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

経済産業省　商務情報政策局　サイバーセキュリティ課

令和 4 年 4 月 8 日

変更履歴

Version	変更年月日	変更箇所	変更内容
1.0	2022 年 4 月 8 日	-	新規作成

目次

1. 新たなデータマネジメントの在り方 4
1-1 CPSF における第 3 層（サイバー空間におけるつながり） 4
1-1-1 CPSF 概論 4
1-1-2 第 3 層の位置づけ 4
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 5
1-3 本フレームワークの目的 7
1-4 本フレームワークの想定読者 9
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 10
2-1 概要編 10
2-1-1 データマネジメントのモデル化の概要 10
2-1-2 リスク分析手順 12
2-2 詳細編 13
2-2-1 モデル化（「イベント」） 13
2-2-2 モデル化（「場」） 19
2-2-3 モデル化（「属性」） 20
3. 活用方法 22
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 22
3-2 ルール間のギャップの分析 24
添付 A ユースケース 25
A-1 POS データの分析 25
A-2 高齢者生活支援事業の提供 37
A-3 IaaS、PaaS、SaaS 等を利用してサービスを提供する例 50
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 64
添付 B イベントごとのリスクの洗い出しのイメージ 75
B-1 イベントごとの典型的なリスクの記載方法等 75
B-2 イベントごとのリスクの洗い出しのイメージ 78

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

[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。

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

---

[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・完全性についても考慮する必要がある。

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

[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。

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
- 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

[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。

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。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、データの取扱に係るマネジメントのルールを提示し、それに従って取り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、本データが取り扱われるべき「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得る。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、取り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・提供も取り扱うこととする。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。

ー　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。

ー　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クが生じ得ることから、「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] 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。

[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。

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、取り扱うデータの性質や、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

[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）

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り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」の一つとして取り扱う。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り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得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

[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。

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。

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。

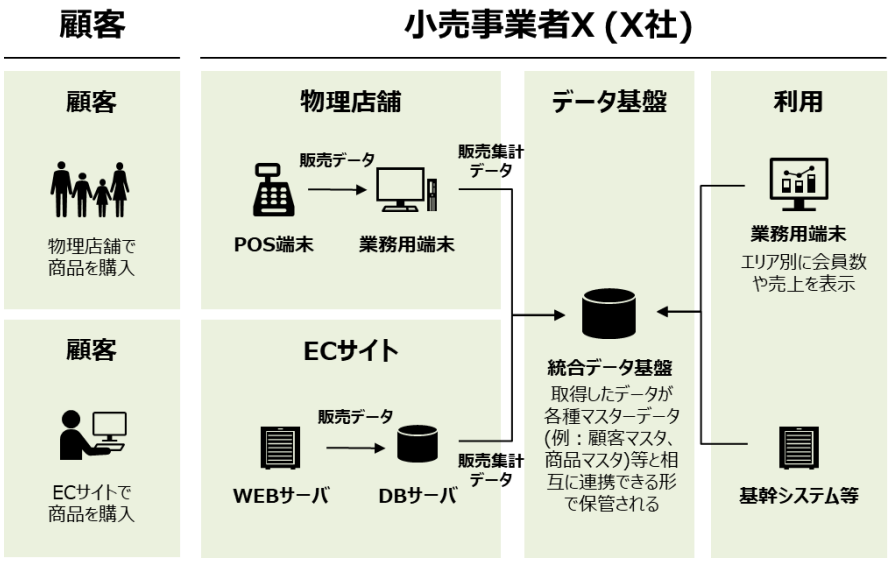
---

[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。

- 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。



図A-1.1 対象プロセスの概要

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]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。

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

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、又は既に整備

[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

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て以下が挙げられる。

- 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

- *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、それに従って取り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。*

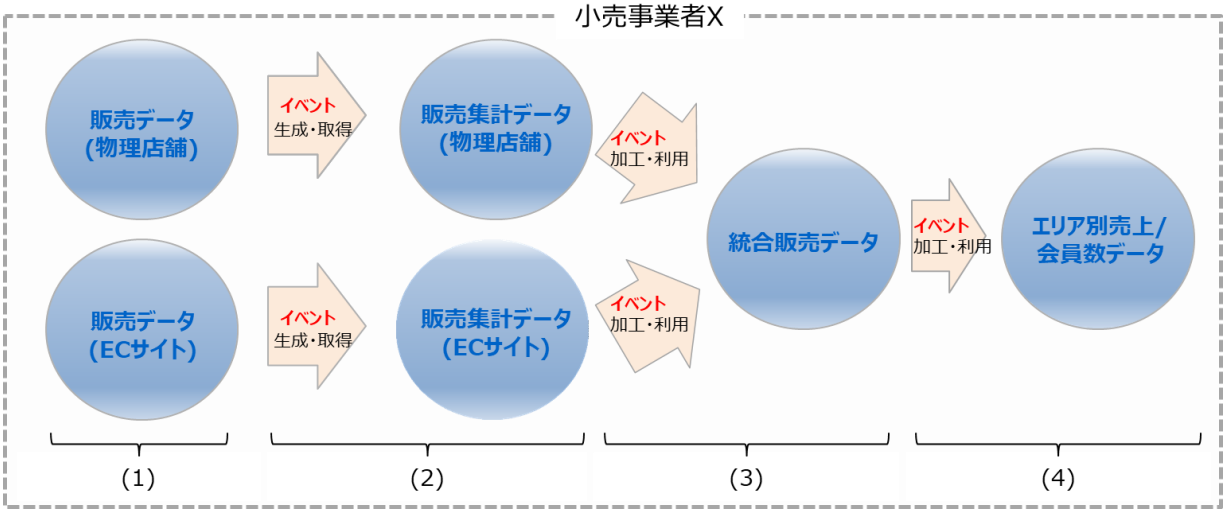
STEP 1は、生成・取得から廃棄に至るまでの一連のデータのライフサイクルにおいて、データがどのようなプロセスで利活用されるのかを理解する段階である。本ユースケースでは図A-1.1で示すように、以下のプロセスにより構成される。

