

尾崎寛氏



松下隆一



金融庁 総合政策局

マネーロンダリング・  
テロ資金供与対策企画室長

金融 × IT 対談

株式会社野村総合研究所

金融グローバル事業推進部長

Profile/Hiroshi Ozaki

1988年 三井銀行入行（現 三井住友銀行）。三井住友銀行米州統括部（在ニューヨーク）、同欧阿中東本部（在ロンドン）、同中東総支配人兼DIFC（ドバイ）支店長、同総務部付部長兼AML金融犯罪対応室長を経て、2018年2月 金融庁総合政策局マネーロンダリング・テロ資金供与対策企画室長。現在に至る。米ニューヨーク大学経営学修士（MBA）、公認AMLスペシャリスト（CAMS）。

Profile/Ryuichi Matsushita

1992年 野村総合研究所（NRI）入社。都市計画、事業開発コンサルティングを担当。2000年 NRIネットワークコミュニケーションズ出向。03年 NRIに戻り企画部、アジア事業推進室を経て、08年 NRIと三菱商事と合併会社である上海菱威深信息技术有限公司（iVision上海）に出向、副総経理。14年 NRIシンガポールに出向し、金融システム事業を担当。17年より現職。

金融のグローバル化が進んだ現在、マネー・ロンダリング・テロ資金供与対策は、各国が連携して取り組むべき事項であり、国際機関FATFによって対応状況の審査も実施されている。審査の結果が悪ければ、国の信用に直結する。日本の金融機関がすぐにでも実行すべき対策は何か、金融庁 マネーロンダリング・テロ資金供与対策企画室長の尾崎寛氏に語っていただいた。

### AML/CFTの第一歩は KYC

**松下** FATF（Financial Action Task Force：金融活動作業部会）による対日相互審査（以下、FATF審査）オンサイト直後のお忙しいところ、お時間をいただきありがとうございます。今日は、今後のマネー・ロンダリングやテロ資金供

与対策（以下、AML/CFT）のポイントについて伺いたいと考えています。

2019年10月に金融庁から出されました「マネー・ロンダリング及びテロ資金供与対策の現状と課題」（以下、「現状と課題」）に、今回のFATF審査では、法令等の整備状況とともに対策の有効性も審査対象になることが記載されていました。前

回のFATF審査以降、様々な法整備がなされてきましたし、18年2月には「マネー・ロンダリング及びテロ資金供与対策に関するガイドライン」（以下、ガイドライン）も出されました。AML/CFTの枠組みという点では取り組みが進んできたという認識です。

今後、対策の実効性を高めていくという観点からはどのようなことが

重要になるのでしょうか。

**尾崎** まずは、AML/CFTのミニマム・スタンダードであるリスクベース・アプローチ（以下、RBA）にしっかりと取り組むことだと考えています。犯罪収益移転防止法などの関連法令とともに、ガイドラインを遵守していただくこと。そして、ガイドラインにある「対応が求められる事項」への取り組みのスピードを上げていただきたいと考えています。

AML/CFTの第一歩は「本人確認」です。口座開設時や取引開始時の「本人確認」を日常業務の基本動作としてしっかりやっていただくことが重要です。特に相手が法人の場合、実質的支配者が誰なのかを見極めつつ、制裁対象者や反社会的勢力のリストと照合して、不適切な取引を水際で排除していただくということです。その上で、顧客属性、商品・サービス、取引形態、国・地域等の要素を勘案し、顧客リスク評価を行う必要があります。

そして、取引開始後も顧客のリスクに応じ、ITシステムや窓口職員の検知によるモニタリングを行い、不自然な取引があった場合、「疑わしい取引の届出」につなげることが重要です。

口座開設時の本人確認では問題がなかったにも関わらず、その後において問題のある顧客になってしまうケースもあるので注意が必要です。このようなケースを検知するには、取引パターンの変化をとらえなければなりません。システムで検知することになるとは思いますが、どのようなシナリオであれば適切に検知できるかを定期的に検証する必要があります。

ます。そして、本人の現在の実態確認が欠かせません。これを対象者のリスクに応じた頻度で行うことが重要です。

**松下** 「本人確認」の精度を高め、維持するということ、つまり、それぞれの金融機関の顧客データの品質が問われるということですね。

**尾崎** その通りです。顧客属性データが最新のものでないと、「本人確認」や顧客リスク評価の有効性を担保することができません。

顧客属性等の情報をアップデートするには、顧客に確認することになるため、顧客にも負担をかけることになります。顧客数も多いですし、大変な作業になることは承知していますが、自らの顧客を守り、日本の金融システムを守る、そしてこれが自身（金融機関）を守ることにもつながりますので、顧客の理解を求めながらやっていただきたいと思います。

