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

適用実証報告書

令和5年3月

経済産業省 商務情報政策局 サイバーセキュリティ課

目次

1. 適用実証の実施概況

経済産業省では、令和4年4月、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けるデータの信頼性確保の考え方を整理した「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」（以下、DMF）を公表した。DMFは、データの利活用を推進する事業者がデータの状態を可視化し、ステークホルダーの間で認識を共有しやすくすることによって、ステークホルダー全体での適切なデータマネジメントの実施につなげるためのフレームワークと捉えることができる。

一方で、DMFの策定に向けた検討会の議論の中では、DMFの記載に未だ抽象的な内容が多く理解が難しいという意見や、地方自治体やOT（Operational Technology）分野のケーススタディをさらに拡充すべきという意見が提示され、DMFの更なる具体化・高度化を望む声が多く聞かれた。

そこで、本年度は、参考となる事例の蓄積を通じた利用促進やDMFの改善点の洗い出しを目的として、先進的な取組を行う事業者より協力を得て、表1-1に示す6件のDMFの適用実証を実施した。各適用実証については、2章で詳細を示す。

表1-1 令和4年度事業で推進した適用実証の一覧

No.	参画事業者	適用対象の名称	記載箇所
1	デンソー	車両データ活用基盤の利用による製品開発・改善の推進等	2-1
2	竹中工務店	ヒューマンファクターと人工知能を用いた次世代建物制御システム	2-2
3	三菱電機	製造装置の稼働データ等を活用した予防保全・製品向上	2-3
4	シップデータセンター	IoS-OP（Internet of Ships Open Platform）による船舶運航データの流通	2-4
5	パナソニック	人起点のデータ取得によるワークプレイスの空間価値の継続的アップデート	2-5
6	富士通	ネットワークインフラシステムのリプレースを対象とした設計構築における関係者間の情報共有	2-6

また、上記適用実証の実施と並行して、参画いただいた各社から、以下のようなDMF

改善のためのデータを収集し、今後のDMF及び関連する検討活動へのインプットとすることとした。それらの内容については、3章を参照されたい。

- 適用した際に感じたメリット/デメリット
- 適用して気付いた新たなリスク
- 適用の際の問題点/悩んだ点 (他の文献とのハレーションを含む)
- DMF改訂に向けた要望

2. 各適用実証事業の概要

2-1. 車両データ活用基盤の利用による製品開発・改善の推進等

近年、コネクテッドカーの普及に伴い、車両メーカーが市場の車両データを入手可能な状況が出来つつあり、近い将来、企業間で車両データを共有し、共同で製品開発・サービス検討を行う業務が生まれることが想定される。そのような環境変化に伴い、一部の自動車関連事業者においては車両データを分析し、品質向上や新価値創出に向けた検討・活用を既に始めている。

本章では、株式会社デンソー（以下、「デンソー」という。）の協力を得つつ、車両から取得したデータを蓄積・分析することを通じて製品開発・改善等に活用する車両データ活用基盤に係る試み（本節において、以下、「本ユースケース」という。）をフレームワークの適用対象として取り上げる。

- デンソーは、自社、グループ会社及び、顧客の運送会社で利用されている社用車にデータ取得装置等を設置し、当該車両の位置情報、車両制御情報等を収集し、外部クラウドインフラ上に構築した「車両データ活用基盤」に蓄積している。収集データについては、今後ドライブレコーダによる「カメラ画像」や、周辺物体データを含む「センサデータ」を追加することを検討している。
- 車両データ活用基盤に蓄積したデータに対して、デンソーの技術者が可視化ツールや機械学習ツールを適宜用いて、走行経路、操作挙動、走行画像等の分析を行い、自社の製品開発・改善の目的で利用する。データ活用基盤の利用範囲としては、現行の国内のデンソー社員に加えて、欧州拠点の社員及びグループ会社員を追加し、デンソーグループ外部である第三者に対して「データ活用レポート」を提供することも検討している。
- システムの開発・運用・保守は、現在、日本の担当者が実施しているが、今後は海外(例：インド)の事業者へ業務委託することも想定している。

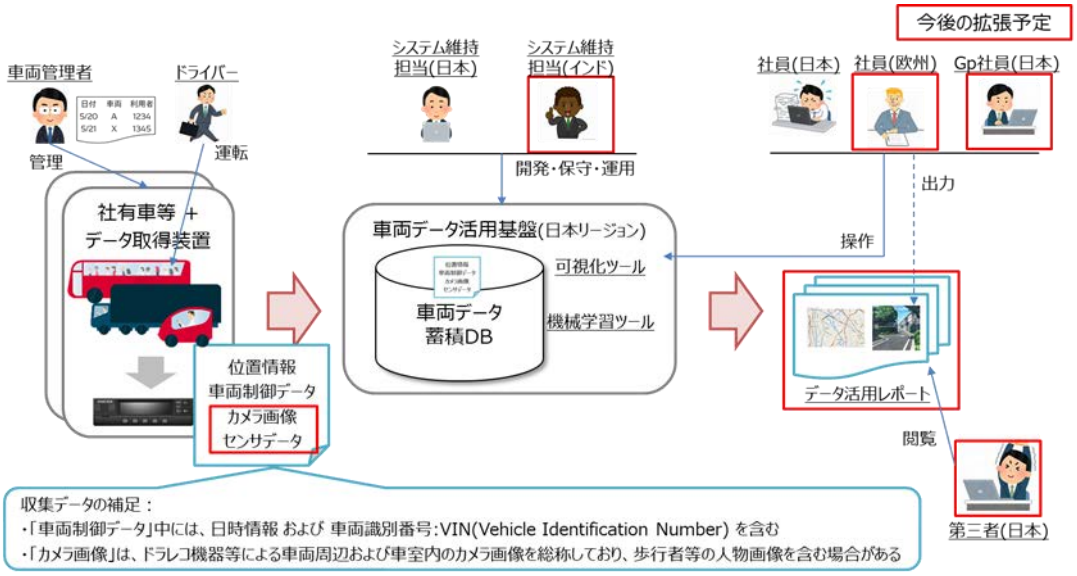

図2.1-1 車両データ活用基盤の概要

デンソーでは基盤を既に運用しており、その企画・設計・開発時に基本的なリスク対応を実施しているが、図2.1-1にて赤枠で示すような今後のサービス拡張部分におけるリスク対応の検討を念頭におきつつ、既存運営領域に対する検討内容の妥当性確認も兼ねて、DMFを用いたリスク及び対策の特定を実施することとした。

その際、本ユースケースにおいて考慮すべきステークホルダーとして以下が挙げられる。

- デンソーおよびグループ会社：自社、グループ会社及び、外部の運送会社向けに車両データ活用基盤の開発・保守・運用を行う。同基盤に係る業務の一部を、日本またはインドに拠点を有するシステム運用支援事業者に委託している。
  - ー 車両管理者及びドライバは、業務実施のためデータ取得装置を設置した社有車を運転する。
  - ー システム維持担当者は、車両データ活用基盤の開発・保守・運用を行う。日本または欧州の拠点から社員は基盤上のデータにアクセスし、許容された目的の範囲内でレポートの作成等を行う。
- 運送会社：自社社有車のデータ取得装置から車両データ活用基盤にデータを提供し、その対価としてデータ活用レポートの提供を受ける。
- 第三者：デンソーおよびグループ会社、運送会社以外の事業者であって、データ活用レポートの提供を受ける者。
- システム運用支援事業者：デンソーからの委託を受けて、車両データ活用基盤の開

発・保守・運用に係る業務を実施する。

2-1-1.　STEP 1　データ処理フロー（「イベント」）の可視化

本ユースケースでは図2.1-2で示すように、以下のプロセスにより構成される。

(1) デンソー及びグループ会社、運送会社の社用車に設置されたデータ取得装置から、位置情報や車両制御情報、ドライブレコーダによるカメラ映像、その他のセンサデータからなる車両関連データを生成・取得する。データ収集は、日本国内の拠点だけでなく、各社の欧州拠点でもなされる。取得されたデータは、無線ネットワーク経由で車両データ活用基盤へ集約される。

(2) 各社から提供を受け車両データ活用基盤上に集約された「統合車両データ」は、技術者(社員)が製品開発や改善の目的に適する「高次データ」（例：走行経路、操作挙動、走行画像）に加工・利用される。

(3) 「高次データ」は、提供先の要求に応じて移転・提供され、場合に応じて各社が有するデータとも突合され、「調査データ」に加工・利用される。また、第三者事業者に対しても、提案内容に応じて「加工・利用」され、活用レポートとして「移転・提供」される。

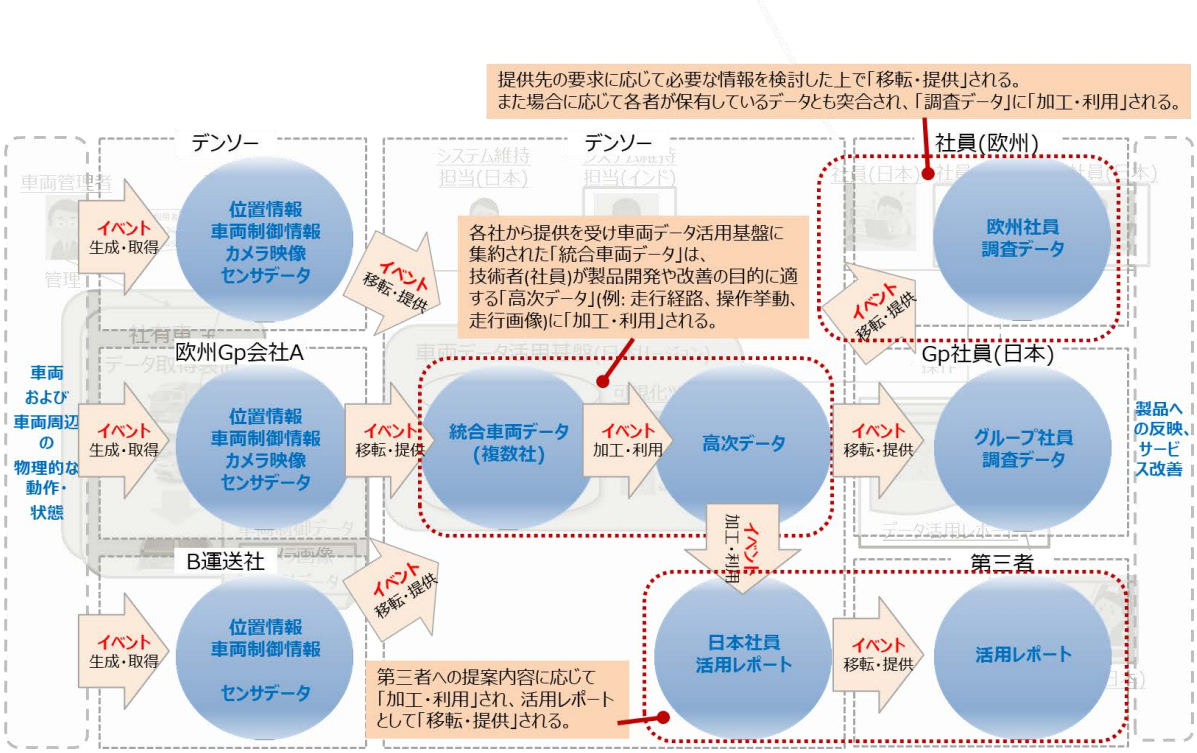

図2.1-2 データ処理フローの可視化（車両データ活用基盤）

2-1-2.　STEP 2　必要な制度的な保護措置（「場」）の整理

STEP 2は、STEP 1で特定された一連のデータ利活用プロセスに対して、「場」としてどのようなデータの保護に係るルール（規範）が課せられ得るかを理解する段階である。本ユースケースにおいて、取扱うデータの性質や事業者の業種等を考慮すると、例えば下記のルールが「場」として特定され得る。

（1）個人情報保護法：デンソー及びグループ会社、運送会社の国内拠点で運用される社有車から取得するデータのうち、ドライブレコーダにより収集される「カメラ画像」には車室内外の映像が含まれ、ドライバ及び歩行者等の人物画像やドライバのIDを含む場合がある。車両制御情報やセンサデータには特定の個人を識別できる情報は含まれていないものの、「統合車両データ」はドライバID等を含めてデンソーによってデータベース化されているので、「個人データ」に該当することになると考えられる。当該データの加工・利用、移転・提供、保管、廃棄にあたっては、加工済みデータの個人データ該当性を考慮したうえ個人情報取扱事業者の義務を遵守しなければならない。

（2）一般データ保護規則（GDPR）：デンソーの欧州所在のグループ会社で運用される社有車から取得される「カメラ画像」の処理や移転にあたっては、GDPRの諸規定への対応が必要となる。欧州拠点で取得した個人データを、十分性認定に基づきEU[1]及び英国域内から日本国内へ移転する場合、移転を受けた個人データを取扱う事業者は、日本の個人情報保護法に加え、「個人情報の保護に関する法律に係るEU及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」（以下、「補完的ルール」という）を遵守することが必要である。図A-1.3では、GDPR及び十分性認定に影響される形で「補完的ルール」の遵守を要する点も含めて示すため、欧州拠点におけるデータ取得及び移転時のみならず、車両データ活用基盤において処理がなされる段階にもGDPRの適用範囲を記している。

---

[1] ここでの「EU」とは、欧州連合加盟国及び欧州経済領域（EEA：European Economic Area）協定に基づきアイスランド、リヒテンシュタイン及びノルウェーを含む、欧州連合（European Union）を指す。

（3）社用車使用要領：デンソー及びグループ会社が内部規則として社用車の利用方法等を定めるもの。データ取扱関連規定については、取得データの利用目的・開示制約として、グループ会社その他業務提携先・業務委託先（”デンソー等”）において交通安全推進・啓発活動、事故・クレーム処理及び車両を使用した研究開発の目的に使用する旨を規定している。

（4）運送車両データの取得及び利用契約書：「車両データ活用基盤」を利用するにあたり、デンソーと運送会社との間で合意されるもの。取得データの利用目的・開示制約として、車両向け製品・サービスの開発を目的に自己の役員および従業員（派遣社員および下請け契約社員を含む）が利用できる点を規定している。本契約書には機密保持条項があり、運送会社から得るデータに含まれる位置情報が対象となる。

（5）車両データ活用基盤利用規約：デンソー及びグループ会社において、車両データ活用基盤の利用に際して遵守しなければならない社内規則であり、以下の条項を含む。

- データは会社業務および自己研鑽の目的においてのみ利用可能
- 基盤にて提供されるデータの再配布は禁止
- 分析結果をOEMやグループ会社へ共有することは問題なし
- 基盤にて提供される一部データは個人情報保護法の対象となる場合があるため、基盤からの抽出後も各部署のサーバーや関連するクラウドサービス等のアクセス管理されたサーバー上で保管し、ローカルPCには保管しない

（6）秘密保持契約等：車両データ活用基盤上でデータを加工して作成される「活用レポート」の提供先となる第三者（デンソー及びグループ会社、運送会社以外の事業者を想定）とデンソーとの間で締結されるもの。「活用レポート」等の第三者へ移転・提供されるデータの目的外利用の禁止、秘密保持義務、その他のデータ取扱い関連の条項を規定する。

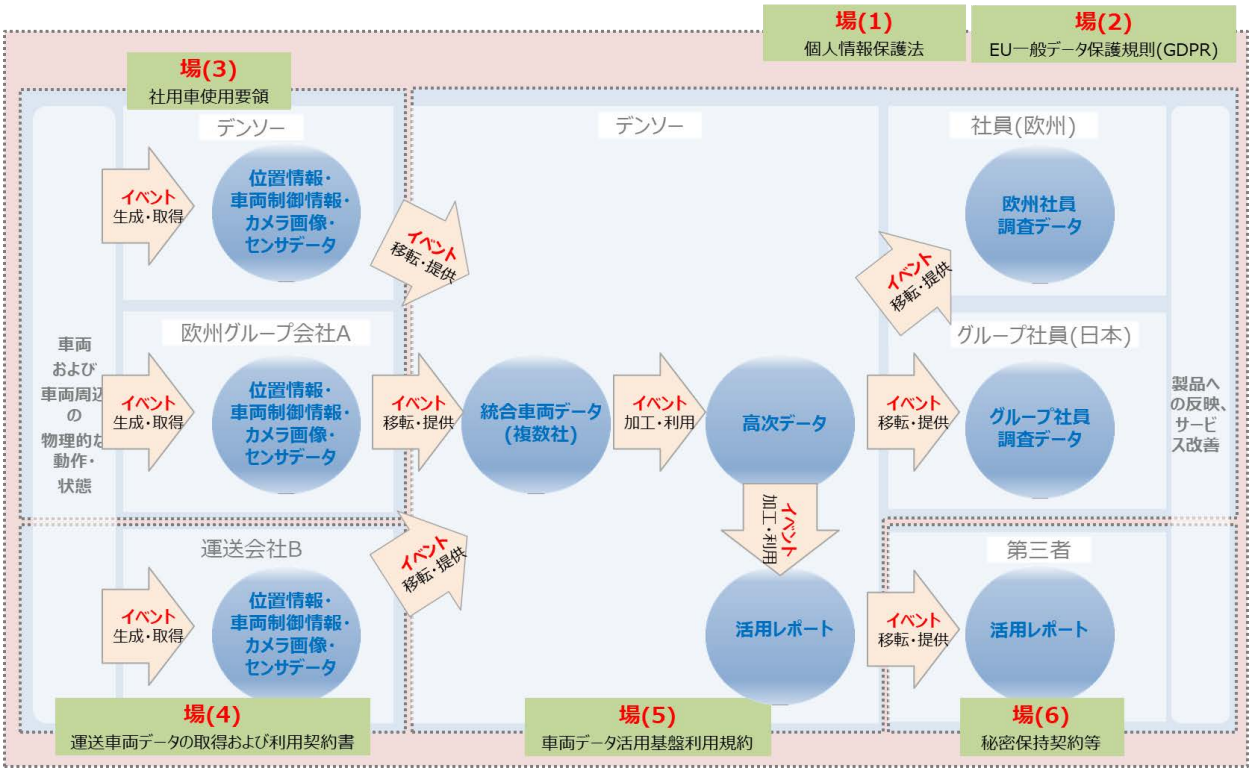

図2.1-3 必要な制度的な保護措置の整理（車両データ活用基盤）

本ユースケースでは、知的財産保護の観点に関連して、著作権・特許権に類する情報を含まない。また、輸出管理の対象となる機微な技術情報は含まれないと想定されるため、「場」として外為法を含めていない。データローカライゼーション（データの国内保管義務等）に関する規定については、基盤およびデータの提供国・地域が追加される度、あるいは法規改訂に基づき、継続的確認が必要である。

2-1-3. STEP 3 「属性」の具体化

属性の具体化にあたり、表A.1-2に示すように、まずはSTEP 2で特定した「場」を、各「属性」項目のパラメータの設定にあたりどのように考慮できるかを検討した。ここで考慮する属性項目としては、DMFに示される一般性のあるものとして、カテゴリ（パーソナルデータ保護、知的財産・営業秘密保護）、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、利用期限を挙げた。

表2.1-1 「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	GDPR	社用車使用要領	運送車両データの取得および利用契約書	車両データ活用基盤利用規約
カテゴリ	パーソナルデータ保護	○	○			○
	知的財産・営業秘密保護				○	○
	…					
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					○	

上記で特定した「場」の関係規定も参照しつつ、各「属性」項目のパラメータを設定した。ここで、属性を設定する対象のデータとしては、STEP 2までに特定した以下のデータを扱う。

- 位置情報・車両制御情報・カメラ画像・センサデータ（デンソー/欧州所在のグループ会社/運送会社にて取得）
- 統合車両データ
- 高次データ
- 活用レポート
- 調査データ（欧州グループ会社社員/国内グループ会社社員）

表2.1-2 本ユースケースにて取扱うデータの「属性」パラメータ例

		位置情報・車両制御情報・カメラ画像・センサデータ(デンソー)	位置情報・車両制御情報・カメラ画像・センサデータ(欧州グループ会社)	位置情報・車両制御情報・センサデータ(運送会社)	統合車両データ
カテゴリ	パーソナルデータ保護	個人情報を含む	個人情報を含む	個人情報を含む	個人情報を含む
	知的財産・営業秘密保護	-	-	運送会社の営業秘密を含む	-
	…	…	…	…	…
開示範囲		(1)デンソーおよびグループ会社、その他業務提携先・業務委託先	(1)と同等	必要のあるデンソーの役員および従業員(派遣社員および下請け契約社員を含む)	(1)と同等
利用目的		(1)車両を使用した研究開発	(1)と同等	運送車両向け製品・サービスの開発	会社業務および自己研鑽
データ管理主体		デンソー	デンソー	デンソー	デンソー
データ権利者		デンソー	グループ会社、デンソー	運送会社、デンソー	デンソー
価値（重要度）		高	高	高	非常に高
媒体・保存先		データ取得装置	データ取得装置	データ取得装置	車両データ活用基盤
利用期限		-	-	契約日から１年間、ただし永続的自動延長あり	-

表2.1-2 本ユースケースにて取扱うデータの「属性」パラメータ例（続き）

		高次データ	活用レポート	欧州社員調査データ	グループ会社 社員調査データ
カテゴリ	パーソナルデータ保護	個人情報を含む	該当なし (統計データ、匿名加工情報へ加工)	該当なし (統計データ、匿名加工情報へ加工)	該当なし (統計データ、匿名加工情報へ加工)
	知的財産・営業秘密保護		-	-	-
開示範囲		(1)デンソーおよびグループ会社、その他業務提携先・業務委託先	(1)デンソーおよびグループ会社、その他業務提携先・業務委託先 (2)第三者	欧州グループ会社社員	グループ会社社員
利用目的		会社業務および自己研鑽	(1)と同等	(1)と同等	(1)と同等
データ管理主体		(2)と同等	デンソー	欧州グループ会社	グループ会社
データ権利者		デンソー	デンソー	欧州グループ会社社員	グループ会社社員
価値（重要度）		非常に高	非常に高	非常に高	非常に高
媒体・保存先		車両データ活用基盤	・車両データ活用基盤 ・デンソーサーバ等 ・第三者サーバー等	欧州グループ会社サーバー等	グループ会社サーバー等
利用期限		-	-	-	-

2-1-4. STEP 4 「イベント」ごとのリスクポイントの洗い出し

2-1-4-1. 「イベント」ごとのリスクポイントの洗い出し

本STEPでは、対象のデータ利活用プロセスにおいて、セキュリティ及び関連する法

制度等の観点からいかなるリスクが想定されるかを特定する。その際、セキュリティの保護に係る観点（機密性、完全性、可用性）及び関連する法制度等の観点（パーソナルデータ保護、知的財産（営業秘密を含む）保護）を考慮してリスクの特定を行う。

ここでは、車両データ活用基盤に係るデータの利活用プロセスを以下の4つに区分して、それぞれでリスクの特定を行った。

- 「位置情報、車両制御情報、カメラ映像、センサデータ」の「生成・取得」及び「移転・提供」
- 「統合車両データ(複数社)」及び「高次データ」への「加工・利用」
- 「高次データ」の「移転・提供」
- 「日本社員活用レポート」への「加工・利用」及び「移転・提供」

「位置情報、車両制御情報、カメラ映像、センサデータ」の「生成・取得」及び「移転・提供」過程においては、セキュリティに係る観点として、データの生成・取得に用いられる車載機器（データ取得装置）、当該機器と車両データ活用基盤との間のネットワーク上で想定される脅威（なりすまし、改ざん等）が抽出された。また、法制度等に係る観点に関しては、「位置情報、車両制御情報、カメラ映像、センサデータ」として個人に関するものを含むデータが取得される点、それらのデータがグループ会社や運送会社から車両データ活用基盤を提供するデンソーに提供される点を踏まえてリスクを特定した。なお、一部のデータは欧州所在のグループ会社で取得され、日本所在の基盤へ移転されることから、欧州拠点におけるGDPRの処理要件遵守に加えて、移転を受けたデンソー側において個人情報保護法に加えて「補完的ルール」の順守が必要な点に留意する必要がある。

表2.1-3 「位置情報、車両制御情報、カメラ映像、センサデータ」の「生成・取得」及び「移転・提供」にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	「位置情報、車両制御情報、カメラ映像、センサデータ」が、車両から車両データ活用基盤までのネットワーク上で内部犯行者又は外部の攻撃者に傍

