

「産業データサブワーキンググループ」

第2回議事要旨

【概要】

- 日時：令和6年7月30日(火) 13:30-16:00
- 場所：オンライン会議

【議事要旨】

1. 開会

2. 第1回WG振り返り、本日の進め方

3. プレゼンテーション・事例のご紹介

- ファクトリーオートメーションの事例を紹介する。製造現場のセンサーや機器から得られるデータを自社クラウドシステムに集約し、データ分析・利用することで、遠隔での現場状況把握、異常の早期検出、トラブル復旧を実現する。機器を海外顧客に販売したり、国内のお客様が海外工場で使う場合に、日本のクラウドシステムに移転する際に、データ越境が発生する。対象データは機器の稼働データであり、個人情報情報は基本的に含まれない。
- データ越境に伴う留意点として、本事例ではEU、中国、台湾、インドからのデータ越境が発生する際のリスクについて、3つの観点から検討した。1つ目は越境移転のための体制整備義務を負うことがあるか、2つ目が当社または利用者がデータ国内保存や現地人スタッフ監理などローカライゼーションの義務を負うか、3つ目が当社または利用者がインシデント報告義務などサイバーセキュリティに関する義務を負うか、となる。
 - ◇ 結果的に中国からデータ越境させる場合に、当該国の外資規制やサイバーセキュリティ法に照らし、中国国内でデータ保持・運営が必要であるということが判明し、運用面での難しさ・コストの観点からハードルが高く、中国からの越境移転を保留・取りやめた。
 - ◇ なお、データ越境以外の検討論点として、外資系企業の参入可否・許認可規制、プラットフォーム・デジタルサービス事業者規制、クラウドサービスシステム設計の規制、電気通信事業規制、AI関連規制、顧客とのデータ取扱いの条件なども検討された。
- リスクの対策として、本事例では中国からのデータ越境を回避したことが主要な対策と考えられる。またデータの共有・利用に関して、顧客とのデータ取り扱い条件も定められている。
 - ◇ 顧客との取り扱い条件は、一般的な秘密保持契約（NDA）として、第三者への開示禁止、目的外利用の禁止が設けられることが多い。一方、契約はデータ利活用における障害にもなりえるため、当社ではできる限り開示元が特定されないデータについて、製品・サービス向上のためにデータを自由に使える契約条件にする方針で、社内を啓発している。
 - ◇ 欧州データアクトにおいて、データ共有の契約書モデルのドラフトが出ると伺っているが、できる限りデータを自由に使える形でのモデルになることを期待している。一方、データを自由に使えることと、営業秘密の区分が難しく、今後重要な論点になると考えている。

- 関連する対策として、全社横断的なデータ利活用を促進するため、昨年4月にDXイノベーションセンターを設立した。データ分析基盤、WebAPI連携基盤、お客様情報基盤などを整備し、事業部横断でのデータ利活用を進めようとしている。
- また2023年に産業サイバーセキュリティ研究会に参画した際の提言となるが、産業データに関して各国でルール整備が進められているところ、個人データにおけるGDPRの充分性認定制度に該当するものが産業データでも定義されると有用と考える。

