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

令和４年 12 月 23 日

有限責任 あずさ監査法人

KPMG

目次

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、第三分冊であり、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のうち、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についてとりまとめたものである。リモートギャンブル事業者[1]を監督するためにオランダで使用されている Control Data Safe (CDB: Controle Databank)と、メキシコの金融規制当局の一つである National Banking and Securities Commission (CNBV: Comisión Nacional Bancaria y de Valores)による SupTech の取組みを調査対象とした。

[1] 本報告書において、ギャンブル事業者とは、ギャンブルサービスを提供する事業者全般を指す。リモートギャンブル事業者とは、ギャンブル事業者のうち、プレーヤーが物理的な施設においてではなく、リモートコミュニケーションツール（インターネット、電話、テレビ、ラジオ、他のテクノロジー等）を使ってプレーするギャンブルサービスを提供する事業者を指す。

2 オランダ

本セクションでは、リモートギャンブル事業者を監督するためにオランダで使用されている、事業者とオランダの規制当局間でデータを交換するための安全な手段である Control Data Safe (Controle Databank: CDB) について KPMG オランダが以下の調査を行い、詳述している。

I. オランダの全般的な規制状況における CDB 導入の背景
II. CDB の概要とステークホルダーに対する位置づけ
III. CDB の技術面の詳細
IV. CDB の最新の動向と将来像
V. 認識されている CDB の効果・課題(業界の見解)
VI. 日本への示唆

CDB の開発と位置づけに関するデスクトップリサーチを実施した。

デスクトップ調査には、法規制関連資料、規制当局からのガイダンス、監督当局からのガイドラインと要件、および他の情報源からの資料が含まれている(Appendix 参照)。関連資料への参照は、脚注に示した。

2.1 CDB について

2021 年 4 月 1 日、オランダギャンブル法(Wet op de kansspelen: Wok)の修正によりリモートギャンブルが認可され、これに基づき、リモートギャンブルに関する政府令 (Besluit kansspelen op afstand) が新たに定められ CDB が導入された。

これらの改正以前には、オランダのリモートギャンブラーは、AML/CFT 対策を含む事項に関する監督・管理が存在しない状況で、オランダの規制当局の監督を受けていない、違法な外国リモートギャンブル事業者を利用していた。改正によって、ライセンス制度が、オランダで合法的なリモートギャンブルサービスの提供を希望する事業者に適用され、ライセンスは 2021 年 10 月 1 日から付与された。

2.1.1 目的と CDB の導入について

CDB とは、事業者とオランダの規制当局間でデータを交換するための安全な手段であり、新しいライセンス制度下における、リモートギャンブル事業者への要件の一つである。すなわち、オランダにおいて認可されている全てのリモートギャンブル事業者は、CDB を用意する必要がある。

リモートギャンブルに関する政府令に基づき、リモートギャンブル事業者は、自身のプラットフォームで発生したイベントのデータを、CDB を通して提供する義務がある。CDB に提供されるデータは、ギャンブルアカウントの取引、アカウントの変更事項、およびプレーヤーの本人確認と検証に関連するものである。取引に関連するデータの例としては、取引のタイプ(例:預金、支払い、賞金、ボーナス)、日付と時刻のスタンプ、使用された支払手段のタイプ(例:クレジットカードや口座引き落とし)、引き落とし口座の口座番号、取引の金額などが挙げられる。CDB は、プレーヤーがリモートギャンブル事業者のプラットフォーム上で実行した様々なアクションの簡易ログととらえることができる。これらのアクションの例としては、プレー資金の預け入れまたは引き出し、オンラインポーカーのプレーなどが含まれ

る。

データは、プレーヤーのプライバシーを保護するために、CDB に疑似匿名で記録される。リモートギャンブル事業者は、プレーヤーに仮名を割り当て、これにより、CDB 内の仮名化されたプレーヤーと、事業者自身のソース・システム内のプレーヤー識別子との結合が可能になる。そのため、1 人のプレーヤーが、異なるリモートギャンブル事業者において異なる仮名を持つことになる。

リモートギャンブル事業者によるデータ操作のリスクを最小限に抑えるために、データをほぼリアルタイムで CDB に格納する必要がある。CDB に格納する必要があるデータの詳細については、技術仕様[2]に記載されており、第 4 章で解説する。

CDB は、オランダのギャンブル当局(Kansspelautoriteit: KSA)および税務当局(De Belastingdienst)を含む特定の監督機関で利用可能である。これにより、これらの監督機関は、リモートギャンブル事業者が、マネー・ローンダリングおよびテロ資金供与防止法(Wet ter voorkoming van witwassen en financieren van terrorisme, hereinafter: Wwft)、1977 年制裁法、賭博税法などの関連法規を遵守しているかどうかを監視することができる。

CDB の配置の概要は図 1 の通り。

図 1: CDB の配置の概要

CDB は、その設計および利用法について KSA が規定する要件のすべてを満たさなければならない(2.3 で参照)。CDB の技術要件は、以下のような内外の関連基準や実務を参考としている[3]。

- 認可ギャンブル事業において同様のデータ保存システムを求めている欧州各国基準(デンマークやフランスなど。セクション 2.1.4.参照)。
- システム監査または財務諸表監査のベスト・プラクティス
- オランダ政府によって設定されたオープンスタンダード

[2] Regeling kansspelen op afstand (Regulation on Remote Gambling), Overheid.nl (Dutch Government Website), https://wetten.overheid.nl/BWBR0044767/2021-10-01

[3] Specifications for the remote gambling data safe (the CDB), Kansspelautoriteit (Netherlands' Gambling Comittiee), https://kansspelautoriteit.nl/publish/library/30/cdb_specification_version_1_00_authorised_for_public_release_17_november_2020.pdf

・ ISO 27001 などの国際規格

2.1.2 法的根拠

法務省は(リモートを含む)ギャンブルに関するすべての法律を管轄する立法機関である。CDB の法的根拠は、様々な規制および下位法令にある。法令ごとの概要と要点は下記表の通り。

法律名	重要なポイント
一般行政法[4]	一般行政法は、オランダにおけるより統一的な一般行政の枠組みを確保するため、オランダのすべての行政機関の手続や規則を定めている。下位法で指針が定められていない場合、KSA などの監督当局はこの法律を参照することができる。
オランダギャンブル法(Wok)[5]	オランダギャンブル法は、賭博一般に関する、オランダで最上位の法令になり、一般規定、定義、および一連の規則を提供している。これには、リモートアクティビティを提供する事業者を含む、すべてのギャンブル事業者に対するライセンス要件が含まれる。
リモートギャンブルに関する政令[6]	リモートギャンブルに関する政令は、リモートギャンブルに関するオランダギャンブル法の一般規定をさらに詳しく規定している。この法令は、広告、求人、依存症予防の規則を定めている。さらに、この法令は、ライセンス保有者のギャンブル・システム、マネー・ローンダリングと八百長の防止、登録に関する要件を定めている。また、1 つのセクションでは CDB の仕様について詳細に記載されている。
リモートギャンブルに関する省令[7]	リモートギャンブルに関する省令は、オランダギャンブル法とリモートギャンブルに関する政令を詳細に定めたものである。この規制には、データの整合性や CDB のロケーション要件など、最低レベルの法的要件が定められている。
アンチマネー・ローンダリングおよびテロ資金供与防止法(Wwft)[8]	Wwft の目的は、金融システムがマネー・ローンダリングやテロ資金調達に使われるのを防ぐことであり、ギャンブル部門も対象に含む。このため、ギャンブル法では Wwft に関して様々な形で参照している。 KSA はマネー・ローンダリングを検出する法的な義務はないが、認可を受けた事業者が八百長やマネー・ローンダリングを防ぐために十分な対策を講じているかどうかをチェックする。ギャンブル事業者にとって重要なポイントは、適切なリスク管理を実施する、顧客デューデリジェンス(CDD) を実施する、資金情報機関(FIU) に異常な取引を報告する、従業員を十分に訓練する、機密データに関する保持義務を果たすといったことである。
1977 年制裁法 (制裁法) [9]	1977 年制裁法は、国際的な制裁を実施するための国内および国際的な規則を策定するための基礎である。KSA は、ギャンブル事業者が制裁法に定められた規則を十分に遵守しているかどうかを評価し、事業者は継続して遵守していない場合にはライセンスを失うリスクがある。

上記の表に概説されている規制および下位法令に続き、KSA はガイドラインとなる文書を起草した。この文書は下記の表に示すように、CDB の仕様、およびデータ転送要件やデータ・モデルに関するガイダンスなどの技術要件

[4] Algemene wet bestuursrecht (General Administrative Law), Overheid.nl (Dutch Government Website), https://wetten.overheid.nl/BWBR0005537/2022-08-02v
[5] Wet op de kansspelen(Regulation on Gambling), Overheid.nl (Dutch Government Website), https://wetten.overheid.nl/BWBR0002469/2022-01-01
[6] Besluit kansspelen op afstand (Decree to Remote Gambling), Overheid.nl (Dutch Government Website), https://wetten.overheid.nl/BWBR0044773/2022-07-15v
[7] Regeling kansspelen op afstand (Regulation on Remote Gambling), Overheid.nl (Dutch Government Website), https://wetten.overheid.nl/BWBR0044767/2021-10-01
[8] Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) (Anti-Money Laundering and Terrorist Financing Act), Overheid.nl (Dutch Government Website), https://wetten.overheid.nl/BWBR0024282/2022-07-07
[9] Sanctiewet 1977 (Sanctions Act 1977), Overheid.nl (Dutch Government Website), https://wetten.overheid.nl/BWBR0003296/2020-05-21

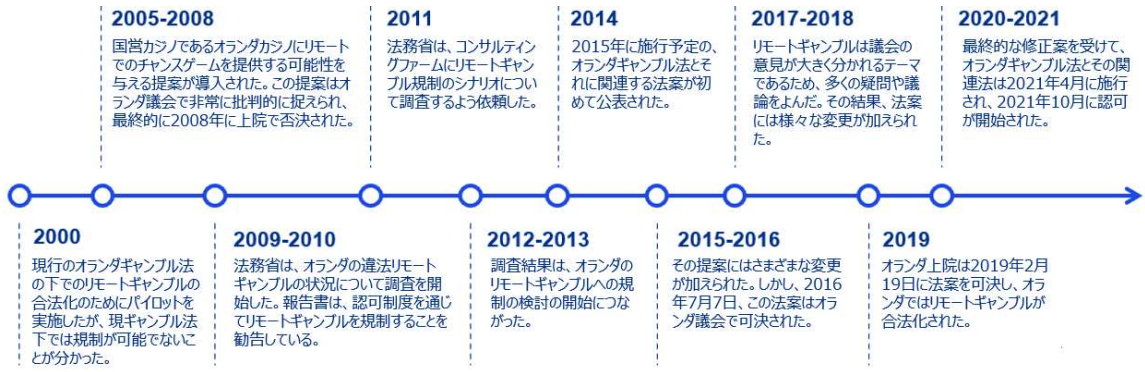
が含まれている。

法律名	重要なポイント
KSA による Wwft ガイドライン[10]	ギャンブル事業者が Wwft に準拠する方法について十分なガイダンスを提供するために、KSA は Wwft ガイドラインを策定した。本文書は、とりわけリスク管理、顧客調査、異常取引の報告に関するガイダンスを提供している。
リモートギャンブルのための CDB の仕様[11]	CDB に関するリモートギャンブル事業者の具体的な要件と背景について説明している。また、リモートギャンブル事業者に対して、CDB の基盤、データストレージおよびアクセス管理、および CDB に関するその他の様々な技術要件に関するガイダンスを提供している。
リモートギャンブルのための CDB のデータ・モデル[12]	CDB で準拠すべきデータ・モデルの特定のための要件の概要を説明している。また、データ転送に関するガイダンスと、必須のデータ・モデルやその他の特定の要件をリモートギャンブル事業者に提供している。

2.1.3 制度導入のタイムライン

2009 年まで、オランダの違法リモートギャンブルの実態と問題についての情報はほとんどなかった。オランダにおける違法リモートギャンブルに関する最初の広範囲な調査は、2009 年にギャンブル法および規制を担当する大臣(Minister for Legal Protection)によって要請され調査が実施された。この調査の結果を踏まえ、オランダにおけるリモートギャンブルの合法化のための規制プロセスが開始された。しかし、リモートギャンブルの合法化をめぐる規制は、調査開始から 10 年以上経過した 2021 年 4 月 1 日に施行されており、図 2 は、リモートギャンブルの合法化をめぐる制度導入の経緯を可視化したものである。

CDB は、2021 年 4 月 1 日に施行された立法措置で導入されたが、同日には直ちに機能しなかった。これは、KSA が要求されたリモートギャンブル事業者のライセンスを承認するための審査期間を必要としたためである。このため、リモートギャンブル事業者の最初のライセンスが交付された 2021 年 10 月 1 日に初めて CDB が稼働した。



[10] Leidraad Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) (Guidance on the Prevention of Money Laundering and Terrorist Financing Act (Wwft)), , Kansspelautoriteit (Netherlands' Gambling Comittiee), https://kansspelautoriteit.nl/publish/library/24/leidraad_wwft_1.pdf

[11] Specifications for the CDB on Specifications for the remote gambling data safe (the CDB), Kansspelautoriteit (Netherlands' Gambling Comittiee), https://kansspelautoriteit.nl/publish/library/30/cdb_specification_version_1_00_authorised_for_public_release_17_november_2020.pdf

[12] Data model for the CDB on Specifications for the remote gambling data safe (the CDB), Kansspelautoriteit (Netherlands' Gambling Comittiee), https://kansspelautoriteit.nl/publish/library/30/cdb_specification_version_1_00_authorised_for_public_release_17_november_2020.pdf

図 2: 制度導入の経緯

リモートギャンブルの合法化のための規制プロセスは、次の 3 つのセクション(2.1.4～2.1.6)で説明する 3 つのフェーズに分けられる。

1) 立法および可能性のある選択肢に関する勧告 (2000~2011 年)

2) リモートギャンブルの合法化に向けた手続きの開始 (2012~2015 年)

3) オランダ議会での最終決定、承認プロセスと導入 (2016~2021 年)

2.1.4 立法および可能性のある選択肢に関する勧告(2000~2011 年)

リモートギャンブルの合法化の動きは 2000 年頃に始まった。この時期に実施された、いくつかの調査によると、オランダには規制のない大規模なオンラインギャンブル市場が存在した。2000 年には、既存のギャンブル法のもとで、リモートギャンブルを合法化するためのパイロットプログラムが試みられた。しかしながら、最終的には、現行のギャンブル法に基づいてこのパイロットプログラムを実施することは不可能だと考えられた。

2005 年には、国有企業である Holland Casino に、ランドベースのカジノ[13]の提供からリモートでのギャンブル提供に拡大するオプションを提供する提案が起草された。この提案は、リモートでのギャンブルを合法化すればプレーヤー人口が増え、ギャンブル依存症患者が増えるとの懸念から、オランダ議会とオランダ上院の双方から道徳的倫理の観点で強く批判され、この提案は最終的に 2008 年に上院で否決された。

2014 年に発表された現在のライセンス制度の基となった提案には、ギャンブル法、賭博税法、およびその他のリモートギャンブルの機関に関連するいくつかの立法条項の修正が含まれていた。

これらの提案は主に、リモートギャンブリングのオンライン市場の外部アドバイザーによって行われた研究[14]からのインプットに基づいていた。

この研究の報告書は、賭博税、法執行、監督、ライセンス制度に関する欧州のギャンブル市場の動向を詳述し、規制当局と事業者の両者が、ギャンブル監督に関してどのような技術的、運用的措置が効果的で現実的かについての合意に向けた方向性を概説している。また、イタリアは試行錯誤を通じて、比較的成功した監督モデルを構築したと述べられ、デンマークやスペインなど他の国もイタリアをそれぞれの国での枠組み検討の出発点にしている。そのため、技術・運用条件に関する厳格性と現実性とのバランスを各国がお互いから学んでいると指摘している。また、オランダ市場の規模が限られていることを考えると、海外の要件に従うのが賢明であるとの意見を示している。

オランダは、欧州においては、リモートギャンブル規制の後発国の一つであったため、他のヨーロッパ諸国からのベストプラクティスを活用した。特に、どのような手段や権限を監督当局が有するべきなのか、ゲーミングシステムにどのような要件を課すべきなのか、どのような責任が監督当局に委任されるべきなのかといったことを他国の例から学んだ。

なお、リモートギャンブルに対する規制は欧州連合内で共通認識が形成されておらず、法的根拠や歴史的背景

---

13 物理的な施設において行うカジノを指す。

14 Boston Consulting Group(2011), Onderzoek Online Markt Kansspelen Eindrapport (Market Research on Remote Gambling), https://www.tweedekamer.nl/downloads/document?id=1b4e2855-209e-4d4e-8f94-d764822bb740

が国によって異なるため、欧州域内の複数の国をまたがる共同 CDB といったものの設置は現時点では考えられてはいない。

2.1.4.1 CDB についての検討事項

様々な国が実装してきた要件の 1 つとして、監督当局によってアクセス可能なデータストレージ内に、ギャンブル事業者の取引やゲームに関連するデータのコピーを持つということがある。外部アドバイザーの報告書によると、このことは問題のあるギャンブラーを特定し、指導し、問題ある行為を抑制するための効果的なツールであることや、苦情が発生した場合にプレーヤーの取引履歴に関する情報を提供するものであると認識されている。報告書は、マネー・ローンダリングなどの違法行為の防止をライセンス制度の決定の際に考慮すべきだと強調している。しかし、報告書は、これらのデータストレージがマネー・ローンダリング防止対策の監督を改善する可能性についてまでは特定していない。

