protiviti®
Global Business Consulting



COMPLIANCE INSIGHTS

新たなバリューチェーン：デジタル資産が金融犯罪、コンプライアンス、そして金融の透明性をどう変えつつあるか

Carol Beaumier、Bernadine Reese著

金融機関は新しいバリューチェーンのリスクに対応する準備ができているか

金融犯罪は新たな時代に突入しました。問題は犯罪者がどのように資金を移動させるかではなく、どのように価値を移転させるかです。価値の移転経路は、銀行口座、ウォレット、ブロックチェーン、トークン化金融商品、デジタルプラットフォームから成るネットワークを通じて急速に拡大しています。

デジタル資産の理解

デジタル資産という用語は、たびたび暗号資産と同義で使われますが、これは今日の金融市場の現実をいっそうに反映しなくなっています。デジタル資産は、価値をデジタル上で表現したものと捉えるのが適切です。その価値は、通貨、証券、コモディティ、預金、所有持分、契約上の権利、サービスへのアクセス権など、さまざまな形を取り得ます。

暗号資産は、従来の金融システムに急速に統合されつつある、はるかに広範なエコシステムの一部に過ぎません。銀行は、従来の預金通貨をブロックチェーン基盤上で移転可能にするトークン化預金の実証を進めています。また、資産運用会社は、トークン化ファンドの検討を進めています。

資本市場の参加者は、トークン化された債券や証券の発行および取引の実証を進めています。世界各国の中央銀行は、中央銀行デジタル通貨の役割について引き続き検討を行っています。さらに、ステーブルコインは国境を越えた価値移転や、異なる金融エコシステム間で価値を移転するための手段として、その重要性をますます高めています。

現在の銀行業界において、デジタル資産とは、価値をデジタル上で表現したものと捉えるのが最も適切です。ここでいう価値とは、貨幣のみならず、投資商品、請求権、資産の所有権、さらにはサービスを利用する権利なども含まれます。

「デジタル資産の進化」、J.P. Morgan

これらの展開を結びつけているのは、表現されている資産の種類ではなく、所有権の記録や価値の移転に使用される基盤となるインフラストラクチャです。分散型台帳技術により、ほぼリアルタイムで更新可能な共有デジタル記録を通じて、資産の発行、移転、決済を行うことができます。多くの場合、取引は従来の銀行営業時間、決済時間帯、地理的境界に制約されず、24時間365日行うことができます。

金融機関にとって、これは考え方の転換を必要とします。従来、コンプライアンスプログラムは、さまざまな金融商品、決済チャネル、および顧客関係の監視に重点を置いてきました。金融機関は、複数のエコシステムやインフラをまたいで価値がどのように移転するかを理解することに、より一層重点を置かなければなりません。決済、証券、預金、デジタル資産という区分よりも、価値が創出・移転・管理される仕組みの方が重要になりつつあります。

この変化は特に重要です。なぜなら、デジタル資産エコシステムは従来の金融システムと切り離された存在ではなくなるからです。銀行、決済事業者、証券会社、カストディアン、取引所、テクノロジー事業者、投資家の相互の結び付きはますます強まっています。こうした境界がさらに曖昧になる中で、デジタル資産を単なるニッチまたは専門的な資産クラスと見なす金融機関は、より広範な戦略面、業務運営面、金融犯罪対策上の影響を見落とすリスクがあります。

最終的に、デジタル資産は完全に新しい金融活動のカテゴリーとして捉えるべきではなく、価値そのもののデジタル化が進展していく過程における次の段階として理解する方が適切です。

なぜ犯罪者はデジタル資産を利用するのか

この質問に対する一般的な回答は、デジタル資産が匿名性を提供するというものです。しかし、それは誤解です。匿名性とは、個人の身元や財務情報が秘密にされることを意味します。ほとんどのデジタル資産の活動が行われているパブリック・ブロックチェーンは、匿名性ではなく仮名性(pseudonymity)を提供します。その理由は次のとおりです。

- 取引は公開台帳に記録されている
- すべての取引はウォレットアドレスに紐付けられており、それが仮名またはデジタル識別子として機能する
- 誰でもウォレットアドレスに関連付けられたすべての取引履歴を見ることができる
- 取引履歴は永久に記録されており、現金よりも追跡しやすい場合が多い

