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３月１７日

経済産業省 商務情報政策局
サイバーセキュリティ課

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. サイバー空間のつながりに関するデータマネジメントを巡る制度の動向

3. 本タスクフォースの検討事項
   a. パブコメでいただいたご意見とそれに対する考え方
   b. ユースケースの修正
   c. フレームワークの名称
   d. 今後のスケジュール
   e. 来年度の取組（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**
  - ガイドライン第1版の策定(2019.6)
- **電力SWG**
  - 小売電気事業者ガイドライン策定(2021.2)
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表(2020.12)
- **スマートホームSWG**
  - ガイドライン1.0版を公表(2021.4)
- **宇宙産業SWG**
  - 2022年2月に第4回を開催
- **工場SWG**
  - 2022年2月に第2回を開催
- ・・・

分野横断SWG

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

検討事項：
データの信頼性確保に向け「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」案のパブリックコメント（2回目）を実施。

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

検討事項：
OSSの管理手法に関するプラクティス集を策定、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。

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. サイバー空間のつながりに関するデータマネジメントを巡る制度の動向

3. 本タスクフォースの検討事項
   a. パブコメでいただいたご意見とそれに対する考え方
   b. ユースケースの修正
   c. フレームワークの名称
   d. 今後のスケジュール
   e. 来年度の取組（案）

欧州ENISA データ保護エンジニアリングに関する報告書

- 2022年1月、欧州サイバーセキュリティ機関（ENISA）は、「データプロテクション・バイ・デザイン」及び「データプロテクション・バイ・デフォルト」の実装を通じて、実務家や組織を支援するため、「データ保護エンジニアリング」（Data Protection Engineering）に関する報告書を公開。
- 本報告書は、データ保護に係る既存の技術と手法を紹介し、GDPR第5条に規定されているデータ保護の原則を満たす上での強みと適用可能性について議論している。

“Data Protection Engineering”に関する報告書の概要

- 本報告書は、「データプロテクション・バイ・デザイン」及び「データプロテクション・バイ・デフォルト」の実装に係る既存の技術と手法を紹介し、GDPR第5条に規定されているデータ保護の原則を満たす上での強みと適用可能性について議論している。

個人データの処理における原則

- 適法性、公平性および透明性の原則
- 目的の限定の原則
- 個人データの最小化の原則
- 正確性の原則
- 保管の制限の原則
- 完全性および機密性の原則

[GDPR 第5条]

実装を支援

データ保護に係る既存の技術と手法 (各手法の課題を含む)

匿名化及び仮名化 (3章)

一般的なデータ匿名化の手法として、k-匿名化、差分プライバシーを紹介

マスキング及びプライバシー保護計算 (4章)

手法として、準同型暗号、セキュアなマルチパーティ計算、信頼できる実行環境(TEE)等を紹介

アクセス、通信、保管 (5章)

通信経路の保護、保管データの暗号化、プライバシーに配慮したアクセス制御手法を紹介

透明性、介入、利用者管理ツール (6章)

ユーザーから見た透明性を確保する手段として、プライバシーポリシー、同意管理システム等を紹介

ステークホルダーに向けた提言

規制当局

- 関連する技術や手法の最先端のソリューションに関連して、**EU全体でグッド・プラクティスを議論し、促進すべき。**
- GDPRの第42条(認証)に基づき、データ保護の適切なエンジニアリングを確保するために、**関連する認証制度の設立を促進**すべき。

研究機関

- EU機関の支援を受けて、**データ保護原則の実装を支援する技術・手法の展開を継続的に探求**すべき。

中国における主なデータ保護関連法規

- 中国では、2017年6月のサイバーセキュリティ法施行を皮切りに、「サイバーセキュリティ審査弁法」や「自動車データセキュリティー管理若干規定（試行）」等の付随規定が盛んに策定されていることに加え、特に2021年に同法とともにデータ管理の法的枠組みを構成するデータセキュリティ法、個人情報保護法が施行された。

中国におけるセキュリティ規制3法

2017年6月施行

サイバーセキュリティ法
[中华人民共和国网络安全法]

- 国家の安全保障を目的として、個人情報の保護、機密情報の保全、国外へのデータ移転規制、セキュリティ製品の認証、法的責任と罰則等について規定 (以下、「CS法」と表記)

2021年9月施行

データセキュリティ法
[中华人民共和国数据安全法]

- 中国国内におけるデータの収集、保存、加工、使用、提供、取引、公開等の行為に関連して、政府によるデータ分類・等級分類及び重要データ管理に関する制度の構築、事業者のデータセキュリティ保護に係る義務等を規定 (以下、「データ法」と表記)

2021年11月施行

個人情報保護法
[中华人民共和国个人信息保护法]

- 個人情報の処理や越境移転に係る規則、個人が行使できる権利等を規定 (以下、「個情法」と表記)

3法の規定に関連して定められた下位法令等(例)