(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-1.2 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データベース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

- *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づけられている。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

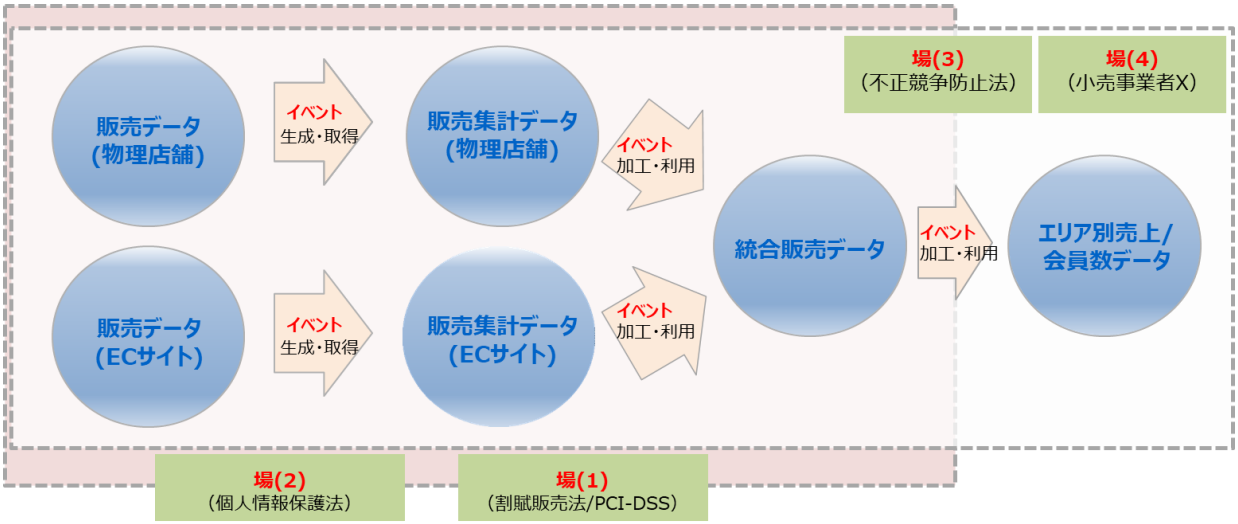
[14] 脅威分析の一環で作成されるデータフロー・ダイアグラム（DFD）において特定される、管理している組織やインターフェイスが変わる場所に引く境界線のことを指す。

[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り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。

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。

（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



図A-1.3 必要な制度的な保護措置の整理（POSデータの分析）[16]

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、本データが取り扱われるべき「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

[16] 図中には必ずしも記載されていないが、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ルールも特定されるべき「場」として含まれ得る。

は以下のとおりと考えられる。

表A.1-2 「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		○	○		○

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「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 to knowの原則[17]やNeed to useの原則[18]に従い、営業秘密管理上の「秘密管理性」を満たすた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ユースケースで取り扱うデータがとり得るパラメータの例を以下に示す。

