資料５

協調的なデータ利活用に向けたデータマネジメント･フレームワーク

適用手順書

Version 1.0

目次

変更履歴

Version	変更年月日	変更箇所	変更内容
1.0	2022/5/24	-	新規作成

1. 「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」の基礎情報

1.1 目的

本文書が参照する「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」(以下、DMF)は、バリュークリエイションプロセスを通じた付加価値創出を支援するため、主体間を転々流通するデータの信頼性を確保するための考え方やプロセス等を整理したものであり、将来的な事業者による活用が期待されるものである。

ここで、バリュークリエイションプロセスとは「様々なモノやデータが動的につながって構成される付加価値の創造活動」であり、様々な組織、システム、サービス等が関与するマルチステークホルダーから構成されるものと考えられる。DMF は、このような複雑なプロセスにおいて利活用されるデータのライフサイクル全体を捉え、その全体に渡り十分な信頼性を確保するために活用されることを念頭に置いている。

本文書は、DMF に基づいたリスクアセスメントを実施しようとする事業者を対象に、かかる活動の手順を示すものである。

＜参考情報＞

- 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
  (https://www.meti.go.jp/policy/netsecurity/wg1/DataManagement-Framework.pdf)

1.2 データマネジメントのモデル

DMF 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、「属性」、「場」、「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。DMF の 2-2 詳細編では、3 つの要素の概要を以下のように記している。

- **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、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。

- **場**
  「場」はデータに対して特定の規範を共有する範囲と定義される。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変動し得る。「場」は例えば、パーソナルデータの保護、知的財産(営業秘密を含む)保護、機微技術管理、適切な社会機能の維持等の観点で整理され得る。

- **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り、「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。

DMF における「データマネジメント」とは、「属性」、「場」、「イベント」という要素を考慮しつつ、対象となるデータの利活用プロセスの全体を正確に把握し、取扱われる個々のデータや適用される規律等の性質を踏まえて細やかなリスク管理を実施するものと捉えることができる。

2. 適用手順（概要）

DMF 適用の目的は、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、データの利活用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にある。その際、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。(概要は、DMF 2-1-2 リスク分析手順 を参照されたい。)

1. データ処理フロー（「イベント」）の可視化 [3-2 にて詳述]
2. 必要な制度的な保護措置(「場」)の整理 [3-3 にて詳述]
3. 「属性」の具体化 [3-4 にて詳述]
4. 「イベント」ごとのリスクの洗い出し [3-5 にて詳述]

3. 適用手順（詳細）

3-1 対象とするデータ利活用プロセスの特定

DMF の適用対象とするデータ利活用プロセスの範囲とその概要を特定する。概要の中では、対象となる利活用プロセスに関わる「主体」(例：サービスの利用者/提供者、社内の関係部署)や取扱われる「データ」及び、「利用環境」(例：端末、サーバ、ストレージ、ネットワーク等)を特定する。この検討を通じて、「どのような情報が、どこからどこに、どのような手段を介してやりとりされるのか」という「データの流れ」を把握することができる。

＜作成にあたっての参考情報＞

- DMF 添付 A 各ユースケース冒頭部における「対象プロセスの概要」

3-2 データ処理フロー（「イベント」）の可視化

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、手順としては、対象プロセスにおいて取り扱うデータを一覧化し、対象プロセスにおけるデータ処理フローに沿って、リストに含まれるデータ間の関係を整理するという順でフローの可視化を行う。

記法としては、DMF において強調されている以下の事項に注意する。

- サーバや端末等のシステム構成要素ではなく、そこで取扱われるデータを中心とした整理を行う。
- データやそれを取扱う環境に量的・質的な変化が生じる箇所を「イベント」として識別する。ここで、「量的・質的な変化」の例、識別され得るイベント類型として以下が想定される。

  - ✓ データの量的変化 (例：複数チャネルから取得したデータの集約) [生成・取得、移転・提供]
  - ✓ データの法的カテゴリや価値の大小を変更する処理(例：個人データの匿名加工、仮名加工) [加工・利用]
  - ✓ データへの実質的な管理権限を有する主体の変更 (例：データの第三者提供) [移転・提供]

✓ データ保管場所の変化、特に適用される法令やポリシー等に変更が生じるもの [移転・提供]

本段階のアウトプット例を図１に示す。図１では、個々のデータを円形、イベントをブロック矢印で記述しているが、事業者における実際の適用にあたって、これらの様式は強制されるものではない。