			受され、漏えいする。
		マルウェア感染	「位置情報、車両制御情報、カメラ映像、センサデータ」がマルウェアに感染した車載機器等から不正な送信先へ共有される。
	完全性	なりすまし	データ取得用途の車載機器等を不正な機器によりなりすまされ、車両データ活用基盤において正確でない「位置情報、車両制御情報、カメラ映像、センサデータ」が生成・取得される。
		改ざん	「位置情報、車両制御情報、カメラ映像、センサデータ」が、車両から車両データ活用基盤までのネットワーク上で内部犯行者又は外部の攻撃者に傍受され、改ざんされる。
	可用性	サービス不能	センサー等の車載機器がマルウェアに感染して稼働停止し、「位置情報、車両制御情報、カメラ映像、センサデータ」を生成・取得できない。
		システムの不具合	「位置情報、車両制御情報、カメラ映像、センサデータ」の生成・取得に係る車載機器に故障等の不具合が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	適法な手段によるデータ取得	「位置情報、車両制御情報、カメラ映像、センサデータ」を取得するデンソー、グループ会社または運送会社が、データの利用目的等の必要事項をデータ元の個人に対して明確に示していない、又は利用の実態と対応した形で提示していない。
			「位置情報、車両制御情報、カメラ映像、センサデータ」を取得するデンソー、グループ会社または運送会社が、偽り等の不正の手段により個人情報を取得している。
			「位置情報、車両制御情報、カメラ映像、センサデータ」に含まれる歩行者等が映り込んだ画像データがアイコン化等の事前に定められた処理を経ることなく車両データ活用基盤に蓄積される。

		許諾等のない第三者提供	グループ会社または運送会社が、事前の本人同意取得又はオプトアウトに係る手続(委託、共同利用等を含む)等の実施なしに、「位置情報、車両制御情報、カメラ映像、センサデータ」をデンソーまたはそのグループ会社に提供する。
		適正な手続きを踏まない越境データ移転	欧州に所在するグループ会社が、GDPRに定めるデータ処理要件の実施なしに、「位置情報、車両制御情報、カメラ映像、センサデータ」をデンソーまたはグループ会社に提供する。
			欧州で生成された「位置情報、車両制御情報、カメラ映像、センサデータ」を扱う日本所在の基盤上で「補完的ルール」の実施がなされていない。
	知的財産・営業秘密保護	適法な手段によるデータ取得	悪意のある従業員又は退職者を含む第三者が、運送会社から得た位置情報等の秘密情報を不正な方法(窃取、詐欺、強迫、その他の不正な手段)で取得している。

社有車から取得したデータが車両データ活用基盤に共有された後の、「統合車両データ(複数社)」及び「高次データ」への「加工・利用」過程では、セキュリティに係る観点としては基盤への不正アクセスやマルウェア感染、データ改ざん、システムの停止等、ITサービスの利用・運用において通常考慮すべきリスクが存在する。一方で法制度等については、パーソナルデータ保護や契約遵守の観点から利用目的の逸脱や、加工の結果として二次的に生成される派生データの取扱い、複数社の要保護データのコンタミネーション等がリスクとして特定された。

表2.1-4 「統合車両データ(複数社)」及び「高次データ」への「加工・利用」にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	加工・利用過程において、権限のない内外の主体(システム維持担当、競合関係にある運送会社等を含む)により対象となるデータの全部又は一部が不正アクセスされ、自社又は他社の機密データが特定され、漏えいする。
		情報漏えい	「統合車両データ(複数社)」及び「高次データ」の加工基準やアクセス管理に不備があり、参照権限のあるサービス利用企業により、本来特定されるべきでない自社又は当該企業以外の他社の機密データが特定される。
	完全性	改ざん	悪意のある内外の主体により車両データ活用基盤上のデータ処理アプリケーションの設定等が改ざんされ、データの処理にあたって不正な処理が行われる。
		改ざん	悪意のある内外の主体により意図的に加工・利用の結果として生じる「統合車両データ(複数社)」及び「高次データ」の全体又は一部が改ざん又は削除される。
		システムの不具合	クラウドサービス事業者が提供する車両データ活用基盤を構成する設備や機器の一部に、故障等による障害や誤動作が発生し、集約結果の完全性が損なわれる。
	可用性	サービス不能	サービス妨害攻撃、マルウェア感染等により、クラウドサービス事業者が提供する車両データ活用基盤を構成する設備や機器が一時的に停止する。
		システムの不具合	過度の処理リクエスト等により、クラウドサービス事業者が提供する車両データ活用基盤を構成する設備や機器に不具合が生じ、処理が一時的に停止する。

		自然災害等	地震や津波等の自然災害により、クラウドサービス事業者が提供する車両データ活用基盤を構成する設備や機器に被害が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	提供先での目的外利用	従業員により必要な手続きを踏むことなく、事前にデータ取得元の個人へと通知したものとは異なる目的で「統合車両データ(複数社)」または「高次データ」が利用される。
	知的財産・営業秘密保護	提供先での目的外利用	必要な手続きを踏むことなく、「統合車両データ(複数社)」または「高次データ」が、「車両データ活用基盤利用規約」においてデータ提供元と合意した利用条件(利用目的、利用権限等)とは異なる方法で利用される。
			正当な手段によりデータを取得した悪意のある内外の主体(退職者を含む)により、不正の利益を得る目的又は権利元に損害を加える目的で「統合車両データ(複数社)」及び「高次データ」が使用される。
			「高次データ」を含む派生データの利用権限が「車両データ活用基盤利用規約」において十分に定められておらず、利用目的や第三者提供の可否等についてデータ取得元の個人や組織からクレーム等が生じる。
		提供先に起因するデータアクセスの制限	データ取得元の個人や組織による「統合車両データ(複数社)」及び「高次データ」に対するアクセスやそれを活用したサービスの利用機会が制限されている。

「高次データ」のデンソー社内及び日欧のグループ会社への「移転・提供」においては、セキュリティの観点からネットワーク上の脅威（なりすまし、改ざん等）、法制度等の観点からは第三者提供時の手続きの不備等がリスクやその要因として特定された。特に、個人データを移転する際には、国内、あるいは国外への移転で実施すべき事項が個別に定められている点に留意が必要である。

表2.1-5 「高次データ」の「移転・提供」にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	「高次データ」が、車両データ活用基盤から第三者のシステムまでのネットワーク上で悪意のある第三者に傍受され、漏えいする。
		なりすまし、情報漏えい	正規の利用者になりすまされる、または脆弱性を悪用され、車両データ活用基盤に不正アクセスされ、「高次データ」が閲覧、または車両データ活用基盤から不正な送信先へ移転される。
	完全性	改ざん	「高次データ」が、車両データ活用基盤から第三者のシステムまでのネットワーク上で悪意のある第三者に傍受され、改ざんされる。
	可用性	サービス不能	サービス妨害攻撃、マルウェア感染等により、クラウドサービス事業者が提供する車両データ活用基盤を構成する設備や機器が一時的に停止する。
		システムの不具合	過度の処理リクエスト等により、クラウドサービス事業者が提供する車両データ活用基盤を構成する設備や機器に不具合が生じ、処理が一時的に停止する。
		自然災害等	地震や津波等の自然災害により、クラウドサービス事業者が提供する車両データ活用基盤を構成する設備や機器に被害が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	許諾等のない第三者提供	デンソーが、事前の本人同意取得又はオプトアウトに係る手続(委託、共同利用等を含む)等の実施なしに、「高次データ」を第三者に提供する。
			「高次データ」の第三者提供を行う際に、提供を行う側(デンソー)、提供を受ける側(グループ会社、第三者)のいずれか又は双方において記録の作成、確認の実施が行われない。
			「高次データ」を外国にある第三者に提供する際、本人同意の取得、適切な情報提供等の遵守すべき手続きが実施されない。

	知的財産・営業秘密保護	許諾等のない第三者提供	悪意のある従業員又は退職者を含む第三者が、不正取得行為（窃取、詐欺、強迫、その他の不正な手段）により取得した営業秘密を移転・提供する。
			「運送車両データの取得および利用契約書」で定められる利用目的等の範囲を超えて、運送会社の許諾等なしに「高次データ」の移転・提供が行われる。

最後に、第三者事業者（デンソー、グループ会社、運送会社以外の事業者を指す）向けの「日本社員活用レポート」への「加工・利用」及び「移転・提供」過程においては、セキュリティに係る観点としては車両データ活用基盤及び、同基盤から第三者のシステム環境までのネットワーク上の脅威を特定した。加えて、法制度等に係る観点からは「日本社員活用レポート」の作成や第三者による閲覧という利用形態が、データ主体の個人へと提示された利用目的や契約等で合意されたものと整合しているか等がリスク要因として検討された。

表2.1-6　「日本社員活用レポート」への「加工・利用」及び「移転・提供」にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	車両データ活用基盤から第三者のシステム環境までのネットワーク上で、「日本社員活用レポート」を含むデータが悪意のある第三者に傍受され、漏えいする。
		なりすまし、情報漏えい	正規の利用者になりすまされる、または脆弱性を悪用され、車両データ活用基盤に不正アクセスされ、「高次データ」が車両データ活用基盤から不正な送信先へ移転される。
	完全性	改ざん	悪意のある内外の主体により車両データ活用基盤上のデータ処理アプリケーションの設定等が改ざんされ、データの処理にあたって不正な処理が行われる。
		改ざん	悪意のある内外の主体により意図的に加工・利用の結果として生じる「日本社員活用レポート」の全体又は一部が改ざん又は削除される。

		なりすまし、改ざん	車両データ活用基盤から第三者のシステム環境までのネットワーク上で、「日本社員活用レポート」を含むデータが悪意のある第三者に傍受され、改ざんされる。
	可用性	サービス不能	サービス妨害攻撃等によりデータの移転・提供に係る設備や機器が一時的に停止する。
		システムの不具合	データの移転・提供に係る設備や機器に不具合が生じ、処理が一時的に停止する。
		自然災害等	地震や津波等の自然災害によりデータの移転・提供に係る設備や機器に被害が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	提供先での目的外利用	「日本社員活用レポート」の作成や第三者による閲覧という利用形態が、事前にデンソー、グループ会社または運送会社に所属するデータ取得元の個人へと通知したものや、「社用車使用要領」、「運送車両データの取得および利用契約書」で示したものと異なる。
		許諾等のない第三者提供	「日本社員活用レポート」を外国にある第三者提供に提供する際、本人同意の取得、適切な情報提供等の遵守すべき手続きが実施されない。
	知的財産・営業秘密保護	提供先での目的外利用	「日本社員活用レポート」の作成や第三者による閲覧という利用形態が、事前にデンソー、グループ会社または運送会社に所属するデータ取得元の個人へと通知したものや、「社用車使用要領」、「運送車両データの取得および利用契約書」で示したものと異なる。
			正当な手段によりデータを取得した悪意のある内外の主体(退職者を含む)により、不正の利益を得る目的又は権利元に損害を加える目的で「日本社員活用レポート」が取得される。

2-1-4-2. 今後のデータ管理の高度化に向けた課題の検討

STEP 1からSTEP 4までの成果を今後のデータ管理の高度化に活用するため、本節ではSTEP 4で特定されたリスクに対応するための主なデータ管理施策を示す。

- ドライブレコーダにより取得される歩行者等が映り込みうるカメラ画像の取扱い[2]
  - ✓ プライバシーに係るリスクアセスメントを実施したうえで取得したデータに対して人物領域のアイコン化を実施し、特定の個人の識別には至らない処理を行うプロセスを含める。
  - ✓ 事前告知時や取得時に、カメラにより歩行者等の画像が取得、利用されていることについて、歩行者等が容易に認識可能となるよう、車両内外の見やすい位置にシールを掲示したり、車内に取組のパンフレットを配置したり、自社ウェブサイト上へ掲載したりする。

- 事業者別のデータ管理
  - ✓ 他社から得た秘密情報については、自社情報と分離して管理する。
  - ✓ 自社情報と、他社情報が混在してしまうと、他社から訴えられたときに「他社の秘密情報を使っていないこと」を立証することが極めて困難となるため、情報が混在しないための管理をしっかり行っていたことを立証できるようにしておくことが重要。

- 「システム維持担当(インド)」による車両データ活用基盤内へのデータアクセス制御
  - ✓ 在インドの事業者により車両データ活用基盤内の個人データへのアクセスが可能な場合、データ取得元からの同意取得、貴社による委託先の安全管理の監督等の対応が必要。
  - ✓ 当該事業者が、個人データを取り扱わないこととなっている場合には、貴社は個人データを提供したことにはならないため、個人情報保護法の規定に基づく「本人の同意」取得、委託先監督等の義務は生じない。
  - ✓ 当該事業者が、個人データを取り扱わないこととなっている場合とは、契約条項によって当該事業者がサーバーに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等が考えられる。

- 「統合車両データ(複数社)」及び「高次データ」の利用目的

[2] より具体的な対策内容については、IoT 推進コンソーシアム・総務省・経済産業省「カメラ画像利活用ガイドブック ver.3.0」の適用ケース(5)等を参照されたい。

- ✓ 「社用車使用要領」、「運送会社との契約書」及び「車両データ活用基盤利用規約」における収集データの利用目的は、第三者への「データ活用レポート」提供等の商用利用を必ずしも示唆していないように見えるため、契約文書の更新(例：利用目的、「高次データ」等の派生データの取扱い)、本人への通知等が必要になる可能性がある。
- ✓ 同意取得等が困難な場合等はレポートを個人情報に該当しない統計情報から構成する、データ取得元の運送会社の競合事業者に当該事業者のレポートを提供しない等の対応が必要になる可能性がある。

- 欧州への越境移転への対応
  - ✓ 日本から欧州へのデータ移転の場合、通常はGDPRではなく日本の個人情報保護法(外国にある第三者への提供に係る規定)の適用を受ける。
  - ✓ EU加盟国及び英国は「我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として規則で定めるもの」に該当するため、国内事業者にデータを提供する際と同様の規律(本人同意の取得、委託・共同利用の適用等)に服することが必要。

2-2. ヒューマンファクターと人工知能を用いた次世代建物制御システム

近年、建設業界において、設計・施工・維持管理業務の デジタル化が進んでおり、スマートビルと呼ばれる高度な制御機能を有した建物が増えてきている。従来のビルの設備システムはオフラインを前提としたローカルシステムであったが、クラウド、IoT（Internet of Things）、人工知能（AI: Artificial Intelligence）、外部データ連携等を用いたスマートビルへの移行を通じて、省エネや快適性・利便性の向上などを実現する方向性が提唱されつつある[3]。スマートビル増加の理由としては、技術革新に加え、3次元形状や部材の属性情報なども含んだ総合データベースといえる BIM（Building Information Modeling）の普及、震災による省エネ・BCP 需要の高まり、人材不足などの社会的要請が挙げられる。

上記の背景を踏まえ、スマートビルを対象としたDMFのユースケースとして、IoTデータやAIを活用した次世代建物制御システム（本節において、以下、「本ケース」という。）を取り上げる。

- 株式会社竹中工務店（以下、「竹中工務店」という。）は、ビルオ－ナーが管理する建物で稼動する建物設備システム群（例：照明システム、空調システム）やIoTセンサー・システム群を通じて、ゲートウェイにてプロトコル変換を行いつつ、自社の運用するデータプラットフォーム“ビルコミ”（以下、「ビルデータPF」）へビル設備の稼働データ（BAデータ）やIoTデータを共有する。
- 上記データは、BIMデータを加工して作成された建物設備やIoTなどが抽象化されたデータ表現である「建物メタデータ」と紐づけられ、テレメトリデータとしてビルの快適性向上や制御の高度化を目的として利用される。

[3] 例えば、情報処理推進機構（IPA）デジタルアーキテクチャ・デザインセンター（DADC）にて実施されているスマートビル将来ビジョン検討会の活動等がある。
（https://www.ipa.go.jp/digital/architecture/project/smartbuilding/about.html）

- ビルデータPFに蓄積されたテレメトリデータは外部のAIサービスプロバイダに提供され、機械学習エンジン（強化学習）による設備制御最適化を実現する。

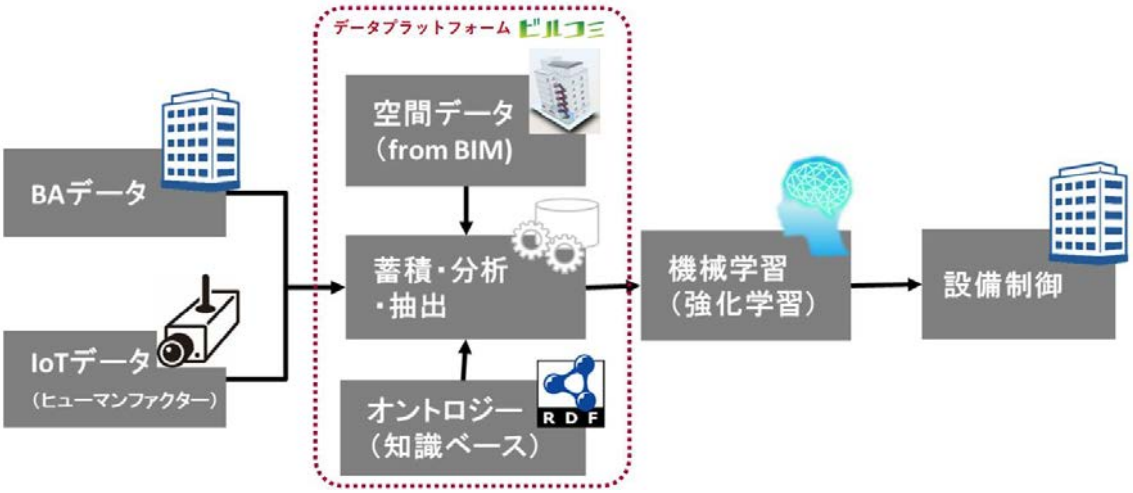

図2.2-1 本ケースで取扱う次世代建物制御システムの概要

竹中工務店では、従来からスマートビルの取組みを支援するプラットフォーム事業を展開しているが、今回は比較的大規模な機能のアップデートに伴い、改めてリスクアセスメント等の取組みを進める中、かかる取組みの一環として、図2.2-1に示す建物制御システムを対象にDMFを活用したリスクアセスメントを実施した。スマートビルの取組みには非常に多くのステークホルダーが関与し、ともすれば責任分界が曖昧になることも想定されるため、本件を通じた責任や対策の明確化を行うことを目的とした。

本ケースにおいて考慮すべきステークホルダーとして以下が挙げられる。

- 竹中工務店：建物の運用効率化・機能高度化を支援するため、ビルオーナー向けにビルデータPFを開発・運用・管理している。同PFに係る業務のうち、設備制御の効率化に必要な分析等をAIサービスプロバイダのサービスを利用する形で実施している。
- ビルオ―ナー：ビルデータPFを通じたサービスの提供を受けるビル及びそれを構成する建物設備システム群の運用・維持管理を行う。
- AIサービスプロバイダ：クラウドサービスとして機械学習エンジン（強化学習）を提供している事業者であり、竹中工務店よりテレメトリデータの提供を受けて、各種ビル設備制御の効率化を支援している。

2-2-1.　STEP 1　データ処理フロー（「イベント」）の可視化

本ケースでは図2.2-2で示すように、以下のプロセスにより構成される。

- ビルオーナーの管理するビルで稼動する設備（ここでは、電力量計、空調機関連、照明器関連を想定）から「照明稼動データ」（輝度・明るさ感）、「空調機稼働データ」（風量、送風温度、熱源の効率など）、「電力使用量」（これらを総称して、「BAデータ」と呼称する）、別途設置しているカメラから「カメラ画像」を生成・取得し、エッジ処理により個人を特定できない「利用者状況」（活動量、着衣量、人流・属性など）へと加工したうえで、それぞれビルデータPFへと移転・提供される。また、ビルオーナー側で保有している「維持管理・運用BIMデータ」についても、一定の加工を行ったうえでゲートウェイを通じてビルデータPFへと移転・提供される。ビルデータPF上では、特定の個人を特定できる情報は取り扱わない仕様となっている。
- ビルデータPF上では、ビルオーナーから受領したデータに対して事前に定義したルールに基づき前処理が行われ、「テレメトリデータ」へと加工・利用される。テレメトリデータは、BIMから取得した空間データと設備／IoTのポイント情報に各ビル設備で生じるイベントの情報を紐づけたものと理解することができる。また、かかるデータ処理はリアルタイム処理のためのスピードレイヤ及びバッチ処理のためのバッチレイヤで処理される。
- リアルタイムに取得された、あるいは蓄積された「テレメトリデータ」のうち必要な部分は、ビルデータPFのAPI[4]を用いて外部のAIサービスプロバイダへ移転・提供される。当該データは、機械学習（強化学習）を通じた照明や空調の制御

[4] “Application Programming Interface”の略で、あるコンピュータプログラム（ソフトウェア）の機能や管理するデータなどを、外部の他のプログラムから呼び出して利用するための手順やデータ形式などを定めた規約を指す。

データの生成（加工・利用）に利用される。

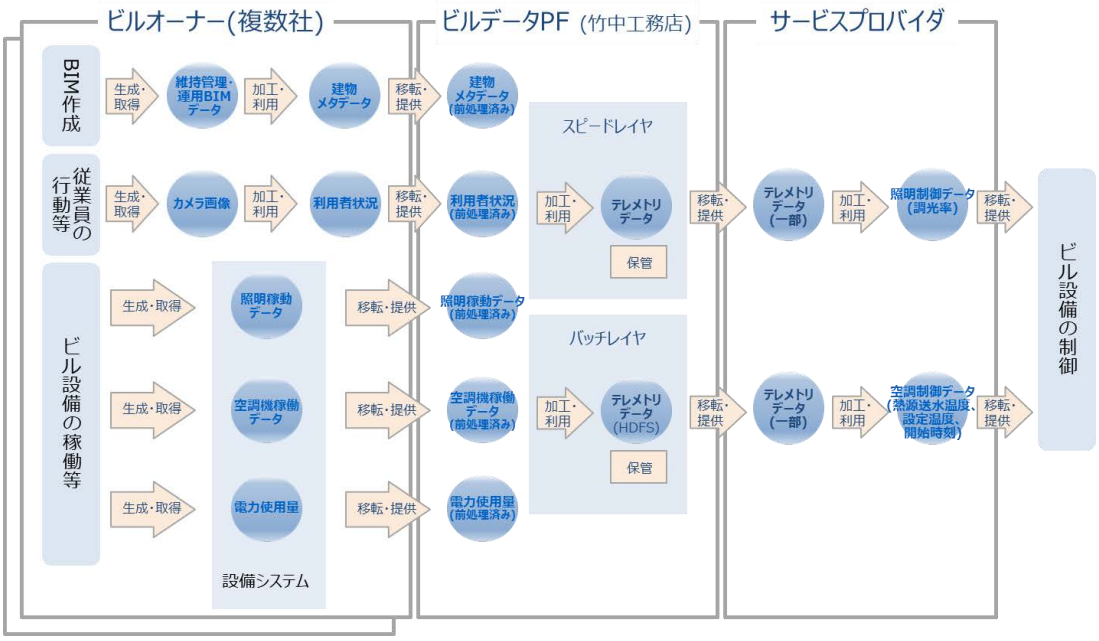

図2.2-2 データ処理フローの可視化

2-2-2. STEP 2 必要な制度的な保護措置（「場」）の整理

STEP 2は、STEP 1で特定された一連のデータ利活用プロセスに対して、「場」としてどのようなデータの保護に係るルール（規範）が課せられ得るかを理解する段階である。本ケースにおいては、取扱うデータの性質や事業者の業種等を考慮すると、例えば下記のルールが「場」として特定され得る。

（1）ビルデータPFサービス利用契約：ビルオーナーとビルデータPFに係るサービスを提供する竹中工務店との間で締結されるものであり、ビルオーナーから受領した各種データの保護や利用権限に関する以下の規定を含み得る。

- 契約による保護の対象となるデータの範囲
- 対象データの利用目的
- 対象データの第三者提供の制限
- 対象データの安全管理（セキュリティ管理）
- 対象データの利用期間、契約終了時の取扱い