- 社内で複数の部門にヒアリングを行い、確認したいいくつかの産業データ流通の実例を紹介したい。
- 1つ目が、サイバーセキュリティの監視データの例となる。EUに海外関連グループ会社があり、ITオペレーションのプロキシログを取得しているが、その中に閲覧されたURLサイトなど、個人情報に該当する情報が含まれる。データ越境においては、プロキシログは越境をさせずに現地で分析し、分析結果だけを国内に移転・共有する形で対応している。
- 2つ目が、海外グループ会社の人事情報の例となる。こちらについては、現地の海外子会社、本社双方で法務に弁護士を立て、各国の法制に基づく対応を確認・実施している。
- 3つ目が、EU地域へ制御装置を販売し、装置からのデータを取得する例となる。EUの顧客に対して、EUにおけるサービス事業者・インテグレーター経由で機器を販売・設置し、保守を実施する。EU側で生成されたデータが日本に移転されることで、データ越境が起こる。
 - ◇ データについて、特にEUのデータアクトの影響が気になる。データには、機器メーカー・ベンダーが利用・分析するための保守データと、ユーザーが確認・利用するための稼働データが存在する。今回Data Actにおいて、保守データも対象となる場合に、これまでベンダー独自で保有していた「収集データの工夫、アイデア等」が外部コンペティターに流出する懸念がある。さらに、制御装置には機器を制御するための各種データも含まれる。この制御データにはメーカーとしてのノウハウが詰まっており、開示対象になることは避けたい旨も社内で言及された。
 - ◇ 一方、ユーザーが使用する稼働データに関しては、基本的に顧客内での業務改善・運用の効率化に利用されるものであり、手続き面での課題・問題がなければ、ベンダー視点での影響・リスクはあまりない認識となる。ただし、GDPRに該当するデータが含まれる場合には、越境において対応が必要となる。

- 当社ではソリューションとして、様々なオファリングを提供し、データ流通・分析を行っている。最近では、DXあるいはサステナビリティトランスフォーメーションに関連するソリューション提供も増えている。本日は、典型例として2つほどご紹介させていただく。
- 1つ目は、サプライチェーンリスクのマネジメントの例となる。顧客企業の取引先データ、保険会社が持つ地震・災害確率などのリスクデータを掛け合わせ、リスク算出とマッピングを行い、業務計画やBCP対応の策定を支援する。
 - ◇ サブシステムとして、企業ごとのサプライチェーン情報、サプライチェーンリスクに関連する外部データソースが存在し、リレーショナルデータベース間での連携・アクセスや、Web API、Excel・CSVによるデータ連携を行っている。様々なサブシステムが国境をまたぐ場合に、データ越境が発生する。

- もう 1 つは、カーボンフットプリント・ESG の情報開示ソリューションとなる。サプライチェーンのリスクマネジメントの例と同様、様々なデータソースからデータを収集し、可視化・情報管理・分析及び、意思決定やシミュレーションを行うことができる。
 - ◇ こちらも同様に、複数のサブシステムで構成され、同様にサブシステムの間が国境をまたぐ場合に、データ越境が発生する。
- 前回の整理によると、これらの例は限定提供データに相当すると考える。多くの企業のサプライチェーンは既にグローバル化し、基本的にデータオーナーの許可を得て、国境をまたぐデータ流通が頻繁に行われている認識となる。
 - ◇ また最近日本企業でも M&A が増えているが、M&A が行われると、今までやり取りがない企業が増えるため、データの共有範囲が急に変化・拡大することが生じる。
- 現状システムに繋ぐ際に細かくデータ連携・利用の許可・合意を得ており、連携の手間がかかるが、データ越境にかかる大きなリスクはないと認識している。一方で、今後越境移転規制や、Data Act のような各国法制の変化がある場合に、特定データにアクセスできず、分析や最適化ができなくなる懸念を持っている。
- また最近では、データスペースと呼ばれる活動にも参加しており、サプライチェーンで共通のデータアーキテクチャー、カタログ、セキュリティ基準などが、少しずつ標準化されつつある。これらが普及すると、工数がかかる利用許可や、取引ごとのデータ抽出の手間が大きく削減できると期待される。
- 第 1 回における座長の総括において、近年電池規則やエコデザイン規則といったような、データの公開・共有を強要するルールの整備が急速に進み、対応方向性の検討が重要とコメントがあった。今回、関連した事例を紹介したい。
- 自動車業界が直面する欧州電池法規は、サーキュラーエコノミーと呼ばれる天然資源から廃棄までの一連のサイクルの中で、責任ある調達、リサイクル材確保、カーボンフットプリント管理・宣言などが求められる。特にカーボンフットプリントに関して、2025 年後半には CFP 宣言、企業デューデリジェンスは同年 8 月に確保されていることを宣言しないとヨーロッパで車を上市できないという法律となる。
- 蓄電池に関する各国法規制を見ると、ヨーロッパは欧州電池法規と、それに紐づく Catena-X やバッテリーパスポートなどのシステムがある。中国は、CFP 国家標準を形成する動きがあり、それを実現する国家データプラットフォームが構想されている。
 - ◇ データ規制については、欧州は個人情報に関連して GDPR がある。中国ではより厳格となり、個人情報に加えて、データ 3 法という法令が存在し、考慮が必要となる。特にデータセキュリティ法において重要データという定義があり、例えば車両の走行や物流等の経済状況を反映するデータなど広範・曖昧な規定となり、データ越境時には、国家インターネット情報部門に申請し、許可通知を得る必要がある。
- 関連して、2つの課題が考えられる。1 つ目は、サプライチェーンがグローバルで部品・材料を調達する中で、中国の取引先からデータを開示されないと、欧州の電池法規を遵守できない懸念・リスクがある。2 つ目は、中国で総合利用管理弁法という法制が準備中となり、その中で国家プラットフォームにデータをアップロードしなければいけない要件が含まれ、ガバメントアクセスの懸念がある。

