# データプーリング、共同分析と
# データ保護にかかるストックテイク
# （仮訳・未定稿）

2021 年 7 月

金融活動作業部会（FATF）は、マネー・ローンダリングやテロリストへの資金供与、大量破壊兵器の拡散への資金提供から世界の金融システムを守るための政策を策定・推進する独立した多国間の枠組みである。FATF 勧告は、グローバルなマネー・ローンダリング防止（AML）及びテロ資金供与対策（CFT）の基準として認められている。

FATF についての詳細は FATF ウェブサイト（www.fatf-gafi.org）を参照されたい。

本文書及び／又は本文書に含まれる地図は、いかなる領域の地位又は主権にも、国際的な境界線及び境界の画定にも、並びに並びいかなる領域、都市又は地域の名称にも影響を与えるものではない。

引用する際の参照先：

FATF (2021), Stocktake on Data Pooling, collaborative analytics and Data Protection, FATF, Paris, France,
https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative-analytics-data-protection.html



## 日本語訳について

- 本文書の翻訳にあたっては、FATF より事前に承諾を得ております。
- 本文書は、FATF の公式の日本語版ではありません。

【免責事項】

- 本文書は、金融機関の皆様その他の関係者の参考のために、翻訳監修主体（ACAMS、FISC、NRI）が無償で提供するものです。したがって、下記事項を含め、本文書の提供に関して一切保証はできません。
- 本文書は、原典にできるだけ忠実に翻訳するよう努めていますが、信頼性、完全性、正確性等を保証するものではありません。

本文書の翻訳監修

・公認 AML スペシャリスト協会

（ACAMS：Association of Certified Anti-Money Laundering Specialists）

・公益財団法人金融情報システムセンター

（FISC ： The Center for Financial Industry Information Systems）

・株式会社野村総合研究所

（NRI：Nomura Research Institute, Ltd.）


ご照会先

・株式会社野村総合研究所（NRI）

お問い合わせ用 Email：aml-qa@nri.co.jp

## 謝　辞

FATF は技術開発者、金融機関及びデータ保護当局を含む官民両セクターのステークホルダーから、本報告書の作成のために、貴重な情報、事例研究やフィードバックをいただいたことに謝意を表したい。

本報告書は、以下に記す FATF 加盟メンバーの専門家グループから寄せられた貴重な情報を基に、FATF 事務局（クリステン・アルマ）がとりまとめを行ったものである。
カナダ、欧州委員会、フランス、ドイツ、イスラエル、イタリア、日本、マネーバル事務局、ロシア、シンガポール、スイス、英国、国連、米国。

# 目 次

# 略　語

| | |
|---|---|
| AI | 人工知能（Artificial Intelligence） |
| AML/CFT | マネー・ローンダリング防止対策（AML）／テロ資金供与対策（CFT）（Anti-Money Laundering/Countering the Financing of Terrorism） |
| API | アプリケーション・プログラミング・インターフェース（Application Programming Interface） |
| CDD | 顧客管理（Customer Due Diligence） |
| DL | 深層学習（Deep Learning） |
| DLT | 分散型台帳技術（Distributed Ledger Technology） |
| DNFBP | 指定非金融業者及び職業専門家（Designated Non-financial Business and Profession） |
| DPP | データ保護とプライバシー（Data Protection and Privacy） |
| EDPB | 欧州データ保護会議(European Data Protection Board) |
| FATF | 金融活動作業部会（Financial Action Task Force） |
| FI | 金融機関(Financial Institution) |
| GDPR | 一般データ保護規則(General Data Protection Regulation) |
| MER | 相互審査報告書（Mutual Evaluation Report） |
| ML/TF | マネー・ローンダリング／テロ資金供与（Money Laundering/Terrorist Financing） |
| MVTS | 資金移動業者（Money or Value Transfer Service） |
| NLP | 自然言語処理（Natural Language Processing） |
| NRA | 国のリスク評価（National Risk Assessment） |
| PEP | 重要な公的地位を有する者（Politically Exposed Person） |
| PSCF | 民間との意見交換フォーラム（Private Sector Consultative Forums） |
| SSB | 基準策定機関（Standard Setting Body） |
| STR | 疑わしい取引の届出（Suspicious Transaction Report） |

# 要旨

1. 近年の技術進歩により、金融機関においては、大量の構造化・非構造化データの分析を効率的に行い、パターンや傾向をより効果的に特定できるようになった。データをプールし共同分析を行うことで、金融機関はマネー・ローンダリングやテロ資金供与リスクを認識、評価し、軽減する能力を高めた。その結果、こうした活動をより動的、効果的かつ効率的に特定できるようになり、民間事業者は、マネー・ローンダリング及びテロ資金供与対策の要件に、よりタイムリーかつ負担の少ない形で適合できるようになるだろう。また、情報格差を犯罪者に悪用されるのを防止する効果もある。犯罪者は不正資金のローンダリングを行うために国内外の複数の金融機関に関与しているが、各々の金融機関が有する取引に関する情報は限定的かつ部分的にとどまるからである。

2. しかし、データプーリングや共同分析もまた、プライバシーに係る個人の基本的権利の保護に抵触する可能性がある。それゆえ、いかなる情報交換を行う際にも、当該国及び国際間でのデータ保護及びプライバシーに関する法的枠組みが必ず尊重されねばならない。

3. 本報告書においては、マネー・ローンダリング対策／テロ資金供与対策（AML/CFT）及びデータ・プライバシーとその保護は、ともに重要な目標の達成に寄与する公共利益として、大きな意義を有しているものと認識されている。これらの目標は、方向性を異にするわけでも、本質的に相互排他的であるわけでもない。国内外の法的手段を通じたデータ保護の原則とルールは、人権と基本的自由の保護、とりわけプライバシー権の保護を目的としている。本報告書は、マネー・ローンダリング／テロ資金供与や大量破壊兵器の拡散資金供与等の金融犯罪を防止するためには、このような双方の目標の達成を容易にする法体制の整備が不可欠であることに留意している。そして、これらがプライバシーとデータ保護に対する個々人の基本的人権を尊重する方法で行われねばならないことに留意している。

4. プライバシー強化に向けた新技術や新興技術は、国内外のデータ保護やプライバシーの枠組みに従って、特定の利用事例における情報を保護する手段として、その将来性が期待される。プライバシー強化技術にはさまざまな暗号化ツールが用いられており、多様なアプリケーションでプライバシーを確保する。こうしたツールを利用すれば、複数の関係者が、相互間でも第三者に対しても、基となる個人情報を明かすことなく、アプリケーションの目的を果たすために、有意義な交信を行うことができる。このテーマに関する研究や議論を行う場は増えているが、技術標準は未だに何も確立されていない。かかる技術標準やオープンソースリファレンスの進展のためになすべきことは多い。それによって、プライバシー強化技術を利用してデータのプライバシーを保護できる個々の事例が明らかとなるだろう。

5. 本ストックテイク（実績評価）報告書においては、規制対象事業者が個別に、又は他の規制対象事業者と共同で実行する高度な AML/CFT 分析を促進する技術であって、商業的に入手できるもの、又

は新しく創生されてくるものについての検討が行われる。また、こうした新技術の意図された利用目的及び利用促進要因についての分析も含まれる。さらに、かかる技術の検討と導入のために、どのような政策的配慮や政治的解決策が必要かも明らかにする。

6. FATF は AML/CFT 監督機関、技術開発者、金融機関、並びにデータ・プライバシー及びデータ保護の担当当局等の関係者との対話を継続的に行う。そして、データ・プライバシーやデータ保護に係る国内及び国際的枠組みに整合する形で、AML/CFT の実効性向上に資する新技術が十分に活用されることを目指す。

## 1. はじめに

7. データプーリング及び共同分析とは、別々のソースから得られた（デジタル）情報を分析するプロセスをいう。これには、複数の当事者によって分析が行われる場合も含まれる。このようなデータプールの構造には、集中型（データプーリング）と分散型（共同分析）とがある。[1]本報告書では、金融機関相互間（国際的金融グループ内とグループ外の双方を含む）でのデータプーリングと共同分析を取り扱うこととする。データプーリングと共同分析はメリットをもたらす一方で、重大なリスク懸念も伴う。データプーリングと共同分析の実施により、マネー・ローンダリング（ML）及びテロ資金供与（TF）リスクに関する共通認識が強化され、リスク評価とリスク軽減策の改善に資する可能性のある分析ツールを利用できるようになり、こうした不法な活動をより動的、効果的かつ効率的に特定できるようになる。フォルスポジティブ（誤検知）の件数が減少するので、民間事業者における法令遵守が効率化され、一層タイムリーに、かつ負担の少ない方法で行えるようになる。さらに、犯罪者が情報格差を悪用して規制逃れできないようにする。犯罪者は、国内外の複数の金融機関と関係を持とうとするが、個々の金融機関が有する取引内容についての情報は限定的かつ部分的である。しかし、個人の基本的権利の保護に抵触する恐れもある。それゆえに、情報交換に当たっては、国内外のデータ保護とプライバシー（DPP）に係る法的枠組みを尊重することが不可欠である。

8. 近年の技術進歩により、金融機関において、大量の構造化・非構造化データの分析を効率的に行えるようになり、パターンや傾向をより効果的に特定できるようになった。ビッグデータや人工知能（AI）[2]等による先進的分析の利用により、金融機関における AML/CFT コンプライアンスの強化を図れる可能性がある。しかし、個人情報がシェアされたり、説明観点で適切ではないプロセスによってバイアスのかかった結果や誤解を招く結果が創出されたりした場合、個人の基本的人権上のリスク懸念が発生する。例えば、金融機関は、疑わしい取引をより的確に特定し、自社の顧客を評価し、リスク管理を行うために、先進的分析を活用できるだろう。先進的分析の的確性は、データセットのサイズ、質及び妥当性と概ね一致するので、こうしたツールの実効性と効率性は、金融機関（金融グループ内外を問わず）の情報共有能力の程度に左右されることになろう。

9. データの交換、プーリング、分析を行う技術は、国内外の法的枠組みに従って、個人情報を保護しなければならない。データ共有の必要性については、AML/CFT 及び DPP との関係を慎重に分析しなければならない。例えば、金融機関が収集・処理することを許される個人情報は、特定かつ明確な目的のため（すなわち目的の限定）、必要とされる範囲（すなわちデータの最小化）に限定すべきであり、かかる目的にそぐわない形でさらなる処理を行うべきではない。個人を特定できる情報への多くのアクセスを必要としない、より侵襲性の低い方法では達しえない特定目的のためにも、情報の共有化が行われるべきである。収集された情報は必要以上長期にわたって保持すべきではなく、適合

---

[1] 共同分析において、他のデータセットとともに分析する目的でデータが移動されることはない。代わりに、分析ツール側がデータに寄せられるのであって、その逆ではない。その結果、データの安全を確保し、誰がどのデータに何を目的としてアクセスしたか、管理を行うことが容易になる。

[2] デジタルトランスフォーメーションに関する基本用語の定義は、附属書 A のリストを参照。

する情報保護規則のない事業者に移転すべきでもない。

10. プライバシー強化のための新技術や新興技術は、法域内外の DPP の枠組みに則って、特定の用途において情報保護を行うための手段として有望視されている。プライバシー強化技術は、各種アプリケーションにおけるプライバシー維持を可能とする一連の異なる暗号化ツールに依存している。[3]このようなツールの狙いは、複数の関係者が、相互間又は第三者との間で、基となる個人情報を明かすことなく、アプリケーションの目的を可能とするために、有意義な交信を行えるようにすることにある。このテーマに関する研究や議論を行う場は増えているが、技術標準は未だに何も確立されていない。かかる技術標準やオープンソースリファレンスを進展させて、特定用途においてプライバシー強化技術を利用することで、データのプライバシーが保護されるかどうかについて明らかにするために、なすべきことは多い。加えて、かかる技術の目的がデータを用いて特定の自然人又は法人を見分ける（例えば口座開設（オンボーディング））ことにある場合、データ・プライバシーの保護が危うくなるかもしれない。それゆえ、現下ではデータ共有のイニシアチブを、DPP 関連の法的要請の範疇外にある非個人データ（例えば、顧客関連情報を除いた企業情報等）に限定している法域もある。

11. ドイツが FATF 議長を務めていた 2020 年 6 月、AML/CFT デジタルトランスフォーメーションに関する議長の判断に従って、FATF はデータプーリング、共同分析及びデータ保護に関するストックテイクを行うことに同意した。このプロジェクトの目的は、商業的に入手可能な技術、又は新興技術であって、規制対象事業者による先進的な AML/CFT 分析又は金融機関同士での共同分析に資するものについて検討を行うことにある。また、国内外の DPP の枠組みに適合しつつ、こうした技術をフル活用して、AML/CFT コンプライアンスの強化を進めていく際の課題や、政治的解決策の可能性についても特定していく。

12. このストックテイク報告書の構成は次の通りである。セクション 2 では、民間事業者におけるデータ共有に関して FATF がこれまでに実施してきた研究のバックグラウンドについて触れる。セクション 3 では、民間事業者におけるデータ共有と分析のために新技術利用で意図される目的と、利用の促進要因について概説する。セクション 4 では、現在開発中、あるいは利用されているさまざまな新技術について要約する。セクション 5 では、こうした技術の開発や展開を行うに当たり、質問状回答者が直面した課題や障害についてリストアップする。セクション 6 では、新技術をもっと幅広く展開する方策として、質問状回答者から寄せられた提案について概観する（これについては、FATF が現時点で正式に承認したものではない）。

13. 本プロジェクトの範囲に関しては、この報告書で取り扱うのは民間事業者間（private-to-private）のデ

---

[3] プライバシー強化技術としては以下のものがある。準同型暗号（HE）、完全準同型暗号（FHE）、ゼロ知識証明（ZKP）、セキュアマルチパーティ計算（SMPC）、関数暗号（FE）、グループ／リング署名（GRS）、個人情報検索（PIR）、プライベートセット交差（PSI）、検索可能暗号（SE）、ブラインド署名（BS）、
https://csrc.nist.gov/CSRC/media/Projects/pec/documents/suite-draft1.pdf; ID ベース暗号（IBE）等。
例えば、https://csrc.nist.gov/projects/pec;
https://csrc.nist.gov/CSRC/media/Presentations/icmc2020-slides/images-media/20200923-PEC-ICMC-slides.pdf;
https://zkproof.org/ を参照。

ータプーリング及び共同分析（公的機関の支援を受けたものや公的機関が進める取組みも含む）とする。官民間での情報共有（特に、報告事業者と金融情報当局機関／法執行当局）のための新技術の利用については、本報告書とは別に、運用機関のための AML/CFT 分野におけるデジタルトランスフォーメーション報告書にて検討を行うこととする。

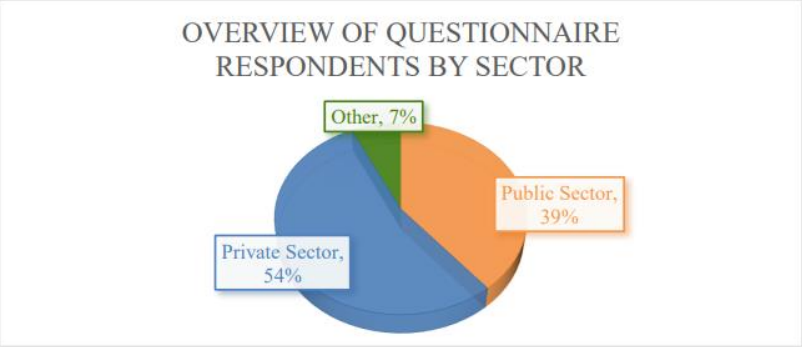
## 2. 方法論

14. FATF は 2020 年 11 月、共同分析の促進のために利用可能なさまざまな新技術を特定すべく、AML/CFT を所管する政府当局や民間セクターのステークホルダー（学識経験者、金融機関、技術開発者を含む）に対して、デジタルトランスフォーメーションに関する質問状をオンラインで送信した。得られた回答総数は 188 であった。本報告書では、この質問状への回答に加え、文献調査や、官民両セクターのステークホルダー（金融機関、技術開発者、並びに AML/CFT 及び DPP 当局の代表者等）へのインタビュー結果についても整理する。

15. 質問状では、共同分析を促進するための新技術利用により期待される効果について、ステークホルダーの見解を伺った。それとともに、データを安全に、共同で分析するために、新技術がどのように利用されているかについても質問した。また、こうした技術の導入に当たっての課題や政策的配慮についての質問や、AML/CFT 及び DPP の監督機関との関与のあり方に関する質問も含まれた。質問状では、回答者（以下、「回答者」とは、質問状への回答者、並びに FATF 各国代表が指名した専門家を含め、事務局がコンタクトした専門家のことをいうものとする）によるグッドプラクティスについて説明するケーススタディの提供も求めた。

16. 回答者の構成は下図に示す通りである。パブリックセクターのレベルでは、回答者の大半が監督機関に分類される。一方、民間セクターのレベルでは、大半のインプットは金融機関及び技術開発者によるものであった。[4]質問状への回答の中心は、「大銀行」に分類される機関からであった。回答の地域別構成をみると、欧州（53%）、米州（20%）、アジア・オセアニア（18%）、アフリカ（9%）の順であった。[5]

**図 1. 質問状への回答のセクター別構成比**




[4] 「民間セクター」と回答したもののうち、54%が「金融機関」、46%が「技術開発者」としている。
[5] 「その他」に分類されるのは、非営利組織、シンクタンク及び学識経験者である。

