等の回収等が生じ得る。	• （破産） • 社会の大混乱
重大な 経済影響	• 影響の範囲が取引先やそれ以外の関係者に及び、長期間影響が及ぶものの、**他の製品等で影響の結果を補うことができる。** • 影響の範囲が取引先やそれ以外の関係者に及び、影響の結果は他の製品・サービスで補えないものの、**影響は短期間で収束する。** • 影響が長時間に及び、影響の結果は他の製品・サービスで補えないものの、**影響の範囲が取引先やそれ以外の関係者に及ばない。**	• 大損害 • 社会の混乱
限定的な 経済影響	• 影響の範囲が取引先やそれ以外の関係者に及ぶものの、**影響は長時間に及ばず、影響の結果は他の製品・サービスで補うことができる。** • 影響の結果は他の製品・サービスで補えないものの、**影響の範囲は取引先やそれ以外の関係者に及ばず、影響は長時間に及ばない。** • 影響が長時間に及ぶものの、**影響の範囲は取引先やそれ以外の関係者に及ばず、影響の結果は他の製品・サービスで補うことができる。**	• 損害、社会の悪影響

275
276 図 4 発生したインシデントの経済的影響の度合いの判断基準

[8] 特定非営利法人 日本ネットワークセキュリティ協会(JNSA)「セキュリティ被害調査 WG の定量化アプローチ」を参考とした。ただし、当該文書の「潜在化被害」はここでは考慮しないものとする。
[9] 直接的な経済影響は内閣サイバーセキュリティセンター(NISC)「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準（初版）」の「サービスの持続可能性への影響」を参考としている。なお、「サービスの持続可能性への影響」はサービス障害の範囲、時間の程度、サービスの代替性の有無から評価するとしている。
[10] DR サイトとは、災害などで主要な IT システム拠点での業務の続行が不可能になった際に、緊急の代替拠点として使用する施設や設備を指す。

(3) マッピング結果の整理と評価の実施

(2)①及び②にて特定された対象機器・システムにおけるリスクの概要(シナリオ)及びその水準(重要度)を、2-2-1 にて確立した自身のリスク基準と比較し、2-2-3 におけるリスク対応の方向性を検討する。

リスク基準との比較の結果、対象の機器・システムが、特定のセキュリティインシデントを通じて受容しがたい水準のリスクをもたらし得ると判断できる場合、適用主体は当該機器・システム等への対処を念頭に置きつつ、適切なリスク対応の手段を選定することが望ましい。その際、対象の機器・システムにおいて想定される相対的に影響の大きなセキュリティインシデントとその実現シナリオを特定[11]し、それが顕在化した場合の影響の度合いを低減することに加え、起こりやすさの低減についても考慮することが適切であると考えられる。ここでは典型的なリスク対応の手段[12]を記載する。

- インシデントの影響の回復困難性の度合い、又は経済的影響の度合いを変えるもの
- インシデントの起こりやすさを変えるもの
- リスクを生じさせる活動を開始、又は継続しないと決定することによってリスクを回避するもの
- 例えば、契約、保険購入等の手段により、リスクを共有するもの
- 情報に基づいた意思決定によって、リスクを保有するもの

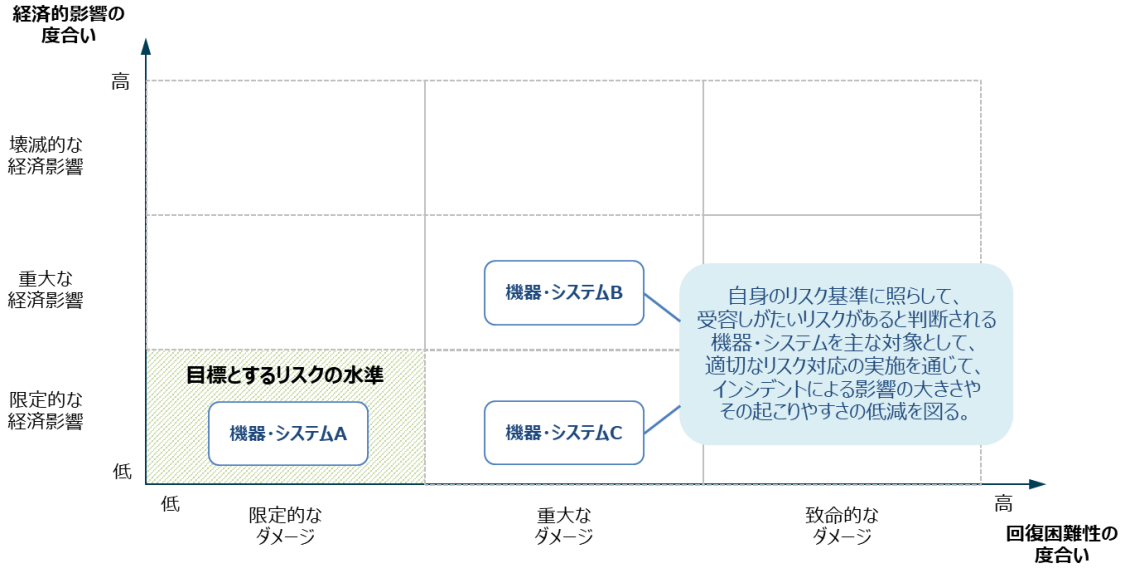


図 5 マッピング結果の整理と評価の実施における考え方

影響が大きいリスクに対処するための対策方針を踏まえた上で行うべきと考えられる対策を適用主体がリスク対応計画等に反映することが有効である。行うべきと考えられる対策の特徴として、例えば以下が挙げられる。

[11] 攻撃シナリオの検討方法等について、本稿では、2-2-3 (1)に示す脅威の整理に留め、詳細なプロセスには言及しない。読者においては、必要に応じて、「制御システムのセキュリティリスク分析ガイド 第2版」の「6. リスク分析の実施(2)～事業被害ベースのリスク分析～」等を参照されたい。

[12] ISO 31000:2018 では、4 つの分類を更に細かく分解し、7 つの選択肢(リスクの回避、リスクの選択、リスク源の除去、起こりやすさの変更、結果の変更、リスクの共有、リスクの保有)を提示している。

・ 生じ得る影響の度合いが相対的に大きいと評価される機器・システムを対象にした対策
・ インシデント等により被り得る影響の度合いが相対的に大きいと評価される主体（例：IoT 利用者）を保護するための対策
・ 効率的に（低コストで）相対的に大きなリスクを低減等することができると見込まれる対策
・ 対象となる機器・システムにおいて法律等により適用が義務とされているもの

2-2-3 リスク対応

リスク対応を行うステークホルダーが、実施すべき対策を整理する。対策を整理するにあたり、以下の手順にて行う。本稿では、システムを構成する機器を網羅的に分析することで対策を強化することが可能な資産ベースのリスク分析手法を参考にしている[13]。

(1) システムを構成する機器ごとの脅威の整理
(2) 脅威への対策の整理
(3) 整理した対策に対する意思決定

(1) システムを構成する機器ごとの脅威の整理

「リスクアセスメント、リスク対応に向けた事前準備」にて整理したシステムを構成する機器に対する脅威を整理する。本稿では、特に、相対的に影響の度合いが大きいと評価された機器・システム及びそこで想定されるセキュリティインシデントに関連した脅威を中心に検討するものとする。

以下に示すように、2-2-2 にて評価されるリスクを引き起こし得る要因は、対象となる機器・システムの故障や性能限界、故意に基づかない人為的ミス、故意による内外からの攻撃等、様々なものが想定され得るが、本稿では情報の機密性、完全性、可用性に影響を及ぼすような「セキュリティ上の脅威」を取扱うこととし、セキュリティ上の脅威とは直接的に関係しない要因（例：機器・システムの欠陥や故障、性能限界）は検討の対象外とする。対象外とした要因への対処等については、機能安全や SOTIF (Safety Of The Intended Functionality)等に関する既存のガイドライン等を参照されたい。

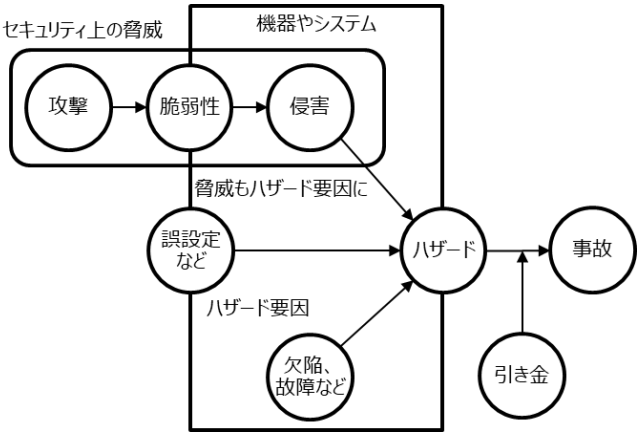


図 6 セキュリティ上の問題がセーフティに影響を与えるモデル[14]

[13] 本稿にて示すリスク対応方法は、資産ベースのリスク分析手法を参考にしているが、シナリオベースのリスク分析手法を制限するものではない。
[14] IoT 推進コンソーシアム、総務省、経済産業省「IoT セキュリティガイドライン ver.1.0」（2016 年 7 月）

321 セキュリティ上の脅威の整理にあたっては、例えば脅威分析手法として広く用いられる STRIDE モデ
322 ル[15]が参考となる。

323 表 2 STRIDE モデルにおける脅威

脅威	内容
なりすまし	コンピュータに対し、他の利用者や機器を装うこと。
データの改ざん・消去	権限なしでデータを改ざん又は削除し、データの完全性を失わせること。
否認	利用者が、あるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと。
情報漏えい	アクセス権限を持たない個人に情報が公開されること。
サービス不能	正規のユーザがサーバやサービス等にアクセスできないこと。 ※DDoS 攻撃やジャミングによるサービス妨害など。
権限の昇格	権限のない利用者がアクセス権限を得ること。

324 上記モデルは IT システムの脅威を抽出する目的で提唱されたものであり、必要に応じて STRIDE モ
325 デル以外の手法[16]を組み合わせた上で、脅威抽出の網羅性を向上させることが望ましい。なお、上記モ
326 デルにて示した脅威に加え、IoT 機器・システムに対する脅威として、例えば以下のような脅威が挙げら
327 れる。

328 表 3 IoT 機器・システムに関する脅威（例）

脅威	内容
不正アクセス	アクセス権限を持たない者にアクセスされること。
マルウェア感染	他の機器への汚染源になる。ランサムウェアなどにより業務妨害を受けること。
踏み台	他の機器へ不正アクセス等を行う際の中継地点として使用されること。
不正改造	不正（違法）なハードウェア、ソフトウェアの改造により、内部データを抜き取り、脆弱性の要因を組み込まれること。
未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性のこと。
不正利用	アクセス権限を持つ者が不正に意図しない用途等でアクセスすること。
利用者によるセキュリティ設定の誤り等	機器が利用者等により十分なセキュリティ設定等がなされずに使われること。

329 これらの脅威は様々な原因によって生じるものであり、実際に対策要件を整理する際には、より具体
330 的に原因を特定することが望ましい。本稿では、上記に示す脅威の洗い出しにとどめているが、より詳
331 細な分析を行う際には既存の文献[17]等を参照して脅威の洗い出しを実施することが望ましい。

[15] STRIDE モデルは Microsoft 社が脅威分析手法として提唱したものであり、脅威分析にあたり国内外で広く参照されている。

[16] 一般社団法人 重要生活機器連携セキュリティ協議会(CCDS)「IoT 機器に対するリスク分析のガイド」の「CCDS-STRIDE モデルによる脅威の分類」や経済産業省 商務情報政策局 サイバーセキュリティ課「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き 別冊 1 脅威分析及びセキュリティ検証の詳細解説書」及び別冊 2「機器メーカに向けた脅威分析及びセキュリティ検証の解説書」を一部参照。

[17] 既存の文献として、独立行政法人 情報処理推進機構(IPA)「制御システムのセキュリティリスク分析ガイド第2版」(2020 年 3 月)及び経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き 別冊 1 脅威分析及びセキュリティ検証の詳細解説書」(2021 年 4 月)等が挙げられる。

(2) 脅威への対策の整理

上記で整理した脅威のうち具体的な対処が必要なものに対して、IoT-SSF における「求められるセキュリティ・セーフティ要求」における 4 つの観点[18]を参照しつつ、リスク対応に有効と考えられる対策を整理する。また、対策の整理にあたっては、4 つの観点のほか、以下の事項を考慮しつつ具体化を図る。

・ 対策の実施主体

一般に IoT 機器・システムの開発、運用等にあたっては、役割の異なる複数の主体が関係することが想定される。その際、適用主体は他の事業者等に対して必要な対策の実施を依頼等することにより、当該主体間で責任分界が不明確になり、結果としてセキュリティ対策の抜け漏れが発生したり、全体の対策水準が十分でなくなったりする事態を防ぐ必要がある。かかる観点から、2-3 における各ユースケースでは、参考として、「リスクアセスメント、リスク対応に向けた事前準備」の「ステークホルダー関連図」にて整理したステークホルダーを参照し、適用主体が実施すべき対策のほか、対象機器・システムの提供又は利用に責任を有する他の事業者又は個人に対応を依頼する対策例を示す。

IoT 利用者(発注側)及び IoT サービス開発者、IoT サービス提供者(受注側)の役割分担を検討するにあたり、以下に参考として、IoT 利用者等が企画・設計の段階からセキュリティ仕様等の策定に積極的に関与し得る場合を想定した、IoT 機器・システムの調達プロセスにおける対策実施の役割分担(例)を示す。

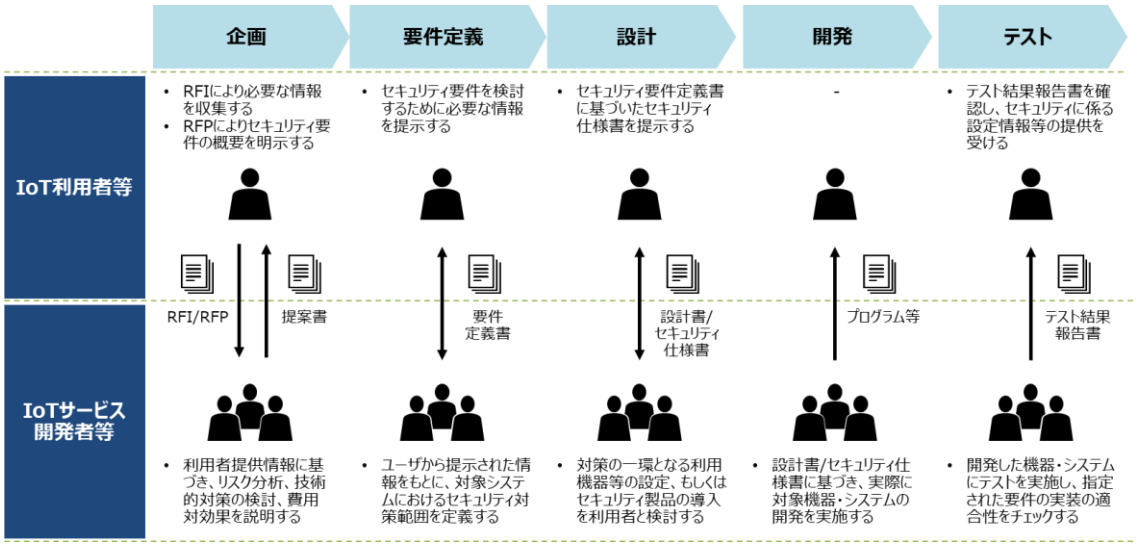


図 7 IoT 機器・システムの調達プロセスにおける対策実施の役割分担(例)[19]

ここで、IoT-SSF の適用主体を IoT 利用者等とすると、自身が将来的に利用する IoT 機器・システム

[18] 第 3 軸「求められるセキュリティ・セーフティ要求」では、第 1 の観点「運用前(設計・製造段階等)におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求」、第 2 の観点「運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求」、第 3 の観点「機器・システムの運用・管理を行う者の能力に関する確認要求」、第 4 の観点「その他、社会的なサポート等の仕組みの要求」という 4 つの観点に分けてセキュリティ・セーフティを確保するための手法を整理している。

[19] 内閣サイバーセキュリティセンター(NISC)「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」、セキュリティ検討プロジェクトチーム「セキュリティ仕様策定プロセス」等を参照し作成。

の企画からテスト、あるいは運用に至るまでのライフサイクルを通じて、設計、開発等の実務を担う IoT サービス開発者等との間で文書を通じたコミュニケーションを行い、最終的な成果物である機器・システムのセキュリティを確保する。また、これらのプロセスにおいては、契約等の適切な合意に基づいて責任が割り振られ、それが適切に実施される必要がある。

IoT 利用者（消費者等）がセキュリティについて十分な知見を有さない場合や、商習慣上このようなプロセスを実施することが困難な場合には、システムインテグレータや IoT 機器製造者等の IoT サービス開発者側が利用者の潜在的なニーズ等を調査してセキュリティ仕様の策定を行う等、上記の例とは異なった対応が必要になる点に留意する必要がある。

・ 対策の実装先

IoT 機器・システムの適切な保護にあたっては、第 3 軸における 4 つの観点の各々に関して、通信の暗号化やユーザ認証の実施等の機器やシステムに対する技術的な対策だけではなく、セキュリティ対応組織の設置や関連するポリシーや手順の策定等のソシキ・ヒトに対する非技術的な対策も含めて検討を行う必要がある。本稿では、参考として、「ソシキ・ヒト」、「プロシージャ」又は「システム」という対策の実装先ごとに想定される要件や対策の例を示す。

・ セーフティ[20]確保に向けた対策の考慮

IoT 機器・システムには、外界に何か物理的な力を与えるアクチュエータが備えられている場合があることを踏まえると、セキュリティ対策とセーフティに関連する対策を両立することも求められる。本稿では機器・システムが IoT 化することによって新たに考慮すべきセーフティの対策も示す。ただし、IoT 化とは必ずしも関連しないと考えられ、従来から必要とされているセーフティに関する対策については、既存の各文献を参照されたい。

本稿においては、国内外で策定された複数の文献を参照し、IoT 機器・システムに関する対策要件を添付 A、実際に講じる対策の例を添付 B に示した。

例えば、第 1 の観点では「運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保」等、第 2 の観点[21]では「IoT 機器・システムの出荷時における安全な設定と構成」等、第 3 の観点では「IoT 機器・システムの運用・管理を行う者に対する要求事項の特定」等、第 4 の観点[22]では「賠償等の対処を実施することが容易ではないケース等における社会的なセーフティネットの構築」等が整理された。ただし、添付 A、添付 B に示す対策要件はあくまで例示にすぎないことに留意されたい。必要に応じて、CPSF「添付C 対策要件に応じたセキュリティ対策例」を参照した上で、対策要件を検討することが望ましい。また、添付 A に示す対策要件のうち、どの主体がどの対策要件を実装するかはユースケース

[20] 本稿では、工場、社会インフラの観点での安全性を「セーフティ」と記載する。

[21] 工場等の製造現場においては工場の稼働停止を防ぐことが重要視されるため、ランサムウェアを始めとするマルウェアへの感染対策に加えて、マルウェアに感染したとしてもそれらの影響を最小限に留めるための対策も重要となる。

[22] 本稿では、第 4 の観点（その他、社会的なサポート等の仕組みの要求）に関する対策を、専ら規制当局や業界団体等による措置に限定して捉えることとする。また、第 4 の観点を踏まえた対策例を含んだ事例は本稿を執筆時点で見受けられなかったため、2-3 以降で示す各ユースケースではこれらを示していない。

に依存することから、本節では記述せず、各ユースケースにおいて記述する。

(3) 整理した対策に対する意思決定

(2)で対策を整理した後で、それらの対策をすべて実装し、想定されるリスクを最小化することが一見理想的なようにも思われるが、IoT-SSF でも触れられているように、対策の実施はコストに直結するものであることから、全ての対策を実装することは現実的ではない。また、運用上重要な要件(例:小型化)を実現しようとする際に一部の対策の実装がそれと矛盾する可能性もある。

各事業者において実際に適用する対策を特定する際には、各ステークホルダーにとって許容可能な範囲までリスクを低減することを前提に、それを可能な限り効率的に(低コストで)かつ、各事業者の負荷を軽減させる形で実装することが目的となる。IoT-SSF でも記載した通り、リスクはインシデントによる影響の度合いと、インシデントの起こりやすさを用いて捉えることとなることから、対策等を検討する際にはインシデントの起こりやすさも踏まえ、システム全体としてのリスクを低減するような対策を検討する必要がある。様々な考え方が適用され得るが、例えば以下のように、リスクがより高いとされる機器や脅威への対策を中心に検討する方法がある。

- 対策の適用対象(どの機器を中心に検討するか)
- 適用する対策の内容(どのように対策を実施するか)

① 対策の適用対象(どの機器を中心に検討するか)

ある機器に係るリスクの大きさを評価しようとする際、例えば、当該機器に影響を及ぼす事象が実際に生じた場合に結果として生じ得る被害の大きさや、当該機器に悪影響を及ぼし得る事象の起こりやすさのそれぞれに着目することができる。

被害の大きさを評価する際、機密性の観点が特に重視される一般的な情報システムとは異なり、IoT 機器・システムではしばしば完全性や可用性が優先される[23]ことから、IoT 機器・システムに関する対策を実装する際には、特に完全性及び可用性の観点で大きなリスク(例:人身事故、設備の損傷、プロセスの停止)が想定される機器への対策を実装することが適切な場合がある。

完全性・可用性の観点で大きなリスクが想定される資産は、物理空間に直接作用する末端の機器及びその制御に関わる機器・システムである場合が多く、一つのシステムに多数の機器が利用される、機器の演算能力が十分でない等の理由で、個々の機器すべてに高いセキュリティ対策を実装することが困難である場合がある。そこで、起こりやすさを低減する観点では、外部からの攻撃への対策は、外部からの脅威にさらされやすい(インターネットに直接接続されている、又は外部ネットワーク、その他のインターフェースからの侵入が比較的容易な領域に位置する)機器に関して対策を実施することで、効率的にリスクを低減させるアプローチも考えられる。その場合、末端の機器における外部からの攻撃への対策が不在になることから、末端の機器においてはフェールセーフの対策を実装することで、被害の大きさを低減させてリスクを小さくとどめることが可能になると考えられる。

[23] IoT 機器・システムにて収集するデータは非常に粒度が細かく、攻撃者にとっても個別の IoT 機器・システムから情報を窃取することはかかる手間に対して割に合わないとされている。特に産業用 IoT 機器では、機密性よりも完全性や可用性が重視される傾向があるとされるが、一方で、消費者用 IoT では、機密性がより重視される場合もある。

② 適用する対策の内容（どのように対策を実施するか）

実施する対策を評価する際、より効率的・効果的にリスクを低減できるものがあれば評価は必然的に高くなる。こうした評価は、例えば当該対策によって見込まれる効果の大きさ（結果として低減されるリスクの大きさ）や、対策に係るコスト等が勘案されるべきである。例えば、同一の機器に対策を行う場合に、コストや労力が同等であればより低減できるリスクの大きいものを採用することが望ましい。

一方で、リスク低減効果の高い対策であっても、対象となる機器の種類によっては、仕様上の制約等の理由で、セキュリティ機能が十分に搭載できない場合がある。こうした機器に対して単体での対策を行うことが現実的、効率的でない場合、よりリソースが十分である「上位の IoT 機器・システム」（例：IoT ゲートウェイ）がシステム単位で対策を担うことも想定される。そのような対策の例としては、以下が挙げられる。

- 末端の IoT 機器等にてマルウェア検出ソフト等の実装が困難な場合、IoT ゲートウェイ等にてマルウェア検査を実施する。
- 末端の IoT 機器等による外部への通信を IoT ゲートウェイ等において監視し、必要に応じて不審なものを検出する。
- 末端の IoT 機器等にて通信の暗号化に対応することが困難な場合、IoT ゲートウェイ等に係る機能を実装することで、インターネットを経由する通信を保護しつつ、エンドポイント機器側の処理を効率化する。

上記に示した対策の一部は、内部ネットワークと外部ネットワークの境界でセキュリティ脅威を阻止する防御機能を果たす境界防御に相当し、一般家庭においてはルータ等、企業においてはファイアウォールや VPN ルータ等によって行われる。これらの対策は第 1 の観点における「適切なネットワークの分離」に該当し、第 2 の観点における「利用者へのリスクの周知等の情報発信」にて、これらの対策の実装を利用者に呼びかけることも有効であると考えられる。

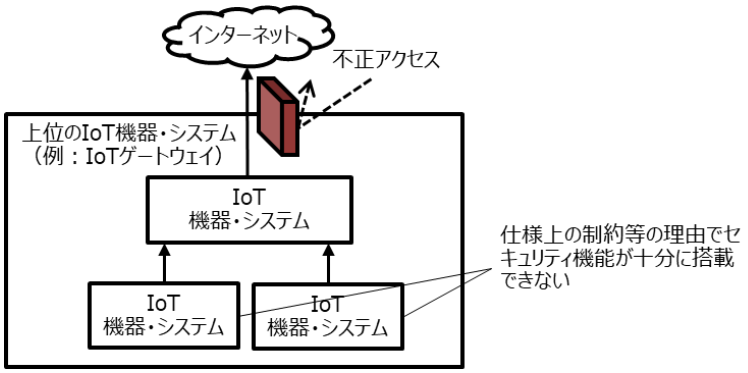


図 8 上位の IoT・機器システムでセキュリティ対策を実装するイメージ[24]

[24] IoT 推進コンソーシアム、総務省、経済産業省「IoT セキュリティガイドライン Ver1.0」（2016 年 7 月）P30 を参照し、修正。

2-3　具体的なユースケース

2-3-1 家庭用ガス給湯器の遠隔操作

「IoT 機器・システムを通じて提供されるサービスの開発者」であるスマートホーム向け IoT 機器・サービスの事業者（ガス給湯器の製造元）が、IoT-SSF の主たる適用主体となってリスクマネジメントを行うユースケースを記載する。

ガス給湯器の製造元はスマートホームを供給する事業者等と協力して新たに遠隔操作を可能とするガス給湯器及びそれに関連するサービスの開発を企画しており、機器のネットワーク接続等に伴い新たに生じ得るサイバーセキュリティに関するリスクを懸念している。

特に、IoT 機器の利用者（消費者等）が、セキュリティについて十分な知見を有さない主体と考えられるため、ガス給湯器の製造元やスマートホームを供給する事業者（ハウスメーカー等）の供給側が中心となって、対象機器・システムに関するリスクアセスメントを行い、残存するリスクに対しては利用者に対応を依頼することで、可能な限り、リスクを低減することを目的とする。

(1)　リスクアセスメント、リスク対応に向けた事前準備

①　対象ソリューションの概要

住まい手が外出先よりスマートフォン用のアプリケーションを通じて、居宅内のガス給湯器[25]を遠隔操作し、自動で浴槽のお湯張り等を実施するケースを想定する。

なお、ガス製品には遠隔操作が禁止されるものも存在するが、本稿では遠隔操作が許容される方式を用いた製品の利用を前提とする。各事業者等において、本稿を参照し、具体的な取組みを進めようとする際には、改めて既存の法律や文献[26]を参照されたい。

- 外出先よりスマートフォンの専用アプリケーションを活用して、自宅のお風呂のお湯張りを行う。
- なお、ガス給湯器は「自然給排気式・開放式」以外の機器を想定している。これは、「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（令和2年7月）にて「自然給排気式・開放式」の遠隔操作が禁止されているため。(※1)

※1経済産業省「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（令和2年7月）では、「自然吸排気式」及び「開放式」以外の機器において「リスク低減策を講じることにより遠隔操作に伴う危険源がないと評価されるもの等の基準に合致し、危険が生ずるおそれがないものは、操作可能」とされている。

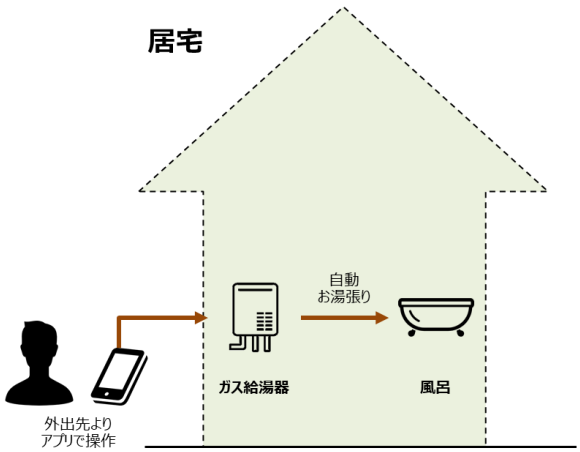


図 9 対象ソリューションの概要

[25] 経済産業省「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（2020 年 7 月）では、「自然吸排気式」及び「開放式」以外のガス給湯器において「リスク低減策を講じることにより遠隔操作に伴う危険源がないと評価されるもの等の基準に合致し、危険が生ずるおそれがないものは、操作可能」とされている。したがって、本稿では「自然吸排気棄式・開放式」以外のガス給湯器を想定する。

[26] 既存の文献として、経済産業省「電気用品、ガス用品等製品の IoT 化等による安全確保の在り方に関するガイドライン」（2021 年 4 月）等が挙げられる。

② ステークホルダー関連図

本稿にて示す取組みに関与するステークホルダーとして、以下に示すように、「スマートホーム向け IoT 機器の事業者」、「スマートホームを供給する事業者」、「住まい手」及び「スマートホーム向けにメンテナンスやサポートを行う事業者」を想定している。

本稿では、既に完成している住宅ではなく、新築の住宅に対して IoT 機器・システムを含む設備一式を納入する事例を想定する。具体的には、「スマートホーム向け IoT 機器の事業者」が製造したガス給湯器は、「スマートホームを供給する事業者」を通じて「住まい手」に納入される。また、「スマートホームを供給する事業者」が提供する専用コントローラは、ガス給湯器以外の IoT 機器・システムにも接続することは想定していない。一般にスマートホームとして戸建住宅もしくは集合住宅が扱われ得るが、本稿では戸建住宅を想定している。

＜IoT サービス開発者/IoT サービス提供者＞

- スマートホーム向け IoT 機器・サービスの事業者

スマートホーム向けの IoT 機器を開発・生産・販売する事業者であり、本稿で想定するガス給湯器の遠隔操作を実現するサービスの提供にあたり、中心となって IoT 機器・システムに関して対策を実装すべき主体である。本稿ではガス給湯器の製造元を想定している。スマートホーム向けにメンテナンスやサポートを行う事業者を本事業者とは分けて記載しているが、しばしば同一の事業者が担い得る。

- スマートホームを供給する事業者

IoT 機器の開発・生産自体は行わないが、IoT 機器や IoT 化された住宅設備を住まい手に対して供給・設置する事業者である。本稿ではハウスメーカーや施工業者等を想定している。

- スマートホーム向けにメンテナンスやサポートを行う事業者

スマートホーム向けのサービスや IoT 機器・システムに関して、メンテナンスはじめ、設置・設定・運用などを行う事業者である。本稿では、遠隔保守サービスなどを提供する事業者等を想定し、脆弱性対応や機能のアップデートに関する更新プログラムの配信等を行う。また、関連法令に基づいて、ガス給湯器を含めた給排気設備などの法定点検調査を行うものとする。

＜IoT 利用者＞

- 住まい手

スマートホームの居住者であり、主として IoT 機器を利用したサービスを受ける。本稿では、戸建住宅に設置されたガス給湯器を遠隔操作する主体となる。

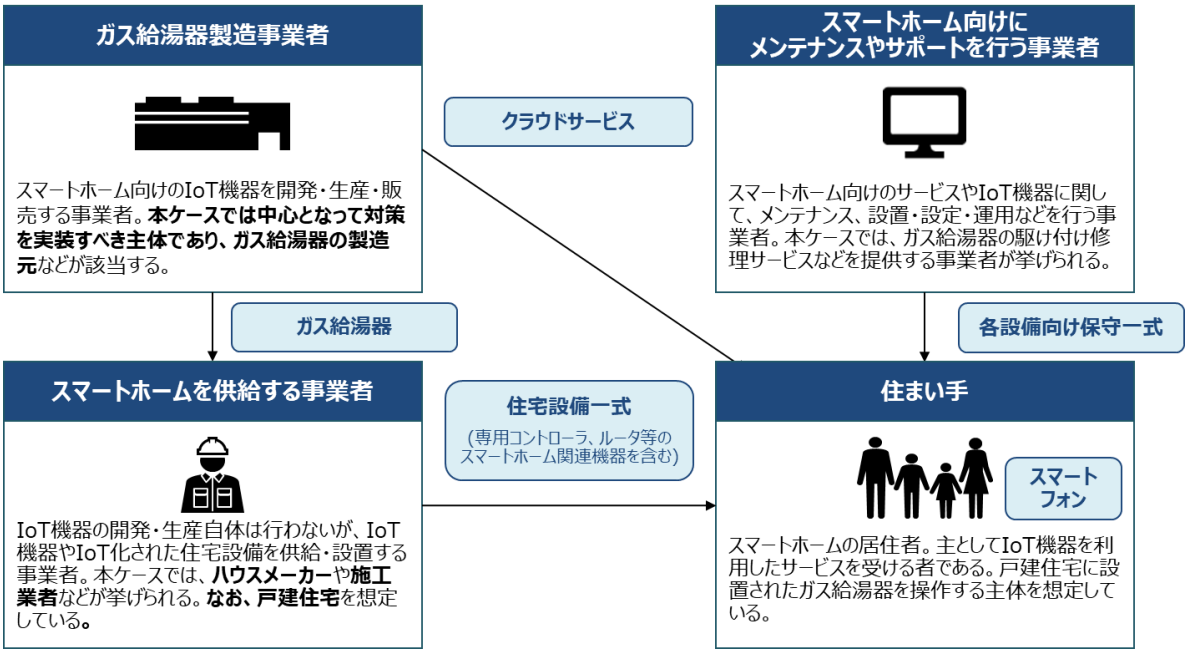


図 10 ステークホルダー関連図

③ システムを構成する機器の一覧

本稿の対象となる機器は以下の通りとする。

表 4 システムを構成する機器の一覧

システムを構成する機器	内容
ガス給湯器	専用コントローラから指示を受けることで、自動湯沸かし等が可能となる機器。 ガス給湯器内に特定の個人に関する情報を保管しないことを想定する。 ガス給湯器は台所等の給湯にも使われ得るが、主な用途を風呂の自動湯沸かしと設定し、居宅外に設置するものとする。 ガス給湯器内の構成要素としては、例えば以下が挙げられる。 ● センサ：水量センサ、水位センサ、CO センサ等 ● アクチュエータ：燃焼ファン、給湯熱交換器等
専用コントローラ	スマートフォンから指示を受け、居宅内のガス給湯器に指示を出す機器。 専用コントローラは、住まい手が簡単に設定変更できる位置に設置するものとする。
ルータ	居宅内に設置され、居宅内のネットワーク及び居外のネットワークを中継する通信機器。 ルータは、居宅内の他の機器にも接続することを目的として住まい手が簡単に設定変更できる位置に設置するものとする。
スマートフォン	専用のアプリケーションをインストールしたスマートフォン。 住まい手は、外出先からスマートフォン上のアプリケーションを操作してガス給湯器の遠隔操作を行う。 スマートフォンは、住まい手が所有するものを使用することとする。
クラウドサービス	スマートフォンから指示を受け、インターネット回線を通じて専用コントローラに指示を出すシステム。 クラウドサービスは、業務効率化を目的として外部の IT サービス事業者が提供するデータセンターから提供するものとする。

④　システム構成図、データフロー図

システム構成図は以下の通りとする。

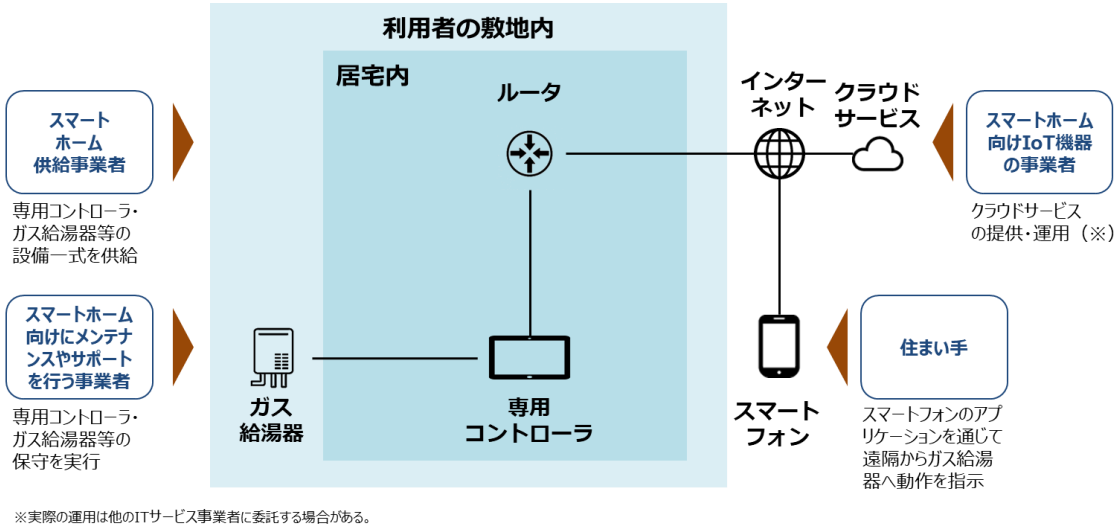


図　11　システム構成図

住まい手が外出先よりスマートフォン専用のアプリケーションを通じて、居宅内のガス給湯器を遠隔操作し、自動お湯張りを実施する場合のデータフローは以下の通りとする。

1. 住まい手が所有するスマートフォンからクラウドサービスに対して、操作指示を出す。
2. クラウドサービスからインターネットを通じて、ルータ経由で専用コントローラに指示を出す。
3. 専用コントローラから居宅内のネットワークを通じてガス給湯器に ON/OFF の指示を出す。

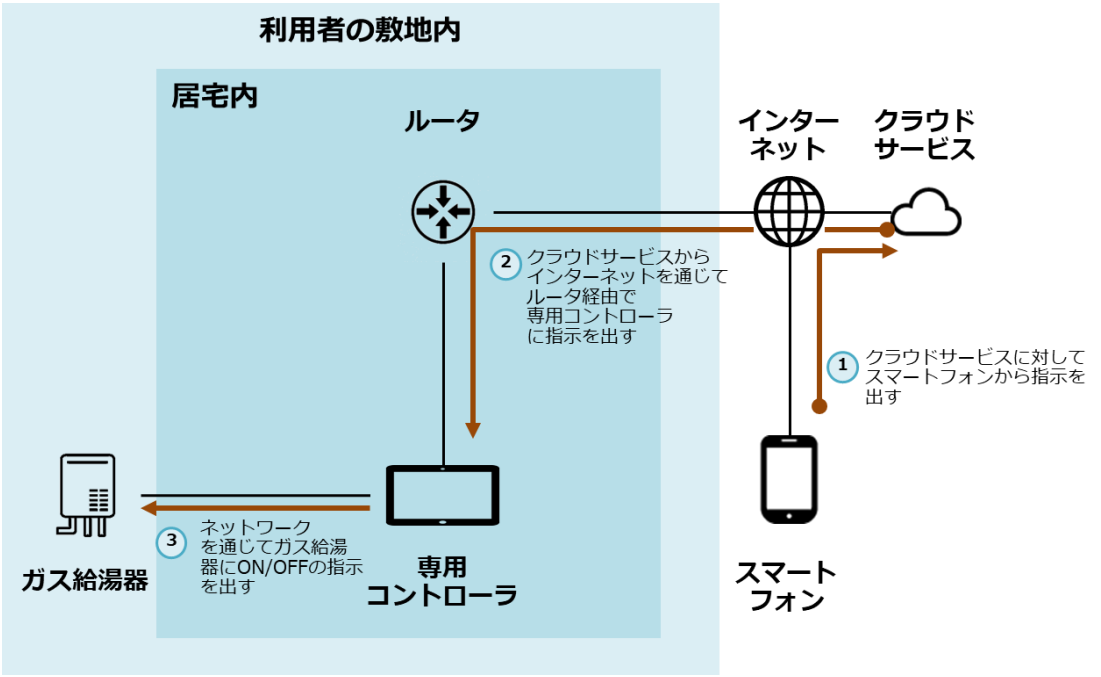


図　12　データフロー図（一部を抜粋）

⑤　リスク基準

「回復困難性の度合い」及び「経済的影響の度合い」に関連付けて整理する。

「回復困難性の度合い」に関しては、自社が定めるセキュリティやセーフティ等に関する基本方針に乗っ取り、住まい手による製品の利用において重大な事故等がないよう、セキュリティ、セーフティの対策を通じて、可能な限り生じ得る被害の度合いを「限定的なダメージ」に抑えることを目指す。

また、「経済的影響の度合い」は、自社の事業規模を考慮し、大規模な製品回収等が生じない、「限定的な経済影響」に抑えることを目指すものとする。

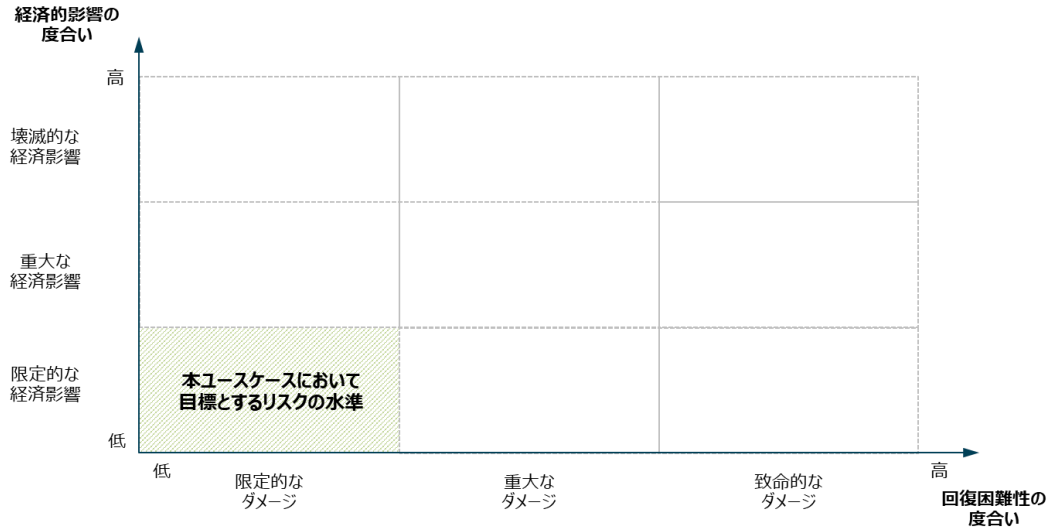


図 13 ガス給湯器システムにて目標とするリスクの水準

(2)　リスクアセスメント

「回復困難性の度合い」及び「経済的影響の度合い」から、ガス給湯器システムのリスクアセスメントを行う。

①　想定されるセキュリティインシデント等とその結果の特定

ガス給湯器システムにおいて、想定され得るセキュリティインシデント等とその結果（影響）を特定する。ガス給湯器システムの提供又は利用に際して想定されるセキュリティインシデント（例）は以下の通り。

- 悪意のある攻撃者がクラウドサービスに対して不正アクセスすることによって、クラウドサーバから利用者の個人情報が流出する。
- クラウドサービスから専用コントローラに送信されるデータが改ざんされ、ガス給湯器が想定されていない動きをする。その結果、住まい手がけがをしたり、住まい手の財産が侵害されたりする。
- 自社環境が不正アクセスされ、配信前のアップデートを改ざんされた上で、スマートホーム向けにメンテナンスやサポートを行う事業者から、専用コントローラに対してネットワークを通じて不正なアップデートの配信やローカル環境で不正なアップデートが実行され、ガス給湯器が想定しない動きをする。その結果、温度の上昇に気付かずに入浴することによって、住まい手がやけど等のけがをする。
- リモートでスマートホーム向けにメンテナンスやサポートを行う事業者により、ガス給湯器内の情報

処理に関わっているコンポートネント（例：ネットワークインターフェース、MCU）が不正に改造される。
その結果、フェールセーフの機能が働かなくなり、住まい手のけがを抑止できない。

② ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーごとに「回復困難性の度合い」「経済的影響の度合い」の観点からリスクアセスメントを行う。

- スマートホーム向け IoT 機器・サービスの事業者
- スマートホームを供給する事業者
- 住まい手
- スマートホーム向けにメンテナンスやサポートを行う事業者

- スマートホーム向け IoT 機器・サービスの事業者（ガス給湯器の製造元）

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点及びセーフティの観点から判断した上で、「回復困難性の度合い」の大きさを評価する。

プライバシーの観点では、クラウドサービスもしくはスマートフォンにインストールされたアプリケーションから住まい手のアカウント情報やサービスの利用状況等が流出する可能性があると想定される。セーフティの観点では、ガス給湯器が予期せぬ動作をしたとしても、スマートホーム向け IoT 機器・サービスの事業者の従業員がけがを負う可能性は低いと想定される。

プライバシーの観点では住まい手の個人情報（アカウント情報やサービスの利用状況等）が流出する可能性があるものの、必ずしも重要な個人情報ではないこと、またセーフティの観点でも影響は限定的と想定されることから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「経済的影響の度合い」は、直接的な経済影響及び間接的な経済影響から評価する。

直接的な経済影響は「内外への直接影響」、「直接影響の継続時間」及び「代替可能性」の観点から評価する。

「内外への直接影響（内部）」の観点では、各家庭に設置されたガス給湯器が停止したとしても、その製造元が運用する製造拠点やその他の活動等の直接的な停止にはつながりにくく、スマートホーム向け IoT 機器・サービスの事業者による経済活動の中断等は生じ難いと想定される。「内外への直接影響（外部）」の観点では、ガス給湯器の停止に加えて、クラウドサービスから送信される指示データ等の改ざんにより、ガス給湯器が誤作動を引き起こすことによって、スマートホーム供給事業者との取引に影響（例：製品・サービスの品質について利用者の間に疑念が広がることによる当該事業者製のガス給湯器の買い控え等）が及び得ると想定される。

「直接影響の継続時間」の観点では、ガス給湯器の故障等の不具合が認められたとしても、大規模なリコールに直結しないと判断される場合、製造等の事業の停止にはつながらないと想定される。

「代替可能性」の観点では、本ユースケースにて想定するインシデントが発生したとしても、事業活動のバックアップが必要になるような経済活動（例：自社工場の停止）等にはつながらないため考慮しない。

間接的な経済影響の観点では、ガス給湯器の修理に対する問い合わせ対応や交換対応に一定のコ

ストを要する可能性があり、また、場合によっては大規模な製品回収が発生する可能性があるものと想定される。

直接的な経済影響では、工場の直接的な停止にはつながらないと判断されたとしても、間接的な経済影響の観点で製品回収が発生する可能性があることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

- スマートホームを供給する事業者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、今回対象としている範囲に限定すれば、従業員の個人情報等が流出する可能性は少ないと想定される。

セーフティの観点では、ガス給湯器が予期せぬ動作をしたとしても、スマートホームを供給する事業者の従業員がけがを負う可能性は低いと想定される。

プライバシーの観点では住まい手の個人情報が流出する可能性が少ないこと、セーフティの観点ではスマートホームを供給する事業者がけがを負う可能性が少ないことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響」の観点では、本来行うべきであった住まい手に対する注意喚起（例：利用方法の説明等）を怠ることにより、ガス給湯器が停止した場合、サービス提供における過失が認められ得る。その結果として、契約上の責任が問われ得る。ただし、ガス給湯器が停止したとしても、「直接影響の継続時間」の観点や「代替可能性」の観点では、スマートホームを供給する事業者には影響が及びにくいと想定される。

同様に、間接的な経済影響の観点では、インシデントによるガス給湯器の大量回収が発生したとしてもスマートホームを供給する事業者が追う責任は限定的であると想定される。

直接的な経済影響及び間接的な経済影響の観点において、「経済的影響の度合い」が大きくなりにくいと想定されることから、「経済的影響の度合い」のレベルは「限定的な経済影響」と評価する。

- 住まい手

A) 発生したインシデントの影響の回復困難性の度合い

自身のプライバシーという観点では、クラウドサービスもしくはスマートフォンにインストールされたアプリケーションから住まい手のアカウント情報やサービスの利用状況等が流出する可能性があると想定される。

セーフティの観点では、セキュリティインシデントに伴って組込まれたセンサやアクチュエータが正常に作動せずガス給湯器が予期せぬ動作をした際に、機器近くにいる利用者がやけど等などの軽傷、あるいはその場の状況によっては重症を負う可能性があると想定される。

プライバシーの観点では住まい手自身の個人情報が流出する可能性があること、セーフティの観点では状況によっては利用者が重症を負う可能性があることから、「回復困難性の度合い」のレベルは「重大なダメージ」と評価する。

B)　発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、ガス給湯器や関連する設備の稼働が停止した場合、住まい手が重症を負う等することによって、自身の生活に支障をきたす可能性があると想定される。

「内外への直接影響（外部）」の観点では、ガス給湯器が停止することによって、利用環境（居宅）外部へ影響は及びにくいものと想定される。

「直接影響の継続時間」の観点では、ガス給湯器の故障等の不具合が認められた場合、修理や交換に一定の時間を要する可能性があると想定される。

「代替可能性」の観点では、停止期間中、給湯が不可能になるものの、外部のサービスを利用することで機能を代替できる場合が一般的であると想定される。ただし、重症を負った場合には外部のサービスを利用することも難しくなる可能性がある。

間接的な経済影響の観点では、適正なガス給湯器の利用を行っている場合には、利用者が被る金銭的な負担等は発生しないと想定される。

間接的な経済影響では大きな影響はないものの、直接的な経済影響では、「直接影響の継続時間」の観点から生活に支障をきたす可能性があり、場合によっては代替的な手段でも代用不可と想定されることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

- スマートホーム向けにメンテナンスやサポートを行う事業者

A)　発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、保守用端末に住まい手のアカウント情報やサービスの利用状況等が保存されていないとすると、これらのデータが流出する可能性は低いと想定される。

セーフティの観点では、ネットワークを通じて専用コントローラへ配信された不正なアップデートプログラムによって、ガス給湯器が予期せぬ動作をした際に、機器近くにいる利用者がやけど等などの軽傷、あるいはその場の状況によっては重症を負う可能性があると想定される。

プライバシーの観点では住まい手の個人情報が流出する可能性は低いものの、セーフティの観点では状況によっては利用者が重症を負う可能性があることから、「回復困難性の度合い」のレベルは「重大なダメージ」と評価する。

B)　発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、配信前のアップデートが改ざんされた上でその不正なアップデートが流されることによって、スマートホーム向けにメンテナンスやサポートを行う事業者による経済活動の中断等は生じる可能性があると想定される。

「内外への直接影響（外部）」の観点では、不正なアップデートプログラムによってアップデートプログラムを適用した多くのガス給湯器の利用者にも影響が及ぶことに加え、サポートの品質について、利用者の間に疑念が広がり得ると想定される。

「直接影響の継続時間」の観点では、ガス給湯器の故障等の不具合が認められる可能性があり、修理や交換に一定の時間を要する可能性があると想定される。

「代替可能性」の観点では、保守用端末に関するサービスの停止を余儀なくされる上に、他のサービスで代替できる可能性は低いと想定される。

間接的な経済影響の観点では、不正なアップデートが流されることによってスマートホーム向けにメン

テナンスやサポートを行う事業者の責任のもとで、大規模な製品回収が生じ得ると想定される。

直接的な経済影響及び間接的な経済影響の観点も含め、「経済的影響の度合い」が大きくなりにくいと想定されることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

③　マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 1 軸「回復困難性の度合い」及び第 2 軸「経済的影響の度合い」からカテゴライズし、マッピングする。

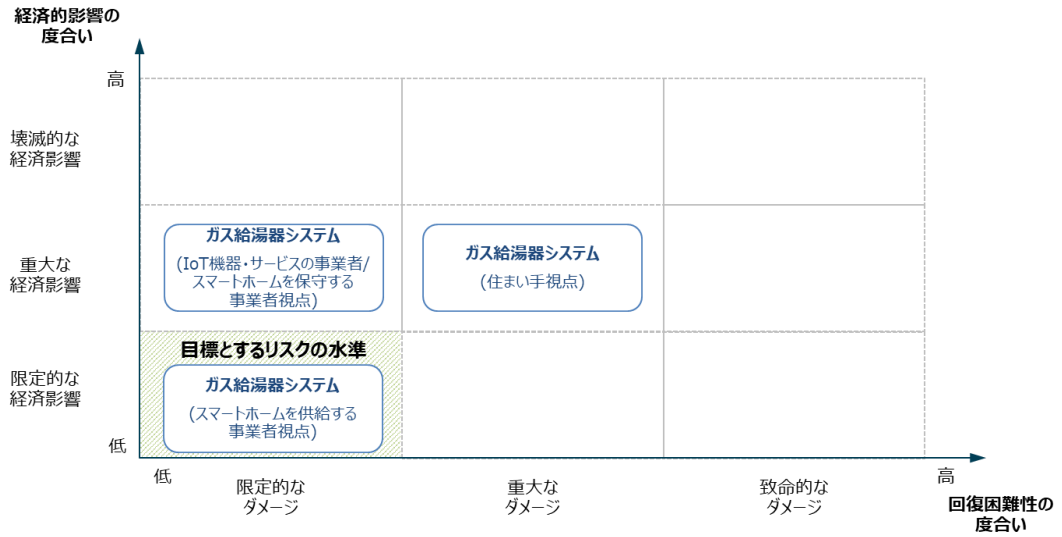


図 14 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

住まい手視点からみたガス給湯器システムの「回復困難性の度合い」及び「経済的影響の度合い」は比較的大きくなると想定される。住まい手がガス給湯器システムのインシデントにより、やけど等の直接的な被害を受ける可能性があること、また、ガス給湯器システムのインシデントが住まい手の生活（例：けがやけど等によって風呂に入れない、毎日の通院を余儀なくされる等）に影響を及ぼしやすいためである。

IoT 機器・サービスの事業者やスマートホーム向けにメンテナンスやサポートを行う事業者視点からみたガス給湯器システムの「回復困難性の度合い」は限定的であるものの、「経済的影響の度合い」は重大になると想定される。ガス給湯器システムの運用段階におけるインシデントが、当該事業者における従業員のけがや個人情報流出等には直結することは想定しがたいものの、製品に何らかの重大な欠陥や不正な機能が発見され、大規模な製品回収等につながった場合に、多額の対応費用が計上され得るためである。

一方で、スマートホームを供給する事業者視点からみたガス給湯器システムの「回復困難性の度合い」及び「経済的影響の度合い」は目標とする水準内に収まると想定される。ガス給湯器システムのインシデントが、スマートホームを供給する事業者が保有するデータの情報流出や従業員のけがにはつながらず、スマートホームへの製造工程や販売工程等の経済活動に影響を与えるとは考えにくいため、「回復困難性の度合い」及び「経済的影響の度合い」にも大きな影響を与えないからであると考えられる。

660 これらを踏まえると、スマートホームを供給する事業者視点からみたガス給湯器システムは、目標と
661 する水準内に収まっているものの、住まい手、IoT 機器・サービスの事業者及びスマートホームを供給す
662 る事業者視点のガス給湯器システムは、目標とする水準には収まっていない。
663 したがって、適用主体である IoT 機器・サービスの事業者（ガス給湯器等の製造元）は、これらのガス
664 給湯器システムがもつリスクを、可能な限り目標とする水準に収めることを目的として、例えば、以下の
665 ように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えら
666 れる対策[27]等の検討を行うことができると考えられる。

667 ● 住まい手にとって影響度が大きいリスクに対処するための対策方針
668 ➢ 自社製品の利用者をけがややけどから守る安全対策の徹底
669 ➢ ガス給湯器システムに対するリスクや安全な使用方法に関する情報提供の実施
670 ➢ IoT 機器・システムの運用・管理を行う者への要求事項の特定
671 ➢ IoT 機器・システムの運用・管理を行う者への要求事項の遵守の確認

672 ● IoT 機器・サービスの事業者にとって影響度が大きいリスクに対処するための対策方針
673 ➢ 大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、
674 セキュリティ・バイ・デザインの取組みの推進

675 ● スマートホーム向けにメンテナンスやサポートを行う事業者にとっての影響度が大きいリスクに対
676 処するための対策方針
677 ➢ ガス給湯器に対する安全なアップデート等の脆弱性対応の実施

678 上記で示した対策方針を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、
679 本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

680 表 5 影響度が大きいリスクに対処するための対策方針及び
681 添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
住まい手	自社製品の利用者をけがややけどから守る安全対策の徹底	IoT 機器・システムの出荷時における安全な初期設定と構成
		セキュリティ設計と両立するセーフティ設計の仕様化
	ガス給湯器システムに対するリスクや安全な使用方法に関する情報提供の実施	利用者へのリスクの周知等の情報発信
		運用手順や利用手順の文書化等の運用・管理を行う者への支援の実施
		IoT 機器・システムの運用・管理を行う者への要求事項の特定
		IoT 機器・システムの運用・管理を行う者への要求事項の遵守の確認
IoT 機器・サービスの事業者	大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守
		企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		セキュリティ設計と両立するセーフティ設計の仕様化
スマートホーム向けにメンテナンスやサポートを行う事業者	ガス給湯器に対する安全なアップデート等の脆弱性対応の実施	プログラムソースコード及び関連書類の保護
		IoT 機器・システムに対するアップデートの適用

682

683 (3) リスク対応

684 ① システムを構成する機器ごとの脅威の整理

685 システムを構成する機器・システムごとに想定される脅威（例）は以下の通り。

686 表 6 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
ガス給湯器	不正利用	悪意のある住まい手により、ガス給湯器が意図しない用途等で利用される。
	不正改造	スマートホーム向けにメンテナンスやサポートを行う事業者により、ガス給湯器内の情報処理に関わっているコンポートネント（例：ネットワークインターフェース、MCU）を不正に改造される。
専用コントローラ	マルウェア感染	外部からの悪意のある攻撃によって、専用コントローラがマルウェアに感染する。
	不正利用	専用コントローラが正規の住まい手によって不正に意図しない用途等で利用される。
ルータ	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、ルータに不正アクセスされる。
	不正利用	ルータが正規の住まい手によって不正な設定等で利用される。
スマートフォン	情報漏えい	スマートフォンのアプリケーションから個人情報等が漏えいする。
	マルウェア感染	外部からの悪意のある攻撃によって、スマートフォンのアプリケーションがマルウェアに感染する。
	利用者によるセキュリティ設定の誤り等	住まい手によるスマートフォンアプリケーションのセキュリティ設定が、スマートホーム向け IoT 機器・サービスの事業者が想定する方法や内容ででなされない。
	データの改ざん	スマートフォンから発信される指示情報等がネットワーク上で改ざんされる。
クラウドサービス	情報漏えい	クラウドサービスに保存された利用者の個人情報が漏えいする。
	サービス不能	クラウドサービスが Wi-Fi ルータやネットワークカメラなどを起点とした大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	クラウドサービスが認可されていない主体により不正にアクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、クラウドサービス内の構成要素がマルウェアに感染する。

687 ② 脅威への対策の整理

688 想定される脅威を踏まえ、第 3 軸「求められるセキュリティ・セーフティ要求」における観点ごとにス

689 マートホーム向け IoT 機器・サービスの事業者にて実装が想定される対策要件を整理する。

690 表 7 スマートホーム向け IoT 機器・サービスの事業者にて実装が想定される対策要件（例）

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般[28]	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の明確化
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守
		全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		不正アクセス	適切な水準のアクセス制御の実施
		データの改ざん	ソフトウェアの完全性の検証
		情報漏えい	ソフトウェアのインストールの制限
		不正アクセス	様々な IoT 機器に接続する際のセキュリティの確保
		データの改ざん 情報漏えい	暗号化によるデータの保護
		データの改ざん 情報漏えい	ライフサイクルに応じた暗号鍵の管理
		マルウェア感染	マルウェア対策の実施
		サービス不能	IoT 機器・システムの十分な可用性の確保
		全般	セキュリティ設計と両立するセーフティ設計の仕様化

[28] 「全般」は特定の脅威でなく、様々な脅威に対して共通に有効な対策であることを示す。

第 3 軸	実装先	想定される脅威（例）	対策要件
		全般	セキュアな開発環境と開発手法の適用
		全般	IoT 機器・システムにおけるセキュリティ機能の検証
		不正アクセス マルウェア感染	IoT 機器・システムの出荷時における安全な初期設定と構成
		全般	IoT 機器・システムにおける運用開始時の正しい設置、設定
第 2 の観点	ソシキ・ヒト	全般	利用者へのリスクの周知等の情報発信
		全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
	プロシージャ	全般	インシデント対応手順の整備と実践
		全般	運用手順や利用手順の文書化と提示
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令及び契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理の実施
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		全般	IoT 機器・システムに対するアップデートの適用
第 3 の観点	ソシキ・ヒト	全般	IoT 機器・システムの運用・管理を行う者への要求事項の特定
		全般	IoT 機器・システムの運用・管理を行う者への要求事項の遵守の確認

③　整理した対策に対する意思決定

対策等を検討する際には、インシデントによる影響の度合いだけでなく、その起こりやすさも踏まえ、システム全体としてのリスクを低減するような対策を検討する。

- 対策の適用対象（どの機器を中心に検討するか）

想定しているインシデントが発生した際に想定される被害の大きさ及び起こりやすさ等を考慮して、資産であるガス給湯器、専用コントローラ、ルータ、スマートフォン・アプリ、クラウドサービス等から、特に対策を検討すべき資産を検討する。

被害の大きさという観点では、本稿で想定する環境に所在する「住まい手」以外のヒトや、居宅内に設置されているガス給湯器システム以外の機器・システムにも影響すると思われる以下の資産を中心として対策を検討すべきである。

- クラウドサービス、スマートフォン・アプリ

  特定の利用者だけでなく、同様のアプリケーションを利用する者全体に対して影響が波及し得る。
- ルータ

  建物内のネットワークに接続するガス給湯器システム以外の機器・システムにも被害を拡大させるおそれがある。一般的に消費者側で対策の必要性を認識していない場合があるため、利用者への周知啓発を行うことも有効であると考えられる。

また、「起こりやすさ」の観点では、外部からのネットワーク経由での攻撃に対して十分に対処する必要があるため、インターネットに直接接続されている資産（例：ルータやクラウドサービス等）を中心として対策を検討することが望ましい。

- 適用する対策の内容（どのように対策を実施するか）

スマートホーム向け IoT 機器・サービスの事業者にて実装が想定される対策要件の例より、より効率

的・効果的にリスクを低減できるものを中心として対策を検討する。具体的には、深刻とされているリスクに対してセキュリティ上、基本的かつ確実に効果が期待できる対策や、一つの対策で複数の脅威に対処できるものを実施することが望ましい。

上記(2)リスクアセスメントでは、各ステークホルダー視点でガス給湯器のリスクを評価した上で、表 5 にて影響度が大きいリスクに対処するための対策方針や行うべきと考えられる対策要件を整理した。また、既存の文書[29]では、例えば、専用コントローラやガス給湯器等の IoT 機器を対象とする初期設定パスワードの変更、脆弱性に関する情報の公開、セキュリティアップデートに関する対策は、特に大きな効果が短期間で得られるとされている。

したがって、上記(2)で示したリスクアセスメントの結果や既存の文書を踏まえ、本ユースケースでは、以下の対策要件を行うべきと考えられる対策に設定した。

なお、ここで行うべきと考えられる対策以外のものであっても、事業者のリスクに対する認識やセキュリティ対策に割けるリソース、IoT 機器の利用環境等によっては積極的に実装を検討すべき項目となる場合がある。したがって、以下に記載されていない対策についても何ら実装を妨げるものではない。

また、ステークホルダー関連図には記載されていないものの、セキュリティインシデントによっては、スマートホーム向け IoT 機器・サービスの事業者はガス供給事業者と連携した対応が求められ得る。

- 運用前(設計・製造段階)における法令及び契約上の要求事項の遵守
- 企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
- セキュリティ設計と両立するセーフティ設計の仕様化
- IoT 機器・システムの出荷時における安全な初期設定と構成
- 利用者へのリスクの周知等の情報発信
- 運用手順や利用手順の文書化等の運用・管理を行う者への支援の実施
- プログラムソースコード及び関連書類の保護
- IoT 機器・システムに対するアップデートの適用
- IoT 機器・システムの運用・管理を行う者への要求事項の特定
- IoT 機器・システムの運用・管理を行う者への要求事項の遵守の確認

上記を踏まえて、ガス給湯器システムがもつリスクが受容可能なリスクの水準に収めることを目的として、IoT 機器・サービスの事業者が実装することとした対策要件の例を以下に示す。

第 1 の観点では、スマートホーム向け IoT 機器の事業者がガス給湯器の遠隔操作に関する新たなサービスの企画段階において、主に当該事業者や住まい手視点のガス給湯器システムのリスクを抑えることを目的として実装することとした対策要件を整理した。

第 2 の観点では、スマートホーム向け IoT 機器の事業者が企画したガス給湯器の遠隔操作に関するサービスの運用中において、主に当該事業者、スマートホーム向けにメンテナンス及びサポートを行う事業者視点のガス給湯器システムのリスクを抑えることを目的として実装することとした対策要件を整理した。

第 3 の観点では、スマートホーム向け IoT 機器の事業者が当該事業者及びスマートホーム向けにメ

[29] 英国デジタル・文化・メディア・スポーツ省 ”Code of Practice for consumer IoT security” (2018 年 10 月)参照

747 ンテナンス及びサポートを行う事業者視点のガス給湯器システムのリスクを抑えることを目的として、ス
748 マートホーム向けにメンテナンス及びサポートを行う事業者に対する要求事項の特定等の対策要件を
749 整理した。
750 第 4 の観点には、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネッ
751 トの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

752 表 8 スマートホーム向け IoT 機器の事業者における実際に講じる対策要件（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● ガス給湯器システムを含む自社が提供する IoT 機器・システムを対象としたセキュリティポリシー（情報セキュリティ関連規定を含む）の策定及び適切な承認権限を有する者の承認 ● 定められた期間ごとの当該ポリシーのレビュー	
2			運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保	● ガス給湯器システムを対象としたセキュリティ管理責任者及びセキュリティ対策担当者の任命 ※ 上記の管理責任者及び開発担当者は、ガス給湯器システムのライフサイクルの各段階（例：開発、運用、保守）において明確化されていることが望ましい。	
3			IoT セキュリティに関するステークホルダーの役割の明確化	● IoT 機器・システムのセキュリティ対策の設計・開発・運用等における関係各社の責任範囲の決定 ● 運用中に発生したセキュリティインシデントにより損害が発生した場合の責任範囲（役割分担や損害賠償）の決定	
4			IoT 機器・システムに係る要員のセキュリティ確保	● 委託する業務に関わる者に対するセキュリティ上の要求事項の規定（退職後も含む） ● 自社内の要員に対する適切な訓練及びセキュリティ教育の実施	
5		システム	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守	● 情報セキュリティに関連する法的、規制（例：製品安全関連法）又は契約上の義務に対する違反を避けるための要求事項の遵守	○ （「大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進」に有効と考えられる対策）
6			企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	● ガス給湯器システムの企画・設計時におけるリスクアセスメントの実施、セキュリティ要件の特定、要件の実装に係る費用の確保 ● 必要なセキュリティ仕様が組み込まれているかを確認する設計レビューの実施	○ （「大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進」に有効と考えられる対策）
7			適切な水準のアクセス制御の実装	● 想定されるリスクの大きさを考慮した方式による、ユーザや IoT 機器の認証 ● クラウド上のアプリケーションへの特権アクセスに対して、多要素認証等の強度の高い認証方式の適用認証済みのユーザ又はアプリケーション等に対する最小権限の原則の適用[30]	

[30] JPCERT/CC によると、最小特権の原則とは場面に応じて必要最小限の権限だけを与えるようにする原則であり、この原則を守ることで、実際にインシデントが発生した場合の被害を最小限に抑えることができるとされている。

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
				● パスワード等の認証情報の安全管理（例：ハッシュ化のうえ保管、通信経路上での保護）	
8			ソフトウェアの完全性の検証	● ガス給湯器システムのソフトウェアに関する完全性の検証機能の実装	
9			ソフトウェアのインストールの制限	● ガス給湯器システムにインストール可能なソフトウェアの種類に関する厳密な方針の策定及び実装	
10			様々な IoT 機器に接続する際のセキュリティの確保	● ガス給湯器等を他の IoT 機器等に接続する際のホワイトリストの適用 ● 識別情報を登録している機器（ガス給湯器等）によるクラウドサービスへの接続に限り許可	
11			暗号化によるデータの保護	● ルータ等による適切な強度の方式による通信経路（住居宅内及び住居外）の暗号化 ● クラウドサービス上に保管されている利用者データ等の暗号化 ※ ガス給湯器等に対して暗号化等のデータ保護措置を十分に講じることが難しい場合、当該機器に機微なデータが保管しない等の代替的な措置をとる。	
12			ライフサイクルを通じた暗号鍵の管理	● 暗号鍵の利用、保護及び有効期間に関するポリシーの策定及び遵守	
13			マルウェア対策の実施	● クラウドサービスにおけるマルウェア対策ソフトウェアの導入 ● ルータにおけるマルウェア対策ソフトウェアの導入	
14			IoT 機器・システムの十分な可用性の確保	● ガス給湯器システムを構成するクラウドサービス等に対する(D)DoS 攻撃を想定し、一定レベルの負荷に耐える容量を確保 ● クラウドサービスにおいて不審な通信（例：特定の IP アドレスからの大量のリクエスト）を検知し、適宜遮断等する ● アプリケーションのテスト段階における一定レベルの負荷試験の実施	
15			セキュリティ設計と両立するセーフティ設計の仕様化	● ガス給湯器の近くにいる人や機器の周辺への危害を回避するための安全機能（本質安全設計、予防安全機能[31]等）の実装 ● ガス給湯器に実装された安全機能と外部との通信回線との分離	○ （「自社製品の利用者をけがややけどから守る安全対策の徹底」及び「大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進」に有効と考えられる対策）
16			セキュアな開発環境と開発手法の適用	● セキュアコーディング手法の適用 ● 委託先を含む開発人員向けのセキュリティ対策、開発環境やコードへのアクセスの制御、開発環境と運用環境の分離等、安全な開発環境に必要な対応の実施 ● 設計書、プログラム、バイナリ等のバックアップ	
17			IoT 機器・システムにおけるセキュリティ機能の検証	● コード分析ツール又は脆弱性スキャナのような自動化ツール等を活用したセキュリティ機能に関する検証の実施	

[31] 「予防安全機能」の概要については、経済産業省「電気用品、ガス用品等製品の IoT 化等による安全確保の在り方に関するガイドライン」の「5. 予防安全機能について」を参照

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
				● クラウドサービス（アプリケーション部分）及びガス給湯器に対するペネトレーションテストの実施	
18			IoT 機器・システムの出荷時における安全な初期設定と構成	● ガス給湯器システムを構成する機器の不要なネットワークポート、その他 USB やシリアルポートなどの物理的又は論理的な閉塞 ● 出荷時点で明らかに不要な IoT 機器・システムが提供する機能、サービス、アプリケーション、アカウントの削除又は無効化 ● ルータ等を含む機器の初期パスワードの変更を促す機能の実装 ● 暗号通信機能（例：TKIP、AES）を有した居宅内無線 LAN への接続を促すガイダンスの提供	○ （「自社製品の利用者をけがややけどから守る安全対策の徹底」に有効と考えられる対策）
19	第 2 の観点	ソシキ・ヒト	利用者へのリスクの周知等の情報発信	● スマートフォン上のアプリケーションや企業ホームページ等を通じたサポート期間終了の予告及び通知、機器・システムの重大な脆弱性、ユーザ情報の漏えいや機器のマルウェア感染等のインシデントに関する情報発信等、ガス給湯器システムに対するリスクやスマートホームを供給する事業者又は住まい手で対応すべき点に関する情報提供の実施	○ （「ガス給湯器システムに対するリスクや安全な使用方法に関する情報提供の実施」に有効と考えられる対策）
20			運用中における IoT セキュリティを目的とした体制の確保	● セキュリティ管理責任者及びセキュリティ対策担当者が異動した場合の後任の選任	
21			過去対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的なインシデント抑制への活用（他社の IoT 機器・システムにおけるセキュリティインシデントを含む）	
22		プロシージャ	インシデント対応手順の整備	● ガス給湯器システムその他の自社が提供する IoT サービスに適応したインシデント対応手順の整備 ● 各要員の役割と責任の識別及び指定された個人によって実行されるアクションの定義・伝達 ● 事業継続上重要な機能を有する外部サービスプロバイダに対する自組織のインシデント対応手順の伝達及び内容調整 ● インシデント対応手順の定期的な訓練（自組織と外部プロバイダとの間で連携を要する部分も含む） ● ※ セキュリティの観点に加え、セーフティの観点を考慮する。	
23			運用手順や利用手順の文書化等の運用・管理を行う者への支援の実施	● 住まい手に対する、以下の内容を含むガス給湯器システムの運用手順や利用手順の作成及び提示 - 初期設定の手順 - 提供者が想定する安全な利用方法 - 不適切な使用によって生じ得るセキュリティ関連のリスク - 不具合を発見した際の連絡先 ● 運用・管理を行う者へのガイドの作成及び提示	○ （「ガス給湯器システムに対するリスクや安全な使用方法に関する情報提供の実施」に有効と考えられる対策）
24		システム	運用中における法令及び契約上の要求事項の遵守	● 情報セキュリティに関連する法的、規制（例：製品安全関連法）又は契約上	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
				の義務に対する違反を避けるための要求事項の遵守	
25			継続的な資産管理の実施	● クラウドサービスに接続するガス給湯器等に関する資産目録（機器上に実装されたソフトウェア及びファームウェア、工場出荷時の設定等を含む）の作成・維持	
26			プログラムソースコード及び関連書類の保護	● 確立した手順に従ってプログラムソースコード管理する ● 施錠可能な文書保管庫での及び関連書類（設計書、仕様書、検証計画書、妥当性確認計画書）の保護の管理	○ （「ガス給湯器に対する安全なアップデート等の脆弱性対応の実施」に有効と考えられる対策）
27			IoT 機器・システムのモニタリング及びログの取得、分析	● ガス給湯器システムを構成するクラウドサービスやスマートフォン上のアプリケーションを対象にした各種ログ（例：ユーザ認証、ネットワークトラフィック）の取得及び保護 ● 取得したログの安全な入手 ● 取得したログの定期的な分析及び異常の検知	
28			IoT 機器・システムに対するアップデートの適用	● 新たに検知されたクラウドサービス、スマートフォン上のアプリケーション及びガス給湯器に係る脅威や脆弱性の報告窓口の設置 ● 報告された脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定 ● 開発委託先等への修正プログラム等開発の依頼 ● スマートホーム向けにメンテナンスやサポートを行う事業者へのセキュリティパッチの提供	○ （「ガス給湯器に対する安全なアップデート等の脆弱性対応の実施」に有効と考えられる対策）
29	第 3 の観点	ソシキ・ヒト	IoT 機器・システムの運用・管理を行う者への要求事項の特定	● 以下の内容を含む、住まい手に能動的な行動を促すためのスマートホーム向けにメンテナンスやサポートを行う事業者への要求事項の明確化 - 使用条件 - 使用上のリスク・注意点 - 使用上のリスク・注意点、異常通知があった場合に取るべき対応（手元操作の優先、近くにいる使用者による通信回線切り離し） - ソフトウェアアップデート時の注意事項	○ （「ガス給湯器システムに対するリスクや安全な使用方法に関する情報提供の実施」に有効と考えられる対策）
30			IoT 機器・システムの運用・管理を行う者に対する要求事項の遵守の確認	● 明確化した住まい手に能動的な行動を促すためのスマートホーム向けにメンテナンスやサポートを行う事業者への要求事項の遵守の確認 ● ソフトウェアアップデート時の注意事項の遵守の確認	○ （「ガス給湯器システムに対するリスクや安全な使用方法に関する情報提供の実施」に有効と考えられる対策）

753 ● スマートホームを供給する事業者に対応を依頼すべき対策要件（例）

754 表 9 スマートホームを供給する事業者に対応を依頼すべき対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	IoT 機器・システムにおける運用開始時の正しい設置、設定	● IoT 機器の事業者から提供されたガイドに従った設置、設定 ● IoT 機器の事業者の想定する仕様に適合したネットワーク環境の整備	

755 • スマートホーム向けにメンテナンスやサポートを行う事業者に対応を依頼すべき対策要件（例）

756 表 10 スマートホーム向けにメンテナンスやサポートを行う事業者に対応を依頼すべき対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 2 の観点	ソシキ・ヒト	IoT 機器・システムの適正な使用	• ガス給湯器システムを対象としたサービス提供や管理のポリシー提示及び遵守 • セキュリティパッチの適用手順の提示	
2		プロシージャ	IoT 機器・システムの適正な運用・保守	• スマートホーム向け IoT 機器の事業者が提示するガイドに従った保守、管理	

757 • 住まい手に対応を依頼すべき対策要件（例）

758 表 11 住まい手に対応を依頼すべき対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	信頼できる IoT 機器やサービスの選定	• 個人情報を含む様々なデータ管理などのポリシーやセキュリティ対策に留意した上で、適切なガス給湯器及びクラウドサービスの選択。	
2	第 2 の観点	プロシージャ	IoT 機器・システムの用途・用法を守った使用	• 仕様書や手順書を把握し、想定された用途・方法でのガス給湯器の使用。	
3		システム	法的及び契約上の要求事項の遵守	• 情報セキュリティに関連する法的、規制（例：製品安全関連法）又は契約上の義務に対する違反を避けるための要求事項の遵守。	

759

2-3-2 ドローンを活用した個人による写真撮影

「IoT 機器・システムを通じて提供されるサービスの開発者」であるドローン製造事業者が IoT-SSF の主たる適用主体となってリスクマネジメントを行うユースケースを記載する。

本事業者は、新たに消費者用ドローンを企画・開発し、家電量販店もしくは EC サイトでの販売を計画しているが、販売するドローンがセキュリティインシデント等によって利用者（消費者等）や周囲環境へ影響を与え得ることを懸念している。

ドローン製造事業者は利用者の周辺環境への影響等を考慮した上で、実際にドローンを製造・販売する前に対象機器・システムに関するリスクアセスメントを行い、適切なリスク対応策を特定することで、可能な限り、リスクを低減することを IoT-SSF 適用の目的とする。

(1) リスクアセスメント、リスク対応に向けた事前準備

① 対象ソリューションの概要

ドローン製造事業者は、利用者がスマートフォンに接続されたコントローラにてドローンを操作し、ドローンに設置されたカメラで風景を撮影することを想定している。なお、公共施設内の土地（屋外）にて許可を得た上でドローンを操作すること、民法や自治体が定める条例に加えて小型無人機等飛行禁止法で禁止されたエリアでは操作しないことについては利用者が責任を持つものと想定している。
また、ドローンの重さが 200g以下であることから、飛行高度が 150m 以上[32]となることがあるものとする。

- ドローン製造事業者は、利用者がスマートフォンに接続されたコントローラにてドローンを操作し、ドローンに設置されたカメラにて風景を撮影することを想定する。
- 利用者は公共施設内の土地（屋外）にて許可を得た上でドローンを操作するものとし、民法や自治体が定める条例に加えて小型無人機等飛行禁止法で禁止されたエリアでは操作しないものとドローン製造事業者は想定している。
- ドローンの重さは、199gを想定。飛行速度は、水平:10 m/s 上昇:3 m/s 下降:3 m/sを想定。

図 15 対象ソリューションの概要

② ステークホルダー関連図

本稿にて関与するステークホルダーは、「ドローン製造事業者」、「利用者」及び「ドローンの飛行箇所の周辺にいる第三者」を想定する。

- ドローン製造事業者

ドローンを製造し、家電量販店や EC サイト等のチャネルにて利用者等へ販売する事業者である。また、本ユースケースにおいて、主にセキュリティ対策を実施する事業者である。

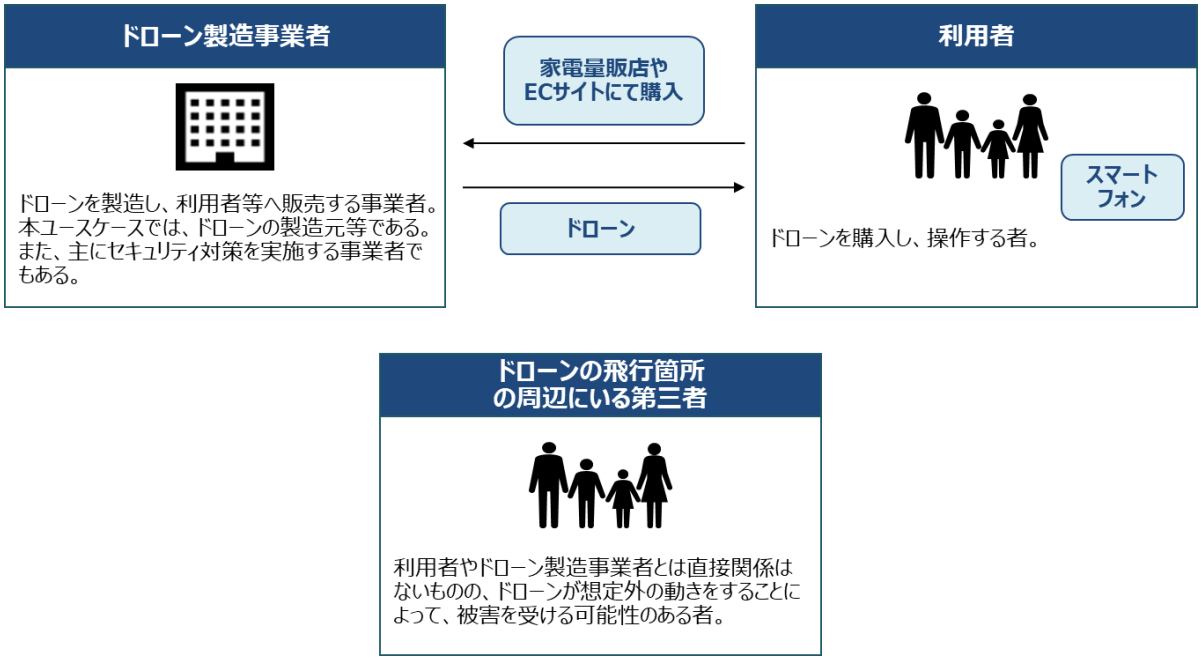
[32] 本稿執筆段階の 2022 年 1 月現在では、200g 未満のドローンは航空法の対象とならないとされている。

783 • 利用者

784 ドローンを購入し、操作する者である。なお、本ユースケースではドローン操作に関する特別な技能を
785 有していないものとする。

786 • ドローンの飛行箇所の周辺にいる第三者

787 利用者やドローン製造事業者とは直接関係はないものの、ドローンが想定外の動きをすることによっ
788 て、被害を受ける可能性のある者。



789

790 図 16 ステークホルダー関連図

791 ③ システムを構成する機器の一覧

792 本稿の対象となる機器は以下の通りである。

793 表 12 システムを構成する機器の一覧

システムを構成する機器	内容
ドローン	カメラが内蔵されたドローン。 画像データは SD カードに保存を行い、利用者自らがスマートフォンへ画像データを転送する。 ドローン製造事業者はドローンの主な用途を個人の風景撮影と設定するものの、他の用途での利用を排除していない。 ドローンの重さは、199g、飛行速度は水平:10 m/s、上昇:3 m/s、下降:3 m/s を想定。 なお、ドローンの構成要素としては、例えば以下が挙げられる。 ● センサ:GPS、ジャイロ(角速度)センサ、加速度センサ、気圧センサ ● アクチュエータ:プロペラ
コントローラ	ドローンの飛行を操縦する機器。 ドローン製造事業者がドローンと併せて販売・製造を行うことを想定。 このコントローラには、製造者側で利用者を認証する仕組みを実装するものとする。
スマートフォン	ドローンが撮影した画像データを転送・確認するためのスマートフォン。 なお、本ユースケースではリスクマネジメントの直接の対象とはしない。
クラウドサービス	スマートフォンから転送された画像データを保存するサービス。 ドローン製造事業者等が提供するサービスではなく、一般に提供されている写真ストレージサービスを想定する。したがって、本ユースケースではリスクマネジメントの直接の対象とはしない。

④ システム構成図、データフロー図

ドローン製造事業者側で想定しているシステム構成図は以下の通りとする。

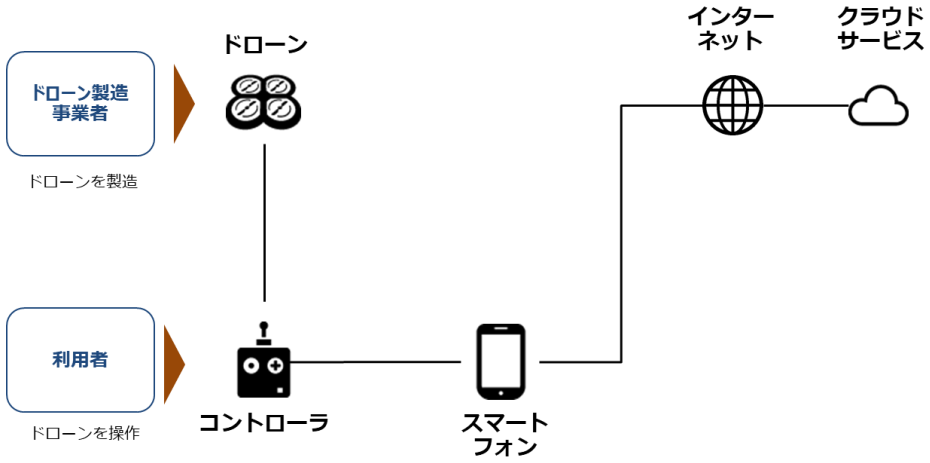


図 17 システム構成図

例えば、公共施設内の土地で許可を取得した上で、利用者がドローンに設置されたカメラにて風景を撮影する場合のデータフローは以下の通りとする。

1. コントローラからドローンに制御データを送信
2. ドローンからコントローラ経由にてスマートフォンに画像データを送信
3. スマートフォンからクラウドサービスに画像データを送信

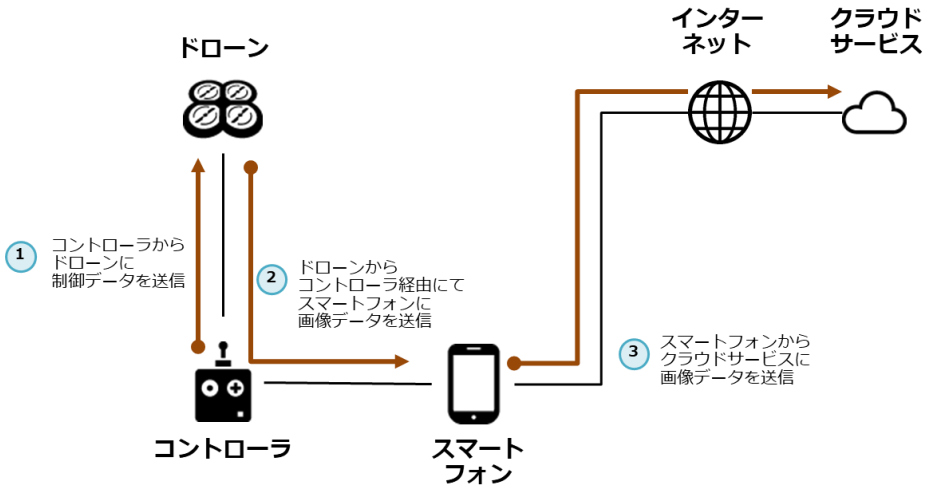


図 18 データフロー図（一部を抜粋）

⑤ リスク基準

「回復困難性の度合い」は、自社が定めるセキュリティやセーフティ等に関する基本方針にのっとり、利用者による製品の利用において重大な事故（例：高高度からのドローンの落下、ドローンの落下に伴う周囲の環境への損害）等がないよう、セキュリティ、セーフティの対策を通じて可能な限り生じ得る被害の度合いを「限定的なダメージ」に抑えることを目指す。

「経済的影響の度合い」は、自社の事業規模を考慮し、大規模な製品回収等が生じないよう、可能な限り「限定的な経済影響」に抑えるものとする。

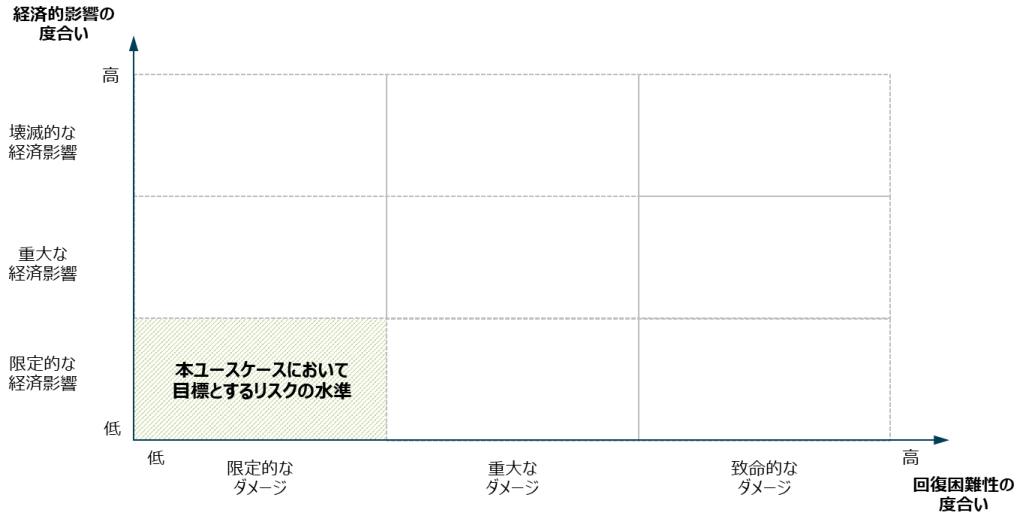


図 19 ドローンにて目標とするリスクの水準

(2) リスクアセスメント

「回復困難性の度合い」及び「経済的影響の度合い」から、ドローンのリスクアセスメントを行う。

① 想定されるセキュリティインシデント等とその結果の特定

ドローンにおいて、想定され得るセキュリティインシデント等とその結果（影響）を特定する。ドローンの提供又は利用に際して想定されるセキュリティインシデント（例）は以下の通り。

- 悪意のある攻撃者により操縦をするための制御権限が奪われ、ドローンが高高度から墜落する。その結果、ドローンが利用者やドローンの飛行箇所の周辺にいる第三者に当たることによって、これらが重症を負う。
- 悪意のある攻撃者によりドローンに内蔵されたカメラが不正アクセスされる。その結果、撮影したデータが外部へ漏えいする。

② ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーごとに「回復困難性の度合い」「経済的影響の度合い」の観点からリスクアセスメントを行う。

- ドローン製造事業者
- 利用者
- ドローンの飛行箇所の周辺にいる第三者

- ドローン製造事業者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、ドローンが撮影した画像データが流出したとしても、ドローン製造事業

者の従業員の情報は含まれておらず、ドローン製造事業者への直接の影響はないと想定される。また、セーフティの観点において、ドローンが攻撃者による機体制御の乗っ取り等により落下した場合においても、ドローン製造事業者への直接の影響はないと想定される。

したがって、プライバシーの観点においてもセーフティの観点においても、ドローン製造事業者の従業員等には直接的な影響はないため、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、機体制御の乗っ取り等の運用時におけるセキュリティインシデントが発生したとしても、その製造元が運用する製造拠点やその他の活動等の直接的な停止等にはつながりにくく、ドローン製造事業者による経済活動の中断等は生じ難いと想定される。一方で「内外への直接影響（外部）」の観点では、運用時におけるセキュリティインシデントが発生することによって、一部の消費者によるドローンの買い控え等が生じると想定される。

「直接影響の継続時間」の観点において、ドローンの故障等が発生した後であっても、同様の製品は比較的流通していると考えられ、大きな影響はないと想定される。

「代替可能性」の観点において、本ユースケースにて想定するインシデントが発生したとしても、事業活動のバックアップが必要になるような経済活動（例：自社工場の停止）等にはつながらないため考慮しない。

ただし、間接的な経済影響の観点において、ドローンに重大な脆弱性が発見された場合、大規模な製品回収につながる可能性があると想定される。

したがって、直接的な経済影響は限定的であると想定されるものの間接的な経済影響は重大であると想定されるため、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

- 利用者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、内蔵されたカメラから利用者本人が映り込んだ画像や利用履歴等が流出することから、個人情報等が漏えいする可能性があると想定される。また、セーフティの観点において、撮影高度がある程度高くなることが想定されることからドローンが落下した場合において、利用者が重症を負う可能性があると想定される。

したがって、プライバシーの観点では個人情報等が流出する可能性があり、セーフティの観点では生じ得る損害が利用者の重症となる可能性があると考えられることから、「回復困難性の度合い」のレベルは「重大なダメージ」と評価する。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では悪意のある攻撃者により操縦をするための制御権限が奪われた場合、ドローンが高高度から落下する可能性がある。その結果、利用者が重症を負うことで生活に支障をきたし得る。また、ドローンによる撮影もできなくなる可能性がある。「内外への直接影響（外部）」の観点においては、ドローンの高高度からの落下により利用者の住居等を傷つける可能性がある。

「直接影響の継続時間」の観点において、ドローンの故障等が発生した場合、製造元に問い合わせた

上で、修理手続き等をとらないといけないため、即座に復旧されることは難しいと想定される。

「代替可能性」の観点において、高高度での撮影を目的としてドローンを購入しているため、同様の製品を新たに購入しない限り、ドローンの代替は難しいと想定される。

間接的な経済影響の観点において、ドローン製造事業者による製品回収が発生したとしても、利用者に対する影響は発生しない。

したがって、直接的な経済影響及び間接的な経済影響を双方踏まえると、利用者への住居や生活に影響を与える可能性があることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