また、この報告書では、このような当局がアクセス可能なデータストレージの 3 つのバージョンを次の表のように示している[15]。当局がアクセス可能なデータストレージに関する法規制を設計する際には、様々な考慮事項がある。これらの考慮事項は、特に、情報をリアルタイムで追跡する必要があるかどうか、どのデータを保存する必要があるか、データストレージの場所はどこかなどである。さらに、この報告書では、ギャンブル事業者にとって特定の技術的要件の実装はコストがかかるとしている。報告書によると、オランダにサーバを物理的に設置し、リアルタイムでのモニタリングを可能にするなどの要件を追加すると、ギャンブル事業者の IT コストが少なくとも 10%増加すると述べている。

選択肢	1)「金庫(Vault)」システム	2)「安全」システム	3)「バックアップ」システム
	必要なデータは、監督当局によってホストされる中央サーバに供給される。	監督当局は、ギャンブル事業者がホストするサーバに *(ほぼ)* リアルタイムでアクセスし、そのサーバ上でデータの抽出できる。	ギャンブル事業者は、システムデータの完全なログをローカルまたは他の協力 *EU* 加盟国所在のサーバに保存する。
長所	・すべての取引のリアルタイム検証が可能 ・データ改ざんの可能性なし	・データは世界中のどこにでも保存可能 ・監督当局者と事業者の両方にとってコスト・パフォーマンスに優れたソリューション	・監督当局と事業者の両方にとってコスト・パフォーマンスに優れたソリューション
短所	・サーバに問題が発生した場合のサービスの中断 ・監督当局向けの非常に広範な IT プロジェクト ・ギャンブル事業者に多大な IT 投資が必要	・データを物理的に監視出来ない ・データ改ざんリスク	・新規ライセンス所有者への追加投資が必要になる可能性
リスク低減措置		・改ざん防止のシステムとする-第三者が、監督当局のために検査および/または監査を行う	

15 Boston Consulting Group(2011), Onderzoek Online Markt Kansspelen Eindrapport (Market Research on Remote Gambling), https://www.tweedekamer.nl/downloads/document?id=1b4e2855-209e-4d4e-8f94-d764822bb740

こうした当局がアクセス可能なデータストレージの導入は、オランダの規制当局にとって大きな関心事だった。KSA向けのリモートギャンブルのより広範な監督に関する諮問報告書においても、KSA のためのそのようなシステム構築に関して概説した[16]。同報告書は、KSA に対し、オランダでこのようなデータストレージの導入を成功させるために満たさなければならない具体的な要件を策定するよう勧告している。また、これらの要件は、KSA がこのデータストレージへのアクセスをどのように想定しているかも示す必要があるとしている。報告書は、KSA がこうしたデータストレージを利用する可能性についてさらに調査し、ギャンブル業界の他の規制機関と連携するよう勧告している。

当局がアクセス可能なデータストレージの可能性に関するさらなる調査が、法務省によって使命付けされた Gamble Compliance という調査チームによる、ギャンブルの近代化に関するフォローアップ報告書において行われた[17]。この報告書には、EU 加盟国によるこのようなデータストレージの使用に関する調査が含まれている。

12 ページ記載の表に示す最初のオプション、すべてのデータがリアルタイムで実行される、監督者にとっての金庫室(”Vault”)のような仕組みは、イタリアで実装されている。デンマークとフランスの監督当局は、データのコピーを保存する特別なサーバという第 2 のオプションを実装しており、これには監督者が安全に(”Safe”)アクセスできる。

ギャンブルの近代化に関する報告書では、フランスのギャンブル事業者は「.fr」ドメインでのサーバをフランスに置かなければならないと述べている。これには、プレーヤーのデータとフランスの消費者が関わるすべての取引の調査を可能にするために必要なインフラを整備することが含まれる。ただし、本社またはプライマリサーバーがフランスにある必要はない。

フランスのギャンブル事業者は、この データベースにリアルタイムでデータを転送しなければならない。プレーヤーとギャンブル事業者間のデータ交換は、このサーバを通過する必要があり、フランスのギャンブル当局は常にこのデータベースにアクセスできる状態であることが必要である。

デンマーク当局は、ギャンブル事業者に対して、ギャンブル当局がアクセスする必要がある固有の「データウェアハウス」(SAFE) を作成することを義務付けている。ライセンス所有者は、ギャンブルデータを SAFE に保存する必要がある。

さらに、デンマークのギャンブル当局は「TamperToken」を導入することで、SAFE に関する公開データが改ざんされるリスクを低減した。当局は、「TamperToken の目的は、標準レコードなどのデータがライセンス所有者側で SAFE に保存されている間も変更されないようにすることである。」と述べている[18]。「TamperToken」は、Message Authentication Code (MAC) の計算に使用される鍵 (トークン) を作成する。MAC は、メッセージの性質と発信元、およびメッセージに含まれるデータの正当性を検証するために使用される。デンマークのギャンブル当局は、SAFE に提出された記録のバッチごとにこれらの MAC を保管し、SAFE の記録が改ざんされていないかどうかを MAC と比較して検証することができる。

---

16 Ex ante uitvoeringstoets van wetsvoorstel ‘kansspelen op afstand’ voor de Kansspelautoriteit (Execution Test of Bill ‘Remote Gambling’ for the Gaming Authority), Bouwen aan de KSA 2.0 (Building the KSA 2.0), Berenschot, https://zoek.officielebekendmakingen.nl/blg-489677.pdfv

17 Modernisation of Games of Chance, Gambling Compliance, https://zoek.officielebekendmakingen.nl/blg-489682.pdf

18 Technical requirements – online casino and betting, Spillemyndigheden (The Danish Gambling Authority), https://www.spillemyndigheden.dk/uploads/2018-11/Technical%20requirements%20-%20online%20casino%20and%20betting%20v2.1.pdf

2.1.5 リモートギャンブルの合法化に向けた手続きの開始 (2012~2015 年)

データ追跡のための利用可能な代替オプション (10 ページ記載の表) を法案の修正案[19]と比較すると、法務省がオプション 2 のようなデータストレージを含めることを決定したことがわかる。これは、KSA が常にアクセスできるリモートギャンブル事業者のデータのコピーを持つサーバである。この「安全」システムは、オランダの法律で CDB と呼ばれるようになった。

提案によると、リモートギャンブル事業者はデータのコピーを格納した CDB をオランダに置かなければならないとしている。これにより、9 ページ記載の表に示すように、監督者がデータに物理的にアクセスできなくなるリスクが低減される。具体的な場所は規定されていないが、リモートギャンブル事業者は KSA に CDB の正確な場所を通知しなければならない。リモートギャンブル事業者は CDB の維持管理を第三者に委託することができる。

データが改ざんされるリスクを低減するために、リモートギャンブル事業者はデータをほぼリアルタイムで CDB に格納する必要がある。これにより、データが改ざんされる可能性のある時間枠を最小限に抑えることができる。どのようなデータを CDB に格納しなければならないかは、提案のこの段階ではまだ詳細に検討されておらず、より下位の法律で規定される予定であった。ただし、CDB に格納されるデータは、規定された目的に沿ったもののみであるべきことが明記されている。これにより、個人情報の不必要な取扱いおよびアクセスが防止され、データ主体に対するプライバシーの影響が限定的なものとなる。

2.1.5.1 CDB に対しての反応と議論

2.1.5.1.1 設置場所

The European Gaming & Betting Association(以下、協会という。)は、リモートギャンブル事業者が自身の CDB をオランダに置くことを義務化する決定を批判した[20]。協会は、このようなローカル CDB を要求する目的は、制御と検証のみであるとし、この目的のためには物理的存在は不可欠ではないと主張した。加えてこの義務は他の EU 加盟国からの新規参入者に対して差別的であり、オランダに所在するリモートギャンブル事業者と比べて著しく不利な立場に置かれると述べている。

次に、CDB への接続や VPN の使用など、効果的であることが確認されている有効な代替法があることを説明している。

協会の主張に沿う形で、オランダ政府に助言している国務院(Raad van State)もまた、CDB をオランダ国内に設置するという要件が、健全な監督のために何故必要なのか明確ではないと述べた[21]。

オランダ政府の CDB についての担当大臣は、CDB をオランダに置くことが KSA および他の当局による監督の有効性のために利点があると回答した[22]。CDB がオランダに設置されることにより、CDB および CDB に含まれるデ

---

19 Wijziging van de Wet op de kansspelen, de Wet op de kansspelbelasting en enkele andere wetten in verband met het organiseren van kansspelen op afstand (Amendment of the Betting and Gaming Act, the Betting and Gaming Tax Act and Some Other Laws Related To Organizing Remote Gambling), Overheid.nl (Dutch Government Website), https://zoek.officielebekendmakingen.nl/kst-33996-2.html

20 Response of the European Gaming & Betting Association, the European Gaming & Betting Association, https://zoek.officielebekendmakingen.nl/blg-359706.pdf

21 Besluit kans-spe-len op afstand (Decree to Remote Gambling), Raad van State (The Council of State), https://www.raadvanstate.nl/adviezen/@121773/w16-20-0229-ii/

22 Response to the advice, Besluit kans-spe-len op afstand (Decree to Remote Gambling), https://www.raadvanstate.nl/adviezen/@121773/w16-20-0229-ii/

ータを、必要に応じて保護、確認、および差し押さえることができること。また、オランダに設置されることにより、CDB が存在する場所に立ち入り、そのデータベースを調査し、そこに存在する個人に協力を求め、データベースまたは CDB が存在する場所を確認することが可能であること。つまり、大臣は、CDB がオランダ国外にある場合、オランダの監督当局はこれらの権限を行使できないと述べている。

また、オランダはホスティングサービスに適した環境にある。したがって、他の EU 加盟国と比較して、オランダにおける CDB の配置に高い追加コストがかかることは予想されないと大臣は主張している。

最後に、CDB をオランダ国内に設置する義務は、リモートギャンブル事業者のプライマリサーバー本体やリモートギャンブル事業者の支店自体をオランダに設置することに比べて、かなり軽い要件であることを強調している。

結論として、リモートギャンブル事業者はオランダにオフィスを持つ義務はない。ただし、CDB はオランダに配置する必要があるとされた。

2.1.5.1.2 データの改ざん

オランダ議会の代表者が出席した修正案に関する委員会の議論の中で、この提案は、記録の改ざんを防ぐために、データはほぼリアルタイムで CDB に転送されるべきであると述べていることが注目された。

委員会は、データを改ざんしようとしているリモートギャンブル事業者にとって数分あればデータを改ざんするのに十分な時間があるということを懸念している。彼らは、さらなる分析がなければ、データが改ざんされたかどうかはわからないと考えている。

ギャンブル法および規制を担当する大臣(Minister for Legal Protection)は、リモートギャンブル事業者は大量のデータを継続的に CDB に転送する義務があると回答し、リモートギャンブル事業者が痕跡を残さずにこれらの大量のデータを数分以内に改ざんする可能性は極めて低いと述べた。さらに、KSA はリモートギャンブル事業者のプライマリーシステムにアクセスする権利を有し、それらのコピーを要求することができる。よって、これらのシステムの監査が行われた場合、プライマリーシステムと CDB のデータを比較することができるため、不正操作が気付かれない可能性は非常に低くなる。

また、2.1.4.1 で説明されているフランスでの事例では、リアルタイムのストレージがギャンブル事業者のゲームシステムに多くの遅延をもたらすことを示しており、こういったことは CDB の目的の望ましくない結果とも考えられる。

最後に、大臣からの回答では、CDB およびデータの送信は様々な技術的および運用上の要件の対象であることが示されている。これらの要件は、認可前に認定検査機関によって検査される。これにより、改ざんのリスクが低減されるとしている。

加えて、オランダ議会の代表者が出席した、リモートギャンブル合法化に向けた法案の修正案に関する委員会は、CDB における安全なデータ保存が常に確保できるかどうかの明確化を求めた。大臣は、リモートギャンブル事業者は、CDB に含まれるデータを、データ紛失や、不正な処理およびトレーサビリティから保護するための適切な措置を講じる責任があると回答した。

結論として、データをほぼリアルタイムで CDB に提供する義務は、データが操作される可能性を最小限に抑えるために必要であるとされた。

2.1.5.1.3　プライバシーの保護

上記の委員会の会議では、リモートギャンブル事業者も特別な個人データを処理していることを考慮し、CDB 内のプレーヤーのプライバシーをどのように保護するかという問題が提起された[23]。特別な個人データとは、例えばギャンブル中毒に関するデータなどの健康データである。EU 一般データ保護規則(General Data Protection Regulation: GDPR)に基づき、特別な個人データの取扱いは禁止されている。この規則の例外は、そういったデータの取扱いが重要な公共の利益のために必要であることだが、その妥当性が確保されなければならない。

ギャンブル法および規制を担当する大臣(Minister for Legal Protection)は、当局による健全な監督を確保するためにこれらのデータの処理が必要であると答えた。大臣は、現行の規制では、リモートギャンブルを提供するライセンス保持者が管理データを保存しなければならないデータベースの管理に関する追加の規則が規定されていることを強調した。プライバシーは、CDB にプレーヤーの疑似匿名データのみに限定されることによって保護される。

プライバシーを考慮すると、一度登録されたデータ保持する期間を必要に応じて出来るだけ短時間にすることが求められる。これは、期間を明確に定義した保存期間に関するガイドラインを作成することによって確保される。さらに、リモートギャンブル事業者は、個人データの保存期間について、個人データが処理されているプレーヤーに通知しなければならない。最後に、妥当性については、監督者に必要なデータのみへのアクセスを許可することによって確保される。

このように、データのプライバシーは、プレイヤーデータの疑似匿名化とデータセキュリティの厳格な管理によって十分に保護されている。

2.1.6　オランダ議会での最終決定、承認プロセスと導入 (2016~2021 年)

リモートギャンブルのライセンス制度を法制化する立法プロセスは非常に広範囲なものとなった。これは主に、リモートギャンブルが道徳的かつ倫理的に問われるテーマであり、議会における意見が大きく異なるという事実によった。この法案はオランダ議会で多くの議論を引き起こした。その結果、プリンシプル・ベースの規制からルール・ベースの規制へと移行し、より詳細な規制が求められるようになった。これは、健全な監督を確保するための具体的な保証と保護措置を策定することに主に関係している。

2016 年 7 月 7 日、(リモートを含む) ギャンブルに関する法律の改正案がオランダ議会 (Tweede Kamer) で可決された。しかし、上院 (Eerste Kamer) が 2019 年 2 月 19 日に法案の修正を可決するまでに、最終的に 3 年を要した。

KSA は 2020 年 11 月 17 日に CDB の最初の仕様を公表した。認可を受けてギャンブルサービスを提供するためにはリモートギャンブル事業者は、下位法と KSA で規定された要件に準拠した CDB をもつことが義務付けられる。

2021 年初頭、大臣は法律の改正が 2021 年 4 月 1 日に施行されると述べた。これは、ライセンスプロセスの進捗状況に応じ、2021 年 10 月 1 日に認可されたオンライン市場が開く予定であることを意味した。法律の改正の施行と実際のオンライン市場の開設の間の期間はリモートギャンブル事業者へのライセンスの承認期間によるものである。

---

[23] Regeling kansspelen op afstand (Regulation on Remote Gambling), Overheid.nl (Dutch Government Website), https://zoek.officielebekendmakingen.nl/stcrt-2021-4507.html#d17e1266

上記の法律の改正と CDB の仕様の公表の期間のタイミングから、リモートギャンブル事業者がオンライン市場の開設と同時に市場に参入した場合においての CDB の実装期間は約 10 カ月であったことが分かる。この実装期間の一部として、統合テストは必須であり、その実施には約 6 週間かかる。検査結果は 3 カ月間有効とされた。

このライセンス制度が施行された日、合計 10 件のライセンスが付与された。その後 2022 年 7 月までの数ヶ月で、KSA はさらに 9 つのギャンブル事業者にオランダでリモートギャンブルを提供するライセンスを与えた。

その間も、CDB の仕様は定期的に更新された。データ・モデルのバージョン 1.1 は 2022 年 4 月 19 日にリリースされた。仕様の更新後、リモートギャンブル事業者は必要な変更を実施するために 4 カ月の猶予を与えられた。したがって、リモートギャンブル事業者は、CDB の運用中に変さらに対応するために継続的な努力が必要とされる。

2.2 CDB の概要と AML 監督上の位置付け

本節では、図 3 に示すように、AML の監督上、CDB がどのように位置付けられているか、また、より広い枠組みの中でどの主体がどのような役割を果たしているかを明らかにする。

