令和５年度規制改革推進のための国際連携事業
我が国データの国際的な流通実態及び技術動向に係る調査

報告書

令和６年３月

野村総合研究所

目次

1　エグゼクティブサマリ

デジタル技術や AI の利活用が進む中、国際的なデータ量は増加の一途を辿っている。我が国は 2019 年に信頼性あるデータ流通（DFFT：Data Free Flow with Trust）を提言してから、その実現に取り組んできた。これまで DFFT における議論では個人データ（個人情報）が中心であったが、産業データ等の非個人データを活用した新たな価値を創造する流れの中、非個人データ（営業機密や知的財産権、安全保障上重要とされるデータ等）の保護に関する議論に注目が集まっている。

本調査では、産業データに焦点を当て、データの流通と保護の実態、信頼性を担保する技術動向、さらにデータの越境移転におけるリスクや対策についての調査を実施した。

諸外国における非個人データに係るデータ保護規則に関する動向として、中国では非個人データの保護に関する法律が存在する。これにはデータの越境移転や国内保存に関する規制が設けられており、具体的な規制対象範囲は政府が定めることとなっている。また米国では包括的な非個人データ保護法は存在しないが、代わりに安全保障目的の技術保全規制や秘密保持命令制度があり、政府機関がクラウドサービスを利用する際のセキュリティに関する制限が存在する。EU では経済安全保障戦略の下で重要技術リストが作成され、流出リスクが評価される。また、クラウドサービスの国外依存から脱却や、デジタル主権追求のためのデータ共有基盤構想も進行中である。

日本企業のデータ流通に関する取り組みとしては、製造業（自動車）で車両データを活用したコネクテッドサービスが広く見られる他、自動車以外の製造業では工場の生産管理を効率化するためのデータ活用、貿易・物流業では貿易実務における商取引データ（注文書、納品書、請求書等）を電子プラットフォーム上でやり取りする等の取り組みが浸透しつつある。またブロックチェーン技術を活用し、輸送貨物に取り付けた IoT デバイスにより温湿度や位置情報等の貨物状態をリアルタイムに把握しつつ、流通上の証跡を管理するサービス等の提供が進んでいる。

企業へのデータ管理に関するインタビューでは、個人データと異なり、非個人データについては社内で統一的な方針や統合的なガバナンスがまだ構築されていない企業も多いことが分かった。またガバメントアクセスに関しては、外国政府により強制的にデータを収集されたとの事例は今回得られなかったが、各企業におけるデータの取り扱いにおいて、オンプレミスでの運用、もしくはクラウド基盤のテナントを日本に限定する等でこれらのリスクに対処しているのが現状である。特に懸念国とのデータ流通においては、法的・技術的措置だけでなく、物理的に切り離す必要があり、このような国で事業を展開していくための対応コストは事業展開の障壁となるだろう。

国内企業がデータの信頼性を確保した形で管理・利活用するためには、法的措置や組織的措置に加えて、秘密計算や暗号化などの技術的措置も重要となる。データ保護の技術は、主に大手の米国 IT 企業や IT ベンダーによって実用化に向けた取り組みが進んでいるが、国内

でも主要企 IT 業や大学機関が連携して実証実験や技術開発が進んでいる。
今後は、国際的なデータ流通量が増え続ける中で、どこまでリスクを許容するか、技術的制約や計算コスト等とのバランスに関する議論が必要となるだろう。

2　背景と目的、調査の全体像

2.1　背景と目的

社会経済活動におけるデジタル技術・AI の利活用は急速に進んでおり、個人情報から衛星データに至るまで、民間事業者の保有するデータ量も増加の一途を辿っている。国際的なデータ流通量も増加している中で、信頼性ある形でのデータ流通はデジタル経済の健全な発展な土台となるという認識の下、我が国は 2019 年に信頼性あるデータ流通 Data Free Flow with Trust を提唱し、その実現に取り組んできた。

IoT やロボティクスの導入が進む中で、特に産業データ等の非個人データが増加し、その活用が個別の企業の競争力にとどまらず、業界等、より広い規模の経済活動に影響をもたらすとして、EU をはじめとした各国において政策的な対応が検討・実施されている。

こうした国際的なデータ流通が進展する中で、 データのセキュリティや知的財産権の保護の重要性も高まっている。秘密計算技術やデータ連携基盤など、信頼性を確保した形でデータを管理・利活用するための技術開発も進んでおり、データの流通実態やこうした技術の発展にも歩調をそろえる形で適切な制度設計を行っていく必要がある。

こうした背景の下、我が国のデータの国際的な収集、利用及び管理の実態、並びに特に知的財産保護やセキュリティといった観点を主としたデータ保護に資する技術に係る調査を行い、今後の政策的検討に資するための情報を収集することを目的として本調査を実施した。

2.2　調査の全体像

以上の背景と目的のもと、本調査は次のタスクを実施した。まず全体として産業データにフォーカスすることとして、次の 3 つのタスクを実施した。

第一に、データに係る実態調査として、ヒアリング調査と文献調査を組み合わせて、日本企業の産業データの流通及び保護の実態を調査した。特に重要かつデータ関連規制に影響を受ける産業を中心に調査することとし、自動車、サプライチェーン管理を中心に情報収集を実施した。

第二に、上記のデータ保護を実施する手段としての信頼性を担保するデータ管理・利活用に関する技術動向の調査である。プライバシー強化技術等、データを保護しつつ活用を推進する技術の動向に関して、文献調査を中心に検討した。

最後に、以上を総合して、日本企業において産業データを越境的に活用する場面において、データの保護に関してどのようなリスクについて、どのような対応策をとればよいかを中心に、検討を実施し、提言を行った。

調査実施タスク	概要
（1）データに係る実態調査（本報告書4.）	産業データの流通実態やその保護の実情について、日本企業へのヒアリング調査、及び関連する文献調査を実施した。
（2）信頼性を担保するデータ管理・利活用に関する技術動向の調査（本報告書5.）	（1）で特定した産業を踏まえ、国内企業の保有するデータの信頼性を確保した形で管理・利活用する技術について、現状の把握と利用拡大にむけた課題特定等、調査・分析を行った。
（3）産業データのガバナンスに関する提言	流通実態とデータ管理・利活用技術を踏まえ、日本企業において産業データを国境を超えて扱う上で、留意すべきポイント（リスクとその対応策）を検討した。

図表 1　本調査における実施タスクとその概要

3　非個人データのデータ保護規則に関する動向

3.1　中国

中国においては、ネットワーク安全法、データ安全法及び個人情報保護法のいわゆる「データ三法」を中心に、非個人情報の越境移転規制や国内保存義務が課されている。規制対象について、主に①重要情報インフラ運営者への該当性と②重要データへの該当性の 2 点に基づき判断される。

①重要情報インフラ運営者は、公共通信及び情報サービス、エネルギー等の「国の安全、国民の経済・生活及び公共の利益に重大な危害が及ぶおそれがある重要な情報インフラ」と定義されるが、具体的な範囲は国務院が定めるとされている。

②重要データは、「ひとたび改竄、破壊、漏洩され、又は違法に取得若しくは利用された場合に、国家安全又は公共利益を害するおそれのあるデータ」と定義されるほか、当局の関係部門が個別に定める「重要データリスト」によっても指定される。例えば、自動車、工業及び情報化分野、中国人民銀行業務分野について、より詳細が定められている。

上記 2 つの観点のいずれにおいても、現状は抽象的な定義にとどまり、具体的な規制対象について政府機関が今後追加することが可能な設計となっている。

3.2　米国

米国においては、連邦レベルの非個人データ保護に関する包括的な法制度は見当たらない。一方、安全保障に関連して重要技術の保全を目的とした輸出規制や対外投資規制、資金提供に付随する技術供与制限による産業技術管理を行っている。

特に国家安全保障の観点から非個人データを含む知的財産を保護する措置として、営業秘密の保護に加え、特許を非公開とする秘密保持命令制度がある。また、連邦政府機関がクラウドサービスを導入する際の認証制度として FedRAMP が存在し、政府のデータ基盤へ

の参加についてセキュリティを中心とした観点から制限している。

3.3　EU

EU では、2018 年に「非個人データの EU 域内自由流通枠組み規則[1]」が定められた。従来、データ流通に関しては個人データを対象とする政策が中心的であったが、経済活動における産業データ等の非個人データの重要性が増す中で、非個人データを対象とする規則が制定された。本規則では EU 域内における自由なデータ流通を確保・推進するため、データローカライゼーションを禁止している。

また、欧州委員会は、経済安全保障戦略の下で重要技術リストを定め、加盟国に対し各分野における技術流出のリスクを評価するよう勧告している。また、加盟国レベルでもクラウドサービスの外資依存からの脱却を目指し、認証制度によってデータローカライゼーションやクラウドサービス提供者の資本構成における国籍制限等、EU 域外企業の参加を制限している。

また、デジタル主権を通じイノベーションを追求する取組みとして、データ共有基盤「Gaia-X」の構想が進められている。Gaia-X では、製品の設計から運用・保守にいたる多くの段階で多様なサプライヤーを含む全体で共有し、設計品質と生産性の向上を図る。開発プロジェクトには欧州企業に限らず、米国や中国等の多国籍企業を含め 300 超の企業が参加し、産業別に具体的なユースケースの検討が行われている。

Gaia-X の理念を自動車産業において実行する取り組みとして「Catena-X」が登場している。自動車産業のバリューチェーンの関係者が参加し、具体的なユースケースに沿って技術基盤やパイロット版のアプリケーションの開発を進めている。

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1807

4　企業のデータ流通に関する事例調査

4.1　企業のデータ流通実態に関する事例調査

企業におけるデータ流通に関する取り組みについて、収集したデータを活用したサービスにおける取り組みについて、公開情報を基に文献調査を行った。対象の業界として、製造業のうち自動車、自動車以外、貿易・物流の 3 つを選定した。

4.1.1 製造業（自動車）

非個人データのうち、車両データを活用したコネクテッドサービスの事例が多かった。コネクテッドサービスにおいては、エンジン回転数や警告灯の車両状態に関するデータや位置情報等、車両から取得した車両データとともに、契約時等に別途取得しているユーザーに関する個人情報の両方を活用するサービスが大半であった。

車両データを活用し、他企業と提携してサービスを提供する事例もみられた。例えば、一般ユーザー向けには、運転傾向を保険料に反映するサービスや、位置情報を基に渋滞情報や道路状況を提供するサービスがあった。また、物流事業者向けに車両データのうち位置情報を利用して最適な配送ルートを案内したり、貨物に関する情報と合わせて発送・配送を管理したりするソリューションを提供する事例もみられた。

4.1.2 製造業（自動車以外）

工場においてデータを活用して生産管理を効率化する事例がみられた。現場の製造機械からリアルタイムで収集したデータを可視化し、最適な生産計画を立てたり、作業員の動作を画像解析して改善に活用したりするため、データを一元管理するシステムを提供している。将来的には工場内に限らず、サプライヤー、部品、製造、品質保証、ユーザー等の各段階のデータベースを統合、集約したデータ活用プラットフォームの構築も検討されている。

また、安定的に調達可能なサプライチェーンの構築のため、自社内の各事業部の半導体に関する調達を一元化する取り組みもみられた。

4.1.3 貿易・物流

貿易実務における電子化のためのプラットフォームの事例がみられた。従来、船会社、保険会社、物流会社、銀行等、多くの関係者の間で紙の文書がやり取りされていたところ、ブロックチェーンによる証跡管理を採用した SaaS サービスに移行することで円滑な取引を実現しようとする取り組みである。先行する海外の貿易プラットフォームは業界や国ごとに分化しているため、複数プラットフォームを連携することを目指している。

また、物流のソリューションとして、輸送貨物に取り付けた IoT デバイスにより温湿度や位置情報等の貨物状態をリアルタイムに把握しつつ、流通上の証跡をブロックチェーンで管理するサービスが提供されている。

中国においても、貿易に関するデータを集約するプラットフォームを構築する動きがみられる。

4.2　国内外企業の公表する透明性レポートに関する調査

4.2.1 国内事業者

国内事象者における透明性レポートの公表状況としては、デジタルプラットフォーム取引透明化法（透明化法）の規制対象となる 7 社を除き、現時点で自主的に透明性レポートを発表している企業は少ない。一方で、徐々に対応する流れも起きてきている。

透明化法では、アマゾンジャパン社、楽天グループ、LINE ヤフー、米 Apple（同社子会社の iTunes)、米 Google、米 Meta に透明性レポート（取引条件などの情報開示、体制整備、実施した措置や概要に自己評価を付した報告書）の提出を義務付けており、規制の対象企業は、EC（電子商取引）では国内流通総額が 3000 億円以上、アプリ市場は流通総額が 2000 億円以上と定められている。

提出が義務付けられている企業以外では、さくらインターネット、CCC、サイボウズ等の企業が透明性レポートを公表しているものの、内容は上記 7 社と比較して必ずしも十分ではないのが現状である。

具体例として、透明化法によって透明性レポートの提出が義務付けられている LINE ヤフーは、半期ごとに透明性レポートを公表しており、ガバメントアクセスの要請件数や対応状況をしている。ガバメントアクセスに関する透明性レポートは LINE サービスとヤフーサービスで分かれており、LINE サービスにおけるアクセス件数は、アクセスを受けた国別に内訳を見ることができる。さらに、LINE ヤフーは、ガバメントアクセスに対するスタンスを明示しており、捜査令状、緊急事態に基づくものを除き、原則として情報を開示しない方針を公表している。