## 3. 背景事情

17. データプーリングと共同分析は、FATF にとって全く新規の取組みというわけではない。FATF 勧告内には、民間セクター相互間での情報共有に関係する要素が含まれている。例えば、勧告 18 では、金融機関グループの顧客管理(カスタマー・デューデリジェンス(CDD))目的及びML/TFリスク管理の文脈における情報共有を求めている。共有される情報としては、不自然とみられる取引や活動についての情報や分析(そのような分析がなされている場合)に加え、疑わしい取引の届出(STR)、その根底にある情報、又はSTRが提出されたという事実が含まれることもある。かかる要求は、FATF 用語集において金融グループと定義されるすべての事業者(国内、クロスボーダー環境の双方)に適用される。[6]さらに、勧告 21 においては、金融機関とその取締役、役員、従業員が、勧告 18 の定めに基づくグループ全体の ML/TF リスク管理要求に従う限りにおいて、STR 又は関連情報を提出したという事実を明らかにできるとされている。最後に、勧告 2(AML/CFT 要求と、DPP 及びこれと類似の規定との整合性を確保するために、政府当局が協力・連携するよう求めるもの)に定める措置には、情報共有への実際上又は認識上の障害対応において、各国政府当局が果たす役割が重要であると強調されている。

18. こうした勧告は、金融グループという文脈において、情報共有の限界を定めたものであるが、FATF 基準においては、現在のところ、金融グループ外の事業者における情報共有の要件について同様の定めがあるわけではない。

19. FATF は 2017 年、Guidance on Private Sector Information Sharing(民間セクターにおける情報共有に関するガイダンス)を公表した。同ガイダンスにおいては、金融機関同士で行われる、FATF 勧告を超える情報共有の取組みにスポットが当てられている(22～25 頁)。これ以降、本分野においては、地域レベル／国レベルで多数の取組みが進められている。例えば、EU による第 5 次マネー・ローンダリング防止指令の、拘束力を有しない前文 46 において、「犯罪者は、不法収益が検知されないよう、多数の仲介機関を経由して資金移動をしている。それゆえ、国内法に定めるデータ保護ルールに十分配慮を払ったうえで、信用機関や金融機関が、同一グループ内だけでなく、他グループの信用機関や金融機関とも情報交換できるようにすることが重要である」[7]と明記されている。欧州データ保護会議(EDPB)は 2020 年 12 月、とりわけ予定されている法律改正[8]は、プライバシー及び個人データの保護と AML/CFT 手段との相互作用の問題や、現場での具体的な適用に取り組む良い機会となるとするステートメントを採択した。EDPB は、この 2 つのルール(AML/CFT と DPP)をより密にかみ合わせることで、個人データ保護と AML 枠組みの効率化の両面で実効が上がると確信している旨記している。EDPB は、個人データ処理のための明確な法的根拠の必要性に繰り返し触れるととも

---

[6] FATF 用語集において、金融グループとは、「親会社又はその他いずれかの種類の法人であって、それ以外の者に対して管理・調整機能(基本原則の下にグループの監督を行う機能)を行使する法人と、グループレベルでの AML/CFT ポリシーや手続きが適用される支店及び／又は子会社とからなるグループをいう」と定義されている。

[7] 2018 年 5 月 30 日付の欧州議会及び欧州理事会指令(EU)2018/843 の前文 46 は、マネー・ローンダリング又はテロ資金供与の目的での金融システムの利用を禁止する指令(EU)2015/849、並びに指令 2009/138/EC 及び指令 2013/36/EU を改正するものである。

[8] EU は AML 分野の規制をハーモナイズする形での単一のルールブックを計画している。

に、EU 一般データ保護規則（GDPR）第 5 条（1）に従って、特に情報共有と国際間のデータ移転に際しては、かかる情報処理を行う目的を明確化し、制限を設けることが必要であると言及してきた。（EDPB、2020[1]）

20. プライバシー保護の強化に向けたさまざまな技術[9]の導入と採用が進むにつれて、民間セクターでは、顧客管理を含むデータのプーリングと共同分析を行うために数多くの取組みが進められ、試験的プログラムが多数開始されている。こうした取組みは、AML/CFT コンプライアンスと違法な活動を特定する能力の強化を目指すものである。このような国際的な取組みにおいて浮き彫りにされているのは、新たな技術進歩を背景として、データプーリングと共同分析への取組みを進めるために、金融機関がリソースの共同利用とプーリングに意欲を示していること、そして、FATF が既存の方向性から一歩踏み出す必要性に迫られていることである。

[9] プライバシー強化技術（PET: Privacy enhancing technologies 又はプライバシー強化暗号と呼ばれることも多い）は、「データ所有者が基となるデータを必ずしも公開しなくても、そのデータの計算を可能とする専門的な暗号化機能。この技術を利用して、クエリ及び検索結果の暗号化を維持して（又は非公開にして）要求者だけ見えるようにし、データ所有者が検索クエリを見られないようにできる。」（マクスウェル、2020[16]）

## 4. 民間セクターにおける AML/CFT 情報共有・分析の目的と前提条件

21. FATF は最近、金融機関・グループ内及び他の金融機関・グループとでケースバイケースで行われる、AML/CFT 目的の（例えば、レッド・フラッグが発せられた顧客についてのレビュー等）、特定情報の狭義の共有に関する調査を実施した。本ストックテイク報告書は、この調査内容を踏まえ、民間事業者間の大規模なデータプーリングと共同分析に依存する技術イノベーションによって、DPP 要件も尊重しつつ、AML/CFT/CPF（Countering Proliferation Financing：拡散金融対策）の目標をどのように円滑に達成できるかについて考察を行うものである。

22. 個人の機微情報の暗号化が行われている他分野（医療分野等）[10]で試行されている新技術は、国内外で相違する DPP 法制を尊重しつつ、AML/CFT 目的のための情報交換や分析を可能とする革新的な解決策につながるかもしれない。事実、質問状回答者の 93%が、新技術によって、これらをはじめとする AML/CFT 分野におけるデータ共有の課題（例えば、競争上の目的のための機密情報保護等）が克服できるかもしれないと述べている。

### 4.1. データ共有を行う理由

23. データ共有を行うことは、マネー・ローンダリング（ML）、テロ資金供与（TF）及び大量破壊兵器の拡散資金供与（PF）に対抗するため、極めて重要である。複数の国をまたぐ ML/TF/PF の企てに国境は関係ない。また、犯罪者は複数の金融機関を悪用して、不法に獲得した資金の洗浄を行う。金融機関と政府当局とが、複数の国境や異なるプラットフォームを横断的に把握し、犯罪者の活動を集約的に調べることができてはじめて、違法行為が明るみに出ることが少なくない。このことは、国際的な資金洗浄を巡るさまざまな事例において、複数の法域にまたがる金融機関の弱点を突いて、犯罪で得られた莫大な収益の洗浄が行われている事実からも明らかである。複数の金融機関が協調して、活動を集約的に分析できるようになれば、金融インテリジェンス全般の質の向上につながるだろう。

24. ML/TF のために国際的な金融システムが悪用されるのをより的確に検知し、防止するために、金融機関は、同一グループ内、及び他の金融グループに属する金融機関と協調的に取り組んでいく可能性について、これが DPP 要件に適合するか否か、またどのような場合に適合するのか、検討すべきだろう。同時に金融機関は、DPP 要件に反した場合に負う責任について認識すべきである。一般的に、金融機関が個人データを共有することは、当該金融機関が営業活動を行う法域において、かかる情報共有が許される範囲（データの種類、共有環境、コミュニケーションチャネル等）が法律上に明記されている場合を除いては推奨されない。

25. 上述したような情報共有を政府当局がサポートすることはあるが、業界レベルで情報共有が行われる場合も同じくある。そして、データ共有を行う範囲と目的とが法律上明確に規定されていて、民間セクターが実行する情報共有に対して、情報保護のための監督が有効になされているならば、政府の

---

[10] 例えば、医療分野においては、情報共有と共同調査を円滑に行うための連合学習データ（連合学習：データを集約せずに分散した状態で機械学習を行う手法）の利用が進んでいる。（ティム・フルセン、2020[19]）

関与は必ずしも必要ではない。

26. 質問状回答者は、より広範なデータセットへのアクセスが可能になることで、結果が改善され、情報に基づく意思決定ができるようになると述べている。それは、誤検知が減少し、優先順位付けが進み、金融犯罪調査の効率がアップし、企業データの質が向上し、運用効率の大幅な上昇が可能になるからである。もちろん、共同分析の全般的な正確さを担保するために、データの質とデータの標準化が重要な要素であることは論を待たない。これについては、セクション 6.2.で改めて述べる。

27. 複数の金融機関が共有しているデータに高度な分析手法を適用することにより、傾向や潜在的に疑わしい活動を明らかにできるようになった。こうした検知を行うことは、従前の、単一金融機関による分析では不可能であった。例えば、質問状回答においては、名寄せ（エンティティ解決）やネットワーク分析等のツールや手法によって、情報間の紐付けができるようになったことが指摘されている。これまでのように、データが断片的にとどまるとともに、調査に用いられる技術的ソリューションが個別事業者へのコンプライアンス型チェック指向であったときには、こうした情報間の相互関係は見逃されがちであった。さらに、分析手法を利用することで、金融機関において、金融犯罪リスクの分析をより大規模に行えるようになるとともに、より先見的なリスク特定が可能になった。結果的に、新技術によって、交換された情報の価値と有用性の向上が図られそうである。次に示すケーススタディは、2018 年から 2020 年にかけて英国で行われたデータ共有の概念実証で得られたメリットの実例を記したものである。

### BOX4.1. 英国におけるトリバンク・パイロット

2019 年に英国において実行されたトリバンク・パイロット（TriBank Pilot）は、3 大銀行の参加の下、仮名化された取引データ（日付、金額、トークン化された出入金口座情報（訳者注記：トークン化とは、機密データを利用可能な意味を持たない非機密データに置き換えること））を結合させて、総合的に分析するものである。参加した銀行は、住所、氏名等、個人の特定につながる情報は公開しなかった。この取組みによって、仮名化された取引データをパイロットに参画する複数の金融機関から安全かつ効果的に収集できること、こうしたデータを結合・紐付けして有意なデータセットとして一元化できること、そして、集中的に分析できることが実証された。当該技術プラットフォームによって、取引口座についての基礎的な情報が一切ない状態であっても、大規模で複雑なクラスターを自動で特定し、広大なアカウントベースから選び出すことができ、参画する金融機関においてさらなる分析を行うべき候補として提示できることが実証された。

このパイロットにおいては、共同 AML/CFT 分析における 2 つの補完的アプローチが実証された。①参加金融機関は、疑わしい／懸念されるアカウントに関する初期情報を提供し、このプラットフォームは先行している知見（インテリジェンス）を大幅に拡張して、「全体像」を提示する、②金融機関から提供される先行知見（インテリジェンス）が一切なくても、このプラットフォーム自体が重大懸念領域を自動認識する。こうした 2 つのアプローチは共生的に作用して、実効性のある銀行横断的な取引モニタリングフレームワークを創り出す。それによって、参画するそれぞれの金融機関は、顧客の秘密情報を一切明かすことなく、自らが保有するインテリジェンスを提供し、他の金融機関が保有するインテリジェンスの便益を享受することができる。

28. 一部の地域においては、フィンテックをはじめとする新業態の企業が銀行業界に参入しはじめていることから、旧来の既存銀行からの顧客離れが発生し、大きな市場シェアを有する単一の銀行でのバンキングに代えて、複数の金融機関を利用してバンキングが行われているとの指摘もあった。このことは、幅広い領域の金融機関に個々の顧客データの拡散が加速し、個別金融機関で得られる情報からだけでは、ML や TF の知見を得るのが一層困難になることを意味している。このような状況を背景として、高度な分析を適用して、顧客リスクの評価や疑わしい取引の可能性の特定をより正確に行うのに十分なデータセットを寄せ集めるために、民間事業者間でのデータ共有や連携がさらに促進されるだろう。

29. そうではあるが、データ処理に際しては、それを行うべき合理的な目的との関連において、相応の程度で行われねばならない。データ処理の全段階を通じて、関連する利害と権利との公正なバランスが確保されねばならない。個人データの扱いに当たっては、公正かつ透明性のある方法で処理を行うとともに、明確、特定かつ合法的目的のために、データ保持ルールに適合する形で収集が行われなければならない。データ共有と技術利用のすべての側面（AML/CFT の実効性、DPP 及び競争上の影響等）にわたる評価が最初に行われるべきである。そのようにして、計画の実行に先立って、すべての側面に適切な配慮が払われるようにしなければならない。

### 4.2. 民間事業者間のデータプーリングの取組みにおいて掲げられている目標

30. 金融機関が情報共有を行う決定（グループ外の金融機関のほか、法域外の可能性も含め）を下す場合、その理由は以下の円滑化を図ることである（本リストは網羅的ではない）。

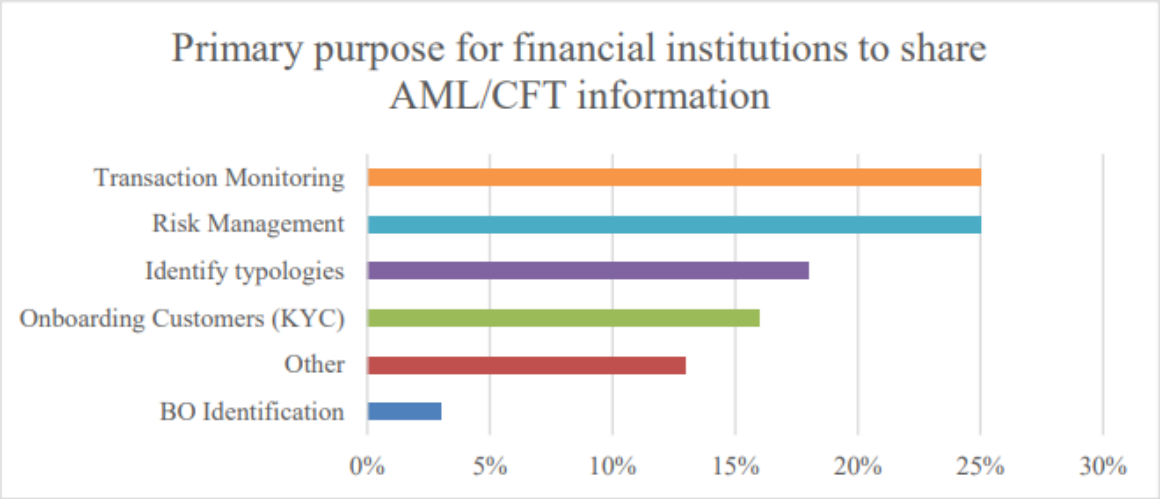
- 例えば以下のような顧客管理**手段**を採用すること。
  - 組織的リスク評価：より正確に ML/TF リスクの測定を行うために、新製品や新サービスの指標を改善する。
  - 顧客口座開設（オンボーディング）：自然人又は法人が、金融グループ内外の他の金融機関において、これまでにリスク警戒や懸念アラートの対象となったことがないか確認する。ビジネスライン横断的に、同様の行為が存在しないかチェックすることにより、顧客のリスクレーティングを検証する。
  - 取引のモニタリング：顧客の取引パターンを調査することによりレイヤリングを検知し、金融プロファイルを評価する。全金融機関にわたって検知されたすべての異常活動に関するフォローアップを実施する。疑わしい取引の特定を改善する。取引の閾値を採用する。
  - 事業関係のリスクマネジメント：顧客情報の継続的アップデートを行う。複数金融機関において同一人物が顧客口座開設（オンボーディング）されることにより、グローバルにリスク・エクスポージャーを認識する。新情報や顧客行動の変化に応じた動的リスクマネジメントを行う。

- 真の受益者の特定：真の受益者把握の正確性の向上。複数の金融機関をまたがる同一の真の受益者の特定。ペーパーカンパニー検知能力の強化。真の受益者情報の記録の効率化。

- 以下のような、エンドツーエンドの**技術フロー**。
  - 犯罪類型の識別：新しい犯罪類型の識別と予防手段の構築を迅速かつ的確に行うとともに、知り得た情報を他の金融機関や公的機関と共有する。
  - インテリジェンスに基づく調査：調査の取組みを整理して、より明確な調査結果を導き出す。

31. 質問状回答によれば、AML/CFT 目的における情報共有又はデータプーリングの主たる目的は、取引モニタリングとされている。しかし、かかる取組みの目的には、前述のリストに記された複数のオプションも含みうるとする回答もあった。次のグラフは、質問状への回答を整理したもので、金融機関が AML/CFT 情報の共有を行うさまざまな理由が記されている。

**図 2. 金融機関が AML/CFT 情報を共有する主な理由**




注：回答者は上記リストから 1 つのみを回答。

32. 上記グラフにおける「その他」回答の主なものは以下の通りである。

- AML/CFT 全般の検知、防止、調査において、より的確な意思決定ができるようにするためのリスク削減。
- データ処理パラメータの開発と最適化のためのフィードバック・ループの円滑化。
- インテリジェンスに基づく調査の実施。
- データに基づく犯罪類型の発展推進。

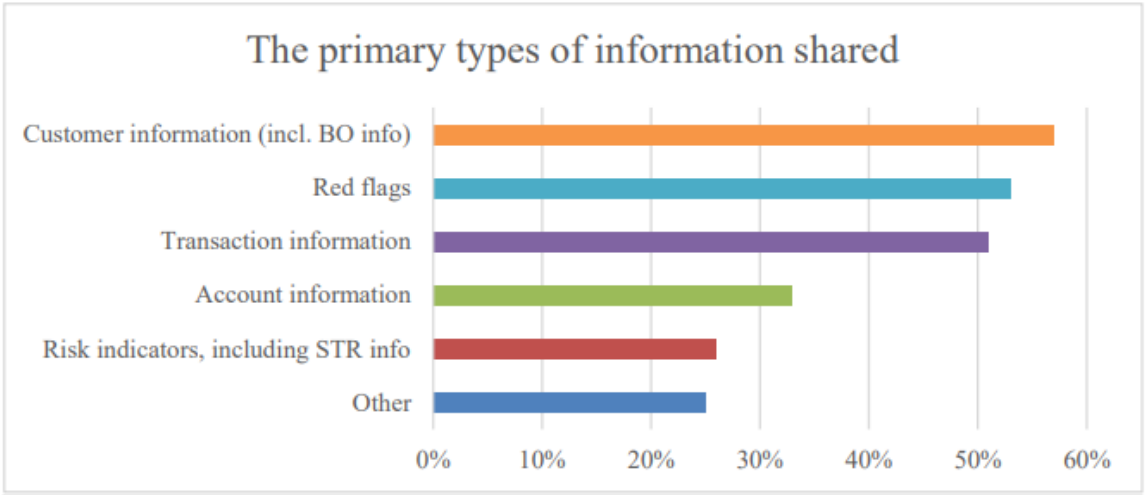
### 4.3. 共有可能なデータ

33. 前述の特定目標のために利用される暗号化された共有データとしては次のものが含まれる：顧客管理（CDD）情報、取引情報、レッド・フラッグ、顧客リスクの兆候（STR 提出の有無等）、コルレスバンキ