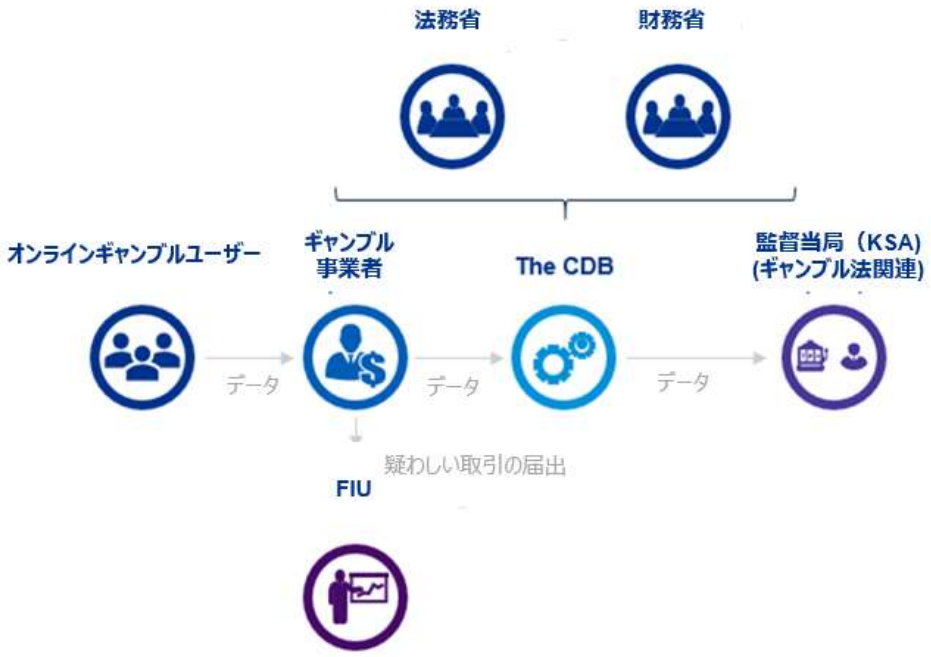


図 3: より広い枠組みでの CDB の位置づけ

2.2.1 法務省と財務省

オランダにおける AML/CFT に関する法律である Wwft の制定の責任は、法務省と財務省の 2 つの省が共同で担っている。EU 加盟国は、欧州指令に基づき、AML/CFT 対策のための法的枠組みを整備する義務がある。EU 加盟国における各省庁は EU 指令に基づく規制を適用している。

第 5 次 AML 指令 (EU) 2018/843 (AMLD 5)はオランダの法律に反映された。この法律には、金融監督法 (Wft) 規制当局と Wwft 規制当局との間で情報を共有するための規定などが含まれている。これにより、金融情報機関 (FIU) や KSA などの監督機関間での情報共有が容易になった。

オランダ賭博法 (Wok) やリモートギャンブルに関する政府令、リモートギャンブルに関する省令を含むギャンブルに関連するすべての法律および規制は、法務省の管轄下にある。

各省庁はこれらの法律および規制に責任を持つため、図 1 に含まれている。ただし、ギャンブル事業者への監督責任は KSA という役割分担となっている。

2.2.2 リモートギャンブル事業者

認可されているリモートギャンブル事業者とは、KSA からオランダでリモートギャンブルを提供するためのライセンスを受けたオランダおよび外国の事業者である。リモートギャンブル事業者は、ライセンスを受ける資格を得るためには、AML ポリシーや CDB に関する文書などの広範な文書パッケージを提出する必要がある。

ライセンスの要件として、リモートギャンブル事業者は KSA に年間の監督に係るコストを支払う義務がある。これらのコストは、事業者の総ゲーム結果の 1.95%に相当する(そのうち 0.25%がギャンブル依存症対策に使用され、1.7%が KSA にいく)。総ゲーム結果とは、受け取った掛け金の合計額から付与された価値を差し引いた差のことである。KSA の予算の 80%以上は (リモートとオンサイトのギャンブル事業者の) 年間の監督に係るコストで賄われている[24]。

ライセンス申請の他の要件として、リモートギャンブル事業者は、KSA が定める技術仕様に従って CDB が実装されること、および CDB が KSA からアクセス可能であることのエビデンスを提供する必要がある。

CDB に関して、事業者は次の文書を提供する必要がある。

- リモートギャンブル事業者とそのサービスの特徴
- CDB の設定
- データ・マッピングとテスト
- CDB の存在
- CDB の撤退計画

撤退計画では、CDB の終了後に、リモートギャンブル事業者がコンプライアンス (例えばデータ保持期間など) をどう保証するかの方法が記述される。KSA は、「撤退時にサードパーティーが CDB の管理を引き継ぐことを契約した場合:権限のある役員によって署名された契約があることを証明し、サービス記述書が撤退計画に記載された解決策に対応しているかどうか、およびその意図された効果を検証する」という例を提供している[25]。

オランダでは、2022 年 7 月の時点で、合計 19 のリモートギャンブル事業者がリモートギャンブルの運営ライセンスを付与されている。ライセンスを付与された事業者を見るとほとんどは海外事業者である(マルタ 9 社、ベルギー3 社)。一方、オランダ国内事業者としては 7 社がリモートギャンブルのライセンスを取得している。図 4 にその推移を示している。

---

24 Jaarverslag Kansspelautoriteit 2021 (KSA annual report 2021), Kansspelautoriteit (Netherlands' Gambling Comittiee), https://kansspelautoriteit.nl/publish/library/35/0006_ksa_jaarverslag_2021_wr_2.pdf

25 Draft Remote Gambling Assessment Scheme (Remote gambling conformity assessment scheme), Kansspelautoriteit (Netherlands' Gambling Comittiee), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjktba_tMv5AhUZg_0HHTIDD_cQFnoECAkQAQ&url=https%3A%2F%2Fkansspelautoriteit.nl%2Fpublish%2Flibrary%2F30%2F20211220_keuringsschema_engels.pdf&usg=AOvVaw2X7xPA-pGuFfrV70piPx_R

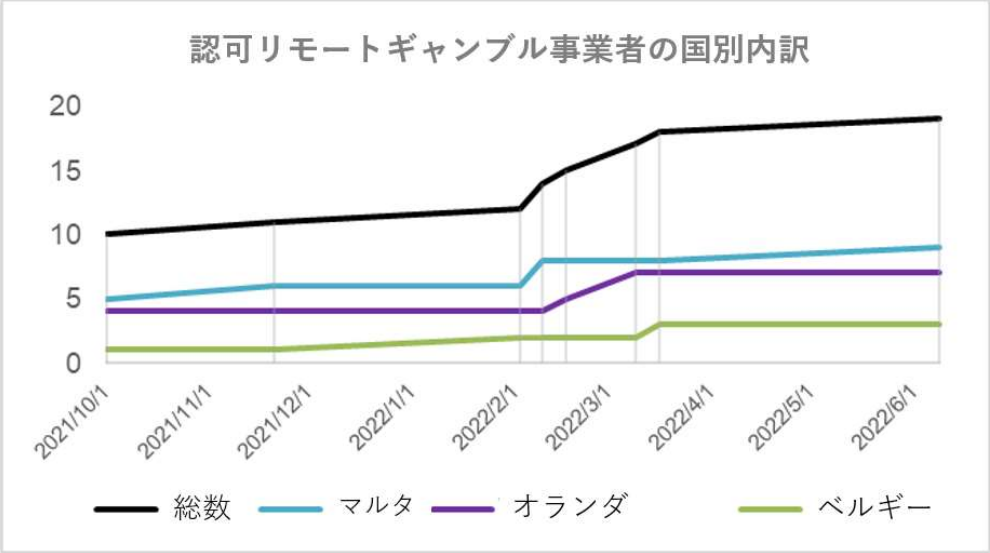


図 4: ライセンス制度導入以降、オランダで付与されたライセンス数

2.2.3 ギャンブル監督当局

オランダにおけるギャンブルの監督当局である KSA は 2012 年 4 月 1 日に設立され、その任務は (リモートを含む) ギャンブルライセンスを付与することによりギャンブルセクターを規制し、ライセンス保有者を監督し、違法ギャンブルと戦い、ギャンブル依存症から消費者を保護することとされている。加えて、KSA は、2.1.2 で解説したとおり、適用される法律および規則の遵守並びにこれらの法律および規則の執行を監督する任務を有する。

ランドベースカジノに対する Wwft 関連の監督は KSA に一任されているため、法務省はリモートギャンブル事業者の監督も KSA に委任するのが理にかなっているとした。

Wwft に関して、KSA には八百長や ML を検出する法的な任務はない。しかし、KSA は、ライセンスを保持する事業者が八百長や ML を防止するために十分な対策を講じているかどうかを検証しなければならない。監督上の観点から、KSA は、ギャンブル事業者が ML を防止するための規制義務を遵守しているかどうかをチェックする。彼らは、ギャンブル事業者が ML と八百長の十分なリスク評価を行ったかどうかを評価し、さらに、ギャンブル事業者が Wwft に規定されているように、資金の出所や一定金額を超過したかどうかなど、各事業者が十分な顧客デューデリジェンスを行っているかどうかをモニタリングする。CDB は、この AML 対策のモニタリングの実行に必要な情報を含む取引情報を KSA に提供する。CDB データを疑わしい取引の届出に関する情報と比較し、他の監督機関と情報を共有することにより、AML 対策の実施状況を監督することができる。

さらに、KSA は CDB データに基づいて、疑わしい取引の届出の数がどの程度期待されるかを特定することで監督に活用することができる。また、KSA は、想定される疑わしい取引の金額を実際の FIU データと比較することができ、大きな相違が生じた場合には、ギャンブル事業者に対してさらに調査することができる。詐欺やマネー・ローンダリング捜査などの特定の状況下では、KSA はギャンブル事業者に対して、CDB 上では疑似匿名化されている顧客の身元を明らかにするよう要求することができる。

KSA はギャンブル市場の責任者であるため、ギャンブル事業者に対し最善と考えるプラクティスを示していく必要がある。KSA は、市場を積極的にモニタリングすることにより、これらのベストプラクティスを把握すべきである。AML

のためのギャンブル事業者に対する十分なガイダンスを提供するために、KSA は Wwft ガイドラインを作成した[26]。本ガイドラインは、特に異常取引の報告に関するガイダンスを提供している。

2.2.4 FIU

FIU は、様々な事業者が顧客の異常取引を報告しなければならない機関である。FIU は、報告された異常取引の分析を行い、マネー・ローンダリング、テロ資金供与、その他の違法行為に関連する可能性のある活動を明らかにしようとする。FIU の長によって取引が疑わしいと宣言された後、オランダの様々な法執行や調査業務に利用できるようになる。

オランダのギャンブル事業者は、実行または意図されたすべての異常取引を FIU に報告する規制上の義務がある。立法者は、取引が異常とみなされる客観的および主観的な指標（2.2.4.1 と 2.2.4.2 で記述）を提供している。

KSA と FIU は報告された異常な取引に関して監査を行ったが、その内容についてはセクション 2.4.1 で記述している。

2.2.4.1 取引が異常とみなされる客観的指標

- マネー・ローンダリングに関連して警察に報告された取引または検察官に報告された取引
- 15,000 ユーロを超えるキャッシュレス支払い取引、または 24 時間以内の複数の取引の合計が 15,000 ユーロを超える取引

2.2.4.2 取引が異常とみなされる主観的指標

- ギャンブル提供者がマネー・ローンダリングに関連している可能性があると考える理由がある取引

  この要件では、ギャンブル事業者がマネー・ローンダリングのシナリオを評価し、その評価に基づいて、そのようなシナリオの検出を可能にするビジネス・ルールを実装する必要がある。これを行う一般的な方法は、リスク分析を実施し、その分析結果に基づいてビジネス・ルールを定義することである。

  その後、事業者が、取引が疑わしいと判断した場合、アラートを分析して FIU に報告する必要がある主観的および客観的な指標に加えて、ギャンブル事業者は以下を報告することが義務付けられている。

- 顧客の CDD の義務を遵守することができず、且つ、当該プレーヤーがマネー・ローンダリングに関与している兆候がある場合
- CDD の義務に従わなかったためにアカウントが閉鎖され、且つ、当該プレーヤーがマネー・ローンダリングに関与している兆候がある場合

---

[26] Leidraad Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) (Guidance on the Prevention of Money Laundering and Terrorist Financing Act (Wwft)), Kansspelautoriteit (Netherlands' Gambling Comittiee), https://kansspelautoriteit.nl/publish/library/24/leidraad_wwft_1.pdf

2.3 CDB の枠組み、オペレーション、テクノロジーとステークホルダーについての詳細

CDB は、オペレーター(ギャンブル事業者)が所有する独自のデータベースであり、ギャンブルユーザーへのサービス提供に使用される基幹システムとは独立して維持される。CDB は、CDB と KSA のデータ取得および検証プラットフォームとの間の自動化された (マシン間) インタフェースを介して KSA に接続される。

図 5 は、ギャンブル事業者 と KSA 間の CDB のハイレベルな統合を示している。この図は、データの抽出と提供の責任がギャンブル事業者にあることを示している。ギャンブル事業者は、基幹システムおよびその他のデータ・ソースからデータを抽出し、CDB にデータを提供する必要がある。

各ギャンブル事業者は、単一の CDB 環境にデータを格納する。ギャンブル事業者が複数のブランド等を通じてサービスを提供する場合、すべてのブランド等のデータは単一の CDB に格納される。この場合、ギャンブル事業者が CDB 内で各ブランド等のデータを確実に区分するという条件が適用される。

CDB の技術的な設定方法の詳細な仕様は、公開されている。いくつかの特徴はセクション 2.3.1 に記載されている。そしてこの章の残りのセクションでは、データとユースケースに関する AML 特有の意味合いについて考察する。

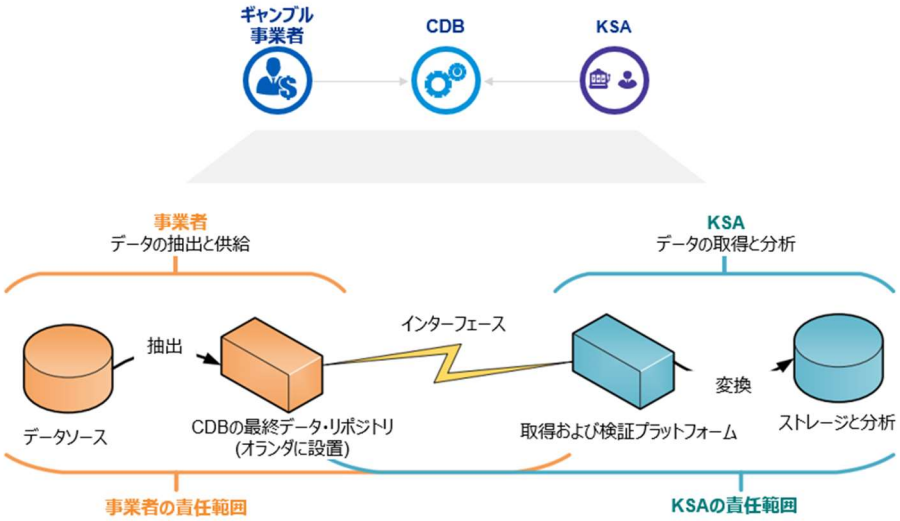


図 5: CDB のハイレベルな統合

2.3.1 CDB 内で AML 関連データがどのように格納されるか

2.3.1.1 データ抽出と提供

ギャンブル事業者は、データを様々な目的のために CDB に格納する必要がある。このセクションでは CDB に格納される AML 関連のデータについて解説する。KSA はギャンブル事業者が Wwft 要件に準拠しているかどうかをモニタリングできる。図 6 は、KSA が Wwft の遵守状況を監督するために使用できる記録の内容を示している。すべての AML 関連データは、「WWFT_Player_Account_Transaction」というファイル構造に格納する必要がある。

取引ごとに、取引量 (Transacion_Amount) と取引が発生した日時 (Transaction_Datetime) が、レコードおよびプレーヤー情報に関するデータの横に入力される。さらに、口座に資金を預金するために使用された預金証書 (Brand_Name_Transaction_Deposit_Instrument) のブランドと名前がレコードに追加される。例えば、銀行間の電子決済の場合には銀行名などである。最後に、取引のタイプ (Transaction_Type)、例えば預け入れ、引き出しおよび賞金といった情報が入力される。

レコードは、ゲームセッションが終了したとき、または取引を行おうと試みたが成立しなかったときに作成される。これらは、ゲームセッション中の 1 つの取引または賞金合計を表し、図 6 に示す取引記録の形式で、取引の発生直後にデータ・ソースから抽出される必要がある。データの抽出後には後述するように、CDB に格納されるまでに様々な手順を踏む。

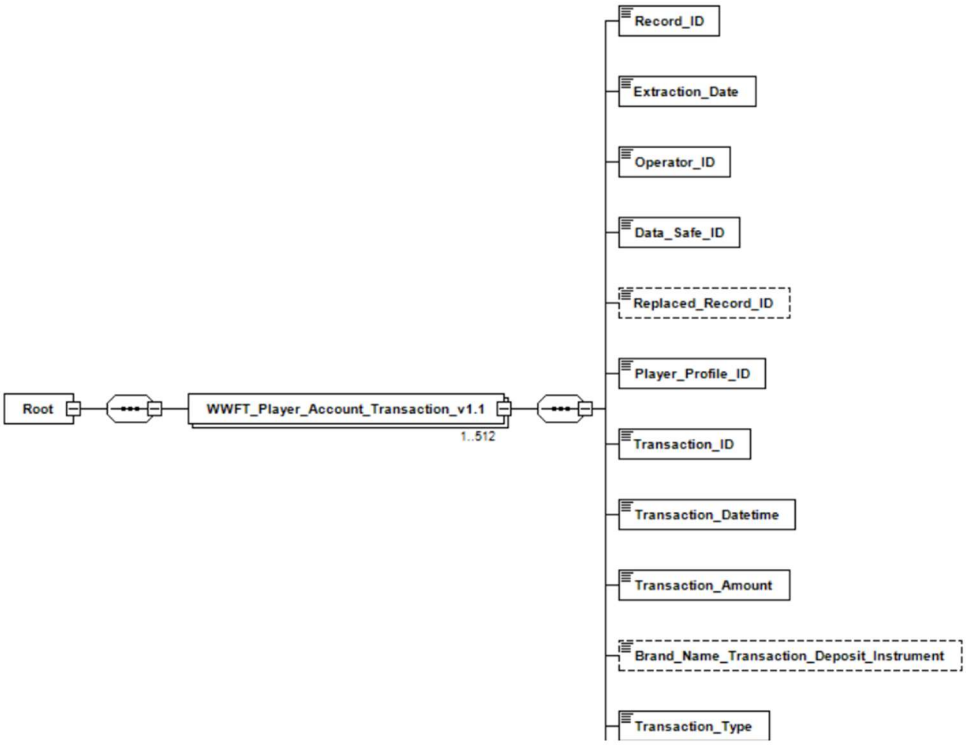


図 6:取引記録の形式（Wwft による監督に使用されたもの）

2.3.1.2　CDB へのデータの格納

ギャンブル事業者は、前述の各取引の Wwft 関連の要件に加えて、次のイベントとデータを CDB に報告する必要がある。

I. プレーヤーの身元を直接たどることができない各プレーヤーの固有の識別情報(擬似匿名化)

II. プレーヤーのプロフィールを変更した日時および内容

III. ギャンブル依存症に関する干渉の理由、時期、内容

IV. ゲームタイプごとの総賭け金と賞金

データは、Extensible Markup Language (XML)ファイル形式を使用して CDB に格納する必要がある。これらの XML ファイルは、KSA によって公開されている XML Schema Definition (XSD)スキームに準拠している必