[17] 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

[18] 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

表A-1.1 本ユースケースにて取扱うデータの「属性」パラメータ例

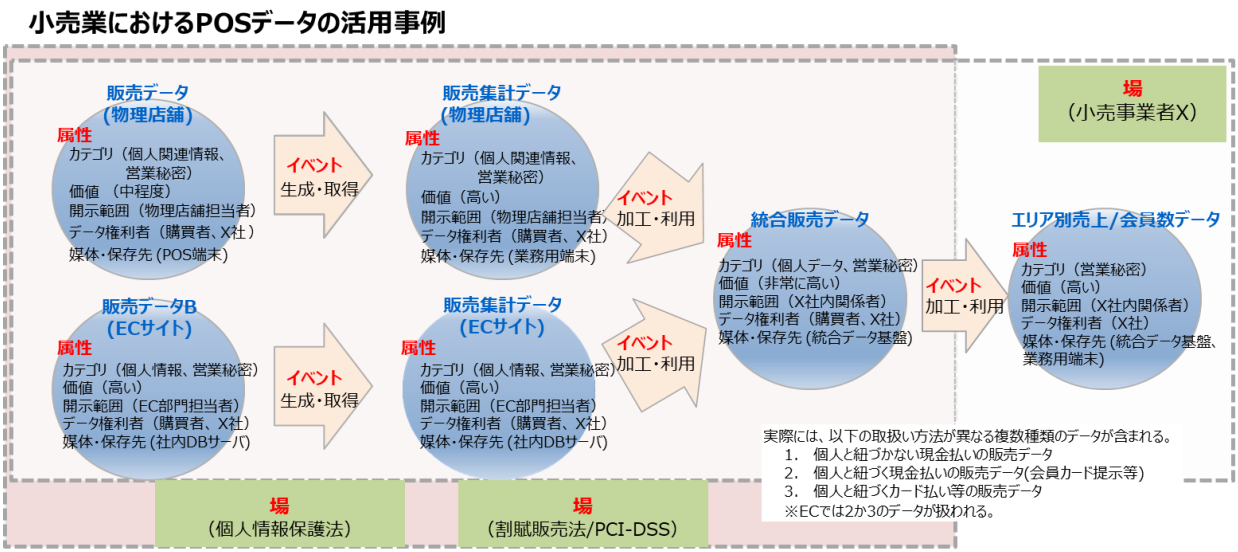
		販売データ（物理店舗）	販売集計データ（物理店舗）	統合販売データ	エリア別売上/会員数データ
カテゴリ	パーソナルデータ保護	個人関連情報 等	個人関連情報 等	個人データ	統計情報（非個人情報）
	知的財産（営業秘密を含む）保護	営業秘密	営業秘密	営業秘密	営業秘密
	…	…	…	…	…
開示範囲		X 社内[19]	X 社内	X 社内	X 社内
利用目的		• 売買契約の履行 • 各種アフターサービスの実施 • 商品企画、開発	左記と同様	左記と同様	広報活動の効率化
データ管理主体		各物理店舗	各物理店舗	情報システム部門	情報システム部門、マーケティング部門
データ権利者		購買者、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

「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

[19] 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。

タが個人情報保護法における「個人関連情報[20]」、「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[21]。

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.1-4 「属性」の提示方法の例

[20] 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。

[21] 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。

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。*
- *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.1-4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[22]。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。

[22] 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。

	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。
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。

ー 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
ー 「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[23]」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[24]。

- 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

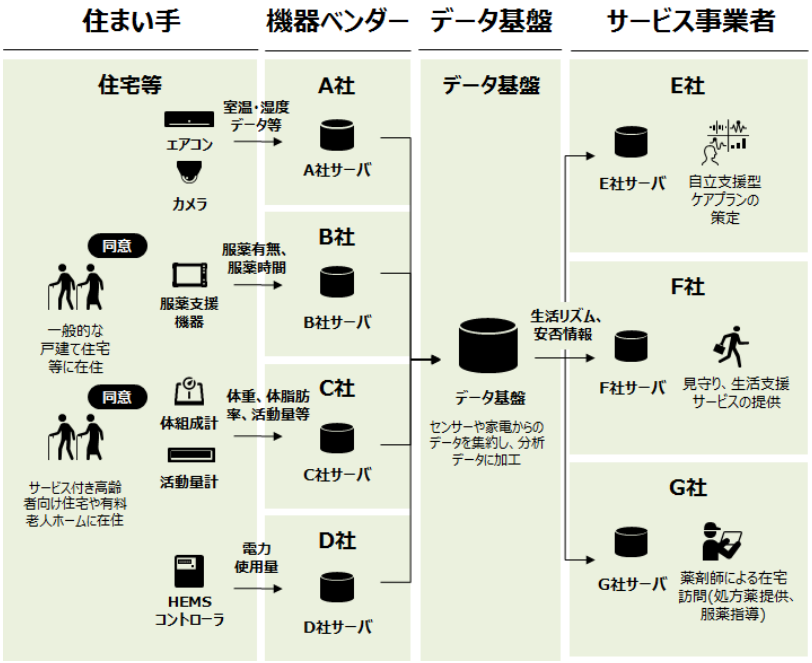
---

[23] 『「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）

[24] 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。

についてあらかじめ同意を取得しているものとする。

- 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、取り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。

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

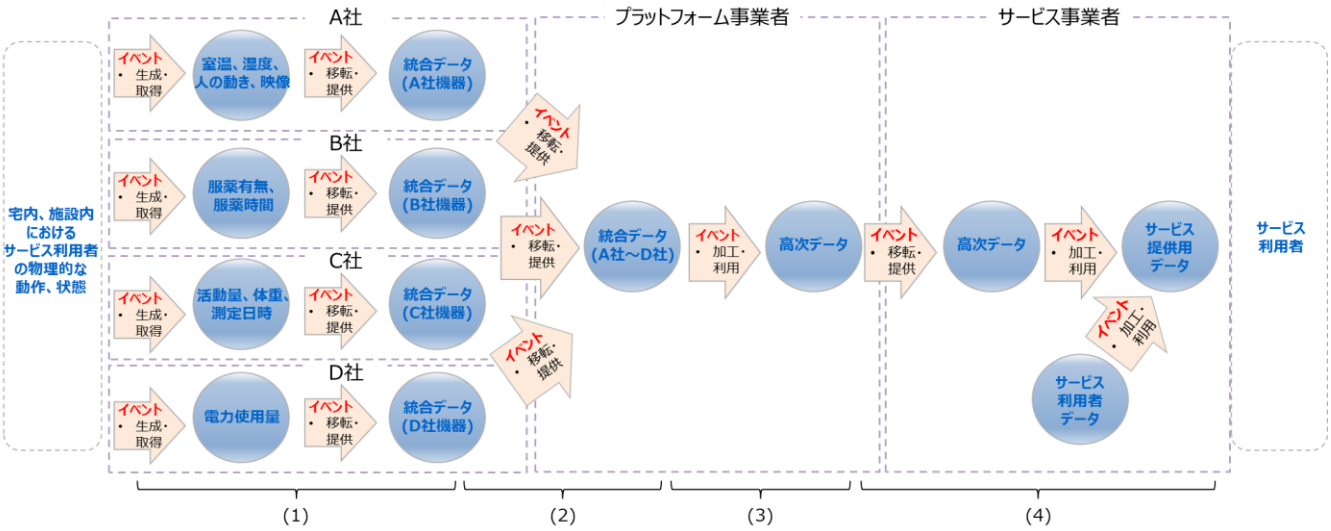
製造・販売者	名称	収集データ
A社	エアコン	室温・湿度情報
	電波センサーによる見守りシステム	ベッド上の呼吸有無・活動状態（動

