経済産業省

（参考資料）
「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」骨子案の概要

令和３年７月

経済産業省 商務情報政策局
サイバーセキュリティ課

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

- これまでのタスクフォースでの議論を踏まえて拡張したデータマネジメントの捉え方を用いた「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮題）」の骨子案を作成。

<目次>

パブリックコメントと並行して作成予定

骨子案として取りまとめ

フレームワーク骨子案の概要：第3層の位置づけ

- 第3層においては**データが信頼性の基点**
  - Society 5.0において、サイバー空間におけるつながりが展開される場が第3層であり、そこでは物理特性に依存しないデータが付加価値を創造（バリュークリエイション）している。
  - データは基本的にシステムや組織に対して中立性を持つものであり、それが求められる規範等に則って適切に扱われることによって、自由に流通・活用される。
- データのライフサイクルには**様々な主体が関与**
  - 関与した主体による不適切な措置によって誤ったデータが流通し活用されることになれば、有害な結果をもたらすことにもつながりかねない。
- **データのライフサイクルは第3層の中に閉じるものではない。**
  - サイバー空間から発信されたIoTシステムへの動作指令が誤った内容であるならば、第2層における“転写”する機能の信頼性を確保することに成功していたとしても、IoTシステムはサイバー空間から届いた誤った指令を“正しく”転写して忠実に動作することで物理的な損害を発生させてしまうかもしれない。
  - データが生成される場所については第3層ではなく第2層に属する場合があり、第3層と第2層とを組み合わせることでデータ生成における信頼性が確保できる。（第2層TFで策定したIoT-SSFと連動）

フレームワーク骨子案の概要：データマネジメントの考え方の確立

＜データマネジメントの捉え方＞

- **データのライフサイクルの各工程において発生する様々な形の“関与”**

＜３つの視点＞

① データマネジメントについて確立した定義は存在しない

- 他の機関等において整理されたデータマネジメントの定義を持ち込むのではなく、CPSFを基礎としてセキュリティ対策を検討するために必要なデータマネジメントの考え方を示す。

② データを軸に置く

- データがライフサイクルの各工程においてどのような関与を受けるかという視点で整理すべき。

③ 関与する主体は同一・単一の主体に限られるものではない

- データマネジメントは複数の主体による協同的活動**（Collective Action）になる**ことを排除しない。例：クラウドサービス

フレームワーク骨子案の概要：本フレームワークの目的・想定読者

＜ 本フレームワークの目的 ＞

（as isの対策）

- データを軸に置き、**データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し、**そのセキュリティを確保するために、ガバナンスを含めた必要な措置を**ステークホルダーが協調して実施する**。
- 洗い出されたリスクへの措置はDMBOK等の既存文書を参照。