- ドローンの飛行箇所の周辺にいる第三者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、利用者が人通りのあるエリアで撮影を行う可能性があり、内蔵されたカメラから、場合によっては第三者の機微な個人情報等が漏えいする可能性があると想定される。また、セーフティの観点において、撮影高度がある程度高くなることが想定されることからドローンが落下した場合において、第三者が重症を負う可能性があると想定される。

したがって、プライバシーの観点では、場合によっては機微な個人情報等が流出する可能性があり、セーフティの観点では生じ得る損害が利用者の重症となる可能性があると考えられることから、「回復困難性の度合い」のレベルは「重大なダメージ」と評価する。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響」の観点では、攻撃者による機体制御の乗っ取られたドローンによって、第三者が重症を負うことによって、生活に支障をきたす可能性がある。

「直接影響の継続時間」や「代替可能性」の観点において、ドローンの故障等が発生したとしても、第三者に対する大きな影響は発生しない。

間接的な経済影響の観点において、ドローン製造事業者による製品回収が発生したとしても、第三者に対する影響は発生しない。

したがって、直接的な経済影響及び間接的な経済影響を双方踏まえると、第三者が重症を負うことによって生活に影響を及ぼし得ることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

③ マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 1 軸「回復困難性の度合い」及び第 2 軸「経済的影響の度合い」からカテゴライズし、マッピングする。

ドローン製造事業者視点からみたドローンの「回復困難性の度合い」は小さくなるものの、「経済的影響の度合い」は比較的大きくなる。これは、当該事業者における従業員のけがや個人情報流出等には直結しないものの、製品に何らかの重大な欠陥や不正な機能が発見され、大規模な製品回収等につながった場合に、多額の対応費用が計上され得るためである。

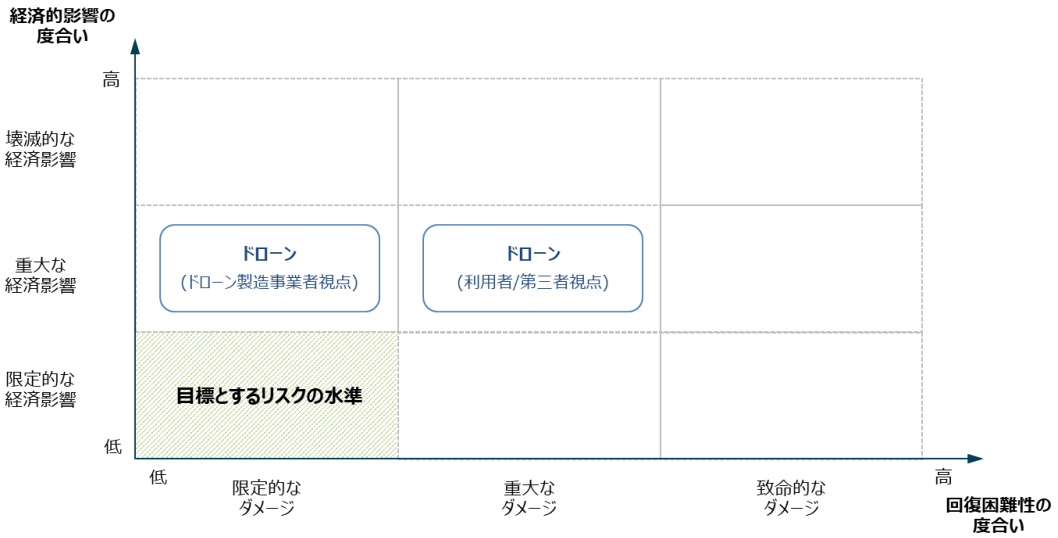


図 20 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

利用者やドローンの飛行箇所の周辺にいる第三者視点からみたドローンの「回復困難性の度合い」及び「経済的影響の度合い」は重大になる。これは、ドローンが「回復困難性の度合い」に与える影響が利用者や第三者を問わず直接危害を加える可能性があることに加えて、その影響が周辺の環境に対して及ぶことが想定され、「経済的影響の度合い」が併せて大きくなるためである。

これらを踏まえると、ドローン製造事業者及び利用者視点のドローンは、目標とするリスクの水準には収まっていない。

したがって、適用主体であるドローン製造事業者は、これらのドローンの利用において想定されるリスクを目標とするリスクの水準に可能な限り収めることを目的として、例えば、以下のように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えられる対策等の検討を行うことができると考えられる。

- ドローン製造事業者にとって影響度が大きいリスクに対処するための対策方針
  - 「経済的影響の度合い」の観点
    ドローン製造事業者にとっては、重大な脆弱性やその他の欠陥が発見されることによって大規模な製品回収が発生することが大きなリスクであり、以下のように、製品の企画、設計の段階からこうしたリスクに対して意識的に取り組むことが有効である。
    - ✧ 大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進

- 利用者にとっての影響度が大きいリスクに対処するための対策方針
  - 「回復困難性の度合い」の観点
    利用者にとっては、自身が映り込んだ画像データが意図せずして流出することや、操作するドローンが落下した際に重症を負うことが主要なリスクである。これらのリスクに対応するため以下の対策が有効であると考えられる。
    - ✧ 利用者への注記喚起の実施

✧ フェールセーフ等を含む安全対策の徹底

➢ 「経済的影響の度合い」の観点

利用者自身がドローンの落下等によりけがを負うことによって普段の生活に支障が生じたり、近隣の家屋や住民に危害が加わることで金銭的な補償等が発生し得たりすることがリスクである。これらのリスクに対応するため以下の対策が有効であると考えられる。

✧ 利用者への注記喚起の実施

✧ フェールセーフ等を含む安全対策の徹底

● ドローンの飛行箇所周辺にいる第三者にとって影響度が大きいリスクに対処するための対策方針

➢ 「回復困難性の度合い」の観点

ドローンの飛行箇所の周辺にいる第三者にとっては、意図せずして自身が映り込んだ画像データが流出することや、ドローンが落下してきた際に自身に直撃することによってけがを負うことがリスクである。これらのリスクに対応するため以下の対策が有効であると考えられる。

✧ 利用者への注記喚起の実施

✧ フェールセーフ等を含む安全対策の徹底

➢ 「経済的影響の度合い」の観点

ドローンの飛行箇所の周辺にいる第三者にとっては、落下したドローンが直撃した結果負うけがで普段の生活に支障が生じることや、落下したドローンが自身の所有する建物等に直撃し、これらが破損することがリスクとして想定される。これらのリスクに対応するため以下の対策が有効であると考えられる。

✧ フェールセーフ等を含む安全対策の徹底

上記で示した対策方針を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

表 13 影響度が大きいリスクに対処するための対策方針及び添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
ドローン製造事業者	大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守
		企画設計段階におけるセキュリティ要求事項の分析及び仕様化
		セキュリティ設計と両立するセーフティ設計の仕様化
利用者	利用者への注意喚起の実施や推奨事項の明確化	利用者へのリスクの周知等の情報発信
		IoT 機器・システムの適正な使用
		IoT 機器・システムの運用・管理を行う者への要求事項の特定
	フェールセーフ等を含む安全対策の徹底	セキュリティ設計と両立するセーフティ設計の仕様化
ドローンの飛行箇所の周辺にいる第三者	利用者への注意喚起の実施や推奨事項の明確化	利用者へのリスクの周知等の情報発信
		運用手順や利用手順の文書化等の運用・管理を行う者への支援の実施

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
		IoT 機器・システムの運用・管理を行う者への要求事項の特定
	フェールセーフ等を含む安全対策の徹底	セキュリティ設計と両立するセーフティ設計の仕様化

954

955 (3) リスク対応

956 ① システムを構成する機器ごとの脅威の整理

957 システムを構成する機器ごとに整理した脅威は以下の通り。

958 表 14 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
ドローン	情報漏えい	ドローンに設置されたカメラ内部に保存された画像データ等が漏えいする。
	サービス不能	ドローンが大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正改造	ドローンに対する不正（違法）なハードウェア、ソフトウェアの改造により、内部データを抜き取り、脆弱性の要因を組み込まれる。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	不正利用	攻撃者によりドローンが乗っ取られ、取扱い説明書に記載された用途以外で利用される。
コントローラ	データの改ざん・消去	コントローラの制御情報等が改ざんされる
	サービス不能	コントローラが大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	コントローラが攻撃者により不正なアクセスを受ける。
	マルウェア感染	コントローラが外部からの攻撃によりマルウェアに感染する。
	踏み台	コントローラが乗っ取られ踏み台になる。
	不正改造	コントローラに対する不正（違法）なハードウェア、ソフトウェアの改造により、内部データを抜き取り、脆弱性の要因を組み込まれる。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。

959

960 ② 脅威への対策の整理

961 想定される脅威を踏まえ、第 3 軸「求められるセキュリティ・セーフティ要求」における観点ごとに有効

962 と考えられるドローン製造事業者にて実装が想定される対策要件を整理する。

963 表 15 ドローン製造事業者にて実装が想定される対策要件（例）

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の決定
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守
		マルウェア感染	マルウェア対策の実施
		サービス不能	IoT 機器・システムの十分な可用性の確保
		データの改ざん 不正アクセス	IoT に適したネットワークの利用
		全般	セキュリティ設計と両立するセーフティ設計の仕様化
		全般	セキュアな開発環境と開発手法の適用
		全般	IoT 機器・システムにおけるセキュリティ機能の検証
		全般	IoT 機器・システムの出荷時における安全な初期設定と構成
第 2 の観点	ソシキ・ヒト	全般	利用者へのリスクの周知等の情報発信
		全般	サービス提供や管理のポリシーの提示・遵守
		全般	過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践

第 3 軸	実装先	想定される脅威（例）	対策要件
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令及び契約上の要求事項の遵守
		全般	プログラムソースコード及び関連書類の保護
		全般	IoT 機器・システムに対するアップデートの適用
		全般	IoT 機器・システムの安全な廃棄又は再利用
第 3 の観点	ソシキ・ヒト	全般	IoT 機器・システムの運用・管理を行う者への要求事項の特定
		全般	IoT 機器・システムの運用・管理を行う者への要求事項の遵守の確認

③　整理した対策に対する意思決定

対策等を検討する際には、インシデントによる影響の度合いだけでなく、その起こりやすさも踏まえ、システム全体としてのリスクを低減するような対策を検討する。

- 対策の適用対象（どの機器を中心に検討するか）

想定しているインシデントが発生した際に想定される被害の大きさ及び起こりやすさ等を考慮して、システムを構成する機器であるドローン、コントローラから、特に対策を検討すべき機器を検討すべきであるが、ドローン及びコントローラは常に通信を行いながら作動する。したがって、これらのどちらかの機器を優先すればよいということではなく、これらの機器一体で対策を行うことが望ましい。なお、前述の通り、スマートフォン、クラウドサービスは本ユースケースで想定するステークホルダー以外の事業者が提供する機器・サービスであることから、リスク対応の対象外とする。

- 適用する対策の内容（どのように対策を実施するか）

本ユースケースの特徴は、2−3−1 と同様にドローンの利用者が IT に関する知見を有していない可能性があることに加え、公共空間でドローンが飛行することによって、ドローンが第三者に対して被害を及ぼす可能性があるということである。

ドローン製造事業者は、利用者や飛行箇所の周囲にいる第三者がけが等をしないよう利用者に対して、ガイドにてセキュリティに関する設定方法及び利用方法等について十分な説明や注意喚起を行うことが望ましい。

したがって、本ユースケースでは、以下の対策要件を行うべきと考えられる対策に設定した。

- 運用前（設計・製造段階）における法令及び契約上の要求事項の遵守
- 企画設計段階におけるセキュリティ要求事項の分析及び仕様化
- セキュリティ設計と両立するセーフティ設計の仕様化
- 利用者へのリスクの周知等の情報発信
- IoT 機器・システムの適正な使用
- IoT 機器・システムの運用・管理を行う者への要求事項の特定

上記を踏まえて、ドローンがもつリスクを目標とする水準に収めることを目的として、IoT 機器・サービスの事業者が実装することとした対策要件の例を以下に示す。

第 1 の観点では、ドローン製造事業者が、ドローンに関する新たなサービスの企画段階において、ドローン製造事業者、利用者や飛行箇所の周囲にいる第三者視点のドローンのリスクを抑えることを目的として実装することとした対策要件を整理した。

993 第 2 の観点では、ドローンの販売後において、ドローン製造事業者、利用者や飛行箇所の周囲にい
994 る第三者視点のドローンのリスクを抑えることを目的として実装することとした対策要件を整理した。
995 第 3 の観点では、ドローン製造事業者が利用者や飛行箇所の周囲にいる第三者視点のドローンのリ
996 スクを抑えることを目的として、利用者に対する要求事項の特定等の対策要件を整理した。
997 第 4 の観点は、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネット
998 の構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

999 表 16 ドローン製造事業者における実際に講じる対策要件（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● ドローン及び周辺機器を対象としたセキュリティポリシー（情報セキュリティ関連規定を含む）の策定及び適切な承認権限を有する者の承認。 ● 定められた期間ごとの当該ポリシーのレビュー。	
2			運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保	● 設計部門又は製造部門におけるセキュリティ管理責任者及びセキュリティ担当者の任命。 ● 情報セキュリティ部門において自社製品のセキュリティを担当する要員の明確化。 ※ 上記の管理責任者及び開発担当者は、ドローンのライフサイクルの各段階（例：開発、運用）において明確化されていることが望ましい。	
3			IoT セキュリティに関するステークホルダーの役割の決定	● ドローン及び周辺機器の運用段階等における利用者との責任分界の決定。	
4			IoT 機器・システムに係る要員のセキュリティ確保	● 設計部門又は製造部門の人員に対して製品のセキュリティ確保に関する適切な訓練及びセキュリティ教育を実施。	
5		システム	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守	● 情報セキュリティに関連する法的、規制（例：製品安全関連法）に対する違反を避けるための要求事項の遵守。	○ （「大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進」に有効と考えられる対策）
6			企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	● ドローン及び周辺機器を現に開発、運用する以前の企画・設計の段階における、想定されるリスクやその程度、具備すべきセキュリティ要求事項の特定。	○ （「大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進」に有効と考えられる対策）
7			IoT 機器・システムの十分な可用性の確保	● ネットワークが停止しても、ドローンが動作を継続してローカルで動作し続ける仕組みの構築。	
8			セキュリティ設計と両立するセーフティ設計の仕様化	● 利用者やドローンの飛行箇所周辺にいる第三者への危害を回避するための安全機能（本質安全設計、予防安全機能等）の実装。	○ （「大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進」及び「フェールセーフ等を含む安全対策の徹底」に有効と考えられる対策）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
9			セキュアな開発環境と開発手法の適用	● セキュアコーディング手法の適用。 ● 委託先を含む開発人員向けのセキュリティ対策、開発環境やコードへのアクセスの制御、開発環境と運用環境の分離等、安全な開発環境に必要な対応の実施。 ● 設計書、プログラム、バイナリ等のバックアップ。	
10			IoT 機器・システムにおけるセキュリティ機能の検証	● ドローン及び周辺機器に対するペネトレーションテストの実施。	
11			IoT 機器・システムの出荷時における安全な初期設定と構成	● 機体の初期パスワードの変更を促す機能の実装。	
12	第 2 の観点	ソシキ・ヒト	利用者へのリスクの周知等の情報発信	● 企業ホームページ等を通じたサポート期間終了の予告及び通知、機器・システムの重大な脆弱性、ユーザ情報の漏えいや機器のマルウェア感染等のインシデントに関する情報発信等、ドローンに対するリスクや利用者で対応すべき点に関する情報提供の実施。	○ （「利用者への注意喚起の実施や推奨事項の明確化」に有効と考えられる対策）
13			運用中における IoT セキュリティを目的とした体制の確保	● 保守部門におけるセキュリティ管理責任者及びセキュリティ担当者の任命。 ● 情報セキュリティ部門において自社製品のセキュリティを担当する要員の明確化。	
14			過去の対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的なインシデント抑制への活用。（他社の IoT 機器・システムにおけるセキュリティインシデントを含む）	
15		プロシージャ	脆弱性対応に必要な手順等の整備と実践	● 脆弱性に関する問題を報告するための連絡窓口の設置。 ● 入手した脆弱性情報に対する対処手順の策定。	
16			IoT 機器・システムの適正な使用	● 利用者に対する、以下の内容を含むドローンの取扱い説明書（利用手順や操作方法）の作成及び提示。 - 初期設定の手順 - 提供者が想定する安全な利用方法 - 不適切な使用によって生じ得るセキュリティ関連のリスク - 不具合を発見した際の連絡先 - ドローンの安全な廃棄方法	○ （「利用者への注意喚起の実施や推奨事項の明確化」に有効と考えられる対策）
17		システム	運用中における法令及び契約上の要求事項の遵守	● 情報セキュリティに関連する法的、規制（例：製品安全関連法）又は契約上の義務に対する違反を避けるための要求事項の遵守。	
18			プログラムソースコード及び関連書類の保護	● 最小限の人員によるプログラムソースコード及び関連書類（例えば、設計書、仕様書、検証計画書、妥当性確認計画書）へのアクセスの限定。 ● アクセスログのレビューの定期的な実施。	
19			IoT 機器・システムに対するアップデートの適用	● 報告された脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定。 ● 開発部門等への修正プログラム等開発の依頼。 ● ホームページを通じたセキュリティパッチの提供。	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
20	第 3 の観点	ソシキ・ヒト	IoT 機器・システムの運用・管理を行う者への要求事項の特定	● 以下の内容を含む、取扱い説明書での利用者に能動的な行動を促すための推奨事項の明確化。 - 使用条件 - 使用上のリスク・注意点 - 異常通知があった場合に取るべき対応（手元操作の優先、近くにいる使用者による通信回線切り離し） - ソフトウェアアップデート時の注意事項。	○ （「利用者への注意喚起の実施や推奨事項の明確化」に有効と考えられる対策）

1000 ● 利用者に対応を依頼すべき対策要件（例）

1001 ドローン製造事業者が全ての対策を行うことは現実的に難しいため、安全なドローンの稼働を目的と
1002 して、利用者に対して主に以下の対策要件を実装するよう依頼する。

1003 表 17 利用者に対応を依頼すべき対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	IoT 機器・システムの出荷時における安全な初期設定と構成	● 機体の初期パスワードの変更。	
2	第 2 の観点	プロシージャ	IoT 機器・システムの適正な運用・保守	● 利用者に対して提示した取扱い説明書に従った管理。	
3		システム	IoT 機器・システムに対するアップデートの適用	● 適切な方法でのホームページを通じて提供されたセキュリティパッチの適用。	
4			IoT 機器・システムの安全な廃棄又は再利用	● ドローンを廃棄するに当たって、ドローン内部やカメラに保存されている情報の削除。	

1004

2-3-3 物流倉庫内の AGV による自動ピッキング

本項では、「IoT 機器・システムを通じて提供されるサービスの開発者」である物流事業者が IoT-SSF の主たる適用主体となってリスクマネジメントを行うユースケースを記載する。

物流事業者は、事業規模拡大に伴って既存の物流倉庫において、省人化や効率化を目的として AGV や倉庫制御システム等の導入を予定しており、新たなシステムや機器の導入によって生じ得るサイバーセキュリティに関するリスクを懸念している。なお、既に在庫管理等を支援する倉庫管理システムは導入済である。

本ユースケースでは、IoT 機器の利用者（物流事業者）が対象機器・システムの稼働前にリスクアセスメント及びリスク対応を行い、それでもなお残存するリスクに対しては運用時にも脆弱性対応等を依頼することで、可能な限りリスクを低減させることを目的とする。

(1) リスクアセスメント、リスク対応に向けた事前準備

① 対象ソリューションの概要

ある物流事業者が運用する工業用間接資材を扱う物流倉庫において、庫内の資材搬送業務の効率化のため、無人搬送車（以下、「AGV」という。）が自動ピッキングを行うケースを想定する。

具体的には、物流倉庫（入荷エリア、保管エリア、ピッキングエリア、梱包エリア、出荷エリア）内の保管エリアにて倉庫制御システムによって制御された AGV が保管棚をピッキングエリアにいる作業員のもと（ピッキングステーション）まで移動させる。作業員は保管棚から対象となる製品をピッキングする作業を行う。

なお、作業員が作業行うピッキングエリアと AGV の稼働する保管エリアは保護柵等で区切られており、かつ、AGV が低速で進むことを前提としている。

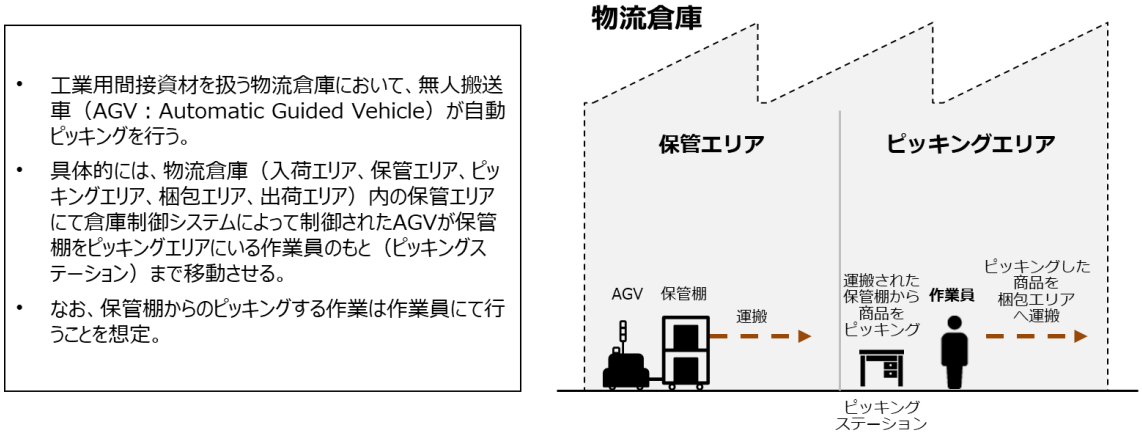


図 21 対象ソリューションの概要

② ステークホルダー関連図

本稿にて関与するステークホルダーは、「物流事業者（委託元企業）」「システムインテグレータ（システム開発の委託先企業）」、「AGV 製造事業者」を想定している。

- 物流事業者（委託元企業）

物流倉庫を運用する事業者であり、本サービスにおいて、中心となって IoT 機器・システムに関して対

策要件を実装する主体である。本事業者の主な顧客となる製造事業者等は工場並びに生産設備システムを所有しており、物流機能の一部を本事業者に委託していると想定する。なお、当該物流倉庫の稼働は 24 時間、年中無休を想定している。

- システムインテグレータ（システム開発の委託先企業）

物流事業者からの委託を受け、AGV を組み込んだ倉庫管理システム及び倉庫制御システムを開発する事業者。物流事業者が定めた仕様に従ってシステム全体の設計、供給、製造などを行い、倉庫管理システム及び倉庫制御システムを物流事業者に納入する。なお、物流事業者とは保守契約を結ぶことを想定しており、倉庫管理システム及び倉庫制御システムのアップデートを配信する。また、AGV の調達及び保守については、システム開発及び保守の一環として物流事業者から受注しており、AGV 製造事業者と契約して実施することを想定している。

- AGV 製造事業者

AGV を製造し、関連する保守サービスを含めてシステムインテグレータに提供する事業者を想定している。AGV のアップデートをシステムインテグレータ経由にて配信することを想定している。

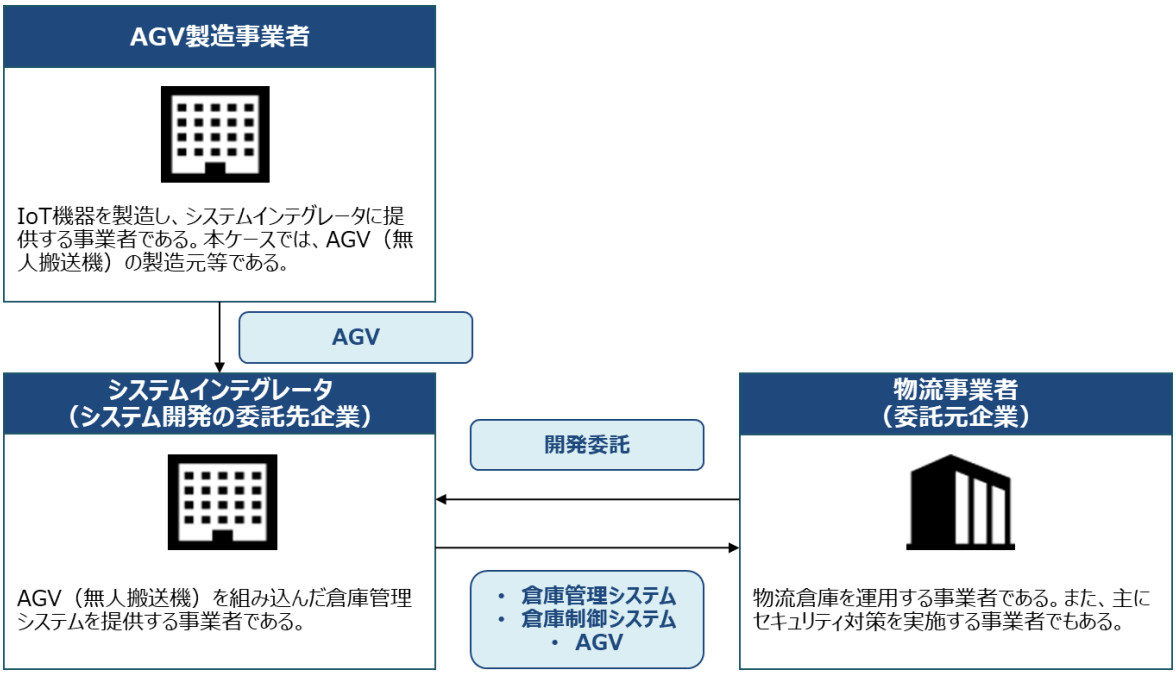


図 22 ステークホルダー関連図

③ システムを構成する機器の一覧

本稿の対象となる機器は以下の通りとする。

なお、以下の機器を包括したシステムを物流倉庫システムと表現するものとする。

表 18 システムを構成する機器の一覧

システムを構成する機器	内容
倉庫管理システム （WMS：Warehouse Management System）	在庫管理、在庫引き当て、出荷指示等を行うシステム。 倉庫管理システムは、オンプレミスにて物流倉庫内にサーバを設置するものとする。 なお、倉庫管理システムは、例えば以下の機能を有するものとする。

システムを構成する機器	内容
	● 入庫管理機能 ● 出庫管理機能 ● 在庫管理機能 ● 棚卸管理機能
操作用端末	倉庫管理システムや倉庫制御システムを操作する端末。 操作用端末はスタンドアロンにて物流倉庫内に設置するものとする。
保守用端末	倉庫管理システムや制御システムの保守を行う端末。 保守用端末はスタンドアロンにて物流倉庫内に設置するものとする。
倉庫制御システム (WCS:Warehouse Control System)	AGV を対象として、工程別指示や制御指示等を行うシステム。 倉庫制御システムは、オンプレミスにて物流倉庫内にサーバを設置するものとする。 なお、倉庫制御システムは、例えば以下の機能を有するものとする。 ● AGV 等の設備の管理機能 ● AGV 等の設備の制御機能
安全制御 PLC (PLC:Programmable Logic Controller)	停電等の有事の際に、作業員による安全確保の処理がなされるまでは勝手に稼働しないような「安全な仕組み」を提供する PLC。 安全制御 PLC は、倉庫内に設置するものとする。
AGV	自動で保管棚を搬送する IoT 機器。 AGV は、倉庫内の保管エリアのみで稼働するものし、倉庫内で常時稼働するものとする。 最大積載量 500 kg、前進移動速度 60m/分(500kg 負荷時)を想定。 日本工業規格 JIS　D 6802「無人搬送車システム−安全通則」に準拠していることを想定。

④　システム構成図、データフロー図

システム構成図は以下の通りとする。

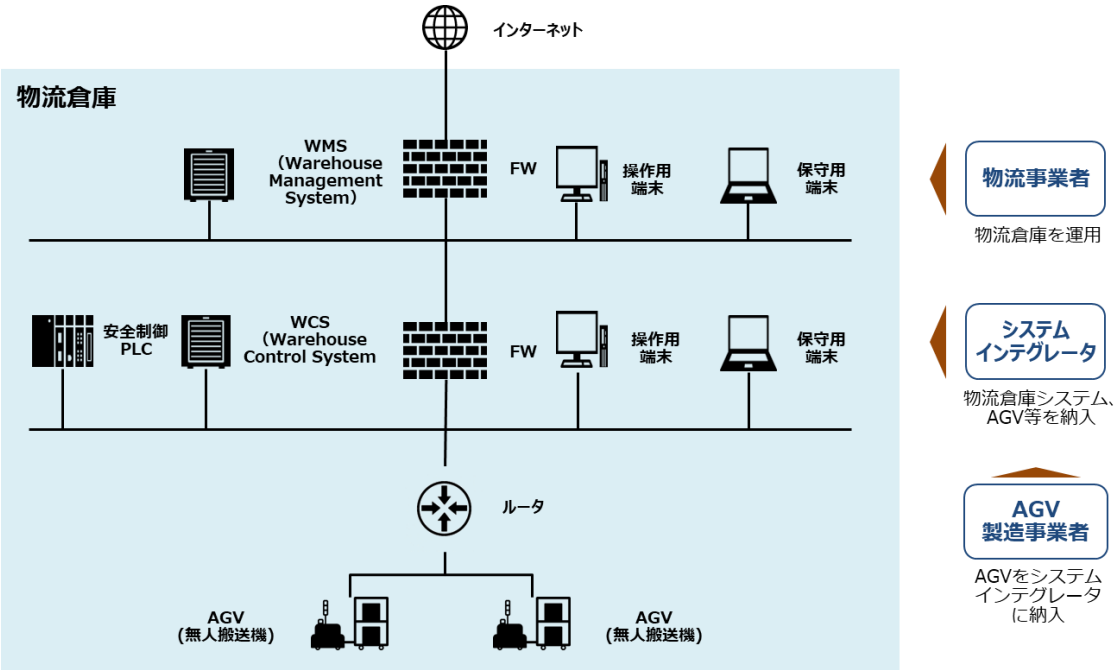


図 23 システム構成図

物流事業者の倉庫管理システムが工場外部の受発注システムから売上データを受領して、対象の商品をピッキングする場合のデータフローは以下の通りとする。

1. 外部の受発注システムから倉庫管理システム(WMS)が売上データを受領
2. 倉庫管理システム(WMS)から倉庫制御システム(WCS)に出荷指示を送信
3. 倉庫制御システム(WCS)から AGV に搬送指示を送信

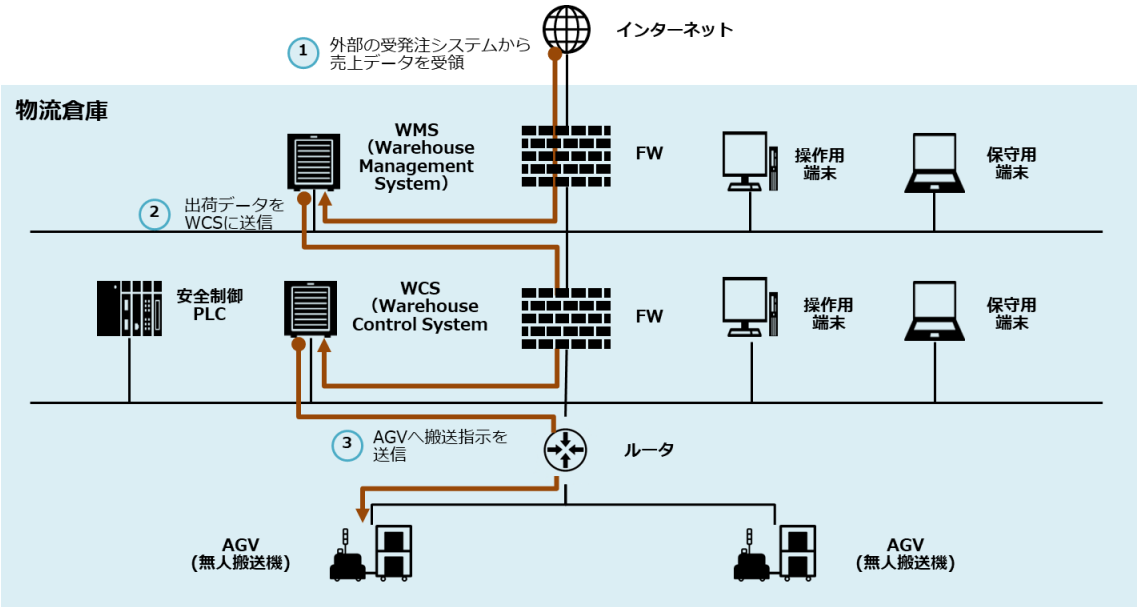


図 24 データフロー図（一部を抜粋）

⑤ リスク基準

「回復困難性の度合い」は、自社が定めるセキュリティやセーフティ等に関する基本方針にのっとり、物流倉庫内の作業員に重大な事故等が発生しないよう、セキュリティ、セーフティの対策を通じて生じ得る被害の度合いを「限定的なダメージ」に抑えることを目指す。

また、「経済的影響の度合い」は、大規模な誤配送が生じないよう「限定的な経済影響」に抑えるものとする。

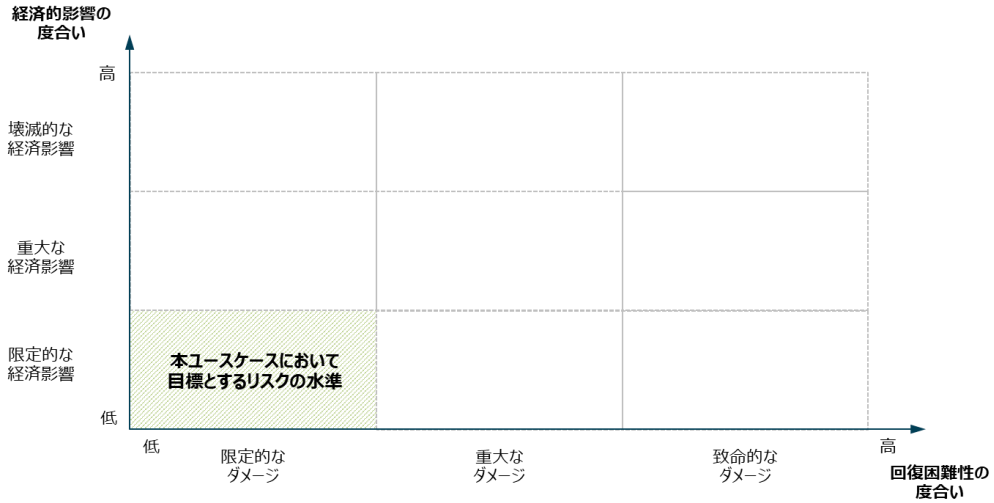


図 25 物流倉庫システムにて目標とするリスクの水準

(2) リスクアセスメント

「回復困難性の度合い」及び「経済的影響の度合い」から、物流倉庫システムのリスクアセスメントを行う。

① 想定されるセキュリティインシデント等とその結果の特定

倉庫管理システム、倉庫制御システム及び AGV 等において、想定され得るセキュリティインシデント等とその結果（影響）を特定する。倉庫管理システム、倉庫制御システム、AGV 等の利用に際して想定されるセキュリティインシデント（例）は以下の通り。

- 悪意のある攻撃者により外部から倉庫管理システムが不正アクセスされる。その結果、顧客情報が流出する。
- 悪意のある攻撃者により外部から倉庫管理システムが不正アクセスされる。その結果、保存されている在庫情報が改ざんされ、配送の停止や誤配送が生じる。
- 不正な外部記憶媒体（USB メモリ等）を挿入された保守用端末を通じて倉庫制御システムがマルウェアに感染する。その結果、AGV が停止することで、庫内の資材搬送業務が停止する。
- システムインテグレータから、ネットワークを通じた不適切な内容を含むアップデートの配信、もしくはローカル環境での不適切な内容を含むアップデートの実行がなされる。その結果、倉庫管理システム、倉庫制御システム及び AGV 等が想定しない動きをすることで庫内の資材搬送業務が停止する。

② ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーごとに「回復困難性の度合い」「経済的影響の度合い」の観点からリスクアセスメントを行う。

- 物流事業者
- システムインテグレータ
- AGV 製造事業者

- 物流事業者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、AGV 等から稼働情報が漏えいする可能性があるものの、物流事業者の従業員の個人情報等が漏えいする可能性は低いと想定される。セーフティの観点においては、作業員が作業するエリアと AGV が稼働するエリアが保護柵で分けられており、かつ、AGV が低速で進むことを前提としているため、ピッキングステーションで商品を集荷する作業員が AGV の誤作動により、重症を負う可能性は低く軽傷で済む可能性が高い。

したがって、プライバシーの観点では個人情報等が流出する可能性があること、セーフティの観点では軽傷を負う可能性があることから、「回復困難性の度合い」のレベルは「限定的なダメージ」とする。

B) 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、倉庫制御システムがマルウェアに感染し AGV が停止する

ことによって倉庫内の経済活動（庫内の資材搬送業務）の中断や資材の誤配送等が生じる可能性がある。その結果として、各事象のステークホルダーを含む関係者に対する損害賠償（配送遅延や誤配送への対応等）の事後的な対応が発生し得る。加えて、「内外への直接影響（外部）」の観点において、担当地域で事業を行う搬送会社や工業資材の利用者等、物流事業者からサービスの提供を受ける倉庫外部の事業者等への影響が及ぶ可能性がある。本件倉庫が多数の在庫を抱えていることを踏まえると、大規模なシステムの障害等が生じた際には、稼働している全 AGV の停止やそれに伴う AGV の修理・交換が必要となった場合、自社のみならず多数の取引先の事業活動に大きな影響を及ぼすことが想定される。

「直接影響の継続時間」の観点においては、障害等が発生した後、AGV の修理や交換に一定の時間を要する可能性があり、業務の停止や効率低下等の影響がすぐには解消されないものと想定される。

「代替可能性」の観点において、AGV が停止した際には集荷を人力で行う必要が生じ、大規模な物流機能を維持するための高い出荷能力を保てない可能性が高いと想定される。

また、間接的な経済影響の観点において、AGV の修理や交換に一定のコストを要する可能性がある。

したがって、直接的な経済影響及び間接的な経済影響を双方踏まえると、広範囲に影響が及ぶ可能性があり、サプライチェーン全体の経済活動も停止する可能性があることから、全体の経済影響は非常に大きくなると想定されるため、「経済的影響の度合い」のレベルは「壊滅的な経済影響」とする。

- システムインテグレータ

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、倉庫管理システム、倉庫制御システム、AGV 等からシステムインテグレータの従業員の個人情報等が漏えいする可能性はなく、また、セーフティの観点においても AGV 等に関する事故がシステムインテグレータに及ぼす可能性はないと考えらえる。

したがって、プライバシーの観点では個人情報等が流出する可能性が低いこと、セーフティの観点でもけがを負う可能性が低いことから、「回復困難性の度合い」のレベルは「限定的なダメージ」とする。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、不正なアップデートを倉庫管理システム、倉庫制御システム、AGV 等に配信した場合、物流事業者のシステムに対する影響範囲を確認する必要があるため、システムインテグレータの経済活動等の直接的な停止につながると想定される。また、「内外への直接影響（外部）」の観点では、倉庫管理システム等を提供している他の物流事業者への影響を確認する必要が生じるため、少なからず影響が生じると想定される。

「直接影響の継続時間」の観点において、不正なアップデートを倉庫管理システム、倉庫制御システム、AGV 等に配信した場合、物流倉庫の現場は混乱をきたしすぐに復旧するとは考えにくい。

「代替可能性」の観点において、不正なアップデートを倉庫管理システム、倉庫制御システム、AGV 等に配信した場合、代わりとなる仕組みを即座に用意することはできない。

間接的な経済影響の観点において、倉庫制御システム等に重大な脆弱性が発見され、システムインテグレータの責任において工場が停止した場合、製品回収が生じる可能性があると想定される。

したがって、直接的な経済影響は重大であり、間接的な経済影響も重大であると想定されるため、「経済的影響の度合い」のレベルは「重大な経済影響」とする。

- AGV 製造事業者

A)　発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、AGV 等から AGV 製造事業者の従業員の個人情報等が漏えいする可能性はなく、また、セーフティの観点においても AGV 等に関する事故がシステムインテグレータに及ぼす可能性はないと考えらえる。

したがって、プライバシーの観点では個人情報等が流出する可能性が低いこと、セーフティの観点でもけがを負う可能性が低いことから、「回復困難性の度合い」のレベルは「限定的なダメージ」とする。

B)　発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、AGV のサイバーセキュリティに関する故障等により、AGV 製造事業者の経済活動等の直接的な停止につながるとは想定しにくい。また、「内外への直接影響（外部）」の観点では、AGV のサイバーセキュリティに関する故障等により他の企業による買い控えが生じる可能性があると想定される。

「直接影響の継続時間」の観点において、AGV のサイバーセキュリティに関する故障等により、物流倉庫の現場は混乱をきたしすぐに復旧するとは考えにくい。

「代替可能性」の観点において、AGV のサイバーセキュリティに関する故障等が生じた場合、代わりとなる仕組みを即座に用意することはできない。

ただし、間接的な経済影響の観点において、AGV に重大な脆弱性が発見され、AGV 製造事業者の責任において工場が停止した場合、製品回収が生じる可能性があると想定される。

したがって、直接的な経済影響は重大であり、間接的な経済影響も重大であると想定されるため、「経済的影響の度合い」のレベルは「重大な経済影響」とする。

③　マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 1 軸「回復困難性の度合い」及び第 2 軸「経済的影響の度合い」からカテゴライズし、マッピングする。

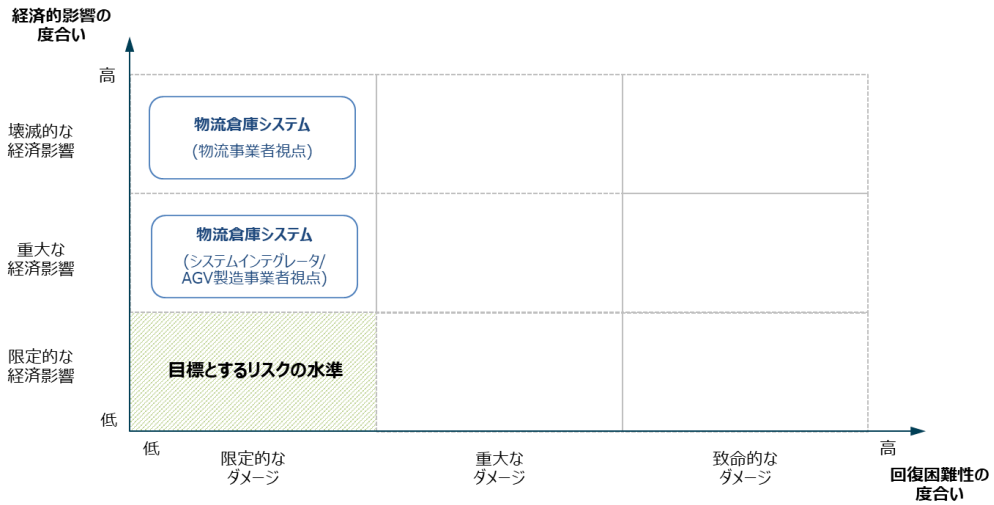


図 26　各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

物流事業者視点からみた物流倉庫システムの「回復困難性の度合い」は低くなるものの、「経済的影響の度合い」は、大きくなる。これは、当該事業者における従業員のけがや個人情報流出等には直結することは想定しがたいものの、物流倉庫システムに何らかの重大な欠陥や不正な機能が発見され、物流倉庫システムの停止につながった場合に、工場が停止し損害を被るためである。

システムインテグレータ、AGV 製造事業者視点からみた対象の機器・システムの「回復困難性の度合い」は物流事業者視点の物流倉庫システムと同様に低くなる。一方で、物流事業者視点の物流倉庫システム程の被害ではないものの、「経済的影響の度合い」は重大になると想定される。これは、各々の経済活動は停止しないものの、製品回収が生じる可能性があるためである。

これらを踏まえると、物流事業者、システムインテグレータ及び AGV 製造事業者視点の対象の機器・システムにおいて想定されるリスクは、目標とするリスクの水準には収まっていないため、適用主体である物流事業者は、これらの対象の機器・システムがもつリスクを目標とするリスクの水準に収めることを目指して対策を行う。

例えば、以下のように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えられる対策等の検討を行うことができると考えられる。

- 物流事業者にとって影響度が大きいリスクに対処するための対策方針
  - 経済的影響の度合いの観点

    物流事業者にとっては、自身が運用する倉庫の長時間の稼働停止及び、それに伴う取引先を含む広範囲にわたるサプライチェーンの途絶等が重要なリスクとなるが、これらのリスクに対応するため以下の対策が有効であると考えられる。
    - ✧ 信頼性の高い物流倉庫の操業を可能にするための仕組みの構築
    - ✧ セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築

- システムインテグレータにとって影響度が大きいリスクに対処するための対策方針
  - 経済的影響の度合いの観点

    システムインテグレータにとっては、開発や保守を担当する倉庫管理システムや倉庫制御システムにおいて、自身の過失（アップデート等を実行する保守端末の管理不備）により契約違反が生じ得ることがリスクである。これらのリスクに対応するため、物流事業者から以下の対策の実施をシステムインテグレータに依頼することが望ましい。
    - ✧ 安全なアップデートプログラムの配信のための仕組みの構築

上記で示した対策例を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

表 19 影響度が大きいリスクに対処するための対策方針及び添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
物流事業者	セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築	様々な IoT 機器を接続する際のセキュリティの確保
		適切なネットワークの分離
	信頼性の高い物流倉庫の操業を可能にするための仕組みの構築	IoT 機器・システムの十分な可能性の確保
		IoT 機器・システムのモニタリング及びログの取得、分析
システムインテグレータ	大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守
		セキュリティ設計と両立するセーフティ設計の仕様化
	安全なアップデートプログラムの配信のための仕組みの構築	IoT 機器・システムに対するアップデートの適用

(3) リスク対応

① システムを構成する機器ごとの脅威の整理

システムを構成する機器ごとに整理した脅威は以下の通り。

表 20 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
倉庫管理システム (WMS：Warehouse Management System)	データの改ざん	倉庫管理システムに保存された情報（例：入庫管理情報、在庫管理情報、出荷管理情報、棚卸管理情報等）が改ざんされる。
	情報漏えい	倉庫管理システムに保存された情報（例：入庫管理情報、在庫管理情報、出荷管理情報、棚卸管理情報等）が漏えいする。
	サービス不能	倉庫管理システムが外部からの大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、倉庫管理システムに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、倉庫管理システムがマルウェアに感染する。
	不正利用	倉庫管理システムが正規の物流事業者の事業員によって不正に意図しない用途等で利用される。
	利用者によるセキュリティ設定の誤り等	物流事業者の従業員による倉庫管理システムのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
操作用端末	データの改ざん	操作用端末に保存された情報が改ざんされる。
	情報漏えい	操作用端末に保存された情報が漏えいする。
	サービス不能	操作用端末が外部からの大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、操作用端末に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、操作用端末がマルウェアに感染する。
	不正利用	操作用端末が正規の物流事業者の事業員によって不正に意図しない用途等で利用される。
	利用者によるセキュリティ設定の誤り等	物流事業者の従業員による操作用端末のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
保守用端末	データの改ざん	保守用端末に保存された情報が改ざんされる。
	情報漏えい	保守用端末に保存された情報が漏えいする。
	サービス不能	保守用端末が外部からの大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、保守用端末に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、保守用端末がマルウェアに感染する。
	不正利用	保守用端末が正規の物流事業者の事業員によって不正に意図しない用途等で利用される。

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
	利用者によるセキュリティ設定の誤り等	物流事業者の従業員による保守用端末のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
倉庫制御システム (WCS：Warehouse Control System)	データの改ざん	倉庫制御システムに保存された情報（例：AGV 等の設備の管理情報、AGV 等の設備の制御情報等）が改ざんされる。
	情報漏えい	倉庫制御システムに保存された情報（例：例：AGV 等の設備の管理情報、AGV 等の設備の制御情報等）が漏えいする。
	サービス不能	倉庫制御システムが外部からの大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、倉庫制御システムに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、倉庫制御システムがマルウェアに感染する。
	不正利用	倉庫制御システムが正規の物流事業者の事業員によって不正に意図しない用途等で利用される。
	利用者によるセキュリティ設定の誤り等	物流事業者の従業員による倉庫制御システムのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
安全制御 PLC	サービス不能	安全制御 PLC が外部からの大規模な DDoS 攻撃を受け、サービスを提供できなくなる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、安全制御 PLC に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、安全制御 PLC がマルウェアに感染する。
ルータ	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、ルータに不正アクセスされる。
	不正利用	ルータが正規の住まい手によって不正な設定等で利用される。
AGV	データの改ざん	AGV に保存された情報（例： AGV 等の設備の制御情報等）が改ざんされる。
	情報漏えい	AGV に保存された情報（例： AGV 等の設備の制御情報等が漏えいする。
	マルウェア感染	外部からの悪意のある攻撃によって、AGV がマルウェアに感染する。
	不正利用	AGV が正規の物流事業者の事業員によって不正に意図しない用途等で利用される。
	利用者によるセキュリティ設定の誤り等	物流事業者の従業員による AGV のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。

② 脅威への対策の整理

想定される脅威を踏まえ、第 3 軸「求められるセキュリティ・セーフティ要求」における観点ごとに有効と考えられ物流事業者にて実装が想定される対策要件を整理する。

表 21 物流事業者にて実装が想定される対策要件（例）

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の決定
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守
		全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		全般	適切な水準のアクセス制御の実装の要求
		全般	ソフトウェアの完全性の検証
		全般	ソフトウェアのインストールの制限
		全般	様々な IoT 機器に接続する際のセキュリティの確保
		全般	暗号化によるデータの保護
		全般	ライフサイクルを通じた暗号鍵の管理
		マルウェア感染	マルウェア対策の実施
		全般	IoT 機器・システムの十分な可用性の確保
		全般	適切なネットワークの分離
		全般	IoT 機器・システムの設置場所等に対する物理的アクセスの制御
		データの改ざん 不正アクセス	IoT 機器システムの構成要素（機器、ネットワーク等）の物理的保護

第 3 軸	実装先	想定される脅威（例）	対策要件
		全般	セキュリティ設計と両立するセーフティ設計の仕様化の指示
		全般	セキュアな開発環境と開発手法の適用の指示
		全般	IoT 機器・システムにおけるセキュリティ機能の検証
		全般	システムインテグレータに対する IoT 機器・システムにおける運用開始時の正しい設置、設定
第 2 の観点	ソシキ・ヒト	全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
		全般	サービス提供や管理のポリシーの提示・遵守
	プロシージャ	全般	脆弱性対応に必要な体制や手順等の整備と実践
		全般	インシデント対応手順の整備と実践
		全般	事業継続計画の策定と実践
		全般	IoT 機器・システムの用途・用法を守った使用
		不正利用 不正アクセス	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令及び契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		不正利用	IoT 機器・システムに対するアップデートの適用
		情報漏えい	IoT 機器・システムの安全な廃棄又は再利用
		全般	IoT 機器・システムに対するアップデートの適用（セキュリティパッチの開発・配布等）

③　整理した対策に対する意思決定

対策等を検討する際にはインシデントの起こりやすさも踏まえ、システム全体としてのリスクを低減するような対策を検討する。従来、工場や物流拠点等において稼働する制御システムは、ベンダーごとに固有の仕様を多く含み、外部ネットワークや共用システムとは接続されていない等の認識の下で、セキュリティの脅威は殆ど問題視されてこなかった。しかし、近年、システム構成やその利用環境の変化、及び制御システムを狙った脅威の高度化等を背景に、セキュリティ対応の必要性が非常に高まってきている[33]ことから、制御システムに特有とされる性質等にも注意を払いながら、対策に関する意思決定を行う。

- 対策の適用対象（どの機器を中心に検討するか）

想定しているインシデントが現に発生した際に生じる被害の大きさ及びその起こりやすさ等を考慮して、本稿における倉庫管理システム、操作用端末、保守用端末、倉庫制御システム及び AGV 等の資産から、特に重点的に対策を検討すべき資産を検討する。

被害の大きさの観点では、情報系ネットワークと制御システムネットワークを分離した上で、本稿で想定する物流倉庫の稼働に直接影響を与えると思われる以下のシステム及びその機器を中心として対策を検討すべきである。

➢ 倉庫管理システム、操作用端末、保守用端末

倉庫制御システムに対して出庫指示ができなくなる結果、倉庫全体に混乱をもたらし、庫内物流機能がストップする上に、倉庫外部の経済活動にも影響を及ぼす可能性がある。

[33] 独立行政法人 情報処理推進機構(IPA)「制御システムのセキュリティリスク分析ガイド第2版」(2020年 3 月)参照。

- 倉庫制御システム、安全制御 PLC、AGV
  人手による出庫ができるため、完全停止までは至らないものの、AGV 等を活用した自動運搬ができなくなった場青ため、大規模な遅延が生じる。

また、起こりやすさの観点では、外部からのネットワーク経由での攻撃に対して十分に対処する必要があるため、倉庫外部のネットワークに直接接続されている機器（例：倉庫管理システム、操作用端末及び保守用端末等）を中心として重点的に対策を検討しつつ、その他の資産も含めて多層的に対策要件を実装することが望ましい。

- 適用する対策の内容（どのように対策を実施するか）

②にて検討した物流事業者にて実装が想定される対策要件の例より、より効率的・効果的にリスクを低減できるものを中心として対策を検討する。例えば、制御システムのセキュリティにおいては、情報の機密性よりも可用性や完全性が重視される傾向があり、運用上の制約等も相まって、AGV や AGV を制御する PLC にエンドポイントセキュリティソフトを導入する等の IT 環境では一般的なセキュリティ対策を実施することが難しいケースがある。その場合には、以下の対策要件を実装した上で、より上位のシステムで守る構成とすることにより、効率的・効果的にリスクを低減することが望ましい。

- 運用前（設計・製造段階）における法令及び契約上の要求事項の遵守
- 企画設計段階におけるセキュリティ要求事項の分析及び仕様化
- 様々な IoT 機器を接続する際のセキュリティの確保
- IoT 機器・システムの十分な可能性の確保
- 適切なネットワークの分離
- セキュリティ設計と両立するセーフティ設計の仕様化
- IoT 機器・システムのモニタリング及びログの取得、分析
- IoT 機器・システムに対するアップデートの適用

上記を踏まえて、AGV がもつリスクを目標とする水準に収めることを目的として、物流事業者が実装することとした対策要件の例を以下に示す。

第 1 の観点では、物流事業者が企画段階において、物流事業者、システムインテグレータ及び AGV 製造事業者のリスクを抑えることを目的として実装することとした対策要件を整理した。

第 2 の観点では、物流事業者の運用段階において、物流事業者、システムインテグレータ及び AGV 製造事業者のリスクを抑えることを目的として実装することとした対策要件を整理した。

第 3 の観点については、本ユースケースが対象とする業務やシステムでは法令等による運用担当者への専門資格保有の要求、あるいはそれに相当する業界又は社内の人事等に関する慣行は必ずしも認められないと考えることから、システムの仕様について知見を有するシステムインテグレータとの平時又は有事の際における協力を念頭に置きつつも、これらに該当する対策要件は必ずしも実装しないこととした。

第 4 の観点には、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネットの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

なお、第 1 の観点及び第 2 の観点における対策要件のうち、物流事業者単体では対応が難しい対

1265 策要件がいくつか見られた。これらの対策要件の実装やその他の技術的支援はシステムインテグレー
1266 タに依頼することとした。

1267 表 22 物流事業者において実際に講じる対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● 対象となっている物流倉庫におけるセキュリティポリシー（例：情報システムを対象としたセキュリティ規定、制御システムを対象としたセキュリティ規定）の策定及び、事業部長等の適切な承認権限を有する者の承認。 ● 定められた期間ごとの当該ポリシーのレビュー。	
2			運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保	● 各倉庫におけるセキュリティ管理責任者の任命。 ● 本社の情報システム部門における自社倉庫のセキュリティを担当する要員の明確化。 ※ 上記の管理責任者及び開発担当者は、物流倉庫システムのライフサイクルの各段階（例：開発、運用）において明確化されていることが望ましい。	
3			IoT セキュリティに関するステークホルダーの役割の決定	● 倉庫制御システム及び関連機器(AGV)のセキュリティ対策の設計・開発・運用等における関係各社の責任範囲の決定。 ● 運用中に発生したセキュリティインシデントにより損害が発生した場合の責任範囲（役割分担や損害賠償）の決定	
4			IoT 機器・システムに係る要員のセキュリティ確保	● 自社の要員及び委託する業務（システムインテグレータに対する倉庫制御システムの開発）に関わる者に対するセキュリティ上の要求事項の規定。（退職後又は契約後も含む） ● 自社内の要員（倉庫にて業務に従事する要員）に対する適切な訓練及びセキュリティ教育の実施。	
5		システム	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守	● 情報セキュリティに関連する法的な規制又は契約上の義務に対する違反を避けるための要求事項の特定及び遵守。	○ （「大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進」に有効と考えられる対策）
6			企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	● 本社の情報システム部門の担当者が中心となり、倉庫における業務担当者を巻き込み、倉庫制御システムの企画・設計時におけるリスクアセスメントの実施、セキュリティ要件の特定、要件の実装に係る費用の確保。 ● 必要なセキュリティ仕様が組み込まれているかを確認する設計レビューの実施。 ● 特定したセキュリティ要求事項を倉庫制御システムの委託仕様書への記載。	○ （「大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進」に有効と考えられる対策）
7			IoT 機器システムの構成要素（機器、ネットワーク等）の物理的保護	● 外部の物理的な脅威から保護されるべき AGV や AGV 制御 PLC、その他の資産への認可されていないアクセスを防ぐ目的で、入退管理（例：職員証や入館ゲート等）を通じた物理的セキュリティ境界の確立。	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
8	第 2 の観点	ソシキ・ヒト	運用中における IoT セキュリティを目的とした体制の確保	● 各倉庫におけるセキュリティ管理責任者の任命。 ● 本社の情報システム部門における自社倉庫のセキュリティを担当する要員の明確化。 ※ 上記の管理責任者及び開発担当者は、物流倉庫システムのライフサイクルの各段階（例：開発、運用）において明確化されていることが望ましい。	
9			過去の対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的なインシデント抑制への活用。（同業他社の IoT 機器・システムにおけるセキュリティインシデントを含む）	
10			サービス提供や管理のポリシーの提示・遵守	● 倉庫制御システムを対象としたセキュリティポリシーの遵守。	
11		プロシージャ	脆弱性対応に必要な体制や手順等の整備と実践	● 本社の情報システム部門における脆弱性情報の収集及び評価の実施。 ● 倉庫制御システム又は倉庫管理システムに関連した脆弱性が明らかになった場合、これらの脆弱性に対応するための手順の整備。 ● 倉庫制御システムを構成するソフトウェアの脆弱性が明らかになった場合の、対応手順の整備。	
12			インシデント対応手順の整備と実践	● 物流事業者が自身で運用する物流倉庫システムに適応したインシデント対応手順の整備。 ● 各要員の役割と責任の識別及び指定された個人によって実行されるアクションの定義・伝達。 ● システムインテグレータ等に対する自組織のインシデント対応手順の伝達及び内容調整。 ● インシデント対応手順の定期的な訓練。（自組織とシステムインテグレータ等との間で連携を要する部分も含む） ※セキュリティの観点に加え、セーフティの観点を考慮する。	
13			事業継続計画の策定と実践	● 危機的な事象が発生した場合に達成すべき事業上の必要性に基づいた復旧目標を規定し、物流倉庫の運用業務に対する事業継続計画の作成。 ● 事業継続計画を支援するバックアップ及び復元の手順の作成。 ※事業継続計画はサイバーセキュリティを主たる脅威として想定したものとなっていることが望ましい。	
14			IoT 機器・システムの適正な使用	● 想定された用途・方法での倉庫管理システム、倉庫制御システム及び AGV 等の使用。	
15			IoT 機器・システムの適正な運用・保守	● システムインテグレータ及び AGV 製造事業者が提示するガイドに従った保守、管理。	
16		システム	運用中における法令及び契約上の要求事項の遵守	● 情報セキュリティに関連する法的な規制又は契約上の義務に対する違反を避けるための要求事項の特定及び遵守。	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
17			継続的な資産管理	● 物流倉庫システムを構成する資産目録（機器上に実装されたソフトウェア及びファームウェア、工場出荷時の設定等を含む）の作成・維持 ※物流倉庫システムが長期の運用となることを想定する。	
18			プログラムソースコード及び関連書類の保護	● 物流倉庫システムに係るプログラムソースコード及び関連書類（例：設計文書）への論理アクセスを最小限にした上で、多要素認証の実施	
19			IoT 機器・システムのモニタリング及びログの取得、分析	● 本社の情報システム部門の担当者による物流倉庫システムを構成する倉庫管理システムや倉庫制御システムを対象にした各種ログ（例：ユーザ認証、ネットワークトラフィック）の取得及び保護。 ● 取得したログの定期的な分析及び異常の検知。	○ （「信頼性の高い物流倉庫の操業を可能にするための仕組みの構築」に有効と考えられる対策）
20			IoT 機器・システムに対するアップデートの適用	● 脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定 ● システムインテグレータ等への修正プログラム等開発の依頼 ● パッチの適用前に動作検証を実施。 ● 提供を受けたセキュリティパッチの適用 ※システムインテグレータ等と相談した上で、パッチを適用することが望ましい。	
21			IoT 機器・システムの安全な廃棄又は再利用	● 物流倉庫システムを構成する機器（例：AGV や AGV 制御 PLC 等）内部に保存されている情報の削除。（読み取り不可処理を含む）	

- 委託仕様書に基づきシステムインテグレータが実装する対策（例）

物流倉庫システムの開発及び保守を委託しているシステムインテグレータへの委託仕様書等に基づいて、システムインテグレータは主に以下の対策要件を実装するものとする。

表 23 委託仕様書等に基づきシステムインテグレータが実装する対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	適切な水準のアクセス制御の実装の要求	● 物流倉庫システムにおけるアカウントの管理について、例えば以下のような自動化されたメカニズムの導入・運用。 ● 倉庫管理システム及び倉庫制御システムからアカウント情報の定期的な自動収集	
2			ソフトウェアの完全性の検証	● 倉庫管理システム、倉庫制御システム、操作用端末、保守用端末のソフトウェアに関する完全性の検証機能の実装。	
3			ソフトウェアのインストールの制限	● 倉庫制御システムを構成する機器（例：AGV、AGV 制御 PLC）にインストール可能なソフトウェアをあらかじめ特定した上で、構成を維持できる機能の実装。 ● ※構成を変更する場合は、システムインテグレータ等と相談した上で、ソフトウェアのインストール等を実施することが望ましい。	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
4			様々な IoT 機器に接続する際のセキュリティの確保	● AGV 制御 PLC 等を他の AGV 機器等に接続する際のホワイトリストの適用。	○ （「セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築」に有効と考えられる対策）
5			暗号化によるデータの保護	● 適切な強度の方式（IPsec-VPN、SSL-VPN 等）による倉庫外（自社の他拠点）からの通信の保護。 ● 倉庫管理システム、倉庫制御システムに保管されている利用者情報、配送先情報、対象商品情報、システム稼働情報等の暗号化。	
6			ライフサイクルを通じた暗号鍵の管理	● 暗号鍵の利用，保護及び有効期間に関するポリシーの策定及び遵守。	
7			マルウェア対策の実施	● 倉庫管理システム、操作用端末、保守用端末におけるマルウェア対策ソフトウェアの導入。 ● 外部の保存媒体（例：USB メモリ）との接続の制限。	
8			IoT 機器・システムの十分な可用性の確保	● 倉庫外部からの通信を受信し得る倉庫管理システム等に対する(D)DoS 攻撃を想定し、一定レベルの負荷に耐える容量を確保。 ● 倉庫管理システム、操作用端末、保守用端末、倉庫制御システム等において不審な通信（例：特定の IP アドレスからの大量のリクエスト）の検知及び遮断。 ● アプリケーションのテスト段階における一定レベルの負荷試験の実施。	○ （「信頼性の高い物流倉庫の操業を可能にするための仕組みの構築」に有効と考えられる対策）
9			適切なネットワークの分離	● リスクレベルに応じた情報ネットワーク、情報制御ネットワーク、制御ネットワーク等の複数のゾーンへのネットワークの分割。 ● FW 等での AGV や AGV 制御 PLC が含まれているゾーンで送受信される全ての不要な通信の遮断。	○ （「セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築」に有効と考えられる対策）
10			IoT 機器・システムの設置場所等に対する物理的アクセスの制御	● AGV や倉庫管理システム等が設置されている自組織の業務上重要な施設への物理アクセスに対する監視カメラ等によるモニタリング。	
11			セキュリティ設計と両立するセーフティ設計の仕様化の指示	● 作業員や機器の周辺への危害を回避するための安全機能（本質安全設計、予防安全機能等）の実装。 ● AGV に実装された安全機能と外部との通信回線との分離。	○ （「大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進」に有効と考えられる対策）
12			セキュアな開発環境と開発手法の適用の指示	● 物流倉庫システム開発時のセキュアコーディング手法の適用。 ● 委託先を含む開発人員向けのセキュリティ対策、開発環境やコードへのアクセスの制御、開発環境と運用環境の分離等、安全な開発環境に必要な対応の実施。 ● 設計書、プログラム、バイナリ等のバックアップ。	
13			IoT 機器・システムにおけるセキュリティ機能の検証	● 倉庫管理システムリリース前の倉庫管理システム、操作用端末、保守用端末、倉庫制御システム等に対するペネトレーションテストの実施。	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
14			システムインテグレータに対する IoT 機器・システムにおける運用開始時の正しい設置、設定	● 倉庫管理システム、倉庫制御システム、AGV 制御 PLC、操作用端末及保守端末の適切な設置・設定。 ● AGV 製造事業者から提供されたガイドに従った AVG 等の設置及び設定。 ● IoT 機器製造事業者が想定する仕様に適合したネットワーク環境の整備。	
15	第 2 の観点	システム	IoT 機器・システムに対するアップデートの適用（セキュリティパッチの開発・配布等）	● 報告された脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定。 ● IoT 機器製造事業者や開発委託先等への修正プログラム等開発の依頼。 ● 物流事業者へのセキュリティパッチの提供。	○ （「安全なアップデートプログラムの配信」に有効と考えられる対策）

1273

2-3-4 化学プラント施設内の蒸留工程の自動制御

「IoT 機器・システムを通じて提供されるサービスの開発者」であるプラント事業者が IoT-SSF の主たる適用主体となってリスクマネジメントを行うユースケースを記載する。

プラント事業者は、一般のビニール製品に広く使用される化学物質を製造する事業者であり、操業開始から既に数十年程度プラントを運用している。当該事業者が製造する化学物質は、装置外部へ流出した場合に人体や環境に悪影響を及ぼす可能性のあるものであり、従来から従業員や立地地域等の安全（セーフティ）や環境の保護に関わる対応を重点的に実施してきたが、昨今世界的にプラント施設等におけるセキュリティインシデントやそれに伴う操業の停止等が多く報告されているため、本社の経営層を中心に機器のオープン化やネットワーク接続等に伴い新たに生じ得るサイバーセキュリティに関するリスクを懸念するようになっている。

本ユースケースでは、本社の経営層の指示により、プラント内のリスク管理部門が中心となって、対象機器・システムのセキュリティに関するリスクアセスメント等を行い、対処が必要なリスクに対しては、自身に加えてシステムインテグレータやプラント事業者向けにメンテナンスやサポートを行う事業者に対応を依頼することで、可能な限りリスクを低減することを目的とする。

(1) リスクアセスメント、リスク対応に向けた事前準備

① 対象ソリューションの概要

製造実行システム（MES）、HMI、プロセス制御 PLC 等からなるプラント制御システムを用いて、化学物質を製造するケースを想定する。

本ユースケースでは、主に以下の工程からなる化学プラントを扱うが、その中でも特に 4.の精製工程における蒸留工程を実施する装置を扱うものとする。

1. 反応工程：原料や酸素等を反応させ化合物を生成する工程
2. 洗浄工程：反応工程で生成された化合物を中和洗浄する工程
3. 分解工程：中和洗浄された化合物を熱によって分解する工程
4. 精製工程（蒸留工程を含む）：成分の沸点の差を利用して、分解工程までで生成された化合物を製品用に分離させる工程

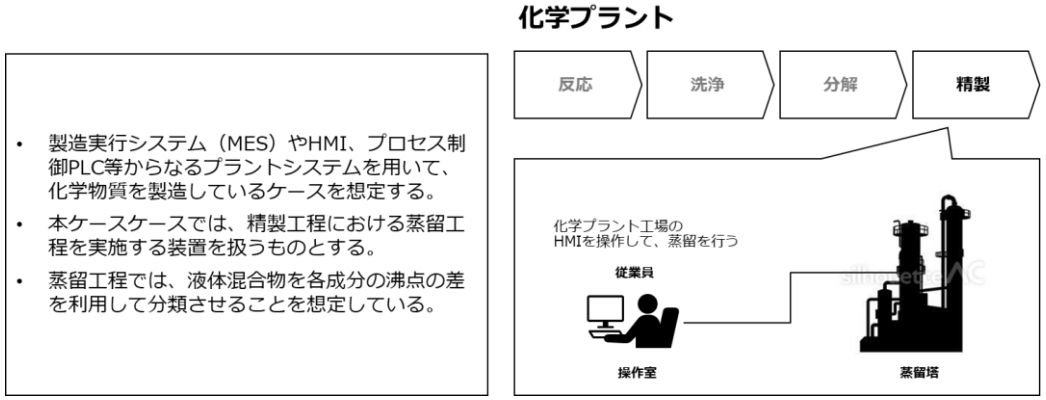


図 27 対象ソリューションの概要

② ステークホルダー関連図

対象の機器・システムの設計や構築、運用に関与するステークホルダーとして、「プラント事業者（委託元企業）」、「システムイングレータ（委託先企業）」「プラントエンジニアリング事業者」及び「プラント周辺の住民」を想定している。

- プラント事業者（委託元企業）

プラントを制御するシステムの開発をシステムインテグレータに対して委託した上で、本プラントを運用・管理する事業者であり、セキュリティ対策等の実施に対して主に責任を有する事業者である。本ユースケースで対象とするプラントは、操業開始から数十年が経過しており、設備の一部に老朽化等が見られるものとする。また、プラント事業者において今回リスクアセスメント等の対象となっている事業所におけるセキュリティ対策等の状況は以下の通り。

- リスク管理部門は存在するものの、プラント制御システムを所掌するセキュリティ責任者や担当者は必ずしも明確になっていない。セキュリティポリシーは存在するものの、情報システムのセキュリティに重点が置かれたものになっている。
- 情報システムにおけるセキュリティを念頭に置いた教育は実施されているものの、制御システムにおけるセキュリティを主に扱った教育は実施されていない。
- 情報資産管理台帳（サーバ、クライアント端末、ネットワーク機器、設備等を対象とする）は既に作成済みであり、特に制御システムについては資産の移動や追加の度に担当者が手動でメンテナンスしている。
- 外部ネットワークとプラント内部ネットワークとの境界及び、情報系ネットワークと制御情報系ネットワークとの境界にファイアウォールを導入しているものの、外部の監視サービス等は特に利用していない。
- 自然災害を想定した事業継続計画や、情報漏えいを想定したセキュリティインシデント対応手順は整備済み。

なお、本プラントは農林水産業が盛んな沿岸地域に立地しており、爆発事故が発生した場合には、人体に有害な物質が外部へ流出することで、プラント周辺の住民だけではなく、住民が営む農林水産業にも影響が生じ得るものとする。

- システムイングレータ（委託先企業）

プラント事業者から委託を受けプラントを制御するシステムを開発した上で、委託元企業に対して、プラント装置を制御するプラントシステム一式を提供する事業者である。

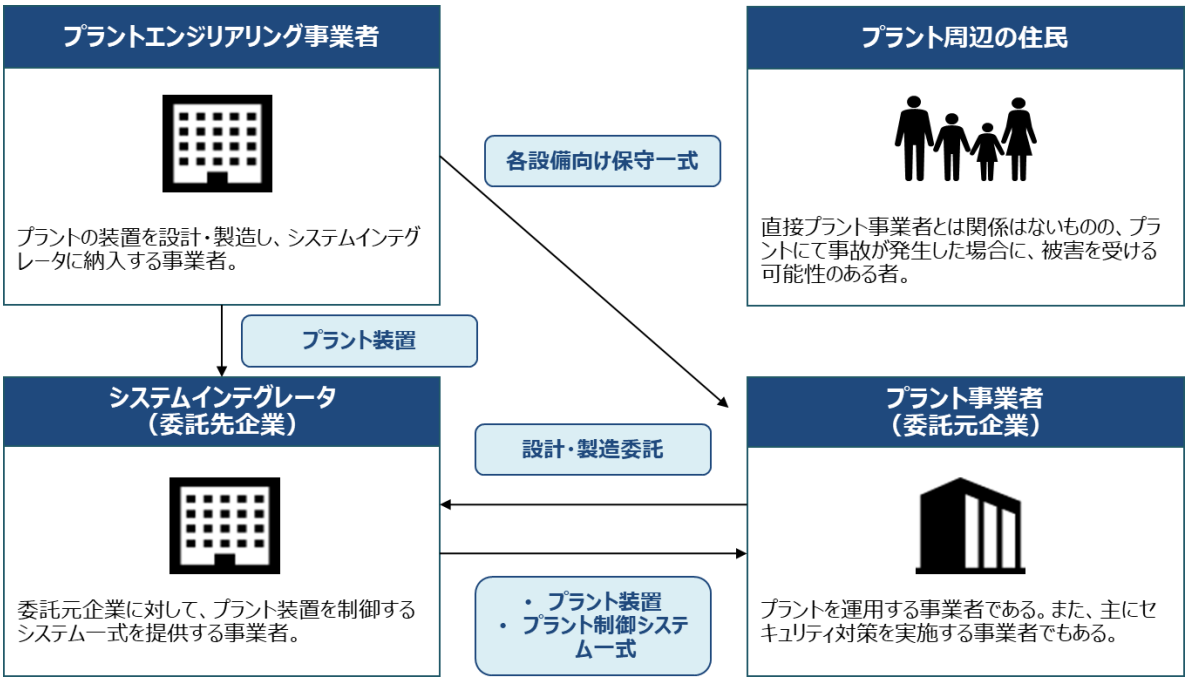
- プラントエンジニアリング事業者

プラントの装置を設計・製造し、システムインテグレータに納入する事業者である。また、プラントシステム（例：MES、HMI 等）のアップデートの配信等プラントの装置の保守・管理を行うことも想定している。

- プラント周辺の住民

直接プラント事業者とは関係はないものの、プラントにて事故が発生した場合に、被害を受ける可能

1335 性のある者。



1336

1337 図 28 ステークホルダー関連図

1338 ③ システムを構成する機器の一覧

1339 本稿の対象となる機器は以下の通りとする。

1340 表 24 システムを構成する機器の一覧

システムを構成する機器	内容
製造実行システム （MES：Manufacturing Execution System）	製造工程の把握や管理、作業者への指示や支援などを行うサーバ。 MES は、プラント事業者所内にサーバを設置するものとする。 なお、主な機能は以下の通り。 ● 作業のスケジュール管理機能 ● 作業手配・製造指示機能 ● 作業者管理機能 ● データ収集機能 ● プロセス管理機能 ● 製品の追跡と製品体系管理機能 ● 実績管理機能 ● 生産資源の配分と監視機能 ● 仕様・文書管理機能 ● 設備の保守・保全管理機能 ● 製品品質管理機能
ヒューマンマシンインターフェース （HMI：Human Machine Interface）	人間の操作と機械の動作をスムーズに結合するために使用されるハードウェアとソフトウェア。 具体的には、タッチパネル式の表示器やパネルコンピュータを指す。
プロセスサーバ	プロセス制御 PLC から収集するデータを扱うサーバ。
データヒストリアン	長期間のプロセス値や管理パラメータを保存し、分析を行うためのサーバ。 プロセス制御 PLC からのデータを収集するプロセスサーバより静的なデータ（ヒストリデータ）を扱う。
業務用サーバ/業務用端末	非制御系の情報を保存、利用するサーバ及び端末。 例えば、ファイルサーバやメールサーバ及びそれらを利用する端末を指す。
保守用端末	プラントシステムの保守を行う端末。 保守用端末はスタンドアロンにてプラント内に設置するものとする。

システムを構成する機器	内容
安全制御 PLC (PLC:Programmable Logic Controller)	停電等の有事の際に、作業員による安全確保の処理がなされるまでは勝手に稼働しないような「安全な仕組み」を提供する PLC。 安全制御 PLC は、プラント内に設置するものとする。
プロセス制御 PLC (PLC:Programmable Logic Controller)	センサからの測定値が設定値に一致する様に、偏差から調節方式に応じて算出した操作量を調節する PLC。
蒸留塔温度センサ	蒸留塔の中の温度を計測するセンサ。
蒸留塔加熱器	蒸留塔の中の温度を上昇させるための蒸気を作成する加熱器。

④　システム構成図、データフロー図

システム構成図は以下の通りとする。各種センサ、アクチュエータ類や、PLC、プロセスサーバ等から構成されるプラント制御システムは、セキュリティのレベルやネットワークの種類等に応じてあらかじめ複数の階層（制御情報系ネットワーク、制御系ネットワーク等）に分離されており、インターネット等の外部ネットワークと接続する情報系ネットワークとは最小限の通信しか行わないよう設計、運用されていることを想定する。

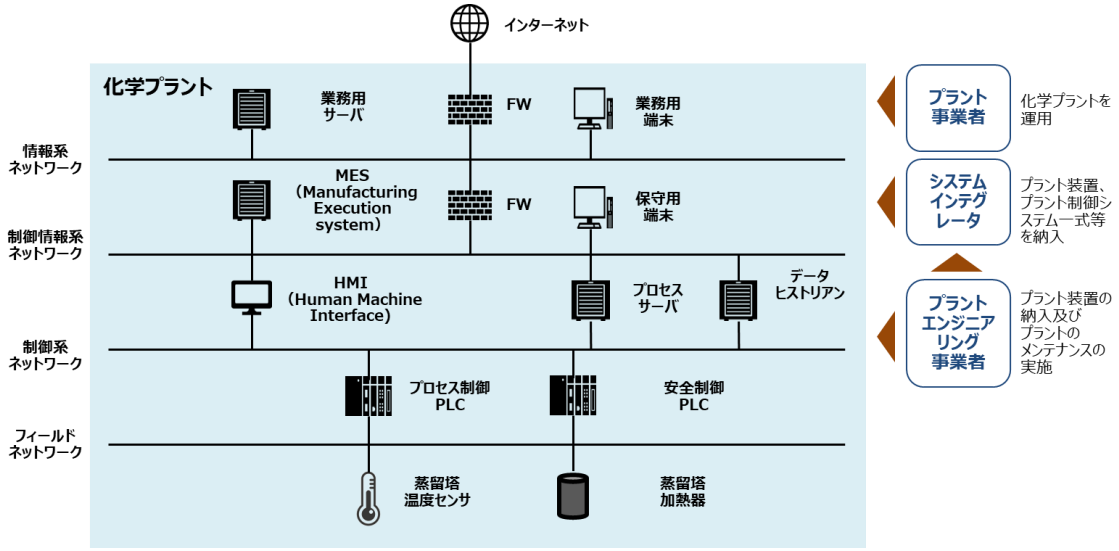


図 29 システム構成図

プラント事業者の従業員が HMI を操作して、蒸留塔内の温度を操作する場合のデータフローは以下の通りとする。

1. 温度センサがプロセス制御 PLC に温度情報を送信する。
2. プロセス制御 PLC が HMI に温度情報を送信する。
3. 従業員が HMI を操作することで、HMI がプロセス制御 PLC に制御コマンドを送信する。
4. プロセス制御 PLC が蒸留塔加熱器に制御コマンドを送信する。

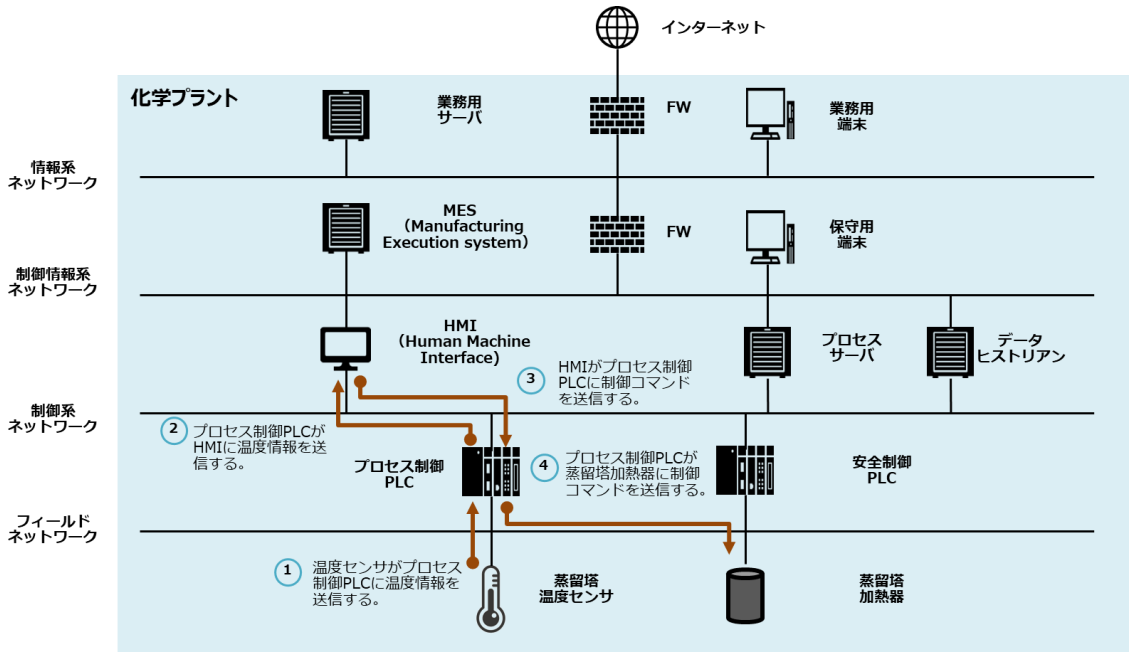


図 30 データフロー図（一部を抜粋）

⑤ リスク基準

化学プラントは、機能が停止、低下又は利用不可能な状態に陥った場合に、国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じる「重要インフラ」の 1 つに位置づけられており[34]、事業者内外を含めた社会という単位で見て、「回復困難性の度合い」及び「経済的影響の度合い」が相対的に大きくなりやすいことが想定される。かかる環境においては、他の業種等と同様に、「回復困難性の度合い」を「限定的なダメージ」なレベルまで、「経済的影響の度合い」を「限定的な経済影響」まで下げることが理想的ではあるが、それが現実的には難しいケースも想定される。ここでは、仮にプラント設備等に係る事故が発生した場合であっても、「高圧ガス・石油コンビナート事故対応要領」における C1 級[35]以上の事故にて想定される被害への発展を可能な限り防ぐことを念頭に置き、対策を講じることとした。

「回復困難性の度合い」に関しては、仮に内外に非常に大規模な影響を及ぼし得るような脅威が顕在化したとしても、C1 級に相当する事故につながらず、安全に業務やサービスの提供を保証できるよう「重大なダメージ」とならないようにすることを目指す。

また、「経済的影響の度合い」に関しては、工場の停止等が社会の大混乱（例：広範囲にわたるサプライチェーンの停止等）を引き起こす可能性があるため、持続的に業務やサービスの提供を保証できるよう「壊滅的な経済影響」とならないようにすることを目指す。

[34] 内閣サイバーセキュリティセンター(NISC)「活動内容」参照。
[35] ① 人的被害（負傷者1名以上5名以下かつ重傷者1名以下）があった事故、② 爆発、火災又は破裂・破損等が発生した事故、③ 毒性ガスが漏えいした事故）を生じた事故、④ ①から③までのほか、反応暴走に起因する事故又は多量漏えいが発生した事故のいずれかに該当するものを指す。

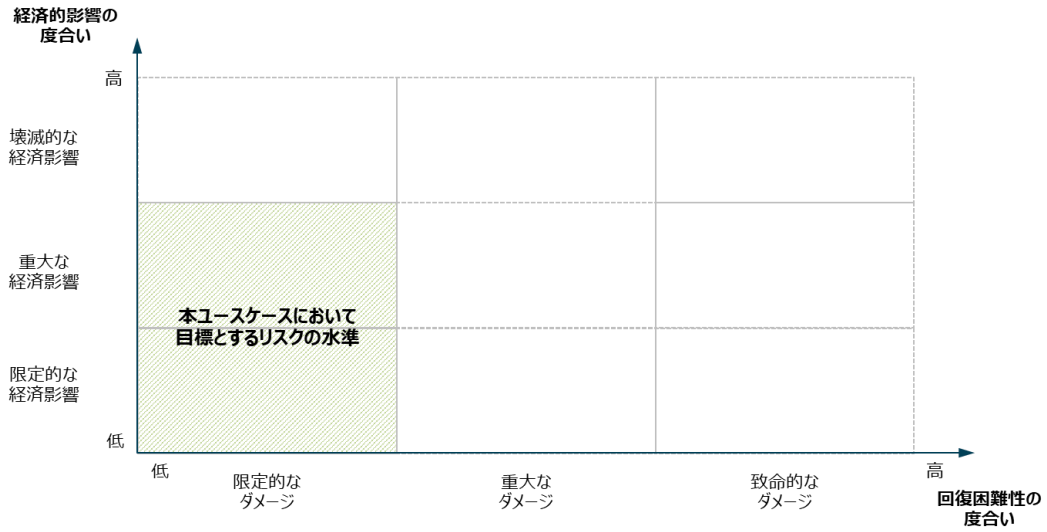


図 31 プラントシステムにて目標とするリスクの水準

(2) リスクアセスメント

「回復困難性の度合い」及び「経済的影響の度合い」から、プラント制御システムのリスクアセスメントを行う。

① 想定されるセキュリティインシデント等とその結果の特定

プラント制御システムにおいて、想定されるセキュリティインシデント等とその結果(影響)を特定する。当該システムの提供又は利用に際して想定されるセキュリティインシデント(例)は以下の通り。

- 生産計画を作成する情報システムや生産活動を実際に制御する制御設備等が外部ネットワークを通じてランサムウェアに感染することにより、プラントの操業が一時的に停止する。フェールセーフの機能が失われた場合、一部の化学反応が進み蒸留塔内部の温度が急速に上昇することによって、蒸留塔での爆発事故等が発生する。
- 不正な USB 等の外部記憶媒体を挿入された保守用端末を通じて、プラント制御システム内の設備がマルウェアに感染し、予期しない動作をする。その結果、蒸留塔内の正確な温度を把握することができなくなる。
- プラントエンジニアリング事業者が、ローカル環境にて MES やプロセス制御 PLC 等に対して不適切な内容を含む不正なアップデートを実行することで、これらの機器が想定しない動作を行う。その結果、プラント設備の稼働が停止する。

② ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーごとに「回復困難性の度合い」「経済的影響の度合い」の観点からリスクアセスメントを行う。

- プラント事業者
- プラント周辺の住民
- システムインテグレータ

- プラントエンジニアリング事業者

- プラント事業者

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、業務用サーバや業務用端末に加えて、MES 等からプラント事業者における従業員の個人情報や取引先担当者等の情報が流出する可能性がある。セーフティの観点では、セキュリティに関するインシデントによりプラント制御システムが停止し、かつ安全設備等が十分に作動しなかった場合に、一部の化学反応が進み蒸留塔内部の温度が上昇し蒸留塔等が爆発することにより、作業員が重症を負うか死亡する可能性がある。

プライバシーの観点では重要な個人情報が流出する可能性があることに加えて、セーフティの観点では、セキュリティインシデントにより、最悪の場合、従業員が死亡する可能性があることから、「回復困難性の度合い」のレベルは「致命的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、マルウェア感染に感染した上に、安全機能が適切に作動しないことで今回評価対象となる蒸留工程で制御設備（蒸留塔）が爆発し得る。また、爆発等の事故が発生した場合、その他の工程も停止する可能性が高く、プラント全体の生産活動が中断すると想定される。その結果として、各事象のステークホルダーを含む関係者に対する損害賠償（住民被害や環境汚染の対応等）の事後的な対応が発生し得る。「内外への直接影響（外部）」の観点では、サプライチェーンの川上に位置するプラントが停止することによって、川下の企業の経済活動にも大きな影響を与える可能性がある。

「直接影響の継続時間」の観点では、操業停止等の事象が発生した場合に稼働開始まで時間を要するとともに、環境汚染が発生した場合には長時間悪影響を及ぼし続けることとなると想定される。

「代替可能性」の観点では、本ユースケースにて想定するインシデントが発生し工場が停止した場合、即座に生産を他のプラント等に移転することは現実的ではなく、設備が再度稼働しなければ製品を精製することはできないと想定される。

間接的な経済影響の観点では、爆発事故等が発生した場合、プラント設備の修理に一定のコストを要する可能性があると想定される。

直接的な経済影響の観点において、爆発事故や工場停止に伴い大きな経済影響が生じる可能性があることから、「経済的影響の度合い」のレベルは「壊滅的な経済影響」と評価する。

- プラント周辺の住民

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点において、プラントにてセキュリティインシデントが発生したとしてもプラント周辺の住民の個人情報等が流出する可能性は低いと想定される。セーフティの観点において、セキュリティに関するインシデントにより、上述の通りプラントシステムが停止し爆発事故が発生した場合、有害物質が流出し周辺の環境を汚染することによって、住民等の健康や安全に多大な影響が生じる可能性があると想定される。

プライバシーの観点では個人情報等が流出する可能性が少ないものの、セーフティの観点では周辺

の住民等に重大な健康被害が生じる可能性があると考えられることから、「回復困難性の度合い」のレベルは「重大なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響」の観点では、セキュリティに関するインシデントにより前述の通りプラントシステムが停止し爆発事故が発生した場合、有害物質が周辺の環境を汚染することによって、農業や水産業に重大な影響を与える可能性がある。

「直接影響の継続時間」の観点において、有害物質が周辺の環境を汚染した場合、その影響は数年から数十年間の長期間にわたって続く可能性があると想定される。

「代替可能性」の観点において、農業や水産業に影響を与えた場合、代替は難しいと想定される。

また、間接的な経済影響の観点において、製品回収等の影響はないと想定される。

したがって、間接的な経済影響は大きくないものの、セキュリティに関するインシデントによりプラント制御システムが停止し爆発事故が発生した場合、直接的な経済影響が大きくなると想定されるため、「経済的影響の度合い」のレベルは「壊滅的な経済影響」と評価する。

- システムインテグレータ

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、システムインテグレータの従業員の個人情報等が流出する可能性は少ないと想定される。

セーフティの観点では、システムインテグレータの従業員がプラントの製造現場に常駐していない限りは、けがを負う可能性は低いと想定される。

プライバシーの観点ではシステムインテグレータの従業員の個人情報が流出する可能性が少ないこと、セーフティの観点ではシステムインテグレータの従業員がけがを負う可能性が少ないことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響」の観点では、セキュリティインシデントに伴いプラント制御システムが停止したとしても、システムインテグレータによる経済活動の中断等は生じ難いと想定される。「直接影響の継続時間」の観点や「代替可能性」の観点でも、システムインテグレータには影響が及びにくいと想定される。ただし、プラント事業者に対する注意喚起(例：設定方法に関する説明等)を怠ることで、サービス提供における過失が認められ得る。その結果として、契約上の責任が問われ得る。

間接的な経済影響の観点では、プラント制御システムが既に稼働していることもあり、システムインテグレータの責任に基づく大規模な製品回収（例：MES やプロセス制御 PLC 等）は起こりにくいと考えられるため、影響は限定的であると想定される。

直接的な経済影響及び間接的な経済影響の観点において、「経済的影響の度合い」が大きくなりにくいと想定されることから、「経済的影響の度合い」のレベルは「限定的な経済影響」と評価する。

- プラントエンジニアリング事業者

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、システムインテグレータと同様、プラントエンジニアリング事業者の従業員

の個人情報等が流出する可能性は低いと想定される。

セーフティの観点では、プラントエンジニアリング事業者の従業員がプラント工場の現場に常駐していない限りは、けがを負う可能性は低いと想定される。

プライバシーの観点ではプラントエンジニアリング事業者の個人情報が流出する可能性が低いこと、セーフティの観点ではプラントエンジニアリング事業者の従業員がけがを負う可能性が低いことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B)　発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、ローカル環境にて不正なアップデートを MES やプロセス制御 PLC 等に実行することで、制御設備（蒸留塔）が停止し得る。その結果として、各事象のステークホルダーを含む関係者に対する損害賠償（システムインテグレータへの補償等）の事後的な対応が発生し得る。また、プラントシステムに対する影響範囲を確認する必要があるため、プラント事業者向けにメンテナンスやサポートを行う事業者の経済活動等の直接的な停止につながると想定される。また、「内外への直接影響（外部）」の観点では、プラントシステムの保守等を提供している他のプラント事業者への影響を確認する必要が生じるため、少なからず影響が生じると想定される。

「直接影響の継続時間」の観点において、不正なアップデートをプラントシステム等に配信した場合、物流倉庫の現場は混乱し、すぐに復旧するとは考えにくい。

「代替可能性」の観点において、不正なアップデートを MES プロセス制御 PLC 等に配信した場合、代わりとなる仕組みを即座に用意することは難しいと想定される。

間接的な経済影響の観点では、プラントエンジニアリング事業者の責任において、製品回収等は生じないと想定される。

したがって、直接的な経済影響は重大であると想定されるため、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