要がある。XML ファイルは、階層要素を介してデータを格納するために使用され、XSD は、このような XML ファイルの構造と内容を検証するために使用される。これらの XML ファイルは、最大 512 個の一意のレコードを含むバッチで CDB に格納される。レコードの例としては、アカウントでの取引やプレイヤープロファイルの変更などがある。

バッチデータファイルは、最大 512 個の一意のレコードに達するか、または次のいずれかの場合にクローズされる。

- 5 分後
- バッチのサイズが 100 MB に達した場合
- 00:00 (UTC)

CDB にバッチデータを公開する前に、KSA の規定されたガイダンスに従ってバッチを処理する必要がある。この処理手順は、次の 9 つのステップで構成されている。

I. XML 形式のバッチデータファイルの作成
II. XML ファイルの圧縮
III. XML ファイルの暗号化
IV. XML ファイルの名前の変更
V. バッチデータファイルのハッシュ値の追加
VI. 以前に送信した XML ファイルのハッシュ値を追加することによる XML ファイルの連鎖
VII. XML ファイル内のデータの場所の参照
VIII. XML ファイルのタイムスタンプ押印
IX. XML ファイルのアーカイブ

データが所定のリアルタイムで CDB に格納されない場合、すなわち、配信の一時停止、あるいはデータが欠落したファイルの配信のいずれかが発生した場合、ギャンブル事業者は、CDB の内容をリストアする必要がある。前者の場合、CDB へのデータの配信が再開されると、配信が失敗したために空になっていたフォルダがバックフィルされる。後者の場合、欠落データは次の定期配信データファイルに取り込まれ(当初のデータファイルとはタイムスタンプは一致しない)、新たなフォルダに格納される。

2.3.1.3 データ保管と取得

処理された XML ファイルは、KSA のガイダンスで規定されているフォルダ構造を使用して CDB に格納する必要がある。この構造を図 7 に示すが、この図は、監督業務の分離がどのように確保されているかも示している。監督の観点から見ると、KSA は Wok (一般的なギャンブル規制) による監督と Wwft (金融取引の規制) による監督の両方の責任を負っている。ただし、これらの責任は KSA 内の別々の部門にあるため、CDB へのアクセスはこれらの部門間で適宜分離される。図 7 の例では、Wok を管理する監督者は Wwft フォルダ内のデータにアクセスできず、Wwft フォルダ内のデータにアクセスする監督者は Wwft フォルダ内のデータにアクセスできないようになっている。

図 7: KSA で必要な CDB のフォルダ構造の例[27]

ギャンブル事業者は、少なくとも 1 年間 CDB にデータを保持する必要がある。これにより、監督当局は、ギャンブル事業者の関与なしに、その期間中のデータを検査できる。この期間が過ぎると、ギャンブル事業者は CDB からデータを削除することを決定できるが、削除は必須ではない。これらのデータは、より効果的な監督のために、広範な保存期間に従ってソース・システムに保存する必要がある。また、KSA は、ギャンブル事業者に対し、監督機関の調査のために過去の期間のデータを提出するよう要請することができる。

図 5 は、インタフェースを介して、KSA が CDB からデータを取得し、検証して独自のプラットフォームに格納できることを示している。このデータにより、KSA は様々な分析を行い、貴重な知見を得て、監督者としての責務を適切に果たすことができる。

2.3.2 CDB を利用した AML 関連監督の可能性と限界

Wwft に基づくコンプライアンスの監督は、CDB の目的の一つである。KSA は、CDB を通じて入手可能なデータを用いた分析を公表していないが、図 6 で示されている監督当局が利用可能なデータの構造を踏まえれば、KSA は、取引に基づく不正行為の分析が可能であると考えられる。KSA は、例えば客観的指標に基づいて、FIU への報告が必要な特定の取引を識別することができる。KSA が不正行為を特定した場合、KSA はギャンブル事業者に対し、特定のケースに関する詳細情報や、ギャンブル事業者がこれらのチェックをどのように行っているかについての洞察を提供するよう要請することができる。

KSA はウェブサイト上で、CDB の目的、内容と利用はギャンブル法とそれに対応する下位法に限定されると述べている。したがって、KSA は、場合によっては、異なる経路を介してデータを要求する必要があると述べている。その場合は、ギャンブル法に基づくものではなく、一般行政法に基づくものとする。KSA は、この一般行政法は、ギャンブル事業者のソース・システムからデータを取得する可能性を高めていると述べている[28]。

---

27 Data model for the remote gambling data safe (the CDB), Kansspelautoriteit (Netherlands' Gambling Comittiee), https://kansspelautoriteit.nl/publish/library/30/ksa_cdb_datamodel_version_1_1_authorized_for_public_release_19_april_2022.pdf

28 Inrichten en beheren controledatabank (Setting up and managing the CDB), Kansspelautoriteit (Netherlands' Gambling Comittiee), https://kansspelautoriteit.nl/voor-zakelijke-aanbieders/online-kansspel/inrichten-beheren-controledatabank/#:~:text=Het%20doel%2C%20de%20inhoud%20en,wet%20bestuursrecht%20(artikel%205.17).

2.3.2.1　CDB に対する KSA の実務上の利用範囲

現在の CDB の実装状況においては、KSA が利用できる可能性の範囲に関する制約が認識されている。この制約は KSA の公式な見解ではなく、あくまでも KPMG Netherlands が認識しているものである。制約の一つ目は、Wwft 目的で CDB に格納されるデータの種類である。Wwft 目的のためにギャンブル事業者が提供する必要があるデータは取引データに限定される。Wwft の監督目的に当てはまらないデータ、例えばギャンブル依存症に関するデータは CDB の他の領域に格納される。そして Wwft 関連の監督者は Wwft 関連ではない CDB のフォルダのデータへのアクセスは認められていない。よって、CDB の Wwft 目的以外の領域のデータを、Wwft 目的の分析で使用することはできない。

認識されている制約の二つ目は、潜在的な疑わしい取引を特定することは KSA の責務ではなく、それを行う必要がないということである。したがって、KSA がその目的で CDB 内でのデータを使用することは想定されない。この制約に沿った、第 3 の制約は、データ・プライバシーの制約から、KSA が様々なギャンブル事業者からのデータを組み合わせて分析することは認められていないことである。複数のギャンブル事業者からのデータを使用したこのようなパターン認識分析は、理論的には KSA に貴重な洞察を提供することができる。例えば、ユーザーが EUR 6,000 を 3 つのギャンブル事業者に預託するとする。15,000 ユーロを超える金額ではないため、これらのそれぞれの取引を FIU に報告する義務はないが、これらのギャンブル事業者のデータを繋ぎ合わせて分析することができた場合には、この状況が疑わしいと判断され、FIU に通知された可能性がある。

例えば、Wwft の監督の観点からは、ギャンブル法の遵守を監督する目的で CDB に公表されたデータを分析することは認められていない。

2.4　CDB についての最近の動向と将来像

CDB とそのユースケースをより広い視野でとらえるため、以下では最近の CDB の動向とオランダ市場における AML 監督に関するより広い動向について考察する。

2.4.1　KSA によるコンプライアンスの調査

Wwft では FIU への疑わしい取引の報告をギャンブル業者に義務付けており、その遵守状況について、2022 年初めに KSA が調査した[29]。この調査は、異常取引の報告に関するデータを FIU からも入手する等して行われた。

調査結果は以下のとおりである。

- すべての異常な取引を FIU に報告しているわけではない(KSA は、報告された疑わしい取引の実際の数が、データに基づく KSA の予想よりも少ないと判断)
- 主観的な指標に基づく異常な取引の多くが、法定期間である 14 日以内に報告されていないこと

これを受けて、KSA はすべてのライセンス保有者に対し、今後も継続的に調査を行うこと、さらなる調査の結果、問題点が解消されていないとされた場合、KSA はギャンブル事業者に処分を科すこと等を通告した。

[29] Online kansspelaanbieders leven Wwft-verplichtingen nog onvoldoende na (Online games of chance providers are still insufficiently complying with Wwft obligations), Kansspelautoriteit (Netherlands' Gambling Comittiee), https://kansspelautoriteit.nl/nieuws/2022/april/online-kansspelaanbieders-leven-wwft/

2.4.2 CDB の導入効果

CDB の導入効果としては、前セクション（2.4.1）で述べた通り、KSA が事業者の規制準拠状況を調査するための有効なツールとして活用されたという点が挙げられる。

3 メキシコ

本セクションは、メキシコの金融規制当局の一つである National Banking and Securities Commission (Comisión Nacional Bancaria y de Valores: CNBV)による SupTech の取組みに関連して KPMG メキシコが実施した調査内容をまとめた。CNBV の SupTech の取組みは、AML/CFT 監督におけるテクノロジー活用事例の一つである。

本セクションでは、次の項目について説明する。

1. SupTech 構想と BIS フレームワークの背景
2. メキシコにおける AML/CFT の一般情勢
3. The RegTech for Regulators Accelerator (R2A) の CNBV の SupTech 変革への関与
4. CNBV の現在の SupTech 全景
5. 認識されている課題 (CNBV および金融機関の見解)

本調査における第 1 段階として、KPMG メキシコは CNBV の年次報告書や R2A によるホワイトペーパーなど、一般に公開されている情報に基づいてデスクトップ調査を実施した。そしてその後、一部の金融機関および CNBV の元職員へのインタビューを実施した。

本章では、略語が頻出するため、以下のとおり略語集を整理した。

KPMG

略語集

略語	正式名称
AI	Artificial Intelligence
AML/CFT	Anti-Money Laundering / Counter Terrorism Financing
API	Application Programming Interface
Banxico	Bank of Mexico
BCBS	Basel Committee on Baking Supervision
BDT	Electronic Transfers Database
BIS	Bank for International Settlements
CEFER	Rating of Financial Institutions with a Risk Approach
CNBV	National Banking and Securities Comission
Cold-Storage	With cold storage, the digital wallet/information is stored on a platform that is not connected to the internet, thereby protecting it from unauthorized access, cyber hacks, and other vulnerabilities that a system connected to the internet is susceptible to
DNFBPs	Designated Non-Financial Businesses and Professions
FinTech	Financial Technology
FIU	Financial Intelligence Unit
FSA	Financial Services Agency. Is the Japanese financial regulator responsible, for, among other aspects, the oversight of the banking sector and stability of the Japanese financial system
KPMG Mexico	KPMG Cardenas Dosal, SC, the Mexican member firm of KPMG International
LFPIORPI	Anti-Money Laundering Law
Mutual Evaluation Report of Mexico	FATF's Anti-money laundering and counter-terrorist financing measures of Mexico, mutual evaluation report of 2018
R2A	Regtech Regulators Accelerator
RegTech	Regulatory Technology
SAT	Tax Administration System
SEGOB	Secretary of the Interior
SFP	Public Function Secretary
SHCP	Subsecretary of the Ministry of Finance and Public Credit
SITI	Interinstitutional Information Transfer System (CNBV)
SOCAPS	Cooperative Savings and Loan Societies
SOFINCOS	Community Financial Societies
SOFIPOS	Popular Financial Societies
SOFOME	Multiple Purpose Financial Societies
SPEI	Interbanking Electronic Payment System
SPID	Interbanking Payment System in Dollars
STRs	Suspicious Transaction Reports
SupTech	Supervisory Technology
VSSP	Vice Presidency of Supervision of Preventive Processes

3.1 SupTech 構想と BIS フレームワークの背景

3.1.1 SupTech の背景

「SupTech」という用語は、金融機関の監督を支援するための監督当局による革新的な技術の活用として、2018 年に国際決済銀行(BIS)によって導入された。

2019 年、BIS は「革新的技術」という用語を特定・明確化するとともに、用語の適用範囲を拡大し、「監督機関および非監督機関がその機能を支援するために革新的な技術、特にビッグデータおよび人工知能を利用すること。」として、概念を再定義した[30]。

このように、SupTech は、監督活動を支援するために規制当局によって導入された技術を指し、前述のように、その活動を支援するために革新的な技術を優遇する、いわゆる金融技術のサブセットである。

SupTech は、監督機関が情報と規制プロセスをデジタル化し、技術化することを支援する。これにより、金融機関のリスクとコンプライアンスの観点から、より効率的でプロアクティブな監督が可能になるが、SupTech ソリューションは、データ入力、検証、マイニング、集約等といった、価値ある情報提供するための特定アプローチ、機能を有している必要である。

規制当局において監督プロセスを強化するために SupTech を採用することができるが、SupTech が有効に機能するためには、監督対象の事業者側での革新的な技術の利用、すなわち RegTech の採用との相互依存がポジティブな形で機能することが重要である。監督対象の事業者の RegTech ソリューションが十分な成熟度を持っていない場合、SupTech ソリューションは非効率的となりうる。

3.1.2 SupTech BIS フレームワーク

2019 年 10 月、BIS はホワイトペーパー「The SupTech Generations」を公表し、規制当局が使用している技術のすべてが SupTech であるとは限らないと説明した。

すなわち、SupTech プロセスのいくつかのステップについて、それぞれの世代の技術ツール内にリストアップされているフレームワークを提案した。BIS は、3G と 4G の世代だけが SupTech と見なされると規定した。(下図参照)

[30] Bank for International Settlements, Financial Stability Institute (2019). FSI Insights on policy implementation No 9: Innovative technology in financial supervision (SupTech) – the experience of early users. https://www.bis.org/fsi/publ/insights9.pdf

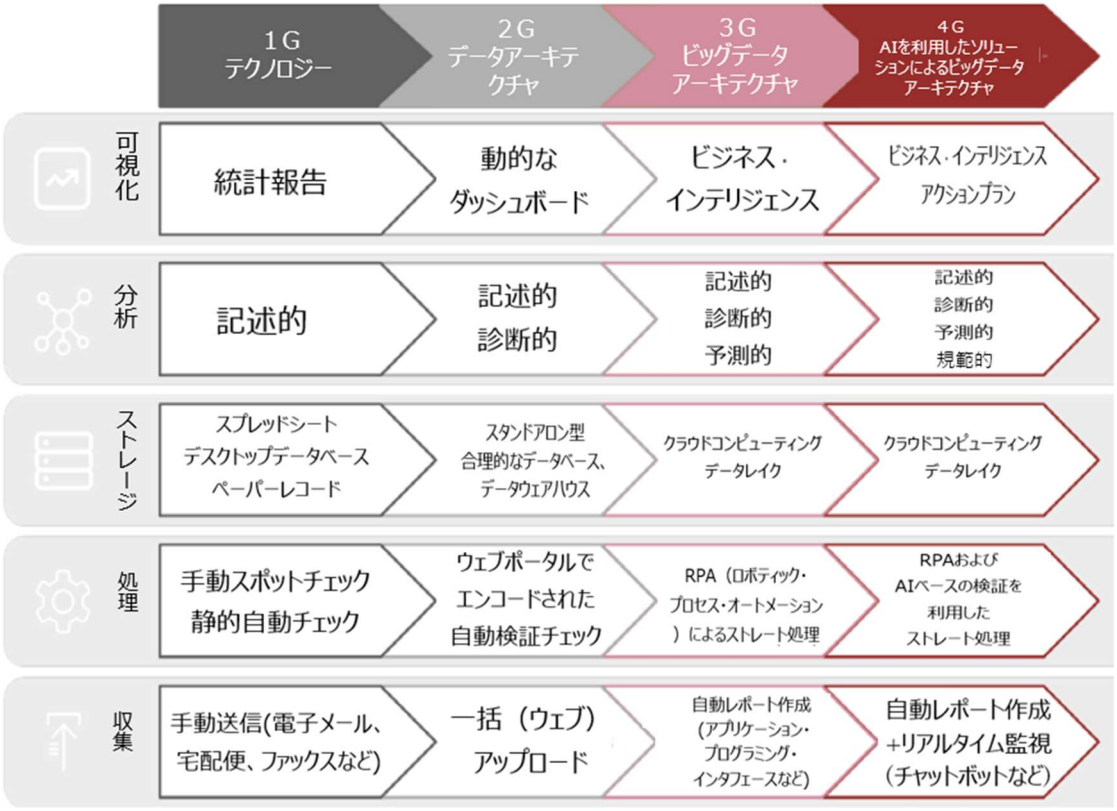


図 9: SupTech の世代(BIS ホワイトペーパーより、KPMG が翻訳)