- ◇ カーボンフットプリントは、1次だけでなく更に上流のサプライヤーまで遡りデータを取得する必要がある。蓄電池では、上流に中国メーカーが占めており、中国からデータ越境できない場合、サプライチェーン全体のカーボンフットプリントを計算できず、結果として欧州電池法規を遵守できない。
- リスクに対する対策の例として、国家間の話となるが、2024年6月に中国のCAC（国家インターネット情報弁公室）と、ドイツの連邦デジタル交通省が、「データ越境移転における中独協力に関する覚書」を結んだ。こうした企業の公平・公正なビジネス環境構築のための、国家間での交渉・交流の動きも進んでいると理解している。
- 本協会は、製造業・ロボットに関連する国内企業・団体に加入いただいております。また日・独の連携協力を民間で進める位置づけにもある。欧州の代表的なデータスペースとコミュニケーションも頻繁に行っており、本日はデータ連携に関わる背景・動向として、重要な要素・ピースをいくつかご紹介させていただきたい。
- 欧州を中心にサーキュラーエコノミーの検討が進んでいる。製造業からすると、物の売上が落ちることに繋がる中で、欧州では物を起点にサービスを強化する動きが加速化し、必然的にデータの利活用の重要性が増している。
- データスペースに関する欧州の危機感と選択について、2018年頃に欧州・ドイツ関係者と議論する中で、当時GAFAsをはじめ米中プラットフォームがグローバルを席巻し、時価総額や投資額は、欧州全体で東になっても追いつかない状況と話されていた。同じアプローチでは負けるため、欧州型データスペース・連携基盤ではデータ主権というコンセプトを打ち出し、データを集約せずデータの場所、保有者、アクセスを管理するアプローチを選択した。そうしたデータスペースの上に、更に欧州のデータ規制が重なり、織り込まれている印象を受ける。
- ビジネスエコシステムの観点として、システムだけでなく、利用者の観点も含まれる。横軸にシステムが分散型か中央型か、縦軸に求められる利用者のケイパビリティが高いか・低いかで、各地域・国の位置づけのマッピング・整理を試みた。
 - ◇ 欧州は分散型で、利用者の高度なケイパビリティを要する位置づけとなる。一方で、実態として欧州でも利用者のケイパビリティが追い付かず、企業のデータガバナンスを向上させるため、急いで環境整備を進める動きがあると漏れ聞こえている。
 - ◇ 日本の現在地は、左下にクエスチョンマークで記載している。ウラノスなどシステムの検討はされる一方で、企業のケイパビリティとしてまだデータガバナンス・マネジメントできている企業は少ない認識となる。特に、規制ドリブンで対応までのタイムリミットのある場合、システム側である程度サポートが必要と考える。
 - ◇ アメリカでも、データスペースに近い検討・取り組みが幾つか始まり、自由度は持たせたい一方、企業が使いこなせる仕組み構築を目指している。事例として米オークリッジナショナルラボラトリーが挙げられる。
- データスペースの構築には標準化も重要である。特に欧州は標準化が非常に速く、強いことが見てとれる。今年4月のハノーバーメッセにおいて、様々なデータスペースの紹介がされており、本協会でも関連してData Actのスタディ・把握を試みた。欧州のようなデータ共有を前提としつつ、法令やアクセス制御をかける考え方と、日本・米国のような契約ベースで進めるアプローチは、データの取り扱いに概念的な違いがあると感じ、法規制の観点からの解釈もポイントになると感じる。

