統合的対策システムによる、サイバーセキュリティ、不正防止、AML態勢の強化

金融犯罪に対抗するための統合的な態勢構築

Building a united front on financial crimes

pwc

www.pwc.com/jp

日本翻訳版発刊にあたり

これまで本邦で「金融犯罪」というと、主に振込詐欺やインターネットバンキングによる預金の不正払い戻しが想起され、預金などの取り扱い機関が対策すべきものとみなされてきました。

しかし、グローバルなビジネスシーンにおいては、マネーロンダリングやテロ資金供与対策を始めとする、「決済、融資、運用、保険・保証などの幅広い金融機能に対する濫用（不正使用）」や「金融システムの信頼や健全性を損なう行為または犯罪」といったより広範な概念を「Financial Crime＝金融犯罪」と位置付けることが一般的です。このような捉え方は、本邦でも徐々にデファクトスタンダードになりつつあります。

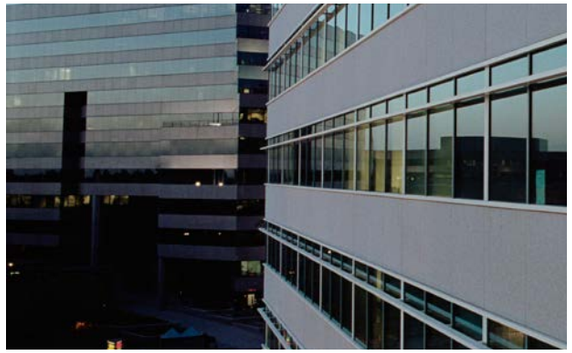
その結果として、金融機能を提供したり金融システムを利用したりするさまざまな企業に対して、自身の行うビジネスを俯瞰的に捉え、金融犯罪に関するリスクを理解・把握した上で、統合的な対策を行うことが求められるようになってきました。

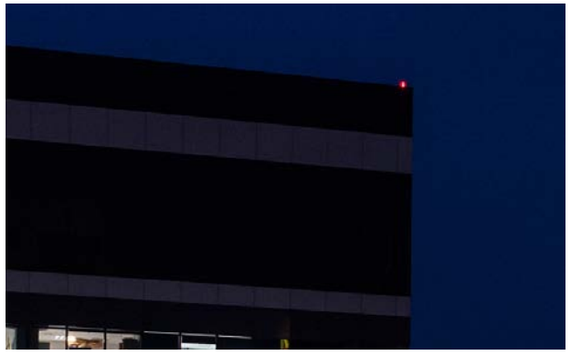
前述の広範囲な金融犯罪のリスクを適切に管理するためには、テクノロジーの活用やデータマネジメントの実践が欠かせません。近年、クラウド環境の浸透・低価格化と、ビッグデータの蓄積を前提としたディープラーニング技術などの進化が加速しています。特に大規模な金融機関にとっては、「データレイク」を構築して企業の情報を統合的・整合的に管理することの有用性が増しています。

もちろん、企業にとって適切な態勢やインフラは、ビジネスの規模や特性によって大きく異なります。そのため、画一的なパッケージソリューションを導入することがゴールとはなりません。企業は自身のビジネス・企業文化・地理的特性・顧客層などを正しく把握し、それに伴う金融犯罪のリスクを特定・評価することを通じて、初めて適切な施策を見いだせます。その結果、効果的・効率的なソリューションを構築することが可能となります。

本レポートが、統合的な態勢構築の必要性・有用性への気付きや社内での態勢検討のきっかけとなれば幸いです。

目次





はじめに

2016年2月、ニューヨーク連邦準備銀行は、バングラデシュ中央銀行からの指図を受けて1日で5件、総額1億米ドル超の引き出しを行い、この資金はスリランカとフィリピンの口座に送金された。しかし後に、これらの指図はバングラデシュ中央銀行が行ったものではなく、サイバー犯罪者が不正な送金指図によりシステムを欺いたものであったことが判明した。当局はこれにタイムリーに反応し、犯罪者が口座から資金を引き出すのを阻止することができなかった。スリランカに送金された資金は回収されたが、フィリピンに送金された8,100万米ドルの大半はフィリピンのカジノ業界で消失した。