（2）AIサービス利用契約：竹中工務店とクラウドサービスとして機械学習エンジン（強化学習）を提供するAIサービスプロバイダとの間で締結されるもの。ここで

は、学習済みモデルのサービス利用契約を想定した。このような契約においては、特にデータの取扱いに関連して、以下を考慮する必要がある[5]。

No.	項目	考慮事項
1	学習済みモデルのカスタマイズ	・ユーザのデータを用いて学習済みモデルをカスタマイズする場合、カスタマイズに用いられた生データ、学習用データセット、カスタマイズされた学習済みモデル、および関連するノウハウの権利帰属や利用条件が問題となり得る。 ・カスタマイズを伴うサービス利用契約においては、これらの権利帰属や利用条件について取り決める必要がある。取決めにあたっての、基本的な考え方や考慮要素は、カスタマイズの程度等、基本的には寄与度およびデータの性質を考慮した上で決定する。
2	入力データ	・サービス利用に伴い、ユーザがベンダのサーバーに送信した入力データについて、ベンダからのアクセスが可能となる。入力データには、ユーザの営業秘密やノウハウが含まれる場合もあるが、このような入力データの法律上の取扱いは必ずしも明確でないことから、入力データの取扱いや利用条件について、サービス利用契約で取り決めることが望ましい。 ・特に争点となり得るのは、ベンダが入力データを、ユーザへのサービス提供以外の目的で利用することを望む場合である。このような場合、主に入力データの収集・蓄積にかかるコストの負担、入力データの機密性、別目的での利用範囲、サービス提供にかかるコストの負担、責任の分担等を考慮の上、ユーザ・ベンダ間で協議して取り決めることになる。 ・利用目的外で利用できる入力データを限定する（たとえば、ユーザが特定できない形に加工したデータに限る等）、別目的での利用範囲を限定する（たとえば、研究開発目的での利用に限定する等）といった条件を設けることにより、ユーザ側の懸念を一定程度解消できる場合もあり得る。

[5] 「AI・データの利用に関する契約ガイドライン - AI 編 -」の「第 5 AI 技術の利用契約」を参照

3	再利用モデル	・学習済みモデルの利用サービスにおいては、当該モデルの精度を維持するため、または精度を高めるために、入力データを用いて追加学習を行うことも想定される。追加学習により、再利用モデルが生成された場合、その取扱いが問題となり得るので、権利帰属や利用条件について、サービス利用契約において取り決めることが望ましい。 ・特に、追加学習で生成された再利用モデルを、ベンダがユーザ以外の第三者へのサービスに利用する場合、基本的には、双方の寄与度や利益のバランスを基準として、第三者へのサービス提供の可否や条件を取り決めることになる。
4	AI 生成物	・学習済みモデルの利用サービスにおいて、ユーザは学習済みモデルを用いて出力された AI 生成物を得ることになるが、当該 AI生成物の取扱いについても、サービス利用契約において取り決めることが望ましい。 ・この場合も、当該 AI 生成物の性質、利用目的、データの提供主体、コストの負担、責任分担等の各要素を考慮の上、具体的な利用条件について取り決めることになる。

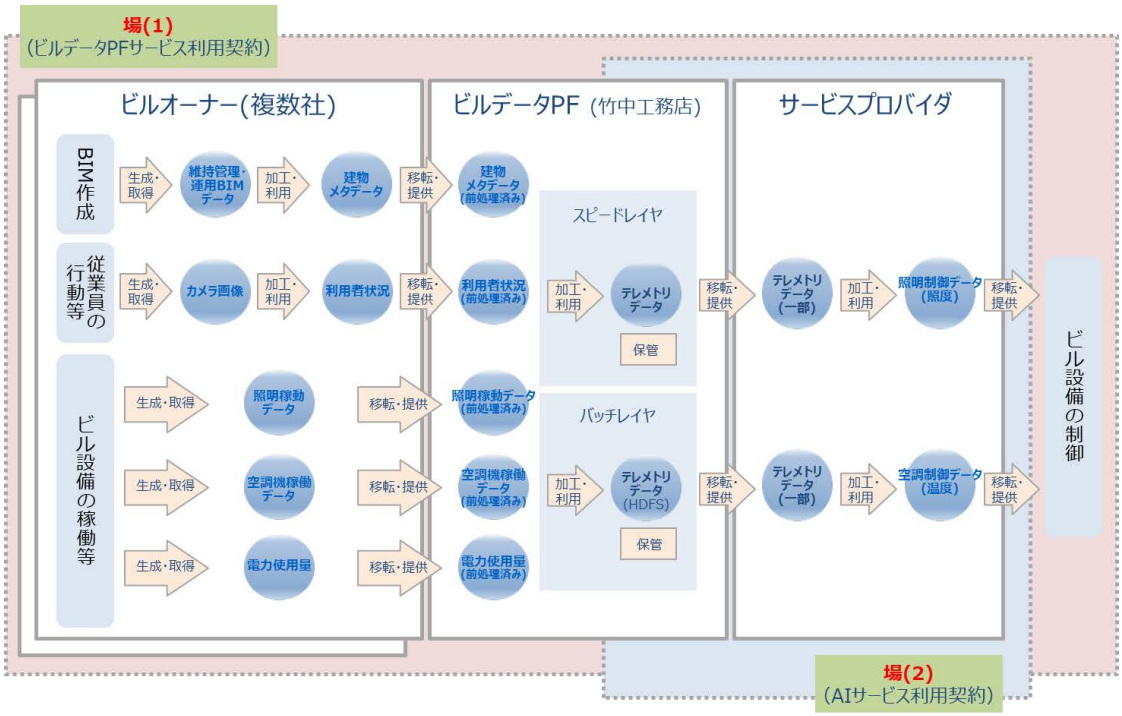

図2.2-3 必要な制度的な保護措置の整理

2-2-3. STEP 3 「属性」の具体化

STEP 3では、STEP 2にて特定されたデータの保護に係るルール（場）の効果的・効率的な遵守に資するデータの「属性」を特定する。

本ケースでは、ビルデータPF上で特定の個人を識別できるデータ、あるいはそれを加工して作成される「匿名加工情報」や「仮名加工情報」等を取扱わないことから、「建物メタデータ」、「利用者状況」、「BAデータ」、「テレメトリデータ」、「制御データ」（「照明制御データ」と「空調制御データ」の双方を含む）には、個人情報保護法による義務は課せられないと考えた。そのため、データの利用権限やその他取扱いに係る属性を特定するにあたっては、2-2-2で示した事業者間の契約の内容に留意することとした。それらを考慮したうえで検討を実施した、本ケースにて取扱うデータの「属性」パラメータ例は以下に示す通りである。

表2.2-1 本ケースにて取扱うデータの「属性」パラメータ例

		建物メタデータ	利用者状況	BA データ	テレメトリデータ	制御データ
カテゴリ	パーソナルデータ保護	-	-	-	-	-
	知的財産・営業秘密保護	ビルデータ PF の営業秘密[*1]	ビルデータ PF の営業秘密[*1]	ビルオーナーの営業秘密	ビルデータ PF の営業秘密[*1]	ビルデータ PF の営業秘密[*2]
	…	-	-	-	-	-
開示範囲		ビルデータ PF、ビルオーナー	ビルデータ PF、ビルオーナー	ビルデータ PF、ビルオーナー	ビルデータ PF、サービスプロバイダ、ビルオーナー	ビルデータ PF、サービスプロバイダ
利用目的		省エネ・快適性の高度化に向けたサービス提供のため				
データ管理主体		ビルデータ PF	ビルデータ PF	ビルデータ PF	ビルデータ PF	サービスプロバイダ

データ権利者	ビルデータ PF、元ビルオーナー	ビルデータ PF、元ビルオーナー	ビルデータ PF、元ビルオーナー	ビルデータ PF、元ビルオーナー	ビルデータ PF、元ビルオーナー
価値（重要度）	高	高	高	非常に高	中
媒体・保存先	ビルデータ PF	ビルデータ PF	ビルデータ PF	ビルデータ PF	サービスプロバイダ管理のサーバー
利用期限	ビルデータ PF サービス利用契約期間中				

2-2-4. STEP 4 「イベント」ごとのリスクポイントの洗い出し

2-2-4-1. 「イベント」ごとのリスクポイントの洗い出し

本STEPでは、これまでの検討を踏まえて、対象のプロセス内でデータ取扱いに関連して想定されるリスクを洗い出し、当該リスクのうち主なものに対して有効と考えられるデータ管理策の検討を実施した。その際、多数のイベントを含むプロセス全体を一度に分析するのは有効ではないと考え、全体のプロセスを、以下に示す4つのイベントに分割して分析を行った。

- 「BAデータ」の生成・取得及び「ビルデータPF」への移転提供
- 「カメラ画像」の生成・取得及び「利用者状況」への加工・利用
- 「テレメトリデータ」への加工・利用
- 「テレメトリデータ」の移転・提供及び「制御データ」への加工・利用

表2.2-2 リスクポイントの洗い出しに際して分析の単位としたイベント群

対象イベント		概要
A	「BA データ」の生成・取得及び「ビルデータ PF」への移転提供	• ビル内に設置した電力量計や空調機、照明器関連の機器から、照明稼動データ、空調機稼働データ、電力使用量を取得し、竹中工務店にて管理するビルデータ PF に送信する。 • ビルオーナー各社と竹中工務店との「ビルデータ PF サービス利用契約」による規律を受ける。

B	「カメラ画像」の生成・取得及び「利用者状況」への加工・利用	• ビルオーナーの管理する建物内に設置したカメラで撮影した画像を特定の個人を識別できない利用者状況（人の位置、エリア内の人数、着衣量）へと加工・利用し、ビルデータ PF に送信する。 • ビルオーナー各社と竹中工務店との「ビルデータ PF サービス利用契約」による規律を受ける。
C	「テレメトリデータ」への加工・利用	• PF 上に共有した「BA データ」及び「利用者状況」に対してビルデータ PF 上で前処理を行い、建物メタデータと紐づけたうえで、「テレメトリデータ」へと加工・利用する。 • ビルオーナー各社と竹中工務店との「ビルデータ PF サービス利用契約」による規律を受ける。
D	「テレメトリデータ」の移転・提供及び「制御データ」への加工・利用	• ビルデータ PF に格納されたテレメトリデータのうち業務の遂行に必要な範囲を抽出したうえで、API を通じて、サービスプロバイダに移転・提供される。当該データを入力として、強化学習の出力が空調制御データ及び照明制御データが二次生成（加工・利用）される。 • 竹中工務店とサービスプロバイダとの「AI サービス利用契約」による規律を受ける。

「BAデータ」の生成・取得及び「ビルデータPF」への移転・提供にあたっては、ビルシステムにて通常想定されるリスク[6]や、各建物からビルデータPFまでのネットワーク上で想定されるリスクが特定された。また、法制度等に係わる観点としては、「BAデータ」には個人に関するデータは含まれないことから、ビルオーナーとPF側の契約に係るデータの不適正な取得がリスクとして特定された。

[6] ビルシステムに対する脅威の動向や具体的な攻撃事例については、別途、「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 第１版」の「2. ビルシステムを巡る状況の変化」を参照されたい。

表2.2-3 「BAデータ」の生成・取得及び「ビルデータPF」への移転・提供にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	照明稼動データ、空調機稼働データ、電力使用量からなる「BA データ」が、ビル設備機器からビルデータ PF までのネットワーク上で内部犯行者又は外部の攻撃者に傍受され、漏えいする。
		マルウェア感染	「BA データ」がマルウェアに感染したビル設備機器等から不正な送信先へ共有される。
	完全性	なりすまし	ビル設備機器等を不正な機器によりなりすまされ、ビルデータ PF において正確でない「BA データ」が生成・取得される。
		改ざん	「BA データ」が、ビル設備機器からビルデータ PF までのネットワーク上で内部犯行者又は外部の攻撃者に傍受され、改ざんされる。
	可用性	サービス不能	ビル設備機器がマルウェア（ランサムウェア等を含む）に感染して稼働停止し、「BA データ」を生成・取得できない。
		システムの不具合	「BA データ」の生成・取得に係るビル設備機器に故障等の不具合が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	-	該当なし
	知的財産・営業秘密保護	適法な手段によるデータ取得	悪意のある従業員又は退職者を含む第三者が、「BA データ」に含まれる秘密情報を不正な方法(窃取、詐欺、強迫、その他の不正な手段)で取得している。
		許諾等のない第三者提供	ビルオーナーが、適切な守秘義務等を含む契約の締結等なしに、「BA データ」を竹中工務店に提供する。

「BAデータ」とは別途取得される「カメラ画像」の生成・取得及び「利用者状況」への加工・利用においては、ネットワークカメラシステムにおいて一般的に想定される脅威[7]が想定されることに加え、一定の加工が加えられる以前の「カメラ画像」には特定の個人を識別可能な情報が含まれることから、ビルデータPFの送信前に一定の処理を行う場合であっても、プライバシーに係る観点でリスクの特定が必要であるという整理がなされた[8]。

表2.2-4 「カメラ画像」の生成・取得及び「利用者状況」への加工・利用にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	カメラから生成される「カメラ画像」または「利用者状況」が、カメラからレコーダ、ビルデータ PF までのネットワーク上で内部犯行者又は外部の攻撃者に傍受され、漏えいする。
		マルウェア感染	「カメラ画像」または「利用者状況」が、不正アクセスされたカメラまたはレコーダ等から不正な送信先へ共有される。
	完全性	なりすまし	データ取得用途のカメラまたはレコーダ等を不正な機器によりなりすまされ、ビルデータ PF において正確でない「利用者状況」が生成・取得される。
		改ざん	カメラから生成される「カメラ画像」または「利用者状況」が、カメラからレコーダ、ビルデータ PF までのネットワーク上で内部犯行者又は外部の攻撃者に傍受され、改ざんされる。
	可用性	サービス不能	カメラまたはレコーダがマルウェアに感染して稼働停止し、「カメラ画像」または「利用者状況」を生成・取得できない。
		システムの不具合	「カメラ画像」または「利用者状況」の生成・取得に係るカメラまたはレコーダに故障等の不具合が生じ、処理が一時的に停止する。

[7] ネットワークカメラシステムにおいて想定されるセキュリティ脅威については、「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」の「5.1. 想定する脅威について」を参照されたい。

[8] かかる観点から想定されるリスクやその他の懸念事項、講ずるべき対策に関しては、別途、「カメラ画像利活用ガイドブック ver3.0」等を参照されたい。

法制度等に係る観点	パーソナルデータ保護	適法な手段によるデータ取得	「カメラ画像」及び「利用者状況」を取得するビルオーナーが、データの利用目的等の必要事項をデータ元の個人に対して明確に示していない、又は利用の実態と対応した形で提示していない。
			「カメラ画像」及び「利用者状況」を取得するビルオーナーが、偽り等の不正の手段により個人情報を取得している。
		許諾等のない第三者提供	ビルオーナーが、事前の本人同意取得又はオプトアウトに係る手続（委託、共同利用等を含む）等の実施なしに、「カメラ画像」を竹中工務店の管理するビル管理 PF に移転・提供する。
	知的財産・営業秘密保護	適法な手段によるデータ取得	悪意のある従業員又は退職者を含む第三者が、「カメラ画像」または「利用者状況」等の秘密情報を不正な方法（窃取、詐欺、強迫、その他の不正な手段）で取得している。

ビルデータPF上で実施される「テレメトリデータ」への加工・利用においては、セキュリティに係る観点としては、なりすましによる不正アクセスやサービス不能（DoS）攻撃、システムの不具合によるサービス停止等のクラウドサービス基盤上で一般的に想定されるリスクが特定されると考えた。法制度等に関連して、契約遵守の観点から合意された内容とは異なる利用条件（利用目的、利用権限等）とは異なる方法、またはその他の不適切な方法によるデータ利用がリスクとして特定された。

表2.2-5 「テレメトリデータ」への加工・利用にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	加工・利用過程において、権限のない内外の主体（システム運用・保守会社、別のビルオーナー等を含む）により対象となるデータの全部又は一部が不正アクセスされ、自社又は他社の機密データが特定され、漏えいする。
		情報漏えい	「テレメトリデータ」の加工基準やアクセス管理に不備があり、参照権限のあるサービス利用企業により、本来特定されるべきでない当該ビルオーナー以外の機密データが特定される。

	完全性	改ざん	悪意のある内外の主体によりビルデータ PF 上のデータ処理アプリケーションの設定等が改ざんされ、データの処理にあたって不正な処理が行われる。
		改ざん	悪意のある内外の主体により意図的に加工・利用の結果として生じる「テレメトリデータ」の全体又は一部が改ざん又は削除される。
		システムの不具合	クラウドサービス事業者が提供するビルデータ PF を構成する設備や機器の一部に、故障等による障害や誤動作が発生し、集約結果の完全性が損なわれる。
	可用性	サービス不能	サービス妨害攻撃、マルウェア感染等により、クラウドサービス事業者が提供するビルデータ PF を構成する設備や機器が一時的に停止する。
		システムの不具合	過度の処理リクエスト等により、クラウドサービス事業者が提供するビルデータ PF を構成する設備や機器に不具合が生じ、処理が一時的に停止する。
		自然災害等	地震や津波等の自然災害により、クラウドサービス事業者が提供するビルデータ PF を構成する設備や機器に被害が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	-	該当なし
	知的財産・営業秘密保護	提供先での目的外利用	必要な手続きを踏むことなく、「テレメトリデータ」が、「ビルデータ PF サービス利用契約」においてビルオーナーと合意した利用条件（利用目的、利用権限等）とは異なる方法で利用される。
			正当な手段によりデータを取得した悪意のある内外の主体（退職者を含む）により、不正の利益を得る目的又は権利元に損害を加える目的で「テレメトリデータ」が使用される。
		提供先に起因するデータアクセスの制限	ビルオーナーによる「テレメトリデータ」に対するアクセスやそれを活用したサービスの利用機会が制限されている。

最後に、AIサービスプロバイダへの「テレメトリデータ」の移転・提供及び「制御データ」への加工・利用においては、データの移転・提供に用いられるインターフェース（API）やネットワーク、移転先のAIサービスプロバイダにて想定されるセキュリティ脅威が考慮された。また、データがAIサービスプロバイダに渡る場合であっても、データの取得元であるビルオーナーから許可された利用目的等との整合を図ることが重要であるという観点から、法制度等に関連したリスクを特定した。

表2.2-6 「テレメトリデータ」の移転・提供及び「制御データ」への加工・利用にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	ビルデータ PF からサービスプロバイダのシステム環境までのネットワーク上で、「テレメトリデータ」を含むデータが悪意のある第三者に傍受され、漏えいする。
		なりすまし、情報漏えい	正規の利用者になりすまされる、または脆弱性を悪用され、ビルデータ PF に不正アクセスされ、「テレメトリデータ」が車両データ活用基盤から不正な送信先へ移転される。
	完全性	改ざん	悪意のある内外の主体によりビルデータ PF 上のデータ処理アプリケーションの設定等が改ざんされ、データの処理にあたって不正な処理が行われる。
		改ざん	悪意のある内外の主体により意図的に加工・利用の結果として生じる「テレメトリデータ」の全体又は一部が改ざん又は削除される。
		なりすまし、改ざん	ビルデータ PF からサービスプロバイダのシステム環境までのネットワーク上で、「テレメトリデータ」を含むデータが悪意のある第三者に傍受され、改ざんされる。
	可用性	サービス不能	サービス妨害攻撃等によりデータの移転・提供に係る設備や機器が一時的に停止する。
		システムの不具合	データの移転・提供に係る設備や機器に不具合が生じ、処理が一時的に停止する。
		自然災害等	地震や津波等の自然災害によりデータの移転・提供に係る設備や機器に被害が生じ、処理が一時的に停止する。

法制度等に係る観点	パーソナルデータ保護	-	該当なし
	知的財産・営業秘密保護	提供先での目的外利用	「テレメトリデータ」及び「制御データ」等派生データのサービスプロバイダによる利用権限が「AI サービス利用契約」において十分に定められておらず、利用目的や第三者提供の可否等についてビルオーナーからクレーム等が生じる。
			正当な手段によりデータを取得した悪意のある内外の主体（退職者を含む）により、不正の利益を得る目的又は権利元に損害を加える目的で「テレメトリデータ」または「制御データ」が取得、利用される。

2-2-4-2. 今後のデータ管理の高度化に向けた課題の検討

前節で特定されたリスクを適切に低減、管理し、データ管理の高度化を実現するために実施され得る対策としては、例えば以下が含まれる。

- ビルオーナー向け：セキュリティを確保したBAシステム、ネットワークカメラシステムの利用
  - ✓ 「BAデータ」の生成・取得及び「ビルデータPF」への移転・提供におけるリスクを軽減し、データの生成・取得段階における信頼性を確保するため、関係するガイドラインやチェックリスト等を参照しつつ、BAシステム、ネットワークカメラシステムへ基礎的なセキュリティ対策を実装する。その際、対策として考慮すべきものには以下が含まれ得る[9]。
    - ー 動作するサービスの最小化（不要なサービスの停止）
    - ー 接続元の IP アドレス等による制限
    - ー 十分な強度による利用者・管理者の識別・認証
    - ー 発覚した脆弱性の評価及び対処
    - ー 連続したログイン失敗、管理者に覚えのない認証成功等の検知、確認

[9] より詳細な記載については、「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 第１版」や「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」等を参照されたい。

- ビル外部との通信の暗号化（HTTPS等）　※適切な場合はビル内部も含む

- ビルオーナー・竹中工務店向け：「テレメトリデータ」の適切な取扱い
  - ✓ ビルオーナーから受領したデータ等を利用して貴社にて作成した「テレメトリデータ」を、「ビルデータPFサービス利用契約」の規定（例：利用目的、第三者提供の可否、加工等の可否、安全管理、契約終了時の取扱い）に適合するよう取扱う[10]。
  - ✓ 各社から収集したデータを、顧客ビルの省エネ・快適性向上以外の用途（自社の新サービス開発等）で用いる場合、以下の事項に留意すべき。
    - 契約に上記の用途が明確に特定できる記載を設ける。既存の契約でそれらの用途が含まれていない場合には、ビルオーナーとの間で利用目的変更等の手続きを行う。
    - あるビルオーナーから得た秘密情報は、他社の秘密情報と分離して管理する。（他社への不正開示等で訴えられたときに当該事業者の秘密情報が開示範囲に含まれないことを立証することが困難となるため）
    - ビルオーナーごとに個別管理しているデータベース内のデータを統合する場合、元のビルオーナーを特定しないように抽象化を行ったうえで、当該処理の実施が契約で許容されている利用目的の範囲に含まれるかを確認する。

- 竹中工務店・AIサービスプロバイダ向け：「テレメトリデータ」及び「制御データ」の適切な取扱い
  - ✓ アプリケーションとしてクラウドサービス型の強化学習エンジンを利用する場合、ビルデータPFからサービスプロバイダのサーバーに送信した入力データ（テレメトリデータ）について、サービスプロバイダからのアクセスが可能となる。入力データ及び学習済みモデルを用いて出力されたAI生成物（派生データ）には、ユーザの営業秘密やノウハウが含まれる場合もあるため、データの取扱いや利用条件について、「ビルデータPFサービス利用契約」の

[10] 具体的な契約の規定内容については、「AI・データの利用に関する契約ガイドライン 1.1 版 - データ編 -」等を参照されたい。

規定との整合性も考慮しつつ、「AIサービス利用契約」で取り決める。

- AIサービスプロバイダがテレメトリデータを、制御データ生成以外の目的で利用することを望む場合、テレメトリデータの収集・蓄積にかかるコストの負担、データの機密性、別目的での利用範囲、サービス提供にかかるコストの負担、責任の分担等を考慮の上、協議して取り決める。ここでは、「ビルデータPFサービス利用契約」の規定に準じて、顧客ビルの省エネ・快適性向上（に必要な制御データの生成）に利用目的を限定することとした。
- 強化学習モデルを用いて出力された制御データ等（派生データ）の取扱いについても、AIサービス利用契約において、利用目的、第三者提供の可否、加工等の可否、安全管理、契約終了時の取扱い等を取り決める。

2-3. 製造装置の稼働データ等を活用した予防保全・製品向上

ドイツの“インダストリー4.0”、フランスの“未来の産業”、中国の“中国製造2025”など、世界の主要各国が、第四次産業革命への対応を進めている中、日本もまた、2017年より我が国の産業が目指すべき姿として“Connected Industries”（データを介して、機械、技術、人など様々なものがつながることで、新たな付加価値創出と社会課題の解決を目指す産業の在り方）を掲げ、IoTやAIを始めとする最新のデジタル技術の活用を含む各種施策を推進している。

