protiviti®
Global Business Consulting

COMPLIANCE INSIGHTS

コラボレーション：サイバー犯罪と金融犯罪をより効果的に管理するための方策

キャロル・ボーミエ、バーナディン・リース著

サイバー犯罪と関連する金融犯罪を効果的に管理するため、情報や教訓を共有することは、ますます重要になってきています。そのため、金融機関はこれまでのリスク管理方法を見直す必要があります。

私たちは、第４次産業革命の中にいます[1]。驚異的な技術の進歩は、私たちの生活や仕事の在り方を変え、これからも変え続けるでしょう。これらの進歩は、莫大な利益をもたらすだけでなく、秩序を乱す行為を誘発する可能性も秘めています。

この秩序を乱す行為は、欧州や米国で発表された最近の報告書が示すように、そのほとんどが経済的利益の欲求を動機とするサイバー犯罪の急激な増加に表れています[2,3]。2020年、米国司法省は、ハマスの軍事組織であるアル＝カッサム旅団、アル・カイーダ、イラクとレバントのイスラム国（ISIS）の３つのテロ組織が関与する、サイバー攻撃によるテロ資金調達行為を摘発したと発表しました[4]。こうした現実は、サイバーリスクマネジメントチームと金融犯罪対策チームの更なる連携強化の必要性と、そのメリットの可能性の両方を示唆しています。

複数の国・地域においては、サイバー犯罪がマネー・ローンダリングの前提犯罪であり、当該国・地域内のマネー・ローンダリング／テロ資金供与対策（AML/CFT）の優先事項であると明確に認識されているにもかかわらず[5,6]、金融犯罪とサイバーリスクの管理は、従来、金融機関において別々に行われてきました。しかし、サイバー犯罪と金融犯罪の検知のため、根本的に、金融機関は次の同じ質問に答

1 Fourth Industrial Revolution, World Economic Forum, www.weforum.org/focus/fourth-industrial-revolution.

2 2022 Data Breach Investigations Report, Verizon, www.verizon.com/business/resources/reports/dbir/.

3 “Cybersecurity: Main and Emerging Threats,” Euroreporter, February 7, 2023, www.eureporter.co/defence/cybercrime-2/2023/02/07/cybersecurity-main-and-emerging-threats/.

4 Global Disruption of Three Terror Finance Cyber-Enabled Campaigns, Internal Revenue Service, August 13, 2020, content.govdelivery.com/accounts/USIRS/bulletins/29a1ec3#:~:text=WASHINGTON%20%E2%80%93%20The%20Justice%20Department%20today%20announced%20the,Islamic%20State%20of%20Iraq%20and%20the%20Levant%20%28ISIS%29.

5 Anti-Money Laundering and Countering the Financing of Terrorism National Priorities, Financial Crimes Enforcement Network, June 30, 2021, www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%2021).pdf

6 Directives, Official Journal of the European Union, European Union, November 12, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN.

える必要があります：我々は誰と関わっているのか、そして彼らの行動が合法的であることをどのように確認するのか。したがって、直感的には、サイバー犯罪と金融犯罪のリスクマネジメントの連携を強化することが、両者のリスクマネジメントの改善につながると思われます。

