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

2026 年４月３日

金融庁

I. 問題意識

暗号資産は、ブロックチェーン技術を基盤とし、インターネット上で移転できる財産的価値である。攻撃者は、従来の金融とは異なり、財産的価値を有する資産そのものを瞬時に窃取することが可能である。また、国境を越えた資産移転も容易であり、盗難後の資産洗浄も即座に行われやすい。こうした特性等により、暗号資産は窃取を目的としたサイバー攻撃の対象となりやすいと考えられ、実際、ビットコインが誕生して以降、全世界において暗号資産交換業者等を標的とした暗号資産の流出に繋がるサイバー攻撃が数多く発生している。

近年の暗号資産の流出事案については、必ずしも署名鍵[1]の盗難が原因ではなく、ソーシャルエンジニアリング[2]や外部委託先への侵入[3]など、間接的な攻撃を含む巧妙な手法が用いられる傾向が顕著である。また、攻撃者が、暗号資産交換業者等に気付かれることなく時間をかけて侵入準備を行い、その後、攻撃を実行するケースも確認されている。このような状況下では、単にコールドウォレット[4]を用いれば安全に管理できていると言える状況ではなくなっており、外部委託先を含めたサプライチェーン全体にわたるサイバーセキュリティ管理態勢の強化が不可欠である[5]。加えて、外貨獲得を目的とする国家の関与が疑われるサイバー攻撃が発生していることも指摘されている[6]。暗号資産の保護は、単に利用者の財産を守ることにとどまらず、外貨獲得等を目的とする国家の関与が疑われる攻撃者の手に我が国の国富を渡らせないという観点からも対応が求められている。

我が国では、世界に先駆けて暗号資産交換業に関する規制を導入し、利用者から受託した暗号資産が流出する事案の発生を踏まえて、流出リスクへの対応やシステムリスク管理等を求めてきた。さらに、国内外の投資家において暗号資産が投資対象と位置付けられる状況が生じている中、暗号資産交換業者が国民に信頼されるためには、各事業者が、利用者財産の流出リスクに関する適切なマネジメントを行い、技術の進化や攻撃手法の高度化に応じたシステムリスク管理の継続的な見直しを実施するなど、強固なサイバーセキ

---

[1] 取引データに対して電子署名を付与し、当該取引が正当な権限者によって実行されたことを証明するために用いる秘密鍵。漏えい時には、不正な資産移転が行われるリスクが生じる。なお、金融庁「事務ガイドライン（第三分冊：金融会社関係）」等においては「秘密鍵」の用語が使われているが、ISO/IEC 14888 の標準規格に沿うと、「署名鍵」の用語を使うべきとの指摘があったため、本方針においては「署名鍵」を用いることとする。

[2] 利用者や職員の心理・行動の隙を突き、偽装メールや電話、なりすまし等を通じて認証情報やシステムへのアクセス権限を不正に取得する攻撃手法を指す。

[3] 事業者のシステムに対する外部からの直接的なサイバー攻撃ではなく、攻撃者がシステム運用・開発等を担う委託先のネットワークやアカウントを侵害し、その権限を足掛かりとしてシステムへ不正に侵入することを指す。

[4] 暗号資産を移転するために必要な署名鍵等を、常時インターネットに接続していない電子機器等に記録して管理する方法その他これと同等の技術的安全管理措置を講じて管理する方法をいう。

[5] 外部委託先のみならず、2025 年９月に発生した広く利用される JavaScript ライブラリへの悪意あるコード混入事案に示されるように、標的型メール等を契機として OSS 開発者を侵害し、依存ライブラリを汚染することで、多くの事業者の情報システム全体へ影響を及ぼす手口等も存在する。こうしたサプライチェーンリスクについても留意する必要がある。

[6] 警察庁サイバー警察局「令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について」（令和７年（2025 年）９月）（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf）
公安調査庁「令和８年（2026 年）内外情勢の回顧と展望」（https://www.moj.go.jp/content/001452738.pdf）

ュリティ管理態勢を構築することが必要となる。その際、各事業者が単独で昨今の脅威に対応できるとは限らず、自助・共助・公助の組み合わせによる官民一体となった対応が求められる。

暗号資産に関する制度の在り方については、2025 年7月以降、金融審議会「暗号資産制度に関するワーキング・グループ」[7]において、議論が重ねられ、同年 12 月 10 日に報告書[8]がとりまとめられた。この中で、暗号資産交換業者におけるサイバーセキュリティの高度化についても取り上げられている。同報告書の内容も踏まえ、金融庁は、各事業者の自助の取組の着実な実施を確保するほか、業界全体の共助の取組を促すとともに、公助の取組からの一定の支援策を実施すべく、今般、「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」を策定することとし、暗号資産交換業者、暗号資産サービス利用者及び関係者等と広く共有するため、公表することとした。

