諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究

その１

調査項目①　　諸外国におけるマネロン情報の共有制度と個人情報保護法制

令和４年 12 月 23 日

有限責任 あずさ監査法人

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG

目次

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

1 はじめに

本報告書は、有限責任 あずさ監査法人が、金融庁から委託を受けた「諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究」の調査研究結果をまとめたものである。調査対象は、

調査項目①　諸外国におけるマネロン情報の共有制度と個人情報保護法制

調査項目②　当局マネロン検査のフォローアップを外部適格コンサルタントに委託する手法(英)の事例研究

調査項目③　海外当局のマネロンリスク分析手法やデジタル技術の活用状況

- デジタル技術等を活用した先進的なリスク分析手法の事例研究
- 暗号資産および暗号資産交換業に関するリスク分析・モニタリング手法の事例研究

と多岐にわたることから、報告書を以下のように 4 分冊構成とした。

分冊	タイトル	内容
第一分冊	諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究　その１	調査項目① 諸外国におけるマネロン情報の共有制度と個人情報保護法制
第二分冊	諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究　その２	調査項目② 当局マネロン検査のフォローアップを外部適格コンサルタントに委託する手法(英)の事例研究
第三分冊	諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究　その３	調査項目③－１ デジタル技術等を活用した先進的なリスク分析手法の事例研究
第四分冊	諸外国におけるマネロン等対策の実態調査と先進事例の分析に関する調査研究　その４	調査項目③－２ 暗号資産および暗号資産交換業に関するリスク分析・モニタリング手法の事例研究

本報告書は、第一分冊であり、調査項目①　諸外国におけるマネロン情報の共有制度と個人情報保護法制を対象としたものである。諸外国における制度を調査し、我が国の今後の制度設計に関する考察をとりまとめた。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2 諸外国における制度について

2.1 オランダ Transaction Monitoring Netherlands（TMNL）

2.1.1 スキームの概要

オランダの主要銀行5 行(①ABN Amro、②ING、③Rabobank、④Triodos Bank、⑤Volksbank)が TMNL B.V.を 2020 年 7 月に設立した。TMNL は、各行がそれぞれの取引データを TMNL に集約し TMNL として、一つの取引モニタリングシステム(TMS)にかける(＝joint monitoring を行う)というものである。TMNL の TMS は、各行で行っている既存の TMS を代替するものではなく、追加的な位置づけとなっている。

2.1.2 スキームの制定経緯

取引モニタリングに関する民民間の情報共有を可能とするための法改正や実務対応等について、関係当局もこの TMNL の構築に深く関与している。

TMNL は、NVB(オランダ銀行協会)がそのスタートを宣言し、同協会の公表文(2019 年 9 月)[1]には以下のとおり構想の背景が記載されている。

1. オランダでは麻薬取引関連犯罪が多い。同国では、主に麻薬取引関連で年間 160 億ユーロ(約 2 兆円)相当の犯罪収益が流通しているとされ、深刻な社会問題となっている。NVB の会長である Chris Buijink 氏(同国政府の経済省出身)は「銀行界がこの問題に取り組むことは銀行の重要な公的義務であり、対処すべきと考えている」旨を述べている。
2. 同国の民間銀行は 2018 年中に 6.8 万件を不自然な取引として報告し、FIU はそのうち 1.5 万件を疑わしいものとして処理している。
3. 今回の取組に参加する 5 行は、年間 98 億件＝1 日平均 27 百万件にのぼる支払指図を処理している。
4. 同国の銀行界では合計で 5,500～6,000 人にのぼる従業員がフルタイムでマネロン対応関係の仕事に従事するなど、対応コストも相当大きい。
   複数かつ多様な銀行が絡む取引をまとめて取引モニタリングできれば、犯罪収益の流れの検知はより容易になる。マネロン対応は、個別銀行単位で行うよりも、国レベル(つながりのある銀行間レベル)で対応することが求められている。
5. 今回の銀行界の取組は 2019 年 7 月に財務相と法務・安全保障相が連名で公表した「Money Laundering Action Plan」も踏まえて、始められている。

2.1.3 スキームの枠組

TMNL は次の 4 フェーズで導入を進めていると、2020 年段階では言われていた。

フェーズ 1　法人取引情報のみを対象として「顧客分析」を行う(後述する法改正前で可能な範囲を実施する)

[1] Dutch banks join forces to combat money laundering, Dutch Banking Association (NVB), https://www.nvb.nl/english/dutch-banks-join-forces-to-combat-money-laundering/

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

フェーズ 2　要配慮個人情報[2]を含む、全ての取引情報について「顧客分析」を行う(法改正後に実施可能)
フェーズ 3　要配慮個人情報を含むすべての取引について「取引モニタリング」を行い、TMNL B.V.が疑わしい取引の届出案の作成を行う(取引モニタリングの業務委託を受ける)
フェーズ 4　TMNLB.V.が疑わしい取引の届出関係の対応全般を行う(取引モニタリングだけではなく疑わしい取引の届出事務の業務委託も受ける)

フェーズ 1 は、取引モニタリング業務の外部委託の形態をとらず、あくまで各行が行う CDD に資するためという位置づけで顧客分析を実施し、結果を各行に提供するという建付とすることとしていた。2020 年 12 月中に各行より暗号化された状態で法人取引情報を TMNL へ共有し、法人取引情報の分析開始を予定しているとあったが、2021 年 11 月段階で実施したのはマルチバンクアラートを提供するところまでである。2021 年時点でフェーズ 1 は完了しておらず、2022 年完了予定とあったが、現在の状況については不明である。フェーズ 2 以降は法改正の後に実現するものであり、フェーズ 3 以降で本来の取引モニタリング業務を参加行からの外部委託という形を予定しているが、2022 年 7 月時点で、法改正自体が完了していない。詳細は以降のセクションで記載する。

2.1.4　スキームと DPP 関連規制との関係性

オランダのプライバシー保護法(AVG)は、GDPR に基づくものである。2020 年の TMNL へのヒアリングによれば、個人情報を含む情報を金融機関の間で共有することについては要配慮個人情報の取扱を除き既に法的課題は解消されているとの明言があった。DPP 当局および AML/CFT 当局間の対話と基準・解釈の明確化、Data Protection-by-design/default Principle に基づく TMNL(および参加行)のプライバシー保護の枠組構築と当局への説明責任が十分果たされた結果と推察される。オランダの ML/FT 防止法である Wwft は、AML/CFT 規制事業者が実施すべき取引モニタリング業務の外部委託を認めていない。そこで、現段階の TMNL は取引モニタリング業務の外部委託という形態をとるのではなく、各行の取引モニタリング業務はそのまま完結するものと整理し、あくまで各行が行うべき CDD に資する当該顧客についての分析情報を提供する位置づけとし、取引モニタリング業務の外部委託とはしない枠組となっている。

そして、フェーズ 2 以降を実現可能とするために、同国の ML/TF 防止法(Wwft)の改正として次の提案が 2020 年時点でなされていた。

① オランダ固有の規制(EU AMLD では禁止されていない)として取引モニタリング業務の外部委託は認められておらず、Wwft の第 10 条の修正により、これを許容するよう改正すること
② Wwft の第 34 条では、金融機関は AML/CFT 目的で個人情報の取得を許可しているが、金融機関の間での要配慮個人情報の共有については不明確であり、要配慮個人情報の共有を認める旨を明確化すること