匿名性：追跡可能性がほとんど、または全くない	仮名性：分析可能な追跡記録
個人の真の身元は不明であり、合理的な手段によって特定することができない	個人の真の身元は識別子によって隠されているものの、本人を特定することができる
永続的識別子が存在しない	永続的識別子が存在する(例えば、ブロックチェーンウォレットアドレス)
一連の活動を実在する人物に容易に結び付けることができない	取引等の活動は、仮名識別子を介して相互に関連付けられることが多く、調査によって実在する人物に結び付けられる

実際のところ、金融犯罪をめぐる大きな皮肉は、デジタル資産の方が現金よりも追跡しやすいということかもしれません。

利用可能な情報の仮名性を解除し、当事者の実際の身元を特定するためには、追加の作業が必要です（このページの「仮名性解除の方法」を参照）。ただし、重要なのは、身元を特定できるかどうかではなく、金融機関が特定に必要な能力を整備しているかどうかです。犯罪者は、金融機関にその能力がないこと、または少なくとも仮名性の解除に時間を要することで、自らに有利な状況が生まれることを期待しています。

犯罪者にとって主な魅力が匿名性でない場合、犯罪者が重視するデジタル資産の利点とは何でしょうか。

利点はいくつかあり、概して、正当な利用者にも魅力となる利点と同じです。具体的には、次のものが含まれます。

- ほぼ即時決済のスピード
- クロスボーダー機能
- 24時間365日の市場アクセス
- 従来の銀行を介する必要がない個人間（P2P）取引

仮名性解除の方法

- KYC記録の交換
- 同一の主体によって管理されているウォレットをグループ化するための、ブロックチェーン分析およびアドレス・クラスタリング
- 取引パターンの特定を通じた行動分析
- オープンソース・インテリジェンス（OSINT）
- トラベルルール情報
- デバイス、IPアドレスおよびメタデータの分析

犯罪者の手口には、複数のウォレットの使用、複数のアドレス間での資金移動、複数のブロックチェーンネットワークの活用、ミキサーやタンブラーの利用、統制が脆弱、または規制・法執行が不十分な法域を経由させることなどが含まれます。要するに、犯罪者の目的は、追跡や特定作業を時間とコストのかかるものにすることです。

しかし、金融機関は複雑さや匿名化・秘匿化の手法を言い訳に、対応を怠ることはできません。実効性のある統制、分析・調査能力は、現代の金融犯罪リスク管理に不可欠であり、デジタル資産取引の背後にいる主体を特定する能力は、中核的な要件といえます。現在デジタル資産商品を提供していない金融機関でも、顧客、取引相手、決済フローを通じてデジタル資産リスクへのエクスポージャーが高まっており、どの金融機関であってもデジタル資産取引の背後にいる主体を特定する能力は無視することができない重要な能力となっています。

デジタル資産はマネー・ローンダリングを変えた

犯罪者は常に、不正資金を移動するための最速で、最も安価で、最も発見されにくい方法を追求してきました。実際のところ、金融機関は長年にわたり共通の課題に直面してきました。それは、犯罪者が新しい技術を違法目的で悪用する方法を、最初に見出してしまうということです。デジタル資産のエコシステムでは、数年単位ではなく数週間単位でイノベーションが生まれることもあり、金融サービス業界には、こうした技術革新のスピードに遅れることなく対応していくという、これまで以上に大きな責任が課されています。

以下は、現在みられるデジタル資産を利用したマネー・ローンダリングの類型の一部です。

- **クロスチェーン・ローンダリング** — クロスチェーン・ローンダリングでは、犯罪者はブリッジ、スワップ、資産変換を利用して断片化された取引経路を構築し、金融機関が資金の出所から最終目的地まで追跡することをより困難にします。追跡が不可能というわけではありませんが、ブロックチェーンが追加されるごとに複雑さが増し、調査の労力も増大します。

- **ステーブルコインによる資金洗浄** — ステーブルコイン・ローンダリングは、ステーブルコインの迅速性、流動性、普及の拡大を悪用し、不正な資金・価値を世界規模で移転する手法です。犯罪者は、価格変動リスクを抑えるために、価格変動の大きい暗号資産をステーブルコインへと換えた上で、その後も取引所、ウォレット、さらには複数の法域をまたいで資金を移転します。ステーブルコインはデジタル資産エコシステムに広く組み込まれていることが多いため、大量の資金を迅速に移転する手段となり得ます。