ング関係の金融機関の最新情報（リスク評価の改善の余地がある顧客情報、当該金融機関において実施されている顧客管理を含む）。

34. 質問状回答によれば、共有（検討中を含む）されているデータの主たるものは、顧客情報（真の受益者情報を含む）、レッド・フラッグ関連情報及び取引データである。回答者は、個々の取組みの目的に応じて、異種情報が組み合わされて共有されることも多いとしている。しかし、顧客情報が共有されるのは、暗号化された状況下で、限定的なPOCにおいて実施する場合に限られるとする回答もあった。下図は質問状回答を整理したもので、回答者が現時点で共有している（又は共有に向けて検討している）情報の類別を示している。

**図 3. 共有されている主な情報の類別**




注：回答者は上記リストから該当するものを複数回答。

35. 上図の「その他」には以下のものが含まれる。

- 取引主体識別子（LEI）[11]参照データ
- 犯罪類型の情報
- アラート処理／結果（社内モデルチューニング向け）

[11] 取引主体識別子（LEI）は、金融取引に参画する取引主体を明確かつ個別に識別できるように割り当てられた20桁の英数字コードである。詳細は、「取引主体識別子（LEI）の導入」、Global Legal Entity Identifier Foundation（GLEIF）、www.gleif.org/en/を参照。

### BOX4.2. 日本における機械学習と人工知能に関する POC

データ保護とプライバシー（DPP）規則に整合したデータ共有を促進するため、日本では、独自の概念実証研究（POC）プロジェクトが進められている。同プロジェクトには日本のいくつかの金融機関が参加し、金融庁の後援の下、新エネルギー・産業技術総合開発機構（NEDO）が主催している。本プロジェクトでは、データの共有やプーリングを行うことなく、各金融機関の取引データセットを統合したアルゴリズムにより、単一の AI モデルを作成する。

本 POC は、取引モニタリング及び制裁スクリーニングにおける真の陽性スコアの可能性を計算することにより、人間による判断を円滑化する AI モデルの構築を目指している。

この POC においては、個々の金融機関の取引データは共有もプールもされず、代わりに次の 2 つのアプローチがとられる。すなわち、(1) 各金融機関のデータセットを学習した AI モデルそのものを統合する。(2) 1 つの金融機関のデータセットを学習済みの AI モデルを調整し直して、別の金融機関のデータセットを再学習させる。このプロセスを繰り返し実行して、この AI モデルの精度を向上させる。

本プロジェクトから得られた結果によれば、AI に基づく取引モニタリング及びスクリーニングシステムの共有化は、検出結果のトリアージ（優先順位決定）プロセス及び誤検知の取扱いを含め、ワークロードを低減させる可能性を十分に有している。正確性と解釈可能性の点では、従来のトリアージプロセスにおいて人が行ってきた作業の一部を AI に基づく判断に置き換えられる可能性が示された。参画する金融機関の間でこうした取組みがもっと幅広く展開されるならば、AML/CFT 全般の効率化と実効性の向上につながるだろう。

## 4.4. 新技術利用の促進要因と前提条件

36. 本セクションにおいては、AML/CFT 目的における、民間事業者間での情報共有及び共同分析の利用に係る現状を概観するとともに、こうした技術の発展とその後の普及を可能にする環境、これを後押しする要因やその前提条件について明らかにしていく。

37. 質問状回答者のうち、当該法域の金融機関において、AML/CFT 目的で他の金融機関とデータ共有やプーリングを行うために新技術が利用されていると回答したのは 40%に過ぎなかった。そのうち 72%は、このような取組みは官民両セクターの連携の下で推進されていると回答した。

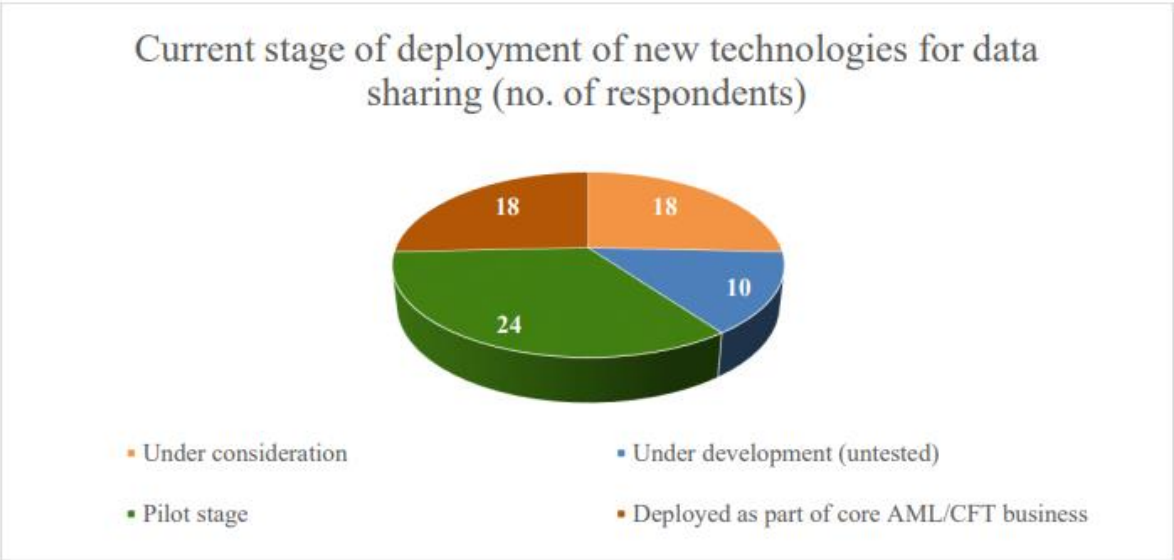
38. 下のケーススタディは、民間事業者間における AML/CFT 情報共有のための環境整備を官民の連携により進めた事例を示している。

### BOX4.3. 中国における情報共有プラットフォームの試行

AML 当局である中国人民銀行の助言と監督の下で、中国の複数の金融機関により、AML リスク情報共有プラットフォーム（以下「情報共有プラットフォーム」という）の試行が進められている。これは、ブロックチェーン、デジタル ID、そして信頼できるプライバシー強化技術を統合するものである。この試行プラットフォームにおいて、これに参画する金融機関は、当該金融機関が認識する高リスク顧客の情報を、デジタル ID 番号（DID）やリスクラベル等で暗号化し、ブロックチェーンにアップロードできるようになっている。参画する金融機関からの当該顧客に関する情報の要求を受けて、安全なコンピューティング・プラットフォームを通じて、ブロックチェーンにおいて照合が行われる。デジタル ID 番号の照合が行われるのは、検索対象となっている個人氏名と国内 ID 番号とが、他の参画金融機関によってアップロードされている場合に限られる。照合が完了すると、情報共有プラットフォームはマネー・ローンダリングのリスク情報を抽出し、復号可能な暗号文で返す。こうした一切の計算結果は、処理ユニットにおいて直ちに削除される。続いて、情報を要求した金融機関は、ある個人が別の金融機関でも高リスクとされている旨のアラートや、他の金融機関からも情報の要求が出されている等のアラートを受信する。このように、本プロジェクトの設計仕様においては、金融機関同士での実際の顧客情報の交換は行われない。

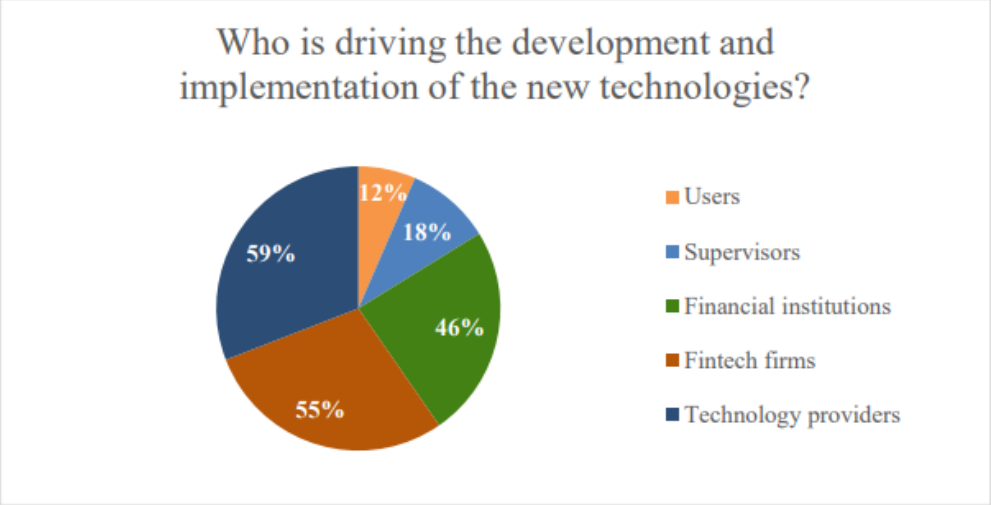
39. 質問状回答において、新技術を利用して民間事業者間の共同分析やデータプーリングを円滑化しようとする取組みの大半が、いまのところ開発や試験の初期段階にあることが明らかとなった。例えば、回答者の大半（74%）が、このような技術の開発段階に関する問いに対して、いまだ検討中か、開発／試験段階にあると回答している。下図は、このような新技術の展開が現時点でどのような段階にあるかという質問への回答を整理したものである。

**図 4. データ共有のための新技術の展開状況**



40. 下図に示す通り、データプーリングと共同分析のための新技術をテストしたり利用したりするさまざまな取組みを牽引しているのは民間セクターであり、とりわけ、大規模な多国籍金融機関、リテールバンク及び商業銀行、並びにインターネットバンク（フィンテック企業等）がその中心であることが質問状回答によりわかる。

**図 5. 新技術の開発及び実行を牽引する事業者**




注：回答者は上記選択肢から複数回答。

41. 情報共有のための新技術の利用を促進する他の要因としては、AML/CFT の効率化と実効性の向上を確実にする新たな技術発展に加え、民間事業者間のデータ共有における新技術の展開に有利で明快な規制枠組みの存在等が挙げられる。

42. 一部の法域においては、AML/CFT の規制当局と監督機関が、民間セクターと密接に関わり合って、AML/CFT 分野における共同分析とデータプーリングのための新たなアプローチや新技術の開発を後押ししている。新たなプロジェクトを立ち上げるに際して、特に AML/CFT 監督機関と DPP 当局に相談しているとする回答もあった。民間セクターの回答において、監督機関や政府当局と率直な対話を行うことが、新技術を利用する取組みを成功させ、最終的には、これを効果的に実行するために不可欠との指摘があった。

43. ある状況においては、民間事業者間の共同分析技術を普及させるためには法改正が前提条件との指摘があった。かかる状況下では、こうした取組みを成功裡に進めるために、AML/CFT 政策立案者や AML/CFT 監督機関と関わり合いをもつことが必要とされる。次のケーススタディは、民間セクター主導による AML/CFT データプーリングの取組み事例であるが、今後のさらなる普及には法改正が必要となる。このケーススタディは、さまざまな所管当局と民間セクター参加者との率直な対話の重要性を示している。

### BOX4.4. オランダの取引モニタリング（TMNL）

TMNL はオランダの 5 つの銀行による協調イニシアチブで、共同で為替取引をモニタリングすることにより、マネー・ローンダリングやテロ資金供与の可能性を示すシグナルを特定するものである。本報告書執筆時点では、TMNL ユーティリティは構築中である。

取引データの組合せに対する共同モニタリングを通じて行うこのイニシアチブの主目標は、個々の銀行だけでは特定できない不自然な取引パターンを特定することにより、マネー・ローンダリングの検出を強化することにある。そのため、TMNL においてはいわゆるマルチバンク・アラートに注目する。こうした共同モニタリング・プラットフォームに加え、参加する銀行は、オランダの AML 法の下での既存の義務に従って、自身の取引に対するモニタリングも継続する。

参加するオランダの銀行がプールする取引データは、オランダで管理される銀行口座上で実行される取引に関連するものに限定される。長期的には、他の銀行も TMNL に参加するとみられている。TMNL の稼働後は、不自然な取引の可能性又はマネー・ローンダリング等の違法な活動の疑いを示唆する一連の取引に TMNL がフラグを立てると、決済チェーンのすべての参加者は、取引に関するアラートを受け取る。アラートを受領した銀行は、TMNL から受領したアラートを独自にレビューした上で、オランダの資金情報機関（FIU）に対して不自然な取引に係る届出を提出するか否かについて、それぞれが決定する（届出を提出するか否かの決定についてはプラットフォームでは共有されない）。本報告書執筆時点では、本プロジェクトは法人顧客関連の取引情報に焦点を当てている。

現時点において TMNL が構築しているプラットフォームは、以下の目的で必要とされるものである。すなわち、すべての取引データを受領すること、共同モニタリングのために取引データを組み合わせること、及び異常なマルチバンク・アラートの疑いを参加銀行に通知すること。このプラットフォームはクラウドベースで、参加銀行の 1 つの、いわゆるアクセラレーター・プラットフォームのコピー上に構築されている。特別に作られたこのプラットフォームの設計方針の 1 つは、構成のコンポーネント化、すなわち、最新のツールを将来使えるようにすることである。銀行と TMNL との間で取引データに関する機微なプライバシー情報を交換する際は、仮名化して行う。

このプロジェクトを進めるため、オランダの参加銀行は、データ保護当局、財務・法務・治安省（Security Ministry）、金融犯罪調査担当機関（Fiscal Information and Investigation Service）及び FIU 等の政府当局と密に共同している。TMNL のフォーメーションは、オランダ政府が 2019 年に公表したマネー・ローンダリング・アクションプランに沿っている。この計画の一環として、共同取引モニタリングを全面的に可能にするため、AML/CFT 法の改正が予想されている。[12] 改正法は、オランダの銀行が、より多くの取引データや不自然な取引に関する情報を共有できるようにし、取引モニタリングプロセスの外部委託の禁止を解除し、共同取引モニタリングプロセスにおいて、固有の個人識別番号である市民サービス番号（Civil Service Number）の使用を可能にすることを目指している。

[12] 本報告書執筆時点において、TMNL の活動を可能とする法律は策定中で、国会には提出されていない。

44. 金融機関と国の AML/CFT 当局や DPP 当局との率直な対話に加えて、質問状回答者は、新技術が国の（又は超国家的な）AML/CFT や DPP に関する法及び規制にどのように影響するか試みることが可能な仕組みである「規制サンドボックス（又はイノベーションハブ）」の価値に言及している。しかし、最近公表された、国連事務総長の「開発のための金融包摂に向けた特別擁護（Special Advocate for Inclusive Finance for Development、UNSGSA）」のフィンテック・ワーキンググループ報告にある通り、規制サンドボックスの設置は複雑で運営費用が嵩むことがある[13]。

45. 質問状回答者は、サンドボックスやイノベーション・オフィス（イノベーション・ハブ）によって、機会、リスク、脆弱性、軽減策を参加金融機関が特定しやすくなることから、新たなアプローチの発展と実行を容易にして促進することになり、これらを牽引し、これらを可能にする環境を形成する役割を果たすと強調している。次の BOX には、AML/CFT データ共有のための新技術の規制サンドボックス及びイノベーション・ハブの事例が含まれている。

[13] UNSGSA フィンテック・ワーキンググループ及びケンブリッジ大学オルタナティブ・ファイナンスセンター（CCAF）（2019）。インクルーシブ・フィンテックを可能にする政策イノベーションに関する初期の教訓：イノベーションオフィス、規制サンドボックス及びレグテック。UNSGSA 及び CCAF 事務局：ニューヨーク及びケンブリッジ（英国）。

### BOX4.5. 新たなアプローチの発展を実現する規制環境

**英国**

金融行為規制機構（FCA）は 2019 年、テック・スプリントを開催し、プライバシー強化技術として知られる暗号化手法により、データセキュリティ法との整合性を維持しつつ、どのようにしてマネー・ローンダリング情報及び金融犯罪懸念情報の共有化を進められるかについて検討を行った。このイベントには業界代表者も参加し、自らのイニシアチブ、技術、得られた結果を紹介した。また、AML 監督機関と英国情報コミッショナーズオフィス（ICO）の代表者らも出席した。FCA は最近、デジタル・サンドボックス・パイロットを運営しており、不正行為や詐欺に対抗するために新しいソリューションやプロダクトを開発しようとしている革新的な企業に対して、統合的な銀行取引データセットへのアクセスを含む一定のサポートを行っている。こうした革新的企業のいくつかは、このようなソリューションの開発に当たり、PET（Privacy enhancing technologies）を採用している。この試みは 2021 年 2 月に完了しており、将来デジタル試験環境を繰り返す際に有益な知見を与えるだろう。

