経済産業省

資料３

『第３層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースの検討の方向性

令和３年１２月１３日

経済産業省 商務情報政策局
サイバーセキュリティ課

1. 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）とその実装へ向けた取組の方向性

2. サイバー空間のつながりに関するデータマネジメントを巡る制度の動向

3. 本タスクフォースの検討事項
   a. パブコメでいただいたご意見とそれに対する考え方
   b. フレームワーク添付資料の追加
   c. 今後のスケジュール

分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化 とテーマ別TFにおける検討

- **6つの産業分野別サブワーキンググループ(SWG)**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、3つの**タスクフォース（TF）を設置**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
(分野ごとに検討するためのSWGを設置)

- **ビルSWG**
  - ガイドライン第1版の策定(2019.6)
- **電力SWG**
  - 小売電気事業者ガイドライン策定(2021.2)
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表(2020.12)
- **スマートホームSWG**
  - ガイドライン1.0版を公表(2021.4)
- **宇宙産業SWG**
  - 2021年11月に第3回を開催
- ・・・

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
データの信頼性確保に向け「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）」骨子案のパブリックコメントを実施。

ソフトウェアTF：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

検討事項：
OSSの管理手法に関するプラクティス集の策定、SBOM活用促進に向けた実証事業（PoC）を検討。

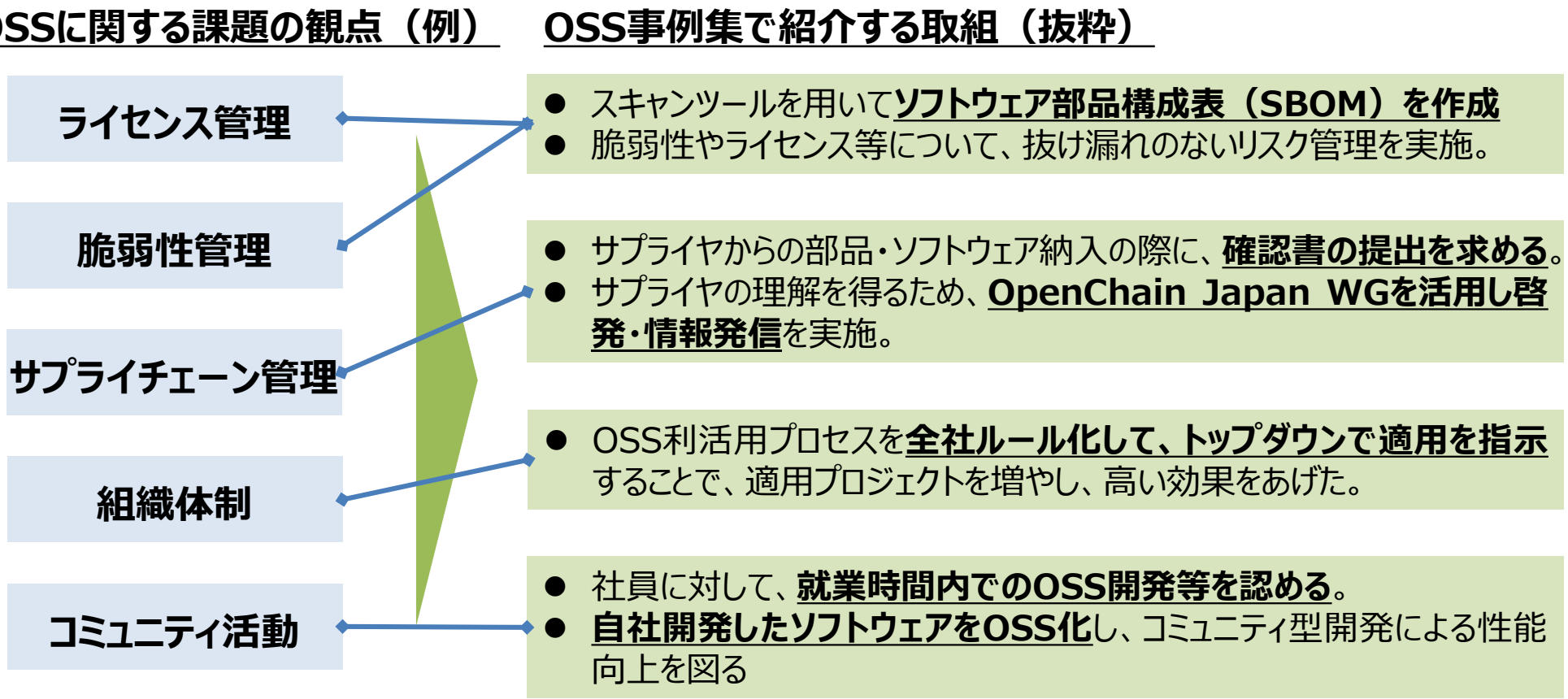
『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。

ソフトウェアTF：OSS管理手法に関する事例集の拡充

- **「OSSの利活用及びセキュリティ確保に向けた管理手法」をまとめた事例集を作成し、2021年4月21日に公開**。参考となる事例を共有して企業における適切なOSS利用を促進。日本から働きかけることで日米でOSSの活用・管理に関するベストプラクティスを共有する機会の確保を目指す。
- 令和3年度も、事例の拡充に向けてヒアリングおよび机上調査を継続。