- 本日は、クラウドコンピューティングに関して、弊社の事例に基づきケーススタディをご説明する。
- クラウドのデプロイメントモデルには、旧来のパブリッククラウド、プライベートクラウド、ハイブリッドクラウドに加え、最近ではマルチクラウド、インタークラウド、フェデレーテッドクラウドなど多くの形態が存在し、顧客から見たクラウドサービス事業者の先は、かなり複雑になっている。またクラウドサービスのカテゴリとしても、IaaS、PaaS、SaaS が存在する。
- 組織とデジタル主権の要件として、インターオペラビリティに加えて、データのポータビリティと、アプリケーションのポータビリティも考慮する必要がある。それら要件を念頭に、3つの問題を記載している。
 - ◇ 1つ目は、例えばシステムのインターオペラビリティなど、純粹にデジタルプラットフォームの問題になる。2つ目は、例えば、国をまたがりデータをやり取りする際に企業が定めるコンプライアンスなど、組織の自立性を考慮する必要がある。さらに、国家のデジタル主権の問題が存在する。今回議論するのは、3つの問題が重なった領域と理解している。
- クラウドコンピューティングにおける主権として、3つの観点が存在する。
 - ◇ 1つ目は、データレジデンシーとして、データは指定された物理的な場所に保存され、その場所を顧客が選択できることが求められる。2つ目は、データ主権として、保存されたデータは、保存・処理される国の法規制の対象となり、また顧客は自らのデータアクセスを完全に管理できることが求められる。最後に、運営上の主権として、サービスの信頼性と確実性、クラウド運用のコントロール、法的・政治的な信頼性等が必要となる。
- 弊社では、6つのデプロイメントモデルを提供し、主権の問題に対応しようとしている。大きく分けて、自社で投資したデータセンターで運用するモデルと、お客様が投資し運用するモデルが存在し、各国や各社が定める機密性要件に合致するよう設計されている。またこれら6つのデプロイメントモデルでは基本的に同じ技術が採用されている。
 - ◇ パブリッククラウドは、24カ国37のクラウド・リージョンをカバーしている。なお、データセンター差し押さえ・技術情報流出の懸念から、中国にはデータセンターを持っていない。Huaweiの事件が起こった際に、すべてのデータセンターおよび、ソースコードを同国から引き揚げた経緯がある。
 - ◇ Dedicatedリージョンは、お客様のデータセンターの一面で、自社のデータセンターを動かすモデルとなる。ネットワークも区画で分離しているため機密性が高く、またコンプライアンスも国際的なコンプライアンスを前提に、顧客専用のコンプライアンスを付与することができる。
 - ◇ 次に特定地域に向けた、European Union Sovereign Cloudというモデルがある。こちらは自社のデータセンター内に、EUリージョン向けの特別なデータセンターを設立し、グローバル向けデータセンターとはハードウェアのラックから完全に切り離し運用するモデルとなる。特筆すべきはコンプライアンスであり、特別にEUの担当者が存在し具体的な要件を作りこんで、運用している。
 - ◇ 企業が弊社のクラウドインフラストラクチャーを導入し、特定のニーズに対応してカスタマイズ・拡張できるモデル（Oracle Alloy）もある。構築・運用の柔軟性が高く、ロケーションとして企業のデータセンターはもちろん、複数ロケーションも選択できる。運用に関しても、例えば日本人がオペレーションしなくてはいけない場合に、日本人による運用を選択できる。例えば、経済安全保障推進法が指す基幹インフラに対しての適用などパブリッククラウドでは支えきれないシーンに有効である。