**フランス**

フランス健全性監督規制機構（French Autorité de Contrôle Prudentiel et de Résolution（ACPR））は、先進的な金融エコシステムを結びつけるフィンテック・イノベーション・ハブを組成した。少人数からなるこの特設チームは、革新的なプロジェクトを有するすべての関係者に開かれ、イノベーションの観測所としての役割を担っている。また、ACPR 内における SupTech の役割も受け持つ。すなわち、監督業務における新技術を統合することである。ACPR フィンテック・イノベーション・ハブは、過去 2 年間に AML/CFT に関連する 4 つのワーキンググループを率いてきた。こうしたワーキンググループには業界代表と公的機関（FIU、セキュリティ・データ保護当局）が集まって、遠隔での顧客確認（KYC）、暗号資産セクターにおける AML/CFT プロセス、AML の観点からみた銀行と暗号資産サービス・プロバイダーとの関係等に関する検討が行われた。さらに、ACPR フィンテック・イノベーション・ハブは、金融部門における新技術の機会と規制上の課題について検討するため、学識経験者との対話も設定した。かかる文脈において、ACPR は 2020 年 3 月、データ共有とデータプーリングを巡るイベントを開催し、最先端手法を用いて、必ずしもデータを共有しなくても、どのように知見を共有できるようになるかを明らかにした。例えば、差分プライバシーを用いたプライバシー保護の保証は、どの金融機関にも公開できない機微データに関する予測モデル（例えば、取引モニタリングシステムに組み入れられているもの）の教育のために利用可能である。その他の手法としてセキュア・マルチ・パーティ計算がある。これは、複数の金融機関でプールされている取引データと顧客データに基づき、不正な IBAN（International Bank Account Number）に関する KPI 作成等の安全化された共同プロセスのための構成部品（ビルディングブロック）である。

46. 最後に、質問状回答においては、データプーリング及び共同分析のための新技術の開発に当たり、徹底したデータ保護影響評価の実施の必要性が強調された。一部の国では、既に明らかとなっている個人の権利に対するリスクを最小限に抑えるため、データ処理に先立ち、こうした評価を行うことが規制上の要件とされている。

## 5. AML/CFT 情報の共有及び分析において確認されている新技術

47. 本セクションでは、金融機関同士がAML/CFT目的で、データ共有及び分析を行うのを容易にする、現在開発中、又は既に利用されているさまざまな新技術について概要を説明する。このような新技術は、文献調査及び質問状回答者へのインタビューの過程で確認されたものである。

### 5.1. 民間事業者間での情報共有において確認された技術

48. 下表は、民間事業者間での共同分析及びデータプーリングを円滑化するために現在検討されているさまざまな新技術について整理したものである。データプーリングと共同分析に利用する技術として最もよく引き合いに出されたのは暗号化技術であり、大規模なデータセットの分析技術として挙げられたのは機械学習であった。しかし、データ共有・分析に取り組むに際しては、国内外のデータ保護とプライバシー要件に的確に従いつつ、セキュリティを確保して大規模なデータセットの分析を行うために、複数のタイプの技術を利用することが必要になるとの回答が多かった。それゆえ、データセキュリティとデータ保護を確実にするために、下表に記すさまざまな技術が併用されることが少なくない。

表 5.1. 民間事業者間での AML/CFT 共同分析のための技術の概要

| 技術の種別 | 概要 | AML/CFT データ共有において考えうるメリット |
|---|---|---|
| **暗号法／暗号化技術** | | |
| 準同型暗号 | 第三者の保有するデータ資産を、検索内容を特定せず、また基となるデータのセキュリティや保有を洩らすことなく、クロスマッチしたり検索したりできる。このことは、別々の当事者が、プライバシー、機密性、守秘義務、規制遵守を維持しつつ、機微なデータを共同化できることを意味している。（マイクロソフト、2016[2]） | より大きなデータセットにアクセスして、結果を改善できる。また、誤検知の減少、金融犯罪調査の効率化、企業データの質の向上及び運営効率の向上が可能なことから、インテリジェンスに基づく意思決定ができるようになる。 |
| ゼロ知識証明 | 本質的に、ゼロ知識証明とは、証明者と検証者との間に発生する暗号方法と検証方法である。証明者は検証者に対して、基となるデータ又は情報そのものを公開することなく、情報を保有していると証明することができる。 | この技術を利用すれば、A 銀行は、顧客の個人情報を共有することなく、B 銀行が当該顧客のデータを保有しているか否かをはっきりさせることができる。 |
| セキュアマルチパーティ計算（SMPC） | セキュアマルチパーティ計算によって、複数の当事者が、異なるデータソースに由来する個人情報の関数を、統合処理やデータ共有をしなくても計算できるようになる。このプロトコルが完了すると、各当事者はその関数値を知ることができるが、それ以外の情報は一切明かされない。（J. シャイブナー、2020[1]） | この技術を完全に異なるデータソースに適用して、データ主権を維持しつつ、別の当事者から、信憑性のある疑わしい取引を抽出することができる。 |
| 差分プライバシー | 暗号化プロトコルを用いて、各当事者が自身のデータの匿名性を維持しつつ、共有インプットすることで、他の当事者らと共同計算を進められる。 | 本技術ではデータの正確性とプライバシーとのトレードオフが発生するが、これは、本技術が、異常の検知や詳細パターンの検知よりも、大きな傾向の分析に最適であることを意味する。 |

| 技術の種別 | 概要 | AML/CFT データ共有において<br>考えうるメリット |
|---|---|---|
| **高度な分析** | | |
| 機械学習（教師付き学習、教師なし学習、強化学習） | AI のサブフィールド（派生）で、特定のタスクを実行するためにプログラミングするのではなく、新しいデータに接したコンピューターが学習アルゴリズムを通じて、自主的に学習することができる。 | 教師付き学習は、検査／監査の結果や履歴に基づいてコンプライアンスリスクのスコアリングモデルを構築するのに利用可能である。<br><br>現状を把握して、最適解を予測できることから、機械学習モデルにより、業務プロセスにおける決定ポイントの最適化が可能。<br><br>スコアリングモデル又は分類モードは、金融取引データ又は他の関連データから、疑わしいネットワーク又は事業者を特定するのに利用できる。 |
| 連合学習 | 連合学習は、ローカルデータを収容する複数の分散型データベースを横断的に、アルゴリズムを教育する機械学習手法である。<br><br>このアルゴリズムは、接続されていない各データベース上の新情報（傾向等）を、データ交換や移動を行わずに学習できる。（G. シフマン、2020[2]） | 例えば、トラベリング・アルゴリズムは、データを移動せずに、別々の金融機関のデータセットにアクセスして問い合わせることができる。この目的は、一つの金融機関だけに存在していた場合に学習できないような、新種の犯罪傾向及び犯罪手法をアルゴリズムに学習させることにある。動的レッド・フラッグ・インジケーター等、より動的な分析ツールの構築が可能になる。 |
| 深層学習（ディープラーニング） | 深層学習は機械学習の一分野で、複数の層からなる学習アルゴリズムを利用して、大量のデータから有意な結果を抽出する。 | 例えば、金融機関における取引モニタリングのために利用が可能である。 |
| 自然言語処理 | 自然言語処理により、人間の言語を用いて人間がコンピューターと会話できるようになり、言語が関係するその他のタスクに拡張できる。コンピューターがテキストを読み、スピーチを聴き、それを解釈し、感情を推し量り、重要なのはどの部分かを判断できるようになる。（SAS、2020[3]） | 一例として、疑わしい取引の届出における自由形式のテキストを、ネットワーク分析で利用可能な構造化データに変換するために利用できる。<br><br>テキストマイニングを用いて、疑わしい取引の届出等いかなる書面にも自動的に注釈付けができ、後日必要となった際に容易に取り出せるようになる。 |
| ロボティック・プロセス・オートメーション | 繰り返し行われる多くの作業を、大量、迅速かつ正確に実行するような相互作用を模倣するために、人間行動に基づいて「ロボット」（すなわちソフトウェア・プログラム）をプログラミングする自動化ソフトウェア技術。 | これまで人手で行ってきた繰り返し作業の自動化によって、効率化が図られる。 |
| ネットワーク分析 | ネットワーク分析とは、ネットワークデータを利用して、大規模なデータプール内の漠然とした傾向やパターンの可能性を検知することである。複雑な事業者ネットワーク及び特定されたリンケージの特性を可視化することが可能になる。 | エンドポイント・レベルでは確認不能であったパターンの引き出し。<br><br>ネットワーク分析は、既知の関心対象に基づく関係事業者のネットワーク特定に利用できる。 |

| 技術の種別 | 概要 | AML/CFT データ共有において考えうるメリット |
|---|---|---|
| **処理と転送のためのインフラ** | | |
| セキュアな実行環境（秘密計算） | 秘密計算とは、コンピューターをハードウェア・ベースのセキュアな実行環境へと切り離すことを通じて、使用しているデータを保護することを意味する。この環境は、ハードウェアのプロセッサとメモリの一部をセキュアにすることによって保護される。（マイクロソフト・アジュール、年次不詳[4]） | 例えば、当事者間で各自のデータを共有することについて合意し（取引データ等）、セキュアな実行環境下でその分析を行う。 |
| セキュアなクラウド技術 | クラウドコンピューティングは、インターネットを通じた情報技術サービスの提供であり、これによって企業と政府機関はイノベーションと連携を加速できるようになる。クラウドセキュリティには、クラウドコンピューティング環境を内外のサイバーセキュリティの脅威から保護するための手続きと技術が含まれる。（マカフィー、2020[5]） | クラウド技術の進歩により、企業においては、従前よりもはるかに大きなデータセットを大幅な低コストで収集、保存、分析できるようになった。クラウド技術では、構造化データと非構造化データのいずれについても、保管と分析を行うことができる。また、この技術を利用すれば、セキュアなクラウド環境にアクセスできる当事者が協力することも容易になる。<br><br>しかし、金融機関 2 社が同じクラウド環境にデータを保有しているか否かに関わりなく、データ共有に対する法的な障害が存在することに変わりはない。 |
| 分散型台帳技術 | ネットワークに属する関係者が維持する、取引を暗号化して記した共通の台帳である。この技術には、台帳を集中管理する組織は存在せず、極めて安全かつ透明性の高い方法で情報の保存を行うことができる。この情報は、原則として記録や時系列の書き換えができない。（OECD、年次不詳[6]） | 例えば、1 社だけがデータ処理を集中管理するのではなく、複数の当事者間でのデータ共有手段として利用できる。しかし、データ共有には法的な障害が残されている。 |
| アプリケーション・プログラミング・インターフェース（API） | API は規制対象事業者によるデータ提出を可能にするインターフェースである。データ生成プロセスが統合されることによって、自動化の一層の進展と報告に要するコスト低減が図られ、規制対象事業者と当局とのやり取りの円滑化に寄与する。（金融安定理事会（FSB）、2020[7]）<br><br>（訳者注記：原文のまま翻訳したが、API の一側面としての解釈と推察される。巻末「用語集」に汎用的な解説がある） | 大規模なデータセットの、より効率的な収集、保存、分析が可能になる。 |

49. 以下のケーススタディは、金融機関の AML/CFT 分野における共同分析を円滑にする新技術で、現在使用されているか開発途上のものの事例である（RegTech に関するこれ以外のケーススタディは附属書 B を参照）。

### BOX5.1. 連合学習

セキュアな連合学習プラットフォームの立ち上げに向けて、ハードウェア技術プロバイダーとソフトウェア・ベンダーにより構成されるチームが取組みを進めている。このプラットフォームでは、複数のデータセットにまたがって機械学習モデルを学習させ、「正常」と「異常」パターンを見分けて分析することを目指している。これらのプラットフォームにおいては、モデルは別々の場所に置かれたデータベースを横断的に移動するが、データはまったく移動しない。ここでは、参加事業者のデータセットに基づいて、プライバシー保護とセキュリティを確保しつつ、モデルは新たな犯罪の傾向や犯行の手口を学ぶことができる。モデルから得られた知見は、参加する全事業者にわたって、リスク・インジケーターを絶え間なく改良して調整するために利用される。

### BOX5.2. セキュアマルチパーティ計算

ある RegTech 企業は、暗号化された顧客確認（KYC）データ、並びに取引行動情報及びログイン活動情報を明かすことなく加工することによって、複数の金融機関が共同でリスク評価関数を計算できる技術を開発した。このリスク評価関数は、プライバシー強化技術を使って実行され、事業者は、いかなる手段及び形態においても、顧客データを実際に共有したり公開したりする必要はない。この技術では、マルチパーティ計算プロトコルにより、各事業者の保有するデータは、決して当該事業者の外部にさらされることなく処理される。参加事業者は、顧客情報のない、完全にランダムな文字列のみを交換する。重要なのは、双方当事者とも、計算のいかなる時点においても、自身のデータを、他の当事者らに公表しないことである。セキュアマルチパーティ計算は、計算を難読化して個別データ情報が分からないようにし、クリアなテキスト状態で共有したかのように結果のみが計算される。本技術は、取引が実際に行われる前に実行される。又は、AML モニタリング段階や分析段階において実行される。本技術では、暗号化した監査証跡を各金融機関に残すこともできる。外部の監査人は、すべての取引顧客から監査証跡が得られれば、決定に至る全プロセスを再構築できる。

### BOX5.3. 準同型暗号

ある RegTech 企業は、金融機関のための、テクノロジー対応のフレキシブルで適応性のあるトラストフレームワークを開発した。このフレームワークにより、顧客確認（KYC）・顧客管理（CDD）プロセスを安全に非公開で容易に行えるようになり、インテリジェンスに基づく意思決定が強化される。このイニシアチブは、データを暗号化したまま個別に処理することを可能にする準同型暗号を利用して、金融機関が第三者と、データ資産を安全に検索、共有し、協力して取り組めるようにするもので、検索内容そのものは一切明かされず、基となるデータの安全性や所有権が損なわれることもない。この分散型データモデルでは、参加者は、データ資産を移動したり統合したりしなくてもよい。データの所有者は、自身のデータ制御と、データへのアクセス管理を継続して行う。

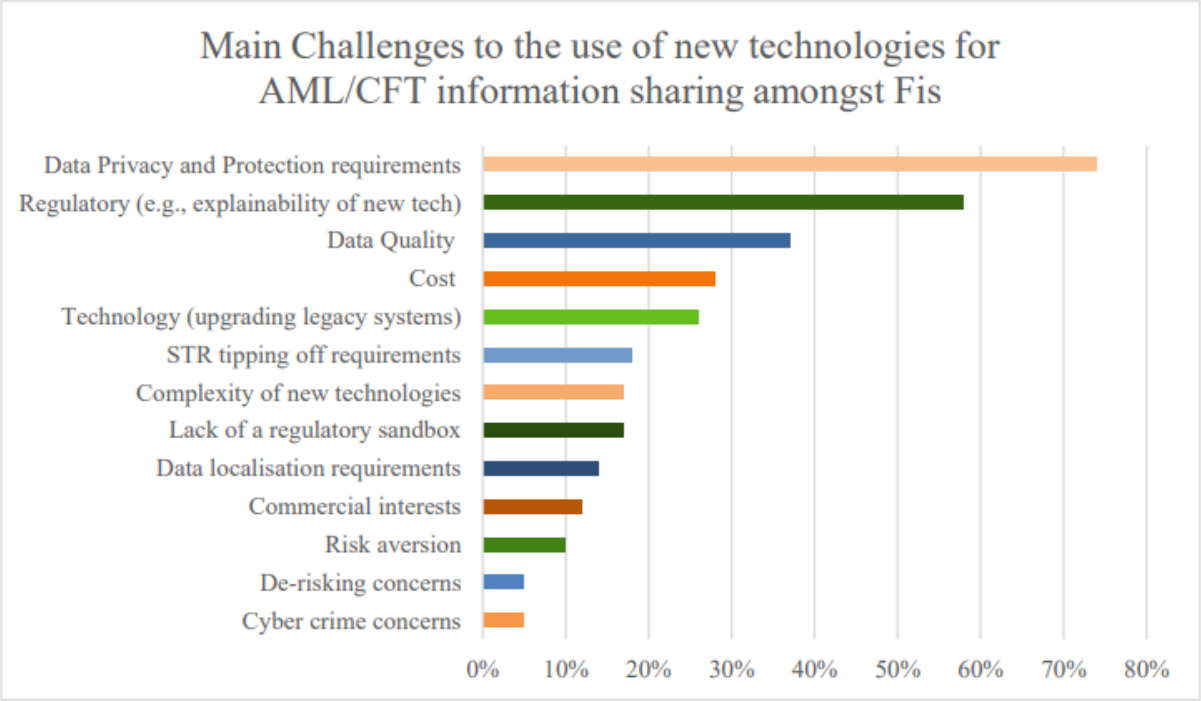
このモデルにおいて、顧客確認（KYC）情報の認証は、信頼できる複数の参加者又は法域によって、データを動かしたりプールしたりせずに行われる。暗号化された検索を通じて、一方の当事者が保有する情報と、他の当事者が保有する情報との検証を行うことができる。アナリストは、プライバシー管轄区域をまたがって、ビジネスに関係する時間枠において、安全かつプライベートに、規制データをクロスマッチして検索することができる。その間、規制要件に従って処理を行うに当たり、機微資産は継続して確実に保護される。このソリューションによる革新的な暗号化手法を採用すれば、金融機関が直面する主要課題にどのように対処できるかが明らかになった。こうした暗号化手法により、事業者は、機微情報を共有し、顧客リスクへの理解を深められるとともに、現実のマネー・ローンダリング及び金融犯罪問題に対して、より良い情報に基づいた迅速な決定を下すことができるようになる。

## 6. データ共同分析のための新技術の利用に関する課題

50. 金融機関同士のデータプーリングや共同分析、とりわけ国をまたぐものや第三者と実施するものは、多くの政策的懸念を惹起する。このような課題の一部については、FATF が 2017 年に公表した前述の「民間セクターにおける情報共有に関するガイダンス」に概説されているが、プライバシー強化技術や AI 等の高度な分析を利用して、より大規模なデータセットの処理を行おうとする場合には、追加的な検討が必要となる。

51. 質問状回答によれば、民間事業者間でのデータ共有のための新技術の開発と展開において、考慮すべき主たる政策課題として、顧客管理要件が挙げられている。それ以外の課題として多く指摘されたものとしては、下図に示すように、規制課題（新技術の説明性／解釈性、並びに規制インセンティブの欠如等）、データの質（データ標準化がなされていないこと等）等があった。