バングラデシュ中央銀行の事件は近年の大規模なデータ漏洩事件の一つであり、データ漏洩が、何億人もの消費者に影響をもたらし、また攻撃者がどのように金融機関のサイバーセキュリティ、不正、マネーロンダリング対策（AML）の弱点をつくかを示している。金融機関におけるこれらの機能は通常、サイロ化されており、連動を欠いている。それはつまり、金融機関が、不完全なデータや不十分なコミュニケーションにより、作業やプロセスを繰り返しているということでもある。

サイバー攻撃、不正、マネーロンダリングを別々の金融犯罪として捉えるのは誤りである。不正取引やサイバー関連の盗難は、違法に獲得された資金が他の口座に送金されることに繋がり、これはマネーロンダリングスキームの第一段階にあたる。

資金を盗む行為、すなわち不正は、ユーザーデバイスに対するマルウェア感染、もしくはユーザーの認証情報を盗むフィッシング攻撃など、システムにおけるサイバーセキュリティの弱点を巧みに利用する可能性がある。バングラデシュ中央銀行の例では、攻撃者がまず管理システムやネットワークのログインシステムを迂回するカスタムマルウェアを設計し、サイバーセキュリティの弱点をついた。そして、銀行のネットワークに不正にアクセスするためにバングラデシュ中央銀行の認証情報を用いた。また詐取した資金を受領し転送するために不正な銀行口座を開設するなど、不正管理の抜け穴を悪用している。そして最終的には、フィリピンのカジノを通じて詐取した資金を洗浄したのである。

金融機関はサイバー犯罪を危惧しているが、これを阻止する最適な方法は知られていない。PwCが行ったグローバル情報セキュリティ調査2018（GSISS）や第21回世界CEO意識調査によると、企業のCEOや役員は、サイバー攻撃をビジネス上、最も懸念する脅威としてあげている。しかし、GSISSでは、回答者の44%が包括的な情報セキュリティ戦略を策定していないと答えている。また、PwCの経済犯罪実態調査2018では、グローバル企業の約半分が過去2年の間に不正の被害に遭っていることが明らかになっており、この数は2016年から13%増加している。金融機関が、脅威の状況をより明確に把握し、不審な取引を迅速に特定するとともに、調査を効率的に行うためには、サイバーセキュリティ、不正対策、AML管理を統合的に強化する必要がある。

統合できる対策・統合すべき対策

サイバーセキュリティ、不正防止、AMLプログラムには共通する要素や管理体制があり、人員、プロセス、テクノロジーの全体を通じて多くの相乗効果が期待できる。今後、多くの企業は、統合すべき特定のプロセスと、分割したままにしておくべきではあるが、より緊密な情報共有が必要なプロセスがあることに気付くだろう。

データ管理は、プロセスの統合を検討する上で最も重要な分野の一つである。これまでサイバーセキュリティ、不正防止、AMLの業務がサイロ化されてきた理由の一つは、データソースが異なるシステムに分かれ、組織内で個別に保管されていることにある。例えば、AMLプログラムは顧客の属性データ（国籍、年齢、住所など）や取引履歴を保有し、不正防止プログラムは、口座の異例な動きや口座設定の変更情報を記録する。またサイバーセキュリティはデバイス、ユーザー、ネットワークのデータを収集していると考えられる。これらの情報を「データレイク」に蓄積し、一元的なアクセス手段を提供することで、組織は、ネットワーク上で何が行われ、誰がどの口座やシステムにアクセスしているかをより詳しく把握することができる。また、外部から得た脅威・脆弱性情報も、データレイクに加えられるべきである。

表1：データの保管場所

データ種別	主なデータオーナー	データ保管期間／使用期間
エイリアス（別名）、Eメールアドレス、住所、電話番号などのユーザー識別情報	AML、不正防止	数年間
IPアドレス、地理的位置、メーカー、OS（基本ソフトウェア）、アプリケーション識別子（またはユーザーエージェント）などユーザーのデバイス情報	不正防止	数カ月から数年間
ログイン／ログアウト、アクセスエラー、アカウント・ロックアウト、パスワード再設定などのシステム・アクセス（顧客およびユーザー）履歴	不正防止、サイバーセキュリティ	数カ月から数年間
顧客／ユーザーの取引、支払指示、サービス・アプリケーション（例えば、クレジットまたはローン）	不正防止、サイバーセキュリティ	数年間
Eメールやファイル転送などによるデータの移動	コンプライアンス、サイバーセキュリティ	数カ月から数年間
新規の特権ユーザーまたは特権の変更、デバイス／アプリケーション／プロセス開始/停止、ソフトウェアや設定の変更などのシステム変更履歴	サイバーセキュリティ、IT業務	数カ月から数年間
作成、閲覧、更新、削除（CRUD）などのデータ／ファイルへのアクセス履歴	サイバーセキュリティ	数日間から数年間