IoTを始めとする最新のデジタル技術を用いて、事業者は、製造工程を構成する研究開発－製品設計－工程設計―生産などの連鎖である「エンジニアリングチェーン」と、受発注－生産管理－生産－流通・販売－アフターサービスなどの連鎖である「サプライチェーン」の双方にて、「R&D支援」、「設計支援」、「販売予測」、「遠隔保守」等のデータの利活用を進める優れたソリューションを可能にすることができる。また、さらに重要なこととして、生産工程から得られる膨大なデータや、何百万台もの機械、プラント、製品から得られる運用データを製品設計と工程設計の双方に活用し、エンジニアリングチェーンとサプライチェーンをシームレスにつなぐことで、新たな付加価値創出を実現することが提案されている[11]。

本節では、かかるエンジニアリングチェーンとサプライチェーンの連携の一例として、以下に概要を示す仮想的なユースケース「製造装置の稼働データ等を活用した予防保全・製品向上」（以下、「本ユースケース」という。）に、フレームワークを適用する。

- A社は、日本に拠点を有し製造装置等を製造・販売する事業者であり、フランス（EU構成国の一例）に所在する多数のユーザ事業者の工場に現地のシステムインテグレータ経由で装置を納め、装置等の運用開始後も振動、温度、動きの情報等の運用データを収集、自社のデータ分析基盤にて異常トレンドの分析等を実施する。
- A社は、自社の製造装置の故障や異常を検知した場合、あるいは定期的に、現地の保守会社（B社）や故障や異常が検知された部品のサプライヤ（かかる事業者は多数想定されるが、簡便化のため単に「C社」とする）に対して、必要かつ適

[11] 2020 年版ものづくり白書（ものづくり基盤技術振興基本法第 8 条に基づく年次報告）66 頁

切な範囲で異常の通知や稼働情報の提供を行う。

- 上記の保守目的でのデータ利用に加えて、A社は、異常トレンドを示した機器の製造番号やその動作履歴を日本に拠点を有する自社設計部門へと提供し、製品設計の改善等を目的として利用している。

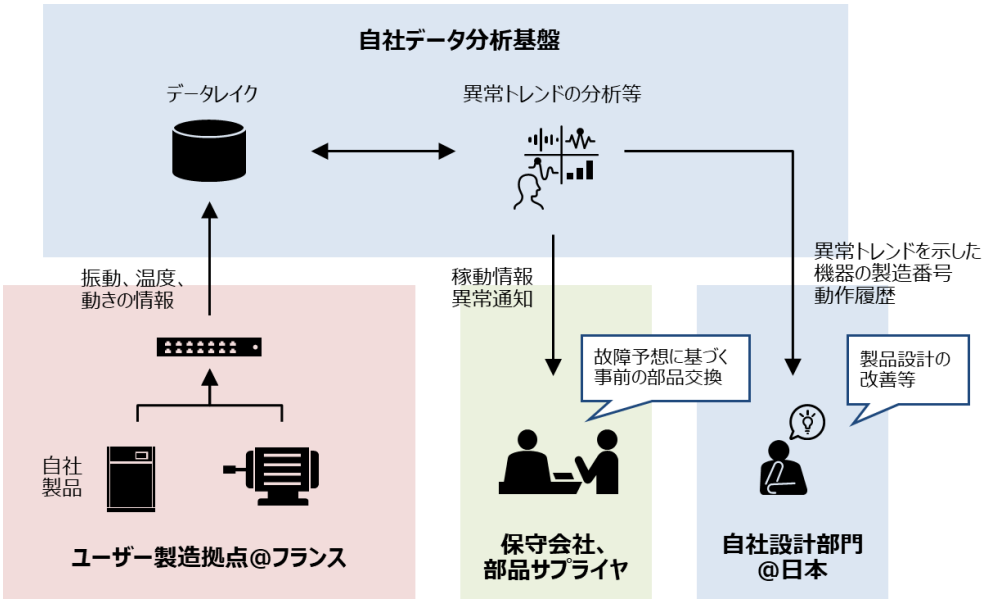

図2.3-1 製造装置の稼働データ等を活用した予防保全・製品向上の概要

三菱電機株式会社では、事務局（委託先：日立製作所）と共同で、上記の仮想的なユースケースに対してフレームワークを適用し、複数事業者間・複数国間に渡るデータの利活用プロセスにおいて想定されるリスク及び有効な管理策を中心に検討を実施した。本件適用を通じて社内等でもデータの取扱いについてより意識を高めていくことを想定している。

その際、本ユースケースにおいて考慮したステークホルダーとして以下が挙げられる。

- ユーザ事業者：フランスに製造拠点を有する事業者で、A社が製造・販売する製造装置の納入及び関連サービス（装置の保守、維持管理等）の提供を受けている。
- A社：日本に本社を有する事業者で、従来から製造業のユーザ事業者向けに装置を製造し、代理店等を通じて海外所在のユーザ事業者に販売している。近年、IoT等を活用した保守事業の付加価値向上を目指し、運用データの収集及びデータ分析基盤の構築・運用を実施している。
- B社：フランスに拠点を有する事業者であり、A社からの委託を受けてユーザ事業

者向けに製造装置の保守業務を担う。

- C社：製造装置を構成するハードウェアまたはソフトウェアからなる部品をA社に提供している事業者であり、装置の運用段階においては、A社からの異常通知やメンテナンス依頼等を受けて、交換用の部品や修正プログラム等を提供する。

2-3-1. STEP 1 データ処理フロー（「イベント」）の可視化

本ユースケースでは図3-2で示すように、以下のプロセスにより構成される[12]。図2.3-2には、A社分析基盤を構成する機器・設備が日本に所在するケースを記載している。

- フランスに所在する製造拠点にて稼働する製造装置からメンテナンスの指標となる変数の値を定期的に測定し、計測時刻とともに「計測値」として「生成・取得」する。データ出力機能のない装置の場合は作業員が別途計測・記録する。それらのデータは、製造拠点内の製造装置側PCに一旦格納された後、定期的にデータ分析基盤へ「移転・提供」される。
- A社分析基盤において、製造装置から収集される各種データが予防保全・製品向上に必要な形へと「加工・利用」される。具体的には、工作機械の各メンテナンス項目に関して、次回保全時刻（余寿命）を計算し、「余寿命」の大小から算出される「保全優先度」を全ての製造機器、全てのメンテナンス項目に関して一覧として可視化する。

[12] 本ユースケースの作成にあたっては、ロボット革命・産業 IoT イニシアティブ協議会（RRI） IoT による製造ビジネス変革ＷＧ 産業機械サブ幹事会 「ケース：工作機械の多様性を考慮した状態監視・可視化システムの協調設計と実証」等を参照した。

- 算出された「保全優先度」や製品の製造番号ごとに期間中の動作状況、異常動作、その他の不具合の有無等に係る「稼動レポート」を、製品工場のためA社設計部門、タイムリーな保守業務の実施のため、B社（保守会社）及びC社（部品サプライヤ）等に適切な範囲で「移転・提供」する。

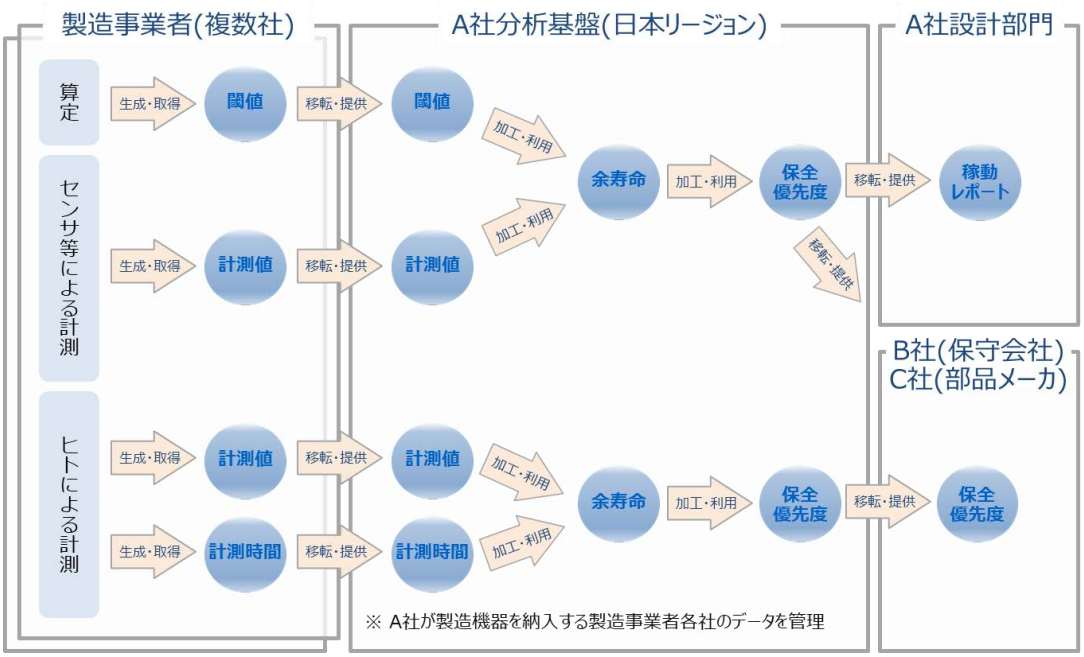

図2.3-2 データ処理フローの可視化

通常、センサーやヒトによる計測内容または計測実施者等の記録には個人情報等が含まれる可能性があるが、今回取扱うデータには、一般データ保護規則（GDPR）や個人情報保護法の対象となる個人データ（個人情報）または輸出管理の対象となる技術情報は含まれないものと仮定する。

図3-2では、A社分析基盤が分析等の拠点のある日本に所在する場合を示しているが、各国・地域における立法の状況やA社のリソースに合わせて地域ごとに構築されたクラウドに集約する等、市場環境を踏まえた柔軟な対応を行うことも想定される。

2-3-2. STEP 2 必要な制度的な保護措置（「場」）の整理

上述したように、STEP 1で特定したデータフローには、個人情報保護法制や輸出管理法制、その他のデータローカライゼーション（データの国内保存義務等）を伴う制度の対象となるデータが現状含まれないと想定されることから、事業者間の契約による保護が制度的な措置の中心となる。取扱うデータの性質や事業者の業種等を考慮し、下記

のルールを「場」として特定した。

（1） 製造事業者 – A社サービス利用契約（または規約）：A社とユーザである製造事業者との間で締結される予防保全に係るサービス契約であり、装置から生成されるデータの取扱いに係る条項を含みうる。製造事業者は多数に渡ることも想定されるため、利用規約や約款による場合もあり得る。契約では、データの利用条件として、以下を当事者間で合意することが想定される[13]。

表2.3-1 当事者間で合意しておくべきデータの利用条件等

項目	定めるべき事項
対象データの範囲	• 取引に関連して創出されるデータ（対象データ）の一覧表を作成する等して、対象データの範囲の明確化を図ること。 • 前記の一覧表から漏れたデータ等、明確に利用権限が合意されなかったデータについて、当該データの利用権限の定め方を規定しておくこと。 • 必要に応じて、営業秘密やノウハウを除去または希薄化できる程度にデータの粒度を粗くし、取得するデータの範囲・内容を限定すること。
利用目的	• 利用目的を定めることにより、対象データの利用権限の範囲を明確にすること（たとえば、特定の事業領域での利用に限定する、当事者において既に決まっている研究開発契約での利用に限定する等）。
加工等の可否と派生データに対する利用権限	• 対象となるデータの加工等の可否およびその方法を定めること。 • 加工等により創出される派生データに対する利用権限について定めること。
データ内容および継続的創出の保証／非保証	• データの内容の正確性等について保証することまたは保証しないことについて合意をすること。 • データに個人情報が含まれる場合には、個人情報保護法を遵守し必要とされる手続が履践されていることを保証すること（利用目的、第三者提供の同意（または、業務委託・共同利用）の内容、確認記録義務の内容等）。 • データが継続的に創出され、データの量が確保されることについて、保証をすることまたはしないことについて合意をすること。
第三者提供の制限	• 第三者に対するデータの提供の可否。 • 第三者へのデータの提供ができる場合、第三者に課される条

[13] 経済産業省「AI・データの利用に関する契約ガイドライン 1.1 版」 55 頁 を参照

	件。
収益および費用の分配	• 対象データを第三者提供すること等により収益を得る場合、収益および費用の分配を定めること。
管理方法・セキュリティ	• データの性質やリスクに即して、具体的なデータの保存先や管理方法等を定めること。
利用期間	• 利用できる期間を定めること。
利用地域	• データを利用できる国・地域を定めること。
契約終了時のデータの取扱い	• 利用期間が終了した後に、派生データを含めて、削除または返還を要するかを規定すること。
準拠法・裁判管轄	• 契約に適用される法律および裁判管轄を合意すること。

（2） A社 – B社/C社データ利用契約：（1）の規定も参照しつつ、A社が収集・分析したデータを参照して保守関連業務を実施するB社及びC社とも締結する契約中にデータの取扱いに係る条項を設ける。

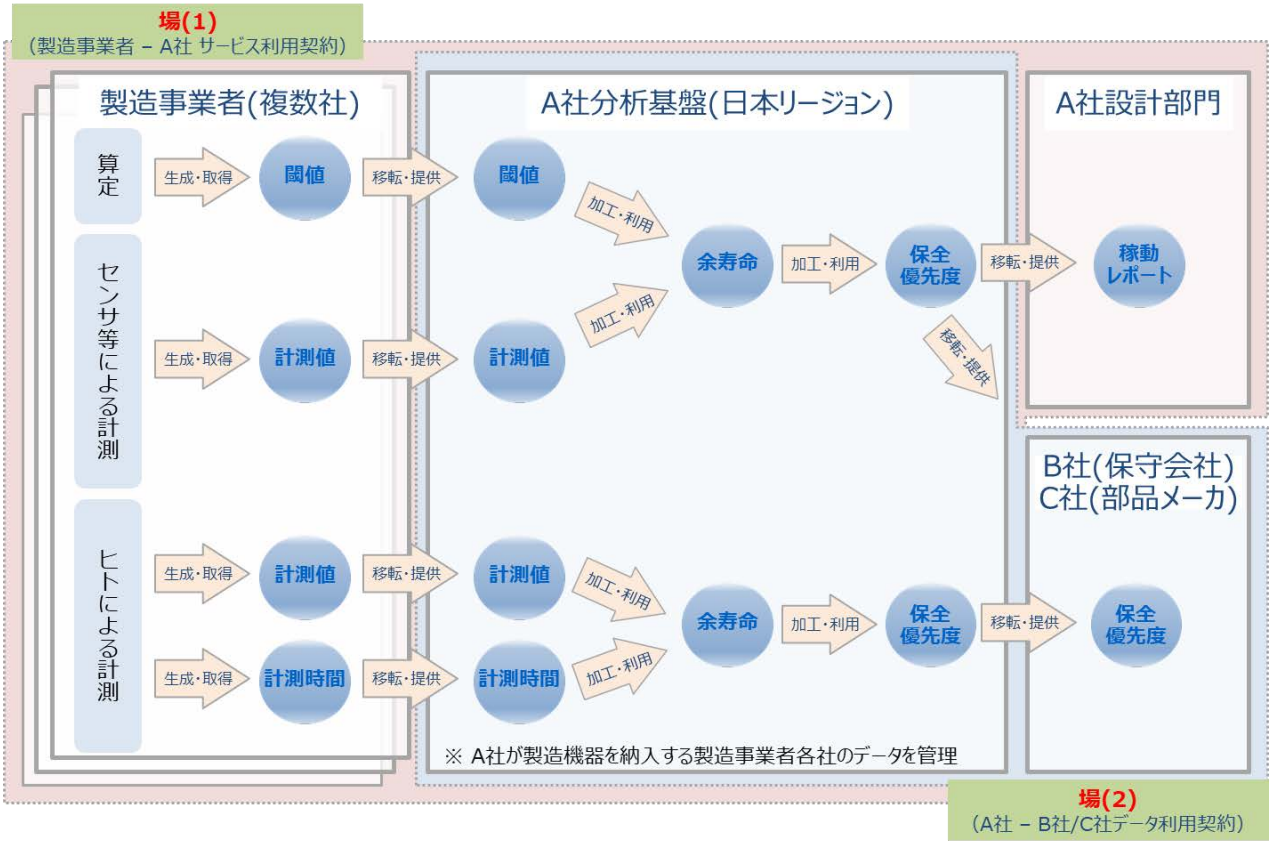

図2.3-3 必要な制度的な保護措置の整理（稼働データ等を活用した予防保全・製品向上）

本ケースにおける取扱いデータに関しては、欧州から日本拠点へのデータ送信を規制

する現行の制度が管見の限り確認されなかった[14]ため、分析基盤を欧州に構築するか、日本に構築するかの判断はA社の事業的な判断によるものと想定した。一方で、非個人データを対象とするものも含め、将来的に一定の安全管理や越境移転に係る規定を設けるルール形成を国内外の政府機関等が実施することも想定されることから、事業者においては国内外の関連動向を注視し、規則の変更等が生じた際には必要な対応を柔軟に実施することが求められる。

2-3-3. STEP 3 「属性」の具体化

前述したように、本ユースケースには、個人情報保護法制や輸出管理法制等の対象となるデータが必ずしも含まれていないことから、各「属性」項目のパラメータを設定するにあたり考慮することが望ましいルールは非個人データ（産業データ）を対象とし得る不正競争防止法の営業秘密、限定提供データ関連規定や事業者間で締結される契約が中心となる。かかる契約では、対象とするデータの範囲、利用目的、加工等の可否と派生データに対する利用権限等を取り決めることが望ましいとされているが、本STEPでは契約条項の内容について一定の仮定を置いたうえでデータがとり得るパラメータの例を以下のように検討した。

表2.3-2 本ユースケースにて取扱うデータの「属性」パラメータ例

		計測値	閾値	余寿命	保全優先度	稼動レポート
カテゴリ	パーソナルデータ保護	該当なし	該当なし	該当なし	該当なし	該当なし
	知的財産・営業秘密保護	製造事業者の営業秘密	製造事業者の営業秘密	A 社の営業秘密	A 社の営業秘密	A 社の営業秘密
	…	…	…	…	…	…

[14] 確認に際しては、「各国のデータガバナンスにおけるデータ越境流通に関連する制度調査 経過報告」（https://www.meti.go.jp/shingikai/mono_info_service/data_ekkyo_iten/pdf/006_04_00.pdf ）等を参照した。

開示範囲	製造事業者、A 社	製造事業者、A 社	製造事業者、A 社、B 社	製造事業者、A 社、B 社	A 社
利用目的	• A 社またはその関連会社による A 社製品の効率的な保守業務の実施 • A 社による製品の開発及び改善				
データ管理主体	製造事業者、A 社	製造事業者、A 社	A 社	A 社	A 社
データ権利者	製造事業者	製造事業者	製造事業者	製造事業者	製造事業者、A 社
価値（重要度）	中	高	高	高	高
媒体・保存先	製造機器側 PC、A 社分析基盤	製造機器側 PC、A 社分析基盤	A 社分析基盤	A 社分析基盤	A 社分析基盤
利用期限	製造事業者 – A 社 サービス利用契約に定める契約期間の終了時				

2-3-4. STEP 4 「イベント」ごとのリスクポイントの洗い出し

2-3-4-1. 「イベント」ごとのリスクポイントの洗い出し

本STEPでは、これまでに理解したデータ利活用プロセスにおいて、セキュリティ及び関連する法制度等の観点からいかなるリスクが想定されるかを特定する。分析の実施にあたり、データ利活用プロセスを以下の 4 つに分けてリスク特定を実施する。

表2.3-3 リスク特定の対象とするイベントの分類

対象イベント		概要
A	計測値等の「生成・取得」及び分析基盤への「移転・提供」	• 製造事業者の拠点（フランス）で稼動する A 社製造機器から振動、温度、動き等の「計測値」を一定間隔で取得し、別途算出する各機器・部品メンテナンス用の「閾値」とともに拠点内の製造機器側 PC 及び A 社分析基盤に送信する。 • 製造事業者各社と A 社との「製造事業者–A 社 サービス利用契約」による規律を受ける。

B	各種データから「余寿命」、「保全優先度」への「加工・利用」	• A 社データ分析基盤にて、各製造事業者から取得した計測値等のデータから各機器・部品の「余寿命」及びそこから算出される「保全優先度」へとデータを加工・利用する。 • 製造事業者各社と A 社との「製造事業者–A 社 サービス利用契約」による規律を受ける。
C	「稼動レポート」への「加工・利用」及び A 社設計部門への「移転・提供」	• 製造各社から取得した「計測値」や「余寿命」等のデータを踏まえ、機器やそれを構成する部品ごとに稼働状況をまとめた「稼動レポート」を作成し、A 社内設計部門にて今後の製品開発における設計改善等に利用する。 • 製造事業者各社と A 社との「製造事業者–A 社 サービス利用契約」による規律を受ける。
D	「保全優先度」の B 社(保守会社)、部品サプライヤ等への「移転・提供」	• 算出した「保全優先度」に基づいて部品交換やその他の修理作業を実施するため、当該データを B 社（現地の保守会社）や部品メーカーに提供する。 • 製造事業者各社と A 社との「製造事業者–A 社 サービス利用契約」及び、A 社と B 社との「A 社–B 社/C 社データ利用契約」による規律を受ける。

イベントA（計測値等の「生成・取得」及び分析基盤への「移転・提供」）では、製造拠点側の端末である製造装置や製造装置側PC、製造拠点からA社データ分析基盤までのネットワーク、そこで扱われる「計測値」等が、機密性・完全性・可用性の観点からセキュリティ観点の分析対象となり得る。

また、法制度等の観点からは、「製造事業者–A社 サービス利用契約」の規定に関連して、不正な方法によるデータの取得、適切な契約や守秘義務等のないA社へのデータ移転がリスクとして特定され得る。

表2.3-4 計測値等の「生成・取得」及び分析基盤への「移転・提供」にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	製造装置または製造装置側 PC が不正アクセスされ、「計測値」または「閾値」が、不正な送信先へ共有される。

		マルウェア感染	「計測値」または「閾値」が、製造拠点から A 社分析基盤までのネットワーク上で内部犯行者又は外部の攻撃者に傍受され、漏えいする。
	完全性	なりすまし	送信元の製造機器または製造機器側 PC を不正な機器によりなりすまされ、A 社分析基盤に正確でない「計測値」または「閾値」が蓄積される。
		改ざん	「計測値」または「閾値」が、製造拠点から A 社分析基盤までのネットワーク上で内部犯行者又は外部の攻撃者に傍受され、改ざんされる。
	可用性	サービス不能	製造機器または製造機器側 PC がマルウェア（ランサムウェア等を含む）に感染して稼働停止し、「計測値」または「閾値」を生成・取得できない。
		システムの不具合	「計測値」または「閾値」の生成・取得に係る製造機器または製造機器側 PC に故障等の不具合が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	-	該当なし
	知的財産・営業秘密保護	適法な手段によるデータ取得	製造機器または製造機器側 PC から、悪意のある従業員又は退職者を含む第三者が、「計測値」または「閾値」に含まれる秘密情報を不正な方法（窃取、詐欺、強迫、その他の不正な手段）で取得している。
		許諾等のない第三者提供	製造事業者が、適切な守秘義務等を含む契約の締結等なしに、「計測値」または「閾値」を A 社に提供する。

イベントB：各種データから「余寿命」、「保全優先度」への「加工・利用」においては、A社データ分析基盤を構成する機器・ソフトウェア及び、同基盤上でのデータ処理に対する脅威（なりすまし、改ざん、不正アクセス等）が基盤上で取扱うデータの漏えいや改ざん、システムの停止等を生じさせ得る。

一方で、法制度等に関しては、契約遵守の観点から、製造事業者から提供を受けたデータの目的外利用や利用終了後の不適切なデータ保管・利用等がリスクになると考え

た。

表2.3-5 各種データから「余寿命」、「保全優先度」への「加工・利用」にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	データ分析基盤で取扱われる「余寿命」、「保全優先度」等のデータに対して、権限のない内外の主体が不正アクセスし、自社又は他社の機密データが特定され、漏えいする。
		情報漏えい	「余寿命」、「保全優先度」へのアクセス管理に不備があり、保守会社または部品サプライヤにより、本来特定されるべきでない機密データ（例：他社製部品に関するデータ）が特定される。
	完全性	改ざん	分析基盤上のデータ処理アプリケーションの設定等が悪意のある主体により改ざんされ、データの処理にあたって不正な処理が行われる。
		改ざん	悪意のある内外の主体により「余寿命」、「保全優先度」の全体又は一部が改ざん又は削除される。
	可用性 可用性	システムの不具合	データ分析基盤を構成する設備や機器の一部に、故障等による障害や誤動作が発生し、集約結果の完全性が損なわれる。
		サービス不能	サービス妨害攻撃、マルウェア感染等により、データ分析基盤を構成する設備や機器が一時的に停止する。
		システムの不具合	過度の処理リクエスト等により、データ分析基盤を構成する設備や機器に不具合が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	-	該当なし
	知的財産・営業秘密保護	提供先での目的外利用	「計測値」、「余寿命」または「保全優先度」が、「製造事業者–A 社 サービス利用契約」において製造事業者と合意したものとは異なる目的で利用される。（例：製造機器の保守のみが利用目的の場合に、各社データの統合を行うこと）