- 左記の3法は内容が原則的であり、詳細は以下に例を挙げる下位の法令(条例、弁法、ガイドライン等)にて順次明確化されている。

サイバーセキュリティ等級保護条例	**2018年6月公布**

CS法21条に基づき、データのサイバーセキュリティ等級と、対応する保護措置を規定

工業情報化分野データセキュリティ管理弁法（試行）	**2021年9月意見募集開始**

データ法第21条等に基づき、工業・情報化分野におけるデータ処理活動に関する規律を規定

重要情報インフラセキュリティ保護条例	**2021年9月施行**

CS法における重要情報インフラ運営者のセキュリティに係る責任と義務を規定

サイバーセキュリティ審査弁法	**2022年2月施行**

CS法第35条、データ法第24条に基づき、重要情報インフラ事業者が特定のIT製品・サービスを調達する際に、国が実施する審査に係る申請手続等を規定

個人情報域外移転安全評価弁法	**2021年11月意見募集開始**

CS法第37条、データ法第31条、個情法第38-41条に基づき、国内で収集した個人情報及び重要データを国外へ移転する際に実施する安全評価の要求及び手順を規定

自動車データセキュリティ管理若干規定（試行）	**2021年10月施行**

データ法第30条等に基づき、自動車産業に関連する個人情報及び重要データについて、国内保存の義務付け、国外移転時の国による安全評価等を規定

中国における主なデータ保護関連法規

- サイバーセキュリティ法、データセキュリティ法、個人情報保護法の規定に関連して、各弁法等が策定され、規定の具体化が進んでいる。

 **個人情報域外移転安全評価弁法**	2021年10月29日から1か月間の意見募集を実施	• サイバーセキュリティ法第37条、データセキュリティ法第31条、第36条、個人情報保護法第38～41条に基づき、主に以下の規定を設けている。 – 重要情報インフラ運用者*1が収集・生成する個人情報や重要データ*2を国外に提供する場合、送信データに重要データが含まれる場合等に、所在する省を通じて、国に当該域外移転のセキュリティ評価を申告する。[4条] – 当局によるセキュリティ評価においては、申告書、データ越境リスク自己評価報告書、データ処理者と域外受領者との間で締結する契約等を提出する。[6条] – 国家ネットワーク通信部門は、受理通知書の発行日から45営業日内にデータ越境安全評価を完了させるが、当該期間を原則60営業日まで延長することができる。[11条]
 **サイバーセキュリティ審査弁法**	2022年2月15日より改正法が施行	• サイバーセキュリティ法第35条等に基づき、主に以下の規定を設けている。 – 重要情報インフラ運用者*1がネットワーク製品・サービスを調達する場合、およびネットワーク・プラットフォームの事業者が国家安全保障に影響を与える可能性のあるデータ処理活動を行う場合、本弁法に基づきサイバーセキュリティ審査を受ける。[2条] – 審査時には、(1)申告書、(2)国家安全保障への影響に関する分析報告、(3)契約書、新規株式公開(IPO)などの上場申請書類の提出等を提出する。[8条] – 「100万件を超える個人情報を保有するネットワーク・プラットフォーム事業者」による海外での上場を審査対象とする。[改正法にて追加]
 **自動車収集データに関するセキュリティ要件(案)**	2021年10月19日より意見募集を実施	• 情報セキュリティ標準化技術委員会(TC 260)が、自動車から収集したデータの送信、保存、出口などの処理活動に関するセキュリティ要件案を策定している。 – 自動車は、匿名化された映像・画像データを除き、データ主体の個別の同意を得ることなく、個人情報を含むデータを外部に送信してはならない。 – 車外のデータおよび位置情報の追跡データは、一部の例外を除き、プラットフォーム等の車外の場所に14日以上保存してはならない。 – 車外のデータ、車内のデータ、位置追跡データを、当局の審査なしに越境してはならない。

*1「重要情報インフラ運用者」とは、重要情報インフラ(公共通信、情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政務、国防科学技術工業などの重要な業界と分野に属しており、またはその他のひとたび機能の破壊もしくは喪失またはデータの漏えいに遭遇すると、国家の安全、経済、民生または公共の利益を著しく脅かす恐れのある重要ネットワーク施設や情報システム等)を運営するものを指す。

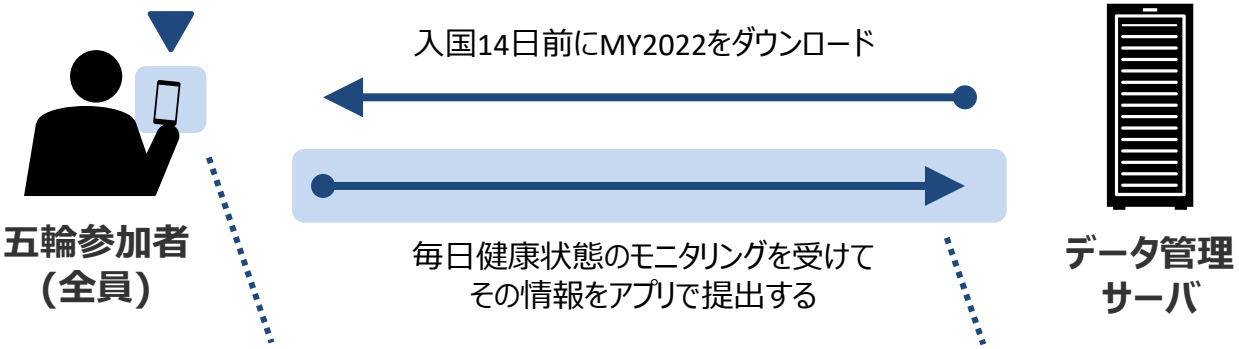
*2「重要データ」とは、「自動車データセキュリティー管理若干規定（試行）」では、「ひとたび改ざん、破壊もしくは漏えいまたは違法な取得もしくは利用に遭遇すると、国家の安全、公共の利益または個人・組織の権益をおびやかす可能性のあるデータ」を指す。