各世代の要約は以下のとおりである。

- 第 1 世代 (1 G) には、手作業が多く、主に記述的な分析を行うデータ管理ワークフローが含まれている。ほとんどの規制対象事業者にとって出発点であり、業務上およびセキュリティ上のリスクを伴う。
- 第 2 世代 (2 G) は、データ・パイプラインにおける特定の紙ベースおよびマニュアルプロセスのデジタル化と自動化を対象としている。通常は、自動化されたチェック機能と組み合わせ、規制対象の事業者からの規制上の申告を行う Web ベースのポータルまたは一括アップロードを伴う。
- 第 3 世代 (3 G) はビッグデータのアーキテクチャをカバーしている。この世代には、API(Application Programming Interface)と RPA(Robotic Process Automation) 技術の組み合わせ、さらにはデータレイクの使用も含まれる。
- 第 4 世代 (4 G) では、その特徴として AI(Artificial Intelligence)の付加がある。この世代は、データ管理と分析の一部を「マシン」に駆動させ、当局による行動を知らせることで、自動化を一歩進めた。

3.2 メキシコにおける AML/CFT の一般情勢

3.2.1 メキシコの AML/CFT 体制、当局および規則

3.2.1.1 AML/CFT の一般情勢

メキシコにおける AML/CFT 対策の状況は、FATF の「2018 年相互審査評価報告書」で示されているように、要件に対応した制度的枠組みが整備され成熟した AML/CFT 体制を有しているとされている。そういった状況に

あるものの、マネー・ローンダリングのリスクは依然として重大であり、その主な原因は、薬物取引、恐喝、汚職、脱税などの組織犯罪に関連する行為と、そういった行為に対する法執行当局による法的な AML/CFT 対策の枠組みの適用に関するコミットメントの低さがあげられる。また、メキシコはメキシコ国外を源泉とする犯罪による収益の洗浄に関連するリスクの高まりに直面している。これらは、米国や稀に中南米との取引の際に発生するメキシコの国際組織犯罪に関連している。

典型的なマネー・ローンダリングの手法には、実質的支配者を隠すためのダミー会社やフロント会社の利用、不動産や高額商品の売買、米国・メキシコ国境の両方向での現金の密輸などがある。現金の大量使用と比較的大きな地下経済によって、犯罪収益がそこから再流入されるリスクを著しく増大させる。

しかし、メキシコ中央銀行の分析[31]によると、金融機関による米ドル現金の入金取引への制限により、メキシコの金融システムにおける米ドル資金の出入が大幅に減少した[32]。一方、メキシコ・ペソ (MXN) 現金の使用は増加している。

当局と民間セクターは、総じてテロ資金供与(TF)のリスクが低いことに同意しているが、同時にいくつかの問題が検出されている。

3.2.1.2 AML/CFT 体制

メキシコの AML/CFT 体制は、「予防」、「検知」、「対処」の 3 つの主要段階に区分される。以下の図に示すように、規制当局が定めたルールに基づき、強固な AML/CFT コンプライアンス・プログラムを構築することを主要な機能とする規制対象 (金融機関および DNFBPs) から制度がスタートしている。

情報の流れは双方向であるため、監督される規制対象機関は、重度の犯罪の報告につながる可能性のある報告書や通知の質を改善するために必要なフィードバックを得ることができる。

予防と検知の段階は行政的なものであり、この段階では起訴されるには至っていないことに注意することが重要である。FIU が疑わしい取引として法執行機関に提出することを決定した場合、連邦検事総長は FIU から提供された情報を使用して調査を実施しなければならない。

---

31 米ドル取引は 2007 年から 2014 年にかけて大幅に減少したが、米ドルでの黒字と輸出は依然として大きい。(2014 年は 50 億米ドル) 。この取引の性質を理解するために、2009 年に FIU とメキシコ中央銀行は、銀行、両替所、証券会社に情報提供依頼書を出した。当局は受け取った情報に基づいても、2007 年の米国ドルの黒字の理由を特定することはできなかったが、当局はこの余剰資金を、国境貿易、観光、または移住者が現金で受け取った送金に起因するものだとした。この余剰資金のうち、正当な経済目的で説明されなかった部分については、不正収益に関連する可能性がある。

32 2010 年には、銀行を通じた不正な現金取引が行われるリスクを軽減するため、金融機関が米ドル建ての現金を受け取ることを制限した。現在でも、金融機関は、いくつかの例外を除いて、米ドルでの現金の受け取りが禁止されている。銀行、証券会社、両替所、貯蓄組合と著名な信用組合は、顧客のためには毎月 4,000 米ドルまで、利用者のためには毎月 1,500 米ドル、一日で 300 米ドルまで、米ドル取引を行うことができる。外国人利用者と取引する場合、両替所には金額制限がない。法人の場合は、これらの国境州 (北部および南部) のみで毎月 14,000 米ドルまでの制限がある。銀行は、AML/CFT ルールに定められた一定の条件の下で、無制限に米ドル建ての現金取引を法人に提供することができる。両替センターは米ドルで取引できるが、一人 1 日につき 1 万米ドルまでに制限されている。送金機には金額制限はない。

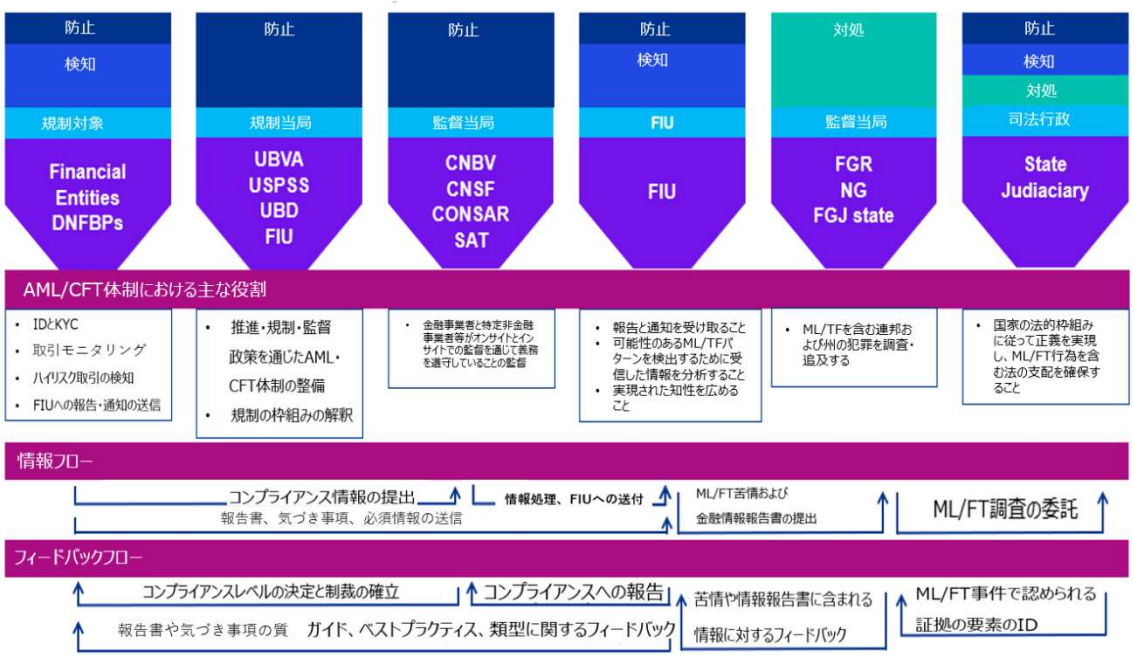


図 10: メキシコの AML/CFT 体制

図 10 に示すように、AML/CFT の当局は、AML/CFT の法令を制定、作成、公布する規制当局と、AML/CFT の法令遵守を監督する監督当局の 2 つのグループに大別される。FIU は、金融機関や DNFBP から提供された報告書や通知を受領し分析する。FIU が事件として認定した場合、それらを連邦公安省に提出し、犯罪行為として起訴できるようにすべきとされている。

3.2.1.3　AML/CFT 規制

AML/CFT の枠組みは、FATF の第 7 次強化評価報告書後の 2014 年に公布され、不正な手段による資金取引の防および特定のための連邦法の範囲内で確立されている。この法律は、銀行向けの AML/CFT 対策の規定が公表された 2009 年以降、金融機関が遵守してきた AML/CFT 対策の規定に変更を加えるものではない。以下の表に示すように、各セクターにはそれぞれ固有の AML/CFT 要件が存在する。

セクター	AML/CFT 規定
銀行	信用機関法第 115 条　一般条項
証券会社	証券法第 212 条　一般条項
ローン・リース機関	信用法附属機関および活動に関する法律第 95 条 BIS　一般条項
取引所	信用法附属機関および活動に関する法律第 95 条　一般条項
普通預金倉庫	
為替センター	信用法附属機関および活動に関する法律第 95 条 BIS　一般条項
送金業者	
貯蓄機関および民衆信用機関	貯蓄および民衆信用法第 124 条　一般条項
投資ファンド	投資信託法第 91 条　一般条項
貯蓄貸付組合	貯蓄貸付組合法第 71 条および第 72 条　一般条項
投資顧問業	証券法第 226 条　一般条項
フィンテック	フィンテック法第 58 条　一般条項

顧客の識別、KYC、報告といった一般的な義務は各セクターに共通する規定となっているがセクター固有の特定の基準も存在する。例えば、銀行のための AML/CFT の規定は、口座を開くための要件を含むが、交換所のための AML/CFT の規定は、通貨の売買取引のための識別要件のみを含むなどがある。また、AML/CFT 法では、ML リスクにさらされている DNFBP を 16 種類定めており、それらの DNFBP が暗号資産の取引を含め、取引が金融機関によって実施されていない場合に従わなければならない義務が規定されている。

3.2.1.4　当局

SHCP は、AML/CFT 義務の遵守に関する全般的な規制に責任を負う機関であるが、業務上の責任は、法令によりそれぞれ CNBV、CNSF、CONSAR、SAT に委任されている。

当局	監督セクター
CNBV	金融機関
CNSF	保険
CONSAR	退職年金
SAT	特定非金融事業者等

メキシコの FATF 相互審査評価報告書でも言及されているように、金融セクターの監督当局は、自らが担当するセクター内のリスクを十分に理解しており、個々の金融機関のリスクを識別するための健全なモデルを開発している。

DNFBP に関しては、SAT のリスク評価の基礎が十分に確立されていないため、状況は不明である。SAT が責任を負う機関の数が膨大であることは、個々の企業レベルのリスクを理解する上で重大な課題となる。

メキシコの相互審査評価報告書によれば、CNBV は、個々の金融機関を分類するためのリスク・モデルの考案と採用において、監督当局の中で最も進んだ手法を有している。2015 年以降、CEFER モデルを採用している。CEFER モデルは、あらゆる形態の監督上のリスク(ソルベンシー、流動性、AML/CFT 等)を単一のツールで評価するように設計されている。AML/CFT リスクは、法律上および風評上のリスクのサブセットとみなされ、全体のリスクの 7%を占める。CEFER への具体的な AML/CFT インプットを決定するために、CNBV は AML/CFT 遵守の監督の基礎として使用される別のモデルを開発した。

CNBV は、メキシコの金融システムを監督する財務省から分権化された機関である。CNBV による監督は、特に、信用リスクおよびオペレーショナル・リスク、AML/CFT 対策のような事項について、オンサイトとオフサイトで実施される。

本報告書の目的は、CNBV における SupTech の動向を紹介することであり、そのためにまず、AML/CFT の監督を任務とする「予防的プロセス監督副総裁室」(the Vice-Presidency of Supervision of Preventive Processes)の組織構造を理解することが重要である。組織構造についての背景は以下の通り。

- 2021 年時点で、約 35 名の職員で構成されている
- 合計 3,363 の事業体を 5 つの主要セクターに分類して監督している(詳細は Appendix V を参照)。

AML/CFT における最新の監督対象セクターである FinTech は、FinTech 法の施行に伴い 2018 年に法人化が認められた。上記の表に記載されているすべての部門は、両替センター、SOFOMES および送金業者を除き、慎重に管理されている。

CNBV は、監督対象の金融機関からの AML/CFT 報告書の受領、処理、FIU への送付を担当しているため、AML/CFT の年次レビューなど、構造化されていない特定の情報の分析も担当している。Appendix VII に詳述されているように、情報はさまざまなチャネルを通じさまざまなタイミングで受信される。これは、CNBV が SupTech を実装するための課題と機会の領域を表している。

3.3 The RegTech for Regulators Accelerator (R2A)の CNBV の SupTech 変革への支援

The RegTech for Regulators Accelerator (R2A)は、デジタルイノベーションに特化したコンサルティング会社である BFA Global 社が、メキシコの CNBV に加えてフィリピン、ナイジェリアの金融当局と連携して開始した次世代 SupTech ソリューションの開発・テストを行う取組である[33]。

メキシコに対するこのプロジェクトの主な目的は、CNBV の監督活動、特に AML/CFT 分野にテクノロジーがどのように役立つかに関するホワイトペーパーを作成し、CNBV を支援することである。

R2A の調査で明らかになった結果および課題は以下の通り。

- 調査時における CNBV の AML 監督に対するアプローチは、定期的な規制報告に関するオフサイト評価とリスクベースのオンサイト検査を組み合わせたものである。すべての監督対象の事業者が CNBV の VSSP と FIU に定期的に報告書を提出することを求めている。
  - オフサイト評価: CNBV は、監督対象の事業者が、必要な規制報告書の送付、年次 AML/CFT レビュー報告書の送付など、AML/CFT の義務を遵守しているかどうかを検証するためにオフサイトの監督を行う。
  - CNBV が情報を受領した後には、以下のように処理される。
    - 規制報告書(詳細は Appendix VII を参照): 規制報告書は、FIU が事業者に提出を求めているものであり、FIU だけがアクセスできる機密情報である。CNBV は電子プラットフォーム(事業者が報告書をアップロードするためのウェブページ)を提供し、報告書は直接 FIU に送信される。ただし、CNBV は、そこから集約された統計情報のみを収集し、リスクスコアリングモデルに利用している。
    - AML/CFT 年次審査報告書: 非監督対象の事業者は、その年の最初の 60 日間に年次 AML/CFT レビュー報告書を提出しなければならない。提出にあたっては、公認監査人[34]によるレビューを受けなければならない。報告書が CNBV に提出されると、CNBV のスタッフは、報告書が規制のガイダンスに従って作成され、評価の対象となるすべてのトピックを網羅していることを確認するために、手作業で報告書を審査する。報告書を処理するために、CNBV のスタッフは、PDF ファイルにある特定のキーワードを「検索」するなどの基本的な機能を使用する。CNBV は、監査人の指摘事項等があり、これに対処すべき行動計画策定の必要が認められた場合は、対

[33] The RegTech for Regulators Accelerator (R2A), BFA Global, https://bfaglobal.com/r2a/

[34] CNBV が 2015 年に導入した公認資格制度。(Certificación CNBV en materia de PLD/FT (CNBV Certification on PLD/FT), Gobierno de México (Federal government of Mexico), https://www.gob.mx/cms/uploads/attachment/file/720711/CertPLD-MasInformacion_2022_2704.pdf)

象事業者にこれを要請する。

- AML/CFT 方針・手続: 監督対象の事業者は、規制上または業務上の必要性から、方針・手続に変更が生じるたびにそれらを提出しなければならない。そして CNBV は年次報告書と同様、Excel ベースでキーワードを検索する等によって、確認を行い、課題が検出されれば、適宜事業者に勧告を発出する。

➢ オンサイトでの監督は、CNBV が使用するリスクスコアリングモデルによって計画される。このモデルは、オンサイトでの監督で得られた指標や、事業地域の広さ、企業の規模、取引件数などの企業関連情報など、いくつかの情報を考慮する。

- 当時の事業者側でのデータ収集プロセスによれば、関連データは勘定系システムから抽出され、特定の報告要件を満たすようにフォーマットされているため、データ操作のリスク、完全性のリスク、そして最終的には時間のかかるプロセスである。

➢ CNBV のオンサイト訪問では、監督対象の事業者に対して、顧客データベース、取引データベース、アラートデータベースを提出するよう求めている。特定の事業者(例: グローバル銀行)はより洗練されたプロセスを持っているが、監督対象の事業者の約 80%は IT 部門を持っていないため、CNBV のデータ要件は通常、Excel または txt 形式のデータを提供している。データは、CD、USB ストレージ、電子メール経由で提出されるが、例外的なケースもある。

- このように、物理的にはデータの書式がまちまちで、散在しているため、リスクスコアリングモデルを強化するために過去の情報を機動的に利用できる可能性はなく、情報は手作業で処理されている。