[2] 個人情報とは個人情報保護法によれば「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実、その他本人に対する不当な差別、偏見その他の不利益が生じないように、その取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」とされている。同法は、EU データ保護指令の十分性の認定を受けるために改正されており、EU での要配慮個人情報の定義と同等の規定となっている。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2.1.5 最近の動向

提案された Wwft の改正案は、上記の通りであり、銀行の支払取引の共同モニタリングと ML/TF のリスクが高いクライアントを調査する機関間のデータ共有を可能にするものだったが、2022 年 7 月の段階で法改正は実現していない。むしろ、改正案に対して国家評議会(the Dutch Council of State)より勧告[3]が出された。(2021/1/13 に設立、2022/6/16 に公表)

同勧告は、銀行、監督当局、捜査当局によるマネー・ローンダリングへの共同アプローチに批判的であり、国家評議会は現在の設計では望ましくないと考えている、としている。詐欺師、犯罪者、テロリストが逮捕される可能性が高いことは、すべての人のプライバシーの侵害を上回るべきものではなく、また、調査業務を銀行に委託することにも批判的であり、主に以下の 3 点を述べている。

- 提案された措置は、機密データとプライバシーを保護するという市民と企業の基本的権利の広範な侵害につながる。ML/TF との闘いは重要だが、国家評議会は、これらの目的が手段を正当化するかどうかを疑問視している。
- 銀行取引が大規模に共同でモニタリングされるのは前例のないものであり、市民や企業に属するデータの機密性の重大な侵害を示す。プライバシーの権利だけではなく、このモニタリングは、排除と差別にもつながる。この共同取引モニタリングの必要性および妥当性が実証されていないとの意見である。
- 提案は、(潜在的な)高リスククライアントを調査する際に、機関が他の機関に問い合わせる義務を課している。その後、要求された機関はデータを共有する義務を負う。国家評議会は、データ共有は機密のビジネスおよび個人データの保護の違反であり、この提案は民法公証人および弁護士の職業上の秘密主義とも矛盾すると述べている。したがって、国家評議会は、この措置の必要性と妥当性がさらに実証されることを勧告している。

その後 2022 年 10 月に財務省は Wwft の改定案[4]をオランダの国会に提出した。この改定案では銀行などを AML 対策におけるゲートキーパーとして情報交換の可能性を拡大しており、これが施行されれば TMNL を通じた銀行による共同での取引モニタリングの実施が可能となる。 この改定案において、財務省としては、プライバシーに関する事項について国家評議会のアドバイスを既に考慮しており、データの疑似匿名化を含む、十分な保証がなされているとしている。現時点において改定案は、議会に提示されているのみで、未だ有効なものとなっておらず、この通り施行されるかは不確実な状況にある。

2.2 英国 Joint Money Laundering Intelligence Taskforce (JMLIT)

2.2.1 スキームの概要

2015 年 2 月に試行的に立ち上げられた後、2016 年 4月に常設組織とされた。JMLIT は、NECC(国家経済犯罪対策センター)内の組織(タスクフォース)として位置付けられており、法執行機関等の政府機関と民間金融機関等および関連団体が、マネー・ローンダリングをはじめとする経済犯罪関係の情報を共有し、分析するためのパートナーシップとされている。参加機関は、法執行機関(NCA：国家犯罪対策庁、HMRC：歳入関税庁、

3 Wet plan van aanpak witwassen (Proposal for Anti-Money Laundering Action Plan), Government of Netherland, https://www.raadvanstate.nl/adviezen/@122774/w06-20-0354-iii/

4 Wetsvoorstel plan van aanpak witwassen (Anti-Money Laundering Act), The Council of State (Netherlands), https://www.rijksoverheid.nl/documenten/kamerstukken/2022/10/21/wetsvoorstel-plan-van-aanpak-witwassen

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

SFO：重大不正捜査局、City of London Police：ロンドン市警察、Metropolitan Police Service：ロンドン警視庁)と FCA(金融行為規制機構)、民間金融機関等 40 余、非営利団体である Cifas(英国詐欺防止サービス)である。

2.2.2 スキームの制定経緯

英国は欧州の金融センターとして、長年にわたり ML/TF との闘いの中心にいたが、2008 年の金融危機後の数年間の捜査では、ML/TF と租税回避の両方で注目を集めた事案がいくつか明らかになった。例えば、ロシアのオリガルヒと結びついた違法資金が英国の主要な金融機関を通じて資金洗浄されており、監督当局やその他の規制当局は、「予防よりも利益の追求を優先する」文化の下で、こうした活動を積極的に追求していなかった。

これらの事実が明らかとなり、抜本的な改革措置の必要性を認識した英国政府は、Financial Services Agency の廃止を含む英国の規制当局の改革に着手し、AML/CFT 監督を含む行為関連の監督を引き継ぐ、新たに設立された金融行為規制機構(2013 年設立の FCA)、および経済犯罪の捜査・訴追に責任を負う最高捜査機関として新たに設立された国家犯罪対策庁(2013 年設立の NCA)を設置した。

この一連の改革の一環として、2014 年、英国のテレサ・メイ内務大臣は、新たに設立された FCA と NCA の代表とともに、金融セクターの大手規制企業約 20 社の CEO を集め、ML/TF および脱税との闘いにおける協力を強化する方法について議論した。これらの議論を経て、2015 年、初の官民パートナーシップ(Public-Private Partnership: PPP) の一つである 官民情報連携パートナーシップ(JMLIT)が結成された。

上記のステークホルダーは、迅速な行動がとれるように JMLIT の開発を優先することを選択したため、ML/TF の疑いが確立された場合に、顧客および取引情報の共有を可能にするという、既存の規制枠組みに依拠したものとなった。JMLIT では、これは後述する Operations Group の形をとっていた。JMLIT は今後も進化を続け、最終的には金融機関間でより広範な情報共有が可能となるよう、必要な規制改革を実施していきたいという方向性である。例えば、個々の金融機関では疑わしいと判断されない取引(Pre-Suspicion)が、複数の金融機関間で情報共有することでより大きなデータベースの中で分析されることによって疑わしいと判断され、より網羅的なモニタリングが実施できる、ということを実現していくことも視野に入れている。

2.2.3 スキームの枠組

JMLIT の活動は、(1) Operations Groups による活動と、(2) Expert Working Groups による活動に大別される。

(1) Operations Groups は、進行中の個別具体的な捜査案件の支援を目的とし、Banking Sector Operation Group と Insurance and Investment Sector Operation Group に分かれている。法執行機関が数社程度の民間金融機関等を具体的に指名し、彼らとの間で、個別具体的な捜査関係の情報の共有・分析等を進める。

(2) Expert Working Groups は、もう少し一般的なテーマを取り上げる。すなわち、犯罪の手口の分類や、新たに登場したリスクの特定のために、テーマ性の強い活動をする。Expert Working Groups が重点的に扱うエリアは、英国の NRA(国家リスク評価書)で特定された脅威や「重大・組織犯罪」について優先対応が求められる分野とされる。そして、作業の結果、得られた情報は金融機関等に「JMLIT Alert」、「red flag」、「犯罪手口(typologies)」として発信される。それらは、受信先となる個別金融機関等に、取引モニ

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

タリングシステムのシナリオや閾値の見直し等を促すことで、「疑わしい取引」のより効果的・効率的な検知を支援するものである。

2.2.4 スキームと DPP 関連規制との関係性

PPP のために適切になされた情報共有(官民間、民民間)はいかなる情報開示の制約に違反するものでもないことが定められている。(官民間：Crime and Court Act 2013 Section 7、民民間：Criminal Finances Act 2017 Section 11)

Crime and Court Act 2013 Section 7 では、民→官、官→民の情報共有を可能としている。

> Crime and Court Act of 2013 の Section 7
> (1) A person may disclose information to the NCA if the disclosure is made for the purposes of the exercise of any NCA function.
> (4) An NCA officer may disclose information obtained by the NCA in connection with the exercise of any NCA function if the disclosure is for any permitted purpose.

