担当者解説

「暗号資産交換業等におけるサイバーセキュリティ強化に向けた取組方針」の概要

金融庁総合政策局暗号資産・ブロックチェーン・イノベーション参事官室
課長補佐　杉野隆弥
課長補佐　那須　翔

金融庁では、暗号資産交換業等におけるサイバーセキュリティ強化に取り組んでいる。具体的には、「金融審議会暗号資産制度に関するワーキング・グループ報告」（2025年12月）において、暗号資産交換業等におけるサイバーセキュリティの重要性が指摘されたことを踏まえ、2026年２月、「暗号資産交換業等におけるサイバーセキュリティ強化に向けた取組方針（案）」を公表し、同年４月、その正式版を公表した。また、「金融商品取引法及び資金決済に関する法律の一部を改正する法律案」（2026年４月10日国会提出。以下「改正法案」という）には、サイバーセキュリティに関する規定も多く含まれている。本稿では、暗号資産交換業者等に求められる実務上の対応について、特に法務・コンプライアンス関係者を念頭に置いて解説する。なお、本稿において意見にわたる部分は、いずれも筆者らの個人的見解である。

1 暗号資産制度に関するワーキング・グループにおける議論

金融審議会は、「国内外の投資家において暗号資産が投資対象と位置づけられる状況が生じていることを踏まえ、利用者保護とイノベーション促進の双方に配意しつつ、暗号資産を巡る制度のあり方について検討を行うこと」との諮問を受け、2025年７月から同年11月にかけて、「暗号資産制度に関するワーキング・グループ」（以下「暗号資産制度WG」という）を開催した。

暗号資産制度WGにおいては、情報提供の充実、適正な取引の確保・無登録業者への対応、投資運用等に係る不適切行為への対応、価格形成・取引の公正性の確保と並んで、セキュリティの確保が、暗号資産をめぐる喫緊の課題として議論された。セキュリティに知見を有する委員からは、①マウントゴックス事件やコインチェック事件では、署名鍵そのものへの攻撃が中心であったが、近年は委託先や関係者を狙うソーシャルエンジニアリング（BOX１参照）が目立つようになっていること、②暗号資産のセキュリティは、暗号アルゴリズムのみによって確保できるものではなく、暗号アルゴリズム、プロトコル、ビジネスロジック、ソフトウェア・ハードウェア実装、運

用の各要素が適切なものでなければならないこと、③暗号資産業界は、既存の標準（BOX 2 参照）を十分に理解し、活用する必要があること、その上で、暗号資産の特殊性（サプライチェーンの複雑さ、スマートコントラクト等に関する管理標準・鍵管理標準の未確立（BOX 3 参照）、情報共有の仕組みの未成熟）を踏まえた対応が必要である旨の指摘がなされた。また、別の委員からは、暗号資産は攻撃者に狙われやすく、ひとたび突破されると、顧客資産が一度に流出し、実質的に回復不能になり得る点で、従来の金融資産とは異なるリスクを抱えている旨の指摘がなされた。

このような議論を踏まえ、暗号資産制度WG報告書では、サイバーセキュリティに係るリスクマネジメントの重要性が明記され、ガイダンスの提供、モニタリングの実施、Delta Wall等の演習をはじめ、金融庁がこれまで進めてきた公助の取組みを着実に実施するとともに、JPCrypto-ISAC等を通じた情報共有を含む共助の取組みを後押しすべきことが明記された。

BOX 1　ソーシャルエンジニアリングーコールドウォレット管理を超えた対応の必要性

ソーシャルエンジニアリングとは、人間の心理的な隙などを利用した攻撃手法を指す。従来、攻撃者は、署名鍵をハッキング等により不正に入手し、不正なトランザクションに正規の署名を行うことで、暗号資産を不正に移転していたが、ソーシャルエンジニアリングを用いた攻撃では、署名鍵を不正に入手するのではなく、署名対象となるトランザクションを改竄し、正当な権限を有する署名者を騙すことで、正規の署名を行わせる、ということが行われる。署名鍵の不正取得に対しては、署名鍵をインターネットから分離すること、すなわちコールドウォレット管理が有効であるが、ソーシャルエンジニアリングに対しては、コールドウォレット管理だけでは十分とはいえず、署名対象となるトランザクションの生成・伝送に関わるシステムのセキュリティや、権限分掌を含む適切な取引承認・署名プロセス等が重要になる。