③　マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 1 軸「回復困難性の度合い」及び第 2 軸「経済的影響の度合い」からカテゴライズし、マッピングする。

プラント事業者視点からみたプラントシステムの「回復困難性の度合い」及び「経済的影響の度合い」はどちらも非常に大きくなると想定される。また、プラント周辺の住民視点からみた「経済的影響の度合い」も非常に大きくなると想定される。これは、プラントシステムにおけるセキュリティインシデントが非常に重大な事故につながり得ること、そしてその事故がサプライチェーンや周辺の環境に大きな影響を与え得るためである。

システムインテグレータ、プラントエンジニアリング事業者視点の「回復困難性の度合い」は限定的となるものの、プラントエンジニアリング事業者視点の「経済的影響の度合い」はシステムインテグレータより比較的大きくなる。これは、プラントエンジニアリング事業者がアップデートの配信等を含む保守作業を担当しているためであり、ローカル環境で不正なアップデートを実行した場合に契約上の責任を問われ得るためである。

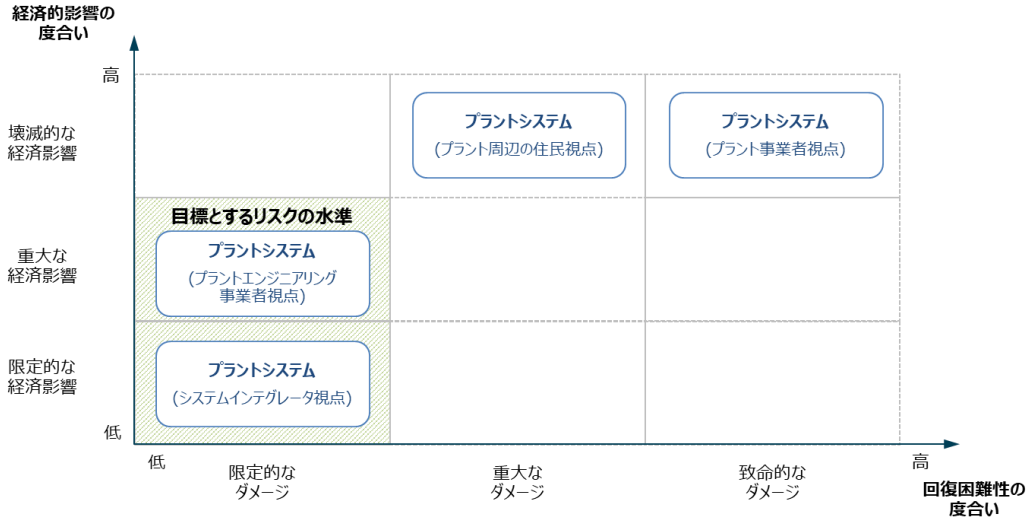


図 32 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

これらを踏まえると、システムインテグレータ、プラントエンジニアリング事業者視点のプラントシステム視点からみたプラントシステムで想定されるリスクは、目標とする水準内に収まっているものの、プラント事業者及びプラント周辺の住民視点のプラントシステムに想定されるリスクは、目標とする水準には収まっていない。

プラント事業者やプラント周辺の住民の視点から回復困難性の度合いを低減するためには、あらかじめ実装している安全設備が事故等の発生時に正しく作動することを確かなものとすることに加え、ネットワーク分離等を通じて被害拡大の抑制を図ったり、セキュリティインシデント対応の体制や手順等の整備を行ったりすることが有効と考えられる。これらの対策は、経済的影響の度合いを低減するためにも、有効なものとなる。

したがって、適用主体であるプラント事業者は、これらのプラントシステムがもつリスクを、可能な限り目標とする水準に収めることを目的として、例えば、以下のように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えられる対策等の検討を行うことができると考えられる。

- プラント事業者にとって影響度が大きいリスクに対処するための対策方針
  - 回復困難性の度合いの観点

    プラント事業者にとっては、セキュリティに関するインシデントによって、重大な事故が発生し従業員が死亡することが主要なリスクである。これらのリスクに対応するため以下の対策が有効であると考えられる。
    - セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築
    - 安全設備が事故等の発生時に正しく作動することを確かなものとする対策
  - 経済的影響の度合いの観点

    プラント事業者にとっては、自身が運用するプラントの長時間の稼働停止及び、それに伴う

取引先を含む広範囲にわたるサプライチェーンの途絶等が重要なリスクとなるが、これらのリスクに対応するため以下の対策が有効であると考えられる。

- ✧ 情報システム部門及び製造部門が一体となってセキュリティインシデント対応を行うための体制の構築
- ✧ 信頼性の高いプラントの操業を可能にするための仕組みの構築

- プラント周辺の住民にとって影響度が大きいリスクに対処するための対策方針
  - ➢ 回復困難性の度合いの観点

プラント周辺の住民にとっては、重大な事故が発生し有害物質が流出することによって、周辺の住民に健康被害が生じることが主要なリスクである。これらのリスクに対応するため以下の対策が有効であると考えられる。

- ✧ セキュリティに関するインシデントが発生したとしても周辺環境への影響を最小限に抑える仕組みの構築[36]

  - ➢ 経済的影響の度合いの観点

プラント周辺の住民にとっては、重大な事故によって環境汚染が発生した場合に地域の農林水産業への悪影響が重要なリスクとなるが、これらのリスクに対応するため以下の対策が有効であると考えられる。なお、回復困難性の度合いにおける対策例が経済的影響の度合いの観点においても有効であると考えられる。

- ✧ セキュリティに関するインシデントが発生したとしても周辺環境への影響を最小限に抑える仕組みの構築

上記で示した対策例を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

表 25 影響度が大きいリスクに対処するための対策方針及び
添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
プラント事業者	安全設備が事故等の発生時に正しく作動することを確かなものとする対策	セキュリティ設計と両立するセーフティ設計の仕様化
	情報システム部門及び製造部門が一体となって対応を行うための体制の構築	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		運用中における IoT セキュリティを目的とした体制の確保
	セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築	様々な IoT 機器を接続する際のセキュリティの確保
		適切なネットワークの分離
		インシデント対応手順の整備と実践
	信頼性の高いプラントの操業を可能にするための仕組みの構築	IoT 機器・システムの十分な可用性の確保
		IoT 機器・システムのモニタリング及びログの取得、分析
		IoT 機器・システムに対するアップデートの適用
プラント周辺の住民		セキュリティ設計と両立するセーフティ設計の仕様化

[36] 本稿ではセキュリティ分野に関する法令等を扱うものとする。それ以外の分野（例：安全分野）においては既存の安全基準やガイドラインに従って、対策を行うことが望ましい。

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
	セキュリティに関するインシデントが発生したとしても周辺環境への影響を最小限に抑える仕組みの構築	運用中における法令及び契約上の要求事項の遵守

(3) リスク対応

① システムを構成する機器ごとの脅威の整理

システムを構成する機器・システムごとに想定される脅威(例)は以下の通り。

表 26 想定される脅威(例)

システムを構成する機器	想定される脅威(例)	生じ得るインシデント(例)
製造実行システム (MES:Manufacturing Execution System)	データの改ざん	製造実行システムに保存された稼働情報等が改ざんされる。
	情報漏えい	製造実行システムに保存された稼働情報等が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、製造実行システムに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、製造実行システムがマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員による製造実行システムのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
ヒューマンマシンインターフェース (HMI:Human Machine Interface)	データの改ざん	ヒューマンマシンインターフェースから出された指示情報等が改ざんされる。
	情報漏えい	ヒューマンマシンインターフェースから出された指示情報等が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、ヒューマンマシンインターフェースに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、ヒューマンマシンインターフェースがマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員によるヒューマンマシンインターフェースのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
プロセスサーバ	データの改ざん	プロセスサーバに保存された稼働情報等が改ざんされる。
	情報漏えい	プロセスサーバに保存された稼働情報等が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、プロセスサーバに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、プロセスサーバがマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員によるプロセスサーバのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
データヒストリアン	データの改ざん	データヒストリアンに保存された稼働情報等が改ざんされる。
	情報漏えい	データヒストリアンに保存された稼働情報が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、データヒストリアンに不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、データヒストリアンがマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員によるデータヒストリアンのセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
業務用サーバ/業務用端末	データの改ざん	業務用サーバ/業務用端末に保存されたデータが改ざんされる。
	情報漏えい	業務用サーバ/業務用端末に保存された稼働情報が外部に漏えいする。
	権限の昇格	権限のない従業員が不正にアクセス権限を取得する。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、業務用サーバ/業務用端末に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、業務用サーバ/業務用端末がマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員による業務用サーバ/業務用端末のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
保守用端末	データの改ざん	保守用端末に保存されたデータが改ざんされる。
	情報漏えい	保守用端末に保存された稼働情報が外部に漏えいする。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、保守用端末に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、保守用端末がマルウェアに感染する。
	未知の脆弱性	まだ公知となっていない脆弱性や、新たな攻撃手法による脆弱性を突かれる。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員による保守用端末のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
安全制御 PLC	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、安全制御 PLC に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、安全制御 PLC がマルウェアに感染する。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員による安全制御 PLC のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
プロセス制御 PLC	データの改ざん	プロセス制御 PLC から発信される制御情報が改ざんされる。
	不正アクセス	既知の脆弱性等を悪用することで、悪意のある攻撃者により、プロセス制御 PLC に不正アクセスされる。
	マルウェア感染	外部からの悪意のある攻撃によって、プロセス制御 PLC がマルウェアに感染する。
	利用者によるセキュリティ設定の誤り等	プラント事業者の従業員によるプロセス制御 PLC のセキュリティ設定が、システムインテグレータが想定する方法や内容でなされない。
蒸留塔加熱器	データの改ざん	加熱器に対する制御情報が改ざんされる。
	情報漏えい	加熱器に対する制御情報が漏えいする。
蒸留塔内温度センサ	データの改ざん	センサから発信される温度情報が改ざんされる
	情報漏えい	センサから発信される温度情報が外部に漏えいする。

② 脅威に対する対策の整理

想定される脅威を踏まえ、第 3 軸「求められるセキュリティ・セーフティ要求」における観点ごとにプラント事業者にて実装が想定される対策要件を整理する。

表 27 プラント事業者にて実装が想定される対策要件（例）

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の明確化
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	データの改ざん	ソフトウェアの完全性の検証
		情報漏えい	搭載するソフトウェアに対するインストール対策の実装
		マルウェア感染	マルウェア対策の実施
		全般	IoT 機器・システムの出荷時における安全な初期設定と構成
第 2 の観点	ソシキ・ヒト	全般	サービス提供や管理のポリシーの提示・遵守
		全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		不正利用 不正アクセス	IoT 機器・システムの適正な運用・保守
		全般	IoT 機器・システムの適正な使用
	システム	全般	運用中における法令及び契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		不正利用	IoT 機器・システムに対するアップデートの適用
		不正アクセス	IoT 機器・システムの安全な廃棄又は再利用

③　整理した対策に対する意思決定

対策等を検討する際には、インシデントによる影響の度合いだけでなく、その起こりやすさも踏まえ、システム全体としてのリスクを低減するような対策を検討する。

- 対策の適用対象（どの機器を中心に検討するか）

計画的な停止期間を除いて持続的な稼働が要求され、システム停止が大きな経済的損失に繋がり得る本プラントシステムでは、「可用性」が非常に重視される。セキュリティ対策の実装（例：IDS/IPS の導入、機器に対する更新プログラムの適用）は、そうしたニーズとは相反して、システムの持続的かつ安定した運用に対して往々にしてネガティブな影響を及ぼし得るために、製造部門とリスク管理部門で利害が対立する可能性がある。例えば、リスク管理部門で IDS/IPS の導入を検討している際、ネットワークの「可用性」が損なわれる可能性があるため製造部門が導入に反対する可能性がある。その際には、どちらか一方が意見を押し付けることなく、製造部門とリスク管理部門が対話をしつつ検討することが望ましい。

- 適用する対策の内容（どのように対策を実施するか）

対策一覧より、より効率的・効果的にリスクを低減できるものを中心として対策を検討する。2-3-3 のユースケースと同様にプラントシステムにおいても、情報の機密性よりも可用性や完全性が重視される傾向があり、運用上の制約等も相まって、プロセス制御 PLC 等にエンドポイントセキュリティソフトを導入する等の IT 環境では一般的なセキュリティ対策を実施することが難しいケースがある。その場合には、より上位のシステムで守る構成とすることにより、効率的・効果的にリスクを低減することが望ましい。

なお、本ユースケースでは新たにシステムを導入するのではなく、既存の対象としてリスクアセスメントを行った。以下の対策を優先して実装することとした。

- 運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
- 運用中における IoT セキュリティを目的とした体制の確保
- IoT 機器・システムのモニタリング及びログの取得、分析
- IoT 機器・システムに対するアップデートの適用

上記を踏まえて、プラントシステムがもつリスクを目標とする水準まで収めることを目的として、プラント事業者が実装することとした対策要件の例を以下に示す。

第 1 の観点では、プラント事業者が、プラント事業者やプラント周辺の住民のリスクを抑えることを目的として既存の組織体制やシステムを踏まえて、新たに実装することとした対策要件を整理した。

第 2 の観点では、プラントシステムの運用段階において、物流事業者、プラント周辺の住民のリスクを抑えることを目的として実装することとした対策要件を整理した。

第 3 の観点では、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

第 4 の観点には、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネットの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

1594

表 28 プラント事業者における実際に講じる対策要件（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● 対象となっているプラント施設におけるセキュリティポリシー（例：情報セキュリティ関連規定を含む）の見直し及び、事業部長等の適切な承認権限を有する者の承認 ● 定められた期間ごとの当該ポリシーのレビュー	
2			運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保	● 製造部門及び情報部門が一体となって対応できるようリスク対応組織を立上げ、組織内で統合的にセキュリティ対策を取る体制の構築。 ● プラントにおけるセキュリティ管理責任者の任命。 ※上記の管理責任者及び開発担当者の役割と責任は、プラントシステムのライフサイクルの各段階（例：開発、運用、保守）において明確化されていることが望ましい。	○ （「情報システム部門及び製造部門が一体となって対応を行うための体制の構築」に有効と思われる対策）
3			IoT セキュリティに関するステークホルダーの役割の決定	● プラント施設のセキュリティ対策の設計・開発・運用等における関係各社の責任範囲の明確化。	
4			IoT 機器・システムに係る要員のセキュリティ確保	● 自社内の要員（プラントにて業務に従事する要員）に対する適切な訓練及びセキュリティ教育の徹底。	
5		システム	システムインテグレータに対する搭載するソフトウェアの改ざん検知機能の実装の要求の指示	● システムインテグレータに以下の内容を指示 - MES やプロセス制御 PLC 等のソフトウェアに関する完全性の検証機能の実装	
6			システムインテグレータに対する搭載するソフトウェアに対するインストール対策の実装の指示	● システムインテグレータに以下の内容を指示 - ホワイトリストの作成等を通じて、認可されていないソフトウェアの使用の防止又は検出。	
7			システムインテグレータに対するマルウェア対策の実施の指示	● システムインテグレータに以下の内容を指示 - 各ネットワークを監視する制御システム向けの機器（例：IDS/IPS）の導入	
8			IoT 機器・システムの出荷時における安全な初期設定と構成	● システムインテグレータに以下の内容を指示 - プラントエンジニアリング事業者から提供されたガイドに従ったセンサ等の設置及び設定 - プラントエンジニアリング事業者が想定する仕様に適合したネットワーク環境の整備	
9	第 2 の観点	ソシキ・ヒト	運用中における IoT セキュリティを目的とした体制の確保	● 製造部門及び情報部門が一体となって対応できるようリスク対応組織を立上げ、組織内で統合的にセキュリティ対策を取る体制の維持	
10			過去の対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的なインシデント抑制への活用（同業他社の IoT 機器・システムにおけるセキュリティインシデントを含む）	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
11		プロシージャ	脆弱性対応に必要な手順等の整備と実践	● 脆弱性が明らかになった場合、これらの脆弱性に対応するための体制の整備 ※システムインテグレータ、プラントエンジニアリング事業者及びプラント事業者向けにメンテナンスやサポートを行う事業者と連携しつつ社内体制を整備する ● プラントシステムを構成するソフトウェアの脆弱性が明らかになった場合の、対応手順の整備	
12			IoT 機器・システムの適正な運用・保守	● システムインテグレータ及びプラントエンジニアリング事業者が提示するガイドに従った保守、管理	
13			IoT 機器・システムの適正な使用	● 想定された用途・方法でのプラントシステムの使用	
14		システム	運用中における法令及び契約上の要求事項の遵守	● 情報セキュリティに関連する法的な規制又は契約上の義務に対する違反を避けるための要求事項の特定及び遵守	○ （「情報システム部門及び製造部門が一体となって対応を行うための体制の構築」に有効と思われる対策）
15			継続的な資産管理	● プラントシステムを構成する資産目録（機器上に実装されたソフトウェア及びファームウェア、工場出荷時の設定等を含む）の作成・維持	
16			プログラムソースコード及び関連書類の保護	● プラントシステムに係るプログラムソースコード及び関連書類(例：設計文書)への論理アクセスを最小限にした上で、多要素認証の実施	
17			IoT 機器・システムのモニタリング及びログの取得、分析	● プラントシステムを構成する MES やプロセス制御 PLC を対象にした各種ログ（例：ユーザ認証、ネットワークトラフィック）の取得及び保護 ● 取得したログの安全な入手 ● 取得したログの定期的な分析及び異常の検知	○ （「信頼性の高いプラントの操業を可能にするための仕組みの構築」に有効と思われる対策）
18			IoT 機器・システムに対するアップデートの適用	● 脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定 ● 開発委託先等への修正プログラム等開発の依頼 ● 製造部門と調整を行った上で、提供を受けたセキュリティパッチの適用	○ （「信頼性の高いプラントの操業を可能にするための仕組みの構築」に有効と思われる対策）
19			IoT 機器・システムの安全な廃棄又は再利用	● プラントシステムを構成する機器（例：プロセス制御 PLC や温度センサー等）内部に保存されている情報の削除（読み取り不可処理を含む）	

1595 ● システムインテグレータに対応を依頼すべき対策要件（例）

1596 プラント事業者にて対応が難しいシステムに関する対策は、システムインテグレータに依頼する。シス
1597 テムインテグレータは、プラント事業者によるリスクアセスメントによって追加で必要となった以下の対策
1598 要件を実装するものとする。

表 29 システムインテグレータに対応を依頼すべき対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	搭載するソフトウェアの改ざん検知機能の実装の要求	● MES やプロセス制御 PLC 等のソフトウェアに関する完全性の検証機能の実装。	
2			搭載するソフトウェアに対するインストール対策の実装	● ホワイトリストの作成等を通じて、認可されていないソフトウェアの使用の防止又は検出	
3			マルウェア対策の実施	● 各ネットワークを監視する制御システム向けの機器（例：IDS）の導入	

- プラント事業者向けにメンテナンスやサポートを行う事業者に対応を依頼すべき対策要件（例）

プラント事業者にて対応が難しい対策は、プラント事業者向けにメンテナンスやサポートを行う事業者に依頼する。プラント事業者向けにメンテナンスやサポートを行う事業者は、プラント事業者に対してシステムの保守を行っているため、主に以下の対策要件を実装するものとする。

表 30 プラント事業者向けにメンテナンスやサポートを行う事業者に対応を依頼すべき対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 2 の観点	システム	IoT 機器・システムに対するアップデートの適用（セキュリティパッチの開発・配布等）の指示	● 報告された脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定 ● プラントエンジニアリング事業者や開発委託先等への修正プログラム等開発の依頼 ● プラント事業者へのセキュリティパッチの提供	

2-3-5 工場内のロボットによる部材加工作業（溶接工程）の自動化

輸送機器等の金属部品を設計、加工し、輸送機器メーカ等に提供する製造事業者（以下、金属部品製造事業者）が主たる適用主体となり、自社工場内に新たに導入する部品加工設備を対象にリスクマネジメントを行うユースケースを以下に記載する。

本事業者は、国内に複数の製造拠点を有し、従前より輸送機器メーカ等を主な顧客として、設計や溶接、プレス等の加工を行った上で輸送機器メーカ等に納入しており、顧客からの注文増等の状況に応じて、設計工程における 3D-CAD/CAM の導入や検査工程における各種検査機器の導入等の生産性向上に向けた投資を進めてきた。一方、溶接工程等の製造工程には熟練技術者による手動のプロセスが残り、本事業者としても品質確保や生産能力の維持・向上、技術者の高齢化による人材不足の面で課題があると認識してきたところ、この度、溶接工程の自動化を進めるためにロボットシステムを導入することとなった。

本ユースケースは、実際にロボットシステム及び他の制御システムとの接続部分を導入し、運用する前に、工場内の設備の企画や管理等を担当する生産技術部及び、本社情報システム部門にて、リスク管理を担当する複数の従業員が中心となって対象システム（ロボットシステム及び関連する制御システム）に対するリスクアセスメントを行い、適切なリスク対応策を特定することで、可能な限り、受容しがたいリスクを低減することを目指すものとする。

(1) リスクアセスメント、リスク対応に向けた事前準備

① 対象ソリューションの概要

上述の通り、主に輸送機器メーカ向けに事業を行う金属部品製造事業者が、品質の確保や生産能力の向上、人材不足の解決を目的として、複数の多関節ロボットを含むロボットシステムを導入し、溶接工程の自動化を図っている。溶接加工の対象となるのは、顧客からの要請に基づいて様々な製品種別がある自動車用ボディフレーム等の比較的サイズの大きな部品であり、溶接時に歪を発生させないため左右同時に溶接を行うことが要求される。

従来は少なくとも 2 名の熟練技術者が溶接工程に関わっていたが、システムの導入後は同工程に直接関わる作業要員は不要となり、ロボットの稼働状況等は遠隔から管理される。稼動状況に関するデータは製造元のロボット製造事業者にも提供され、効率的な保守サービスの提供に活用される。

なお、ロボットが稼働するエリアには、労働安全衛生を確保する観点から安全柵やレーザースキャナを設置し、作業員が不用意に立ち入り、不測の事故が発生することを防止している。

- 金属部品製造事業者の工場において、多関節ロボットを含むロボットシステムを導入し、従来の人手による溶接工程を自動化する。
- 加工対象となるのは、自動車用ボディフレーム等の比較的サイズの大きな部品であり、溶接時に歪を発生させないため左右同時溶接が要求される。
- ロボットが稼働するエリアには安全柵やレーザースキャナが設けられており、基本的に作業員は立ち入れない。
- ロボット製造事業者は、ロボットの稼動データを取得、分析し、効率的な保守サービスの提供に活用する。

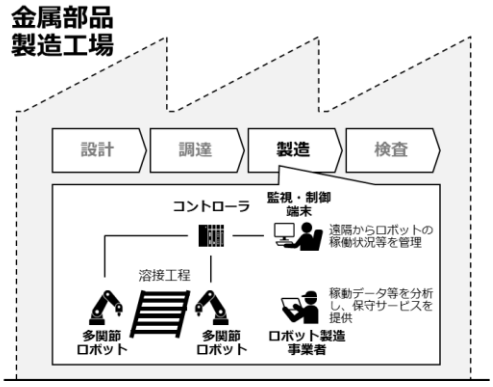


図 33 対象ソリューションの概要

② ステークホルダー関連図

本稿にて関与するステークホルダーとして、「金属部品製造事業者（委託元企業）」「システムインテグレータ（システム開発の委託先企業）」及び「ロボット製造事業者」を想定している。

- 金属部品製造事業者（委託元企業）

輸送機器用の金属部品を製造する事業者であり、自社工場の溶接工程において新たに多関節ロボットを含むロボットシステムの構築（既存システム（SCADA 等）との接続部分も含む）及び、ロボット及び周辺機器のリモート保守サービスの利用を進めようとしている。本ユースエースにおいて、主にセキュリティ対策を検討する主体である。なお、今回リスクアセスメント等の対象となっている同事業者の工場におけるセキュリティ対策等の現状は以下の通り。

- 当該工場は製造機能（工場）だけでなく、本社機能も有している。本社機能として、CIO（最高情報責任者）及び情報システム部門は存在するものの、その所掌範囲は、情報系ネットワークに所在する OA 系システムへの対応に留まっている。工場内の生産設備を所掌する生産技術部ではセキュリティ責任者や担当者が必ずしも明確になっておらず、ロボットシステムを含む制御システムのセキュリティに対する現場の関心は低い。
- 一方で、従業員や設備の安全（セーフティ）確保は重視されており、安全衛生の観点から組織的に労働災害ゼロを目指した活動等が実施されている。
- 情報資産管理台帳やネットワーク構成図は作成されているが、変更があるたびに更新されているわけではなく、内容の一部に現実との相違が存在しており、また、そのことが認識されていない。
- 工場内のネットワークと外部ネットワークや情報系ネットワークとの通信はファイアウォールを通じて必要なものだけに制御されており、その点が現場のセキュリティに対する自信の根拠となっている。ただし、工場内のファイアウォール等のログや設定を定期的に確認するプロセスは整備されていない。
- 工場内には、ID カードを付与された同社又は関係先の従業員のみが入場できるようになっており、監視カメラ等も稼働していることから、外部からの工場内部への物理的な侵入は困難である。
- 自然災害を想定した事業継続計画や、情報漏えいを想定したインシデント対応手順は整備済み。

- システムインテグレータ（システム開発の委託先企業）

金属部品製造事業者との委託契約に基づき、多関節ロボットを組み込んだロボットシステム一式を提供する。

- ロボット製造事業者

多関節ロボットやそれに対応したコントローラ等を製造し、システムインテグレータに提供する。システムの納入後は、金属部品製造事業者に対して、稼働データ等の収集・分析を通じて効率的な運用・保守等（リモートでの状態監視、適宜オンサイトでの保守）を行うサービスを提供する。

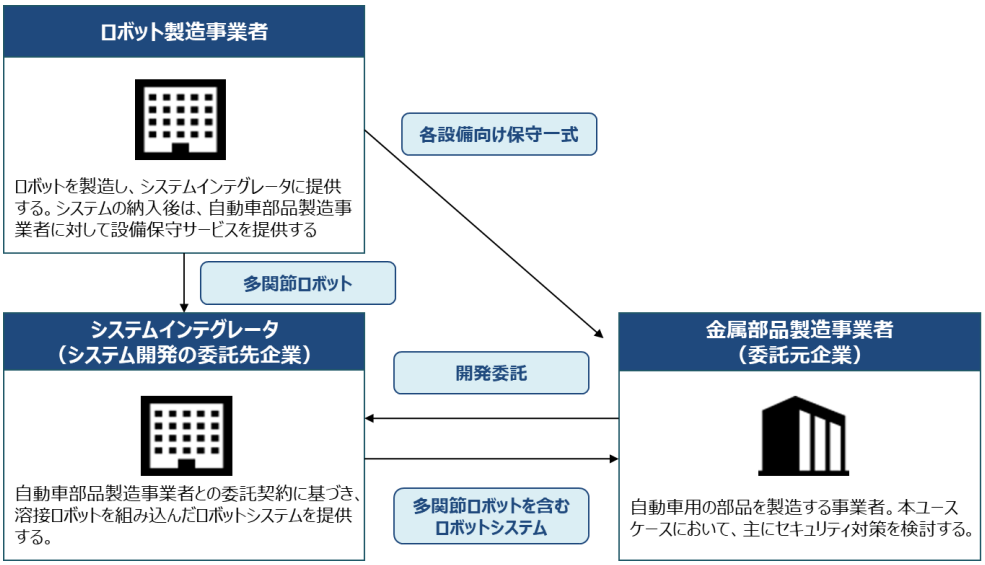


図 34 ステークホルダー関連図

③ システムを構成する機器の一覧

本稿の対象となる機器は以下の通りとする。

表 31 システムを構成する機器の一覧

システムを構成する機器	内容
業務用サーバ/端末	非制御系の情報を保存、利用するサーバ及び端末。例えば、ファイルサーバやメールサーバ及びそれらを利用するサーバ及び端末を指す。
ファイアウォール（FW）	外部ネットワークと工場内のネットワーク、工場内の情報系ネットワークと制御情報ネットワークとの間の通信を論理的に制御するネットワーク機器。
MES サーバ	製造工程の把握や管理、作業者への指示や支援などを行うサーバ。 物理サーバは、工場内のサーバ室に設置するものとする。
SCADA サーバ/端末	ロボットシステムを含む工場内で稼動するシステムの監視及びプロセス制御(制御コマンドの発行等)を行うサーバ及び端末。 SCADA とは、Supervisory Control And Data Acquisition の略称。
エンジニアリング端末	コントローラのプログラム開発及びプログラムの変更等を行うための端末。エンジニアリング用の専用ソフトウェアをインストールしている。
リモートアクセスサーバ/保守用端末（リモート保守システム）	ロボット及び周辺機器の OS やソフトウェアの更新プログラムを開発し、リモートから配信するサーバ及び端末。
コントローラ	プログラムで定められた順序や条件に従い、多関節ロボット及び周辺機器の位置、速度などの動きを制御する装置。 作業場所近くに設置された制御盤に格納されており、作業員が状態を視認、操作できるように操作画面を備えている。
多関節ロボット	アームに 3 つ以上の関節（ジョイント）を持つロボットであり、本ユースケースにおいては金属材料に対する溶接作業を行う。ロボットの可動に必要なビジョンセンサ等の周辺機器も含むこととする。

④ システム構成図、データフロー図

システム構成図は以下の通りとする。本ユースケースでは、金属部品加工工場にて稼働する「ロボットシステム」と、ロボット製造事業者が自社に構築した「リモート保守システム」の2つのシステムを考慮するものとする。ロボットシステムとは、コントローラ及び多関節ロボットを指した上で、他のシステムとの接続部分を含めてリスクアセスメントの対象とする。

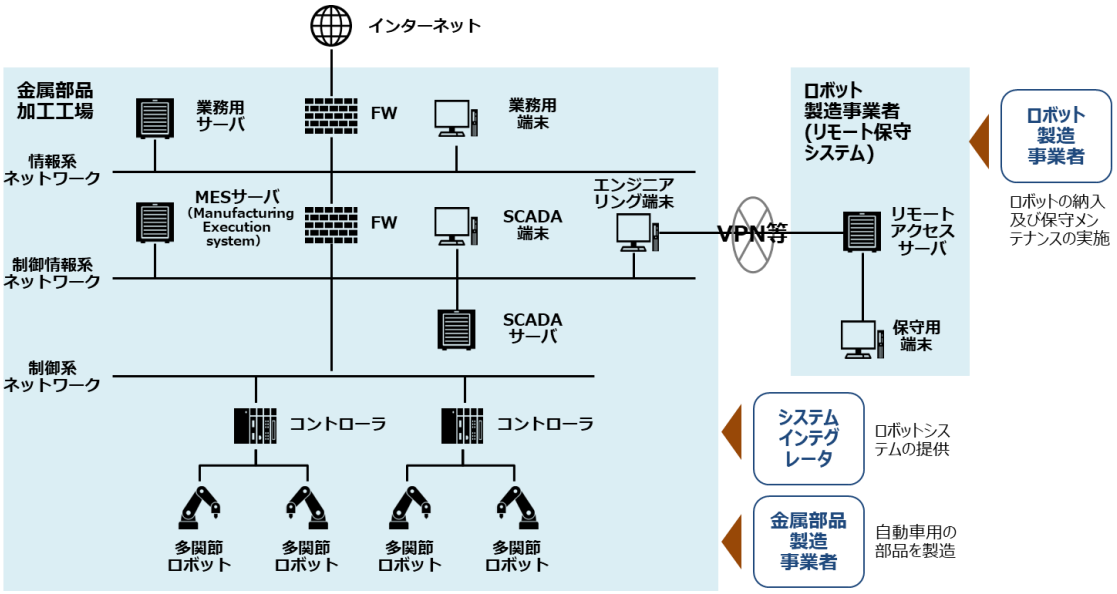


図 35 システム構成図

金属部品製造事業者が、顧客事業者からの発注を受け、設計等の前工程を終えた後に溶接工程を実施する際のデータフロー（一部を抜粋）は以下の通りである。

1. エンジニアリング端末にて制御プログラムを作成し、コントローラにインストールする。
2. ビジョンセンサ等のセンサ類から制御に必要な数値情報を取得し、コントローラに送信する。
3. コントローラが多関節ロボットに制御コマンドを送信する。
4. 多関節ロボットの稼働実績に関するデータが SCADA サーバや MES サーバに送信される。

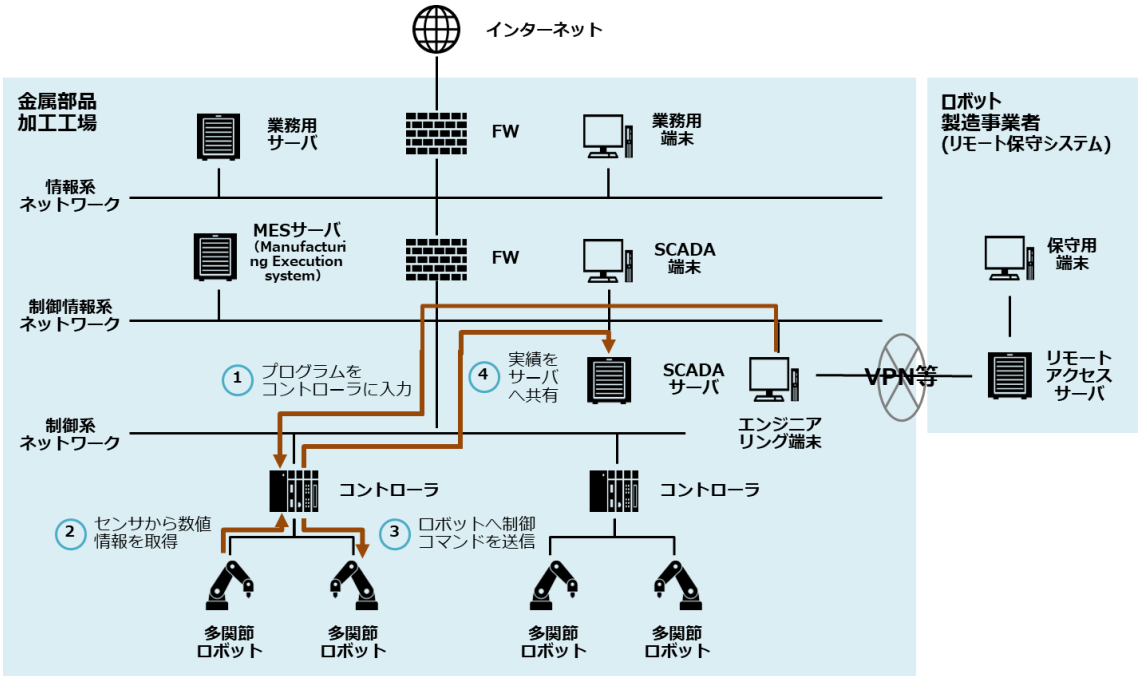


図 36 データフロー図（一部を抜粋）

⑤　リスク基準

適用主体の金属部品製造事業者においては、かねてより SQCD の観点から、それぞれセーフティ（Safety）、品質（Quality）、コスト（Cost）、納期（Delivery）の順に優先順位づけを行い、現場の改善活動等を行ってきた。今回の評価に際しても、それらの優先順位づけと矛盾がないようにリスクに関する意思決定を行う必要があることから、既に社内で策定されている基準を参照することとした。

「回復困難性の度合い」に関連して、社内ではセーフティは他の項目（品質、コスト、納期）よりも優先すべきものとみなされており、安全衛生の観点から組織的に労働災害ゼロを目指した活動等を実施していることから、本ユースケースにおいてもセキュリティ、セーフティの対策を通じて生じ得る被害の度合いを「限定的なダメージ」に抑えることを目指す。

また、同社は、コストや納期を重視しつつも、顧客事業者から見た自社製品の品質を競合他社との主な差別化要因と考えている。よって、設備の停止等による納期遅延やコスト超過以上に、不良品の出荷やそれによる返品、それらにかかる対応コスト等はできる限り避けなければならないと意識されている。上記を踏まえ、本ユースケースでは、「経済的影響の度合い」についても、「回復困難性の度合い」と同様に、「限定的な経済影響」に抑えることを目指すものとする。

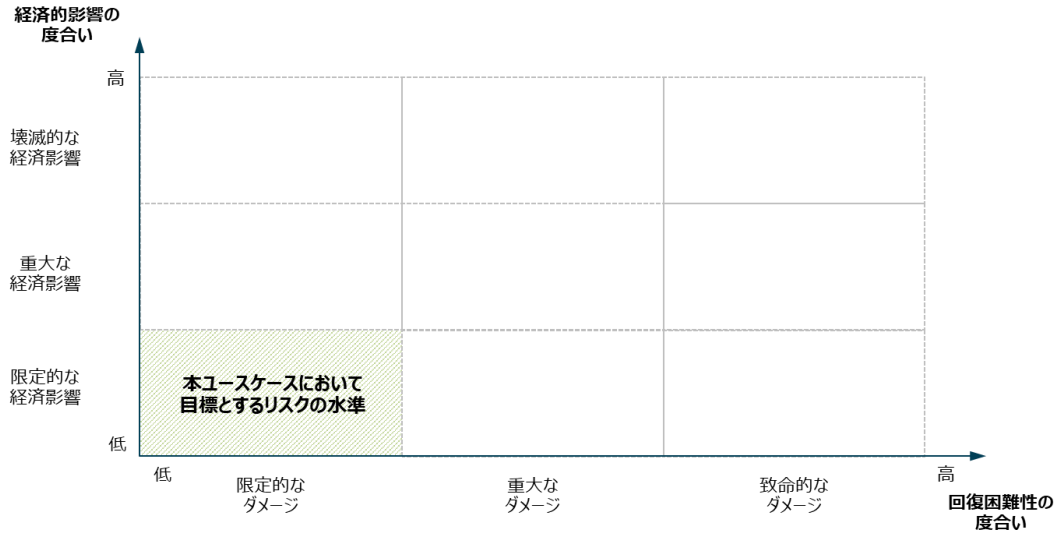


図 37 ロボットシステム及び関連する制御システムにて目標とするリスクの水準

(2)　リスクアセスメント

回復困難性の度合い」及び「経済的影響の度合い」から、プラント制御システムのリスクアセスメントを行う。

①　想定されるセキュリティインシデント等とその結果の特定

対象のロボットシステムにおいて、想定され得るセキュリティインシデント等とその結果（影響）を特定する。対象システムの利用に際して想定されるインシデント（例）は以下の通り。

・　外部に接続している情報系ネットワークを経由して、制御情報系ネットワークに設置された MES サーバや SCADA サーバがマルウェアに感染する。その結果、生産活動が一時的に停止する。
・　リモート保守サービスを受けるために外部ネットワークに接続しているエンジニアリング端末が不正

アクセスされ、コントローラの制御プログラムを改ざんされる。その結果、本来の仕様を満たさない不良品が生産される。

・ 金属部品製造事業者又は保守業務委託先のロボット製造事業者の従業員が、誤って不正な USB 等の外部記憶媒体をエンジニアリング端末に挿入してしまい、同端末及び制御情報系ネットワーク内の他のサーバや端末がマルウェアに感染する。

② ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーそれぞれの立場を考慮し、適用主体である金属部品製造事業者から見て、「ロボットシステム」と「リモート保守システム」に対して、「回復困難性の度合い」「経済的影響の度合い」の観点でリスクアセスメントを行う。

＜ロボットシステムに関連する主なステークホルダー＞

- 金属部品製造事業者
- システムインテグレータ
- ロボット製造事業者

＜リモート保守システム[37]に関連する主なステークホルダー＞

- 金属部品製造事業者

＜ロボットシステム＞

- 金属部品製造事業者

A) 発生したインシデントの影響の回復困難性の度合い

プライバシー及びセーフティの観点を踏まえ、総合的な「回復困難性の度合い」の大きさを評価する。

先に述べたとおり、物理的な不正アクセス等（例：USB 等の外部記憶媒体の接続によるマルウェア感染）により、従業員情報やその他ビジネスに関する情報が外部に漏えいする可能性が指摘されている。ただし、ロボットシステムを構成する制御情報系ネットワークや制御系ネットワークでは、工場の稼働状況や設備に関する情報等の機微なデータを取扱うものの、プライバシーに影響をもたらすような個人情報にあたるデータはほとんど扱われていない。

セーフティの観点では、制御プログラムの改ざん等により生じるロボットの誤動作や停止等が周囲の従業員に影響を及ぼすことが懸念され得るが、稼働するロボットにはあらかじめ安全機能が実装されており、さらに、金属部品製造事業者側では安全衛生確保の観点からロボットの動作環境に安全柵を設け、レーザースキャナにより不適切な侵入を検知できることから、仮にロボットに誤作動が認められた場合であっても従業員等を巻き込んだ事故となる可能性は非常に低いと考えられる。

プライバシーの観点では、従業員の個人情報（氏名、社員番号、所属部署等）が流出する可能性は少なく、セーフティの観点でもロボットの誤動作等は懸念されるものの各種の安全対策により従業員の安全に及ぶ影響は限定的と想定されることから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

[37] 適用主体外部の事業者が管理するシステムをアセスメントにて考慮する場合、当該システムにおけるインシデントが及ぼし得る適用主体への影響を主に考慮することとする。

B)　発生したインシデントの経済的影響の度合い

「経済的影響の度合い」を、直接的な経済影響及び間接的な経済影響に分けて評価する。

そのうち、直接的な経済影響は「内外への直接影響」、「直接影響の継続時間」及び「代替可能性」の観点を考慮して総合的に評価する。

「内外への直接影響（内部）」について、金属部品製造事業者にとっての金銭的な被害につながるものとしては生産設備の停止や不良品の発生、営業秘密の漏えい等が挙げられるが、いずれも事業者の本業に影響し得る重要なリスクである。前述したように、品質確保は事業者において特に重視する観点であり、後の検査工程にて発生した不良品を検出したとしても、一定の業績悪化は避けられないと考えられる。さらに、「内外への直接影響（外部）」としては、顧客となる輸送機器メーカにおいても完成車の納品遅延等の影響が及ぶ可能性があり、影響は内部に留まらない。

また、インシデントの初期対応や原因究明等に係る時間を考慮すれば、インシデント発生後速やかに通常の運用に戻るとは考え難く、「直接影響の継続時間」も無視できないものとなることが想定される。

「代替可能性の観点」では、対象のプロセスは元々人手で行われていたものであり、有事の際には従来の運用に戻すことで、生産能力が低くなるものの、工場の運用は可能であると想定される。

一方で、間接的な経済影響の観点としては、生産停止や不良品の出荷等に伴う顧客との関係悪化（例：取引の縮小）等が懸念される。

よって、セキュリティインシデントの影響が最悪の場合、自社内での損益悪化に留まらず顧客の事業にも影響を及ぼし得る点を考慮し、「経済的影響の度合い」のレベルを「重大な経済影響」と評価する。

- システムインテグレータ

A)　発生したインシデントの影響の回復困難性の度合い

システムインテグレータは本ユースケースにおいて、金属部品製造事業者に対してロボットシステム一式を納品することを役割としており、運用中のロボットシステムにおいてセキュリティインシデントが発生したとしても、必ずしも同社従業員の個人情報が漏えいしたり、機器の誤動作等によりけがを負ったりすることは想定されない。そのため、「回復困難性の度合い」のレベルを「限定的なダメージ」と評価する。

B)　発生したインシデントの経済的影響の度合い

システムインテグレータは対象システムの運用において大きな役割を有さないことを念頭に置けば、運用時に発生するセキュリティインシデントが同社に与える「直接影響」、「直接影響の継続時間」は、限定的なものになると想定される。ただし、金属部品製造事業者に対する注意喚起(例：設定方法に関する説明等)を怠ることによって、サービス提供における過失が認められ得る。その結果として、契約上の責任が問われ得る。

間接的な経済影響としても、同社が設計、開発したロボットシステムにおいてセキュリティに係る仕様の不遵守がないことを前提とすれば、仮に金属部品製造事業者による運用においてインシデントが発生したとしても責任は限定的であると想定される。

よって、「経済的影響の度合い」のレベルを「限定的な経済影響」と評価する。

- ロボット製造事業者

A)　発生したインシデントの影響の回復困難性の度合い

ロボット製造事業者は、本ユースケースにおいて、多関節ロボット及び周辺機器の製造及び保守を行うが、運用中のロボットシステムにおいてセキュリティインシデントが発生した場合であっても、必ずしも同社従業員の個人情報が漏えいしたり、機器の誤動作等により従業員がけがを負ったりすることは想定されない。そのため、「回復困難性の度合い」のレベルを「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

ロボット製造事業者にとって、経済的な影響の観点から大きな問題となり得るのは、提供しているロボット又はコントローラ等の周辺機器に何らかの重大な（セキュリティ上の）欠陥が存在しており、製品回収等に発展する場合と考えられる。この点については事例等も多いわけではなく、特にサイバーセキュリティを念頭に置いた場合にどこまでが製造者側の責任かという範囲を特定することが困難な側面もあるが、「内外への直接影響」としては、大規模な製品回収が発生するリスクの顕在化も否定できない。そのような背景から、必ずしも判断が容易ではない部分は残るが、将来的な問題の顕在化に備え、「経済的影響の度合い」のレベルを「重大な経済影響」と評価する。

＜リモート保守システム＞

- 金属部品製造事業者

A） 発生したインシデントの影響の回復困難性の度合い

ロボットシステムを運用する金属部品製造事業者にとって、外部ネットワークとは論理的に分離した形で構築している制御情報系ネットワーク、制御系ネットワークに対して外部からのアクセスを許可することには、一定の不正アクセスやマルウェア感染等のリスクが伴う。

しかしながら、既に「ロボットシステム」に関する評価で述べたように、仮にかかるセキュリティ上の脅威が顕在化した場合であっても、一定の前提（ロボット稼働範囲における安全柵の設置等）を置けば、プライバシーの観点とセーフティの観点のそれぞれについて、「回復困難性の度合い」のレベルを「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

事前の対策が十分ではなかった結果として、ロボット製造事業者が管理するリモート保守システム、及び当該システムと金属部品製造事業者の内部ネットワークの境界が攻撃の侵入口として機能してしまう場合は、外部から保護すべき制御情報系ネットワーク、制御系ネットワークへ不正アクセスされるおそれがあり、ロボットシステムと同じく、セキュリティインシデントの発生により、自社に留まらず顧客の事業にも影響を及ぼし得る。そのため、適用主体である金属部品製造事業者以外の事業者が管理するシステムではあるが、「経済的影響の度合い」のレベルを「重大な経済影響」と評価する。

③ マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 1 軸「回復困難性の度合い」及び第 2 軸「経済的影響の度合い」からカテゴライズし、マッピングする。

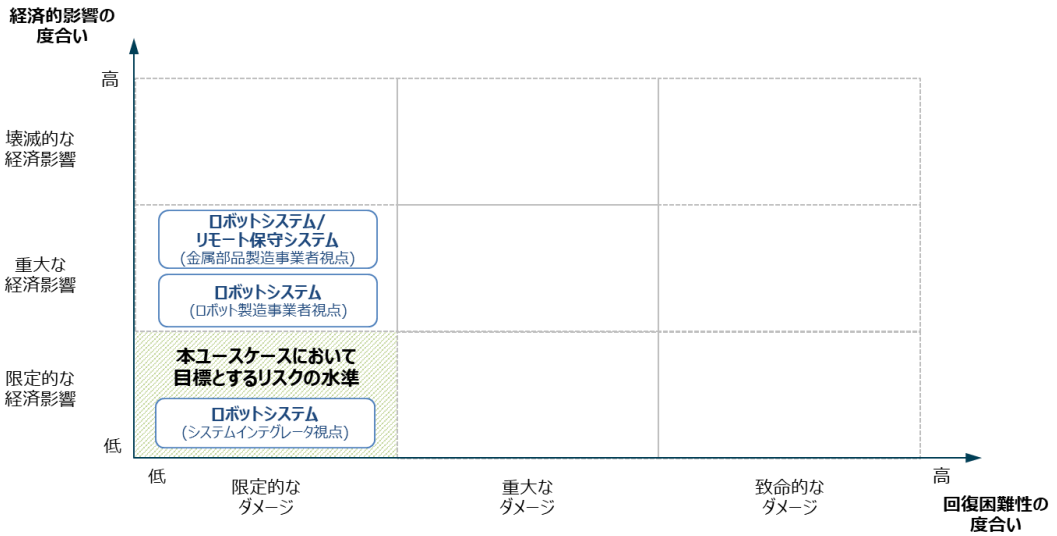


図 38 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

上記で検討した各システム/ステークホルダーごとに想定される被害の程度と(1)⑤において規定したリスク基準を比較すると、金属部品製造事業者から見たロボットシステム及びリモート保守システムの「経済的影響の度合い」、ロボット製造事業者から見たロボットシステムの「経済的影響の度合い」は目標とするリスクの水準に収まっていない。

金属部品製造事業者にとっては、品質、コスト、納期に対する悪影響(例:不良品の増加、製造にかかるコストの増大、納品の遅延)を及ぼし得る脅威が特に優先的に対処すべきものであり、中でも品質の観点を重視している。一方でロボット製造事業者にとっては、提供しているロボット又はコントローラ等の周辺機器における重大な(セキュリティ上の)欠陥及びそれに起因する製品回収等が重大なリスクと考えられる。適用主体の金属部品製造事業者にとっても利用機器のセキュリティ上の欠陥は避けるべきものであることから、金属部品製造事業者からの要請、又はロボット製造事業者の自主的な取組み等に基づき、何らかの対処(セキュリティ基準の遵守確認等)を講じることが望ましい。

以上を踏まえると、適用主体である金属部品製造事業者は、対象のシステムにて想定されるリスクを可能な限り目標とする水準に収めるために、例えば、以下のように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えられる対策等の検討を行うことができると考えられる。

- 金属部品製造事業者にとって影響度が大きいリスクに対処するための対策方針
  - 経済的影響の度合いの観点
    運用時におけるロボット及びその制御に必要な設備(制御プログラムを含む)の信頼性をより確かなものとして、製品の品質、次いでロボット等の製造設備の可用性に影響を及ぼすような脅威を低減する対策が有効であると考えられる。
    - ロボットの制御に関わる設備(例:コントローラ、エンジニアリング端末、SCADA)の保護
    - リモート保守システムからのアクセスの保護

- ロボット製造事業者にとって影響度が大きいリスクに対処するための対策方針

➢ 経済的影響の度合いの観点

運用時におけるサポートに加え、ロボットや周辺機器の設計、開発の段階からセキュリティを十分に考慮し、あらかじめ脅威に対処しておくことで、長期にわたり利用されることが想定される機器においても一定のセキュリティを確保し、ロボット製造事業者とユーザ事業者（金属部品製造事業者を含む）のリスク低減に資することができる。

✧ セキュアなロボット及び周辺機器（コントローラ等）の調達/提供

✧ 十分な期間のサポート契約締結

上記で示した対策例を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

表 32 影響度が大きいリスクに対処するための対策方針及び添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
金属部品製造事業者にとっての「経済的影響の度合い」を低減するための対策	ロボットの制御に関わる設備の保護	適切な水準のアクセス制御の実装
		ソフトウェアのインストールの制限
		IoT 機器・システムにおける運用開始時の正しい設置、設定
	リモート保守システムからのアクセスの保護	適切な水準のアクセス制御の実装
		IoT 機器・システムの適正な運用・保守
		暗号化によるデータの保護（通信経路の保護等）
		ソフトウェアの完全性の検証
ロボット製造事業者に由来する「経済的影響の度合い」を低減するための対策	セキュアなロボット及び周辺機器の調達/提供	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化（ロボット製造事業者において適切に実施されていることが調達前に確認されるべき対策）
	十分な期間のサポート契約締結	IoT 機器・システムに対するアップデートの適用

(3) リスク対応

① システムを構成する機器ごとの脅威の整理

システムを構成する機器・システムごとに想定される脅威（例）は以下の通り。業務用サーバ/端末における一部の脅威を除き、これらの多くは制御プログラムの書き換えやコマンドの不正発行、マルウェア感染による操業の停止等につながり得る影響の大きいものとなっている。

表 33 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
業務用サーバ/端末	データの改ざん・消去	標的型メール攻撃等を通じて外部からの不正侵入を受け、業務用サーバ/端末に格納されているデータが改ざん又は消去される。
	情報漏えい	標的型メール攻撃等を通じて外部からの不正侵入を受け、業務用サーバ/端末に格納されているデータが漏えいする。
	踏み台	マルウェアに感染した業務用サーバ/端末を踏み台にして、顧客のシステムに不正アクセスを試みたり、工場内ネットワークの調査等に悪用されたりする。
MES サーバ	なりすまし	MES サーバの管理者になりすまされ、生産計画、生産実績等の重要データに不正アクセスされる。
	マルウェア感染	MES サーバが情報系ネットワークを経由して受信したランサムウェアに感染し、製造ラインに対する指示が滞る。
SCADA サーバ/端末	不正アクセス	SCADA 製品の脆弱性を悪用し、同サーバへ不正ログインしたうえで、不正な制御プログラムを作成し、実行させる。
	マルウェア感染	SCADA サーバ/端末がマルウェアに感染し、製造現場の情報を遠隔から正確に把握することができなくなる。

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
エンジニアリング端末	不正アクセス	アクセス制御の実装が不十分であるために、エンジニアリング端末が外部からの不正アクセスを受け、制御情報系ネットワーク/制御ネットワークの調査等に悪用される。
	マルウェア感染	エンジニアリング端末に不正な USB メモリが挿入され、端末がマルウェアに感染し、外部からの不正操作を受ける。
リモートアクセスサーバ/保守用端末（リモート保守システム）	不正アクセス	リモートアクセスサーバ/保守用端末に外部から不正アクセスされ、保守サービス利用者向けの更新プログラムに不正なプログラムを混入される。
	不正改造	リモートアクセスサーバ/保守用端末に外部から不正アクセスされ、ロボットシステムの構成や稼働状況等の保守サービス利用者のデータが漏えいする。
コントローラ	情報漏えい	機器外からのアクセスに対して認証が設定されていない、又はエンジニアリング端末がマルウェアに感染している等の原因で、コントローラに外部化から不正にアクセスされ、プログラムや動作設定データ等が漏えいする。
	不正利用	エンジニアリング端末や制御盤の操作画面が不正操作され、コントローラが処理する制御プログラムや設定が変更される。
多関節ロボット	不正利用	制御プログラムの改ざんや不正な制御コマンドの発行等を通じて、多関節ロボットが予期せぬ動作を行い、周辺設備への危害や、製品の品質低下等が発生する。

② 脅威に対する対策の整理

想定される脅威を踏まえ、第 3 軸「求められるセキュリティ・セーフティ要求」における観点ごとに金属部品製造事業者にて実装が想定される対策要件を整理する。

表 34 金属部品製造事業者にて実装が想定される対策要件（例）

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
			IoT セキュリティに関するステークホルダーの役割の明確化
			IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		なりすまし 不正アクセス	適切な水準のアクセス制御の実装
		マルウェア感染	ソフトウェアの完全性の検証
		マルウェア感染	ソフトウェアのインストールの制限
		なりすまし 情報漏えい	暗号化によるデータの保護
		なりすまし 情報漏えい	ライフサイクルを通じた暗号鍵の管理
		マルウェア感染	マルウェア対策の実施
		不正アクセス	適切なネットワークの分離
		不正利用	セキュリティ設計と両立するセーフティ設計の仕様化
		全般	セキュアな開発環境と開発手法の適用
		全般	IoT 機器・システムにおけるセキュリティ機能の検証
		全般	信頼できる IoT 機器やサービスの選定
		全般	IoT 機器・システムにおける運用開始時の正しい設置、設定
第 2 の観点	ソシキ・ヒト	全般	運用中における IoT セキュリティを目的とした体制の確保
			過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		全般	インシデント対応手順の整備と実践
		全般	事業継続計画の策定と実践
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令及び契約上の要求事項の遵守
		全般	継続的な資産管理
		全般	IoT 機器・システムのモニタリング及びログの取得、分析
		マルウェア感染	IoT 機器・システムに対するアップデートの適用

③　整理した対策に対する意思決定

対策等を検討する際には、インシデントによる影響の度合いだけでなく、その起こりやすさも踏まえ、システム全体としてのリスクを低減するような対策を検討する。

- 対策の適用対象（どの機器を中心に検討するか）

金属部品製造事業者にとって、自社製品の品質や工場の事業継続こそが守るべき価値であり、それらに対して強い影響を及ぼし得る機器には十分な保護が必要と考えられる。

セキュリティの観点では、製品の品質低下（不良品の増加等）は、制御プログラムや設定の改ざん、制御コマンドの改ざん、不正発行等によりロボットが適切でない制御を実行することで生じ得る。かかるインシデントに関係し得る金属部品製造事業者の資産として以下が挙げられる。

- コントローラ：プログラムや設定の改ざんを通じて、適切でない制御を実行させる可能性がある。
- エンジニアリング端末：コントローラに不正なプログラムや設定を入力される可能性がある。
- SCADA 端末/サーバ：管理者権限を奪われた場合等に制御コマンドの不正発行が実行される可能性がある。
- FW：通信制御の設定を誤ったり、改ざんされたりすることによって、避けるべきセキュリティインシデントをまねく脆弱性を拡大させ得る。

また、適用主体外部のシステムではあるが、「リモート保守システム」及び工場内システムとの間のネットワークについてもエンジニアリング端末等につながるものとして一定のセキュリティ対策を要求することが有効と考えられる。

これらの機器では上記以外の機器と比較して相対的にセキュリティ対策の意義が大きい一方で、製造現場の運用に対してネガティブな影響を及ぼし得るために、工場内部の部門から対策強化に異論が生じる可能性がある。その際には、生産技術部等においてセキュリティ対策に責任を持つ者が、各部門と継続的にコミュニケーションをとりつつ、対策の範囲や内容について意見をくみ取り、合意を得ていくことが望ましい。

- 適用する対策の内容（どのように対策を実施するか）

(1)②にて述べた適用主体における対策の現状を踏まえると、セキュリティに責任のある従業員が不明確な状況では今後の対策推進もままならないと考えられることから、まずは第 1 の観点として、組織内部で「セキュリティを目的とした体制の確保」を進め、ロボットシステムを含む工場内のシステムに係る責任者及び担当者とそれらが負う責任を明確にすることが望ましい。

今回はロボットシステムを溶接工程に新たに導入することから、以降の段階におけるセキュリティ投資のコストを効率化することも目指し、上記で定めた責任者等が中心となり、「企画・設計段階におけるセキュリティ要求事項の分析及び仕様化」を行い、「適切な水準のアクセス制御の実装」や「ソフトウェアのインストールの制限」等の基本的なセキュリティ要求事項を明確化し、システムインテグレータへの発注の際に提示できるようにしておくことが望ましい。システムの運用段階で新たにセキュリティ対策を追加することには困難も想定されることから、設計、開発段階でこれらの要求事項が明確にされていることが重要である。

かかる対策は、前述したように、コントローラ、エンジニアリング端末、SCADA 端末/サーバの機能を、

プログラムの改ざんや不正アクセス等の脅威から保護するものとすべきである。一方で、セキュリティ対策の実装が本来求められる稼動に悪影響を及ぼすことを避けることが求められるため、実際の実施内容はそれらのバランスをとった内容となっていることが望ましい。

ロボットシステムの運用中は第 2 の観点のうち、基礎的な対策として「継続的な資産管理」を行うとともに、必要に応じて「IoT 機器・システムに対するアップデートの適用」がなされるべきである。この点については、ロボット及び周辺機器の保守業務を担うロボット製造事業者の支援を受けつつ、セキュリティ責任者/担当者が製造部門と十分に調整のうえ実施することが望まれる。その際、ロボット製造事業者が管理するリモート保守システムにおいて、不正アクセス対策等の一定のセキュリティ対策の実装を求めることも想定される。

第 3 の観点については、本ユースケースに登場する業務及びシステムの安全な運用において特別な資格等が必要なケースは必ずしも想定されないと考えられることから、これらに該当する対策要件は実装しないこととした。

さらに、第 4 の観点としても、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネットの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。

表 35 金属部品製造事業者における実際に講じる対策要件（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● ロボットシステムを含む工場システムにおけるセキュリティポリシーを策定し、従業員や他の関係者への周知を実施 ● 策定したセキュリティポリシーについて、関係者にて少なくとも1年に1度レビューを実施	
2			運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保	● ロボットシステムを含む工場内のシステムの企画・設計、開発段階におけるセキュリティに係る責任者及び担当者、それらの責任の明確化 ● 本社情報システム部門との連携の確立、役割分担の明確化	
3			IoT セキュリティに関するステークホルダーの役割の明確化	● 対象ロボットシステムのセキュリティ対策実施に係るステークホルダー（例：自社の他に、システムインテグレータ、ロボット製造事業者）を特定し、設計・開発における責任範囲を明確化	
4		システム	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	● 本社情報システム部門のセキュリティ担当者と工場内のセキュリティ担当者が中心となり、ロボットシステムの企画・設計時においてリスクアセスメントを実施し、セキュリティ要件を特定、要件実装に係る費用を確保 ● 特定したセキュリティ要求事項をロボットシステムの委託仕様書へ記載	○ （「セキュアなロボット及び周辺機器の調達/提供」に有効と考えられる対策）
5 6	第 2 の観点	ソシキ・ヒト	運用中における IoT セキュリティを目的とした体制の確保	● ロボットシステムを含む工場内のシステムの運用段階におけるセキュリティに係る責任者及び担当者、それらの責任の明確化 ● 本社情報システム部門との連携の確立、役割分担の明確化	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
7		プロシージャ	事業継続計画の策定と実践	● 本社情報システム部門のセキュリティ担当者と工場内のセキュリティ担当者が既存の事業継続計画をレビューし、ロボットシステム等の工場システムの故障や停止による影響等が十分に考慮されているかを確認する。	
9			IoT 機器・システムの適正な使用	● ロボット製造事業者又はシステムインテグレータから提供される機器・システムの運用手順に沿って、機器・システムを設定し、利用	
10		システム	継続的な資産管理	● 工場内のネットワークに接続している機器（サーバ、端末、ネットワーク機器、その他の設備）の管理台帳を作成し、適時に反映を実施 ● 必ずしも常時工場内のネットワークにつながっているわけではないモバイル機器（例：タブレット端末、スマートフォン、ハンディ端末）や可搬媒体（例：USB メモリ、DVD/CD）の持ち込み、持ち出し、利用状況等の厳重な管理を実施	
11			プログラムソースコード及び関連書類の保護	● ロボットシステムに関するプログラムソースコード及び関連書類（例：設計書、仕様書）へのアクセスや変更履歴（例：作成日時、変更日時、変更点）について、開発要員によるアクセスを最小限にする、アクセスログを取得する等の方法で、厳重な管理を実施	
12			IoT 機器・システムのモニタリング及びログの取得、分析	● ロボットシステムを構成する以下の機器等からログを収集しておき、定期的に、あるいは異常検知時に分析を実施 – 工場システム内2か所に設置した FW の通信ログ – SCADA 端末/サーバ、エンジニアリング端末、MES サーバへの操作ログやアクセスログ（保守用のリモートアクセスを含む）	
13			IoT 機器・システムに対するアップデートの適用	● ロボット及び周辺機器に関して、ロボット製造事業者と十分な期間の保守契約を締結する。 ● セキュリティアップデートを含むソフトウェアやファームウェアの更新を、以下のような措置を通じて不正アクセス等から保護したうえで実施 – 自社の担当者又は保守を担当するロボット製造事業者から提供されたことが確かなプログラムを適用 – 更新をネットワーク経由で遠隔から行う場合、通信経路を適切な方式により暗号化 – 更新実行前にあらかじめ動作検証等を実施	○ （「十分な期間のサポート契約締結」に有効と考えられる対策）

1916 ● 委託仕様書に基づきシステムインテグレータが実装する対策（例）

1917 ロボットシステムの開発業務を行うシステムインテグレータへの委託仕様書等に基づいて、システムイ

1918 ンテグレータは主に以下の対策要件を実装するものとする。

1919 表 36 システムインテグレータに対応を依頼すべき対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	適切な水準のアクセス制御の実装	● 設備等の設置エリアに至るまでに物理セキュリティ対策が講じられているという前提のもと、SCADA 端末/サーバやエンジニアリング端末等の操作を許可する前に、操作者に対する ID、パスワードによる認証の要求 ● エンジニアリング端末等からコントローラへの接続を行う際、端末 ID 及びパスワードによる認証 ● 従業員及び関連会社の職員に対しては、各々の職務に応じて最小限の権限のみの付与	○ （「ロボットの制御に関わる設備の保護」に有効と考えられる対策）
2			ソフトウェアのインストールの制限	● エンジニアリング端末や SCADA 等のロボットシステムを構成する機器において、起動を許可するソフトウェアやプロセスを定めたホワイトリストの作成、及びリストに掲載されていないもののインストールや起動の防止	○ （「ロボットの制御に関わる設備の保護」に有効と考えられる対策）
3			マルウェア対策の実施	● ロボットシステムを構成する機器において、USB メモリ等の外部記憶媒体を接続する際、登録されたもののみを利用できるようにしたうえで、事前にセキュリティスキャンの実施 ● 制御情報系ネットワークにおいて侵入検知システム（IDS/IPS）を導入し、ロボットシステムを構成する機器の脆弱性を突いた攻撃の検知・遮断 ● ロボットシステムを構成する機器において重大な脆弱性が発見された際に、サポート切れや運用上の問題でパッチ適用が困難な場合、仮想パッチとして機能させることを目的とした IDS/IPS の設定	
5			適切なネットワークの分離	● ロボットシステムを構成する機器は、既に運用されている制御情報系ネットワーク及び制御系ネットワーク内で稼動するように開発し、当該ネットワーク内外での通信を必要最小限にするよう FW 等の設定	
6			セキュリティ設計と両立するセーフティ設計の仕様化	● ロボットシステムにおいて、不正操作、誤操作、誤動作、異常発生時に設備、装置、システム、機器等を安全な方向に導くフェールセーフの仕組みの導入 ● 無関係な従業員等が無断で立ち入れないようにすることを目的として、ロボットが稼働するエリアの周辺に安全柵の設置	
7			セキュアな開発環境と開発手法の適用	● ロボットシステムの開発環境を、本番環境を含む他の環境と分離し、当該環境に対するアクセスの制限 ● 開発環境の変更及び、保管されたコードに対する変更の継続的な監視	
8			IoT 機器・システムにおけるセキュリティ機能の検証	● 開発したロボットシステムに対して、ペネトレーションテストを実施し、侵入に使用できる攻撃手法や脆弱性の特定及び、対処	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
			IoT 機器・システムの出荷時における安全な初期設定と構成	● 運用前の段階で利用しないと考えられる、ロボットシステムを構成する機器のネットワークポート、USB やシリアルポートの物理的又は論理的な閉塞 ● ロボットシステムを構成する機器において運用前の段階で不要と考えられるアプリケーション、機能がある場合、運用開始までの削除、無効化、停止	
10			IoT 機器・システムにおける運用開始時の正しい設置、設定	● ロボットシステムを構成する設備を設置、設定する際、機器の動作仕様を考慮しつつ、運用開始までに動作状況の確認	○ （「ロボットの制御に関わる設備の保護」に有効と考えられる対策）

1920 ● ロボット製造事業者に対応を依頼すべき対策要件（例）

1921 ロボット及び周辺機器の保守業務を行うロボット製造事業者に対して、保守業務に係る契約書の条項
1922 等に基づいて、例えば以下の対策要件の実装を求めるものとする。

1923 表 37 ロボット製造事業者に対応を依頼すべき対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	暗号化によるデータの保護	● 遠隔からの監視や保守に用いる通信経路を適切な方式（例：IPsec）により暗号化	
2			ライフサイクルを通じた暗号鍵の管理	● 利用開始後、一定の期間を経過した暗号鍵や一定の回数使用した暗号鍵の更新を実施 ● 暗号鍵の危殆化が発覚した場合、漏えいした暗号鍵の不正利用を防止するため、速やかに暗号鍵の更新を実施	
3	第 2 の観点	ソシキ・ヒト	利用者へのリスクの周知等の情報発信	● ロボット及び周辺機器の運用手順において、提供機器の正しい利用方法や保守契約の期間や内容、利用者側で実施すべき事項等を発信 ● 上記製品に何らかの重大な脆弱性が発見された場合に、推奨策とともに金属部品製造事業者へ注意喚起を実施	
4		プロシージャ	IoT 機器・システムの適正な運用・保守	● 提供するロボット及び周辺機器の運用手順（取扱方法等を含む）を文書化し、金属部品製造事業者に提供 ● ロボット及び周辺機器に係る保守の実施手順を明確にするか、あるいは金属部品製造事業者から受領し、当該手順に沿って保守業務を実行	○ （「リモート保守システムからのアクセスの保護」に有効と考えられる対策）
5		システム	運用中における法令及び契約上の要求事項の遵守	● 保守契約にて規定された業務の実施方法やその他の要求事項（セキュリティ規定を含む）を認識し、確実な遵守	
6			プログラムソースコード及び関連書類の保護	● ロボットシステムに関するプログラムソースコード及び関連書類（例：設計書、仕様書）へのアクセスや変更履歴（例：作成日時、変更日時、変更点）について、開発要員によるアクセスを最小限にする、アクセスログを取得する等の方法で、厳重な管理を実施	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
7			IoT 機器・システムに対するアップデートの適用	● セキュリティアップデートを含むソフトウェアやファームウェアの更新を、以下のような措置を通じて不正アクセス等から保護したうえで実施 – リモートアクセスを行う際、担当者に多要素認証の実施 – 更新をネットワーク経由で遠隔から行う場合、通信経路を適切な方式による暗号化	○ （「リモート保守システムからのアクセスの保護」に有効と考えられる対策）

1924

2-3-6 金属製造現場の温度センサ等による製造設備の状態監視

(1) リスクアセスメント、リスク対応に向けた事前準備

本項では、IoT 機器・システムを通じて提供されるサービスの開発者又は提供者である製造事業者向けにメンテナンスやサポートを行う事業者（以下、「サポート事業者」という。）が IoT-SSF の主たる適用主体となってリスクアセスメント等を行うユースケースを記載する。

サポート事業者は、工場の設備等に設置した各種センサから得たデータに基づいて稼働情報を可視化することで、各設備・機器の状態を常時監視するサービスを企画している。サービスの提供を受ける事業者（以下、「ユーザ事業者」という。）は、当該サービスの導入によって、既存設備の設備管理業務の一部を外部に委託することが可能となるとともに、安定的に高品質の製品を製造することが可能となる。

サポート事業者は、今後のシステム構築、サービスの提供開始及び将来のサービス展開を見据え、新たに生じ得るサイバーセキュリティに関するリスクを懸念しており、この度、ユーザ事業者を設定し、リスクアセスメント及びリスク対応を実施することとした。

本ユースケースでは、サポート事業者がサービスの提供開始前に行ったリスクアセスメント及びリスク対応の結果、残存するリスクに対しては、ユーザ事業者に脆弱性対応等を依頼することで、可能な限り、受容しがたいリスクを低減させることとする。

① 対象ソリューションの概要

本ユースケースでは、サポート事業者のソリューションに加え、ユーザ事業者の対象業務も明示した。本ユースケースでは、具体的なユーザ事業者を金属製品製造事業者とした。

- サポート事業者

サポート事業者は、工場の各設備に設置された各種 IoT 機器を通じて、稼働情報等を常時収集するとともに、収集した情報が適切な範囲に収まっているかを示すレポートを提供するものとする。また、各設備の保守業務も請け負うこととし、もし設備の異常を検知した場合には、管理者にメール等で通知するとともに、即座に現場に駆け付けることを想定している。

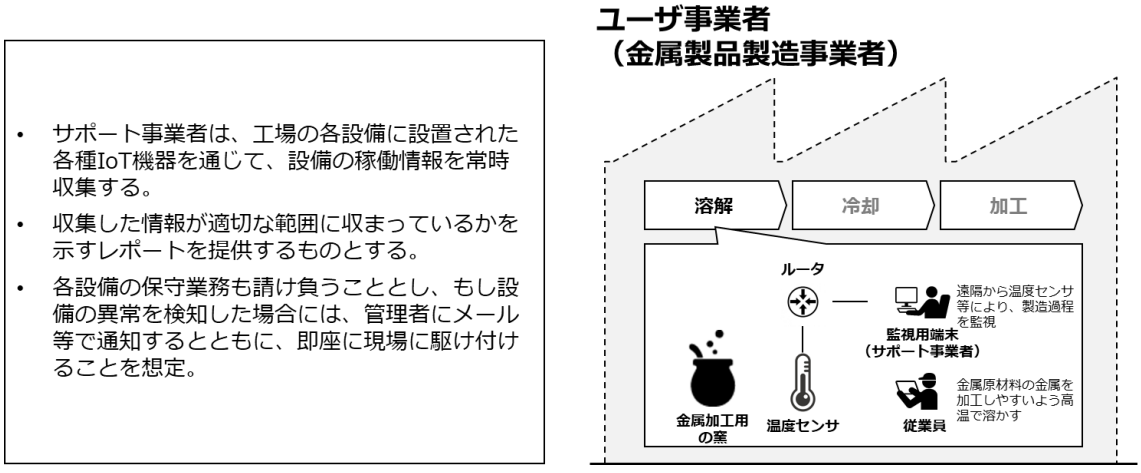


図 39 対象ソリューションの概要

- ユーザ事業者（金属製品製造事業者）

ユーザ事業者（金属製品製造事業者）の工場内で対象とする業務内容を整理する。

ユーザ事業者（金属製品製造事業者）の工場では以下の 3 つの作業を行っており、本ユースケースでは、既にサポート事業者の関連会社が設備を導入している 1 の溶解作業で使用する窯に各種センサを設置する。これらの窯は非防爆エリアに配置されており、フェールセーフの機能が備わっているものとする。

1. 溶解作業：原材料の金属を加工しやすいよう高温で溶かす作業
2. 加工作業：溶かした金属を型に流し込み加工する作業
3. 冷却作業：型に流し込んだ金属を冷却する作業

今回、新たに導入する温度センサ、重量センサ及び振動センサによって、温度情報や重量情報を含む設備の稼働情報が可視化されることを想定している。

なお、ユーザ事業者では、既に導入している生産制御システム等とサポート事業者が提供する各種センサや情報収集サーバからなる状態監視システムとは接続しない前提とする。

② ステークホルダー関連図

本稿にて関与するステークホルダーは、「サポート事業者」、「センサ製造事業者」及び「ユーザ事業者（金属製品製造事業者）」を想定する。

- サポート事業者

既存の工場の設備に対して、新たに温度センサ、重量センサ及び振動センサ等を導入し、設備の状況をリアルタイムで監視するサービスを提供する事業者である。また、設備の運用保守を行い、故障などの際には現場に駆け付けることを想定している。セキュリティ対策等の実施に対して主に責任を有する事業者である。

- センサ製造事業者

製造設備の温度センサ、重量センサ及び振動センサ等をサポート事業者に提供する事業者である。

- ユーザ事業者(金属製品製造事業者)

サポート事業者が設定したサービスの提供を想定する事業者であり、既に稼働している工場で金属製品を製造する事業者を想定する。

また、ユーザ事業者（金属製品製造事業者）では既に以下の対策は既に実施済みである。

- IoT 機器・システムの設置場所等に対する物理的アクセスの制御
- IoT 機器システムの構成要素（機器、ネットワーク等）の物理的保護

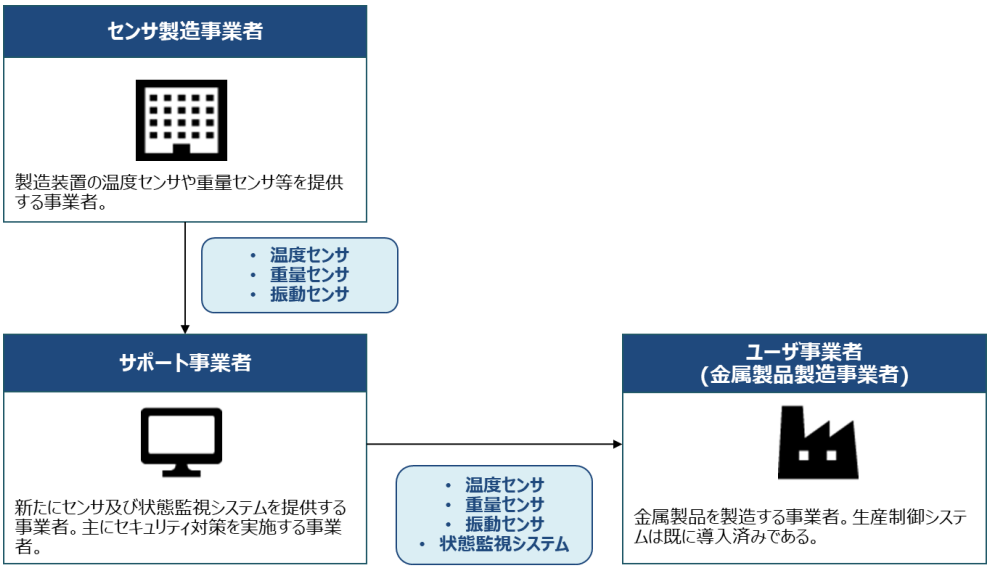


図 40 ステークホルダー関連図

③ システムを構成する機器の一覧

本稿の対象となる機器は以下の通りとする。

表 38 システムを構成する機器の一覧

システムを構成する機器	内容
情報収集サーバ	温度データ、重量データ、振動データ等を収集するサーバ。 異常が発生した場合には、監視用端末にアラートを出す。 状態監視システムとは、情報収集サーバ及び各種センサを含めたシステムを指す。 情報収集サーバは、サポート事業者内に設置されるものとする。
監視用端末	情報収集サーバのデータを監視し、異常が発生していないかを監視する端末。 監視用端末は、サポート事業者内に設置されるものとする。
ルータ	工場内に設置され、工場内のネットワーク及び工場外のネットワークを中継する通信機器。 ルータは、工場内の各センサやカメラの情報を取得できる位置に設置するものとする。
温度センサ	金属加工用の窯の温度を計測するセンサ。 窯の内部に設置されているものとする。サポート事業者よりリースにて提供される。
重量センサ	金属加工用の窯の重量を計測するセンサ。 窯の外部に設置されているものとする。 サポート事業者よりリースにて提供される。
振動センサ	金属加工用の窯の振動を計測するセンサ。 窯の外部に設置されているものとする。 サポート事業者よりリースにて提供される。

④ システム構成図、データフロー図

システム構成図は以下の通りとする。状態監視システムは既存の生産制御システムのネットワークとは分かれており、これらのシステム間で通信がなされないことを想定する。

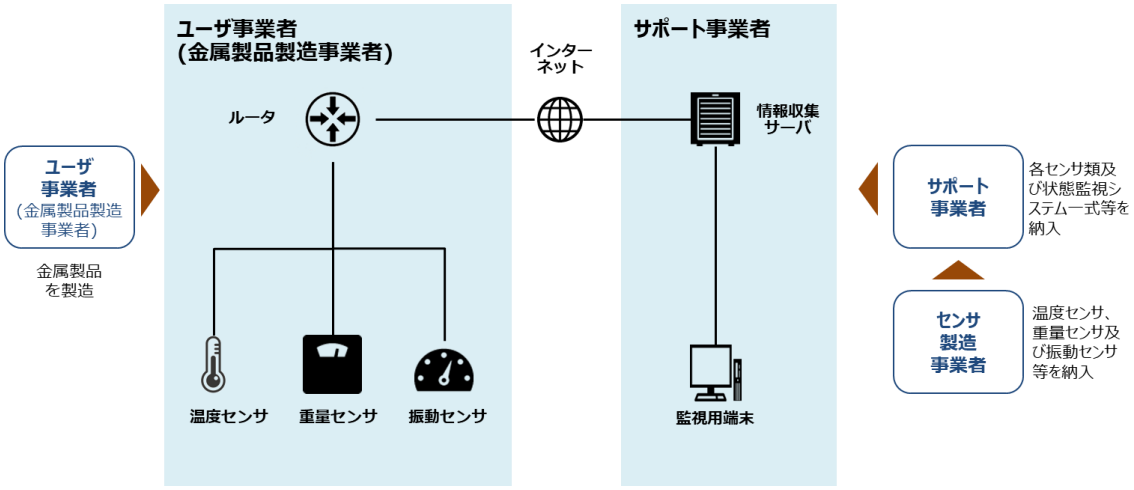


図 41 システム構成図

サポート事業者の従業員が窯の状態を遠隔監視する場合のデータフローは以下の通りとする。

1. 各センサ等がルータを通じて取得した情報を情報収集サーバに送信する。
2. 情報収集サーバの情報を監視用端末が確認する。

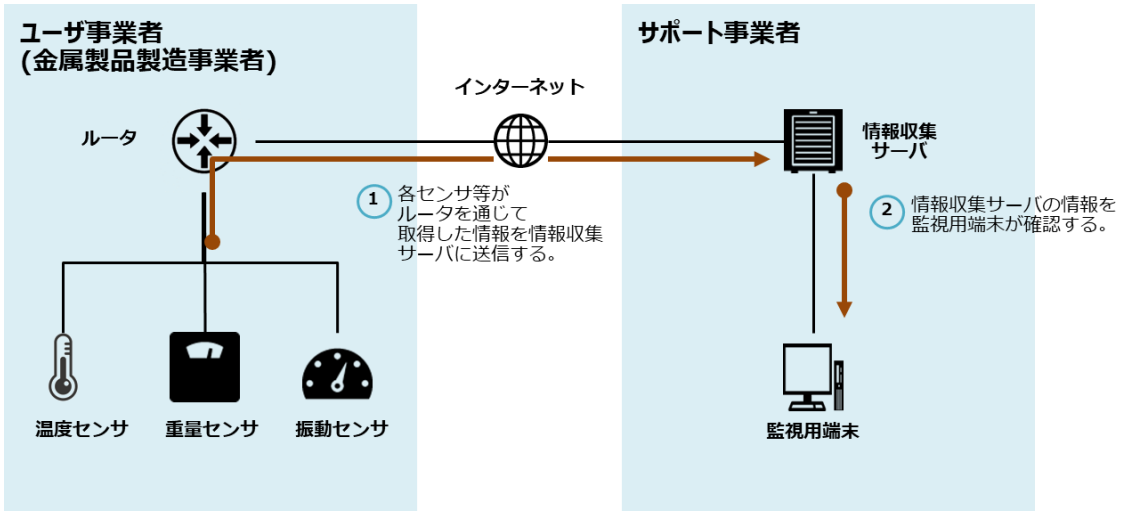


図 42 データフロー図(一部を抜粋)

⑤ リスク基準

「回復困難性の度合い」において、自社が定めるセキュリティ及びセーフティに関する基本方針にのっとるとともに、個人情報等の漏えい等がないよう、セキュリティ対策を通じて生じ得る被害の度合いを「限定的なダメージ」に抑えることを目指す。

「経済的影響の度合い」において、稼働情報を可視化し継続的にサービスを提供することが重要視される。したがって、サービスの停止が生じないようセキュリティ対策を通じて「限定的な経済影響」に抑えることを目指す。

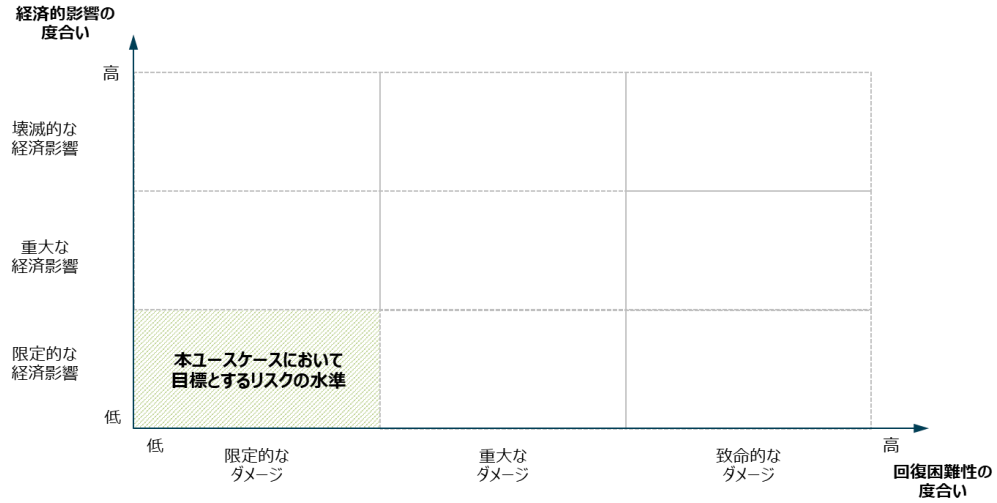


図 43 状態監視システムにて目標とするリスクの水準

(2) リスクアセスメント

「回復困難性の度合い」及び「経済的影響の度合い」から、状態監視システムのリスクアセスメントを行う。

① 想定されるセキュリティインシデント等とその結果の特定

状態監視システムにおいて、想定され得るセキュリティインシデント等とその結果(影響)を特定する。当該システムの提供又は利用に際して想定されるセキュリティインシデント(例)は以下の通り。

- 悪意のある攻撃者又はサポート事業者の従業員が、インターネット又はローカルネットワーク経由でサポート事業者が管理する情報収集サーバに不正アクセスすることによって、営業秘密として管理しているユーザ事業者(金属製品製造事業者)及び他の顧客における設備の稼働情報等が流出する。
- 悪意のある攻撃者が、インターネット又はローカルネットワーク経由でサポート事業者が管理する情報収集サーバをマルウェア(例:ランサムウェア)に感染させることによって、サーバの一部機能を停止させる。悪意のある攻撃者より脅迫を受けることで、サポート事業者が金銭的な被害を受ける。
- 悪意のある攻撃者又はサポート事業者の従業員が、インターネット又はローカルネットワーク経由でサポート事業者が管理する情報収集サーバに DoS 攻撃を仕掛けることによって、サーバの一部機能を停止させることで、温度情報等を正確に表示することができなくなる。

ステークホルダーごとの観点を踏まえたリスクアセスメント

以下に示すステークホルダーごとに「回復困難性の度合い」「経済的影響の度合い」の観点からリスクアセスメントを行う。

- サポート事業者
- センサ製造事業者
- ユーザ事業者(金属製品製造事業者)

- サポート事業者

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、情報収集サーバに従業員の個人情報等が保存されていないとすれば、仮に何らかの情報流出があったとしても、プライバシーに係る影響は限定的である。

セーフティの観点では、インターネット経由で情報収集サーバがマルウェア（例：ランサムウェア）に感染したり、DoS 攻撃を受けたりすることでセンサの情報を適切に処理できなくなった場合に、サポート事業者の従業員は現場へ駆け付けることを想定している。ただし、各設備にはフェールセーフ等の機能が具備されていたり、予め温度センサ等が正確な情報を取得できていないことを従業員が理解できていたりするため、けがを負う可能性は低いと想定される。

プライバシーの観点ではサポート事業者の従業員の個人情報が流出する可能性は低く、セーフティの観点においても従業員がけがをする可能性が低いことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B） 発生したインシデントの経済的影響の度合い

「内外への直接影響（内部）」の観点では、インターネット経由で情報収集サーバがマルウェア（例：ランサムウェア）に感染した場合に悪意のある攻撃者による脅迫により金銭的な被害を受ける可能性や、DoS 攻撃を受けることでセンサの情報を適切に処理できなくなった場合にユーザ事業者（金属製品製造事業者）を含むサービスを利用する事業者全体に対してサービスを提供できなくなる可能性がある。また、「内外への直接影響（外部）」の観点では、情報収集サーバにおけるマルウェア感染によって、他の事業者に対してサービスを提供できなくなる可能性があり、影響が広範囲にわたって及ぶと想定される。

また、インシデントの初期対応や原因究明等にかかる時間を考慮すれば、インシデント検知後速やかに通常の運用に戻るとは考え難く、「直接影響の継続時間」も無視できないものとなることが想定される。

「代替可能性」の観点において、情報収集サーバがマルウェアに感染したり、DoS 攻撃を受けたりした場合、代わりとなる仕組みを即座に用意することはできず、影響が一定期間継続するため、代替となるサービスを提供することはできないと想定される。

間接的な経済影響の観点において、情報収集サーバや各種センサの修理や交換に一定のコストを要する可能性があると想定される。

したがって、直接的な経済影響は重大であり、間接的な経済影響も重大であると想定されるため、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

- センサ製造事業者

A） 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、従業員の個人情報等が流出する可能性は少ないと想定される。

セーフティの観点では、従業員が金属製品製造工場の現場に常駐していない限りは、けがを負う可能性は低いと想定される。

プライバシーの観点ではセンサ製造事業者の個人情報が流出する可能性が少ないこと、セーフティの観点ではセンサ製造事業者及び監視カメラ製造事業者の従業員がけがを負う可能性が少ないことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B)　発生したインシデントの経済的影響の度合い

センサ製造事業者が状態監視システムの運用において大きな役割を有さないことを念頭に置けば、運用時に発生するセキュリティインシデントが同社に与える「直接影響」、「直接影響の継続時間」は、限定的なものになると想定される。ただし、サポート事業者に対する注意喚起(例：設定方法に関する説明等)を怠った場合には、サービス提供における過失が認められ得る。その結果として、契約上の責任が問われ得る。

間接的な経済影響としても、センサ製造事業者が設計、開発した各種センサ等において契約上大きな問題がない場合、仮にサポート事業者による運用においてセキュリティインシデントが発生したとしても責任は限定的であると想定される。

よって、「経済的影響の度合い」のレベルを「限定的な経済影響」と評価する。

- ユーザ事業者（金属製品製造事業者）

A)　発生したインシデントの影響の回復困難性の度合い

プライバシーの観点では、情報収集サーバに設備の稼働情報は保存されているものの、ユーザ事業者（金属製品製造事業者）の従業員の個人情報等が保存されていないため、セキュリティインシデントによって個人情報が流出する可能性は低いと想定される。

セーフティの観点では、情報収集サーバ等がマルウェア感染し正確な数値を表示できなくなった場合、生産制御システムとは接続されておらず、これらのシステムもフェールセーフ等の機能が具備されていると想定すると、従業員がけがを負う可能性は低いと想定される。

プライバシーの観点ではユーザ事業者（金属製品製造事業者）の個人情報が流出する可能性が低く、セーフティの観点においては従業員がけがを負う可能性は低いことから、「回復困難性の度合い」のレベルは「限定的なダメージ」と評価する。

B)　発生したインシデントの経済的影響の度合い

「内外への直接影響(内部)」の観点では、インターネット又はローカルネットワーク経由でサポート事業者が管理する情報収集サーバが不正アクセスされることによって、営業秘密として管理しているユーザ事業者（金属製品製造事業者）における設備の稼働情報等が流出し、ユーザ事業者（金属製品製造事業者）の金属製造に係るノウハウが外部へ流出する。競争力の源泉となっていたノウハウが流出することで、ユーザ事業者（金属製品製造事業者）の競争力が失われ事業上の損害が生じる可能性がある。

「内外への直接影響（外部）」の観点では、設備の稼働情報が流出したとしてもユーザ事業者外部への影響は限定的であると想定される。

「直接影響の継続時間」の観点では、状態監視システムが停止した場合においても、生産制御システムとは接続しておらず工場内で運用されている監視の仕組みが正常に稼働しているならば、工場の稼働停止にはつながらないと想定される。

「代替可能性」の観点では、上記の通り、状態監視システムがセキュリティインシデントに伴って停止したとしても、上述した理由により、製造プロセスに必ずしも異常は生じないと想定される。

間接的な経済影響の観点では、マルウェア（例：ランサムウェア）に感染したり、DoS 攻撃を受けたりすることにより、情報収集サーバがセンサの情報を適切に処理できなくなったとしても、ユーザ事業者（金属製品製造事業者）の工場内での運用によって、金属製品の品質や製造設備の劣化等は防げると

想定されるため、ここでは設備の稼働停止等による間接影響を考慮しない。

直接的な経済影響の観点から、「経済的影響の度合い」が比較的大きくなると想定されることから、「経済的影響の度合い」のレベルは「重大な経済影響」と評価する。

② マッピング結果の整理と評価の実施

上記を踏まえ、フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて、ステークホルダーごとに第 1 軸「回復困難性の度合い」及び第 2 軸「経済的影響の度合い」からカテゴライズし、マッピングする。

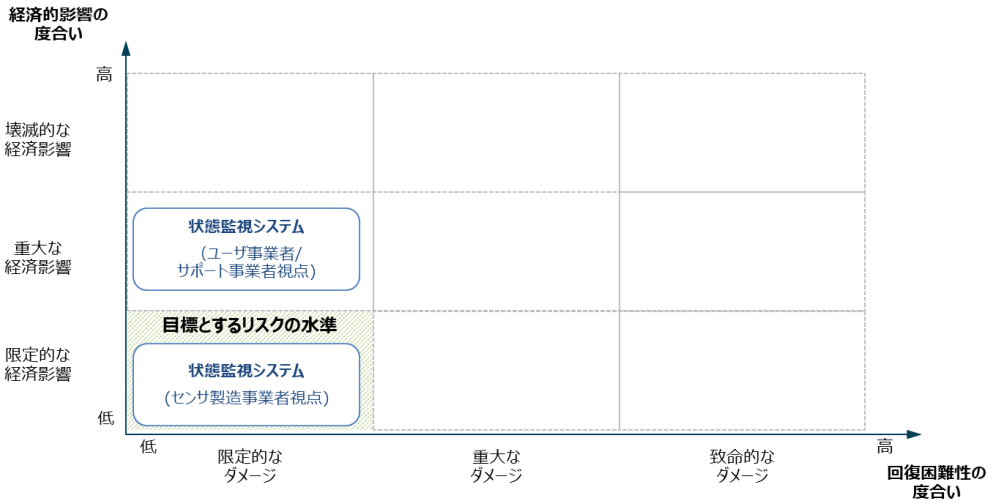


図 44 各ステークホルダーの観点を考慮した対象システムに想定されるリスク(例)のマッピング結果

マッピング結果を踏まえると、センサ製造事業者視点の状態監視システムが保有するリスクは目標とする水準内に収まっているものの、サポート事業者やユーザ事業者（金属製品製造事業者）視点の情報監視システムが保有するリスクは目標とする水準内に収まっていない。

