

レグテック(RegTech)とIWT

マネー・ローンダリングおよびテロ資金供与（AML/CFT）対策は、近年のレグテック（RegulationとTechnologyを組み合わせた造語）開発が進む重要な分野です。金融機関は、取引の監視、制裁スクリーニング、有害メディアスクリーニング、KYCシステムなどのテクノロジーを使用して、潜在的なIWTアクティビティやIWTとのつながりを検出、識別しています。

今回のIWTリサーチの一環としてThemisの調査に協力した金融セクターの専門家たちは、IWTリスクへの対応におけるテクノロジーについて、取引モニタリングの有効性（82%）、有害メディア検索（66%）、制裁措置リスト（56%）が重要であると回答しています。また、回答者の圧倒的多数（96%）が、関連するレグテックシステムやツールに関して、潜在的なIWTとのつながりを検出する方法に関してさらなるガイダンスを期待すると回答しています。

金融機関が組織全体で厳格なリスク評価を行い、リスクを把握することで、それぞれのユースケースに対して、ツールキットに記載されているさまざまな選択肢を確認しながら、適切なテクノロジーを選択することができます。

金融機関は、ビッグデータ、自然言語処理、人工知能、機械学習などの高度なデータ分析、分類機能を備えたソリューションにより、調査を加速し、手動のプロセスでは見逃していた可能性のある犯罪ネットワークや組織犯罪の口座のつながりを検出できるようになります。

これらのテクノロジーをより広範かつ戦略的に採用し、金融犯罪コンプライアンスプログラムに統合することで、よりターゲットを絞ったインテリジェンス主導の検出能力が備わり、結果として金融機関は、関係当局により多くの、効果的な疑わしい取引の届出（STR）を提出することができます。

IWTの複雑性、大規模な犯罪組織や重大犯罪シンジケートとの密接なつながり、レッドフラグ類型の継続的な進化により、IWTに関連する疑わしい取引の検出と報告を支援するテクノロジーの必要性はさらに高まっています。

このガイドでは、以下に関して、さらなる推奨事項とケーススタディを紹介します。

1. 既存のテクノロジーで検出ロジックを構成する
2. IWT対策として新しいレグテックソリューションの導入を検討する

既存のテクノロジーで検出ロジックを構成する

このセクションでは、具体的なユースケースを使って、金融機関の既存のレグテックソリューションでIWT対策への取り組みの効率と効果を向上させる方法を説明します。

ユースケース1：既存のAML/CFTシステムの監査とテスト

金融機関はまず、IWTの指標を検出するための正しいAML/CFTテクノロジーが採用されていることを確認する必要があります。堅牢な制裁スクリーニングシステムが導入され、世界的に重要な制裁対象リスト上の名前に対してアラートを出すように設定されていることを確認し、制裁対象の名前が変更された場合でもアルゴリズムを使ってフラグを立てるように調整されたスクリーニングシステムのファジーロジック照合機能を評価する必要があります。

アルゴリズムを操作して、スクリーニングシステムのストレステストを実施し、システムが制裁レコードを識別し、アラートを出すことが難しいエリアを確認します。システムでは、金融機関の取引選別プロセスの一部としてIWTに関連するキーワードに対してアラートが出せるようにする必要もあります。

制裁スクリーニングシステムは定期的にテストを行い、想定通りに機能していること、およびシステムによって発生する偽陽性の数が管理できる量であり、利用可能なリソースを圧迫しないことを確認する必要があります。

世界的に重要な制裁リストは常にアップデートされます。金融機関はシステム監査の一環として、制裁リストデータが適切な頻度で更新されていることを確認しなければなりません。有害メディアについても同様です。すべてのAML/CFTリスク（IWTに特に関連するものを含む）を軽減するために、最新のデータをKYC、CDD、EDDチェックに使用する必要があります。

金融機関は、取引監視テクノロジーを搭載したシステムで顧客の金融行動の全体像を把握する必要があります。このシステムは、リスクレベルをカバーするもので、顧客のリスクプロファイルを確認して将来の活動を予測し、定義されたリスクプロファイルから外れた取引が行われたときにはアラートを出す必要があります。

取引監視システムのテストとIWTルールの検証を行うことで、不正確な点を洗い出し、取引監視システムが不必要なアラートを出したり、IWTとの関連性の高い行動型の取引を見逃す原因となる不正確な閾値パラメータを特定することができます。

ユースケース2：既存のAML/CFTシステムの調整と最適化

制裁スクリーニングシステムのテストを行うことで、金融機関はシステムの構成を理解し、事前定義された検出パラメータが内包する弱点を特定することができます。テストでは、制裁スクリーニングシステムの効率と効果最適化のための継続的な調整を繰り返すことで、システムのパフォーマンスを改善し、強化します。これは、金融機関が既知のIWT関連キーワードを検出する能力の向上につながります。