北京五輪参加者向けアプリにおけるセキュリティの脆弱性

- 2022年2月に開催された北京五輪において、参加者全員にインストールが義務づけられていた健康管理アプリ「MY2022」に、複数のセキュリティ上の欠陥があることが、カナダのセキュリティ研究者の分析により判明した。
- アプリには、暗号化の不具合だけでなく政治的なキーワードの検閲に関連するデータも搭載されていたとされる。

健康管理アプリケーション「MY2022」

- 北京五輪で、**参加者全員に対してインストールが義務づけ**られている
- **選手らの新型コロナウイルスワクチン接種情報などの収集を目的**に、北京金融控股集団という中国の国有企業が開発



アプリケーションの脆弱性①

- アプリがSSL/TLS証明書を検証していないため、**データの送信先を検証できない**
- 第三者がアプリとサーバとの通信を妨害して本来のサーバになりすますことで、パスポート情報や医療情報を盗んだり、ターゲットに偽の指示を送ったりするおそれがある

アプリケーションの脆弱性②

- **一部の機密データを暗号で保護せずに送信する**
- データには、メッセージの送信者と受信者の名前、ユーザーアカウントの識別子などプライバシー性の高いものが含まれており、外部から盗聴されるおそれがある

＊上記のほか、MY2022がユーザー情報をどんな組織と共有するかがプライバシーポリシーに明記されていないという問題、 Android版には、中国で政治的とされるキーワード2442個のリスト「illegalwords.txt」も付随していたという問題も指摘されている

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. サイバー空間のつながりに関するデータマネジメントを巡る制度の動向

3. 本タスクフォースの検討事項
   a. パブコメでいただいたご意見とそれに対する考え方
   b. ユースケースの修正
   c. フレームワークの名称
   d. 今後のスケジュール
   e. 来年度の取組（案）

データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク

- 「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮題、以下フレームワーク）」の第2回パブコメを実施。（2022年2月2日～3月3日）　→　9つの組織・個人から24の意見提出あり。
- 第6回タスクフォースでは、パブコメでいただいたご意見と対応方針についてご確認いただきたい。

【本文】

1. 新たなデータマネジメントの在り方
- 1-1 CPSFにおける第3層（サイバー空間におけるつながり）
  - 1-1-1 CPSF概論
  - 1-1-2 第3層の位置づけ
- 1-2 データの信頼性確保：データマネジメントの考え方の確立
- 1-3 本フレームワークの目的
- 1-4 本フレームワークの想定読者

2. 本フレームワークにおけるデータマネジメントのモデル
- 2-1 概要編
  - 2-1-1 データマネジメントのモデル化の概要
  - 2-1-2 リスク分析手順
- 2-2 詳細編
  - 2-2-1 モデル化（「イベント」）
  - 2-2-2 モデル化（「場」）
  - 2-2-3 モデル化（「属性」）

3. 活用方法
- 3-1 サプライチェーンを構成するステークホルダー間での活用
- 3-2 ルール間のギャップの分析

【添付資料】

添付A. ユースケース

添付B. イベントごとのリスクの洗い出しのイメージ

第1回パブコメ後に追加した箇所

第1回パブコメを受けて修正

第2回パブコメを実施

主なご意見と考え方①

いただいたご意見

- 表A-3.2で示す属性項目以外に「サーバ所在地」等の項目を設け、直接契約結ぶクラウドサービスプロバイダ等に情報の開示を求める等して現にデータが所在する国を把握できるようにしておくことが望ましい。と記載されています。
この点、**個人情報保護法の令和2年改正**で、個人情報取扱事業者の安全管理措置義務（令和3年改正により23条（現在20条））の内容としてガイドラインに明示された「外的環境の把握」には「個人情報取扱事業者が、外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じなければならない」と記載されており、また、保有個人データについては「『保有個人データの安全管理のために講じた措置』を本人の知りうつ状態に置かなければならない」（令和3年改正により32条1項4号（現在27条）、政令10条1項）として、ガイドラインには（外的環境の把握）の事例として「個人データを保管しているA国における個人情報の保護に関する制度を把握した上で安全管理措置を実施」と記載されており、さらにこの事例の部分には「外国（本邦の域外にある国または地域）の名称については、必ずしも正式名称を求めるものではないが、本人が合理的に認識できると考えられる形で情報提供を行う必要がある」とされています。
そうすると、個人情報保護委員会が出している個人情報保護法のガイドラインとの整合性を保つには、「現にデータが所在する国を把握できるようにしておくことが望ましい。」という部分は「**現にデータが所在する国や地域を把握し、保有個人データの本人には合理的に認識できると考えられる形で情報提供を行う必要がある**」と修正した方が良いと思料します。

考え方

- いただいた御意見を踏まえ、1203行目以降の記述を以下のとおり修正いたします。

  なお、保有個人データを外国で取り扱う場合には、「保有個人データの安全管理のために講じた措置」として、クラウドサービスプロバイダ及び当該データが保存されるサーバが所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を公表等する必要がある。

