経済産業省

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

令和４年４月

経済産業省 商務情報政策局
サイバーセキュリティ課

第3層タスクフォースの位置づけ

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

データマネジメントの考え方の確立

＜データマネジメントの捉え方＞

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

＜３つの視点＞

① データマネジメントについて確立した定義は存在しない

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

② データを軸に置く

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

③ 関与する主体は同一・単一の主体に限られるものではない

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

本フレームワークの目的・想定読者

＜ 本フレームワークの目的 ＞

as isの対策

- データを軸に置き、**データのライフサイクルを通じて、データの置かれている状態を可視化してデータに対するリスクを洗い出し、**そのセキュリティを確保するために、ガバナンスを含めた必要な措置を**ステークホルダーが協調して実施する**。
- 洗い出されたリスクへの対策要件例として、これまでに公表されてきた情報セキュリティに関する様々な国際標準等を参照。

to beの対策

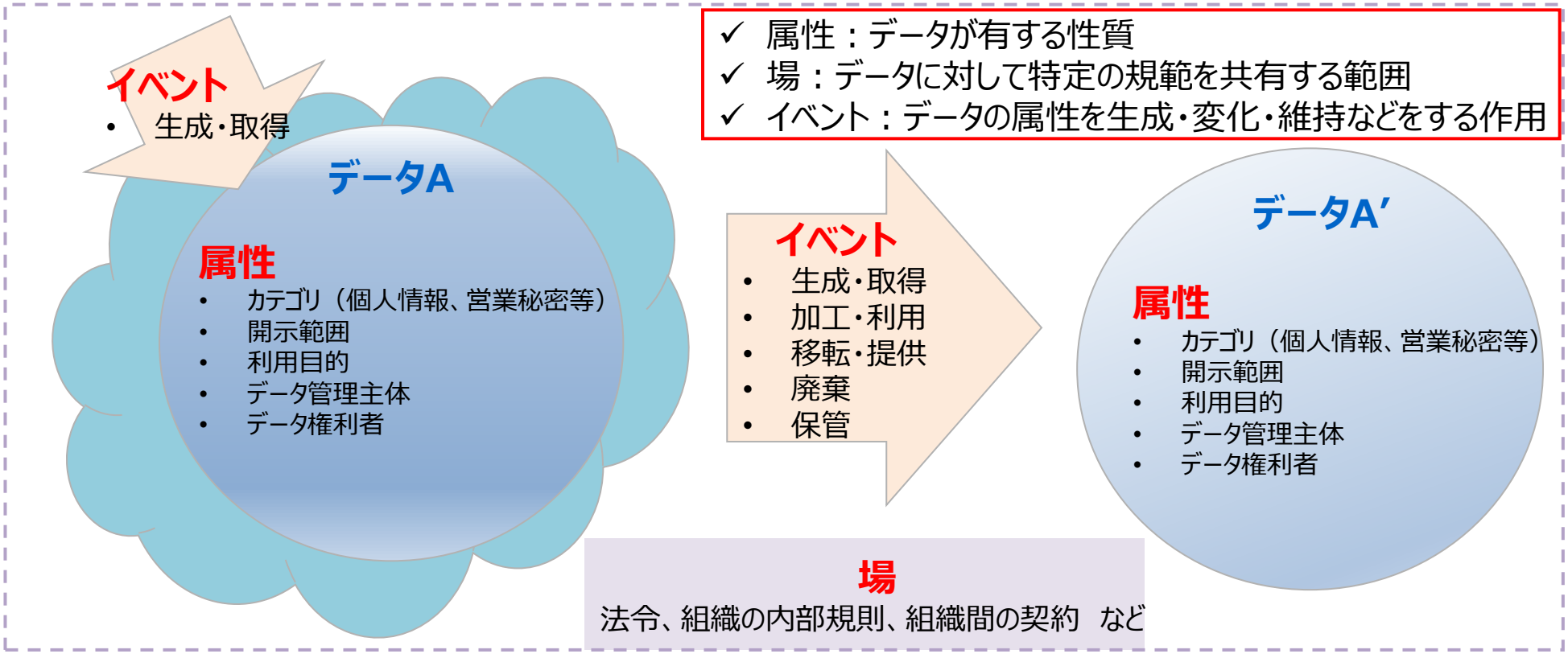
- データの流通を促進するために必要な条件を明確化。プロトコルの設計が容易に。
- 強い立場にあるシステムが**プロトコルのブラックボックス化によって「バンドル」することを難しく**させ、**オープン化された環境でデータ連携やシステムの組み合わせの自由を確保することを可能に**。
- 主体の在り方などを過度に考慮することなく、データに対して本来求められる要求事項を歪めることなく整理することが可能であり、**各国の制度間のギャップ分析**を行い必要な調整措置を明らかに。

＜ 本フレームワークの想定読者 ＞

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

データマネジメントのモデル化の概要

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



リスク分析手順

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

STEP 1
データ処理フロー（「イベント」）の可視化

STEP 2
必要な制度的な保護措置（「場」）の整理

STEP 3
「属性」の具体化

STEP 4
「イベント」ごとのリスクの洗い出し

モデル化（「イベント」）～ 生成・取得、加工・利用 ～

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

＜ 生成・取得 ＞

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

＜ 加工・利用 ＞

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

モデル化（「イベント」）～ 移転・提供 ～

＜ 移転・提供 ＞

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

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

モデル化（「イベント」）～ 保管、廃棄 ～

＜ 保管 ＞

- **保管は、他のイベントに付随して必ず生じる「イベント」**である。データはライフサイクルの様々な段階において、ネットワーク接続されたストレージ機器（オンプレミス、クラウドの双方を含む）・クライアントのハードディスク、USBメモリのような可搬媒体、機器の一時記憶領域等に保管され得る。
- データの取扱に関してリスクを洗い出し、セキュリティ対策を検討する上では、**移転・提供、加工・利用されるデータとは異なるリスクが生じうる**ことから、「イベント」の一類型として整理し、リスクの洗い出しを実施することが適切。