以下では、まずサポート事業者やユーザ事業者（金属製品製造事業者）において目標とするリスク水準に収まっていない原因を整理した上で、リスクを低減するための対策を検討するものとする。

サポート事業者及びユーザ事業者（金属製品製造事業者）視点からみた状態監視システムの「回復困難性の度合い」は小さいものの、「経済的影響の度合い」は比較的大きくなる。

サポート事業者及びユーザ事業者（金属製品製造事業者）の「経済的影響の度合い」が比較的大きくなるのは、営業秘密として管理しているユーザ事業者（金属製品製造事業者）の設備の稼働情報が外部に流出した場合である。これらを引き起こすと考えられる脅威は、例えば以下の通りである。

- 情報収集サーバに保存しているデータに対して不正アクセスされる

上記を踏まえて、IoT-SSF の適用主体であるサポート事業者は、これらの状態監視システムがもつリスクを、可能な限り目標とする水準に収めることを目的として、例えば、以下のように影響度が大きいリスクに対処するための対策方針を明確にすることで、以降の行うべきと考えられる対策等の検討を行うことができると考えられる。

● サポート事業者にとってのリスクを低減するための対策方針

➢ 経済的影響の度合いの観点

サポート事業者にとっては、情報収集サーバに保存された稼働情報の漏えいやマルウェア感染（例：ランサムウェア）が重要なリスクとなるが、これらのリスクに対応するため以下の対策が有効であると考えられる。

✧ 稼働情報の漏えいを防ぐ仕組みの構築

✧ 信頼性の高い状態監視システムを可能にするための仕組みの構築

● ユーザ事業者（金属製品製造事業者）にとってのリスクを低減するための対策方針

➢ 経済的影響の度合いの観点

ユーザ事業者（金属製品製造事業者）にとっては、情報収集サーバに保存された稼働情報が漏えいし、事業上の損失を負うことが重要なリスクとなるが、これらのリスクに対応するため以下の対策が有効であると考えられる。

✧ 稼働情報の漏えいを防ぐ仕組みの構築

上記で示した対策例を添付 A に示す対策要件と比較した上で、対応関係を整理することによって、本稿で整理した対策要件のうち、行うべきと考えられる対策を明らかにすることができる。

表 39 影響度が大きいリスクに対処するための対策方針及び添付 A に記載された対策要件との関係性

影響度が大きいリスクに対処するための対策方針		添付 A に記載された対策要件
サポート事業者	稼働情報の漏えいを防ぐ仕組みの構築	適切な水準のアクセス制御の実装
		暗号化によるデータの保護
	信頼性の高い状態監視システムを可能にするための仕組みの構築	IoT 機器・システムの十分な可用性の確保
		暗号化によるデータの保護
ユーザ事業者（金属製品製造事業者）	稼働情報の漏えいを防ぐ仕組みの構築	適切な水準のアクセス制御の実装
		暗号化によるデータの保護

(3) リスク対応

① システムを構成する機器ごとの脅威の整理

システムを構成する機器・システムごとに想定される脅威（例）は以下の通り。

表 40 想定される脅威（例）

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
情報収集サーバ	情報漏えい	情報収集サーバから製品製造事業者の工場における設備の稼働情報が流出する。
	サービス不能	情報収集サーバが(D)DoS 攻撃を受けて、サポート事業者やユーザ事業者（金属製品製造事業者）がサーバやサービス等にアクセスできなくなる。
	不正アクセス	インターネット経由で情報収集サーバに保存されたデータに対して、不正アクセスされる。
	マルウェア感染	情報収集サーバがマルウェア感染する。
監視用端末	マルウェア感染	監視用端末がマルウェア感染する。
ルータ	不正アクセス	既知の脆弱性等を悪用することでルータに不正アクセスされる。
温度センサ	データの改ざん	温度センサから発信される通信中に温度情報が改ざんされる
	情報漏えい	温度センサから発信される温度情報が外部に漏えいする。
重量センサ	データの改ざん	重量センサから発信される通信中に重量情報が改ざんされる

システムを構成する機器	想定される脅威（例）	生じ得るインシデント(例)
	情報漏えい	重量センサから発信される温度情報が外部に漏えいする。
振動センサ	データの改ざん	振動センサから発信される通信中に振動情報が改ざんされる
	情報漏えい	振動センサから発信される温度情報が外部に漏えいする。

② 脅威に対する対策の整理

想定される脅威を踏まえ、第 3 軸「求められるセキュリティ・セーフティ要求」における観点ごとにサポート事業者にて実装が想定される対策要件を整理する。

表 41 サポート事業者にて実装が想定される対策要件（例）

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の明確化
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守
		全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		不正アクセス	適切な水準のアクセス制御の実装
		データの改ざん	ソフトウェアの完全性の検証
		情報漏えい	ソフトウェアのインストールの制限
		全般	様々な IoT 機器に接続する際のセキュリティの確保
		データの改ざん 情報漏えい	暗号化によるデータの保護
		データの改ざん 情報漏えい	ライフサイクルを通じた暗号鍵の管理
		マルウェア感染	マルウェア対策の実施
		全般	IoT 機器・システムの十分な可用性の確保
		全般	IoT に適したネットワークの利用
		全般	適切なネットワークの分離
		全般	IoT 機器・システムの設置場所等に対する物理的アクセスの制御
		全般	IoT 機器システムの構成要素（機器、ネットワーク等）の物理的保護
		全般	セキュアな開発環境と開発手法の適用
		全般	IoT 機器・システムにおけるセキュリティ機能の検証
		不正アクセス マルウェア感染	IoT 機器・システムの出荷時における安全な初期設定と構成
		全般	IoT 機器・システムにおける運用開始時の正しい設置、設定
第 2 の観点	ソシキ・ヒト	全般	利用者へのリスクの周知等の情報発信
		全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		全般	インシデント対応手順の整備と実践
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令及び契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		全般	IoT 機器・システムに対するアップデートの適用

③ 整理した対策に対する意思決定

対策等を検討する際にはインシデントの起こりやすさも踏まえ、システム全体としてのリスクを低減するような対策を検討する。

- 対策の適用対象（どの機器を中心に検討するか）

想定しているインシデントが発生した際に想定される被害の大きさ及び起こりやすさ等を考慮して、情報収集サーバ、監視用端末、ルータ、各種センサ等から、特に対策を検討すべき資産を検討する。

被害の大きさという観点では、個々のセンサ等では個別の稼働情報のみが保管、送信されている状況に留まっていることを考慮すれば、各種センサ等からのデータを集約し、より多くの価値あるデータを取扱っていると考えられる以下の資産を中心として対策を検討すべきである。

- 情報収集サーバ

  自社の事業継続及び、サービスの提供を想定しているユーザ事業者（金属製品製造事業者）だけでなく、同様のサービスを利用する事業者全体に対して影響が波及し得る。

また、「起こりやすさ」の観点では、外部からのネットワーク経由での攻撃に対して対処する必要があるため、インターネットに直接接続されている資産（例：情報収集サーバやルータ等）を中心として対策を検討することが望ましい。

- 適用する対策の内容（どのように対策を実施するか）

②にて検討した事業者にて実装が想定される対策要件の例より、より効率的・効果的にリスクを低減できるものを中心として対策を検討する。例えば、ユーザ事業者（金属製品製造事業者）の工場に設置される各種センサは、非常に数が多いうえに簡単な構成であり、各種センサにエンドポイントセキュリティソフトを導入する等の IT 環境では一般的なセキュリティ対策を実施することが難しいケースがある。一方で、上述したように、情報収集サーバには各種データが集約され、攻撃者にとってもより魅力的な標的としてとらえられる可能性が高い。その場合には、サーバ側で以下の対策要件を実装した上で、より上位のシステムで守る構成とすることにより、システム全体として効率的・効果的にリスクを低減することが望ましい。

- 適切な水準のアクセス制御の実装
- 暗号化によるデータの保護
- マルウェア対策の実装
- IoT 機器・システムの十分な可用性の確保

上記を踏まえて、状態監視システムがもつリスクを目標とする水準に収めることを目的として、サポート事業者がシステムの設計、開発、運用等の段階で実装することとした対策要件の例を以下に示す。

第 1 の観点では、サポート事業者が企画段階において、当該事業者やユーザ事業者（金属製品製造事業者）のリスクを抑えることを目的として実装することとした対策要件を整理した。

第 2 の観点では、サポート事業者の運用段階において、当該事業者やユーザ事業者（金属製品製造事業者）のリスクを抑えることを目的実装することとした対策要件を整理した。

第 3 の観点については、本ユースケースが対象とする業務やシステムでは法令等による運用担当者への専門資格保有の要求、あるいはそれに相当する業界又は社内の人事等に関する慣行は必ずしも認められないことから、これらに該当する対策要件は実装しないこととした。

第 4 の観点には、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネッ

2188 トの構築等）が該当するため、本ユースケースにてこれらに該当する対策要件は実装しないこととした。
2189 　なお、第 1 の観点及び第 2 の観点における対策要件のうち、サポート事業者単体では対応が難しい
2190 対策要件がいくつか見られた。これらの対策要件の実装はユーザ事業者（金属製品製造事業者）に依
2191 頼することとした。

2192 表 42 サポート事業者において実際に講じる対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● 自社が提供するサービスを対象としたセキュリティポリシー（情報セキュリティ関連規定を含む）の策定及び適切な承認権限を有する者の承認 ● 定められた期間ごとの当該ポリシーのレビュー	
2			運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保	● 状態監視システムのセキュリティ管理責任者及びセキュリティ対策担当者の任命 ※ 上記の管理責任者及び開発担当者は、状態監視システムのライフサイクルの各段階（例：設計、開発）において明確化されていることが望ましい。	
3			IoT セキュリティに関するステークホルダーの役割の明確化	● 状態監視システムのセキュリティ対策の設計・開発・運用等における関係各社の責任範囲の決定 ● 運用中に発生したセキュリティインシデントにより損害が発生した場合の責任範囲（役割分担や損害賠償）の決定	
4			IoT 機器・システムに係る要員のセキュリティ確保	● 自社内の要員に対する適切な訓練及びセキュリティ教育の実施	
5		システム	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守	● 状態監視システムや監視用端末にて扱う情報セキュリティに関連する法的、規制（例：製品安全関連法、知的財産法）又は各製造事業者にサービスを提供する場合に契約上の義務に対する違反を避けるための要求事項の遵守 ● 関係省庁から公表されているガイドライン（例：経済産業省「AI・データの利用に関する契約ガイドライン」、「営業秘密管理指針」等）の参照	
6			企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	● 状態監視システムの企画・設計時におけるリスクアセスメントの実施、セキュリティ要件の特定、要件の実装に係る費用の確保 ● 必要なセキュリティ仕様が組み込まれているかを確認する設計レビューの実施	
7			適切な水準のアクセス制御の実装	● あるユーザ事業者（（金属製品製造事業者以外の事業者も含む）から収集した稼働情報を、他のユーザ事業者から情報収集サーバ上で閲覧できないように、ユーザ事業者ごとに適切なアクセス権限の設定 ● 想定されるリスクの大きさを考慮した方式による、ユーザ事業者や自社の従業員、接続する IoT 機器の認証 ● 情報収集サーバのアプリケーションへの特権アクセスに対して、多要素認証を適用 ● パスワード等の認証情報の安全管理（例：ハッシュ化のうえ保管）	○ （「稼働情報の漏えいを防ぐ仕組みの構築」及び「信頼性の高い状態監視システムを可能にするための仕組みの構築」に有効と考えられる対策）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
8			ソフトウェアの完全性の検証	● 情報収集サーバや監視用端末のソフトウェアや格納されたデータにおける完全性の検証機能の実装	
9			ソフトウェアのインストールの制限	● 情報収集サーバや監視用端末の構成についてベースラインを作成し、必要な変更がなければ当該構成を継続的に維持	
10			様々な IoT 機器に接続する際のセキュリティの確保	● あらかじめ識別情報（例：MAC アドレス）を登録している機器（各種センサ等）による情報収集サーバへの接続に限り許可	
11			暗号化によるデータの保護	● 通信中のデータにおける完全性の検証 ● 情報収集サーバ上に保管されている稼働情報等の暗号化	○ （「稼働情報の漏えいを防ぐ仕組みの構築」及び「信頼性の高い状態監視システムを可能にするための仕組みの構築」に有効と考えられる対策）
12			ライフサイクルを通じた暗号鍵の管理	● 暗号鍵の利用、保護及び有効期間に関するポリシーの策定及び遵守	
13			マルウェア対策の実施	● 情報収集サーバ及び監視用端末におけるマルウェア対策ソフトウェアの導入 ● 不正通信検知機能を有するルータ等の導入	○ （「信頼性の高い状態監視システムを可能にするための仕組みの構築」に有効と考えられる対策）
14			IoT 機器・システムの十分な可用性の確保	● 情報収集サーバやルータに対する(D)DoS 攻撃を想定し、一定レベルの負荷に耐える容量や負荷分散用機器を確保 ● 情報収集サーバやルータにおいて不審な通信（例：特定の IP アドレスからの大量のリクエスト）を検知し、適宜遮断等する ● アプリケーションのテスト段階における一定レベルの負荷試験の実施	○ （「信頼性の高い状態監視システムを可能にするための仕組みの構築」に有効と考えられる対策）
15			IoT に適したネットワークの利用	● ユーザ事業者（金属製品製造事業者）内の設備に設置された各種センサを、暗号化機能を有した Wi-Fi（例：WPA2-PSK（AES）等）に接続 ● ユーザ事業者（金属製品製造事業者）における既存の帯域を圧迫しない通信方法の選択（例：既存の制御システムとは別のネットワークを整備する）	
16			セキュアな開発環境と開発手法の適用	● セキュアコーディング手法の適用 ● 委託先を含む開発人員向けのセキュリティ対策、開発環境やコードへのアクセスの制御、開発環境と運用環境の分離等、安全な開発環境に必要な対応の実施 ● 設計書、プログラム、バイナリ等のバックアップ	
17			IoT 機器・システムにおけるセキュリティ機能の検証	● コード分析ツール又は脆弱性スキャナのような自動化ツール等を活用したセキュリティ機能に関する検証の実施 ● 情報収集サーバや監視用端末に対するペネトレーションテストの実施	
18			IoT 機器・システムの出荷時における安全な初期設定と構成	● 情報収集サーバや監視用端末の不要なネットワークポート、その他 USB やシリアルポートなどの物理的又は論理的な閉塞	
19			IoT 機器・システムにおける運用開始時の正しい設置、設定	● IoT 機器の事業者から提供されたガイドに従った設置、設定	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
20	第 2 の観点	ソシキ・ヒト	利用者へのリスクの周知等の情報発信	● 営業担当者、保守担当者、企業ホームページ等を通じたユーザ情報の漏えいや機器のマルウェア感染等のインシデントに関する情報発信の実施	
21			運用中における IoT セキュリティを目的とした体制の確保	● セキュリティ管理責任者及びセキュリティ対策担当者が異動した場合の後任の選任	
22			過去の対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的なインシデント抑制への活用（他社の類似サービスにおけるセキュリティインシデントを含む）	
23		プロシージャ	脆弱性対応に必要な手順等の整備と実践	● 脆弱性情報の収集及び評価の実施。 ● 状態監視システムに関連した脆弱性が明らかになった場合、これらの脆弱性に対応するための手順の整備。	
24			インシデント対応手順の整備と実践	● 状態監視システムに適応したインシデント対応手順の整備。 ● サポート事業者とユーザ事業者（金属製品製造事業者）の役割と責任の識別及び指定された個人によって実行されるアクションの定義・伝達 ● インシデント対応手順の定期的な訓練。	
25			IoT 機器・システムの適正な運用・保守	● 状態監視システムの適切な運用手順の整備 ● 運用手順に従った保守、管理	
26			IoT 機器・システムの適正な使用	● 状態監視システムを対象としたサービス提供や管理のポリシー提示及び遵守 ● 状態監視システムを対象としたセキュリティパッチの適用手順の提示	
27		システム	運用中における法令及び契約上の要求事項の遵守	● 状態監視システムや監視用端末にて扱う情報セキュリティに関連する法的、規制（例：製品安全関連法、知的財産法）又は各製造事業者にサービスを提供する場合に契約上の義務に対する違反を避けるための要求事項の遵守 ● 関係省庁から公表されているガイドライン（例：経済産業省「AI・データの利用に関する契約ガイドライン」、「営業秘密管理指針」等）が更新された場合、更新されたガイドラインへの対応	
28			継続的な資産管理	● 各種センサを含む状態監視システムの資産目録（機器上に実装されたソフトウェア及びファームウェア、工場出荷時の設定等を含む）の作成・維持	
29			プログラムソースコード及び関連書類の保護	● 状態監視システムに係るプログラムソースコード及び関連書類（例：設計文書）への論理アクセスを最小限にした上で、閲覧、編集等に際して多要素認証を実施	
30			IoT 機器・システムのモニタリング及びログの取得、分析	● 状態監視システムを構成する情報収取サーバや監視用端末を対象にした各種ログ（例：ユーザ認証、ネットワークトラフィック）の取得及び保護。 ● ルータを対象としたネットワークトラフィックの取得及び保護。 ● 取得したログの定期的な分析及び異常の検知。	

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
31			IoT 機器・システムに対するアップデートの適用	● 報告された脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定 ※新たに検知された情報収集サーバ上のアプリケーション及び各種センサに係る脅威や脆弱性の報告窓口は既に設置されているものとする。	

2193

2194 ● ユーザ事業者（金属製品製造事業者）が実装する対策（例）

2195 ユーザ事業者（金属製品製造事業者）で対応が必要な対策について、サポート事業者はサービス提供
2196 時に対策を依頼するものとする。ユーザ事業者（金属製品製造事業者）は主に以下の対策要件を実装
2197 するものとする。

2198 ただし、ユーザ事業者（金属製品製造事業者）では、「IoT 機器・システムの設置場所等に対する物理
2199 的アクセスの制御」及び「IoT 機器システムの構成要素（機器、ネットワーク等）の物理的保護」の対策を
2200 既に実施済みである想定だが、ここでは改めて対策の例を記載する。

2201 表 43 ユーザ事業者（金属製品製造事業者）が実装する対策（例）

No	第 3 軸	実装先	対策要件	実際に講じる対策（例）	影響度が大きいリスクに対処するための対策要件
1	第 1 の観点	システム	適切なネットワークの分離	● 新たに導入するセンサを含むネットワークと既存の生産制御システムを含むネットワークの分離	
2			IoT 機器・システムの設置場所等に対する物理的アクセスの制御	● 外部の物理的な脅威から保護されるべき各種センサやルータへの認可されていないアクセスを防ぐ目的で、入退管理（例：職員証や入館ゲート等）を通じた物理的セキュリティ境界の確立。	
3			IoT 機器システムの構成要素（機器、ネットワーク等）の物理的保護	● 業務上重要な施設への物理アクセスに対する監視カメラ等によるモニタリング。	
4			IoT 機器・システムにおける運用開始時の正しい設置、設定	● IoT 機器の事業者の想定する仕様に適合したネットワーク環境の整備	

2202

添付 A　対策要件

「IoT セキュリティ・セーフティ・フレームワーク」の第 3 軸「求められるセキュリティ・セーフティ要求」における 4 つの観点を参照しつつ、有効と考えられる対策要件を以下に整理する。

対策要件の実装先は、「ソシキ・ヒト」、「プロシージャ」及び「システム」に分けられる。

「ソシキ・ヒト」には、「バリュークリエーションプロセスに参加する組織・団体・組織」や「その組織に属する人及び価値創造過程に直接参加する人」のセキュリティ向上を目的とした非技術的な対策要件（例：セキュリティ対応組織の設置や関連するポリシーの策定等）が該当する。

「プロシージャ」には、セキュリティ能力の向上を目的として、「目的を達成するための一連の活動の手続き」を定めた非技術的な対策要件（例：脆弱性対応に必要な手順等の整備と実践等）が該当する。

「システム」には、「目的を実現するためにモノで構成される仕組み・インフラ」のセキュリティ能力の向上を目的とした技術的な対策要件が該当する。

「システム」に該当する対策要件は、IoT 機器・システムにて一般的に想定されるライフサイクルの段階の順で示す。

例えば、第 1 の観点は以下の段階の順で示す。

- 企画・設計（例：企画・設計段階におけるセキュリティ要求事項の分析及び仕様化）
- 開発（例：適切な水準のアクセス制御の実装）
- 試験（例：IoT 機器・システムにおけるセキュリティ機能の検証）
- 設置（例：IoT 機器・システムにおける運用開始時の正しい設置、設定）

第 2 の観点は、以下の段階の順で示す。

- 運用（例：継続的な資産管理の実施）
- 廃棄（例：IoT 機器・システムの安全な廃棄又は再利用）

表 A-1 対策要件（例）

第 3 軸	実装先	対策要件
第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定
		運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		IoT セキュリティに関するステークホルダーの役割の明確化
		IoT 機器・システムに係る要員のセキュリティ確保
	システム	運用前（設計・製造段階）における法令及び契約上の要求事項の遵守
		企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		適切な水準のアクセス制御の実装
		ソフトウェアの完全性の検証
		ソフトウェアのインストールの制限
		様々な IoT 機器に接続する際のセキュリティの確保
		暗号化によるデータの保護
		ライフサイクルを通じた暗号鍵の管理
		マルウェア対策の実施
		IoT 機器・システムの十分な可用性の確保
		IoT に適したネットワークの利用
		適切なネットワークの分離
		IoT 機器・システムの設置場所等に対する物理的アクセスの制御
		IoT 機器システムの構成要素（機器、ネットワーク等）の物理的保護
		セキュリティ設計と両立するセーフティ設計の仕様化
		セキュアな開発環境と開発手法の適用

第 3 軸	実装先	対策要件
		IoT 機器・システムにおけるセキュリティ機能の検証
		信頼できる IoT 機器やサービスの選定
		IoT 機器・システムの出荷時における安全な初期設定と構成
		IoT 機器・システムにおける運用開始時の正しい設置、設定
第 2 の観点	ソシキ・ヒト	利用者へのリスクの周知等の情報発信
		運用中における IoT セキュリティを目的とした体制の確保
		過去の対応事例からの学習
	プロシージャ	脆弱性対応に必要な手順等の整備と実践
		インシデント対応手順の整備と実践
		事業継続計画の策定と実践
		IoT 機器・システムの適正な使用
		IoT 機器・システムの適正な運用・保守
	システム	運用中における法令及び契約上の要求事項の遵守
		継続的な資産管理
		プログラムソースコード及び関連書類の保護
		IoT 機器・システムのモニタリング及びログの取得、分析
		IoT 機器・システムに対するアップデートの適用
		IoT 機器・システムの安全な廃棄又は再利用
第 3 の観点	ソシキ・ヒト	IoT 機器・システムの運用・管理を行う者に対する要求事項の特定
		IoT 機器・システムの運用・管理を行う者に対する要求事項の遵守の確認
第 4 の観点	ソシキ・ヒト	賠償等の対処を実施することが容易ではないケース等における社会的なセーフティネットの構築

2225

添付 B 実際に講じる対策の例

本添付資料では、事業者が具体的なセキュリティ対策等を検討する際に参照できる情報として、添付 A に示された対策要件ごとに講じる対策の例を示す[38]。具体的な対策の内容は、業種や事業者に固有の条件等により様々に異なることが想定されるが、以下の内容は、そうした個別の検討を行う際の共通的な基礎のひとつになることを意図するものである。

なお、読者においては、以下の記載事項が何ら事業者にとっての義務的な事項を含んだものではなく、単に IoT 機器・システムにおいてセキュリティ対策等を実装する際の参考情報を示すものとなっている点に留意されたい。

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
第 1 の観点	ORG	対象の IoT 機器・システムにおけるセキュリティポリシーの策定	● 自組織が提供又は利用する IoT 機器・システム、サービスのセキュリティに関する方針（ポリシー）を策定し、社内に周知するとともに、継続的に実現状況を把握し、定期的にレビューする。 - かかるポリシーとして、自組織の役割に応じて、IoT 機器・システムの管理のポリシー、IoT サービス提供のポリシー、個人情報を含むデータ管理などのポリシー等が策定され得る[40]。 - IoT 機器・システム、サービスのセキュリティポリシーは以下の事項に関する記述を含むことが望ましい。 ➢ 対象となる IoT 機器・システム、サービスの概要 ➢ IoT 機器・システム、サービスに係る自組織の役割（例：IoT ユーザ、IoT サービス提供者、IoT サービス開発者） ➢ IoT 機器・システム、サービスに対するセキュリティ対策の目的 ➢ 組織内における IoT 機器・システム、サービスのセキュリティに対する役割と責任 ● 上記の全体的な方針に加え、特定の IoT 機器・システム、サービスを対象としたより具体的なポリシー、対策基準等を策定する。かかる対策基準等のトピックとして、以下の事項に関する記述を含むことが望ましい。 - アクセス制御 - 情報分類及び取扱い - その他の対策領域	CPS.BE-2 CPS.GV-1 CPS.GV-2
		運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保	● 自組織の IoT 機器・システム、サービスの提供又は利用に係るセキュリティポリシーに沿って、対象機器・システムのセキュリティに対する役割と責任の割り当てを行い、その内容を文書化した上で関係者に周知する。 ● 割り当てる役割と責任には、以下が含まれていることが望ましい。 - 意思決定等を行う経営層（CISO 等）及びその補佐 - 機器・システムの企画・設計段階におけるセキュリティ仕様の検討 - 機器・システムの開発段階におけるセキュリティ対策の実装と運用 - IoT 機器・システムに係る調達先及び委託先の管理	CPS.AE-2 CPS.RM-1

[38] 第 4 の観点には、主に政策立案者が講じる対策要件（例：保険加入を義務づける等のセーフティネットの構築等）が該当するが、IoT 機器・システムを開発、提供あるいは利用する事業者が講じるべき対策とは性質が異なる内容のため、本添付資料での記載は割愛している。

[39] 添付 B では、実装先として添付 A に示したもののうち、「ソシキ・ヒト」を「ORG」、「システム」を「SYS」、「プロシージャ」を「PRO」と表記する。

[40] 産業サイバーセキュリティ研究会ワーキンググループ 1（制度・技術・標準化）スマートホームサブワーキンググループ「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン Version 1.0」添付E-5

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			- 機器・システムの企画や設計、開発を担当する者を対象にした意識向上、教育・訓練プログラム - 開発環境等における脆弱性やインシデントへの対応 ※ より具体的な実施内容等については、経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き 第1.1版」等を参照されたい。	
		IoT セキュリティに関するステークホルダーの役割の明確化	● IoT 機器・システムのライフサイクルの全体にわたり、IoT 機器・システムの提供又は利用に係る自身の役割を考慮しつつ、関係する IoT 利用者、IoT サービス開発者、IoT サービス提供者の責任を特定することが望ましい。 - IoT サービス開発者は、適宜 IoT 利用者と連携し、例えば以下の要件に対応した開発、実装における役割を果たすことが望ましい。 ➢ 企画・設計段階におけるセキュリティ要求事項の分析及び仕様化 ➢ セキュアな開発環境と開発手法の適用 ➢ IoT 機器・システムにおけるセキュリティ機能の検証 - IoT サービス提供者は、IoT 機器・システム及び関連サービスの運用、保守において、IoT 利用者との分担も念頭に置きつつ、例えば以下の要件に対応した役割を担うことが望ましい。 ➢ 脆弱性対応に必要な手順等の整備と実践 ➢ サービスと IoT 機器・システムのガイドに従った保守、管理 ➢ IoT 機器・システムのモニタリング及びログの取得、分析 - IoT 利用者は、IoT 機器・システム及び関連サービスの利用において、例えば以下の要件に対応した役割を担うことが望ましい。 ➢ IoT 機器・システムにおける運用開始時の正しい設置、設定 ➢ IoT 機器・システムの用途・用法を守った使用 ➢ IoT 機器・システムの安全な廃棄又は再利用 ● 機器・システムの運用中に発生したインシデントにより損害が発生した場合の責任範囲や対応を契約関連文書等において明確にしておくことが望ましい。 - 契約内容に違反した場合の措置 - インシデントが発生した場合の対応 - 新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応 - 契約終了後の情報資産の扱い（返却、消去、廃棄等）	CPS.AM-7 CPS.BE-1 CPS.BE-3 CPS.SC-2 CPS.SC-10 CPS.DP-1
		IoT 機器・システムに係る要員のセキュリティ確保	● IoT 機器・システムの提供又は利用に係る自組織の要員及び委託先の従業員等が、雇用前、雇用期間中、雇用終了後にわたってセキュリティに関する役割を認識し、実行できるよう、例えば以下に示す対策を実施することが望ましい。 - 雇用前の対策 ➢ 対象者が、セキュリティに関する役割と責任を果たすために必要な能力を備えているかどうかの確認 ➢ 秘密保持契約書又は守秘義務契約書への署名 - 雇用期間中の対策 ➢ 対象者へのセキュリティ上の役割と責任に関する要点の伝達 ➢ チェックリストの確認やログのレビュー等を通じた、対象者によるセキュリティ上の要求遵守の定期的な確認 - 雇用終了後の対策 ➢ 雇用の終了以降も一定期間継続する秘密保持契約等の適用 ● IoT 機器・システムの提供又は利用に係る自組織の要員及び委託先の従業員等は、職務に対応した適切な教育や訓練を受け、自身のセキュリティに係る役割と責任について十分な認識を有していることが望ましい。教育の内容は当事者の役割等により変わり得るが、組込まれ得る事項として、例えば以下がある。 - インシデントを通じて組織や個人が被り得る影響とその一般的な動向 - 組織内のセキュリティ関連規則、手順等の内容	CPS.SC-5 CPS.SC-9 CPS.AT-1 CPS.AT-2 CPS.AT-3 CPS.IP-9

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			- セキュリティに関する手順(例:インシデントの報告)や管理策(例:パスワード等の設定、ソフトウェアの更新、開発環境のセキュリティ確保)の実施方法	
	SYS	運用前(設計・製造段階)における法令及び契約上の要求事項の遵守	● IoT 機器・システムの提供又は利用に係る組織は、新たに機器・システムを開発する場合、あるいは既に開発されている機器・システムにおいて関連する法令等が変更された場合に、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みをレビューし、最新に保つことが望ましい。 ● 関連する法令、規制及び契約上の要求事項を特定する際には、対象機器・システムに限定せず、全社的に日頃より自組織が受ける法的な規制やガイドラインを明確化し、各システムが規制対象となる場合の法令等と遵守事項、罰則などを文書化しておく。 ● 特に個人情報保護法は 3 年毎の見直しに連携し、業界向けのガイドラインの改定もあるため留意する。また、GDPR を始めとする他国の規制について、関連があれば文書化しておく。	CPS.GV-2
		企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	● IoT 機器・システムを現に開発、運用する以前の企画・設計の段階で、当該機器・システムに想定されるリスクやその程度、具備すべきセキュリティ要求事項を特定すること(いわゆる、「セキュリティ・バイ・デザイン」)が望ましい。 ● セキュリティ・バイ・デザインを具体的に実践する過程では、以下の活動を実施することが望ましい。 - 適用範囲の決定:セキュリティ対策の対象となる IoT 機器・システム及び関連する組織、ヒトの活動を特定する。 - リスクアセスメント:対象の IoT 機器・システムによる目的の達成を妨げ得るリスクを網羅性も意識しつつ特定し、その影響の大きさや起こりやすさ等を考慮して、対応策を検討するうえでの優先順位づけを行う。 - リスク対応策の具体化:上記にて特定され、評価されたリスクに対処するための方策を選定し、具備すべき要求事項として仕様化する。セキュリティ要求事項には様々なものが選定され得るが、例えば以下が挙げられる。 ➢ 適切な水準のアクセス制御の実装 ➢ 暗号化によるデータの保護 ➢ マルウェア対策の実施 ※ より具体的な実施内容、プロセス等については、IPA「制御システムのセキュリティリスク分析ガイド 第 2 版」や ISO 31000:2018 等を参照されたい。	CPS.RA-3 CPS.RA-5 CPS.RA-6 CPS.IP-3
		適切な水準のアクセス制御の実装	● 想定されるリスクの大きさに応じて、単一又は複数の要素を組み合わせた適切な手法により IoT 機器や関連するシステムにアクセスするユーザ、機器の識別及び認証を行う。適用可能な要素とその具体例は以下の通り。 ＜ユーザ(ヒト)の認証＞ - 知識:パスワード - 所有物:IC カード等のハードウェア - 生体情報:指紋、顔、指静脈等 ＜IoT 機器の認証＞ - MAC アドレス等の機器に割り振られる識別情報 - ハードウェア機構により保護された電子証明書等 ● 以下の対策等を通じて、上記の要素による認証に必要な情報を安全に保つ。 - パスワードは、文字数や文字種等の観点で十分な複雑性を持たせ、ハッシュ化等したうえで適切に保護する。 - IC カード等の認証用の所有物は、紛失、盗難等から厳重に保護する。	CPS.AC-1 CPS.AC-3 CPS.AC-4 CPS.AC-5 CPS.AC-6 CPS.AC-9

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			● 機器内外に保存されている IoT 機器の識別、認証情報は、論理的又は物理的な不正アクセスから適切に保護する。	
		ソフトウェアの完全性の検証	● IoT 利用者又は IoT サービス提供者は、ソフトウェアを実行する前に、当該ソフトウェアの完全性を確認することが望ましい。 ● ソフトウェアの完全性を検証する際、確認すべきものとして以下がある。 – 信頼の基点とセキュアブートメカニズム – ソフトウェアの出所（当該ソフトウェアがベンダーによって署名された信頼できるソースのものか） – ソフトウェアの入手経路のセキュリティ（例：暗号化された接続を介してダウンロードされているか） – ソフトウェアの署名又はチェックサム	CPS.DS-10 CPS.DS-13 CPS.CM-4
		ソフトウェアのインストールの制限	● 不要なソフトウェアや既知の脆弱性を持つソフトウェアは、バックドアの設置や脆弱性の悪用等を通じて攻撃者に利用される可能性があることから、IoT 利用者又は IoT サービス提供者は、組織内でソフトウェアのインストールを管理するための規則を確立し、実施することが望ましい。 ● 具体的な管理策には以下のようなものがある。 – ホワイトリストの作成等を通じて、認可されていないソフトウェアの使用を防止又は検出する。 – ブラックリストの作成等を通じて、悪意のあるソフトウェアであると知られている、又は疑われるソフトウェアの使用を防止又は検出する。 – 上記のリストは、ベンダーから提供されるか、又はベンダーとの協議で定義され、定期的に、又はシステムの変更を実施する際に見直す。 – 特定の特権を許可された利用者によりソフトウェアのインストールが可能となることがあるため、特権の付与を最小限にする。	CPS.IP-2
		様々な IoT 機器に接続する際のセキュリティの確保	● IoT 機器、ネットワーク、サーバ等から構成されるシステムは、様々な IoT 機器との接続を適切に管理し、意図したセキュリティ水準を維持すべきである。 ● 設計、開発の段階で予定している IoT 機器又はサーバ等との接続に関しては、接続する IoT 機器に関する情報（例：製造者、モデル、製造年、準拠規格）を明確化し、提供する機能や情報の範囲を特定したうえで、運用前に動作確認を行う。 ● 設計、開発段階で必ずしも想定していなかった機器との接続を行う場合、製造者等が事前に十分な検証を実施できないことも想定されるが、このような状況に備えて、システムに以下のような機能を実装することが検討され得る。 - ホワイトリストを使用して他の IoT 機器との接続を制御する。 - 機器との接続交渉時、接続先機器に関する情報（例：製造者、モデル、製造年、準拠規格）を取得し、接続可否の判断や、提供する機能、情報の範囲の調整を行う。	CPS.AC-8
		暗号化によるデータの保護	● 技術的に可能な場合、IoT 機器やサーバ等の記憶媒体に保管されるデータ及び、ネットワークを通じて転送されるデータの機密性や完全性を、暗号技術を適切に利用しつつ保護する。 ● サーバ上の保管データに対して、データの保管形態や重要度に応じてファイルの暗号化やデータベースの暗号化を行う。 ● ネットワークを通じて転送されるデータに対して、技術的に可能な場合、機密性だけでなく完全性や真正性も含めた保護を行うため、TLS や IPsec 等のプロトコルを利用する。	CPS.DS-2 CPS.DS-3 CPS.DS-4 CPS.DS-11 CPS.CM-4

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			● 利用する暗号技術については、信頼できる機関が発行する文書等（例：CRYPTREC 暗号リスト(電子政府推奨暗号リスト)）を参照し、安全でない方式を無効にする。 ● 機能や性能が限られた IoT 機器では、暗号等のセキュリティ対策を適用できない場合があるため、機器内に機微なデータを保管しない、ゲートウェイ等のネットワーク機器にてセキュリティ機能を補完する等の措置を実施する。	
		ライフサイクルを通じた暗号鍵の管理	● 暗号によりデータを保護する期間の全体にわたって、利用する暗号鍵を安全に管理する。その際、以下の事項に関して検討を行うことが望ましい。 - 暗号鍵管理システムの設計原理と運用ポリシー - 暗号アルゴリズム運用のための暗号鍵管理オペレーション対策 - 暗号アルゴリズムの選択 - 暗号アルゴリズム運用に必要な鍵情報の管理 - 暗号鍵管理デバイスのセキュリティ対策 - 暗号鍵管理システムのオペレーション対策 ※ 各事項における具体的な実施内容等については、IPA「暗号鍵管理システム設計指針（基本編）Ver. 1」等を参照されたい。	CPS.DS-5
		マルウェア対策の実施	● IoT 機器・システムをマルウェアから保護するため、「IoT 機器・システムに対するアップデートの適用」や「搭載するソフトウェアに対するインストール対策の実装」等の実施に加え、端末及びネットワーク上にて多層的に以下の対策を実施することが望ましい。 - 外部ネットワーク又は可搬媒体経由でファイル及びソフトウェアを取得する際にマルウェア検出を実施する。 ➢ 端末にマルウェア対策ソフトウェア（パターンファイル、振舞い検知等の方式による）を導入し、外部から取得した全てのファイルに対して使用前の検査を行う。 ➢ ネットワーク上にセキュリティ機器（例：IDS/IPS、ウェブアプリケーション・ファイアウォール）を導入し、セキュアでない外部サイトとの通信や不審な通信を検知し、適宜遮断等の対応を実施する。 - マルウェアの検知に利用するソフトウェア等のバージョンを、信頼できる出所を利用して、常に最新の状態に維持、更新する。 - パソコンやサーバ等の端末の状況及び通信内容などを監視し、異常、あるいは不審な挙動を検知した際に管理者に通知する。 - マルウェア等の脅威について最新の情報を収集する手段やプロセス（例：ISAC への参画、脅威インテリジェンスに係るサービスの利用）を整備する ● 機器の種類によっては、計算能力が低い、OS が実装されていない等の理由で十分なマルウェア対策を実装できない場合がある。そのような場合、かかる機器が接続する「上位の IoT 機器・システム」（例：IoT ゲートウェイ、ルータ）にて通信ファイル等に対するマルウェア検査を実施することが望ましい。	CPS.DS-10 CPS.CM-3
		IoT 機器・システムの十分な可用性の確保	● IoT サービス開発者又は IoT 利用者は、対象機器・システムの可用性に関する業務上の要求事項を特定し、機器・システムを設計、開発する。また、機器・システムの運用時においても、リソースの利用を監視・調整し、将来必要とする容量・能力を予測することが望ましい。 ● 対象において高い可用性の保証が求められる場合、通常稼働するものとは別に構成要素を複数用意しておき、異常が発生した際であってもシステム全体の停止を回避できるよう、システムを冗長化する。その場合、冗長化した構成要素への切替えを意図したとおりに行うため、あらかじめ試験を行っておくことが望ましい。	CPS.DS-6 CPS.DS-7 CPS.IP-4 CPS.IP-5

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			● 機器の故障、自然災害等によるデータの消失に備えるため、IoT サービス提供者又は IoT 利用者は、データ、ソフトウェア及びシステムイメージのバックアップを定期的に取得し、検査することが望ましい。 ● 他の機器・システム等との関係で高い可用性や信頼性が必要とされる場合、ネットワークの停止や停電が発生した場合でもローカルで動作を継続し、停電等から回復した場合にはスムーズに復旧する回復性(レジリエンス)を機器やサービスに組み込むことが望ましい。	
		IoT に適したネットワークの利用	● IoT 機器間又は IoT 機器とサーバの間の通信で利用するネットワークの方式(例:Wi-Fi、Bluetooth、LPWA、5G 等の移動通信)を、セキュリティ機能、通信速度等のパフォーマンス、以下に示すその他の観点を踏まえて決定する。 - 通信元の IoT 機器と通信先の物理的な距離 - IoT 機器の可動性の有無 - ネットワークの帯域幅 - 同時接続可能な機器の数 - 消費電力量	-
		適切なネットワークの分離	● IoT 機器・システムを構成するネットワークに関して、必要に応じて、共通のセキュリティレベルを持つセグメントを構築し、他のセグメントと論理的又は物理的に分離する。本番環境と開発環境、インターネット経由でアクセス可能な社内ネットワークと生産拠点の制御ネットワークの分離等がかかる例に該当し得る。生産拠点等の情報システム及び制御システムのネットワークについて、下記のように階層化を行う場合がある。 – 情報系ネットワーク 企業内で構築された LAN で、外部ネットワーク(インターネット等)との接続点に存在する。 – 制御情報系ネットワーク 情報系ネットワーク又は DMZ 上のサーバ等との間で、制御目的に使用するためのステータス情報やデータを転送する。 – 制御系ネットワーク 制御ネットワーク及びフィールドネットワーク上の機器(コントローラ)との間で、制御目的に使用するためのステータス情報やデータを即時転送するためのネットワークであり、制御に特化した高い応答性を持つ。 – フィールドネットワーク 制御ネットワークのコントローラ等の接続機器とフィールドに存在する機器の間の通信に用いられる。 ● 上記環境では、基本的に同一セグメント内でのみ通信を行い、セグメント間の通信を行う場合はファイアウォールやゲートウェイ等のネットワーク機器により制御する。 ● 可能であれば、安全計装用のネットワークを他のネットワークから分離する。	CPS.AC-7 CPS.AC-8 CPS.DS-9 CPS.CM-1
		IoT 機器・システムの設置場所等に対する物理的アクセスの制御	● IoT 機器・システムが設置される領域(例:事業所、サーバ室)を保護するために, 物理的セキュリティ境界を定めることが望ましい。 ● 定められた物理的セキュリティ境界の内部に認可されていない者がアクセスできないよう、適切な入退管理(例:IC カードによる認証)を行う。その際、機微なデータや重要なプロセスを取扱う資産が所在する場所については、組織内又は関係する取引先等であってもアクセスできる要員を最小限にする。	CPS.AC-2 CPS.CM-2

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			● 物理的セキュリティ境界内部に対するあらゆる物理的なアクセスの記録を保管しておき、定期的にレビューする。	
		IoT 機器・システムの構成要素（機器、ネットワーク等）の物理的保護	● 自然災害（例：火災、洪水、地震）や他の物理的な脅威（例：盗難、破壊、改造）に起因する障害に対処するため、IoT 機器・システム及びそれが設置される施設等は適切に保護（例：耐震性や火災への耐性の確保）されていることが望ましい。 ● 電磁波の放射等による情報漏えい（サイドチャネル攻撃）のリスクを最小限にするため、機微なデータを処理する機器を保護する。 ● IoT 機器・システムが外部からの物理的な脅威に晒されやすい場所（例：公共空間等の拠点外で管理者のいない場所）に所在し得る場合、以下を考慮することが望ましい。 - 耐タンパ化等により、末端の IoT 機器（センサ、アクチュエータ）を物理的な盗難、破壊、改造から保護する。そのような保護が限られる場合、機器・システムの利用者は物理的な脅威によるリスクが残存することを認識し、運用中に必要に応じて当該機器・システムが正しい状態で稼動しているかを確認することが望ましい。 - 暗号鍵等の機微なデータを取扱う機器内のコンポーネントを不正な開示や改ざんから保護する。	CPS.DS-8
		セキュリティ設計と両立するセーフティ設計の仕様化	● IoT 機器・システムの開発者は、セキュリティインシデントが結果的に機器・システムのセーフティ側面に及ぼし得るリスク（例：制御データの改ざんによる誤動作の発生、マルウェア感染による機器・システムの安全機能の停止）を認識し、それらに適切に対処する方策を検討する。有効となり得る方策として、例えば以下が挙げられる。 - 異常検知時にフェールセーフを実現する安全機能を実装する。 - 安全機能の動作に影響を与える可能性のある IoT システムに対する脅威を考慮し、当該安全機能を通信機能と分離する 等 ● IoT サービス開発者は、実装しようとするセキュリティ管理策が IoT システムとその安全機能の動作に与える影響も考慮して、実際に履行する管理策の検討を行う。	CPS.RA-4 CPS.PT-3
		セキュアな開発環境と開発手法の適用	● IoT 機器・システムの開発に係るヒトやプロセス、設備（開発環境）をより安全なものとするため、以下の点を考慮することが望ましい。 - 開発環境で業務に従事する人員（外部委託を含む）のセキュリティに係る能力 - 上記人員に対する開発環境へのアクセス制御 - 本番環境や別の開発環境との分離、環境間でのデータ移動の管理 - 開発環境の変更及び、保管されたコードに対する変更の監視 ● 機器・システムの開発に際して、フリーソフトウェア/オープンソースソフトウェア（FOSS）や関連 OS 及び利用コンポーネントの脆弱性管理を実施する。FOSS について、開発環境を狙った不正コードを含むコンポーネントも報告されており、適切な管理を通じて開発環境の汚染を抑制することが望ましい。 ● 以下に示すようなセキュアなソフトウェア開発の手順や手法を、IoT 機器・システムの開発に適用する。 - 安全なソフトウェア開発のためのライフサイクル - 言語別のセキュアコーディングに関する指針	CPS.AC-7 CPS.IP-3
		IoT 機器・システムにおけるセキュリティ機能の検証	● IoT 機器・システムの開発者、又は利用者は、当該機器・システムを現に利用し始める前に、セキュリティ機能を含む要求事項が設計した通りに実装され、正しく機能することを検証する必要がある。検証の実施に際しては、信頼できる外部事業者による検証サービスを利用することも想定される。	CPS.IP-3 CPS.DP-3

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			● 機器・システムの開発者、利用者及び（適切な場合）外部の検証サービス事業者は、検証実施に際して以下を実施することが望ましい。 - 準備：必要な情報の整理や検証目的、スコープの明確化を行う。 - 計画：検証に係る体制や環境を構築し、検証項目やその手法を具体化する。検証の手法には、静的手法（例：設計文書レビュー、ソースコード解析、バイナリ解析）と動的手法（例：ネットワークスキャン、既知脆弱性の診断、ファジング）等が存在するが、検証の目的や費用、検証実施者のスキル等を考慮して適切なものを選択することが望ましい。 - 検証の実施：計画段階で特定された項目について、合意された手法により検証を行う。 - 分析：検証結果に基づき、特定・検出された脆弱性や脅威がある場合、想定される影響や対応策の案を分析する。 - 報告：分析・整理された検証結果に基づき、検証報告書を作成する。 ※ IoT 機器をはじめとするネットワークに常時接続する機器、及び関連サービス（ただし、IoT 機器等が接続するサーバやシステム全体の検証は除く）のセキュリティ検証において、検証依頼者と検証サービス事業者が行うべき事項等を詳細化する場合は、別途、経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」等を参照されたい。	
		信頼できる IoT 機器やサービスの選定	● IoT の利用者、又は他の事業者から機器・システムのコンポーネントを調達してサービス等の開発・提供を行う事業者は、自身が取得する機器・システム及びコンポーネントのセキュリティに関する要求事項や、以下に例示するようなその他の要求事項を定めることが望ましい。 - 機器・システムに係るサポートの実施及び、それを受けられる期間 - 開発者や供給者が機器・システム等の仕様変更を行う際の事前の通知 - セキュリティ等に係る問題を検知した際の問合せ先 ● かかる要求事項を検討する際、既存のガイドライン等を参照して対象の特性を踏まえつつ、セキュリティ要求事項を具体化することが望ましい。 ＜業種横断的な参照ガイドラインの例＞ - ISO/IEC 27001:2013 - ISO/IEC 27017:2015 [対象：クラウドサービス] - NISTIR 8259 シリーズ [対象：個々の IoT 機器] - IoT セキュリティガイドライン Ver.1.0 [対象：IoT システム] ● 利用者自身で適切な IoT 機器・システム及び関連サービスの選定が困難な場合、販売店や Web サイト等で公開されている資料の活用、IoT 機器やサービスの選定が可能な事業者への相談等の対応を実施することが望ましい。	CPS.SC-1 CPS.SC-3 CPS.SC-4 CPS.DS-15
		IoT 機器・システムの出荷時における安全な初期設定と構成	● IoT 機器やサービスの運用前（設計・製造段階）の初期設定や構成を、一定水準のセキュリティが確保できるものとする。その際に考慮すべき IoT 機器やサービスの設定や構成、想定される対策例として以下のようなものがある。なお、一定水準のセキュリティとは、機器・システムごとに異なる。一方で、ポリシーで一定水準が定義される場合、当該ポリシーを参照するものとする。 - ネットワークポート、その他 USB やシリアルポート：運用前の段階で利用しないと考えられるものを、物理的又は論理的に閉塞する。 - ソフトウェアのバージョンとパッチ：IoT 機器・システムに運用前の段階で不要と考えられるアプリケーション、機能がある場合、利用者への提供までに削除、無効化、停止する。	CPS.IP-1 CPS.PT-2

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			- サービスの機能やデータへのアクセス制御：IoT 機器・システムが利用者にパスワードを要求する場合、初期段階も含めて製品のライフライクル全体をとおしてセキュリティ強度を高く維持できるようにする。 ● 特に IoT 機器は、初期段階に弱いパスワードが設定される場合が多く、初期段階でパスワード強度を上げるメカニズムが必要である。そのような措置として、例えば、機器ごとに固有の推測されにくいパスワードを用意する、又は機器ごとに初期パスワードが同一である場合に初回の利用時等に一定の複雑さを持つパスワードを変更しない限り利用できないようにする等が考えらえる。	
		IoT 機器・システムにおける運用開始時の正しい設置、設定	● IoT サービス開発者は、IoT 機器やシステムを構成するその他の設備を設置、設定する際、機器の動作仕様を考慮しつつ、想定されるセキュリティインシデントや危害を回避や軽減するために提示されたガイドやポリシーに従って業務を行い、運用開始までに動作状況を確認することが望ましい。 ● IoT 機器を公共空間や事業者の敷地外、住戸外等の外部のヒトが接触可能な場所に設置する場合、IoT サービス開発者/提供者は、不正な改造や不正なソフトウェアのインストール、ネットワークの不正利用防止についてあらかじめ留意しておくことが望ましい。	CPS.IP-1
第 2 の観点	ORG	利用者へのリスクの周知等の情報発信	● IoT 機器・システムの運用段階において、セキュリティ対策の一部を IoT 利用者が実施する必要があることから、IoT サービス開発者(IoT 機器製造者を含む)又は IoT サービス提供者は、 以下のようなサイバーセキュリティ関連情報について、想定されるリスクとともに利用者に発信することが望ましい。 – 提供する IoT 機器・システムの正しい利用方法（例：設定や構成の変更方法） – サポート対象の IoT 機器・システム及びその構成要素 – ソフトウェア更新の有無 – 利用者側で実施が必要な保守作業 – 脆弱性及び緩和措置に関する注意喚起 – サポート又はサービス提供の終了時期 – 利用者向け窓口の連絡先 ● 対策の内容の機密性等にも配慮しつつ、IoT サービス開発者(IoT 機器製造者を含む)又は IoT サービス提供者が、例えば以下の発信を通じて、機器・システムにおけるセキュリティ対策の水準を対外的に広報することも、利用者からの信頼を確保する上で有用と考えらえる。 – 取得している第三者認証等 – 適用している規格や対策の概要 – 情報セキュリティ報告書における取組み内容の紹介	-
		運用中における IoT セキュリティを目的とした体制の確保	● 自組織の IoT 機器・システム、サービスの提供又は利用に係るセキュリティポリシーに沿って、対象機器・システムのセキュリティに対する役割と責任の割り当てを行い、その内容を文書化した上で関係者に周知する。 ● 割り当てる役割と責任には、以下が含まれていることが望ましい。 - 意思決定等を行う経営層（CISO 等）及びその補佐 - 機器・システムの運用段階における対策の実装と運用 - IoT 機器・システムの運用に係るサービスの委託先の管理 - 機器・システムの運用担当者や利用者向けの意識向上、教育・訓練プログラム - 機器・システムの運用時における脆弱性やインシデントへの対応 ※ より具体的な実施内容等については、経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリ	CPS.RM-1 CPS.AE-2

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			ティ体制構築・人材確保の手引き 第1.1版」等を参照されたい。	
		過去の対応事例からの学習	● IoT 利用者又は IoT サービス提供者は、自身が管理する IoT 機器・システム又は関連するその他の機器・システムにおいて発生したセキュリティインシデントから得られた知見を、今後の対策強化に活用することが望ましい。 ● 取得できる知見の情報源として、例えば以下が挙げられる。 － 自社で発生したインシデントへの対応結果及び、対応後の原因分析 － 信頼できる外部機関（例：セキュリティベンダ、情報共有基盤（ISAC/ISAO）、政府機関、学会等）からの情報発信や注意喚起 ● 機密性の側面に留意する必要はあるが、実際に発生したセキュリティインシデントを、それに対する対応や事前に取るべきだった対策等を含め、利用者向けの教育のコンテンツとして用いることができる。 ● 取得した知見に基づき、機器・システムの管理者は、必要に応じて以下をレビューすることが望ましい。 － リスクアセスメントの結果（例：想定されるセキュリティインシデント等とその結果、機器・システムに潜むリスクの程度、脅威の整理結果への変更） － リスク対応の内容 － インシデントや脆弱性への対応体制や手順等	CPS.IP-7 CPS.IM-1 CPS.IM-2
	PRO	脆弱性対応に必要な手順等の整備と実践	● IoT サービス開発者又は IoT サービス提供者は、自身が開発、提供している機器・システムに係る脆弱性の情報を収集、分析、必要に応じて関係者に周知し、最終的にソフトウェアやファームウェアの更新等の措置を講じる必要がある。 ● 脆弱性対応の手順には、以下の対処が含まれていることが望ましい。 － 脆弱性情報の収集： 製品開発者が提供する情報や、セキュリティベンダやセキュリティ関連機関（IPA、JPCERT/CC、ISAC 等）がホームページやメール等で提供するアドバイザリ等を利用して情報収集を行う。また、自社製品に関する脆弱性情報に関する連絡を受けるため、対外的な窓口を設置することが望ましい。 － セキュリティ上の問題の有無に関する調査： 入手した脆弱性情報について、自社システム上の脆弱性の有無や問題が発生する条件等を調査する。 － 影響と対策の方向性の検討： 問題箇所が及ぼす影響を特定し、修正方法や回避方法を検討する。 － 対策作業計画の策定 対策作業を進める手順や期間等について計画を策定する。費用、人員等を勘案しつつ、機器・システムの利用部門（例：製造部門）とも十分にコミュニケーションをとったうえで、代替機でのテスト、対策実施に伴うサービスの停止と再開等を計画する。 － 対策の実施 作業計画に基づき対策を実施する。具体的な方法等については、「IoT 機器・システムに対するアップデートの適用」も参照されたい。	CPS.RA-2 CPS.IP-10 CPS.CM-7 CPS.RP-2
		インシデント対応手順の整備と実践	● セキュリティインシデントに対する迅速，効果的かつ順序だった対応を確実にするため、管理層の責任及び手順を確立することが望ましい。	CPS.AE-4 CPS.AE-5 CPS.RP-1 CPS.RP-2 CPS.CO-1 CPS.AN-1

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			● 組織は、自身の役割や対応の対象となるシステムの種別等を考慮して、例えば以下に挙げるようなインシデント対応組織を確立することが望ましい。 － IT システム：CSIRT（Computer Security Incident Response Team） － 製造現場：FSIRT（Factory Security Incident Response Team） － 製品・サービス：PSIRT（Product Security Incident Response Team） ● インシデント対応手順には、以下のプロセスを含めることが望ましい。 － 検知・受付連絡： 「IoT 機器・システムのモニタリング及びログの取得、分析」に示す組織内部の活動や、外部からの通報受付を通じて、インシデントの発生を検知する。 － トリアージ： 得られた情報に基づいて、事実関係を確認し、その情報を得たインシデント対応組織が対応すべきインシデントか否かを判断する。 － インシデント対応： インシデントにより生じた被害の特定、原因の分析を行ったうえで、被害の拡散を防止し、被害箇所の原因の根絶、修復を行い、復旧をする。 － 報告/情報公開 必要に応じて、組織内部への情報展開の他、メディアや一般に向けたプレスリリースや監督官庁への報告を行なう。 ※ より具体的な実施内容等については、JPCERT/CC「インシデントハンドリングマニュアル」等を参照されたい。	CPS.AN-2 CPS.AN-3 CPS.MI-1
		事業継続計画の策定と実践	● IoT 利用者又は IoT サービス提供者は、対象の IoT 機器・システムを含む自身が管理するシステム群の継続を、自社の事業継続計画（BCP）や事業継続管理（BCM）プログラムに組み込むことが望ましい。 ● 策定する BCP には、以下の事項を含めることが望ましい。 － 対象業務及びシステム群を対象とした BCP の実施・運用体制 － 想定する危機的事象 － 被害状況の想定 － 業務及びシステムの復旧優先度、目標復旧時間 － システム構成要素ごとの対策目標 ● BCP/BCM において規定している事業継続上の要求事項を満たすため、例えば以下に示す対策要件のレビューや追加的な実装を行うことが望ましい。 － IoT 機器・システムのモニタリング及びログの取得、分析 － インシデント対応手順の整備と実践 － IoT 機器・システムの十分な可用性の確保 ● BCP/BCM においては、危機的事象として、自然災害のみならず、サイバー攻撃を考慮し、以下に示すような特性を十分に踏まえることが望ましい。 － 災害等とは異なり、標的を定めて攻撃が行われることが多い － 被害状況を把握しづらく、早期発見には障壁がある － 対処後も再度攻撃を受ける可能性があるため、原因究明が必要	CPS.AE-4 CPS.AE-5 CPS.RP-3 CPS.CO-2 CPS.CO-3
		IoT 機器・システムの適正な使用	● IoT サービス開発者又は IoT サービス提供者は、IoT 利用者に対して、機器・システム及び関連するサービスの適正な使用に関するガイダンスを提供することが望ましい。 ● IoT 利用者は、IoT サービス開発者/提供者から提示されるガイダンスに従い、機器・システムを設定し、利用する。	CPS.IP-1 CPS.PT-2

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			● 利用者に提示されるガイダンスの内容には以下が含まれ得る。 － 設置方法 － 安全な使用環境（例：ネットワーク設定、構成）、使用方法 － IoT 機器が収集する情報 － セキュリティアップデートの適用方法 － 適格なパスワードの基準 － サポート期間 ● 上記に加え、IoT 利用者には機器・システムの使用に伴い発生し得る、例えば以下のようなセキュリティインシデントや危害も通知されることが望ましい。 － IoT 機器のマルウェア感染 － 個人情報の漏洩 － 企業情報の漏洩 － IoT 機器の踏み台化	
		IoT 機器・システムの適正な運用・保守	● IoT サービス開発者又は IoT サービス提供者は、提供する機器・システムの運用手順を文書化し、利用者に対して示すことが望ましい。また、IoT 利用者及び IoT サービス提供者は、提示された運用手順に沿って、機器・システムの操作や保守を行う必要がある。 ● 提示する機器・システムの運用・保守に関する手順には、例えば以下の事項に関する説明を示すことが望ましい。 － 機器の（再）起動又は停止の手順 － バックアップの取得及び管理 － 外部媒体（例：USB メモリ）の取扱い － アップデートの適用 － 障害等が発生した際にサポートを受けるための連絡先 － 機器・システムのパフォーマンスや問題事象等の監視 ● 機器・システムを外部の事業者に委託等する場合、IoT 利用者及び IoT サービス提供者は、作成した運用・保守に関する手順書を委託先に示し、契約期間中も手順の遵守を定期的に確認することが望ましい。	CPS.IP-1
	SYS	運用中における法令及び契約上の要求事項の遵守	● IoT 機器・システムの提供又は利用に係る組織は、新たに機器・システムを開発する場合、あるいは既に開発されている機器・システムにおいて関連する法令等が変更された場合に、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みをレビューし、最新に保つことが望ましい。 ● 関連する法令、規制及び契約上の要求事項を特定する際には、対象機器・システムに限定せず、全社的に日頃より自組織が受ける法的な規制やガイドラインを明確化し、各システムが規制対象となる場合の法令等と遵守事項、罰則などを文書化しておく。 ● 特に個人情報保護法は 3 年毎の見直しに連携し、業界向けのガイドラインの改定もあるため留意する。また、GDPR を始めとする他国の規制について、関連があれば文書化しておく。	CPS.GV-2 CPS.DP-2
		継続的な資産管理の実施	● IoT 機器・システムの運用を担当する IoT サービス提供者又は IoT 利用者は、管理対象の IoT 機器・システムの資産目録（インベントリ）を作成し、継続的に管理する。 ● 資産目録では、各資産に管理責任者や重要度等を割り当て、手動又は自動的な方法により、正確かつ最新の内容となるように管理する。 ● 管理対象となる資産及び管理すべき情報(例)には以下が含まれる。 － ハードウェア	CPS.AM-1 CPS.AM-6 CPS.RA-1 CPS.CM-6

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			機器種別、名称、ネットワークアドレス、管理者、性能情報、OS 情報 － ソフトウェア及びファームウェア 名称、バージョン、ライセンス情報、アップデートの適用状況 － 取扱われるデータ 名称、種別（例：個人情報、営業秘密）、重要度、管理者、保管媒体、 利用目的	
		プログラムソースコード及び関連書類の保護	● 想定していない機能の組込みや意図しない変更を回避するため、IoT サービス開発者又は IoT サービス提供者は、対象となる IoT 機器・システムに関連したプログラムソースコード及び関連書類（例：設計書、仕様書、検証計画書、妥当性確認計画書）へのアクセスや変更履歴（例：作成日時、変更日時、変更点）を厳重に管理する。 ● プログラムソースコードはデータベース（リポジトリ）に格納し、以下に示すような管理を適切に行いつつ、複数の開発者間で閲覧及び編集を行えるようにする。 － プログラムソースコードを運用システムの中に保持しない。 － 委託先等も含めた開発要員によるリポジトリへのアクセスを最小限にする。 － リポジトリ及び格納されているプログラムソースコードへの全てのアクセスのログを取得し、保持する。 － プログラムソースコードの保守及び複製を行う際は、あらかじめ定められた管理手順に従う。 － プログラムソースコードの公開を意図している場合、その完全性を保証するために追加の管理策（例：デジタル署名）を考慮することが望ましい。	CPS.AC-1 CPS.AC-4 CPS.AC-5 CPS.AC-6 CPS.AC-9
		IoT 機器・システムのモニタリング及びログの取得、分析	● 機器・システムの故障、不審な動作等を早期に検知し、対処するため、対象の IoT 機器・システムの運用時において、IoT 利用者又は IoT サービス提供者は、利用者の活動、機器・システムの挙動、セキュリティに係る事象を記録したログを取得し、安全に保持し、定期的にレビューすることが望ましい。 ● 取得及びレビューの対象となり得るもの、現に取得やレビュー等を行おうとする際の注意事項等として、例えば以下が挙げられる。 ＜対象となる機器・システムの例＞ － 末端の IoT 機器（センサ及びアクチュエーター） － 制御システムを構成する機器等（例：PLC、DCS、SCADA） － ネットワーク機器（例：IoT ゲートウェイ、ルータ、ファイアウォール） － サーバ（クラウドとオンプレミスの双方を含む） － 業務用端末 ＜対象となり得るログ等の例＞ － 機器・システムに対するアクセス（例：ユーザ認証の成功及び失敗） － 機器・システムの操作履歴、特に正常でないとみなされ得る動作（例：事前に想定されていない外部サーバ等との通信、不正なプログラムのインストール） － センサ又はアクチュエータの通常の範囲を超えた値 － 対象システムの構成変更 － 対象システム内又は外部ネットワークとの間のネットワークトラフィック － IoT 機器又はシステムを構成するその他の機器の停止 － プロセッサとメモリの使用状況 － IoT 機器の物理的な位置 － 温度や湿度等の機器が位置する環境の状況 ＜注意事項等＞ － ログの取得や保管、通信等にかかるリソースを考慮すると、あらゆる機器からあらゆる種類のログを取得し、レビューすることは現実的ではないため、対象となる機器やログの種類に優先順位をつける必要がある。例えば、ログの取得や保管、異常の報告ができない IoT 機器が含まれる場合、システムを構成す	CPS.DS-9 CPS.PT-1 CPS.AE-3 CPS.CM-1 CPS.CM-2 CPS.CM-5

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			るサーバやネットワーク機器でモニタリングやログの取得を行う必要がある。 － 取得し、レビューするログの正確性を担保するため、IoT システム内で時計を同期させることが望ましい。 － 論理的又は物理的なアクセス制御、バックアップの取得、改ざん検知、暗号化等を通じて、機器・システムのログ機能及びログを、改ざん及び不正なアクセスから保護することが望ましい。	
		IoT 機器・システムに対するアップデートの適用	● IoT 機器・システムを構成するソフトウェアやファームウェアの更新は、以下の機能の実装等を通じて、不正アクセス等の脅威に対して安全に実施される必要がある。 － 更新プログラムは、IoT 機器・サービスの開発者の正規のウェブサイト等、信頼できるソースから提供されるべきである。 － 更新プログラムを受信する機器は、更新を開始する前に、当該プログラム及び発信者の完全性及び真正性を検証する必要がある（例：デジタル署名、署名証明書、署名証明書チェーンの検証）。 － 更新が無線ネットワーク経由で遠隔から行われる場合、通信経路は適切な方式により暗号化されるべきである。 － 更新に利用される暗号鍵は、完全性と真正性を保護するために安全に管理されるべきである。 － 更新を実行することにより機器・システムの既存の運用が悪影響を受けないよう、更新の実行前にあらかじめ動作検証等を行うことが望ましい。 ● 更新を実行したことにより IoT 機器・システムのセキュリティレベルが低下する事態を防ぐため、遠隔からの更新処理は、完全に成功するか、失敗したとしても以下に示すようにロールバック可能な状態となっている必要がある。 － 更新の失敗に備え、ソフトウェアやファームウェアをロールバックする仕組みを実装することが望ましい。 － 平時の運用において、不正なダウングレードやロールバックがなされないよう、それらを防止する仕組みを実装することが望ましい。	CPS.MA-1 CPS.MA-2
		IoT 機器・システムの安全な廃棄又は再利用	● IoT 機器やIoTシステムを構成するその他の機器を廃棄したり、中古品として売買したりする際、保管されているデータの重要度や各種法の実行可能性等を加味しつつ、以下に挙げる方法等に基づき、機微情報やライセンスされたソフトウェア等の消去、あるいはデータの上書きを行うことが望ましい。 － データ抹消ソフトウェア（データに異なるランダムなデータを複数回上書きしてデータを抹消するソフトウェア）によりファイルを抹消する － ハードディスクを消磁装置に入れてディスク内のデータを抹消する － 媒体を物理的に破壊する － データが暗号化された状態で保管されている場合に、暗号鍵を消去することで、元データへと複合できないようにする － 機器を工場出荷時の状態に初期化する ※ データ保管媒体の安全な廃棄方法に関するより詳細な情報については、米国国立標準技術研究所（NIST）「SP 800-88 rev.1 媒体のデータ抹消処理（サニタイズ）に関するガイドライン」（IPA 翻訳）等を参照されたい。	CPS.IP-6
第 3 の観点	ORG	IoT 機器・システムの運用・管理を行う者に対する要求事項の特定	● IoT 利用者又は IoT サービス提供者は、現に機器・システムの運用・管理を行う自社又は委託先等の担当者が、安全で信頼できる運用を実現しようとするにあたり有すべき適格性（知識や技能等）に関する要求事項を特定し、担当者を割り当てる際に十分考慮することが望ましい。	CPS.SC-5

第 3 軸における観点	実装先[39]	対策要件	実際に講じる対策の例	対応する CPSF の対策要件 ID
			● かかる適格性に関する要求事項には、業種や業務によって様々なものが含まれ得るが、担当する業務の執行に係る知識や経験、それらと関連する限りにおいてパーソナリティ側面等が考慮され得る。 ● 業種や業務によっては、業法や関連する資格制度等により能力が規定され、資格の取得等が（事実上）義務化されている場合がある。	
		IoT 機器・システムの運用・管理を行う者に対する要求事項の遵守の確認	● IoT 利用者又は IoT サービス提供者は、IoT 機器・システムの運用・管理を担当する者（候補者を含む）が特定された要求事項を満たしているかどうかを、業務の実施前又は実施中の適切なタイミングで、例えば以下の手段により確認することが望ましい。 – 推薦状（例えば、業務や人物に関するもの） – 該当者の履歴書（記載が正確であるかの確認を含む） – 業務に係る資格等の（公的な）証明書 – 信用情報や犯罪履歴等の入手 ● 上記の確認は、プライバシー保護及び雇用に関する法令の全てを考慮に入れた適切な方法で行われなければならない。	CPS.SC-5

2234

別紙4

IoTセキュリティ・セーフティ・フレームワーク Version 1.0
実践に向けたユースケース集
(概要版)

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. 本ユースケース集の構成

3. 各ユースケースの概要

- 3-1.家庭用ガス給湯器の遠隔操作
- 3-2.ドローンを活用した個人による写真撮影
- 3-3.物流倉庫内のAGVによる自動ピッキング
- 3-4.化学プラント施設内の蒸留工程の自動制御
- 3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
- 3-6.金属製造現場の温度センサ等による製造設備の状態監視

1. IoT-SSFの概要（1/2）

- IoTセキュリティ・セーフティ・フレームワーク」（以下、「IoT-SSF」という。）は、IoTが社会に効果的に需要できるようIoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するための「基本的共通基盤」を提供するものである。

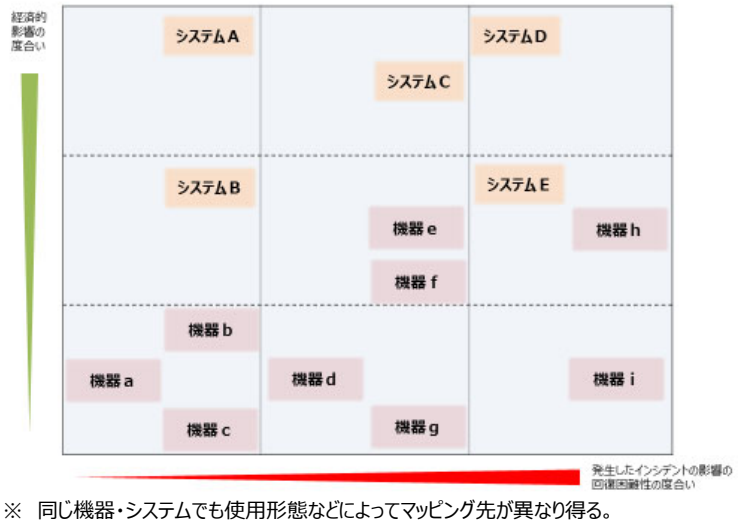
IoT-SSFの基本情報

背景	• サイバー空間とフィジカル空間をつなぐ機器・システムのセキュリティ・セーフティに関して、包括的に課題を捉える**統一的な手法が欠如**しているため、それぞれの分野/業界において別々の検討プロセスを経て、**独自のセキュリティ・セーフティ対策等が設定されることが懸念される**。 • それぞれの対応策に不整合が生じれば、**社会として新たな仕組みを受容・管理していくためのコストが増大する**おそれがある。
目的	• **異なる分野/業界のプレーヤー**がサイバー空間とフィジカル空間をつなぐ機器・システム、つまり IoT 機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するための**「基本的共通基盤」**を提供し、**IoTという新たな仕組みを社会として効果的に受容できる**ようにすることを目的とする。
想定読者	• IoTを活用してサイバー空間とフィジカル空間をつなぐ新たな仕組み・サービスを実現しようとする者 • そのような新たな仕組み・サービスで活用されるIoT機器・システムの開発を行う者 • そのような新たな仕組み・サービスを適切に管理していく制度・環境を実現していこうとする者 • そのような新たな仕組み・サービスを受ける者

1. IoT-SSFの概要（2/2）

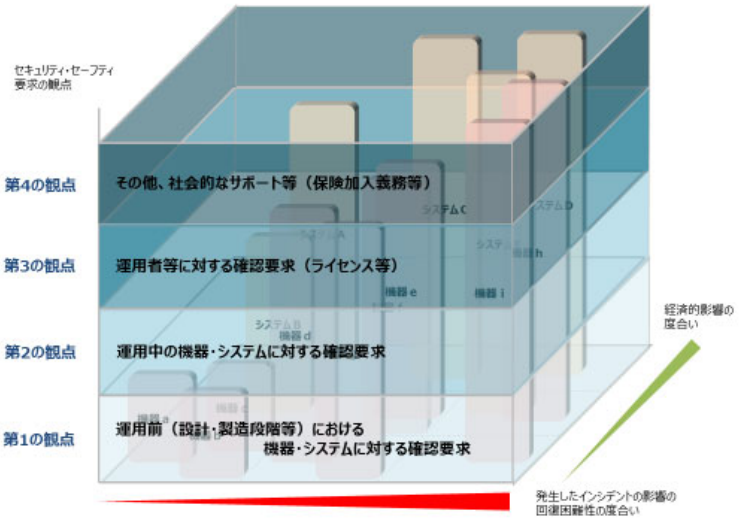
- 本フレームワークで、IoT機器・システムをカテゴライズし、カテゴリごとに求められるセキュリティ・セーフティ要求の観点を把握・比較することにより、**それぞれに求める対策の観点・内容の整合性を確保できる**。

フィジカル・サイバー間をつなげる
機器・システムのカテゴライズのイメージ



※ 同じ機器・システムでも使用形態などによってマッピング先が異なり得る。
例えば、機器ｇと機器ｈが同じ機器で異なる使用形態である場合などがあり得る。）

カテゴリに応じて求められる
セキュリティ・セーフティ要求の観点のイメージ



1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. ユースケース集の構成

3. 各ユースケースの概要

3-1.家庭用ガス給湯器の遠隔操作
3-2.ドローンを活用した個人による写真撮影
3-3.物流倉庫内のAGVによる自動ピッキング
3-4.化学プラント施設内の蒸留工程の自動制御
3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
3-6.金属製造現場の温度センサ等による製造設備の状態監視

2-1.「本稿の位置付けと構成」の概要

- IoT-SSFの概要や本稿の位置づけと構成、想定読者と利用用途を記載する。
- 本稿における記述はあくまで一例であり、事業者等による実際の適用に当たっては本稿に必ずしも記述されていないリスクや対策等が新たに抽出され得ることに留意されたい。また、本資料はユースケース集の概要版であるため、詳細については本文を参照されたい。

1-1 「IoTセキュリティ・セーフティ・フレームワーク」の概要

- IoTという新たな仕組みを社会として効果的に受容できるにすることを目的として、IoT機器・システムについて、リスクの捉え方とその対応に係る基本的な考え方を集約した3つの軸を活用し、機器・システムをカテゴライズするとともに、適切な対策の内容を整理して比較・検討することを提案している。

1-2 本稿の位置づけと構成

- 本稿では、今後様々な分野/業界のプレーヤーが、IoT-SSFを「基本的共通基盤」として活用するために、既存のリスクマネジメントのプロセスも考慮しつつ、一連のIoT-SSFの適用の流れを複数のユースケースを用いて例示する。
- 1章を導入として、2章ではユースケース選定の考え方(2-1)や各ユースケースに共通する記載項目(2-2)、6件の具体的なユースケース(2-3)を記述する。
- 添付としては、本編でも参照されるセキュリティ、セーフティの確保に資する対策要件（添付A）、添付Aに示された対策要件ごとに実際に講じる対策の例（添付B）を整理している。これらは各ユースケース固有の事情に依存しない一般的に適用し得る内容を示しているため、想定読者において具体的な対策を検討する際に適宜参照されたい。
- 本稿における用語法は、CPSF及びIoT-SSFに準じることとする。各種用語定義については、それらを参照されたい。
- 個別のユースケースに記載される対策としてはセキュリティに関連した対策を記述し、セキュリティに直接関連しない対策（例：機器・システムの経年劣化による欠陥や故障に対する対策）については本稿の対象外とした上で、これらを含む対策の整理については本稿の改訂時における課題とする。

1-3 想定読者と利用用途

主にIoT機器・システム及び関連サービスに係る様々な主体（事業者）により活用されることを想定する。

- IoT機器・システムを通じて提供されるサービスのユーザ （IoT利用者）
- IoT機器・システムを通じて提供されるサービスの開発者 （IoTサービス開発者）
- IoT機器・システムを通じて提供されるサービスの提供者 （IoTサービス提供者）
- IoT機器・システム及び関連サービスを適切に管理する制度・環境を検討する者

2-2.「対象となるユースケース」の概要

- 選定基準を踏まえて６種類のユースケースを選定する。

No	利用者の区分	利用環境	ユースケース	想定する適用主体	具体的な選定理由
1	個人又は家庭	家庭	**家庭用ガス給湯器の遠隔操作**	IoTサービス開発者、IoTサービス提供者(ガス給湯器製造事業者)	• 家庭用ガス給湯器は現状多くの住宅等に備えられており、その遠隔操作についても、今後利用の拡大が見込まれるため • インシデントが利用者の負傷につながりやすく、セーフティの側面がより重要となるケースであるため
2		公共空間	**ドローンを活用した個人による写真撮影**	IoTサービス開発者、IoTサービス提供者(ドローン機器事業者)	• 多種多様な活用方法が想定されるドローンは、ビジネス用途を含めて、今後様々な業界で利用の拡大が見込まれるため • 利用者に限らず周囲のヒトやモノへ被害を及ぼす可能性があり、利用者のスキルや社会的な制度等が要求事項として含まれ得るため
3	事業者(主に産業)	物流現場	**物流倉庫内のAGVによる自動ピッキング**	IoT利用者(物流事業者)	• AGVは様々な利用シーンでの活用が想定される機器であり、物流業界や製造業界等において今後利用の拡大が見込まれるため • 機器・システムの停止等が、サプライチェーンにおける多くのステークホルダーに影響しやすいケースであるため
4		製造現場(原料製造)	**化学プラント施設内の蒸留工程の自動制御**	IoT利用者(プラント事業者)	• 自動制御システムは既に多くの現場で採用されており、特にPA（Process Automation）技術を活用する事業者にとって参考になると考えられるため • 自動制御システムの停止等、可用性の損失が課題になるケースであるため
5		製造現場(製品製造)	**工場内のロボットによる部材加工作業（溶接工程）の自動化**	IoT利用者(自動車部品製造事業者)	• 製造現場におけるロボットは引き続き利用の拡大が見込まれており、特にFA（Factory Automation）技術を活用する多くの事業者にとって参考になると考えられるため • 制御データの改ざんによる異常動作及びそれに伴う品質劣化等が課題になるケースであるため
6			**金属製造現場の温度センサ等による製造設備の状態監視**	IoTサービス開発者、IoTサービス提供者(サポート事業者)	• 温度センサ等による設備の状態監視は産業用途（例：原料製造、製品製造）における共通的な要素であり、多様な現場にて参考になると考えられるため • 状態監視は品質管理上、重要な要素であり、これらに関連するインシデントが事業者にとっての大規模な経済影響等につながりやすいため • 遠隔にて設備の状況を監視する点は、各種サービス業においても参考になると考えられるため

2-3.「ユースケースにおける記載事項」の概要

- CPSFでは、「分析対象の明確化」、「想定されるセキュリティインシデント及び事業被害レベルの設定」、「リスク分析の実施」及び「リスク対応」のステップでリスクマネジメントを実施するとしている。
- 上記を踏まえ、以下のステップでリスクマネジメントを実施し、個別のユースケースを整理した。

1 リスクアセスメント、リスク対応に向けた事前準備

- 事前準備として必要となる以下の情報を整理する。
  - ✓ 対象ソリューションの概要
  - ✓ ステークホルダー関係図
  - ✓ システムを構成する機器の一覧
  - ✓ システム構成図、データフロー図
  - ✓ リスク基準

2 リスクアセスメント

- 第1軸「回復困難性の度合い」及び第2軸「経済的影響の度合い」の判断基準を考慮し、IoT機器・システムをマッピングする。
  - ✓ 想定されるセキュリティインシデント等とその結果の特定
  - ✓ 機器・システムの重要度の判断基準及び判断された重要度の一覧
  - ✓ マッピング結果の整理と評価の実施

3 リスク対応

- リスク対応を行うステークホルダーが実際に講じる対策を以下の項目に沿って整理する。
  - ✓ システムを構成する機器ごとの脅威の整理
  - ✓ 脅威に対する対策の整理
  - ✓ 整理した対策に対する意思決定

※想定読者に示したIoT利用者、IoTサービス開発者、IoTサービス提供者において、リスクマネジメントに関連する部門は多岐にわたると想定される。したがって、適用主体においては対応部署の特定は慎重に行うことが望ましい。また、社内の情報システム部門や情報システムの担当者、製品の開発者、工場の生産技術担当者等の現場の担当者だけではなく、それらを管理する経営層やリスク管理部門等も一体となって全社的にリスクに対応することが望ましい。

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. 本ユースケース集の構成

3. 各ユースケースの概要

3-1.家庭用ガス給湯器の遠隔操作

3-2.ドローンを活用した個人による写真撮影

3-3.物流倉庫内のAGVによる自動ピッキング

3-4.化学プラント施設内の蒸留工程の自動制御

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化

3-6.金属製造現場の温度センサ等による製造設備の状態監視

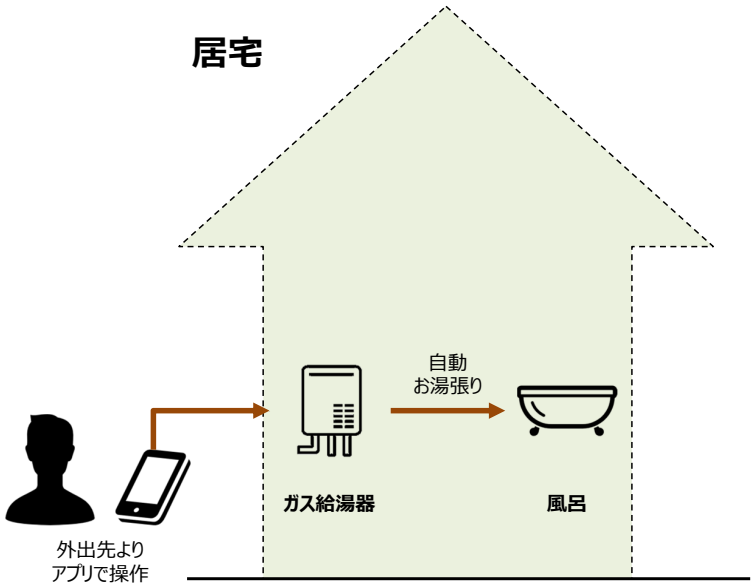
3-1.ガス給湯器の遠隔操作（ガス給湯器）

①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースの適用主体は、ガス給湯器の製造元であるスマートホーム向けのIoT機器を開発・生産・販売する事業者とする。
- 当該事業者は、既にスマートホームを供給する事業者等と協力して製造販売しているガス給湯器を活用して、新たにIoT機器サービスを企画しており、サイバーセキュリティに関するリスクを懸念している。

- 外出先よりスマートフォンの専用アプリケーションを活用して、自宅のお風呂のお湯張りを行う。
- なお、ガス給湯器は「自然給排気式・開放式」以外の機器を想定している。これは、「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（令和2年7月）にて「自然給排気式・開放式」の遠隔操作が禁止されているため。（※）

※経済産業省「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（令和2年7月）では、「自然吸排気式」及び「開放式」以外の機器において「リスク低減策を講じることにより遠隔操作に伴う危険源がないと評価されるもの等の基準に合致し、危険が生じるおそれがないものは、操作可能」とされている。

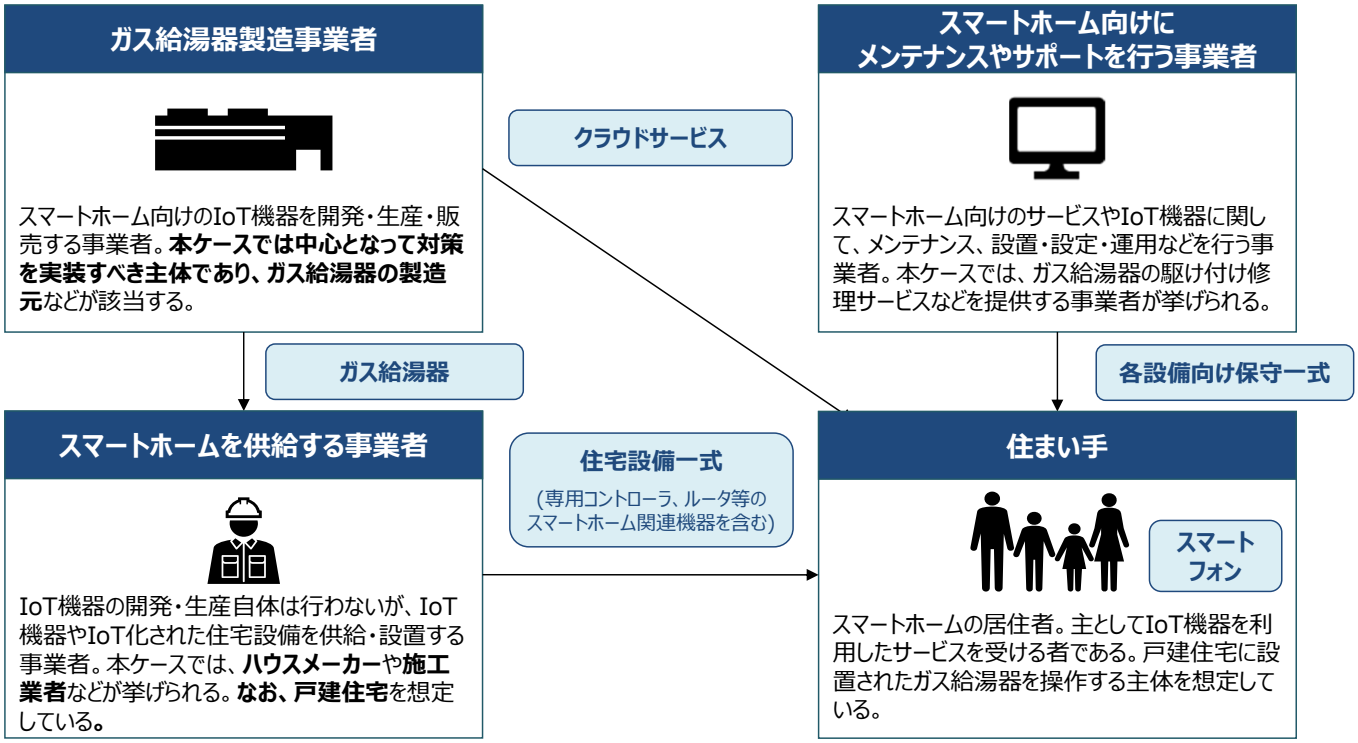


［参考］経済産業省「令和２年度 産業保安等技術基準策定研究開発等事業 （電気用品等製品の IoT化等による安全確保の在り方に関する動向調査）」等

3-1.ガス給湯器の遠隔操作（ガス給湯器）

①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

- ステークホルダーは、「スマートホーム向けIoT機器の事業者」「スマートホームを供給する事業者」「スマートホーム向けにメンテナンスやサポートを行う事業者」「住まい手」の４者。



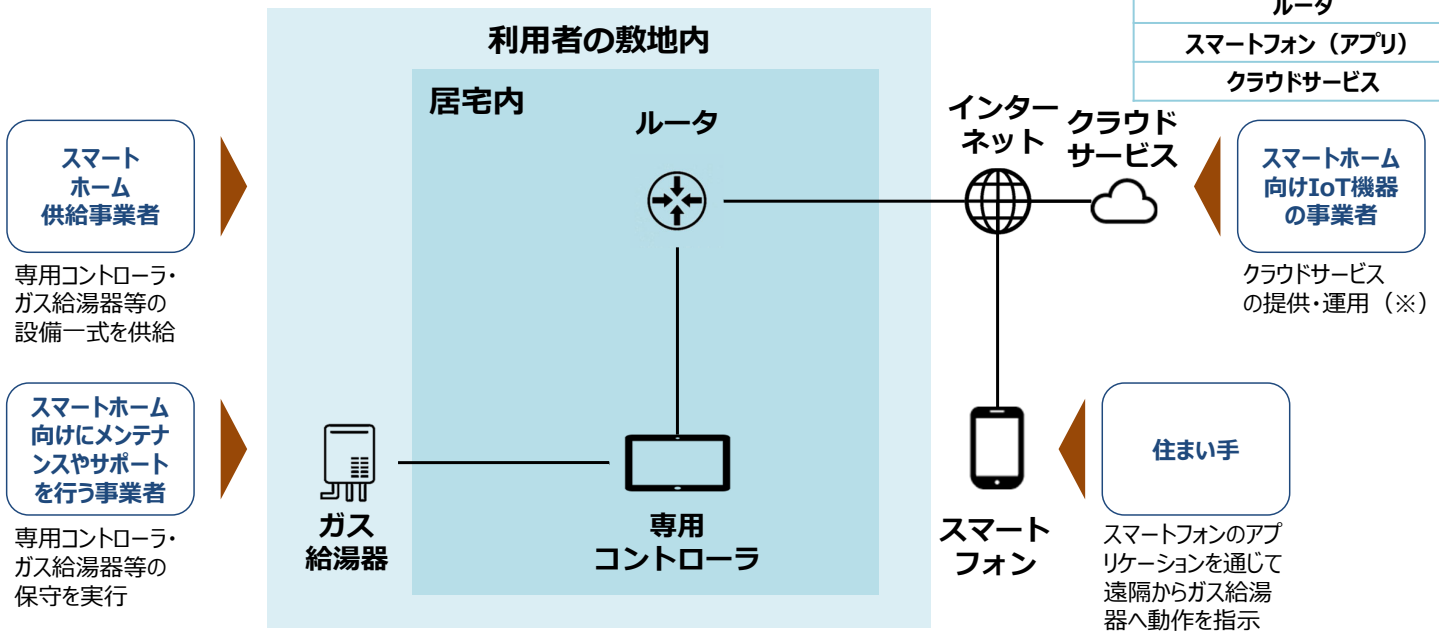
[参考] 経済産業省「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドラインスマートホームガイドライン」等

3-1.ガス給湯器の遠隔操作（ガス給湯器）

①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定する。

システムを構成する機器の一覧
ガス給湯器
専用コントローラ
ルータ
スマートフォン（アプリ）
クラウドサービス



※実際の運用は他のITサービス事業者に委託する場合がある。

[参考] 経済産業省「令和２年度 産業保安等技術基準策定研究開発等事業 （電気用品等製品の IoT化等による安全確保の在り方に関する動向調査）」等

3-1.ガス給湯器の遠隔操作（ガス給湯器）
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・システムにおいて想定されるセキュリティインシデント及び想定される被害（例）を整理。

分類	想定されるセキュリティインシデント	想定される被害(例)
スマートホーム向けIoT機器の事業者にとってのリスク	クラウドサービスから専用コントローラに送信される**データがネットワーク上で改ざん**されることによって、ガス給湯器が想定していない動作をする。	住まい手が異常に気づかずに入浴することによって、やけど等を負う。その結果、**製品回収等が生じ得る。**また、**製品・サービスの品質について利用者の間に疑念が広がり得る。**
スマートホーム向けにメンテナンスやサポートを行う事業者にとってのリスク	開発するアップデートプログラムが改ざんされ、そのまま配信されることで、配信先の専用コントローラ等が**マルウェア感染**し、想定していない動作をする。	住まい手が異常に気づかずに入浴することによって、やけど等を負う。その結果、**製品回収が生じ得る。**また、**サポートの品質について利用者の間に疑念が広がり得る。**
住まい手にとってのリスク	改ざんされたアップデートプログラムの配信等により専用コントローラが**マルウェア感染**し、ガス給湯器が想定していない動きをする。	異常に気づかずに入浴することで、**やけど等を負う可能性がある。**
	悪意のある攻撃者やIoT機器・サービスの事業者が、クラウドサービスに対して**不正アクセス**する。	**個人情報が流出し得る。**
	クラウドサービスからから専用コントローラに送信される**データをネットワーク上で改ざん**されることによって、ガス給湯器が想定していない動作をする。	異常に気づかずに入浴することで、やけど等の重症を負う。その結果、**生活に支障をきたし得る。**
スマートホームを供給する事業者にとってのリスク	住まい手に対して注意喚起(例：利用方法の説明等)を怠る。	ガス給湯器が停止する可能性があり、サービス提供における過失が認められ得る。

