

**NICE**  
ACTIMIZE

# アンチマネー ロンダリング (AML) に おけるAI: 変化は進行中

NICE Actimizeインサイトレポート

Ted Sausen

アンチマネーロンダリング(AML) 問題エキスパート | NICE Actimize

アン・リゲル

シニアAML製品マーケティングマネージャー | NICE Actimize

2020年以降のAML環境における傾向と変化を提供する手段として、NICE Actimizeは、機械学習とアンチマネーロンダリング（AML）プログラムを搭載した自動化技術の認識の相違を理解するために年次業界調査を実施しています。

研究に基づいたこの業界調査で、取引監視のためのソリューション内にある継続的な課題を評価し、機械学習と自動化技術を用いたAMLプログラムの近代化に向け金融サービス機関の視点が大きく変化していることを検証します。

調査結果から得られた推論は、今日の金融犯罪の巧妙さと多様性により、いかにAMLソリューションが複雑化し、効果的なAMLプログラム維持を実現するための終わりなき課題に拍車がかけているかを示しています。リスクおよびコンプライアンスの責任者が業務量を維持するリソースの確保に日々苦労している中、不審なトランザクションアラートの量は増加し続け、規制当局からの期待はますます高まっています。

全世界の回答者は、多様な資金規模の金融サービス機関にわたり、第1層銀行から中堅銀行、および100億ドル未満の資産を持つ銀行におよびました。大半の回答者は、リスクとコンプライアンス、運営、技術部門のいずれかに従事し、主に取引監視に重点を置いていました。

## 調査結果の概要：

- 2019年には、回答者の約半数がアラート量とアラート品質が取引監視ソリューション内で最も重要な課題であると回答。これはデータ整合性の問題に密接に関連し、コンプライアンスの全体的なコストにつながる。
- また2019年には、回答者の90%がシステムは1年間に1回から4回チューニングする必要があると答えた。（より頻繁にチューニングすることで、アラート量と関連コストの削減が可能）
  - これは業界のベストプラクティスであるが、利用可能なリソース（調査担当者、技術、知識豊富なスタッフなど）がないために実行できると回答した組織は半数にとどまった。
- 「画一的」モデルが機能していないため、顧客セグメントの適切な整合性を確保することが明確なニーズとなりつつある。
  - チューニングと同様に、セグメントメンテナンスも定期的に行われるべきであるが、実際にその頻度は常に定期的ではない。
- AI、機械学習および自動化技術を取り巻くセンチメントは、着実に変化している。業界のユースケースでは、誤検知の減少やアラートの質の向上などのメリットが明らかになり始めているため、多くの金融サービス機関が既存のソリューションを再評価している。
  - 2019年の回答者の90%が、現在こうした評価の実施過程であると回答。
- 既存のもので間に合わせることは、金融サービス機関にとってもはやサステナブルではない。スタッフやリソース、それを支える予算は、仕事量の軌道に乗っておらず、逆の方向に向かっているケースが多い。2020年に突入した今、この現実、この新しい10年を経てAMLプログラムの今後を形作るものとなっている。

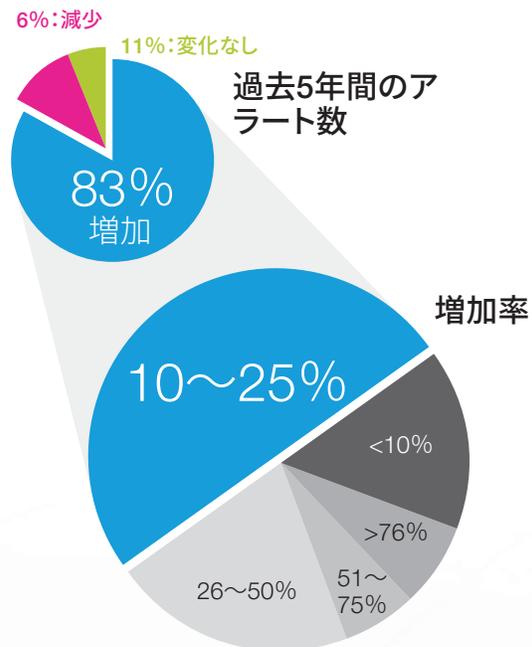
# 取引監視量の複合化

既存のAMLソリューションは、新たに進化するダイナミックな脅威とガバナンスプログラムの強化により、仮想通貨、人身売買、テロ資金調達などのシナリオに対応するために新たな分析機能を追加が必要となっています。これは最新の2019年の調査でも確認されており、回答者の半数がトランザクション監視プログラムにこれらの新しいアナリティクスを年単位で追加していると回答しています。