（to beの対策）

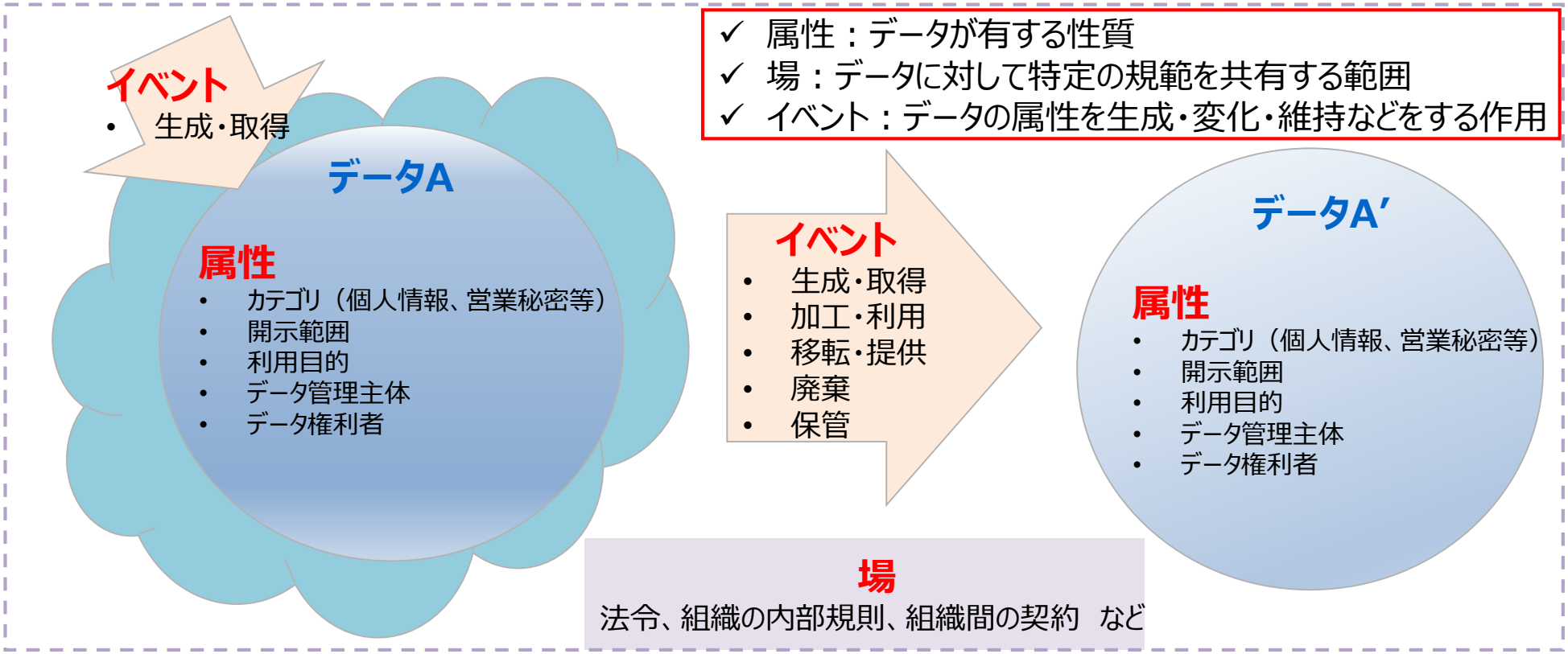
- データの流通を促進するために必要な条件を明確化。プロトコルの設計が容易に。
- 強い立場にあるシステムが**プロトコルのブラックボックス化によって「バンドル」することを難しく**させ、**オープン化された環境でデータ連携やシステムの組み合わせの自由を確保することを可能に**。
- 主体の在り方などを過度に考慮することなく、データに対して本来求められる要求事項を歪めることなく整理することが可能であり、**各国の制度間のギャップ分析**を行い必要な調整措置を明らかに。

＜ 本フレームワークの想定読者 ＞

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

フレームワーク骨子案の概要：データマネジメントのモデル化の概要

- データマネジメントを「**データの属性が場におけるイベントにより変化する過程を、ライフサイクルを踏まえて管理すること**」と定義。
- **「属性」「場」「イベント」の3つの要素はそれぞれが相互に影響**しあう関係。
- データの遷移による**データの変化に関する一定の予見可能性を確保、ステークホルダーの間で認識を共有しやすく**なる。
- 共通の理解に基づいてそれぞれの主体が実施すべき措置についての検討を進めることが可能となり、**ステークホルダー全体で適切なデータマネジメントを実施していくことができる環境を実現**していく。



フレームワーク骨子案の概要：リスク分析手順

- **下記の4つのステップに沿ってバリュークリエイションプロセスにおけるデータの状態を可視化**。
- 「属性」、「場」、「イベント」が相互に依存する関係にあることから、STEP1～3の**各ステップは不可逆的なものではなく、互いにフィードバックをかけながら検討されることが適切**。
- リスクの洗い出しに当たっては、機密性・完全性・可用性といったサイバーセキュリティに係る観点の他、各法制度等に係るコンプライアンスの観点でのリスクについても洗い出す必要。

STEP 1
データ処理フロー（「イベント」）の可視化

STEP 2
必要な制度的な保護措置（「場」）の整理

STEP 3
「属性」の具体化

STEP 4
「イベント」ごとのリスクの洗い出し

フレームワーク骨子案の概要：モデル化（「イベント」）～ 生成・取得、加工・利用 ～

- データの属性を生成・変化・維持などをする作用である「イベント」に関しては、**大きくは「生成・取得」「加工・利用」「移転・提供」「保管」「廃棄」の5つに区分することが可能**。
- 5つの「イベント」はそれぞれ重複する性質を持つ場合があり、目的に応じて適切に「イベント」を捉え、リスクの洗い出しを実施する必要（例：閲覧は加工・利用だが移転・提供の要素を含み得る）。