取引監視システムのテストと検証では、取引監視システムのアラート機能がもつ脆弱性を特定することができます。これにより、金融機関のITチームは、既存のIWTレッドフラグの前提条件を理解し、時間の浪費につながる不正確さをシステムから排除するための修正作業とテスト後の強化作業を実施するための情報を得ることができます。

システムを調整することで、アナリストは既知のIWTの種類と一致する取引パターンと行動をより簡単に特定できるようになり、チームが効率的に作業できるようになって、より多くの高品質なSTRを当局に提出できるようになります。

ユースケース3：AML/CFTシステムの効率と効果の継続的なモニタリング

最後のステップは、制裁スクリーニングと取引監視システムの効率と効果を継続的に監視することです。すべてのAML/CFTテクノロジーが正しく調整され、システムが生成する誤検出の数がコントロール可能なレベルに保たれるように継続的に監視することが必要です。

目的に合わせて適切に調整されたAML/CFTシステムでは、適切かつ有効なIWTアラートが生成され、偽陽性の誤検出が引き起こす過剰なシステムノイズの干渉も避けることができます。

IWT対策として新しいレグテックソリューションを導入する

IWTの類型を適切かつ正確に検出するための既存のシステムの更新の他にも、IWTリスクに対抗するための新しいテクノロジーの導入、利用も効果的です。リスクベース・アプローチを実施する過程で、管理を強化し、確実に潜在的なIWTリスクを検出するために、新しいテクノロジーを導入する必要がある金融機関もあるかもしれません。

以下に挙げるのは、IWT対策として現在実用化されている新しいレグテックの具体的なユースケースです。

ユースケース4：強化された顧客リスクプロファイリング レグテックカテゴリ：機械学習（ML）

既存のテクノロジーにMLモデルを追加して採用することで、定義済みの顧客リスクプロファイルを強化して、疑わしい取引を識別する取引監視システムの能力を強化できます。MLは、リアルタイムで動作する行動プロファイリングシステムの設定調整を支援し、他の方法では検出できない銀行口座の異常の検出につなげることができます。MLモデルは、IWTの指標を検出できるように調整することが可能です。

ユースケース5：TBMLに関連するIWTレッドフラグの検出 レグテックカテゴリ：海運業界AI

規制リスクは、買い手、売り手、都市、地域、港、商品、商品の出荷プロセスに関与する船舶など、貿易取引のあらゆる側面に関連する可能性があります。

貿易取引に便乗したマネー・ローンダリング（TBML）は、IWTの関係者やそれによって利益を受ける者が違法な商品を隠し、資金を洗浄するために使用する手口であり、引き続き重要視されています。特に、海運業界を対象とした新しいAIテクノロジーでは、密輸の可能性のあるルート、貨物、出荷書類に記載された内容と貨物の実際の重量が比較して監視され、出荷とそれに関連する行動を追跡することが可能です。

ユースケース6：より効果的なデータの管理と報告 レグテックカテゴリ：ガバナンスリスクおよびコンプライアンス（GRC）レポートプラットフォーム

近年、金融機関の報告義務、特にSTRの提出を自動化できるGRCプラットフォームの利用が増加しています。このシステムでは、規制機関や、場合によっては官民連携（PPP）への情報報告を自動化し、透明性を向上させることができます。

IWTのような違法行為やマネー・ローンダリングの類型に合わせて調整されたGRCプラットフォームでは、さまざまなデータフィードをまとめ、リアルタイムで包括的かつ正確なレポートを生成することができます。

テクノロジーの重要性

テクノロジーは、今でも多くの組織において変化の原動力となっています。もちろん、IWTの撲滅を目的とする画期的なレグテックソリューションにもこれは当てはまります。このようなイノベーションを推進するためには、まず、的確かつ正確でクリーンなデータを利用できるようにします。金融機関はそれを読み解き、貴重なインサイトを獲得して、金融犯罪リスクを軽減するためのより良い意思決定に利用できるようにする必要があります。

官民連携（Public-Private Partnership: PPP）

官民連携（PPP）も、IWTとの闘いにおける重要なポイントです。業界は多くの政府機関からの支援を受けて、官民連携を推し進めようとしています。違法な金融活動に関する情報の伝達を可能にするPPPは、コンプライアンス業界からの支持を集めています。サプライチェーンと資金の流れが全世界にまたがるIWTとの闘いでは、PPPが大きな意味をもちます。

NGO、政府、民間企業が参加するPPPは、業界全体の取り組みを促進するために欠かせない情報へのアクセスを可能にするという点で重要であり、金融機関からのIWTの追放、違法な資金フローの阻止、そしてIWTに対する国際的な闘いを前進させることにつながります。これは現在進行形の取り組みであり、銀行およびその他の金融機関すべてが重要な役割を担っています。

このガイドは、以下の組織との連携により作成されました。



McDonnell-
Nadeau