- ◇ 政府、防衛、および諜報機関向けのクラウドサービスも存在する。英国政府向けに2つのデータセンターを運用しており、UK Oracle がグローバルデータセンターとは完全に区画を切ってオペレーションしている。オーストラリア政府も同様のモデルを採用している。さらに、本当に最高機密が求められる場合に、例えば、米国国防総省の最高機密を扱う場合などはインターネットコネクション自体を切るモデルがあり、これはエアギャップ（Air-Gap）と呼ばれている。
- クラウドサービス事業者には、データ保管の場所、アクセスコントロール、オペレーションサポート、規制要件、インターネット接続性/エアギャップの要件が求められると整理できる。
 - ◇ セキュリティ要件も重要な要因ではあるが、加えて、インフラストラクチャーとしてのサービスの信頼性と確実性および、機能の安定性がある。これまで DFPT や知的財産権などの議論では、セキュリティやプライバシーに焦点が当てられたことが多いが、サービス信頼性、機能の安定性がないと、データ共有・利活用の根幹が成り立たない。

4. ディスカッション

- 今後のマニュアル取りまとめに向けて、整理の視点をいくつかコメントする。人事やセキュリティ監視など、自社オペレーションでデータ越境するケースは、業種を問わず汎用的で参考になると感じた。また規制に対応する上での越境もある。さらに、本日プレゼンされた産業機器のデータ、またサプライチェーンのデータ共有は、日本企業の典型的なモデルで、掘り下げるべきケースになると感じた。類似して近年は、IoTの進化によるコネクテッドサービス、関連 SaaS サービスも出てきており、越境のパターンの類型化にも反映できるとカバー範囲が広がると感じた。
- また本日はサービス提供者・ベンダーの立場からのケースご紹介が多かった。BtoB のケースは概ねカバーされたと感じる一方で、BtoC のケースとして、自動車のコネクテッドサービスや、家電なども想定される。加えて、サービスを受けるユーザーの視点で、契約や利用の留意点も深掘できると良いと感じた。
- 整理すると、分類としてモデルとして自社業務・利用、規制対応、保守・コネクテッドサービス、3つほどのモデル、それぞれにベンダー・利用企業の立場、さらにサービスによって BtoB、BtoC が存在することを意識して整理を進められると、今回のマニュアルの有用性が非常に高まると感じた。
- プレゼンテーションの中で、営業秘密が触れられていたが、営業秘密に対して、事前の対応が重要になると考える。漏えいを防ぐために、越境元・越境先の関連法規制を把握の上、契約等の手当を行うケースが企業実務では多いと認識している。もし移転先の法規制などにより、十分な保護を受けられないと考える場合に、重要データの移転を見送ることも考えられる。
- 営業秘密に関連して、Data Act の懸念に賛同する。特に、収集データから企業の工夫・アイデアが漏れる懸念については、欧州当局に政策提言を行った。現状の Data Act では、データ保有者がデータの開示により深刻な損害が発生する場合に開示を拒否できる旨追記されているが、その実運用は注視が必要と考える。
- データ越境には複数部署をまたぐ検討が必要となり、社内連携が重要と考える。全社横断でのデータ連携組織の設立に関連して、社内連携の工夫があればご教示いただきたい。
 - ◇ 当初は技術的な基盤整備が中心だったが、段々とソフト面の整備として、法的な対応も含め、全社共通するデータ利活用の共通事項・ルールを抽出している。