**図 6. 金融機関同士で AML/CFT 情報共有を行うための新技術利用に当たっての主な課題**




注：回答者は上記リストから最大 4 項目を選択。

52. 以下のセクションでは、質問状回答、インタビュー及び調査に基づき、データプーリング及び共同分析との関連において認識された課題と障害について深掘りする。

### 6.1. データ保護とプライバシーの確保、強化

53. マネー・ローンダリング／テロ資金供与対策（AML/CFT）とデータ保護とプライバシー（DPP）とは、ともに重要な目的に資する公共利益であり、相互に対立するものでも本質的に排他的なものでもない。[14]国内外の法的手段を通じてデータ保護の原則とルールを実行する目的は、人権と自由の保護、特にプライバシーの保護にある。プライバシーやデータ保護といった個人の基本的人権を尊重しつつ、マネー・ローンダリング、テロ資金供与や大量破壊兵器拡散資金供与等の金融犯罪を防止するために、公共利益の強化に向けた法制度の整備が不可欠である。金融情報には、財政状況、家族関係、行動や習慣、健康状態等を明らかにするような、個人に関す又は最も機微なデータが含まれるだろう。それゆえに、人権法を含む国際法の下での加盟各国の義務に従って、AML/CFT と DPP の双方に配慮し、これらのバランスをとるようにしなければならない。こうした法の下での最も重大な要求の一つは、個人データを処理するための有効な法的基盤の存在を確保することである。さらに、同じ目標を達成するための代替的手段との釣り合いという観点も尊重されねばならない。次のケーススタディは、1981 年 1 月 28 日に調印された、個人データの自動処理に関する個人の保護に関する条約（欧州評議会条約第 108 号）におけるこうした要求に焦点を当てたものである。同条約は、データ保護分野で初の、法的拘束力をもつ国際条約である。

[14] 例えば、プライバシー権は、世界人権宣言、市民的及び政治的権利に関する国際規約、並びに地域レベルでは欧州人権条約に基づく普遍的な人権である。

**BOX6.1. 個人データの自動処理に関する個人の保護に関する条約（欧州評議会条約第 108 号＋（改正後の欧州評議会条約第 108 号））**

条約 108 号＋では、以下に基づいて個人データの処理を行うことができるとされている。すなわち、(1)個人データの処理について、データ主体が、自由で、具体的な、情報を踏まえた形で、明確に同意している。(2)法の定めに従い、他の合法的な根拠（契約の履行、公共利益、公共の安全確保、管理者の正当な利益等）に基づいてデータの処理（収集を含む）を行う。前記の同意、公共利益又は正当な利益が有効な法的根拠として要求されるか否かについて、内外の AML/CFT、DPP 及び人権の各分野の関係者は、基礎をなす論理的根拠を慎重に分析し明確にすべきである。

欧州条約第 108 号＋の第 11 条に概説されている通り、共有対象となるデータの区分は、それを処理する目的とともに、明確に定義されねばならない。これは、当該データの保持が認められる期間を明らかにするとともに、私生活を尊重される権利への干渉が合理的な程度であって、正当化されうるものであるか否かを明らかにするために必要とされる。さらに、第 6 条には、データ主体に悪影響が及ばないようにするために、合法的な目的のために機微データの処理を行う場合は適切なセーフガードを追加的に講じるべき旨が記されている。適切なセーフガードとしては、当該主体による明確な同意、当該事例に適用される明確な法的規定の存在、専門的な秘密保持義務、そして特別な技術的セキュリティ方策（データ暗号化等）等がある。

54. 上述の通り、マネー・ローンダリング及びテロ資金供与活動には複数の機関や法域が関与することが多い。疑わしい取引をより的確に特定して、金融システムの悪用を減らすため、金融機関がその顧客に関する情報や分析を授受することは有益であり、それには越境授受も含まれる。新しい犯罪傾向や犯罪のタイプへの理解を深めるため、より大きなデータセットを処理することも、金融機関にとって有益であろう。同様に、金融機関は、顧客の個人データ保護のための法的義務も負っている。

55. データ保護とプライバシーに関する国内法、国際法及び各法域間でこうした法律に相違があると、金融機関が AML/CFT 義務を実行したり、民間事業者間で情報共有を進めたりする際の課題となりうる。AML/CFT 要件や DPP 義務の規制が明確でなかったり、アプローチが不適切であったりすると、こうした問題はさらに悪化する。さまざまな DPP アプローチがあって複雑なことは、民間セクターにおける情報入手、情報へのアクセス、情報処理及び共有に影響する。

56. 民間事業者間の情報共有やデータプーリングにおける重大な課題として調査の過程及び質問状回答で明らかになったのは、情報共有を進めて AML/CFT コンプライアンスの効率と実効性を向上させたい金融機関側と、顧客のプライバシー保護を主眼とする既存の法規制という、対立関係にある認識である。多くの法域で、他の金融グループの事業者とのこうした情報共有は、データ・プライバシー要件のため規制対象とされている。反対に、ある一つの法域（米国）では、別々のグループに属する金融機関の間で行われる AML/CFT 目的の情報共有を除外する規定（セーフハーバー・ルール）が存在する（概要は以下の BOX を参照）。

### BOX6.2. 米国愛国者法 第 314 条(b)

米国愛国者法第 314 条(b)(金融機関間における情報共有)は、複数の金融機関及びそのすべての関連機関が自発的に、テロ又はマネー・ローンダリング活動への関与の可能性が疑われるすべての個人、事業者、組織及び国家に関連する情報を共有できると規定している。テロ又はマネー・ローンダリングへの関与の可能性がある活動を特定して報告する目的で、その情報を伝達・受領、又は共有する金融機関・関連機関が公表を行うこと、又は公表の対象者もしくは公表により特定されるすべての者に対して、公表を行った事実通知をしないことについて、米国のいかなる法・規則の下においても、いかなる州・政府の憲法・法・規則の下においても、又は法的強制力のある契約(すべての仲裁契約を含む)の下においても、いかなる者に対しても責任を負わないものとする。(FATF、2017[8])

第 314 条(b)のセーフハーバーを利用するには、金融機関・その関連機関は、共有された情報がマネー・ローンダリング又はテロに関与する可能性のある活動に関係していると信ずるに足る合理的な根拠を有しており、かつ、第 314 条(b)及びその施行規則に則って適切な目的のために情報共有がなされていれば、十分とされる。それゆえに、金融機関・その関連機関は、マネー・ローンダリング又はテロ活動への関与が疑われる活動に関連する情報を共有することができる。そしてこれは、当該金融機関・その関連機関が、特定の違法行為によって得られ、洗浄された収益を仮に特定できなくても認められる。(金融犯罪捜査網(FinCEN)、2020[9])

57. 質問状回答では、個人の基本的 DPP の権利を尊重しつつ、民間事業者間のデータ共有を進めることに係るこれまでの懸念事項は、新技術によって概ね対処可能であると考えられていることが示された。特に、国内及び国際的にルールを整備して、いつ、いかなる目的であれば(そしていかなるタイプのデータであれば)、AML/CFT 目的における金融機関同士での(特に他の金融グループに属する金融機関との)データの共有又はプーリングが認められるかを明白にするよう望む回答が多かった。さらに、新技術や新興技術を採用する目的が、例えば顧客口座開設(オンボーディング)時に、特定の自然人・法人を識別するためにデータを利用することにあるのであれば、「プライバシー保護」的ではないと指摘された。

58. デジタル分野での協力促進のために、世界的なデータ保護基準が必要との認識はあるものの、現在のところ、その発展に向けた調整を担う組織は存在しない。それどころか、このような基準の策定は、関係各国によって国家的、超国家的に進められている。それは、法域内での DPP 法の枠組みを確立する責任が各国政府にあるからである。その結果、金融機関同士で共有することが認められるデータや情報の種類に関するガイドラインがほとんどなく(共同分析の利用に関するものすらない)、上述の新技術・新興技術及び新プロセスによって、当該国あるいは超国家的なプライバシー保護要件を引き続き遵守できるかも分からない状況になっている。

59. 国連貿易開発会議(UNCTAD)によると、194 カ国中 132 カ国が、データ及びプライバシー保護を目的とする法制度を何らかの形で定めている。(UNCTAD、2020[10])とはいうものの、セーフガードや

DPP コンプライアンスの水準は、各国間で大きなばらつきがある。EU 一般データ保護規則（GDPR）の施行は、EU 域内や欧州経済領域（EEA）での DPP ルールの統一化にとどまらず、世界中の多くの国に、プライバシー保護ルールの近代化に向けた検討を促す契機となった。

60. 下の BOX は、EU のデータ保護規則のケーススタディである。

**BOX6.3. EU のデータ保護規則**

プライバシー権とデータ保護の権利に関する規定は、欧州連合基本権憲章（第 7 条及び第 8 条）において法制化されている。

EU 一般データ保護規則（GDPR）は 2018 年 5 月 25 日付で施行され、企業における個人データの個別処理についての規則を定めている。GDPR において企業に特に求められているのは、特定かつ明確な目的（すなわち目的上の限定）を遂行するのに必要となる個人データのみを収集・処理する（すなわちデータの最小化）ことであり、こうした目的にそぐわない形で、これ以上の処理をしてはならないとしている。また特に情報収集対象者に対して、データの収集がいつ行われたか、また当該データを何の目的で処理するかについての情報を提供するよう求めている。個人情報の処理が認められる法的根拠に係る限定的リストが設けられ、情報へのアクセス権、情報を訂正及び抹消する権利、並びに自動化された処理結果だけに基づく決定に支配されない権利（プロファイリングを含む）等の一連の個人的権利を確立している。

GDPR を監督・執行するのは、EU 加盟各国のデータ保護当局（DPA）である。加盟各国の DPA と欧州データ保護監督官とで構成される EDPB が、EU 全域での GDPR の一貫した適用を確保する。

第三国又は国際機関への個人情報の移転は、それが GDPR による保証を弱体化させないよう、特に厳重な条件下に置かれる。とりわけこのようなケースでの移転は、第三国でのデータ保護水準が EU で保証されているものと本質的に同等の水準にあるという、欧州委員会の採用する「適切性についての決定」に基づいて行われる。

GDPR において、匿名化データ（データ主体の特定ができないか、できなくなっているような方法で、個人データが匿名の状態にされているもの）にはデータ保護の原則が適用されない点は重要である。こうしたデータは GDPR 要件の範疇外とされている。一方、仮名化データ（追加情報がなければ、個別データ主体の帰属がわからないようにされている個人データ）については、GDPR の範疇内の個人データとみなされる。

61. データ保護とプライバシーに関する法律は各法域間で異なるものの、共通する傾向を見出すことができる。例えば、データ保護の枠組みが適用される場合、そこには類似した重要な特徴が見出される傾向がある［すなわち、包括的な法律であって、セクター別のルール、データ保護に関する主要原則や義務、自らの個人データの管理への強制的権利（データ訂正や削除等）の個人への付与、及び強制力を有する独立の監督当局の創設等ではないこと］。さらに、欧州評議会条約第 108 号＋

（データ保護の分野で唯一、法的拘束力を有する多国間の文書）、OECD プライバシー保護ガイドライン等の国際基準に、こうした文脈における前向きな傾向が表れている。また国連においても、反テロに向けた国際協力を促進すべく、推奨される法的規定や、既存のデータ保護ルールに関するグッドプラクティスの概要策定が行われている（“UN CT Programme on Data Protection”（国連データ保護に関する反テロリズムプログラム））。

62. しかし、FATF が 2017 年に公表した民間セクターにおける情報共有に関するガイダンスに記されているように、合意や公共利益の例外に基づいて、金融機関が金融犯罪に対抗するために顧客データの処理（他者へのデータ移転を含む）を行うのは困難であるか不可能であろう。さらに、越境移転を行う際の法的条件も満足することが求められる。適切なセーフガード又はガイダンスのための条項が法律上に設定されて、可能な場合、どのような条件下において、こうした目的での顧客データの越境移転が認められるか明確に定められれば、情報共有が促進されよう。（FATF、2017[8]）

63. しかしながら、民間セクターのデータ移転を認める有効な法的枠組みが存在する場合においても、金融機関が共有するデータが不正確であったり不完全であったりする可能性がある。それゆえに、データプーリングや共同分析を行うことは、AML/CFT コンプライアンス（顧客管理の実行等）において他の金融機関を支援することになろうが、データの正確性の保証責任は、これを利用する金融機関が負うことに変わりはない。金融機関は、それゆえ、他の金融機関によって収集された内容や、実行されたチェックが最新のものであるか否か、また AML 義務を遂行するのに適しており十分であるか否かの評価を行って、共有されたデータの質を検証すべきである。

64. 一部の法域では、個人から金融機関に対して、収集、移転、保持されている情報へのアクセス要求がなされた場合、金融機関は情報管理者として、アクセスを認めるよう求められている。[15]その意図するところは、自分自身のどんなデータが入手できるのか、個人が認知できるようにして、不正確・不要な情報の訂正、又は削除を要求できるようにすることにある（すなわち、一定条件の下で、こうした情報の修正、削除を行う権利）。違法な活動が疑われる個人や、正式な調査対象となっている個人から、自分に不利な情報の削除に係る要求がなされた場合、緊張関係が生じる可能性がある。しかしながら、個人の権利を実行することにより法律上の義務の遵守に影響が及ぶ場合、又は実施中のリスク調査に支障が及ぶ場合には、何らかの（しかも十分に正当化しうる）制約を法律上に規定することができよう。

65. 匿名化された個人データの移転を許可する法域に関する課題も存在する。質問状回答では、匿名化データを共有する組織の能力に関する曖昧さの指摘もあった。というのは、匿名化[16]と仮名化[17]の要件が明白でなく、法域によってまちまちかもしれないと認識されているからである。

---

[15] 欧州評議会条約第 108 号＋第 9 条を参照。

[16] 匿名化データは、特定可能な自然人に関係しない情報、又はデータ主体がもはや特定不能となっている（そして再度特定される可能性がない）情報を記述する。（”ICO、個人データとは何か。”、2020 年 12 月アクセス〈ico.org.uk〉）。

[17] 仮名化とは、データセット中の個人を特定する情報を置換又は除去する安全化手法である。しかし、データ主体の再特定が可能（例えば、何者かが暗号鍵を保有している等）なので、この情報は依然として個人データであると考えられている。（同上）

66. 加えて、法域間移転に関するルールが民間同士（異なる金融グループ間）のデータ共有に影響しよう。多くの場合、公的機関や民間事業者は、相手の法域におけるデータ保護水準が同等であるか、データ保護を保証するための適切なセーフガードが存在しなければ、国外にデータを移転できない。しかも、データ・ローカライゼーション法においては通常、以下の 2 点が要求される。すなわち、(1)市民の個人データが国内又は法域グループ内のデータセンターに置かれていること、(2)データの取扱い及び処理を同一法域で行うこと。このこともまた、各国の法的枠組みに基づく情報移転の制約要因となる。結果的に、金融機関は、金融犯罪リスクの疑いのある特定のデータを、国外や同一の金融グループ内の相手方金融機関と共有できなくなるか、又は国内の文脈において行う場合と違って、データ共有に伴う責任から保護されないことになる。[18]

67. 最後に、データプーリングや共同分析のための新技術の広範な普及の支障になっていると質問状回答者が指摘したのは、国内外の AML/CFT 担当と DPP 担当の当局間の交流がないことである。このような調整や協力の欠如は、協力に関する FATF 勧告 2 の要求に影響し、場合によっては、AML/CFT 要求と DPP ルールとの両立を確保するための、AML/CFT 関係当局間の調整にも影響する。

### 6.2. データの質

68. データ標準とデータ形式は、組織、法域、インフラ、メッセージネットワークごとの多様性が著しい。このような相違は、データ分析の障害となり、銀行業務を遅延させ、コンプライアンス費用を増大させる。不正確なデータや古いデータ等の質の悪いデータによって、誤解を招く分析結果につながり、データプーリングや共同分析のメリットが台無しになりかねない。高度な分析のための自動化ツールは、特に、正確に標準化されたインプットに依存する。

69. 回答者は、集中型又は分散型のデータセットの高度な分析を展開する際の主要な課題はデータの質だとしている。回答者が特に注目したのは、データの質が劣る金融機関が存在することと、金融機関同士のデータ標準が一様でなく、互換性もないことであった。データの質は、バイアスのない結論を引き出すために必要とされるデータセット（正しくて一貫性のある形式のもの）を得るに当たっての変わらぬ大きな障害となっている。結論にバイアスがかかると、最悪の場合、金融排除を招く恐れがある。このような障害は、データが暗号レイヤーにオーバーレイされると一層悪化する。というのは、データの誤りの特定がさらに困難になり、アウトプットの誤りにつながるからである。

### 6.3. 明確でない規制

70. 相当数の回答者が、新技術の利用に対する規制要件や方向性が明確でないことが、民間セクターにおけるデータプーリングや共同分析の利用上の課題となっていると指摘している。一部の法域では、金融機関同士のデータ共有や共同分析が可能となるよう、ルールの明確化やルールの適用に

---

[18] 詳細は（IIF、2019[17]）参照。

向けた取組みが進められているほか、金融情報共有パートナーシップを設けている法域も存在する。回答者のなかには、方向性が不明確なことや、規制当局の確実性の欠如が、共同分析の促進効果が見込まれる新技術に優先的に多大の投資をして実行しようとするインセンティブの低下を招いているとの指摘もあった。

71. ある回答者は、現在の法的枠組みはプライバシー保護のために新技術を利用する可能性を念頭に置いていないので、こうした技術を採用する際の明確な境界が定められていないとも指摘している。