主なご意見と考え方②

いただいたご意見

- １２行「あたって」と、３３１行「当たって」とは、どちらかに字句を統一したほうがよい。
- ２９行「拡がって」と、１５０行「広げる」とは、どちらかに字句を統一したほうがよい。
- ５３行「とおり」と、５７０行「通り」とは、どちらかに字句を統一したほうがよい。
- １０３行「一つ」と、４６７行「ひとつ」とは、どちらかに字句を統一したほうがよい。
- ２９６行「または」は、９１３行「又は」とは、どちらかに字句を統一したほうがよい。

- ５７９行「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）」は「CPSF」のほうがよい。１２行で略語を定義しているから。
- ６２７行「という」は「という。」のほうがよい。
- １１９７行の表の大分類欄の記載の一部が見えない。

考え方

- 「あたって」「広げる」「とおり」「一つ」「または」の表記に統一いたします。

- いただいた御意見のとおり、修正いたします。
- 「という」はご指摘の個所を含め、いただいた御意見のとおり、修正いたします。
- いただいた御意見を踏まえ、ご指摘の個所を編集し、全体の記載が見えるように対応いたします。

主なご意見と考え方②

いただいたご意見

- ２１２行「個人情報保護法」は、５４ページの脚注３８の法律の**略称であること**を記載したほうがよい。
- ６２７行「本ユースケース」と、８１６行「本ユースケース」とは、**それぞれが別のものを指している**のだから、別の用語としたほうがよい。
- ７４４行の表の「**内部情報管理規則**」はどの省庁の省令か？

考え方

- 個人情報保護法については、指摘箇所に以下の註を挿入いたします。
  本稿では、「個人情報の保護に関する法律（平成十五年法律第五十七号）」の略称として、「個人情報保護法」という表記を用いる。
- 「ユースケース」については、ご指摘の個所の記載を以下のように修正いたします。
  （A-2内において、以下、「本ユースケース」という。）
- 「内部情報管理規則」とは、ユースケース内でX社が社内規則として定めるものを意図しております。いただいた御意見を踏まえ、記載の明確化のため、該当部の記述を「X社内部情報管理規則」といたします。

主なご意見と考え方③

いただいたご意見

- 「場」という概念は、明文化されていないルール等の必ずしも規範として扱われない内容も含むということですが、本文には**そのような説明が見受けられません**。例示やユースケースで挙げられているのは、個人情報保護法など法制度、またP27においても、下記記載にある、明文化されている事例であり、「明文化していないものも含む。」と本文に記載した方がよいのではないでしょうか。
- また、これは**英語ではどのように訳すのでしょうか**。Place? Space? Scope? 英語にしたときに混乱しない訳し方、説明の工夫も必要であると考えます。

- **「場」として特定され得る規範**には多様なものが含まれ得ると思いますが、**参考となる関連規定の分類方法**としては、本文に記載されているものの他、以下の分類があると思います。
  - 情報を管理する事業者に管理責任を課す類型：情報を管理する者に対して当該情報に対する管理責任を負わせる類型の法制度であり、個人情報保護法における個人情報取扱事業者の義務等を含む。
  - 不正行為者に法的責任を問う類型：不正行為者に対して法的責任を問う類型の法制度であり、不正競争防止法における営業秘密保護規定等を含む。

考え方

- いただいた御意見を踏まえ、本文及び各ユースケースの記載において、**明文化されていないルール等の必ずしも規範として扱われない内容も含む**点がより明確になるよう内容を修正いたします。
- 現在、「場」の英訳として“**domain**”を対応させておりますが、いただいた御意見は、フレークワークの更なる検討を進めていくにあたって参考にさせていただきます。
- いただいた御意見を踏まえ、**A-1に記載していたご指摘の記述を、2-2-2に移す**よう修正いたします。
  （※TF終了後に反映予定）

主なご意見と考え方③

いただいたご意見

- P12に記載の「イベント」において、**ある特定の移転・提供事象**とありますが、特定とはどういう場合でしょうか。

- P12で、**４つの単位（国・地域・組織・人、システム・サービス、機器）の単位でリスクを整理する**とありますが、示されているユースケースでは（例 P43（各機器ベンダーが保有する「統合データ」の PF 事業者への「移転・提供」にて想定されるリスク（例））では、**この観点が抜けている**ため、例示すべきと考えます。**４つの単位で行うリスク整理と、STEP4のイベントごとに行うリスクの洗い出しとの関係が解り難い**と思います。