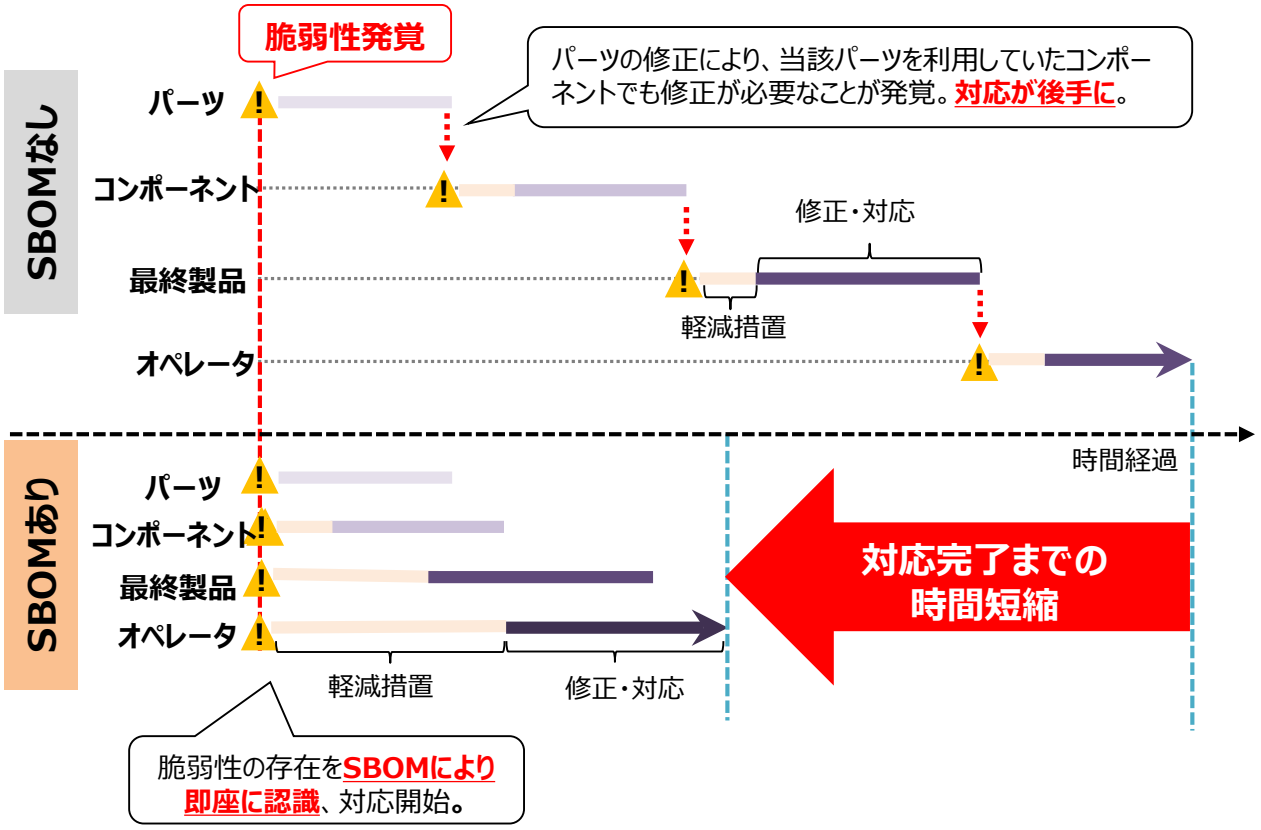
https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html



ソフトウェアTF：SBOM

- ソフトウェアの成分構成を表す**SBOM（Software Bill of Materials）**を活用することにより、**ソフトウェアに何が含まれ、誰が作り、どのような構成となっているか**等の把握が容易になる。
- 米国NTIAが2018年から主導するSoftware Component Transparencyでは、ヘルスケア分野における実証事業（PoC）に続いて、自動車産業・電力分野にも取組が拡大。
- 日本においても業界構造や商習慣を考慮しつつ、SBOM活用に向けた実証事業を実施中。

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



米国NTIAにおけるSBOMのPoC

ヘルスケア分野（病院、医療機器）

病院、医療機器メーカー、ベンダーが参加。2回のPoCを経てSBOM活用の手法、課題等を公開。4/29のNITA会合にて、医療機器メーカーにおけるSBOM活用に向けたガイドラインを取りまとめる予定と発表。

自動車産業分野

Auto-ISACを中心としたサプライヤー中心のプロジェクト。ヘルスケア分野のPoCを参考にしつつ、自動車産業分野でのSBOMの普及促進を目的として、SBOM構築方法や得られた教訓・課題等を確認する。12ヶ月ほどかけてサプライヤー向けの推奨事項がとりまとめられる予定。

電力分野

INL主導で、電力会社、電力機器ベンダー、ソフトウェアベンダー、電気協会等が参加。米国エネルギー省からもプレゼンターとして参加。2021年中のPoC実施完了に向け、目的、実施内容、スケジュールに関する議論を経て、9/1からPoCを実施中。

