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４年１０月３１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. 今年度事業の方針
   b. DMFの適用実証及び有効性検証

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
- ガイドライン第1版の策定(2019.6)

電力SWG
- 小売電気事業者ガイドライン策定(2021.2)

防衛産業SWG
- 防衛産業サイバーセキュリティ基準の改訂を公表(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
- 2022年2月に第4回を開催

工場SWG
- 2022年夏を目途にガイドライン案を作成予定

・・・

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

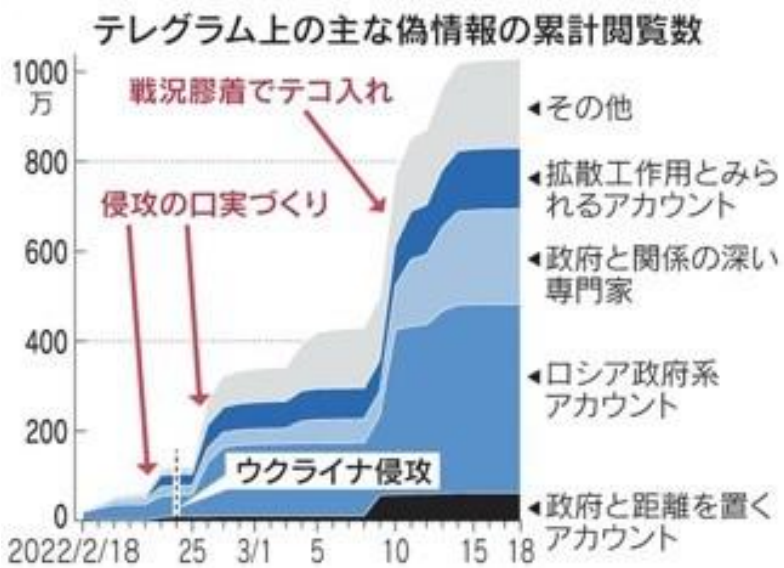
4. 本タスクフォースの検討事項
   a. 今年度事業の方針
   b. DMFの適用実証及び有効性検証

ウクライナ侵攻にともなう偽情報の拡散及び対応の状況

- ウクライナ侵攻前後からロシア政府は偽情報拡散を強化しており、独立系メディアの検閲が厳格化される中こうした傾向が一層顕著になっているとされており、在日米国大使館は、ロシア政府による偽情報の拡散を非難し、情報の真偽を見極めるよう日本語で注意を呼びかけた。

テレグラム上での偽情報の拡散状況

- 「政府と距離を置くアカウント」が偽情報に批判的な見解を拡散しているが、政府寄りのアカウントに拡散量で圧倒されている。



在日米国大使館による注意喚起

- 注意喚起には、リアルタイムで共有されるネットニュースの信頼性を検証するための助言が掲載されている。
- オンライン情報を見極める方法として、「SIFT」が紹介されている。

S	ストップ (stop)
I	発信元の調査 (investigate)
F	よりよい報道を探す (find)
T	主張・引用・報道を、発信元まで追跡する (trace)

SIFT考案者は、ウクライナ関連のニュースの取り扱いで「S」の重要性を指摘、ユーザーに対して、目の前にある情報に反応し、共有する前にいったん立ち止まる必要があると注意喚起している。

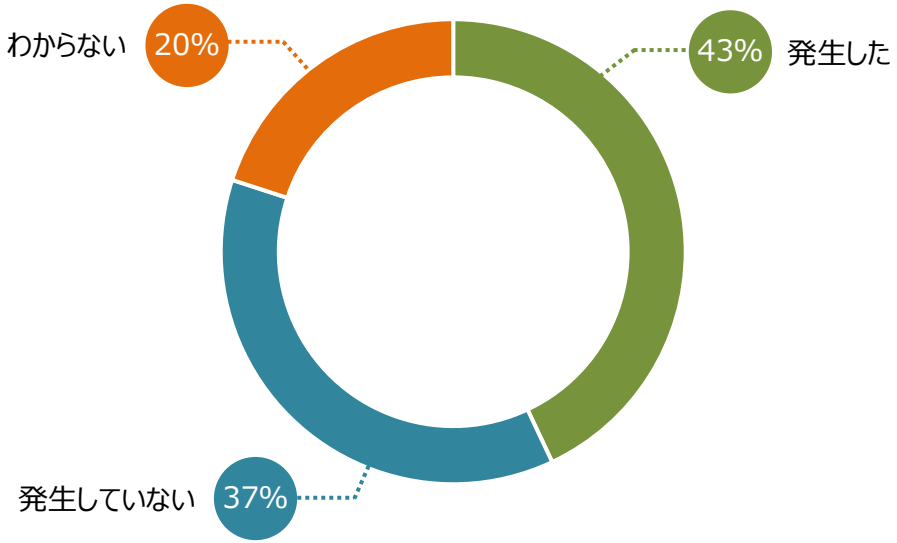
[出典] ロシアの偽情報工作の歴史は？（日本経済新聞 2022年4月8日）
(https://www.nikkei.com/article/DGXZQODL0791O0X00C22A4000000/)
戦時でも正しいオンライン情報と作り話を見分ける
(https://amview.japan.usembassy.gov/how-to-tell-fact-from-fiction-online-even-in-wartime/)