サイバー犯罪と金融犯罪を検知するには、金融機関は同じ問いに答える必要があります。

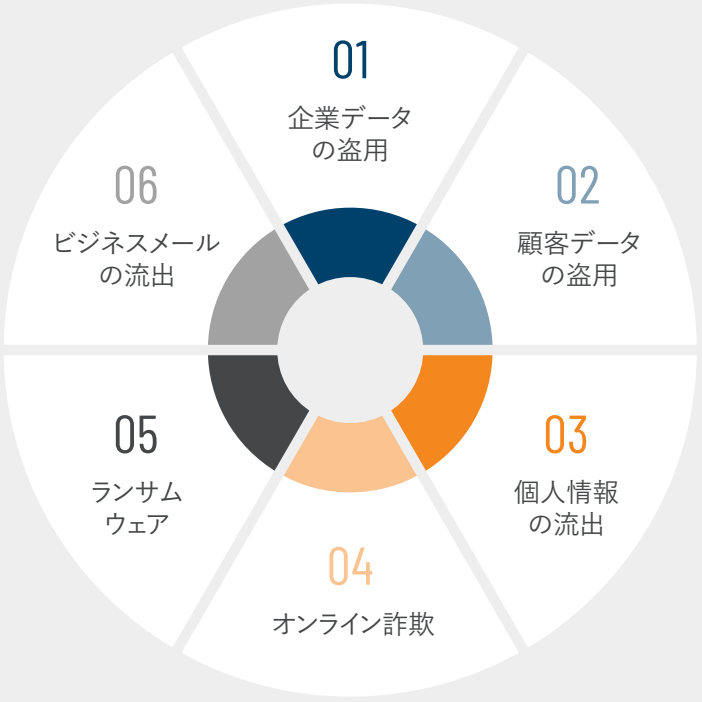
高まるサイバー犯罪の潮流

サイバー犯罪とは、簡単に言えば、コンピュータやインターネットを利用して行われる犯罪行為のことです。サイバー犯罪がいつ始まったかについては議論がありますが、電子メールが一般的に使われるようになった1980年代後半に見られ始めたというのが、多くの専門家の見解です[7]。今でも存在している一匹狼のハッカーが初期のサイバー犯罪の実行犯でしたが、今日のサイバー犯罪には、政府から犯罪集団まで、組織立った実行犯も含まれています。

COVID-19の流行期には、より多くの従業員がリモートで働き、従来は一元管理されていたデータがより自由に、より頻繁に共有され、従業員はそれまで経験のない新しいツールやテクノロジーに接するようになりました。この状況は、ハイブリットワークの環境下でもある程度続いています。このような中、2022年の全世界におけるサイバー犯罪対策のコストは8.4兆ドルと推定されています。2026年までには、全世界のサイバー犯罪対策の年間コストは20兆ドルを超え、約150%増加する可能性があります[8]。

経済的利益を得るために行われるサイバー犯罪は、データへのアクセスや不正利用を伴います。金融機関にとっては、自社のデータや顧客のデータがリスクにさらされることになります。サイバー犯罪の手口は多岐にわたり、例えば以下のようなものがあります。

サイバー犯罪の行為者が金融犯罪を行う際に使用する手法



7 "Cybercrime's Evolution Since the 80's: Historical Facts and Figures," by Andrew Douthwaite, Virtual Armour, October 26, 2022, https://virtualarmour.com/cybercrimes-evolution-since-the-80s/#:~:text=Experts%20agree%20that%20%E2%80%9Ccybercrime%E2%80%9D%20as,today%20originated%20in%20the%201980s.&text=Cybercrime%20has%20increased%20300%25%20since,roughly%201.5%20million%20in%202010.

8 Estimated Cost of Cybercrime Worldwide From 2016 to 2027," Statista, www.statista.com/statistics/1280009/cost-cybercrime-worldwide/#:~:text=The%20global%20cost%20of%20cybercrime,U.S.%20dollar%20mark%20in%202023.

サイバー犯罪による金融機関のデータ流出件数は、2018年1月から2022年6月までに米国だけで1億5,330万件にのぼっています[9]。では、サイバー犯罪の実行犯は、これらのサイバー犯罪からどのように金銭的利益を得るのでしょうか。直接的な利益につながる場合（例えば、ランサムウェア）もあれば、間接的に利益につながる場合（例えば、盗んだデータの違法なマーケットでの販売、融資や他の金融機関の口座へのアクセスのための使用）もあります。サイバー犯罪の実行犯にとって個人データは非常に貴重な情報であるため、サイバーセキュリティに対する攻撃の11%はデータを盗むことを直接の目的としていると推定されています[10]。