		提供先に起因するデータアクセスの制限	悪意のある内外の主体（退職者を含む）により、不正の利益を得る目的又は権利元に損害を加える目的で「計測値」、「余寿命」または「保全優先度」が使用される。
		利用期間外のデータ利用	契約で定められた期間を越えて、A 社が分析基盤上で「計測値」、「余寿命」または「保全優先度」にアクセスしたり、それを活用したりする。

イベントC：「稼動レポート」への「加工・利用」及びA社設計部門への「移転・提供」においては、データ分析基盤とA社設計部門が利用するシステムとの間の通信やネットワーク等が分析の対象となる。法制度等に係る観点としては、イベントBと同様に利用目的の整合（目的外利用の該非）や利用期間外のデータ保管・利用等がリスクとなり得る。また、データ分析基盤を外国に構築する場合はA社設計部門へのデータ提供が越境移転に該当し得ることから、今後かかる観点からも潜在的にリスクが生じる可能性がある。

表2.3-6 「稼動レポート」への「加工・利用」及び設計部門への「移転・提供」にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、情報漏えい	正規の利用者になりすまされる、または脆弱性を悪用され、データ分析基盤または A 社設計部門の環境に不正アクセスされ、「稼動レポート」が車両データ活用基盤から不正な送信先へ移転される。
	完全性	改ざん	悪意のある内外の主体によりデータ分析基盤上のデータ処理アプリケーションの設定等が改ざんされ、データの処理にあたって不正な処理が行われる。
		改ざん	悪意のある内外の主体により意図的に、データ分析基盤または A 社設計部門の環境で取扱われる「稼動レポート」の全体又は一部が改ざん又は削除される。
	可用性	サービス不能	サービス妨害攻撃等によりデータの移転・提供に係る設備や機器が一時的に停止する。

		システムの不具合	データの移転・提供に係る設備や機器に不具合が生じ、処理が一時的に停止する。
		自然災害等	地震や津波等の自然災害によりデータの移転・提供に係る設備や機器に被害が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	-	該当なし
	知的財産・営業秘密保護	提供先での目的外利用	「稼動レポート」の作成を通じた製品設計の改善等が「製造事業者–A 社 サービス利用契約」において規定されておらず、製造事業者からクレーム等が生じる。
			ある製造事業者における「稼動レポート」等の秘密情報を含むデータが、A 社を介して元の事業者の競合事業者等へ渡る。
		利用期間外のデータ利用	「製造事業者–A 社 サービス利用契約」において定められたデータの利用期間を越えても、分析基盤上または A 社設計部門の環境で「計測値」、「余寿命」または「保全優先度」等が削除等されず、利用可能となっている。

最後に、イベントD：「余寿命」、「保全優先度」のB社（保守会社）、部品サプライヤ等への「移転・提供」に際しては、イベントCと同様にネットワーク上でのセキュリティ脅威が想定されることに加え、A社とB社及びC社との契約の範囲内でデータが取扱われているかという観点でリスクが特定された。

表2.3-7 「余寿命」、「保全優先度」のB社（保守会社）、部品サプライヤ等への「移転・提供」にて想定されるリスクの例

大分類	中分類	脅威分類	想定されるリスク
セキュリティに係る観点	機密性	なりすまし、　情報漏えい	データ分析基盤から B 社（保守会社）、部品サプライヤのシステム環境までのネットワーク上で、「余寿命」、「保全優先度」を含むデータが悪意のある第三者に傍受され、漏えいする。
		なりすまし、　情報漏えい	正規の利用者になりすまされる、または脆弱性を悪用され、データ分析基盤または部品サプライヤのシステム環境に不正ア

			クセスされ、「余寿命」、「保全優先度」が不正な送信先へ移転される。
		情報漏えい	「余寿命」、「保全優先度」へのアクセス管理に不備があり、保守会社または部品サプライヤにより、本来特定されるべきでない機密データ（例：他社製部品に関するデータ）が特定される。
	完全性	なりすまし、 改ざん	データ分析基盤からB社（保守会社）、部品サプライヤのシステム環境までのネットワーク上で、「余寿命」、「保全優先度」を含むデータが悪意のある第三者に傍受され、改ざんされる。
		改ざん	悪意のある内外の主体により意図的に、データ分析基盤またはB社（保守会社）、部品サプライヤの環境で取扱われる「余寿命」、「保全優先度」の全体又は一部が改ざん又は削除される。
	可用性	サービス不能	サービス妨害攻撃等によりデータの移転・提供に係る設備や機器が一時的に停止する。
		システムの不具合	データの移転・提供に係る設備や機器に不具合が生じ、処理が一時的に停止する。
		自然災害等	地震や津波等の自然災害によりデータの移転・提供に係る設備や機器に被害が生じ、処理が一時的に停止する。
法制度等に係る観点	パーソナルデータ保護	-	該当なし
	知的財産・営業秘密保護	提供先での目的外利用 利用期間外のデータ利用	「余寿命」、「保全優先度」等派生データの利用権限が「製造事業者 – A社 サービス利用契約」及び「A社–B社データ利用契約」において十分に定められておらず、利用目的や第三者提供の可否等について製造事業者からクレーム等が生じる。
			悪意のあるB社（保守会社）、部品サプライヤ関係者（退職者を含む）により、不正の利益を得る目的又は権利元に損害を加える目的で「余寿命」、「保全優先度」が取得、利用される。

			製造事業者–A 社 サービス利用契約」及び「A 社–B 社データ利用契約」において定められたデータの利用期間を越えても、分析基盤上または B 社（保守会社）、部品サプライヤの環境で「計測値」、「余寿命」または「保全優先度」等が削除等されず、利用可能となっている。

2-3-4-2. 今後のデータ管理の高度化に向けた課題の検討

上記で特定されたリスクへの対応は多岐にわたり得るが、中でも法制度等に係るリスクを中心に、A社によるデータ管理の更なる高度化に向けて有益と考えられる施策を列挙する。

- 製造事業者各社から取得したデータの管理
  - ✓ 製造各社から収集したデータを、彼らが通常想起しやすい保守サービスの高度化だけでなく、A社内の用途（製品向上等）のための分析やその他の目的で利用する場合、製造事業者との契約で規定した利用目的と実際の利用が整合しているかどうかが問題となるが、実際の管理においては以下の事項に留意すべきである。
    - ・ 契約で定める利用目的に、上記の用途が明確に特定できる記載を設ける。既存契約でそれらの用途が含まれていない場合には、利用目的の変更等を実施する。
    - ・ ある製造事業者から得た秘密情報は、他社の秘密情報と分離して管理する。（他社への不正開示等で訴えられたときに当該事業者の秘密情報が開示範囲に含まれないことを立証することが困難となるため）
    - ・ 製造業者ごとに個別管理しているデータベース内のデータを一つのデータベース統合する場合、製造業者を特定しないように抽象化を行ったうえで、当該処理の実施が契約で許容されている利用目的の範囲に含まれるかを確認する。

- 派生データの取扱い
  - ✓ 元データを基に作成された派生データや加工データ、モデルその他成果物を総称したものである派生データ等（ここでは、余寿命、保全優先度、稼動レ

ポート等）の利用条件を、「製造事業者–A社サービス利用契約」及び「A社–B社データ利用契約」において明示する必要がある。かかるデータの利用条件の曖昧さや認識の相違は、データの取扱いにおける不確実性につながり得ることから、以下の項目（例）について条件を明確化することが想定される。

- 利用目的
- 第三者提供の可否
- 加工等の可否
- 契約終了時の取扱い　等

- A社設計部門、保守会社、部品サプライヤ等におけるデータの取扱い
  - ✓ 各種データへのアクセス権限を有する組織間で、組織やシステムのセキュリティ水準が異なることが想定されるが、管理の水準が低い組織が存在する場合、A社にとって予期せぬセキュリティインシデントが生じる可能性がある。
  - ✓ A社と各社との契約の中にデータの安全管理に関する条項を設け、適宜チェックシートによる対策状況の確認を実施したりすることに加え、データに機密性の高い情報が含まれる場合は、セキュリティやデータ保護の観点から、A社設計部門、保守会社、部品サプライヤの環境にはダウンロードできないようにする等の利用制限を含む対応をとることも想定される。

[その他] データ越境移転時の留意点

- ✓ データ分析基盤が日本国内に所在する場合、製造事業者からA社、A社からB社へのデータ移転は、いわゆる越境移転に該当することから、以下の事項に留意する必要がある。
  - フランス所在の事業所に設置されている製造機器から収集するデータに個人データが含まれる場合、GDPRにおける個人データ処理・移転関連規定を遵守する。
  - 海外の製造業者等とデータ取扱いに係る契約を締結する場合は、準拠法や紛争解決手段の選択を慎重に行う。
  - その他、関連する制度の動向を注視し、新たなルール形成が実施される際には、早期にデータフローの見直し等を行う。

参考：適用実証を踏まえた所見

GAIA-X等のセキュアデータ交換プラットフォーム構築・活用は、各社、各国単独で構築するのではなく協調領域として産官連携で取り組む領域と考える。

セキュリティの確保と、個別に契約対応・法理遵守対応を実施費用よりも、プラットフォームに参加する参加費用の安価に抑えるという点を参加者の共通の目標として構築・活用を推進するべきである。

2-4. IoS-OP（Internet of Ships Open Platform）による船舶運航データの流通

海運業、造船業や舶用工業等を含む海事産業においては、近年急速にデジタライゼーションが発展を遂げており、産業を構成する諸企業・組織・団体が、実ビジネスにおけるそれぞれの立場で船舶IoTデータの共有とそのデータを利活用する場が求められている。

IoS-OP（Internet of Ships Open Platform）は、上記のような背景を踏まえ、海事業界におけるデータ流通を実現し、デジタル時代における新たな海事クラスターの形をつくり、次世代につなぐべく、データの創出・送受信・蓄積・活用など上流から下流までの作業を役割分担し、各社が得意分野に自由に参画できるデータ流通基盤を形成している。関係者が、データを活用したイノベーション、新規サービス開発といった競争領域に注力できるよう、データ流通に関わる部分を協調領域とする環境を整備する。

IoS-OPでは、データ収集、活用に関わるステークホルダーを以下のように整理し、それぞれの役割を定義している[15]。

- PU（Platform User）
  データ収集にかかる費用（船上装置や通信費）を負担するデータ利用権管理者。主に船主、船舶管理会社、傭船者、造船所など。
- PP（Platform Provider）
  船上データサーバーの販売者や船上データ収集サービスの提供者。主に船上データ収集装置のメーカーまたは販社。
- ShipDC（Shore Datacenter）
  クラウド上の安全なデータ保管、秘密鍵を使ったアクセスコントロール、およびRESTful API によるデータ配信を行う陸上データセンター。
- SP（Solution Provider）
  遠隔メンテナンスサポートや性能解析レポート、状態監視など、データ分析や高付加価値サービスの提供者。
- SU（Solution User）
  船舶の運航に寄与する目的で、データの利用許諾を受けるデータ利用者。主に船主、船舶管理会社、傭船者、船員など。

[15] ステークホルダーの役割（https://www.shipdatacenter.com/ios-op-terms/stakeholder ）

- DB（Data Buyer）
  自社製品の改善などのためにデータの利用許諾を受けるデータ利用者。主に造船所、舶用メーカーなど。

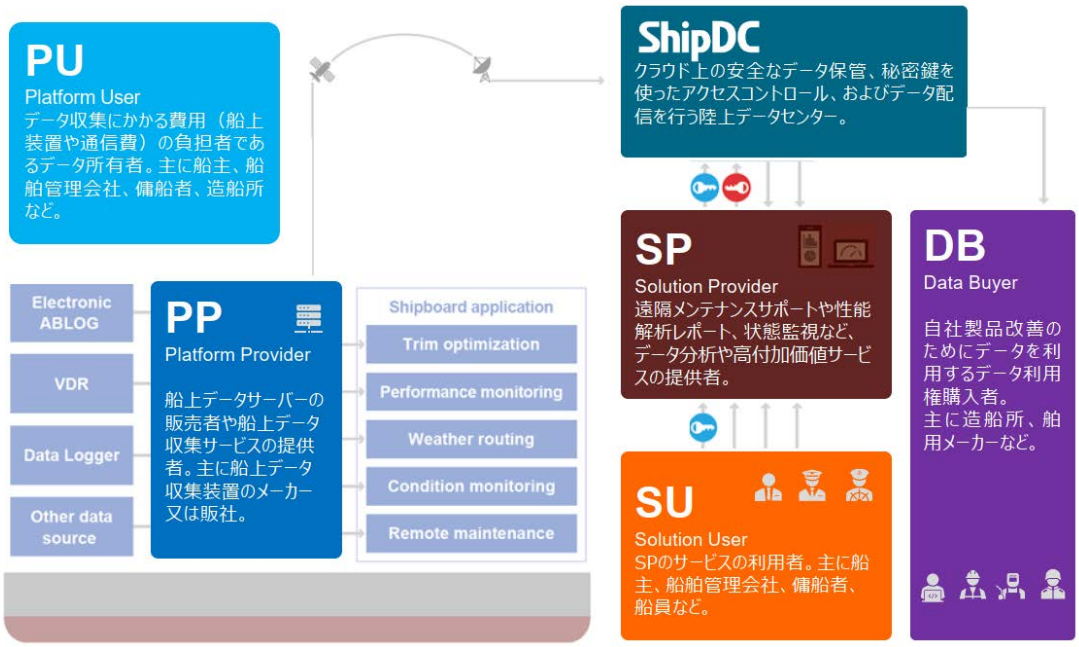

図2.4-1 IoS-OPとステークホルダーの全体像

本節では、マルチステークホルダー環境におけるリスクの洗い出しや対策の導出を行い、関係各社に展開することで、よりよいデータ管理の実践を進めることを目的として、IoS-OPを対象にDMFを適用する。

2-4-1.　STEP 1　データ処理フロー（「イベント」）の可視化

STEP 1では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」を可視化するところ、本ケースでは、最初に、図2.4-1に示した全体像におけるステークホルダーと「イベント」との関わりを図2.4-2のように可視化した。

- PU（Platform User）：船上データ収集装置で収集したデータの「保管」、「加工・利用」
- PP（Platform Provider）：船上データ収集装置によるデータの「生成・取得」、船上データサーバーにおける収集データの「保管」、「加工・利用」
- ShipDC（Shore Datacenter）：船上データ収集装置で収集したデータの「保管」、「加工・利用」、SPやDBへのデータの「移転・提供」

- SP（Solution Provider）：ShipDCから提供を受けたデータの「加工・利用」
- DB（Data Buyer）： ShipDCから提供を受けたデータの「加工・利用」

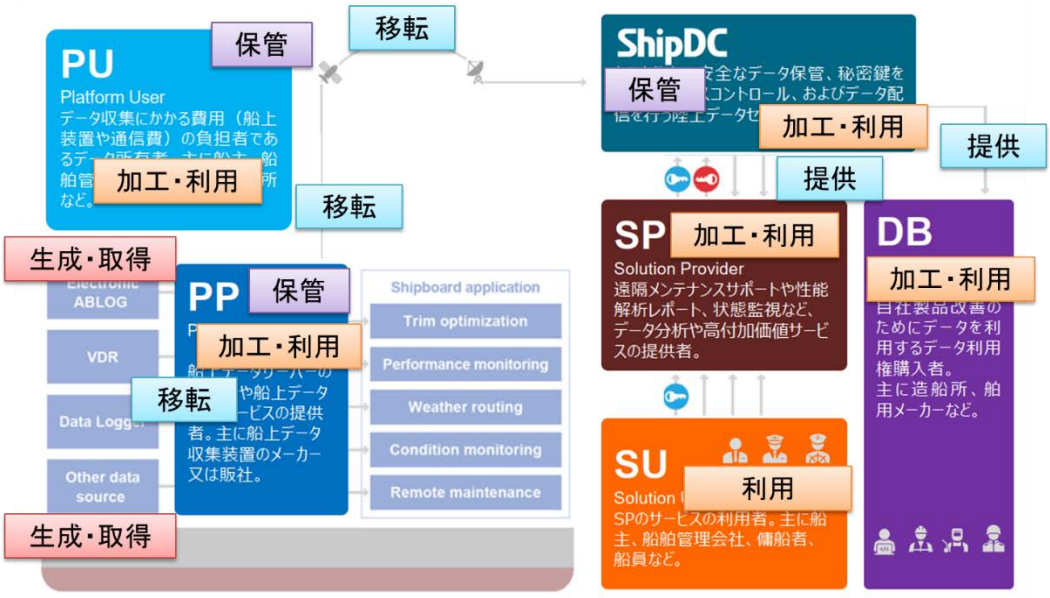

図2.4-2 ステークホルダーと「イベント」との関わり

図2.4-2で整理した内容に沿って、今回分析の対象とするデータフローとして、活動全体の中から、リスク及び重要度を考慮した具体的な利用事例を基に絞りこんだ。

（1） 船上（PP）に設置された機器（VDR：Voyage Data Recorder、AMS：Alarm Monitoring System）から「計測データ」が「生成・取得」され、船上データサーバーへ「移転・提供」される。船上データサーバーでは、それらのデータは「統合計測データ（秒間隔）」として「保管」され、適宜、「統計・解析データ」へと「加工・利用」される。

（2） 船上に保管された「統合計測データ（秒間隔）」のうち、必要な部分が「間引きデータ」としてShipDCの陸上データセンターへと「移転・提供」され、「時系列データ」として「保管」される。PUからの許諾等に基づいて、当該データはSPに「移転・提供」される。

（3） SPに移転された「提供データ」はサービス内容等に応じて、「統計・解析データ」や「AI・学習・教師データ」へと「加工・利用」される。

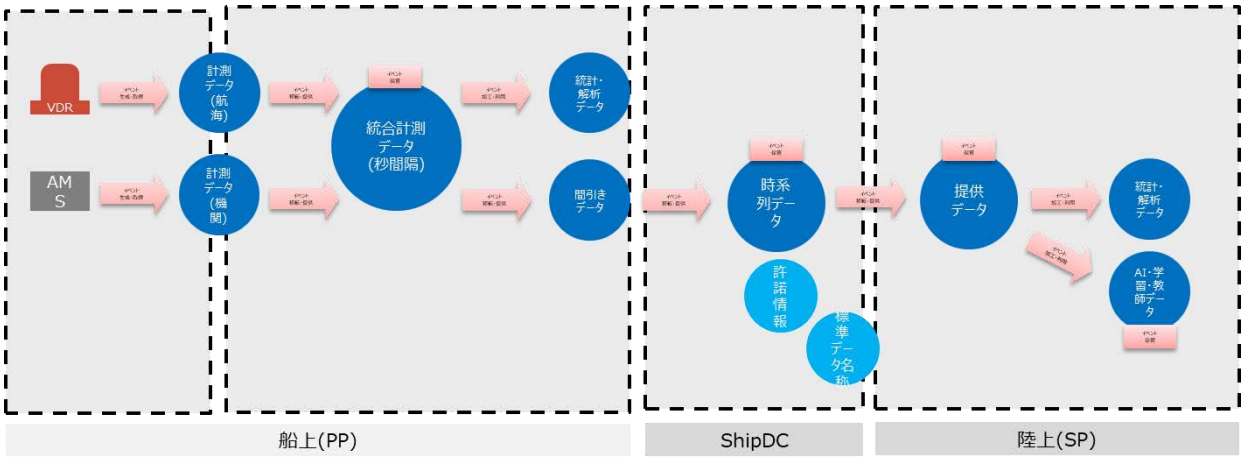

図2.4-3 データ処理フローの可視化

2-4-2. STEP 2 必要な制度的な保護措置（「場」）の整理

STEP 2では、STEP 1で特定したデータフローにおける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した。

（1） 海上国際条約

国際航海する船舶には国際条約が適用される。海上人命安全条約（SOLAS条約）における国際安全管理（ISM）コードにおいて、船主・運航者に対し、サイバーリスク対策実施（データのセキュリティ強化を含む）が強く推奨されている。

（2） 不正競争防止法

データが不正競争防止法上の営業秘密や限定提供データに該当する可能性があり、この場合、不正な取得、使用、開示に対する差止請求、損害賠償請求が認められる。IoS-OP利用規約では、秘密保持義務、第三者提供禁止義務等、不正競争防止法上の営業秘密、限定提供データ制度に基づく法的保護を意識した規約を策定している。

（3） PP-PU間個別契約（機器、ソフト購入/設置、サービス契約）

PPがPUに提供するサービスについて2者間でおこなう契約で、通常は、サービス内容や禁止事項、利用条件、セキュリティ等が取り決められる。但

し、2者間の相対契約であるため、本適用実証の範囲外としている。

（４） IoS-OP利用規約[16]

経済産業省の「データの利用権限に関する契約ガイドラインver1.0」をベースに、海事業界内でのデータオーナーシップの整理、データの利用範囲、二次加工、匿名化などについて協議を重ねて制定したもの。 IoS-OP利用規約は、IoS-OP利用者全員が遵守すべき基本規約と、それぞれのステークホルダー間ごとの規約で構成される。データオーナーシップの権利関係整理用にデータ利用権限設定のひな形や、各種ケース別の適用ガイドラインも用意している。

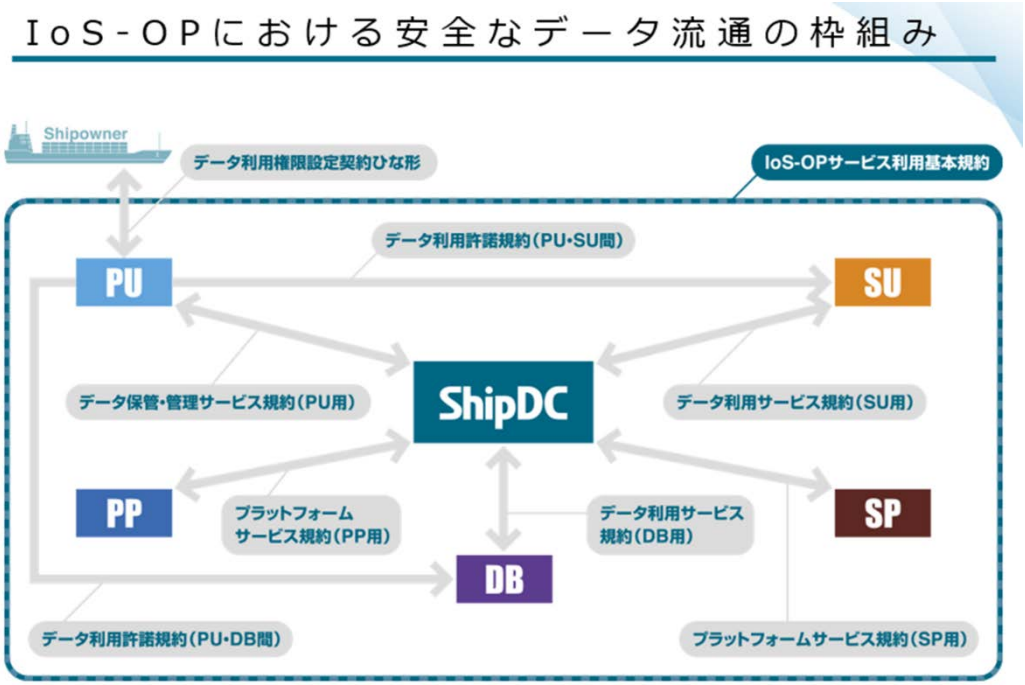

図2.4-4 IoS-OP利用規約の概要

（５） SP-SU 間個別契約

SPがSUに提供するサービスについて２者間で行う契約で、通常、サービス内容や禁止事項、利用条件、セキュリティ等が取り決められる。但し、2者間の相対契約であるため、本適用実証の範囲外としている。

（６） イベント発生/データ収集国法律

[16] 概要については、以下を参照されたい。
IoS-OP 利用規約（https://www.shipdatacenter.com/ios-op-terms/terms-2 ）