SaaSの設定ミス等によるセキュリティインシデントの発生状況

- クラウドセキュリティアライアンス(CSA)が公開した報告書によれば、少なくとも43%の組織が、SaaS の設定ミスが原因で 1 つ以上のセキュリティインシデントに対処している。

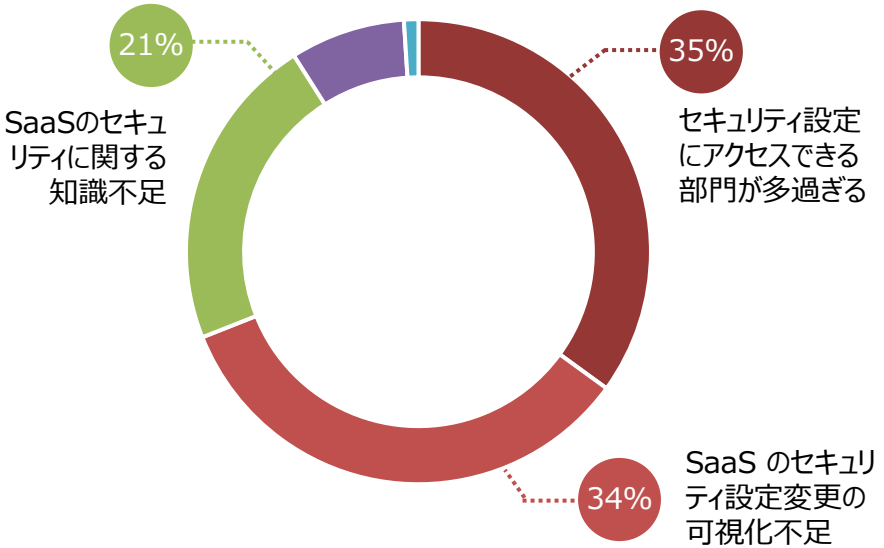
SaaSの設定ミスに起因するセキュリティインシデントの発生状況

- 少なくとも43%の組織が、SaaS の設定ミスが原因で 1 つ以上のセキュリティインシデントに対処している。
- 設定ミスが原因でセキュリティインシデントを経験したかどうかがわからない組織を含めると、最大で63%にもなる可能性がある。



SaaSの設定ミスに起因するセキュリティインシデントの主な原因

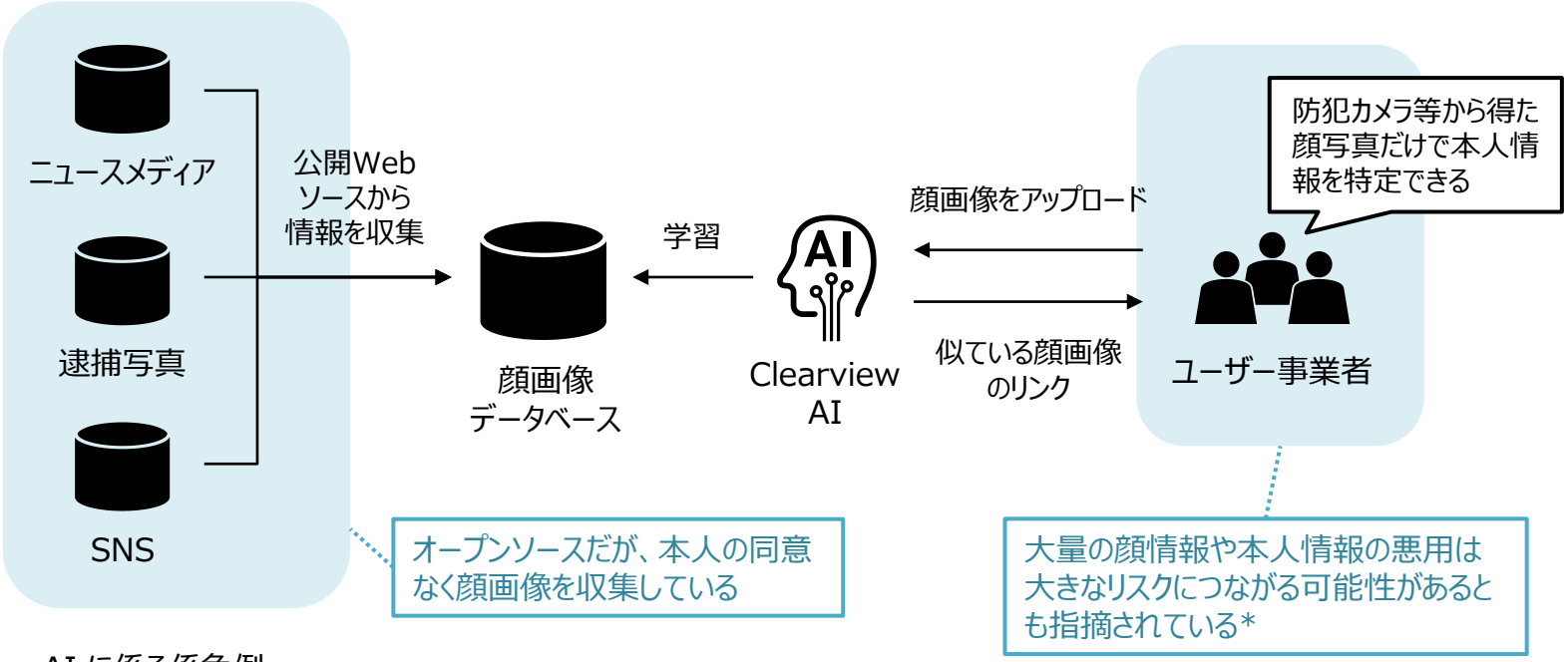
- セキュリティインシデントの主な原因は、SaaS のセキュリティ設定にアクセスできる部門が多すぎる(35%)こと、SaaS のセキュリティ設定変更の可視化不足(34%)だった。