サイバー犯罪の実行犯は、金融システムも直接の標的にしています。2016年のバングラデシュ中央銀行における強盗事件は、北朝鮮を拠点とするラザルスグループ（Lazarus Group）が実行したのではないかとも考えられており、SWIFT（Society for Worldwide Interbank Financial Telecommunication）システムを通じてバングラデシュ中央銀行から8,100万ドルが盗み出されました。この事例では、ハッカーがマルウェアにより盗んだ銀行の認証情報を使用して口座管理先であるニューヨーク連邦準備銀行からフィリピンの銀行に開設した口座に送金され、すぐに引き出されました。

ハッカーによるSWIFTへの送金指示の総額が10億ドル近くだったため、実際には更に被害が拡大する可能性がありましたが、スペルミスを起因として不正な大量送金を疑ったニューヨーク連邦準備銀行が30件の取引を中止しました。

スペルミスは、組織内のセキュリティ研修において習うように、不正取引の兆候を示す一般的な情報です。

しかし、8,100万ドルというバングラデシュ中央銀行における強盗事件は、金融機関史上最も大きな強盗事件の被害額にはおよびません。日本の暗号資産交換所であるCoincheckにおける2018年のハッキングでは、北朝鮮系と思われる実行犯が5億3,400万ドルの経済的利益を得ています。実際、近年のハッキングのトップ5のうち4件が暗号資産交換業者をターゲットにした事案であり、サイバー犯罪の実行犯により14億3,000万ドルが強奪されました[11]。

人工知能（AI）は、多数の金融機関が多くの金融犯罪を検知・評価する先進的な方法として捉えている一方、AIの技術自体がサイバー犯罪に対して脆弱性をはらんでいるという側面があります。2020年、顔認識ソフトウェアの新興企業であるクリアビューAIは、サイバー犯罪の実行犯によるハッキングにより、同社の顧客リストへ不正アクセス[12]があったことを明らかにしました。AIのモデリングやその使用方法を変更するためのアクセスが可能となってしまうと、AIの使用や採用、社会的信頼に深刻な影響を与える可能性があります。

連携により両リスクの管理をいかに改善するか

サイバーリスク管理チームが、サイバー犯罪のリスクが高いとされる国や、ロシアの制裁逃れを支援していると思われる国から、自社のウェブサイトにアクセスしようとする試みが増加しているとの情報を入手した場合、金融犯罪対策チームのリスク管理の向上につながるでしょうか。逆に、金融犯罪対策チームが、最近発生した一連のID窃盗事件について大規模な調査を行い、いくつかのパターンを特定した場合、サイバーリスクマネジメントチームのリスク管理の向上につながるでしょうか。これらの質問に対する答えは「イエス」です。これらの情報を共有することで、両チームはより効果的なリスク管理が可能となります。すでに情報を共有している金融機関もありますが、多くの金融機関のプロセスはまとまりなく、場当たり的な対応に留まっています。

サイバーリスクと金融犯罪リスクは、一般的に取締役会のリスク管理委員会の管轄下にありますが、これらのリスクの日常的な管理は多くの場合、切り離されています。金融犯罪は、多くの場合、最高リスク責任者または最高コンプライアンス責任者に報告を行うマネー・ローンダリング報告責任者（MLRO）が率いるコンプライアンスチームにより管理

9 Financial Data Breaches Accounted for 153.3 Million Leaked Records From January 2018 to June 2022," by Paul Bischoff, Comparitech, July 27, 2022, www.comparitech.com/blog/vpn-privacy/financial-data-breaches/.

10 "The Chance of Data Being Stolen in a Ransomware Attack Is Greater Than One in Ten," Emisoft, July 13, 2020, www.emsisoft.com/en/blog/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.

11 "Here Are the Biggest Digital Heists of the Last Decade," by Chris Stokel-Walker, Cybernews, June 29, 2022, https://cybernews.com/editorial/here-are-the-biggest-digital-heists-of-the-last-decade/.