新しい分析は金融サービス機関を保護するために不可欠ですが、それらの導入はすでに要求の厳しいワークロードに悪影響を与えます。2019年は、83%の回答者が過去5年間でアラート量が増加したと回答しています。ほとんどの人がアラートの数が10~25%増加したと回答しており、中には75%増という回答もありました。

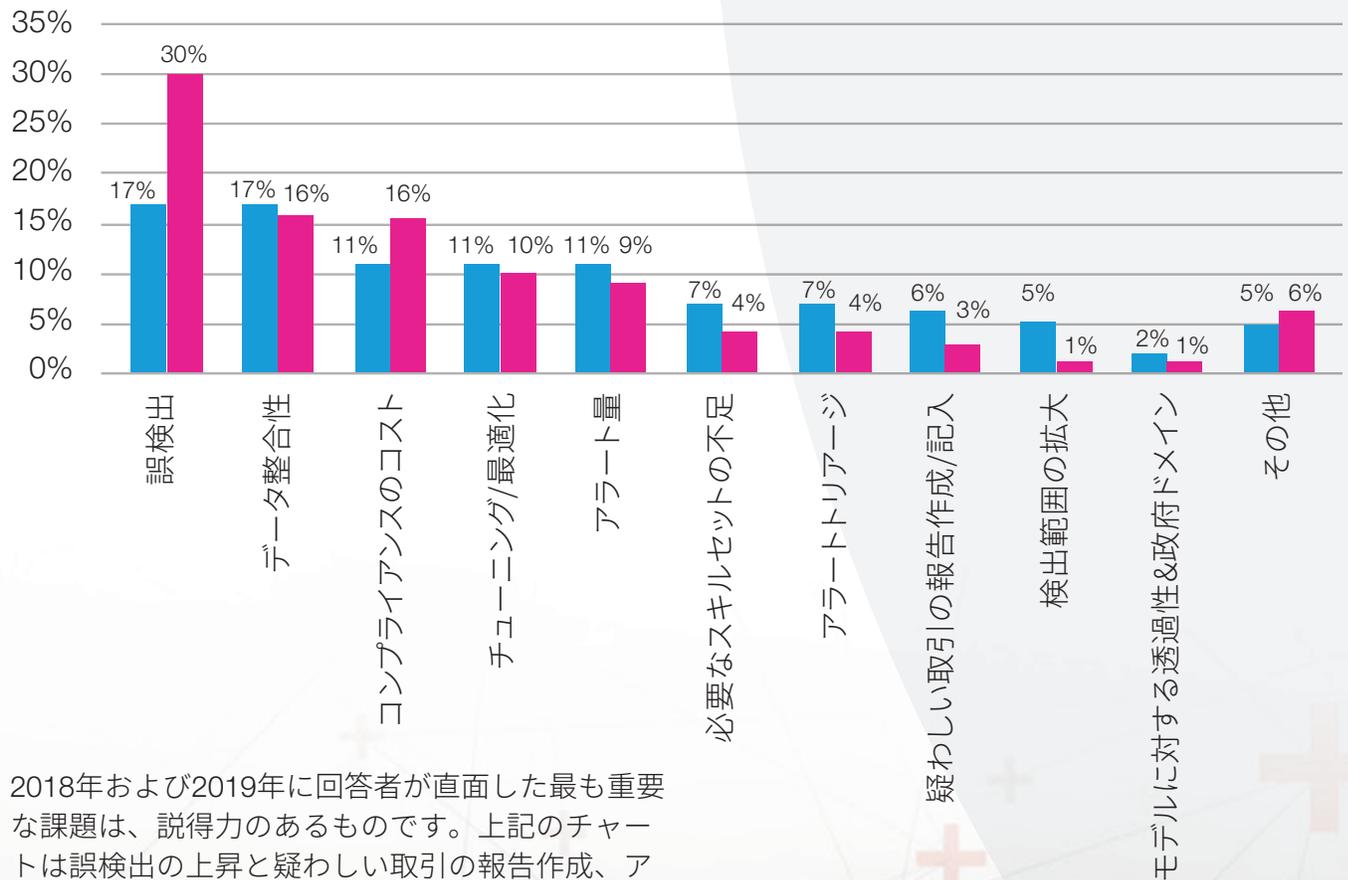
今日の取引監視システムのアラートのほとんどのアラートは、偽陽性です。「偽陽性」の定義については意見が分かれるところですが、本報告では、不審な活動報告がなされなかった場合を偽陽性と定義しています。