- **レイヤード・ウォレット・ネットワーク** — レイヤード・ウォレット・ネットワークは、資金を多数のウォレットと取引に分散させ、送金人と最終受益者の関係を隠します。従来型のマネー・ローンダリングにおけるレイヤリングと同様、ウォレットや送金を重ねるごとに、取引分析をより困難にし、所有関係を不明瞭にすることを目的としています。高度なネットワークでは、数百から数千もの相互接続されたアドレスが関与する場合もあります。

Lazarus グループによる Harmony Horizon Bridge 社のハッキング事件

2022年6月、北朝鮮の主要情報機関である偵察総局（RGB）と関係がある国家支援型のサイバー脅威組織、北朝鮮のLazarus グループと関係のあるハッカーが、Harmony Horizon Bridge社から1億米ドルを盗みました。Harmony Horizon Bridge社は、カリフォルニアを拠点とするブロックチェーンおよび暗号資産関連企業でクロスチェーン型の暗号資産ツールとして機能し、Harmonyネットワーク、Ethereum、Binance間でデジタルマネーを移動できる仕組みを提供していました。

捜査当局は、盗まれた資金が多数の中継ウォレット（階層化されたウォレット・ネットワーク）を経由して移転され、分散型取引所（DEX）を通じて送金され、クロスチェーン・ブリッジを利用して複数のブロックチェーン間で移転され（クロスチェーン・ローンダリング）、取引の追跡経路を隠すためにプライバシー強化サービス（PES）を経由していたと報告しました。ハッカーによるこうした努力にもかかわらず、ブロックチェーン分析および国際的な法執行機関の協力により、捜査当局は資金の相当部分を追跡し、その活動をLazarus グループによるものと特定することができました。

1億米ドルのうち、回収されたのはごく一部にとどまりました。Harmony Horizon Bridge社は、ハッキング事件を受けて業務を停止しました。

- **分散型取引所（DEXs）** — 分散型取引所は、ユーザーが従来の仲介者に依存することなく、スマートコントラクトを通じてデジタル資産を直接交換できるようにします。ユーザーの本人確認（KYC）は不要であり、異なるブロックチェーンネットワーク間で即時取引が可能なため、違法資金と犯罪者の関係を隠すことができます。

- **セルフホステッド・ウォレット** — セルフホステッド・ウォレットは、金融機関や取引所ではなくユーザー自身が直接管理するデジタルウォレットです。正当な用途も多い一方、規制対象機関からはデジタル資産の所有者や移転状況が見えにくくなる場合があります。犯罪者は、資産を従来型のコンプライアンス態勢や取引モニタリングの直接的な監視範囲から外すため、セルフホステッド・ウォレットに資金を移すことがよくあります。

- **プライバシー強化サービス（PES）** — 暗号資産ミキサー、コインジョインサービス、プライバシープロトコルなどの技術は、デジタル資産取引の追跡や関与する個人の特定をより困難にします。これらのサービスは、取引の流れを不明瞭にし、送金人と受取人の間の可視的なリンクを断ち切るなど、通常はパブリック・ブロックチェーン上で見えるウォレット間の関係を隠したりすることがあります。

デジタル資産のマネー・ローンダリングは、単一の隠蔽手法に依存することはほとんどありません。犯罪者は複数の類型を組み合わせる傾向を強めており、従来型の金融犯罪対策を先回りすることを意図して、ウォレット、取引所、ブロックチェーン、仲介者から成る複雑なネットワークを構築しています。

金融機関にとっては、デジタル資産を回避することが答えではありません。それはそもそも不可能かもしれません。むしろ、金融機関はデジタル資産を理解する能力を高める必要があります。理想的には、これらを悪用しようとする犯罪者と同等以上に理解できるようになるべきです。

デジタル資産詐欺の増加

デジタル資産における金融犯罪リスクの議論では、これまでマネー・ローンダリングが主に取り上げられてきましたが、近年では詐欺が消費者および金融機関の双方にとって最も重大な脅威として浮上しています。グローバルな到達範囲、迅速な決済、比較的容易なアクセス、そして多くの場合取り消し不可能な取引という要素が組み合わさることで、詐欺師が大規模に被害者を狙う魅力的な環境が生まれています。多くの場合、デジタル資産自体が詐欺の根本原因なのではなく、犯罪収益を受領・移転・分散するために選好される手段となっています。より重大なデジタル資産詐欺の脅威には、次のようなものがあります。