まず、Subsection(1)において、何人も NCA の職務執行の目的であれば NCA に対して情報を開示することが認められている(民→官の情報開示)。NCA の職務執行の目的のためであれば個人情報を含む情報開示が法律上認められることから、JMLIT の Operation Group の中で民間の主体が個別具体的な捜査に資する関連情報を当局に開示することが可能となる。この情報開示は疑わしい取引の届出に関連する情報の開示に限定されない。

また、Subsection(4)において、NCA officer は NCA がその職務執行に関連して取得した情報を「認められた目的」のために情報開示することが認められている(官→民の情報共有)。「認められた目的」のための情報開示の例示として、NCA が入手した犯罪を疑わせる取引に関する情報を、民間金融機関等に共有することで犯罪の防止や検挙という目的に資すると NCA が判断した場合の情報開示 等が示されている。

そして、官→民、民→官の情報開示に関連して、情報保護・プライバシーや守秘義務の観点で、以下の規定が定められている。

> Crime and Court Act of 2013 の Section 7
> (8) A disclosure of information which is authorised or required by this Part does not breach—
> (a) an obligation of confidence owed by the person making the disclosure, or
> (b) any other restriction on the disclosure of information (however imposed).
> (9) This section is subject to Schedule 7 (information: restrictions on disclosure).

Subsection(8)において、Section 7 により認められた情報開示は、金融機関等が顧客等に対して負っている守秘義務(a)、その他のいかなる情報開示の制約(b)に違反するものではないことが保証されており、ここでの(b)の「いかなる情報開示の制約」には、個人情報保護 の法律も含まれると考えられる。

また、Subsection(9)が参照する Schedule 7 において、NCA から民間金融機関等へ開示してはならない情報の種類を定める規定や、NCA から情報開示を受けた者がその情報を他者にさらに開示することを制限する規定等を設けており、情報開示が認められる範囲を明確にしている。

英国においては 2013 年の段階でこのような法令が整備されたことから 2015 年からの JMLIT の円滑な運営が可能となったものと考えられる。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

さらに、上記「Crime and Courts Act 2013」に続いて、下記の「Criminal Finances Act 2017」の Section 11「Sharing of information within the regulated sector」において、「民→民の情報共有」が可能となる条件についても明確化されたことから、さらに JMLIT の円滑な運営が可能となったものと考えられる。

Criminal Finances Act 2017

11 Sharing of information within the regulated sector

"339ZB Voluntary disclosures within the regulated sector

(1) A person (A) may disclose information to one or more other persons if conditions 1 to 4 are met.

(2) Condition 1 is that—

(a) A is carrying on a business in the regulated sector as a relevant undertaking,
(b) the information on which the disclosure is based came to A in the course of carrying on that business, and
(c) the person to whom the information is to be disclosed (or each of them, where the disclosure is to more than one person) is also carrying on a business in the regulated sector as a relevant undertaking (whether or not of the same kind as A).

(3) Condition 2 is that—

(a) an NCA authorised officer has requested A to make the disclosure, or
(d) the person to whom the information is to be disclosed (or at least one of them, where the disclosure is to more than one person) has requested A to do so.

(4) Condition 3 is that, before A makes the disclosure, the required notification has been made to an NCA authorised officer (see section 339ZC(3) to (5)).

(5) Condition 4 is that A is satisfied that the disclosure of the information will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering.

A person may disclose information to A for the purposes of making a disclosure request if, and to the extent that, the person has reason to believe that A has in A's possession information that will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering.

11 Sharing of information within the regulated sector

339ZF Section 339ZB: supplementary

(1) A relevant disclosure made in good faith does not breach—

(a) an obligation of confidence owed by the person making the disclosure, or
(b) any other restriction on the disclosure of information,

however imposed.

また、この Criminal Finances Act 2017 においても、以下のとおり、上記の Crime and Court Act 2013 と同様の情報保護・プライバシーおよび守秘義務についての規定が定められている。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2.2.5 最近の動向

JMLIT 策定後の数年間、JMLIT 参加金融機関は、上述の情報共有の強化といった戦略的イニシアティブよりも、個々の金融機関における AML/CFT コンプライアンス取り組みの強化に焦点を当て、戦術レベルに焦点を戻している。その結果、英国市場における議論と関心は続いているものの、Pre-Suspicion のような高度な情報共有を可能にするために必要な規制改革に向けた具体的な措置はとられていない。

2.3 オーストラリア Fintel Alliance

2.3.1 スキームの概要

2017 年 3 月に 22 の参加主体で始まり、その後参加主体の数が増えている。豪州は、連邦制国家であるために法執行機関の数が多いなどの特徴があり、それを反映して Fintel Alliance の参加主体は数が多く(2020 年 9月時点で 28)かつ多彩であることが特徴である。参加メンバーには海外の機関(英国の NCA とニュージーランド警察)も含まれる。

規制監督当局である AUSTRAC は英国の JMLIT のような情報共有を受け入れる窓口は持っていない。代わりに、Fintel Alliance では、Anti-Money Laundering and Counter-Terrorism Financing Act 2006 の下で、民間部門から AUSTRAC へ出向者を出させる当局の権限を利用して情報共有を行い、当局者が出向者に対して、調査を行う際の情報保護の環境を整備している。

2.3.2 スキームの制定経緯

オーストラリア当局(金融監督機関は Australian Prudential Regulation Authority: APRA、AML/CFT 規制当局および FIU は Australian Transaction Reports and Analysis Centre: AUSTRAC)は、もともと金融機関における AML/CFT 規制遵守状況について十分監督できておらず、主要銀行も関連規制対応への投資には積極的ではなかった。

しかし、オーストラリア・コモンウェルス銀行(CBA)において疑わしい取引の報告に関する不備が発生し、7 億オーストラリアドルの罰金など厳しい行政処罰が下されたことや、AML/CFT に限らず複数の金融機関においてコンダクト上の問題が頻発したことから、2018 年にはオーストラリア王位委員会(特別組織)による銀行への違法性一斉調査が開始されている。このような中、つい最近まで国民に公表していなかった 2000 万人以上に影響を与えた CBA での個人情報漏洩も発覚し、銀行や当局に対する信頼が低下している状況にある。AML/CFT 態勢不備への関心が集まる中、銀行側も自身のコンプライアンス態勢高度化は必要との危機意識を持っており、情報共有も含めた様々な選択肢を検討し始めた段階にある。

一方で、オーストラリアの AML/CFT コンプライアンスの状況は、例えば英国と比較して、成熟度は発展途上の段階にあり、金融機関間の情報共有の必要性を強調するようなイベント(例：米国での 2001 年 9 月 11 日の大規模テロ事件)等もオーストラリアではないこともあり、文化的にオーストラリアの一般消費者は政府機関以外の機関の間でこのような情報を共有することについて抵抗感がある。