偽陽性アラートは、現在金融サービス機関が直面している最も重大な課題です。結果はアラートのほぼ95%が偽陽性であることを示しており、一部の金融サービス機関はより高いパーセンテージを示しています。また、2018年から2019年にかけては、最も重要な課題として報告する人が倍近くになっていたことも見逃せません。



この課題に対処することは、調査担当者に代わって多大な努力が必要です。これを考慮すると、約6万人のAML調査員とコンプライアンス責任者を擁する英国の主要多国籍組織は、一般的に低レベルの偽陽性の調査に5分から30分を費やしていると述べています。<sup>1</sup>より複雑なアラートは、解決までに数時間または数日を要する可能性があります。そのため、アナリスト、調査官、コンプライアンス担当者には負担がかかり、時にはアカウントマネージャーやその他の担当者の支援も必要になることがあります。

現在あなたの部門にとって最も重要な課題は、取引監視プログラムのどのような側面ですか？



2018年および2019年に回答者が直面した最も重要な課題は、説得力のあるものです。上記のチャートは誤検出の上昇と疑わしい取引の報告作成、アラートトリアージ、検出、モデル検証などのタスクの低下を示しています。これは、運用面から見た組織の成熟度が高まっていることを意味しており、適切な人材とプロセスを確保しているにもかかわらず、AMLプログラムの全体的なコスト増加の一因となる誤警告を削減することができていないことを意味しています。

# テクノロジー の再開発

## 問題に対処するために

---

高い誤検出率に対処するには、2段階のプロセスが必要です。まず、金融サービス機関はクライアントの集団が適切にグループ化されていることを確認します。「画一的な」モデルは機能していないことがわかっているため、顧客セグメントの適切なメンテナンスを確認する必要があります。2つのガスステーションの例を見てみましょう。1つのガスステーションにはコンビニエンスストアと商業的ATMが併設されており、もう一方のガスステーションはコンビニエンスストア、プライベートATMおよびギャンブル用のゲーム機が設置されています。2つは非常に似ていますが、適切に監視するために異なるセグメントに分ける必要があります。

クライアント集団を適切にグループ化することにより、顧客間の取引行動を類似した特性で比較することができます。特定のアクティビティがこれらのセグメントの典型的な行動に当てはまらない場合、アラートが生成されます。実際には、これらのセグメントのレビューは毎年行うべきです。顧客は必要に応じて異なるセグメントに移動するため、可能であれば、顧客の行動に基づいてより頻繁にレビューするのが効果的です。また、顧客は企業との関係性が進む中で、顧客の行動は参加当時と比べて変化し得るという点を念頭に置いておくことも重要です。セグメントのメンテナンスが不適切な場合、活動を通常とは異なるものとして分類してしまい、余分なアラートが発生します。実際には、行動とリスクに基づいて共通の属性を持つ、ターゲットを絞ったセグメントを作成することです。類似したものを集めることで、閾値を綿密に最適化することができます。

## セグメント管理

2018年と2019年の調査では、セグメンテーションの管理に対する回答に大きな共通点がありました。調査対象となったほとんどの組織では、少なくとも年1回はセグメンテーションを見直しており、75%が過去2年以内に見直したと回答しています。これまでセグメンテーションへの注目度が低かったことを考えると、業界は前向きな一歩を踏み出したこととなります。

高い誤検出率に対処する2つ目のステップは、チューニング分析モデルです。チューニングとは、パラメータと閾値を最適化して、前述の定義されたセグメントのそれぞれに適切であることを確認するプロセスです。最大の課題は、より多くのセグメントが作成される時にどれほど負荷が増えるかということです。金融サービス機関は、チューニングの労力が法外なものになり定期的に行われなようなシナリオを作らずに、適切なセグメント数を決定して顧客を効果的に監視しなければなりません。重要なのは適切なセグメントです。これがなければ、類似性のないアクティビティを持つクライアントに適切なパラメータを設定することはできません。

2019年の回答者の90%が、チューニングは少なくとも年に1回は行うべきであることに同意しています。頻繁にチューニングを行うことで、アラート量とそれに伴うコストが削減されます。

- これは業界のベストプラクティスですが、チューニングを実行するためのリソース（調査担当者、技術、その他の知識豊富なスタッフなど）を持っている組織は半数にすぎませんでした。多くの組織は、代わりにモデルのサブセットをチューニングすることを選択しましたが、これはつまり完全にチューニングされたモデルを保有していないことを意味します。

このような活動は変数の数が多いため、従来の方法では効果的に達成することが人間的に不可能になってきています。これが、金融サービス機関が従来の手法から方向転換し、機械学習やクラスタリング技術を取り入れたアプローチを模索し始めている理由です。