12 "Clearview AI: Face-Collecting Company Database Hacked," BBC, February 27, 2020, www.bbc.com/news/technology-51658111.

され、サイバーセキュリティは、通常、最高技術責任者または最高情報責任者に報告を行う最高情報セキュリティ責任者（CISO）が率いる情報技術（IT）セキュリティチームにより管理されています。

このように分離された管理は、金融機関におけるリスク評価と管理方法に影響します。金融犯罪対策チームとサイバーリスクマネジメントチームは、より高度化された手段を用いるサイバー犯罪の実行犯に対抗可能と思われますが、金融犯罪とサイバーリスクマネジメントの技術的なコンプライアンス要件は異なっています。多くの場合、コンプライアンスチームと IT セキュリティチームは異なる認識を有しています。しかし、このようなサイロ化したアプローチでは、犯罪行為の防止、あるいは少なくともより効果的な検知に役立つデータを共有できていない可能性があります。

より広い視野でリスクをとらえる

金融機関は、顧客と資産をより効果的に保護するために、サイバー犯罪と金融犯罪の重なりがより大きくなっていることを考慮する必要があります。具体的な取組みとして、サイバー犯罪対策と金融犯罪対策の2つの分野の更なる連携や、MLRO および CISO 間における定期的な情報共有により、組織が直面する犯罪脅威の共通理解を醸成することが考えられます。

ロシア制裁を契機として、マネー・ローンダリング（AML）チームと制裁チームが連携するようになりましたが、そこから学ぶべき有益な教訓があります。当該2チームは、それぞれ金融犯罪のコンプライアンスに特化しているものの、従来各部門が独自に業務遂行しており、主に制裁対象に該当した案件が AML チームに共有され、また、疑わしい取引の届出の提出要否を判断する場合に連携を行っていました。この1年、各チームは、チーム間の定期的な連携の場において、各チームの情報を共有することにより、双方のチームにとってより良い共通認識が得られるという教訓を得ました。この教訓は、金融犯罪やサイバー犯罪のチームにも当てはまるでしょう。

金融機関は、リスクアペタイト方針、リスク識別、評価、モニタリング、測定基準および報告などを含む、各チームのリスクフレームワークの整合性を高めることも検討すべきかもしれません。このようなリスクに関する連携は、シニア・マネジメント層によるより広い視点での監督にも役立つでしょう。

以下は、サイバー犯罪と金融犯罪のリスクマネジメントを統合し、改善するために金融機関が取り得る6つのステップです。

1. 従業員の研修と意識向上：社内研修や意識向上プログラムへのサイバー犯罪に関するリスクの組み入れの確保。従業員が組織内の金融犯罪管理を理解することは規制上の要件であり、特に、サイバーセキュリティリスクとその管理を、より広範な金融犯罪類型の中に含めることは、より効果的な取組みとなります。シニア・マネジャーや取締役会は、全体的なリスク評価を理解し、金融犯罪リスクの枠組みについて、情報に基づいた課題を提供できるようになることが求められます。

2. リスク評価：サイバーリスクが金融機関におけるマネー・ローンダリング / テロ資金供与対策（AML/CFT）の リスクアセスメントに十分に組み込まれているかの検討。金融犯罪対策チームは、金融機関のサイバー犯罪の脅威に係る評価を理解し、当該評価を、地理、提供する商品またはサービス、顧客グループ、および支払手段に関連す

金融機関への質問：

- 金融犯罪やサイバー犯罪に関連するリスクや情報は、組織内でどのように共有されていますか。
- サイバー犯罪者に最も利用されやすい商品やサービス、場所について把握していますか。
- マーケットでサイバー事案が発生した場合、全ての脆弱性がサイバー犯罪と金融犯罪の両方の観点から評価されていますか。
- サイバー犯罪の脆弱性を理解することで、金融犯罪の予防・検知の管理をどう向上させることができますか。