- **「ピッグ・ブッチャリング（pig-butchering）」詐欺**は、ソーシャル・エンジニアリング、関係構築、偽の投資機会を組み合わせ、被害者を欺いて詐欺プラットフォームに送金させる手口です。デジタル資産により、犯罪者は犯罪収益を複数の法域にまたがって迅速に移転・重層化できるため、回収が困難になります。

- **投資詐欺**は、偽のトークン発行、詐欺的な取引プラットフォーム、なりすまし詐欺、誤解を招く宣伝を通じ、デジタル資産市場で進化してきました。こうした手口では、正当な事業に見せかけるため、一見すると専門的に作り込まれたウェブサイト、ソーシャルメディア上のキャンペーン、AI生成コンテンツ、高度な顧客サポートが利用されています。

- **ビジネスメール詐欺（BEC）やサイバー技術を悪用した詐欺**では、現在、乗っ取られたメールアカウント、ディープフェイク、ソーシャル・エンジニアリングを使って、支払先をデジタル資産ウォレットへ変更させる手口が頻繁にみられます。デジタル資産取引の迅速性とグローバルな到達範囲は、回収活動を著しく困難にします。

デジタル資産詐欺の際立った特徴は、被害者が一度実行された取引を実質的に取り消す手段を持たないことが多い点です。従来の決済手段とは異なり、紛争解決やチャージバック権、金融機関による介入が提供される場合もありますが、多くのデジタル資産移転は、事実上取り消すことができません。ブロックチェーンの透明性は、調査担当者が資金を追跡するために役立つ場合がありますが、回収を保証するものではありません。

金融機関にとって、この変化は重要な意味を持ちます。詐欺防止を、従来型の決済統制だけで捉えることはもはやできません。金融機関は、デジタル資産へのエクスポージャー、顧客と暗号資産プラットフォームとの関わり、ウォレット関連活動、新たな詐欺類型を把握する必要性が高まっています。実効的な詐欺リスク管理には、従来型の詐欺対策チーム、サイバー専門家、制裁対応の専門家、AML調査担当者の連携が必要です。

制裁回避および国家安全保障リスク

世界各地で高まる地政学的な緊張を背景に、政策当局はデジタル資産を金融犯罪対策上の問題としてだけでなく、国家安全保障上の問題としても捉えています。価値を世界規模で迅速に、かつ従来の銀行チャネルを介さずに移転できる点は、従来型金融ネットワークの代替手段を求める国家主体、サイバー犯罪組織、テロ組織、制裁回避を図る者たちの注目を集めています。

最も重大な懸念の一つは、北朝鮮を含む国家支援主体による活動であり、その代表例がLazarus グループによるHarmony Horizon Bridge社の事件です（4ページの「Lazarus グループによる Harmony Horizon Bridge 社のハッキング事件」を参照）。政策当局が懸念しているのは、窃盗そのものだけではなく、その収益が非友好国の戦略的目標や活動を支援するために利用される可能性があるということです。

もう一つの懸念は、制裁対象の個人・団体・法域が関与する取引を促進しかねない取引所やサービス提供者です（Garantex事件がその代表例）。これらのプラットフォームは、不正な金融活動の経路となり得ます。従来型の金融機関が制裁対象者の関与する取引を促進することを禁じられているのと同様、デジタル資産サービス提供者にも、実効性のある制裁コンプライアンスプログラムの維持が求められます。これを怠れば、制裁対象主体が経済制裁をかいくぐって世界の金融市場にアクセスする経路となる可能性があります。

ランサムウェアのエコシステムの拡大も注目を集めています。ランサムウェア攻撃者は、暗号資産が国境を越えて迅速に移転でき、複数のウォレット、取引所、ブロックチェーンネットワークを通じて重層化できるため、暗号資産での支払いを頻繁に要求します。その結果、調査は複雑になり、盗まれた資金を回収できる可能性が低下します。

政策当局は、デジタル資産がテロ資金調達や拡散資金調達に利用される可能性についても引き続き監視しています。これらの活動は、全体のデジタル資産活動のごく一部を占めると報告されていますが、従来の金融チャネルの外で価値を調達、移転、保管できる能力は依然として懸念を生じさせています。このため、規制当局や国際的な基準設定主体は、テロリストがデジタル資産を悪用する可能性について、警告や注意喚起を公表しています。