		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。



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）

A-2-2 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、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： 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[25]。「サービス提供用データ」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。当該データは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ため、各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

[25] 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。

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[26]。

- 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[27]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

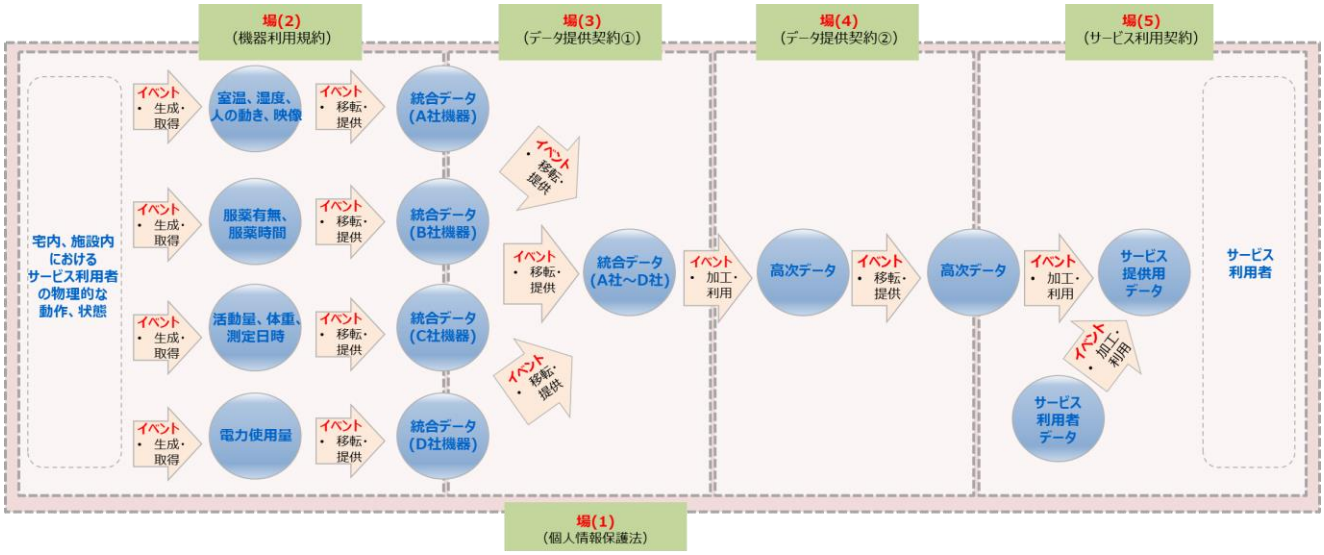
[26] 具体的な規定等については、「個人情報の保護に関する法律についてのガイドライン（通則編）」の「3-4-3 第三者に該当しない場合（法第 23 条第 5 項・第 6 項関係）」等を参照されたい。

[27] 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。

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））
  - ー　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
  - ー　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
  - ー　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その他の成果物の取扱いはいかなるものか
- 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））
  - ー　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
  - ー　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
  - ー　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の成果物の取扱いはいかなるものか

（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しい。



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り扱うことから、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			○	○	○