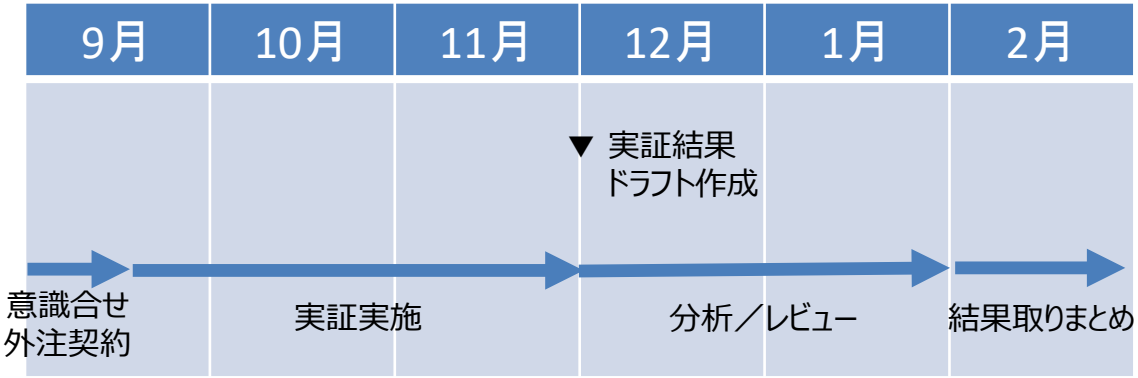
SBOM実証の対象ソフトウェア・体制・スケジュール

- ユーザー企業や製品ベンダーからのご協力が見込まれることから、**自動運転システム検証基盤ソフトウェア「GARDEN」を実証の対象ソフトウェアに選定**。

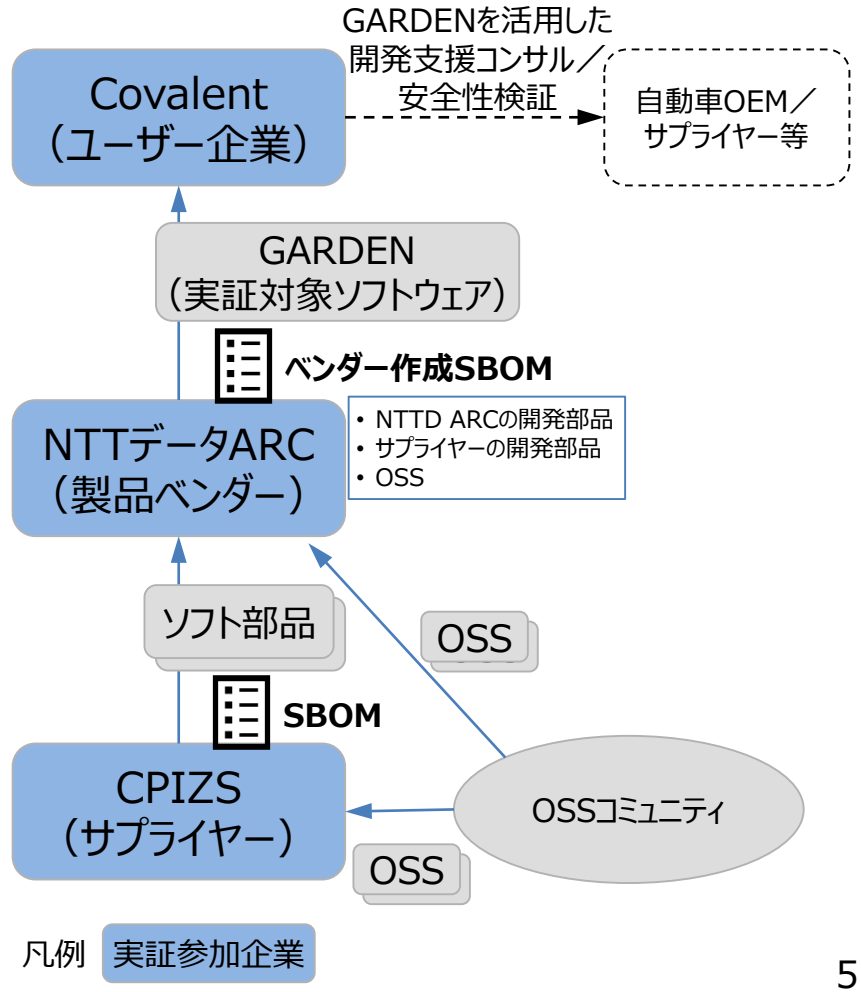
実証対象ソフトウェア 「GARDEN」

名称	GARDEN Scenario Platform
製品ベンダー	株式会社NTTデータ オートモビリジェンス研究所（NTTデータARC）
概要	• 自動運転システム開発向け検証基盤ソフトウェア。 • 自動運転ソフトウェアの安全性評価のための機能動作シミュレーションのシナリオ生成機能を提供。 ➢ モデリング、走行データ分類、軌跡抽出道路編集、シナリオ組合せテスト、シナリオ実行 • オープンソースとして、ソースコードを公開。

想定スケジュール



実証体制（GARDENのサプライチェーン）



1. 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）とその実装へ向けた取組の方向性

2. サイバー空間のつながりに関するデータマネジメントを巡る制度の動向

3. 本タスクフォースの検討事項
   a. パブコメでいただいたご意見とそれに対する考え方
   b. フレームワーク添付資料の追加
   c. 今後のスケジュール

経済産業省 データの越境移転に関する研究会

- 2019年1月、ダボス会議において日本がDFFT（Data Free Flow with Trust）を提唱し、同年6月のG20貿易・デジタル閣僚会合でDFFTを盛り込んだ閣僚宣言に同意。
- 2023年に日本で開催される予定のG7に向けて、研究会では各国における規制状況の把握、相互運用可能な枠組みに向けた検討を進める。

【第１段階】データの取扱に関する制度の問題点をお互いに指摘し合う

- 2021年秋に勉強会を立ち上げ、2021年度内に成果を公表。
  - 越境流通のニーズが高いデータ（具体例）
  - 各国のデータ取り扱いに関する制度の概要
  - 比較分析に必要な枠組みの要素
  - ペインポイントの特定

【第２段階】各国間のギャップ分析をOECDなど国際機関と連携して実施

- データ取扱に関する各国の制度を同じ尺度で比較分析する調査を2022年度中に実施
- 比較分析の枠組みとして、日本で検討中の「データ・マネジメント・フレームワーク」※を応用することも選択肢

※データを軸に置き、データのライフサイクルを通じて、その置かれている状態を可視化してリスクを洗い出し、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フレームワーク。経産省が提案（2021年10月一次パブコメ終了）。

【第３段階】各国間のギャップの調整措置を行うための体制の構築を決定（2023年G7）

- 各国間のギャップを調整する措置の実行とモニタリングを行う体制を有志国で構築することをG7（2023年日本開催）で宣言。

1. 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）とその実装へ向けた取組の方向性

2. サイバー空間のつながりに関するデータマネジメントを巡る制度の動向

3. 本タスクフォースの検討事項
   a. パブコメでいただいたご意見とそれに対する考え方
   b. フレームワーク添付資料の追加
   c. 今後のスケジュール

タスクフォースの検討の方向性（第4回TF資料再掲）

- **タスクフォースの目標**
  - 主体間を転々流通するデータのセキュリティ対策を検討するにあたり、**ステークホルダー間の議論に際し、リスクを適切に把握することに資する枠組み**の提供
  - 組織を越えてデータを利活用するバリュークリエイションプロセス（価値創造過程）において、本枠組みを用いてデータの流通プロトコルや連携APIの在り方を明確にすることで**データの囲い込みを回避（アンバンドル化）し**、多様な価値創造を促進。
- **データマネジメントの捉え方**：
  「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全体にわたって管理すること」という定義を提案

➡ こうしたプロセスにて、「検証可能な方法でステークホルダーの期待を満たす」のが「信頼性」を確保すること

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

- 「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、以下フレームワーク）」の骨子案のパブコメを実施。（2021年7月15日～10月11日）
- 第5回タスクフォースでは、「本文修正案」及び今回作成した「添付A」「添付B」の内容についてご議論いただきたい。

【本文】

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
  - 1-1-2 第3層の位置づけ
- 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
- 1-3 本フレームワークの目的
- 1-4 本フレームワークの想定読者

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
  - 2-1-2 リスク分析手順
- 2-2 詳細編
  - 2-2-1 モデル化（「イベント」）
  - 2-2-2 モデル化（「場」）
  - 2-2-3 モデル化（「属性」）

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
- 3-2 ルール間のギャップの分析

【添付資料】

添付A. ユースケース

添付B. イベントごとのリスクの洗い出しのイメージ

今回作成したもの

パブコメを受けて修正

最終案パブコメを予定

フレームワークのパブコメ概要

- 「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、以下フレームワーク）」の骨子案のパブコメを実施。（2021年7月15日～10月11日）
- 11の組織・個人より、約70件の意見提出あり。