＜ 廃棄 ＞

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

モデル化（「場」）

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

モデル化（「属性」）

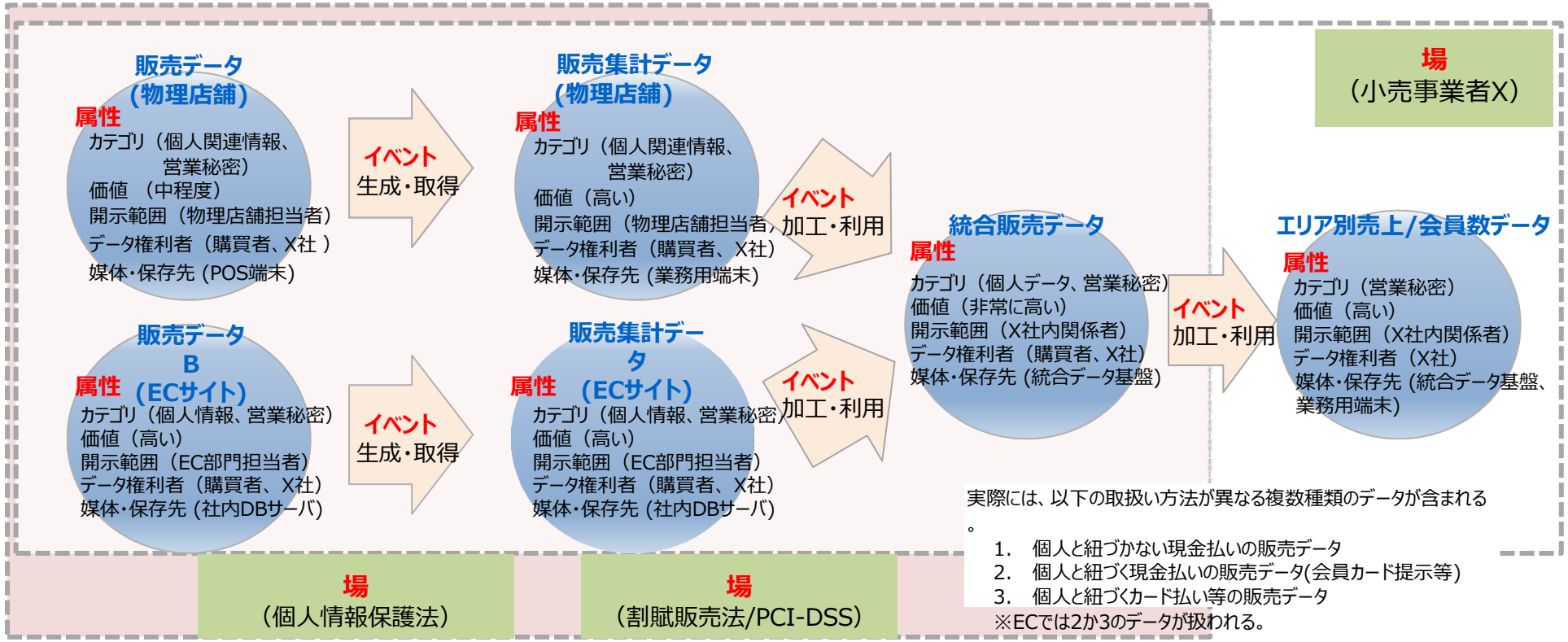
- 代表的な「属性」やパラメータ、整理のポイントを示す。
- 整理した「場」からデータに対する要求を検討し、関連する「属性」を適切に具体化することが重要。

- **カテゴリ**
  - 特に「場」と連動して、データに対して特別な作用（「イベント」）を求める場合（個人情報・匿名加工情報、営業秘密・限定提供データなど）、カテゴリとして法令等における位置づけを整理する。
- **開示範囲**
  - 民法上の契約や組織内規則も含め、データに定められている開示範囲を整理する。その際、組織内での取扱であっても、国・地域間での移転が伴う場合や、米国輸出管理法上のみなし輸出に該当する場合等、開示範囲の制限が複層的に適用される可能性がある点に留意。
- **利用目的**
  - 個人情報やライセンスなど、法令等に基づいて利用目的に制限が設けられている場合、当該利用目的の範囲内で取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**
  - データに軸を置く本フレームワークにおいては、データに作用を及ぼす主体についても、データが転々流通する過程で移り変わるものであり、あくまで「属性」の一つとして整理する。
- **データ権利者**
  - データが個人情報である場合、企業の競争力に関わる場合など、データ管理主体とは別に、データに対して権利を有する主体が存在することがある。移転・提供が行われて別の主体がデータを取得した場合でも、データ権利者は当該主体の管理下にあるデータに対して引き続き権利を有すると考えられるため、管理主体が転々と移っていく過程でも、「属性」として管理する必要がある。

活用方法 ～ サプライチェーンを構成するステークホルダー間での活用 ～

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

小売業におけるPOSデータの活用事例



添付A：ユースケース

- フレームワークの読者に対し、より理解を深めていただくために、実践的なユースケースに基づくモデル化とリスクの洗い出しのイメージを添付Aとして作成。
- 添付Aでは、特徴的な以下4つのユースケースを選定した。
  （次ページ以降で②及び③の概要を提示）