その他、金融機関が統合を検討すべき分野として以下があげられる：

- **リスクアセスメント：**サイバー、マネーロンダリング、不正のリスクアセスメントを統合することで、企業におけるリスクの全体像を示すことが可能になる。
- **ケースマネジメント：**マネーロンダリングや不正の兆候を示すアラートは、同一の管理ツール（市販のパッケージソフトウェアであるActimizeやMantasなど）を使用することでより効果的・効率的に処理することが期待できる。
- **カスタマー・エクスペリエンス：**この分野での統合は、金融犯罪防止の観点とは異なるが、顧客に対して、同じ情報の提出を複数回求めたり、異なる分野からの審査承認を待たせたり、非効率なプロセスを排除することで、顧客との軋轢を回避することができる。

これらのタスクとプロセスを統合することで、金融機関は金融犯罪の防止に適切に対処することが可能となるが、それ以外にも、決済の迅速化やオープンバンキングといった新たなテクノロジーの可能性を追求することにも繋がる。金融機関は、不審な取引があった場合、即座に差し戻しできるようにする必要がある。なぜなら、顧客は決済やその他のリクエストが瞬時に処理されることを当然のこととして期待しているからである。支払指図の真偽を見極めるために、ユーザーが使用する携帯端末のモデルやIPアドレス、過去の決済履歴などといった顧客の行動パターンを即座に参照できるようにしなければならない。これは金融機関内で情報共有の仕組みが整い、完全なデータを得ることができるようになって初めて可能となる。

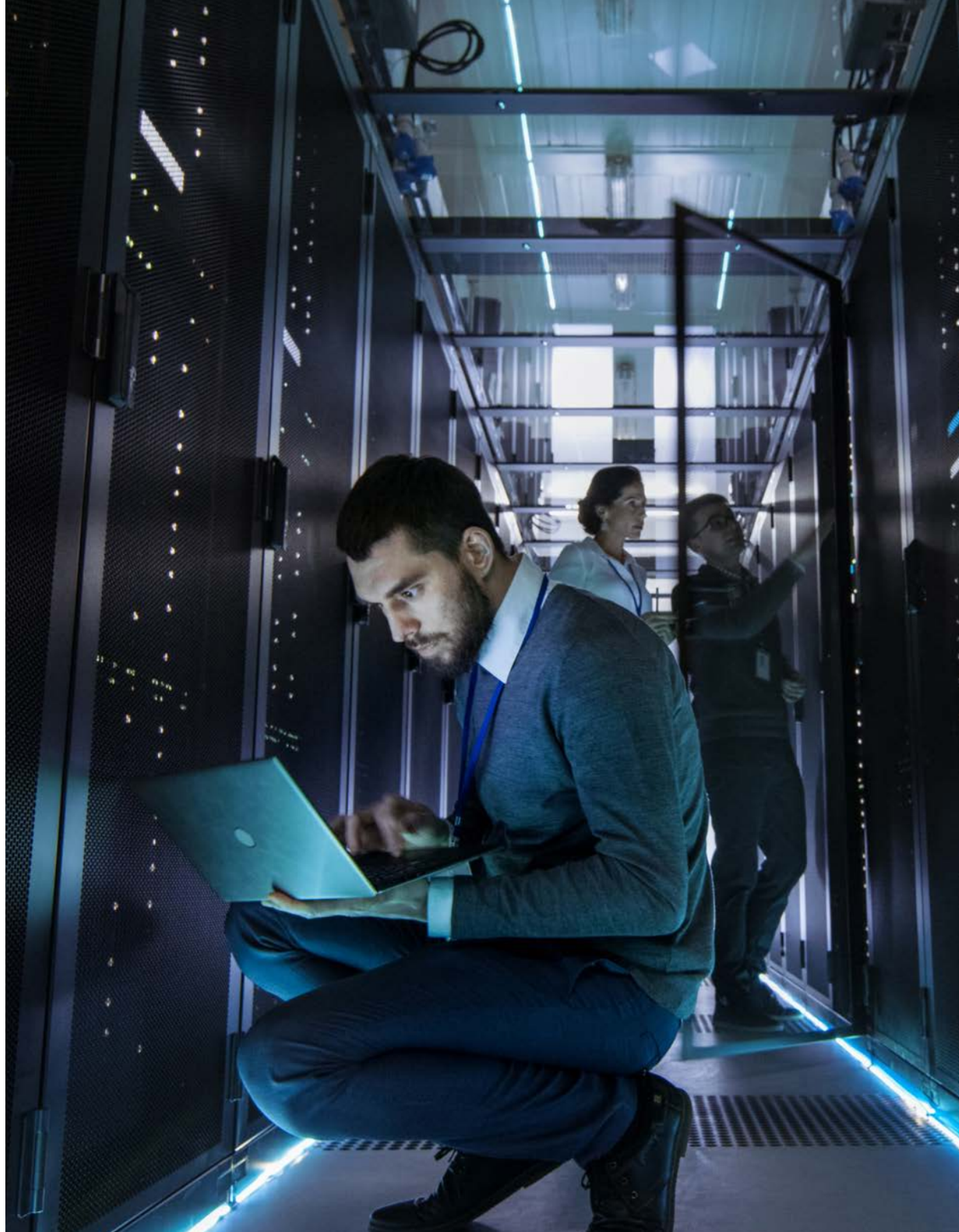
金融機関は不審な取引があった場合、即座に差し戻しできるようでなくてはならない。なぜなら、顧客は決済やその他のリクエストが瞬時に処理されることを当然のこととして期待しているからだ。