※:その結果として、契約上の責任が問われ得る。

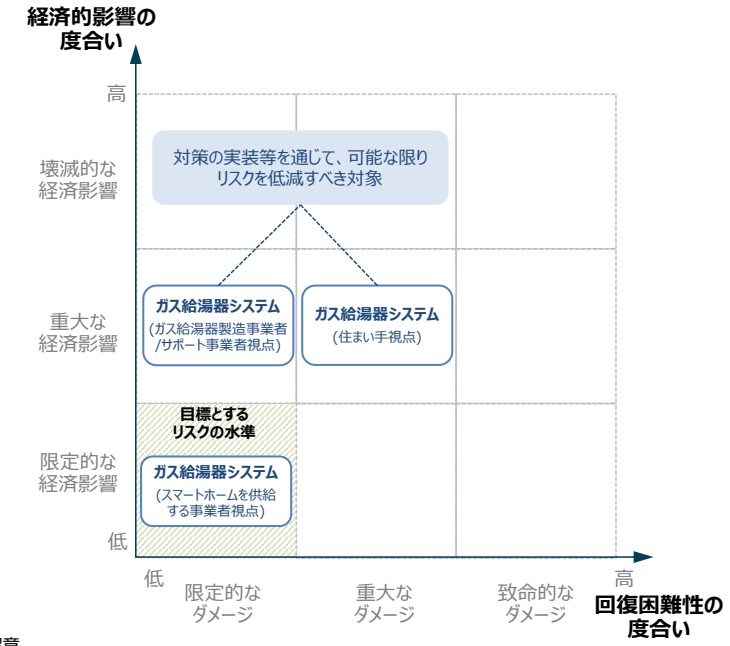
3-1.ガス給湯器の遠隔操作（ガス給湯器）
②リスクアセスメント->マッピング結果の整理と評価の実施

- 誤動作等により被るリスクが大きくなり得ると想定される「住まい手」は、一般にセキュリティに関する知見を十分に持たない場合が多いため、IoT-SSFの適用主体である「ガス給湯器製造事業者」は、これを考慮してリスクの低減に努める必要がある。

リスクの大きさ（※1）

ステークホルダー	回復困難性の度合い	経済的影響の度合い(※2)
スマートホーム向けIoT機器の事業者	• 従業員が重症を負う可能性は低い。	• 大規模な製品回収につながるおそれがある。
スマートホーム向けにメンテナンスやサポートを行う事業者	• 従業員が重症を負う可能性は低い。	• 開発するアップデートプログラムが改ざんされ、大規模な製品回収につながる可能性がある。
住まい手	• 個人情報が流出する可能性がある。 • やけど等の重症を負う可能性がある。	• 重症を負った場合、生活に支障をきたい得る。
スマートホームを供給する事業者	• 従業員が重症を負う可能性は低い。	• サービス提供における過失が認められ得る。

想定されるリスク(例)のマッピング結果

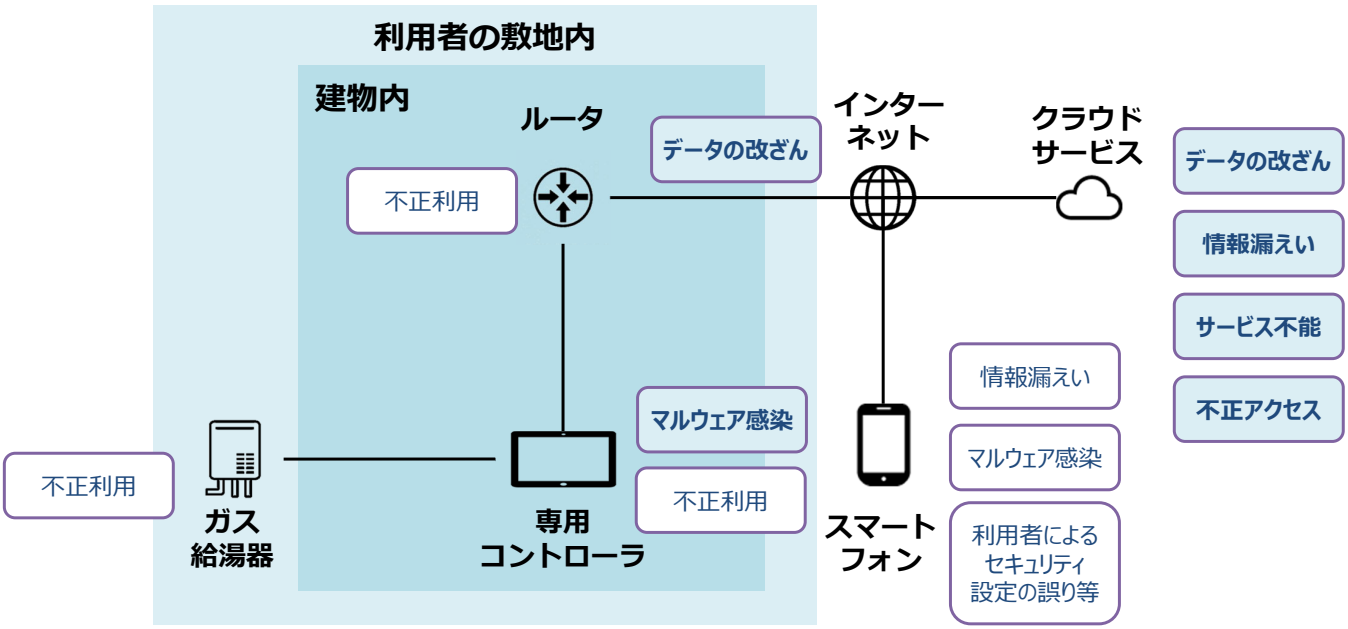


※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->脅威に対する対策の整理

- 適用主体であるIoT機器・サービスの事業（ガス給湯器等の製造元）は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

住まい手にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
自社製品・サービスの利用者をけがや、やけどから守るための対策の徹底	• IoT機器・システムの出荷時における安全な初期設定と構成 • セキュリティ設計と両立するセーフティ設計の仕様化
ガス給湯器システムに対するリスクや安全な使用方法に関する情報提供の実施	• 利用者へのリスクの周知等の情報発信 • 運用手順や利用手順の文書化等の運用・管理を行う者への支援の実施 • IoT機器・システムの運用・管理を行う者への要求事項の特定 • IoT機器・システムの運用・管理を行う者に対する要求事項の遵守の確認

ガス給湯器製造事業者(自身)にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進	• 運用前（設計・製造段階）における法令及び契約上の要求事項の遵守 • 企画・設計段階におけるセキュリティ要求事項の分析及び仕様化 • セキュリティ設計と両立するセーフティ設計の仕様化

サポート事業者にとってのリスクを低減するため対応を要請する対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
ガス給湯器に対する安全なアップデート等の脆弱性対応の実施	• プログラムソースコード及び関連書類の保護 • IoT機器・システムに対するアップデートの適用

※セキュリティインシデントによっては、ガス給湯器製造事業者はガス供給事業者と連携して対応することが必要となる場合がある

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->脅威に対する対策の整理

- 想定される脅威を踏まえ、第3軸「求められるセキュリティ・セーフティ要求」における観点ごとにスマートホーム向けIoT機器・サービスの事業者にて実装が想定される対策要件を整理する。

スマートホーム向けIoT機器・サービスの事業者にて実装が想定される対策要件の例

第３軸	実装先	想定される脅威（例）	対策要件
第１の観点	ソシキ・ヒト	全般[1]	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の明確化
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
		全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		不正アクセス	適切な水準のアクセス制御の実施
		全般	IoT 機器・システムにおける運用開始時の正しい設置、設定
第２の観点	ソシキ・ヒト	全般	利用者へのリスクの周知等の情報発信
		全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
	プロシージャ	全般	インシデント対応手順の整備と実践
		全般	運用手順や利用手順の文書化と提示
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令および契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理の実施
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		全般	IoT 機器・システムに対するアップデートの適用
第３の観点	ソシキ・ヒト	全般	IoT 機器・システムの運用・管理を行う者への要求事項の特定
		全般	IoT 機器・システムの運用・管理を行う者への要求事項の遵守の確認

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。

観点	対策要件	実際に講じる対策の例
第1の観点	**運用前（設計・製造段階）における法令及び契約上の要求事項の遵守**	• 本件に関連する法的、規制（例：製品安全関連法）又は契約上の義務の明確化及び、それらの違反を避けるための要求事項の遵守
	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	• ガス給湯器システムの企画・設計時におけるリスクアセスメントの実施、セキュリティ要件の特定、要件の実装に係る費用の確保 • 必要なセキュリティ仕様が組み込まれているかを確認する設計レビューの実施
	セキュリティ設計と両立するセーフティ設計の仕様化	• ガス給湯器の近くにいる人や機器の周辺への危害を回避するための安全機能（本質安全設計、予防安全機能 等）の実装 • ガス給湯器等に実装された安全機能と外部との通信回線との分離
	IoT機器・システムの出荷時における安全な初期設定と構成	• ガス給湯器システムを構成する機器の不要なネットワークポート、その他USBやシリアルポートなどの物理的又は論理的な閉塞 • 出荷時点で明らかに不要なIoT機器・システムが提供する機能、サービス、アプリケーション、アカウントの削除又は無効化 • ルータを含む機器の初期パスワードの変更を促す機能の実装 • 暗号通信機能（例：TKIP、AES）を有した居内無線LANへの接続を促すガイダンスの提供

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->整理した対策に対する意思決定

観点	対策要件	実際に講じる対策の例
第2の観点	**利用者へのリスクの周知等の情報発信**	• スマートフォン上のアプリケーションや企業ホームページ等を通じた、ガス給湯器システムに対するリスクやスマートホームを供給する事業者又は住まい手で対応すべき点に関する情報提供の実施（例えば、サポート期間終了の予告及び通知、機器・システムの重大な脆弱性、ユーザー情報の漏えいや機器のマルウェア感染等のインシデントに関する情報発信等）
	運用手順や利用手順の文書化等の運用・管理を行う者への支援の実施	• 住まい手に対する、以下の内容を含むガス給湯器システムの運用手順や利用手順の作成及び提示 ✓ 初期設定の手順 ✓ 提供者が想定する安全な利用方法 ✓ 不適切な使用によって生じ得るセキュリティ関連のリスク ✓ 不具合を発見した際の連絡先 • 運用・管理を行う者へのガイドの作成及び提示
	プログラムソースコード及び関連書類の保護	• 確立した手順に従ってプログラムソースコードを厳重に管理する • （該当する文書が書面で保管される場合）施錠可能な文書保管庫での関連書類（設計書、仕様書、検証計画書、妥当性確認計画書）の保護
	脆弱性対応に必要な手順等の整備と実践	• 新たに検知されたクラウドサービス、スマートフォン上のアプリケーション及びガス給湯器に係る脅威や脆弱性の報告窓口の設置 • 以下を含む、脆弱性対応手順の策定 ✓ 報告された脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定 ✓ 開発委託先等への修正プログラム等開発の依頼 ✓ セキュリティパッチの提供
	IoT機器・システムに対するアップデートの適用	• セキュリティパッチを提供する前に、それらが有効であることや副作用がないかについて確認を実施 • 正規のウェブサイト等から適切な方法（例：通信経路の暗号化、機器間の相互認証）によるセキュリティパッチの提供

3-1.ガス給湯器の遠隔操作（ガス給湯器）
③リスク対応->整理した対策に対する意思決定

観点	対策要件	実際に講じる対策の例
第3の観点	**IoT機器・システムの運用・管理を行う者への要求事項の特定**	• 以下の内容を含む、住まい手に能動的な行動を促すためのスマートホーム向けにメンテナンスやサポートを行う事業者への要求事項の明確化 ✓ 使用条件 ✓ 使用上のリスク・注意点 ✓ 使用上のリスク・注意点、異常通知があった場合に取るべき対応（手元操作の優先、近くにいる使用者による通信回線切り離し） ✓ ソフトウェアアップデート時の注意事項
	IoT機器・システムの運用・管理を行う者に対する要求事項の遵守の確認	• 明確化した住まい手に能動的な行動を促すためのスマートホーム向けにメンテナンスやサポートを行う事業者への要求事項の遵守の確認 • ソフトウェアアップデート時の注意事項の遵守の確認

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. 本ユースケース集の構成

3. 各ユースケースの概要

3-1.家庭用ガス給湯器の遠隔操作
3-2.ドローンを活用した個人による写真撮影
3-3.物流倉庫内のAGVによる自動ピッキング
3-4.化学プラント施設内の蒸留工程の自動制御
3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
3-6.金属製造現場の温度センサ等による製造設備の状態監視

3-2.ドローンを活用した個人による写真撮影（ドローン）

①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

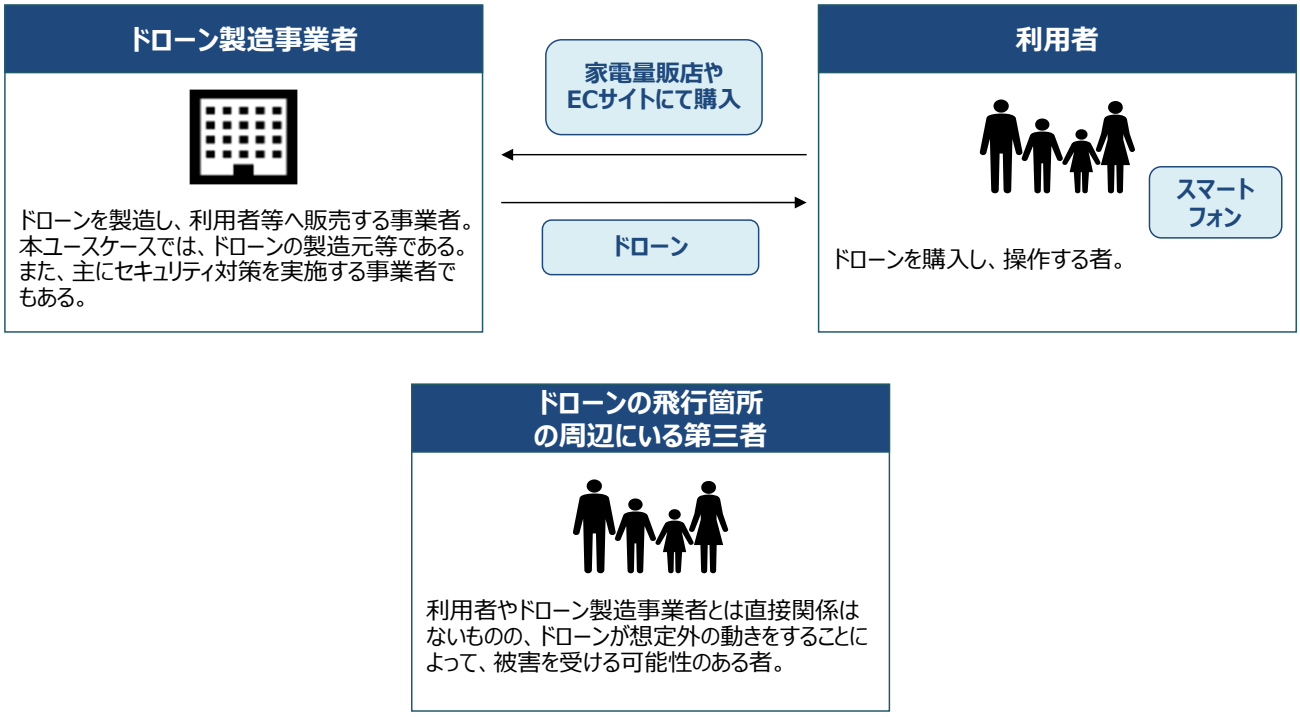
- 本ユースケースの適用主体は、ドローン製造事業者とする。
- 新たに消費者用ドローンを企画・開発し、家電量販店もしくはECサイトでの販売を計画しているが、販売するドローンがセキュリティインシデント等によって利用者（消費者等）や周囲環境へ影響を与え得ることを懸念している。

- ドローン製造事業者は、利用者がスマートフォンに接続されたコントローラにてドローンを操作し、ドローンに設置されたカメラにて風景を撮影することを想定する。
- 利用者は公共施設内の土地（屋外）にて許可を得た上でドローンを操作するものとし、民法や自治体が定める条例に加えて小型無人機等飛行禁止法で禁止されたエリアでは操作しないものとドローン製造事業者は想定している。
- ドローンの重さは、199gを想定。飛行速度は、水平:10 m/s　上昇:3 m/s　下降:3 m/sを想定。

［参考］ 経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」等

3-2.ドローンを活用した個人による写真撮影（ドローン）
①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

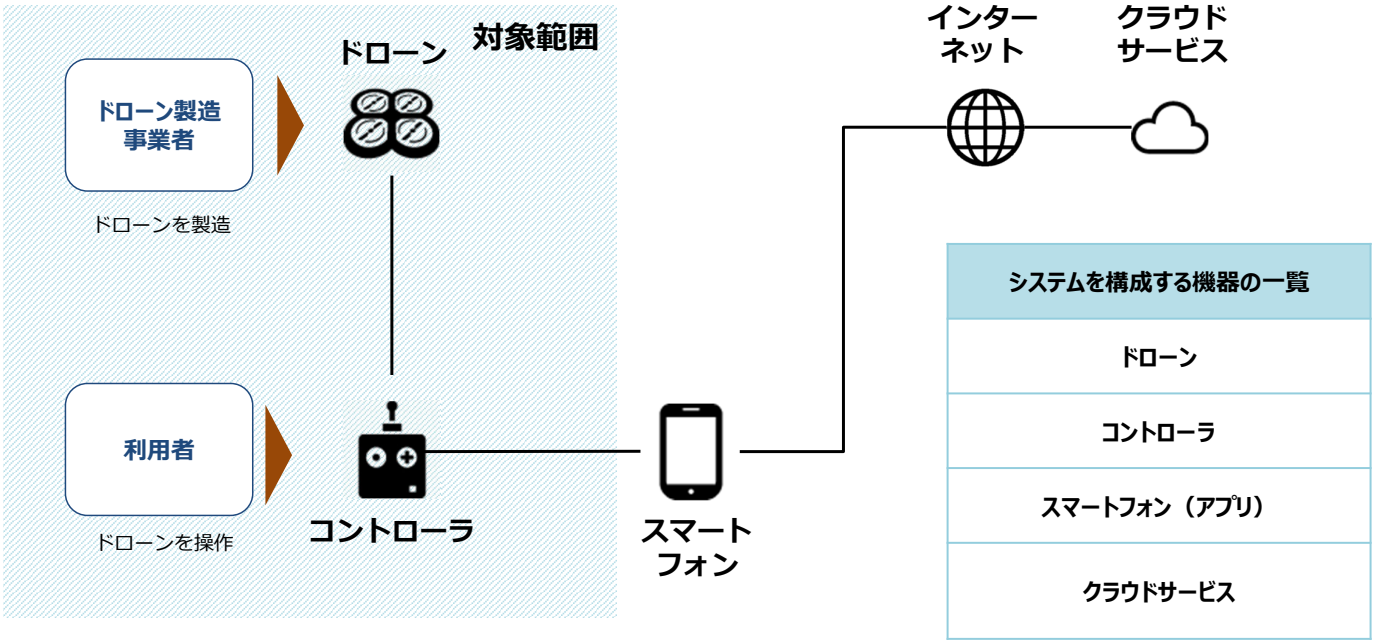
- ステークホルダーは、「ドローン製造事業者」「利用者」及び「ドローンの飛行箇所の周辺にいる第三者」の3者を想定する。



[参考]一般社団法人セキュアドローン協議会「ドローンセキュリティガイド-第2版-」等

3-2.ドローンを活用した個人による写真撮影（ドローン）
①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。



システムを構成する機器の一覧
ドローン
コントローラ
スマートフォン（アプリ）
クラウドサービス

[参考] 経済産業省「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」等

3-2.ドローンを活用した個人による写真撮影（ドローン）
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・システムにおいて想定されるセキュリティインシデント及び想定される被害（例）を整理。

分類	想定されるセキュリティインシデント	想定される被害(例)
ドローン製造事業者にとってのリスク	ドローンに重大な脆弱性が発見される。	**大規模な製品回収等が生じ得る。**
利用者にとってのリスク	悪意のある攻撃者によって、**内蔵されたカメラが不正アクセスされる。**	利用者本人が映り込んだ画像や利用履歴等**の個人情報等が漏えいし得る。**
	悪意のある攻撃者によって、ドローンの**機体制御が乗っ取られる。**	ドローンが高高度から落下し、利用者が**けがをする可能性がある。**また、**けがを負うことによって生活に支障をきたし得る。**
ドローンの飛行箇所の周辺にいる第三者にとってのリスク	悪意のある攻撃者によって、**内蔵されたカメラが不正アクセスされる。**	ドローンの飛行箇所の周辺にいる第三者が映り込んだ画像や利用履歴等の**個人情報等が漏えいし得る。**
	悪意のある攻撃者によって、ドローンの**機体制御が乗っ取られる。**	ドローンが高高度から落下し、ドローンの飛行箇所の周辺にいる第三者が**けがをする可能性がある。**

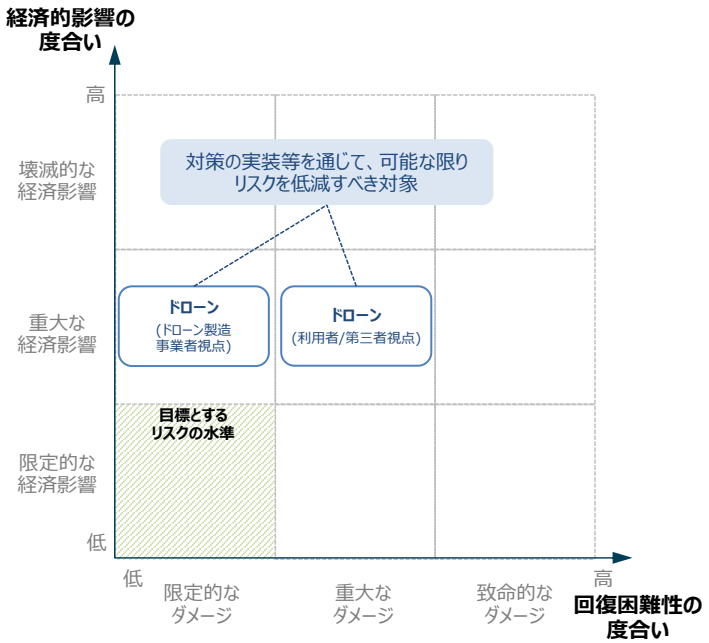
3-2.ドローンを活用した個人による写真撮影（ドローン）
②リスクアセスメント->マッピング結果の整理と評価の実施

- セキュリティインシデントによってドローンの航行に影響が及んだ場合、周辺の第三者や住宅等の環境へ影響を及ぼし得ることから、IoT-SSFの適用主体である「ドローン製造事業者」は、「利用者」に加えて「第三者」が被り得るリスクを考慮して対策を実装する必要がある。

リスクの大きさ（※1）

ステークホルダー	回復困難性の度合い	経済的影響の度合い(※2)
ドローン製造事業者	• 従業員が重症を負う可能性は低い。	• 大規模な製品回収につながるおそれがある。
利用者	• 個人情報が流出する可能性がある。 • 利用者が重症を負う可能性がある。	• 重症を負った場合、生活に支障をきたす可能性がある。
ドローンの飛行箇所の周辺にいる第三者	• 個人情報が流出する可能性がある。 • 利用者が重症を負う可能性がある。	• 重症を負った場合、生活に支障をきたす可能性がある。

想定されるリスク(例)のマッピング結果

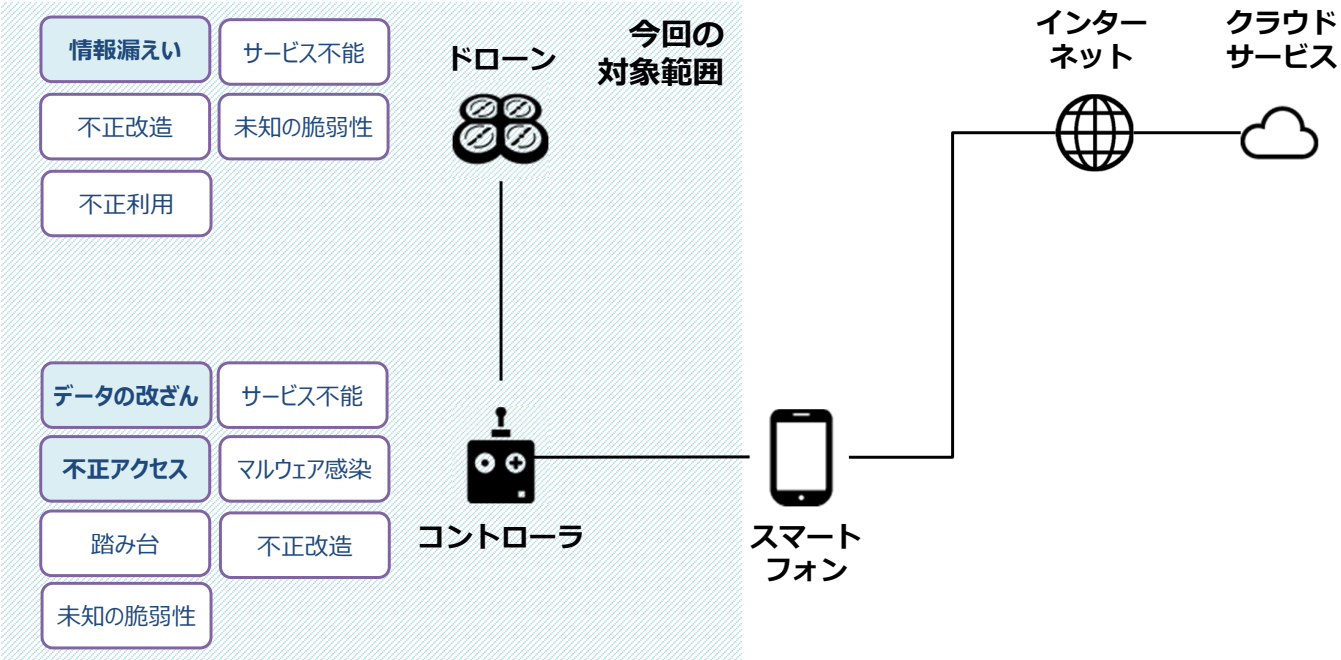


※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-2.ドローンを活用した個人による写真撮影（ドローン）
③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-2.ドローンを活用した個人による写真撮影（ドローン）
③リスク対応->脅威に対する対策の整理

- 適用主体であるドローン製造事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

ドローン製造事業者(自身)にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進	• 運用前（設計・製造段階）における法令及び契約上の要求事項の遵守 • 企画・設計段階におけるセキュリティ要求事項の分析及び仕様化 • セキュリティ設計と両立するセーフティ設計の仕様化

利用者及びドローンの飛行箇所の周辺にいる第三者にとってのリスクを低減するため対応を要請する対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
利用者への注意喚起の実施や推奨事項の明確化	• プログラムソースコード及び関連書類の保護 • IoT機器・システムに対するアップデートの適用 • IoT機器・システムの運用・管理を行う者への要求事項の特定
フェールセーフ等を含む安全対策の徹底	• セキュリティ設計と両立するセーフティ設計の仕様化

3-2.ドローンを活用した個人による写真撮影（ドローン）
③リスク対応->脅威に対する対策の整理

- 想定される脅威を踏まえ、第3軸「求められるセキュリティ・セーフティ要求」における観点ごとに有効と考えられるドローン製造事業者にて実装が想定される対策要件を整理する。

ドローン製造事業者にて実装が想定される対策要件の例

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の決定
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
		マルウェア感染	マルウェア対策の実施
		サービス不能	IoT 機器・システムの十分な可用性の確保
		データの改ざん 不正アクセス	IoT に適したネットワークの利用
		全般	セキュリティ設計と両立するセーフティ設計の仕様化
		全般	セキュアな開発環境と開発手法の適用
		全般	IoT 機器・システムにおけるセキュリティ機能の検証
		全般	IoT 機器・システムの出荷時における安全な初期設定と構成
第 2 の観点	ソシキ・ヒト	全般	利用者へのリスクの周知等の情報発信
		全般	サービス提供や管理のポリシーの提示・遵守
		全般	過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令および契約上の要求事項の遵守
		全般	プログラムソースコード及び関連書類の保護
		全般	IoT 機器・システムに対するアップデートの適用
		全般	IoT 機器・システムの安全な廃棄または再利用
第 3 の観点	ソシキ・ヒト	全般	IoT 機器・システムの運用・管理を行う者への要求事項の特定
		全般	IoT 機器・システムの運用・管理を行う者への要求事項の遵守の確認

3-2.ドローンを活用した個人による写真撮影（ドローン）
③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。
- ドローン及びコントローラは常に通信を行いながら作動する。したがって、これらのどちらかの機器を優先すればよいということではなく、これらの機器一体で対策を行うことが望ましい。

観点	対策要件	実際に講じる対策の例
第1の観点	**運用前（設計・製造段階）における法令及び契約上の要求事項の遵守**	• 情報セキュリティに関連する法的、規制（例：製品安全関連法）に対する違反を避けるための要求事項の遵守
	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	• ドローン及び周辺機器を現に開発、運用する以前の企画・設計の段階における、想定されるリスクやその程度、具備すべきセキュリティ要求事項の特定
	セキュリティ設計と両立するセーフティ設計の仕様化	• 利用者やドローンの飛行箇所周辺にいる第三者への危害を回避するための安全機能（本質安全設計、予防安全機能等）の実装

3-2.ドローンを活用した個人による写真撮影（ドローン）
③リスク対応->整理した対策に対する意思決定

観点	対策要件	実際に講じる対策の例
	利用者へのリスクの周知等の情報発信	• 企業ホームページ等を通じたサポート期間終了の予告及び通知、機器・システムの重大な脆弱性、ユーザ情報の漏えいや機器のマルウェア感染等のインシデントに関する情報発信等、ドローンに対するリスクや利用者で対応すべき点に関する情報提供の実施
第2の観点	**IoT機器・システムの適正な使用**	• 利用者に対する、以下の内容を含むドローンの取扱い説明書（利用手順や操作方法）の作成及び提示 ✓ 初期設定の手順 ✓ 提供者が想定する安全な利用方法 ✓ 不適切な使用によって生じ得るセキュリティ関連のリスク ✓ 不具合を発見した際の連絡先 ✓ ドローンの安全な廃棄方法
第3の観点	**IoT機器・システムの運用・管理を行う者への要求事項の特定**	• 以下の内容を含む、取扱い説明書での利用者に能動的な行動を促すための推奨事項の明確化 ✓ 使用条件 ✓ 使用上のリスク・注意点 ✓ 異常通知があった場合に取るべき対応（手元操作の優先、近くにいる使用者による通信回線切り離し） ✓ ソフトウェアアップデート時の注意事項

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. 本ユースケース集の構成

3. 各ユースケースの概要

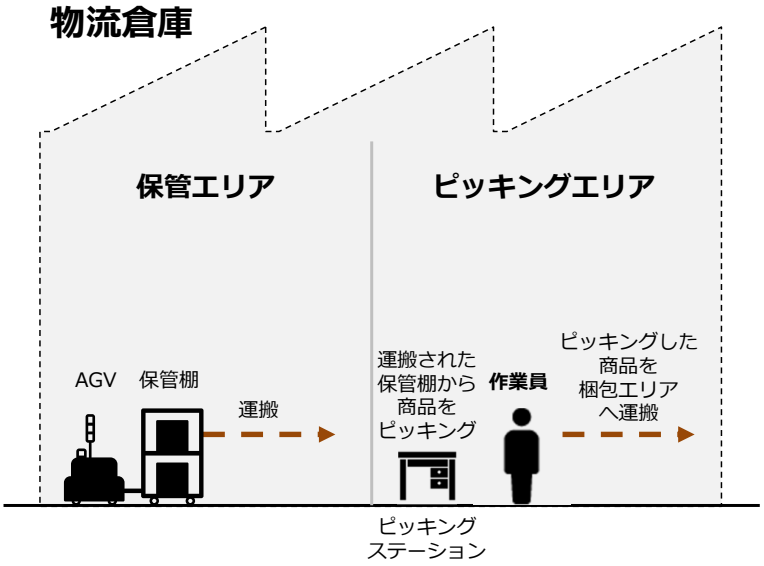
3-1.家庭用ガス給湯器の遠隔操作
3-2.ドローンを活用した個人による写真撮影
3-3.物流倉庫内のAGVによる自動ピッキング
3-4.化学プラント施設内の蒸留工程の自動制御
3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
3-6.金属製造現場の温度センサ等による製造設備の状態監視

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）

①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースのIoT-SSFの適用主体は、物流事業者とする。
- 当該事業者は、事業規模拡大に伴って既存の物流倉庫において、省人化や効率化を目的としてAGVや倉庫制御システム等の導入を予定しており、新たなシステムや機器の導入によって生じ得るサイバーセキュリティに関するリスクを懸念している。

- 工業用間接資材を扱う物流倉庫において、無人搬送車（AGV：Automatic Guided Vehicle）が自動ピッキングを行う。
- 具体的には、物流倉庫（入荷エリア、保管エリア、ピッキングエリア、梱包エリア、出荷エリア）内の保管エリアにて倉庫制御システムによって制御されたAGVが保管棚をピッキングエリアにいる作業員のもと（ピッキングステーション）まで移動させる。
- なお、保管棚からのピッキングする作業は作業員にて行うことを想定。

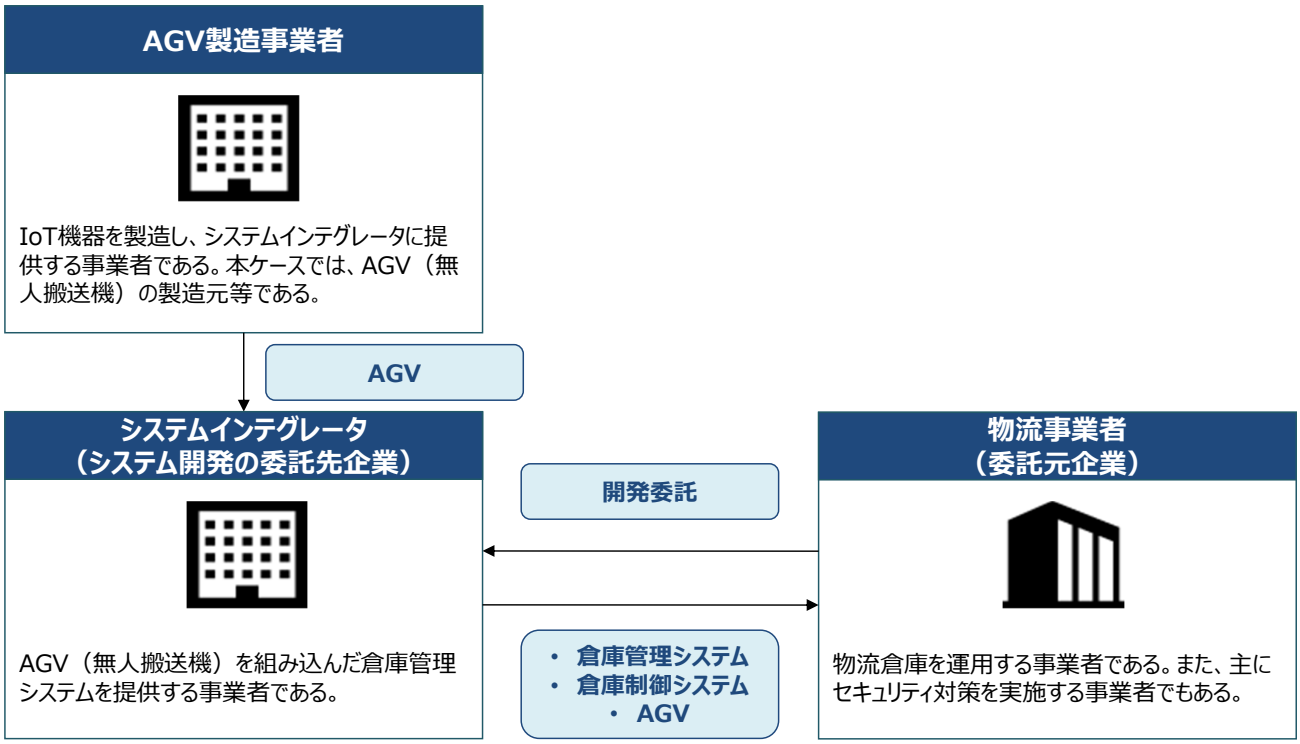


[参考] 国土交通省「物流分野における情報セキュリティ確保に係る安全ガイドライン」等

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）

①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

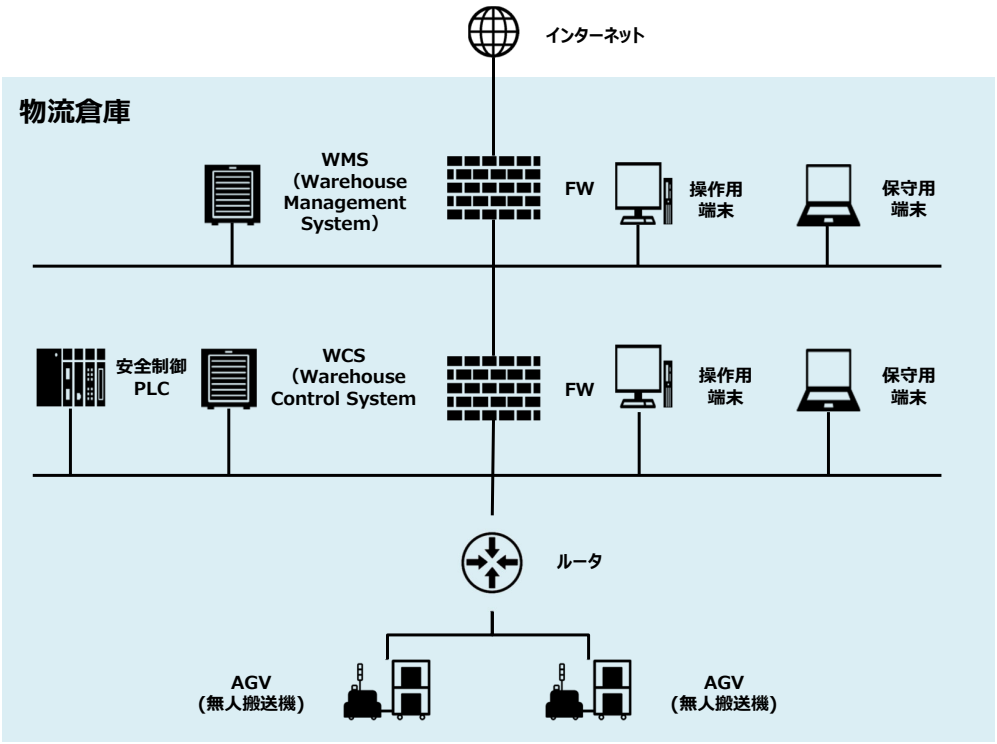
- ステークホルダーは、「物流事業者」「システムインテグレータ」「AGV製造事業者」の３者。



[参考] 国土交通省「物流分野における情報セキュリティ確保に係る安全ガイドライン」等

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。



システムを構成する機器の一覧
倉庫管理システム
操作用端末
保守用端末
倉庫制御システム
安全制御PLC
AGV

[参考] 国土交通省「物流分野における情報セキュリティ確保に係る安全ガイドライン」等

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・システムにおいて想定されるセキュリティインシデント及び想定される被害（例）を整理。

分類	想定されるセキュリティインシデント	想定される被害(例)
物流事業者にとってのリスク	悪意のある攻撃者により外部から倉庫管理システムが不正にアクセスされ、保存されている在庫情報が改ざんされる。	配送の停止や誤配送が生じ得る。（※） **<u>配送の停止や誤配送</u>**が生じることによって、担当地域で事業を行う搬送会社や工業資材の利用者等、物流事業者からサービスの提供を受ける**<u>倉庫外部の事業者等へ影響が及ぶ</u>**可能性がある。
システムインテグレータにとってのリスク	開発するアップデートプログラムが改ざんされ、そのまま配信されることで、倉庫制御システムやAGV等が**<u>マルウェアに感染</u>**する。	AGVが想定していない動作をすることで、物流工場が停止することにより、**<u>大規模な製品回収が生じ得る</u>**。
AGV製造事業者にとってのリスク	AGVに重大な脆弱性が発見される。	**<u>大規模な製品回収等が生じ得る。</u>**

※その結果として、各事象のステークホルダーを含む関係者に対する損害賠償（配送遅延や誤配送への対応等）の事後的な対応が発生し得る。

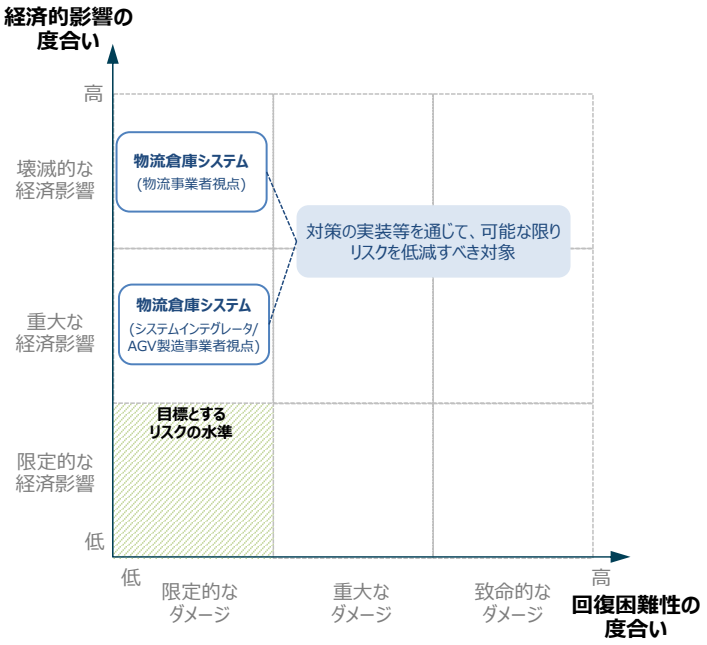
3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
②リスクアセスメント->マッピング結果の整理と評価の実施

- セキュリティインシデントによって「物流事業者」が保有する倉庫内の業務が停止することで、倉庫内のみならず取引先、サプライチェーン規模で影響が波及し、結果として生じる経済的影響が大きくなる可能性がある。

リスクの大きさ（※1）

ステークホルダー	回復困難性の度合い	経済的影響の度合い(※2)
物流事業者	• 従業員が重症を負う可能性は低い。	• 物流事業者からサービスの提供を受ける倉庫外部の事業者等へ影響が及ぶ可能性がある。 • 配送の停止や誤配送が生じる可能性がある。
システムインテグレータ	• 従業員が重症を負う可能性は低い。	• 開発するアップデートプログラムが改ざんされ、大規模な製品回収につながる可能性がある。
AGV製造事業者	• 従業員が重症を負う可能性は低い。	• 大規模な製品回収につながるおそれがある。

想定されるリスク(例)のマッピング結果

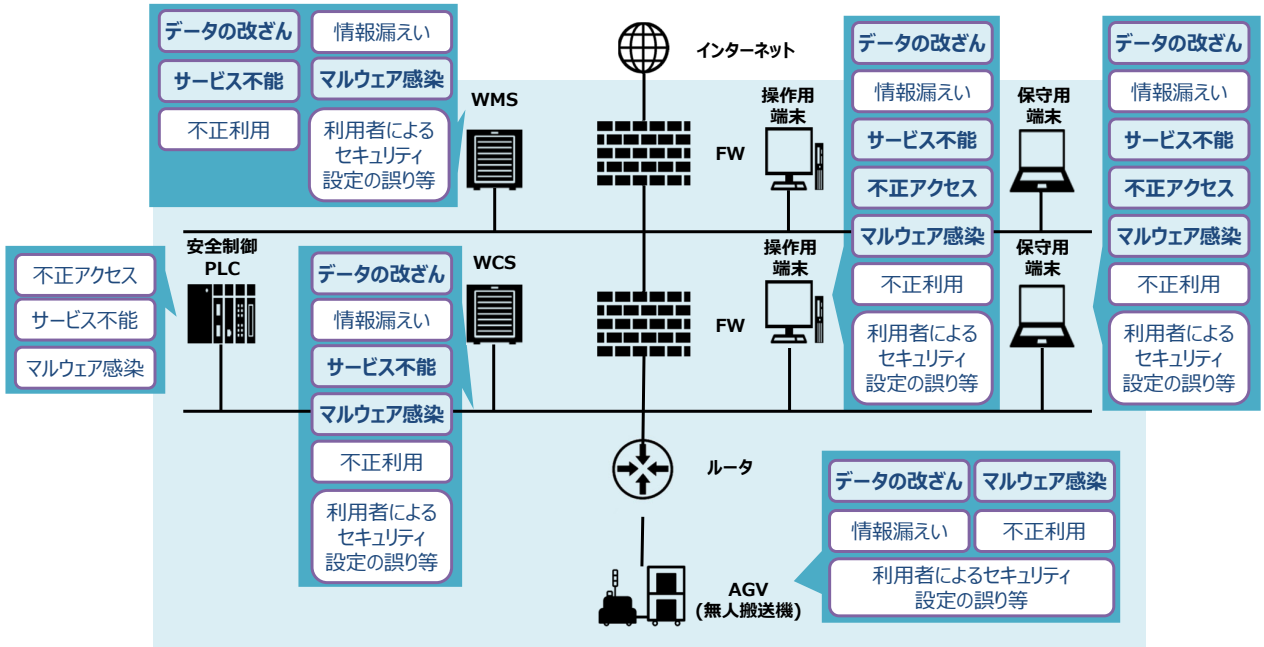


※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
③リスク対応->脅威に対する対策の整理

- 適用主体である物流事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

物流事業者(自身)にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築	• **様々なIoT機器を接続する際のセキュリティの確保** • **適切なネットワークの分離**
信頼性の高い物流倉庫の操業を可能にするための仕組みの構築	• **IoT機器・システムの十分な可能性の確保** • **IoT機器・システムのモニタリング及びログの取得、分析**

システムインテグレータにとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
大規模な製品回収等につながり得る機器・システムのセキュリティ上の欠陥を防ぐための、セキュリティ・バイ・デザインの取組みの推進	• **運用前（設計・製造段階）における法令及び契約上の要求事項の遵守** • **セキュリティ設計と両立するセーフティ設計の仕様化**
安全なアップデートプログラムの配信のための仕組みの構築	• **IoT機器・システムに対するアップデートの適用**

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
③リスク対応->脅威に対する対策の整理

- 被害の大きさだけでなく、その起こりやすさも踏まえ、システム全体としてのリスクを低減することを目的として対策の適用対象を検討する。

物流事業者にて実装が想定される対策要件の例想定される脅威（例）

第３軸	実装先	想定される脅威（例）	対策要件
第１の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の決定
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
			置、設定
第２の観点	ソシキ・ヒト	全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
		全般	サービス提供や管理のポリシーの提示・遵守
	プロシージャ	全般	脆弱性対応に必要な体制や手順等の整備と実践
		全般	インシデント対応手順の整備と実践
		全般	事業継続計画の策定と実践
		全般	IoT 機器・システムの用途・用法を守った使用
		不正利用 不正アクセス	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令および契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		不正利用	IoT 機器・システムに対するアップデートの適用
		情報漏えい	IoT 機器・システムの安全な廃棄または再利用
		全般	IoT 機器・システムに対するアップデートの適用（セキュリティパッチの開発・配布等）

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
③リスク対応->整理した対策に対する意思決定

- 近年、システム構成やその利用環境の変化、及び制御システムを狙った脅威の高度化等を背景に、セキュリティ対応の必要性が非常に高まってきていることから、制御システムに特有とされる性質等にも注意を払いながら、対策に関する意思決定を行う。

物流事業者において実際に講じる対策の例

観点	対策要件	実際に講じる対策の例
第1の観点	**運用前（設計・製造段階）における法令及び契約上の要求事項の遵守**	• 情報セキュリティに関連する法的な規制又は契約上の義務に対する違反を避けるための要求事項の特定及び遵守。
	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	• 本社の情報システム部門の担当者が中心となり、倉庫における業務担当者を巻き込み、倉庫制御システムの企画・設計時におけるリスクアセスメントの実施、セキュリティ要件の特定、要件の実装に係る費用の確保。 • 必要なセキュリティ仕様が組み込まれているかを確認する設計レビューの実施。 • 特定したセキュリティ要求事項を倉庫制御システムの委託仕様書への記載。
第2の観点	**IoT機器・システムのモニタリング及びログの取得、分析**	• 本社の情報システム部門の担当者による物流倉庫システムを構成する倉庫管理システムや倉庫制御システムを対象にした各種ログ（例：ユーザ認証、ネットワークトラフィック）の取得及び保護。 • 取得したログの定期的な分析及び異常の検知。

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
③リスク対応->整理した対策に対する意思決定

- システムインテグレータに対応を依頼することとした対策例は以下の通り。

システムインテグレータにおいて実際に講じる対策の例（1/2）

観点	対策要件	実際に講じる対策の例
第1の観点	**様々なIoT機器に接続する際のセキュリティの確保**	• AGV制御PLC等を他のAGV機器等に接続する際のホワイトリストの適用。
	IoT機器・システムの十分な可用性の確保	• 倉庫外部からの通信を受信し得る倉庫管理システム等に対する(D)DoS 攻撃を想定し、一定レベルの負荷に耐える容量を確保。 • 倉庫管理システム、操作用端末、保守用端末、倉庫制御システム等において不審な通信（例：特定のIPアドレスからの大量のリクエスト）の検知及び遮断。 • アプリケーションのテスト段階における一定レベルの負荷試験の実施
	IoT機器・システムの十分な可用性の確保	• 倉庫外部からの通信を受信し得る倉庫管理システム等に対する(D)DoS 攻撃を想定し、一定レベルの負荷に耐える容量を確保。 • 倉庫管理システム、操作用端末、保守用端末、倉庫制御システム等において不審な通信（例：特定のIPアドレスからの大量のリクエスト）の検知及び遮断。 • アプリケーションのテスト段階における一定レベルの負荷試験の実施。

3-3.物流倉庫内のAGVによる自動ピッキング（AGV）
③リスク対応->整理した対策に対する意思決定

- システムインテグレータに対応を依頼することとした対策例は以下の通り。

システムインテグレータにおいて実際に講じる対策の例（2/2）

観点	対策要件	実際に講じる対策の例
第1の観点	**適切なネットワークの分離**	• リスクレベルに応じた情報ネットワーク、情報制御ネットワーク、制御ネットワーク等の複数のゾーンへのネットワークの分割。 • FW等でのAGVやAGV制御PLCが含まれているゾーンで送受信される全ての不要な通信の遮断。
	セキュリティ設計と両立するセーフティ設計の仕様化の指示	• 作業員や機器の周辺への危害を回避するための安全機能（本質安全設計、予防安全機能等）の実装。 • AGVに実装された安全機能と外部との通信回線との分離。
第2の観点	**IoT機器・システムに対するアップデートの適用（セキュリティパッチの開発・配布等）**	• 報告された脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定。 • IoT機器製造事業者や開発委託先等への修正プログラム等開発の依頼。 • 物流事業者へのセキュリティパッチの提供。

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. 本ユースケース集の構成

3. 各ユースケースの概要

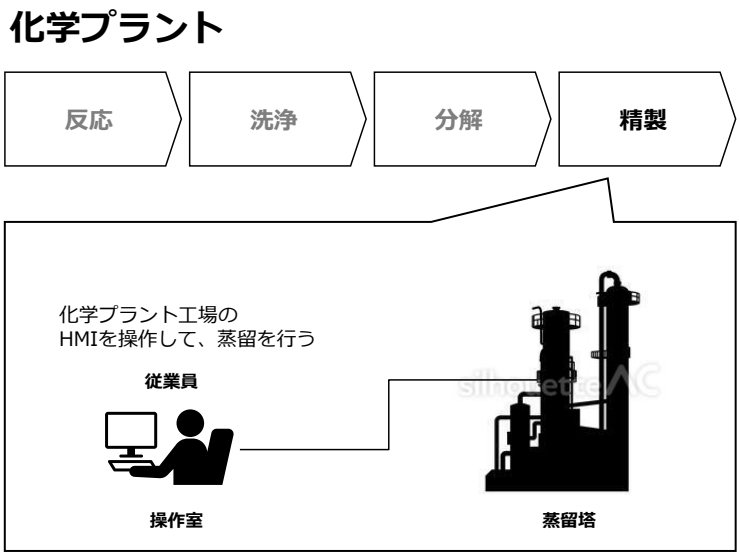
- 3-1.家庭用ガス給湯器の遠隔操作
- 3-2.ドローンを活用した個人による写真撮影
- 3-3.物流倉庫内のAGVによる自動ピッキング
- 3-4.化学プラント施設内の蒸留工程の自動制御
- 3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
- 3-6.金属製造現場の温度センサ等による製造設備の状態監視

3-4.化学プラント施設内の蒸留工程の自動制御

①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースの適用主体は、プラント事業者とする。
- 当該事業者は、化学物質を製造する事業者であり、操業開始から既に数十年程度プラントを運用しているが、本社の経営層を中心に新たに生じ得るサイバーセキュリティに関するリスクを懸念している。

- 製造実行システム（MES）やHMI、プロセス制御PLC等からなるプラントシステムを用いて、化学物質を製造しているケースを想定する。
- 本ケースケースでは、精製工程における蒸留工程を実施する装置を扱うものとする。
- 蒸留工程では、液体混合物を各成分の沸点の差を利用して分類させることを想定している。

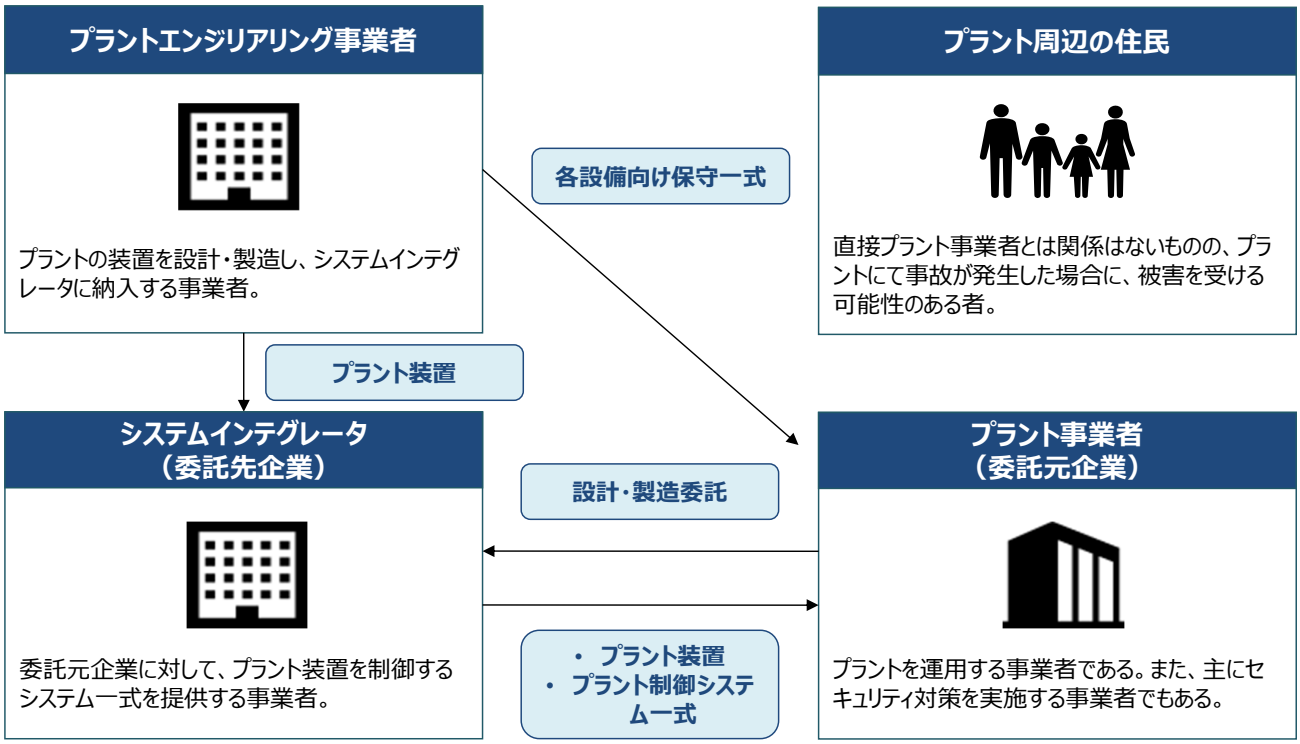


[参考] 経済産業省、国立研究開発法人新エネルギー・産業技術総合開発機構「IoTセキュリティ対応マニュアル産業保安版（第２版）」等

3-4.化学プラント施設内の蒸留工程の自動制御

①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

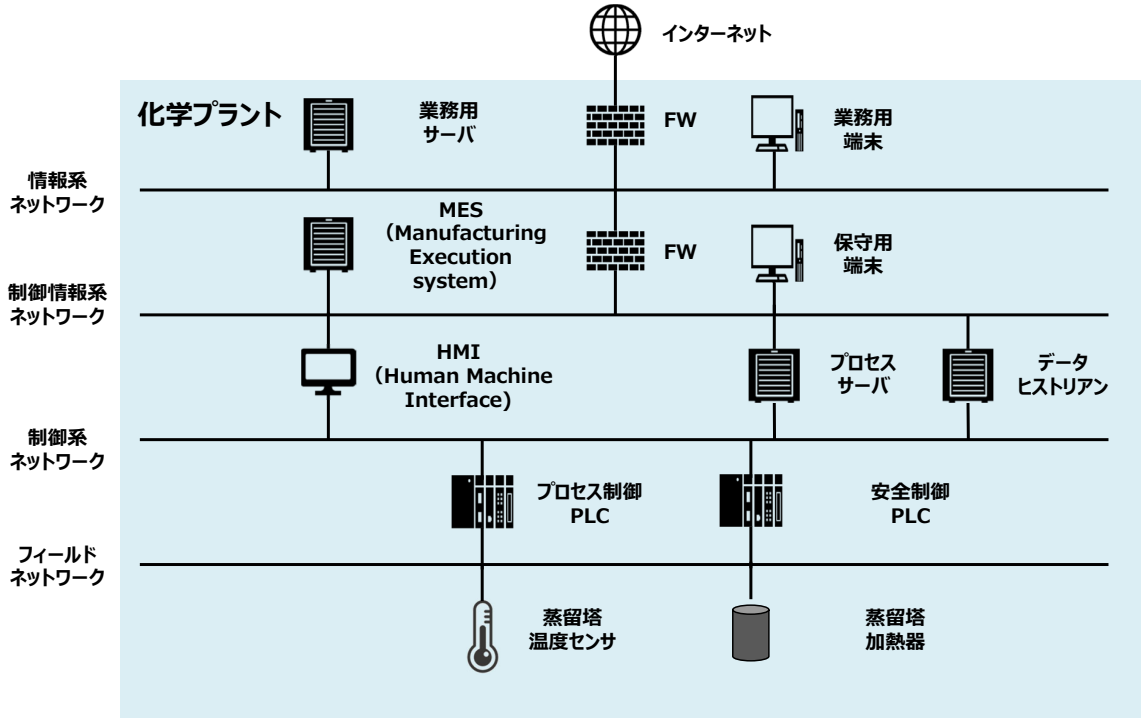
- ステークホルダーは、「プラント事業者」、「システムインテグレータ」、「プラントエンジニアリング事業者」及び「プラント周辺の住民」の４者。

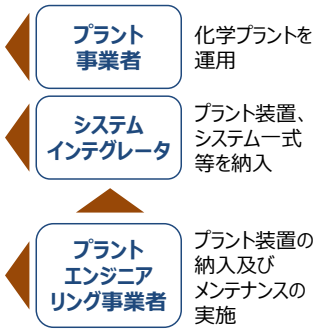


[参考] 経済産業省、国立研究開発法人新エネルギー・産業技術総合開発機構「IoTセキュリティ対応マニュアル産業保安版（第２版）」等

3-4.化学プラント施設内の蒸留工程の自動制御
①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。





システムを構成する機器の一覧
MES(製造実行システム)
HMI(ヒューマンマシンインターフェース)
プロセスサーバ
データヒストリアン
業務用サーバ/業務用端末
安全制御PLC
プロセス制御PLC
蒸留塔温度センサ
蒸留塔加熱器

[参考] 経済産業省、国立研究開発法人新エネルギー・産業技術総合開発機構「IoTセキュリティ対応マニュアル産業保安版（第２版）」等

3-4.化学プラント施設内の蒸留工程の自動制御
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・システムにおいて想定されるセキュリティインシデント及び想定される被害（例）を整理。

分類	想定されるセキュリティインシデント	想定される被害(例)
プラント事業者にとってのリスク	悪意のある攻撃者が、業務用サーバや業務用端末に加えて、MES等に**不正アクセス**し、**情報を漏えい**させる。	従業員の個人情報や取引先担当者等の情報が流出する可能性がある。
	プラント制御システムが**マルウェアに感染**（例：ランサムウェア）し、かつ安全設備等が十分に作動しない。	一部の化学反応が進むことで、蒸留塔内部の温度が上昇し、**蒸留塔等が爆発し得る**。その結果、プラント工場が停止するとともに、**従業員が重症を負うか死亡する可能性がある。**（※1）
	プラント制御システムが**マルウェアに感染**（例：ランサムウェア）し、蒸留工程に関する設備が停止する。	その他の工程も停止することにより、**工場全体の稼働が停止する**とともに、川下の企業の経済活動にも大きな影響を与える。
プラント周辺の住民	プラント制御システムが**マルウェアに感染**（例：ランサムウェア）し、かつ安全設備等が十分に作動しない。	一部の化学反応が進むことで、蒸留塔内部の温度が上昇し、蒸留塔等が爆発することにより、環境汚染が生じた場合には、**住民等の健康や安全に多大な影響**が生じる可能性がある。また、**住民の生活にも大きな支障をきたす**可能性がある。
システムインテグレータにとってのリスク	プラント事業者に対する注意喚起(例：設定方法に関する説明等)を怠る。	サービス提供における過失が認められ得る。（※2）
プラントエンジニアリング事業者にとってのリスク	開発するアップデートプログラムが改ざんされ、そのまま配信されることで、MESやプロセス制御PLC等が**マルウェアに感染**する。	MESやプロセス制御PLCが想定していない動作をして、**蒸留塔等の設備が停止する。**（※3）

※1:その結果として、各事象のステークホルダーを含む関係者に対する損害賠償（住民被害や環境汚染の対応等）の事後的な対応が発生し得る。
※2:その結果として、契約上の責任が問われ得る。
※3:その結果として、各事象のステークホルダーを含む関係者に対する損害賠償（システムインテグレータへの補償等）の事後的な対応が発生し得る。

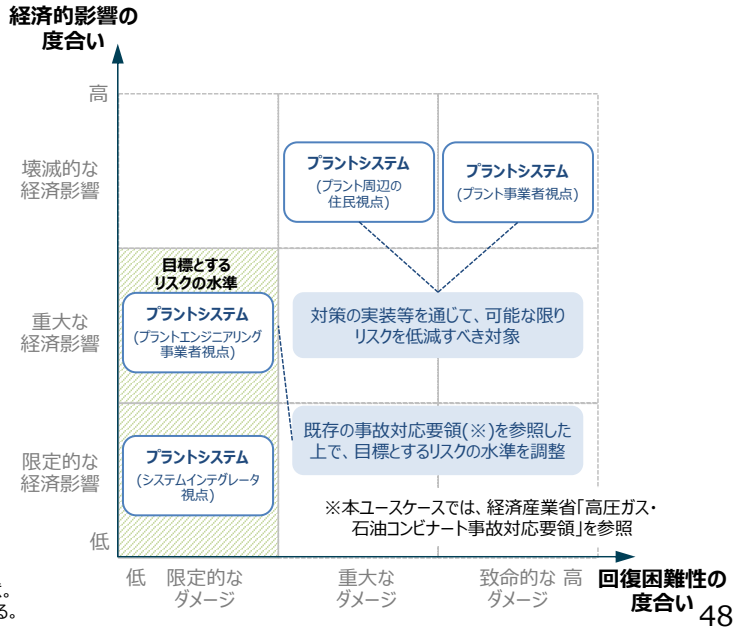
3-4.化学プラント施設内の蒸留工程の自動制御
②リスクアセスメント->マッピング結果の整理と評価の実施

- セキュリティインシデントが設備損傷や爆発等の安全上の事象に発展する場合、「プラント事業者」にとってのリスクは「回復困難性の度合い」及び「経済的影響の度合い」の双方が非常に大きくなる。また、それらの事故により自身だけではなく、「プラント周辺の住民」へも影響が及ぶ可能性がある。
- 監督官庁から公表されている事故対応要領等を参照した上で、目標とするリスクの水準を調整。

リスクの大きさ（※1）

ステークホルダー	回復困難性の度合い	経済的影響の度合い(※2)
プラント事業者	• 爆発事故によって、従業員が死亡する可能性がある。	• 大規模な製品回収につながるおそれがある。
プラント周辺の住民	• プラント周辺の住民が重症を負う可能性がある。	• 農林水産業への打撃により、住民の生活にも大きな支障をきたすおそれがある。
システムインテグレータ	• 従業員がけがをする可能性は低い。	• サービス提供における過失が認められ得る。
プラントエンジニアリング事業者	• 従業員がけがをする可能性は低い。	• 開発するアップデートプログラムが改ざんされ、大規模な製品回収につながる可能性がある。

想定されるリスク(例)のマッピング結果

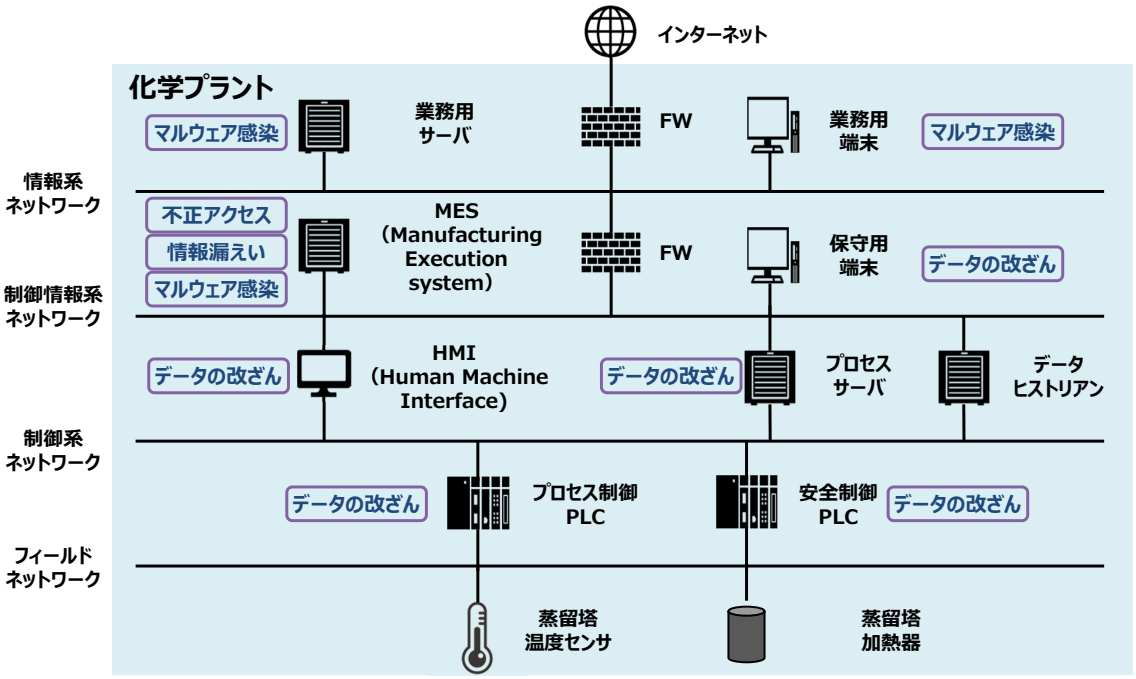


※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-4.化学プラント施設内の蒸留工程の自動制御
③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-4.化学プラント施設内の蒸留工程の自動制御
③リスク対応->脅威に対する対策の整理

- 適用主体であるプラント事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

プラント事業者（自身）にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
等の発生時に正しく作動することを確かなものとする対策	• セキュリティ設計と両立するセーフティ設計の仕様化
情報システム部門及び製造部門が一体となって対応を行うための体制の構築	• 運用前（設計・製造段階）におけるIoTセキュリティを目的とした体制の確保 • 運用中におけるIoTセキュリティを目的とした体制の確保
セキュリティインシデントが発生したとしても、それらの被害を最小限にするための仕組みの構築	• 様々なIoT機器を接続する際のセキュリティの確保 • 適切なネットワークの分離 • インシデント対応手順の整備と実践
信頼性の高いプラントの操業を可能にするための仕組みの構築	• IoT機器・システムの十分な可用性の確保 • IoT機器・システムのモニタリング及びログの取得、分析 • IoT機器・システムに対するアップデートの適用

プラント周辺の住民にとってのリスクを低減するため対応を要請する対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
セキュリティに関するインシデントが発生したととしても周辺環境への影響を最小限に抑える仕組みの構築	• セキュリティ設計と両立するセーフティ設計の仕様化 • 運用中における法令及び契約上の要求事項の遵守

3-4.化学プラント施設内の蒸留工程の自動制御
③リスク対応->脅威に対する対策の整理

- 想定される脅威を踏まえ、第3軸「求められるセキュリティ・セーフティ要求」における観点ごとにプラント事業者にて実装が想定される対策要件を整理する。

プラント事業者にて実装が想定される対策要件の例

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の明確化
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	データの改ざん	ソフトウェアの完全性の検証
		情報漏えい	搭載するソフトウェアに対するインストール対策の実装
		マルウェア感染	マルウェア対策の実施
		全般	IoT 機器・システムの出荷時における安全な初期設定と構成
第 2 の観点	ソシキ・ヒト	全般	サービス提供や管理のポリシーの提示・遵守
		全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		不正利用 不正アクセス	IoT 機器・システムの適正な運用・保守
		全般	IoT 機器・システムの適正な使用
	システム	全般	運用中における法令および契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		不正利用	IoT 機器・システムに対するアップデートの適用
		不正アクセス	IoT 機器・システムの安全な廃棄または再利用

3-4.化学プラント施設内の蒸留工程の自動制御
③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。

観点	対策要件	実際に講じる対策の例
第1の観点	**運用前（設計・製造段階）における法令及び契約上の要求事項の遵守**	• 製造部門及び情報部門が一体となって対応できるようリスク対応組織を立上げ、組織内で統合的にセキュリティ対策を取る体制の構築。 • プラントにおけるセキュリティ管理責任者の任命。 • ※上記の管理責任者及び開発担当者の役割と責任は、プラントシステムのライフサイクルの各段階（例：開発、運用、保守）において明確化されていることが望ましい。
第2の観点	**運用中における法令及び契約上の要求事項の遵守**	• 情報セキュリティに関連する法的な規制又は契約上の義務に対する違反を避けるための要求事項の特定及び遵守
	IoT機器・システムのモニタリング及びログの取得、分析	• プラントシステムを構成するMESやプロセス制御PLCを対象にした各種ログ（例：ユーザ認証、ネットワークトラフィック）の取得及び保護 • 取得したログの安全な入手 • 取得したログの定期的な分析及び異常の検知
	IoT機器・システムに対するアップデートの適用	• 脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定 • 開発委託先等への修正プログラム等開発の依頼 • 製造部門と調整を行った上で、提供を受けたセキュリティパッチの適用

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. 本ユースケース集の構成

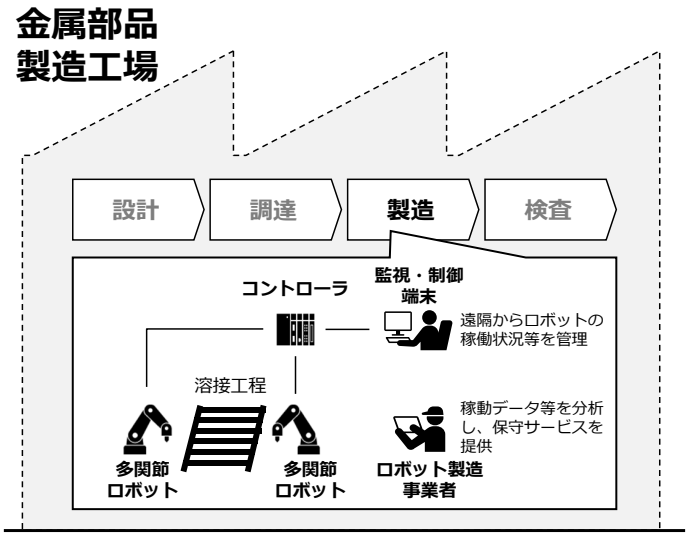
3. 各ユースケースの概要

3-1.家庭用ガス給湯器の遠隔操作
3-2.ドローンを活用した個人による写真撮影
3-3.物流倉庫内のAGVによる自動ピッキング
3-4.化学プラント施設内の蒸留工程の自動
3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
3-6.金属製造現場の温度センサ等による製造設備の状態監視

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースの適用主体は、金属部品製造事業者とする。
- 当該事業者は、生産能力の維持向上等を目的として、溶接工程の自動化を進めるためにロボットシステムの導入を予定しているが、新たに生じ得るサイバーセキュリティに関するリスクを懸念している。

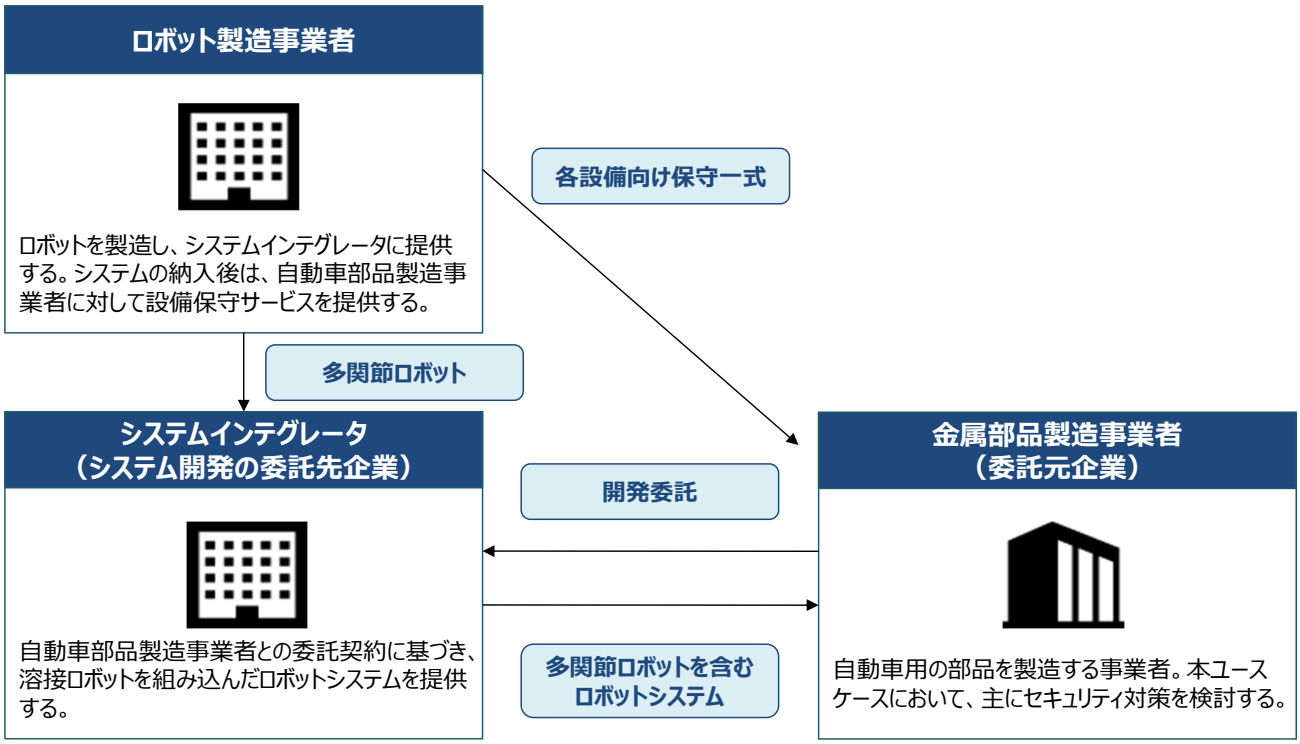
- 金属部品製造事業者の工場において、多関節ロボットを含むロボットシステムを導入し、従来の人手による溶接工程を自動化する。
- 加工対象となるのは、自動車用ボディフレーム等の比較的サイズの大きな部品であり、溶接時に歪を発生させないため左右同時溶接が要求される。
- ロボットが稼働するエリアには安全柵やレーザースキャナが設けられており、基本的に作業員は立ち入れない。
- ロボット製造事業者は、ロボットの稼動データを取得、分析し、効率的な保守サービスの提供に活用する。



[参考] 経済産業省、一般社団法人日本ロボット工業会「ロボット導入実証事業事例紹介ハンドブック2018」等

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

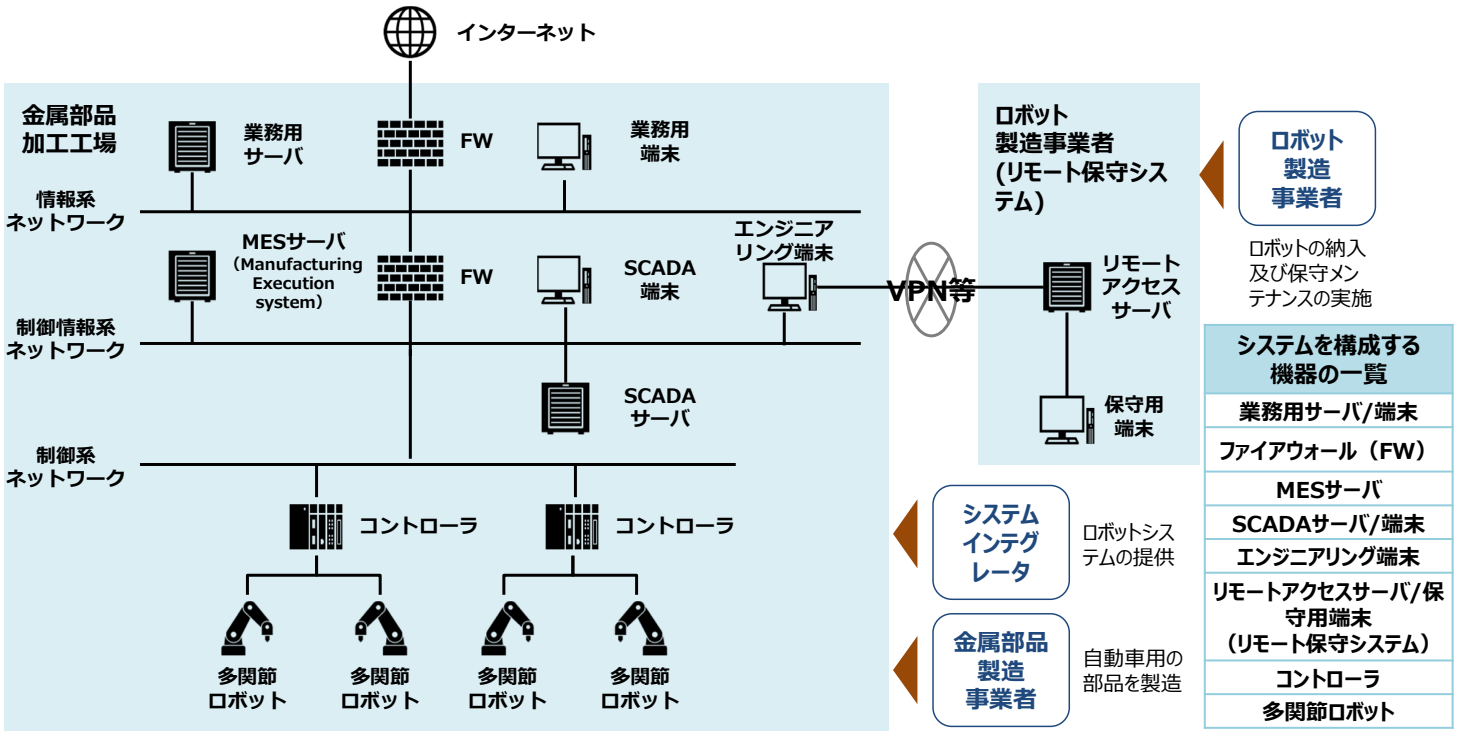
- ステークホルダーは、「金属部品製造事業者」、「システムインテグレータ」及び「ロボット製造事業者」の３者。



[参考] 経済産業省、一般社団法人日本ロボット工業会「ロボット導入実証事業事例紹介ハンドブック2018」等

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。



［参考］経済産業省　国立研究開発法人新エネルギー・産業技術総合開発機構「IoTセキュリティ対応マニュアル産業保安版（第２版）」等

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・システムにおいて想定されるセキュリティインシデント及び想定される被害（例）を整理。

分類	想定されるセキュリティインシデント	想定される被害(例)
金属部品製造事業者にとってのリスク	外部に接続している情報系ネットワークを経由して、制御情報系ネットワークに設置された**MESサーバやSCADAサーバがマルウェアに感染する。**	**生産活動が一時的に停止**する。
	リモート保守サービスを受けるために外部ネットワークに接続している**エンジニアリング端末が不正アクセスされ、コントローラの制御プログラムを改ざんされる。**	仕様を満たさない**不良品が生産される。**
システムインテグレータにとってのリスク	金属部品製造事業者に対する注意喚起(例：設定方法に関する説明等)を怠る。	サービス提供における過失が認められ得る。（※）
ロボット製造事業者にとってのリスク	保守業務委託先のロボット製造事業者の従業員が、誤って不正なUSB等の外部記憶媒体をエンジニアリング端末に挿入することで、**同端末及び制御情報系ネットワーク内の他のサーバや端末がマルウェアに感染する。**	**製品回収が発生する。**

※:その結果として、契約上の責任が問われ得る。

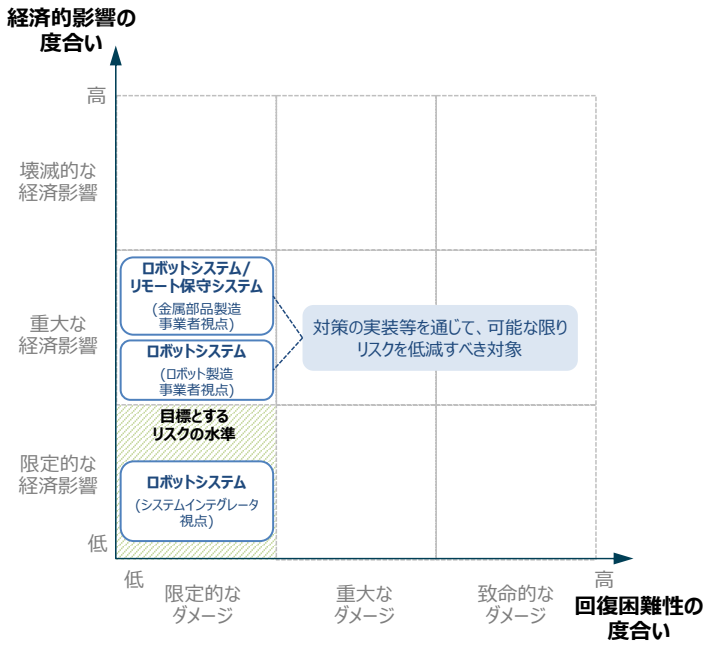
3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
②リスクアセスメント->マッピング結果の整理と評価の実施

- 自社が管理するシステムだけでなく、リモート保守システムにおけるセキュリティインシデントによってもロボットシステムに影響が及び得るため、IoT-SSFの適用主体である「金属部品製造事業者」は、ロボットシステムに加えてリモート保守システムに対しても対策を具備させる必要がある。

リスクの大きさ（※1）

ステークホルダー	回復困難性の度合い	経済的影響の度合い(※2)
金属部品製造事業者	• 保護柵があるため、従業員が重症を負う可能性は低い。	• 生産設備の停止や不良品の発生によって、経済的な損失を被る可能性がある。
システムインテグレータ	• 従業員が重症を負う可能性は低い。	• サービス提供における過失が認められ得る
ロボット製造事業者	• 従業員が重症を負う可能性は低い。	• 製品回収が発生するおそれがある。

想定されるリスク(例)のマッピング結果

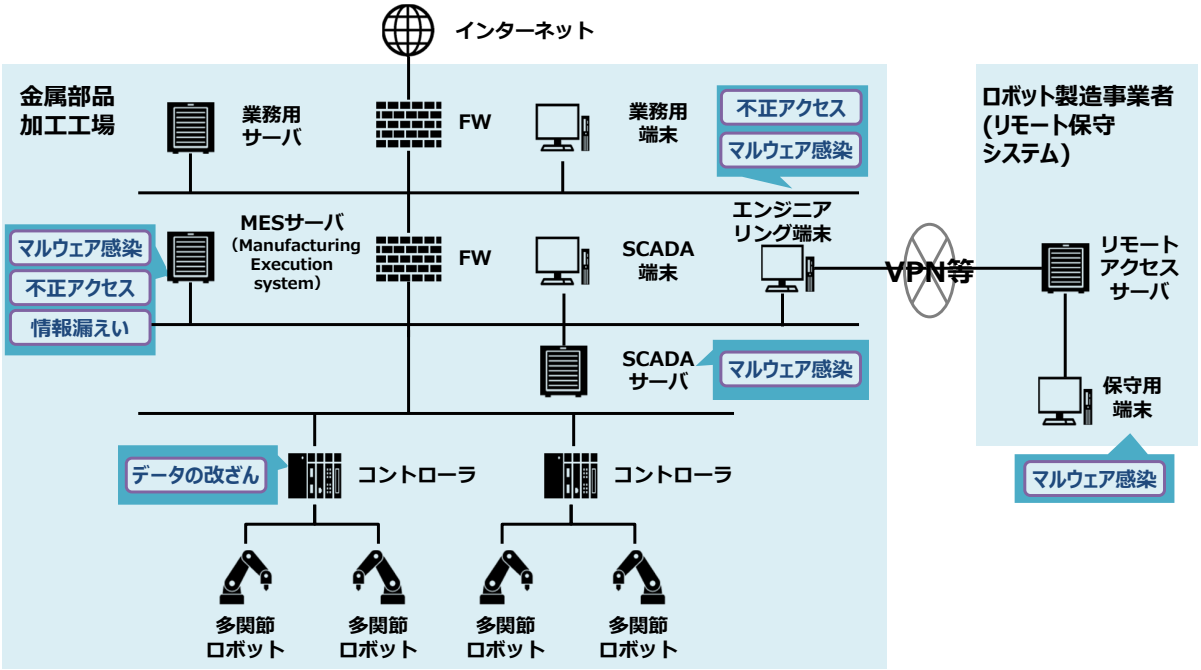


※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
③リスク対応->脅威に対する対策の整理

- 適用主体である金属部品製造事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

金属部品製造事業者（自身）にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
ロボットの制御に関わる設備の保護	• 適切な水準のアクセス制御の実装 • ソフトウェアのインストールの制限 • IoT機器・システムにおける運用開始時の正しい設置、設定
リモート保守システムからのアクセスの保護	• 適切な水準のアクセス制御の実装 • IoT 機器・システムの適正な運用・保守 • 暗号化によるデータの保護（通信経路の保護等） • ソフトウェアの完全性の検証

サポート事業者にとってのリスクを低減するため対応を要請する対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
セキュアなロボット及び周辺機器の調達/提供	• 企画・設計段階におけるセキュリティ要求事項の分析及び仕様化 • （ロボット製造事業者において適切に実施されていることが調達前に確認されるべき対策）
十分な期間のサポート契約締結	• IoT機器・システムに対するアップデートの適用

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
③リスク対応->脅威に対する対策の整理

- 想定される脅威を踏まえ、第3軸「求められるセキュリティ・セーフティ要求」における観点ごとに金属部品製造事業者にて実装が想定される対策要件を整理する。

金属部品製造事業者にて実装が想定される対策要件の例

第 3 軸	実装先	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
			IoT セキュリティに関するステークホルダーの役割の明確化
			IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		なりすまし 不正アクセス	適切な水準のアクセス制御の実装
		マルウェア感染	ソフトウェアの完全性の検証
		マルウェア感染	ソフトウェアのインストールの制限
		なりすまし	暗号化によるデータの保護
		不正アクセス	適切なネットワークの分離
		不正利用	セキュリティ設計と両立するセーフティ設計の仕様化
		全般	セキュアな開発環境と開発手法の適用
		全般	IoT 機器・システムにおけるセキュリティ機能の検証
		全般	信頼できる IoT 機器やサービスの選定
		全般	IoT 機器・システムにおける運用開始時の正しい設置、設定
第 2 の観点	ソシキ・ヒト	全般	運用中における IoT セキュリティを目的とした体制の確保
			過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		全般	インシデント対応手順の整備と実践
		全般	事業継続計画の策定と実践
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令および契約上の要求事項の遵守
		全般	継続的な資産管理
		全般	IoT 機器・システムのモニタリング及びログの取得、分析
		マルウェア感染	IoT 機器・システムに対するアップデートの適用

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。

金属部品製造事業者における実際に講じる対策要件の例

観点	対策要件	実際に講じる対策の例
第1の観点	**企画・設計段階におけるセキュリティ要求事項の分析及び仕様化**	• 本社情報システム部門のセキュリティ担当者と工場内のセキュリティ担当者が中心となり、ロボットシステムの企画・設計時においてリスクアセスメントを実施し、セキュリティ要件を特定、要件実装に係る費用を確保 • 特定したセキュリティ要求事項をロボットシステムの委託仕様書へ記載
第2の観点	**企画・設計段階におけるセキュリティ要求事項の分析及び仕様化**	• ロボット及び周辺機器に関して、ロボット製造事業者と十分な期間の保守契約を締結する。 • セキュリティアップデートを含むソフトウェアやファームウェアの更新を、以下のような措置を通じて不正アクセス等から保護したうえで実施 ✓ 自社の担当者又は保守を担当するロボット製造事業者から提供されたことが確かなプログラムを適用 ✓ 更新をネットワーク経由で遠隔から行う場合、通信経路を適切な方式により暗号化 ✓ 更新実行前にあらかじめ動作検証等を実施

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。

システムインテグレータに対応を依頼すべき対策の例

観点	対策要件	実際に講じる対策の例
第1の観点	**適切な水準のアクセス制御の実装**	• 設備等の設置エリアに至るまでに物理セキュリティ対策が講じられているという前提のもと、SCADA端末/サーバやエンジニアリング端末等の操作を許可する前に、操作者に対するID、パスワードによる認証の要求 • エンジニアリング端末等からコントローラへの接続を行う際、端末ID及びパスワードによる認証 • 従業員及び関連会社の職員に対しては、各々の職務に応じて最小限の権限のみの付与
	ソフトウェアのインストールの制限	• エンジニアリング端末やSCADA等のロボットシステムを構成する機器において、起動を許可するソフトウェアやプロセスを定めたホワイトリストの作成、及びリストに掲載されていないもののインストールや起動の防止
	IoT機器・システムにおける運用開始時の正しい設置、設定	• ロボットシステムを構成する設備を設置、設定する際、機器の動作仕様を考慮しつつ、運用開始までに動作状況の確認

3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
③リスク対応->整理した対策に対する意思決定

- 影響度が大きいリスクに対処するための対策方針を踏まえて実装することとした対策例は、以下の通り。

ロボット製造事業者に対応を依頼すべき対策の例

観点	対策要件	実際に講じる対策の例
第2の観点	**IoT機器・システムの適正な運用・保守**	• 設備等の設置エリアに至るまでに物理セキュリティ対策が講じられているという前提のもと、SCADA端末/サーバやエンジニアリング端末等の操作を許可する前に、操作者に対するID、パスワードによる認証の要求 • エンジニアリング端末等からコントローラへの接続を行う際、端末ID及びパスワードによる認証 • 従業員及び関連会社の職員に対しては、各々の職務に応じて最小限の権限のみの付与
	IoT機器・システムに対するアップデートの適用	• セキュリティアップデートを含むソフトウェアやファームウェアの更新を、以下のような措置を通じて不正アクセス等から保護したうえで実施 ✓ リモートアクセスを行う際、担当者に多要素認証の実施 ✓ 更新をネットワーク経由で遠隔から行う場合、通信経路を適切な方式による暗号化

1. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）の概要

2. 本ユースケース集の構成

3. 各ユースケースの概要

3-1.家庭用ガス給湯器の遠隔操作
3-2.ドローンを活用した個人による写真撮影
3-3.物流倉庫内のAGVによる自動ピッキング
3-4.化学プラント施設内の蒸留工程の自動制御
3-5.工場内のロボットによる部材加工作業（溶接工程）の自動化
3-6.金属製造現場の温度センサ等による製造設備の状態監視

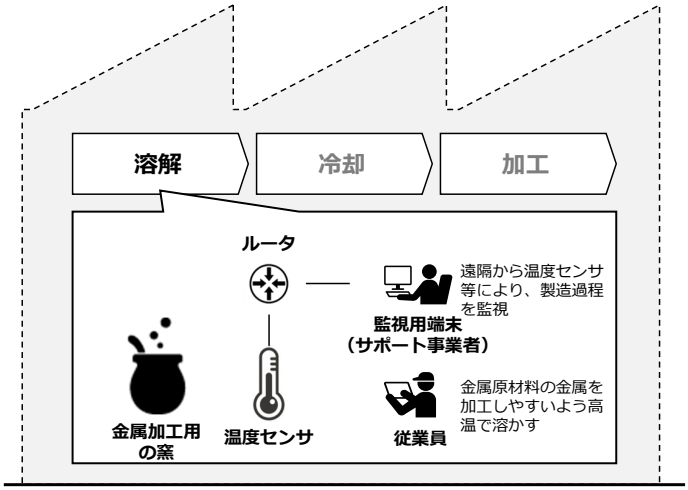
3-6.金属製造現場の温度センサ等による製造設備の状態監視

①リスクアセスメント、リスク対応に向けた事前準備->対象ソリューションの概要

- 本ユースケースの適用主体は、ユーザ事業者にサービスを提供するサポート事業者とする。
- 当該事業者は工場の設備等に設置した各種センサから得たデータに基づいて稼働情報を可視化することで、各設備・機器の状態を常時監視するサービスを企画しており、サービス提供を見越して金属製品製造事業者をユーザ事業者と設定して、リスクアセスメント及びリスク対応を実施。