こういった背景から、(a)顧客または取引に関連する異なる金融機関間での情報共有を可能にする現行の法的枠組みは存在せず、(b)情報共有以前の問題として、オーストラリアの個々の金融機関としての AML/CFT 態勢整備について喫緊の課題として優先して取り組む必要性がある、といった状況である。よって、Fintel Alliance

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

は、金融機関同士ではなく、規制当局と金融機関との間で、既存の規制枠組みの下で許容される情報共有(リスク・犯罪の動向・手口に関する情報の共有)を優先するように 2017 年 3 月に策定され、進化してきたと考えられる。

2.3.3 スキームの枠組

Fintel Alliance は、「Operation Hub」と「Innovation Hub」の 2 つの組織で活動している。

1. Operation Hub
   Operation Hub での活動に民間部門から参加する者は、AUSTRAC に「出向」する形をとることによって、彼らが持っている取引先の情報を当局に伝えることができる。参加者は「プロジェクト」ごとに情報を共有し、それぞれの知見を活かして、成果を生むように努力する。
2. Innovation Hub
   Innovation Hub は、Operation Hub の運用をより高度化するための技術的ソリューションの開発やテストを参加メンバーと行っている。

2.3.4 スキームと DPP 関連規制との関係性

情報保護義務違反の責任を免れるための特段の法的な手当てはなされておらず、AUSTRAC 出向者間でのみ情報共有することで整理している。

疑わしい取引の届出に該当しないような情報を当局が得るためには、AUSTRAC は民間の Fintel Alliance メンバーに対して、正式な要請通知を発出する必要があり、一定の法的保護はあるものの、民間メンバーは、要請に正確に応えられなかった場合や要請されていない情報を伝えてしまったような場合に、罰則を受けるリスクがある。また、疑わしい取引の届出のように認められた形以外では、民間メンバーに自発的で早期の情報共有を認める仕組みは存在せず、民民間の情報共有の窓口も存在しない。ただし、民間から AUSTRAC への出向者に限っては、「Anti-Money Laundering and Counter-Terrorism Financing Act 2006 121 Secrecy—AUSTRAC information and AUSTRAC documents」法の下で適切に AUSTRAC が入手した情報を幅広く知ることができ、出向元以外の他の金融機関が届け出た疑わしい取引に関する情報やそれに関連して AUSTRAC が追加で入手した個別の顧客情報を含む捜査情報を知ることが可能となっている。

AUSTRAC への出向者がこのような情報を知ることが出来る点については、Anti-Money Laundering and Counter-Terrorism Financing Act 2006 により、以下の通り定められている。

> Anti-Money Laundering and Counter-Terrorism Financing Act 2006
> 121 Secrecy—AUSTRAC information and AUSTRAC documents
> (1)This section restricts what a person (the entrusted public official) who is or was:
> (a) the AUSTRAC CEO; or (b) a member of the staff of AUSTRAC; or (c) a person engaged as a consultant under subsection 225(1); or (d) a person whose services are made available to the AUSTRAC CEO under subsection 225(3) ; or (e) the Director of AUSTRAC; or (f) a person engaged as a consultant under repealed section 40A of the Financial Transaction Reports Act 1988;
> may do with AUSTRAC information or documents containing AUSTRAC information.
> (2)The entrusted public official commits an offence if:
> (c)the official has obtained AUSTRAC information (otherwise than under Division 4); and
> (e)the official discloses the information to another person.

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

AUSTRAC への出向者が知ることが出来るこのような情報は、AUSTRAC の外部、すなわち出向元の金融機関等と共有することは認められていない。しかし、出向元の金融機関等へ情報が漏洩するリスクがあるため、Fintel Alliance は情報共有に関するメンバー間で合意されたルール(プロトコル)を定めている。

Fintel Alliance が発行している Annual Report 2018-19 によると、このプロトコルの概要は以下のとおり。

> Fintel Alliance Partners agree that information disclosed to them within Fintel Alliance will only be used for the purposes for which the information was provided. Under the Protocol, each partner agrees that it is responsible for ensuring there is no mishandling or inappropriate use (including unauthorised copying, reproduction and storage of any kind) or disclosure of information they access within the Fintel Alliance.
> The Protocol requires all Fintel Alliance partners to comply with their privacy obligations under applicable privacy legislation and with any common law confidentiality obligations.

ここで、上記の最後にあるように、Fintel Alliance メンバーは、プライバシー保護義務を遵守することが求められており、英国で、情報保護義務違反の責任を免れるための特段の法的な手当てがなされているのとは異なる。

また、Fintel Alliance の同 Annual Report 2018-19 には、個人情報保護について以下のようにも記載されており、AUSTRAC は、法により、収集された個人情報を安全に扱う責任を負っており、情報保護に関するポリシーを定めて情報の安全をコントロールすることが要求されている。

> AUSTRAC ensures that any personal information collected is dealt with responsibly and respectfully by Fintel Alliance, in accordance with its legal obligations under the AML/CTF Act, the Financial Transaction Reports Act 1988, and the Privacy Act 1988.(中略)
> The Privacy Act also requires agencies and entities bound by the APPs, including AUSTRAC, to have a privacy policy for handling and managing personal information. AUSTRAC's privacy policy outlines AUSTRAC's practices for the handling and management of personal information and also covers the Fintel Alliance.

このように、豪州の Fintel Alliance においては、情報保護義務違反の責任を免責することにより情報共有を促すのではなく、AUSTRAC の中でのみ情報共有を認め、その AUSTRAC の中での情報保護の環境を整備することにより、AML/CFT の目的に必要な情報共有を促すという手法を採っていると考えられる。

2.3.5 最近の動向

今後の展開として、Fintel Alliance 2020-21 年次報告書[5]には、次のようなプロジェクトを通して情報共有の継続的な進化の重要性を認識し、取り組んでいるとの記載がなされていた。

(a) 情報共有プラットフォーム
機密情報を安全に情報共有可能なプラットフォーム構築への取り組み。

(b) アラートプロジェクト
金融システムにおける資金移動の情報を捉え、異なる金融機関間の情報をネットワークとしてリンクするなど、疑わしい取引の分析を可能とするプラットフォーム構築への取り組み。このプラットフォームは、AUSTRAC が開発した最先端のプライバシー保護アルゴリズムを利用しプライバシーを保護する。

---

5 Fintel Alliance Extract 2020-21 AUSTRAC Annual Report, (austrac.gov.au), https://www.austrac.gov.au/sites/default/files/2021-11/FintelAlliance_PerformanceReport20-21_v5_Web.pdf

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

上記(a)(b)のプロジェクトについて、KPMG Australia に確認したところ、下記の通りの現状であるということが認識された。

(a) 情報共有プラットフォームの機能は、Fintel Alliance の年次報告書で誇張されていた。実際には、情報共有プラットフォームとは単に Microsoft Teams の使用を指しており、Microsoft Teams は非機密情報の共有にのみ使用されているようである。

(b) 現在のところ、アラートプロジェクトの実施は構築が複雑で困難であると判断されており、当面は優先順位を下げているようである。

2.4 香港 Fraud and Money Laundering Intelligence Taskforce (FMLIT)

2.4.1 スキームの概要

2017 年 5 月に試行開始され、2019 年 6 月に常設化された。その目的は、官民がその知見を一堂に集め、協働することで、より効率的、効果的に ML/TF 等に対処することとしている(他の官民連携と同じ)。HKPF(香港警察)が中心に位置づけられており、HKMA(香港金融管理局)はこれを支援する立場である。民間からは、香港の銀行10 行と HKBA(香港銀行協会)が参加している。