＜ 生成・取得 ＞

- バリュークリエイションプロセスにおいて、サイバー空間でやりとりされるデータは、**何らかの形で生成・取得されることによってそのライフサイクルが始まる**。
- サイバー空間とフィジカル空間が高度に融合し、フィジカル空間の情報が大量にサイバー空間に転写され、リアルタイムに共有されるようになると、サイバー空間のつながりにおけるデータの信頼性を検討する場合、従来はデータを管理する範疇に捉えられていなかった、**データの生成・取得に関わる機器・システムなどの信頼性についても検討する必要**。
  - 代表的なリスク：計測結果が実際と異なる、計測機器をなりすまされる等の転写の失敗など。

＜ 加工・利用 ＞

- データに**付加価値を生み出すための作用を加工・利用と捉える**。
  - ✓ 分析過程や保管されたデータセットから**データの一部の項目や要素、レコードなどを取り除く作用については、加工の一形態として捉える**ものとし、後述する廃棄とは区別する。
  - ✓ データを保有しない者が**データにアクセスする作用（閲覧）については、利用の一形態として捉える**ことが適切であるが、リスクを洗い出す際は**移転・提供の要素を考慮**に入れる必要。
  - 代表的なリスク：データの目的外利用、不適切な加工など。

フレームワーク骨子案の概要：モデル化（「イベント」）～ 移転・提供 ～

＜ 移転・提供 ＞

- サプライチェーンを動的に構成する場合、効果を最大限に引き出すためには**より自由にデータの移転・提供を実施できる環境にすること**、**リスクに対してより効果的に対応すること**が求められる。
- 特定の移転・提供事象について、国・地域、組織・ヒト、システム・サービス、機器という**4つの単位で整理**。
- **イベントをどの程度詳細に記述するかは、データフローの整理の目的に応じて調整する必要**。

単位	考慮すべき事項	単位ごとのリスク(例)
国・地域	データの移転・提供に関連する国・地域及び、当該国・地域におけるデータ保護関連の政策、法令、ガイドライン等	● データの移転元/移転先に相当する国・地域にデータ保護関連法令が存在しない又は内容として不十分な場合、移転元/移転先間における保護水準の不整合が生じる結果、移転先で移転元の保護水準が確保できない。
組織・ヒト	データの移転・提供の関係主体となる組織及びヒト、当該主体におけるデータ保護関連の方針、体制等	● 組織のセキュリティポリシーが存在しない又は内容として不十分な場合、データ移転に関わるステークホルダ間にてセキュリティ水準の不整合が生じる結果、移転先で移転元の保護水準が確保できない。
システム・サービス	複数の機器から構成され、データの移転・提供を実行するシステムと提供されるサービス	● システム・サービスにおけるセキュリティ実装が十分でないことにより以下のようなセキュリティ上のリスクが生じうる。 - ネットワーク上での盗聴 - 送信元/送信先のなりすまし
機器	データの移転・提供を実行するサーバ、IoT機器、ネットワーク機器等のデータを物理的に取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

フレームワーク骨子案の概要：モデル化（「イベント」）～ 保管、廃棄 ～

＜ 保管 ＞

- **保管は、他のイベントに付随して必ず生じる「イベント」**である。データはライフサイクルの様々な段階において、ネットワーク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。

＜ 廃棄 ＞

- 本フレームワークにおける**廃棄は、データセット全体を使用不可能な状態とすること**を指す。
- 同意に基づいて収集したパーソナルデータに関して、特定の個人が同意を撤回する等により、当該個人のデータをデータセットから除外する行為は、加工・利用の一形態として捉えるのが適切。
  - 代表的なリスク：廃棄すべきデータが残存して漏えいする、本来は廃棄すべきでないデータまで廃棄してしまうなど。

フレームワーク骨子案の概要：モデル化（「場」）

- 「場」は、それぞれの状況や関係する者の事情などによって適用される形態等が異なり、**一律に設定方法や形態が決まるものではない**。
- 例えば、「場」を構成する重要な要素の一つに法令等があるが、**「場」の設定を行うに当たって、必要な観点を漏らすリスクを低減**しながら検討するために、**下記のような4つのカテゴリから整理**。
- 4つのカテゴリは、「場」が、データに関して何らかの共通の取扱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**。