# 90%

がチューニングは少なくとも1年に1回行う必要があると回答

# AIと機械学習：新しい基準

機械学習やAIをAMLに導入することは、当初さまざまな抵抗に直面しました。アナリスト、調査担当者および規制当局は従来の規則ベースのモデルに慣れていたので、機械学習のアプローチは異なりました。モデルの入力および出力は知られていましたが、その間のプロセスは透明性に欠け、理解しやすいものではありません。

2018年には、規制に対して機械学習によって強化されたモデルを正当化することがコンプライアンス・チームにとっての第1の懸念事項であり、第2の懸念事項は、それらを実装するコストでした。興味深いことに、1年後の2019年には懸念事項が逆転し、実装コストが第1の懸念事項、規制に対する正当化が第2の懸念事項となりました。こうした結果とその他の業界観察に基づき、規制の受け入れは以前ほど大きな懸念事項ではなくなりました。金融サービス機関は、既存のAMLプログラムを補完するために、「慎重に観察」する姿勢から積極的にこうした技術を追求める姿勢へと変わりました。

センチメントの変化は、複数の要因によって促進されました。

- 結果が現実味を帯びてきたこと。実験をスタートさせたアーリーアダプターは、ポジティブな結果を確認していた。
- 一部のベンダーは「ブラックボックス」の透明性の欠如に素早く対応し、説明可能なアナリティクスを開発して不安を解消した。
- 規制当局による裏付けと推奨。

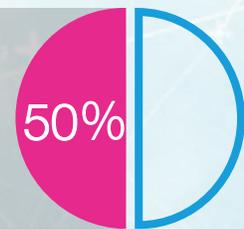
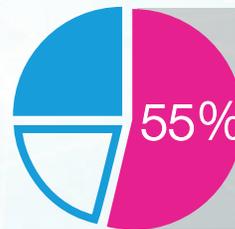
規制上の障壁を取り除くことにより、いくつかの結論が生まれました。

- 金融サービス機関はセーフハーバーが与えられ、これらの革新的技術が従来のAMLプログラムでは検出されなかった新たなマネーロンダリングスキームを発見したとしても、罰せられることはない。これにより、コストがかかる振り返り作業を行う必要があると考える企業の不安が軽減された。
- 規制当局は、新しい革新的な技術を導入しないことを選択した組織にペナルティを課すことはないと思われる。そうすると、あえてそれに触れる必要はなくなるのではないか。

2019年には、回答者の15%が、機械学習が簡単に規制に適合するとはまだ考えていないと回答しています。さらに複数の質問に対する回答から、これらの新テクノロジーに信頼を寄せていることを示す一方で、データ科学者が実装するためのデータ科学者を見つける段階になるとこの自信が薄れることがわかります。これらの疑念は、統合に必要なコスト、リスクへの嫌悪、ROIを正確にマッピングする計画の欠如などが主な原因です。

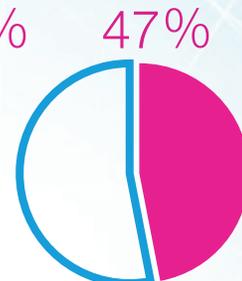
一方で、回答者の25%が既存のAMLソリューションにAIや機械学習技術をすでに統合しており、半数以上の回答者が積極的に評価していると回答しています。そのうち、50%が来年中に統合する予定だと明らかにしています。

2018年および2019年の調査では、回答者はAMLにおける機械学習の主なビジネスドライバーとして、異常検知、セグメンテーション、モデルチューニング(いずれも併用)を挙げています。特に興味深いのは、ビジネスドライバーとしての「セグメンテーションのための機械学習」が2018年から2019年にかけて、13%から47%へと顕著な飛躍を遂げたことです。



25%: AIを導入済み  
55%: 現在評価中  
20%: 評価または計画しない

現在評価中である55%のうち、半数が来年内に統合する予定



2018年

2019年

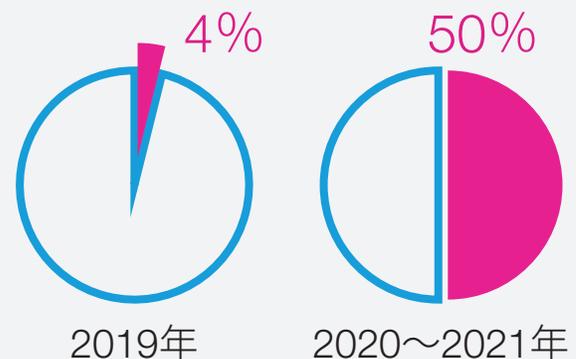
ほとんどの組織がAI、機械学習、自動化技術に向かっており、それらが新たな規範となり、おそらくは要件となる日が急速に近づいています。