船舶が沿岸国の領海内を航行、寄港する際にデータに関するイベントが発生する場合、そのイベントに沿岸国の法律が適用される可能性がある。

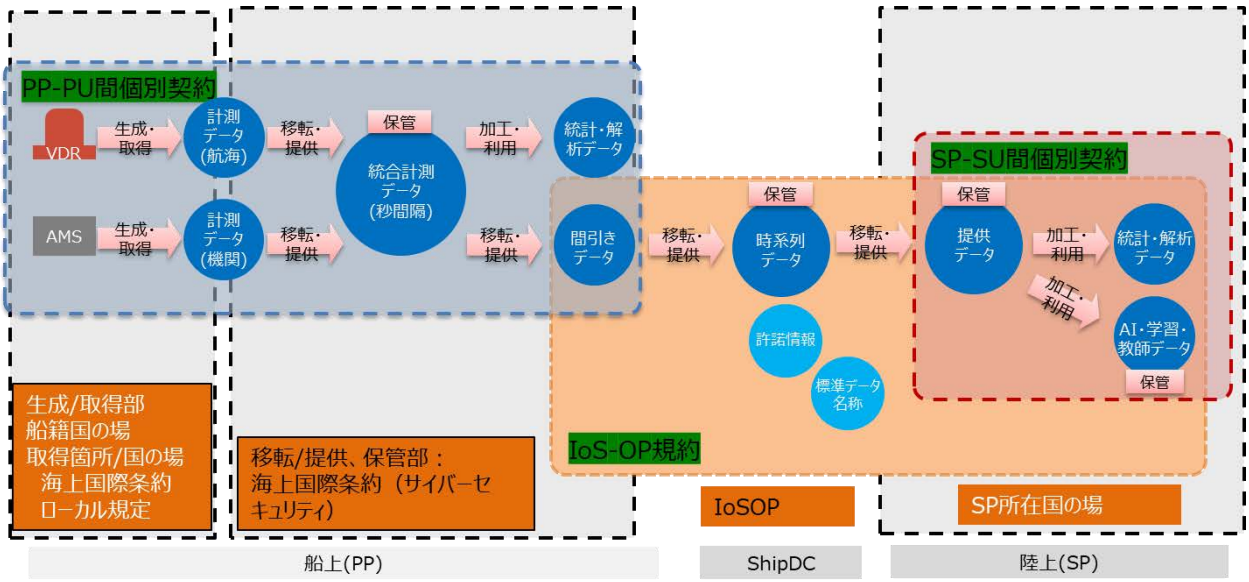

図2.4-5 必要な制度的な保護措置の整理

「場」については法律・契約の観点から絞り込みや具体的な内容の把握が必要だが、本STEPでは、まずは考えられるものをすべてリストアップし、絞り込みはSTEP 3で行うこととした。

2-4-3. STEP 3 「属性」の具体化

STEP 3では、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STEPの最初の検討として、表2.4-1にあるように、前STEPにて特定した「場」と「属性」項目との関係を整理した。

表2.4-1 特定した「場」毎のデータ管理に資する「属性」[17]

	海上国際条約、船籍国/地域規制	不正競争防止法	PP-PU 間個別契約	IoS-OP 規約	SP-SU 間個別契約	イベント発生/収集国法律
カテゴリ	○（サイバーセキュリティ）SOLAS[18]9章	○（営業秘密）（限定提供データ）	メーカー間契約	内部規約	メーカー間契約	
開示範囲	―	○	△	○（契約毎に PU が指定）	△	
利用目的		○（保護を受けるため）	△	○（契約毎に SU,DB が宣言、PU が了承）	△	
データ管理主体	―	―	△PP	○(PP/ShipDC/SP)	△SP	
データ権利者	―	○	△PU	○（PU が協議）	△[PU] or[SU が許諾されているべき]	
価値（重要度）		―	―	価値あるものとの前提	―	
媒体・保存先	○	―	△（IoS-OP で規定無し）	○ローカル(PP/SP/SU), クラウド(PU, ShipDC)	△（IoS-OP が要求）	

[17] △：個別契約だが考慮を推奨しているもの。

[18] SOLAS 条約（海上人命安全条約）とは、船舶の安全確保を目的とする国際条約。9 章では、船舶の安全運航の管理について規定。

利用期限	―	―	△	PU-SP/SU/DB 間で定める	△	
利用制限	○	○	△	○第三者提供禁止 目的外利用禁止 その他利用制限あり	△	○データ越境移転規制

次に、各「場」において課される具体的なデータ利用制約等について具体化を図ったうえで、各種データ管理に資する属性のパラメータを識別した。

表2.4-2 各種データ管理に資する属性

		船上 PP			ShipDC クラウド	陸上 SP		
属性の項目		運航データ			時系列データ	(ShipDC が) 提供したデータ	解析データ (加工済)	SP AI 解析用データ
		計測データ	統合計測データ	間引きデータ				
カテゴリ	パーソナルデータ保護	―			―	―	―	―
	知的財産（営業秘密）	営業秘密、限定提供データ			営業秘密、限定提供データ	営業秘密、限定提供データ	営業秘密、限定提供データ	営業秘密
開示範囲					SP/SU	SU	SU	SP 限定
利用目的		取得データを活用した各種サービスの提供			サービス提供	参照用サービス利用	運航解析	AI 機械学習
データ管理主体		PU			ShipDC	SP	SP	SP
データ権利者		PU			PU	PU	SP	SP
価値（重要度）		中（狙い通りの価値）			中	中	高	中⇒高

		（⇒高ビッグデータ化）			
媒体・保存先	船上サーバー	ShipDC クラウドサーバー	SP クラウドサーバー	SP クラウドサーバー	SP クラウドサーバー
利用期限	PU が決める	PU が決める	PU が決める	SP が決める	SP が決める
利用制限	第三者提供禁止、目的外利用禁止	目的外利用禁止	第三者提供禁止、目的外利用禁止	△ 第三者提供禁止、目的外利用禁止	△ 第三者提供禁止、目的外利用禁止

△：個別契約だが考慮を推奨しているもの。

2-4-4.　STEP 4　「イベント」ごとのリスクポイントの洗い出し

2-4-4-1.「イベント」ごとのリスクポイントの洗い出し

STEP 4において、対象とするプロセスにおけるデータ取扱いに係るリスク及び、それらに対する有効な対処を特定するにあたり、本件においては以下のような流れで検討を行った。

1. ライフサイクル全体を俯瞰して、リスク特定の対象とするイベントを選択する。
2. 選択したイベント毎に、法律/契約上の観点及びサイバーセキュリティに係る観点からリスクを洗い出す。
3. 特定したリスクを、影響度、起こりやすさ等の観点から評価し、優先的に対処するべきものを明確化する。
4. 上記リスクを管理するために必要な措置を識別し、実行していることを確認する。

上記1. の実施を通じて、以下４件のイベントについて、法・契約に関連するものを中心とするリスクの洗い出しや必要な措置の明確化を行うこととした。

- 船上機器を通じた「計測データ」の「生成・取得」
- 船上（PP）からShipDCクラウドへのデータ「移転」
- 船上からの移転されたデータのShipDCクラウド上での「保管」
- ShipDCから移転された「提供データ」のサービス提供者による「加工・利用」

○ 船上機器を通じた「計測データ」の「生成・取得」

	保護の観点	脅威主体の区分	想定されるインシデント	脅威	有効な対策要件
法律上（契約）	営業機密、限定提供データ	偶発的/アドバーサリ	データの持ち主の取り決めが不十分	不十分なコンプライアンス	データ利用契約（船主⇔PU）
	営業機密、限定提供データ	偶発的/アドバーサリ	不適切な方法によるデータ取得	不十分なコンプライアンス	データ利用契約（船主⇔PU）

○ 船上（PP）からShipDCクラウドへのデータ移転

	保護の観点	脅威主体の区分	想定されるインシデント	脅威	有効な対策要件
法律上	各国の安全、公共/組織の利益等	偶発的	現地のデータ越境移転規制の対象となるデータの取得、移転等	不十分なコンプライアンス	各国法令の適用確認
	営業秘密、限定提供データ	アドバーサリ	悪意のある従業員が、本船固有情報や営業秘密等を権限のない第三者に移転・提供する	不十分なコンプライアンス	秘密管理性、電磁的管理性（ID、パスワード等による管理）を確保した管理 IoS-OP 規約（情報セキュリティガイドラインの作成と遵守）→違反した場合の規定もあり
ISMS（セキュリティ）	機密性	偶発的	提供元による許諾のない第三者提供「データが悪意のない正規の利用者により本来想定されていない送信先へ移転・提供される。」	情報漏えい	外部向き通信の監視、対処 IoS-OP 規約 (データ利用権限に関する表明保証)
	機密性	偶発的	(同一事業者内であっても)設定された開示範囲を越えたデータ開示・提供	情報漏えい	秘密管理性、電磁的管理性を確保した管理 IoS-OP 規約 データ利用権限に関する表明保証)

○　船上からの移転されたデータのShipDCクラウド上での「保管」

	保護の観点	脅威主体の区分	想定されるインシデント	脅威	有効な対策要件
法律上（契約）	営業秘密、限定提供データ	偶発的	他社より提供を受けた営業秘密情報等について、利用期限が過ぎているにもかかわらず、別途許可等を得ることなく保管されたままとなっている。	不十分なコンプライアンス	データの遅滞のない消去 適切な情報管理・運用体制の確保
	営業秘密、限定提供データ	アドバーサリー	悪意のある外部の攻撃者、従業員又は退職予定者等により、営業秘密、限定提供データとして管理される保管データがアクセスされ、データが外部へ漏えいする。	情報漏えい	秘密管理性、電磁的管理性を確保した管理

○ ShipDCから移転された「提供データ」のサービス提供者による「加工・利用」

	保護の観点	脅威主体の区分	想定されるインシデント	脅威	有効な対策要件
法律上	営業秘密、限定提供データ	偶発的/アドバーサリ	従業員により必要な手続きを踏むことなく、事前にデータ取得元の組織人と合意した利用条件（利用目的、利用制限、利用期限など）とは異なる条件でデータが利用される。(ここには、複数組織から受領したデータの無許可の突合、コンタミネーション等も含まれ得る。)	不十分なコンプライアンス	IoS-OP 規約（利用条件の確認、制限） →違反した場合の規定もあり
ISMS（セキュリティ）	機密性	偶発的	アプリケーションやデータベース等におけるアクセス制御等の設定ミスにより本来保護が必要なデータが外部から閲覧可能となってしまう	情報漏洩	適切な情報管理・運用体制の確保 IoS-OP 規約（情報セキュリティガイドラインの作成と遵守） →違反した場合の規定もあり

上記で検討したリスクのうち、影響度、起こりやすさ等の観点から評価し、優先的に対処するべきものとして、以下が明確化された。

＜船上（PP）からShipDCクラウドへのデータ移転＞

■ 現地のデータ越境移転規制の対象となるデータの移転等

[有効と考えられる施策]

・ データの移転等が、特定のデータの越境移転を制限し、国内保存を義務付ける等の現地データ越境移転規制の対象となるかを確認する必要がある。適用対象となる可能性がある場合、同規制の内容、執行状況などに留意することが望ましい。

■ 悪意のある従業員が、本船固有情報や営業秘密等を権限のない第三者に移転・提供する

[有効と考えられる施策]

・ 悪意のある従業員による営業秘密等の不正な使用、開示等に対しては、営業秘密としての秘密管理性を確保した管理を行うとともに、限定提供データとしての保護を受けるためにID、パスワード等による電磁的管理を実施することが望ましい。

・ （PPのもとでの情報の不正な開示等は、ShipDCへのデータ移転前のイベントであり、一次的にはPU-PPサービス契約で定めるべきことではあるが、）PPが同意すべきShipDCのプラットフォームサービスの利用規約・セキュリティガイドラインにおいて、PPが満たすべきセキュリティ要件を定め、セキュリティガイドラインの遵守を求めるとともに、利用・管理状況についての報告義務を課し、報告が十分でない場合はShipDCが監査を実施する。

＜ShipDCから移転された「提供データ」のサービス提供者による「加工・利用」＞

■ 従業員により必要な手続きを踏むことなく、事前にデータ取得元の組織人と合意した利用条件（利用目的、利用制限、利用期限など）とは異なる条件でデータが利用される。

[有効と考えられる施策]

- SPが同意すべきShipDCのプラットフォームサービスの利用規約において、利用条件を明確に規定し、利用条件に反する利用を制限する。また、利用条件に従った利用を確保するため、セキュリティガイドラインの遵守を求めるとともに、利用・管理状況についての報告義務を課し、報告が十分でない場合はShipDCが監査を実施する。

2-4-4-2. 今後のデータ管理の高度化に向けた課題の検討

今回の適用を通じて、今後の課題として、以下のように関係する主体間で必要な対策について協議することの重要性が再認識された。

- 「場」“PU-PP間個別契約” 及び“SU-SP間個別契約”は、当事者（PU-PP、SU-SP）間の取り決めであり、個々のサービス契約の内容については、今回の適用実証の範囲外としている。
- 今回の検討で、今回高優先度と選択されたイベントとも関連し、対策要件として整備しているIoS-OP規約とも関連があることが明確となり、STEP 3 では、“△個別契約だが考慮を推奨”を新設した。
- 今回の検討結果を基に、PU-PP間個別契約及びSU-SP間個別契約を実施している主体と、詳細な検討と必要な対策について協議することが望ましいため、今後の検討課題としたい。

2-5. 人起点のデータ取得によるワークプレイスの空間価値の継続的アップデート

昨今、コロナ禍における在宅勤務の増加等、従業員の働き方のさらなる多様化が指摘されており、オフィスで働くことの価値が改めて再考・再認識されつつある。これまでも働き方改革の流れの中で、フリーアドレス制に留まらず、オフィスワーカーが働く内容と場所を自ら決めるABW（Activity Based Working）等、多様な働き方が採用されてきたが、コロナ禍による変容はワークプレイスのあるべき姿やオフィスの価値等を見直す流れを大幅に強めたと言える。

上記の背景を踏まえたニューノーマル時代のワークプレイス創造を目指す取組みの一例として、パナソニック株式会社（以下、「パナソニック」という。）では以下を概要とするワークプレイス向けソリューション（本節において、以下、「本ユースケース」という。）を提供しているところ、本章ではDMFの適用対象として同ソリューションを取り上げた。

- パナソニックは、顧客会社オフィス（主に商業ビルに入居するテナント）に設置された機器から、空間のCO_2濃度や湿度などの環境データ、機器の稼働状況などの設備データを取得、クラウド上で解析を行い、サイネージやスマートフォンでの可視化や、照明・空調・熱交換気、音響機器等の設備運用へのフィードバックを行う。また、バイタルや位置情報、会話量などのヒトデータを取得・解析することで、人起点の空間最適化を行うとともに、効率的な施設管理・運営やそのために必要なコンサルティングレポートの作成等を行う。
- 顧客会社に提供するコンサルティングレポートの作成は基本的にソリューション提供会社であるパナソニックが実施するが、分析内容が高度である場合などは、適宜外部のコンサルティング会社に委託して実施される。

パナソニックでは図2.5-1に示すサービスの一部を既に提供しているが、今回は改めて当該サービスの企画構想段階に立ち返り、DMFを用いてリスク及び対策の特定を行うこととした。

その際、本ユースケースにおいて考慮すべきステークホルダーとして以下が挙げられる。

- パナソニック：クラウド提供会社が提供するクラウドサービスやコンサルティング会社によるデータ分析サービス（適宜）を利用しつつ、顧客会社向けにワークプレイス向けソリューションを提供する。
- 顧客会社：主に商業ビルに入居するテナントであり、パナソニックが提供するソリューションを利用し、オフィス運用の効率化・高度化を推進する。
- クラウド提供会社：パナソニック向けに、各種データを格納するクラウド基盤（東京リージョン）及び、同基盤上で可視化やレポーティング、制御判定を行うためのアプリケーションを提供する。
- コンサルティング会社：パナソニックからレポーティングデータ及び各種環境データ、設備データ等の提供を受けて、データ分析（深掘り）を行った上で、委託元へコンサルティングデータを提供する。

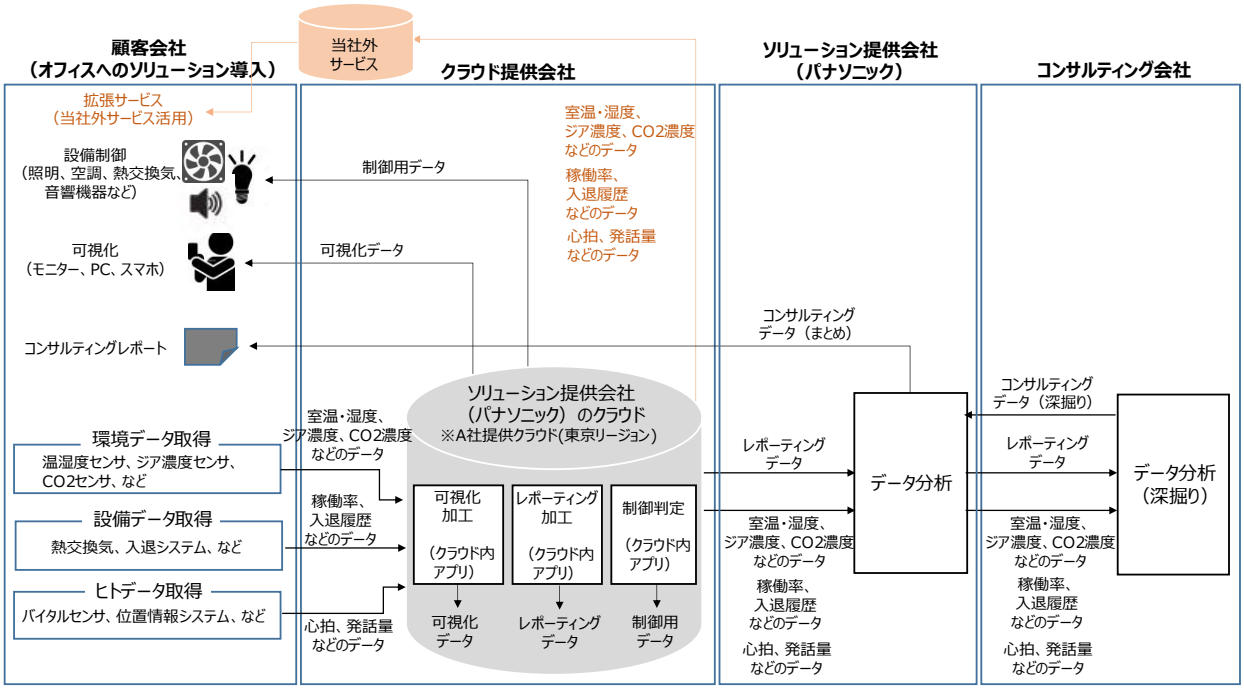

図2.5-1 ワークプレイス向けソリューションの概要

2-5-1. STEP 1 データ処理フロー（「イベント」）の可視化

本ユースケースでは図2.5-2で示すように、以下のプロセスにより構成される。

- 顧客会社（オフィス）に設置したセンサーやビル設備等から、「環境データ」、

「設備データ」、「ヒトデータ」が生成・取得され、パナソニックのクラウドに移転・提供される。各データの取得対象機器や内容は以下に示す通り。

表2.5-1. 取得データの取得対象機器と内容

データの種別	データ取得対象機器	取得データの内容
環境データ	温湿度センサー	室内の温度、湿度
	ジア濃度センサー	室内の次亜塩素酸濃度
	CO2 センサー	室内の二酸化炭素濃度
設備データ	熱交換気ユニット	熱交換気稼働状態
	入退システム	入退履歴
ヒトデータ	バイタルセンサ	オフィス内の個人の心拍数、発話量
	屋内位置情報システム	オフィス内の個人の位置情報

- パナソニックのクラウドでは、顧客会社（オフィス）内のセンサーからの各種データ（環境データ、設備データ、ヒトデータ）を纏めた「統合データ」から、顧客会社（オフィス）の設備制御に必要な「制御用データ」、統合データをスマホやモニターで見られるように加工した「可視化データ」、統合データを分析用に纏めた「レポーティングデータ」が二次的に生成（加工・利用）され、設備制御や可視化のため顧客企業に移転・提供される。「統合データ」は、必要に応じてパナソニック外部へと拡張サービス提供のため移転・提供される。
- 「統合データ」は設備制御や可視化のほか、顧客企業向けのレポート作成のため、効率改善等のアドバイスを付加した「コンサルティングデータ」に加工・利用される。高度な分析が必要な場合は、「統合データ」や「レポーティングデータ」がコンサルティング会社に移転・提供され、「コンサルティングデータ（深掘り）」に加工・利用されたうえで、パナソニックに移転・提供され、パナソニックが自社で実施した内容と合わせて最終的に顧客企業に提供される「コンサ

ルティングデータ（まとめ）」となる。

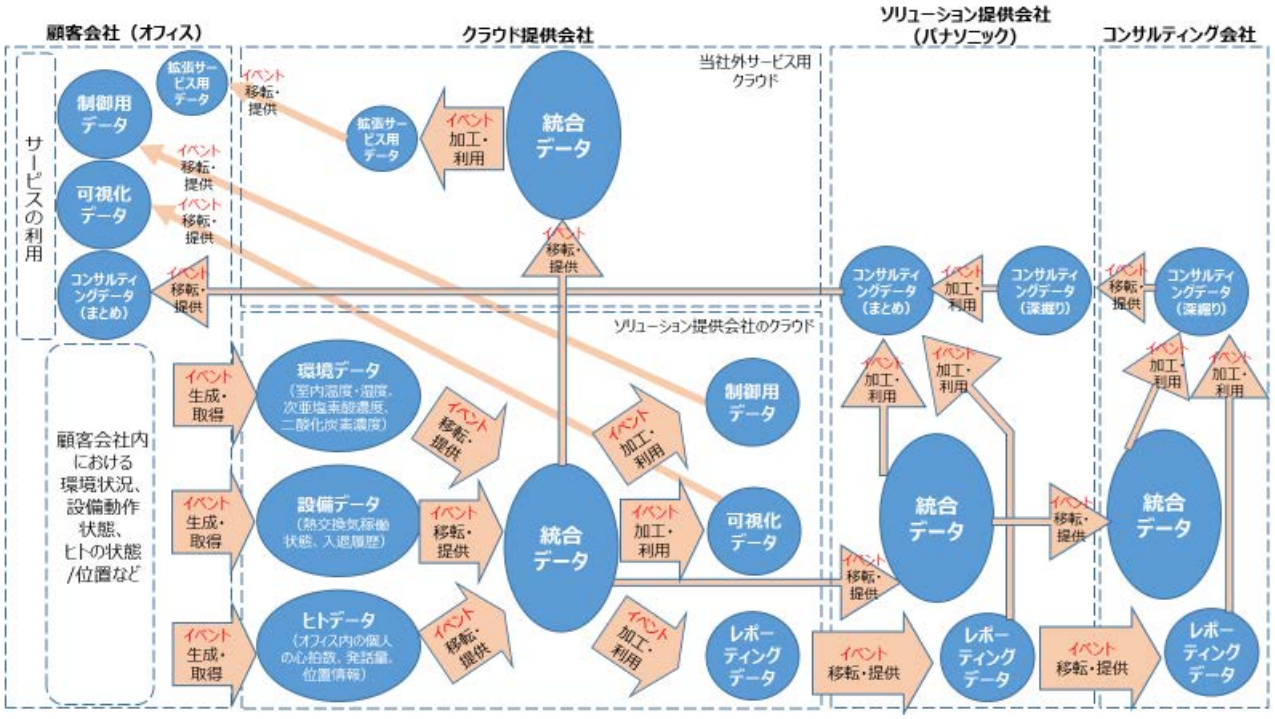

図2.5-2 データ処理フローの可視化

2-5-2.　STEP 2　必要な制度的な保護措置（「場」）の整理

本ユースケースでは、取扱うデータの性質や事業者の業種等を考慮すると、例えば下記のルールが「場」として特定され得る。

（1）個人情報保護法：顧客企業から取得、活用されるデータには、ヒトデータのように個人情報を含むデータが含まれることから、個人情報保護法の第17条から第40条に定めのある個人情報取扱事業者に課せられる義務を遵守する必要がある。それらの規定には例えば、利用目的の特定（第17条）、利用目的による制限（第18条）、安全管理措置（第23条）、委託先の監督（第25条）、第三者提供の制限（第27条）等が含まれる。

（2）データ提供契約含むサービス利用契約：ワークプレイス向けソリューション提供のために顧客企業とパナソニックとの間で締結されるもの。データの取扱いに係る規定として、以下を含む。