- サプライチェーンリスク管理の事例において、情報基盤におけるデータの信頼性・真正性を担保する手法があればご教授いただきたい。
 - ◇ データの真正性には、技術的には最近ではブロックチェーンが使われることが多い。ただし前提として、正しい取引先か、あるいはデータ入力を行っている個人や装置が特定・認定できているかも併せて保証する必要がある。
- 蓄電池のトレーサビリティについて、海外連携の課題や工夫などありましたらご教示いただきたい。
 - ◇ 各地域にデータプラットフォームが構築された場合、サプライヤーからすると、異なる OEM・データプラットフォームに同じデータを共有する必要がある。データプラットフォーム間でのインターオペラビリティがあると望ましく、またガバナンスとして、データプラットフォーム参加者のトラスト、クレデンシャルなどの整合性の担保も論点となる。
- プレゼンテーションの中で、クラウドサービスにおける、データのロケーション、データ管理者について言及した。事例において、例えば蓄電池ではどうなっているか、ご教示いただきたい。
 - ◇ アーキテチャー設計は IPA が行っており、詳細はそちらにお伺いすると正確と考えるが、理解の範囲内では、データ主権の確保を念頭に、レジデンシー・ロケーションはどこに置かれていても良いということが尊重されていると伺っている。
 - ◇ 例えば中国のサプライヤーにおいて、中国内にデータがあり、それを日本のデータベースに送るのか、または OEM がデータを全て管理するのかなど、またわかる範囲で詳細をご教示いただきたい。
- プレゼンテーションをお伺いし、越境移転において個人データの問題は引き続き重要だが、産業データについても、やはりリスクや障害が存在すると認識を新たにした。例えば、EU の電池規則との関係でも中国のデータローカライゼーションの影響が触れられ、特定地域を切り出して完結する形でビジネスができる場合ばかりではなく、中国を含め地域間でデータ共有を進めないとビジネスができない場面も出てきているため、データローカライゼーションのリスクは非常に重要と感じた。
 - ◇ データローカライゼーションは、規制拡大のトレンドについて OECD のレポートなどでも触れられており、企業として問題意識を持っていくべき論点と改めて認識した。
 - ◇ また本日のプレゼンテーションでは、自動車産業の電池規則が触れられたが、人権や環境等のサステナビリティの観点から、トレーサビリティが求められていくトレンドが強化されていることを踏まえると、今後鉄鋼や金属等の他の分野でも同様の課題に直面することが考えられる。
- データローカライゼーション以外には、データのセキュリティや、産業競争力や安全保障の観点からのガバメントアクセスへの対応も非常に重要と考える。
- また産業データにおいて、データの移転先・保管先のセキュリティ、ガバメントアクセスなどの影響・評価の考え方も論点となる。個人データでは検討が進んできているが、産業データでも等しく掘り下げる価値があると思う。
- データ越境のリスクに関して、データの性質、データの処理方法、ロケーションに起因するものなど多角的な物差しがあると感じた。また対策において、リスクを意識して事前対応するという話、リスクが顕在化した後に事後対応をするという話、そうした観点からのリスク対応の分類も、整理する上で有益ではないかと感じた。