また、提出が義務付けられていないさくらインターネットも LINE ヤフーと同様に半期ごとに透明性レポートを更新しており、ガバメントアクセス等の要請件数を公表している。一方、最新のレポートの分量は 3 ページにとどまり、豊富ではないのが現状である。
デジタルプラットフォームにおける透明性・公正性の担保のためには、企業の自主的な報告書公表もしくは、規制対象を広げる際には、報告内容に強弱をつける必要があるだろう。

4.2.2 国外事業者及び海外動向

国外事象者における透明性レポートの動向として、米 Google と米 Microsoft は、半期ごとに国別のユーザー情報に対するガバメントアクセス件数を公表しており、その内数として秘密保持令を伴う開示リクエストについて公開している。さらに Google は、ホワイトペーパーにてユーザー情報の提供リクエストに対する対応フローを公表している。

またこの 2 社は、米国政府の秘密保持令に対する異議申し立て等、必要以上の情報を求める開示申請の却下や開示状況をデータ主体者へ通知する等のガバメントアクセスに対する透明性を確保すべきとのスタンスをとっている。

しかし、サービスの性質上、Google 及び Microsoft のガバメントアクセスにおける言及は、ユーザー情報や個人データにおける開示要請にとどまっており、営業秘密に関わる産業

データに対するガバメントアクセスへの対応については言及されていないのが現状である。

Alibaba 社については、個人データへのガバメントアクセスの可能性について言及されているものの、上記 2 社と比較して詳細な情報は公開していない。中国政府は Alibaba グループの株式取得を進めており、同社に対する影響力を強めつつあることから、中国政府からのガバメントアクセスの要請に対して拒否できる立場にないことが推察される。

このように、Google や Microsoft などの米国大手プラットフォーマーは、透明性レポート上にてアクセスを受けた国やアクセスの種類の内訳も含めてのガバメントアクセス件数の公表や対応方針の公表も行っている。一方で、ガバメントアクセスの言及は個人データにとどまっており、営業秘密などに係る産業データに対するガバメントアクセスのリスクについては言及されていない。

また、Alibaba 社などの国家権力による影響を強く受けるプラットフォーマーは、ガバメントアクセスに関する情報開示を積極的に行っていない状況も確認された。

4.3　企業のデータ流通実態把握に係る企業インタビューの実施

4.1 章、4.2 章において、公開情報での企業のデータ流通実態に関する机上調査を実施してきた。しかしながら、企業におけるデータ流通の実態把握において、特に非個人データ（産業データ）の扱いに関するデータガバナンス（データの管理体制等）に関する取り組みは、公開されている情報が非常に限られている。またこれらの企業がデータ流通網を構築する上で抱えている課題、特に非個人データの流通が今後活発化していく上で、懸念されるであろう、越境移転やガバメントアクセスへの対応について詳細を確認するために、企業インタビューを実施した。

インタビューの対象企業は、製造業（自動車）、製造業（自動車/自動車部品以外）、貿易を中心に制度面や技術面に関する団体・企業等を考慮し、9 社を選定した。

またインタビュー項目は、下記の 5 項目を中心に、個社の事業内容に応じて追加で聴取している。

（1）貴社におけるデータの取り扱いについて

- 特にサプライチェーンのデータや研究開発データ等の産業データを念頭に置いた際、越境するデータの収集、保管、分析がどのように行われているか。

（参考：想定されるケース）

- サプライチェーンデータの越境流通（外国にある外国企業との共有のほか、日本における外資企業との共有を含む）
- 研究開発に向けた自社製品（IoT 製品等）の越境的なデータの収集、移転
- グループ企業内での移転を含むクラウドの活用による（必ずしも意図的でない）移転
- 開発やアフターサービスの再委託等、ソフトウェアサプライチェーン上の移転

（2）貴社内でのデータ管理について

- （1）のうち、貴社内においてデータガバナンスをどのように担保しているか。また、どのような貴社内の組織において行われているか。

（3）ガバメントアクセスの実例及びその対処について

- 特に個人情報保護法上の手当てのない、産業データに対して、外国政府により強制的にデータを収集される/される可能性がある事例（ガバメントアクセス）について、自社またはデータの共有先/元が経験したことがあるか。
- 上記について、どの程度リスクを意識してデータガバナンスを構築しているか。またどのようなデータについて、どのような保護措置を行っているか。

（保護措置の例）

- 法的措置：契約での共有範囲の規定、外国政府への提供の制限に関する義務の規定、等
- 技術的措置：暗号化や秘密計算等データの移転リスクを低減させる措置、等
- 組織的措置：委託先や企業内のデータ共有範囲の変更等のデータフローの改変、等

（4）各国のデータ保護規制について（途中追加）

- 貴社が事業を展開している国・地域におけるデータ保護規制について、課題もしくは懸念を感じている点はあるか。
- （貴社が欧州で事業を展開されている場合、）特に欧州データ法（Data Act）について、貴社のビジネスへの影響を分析しているか。分析した際に、懸念している点はあるか。

（5）データ保護規制に関する意見

- 外国政府によるガバメントアクセスへの対処を含む、越境データの管理に際して、日本政府に対して要望はあるか。

5　データ保護の技術的措置に関する調査

5.1　調査の対象とする技術

国内企業の保有するデータの信頼性を確保した形で管理・利活用する技術について、現状の把握と利用拡大にむけた課題特定等に向けた調査・分析を行った。本調査では、データのライフサイクルにおいて、データの有意性を保ったまま「加工・活用」する技術及びデータ流通において重要な「蓄積・保管」「共有・連携」する技術を中心に取り扱う。よって、調

査対象とする具体的な技術は以下 6 つの技術である。調査対象の技術において、技術の概要、技術に関する近年のトレンド/トピック、関連する主要プレイヤーの動向、主なユースケース/事例、技術的課題について調査を行った。詳しい調査内容は、Appendix 4 を参照する。

＜調査対象とする技術＞

- 「加工・活用」に関する技術
  - 秘密計算
  - 連合学習
  - 差分プライバシー
- 「蓄積・保管」に関する技術
  - ブロックチェーン
- 「共有・連携」に関する技術
  - 分散型 ID(DID)とデジタルアイデンティティウォレット(DIW)
  - データ連携基盤

5.2　データ保護の技術動向調査結果

データ保護の技術は主に GAFAM などの大手米国 IT 企業や、IBM 等の IT ベンダーによって実用化に向けた取り組みが進んでいる。国内企業では、NEC や NTT、LayerX、日立などが主要プレイヤーとなって実証実験や技術開発を進めている。また、連合学習や DID(Decentralized Identifiers)等の技術に関しては、大学や研究機関等との連携によって先進的な取り組みが進められている。

具体的な各技術の現状と課題として、データ連携基盤技術は、業界や国境をまたいだデータ流通やシステム連携を実現するための取り組みで、欧州が先行しているが、技術開発以外の課題・調整事項等も多く、実用化前の段階にあるのが現状である。

ブロックチェーン技術は、ネットワーク内の取引データを分散管理する技術であり、改ざんされにくく、多分野で活用されている。医薬品流通など、証跡管理が重要な場面で導入が進んでいるが、取引量の増加に伴う処理速度の低下や、セキュリティ面の懸念等、課題も残る。

秘密計算は、データを暗号化したまま計算処理することで、企業秘密の内容を社外に知られることなく共有・分析等を可能にする技術で、企業間のデータ共有におけるリスクや懸念を低減することができる。一方で、NEC、NTT ら 4 社によって秘密計算の安全性基準を定めた文書の策定等が行われているが、個人データの取扱いにおける個人情報保護的観点での法的該当性などに不明な部分が残っているのが現状である。

差分プライバシーは、統計データに対してノイズを加えることで、統計的な有用性を維持しつつ元データの個人の特定や属性情報の推定を不可能にするためのプライバシー技術であり、Google、Apple 等が活用を進めている。また、米国国勢調査や、あいおいニッセイ同和損害保険株式会社のテレマティクス自動車保険等でも活用されている。一方で、差分プラ

イバシーは、プライバシーとデータの有用性の最適なバランスをとることが難しいのが現状で、導入分野ごとにプライバシーパラメータの合意形成が必要になる。

連合学習は、データを 1 か所に集めず分散している環境に AI モデルを配布することで、データ集約によるリスクを避けながらモデリングする技術で、組織を超えたモデルを構築する際に組織間で AI モデルをやり取りすることで、データ利用の高度化とプライバシー保護を同時に解決することが可能になる。特に製薬・医療分野においての実証実験が進んでおり、データセットの情報漏洩防止や、一部クライアントの異常行動による全体への影響を防ぐため、差分プライバシーを用いたプライバシー保護や、モデルの頑健性が重要になる。

分散 ID（DID）は、ユーザーが自分の属性情報に関するコントロール権を確保した上で、各データ保有者の属性情報のうち必要な情報を、ユーザーの許可した範囲で連携し合う考え方であり、World Wide Web Consortium（W3C）において標準化がされている。また DID の実装としてデジタルアイデンティティウォレット（DIW）があり、「耐改ざん性」等の観点でブロックチェーン技術の活用も期待される。DID と DIW の組み合わせにより、これまでの集中型アイデンティティによる管理から自己主権型/分散型アイデンティティに移行することで、ユーザーは自分のデータをコントロールできるようになるとともに、サービス提供者側もアプリケーション、デバイス、サービスプロバイダーに対してより高い信頼性とセキュリティを担保することが可能となる。EU 加盟国や中国が政府主導による活用検討が進む他、日本では、「Trusted Web」を実現するための取り組みが実施されている。今後の実装における課題として、ユーザーが使いやすい UI 設計や利用意向を高めるインセンティブ設計が必要である他、プライバシー保護の観点でも考慮すべき項目も多く存在する。

5.3　データ保護技術に係る企業インタビューの実施

5.1 章、5.2 章において、公開情報でのデータ保護技術に関する動向調査を実施した。産業データ（非個人データ）を扱う企業の抱える課題、またデータを処理する事業者の課題は何か、またこれらの課題に対して技術面での対応状況はどのように検討されているのかについて詳細を確認するため、企業インタビューを実施した。

インタビューの対象企業は、越境データを利活用する企業目線での実態の他、データ保護技術に関する動向や今後の動きについても把握することを考慮して選定し、インタビューを実施した。

またインタビュー項目は、下記の項目を中心に聴取した。

- 産業データ（非個人データ）を扱う企業の抱える課題、またデータを処理する事業者の課題はなにか。
  - 例：技術そのものへの認知が不足しているのではないか
  - 例：組織・企業のデータ加工・評価技法を使うための知識やスキル不足があるのではないか

- 例：ガバメントアクセスからの保護や安全管理措置等における課題があるのではないか　等

- 技術課題等　・データ保護技術に関する今後の動向をどのようにみているか。また個別の技術（秘密計算、連合学習等）に加え、これらを支える実行環境等の動向及び技術の勢力動向についてはどうか。
  - 例：差分プライバシーのカバレッジも秘密計算に侵食され得る、つまり勢力図が上書きされていく可能性　等
  - ※ 秘密計算の実行環境のひとつである TEE(Trusted Execution Environment)は、Intel SGX が著名のようだが、アーキテクチャの変化によってここ数年で扱えるデータサイズが指数関数的に飛躍しているため、秘密計算が他の技術の上位互換として塗り替えられるのではないかと推察。（経済産業省コメント）

- データ保護技術が抱える課題や懸念事項（法制度や環境要因等）はなにか。
  - 例：法規制や環境の整備、企業側の理解が進んでいないため、実運用までには時間を要する
  - 例：現行法制度とのコンプライアンスに障壁があるのではないか　等

5.4　インタビューの結果等から得られた技術の利用拡大に向けた論点

国内企業の保有するデータの信頼性を確保した形でデータを管理・利活用するためには、法的措置や組織的措置以外で、技術的措置（秘密計算や暗号化等）によるデータ流通におけるリスクの低減が必要となる。

5.4.1 技術的観点からみたデータ保護技術の導入状況と抱える課題

今後、産業データを国際的に流通させることで新たな価値創造を目指す際に、知財や安全保障に係るデータを守る必要性が生まれる。その際に、データ保護技術が抱える課題として、機能面と非機能面の 2 つに大分される。

機能面において、データ保護技術は特定の目的に特化したものと汎用的な計算を行うものに分けられるが、特定の目的に特化したデータ保護技術は機能の幅が少ない分、一部の開発ベンダーだけで実装するころで大きな問題はない。しかし、汎用的なデータ保護技術（データを隠したまま機械学習させる技術等）は汎用性が高いがゆえに、開発・実装できる技術者が増えないとプロダクトやソリューションが出てこない点に問題がある。これは、開発できる技術者の不足と、技術者がいたとしても目指すべきプロダクトが具体的でないことが機能実現に向けての課題となる。

もう 1 つは非機能面だが、企業がデータ保護技術を導入するベネフィットが出てくるような仕組みが示されておらず、企業にとって技術的保護措置を行うモチベーションがないこと

が問題である。また技術導入にはコストがかかることから、費用対効果の観点からそのベネフィットに対して、投資判断ができるセキュリティの姿を示す必要があると言えるだろう。

例えば、データ保護の程度やレベルを定量的に表現することができれば、企業によってデータ保護に取り組むベネフィットを議論できるが、非個人データを外部に漏らさないことによるベネフィットは企業によって異なるため、画一的な議論をすることは難しい。