## クラウドの受け入れ

AMLプログラム内で機械学習を効果的に実装することは大量のデータに大きく依存することを意味し、これによって多くの要件と要求が発生します。これを管理できるようにするため、多くの金融サービス機関がクラウドに転向しています。回答者が示したクラウドの推進力の上位2位は、他の技術との統合のしやすさと、クラウドが提供するスケーラビリティでした。クラウドベースのソリューションには、他に次のようなメリットがあります。

- コスト削減（クラウドベースのストレージおよびその他のハードウェア）
- 俊敏性を高めたコンピューティング・パフォーマンスをもたらす、より良いオプション
- データサイエンスリソース（第三者プロバイダーがサービスとして提供するものなど）
- 複数の組織で活用されたデータからの集成的なインテリジェンス（ピア・ベンチマーキングと高度な異常検出）

2019年の回答者のうち、現在パブリッククラウドベースのAMLソフトウェアやサービスを利用していると答えたのはわずか4%で、今後2年以内にパブリッククラウドの利用を計画していると答えたのは50%に達しています。



## 今後の展望

2020年以降を見据え、業界はAMLプログラムの近代化を急ピッチで優先させます。新技術の定量化可能なメリットを示すケーススタディが表面化し始めており、まだシフトを導入していない組織は、その費用を正当化するために独自のビジネスケースを構築する際の検証材料として利用することになるでしょう。

これまでのところ、機械学習とAIの観点からの焦点の多くはトランザクションのモニタリングにありましたが、今後はスクリーニングや顧客のデューデリジェンスのプロセスにまで拡大していくことが予想されます。機械学習は、取引行動と組み合わせた大量のクライアント属性を活用して異常行動をさらに特定できるようになり、今日の多くの取引監視システムに存在する「ノイズ」を大幅に軽減します。

顧客理解（KYC）プロセスの弱点が顧客理解（KYC）/顧客デューデリジェンス（CDD）プログラム全体をどのように劣化させ、トランザクション監視やウォッチリストフィルタリングなどの他の分野に影響を与える下流効果をもたらすかを理解することが重要です。最新技術革新を活用することにより、リスクの範囲拡大、顧客理解（KYC）申請のオンボーディング、継続的な顧客デューデリジェンス（CDD）、デューデリジェンスプロセスの強化など、顧客のライフサイクルアセスメント全体のあらゆる側面を簡素化し、統合されたAMLソリューションが実現します。これにより運営効率が向上し顧客リスクの全体像が得られるため、金融サービス機関は顧客に対する理解を常に最新の状態に保つことができます。

2020年はそれ以前の年と同様、2019年に席卷したすべての金融犯罪テクノロジーテーマに対してアクションを起こす一年となります。これらのテーマの中から、金融犯罪対策やマネーロンダリング防止活動に大きな影響を与える5つの重要な分野が浮かび上がってくると考えられます。

- ① プライベートからプライベートへの情報が進む
- ② 共有 コンテキスト化された金融犯罪が進む
- ③ リアルタイムAML監視
- ④ 量ではなく質の影響
- ⑤ 基準の整合性の向上

一つ確かなことは、金融犯罪が絶えず進化し、ますます複雑化していくということです。この戦いに、負けることは許されません。NICE Actimizeは皆様を支援し、この調査で取り上げたテーマやアプローチに取り組んでまいります。AML業界の最新動向や展望について、さらなる最新の洞察を提供します。お気軽にお問い合わせください。



引用

1. McGowan, J. (2018年)。「誤検出を減らすために作成されたAI」 Celent, 3-3

# NICE ACTIMIZE

## NICE Actimizeについて

NICE Actimizeは、地域の金融機関、国際的な金融機関、および政府の規制当局を対象とする、金融犯罪、リスク、コンプライアンス対策ソリューションの最大のプロバイダーであり、最も広範なサービスを提供しています。NICE Actimizeの専門家はこの分野で常に最上位にランクされており、革新的な技術を活用して金融犯罪を特定し、不正行為を予防し、規制に準拠することによって、組織を保護し、消費者と投資家の資産を保護します。NICE Actimizeは、支払い詐欺、サイバー犯罪、制裁措置監視、市場における不正行為、顧客デューデリジェンス、インサイダー取引などの問題に対処するためのリアルタイムでクロスチャネルの不正防止、アンチマネーロンダリング検出、取引監視のソリューションを提供します。

© Copyright 2020 Actimize Inc. All rights reserved.