なお、2024年に発生した暗号資産の大規模流出事案では、実際にソーシャルエンジニアリングが用いられたが、米国連邦捜査局（FBI）、米国国防省サイバー犯罪センター（DC３）及び警察庁が共同して、具体的な手口を示したパブリックアトリビューションを行うとともに、警察庁、内閣サイバーセキュリティセンター及び金融庁が共同して、北朝鮮による暗号資産の手口や対応策を示した注意喚起を行っている。暗号資産交換業者等においては、このような公開情報を収集し、活用することが期待される。

BOX 2　既存のセキュリティ基準

暗号資産交換業者には、「事務ガイドライン（第三分冊：金融会社関係）16. 暗号資産交換業者関係」のほか、「金融分野におけるサイバーセキュリティに関するガイドライン」（2024年10月４日制定、2025年７月４日一部改正。以下「サイバーガイドライン」という）が適用される。

事務ガイドラインでは、主として、分別管理、流出リスクへの対応、システムリスク管理、外部委

託先管理等に関して、セキュリティに関する事項が定められている。

サイバーガイドラインは、国内外のセキュリティ基準を参照して作成されており、①サイバーセキュリティ管理態勢の構築（基本方針、規程類の策定等；規程等及び業務プロセスの整備；経営資源の確保、人材の育成；リスク管理部門による牽制；内部監査）、②サイバーセキュリティリスクの特定（情報資産管理；リスク管理プロセス；ハードウェア・ソフトウェア等の脆弱性管理；脆弱性診断及びペネトレーションテスト；演習・訓練）、③サイバー攻撃の防御（認証・アクセス管理；教育・研修；データ保護；システムのセキュリティ対策）、④サイバー攻撃の検知（監視）、⑤サイバーインシデント対応及び復旧（インシデント対応計画及びコンティンジェンシープランの策定；インシデントへの対応及び復旧）、⑥サードパーティリスク管理のそれぞれに関して、「基本的な対応事項」すなわち金融機関等が一般的に実施する必要のある事項と、「対応が望ましい事項」すなわち金融機関等の規模・特性等を考慮し、インシデント発生時に大きな影響を及ぼし得る金融機関等に期待される事項を明確化している。

このほか、金融業界の事実上の標準として、金融情報システムセンター（FISC）による「金融機関等コンピュータシステムの安全対策基準・解説書」が挙げられる。サイバーガイドラインは、サイバーリスク管理の枠組みを定めているのに対し、FISC安全対策基準は、より具体的な対策を定めており、暗号資産交換業者においても、自らの業務・システムの特性に留意しつつ、参考とすることが考えられる。

BOX 3　鍵管理に関する基準等

公開鍵暗号を用いたデジタル署名は、暗号資産以前から広く利用されてきており、当該使用方法のもとでの鍵管理については、NIST SP 800-57 Recommendation for Key Management及びこれに関連する基準が事実上の標準として機能してきた。

一方で、暗号資産の鍵管理については、①伝統的な公開鍵基盤と異なり、鍵が危殆化した時の失効管理の仕組みがないこと、②伝統的な金融情報システムと異なり、一度署名済みのトランザクションがブロードキャストされれば基本的にそれを取り消すことはできないこと、③署名鍵と資産が不可分に結びついており、長期にわたる鍵管理が必要となる場合があること、④1つのフレーズから複数の鍵ペアを生成する「階層決定性（hierarchical deterministic：HD）ウォレット」、⑤移転に複数人の署名を必要とする「マルチシグ」や、署名鍵を分割し、鍵断片を独立に管理しつつ、鍵断片を集約することなく署名を行う「マルチパーティ計算（multi-party computation：MPC）」の活用、⑥（実装次第であるが）人手による操作の多さなど、特殊な要素も多い。

この点に関して参考となり得る公開資料としては、例えば、CryptoCurrency Certification Consortium（C4）「CryptoCurrency Security Standard（CCSS）」、Cryptoassets Governance Task Force（CGTF）「暗号資産カストディアンのセキュリティ対策についての考え方 第5版」、Open Worldwide Application Security Project（OWASP）「Transaction Authorization Cheat Sheet」が挙げられる。金融庁においても、後述のブロックチェーン国際共同研究をはじめ、継続的に