1

POSデータの分析
モデル化の全体像を把握しやすく単純化した事例

2

高齢者生活支援事業の提供
多数のステークホルダーが関係する事例

3

IaaS、PaaS、SaaSを利用してサービスを提供する例
クラウドサービスの多層化・重層化事例

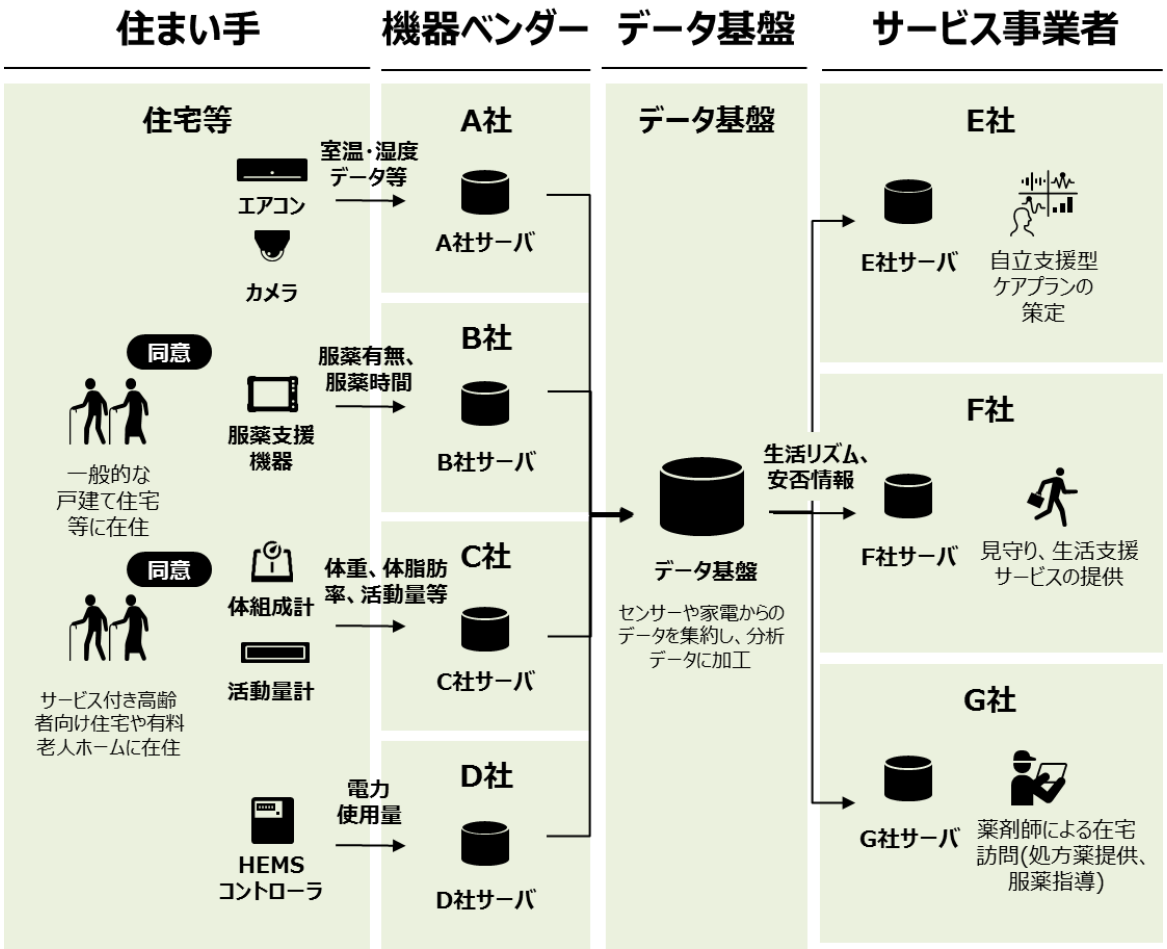
4

国内で提供されるITサービスに関して、海外で開発や運用等を実施する例
国外で開発や運用等を実施する事例（データの越境移転）

ユースケース② ｜ 高齢者生活支援事業 概要

- 2018年に実施された国立研究開発法人　新エネルギー・産業技術総合開発機構（NEDO）／パナソニック株式会社他による「IoT家電・センサーからのライフデータによる高齢者の生活サポートサービス基盤の研究開発事業」を取り上げる。

https://www.nedo.go.jp/news/press/AA5_101002.html



- 一般的な戸建て住宅や有料老人ホーム等に設置される多数の機器群を通じて、高齢者の生活や健康の状況に関するデータが**生成**され、各機器ベンダー（A社～D社）の運用するサーバに**蓄積**
- 各機器ベンダーは一定の収益を得る代わりに、第三者（プラットフォーム事業者）の運用するデータ基盤に各々が収集したデータを**提供**する。各機器ベンダーから提供されたデータは特定の個人を特定できない形でデータ基盤上に**集約**され、高齢者の生活リズム情報や安否情報というより高次なデータへと**加工**される。
- 高齢者の生活リズム情報や安否情報等のデータは、必要に応じてサービス事業者等に第三者提供され、データ主体の個人と紐づけたうえでより高度な支援サービスの提供等に**加工・利用**される。