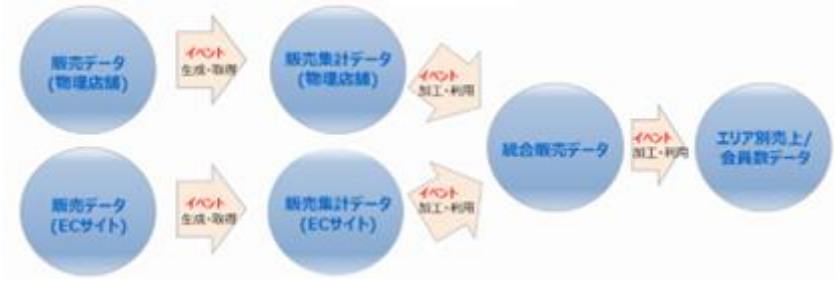

図１ データ処理フローの可視化(例)

＜収集しておくべき情報とその情報源(例)＞

・ 対象とするデータ利活用プロセスにおいて取り扱うデータの一覧 (情報源の例：情報資産管理台帳)
・ 上記データに対して実施する処理の流れ (情報源の例：設計ドキュメント、概念設計)

＜実施手順＞

1. 対象プロセスにおいて取扱うデータをリスト化する。
2. 対象プロセスにおけるデータ処理フローに沿って、リストに含まれるデータ間の関係を整理する(例：サービス利用者がスマホアプリ上で入力して「生成・取得」された個人データ A が、匿名加工処理という「加工・利用」を通じて、匿名加工情報 B へと遷移する)。当該フローには典型的に、データの生成・取得、加工・利用、移転・提供等が含まれ得る。

＜作業成果物が満たすべき要件＞

・ 対象のデータ利活用プロセスで取扱われるデータが漏れや重複なく記載されている
・ 上記データを対象とするイベントが、「生成・取得」「加工・利用」「移転・提供」「保管」「廃棄」の区分に沿って、漏れや重複なく記載されている

＜作成にあたっての参考情報＞

・ DMF 添付 A 各ユースケースにおける「STEP 1 データ処理フロー（「イベント」）の可視化」

3-3 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」(必要な制度的な保護措置)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も想定される。

適用にあたっては、いかなる規範が「場」として識別されるかという点が第一に検討されるべきである。「データフローの可視化」において識別された各データに対して、以下の観点から各「場」に係る簡易的な該非の判断を行うことが望ましい。

・ パーソナルデータの保護（関係法令の例：個人情報保護法(日)、GDPR(EU)）

✓ (日本法の適用を想定する場合) 対象のプロセスにおいて、個人データ、仮名加工情報、匿名加工情報、個人関連情報等の、個人情報保護法の規律が適用される種類のデータが含まれるか。

・ 知的財産(営業秘密を含む)保護（関係法令の例：不正競争防止法(日)、著作権法(日)）

✓ (日本法の適用を想定する場合) 対象のプロセスにおいて、不正競争防止法において定義される営業秘密、限定提供データ、著作権法の定める著作物等として保護すべき種類のデータが含まれるか。

・ 機微技術管理（関係法令の例：外為法(日)、2018 年輸出管理改革法(米)）

✓ 対象のプロセスにおいて、外為法または外国の輸出管理関連法令にて規律の対象となるデータ、輸出行為に相当する種類のイベントが含まれるか。

・ 適切な社会機能の維持（関係法令の例：金融商品取引法(日)、秘密保持契約）

✓ 対象のプロセスにおいて、金融商品取引法におけるインサイダー取引関連規定、その他秘密保持契約(NDA)等により取扱いが規律されるデータが含まれるか。

適用される「場」を特定した後、それが適用される範囲を 3-2 にて特定したデータフローの範囲内で識別する。本段階のアウトプット例を図 2 に示す。図 2 では、個々の「場」とそれが考慮される範囲を四角形(枠線は点線)で記述しているが、事業者における実際の適用にあたって、これらの様式は強制されるものではない。