調査・研究及び情報提供を行うことを予定している。

2 自助、共助、公助の組合せによる官民一体での取組み

冒頭で紹介したとおり、金融庁は暗号資産WGにおける議論を踏まえ、2026年４月に「暗号資産交換業等におけるサイバーセキュリティ強化に向けた取組方針」（以下「取組方針」という）を公表した。取組方針は、暗号資産のサイバー攻撃の標的となりやすい性質や、攻撃者は国家レベルで攻撃手法を高度化させていること等の背景を指摘した上で、自助、共助、公助の組合せによる官民一体での取組みの必要性を指摘している。以下、それぞれについて解説する。

(1) 自　助

自助の第１は、**業界への重点モニタリング**である。2026事務年度以降、すべての暗号資産交換業者にサイバーセキュリティセルフアセスメント（**BOX 4** 参照）の実施を求めることを含め、暗号資産特有のリスク（**BOX 5** 参照）や最新の攻撃動向を踏まえつつ、必要な対話を行っていくことを示している。

BOX 4　サイバーセキュリティセルフアセスメント（CSSA）

サイバーセキュリティセルフアセスメント（CSSA）は、金融庁、日本銀行及びFISCが合同で行っている中小金融機関、新形態銀行、系統中央機関等向けの取組みであり、金融庁らが開発した自己点検票に基づき、自己評価の実施を求め、結果を還元している。2023年度の結果は、「地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2023年度）」として公表されている。

BOX 5　暗号資産交換業者のシステム構成の特徴とサードパーティリスク管理・ゼロトラストの重要性

サイバーガイドラインは、金融機関等のサードパーティへの依存が増大するとともに、金融機関等のサプライチェーンが拡大・複雑化する中で、サプライチェーンに由来するインシデントにより、金融機関等が多大な影響を受ける事例が発生していることを指摘し、サードパーティリスクの適切な管理を求めている。暗号資産交換業者の多くは、基幹的な業務においても、様々なオープンソースソフトウェア（ブロックチェーン上のスマートコントラクトを含む）やクラウドサービスを使用しているため、相対的に大きなサードパーティリスクを抱えており、サードパーティに対するデューデリジェンスは特に慎重に行う必要がある。

また、クラウドサービスを多用する環境においては、ネットワーク分離とファイアウォール、侵入検知・防止システム（IDS/IPS）等による「境界防御」とともに、内部ネットワークへの侵入を前提として、個々のシステム・サービスごとに適切かつ最小権限での認証・認可を行うこと等を中心とする、「ゼロトラストアーキテクチャ」が有効とされている。この点については、例えば、NIST SP 800-207 Zero Trust Architecture及びSP 1800-35 Implementing a Zero Trust Architecture: High-Level

Documentのほか、デジタル庁「ゼロトラストアーキテクチャ適用方針」が参考になる。

自助の第2は、**事務ガイドラインの水準引上げ**である。重点モニタリング、後述のブロックチェーン国際共同研究等の結果を踏まえ、例えば、サイバーセキュリティに係る人的構成要件（必要とされる専門性、適切な人員配置、サイバーセキュリティ責任者の権限に係る基準の在り方）、外部監査の要件（システムリスク管理、署名鍵管理等を対象とする外部検証の在り方）、外部委託先に求めるべきサイバーセキュリティ要件（実務上の課題と最新の技術動向を踏まえた包括的な要件の在り方）について見直しを行うこととしている（金商法改正との関係については、BOX 6参照）。

BOX 6　「暗号資産の金商法移行」とサイバーセキュリティ

改正法案のもとでの、暗号資産交換業者（改正法案では「暗号資産取引業者」）に求められるサイバーセキュリティ管理態勢については、今後、以下のような内容が整備されていくことが考えられる。

まず、①金融商品取引業者には、登録拒否要件として、いわゆる人的構成要件が定められており、暗号資産交換業者にも、サイバーセキュリティの観点も加味した、一定の人的構成が求められることになると考えられる。また、②改正法案では、暗号資産交換業者の義務として、分別管理に加えて、善管注意義務、暗号資産等管理業務の方法、委託先・システム提供者の適切な選定・指導等の規定が新たに盛り込まれており、これらは、暗号資産交換業者のサイバーセキュリティ管理に関する規制枠組みを構成することが想定される。さらに、③暗号資産交換業者には、責任準備金の積立義務が課されるが、この枠組みは、サイバーセキュリティ管理態勢の整備を促し、顧客財産をサイバー攻撃から保護する役割を果たすと考えられる。