ユースケース② ｜ 高齢者生活支援事業 ステークホルダー

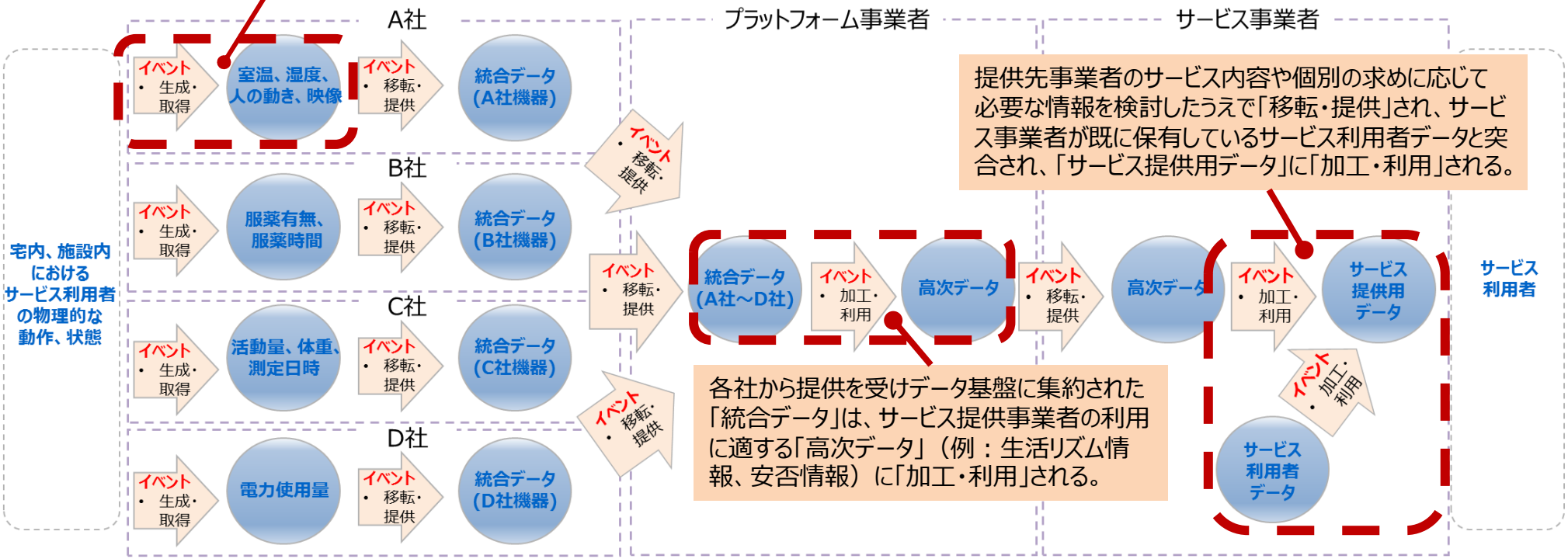
- 機器ベンダー（A社～D社）、プラットフォーム事業者、サービス事業者等は、コンソーシアムを組成し、共通して適用される規則の策定や適時の情報共有等を行っている 。
- 取り扱うデータには機微な個人データとなり得るものも含まれることから、コンソーシアム等での協議を実施し、サプライチェーンの全体で十分な水準のデータ保護措置を講じる必要がある。

ステークホルダー	説明
住まい手	日常生活の中で各種IoT機器・サービス等を利用し、それに伴って生成される自身に関するデータを同意等の適切な手続きを経たうえで事業者に提供する。 • 一般的な戸建て住宅等に在住する高齢者 • サービス付き高齢者向け住宅や有料老人ホームに在住する高齢者
機器ベンダー（A社～D社）	宅内や施設内に設置されている機器を製造・販売し、本人同意等の適切な手続きを経たうえで各々運用中の機器から取得したデータを収集し、管理している。
A社	エアコンや見守りカメラ等の家庭用IoT機器を製造・販売し、収集したデータを自社サービスで活用するだけでなく、プラットフォーム事業者にも提供する。
B社	処方薬の服薬有無や服用時間等をセンシングする服薬支援機器を製造・販売し、収集したデータを自社サービスで活用することに加え、プラットフォーム事業者にも提供する。
C社	体組成計や活動量計等のヘルスケア機器を製造・販売し、収集したデータを自社サービスで活用するだけでなく、プラットフォーム事業者にも提供する。
D社	スマートメータが実装された家庭向けに電力使用状況を可視化するサービスを提供し、収集したデータをプラットフォーム事業者にも提供する。
プラットフォーム事業者	各住宅、施設に設置した機器等からのデータを集約し、適宜加工・分析等を実施する。
サービス事業者（E社～G社）	プラットフォーム事業者からデータの提供を受け、より高度な高齢者支援サービスの提供等に活用する。