いただいたご意見を以下の４つに分類。
次ページ以降で主なご意見とそれに対する考え方をまとめた。

1. CPSFや本フレームワークのコンセプトやスコープに関するご意見
2. 例示やユースケースに関するご意見
3. 越境移転に関するご意見
4. その他　（スライドとしてはありません。）

主なご意見と考え方：
１．CPSFや本フレームワークのコンセプトやスコープに関するご意見

いただいたご意見

- 「異なるデータ管理のルール」を「跨いでデータが流通した場合」のセキュリティ確保に必要な調整を図るため、「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理解を得」たいという考え方に賛同します。
- 「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」の実現を可能にするという目的に賛同します。
- 2.1. 概要データマネジメントをモデル化するための記述スタイル（整理の仕方）を決めるという提案と理解しました。整理の仕方を決め、種々のステークホルダが情報を出し合い、議論を活性化しようとする取り組みは良い事と考えます。モデルはいろいろあると思いますが、まずは提案された「属性」「場」「イベント」という考え方でスタートし、使う中でブラッシュアップしていくので良いのではないでしょうか。

考え方

- 本フレームワークに対する肯定的なご意見として承ります。

主なご意見と考え方：
1．CPSFや本フレームワークのコンセプトやスコープに関するご意見

いただいたご意見

- CPSF概論の冒頭において、データ生成の主体が人以外も含めて生成していることに触れた方が良いのではないかと考えます。

- 【263行目】Step4が完了した後も、３つの要素が変化することでリスクが新たに出現したり変化したりすることが考えられますため、Step4については、「場」「属性」「イベント」が時間の経過とともに変化することを前提にした記述とし、その結果CPSFの利用シーンは、これから開発するシステムを企画する際のリスク分析や、インシデントが発生した際のセキュリティ分析など、と明確にすることも一案かと考えます。

考え方

- 以下のように修正いたします。
  - 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また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。
- 以下を追記いたします。
  - また、STEP 4までの取組みが完了した後も、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それを取り巻く環境等に何らかの変更が行われることを認識した場合、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。

主なご意見と考え方：
1．CPSFや本フレームワークのコンセプトやスコープに関するご意見

いただいたご意見

- 2-2-2 モデル化（「場」）（PP. 13-14）「場」の設定は容易ではないと考える。この部分では、各国・地域等の法令、組織の内部規則、組織間の契約等に触れながら、パーソナルデータの保護、知的財産・営業秘密保護、機微技術管理、適切な社会機能の維持の4つのカテゴリが挙げられているが、以下3点を指摘する。
  - 各国・地域等の法令の適用範囲は多種多様であり、域外適用をどのように考えるのか、A国所在の事業者Xが、A国からB国のユーザーに越境でサービス提供をしていた場合であって、B国が域外適用規定を有していた場合、A国所在の事業者Xは、A国法令に加えてB国法令にも遵守しなければならない。こうしたケースを踏まえる必要がある。
  - 組織の内部規則についても、多国籍企業と純粋国内企業では異なる訳であり、グローバル共通の規則＋特定国向けの規則の組み合わせを有する前者と、単に特定国向けの規則を有する後者とでは異なる訳であり、その点も踏まえる必要がある。
  - 4つのカテゴリについても、本当にこの切り分けが適切かつ十分なのかといった点がある他、うまく切り分けられるか重複してしまうかは結局コンテキストや観点次第なのであるから、その点も考慮に入れる必要がある。

考え方

- 以下のように修正いたします。
  - 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。(381行目に追記)
  - 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。(387-388行目を修正)
  - なお、4つのカテゴリはひとつの例であり、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。(390行目に追記)

主なご意見と考え方：
２．例示やユースケースに関するご意見

いただいたご意見

- 保管については、オンプレミス環境を想定しているように読み取れますが、利活用の進むクラウドサービスプロバイダー等が提供するクラウドストレージの例示を加えることも一案かと考えます。
- モデル化イベントにおける整理のポイントとして、「生成・取得」「加工・利用」「移転・提供」「保管」「廃棄」に加えて、「アーカイブ」を加えるのも一案と考えます。
    - 組織はリアルタイムでのデータ使用が要求されない場合、法・規制または組織の方針に従い、アーカイブの対応が必要と考えます。その際、アーカイブのデータが組織内またはサプライヤーが再取得した際、アーカイブデータの真正性の確保が必要になります。本フレームワーク内において、利用期限についても言及されていることから、アーカイブのイベントについてもデータセキュリティライフサイクルマネジメントのイベントとして定義する必要があると考えられますため。

考え方

- 以下のように修正いたします。
    - 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。
- データを専用の保存領域や記録装置にて長期的に保存する行為としての「アーカイブ」は、「保管」に含まれるものと考えます。

主なご意見と考え方：
２．例示やユースケースに関するご意見

いただいたご意見

- 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、とありますが保有するデータを廃棄できても、流通過程で複製されたデータ全てを廃棄することは一般的に困難であると考えられるため、現実的に定義された廃棄は困難ではないかと考えます。
  - 本イベントは論理的な廃棄を意味するものと理解しますが、物理メディアの廃棄と混同される恐れがあり、保有データの消去・消滅など明確な定義を行う必要があると考えられますため。
- 【343行目】４つの単位について、「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。」とありますが、４つの単位について、言葉の定義、説明を追記していただきたい。例えば、システム・サービス　とは、サービスを提供するシステムのことか？システムとサービスは常に一緒に扱うのか？など。

考え方

- いただいたご意見も参考に、以下の記述を追記いたします。
  - 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調しつつ、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。
- 指摘箇所に移転・提供に係る４つの単位に関する説明を追記いたします。
  - （追記内容が長いためここでは割愛）

主なご意見と考え方：
２．例示やユースケースに関するご意見

いただいたご意見

- 2.2.1.モデル化（「イベント」）にて、第2層と第3層が組み合わされ、第3層にて第2層のデータが転々流通していく場合、第2層のセンサ・デバイスが信頼の基点(Root of Trust)となり、転々流通していく過程で信頼の鎖(chain of trust)が形成されるケースが考えられます。本フレームワークでも示唆されていると感じますが、より明確に例示として記載するとデータマネジメントにおけるセキュリティのイメージが伝わると考えます。

考え方

- 以下の記述を追記いたします。
  - 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。

主なご意見と考え方：
３．越境移転に関するご意見

いただいたご意見

- ３-２　ルール間のギャップの分析（PP. 17-18）の欧州から日本へのデータの移転について、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。まずEUの一般データ保護規則（GDPR）という「場」を前提として話をすれば、EU域内から日本国内への個人データの移転で捉えられるべき「イベント」は、「移転（transfer）」のみならず「処理（process）」もあることを忘れてはならない。
- つまり、十分性認定はあくまでも「移転」を合法化するための措置であって、EU域内の事業者から日本国内への事業者にデータを提供すること自体については、別途「処理」というイベントに対する合法性（同意や正当な利益等）もなければならない。
- これを踏まえれば、後段の「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」という記述は正確ではなく、データの「属性」の変化については、「処理」というイベントとの関係で整理されるべき事項であると考える。