[出典] SaaS Security and Misconfigurations Report
(https://cloudsecurityalliance.org/artifacts/saas-security-and-misconfigurations-report/)

顔認識サービスClearview AI に係る係争

- インターネット上に公開された顔情報をスクレイピングし、ユーザー事業者に顔認識関連サービスを提供するClearview AIについて、様々な国・地域にて問題が指摘され、係争が生じている。
- 英国情報コミッショナー局(ICO)はClearview AI社に対し、750万ポンド（約12億円）以上の罰金を課し公開されている英国居住者の個人データの取得と使用を停止するとともに、同社のシステムからの削除を命じる執行通知を発出。



Clearview AI に係る係争例

- イリノイ州生体情報プライバシー法(BIPA)違反を問う訴訟、スウェーデンのデータ保護当局による罰金、英国データ保護当局による罰金、データ使用停止等

[出典]　NY Times - The Secretive Company That Might End Privacy as We Know It
(https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html)

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. 今年度事業の方針
   b. DMFの適用実証及び有効性検証

環大西洋データプライバシーフレームワークの合意

- 2022年3月、欧州委員会と米商務省は、EUと米国間の個人データの移転に関する新たな枠組みとなる「環大西洋データ・プライバシー枠組み」にも原則合意したと発表。
- 2020年7月にEU司法裁判所が従前より運用されていた「プライバシー・シールド」を無効とする判決を出したことから、代替枠組みの策定が検討されていた。新たな枠組みでは、無効判決で指摘された、米国政府による個人データ保護上の不備が修正される見通し。

重要な原則

- 新しいフレームワークに基づき、参加する米国企業とEUとの間で、データが自由かつ安全に行き来できるようになる。
- 米インテリジェンス機関によるデータアクセスを国家安全保障を守るために必要かつ適切なものに限定するため、新しい規則と拘束力のある防護策を確立する。
- 米インテリジェンス機関は、プライバシーと市民の自由の基準を効果的に監督する新しい手続きを採用する。
- データ保護審査裁判所(Data Protection Review Court)を含め、米インテリジェンス機関によるデータアクセスに対する欧州市民の苦情を調査・解決するための2段階の新しい救済制度を確立する。
- EUから移転されたデータを処理する企業に対する強力な義務を課す。(米国商務省を通じて原則の遵守を自己証明する要求事項を引き続き含めること)
- 具体的なモニタリングとレビューの仕組みを確立する。

フレームワークによるメリット

- 米国に移転した欧州市民のデータの適切な保護、欧州司法裁判所の判決(Schrems II)への対応
- 安全かつセキュアなデータフロー
- 持続的かつ信頼できる法的基盤
- 年間9000億ユーロに及ぶ越境商取引を支えるデータフローの継続

今後のステップ

- 本合意は、今後、法的文書に反映される。米国側のコミットメントは、欧州委員会による妥当性判断の基礎となる大統領令に盛り込まれる予定である。

[出典] Joint Statement on Trans-Atlantic Data Privacy Framework
(https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087)

NIST SP800-171 及びSP 800-172の策定・改定状況

- 2022年3月、SP 800-172で提示されている高度なセキュリティ要件への準拠を評価するための手順及び方法論を示すSP 800-172Aが公開。
- 上記を含む、SP 800-171及び関連文書の今後の改善に向けて、米国NISTは2022年９月16日まで、意見募集を実施した。