ユースケース② ｜ 高齢者生活支援事業 STEP 1

- STEP 1として、**データ処理フロー（イベント）の可視化**を行う。

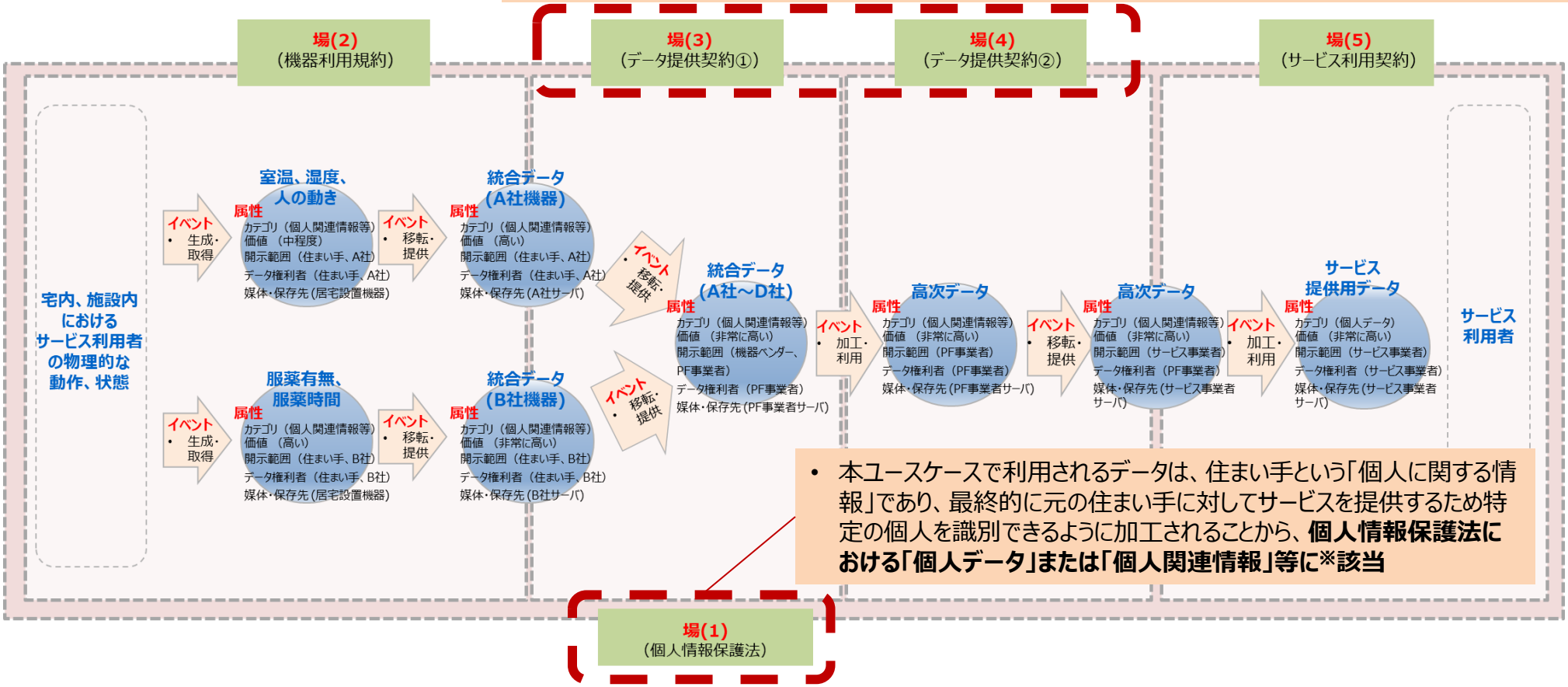
製造・販売者	名称	収集データ
A社	エアコン	室温・湿度情報
	電波センサーによる見守りシステム	ベッド上の呼吸有無・活動状態（動き）
	コミュニケーションカメラ	室温、人の動き、映像



ユースケース② ｜ 高齢者生活支援事業 STEP 2

- STEP 2として、**必要な制度的な保護措置（場）の整理**を行う。

- 各機器ベンダーが保有するデータに加え、「統合データ」についても、匿名的な利用者IDや機器IDに基づいて必ずしも特定の個人に紐づかない形で管理されていることを仮定しているため、「個人データ」ではなく「個人関連情報」等に該当すると考えられるが、提供先のサービス事業者において個人データとして取得されることが容易に想定される。そのため、各機器ベンダー及びPF事業者においては、**個人関連情報取扱事業者として本人からの同意取得の確認、提供元における記録等の義務が生じる**点に留意が必要



- 本ユースケースで利用されるデータは、住まい手という「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」または「個人関連情報」等に※該当**

※令和2年の改正個人情報保護法において規定。令和４年４月１日に施行される予定。

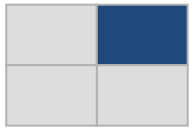
ユースケース② ｜ 高齢者生活支援事業 STEP 3-1

- STEP 3として、前STEPにて特定した「場」を踏まえ、**各種データの管理に資する属性を特定**する。
- 個人情報保護法制の他、開示範囲やデータ管理主体、利用期限等の事業者間の責任分解にも関連する内容を特定する際には、当事者間で締結される各種契約・規約が有用。

「属性」の検討において考慮すべきルール（場）

		個人情報保護法	機器利用規約	データ提供契約	サービス提供契約
カテゴリ	パーソナルデータ保護	○			
	知的財産（営業秘密を含む）保護			○	
	…	…	…	…	…
開示範囲		○	○	○	○
利用目的		○	○	○	○
データ管理主体			○	○	○
データ権利者		○	○	○	○
価値（重要度）			○	○	○
媒体・保存先			○	○	○
利用期限			○	○	○

ユースケース② ｜ 高齢者生活支援事業 STEP 3-2



- STEP 3として、前STEPにて特定した「場」を踏まえ、**各種データの管理に資する属性を特定**する。

本ユースケースにて取扱うデータ（一部）の「属性」パラメータ例

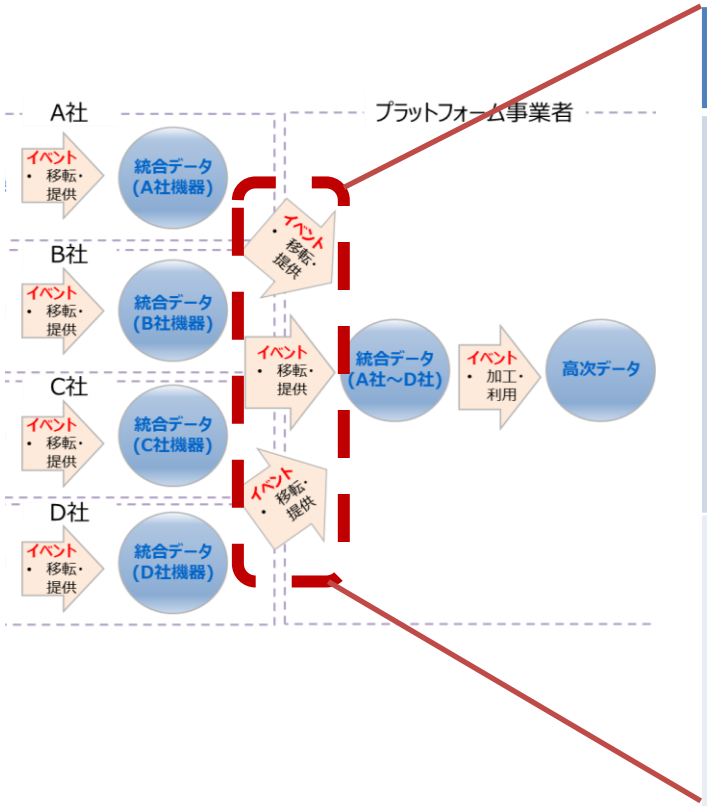
		統合データ（A社）	統合データ（A社～D社）	高次データ	サービス提供用データ
カテゴリ	パーソナルデータ保護※1	個人関連情報 等	個人関連情報 等	個人関連情報 等	個人データ
	知的財産※2（営業秘密を含む）	営業秘密 等（A社）	営業秘密（PF事業者）	営業秘密 等（PF事業者）	営業秘密（サービス事業者）
開示範囲		A社内	PF事業者内	PF事業者内	サービス事業者内
利用目的		取得データを活用した各種サービスの提供	左記と同様	左記と同様	左記と同様
データ管理主体		A社	PF事業者	PF事業者	サービス事業者
データ権利者		住まい手、A社	住まい手、機器ベンダー、PF事業者	住まい手、PF事業者	住まい手、サービス事業者
価値（重要度）		高い	非常に高い	非常に高い	非常に高い
媒体・保存先		A社サーバ	PF事業者サーバ	PF事業者サーバ	サービス事業者サーバ
利用期限		特になし	データ提供契約終了から1年	データ提供契約終了から1年	サービス提供期間終了まで