考え方

- 以下のように修正いたします。
  - 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(注釈を挿入)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。
  - 注釈：ここで、「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。

主なご意見と考え方：
3．越境移転に関するご意見

いただいたご意見

- 513行目以降に、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についての記述があるが、まず、2020年の欧州司法裁判所（CJEU）Schrems II事件でプライバシーシールドは無効となっており、現在、米EU間で「強化されたプライバシーシールド」に関する議論が行われているため、無効となったものを前提に議論を進めるべきではないと考える。
- その上で、欧州から米国への移転について、「イベント＝移転」という形で捉えているが、プライバシーシールドはいわば部分的十分性認定であり、あくまでも移転を合法化する措置に過ぎない。したがって、EU域内の事業者から米国国内の事業者への個人データの提供という「処理」も「イベント」として捉えられるべきであり、その点が欠落しているように見受けられる。
- さらに、515行目以降に、「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」との記述があるが、なぜこの移転単体をもって「開示範囲に米国政府が加わる形で「属性」が変化」しているのかの詳細な論述がなく、あまりにも乱暴な議論のように感じる。
- この後の文章においても、「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」との記述があるが、今一度判決文をご一読いただいた上で、本当にこのように判断したのか、ご検討いただきたい。

考え方

- プライバシーシールドに基づく欧米間のデータ移転について述べた記述を以下のように修正いたします。
  - 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。
- また、以下の記述を注記いたします。
  - 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 。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。

1. 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）とその実装へ向けた取組の方向性

2. サイバー空間のつながりに関するデータマネジメントを巡る制度の動向

3. 本タスクフォースの検討事項
   a. パブコメでいただいたご意見とそれに対する考え方
   b. フレームワーク添付資料の追加
   c. 今後のスケジュール

添付A：ユースケース

- フレームワーク骨子案では、概念やモデル化の定義等が中心だったが、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資料として作成。
- 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。