SP 800-171及び関連文書の策定・改定状況

SP 800-171 Rev. 2
連邦政府外のシステムと組織における管理された非格付け情報(CUI)の保護
2020年2月公開

- 対策要件は変更されていないが、付録Fに記載されていたディスカッションがセキュリティ要件に併記される形となった。

SP 800-171A
管理された非格付け情報向けセキュリティ要件の評価
2018年6月公開

- SP 800-171で提示されているセキュリティ要件への準拠を評価するための評価手順及び方法論を提供する。

SP 800-172
CUIを処理する重要性の高いプログラム及び価値の高い資産向け高度セキュリティ要件
2021年2月公開

- 重要なプログラムや価値の高い資産で扱われるCUIの機密性保護に推奨される高度なセキュリティ要件を提供する。

SP 800-172A
管理された非格付け情報向け高度セキュリティ要件の評価
2022年3月公開

- SP 800-172で提示されているセキュリティ要件への準拠を評価するための評価手順及び方法論を提供する。

2022年９月16日まで、今後の改善に向けた意見募集を実施した。

EUデータ関連法の整備状況

- 欧州では、2020年2月のデータ戦略公開以降、データガバナンス法、デジタル市場法、デジタルサービス法、データ法等を含む、データアクセスと利用のための分野横断型のガバナンス枠組みの構築を目指した立法措置が進められている。

EU データ戦略 (the European data strategy) — 2020年2月公開

- 4つの柱のひとつとして、「データアクセスと利用のための分野横断型のガバナンス枠組みの構築」を提案し、以下の法律等の検討を示唆

データガバナンス法 (Data Governance Act) — 2022年6月に欧州官報で公布 / 2023年9月から施行

- 公的機関が保有する特定のデータを、個人データ、知的財産権、企業の機密情報などの保護を条件に、民間による再利用を可能にするためのメカニズムを規定

デジタル市場法 (Digital Markets Act) — 2022年7月最終承認

- デジタル市場の公平性確保等を目的に、大規模なプラットフォーマーに対してランキングサービスにおける自社製品・サービスの優遇禁止などを規定

デジタルサービス法 (Digital Service Act) — 2022年4月に政治合意

- デジタル市場の公平性の確保を目的に、大規模なオンライン・プラットフォーマーに対して違法なコンテンツへのリスク評価や対策義務等を規定

データ法 (Data Act) — 2022年2月に案を公開

- 非個人データの取扱いにおける消費者等の権利保護や産業競争力強化に向けたデータ利活用促進を目的として、非個人データへのアクセス・利活用における主体間の権利や義務を規定

デジタル市場法（DMA）の最終承認

- 2022年7月、欧州理事会はデジタル市場法(DMA)に対して最終的な承認を与えたと発表。
- デジタル市場の公平性確保等を目的に、大規模なプラットフォーマーに対してランキングサービスにおける自社製品・サービスの優遇禁止などを規定するもの。

EU デジタル市場法の概要と目的

分類	概要
立法の目的	• ゲートキーパー(gatekeeper)が存在するEU域内において、競争力があり、かつ公正なデジタルセクターの市場を確保するために、統一されたルールを設ける • 経済的不均衡、ゲートキーパーによる不公正なビジネス慣行、それらのネガティブな結果、たとえばプラットフォーム間で行われる競争における競争力低下にかかわる
規制の対象	• 以下の要件を満たすコアプラットフォーム提供者(ゲートキーパー) － 直近3年間におけるEU域内の売上高が75億ユーロ以上、または過去の平均時価総額もしくは同等の市場価値が750億ユーロ以上で少なくとも3加盟国で同一のプラットフォームサービスを提供している － 月間のアクティブなエンドユーザー数が4500万人以上
ゲートキーパーに適用される規定	• 個人の同意がないのに、コアプラットフォームから得た個人データを、GKが提供する他の事業から得た個人データまたは第三者のサービスから得た個人データと結合してはならない • コアプラットフォーム経由で獲得したエンドユーザーに対して、ビジネスユーザーが契約を提案し、締結することを認めるべき • ビジネスユーザーが、ゲートキーパーの行為について公の機関に問題を提起することを禁止・制限をしてはならない • 提供した広告に関して、広告主と媒体社の請求に応じて、広告主が支払った対価と媒体社に対して支払った報酬に関する情報を提供しなければならない

[出典] Infographic - Digital Markets Act
(https://www.consilium.europa.eu/en/infographics/digital-markets-act/)

EUデータガバナンス法の公布

- 2022年6月、データによる技術革新や経済成長に向けて、EU域内での官民データ共有促進、データ取扱いの安全性確保、データ共有への信頼性を高めるためのデータガバナンス法が欧州官報で公布された。本規則は、2023年09月24日から施行される。

EU データガバナンス法案の概要と目的

章	表題	規定の概要
2	公的機関が保有するデータの二次利用	• 官民保有データのうち、センシティブデータ(個人データ、知的財産、企業秘密等を含むデータ)の二次利用に関する条件を規定 – 官民データの二次利用は無料 – 利用者にデータを渡す際、当該データは匿名化されていること。匿名化解除には、データ保有者の承諾が必要 – データ分析は公的機関が監督する十分安全な環境で行われること – 非個人データの域外移転は、①EUが認定する同等国、または②データ移転後も二次利用者が義務を負う場合に限る – センシティブなデータの域外移転については別途ルールを定める
3	データ共有サービス提供者に適用される要件	• データ共有サービス事業に関する届出制度、遵守事項を規定 – データ共有サービスを行おうとするものは、事前に加盟国当局に通知が必要 – EU域内に設置または代理人を選定 – データを共有サービス以外に利用することを禁止 – 他サービスとの構造的分離
4	データ利他主義	• 企業・個人による科学研究等の公益のための自発的なデータ提供を鵜な挙がすため、サービスの登録制度を規定