欧州で検討されているデータ法の状況を把握しつつ、対応の必要性は認識しているものの、どのように対応すればよいのか分からない状況にあるのが現状と言えるだろう。

5.4.2 データ連携基盤を設計する上で留意すべき技術的課題

様々なデータ保護規制への対応や法文で規定された要求事項を満たしていく上で、いかに開示する情報を少なくするかは技術の問題と言える。

例えば、サプライチェーンにおいてカーボンフットプリント（CFP）の連携が進まない要因の１つに、コスト構造が明らかになってしまう懸念が挙げられる。これは、カーボンフットプリントを算出する上で、生データを入力すると四則演算でコスト計算ができてしまう。このような課題を解決するために、元データの特定を防ぐ各種プライバシー保護技術の活用が望まれる。

さらに業務とのバランス、費用対効果においても、どのようにデータを取得するのが望ましいのかを検討するのが、データ流通分野での課題の一つと言えるだろう。

WBCSD（World Business Council for Sustainable Development：持続可能な開発のための世界経済人会議）の PACT（The Partnership for Carbon Transparency：炭素の透明性のためのパートナーシップ）においても、カーボンフットプリント値のみとすることに力点を置いていた。

またバッテリーパスポートにおいても同様に、サプライチェーンから集めるデータと報告者（輸入者）が記入する情報（製品番号、生産工場、アセンブリの場所等）等、多くのデータ項目がある。しかしルール上では、取引を追跡できるようにする必要性があるが、取引関係を開示するようには規定されていない。そのため、情報としてはトレーサビリティを全て取得していくが、取引関係等を開示しないように情報制御をすれば、法律上の要件を満たすことが可能である。秘密計算、機械言語でのやり取り等の技術を組み合わせながら、様々なやり方で対応できるだろう。また誰に対してデータを開示できるのかという権限（データ主権、アクセス制御）と送付したデータをいつまで閲覧できるのかといった部分に制御（情報参照の有効期限）をかける方法で対応しようとしている。データ連携基盤には、多くの情報が集約されることから、一般的な関係者に対するアクセス制御とは別に、当局によるガバメントアクセスのリスクも懸念されている。当局であっても秘密計算等を義務付ける必要性など法的課題も今後検討していくことが望まれる。

5.4.3 データ保護技術の技術動向

5.2 章でも述べたように、近年ではブロックチェーン技術や秘密計算技術等の高度な機密性を保つことのできるデータ保護技術が登場している。これらの新しい技術は、既存の技術との勢力図を大きく変えるものではなく、技術の分担は今後も従来と比べて大きくは変化しないと考えられる。

例えば、秘密計算技術は入力するデータのプライバシーを守る技術であるのに対し、差分プライバシー技術は出力データのプライバシー、つまり計算結果から元の入力データを推察されにくくする技術であることから、それぞれ役割が異なる技術と言える。

そのため、差分プライバシーが活用されうる分野では引き続き差分プライバシーが使われていくべきであり、秘密計算が適切な分野に関しては、特に差分プライバシー技術を元々使っていたわけでなく、秘密計算技術を使用するのが自然だと言える。ただし、AI の学習モデルなどにおいて、最終的にユーザーに提供したい出力結果を得るまでに、中間出力データを出すような場合は、状況が異なることに留意したい。この場合は、中間出力を秘密分散された状態のままで計算に使う際は確かに秘密計算が差分プライバシーに置き換えられるだろう。

また最近では、厳密にデータを保護するよりも、ある程度の機密性を諦めることでプライバシー保護技術を使うにあたって生じるデメリットを減らしていく、つまり妥協点を探していくフェーズに入りつつある。厳密にデータを保護しないことは、何かしらの技術的制約を突破することがメリットになるが、最たるものは計算コストの低下である。

例えば、秘密計算は本来すべてのデータを暗号化したまま計算処理をすることが特徴であるが、一部の環境において必要最小限のデータを復号して（暗号化せず）計算処理を行うことを許容することで、計算コストを下げることが可能となる。もちろん妥協点はセキュリティの弱点になるためデータ漏洩のリスクが高まる懸念はあるが、そのリスクを許容した上でプライバシー保護の技術を普及させようとするのが最近の傾向と言える。

国際的なデータ流通を積極的に促していきつつも、どこまでリスクを許容するかのバランスに関する議論は今後必要となるだろう。

6　日本政府がとり得る対応の整理

6.1. 産業データの保護の必要性に関する認知度の向上

産業データについてガバナンスを行う組織的な対応が行われていない日本企業が、大手企業を含めて存在する。弊社が実施したヒアリングにおいても、複数の大手日本企業において、産業データの保護に関する担当者や担当部署がわからない、という形でヒアリングへの対応が困難となった事例があった。

このような現状を鑑みると、日本における産業データに関する取り組みの必要性、例えばガバメントアクセスなど外国における事業上のリスクを生じさせる制度的発展やその実例について、本調査等を基にして政府として認知度を向上させていく必要があるといえる。

6.2. 産業データの保護に関する指針策定の提案

他方、既に本調査で検討した産業データの保護について、その重要性を認識し、実践し始めている企業も聴取された。しかし、産業データの保護や管理の手法は、個人情報保護に比べて確立した手法に乏しく、本調査に基づく限り、各社とも手探りに近い状態で、個社が自ら外国の情報や最新の技術トレンドを調査して対応を個別に検討しているのが実情である。

しかし、個社毎のデータ保護に関する対応は個社のリソースや意識に依存するため、国として最低限度保護をすべきデータに対しても十分な保護水準を維持できていない可能性が存在することは否定できない。

そこで、政府として各社が産業データの保護を進める際に参考となる資料、例えば産業データの保護に関する指針を示すことができれば、日本企業における産業データの保護水準を全般として高めることができる。以下、このような指針の案として想定し得る内容を検討する。

6.2.1.　産業データの保護に関する指針の概要

産業データの保護に関する指針の内容は、産業データが個人データと非個人データの双方を含み得る概念であることをも考慮し、既に日本企業においても対応が進んでいる個人データに関するデータガバナンスの考え方を応用することが、企業にとって理解が進みやすいと考えられる。実際、経済安全保障とデータガバナンスを扱った論考も、同様のアプローチをとっている[2]。

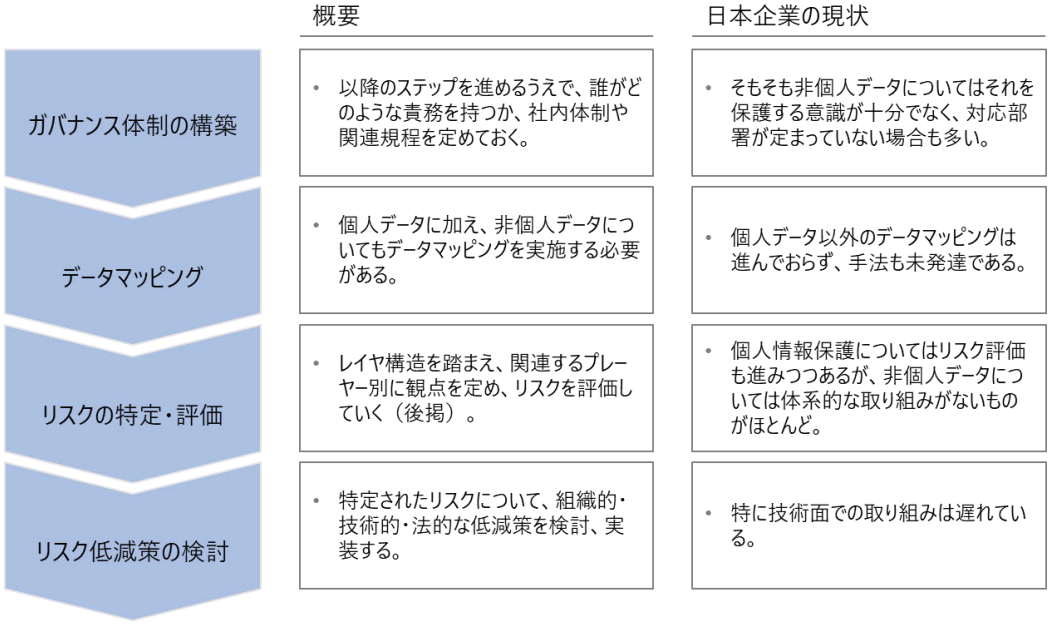
---

[2]　山郷琢也・三代川英嗣「経済安全保障の視点を取り入れたデータガバナンスの実務-各国において高まるガバメントアクセスの懸念を背景として」『NBL』（2022 年 10 月号）、渡辺翔太「経済安全保障の観点を含めたデータガバナンスを推進するうえでの企業実務対応のポイント」（https://www.nri.com/jp/knowledge/publication/mcs/region/lst/2022/07/03）

すると、大枠の対応の進め方は下記の通りとなる。

まず、企業側ではそもそも誰が、どのような社内ルールでもって産業データの保護を行うかが不明確である事例も少なくないため、まずは社内全体として産業データの保護のためのガバナンス体制の構築を行っていく必要がある。先に述べた通り、本調査のヒアリングを打診する際にも、社内調整が必要である、担当部署が不明といった理由で社内調整が煩雑になることからヒアリングに対応できない企業が複数存在した。

次に、自社の扱う産業データ全般についてのデータマッピングを行い、それぞれのデータについてリスクの特定・評価を実施した後で、リスク低減策を検討することとなる。



図表 2　企業側の産業データ保護に向けた対応

6.2.2. ガバナンス体制の構築

ガバナンス体制の構築においては、まず個人データの保護と同様、産業データの保護や管理が経営上重要な意義を持つことを明らかにするとともに、経営レベルの所掌事項として、その責任者を定めるとともに、具体的な担当部署を定めるべきである。

担当部署については、現状、一般的な日本企業（製造業）を想定すると、知的財産・営業秘密の保護を扱う部署、安全保障に関する法令上の情報保護を扱う部署（主に安全保障貿易管理）、さらには個人データを扱う部署が分かれて存在していることが一般的であるため、これらを連携させつつ、社内調整を進めていく必要がある。

また、体制構築と併せて以降実施する手順を含む社内ルールを定めていく必要がある。

6.2.3. データマッピング

担当の経営層や部署、手続きが定められれば、続いてデータマッピングを行うこととなる。データマッピングとは、誰に対して、どのようなデータがどのような目的で提供されているか、いわば社内のデータ流通の実態を明らかにする作業である。

一般的には各部署への質問票調査と、特に重要な部署（リスクが高そうな部署や管理体制が明らかでない部署等）については、ヒアリング調査を並行して実施することとなる。

6.2.3.1. データの種類

データの種類として、少なくとも下記の２つの類型、安全保障に関連するデータと自社の競争力に影響するデータについて保護を検討する必要がある。安全保障に関連するデータとは、安全保障に関連するデータとして流通が制限されているもの（安全保障貿易管理等）や、経済安保推進法でいう特定重要物資に関連するデータなど、（経済）安全保障上の観点から企業が保護すべきと考えるデータである。具体例としては、ミサイルや生物兵器の開発につながり得るデータや、重要な戦略資源として特定重要物資として指定される産品、重要インフラに関連する情報がある。また、大量の個人情報についても該当する。

次に、自社の競争力に影響するデータとは、営業秘密や著作権で保護されるデータなど、競合に漏洩することや、レピュテーションが損なわれることで自社の競争力が損なわれる可能性のあるデータを指す。このデータについては、企業側の判断によって保護範囲は異なり得る。具体例として、営業秘密や著作物、試験データ等が該当する。

上記に含まれない、保護を必要としないデータとしては公開されている特許や商標などがある。以上をまとめると、下の図表のとおりとなる。

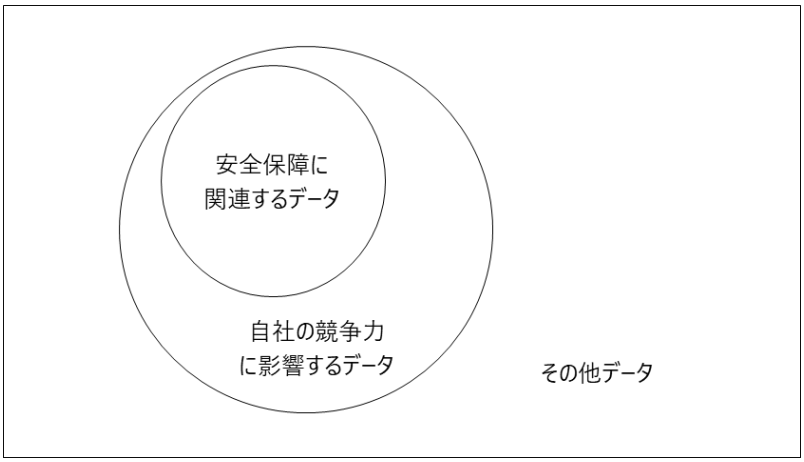
図表 3　データの３つの類型

保護すべき産業データの類型	説明	対象となるデータの例
安全保障に関連するデータ	安全保障に関連するデータとして流通が制限されているもの（安全保障貿易管理等）や、経済安保推進法でいう特定重要物資に関連するデータなど、（経済）安全保障上の観点から企業が保護すべきと考えるデータ	• 安全保障貿易管理の対象となるデータ • 特定重要物資（半導体や石油等）のサプライチェーンに関するデータ • 重要インフラに関連する情報（発電所の運転情報等） • SNS 上の利用者情

