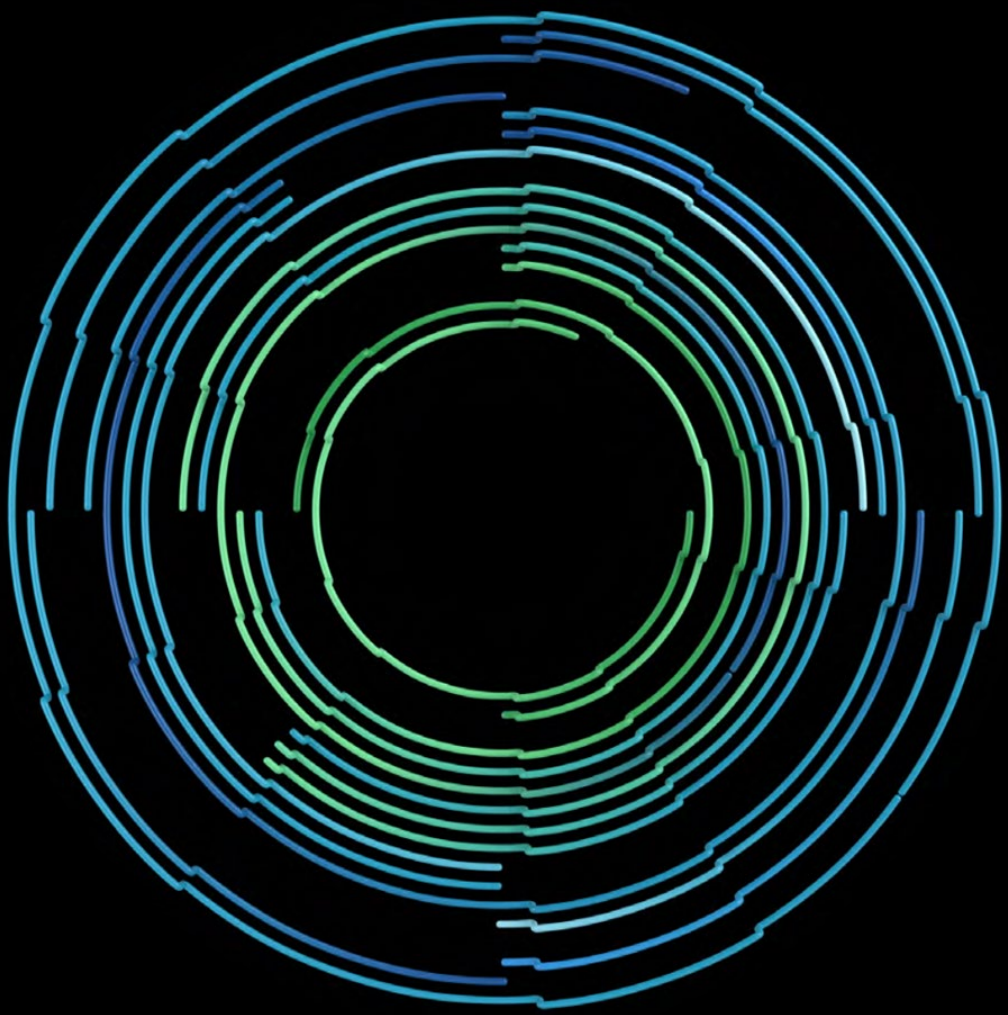
Deloitte.
デロイト トーマツ

UOB



金融犯罪コンプライアンスの未来

デジタルとフィジカルが融合した世界におけるイノベーションの説得力ある活用

第 2 巻

Forensic

目次

用語集

AI	―	Artificial Intelligence	人工知能
AML	―	Anti-Money Laundering	マネー・ローンダリング対策
AMLS	―	Anti-Money Laundering Suite	マネー・ローンダリング対策スイート
CFT	―	Counter Terrorist Financing	テロ資金供与対策
FCC	―	Financial Crime Compliance	金融犯罪コンプライアンス
FEAT	―	Promote Fairness, Ethics, Accountability and Transparency	公平性・倫理・説明責任・透明性推進のための原則
FINTECH	―	Financial Technology	フィンテック
GDPR	―	General Data Protection Regulation	一般データ保護規則
GFIN	―	Global Financial Innovation Network	グローバル・ファイナンシャル・イノベーション・ネットワーク
KYC	―	Know Your Customer	ノウ・ユア・カスタマー
MAS	―	Monetary Authority of Singapore	シンガポール金融庁
ML	―	Machine Learning	機械学習
NLP	―	Natural Language Processing	自然言語処理
PSD2	―	Payment Services Directive	決済サービス指令
POC	―	Proof of Concept	概念実証
PPP	―	Public-private Partnerships	官民パートナーシップ
REGTECH	―	Regulatory Technology	規制テクノロジー
RPA	―	Robotics Processing Automation	ロボティック・プロセス・オートメーション
SAR	―	Suspicious Activity Report	疑わしい活動報告書
STR	―	Suspicious Transaction Report	疑わしい取引報告書
UOB	―	United Overseas Bank	ユナイテッド・オーバーシーズ銀行

序文

デロイトとユナイテッド・オーバーシーズ銀行（UOB）が共同作成したこの白書は、テクノロジーによる創造的破壊がいかに金融犯罪コンプライアンスを変えてきたかを考察します。

銀行業界にとって、変化するサービス提供環境と消費者行動に対してコンプライアンス能力を高める必要性は、最も重要な課題となっています。金融サービスセクターは、コンプライアンスの難しい課題 – 常にコンプライアンスを念頭に置きながら収益性を管理すること – に取り組まなければなりません。新規参入者との競争の激化は、金融機関が新たな商品やサービスを生むようなイノベーションを加速する必要性も高めています。

顧客を獲得し維持することの重要性は不変です。しかし、銀行間競争における本質の進化と、より革新的なビジネスモデルが求められる第4次産業革命の到来が相まって、金融犯罪コンプライアンスの未来の限界は押し広げられ続けています。

金融犯罪は金融機関にとって大きなリスクであるため、コンプライアンス能力を構築し直す必要があるか熟考することは当然必要となります。金融犯罪に対する防御を続けるためには、金融機関がイノベーションによって自らの能力を研ぎ澄ませることが引き続き重要です。

この白書では、まず金融犯罪との闘いにおける金融サービスセクターの役割の重要性について説明します。次に、金融犯罪コンプライアンスにおけるテクノロジーの活用がもたらす多岐にわたる機会と検討事項をリストアップします。

「マネー・ローンダリングおよびテロ資金供与対策への人工知能（AI）活用例（原題：The case for artificial intelligence in combating money laundering and terrorist financing）」と題した前回の白書[1]（第1巻）で、デロイトとUOBは、金融犯罪コンプライアンスの実効性を高めるためのイノベーションの活用について考察し、見解を共有する行程を開始しました。UOBが規制テクノロジー（RegTech、レグテック）ソリューションプロバイダーと協力してマネー・ローンダリング防止システムの概念実証（POC）を開発し、銀行内のサンドボックス環境でそれをテストした事例を参考に、人工知能（AI）、機械学習（ML）、ロボティック・プロセス・オートメーション（RPA）の活用が分析されました。パイロットプログラムは成功し、結果として疑わしい口座や取引の識別の正確性は向上しました。このソリューションによって誤検出のアラートを減らせたことで、UOBのコンプライアンス担当者は疑わしい事案の調査を合理化し、より価値の高い作業に時間を使えるようになりました。

1年が経って、この第2巻では、金融犯罪コンプライアンスの転換を図るためにUOBが続けている行程を見ていきます。

UOBはビジネスと規制当局のニーズを満たす革新的ソリューションを開発するために、金融犯罪コンプライアンスの領域で次世代テクノロジーを活用しています。この白書では、金融犯罪コンプライアンスを確保するための同行の戦略を深掘りします。

Cheng Pui Yuen
CEO, Deloitte
Singapore

「テクノロジーは企業の業務のやり方を変えています。金融サービスセクターではフィジカル（物理的）な商品・サービスとデジタルな商品・サービスが融合し、両者の境界が曖昧になってきたことで、コンプライアンスの未来に関する興味深い問いが生まれてきています。どのような業務体制や文化を構築する必要があるのか、どのような投資をすればよいのか。また、業界は金融犯罪の問題によりうまく対処するために、どのように革新的なテクノロジーを活用できるのかという問いです。そのすべてが、新たな次元と物事のやり方を模索する機会をもたらしています。この白書は、この先何が起きるのかを描き出します。シンガポールは「スマートネイション（スマートな国家）」を目指す取り組みにおいて、将来を方向づける際に幅広い信頼感をもたらす産業連携や共同開発の恩恵を受けるでしょう。」

Victor Ngo
Head of Group
Compliance, UOB

「ますます複雑化する規制環境において、銀行は顧客の利益を守り、ステークホルダーの信頼を維持するために、強力なコンプライアンス文化を確保し続けなければなりません。特にデジタル化が進む世界では、毎日出現する新たなリスクの一歩先を行けるように、常に気を配り続けることが重要です。デジタル時代が提供する技術革新の機会によって、金融機関は防止、検知、執行の各措置を拡充し、リスク管理モデルを強化することもできます。この白書には私たちがリスク管理慣行を強化し、現在および未来の金融犯罪を防ぐために、新たなテクノロジーを活用したコンプライアンス戦略を策定した際の学びと経験が盛り込まれています。」

はじめに

創造的破壊が起きた金融サービスの新たな世界

現在、金融サービスセクターは数々のリスクにさらされていますが、おそらく最も大きな不安要素は金融犯罪リスクの影響でしょう。

3兆ドル規模の脅威が広範囲にわたる影響を及ぼしており、脅威との闘いはグローバル金融経済のすべての参加者にとって気の重い作業です。金融犯罪の問題は、規模の大小を問わず、あらゆる金融機関が抱える共通の課題だということに留意すべきです。すべての金融機関にとって、規制当局から科される多額の罰金、膨らむコンプライアンス費用、評判への影響が自らに及ぶか否かは賭けのようなものです。