※1 対象のデータが、個人情報保護法上のいかなる情報の類型に属するかは、改正個人情報保護法の動向も踏まえつつ、適用主体において慎重な検討が必要である。
※2 上記のデータのうち、特定の事業者間で共有されるものについては、不正競争防止法上の「限定提供データ」に該当する場合も想定される。

ユースケース② ｜ 高齢者生活支援事業 STEP 4

- STEP 4として、STEP 1～3で特定した内容を踏まえ、**イベントごとのリスクポイントの洗い出し**を行う。

各機器ベンダー「統合データ」のPF事業者への「移転・提供」にて想定されるリスクの例



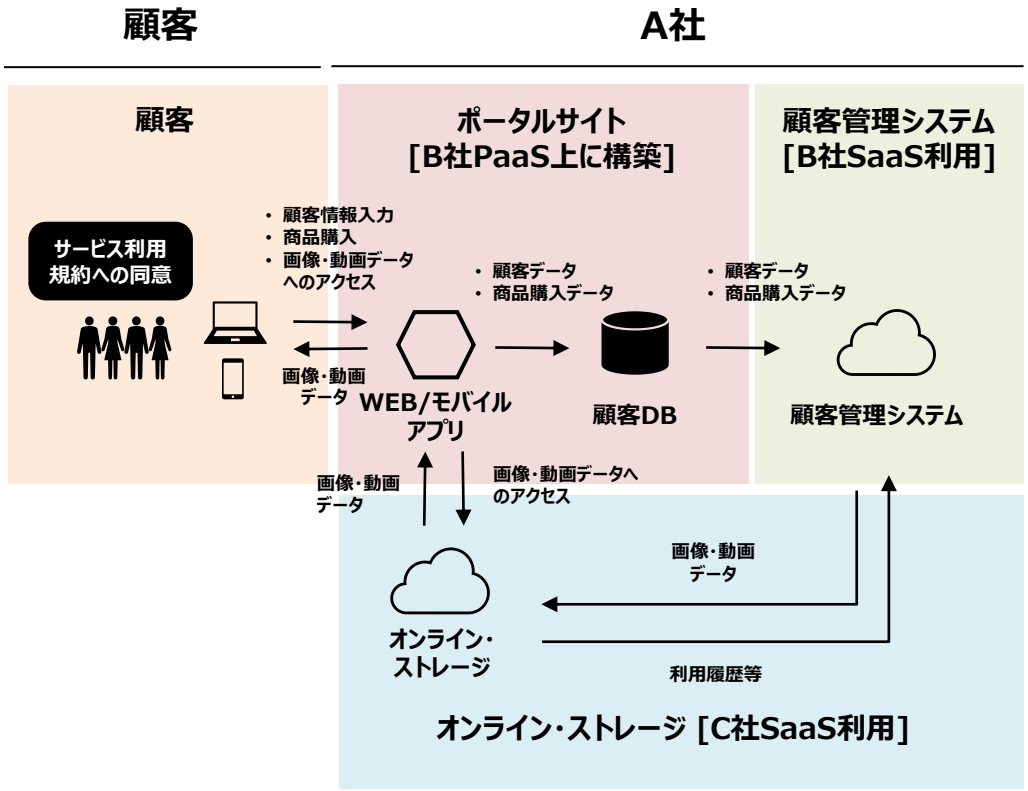
大分類	中分類	各機器ベンダーが保有する「統合データ」のPF事業者への「移転・提供」にて想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、通信内容が漏えいする。 ● 悪意のある内外の主体が機器ベンダーの管理するサーバから当初接続を意図していなかったサーバ等にデータを送信する。
	完全性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、データを改ざんする。
	可用性	● 悪意のある第三者がデータ基盤のAPI を無作為に呼び出すような DoS攻撃を行い、プラットフォーム事業者サーバの処理が停止する。
関連する法制度等に係る観点	パーソナルデータ保護	● 統合データの提供前に、提供元の機器ベンダーが提供先のプラットフォーム事業者において当該データが個人情報として取得されるかどうかを確認していない。 ● プラットフォームにて特定の個人の特定を行う場合に、住まい手の同意等を得ることなくデータがプラットフォーム事業者に提供される。
	知的財産（営業秘密を含む）保護	● 各社の統合データが悪意のある内外の主体により不正な手段で取得され、開示、使用される。