72. 最後に、国内の既存の規制が、民間事業者間のデータ共有（同一の金融グループ内での情報共有以外）を完全に妨げているとの指摘も多かった。

### 6.4. 説明可能性と解釈可能性

73. 欧州銀行監督機構（EBA）は 2020 年 1 月、欧州の銀行システムにおけるビッグデータと高度な分析の利用に関する報告書を公表した。同報告書において、欧州の金融機関は簡単な機械学習モデルを用いた高度な分析利用の初期段階にあるものとみられた。そして、説明可能性と解釈可能性を優先事項とした。より複雑な分析モデルの利用に関連する課題の一つは、監督機関への説明可能性と解釈可能性、そしてバイアスと意図せざる結果への懸念である。EBA によると、あるモデルが説明可能とされるのは、その内部の動作が人間にとって直感的に理解可能（解釈が可能）である場合、又は、アウトプットを導き出した主たる要因が説明可能（根拠が正当）な場合である。（欧州銀行監督機構（EBA）、2020[11]）このように理解することができない技術は、監督機関から「ブラックボックス」と認識される可能性がある。そうなると、監督機関は、適切な検査やリスク評価を行えなくなり、こうした技術の利用に関連して発見されたリスク管理やリスク削減を適切に行えなくなることから、新技術の展開に影響が及ぶ。とりわけこれが該当するのは、高水準な自動化に基づく意思決定がなされ、かつ、その意思決定が顧客に直接的な影響を及ぼす場合である。こうした課題に対処するため、規制当局は官民両セクターの技術者や他の関係ステークホルダーと協力して、評価を行うとともに、AML/CFT への適用という文脈の中で、高度な分析について説明し、文書化し、管理していくための適切なプラクティスを広めることができる。[19]この作業には、リスクベース・アプローチに沿った形で説明可能性の要求を採用できるか、どのように採用できるかが含まれる。例えばそれは、このモデルが、顧客の事業の継続を左右し、顧客に被害を及ぼす可能性も増大することを受けて、説明可能性の要件を一層厳格化することである。

74. ある回答者は、金融機関が AML/CFT 分野におけるデータ共有・分析のための新技術の実行を躊躇している旨を指摘している。それは、完全に理解可能な暗号化や機械学習モデルを、規制当局

---

[19] 米連邦銀行局の、金融機関における機械学習を含む AI の利用に関する情報及び意見募集 www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-informationand-comment-on-financial-institutions-use-of-artificial-intelligence.を参照。また、米連邦銀行局による情報募集を受けて、FinReglab 及びスタンフォード大学が行った同様のイニシアチブ（融資引受のための機械学習モデルを説明、文書化及び管理するための新しいプラクティスを評価することを目指すもの） https://finreglab.org/ai-machinelearning/explainability-and-fairness-of-machine-learning-in-credit-underwriting/も参照。

側が期待しているからである。当該技術が第三者ベンダーによって開発され、彼らが基本技術の技術仕様に対する所有権を持っている場合や、金融機関側で、高度な暗号技術や分析を解する的確な技術リテラシーのある人材を欠いている場合には、それは特に困難なことである。回答者の 1 人は、規制当局の視点からすれば、アルゴリズム・モデルは、同一のインプットデータに対して、いつでも同じ結果を再現できるような設計になっているべきとみられている旨を記している。機械学習においては、常にこれが可能なわけではない。

75. 回答者から言及のあった重要な事項は、人手によって、高度な分析（AI や機械学習等）が導き出した結果のレビューを行い、結果の正確性を担保するとともに、アルゴリズム・モデルを継続的にリファインしていく必要性である。単純なモデルで遂行可能な基礎的ルーティンワークから解放される人間が、より複雑な分析結果のレビューを行うというアプローチは、回答者からグッドプラクティスであるとみなされている。しかし、金融機関において、こうした技術の機能や目的をよく理解しないまま、高度な分析が行われ、アウトプットの検証がなされず信頼できない結果を招いている事例もあるとの回答もあった。同様に、AML/CFT 監督機関側も、金融機関においてモデルがどのように設計され実証されているかを試すために、高度な分析モデルを理解するか、さもなければ理解できるチームにアクセスすべきだろう。

76. 最後に、規制対象事業者が、監督機関だけでなく自分自身に対しても、配備されつつある新技術によって以前よりも良好な結果が出ている事実を裏付けできることが重要であり、とりわけ、AML/CFT の実効性向上に新技術が貢献しているか分かりにくい分野においては特に重要だとの指摘があった。

### 6.5. 疑わしい取引の届出（STR）の機密性、守秘義務保持と顧客への情報漏洩

77. 疑わしい取引の届出（STR）の機密性、守秘義務保持に係るルールは、STR の共有（又は、STR が提出されたという事実もしくは当該 STR の基となる情報の共有）に制限を課する可能性がある。STR の機密性、守秘義務保持は、この報告制度を有効に機能させるために極めて重要である。STR の対象者や第三者の情報が漏れないようにするために、STR の機密性、守秘義務保持は不可欠である。秘密が漏れた場合、機密情報収集や調査に逆効果になり、被疑者が資産を処分したり、資産とともに姿をくらます余地を与えたりすることになるからである。機密性、守秘義務保持によって、STR 対象者の名誉も保護され、STR の報告を行う者の安全とセキュリティも確保される。機密性、守秘義務保持が破られれば、STR 制度そのものの土台が揺らぐ恐れがある。STR を不正に漏洩した金融機関に対して、刑事責任を課している法域が多いだろう。このような懸念は、必然的に、STR の共有を制約することになる。（FATF、2017[8]）

78. 情報共有が越境してなされる場合、STR の機密性、守秘義務保持は一層複雑になる。国によって法律が異なるからである。例えば、司法手続において、入手できる記録の発見を容易にして提示することに関連する国の規定がこれに含まれる。国内の STR については、裁判上の請求通知及び召喚令状に関する規制当局の通知を法令によって求め、司法手続において STR の機密性、守秘義務が

確保されるよう、規制当局が介入できるようにしている国もあるものの、このような法令によっても、国外の FIU に提出された国外の STR を保護することにはならないだろう。

79. STR の機密性、守秘義務保持は民間事業者間の情報共有に制約を課すことになろうが、顧客への情報漏洩防止のためには重要である。個人データの匿名性や暗号化を確実にするために、法的・技術的な仕組みで代替を図ることにより、AML/CFT の実効性を犠牲にすることなくセーフガードを整備することができよう。

### 6.6. 市場の構造と競争

80. データの収集と分析の広範な普及は、特に新しい現象ではない。しかし、現在の技術革新によって、保存できる情報量は顕著に増加し、瞬時に分析できるようになった。情報量が多ければ多いほど、より正確な分析結果が得られる可能性が高まる。現在のところ、高度なデータ分析の効率的利用に堪えるような、十分な規模のデータセットを有しているのは、既存の大規模金融機関に限られる。それゆえに、金融機関相互間でのデータ処理に対する意識を高めて、中小金融機関も新技術のメリットを得られるようにしていく必要がある。それによって、こうした新技術の利用がもたらすコスト効果を共有できるようになる。

81. 複数の金融機関において多数の顧客情報を分析することは、回答者の多くが指摘するように、競争上の懸念を惹起する懸念がある。その結果、少数の「信頼できる」金融機関同士での選択的なデータ共有が行われることになり、共有の枠組みに不均衡が生じる。そして、情報共有メカニズムを有する金融機関から、そうでない金融機関に、マネー・ローンダリングやテロ資金供与リスクが転移される。前者から排除された金融犯罪者は、検知される可能性を低減するため、後者に集まってくるだろう。このようにして、情報共有の仕組みのない金融機関や金融セクターは、ますます ML/TF リスクを抱え込むことになり、さらなるリスク軽減措置の検討を迫られることになろう。

82. 金融機関は、市場における競争を阻害する可能性のある、商業的に機微な情報の共有にも消極的であろう。金融機関の IT 能力が一様でないことも、効果的な情報共有の阻害要因となろう。別々で不適切な IT システムと不統一なデータフォーマットのために、金融機関の横断的なプーリングや共同分析を行うための互換性が損なわれるからである。同様に、旧来の IT インフラや IT システムに依存する金融機関も不利な状況に立たされ、データ共有イニシアチブから取り残されることになるだろう。

83. 大規模なデータセットに瞬時にアクセスできることが金融サービス業務の競争力をますます左右するようになっていることから、限られた金融機関同士でデータのアクセスや交換が行われることにより、こうした金融機関が競争上、アンフェアに有利な立場を獲得することがあってはならない。それゆえに、AML/CFT 分野でのデータ共有の取決めの評価においても、公平な競争条件の維持と潜在的競争相手による排他的行為を回避するという点において、競争法上の懸念が存在する。したがって、データへのアクセスが認可される際には、公平で、合理的、かつ、差別的でない条件で認可されね

ばならず、癒着を可能にすることがあってはならない。さらに、データ交換が認められるのは、それが絶対に必要な場合のみに限定しなければならない。

### 6.7. 技術的コストと制約

84. 多くの回答者が、プライバシー強化技術や高度な分析の立ち上げに膨大なコストを要することが、こうした技術の拡張性に影響を与えていると指摘している。大規模金融機関には、このような技術に投資したり、第三者の技術にアクセスするライセンスを購入したりするリソースがあるかもしれないが、中小金融機関の多くは、依然として、既存の旧技術を更新するだけで、立ち遅れている。その結果、こうした新技術の立ち上げコストを負担できる金融機関から得られたデータしかデータプールに取り込まれず、データプールが小規模になってしまう可能性がある。

85. 機械学習等の高度な分析の実行や維持に要する費用も、また高額にのぼるとする回答もあった。新しい分析システムと旧システムとの統合が必要な場合は、追加的な更新コストが発生し、状況はますます悪化する。新しい高度な分析を試行しつつ、並行的に既存システムも運用するのは、多大な費用を要することから、進行の妨げとなると指摘されている。さらに、複雑なモデルを開発し、長期的にはこれをリファインしていくために、新技術について十分な専門知識を有する専門技術者を維持しなければならず、高度な分析の利用に当たっては、こうした関連コストが追加的に発生する。

86. 大量のデータのプーリングと分析における技術的課題として追加的に発生するのは、アルゴリズム・モデルを運用するために、十分な計算能力が必要とされることである。データセットのサイズは、計算するためのコストに大きな影響を及ぼすことがある。

87. AML/CFT データのプーリング又は共有には、例えば取引情報や顧客情報等、大量のデータセットの移転を伴うことがある。このように大規模なデータセットは、「重くて」動かすのが容易でない（以下データグラビティという）。それゆえ、データプーリングに向けた取組みを進める際に、データグラビティを考慮することは不可欠である。同時に、集中化された場合、データグラビティが増大する可能性があることも考慮しなければならない。

88. 最後に、AML/CFT 分野において、機械学習等の高度な分析を配備する際のさらなる課題として、データの認定（個々の取引が真に犯罪行為を示唆するか否かを確定させること）の必要性が挙げられる。マネー・ローンダリングやテロ資金供与の分野においては、調査が結論に至るまで数年を要することがあるので、モデルの検証は特に困難である。多くの場合、金融機関は、FIU に提出した疑わしい取引の届出の最終結論を知らされることはなく、報告した活動がマネー・ローンダリングやテロ資金供与活動と認定されたか否かを知ることもできない。

### 6.8. 防御的報告とデリスキング

89. AML/CFT 目的での共同分析の利用事例として最も引き合いに出されるのは、複数の金融機関を股にかける犯罪行為の特定である。プライバシー強化技術を利用して、金融機関は例えば、データ・ロ

ーカライゼーションや STR の機密性、守秘義務保持義務を克服して、自らの顧客に対して他の金融機関から STR が提出されていないかに関する知見を、STR の基となる機微データには触れることなく得ることができる。しかし、これは防衛的な STR 提出行動を増幅させる恐れがある。疑わしい取引の情報を共有するシステムに過度に依存すると、金融機関は、第三者の情報だけに基づいて顧客を疑うような状況になりかねない。こうした情報は正確性を欠くかもしれず、また、疑わしいとする根拠が最終的に FIU によって却下されるかもしれないからである。このような状況になれば、合法的な顧客が金融システムにアクセスするのを阻むという、反倫理的で意図せざる影響が生じ、顧客に対して、取引の性質や目的を明らかにするための追加説明を要求することになって、銀行サービスの実行の遅延を招くことになる。

90. 加えて、単に疑いがあるというだけでは、かかる疑いの情報を受領した他の金融機関が組織的に STR を提出する必要は生じない。というよりも、これは、金融機関によるリスク分析のための重要な要素であり、顧客管理手段の高度化につながるだろう。共同分析やデータプーリングが広範に導入されれば、疑わしい取引として特定されるケースが増加し（とりわけ、防衛的報告が行われている場合にこれが該当する）、高度な顧客管理手法の採用が大幅に増える可能性がある。これらは、コンプライアンス・コストの増大をもたらそう。こうしたことから、この技術を利用する意欲が阻害され、デリスキング行動につながるだろう。

### 6.9. セキュリティ

91. データのプーリングや処理のための新技術の導入に伴い、サイバー犯罪者にセキュリティ上の脆弱性を突かれて悪用されるという、脆弱性の面での重大な懸念も新たに生じている。例えば、集中型データプール構築技術の利用に伴って、サイバーセキュリティ上、重大な脆弱性が生じるとともに、国家的なセキュリティ上の懸念をもたらしている。それはまた、データリポジトリの安全監視責任を最終的にだれが負うのか、そして、不具合やサイバーアタックについての責任を負うのはだれかということに関する政策的な配慮の重要性を提起している。プールするデータ量が大きくなれば、単一の事業者から、破滅的なほどに大量のデータが流出する可能性が高くなる。したがって、データのプーリングと共有の可能性が増大するにつれて、組織内部の脅威からの防御がより重要になってくる。

92. 仮名化技術を利用する共同分析の進歩により、データ保護がいくぶん進展した。ただし、識別情報が別途に保存され、かつ、個人情報が、特定された（又は特定可能な）自然人に絶対に帰属しないようにするために、技術的及び組織的な手段が講じられていることが条件である。仮名化技術が進歩したとはいえ、データ保護法制は現在も適合し、再特定されるリスクにも考慮が必要である。それは、データの性質、データ利用の背景、既存の再特定技術、関連コストの点において、必要となる時間、取組み、リソースの評価を要するからである。仮名化技術を利用する共同分析が関わっているイニシアチブにおいては、データ保護・プライバシー当局による厳格な監督も必要とされるだろう。

### 6.10. 人工知能における分析バイアスの回避

93. プールされた情報に対するデータ分析（すなわち AI）の利用に関して、考慮すべき極めて重要な事項は、高度な分析が人間のバイアスを除去するということ、そしてそれゆえ差別（宗教、人種、性別、年齢、性的指向、民族等）を回避できるということである。システムへの特定データの導入（又は排除）を通じて、また、アルゴリズム・モデルのプログラミング過程において、システムにバイアスが持ち込まれることがある。[20]こうした分析手段の開発と訓練に当たって、バイアスのないデータを用いること、そして、人間の偏見や差別を増幅しないアルゴリズムを開発することが不可欠である。

### 6.11. 人権

94. 民間セクターの事業者は、商業的利益のために、個人のプロファイリングを後押しするかもしれない。これは究極的に、人種、性別、政治・宗教的信条等に基づく差別を招くことになる可能性がある。それゆえに、監督者と DPP 当局は、データプーリングと共同分析において実行されるいかなるツールに対しても十分に厳格な監視・監督を行い、透明性が完全に確保されるようにする必要がある。仮名化技術を利用するツールも例外ではない。なぜなら、個人データやそのデータベースに登録された個人のアイデンティティを推定するために、再追跡（特定）される恐れがあるからである。

## 7. データプーリングと高度な分析の普及を可能にする環境

95. 質問状回答によれば、データプーリングと共同分析のための新技術の利用の普及を促進するとともに、上述の課題の一部に対処するために最も有用な解決策は、このような新技術の利用を巡る規制の確実性を高めることである。次のセクションでは、民間事業者間での情報共有や分析における新技術の利用拡大に寄与する解決策として、今回実施した調査や民間セクターのステークホルダーによって認識されたさまざまな方策について要約する。こうした解決策は、FATF と民間セクター及び DPP 当局との対話の出発点となり、将来的には FATF における取組みの出発点となるものである。ただし、データプーリングと共同分析の幅広い利用を可能にする環境形成に役立つこのような方策は、FATF が現時点で承認したものではない。

### 7.1. 規制の確実性

96. 質問状回答において、民間セクターによるデータ共有又はプーリング（AML/CFT データを含む）に関わるあらゆる領域を包含するデータフレームワークの構築が急務になっていると指摘されている。また、そのためには、AML/CFT 当局（規制当局を含む）と DPP 当局との連携強化が必要であるとも指摘されている。それができれば、現状で認識されている不確実性を理由として業界がリスク回避を行うのを抑制できるような、適切な環境の整備に資するであろう。回答者の大部分は、金融機関同士での共有が認められるデータの種類や、どのような技術（準同型暗号等）やプロセスであれば国又は国を超えた立場において、プライバシー保護規制に加え金融セクターに固有の規制に適合できるか

[20] AI 倫理についての詳細は、附属書 B の（FSB、2017[15]）を参照。

について、国の金融規制当局が明確な方針を示すことを求めている。明確な方針が提示されれば、技術、教育、人材、そしてデータ共有ソリューションの本番環境に、安心して投資できるようになるだろう。同様に、新技術の強力な利用事例（すなわちベストプラクティス）の統合や公表を行い、民間事業者間のデータ共有に関連するプライバシー保護の懸念に、特定の新技術を用いてどのように対処できるかについて詳述することも求められている。

97. 国が法律上に、セーフハーバー条項を設けるよう求める意見もある。これは金融機関同士が、必要性原則及び比例原則に基づいて、明確な AML/CFT 目的で自発的にデータ共有を行うのを認めるものである。

98. STR の顧客への情報漏洩要件に関しては、STR の規制要件そのものを改正して、ある特定の人物に関する STR が提出されているか否かについて、また当該 STR の基となるデータについて、金融機関がもっと自由に情報共有できるようにすべきとの意見もあった。