結論として、デジタル資産は制裁遵守を著しく複雑化させています。その結果、金融機関は従来のネーム・スクリーニングや顧客デューディリジェンスを超えて、ネットワーク分析、ブロックチェーン分析、そして制裁回避の類型に対する明確な理解を含めた制裁コンプライアンス能力を拡大する必要があります。制裁コンプライアンスプログラムを拡大しない機関は、規制当局による精査だけでなく、デジタル時代における最も重大な金融犯罪や国家安全保障上の脅威にさらされるリスクもあります。

ステーブルコイン、DeFi、NFT、およびゲームエコシステムの新たなリスク

デジタル資産における金融犯罪リスクの進化は、暗号資産だけによって推進されているわけではありません。価値を新たな方法で創出・移転・交換できる新興エコシステムへと、ますます注目が移っています。

規制当局が大きな注目を寄せている分野の一つがステーブルコインです。多くの暗号資産とは異なり、ステーブルコインは法定通貨やその他の資産を参照することで比較的安定した価値を維持するよう設計されています。その価格の安定性、流動性の拡大、デジタル資産および従来の金融市場との統合の進展により、ステーブルコインは正当な商取引にとって魅力的な存在となっています — しかし同時に、価値を国際的に効率的に移動させる手段を求める犯罪者にとっても魅力的な存在となっています。

分散型金融(DeFi)は、さらなる複雑性をもたらします。スマートコントラクトを通じて、ユーザーは従来の仲介者に依存することなく、資産の借入、貸付、交換、または投資を行うことができます。DeFiプラットフォームは革新性と効率性をもたらす一方、ガバナンス、説明責任、顧客の本人確認、制裁スクリーニング、取引モニタリング、規制執行に関する課題も生じさせ得ます。DeFiサービスが規制対象機関の従来の機能を担うようになるにつれ、監督当局は、既存の規制上の期待を分散型環境にどう適用すべきか、引き続き検討しています。

非代替性トークン(NFT)には、これとは異なる論点があります。近年の投機的なNFTブームへの関心は薄れたものの、評価、所有権、市場操作、ウォッシュトレーディング、NFTが当事者間の価値移転手段として利用される可能性をめぐる問題は残っています。

ゲームおよびバーチャルエコシステムも、関心が高まっている分野の一つです。高度化するオンライン環境には、デジタル通貨、暗号資産、マーケットプレイス、そして従来の金融システムに関連付けられてきた特徴を持つ個人間取引メカニズムが含まれています。これらのエコシステムでは、統制の進化が基盤技術に追いついていない場合、価値移転、詐欺その他の金融犯罪が行われる余地が生じる可能性があります。

これらの展開に共通する点は、デジタル資産エコシステムが従来金融サービスと関連付けられてきた枠組みを超えて徐々に拡大していることです。価値がますますプログラム可能となり、移転可能で、デジタル環境全体に組み込まれていく中で、金融機関は金融犯罪リスクがどこで発生し得るか、そして一見無関係に見えるエコシステム間をどのように移動し得るかについての理解を広げる必要があります。

銀行および金融機関への影響

多くの金融機関にとって、デジタル資産が自社のリスクプロファイルに影響を与えるかどうかではなく、その影響がどれほど早く現れるかが問題となっています。暗号資産関連の商品・サービスを直接提供していない金融機関でも、顧客、決済フロー、取引相手、投資、コルレス関係、調査、制裁レビュー、不正事案、第三者サービス提供者を通じて、デジタル資産へのエクスポージャーを抱えるケースが増えています。従来型金融とデジタル資産市場の統合が進むなか、金融機関はもはや、デジタル資産が自社の統制環境の対象外とみなすことはできません。

そのため、**金融犯罪対策の枠組みは、従来の商品別・チャネル別アプローチを超えて進化しなければなりません。**リスク評価では、顧客属性、商品、法域、販売・流通チャネル、事業活動を横断して、デジタル資産へのエクスポージャーをこれまで以上に考慮する必要があります。取引モニタリング・プログラムでは、従来型のモニタリング・ソリューションに加え、ブロックチェーン分析やウォレット・インテリジェンスの統合が必要となる可能性があります。

