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５年２月８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事案及び制度動向

3. 本タスクフォースの検討事項

- **a. 今年度の取組み（DMFの適用実証等）**
- **b. 本タスクフォースの今後の進め方（案）**

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

- **7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(空調システム)の策定(2022.10)
- **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**
  - 防衛産業サイバーセキュリティ基準の改訂(2022.4)
- **自動車産業SWG**
  - ガイドライン2.0版を公表(2022.4)
- **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**
  - ガイドライン1.0を公開(2022.7)
- **工場SWG**
  - ガイドライン1.0を公開(2022.11)
- ・・・

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：
「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」を公開。

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を策定、SBOM活用促進に向けた実証事業（PoC）を実施。

『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。このIoT-SSFをわかりやすく理解するためのユースケースを新たに公開。

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

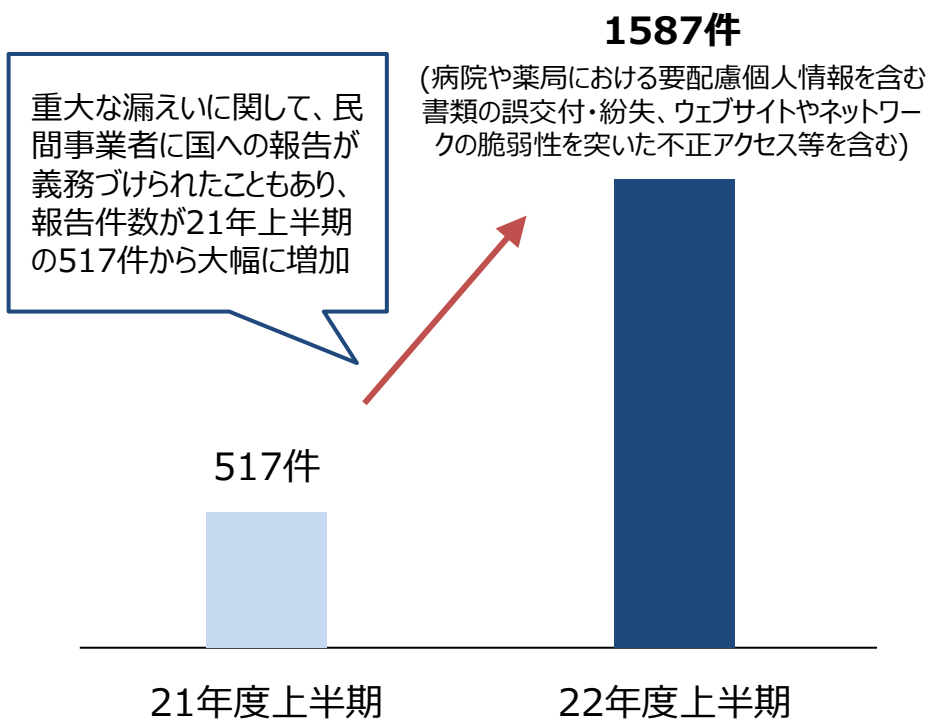
2. サイバー空間のつながりに関する事案及び制度動向

3. 本タスクフォースの検討事項
   a. 今年度の取組み（DMFの適用実証等）
   b. 本タスクフォースの今後の進め方（案）

2022年度上半期における個人データ漏えいの状況

- 個人情報保護委員会は、2022年4月から9月までの半年間に、民間事業者から直接、委員会に報告があった個人情報の漏えいの事案が1587件あり、前の年の同じ時期の517件の3倍以上だったことを公表した。

個人情報保護委員会へ直接報告された個人データの漏えい等事案の件数



左記を受けた個人情報保護委員会からの注意喚起事項

1. 病院・薬局における要配慮個人情報を含む個人データの漏えい等について

病歴などの要配慮個人情報は、特に慎重な取扱いが求められるものであり、「個人情報の保護に関する法律についてのガイドライン(通則編)」及び「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」を踏まえ、以下のような適切な安全管理措置を講ずることが必要。

- 業務プロセスやマニュアルの見直し
- 個人情報の取扱いに関する意識の涵養やマニュアルに基づく対応について、従業者への 研修等を通じて継続的に周知徹底する

2. ウェブサイトやネットワークの脆弱性を突いた不正アクセス等による個人データの漏えい等について

セキュリティパッチ適用による脆弱性への対処や不審なメール等を開封しないといった基本的な対応により、不正アクセス等を防止できるケースが多い。ついては、「個人情報保護法ガイドライン(通則編)」に定められている組織的・人的・技術的安全管理措置等を講ずることが必要。

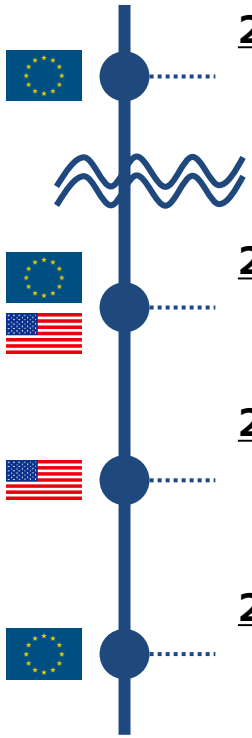
Europrivacy認証を欧州データ保護シールとして承認

- 2022年10月、欧州データ保護委員会（EDPB）は、「Europrivacy」を欧州一般データ保護規則 （GDPR）第42条（5）に基づく認証となる「欧州データ保護シール」として承認した。
- EuroprivacyはEU加盟国で正式に承認され、訴訟時にデータ保護監視当局により考慮される。

「EU米国データ・プライバシー枠組み」の十分性を認める決定案の発表

- 欧州委員会は2022年12月、一般データ保護規則（GDPR）に基づき、「EU米国データ・プライバシー枠組み（DPF）」の十分性を認定する決定案を発表するとともに、決定案の正式な採択に向けた手続きを開始したと発表した。DPFの十分性認定が採択されれば、追加的な保護措置をとることなく、EU域内から米国のDPF参加企業への個人データの移転が認められることになる。

EU米国間の枠組みに向けた検討状況



2020年7月
EU司法裁判所による「プライバシー・シールド」無効判決 (シュレムスII判決)

2022年3月
EU米国データ・プライバシー枠組み(DPF)の原則合意

2022年10月
DPFの実施に関する大統領令に署名
(Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities)

2022年12月
欧州委、DPFのGDPR上の十分性を認める決定案を発表

欧州委員会は今後、欧州データ保護会議(EDPB)による意見、加盟国代表者からなる委員会の承認と、欧州議会による審査を受け、決定を採択する。

十分性認定に係る決定案の概要

欧州委員会は、以下の点などを挙げ、DPFはEUの個人データ保護と同等の保護を提供していると結論づけている。

プライバシー原則を遵守する事業者の認定

- 米国企業は、Annex I にて規定されたプライバシー原則(個人情報が目的に必要でなくなった場合に削除すること、個人情報を第三者と共有する場合には保護の継続性を確保すること等を含む) を遵守しDPFに参加する

EU市民向け救済措置の整備

- EU市民は、DPFに違反した個人データ取扱いがなされた場合、独立した紛争解決機構や仲裁パネルでの無料での救済等、複数の救済手段を利用することが可能である

米国大統領令による対策の実施

- 米国大統領令によって導入された新しい規則等により、米国の情報機関による欧州のデータへのアクセスは、国家安全保障を守るために必要かつ適切な範囲に限定される。

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事案及び制度動向

3. 本タスクフォースの検討事項

   a. 今年度の取組み（DMFの適用実証等）

   b. 本タスクフォースの今後の進め方（案）

DMF適用実証の実施概況

- 参考となる事例の蓄積によるDMFの活用促進、DMFの改善点の洗い出しを目的として、参画事業者からの協力をいただきつつ、6件の適用実証を実施した。

No.	参画事業者	適用対象の名称
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	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
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
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
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
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での情報共有