ルールベースのアルゴリズムによる既存の金融犯罪コンプライアンスモデルが今もすたれていない一方で、不正資金フローの防止、検知、予測に関して、規制当局が金融機関に寄せる期待の変化に応えることが緊急に求められています。犯罪が巧妙化しているにもかかわらず、時代遅れの方法、まとまりのない業務体制や金融犯罪対策が変わらなければ、問題はさらに深刻化します。従来の監視テクノロジーは、たとえ最適化されている場合でも不十分です。と言うのも、従来の監視テクノロジーは最も重要な事項に焦点を当てることが必ずしもできておらず、いまだにあまりにも多くの誤検出を出し続けているからです。

事業環境と規制当局の期待の変化がもたらした新たなリスクの複雑さは、基準、監視能力、統制、社内方針および手続を向上させるアプローチの刷新を必要とします。端的に言えば、環境の変化はビジネスの変革のみならず、コンプライアンスの変革をも必要としています。

成功は、事業戦略、法規制の遵守、リスク管理、テクノロジー、業務のシームレスな統合によって推進されます。

金融機関はリスク管理機能（第1・第2の防衛線の役割分担および主な責任を含む）を見直すべきです。

金融犯罪との闘いに特効薬はありませんが、新たなより良いコンプライアンスの枠組みと統制により、金融機関は犯罪者やマネー・ローンダラーの一歩先を行き続けることができます。

「金融犯罪コンプライアンスにおいてAI、機械学習、RPAを導入するイノベーションは、今日、金融機関が賢く抜け目のない方法でリスクと脅威を監視する上での基本的ニーズとなっています。次の段階として、社内外の重要なリスクへの見方を強化し金融犯罪を総合的な観点から監視および評価するために、イノベーションに一段と力を入れなければならないと思います。次の差し迫ったステップとしては、革新的な技術力を活用して取引、犯罪類型、脅威をよりシームレスに監視するために、業界レベルのユーティリティの構築を目的とする官民パートナーシップが必要だと考えます。単一の金融機関が自らのインフラを使って自らのことだけを考えてリスクを捉えるのでは、ビジネス環境の進化や金融犯罪の巧妙化など、この急速に変化する環境で求められる成果を生まない可能性があります。多数のステークホルダーが責任を共有することで、金融機関の負担のバランスをもっと理に適ったものにしていかなければなりません。」

Radish Singh
Southeast Asia Financial Crime Compliance Leader and AML Partner,
Deloitte Financial Advisory, Forensic, Deloitte

第1章

金融犯罪コンプライアンスの動向を詳しく見る

デジタル革命が金融サービスの形をどう変えるかについての考察

2018年、世界の金融機関は、フロントオフィスのデジタルバンキング能力を強化するために97億ドルを投資する計画を立てていました[2]。金融機関が顧客向けサービスやソリューションを拡充するデジタル技術への投資によって競争力を維持しようと競い合う一方で、多面的な金融犯罪リスクの低減にも同じような注意を向ける必要があります。

本章では、デジタル革命および潜在的な金融犯罪リスクに関する最新動向について考察します。

第一に、デジタルバンクやオンライン銀行、そして従来とは異なるプラットフォームの到来です。欧州では、顧客の需要に突き動かされてデジタルバンキングが主流となり、それを受けて「決済サービス指令（PSD）」が改正されました（PSD2）。欧州連合のこの重要な規制イニシアチブは、金融機関、新興金融テクノロジー（フィンテック）企業、その他の第三者を対象とした公平な競争の場を作ることにより、イノベーションと競争を促進することを目的としています[3]。欧州の規制当局は「グローバル・ファイナンシャル・イノベーション・ネットワーク（GFIN）」を介して、現在までこの領域の先駆者であり続けています。GFINは、規制当局の洞察を得て規制環境で商品やサービスのテストや見積もりを実施したいと考えるフィンテック企業のために2018年初めに設立された世界的なイノベーションのサンドボックスで、35の金融サービス規制当局が支援しています[4]。

アジアでも、デジタルバンキングは新しいものではありません。従来の銀行業務に創造的破壊をもたらすインターネットバンキングの認可がアジアに到来したのは2000年代初めのことで、日本、中国、韓国から始まりました。2019年には、香港でも8社がインターネットバンキングの免許を付与されました。

最近ではシンガポールも取り組みを強化しており、5社が新たなデジタルバンクとして認可されました。銀行とノンバンク企業との競争は激化するでしょう。「シンガポールにおける銀行自由化への道のりの次の章」としてこの措置を講じたシンガポール金融庁（MAS）は、「アジア、そして世界において、高い競争力を有し成長する金融センターの座を確実にする[5]」ために、銀行・金融セクターを拡大しています。

デジタルバンクは新たな顧客体験をもたらしています。また、実在する銀行店舗からインターネット上のオムニチャネルの銀行サービスへの移行は、市場開拓および金融サービス提供の迅速化ももたらしました。

急速な変化の圧力を受けて、従来型の銀行も現在、サービス提供プラットフォームやチャネルのデジタル化に向けて迅速な転換に取り組んでいます。デジタルバンクは、顧客体験を向上させる傍ら、新たな次元の金融犯罪も登場させました。デジタルバンクには一般的に支店がなく、より簡単な手続で匿名のクロスボーダー送金ができるため、金融機関や当局による取引のモニタリングをより複雑にしています。

また、従来型の銀行の技術革新は、新たなビジネスモデルを監督および監視するための適切な規制を必要とします。新たなビジネスモデルは機会だけでなく、規制のギャップや抜け穴がある場合には新たなリスクももたらすためです。

デジタルトランスフォーメーションに向けた転換を前提として考えると、金融犯罪に対する脆弱性は、クロスボーダー取引や複数の国・地域間の相互のつながりの中に出現し続けることになります。各国・地域の準拠する規制要件は、内容が緩いものから厳しいものまで広範囲にわたるためです。

どのようなケースであれ、規制当局の基本的な期待は、金融機関が特にAMLおよびCFTリスクに関して、市場の完全性、実効性のある顧客デューデリジェンスプロセス、継続的な監視を確保しなければならないということです。

その結果、デジタルまたはインターネットバンキングモデルにおいて、金融犯罪コンプライアンスの世界はまさに変革の最先端にあるのです。

サービス提供チャネルを問わず、金融犯罪リスクは管理されなければなりません。その管理方法は、ビジネスモデルおよび商品・サービスのリスクに対する脆弱性に見合ったやり方でなければなりません。

従来のノウ・ユア・カスタマー（KYC）プロセスを考え直し、加速する必要があるでしょう。その理由は、顧客が人間とのやり取りを可能な限り回避できる24時間対応のデジタルサービスを享受しているからです。このような進歩はメリットと同時に次なる複雑さももたらします。支店のない銀行サービスにはより迅速なオンボーディングが期待できますが、AML/CFTの身元確認や基本的な顧客デューデリジェンスには、潜在的なリスク評価において依然として特別な注意を払う必要があります。

金融犯罪コンプライアンスを引き続き最前線に据えなければなりません。例えば、UOB初のモバイル専用銀行TMRWは、ミレニアル世代に差別化された顧客体験を提供することに加えて、顧客の利益を守り銀行システムへのリスクを低減することを目指しています。

TMRWは2019年3月、ASEAN市場で最初の進出先となるタイでサービス提供を開始しました[6]。

堅牢なコンプライアンス管理を損なうことなく、デジタルバンク向けのビジネスモデルを支援するために、UOBはまずTMRWのリスクポートフォリオを識別しました。次に、UOBはデジタルバンクで金融犯罪コンプライアンスを確保する方法を決定しました。

第二に、よりアクセスしやすく便利な代替決済手段を提供するノンバンクおよび決済業者（フィンテック）の出現です。決済の領域での成長の主なけん引役は、顧客中心に重点を置く姿勢に立ち返ろうとする潮流であり、デジタルウォレット、モバイルウォレット、クロスボーダー決済、暗号資産（トークンおよび取引所）など、決済を実行するまでのフリクション（心理的負荷）を軽減し、取引をサポートする多種多様な決済オプションを提供することです。このような決済方法が新たな金融犯罪リスクを生み出し、それに対処する新たな規制が必要になる可能性があります。

例えば、暗号資産と、それをテロ資金供与の手段として悪用する可能性は、特にその匿名性と規制当局の監督の不在が不当に利用された場合、大きな脅威となります。

ポイントは明白です。金融機関と金融テクノロジー（フィンテック）企業が「商品化に要する時間」の短縮やコスト効率の高い商品・サービスの提供を目指して新たなモデルを試みれば、その分、犯罪者たちは不正に得た資金を洗浄するより巧妙な方法を探し出します。その一方で、金融犯罪と闘うためにより実効性の高いシステムが常に生み出されるよう、境界線は押し広げられることとなるでしょう。

シンガポールでは「決済サービス法案」が議会で可決され、すべての決済サービスが単一の法の下に置かれることとなりました。ここ最近の新たな動向や、AMLおよびテロ資金供与対策（CFT）にもたらす様々なリスクが考慮されたものです[7]。

シンガポールは、デジタル決済イノベーションの推進とリスク低減の微妙なバランスを取るために、新たな免許制度を導入した世界で最初の国々のひとつです。同法案により、決済業者と取引所はAMLおよびCFTリスクを考慮しなければならなくなります。ただし、この義務は、煩わしく堅苦しい規制の負担を避けるために、適切な水準の範囲で課されることとなります。

いずれにせよ、デジタル決済サービスを対象とした新たな規制の枠組みの導入は、業界の最新のイノベーションおよびビジネスモデルに対する肯定的な反応です。

第三に、決済の迅速化です。前述のとおり、より柔軟に速く資金を管理し動かしたいという消費者の期待の高まりは、銀行業界の変革を促し続けます。決済を最新化することは、送金やeコマース分野などの企業に成長の利益をもたらします。それがひいては顧客体験を改善し、ビジネス取引の加速に役立つことになるからです。

さらに、技術革新により、高速で国境を越えて資金を移動させることが、以前よりもずっと容易になっています。このことがAMLおよびCFTコンプライアンスに関する新たなプレッシャーと期待を生み出しています。

現行のAMLコンプライアンスモデルでは、適切なレビューとKYC確認を確実に行うために取引を遅らせることになれば、顧客が望み期待する効率に直接の影響を与えます。決済を高速化すればモニタリングの時間はわずかとなり、金融機関のフロントとミドルオフィスの業務や能力では解決が難しい問題が生じかねません。