- データの利用目的：ソリューション提供会社（パナソニック）は、ソリューションサービスの実現・提供・向上のために必要なデータを収集・利用する。
- データの守秘とその期間：本サービス契約期間および満了後も、ソリューション提供会社は、本ソリューションサービスにより知り得た利用者の経営情報や個人情報の守秘義務を負う（第三者への開示および漏洩不可）。ソリューション提供会社からの提案やフィードバックなどのデータは、ソリューション提供会社が制約無く使用可能とする。
- データの加工と提供範囲：収集したデータは、ソリューションサービスの利用者（法人およびその法人の従業員）が特定できないように加工した上で、ソリューション提供会社およびその子会社が、ソリューションサービスや付随する活動のために使用することができる。

（3）秘密保持契約含むコンサル契約：高度なデータ分析実施のため、パナソニックとコンサルティング会社との間で締結されるもの。　データの取扱いに係る規定として、以下を含む。

- データの利用目的と守秘：コンサルティング会社は、パナソニックの委託により提供されたデータを委託内容以外のことに使用せず、パナソニックが「秘密」と指定して提示したデータについての守秘義務を負う。また、委託元の要求時および本契約終了時に、「秘密」指定データをソリューション提供会社に返却・消去する。
- データの帰属：ソリューション提供会社の委託によりコンサルティング会社が作成したデータ（コンサルティングデータ）は、ソリューション提供会社に帰属する。

（4）クラウドサービス（PaaS）利用契約：パナソニックとクラウド提供会社との間で締結されるものであり、データ取扱いに関連して以下の規定を含む。

- セキュリティ、データプライバシー：クラウド提供会社は、サービス利用者コンテンツを、事故、紛失、不正アクセスから保護するために適切な対策を実施する。
- クラウドサービス利用者の責任：クラウド提供会社自身の契約違反を除き、不正アクセスの責任はクラウドサービス利用者が負う。
- クラウドサービス提供会社によるサービス解除・解約：クラウドサービス

提供会社は、正当な事由があれば、サービスを解除することができる。

ー　また、クラウドサービ提供会社の都合により、契約の解約ができる。

（5）外部サービス利用契約：パナソニックと外部のサービス提供会社との間で締結されるものであり、秘密保持に関する以下の規定を含み得る[19]。

ー　秘密として取扱うデータの条件

ー　データの利用目的の明示、当該目的内での利用の制限

ー　データの第三者提供の制限

ー　データの利用期間、契約終了時の取扱い

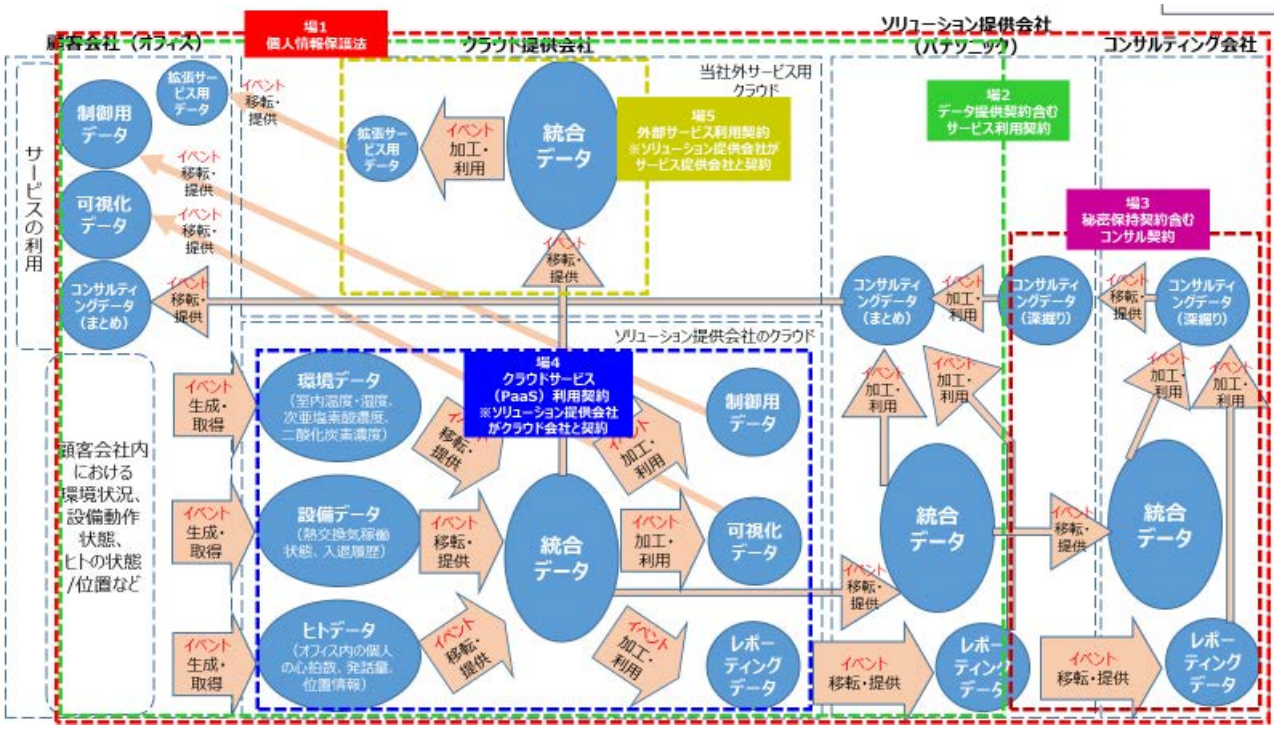

図2.5-3 必要な制度的な保護措置の整理（ワークプレイス向けソリューション）

2-5-3.　STEP 3　「属性」の具体化

STEP 3では、STEP 2にて特定されたデータの保護に係るルール（場）の効果的・効率的な遵守に資するデータの「属性」を特定する。

まず、STEP 2にて検討した「場」を、取扱いデータの「属性」（例：カテゴリ、開

[19] かかる規定の具体例については、「秘密情報の保護ハンドブック ～企業価値向上に向けて～」における「（参考資料２）各種契約書等の参考例 第６ 業務委託契約書（抄）の例」等を参照されたい。

示範囲、利用目的、媒体・保存先、利用期限）具体化にあたりどのように考慮すべきかを整理した。

表2.5-2 「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	データ提供契約含むサービス利用契約	秘密保持契約含むコンサル契約	クラウドサービス（PaaS）利用契約	外部サービス利用契約
カテゴリ	パーソナルデータ保護	○	○	○	○	○
	パーソナルデータ以外のデータ保護		○	○	○	○
	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			○	○	○	○

次に、STEP 1で洗い出されたデータのそれぞれに対して、ルール（場）で具体的に規定されている事項を踏まえて管理上把握しておくべき「属性」を割り当てた。

表2.5-3 本ユースケースにて取扱うデータの「属性」パラメータ例

		環境データ	設備データ	ヒトデータ	統合データ	制御用データ
カテゴリ	パーソナルデータ+それ以外のデータ保護	契約内容	契約内容	個人情報保護法 等、契約内容	個人情報保護法 等、契約内容	契約内容
	知的財産(営業秘密を含む)保護	–	–	–	–	–
開示範囲		顧客会社、ソリューション提供会社	顧客会社、ソリューション提供会社	顧客会社、ソリューション提供会社	顧客会社、ソリューション提供会社、コンサルティング会社	顧客会社、ソリューション提供会社
利用目的		取得データ活用による各種サービスの提供	取得データ活用による各種サービスの提供	取得データ活用による各種サービスの提供	取得データ活用による各種サービスの提供	設備制御
データ管理主体		ソリューション提供会社	ソリューション提供会社	ソリューション提供会社	ソリューション提供会社	ソリューション提供会社
データ権利者		顧客会社、ソリューション提供会社	顧客会社、ソリューション提供会社	顧客会社、ソリューション提供会社	顧客会社、ソリューション提供会社	顧客会社、ソリューション提供会社
価値・重要度		中	中	高	高	高
媒体・保存先		クラウド(ソリューション提供会社)	クラウド(ソリューション提供会社)	クラウド(ソリューション提供会社)	クラウド(ソリューション提供会社、外部サービス会社)サーバ(ソリューション提供会社、コンサルティング会社)	クラウド(ソリューション提供会社)
利用期限		サービス利用・データ提供契約期間	サービス利用・データ提供契約期間	サービス利用・データ提供契約期間	サービス利用・データ提供契約期間	サービス利用・データ提供契約期間

表2.5-3 本ユースケースにて取扱うデータの「属性」パラメータ例（続き）

		可視化データ	レポーティングデータ	コンサルティングデータ(深掘り)	コンサルティングデータ(まとめ)	拡張サービス用データ
カテゴリ	パーソナルデータ+それ以外のデータ保護	個人情報保護法 等、契約内容	個人情報保護法 等、契約内容	個人情報保護法 等、契約内容	個人情報保護法 等、契約内容	個人情報保護法 等、契約内容
	知的財産(営業秘密を含む)保護	–	–	–	–	–
開示範囲		顧客会社、ソリューション提供会社	ソリューション提供会社、コンサルティング会社	ソリューション提供会社、コンサルティング会社	顧客会社、ソリューション提供会社	外部サービス会社
利用目的		現状の見える化	現状分析	現状報告、改善や新サービスの提案	現状報告、改善や新サービスの提案	拡張サービスによる
データ管理主体		ソリューション提供会社	ソリューション提供会社	コンサルティング会社	ソリューション提供会社	外部サービス会社
データ権利者		顧客会社、ソリューション提供会社	ソリューション提供会社	ソリューション提供会社 コンサルティング会社	顧客会社、ソリューション提供会社	顧客会社、ソリューション提供会社
価値・重要度		高	高	特高	特高	拡張サービスによる
媒体・保存先		クラウド(ソリューション提供会社)	クラウド(ソリューション提供会社)サーバ(ソリューション提供会社、コンサルティング会社)	サーバ(ソリューション提供会社、コンサルティング会社)	サーバ(顧客会社、ソリューション提供会社)	クラウド(外部サービス会社)
利用期限		サービス利用・データ提供契約期間	秘密保持契約記載の期間	秘密保持契約記載の期間	データ提供契約終了後X年	外部サービス利用契約期間

2-5-4. STEP 4 「イベント」ごとのリスクポイントの洗い出し

STEP 4では、STEP 3までの内容を前提として、セキュリティ及び関連する法制度等の観点からいかなるリスクが想定されるかを特定し、必要な対策案を立案する。リスクの特定にあたっては、主にネットワーク越しの外部からの脅威や内部脅威を念頭に置いたセキュリティの保護に係る観点（機密性、完全性、可用性）だけでなく、昨今重要度が増しているデータの取扱いに関連する法制度等の観点（パーソナルデータ保護、知的財産（営業秘密を含む）保護）も踏まえた検討を実施した。

本ユースケースは、顧客企業環境からのデータ取得、クラウド上でのデータの加工・利用、コンサルティング会社や外部のサービス提供会社へのデータ提供等の様々なイベントから構成されている。本適用では、はじめにデータ利活用プロセス全体をいくつかの部分に分けてそれぞれでリスクの特定を実施した後で、下記に示すように最終的にそれらをまとめて提示することとした。

セキュリティの観点からは、顧客企業からのデータを集約するクラウドに格納された「統合データ」等への内外からの不正アクセス、それにつながり得るアクセス権限等の設定ミス、クラウドサービスの停止が重要度の高いリスク、脅威として特定された。また、それらに対する対策案として、「ユーザとサービスを紐付した上での認証の設定（適切なアクセスコントロール）」、「最小権限の原則による権限割り当て」、「データへのアクセスログの取得（トレーサビリティの確保）」、「データ改竄チェック機能の適用とデータバックアップの定期実施」、「縮退動作の確保（エッジコンピューティングによる）」が示された。

表2.5-4. オフィス向けIoTシステムにおけるデータの「生成・取得」、「移転・提供」、「加工・利用」、「保管」にて想定されるリスク①

大分類	中分類	想定されるリスク	対策案
セキュリティの保護に係る観点	機密性	・悪意のある外部の主体が、ソリューション提供会社の利用する外部クラウドストレージサービスの脆弱性を悪用して格納された　統合データに不正アクセスする。 ・ソリューション提供会社従業員によるクラウドストレージサービスにおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体に統合データが開示される。 ・悪意のある外部の主体が、顧客会社の利用する外部クラウドストレージサービスの脆弱性を悪用して格納された統合データに不正アクセスする。 ・顧客会社従業員によるクラウドストレージサービスにおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体に統合データが開示される。 ・ソリューション提供会社従業員による同社サーバーおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体に統合データが開示される。 ・コンサルティング会社従業員による同社サーバーおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体に統合データが開示される。 ・悪意のあるソリューション提供会社従業員により、統合データが不正に外部に持ち出される。 ・悪意のあるコンサルティング会社従業員により、統合データが不正に外部に持ち出される。	・ユーザとサービスを紐付した上での認証の設定（適切なアクセスコントロール） ・最小権限の原則による権限割り当て ・データへのアクセスログの取得（トレーサビリティの確保）
	完全性	・悪意のある外部の主体が、ソリューション提供会社の利用する外部クラウドストレージサービスの脆弱性を悪用して格納された統合データを改竄する。 ・ソリューション提供会社従業員によるクラウドストレージサービスにおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体が統合データを改竄する。	・ユーザとサービスを紐付した上での認証の設定（適切なアクセスコントロール）

		・悪意のある外部の主体が、顧客会社の利用する外部クラウドストレージサービスの脆弱性を悪用して格納された統合データを改竄する。 ・顧客会社従業員によるクラウドストレージサービスにおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体が統合データを改竄する ・ソリューション提供会社従業員による同社サーバーおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体が統合データを改竄する。 ・コンサルティング会社従業員による同社サーバーおけるアクセス権限等のセキュリティ設定が不十分な状態となっており、事前に想定されていない主体が統合データを改竄する。 ・悪意のあるソリューション提供会社従業員により、統合データが改竄される（クラウド、サーバー）。 ・悪意のあるコンサルティング会社従業員により、統合データが改竄される（クラウド、サーバー）。	・最小権限の原則による権限割り当て ・データへのアクセスログの取得（トレーサビリティの確保） ・データ改竄チェック機能の適用とデータバックアップの定期実施
	可用性	・外部クラウドストレージサービスを提供するサーバーの停止や通信トラブル等により、統合データの移転・提供（データを活用したサービス）に遅延が生じる。	・縮退動作の確保（エッジコンピューティングによる）

一方で法制度等に関連して、パーソナルデータ保護の観点から、利用目的の不遵守、不適切な手法によるデータ取得、自社従業員または委託先の監督不備、利用期間を越えたデータ保管・利用等がリスクとして特定された。また、個人情報を含まないデータに関しても、事業者間の契約の観点から、利用目的の不遵守、自社従業員または委託先の監督不備、複数事業者のデータのコンタミネーション、クラウドサービスの停止による事業影響等がリスクとして識別された。

上記リスクへの対応としては、自社だけでなくステークホルダー全体での保護を確保するため、「組織での情報管理ルールおよび体制の構築（定期チェック含む）」や「利用目的に不要な部分削除等のデータ加工（リスク軽減）」に加えて、委託先等を含めた施策である「契約書等への利用目的（範囲）の明記」、「契約内容周知、コンプライアンス教育の実施」、「委託先組織の情報管理ルールおよび体制の確認」、「委託内容に

不要な部分削除等のデータ加工（リスク軽減）」等が特定された。

表2.5-4 オフィス向けIoTシステムにおけるデータの「生成・取得」、「移転・提供」、「加工・利用」、「保管」にて想定されるリスク②

大分類	中分類	小分類	想定されるリスク	対策
関連する法制度等に係る観点	パーソナルデータ＋それ以外のデータ保護	個人情報保護法等	・ソリューション提供会社の社員により、顧客に通知された利用目的以外の用途でヒトデータが利用される。	・契約書等への利用目的（範囲）の明記 ・利用目的に不要な部分削除等のデータ加工（リスク軽減） ・契約内容周知、コンプライアンス教育の実施
			・ソリューション提供会社の社員が、不適正な方法で、ヒトデータを取得する。	・コンプライアンス教育の実施
			・ソリューション提供会社の管理/監督不備により、ヒトデータが漏洩する。 ・ソリューション提供会社が、契約に定められた利用期限を超えてヒトデータ利用・保管を行う。	・組織での情報管理ルールおよび体制の構築（定期チェック含む） ・コンプライアンス教育の実施
			・ソリューション提供会社の委託先（コンサルティング会社や外部サービス提供会社）の管理/監督不備により、ヒトデータが漏洩する。 ・ソリューション提供会社の委託先（コンサルティング会社や外部サービス提供会社）が、契約に定められた利用期限を超えてヒトデータ利用・保管を行う。	・契約書への要管理の明記 ・委託先組織の情報管理ルールおよび体制の確認 ・委託内容に不要な部分削除等のデータ加工（リスク軽減）
		契約内容	・ソリューション提供会社の社員により、顧客に通知された利用目的以外の用途でデータが利用される。	・契約書等への利用目的（範囲）の明記

				・契約内容周知、コンプライアンス教育の実施
			・ソリューション提供会社の管理/監督不備により、データが漏洩する。 ・ソリューション提供会社が、契約に定められた利用期限を超えてデータ利用・保管を行う。	・組織での情報管理ルールおよび体制の構築（定期チェック含む） ・コンプライアンス教育の実施
			・ソリューション提供会社の委託先（コンサルティング会社や外部サービス提供会社）の管理/監督不備により、データが漏洩する。 ・ソリューション提供会社の委託先（コンサルティング会社や外部サービス提供会社）が、契約に定められた利用期限を超えてデータ利用・保管を行う。	・契約書への要管理の明記 ・委託先組織の情報管理ルールおよび体制の確認
			・ソリューション提供会社内で、異なる顧客のデータのコンタミネーションが発生し、意図せず（悪意は無く）秘密情報の漏洩を生じさせる。	・コンプライアンス教育の徹底
			・クラウド提供会社が（クラウド提供会社の都合で）サービス終了や契約解除を行う（可用性の阻害）。	・クラウド提供会社とは、サービス終了や契約解除の事前通知から執行までの期間の長い契約を結ぶ（移行期間確保のため）

ここまでで示した施策のうち汎用性が高いものとしては、以下が挙げられた。単に社内規則や契約等に遵守事項を示すだけでなく、これらの施策を通じて関係者内へリスクへの認識や実施すべき対策を周知、教育することは、より確実に想定されるリスクを低減する上で有効と考えられる[20]。

- パナソニック関係者内でサービスに係る契約内容を周知する
- パナソニック関係者内でコンプライアンス教育を行う

今回、パナソニックはワークプレイス向けソリューションの企画構想段階に立ち返ってDMFを適用した。今後も、新サービスの運用開始前等のタイミングでの、新たなリスクの抽出及びリスクへの対策案の導出にDMFを用い、アセスメントレベルの向上を図る。

[20] 自社及び取引先従業員の教育研修にあたっては、IPA が公開している各種動画を従業員に視聴させるといった取組みも有効である。その他にも、IPA では研修に用いることのできる各種素材を公表している。
＜映像で知る情報セキュリティ＞
https://www.ipa.go.jp/security/videos/list.html#keihatsu
＜情報セキュリティ関連サイト＞
https://www.ipa.go.jp/security/guide/keihatsu.html

2-6. ネットワークインフラシステムのリプレースを対象とした設計構築における関係者間の情報共有

デジタル時代では、サプライチェーン間におけるデジタルデータの流通が進み、イノベーションが起こることが期待されている。組織間で情報を広く、迅速に共有することが企業の競争力を高める上で必要不可欠である。一方で、外的な脅威も高まっている環境の中、セキュアな情報共有空間が求められている。特に現在の不確実な世界情勢では、一部の企業の脆弱性が突かれることによる情報漏えいがサプライチェーン全体に多大な影響を及ぼすリスクが大きくなっている。

ITシステムの構築においては、顧客との要件定義から社内の顧客担当セールス部門、システム設計・構築を実施する開発部門の関係者、更に構築に携わるビジネスパートナー様の技術者の間での迅速、かつ頻繁な情報共有をセキュアに行うことが求められる。セキュアな情報共有は、設計、構築の開発のみならず、システム改修、日々の運用においても継続的に実施されなければならない。

このような背景から、富士通では公共機関および民間企業が保有する重要情報を保護し、組織内・組織間で安心・安全に情報共有、コラボレーションを実現するクラウドサービスである「Fujitsu NIST対応トラステッドコネクトサービス」を提供している。重要情報を保護するためのサイバーセキュリティ対策基準であるNIST SP800-171に準拠しており顧客のサイバーセキュリティ強化を安全かつ経済的に実現しているが、本書で取り上げる実在するネットワークインフラシステムのリプレース事業での設計構築における関係者間の情報共有を対象としたユースケースでも活用され、さらにセキュリティレベル向上を図る試みとしてデータマネジメント・フレームワークを適用した。

本ユースケースは、ネットワークインフラシステムのリプレースを対象とした設計、構築を行う事業で、顧客からの仕様書を基に設計書を作成して、レビュー、承認審査を経て設計書を納品する情報管理の一連の流れを対象とする。設計書等のドキュメントは、NIST対応トラステッドコネクトサービスを活用して関係者間での情報共有を行う。

- ネットワークインフラシステムの概要
  国内広域に展開する拠点、支店を結ぶ高速・大容量のネットワーク上に構成されたインフラシステムは、サービスとしてインターネット接続を含み、音声・

チャットサービス、テレビ電話サービス、情報共有サービス等を提供する。

- 設計、構築

  顧客から受領した仕様書に基づき、ネットワークインフラシステムリプレースの設計、構築を実施する。仕様書には、ネットワークインフラシステムに要求される機能、性能、品質、非機能要件、スケジュール納期、セキュリティ要件等がカバーされており、仕様要件を網羅するめの設計を行う。本開発プロセスはNIST SP800-171に準拠したNIST対応トラステッドコネクトサービスの中で実施する。

- 納品

  顧客審査会を受審し、仕様書を網羅している事の承認を得て、設計書は納品される。納品物である設計書はNIST対応トラステッドコネクトサービスから提供される。納品後の設計書自身のデータ管理は対象外とする。

本ユースケースでは、NIST対応トラステッドコネクトサービスを活用しているが、考慮すべきステークホルダーとして以下が挙げられる

- 顧客

  顧客はサービスが満たすべき条件や内容等を明確化した仕様書を提供し、さらに、設計業者（当社）との間で認識齟齬な発生しないように、また仕様の抜け漏れが起こらないようにするために、定期的あるいは不定期での打ち合わせや調整会を実施する。設計完成時には審査会を開催し、仕様書がカバーされている事を確認する。

- 当社

  当社は、セールス部門、プロジェクトマネージャ、法務部門、プロジェクトオフィス、SIチーム、ビジネスパートナー、品質部門、施設工事者等で構成され、取り扱うデータにより、利権者は異なる。

- ビジネスパートナー

当社メンバーに加えて、数社のビジネスパートナーの参加により、設計チームを構成する。ビジネスパートナーは、プロジェクトルームへの施設立ち入りや、NIST対応トラステッドコネクトサービスへのアクセスに関して、プロパーと同様に社内情報セキュリティルールやサービス利用規約に従う。図2.6-1に対象プロセスの概要を示す。