また、改正法案では、新たな業として、「暗号資産管理関係業務提供者」が定義されている。これは、暗号資産制度WGにおいて重要なシステム提供者ないしウォレット提供者として議論されていたものであり、届出制のもと、欠格事由、善管注意義務、業務管理体制・安全管理措置が盛り込まれている。ウォレットのセキュリティは顧客財産保護の要であるところ、それを確保する上で、この制度が重要な役割を果たすと考えられる。

⑵　共　助

共助の第1は、**自主規制機関の体制強化**である。自主規制機関は、当局に比してより実務に近い位置にあり、実務の知見を活用しやすい立場にある。業界全体のサイバーセキュリティ管理態勢の強化を図る上では、当局のガイドラインに基づくモニタリングと、このような自主規制機関の自主規制規則に基づくモニタリングが相互補完的に機能することが重要である。取組方針では、JVCEA（BOX 7参照）の体制強化、自主規制の継続的改善、監査の実効性確保を求め、これらを継続的にフォローアップすることとしている。

BOX 7　JVCEAのセキュリティに関する自主規制規則

暗号資産交換業者は、原則として日本暗号資産等取引業協会（JVCEA）に加入しているところ、同協会の「暗号資産交換業に係る利用者財産の管理等に関する規則・ガイドライン」「暗号資産交換業に係るシステムリスク管理に関する規則・ガイドライン」「暗号資産交換業に係る緊急時対応に関する規則・ガイドライン」「暗号資産交換業に係る情報の安全管理に関する規則・ガイドライン」は、セキュリティに関して、暗号資産交換業特有のリスクに応じたより具体的な定めを行っている。

共助の第2は、**情報共有機関の体制強化と参加の慫慂**である。サイバーセキュリティ管理においては、まずは自身が抱えるリスクを的確に把握した上で、当該リスクに即したコントロールを採用していくことが重要であり、そのためには、攻撃者の動向等の「脅威」と、自らのシステム等の「脆弱性」に関する情報収集・分析が不可欠である。これらは、個社で行っても効率性・有効性に限界があり、共通の脅威に直面し、かつ共通の脆弱性を抱える業界レベルで行って初めて効率的・効果的に行うことができる。既存の金融業界では、金融ISAC（**BOX 8** 参照）がこのような役割を担っているが、暗号資産業界では、JPCrypto-ISACが2025年1月に設立されている。取組方針でも言及したとおり、JPCrypto-ISACについては、暗号資産交換業者等の積極的な参加と、活動内容のさらなる発展が期待されている。

BOX 8　ISACの情報共有・分析を超えた役割

ISAC（Information Sharing and Analysis Center）は、特定の業界の企業等が、脅威、脆弱性、インシデント等に関する情報を共有し、分析するために設立する組織であり、米国クリントン政権が重要インフラ防護のためにPresidential Decision Directive 63（PDD-63）で設立を推奨したことが始まりである。我が国では、2002年に初めてTelecom-ISAC Japanが設立されたが（2016年ICT-ISAC Japanに改組）、2014年に2番目のISACとして金融ISACが設立され、10年以上にわたって活動している。ISACは、情報の共有・分析のみならず、業界のCISOを含むセキュリティ担当者間の知見（特に暗黙知）の共有やコミュニティ形成、インシデント発生時における支援、教育・研修の共同化といった機能を通じて、各業界の信頼性向上に貢献している。

(3) 公　助

公助の第1は、**ブロックチェーン国際共同研究プロジェクト**である。金融庁は、2017年度から当該プロジェクトを実施し、分散型金融システムに内在するリスクに関する知見を提供してきたところ、2025年度は、「暗号資産関連業者におけるサイバーセキュリティの課題と対策に関する研究調査」を実施し、国内外で発生した代表的なサイバー攻撃事例を取り上げ、攻撃手法やリスク、対応策に関する分析を行っている。暗号資産交換業者や情報共有機関等においては、これらの研究結果も踏まえ、サイバーセキュリティ管理態勢の強化に活用することが期待される。