制裁スクリーニングの手法は、ウォレットアドレス、ネットワーク分析、および新たに出現する制裁回避の類型を組み込むように適応しなければなりません。

ガバナンスも同様に重要になります。取締役会と経営陣は、デジタル資産リスクが、全社的リスク管理の枠組み、金融犯罪対策プログラム、詐欺対策戦略、オペレーショナル・レジリエンス計画、サードパーティリスク管理の監督に適切に反映されていることを確保すべきです。もはや専任の暗号資産チームが存在するかどうかが問題なのではなく、デジタル資産が組織全体のリスクプロファイルにどのように影響するかを理解するための十分な組織的能力を、その機関が構築しているかどうかが問われています。

おそらく最も重要なのは、金融機関がデジタル資産をコンプライアンス義務だけの観点から捉えないことです。デジタル資産、トークン化、プログラマブル・ファイナンス、ブロックチェーン基盤のインフラは、金融システム全体で価値が移転する仕組みを変えつつあります。将来、戦略的に優位に立つ可能性が高いのは、この変革がもたらす機会とリスクの双方を理解する金融機関です。

金融機関の未来：金融犯罪を対象とする統制から、価値移転を対象とする統制へ

デジタル資産の出現は、技術的な変革として説明されますが、その長期的な影響はより広範である可能性があります。本質的には、デジタル資産は価値の表現、移転、保管、交換の方法を変えつつあります。歴史的に、金融機関は送金エコシステムの中心的な存在でした。今、価値はパブリック・ブロックチェーン、トークン化資産、デジタルウォレット、スマートコントラクト、分散型アプリケーション、そして統合された金融プラットフォームを通じて移動することができます。

同時に、既存の商品・サービスに組み込まれたデジタル資産サービスにより、従来型の金融商品を通じてブロックチェーン機能を利用できるようになり、従来型金融とデジタル金融の間に新たな接点が生まれています。一方、AIを活用したブロックチェーン分析の進歩により、不審な行動の検知、ウォレット間の関係の特定、クロスチェーン活動の追跡、従来は隠れていた金融ネットワークの解明に関する金融機関の能力が向上しています。

これらの展開を総合すると、金融犯罪コンプライアンスの将来は、取引が法定通貨かデジタル資産かを判定することよりも、価値がどのように移転するかを理解することに重点が移る可能性が示唆されます。新たな原則は、「商品ではなく、価値を追え」となるべきです。

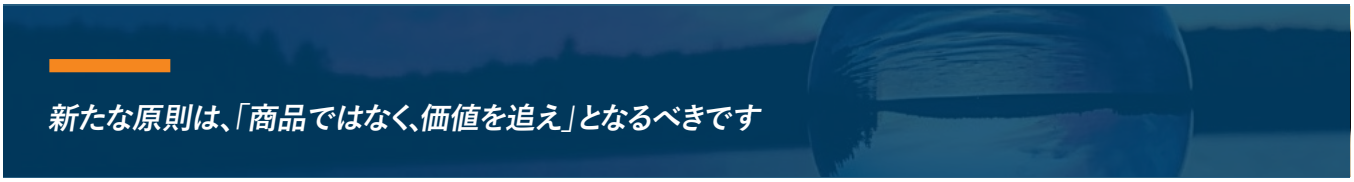
金融機関の管理態勢が引き続き商品の区分を中心に組み立てられたままであれば、顧客、取引相手、法域、決済チャネル、ウォレット、貿易書類、仲介業者をまたいで価値がどう移転するかを捉え損ね、金融機関が犯罪者に翻弄されることになりかねません。

結論

現金は依然として犯罪者にとって魅力的です。電信送金は引き続き犯罪収益の移転に利用されています。実体のない会社は、今なお実質的支配者を覆い隠します。貿易取引を利用したマネー・ローンダリングは、国境を越える価値移転を偽装する最も効果的な手法の一つであり続けています。今日、金融機関が直面する金融犯罪リスクの多くは、数十年前の捜査担当者にもなじみあるものです。デジタル資産が、こうした長年用いられてきた類型を終わらせたわけではありません。

しかし、デジタル資産は、金融犯罪が生じる領域を拡大しました。また、従来型の金融商品と並存し、次第に交差する形で、価値を移動・偽装・保管・移転する新たな手法をもたらしています。クロスチェーン転送、分散型取引所、セルフホステッド・ウォレット、プライバシー強化技術、トークン化資産、ブロックチェーンベースのエコシステムは、不正行為の特定と阻止を目指す金融機関、規制当局、法執行機関にとって新たな課題を生み出しています。