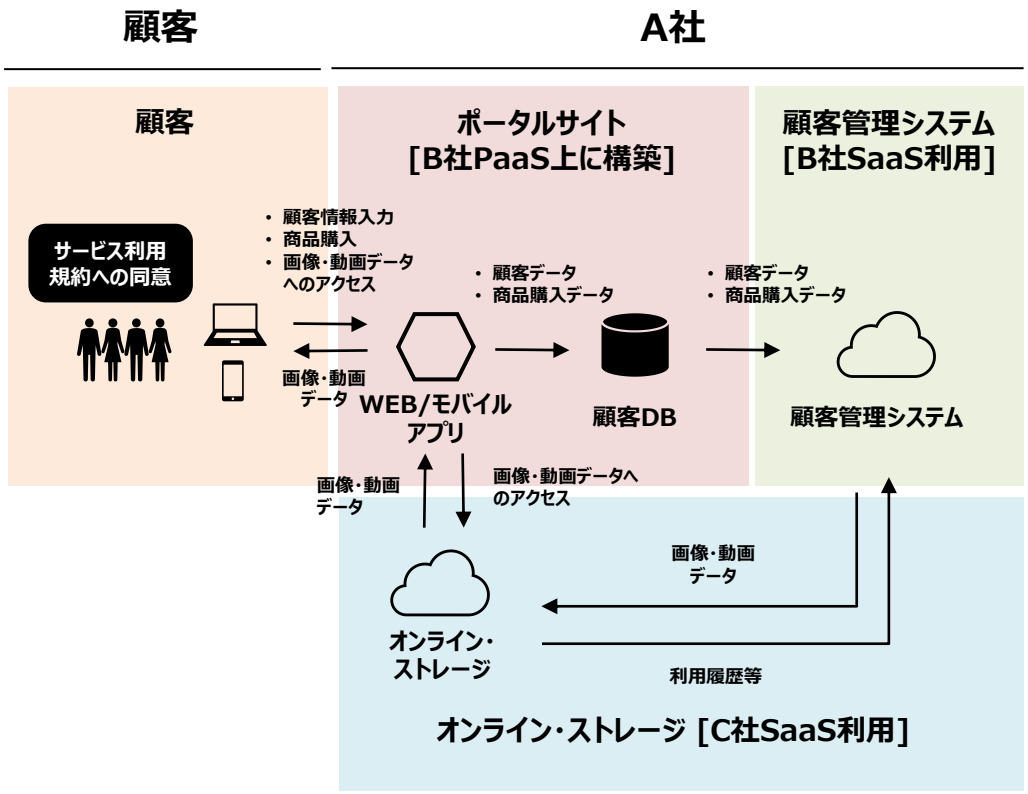
考え方

- 「ある特定の移転・提供事象」とは、本フレームワークの適用対象となる移転・提供事象を意図しておりました。いただいた御意見を踏まえ、記載の明確化のため、該当部の記述を「**対象となる移転・提供事象**」といたします。
- いただいた御意見を踏まえ、各ユースケースの記載において、**４つの単位で行うリスク整理の結果が見えるように**内容を修正いたします。

ユースケースの内容修正 - クラウドサービスを提供する例 概要

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

システム・サービス概要



事業者の業種をより一般的な用語に修正

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

フレームワークの名称

- Ver.1.0の公開にあたり、本フレームワークの正式名称を以下のいずれかとしたい。

案①

データによる価値創造（Value Creation）を促進するための
新たなデータマネジメントの在り方とそれを実現するためのフレームワーク

New Data Management Methods and Framework to Promote Value Creation through Data

案②

データマネジメントに関する新たなフレームワーク
～データによる価値創造の信頼性確保に向けて

New Framework for Data Management
- Toward a trustworthy data-driven value creation

案③

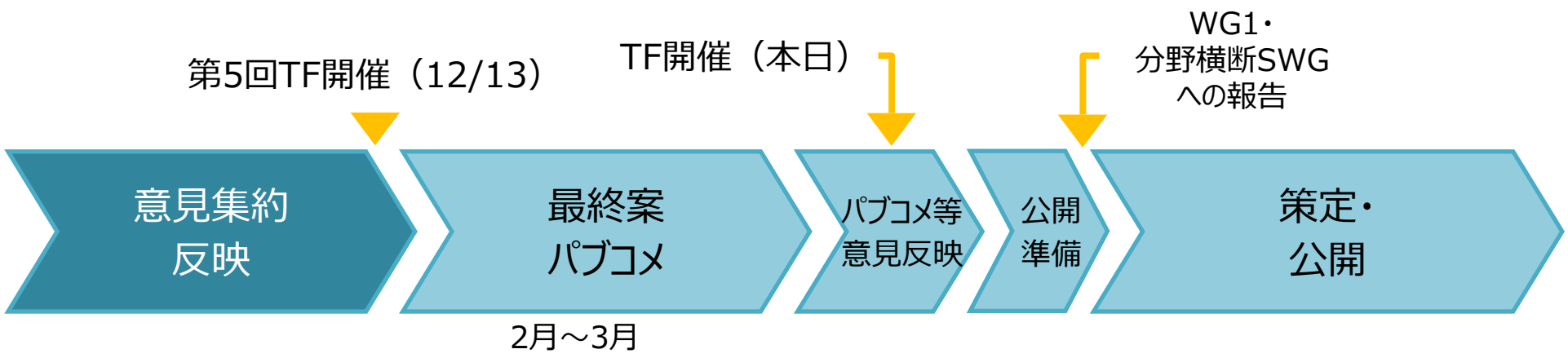
協調的で信頼あるデータ利活用に向けたデータマネジメント・フレームワーク
～データによる価値創造の信頼性確保に向けた新たなアプローチ

Data Management Framework for collaborative data utilization with trust
- A new approach toward an establishment of trust in a data-driven value creation