公助の第2は、**金融業界横断的なサイバーセキュリティ演習**（**BOX 9** 参照）である。金融庁は、金融業界全体のインシデ

ント対応能力の向上のため、2016年度から当該演習を実施してきており、2025年度は、暗号資産交換業者向けのシナリオと評価基準を新たに設定している。取組方針では、今後も最新の攻撃動向等も考慮しながら継続的に見直しを行うとともに、３年以内にすべての暗号資産交換業者の参加を目指すとしている。

BOX 9　金融業界横断的なサイバーセキュリティ演習（Delta Wall）

Delta Wallは、金融業界横断的なサイバーセキュリティ演習であり、2025年10月実施の「Delta Wall 2025」では、177者が参加して行われた。Delta Wallは、事務局において業態ごとにセキュリティインシデントのシナリオを設定し、各金融機関等において初動対応、攻撃内容の調査・分析、顧客対応、復旧対応等の業務継続等について対応を検討し、事務局において検討結果を集約・評価・フィードバックするという手順で行われ、具体的な改善策や優良事例を示すなど、フィードバックに力点を置いている。

公助の第３は、**脅威ベースのペネトレーションテスト（TLPT）実証事業（BOX10参照）**である。TLPTとは、攻撃者が採用する戦術、手法を模倣した疑似的な攻撃を行うことで、侵入・改竄の可否や検知の可否、対応の迅速性・適切性を検証する、より実践的なテストを指す。金融庁はこれまで、取組事例に関する情報提供や、地域金融機関等に対するTLPT実証事業等を行ってきた。取組方針では、2026年中に、金融庁の事業として、暗号資産交換業者数社に対して、実運用環境へのTLPTを実施し、対象事業者に評価結果を通知するとともに、抽出した共通課題を業界全体に共有するとしている。

BOX10　脅威ベースのペネトレーションテスト（TLPT）

従来のペネトレーションテストと比較したとき、TLPTは、レッドチーム（セキュリティベンダー等の攻撃側のチーム）が実際の脅威アクターの行動を模倣して攻撃を行う点に特色がある。金融庁「金融分野におけるITレジリエンスに関する分析レポート」においては、TLPTを実施するにあたっての推奨事項を整理しており、①TLPTの目的（自組織のリスクの可視化、検知力・対応力の評価）を関係者間で共有すること、②組織全体を対象に本番環境で検証すること、③経営層が主導すること、④ブルーチーム（CSIRT等の防御側のチーム）には原則非通知で実施すること、⑤ホワイトチーム（調整役のチーム）の役割（TLPTと実際のサイバー攻撃によって発生するアラート等の切り分け、関係者からの照会に応じること等）とレッドチームとの連絡の最小化、⑥共同利用システムも可能な限り対象に含めることを挙げている。

3　おわりに

暗号資産交換業等のサイバーセキュリティ強化は、単なる規制対応にとどまらず、市場全体が利用者の信頼を獲得し、業界を持続可能にするために不可欠なものであ

る。昨今のような脅威環境のもとでは、経営陣がリスクの変化を的確に捉え、必要な人材、体制、投資を継続的に確保し、平時から対策の有効性を検証し続けることが求められる。また、暗号資産交換業者は、今後、現物暗号資産の売買・管理に加え、暗号資産ETFに関連する管理（カストディ）業務や、機関投資家向けのトークン化資産の取扱いなど、より重要かつ社会的責任を伴う役割を担うようになる可能性がある。暗号資産交換業者等は、金融サービスの担い手であると同時に、顧客に暗号資産の安全な管理を提供するというセキュリティサービスの提供者でもあることを自覚し、サイバーセキュリティを経営の中心課題として位置付け、形式ではなく実質（＝実効性）にコミットしたサイバーセキュリティ管理を実践していくことが期待される。

すぎの　たかや

2018年金融庁入庁、2023年ノースウェスタン大学ケロッグ経営大学院卒、2023～2025年ジョージタウン大学客員研究員、2025年７月から現職。

なす　しょう

2021年早稲田大学大学院法務研究科修了、同年司法修習生、2023年TMI総合法律事務所入所、2024年９月から現職。弁護士、情報処理安全確保支援士。