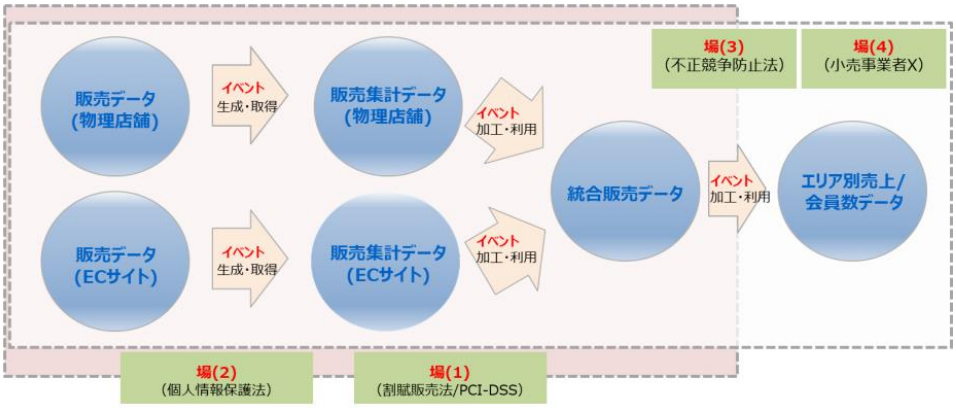

図 2 必要な制度的な保護措置の整理(例)

＜収集しておくべき情報とその情報源(例)＞

・ データ保護に関連する法令、それらの適用範囲及び、事業者に適用される規律（情報源の例：各種法令、ガイドライン文書）

＜実施手順＞

1. 「場」に相当する法令の規定、その他の規範を識別する。
2. 各「場」が適用される範囲を識別する。

＜作業成果物が満たすべき要件＞

・ 対象のデータ利活用プロセスに適用され得る法令、その他の規律が漏れや重複なく記載されている。

・ 識別された法令、その他の規律が適用され得る範囲がデータフロー上で記載されている。

＜作成にあたっての参考情報＞

・ DMF 添付 A 各ユースケースにおける「STEP 2 必要な制度的な保護措置（「場」）の整理」

3-4 「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。

属性としては、ユースケースの性質に応じて様々な項目が識別され得ると考えられるが、様々なケースにて共通的に適用し得ると考えられる主な項目の概要及びパラメータの例を以下に示す。

・ カテゴリ

3-3 にて特定される「場」と連動して、例えば以下のようにデータの法令等に係る位置づけ及び、管理上必要と考えられる措置を特定する。

- パーソナルデータの保護：個人データ/仮名加工情報/匿名加工情報/個人関連情報 等
- 知的財産(営業秘密を含む)保護：営業秘密/限定提供データ 等
- 機微技術管理：規制対象の技術情報 等

・ 開示範囲

関連する法令や契約による取決めや組織内規則も含め、データに定められている開示範囲(事業者、部署、担当者)を整理する。その際、3-3 にて特定される「場」との関係で考慮すべき観点の例を以下に挙げる。

- 対象データが個人情報等に該当する場合
  技術的安全管理措置の一環として、担当者及び取扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御が行われていると認められるよう開示範囲を設定する。
- 対象データが営業秘密等に該当する場合
  対象データが「秘密として管理されている」ことを確保するため、合理的と考えられる秘密管理措置の実施及び、それに対応する開示範囲を設定する。
- 対象データが契約上の規律を受ける場合
  契約等に基づいてデータを取扱ううえで、許可のない第三者への提供を認めない等の趣旨の規定が存在する場合、それに対応するよう開示範囲を制限する必要がある。

・ 利用目的

個人情報やライセンス等の取扱いにおいて、あらかじめ利用目的に制限が設けられている場合、当該目的をパラメータとして明確にしておき、後の利活用においても許可された目的からの逸脱が生じないように継続的に管理しておく必要がある。

・ データ管理主体

情報資産管理台帳等に既に規定されているもの等を参照し、対象データの管理責任者(事業者、部署、担当者)を特定する。データが複数の事業者間で共有される場合、対象のデータに対してどの事業者がいかなる管理上の責任を有しているかが不明確になりやすいと考えられる。かかるケースにおいても、事業者間の契約やサービス等の利用規約等の規定に基づき、関係者間での責任範囲の明確化を図ることが望ましい。

・ データ権利者

データ管理者とは別に、対象データに対して権利・利益を有している者(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)及びそれらに関して生じ得る措置を特定しておくことが望ましい。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等がそれらに該当し得る。

・ 価値(重要度)

機密性、完全性、可用性の観点から生じ得る影響度等を考慮し、対象データの事業上の価値(重要度)を特定する。その際、ここでパラメータとして設定されるものを、組織内の情報資産管理等で既に整理されている重要度等と整合させることが望ましい。設定されるパラメータの例は以下の通り。