**松下** 「本人確認」がAML/CFTの最初の一步であることはよくわかりましたが、最近では、お客様のお客様はどうなのかということも話題にあがります。KYC（Know Your Customer）を超えたKYCC（Know Your Customer's Customer）です。

**尾崎** ガイドラインでもKYCCまでは求めておりません。

KYCCについては、コルレス銀行を例に説明するとわかりやすいと思います。A銀行が、外国のB銀行とコルレス契約を結んでいるとします。A銀行、B銀行のそれぞれに求められているのは、相手方の銀行を見極めることを自らの管理態勢の中に組み込むということです。相手先

の顧客のKYCまでの対応は求めないものの、相手方がどのような顧客管理をしているのか、どのようなリスク管理態勢で取り組んでいるのかを確認する必要があります。

**松下** 顧客情報を管理する相応のデータベース、また、顧客情報は機微なものですので、データガバナンスも重要になってきます。

**尾崎** 金融機関の規模にもよりますが、AML/CFT管理のための顧客情報は紙でファイルするといった類のものでなく、顧客リスク評価に基づいた評価の見直し及びその管理が可能となるレベルのデータベースの整備が求められます。例えば、顧客情報の最新性を保つための期日管理など、本人確認業務のタスクも管理できるようなデータベースが必要です。それぞれの業態や規模に見合ったもので良いので、是非、データベースの整備を進めていただきたい。

また、データベースやITシステムは導入して終わり、というわけにはいきません。定期的に検証し、検証結果を踏まえて必要に応じ改善を図ることが求められますし、管理や調整に専門的な人材も求められます。その観点から、金融機関の業務規模に関わらず活用できるような、ITシステムや事務の共同化の検討が重要になってくると思います。昨年度から全国銀行協会では、このような共同化に関する研究が進められています。そこでの成果物を今後どのように実際に活用していくのかを真剣に考えていく必要があると思います。

**松下** AML/CFTは預金取扱金融機関にとどまらず、金融機関全体の課題です。そのような意味では、この



## AML/CFTの第一歩は「本人確認」です

研究会の成果を基に業態横断的な共同化に結びつけていくことも考える必要があるのではないのでしょうか。

**尾崎** そうですね。預金取扱金融機関に限らず、システム共同化が促進されることは望ましいと思います。

### AML/CFTにおける リスクベース・アプローチ

**松下** AML/CFTの考え方の基本にあるのが、RBAです。規制対応はともするとルールベース・アプローチ的に臨んでしまうことになりかねません。

**尾崎** 冒頭にも申し上げましたが、RBAはまさしくミニマム・スタンダードです。ではRBAとは、何をすればよいのか？

顧客属性、商品・サービス、取引形態、国・地域など地理的要因、最低限、これら4つの項目に着目して、それぞれにどのようなリスクがあるのかを特定します。そして、そのリスクの大小を評価します。評価は定性的なものでも、スコアリングなど定量的なものでもいいのです。これが包括的、網羅的にできているかが重要なポイントです。

実は、コンプライアンス部門は金融機関自らが扱っている商品・サービスのすべてを把握しきれてい

ない可能性があります。まず、商品・サービスを扱う部門ですべての洗い出しをしないと行けません。そして、「預金」とか「送金」というざっくりとした区分だけではなく、包括的かつ具体的に検証すること。その上で、それぞれのリスクを特定し、評価を行う。コンプライアンス部門は、リスクの評価に応じたリスク低減策がとられているかどうかをしっかりと確認する。これが第1ステップです。

次に、顧客リスク評価です。4つのリスク項目、すなわち、どのような顧客属性の人が、どのような商品・サービスを、どのような取引形態で、どのような国・地域にかかる取引なのか、といった情報を集約し、総合的に顧客リスク評価をするのが第2ステップです。

**松下** そうしたリスク評価を基に、リスクの低減策をとるということで

**尾崎** そうです。これには取引そのものに着目したリスク低減策と個々の顧客に着目したリスク低減策の2つがあります。

RBAという観点では、ここまですべてがミニマム・スタンダードで足元の課題としては、こうした対応のスピードアップであると考えています。

**松下** 金融機関のなかには、例えば、顧客のリスク評価で、リスク項

目を多く設定し過ぎて、評価（リスクスコア）にほとんど差が出ないということもあるようです。当初の段階ではリスクが浮き彫りになるようにリスク項目を絞り、徐々にリスク項目を充実させていって、評価のレベルを上げていくことが必要ではないかと思います。