今後のスケジュール

- 本TF開催後、公開準備を進めWG1・分野横断SWGへ報告を行った後、フレームワークVer1.0を4月以降に公開する予定。

今後の進め方



1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. サイバー空間のつながりに関するデータマネジメントを巡る制度の動向

3. 本タスクフォースの検討事項
   a. パブコメでいただいたご意見とそれに対する考え方
   b. ユースケースの修正
   c. フレームワークの名称
   d. 今後のスケジュール
   e. 来年度の取組（案）

経済産業省 データの越境移転に関する研究会 （再掲）

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

【第１段階】データの取扱に関する制度の問題点をお互いに指摘し合う

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

→ 本年度の報告書を公開
次ページ以降で概要を紹介する

【第２段階】各国間のギャップ分析をOECDなど国際機関と連携して実施

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

※データを軸に置き、データのライフサイクルを通じて、その置かれている状態を可視化してリスクを洗い出し、そのセキュリティを確保するために必要な措置を適切なデータマネジメントによって実現することを可能とするフレームワーク。経産省が提案（2021年10月一次パブコメ終了）。

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

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

データの越境移転に関する研究会 - １．報告書のポイント

- 「Data Free Flow with Trust（DFFT）」のビジョンを制度として具体化していくためには、**基本的な価値観を共有する国同士が、プライバシーやセキュリティ、知的財産の保護などの規制的要請を踏まえた上で、相互運用可能な仕組みを構築・提案**していくことが重要。
- また、国際的なデータ流通を円滑にするためには、政府間の「信頼」のみならず、企業、自然人、規制当局、国際機関など**データのライフサイクルに関わる全てのステークホルダーの間に「信頼」が存在すること**が必要。
- このため、DFFTの具体化が目指す国際的な枠組みは、**ボトムアップな視座から、このような様々な主体の間に現在存在する障壁を特定し、それを解消すること**も射程に含めていくべきである。

➢ 本報告書では、以下の３つの論点に焦点を当て、企業ヒアリング及び各国の法令調査等の結果をまとめた。

① 企業によるデータの利活用において、越境移転がどのように行われているのか
（データのライフサイクル、ライフサイクルに関わるステークホルダー、越境移転のパターンの特定）

② また、企業がデータを越境移転させる場面においてどのような障壁に直面しているのか

③ 各国のデータ関連規制が主にどのような観点から行われているのか

類型１：オンラインアプリ企業の商品開発におけるデータの利活用

■概要

顧客の基本データと当該顧客のアプリ利用実績から、顧客のタイプごとに利用傾向などを分析し、公的データなどの外部から入手したデータと組み合わせ、アプリの改善や新規サービスの開発に利用する。また第三国の企業からデータ提供を受けることもある。

■データ管理方法

顧客から収集したデータは、一旦リージョンごとのクラウドに保存して、ある程度構造化・統合した上で、開発拠点がある国のクラウドに移転される。また、エンジニア等の人材をグローバルに採用しているため、分析・開発作業等の際に、社内の「越境アクセス」が発生する。

データのライフサイクル

生成・取得

A)データの状況
- 顧客のアプリ利用に関して、データが発生。主なデータは、顧客の属性データ及び顧客の利用状況データの２つ。

B）企業の要望
- 開発拠点や本社等のクラウドに集約する、地域ごとのクラウドで管理するなどを市場環境に合わせて柔軟に選択できるのが望ましい。

C）企業から見た課題
- 国によってデータを域外移転する際の要件が異なり、同意の要件も用途によって異なる等から、定型的な対応も難しい。また、第三国提供の場合、移転先国の法令準拠も求められ、対応に苦慮。
- 法令が国毎に異なると、1国１拠点や越境前の処理対応が必要となるため、スタートアップや中小企業にとって参入障壁が高すぎる。

加工

A)データの状況
- 作業の効率化や法令遵守などの観点から、データの越境前にエンジニアが個人情報の切り分け等の処理を行う。

B）企業の要望
- 開発拠点や本社等のクラウドに集約する、地域ごとのクラウドで管理するなどを市場環境に合わせて柔軟に選択できるのが望ましい。

C）企業から見た課題
- 「個人情報」の定義や要件が法令本体だけなく、ガイドラインや申し合わせ等にまで及んでおり解釈が難しい。
- 収集データの増加すると、「個人情報」の該当判断が微妙になる。
- 国境を越えた複数リージョン間のデータ統合や越境データアクセスが「越境移転」に該当するか分からず、予防的措置が必要。

移転

A)データの状況
- データを開発拠点に集約。開発チームがいる地域のクラウドにデータを移転するか、開発チームが利用可能な環境に、加工後のデータを保存する。

B）企業の要望
- 越境アクセスには情報通信コストがかかるので、開発等のリソースがある場所にデータを集約させたい。
- 提供サービスによって開発に「個人特定性」が必要か否かが決まる。

C）企業から見た課題
- 各国法令上、「個人特定性」の定義が分かりにくく、匿名化等しても、重要情報として規制対象になる懸念あり。
- 第三国から情報提供を受ける際の法令等の要件に対応するのが難しい。
- 複数リージョン間をまたいでビッグデータ化したくても、各国法令が異なる、その解釈が不透明等の理由から、踏み出せない。