データによる技術革新や経済成長に向けて、EU域内での官民データ共有促進、
データ取扱いの安全性確保、データ共有への信頼性を高める

EUデータ法案（Data Act）の公開

- 2022年2月23日、欧州委員会は「非個人データの公平なアクセスと利用の調和に関する法案(EU データ法)」案を公表。
- 本法はデータガバナンス法を補完するものであり、同法がデータを促進するプロセスを構築する一方、データ法はデータによる価値創造を行う際の条件を明確にするものとされる。

EU データ法案の主な規定と目的

章	表題	主な規定
2	B2C・B2Bのデータ共有	• ユーザが簡単に生成されたデータにアクセスできるようなIoT 機器の設計・製造実施、関連サービスの提供 (第3条1項) • データへのアクセス方法、データの利用目的等に関するユーザへの情報提供 (第3条2項) • ユーザの要請に基づくユーザ及び第三者へのユーザデータの提供 (第4条)
3	データを利用可能にする法的義務を負うデータ保持者の義務	• 公正、合理的かつ非差別的な条件および透明性の確保されたデータ提供 (第8条1項) • データへの不正アクセス防止、契約遵守確保に向けた技術的保護手段の適用 (第11条1項)
5	例外的な必要性に基づく公共機関、組合、団体へのデータ提供	• 公共の緊急事態(パンデミック等)への対応や復旧等の例外的な必要性がある場合には、民間企業からEU機関に求められたデータを提供すること (第14条1項)
6	データ処理サービスの切り替え	• ユーザが他事業者のサービスに変更できるよう、情報処理サービス提供者が、ビジネス、技術、契約、組織上の障害を取り除くこと (第23条1項)
7	国際的な文脈における非個人データの保護措置	• 情報処理サービス提供者に対し、非個人データの越境移転に際して、EU及び加盟国法への抵触がある場合、当該データの越境移転及び政府アクセスを防ぐための技術的・法的・組織的措置を講じることを規定 (第27条1項)

データ法により、デジタル環境における公平性を確保し、競争力のあるデータ市場を刺激しつつ、データ主導型イノベーションの機会を開き、すべての人がデータにアクセスできるようにする。

[出典] Data Act (https://digital-strategy.ec.europa.eu/en/policies/data-act)

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. 今年度事業の方針

b. DMFの適用実証及び有効性検証

2022年度の取組案（再掲）

- 現在のフレームワークの理解が難しい点もあり、まずは包括的視点でアーキテクチャを整理している行政分野での取組における適用・応用を目指す。そこから民間への横展開や基盤・ツールでの展開が考えられる。
- 経産省「データの越境移転に関する研究会」のデータの取扱に関する各国の制度のギャップ分析において、本フレームワークの応用が進行中。今後国際機関との連携も視野に。
- 民間においても先進的なユーザ・事業を対象に、実証を通じて有効性の検証を行えないか。
- これらの取組を通して得られた知見や課題を、今後のフレームワーク改訂の参考とする。

データ マネジメント フレームワーク

観点	実施内容
① ルール・標準化	データ越境移転（DFFT）
② 国際連携	
③ 適用・応用	データEX、トラスト、スマートシティ等 民間における実証

今後の改訂に向けた検討

これまでにいただいたご意見と本TFの取組み

- 昨年度に開催したTFでは、DMFの内容及び今後の課題に関するご意見に加え、今後のデータの信頼性確保に資する取組み全般に係るご意見を頂戴した。
- これまでのTF等でのご意見を踏まえ、①DMFの適用実証及び有用性検証、②さらなる具体化に向けた検討の2点に取組んでいくことを想定。

これまでのTFにおけるご意見

適用の拡充

- 今後の取り組みについて、行政を主体として進めるということは大変良い。可能であれば、**自治体をうまく巻き込んで、ケーススタディができると望ましい。**
- **OT分野のユースケース等を策定**いただければ活用に資すると思われる。

さらなる検討の具体化

- DFFTという目標を考えると、**コレクティブ・マネジメントという概念と内容の具体像**が示された方がわかりやすさが増すと考える。
- **場を主体的にまとめる主体は誰なのかという深堀**が必要。例えば、ユースケース#2で誰が取りまとめを行うべきか等の議論があった方がよい。
- **「場」が転移した際に、どのようなマネジメントが主体間で必要なのかという深堀**が必要かもしれない。

本TFの取組み(案)

① 適用実証及び有用性検証 実施中

- 委員等の協力も仰ぎ、より具体的かつ実際の運用に即したDMFのケーススタディを実施する。

DMFの適用実証

- 上記と並行して、内容のさらなる改善に向け、DMFの有効性の検証を行う。

DMFの有効性検証

② さらなる具体化に向けた検討

- データ流通の促進に資するより具体的なガイダンス文書の検討(「コレクティブ・マネジメント」の具体化)等

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. 今年度事業の方針
   b. DMFの適用実証及び有効性検証