- **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

フレームワーク骨子案の概要：モデル化（「属性」）

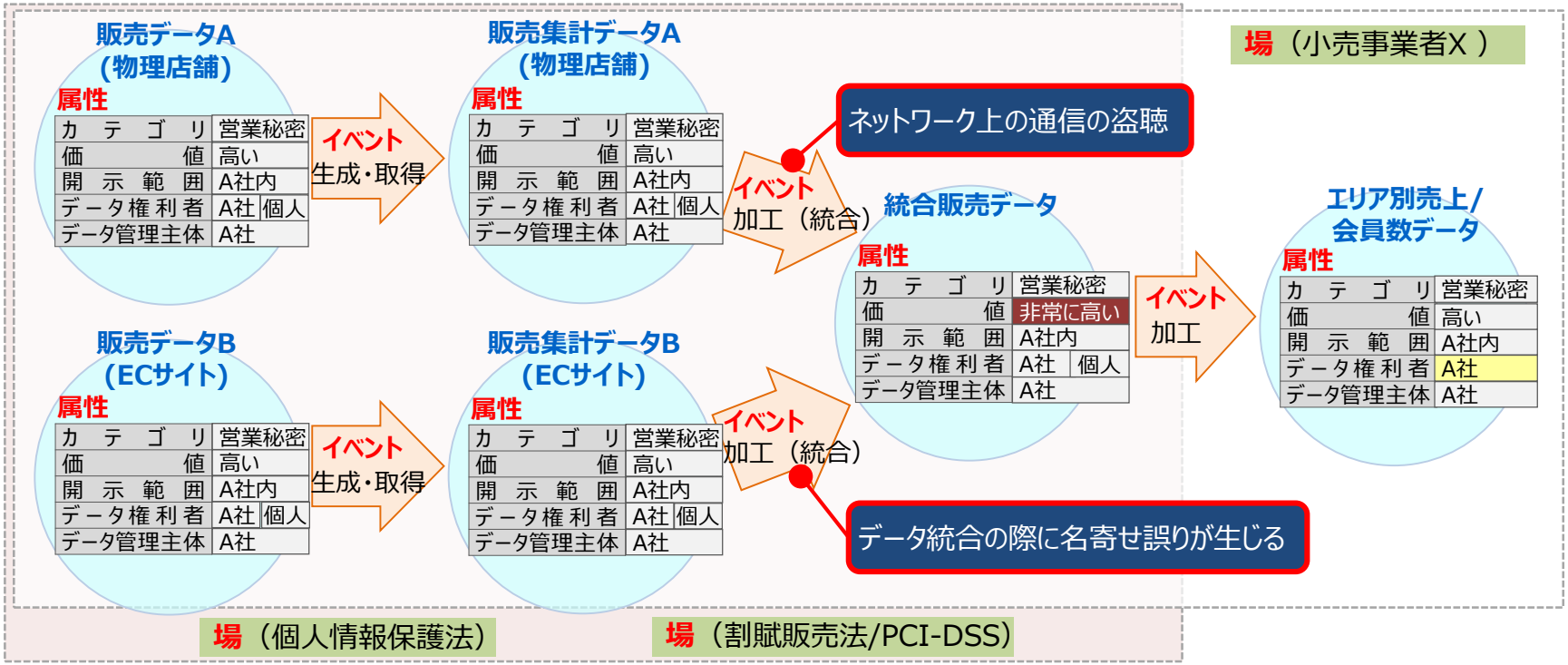
- 代表的な「属性」やパラメータ、整理のポイントを示す。
- 整理した「場」からデータに対する要求を検討し、関連する「属性」を適切に具体化することが重要。

- **<u>カテゴリ</u>**
  - 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。
- **<u>開示範囲</u>**
  - 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。
- **<u>利用目的</u>**
  - 個人情報やライセンスなど、法令等に基づいて利用目的に制限が設けられている場合、当該利用目的の範囲内で取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。
- **<u>データ管理主体</u>**
  - データに軸を置く本フレームワークにおいては、データに作用を及ぼす主体についても、データが転々流通する過程で移り変わるものであり、あくまで「属性」の一つとして整理する。
- **<u>データ権利者</u>**
  - データが個人情報である場合、企業の競争力に関わる場合など、データ管理主体とは別に、データに対して権利を有する主体が存在することがある。移転・提供が行われて別の主体がデータを取得した場合でも、データ権利者は当該主体の管理下にあるデータに対して引き続き権利を有すると考えられるため、管理主体が転々と移っていく過程でも、「属性」として管理する必要がある。