リスクを可視化した上で、各主体がそれぞれ実施すべき対策を他の主体と協議しながら取り組むことにより、データの信頼性を確保することが期待される。

ユースケース③ ｜ クラウドサービスを提供する例 概要

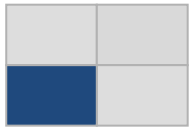
- サービス・物販事業者が提供する画像・動画データ管理を行うクラウドサービス事例を取り上げる。
- クラウドサービスを活用することで、コスト低減、技術革新対応力・柔軟性の向上等のメリットが得られる一方、サービス提供者と利用者の間の責任分界に対する認識が曖昧になりがちであったり、データの地理的所在等の透明性の不足等の課題が存在する。

システム・サービス概要



- サービス・物販事業者を運営するA社は、従来の店舗サービスの提供に加え、顧客向けポータルサイトにて画像・動画データをダウンロードするサービスを提供している。
- A社のポータルサイトは、B社の提供するPaaS上に構築され、さらにB社SaaSとして提供される顧客管理システムにもデータ同期を行う。
- データはC社IaaSとして提供されるオンライン・ストレージに格納され、顧客はポータルサイトを経由してアクセスすることができる。

ユースケース③ ｜ クラウドサービスを提供する例 ステークホルダー



- 本ユースケースで考慮すべきステークホルダーは以下の通り。
- 本ユースケースでは、A社のシステム構築のため契約するB社SaaS及びPaaSが、実際はC社IaaS上で構築されるといった関係がある。こうした「クラウドサプライチェーン」を米国国立標準技術研究所（NIST）等の分類を元に整理する。

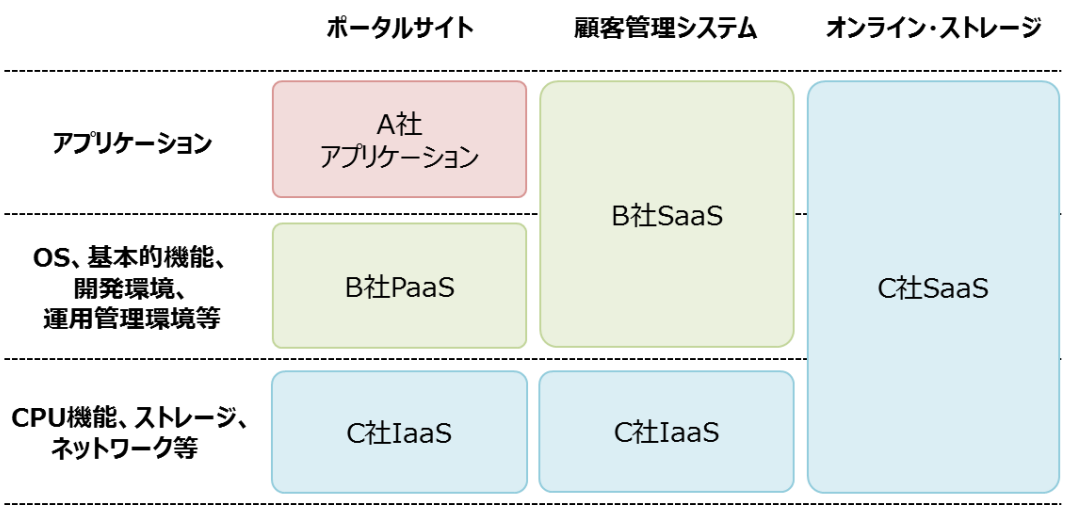
ステークホルダー	説明
顧客	A社が提供するポータルサイトにアクセスし、過去に撮影した画像・動画データの加工、ダウンロードや関連商品の購入を行う。
A社	写真撮影スタジオの運営等を業として行い、顧客価値を高めるための試みとして**クラウドサービスカスタマ**としてB社やC社から提供される各種クラウドサービスを利用しつつポータルサイトや顧客管理システム等を構築、運用している。
クラウドサービスプロバイダ	A社に各種のクラウドサービスを提供する事業者
B社	ポータルサイト向けにWebアプリ開発・運用基盤をPaaSとして、顧客管理システム・サービスをSaaSとしてA社に提供する。
C社	画像・動画データを格納するオンライン・ストレージサービスをSaaSとしてA社に提供し、**ピアクラウドサービス**としてB社の提供するサービスの基盤となっているIaaSも別途提供している。
クラウドサービスパートナー	B社PaaS上にポータルサイトを構築することに加え、各サービス間の連携部分を開発する。

クラウドサービスプロバイダ（CSP / cloud service provider）：
「クラウドサービスを利用できるようにするパーティ」を指す。(ISO/IEC 17789:2014)
クラウドサービスカスタマ（CSC / cloud service customer）：
「クラウドサービスを使うためにビジネス関係にあるパーティ」を指す。(ISO/IEC 17789:2014) クラウド利用者とも呼ばれる。
ピアクラウドサービス（peer cloud service）：
「クラウドサービスプロバイダのクラウドサービスの一部として使用されるクラウドサービス」を指す。(ISO/IEC 17789:2014)

ユースケース③ ｜ クラウドサービスを提供する例 ステークホルダー

- 本ユースケースで考慮すべきステークホルダーは以下の通り。
- 本ユースケースでは、A社のシステム構築のため契約するB社SaaS及びPaaSが、実際はC社IaaS上で構築されるといった関係がある。こうした「クラウドサプライチェーン」を米国国立標準技術研究所（NIST）等の分類を元に整理する。

クラウドサービス提供に係るサプライチェーンの概要



経済産業省「クラウドセキュリティガイドライン活用ガイドブック 2013 年度版」クラウドサプライチェーンにおける一般的な課題

- A社のようなクラウドカスタマから見た直接の契約先（ここではB社）に問題がない場合にも、**配下に存在するPaaSやIaaSに問題が生じた際、連鎖的な問題に巻き込まれる。**
- 障害が要因となり事業活動に何らかの損害が生じた場合に**事業者間で責任分界があいまいになりやすい。**
- 法規制上の問題やクラウドサービスカスタマのセキュリティポリシー等に関連して、外国や外国法適用配下に情報を置くべきでないとされているにも関わらず、サプライチェーンの配下に該当する事業者が存在し、**カスタマの意図に反する状態に陥ってしまう。**