るリスクに係る情報の提供に役立てるために活用すべきです。このような理解は、調査を行う金融犯罪対策チームや疑わしい取引の届出に関する高度化に役立ちます。

3. 顧客受入：口座開設時のデューデリジェンスへのサイバー犯罪のレッドフラッグの組入れ。新規顧客の口座開設と定期的な顧客情報の更新を担当する従業員は、サイバー犯罪の実行犯が窃取したデータを使用し、金融機関に口座を開設する方法に関する知見を有する必要があります。米国の金融犯罪取締ネットワーク（FinCEN）は、他の国家機関とともに、窃取された文書の使用に関連する多くのレッドフラッグ[13]を特定しており、以下を含んでいます。

- 顧客から提出された氏名のスペルが、政府機関発行の身分証明書のスペルと一致しない。
- 身分証明書の写真が不鮮明または低解像度である、または細工されたような形跡がある。
- 顧客の身体的特徴と身分証明書に記載されている情報が一致しない。
- 顧客が補足書類の提出を拒む、または躊躇している。

個人情報窃取の疑いがある場合、特に金融機関の現在または過去の顧客が関与している場合は、サイバーリスクマネジメントチームと共有する必要があります。これらの事例は、金融機関がハッキングされた可能性が高いことを示しています。

4. モニタリングと検知：サイバー犯罪の実行犯が金融犯罪を行う際に使用する類型の、金融犯罪対策チームおよびサイバーリスクマネジメントチーム間での情報共有枠組みの確立。金融犯罪とサイバー犯罪の予防と検知は、活動の背後にいる人物とその真の目的を隠すような事象に対するモニタリングと探知に依拠しています。金融犯罪対策としての取引モニタリングや監視ソフトウェアの使用は、金融犯罪とサイバー犯罪の予防および検出方法として、十分に確立されています。サイバー犯罪に関連する可能性のある特定の取引タイプや顧客プロファイルに関するリスク情報は、サイバー犯罪を示す可能性のある疑わしい活動を検知するシステムの能力向上に寄与します。

サイバー犯罪収益のローンダリングは、複数のよく知られた方法により行われるため、金融機関はこの活動を検知するための監視・モニタリングシステムの調整を確実に行う必要があります。最も一般的な方法として、少額資金の検知を回避するためのマネーミュールを介する方法、犯罪者の身元を隠すためのフロント企業を介する方法、特定の高リスク国における現金ビジネスまたは金融担当者を介する方法などが挙げられます[14]。暗号通貨もハッキングやランサムウェア攻撃の収益のローンダリングに多く使用されており、金融機関はこのような先について更に精査を行うべきです。

また、サイバー犯罪のレッドフラグとして指摘されている、リスクの高い国の関係者とのオンライン取引や、プリペイドカードによる支払いの多さについても、優先的に精査する必要があります。顧客基盤の広い範囲に影響を及ぼす可能性のある既知のサイバーインシデントが発生した場合は、モニタリング手続きを強化する必要があります。これは、口座情報の変更を確認するための厳格な手続きから、リスクのある顧客層を検知するための敷居値や取引額の引き下げまで、さまざまな対応の可能性があります。

5. インシデント対応の組合せ：セキュリティ侵害に関連する情報の可能な限りの素早い金融犯罪チームとの共有の必要性。金融機関やその顧客に対する金融犯罪における、サイバー攻撃で窃取されたデータの悪用方法に関する評価を含む複合的なインシデント対応は、更なる犯罪を防止または特定する金融機関の能力を高める可能性があります。インシデントが発生した場合に、対応策を文書化している金融機関はより効果的な対応が可能となり、また、金融犯罪の他面的な影響を考慮することは、脆弱性のある全ての領域を特定する助けとなります。

6. 顧客とのコミュニケーションおよび教育：金融犯罪対策チームとサイバーリスクマネジメントチームにおける顧客向けの研修および認識共有の最適化のための連携。金融犯罪やサイバー犯罪において、サイバー攻撃の脅威が時と共に変化したり、犯罪者がサイバー犯罪や詐欺を行うために新しい方法をとるため、顧客とのコミュニケー

13 Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic, FinCEN Advisory, July 30, 2020, www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf.