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

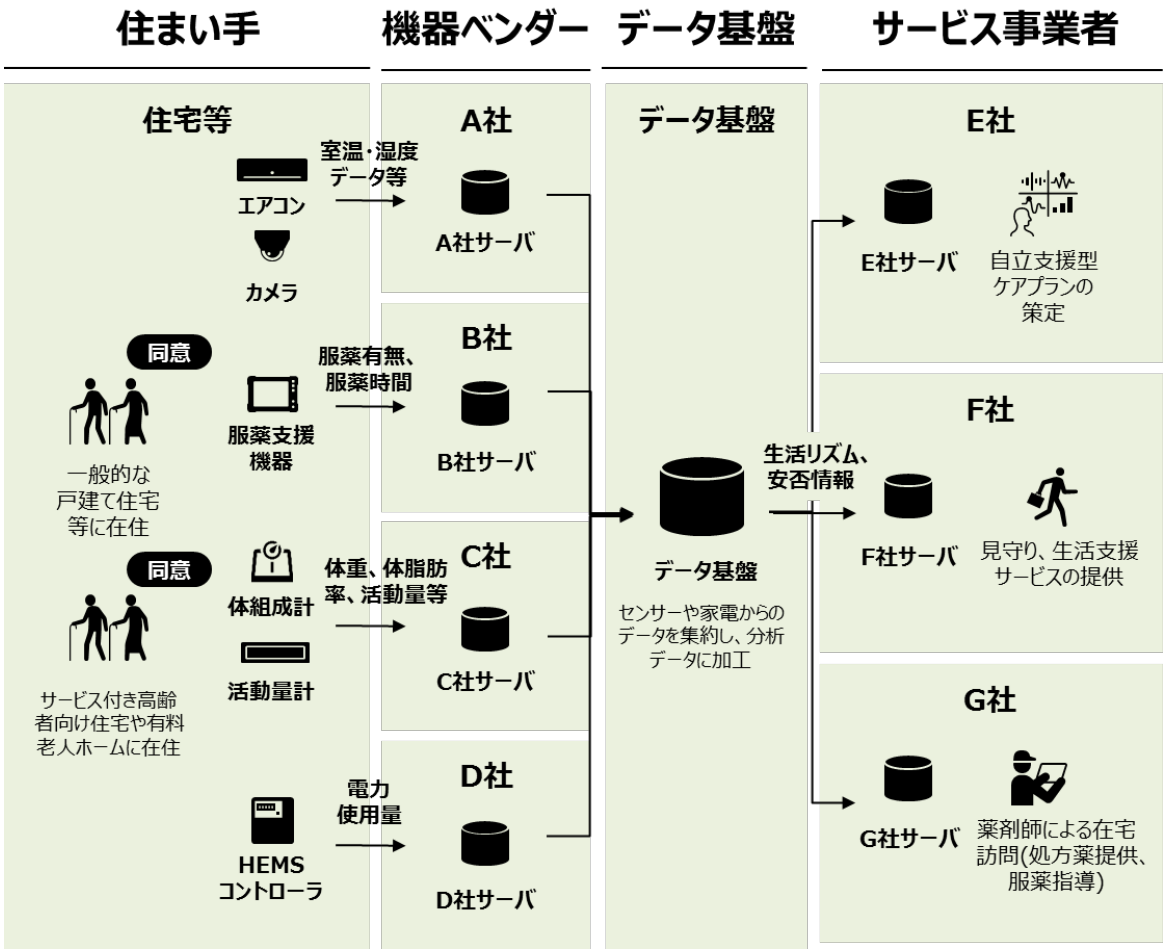
4

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

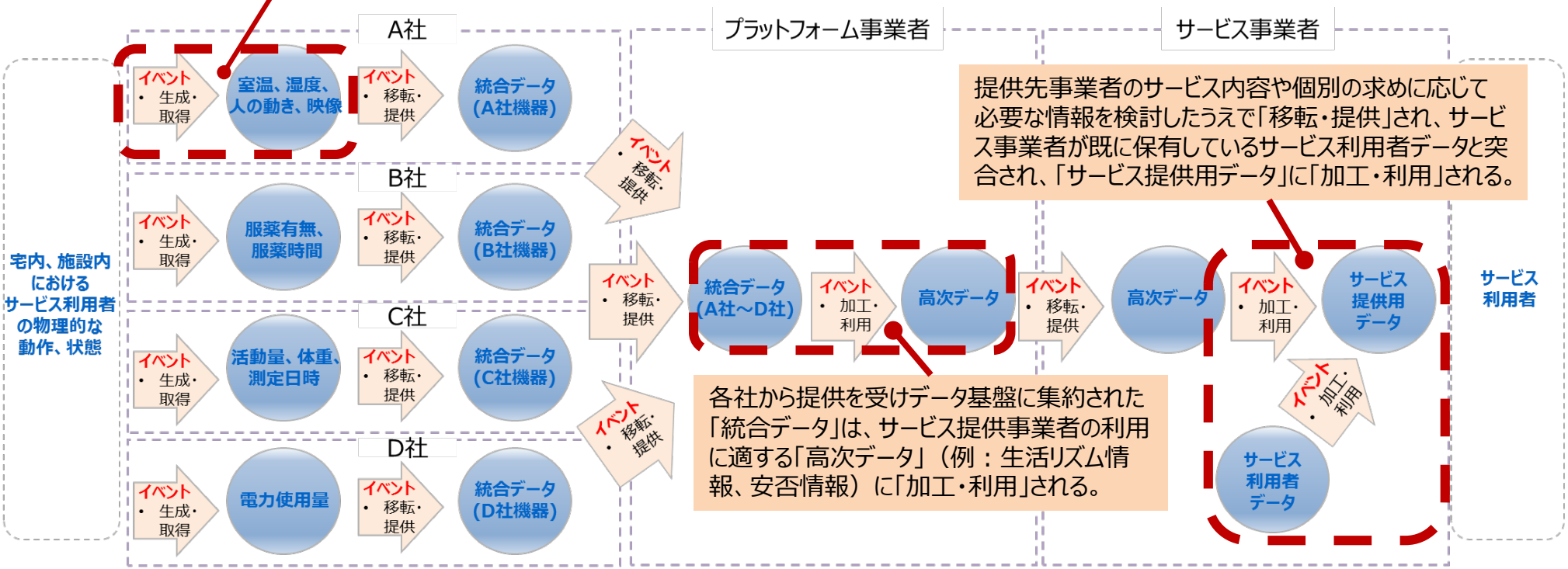
- 機器ベンダー（A社～D社）、プラットフォーム事業者、サービス事業者等は、コンソーシアムを組成し、共通して適用される規則の策定や適時の情報共有等を行っている 。
- 取り扱うデータには機微な個人データとなり得るものも含まれることから、コンソーシアム等での協議を実施し、サプライチェーンの全体で十分な水準のデータ保護措置を講じる必要がある。

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。

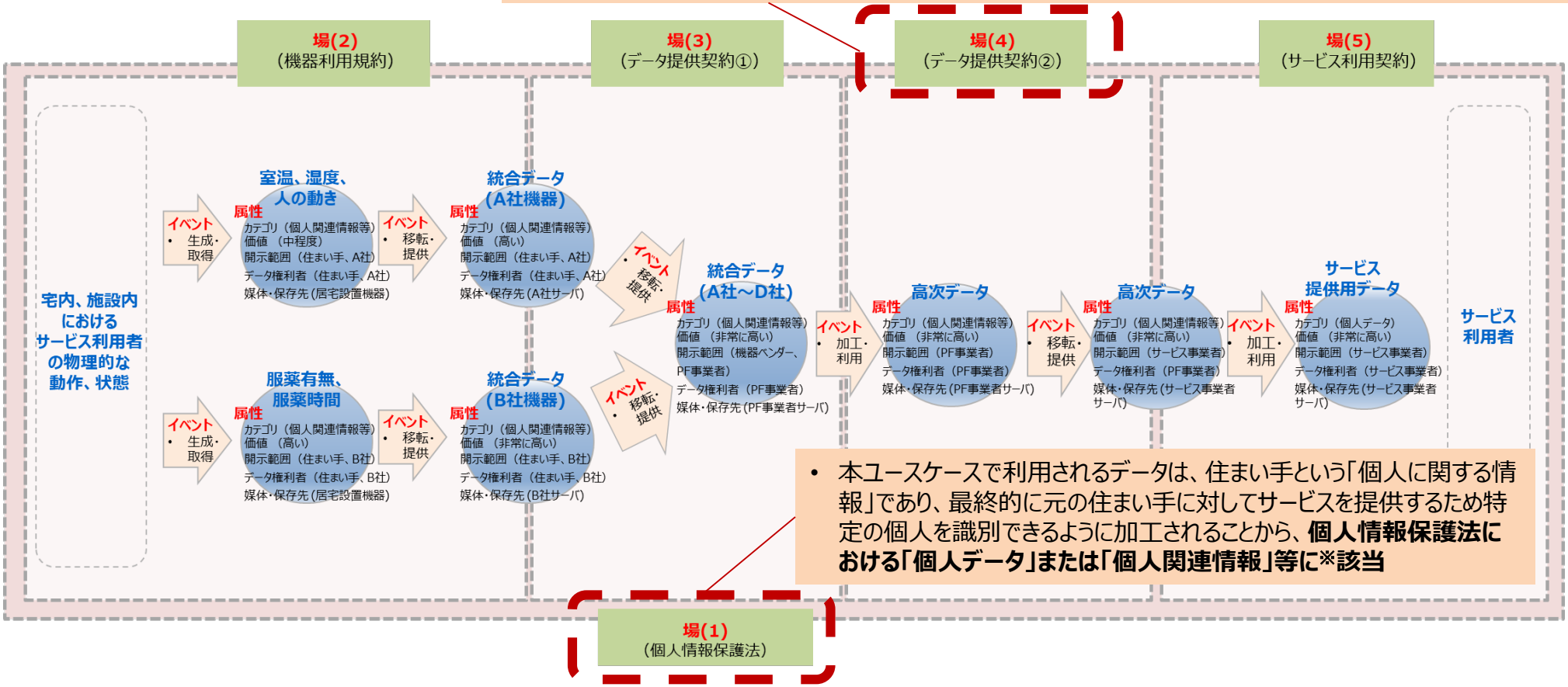
製造・販売者	名称	収集データ
A社	エアコン	室温・湿度情報
	電波センサーによる見守りシステム	ベッド上の呼吸有無・活動状態（動き）
	コミュニケーションカメラ	室温、人の動き、映像