いかに統合するか?

金融犯罪防止プロセスの統合を実現するためには、プログラム全体の骨格となる明確な運用モデルを構築することが重要である。効果的な運用モデルが成り立つためには、構造、監視、機能というそれぞれの構成要素が適切である必要がある。

構造：金融機関は、金融犯罪リスク委員会やその方針、エスカレーションの手順、組織構造、人事、職員の配属や意思疎通のモデルから成る企業全体のガバナンスモデルを規定すべきである。これには、組織における三つの防衛線の全体にわたり、その役割、責任、コミュニケーションを具体化（そして明確に文書化）することが含まれる。三つの防衛線とは、不正リスクの管理・対処に一義的な責任を負う事業部門、不正リスクの監視および管理を担う独立したリスク管理部門、そして不正リスク管理に対して独立した監査を通じて保証を提供する内部監査部門である。

こうしたタイプのガバナンスモデルを構築するにあたり、金融機関はどのチームであれば合併可能であるかを見定め、プロセスを統合する必要がある。このような方法を用いることで、重複する作業を洗い出し、整理することができる。例えば、エスカレーションされたマネーロンダリングのアラートを調査する専門チームと、同じようにエスカレーションされた不正のアラートを調査する別の専門チームを設置するのではなく、合同チームを設置して両者に対応することが考えられる。マネーロンダリングに関する調査業務と不正に関する調査業務には重複する内容が多いため、データの可視性が向上すれば、合同チームにより対処する方がより効果的であろう。



統合プロセスの第一段階として、経営幹部や取締役会が金融犯罪リスクを一元的に把握できるよう、企業は現行の報告体制を見直し、合理化する箇所を特定すべきである。

監視：金融犯罪の防止にかかわるさまざまな規律を効果的に管理するために、全社にわたるガバナンスのフレームワークを構築し、サイバーセキュリティ、不正防止、AMLプログラムの管理・実施・監視を支援する金融犯罪リスク委員会を正式に設置すべきである。そうすることで、金融犯罪の防止戦略や方針の実行が可能になる。また、事業部門が戦略を策定するにあたり、金融犯罪に対するリスク許容度を確実に理解し、考慮することができるようになる。統合プロセスの第一段階として、経営幹部や取締役会が金融犯罪リスクを一元的に把握できるよう、企業は現行の報告体制を見直し、合理化する箇所を特定すべきである。これはサイバーセキュリティ、脅威・脆弱性情報、物理的なセキュリティ、不正防止などを含む関連業務を、チーフ・セキュリティ・オフィサーの下に集約するということにもなるだろう。