デジタル競争に参加する意欲のある金融機関は、ベストプラクティスとコンプライアンスリスク管理を早期に確立することが死活的に重要であることに気付くでしょう。

「銀行業務はテクノロジーの
範囲を超えています。
フィンテック企業は銀行
サービスを提供するために、
リスク管理および規制遵守のすべての要素と責任を
確実に整備しなければ
なりません。」

Dennis Khoo
Regional Head of
TMRW Digital Group, UOB
The Business Times, 08 May 2019

第2章

金融犯罪コンプライアンスの新たなパラダイムに向けて

デジタルとフィジカルが融合した世界におけるスマートテクノロジーの組み合わせに関する考察

従来のアプローチ

金融犯罪コンプライアンスの従来の枠組み（図1参照）は、方針、手続、プロセスが迷路のように入り組んでいます。前述した環境の変化が起こる前は、設計も実効性も適正だったのかもしれません。しかし、金融機関がますます複雑化する金融犯罪に対して実効性を確実に持ち続けるためには、レガシープロセスを見直す必要があります。

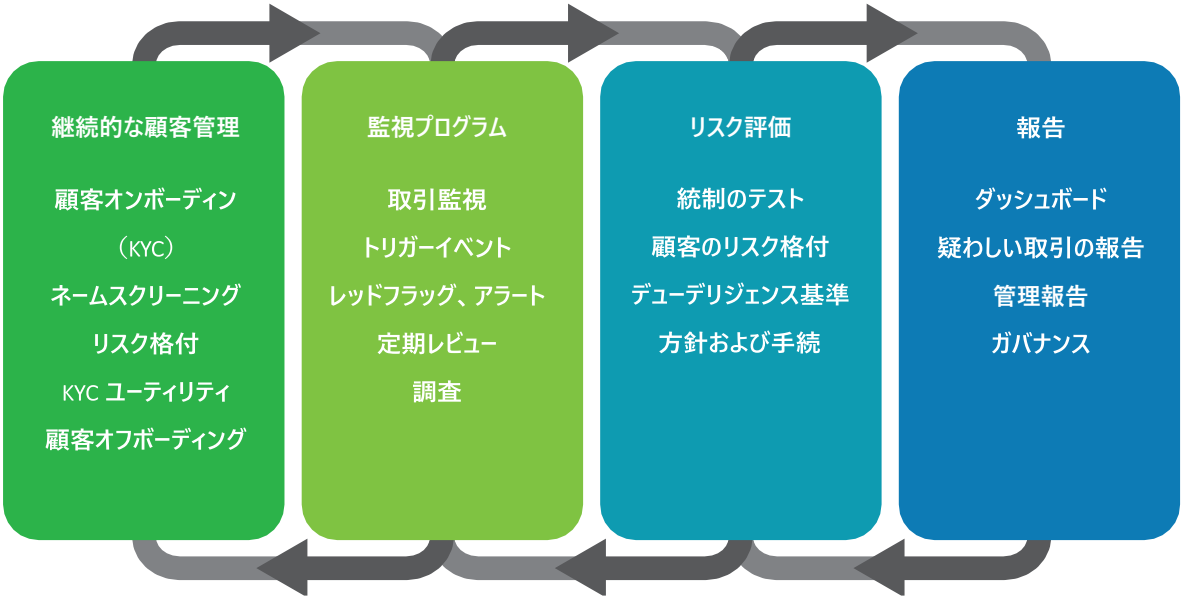
見直しとは、典型例としては縦割り型の運用で構造が煩雑な、レガシープロセスと設計原理を再設計することかもしれません。また、人為ミス、アジリティの欠如、複雑なオペレーティングモデルを含む関連課題が山積みの手作業プロセスを改善することかもしれません。

したがって、縦割り構造を打破し、企業の商品・サービスポートフォリオ全体に必要な安全策が確実に整備されるようにするためには、顧客体験の行程とコンプライアンスプロセスを綿密に計画した新たなアプローチが必要です。このコンプライアンスプロセスには、ノウ・ユア・カスタマー（KYC）、顧客の顧客に対するKYC（KYCC）、より厳格なデューデリジェンス、継続的監視、ネームスクリーニング、取引モニタリング、アシュアランス、リスク評価、報告が含まれます。

私たちはコンプライアンスプログラムには3つの段階があると考えています。

- 説明したとおり、第1段階は従来のモデルです。
- 第2段階は次世代コンプライアンスの枠組みです。金融機関は、AI/機械学習とRPAを重要なプロセスやテクノロジーに結び付けるイノベーションにより、金融犯罪管理の実効性を高めることを目指します。
- 第3段階は、金融犯罪の脅威を包括的に監視、分析することにより、未来的なアプローチへと前進することです。これはまだテストされていない段階です。

図1： 従来の金融犯罪コンプライアンスアプローチ



新たなアプローチ

この新たなアプローチを実行するためには、事業部門（第1の防衛線）とコンプライアンス部門（第2の防衛線）が、監視の必要な主な脅威、代表的な統制、リスクオーナーについて合意しなければなりません。米国では、連邦準備理事会（FRB）のガイダンスが、ビジネスリーダーがリスクオーナーに対して説明責任を負うという基調を打ち出しています。 同様に、シンガポールのMASは、取締役会とビジネスリーダーがマネー・ローンダリングおよびテロ資金供与リスクを事前対応的に管理する必要があるというガイダンスを示しました[8]。したがって、統制の実施は、コンプライアンス部門からの助言を得て、ビジネス部門が主導しなければなりません。

このガイダンスに沿って、イニシアチブの導入に向けた堅牢で包括的なロードマップを策定しなければなりません。つまり、第1の防衛線は、規制上の義務を理解する重要な役割を果たすとともに、適切なリスク低減措置と適切な統制の整備が確保されるようコンプライアンス部門と緊密に連携する必要があります。

金融犯罪コンプライアンスが取締役会のアジェンダと見なされることで、2つの防衛線間の協力は、強力なコンプライアンス文化を構築するとともに、金融機関と顧客の利益の長期的な防衛と維持を確保するものとなるはずです。

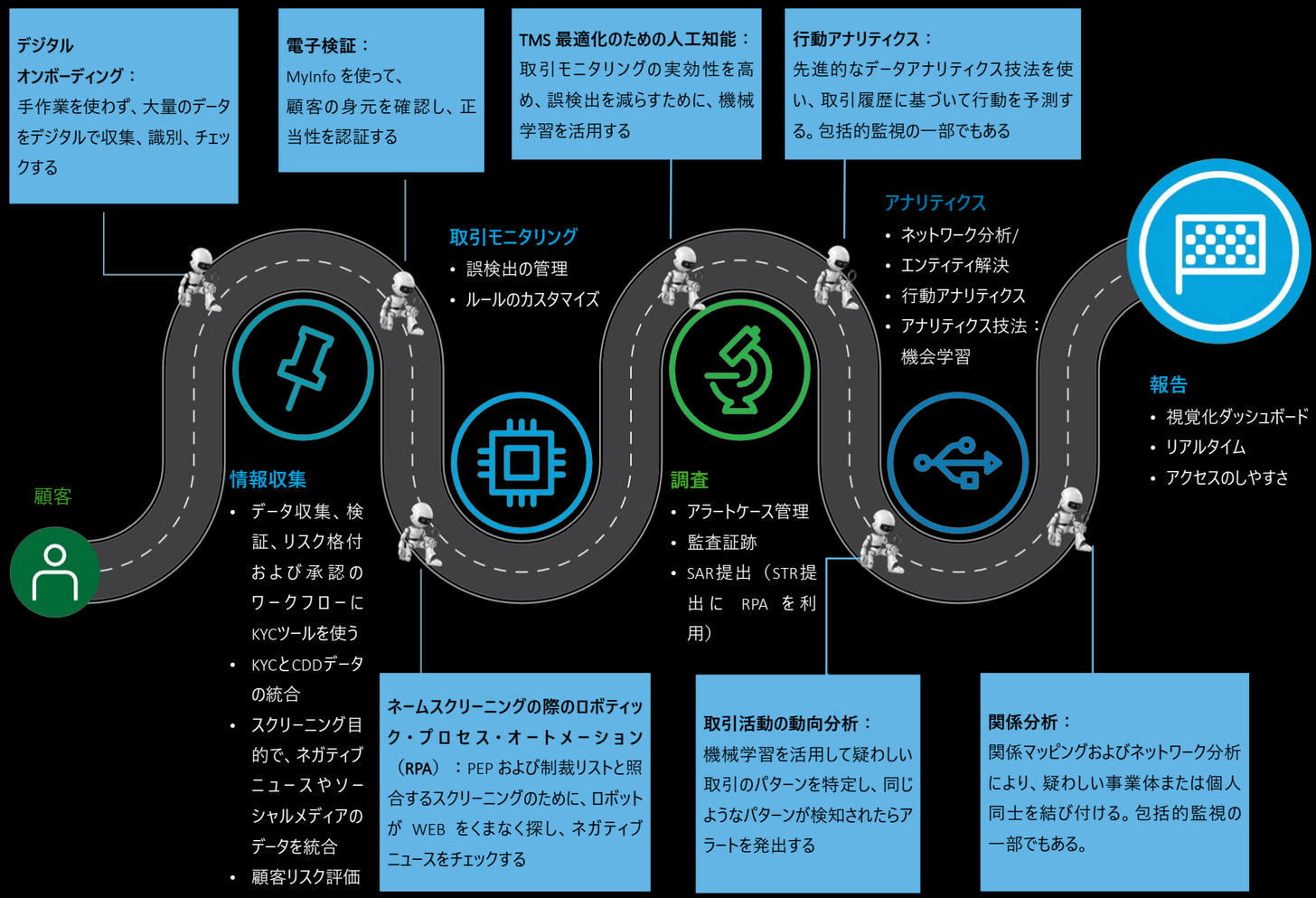
金融犯罪リスク管理体制全体で、バリューチェーンの中にデータアナリティクス、AI、機械学習、RPA、自然言語処理、認知インテリジェンスなどの技術革新を適用できる分野は多数あります。

テクノロジーを導入する方法は、金融機関ごとに異なります。取り組み方は主に、その会社のビジョン、短期・中期・長期目標、制約、デジタルトランスフォーメーションに対するリスク・アペタイトによって決まります。