2.4.2 スキームの制定経緯

香港は長年にわたり英国の植民地だったため、自由市場資本主義経済の下で発展し、シンガポールとともに ASPAC の主要金融センターとして台頭してきた。中国政府は香港が中国経済において重要な役割を果たしていることを認めており、前述の状況は 1997 年に香港が中国に返還された後も続いたため、「一国二制度」モデルに基づく特別行政区として活動することを認めた。その結果、香港の規制の枠組みと監督制度(AML/CFT 規制枠組み、AML/CFT 主監督機関である HKMA の発展と体制を含む)は、中国のものというよりも欧米先進国の枠組みに沿ったものとなっている。香港が金融の中心地であるということは、世界中から投資が集まるだけでなく、日々の大量の取引に紛れて、海外での犯罪から得た犯罪収益の出所を隠そうとするマネー・ローンダリングを行う犯罪者も集まるリスクがあることを意味する。また、香港は中国本土との間の合法的な資金と違法な資金の両方の玄関口として、利用され続けている。

HKMA は、自身の役割および ASPAC の主要な金融センターとしての地位を認識し AML/CFT 遵守の監督に積極的に取り組んでいる。しかし FATF が香港の相互審査結果報告書において指摘しているように、ASPAC を中心とした犯罪者が直接または間接に関与する大規模な ML/TF 事件が発生している。例えば、1 MDB スキャンダルの取引の多くは、2012 年から 2013 年にかけて香港に所在する外国金融機関において行われたものである。これに関連して、香港証券先物委員会 (SFC) が、香港に所在する Goldman Sachs (Asia) L.L.C.(GS アジア)に対し、1 MDB の債券取引に関与したとして 3 億 5000 万米ドルの制裁金を科した。1MDB スキャンダルの債権取引は Goldman Sachs International のもとで行われたものの、アジアにおける GS のコンプライアンス&コントロール・ハブである GS Asia が、1 MDB の債権の組成・承認・執行・販売プロセスに多大な関与をしたと判断されたことなどが制裁の大きな要因となっている。多くの外国金融機関にとって、ASPAC のハブである香港は、上記の例が示すように、香港に所在する機関のみならず地域全体からも重大な

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

AML/CFT リスクにさらされている。

香港政府は、JMLIT が最初の PPP の一つとして設立された後、シンガポール政府との議論と並行して、市場の利害関係者とのこうしたリスクや傾向に対する認識を高める必要性を認識した。HKPF、HKMA、香港銀行協会、および選出された銀行が FMLIT を開発、2017 年にローンチした。英国の JMLIT と同様に、FMLIT は、香港の既存の規制制度内で許容される事項の対応を優先して立ち上げられたため、結果として、情報共有の範囲は ML の手口傾向と方法論の共有に限定された。一方で、英国と香港の規制枠組みの大きな相違点は、香港の規制枠組みでは、金融機関間の顧客・取引情報の共有については、いかなる場合においても許容されていないことである。FMLIT にはそのような情報共有のための仕組み(英国では、JMLIT の Operations Group で特定の捜査についての情報共有を行うことが認められている。詳細については、英国の項目を参照)が含まれていない。

香港における AML/CFT 関連の情報共有を拡大し、民間の金融機関間による情報共有を促進しようとすることへの意思については情報が限られている。また、2019 年以降、香港に対する中国の直接的な政治的統制が強化されたことを含む多くの外的要因により、金融機関および香港の規制当局は、組織レベルでの安定を維持するために、OFAC による経済制裁や香港市場からの撤退といった緊急かつ重大な問題への対応に焦点を移すことを余儀なくされた。

2.4.3 スキームの枠組

(1) Strategic Group と(2) Operations Group の 2 つの組織で活動している。

(1) Strategic Group
FMLIT の頭脳として Strategic Group という組織が用意されている。各参加主体の代表者が構成員となり、FMLIT の戦略的な方向性や機能の仕方を決める存在。

(2) Operations Group
FMLIT のいわば実働部隊であり、香港警察が情報を求める個別の犯罪捜査対象案件等に関連する銀行が当局(HKPF、HKMA)と実際に集まるかたちで情報交換を行う。

HKPF は、まず参加メンバーのうち、当該捜査対象に関する情報を有する個別の銀行に捜査対象の特定の顧客の名前を示す。当該銀行は当該顧客と取引が行われていることを確認し、HKPF に報告する。さらに、HKPF の求めに応じて具体的な取引内容などを報告する。

2.4.4 スキームと DPP 関連規制との関係性

各銀行は HKPF とのみ直接連絡をとり、HKPF に共有した情報は他の参加メンバーである銀行とは共有されないため、特段の法的手当てはとられていない。また、犯罪捜査方針に関係する情報は、プライバシー保護法における例外規定に基づき共有されることになるが、例外規定の解釈が複数の司法当局者間で異なり得ることから、遵法上の不透明性が生じている。

2.4.5 最近の動向

金融機関および HKMA は、コンプライアンスの負担をさらに軽減し、実効性を高めるためのテクノロジーの活用、および地域における最大のライバルであるシンガポールに後れを取らないよう競争力を維持するために、

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

AML/CFT コンプライアンスの継続的な進展、特に、情報の効果的な共有に関して改めて関心を示している。

関連するイニシアティブの例として、香港銀行協会の AML 委員会の下で最近開始されたパイロット・プログラムがある。このイニシアティブは 2 年間議論されてきており、現在のパイロット期間中に香港の主要銀行 5 行が、法人の口座に関する情報共有への参加を求められた。この取り組みについてはまだ情報が公表されておらず、詳細な情報は現在限られている状態である。

2.5 シンガポール AML/CFT Industry Partnership (ACIP)

2.5.1 スキームの概要

2017 年 4 月に開始。従来はベストプラクティスペーパにつながるような、特定のテーマについての調査が中心であったが、個別捜査案件の支援のために個別事業者と捜査当局の間の情報交換も始めた。

共同議長は CAD(シンガポール警察)、MAS(シンガポール金融管理局)で、Steering Group メンバーとして民間金融機関 8 行(①DBS、②UOB、③OCBC、④Citi、⑤HSBC、⑥Standard Chartered、⑦UBS、⑧BNP Pariba)と ABS(シンガポール銀行協会)が参加している。

2.5.2 スキームの枠組

特定のテーマについての調査と個別捜査案件の支援のための情報交換に加えて、ACIP は、シンガポールの関係当局が優先的な対応が必要と考えている犯罪について、新たな手口等への気付きを促すための「アドバイザリー」(助言)の配信も行っている。さらに、ACIP に参加する金融機関は、彼らが金融界において重大なリスクが出現しつつあることを検知したときに、それを金融界全体に知らしめるための手段としてこの「アドバイザリー」の配信を ACIP の共同議長に対して提案することができる。

また、共同議長と Steering Group メンバーに加え、ノンバンク等の金融事業者、法律事務所、会計・監査法人、経営管理会社(Company service providers)などの民間事業者参加し、テーマに応じた複数のワーキンググループ(Expert Working Groups)が設置されている。

2.5.3 スキームと DPP 関連規制との関係性

本スキームにおいては、事業者間で、疑わしい取引情報や個別の顧客情報に関する情報共有は行われておらず、本スキームに関して、民民での情報共有に関する特段の法的な手当てはなされていない。

2.6 シンガポール Project COSMIC(for “Collaborative Sharing of ML/TF Information & Cases”)