- サポート事業者は工場の各設備に設置された各種IoT機器を通じて、設備の稼働情報を常時収集する。
- サポート事業者は収集した情報が適切な範囲に収まっているかを示すレポートを提供するものとする。
- サポート事業者が各設備の保守業務も請け負うこととし、もし設備の異常を検知した場合には、ユーザ事業者（金属製品製造事業者）の管理者にメール等で通知するとともに、即座に現場に駆け付けることを想定。

ユーザ事業者
（金属製品製造事業者）

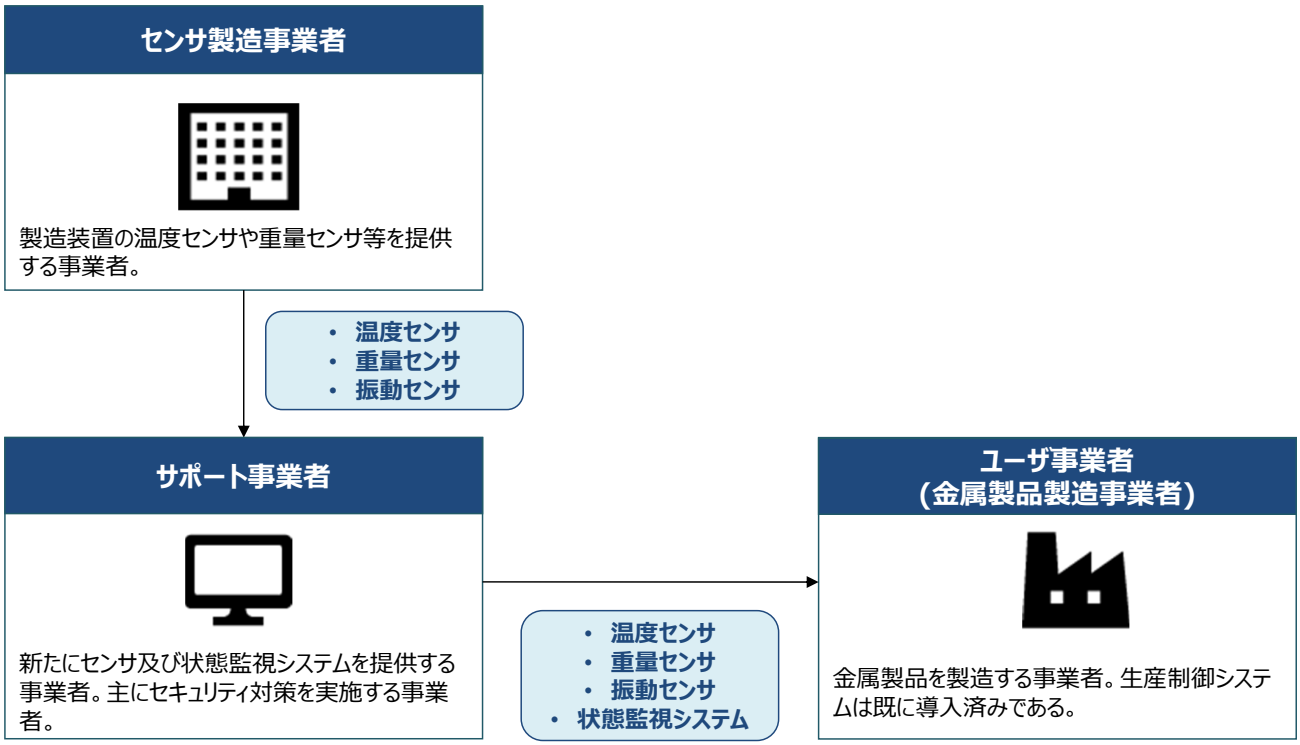


[参考] 経済産業省「中小ものづくり企業IoT等活用事例」等

3-6.金属製造現場の温度センサ等による製造設備の状態監視

①リスクアセスメント、リスク対応に向けた事前準備->ステークホルダー関係図

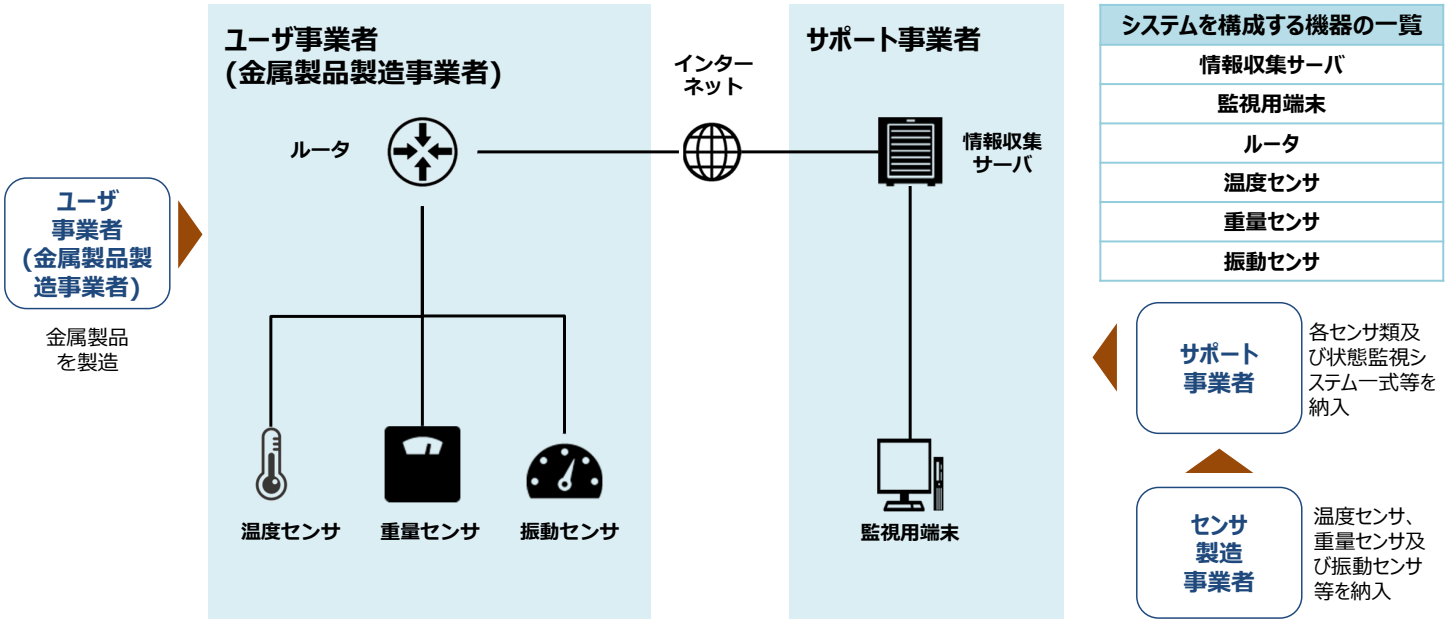
- ステークホルダーは、「サポート事業者」、「ユーザ事業者（金属製品製造事業者）」及び「センサ製造事業者」の３者。



[参考] 経済産業省「中小ものづくり企業IoT等活用事例」等

3-6.金属製造現場の温度センサ等による製造設備の状態監視
①リスクアセスメント、リスク対応に向けた事前準備->システム構成図

- システムを構成する機器は以下を想定。



[参考] 経済産業省「中小ものづくり企業IoT等活用事例」等

3-6.金属製造現場の温度センサ等による製造設備の状態監視
②リスクアセスメント->想定されるセキュリティインシデント等とその結果の特定

- ステークホルダーごとにリスクアセスメントを行うにあたり、対象機器・システムにおいて想定されるセキュリティインシデント及び想定される被害（例）を整理。

分類	想定されるセキュリティインシデント	想定される被害(例)
サポート事業者にとってのリスク	悪意のある攻撃者が、インターネット又はローカルネットワーク経由でサポート事業者が管理する情報収集サーバを**マルウェア（例：ランサムウェア）に感染させる。**	サーバの一部機能が停止することで、サポート事業者が**ユーザ事業者に対してサービスを提供できなくなるおそれがある。**
	悪意のある攻撃者又はサポート事業者の従業員が、インターネット又はローカルネットワーク経由でサポート事業者が管理する**情報収集サーバにDoS攻撃**を行う。	サーバの一部機能が停止することで、**温度情報等を正確に表示することができなくなる。**
ユーザ事業者(金属製品製造事業者)にとってのリスク	悪意のある攻撃者又はサポート事業者の従業員が、インターネット又はローカルネットワーク経由でサポート事業者が管理する**情報収集サーバに不正アクセス**する。	営業秘密として管理しているユーザ事業者（金属製品製造事業者）及び他の顧客における**設備の稼働情報等が流出することで、競争力が失われる。**
センサ製造事業者にとってのリスク	サポート事業者に対する注意喚起(例：設定方法に関する説明等)を怠る。	サービス提供における過失が認められ得る。（※）

※:その結果として、契約上の責任が問われ得る。

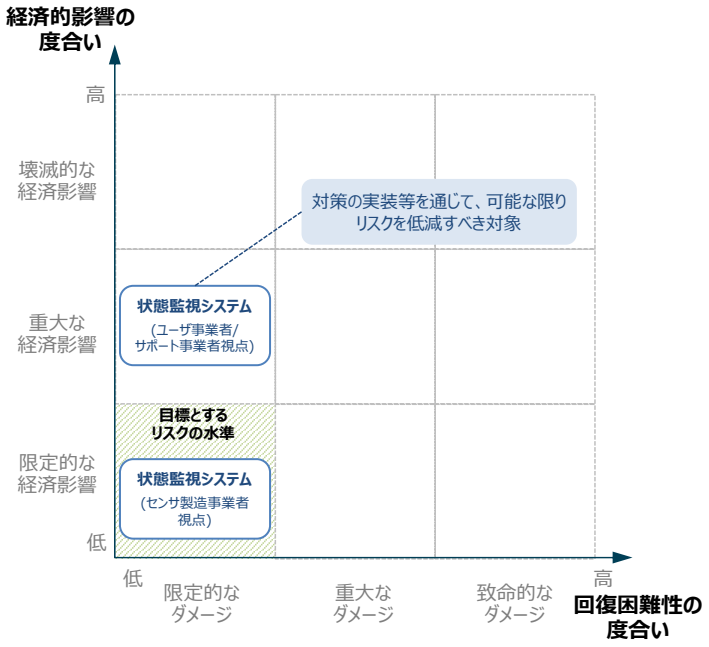
3-6.金属製造現場の温度センサ等による製造設備の状態監視
②リスクアセスメント->マッピング結果の整理と評価の実施

- IoT機器によって稼働情報を可視化しクラウド上でデータを管理する場合に、クラウドサーバから「ユーザ事業者」の営業秘密が外部へ流出する可能性が生じるため、IoT-SSFの適用主体である「サポート事業者」は、これらのリスクを踏まえて対策を実装することが望ましい。

リスクの大きさ（※1）

ステークホルダー	回復困難性の度合い	経済的影響の度合い(※2)
サポート事業者	• 従業員が重症を負う可能性は低い。	• ユーザ事業者に対してサービスを提供できなくなるおそれがある。
ユーザ事業者（金属製品製造事業者）	• 従業員が重症を負う可能性は低い。	• 営業秘密が流出することによって、競争力が失われるおそれがある。
センサ製造事業者	• 従業員が重症を負う可能性は低い。	• サービス提供における過失が認められ得る。

想定されるリスク(例)のマッピング結果

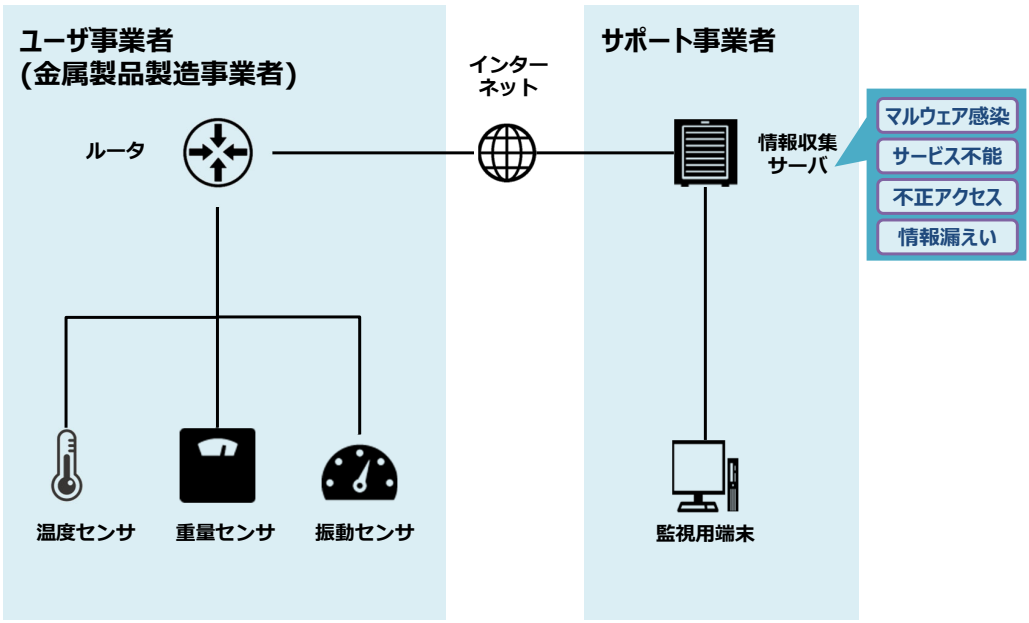


※1：「回復困難性の度合い」及び「経済的影響の度合い」では、主要な被害のみを記載していることに留意。
※2：「経済的影響の度合い」では、金銭的影響に加えて、社会的・生活的影響を含めて考慮するものとする。

3-6.金属製造現場の温度センサ等による製造設備の状態監視
③リスク対応->システムを構成する機器ごとの脅威の整理

- 「リスク評価、リスク対応に向けた事前準備」にて整理した機器ごとに脅威を整理する。

想定される脅威（例）



※太字・水色網掛けで示した脅威は、主要な被害を引き起こす可能性のある脅威を示す。

3-6.金属製造現場の温度センサ等による製造設備の状態監視
③リスク対応->脅威に対する対策の整理

- 適用主体であるサポート事業者は、リスクを目標とする水準に収めるため、影響が大きいリスクに対処するための対策方針を明確にした上で、行うべきと考えられる対策要件（例）を検討する。

サポート事業者（自身）にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
稼働情報の漏えいを防ぐ仕組みの構築	• 適切な水準のアクセス制御の実装 • 暗号化によるデータの保護
信頼性の高い状態監視システムを可能にするための仕組みの構築	• IoT機器・システムの十分な可用性の確保 • マルウェア対策の実施

ユーザ事業者（金属製品製造事業者）にとってのリスクを低減するための対策

影響が大きいリスクに対処するための対策方針	行うべきと考えられる対策の例
稼働情報の漏えいを防ぐ仕組みの構築	• 適切な水準のアクセス制御の実装 • 暗号化によるデータの保護

3-6.金属製造現場の温度センサ等による製造設備の状態監視
③リスク対応->脅威に対する対策の整理

- 想定される脅威を踏まえ、第3軸「求められるセキュリティ・セーフティ要求」における観点ごとにサポート事業者にて実装が想定される対策要件を整理する。

サポート事業者にて実装が想定される対策要件の例

第３軸	実装先	想定される脅威（例）	対策要件
第１の観点	ソシキ・ヒト	全般	IoT 機器・システムにおけるセキュリティポリシーの策定
		全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
		全般	IoT セキュリティに関するステークホルダーの役割の明確化
		全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	全般	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
		全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
		不正アクセス	適切な水準のアクセス制御の実装
		データの改ざん	ソフトウェアの完全性の検証
		情報漏えい	ソフトウェアのインストールの制限
		全般	様々な IoT 機器に接続する際のセキュリティの確保
		データの改ざん	暗号化によるデータの保護
		マルウェア感染	
		全般	IoT 機器・システムにおける運用開始時の正しい設置、設定
第２の観点	ソシキ・ヒト	全般	利用者へのリスクの周知等の情報発信
		全般	運用中における IoT セキュリティを目的とした体制の確保
		全般	過去の対応事例からの学習
	プロシージャ	全般	脆弱性対応に必要な手順等の整備と実践
		全般	インシデント対応手順の整備と実践
		全般	IoT 機器・システムの適正な使用
		全般	IoT 機器・システムの適正な運用・保守
	システム	全般	運用中における法令および契約上の要求事項の遵守
		不正アクセス マルウェア感染	継続的な資産管理
		全般	プログラムソースコード及び関連書類の保護
		不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
		全般	IoT 機器・システムに対するアップデートの適用

3-6.金属製造現場の温度センサ等による製造設備の状態監視
③リスク対応->整理した対策に対する意思決定

- サポート事業者がシステムの設計、開発、運用等の段階で実装することとした対策要件の例を以下に示す。

観点	対策要件	実際に講じる対策の例
第1の観点	**適切な水準のアクセス制御の実装**	• あるユーザ事業者（金属製品製造事業者以外の事業者も含む）から収集した稼働情報を、他のユーザ事業者から情報収集サーバ上で閲覧できないように、ユーザ事業者ごとに適切なアクセス権限の設定 • 想定されるリスクの大きさを考慮した方式による、ユーザ事業者や自社の従業員、接続するIoT機器の認証 • 情報収集サーバのアプリケーションへの特権アクセスに対して、多要素認証を適用 • パスワード等の認証情報の安全管理（例：ハッシュ化のうえ保管）
	暗号化によるデータの保護	• 通信中のデータにおける完全性の検証 • 情報収集サーバ上に保管されている稼働情報等の暗号化
	マルウェア対策の実施	• 情報収集サーバ及び監視用端末におけるマルウェア対策ソフトウェアの導入 • 不正通信検知機能を有するルータ等の導入
	IoT機器・システムの十分な可用性の確保	• 情報収集サーバやルータに対する(D)DoS攻撃を想定し、一定レベルの負荷に耐える容量や負荷分散用機器を確保 • 情報収集サーバやルータにおいて不審な通信（例：特定のIPアドレスからの大量のリクエスト）を検知し、適宜遮断等する • アプリケーションのテスト段階における一定レベルの負荷試験の実施

付録　「具体的なユースケースにおける記載事項」の概要

- 「具体的なユースケース」の記載事項とIoT-SSFにおける3つの軸の対応は、以下の通り。

記載項目

リスクアセスメント、リスク対応に向けた事前準備
- 対象ソリューションの概要
- ステークホルダー関係図
- システムを構成する機器の一覧
- システム構成図、データフロー図
- リスク基準

リスクアセスメント
- 想定されるセキュリティインシデント等とその結果の特定
- 機器・システムの重要度の判断基準及び判断された重要度の一覧
- マッピング結果の整理と評価の実施

リスク対応（ステークホルダー別の対策例一覧）
- システムを構成する機器ごとの脅威の整理
- 脅威への対策の整理
- 整理した対策に対する意思決定

IoT-SSFにおける3つの軸

第1軸：回復困難性の度合い

インシデントの影響の回復の困難性からリスクを捉えるもの

第2軸：経済的影響の度合い

インシデントによる影響の回復の可能性・困難性という観点を除き、インシデントによる影響の大きさを金銭的価値に換算した場合の大きさ・度合いを基準としたもの

第3軸：求められるセキュリティ・セーフティ要求

フィジカル・サイバー間をつなぐ機器・システムのセキュリティ対策を包括的に整理するため、セキュリティ・セーフティを確保するための手法を4つの観点から整理したもの

別紙 5

協調的なデータ利活用に向けたデータマネジメント・フレームワーク
～データによる価値創造の信頼性確保に向けた新たなアプローチ

Version 1.0

目次

1. 新たなデータマネジメントの在り方 3
1-1 CPSF における第 3 層（サイバー空間におけるつながり） 3
1-1-1 CPSF 概論 3
1-1-2 第 3 層の位置づけ 3
1-2 データの信頼性確保：データマネジメントの考え方の確立 4
1-3 本フレームワークの目的 6
1-4 本フレームワークの想定読者 8
2. 本フレームワークにおけるデータマネジメントのモデル 9
2-1 概要編 9
2-1-1 データマネジメントのモデル化の概要 9
2-1-2 リスク分析手順 10
2-2 詳細編 12
2-2-1 モデル化（「イベント」） 12
2-2-2 モデル化（「場」） 17
2-2-3 モデル化（「属性」） 19
3. 活用方法 21
3-1 サプライチェーンを構成するステークホルダー間での活用 21
3-2 ルール間のギャップの分析 22
添付 A.　ユースケース 24
A-1.　POS データの分析 24
A-2.　高齢者生活支援事業の提供 36
A-3.　IaaS、PaaS、SaaS 等を利用してサービスを提供する例 49
A-4.　国内で提供される IT サービスに関して、海外で開発や運用等を実施する例 62
添付 B　イベントごとのリスクの洗い出しのイメージ 72
B-1 イベントごとの典型的なリスクの記載方法等 72
B-2 イベントごとのリスクの洗い出しのイメージ 75

1. 新たなデータマネジメントの在り方

1-1 CPSFにおける第3層（サイバー空間におけるつながり）

1-1-1 CPSF概論

サイバー空間とフィジカル空間が高度に融合した産業社会においては、製品・サービスという価値を生み出す工程（サプライチェーン）が従来の定型的・直線的なものから、多様なつながりによる非定型的なものへと変化している。このような新たな価値創造過程（バリュークリエイションプロセス）のセキュリティ上の課題とその対策を整理することによって、新たな産業社会のセキュリティを確保していく考え方をまとめたものが、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）である。CPSF では、「バリュークリエイションプロセスのセキュリティ確保にあたっては、従来のサプライチェーンで想定されているマネジメントの信頼できる企業間のつながりによって付加価値が創造される領域を越えて、フィジカル空間の情報が IoT によってデジタル化され、データとしてサイバー空間に取り込まれ、そうしたデータがサイバー空間で自由に流通することで、多様なデータが新たなデータを生み出して付加価値を創出することや、新たに創出されたデータが IoT によってフィジカル空間にフィードバックされることで新たな製品やサービスを創出するという、新たな付加価値を創造するための一連の新たな活動を視野に入れる必要がある」とし、企業間のつながりに信頼性の基点を置く第 1 層、フィジカル空間とサイバー空間のつながりに信頼性の基点を置く第 2 層、サイバー空間におけるつながりに信頼性の基点を置く第 3 層という異なる 3 つの信頼性の基点を設定し、これらの基点を中心に経済社会全体のセキュリティ上の課題の洗い出しとその対策をまとめている。

1-1-2 第3層の位置づけ

あらゆるモノがネットワークにつながっていくことでサイバー空間が急激に拡大し、それらの間で行き交うデジタル化されたデータが爆発的に増大している。サイバー空間の中では、データが自由に流通し、物理的な距離に縛られることなくデータを入手して編集・加工したり、これまでは処理が容易ではなかった大量のデータを様々な切り口から分析してインテリジェンスを抽出したりするような、新たな価値を創造する活動が加速度的に広がっている。ネットワーク越しに提供される新たなサービスは、サーバなどの物理的な情報システムの上で展開されているが、その多くにおいてサービスを生み出す活動は物理上の特性ではなく、論理によって実現され[1]、付加価値を創造しているのは物理特性に依存しないデータである。データは基本的にシス

[1] 以前は特定のハードウェアでしか実現できなかった機能が、ミドルウェアの発達等により、ハードウェアの特性に縛られずにソフトウェアによって実現されるようになっている。

テムや組織に対して中立性を持つものであり、それが求められる規範等に則って適切に扱われることによって、自由に流通・活用される。こうした活動、サイバー空間におけるつながりが展開される場が第3層であり、ここでは、データがサイバー空間で付加価値を創出する基礎となる。

第3層におけるデータの生成・移転・加工等のライフサイクルの各工程には、第1層においてマネジメントの信頼性が確認された企業（組織）のみが関わる訳ではない。データのライフサイクルには様々な主体が関与し、関与した主体による不適切な措置によって誤ったデータが流通し活用されることになれば、そのデータが関わったバリュークリエイションもまた価値をもたらすことはなく、有害な結果をもたらすことにもつながりかねない。例えば、サイバー空間から発信されたIoTシステムへの動作指令が誤った内容であるならば、第2層における“転写”する機能の信頼性を確保することに成功していたとしても、IoTシステムはサイバー空間から届いた誤った指令を“正しく”転写して忠実に動作することで物理的な損害を発生させてしまうかもしれない。

つまり、第3層においては、データそのものが正しいことが最も重要な前提であり[2]、付加価値の創出（バリュークリエイション）の基礎となるデータが、バリュークリエイションプロセスの信頼性を確保するための信頼性の基点でなければならない。

1-2 データの信頼性確保：データマネジメントの考え方の確立

CPSFは、サイバー空間とフィジカル空間が高度に融合した産業社会において動的に構成されるサプライチェーンをバリュークリエイションプロセスとして捉え、産業社会に対して3つの層を設定してこれに合わせて信頼性の基点を導入することで、動的かつ複雑な姿を見せるバリュークリエイションプロセスにおけるリスクを包括的に洗い出し、対応策を実施できるようにするためのフレームワークである。その中の第3層の位置づけは既に述べたとおりだが、データ自体に信頼性の基点を置いて包括的なセキュリティ対策を実施するためには、データのライフサイクル全体にわたってリスクを洗い出し、セキュリティ確保のための様々な措置を実施することが必要となる。

ここで留意すべきことは、第3層では信頼性の基点をデータに置いている一方、データのライフサイクルは第3層の中に閉じるものではないということである。

CPSFでは、「第3層においては、サイバー空間のデータ及び、その加工・分析・保管という諸

[2] セキュリティの確保に向けては、データの機密性、完全性及び可用性を維持することが必要である。ここでは、そのうち、第三層におけるデータそのものが正しいこと（完全性）の重要性を特に強調して説明しているものであり、対策等を検討するにあたっては、機密性・可用性についても考慮する必要がある。

機能の信頼性を確保する」ことが必要であるとするとともに、「フィジカル空間からサイバー空間に転写されたデータは第2層の転写機能の信頼性を確保することによってデータの信頼性が確保されるが、サイバー空間では様々なデータが生成・編集・加工され、自由に流通し、かつ、こうした過程はマネジメントの信頼性が確認された企業（組織）によってのみ扱われるわけではない」とし、データが生成される場所については第3層ではなく第2層に属する場合があることを明確にし、第3層と第2層とを組み合わせることでデータ生成における信頼性を確保する考え方を示している。

つまり、データの信頼性を確保するためには、CPSFの第3層の考え方を基礎とした上で、そのコンセプトの適用範囲を拡張し、データを軸として、データの生成・取得から廃棄に至るライフサイクル全体を視野に入れた対応、つまり、データマネジメントの在り方に関する枠組みを設定することが必要になる。この枠組みでは、データのライフサイクルの各工程において発生する様々な形の“関与”をデータマネジメントとして捉え、これをモデル化することでデータに関わるリスクの洗い出しと対応策の整理を行うことになる。

この考え方で整理を進めていくにあたって、以下の3つの視点を押さえておく必要がある。

①データマネジメントについて確立した定義は存在しない。

②データの信頼性の観点からデータマネジメントを捉える場合、データに関与する主体の視点からではなく、データを軸に置く必要があり、データがライフサイクルの各工程においてどのような関与を受けるかという視点で整理すべきある。

③データマネジメントをデータのライフサイクルの各工程おいて発生する様々な関与の総体を意味するものと整理した場合、関与する主体は同一・単一の主体に限られるものではないことから、データマネジメントは複数の主体による協同的活動（Collective Action）になることを排除しない。

①の視点から導かれることは、データマネジメントという言葉に対する各人の理解は現時点では一致しているわけではないということである。

本フレームワークは、他の機関等において整理された既にあるデータマネジメントの定義を持ち込むのではなく、CPSFを基礎としてデータを軸においてセキュリティ対策を検討するために必要なデータマネジメントの考え方を示すものである。ここで示すデータマネジメントの考え方を改めて共有することにより、これまで各組織や各国においてデータ管理に関する議論がなかなか噛み合わず、それぞれが整備したデータ管理に関するルール等の間の調整を図ることが難しかったところ、共通の尺度として本フレームワークを活用してデータマネジメントに関する共通の理解を得ることで、異なるデータ管理のルール等の間について、ルール間を跨いでデータが

流通した場合でもデータのセキュリティが同じように確保されるために必要な調整を図ることが可能となる。

②の視点を強調しているのは、様々な団体等がこれまでに提示してきたデータマネジメントの考え方は「データという資産を組織が如何に生かすか」という視点で整理され、データのライフサイクル全般を捉えたものではないため、データの信頼性を包括的に確保するためのフレームとはなっていないことを明らかにする必要があるためである。

データの信頼性は、データが基本的に組織等からの中立性を持っていることを踏まえ、データを軸に置き、当該データの信頼性を確保するために求められる措置を整理して実施することで確保されるのであり、それに関与する主体の立場から整理された当該主体が実施すべき必要な措置は、データに対して本来求められる措置全体に対する部分的な措置でしかないことを改めて明確にする必要がある。

③の視点は、②の視点によってデータマネジメントが単一の主体によるマネジメントであるという考え方から解放されたことで、ライフサイクルの工程において関与する主体は一つのモノに限定されるのではなく、複数の主体が同時に関与し、かつ、関与する際に求められる措置も各主体によって異なることがあるということを明らかにするものである。この③の視点を導入することで、サービスを構成するシステムが複数のサービサーによって実現されるクラウドサービス（例えば、ユーザー企業A社が利用するB社のSaaSはC社のPaaSの上で展開し、C社のPaaSはD社のIaaSで展開されるようなケース）におけるデータの扱いを考える場合などにおいて各主体に求められることや、データがシステム等に対して基本的に中立性を持っていることを踏まえたゼロトラストの概念に基づくアーキテクチャを明確に整理することができることになる。

以上の3つの視点は、本フレームワークを理解するための基礎条件となるものであり、改めて、その重要性をここで強調しておきたい。

1-3 本フレームワークの目的

本フレームワークは、主体間を転々流通するデータの信頼性を確保することでバリュークリエイションプロセスが付加価値を生み出していくために、データを軸に置き、データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し、そのセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することを可能とすることを目的としている。データのライフサイクルの各工程において直面するリスクは、単一の主体が実施可能な措置によって対応できるものに限定されるわけではないため、データのライフサイクルの工程に関与する主体がそれぞれ実施すべき措置を他の主体と協調して取

り組むことによってデータのセキュリティを確保することが必要になる。なお、協調的な取組の一環として各主体においてそれぞれ行うべきとされた具体的な措置は、各主体のガバナンスのもとで適切に実施される必要がある。

したがって、本フレームワークは、単独の組織のマネジメントの在り方について整理したものではなく、データを軸においてそのリスクに対処するという観点から、データに関与する主体＝ステークホルダーが協調して、組織のガバナンスを含めた必要な措置を実施することを促進する枠組みとなる。

データのセキュリティを確保するために必要な措置自体については、これまでに公表されてきた情報セキュリティに関する様々な国際標準等が「データマネジメント知識体系（DMBOK）」として既にまとめられていることから、本フレームワークを使って洗い出されたリスクに対する措置はDMBOK等の既存文書を参照して具体的な措置内容を選択することが可能である。

また、本フレームワークは、データが置かれた環境におけるリスクを明らかにして、セキュリティを確保するという役割に加え、データの流通を促進するための環境を実現するために必要な条件を明確化する役割も果たすことが可能である。

本フレームワークは、データの置かれている状態を可視化することでリスクを洗い出し、リスクに対処するために関与する主体それぞれに求められる適切な措置を明確化する（as is の対策）が、この考え方を拡張し、データを異なった環境に遷移させようとする際にデータの状態がどのような条件を満たせば異なる環境でもセキュリティが確保され、問題なく遷移させることが可能となるかを明らかにする（to be の対策）ことができる。例えば、データ交換プラットフォームとなっている異なるシステムの間で、特別な措置を必要とせずに自由にデータ交換を行うことができる環境を実現するためには、システム間の機能連携のためのAPIを設定することに加え、両システムで共有するデータ交換のためのプロトコルを整備することが必要になるが、本フレームワークを活用することで、プロトコルの設計が容易になる。

また、本フレームワークの考え方が広く共有され、一般的な活動として定着すれば、影響力に違いのあるシステム間において強い立場にあるシステムがデータ交換に必要なプロトコルをブラックボックスにすることで当該システムに他のシステムを依存させようとする（「バンドルする」）ことを難しくさせ、オープン化された環境でデータ連携やシステムの組み合わせの自由を確保し、より効率的なデータ活用モデルを実現することが可能となる。

更に視野を広げると、データ管理に関わる制度間における、データのセキュリティの確保のために要求されている条件や措置の相違（ギャップ）を明確化するためのモデルとしても活用することが可能である。

各組織が整備したデータ管理に関わる制度は、プライバシー保護や情報の機微性保持等のそれぞれの目的からデータ管理に関する条件や措置を設定しているが、制度間で自動的に調整する機能がないことから、制度ごとに条件等が異なることで事実上データが一つの制度の中に“囲い込まれる”ことになり、データの流通が妨げられていることが少なくない。国際的にも、個人情報保護を目的としながらも、同じ目的であるにも関わらず各国で制度的な条件や措置が異なり、事実上国境を跨いでデータを流通させることが困難になってしまっているようなケースが見られる[3]。

こうした制度で要求されているデータ管理に関する条件や措置は、同じ目的であるならばデータ管理についての条件や措置も同じ内容であるべきだが、実際には、データの状態に着目するのではなく、これに関わる主体を管理することを考慮して設定されたと思われることが少なくなく、このことが制度間のギャップをもたらしている。

本フレームワークは、データを軸にして、客体であるデータの状態を可視化し、データの状態が満たすべき条件や実施されている措置を明らかにするものであり、関与する主体の在り方などを過度に考慮することなく、データに対して本来求められる条件等を歪めることなく整理することが可能であることから、本フレームワークを活用して各国の制度間に存在するギャップ分析を行い、分析結果をモデル化し、データ流通を可能とするために必要なギャップの調整措置を明らかにすることが可能となる。

1-4 本フレームワークの想定読者

上記のとおり、本フレームワークは、データのセキュリティ確保のためのデータマネジメントを可能とする機能に加え、データを流通させるための環境を実現するための、データ遷移をする地点間のギャップの的確な分析を可能とする機能を持つものであり、データを管理する現場レベルでの活用から、データ管理に関する仕組みや制度設計、更に国際的なデータ共有の仕組み作りにまで活用することができるものである。

したがって、本フレームワークは以下のような者に活用してもらうことが期待される。

- ●真正であり、適切なセキュリティを確保することが求められるデータを扱う者、特に、データを利活用して価値を創造するバリュークリエイションプロセスに参加する者
- ●データ利活用に関するサービスを提供する者
- ●データ利活用に関するサービスを提供するシステムの設計・構築・運用に関わる者

[3] 一方で、GDPR における「データポータビリティ権」など、制度がデータの囲い込みの手段ではなく、データの可搬性（ポータビリティ）を確保する役割を果たす場合もある。

●データに求められる条件として適切なトラストを保証することが必要な場合の適切な水準のトラストサービスを提供しようとする者

●データセキュリティに関わるガイドライン等のルール設定に関わる者

2. 本フレームワークにおけるデータマネジメントのモデル

2-1 概要編

2-1-1 データマネジメントのモデル化の概要

データは、目的を持って生成・取得され、それが転々流通し、その属性を変えながら様々な形で活用されて付加価値を生み出していく。データのライフサイクル全般にわたってセキュリティを確保することが、第3層における付加価値を創造する活動の鍵となる。そのため、本フレームワークでは、データを軸に置き、データのライフサイクルを通してデータの置かれている状態を可視化することにより、データのライフサイクル全般にわたってリスクベースでデータのセキュリティを確保するための取組を進められる環境の実現を目指している。

このアプローチの鍵となるのが、データの置かれている状態を可視化する方法であり、可視化の枠組みとして機能することになるデータマネジメントのモデルである。

本フレームワークでは、データマネジメントを「データの属性が場におけるイベントにより変化する過程を、ライフサイクルを踏まえて管理すること」と定義し、データマネジメントを、データが有する性質である「属性」、データに対して特定の規範を共有する範囲である「場」、データの属性を生成・変化・維持などをする作用である「イベント」の3つの要素から構成されるモデルとして整理する。

この3つの要素を使ってデータの置かれた状態を可視化することにより、データに対してどのようなリスクが存在し、それに対してどう対処すべきか、ということを明確にすることができる。また、この3つの要素はそれぞれが相互に影響しあう関係にあるため、データが移転して要素の一つが変化することで他の要素も変化するという、状態の変化を連続的なものとして捉え、次に発生する変化の予見可能性を高めることにより、データマネジメントを行う際のポイントを把握しやすくする。

3つの要素がどのような関係を持つか、整理する。

「属性」は、どのようなカテゴリに区分されるのか、どのような機密性が求められるのか、誰が権利を行使し得るのか等のデータの持つ性質であるが、この「属性」は、個人情報が匿名加工という作用を経て匿名加工情報になるように、データに対する作用(「イベント」)によって変化

するものであるだけでなく、例えば、個人情報保護法[4]に基づいてデータがどのように扱われなければならないのか、特定組織の内部規程でデータのアクセス権者をどのように定めているか等の「場」の要求によって「属性」の内容が決められる部分が存在し、「属性」と「場」は相互に依存する関係にある。同様に、例えば、電気事業に関する法令では、電気事業者が持つ電気利用に関する顧客のデータを電気事業者以外の者が利用することを目的に電気事業者がデータを提供する場合に、電気事業者が行うべきデータの加工処理の内容が定められているように、データの存在する「場」がデータの「属性」を適切に管理するために特定の作用「イベント」を要求することが頻繁に発生する。したがって、「場」と「イベント」についても、それぞれ関連するものと捉えることが必要になる。

つまり、「属性」と「場」と「イベント」は相互に影響しあう関係にあり、それぞれが他の要素の影響を受けることなく独立して決定されることは限られた場合であり、「属性」、「場」が「イベント」によって変化する場合には、それぞれが関連して連続性を持つことになる。したがって、データのライフサイクルを連続的なデータの状態の変化とし、予見可能性に基づいて、次の状態に遷移する場合の3つの要素について許容される変化の内容や変化幅を捉えることができる本モデルを使うことで、データマネジメントにおいてより現実的かつ効率的な対処を検討するに際してその機能を発揮する。

また、本フレームワークの目的で述べたように、データのライフサイクルの各工程には複数の主体が関与することになり、ステークホルダーの間で共通の理解に基づいたデータマネジメントの取組が必要となるが、3つの要素によってデータの状態が可視化され、かつ、3つの要素の相互依存関係から、データの遷移によるデータの変化に関する一定の予見可能性が確保されることから、ステークホルダーの間で認識を共有しやすくなる。その結果、ステークホルダーの間では、共通の理解に基づいてそれぞれの主体が実施すべき措置についての検討を進めることが可能となり、ステークホルダー全体で適切なデータマネジメントを実施していくことができる環境を実現していくことにつながっていく。

2-1-2 リスク分析手順

一連のバリュークリエイションプロセスに関わるステークホルダーが、共通の理解に基づいてそれぞれの主体が実施すべき措置の検討を進めるためには、当該バリュークリエイションプロセスにおけるデータに関わるリスクを洗い出し、主体間で認識を共有することが必要である。

---

[4] 本稿では、個人情報の保護に関する法律（平成十五年法律第五十七号）の略称として、「個人情報保護法」という表記を用いる。

その際、「属性」、「場」及び「イベント」の3つの要素によってデータの状態を可視化することでリスクの洗い出しを行うことが可能となるが、その際には下記の4つのステップに沿ってバリュークリエイションプロセスにおけるデータの状態を可視化することで、データに関わるリスクの洗い出しと対応策の整理を実施することが可能となる。

STEP 1　データ処理フロー（「イベント」）の可視化

- まず、データの生成・取得から廃棄に至るまで、想定されるデータ利活用プロセスにおける大まかなデータフロー及び「イベント」を可視化する。
- その際、「イベント」をどの程度詳細に記述するかは、データフロー整理の目的に応じて調整する必要がある。例えば、企業内ネットワークでのサーバ・クライアント間のデータの移転という「イベント」は、複数のステークホルダー間で転々流通するデータを扱う際の対策等を検討するには、検討の本質とは異なる場合があることから省略し、データの取扱いに係るマネジメントのルールを提示し、それに従って取扱っていることを示すことで代替することも考えられる。

STEP 2 必要な制度的な保護措置（「場」）の整理

- データ保護に資する「場」を検討し、法律・契約の観点から適切なものを設定する。その際、一つのデータに対して複数の「場」が重なり合う、つまり、データに対して様々な観点からの要求がなされることが考えられる。

STEP 3 「属性」の具体化

- 設定されたデータや「イベント」、「場」に基づいて、管理上あるべき「属性」を特定する。
- 場合によっては、データの「属性」を整理していく中で、本データが取扱われるべき「場」や実施されるべき「イベント」に漏れがあった場合、適宜追加等を実施する。

STEP 4 「イベント」ごとのリスクポイントの洗い出し

- 設定された「場」という観点から、「イベント」ごとに想定されるリスクを抽出し、設定した「属性」をレビューする。
- その際、機密性・完全性・可用性といったサイバーセキュリティに係る観点のほか、各法制度等に係るコンプライアンスの観点でのリスクについても洗い出す必要がある。

なお、上記のとおり、「属性」、「場」、「イベント」が相互に依存する関係にあることから、STEP 1～3については、お互いにフィードバックをかけながら検討されることが適切であると言える。すなわち、各ステップは不可逆的なものではなく、例えばSTEP 3を検討中に「イベント」の追加が必要であることが判明することもありうる。その際にはSTEP 1に戻って当該必要な「イベント」を追加し、その状態でSTEP 2やSTEP 3を再度検討することで、「属性」、「場」、「イベント」が十

分に整理し、その後にSTEP 4に進むことで、適切な形でリスクの洗い出しを実施することが可能になる。また、STEP 4までの取組が完了した後も、内外の要因により従前に特定した「属性」、「場」、「イベント」の内容が変更されることで、新たなリスクが出現したり、想定していた内容が変化したりすることが想定される。そのため、データ利活用のプロセスや関連する法制度等に何らかの変更を認識した場合、あるいは対象となるプロセスや扱われるデータの特性等を踏まえて設定された適切な間隔で、STEP 1からSTEP 3までの検討結果をレビューし、改めてリスクポイントの洗い出しを行うことが望ましい。

2-2 詳細編

2-1において、本フレームワークを用いたリスクの洗い出しの方法を概観してきたが、実際に本フレームワークを活用するにあたっては、「属性」、「場」、「イベント」を適切に設定することが肝要である。そこで、以下にモデル化やリスク分析の詳細を整理する。

ただし、特に「場」や「属性」に関しては、取扱うデータの性質や、バリュークリエイションプロセスを構成するステークホルダーの性質によってその内容は多様であり、網羅的に示すことには困難が伴う。フレームワークの活用にあたっては、下記の記述を参考にしながら、組織等の実情を踏まえて必要な「イベント」、「場」、「属性」を設定し、リスクの洗い出しを実施する必要がある点に留意されたい。

2-2-1 モデル化（「イベント」）

データの属性を生成・変化・維持などをする作用である「イベント」に関しては、大きくは「生成・取得」「加工・利用」「移転・提供」「保管」「廃棄」の5つに区分することが可能である。なお、それぞれの「イベント」ごとに考慮すべきリスクの例は、添付の形で示す。

- 生成・取得

  バリュークリエイションプロセスにおいて、サイバー空間でやりとりされるデータは、センサーによる計測等の自動的な手段又は人手による入力等を介して生成・取得されることによってそのライフサイクルが始まる。

  これまでに、データが生成される場所については第3層ではなく第2層に属する場合があることを明確にし、第3層と第2層とを組み合わせることでデータ生成における信頼性を確保する考え方を示している。サイバー空間とフィジカル空間が高度に融合し、センサーによるデータの取得など、フィジカル空間の情報が大量にサイバー空間に転写され、リアルタイムに共有されるようになると、サイバー空間のつながりにおけるデータの

信頼性を検討する場合、センサー等によって物理的な情報がデータとして正しく転写されているかなど、従来はデータを管理する範疇に捉えられていなかった、データの生成に関わる機器・システムなどの信頼性についても検討する必要がある点に留意が必要である。例えば、第2層においてサイバー空間への転写が正しく行われるよう、セキュリティ侵害（例：ソフトウェアの改ざん）を受けていない信頼できるIoT機器によりデータを生成し、なりすましやネットワーク上での改ざん等がないようサーバ等へ正確に当該データを送信することを通じて、第3層において利活用するデータの信頼性をデータライフサイクルの初期段階から確保することが可能である。なお、本件に関しては、CPSFの第2層（サイバー空間とフィジカル空間のつながり）における信頼性の確保として、IoT機器・システムのセキュリティ・セーフティ対策を検討した「IoTセキュリティ・セーフティ・フレームワーク」でも触れられており、フレームワーク間で連動する構造になる。

本イベントにおいて考えられる代表的なリスクとして、計測結果が実際と異なる、計測機器をなりすまされる等の転写の失敗、システム障害等に起因する生成・取得の停止、不適切なプロセスによる個人情報の取得などが挙げられる。

- 加工・利用

生成・取得されたデータは必ずしもそのまま単純に付加価値を生み出すというわけではなく、何らかの作用を通じて付加価値を伴うものとなっていく。例えば、いわゆる生データから、利用目的に合わせて抽出やトリミングなど様々な処理を行い、データを利用しやすくした上で、そのデータを閲覧したり、そのようなデータからAI等を利用することでインテリジェンスを抽出したりすることによって付加価値につながる。本フレームワークでは、このような付加価値を生み出すための作用を加工・利用と捉える。

なお、データの一部の項目や要素、レコードなどを、その分析過程や保管されたデータセットから取り除く作用については、加工の一形態として捉えるものとし、後述する廃棄とは区別して捉えるものとする。

また、データを保有しない者がデータにアクセスする作用（閲覧）については、付加価値を生み出すための作用である点から利用の一形態として捉えることが適切であるが、データを複製して共有することで閲覧させる場合には、複製元のデータを保有する移転元だけでなく、移転先もデータを管理することとなるため、リスクを洗い出すにあたっては移転・提供の要素を考慮に入れる必要がある。

本イベントにおいて、考えられる代表的なリスクは、データの目的外利用、不適切な

加工などである。

- 移転・提供

サイバー空間とフィジカル空間が高度に融合した社会であるSociety5.0においては、様々な主体が動的にサプライチェーンを構成することになるが、その過程では、必ず組織を跨ぐ移転が行われる。企業間のつながりで固定的なサプライチェーンを構成する場合であっても、データの組織間の移転・提供は一定のリスクを孕むものとして慎重に処理されてきたが、サプライチェーンを動的に構成する場合には、その効果を最大限に引き出すためにはより自由にデータの移転・提供を実施できる環境にすることが求められ、その裏腹の関係として、リスクに対してもより効果的に対応することが求められることになり、そのための制度も含めた環境を整備しなければならない。

また、データの移転・提供は、一般にデータが複製されて移転元にデータが残ったまま移転先でもデータを管理することになる。そのため、加工・利用の説明において既に述べたとおり、データを保有しない者がデータにアクセスする作用（閲覧）については、リスクを洗い出すにあたっては移転・提供の要素を考慮に入れる必要がある。

なお、本フレームワークにおける移転・提供には、機器と機器、例えばサーバとクライアントの間でのデータの移転・提供も取扱うこととする。これによって、悪意のある者によるネットワーク上での盗聴やデータの移転・提供に係るシステムの不具合等によるデータの損傷等のリスクを捉えることが可能になる。

そこで、本フレームワークにおいては、対象となる移転・提供事象について、国・地域、組織・ヒト、システム・サービス、機器という4つの単位で整理することとする。単一の移転・提供事象についてリスクやその他の留意事項を整理しようとする際、その具体的な方法等に応じて、同時に複数の単位が考慮され得る。これにより、技術的・非技術的なリスクを網羅的に識別するにあたり有用と考えられる。4つの単位の概要や実際に考慮すべき事項は下記のとおり整理できる。

ー　国・地域

この単位においては、対象となる移転・提供事象に関連する国・地域及び、域外適用されるものも含めて当該国・地域におけるデータ保護関連の政策、法令、ガイドライン等を特定し、それらに係るリスクや対応に必要な手続き等を整理する。当該移転・提供事象が現に特定の法令等が適用される国・地域を越えて行われ

ている、あるいは国・地域内の移転・提供であっても境界を越えているとみなせる方法（例：「みなし輸出」に該当する行為）で行われている場合に考慮すべき単位である。具体的には、個人情報保護関連法令における個人情報の越境移転や外為法等の輸出管理関連法令における技術情報等の輸出、海外のデータ保護法令における特定データの国内保存に関する規定や域外適用に関する規定等が該当し得る。検討にあたっては、それらに係るリスク（例：法令違反、社会的な信用の失墜）、適正な移転・提供実施のために必要な手続き（例：個人情報を日本から海外にある第三者に移転する際の本人同意の取得、本人への情報提供等）を含めて特定することが望ましい。

- 組織・ヒト

この単位においては、対象となる移転・提供事象に関連する組織及びヒト、当該主体におけるデータ保護関連の方針、体制等を特定し、それらに係るリスクや必要となる対処等を整理する。当該移転・提供事象が、ある組織・ヒトからセキュリティポリシー等の異なる別の組織・ヒトへ行われる場合に考慮すべき単位である。同一の法人内のデータ移転・提供であったとしても、適用されるセキュリティポリシーが異なる部門（例：本社と生産拠点）間で行われる場合はこちらに該当する点に注意が必要である。例えば、ある組織から事業上有用なデータを他の組織に移転・提供する際、セキュリティ水準が相対的に低い組織・ヒトから重要なデータが漏えいするリスクが懸念されるため、移転先となる組織及びヒトに係るセキュリティ対策やその他のデータ保護措置の実施状況（例：ISMS認証等の取得有無）を確認する等の対処が特定され得る。

- システム・サービス

この単位においては、移転・提供を実行するシステム及び当該システムが提供する機能としてのサービス（用いられるプロトコル等を含む）、それらが備えるデータ保護機能を特定し、想定されるリスク（例：ネットワーク上での盗聴、送信元/送信先のなりすまし）や必要な対処を整理する。当該事象が、ネットワークを通じて機器間で電子的に行われる場合に考慮すべき単位である。データの移転・提供に用いられるシステム・サービスには、例えば、クラウドストレージ、電子メール、ファイル転送（例：FTP、HTTP）等、様々なものが含まれるが、現に移転・提供されるデータのカテゴリや価値（重要度）等を考慮して、十分なセキュリティ等の水準を有している手法が利用されるべきである。例えば、クラウドストレージを用い

てデータを移転・提供する際、クラウドストレージ側の脆弱性を悪用されデータが漏えいするリスクや、サービス利用者側の設定ミス等によりデータが外部からアクセス可能となるリスク等が想定されることから、事前に当該クラウドサービスにおけるセキュリティ機能の実装状況を確認する、サービス利用時に利用者側で実施すべき事項を文書化しておく等の対処が特定され得る。

ー 機器

この単位においては、移転・提供事象を実行する単体のシステムコンポーネント（例：サーバ、IoT機器、ネットワーク機器）及びそれらが備えるデータ保護機能を特定し、想定されるリスク（例：機器内の不正なコンポーネントを通じた意図しないデータ移転、サービス拒否攻撃等による機器の稼働停止）や必要な対処を整理する。当該事象が、ネットワーク又は可搬媒体等を通じて行われる場合に考慮すべき単位である。例えば、クラウドストレージを用いてデータを移転・提供する際、クラウドサービスにアクセスする端末が外部から不正アクセスされ、クラウドストレージのデータにアクセスされる等のリスクが想定されることから、当該端末を利用しようとする際の認証機能を強化する、同端末におけるエンドポイント向けのセキュリティ対策（例：マルウェア対策ソフトウェア、EDRの導入）を強化する等の対処が特定され得る。

前述のとおり、「イベント」をどの程度詳細に記述するかは、データフローの整理の目的に応じて調整する必要がある。例えば、企業内ネットワークでのサーバ・クライアント間のデータの移転という「イベント」は、複数のステークホルダー間で転々流通する場合のデータマネジメントを検討する際には省略されることも考えられる。

- 保管

保管については、他のイベントに付随して必ず生じる「イベント」である[5]。データはライフサイクルの様々な段階において、ネットワーク接続されたストレージ機器（オンプレミス、クラウドの双方を含む）、クライアントのハードディスク、USBメモリのような可搬媒体、機器の一時記憶領域等に保管され得る。データの取扱に関してリスクを洗い出し、セキュリティ対策を検討する上では、移転・提供、加工・利用されるデータとは異なるリス

[5] 本稿では、データを長期保存する際に行われる「アーカイブ」も保管に含まれるものと捉える。

クが生じうることから、「イベント」の一類型として整理し、リスクの洗い出しを実施することが適切と考えられる。

- 廃棄

加工・利用されたデータは、ライフサイクルの終わりとして、適切に廃棄される必要がある。

なお、本フレームワークにおける廃棄は、データセット全体を使用不可能な状態とすることを指す[6]。データは自組織が直接的に管理する媒体だけでなく様々な媒体に複製され得るが、当該データのカテゴリや重要度等を勘案して、組織は当該データに対する権限や複製、配布等の状況について適切に管理する必要がある。元のデータを廃棄する際に、複製先のデータも含めて廃棄する必要がある場合には、関連するステークホルダーと協議する等、文脈に応じて適切な廃棄の取組を推進する必要がある。なお、個人の同意に基づいて収集したパーソナルデータに関して、特定の個人が同意を撤回する等により、当該個人のデータをデータセットから除外する行為は、加工・利用の一形態として捉えるのが適切である。

本「イベント」における代表的なリスクは、廃棄すべきデータが残存して漏えいする、本来は廃棄すべきでないデータまで廃棄してしまう等が考えられる。

5つの「イベント」は、それぞれ重複する性質を持つ場合がある。例えば、国外にある他組織が公開しているデータを閲覧することは、データの加工・利用の性質を有するが、国・地域間及び組織間におけるデータの移転・提供という性質を内包する。さらに、自組織内における機器間での移転も含まれることから、目的に応じて適切に「イベント」を捉え、リスクの洗い出しを実施する必要がある。

2-2-2 モデル化(「場」)

前述のとおり、「場」はデータに対して特定の規範を共有する範囲と定義している。データに対する規範は、各国・地域等の法令によって定められているもの、組織で定められた内部規則、組織間で個別に取り交わされる契約などの様々な形態が存在し、取扱うデータの性質や、

[6] データの「属性」や「場」の規範等によって、データの廃棄について、ハードディスク等の物理的な破壊や暗号化消去等の特定の方法を求めるのか、一般的な方法を許容するのか等、廃棄への要求水準は異なると考えられるため、個々の事情に応じて要求される適切な廃棄方法を実施することが重要である。

データを利活用する所在地によっても設定される「場」は変わり得る。その際、現にデータが所在している国の法令のみならず、該当する場合は域外適用規定を有する他国の法令も含めて「場」として特定する必要がある点に留意が必要である。さらには、データの取扱に関して、特定のコミュニティにおいて暗黙のうちに共有されている共通認識（必ずしも明文化されていないものも含む）や、デジタルプラットフォーム等の利用規約も、「場」として機能していると言える。このように、「場」は、それぞれの状況や関係する者の事情などによって適用される形態等が異なることになり、一律に設定方法や形態が決まるものではない。そうした「場」に関するより具体的な検討は、今後の議論や事例の蓄積を通じて、精緻化されることが想定される。

対象となるデータ利活用プロセスに係るデータ保有者のようなステークホルダーが「場」の設定を行うにあたって、例えば、「場」を構成する重要な要素の一つに法令等があるが、必要な観点を漏らすリスクを低減しながら検討するためには、例えば下記のような4つのカテゴリから整理することで適切な設定につながると考えられる。4つのカテゴリは、「場」が、データに関して何らかの共通の取扱を求める法令等と連動して設定されることを背景に、データに共通の取扱を求める目的としてはどのようなものが考えられるか、という観点から整理している。なお、4つのカテゴリは一つの例であり、フレームワークを適用する対象が位置する文脈や重視する観点等により重複や漏れが生じる場合も想定されることから、必ずしも完全なものではない。

その際、「場」の要求に応じて設定される「属性」の例も併せて記載するので、「場」や「属性」の洗い出しに活用されたい。

- パーソナルデータの保護
  - ・「場」の例：個人情報保護法（日本）、GDPR（欧州関係）、個人情報を取得する際に当該個人が同意した利用目的
  - ・規定される「属性」の例：カテゴリ（個人情報、匿名加工情報）、データ権利者、データ管理主体
- 知的財産（営業秘密を含む）保護
  - ・「場」の例：不正競争防止法、著作権法、主体間の契約（NDA等）
  - ・規定される「属性」の例：カテゴリ（営業秘密、限定提供データ）、開示範囲、データ権利者
- 機微技術管理
  - ・「場」の例：外為法、米国輸出管理規則
  - ・規定される「属性」の例：カテゴリ（輸出管理等対象技術）、開示範囲、データ管理主体
- 適切な社会機能の維持
  - ・「場」の例：金融商品取引法（インサイダー取引）、各種守秘義務関係

・規定される「属性」の例：開示範囲

また、関連規定等の分類方法には、上記で示したものとは別の観点からまとめたものとして、以下の分類[7]がある。

- 情報を管理する事業者に管理責任を課す類型：情報を管理する者に対して当該情報に対する管理責任を負わせる類型の法制度であり、個人情報保護法における個人情報取扱事業者の義務等を含む。
- 不正行為者に法的責任を問う類型：不正行為者に対して法的責任を問う類型の法制度であり、不正競争防止法における営業秘密保護規定等を含む。

2-2-3 モデル化（「属性」）

「属性」は、対象データの法的なカテゴリや開示範囲、取得元から許容された利用目的等のデータが有する性質を示すものである。組織は、当該データの「属性」の整理を通じて、関連する利用上の制約を特定し、セキュリティを確保するために必要な措置を講ずることによってデータの適切な取扱を実現することが可能になる。かかるデータの「属性」の項目を網羅的に示すことは困難だが、代表的な「属性」やパラメータ、「属性」の整理のポイントを下記に示す。

なお、前述のとおり、「属性」は「場」の要求によってその内容が決められる部分が存在し、2-2-2においても「場」によって規定される「属性」の例を挙げている。整理した「場」に関して、データに対する要求を検討し、関連する「属性」を適切に具体化することが重要である。

- カテゴリ

  特に「場」と連動して、データに対して特別な作用（「イベント」）を求める場合（個人情報・匿名加工情報、営業秘密・限定提供データなど）、カテゴリとして法令等における位置づけを整理する。

- 開示範囲

  民法上の契約や組織内規則も含め、データに定められている開示範囲を整理する。その際、組織内での取扱であっても、国・地域間での移転が伴う場合や、米国輸出管理法上のみなし輸出に該当する場合等、開示範囲の制限が複層的に適用される可能性がある点に留意する。

- 利用目的

  個人情報やライセンスなど、法令等に基づいて利用目的に制限が設けられている場

[7] 経済産業省「情報セキュリティ関連法令の要求事項集」（2011 年 4 月）

合、データが主体間を転々として付加価値を生み出していく過程全体を通じて、当該利用目的の範囲内で取扱われる必要があることから、「属性」として明示しておく必要がある。

- データ管理主体

サプライチェーンが動的に構成される中、データに対して様々なプレーヤが関与することとなるが、法令上あるいは契約上、データフローのある時点において、データの管理に責任を負うべき主体が特定される。当該主体は、実際にサイバーセキュリティ対策を講じる際に、重要な推進主体となる。データを軸に置く本フレームワークにおいては、データが転々流通する過程で管理主体も移り変わるものであり、データが有する「属性」の一つとして取扱う。なお、クラウドサービス等を利用する場合や、データの処理を外部委託等する場合等、管理主体が曖昧になるケースがあるため、データ管理主体を特定し、その変化を適切に捉えることは重要である。

- データ権利者

データ管理主体とは別に、データに対して権利を有する主体が存在することがある。バリュークリエイションプロセスの中で、移転・提供が行われて別の主体がデータを取得した場合でも、データ権利者（例：個人情報ならばデータ主体となる本人、事業上有用なデータならば権利元の組織）は当該主体の管理下にあるデータに対して引き続き権利を有すると考えられる。例えば、個人情報保護法上の同意の取り下げや、著作権法等のライセンスに関する規定上の取扱、企業の競争力に関わるデータ（例：製品の設計データ、製造拠点における機器・設備の稼働状況）を提供している場合等は、管理主体が転々と移っていく過程でも、「属性」として管理する必要がある。

- 価値（重要度）

対象データの事業上の価値(重要度)を特定する。組織は、特定された価値の大きさに応じて、現に対象データを取扱うシステムや組織に対して適切なリスク対応策を採用することが望ましい。価値の算定にあたっては、データのカテゴリや業種等に応じて様々な方法を適用することが可能だが、一例として、機密性、完全性、可用性の観点からデータ侵害によって生じうる事業への影響の度合いを評価し、そのうち最大のものを評価値とするものがある。

- 媒体・保存先

一般に、電子化されたデータは複製等が容易であるが、データのカテゴリや適用されるポリシーの内容等によっては、データを保管、加工・分析等するために利用している媒

体やサービスを特定し、求められるセキュリティ水準を維持できるようにデータの所在を継続的に管理することが必要な場合がある。主な媒体・保存先の種別としては、可搬電子媒体、PC、モバイル端末、社内サーバ、社外サーバ(例:クラウドサービス)等がある。

- 利用期限

  法律や別途締結される契約、関連するポリシー等でデータの利用期限や利用完了後の遅滞ない廃棄、提供元への返還等が定められる場合、当該データ利用の開始日と終了日を特定し、利用期限を過ぎてもデータが利用可能なままとなっていないか等を管理することが必要となる。

3. 活用方法

3-1 サプライチェーンを構成するステークホルダー間での活用

本フレームワークの目的で述べたように、本フレームワークを活用することで、データを軸に置き、データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し、そのセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することが可能になる。

バリュークリエイションプロセスに関わるステークホルダーの間で、複数の主体の協同的活動によって必要なセキュリティ対策を検討するにあたっては、データのライフサイクルの各工程において直面するリスクに関する認識を共有することが必要である。本フレームワークを活用してリスクを可視化した上で、各主体がそれぞれ実施すべき対策を他の主体と協議しながら取り組むことによって、データの信頼性を確保することが期待される。

また、既に述べているように、データは基本的に中立性を有しており、バリュークリエイションプロセスにおけるデータとデータに関与する主体は切り離して考えるべきで、例えば流通しているデータの誤用や悪用はデータ自体の問題ではなく、それを行った主体の問題として理解することができる。したがって、バリュークリエイションプロセスに参加する各主体は、関係するステークホルダーの間で互いにデータ流通に係る条件を提示した上で契約等を締結、履行することで、本フレームワークで示す協同的活動における責任を果たすことができる。その上で、各主体において当該契約等が履行されているかは、監査等の方法で確認され得ることから、将来的には、経営者によるITガバナンス(デジタルガバナンス)の検討にも本フレームワークが活用されることが期待できる。

なお、本フレームワークにおいては、主体間を転々流通するデータに関するリスクの洗い出しに関する考え方を整理している。可視化されたリスクに対して、各主体が実施すべきセキュリ

ティ対策は、これまでに公表されてきた情報セキュリティに関する様々な国際標準等において既にまとめられている。具体的な措置内容の選択にあたっては、既存の規格等を参照いただきたい。主な規格は次のとおり。

＜リスクマネジメントの全体プロセスを示すもの（例）＞

- ISO 31000:2019
- ISO/IEC 27001:2013
- NIST SP 800-30 Rev.1

＜全般的にセキュリティ対策要件等を示すもの（例）＞

- データマネジメント知識体系ガイド（DMBOK） 第2版
- ISO/IEC 27001:2013 附属書A, ISO/IEC 27002:2013
- NIST SP 800-53 Rev.5
- CPSF

＜各イベントのセキュリティ対策等の詳細を示すもの（例）＞

- 生成・取得：安全なウェブサイトの作り方　改訂第7版（生成・取得の手段としてウェブサイトを用いる場合）、NISTIR 8259（生成・取得の手段としてIoT機器を用いる場合）
- 移転・提供：ISO/IEC 27033-1:2015, NIST SP 800-47 Rev. 1
- 加工・利用：AI・データの利用に関する契約ガイドライン 1.1版
- 廃棄：NIST SP 800-88 Rev.1

3-2 ルール間のギャップの分析

本フレームワークの目的のところで述べてきたように、本フレームワークは、データ管理に関わる制度間における、データのセキュリティの確保のために要求されている条件や措置の相違（ギャップ）を明確化するためのモデルとしての活用も可能である。

例えば、欧州からの個人情報の移転に関して、GDPRに関するSchrems Ⅱ判決でプライバシーシールドが無効と判断された米国と、十分性認定を受けている我が国の差異について下記のように整理することが可能と考えられる。ここでは、状況を単純化するため、同一事業者の国外拠点への移転を想定し、事前に設定された利用目的の範囲内での移転であることとする。

欧州から日本への移転については、移転という「イベント」によって、「場」が欧州のGDPR等の法制度から、日本の個人情報保護法制の下に移る。その際、日本は十分性認定を取得していることから、欧州GDPRで求められているデータ保護が、日本の個人情報保護法制の下でも実質的に確保されていると考えられる。データの「属性」に関しては、データ管理主体に日本拠

点が加わるのみであるが、関連する処理[8]に際して、GDPRの規定する個人データの適法な処理の要件が満たされていることを前提とすると、十分性認定により、データ管理主体の変化に関しては事前に認められ、許容されていると言える。

一方、欧州から米国への移転をGDPR等に定めのある適法な手段に基づいて行おうとする場合、データが米国に所在する状況では、「場」が米国の各種法制度に基づいたものに変化している。例えば、米国の法制度の下では、安全保障などを目的とした米国政府機関による監視の対象となる場合があることから、移転という「イベント」を経てデータの物理的な所在地が米国となることを通じて、データ「属性」に関して、データ管理主体の変化の他に、潜在的な開示範囲に米国政府が加わる形で「属性」が変化していると考えられる。このような状況も反映し、現状では、欧州から米国への個人データの越境移転を、欧州委員会が認めた標準的契約条項（SCC）の締結に基づいて実施することが求められている[9]。そのため、十分性認定に基づきかかる移転を行う日本と米国との間には、欧州からの個人データの越境移転に関するルール間のギャップが存在すると言える。

このように、データに関する「場」の変化や「属性」の変化を可視化することで、データのセキュリティの確保のために要求されている条件や措置の相違を把握することにつながる。

[8] ここでの「処理」とは、GDPR における定義にならい、「自動的な手段であるか否かに関わらず、個人データ、または個人データの集合に対して行われる、あらゆる単一の作業、または一連の作業」を意味するものとする。
[9] なお、欧州から米国への移転・提供にあたって、SCC を利用する場合であっても、米国政府への開示に関する対応について、特に留意して実施する必要がある。

添付A.　ユースケース

A-1. POSデータの分析

直接的な消費者との接点を有する小売・流通業は、従来から他産業に比べ多様かつ大量のデータを保有し、顧客へのサービスの向上や効率化のため、販売・仕入れ等に付随して発生するデータの活用に取り組んできた。特に小売業が持つPOSデータ・ID-POSデータの活用が進んでいる。

また、実店舗と EC 等の融合を目指す「オムニチャネル」の取組も、各事業者にて環境整備が進められており、スマートフォンやソーシャルメディア（SNS）が普及したことで、消費者が様々な販売チャネルを活用して、新たな購買体験を経験することが可能になっている[10]。事業者は、それら複数のチャネルから収集されるデータをチャネルや部門ごとにばらばらに蓄積、活用するのではなく、統合的に活用することで、より効果的に取組を進めることができるとされている。

上記の背景を踏まえ、小売・流通業に係る本フレームワークのユースケースとして以下の流れによるデータの利活用プロセス（A-1内において、以下、「本ユースケース」という。）を取り上げる。

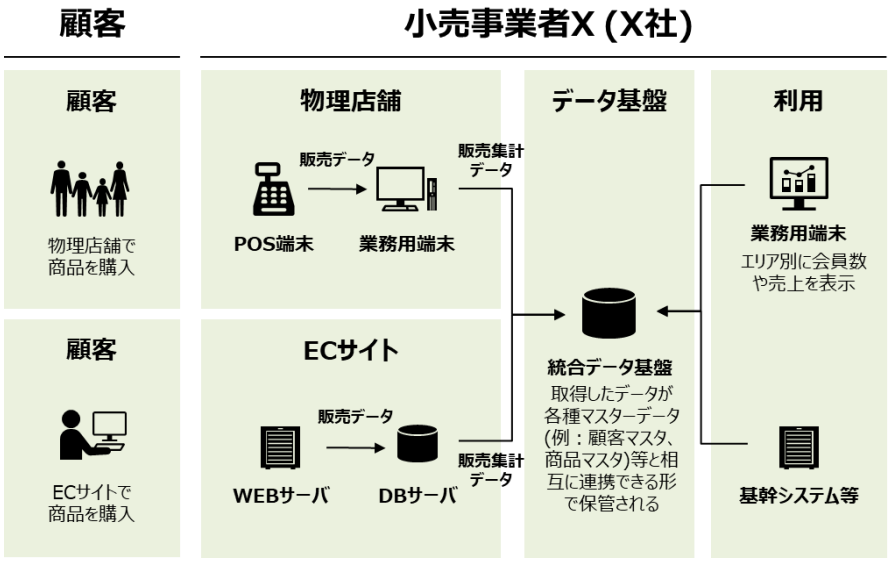
- 小売事業者X（X社）は、従来から国内各地に店舗を構える小売事業者で、現在は物理店舗とECサイトという複数のチャネルで商品を販売しており、会員証等を活用しながら購入者のID[11]と購入物等を紐づけられる形で販売データを収集している。
- 個々のチャネルから得られたデータは他のデータと相互に連携できる形で個別に保管され、別途作成される各種マスターデータ（例：顧客マスタ[12]、商品マスタ）等も参照しながら、マーケティング用途等のニーズに応じて統合される。
- 統合されたデータは多種多様な用途で活用され得るが、ここでは事業者X自身がチラシ配布や広告表示等の広報の最適化を図るため、地図ソフトと連携してエリア別に会員数や売上を表示する事例を取扱う。

---

[10] 経済産業省 商務流通保安グループ「流通・物流分野における情報の利活用等に関する研究会　調査報告書」（2016 年 2 月）

[11] 本ユースケースでは、物理店舗と EC サイトで共通の会員 ID が利用されていると仮定する。

[12] X 社の顧客マスターデータを、本稿では「会員情報」（会員の氏名、性別、住所、連絡先等の情報を内容として含む）と呼称する。



697 図A−1.1 対象プロセスの概要

698 小売・流通業におけるサプライチェーンには、図A−1.2に示すように、製造、中間流通、販売[13]
699 等の段階があり、SPA（製造小売業）等の例外を除いて、それぞれ別の事業者がビジネスを
700 行っている。小売・流通業におけるデータ利活用としては、取扱い製品の製造段階や中間流通
701 段階を対象にしたものも想定されるが、本ユースケースにおいては、特に小売段階における販
702 売データ等のマーケティング活動等への利用を扱うこととする。

703 図A−1.2 小売・流通業のサプライチェーンにおける対象プロセスの位置づけ

704 X社が図A−1.1に示すようなデータ利活用の仕組みを今後整備しようとする際、又は既に整
705 備した仕組みを見直そうとする際に、関係部門（例：物理店舗部門、EC事業部門、情報システ
706 ム部門）で連携しつつ全体として一貫性のあるセキュリティ対策等を実装するために、本フレー
707 ムワークは活用され得る。その際、本ユースケースにおいて考慮すべきステークホルダーとし
708 て以下が挙げられる。

[13] 経済産業省 商務流通保安グループ「流通・物流分野における情報の利活用等に関する研究会　調査報告書」（2016 年 2 月）「5) 製・配・販連携によるサプライチェーンの高度化」等を参照

- 顧客：X社が運営する店舗から商品を購入する
  - 物理店舗を利用する顧客
  - ECサイトを利用する顧客
- X社：顧客が利用する店舗を管理・運営する
  - 物理店舗の管理・運用に係る部門
  - ECサイトの管理・運用に係る部門（EC事業部門）
  - 情報システム部門
  - マーケティング部門
- ITサービス事業者：X社からの委託を受けシステムの開発、運用等を行う

A-1-1. STEP 1 データ処理フロー（「イベント」）の可視化

> ***本文の記載***
>
> ・ *まず、データの生成・取得から廃棄に至るまで、想定されるデータ利活用プロセスにおける大まかなデータフロー及び「イベント」を可視化する。*
>
> ・ *その際、「イベント」をどの程度詳細に記述するかは、データフロー整理の目的に応じて調整する必要がある。例えば、企業内ネットワークでのサーバ・クライアント間のデータの移転という「イベント」は、複数のステークホルダー間で転々流通するデータを扱う際の対策等を検討するには、検討の本質とは異なる場合があることから省略し、データの取扱に係るマネジメントのルールを提示し、それに従って取扱っていることを示すことで代替することも考えられる。*

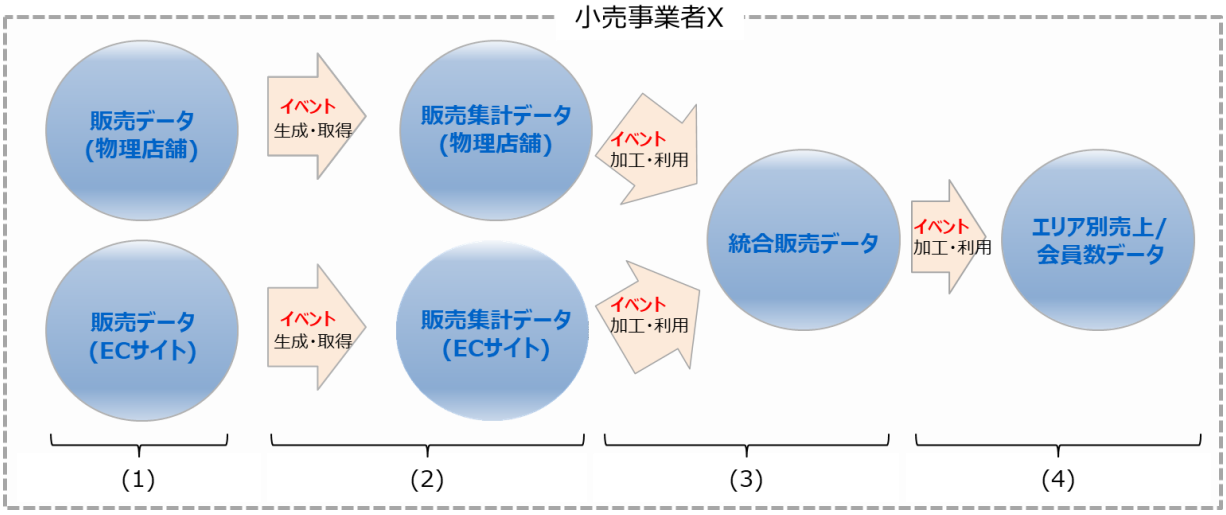
STEP 1は、生成・取得から廃棄に至るまでの一連のデータのライフサイクルにおいて、データがどのようなプロセスで利活用されるのかを理解する段階である。本ユースケースでは図A-1.1で示すように、以下のプロセスにより構成される。

(1) 物理店舗とECサイトという各販売チャネルにおいて顧客による購買が行われる都度、個別の「販売データ」が「生成・取得」される。「販売データ」には、販売の日時や店舗、購入された商品とその価格、個数等が含まれる。

(2) 「販売データ」は各店舗又はサイト等の単位で「販売集計データ」として蓄積される。

(3) 各店舗やサイト等で保管された「販売集計データ」は、X社の統合データ基盤に集約された後、複数の販売チャネルを連携させたマーケティング分析等の基盤となるよう、「統合販売データ」に「加工・利用」される。

(4)「統合販売データ」は、チラシ配布等の広報の最適化を図るため、地図ソフトと連携して「エリア別売上/会員数データ」に「加工・利用」される。



図A-1.3 データ処理フローの可視化(POSデータの分析)

なお、図A-1.2では割愛しているが、(1)から(4)という4つの段階からなる上記プロセスにおいて、各種データの適時かつ適法な利用に資するよう、「販売集計データ」、「統合販売データ」、「エリア別売上/会員数データ」は業務用端末や各種DBに中長期的に保管され、あらかじめ設定した利用期限の終了とともに適切な手法を通じてレコード単位で削除、又はデータセット単位で廃棄される。データの保管や廃棄に係る要件はSTEP 3にてデータの管理に資する「属性」を特定する際の重要なインプットとなるため、可能であればSTEP 2やSTEP 3において特定しておくことが望ましい。

また、図A-1.2に示すプロセスとは別途、X社はECサイト上の会員登録画面や物理店舗に設置された申込用紙への記入等を通じて顧客から会員情報を「生成・取得」しており、共通する会員IDに基づいて当該情報と各種販売データを突合することで、個人情報としての「統合販売データ」等へと「加工・利用」している。この際、申込用紙等を通じて各物理店舗にて取得された会員情報は、個人情報保護の観点から各店舗や各地域の支社では保管されず、本社情報システム部門が管理する統合データ基盤にて集中的に管理されるという運用を想定する。

「生成・取得」や「加工・利用」等の「イベント」をどの程度詳細に記述するかは、データフロー整理の目的に応じて調整されるが、ここでは、データの管理水準や対策の内容に少なからず影響するデータの「属性」である事業上の重要度やカテゴリ(例:個人情報の該当性)を変化させる

ものや、「信頼境界」[14]を構成すると考えられるものを抽出した。

A-1-2. STEP 2 必要な制度的な保護措置(「場」)の整理

本文の記載

- *データ保護に資する「場」を検討し、法律・契約の観点から適切なものを設定する。その際、一つのデータに対して複数の「場」が重なり合う、つまり、データに対して様々な観点からの要求がなされることが考えられる。*

STEP 2は、STEP 1で特定された一連のデータ利活用プロセスに対して、「場」としてどのようなデータの保護に係るルール(規範)が課せられ得るかを理解する段階である。本ユースケースにおいて、取扱うデータの性質や事業者の業種等を考慮すると、例えば下記のルールが「場」として特定され得る。

(1) 割賦販売法/PCI DSS[15]:物理店舗やECサイトでの決済にクレジットカードを用いる場合、割賦販売法第35条の16により加盟店たるX社は、クレジットカード番号等に該当する「販売データ」等の適切な管理や自らの委託先に情報管理に係る指導等を行うことが義務付けられている。実務上の指針とされる「クレジットカード・セキュリティガイドライン」では、具体的な管理として、カード情報を保持しない非保持化又はカード情報を保持する場合はPCI DSS準拠のいずれかの対応が必要とされる。

(2) 個人情報保護法:各種チャネルにおける「販売データ」等は会員IDにより個々の顧客を識別しており、それ単体では特定の個人を識別できるものではないが、統合データ基盤等において別途会員情報と突合等されることで個人データに「加工・利用」される。X社内部の情報管理規則において各物理店舗等において個人データを取扱わないこととしている場合、会員情報を扱う統合データ基盤等に対して物理店舗の担当者その他の関係者からのアクセスができないようにする等して、「販売データ」等を他の情報と容易に照合できないようにする必要がある。なお、X社が個人データ(例:「販売集計データ(ECサイト)」、「統合販売データ」)を管理する場合、利用目的の明確化・利用目的による制限、安全管理措置、第三者提供時の手続等の個人情報保護法において個人情報取扱事業者の義務として定められる各種の規律を遵守する必要がある。

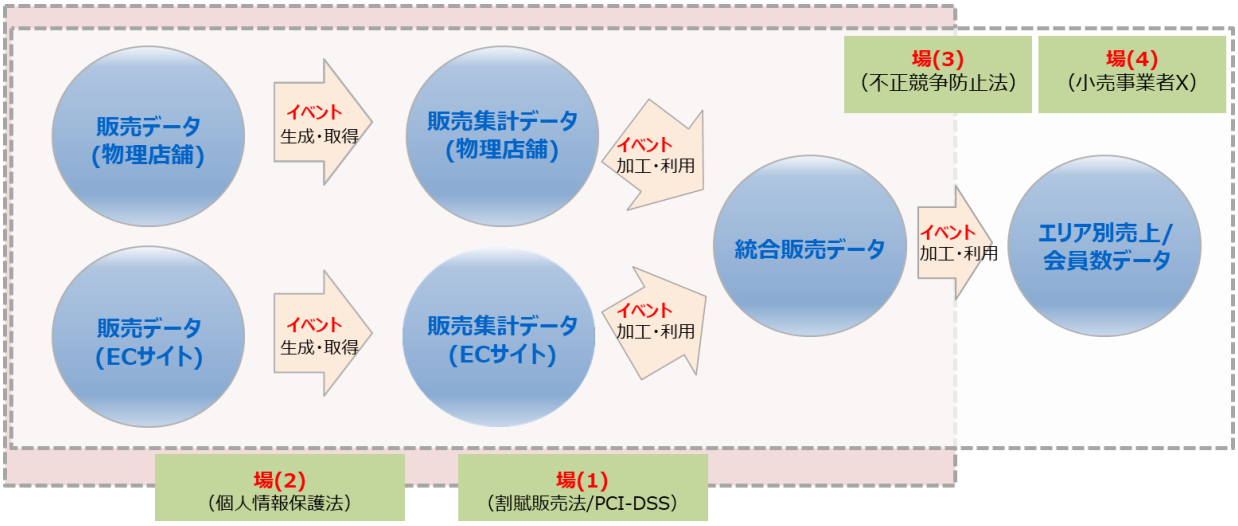
---

[14] 脅威分析の一環で作成されるデータフロー・ダイアグラム(DFD)において特定される、管理している組織やインターフェイスが変わる場所に引く境界線のことを指す。

[15] 加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取扱う事を目的として策定されたセキュリティ基準 "Payment Card Industry Data Security Standard" を指す。

（3）不正競争防止法：X社が収集し、保管する「販売集計データ」や「統合販売データ」等は通常、事業上の価値が高い情報であって、「営業秘密」として不正な取得、使用、開示から法的な保護を受けられるよう管理することが一般的と考えられる。

（4）X社内部の情報管理規則（物理店舗やECサイトの運営にあたり、必ずしも明文化していないが担当部署等において共有されているものも含む）



図A-1.4 必要な制度的な保護措置の整理（POSデータの分析）

A-1-3. STEP 3 「属性」の具体化

- *設定されたデータや「イベント」、「場」に基づいて、管理上あるべき「属性」を特定する。*
- *場合によっては、データの「属性」を整理していく中で、本データが取扱われるべき「場」や実施されるべき「イベント」に漏れがあった場合、適宜追加等を実施する。*

STEP 3は、STEP 2にて特定されたデータの保護に係るルール（場）の効果的・効率的な遵守に資するデータの「属性」を特定する段階である。内容を特定すべき「属性」項目のうち主なものは本文2-2-3に示したとおりだが、STEP 2で特定される「場」と強く関連したものが多く含まれる。各「属性」項目のパラメータを設定するにあたり考慮することが望ましいルールは以下のとおりと考えられる。

799 表A.1-1「属性」の検討において考慮すべきルール（場）

		割賦販売法等	個人情報保護法	不正競争防止法	X 社内部情報管理規則
カテゴリ	パーソナルデータ保護	○	○		
	知的財産（営業秘密を含む）保護			○	
	…	…	…	…	…
開示範囲		○	○	○	○
利用目的			○		
データ管理主体		○	○		○
データ権利者		○	○		
価値（重要度）		○	○	○	○
媒体・保存先			○		○
利用期限		○	○		○

800 本ユースケースにて取扱われるデータの多くは個人データに該当するため、「利用目的」や
801 「利用期限」、「開示範囲」の適切な設定と遵守状況のモニタリング等は特に重要になる。「利用
802 目的」や「利用期限」は会員規約等における規定を参照して具体化しつつ、「開示範囲」はNeed
803 to knowの原則[16]やNeed to useの原則[17]に従い、営業秘密管理上の「秘密管理性」を満たすた
804 めにも社内でも関係者のみに限定することが望ましい。上記の事項を考慮して具体化した本
805 ユースケースで取扱うデータがとり得るパラメータの例を以下に示す。

[16] それぞれの職務を実施するために必要な情報へのアクセスだけが認められるべきという考え方
[17] それぞれの職務、業務を実施するために必要な IT 機器、アプリケーション、手順、部屋等へのアクセスだけが認められるべきという考え方

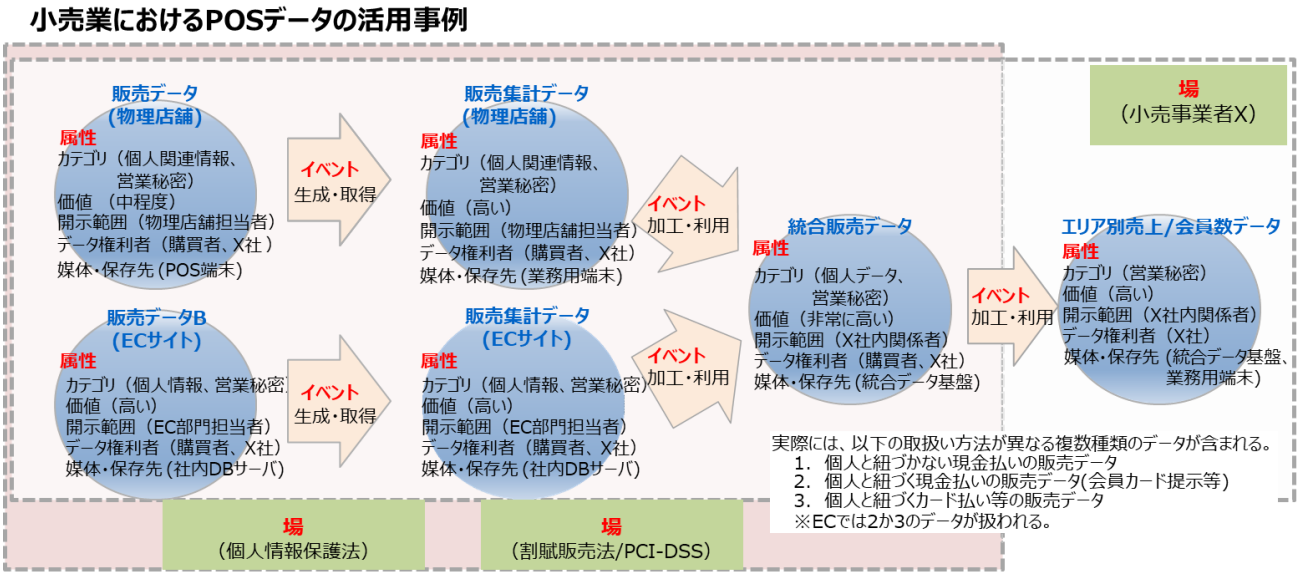
806 表A-1.2 本ユースケースにて取扱うデータの「属性」パラメータ例

		販売データ（物理店舗）	販売集計データ（物理店舗）	統合販売データ	エリア別売上/会員数データ
カテゴリ	パーソナルデータ保護	個人関連情報 等	個人関連情報 等	個人データ	統計情報（非個人情報）
	知的財産（営業秘密を含む）保護	営業秘密	営業秘密	営業秘密	営業秘密
	…	…	…	…	…
開示範囲		X 社内[18]	X 社内	X 社内	X 社内
利用目的		• 売買契約の履行 • 各種アフターサービスの実施 • 商品企画、開発	左記と同様	左記と同様	広報活動の効率化
データ管理主体		各物理店舗	各物理店舗	情報システム部門	情報システム部門、マーケティング部門
データ権利者		購買者、X 社	購買者、X 社	購買者、X 社	X 社
価値（重要度）		中程度	高い	非常に高い	高い
媒体・保存先		POS 端末（店舗に所在）	業務用端末（店舗に所在）	社内サーバ（統合データ基盤）	社内サーバ、業務用端末
利用期限		会員契約終了から 5 年	（各レコード単位で）会員契約終了から 5 年	左記と同様	特になし

[18] 本ユースケースでは X 社内で複数の部門が利活用に関与するが、当該部門間での責任分界を明確にするため、実際の資産管理にあたっては部門や役割等のより詳細な単位で開示範囲の記載を行うことが望ましい。

「カテゴリ」としては、「場」として設定されている複数のルールに対応して、取扱うデータが個人情報保護法における「個人関連情報[19]」、「個人データ」又は「非個人情報」、不正競争防止法における「営業秘密」として管理すべきデータに該当すると特定できる。その際、個人情報保護や営業秘密保護等の異なる体系による複数の類型が同一のデータに適用され得る点について留意する必要があるが、この中でも特に、個人情報保護法における位置づけが利活用プロセスの中で変化しており、データごとに異なる管理が必要となっている点を確実に認識する必要がある[20]。

上記では表形式でデータとその属性の一覧を提示したが、データ利活用プロセスの全体におけるデータの属性の変化とイベントとの関係をより俯瞰的に示すために、図A-1.4のように、STEP 2までに作成している図に属性を記入する方法も効果的と考えられる。



図A-1.5「属性」の提示方法の例

A-1-4. STEP 4「イベント」ごとのリスクポイントの洗い出し

- *設定された「場」という観点から、「イベント」ごとに想定されるリスクを抽出し、設定した「属性」をレビューする。*

[19] 生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないものをいう。（個人情報保護法第 26 条の 2（第 1 項））Cookie 等の端末識別子を通じて収集された、ある個人のウェブサイトの閲覧履歴や、ある個人の商品購買履歴・サービス利用履歴が事例として挙げられる。

[20] 例えば、POS 端末にて生成された段階では個々の「販売データ」は必ずしも特定の個人を識別可能な情報とは言えないが、店舗内の業務用端末に格納される「販売集計データ」は、同端末にて管理される会員情報と照合することで容易に特定の個人を識別し得るデータとなる。

・ *その際、機密性・完全性・可用性といったサイバーセキュリティに係る観点のほか、各法制度等に係るコンプライアンスの観点でのリスクについても洗い出す必要がある。*

A-1-4-1. 「イベント」ごとのリスクポイントの洗い出し

STEP 4は、STEP 3までに理解したデータ利活用プロセスにおいて、セキュリティ及び関連する法制度等の観点からいかなるリスクが想定されるかを特定する段階である。セキュリティの保護に係る観点（機密性、完全性、可用性）及び関連する法制度等の観点（パーソナルデータ保護、知的財産（営業秘密を含む）保護）から、例として、本ユースケースのうち、図A.1-5に示す「販売集計データ（ECサイト）」の「生成・取得」及び付随する「保管」のプロセスに関して以下のようなリスクを想定することができる[21]。下記と同様の検討は、全体プロセスにおける他のデータやイベントに対しても同様の方法でなされる。

表A.1-2 「販売集計データ（ECサイト）」の「生成・取得」及び「保管」にて想定されるリスクの例

大分類	中分類	「販売集計データ」の「生成・取得」及び「保管」にて想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 販売集計データが保管された社内 DB サーバが悪意ある第三者により不正アクセスされ、同データが漏えいする。 ● 社内サーバに保管された販売集計データが、正規の従業員により故意に持ち出される。
	完全性	● 正規ユーザーへのなりすましにより、不正な商品取引が実施される。 ● 社内サーバに保管された販売集計データが、正規の従業員により故意に改ざんされる。
	可用性	● サービス妨害攻撃等により EC サイトにおける取引が一時的に停止する。 ● 販売集計データが保管された社内サーバがマルウェアに感染し、同データが暗号化される等して利用できない。 ● EC サイト運用に係る設備や機器に不具合が生じ、取引が一時的に停止する。 ● 地震や津波等の自然災害により EC サイト運用に係る設備や機器に被害が生じ、取引が一時的に停止する。

[21] 考慮すべきリスク（脅威）を網羅的に抽出する際に適用できる既存の枠組み等については、添付 B を参照されたい。

大分類	中分類	「販売集計データ」の「生成・取得」及び「保管」にて想定されるリスク（例）
関連する法制度等に係る観点	パーソナルデータ保護	● 規約等において生成・取得する販売データの利用目的が明確に示されていない、又は利用の実態と対応していない。 ● 販売集計データを取扱う従業員を適切に監督していない。
	知的財産（営業秘密を含む）保護	● 販売集計データが悪意のある第三者により不正な手段で取得され、開示、使用される。
	…	…

なお、リスクを特定した後で、かかるリスクの低減に資する「属性」項目を再度レビューし、必要に応じてSTEP 3の成果に追加等することができる。

A-1-4-2. 今後のデータ管理の高度化に向けた課題の検討

STEP 1からSTEP 4に至るまでのフレームワーク適用プロセスを通じて、X社は自社のデータ利活用の具体的な姿やその中に潜むリスクを適切に理解し、継続的にリスク管理を改善するための基礎を強化することができる。具体的に示唆される改善の内容は、X社による現状のデータ管理の実態に応じて多岐にわたると考えられるが、例えば以下が含まれる可能性がある。