データの越境移転に関する研究会 - 3. 各国データ関連規制の現状①

- 各国で順次導入されているデータ関連規制について、越境移転規制や国内保存・国内保管義務にかかる規定を整理した。**越境移転規制の対象となる情報や越境移転が許容されるための要件、国内保存・国内保管義務の有無や内容といった各国法令における規定ぶりが国によって大きく異なっており、**グローバルに事業展開を行う**企業の各国法令への対応コストは、近年ますます大きくなってきている**状況。
- 一方で、「データ」という存在自体、多面的な性質を持っているため、目的や文脈によって様々な分類が可能でありながら、その境界線には常に解釈の問題が存在しており、シンプルかつ履行しやすい形で一般的なタクソノミー（定義・分類）することは困難。

	越境移転規制							国内保存・国内保管義務			
	法令名	規制の対象となる情報	規制の対象者	越境移転が許容されるための要件				法令名	規制されるデータ	規制の対象者	義務の内容
				当局の認証等	所定の契約	本人の同意	その他				
EU	GDPR	個人データ（識別され又は識別可能な自然人に関する情報）	管理者又は処理者	可能（十分性認定）	可能（SCC、ad hoc契約）	可能	拘束力ある社内規程、公的機関の認証、契約の履行の確保、重大な公益・生命の保護等	個人情報保護法制上は、規制なし			
米国	個人情報保護法制上は、規制なし							個人情報保護法制上は、規制なし			
カナダ	個人情報保護法制上は、規制なし							個人情報保護法制上は、規制なし			

データの越境移転に関する研究会 - 3．各国データ関連規制の現状②

	越境移転規制							国内保存・国内保管義務			
	法令名	規制の対象となる情報	規制の対象者	越境移転が許容されるための要件				法令名	規制されるデータ	規制の対象者	義務の内容
				当局の認証等	所定の契約	本人の同意	その他				
中国	個人情報保護法	個人情報（識別され又は識別可能な自然人に関する匿名化していない情報）	個人情報取扱者	他の手続（本人同意）と組み合わせて可能（※）	他の手続（本人同意）と組み合わせて可能（※）	他の手続（安全評価等）と組み合わせて可能	安全評価、法令の定めるその他の条件（※）	個人情報保護法	個人情報	①国家機関、②重要情報インフラ運営者、③一定数に達する個人情報の取扱者	国内保存義務・安全評価
										個人情報取扱者	国外の政府機関への提供につき主管機関の認可
	サイバーセキュリティ法	①個人情報（自然人の身分を識別可能な氏名等の情報）、及び②重要データ（国の安全、経済発展等に密接に関連するデータ）	重要情報インフラ運営者	（規定なし）	（規定なし）	（規定なし）	安全評価	サイバーセキュリティ法	個人情報及び重要データ	重要情報インフラ運営者	国内保存義務・安全評価
	データセキュリティ法	国の安全・利益や国際的義務の履行の維持に関連する管理品目のデータ	（規定なし）	（規定なし）	（規定なし）	（規定なし）	輸出管理	データセキュリティ法	重要データ	重要情報インフラ運営者	国内保存義務・安全評価
										その他のデータ処理者	別途法令で定める
		重要データ	重要情報インフラ運営者	（規定なし）	（規定なし）	（規定なし）	安全評価		（規定なし）	中国国内の組織又は個人	国外の政府機関への提供につき主管機関の認可
			その他のデータ処理者	（規定なし）	（規定なし）	（規定なし）	別途法令で定める				

※重要情報インフラの運営者又は取り扱う個人情報が一定数に達する個人情報取扱者に該当する場合には依拠不可

データの越境移転に関する研究会 - 3．各国データ関連規制の現状③

	越境移転規制							国内保存・国内保管義務			
	法令名	規制の対象となる情報	規制の対象者	越境移転が許容されるための要件				法令名	規制されるデータ	規制の対象者	義務の内容
				当局の認証等	所定の契約	本人の同意	その他				
インド	個人情報保護法制上は、規制なし							支払システム情報の保存に関する政令	支払システム情報（エンドツーエンドの取引詳細及び情報）	認可対象となる支払システムの提供者	国内のみでの保存義務
								電気通信分野における統一ライセンス法	サービス利用者の財務情報及び利用者情報	電気通信サービス事業者	国外への移転禁止
ベトナム	個人情報保護に関する政令案	個人情報（個人に関する情報、又は特定の個人を識別し若しくは識別可能な情報）	個人情報に関係する機関、組織及び個人	他の手続（同意、国内保存等）と組み合わせて可能	（規定なし）	他の手続（国内保存、当局承認等）と組み合わせて可能	（規定なし）	サイバーセキュリティ法	個人情報に関するデータ、サービス利用者の関係に関するデータ又はサービス利用者の作成したデータ	ネットワーク上のサービス提供事業者	国内保存義務及び国内拠点設置義務
								政令72号	（規定なし）	オンラインサービス事業者	国内サーバー設置義務
インドネシア	2019年政令及び2016年省規則	個人情報（直接又は間接に個人を識別できる情報）及び個人データ（保管・管理され、秘密性が保護されなければならない情報）	電子システム提供者	（規定なし）	（規定なし）	（規定なし）	通信情報大臣との連携	2019年政令	（規定なし）	公的機関から任命された電子システム提供者	国内での管理・処理・保存義務
	個人データ保護法案	個人データ（保管及び管理された一定の個人データであって、その秘密性が保護されるべき情報）	管理者	（規定なし）	可能	可能	移転先国の規制の同等性、国家間同意の存在	金融庁規則	（規定なし）	ノンバンク金融機関、商業銀行等	国内保存義務