- リスク評価について、一般的には発生可能性・蓋然性と、発生時のインパクトの大きさの掛け算で算出されると考える。例えば、ガバメントアクセスは、可能性としては高くないが、発生時に非常に大きいインパクトをもたらすということは、個人データの事例を見ても明らかと考える。
- 企業がデータガバナンス、マネジメントの仕組みをしっかりと持つことがデータ越境の大前提と認識しており、いかに企業を啓蒙し、同時に相手国の企業のデータガバナンス・マネジメントが十分か確認することが重要と感じる。
- データ越境において、企業から見れば営業機密が守れる、あるいはサステナビリティ規制に対応できるなどが重要となり、データ流通のルールと合わせて、目的と守らなければいけないことを整理できるとよいと感じた。
- 企業がクラウドサービスを利用する場合に、そのサービスがどのような条件で運営されているのか、ユーザーにとって気になる。欧州の EUCS（EU Cloud Certification Scheme）など、クラウドサービス認証の仕組みなど、関連情報を継続的に企業に発信・提供される仕組みがあると有用と感じた。
- 全社横断のデジタル基盤において、具体的にどのようなグループ企業や部署が、特に参画・利用のモチベーションが高いか、ご教示いただきたい。
 - ◇ 弊社はいくつかの事業本部に分かれているが、基本的にはデータを取り扱う全ての事業本部が、デジタル基盤に参画する形で進められている。
- サプライチェーンリスク管理のデータプラットフォームに関して、多くの産業でカーボンフットプリント可視化・共有が盛りあがっている認識だが、具体的にそのような産業群・企業が、ユーザーとして多くなっているか。また企業における競争領域のデータも含まれる認識だが、どういったモチベーションで産業群がまとまっているかもご教示いただきたい。
 - ◇ 産業として、まず自動車の EV バッテリー関連が、直近ニーズとして一番大きいと感じる。またヨーロッパで ESG 情報を会計報告に織り込む動きが始まろうとしている中で、電気業界の関心が高まっており、自社でも対応を始めようとしている。加えて、直接の会話・把握しているわけではないが、CO2 排出量の大きな産業として、石油・エネルギー系、鉄鋼なども想定される。
 - ◇ またカーボンフットプリントに近いテーマとして、サーキュラーエコノミーが挙げられる。これもヨーロッパのデジタルプロダクトパスポートに対する問い合わせが増えており、繊維業界、電気業界などの関心が高まっている。
- 蓄電池プラットフォームに関して、中国サプライヤからのデータ越境・情報取得の懸念が触れられたが、具体的にどのような部品・素材が想定されるか。またドイツが中国当局と覚書を結ぶ一方、米国では大統領令でコネクテッドカーの情報取得の懸念が挙げ牽制を強めている。自工会として中国に対する対応・立ち位置の方向性の認識があれば、ご教示いただきたい。
 - ◇ 対象部品・素材はまだ確定していないが、現時点の想定として、例えば電極やセパレーターなどが挙げられる。今後、対象を正確に確認していく必要がある。
 - ◇ 中国におけるデータローカライゼーションの懸念がある中、自工会として、経済産業省自動車課とも連携し、対応を合わせていくスタンスとなる。

- サステナビリティに関連して、欧州電池法規など、今後企業にとって予期せぬ負荷がかかるポイントがあれば、検討に織り込むべきと考える。また EUCS についても、データ主権に基づく制度となるため、今後検討に織り込めると良い。
- リスク可視化に関する法規制に関して、過去調査では、具体的にどのような対象国が入っていたか。
 - ◇ 複数国の情報が含まれるが、まずは日本企業への影響の大きいアメリカ・欧州・中国をメインにまとめていくということを考えている。
- GDPR の十分性認定制度について、どのような内容をイメージされているか。
 - ◇ 産業データに関して、例えばセキュリティ基準が複数国で策定されている認識だが、個社ですべての情報を把握するのは難しい側面もあるため、認定制度としてわかりやすい形で要件が整理されると、有用性が高いと考える。

- 改めて、本日のような具体の課題と取り組みをご紹介いただく機会は本当に貴重と考える。既に言及されたように、個人データに関しては、これまでに議論がなされ問題も共有されている。しかし産業データについて、ガバメントアクセス、Data Act、あるいはエコデザイン・電池規則など、実態の悩みがまだ国内でも共有されていないことが理解できた。まさにこうした観点からガイドブックを取りまとめていくことの価値が高いことを改めて感じ、取りまとめに向けて是非引き続きご協力を賜りたい。

5. 閉会