資料４

「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

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当たっては、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するような、新たな価値を創造する活動が加速度的に拡がっている。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

---

[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。

[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当たっては、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および、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当たって、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始めから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

[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。

●データ交換のプラットフォームサービスを提供する者

●データ交換プラットフォームとなるシステムの設計・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、誰が権利を行使しう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

エ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。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、STEP1～3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STEP3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STEP1に戻って当該必要な「イベント」を追加し、その状態でSTEP2やSTEP3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STEP4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。

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当たっては、「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当たっては、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、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。

  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。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、移転的な要素も含むものであり、リスクを洗い出すにあたっては移転的な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、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、ネットワーク上での盗聴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、ある特定の移転・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つの単位で整理することとする。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。それぞれの考慮すべき事象やリスクは下記のとおり整理できる。

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り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

なお、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。データはライフサイクルの様々な段階において、ネットワークに接続されたストレージ機器・サービスや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や、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、データセット全体について、完全に使用不可能な状態とすることを指す。例えば、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・地域間およ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や、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。このように、「場」の設定は個別の事情によるところが大きく、一律に設定方法を提示することは困難である。

「場」の設定を行うに当たって、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、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。

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

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。価値の算定に当たっては、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。

  注：パブリックコメント開始の前後で、記載を充実させる予定。

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当たっては、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合意形成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当たっては、既存の規格等を参照いただきたい。主な規格は次の通り。

＜リスクへの対応＞

ISO31000

＜各主体のデータ管理＞

DMBOK

ISO27001, 27002

＜各イベントのセキュリティ対策要件＞

SP800-88(廃棄関係)

注：パブリックコメントと並行して、記載を充実させる予定。

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、その際、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プライバシーシールドを根拠として行おうとする場合、米国においては、「場」が米国の各種法制度に基づいたものに変化している。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「属性」に関して、データ管理主体の変化の他に、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。判決文によれば、この「属性」の変化がGDPR上の保護と実質的に同等とは認められないと判断された根拠となっている。したがって、今後、欧州から米国への移転・提供に当たって、欧州委員会が認めた標準的契約条項（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ことになる。

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。

添付A.　ユースケース

（候補例）

・POSデータの分析（第3回TF資料より）

・高齢者生活支援事業の提供（第3回TF資料より）

・IaaS、SaaS、PaaS等を利用してサービスを提供する例

・国内で提供するサービスに関して、海外に開発等を実施する例

添付B.　イベントごとのリスクの洗い出しのイメージ（第三回TF資料P38などを参照）

注：添付A,Bはパブリックコメントと並行して作成予定。