フレームワーク骨子案の概要：活用方法
～ サプライチェーンを構成するステークホルダー間での活用 ～

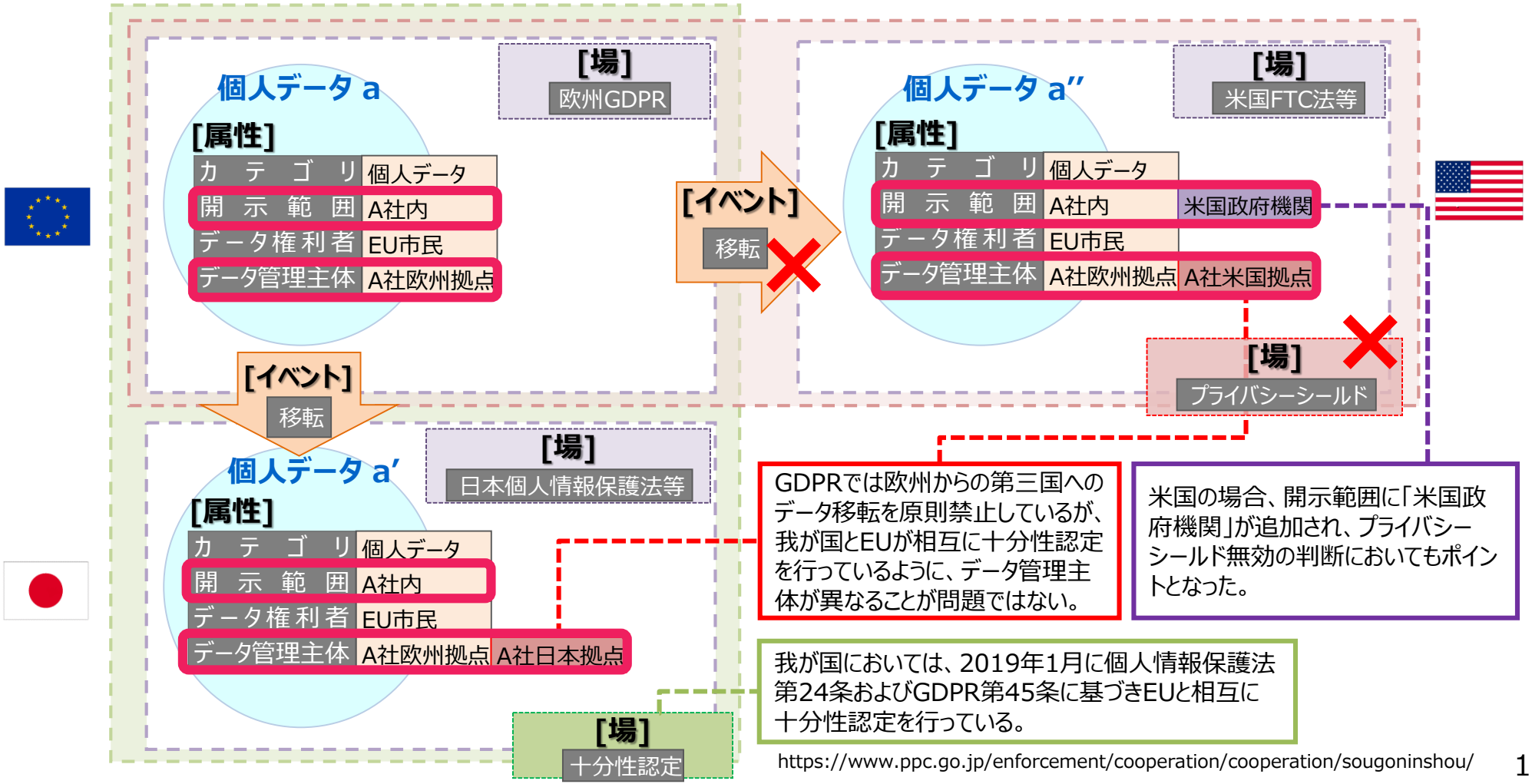
- バリュークリエイションプロセスに関わるステークホルダーの間で、データのライフサイクルの各工程においてリスクを可視化した上で、各主体がそれぞれ実施すべき対策を他の主体と合意形成しながら取り組むことにより、データの信頼性を確保することが期待される。
- 可視化されたリスクに対して各主体が実施すべきセキュリティ対策は、これまでに公表されてきた情報セキュリティに関する様々な国際標準等を参照。
- **将来的には経営者によるITガバナンス（デジタルガバナンス）の検討への活用も期待。**