- 各物理店舗等におけるデータ取扱いに対するガバナンス強化
  国内に多数存在する各物理店舗においては「販売データ」や「販売集計データ」といった個人に関連する情報を取扱うものの、統合データ基盤やECサイト等とは異なり、一律の高度なデータ保護水準を確保することが難しい場合も想定される。本ユースケースでは、そうした懸念に対応するため、各物理店舗では別途収集される会員情報との照合をせず、各店舗では個人データの取扱いをしないこととしているが、かかる管理をより確実なものとすべく、各物理店舗の個人利用に関するニーズを確認したうえで、統合データ基盤で管理される会員情報に対する各物理店舗等によるアクセス状況のレビュー、アクセス制御ポリシーその他の運用規定のレビュー等を行うことが具体的な施策として検討され得る。

- マーケティング部門等におけるデータ利用の実態を踏まえた保護施策の検討
  図A-1.2に示されている利用形態に限らず、統合データ基盤にて管理される「統合販売

データ」等の利用実態や自社の個人情報保護方針や会員規約等の記載事項（例：利用目的に関する条項）との対応状況を確認し、当初提示していた利用目的との乖離が存在する、あるいは将来的に予想される場合に、例えば以下のような施策を検討することが可能と考えられる。

- 個人情報保護方針や会員規約等における関係規定（例：利用目的に関する条項）の改定、顧客への通知、その他の必要な手続きの実施
- 「統合販売データ」等の仮名加工情報、匿名加工情報への加工及び利用

A-2. 高齢者生活支援事業の提供

昨今、消費者向け製品のIoT化に伴い、家電やウェアラブル、センサー等の多様な機器で生活情報を収集できるようになっており、「子育て世代、高齢者、単身者など、様々なライフスタイル／ニーズにあったサービスをIoTにより実現する新しい暮らし[22]」と定義されるスマートホームが急速に普及していくと見込まれている。

かかるスマートホームの実現に向けた具体的な取組の例として、宅内や施設内から収集したデータを活用した高齢者生活支援サービスの提供が挙げられる。高齢者向けの生活支援に関しては、かねてより住まい・医療・介護・予防・生活支援が一体的に提供される「地域包括ケアシステム」の実現が標榜されてきたが、在宅高齢者の生活実態や健康状態を正確に把握するデータが不足していることもあり、高齢者を支えるサービスが質・量ともに不足している点が課題だと認識されてきた。

上記の背景を踏まえ、スマートホーム分野に係る本フレームワークのユースケースとして、複数の事業者が保有するデータを活用した高齢者生活支援事業（A-2内において、以下、「本ユースケース」という。）を取り上げる[23]。

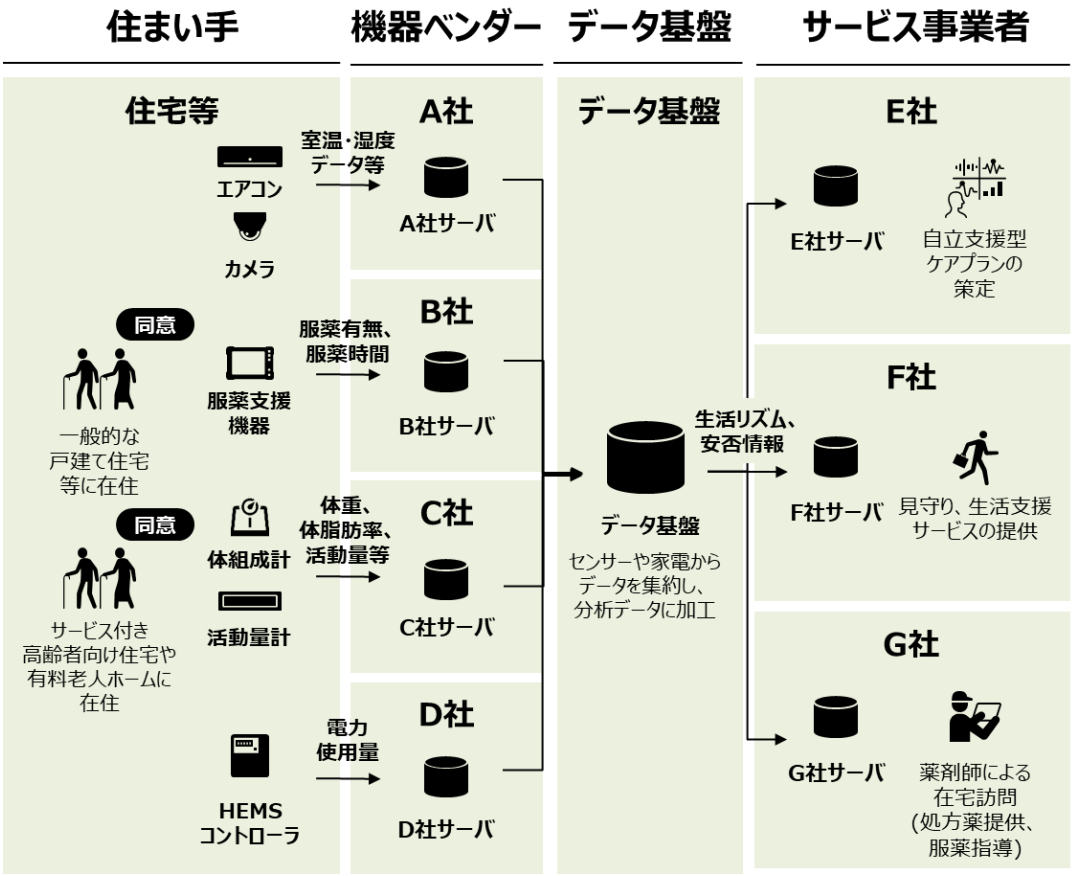
- 一般的な戸建て住宅や有料老人ホーム等に設置される多数の機器群を通じて、高齢者の生活や健康の状況に関するデータが生成され、各機器ベンダー（A社～D社）の運用するサーバに蓄積される。
- 各機器ベンダーは、一定の収益を得る代わりに、第三者（プラットフォーム事業者）の運用するデータ基盤に各々が収集したデータを提供する。各機器ベンダーから提供されたデータは特定の個人を特定できない形でデータ基盤上に集約され、高齢者の生活リズム情報や安否情報というより高次なデータへと加工される。
- 高齢者の生活リズム情報や安否情報等のデータは、必要に応じてサービス事業者等に第三者提供され、データ主体の個人と紐づけたうえでより高度な支援サービスの提供等に活用される。サービス事業者等は、見守りサービス等の提供のため、各種機器から取得したデータを特定の住まい手に紐づけて取扱う点や機器から取得したデータの利活用プロセス等についてあらかじめ同意を取得しているものとする。

---

[22]『「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」を策定しました』（https://www.meti.go.jp/press/2021/04/20210401005/20210401005.html）

[23] 本ユースケースに係る詳細については、「2018年度成果報告書　IoT を活用した新産業モデル創出基盤整備事業　研究開発項目⑥IoT 技術を活用したライフデータの高度利用システムの開発　IoT家電・センサーからのライフデータによる高齢者の生活サポートサービス基盤の研究開発」を参照されたい。

- サービスの提供に直接的又は間接的に関わる機器ベンダー（A社～D社）、プラットフォーム事業者、サービス事業者等は、コンソーシアムを組成し、共通して適用される規則の策定や適時の情報共有等を行っている。



図A-2.1 対象プロセスの概要

本ユースケースにおいては、以下に示すとおり非常に多数のステークホルダーが存在しているが、取扱うデータには機微な個人データとなり得るものも含まれることから、コンソーシアム等での協議を実施し、データの利用に係るサプライチェーンの全体で十分な水準のデータ保護措置を講じる必要がある。

- 住まい手：日常生活の中で各種IoT機器・サービス等を利用し、それに伴って生成される自身に関するデータを同意等の適切な手続きを経たうえで事業者に提供する。
  - 一　一般的な戸建て住宅等に在住する高齢者
  - 一　サービス付き高齢者向け住宅や有料老人ホームに在住する高齢者
- 機器ベンダー（A社～D社）：宅内や施設内に設置されている機器を製造・販売し、本人同意等の適切な手続きを経たうえで各々運用中の機器から取得したデータを収集し、管理している。

- A社：エアコンや見守りカメラ等の家庭用IoT機器を製造・販売し、収集したデータを自社サービスで活用するだけでなく、プラットフォーム事業者にも提供する。
- B社：処方薬の服薬有無や服用時間等をセンシングする服薬支援機器を製造・販売し、収集したデータを自社サービスで活用することに加え、プラットフォーム事業者にも提供する。
- C社：体組成計や活動量計等のヘルスケア機器を製造・販売し、収集したデータを自社サービスで活用するだけでなく、プラットフォーム事業者にも提供する。
- D社：スマートメータが実装された家庭向けに電力使用状況を可視化するサービスを提供し、収集したデータをプラットフォーム事業者にも提供する。

● プラットフォーム事業者：、各住宅、施設に設置した機器等からのデータを集約し、適宜加工・分析等を実施する。

● サービス事業者（E社～G社）：プラットフォーム事業者からデータの提供を受け、より高度な高齢者支援サービスの提供等に活用する。

このような組織横断的なデータ利活用の仕組みを整備しようとする際、本フレームワークの活用を通じて、コンソーシアム等の場においてステークホルダー間でデータのライフサイクルの各工程において想定されるリスクに関する認識を共有し、各主体がそれぞれ実施すべき対策について他の主体と協議していく試みをより円滑なものとすることが望まれる。

A-2-1. STEP 1 データ処理フロー（「イベント」）の可視化

本ユースケースにおけるデータ処理フローは図A-2.2で示すように、以下のプロセスにより構成される。

(1) 高齢者の在住する宅内又は施設内に設置された機器類から、同意等の適切な手続きを経たうえで各種データが「生成・取得」され、各機器ベンダー（A社～D社）の管理するサーバへと「移転・提供」された後、「統合データ」として蓄積、保管される。これらのデータは取得時から各機器の識別情報に紐づけられ、当該機器が誰の住宅等に設置されているかは機器ベンダーからはわからないものとする。煩雑となるため図では割愛しているが、以下に示すように、宅内、施設内には複数の事業者が提供する多数の機器が設置されている。利活用上の需要に基づいて設置機器は増減する可能性があるが、住まい手や各機器ベンダー等は機器構成の変更を把握し、適切に管理することが望ましい。

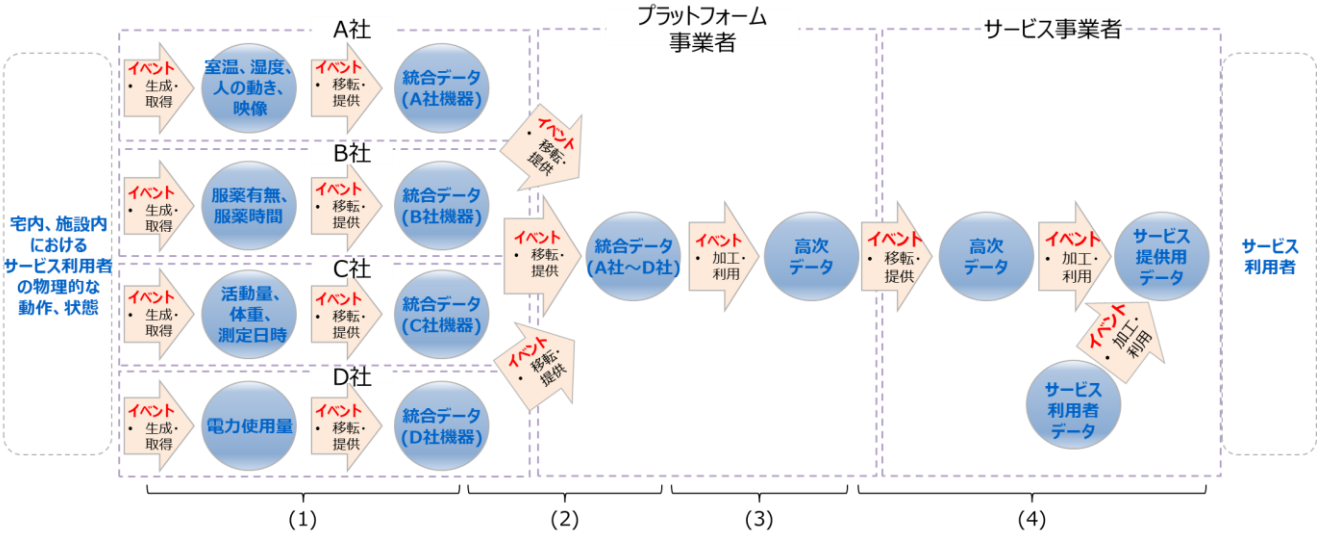
表A-2.1 主な設置機器と収集データ

製造・販売者	名称	収集データ
A社	エアコン	室温・湿度情報
	電波センサーによる見守りシステム	ベッド上の呼吸有無・活動状態（動き）
	コミュニケーションカメラ	室温、人の動き、映像
B社	服薬支援機器	服薬有無、服薬時間
C社	活動量計	活動量、歩数
	体組成計	体重、測定日時
D社	HEMSを用いた電力使用量集約基盤	電力使用量

(2) 各機器ベンダーが保有する「統合データ」は、プラットフォーム事業者が運営するデータ基盤に「移転・提供」され、統合、保管される。統合データは、機器の識別情報に紐づく利用者識別情報に基づき管理されており、当該データから個人を識別することはできないように構成されているものとする。組織横断的なデータ利活用の仕組みを整備するという本検討の趣旨を踏まえ、ここでは、各機器ベンダーが個別に行う自社保有データの活用はフローから省略し、事業者間でのデータ移転・提供により焦点を当てることとする。

(3) 各社から提供を受けデータ基盤に集約された「統合データ」は、サービス提供事業者の利用に適する「高次データ」（例：生活リズム情報、安否情報）に「加工・利用」される。なお、(2)、(3)のプロセスにおいて、取扱うデータと特定の個人への紐づけは行われないものとする。

(4) 「高次データ」は、プラットフォーム事業者から提供先事業者のサービス内容や個別の求め応じて必要な情報を検討したうえで「移転・提供」され、サービス事業者が別途保有しているサービス利用者データと突合され、「サービス提供用データ」に「加工・利用」される。



946 図A-2.2 データ処理フローの可視化（高齢者生活支援事業の提供）

947 A-2-2. STEP 2 必要な制度的な保護措置（「場」）の整理

948 本ユースケースにおいて、取扱うデータが「個人に関連した情報」である点や当該データが
949 複数の事業者に提供され得る点等を考慮すると、例えば下記のルールや各社の必ずしも明文
950 化されていないルール等が「場」として特定され得る。

951 （1）個人情報保護法：本ユースケースで利用されるデータは住まい手（ここでは高齢者）と
952 いう「個人に関する情報」であり、最終的に元の住まい手に対してサービスを提供するた
953 め、サービス事業者にて特定の個人を識別できるように加工されることから、個人情報
954 保護法における「個人データ」又は「個人関連情報」等に該当すると考えられる[24]。「サー
955 ビス提供用データ」が「個人データ」であるため、サービス事業者が個人情報取扱事業
956 者に該当することに加えて、各機器ベンダーにより収集されるデータやプラットフォーム
957 に集約される「統合データ」は、匿名的な利用者識別情報や機器識別情報に基づいて
958 必ずしも特定の個人に紐づかない形で管理されていることを仮定しているため、「個人
959 データ」ではなく「個人関連情報」等に該当すると考えられる。当該データは、提供先の
960 サービス事業者において個人データとして取得されることが容易に想定されるため、各
961 機器ベンダー及びプラットフォーム事業者においては、個人関連情報取扱事業者として
962 本人からの同意取得の確認、提供元における記録等の義務が生じる点に留意が必要

[24] 対象のデータが、個人情報保護法上のいかなる情報の類型に属するかは、改正個人情報保護法の動向も踏まえつつ、適用主体において慎重な検討が必要である。

である。一方で、本ユースケースにおける想定とは異なって、各機器ベンダー又はプラットフォーム事業者が保有する「統合データ」が「個人データ」として管理され、サービス事業者に提供される場合、個人情報保護法第23条第5項に示される事由に基づき、コンソーシアムに参加する事業者間で円滑に当該個人データの提供がなされるよう、例えば以下のような仕組みを導入することも想定される[25]。

- 委託（法第23条第5項第1号関係）
  提供元事業者（機器ベンダーやプラットフォーム事業者）が、利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部をサービス事業者等へ委託することを通じて、当該個人データの提供先を「第三者」に該当しないものとする。
- 共同利用（法第23条第5項第3号関係）
  機器ベンダー、サービス事業者等において共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称を、あらかじめ、本人に通知等することを通じて、当該個人データの提供先を「第三者」に該当しないものとする。

（2）機器利用規約：住まい手と各機器ベンダーとの間で締結される。本ユースケースにて収集されるデータはそれ単体では必ずしも「個人データ」に該当するわけではないが、住まい手からデータの取扱い（例：機器から取得したデータのプラットフォーム事業者への提供）等が規定された規約に対して同意を得ることも想定される。

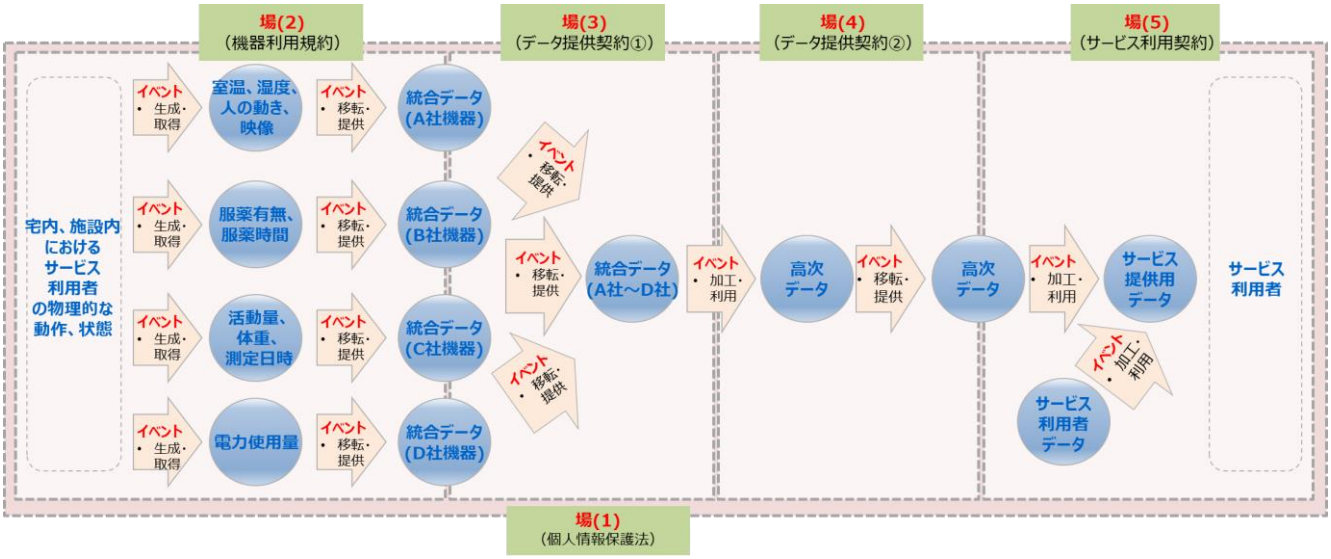
（3）データ提供契約：本ユースケースでは、プラットフォーム事業者を介して各機器ベンダーとサービス事業者とのデータの流通がなされることで高度なサービスを高齢者に提供することが想定されている。データの流通には営業秘密の漏えいやプライバシーの侵害等のリスクが想定されるが、適切な契約上・技術上の措置を採ることによって各々の役割と責任分界を明確にしつつ、リスクの最小化に寄与できるとされている[26]ことから、以下2種類のデータ提供事象について、事業者間及び住まい手も含めた形で様々な条件等を協議し、合意する必要がある。

- 機器ベンダーからプラットフォーム事業者への提供（図A-2.3における場（3））

---

[25] 具体的な規定等については、「個人情報の保護に関する法律についてのガイドライン（通則編）」の「3-4-3 第三者に該当しない場合（法第 23 条第 5 項・第 6 項関係）」等を参照されたい。
[26] 契約にて考慮すべき事項の詳細については、「AI・データの利用に関する 契約ガイドライン 1.1 版」の「第 6 「データ共用型（プラットフォーム型）」契約（プラットフォームを利用したデータの共用）」を参照されたい。

990 ― プラットフォーム事業者に対してどのような内容のデータを提供するか
991 ― プラットフォーム事業者がどのような目的・方法で提供データを利用できるか
992 ― プラットフォーム事業者による加工処理等により生じる派生データの利用権限
993 その他の成果物の取扱いはいかなるものか
994 ● プラットフォーム事業者からサービス事業者への提供（図A-2.3における場（4））
995 ― 機器ベンダーから提供を受けたデータのうち、提供される予定のサービスの内
996 容等を踏まえて、どの内容を個別のサービス事業者に提供するか
997 ― 各サービス事業者がどのような目的・方法でデータ、サービスを利用できるか
998 ― サービス事業者による加工処理等により生じる派生データの利用権限その他
999 の成果物の取扱いはいかなるものか
1000 （4）サービス利用契約：住まい手と各サービス事業者との間で締結され、サービスの内容や
1001 提供期間に加え、取得する個人データの取扱いに係る条項を含む。本ユースケースで
1002 は、サービス事業者が個別に取得する個人データに加えて、機器ベンダーが提供する
1003 多数の機器から住まい手に関するデータを取得することから、住まい手から見て全体の
1004 データ利活用プロセスについて透明性を確保できるような説明を伴っていることが望ま
1005 しい。



1006 図A-2.3 必要な制度的な保護措置の整理（高齢者生活支援事業の提供

A-2-3.　STEP 3 「属性」の具体化

前STEPにて特定した「場」を踏まえ、各種データの管理に資する属性を特定する。本ユースケースにおいては、高齢者という個人に関する情報を取扱うことから、属性の検討に際しても個人情報保護法制はまず参照されるべきルールとなる。加えて、開示範囲やデータ管理主体、利用期限等の事業者間の責任分解にも関連する内容を特定する際には、当事者間で締結される各種契約・規約が有用である。

表A-2.2 「属性」の検討において考慮すべきルール（場）

		個人情報保護法	機器利用規約	データ提供契約	サービス提供契約
カテゴリ	パーソナルデータ保護	○			
	知的財産（営業秘密を含む）保護			○	
	…	…	…	…	…
開示範囲		○	○	○	○
利用目的		○	○	○	○
データ管理主体			○	○	○
データ権利者		○	○	○	○
価値（重要度）			○	○	○
媒体・保存先			○	○	○
利用期限			○	○	○

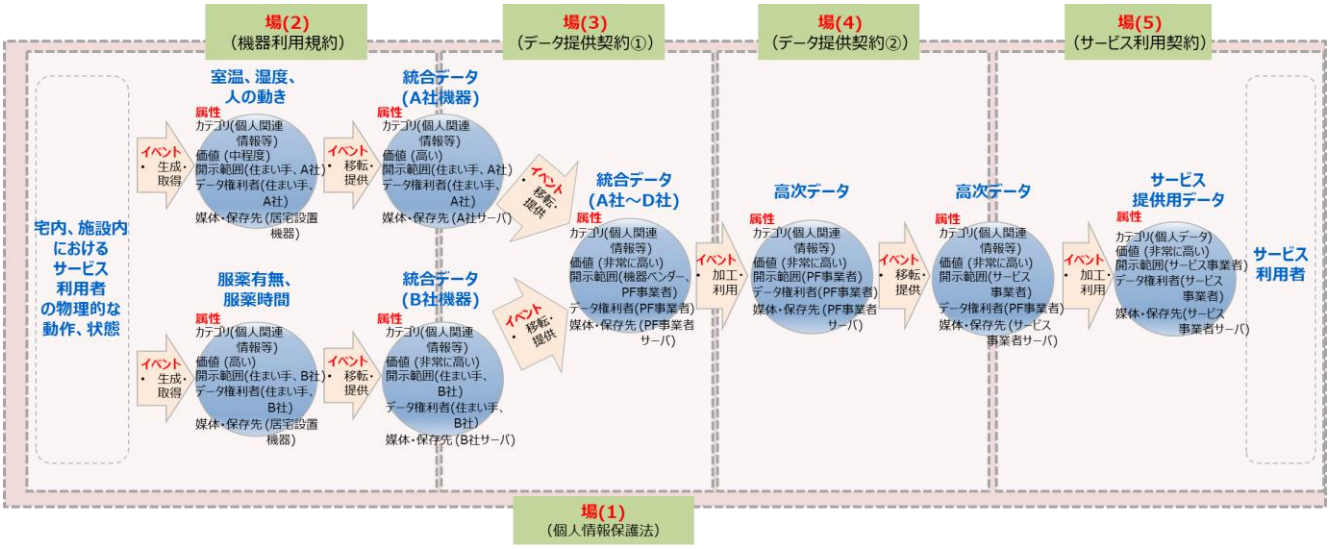
本ユースケースにて取扱われるデータの多くは個人データ又は個人関連情報等に該当する。機器から収集したデータは、別途利用者データ等と突合されない場合は「カテゴリ」が個人関連情報等に該当すると考えられるが、第三者提供先において個人データとなることが想定されるかどうか、その場合に本人同意が得られていることが確認できているかどうかが重要となるため、後述するように、上記に示した属性項目とは別途同意の取得状況等が管理されていることが望ましい。上記の事項を考慮して具体化した本ユースケースで取扱うデータがとり得るパラメータの例を以下に示す。

表A-2.3 本ユースケースにて取扱うデータ（一部）の「属性」パラメータ例

		統合データ（A 社）	統合データ（A 社～D 社）	高次データ	サービス提供用データ
カテゴリ	パーソナルデータ保護	個人関連情報 等	個人関連情報 等	個人関連情報 等	個人データ
	知的財産（営業秘密を含む）保護	営業秘密（A 社）	営業秘密 等[27]（PF 事業者）	営業秘密 等（PF 事業者）	営業秘密（サービス事業者）
	…	…	…	…	…
開示範囲		A 社内	PF 事業者内	PF 事業者内	サービス事業者内
利用目的		• 取得データを活用した各種サービスの提供	左記と同様	左記と同様	左記と同様
データ管理主体		A 社	PF 事業者	PF 事業者	サービス事業者
データ権利者		住まい手、A 社	住まい手、機器ベンダー、PF 事業者	住まい手、PF 事業者	住まい手、サービス事業者
価値（重要度）		高い	非常に高い	非常に高い	非常に高い
媒体・保存先		A 社サーバ	PF 事業者サーバ	PF 事業者サーバ	サービス事業者サーバ
利用期限		特になし	データ提供契約終了から 1 年	データ提供契約終了から 1 年	サービス提供期間終了まで

上記では表形式でデータとその属性の一覧を提示したが、データ利活用プロセスの全体におけるデータの属性の変化とイベントとの関係をより俯瞰的に示すために、STEP 2までに作成している図に属性を記入すると図A.2-4のようになる。

[27] 表 A-2.3 のデータのうち、特定の事業者間で共有されるものについては、不正競争防止法上の「限定提供データ」に該当する場合も想定される。



図A.2-4「属性」の提示方法の例

A-2-4. STEP 4「イベント」ごとのリスクポイントの洗い出し

A-2-4-1. 「イベント」ごとのリスクポイントの洗い出し

ここまでで特定したデータ利活用フローや認識すべきルール(場)、データの管理に資する属性の内容を踏まえ、本ユースケースのうち、図A.2-2に示す各機器ベンダーが保有する「統合データ」の「移転・提供」プロセスに関して以下のようなリスクを想定することができる。下記と同様の検討は、全体プロセスにおける他のデータやイベントに対しても同様の方法でなされる。

前述したように、本フレームワークでは、対象の移転・提供事象について、4つの単位(国・地域・組織・人、システム・サービス、機器)の単位でリスクを整理することが可能としているが、本ユースケースにおいては一例として以下のようなリスクが特定され得る。

＜国・地域＞

- 国や地域をまたがるデータの移転・提供は想定していないため、非該当

＜組織・ヒト＞

- 統合データの提供前に、提供元の機器ベンダーが提供先のプラットフォーム事業者において当該データが個人情報として取得されるかどうかを確認していない。
- プラットフォームにて特定の個人の特定を行う場合に、住まい手の同意等を得ることなくデータがプラットフォーム事業者に提供される。

＜システム・サービス＞

- 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、通信内容が漏えいする。

＜機器＞

- 悪意のある内外の主体が機器ベンダーの管理するサーバから当初接続を意図していなかったサーバ等にデータを送信する。

表A.2-4 各機器ベンダー「統合データ」のPF事業者への「移転・提供」にて想定されるリスクの例

大分類	中分類	各機器ベンダーが保有する「統合データ」の PF 事業者への「移転・提供」にて想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、通信内容が漏えいする。 ● 悪意のある内外の主体が機器ベンダーの管理するサーバから当初接続を意図していなかったサーバ等にデータを送信する。
	完全性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、データを改ざんする。
	可用性	● 悪意のある第三者がデータ基盤の API を無作為に呼び出すような DoS 攻撃を行い、プラットフォーム事業者サーバの処理が停止する。
関連する法制度等に係る観点	パーソナルデータ保護	● 統合データの提供前に、提供元の機器ベンダーが提供先のプラットフォーム事業者において当該データが個人情報として取得されるかどうかを確認していない。 ● プラットフォームにて特定の個人の特定を行う場合に、住まい手の同意等を得ることなくデータがプラットフォーム事業者に提供される。
	知的財産（営業秘密を含む）保護	● 各社の統合データが悪意のある内外の主体により不正な手段で取得され、開示、使用される。
	…	

なお、本ユースケースのように提供先において高度なサービス提供等のために個人関連情報等が個人データとして取得されることが想定される場合、「機密性」や「パーソナルデータ保護」等の観点でより影響度の大きいリスクが顕在化する可能性がある。そのようなリスクには、通常サイバーセキュリティの文脈で着目される外部の攻撃者によるデータ漏えい等だけでなく、正規の事業者によるデータの不正利用（意図的なものと非意図的なものの双方を含む）が含まれる。本ユースケースでは、関連する規定を考慮すると、A-2-3にて述べたものに加えて、当該データの処理に関する同意の取得状況、有効性等を管理すべき属性として指定し、関連する組織等の

ポリシーやシステムに管理の仕組みを設計・構築等することでプライバシー保護に係るリスクの低減に資することが想定される。

A-2-4-2. 今後のデータ管理の高度化に向けた課題の検討

STEP 1からSTEP 4に至るまでのフレームワーク適用プロセスを通じて明らかになったように、本ユースケースでは様々な機器によるデータの収集からその加工、最終的な利用に至るまで多数の事業者が関与しており、そのように複雑なビジネス構造には、事業者間の相互依存性等に根差す特有のリスクも想定される。こういった体制が事前に予見されている、又は現に行われている場合、コンソーシアム等の枠組みを活用して、参画する各社が相互に連携してリスクを低減する試みを進めることが有効になると考えられる。そこで必要になる対策は、複雑なデータ利活用の実態を踏まえれば非常に多岐にわたると考えられるが、例えば以下が含まれる可能性がある。

- 複雑なデータ利活用プロセスに配慮した利用目的の提示や同意の取得等
  本ユースケースのような多数の機器、サービス、事業者が関与する複雑なビジネス構造の中では、データ主体である住まい手に対してデータ利活用プロセスの透明性を確保することがより困難なものとなる。本ユースケースにおいて健康状態や詳細な行動ログ等の機微なデータが活用されるという点も踏まえれば、最悪の場合、サービスの継続に係る課題につながる可能性もある。そのようなデータ利活用の透明性に関連したリスクを低減するためには、データ主体（ここでは高齢者を含む住まい手）に対する、各事業者の役割を含むサービスの全体像及びデータ主体が得られる効用や、統合的な個人データ等の取扱いポリシーの提示、それらに関する理解しやすい説明等が重要である。一方で、それらの取組は事業者やサービスの利用者に一定の負担をかけるものだが、いわゆる「同意疲れ」等の問題も指摘されていることから、そのような負担にも配慮した方法が検討されることが望ましい。

- 機微なデータの生成・取得に関連し得る各種IoT機器におけるセキュリティ等の確保
  本ユースケースでは、特にデータの「生成・取得」段階において、エアコンや服薬支援機器、活動量計等の製造者の異なる多数の機器が利用される。それらのデータが集約され、統合的に処理される情報システムのセキュリティ管理は従来から課題視される傾向にあるが、一方でそれらのデータを生成・取得する末端のIoT機器については、それらがデータの信頼性を確保しようとするにあたり重要な構成要素であるにもかかわらず、セ

キュリティ等の確保に向けた対処は未だ途上にある場合が多いと考えられる。機器によっては個人に関する比較的機微なデータを取扱う可能性があることから、想定されるリスクやその程度を踏まえつつ、各機器ベンダーにおいて適切な水準のセキュリティ対策を実装し、それらを取りまとめる事業者やサービス利用者はその旨を確認することが望ましい。

A-3. IaaS、PaaS、SaaS等を利用してサービスを提供する例

デジタル技術を活用した価値創出の推進が社会的な課題と認識される中、重要な基盤技術の一つとしてクラウドコンピューティング技術に注目が集まっており、ますます多くの利用者がクラウドサービスを利用するようになっている。かかるサービスの適切な利用を通じて、利用者は費用負担や導入にかかる時間的コストの効率化、セキュリティ水準や技術革新対応力、柔軟性の向上等のメリットが得られると考えられている[28]。

従来から課題として認識されていたセキュリティ水準等の懸念が、クラウドインフラのセキュリティ向上や利用者支援機能の充実等を通じて低減されてきた一方で、サービス提供者と利用者との間の責任分界に対する認識が不十分であることに起因するクラウド利用者自身の設定ミス等によるインシデントの増加、システムの複雑化に伴うデータの地理的所在等の透明性の不足等の課題が残存している点が指摘されている[29]。

上記の背景を踏まえ、事業者間の責任分界の明確化やデータフローの透明性確保に資する検討の例として、クラウドサービスを利用した以下の流れによるデータの利活用プロセス（A-3内において、以下、「本ユースケース」という。）を取り上げる。

- サービス・物販事業を運営するA社は、従来から行っている物理店舗を通じた製品・サービスの提供に加え、近年は会員用ポータルサイトの構築や顧客管理サービス（SaaS）の利用等を通じた更なる顧客価値の向上に取り組んでいる。
- 顧客はA社の運用するポータルサイトに登録、ログインした上で画像・動画データを自身のPCやスマートフォンにダウンロード等できる。また、顧客はポータルサイト経由で、関連する商品を購入することもできる。従来、画像・映像はA社従業員がCDやDVD等の媒体にコピーしたうえで顧客に郵送等していたが、本システムの導入により顧客への画像・映像の受け渡しにかかる工数が大幅に削減され、顧客としても撮影した画像・動画データを複数の端末から閲覧でき、自らの趣向に合わせて加工したりダウンロードしたりできる等のメリットが得られる。
- A社のポータルサイトはB社の提供するPaaS（Webアプリ開発・運用基盤）上に構築されており、そこで取得される会員情報や商品購入情報等はポータルサイトを構成する顧客DBに格納されるだけでなく、B社より別途SaaSとして提供され商品の販売管理等を行う

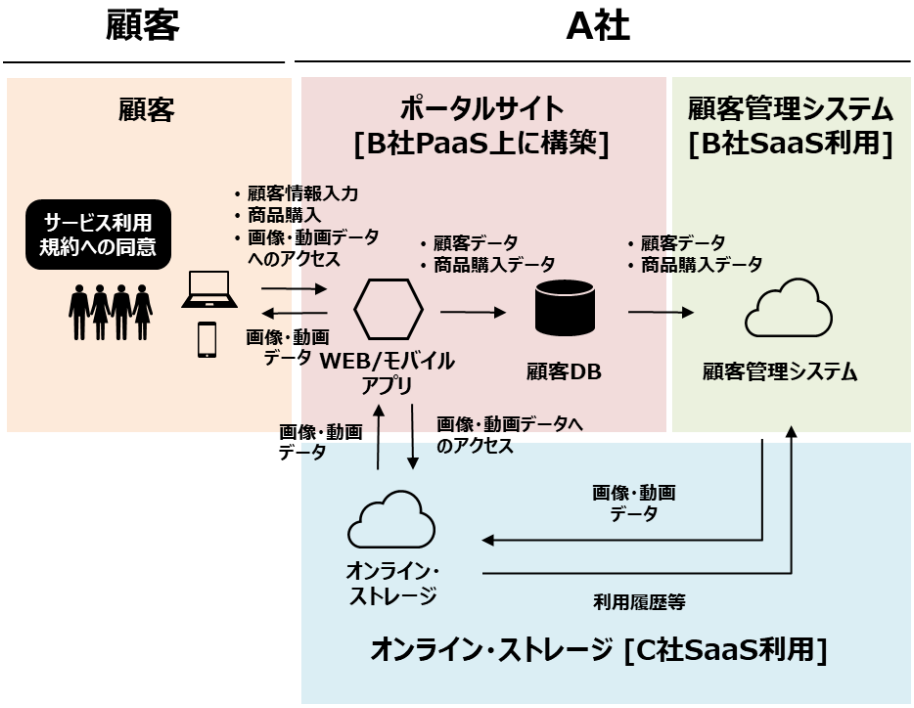
---

[28]『政府情報システムにおけるクラウドサービスの利用に係る基本方針』（https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20210330kihon.pdf ）

[29] クラウドサービス利用にかかわるリスクに関しては、経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 2013 年度版附属書」の「A（参考）クラウドサービス利用にかかわるリスク」、Cloud Security Alliance (CSA)「クラウドの重大セキュリティ脅威 11 の悪質な脅威」」等を参照。

A社顧客管理システムにも共有される。

- A社は、顧客が画像・動画データをC社の提供するSaaSを利用した自社のオンライン・ストレージにアップロードする。上述のとおり、顧客はポータルサイト経由で同ストレージにアクセスし、画像・動画データをダウンロードしたり、加工したりすることができる。データのダウンロード等の履歴は顧客管理システムに定期的に共有される。



図A-3.1 対象プロセスの概要

本ユースケースでは、A社がPaaSやSaaS等の性質の異なる複数のクラウドサービスを利用しているが、A社が上記のスコープにて適切な水準のセキュリティ等の信頼性を確保しようとする際に、考慮すべきステークホルダーとして以下が挙げられる。

- 顧客：A社が提供するポータルサイトにアクセスし、画像・動画データの加工、ダウンロードや関連商品の購入を行う。
- A社：サービス・物販事業等を業として行い、顧客価値を高めるための試みとしてクラウドサービスカスタマ[30]としてB社やC社から提供される各種クラウドサービスを利用しつつポータルサイトや顧客管理システム等を構築、運用している。

[30] クラウドサービスカスタマ（cloud service customer）とは、「クラウドサービスを使うためにビジネス関係にあるパーティ」を指す。(ISO/IEC 17789:2014) クラウド利用者とも呼ばれる。

- クラウドサービスプロバイダ[31]：A社に各種のクラウドサービスを提供する事業者
  - B社：ポータルサイト向けにWebアプリ開発・運用基盤をPaaSとして、顧客管理システム・サービスをSaaSとしてA社に提供する。
  - C社：画像・動画データを格納するオンライン・ストレージサービスをSaaSとしてA社に提供し、ピアクラウドサービス[32]としてB社の提供するサービスの基盤となっているIaaSも別途提供している。
- クラウドサービスパートナ：B社PaaS上にポータルサイトを構築することに加え、各サービス間の連携部分を開発する。

上記に示すように、本ユースケースではクラウドサービスカスタマであるA社と直接契約するB社が当該契約上は第三者であるC社のIaaSを利用してPaaSやSaaSを提供しているという「クラウドサプライチェーン」がある。クラウドサービスのサービスモデルの分類[33]を参照しつつ、本ユースケースにおけるクラウドサービス提供に係るサプライチェーンの概要を示したものが図A-3.2である。一般にこうしたクラウドサプライチェーンにおいては、以下のような課題が生じ得る[34]ために、クラウドサービスプロバイダ及びクラウドサービスカスタマの双方において適宜情報開示や適切な契約等に基づく監査の実施等の対策[35]を行うことが望ましい。

- A社のようなクラウドカスタマから見た直接の契約先（ここではB社）に問題がない場合にも、配下に存在する PaaSやIaaSに問題が生じた際、連鎖的な問題に巻き込まれる。
- 障害が要因となり事業活動に何らかの損害が生じた場合に事業者間で責任分界があいまいになりやすい。

---

[31] クラウドサービスプロバイダ（cloud service provider）とは、「クラウドサービスを利用できるようにするパーティ」を指す。（ISO/IEC 17789:2014）

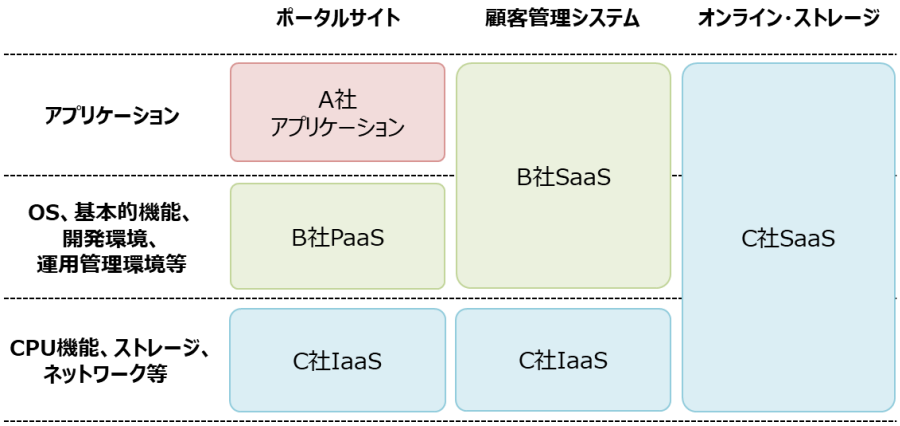
[32] ピアクラウドサービス（peer cloud service）とは、「一つのクラウドサービスプロバイダのクラウドサービスであって、他の一つ以上のクラウドサービスプロバイダのクラウドサービスの一部として使用されるクラウドサービス」を指す。（ISO/IEC 17789:2014）

[33] サービスモデルの分類を定義する主な文献として、米国国立標準技術研究所（NIST）「NIST によるクラウドコンピューティングの定義」や各府省情報化統括責任者（CIO）連絡会議決定「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等を参照

[34] 経済産業省「クラウドセキュリティガイドライン活用ガイドブック 2013 年度版」

[35] 具体的な取組みの例として、ホワイトペーパーの活用、確認等によるクラウドセキュリティ認証制度（例：ISMSクラウドセキュリティ認証、政府情報システムのためのセキュリティ評価制度（ISMAP））の認証基準への対応状況の確認や、既存の監査報告書（例：SOC2 報告書）の活用、個別の調査等による確認が挙げられる。

- 法規制上の問題やクラウドサービスカスタマのセキュリティポリシー等に関連して、外国や外国法適用配下に情報を置くべきでないとされているにも関わらず、サプライチェーンの配下に該当する事業者が存在し、カスタマの意図に反する状態に陥ってしまう。



図A-3.2　クラウドサービス提供に係るサプライチェーンの概要

A-3-1.　STEP 1　データ処理フロー（「イベント」）の可視化

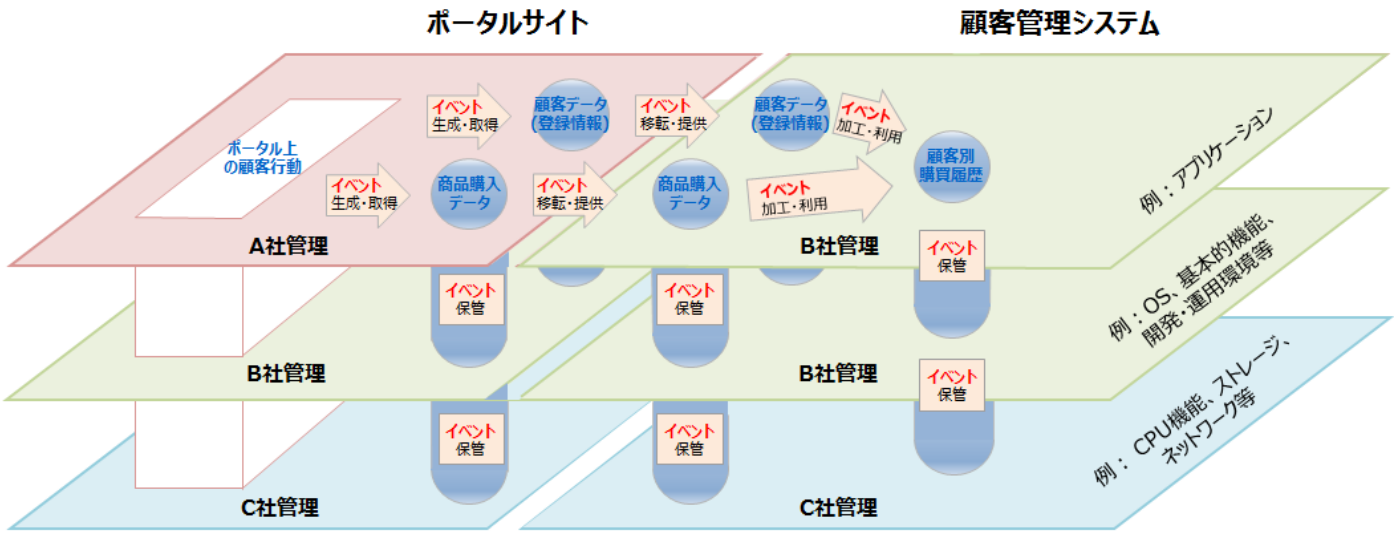
本ユースケースにおけるデータ処理フローは図A-3.3で示すように、以下のプロセスにより構成される。本節以降では、特に(2)のプロセスについて、データ処理フローの可視化、必要な制度的な保護措置（「場」）の整理等を行う。

(1) 適切な契約等に基づいて、顧客の画像・動画データが「生成・取得」され、A社従業員によりC社の提供するオンライン・ストレージへ「移転・提供」され、「保管」される。画像・動画データは、顧客からの求めに応じて「加工・利用」（オンライン・ストレージ上での画像編集等）されたうえで顧客所有の端末（PC、スマートフォン等）に「移転・提供」される。

(2) ポータルサイト上では顧客による自身のデータの入力や製品等の注文、その他の行動に応じて、「顧客データ」、「商品購入データ」等が「生成・取得」され、顧客DBに格納される。当該データは、適時にB社が提供する顧客管理システムに「移転・提供」され、A社内の個別のニーズに応じてA社従業員により「加工・利用」される。フローを可視化する際は、ポータルサイトはC社がIaaSとして提供する物理・仮想インフラ（CPU機能、ストレージ、ネットワーク等）上にOS、開発環境、運用環境等を整備したB社PaaS上に構築されている点に留意する必要がある。

前述したように、本ユースケースのように複数の事業者のサービスからなるサプライチェーンを編成したクラウドサービスを利用する場合、その複雑性等に起因する特有のリスクが想定される。そのため、データ処理フローや必要な制度的な保護措置（「場」）を整理し、想定される

リスクを可能な限り網羅的に特定しようとする際には、必要に応じて、クラウドサプライチェーンの透明性の確保や責任分界の明確化という観点から、多層的なサービスの提供体制を踏まえた検討を実施することが望ましい。サービスの多層性を表現する際の観点は様々なものが考えられ得るが、図A-3.3では、一例として図A-3.2と同様の分類に基づいて、①アプリケーション、②OS、基本的機能、開発・運用環境等、③CPU機能、ストレージ、ネットワーク等の3つの異なる観点から各社の責任分界を含む「場」を示し、それらが一体となってデータ処理（イベント）を実施している態様を記述している。



図A-3.3 データ処理フローの可視化イメージ（IaaS、PaaS、SaaS等を利用したサービス）

A-3-2. STEP 2 必要な制度的な保護措置（「場」）の整理

本ユースケースにおいて、顧客データ等が個人データに該当する点や、当該データを処理、管理するシステムが複数のクラウドサービスを組み合わせて実現されている点等を考慮すると、例えば下記のルールや各社の必ずしも明文化されていないルール等が「場」として特定され得る。

（1）A社サービス利用規約等：A社は顧客との間でポータルサイトの利用等に関連して規約を設定し、同意を得る必要がある。規約又は別途定められる個人情報保護方針等にはサービスの内容や利用に際しての禁止事項、免責事項等に加え、氏名、住所、連絡先等の顧客データ（登録情報）や画像・動画データの保護に関する規定が含まれるべきである。かかる規定は、本ユースケースにおいて該当する個人データを取扱うすべてのプロセスにおいて遵守されるべきものである。

（2）個人情報保護法：A社が顧客から取得する顧客データや結果として取得される顧客別

購買履歴は個人データに該当すると考えられることから、A社は個人情報取扱事業者に課せられる規律を遵守する必要がある。また、A社によるB社及びC社提供クラウドサービスの利用が、個人データの第三者提供に該当するかどうか（B社及びC社が個人情報を取扱うかどうか）、該当する場合はそれがB社又はC社への「委託」にあたるか、本人からの同意を得る必要があるか[36]、当該提供行為が「外国にある第三者への提供」にあたるかどうか等を確認し、その結果に応じて適切な管理を行うことが必要となる。本ユースケースにおいては、①ポータルサイトの開発・運用に関連して利用されているB社、及びC社のサービス、②顧客管理システムの開発・運用に関連して利用されているC社サービスでは、サーバに保存された個人データを取扱わない旨を契約条項により定め、適切にアクセス制御を行っているものと想定する。

（3）各種クラウドサービス利用規約：本ユースケースにおけるA社の各種システムは、B社、及びC社が提供するクラウドサービスを利用して開発・運用されているが、前述したクラウドサプライチェーンや、それに係るリスクを踏まえた検討を行う場合、関連するクラウドサービス利用規約等を「場」として特定することが望ましい。ここで、特定されるべき規約等としては例えば以下があると考えられる。

- A社がポータルサイトを運用するために必要なA社とB社、及びB社とC社とのサービス利用規約（それぞれを、「B社PaaS利用規約」、「C社IaaS利用規約」と呼ぶ）
- A社が顧客管理システムを利用するために必要なB社の規約（B社SaaS利用規約）、及びB社に物理・仮想インフラ（CPU機能、ストレージ、ネットワーク等）を提供するC社の規約（C社IaaS利用規約）
- A社のポータルサイトと顧客管理システムとのデータ連携機能（B社提供）の運用に係る契約

また、上記規約等により規定される各組織のセキュリティに関する役割と責任を明確化しておくことが望ましい。例えば、A社がB社の提供する顧客管理システム（SaaS）を利用する際、各種ハードウェアやOS、ミドルウェア、アプリケーションへの脆弱性対応等の各

---

[36] クラウドサービスの利用が、「本人の同意が必要な第三者提供」または「委託」に該当するかどうかは、クラウドサービスを提供する事業者において個人データを取扱うこととなっているのかどうかが判断の基準になるとされる。その際、クラウドサービスプロバイダが、個人データを取扱わないこととなっている場合としては、「契約条項によって当該外部事業者がサーバに保存された個人データを取扱わない旨が定められており、適切にアクセス制御を行っている場合等」が想定される。当該クラウドサービスプロバイダが、個人データを取扱わないこととなっている場合には、個人情報取扱事業者は個人データを提供したことにはならないため、「本人の同意」を得る必要はないとされる。［個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ&A Q7－53］

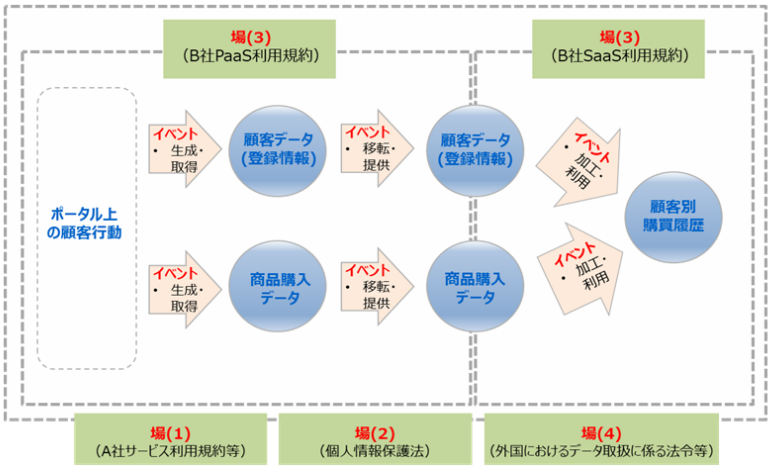
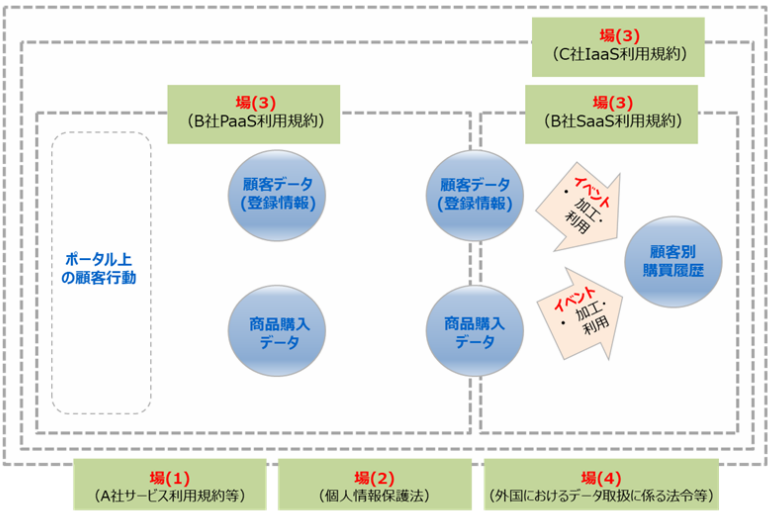
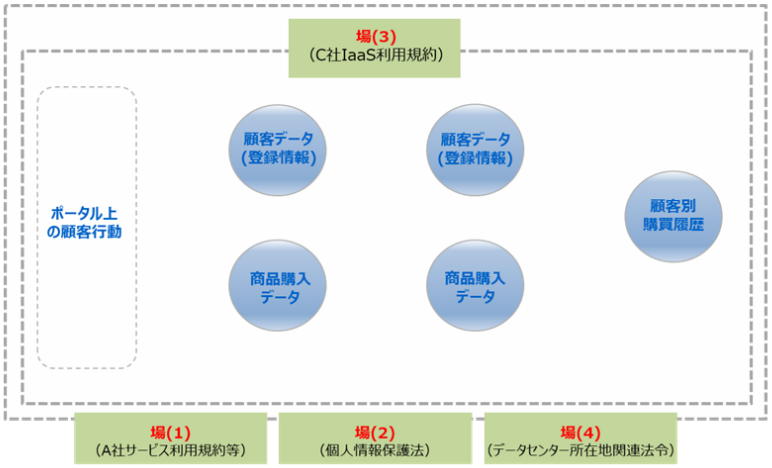
種セキュリティ対策についてはB社又はC社が担うが、SaaSを利用する端末におけるセキュリティ対策やファイルの開示範囲等の設定、社員等のアカウント管理、認証・認可等の対策は一般的にA社側で実施する必要がある。自組織の役割と責任、その履行状況等を正確に把握できないことは、意図せざるセキュリティインシデントの発生につながり得るものであり、関係者のそれぞれにおいて慎重に検討、対処されることが望ましい。

(4) データセンター所在地関連法令(外国におけるデータ取扱に係る法令等):

インターネット経由でクラウドサービスが提供される場合、サービス運用コスト等の関係でデータセンターが海外に所在しているケースが珍しくないが、当該サービスの提供者及び利用者が「場」を明確にするという観点からは、セキュリティインシデント等の事象が発生した際にどの国の法律に基づき、どの国の裁判所の判断を仰ぐ必要があるのかを認識することが重要である。私法[37]関係はクラウドサービスカスタマとクラウドサービスプロバイダとのサービス提供契約等において準拠法の指定条項や合意裁判管轄条項が含められていることが一般的である。一方で、公法関係は原則として属地主義が採用されるため、クラウドサービスカスタマのデータがデータセンター所在国の捜査機関により捜索押収される等の想定外のリスクが顕在化する恐れもあり、その場合は本ユースケースにおけるあらゆるステークホルダー(例:A社、A社サービスを利用する個人)が影響を被り得る。上記に関連して、A社及びB社におけるクラウドサービス等の利用に際しては、外国におけるデータ取扱に係る法令等に関連して具体的な争訟リスクが予見されるかどうかも考慮して、データセンターの所在地を含めたサービスの検討がなされることが望ましい。

図A-3.4において、上記で特定した(1)から(4)の場を、図A-3.2に示した各事業者の責任分界を念頭に置きつつ、関連する事業者ごとに各々の立場から整理している。なお、図中におけるイベントの記載有無は、対象の事業者が当該イベントの実施に対して責任を有しているかどうかを示している。

[37] ここで、公法とは、「国家と私人との法律関係」を規律する法であり、私法は「私人と私人との法律関係」を規律する法を指すものとする。

事業者ごとの観点を踏まえた整理	必要な制度的な保護措置の整理例（IaaS、PaaS、SaaS等を利用したサービス）
A社から見た整理	
B社から見た整理	
C社から見た整理	

1243 図A-3.4 必要な制度的な保護措置の整理例（IaaS、PaaS、SaaS等を利用したサービス）[38]

[38] 図中の破線部はポータルサイト及び顧客管理システムで同一の規範が適用され得る範囲を示し、実線部は両者で別個の規範が適用され得る範囲を示している。

A-3-3.　STEP 3 「属性」の具体化

本ユースケースにおいては、顧客本人又は関連する人物が映った画像・動画データを取扱うことから、A-2と同様に属性の検討に際して個人情報保護法制はまず参照されるべきルールとなる。加えて、データの開示範囲やデータ管理主体、利用期限等の利用上の制約に係る事項を特定する際には各種クラウドサービス利用規約の条項、媒体・保存先の適切性等を検討する際にはデータセンター所在地関連法令等を参照することが有用である。

表A-3.1「属性」の検討において考慮すべきルール（場）

		A 社サービス利用規約等	個人情報保護法	各種クラウドサービス利用規約	データセンター所在地関連法令
カテゴリ	パーソナルデータ保護	○	○		
	知的財産（営業秘密を含む）保護			○	
	…	…	…	…	…
開示範囲		○	○	○	
利用目的		○	○	○	
データ管理主体		○	○	○	
データ権利者		○	○		
価値（重要度）		○	○		
媒体・保存先				○	○
利用期限		○		○	

上述したとおり、顧客データや商品購入データ、画像・動画データがいずれも個人データに該当することから、データ権利者は顧客自身となり、A社は個人情報取扱事業者の義務の一環として顧客からの「開示等の請求等」[39]に適切に対応する必要がある。また、顧客管理システムの開発・運用に関連して利用されているC社サービスでは、サーバに保存された個人データを取扱わない旨を契約条項により定め、適切にアクセス制御を行うとされていることから、実質的

[39] 個人情報の保護に関する法律（最終改正：令和 2 年 6 月 12 日法律第 44 号）第 32 条を参照

にデータへアクセスし、一定の管理責任を有しているA社、B社をデータ管理主体として設定している。なお、本ユースケースのように複数のクラウドサービスプロバイダが、分業して特定のサービスが提供される場合、A社のようなクラウドサービスカスタマはC社のような事業者を必ずしも認知せずサービスを利用する状況になり得る。特に、関連する法制度や組織内のポリシー等でデータの所在地に制約を課しているようなケースでは、契約前にクラウドサービスプロバイダ（本ユースケースにおいてはB社）に対して情報の開示を要求し、下記の媒体・保存先に相当するデータの所在地等に関する情報を収集しておく必要がある。

表A-3.2 本ユースケースにて取扱うデータ（一部）の「属性」パラメータ例

		顧客データ[40]	商品購入データ	画像・動画データ
カテゴリ	パーソナルデータ保護	個人データ	個人データ	個人データ
	知的財産（営業秘密を含む）保護	A 社の営業秘密	A 社の営業秘密	-
	…	…	…	…
開示範囲		A 社、顧客	A 社、顧客	A 社、顧客
利用目的		・ 顧客への各種サービスの提供 ・ 顧客からの問合せへの対応 ・ 顧客への広告・メールマガジンの送付		・ 顧客への各種サービスの提供
データ管理主体		A 社、B 社	A 社、B 社	A 社
データ権利者		顧客	顧客	顧客
価値（重要度）		高い	高い	高い
媒体・保存先		B 社 SaaS（C 社 IaaS）	B 社 SaaS（C 社 IaaS）	C 社 SaaS
利用期限		会員契約終了から 2 年	会員契約終了から 2 年	撮影後 2 年間

[40] A-3-3 では、「顧客データ」及び「商品購入データ」として、A 社顧客管理システム内に保管されているデータを専ら取扱う。「顧客データ」には、識別子、認証情報、住所、氏名、メールアドレス等を含む。

A-3-4. STEP 4「イベント」ごとのリスクポイントの洗い出し

A-3-4-1. 「イベント」ごとのリスクポイントの洗い出し

STEP 3までの検討事項を踏まえ、以下では本ユースケースのうち、図A.3-4に示すA社がB社により提供される顧客管理システム上で取扱う「顧客データ」の「加工・利用」及び「保管」のプロセスに関して以下のようなリスクを想定することができる。A-1及びA-2と同様、下記の検討は、全体プロセスにおける他のデータやイベントに対しても同様の方法でなされる。

表A.3-3 顧客管理システムにおける「顧客データ」の「加工・利用」「保管」で想定されるリスク(例)

大分類	中分類	A 社が B 社により提供される顧客管理システム上で取扱う「顧客データ」の「加工・利用」及び「保管」にて想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 悪意のある外部の主体がパスワードリスト攻撃等により A 社従業員になりすまし、顧客管理システムに保管された顧客データを外部に漏えいさせる。 ● 悪意のある外部の主体が顧客管理システム（B 社 SaaS）の脆弱性を悪用して顧客管理システムに不正アクセスし、顧客データを外部に漏えいさせる。 ● A 社従業員による B 社 SaaS のアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体に顧客データが開示される。 ● 国内又は国外の司法機関等からの求めに応じて共同利用しているサーバ等の押収がなされる際、十分な保護が必要な顧客データが開示される。
	完全性	● 悪意のある内外の主体によりアプリケーションが改ざんされ、顧客データの処理にあたって不正な処理が行われる。 ● 悪意のある内外の主体により保管中の顧客データが改ざんされる。
	可用性	● 悪意のある第三者が B 社 SaaS に対して DoS 攻撃を行い、A 社システムを含む多数のカスタマ向けの処理が停止する。 ● 悪意の有無を問わず、B 社 SaaS 又は C 社 IaaS に対して過度のトラフィックが集中し、急激なピーク負荷がかかることで、A 社システムを含む多数のカスタマ向けの処理が停止する。

大分類	中分類	A 社が B 社により提供される顧客管理システム上で取扱う「顧客データ」の「加工・利用」及び「保管」にて想定されるリスク（例）
関連する法制度等に係る観点	パーソナルデータ保護	● A 社又は B 社の正規の利用者により、顧客に通知された利用目的以外の用途で顧客データが利用される。 ● A 社の担当者等により B 社に対する必要かつ適切な監督が十分行われない。
	知的財産（営業秘密を含む）保護	● 顧客データが正当な手段によりデータを取得した悪意のある内外の主体（B 社従業員を含む）により不正の利益を得る目的、又は A 社に損害を加える目的で使用される。
	…	

1272 なお、本ユースケースのように、クラウドサービスカスタマにおいて、サービス提供に係るクラ
1273 ウドサービスプロバイダが個人データを取扱わないことを契約で取り決める場合は、自社が取
1274 扱う個人データとして安全管理措置を講じる必要がある。また、外国で個人データを取扱う場合
1275 に該当する場合[41]には、当該国における個人情報保護に関する制度等を把握した上で安全管
1276 理措置を講じる必要がある。そのため、表A-3.2で示す属性項目以外に「取扱い国」等の項目を
1277 設け、当該国における個人情報保護に関する制度等を把握する必要がある。また、この検討
1278 等に必要な情報を収集するため、クラウドサービスプロバイダ等との間の契約において、情報
1279 の開示を求める等して、データセンター所在地等を把握できるようにしておくことが望ましい。な
1280 お、保有個人データを外国で取扱う場合には、「保有個人データの安全管理のために講じた措
1281 置」として、クラウドサービスプロバイダ及び当該データが保存されるサーバが所在する外国の
1282 名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を公表等する必要が
1283 ある。

1284 A-3-4-2. 今後のデータ管理の高度化に向けた課題の検討

1285 STEP 1からSTEP 4に至るまでのフレームワーク適用プロセスを通じて明らかになったよう
1286 に、本ユースケースでは、クラウドサービスカスタマが、複数の事業者がサプライチェーンを構

41 外国にある支店・営業所に個人データを取扱わせる場合や外国にあるクラウドサービスプロバイダの提供するクラウドサービスを利用し、その管理するサーバに個人データを保存する場合（日本国内に所在するサーバに個人データが保存される場合においても同様）等には、外国で個人データを取扱う場合に該当する。
https://www.ppc.go.jp/files/pdf/2109_APPI_QA_4ejj3t.pdf

成して提供するサービスを含め、機能別に複数のクラウドサービスを利用しており、そこではオンプレミスでシステムを構築し、運用する際とは異なる複数のリスクが想定される。そのようなリスクに対してA社及び関連する事業者が実施できる対応策として、例えば以下が挙げられる。

- データの物理的な所在に関する透明性の確保
  ポータルサイトの運用が既に行われているかにかかわらず、顧客データや商品購入データ等が現に保管されるデータセンターの所在地がフレームワークの適用段階で明確でない場合、A社は直接のサービスの提供者であるB社（ポータルサイト、顧客管理システム）及びC社（オンライン・ストレージ）の担当者にかかる情報の開示を求め、自社のサービス利用規約等における規定との整合やデータセンター所在地の法制度等をさらに調査し、確認したうえで、顧客の知り得る状態にしておく必要がある。

- 自社の責任分界の明確化及び運用状況のレビュー
  クラウドサービスの提供又は利用においては、オンプレミスでの管理とは異なり、クラウドサービスカスタマ及びクラウドサービスプロバイダの間でセキュリティやコンプライアンスに係る管理責任が分担されており、双方が自身の責任を果たしつつ適宜必要な情報開示等を行うことで全体として適切な管理が実現されることとなっている。このような管理のあり方は、「責任共有モデル」と呼ばれる場合がある[42]。本ユースケースにおいて、A社はSaaSやPaaS等、責任範囲が異なる複数のサービスを利用しているが、前述したように、クラウドサービスカスタマとしてのA社が責任を果たすべきアプリケーションの運用管理やアクセス権限等のセキュリティ設定が不十分な状態となることで、顧客データ等のセキュリティが侵害される恐れがある。そのようなカスタマ側の管理に起因するリスクを低減するため、A社では、STEP 2で明確化された事業者間の責任分界をさらに具体化する形で、それぞれのクラウドサービス利用において自社にて実施が必要な管理策（例：クラウドサービスにアクセスする端末の保護、アクセス権限の管理）を改めて洗い出し、運用支援ツール等も活用しつつその履行状況をレビューすることが望ましい。

[42] クラウドサービスプロバイダとクラウドサービスカスタマの責任の相違を表現しようとする際、プロバイダが責任を有するのが「クラウドのセキュリティ」(Security ‘of’ the Cloud)であり、カスタマが責任を有するのが「クラウドにおけるセキュリティ」(Security ‘in’ the cloud)と言い表すことがある。
（https://aws.amazon.com/jp/blogs/news/rethinksharedresponsibility/）

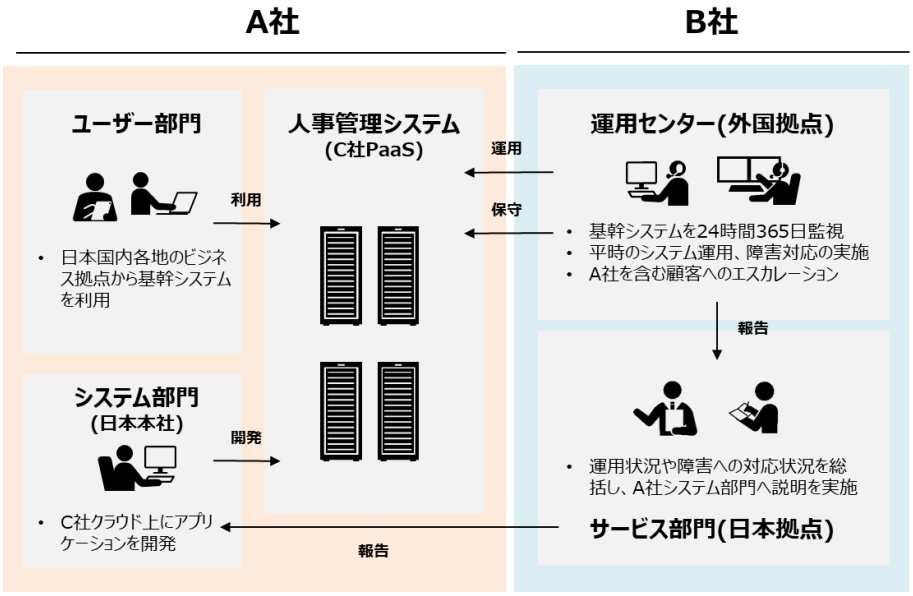
A-4. 国内で提供されるITサービスに関して、海外で開発や運用等を実施する例

デジタルトランスフォーメーション（DX）の実現等、デジタル技術の高度な活用を通じた事業等の変革の重要性が社会的に認められている一方で、高度な専門性を必要とするITシステムの開発や保守、運用等の業務に対して、自社で人的リソースを確保しそれらを内製化するのが困難なケースが広く見られる。そのような場合、長期的には自社でリソースを確保することも志向しつつ、かかる業務を適切に外部委託することで、ユーザー事業者は質の高いサービスを享受しつつ、それ以外の業務に対するリソースを確保しやすくなるとされている。さらに、IT関連のアウトソーシングに関しては、従前から事業のグローバル化への対応やコスト削減等の観点から海外に拠点を置く事業者への委託がしばしば行われている。

一方、国内ではなく国外で事業上有用な技術情報等のデータや個人データを取扱う際には、一般に個人情報保護や技術情報に係る輸出管理等の側面から十分な注意を払う必要がある。データが組織や国・地域の境界を越えて取扱われることが施行される昨今において、かかる課題は従前よりさらに重要なものになっていると考えられる。

上記の背景を踏まえ、海外で事業上のデータを取扱うことが想定される場合における、当該データに対する適切な管理の検討に資する例として、以下の流れによるプロセス（A-4内において、以下、「本ユースケース」という。）を取り上げる。

- A社は国内にて全国的に事業を展開する事業者で、従来は複数あるグループ会社ごとにシステムを構築、運用し、適宜本社へのデータ共有を実施していたが、グループ内人材のタレント管理から人事・給与まであらゆる人事業務をクラウドで行うため、全社的に統合されたシステムをC社の提供するクラウドサービスを利用して構築している。
- A社は上記システムのうち自身で責任を有する部分の運用をB社に委託している。具体的には、B社にてヘルプデスク（問合せ対応）や常時監視、障害対応、必要に応じてアドオン機能の開発等を行う。
- B社の運用センターは外国に設けられており、ITシステムの運用に対して高い専門性を有するスタッフが24時間365日対応を行っている。本社に所在するA社システム部門へ運用状況や障害への対応状況を報告等する場合は、運用センターからの報告を受け、B社日本拠点のスタッフが実際の対応を実施する



図A-4.1 対象プロセスの概要

本ユースケースにおいて、A社が全体的なセキュリティ等の管理を行うにあたり、考慮すべきステークホルダーとして以下が挙げられる。

- A社：日本各地に事業拠点を有する事業者であり、全社共通の人事管理システムをC社クラウドサービス上に構築、運用する。
- B社：A社からの委託を受け、過去に人事管理システムの構築を支援し、そこで得た知見も活用しつつ、外国の運用センターを活用してA社人事管理システムに係る運用・保守業務等を行う。
- C社：A社にクラウドサービスを提供する。

A-4-1. STEP 1 データ処理フロー(「イベント」)の可視化

本ユースケースにおけるデータ処理フローは図A-4.2で示すように、以下のプロセスにより構成される。

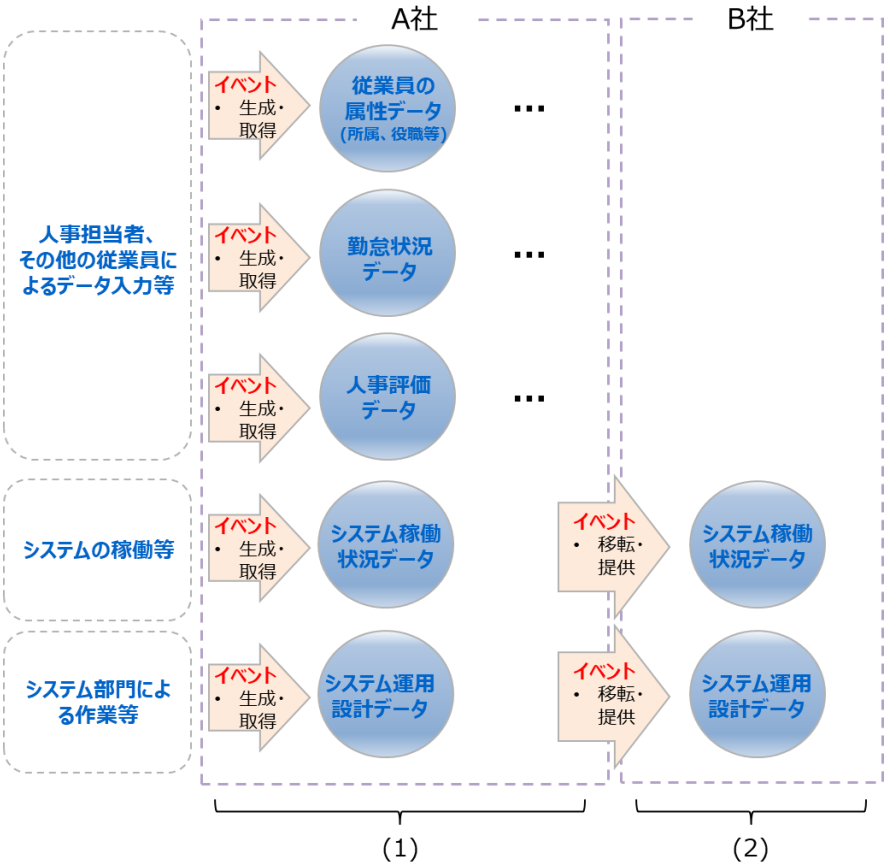
(1) 人事担当者やその他の従業員等の人事管理システムのユーザー部門の入力により、各種人事管理関連データ(図A-4.2では、従業員の属性データ、勤怠状況データ、人事評価データを記載しているが、これらに限定されない)が「生成・取得」される。これらのデータは、例えば給与計算のような従来からの用途だけでなく、人材育成や離職率低下等の目的で「加工・利用」され得る[43]。また、上記の一連のシステム利用を通じて、システ

[43] こうした「加工・利用」の在り方は多様であり得るが、その点への考慮は本ユースケースの本旨とは異なることから、図 A-4.1 では詳述しない。

ム稼働状況データが継続的に「生成・取得」される。

(2) システム稼働状況データや、運用管理等に必要なデータ（システム運用設計データ等）は運用保守の委託先であるB社に「移転・提供」され、サービス提供のために活用される。なお、少なくとも下記に挙げるような平時の運用業務を実施するにあたっては、B社は各種人事管理関連データの提供を受けないものとする。

- 各種アプリケーションのパフォーマンス管理
- 人事管理システムを対象にした修正パッチの配布、適用
- A社システム部門経由で行う問合せ対応、障害発生時の調査、対応



図A-4.2 データ処理フローの可視化

（国内で提供されるITサービスに関して、海外で開発や運用等を実施する例）

A-4-2. STEP 2 必要な制度的な保護措置（「場」）の整理

本ユースケースにおいて、顧客データ等が個人データに該当する点や、当該データを処理、管理するシステムが複数のクラウドサービスを組み合わせて実現されている点等を考慮する

と、例えば下記のルールや各社の必ずしも明文化されていないルール等が「場」として特定され得る。

（1） 個人情報保護法：A社は機密性の高い人事データを保有しているため、個人情報取扱事業者に課せられる義務の遵守が求められる。さらに、A社以外の適用範囲を考慮するうえでは、委託先となるB社やC社が、契約内容から見てA社から個人データの提供を受けているのかという点について明確化がなされる必要がある。その際、A-3でも記載したように、委託先の事業者がシステム内の個人データを取扱うこととなっている場合には、個人データを提供したことになり、本人同意の取得、又は委託契約の締結等による正当性の確保を行う必要がある。なお、上記の場合はA社から委託先に対して個人情報保護法第20条に基づき自らが講ずべき安全管理措置と同等の措置が講じられるよう監督を行う[44]必要がある点にも留意する必要がある。一方で、委託先の事業者が、契約条項において個人データを取扱わない旨を規定している場合、適切にアクセス制御を行っている場合等であれば、B社やC社へ個人データが提供されたことにはならない[45]。その場合は、B社やC社のような委託先にて個人データが取扱われていないことを確実にしたうえで、A社自身が自ら果たすべき適切な安全管理措置を講じる必要がある[46][47]。

（2） 輸出管理関係法令[48]：一般に、各社の貨物の輸出、技術情報（例：設計書、ソースコード、運用ツール）等の非居住者（日本に定住していない外国人及び日本人）への提供の際には、貨物又は技術情報等の提供が外国為替及び外国貿易法（外為法）による輸出規制の対象に該当するかどうかを判定し、必要に応じて所管省庁から許可を得る等の手続きを実施する必要がある。本ユースケースでは、システム運用設計データのような役務の実施に必要なデータのほか、該当する場合は運用ツールの提供、現地で

---

44 個人情報の保護に関する法律についてのガイドライン（通則編） 3-3-4 委託先の監督（法第 22 条関係）

45 個人情報保護委員会『「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関する Q&A』 Q7－53

46 同 Q7－54

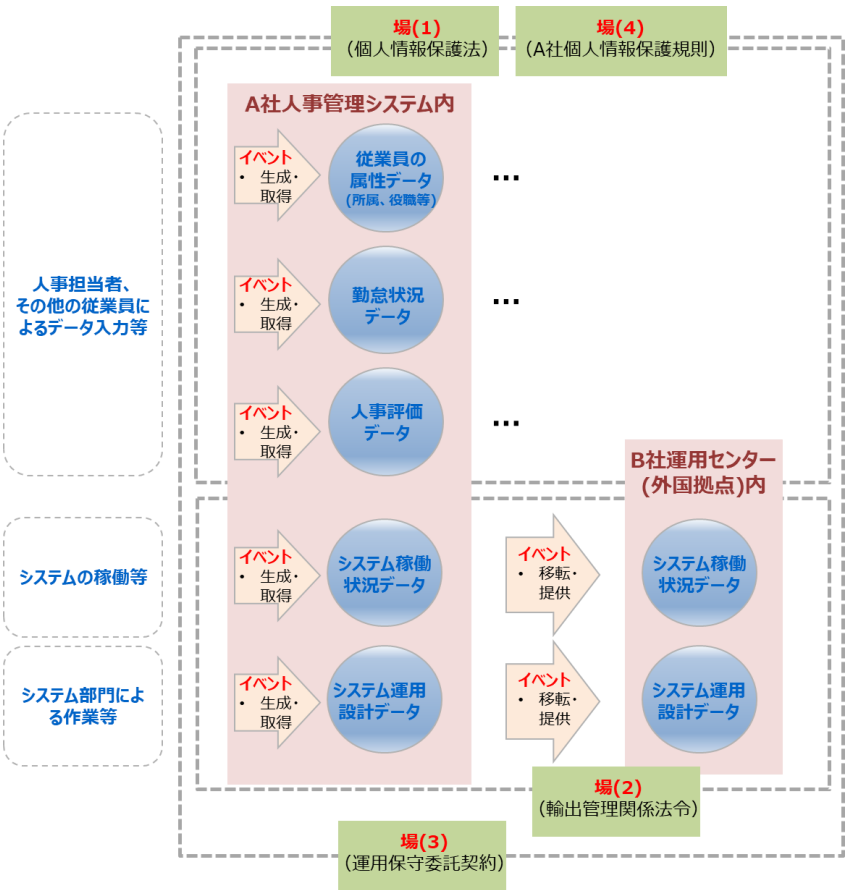
47 B 社や C 社が契約上個人データを取扱わないこととなっている場合、個人情報取扱事業者となる A 社は、外国において個人データを取扱うこととなるため、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理措置の一環として、クラウドサービスプロバイダ（ここでは B 社）が所在する外国の名称及び個人データが保存されるサーバが所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く必要がある。それが困難な場合、サーバが所在する外国の名称に代えて、①サーバが所在する国を特定できない旨及びその理由、及び、②本人に参考となるべき情報を本人の知り得る状態に置く必要がある。（同 Q10－25 を参照）

48 日本における輸出管理関係法令に関するより詳細な情報については、経済産業省 貿易経済協力局 貿易管理部 安全保障貿易検査官室「安全保障貿易管理ハンドブック（第 10 版）」等の資料を参照されたい。

の指導等が輸出管理の対象となり得る。A社及びB社は、あらかじめ輸出管理に必要な社内の手続きを整備しておき、取引前や出荷時に輸出の可否を審査、確認する必要がある。

（3） 運用保守委託契約：A社とB社の間で委託業務の仕様やその他の事項について取り決めておくものであり、例えば、A社従業員の個人情報をB社は業務の実施にあたり取扱わない点、A社技術情報等の取扱い（例：秘密保持契約）等について明確に規定する必要がある。

（4） A社個人情報保護規則



図A-4.3 必要な制度的な保護措置の整理例

（国内で提供されるITサービスに関して、海外で開発や運用等を実施する例）

A-4-3. STEP 3 「属性」の具体化

本ユースケースにおいては、A社が人事管理のために自社の従業員に関するデータを取扱うことから、カテゴリや開示範囲等の検討に際して、属性項目の検討に際して個人情報保護法制の参照が必要と考えられる。また、従業員に係るデータの利用目的やデータ管理主体、媒体・保存先

や利用期限の特定にあたっては、社内の個人情報保護規則が有用な材料となるだろう。さらに、A社とB社間の運用保守委託契約からは各データの開示範囲（取扱いの有無を含む）や媒体・保存先、利用期限等に関する規定を得ることが可能と考えられる。

表A-4.1「属性」の検討において考慮すべきルール（場）

		個人情報保護法	輸出管理関係法令	運用保守委託契約	A 社個人情報保護規則
カテゴリ	パーソナルデータ保護	○			○
	知的財産（営業秘密を含む）保護			○	○
	…	…	…	…	…
開示範囲		○	○	○	○
利用目的		○			○
データ管理主体		○			○
データ権利者		○			○
価値（重要度）		○			○
媒体・保存先			○	○	
利用期限		○		○	○

図A-4.2及び図A-4.3にて特定したデータのうち、従業員の属性データ、システム稼働状況データ、システム運用設計データの3つについて、表A-4.2にて各種属性項目のパラメータを示している。前述したように、従業員の属性データは個人データに該当し、利用目的の特定や安全管理等の個人情報取扱事業者の義務がA社に課せられる。A社自身の従業員を対象とした個人情報保護規則を参照し、開示範囲や利用目的、データ権利者（及び権利者たる従業員が行使できる権利の内容）、利用期限等の属性項目を具体化することができる。また、人事管理システムはC社が提供するPaaS上に構築されていることから、媒体・保存先としてC社PaaSを特定することができる。A社とC社の契約では、C社では個人データを取扱わないと規定していることから、開示範囲をA社内として、現にそのような管理が行われるようアクセス制御等を適切に行う必要がある。

従業員の属性データとは異なり、システム稼働状況データやシステム運用設計データは、B社においてもC社と同様に個人データが取扱われないこととなっていることも踏まえ、現に個人データを含まないデータとして管理されるべきである。また、C社に同様にB社対しても、従業員に関するデータを含むA社が管理する各種個人データに対するアクセスが適切に制御され、その状態が継続的に維持・管理される必要がある[49]。契約に基づいてB社に移転・提供されるシステム稼働状況データやシステム運用設計データ等は、運用保守委託契約を参照し、対象システムの運用、保守業務の実施や障害対応の実施等の目的で、委託契約の期間中に限り利用され、当該期間終了後に適切な手法で廃棄される。

表A-4.2 本ユースケースにて取扱うデータ（一部）の「属性」パラメータ例

		従業員の属性データ	システム稼働状況データ	システム運用設計データ
カテゴリ	パーソナルデータ保護	個人データ	非個人情報	非個人情報
	知的財産（営業秘密を含む）保護	A社の営業秘密	A社の営業秘密	A社の営業秘密
	…	…	…	…
開示範囲		A社内	A社システム部門、 B社運用担当者	A社システム部門、 B社運用担当者
利用目的		・ 人事、給与の計算、決定、支払 ・ 入社、退職、勤怠、その他の雇用管理 ・ 従業員の健康管理 ・ 会社から従業員への連絡等	・ 対象システムの運用、保守業務の実施 ・ 障害対応の実施 ・ 障害の再発防止、運用の更なる効率化に向けた対策等の検討	・ 対象システムの運用、保守業務の実施 ・ 障害対応の実施
データ管理主体		A社	A社、B社	A社、B社
データ権利者		A社、従業員	A社	A社

[49] 個人情報保護委員会『「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ&A』Q5－35等を参照

価値（重要度）	非常に高い	高い	非常に高い
媒体・保存先	C 社 PaaS	B 社端末、C 社 PaaS	B 社端末
利用期限	雇用契約期間中	委託契約期間中	委託契約期間中

A-4-4.　STEP 4「イベント」ごとのリスクポイントの洗い出し

A-4-4-1.　「イベント」ごとのリスクポイントの洗い出し

STEP 3までの検討事項を踏まえ、以下では本ユースケースのうち、図A.4-2及び図A.4-3に示す「システム運用設計データ」の「移転・提供」及びその後の「保管」のプロセスに関して以下のようなリスクを想定することができる。データの移転・提供過程にて想定されるリスクは用いられる技術的手段により異なることが想定されるが、ここでは当該移転・提供行為が外部クラウドストレージサービス（SaaS）を利用して行われるとしてリスクを抽出している。なお、以下では、上記データの「移転・提供」が技術情報の外国への「輸出」に該当し得ることに鑑み、「関連する法制度等に係る観点」として、「機微技術管理」を新たに加えている。

対象の移転・提供事象について、4つの単位（国・地域・組織・人、システム・サービス、機器）の単位でリスクを整理することを通じて、一例として以下のようなリスクが特定され得る。

＜国・地域＞

- パーソナルデータ保護の観点については、システム運用設計データに個人に関する情報が含まれていないことを前提とすれば、非該当
- システム運用設計データが現に移転・提供される以前に、A社内で実施される輸出管理関連手続きにおいて、技術情報の提供に係る輸出管理上の懸念が認められるかどうかの確認がなされない。

＜組織・ヒト＞

- 悪意のある海外拠点のB社従業員により、USBメモリの挿入等を通じてシステム運用設計データが不正に外部に持ち出される。

＜システム・サービス＞

- A 社従業員によるクラウドストレージサービスにおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体にシステム運用設計データが開示される。
- 悪意のある第三者が A 社の業務端末と外部クラウドストレージサービスを提供するサーバとの間の通信に介入し、データを改ざんする。

＜機器＞

- 外部クラウドストレージサービスを提供するサーバがマルウェアに感染し、システム運用設計データの移転・提供に遅延が生じる。

表A-4.3「システム運用設計データ」の「移転・提供」及びその後の「保管」で想定されるリスク（例）

大分類	中分類	「システム運用設計データ」の「移転・提供」及びその後の「保管」で想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 悪意のある外部の主体がA社の利用する外部クラウドストレージサービスの脆弱性を悪用して格納されたシステム運用設計データに不正アクセスされる。 ● A社従業員によるクラウドストレージサービスにおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体にシステム運用設計データが開示される。 ● 悪意のある外部の主体がB社の保有する運用・保守用の端末に不正アクセスし、システム運用設計データに不正アクセスする。 ● 悪意のある海外拠点のB社従業員により、USBメモリの挿入等を通じてシステム運用設計データが不正に外部に持ち出される。
	完全性	● 悪意のある第三者がA社の業務端末と外部クラウドストレージサービスを提供するサーバとの間の通信に介入し、データを改ざんする。
	可用性	● 外部クラウドストレージサービスを提供するサーバがマルウェアに感染し、システム運用設計データの移転・提供に遅延が生じる。
関連する法制度等に係る観点	パーソナルデータ保護	● システム運用設計データに個人に関する情報が含まれていないことを前提とすれば、該当なし。
	知的財産（営業秘密を含む）保護	● システム運用設計データが悪意のある内外の主体（例：外部の攻撃者、B社の従業員）により不正な手段で取得され、開示、使用される。
	機微技術管理	● システム運用設計データが現に移転・提供される以前に、A社内で実施される輸出管理関連手続きにおいて、技術情報の提供に係る輸出管理上の懸念が認められるかどうかの確認がなされない。

A-4-4-2. 今後のデータ管理の高度化に向けた課題の検討

前述のフレームワーク適用プロセスからわかるように、本ユースケースでは、事業者（A社）が外部の事業者の支援を受けつつ構築した人事管理システムという汎用的なシステムの運用を、コスト削減や品質の向上等を目的として、海外に保守拠点を有する外部の事業者（B社）に委託するケースを取扱った。このような場合、多くの個人データを取扱う人事管理システムそれ

自体を保護するだけでなく、そこで取扱われる従業員に関するデータやシステムの運用に係るデータの移転・提供に係るガバナンスを確保すること等が特有の課題となる。そのような課題に対してA社及び関連する事業者が実施できる対応策として、例えば以下が挙げられる。

- B社からA社データへのアクセス状況のレビュー
  前述のとおり、B社はA社の管理する個人データを取扱うことはないとされているが、前提となる契約等の条項が継続的に遵守されていることを確実にする必要がある。例えば、委託される業務内容に個人データを用いて情報システムの不具合を再現させ検証する等の個人データを取扱い得るものが含まれていないこと、かかる条項が含まれていない場合に現にB社拠点から個人データへのアクセスが行われていないことを確認すること（例：付与されているアカウントやアクセス権限の分析、契約期間中のアクセスログのレビュー）が対処として想定される。

- B社海外拠点におけるセキュリティマネジメントの確認
  B社はA社の従業員等に関する個人データを取扱うことはないものの、システム運用設計データやシステム稼働状況データ等のA社にとって事業上の価値があるデータを自社の拠点にて取扱う。昨今、本ユースケースにおけるB社のような委託先や海外支社等において、相対的にセキュリティ管理が行き届いていないことに起因して、外部からの攻撃や内部不正、その他のヒューマンエラー等による情報漏えい等の事例が報告されている点を踏まえると、A社とB社との委託契約等においてフレームワークの適用を行う際にかかるリスクへの対応が十分になされていない場合は、A社からB社に対して自社と同等の管理水準を達成するためのより具体的な安全管理策を規定し、書面又は監査等により遵守状況を確認したりする等の施策が有用と考えられる[50]。

[50] 業務委託先等に対するセキュリティ管理策に関しては、JIS Q 27002:2014 の「15.1 供給者関係における情報セキュリティ」における各種実施策等も参照されたい。

添付B　イベントごとのリスクの洗い出しのイメージ

B-1 イベントごとの典型的なリスクの記載方法等

本章では、フレームワークの適用を行う事業者等が、自身のデータ利活用プロセスにおいて想定されるリスクを特定するにあたり、考慮することが望ましい典型的なリスクや有効な対策要件（例）を列挙する[51]。

表B-1.1　添付Bにおけるイベントごとの典型的なリスクの記載方法

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	生成・取得されるデータがネットワーク上で悪意のある内部犯行者又は外部の攻撃者に傍受され、漏えいする。	情報漏えい	暗号化等による通信経路の保護

B-2では、表B-1.1に示す様式に沿って、イベント類型（生成・取得、加工・利用、移転・提供、保管、廃棄）ごとに対象となる機能、資産の例を示したうえで、典型的なリスクを列挙する。その際、「リスク」の記述に該当する「想定されるセキュリティインシデント等（例）」に加え、特定するリスクの網羅性やスコープをより明確なものとするため、以下に概要を示す事項を併記している。

- 保護の観点
  「想定されるセキュリティインシデント等（例）」を特定する際に、考慮すべき保護の観点を提示している。かかる観点には、セキュリティの保護に関わるもの（機密性、完全性、可用性）と関連する法制度等に関わるもの（パーソナルデータ保護、知的財産（営業秘密を含む）保護等）が含まれる。
- 脅威主体の区分
  対象となるデータ利活用プロセスに対して（多くの場合ネガティブな）影響を及ぼし得る脅威の主体を以下の4つに分類している。

[51] 個々の適用ケースで特定され得るリスクはここで列挙されるものに必ずしも限定されない。

表B-1.2 脅威主体の区分（例）[52]

脅威主体の区分	概要
アドバーサリ （悪意のある主体）	サイバー資源（すなわち、電子的形態の情報、情報及び通信技術、ならびにそれらの技術によって提供される通信及び情報処理能力）に対する組織の依存を利用しようとする個人、グループ、組織、又は国家。一般的には、外部からのサイバー攻撃又は物理的な攻撃、内部犯行等が含まれる。
偶発的	日々の責務を実施する過程で必ずしも悪意のない個人が取る誤ったアクション（ヒューマンエラー等を含む）。
構造上	老化、リソースの枯渇、又は予測されたオペレーティングパラメータを超えるその他の状況に起因する、機器の故障、環境制御の失敗、又はソフトウェアの不具合。
外部環境上	組織が依存するが、組織のコントロールの範囲外である重要インフラに対する自然災害、及びそれらのインフラの故障。