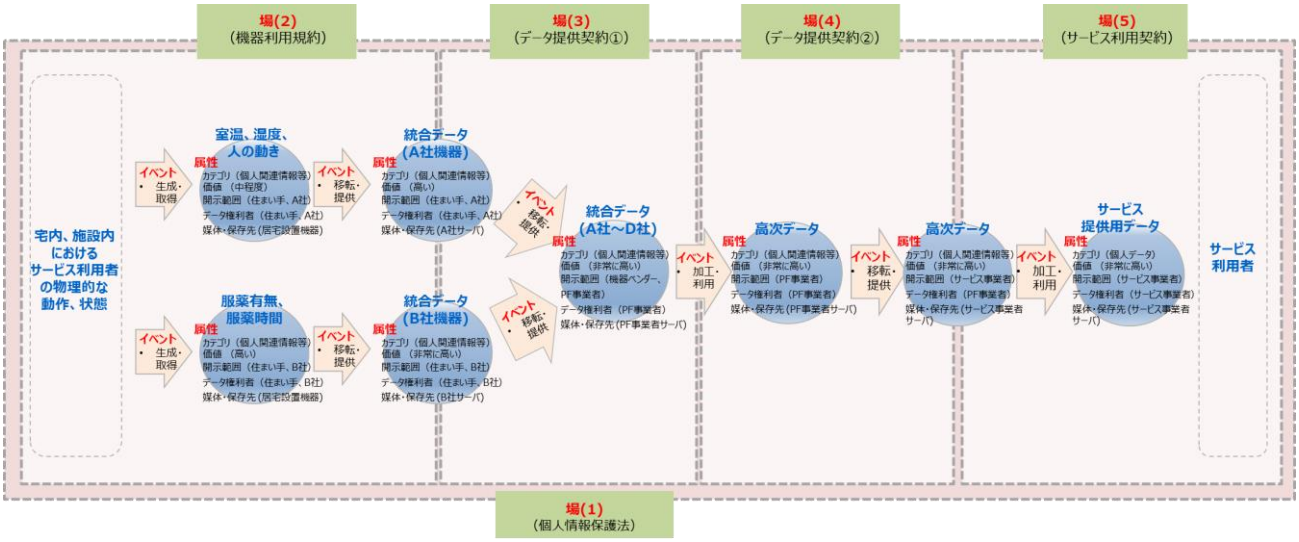
本ユースケースにて取扱われるデータの多くは個人データ又は個人関連情報等に該当する。機器から収集したデータは、別途利用者データ等と突合されない場合は「カテゴリ」が個人関連情報等に該当すると考えられるが、第三者提供先において個人データとなることが想定されるかどうか、その場合に本人同意が得られていることが確認できているかどうかが重要となるため、後述するように、上記に示した属性項目とは別途同意の取得状況等が管理されていることが望ましい。上記の事項を考慮して具体化した本ユースケースで取り扱うデータがとり得るパラメータの例を以下に示す。

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[28]（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

[28] 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。

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。



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	● 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。

	を含む）保護	
	・・・	

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[29]。

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[30]。

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

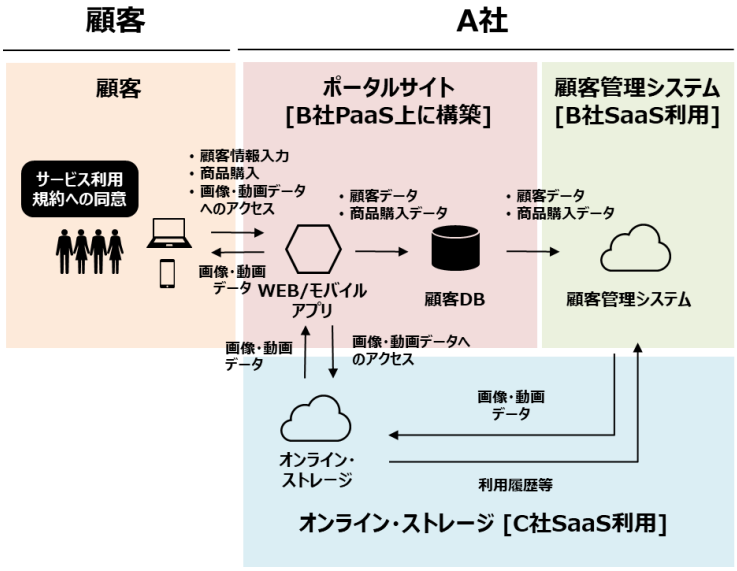
---

[29] 『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　）

[30] 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。

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[31]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。

[31] 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[32]：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[33]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。

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[34]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[35]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[36]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

---

[32] 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)

[33] 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)

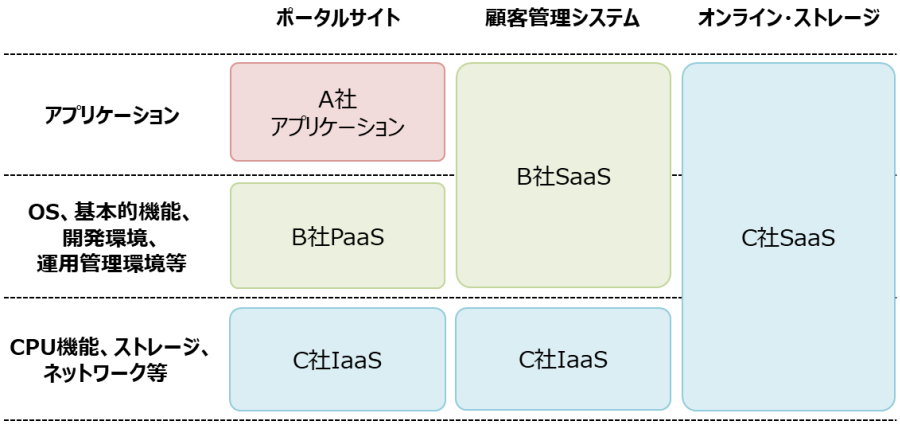
[34] サービスモデルの分類を定義する主な文献として、米国国立標準技術研究所（NIST）「NIST によるクラウドコンピューティングの定義」や各府省情報化統括責任者（ＣＩＯ）連絡会議決定「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等を参照