### 7.2. 環境の整備

99. 回答者の多くが、AML/CFT 監督機関がもっとパイロットプログラム、規制サンドボックス及びイノベーション・ハブを開始して、金融機関が実行フェーズ入りするに当たって、懲罰的であったり厳しすぎたりする規制を強制されることなく、データ共有と分析のための新技術をテストできる環境を整えるよう求めている。こうしたイニシアチブによって、たとえパイロットプログラムが最終的にうまくいかなかったとしても、監督上の批判にさらされなくて済むので、この分野におけるイノベーションが促進されることになろう。かかるイニシアチブの成否は、国の DPP 当局による関与と参加の程度にも左右される。このような関与がなされるならば、モデル管理、モデリング手法等の課題への対応のため、また、データ分析において ML/TF リスク分野を絞り込む方法やデータ共有を円滑化する方法等の課題に対応するため、連携や共通学習を行うことが容易になり、明確さの向上にも資するだろう。それと同時に、DPP 要件を尊重することもできよう。

100. FATF は、「ポジティブかつ責任あるイノベーションの追求」のための 2017 年サンノゼ原則をさらに進めるものとして、” Suggested Actions to Support the Use of Technology in AML/CFT”「AML/CFT 分野における技術利用を支援する行動に係る提案」（附属書 C 参照）も明らかにしている。これらの提案は、AML/CFT 分野における新技術が、脅威と機会の両方を反映する形で開発され実行されねばならないことに留意している。そして、その利用に当たっては、データ保護とプライバシー、そしてサイバーセキュリティに係る国際基準に確実に適合させる必要があるとしている。

### 7.3. データの標準化とガバナンス

101. データの質の向上を図るために、一部の回答者は、データ収集に利用する調査様式の標準化とともに、顧客と金融機関との情報共有を可能にするオープン API の利用促進を求めている。所管当局は、金融機関にデータ品質要件を知らせるためのフィードバック機構として、そのコンプライアンス権

限を利用し、容認できる水準までデータ品質を向上させるために適切な手立てを講じるよう強制することができる。

102. データガバナンスとの関連において、回答者は、金融機関がデータガバナンス・ポリシー及びデータガバナンスの枠組みや管理の仕組みを導入して、以下の各項を確実にすることが必要であると強調している。

a. データの質の確保。これには、データの完全性、最新性と更新状況、構造化されていて機械可読な形式になっているか否か、並びにデータソースがデータの解釈と信頼性に影響をおよぼすことはないか、等の事項が含まれる。

b. データ源泉（データ監査証跡の記録も含む）の追跡ができること。

103. 本人確認にデジタル ID を利用するのは、データ品質問題への対処法として有望な方策とみなされている。というのは、デジタル ID が、第三者に依存して本人確認する、標準的なツールになりそうで、データ共有の促進に役立ちそうだからである。同様に、取引主体識別子（LEI）も、法人顧客の管理におけるドキュメントソースとして利用できる可能性がある。LEI を含めることによって、法人名の照合に依存するのではなく、各々の法人に対して固有の識別子が紐付けされるようになる。

104. 回答者に対するインタビュー結果では、共通報告基準（CRS）がモデルとして挙げられていた。CRS において、所管当局は、所管する金融機関から特定の情報を収集して、脱税に対抗するため、収集された情報を他の所管当局と毎年自動交換することを求められる。（OECD、年次不詳[12]）回答者は、このモデルによって、AML/CFT を目的とする情報共有におけるデータ品質に関する検討に情報を提供できると考えている。それは、特定データの標準化要件（すなわち、収集・交換を行うべき情報の特定）がこのモデルに含まれるからである。

### 7.4. 人工知能におけるバイアスの防止

105. 最後に、人間の偏見と AI の不公平さの防止に関連して、回答者は、データソースの正当性と信頼性を定期的に見直すこと、大規模なモデルの検証を行うこと、そして、継続的にモデルを監視することが重要であると強調している。例えば、特定のグループに属する人々を過大又は過少に反映している可能性があるデータセットに対しては、正確さと公平さを強化するために、追加的な教育データが必要となる。

106. 2019 年 5 月に加盟国により採択された AI に係る原則において、OECD は、AI システムの設計に当たっては、法の支配、人権、民主主義的価値観及び多様性を尊重すべきであり、かつ、適切なセーフガード策（必要な際には人的介入を可能にすること等）を講じて、公平で公正な社会を実現すべきであると述べた。AI システムは、そのライフサイクルを通じて一貫して堅固、セキュアかつ安全な状態で機能しなければならず、潜在的なリスクは継続的に評価され、管理されるべきである。それゆえに、規制的背景において予測モデルを利用するに際しては、まず初めに、これを利用するための倫理が確実に理解されていなければならない。なぜなら、AI システムを開発、配備、運用する組織や個

人は、システムを適切に機能させる責任を負うことになるからである。（OECD、2019[13]）

## 8. 結語

107. ここまで、民間事業者間での AML/CFT データ共有について検討してきたが、これは FATF にとって目新しいものではない。しかし、既存技術や新技術の進歩によって、これまでとは違う方法でデータ共有と分析ができるようになり、疑わしい取引の可能性を検知し、その他の AML/CFT 義務に適合していくことがもっと効率化されて効果的になるだろう。新技術により、個人データの保護の強化に資するソリューションが生み出されるだろう。その目指すところは、情報の交換や処理のすべてが、国内外のデータ保護・プライバシーに関する法制度を尊重して行われるようにすることにある。しかし、検討されている技術開発が法域のデータ保護要件に適合するかどうかは、基本的権利の保護の妨げとならないよう、実行する前に、十分に評価する必要がある。現時点においては、こうしたイニシアチブを法的に認めていない法域があるかもしれない。

108. このストックテイク報告書においては、金融機関同士のデータプーリングと共同分析を円滑化できる既存の技術や新技術を明らかにするとともに、回答者から指摘された政策的配慮、法的課題、可能な解決策を検討してきた。本報告書では、データプーリングと共同分析の取組みには、多くの重要な政策的配慮が求められることが認識された。例えば、データプーリングと共同分析の取組みにおいては、その実行に先立って、デリスキング及び合法的な顧客が金融サービスを利用できなくなるというリスクを等しく検討し、軽減することが重要である。FATF は、このストックテイク報告書の成果を踏まえ、AML/CFT 監督機関、技術開発者、金融機関、DPP 当局及び他の関係専門家による対話を継続実施し、国内外の DPP の枠組みに適合する形で新技術が十分に活用され、AML/CFT の実効性向上が図られていくように努めていく。

# 附属書 A. 用語集

- **アドバンスト・アナリティクス**：アドバンスト・アナリティクスとは、高度な技術やデジタルツールを用いて、データ又はコンテクストの調査を自律的又は半自律的に行うことを意味する。一般的に、その範囲は従前のビジネスインテリジェンスを超えて、深い洞察を見出したり、予測を行ったり、提言を行ったりする。アドバンスト・アナリティクス技術には、データ／テキストマイニング、機械学習、パターンマッチング、フォアキャスティング、可視化、セマンティック分析、センチメント分析、ネットワーク分析及びクラスター分析、多変量解析、グラフ分析、シミュレーション、複雑事象処理、ニューラルネットワーク等が含まれる。多くの場合、アドバンスト・アナリティクスはビッグデータの利用に依存する。
- **アプリケーション**：ユーザーが特定の作業を行えるように設計されたコンピューターソフトである。
- **アプリケーション・プログラミング・インターフェース（API）**：API は、アプリケーションソフトの構築と統合を行うための一連の定義とプロトコルである。API によって、デジタル機器やサービスと、別の機器やサービスとのやり取りが容易になる。
- **アルゴリズム**：コンピューターアルゴリズムは、特定のタスクを処理するための指示を手順ごとに示したものである。
- **人工知能（AI）**：AI システムは、人間が定義した一連の所与の目標のために、リアル環境又はバーチャル環境に影響するような予測、提言、決定を行える（作動時の自律度はさまざまある）マシンベースのシステムである。（OECD、2020[14]）AI の目標は、いくつかの側面の分析をコンピューターにより自動化することにあり、人間が行う仕事を減らして人手をもっと繊細な業務に充てたり、人間では不可能な洞察を得たりできる潜在性がある。AI には、数多くの応用が利くいくつかのコンポーネント技術がある。何が「思考」や「知能」を構成するか、また「完全自律」が意味するところが何であるかについて明確な定義はなく、加えて、いろいろな種類の AI が存在する。しかし、概して言えば、程度の違いこそあれ、AI システムというのは、意図していることと知性や適応力を結合させる「スマートマシン」を構築するものである。現時点では、最も進んでいて馴染みのある AI の形態は機械学習である。
- **ビッグデータ**：金融安定理事会（FSB）は、ビッグデータを「デジタル機器や情報システムの利用が増えることによって生み出される巨大なデータ群」と定義している。こうしたデータとしては、金融取引データ、ソーシャルメディアデータ、マシンデータ（例えば IoT、コンピューターや携帯電話のデータ）等が含まれる。（FSB、2017[15]）
- **ブラックボックス**：ブラックボックスとは、AI、機械学習をはじめ、漠然としていて直感で理解できない技術であって、意思決定や予測、結果に関する的確な情報を知り得ない技術をいう。すなわち、ブラックボックス技術には説明性が欠如している。
- **ベンチマーキング**：ベンチマーキングとは、ある技術をベースとするプロセス、製品、サービスについて、実際及び相対的な能力水準を決定し、当該機能、タスク、目標において達成されたベストプラク

ティスを指標としてこれを検証することで、改善すべき点を見出す手法である。対象とするのは、個々の事業者又は組織内、業界全体、又は異業種のいずれもあり、定められたベンチマーク基準を指標としたハードパフォーマンスデータが使われる。新技術と旧システムとの間、又はある新技術と他の新技術の間のパフォーマンス計測（比較）にベンチマーキングを利用できる可能性もある。

- **共同分析**：共同分析では、他のデータアセットと合わせて分析するために、データはセントラルロケーションに移されない。その代わりに、分析ツールがデータの側に寄ってくるのであって、その逆ではない。その結果、データの安全を確保し、だれが何の目的でどんなデータにアクセスしたかを管理することが容易になる。
- **サイバーセキュリティ**：サイバーセキュリティは、データセキュリティよりも広範な用語で、包括的なデータ保護プロセスやそのデータの移動、保存、認証のためのシステムを意味する。
- **データプール（データプーリング）**：データプーリングは、別々のソースから得られたデジタルデータを結合し、分析（複数のパーティによる分析を含む）を行うためのより完全かつ有用なデータセットを生成するプロセスを意味する。このようなプールは集中化された方式で組織化される。
- **データセキュリティ**：データセキュリティとは、データのライフサイクルを通して、承認されていないアクセスや破損からデータを保護する手段のことをいう。データセキュリティの手法としては、データ暗号化、ハッシュ化、トークン化、キー管理等があり、あらゆるアプリケーションやプラットフォームにわたってデータを保護する。データセキュリティはサイバーセキュリティよりも狭義の概念である。
- **データ標準化**：データ標準化は、データを統一的なフォーマットに変換し、ユーザーがこれを加工・分析できるようにする手法である。データ標準化は、ビッグデータ加工や高度な分析、その他の先進的デジタルツールやメソドロジーの開発及び適用に不可欠である。例えば、金融データは、事業者内あるいは事業者全体で異なっている可能性がある。こうした場合に、データ標準化によってデータを共通様式に変換し、大規模で洗練された分析ができるようになる。
- **デジタルアイデンティティ（ID）システム／ソリューション**：デジタルアイデンティティ（ID）システム／ソリューションは、本人確認システム又は本人確認プロダクト及びそのサービスであり、個人（自然人又は法人）のアイデンティティの確認及び検証を実行するプロセスである。そのプロセスは、立証されたアイデンティティをデジタル認証に結び付け、デジタル認証や場合によっては他の認証要素も利用して、自分のアイデンティティを主張している人物が、確認済の身元情報（すなわちこの人物が主張しているアイデンティティ）と一致しているか確認する。
- **分散型台帳技術（DLT、ブロックチェーンとして知られている）**：DLT は、複数の（普通は複数事業者や複数地域にまたがる）コンピューター上に分散された不変の台帳（デジタルレコード）に、同時にアクセスし、検証し、アップデートすることを可能とする技術的プロトコルの一種である。つまり、DLT は分散型デジタルデータベースを構築するものである。
- **ディープラーニング（DL）**：DL は機械学習の発展形で、多層（深層）構造を有する人工のニューラル

ネットワーク（人間の脳をモデルにしたアルゴリズム）が、極めて自律的な方法で大量のデータを学習する。

- **デジタライゼーション**：デジタライゼーションとは、デジタル技術とデジタル化されたデータを利用して、ビジネスモデルを変革したり、仕事のやり方にインパクトをもたらしたり、顧客と企業との交流方法を変換したり、新たな収益や価値創造の機会を獲得したりすることである。
- **デジタイゼーション**：デジタイゼーションとは、データ、情報、テキスト、画像、音声等、アナログ形式で表現されているものをデジタル形式（バイナリーコード）に変換して、コンピューターで処理できるようにすることである。
- **動的データ**：動的データとは、連続したリアルタイムのデータポイントのデジタルストリームであって、常に変化していることが知られているものである。その結果、データセットは時間の経過につれて絶え間なく変化し、ほとんど時間経過の影響を受けない静的データと対照をなす。
- **説明可能性**：新技術という文脈のなかでは、説明可能性は、技術ベースのプロセス、ソリューション又はシステムが説明、理解、釈明可能であることをいう。説明可能性により、ソリューションがどのように作用して結果を出すに至るのかについて、的確に理解できるようになる。説明可能性は、信頼性や責任ある利用のための基本条件である。説明可能な AI 技術は、結果を出すために用いられたデータ、変数、決定ポイントの透明化につながる。
- **フィンテック**：フィンテックというのは、大まかにいえば、金融セクターにおいて、広範かつ多岐にわたる目的のために、デジタル新技術や新興技術を利用することである。当初、「フィンテック」は主として、顧客向けの新たな金融商品やサービス（例えば、モバイル決済ソリューション、オンライン上でのマーケットプレイス・レンディング、アルゴリズム貯蓄・投資ツール、仮想通貨による支払い、資金調達（クラウドファンディング）、預金受入（リモートチェックキャプチャ、モバイルバンキング）等）を提供するために、技術ベースのイノベーションを適用することを意味していた。今では、フィンテックには、新技術や新興技術を利用して、自動化されたミドルオフィスやバックオフィスエンタープライズ機能（アルゴリズム、ビッグデータ、AI、機械学習等）を提供したり、決済、支払等の卸仲介（例えば証券、デリバティブ、卸金融、支払いや規制コンプライアンス活動等）の分析結果にリンクしたりすることも含まれるようになった（下記 RegTech の定義の項参照）。フィンテックには、これら以外にも適用の余地がある。
- **ファジー論理**：ファジー論理は AI のサブセットで、オープンで不正確なデータ範囲（不正確なインプット）を取り込んで、「真」と「偽」の中間の可能性（例えば、確実に真、おそらく真、分からない、おそらく偽、確実に偽）を範囲に含むアウトプットを生成するような方法で、複数値を加工する。ファジー論理システムは、不完全で曖昧でゆがんだインプットや不確かな（ファジーな）インプットに対応して、人間の意思決定を旧来の真偽ロジックよりも入念に模倣することによって明確なアウトプットを返す。ハードウェア、ソフトウェア又はその双方の組合せのすべてで、ファジー論理を実行できる。
- **モノのインターネット（IoT）**：インターネットを使えるすべてのデバイスや機器の世界的ネットワーク。こ

うしたデバイスや機器にはセンサ、プロセッサやコミュニケーションハードウェアが埋め込まれていて、インターネットに接続され、人間が介在することなく、データ上で収集、送信、共有、行動ができる。IoT によって、莫大な量のデータがリアルタイムで生み出される。こうしたデータを分析し、望ましいアクションをとって事業成果を向上させるために利用されている。(ビッグデータの項参照)

- **相互運用性**:複数の異なる情報技術システムやソフトウェアアプリケーション間での通信やデータ交換が可能で、情報をリアルタイムで途切れなく利用できることを意味する。利用するシステムに関係なく、すべての者が運用できるようになる。
- **機械学習**:機械学習はAIの一種(サブセット)で、コンピューターシステムに「訓練」を施して、最小限の人的介入を以て、データから学習し、パターン認知を行い、意思決定をさせるものである。機械学習には、経験を通じて問題解決を自動的に行うための一連のアクション設計及びパターン認知アルゴリズムの発展を、人手を全く介さないかこれを最小限に抑えつつ行うことが含まれる。すなわち、機械学習は、分析モデルの構築を自動化するデータ分析方法である。
- **機械可読な規則**:機械可読な規則は、自然言語で書かれた法律用語で記載される規則類をコンピューター・コードに置き換えることにより、規制報告目的での AI 利用を可能にする。
- **自然言語処理(NLP)**:NLP は AI のサブセットで、コンピューターが人間言語を理解し、解釈し、操れるようにするものである。NLP によって、人間が機械と対話できるようになる。
- **プライバシー保護を強化する技術**:「データ所有者が、その基礎的データを必ずしも公開することなしに、基礎的データの計算を可能とする専門的な暗号能力。この技術を利用して、クエリ及び検索結果の暗号化を維持して(又は非公開にして)要求者だけ見えるようにし、データ所有者が検索クエリを見られないようにできる。」(N. マクスウェル、2020[16]) それゆえ、プライバシー保護を強化する技術という用語には、暗号を利用する多くの技術が包含され、主としてデータが利用される際のプライバシー保護を可能とする点において有用である。
- **リアルタイム分析**:リアルタイム分析とは、システムによって、入力されたデータの処理と分析が瞬時に行われ、ほぼリアルタイムで有意なアウトプット(情報、予測、決定等)が出力される機械学習プロセスである。
- **リアルタイムデータ(RTD)**:RTD は収集された途端に配信される情報をいう。それによって、供給される情報の適時性を保証する。RTD はリアルタイム分析を可能とし、動的でも静的でもありうる(特定時間における特定ロケーションを示す新しいインプット等)。
- **RegTech**:RegTech はフィンテックのサブセットで、新技術を利用して、既存の能力よりも、規制要件への遵守の効率と有効性を向上させる。
- **責任あるイノベーション**:適用される規制要件(AML/CFT、消費者保護、サイバーセキュリティ、プライバシー保護等)の目的に適合し、これを遵守するに当たり、イノベーションは責任を有する。
- **スマートマシン**:AI アルゴリズムを利用するコンピューターハードウェア及びソフトウェアシステム。ス