フレームワークの適用主体は、サイバー攻撃等を行う悪意のある内外の主体（アドバーサリ）だけでなく、正規の従業員等によるヒューマンエラー（偶発的）や自然災害、インフラの故障等も含め、可能な限り網羅的な観点から、自身のデータ利活用プロセスに対する脅威を担いうる主体とそれによるリスクを特定することが望ましい。

- 脅威

上記区分の主体により担われ得る具体的な脅威を記載する。ここでは、脅威を洗い出すための手法の一つであるSTRIDEを基礎としつつ、生成・取得や加工・利用等に関わりうるIoT機器等の性質やアドバーサリ以外の主体による脅威も考慮した上で、追加の脅威類型（マルウェア感染、不正改造、誤使用[53]、システム等の不具合、自然災害等）を含めて提示している[54]。

[52] NIST Special Publication 800-30 Revision 1（IPA 訳）における「付録 D 脅威源 脅威事象を開始することができる脅威源の分類体系」を参照し、適宜追記等を実施

[53] 「誤使用」として、ここでは専ら、使用者に悪意のないものを指す。

[54] 経済産業省サイバーセキュリティ課「機器のサイバーセキュリティ確保のための セキュリティ検証の手引き 別冊 1 脅威分析及びセキュリティ検証の詳細解説書」における「STRIDE によって抽出されない可能性が高い」脅威の記述も踏まえ、アドバーサリ（悪意のある主体）以外の脅威主体による脅威類型を適宜追加している。

表B-1.3　STRIDEによる脅威の分類例

脅威	内容
なりすまし	コンピューターに対し、他の利用者や機器を装うこと。
改ざん	権限なしでデータを改ざんし、データの完全性を失わせること
否認	利用者が、あるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと
情報漏洩	アクセス権限を持たない個人に情報が公開されること
サービス不能	正規のユーザーがサーバやサービス等にアクセスできないこと ※DDoS攻撃やジャミングによるサービス妨害など
権限の昇格	権限のない利用者がアクセス権限を得ること

表B-1.4 本稿にて追加で定義している脅威の分類例

脅威	内容
マルウェア感染	他の機器への汚染源になる。ランサムウェア等により業務妨害を受けること
不正改造	不正（違法）なハード、ソフトウェアの改造により、内部データを抜き取り、脆弱性の要因を組み込まれること
誤使用	機器が利用者により事前に意図しない用途等で使われること
システム等の不具合	機器の故障、環境制御の失敗、又はソフトウェアの不具合が生じること
自然災害等	地震や津波、豪雨等の自然現象及び、電気、通信、給水、ガス等の外部のユーティリティの不具合によりデータ利活用プロセスに負の影響が及ぶこと

- 有効な対策要件（例）

特定されたリスクを低減するために有効と考えられる対策要件の例を、以下に示す参照文献との対応関係とともに記載している。参照文献としては、すべてのイベント類型に関連する内容を持つ「一般」と、各イベント類型にある程度特化した内容を持つものを扱う。

＜一般＞

- CPSF
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations
- データマネジメント知識体系ガイド（DMBOK） 第2版

＜生成・取得＞

- 安全なウェブサイトの作り方　改訂第7版
- NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers

＜移転・提供＞

- SP 800-47 Rev. 1 Managing the Security of Information Exchanges
- ISO/IEC 27033-1:2015 Information technology — Security techniques — Network security — Part 1: Overview and concepts

＜加工・利用＞

- AI・データの利用に関する契約ガイドライン 1.1版

＜廃棄＞

- SP 800-88 Rev. 1 Guidelines for Media Sanitization

また、保護の観点として、パーソナルデータ保護や知的財産（営業秘密を含む）保護を参照しているインシデント等に対しては、参照文献として、以下に例示する各種法令に係るガイドライン文書との対応を示している。

＜パーソナルデータ保護＞

- 個人情報の保護に関する法律についてのガイドライン（通則編）
- 個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）
- 個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）

＜知的財産（営業秘密を含む）保護＞

- 営業秘密管理指針

B-2 イベントごとのリスクの洗い出しのイメージ

本節では、表B-1.1に示した様式に沿って、イベント類型（生成・取得、加工・利用、移転・提供、保管、廃棄）ごとに対象となる機能、資産の例を示したうえで、典型的なリスクや有効な対策要件（例）を示す。

B-2-1 データの生成・取得過程におけるリスクの洗い出しのイメージ

センサーによる計測や人手による入力等によるデータの生成・取得は、データライフサイクル

の初期段階を構成しており、以降の利活用プロセスにおけるデータの信頼性を確保するうえで重要な位置を占めている。生成・取得は様々な手段で実行され得るため、実際のリスクアセスメントはその方法を具体的に特定したうえで実施することが望ましいが、以下では、様々な手法等に対して共通に適用し得るものとして、対象となる機能及び資産、想定されるリスク及び有効な対策要件(例)を示す。

＜対象となる機能＞

- フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、サイバー空間へ送る機能
- 上記のほか、オンラインシステム等への直接の入力や使用履歴の収集等により、データを生成・取得する機能

＜対象となる資産＞

- データの生成・取得に係る設備や機器(例:センサー、WEBサーバ、業務用端末)
- 上記に接続するネットワーク

表B-2.1 データの生成・取得過程におけるリスクの洗い出しのイメージ

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等(例)	脅威	有効な対策要件(例)
機密性	アドバーサリ(悪意のある主体)	生成・取得されるデータがネットワーク上で悪意のある内部犯行者又は外部の攻撃者に傍受され、漏えいする。	情報漏えい	暗号化等による通信経路の保護 通信経路、端末の挙動等の監視、対処
	アドバーサリ(悪意のある主体)	生成・取得されるデータがマルウェアに感染した機器・設備等から不正な送信先へ共有される。	情報漏えい	脆弱性対応プロセスの整備、実行 端末、ネットワーク上におけるマルウェア対策の導入 外部向き通信の監視、対処
	偶発的	データの生成・取得に係る設備や機器に不適切な設定がなされており、データが本来想定していない主体から閲覧できるようになっている。	情報漏えい	機器・サービスの初期設定及び設定等の変更管理 ユーザー、機器、サービス等に対する適切な水準の認証の実施 通信経路、端末の挙動等の監視、対処
完全性	アドバーサリ(悪意のある主体)	(特に人手のデータ入力が行われる場合) 正規ユーザーへのなりすましにより、不正確なデータが生成・取得される。	なりすまし	ユーザー、機器、サービス等に対する適切な水準の認証の実施 入力値の検証

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
	アドバーサリ（悪意のある主体）	データ生成元の機器を不正な機器によりなりすまされ、正確でないデータが生成・取得される。	なりすまし	機器等が設置された物理的環境におけるアクセス制御 機器等が設置された物理的環境の監視 通信経路、端末の挙動等の監視、対処 入力値の検証
	アドバーサリ（悪意のある主体）	稼働中のデータ生成元の機器が不正改造され、正確でないデータが生成・取得される。	不正改造	機器等の物理的耐性の強化 機器等が設置された物理的環境におけるアクセス制御 機器等が設置された物理的環境の監視
	アドバーサリ（悪意のある主体）	悪意のある従業員又は第三者の物理的な攪乱により、データ生成元の機器から正確でないデータが生成・取得される。	なりすまし	入力値の検証 機器等が設置された物理的環境の監視
	アドバーサリ（悪意のある主体）	正規の機器から生成・取得されたデータがネットワーク上で傍受され、改ざんされる。	改ざん	暗号化等による通信経路の保護 データの完全性、真正性保護
	構造上	品質や信頼性の低い IoT 機器がネットワーク接続され、故障や正確でないデータの送信、想定していない通信先へのデータ送信等が発生する。	システム等の不具合	運用時の機器・システムの真正性確認
	偶発的	（特に人手のデータ入力が行われる場合）正規ユーザーの誤入力により、不正確なデータが生成・取得される。	誤使用	入力値の検証
可用性	アドバーサリ（悪意のある主体）	サービス妨害攻撃等によりデータの生成・取得に係る設備や機器が一時的に停止する。	サービス妨害	機器、通信機器、回線等の冗長化及びバックアップの確保 通信経路、端末の挙動等の監視、対処
	アドバーサリ（悪意のある主体）	センサー等の設備や機器がマルウェアに感染して稼働が停止し、データを生成・取得できない。	マルウェア感染	脆弱性対応プロセスの整備、実行 端末、ネットワーク上におけるマルウェア対策の導入
	構造上	データの生成・取得に係る設備や機器に不具合が生じ、処理が一時的に停止する。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
	環境上	地震や津波等の自然災害によりデータの生成・取得に係る設備や機器に被害が生じ、処理が一時的に停止する。	自然災害等	機器、通信機器、回線等の冗長化及びバックアップの確保

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等(例)	脅威	有効な対策要件(例)
パーソナルデータ保護	偶発的	データ取得先の組織が、生成・取得するデータの利用目的をデータ元の個人に対して明確に示さしていない、又は利用の実態と対応して提示していない。	不十分なコンプライアンス	データ取得時の利用目的等の提示
	偶発的	データ取得先の組織が、偽り等の不正の手段により個人情報を取得している。	不十分なコンプライアンス	正当な手段によるデータの取得
知的財産(営業秘密を含む)保護	アドバーサリ(悪意のある主体)	悪意のある従業員又は退職者を含む第三者が、紙等で管理されている営業秘密を不正な方法(窃取、詐欺、強迫、その他の不正な手段)でデータとして取得している。	情報漏えい	秘密管理性を確保した営業秘密等の管理
	偶発的	他社から転職者等を受け入れる場合、その転職者が持ち込むデータの中に、他社の営業秘密等が含まれる等、意図せぬ形で他社の営業秘密等を取得してしまう。	不十分なコンプライアンス	自組織及び委託先等における要員のセキュリティ確保

B-2-2 データの加工・利用過程におけるリスクの洗い出しのイメージ

データは生成・取得して保管するだけでは必ずしも付加価値を生み出すわけではなく、何らかの加工・利用を通じて付加価値をもたらす。他方、加工・利用過程に何らかの障害が発生すれば、データの信頼性、ならびにデータの利活用から得られるはずだったメリットを大きく損なわせる可能性があることから、他のイベントと同様、リスクを正しく認識し、適切に対処することが重要である。以下にて、加工・利用過程の対象となる機能及び資産、想定されるリスク及び有効な対策要件(例)を示す。

＜対象となる機能＞

・ データを加工・分析する機能

＜対象となる資産＞

・ データの加工・利用に係る設備や機器(例:サーバ、業務用端末、それらにインストールされたソフトウェア資産)

表B-2.2 データの加工・利用過程におけるリスクの洗い出しのイメージ

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等(例)	脅威	有効な対策要件(例)
機密性	アドバーサリ(悪意のある主体)	加工・利用過程において、悪意のある内外の主体により対象となるデータの全部又は一部が正当な権限なく参照され、自社又は他社の機密データが特定される。	情報漏えい	暗号化等による加工・利用過程の保護

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
	偶発的	アプリケーションや DB 等におけるアクセス制御等の設定ミスにより本来保護が必要なデータが外部から閲覧可能となってしまう。	情報漏えい	最小権限の原則による権限の割り当て
				機器・サービスの初期設定及び設定等の変更管理
完全性	アドバーサリ（悪意のある主体）	悪意のある内外の主体によりアプリケーションが改ざんされ、データの処理にあたって不正な処理が行われる	改ざん	ユーザー、機器、サービス等に対する適切な水準の認証の実施
				最小権限の原則による権限の割り当て
				継続的なアプリケーションのセキュリティ管理
	アドバーサリ（悪意のある主体）	悪意のある内外の主体により意図的に加工・利用の結果として生じるデータの全体又は一部が改ざん又は削除される。	改ざん	適切な要員、サービスの選定
				自組織及び委託先等における要員のセキュリティ確保
				通信経路、端末の挙動等の監視、対処
	偶発的	正規の従業員が悪意なく誤って加工・利用の結果として生じるデータの全体又は一部を変更又は削除する。	誤使用	適切な要員、サービスの選定
				自組織及び委託先等における要員のセキュリティ確保
				機器、通信機器、回線等の冗長化及びバックアップの確保
	構造上	データの加工・利用を行う設備や機器の一部に障害や誤動作が発生し、集約結果の完全性が損なわれる。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
可用性	アドバーサリ（悪意のある主体）	サービス妨害攻撃、マルウェア感染等によりデータの加工・利用に係る設備や機器が一時的に停止する。	サービス妨害	機器、通信機器、回線等の冗長化及びバックアップの確保
			マルウェア感染	脆弱性対応プロセスの整備、実行
				入力値の検証
				端末、ネットワーク上におけるマルウェア対策の導入
	構造上	過度の処理リクエスト等によりデータの加工・利用に係る設備や機器に不具合が生じ、処理が一時的に停止する。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
	環境上	地震や津波等の自然災害によりデータの加工・利用に係る設備や機器に被害が生じ、処理が一時的に停止する。	自然災害等	機器、通信機器、回線等の冗長化及びバックアップの確保
パーソナルデータ保護	アドバーサリ（悪意のある主体）	従業員により必要な手続きを踏むことなく、事前にデータ取得元の個人へと通知した目的とは異なる目的でデータが利用される。	不十分なコンプライアンス	利用目的等による加工・利用の制限
	アドバーサリ（悪意のある主体）	元の個人情報の本人を識別する目的で、仮名加工情報や匿名加工情報を他の情報と照合する。	不十分なコンプライアンス	仮名加工情報や匿名加工情報に対する識別行為の禁止

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
	偶発的	個人情報を仮名加工情報や匿名加工情報にする際に行う加工が法令等により定められる要求を満たした方法で適切に行われない。	不十分なコンプライアンス	仮名加工情報、匿名加工情報の適正な加工
知的財産（営業秘密を含む）保護	アドバーサリ（悪意のある主体）	正当な手段によりデータを取得した悪意のある内外の主体(退職者を含む)により、不正の利益を得る目的又は権利元に損害を加える目的でデータが使用される。	不十分なコンプライアンス	自組織及び委託先等における要員のセキュリティ確保
				通信経路、端末の挙動等の監視、対処
	偶発的	従業員により必要な手続きを踏むことなく、事前に提供元の組織人と合意した利用条件(利用目的、利用権限等)とは異なる方法でデータが利用される。	不十分なコンプライアンス	利用目的等による加工・利用の制限

B-2-3 データの移転・提供過程におけるリスクの洗い出しのイメージ

近時、ますます多くのデータが生成・取得、加工・利用される中で、データに由来するメリットを最大限享受するために、組織内あるいは複数の組織間でデータを共有（移転・提供）することの重要性が認識されている。一方で、移転・提供が主に行われるネットワーク上は、加工・利用や保管の過程とは異なるリスクや脅威が想定される場でもあり、それらを正しく認識し、対処することが重要である。移転・提供過程の対象となる機能及び資産、想定されるリスク及び有効な対策要件（例）を以下に示す。

＜対象となる機能＞

- データを送受信する機能

＜対象となる資産＞

- データの移転・提供に係る設備や機器(例：ネットワーク、ネットワーク機器、サーバ、業務用端末)

表B-2.3 データの移転・提供過程におけるリスクの洗い出しのイメージ

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	データが移転・提供に係るネットワーク上で悪意のある第三者に傍受され、漏えいする。	情報漏えい	暗号化等による通信経路の保護
	アドバーサリ（悪意のある主体）	データがマルウェアに感染した機器・設備等から不正な送信先へ移転・提供される。	マルウェア感染	脆弱性対応プロセスの整備、実行
				端末、ネットワーク上におけるマルウェア対策の導入

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
			情報漏えい	外部向き通信の監視、対処
	アドバーサリ（悪意のある主体）	データが正規の送信先になりすました不正な送信先へ移転・提供される。	なりすまし	暗号化等による通信経路の保護
				通信経路、端末の挙動等の監視、対処
	偶発的	データが悪意のない正規の利用者により本来想定されていない送信先へ移転・提供される。	情報漏えい	通信経路、端末の挙動等の監視、対処
				外部向き通信の監視、対処
完全性	アドバーサリ（悪意のある主体）	データが移転・提供に係るネットワーク上で悪意のある第三者に傍受され、改ざんされる。	改ざん	暗号化等による通信経路の保護
				データの完全性、真正性保護
可用性	アドバーサリ（悪意のある主体）	サービス妨害攻撃等によりデータの移転・提供に係る設備や機器が一時的に停止する。	サービス妨害	機器、通信機器、回線等の冗長化及びバックアップの確保
				通信経路、端末の挙動等の監視、対処
	アドバーサリ（悪意のある主体）	データの移転・提供に係る設備や機器がマルウェアに感染し、データを移転・提供できない。	マルウェア感染	脆弱性対応プロセスの整備、実行
				端末、ネットワーク上におけるマルウェア対策の導入
	構造上	データの移転・提供に係る設備や機器に不具合が生じ、処理が一時的に停止する。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
	環境上	地震や津波等の自然災害によりデータの移転・提供に係る設備や機器に被害が生じ、処理が一時的に停止する。	自然災害等	機器、通信機器、回線等の冗長化及びバックアップの確保
パーソナルデータ保護	偶発的	法令に基づく場合等の特定の事由に該当しない場合に、事前の本人同意取得又はオプトアウトに係る手続等の実施なしに、個人データを第三者に提供する。	不十分なコンプライアンス	第三者提供に係る正当な根拠の確保
	偶発的	個人データの第三者提供を行う際に、提供を行う側、提供を受ける側のいずれか又は双方において記録の作成、確認の実施が行われない。	不十分なコンプライアンス	第三者提供時の記録・確認の実施
	偶発的	個人データを外国にある第三者提供に提供する際、本人同意の取得、適切な情報提供等の遵守すべき手続きが実施されない。	不十分なコンプライアンス	外国にある第三者へのデータ提供時に必要な手続きの実施
知的財産（営業秘密を含む）保護	アドバーサリ（悪意のある主体）	悪意のある従業員又は退職者を含む第三者が、不正取得行為(窃取、詐欺、強迫、その他の不正な手段)により取得した営業秘密を移転・提供する。	不十分なコンプライアンス	秘密管理性を確保した営業秘密等の管理

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
	アドバーサリ（悪意のある主体）	不正取得行為が介在したことを、移転・提供先が故意にもしくは重過失により知らないで営業秘密を取得する。	不十分なコンプライアンス	秘密管理性を確保した営業秘密等の管理
	偶発的	移転・提供元が不正取得行為の介在について善意・無重過失で営業秘密を取得していても、取得後に不正取得行為の介在について悪意・重過失に転じ、当該営業秘密を第三者に開示する。	不十分なコンプライアンス	秘密管理性を確保した営業秘密等の管理
	アドバーサリ（悪意のある主体）	移転・提供元から営業秘密を示された場合、不正の利益を得る目的で、又は、その保有者に損害を加える目的で、その営業秘密を開示する。	不十分なコンプライアンス	秘密管理性を確保した営業秘密等の管理
	偶発的	従業員又は退職者が、自社の管理する営業秘密をそうとは認識せずに外部の事業者等に開示する。	不十分なコンプライアンス	営業秘密を企業内外で共有する場合の秘密管理性の確保

B-2-4 データの保管過程におけるリスクの洗い出しのイメージ

データは、ライフサイクルの様々な段階において、外部サービス（クラウドストレージを含む）やネットワーク接続されたストレージ機器、クライアントのハードディスク、USBメモリのような可搬媒体、機器の一時記憶領域等に保管され得る。データの利活用が活発に行われ、蓄積されるデータの種類や量がますます増加する中で、大規模なデータストレージ及び保管されるデータはますます重要な保護対象となっている。かかる過程の対象となる機能及び資産、想定されるリスク及び有効な対策要件（例）を以下に示す。

＜対象となる機能＞

・ データを保管する機能

＜対象となる資産＞

・ 各種データ処理に関連しデータを保管し得る設備や機器(例：サーバ、業務用端末、長期保存用の媒体)

表B-2.4 データの保管過程におけるリスクの洗い出しのイメージ

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	外部の攻撃者により、弱いパスワード、ソフトウェアの脆弱性等が原因でデータを保管する機器・システムが外	情報漏えい	ユーザー、機器、サービス等に対する適切な水準の認証の実施
				最小権限の原則による権限の割り当て

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
		部から不正アクセスされ、データが漏えいする。		保管されたデータ等の暗号化
				脆弱性対応プロセスの整備、実行
				外部向き通信の監視、対処
	アドバーサリ（悪意のある主体）	悪意のある従業員や退職予定者、外部委託先の従業員等により、データを保管する機器・システムがアクセスされ、保護すべきデータが漏えいする。	情報漏えい	自組織及び委託先等における要員のセキュリティ確保
				機器等が設置された物理的環境の監視
				保管されたデータ等の暗号化
				通信経路、端末の挙動等の監視、対処
	アドバーサリ（悪意のある主体）	外部の攻撃者や悪意のある内外の従業員等により、データを保管する媒体（例：端末内の HDD や SSD、USB メモリや CD、DVD 等の可搬媒体）が盗難されたり、不正に読み出されたりする。	情報漏えい	機器等が設置された物理的環境におけるアクセス制御
				保管されたデータ等の暗号化
				機器等が設置された物理的環境の監視
	偶発的	データの保管に係る設備や機器に不適切な設定がなされており、保管データが本来想定していない主体から閲覧できるようになっている。	情報漏えい	機器・サービスの初期設定及び設定等の変更管理
				保管されたデータ等の暗号化
				通信経路、端末の挙動等の監視、対処
		国内又は国外の司法機関等からの求めに応じて共同利用しているサーバ等の押収がなされる際、十分な保護が必要なデータが開示される。	情報漏えい	データを処理、保管するサーバ等設備の所在地の確認
完全性	アドバーサリ（悪意のある主体）	悪意のある内外の主体により意図的に保管データの全体又は一部が改ざん又は削除される。	改ざん	ユーザー、機器、サービス等に対する適切な水準の認証の実施
				最小権限の原則による権限の割り当て
				データの完全性、真正性保護
	アドバーサリ（悪意のある主体）	マルウェア感染等により保管データの全体又は一部が改ざん又は削除、破壊される。	マルウェア感染	機器・サービスの初期設定及び設定等の変更管理
				脆弱性対応プロセスの整備、実行
				端末、ネットワーク上におけるマルウェア対策の導入
	偶発的	正規の従業員（自社又は外部委託先等）が悪意なく誤って保管データの全体又は一部を変更又は削除する。	非意図的な誤使用	機器、通信機器、回線等の冗長化及びバックアップの確保
	構造上	外部委託先等が運用するものを含め、データを保管する設備や機器の一部に障害や誤動作が発生し、保管データの全体又は一部が損なわれる。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
可用性	アドバーサリ（悪意のある主体）	サービス妨害攻撃、マルウェア感染等によりデータの加工・利用に係る設備や機器が一時的に停止する。	サービス妨害	機器、通信機器、回線等の冗長化及びバックアップの確保
			マルウェア感染	脆弱性対応プロセスの整備、実行
				端末、ネットワーク上におけるマルウェア対策の導入

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
	構造上	外部委託先等が運用するものを含め、データを保管する設備や機器の一部に障害や誤動作が発生し、処理が一時的に停止する。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保
	環境上	地震や津波等の自然災害によりデータの保管に係る設備や機器に被害が生じ、処理が一時的に停止する。	自然災害等	機器、通信機器、回線等の冗長化及びバックアップの確保
パーソナルデータ保護	偶発的	事業者が保有し、利用する個人データの内容が事実でないという理由で、本人から訂正や削除を求められた際の対応が十分に行われない。	不十分なコンプライアンス	本人からの求めに応じた保有個人データの訂正・利用停止等
	偶発的	事業者が保管する個人データに対して、適切な安全管理策(従業員の監督、委託先の監督を含む)が講じられていない。	不十分なコンプライアンス	個人データに対する安全管理措置の実施
	偶発的	既に必ずしも利用しなくてもよい状況となっている個人データが不必要に保持又は利用されている。	不十分なコンプライアンス	データの遅滞ない消去
知的財産（営業秘密を含む）保護	アドバーサリ（悪意のある主体）	悪意のある外部の攻撃者、従業員又は退職予定者等により、営業秘密として管理される保管データがアクセスされ、データが外部へ漏えいする。	情報漏えい	ユーザー、機器、サービス等に対する適切な水準の認証の実施 最小権限の原則による権限の割り当て 通信経路、端末の挙動等の監視、対処
	偶発的	他社より提供を受けた営業秘密情報等について、利用期限が過ぎているにもかかわらず、別途許可等を得ることなく保管されたままとなっている。	不十分なコンプライアンス	自組織及び委託先等における要員のセキュリティ確保 データの遅滞ない消去
	偶発的	自社の保有する知的財産等に外部の知的財産等が混入(コンタミネーション)し、他社の知的財産等情報を不用意に使用・開示してしまう。	不十分なコンプライアンス	自組織及び委託先等における要員のセキュリティ確保 他社の秘密情報等の分離管理

B-2-5 データの廃棄過程におけるリスクの洗い出しのイメージ

様々な目的で利活用されたデータは、データの上書きや媒体の物理破壊、ディスク全体の暗号化等の適切な方法により廃棄され、復元できない状況とされることでそのライフサイクルを終える。かかる過程の対象となる機能及び資産、想定されるリスク及び有効な対策要件（例）を以下に示す。

＜対象となる機能＞

－

＜対象となる資産＞

・ 各種データ処理に関連しデータを保管し得る設備や機器(例：サーバ、業務用端末における記憶媒体)

表B-2.5 データの廃棄過程におけるリスクの洗い出しのイメージ

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	外部の攻撃者や悪意のある従業員等により、事業者が利用を終了し、十分でない方法により廃棄されたデータが不正に復元される。	情報漏えい	適切な要員、サービスの選定 適切な方法によるデータ及び媒体の廃棄
	アドバーサリ（悪意のある主体）	悪意のある従業員又はデータの廃棄を委託された事業者の従業員により、廃棄を予定していたデータが外部に開示される。	情報漏えい	適切な要員、サービスの選定 データ及び媒体廃棄の履行確認
	偶発的	廃棄作業を委託する場合に、委託先が確実に削除又は廃棄したことについて証明書等を取得していない等の原因で事実を確認することができない	不十分なコンプライアンス	データ及び媒体廃棄の履行確認
完全性	偶発的	記憶媒体等を処分する際に、本来は廃棄すべきでないデータまで廃棄してしまう。	誤使用	機器、通信機器、回線等の冗長化及びバックアップの確保

B-2-6 対策要件（例）と参照ガイドライン

B-2-1からB-2-5にて示した有効な対策要件（例）について、データの信頼性確保に係る取組を進めていく際の参考情報として、各種参照ガイドラインとの対応関係を以下に示す。なお、有効な対策要件（例）は、適用主体においてリスク管理のプロセスが一とおり整備されていることを前提に、リスク対応の段階において実施すべき「防御」や「検知」に係る主な対策要件を記載している。

表B-2.6 対策要件（例）と参照ガイドライン

対策	適用対象イベント	参照ガイドライン
適切な要員、サービスの選定	加工・利用、廃棄	・CPSF Ver.1.0 CPS.SC-4, CPS.SC-5 ・ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.2.1 ・NIST SP 800-53 Rev. 5 PS-7, SR-5, SR-6 ＜より詳細なガイドライン＞ ・AI・データの利用に関する契約ガイドライン データ編 第5．2（1），(9)，第6．4（1），(5)

対策	適用対象イベント	参照ガイドライン
		・NIST SP 800-88 Rev. 1 4.7 Verify Methods
自組織及び委託先等における要員のセキュリティ確保	加工・利用、保管	・CPSF Ver.1.0 CPS.GV-1, CPS.SC-5, CPS.AT-1, CPS.AT-2 ・ISO/IEC 27001:2013 A.6.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.3.1, A.15.1.1 ・NIST SP 800-53 Rev. 5 AT-1, AT-2, AT-3, AT-4, PS-7, SA-9, SA-16, SA-21 ・DAMA-DMBoK(第7章) 5.4 アウトソーシングにおけるデータセキュリティ ＜より詳細なガイドライン＞ ・AI・データの利用に関する契約ガイドライン データ編 第5. 2 (1) , (9), 第6. 4(1) , (5)
ユーザー、機器、サービス等に対する適切な水準の認証の実施	生成、取得、移転・提供、加工・利用、保管	・CPSF Ver.1.0 CPS.AC-1, AC-4, AC-9 ・ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 ・NIST SP 800-53 Rev. 5 AC-2, AC-3, AC-7, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 ・DAMA-DMBoK(第7章) 3.3 アイデンティティ管理技術 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・NISTIR 8259A Logical Access to Interfaces ・安全なウェブサイトの作り方 改訂第7版 1.4 セッション管理の不備、1.11 アクセス制御や認可制御の欠落、2.5 パスワードに関する対策 ・AI・データの利用に関する契約ガイドライン データ編 第5. 2 (1) , (9), 第6. 4 (1), (5) ・ISO/IEC 27035-1:2015 8.4 Identification and authentication ・NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan
最小権限の原則による権限の割り当て及び認可の実施	加工・利用、保管	・CPSF Ver.1.0 CPS.AC-5, CPS.AC-9 ・ISO/IEC 27001:2013 A.6.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 ・NIST SP 800-53 Rev. 5 AC-1, AC-3, AC5, AC-6, AC-24 ・DAMA-DMBoK(第7章) 2.3.5.3 データセキュリティの管理と保守 ＜より詳細なガイドライン＞ ・AI・データの利用に関する契約ガイドライン データ編 第5. 2 (1) , (9) , 第6. 4(1) , (5)
暗号化等による通信経路の保護	生成、取得、移転・提供	・CPSF Ver.1.0 DS-23 ・ISO/IEC 27001:2013 A.13.2.1, A.13.2.3 ・NIST SP 800-53 Rev. 5 CA-3, SC-8, SC-11, SC-12, SC-13

対策	適用対象イベント	参照ガイドライン
		・DAMA-DMBoK(第7章) 3.2 HTTPS ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・NISTIR 8259A Data Protection ・安全なウェブサイトの作り方 改訂第7版 2.3 ネットワーク盗聴への対策 ・ISO/IEC 27035-1:2015 7.2.2 Information on current/planned networking, 8.8 Cryptographic based services ・NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan
保管されたデータ等の暗号化	保管	・CPSF Ver.1.0 DS-3 ・ISO/IEC 27001:2013 A.10.1.1 ・NIST SP 800-53 Rev. 5 SC-28
暗号化等によるデータの加工・利用過程の保護	加工・利用	-
データの完全性、真正性保護	移転・提供、保管	・CPSF Ver.1.0 CPS.DS-11, CPS.CM-4CPS.DS-10, CPS.CM-3 ・ISO/IEC 27001:2013 A.13.2.3, A.14.1.2, A.14.1.3A.12.2.1, A.12.5.1, A.14.2.4 ・NIST SP 800-53 Rev. 5 SC-16, SI-7SI-3, SI-7 ・DAMA-DMBoK(第7章) 2.3.5.3 データセキュリティの管理と保守3.1 ウイルス対策ソフトウェア/セキュリティソフトウェア ＜より詳細なガイドライン＞ ・ISO/IEC 27035-1:2015 7.2.2 8.8 Cryptographic based services ・NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan
適切な方法によるデータ及び媒体の廃棄	廃棄	・CPSF Ver.1.0 CPS.DS-6, CPS.IP-6 ・ISO/IEC 27001:2013 A.8.3.2, A.11.2.7 ・NIST SP 800-53 Rev. 5 MP-6 ・DAMA-DMBoK(第7章) 4.7 ドキュメントのサニタイズ ＜より詳細なガイドライン＞ ・NIST SP 800-88 Rev. 1 4 Information Sanitization and Disposition Decision Making
データ及び媒体廃棄の履行確認	廃棄	・ISO/IEC 27001:2013 A.8.3.2, A.11.2.7 ・NIST SP 800-53 Rev. 5 MP-6

対策	適用対象イベント	参照ガイドライン
		＜より詳細なガイドライン＞ ・NIST SP 800-88 Rev. 1 4.7 Verify Methods, 4.8 Documentation
機器・サービスの初期設定及び設定等の変更管理	生成、取得、保管	・CPSF Ver.1.0 CPS.AM-1, IP-1, IP-2, .PT-2 ・ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.14.2.2, A.14.2.3, A.14.2.4 ・NIST SP 800-53 Rev. 5 CM-2, CM-7, CM-8, CM-11, PE-20 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・NISTIR 8259A Device Identification, Device Configuration ・NISTIR 8259B Documentation, Education and Awareness
運用時の機器・システムの真正性確認	生成、取得	・CPSF Ver.1.0 CPS.DS-13 ・ISO/IEC 27001:2013 A.11.2.4 ・NIST SP 800-53 Rev. 5 SA-10, SI-7
継続的なアプリケーションのセキュリティ管理	加工・利用、移転・提供	・CPSF Ver.1.0 CPS.DS-10, CPS.DS-13, CPS.IP-2, CPS.MA-1 CPS.CM-3 ・ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.12.6.1, A.14.2.4, A.14.2.5 ・NIST SP 800-53 Rev. 5 CM-2, CM-5, SI-3, SI-7 ・DAMA-DMBoK(第7章) 3.1 ウイルス対策ソフトウェア/セキュリティソフトウェア ＜より詳細なガイドライン＞ ・AI・データの利用に関する契約ガイドライン データ編 第5. 2 (9), 第6. 4 (5) ・ISO/IEC 27035-1:2015 ・NIST SP 800-47 Rev.1 3.2.2 Step 2: Execute the Implementation Plan, 3.3 Maintaining the Information Exchange
端末、ネットワーク上におけるマルウェア対策の導入	生成、取得、移転・提供、加工・利用、保管	・CPSF Ver.1.0 CPS.DS-10, CPS.CM-3 ・ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.2.4 ・NIST SP 800-53 Rev. 5 SI-3, SI-7 ・DAMA-DMBoK(第7章) 3.1 ウイルス対策ソフトウェア/セキュリティソフトウェア ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・NISTIR 8259A Cybersecurity State Awareness ・NISTIR 8259B Information and Query Reception

対策	適用対象イベント	参照ガイドライン
		・安全なウェブサイトの作り方 改訂第7版 2.1.1 OS やソフトウェアの脆弱性情報を継続的に入手し、脆弱性への対処を行う、2.6 WAF によるウェブアプリケーションの保護 ・AI・データの利用に関する契約ガイドライン データ編 第5．2 (9), 第6．4 (5)
脆弱性対応プロセスの整備、実行	生成、取得、移転・提供、加工・利用、保管	・CPSF Ver.1.0 CPS.RA-1, CPS.RA-2, CPS.IP-10, CPS.MA-1, CPS.CM-7 ・ISO/IEC 27001:2013 A.6.1.4, A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.3 ・NIST SP 800-53 Rev. 5 CA-2, CA-7, CA-8, RA-3, RA-5, SI-2, SI-4, SI-5 ・DAMA-DMBoK(第7章) 4.2 セキュリティパッチの即時適用 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 4, Activity 5, Activity 6 ・NISTIR 8259A Device Configuration, Software Update ・NISTIR 8259B Information Dissemination ・安全なウェブサイトの作り方 改訂第7版 2.1.1 OS やソフトウェアの脆弱性情報を継続的に入手し、脆弱性への対処を行う ・AI・データの利用に関する契約ガイドライン データ編 第5．2 (4) , (9) , 第6．4 (5) ・ISO/IEC 27035-1:2015 8.2.5 Evaluating network security, 8.3 Technical vulnerability management ・NIST SP 800-47 Rev.1 3.3 Maintaining the Information Exchange
機器等が設置された物理的環境におけるアクセス制御	生成、取得、保管	・CPSF Ver.1.0 CPS.AC-2 ・ISO/IEC 27001:2013 A.11.1.2, A.11.1.3, A.11.2.1, A.11.2.6, A.11.2.8 ・NIST SP 800-53 Rev. 5 PE-2, PE-3, PE-4, PE-5 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3
機器等が設置された物理的環境の監視	生成、取得、保管	・CPSF Ver.1.0 CM-2 ・ISO/IEC 27001:2013 A.11.1.2, A.11.2.5, A.11.2.6 ・NIST SP 800-53 Rev. 5 CA-7, PE-3, PE-6, PE-8, PE-20 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3
機器等の物理的耐性の強化	生成、取得	・CPSF Ver.1.0 CPS.DS-8 ・ISO/IEC 27001:2013 A.8.2.3, A.10.1.2, A.11.1.4, A.11.1.5, A.11.2.1

対策	適用対象イベント	参照ガイドライン
		・NIST SP 800-53 Rev. 5 SR-9, SR-11 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3
ネットワークの分離等によるデータフローの制御	移転・提供	・CPSF Ver.1.0 CPS.AM-4, CPS.AC-7, CPS.CM-1 ・ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 ・NIST SP 800-53 Rev. 5 AC-4, CA-3, CA-9, SC-7 ・DAMA-DMBoK(第7章) 3.5 ファイアウォール（予防） ＜より詳細なガイドライン＞ ・ISO/IEC 27035-1:2015 8.2.5 Evaluating network security, 8.3 Technical vulnerability management ・NIST SP 800-47 Rev.1 3.3 Maintaining the Information Exchange
通信経路、端末の挙動等の監視、対処	生成、取得、移転・提供、加工・利用	・CPSF Ver.1.0 CM-1, CM-5, CM-6 ・ISO/IEC 27001:2013 A.12.4.1, A.12.4.2 ・NIST SP 800-53 Rev. 5 AU-12, AU-13, AU-14, CA-7, PE-21, SC-7, SI-4 ・DAMA-DMBoK(第7章) 2.3.5.3 データセキュリティの管理と保守、3.4 侵入検知と防止ソフトウェア、3.5 ファイアウォール ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・NISTIR 8259A Cybersecurity State Awareness ・NISTIR 8259B Information and Query Reception ・安全なウェブサイトの作り方 改訂第7版 2.6 WAFによるウェブアプリケーションの保護 ・AI・データの利用に関する契約ガイドライン データ編 第5. 2 (1) , (9) , 第6. 4(1) , (5) ・ISO/IEC 27035-1:2015 8.2.4 Network monitoring, 8.5 Network audit logging and monitoring ・NIST SP 800-47 Rev.1 3.3.3 Maintaining the Information Exchange
入力値の検証	生成、取得、加工・利用	・CPSF Ver.1.0 CPS.CM-3 ・ISO/IEC 27001:2013 A.12.2.1 ・NIST SP 800-53 Rev. 5 SI-10 ＜より詳細なガイドライン＞

対策	適用対象イベント	参照ガイドライン
		・NISTIR 8259 Activity 3 ・安全なウェブサイトの作り方 改訂第7版 1.1 SQL インジェクション、1.2 OS コマンド・インジェクション、1.3 パス名パラメータの未チェック／ディレクトリ・トラバーサル、1.10 バッファオーバーフロー、2.6 WAF によるウェブアプリケーションの保護プリケーションの保護 ・AI・データの利用に関する契約ガイドライン データ編 第5. 2 (1) , (9) , 第6 4(1) , (5)
外部向き通信の監視、対処	生成、取得、移転・提供、加工・利用、保管	・CPSF Ver.1.0 CPS.DS-9 ・ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.13.1.1, A.13.2.1 ・NIST SP 800-53 Rev. 5 AC-4, SC-7, SI-4 ・DAMA-DMBoK(第7章) 2.3.5.1 機密レベルの割り当て、2.3.5.2 規制対象カテゴリの割り当て、2.3.5.3 データセキュリティの管理と保守、3.6 メタデータの追跡 ＜より詳細なガイドライン＞ ・NISTIR 8259 Activity 3 ・安全なウェブサイトの作り方 改訂第7版 2.6 WAFによるウェブアプリケーションの保護 ・AI・データの利用に関する契約ガイドライン データ編 第5. 2 (1) , (9) , 第6. 4(1), (5)
データ取得時の利用目的等の提示	生成、取得	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-1-1 利用目的の特定, 3-1-2 利用目的の変更, 3-3-2 要配慮個人情報の取得, 3-3-3 利用目的の通知又は公表, 3-3-4 直接書面等による取得, 3-3-5 利用目的の通知等をしなくてよい場合
正当な手段によるデータの取得	生成・取得	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-3-1 適正取得（法第17条第1項関係）
第三者提供に係る正当な根拠の確保	移転・提供	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-4-1 第三者提供の制限の原則（法第 23 条第 1 項関係）, 3-4-2 オプトアウトによる第三者提供（法第 23 条第 2 項～第 4 項関係）, 3-4-3 第三者に該当しない場合（法第 23 条第 5 項・第 6 項関係）, 3-4-4 外国にある第三者への提供の制限（法第 24 条関係） ・個人情報保護法ガイドライン（外国にある第三者への提供編）全般
第三者提供時の記録・確認の実施	移転・提供	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-4-5 第三者提供に係る記録の作成等（法第 25 条関係）, 3-4-6 第三者提供を受ける際の確認等（法第 26 条関係）

対策	適用対象イベント	参照ガイドライン
		・個人情報保護法ガイドライン（第三者提供時の確認・記録義務編）全般
外国にある第三者へのデータ提供時に必要な手続きの実施	移転・提供	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-4-4 外国にある第三者への提供の制限（法第24条関係） ・個人情報保護法ガイドライン（外国にある第三者への提供編） 全般
仮名加工情報、匿名加工情報に対する識別行為の禁止	加工・利用	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-1-3 利用目的による制限（法第16条第1項関係）, 3-1-4 事業の承継（法第16条第2項関係）, 3-1-5 利用目的による制限の例外（法第16条第3項関係） ・個人情報の保護に関する法律についてのガイドライン （匿名加工情報編） 3-6 識別行為の禁止（法第 36 条第 5 項、第 38 条関係）
仮名加工情報、匿名加工情報の適正な加工	加工・利用	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編）2-8　匿名加工情報（法第2条第9項関係） ・個人情報の保護に関する法律についてのガイドライン （匿名加工情報編） 3-2 匿名加工情報の適正な加工（法第 36 条第 1 項関係
本人からの求めに応じた保有個人データの訂正・利用停止等	保管	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-5-3 保有個人データの訂正等（法第29条関係）, 3-5-4 保有個人データの利用停止等（法第30条関係）, 3-5-5 理由の説明（法第31条関係）, 3-5-6 開示等の請求等に応じる手続（法第32条関係）
個人データに対する安全管理措置の実施	保管	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編）3-3-2 安全管理措置（法第20条関係）, 3-3-3 従業者の監督（法第21条関係）, 3-3-4 委託先の監督（法第22条関係）
データの遅滞ない消去	保管	＜より詳細なガイドライン＞ ・個人情報保護法ガイドライン（通則編） 3-3-1 データ内容の正確性の確保等（法第19条関係）
秘密管理性を確保した営業秘密等の管理	生成、取得、移転・提供	＜より詳細なガイドライン＞ ・営業秘密管理指針 2. 秘密管理性について（2）必要な秘密管理措置の程度＜
営業秘密を企業内外で共有する場	移転・提供	＜より詳細なガイドライン＞

対策	適用対象イベント	参照ガイドライン
合の秘密管理性の確保		・営業秘密管理指針 2. 秘密管理性について(4)営業秘密を企業内外で共有する場合の秘密管理性の考え方
他社の秘密情報等の分離管理	保管	＜より詳細なガイドライン＞ ・営業秘密管理指針 2. 秘密管理性について(4)営業秘密を企業内外で共有する場合の秘密管理性の考え方
データを処理、保管するサーバ等設備の所在地の確認	保管	-

1625

別紙6

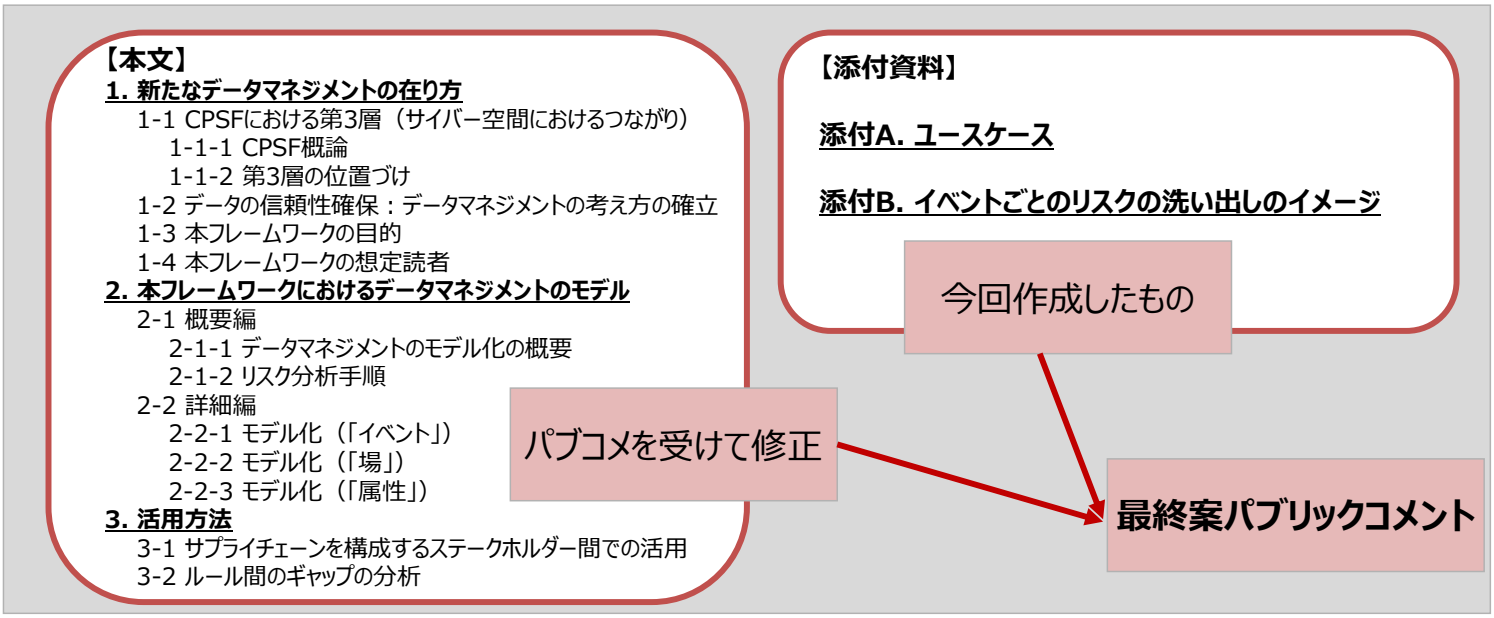
協調的なデータ利活用に向けた
データマネジメント・フレームワーク
～データによる価値創造の信頼性確保に向けた新たなアプローチ
（概要）

第3層タスクフォースの位置づけ

- 第3層TFにおいては**データが信頼性の基点**
  - Society 5.0において、サイバー空間におけるつながりが展開される場が第3層であり、そこでは物理特性に依存しないデータが付加価値を創造（バリュークリエイション）している。
  - データは基本的にシステムや組織に対して中立性を持つものであり、それが求められる規範等に則って適切に扱われることによって、自由に流通・活用される。
- データのライフサイクルには**様々な主体が関与**
  - 関与した主体による不適切な措置によって誤ったデータが流通し活用されることになれば、有害な結果をもたらすことにもつながりかねない。
- **データのライフサイクルは第3層の中に閉じるものではない。**
  - サイバー空間から発信されたIoTシステムへの動作指令が誤った内容であるならば、第2層における“転写”する機能の信頼性を確保することに成功していたとしても、IoTシステムはサイバー空間から届いた誤った指令を“正しく”転写して忠実に動作することで物理的な損害を発生させてしまうかもしれない。
  - データが生成される場所については第3層ではなく第2層に属する場合があり、第3層と第2層とを組み合わせることでデータ生成における信頼性が確保できる。（第2層TFで策定したIoT-SSFと連動）

データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク

- 「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮題、以下フレームワーク）」の骨子案のパブリックコメントを実施。（2021年7月15日～10月11日）
- 骨子案パブリックコメントでいただいた御意見の反映を行うとともに、添付資料として「ユースケース」及び「イベントごとのリスクの洗い出しのイメージ」を追加。



データマネジメントの考え方の確立

＜データマネジメントの捉え方＞

- **データのライフサイクルの各工程において発生する様々な形の“関与”**

＜３つの視点＞

① データマネジメントについて確立した定義は存在しない

- 他の機関等において整理されたデータマネジメントの定義を持ち込むのではなく、CPSFを基礎としてセキュリティ対策を検討するために必要なデータマネジメントの考え方を示す。

② データを軸に置く

- データがライフサイクルの各工程においてどのような関与を受けるかという視点で整理すべき。

③ 関与する主体は同一・単一の主体に限られるものではない

- データマネジメントは複数の主体による協同的活動**（Collective Action）になる**ことを排除しない。例：クラウドサービス

本フレームワークの目的・想定読者

＜ 本フレームワークの目的 ＞

as isの対策

- データを軸に置き、**データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し、**そのセキュリティを確保するために、ガバナンスを含めた必要な措置を**ステークホルダーが協調して実施する**。
- 洗い出されたリスクへの対策要件例として、これまでに公表されてきた情報セキュリティに関する様々な国際標準等を参照。

to beの対策

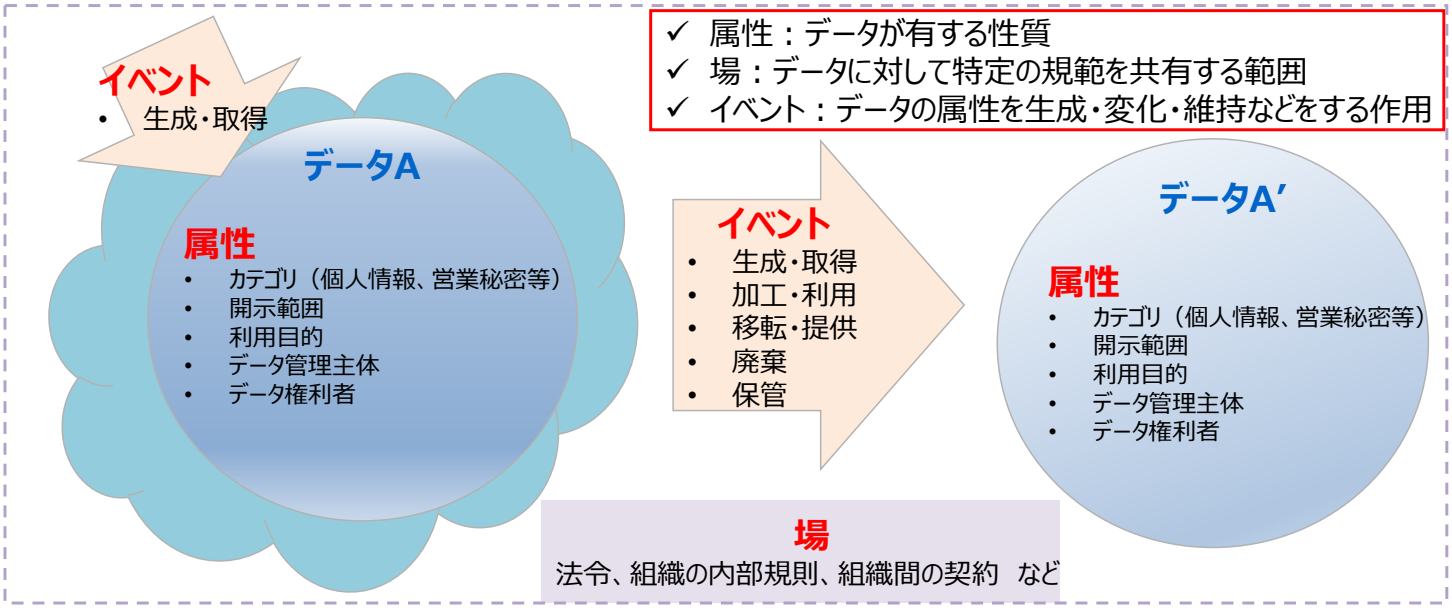
- データの流通を促進するために必要な条件を明確化。プロトコルの設計が容易に。
- 強い立場にあるシステムが**プロトコルのブラックボックス化によって「バンドル」することを難しく**させ、**オープン化された環境でデータ連携やシステムの組み合わせの自由を確保することを可能に**。
- 主体の在り方などを過度に考慮することなく、データに対して本来求められる要求事項を歪めることなく整理することが可能であり、**各国の制度間のギャップ分析**を行い必要な調整措置を明らかに。

＜ 本フレームワークの想定読者 ＞

- バリュークリエイションプロセスに参加する者
- データ利活用に関するサービスを提供する者
- データ利活用に関するサービスを提供するシステムの設計・構築・運用に関わる者
- トラストサービスを提供しようとする者
- データセキュリティに関わるガイドライン等のルール設定に関わる者

データマネジメントのモデル化の概要

- データマネジメントを「**データの属性が場におけるイベントにより変化する過程を、ライフサイクルを踏まえて管理すること**」と定義。
- **「属性」「場」「イベント」の3つの要素はそれぞれが相互に影響**しあう関係。
- データの遷移による**データの変化に関する一定の予見可能性を確保、ステークホルダーの間で認識を共有しやすく**なる。
- 共通の理解に基づいてそれぞれの主体が実施すべき措置についての検討を進めることが可能となり、**ステークホルダー全体で適切なデータマネジメントを実施していくことができる環境を実現**していく。



リスク分析手順

- **下記の4つのステップに沿ってバリュークリエイションプロセスにおけるデータの状態を可視化**。
- 「属性」、「場」、「イベント」が相互に依存する関係にあることから、STEP1～3の**各ステップは不可逆的なものではなく、互いにフィードバックをかけながら検討されることが適切**。
- リスクの洗い出しに当たっては、機密性・完全性・可用性といったサイバーセキュリティに係る観点の他、各法制度等に係るコンプライアンスの観点でのリスクについても洗い出す必要。

STEP 1
データ処理フロー（「イベント」）の可視化

STEP 2
必要な制度的な保護措置（「場」）の整理

STEP 3
「属性」の具体化

STEP 4
「イベント」ごとのリスクの洗い出し

モデル化（「イベント」） ～ 生成・取得、加工・利用 ～

- データの属性を生成・変化・維持などをする作用である「イベント」に関しては、**大きくは「生成・取得」「加工・利用」「移転・提供」「保管」「廃棄」の5つに区分することが可能**。
- 5つの「イベント」はそれぞれ重複する性質を持つ場合があり、目的に応じて適切に「イベント」を捉え、リスクの洗い出しを実施する必要（例：閲覧は加工・利用だが移転・提供の要素を含み得る）。

＜ 生成・取得 ＞

- バリュークリエイションプロセスにおいて、サイバー空間でやりとりされるデータは、**何らかの形で生成・取得されることによってそのライフサイクルが始まる**。
- サイバー空間とフィジカル空間が高度に融合し、フィジカル空間の情報が大量にサイバー空間に転写され、リアルタイムに共有されるようになると、サイバー空間のつながりにおけるデータの信頼性を検討する場合、従来はデータを管理する範疇に捉えられていなかった、**データの生成・取得に関わる機器・システムなどの信頼性についても検討する必要**。
  - ➢ 代表的なリスク：計測結果が実際と異なる、計測機器をなりすまされる等の転写の失敗など。

＜ 加工・利用 ＞

- データに**付加価値を生み出すための作用を加工・利用と捉える**。
  - ✓ 分析過程や保管されたデータセットから**データの一部の項目や要素、レコードなどを取り除く作用については、加工の一形態として捉える**ものとし、後述する廃棄とは区別する。
  - ✓ データを保有しない者が**データにアクセスする作用（閲覧）については、利用の一形態として捉える**ことが適切であるが、リスクを洗い出す際は**移転・提供の要素を考慮**に入れる必要。
  - ➢ 代表的なリスク：データの目的外利用、不適切な加工など。

モデル化（「イベント」）～ 移転・提供 ～

＜ 移転・提供 ＞

- サプライチェーンを動的に構成する場合、効果を最大限に引き出すためには**より自由にデータの移転・提供を実施できる環境にすること**、**リスクに対してより効果的に対応すること**が求められる。
- 特定の移転・提供事象について、国・地域、組織・ヒト、システム・サービス、機器という**4つの単位で整理**。
- **イベントをどの程度詳細に記述するかは、データフローの整理の目的に応じて調整する必要**。

単位	考慮すべき事項	単位ごとのリスク(例)
国・地域	データの移転・提供に関連する国・地域及び、当該国・地域におけるデータ保護関連の政策、法令、ガイドライン等	● データの移転元/移転先に相当する国・地域にデータ保護関連法令が存在しない又は内容として不十分な場合、移転元/移転先間における保護水準の不整合が生じる結果、移転先で移転元の保護水準が確保できない。
組織・ヒト	データの移転・提供の関係主体となる組織及びヒト、当該主体におけるデータ保護関連の方針、体制等	● 組織のセキュリティポリシーが存在しない又は内容として不十分な場合、データ移転に関わるステークホルダ間にてセキュリティ水準の不整合が生じる結果、移転先で移転元の保護水準が確保できない。
システム・サービス	複数の機器から構成され、データの移転・提供を実行するシステムと提供されるサービス	● システム・サービスにおけるセキュリティ実装が十分でないことにより以下のようなセキュリティ上のリスクが生じうる。 - ネットワーク上での盗聴 - 送信元/送信先のなりすまし
機器	データの移転・提供を実行するサーバ、IoT機器、ネットワーク機器等のデータを物理的に取扱う単体のシステムコンポーネント	● 機器におけるセキュリティ実装が十分でないことにより以下のようなセキュリティ上のリスクが生じうる。 - 機器内の不正なコンポーネントを通じた意図しないデータ移転 - DDoS攻撃等のサービス拒否攻撃による機器の稼働停止

モデル化（「イベント」）～ 保管、廃棄 ～

＜ 保管 ＞

- **保管は、他のイベントに付随して必ず生じる「イベント」**である。データはライフサイクルの様々な段階において、ネットワーク接続されたストレージ機器（オンプレミス、クラウドの双方を含む）・クライアントのハードディスク、USBメモリのような可搬媒体、機器の一時記憶領域等に保管され得る。
- データの取扱いに関してリスクを洗い出し、セキュリティ対策を検討する上では、**移転・提供、加工・利用されるデータとは異なるリスクが生じうる**ことから、「イベント」の一類型として整理し、リスクの洗い出しを実施することが適切。

＜ 廃棄 ＞

- 本フレームワークにおける**廃棄は、データセット全体を使用不可能な状態とすること**を指す。
- 同意に基づいて収集したパーソナルデータに関して、特定の個人が同意を撤回する等により、当該個人のデータをデータセットから除外する行為は、加工・利用の一形態として捉えるのが適切。
  - ➢ 代表的なリスク：廃棄すべきデータが残存して漏えいする、本来は廃棄すべきでないデータまで廃棄してしまうなど。

モデル化（「場」）

- 「場」は、それぞれの状況や関係する者の事情などによって適用される形態等が異なり、**一律に設定方法や形態が決まるものではない**。今後の議論や事例の蓄積を通じて、精緻化されることが想定される。
- 例えば、「場」を構成する重要な要素の一つに法令等があるが、**「場」の設定を行うに当たって、必要な観点を漏らすリスクを低減**しながら検討するために、**下記のような4つのカテゴリから整理**。
- 4つのカテゴリは、「場」が、データに関して何らかの共通の取扱いを求める法令等と連動して設定されることを背景に、**データに共通の取扱いを求める目的としてはどのようなものが考えられるか、という観点から整理**。

- **パーソナルデータの保護**
  - 「場」の例：個人情報保護法（日本）、GDPR（欧州関係）、個人情報を取得する際に当該個人が同意した利用目的
  - 規定される「属性」の例：カテゴリ（個人情報、匿名加工情報）、データ権利者、データ管理主体
- **知的財産・営業秘密保護**
  - 「場」の例：不正競争防止法、著作権法、主体間の契約（NDA等）
  - 規定される「属性」の例：カテゴリ（営業秘密、限定提供データ）、開示範囲、データ権利者
- **機微技術管理**
  - 「場」の例：外為法、米国輸出管理規則
  - 規定される「属性」の例：カテゴリ（輸出管理等対象技術）、開示範囲、データ管理主体
- **適切な社会機能の維持**
  - 「場」の例：金融商品取引法（インサイダー取引）、各種守秘義務関係
  - 規定される「属性」の例：開示範囲

モデル化（「属性」）

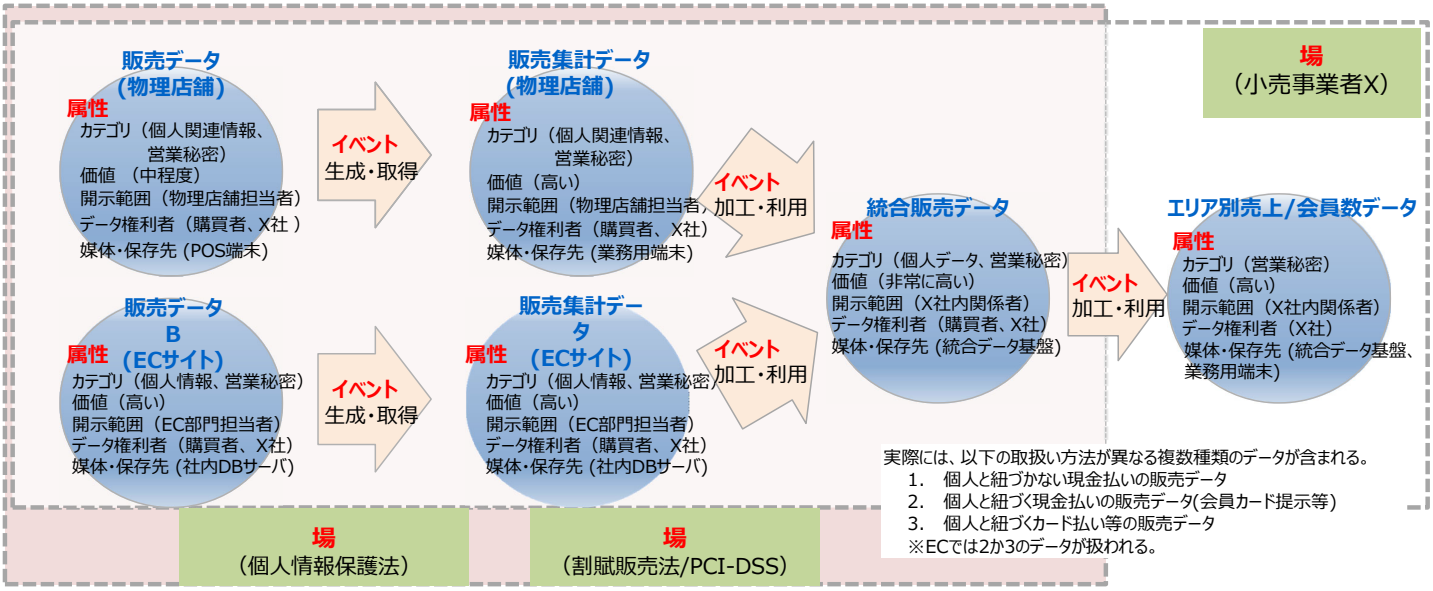
- 代表的な「属性」やパラメータ、整理のポイントを示す。
- 整理した「場」からデータに対する要求を検討し、関連する「属性」を適切に具体化することが重要。

- **カテゴリ**
  - 特に「場」と連動して、データに対して特別な作用（「イベント」）を求める場合（個人情報・匿名加工情報、営業秘密・限定提供データなど）、カテゴリとして法令等における位置づけを整理する。
- **開示範囲**
  - 民法上の契約や組織内規則も含め、データに定められている開示範囲を整理する。その際、組織内での取扱いであっても、国・地域間での移転が伴う場合や、米国輸出管理法上のみなし輸出に該当する場合等、開示範囲の制限が複層的に適用される可能性がある点に留意。
- **利用目的**
  - 個人情報やライセンスなど、法令等に基づいて利用目的に制限が設けられている場合、当該利用目的の範囲内で取扱われる必要があることから、「属性」として明示しておく必要がある。
- **データ管理主体**
  - データに軸を置く本フレームワークにおいては、データに作用を及ぼす主体についても、データが転々流通する過程で移り変わるものであり、あくまで「属性」の一つとして整理する。
- **データ権利者**
  - データが個人情報である場合、企業の競争力に関わる場合など、データ管理主体とは別に、データに対して権利を有する主体が存在することがある。移転・提供が行われて別の主体がデータを取得した場合でも、データ権利者は当該主体の管理下にあるデータに対して引き続き権利を有すると考えられるため、管理主体が転々と移っていく過程でも、「属性」として管理する必要がある。

活用方法 ～ サプライチェーンを構成するステークホルダー間での活用 ～

- バリュークリエイションプロセスに関わるステークホルダーの間で、データのライフサイクルの各工程において**リスクを可視化した上で、各主体がそれぞれ実施すべき対策を他の主体と合意形成しながら取り組むことにより、データの信頼性を確保することが期待**される。
- 可視化されたリスクに対して各主体が実施すべきセキュリティ対策は、これまでに公表されてきた情報セキュリティに関する様々な国際標準等を参照。
- **将来的には経営者によるITガバナンス（デジタルガバナンス）の検討への活用も期待**。

小売業におけるPOSデータの活用事例



添付A：ユースケース

- フレームワークの読者に対し、より理解を深めていただくために、実践的なユースケースに基づくモデル化とリスクの洗い出しのイメージを添付資料として作成。
- 添付Aでは、特徴的な以下4つのユースケースを選定した。
  （次ページ以降で②及び③の概要を提示）

1

POSデータの分析
モデル化の全体像を把握しやすく単純化した事例

2

高齢者生活支援事業の提供
多数のステークホルダーが関係する事例

3

IaaS、PaaS、SaaSを利用してサービスを提供する例
クラウドサービスの多層化・重層化事例

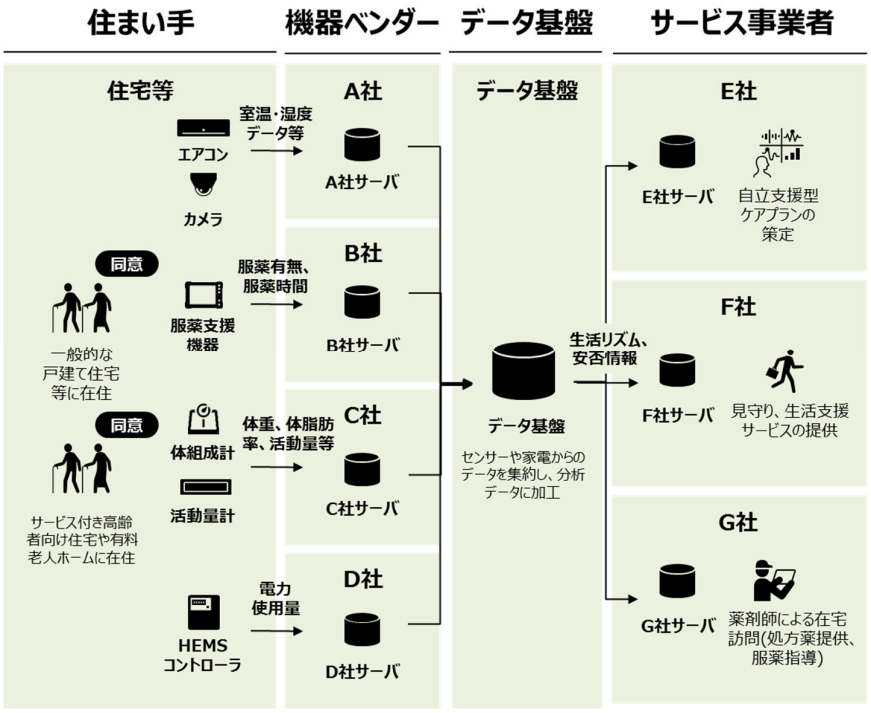
4

国内で提供されるITサービスに関して、海外で開発や運用等を実施する例
国外で開発や運用等を実施する事例（データの越境移転）

ユースケース② ｜ 高齢者生活支援事業 概要

- 2018年に実施された国立研究開発法人　新エネルギー・産業技術総合開発機構（NEDO）／パナソニック株式会社他による「IoT家電・センサーからのライフデータによる高齢者の生活サポートサービス基盤の研究開発事業」を取り上げる。

https://www.nedo.go.jp/news/press/AA5_101002.html



- 一般的な戸建て住宅や有料老人ホーム等に設置される多数の機器群を通じて、高齢者の生活や健康の状況に関するデータが**生成**され、各機器ベンダー（A社～D社）の運用するサーバに**蓄積**
- 各機器ベンダーは一定の収益を得る代わりに、第三者（プラットフォーム事業者）の運用するデータ基盤に各々が収集したデータを**提供**する。各機器ベンダーから提供されたデータは特定の個人を特定できない形でデータ基盤上に**集約**され、高齢者の生活リズム情報や安否情報というより高次なデータへと**加工**される。
- 高齢者の生活リズム情報や安否情報等のデータは、必要に応じてサービス事業者等に第三者提供され、データ主体の個人と紐づけたうえでより高度な支援サービスの提供等に**加工・利用**される。

ユースケース② ｜ 高齢者生活支援事業 ステークホルダー

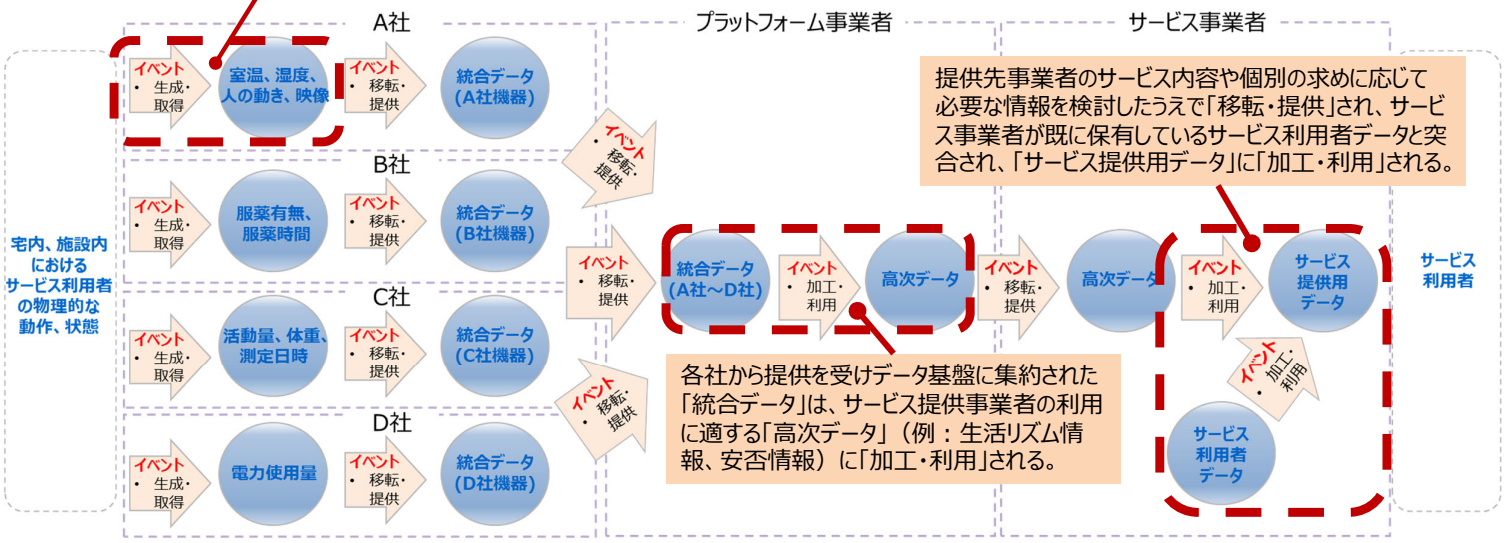
- 機器ベンダー（A社～D社）、プラットフォーム事業者、サービス事業者等は、コンソーシアムを組成し、共通して適用される規則の策定や適時の情報共有等を行っている 。
- 取扱うデータには機微な個人データとなり得るものも含まれることから、コンソーシアム等での協議を実施し、サプライチェーンの全体で十分な水準のデータ保護措置を講じる必要がある。

ステークホルダー	説明
住まい手	日常生活の中で各種IoT機器・サービス等を利用し、それに伴って生成される自身に関するデータを同意等の適切な手続きを経たうえで事業者に提供する。 • 一般的な戸建て住宅等に在住する高齢者 • サービス付き高齢者向け住宅や有料老人ホームに在住する高齢者
機器ベンダー（A社～D社）	宅内や施設内に設置されている機器を製造・販売し、本人同意等の適切な手続きを経たうえで各々運用中の機器から取得したデータを収集し、管理している。
A社	エアコンや見守りカメラ等の家庭用IoT機器を製造・販売し、収集したデータを自社サービスで活用するだけでなく、プラットフォーム事業者にも提供する。
B社	処方薬の服薬有無や服用時間等をセンシングする服薬支援機器を製造・販売し、収集したデータを自社サービスで活用することに加え、プラットフォーム事業者にも提供する。
C社	体組成計や活動量計等のヘルスケア機器を製造・販売し、収集したデータを自社サービスで活用するだけでなく、プラットフォーム事業者にも提供する。
D社	スマートメータが実装された家庭向けに電力使用状況を可視化するサービスを提供し、収集したデータをプラットフォーム事業者にも提供する。
プラットフォーム事業者	各住宅、施設に設置した機器等からのデータを集約し、適宜加工・分析等を実施する。
サービス事業者（E社～G社）	プラットフォーム事業者からデータの提供を受け、より高度な高齢者支援サービスの提供等に活用する。

ユースケース② ｜ 高齢者生活支援事業 STEP 1

- STEP 1として、**データ処理フロー（イベント）の可視化**を行う。

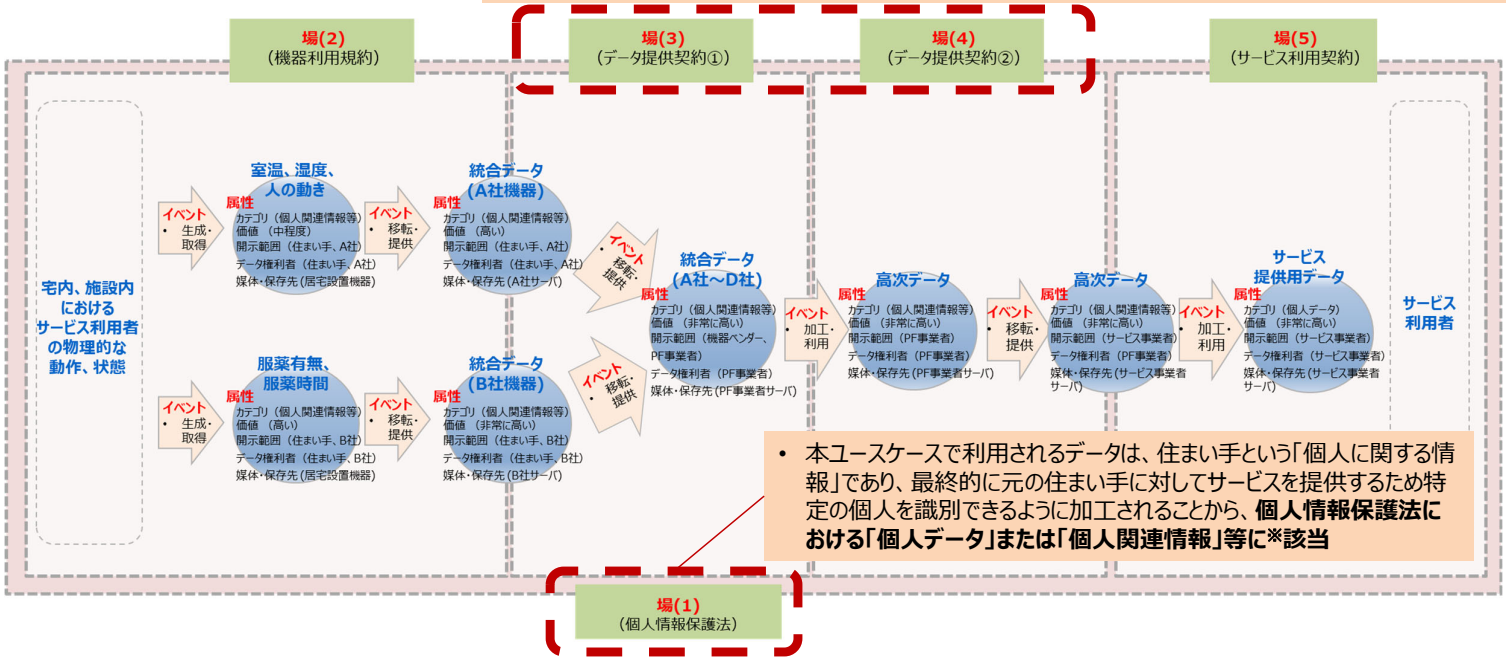
製造・販売者	名称	収集データ
A社	エアコン	室温・湿度情報
	電波センサーによる見守りシステム	ベッド上の呼吸有無・活動状態（動き）
	コミュニケーションカメラ	室温、人の動き、映像



ユースケース② ｜ 高齢者生活支援事業 STEP 2

- STEP 2として、**必要な制度的な保護措置（場）の整理**を行う。

- 各機器ベンダーが保有するデータに加え、「統合データ」についても、匿名的な利用者IDや機器IDに基づいて必ずしも特定の個人に紐づかない形で管理されていることを仮定しているため、「個人データ」ではなく「個人関連情報」等に該当すると考えられるが、提供先のサービス事業者において個人データとして取得されることが容易に想定される。そのため、各機器ベンダー及びPF事業者においては、**個人関連情報取扱事業者として本人からの同意取得の確認、提供元における記録等の義務が生じる**点に留意が必要



※令和2年の改正個人情報保護法において規定。令和４年４月１日に施行される予定。

ユースケース② ｜ 高齢者生活支援事業 STEP 3-1

- STEP 3として、前STEPにて特定した「場」を踏まえ、**各種データの管理に資する属性を特定**する。
- 個人情報保護法制の他、開示範囲やデータ管理主体、利用期限等の事業者間の責任分解にも関連する内容を特定する際には、当事者間で締結される各種契約・規約が有用。

「属性」の検討において考慮すべきルール（場）

		個人情報保護法	機器利用規約	データ提供契約	サービス提供契約
カテゴリ	パーソナルデータ保護	○			
	知的財産（営業秘密を含む）保護			○	
	…	…	…	…	…
開示範囲		○	○	○	○
利用目的		○	○	○	○
データ管理主体			○	○	○
データ権利者		○	○	○	○
価値（重要度）			○	○	○
媒体・保存先			○	○	○
利用期限			○	○	○

ユースケース② ｜ 高齢者生活支援事業 STEP 3-2

- STEP 3として、前STEPにて特定した「場」を踏まえ、**各種データの管理に資する属性を特定**する。

本ユースケースにて取扱うデータ（一部）の「属性」パラメータ例

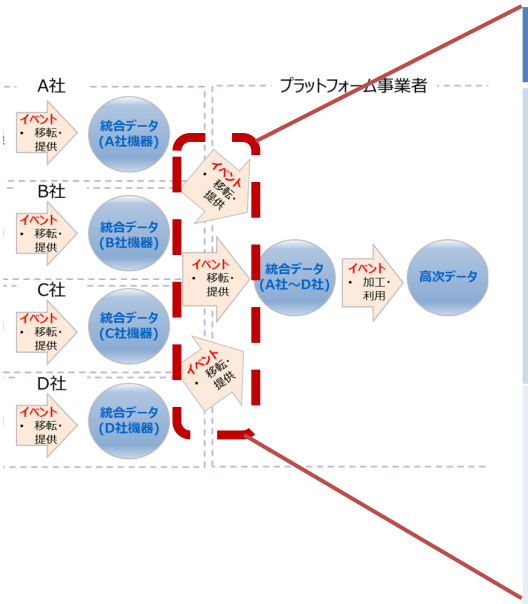
		統合データ（A社）	統合データ（A社～D社）	高次データ	サービス提供用データ
カテゴリ	パーソナルデータ保護※1	個人関連情報 等	個人関連情報 等	個人関連情報 等	個人データ
	知的財産※2（営業秘密を含む）	営業秘密 等（A社）	営業秘密（PF事業者）	営業秘密 等（PF事業者）	営業秘密（サービス事業者）
開示範囲		A社内	PF事業者内	PF事業者内	サービス事業者内
利用目的		取得データを活用した各種サービスの提供	左記と同様	左記と同様	左記と同様
データ管理主体		A社	PF事業者	PF事業者	サービス事業者
データ権利者		住まい手、A社	住まい手、機器ベンダー、PF事業者	住まい手、PF事業者	住まい手、サービス事業者
価値（重要度）		高い	非常に高い	非常に高い	非常に高い
媒体・保存先		A社サーバ	PF事業者サーバ	PF事業者サーバ	サービス事業者サーバ
利用期限		特になし	データ提供契約終了から1年	データ提供契約終了から1年	サービス提供期間終了まで

※1 対象のデータが、個人情報保護法上のいかなる情報の類型に属するかは、改正個人情報保護法の動向も踏まえつつ、適用主体において慎重な検討が必要である。
※2 上記のデータのうち、特定の事業者間で共有されるものについては、不正競争防止法上の「限定提供データ」に該当する場合も想定される。

ユースケース② ｜ 高齢者生活支援事業 STEP 4

- STEP 4として、STEP 1～3で特定した内容を踏まえ、**イベントごとのリスクポイントの洗い出し**を行う。

各機器ベンダー「統合データ」のPF事業者への「移転・提供」にて想定されるリスクの例



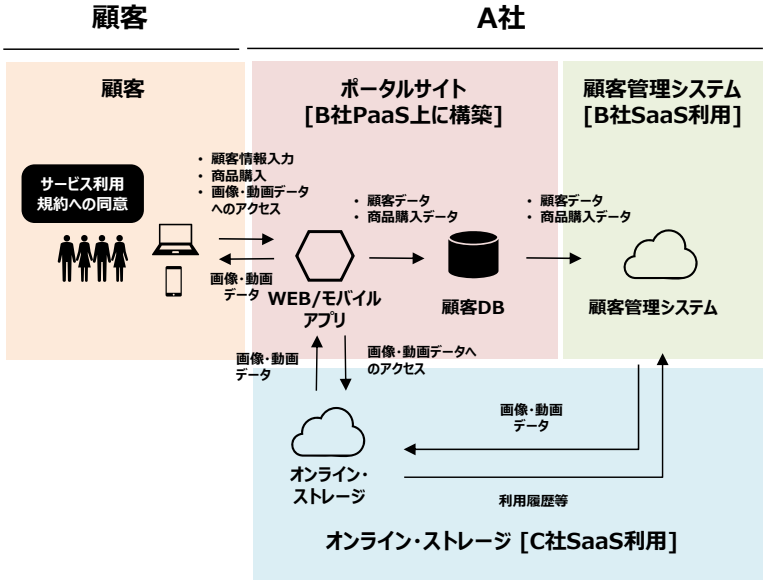
大分類	中分類	各機器ベンダーが保有する「統合データ」のPF事業者への「移転・提供」にて想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、通信内容が漏えいする。 ● 悪意のある内外の主体が機器ベンダーの管理するサーバから当初接続を意図していなかったサーバ等にデータを送信する。
	完全性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、データを改ざんする。
	可用性	● 悪意のある第三者がデータ基盤のAPI を無作為に呼び出すような DoS攻撃を行い、プラットフォーム事業者サーバの処理が停止する。
関連する法制度等に係る観点	パーソナルデータ保護	● 統合データの提供前に、提供元の機器ベンダーが提供先のプラットフォーム事業者において当該データが個人情報として取得されるかどうかを確認していない。 ● プラットフォームにて特定の個人の特定を行う場合に、住まい手の同意等を得ることなくデータがプラットフォーム事業者に提供される。
	知的財産（営業秘密を含む）保護	● 各社の統合データが悪意のある内外の主体により不正な手段で取得され、開示、使用される。

リスクを可視化した上で、各主体がそれぞれ実施すべき対策を他の主体と協議しながら取り組むことにより、データの信頼性を確保することが期待される。

ユースケース③ ｜ クラウドサービスを提供する例 概要

- サービス・物販事業者が提供する画像・動画データ管理を行うクラウドサービス事例を取り上げる。
- クラウドサービスを活用することで、コスト低減、技術革新対応力・柔軟性の向上等のメリットが得られる一方、サービス提供者と利用者の間の責任分界に対する認識が曖昧になりがちであったり、データの地理的所在等の透明性の不足等の課題が存在する。

システム・サービス概要



- サービス・物販事業を運営するA社は、従来の店舗サービスの提供に加え、顧客向けポータルサイトにてスタジオで撮影した画像・動画データをダウンロードするサービスを提供している。
- A社のポータルサイトは、B社の提供するPaaS上に構築され、さらにB社SaaSとして提供される顧客管理システムにもデータ同期を行う。
- スタジオで撮影したデータはC社IaaSとして提供されるオンライン・ストレージに格納され、顧客はポータルサイトを経由してアクセスすることができる。

ユースケース③ ｜ クラウドサービスを提供する例 ステークホルダー

- 本ユースケースで考慮すべきステークホルダーは以下の通り。
- 本ユースケースでは、A社のシステム構築のため契約するB社SaaS及びPaaSが、実際はC社IaaS上で構築されるといった関係がある。こうした「クラウドサプライチェーン」を米国国立標準技術研究所（NIST）等の分類を元に整理する。

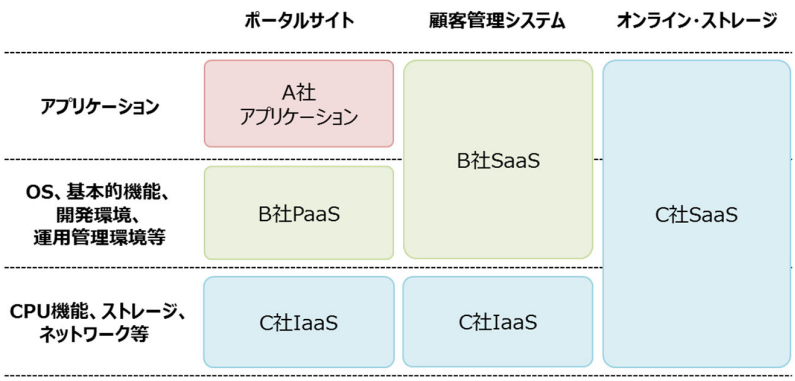
ステークホルダー	説明
顧客	A社が提供するポータルサイトにアクセスし、過去に撮影した画像・動画データの加工、ダウンロードや関連商品の購入を行う。
A社	サービス・物販事業を業として行い、顧客価値を高めるための試みとして**クラウドサービスカスタマ** としてB社やC社から提供される各種クラウドサービスを利用しつつポータルサイトや顧客管理システム等を構築、運用している。
クラウドサービスプロバイダ	A社に各種のクラウドサービスを提供する事業者
B社	ポータルサイト向けにWebアプリ開発・運用基盤をPaaSとして、顧客管理システム・サービスをSaaSとしてA社に提供する。
C社	画像・動画データを格納するオンライン・ストレージサービスをSaaSとしてA社に提供し、**ピアクラウドサービス** としてB社の提供するサービスの基盤となっているIaaSも別途提供している。
クラウドサービスパートナー	B社PaaS上にポータルサイトを構築することに加え、各サービス間の連携部分を開発する。

クラウドサービスプロバイダ（CSP / cloud service provider）：
「クラウドサービスを利用できるようにするパーティ」を指す。(ISO/IEC 17789:2014)
クラウドサービスカスタマ（CSC / cloud service customer）：
「クラウドサービスを使うためにビジネス関係にあるパーティ」を指す。(ISO/IEC 17789:2014) クラウド利用者とも呼ばれる。
ピアクラウドサービス（peer cloud service）：
「クラウドサービスプロバイダのクラウドサービスの一部として使用されるクラウドサービス」を指す。(ISO/IEC 17789:2014)

ユースケース③ ｜ クラウドサービスを提供する例 ステークホルダー

- 本ユースケースで考慮すべきステークホルダーは以下の通り。
- 本ユースケースでは、A社のシステム構築のため契約するB社SaaS及びPaaSが、実際はC社IaaS上で構築されるといった関係がある。こうした「クラウドサプライチェーン」を米国国立標準技術研究所（NIST）等の分類を元に整理する。

クラウドサービス提供に係るサプライチェーンの概要



経済産業省「クラウドセキュリティガイドライン活用ガイドブック2013 年度版」クラウドサプライチェーンにおける一般的な課題

- A社のようなクラウドカスタマから見た直接の契約先（ここではB社）に問題がない場合にも、**配下に存在するPaaSやIaaSに問題が生じた際、連鎖的な問題に巻き込まれる。**
- 障害が要因となり事業活動に何らかの損害が生じた場合に**事業者間で責任分界があいまいになりやすい。**
- 法規制上の問題やクラウドサービスカスタマのセキュリティポリシー等に関連して、外国や外国法適用配下に情報を置くべきでないとされているにも関わらず、サプライチェーンの配下に該当する事業者が存在し、**カスタマの意図に反する状態に陥ってしまう。**

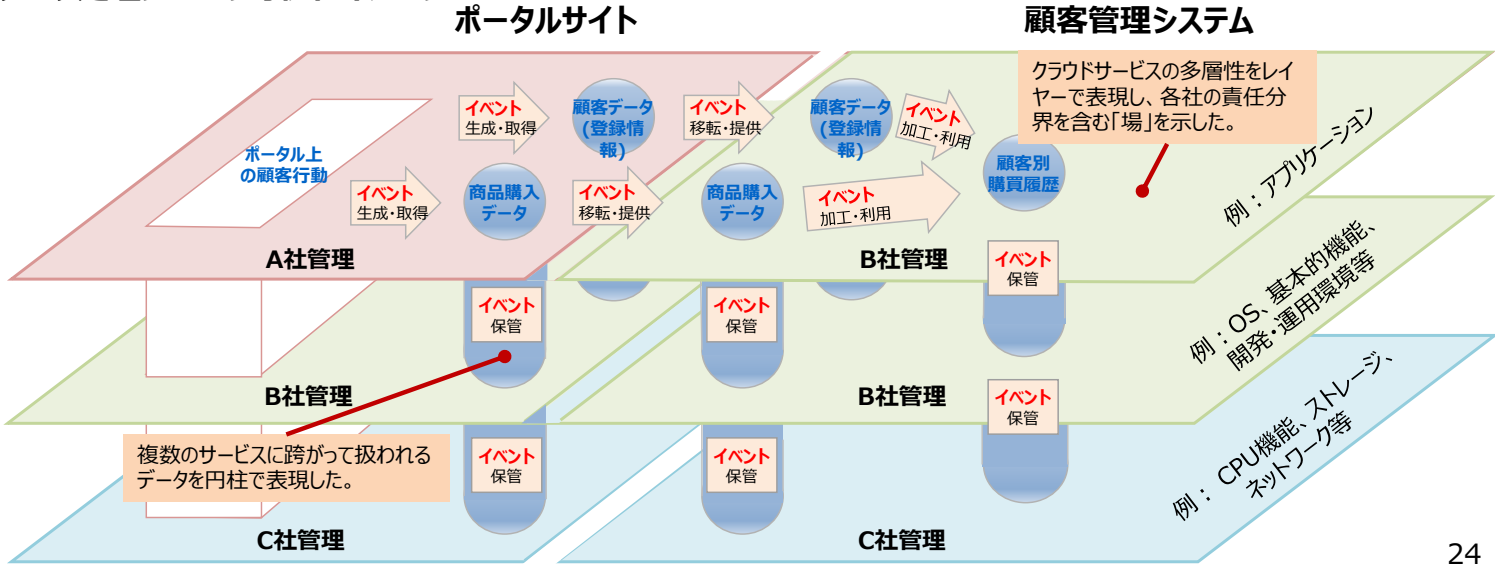
ユースケース③ ｜ クラウドサービスを提供する例 STEP 1～2

- 多層的なサービスにおけるデータ処理フローの可視化と必要な制度的な保護措置を整理する。

今回のデータ処理フローで取扱う部分
- ポータルサイト上では顧客による自身のデータの入力や製品等の注文、その他の行動に応じて、「顧客データ」、「商品購入データ」等が「生成・取得」され、顧客DBに格納される。
- 当該データは、適時にB社が提供する顧客管理システムに「移転・提供」され、A社内の個別のニーズに応じてA社従業員により「加工・利用」される。

今回のデータ処理フローで取扱わない部分
- A社所有の撮影機材により、顧客の画像・動画データが「生成・取得」される。
- A社従業員によりC社の提供するオンライン・ストレージへ「移転・提供」され、「保管」される。
- 画像・動画データは、顧客からの求めに応じて「加工・利用」（オンライン・ストレージ上での画像編集等）されたうえで顧客所有の端末（PC、スマートフォン等）に「移転・提供」される。

データ処理フローの可視化イメージ



添付B：イベントごとのリスクの洗い出しのイメージ

- 添付Bでは、フレームワークの適用を行う事業者等が、自身のデータ利活用プロセスにおいて想定されるリスクを特定するにあたり、考慮することが望ましい典型的なリスクを列挙する。
- 有効な対策要件例として、これまでに公表されてきた情報セキュリティに関する様々な国際標準等を参照。

イベントごとの典型的なリスクの記載方法

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	生成・取得されるデータがネットワーク上で悪意のある内部犯行者または外部の攻撃者に傍受され、漏えいする。	情報漏えい	暗号化等による通信経路の保護

セキュリティの保護に関わるもの
- 機密性
- 完全性
- 可用性

関連する法制度等に関わるもの
- パーソナルデータ保護
- 知的財産（営業秘密を含む）保護

- アドバーサリ（悪意のある主体）
- 偶発的
- 構造上
- 外部環境上

STRIDEによる分類
- なりすまし
- 改ざん
- 否認
- 情報漏洩
- サービス不能
- 権限の昇格

本稿にて追加した分類
- マルウェア感染
- 不正改造
- 誤使用
- システム等の不具合
- 自然災害等

以下の参考文献との対応関係を記載
- CPSF
- ISO/IEC 27001:2013
- SP 800-53
- DMBOK 第2版 等