2.6.1 スキームの概要

2021 年 10 月 1 日に発表された。COSMIC、「ML/TF 情報と事例の共同共有」は、重要なリスクの閾値を超える顧客や取引に関する情報を安全に共有するための金融機関向けデジタルプラットフォームである。MAS とシンガポールの主要商業銀行 6 行(DBS、OCBC、UOB、SCB、Citibank および HSBC)によって共同設立している。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2.6.2 スキームの制定経緯

ほとんどの国・地域で金融機関にとって共通の課題として挙げられている、顧客口座における異常な活動について、金融機関が互いに警告できないことが背景としてある。

シンガポール政府による KYC ユーティリティプロジェクトから得られた多くの教訓として下記がある。

- 複数の銀行にまたがる情報を統合する大規模な顧客データベースを構築したり、そのデータを処理、分析するデータベースを構築するのはサイバーセキュリティリスク等が高い
- 複数の銀行間で業務基準とリスク・アペタイトを調和させることは非常に困難であり、かつコストがかかる

このため、1 つの大きなトランザクションデータベースを構築するのではなく、解決すべき問題を焦点に当てて「KYC 中心の課題」から脱却し、銀行間の情報の非対称性につけ込む犯罪を阻止することが決定された。(詳細はスキームの枠組を参照)

2.6.3 スキームの枠組

提案された枠組みの下で、金融機関は COSMIC を通じて、(1) 依頼、(2) 提供、(3) 警告の 3 つの方法で他の金融機関とリスク情報を共有することができる。(COSMIC へのアクセスは、Web ベースのプラットフォームと自動情報交換(API)の両方で可能となっている。)

(1) 依頼(Request)

- 顧客が何らかのレッドフラグに該当する行動を示した場合、金融機関は、その活動に関連する当該顧客に関するリスク情報を他の金融機関に依頼することができる。
- Request メッセージでは、顧客が示した特定のレッドフラグに該当する行動についての疑いの可能性について明確にする必要がある。
- メッセージでは、観察されたレッドフラグと顧客の関連リスク情報を含め、依頼の状況を説明する必要がある。
- 金融機関は、その依頼元の金融機関の顧客の疑いを立証するまたは晴らすのに役立つ情報のみを求めることができる。
- 依頼先の金融機関は、リスク情報が ML/TF/PF のリスクの評価と決定を支援する可能性があると納得すれば、要求されたリスク情報を合理的な期間内に提供すべきである。
- 依頼先の金融機関はまた、依頼元から受領したリスク情報を使用して、自らの顧客の AML/CFT 評価を実施する。

(2) 提供(Provide)

- 顧客の異常な活動がより高い閾値を超え、顧客が不正活動に関与するリスクがより高い場合、金融機関は当該顧客の活動へのつながりがある他の金融機関に対し、顧客のリスク情報を積極的に提供しなければならない。
- 金融機関は、顧客の行動が関連する閾値を超えた場合、COSMIC 上の他の金融機関に Provide メッセージを送信する必要がある。Request メッセージと同様に、Provide メッセージでは、観察されたレッドフラグや顧客の関連リスク情報など、懸念事項の状況を説明する必要がある。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

- 金融機関は、Provide メッセージを受領した場合、受領した情報を考慮し、合理的な期間内に、自らの顧客の AML/CFT 評価を実施しなければならない。
- 必要であれば、Provide メッセージを受領した金融機関は、同じ金融機関または他の参加金融機関に対して、さらなる Request および/または追加の Provide メッセージを発行することもできる。

(3) 警告(Alert)

- 顧客の活動がより高いレッドフラグの閾値を示し、かつ、金融機関が顧客に対して STR を提出し、関係の終了を決定した場合、金融機関は、当該顧客について COSMIC の「ウォッチリスト」上でアラートを発出すべきである。
- 金融機関は、提出書類の中で、観察されたレッドフラグや顧客の関連リスク情報など、懸念事項の理由を説明する必要がある。
- COSMIC の参加金融機関は、潜在的な顧客または既存顧客が監視対象リストに含まれているかどうかを確認し、潜在的な顧客または既存顧客に関する AML/CFT 評価の一部としてリスク情報を活用すべきである。

(1)依頼、(2)提供、(3)警告、いずれも本スキームの当初の段階では、「任意」の取り扱いである。将来的には、(2)提供と(3)警告、ならびに(1)依頼を受けた金融機関からの回答については「必須」化(不遵守への罰則を伴う)したいという MAS の意向が示されている。

2.6.4 スキームと DPP 関連規制との関係性

COSMIC の法的枠組みとして、FSMA(Financial Services and Markets Bill)において、AML/CFT の目的に限定して、金融機関間でリスク情報を共有することとともに、プラットフォームから取得した情報の利用および秘密性に関する保護について規定する。この規定に沿った形での、COSMIC による民民間の情報共有に関して、DPP 規制や、金融機関の守秘義務に関して、金融機関は保護される枠組みが提案されている。

MAS はまた、COSMIC のすべての参加者に対し、COSMIC の情報が許可なく使用されたり、開示されたりしないようにするための強固な措置を実施することを要求する。MAS は、金融機関がこれらの要件を遵守しているかどうかを監督し、誤った金融機関に対しては措置を講じる。

以下の規制改正案により金融機関間の情報共有を可能としている。

Annex B　PROPOSED PROVISIONS ON PROPOSED FI-FI INFORMATION-SHARING PLATFORM FOR AML/CFT[6]

PART [X]　FINANCIAL INSTITUTIONS' INFORMATION SHARING PLATFORM

COSMIC の規制枠組みでは、共有される情報の種類、および情報共有が許可または義務付けられる状況が明確に規定されるよう提案されている。MAS は、COSMIC からの情報をリスクの監視に活用し、金融システムで運用されている不正なネットワークを検出し、これらの情報と分析結果を踏まえた金融システムの監督にタイムリーに活用する。

6 Proposed Provisions on Proposed FI-FI Information-Sharing Platform for AML/CFT, (mas.gov.sg), https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/1-Oct-2021-FI-FI-Information-Sharing-Platform-for-AMLCFT/Annex-B---Proposed-Provisions-for-FI-FI-Information-Sharing-Platform-for-AMLCFT.pdf

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2.6.5 最近の動向

MAS は COSMIC プラットフォームを 2023 年上半期に立ち上げる予定で、まず、商業銀行における 3 つの主要な金融犯罪リスク(ペーパーカンパニーの濫用、不正目的のための貿易金融の悪用、拡散金融)に焦点を当てる。COSMIC の開発に関与する 6 行が参加し、初期フェーズにおいては COSMIC 内で情報を共有することが認められる。MAS は、COSMIC の対象範囲を、より多くの金融機関や重点分野に順次拡大し、共有の一部の側面を義務化する予定である。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

3 我が国の今後の制度設計に関する考察

金融機関に課せられている疑わしい取引の届出義務は、一金融機関として収集可能な情報(当該金融機関が知り得る顧客とその取引)のみを対象として、そこから疑わしい「取引」を届けさせるという前提での法律要件ということができる。一方で金融システムを悪用しようとする勢力は、複数金融機関や法域をまたいでレイヤリングを敢行する実態が見られる。これまで見てきた海外事例は、現行の疑わしい取引の届出義務の範囲を超えた情報共有によって、従来十分できていなかった金融システムを悪用する手口の検知についての実効性を向上させようとする試みであると位置づけることができる。

このような観点から、本セクションでは、海外事例を、取り扱う情報等によって分類・整理し、これに基づいて我が国として同様のマネロン情報の共有制度を導入するにあたってのインプリケーションについて整理する。