		報等の集積された個人情報
自社の競争力に影響するデータ	営業秘密や著作権で保護されるデータなど、競合に漏洩することや、レピュテーションが損なわれることで自社の競争力が損なわれる可能性のあるデータ。企業によってどこまでを保護すべきか判断が異なり得る。	• 営業秘密（製品の作成ノウハウ、コスト管理情報等） • 著作物（ソースコード、アルゴリズム等） • 医薬品の試験データ • コネクテッドカーの走行試験データ
その他データ（オープンデータ等）	上記いずれの観点からも、保護する必要性が企業から認められないデータ	• 特許・商標等の公表されているデータ • 未加工の政府統計データ • 自社の IR データ

上記の３つの類型は下図の通り重複があるが、２つの類型を共に保護していく必要がある。

図表 4　データの３つの類型の関係性



6.2.3.2. データの提供・共有の態様

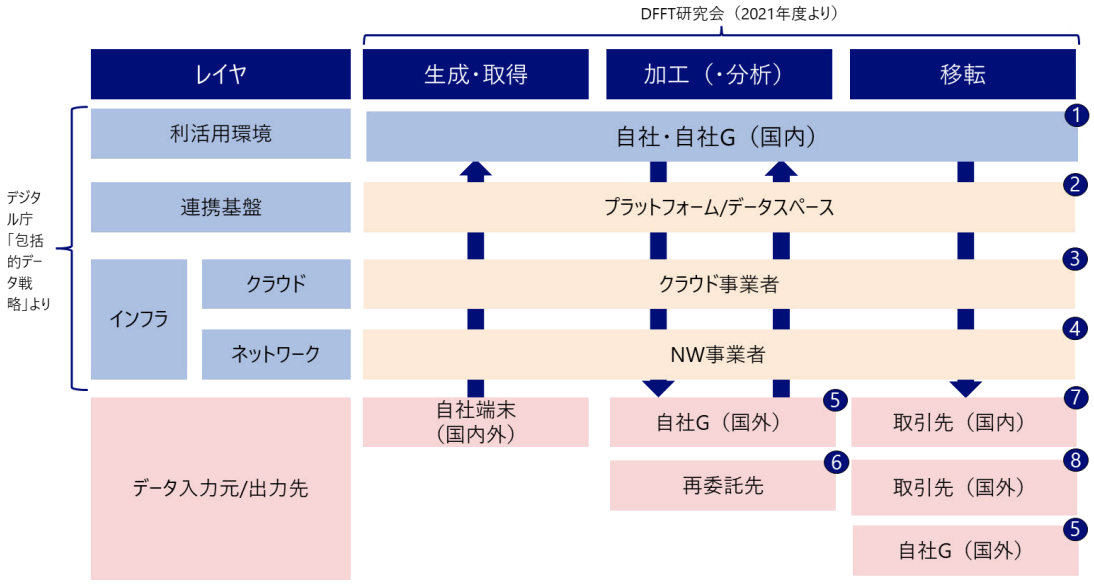
次に、データの共有先を含む共有の態様である。本件調査で明らかになった通り、近時は

クラウドサービスの利用が一般的であり、単に社内でデータをクラウドに保管する場合であっても、当該クラウドサービスの選定や契約における留意点が増えている。

さらに、二酸化炭素排出量等のサプライチェーンを通じた環境関連規制の進展やサプライチェーンのデジタル化に伴い、サプライチェーン全体を通じてデータを共有することが増加していくことが見込まれる。このような場面では、いわゆるデータスペースと呼ばれるデータ共有基盤となるサービスの利用が拡大していくと考えられる。同様に、例えば貿易や物流等の分野に特化した取引プラットフォームが発達している。こうしたプラットフォームやデータスペースの利用は、自社で能動的に DX の一環として取り入れるほか、調達元から取引関係上、実質的に導入を促される場合も多いことが推察される。また、これらをつなぐ通信の過程（ネットワーク）についても気を配る必要がある。

すなわち、従来の生成・取得、加工（・分析）、移転というデータのライフサイクルに加えて、それぞれの過程におけるデータのやり取りがどのレイヤで行われているか、当該レイヤはどの範囲の者にデータのアクセスを許容するものか（提供・共有先はどこか）、といった要素をも気にしつつデータの提供・共有の態様の全体像を整理しながらデータマッピングを進めていく必要がある。

以上をまとめると、下図の通りとなり、少なくともこれらの①～⑧について対策を進めていく必要がある。また、例えば複数のクラウドサービスを統合したり、同じクラウドのレイヤでも IaaS の上に SaaS を構築している等、さらにレイヤが細分化される可能性もある。



図表 5　データの提供・共有の態様

6.2.4. リスクの特定・評価/低減策の検討

ここではリスクの特定・評価と特定されたリスクについて、それをいかに低減していくか、

その施策を検討する。ここで重要なことは、産業データの保護についてどのようなリスクがあるかを特定したうえで、そのリスクが自社にとって受容できるか否かを検討することである。

まずリスクの特定については、どのように（本来利活用や管理のあり方は自主的に決定できるはずの）自社の保有する産業データが、自社にとって意図・想定されていない形で利用され、それが自社の事業に悪影響を与える可能性があるかという形で特定していく。そのうえで、当該リスクがどの程度受容可能なものかを判断していく必要がある。

特に留意すべきは外国におけるガバメントアクセスであるが、それ以外にも各種産業データの自主的な保護や管理に制約を与え得る規制や、共有先が無断でデータを意図しない形で利用するといったリスクが生じる可能性等も存在する。

リスクシナリオ		概要
ガバメントアクセス	法人	法令の定めに基づき、データの所在地国、法人の設立国、法人の本支店の所在国等から、管理権を持つデータの提出を、強制力を持って求められる
	自然人	上記について、法令によっては法人のほか、国籍国や、物理的に所在している国等から管理権を持つデータの提出を求められる
移転先での無断利用		データを移転した後、移転先（プラットフォームや取引先等）において、当該データを無断で利用されてしまう
共有範囲の拡大		プラットフォームやデータスペースに特有のリスクであるが、これらサービスは時間の経過とともに参加者が拡大し、データの共有先となり得る主体が増加していくため、当初想定していなかった相手方にデータが共有され得る

図表 6　想定するリスクシナリオの代表例

次に、リスクの評価であるが、これはリスクが生じた場合、経営にどのような悪影響があるか、単に自社事業の競争優位のみならず、特に安全保障上の重要データについては、それが生じさせる経済的インパクトのみならず、レピュテーションリスクをも考慮に入れていく必要がある。例えばいわゆる LINE 事件では、越境移転規制それ自体の違反は問われなかったものの、重要なデータを外国に置いたことがレピュテーションリスクを生じさせた。

最後に低減策の検討であるが、これはおおむね下記のような方向性で、組織的、技術的及び法的な低減策を検討していくことになる。

図表 7　リスク低減策の主な方向性

主な方向性	概要	低減策の具体例
データの重要性を下げる	共有されるデータが相手方にとって悪用する価値がないものとしていく	【組織的】データの内容や容量について、必要最低限のものとする（余計なデータを共有しない） 【技術的】データの暗号化
データ共有先の見直し	データの共有先を減らす	【組織的】データの共有先について、事業上の必要性を検討して削減する 【技術的】データの共有許可範囲を削減する 【法的】追加的な契約でガバメントアクセスに関するポリシーの策定や利用者への通知を規定する、契約で第三者提供に制限をかける
データフローの見直し	データを国内保管する、またはクラウドサービスの所在国を変更する等の措置をとる	【組織的】クラウドやプラットフォームの変更（国内保管等） 【技術的】クラウド等のリージョン変更

以下、6.2.3.2.で述べた共有態様のうち、特に共有先に応じた形で、リスクの特定・評価とその低減策の検討例を記載する。

6.2.4.1. 自社・自社グループ企業（国内）

（1）リスクの特定・評価

自社やその国内グループ企業については、外国にデータを移転する場面に比べると留意すべき事項は多くない。最も大きなリスクはガバメントアクセスリスクであり、外国籍の従業員が、自国政府から当該国の国民であること（国籍）を理由に保護すべきデータの窃取に協力するよう求められる可能性がある。これは安全保障貿易管理におけるみなし輸出に近い類型のリスクであり[3]、同様の対策が必要となろう。

（2）リスク低減策の検討

ガバメントアクセスのリスクについては、組織的な措置、すなわちデータへのアクセス権限やログの保管等が基本となる。加えて、従業員のバックグラウンドチェックが必要になり、特に安全保障に関連するデータについては、今後導入が予定されるセキュリティクリアラ

[3] みなし輸出について；https://www.meti.go.jp/policy/anpo/anpo07.html

ンスの制度を活用することも検討すべきである[4]。

6.2.4.2. プラットフォーム・データベース

（1）リスクの特定・評価

対処すべきリスクは下記のとおりである。それぞれについて、提供されるデータの種類、相手方の所在地や相手方のデータ保護の水準（データ保護ポリシーや組織内の体制整備）、等の要素を勘案して、どの程度のリスクがあるかを判断していくことになる。

対処すべきリスク		ガバメントアクセス	PF 等によるデータの無断利用	データ共有範囲の拡大（データスペース）
リスク評価の観点	相手方の所在地・国籍国（法人のほか従業員を含む）	• ガバメントアクセスの可能性はあるか？ -移転先となる PF やデータ空間の管理者の所在地・国籍国の確認 - 物理的なデータの所在地の確認 - 上記所在地国におけるガバメントアクセス権限の把握（※本調査結果や PPC の資料等を参考とする）	• データの無断利用の可能性はあるか？ - 相手方の所在国における法的保護の度合い、執行の容易性（費用、時間）	• データスペースにどのような主体が参加するか？ - 参加者の審査はあるか。ある場合、誰によってどのように行われているか、その基準は何か -上記審査の運用が適切に行われているか
	相手方のデータ保護水準	- ガバメントアクセス要求を受けた場合、PF 等はユーザーを守るためそれを拒否する可能性があるか？ PF のガバメントアクセスへの対応ポリシーや過去の対応状況	• PF はデータを無断利用するインセンティブがあるか？ • 競業を行っているかといった PF の事業内容の確認	• PF やデータスペースにおいて自社のデータが共有されうる相手方はどの程度のデータ保護の水準を担保されているか？

[4] 同制度の創設法案は 2024 年 2 月に閣議決定されている；
https://www3.nhk.or.jp/news/html/20240227/k10014371891000.html

		の確認	• データの無断利用を禁ずる法的措置が取られているか？ • PF との契約内容の確認	
	提供されるデータの種類	• 3類型のどれに該当するか		
	データ提供の方法	• どの程度加工（暗号化や連合学習等）が行われるか		

（2）リスク低減策の検討

（1）で述べた通り、リスク評価の要素は多岐にわたるが、特に高いリスクがあると思われる場合（シナリオ）について、リスク低減策の例を記載する。

なお、ガバメントアクセス自体は国家安全保障や犯罪捜査を目的として民主主義国を含むあらゆる国家において行われており、それ自体のリスクをなくすることは困難である。他方で、民主的価値や法の支配と矛盾し、無制限で不合理、恣意的で比例的ではないガバメントアクセスについては、これを正当なものと認めることはできない。

このようなガバメントアクセスが行われるリスクが高い国を、以下、民主的価値や法の支配等と矛盾するおそれのある地域と表現する。

① ガバメントアクセス

#	データの種類	相手先	リスク低減策の例
1	安全保障に関連するデータ	民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国の PF/データスペース	• 民主的価値や法の支配等と矛盾するガバメントアクセスがなされるおそれのある地域・懸念国に経済安保に関連するデータを移転・保管することはガバメントアクセスのリスクがあり、移転・保管それ自体にもレピュテーションリスクが懸念されるため、保管先を国内に改めることが考えられる。 • ガバメントアクセスのリスクについてはデータの移転・保管形式（暗号化等）の変更による対応もあり得るが、レピュテーションリスクへの対応ができない懸念が残る。

2	同上	上記地域以外の懸念国以外のPF/データスペース	• 上記以外の地域にある懸念国以外であれば民主的価値や法の支配等と矛盾するガバメントアクセスのリスクは高くないが、プラットフォームやデータスペースのガバメントアクセスに関するポリシーを確認するとともに、ＰＦやデータスペースと交渉して追加的な保護措置（ガバメントアクセスの通知、透明性レポートの共有等）を導入する。
3	競争力に影響するデータ	民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国の PF/データスペース	• #1 と同様にガバメントアクセスのリスクがあるが、レピュテーションリスクは#1 に比べると低い。そのため、データの暗号化等の対応が考えられる。 • ガバメントアクセスのリスクと、データを当該国に保管するメリット（現地政府や企業との関係性）を衡量して現地保管を維持すべきか検討すべきである。

② PF 等によるデータの無断利用

#	データの種類	相手先	リスク低減策の例
1	安全保障に関連するデータ競争力に影響するデータ	PF/データスペース	• PF やデータスペースの所在国が私法上の権利の保護に積極的でない場合や容易に代替のプラットフォーム・データスペースが見つかる場合には、共有をとどまる、変更する方策がある。 • また、共有を行う場合でも、データの暗号化等でデータを技術的に保護する、契約で無断使用時の対応を規定する等が考えられる。 • 無断使用のリスクと、データを当該 PF/データスペースに共有するメリット（取引先との関係性や事業機会等）を衡量して共有を維持すべきか検討すべきである。

③ データ共有範囲の拡大（データスペース）

#	データの種類	リスク低減策の例
1	安全保障に関連するデータ競争力に影響するデータ	• 審査が適切に機能していない場合、審査の運用改善を促す • 契約において、共有先を増やす場合には、自らの許可を得る必要があるとの規定や、追加される主体について適切なデータ保護の水準を担保していることをあらかじめ確認する規定を入れておく。 • 追加先へのデータ共有を自らが判断できる仕組み（いわゆるデータ主権の確保）を法的、技術的に導入する。 • 技術的措置として、暗号化や連合学習等、データ共有先が増加したとして