DMFの適用実証

- 官民の先進的なケースを対象にDMFの適用実証を進め、現状版の課題を明確化し、今後の取組みの材料とする。
- 適用の成果物としては、① ユースケース、② DMF改善のためのデータ の2つを想定。

適用実証の概要

- 参画事業者に対象システム/サービスを選定いただき、事務局も支援しつつDMFを適用し、今後の改善等に向けた課題の整理を行う。

1 対象システム/サービスの選定 → 2 DMFの適用 → 3 課題等の整理

- TF委員等の協力を得て、５件の適用実証を実施している。

参画事業者	適用対象
㈱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
㈱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
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
㈱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
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
（他数件を調整中）	

想定する成果物

① ユースケース

- 対象システム/サービス
- 取扱うデータの種類とデータフロー
- 想定されるリスクと対応策

② DMF改善のためのデータ

- 適用作業に要した期間・工数(人月)
- 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　等

事例①：竹中工務店 IoT等を活用した次世代建物制御システム

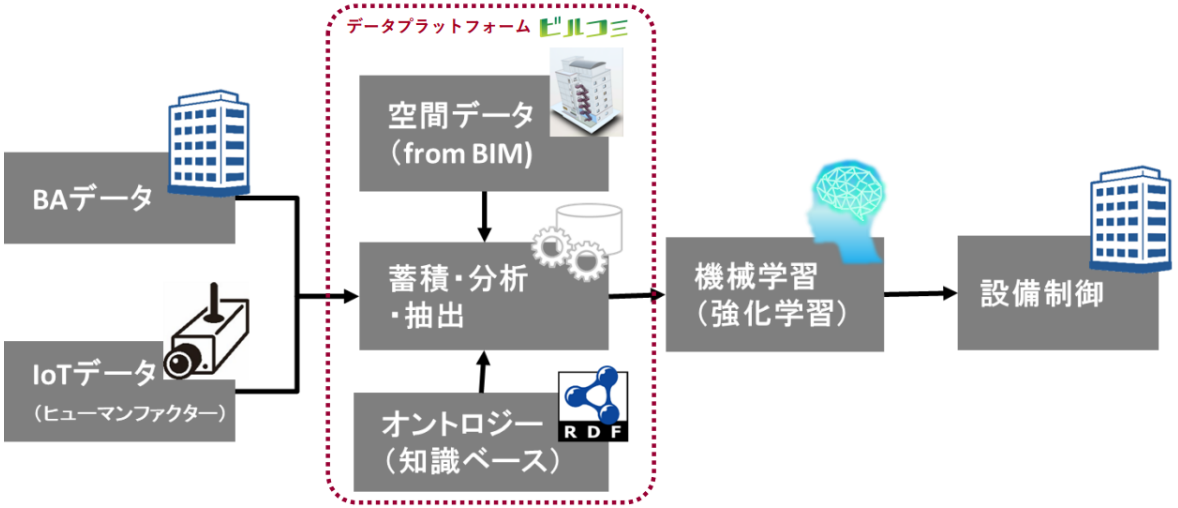
名称 (協力事業者)

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。

図1 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。

[参考] 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（http://www.uit.gr.jp/tech_research/presentation/file/A03.pdf ）

事例②：デンソー 車両データ活用基盤の利用

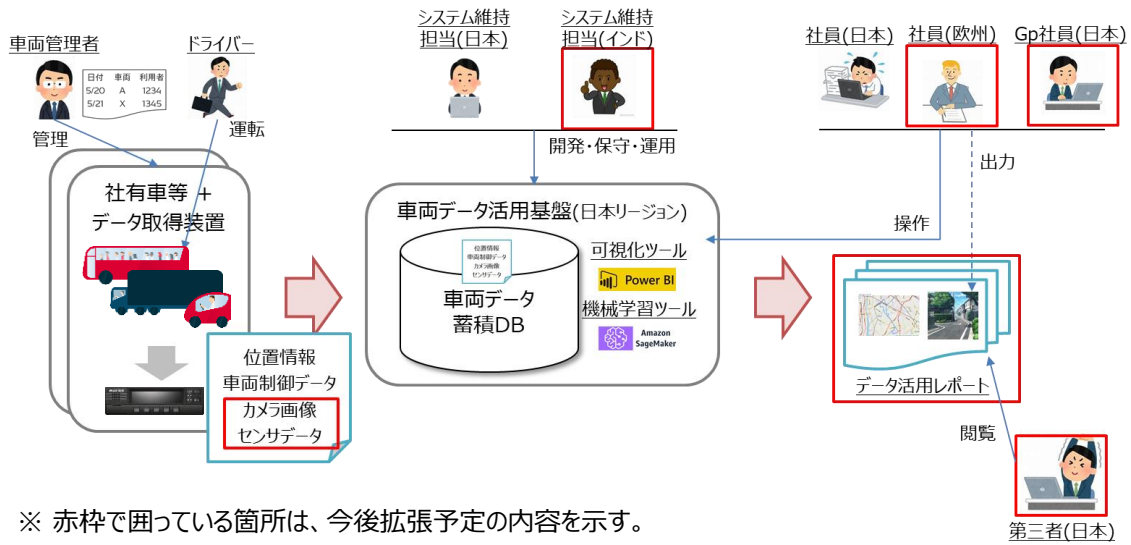
名称 (協力事業者)