[35] 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」

[36] 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。

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。



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

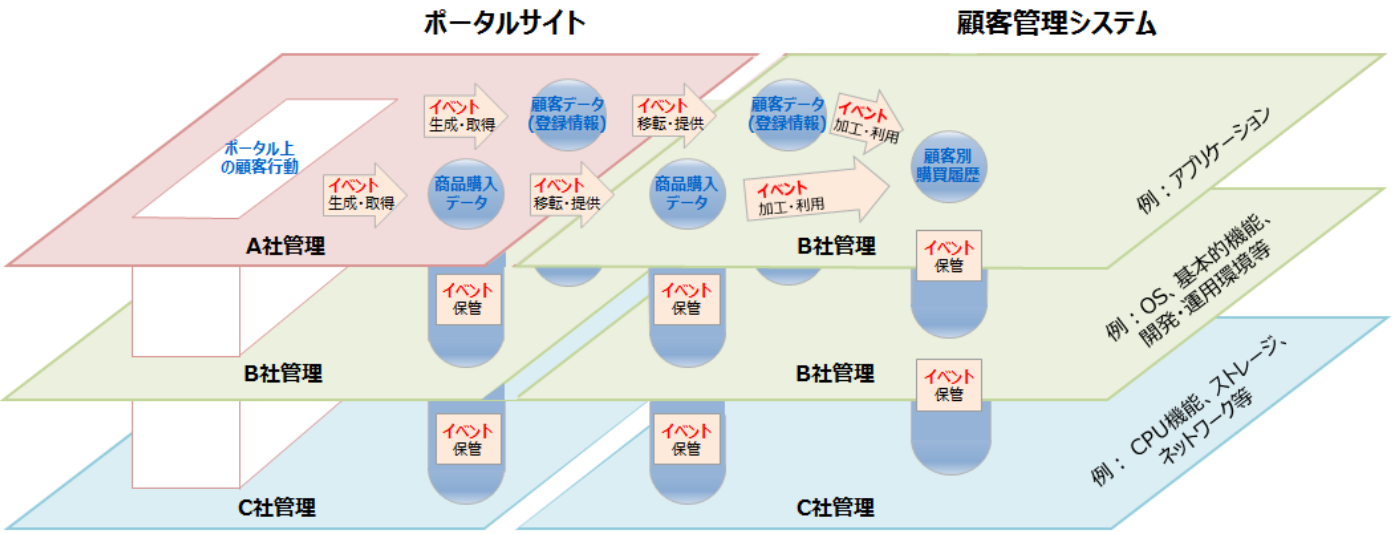
A-3-1 STEP 1　データ処理フロー（「イベント」）の可視化

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[37]、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り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）、

---

[37] 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り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、個人データを取り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り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、個人データを取り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］