		も、データ保護の水準を維持できる技術的措置を導入する。

6.2.4.3. クラウドサービス提供者

（1）リスクの特定・評価

対処すべきリスクは下記のとおりであり、ほぼプラットフォームやデータスペースと同一であるが、共有される範囲の拡大については考慮する必要がなくなる。

対処すべきリスク		ガバメントアクセス	クラウドサービス提供者によるデータの無断利用
リスク評価の観点	相手方の所在地・国籍国（法人のほか従業員を含む）	• ガバメントアクセスの可能性はあるか？ -移転先となるクラウドサービス提供者の所在地・国籍国の確認 - 物理的なデータの所在地の確認 - 上記所在地国におけるガバメントアクセス権限の把握（※本調査結果や PPC の資料等を参考とする）	• データの無断利用の可能性はあるか？ • - 相手方の所在国における法的保護の度合い、執行の容易性（費用、時間）
	相手方のデータ保護水準	- ガバメントアクセス要求を受けた場合、クラウドサービス提供者はユーザーを守るためそれを拒否する可能性があるか？ - クラウドサービス提供者のガバメントアクセスへの対応ポリシーや過去の対応状況の確認	• クラウドサービス提供者はデータを無断利用するインセンティブがあるか？ • 競業を行っているかといったクラウドサービス提供者の事業内容の確認 • データの無断利用を禁ずる法的措置が取られているか？ • クラウドサービス提供者との契約内容の確認
	提供されるデータの種類	• 3 類型のどれに該当するか	
	データ提供の	• どの程度加工（暗号化や連合学習等）が行われるか	

	方法	

（2）リスク低減策の検討

（1） 同様、リスクシナリオが類似するため、対応策も類似のものとなる。

① ガバメントアクセス

#	データの種類	リスク低減策の例
1	安全保障に関連するデータ	【民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国】 • 民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国に経済安保に関連するデータを移転することはガバメントアクセスのリスクがあり、移転それ自体にもレピュテーションリスクが懸念されるため、移転を実施しないことが考えられる。 • ガバメントアクセスのリスクについてはデータの保管形式（暗号化等）の変更による対応もあり得るが、レピュテーションリスクへの対応ができない懸念が残る。 【懸念国以外】 • 懸念国以外であればガバメントアクセスのリスクは高くないため、自社と同水準の子会社については移転先となりうる。 • ただし、ガバメントアクセスへの対応指針をあらかじめ定めるとともに、本社の関連部門と連携して対応できる体制を構築しておくべきである。
2	同上	• 懸念国以外であればガバメントアクセスのリスクは高くないが、クラウドサービス提供者のガバメントアクセスに関するポリシーを確認するとともに、クラウドサービス提供者と交渉して追加的な保護措置（ガバメントアクセスの通知、透明性レポートの共有等）を導入する。
3	競争力に影響するデータ	• #1 と同様にガバメントアクセスのリスクがあるが、レピュテーションリスクは#1 に比べると低い。そのため、データの暗号化等の対応が考えられる。 • ガバメントアクセスのリスクと、データを当該国に保管するメリット（現地政府や企業との関係性）を衡量して現地保管を維持すべきか検討すべきである。

② クラウドサービス提供者によるデータの無断利用

#	データの種類	リスク低減策の例
1	安全保障に関連するデータ競争力に影響するデ	• クラウドサービス提供者の所在国が私法上の権利の保護に積極的でない場合や容易に代替のプラットフォーム･データスペースが見つかる場合には、共有をとどまる、変更する方策がある。

	ータ	• また、共有を行う場合でも、データの暗号化等でデータを技術的に保護する、契約で無断使用時の対応を規定する等が考えられる。 • 無断使用のリスクと、データを当該クラウドサービス提供者に共有するメリットを衡量して共有を維持すべきか検討すべきである。

6.2.4.4. ネットワーク

（1）リスクの特定・評価

ネットワークについては、基本的にガバメントアクセスリスクのみを検討すればよい。ネットワークレイヤでのガバメントアクセスは、海底ケーブルのほか、ISP などエンドトゥエンドでネットワークを構成する多様な主体への関与があり得る。また、インターネットの技術的な仕様上、そもそもあらかじめ伝送経路を特定することが困難である。

ただし、相手先が特にネットワークに対するガバメントアクセスリスクの高い、民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国である場合には、ネットワークレイヤでのリスクも高くなるといえる。

（2）リスク低減策の検討

上記の通り、関与する主体が多く、かつ事前に経路が判明しないため、組織的または法的な対応策が困難である。

そのため、技術的な保護措置が中心となり、暗号化や専用線の利用、またデータ自体の加工等が対策の中心となる。

6.2.4.5. 自社グループ企業（国外）

（1）リスクの特定・評価

基本的にはガバメントアクセスのリスクに対応すべきであるが、外国においては、事業の開始時（許認可の取得や実証実験など）と事業運営中、双方のタイミングでガバメントアクセスが行われる可能性があり、これらを区別して対処していく必要がある。

対処すべきリスク		事業開始段階でのガバメントアクセス	事業運営段階でのガバメントアクセス
リスク評価の	相手方の所在地・国籍国（法人のほか従業員	• 許認可や会社の設立、商用利用に向けた試験等に際してガバメントアクセスが行われる可能性はあるか？ - 所在地の確認 - 物理的なデータの所在地の確認 - 上記所在地国におけるガバメントアク	• 事業運営中にガバメントアクセスが行われる可能性はあるか？ - （確認内容は左に同じ）

観点	を含む）	セス権限の把握（※本調査結果や PPC の資料等を参考とする）	
	相手方のデータ保護水準	—（自社のグループ会社であり、基本的には自社と同水準と考えられる）	
	提供されるデータの種類	• 3類型のどれに該当するか	
	データ提供の方法	• どの程度加工（暗号化や連合学習等）が行われるか	

（2）リスク低減策の検討

① 事業開始段階でのガバメントアクセス

#	データの種類	リスク低減策の例
1	安全保障に関連するデータ	【民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国】 • 民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国に経済安保に関連するデータを移転することはガバメントアクセスのリスクがあり、移転それ自体にもレピュテーションリスクが懸念されるため、移転を実施しないことが考えられる。 • ガバメントアクセスのリスクについてはデータの保管形式（暗号化等）の変更による対応もあり得るが、レピュテーションリスクへの対応ができない懸念が残る。 • 業務上データの利用が不可欠であれば、例えば、懸念国外のクラウドサービスにデータを保管し、必要な際に都度アクセス権限を付与する、ローカルにはデータを保存しないといった手法をとる必要がある。 【懸念国以外】 • 懸念国以外であればガバメントアクセスのリスクは高くないため、自社と同水準の子会社については移転先となりうる。 • ただし、ガバメントアクセスへの対応指針をあらかじめ定めるとともに、本社の関連部門と連携して対応できる体制を構築しておくべきである。

2	競争力に影響するデータ	• #1 と同様にガバメントアクセスのリスクがあるが、レピュテーションリスクは#1 に比べると低い。そのため、データの暗号化等の対応が考えられる。 • ガバメントアクセスのリスクと、データを当該国に移転・保管するメリット（許認可の取得による市場アクセスの利益、現地政府や企業との関係性）を衡量して移転・保管をすべきか検討すべきである。

② 事業運営段階でのガバメントアクセス

#	データの種類	リスク低減策の例
1	安全保障に関連するデータ	【民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国】 • 民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国に経済安保に関連するデータを移転することはガバメントアクセスのリスクがあり、移転それ自体にもレピュテーションリスクが懸念されるため、移転を実施しないことが考えられる。 • ガバメントアクセスのリスクについてはデータの保管形式（暗号化等）の変更による対応もあり得るが、レピュテーションリスクへの対応ができない懸念が残る。 【懸念国以外】 • 懸念国以外であればガバメントアクセスのリスクは高くないため、自社と同水準の子会社については移転先となりうる。 • ただし、ガバメントアクセスへの対応指針をあらかじめ定めるとともに、本社の関連部門と連携して対応できる体制を構築しておくべきである。
2	競争力に影響するデータ	• #1 と同様にガバメントアクセスのリスクがあるが、レピュテーションリスクは#1 に比べると低い。そのため、データの暗号化等の対応が考えられる。 • ガバメントアクセスのリスクと、データを当該国に保管するメリット（現地政府や企業との関係性）を衡量して現地保管を維持すべきか検討すべきである。

6.2.4.6. 委託先

（1）リスクの特定・評価

委託先についても、クラウドと同様のリスクとなる。

対処すべきリスク		ガバメントアクセス	委託先によるデータの無断利用
リス	相手方の所在	• ガバメントアクセスの可能性はあるか？	• データの無断利用の可能性はあるか？

ク評価の観点	地・国籍国（法人のほか従業員を含む）	-移転先となる委託先の管理者の所在地・国籍国の確認 - 物理的なデータの所在地の確認 - 上記所在地国におけるガバメントアクセス権限の把握（※本調査結果や PPC の資料等を参考とする）	• - 委託先の所在国・国籍国における法的保護の度合い、執行の容易性（費用、時間）
	相手方のデータ保護水準	- ガバメントアクセス要求を受けた場合、委託先は委託元を守るためそれを拒否する可能性があるかの確認 - 委託先のガバメントアクセスへの対応ポリシーや過去の対応状況の確認	• 委託先はデータを無断利用するインセンティブがあるか？ • 競業を行っているかといった取引先の事業内容の確認 • 契約など、データの無断利用を禁ずる法的措置が取られているかの確認
	提供されるデータの種類	• 3類型のどれに該当するか	
	データ提供の方法	• どの程度加工（暗号化や連合学習等）が行われるか	

（2）リスク低減策の検討

リスクシナリオが類似するため、対応策も類似のものとなる。

①ガバメントアクセス

#	データの種類	リスク低減策の例
1	（経済）安保データ	【民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国】 • 民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国に経済安保に関連するデータを保管・移転することはガバメントアクセスのリスクがあり、保管・移転それ自体にもレピュテーションリスクが懸念されるため、移転を行わないことが考えられる。 • ガバメントアクセスのリスクについてはデータの保管形式（暗号化等）の変更による対応もあり得るが、レピュテーションリスクへの対応ができな

		い懸念が残る。 【懸念国以外】 • 懸念国以外であればガバメントアクセスのリスクは高くないが、取引先のガバメントアクセスに関するポリシーを確認するとともに、取引先と交渉して追加的な保護措置（ガバメントアクセスの通知、ガバメントアクセスへの対応指針の策定等）を導入する。
2	競争力に影響するデータ	• #1 と同様にガバメントアクセスのリスクがあるが、レピュテーションリスクは#1 に比べると低い。そのため、データの暗号化等の対応が考えられる。 • ガバメントアクセスのリスクと、データを当該国に保管・移転するメリット（取引先との関係性）を衡量して移転・保管を行うか検討すべきである。

②委託先によるデータの無断利用

#	データの種類	リスク低減策の例
1	競争力に影響するデータ	• 委託先の所在国が私法上の権利の保護に積極的でない場合や容易に代替先が見つかる場合には、共有をとどまる、変更する方策がある。 • また、共有を行う場合でも、データの暗号化等でデータを技術的に保護する、契約で無断使用時の対応を規定する等が考えられる。

6.2.4.7. 取引先（国内）

クラウドに類似する内容となり、ガバメントアクセスと移転先での無断利用がリスクシナリオとなる。

（1）リスクの特定・評価

対処すべきリスク		ガバメントアクセス	取引先によるデータの無断利用
リスク評価の観点	相手方従業員の・国籍国（法人のほか従業員を含む）やデータの保管場所	• ガバメントアクセスの可能性はあるか？ -移転先となる取引先の従業員に関する国籍国の確認 - 物理的なデータの所在地の確認 - 上記国籍国や所在国におけるガバメントアクセス権限の把握(※本調査結果や PPC の資料等を参考とする)	• データの無断利用の可能性はあるか？ •
	相手方のデ	- ガバメントアクセス要求を受けた	• 取引先はデータを無断利用する

	ータ保護水準	場合、取引先は自社を守るためそれを拒否する可能性があるか？ 取引先のガバメントアクセスへの対応ポリシーや過去の対応状況の確認	インセンティブがあるか？ • 競業を行っているかといった事業内容の確認 • 契約など、データの無断利用を禁ずる法的措置が取られているか？
	提供されるデータの種類	• 3類型のどれに該当するか	
	データ提供の方法	• どの程度加工（暗号化や連合学習等）が行われるか	

（2）リスク低減策の検討

リスクシナリオが類似するため、対応策も類似のものとなる。

① ガバメントアクセス

#	データの種類	リスク低減策の例
1	（経済）安保データ	• 国内であれば取引先自体に対するガバメントアクセスのリスクは高くないが、従業員に関するリスクは残る。 • 取引先のガバメントアクセスに関するポリシーや業務従事者の国籍、社内の情報管理体制を確認するとともに、取引先と交渉して追加的な保護措置（ガバメントアクセスの通知、ガバメントアクセスへの対応指針の策定等）を導入する。
2	競争力に影響するデータ	• 基本的には上記と同様の対応をとるべきである。

② 取引先によるデータの無断利用

#	データの種類	リスク低減策の例
1	安全保障データ、競争力に影響するデータ	• 国内であれば契約内容の履行を法的に期待しうるため、まずはデータの保護に関する契約の内容やそれに付随する取引先での情報管理体制の構築を確認する。 • 無断利用のリスクと、データを当該取引先に共有するメリット（取引先との関係性、事業機会等）を衡量して共有を維持すべきか検討すべきである。