顧客のライフサイクル全体でテクノロジーを活用する

イノベーションの主な機会および各段階で金融犯罪を阻止するためのテクノロジーとアナリティクスの活用方法

図2： 金融機関がイノベーションを通じてAI/機械学習とRPAを重要プロセスに組み込む、新世代のコンプライアンスの枠組みに対するデロイトの見解



ほとんどのトランスフォーメーションプロジェクトがそうであるように、業務の枠組みの内部の働きが成果と成功を支えます。

この行程では、技術の設計と実行を詳細に考察することが求められます。これには以下のような重要な側面への対応が含まれます:

- 施行されているEU一般データ保護規則（GDPR）およびシンガポールの「公平性・倫理・説明責任・透明性（FEAT）推進のための原則」に定められた、データプライバシーの新しい時代におけるデータの質およびデータマイニング
- 複数の情報源からのデータの統合およびデータセキュリティ
- AIや機械学習などの複雑なテクノロジーのガバナンス
- ハイブリッドな労働力：人材、機械および将来のスキル。

コンプライアンス要件に対してテクノロジーを管理・導入するため、そして望ましいビジネス成果を得るためには、すべての側面が必要です。コンプライアンス部門、データサイエンティスト、ITチームは、求められている目標を達成するためのアプローチの評価および整理において、極めて重要な役割を担っています。

スマート金融センターを目指すシンガポールの奮闘

2019年1月、シンガポール政府は、AIテクノロジーの導入に際して発生する主な倫理・ガバナンスの問題に組織が実践的に対処できるよう、「モデルAIガバナンスの枠組み」と題した指針を公表しました[9]。

具体的には、以下の4つの重点分野を取り上げています。

I. 社内のAIガバナンス体制および措置

II. 自律的意思決定におけるリスク管理

III. 業務管理

IV. 顧客関係管理

シンガポールはAIガバナンスを非常に重視しています。こうした姿勢から公表されたガイダンスは、AIを活用する可能性がある場合に、金融機関およびコンプライアンス実務担当者が考慮すべき重要原則を明確化した待望の内容となっています。

何を採用する場合でも一般的にそうであるように、ガバナンス、文書化、複雑なエンタープライズテクノロジーを取り扱うしかるべき人材とリソースをめぐって、懸念が生じます。

また、規制当局はAIモデルの本番稼働と採用に大きな期待を寄せている可能性があります。このようなモデルをテストする前に、まずは正当で体系的なアプローチを策定することに注力する必要があります。既存のリスクは以下に潜んでいます。

- データプライバシーおよびデータ保護規制違反（例：GDPR、PDPA、FEAT）
- 成果の正当性を主張できるか
- 不明確または矛盾する規制
- 基準や規制の欠如
- 監査証跡および追跡可能性の欠如

当局の見解を踏まえて、総合的な未来の金融犯罪コンプライアンスモデルへの中長期的な移行は、金融機関が置かれている金融犯罪リスク環境全体を包括的、継続的、知的に捉える機能を備えることを目指さなければなりません。そのためには、複数のチャネルからのデータソースの活用と分析に習熟する必要があり、金融犯罪コンプライアンス専門家と次世代テクノロジーが持つ専門知識の組み合わせを通じて、より大きな自信を持って金融犯罪リスクを正確に示せる必要があります。これには、金融機関にリスクをもたらし得る社内外の脅威の分析が含まれます。

そうすることにより、金融機関が早期検知能力を強化し、タイムリーかつ迅速に予防措置を講じ異常や疑わしい活動を報告できるようになることが期待されます。

金融犯罪コンプライアンスの予想される将来像への移行

将来像の設計には以下の検討事項が含まれなければならないと考えます。

1. **官民パートナーシップおよび情報共有。**例えば、国家レベルの KYC ユーティリティがあれば、顧客プロファイルの把握に必要な様々な情報源からのデータやインテリジェンスの評価が可能でしょう。これには、リスク格付された顧客とのつながりを、エンティティ解決を使って把握することが含まれます。定期レビューの実施方法は、最先端の技術力を活用して革新されなければなりません。これは、大量の書面収集によって誠実な顧客の体験を損なうよりも有意義だと考えられます。

2. **顧客オンボーディングは、融通の利かない兆候に基づいて顧客リスクを大まかに推測するのではなく、顧客のプロフィールプロファイルと金融犯罪の脅威に対する脆弱性に基づいて行うこと。**前者（大まかな推測）は、説得力のある証拠に基づいた情報が求められる複雑化が進む世界では魅力を失っています。

3. **真の脅威を評価するために、大量の誤検出が生じる厳格なルールを使うのではなく、AI および ML 機械学習モデルを使って、取引のスクリーニングとモニタリング監視を行うこと。**このプロセスは、枠組みに内蔵されている自動アシュアランス機能の中に、テクノロジーの活用を通じて組み込まれなければなりません。このような取り組みが、活用されるモデルの防御性および全般的な実効性と効率性についてのひとつの見解をもたらすことが期待されます。最終的な目標は、業界レベルのユーティリティが取引監視を引き受けることに置かれるべきでしょう。

4. 第 **1、第 2、第 3 の防衛線が実施するアシュアランス、**リスク評価および脅威ベースのリスク分析においては、あらゆるソースから入手したデータに基づき、デジタルプラットフォームを活用すること。固有リスクの算出においては、金融機関が実際にさらされている金融犯罪の脅威に関連するデータを考慮に入れる必要があります。これが、第 1 および第 2 の防衛線のアシュアランスプログラムにおける重点箇所を特徴付けるはずです。
リスクと統制の実効性は、商品・サービスに対して実施する様々なアシュアランスプログラムや分析、リスク評価、KYC、AI/機械学習を活用したスクリーニングや監視等を通じて組織全体で見つかった弱点を理解することにより、単一のアシュアランスプラットフォームから評価すべきです。

5. **あらゆる報告の要求に対して RPA およびデジタル化を活用すること。**これには社内報告と対外的報告の両方が含まれるため、数え切れないほどの報告書作成に伴う手作業を最小限に抑えます。RPA の活用により、手作業による報告では見逃しやすいつながりやテーマを抽出することも容易になるはずです。

6. **重大なリスクが見過ごされることのないよう、包括的監視を行い、コミュニケーションを完結させること。**

図3はデロイトの包括的監視モデルと青写真を簡略化した説明図です。

私たちは、包括的監視メカニズムとは金融機関内のあらゆる関連情報ソースからのデータを使って金融犯罪リスクの視覚化を変革することだと考えています。包括的監視により金融機関が重要なリスクを監視し、それに焦点を合わせられるようになることを期待します。このメカニズムは、予防措置を講じるための早期警告の兆候や組織内のどこにリスクが集中しているかの実態を示し、すべてのデータソースに基づいて組織がさらされる重大な脅威により強い焦点を当てます。

包括的監視メカニズムの設計にあたって、私たちは、脅威について学び評価する目的でのAIおよび機械学習モデルの活用、そしてリスクを視覚化し金融犯罪リスクに関連するデータを文脈に当てはめる目的でのデータアナリティクスの活用を検討しています。

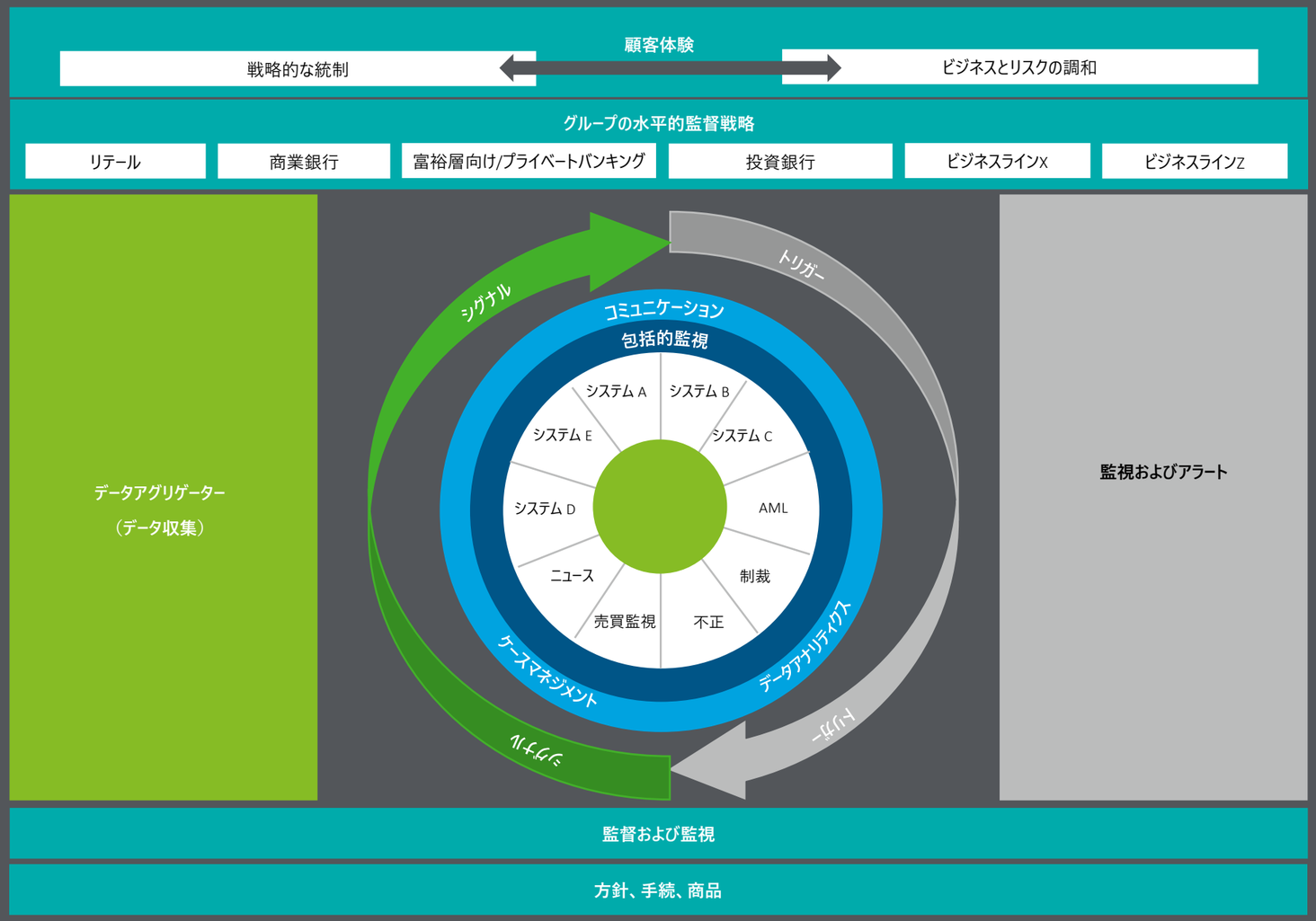


図 3：デロイトの包括的監視モデルの青写真。これは、デロイト（Delloite Touche Tohmatsu Services, Inc.）の知的財産であり、デロイトの書面による事前の同意または許可なく複写または複製することは禁じられていることにご留意下さい。