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。

事例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

名称（協力事業者）

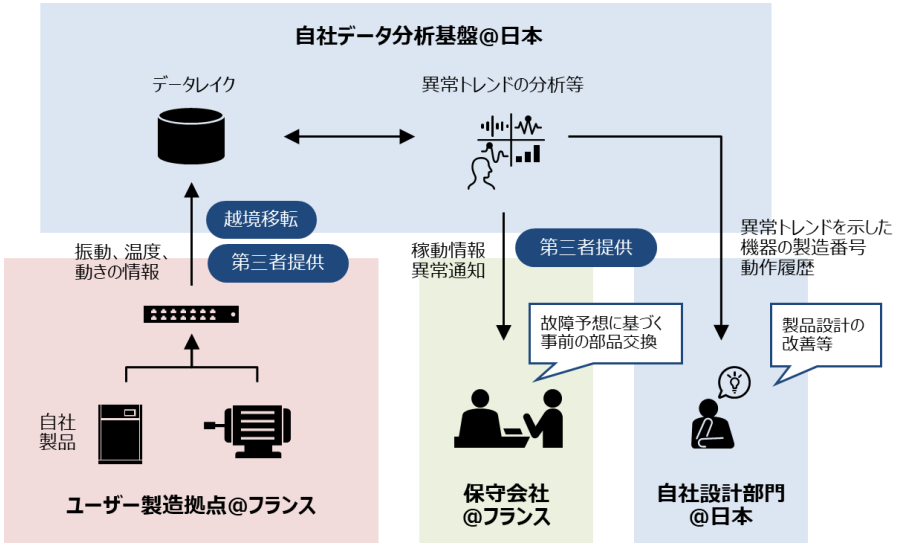
製造装置の稼働データ等を活用した予防保全・製品向上（三菱電機）

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。

事例④：シップデータセンター 共通基盤（IoS-OP）を介した船舶運航データの流通

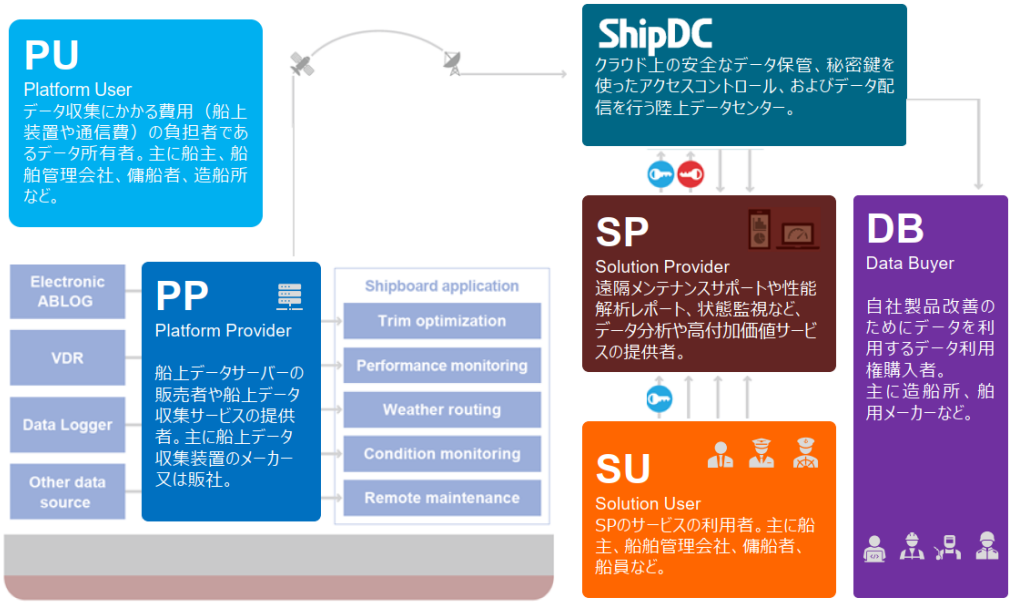
名称 (協力事業者)

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。

[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/)