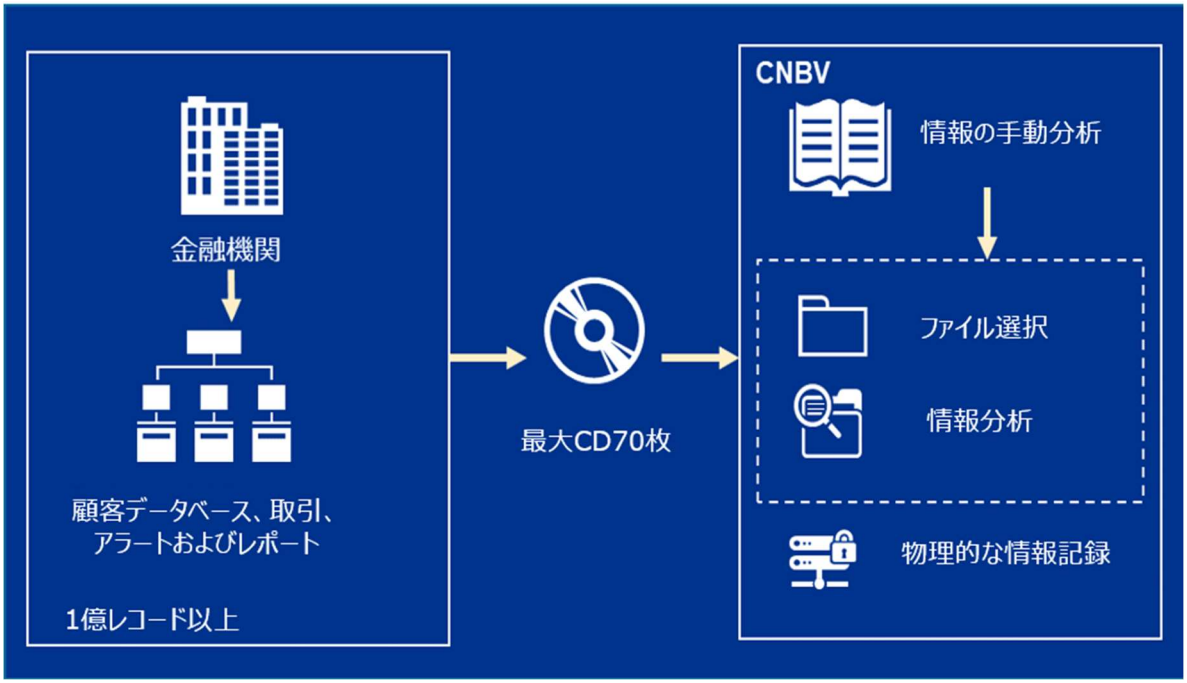


図 11: 現在の AML/CFT フロー(R2A 公式文書情報より)

R2A のホワイトペーパーによると、AML データのアーキテクチャの非効率性は、遅延を引き起こし、より再現性の高い監督業務の妨げとなる恒常的な要因となっている。AML 監督のステップごとの主な問題点は以下の通り。

- データ抽出:事業者は CNBV の報告要件に必ずしも完全に準拠しておらず、不完全、誤った、または形式が不適切な AML レポートを送信することがある。さらに、情報は、長期にわたるオンサイト監督の間に監督当局によって取得されるが、CNBV に戻って初めて確認できる。そこからエラー、データ排出、書式設定を修正するため、データ提出の準備と妥当性確認が著しく遅くなる。

- データ送信:取引データは、監督対象の事業者からの電子メールまたは CD を介してプレーンテキストまたはスプレッドシートで送信される。これにより、送信できるファイルのサイズが制限されるだけでなく、本質的に安全ではなく、例えばファイルを間違った宛先に送信するなどの運用上のリスクも伴う。

- データストレージ:監督対象の事業者の履歴レコードは、現在、約 1,200 枚の CD や紙のファイルを含むさまざまな形式で、整合性のないデータベースに保存されている。これにより、データのダウンロードはほとんどが手作業で行われ、非常に時間がかかる。特定の監督対象エンティティの完全な履歴や、監督対象の事業者のグループ内のグループ各社の情報を繋げて見るためのデータを取得する実用的な方法はない。

- データ分析: 前述した問題点に加え、分析のために記憶媒体を使った「コールドストレージ」からデータを読み込むのは非常に面倒な作業である。ファイルやスプレッドシートのサイズ制限は、より複雑なデータマイニングや予測分析はおろか、粒度の細かい取引データの分析に必要なメモリよりも少ないことが多いため、Excel に依存することも制約のひとつである。また、適用可能な統計モデルと生成可能な可視化のタイプにも制限がある。

上記で述べた R2A の調査で明らかになった課題の解決のために作成された CNBV の SupTech ロードマップには、次の 7 つのステップが含まれている。

① キックオフ: 協力関係の構築とコミットメントの確保

2017 年 2 月に CNBV の代表者が RegTech に関心を持ち R2A にアプローチした際、メキシコの金融当局はすでに、金融包摂戦略、デジタルメキシコ戦略、FinTech 法を含む、コミットメントを強調した多数の好結果のプロジェクトや政策イニシアティブを志向していた。CNBV は中央銀行と協力し、2017 年に FinTech 法を議会に提出した。この法律の目的は、成長著しいメキシコのフィンテック業界に過度の負担をかけることなく、消費者保護を強化し、金融安定化リスクを軽減することである。CNBV により、RegTech の将来のソリューションは、デジタル金融エコシステムを育成するという広範な使命を支えることになるとされた。これらは金融機関からの強力な支持を得た。

② プロジェクト分析

AML ソリューションは、プロジェクト開始時に CNBV と R2A が検討していた RegTech/SupTech プロジェクトの 1 つである。その他のユースケースには、金融サービス事業者のライセンスを管理するためのツールや、既存の健全性報告システムをアップグレードするためのツールが含まれていた。R2A は、技術者、政策専門家、CNBV の利害関係者と議論を重ね、複数のユースケースを、期待される効果、技術的および運用上の実現可能性、全体的な戦略的適合性の観点から評価した。

技術業界で広く採用されている分析フレームワークは、問題点とそれに対応する技術的な改善効果という観点からソリューションの価値を明確にするのに役立った (下図参照) 。検討した結果、AML ソリューションが優位だった。特に、苦情処理の合理化によって効率性が向上したことで、他のプロジェクトに振り向けることのできるリソース

が大幅に解放された。さらに、その新規性を考えると、RegTech/SupTech の変革の力を実証し、示すのに役立つ可能性がある。

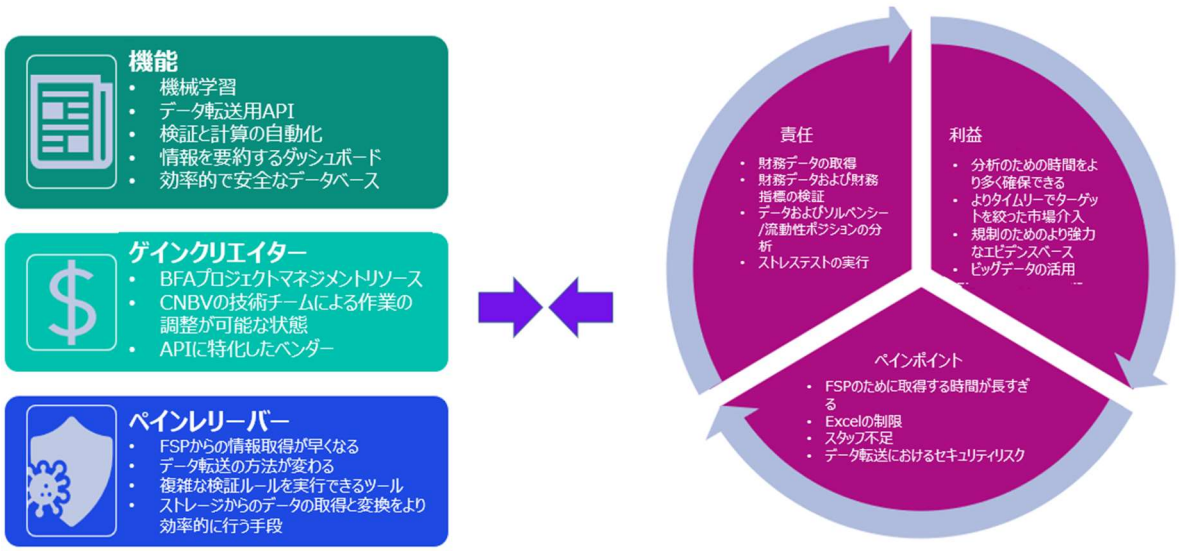


図 12: R2A による提案(R2A の情報より KPMG メキシコ作成)

③ プロジェクトの立ち上げ

すべてのステークホルダーのコミットメントを確保し、ユースケースに合意した後、次のステップは、R2A と CNBV のチームの作業範囲と作業レベルを示すプロジェクト計画を作成することだった。その中で、CNBV と R2A は、14 ヶ月の間に市場に出せる AML 監督ソリューションのプロトタイプの設計、開発、テストに協力することに合意した。プロトタイプではあるが、より広い市場に展開する際の実行可能性、拡張性を評価することを企図したものである。

また、このプロジェクトにおいては、プロジェクトの関係者に役割と責任を含めたプロジェクト憲章を明確に定めた。R2A は、設計と開発を指導する技術専門家や、効果的な導入作業を進め調整を行うプロジェクトマネージャー、およびベンダー選定プロセスと落札のためのノウハウ等を提供した。CNBV は、プロジェクトのスポンサーとして、プロジェクトの戦略的方向性を示し、主要なマイルストーンを承認する役職者(エグゼクティブチャンピオン)、日々の活動を管理するマネージャー、R2A チームおよびベンダーとの連絡役を務めるプロジェクトリーダーを任命した。

④ 設計/構築/PoC(実証実験)

この段階では、R2A チームはその後の開発作業のための大まかな青写真を描くことを目的とした「デザインスプリント」を実施した。このとき CNBV は、データ収集に API を、保存に SQL データベースを使用するプロトタイプをすでに構想していた。既に標準化され、ベストプラクティスとして広く認められているこれら 2 つの技術を、本件目的のために適用し、CNBV の厳格なセキュリティ・プロトコルを充足させることがこの PoC の目的であった。

R2A の技術者と政策の専門家は、CNBV と密接に協力して、データアーキテクチャ、データセキュリティ、可視化に関するニーズと要望を、将来の開発者が理解しやすいように具体的な機能・技術仕様に変換した。中心となる機能要件は以下の通り。

- 監督対象の事業者へ標準化された自動リクエストを生成し、そのレスポンスを API 経由で受け取り、中央データストアに送り込むための中央プラットフォーム。

- 「コールド/物理ストレージ」から既存の履歴記録を中央データストアにインポートするためのプロセスとメカニズム。
- 時系列での制度の変化やグループ内の全主体の分析に焦点を当て、中央データストアから主要な指標を分析・提示するための最先端の分析ツール(例: アルゴリズム、通知、ダッシュボード)。

これらの基本コンポーネントに加え、CNBV と R2A のスタッフは、新たに最適化されたプラットフォームに保存されることになる大量のデータを活用できるようにするための、追加の分析アプリケーションを検討した。機械学習モデルやデータフィルタリングツール[35]によって、CNBV のスタッフが疑わしい金融取引を検知し監督する能力を強化する可能性がある。

⑤ リソース調達―ベンダーの選択

R2A チームが共同作成プロセスで果たす重要な役割の 1 つは、プロトタイプを仕様にまとめる有能なテクノロジーベンダーと金融機関を連携させることである。このためには、表彰歴、ハッカソン/ブートキャンプの実施など、さまざまな選定方法が考えられる。CNBV のプロジェクトでは、提案型ソリューションの機能要件とセキュリティ要件が比較的厳しく、提案依頼書(RFP)方式が適切であると判断された。R2A は 10 万米ドルの助成金のための国際入札を手配した。この助成金で、スタッフの作業時間、ハードウェア、ソフトウェア、出張費、その他プロジェクト関連のすべての費用を含む、開発およびテスト作業に関連するすべての費用がカバーされる。

⑥ プロトタイピング―反復的なテストと開発

青写真が手元にあり、開発チームの準備が整っていれば、プロトタイプを構築する実際の作業を始めることができる。Gestell (選定されたベンダー) は、ステップ④で CNBV と R2A によって作成され、RFP で詳述された技術仕様と機能仕様に従い適切なテクノロジーコンポーネントを選択した。まず、API をクライアント側のソフトウェアと統合する必要があり、次に、ダミーデータを使用したバックエンド統合と API ストレステストが必要だった。

特に重点を置いたのが、暗号化とストレージコンポーネント、およびデータ分析と可視化ダッシュボードのユーザーインターフェースである。すべての部品が組み立てられた後から、データストリームを有効にして機械学習モデルが適正に稼働するかの確認ができる。参加した金融機関からのパイロットデータを使って何度かテストを繰り返した後、プロトタイプは次のステップへ進む準備が整った。

⑦ 製品化

R2A プロトタイプがすべての利害関係者の満足のいくように開発されると、その製品を大規模に採用するかどうかについて、ベンダーと財務当局の間で決定が下される。メキシコのケースでは、ライブデータを用いた繰り返しテストにより、AML ソリューションの実現可能性と付加価値が明確に実証されており、CNBV はこのソリューションを全国的に展開する方法を模索し始めた。

その結果、データリクエスト API(CNBV から監督対象の事業者へ)とストレージプラットフォーム、および消費者を保護し金融システムの安定性を守りながら新しいフィンテックを受け入れることができる AML 監督のためのアーキテクチャが完成した。これは、API やダッシュボード(分析)などの技術を使用し、すべての規制報告書の「オンライン」監督を行い、監督対象の事業者のリスクが高いことを意味する可能性のあるアラートを早期に取得するために行った。R2A の設計開発プロセスから生まれたプロトタイプは、API ベースの AML データのアーキテクチャと AI 駆

[35] 機械学習モデルに基づいて、最も関連性のある情報をユーザーに提供するツール。

動の分析ツールであると位置づけられる (下図参照) 。

これは、既存のレポートシステムのさまざまな問題点を対象として、ライセンスフィーが発生しないオープンソースのテクノロジーの組み合わせで構成されている。

両者は協力して、(1) 伝送、(2) 処理、(3) 保管、(4) 銀行の取引データの分析、のための一貫性のある合理化されたアーキテクチャを形成した。このセクションでは、これらの技術的なレイヤーを色分けし、レポート作成プロセスの重要な側面を合理化および自動化することで得られる効率性の向上について説明する。

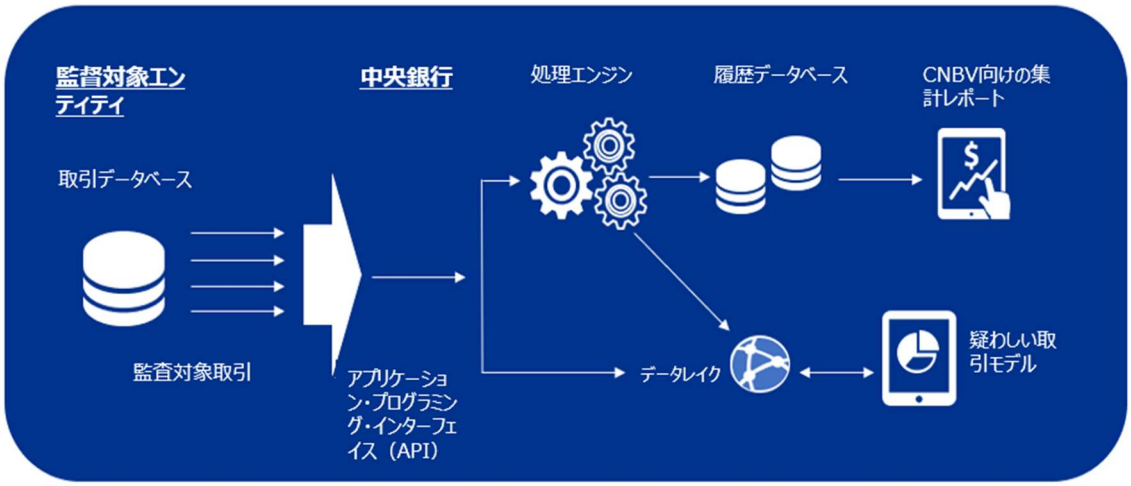


図 13: R2A/CNBV― AML データアーキテクチャ(R2A の公表文書より)

R2A が説明するプロトタイプの主な構成要素は以下の通り。

(1) 伝送―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、監督対象の事業者の取引データベースと CNBV の処理エンジンの間で、安全かつ直接的にマシンからマシンへのデータ伝送ラインを確立するものである。生データは CNBV のシステムに直接送信または CNBV のシステムによって引き出され、監督当局は生データだけでなく疑わしい取引も選択できるようになり、スプレッドシート・テンプレートの作成、電子メールや CD によるデータの共有が不要になった。これにより、これまで数日、数週間かかっていたデータ収集が、数秒で完了するようになった。

(2) 処理―処理エンジン

処理エンジンがデータを受け取り、即座に検証テストを実行し、レポートの品質、内容、構造を確認する。不正確なレポートや不完全なレポートは、自動的に拒否される。処理エンジンを 1 つ持つことで、数式が矛盾していたり、壊れていたり、古かったりする可能性のある別々のスプレッドシートではなく、すべてのテストが一律に実行されることが保証される。また、Excel では不可能な複雑な数値計算が可能になり、処理時間が大幅に短縮される。

(3) 保管―データベース

処理されたデータは、元の生データや AML モデルの出力データとともに、「データレイク」に保管される。CNBV のプラットフォームで流れているすべての情報を保持することで、すべての変換を元のソースにさかのぼって行うことができるようになる。

このデータレイクは、履歴データウェアハウス(レポーティングと分析のために「処理済み」データを保存する SQL データベース)の準備エリアとしての役割も果たしている。旧システムでは、データはバラバラのデータベースや物理的な書類棚に格納されたが、このアーキテクチャでは、アクセスが制御された単一のストレージプラットフォームに統合されている。プラットフォーム全体のデータの流れは、エッジコンピューティングの数式によって自動的に制御されるため、手作業を排除し、ソリューションの効率性をさらに高めている。

