# マネー・ローンダリング対策：基礎編

## 第７回：暗号資産

「暗号資産」とは分散型台帳技術（DLT）を基盤にした多種多様な新しい資産の種類です。DLTを用いることによってデータを共有ネットワーク上の複数箇所で保存できるため（すなわち「分散」）、ビットコインに代表される暗号資産の所有権の追跡や移転を各参加者が行うことができます。暗号資産には従来型の資産や決済手段とは違った特有の特徴やメリット・デメリットがあります。職業会計士は、資金洗浄者やテロ資金供与者がしばしば規制された金融システムの外で価値を手に入れ、動かし、蓄え、資金の出所や目的地を隠すために暗号資産の特徴をどのように悪用しているかを十分理解しておく必要があります。

### 暗号資産を悪用する犯罪者の手口

暗号資産はマネー・ローンダリングのどの段階にも関与する可能性があります。

- 前提犯罪：違法行為による資金収集。暗号資産を対価に違法な物品又はサービスを販売する等を行います。
- 預入（プレイスメント）：違法に得た暗号資産を従来の金融システム内で不換通貨に交換します。
- 隠匿：暗号取引は通常、ブロックチェーン解析による追跡が可能ですが、規制境界外で行われた場合は取引と特定個人とのリンクがないケースもあります。また、犯罪者がミキサーやタンブラー等と呼ばれる匿名化サービスを利用し、暗号取引間のリンクを解除することもあります。
- 分別（レイヤリング）：不換通貨を暗号資産に交換する、暗号資産を両替する、暗号資産同士をコンバートする、暗号資産を不換通貨に交換する等を行います。
- 統合（インテグレーション）：汚れた不換通貨を洗浄する場合と同様、暗号通貨決済を受け付けるオンライン会社を立ち上げ、所得を合法化して汚れた暗号資産を洗浄します。

### 定義

暗号資産（VA）：移動や決済目的での使用が可能なデジタル表現された価値。デジタル不換通貨は含みません。

暗号通貨：暗号化技術によって保護された分散型暗号資産。交換手段としての使用、移動、保管、取引を電子的に行うことができます。数多ある暗号通貨の中でも知名度が高いのが「ビットコイン」と「イーサ（イーサリアム）」です。

NFT（非代替性トークン）：完全にただ一つだけの暗号資産。ビットコインは多数存在しますが、NFTは唯一無二です。代表例はデジタルアート作品、その他一部のデジタル資産又は実物資産にも用いられます。

暗号資産サービスプロバイダー（VASP）：次のサービスのいずれかを提供する事業者

- 暗号資産と不換通貨、又は種類の異なる暗号資産同士の移転や交換
- 暗号資産の保管・管理
- 暗号資産の発行に関わる金融サービスの提供

仮想通貨ウォレット：暗号資産を所有、保管、移転させるための手段

## ケーススタディ

### コロニアル・パイプライン社へのランサムウェア攻撃

暗号資産はランサムウェア型サイバー攻撃の身代金支払い手段として急速に広がっており、監査人をはじめとする職業会計士やその依頼人が目にする機会が増えています。
アメリカのコロニアル・パイプラインへのランサムウェア攻撃は、企業が日常的に被害を受けているこの種の攻撃の代表例です。2021年５月、コロニアル・パイプラインは大規模なランサムウェア型サイバー攻撃を受け、５日間の操業停止を余儀なくされました。攻撃者は身代金として440万ドルに相当する75ビットコインを要求し、コロニアル・パイプラインはこれに応じました。当局が身代金の大半の回収に成功したものの、その後の調査によって攻撃者はその前年に47の攻撃先から総額9,000万ドルを超えるビットコインを得ていたことが判明しました。
こうした違法収益は最終的に合法的な金融システムに組み込む必要があり、そこは職業会計士が気づき、報告するチャンスです。一方で、ランサムウェア攻撃は有効なサイバーセキュリティ対策の重要性を浮き彫りにしています。

## FATF基準の最近の改定（追加）

2018年の改定によって、「暗号資産」「暗号資産サービスプロバイダー」という言葉がFATF用語集に新たに加えられています。また、FATF規制枠組みに暗号資産サービスプロバイダー（VASP）が追加されました。マネー・ローンダリング及びテロ資金供与対策の観点から暗号資産又は暗号資産サービスプロバイダーについて詳しく知りたい場合は、FATFの「Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers」を参照してください。

## その他の資料

一般的ガイダンスについては、金融活動作業部会（Financial Action Task Force：FATF）が作成した「Guidance for a Risk-Based Approach for the Accountancy Profession」を参照してください。適用規制要件等、各国・地域別の情報については、ご自身の所属する職業会計士団体にお問い合わせください。

## ⚠ 重要な危険信号

従来型のマネー・ローンダリングに対する危険信号が当てはまりますが、それ以外にも次の点に注意が必要です。

- 依頼人の財産の出所の大部分が暗号資産への投資に由来し、書面による証跡がない。
- 依頼人の財産の出所がマネー・ローンダリング/テロ資金供与対策が甘い暗号資産サービスプロバイダーが取り扱う暗号資産に偏っている。
- 依頼人がマネー・ローンダリング/テロ資金供与対策が甘い高リスク国・地域の暗号資産取引所を利用している。
- 依頼人が個人識別情報（eメールアドレス、IPアドレス等）を頻繁に変える。

最近の暗号資産マネー・ローンダリングの仕組みでは次のような場所や手段が悪用されています。

- 規制されていない暗号通貨取引所（マネー・ローンダリング対策やKYC規則が実行されていない）
- ギャンブルサイト又はゲームサイト
- ミキサー又はタンブラーと呼ばれる匿名化サービス（Anonymix等）
- リスク管理が脆弱な暗号ATM
- プリペイド式暗号デビットカード

これらの商品又はサービスを利用した目立つ活動については、会計士による慎重な検討と詳細な調査が必要です。

## 撤退するタイミング

- 自分の専門分野外の専門性を必要とするであろう業務を依頼された。
- 資金の出所を詳細に示す取引記録又は投資記録がない。
- 暗号資産又はその発行者や取引所の評判に懸念がある。
- その発行者又は取引所が有効なマネー・ローンダリング/テロ資金供与対策を講じていない。
- 提供された情報の正確さや、その他依頼人に対して不安がある。

## 疑わしい取引の届出（SAR）

資産移転に関して犯罪行為又は犯罪収益の可能性が疑われる場合は、最寄りの資金情報機関に届け出ることを推奨します。一部の国では、職業会計士に対してこれが法的に義務付けられています。

IFAC International Federation of Accountants®
529 Fifth Avenue, New York 10017
www.ifac.org | +1 (212) 286-9344 | @ifac | company/ifac

ICAEW
www.icaew.com
@icaew | company/icaew