注：水色部分は法案段階のもの

データの越境移転に関する研究会 - ４．まとめ

- これまでの検討結果を踏まえ、今後の検討方針として、以下の**DFFT具体化に向けて核となる５つの領域**を特定。

透明性の確保 – Transparency

データの越境移転に関する規制について、透明性確保に関する課題を共有するとともに、その改善に向けた国際協力の内容（例えば、情報共有、通報制度、ガイドラインやベストプラクティスの共有など）の検討を行う。

技術と標準化 - Technology and Standardization

第三国へデータを移転する際にプライバシーやセキュリティ等を確保する上で、目安となるような技術や、その技術の実装に係る標準について、国際的な理解と議論を喚起し、産業界等のステイクホルダーに対して連携・関与を求める。

相互運用性 – Interoperability

データの越境移転に係る各国国内制度が異なることを前提に、既存の認証制度を含め、「相互運用性」を確保するための政策オプションの調査・検討を行う。

関連する制度との補完性 – Complementarity

データの越境流通に係る既存の通商ルールや一般原則に加え、プライバシーやセキュリティ分野におけるデータ取扱いに係る議論などとの相互補完的かつ調和した形で検討を進める。

DFFT具体化の履行枠組みの実装 – Implementation

DFFTのビジョンに賛同が得られた国との間で、例えば、透明性確保のため各国の法改正に関する通報制度や関連する取り組みに係るレビューなど、DFFTに親和的な政策を推進するための協力枠組みのあり方を検討する。

（参考）内閣官房 データ戦略TF 包括的データ戦略（令和3年6月15日）

ビジョン 現実空間とサイバー空間が高度に融合したシステム（デジタルツイン）により、新たな価値を創出する人間中心の社会

データ戦略のアーキテクチャ

人材・セキュリティ

- 戦略・政策
- 組織（行政／民間）
- ルール（データガバナンス／連携ルール）
- 連携基盤（ツール）
- データ
- 利活用環境
- インフラ

第一次取りまとめ	包括的データ戦略　検討項目
データ戦略の理念とデータ活用の原則の提唱	・**データ活用原則** （①データがつながり、使える、②勝手に使われない、安心して使える、③みんなで協力する） ・**行政におけるデータ行動原則の構築** ①データに基づく行政(文化の醸成)、②データエコシステムの構築、③データの最大限の利活用 ・**プラットフォームとしての行政が持つべき機能**
社会実装・業務改革 デジタルツインの視点で ビジネスプロセスの見直し	・**デジタル庁の策定する情報システムの整備方針にデータ戦略を反映**
トラストの枠組み整備 トラストの要素（意思表示の証明、発行元証明、存在証明）を整理	・**トラスト基盤の構築（認定スキームの創設）** 【デジタル庁を中心として関係省庁が協力して、2020年代早期の実装を目指す】 ・**トラスト基盤構築に向けた論点整理** （トラスト基盤の創設[各プレイヤーの役割の明確化]、認定基準、国際的な相互承認　等）
プラットフォームの整備 分野共通ルールの整理 分野毎のプラットフォームにおける検討すべき項目の洗い出し (官民検討の場、ルール、ツール等)	・**データ連携に必要な共通ルールの具体化、ツール開発** ・**データ流通を促進・阻害要因を払拭するためのルールの整理** （意図しないデータ流通・利用防止のための仕組みの導入／ロックイン防止 等） 【デジタル庁と知財本部事務局は、2021年末までにガイドライン策定】 ・**重点的に取組むべき分野(健康・医療・介護、教育、防災等)のプラットフォーム構築** 【関係省庁はデジタル庁と協力して、2025年までに実装を目指す】 ・**データ取引市場のコンセプトの提示**
ベース・レジストリの整備 **オープンデータ** **データマネジメント**	・**ベース・レジストリの指定**（法人３情報、地図情報、法律・政令・省令、支援制度　等） ・**ベース・レジストリの整備に向けた課題の抽出と解決の方向性の検討** 【デジタル庁と関係省庁は協力して、2025年までの実装を目指す】 ・**データマネジメントの強化／オープンデータの推進**
引き続き検討すべき事項 データ利活用の環境整備 民間保有データの 活用の在り方 人材／国際連携／インフラ	

デジタルインフラ	・通信インフラ（Beyond 5G）（2025年大阪・関西万博にて成果提示）、計算インフラ（富岳等コンピューティングリソースの民間利用）、半導体産業基盤の強化、データ取扱いのルール等の一体的整備
人材・組織	・データ戦略に必要な人材像、データ整備・AI活用を含むデータ戦略責任者の設置
セキュリティ	・セキュリティバイデザインの推進、安全安心なサイバー空間の利用環境の構築
国際展開	・理念を共有する国との連携や様々なフォーラムにおけるDFFTの推進 （貿易、プライバシー、セキュリティ、トラスト基盤、データ利活用、次世代インフラ） ・G７DFFTロードマップへのインプット【2023年G7日本会合を見据え成果を目指す】

来年度の取組（案）

- 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。