(4) 銀行の取引データの分析―分析ツール

中央で管理されたウェアハウスにより、AML に活用できる分析・可視化ツールの種類が大幅に増加する。このソリューションで採用されている分析ツールは以下の通り。

- 顧客、商品、取引の種類ごとに各金融機関の AML リスクエクスポージャーを可視化するダッシュボード: ダッシュボードのレポートは新しい情報が入ると自動的に更新され、CNBV は AML リスクの状況をほぼリアルタイムで把握できるほか、基礎データについて掘り下げたり、エクスポートしたりすることが可能である。
- クラスタリング、ニューラルネットワーク(NLP)、ロジスティック回帰、ランダムフォレストなどの予測分析および機械学習技術を使用して疑わしい取引を検出する人工知能(AI): これにより、CNBV は人間の目には見えないパターンや関係を見つけ出し、マネー・ローンダリングが行われる前に阻止できる可能性がある。(注: NLP やランダムフォレストなどの機能は実証実験に使用されたにすぎず、さらなる発展が必要ではあるが、一般的なアイデアとして含まれると判断された)。
- 金融機関の根本的なリスクエクスポージャーに基づき、AML 手続/アラートを推奨できる機械学習モデル: 例えば、信用組合が商業銀行と同じ AML リスクを抱えている場合、その AML モデルや手続きはそれに応じて適応されるべきである。初期のデータマイニングの結果、現在のリストに追加可能な 12 の新しい取引アラートが得られた。
- 金融機関の顧客と監視リスト上の個人(例: PEPs、外国資産管理局(OFAC)による制裁を受けた個人)を自動的に相互参照する監視リスト・トラッカー。

3.4 CNBV における最新の SupTech の状況

3.4.1 CNBV の AML/CFT の SupTech フレームワークと、BIS の SupTech フレームワークの比較

既述のとおり、CNBV は SupTech の開発を進めているが、まだ実装には至っていない状況にある。

以下の表は、「3.1.2 SupTech BIS フレームワーク」で述べた BIS フレームワークを用い、KPMG メキシコが CNBV の現状を評価したものである。

コンポーネント	評価結果
収集	・ 報告書、AML/CFT 方針・手続、AML/CFT 年次レビューなど、構造化情報と非構造化情報双方の収集は、SITI AML/CFT などの従来の Web ポータルにおける情報の手動でのアップロードによって行われており、非効率性が生じている。このコンポーネントは 2G レベル(プラットフォームロードまたは大量ロード)と位置付けられる。 ・ なお、SupTech プラットフォームとして API を介して行われる収集部分に関する開発中の案件は、3G レベルのビッグデータアーキテクチャに位置付けられる。(開発対象は銀行セクターのみである)
処理	・ SITI AML/CFT ポータルには、主に規制当局の報告書に関連する自動化された検証プロセスがいくつかあるが、AML/CFT 方針・手続や AML/CFT の年次レビュー報告書などの重要な処理の大部分が引き続き手作業で収集されていることから、SupTech の処理レベルは 2G と考えられる。 ・ 将来構想として示されているロードマップとしては、情報を直接かつ自動的に処理することを目指しており、これが実現すれば 3G レベルのビッグデータアーキテクチャとして位置付けられる。
保存	・ CNBV はデータレイクを含む 3G ストレージメカニズムを開発したが、これらは SupTech ダッシュボードにその利用が限定されている。それ以外の情報は、構造化情報および非構造化情報の両方で、個々の独立したデータベースや物理的な形式で保存されていることから、このコンポーネントは 2G レベルである。 ・ 一部の情報のストレージはクラウドやデータレイクといったストレージモデルに未接続であり、BI ツールで処理できるような機能情報に変換するための追加手順が必要である。
分析	・ このコンポーネントは 2G レベルのデータアーキテクチャとなっている。3G の分析を実行できる特定の SupTech ダッシュボードと BI ツールを使用できるが、これらは純粋に API を介したオフサイト監督(顧客データベース、トランザクション情報の収集など)の一部として要求された情報を利用することに焦点を当てており、CNBV が追加またはオンサイト監督(AML/CFT 方針手続、AML/CFT 年次レビュー報告書、その他)で受け取る構造化された情報や構造化されていない情報を分析するために拡張されていない。 ・ 手作業による情報分析は、依然として AML/CFT 監督局における情報分析のためのメカニズムの重要な一部であり、データの背後にあるアイデアへの気づき等は職員の作業に大きく依存している一方、情報量が多いため、全体から得られる知見とその活用の機会を著しく阻害している。結果として(全体構造をとらえるような関連性の高い知見の集合ではなく)個別性の強い狭い領域での知見や個々のセクター固有の小さな問題のみに焦点が当たりがちである。 ・ CNBV が他の行政機関からの情報を利用できるようにする(例えば、行政省の公務員のリストにアクセスできる API を確立すること等)には大きな課題がある。
可視化	・ CNBV は、より動的な分析やデータ可視化を支援するために BI ツールを実装した SupTech ダッシュボードを開発したが (3G レベル) 、対象は、一部に限られ、ほとんどの構造化情報および非構造化情報の可視化を可能にする技術ツールがない。分析と報告のほとんどが未だに集約情報中心であることから 1G レベルと言わざるを得ない。

3.5 認識されている課題と教訓

3.5.1 CNBV からの教訓

CNBV の元職員へのインタビューによると、CNBV は、投資と開発の効率性を得るために、金融機関に対しセクターに関わらず RegTech ソリューションを実装することを求めている。CNBV は、RegTech が存在しない環境では SupTech が存在できないことを認識しており、そのためこの連携が重要な鍵を握っていると考えている。一例として、CNBV は、いつ、どのように登録情報を更新しなければならないかをサポートする共有ツールの開発を提案している。

CNBV は、SupTech ツールを開発する際に、すべての事業者の協力が不可欠であると考えている。このような協力の下に、結果として、各事業者の開発コストが削減され、同時に、CNBV は事業者のノウハウを効率的に活用し、セクター全体にわたるプロアクティブで洞察力のある監督に注力することができるようになることを期待している。

3.5.2 監督対象事業者からの教訓

メキシコに支店を持つ国際的な銀行、送金業者、為替業者にインタビューを行い、各セクター固有の状況を把握した。技術的な課題は各セクターで異なるものの、サイバーセキュリティ、投資、顧客識別のための公式データベースがないことなどが共通の課題として挙げられた。

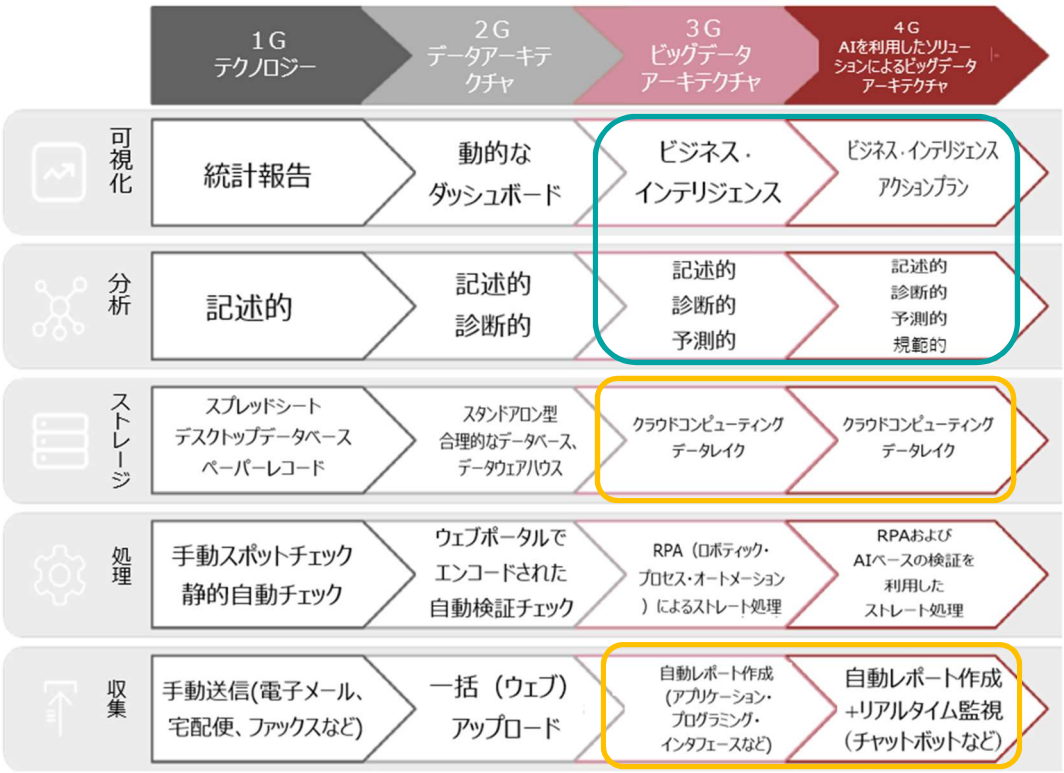
各インタビューのポイントは以下の通り。

- 銀行の場合: 主な懸念事項の 1 つは、SupTech のプラットフォームのサイバーセキュリティへの投資である。特にこの銀行では、技術開発は海外にある本社の承認が必要であり、メキシコのローカル API 経由での情報共有が、本社が求めるセキュリティ基準に照らして承認されないという潜在的な課題があると言及された。
- 送金業者の場合: インタビューを行った事業者は、RegTech 環境の整備を進め、取引モニタリングシステムを強化している。この実装では、高度なアルゴリズムを使用し、誤検知を減らしているが、第一線のオペレーターによる顧客データの誤認識が課題として残っている。また、公的な国民 ID データベースが存在しないため、オンラインで本人確認を行う手段がないことも課題となっている。
- 両替商の場合: このセクターが直面している主な問題は、法律により現金での取引しかできず、取引のほぼ 9 割が顧客 ID を必要としないことである(法律では、基準額は 500 米ドル以上)。さらに、これらのビジネスはほとんどが家族経営であり、義務的でない規制のための投資が非常に制限されている。

それ以外、一部のセクターは技術的な環境の整備を進め、いくつかの改善が見られるものの、メキシコの企業は、G7 内の銀行など、より進んだ企業との間に依然として大きな格差がある。これらの銀行がインターネットやソーシャルメディアを通じてネガティブメディアの調査を行っている一方で、メキシコの両替商や送金業者は、誤検知を減らすために取引モニタリングシステムをどのように調整するか、まだ苦労している。国内と海外の事業者の違いは大きく、CNBV もまた、監督対象の事業者全体に共通するこの種の課題に直面し続けている。

4 我が国への示唆

本稿で示した事例は、メキシコで示したバーゼルのホワイトペーパー「The SupTech Generations」の枠組(以下に再掲)で位置づけを整理すると以下の通りとなる。



オランダ、メキシコ共に共通するのは、事業者からの情報収集について、中央データベースないしはデータレイクを用意し、これに事業者からの高粒度情報を収集・格納するというものである。(上図　　)

さらに、メキシコについては実験段階ではあるものの、これらの収集データを活用して、分析・可視化する領域に踏み込んで取り組んだものである。(上図　　)

監督対象事業者からの情報は、現状、表計算ソフト等のプログラムファイルや PDF 形式[36]で収集されることもあれば、紙ベースの場合もある。前者であってもデジタル的に処理、活用される度合いは低く、モニタリング業務においては、主に目視による精査という形で処理されている部分が多いと想定される。(上図の 1G レベル)

このような現状から踏み込み、表計算ソフト上の様式を統一化し、これをデータベース化し、さらには横断的な分析処理を行うという取組(上図の 2G レベル)も見られる。ただし、この場合は、ファイルとして提出されたデータの品質に少なからず課題[37]があり、デジタル化の取組を著しく阻害している。収集されたファイルを基に、RPA 等を活用した自動化の試み(上図で言えば、処理のレイヤー)が、必ずしも成果を挙げられないのもこう言った要因によることが多い。

オランダ、メキシコでの取組を踏まえ AML/CFT の規制・監督に関する事業者からの情報の流れでは、以下の観

36 PDF 形式でもたとえば、デジタル的に文字や数値情報が認識できないものも少なくない。

37 数値データでの入力を期待しているところ、文字として入力されたり、数値として入力されていても、その後に文字情報で補記説明が付されていたり、単位が異なっていたり、といった問題に直面することが多い。

点が有益であると考えられる。

1. 当局としての期待目線が、ガイドライン、FAQ 等と精緻化されてきたことに鑑み、これらと整合的、かつ検証可能な形で事業者から徴求すべき必要情報を適時確認すること
2. 特に、集約された情報ではなく、高粒度[38]の情報収集という観点
3. 一事業者毎の精査というモニタリング業務は引き続き重要[39]であることに加え、収集情報のデジタル化とその横断的な活用という観点[40]
4. 一方で、事業者のリスク評価等の非構造情報も、引き続き価値のある情報であり、これについてもテキストマイニング手法やその他のメタ情報を活用した定量的なクラスタリング、スコアリング手法を適用し、目視による精査とあわせて全体の品質向上を必要に応じて検討すること[41]

また、以下のような取組についても必要に応じて検討することが重要であると考えられる。

1. 徴求情報についてデータ・モデルという観点からの現状調査(表計算ソフトウェア等を中心に利用していること等に起因するデータ品質上の課題整理や、徴求情報が本来のガイドライン規定事項達成を測るうえで適切なものとなっているかの確認等を含む)
2. 現状、横断的な取組(リスクレーティング等)において、徴求情報がどの程度活用されているか、当該情報や、分析評価手法が、本来の目的に照らしてどの程度適切かの検証
3. 適用可能な技術要素の研究と上記 1, 2 を踏まえた今後の方向性の整理と、事業者リスク評価モデルの構築[42]
4. 非構造データ(例: 事業者のリスク評価書)について、テキストマイニングあるいは機械学習等を活用したクラスタリングやベンチマーク分析の試行

---

38 現段階で、個別取引までさかのぼることは現実的ではないが、たとえばガイドライン項目についてギャップの有無というハイレベルな情報ではなく、ギャップの有無を判断する根拠となるようなレベルに情報(できれば事業者の判断に依拠するのではなく、事実関係確認するような形)を細分化する、といったようなことが想定される。

39 バーゼルの枠組では、分析のレイヤーでの 1G から 2G にかけての取組と位置付けられる。

40 多岐に渡る徴求データにつき、生データレベルとするもの、要約データ（KPI 的なもの）とするもの、数値のレンジ設定、あるいは自由記載の類型化指定等で、パラメータ化して回答させるもの、自由記載項目の要否等について、どのような分析を行うのか、どのようなツールを利用するのか等、継続的な PDCA の枠組みは有益であると考えられる。

41 当局ガイドラインとの整合性、NRA との類似性、事業者同士の類似性等といった仮説を立てて、テキストマイニング技術を活用して、事業者のリスク評価書を横断的に類型化、スコアリングに役立てるといったことが有益であると考えられる。

42 たとえば、別途検討されている共同データプラットフォーム(「共同データプラットフォームの構築に向けた基礎調査」報告書の公表について，金融庁 (fsa.go.jp), https://www.fsa.go.jp/common/about/research/20220413/20220413.html)の 1 ユースケースとして取り組むこと等も想定される。

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。

Appendix

Appendix I: Sources used

Note that the list below is not aligned with the footnotes in the report, as duplicates have been removed from this list.

1 Regeling kansspelen op afstand

2 Specifications for the remote gambling data safe (the CDB)

3 Algemene wet bestuursrecht

4 Wet op de kansspelen

5 Besluit kansspelen op afstand

6 Regeling kansspelen op afstand

7 Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)

8 Sanctiewet 1977

9 Guideline Wwft

10 Data model for the CDB

11 Onderzoek Online Markt Kansspelen Eindrapport – Boston Consultancy Group (2011)

12 Bouwen aan de KSA 2.0 - Berenschot

13 Modernization of Games of Chance by Gambling Compliance
https://zoek.officielebekendmakingen.nl/blg-489682.pdf

14 Technical requirements – online casino and betting - Spillemyndigheden

15 Wijziging van de Wet op de kansspelen, de Wet op de kansspelbelasting en enkele andere wetten in verband met het organiseren van kansspelen op afstand

16 Response of the European Gaming & Betting Association

17 Raad van State on Besluit kansspelen op afstand.

18 Response to the advice of the Raad van State

19 The implementation of AMLD 5 into Dutch legislation – KPMG (2020)

20 KSA annual report 2021 (in Dutch)

21 Vragenformulier CDB – KOA Aanvraag

22 Draft Remote Gambling Assessment Scheme (Remote gambling conformity assessment scheme)

23 Leidraad Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)

24 Setting up and managing the CDB

25 Online games of chance providers are still insufficiently complying with Wwft obligations

26 Transaction Monitoring Netherlands – About us

27 Wet plan van aanpak witwassen

28 German gambling law – Update 2020/2021

29 Onlinebank Bunq voert ongekend felle strijd tegen DNB over witwasregels

30 The JFSA Strategic priorities – July 2021 – June 2022

KPMG

Appendix II: Essential features of a SupTech model

SupTech tools potentiate analysis, supervision and surveillance capabilities through on-demand and real-time analysis of critical risk indicators, enabling prescriptive supervision mechanisms and allowing the development of public policies that consider the emerging risks derived from new business models and technological enablers.