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。

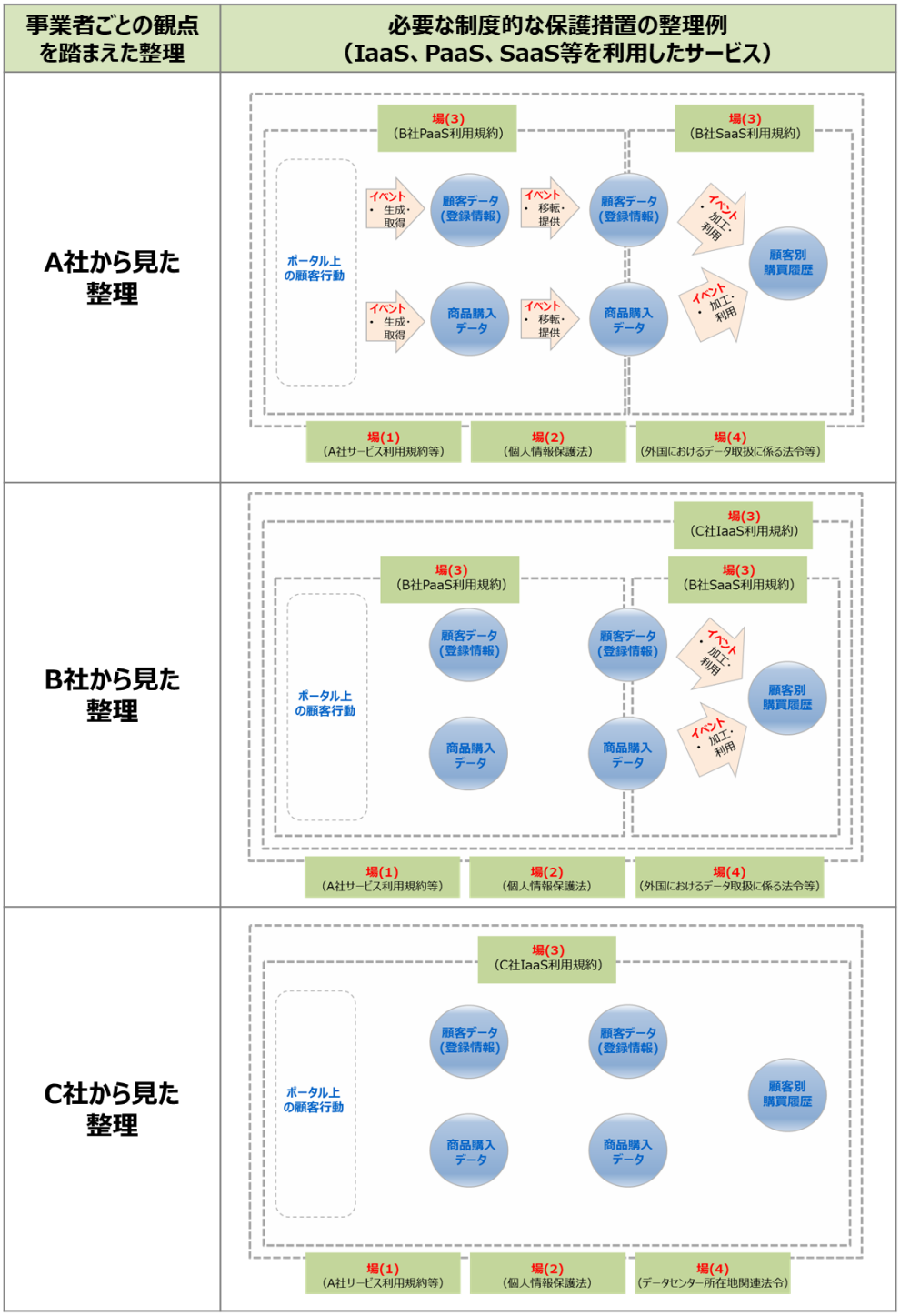
（4）データセンター所在地関連法令（外国におけるデータ取扱に係る法令等）：

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[38]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

[38] 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。

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。



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）[39]

[39] 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・動画データを取り扱うことから、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」[40]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

[40] 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

を取り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[41]	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

[41] 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り扱う。「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。

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。
	・・・	

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ウドサービスプロバイダが個人データを取り扱わないことを契約で取り決める場合は、自社が取り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り扱う場合に該当する場合[42]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。なお、保有個人データを外国で取り扱う場合には、「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ある。

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

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、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

[42] 外国にある支店・営業所に個人データを取り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り扱う場合に該当する。
https://www.ppc.go.jp/files/pdf/2109_APPI_QA_4ejj3t.pdf

構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[43]。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。

---

[43] 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

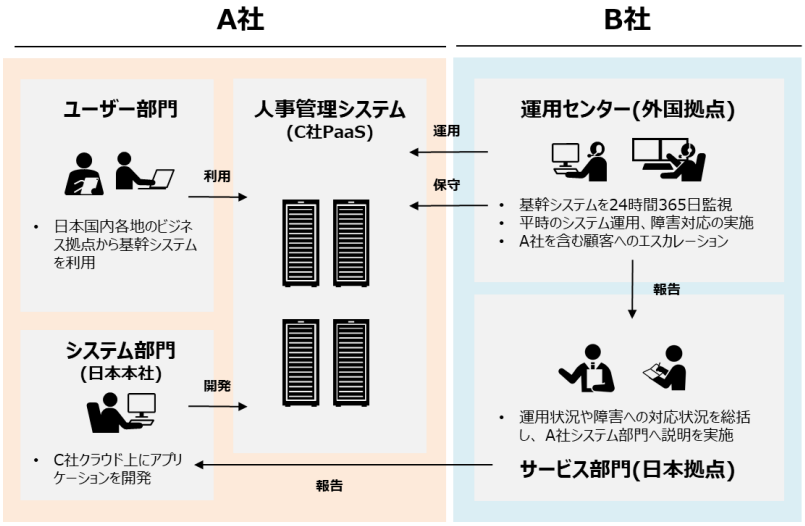
デジタルトランスフォーメーション（DX）の実現等、デジタル技術の高度な活用を通じた事業等の変革の重要性が社会的に認められている一方で、高度な専門性を必要とするITシステムの開発や保守、運用等の業務に対して、自社で人的リソースを確保しそれらを内製化するのが困難なケースが広く見られる。そのような場合、長期的には自社でリソースを確保することも志向しつつ、かかる業務を適切に外部委託することで、ユーザー事業者は質の高いサービスを享受しつつ、それ以外の業務に対するリソースを確保しやすくなるとされている。さらに、IT関連のアウトソーシングに関しては、従前から事業のグローバル化への対応やコスト削減等の観点から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

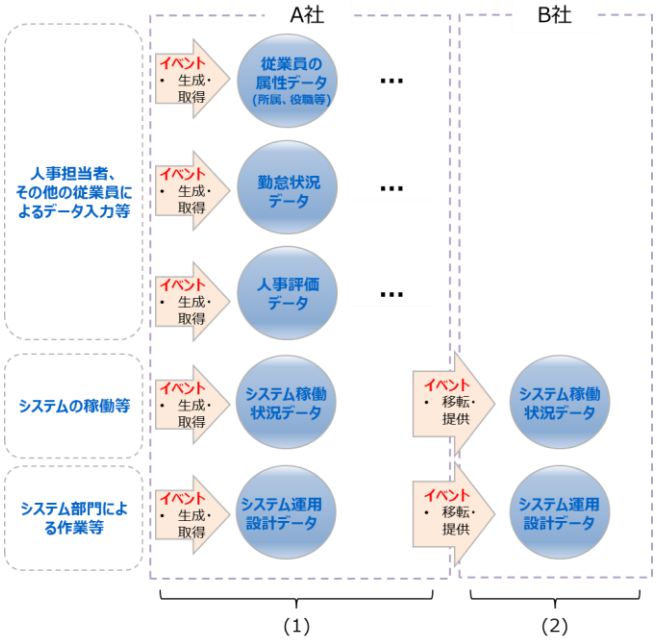
本ユースケースにおけるデータ処理フローは図A-3.2で示すように、以下のプロセスにより構成される。