－ 高/中/低 等

・ 媒体・保存先

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。媒体・保存先として、設定されるパラメータの例は以下の通り。

－ 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

・ 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、関連して必要な措置を特定する。

本段階のアウトプットの例として、(1) 図２に示したフロー図の各データ(円)内に各属性項目及びパラメータを記述する方法、(2) 表形式でデータごとに属性項目に対応するパラメータを記述する方法(表１)等の様式が想定されるが、これら以外の様式の採用を否定するものではない。

表１ 「属性」の具体化方法(例)

属性項目		データＡ	データＢ	データＣ
カテゴリ	パーソナルデータの保護	個人データ	個人データ	匿名加工情報
	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	・・・	・・・	・・・
・・・	・・・	・・・	・・・

＜収集しておくべき情報とその情報源(例)＞

・ データの重要度、管理責任者、媒体・保存先、利用期限等 (情報源の例：情報資産管理台帳)

・ 対象プロセスにおける各データに対する事業者間の責任範囲、データの開示範囲 (情報源の例：事業者間の契約、サービスの利用規約等)

＜実施手順＞

・ 対象のプロセスにて取扱われるデータに関連して、管理すべき属性の項目を一覧化する。

・ 各データについて、上記の事例を参考に各項目のパラメータを特定する。

＜作業成果物が満たすべき要件＞

・ 上述したものを中心に、洗い出されているべき属性項目が検討され、識別されている。

・ 識別された各属性項目にもれなくパラメータが記入されている。

＜作成にあたっての参考情報＞

・ DMF 添付 A 各ユースケースにおける「STEP 3 「属性」の具体化」

3-5 「イベント」ごとのリスクの洗い出し

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する。その際、機密性(例：データ漏えい)、完全性(例：データ改ざん、破壊)、可用性(例：システム停止)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(例：パーソナルデータの保護、知的財産の保護)も踏まえてリスクを洗い出すことが有効である。イベント類型(生成・取得/加工・利用/移転・提供/保管/廃棄)ごとに想定されるリスクの事例については、DMF 添付 B における「B-2 イベントごとのリスクの洗い出しのイメージ」を参照されたい。

これまでのフレームワーク適用プロセスを通じて、適用主体は自身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。具体的な改善策は、特定されるリスクの種類やその影響の度合い等に依存するが、取扱われるデータの種類や環境の性質に応じて、以下を例とする様々なガイドライン等が参照され得る。

・ サイバーセキュリティの確保に資する対策

CPSF、ISO/IEC 27001:2013、ISO/IEC 27002:2022、NIST SP 800-53 等

・ パーソナルデータの取扱いに係る対策

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(外国にある第三者への提供編)、個人情報の保護に関する法律についてのガイドライン(仮名加工情報・匿名加工情報編) 等

・　知的財産(営業秘密を含む)保護に資する対策
　　営業秘密管理指針、限定提供データ管理指針、秘密情報の保護ハンドブック　～企業価値向上にむけて～ 等

＜収集しておくべき情報とその情報源(例)＞
・　過去に発生したインシデント等に関する情報 (情報源の例：セキュリティやデータ保護等に関する情報を取扱う各種メディア等)
・　特定された影響度の大きい、あるいは十分に対処されていないリスクに対処する対策に関する情報(情報源の例：取扱われるデータの種類や環境の性質に応じたガイドライン等)

＜実施手順＞
・　全体プロセスの中から、リスク特定の対象とするイベントを選択する。
・　選択したイベントにて想定されるリスクを、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から洗い出し、一覧化する。
・　特定したリスクを、想定される影響の大きさ、起こりやすさ、現在の対策状況等の観点から評価し、適用主体において優先的に対処すべきものを明確化する。
・　政府機関等から公開されているガイドライン等を参照し、上記リスクを管理するために必要な措置を識別し、実行する。

＜作業成果物が満たすべき要件＞
・　対象とするイベントにおけるリスクが、典型的に想定されるものも含め、網羅的に特定されている。
・　特定されたリスクが、影響の大きさ、起こりやすさ、現在の対策状況等の観点で評価され、優先順位づけされている。
・　上記の優先順位づけに基づき、ガイドラインの参照も伴いつつ、実施すべき対策が一覧化されている。

＜作成にあたっての参考情報＞
・　DMF 添付 A 各ユースケースにおける「STEP 4 「イベント」ごとのリスクポイントの洗い出し」

以上