The use of technology to automate the generation of reports from the integration of data from different sources is only the beginning, however, SupTech solutions must have at least the following characteristics to truly provide valuable and actionable information through efficient mechanisms:

- **Data Entry Approach:** Supervised institutions should automate the submission of data in standard and highly granular formats according to the specifications required by the supervisory authority and submit it through secure channels.
- **Data validation approach:** Automated data validation should be performed through data receipt checks, data integrity checks, data correctness checks, and plausibility and consistency checks.
- **Data Mining Approach:** Use of automated processes, activated, and controlled by the supervisor, to collect and standardize raw data directly from the entities operating systems.
- **Data aggregation approach:** The data information sent by entities (push) and/or automatically extracted by supervisors (pull) must be integrated into centralized repositories that have structures that allow different granularities to be analyzed, from transactional data (detail by entity) to the aggregation of data to explore different dimensions (grouping by type of institution/ risks, global indicators).
- **Organization of data types:** The data must be classified and categorized according to the needs of the different participating areas and their structure. These data can be Structured and Unstructured and should be categorized into 1. Regulatory Consumption, 2. Statistical Description, and 3. Market Behavior.
- **Dynamic and predictive supervision:** Adoption of mechanisms that allow supervisors to generate information on demand (pull), creating independence of entities and enabling prescriptive and preventive supervision models.
- **Real-time access:** Supervisors can extract or 'view' operational data at will (instead of waiting on predetermined reporting periods) by directly accessing institutions' operating systems, which could enable real-time supervision.
- **Information utilities:** Centralized structures that function not only as a common database to safeguard reported granular data, but also as a repository for the interpretation of information standards, in a readable format, that is, semantic information utility.
- **Gather intelligence from unstructured data:** Gather and analyze unstructured data more efficiently, which could free supervisors from time-consuming tasks such as reading numerous PDF files, Internet searches, and others.
- **Regulatory submissions and data quality management:** Fully automated procedures to manage data submission and quality by entities, including validation testing of reported data.

Appendix III: Summary of SupTech strategies from regulatory agencies

From the analysis of some case studies of advanced geographies in this type of mechanism such as the Monetary Authority of Singapore, the Financial Services Agency and the European Central Bank, the strategies focus on enabling the following components:

- Institutional evangelization through the sponsorship of Presidents and Vice Presidents.
- Implementation of a Data Governance at an Institutional level commanded by the Chief Data Officer.
- Development of centralized information repositories with specific structures for the needs of each of the business areas within the supervisory entities.
- Technology training and ongoing training programs for front line supervisors as end users of the tools.
- Attraction and retention of professionals with the necessary skills and capabilities for the development, implementation, maintenance, and improvement of these mechanisms, increasing the chances of success in integration and adoption.
- Establishment of regulatory Sandboxes as an intra-entrepreneurship mechanism, to support new business models, early identification of emerging risks and experimentation with new tools and technologies to observe viable initiatives and rule out exercises of little value.

—

Appendix IV: Benefits, challenges, and risks

The implementation of innovative mechanisms by supervised entities and supervised institutions allows efficiencies from the automation of manual processes and the directed and actionable use through monitoring and risk management. With these advantages come equally significant challenges, as regulators must constantly understand and observe the new challenges arising from the use of disruptive technologies, some even unknown at the time.

Benefits

- **Potentializing capacities:** Integration of high volumes of structured data and new sources of unstructured data, identification of detailed performance by type of risk and institution, and early identification of possible problems and irregularities before they materialize.

- **Reduction of operating costs:** optimization of operating processes, reduction of infrastructure and legacy and satellite systems, as well as reduction of the workforce.

- **Exception-Based Monitoring:** Automated checks on entity data and other information automatically collected and analyzed to identify "exceptions" or "outliers" against predetermined parameters.

- **Automated application of supervisory measures:** Trends created automatically to facilitate decision making, for example, capital increases based on automated data analysis.

- **Algorithmic regulation and supervision:** It can be used for the supervision of activities related to high-frequency trading, algorithm-based credit rating, robo-advisors or any service or product that automates decision-making.

- **Efficiency:** It can reduce compliance costs for the regulated entity and improve risk management, benefiting the stability and efficiency of the market. Regulatory technology can promote the standardization of the interpretation of regulations and improve the management of deadlines.

- **Support for innovation:** The mandates of many regulators include the promotion of innovation. By identifying adequate technologies, supervisors can help companies allow better manage regulatory requirements.

  - **Real-time supervision:** Supervisors can monitor data as it is created in the operating systems of regulated institutions, strengthening their presence and impact.

Challenges

- **Integration of external sources:** The integration of data from external sources such as sites and databases of other government entities, open data generated by citizens and ONGs enriches and contextualizes indicators, however, access to it is complicated by its unstructured nature or no granular correspondence. Its integration requires risky mechanisms such as web scrapping, natural language processing and the establishment of advanced structures such as data lakes.

- **Legacy system problems:** It is relatively simple to build SupTech systems within a new or recently created Authority, however it becomes difficult to do in existing systems and Authorities, mainly due to supervisors' resistance to change, data migration and stability, among others.

- **Data quality problems:** Complexity when analyzing or validating the Big Data collected from non-traditional information sources, such as, for example, the data contained in social networks.

- **Resource issues:** Supervisors may face budget constraints, and even a lack of qualified staff to deploy SupTech applications.

Risks

- **Legal risk:** Supervisors should be aware of existing data protection laws in jurisdictions, given the ongoing collection and availability of more data from alternative sources.

- **Operational risk:** A greater number of data means that Entities and supervisors have become more attractive targets for cybercriminals and may require stricter cybersecurity measures to detect any form of attack.

- **Reputational risk:** Inadequate validation of the data by SupTech applications, for example, a failure of the algorithms, can lead to misinterpretation and possible inaccurate supervisory actions. This can affect the reputation of both the Entity and the supervisor.

- **Cyber security risk:** Increased vulnerability given the interconnection and creation of communication channels between supervisors and entities. The involvement of third parties such as infrastructure and platform providers increase the chances of breaches, information theft and cyber-attacks.

- **Third-party risk:** The need to rely on providers of cloud infrastructure, specialized hardware, legacy software, and development of platforms parameterized to the needs of regulators according to local criteria, represent dependency and concentration risks.

- **Counterpart risk:** In the process of implementing SupTech solutions, regulators face the risk that RegTech mechanisms do not exist in the sector or that the regulated entities do not have the corresponding technological capacity, which can not only cause not only losses derived from deficient extraction processes or incomplete information analysis to possible breaches for the entities.

- **Model risk:** In the development of analytical models there is a risk that they may reflect the biases of the teams that design, implement or train them, which may lead to a lack of confidence or methodological accuracy regarding the conclusions or results.

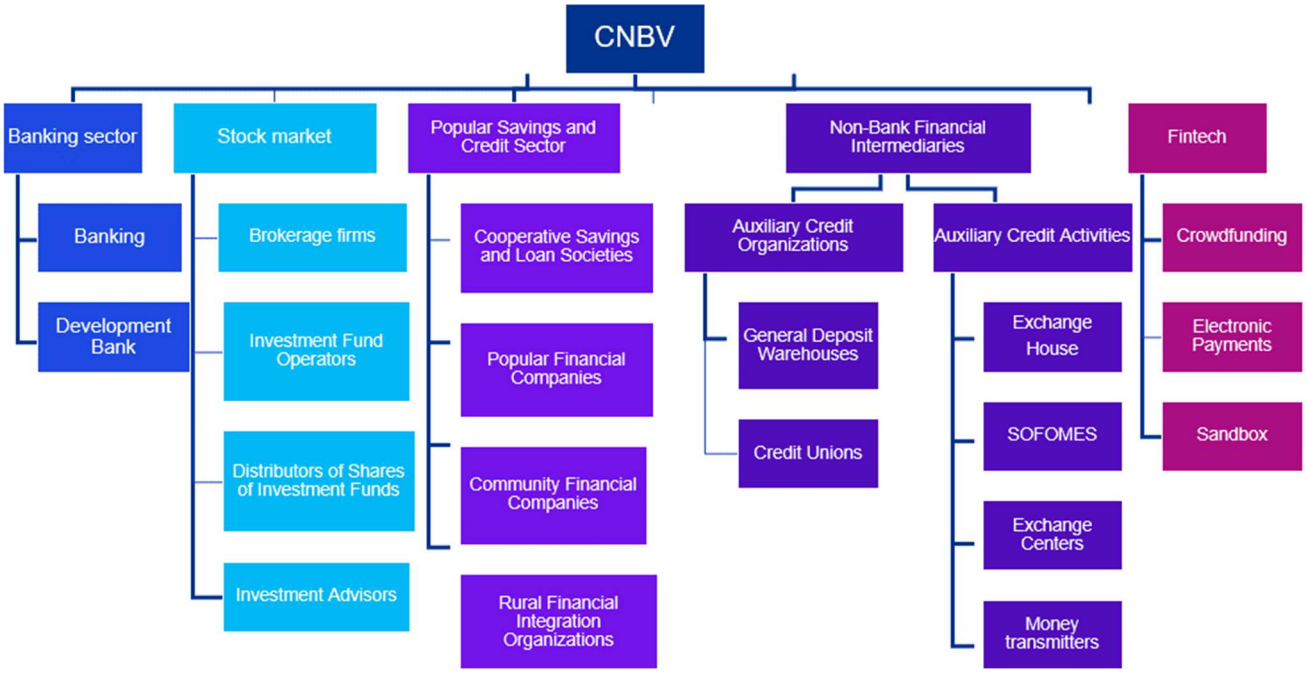
- **Ethical risk:** Analytical models must follow the principles of transparency, auditability and explainability.

- **Transparency:** ability to describe, inspect and reproduce the mechanisms and data used.

- **Auditability:** ability for an external entity (regulator, external auditor) to review the details of the development of an algorithm without compromising intellectual property.

- **Explainability:** ability to expose the reality regarding the results of the algorithm in a way that can be easily understood.

Appendix V: CNBV AML/CFT supervised sector



Appendix VI: AML/CFT Vice-presidency tasks and organization

The VSSP is divided into two main offices (AML/CFT oversight office A and B), which supervise the AML/CFT compliance of the sectors as follows:

Attributions of the AML/CFT oversight offices:

- Within the powers of the AML/CFT oversight offices are those described in article 43 of the Internal Regulations of the CNBV, highlighting the following:
  - Supervise through inspection visits or surveillance actions that the supervised entities comply with what is established in the AML/CFT rules.
  - Impose administrative sanctions on supervised entities.
  - Receive through the SITI, information related to various reports that the supervised entities must send to the SHCP, acting as a technological bridge to immediately transmit said information to the FIU.
  - Issue an opinion to the Secretariat regarding the AML/CFT rules, as well as the proposals and consultations formulated by the supervised entities that imply the issuance of interpretation criteria regarding what is established the AML/CFT rules.
  - Issue the AML/CFT certification for independent auditors, compliance officers and other professionals.
  - Ensure that the list of blocked persons is available to supervised entities.
  - Issue the technical opinion for exchange centers, money transmitters and SOFOMES (ENR).
  - Issue guidelines, best practices, criteria, directives, guides, and other provisions for proper compliance with the AML/CFT rules.
  - Monitor that the information exchange mechanisms between credit institutions and foreign financial entities are carried out in an orderly manner.

- Maintain communication with the supervised entities to understand and communicate areas of opportunity and improvement, improve understanding of the risks, and guide them in the fulfillment of their AML/CFT obligations.

Appendix VII: AML/CFT structured and unstructured information

AML/CFT Oversight Office B

Information Received	Platform	Timeframe
AML / CFT P&Ps	SITI AML/CFT Email	• 20 business days after approval of changes • Along with registration request • Per event based on the annual supervision program • In cases of visits or special supervision
Risk Based Approach Methodology	SITI AML/CFT	• 20 business days following the approval of the AML/CFT Manual
AML/CFT anual Review Report	SITI AML/CFT	• 60 calendar days following the end of the fiscal year
AML/CFT Risk Model Results	Email	• Applicable only to Credit Financial Institutions (Bank), 60 business days of each year
Information on the Communication and Control Committee	SITI AML/CFT	• 15 business days following the date of integration or changes
Compliance officer	SITI AML/CFT	• 2 business days after appointment. • Interim and Revocation: next business day
Identity of the person or group of persons exercising control	SITI AML/CFT	• Applicable only to exchange houses, SOCPAS, SOFPIPOS and SOFOMES ER, 10 business days following which the Administration is notified
Share transfer for more than 2%	SITI AML/CFT	• Applicable only to exchange houses and SOFOMES ER, 3 business days following their registration in the Public Registry
Information exchange agreement	SITI AML/CFT	• Applicable only to General Warehouses companies, Credit Institutions, Brokerage Firms, Investment Advisors and SOFOMES ER, prior to exchanging information
Transaction Reports* and their evidence	SITI AML/CFT Email	• According to each term established in the Corresponding Provisions • Per event based on the annual supervision program • In cases of visits or special supervision
Response to information requests	Email	• According to each term established by the CNBV
Databases of clients, users, operations and alerts	Suptech platform	• Per event based on the annual supervision program • In cases of visits or special supervision
Identification files	Email	• Per event based on the annual supervision program • In cases of visits or special supervision
Different acts	Email	• Per event based on the annual supervision program • In cases of visits or special supervision
Images of system tests	Email	• Per event based on the annual supervision program • In cases of visits or special supervision
Questionnaire of transactions	Web Portal	• At the request of the CNBV, generally on an annual basis.

*See section "Operations Reports"

AML/CF Oversight Office A

Information Received	Platform	Timeframe
AML / CFT P&Ps	SITI AML/CFT Email	• 20 business days after approval of changes • Together with the request to obtain or renew the Technical Opinion • Together with registration request* • Per event based on the annual supervision program • In cases of visits or special monitoring
Risk Based Approach Methodology**	SITI AML/CFT	• 9 months after the 2019 Reform • When there are updates to the NRA and the CNBV requests it • Along with registration request*
Information on the Communication and Control Committee**	SITI AML/CFT	• 15 business days following the date of integration or changes
Compliance officer**	SITI AML/CFT	• Exchange Center, Money Remitters and SOFOM ENR: 2 business days following the designation. • Financial Technology Institutions (FINTECH): 10 business days after appointment
AML/CFT anual Review Report	SITI AML/CFT	• 60 calendar days following the end of the fiscal year
Identity of the person or group of persons exercising control	SITI AML/CFT	• SOFOMES ENR and Money Remitters: 10 business days after the Company's Administration is notified • Exchange Centers: 20 business days after the Company Administration is notified
Share transfer for more than 2%	SITI AML/CFT	• 3 business days following its registration in the Public Registry
List of related agents	SITI AML/CFT	• Applicable only to Money Remitters, 15 business days following the beginning of the fiscal year
Information exchange agreement	SITI AML/CFT	• Applicable only to Financial Technology Institutions (FINTECH) , prior to exchanging information
Transaction reports*** and their evidence	SITI AML/CFT Email Physical	• According to each term established in the Corresponding Mexican law regulation • Per event based on the annual supervision program • In cases of visits or special monitoring
Information regarding the Technical Opinion	AML/CFT Agent	• 150 calendar days prior to the expiration of the technical opinion
Response to information requests	Email	• According to each term established by the CNBV
Databases of clients, users, operations and alerts	Email	• Per event based on the annual supervision program • In cases of visits or special supervision
Identification files	Email	• Per event based on the annual supervision program • In cases of visits or special supervision
Different acts	Email	• Per event based on the annual supervision program • In cases of visits or special supervision
Images of system tests	Email	• Per event based on the annual supervision program • In cases of visits or special supervision
Financial Statements and Annual Declarations	Email	• Per event based on the annual supervision program • In cases of visits or special supervision
Questionnaire of transactions	Web Portal	• At the request of the CNBV, generally on an annual basis.

*Applicable only to Fintech
** Does not apply to Investment Advisors
*** See section "Transaction Reports"

Type of transactions	Sector		Amount	Timeframe	
CTR	All except Investment Advisors	Prudential and SOFOMES*	> = 7,500 USD (or equivalent)	First 10 working days **Fintech	First 10 working days of the months of January, April, July and October
		FNDARFP y No CNBV	> = 10,000 USD (or equivalent)		
		Exchange centers, money transmitters and fintech**	> = 5,000 USD (or equivlalent)	Last 10 working days *SOFOMES	
Suspicious Transactions	All		Not apply	3 working days after the dictaminación is issued / 60D FNDARFP - 60 calendar days -Banks have an additional 30 calendar days if established in The AML/CFT P&Ps	
Suspicious Internal Transactions					
24 Hours Report				24 hours from the time the information is known	
Cash dollar Transactions	Banks, Brokerage, SOFIPOS & SOFINCOS and SOCAPS		Users >= 250 USD Customers >= 500 USD	First 10 working days	First 10 working days of the months of January, April, July and October
	Credit Unions y FNDARFP		Transactions >= 500 USD		
	Exchange Houses		Users >= 250 USD Fully identified users >= 500 USD		
	Exchange centers		Transactions >= 1,000 USD	Last 10 WD	
International Transfers	Banks, Brokerage, Exchange Houses, SOFIPOS & SOFINCOS, SOCAPS, TDs, Fintech		>= 1,000 USD (or equivalent)	Monthly: First 15 working days of the following month	
Cashier's Check Transactions	Credit Institutions (Banks)		> = 10,000 USD (or equivalent)	Quarterly: First 10 working days of January, April, July and October	
Total Foreign Currency Amounts	Exchange centers		The total amounts of foreign currencies purchased and sold as part of the transactions carried out during the quarter in question.	Quarterly: Last 10 working days of January, April, July and October	
Money Transmission Services	Fintech, Virtual Assets & Money Transmission only IFPE		>= 1,000 USD (or equivalent)	Monthly: First 15 working days of the following month	
Virtual Assets Transactions			>= 500 USD (or equivalent)	Quarterly: First 10 working days of January, April, July and October	
			>= 7,500 UDIS		
	Banks		Purchase: regardless of amount Sale: >= 2,250 USD		
Blocked Persons List	All		Not Apply	24 hours after the information is known.	