包括的監視アプローチの課題

最先端イノベーションを活用し、未知の領域に足を踏み入れるには、経営幹部のコミットメントが必要です。

したがって、主な課題は以下のとおりです：

社内の積極的な賛同を求めること。目に見える実績やデータポイントを伴っておらず、一見すると机上の空論のように思われる考え方を取り扱う場合には、簡単なことではありません。

サンドボックス環境において新たなアイデアのインキュベーション（培養）に取り組み、テスト環境を構築すること。目標状態に向かって取り組むためには、公的支援、時間、リソースが必要です。

インキュベーションが導入可能な結果の変容をもたらすよう確保すること。成功へのプレッシャーは、良きガバナンス、計画策定、合理的なスケジュール、データやレガシーシステムによるトラブル解決の問題とのバランスが取れたものでなければなりません。テストとアシュアランスにおいても、運用可能で、困難な課題に耐えることができ、説明のつく正当なアプローチを必要とします。

堅牢な選定プロセスを経て適切なパートナーを選ぶこと。

エコシステムの不在は、サステナビリティの観点から、この行程をさらに不安定で脆弱なものにします。

第3章

UOBの行程：今日の傍流、明日の優位

ユナイテッド・オーバーシーズ銀行（以下、「UOB」または「同行」）は、次世代テクノロジーを活用して強力なリスク重視の文化を持つ銀行になるというコミットメントを守り、常に変化する金融犯罪情勢に油断なく対処し続けています。

UOBの金融犯罪コンプライアンスアプローチ

UOBは、リスク重視の組織文化を維持することに重点を置いた取り組みの一環として、技術イノベーターや業界リーダーと連携してコンプライアンス能力の向上を図り、新たに出現するリスクの一歩先を行くことを目指しています。金融犯罪コンプライアンスの分野では、「AML/CFTテクノロジーロードマップ」を作成し、AIおよび機械学習主導型の次世代テクノロジーの活用によってマネー・ローンダリングおよびテロ資金供与に対抗しようとしています。

ロードマップの実行にあたっては、いくつかの要因が検討されました。UOBは、AML、CFT、制裁管理の実行に必要なアジリティ、拡張可能性、既存ITインフラとの相互運用性の観点から、同行のニーズに合いそうな多種多様のレグテックソリューションをレビューしました。最適なテクノロジーの選択は、投資利益目標、そして目に見えるメリットと成果を満たすだけでなく、最も重要なこととして、業績を促進し、同行の事業部門による顧客へのサービス提供方法を改善させられるものでなければなりませんでした。

UOBはまた、既存のルールベースのAMLシステムと並行して機械学習モデルを構築しています。目指すのは、機械学習モデルと他のAIの領域の活用により、ルールベースのシステムの範囲を超え、これまで以上のパフォーマンスを実現することです。

金融犯罪の実行方法は変化し続けており、リスクと脅威の状況を包括的に捉えることが重要となっています。UOBの「トリプルAアプローチ」（図4参照）は、同行が金融犯罪の一歩先を行き、より鋭く、賢く、迅速に高リスクの活動を検知できるように、AI、自動化、アナリティクスを活用しています。また、データやAIのスキルと経験を有する専門家のチームを拡充しました。デロイトはナレッジパートナーとして、AIと自動化のプロセスに同行と共に取り組みました。

UOBは、同行のコンプライアンスの目標の促進に役立つ適切なレグテックを評価するために、金融犯罪コンプライアンスの2つの分野 – 取引監視とネームスクリーニング – を識別し、新たなイノベーションをテストしました。次は、テストで成果を上げたイノベーションのうち、同行全体のコンプライアンス戦略と整合するものを実行に移す予定です。「トリプルAアプローチ」の採用、そして選別と分類を行い、最終的には重要事項に注力することから得られる有望な結果について、本章の残りの部分でご紹介していきます。

具体的には、

1. UOBのAIの行程の内側：AIの導入に向けたビジョンの実現
2. 自動化と人的資源の有望な組み合わせ
3. アナリティクスで洞察の限界を引き上げること

図4：取引監視に関するUOBの「トリプルAアプローチ」

❶

UOBのAIの行程の内側：AIの実装というビジョンの実現

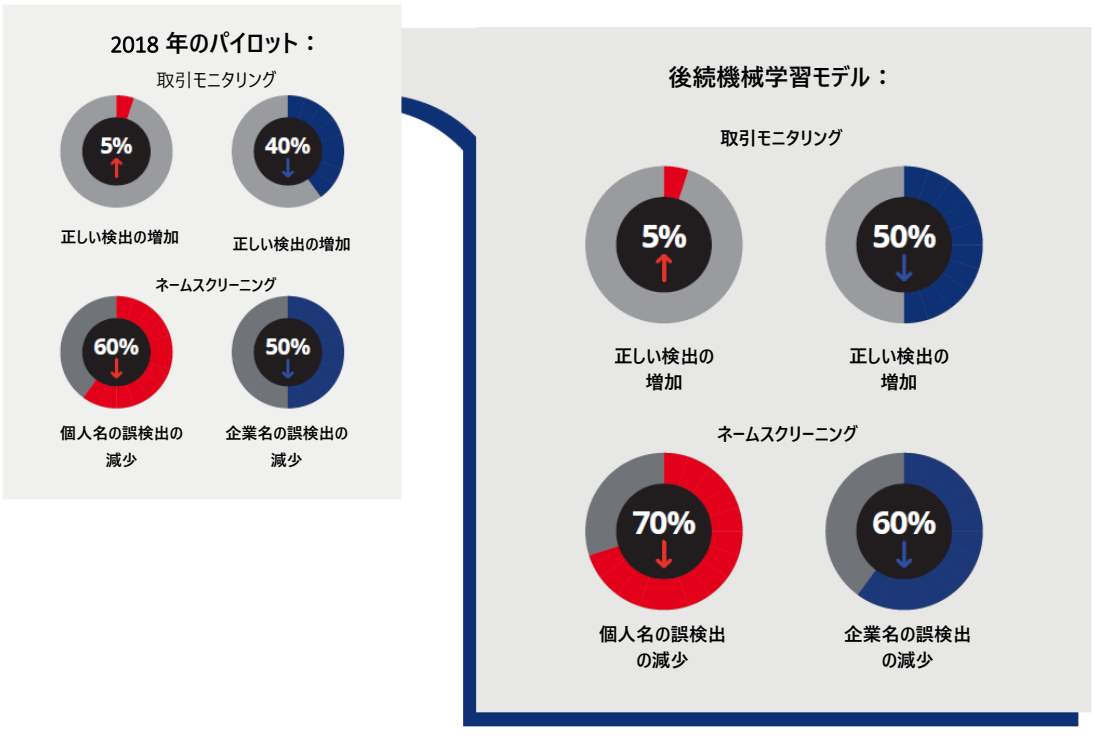
マネー・ローンダリングおよびテロ資金供与と闘うための機械学習モデルのパイロットプログラムが本格的に実施され、UOBは本番稼働に向けて前進しています。

2018年、UOBはマネー・ローンダリング防止プログラムの一部として機械学習を活用するために、シンガポールに拠点を置くレグテックのスタートアップ企業 Tookitakiと提携しました。Tookitakiの「マネー・ローンダリング対策スイート（AMLS）」は、エンド・ツー・エンドの取引モニタリングおよびネームスクリーニングシステムです。教師ありと教師なしの機械学習技法を組み合わせ、疑わしい取引の検知と高リスクの顧客の識別をより速く正確に実施しようとするものです。2018年のパイロットプログラムにおいて、デロイトは独立した立場からモデルの精度検証を行いました。具体的には、レビューと検証技法を用いて、同行の機械学習モデルの概念の堅牢性を評価しています。その結果の詳細については、UOBとデロイトの共著による白書の第1巻に収載された「UOB、Tookitakiおよびデロイトが、マネー・ローンダリングとの闘いを加速するための機械学習パイロットプログラムを準備（原題：UOB、Tookitaki and Deloitte readies machine learning pilot to accelerate the fight against money laundering）」と題したケーススタディに詳述されています。

2018年のパイロットプログラムの結果と後続機械学習モデルについて、下記説明図に示しました。

後続機械学習モデルは独自のデータセットでテストされましたが、**取引モニタリング**プロセスについては、2018年のパイロットプログラムでは誤検出40パーセント減だったのに比べ、後続機械学習モデルでは50パーセント減を達成しました。同様に、ネームスクリーニングプロセスについては、後続機械学習モデルは、個人名の誤検出が70パーセント減、企業名の誤検出が60パーセント減という好結果を出しました。

成功裡に終わった結果は、UOBに次の段階、すなわち機械学習モデルを本番運用段階に移すことに着手する自信を与えました。しかし、それに先立って、UOBはモデルの堅牢性を確実にするために、モデルの検証をもう1ラウンド行うこととなっています。



「私たちは、銀行の既存インフラ内で機械学習を使ったマネー・ローンダリング防止（AML）ソリューションを運用可能にする世界でも数少ない企業のひとつであることをうれしく思います。Tookitakiの「マネー・ローンダリング対策スイート（AMLS）」は、分散データ並列アーキテクチャと機械学習を組み合わせて使うことで、銀行の複数の事業分野および既存のテクノロジーとシステムの複雑な層全体にわたる拡張可能性を確保しています。