適用実証の成果物（想定）

① ユースケース

② DMF改善のためのデータ

- 適用した際に感じたメリット/デメリット、適用して気づいた新たなリスク、適用の際の問題点/悩んだ点
- DMF改訂に向けた要望

デンソー 車両データ活用基盤の利用

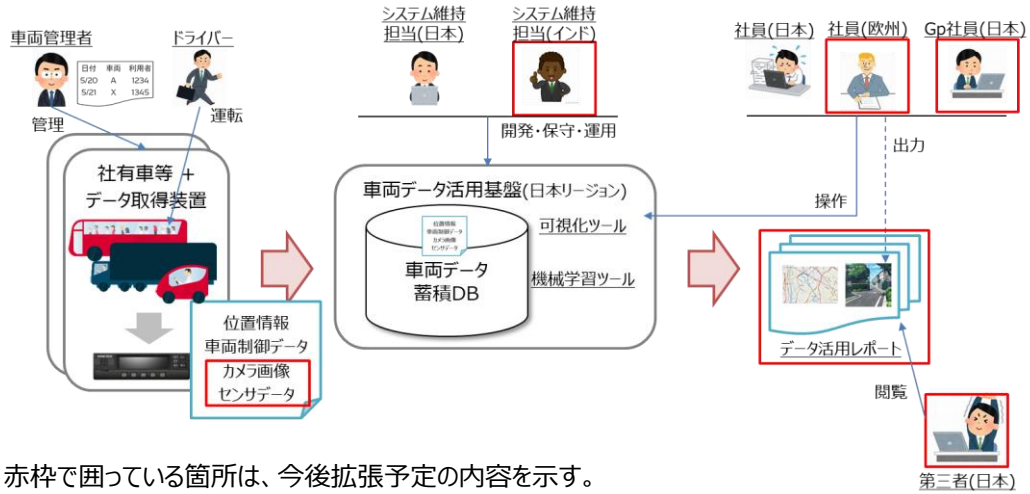
名称 (協力事業者)

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（デンソー）

適用対象の概要

- 本適用実証では、デンソーが自社の製品開発・改善を目的として構築・運用している車両データ活用基盤を扱う。
- 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車両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。
- 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。

車両データ活用基盤の概要



※ 赤枠で囲っている箇所は、今後拡張予定の内容を示す。

DMF適用の狙い

DMFは、複数の組織間で取扱うデータに対するリスクを特定し、対策の認識を合わせる際に有用なツールと理解しており、これまでに実施したリスクアセスメント等で洗い出せていなかったリスクの発見や、今後のサービス拡張等において想定されるリスクや対策等の洗い出しに使えるのではないかと考えている。

適用結果への所見

適用を通じて、今後のサービス拡張等において想定されるリスクや対策等の特定に向けた検討を進めることができた。

一方で、DMFは脅威が顕在化しやすい物理的・論理的なシステムおよびインターフェイスの端点といった観点を必ずしも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の明確化が課題と考えられる。

デンソー 車両データ活用基盤の利用

- 車両データ活用基盤を対象に、DMFの適用プロセスに沿ってデータフローを可視化し、必要な制度的な保護措置(「場」)や「属性」の明確化を図った。

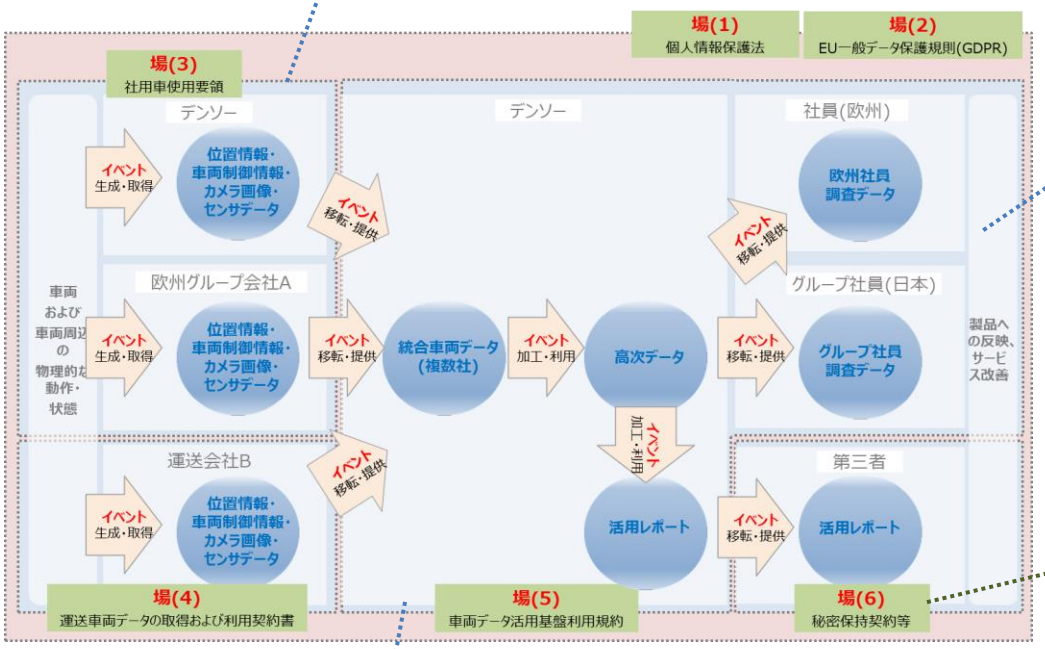
STEP 1
データ処理フローの可視化

STEP 2
必要な制度的な保護措置(「場」)の整理

STEP 3
「属性」の具体化

STEP 4
「イベント」ごとのリスクの洗い出し

STEP 1-1
- デンソー及び国内・欧州のグループ会社、運送会社の社用車に設置したデータ取得装置から「位置情報、車両制御情報、カメラ映像、センサデータ」を生成・取得し、デンソーが供用する車両データ活用基盤（日本所在）へと移転・提供する。



STEP 1-2
- デンソー及びグループ会社社員は、車両データ活用基盤の「統合車両データ」を加工・利用し、高次データ（例：走行経路、操作挙動、走行画像）を生成する。

STEP 1-3
- 「高次データ」は、提供先の要求に応じて移転・提供され、「調査データ」に加工される。
- 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。

STEP 2
- 本ケースでは、以下に示す6つのルールを「場」として特定した。
  - 個人情報保護法
  - 一般データ保護規則
  - 社用車使用要領
  - 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利用規約
  - 秘密保持契約等

デンソー 車両データ活用基盤の利用

- STEP 4「イベント」ごとのリスクの洗い出しの実施を通じて、イベントごとに想定されるリスクとともに、以下を例とする推奨施策を特定した。

想定リスク(例)	推奨施策(例)
ドライブレコーダのカメラ画像への歩行者等の映り込みにより生じ得るプライバシーリスク	• 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。
システム維持の外部委託により生じ得る意図しない個人データの国外移転	• 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。
データ利用目的の不整合の発生	• 「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。