小売業におけるPOSデータの活用事例



フレームワーク骨子案の概要：活用方法　～ルール間のギャップの分析 ～

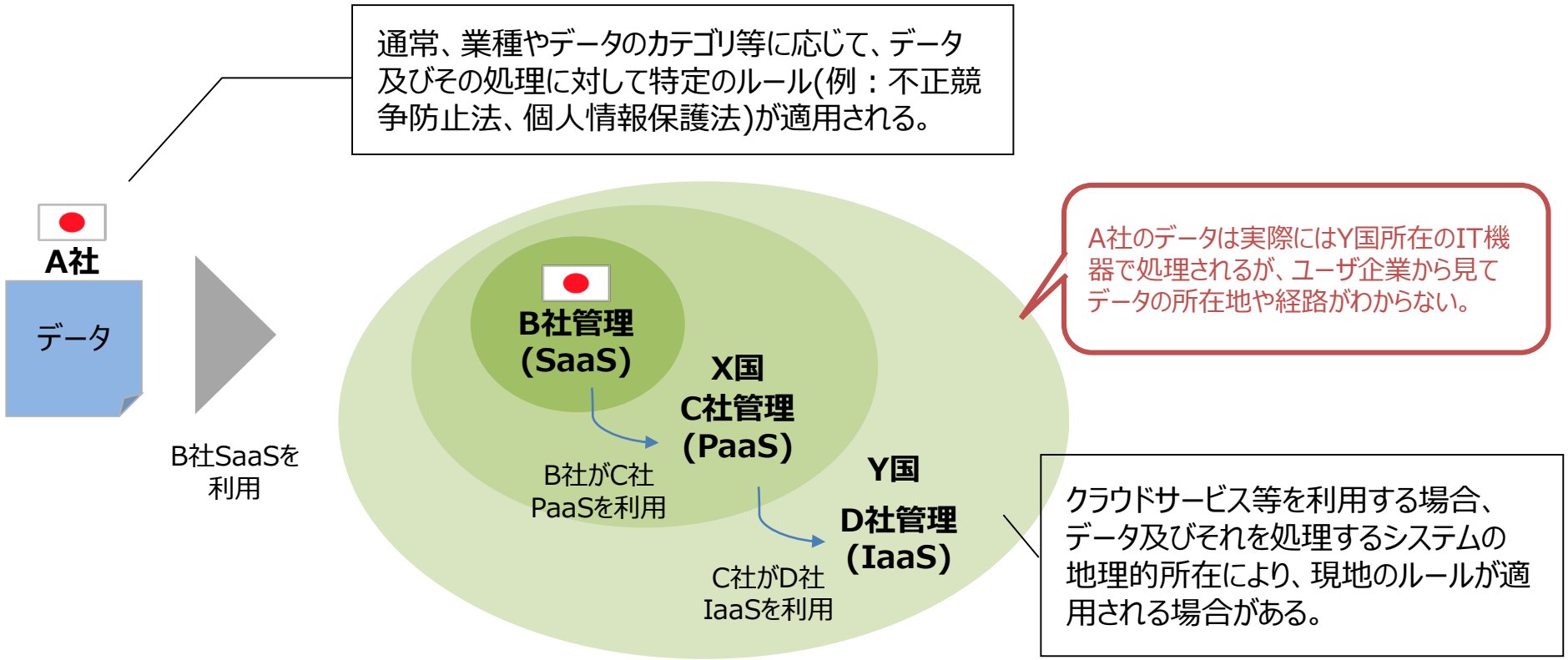
- 本フレームワークは、**データ管理に関わる制度間における、データのセキュリティの確保のために要求されている条件や措置の相違（ギャップ）を明確化するためのモデルとしての活用も可能**。
- データに関する**「場」や「属性」の変化を可視化することで、**データのセキュリティの確保のために**要求されている条件や措置の相違を把握**することにつながる。



https://www.ppc.go.jp/enforcement/cooperation/cooperation/sougoninshou/

（参考）システム構成の多層化・重層化によるデータマネジメントの複雑化

- クラウドサービスの利用の進展により、データが生成され価値を生む場所と実際にデータが処理される場所が異なることがあるなど、**<u>システムの多層化・重層化が進展している</u>**。
- システムの複雑性が増すほど、データが取り扱われる「場」がフィジカル空間と乖離することがある。



（参考）システム構成の多層化・重層化によるデータマネジメントの複雑化

- B社SaaSはC社PaaS上で、C社PaaSはD社IaaS上で稼働している場合等において、**A社がB社と契約してデータを保管する際**、A社から見たデータの保存先はB社SaaSだが、**実際のデータの保存先はD社IaaSとなり、A社・B社間の関係だけからは見えないリスクが内在**する。
- このような複雑なケースがあることを認識した上で、扱うデータの機微性等に応じてバリュークリエイションプロセスの**データフローを可視化し、サービス契約の約款や契約相手へ確認することが重要**。