3.1 海外事例の分類・整理

今回の調査で把握した、諸外国における情報共有制度を類型化し整理すると以下のとおり４つに分けられる。

タイプ	情報の種類	共有発生の契機	該当する海外事例	DPP とのコンフリクト
A	個別の顧客・取引に関する情報	Post-Reporting: 一金融機関から FIU への疑わしい取引の届出もしくは捜査当局からの照会[7]	シンガポール:ACIP	なし
			オーストラリア:Fintel Alliance	あり[8]
B		Post-Suspicious: 金融機関における疑わしいとの合理的な評価を契機とした情報共有	英:JMLIT シンガポール:COSMIC	なし
C		Pre-Suspicious: 通常の顧客・取引に関する情報共有	オランダ:TMNL	あり
D	リスク・犯罪の動向・手口	FIU での分析や基礎情報や、金融機関から収集した情報を踏まえたフィードバックやアラート、手口の共有	英:JMLIT オーストラリア:Fintel Alliance 香港:FMLIT シンガポール:ACIP	なし

以下、個別の顧客・取引に関する情報(タイプ A, B, C)、リスク・犯罪の動向手口(タイプ D)に分けてマネロン情報の共有制度導入に関して考察する。

7 他のタイプと異なり、タイプ A は、あくまで当局が複数金融機関からの情報を収集するものであり、参加した金融機関同士の横の情報共有はない。

8 オーストラリアの Fintel Alliance は、便宜上タイプ A に分類したが、本来はタイプ B の情報共有を企図したものである。ただし、情報共有のための法的枠組みがないことから、苦肉の策として金融機関から FIU への出向という形での情報共有を行っている。この点で、情報保護義務違反の責任を免れるための特段の法的な手当てはなされておらず、DPP とのコンフリクトは「あり」と整理した。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

3.2 個別の顧客・取引に関する情報共有についての考察

我が国において、個別の顧客・取引に関するマネロン情報の共有制度を導入するにあたっては、タイプ B の Post-Suspicious を対象とした枠組みが最も参考になるものと思われる。

まず、タイプ A については、金融機関同士の横の情報共有を促すものではない。金融機関にとって得るものは少なく、本来の目的(現行の疑わしい取引の届出義務の範囲を超えた情報共有によって、金融システムを悪用する手口の検知についての実効性を向上させる)達成の観点では、タイプ B に劣後するものと思料する。

次にタイプ B については、タイプ A と同様、金融機関に DPP に関連するコンフリクトが発生しないようなセーフハーバーを制度上担保することを前提として、導入効果、金融機関にとってのメリット等を勘案すると、最も実現を推進すべき形ではないかと思われる。

タイプ A が、主に一金融機関からの疑わしい取引の届出を端緒とした Post-Reporting を前提としているのに比べて、タイプ B は、金融機関が疑わしい取引として届け出るかの判断をより合理的に行うための調査・分析を共有する場を提供する、すなわち金融機関が「疑わしい」可能性があると合理的に評価したことを契機とした情報共有(Post-Suspicious)であることが大きく異なる。これによって従来は情報不足により届け出ないと判断した(FIU の立場からは届け出ることが断念された)取引がより幅広に情報共有や調査の俎上に乗り、疑わしい取引として届け出られる効果が期待される。金融機関にとっても、この枠組み活用によって、

① 疑わしい取引判断に資する情報が取得できること
② より広い見地からの情報分析・判断が行いやすくなり、従来検知できていなかった複数金融機関をまたぐレイヤリング手口等も補足できること
③ このような取組みを通して金融機関同士の情報共有のメリットが体感でき、金融犯罪撲滅に向けたコミュニティ形成やノウハウ高度化が図れること等のメリットが享受できること

が期待できる。

一方で海外導入事例においては、この制度への参加に対して、金融機関側の負担に関する懸念や制度参加義務に対する不遵守があることも事実である。ただし、日本の金融機関においては、セーフハーバーがない中での、金融機関同士での疑わしい取引届出に関する情報交換・共有は、依頼を受けた金融機関側のリソース制約に加えて、顧客に対する守秘義務とのコンフリクトから情報提供を躊躇するケースが少なからずあり、依頼する金融機関から見ると、中々協力を得られにくい、依頼先金融機関や担当によっても対応スタンスが異なる等、金融機関同士で協力して金融犯罪を検知するというインセンティブが醸成しにくく、現行制度下での調査自体、既に相当の制約や負担になっているという現状を改めて認識する必要がある。このような現状との比較考量において、タイプ B の制度導入を検討すべきであり、たとえば、

① セーフハーバーが確保されること(現行は確保されておらず、金融機関や担当者のスタンスや意識に大きく左右される)
② 依頼を受けた金融機関側での一定の協力体制整備が義務付けられること(現状、一部の意識の高い有識者による、自金融機関でさえ理解を得られにくい中での自発的な取り組みに大きく依拠している)

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

③ これによって一定の負担を金融機関に強いるものではあるが、疑わしい取引をより広く検知すること(上記制約から、現行取組では自身の金融機関が収集可能な情報を超えたスコープでの疑わしい取引検知には限界がある)
④ またその土台としてのコミュニティ形成やノウハウ高度化が図れること(②で述べた有識者は未だ孤立感を持ちつつ、業務を行っている現状)

等の効果が期待される。

Pre-Suspicious を対象としたタイプ C の取組については、最も野心的で、導入効果は大きいと想定される。すなわち、タイプ B は、一金融機関が一定基準で疑わしい可能性があると判断した時点(Post-Suspicious)が契機となることから、そもそもそれをかいくぐる False Negative 取引は補足できないという限界がある。タイプ C は、通常の取引を幅広に収集し、ネットワーク分析等によって、一金融機関では補足できない異常な取引(統計的なアウトライヤー)を特定しようとする試みである。

しかしながらオランダの事例のとおり、この取組みについては、DPP とのコンフリクトを解消することは容易ではなく、早期実現は困難と言わざるを得ない。まずはタイプ B の導入を視野に、海外動向を見ながらタイプ C 導入についてのフィージビリティを中長期的に検討するのが現実的である。

タイプ C の導入を検討するうえでは、オランダと日本は以下のような DPP 制度上の相違があり、グローバルな観点から我が国の制度上の特徴を認識しておく必要がある。

わが国の個人情報保護に係る法規制においては、個人情報の利用目的の拡大や第三者提供に係る規制の適用除外ケースが以下のように限定列挙されており、AML/CFT や金融犯罪捜査目的での個人情報の第三者提供等は、この中の「①法令に基づく場合」に該当するとされている。

① 法令に基づく場合
② 人の生命・身体・財産の保護のために必要があり本人同意を得ることが困難な場合
③ 公衆衛生の向上または児童の健全な育成の推進のために特に必要があり本人同意を得ることが困難な場合
④ 国の機関・地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合で本人同意を得ることが当該事務の遂行に支障を及ぼすおそれがあるとき

現行の法規上は、AML/CFT や金融犯罪捜査目的での個人情報の第三者提供等は「②人の財産保護」に該当するものではなく「①法令に基づく場合」に該当するとされている。しかし、現時点でタイプ C の根拠となる法令は存在しないため、その導入を進めるためには今後新たな法令上の規定が必要になると考えられる。また、現在「①法令に基づく場合」として整理している取り扱いについても、今後 AML/CFT を目的とする情報共有の取組みに広く理解・協力を得ていくためには、この適用除外に該当する旨をガイドライン等で明文化しておくことが望ましい。