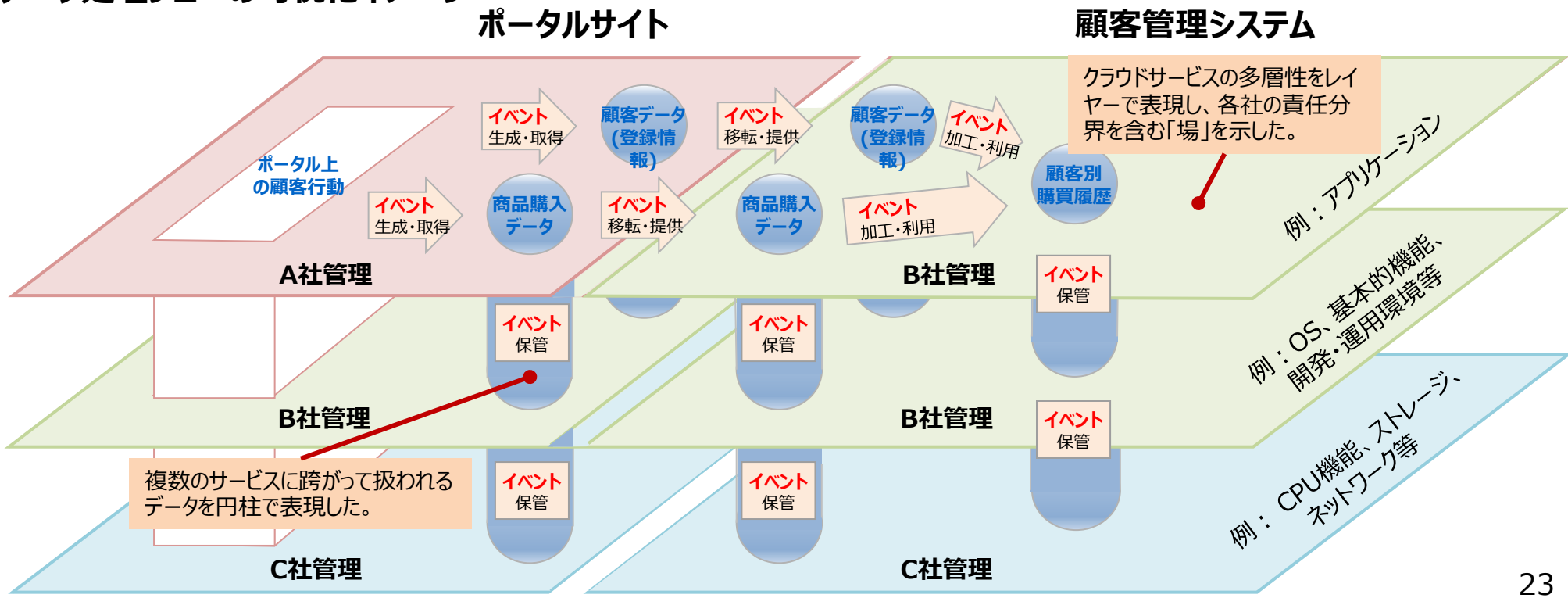
ユースケース③ ｜ クラウドサービスを提供する例 STEP 1～2

- 多層的なサービスにおけるデータ処理フローの可視化と必要な制度的な保護措置を整理する。

今回のデータ処理フローで取り扱う部分
- ポータルサイト上では顧客による自身のデータの入力や製品等の注文、その他の行動に応じて、「顧客データ」、「商品購入データ」等が「生成・取得」され、顧客DBに格納される。
- 当該データは、適時にB社が提供する顧客管理システムに「移転・提供」され、A社内の個別のニーズに応じてA社従業員により「加工・利用」される。

今回のデータ処理フローで取り扱わない部分
- A社所有の撮影機材により、顧客の画像・動画データが「生成・取得」され、
- A社従業員によりC社の提供するオンライン・ストレージへ「移転・提供」され、「保管」される。
- 画像・動画データは、顧客からの求めに応じて「加工・利用」（オンライン・ストレージ上での画像編集等）されたうえで顧客所有の端末（PC、スマートフォン等）に「移転・提供」される。

データ処理フローの可視化イメージ



添付B：イベントごとのリスクの洗い出しのイメージ

- 添付Bでは、フレームワークの適用を行う事業者等が、自身のデータ利活用プロセスにおいて想定されるリスクを特定するにあたり、考慮することが望ましい典型的なリスクを列挙する。
- 有効な対策要件例として、これまでに公表されてきた情報セキュリティに関する様々な国際標準等を参照。

イベントごとの典型的なリスクの記載方法

保護の観点	脅威主体の区分	想定されるセキュリティインシデント等（例）	脅威	有効な対策要件（例）
機密性	アドバーサリ（悪意のある主体）	生成・取得されるデータがネットワーク上で悪意のある内部犯行者または外部の攻撃者に傍受され、漏えいする。	情報漏えい	暗号化等による通信経路の保護

セキュリティの保護に関わるもの
- 機密性
- 完全性
- 可用性

関連する法制度等に関わるもの
- パーソナルデータ保護
- 知的財産（営業秘密を含む）保護

- アドバーサリ（悪意のある主体）
- 偶発的
- 構造上
- 外部環境上

STRIDEによる分類
- なりすまし
- 改ざん
- 否認
- 情報漏洩
- サービス不能
- 権限の昇格

本稿にて追加した分類
- マルウェア感染
- 不正改造
- 誤使用
- システム等の不具合
- 自然災害等

以下の参考文献との対応関係を記載
- CPSF
- ISO/IEC 27001:2013
- SP 800-53
- DMBOK 第2版 等