マートマシンは、多くの場合リアルタイムデータを利用して意思決定を行えるよう設計されている。機械的レスポンスや既定のレスポンスしかできない受動的なマシンと違って、スマートマシンは、センサ、デジタルデータ、リモートインプットを使って、こうした別々のソースから得られた情報をつなぎ合わせ、このインプットを即座に分析し、そのデータから得られた洞察に基づいて行動する。スマートマシンは、人間の知能に倣って、進んだコンピューター処理によって瞬時に分析を行い、それに基づいて判断を下す。

- **静的データ**：静的データとは、固定されたデータセット（収集された後は変化しないデータ）を意味する。
- **教師あり学習**：教師あり学習は、結果が判明しているアルゴリズム入力データを与えることにより、アルゴリズム予測モデルを学ばせる機械学習プロセスである。すなわち、教師あり学習は、実例によってアルゴリズムを学ばせることである。入力と出力のペア（ラベル付けされたデータ）でアルゴリズムのためのフィードバックを与える。それには、エラーを最小化するために、学習データセットを利用してモデルを修正する。例えば、学習データセットには、異なる種類の動物の画像を入れておき、それぞれの画像に関連するラベルを付ける。このようにして、予測されるラベルと正解とをアルゴリズムで比較できるようにする。教師あり学習においては、検証データセットを用いて、アルゴリズムのモデル学習進捗度を計測するとともに、テストデータセットを用いて、初見のデータに対するモデルのパフォーマンスを評価する。そして、モデルが学習データを効果的に学習して、一般化して新たなデータにできるようになっているかを決定する。
- **SupTech**：SupTech は、監督当局が先進的技術を利用して監督・検査を支援することをいう。
- **教師なし学習**：教師なし学習は機械学習手法の一つで、*ラベル付けされていない*データセットの分析やクラスタリングを、人間が介入することなくアルゴリズムで行い、隠れた規則性、データの類似性、異常値を発見する。入手したデータをアルゴリズムで解析し、解答キーを使うことなく推論を引き出し、類似性のあるものをグループ分けして、自律的観察と洞察に基づいて相関性や関係性を決定する。アルゴリズムが触れるデータ量が増えるにつれて、より正確で洗練されたモデル構築ができるようになる。

# 附属書 B. AML/CFT 分野における民間事業者間のデータ共有と分析のための新技術に係る追加的な RegTech ケーススタディ

### ケーススタディ：準同型暗号による暗号化クエリのパイロット

これは、金融機関と提携実施している RegTech で、銀行間の情報共有におけるプライバシー強化を目指すシステムである。準同型暗号を用いるこの技術では、規制を遵守しつつ、金融犯罪やコンプライアンスに関する暗号化クエリを展開できる。現在、この RegTech 開発者と金融機関は、このパイロットプログラムに参加する金融機関数の増加に努めており、新たなユースケース（顧客リスク評価及びモデル閾値を巡る、銀行内でのクロスボーダー利用のケース等）の明確化、並びに本番環境への移行に取り組んでいる。この取組みにおいて準同型暗号は、機微な情報が露出しないよう保護するために、特に利用されているが、複数の金融機関の間でのデータを用いた分析・照合もできるようになっている。プライバシー保護的な分析機能の利点は、検索キーワードを互いに明かすことなく、検索クエリを共有できることである。これによって、参加を検討する金融機関に対して分析能力を提供しつつ、開示、顧客への情報漏洩、規制違反のリスクが排除される。このプロジェクトの主たる障害となっているのは、共有が許されるデータの種類、許される環境、方法に関する規制が不明瞭なことである。

### ケーススタディ：ドイツにおける共有分析プラットフォーム

あるフィンテック企業が、主要な金融機関、ソフトウェア・ベンダー及び学界と提携して、金融犯罪と闘うための共同分析プラットフォームを新たに開発している。同プラットフォームには、金融機関の間で共有された取引データ及び金融データをプーリングして分析するためのツールセットが含まれている。犯罪行為や犯罪ネットワークは、個別の金融サービス事業者だけでなく、金融システム上に横断的に現れるので、同プラットフォームを通じて、こうした動向に関する最新の知見を得ることができる。こうした情報が得られれば、ドイツ全土と欧州の金融機関は、より広範な金融システムの視点から、顧客の活動ネットワーク全般に関する見識を構築できるようになろう。それによって、これまで察知できなかった、取引行動における隠された関係やパターンを明らかにして、マネー・ローンダリングのネットワークを絞り込むことができる。

### ケーススタディ：北欧の KYC プラットフォーム

北欧諸国の主要銀行 6 行は 2019 年、北欧市場における AML 規制に対処するための共同イニシアチブとして、RegTech 企業を設立した。創設メンバーである 6 行は、この RegTech 企業の KYC サービスとデジタル・プラットフォーム（顧客・エンドユーザーポータルを含む）を通じて利用できるよう、KYC 情報のための共通のデータ標準を開発した。同社のプラットフォームは完全に独立したもので、規制に適合した実効性のある KYC 情報を必要とする参加金融機関からアクセスできるようになっている。参加金融機関は、自行におけるリスク評価の基礎情報として、この KYC 情報に確実にアクセスして利用できる。顧客体験が一層顧客に密着したものとなって、金融機関と顧客との関係も改善されるので、顧客にも利益が及ぶことになる。顧客との関係の管理は金融機関側が引き続き担う。同社は、プライバシーをベ

ースにしたセキュアなハイブリッド・クラウドアーキテクチャの採用と、設計方針による保証を通じ、ソリューション全体にわたって個人データのプライバシーを保証する。

### ケーススタディ：金融犯罪インデックス

ある銀行において、RegTech 金融犯罪インデックスを利用して、金融犯罪リスクへのアプローチを強化する取組みが開始された。このインデックスは、銀行自身が保有するデータや公開情報と、RegTech が所有権を有するデータセットとを組み合わせて、全般的な金融犯罪リスクを毎月採点するとともに、9 つに区分された金融犯罪リスクの採点と報告を行う。

### ケーススタディ：セキュアなエンドツーエンドのプラットフォーム

ある RegTech 開発者によって、情報・データ交換プラットフォームが構築され、銀行等の金融機関がマネー・ローンダリングに関する情報を交換できるようになった。このプラットフォームを通じて交換される情報は、1 対 1 のメッセージング（情報依頼（RFI））又は 1 対多のデータプーリングに利用可能で、金融機関には以下のメリットがある。(1) 基本的な問い合わせの解決（相手方金融機関からの追加的情報を必要とする制裁アラート等）。(2) より複雑な共同調査（複数の金融機関が関与するセカンドレベルの取引モニタリングアラートに係る調査等）。(3) 高リスク顧客の管理に用いられるデータの高度化（PEP の根本原因分析（RCA）、実質的支配者（UBO）、資金源等に関する情報の共有等）。

本プラットフォームは、エンドツーエンド暗号化を用いて構築される。交換されるすべてのデータは暗号鍵で保護され、パスワード保護でバックアップされる。データプーリングのために一方向暗号やハッシュ関数が使われており、金融機関は複数の当事者と情報を共有できる。そこでは、ハッシュ関数により、交換されたデータやファイルが正しいことが検証される。このプラットフォームにおいて、ホストは暗号化されていない、いかなるデータにもアクセスできない。重要な活動はすべて記録されるので、このプラットフォームには完全な監査可能性が備わっている。

### ケーススタディ：準同型暗号を使用する記録のブラインドマッチング

あるソフトウェア会社が公的機関と共同で、準同型暗号を使った記録のブラインドマッチングのためのパイロットを進めていた。この公的機関は、複数の金融機関を含む官民のさまざまなソースから情報を収集して紐付けし、公共政策立案に必要な情報源となる統計の作成に役立てたいと考えていた。このソリューションプロバイダーは、データ提供者から、暗号化されたデータが受領者に渡るように、以下の要領で、技術、構造の両面の組合せで管理を行った。

1. 情報提供者の環境から送信されるのは、暗号化されたデータに限られる。
2. データは受領者に届くまで紐付けされない。受領者は、提供者から受領した暗号データを、トークン化されて紐付け可能なデータに変換するよう、第三者（仲介者）に依頼する。
3. 受領者は、提供者のオリジナルデータ（生データ）を得るために処理を逆行することはできなかったが、データセットを紐付けすることは可能とされた。

このパイロットによって、このソリューションを利用してデータの共通属性に係る紐付けができること、そして、受領者の環境を離れた後は、いかなる者もその属性を見ることができないことが成功裡に立証された。このように、個人のプライバシーを保護しつつ、政策立案に必要な集団分析情報が得られるようになった。同技術は、英国で本番環境入りしており、国民医療制度のデジタル化のため利用されている。

# 附属書 C. AML/CFT 分野における技術利用を支援する行動に係る提案

デジタルアイデンティティや、最先端の取引モニタリング・分析ソリューション（共同分析を含む）等の新技術の責任ある利用を行えば、官民両セクターにおいて FATF 基準を効果的に、リスクベースで実行するのに役立てることができ、金融包摂の進展にも資するであろう。

以下に記す原則は、2017 年に FATF が承認した、積極的かつ責任あるイノベーション推進のためのサンノゼ原則をさらに進めるものである。AML/CFT のための新技術の開発と実行は、その機会だけでなく脅威も反映する形でなされねばならず、新技術の利用に当っては、データ保護とプライバシーに関する国際基準、並びにサイバーセキュリティへの適合が確保されねばならない。

1. AML/CFT の実効性向上のための、政府と民間セクターによる、責任あるイノベーションを可能とする以下のような環境の創出。
   i. AML/CFT 手段（リスク評価、顧客管理等の要件を含む）の実行を促進し、その監督と検査を強化する革新的ソリューション。
   ii. 旧来の社内システムの更新やこれを新技術で置き換えるための優れたプラクティス。
   iii. 新たな AML/CFT ソリューションのための、次のような適切なセーフガードと特性。
      - プロセスと結果の説明性と透明性
      - 人間による監視
      - プライバシーとデータ保護の尊重
      - 高度なサイバーセキュリティ
      - 国際基準、国家基準、技術標準及びベストプラクティスとの整合
2. 新技術の実行に当たっての、プライバシー保護とデータ保護の徹底
   i. 新技術導入時において、個人情報処理のための有効な法的根拠の存在を確認すること。
   ii. 国内及び国際的な法的枠組みに沿った個人情報保護を行うこと。
   iii. 明確で、特定的かつ合法的な目的のために、国内及び国際的なルールに適合したデータの処理を行うこと。
   iv. 先進的なプライバシー保護技術の責任ある開発と採用を支援して、プライバシーを保護しつつ、強固な AML/CFT 情報共有・分析を可能にすること。
3. 計画的に金融包摂をサポートする AML/CFT イノベーションの推進
   i. 先進的ソリューションの開発と実行を通じて、金融包摂の障害を軽減すること。
   ii. 金融包摂を促進する FATF 目標と整合的な、責任あるイノベーションを確かにすること。

4. 柔軟で技術中立、結果ベースで、リスクベース・アプローチに沿ったイノベーションのための政策とアプローチの進展と伝達

   i. 新技術がもたらす構造的・組織的変化、意図せざる結果の可能性、AML/CFT の実効性に対する全体的な影響、金融包摂の観点から、新技術の効果を総体的に検討すること。

   ii. AML/CFT のための新技術の責任ある利用について情報提供したり促進したりするために、必要に応じて、明確な政策、ガイダンス、活用事例、ベストプラクティス、又は規制を公表し、その見直しを行うこと。

   iii. カウンターパートや規制対象事業者と協議を行い、関連政策及び意思決定過程について情報提供すること。

5. 情報に基づく監督の実施

   i. 新技術についての専門知識を構築し、新技術の活用に対して、特定の AML/CFT コンプライアンス目的を含め、情報に基づいた規制や監督を行えるようにすること。

   ii. AML/CFT 監督と検査のための、曖昧さがなく、明確に定義された新技術の活用を確認すること。

   iii. 新技術に関連するリスクとメリット、及びメリットを失わないための適切なリスク軽減策を理解すること。

   iv. AML/CFT 監督の高度化のために新技術を活用すること。

6. 協力関係の促進と円滑化

   i. データ保護やプライバシー保護の所管を含むすべての関係当局と協力及び連携して、AML/CFT のための新技術の利用のリスクとメリットを理解して取り組むための、包括的で統一的なアプローチを円滑にする。

   ii. 新技術や先進的ソリューションについての、政府横断的な研究開発、かつ／又は官民での研究開発を円滑化する協力環境を進展させるよう考慮すること。

   iii. AML/CFT 新技術の活用を管理する世界共通の原則を発展させる国際的な取組みに参画し、新技術の活用が、人権と整合的な形で、かつ、AML/CFT の世界的な実行、サイバーセキュリティ、データ機密性やデータ保護手段、そして関連の技術的基準や信頼できる枠組みを改善する形で確実に行われるようにすること。

# 参考文献


欧州銀行監督機構(2020),ビッグデータと高度な分析 [13]

欧州データ保護委員会(EDPB)(2020)、マネー・ローンダリング及びテロ資金調達の防止に関連して処理される個人データの保護に関する声明、 [1]
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_aml_actionplan_en.pdf.

FATF(2017)、民間セクターにおける情報共有ガイダンス、 [10]
https://www.fatfgafi.org/publications/fatfgeneral/documents/guidance-information-sharing.html.

金融犯罪取締捜査網(FinCEN)(2020)、ファクトシート、セクション 314(b)、 [11]
http://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

金融安定理事会(FSB)(2020)、規制当局と規制対象事業者による監視・規制技術の利用について、32 ページ、 [9]
http://www.fsb.org/2020/10/the-use-of-supervisory-and-regulatorytechnology-by-authorities-and-regulated-institutions-market-developments-and-financialstability-implications/.

金融安定理事会(FSB)(2017)、金融サービスにおける人工知能及び機械学習の利用について、 [17]
https://www.fsb.org/wp-content/uploads/P011117.pdf.

GLEIF(年次不詳)、取引主体識別子(LEI)の導入について、 [21]
http://www.gleif.org/en/.

国際金融協会(IIF)(2019)、データの越境移転 – データ・ローカライゼーション制約の克服、 [19]
http://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf.

N.マクスウェル(2020)、イノベーション及びディスカッションペーパー:金融犯罪対策としてのプライバシー保護分析の利用に関するケーススタディ、 [18]
http://www.futurefis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_-_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf.

マカフィー(2020)、クラウドセキュリティとは何か? [7]
http://www.mcafee.com/enterprise/en-us/securityawareness/cloud.html.

マイクロソフト(2016)、準同型暗号、 [2]
http://www.microsoft.com/enus/research/project/homomorphic-encryption.

マイクロソフト・アジュール(年次不詳)、コンフィデンシャル・コンピューティング、 [6]
https://azure.microsoft.com/enus/solutions/confidential-compute. (2020 年 12 月にアクセス)

OECD(2020)、「AI 原則」、 [16]
https://www.oecd.ai/ai-principles.

OECD（2019）、人工知能に係る原則、 [15]
http://www.oecd.org/goingdigital/ai/principles/.

OECD（年次不詳）、ブロックチェーンプライマー、 [8]
http://www.oecd.org/finance/OECD-Blockchain-Primer.pdf （2020 年 12 月にアクセス）

OECD（年次不詳）、CRS とは何か？ [14]
http://www.oecd.org/tax/automatic-exchange/commonreporting-standard/ （2020 年 12 月にアクセス）

SAS（2020）、自然言語処理、 [5]
http://www.sas.com/en_us/insights/analytics/whatis-natural-language-processing-nlp.html.

J. シャイブナー（2020）、健康データのマルチサイトリサーチにおけるデータ保護及び倫理要件：法的ガバナンス体制及びデータ保護技術の役割に関する比較検討、 [3]
http://www.ncbi.nlm.nih.gov/pmc/articles/PMC7381977/pdf/lsaa010.pdf.

G. シフマン（2020）、「革新的技術を通じた連合学習（白書）」 [4]

ティム・フルセン（2020）、シェアリングはケアリング～ヘルスケア分野におけるデータ共有イニシアチブ、 [20]
http://www.mdpi.com/1660-4601/17/9/3046/pdf.

UNCTAD（2020）、世界各国のデータ保護とプライバシー法制、 [12]
https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

## データプーリング、共同分析とデータ保護にかかるストックテイク

近年の技術進歩により、金融機関において大量のデータをより効率的に分析して、パターンや傾向を効果的に特定できるようになった。データプーリングと共同分析を行うことで、金融機関が共同して、マネー・ローンダリングとテロ資金供与のリスクを、より的確に認識、評価及び軽減できるようになるかもしれない。FATF は、犯罪行為のより迅速かつ効果的な特定に資すると思われる革新的技術について検討を行った。それは同時に、誤検知を低減し、犯罪者による金融機関の間の情報格差の悪用を回避する技術でもある。

本報告書では、データ保護とプライバシーの必要性についても強調されている。マネー・ローンダリング/テロ資金供与の防止と、データ保護とプライバシーとの両立は、重大な公共利益であり、重点目標として取り組むべき課題だからである。プライバシー強化のための新技術や新興技術は、国内外のデータ保護とプライバシーの枠組みに従って特定用途に供される情報を保護する手段として、その将来性が期待される。