一方で、オランダを含む EU 諸国においては、GDPR 第 6 条 1 項によれば、個人情報取扱が認められる法的根拠は以下のとおりである。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

(a) データ主体が、一つまたは複数の特定の目的のために、自己の個人データの取扱いに同意を与えた場合
(b) データ主体が当事者となっている契約の履行のために取扱いが必要な場合、または契約の締結前のデータ主体の求めに応じて手続を履践するために取扱いが必要な場合
(c) 管理者が従うべき法的義務を遵守するために取扱いが必要な場合
(d) データ主体または他の自然人の重大な利益を保護するために取扱いが必要な場合
(e) 公共の利益または管理者に与えられた公的権限の行使のために行われる業務の遂行において取扱いが必要な場合
(f) 管理者または第三者によって追求される正当な利益のために取扱いが必要な場合。ただし、データ主体の、特に子どもがデータ主体である場合の個人データの保護を求めている基本的権利および自由が、当該利益に優先する場合を除く。

GDPR は、上記(f)にあるように、事業者がデータ主体のデータ保護の要求・必要性よりも、「管理者または第三者によって追及される正当な利益」を優先する必要性が十分大きいと疎明できるならば、第三者提供を含むデータ処理が認められ得る法制度となっている。すなわち、日本の個人情報保護法のように、第三者提供禁止を原則として規定したうえで例外規定を設ける、という形式ではなく、比較考量によりデータ処理の法的根拠を規定できる余地が残されている。

PPP のような AML/CFT 目的での情報共有について、欧州委員会は、2020 年 5 月に「『EU における ML/TF 阻止のための包括的な政策に関する行動計画書』についての欧州委員会からのコミュニケーション」[9]を公表し、2020 年 7 月には、EU における個人情報保護の監督当局である欧州データ保護観察官(EDPS: European Data Protection Supervisor)が意見書(「欧州委員会による『EU における ML/TF 阻止のための包括的な政策に関する行動計画書』についての意見書」)[10]を公表している。この意見書では、GDPR やそれに準ずる Regulation 2018/1725 (欧州連合の主な機関・団体におけるデータ保護規則)等に基づき、以下の 3 つの原則を守るべきことを主張している。

① The Principle of Proportionality
EDPS は、ML/TF と闘うための実効性ある AML/CFT 制度の適用は重要であり、欧州 AML 指令の現状および今後の改定の方向性を歓迎し、DPP との適切なバランスを確立すべきであると述べている。

② Data Protection-by-design/default Principle
データ処理のシステムを設計し、このシステムをデータ処理に利用する場合、データ管理者は、データ主体の権利を保護し、EU データ保護規則の遵守を確保するための技術的・組織的措置を予め講じなければならない、また、初期設定で、データ処理行為が処理目的に必要な最小限に限定されるようにする義務がある。

③ Accountability Principle

9 Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, European Commission, https://www.politico.eu/wp-content/uploads/2020/05/Communication-on-Action-Plan.pdf
10 Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, European Data Protection Supervisor, https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

データ管理者は、(先行する原則への)コンプライアンスに責任を負い、コンプライアンスを証明することができなければならない。

DPP 規制要件と AML/CFT 規制要件の調和はオランダをはじめとする欧州においても容易ではないが、The Principle of Proportionality に基づいて関連当局間の建設的でオープンな対話がなされ、Data Protection-by-design/default Principle および Accountability Principle に基づいた PPP 取組主体による基準の明確化と説明責任の確保が求められるという点が、マネロン情報共有について、個人情報保護法令の適用除外と整理している我が国と異なる。

3.3 リスク・犯罪の動向・手口に関する情報共有についての考察

リスク・犯罪の動向・手口に関する情報共有(タイプ D)は、特定の顧客あるいは当該顧客が特定される可能性のある個別の取引情報を含まないという点で、DPP とのコンフリクトは発生せず、比較的取組みやすいということができる。

実際、このような動向・手口に関する情報の共有は、我が国においても、「犯罪収益移転危険度調査書」や「犯罪収益移転防止に関する年次報告書」による情報開示等、FIU や金融監督当局からの情報発信、あるいは金融業界団体での金融機関同士の情報共有等によってある程度行われている。

海外においてはこのような取組みが、個別の顧客・取引に関する情報(タイプ A, B, C)とあわせて効果的に実施されている事例も見られる。たとえば英:JMLIT では、個別の顧客・取引情報共有を担う Operations Groups と、動向・手口情報共有を担う Expert Working Groups 双方を包含するような形で組織化されている。タイプ A, B, C の取組に参画した金融機関へのフィードバックや、より広く金融機関全般に対する参画意識醸成といった効果も期待される。すなわちタイプ D 単独での施策ではなく、タイプ A, B または C の枠組みを設定したうえでの両者の相乗効果を狙う施策が効果的であるということができる。

既述のとおり、疑わしい取引の届出制度自体が、一金融機関として収集可能な情報を対象として、そこから疑わしい「取引」を届けさせるという前提での法律要件であることから、タイプ D の情報共有は、いかに個別の届出の網羅性・精度を向上させるかが重要であるため、今後は以下の観点での情報共有を検討する必要があると思料する。

- 匿名化した個別事案ではなく、より分析を深めた手口類型情報やその傾向分析
  個別取引、あるいは個別事案としてではなく、全体の動向・傾向として特徴的な手口を特定することに焦点を当てた分析を深め、直近の動向を遅滞なく幅広に情報発信する。個別事案よりもより一般化・特徴化した手口情報の方が金融機関にとって参考になること、特定の金融機関で悪用され、成功した手口は次々と別金融機関に波及する傾向がある(裏を返すと他金融機関での手口情報共有が十分ではない無防備な金融機関が狙われる)ことから、このような手口をいち早くとらえ情報還元することが重要である。つまり年次報告書での事例紹介といった静態的な情報還元ではなく、現場で発生している動向をいち早く伝えるインテリジェンス機能を強化し動的な情報発信を行う体制を整えること
- データアナリティクスを活用した定量情報
  上記のような情報共有に当っては、FIU に収集された情報等の一層の活用が重要であり、デジタル化の推進と当該デジタル化をベースとしたデータアナリティクスを活用した傾向分析(ネットワーク分析を基にしたクラ

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

スタリング等)を適用することで、個人情報を特定しない形での、より効果的な手口情報を定量的に提供できる余地が大いにある。こういった定量情報によって、金融機関にとっては、それぞれの取引モニタリングシステムにおけるシナリオや閾値設定への有用なフィードバックとなり得る。

本報告書は、金融庁の委託により有限責任 あずさ監査法人が実施した調査結果を取りまとめたものです。私たちは、調査時点で入手した情報に基づき本報告書を適時に取りまとめるよう努めておりますが、本調査報告書の内容は、本調査の対象に含まれない特定の個人や組織が置かれている状況に対応するものとは限らず、また、情報を受け取った時点およびそれ以降において、その情報の正確性や完全性を保証するものではありません。この調査報告書での KPMG の見解が常に規制当局の見解と一致することは保証できず、また、本調査報告書は法的見解を提供する、または保証意見を表明するものではございません。本報告書は委託者である金融庁に対してのみ提出したものであり、本報告書を閲覧あるいは本報告書のコピーを入手閲覧した第三者の本報告書の利用に対して、有限責任 あずさ監査法人は直接ないしは間接の責任を負うものではありません。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.