この話はリスクの増大だけにとどまりません。デジタル資産は、透明性、分析、調査上の知見について、これまでにない可能性も生み出しています。不透明な構造や断片的な記録に依存する従来型の金融犯罪類型（手口）とは異なり、ブロックチェーン上の活動は、多くの場合、永続的で詳細な



情報の証跡を残します。その情報を分析するための技術、専門性、調査能力を整備した金融機関は、従来型金融システムでは特定が難しい関係やパターンを見いだせる場合が多くあります。

結局のところ、今後10年間で成功する金融機関は、デジタル資産を単独の市場や商品としてではなく、価値が移転する方法そのものの変革の一部として捉えることができる金融機関です。問うべきことは、デジタル資産が金融犯罪リスクに影響するかどうかではありません。問われるべきことは、金融機関が、そのリスクを理解・監視・管理するために迅速に対応できるかどうかです。

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・プラクティスに所属するシニア・マネージング・ディレクタ。Phoenixを拠点に、30年以上にわたり、さまざまな業界の幅広い規制問題に携わってきました。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規制リスクサービス部門のパートナーを務め、The Secura Groupのマネージングディレクタ兼創設パートナーとしてリスク管理サービス部門を率いていました。コンサルタント業務に就く以前は、米国通貨監督庁（Office of the Comptroller of the Currency：OCC）において、主に多国籍および国際的に活動する銀行の検査官として、そのほかにもOCC長官の上級秘書官、OCC経営チームメンバーやOCC長官の庁内外渉外責任者として、11年間勤務しました。Beaumier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ます。

Bernadine Reese は、プロティビティのリスク・コンプライアンス部門のマネージングディレクタ。ロンドンを拠点とするReeseは、KPMGの規制サービス部門から2007年にプロティビティに入社。30年以上にわたり、さまざまな金融機関のクライアントと共に、リスク、コンプライアンス、ガバナンスの変革を成功裏に実行し、これらの業務を最適化することでビジネスパフォーマンスを向上させてきました。認定気候リスク専門家（Certified Climate Risk Professional）でもあります。

プロティビティのコンプライアンスリスク管理プラクティスについて

規制遵守の負担を管理する、より良い方法があります。各機能が事業目標と整合し、プロセスが最適化され、手続がデータとテクノロジーによって自動化・簡易化されたとしたらどうでしょうか。規制要件は、より効率的に満たされ、統制は事後対応型ではなく予測型へと進化します。従業員は自身の役割からより高い価値を得られるようになり、企業はレピュテーションが守られているという安心感のもと、成長とイノベーションにより注力することが可能になります。

プロティビティは、コンプライアンスをアジャイルリスクマネジメント・チームに統合し、フォワードルッキングかつ予測型の統制を実現するために分析を活用するとともに、規制コンプライアンスに関する専門知見を適用しています。また、規制当局による是正措置やコンプライアンス上の課題への対応をより効率的に進めるための自動化されたワークフローツールの活用、新商品・新サービスにおける顧客ニーズおよびコンプライアンス要件の設計要件への落とし込み、さらに規制コンプライアンスの実施状況を継続的にモニタリングするための仕組みの構築を通じて、組織を支援しています。プロティビティのコンプライアンスリスク管理サービスの詳細はこちらをご覧ください。

プロティビティについて

プロティビティは、クライアントがビジネスの変革や防護、また計画された事象や予期せぬ事象に対応できるように支援するグローバルコンサルティングファームです。25か国、90を超える拠点で、プロティビティとそのメンバーファームはクライアントに、テクノロジー、AI、データ、オペレーション、ファイナンス、法務、コンプライアンス、人材・組織、マーケティング、デジタル、リスク、内部監査の分野において、高い専門性とお客様ごとに的確なソリューションを提供しており、組織の変革の加速、リスクへの対応、最も重要な価値の保護を実現します。プロティビティは、2015年以来、米国フォーチューン誌の働きがいのある会社ベスト100に継続して選出され、Fortune100の80％以上、Fortune500の約80％の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。プロティビティは、Robert Half Inc.（NYSE:RHI）の100％子会社です。

© 2026 Protiviti Inc. All rights reserved. 複写禁、転載禁

protiviti®