(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[44]。また、上記の一連のシステム利用を通じて、システ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

[44] 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。

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り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[45]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り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[46]。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[47][48]。

（2）輸出管理関係法令[49]：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

---

[45] 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）

[46] 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

[47] 同 Q7－54

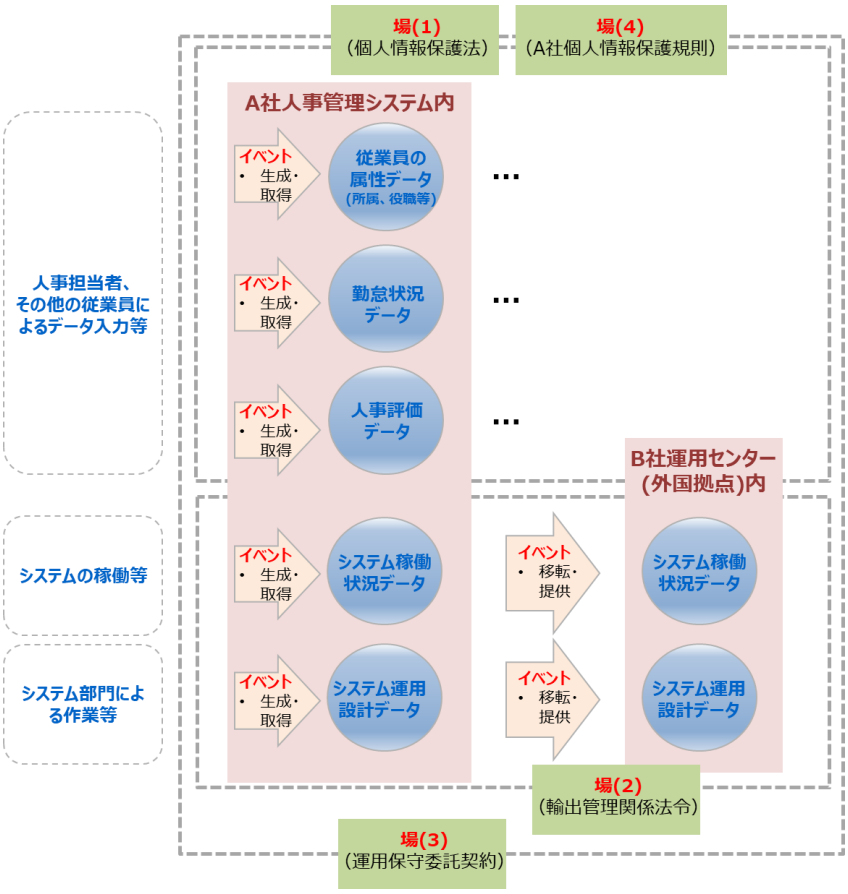
[48] B 社や C 社が契約上個人データを取り扱わないこととなっている場合、個人情報取扱事業者となる A 社は、外国において個人データを取り扱うこととなるため、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理措置の一環として、クラウドサービスプロバイダ（ここでは B 社）が所在する外国の名称及び個人データが保存されるサーバが所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く必要がある。それが困難な場合、サーバが所在する外国の名称に代えて、①サーバが所在する国を特定できない旨及びその理由、及び、②本人に参考となる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）

[49] 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。

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り扱うことから、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[50]。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	• 対象システムの運用、保守業務の実施 • 障害対応の実施	• 対象システムの運用、保守業務の実施 • 障害対応の実施

[50] 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

	• 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	• 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	
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
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[51]。

[51] 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[52]。

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。

[52] 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）[53]

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得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・利用等に関わり得る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て、追加の脅威類型（マルウェア感染、不正改造、誤使用[54]、システム等の不具合、自然災害等）を含めて提示している[55]。

[53] 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

[54] 「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。

[55] 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	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

		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。		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
	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	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

		設備や機器が一時的に停止する。		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
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
	偶発的	アプリケーションやデータベース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
	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	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

		又は権利元に損害を加える目的でデータが使用される。		
	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

			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
	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・システムが外部から不正アクセスされ、データが漏えいする。	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
				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	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

		閲覧できるようになっている。		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
	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	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

		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。		
	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) ・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 ・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 ＜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 ・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	生成、取得、	・CPSF Ver.1.0 CPS.RA-1, CPS.RA-2, CPS.IP-10, CPS.MA-1,

行	移転・提供、加工・利用、保管	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

		・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、	・CPSF Ver.1.0 CPS.CM-3

	加工・利用	・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＞ ・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） ・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	保管	＜より詳細なガイドライン＞

人データの訂正・利用停止等		・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合の秘密管理性の確保	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（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	-