モデルの精度の高さ、継続的な学習、アウトプットについての詳細な説明、銀行の上流・下流システムとの統合の容易さにより、AMLSは、拡張可能な設計を有するすべての持続可能なAMLコンプライアンスプログラムにとって、最も適した選択肢となっています。

しかし、本番環境への導入の成功は、ソフトウェアベンダーと、銀行内のテクノロジー、AMLコンプライアンス、内部監査、モデル検証チームとの間の協調的な努力にかかっています。」

Mr Abhishek Chatterjee
Founder & CEO, Tookitaki

現在、UOB はデロイトおよび Tookitaki と積極的に協働し、機械学習モデルの本格運用開始に向けて本番前環境と本番環境の準備に取り組んでいます。

AML コンプライアンスへの機械学習モデル活用により、以下のようなメリットが実際に観察されました。

- 疑わしい取引の識別の実効性が向上する
- 基準値をトリガー要因にするよりも、データ異常に焦点を強く合わせることができる
- 特定のリスクを正確にターゲットにするためにデータ機能をカスタマイズしやすい
- 複雑なシナリオを検知するために、遡及対象期間を長期化できる

Tookitaki

- AMLS ソリューションは、Singapore Business Review から「AI in Banking」部門の優秀賞を受賞しました [10]
- AMLS ソリューションは、世界経済フォーラムの「Technology Pioneer Cohort 2019」のひとつに選ばれました [11]
- AMLS ソリューションは、「2019 SG:D Techblazer Award」の最も有望なイノベーションのカテゴリーで銀賞を受賞しました

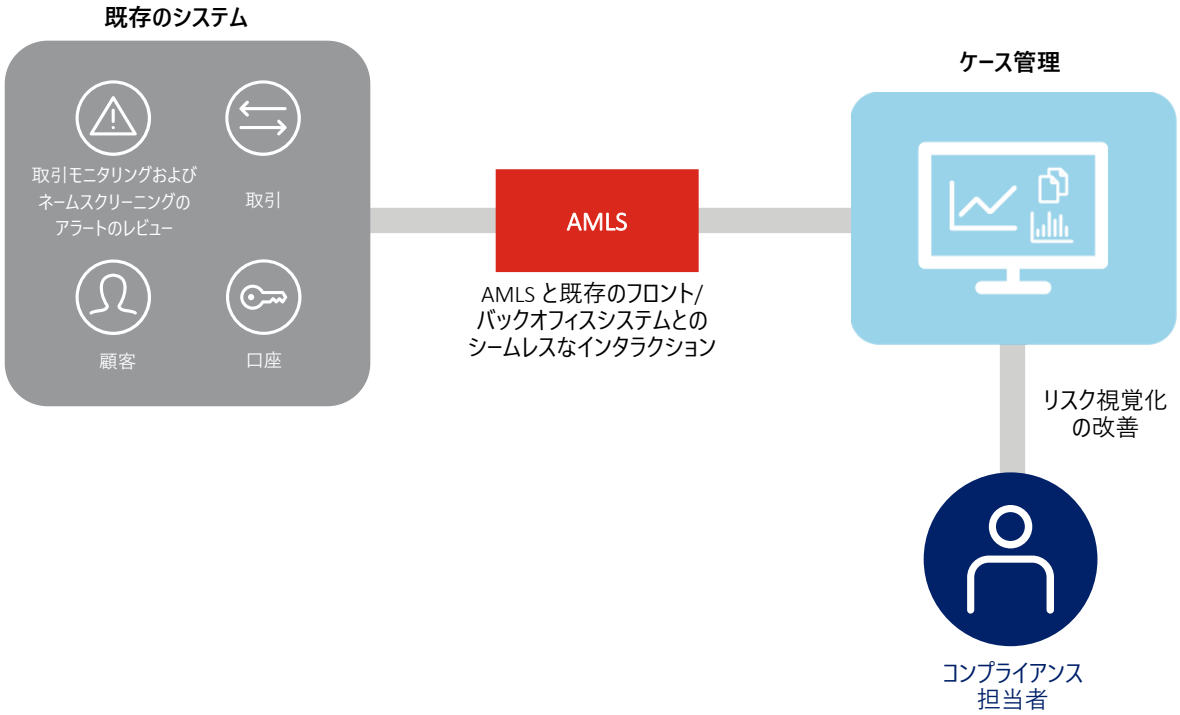
本番前の準備

この段階で新たなリスク要因が生じると、検討課題は増大します。UOBの複数の事業分野、そしてインフラやシステムの複雑な層全体にわたってモデルを拡張できるようにする前に、こうした課題を解決しなければなりません。

運用化

AMLSを運用可能にするにあたり、UOBの現行インフラにうまく統合できるか確認する目的で、実際のデータセットに対するモデルの信頼性を確認する追加のアシュアランスとテストが行われます。データ管理、プライバシーとデータの問題、そしてモデルを監督するための適切なスキルセットや能力の必要性といった検討事項も、機械学習モデルを本番移行することの意味を理解する上で不可欠な部分です。UOBはTookitakiと共同で、デロイトが実行する検証作業に従って、ここに概略を示した検討事項に対処しています。AMLSと同行の既存のテクノロジーおよびシステムとの統合に関しては、AMLSという新たな層を加えることで通常のビジネスプロセスや活動に中断が生じないようにするために、主要なステップが計画されています。AMLSの導入により、アラートからの出力ファイルは既存のケース管理システムとの互換性を持たせるように構築され、コンプライアンス担当者がアラートへのアクセスや調査の優先順位付けを容易にできるようになっています（図5参照）。このアプローチを持つことの利点は、コンプライアンスチームがすでにアラート管理のワークフローに精通しており、再研修は最小限で済むということでした。UOBは、価値の低いアラートには相応の注意が払われることを確保するために、ガバナンスレビューとアシュアランスプロセスに取り組んでいます。これは、UOBの堅牢なリスク管理アプローチとも一致しています。

図5



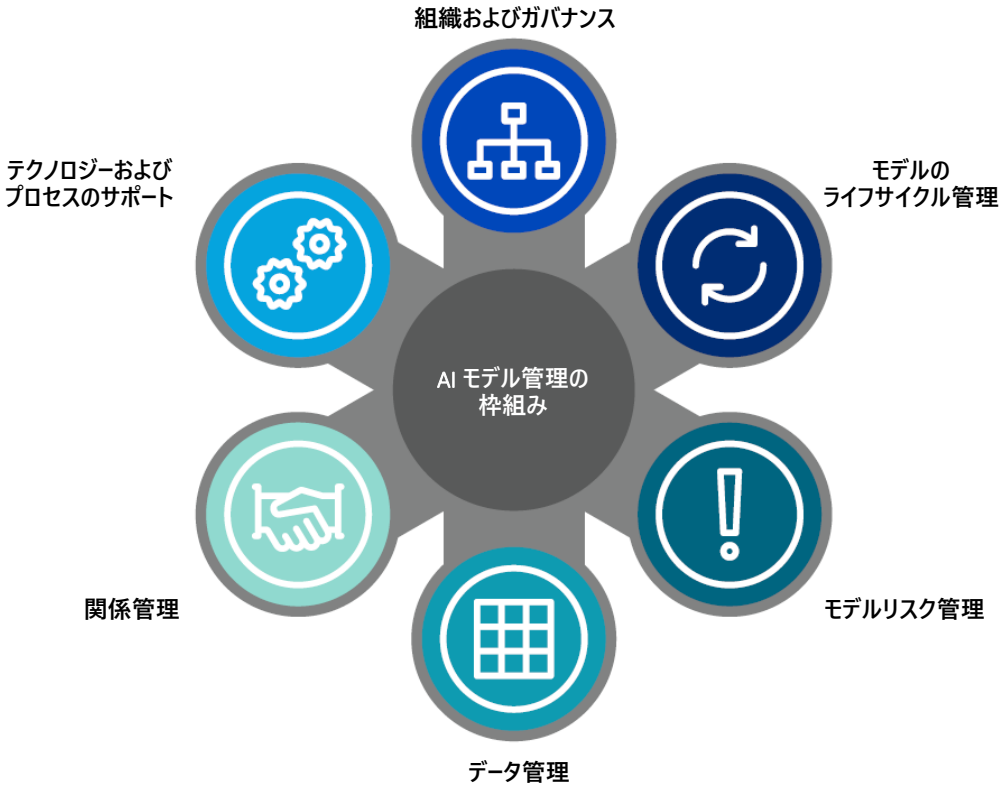
ガバナンス

監督とガバナンスの領域では、UOBは金融犯罪コンプライアンスにおいてAIを大規模に採用するための実務的なステップを策定する際に、シンガポールの「AIモデルの枠組み」からの原則も採用しました。UOBとデロイトは、金融犯罪コンプライアンスにおけるレジリエントなガバナンスの「AIモデル管理の枠組み」（図6参照）を協力して策定しました。これは機械学習モデル導入の最初の指針となるアプローチを形成しており、モデルリスク管理、バイアスの管理、モデルの説明可能性、データプライバシーおよびFEAT原則の適用、データ管理、モデルのアシュアランスおよびテスト、インシデントの解決が含まれています。十分に構造化されたフィードバックループを利用して、このような機械学習モデルの受容性に関する継続的なレビューを行うことが必要不可欠です。最終的には、同行にもたらされる脅威とリスクの判定は、人間であるアナリストの適正な判断によって決まります。後者はUOBとデロイトが共有する希望であり、規制当局、レグテック企業、金融サービスセクターなどが参加する広範なエコシステムを巻き込むことを目的としています。

同行は現在、本番移行の準備段階にあり、体系的なアプローチでモデルを微調整し拡大するために、運用化とガバナンス設計のレビューを行っています。最初に本番移行する機械学習モデルの稼働開始は、現在のところ2020年上半期を予定しています。

この機械学習モデルは、UOBの取引モニタリングとネームスクリーニングを行う既存AMLシステムの上位層として組み込まれます。つまり、UOBがAIと機械学習のプラットフォームを導入しても、既存のルールベースのシステムの最適化も継続されるということです。

図6：AIモデル管理の枠組み



機械学習モデルの活用に際して関連するガバナンスの課題:

- 機械学習モデルとアルゴリズムに影響を及ぼす**人間のバイアス**。人間のバイアスは可能な限りモデルから排除されなければなりません。バイアスを除去することで、金融犯罪コンプライアンスには不可欠の犯罪類型やレッドフラッグベースのモニタリングまで除去することがないよう、微妙なバランスを取り十分な注意を払うことが必要です。

- **透明性に対する懸念**および「ブラックボックス」設計。規制当局はブラックボックスを認めません。必要な取り組みのすべてに尽力し、モデルの説明可能性を確保しなければなりません。

- 金融犯罪リスク管理の実効性を高めるためには、イノベーションのメリットを明確に実証する必要性があるにもかかわらず、**使用方法とテクノロジーが正しく理解されないこと**。

- **ガバナンスが正しく理解されないこと**、倫理上の課題および適用。規制当局は、取締役会および経営幹部が金融機関に採用されたイノベーションを常に掌握していることを期待しています。また、アシュアランスを付与するために、プロセスを批判するモデルリスク管理が必要です。

- 「教師あり」および「教師なし」の学習に対する**統制**。

「価値観に基づいた銀行として、顧客に寄り添い、
顧客のために正しいことをするよう確保することが、
私たちのすべての行いの中心にあります。
UOBのコンプライアンス部門は、銀行内の
テクノロジーチーム、業務チーム、事業部門と
緊密に連携し、堅牢なコンプライアンス統制を維持し、
変化する業界の状況に遅れを取らないようにしています。
私たちは一体となって、強力なリスク文化を銀行内に確保し、
顧客に大きな違いをもたらすソリューションやサービスを設計する
イノベーションの原動力を補完することを目指しています。」

Victor Ngo Head of Group
Compliance, UOB
IBF Distinguished Fellow (2019)

❷

自動化と人的資源の有望な組み合わせ

規制コンプライアンスを維持することは、困難な作業になる可能性があります。特に、金融犯罪コンプライアンス活動の実施において、細分化された手作業のプロセスを使い続けている組織の場合は、困難が増大します。多数のデータポイント、ファイルの抽出および同期、報告書作成、ワークフローを考えると、RPAの活用は規制コンプライアンスの改善に効果的で有益なツールとなります。特に、ネームスクリーニング、取引モニタリング、アラートの解除、SAR/STR報告などには、自動化の機会が豊富にあります。これらは反復可能またはルーチン化されたルールベースのプロセスであり、人間の介入を最小限に抑えて実行できるため、RPAに最も適しています。

例えば、KYC改善におけるネームスクリーニングに対する従来のアプローチは、手作業が多く、反復的で、リソースを大量に必要とします。RPAを使えば、アシュアランスは高く、コストは低く、実行のスピードは高くなり、規模と価値を達成できます。特に以下のような具体的なメリットが確認されるにつれて、ロボットへの関心が高まり、活用が増えています。

- 生産性：ロボットは年中無休24時間体制で稼働可能。
- 効率、品質、正確性：人間は手作業でミスを起こしやすく、特にルーチン化された面倒な大量のアラートの場合にその傾向が出やすい。
- 時間と費用の節約：ロボットはピーク需要に合わせて規模を拡大させることが可能で、ルールベースの事務作業を引き継ぐことができる。

「これは私たちにとって絶えず続く行程です。私たちが優先するのは、すべての投資が目に見える成果を生み出し、概念実証後に銀行全体に規模拡大できるよう確保することです。結果として、公開実験を行うよりも、長い時間をかけてでも、ビジネスケースを熟考したり、適切なパートナーと連携して UOB 固有の状況の中で何ができるかに焦点を当てるのに力を貸してもらったりする方がよいと思っています。最終的に、当行のニーズに最も適しており、長期にわたって持続可能な成果を得たいのです。」

Victor Ngo
Head of Group Compliance, UOB
IBF Distinguished Fellow (2019)

デロイトは、UOBの自動化の取り組みの一環として、同行の取引モニタリングの枠組み内から選ばれたいくつかのプロセスの改善に役立つよう、RPAの導入を支援しました。これには、アラートレビューの追跡、アラートレビュー、アラートの割当、STRのアップロードおよびリスト作成などが含まれます。

RPAに関して言えば、これらの選ばれたプロセスは出発点であり、使用の有効性の試験台です。

RPAの導入により、UOBはマンアワーを30パーセント削減し、反復可能な手作業プロセスを自動化するメリットを実証しました。

その他の実現したメリットには、以下のような事項が含まれます。

- 手作業だった活動の自動化によるエラー率の低下
- コンプライアンス向上および活動の監査可能性の向上
- アナリストチームが実施する手作業時間を削減し、節約できた貴重な時間をより価値の高い作業に配分すること
- 同行全体の取引モニタリングプロセスの標準化
- 「ロボット」のバリューチェーン： RPAから収集したデータは他の下流プロセスにも使用可能

UOBは効率向上を歓迎していますが、RPAの最善の成果は、監督と運用を改善できるところにあります。

前述のメリットを考慮すると、UOBのアナリストチームは疑わしいアラートに対して今までよりはるかに大きな注意を払えるようになり、金融犯罪の検知と防止において、調査に関する専門知識と独自の価値判断を最大限に活かせるようになります。

長期的に見ると、UOBが手に入れる価値は、より強力なリスク管理の枠組み、そして人間と機械の連携作業によるシナジー効果です。取引モニタリングにおけるRPAの活用の成功が実証されたことを受けて、UOBはコンプライアンス業務の枠組みの他の分野へのRPA導入を検討する予定です。

「トリプルAアプローチ」は、RPAの活用によって、ネームスクリーニングと取引モニタリングのプロセスに連続性を生み出すことを模索しています。例えば、機械学習の活用によりアラートの選別プロセスの有効性が高まれば、その次のプロセスである高リスクアラートの処理または調査は、RPAの導入によって迅速に最適化されるでしょう。

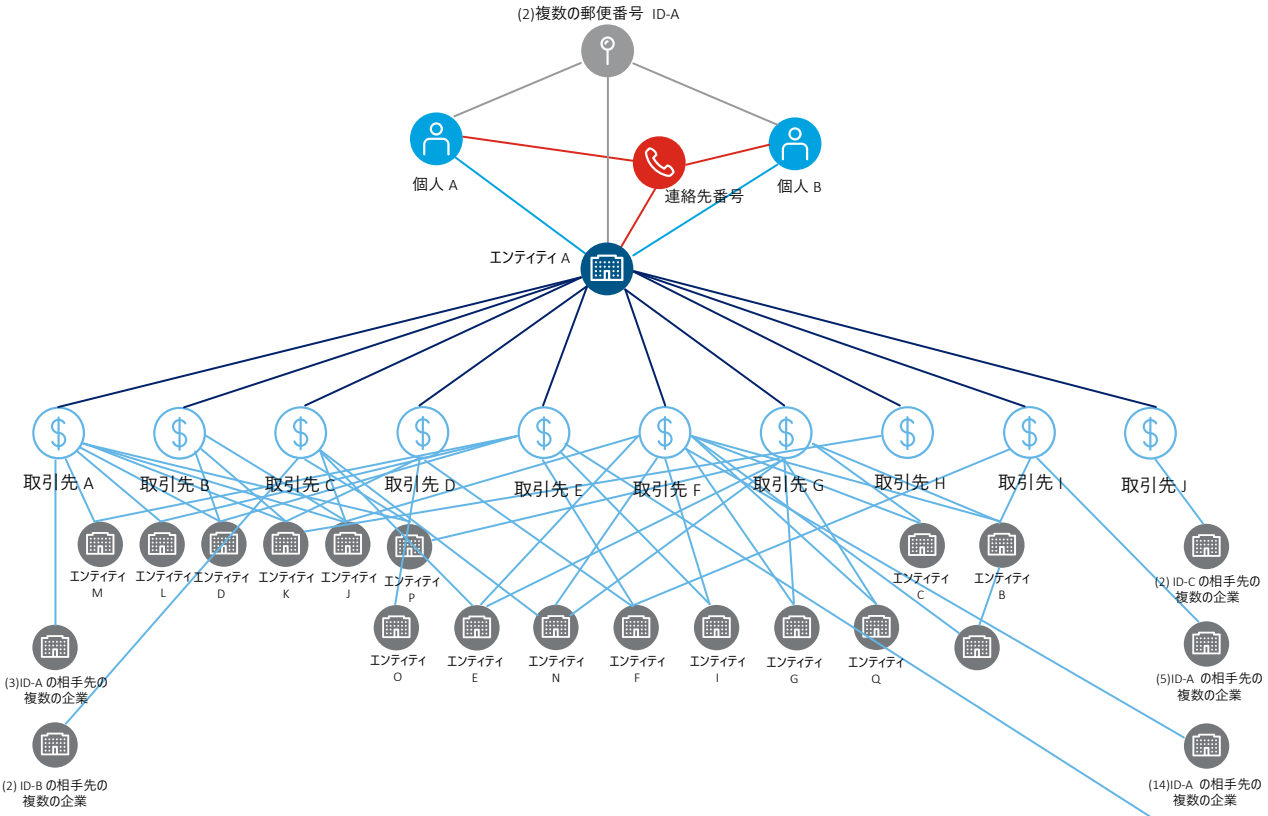
図 7：The use of RPA in UOB's 'Triple-A approach'.