6.2.4.8. 取引先（海外）

（1）リスクの特定・評価

取引先についても、クラウドに類似する内容となり、ガバメントアクセスと移転先での無断利用がリスクシナリオとなる。

対処すべきリスク		ガバメントアクセス	取引先によるデータの無断利用
リスク評価の観点	相手方の所在地・国籍国（法人のほか従業員を含む）	• ガバメントアクセスの可能性はあるか？ -移転先となる取引先の所在地・国籍国の確認 - 物理的なデータの所在地の確認 - 上記所在地国におけるガバメントアクセス権限の把握（※本調査結果や PPC の資料等を参考とする）	• データの無断利用の可能性はあるか？ • - 取引先の所在国・国籍国における法的保護の度合い、執行の容易性（費用、時間）
	相手方のデータ保護水準	- ガバメントアクセス要求を受けた場合、取引先は自社を守るためそれを拒否する可能性があるかの確認 取引先のガバメントアクセスへの対応ポリシーや過去の対応状況の確認	• 取引先はデータを無断利用するインセンティブがあるか？ • 競業を行っているかといった取引先の事業内容の確認 • 契約など、データの無断利用を禁ずる法的措置が取られているかの確認
	提供されるデータの種類	• 3類型のどれに該当するか	
	データ提供の方法	• どの程度加工（暗号化や連合学習等）が行われるか	

（2）リスク低減策の検討

リスクシナリオが類似するため、対応策も類似のものとなる。

①ガバメントアクセス

#	データの種類	リスク低減策の例
1	（経済）安保データ	【民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国所在】 • 民主的価値や法の支配等と矛盾するおそれのある地域に所在する懸念国に経済安保に関連するデータを保管・移転することはガバメントアクセスのリスクがあり、保管・移転それ自体にもレピュテーションリスクが懸念されるため、移転を行わないことが考えられる。 • ガバメントアクセスのリスクについてはデータの保管形式（暗号化等）の変更による対応もあり得るが、レピュテーションリスクへの対応ができない懸念が残る。 【懸念国以外】 • 懸念国以外であればガバメントアクセスのリスクは高くないが、取引先のガバメントアクセスに関するポリシーを確認するとともに、取引先と交渉して追加的な保護措置（ガバメントアクセスの通知、ガバメントアクセスへの対応指針の策定等）を導入する。
3	競争力に影響するデータ	• #1 と同様にガバメントアクセスのリスクがあるが、レピュテーションリスクは#1 に比べると低い。そのため、データの暗号化等の対応が考えられる。 • ガバメントアクセスのリスクと、データを当該国に保管・移転するメリット（取引先との関係性）を衡量して移転・保管を行うか検討すべきである。

②取引先によるデータの無断利用

#	データの種類	リスク低減策の例
1	競争力に影響するデータ ※①に基づいて、安全保障関連のデータは移転されない）	• 取引先の所在国が私法上の権利の保護に積極的でない場合や容易に代替の取引先が見つかる場合には、共有をとどまる、変更する方策がある。 • また、共有を行う場合でも、データの暗号化等でデータを技術的に保護する、契約で無断使用時の対応を規定する等が考えられる。 • 無断使用のリスクと、データを当該取引先に共有するメリット（取引先との関係性、事業機会等）を衡量して共有を維持すべきか検討すべきである。

Appendix

1. 透明性レポートに関する調査

1.1 Google

・アクセス件数の公表

米 Google は、半期ごとに透明性レポートを更新しており、レポート上で各国政府からのユーザー情報の開示リクエスト件数を公開している。

様々な法律によって、世界中の政府機関が民事、行政、刑事、および国家安全保障の目的でユーザー情報を要求することが認められているため、Google は、透明性レポート上の「グローバルなリクエストに関する報告」にて、各国政府機関から Google が受けたリクエストの数と種類に関する情報を公開している。ただし、国家安全保障法に基づく米国機関からのリクエストは、グローバルなリクエスト件数には含まれていない。

また、公表されているのは件数のみで、具体事例についての詳細な言及はない。
レポート上では、要請を受けた期間や国別に件数を確認することが可能で、国別の要請件数では、召喚状（Subpoenas）、捜査令状（Search warrants）、その他の裁判所命令（Other court orders）などの要請の種類の内訳も公表している。

・ガバメントアクセスへの対応

Google は、特に政府による Google Cloud ユーザー情報の提供リクエストに対して、対応する際のフローを定めている。

政府からの情報提供のリクエストに対する Google のアプローチは、要請の種類にかかわらず、適用される法律で禁止されている場合や不合理な場合を除き、対処されるフローが下記のように Google Cloud ホワイトペーパー（2022 年 2 月）「クラウドユーザーデータへのガバメントアクセス」[5]上で公表されている。

1.リダイレクト

Google が政府機関からクラウドの顧客データに関する要請を受けた場合、米国政府の方針および Google の契約上の約束に沿って、当該機関に直接要請を出すよう政府機関に通知する。

2.法的有効性の評価

リダイレクトにもかかわらず政府が Google に顧客データの要求に応じるよう強制した場合、Google の弁護士と特別な訓練を受けた担当者で構成される専門チームがその要求が合法的かつ適切で Google のポリシーを満たしているかを慎重に検討

[5] Google Cloud Whitepaper February 2022「Government Requests for Cloud Customer Data」
https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf

する。

ユーザーデータのリクエストはすべて、データが利用可能になる前に専門チームによって処理され、承認され、適用範囲が広すぎる、不釣り合いである、適用法に適合しない、またはその他の方法で違法であると合理的に判断した法的手続きに対しては、異議の提唱、制限または修正を行う。

3.顧客への通知と透明性

Google は、法律で禁止されている場合や政府の捜査を妨害する可能性がある場合、個人の死亡や身体への重大な危害につながる場合を除き、顧客データが開示される前にユーザーに通知する。Google のポリシーでは、事前の通知が適用法で禁止されている場合、法定または裁判所の命令による開示禁止期間が満了した場合など、最終的に禁止が解除されたときにお客様に通知することが決められており、通知は通常 Google Cloud ユーザーの連絡先に送信される。

4.ユーザーの異議申し立て

Google は、法律および政府からの要請の条件によって認められる限りにおいて、ユーザーが関連裁判所に開示に対する異議申し立てを行い、その写しを Google に提供するなどの要請に反対するユーザーの取り組みに関する合理的な要請に応じる。Google がユーザーデータに対する法的要請をユーザーに通知し、その後、ユーザーが適切な裁判所に開示に対する異議申し立てを行い、異議申し立ての写しを Google に提供した場合、Google は、ユーザーによる異議申し立ての係属期間中、法的に許容される限り、要請に応じたデータの提供を行わず、データをエスクロー（預託）に保管する。

また、Google は、Google が保有するすべてのユーザー情報へのガバメントアクセスに対する法的有効性の評価についても公表[6]している。

法的有効性の評価は Google サービスプロバイダーによって異なり、ほとんどのサービスは、Google LLC(米国の法律に基づいて運営されている)または Google Ireland Limited(アイルランドの法律に基づいて運営されている)のいずれである。国外からのユーザー情報のリクエストを受け取った場合、国内法、国際規範、Google のポリシー等との合致を検討している。

Google LLC の場合は、以下のすべてに一致する場合に限り、ユーザーデータを提供することがあるとしている。

- 米国法：電子通信プライバシー法（ECPA）など、適用される米国法の下でアクセスや開示が許可されていること
- 要請国の法律：同様のサービスを提供する現地プロバイダに対して要請を行った場合に適用される適正手続きと法的要件に従うよう、当局に要請すること

[6] Google Privacy＆Terms https://policies.google.com/terms/information-requests?hl=en-US

- 国際規範：Global Network Initiative の「表現の自由とプライバシーに関する原則」および関連する実施ガイドラインを満たす要求に対してのみデータを提供すること
- Google のポリシー：適用される利用規約やプライバシー ポリシー、表現の自由の保護に関するポリシーを含む

Google Ireland は、欧州経済領域とスイスに所在するユーザーにサービスを提供しており、アイルランド以外の政府当局からデータ開示の要請を受けることがあり、この場合、以下のすべてに一致する場合に限り、ユーザーデータを提供することがあるとしている。

- アイルランドの法律：アイルランド刑事司法など、適用されるアイルランドの法律の下でアクセスおよび開示が許可されていること
- アイルランドで適用される欧州連合(EU)法：一般データ保護規則（GDPR）を含む、アイルランドで適用される EU 法
- 要請国の法律：同様のサービスを提供する現地プロバイダに対して要請を行った場合に適用される適正手続きと法的要件に従うよう、当局に要請すること
- 国際規範：Global Network Initiative の「表現の自由とプライバシーに関する原則」および関連する実施ガイドラインを満たす要求に対してのみデータを提供すること
- Google のポリシー：適用される利用規約やプライバシー ポリシー、表現の自由の保護に関するポリシーを含む

・秘密保持特例に対するスタンス

Google は、2022 年 4 月 6 日に NDO 公正法（NDO Fairness Act ）が連邦下院司法委員会によって可決されたことを受け、2022 年 6 月 22 日のニュースリリース[7]にて、ガバメントアクセスに関する透明性を高めるべきであると述べており、NDO 公正法が超党派で下院を通過し、正当な理由と期間のみ NDO が発行されるようになったことを称賛している。

また、Google は長い間ガバメントアクセスに関する透明性を提唱しており、 Global Network Initiative と Reform Government Surveillance 連合を共同設立した背景がある。さらに、e メール・プライバシー法や国家安全保障に関する要請をよりオープンにできるようにする法案などの監視改革を長年にわたって支持している。

1.2 Microsoft

・ガバメントアクセス件数の公表

[7] Google https://blog.google/outreach-initiatives/public-policy/its-time-for-more-transparency-around-government-data-demands

米マイクロソフトは、半期ごとに透明性レポート[8]を更新しており、レポート上で各国政府からのユーザー情報の開示リクエスト件数を公開しておいる。透明性レポートは 2013 年までさかのぼって法執行機関の要請を確認することができる。
また、公表されているのは件数のみで、具体事例についての詳細な言及はない。
レポート上では、要請を受けた期間や国別に件数を確認することが可能で、全体のアクセス数と合わせて、民事訴訟、捜査令状に基づくもの、緊急事態などのアクセスの種類別内訳も公表されている。開示リクエストを受けたデータ件数と合わせて、実際に開示された割合もレポート上で示されている。

・ガバメントアクセスへの対応

マイクロソフトは、民事訴訟、捜査令状、緊急事態に基づくガバメントアクセスについて、提供するデータが捜査や緊急事態の対処に役立つかを評価し、データ開示を行っている[9]。
正当な理由に基づく捜査令状（または同等の手続き）が提示されたガバメントアクセスに対しては、コンテンツを開示している。一方で、政府の要求に対して、提供するデータの種類や量を制限するよう求めたり、政府が顧客から直接データを取得するよう求めたりするなどして、要請による情報提供の範囲を狭めようとすることもある。また、法的命令の変更または取り消しを求めて裁判所に正式な法的異議を申し立てることもあるとしている。

捜査令状に基づくアクセス以外では、法律で許可されている場合の限られた状況において、人の死亡または身体への重大な傷害の危険を伴う緊急事態（自殺予告、児童誘拐等）を防止するために必要であるとマイクロソフトが判断した場合に、刑事法執行機関に情報を開示することがあるとしている。

これらの緊急要請は、公的なレターヘッドに記載され、法執行当局によって署名された書面が必要となり、要請には、緊急事態の概要と求められる情報が緊急事態に対処するために法執行機関をどのように支援するかの説明が含まれる必要がある。
各リクエストは、データが開示される前にマイクロソフトのコンプライアンスチームによって慎重に評価され、開示は、法執行機関が緊急事態に対処するのに役立つとマイクロソフトが考えるデータに限定されるとしている。

さらに、マイクロソフトは、各政府が開示要請を行う際は連邦法または地域の法律および規則に従って発行された、署名された法的に有効な正式な手続きを必要としている。具体的には、非コンテンツを開示する前に召喚令状（またはそれに相当するもの）を要求し、捜査令状（またはそれに相当するもの）に応じて法執行機関にのみコンテンツを開示している。
また、マイクロソフトのコンプライアンスチームは、顧客データに対する政府からの要求が

---

[8] Microsoft Law Enforcement Requests Report　https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

[9] 同上

有効であることを確認し、有効でないものは拒否し、法的命令で指定されたデータのみを提供する。法的に許可されている場合には、政府をリダイレクトして、企業顧客自身からデータを求めるように伝えている。

・秘密保持特例に対するスタンス

民事訴訟、捜査令状、緊急事態に基づくガバメントアクセス以外の強制アクセスに関して、2022 年下半期、マイクロソフトは、連邦、州、地方の法執行機関の要求を含む米国の法的要求の 28%、合計 1,465 件の秘密保持命令を受けたことを報告している。このうち 1,184 件は連邦法執行当局によるもので、米国政府が顧客のデータを求める際に、マイクロソフトが顧客に通知することを妨げる秘密保持命令を通達した[10]。