竹中工務店 IoT等を活用した次世代建物制御システム

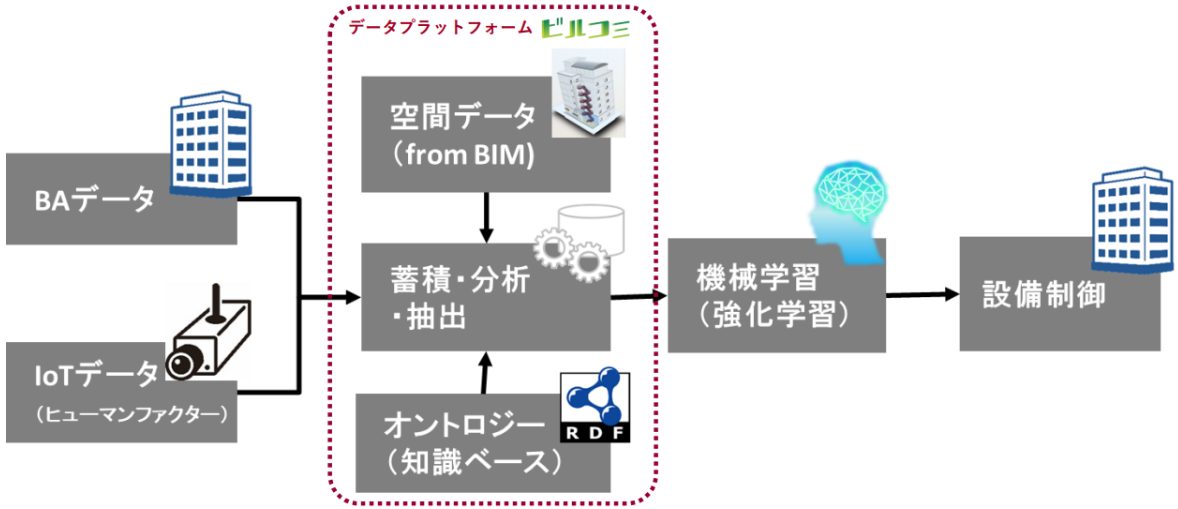
名称（協力事業者）

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（竹中工務店）

適用対象の概要

- 本適用実証では、人材不足等を踏まえた建物管理業務の高度化を目的とした、ヒューマンファクター（活動量、着衣量、人流・属性など）を収集・抽出するIoTと建物設備専用AI技術を用いた次世代の建物設備システムを扱う。
- 各ビルから収集される設備の稼働データ等（BAデータ）やIoTデータをデータプラットフォームに集約・蓄積し、一定の加工等を行ったうえで、建物管理者の経験やノウハウに基づく設備制御を学習し実施する人工知能を用いた管理を行う。
- システム全体の最適化を図ることで、空調・照明の省エネと快適性の両立を実現する。

次世代建物設備システムの概要



DMF適用の狙い

SoS（System of Systems）の社会では、関係する各主体のデータ取扱に係る責任やリスクが明確になっていなければならないと考えているが、DMFの適用によってこれらが明確になる可能性がある点に期待がある。

適用結果への所見

リスク分析にあたっては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／論理的なフレームに視点が行きがちなところ、法律、契約などの法的な観点を含めて変換といった機能で俯瞰できることが、定性的な分析に役立っていると感じた。

竹中工務店 IoT等を活用した次世代建物制御システム

- 次世代建物制御システムを対象に、DMFの適用プロセスに沿ってデータフローを可視化し、必要な制度的な保護措置(「場」)や「属性」の明確化を図った。

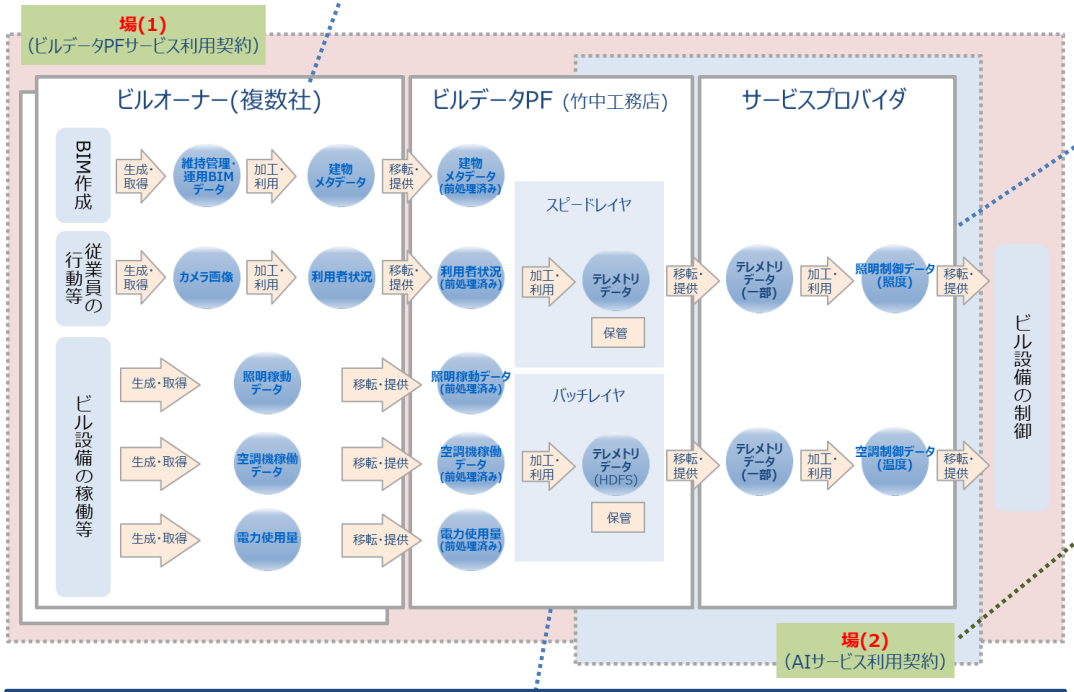
STEP 1
データ処理フローの可視化

STEP 2
必要な制度的な保護措置(「場」)の整理

STEP 3
「属性」の具体化

STEP 4
「イベント」ごとのリスクの洗い出し

STEP 1-1
- ビル内の電力量計や空調機、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。
- 撮影したカメラ画像にエッジ処理を加え、人の位置、エリア内の人数、着衣量へと加工し、ビルデータPFに送信する。



STEP 1-2
- PF上に共有した「BAデータ」及び「利用者状況」に対してビルコミ上で前処理を行い、BIM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。

STEP 1-3
- ビルデータPFのデータのうち必要な範囲を抽出し、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される。

STEP 2
- 本サービスでは、ビルオーナー各社と竹中工務店、竹中工務店とサービスプロバイダとの間で締結される2つの契約が「場」として特定された。
  - ビルデータPFサービス利用契約
  - AIサービス利用契約

竹中工務店 IoT等を活用した次世代建物制御システム

- STEP 4「イベント」ごとのリスクの洗い出しの実施を通じて、イベントごとに想定されるリスクとともに、以下を例とする推奨施策を特定した。

想定リスク(例)	推奨施策
データ生成・取得を行うビル設備機器等へのセキュリティ侵害	• データ生成・取得段階の信頼性を確保するため、ビルオーナーが管理するBAシステム、ネットワークカメラシステムにおける以下を含む基礎的なセキュリティ対策の実装を確認する。 – 動作するサービスの最小化 – 接続元の IP アドレス等による制限 – 利用者・管理者の識別・認証 – 発覚した脆弱性の評価及び対処 – 管理者に覚えのない認証成功等の検知、確認 – ビル内外の通信の暗号化(HTTPS等)
ビルオーナと合意した利用条件(利用目的、利用権限等)とは異なる方法や目的によるデータ利用	• 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。 • 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(サービス開発等)で用いる場合、以下の事項に留意する。 – 既存の契約でそれらの用途が含まれていない場合には、利用目的の変更等を行う。 – 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。 – 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、元のオーナーを特定しないよう抽象化したうえで、当該処理が契約で許容される利用目的に含まれるかを確認する。
サービスプロバイダが有する派生データの利用権限が十分に定められていないことによる不整合の発生	• 外部の強化学習エンジンを利用する場合、当該サービスへの入力データ(テレメトリデータ)及びAI生成物(派生データ)の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。 – 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。 – 強化学習モデルから出力された制御データ(派生データ)の取扱いについても、AIサービス利用契約にて、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を取り決める。