14 Follow the Money: Understanding the Money Laundering Techniques That Support Large-Scale Cyber-Heists, BAE Systems and The Society for Worldwide Interbank Financial Telecommunication, 2020, www.swift.com/sites/default/files/files/swift_bae_report_Follow-The%20Money.pdf.

ションや認識共有が特に重要です。多くの顧客は、金融犯罪やサイバー犯罪で悪用されるさまざまな方法の認識を深めていますが、企業の顧客向けの教育活動においては、脆弱な顧客など特定の顧客グループのニーズを特に取り上げる必要があります。

結論

テクノロジーの進化は、私たちの働き方や生活に大きな可能性をもたらしますが、同時に、ますます巧妙で広範囲に及んだサイバー犯罪のリスクも伴います。金融犯罪は従来、サイバー犯罪と別々に管理されてきましたが、金融機関がより総合的なアプローチをとることで、その予防と検知を向上させることが可能です。サイバーセキュリティと金融犯罪のコンプライアンスには、情報共有、分析、サイバー犯罪の実行犯に関するリスク評価、厳格なモニタリングおよび検知の強化の余地があります。テクノロジーがさらに発展し、テクノロジーを金融犯罪に悪用する犯罪者が増加するにつれ、サイバーセキュリティと金融犯罪に係るコンプライアンス強化は、あらゆるレベルにおける積極的かつ広範囲の対応が必要な問題になると考えられます。

著者について

Carol Beaumier は、プロティビティのリスク・コンプライアンス部門のシニア・マネージング・ディレクターで、同社の APAC 金融サービス部門のリーダーを務める。メトロ D.C. を拠点に、複数の業界にわたる幅広い規制問題に携わってきた経験を持つ。プロティビティに入社する以前は、アーサー・アンダーセンのレギュラトリー・リスク・サービスのパートナー、セキュラ・グループのマネージング・ディレクター兼創業パートナーとして、リスクマネジメントの実務を統括。コンサルティングの前は、米国通貨監督庁（OCC）に 11 年間勤務し、審査官として多国籍銀行や国際銀行に重点を置いていた。また、会計監査人のエグゼクティブアシスタント、OCC のシニアマネジメントチームのメンバー、会計監査人の庁内外での連絡役も務めた。ボーミエは、規制やその他のリスク問題に関して頻繁に執筆や講演を行っている。

Bernadine Reese は、プロティビティのリスク・コンプライアンス・プラクティスのマネージング・ディレクターである。現在、ロンドンを拠点に、金融サービス業界のクライアントとリスクおよび規制に関するアドバイザリー業務に携わってきた経験を持っている。マネー・ローンダリング対策や制裁コンプライアンスを含む金融犯罪法に関する対応において、さまざまな金融機関と協働している。

プロティビティの金融犯罪とサイバーセキュリティのプラクティスについて

プロティビティの金融犯罪プラクティスは、金融機関が規制上の義務を果たし、AML/CFT および制裁リスク評価、統制強化、効果的なオペレーショナルリスクとコンプライアンスのフレームワークを提供する変更能力を組み合わせて、金融犯罪のエクスポージャーを減らすための支援を専門としています。当社の専門チームは、金融犯罪、詐欺、汚職、職業上の不正行為、その他の金融ビジネスリスク問題に対する企業の脆弱性について積極的に助言し、企業のブランドと評判を保護することを支援します。

当社の金融犯罪対策のスペシャリストは、当社のサイバーセキュリティ・プラクティスと連携し、進化するプライバシーリスクを金融機関が理解、管理し、サイバーセキュリティガバナンスを調整し、利害関係者と効果的にコミュニケーションできるよう支援します。当社のサイバーチームは、機密データを保護するための脆弱性を特定し、実行可能な改善提案を行うことにより、ビジネス価値の維持に貢献します。

protiviti®