マイクロソフトは、秘密保持は通常ではなく機密調査を保護するために一時的かつ明らかに必要な場合にのみ使用される例外であるべきだとの考えを示しており、米国政府に対し非開示命令や秘密保持命令の使用を制限するよう何度も異議を唱え、その訴えが認められている。具体例としては、2018 年 9 月 5 日、マイクロソフト、連邦国家安全保障捜査に関連してニューヨーク州ブルックリンの連邦判事によって出された秘密保持命令に異議申し立てを行っている。（秘密保持命令により、マイクロソフトがデータ開示を請求する令状を受け取ったことを企業顧客に通知することができなくなる。）また、2019 年 12 月には、メリーランド州連邦裁判所で、企業顧客に対してデータ提出の要請を伝えることを禁じた秘密保持命令に異議申し立てを行い、2020 年 1 月に政府はマイクロソフトが顧客に通知することを認めることに同意している。2020 年 9 月には、ニューヨーク連邦裁判所で、別の企業顧客のデータ要求に関連する同様の秘密保持命令に異議申し立てを行い、10 月にこの異議申し立てに対し、政府はこの顧客に通知することに同意した。

これらの訴訟活動についてマイクロソフトは、競合企業、元連邦検察官、報道機関や業界団体から支持を得ており、具体的には、競合他社の Amazon、Apple、Google、36 名の元連邦検察官、AP 通信、ガネット、ニューヨーク・タイムズ、ポリティコ、シアトル・タイムズ、ワシントン・ポストなどの報道機関、全米製造業者協会や米国商工会議所などの業界団体が署名した 5 つのアミカスブリーフから支持を得ている。

1.3 Alibaba

・ガバメントアクセスについて

Alibaba グループおよび Alibaba Cloud のプライバシーポリシーおよびセキュリティ・ホワイトペーパーには、ガバメントアクセントの可能性について言及があるが、非個人データについては言及されていない。また、ガバメントアクセスの対個人データへのガバメントア

[10] Continued progress and support in fighting secrecy orders　https://blogs.microsoft.com/on-the-issues/2021/01/05/secrecy-orders-protection-enterprise-data/

クセス対応件数やフローについて、公開情報上に記載がなかった。

・セキュリティ対策について

Alibaba Cloud のセキュリティ・ホワイトペーパーにおいて、技術的措置を中心に、細分化して説明されているが、ガバメントアクセスに関する記載はない。

Bloomberg の報道[11]では、Alibaba が米国証券取引委員会に提出した資料によると、12 以上の事業部門が中国政府や海外の政府系ファンドから出資を受けていると判明した。特に物流事業の 2 社は中国政府の出資比率が 73.5%であった。

1.4 LINE ヤフー

・ガバメントアクセス件数

LINE ヤフーは当該 6 ヶ月間で捜査機関から受領した情報開示請求と、実際に開示を行った件数について公表しており、LINE サービスとヤフーサービスで別々のレポート[12]上で公表している。

LINE サービスの透明性レポートでは、要請件数は期間ごとに、LINE、LINE Pay、その他のサービス別で公表されている。また、開示請求を受けた国ごとに、令状、操作関係事項照会、緊急避難の要請種類別内訳も公表している。

ヤフーサービスの透明性レポートでは、法執行機関からのユーザー情報開示要請について、期間ごとに、捜査関係事項照会、令状、緊急要請の要請種類別内訳と、実際に受領した要請のうち開示した割合を示している。

また、LINE サービス、ヤフーサービスともに、透明性レポート上で要請を受けた具体的な事例についての記載はない。

・ガバメントアクセスに対する対応

LINE ヤフーはガバメントアクセスに対し、捜査令状、緊急事態に基づくものを除き、原則として情報を開示しないスタンスを公表[13]している。

法執行機関よりユーザーに関する情報の開示を求められた場合でも、裁判官が発する令状によるものや関係法令によって直接 LINE ヤフーに開示を義務付ける手続きによるもの（明文の法令によって開示を間接的に強制されている場合を含みます）でない限り、原則として、

---

[11] Bloomberg　https://www.bloomberg.com/news/articles/2024-02-26/alibaba-discloses-state-ownership-in-more-than-12-business-units

[12] LINE ヤフー　透明性レポート　https://www.lycorp.co.jp/ja/privacy-security/privacy/transparency/

[13] LINE ヤフー　捜査機関への対応　https://www.lycorp.co.jp/ja/privacy-security/privacy/transparency/guideline01/

ユーザーに関する情報を開示しないとのスタンスを示している。

例外的に、LINE ヤフーにおいて開示の必要性と相当性の双方が認められる範囲においては、開示請求に応じることを検討するとしており、例外となる具体例（下記参照）を公表している。

- 例外的に、必要性が認められると考えられる場合は以下；

1．人の生命身体に対する具体的な危険がある場合であって、LINE ヤフーにおいて緊急性を認める場合

2．開示請求の根拠となっている具体的な犯罪事実が存在する蓋然性が高いと LINE ヤフーにおいて認める場合（探索的な情報の開示請求には応じない）

＜具体例＞

LINE ヤフーが提供するサービス上で行われた脅迫、ストーカーなどの事案

決済情報を不正利用され、LINE ヤフーからの身に覚えのない請求が発生した事案

LINE ヤフーが提供するアカウントサービスにおいて発生した不正アクセス事案

LINE ヤフーが提供するサービス上で行われた財産犯（詐欺など）で、LINE ヤフーが経緯などを認知できる事案

- 例外的に、相当性が認められると考えられる場合は以下；

1．上記 1 において、その危険を除去するために必要であると LINE ヤフーにおいて認める情報

2．上記 2 において、具体的な請求の根拠となっている事実や状態に直接関係があると LINE ヤフーにおいて認める情報

＜具体例＞

被疑者を特定するために LINE ヤフーが提供する ID の登録情報

LINE ヤフーサービス上で行われた被疑事実に関するログイン履歴

LINE ヤフーサービス上で行われた被疑事実に関する ID の当該サービスにおける利用履歴

- ただし以下に該当する情報については、必要性と相当性が認められる範囲であっても令状の執行によるものでない限り、開示しない。

通信の秘密の保護対象となる情報およびそのおそれのある情報

LINE ヤフーにおいて、プライバシー性が高いと判断する情報（要配慮個人情報、クレジットカード情報、対象期間や項目が広範囲にわたる情報など）

被疑者以外の者に関する情報（ただし人の生命身体の保護に係る緊急要請を受けた場合は除く）

また、LINE ヤフーはガバメントアクセスにおいて根拠となる法令についても公表[14]している。

LINE ヤフーのサービスは日本法に準拠して運用されており、日本国内からの要請の場合、検察官、検察事務官又は司法警察職員は、犯罪の捜査をするについて必要があるときは、裁判官の発する令状により、捜索・差押えをすることができ、事業者がその命令に従う義務が生じる。(刑事訴訟法 218 条 1 項) また、捜査機関は、捜査については、捜査関係事項照会等に基づき、必要な事項の報告を求めることができる。(刑事訴訟法 197 条 2 項) さらに、緊急避難として、たとえば自殺予告や誘拐等の人命の保護の必要がある場合など、人の生命、身体等に対する現在の危難を避けるため、やむを得ずに情報を開示することが適切と判断される状況となることがある。(刑法 37 条 1 項) 以上の法律がガバメントアクセスの根拠となると明示している。

日本国外の国家からの要請の場合は、「国際捜査共助等に関する法律」や、特定国家との刑事共助条約 (MLAT) 等、国際捜査協力の枠組みに基づき要請を受けることがある。これには、国際刑事警察機構 (ICPO) を経由して日本の警察が受領するケースや、大使館を通じて日本の外務省が要請を受領するケース等が含まれる。この場合においても、令状の受領やプライバシー保護組織による検証等、同様の取り扱いルールが適用されるとしている。

政府機関から開示要請が場合の対応プロセスも定め、セキュリティ＆ポリシーのページで公表[15]している。プロセスとしては、まず捜査機関等からの要請を受領したのち、あるいは緊急避難が成立し得る事態を認識したのち、適法性や適切性の検証を行い、必要に応じて社内プライバシー保護関連部門において内容を審議したうえで対応を決定する。捜査機関からの要請に法的不備や、開示請求の根拠の蓋然性が認められない場合は対応しない。検証の結果、適法性、必要性と相当性等の確認が取れた場合のみ、担当者が捜査機関への対応を行う。捜査機関への情報提供は社内で定める厳格なプロセスに則ってのみ行われており、LINE ヤフーが策定したプライバシー保護政策に反して捜査機関に盗聴やバックドアの設置を認めることはない。また、国家安全保障 (公安・テロ対策) 上の要請や検閲等、当社サービスを利用した犯罪を原因としない要請に対して当社が応じることはないとしている。

・データの保護措置

LINE ヤフーでは、ユーザーデータの保護や管理体制に対する助言・監視等を通じて、適切なデータ活用を推進することを目的に、「データ・プロテクション・オフィサー (DPO)」を任命・設置している。また、PIA (プライバシーインパクトアセスメント) の導入により、

---

[14] LINE ヤフー　捜査機関への対応　https://www.lycorp.co.jp/ja/privacy-security/privacy/transparency/guideline01/

[15] LINE ヤフー　プライバシー＆セキュリティ　https://www.lycorp.co.jp/ja/privacy-security/

ユーザーから取得したデータについて、人権を含むプライバシーをはじめとした権利利益に影響を与えるシステム、サービスおよび機能に対する PIA の実施体制を構築している。さらに、CBPR システム（APEC 越境プライバシーシステム）の取り組みを推進しており、国境を越えて移転するデータを適切に保護するルールである「APEC プライバシー原則」に企業が適合しているかを国際的に認証する CBPR システムの取得推進を行っている。加えて、NIST プライバシーフレームワークによる成熟度評価の導入・運用も行っている。

1.5 さくらインターネット

・ガバメントアクセス件数の公表

さくらインターネットは、半年に 1 回透明性レポート[16]においてガバメントアクセスの要請状況や対応内容を公表しており、約款[17]においても、公的機関からの要請で情報を開示する可能性に言及している。レポートにおける対象サービスは、「さくらのレンタルサーバ」「さくらの VPS」「さくらのクラウド」「さくらの専用サーバ」「さくらのドメイン」「ハウジング」の 5 つで、透明性レポートの分量としては、2024 年 2 月に公開された、2023 年 7~12 月対象のレポートは合計 3 ページであり、比較的少ない。

具体的には、捜査機関等からの契約に関するデータの照会対応件数を開示[18]しており、契約に関する情報について、照会対応や差押えのために提出した事例がある。

捜査機関等からの捜査関係事項照会等の要請に対し、「個人情報保護と電気通信事業に関わる法令を遵守し、開示することが適切と判断される状況であると当社が認める範囲で開示する」と述べられている。

契約に関する情報：登録された契約者の情報（契約者名、住所、電話番号、メールアドレス、生年月日等）、契約サービス情報、サービス利用料の支払情報等

契約者のデータ：契約者が契約している、さくらインターネット社提供のサーバーに記録されたデータ

・ガバメントアクセスへの対応

政府機関からの要請への対応方針としては、個人情報保護法、電気通信事業法、プロバイダ責任制限法等の関係法令やガイドラインの遵守を通じて、「個人情報」「表現の自由」「通信の秘密」の保護に努めていると記載されている。

---

[16] さくらインターネット「透明性レポート」 https://www.sakura.ad.jp/corporate/wp-content/themes/sakura-corporate/assets/pdf/TransparencyReport2023H2.pdf

[17] さくらインターネット「基本約款」 https://www.sakura.ad.jp/corporate/wp-content/themes/sakura-corporate/assets/pdf/%5Ba%5Dyakkan1_rentalserver.pdf?v=2024-01-24

[18] さくらインターネット「透明性レポート」 https://www.sakura.ad.jp/corporate/wp-content/themes/sakura-corporate/assets/pdf/TransparencyReport2023H2.pdf

基本約款においては、公的機関の規則や命令に基づき必要な範囲で情報を開示する可能性について言及がある。

2. データ保護の技術動向調査の詳細

2.1 秘密計算

秘密計算とは、データの内容を秘匿化したまま計算することができる技術の総称で、データを暗号化したままで計算処理できるため、復号による漏えい等のリスクを低減できる。複数企業が持つデータを共有して分析・活用する際、機密データの内容を社外に知られることなく企業間で活用することができる。

秘密計算の主要な関連プレイヤーは MPC Alliance、NEC、NTT、Acompany、LayerX などで、MPC Alliance は秘密計算の実装を通じた個人データと産業データのプライバシーとセキュリティ向上を目的に 2019 年 11 月に設立し、約 60 社が参加し、技術の認知度向上等に取り組む。

また、NEC、NTT ら 4 社が 2022 年 3 月、秘密計算の安全性基準を定めた文書を策定[19]した。この統一的な基準は、これまで技術を提供する IT ベンダーによって、技術の形式や暗号化される範囲が異なっており、企業が導入を検討する際に比較検討しづらい点で課題となっていたものを解消する狙いがある。

秘密計算の主なユースケース/事例としては、NEC と旭化成による、企業間でデータを秘匿したまま安全に連携させる分析基盤の構築等が挙げられる。NEC と旭化成は、秘密情報を取り扱う材料分野の製品開発において、原料サプライヤー、加工メーカー、部品メーカー等の企業間で原料情報、加工条件、評価情報等の重要データを暗号化したまま統合し、材料開発のシミュレーションを実行可能にしている。

また、データ社会推進協議会の秘密計算活用ワーキンググループの調査では、物流における共同配送可能性の判断や EV 充電設備の需要予測、系列や国をまたいだ発注管理の最適化、人工衛星の衝突回避等のユースケースが提案された。