❸

アナリティクスで洞察の限界を押し広げる

数多くのチャネル、システム、インフラが支配する現在のハイパーコネクテッドな世界において、ペタバイト規模の情報やデータポイントを抱える組織は、金融犯罪との闘いに向けて知的なアプローチを採る必要があります。その中核となり得るUOBの「トリプルAアプローチ」は、金融犯罪のもたらす問題を防ぐために高度なアナリティクスなどの多様なテクノロジーを組み合わせ、より良い対策を提供しています。UOBは、社内で開発されたネットワーク分析アプローチにより、資金フローの分析能力の強化に注力し、隠されたつながりや異常、重層化により関係隠ぺいを図る高度なスキームの発見に努めています。

図8：



凡例

- SG ディレクター
- フォーカスエンティティ（クラスターグループ内）
- エンティティ（クラスターグループ外）
- 送金
- 共通の連絡先（メール、電話）
- 共通の住所

1. オーナーシップ：BO（個人 A）はシンガポールの非定住外国人
2. KYC：エンティティ A は登録住所であり、BO（個人 A）の住所から企業秘書会社（個人 B）の住所が明らかになった
3. KYC：エンティティ A BO（個人 A）と個人 B（企業秘書）の共通の連絡先（電話、メールなど）
4. 支払情報：エンティティ A が送金/TT 指示書に記載した会社住所も、会社秘書と同じ住所になっている

例えば、ペーパーカンパニーや実質的支配者の問題に取り組むために、UOBはリンク（つながり）分析を使い、直接・間接的な関係を評価・特定し、ペーパーカンパニーの特徴を持つ不正資金フローを追跡しました。複数の情報源からのデータ（例：取引データ、顧客プロファイルデータ、共通の連絡先詳細、取引先データ）を組み合わせることで、UOBは高リスクの疑わしい行為をより正確に評価できるようになりました。

孤立した口座をレビューする従来型の方法を使っていると、つじつまの合わない関係や異常な送金・取引を推定するための分析に何カ月もかかる可能性があります。ネットワーク・リンク分析を使うことで、UOBは、AMLおよびCFTリスクを伴うネットワーク化された関係の絞り込みと調査を数日以内に行う能力を持ちました。

技術の進歩とグローバルな商取引の増加により、組織犯罪シンジケートは状況に適応し、グローバル金融経済のギャップとクロスボーダー取引の普遍性を悪用するためのテクニックを進化させ続けています。資金フローを追跡し、真の資金源や富の源を隠すために設立された会社を識別する能力を持つことは、銀行にとって決定的に重要です。ネットワークアナリティクス（図8参照）の活用により、循環するループ状の資金フローを識別できるようになりました。

成果

ネットワーク・リンク分析により、UOB はレビューの迅速化と効率の向上を実現しました。

つまり、ネットワーク化された関係の調査に要する期間が、数カ月から数日に短縮されたということです。

さらに、UOB はその中から疑わしい取引を突き止め、その結果、50 以上の関係を終了することになりました。

第4章

新しい世界に備える

どのテクノロジーを活用するかを決定し、それを様々なビジネス目的にマッチさせ、規制コンプライアンスの期待に応えることは、非常に骨の折れる作業です。しかし、銀行が競争力とレジリエンスを保つためには、進化する金融犯罪の問題に取り組むための新たなアプローチを用いることが重要です。

業界のプレイヤー（金融機関に限らない）は、人材の能力構築、AI、機械学習、RPAおよび金融犯罪コンプライアンスの認知技術のプレイヤーとユーザーの十分な育成、そして未来のインフラアーキテクチャに対して投資を行っていく必要があります。

大胆な提案を持って一歩踏み出した者は少ないものの、金融犯罪コンプライアンスの未来は確かにここにあります。取引モニタリングとネームスクリーニングだけではなくすべてのプロセスにAI、機械学習、RPA、NLPを活用する金融犯罪コンプライアンスの将来像は、設計の途上にあります。

目標は、金融犯罪コンプライアンスのオペレーティングモデルの設計に、これまで以上の実効性と堅牢性をもたらすことです。

より良い監視アプローチとは、何もかもを監視しようとすることでリソースを痩せ衰えさせ、それにより集中力と勢いを失うのではなく、脅威ベースでなければならないと考えます。

究極のモデルは、KYC、顧客デューデリジェンス、取引モニタリングのための業界レベルでのコンプライアンスユーティリティの増加です。そのために、この同じコンプライアンスユーティリティは、技術的には次世代テクノロジーによって駆動されるべきです。同じように、金融機関が未来に進む中でこのようなユーティリティとつながる準備を整えるために自らイノベーションの行程を始めることについては、説得力のある理由があります。

これを達成するために、現在、コンプライアンスやデータが競争優位性を奪うという誤った考えに妨げられることなくデータや洞察を共有できるような官民パートナーシップの必要性が高まっています。

そのような共有は、脅威の統一基準や分析という形のメリットを生む可能性があります。それは、リスク監視能力の強化に有効なだけでなく、より長期的な効率向上ももたらすでしょう。

金融犯罪コンプライアンスを確保するためのテクノロジー活用にさらなる進歩が見られれば、UOBによる機械学習モデル採用から得られるさらなる学び、エコシステム構築の発展に関する私たちの考え、包括的監視アプローチの成果について、今後情報を提供する予定です。情報には私たちの見解も補足します。そのときまでに、その見解が金融犯罪コンプライアンスの未来にとっての目標になっていてほしいと願っています。

銀行は、仕事の将来像に備えるために、人材管理アプローチを刷新する必要があります。自動化、ギグエコノミー、クラウドソーシング、人口動態の変化はすべて、将来の仕事のやり方に影響を与えます。将来的には、問題解決と独創性による価値の創出がこれまでよりもはるかに重要となります。機械が主流となる世界において、問題解決スキルが、独創性、判断力、説得力、共感力を使いこなす必要があります。学習を加速させる必要があると同時に、学んだ知識を他者に伝えることも優先事項としなければなりません。

出典：Talent: With the future of work near, learning how to learn could be crucial, p13, 2019 Banking and Capital Markets Outlook, Deloitte

早急な投資対応が必要な重要分野は以下のとおりです。

スキルおよび専門知識：新たなテクノロジーやイノベーションが仕事の性質を変えていく中で、金融機関のコンプライアンス担当者が金融犯罪コンプライアンスの領域内のテクノロジーを監視・監督する必要性が高まります。

エコシステムの構築：銀行が今すぐ活用できるエコシステムがなければ、意図的にエコシステムを「構築」する必要があると思います。これは、金融犯罪との闘いの中で直面する数々の課題に対して浮上しつつある答えの持続可能性を確保するためです。「一度限りの成功の奇跡」になるのを避けるために、慎重に策を練る必要があります。

既成概念の枠を超え、他のプレイヤーに同じ行程に乗り出すよう勧誘するために、成功談を共有することは、ただ重要なだけでなく必要不可欠です。エコシステムがあれば、活動に拍車をかけ、能力を強化し、価値を創出し、イノベーションの成功を実現できます。それによって、強力で進化した参加者の需要と供給が生み出され、業界全体がその恩恵を受けるでしょう。UOB はエコシステムの構築への貢献に向けて革新的な対策を講じてきました。

「シンガポールはデジタル競争の最前線に立っており、真っ先に創造的破壊の的になるのは金融機関です。技術革新がニューノーマルとなり、明確な目的、動機、意思決定を持って速いペースの変化に対応しなければなりません。シンガポール初のAIモデルによるガバナンスの枠組みに従って、私たちのチームはUOBと共に、極めて重要な行程に乗り出しています。金融犯罪コンプライアンスの未来は、新しい観点から捉えられる可能性があり、スマートテクノロジーとのシームレスな連携により、リスクと機会の両方の角度からより優れた洞察を得られる場としての重要性は高まっていくでしょう。」

Ho Kok Yong
SEA Financial Services Leader, Deloitte

巻末注

1. Radish Singh, Nick Lim, Eric Ang, 'The Case for Artificial Intelligence in combating money laundering and terrorist financing', Volume 1, November 2018, Deloitte and UOB, https://www2.deloitte.com/sg/en/pages/financial- advisory/articles/the-case-for-artificial-intelligence-in-combating-money- laundering-and-terrorist-financing.html
2. Val Srinivas, Angus Ross, 'Accelerating digital transformation in banking', October 9, 2018, https://www2.deloitte.com/us/en/insights/industry/ financial-services/digital-transformation-in-banking-global-customer- survey.html#endnote-sup-2
3. Bernardo Arnaud, 'Open banking, and what it means for European fintechs and consumers – part 1', September 12, 2019, https://www.eu-startups.com/2019/09/open-banking-and-what-it-means-for-european-fintechs-and- consumers-part-1/
4. Financial Conduct Authority, 'Global Financial Innovation Network (GFIN), August 9, 2019, https://www.fca.org.uk/firms/global-financial-innovation- network
5. Mr Tharman Shanmugaratnam, 'Banking Liberalisation's Next Chapter: Digital Banks', Keynote address by Senior Minister and Chairman, Monetary Authority of Singapore at The Association of Banks in Singapore's Annual Dinner, June 28, 2019, https://www.mas.gov.sg/news/speeches/2019/ banking-liberalisations-next-chapter-digital-banks
6. DigFin, 'How UOB will position its digital bank', September 3, 2018, https://www.digfingroup.com/uob/
7. Monetary Authority of Singapore, Media Release, 'New regulatory framework to enhance payment services in Singapore', November 19,2018, https://www.mas.gov.sg/news/media-releases/2018/new-規制当局の- framework-to-enhance-payment-services-in-singapore
8. Monetary Authority of Singapore, Guidelines to MAS Notice 626 on prevention of money laundering and countering the financing of terrorism, April 24, 2015, https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/規制当局の-and- Supervisory-Framework/Anti_Money-Laundering_Countering-the- Financing-of-Terrorism/Guidelines-to-MAS-Notice-626--April-2015.pdf?la=en&hash=4ADAD30E6B7E97D4E67B3650AFC90F72639C2571
9. Personal Data Protection Commission, Singapore, 'A proposed model AI governance framework', first edition, January, 2019, https://www.pdpc.gov. sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Model-AI- Framework---First-Edition.pdf
10. Singapore Business Review, 'Tookitaki Holding takes home AI Award for banking at SBR's inaugural Technology Excellence Awards', 31 May 2019, https://sbr.com.sg/co-written-partner/more-news/tookitaki-holding-takes- home-ai-award-banking-sbrs-inaugural-technology
11. World Economic Forum, Technology Pioneers 2019, https://widgets.weforum.org/techpioneers-2019/companies/tookitaki/

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイトトーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイトトーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT 弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約 30 都市以上に 1 万 5 千名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト（ www.deloitte.com/jp ）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTL および DTTL の各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTL はクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。
デロイト アジア パシフィック リミテッドは DTTL のメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける 100 を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務、法務などに関連する最先端のサービスを、Fortune Global 500®の約 9 割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来 175 年余りの歴史を有し、150 を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約 345,000 名のプロフェッショナルの活動の詳細については、（ www.deloitte.com ）をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001