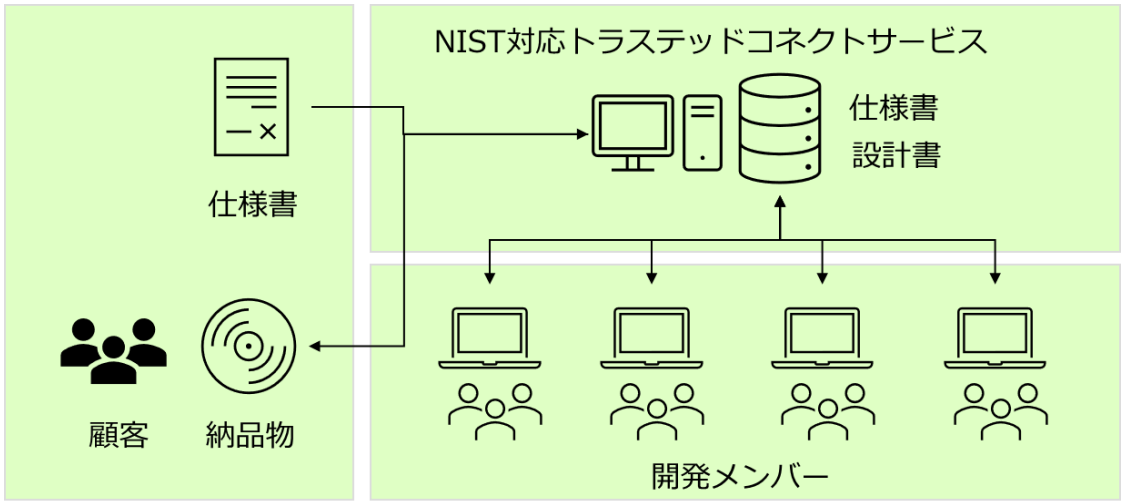

図2.6-1. 対象プロセスの概要

■　対象範囲

対象とする事業において、「設計」、「レビュー」、「審査」、「納品」を対象範囲とする。図3-1.1に対象とする事業フェーズの概要を示す。

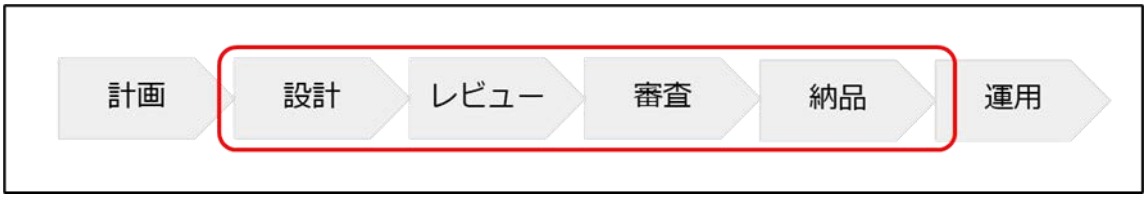

図2.6-2. 対象とする事業フェーズの概要

対象とする事業のフェーズで取り扱うデータのうち、「設計データ」を対象範囲とする。なお、具体的な「設計データ」は以下とする。

- 方式設計書
- 環境設計書
- デザインシート
- パラメータシート

・　インストール手順書

2-6-1.　STEP 1 データ処理フロー（「イベント」）の可視化

本ユースケースにおけるデータの処理フローを図2.6-3に示す。データ処理フローは、以下のプロセスにより構成される。

(1) 適切な契約に基づいて、顧客より仕様書を入手し、NIST 対応トラステッドコネクトサービスに「移転・提供」され、「保管」される。

(2) NIST 対応トラステッドコネクトサービス上の仕様書から、設計データ（初版）を「生成・取得」する。設計データはプロジェクトに関わるデータ権利者の手により「加工・利用」されることで設計データ（改版）に更新される。NIST 対応トラステッドコネクトサービスはデータ利権者の管理、権限の付与が厳格化され、セキュリティ上強固な対策が施されていることを前提としている。なお、NIST 対応トラステッドコネクトサービスは、物理層からアプリケーション層全てを包含している。

(3) 顧客審査を受けて承認が得られた設計書は、顧客先に「移転・提供」され、設計データ（納品版）として納品される。

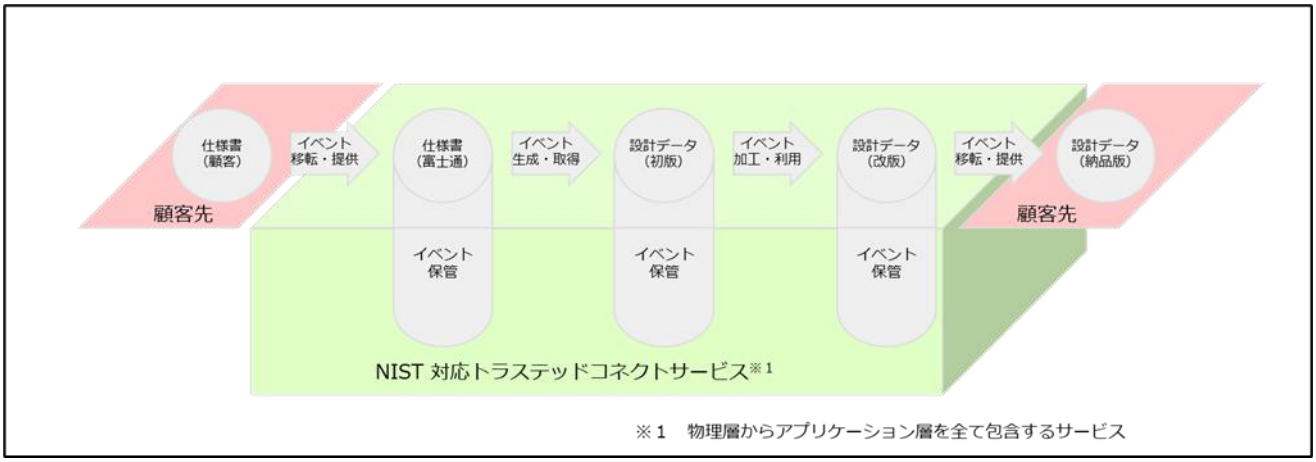

図2.6-3. データ処理フローの可視化イメージ

2-6-2. STEP 2 必要な制度的な保護措置（「場」）の整理

本ユースケースにおいて、取扱うデータの性質や事業者の業種等を考慮すると、例えば下記のルールが「場」として特定され得る。

(1) 情報セキュリティ特約：顧客が定める取り扱い情報のセキュリティレベルを示したもので本規約に従って取り扱いが制限される。なお、本規約は全てのフェーズにおいて適用される。

(2) 契約書：本事業において、顧客および富士通の権利・義務等の合意内容を記している。仕様書は契約書に則り提供される。

(3) 個人情報保護法：個人の権利・利益を保護することを目的とした個人情報の取り扱いに関連する法律。本事業で設計データを扱う要員を名簿にて管理するため、その際に個人情報保護法を考慮する必要がある。したがって、顧客から仕様書を入手後、設計データ作成から、設計データ納品までのフェーズで適用される。

(4) 社内情報セキュリティルール：顧客から提供される情報に加え、提供された情報をもとに作成された情報の取り扱いルールを定めている。当社の情報セキュリティガイドラインに沿って作成し遵守すべき規制である。顧客から仕様書を入手後、設計データ作成から、設計データ納品までのフェーズで適用される。

(5) 著作権法：著作物を創作した者が持つ権利を保護するとともに著作物の公正な利用を確保することを目的とする法律。

(6) サービス利用規約：NIST対応トラステッドコネクトサービス等を利用するための規則や手順等を記載している。顧客から仕様書を入手後、設計データ作成から、設計データ納品までのフェーズで適用される。

図2.6-4に必要な制度的な保護措置の整理結果を示す。

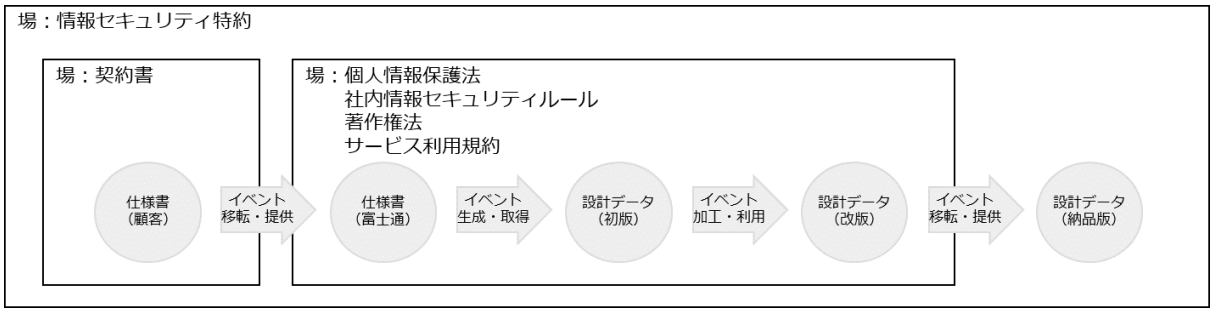

図2.6-4. 必要な制度的な保護措置の整理

2-6-3.　STEP 3 「属性」の具体化

各「属性」項目のパラメータを設定するにあたり考慮することが望ましいルールは以下のとおりと考えられる。表2.6-1に「属性」の検討において考慮すべきルール（場）を示す。

表2.6-1. 「属性」の検討において考慮すべきルール（場）

		情報セキュリティ特約	契約書	個人情報保護法	社内情報セキュリティルール	著作権法	サービス利用規約
カテゴリ	パーソナルデータ保護		○	○			
	知的財産（営業情報を含む）保護	○	○		○	○	○
展示範囲		○	○	○	○		○
利用目的		○	○	○	○	○	○
データ管理主体		○	○	○	○	○	○
データ利権者		○	○	○	○	○	
価値（重要度）		○	○	○	○		
媒体・保存先		○	○		○		○
利用期限		○	○		○		

本ユースケースにて取扱われるデータは情報セキュリティの確保が重要視されるため、「展開範囲」や「データ管理主体」、「データ利権者」、「媒体・保存先」の適切な設定と遵守状況のモニタリング等は特に重要となる。表4-3.2に本ユースケースにて取扱うデータの「属性」パラメータ例を示す。

表2.6-2. 本ユースケースにて取扱うデータの「属性」パラメータ例

		仕様書（顧客）	仕様書（富士通）	設計データ（初版）	設計データ（改版）	設計データ（納品版）
カテゴリ	パーソナルデータ保護	–	作業従事者関連情報	左記と同様	左記と同様	–
	知的財産（営業情報	顧客の秘密	顧客の秘密 富士通の秘密	左記と同様	左記と同様	左記と同様

	を含む）保護					
展示範囲		顧客内	関係者内	左記と同様	左記と同様	顧客内
利用目的		設計製造	左記と同様	左記と同様	左記と同様	運用維持
データ管理主体		顧客	プロジェクトマネージャ	左記と同様	左記と同様	顧客
データ利権者		顧客	セールス部門、プロジェクトマネージャ、法務部門	プロジェクトマネージャ、プロジェクトオフィス、SI チーム、ビジネスパートナー、品質部門、施設工事者		顧客
価値（重要度）		非常に高い	左記と同様	左記と同様	左記と同様	左記と同様
媒体・保存先		顧客先	NIST 対応トラステッドコネクトサービス	左記と同様	左記と同様	顧客先
利用期限		開発期間	左記と同様	左記と同様	左記と同様	運用期間

上記では表形式でデータとその属性の一覧を提示したが、プロセスの全体におけるデータの属性の変化とイベントの関係をより俯瞰的に示すために、STEP 2までに作成している図に属性を記入する。記入した例を図2.6-5に示す。

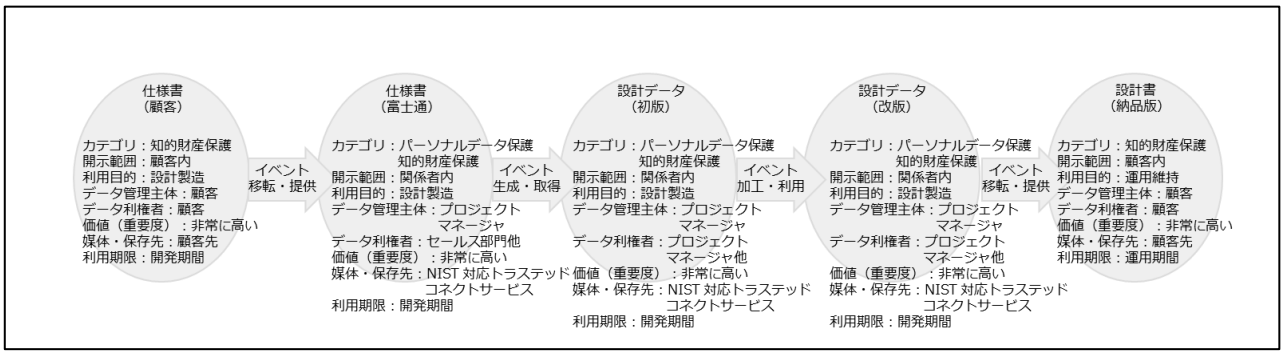

図2.6-5.「属性」の提示方法の例

2-6-4.　STEP 4　「イベント」ごとのリスクポイントの洗い出し

2-6-4-1.　「イベント」ごとのリスクポイントの洗い出し

STEP 3までの検討事項を踏まえ、「設計データ」の「移転・提供」、「生成・取得」、「加工・利用」、「保管」および「破棄」について以下のようなリスクを想定することができる。設計データに関して想定されるリスクは用いられる技術的手段により異なるこが想定されるが、ここでは当該の「生成・取得」、「加工・利用」、「保管」および「破棄」の行為が外部のNIST 対応トラステッドコネクトサービスを利用して行われるとしてリスクを抽出している。リスク抽出にあたり、より明確化するため、「保護の観点」と「脅威主体の区分」を併記する。

- 保護の観点
  リスク抽出を行う際に考慮すべき保護の観点を提示する。セキュリティの保護に関わるもの（機密性、完全性、可用性）と関連する法制度等に関わるもの（パーソナルデータ保護、知的財産保護等が含まれる。

- 脅威主体の区分
  対象となるプロセスに対して影響を及ぼし得る脅威の主体を以下の4つに分類している。表2.6-3に脅威主体の区分を示す。

表2.6-3. 脅威主体の区分

脅威主体の区分	概要
アドバーサリ（悪意のある主体）	サイバー資源（すなわち、電子的形態の情報、情報及び通信技術、ならびにそれらの技術によって提供される通信及び情報処理能力）に対する組織の依存を利用しようとする個人、グループ、組織、又は国家。一般的には、外部からのサイバー攻撃又は物理的な攻撃、内部犯行等が含まれる。
偶発的	日々の責務を実施する過程で必ずしも悪意のない個人が取る誤ったアクション（ヒューマンエラー等を含む）。
構造上	老化、リソースの枯渇、又は予測されたオペレーティングパラメータを超えるその他の状況に起因する、機器の故障、環境制御の失敗、又はソフトウェアの不具合。
外部環境上	組織が依存するが、組織のコントロールの範囲外である重要インフラに対する自然災害、及びそれらのインフラの故障。

なお、本ユースケースでは、「生成・取得」、「加工・利用」、「保管」および「破棄」の行為のうち、「生成・取得」のみ記載する。表2.6-4にデータの生成・取得過程におけるリスクの洗い出しイメージを示す。

表2.6-4. データの生成・取得過程におけるリスクの洗い出しイメージ

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	脅威	有効な対策要件
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又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 通信経路(*) 端末の挙動等の監視、対処
	アドバーサリ（悪意のある主体）	生成・取得されるデータがマルウェアに感染した機器・設備等から不正な送信先へ共有される。	情報漏えい	脆弱性対応プロセスの整備、実行(*) 端末、ネットワーク上におけるマルウェア対策の導入 外部向き通信の監視、対処
	偶発的	データの生成・取得に係る設備や機器に不適切な設定がなされており、データが本来想定していない主体から閲覧できるようになっている。	情報漏えい	機器・サービスの初期設定及び設定等の変更管理(*) ユーザ、機器、サービス等に対する適切な水準の認証の実施(*) 通信経路、端末の挙動等の監視、対処
完全性	アドバーサリ（悪意のある主体）	（特に人手のデータ入力が行われる場合）正規ユーザへのなりすましにより、不正確なデータが生成・取得される。	なりすまし	ユーザ、機器、サービス等に対する適切な水準の認証の実施(*) 入力値の検証
	アドバーサリ（悪意のある主体）	悪意のある従業員又は第三者の物理的な攪乱により、データ生成元の機器から正確でないデータが生成・取得される。	なりすまし	入力値の検証 機器等が設置された物理的環境の監視(*)
	アドバーサリ	正規の機器から生成・取	改ざん	暗号化等による通信経路の

	（悪意のある主体）	得されたデータがネットワーク上で傍受され、改ざんされる。		保護(*) データの完全性、真正性保護(*)
	構造上	品質や信頼性の低い IoT 機器がネットワーク接続され、故障や正確でないデータの送信、想定していない通信先へのデータ送信等が発生する。	システム等の不具合	運用時の機器・システムの真正性確認(*)
	偶発的	（特に人手のデータ入力が行われる場合） 正規ユーザの誤入力により、不正確なデータが生成・取得される。	誤使用	入力値の検証
可用性	アドバーサリ（悪意のある主体）	サービス妨害攻撃等によりデータの生成・取得に係る設備や機器が一時的に停止する。	サービス妨害	機器、通信機器、回線等の冗長化及びバックアップの確保(*) サービス妨害対策機能(*) 通信経路、端末の挙動等の監視、対処
	アドバーサリ（悪意のある主体）	センサー等の設備や機器がマルウェアに感染して稼働が停止し、データを生成・取得できない。	マルウェア感染	脆弱性対応プロセスの整備、実行(*) 端末、ネットワーク上におけるマルウェア対策の導入
	構造上	データの生成・取得に係る設備や機器に不具合が生じ、処理が一時的に停止する。	システム等の不具合	機器、通信機器、回線等の冗長化及びバックアップの確保(*)
	外部環境上	地震や津波等の自然災害によりデータの生成・取得に係る設備や機器に被害が生じ、処理が一時的に停止する。	自然災害等	機器、通信機器、回線等の冗長化及びバックアップの確保(*) 遠方拠点へのバックアップの確保
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）	悪意のある従業員又は退職者を含む第三者が、紙等で管理されている営業秘密を不正な方法（窃取、詐欺、強迫、その他の不正な手段）でデータ	情報漏えい	秘密管理性を確保した営業秘密等の管理 社内情報セキュリティルールの徹底

		として取得している。		
	偶発的	他社から転職者等を受け入れる場合、その転職者が持ち込むデータの中に、他社の営業秘密等が含まれる等、意図せぬ形で他社の営業秘密等を取得してしまう。	不十分なコンプライアンス	自組織及び委託先等における要員のセキュリティ確保 社内情報セキュリティルールの徹底

(*) NIST対応トラステッドコネクトサービスで対応

2-6-4-2. 今後のデータ管理の高度化に向けた課題の検討

本ユースケースを通じて、要件定義を行う顧客、社内の顧客担当セールス部門、システム設計・構築を実施する開発部門、更に構築に携わるビジネスパートナー様を含むステークホルダー間において、迅速・頻繁かつセキュアな情報共有を介してITシステムを構築する一連プロセスのアセスメントを実施し、組織内・組織間で安心・安全に情報共有、コラボレーションを実現する事が確認できた。今後は、産官連携のもと、本ユースケースを適用した業務実践を蓄積拡大してデータメネージメントフレームワークを普及していく事が、安全・迅速・経済的に重要情報の保護・共有を実現し、デジタルビジネスの拡大につながると考える。

3. 参画各社より頂戴した主なご意見

適用実証では、2章で紹介したユースケースの作成と並行して、適用に際して参画事業者が感じた所見や今後に向けた要望をヒアリングした。そこでいただいた主なご意見について、以下で示す。

- 適用した際に感じたメリット、適用して気付いた新たなリスク

サマリ	実際に寄せられたご意見
DMFは法律や契約、その他の制約に係るリスクの洗い出しや対策の抜け漏れ防止に有用	・ハードウェアやソフトウェアのコンポーネントといった物理／論理的なフレームから離れて、イベントといった機能で俯瞰できること、定性的な分析に役立っていると感じた。 ・法律、契約などの法的な観点から、対策を検討できた点は技術的な面に視点が行きがちであるため良いと感じました。 ・IT 部門と法的部門の意見が合わないことが多いところ、両方の視点を盛り込んだフレームワークとして、DM がよりどころになるとよい。 ・法律や契約、その他の制約が、どの範囲に関わるのか、それらの把握と、事業的に必要な大きな対策/対応の抜け漏れ防止に本DMFは有効と思われます（マクロ、事業視点）。 ・ 「場」と「属性」の関係を整理する表は、開示範囲、利用目的等の複数・全体の場（規制）の中での整合性を確認するのに有用。 ・ 場の規則がかけている“縛り”を見える化するため、属性に「利用制限」を追加した。属性の活用の際有益。これにより、特に、価値、起こりやすさを判断する指標が増え、STEP 4の優先順位付けのための精度が上がった。

- 適用の際の問題点/悩んだ点(他の文献とのハレーションを含む)

サマリ	実際に寄せられたご意見
セキュリティリスク分析の実施には、DMFで求める情報だけでは不足があり、別途実装レベルの情報を補った上でのアセスメントの実施が必要	・詳細なCIAリスクについては、実装レベルまで含めたリスクアセスメント（ミクロ、システム視点）が必要ではないかと考える（当社で通常実施）。 ・DMFによるマクロ的アプローチとミクロ的アプローチの併用が有効なのではないか、との認識を持った。 ・実際のデータ処理におけるリスクとしては物理的・論理的なシステムおよびインターフェイスの端点に脅威が生じるケースが多い。一方でDMFにおいてはこういった観点を考慮しないモデルとなっており、その意義やリスク検討における位置付けがクリアではないように思う。 ・実物理構成を加味しないモデルに抽象化しているため、セキュリティ観点については具体的なリスク・対策可否まで踏み込めない。DMF の有り様からすれば、「場」によるリスク・対策の言及にスコープを留めるべきではないかと思う。
CPSFにおける三層構造とのリンクが不明確	・DMF において謳われている「三層構造」における「層とその繋がり」は、DMF で検討する処理フローには明確に表現されないため、何故言及したのかが理解しづらい。実物理構成をリスク・対策分析で加味するならばそこで取り入れるべきだが、そういう検討ステップにはなっていないように思う。
法制度等に係るリスクの特定や対策の検討には、別途法令等の調査や知見の積み上げが必要	・サイバーセキュリティの観点に目が行きがちであるが、法律的なデータの取り扱いなどにも注意が必要であり対象となる法令を調べる必要があると感じた。 ・法的な観点で抽出するにあたり、適用するにあたり担当者がサイバーセキュリティや個人情報に関わる法律等の理解が必要なため、技術だけでなく法的事項の研賛が必要ではないかと感じた。
ケースによっては、データフローは多種多様でゼロからの整理には困難が伴う	・対象とするデータフロー整理について、既存の活動の中でステークホルダーの構成に基づき体系的にまとめられており困難はほぼ無かったが、実際のデータの流れを忠実にす

	べて起こすと発散する（流れが多種多様）。 ・“○○データ”とはどのような表現法がよいか悩んだ。データの種類は同じであるため、何の違いに注目すればよいのか？データ用途もしくはサービスか？
データの「価値」算定に利用者による恣意的な評価が入り込み得る	・データ属性における「価値」について、DMF における「価値の算定モデル(誰にとって、どのような指標で算定すべきか)」を策定しない場合、DMF 利用者による恣意的な評価となるのではないかと思う。検討開始時に「価値の算定モデル」を定義させるような手順にするのも一手かと思う。 ・属性の「価値」の高低の判断が難しい。損失時の経済的・セキュリティ上被害度とのことだが、主体者で価値が変わる認識。
カテゴリ等の抜け漏れない設定の判断が困難	・カテゴリなどをどのように設定・記述すれば漏れのない書出しが出来ていると言えるのか判断できない。マニュアルに基準や具体的指示があるべきではないかと思う。
リスク洗い出し結果の網羅性判断が困難	・リスクの洗い出しに関し、網羅性の観点から、どうすれば網羅したと言えるのかがわからない。

- DMF改訂に向けた要望

サマリ	実際に寄せられたご意見
チェックリスト等の作成	・法令からリスクを洗い出し対策を抽出したが、対策のチェックリストがあると対応がしやすい。開発時はサイバーセキュリティの技術的な観点で対応することが多いが、今回のように法的な観点を開発時に考慮するためにチェックリストがあると良い ・脅威例データベース、対策例データベースなどが整備されると、リスクおよび対策の致命的な抜け漏れ防止になり、本 DMF の有効性が高まるのではないかと思う。 ・リスク洗い出しの表作成の際、参考資料の例がもっとあると参考になる。
更なるユースケースの提供	・DMF 利用シーンのイメージが完全には把握出来ておらず、理想的な適用ユースケースを示して欲しい。 ・記載すべき事項のメッシュ感を知るために、ユースケースがたくさんあった方がイメージしやすい。
データフロー記法の改善	・UML 図の様に属性などもデータフローの中に表せると良い。
適用手順書の改定	・手順書の適用手順 (概要)には、対象とするデータ利活用プロセスの特定が無いが、適用手順 (詳細)にはあるので、手順の概要と詳細の項目を合わせるべき。 ・解説には、「リスクの洗い出し」を行った後の検討手順について、もう少し詳しい説明があると使いやすい。

以上