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。

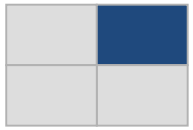
ユースケース② ｜ 高齢者生活支援事業 STEP 3-1

- 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

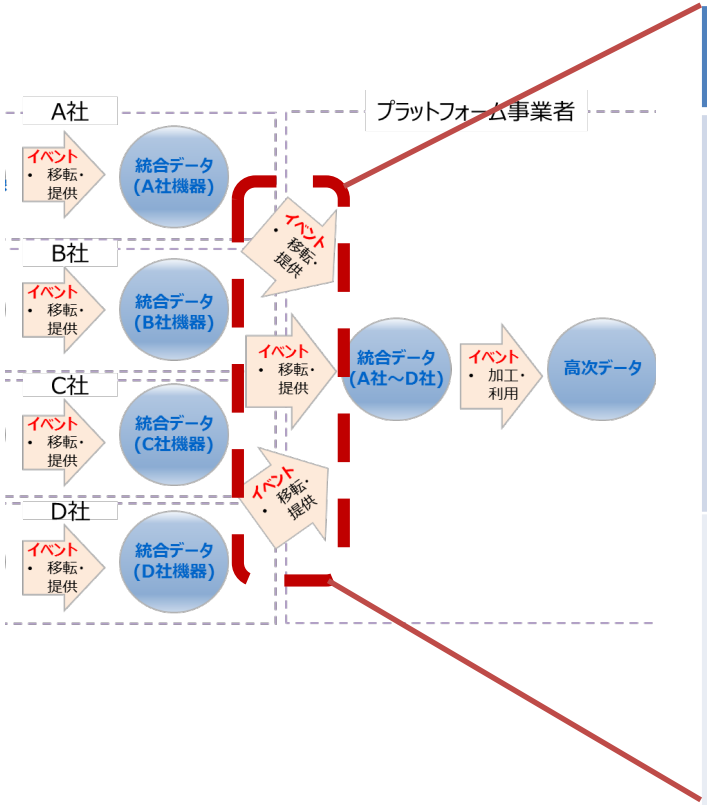
		統合データ（A社）	統合データ（A社～D社）	高次データ	サービス提供用データ
カテゴリ	パーソナルデータ保護※1	個人関連情報 等	個人関連情報 等	個人関連情報 等	個人データ
	知的財産※2（営業秘密を含む）	営業秘密 等（A社）	営業秘密（PF事業者）	営業秘密 等（PF事業者）	営業秘密（サービス事業者）
開示範囲		A社内	PF事業者内	PF事業者内	サービス事業者内
利用目的		取得データを活用した各種サービスの提供	左記と同様	左記と同様	左記と同様
データ管理主体		A社	PF事業者	PF事業者	サービス事業者
データ権利者		住まい手、A社	住まい手、機器ベンダー、PF事業者	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



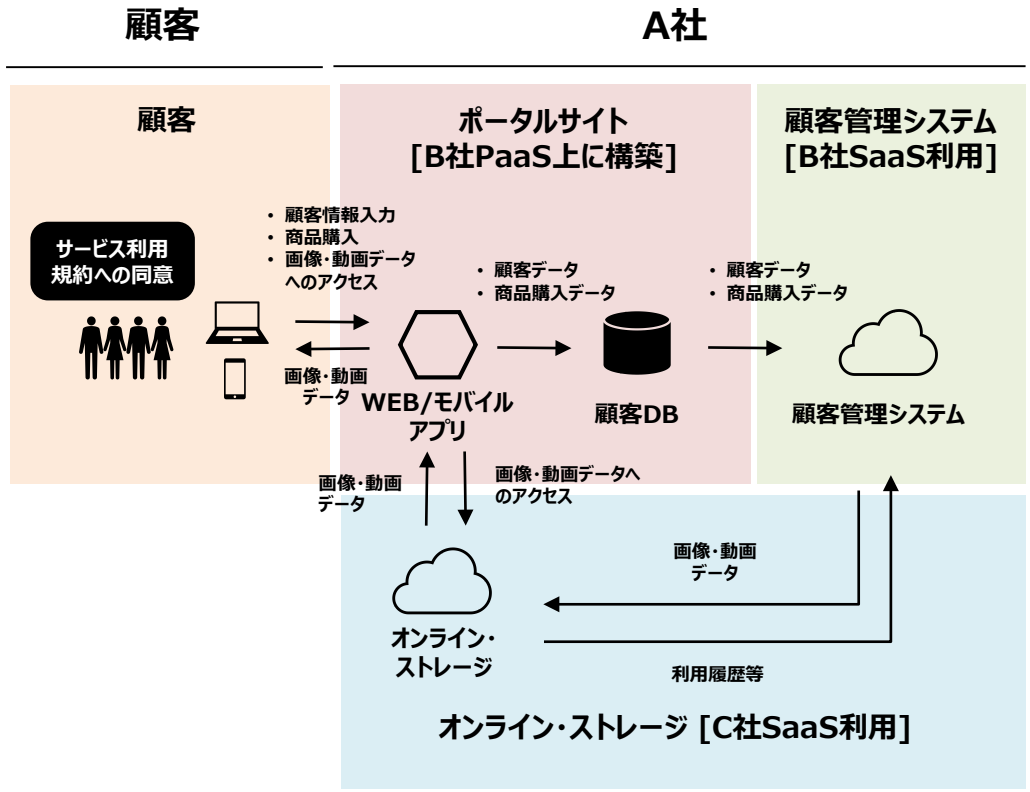
大分類	中分類	各機器ベンダーが保有する「統合データ」のPF事業者への「移転・提供」にて想定されるリスク（例）
セキュリティの保護に係る観点	機密性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、通信内容が漏えいする。 ● 悪意のある内外の主体が機器ベンダーの管理するサーバから当初接続を意図していなかったサーバ等にデータを送信する。
	完全性	● 悪意のある第三者が機器ベンダーの管理するサーバとプラットフォーム事業者サーバ間の通信に介入し、データを改ざんする。
	可用性	● 悪意のある第三者がデータ基盤のAPI を無作為に呼び出すような DoS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

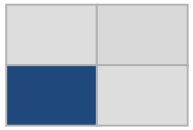
- 写真撮影スタジオが提供する画像・動画データ管理を行うクラウドサービス事例を取り上げる。
- クラウドサービスを活用することで、コスト低減、技術革新対応力・柔軟性の向上等のメリットが得られる一方、サービス提供者と利用者の間の責任分界に対する認識が曖昧になりがちであったり、データの地理的所在等の透明性の不足等の課題が存在する。