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

名称（協力事業者）

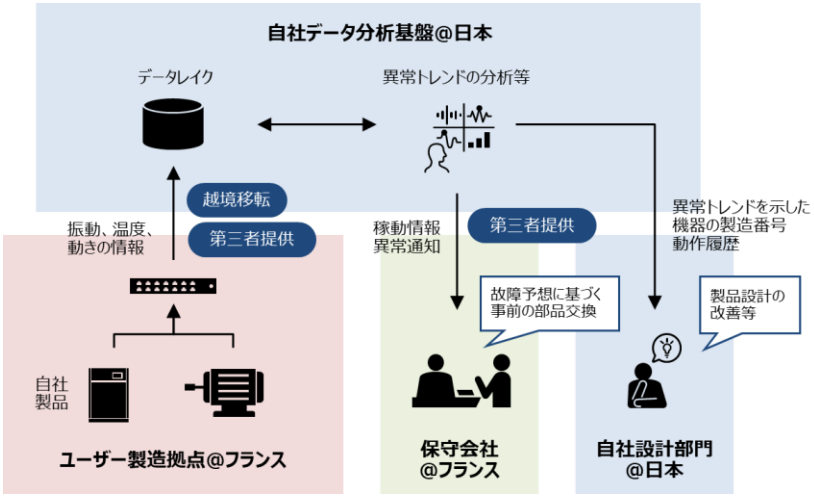
製造装置の稼働データ等を活用した予防保全・製品向上（三菱電機）

適用対象の概要

- 昨今の製造業では、デジタル化を通じて、製品開発プロセスの高度化とリードタイム短縮の両立等のエンジニアリングチェーン強化を進めることが必要とされている*。
- 本適用実証では、データ利活用によるエンジニアリングチェーン強化の一例として、製造装置の稼働データ等を活用した予防保全・製品向上を扱う。
- 日本の製造機器メーカがフランス（EU構成国の一例）のユーザ企業の工場にシステムインテグレータ経由で機器を納入し、運用後も機器に装着したセンサから装置の稼働データを収集・分析し、予防保全及び設計の改善に活用するというケースを想定する。

*経済産業省 製造産業局 “製造業 DX レポート ～エンジニアリングのニュー・ノーマル～”

稼働データ等を活用した予防保全・製品向上の概要



DMF適用の狙い

デジタル化の取組みを進めようとする際、システム仕様やそれに必要な技術に関する検討と比較して、達成すべきビジネス上の価値やそれに必要なデータの種類、その取扱い方法に関する検討は相対的に重きを置かれていない状況があり、DMFの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点に本適用実証の狙いがある。

適用結果への所見

DMFの適用を通じて、外国を含めて顕在化しつつある制度の状況を可視化し、そこで今後何をすればよいかが明確となった点で有益だった。それらは今後のビジネスを考えるうえで必要と認識している。

一方で、現状のDMFの内容は抽象度が高く、現場に課題を真に感じてもらうには、分野を絞った具体的な試みが必要と考える。

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

- 製造装置の稼働データ等を活用した予防保全・製品向上というケースを対象に、適用プロセスに沿ってデータフローを可視化し、必要な制度的な保護措置(「場」)や「属性」の明確化を図った。

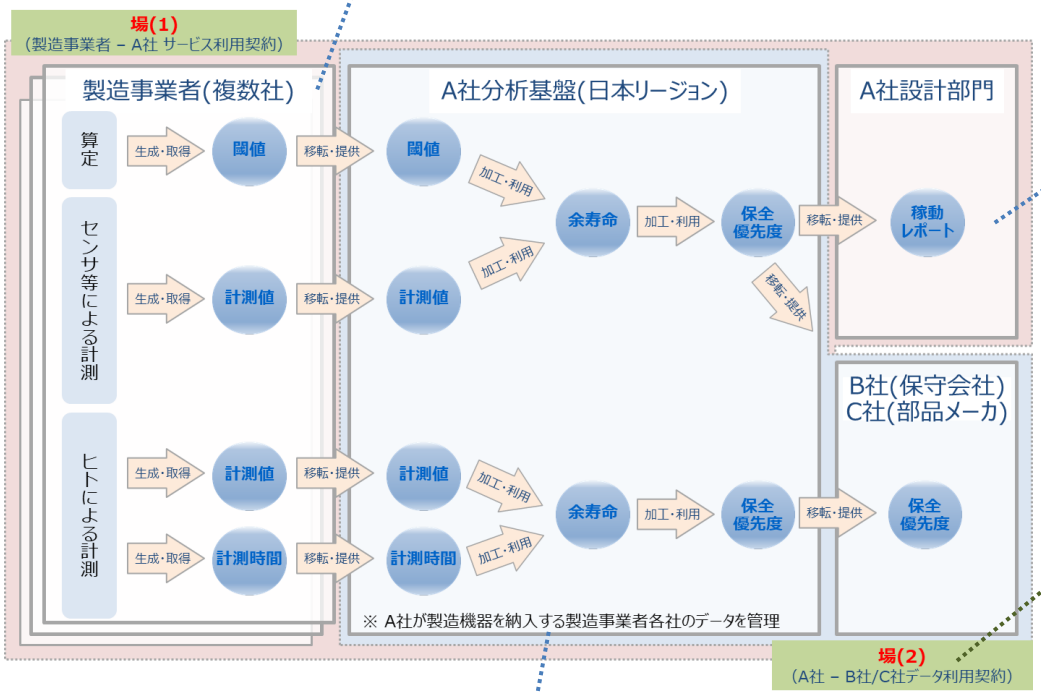
STEP 1
データ処理フローの可視化

STEP 2
必要な制度的な保護措置(「場」)の整理

STEP 3
「属性」の具体化

STEP 4
「イベント」ごとのリスクの洗い出し

STEP 1-1
- 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。



STEP 1-2
- 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。

STEP 1-3
- 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。

STEP 2
- 本ケースでは、以下2つの契約が「場」として特定された。
  - 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」
  - A社とB社・C社との「A社–B社/C社データ利用契約」

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

- STEP 4「イベント」ごとのリスクの洗い出しの実施を通じて、イベントごとに想定されるリスクとともに、以下を例とする推奨施策を特定した。

想定リスク（例）	推奨施策（例）
契約上の利用目的と利用実態との乖離	• 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、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。 – 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。
委託先・取引先である保守会社や部品サプライヤからのデータ漏えい・改ざん	• 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。
データの越境移転に係る法令遵守の不備	• 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。

シップデータセンター IoS-OPによる船舶運航データの流通

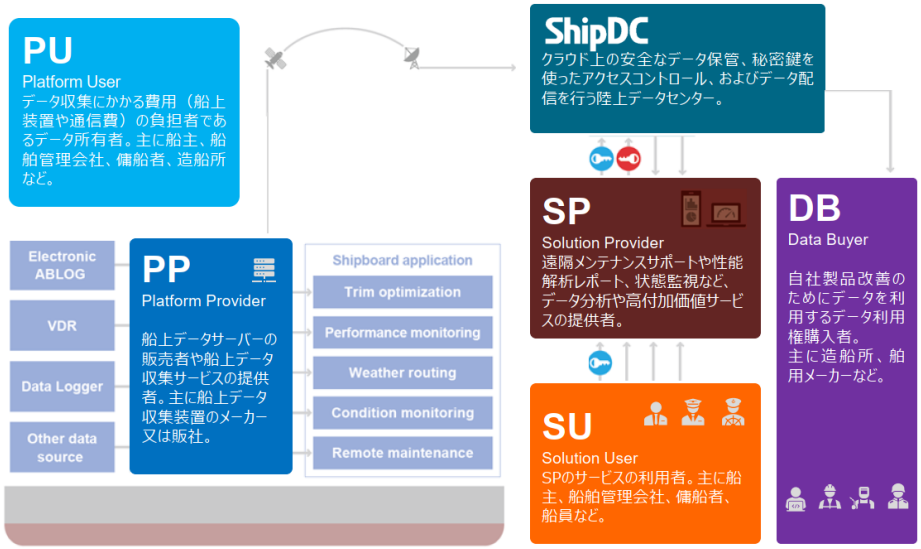
名称（協力事業者）

IoS-OP（Internet of Ships Open Platform）による船舶運航データの流通（シップデータセンター）

適用対象の概要

- IoS-OPは船舶の運航データを、データ提供者の利益を損なわずに、ステークホルダー間での共有や、造船所やメーカー等への利用権販売、各種サービスへの提供を可能とすべく、海事業界内で合意されたルールと、データセンターで構成された共通基盤である。
- 船主等のPU（Platform User）が船上データ収集装置により収集したデータを船上サーバ等に蓄積し、項目の標準化等を行ったうえで海事業界内で合意されたルールと、データセンターで構成された共通基盤（ShipDC）に共有される。
- かかるデータは、遠隔メンテナンスサポートや性能解析レポート、状態監視等のサービスを提供するSP（Solution Provider）に提供され、船主、船舶管理会社等のSU（Solution User）に向けたサービスに利用される。