**尾崎** その通りです。RBAのもう一つのポイントは、ダイナミックなプロセスであることです。

「PDCAサイクルを回す」とも言えます。リスクを評価し、リスク低減策を講じる。その結果、リスク低減策がどれくらい効いていたのか、この商品・サービスに関しては適切なリスク低減策だったのか、「疑わしい取引の届出」は減ったのか、または増えたのか、ということを確認するということです。

プログラム全体の評価を行った上で、足りない部分に関しては追加的に行う、リスク評価が細か過ぎるのであれば集約する、といったような見直しを少なくとも年に1回はやっていただき、それを毎年回していくことが重要になると思います。

**松下** 見直しの際、気をつけるべきポイントはどこでしょうか。

**尾崎** 自らが直面しているリスクをどう把握するかです。「疑わしい取引の届出」の中身や、特殊詐欺被害の状況を分析する、リスクが低減しているのか高まっているのか、それは金融機関の一般的な状況と比べてどうなのかといったこと等を分析することで、地に足の着いたリスク評価につながると思います。

国家公安委員会が出している「犯

罪収益移転危険度調査書」も参照してください。

**松下** リスクの分析など、AML/CFTの高度化のためには、他行とのナレッジの共有も重要になってくるのではないかと思います。

**尾崎** おっしゃる通りです。そこは、各業界団体が中心となって、それぞれの業界で共有していただきたいと思います。金融庁としても、金融機関の現状と課題を示したレポート等必要な情報を発信していきたいと考えています。

また、FATFのRBAのガイダンスにも、国ごとのベスト・プラクティスが掲載されています。そういった海外の情報も参考になると思います。

## ITベンダーへの期待

**松下** 野村総合研究所は、金融機関に情報システムを提供していますが、AML/CFTの観点から、ITベンダーに対する期待がありましたらお聞かせいただければと思います。

**尾崎** AML/CFTに使うデータベースやITシステムには、フィルタリング、スクリーニング、モニタリングの分析系システムと、ケースマネジメントのための業務管理系システムがあると思います。

ITシステムは絶えず見直していく必要があり、スクリーニングシステムであれば曖昧検索機能が適切な設定なのかどうか、モニタリングシステムであればシナリオが有効なのかどうかを検証し、調整を続けていかなければいけません。また、One

fits to allのものではなく、金融機関それぞれの事業特性によって変わってきます。その辺りのきめ細かい調整を金融機関とITベンダーが一緒になって推進できる体制があるといいと思います。

また、ITシステムやデータベースの有効性を検証するツールを考えていただけたらありがたいです。例えば、内部監査部門や外部の監査法人が、独立した立場からITシステムやデータベースの有効性検証を行うことができるツール。そうしたものを是非考えていただきたいというのがあります。

**松下** 例えば、検知すべき顧客情報や取引を忍び込ませた有効性検証用データのようなものを金融機関に提供し、それを金融機関のITシステムで分析してみて、「どれだけきちんと検知できますか」ということでしょうか。

**尾崎** それも一つだと思います。検証用データを流してみても、誤検知の比率を内部監査部門が確認できると良いと思います。そういうところも独立した立場のITベンダーやコンサルティング会社がサポートできるのいいのではないのでしょうか。また、客観性や独立性の観点から監査法人などの第三者が行うこともあり得るでしょう。

**松下** 11月に「Singapore FinTech Festival 2019」が開催されました。昨年と比べると、KYCの変化を感じます。オルタナティブデータといった外部データまでを持ち込んできて、KYCの精度や事務効率を上げる製品やベンダーが目立つようになりました。

**尾崎** 非構造化データまでを含めた情報の収集や分析、例えば、さまざまなソーシャルメディアを見に行って、そこから情報を得るというような、ITを活用して、顧客に紐づく情報を自動的に収集して、顧客情報を充実させていくのが、次世代のKYCではないかと思っています。そのためには、まずは顧客属性や銀行に届けなければいけない、法令で定められている情報を常に更新して最新の状況に維持しておく必要があります。

**松下** 金融機関に限らず、あらゆる産業でデジタルトランスフォーメーション（DX）が経営課題となっています。DXの肝は、KYCとデータガバナンスであり、そうした意味では、AML/CFTで蓄積したKYCやデータガバナンスに関する知見やノウハウがDXにも活かせる、AML/CFTの経験が生きる、ということも言えそうですね。

**尾崎** その通りです。AML/CFTも取り扱う情報量の多さから、DXの世界に移行していくと思います。ただし、個人情報保護については十分に留意する必要があることは言うまでもありません。

**松下** 本日は貴重なお話をありがとうございました。

(文中敬称略)