2.2 連合学習

連合学習とは、データを 1 か所に集めず分散している環境に AI モデルを配布することで、データ集約によるリスクを避けながらモデリングする技術である。組織を超えたモデルを構築する際に、組織間でデータを直接やり取りすることを避け、モデルを組織間でやり取りすることで、データ利用の高度化とプライバシー保護を同時に解決することができる。

主に製薬などヘルスケアにおける活用に注目が集まっており、2020 年より、日本医薬研究開発機構（AMED）が旗振り役となり、京都大学等の学術機関と、武田製薬など製薬 17

[19] NEC「秘密計算の提供者向けの安全性基準を提案」
https://jpn.nec.com/press/202203/20220310_01.html

社による「連合学習」技術を用いた創薬 AI 共同プロジェクトが開始している。

連合学習の関連する主要プレイヤーは、Google や NICT、NEC などで、NICT は連合学習実用化に向け、暗号技術と組み合わせることで機微な情報を使った学習結果も共有できる技術「ディーププロテクト」を開発し、GMO サイバーセキュリティなどに供与。今後は EC サイトでの活用に向けた実験を進める予定である。

また、NEC は連合学習技術と秘密計算技術を用いた複数組織間のデータ統合の有効性の検証を目的に、京都大学大学院 医学研究科小島諒介講師、岩田浩明特准教授、奥野恭史教授との継続的な議論をふまえて、創薬における予測モデルの構築に関する実証実験を 2021 年 10 月から 2022 年 2 月の 5 か月間実施した。

連合学習の主なユースケース/事例としては、NVIDIA は 20 の医療機関のもつ胸部 X 線やバイタル情報、臨床検査値等を用いて COVID-19 に罹患した患者の酸素投与判断モデルを、連合学習を用いて構築している。

また、Google は各スマートフォンユーザーの予測変換履歴から連合学習を用いて予測変換モデルを学習させている。各ユーザーの予測変換履歴は非常にプライベートな情報で従来の学習法では取り扱いが困難だったが、連合学習を用いることで学習が可能になった。その他、自動運転などの IoT 分野での応用事例がある。

連合学習の技術的な課題としては、通信コストが高いため、必要通信回数を減らす効率的な連合学習アルゴリズムにより、通信量を削減する必要があることが挙げられる。また、共有した学習モデルから学習に用いたデータセットの情報が漏洩しないよう、差分プライバシー等を用いる際にプライバシー保護を保証する必要がある。さらに、一部のクライアントが異常な行動を起こしても全体処理に影響をきたさない頑健性が必要になる。

2.3 差分プライバシー

差分プライバシーとは、統計データに対してノイズを加えることで、統計的な有用性を維持しつつ元データの個人の特定や属性情報の推定を不可能にするためのプライバシー技術である。セントラル差分プライバシーとローカル差分プライバシーの二種類があり、分析の結果から個人データを再識別できないように保護することができる。

差分プライバシーの技術は、GAFA や米国政府などが積極的に研究・開発を行っており、2021 年 12 月欧州委員会と欧州議会が合意した「データガバナンス法案（2023 年施行）」において、匿名化・一般化・抑制などと並ぶプライバシー保護方法として、差分プライバシーが取り上げられている。

差分プライバシーの関連する主要プレイヤーは、GAFA を代表する米国 IT 企業や、LayerX

などのIT ベンダーで、LayerX は、2022 年 5 月、プライバシー保護技術に関する共同研究をリクルートと実施している。また、2022 年 6 月には、差分プライバシー技術を用いたパーソナルデータ活用ソリューション「Anonify」提供を開始している。

Google 社はブラウザ GoogleChrome の統計情報について自社で開発した手法により端末側でノイズを付与した上でデータを Google のサーバーに送信している。

Apple 社は、デバイスの情報を収集して絵文字やキーボードのサジェストに役立てているが、こちらも端末側でノイズを付与した上で Apple 社のサーバーに送信している。

差分プライバシーの主なユースケース/事例としては、米国の国勢調査が挙げられる。米国では、10 年ごとに行われる国勢調査において、個人のプライバシー保護と調査データの利便性を良質させるため、2020 年の調査において差分プライバシーを利用しており、国勢調査局はアルゴリズムのコードと文書を公開[20]している。

また、国内の事例では、あいおいニッセイ同和損害保険株式会社が LayerX の「Anonify」を活用し、テレマティクス自動車保険で蓄積した走行データを交通安全マップの作成に活用している。

その他、Uber 社の内部データ分析や Facebook が公開する社会科学研究用とのデータセットにも差分プライバシーが用いられている。

差分プライバシーを実務で利用する際には、加えるノイズと元のデータの有用性のバランスをどのようにとるかを留意する必要がある。差分プライバシーは統計データにノイズを加えることにより安全性を向上させる技術であるが、ノイズを加えるということは元の統計データとの誤差が発生する分、有用性が低下するとも言える。そのため、データそのものが持つプライバシーリスクや公開範囲によるリスクなどを踏まえ、調整する必要がある。

2.4 ブロックチェーン

ブロックチェーンとは、ネットワーク内で発生した取引のデータをブロック単位で連鎖させつつ分散管理する技術で、改ざん耐性に優れるほか、分散型の管理であるため、システムの一部に障害は発生しても維持することができる。ブロックチェーンの種類には、管理者不在で参加自由なパブリックブロックチェーンと、特定組織・団体が運営するクローズドのプライベートブロックチェーンがある。電子署名、権利移転、真贋認証、暗号資産、サプライチェーンの追跡等、デジタルデータにおける改ざん耐性を活かし、多分野で活用されており、パブリックブロックチェーンにおけるセキュリティや機密性の向上、ブロックチェーン

[20] United States Census Bureau　https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance/differential-privacy.html

間での相互運用性確保によるスケール拡大が進んでいる。

ブロックチェーン技術に関連する主要プレイヤーは、IBM、Microsoft、Oracle、Bitcoin、Ethereum などで、その動向としては、IBM は三菱倉庫、日本通運と提携し、医薬品物流における温度や位置情報に基づく品質管理を支援するシステムの検証を 2023 年 4 月に開始。製薬企業や医療機関と設立した事業体「ヘルスケア・ブロックチェーン・コラボレーション」と検討していた情報基盤を活用している。

Microsoft はブロックチェーンのベンダーAnkr 社と提携し、自社のクラウド Azure を通じ世界中から低遅延でブロックチェーンにアクセスできるようにし、Web3 のプロジェクトやプロタクト開発を支援している。

ブロックチェーンの主なユースケース/事例としては、日立によるブロックチェーン技術を活用した企業間情報連携基盤の PoC などがある。KDDI が保有する契約時の本人確認情報を積水ハウスに提供し、賃貸物件の内見申し込みの入力簡略と、スマートキーを発行した不動産会社の立会なしでのセルフ内見を実現。プロセスの証跡としてブロックチェーン上に記録している。

また、富士通では、データトラスト基盤へのブロックチェーンシステムの連携が行われており、ブロックチェーン間の相互運用性を実現する技術により、データトラスト基盤上での複数のブロックチェーンの接続を実現し、Web3 サービスの構築の円滑化を進めている。

ブロックチェーンの技術的課題としては、代表的なパブリックブロックチェーンでは、取引量が増えると手数料が高くなるとともに、処理速度が低下することが挙げられる。また、取引所への不正アクセス等による暗号資産の盗難や、ブロックチェーン間の相互運用技術を狙った攻撃等、セキュリティの懸念がある。企業利用では機密情報を扱うため、プライベートブロックチェーンの利用が多いが、維持管理コストがかかることも課題の一つといえる。

2.5 分散 ID（DID）とデジタルアイデンティティウォレット

分散 ID（DID）は、ユーザーが自分の属性情報に関するコントロール権を確保した上で、各データ保有者の属性情報のうつ必要な情報を、ユーザーの許可した範囲で連携し合う考え方である。また DID の実装としてデジタルアイデンティティウォレット（DIW）があり、「耐改ざん性」等の観点でブロックチェーン技術の活用も期待される。DID と DIW の組み合わせにより、これまでの集中型アイデンティティによる管理から自己主権型/分散型アイデンティティに移行することで、ユーザーは自分のデータをコントロールできるようになるとともに、サービス提供者側もアプリケーション、デバイス、サービスプロバイダーに対してより高い信頼性とセキュリティを担保することが可能となる。

2021 年 6 月に公開された、欧州デジタルアイデンティティフレームワークに関する規制案の中で European Digital Identity Wallet（EUDIW）が取り上げられている。EUDIW は、EU の公的・民間のデジタルサービス利用における本人確認/属性証明に利用できる DIW を、希望する全 EU 市民、在留者、企業が利用できることを加盟国に求めるものである。EUDIW の規則が施行されることで、DIW は EU 加盟国を中心に急速に広がっていくことが予想される。2023 年 8 月、EU 加盟国において、行政サービス・企業・教育機関・オンライン取引・電子署名・電子処方箋等のデジタル ID サービスと連携する「EU デジタルアイデンティティウォレット」の実証実験が開始し、社会実装の第一歩として注目を集めている。

また、中国政府関連団体が主導するブロックチェーンサービスネットワーク（BSN）は、中国国民向けに DID プラットフォームを開設。国家レベルで運営される世界初の実名分散型 ID システムになる。

日本では、「Web で流通される情報やデータの信頼性を保証する仕組み」に関する概念である「Trusted Web」を実現するための取り組みが実施されている。内閣官房のデジタル市場競争本部が「Trusted Web 推進協議会」を設立し、特定のサービスに過度に依存せずにデータ自体とそのやり取りを検証できる領域を拡大して信頼性を向上させるフレームワーク「Trusted Web」の国内推進母体として、2030 年頃の実現をめざし、ホワイトペーパーの策定や情報発信を行っている。

DID の関連する主要プレイヤーの動向として、W3C の DID ワーキンググループが DID に関する仕様の標準化を進めており、2022 年 3 月、検証可能な属性データのデータモデル「VC（Verifiable Credentials）Data Model v1.1」を発表した。

また、Ethereum でも、ERC725/ERC734/ERC735 として DID の標準化を推進している。Decentralized Identity Foundation（DIF）はオープンソースの分散型 ID エコシステムの構築に取り組んでおり、Microsoft や Accenture などの大手企業、Consensys、Blockstack、Hyperledger などのブロックチェーン関連企業がメンバーとなっている。

DID の主なユースケース/事例としては、慶應義塾大学では DID を活用したデジタル学生証の試用実験を行っている。デジタル証明書とスマホを連携し、在籍照明や単位証明、オンライン授業の本人確認などを完結できる仕組みである。また、「Known Traveler Digital Identity」は世界経済フォーラム（WEF）が開催する「ダボス会議」で取り組みが始まったプロジェクトで、海外旅行で必要なビザ申請や入国審査、セキュリティ検査などの負担を DID で軽減する取り組みが行われている。

DIW の技術的な課題としては、普及させるためには、使い易いユーザーインターフェイスとユーザーが分散型 ID を使うインセンティブとなるアプリケーションが必要になるこ

とが挙げられる。
実装面では、単純に ID を分散型システムで取り扱うだけでは必ずしもセキュリティやプライバシーが守られるわけではないため、DID の仕様に基づき実装する際にはセキュリティやプライバシーについて考慮すべき項目が多いことも課題の一つである。

2.6 データ連携基盤

データ連携基盤とは、企業や業界、国境を跨ぐ横断的なデータ流通やシステム連携の実現を目指す取り組みの総称を指す。分野を越えたデータ探索が容易になり、データ活用サービス間の相互運用性を高め、社会実装・国際展開を促進することで、学術分野だけでなく、産業やビジネス、行政や医療、教育など、さまざまな分野における課題解決が期待されており、データ主権を確保しつつデータ連携に向け、プラットフォーム整備が各国で進んでいる。

データ連携基盤に関連する主要プレイヤーは Gaia-X、IDSA、Siemens、SAP、Rockwell Automation、GAFAM、日立、NEC、NTT コミュニケーションズの他、データ社会推進協議会が挙げられる。その動向としては、Gaia-X は、欧州の主要企業 22 団体で構成される非営利団体で、ドイツ政府、フランス政府、欧州委員会の支援を受け、透明性、相互運用性、信頼性、データ主権を遵守したクラウドフェデレーションの普及を目指している。2022 年 4 月、Gaia-X はクラウドデータ交換モデルである Federation services V1 をリリースしている。
また、2023 年 2 月に Google Cloud と AWS が Catena-X（自動車バリューチェーン全体でデータを共有するためドイツで設立されたアライアンス）に参加している。

データ連携基盤の主なユースケース/事例については、Gaia-X、IDSA などから既に多くのユースケースが提示されており、Skywise、Catena-X など業界におけるバリューチェーンを横断したユースケースも実装済みである。
IoT プラットフォームとして各社がソリューションの開発を進めており、IT/OT コンバージェンスの支援やエッジ処理等のアナリティクス用途が多い。
データエコシステムは、予測モデリングにおけるインプットとして、意思決定や研究開発プロセスで活用可能である。

データ連携基盤の技術的な課題としては、研究開発のフェーズからサービス開発、実装フェーズにシフトしつつある今、データ品質等の標準化やクラウド型ソリューションのデザインマーケティングが課題で、特に日本は海外との環境認識の差が大きい。また、データのプライバシー、（法的）権利、セキュリティ、現行法の適法性やコンプライアンスに関する課題もある。

令和５年度規制改革推進のための国際連携事業
我が国データの国際的な流通実態及び技術動向に係る調査
令和６年３月

株式会社 野村総合研究所

〒100-0004　東京都千代田区大手町 1-9-2
大手町フィナンシャルシティ グランキューブ
TEL: 03-5533-2111（代表）