IoS-OPの概要とステークホルダー



DMF適用の狙い

DMFのポイントである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たい。

適用結果への所見

今回特定した重要リスク及び必要な措置の検討結果を基に、IoS-OPの外側で個別に行われている船主と船上機器メーカー間の契約等についても、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。

[参考] IoS-OP (Internet of Ships Open Platform) 秩序あるデータ収集・流通・活用を実現するオープンプラットフォーム (https://www.shipdatacenter.com/)

シップデータセンター IoS-OPによる船舶運航データの流通

- IoS-OPによる船舶運航データの流通を対象に、DMFの適用プロセスに沿ってデータフローを可視化し、必要な制度的な保護措置(「場」)や「属性」の明確化を図った。

STEP 1
データ処理フローの可視化

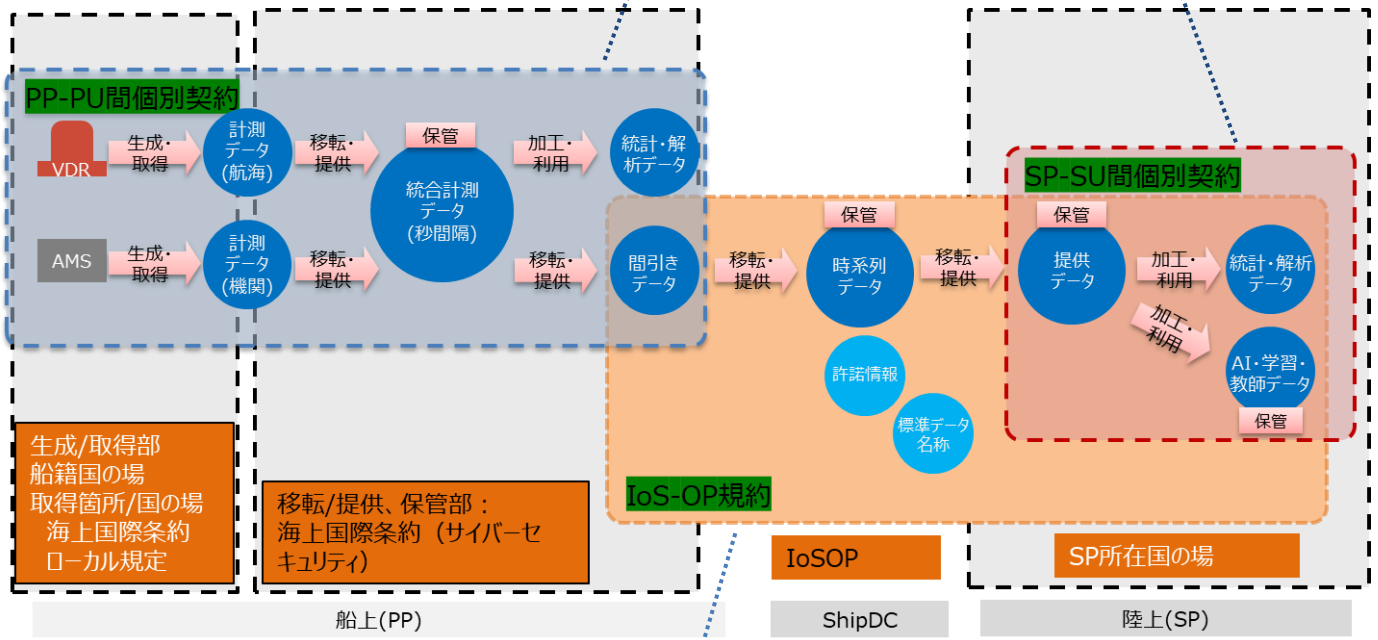
STEP 2
必要な制度的な保護措置(「場」)の整理

STEP 3
「属性」の具体化

STEP 4
「イベント」ごとのリスクの洗い出し

STEP 1-1
- 船上に設置された機器から「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。

STEP 1-3
- 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。



STEP 1-2
- 船上に保管された「統合計測データ（秒間隔）」のうち、「間引きデータ」が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。
- 当該データはSPに「移転・提供」される。

STEP 2
データの取扱いに係る6つの「場」を特定した。
- 海上国際条約、船籍国/地域規制
- 不正競争防止法
- IoS-OP利用規約 等

シップデータセンター IoS-OPによる船舶運航データの流通

- STEP 4「イベント」ごとのリスクの洗い出しの実施を通じて、イベントごとに想定されるリスクとともに、以下を例とする推奨施策を特定した。
- また、それらのリスクへの対処を既存の規定類等にて既に実行していることを確認した。

想定リスク(例)	推奨施策
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	• データの移転等への現地データ越境移転規制の適用確認 • 適用対象となる可能性がある場合の規制内容、執行状況等への留意
悪意のある従業員が、本船固有情報や営業秘密を第三者に移転・提供する	• 秘密管理性の確保、ID、パスワード等による電磁的管理性の確保等 • PU-PPサービス契約における、セキュリティ要件の定め、セキュリティ要件遵守の履行確保 • IoS-OP利用規約におけるセキュリティガイドラインの遵守、利用・管理状況についての報告、監査実施
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	• IoS-OP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制限 • IoS-OP利用規約における、セキュリティガイドラインの遵守、利用・管理状況についての報告、監査実施

パナソニック ワークプレイス向けソリューション

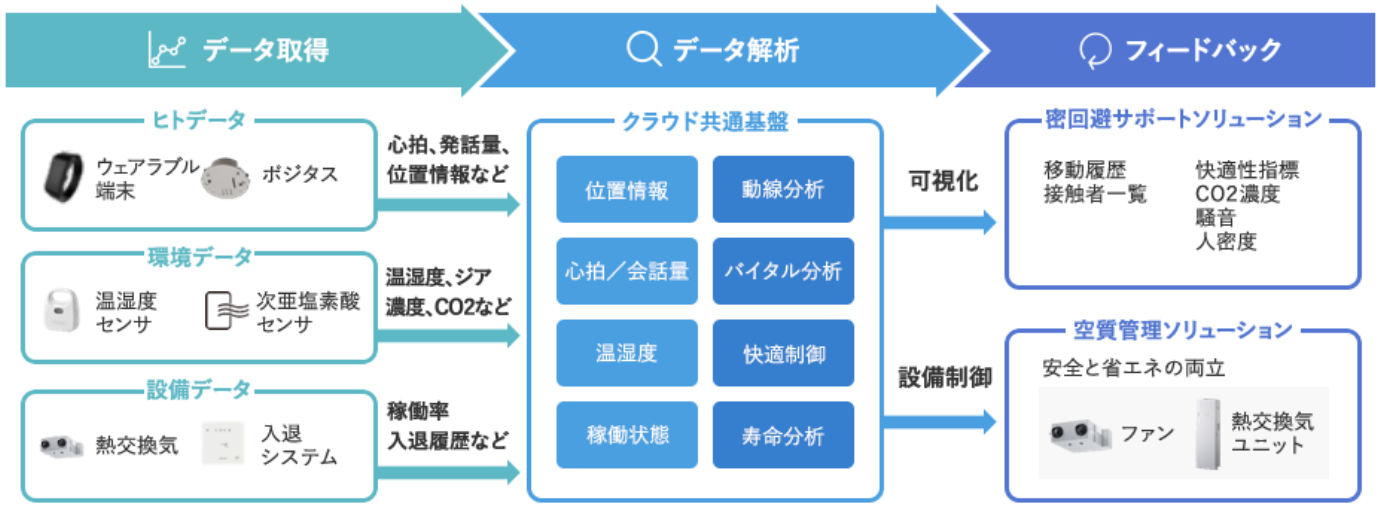
名称 (協力事業者)