また、物理的なセキュリティは、金融犯罪システムが統合されることにより、特に内部の脅威プログラムを補完し、さらに不正の犯人を特定することで、重要な役割を担うことができる。この分野は見落とされがちであるが、共通のケース・マネジメント・システム、インテリジェンス、法の執行にかかる協力、行動分析など、重要な相乗効果が存在する。

機能：標準化されたプロセスや、単一のケース・マネジメント・システムおよび一貫性のある根本原因分析といった中央集権型のテクノロジーソリューションを用いることで、協調的で効果的かつ再現しやすい調査プロセスを実行することができる。

また、グループ間の情報共有は、包括的な調査を促進し、またこれにより組織は一つのフレームワークの中で、一貫性のあるプロセスの育成を余儀なくされるだろう。こういった対応により、全体的なリスクは軽減する。AML、サイバーセキュリティ、不正防止管理を収束することは、金融機関がいかに規制義務も果たしながら、これらのプロセスを統合するかを改めて考察する機会となる。

おわりに：万能薬はない

適切なソリューションは組織により異なり、さまざまな要因を踏まえて決まるものである。例えば提供する製品・サービス、地理的拠点、現地の法律および規制上の要求事項、顧客層などがあげられるが、これに限られるものではない。

では、今後、企業はどのような行動をとるべきなのだろうか？

- 他の金融犯罪対策部門の責任者と打ち合わせをもち、統合案に関する議論を始める。ここでは、短期的な利益を明らかにし、フィードバックを引き出すことで、対話を継続する。

- 活用できるさまざまなテクノロジーやツールを見極め、より効果的なソリューションの導入に向け必要なステップを決定する。

プロセス統合への道のりは、特に大規模で複合的な金融機関にとって、容易なものではなく、即座に対応できるものでもない。ただちに統合の機が熟す場合もあれば、将来的に統合すべきものや統合すべきではない（今後も別々であるべき）ものもある。重要なのは、組織が統合についてすぐさま話し合いを始めることである。

お問い合わせ先

John Garvey
Global Financial Services Leader
PwC US
+1 (646) 471 2422
john.garvey@pwc.com

Paul O'Rourke
Global FS Cyber Leader
PwC Australia
+61 419 109 214
paul.orourke@pwc.com

Sean Joyce
Global Financial Crimes Leader –
US and Americas Cybersecurity
and Privacy Leader
PwC US
+1 (703) 918 3528
sean.joyce@pwc.com

Grant Waterfall
EMEA Cyber Security and Privacy Leader
PwC UK
+44 7711 445396
grant.r.waterfall@pwc.com

Alex Petsopoulos
Partner
PwC UK
+44 07941454210
alex.petsopoulos@pwc.com

Richard Horne
Partner
PwC UK
+44 (0)20 721 33227
richard.horne@pwc.com

Andrew Rosenberg
Manager, Financial Services Advisory Practice
PwC US
+1 (646) 335 4495
andrew.r.rosenberg@pwc.com

Michael Horn
Manager, Financial Services Advisory Practice
PwC US
+1 (646) 471 8052
michael.b.horn@pwc.com

Reema Bagai
Manager, Internal Firm Services
PwC US
+1 (646) 471 8801
reema.bagai@pwc.com

日本のお問い合わせ先

PwCあらた有限責任監査法人

〒100-0004　東京都千代田区大手町1-1-1
大手町パークビルディング
Tel: 03-6212-6800

西川　嘉彦
パートナー
yoshihiko.nishikawa@pwc.com

加藤　俊直
パートナー
toshinao.kato@pwc.com

竹内　秀輝
パートナー
hideki.h.takeuchi@pwc.com

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立して事業を行い、相互に連携をとりながら、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、法務のサービスをクライアントに提供しています。
PwCは、社会における信頼を築き、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界158カ国に及ぶグローバルネットワークに250,000人以上のスタッフを有し、高品質な監査、税務、アドバイザリーサービスを提供しています。
詳細はwww.pwc.comをご覧ください。

本報告書は、PwCメンバーファームが2018年10月に発行した『Building a united front on financial crimes』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。　www.pwc.com/jp/ja/knowledge/thoughtleadership.html
オリジナル（英語版）はこちらからダウンロードできます。　www.pwc.com/gx/en/industries/financial-services/publications/presenting-a-united-front-on-financial-crimes.html
日本語版発刊年月：2019年2月　管理番号：I201810-3