事例⑤：パナソニック ワークプレイス向けソリューション

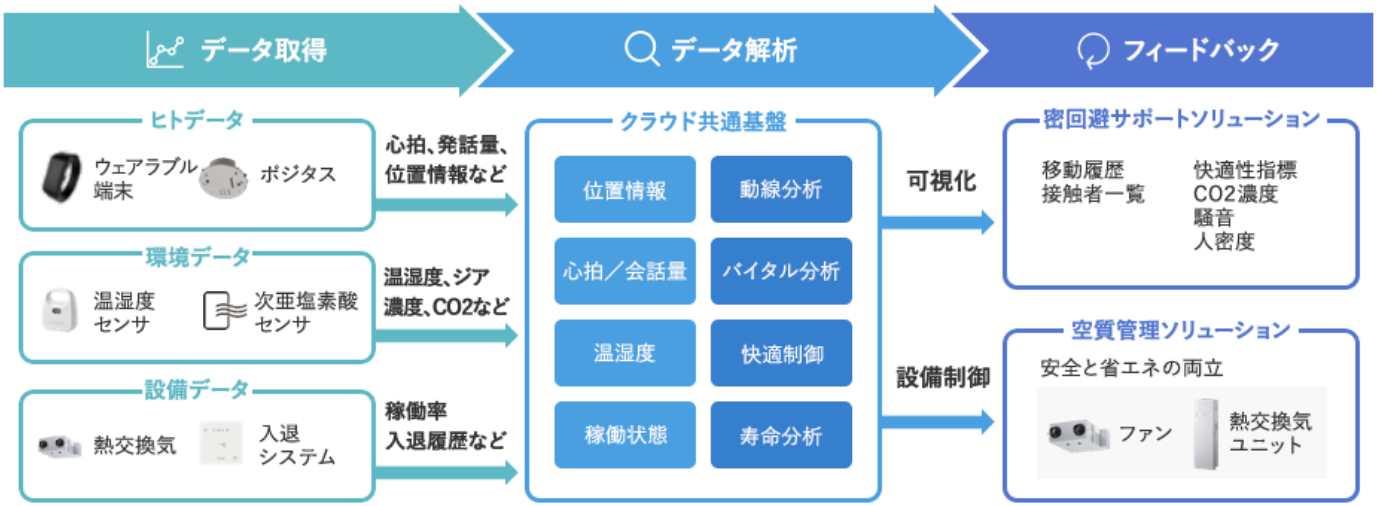
名称 (協力事業者)

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。

[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/)

[参考] 参画各社より頂戴した主なご意見（現状の整理）

- 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。

分類	概要
DMFの有用性や他の手法等と比較した位置づけ	• **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**と思われる。 • 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。**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。 • **DMFによるマクロ的アプローチと、詳細なシステム構成等に基づく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。
検討の進め方等の更なる具体化が望ましい事項	• 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。 • **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。
今後の施策等	• **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。

DMFの有効性検証

- 事業者の協力を得て実施するDMFの適用実証と並行して、過去に生じたインシデント・事故事例を対象にしたDMFの机上検討を進め、DMFの有効性検証、今後の改善に向けた課題の特定等を進める予定。
- 適用実証での適用事業者への確認結果とも照らし合わせて、最終的な有効性検証の結果として取りまとめることを想定。

机上検討

過去のインシデント等に対する机上でのDMFの適用、課題の特定 等

＜検証事項の例＞

- DMFの方式によるデータフロー可視化の有効性
- DMFにおけるリスク特定の組みの有効性

有効性に関する仮説の提示

適用実証

実際のシステム/サービスに対するDMFの適用を通じた課題の特定 等

成果の統合

有効性検証結果

DMFの適用が有効と考えられるケース、
有効とは言えないケースをそれぞれ整理し、より利便性の高い内容とするために必要な修正等を具体化する。
2023年1月の第8回TF開催時までを目途に取りまとめる。

適用実証の成果とも合わせて、現状のDMFの改善に向けた課題を特定し、
DMF改訂を含む今後の検討へのインプットとする。

DMFの有効性検証　検討に向けた仮説

- DMFの核となっている、「データのライフサイクル可視化」及び、「データに基点を置いた整理に基づくリスクアセスメントの実施」という点について検証することを通じて、DMFの有効性を主張することが可能ではないかと考える。

評価項目		概評	評価の観点
データのライフサイクル可視化による効用		• 有効に機能した • 有効だった可能性がある • 有効だったとは言えない	• データの生成・取得から加工・利用、廃棄に至るまでのライフサイクルを可視化し、関係者間で共通の理解を得ること(具体的なセキュリティ管理策の実装等は含まない)が、インシデント等を未然に防ぐ、あるいは被害を最小限に抑えるにあたって有効に作用したかを評価する。
事前のリスクアセスメントによる効用	事前にリスクアセスメントを実施することそのものの有用性の評価	• 有効に機能した • 有効だった可能性がある • 有効だったとは言えない	• DMFで提示されている方法かを問わず、事前に対象システム・サービスにおいてリスクアセスメントを通じたリスクの特定及び評価、緩和策の実施がなされていた場合に、インシデント等の発生を未然に防ぐことができていたか、あるいは被害を最小限に抑えることができていたかを評価する。
	データに基点を置いた整理に基づいてリスクアセスメントを実施することの有用性の評価	• 有効に機能した • 有効だった可能性がある • 有効だったとは言えない	• リスクアセスメントにおいてDMFで示されるデータに軸を置いた整理、イベントごとの評価を行った場合に、他の方法と比較して、インシデント等の未然防止あるいは被害の最小化に対する寄与が認められるかを評価する。 • 特に、データという粒度の高い単位で分析をすること、セキュリティに関する観点に加えて法制度等に関する観点を含めてリスクの特定を行うことによるメリット(またはデメリット、対応の不足等)が認められるかという点が評価され得る。

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。