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（パナソニック）

適用対象の概要

- パナソニックでは、従来のようにスペースの効率性だけを追求するのではなく、多様な働き方に応じて、働きやすさと生産性の高さを両立させるこれからの時代のワークプレイスを提案している。
- 具体的には、各種機器よりヒト・環境・設備データを取得し、クラウド共通基盤にて分析を行い、可視化や設備制御を通じてワークプレイス空間にフィードバックすることで、空間価値の向上を継続化し、お客様の事業の成長を支援する。

ワークプレイス向けソリューションにおけるデータ利活用の概要



DMF適用の狙い

社内では上記ソリューションに対して既に脅威分析やシステム脆弱性診断などを行っているが、DMFの適用を通じて従来の方法とは異なる観点からリスク分析を行うことに意義があると考えている。

適用結果への所見

法律や契約、その他の制約が関わる範囲の把握と、事業的に必要なマクロな対策/対応の抜け漏れ防止に本DMFは有効。

本適用実証後も、このような適用を適時に行い、アセスメントの精度を上げていくことが必要と考える。

[参考] パナソニックの空間ソリューション - ワークプレイス向けソリューションとは (https://www2.panasonic.biz/jp/solution/office/strengths/)

パナソニック ワークプレイス向けソリューション

- ワークプレイス向けソリューションを対象に、DMFの適用プロセスに沿ってデータフローを可視化し、必要な制度的な保護措置(「場」)や「属性」の明確化を図った。

STEP 1
データ処理フローの可視化

STEP 2
必要な制度的な保護措置(「場」)の整理

STEP 3
「属性」の具体化

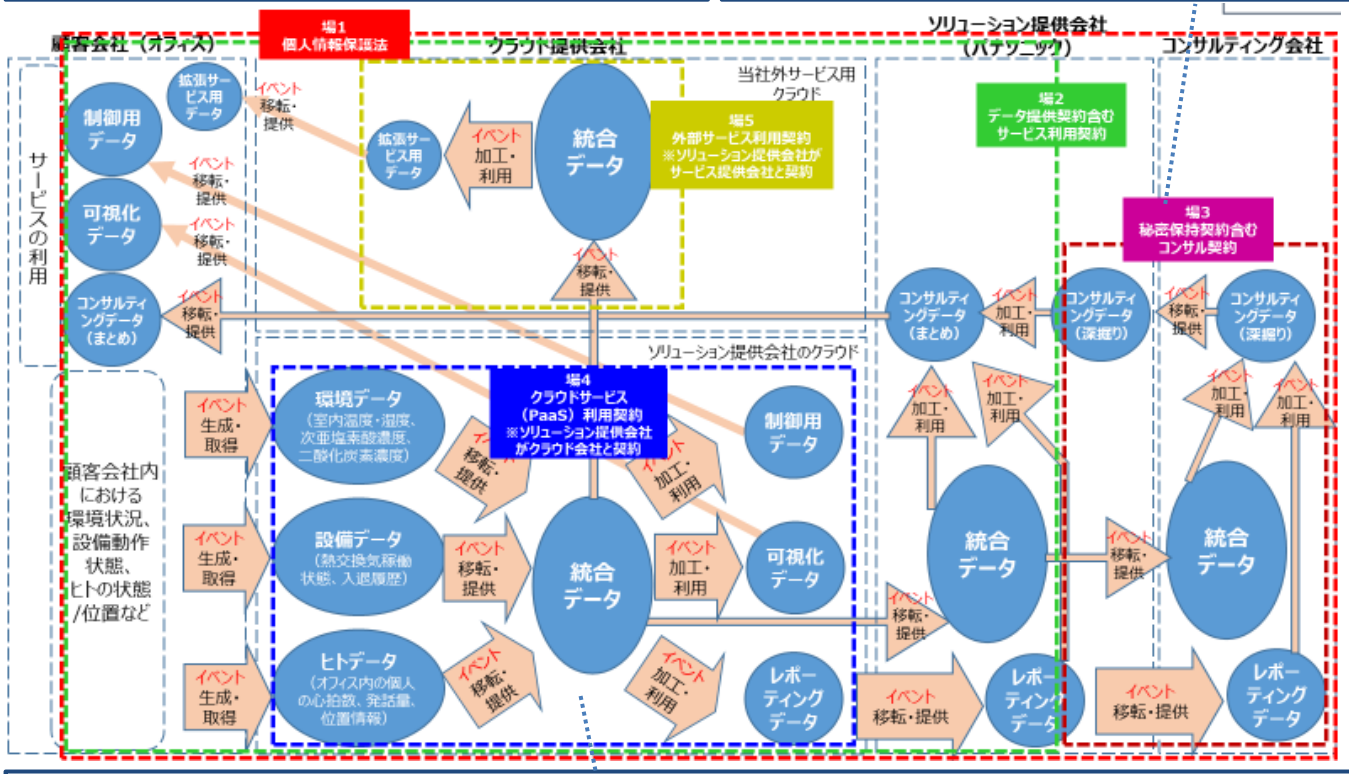
STEP 4
「イベント」ごとのリスクの洗い出し

STEP 1-1

- 顧客会社（オフィス）に設置したセンサやビル設備等から、「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。

STEP 1-3

- 「統合データ」は設備制御や可視化のほか、レポート作成のため、高度な分析が必要な場合はコンサルティング会社の協力を得たうえで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。



STEP 2

パナソニックと顧客及びビジネスパートナーと締結する5つのルールを「場」として特定。

- 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

STEP 1-2

- パナソニックのクラウドでは、各種データを纏めた「統合データ」から、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」が加工・利用され、顧客企業に移転・提供される。

パナソニック ワークプレイス向けソリューション

- STEP 4「イベント」ごとのリスクの洗い出しの実施を通じて、イベントごとに想定されるリスクとともに、以下を例とする推奨施策を特定した。

想定リスク(例)	推奨施策
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、それにつながる設定ミス	• ユーザー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）
外部クラウドサーバの停止や通信トラブル等によるサービス提供の遅延等	• 縮退動作の確保（エッジコンピューティングによる）
内外の関係者による収集データの目的外利用	• 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
自社従業員または委託先への監督不備に起因するデータ漏えい等	• 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）
クラウド提供会社都合によるサービス終了・契約解除	• 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）。

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での情報共有

名称 (協力事業者)

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での情報共有（富士通）

適用対象の概要

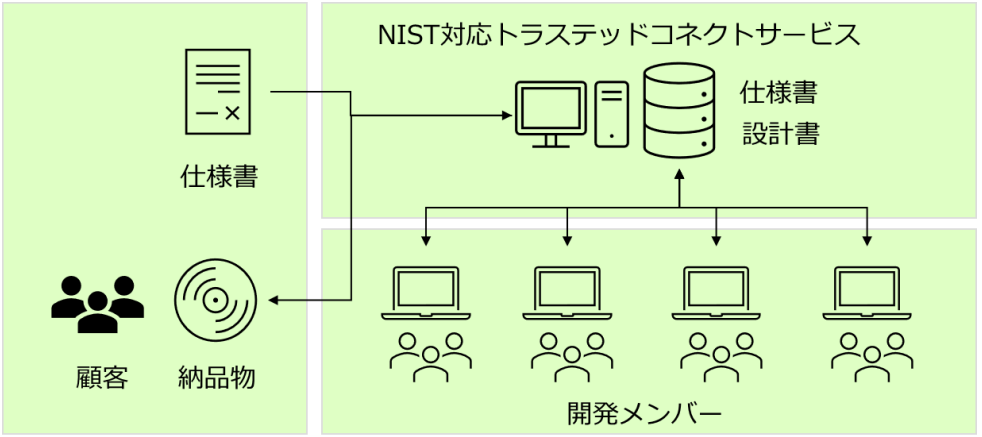
- ネットワークインフラシステムの概要

  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、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関係者間で情報共有を行いながら実施する。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。