システム・サービス概要



- 写真等撮影スタジオを運営する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スタジオで撮影した画像・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。
- スタジオで撮影したデータは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。

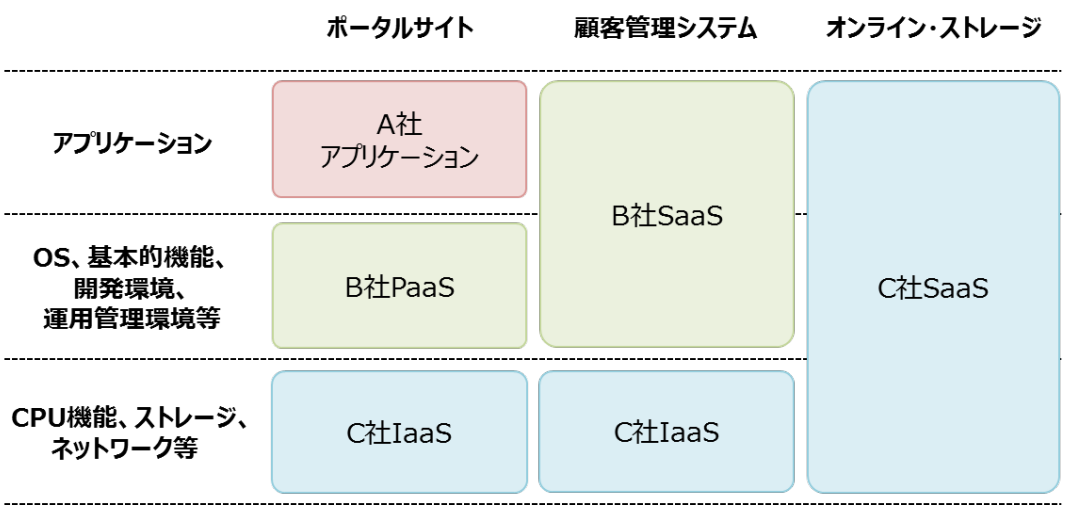
ステークホルダー	説明
顧客	A社が提供するポータルサイトにアクセスし、過去に撮影した画像・動画データの加工、ダウンロードや関連商品の購入を行う。
A社	写真撮影スタジオの運営等を業として行い、顧客価値を高めるための試みとして**クラウドサービスカスタマ**としてB社やC社から提供される各種クラウドサービスを利用しつつポータルサイトや顧客管理システム等を構築、運用している。
クラウドサービスプロバイダ	A社に各種のクラウドサービスを提供する事業者
B社	ポータルサイト向けにWebアプリ開発・運用基盤をPaaSとして、顧客管理システム・サービスをSaaSとしてA社に提供する。
C社	画像・動画デ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

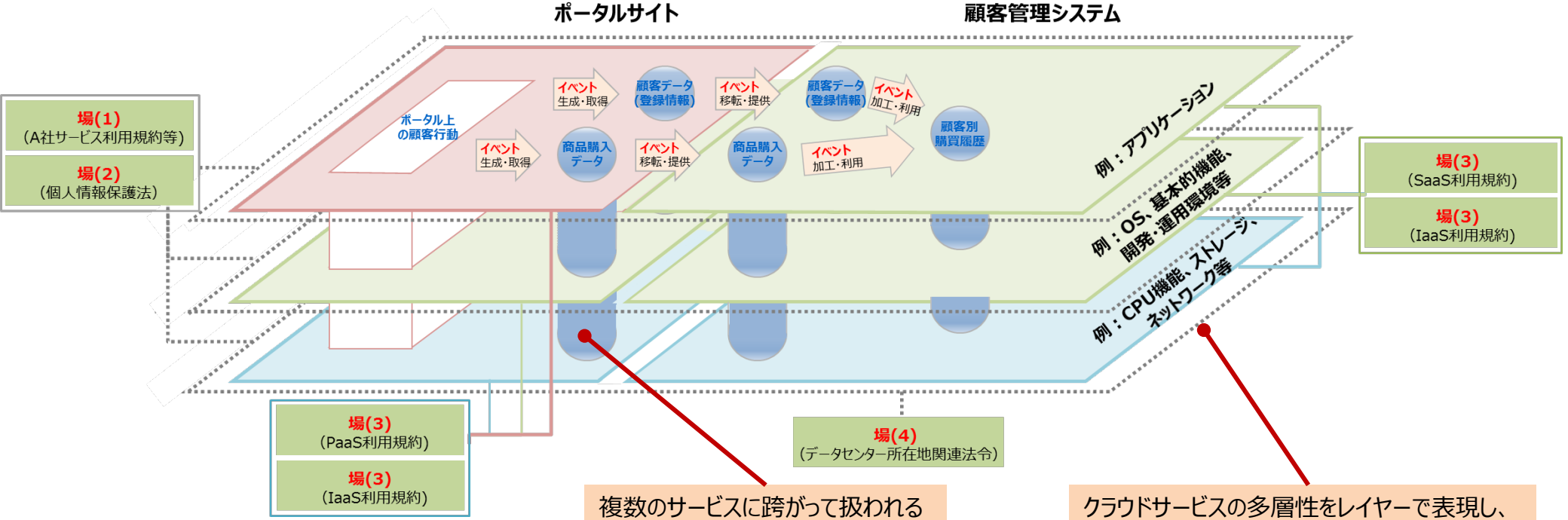
- A社のようなクラウドカスタマから見た直接の契約先（ここではB社）に問題がない場合にも、**配下に存在するPaaSやIaaSに問題が生じた際、連鎖的な問題に巻き込まれる。**
- 障害が要因となり事業活動に何らかの損害が生じた場合に**事業者間で責任分界があいまいになりやすい。**
- 法規制上の問題やクラウドサービスカスタマのセキュリティポリシー等に関連して、外国や外国法適用配下に情報を置くべきでないとされているにも関わらず、サプライチェーンの配下に該当する事業者が存在し、**カスタマの意図に反する状態に陥ってしまう。**

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。



複数のサービスに跨がって扱われるデータを円柱で表現した。

クラウドサービスの多層性をレイヤーで表現し、各社の責任分界を含む「場」を示した。

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。

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

特にご議論いただきたい内容

- 今後の進め方について、フレームワーク案（本文＋ユースケース等）をパブリックコメントにかけることとしてよいか。

フレームワーク案について、特にご意見をいただきたい事項

- パブコメを受けての修正箇所について
- ユースケース、リスクの洗い出しについて
- フレームワークVer1.0公開に向けた進め方
- 今後の展開について

今後の進め方（案）