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での情報共有の概要



DMF適用の狙い

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。

適用結果への所見

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。

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での情報共有

- DMFの適用プロセスに沿ってデータフローを可視化し、必要な制度的な保護措置(「場」)や「属性」の明確化を図った。

STEP 1
データ処理フローの可視化

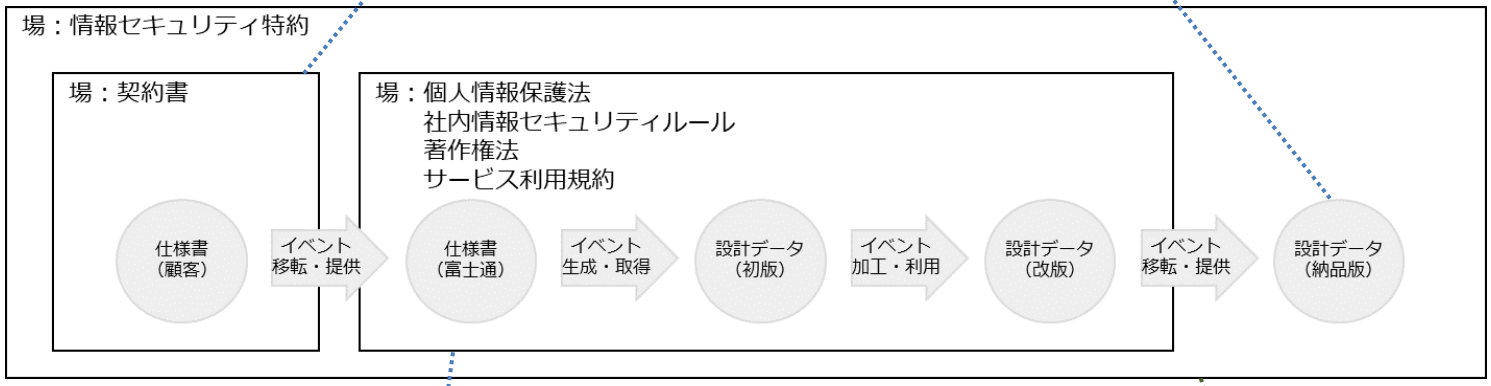
STEP 2
必要な制度的な保護措置(「場」)の整理

STEP 3
「属性」の具体化

STEP 4
「イベント」ごとのリスクの洗い出し

STEP 1-1
- 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。

STEP 1-3
- 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。



STEP 1-2
- 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。

STEP 2
- 本ケースでは、以下に示す6つのルールを「場」として特定した。
  - 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

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での情報共有

- STEP 4「イベント」ごとのリスクの洗い出しの実施を通じて、イベントごとに想定されるリスクとともに、以下を例とする推奨施策を特定した。

脅威主体の区分	想定リスク(例)	推奨施策(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又は外部の攻撃者に傍受され、漏えいする。	• 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
【機密性】 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。	• 機器・サービスの初期設定及び設定等の変更管理(*) • ユーザー、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
【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。	• 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

(*) NIST対応トラステッドコネクトサービスで対応

参画各社より頂戴した主なご意見

- 適用実証を進める過程で、各社から以下に示すようなDMF改善のためのデータをいただいており、今後の検討に向けたインプットとして活用することを想定。

■ 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、STEP4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

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ます（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、との認識を持ちました。 • 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。

参画各社より頂戴した主なご意見

- 適用実証を進める過程で、各社から以下に示すようなDMF改善のためのデータをいただいており、今後の検討に向けたインプットとして活用することを想定。

■ 適用の際の問題点/悩んだ点 (続き)

サマリ	実際に寄せられたご意見
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鑽が必要ではと感じた。
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、主体者で価値がかわる。
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。

参画各社より頂戴した主なご意見

- 適用実証を進める過程で、各社から以下に示すようなDMF改善のためのデータをいただいており、今後の検討に向けたインプットとして活用することを想定。

■ 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、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います。 • 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と感じた。
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だと思います。 • 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。

適用結果のとりまとめ方法等

- 今年度の適用実証の成果は、DMFの改訂を含む今後の検討の材料とすることに加え、DMFのさらなる普及・啓発を図るため、事例集等の形で公表したい。
- DMF改善のためのデータについては、DMF改訂を含む今後の検討への活用を見込む。

適用結果のとりまとめ・活用

1. ルール・標準化

- より実務に即したDMFへの改訂
- より具体的なルールの策定・検討 等

2. 国際連携

- 「データの越境移転に関する研究会」における検討 等

3. 適用・応用

- DMFのさらなる普及・促進
- 優れたデータマネジメント施策等の発信 等

1. 「DMFに基づく適切なデータマネジメント実践に向けた事例集」(仮)の公開
2. DMF改訂を含む今後の検討への活用*

＊ 今回の適用実証の結果及び、机上でのDMFの有効性検証の結果等を踏まえて課題の具体化を行う予定。

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

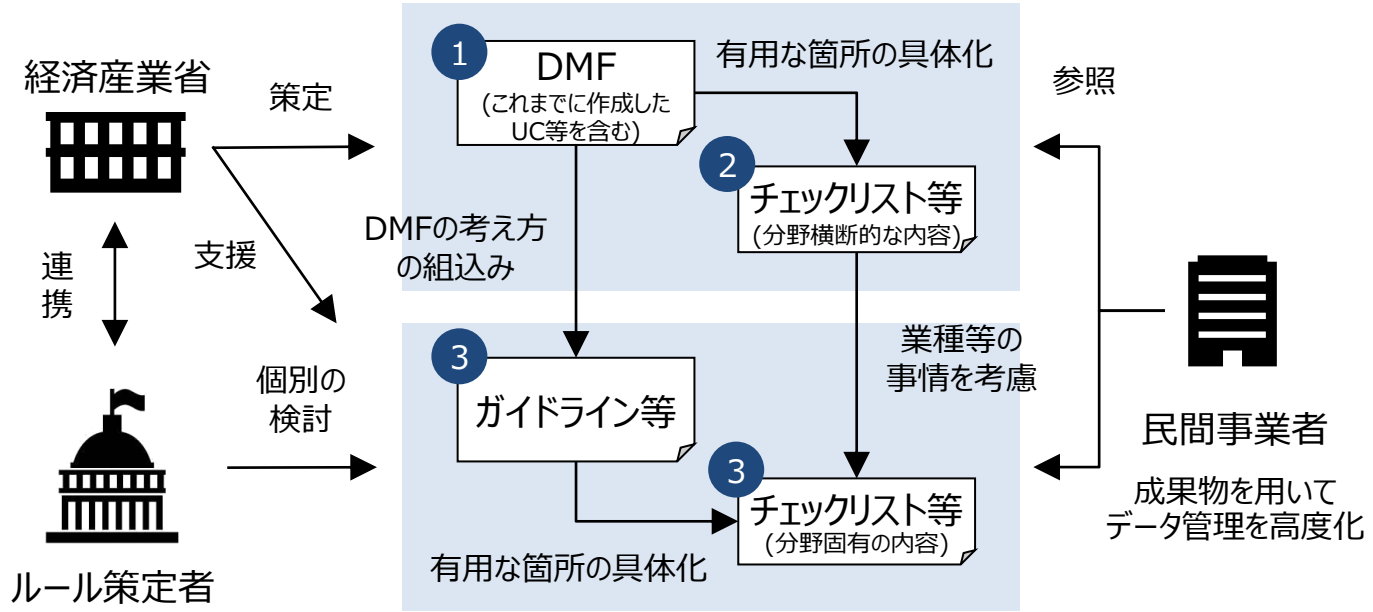
2. サイバー空間のつながりに対する攻撃事案

3. 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

4. 本タスクフォースの検討事項
   a. 今年度の取組み（DMFの適用実証等）
   b. 本タスクフォースの今後の進め方（案）

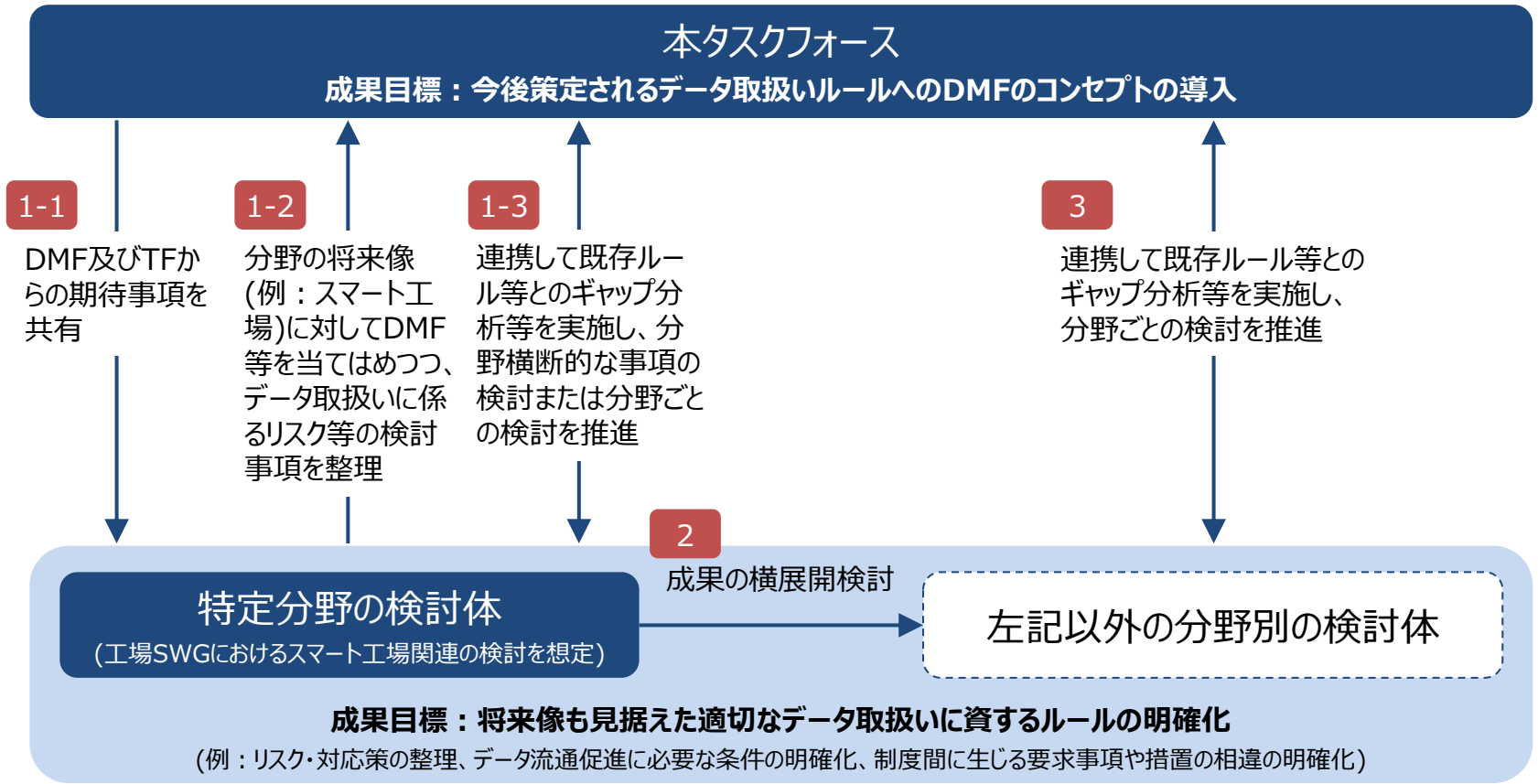
DMFに係る活動の今後の進め方に関する基本的な考え方

- 第3層TF関連の検討の今後の進め方・目標として、以下のような全体像を想定。

目的	• 信頼ある企業間データ流通・利活用の促進 – 特に、企業内または企業間でデータの利活用を実施する際に想定されるリスクをサービスの企画・構想段階から特定し、運用段階、サービス終了に至るまで継続的に対処することに資する枠組みの確立 – その際特定・対処するリスクとしては、サイバーセキュリティに係るものには限定せず、データ取扱いに係る法制度・契約等に関連するものも含めて対象とすることを想定
DMFの利用イメージ (あるべき姿)	
実施事項 (例)	1. 適用実証にて頂戴したご意見等を踏まえたDMFのさらなる改善 2. 分野横断的に適用可能なより具体的な成果の作成とその普及啓発 3. 他のルール策定者等と連携した分野等を絞った具体的成果の作成

ルール策定者との連携の流れ(案)

- 今後の成果目標としては、将来像も見据えたより具体的なデータ取扱いルールの策定にDMFのコンセプトを入れ込んでいくことを想定。
- 連携先との検討として、まずはスマート工場等に分野をある程度絞って他の分野からも参考にできるケースをつくり、他の領域にも成果を横展開していく。



第3層TF側からルール策定者へ提示する期待事項（例）

- 他の策定者により検討されるデータ信頼性確保に資するルール(リスク・対応策の整理、データ流通促進に必要な条件の明確化、データ管理に関わる制度間に生じる要求事項や措置の相違(ギャップ)の明確化)に対して、第3層TFから考慮を期待するDMFのエッセンスには以下が挙げられるのではないか。

■ ルール策定者への期待事項(例)

1. 組織や部署等の境界を越えて、データの生成・取得から廃棄に至るまでのライフサイクル全体に着目すること
2. データを取扱う物理的・論理的な機器・システムだけでなく、そこで取扱われる基本的にすべてのデータとその属性(特に、当該データの利用条件に係るもの等)にも着目すること
3. データのライフサイクル全般にわたって具体的な対応等を検討する際、リスクベースでの対応を志向すること
4. サイバーセキュリティで通常考慮される観点に加え、データを取扱う上で考慮が必要な法律・契約等の観点も含めた包括的なリスク特定・対応を行うこと
5. データの取扱い条件や措置の特定や比較を通じて、異なる国家間、組織間、またはシステム間でデータ管理に関するルール等の間の調整を図ること
6. セキュリティの専門家だけでなく、データの取扱いに係る事業の実務家、法律・契約の専門家等を含めた横断的チームを組成し、検討を推進すること

ご議論いただきたい事項

1 適用実証の結果等を踏まえ、第3層TFとしてさらに検討を深めるべき事項について

- 民間事業者のデータ管理の高度化に資する成果として、どのようなものがより具体的に望まれるか。

  ＜より具体的な成果の例＞

  ー　イベント類型ごとに必要な対処等に関するガイダンス文書やチェックリスト

  ー　データマネジメント実施を支援する機能・ツール等

- 上記成果を民間事業者に展開する際、より効果的・効率的な普及方法としてどのようなものが想定されるか。（例：業界団体との連携方針等）

2 第3層TF外の連携先・連携方針の妥当性について

- 産業サイバーセキュリティ研究会WG1にて既に分野別SWGを設置している分野以外で、優先して連携すべき業種、検討体等はあるか。

  ＜過去の検討会等でご意見をいただいた対象等＞

  ー　地方自治体

  ー　CPSFやDMFの動向等を必ずしも認知していない民間事業者（スタートアップ事業者等を含む）

- 当該連携先との間で検討すべき事項として何があるか。その際、ベンチマークとすべき国内または外国の取組みとしてどのようなものがあるか。

- 連携の中で作成すべき分野別/分野横断的な成果物としてどのようなものが望ましいか。