Ⅱ. 自助

Ⅰ.問題意識のとおり、暗号資産交換業者への攻撃手法の巧妙化の傾向を踏まえると、各事業者が、収集した情報を踏まえながらサイバーセキュリティ対策を常に進化させていくことが不可欠である。このため、各事業者の経営陣は、サイバーセキュリティ対策をコストと捉えて、最低限の水準を満たすことが目的化するようなことはあってはならない。強固なサイバーセキュリティ対策は、事業の収益を守り、持続的な成長を支えるための戦略的投資であって、前述のとおり、経営陣は、攻撃者が狙う我が国の国富を守るべき立場でもあることを認識する必要がある。

また、ブロックチェーン技術はイノベーションを進めるものであるが、それ自体は既存技術の組み合わせで構築されたものに過ぎない。したがって、各事業者においては、暗号資産特有のリスクに対応する観点だけでなく、既存の金融機関に求められるのと同様のサイバーセキュリティ管理態勢の確保も当然不可欠であり、その際には単に技術的対策を講じるだけでなく、人及びプロセスの面を含めた総合的なサイバーセキュリティ対策を適切に講じる必要がある。

以上を踏まえて、金融庁は、各事業者のサイバーセキュリティ管理態勢に係る実態把握を進めつつ、その水準の引き上げに資する「事務ガイドライン（第三分冊：金融会社関係）」の「16. 暗号資産交換業者関係[9]」（以下「事務ガイドライン」という。）の在り方を検討し、当局及び自主規制機関によるモニタリングを通じて、自助の取組の着実な実施を確保していく。

1. 業界への重点モニタリング

金融庁では、各暗号資産交換業者における流出リスクへの対応及びシステムリスク

[7] https://www.fsa.go.jp/singi/singi_kinyu/angoshisanseido_wg/angoshisanseido_wg_index.html
[8] https://www.fsa.go.jp/singi/singi_kinyu/tosin/20251210.html
[9] https://www.fsa.go.jp/common/law/guide/kaisya/16.pdf

管理について、これまでの大規模な流出事案を踏まえ、重点的にモニタリングを行い、各事業者が脅威の高度化に対応できるよう、サイバーセキュリティの強化を促してきた。さらに、2026 事務年度以降は、金融庁がこれまで他の金融業態向けに実施しているサイバーセキュリティセルフアセスメント（CSSA）[10]を暗号資産交換業者全社に実施することを求めることを含め、暗号資産特有のリスク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とする。継続的な対話を通じて、各事業者のサイバーセキュリティ管理態勢の状況を把握するとともに、高度化する脅威に対応するための必要な改善を促していく。

2. 事務ガイドラインの水準引上げ

以上の業界への重点モニタリングを通じて把握した各事業者における実態及び2025年度実施のブロックチェーン「国際共同研究」（後述）等の結果を踏まえて、事務ガイドラインで暗号資産交換業者に求めているサイバーセキュリティの水準の引上げを図る。例えば、以下の点について、実効性を確保する観点を踏まえつつ、検討を行う。

- 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

Ⅲ. 共助

個々の暗号資産交換業者が、日々変化するサイバー攻撃のリスクを単独で調査・把握するには限界がある。そこで、自主規制機関や情報共有機関が、必要に応じて当局と連携しながら、金融機関等にとって参考となる情報や対応事例の共有、態勢構築に関する支援など、業態全体のサイバーセキュリティ管理態勢の強化に向けた活動等（共助の取組）を推進することが望ましい。

共助の取組の実効性を確保するためには、業界団体等が、単に形式的な組織体制を整えるだけではなく、実質的に機能する仕組みを構築することが重要である。このため、金融庁は、業界団体等に対して、共助の取組の意義を踏まえ、実効的な運用体制の整備を促していく。

---

[10] 「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」（https://www.fsa.go.jp/common/law/cybersecurity_guideline.pdf）と整合した設問による自己評価を求めることで、自助の機会を提供するとともに、業界内で自組織の位置づけを可視化し、自律的な改善を促すことを目的としている。

1. 自主規制機関の体制強化

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、法令や当局によるガイドラインだけではなく、技術的・実務的な点を自主規制で定めることも重要である。自主規制機関は、高度化する脅威に的確に対応して自主規制のアップデートを継続的に行うとともに、各事業者における遵守状況のモニタリングを実効的に行うことが求められる。金融庁は、このための自主規制機関の体制整備について継続的にフォローアップを実施するとともに、必要に応じて改善を促していく。

具体的には、専門性を有する人材の確保・育成を通じて、セキュリティ委員会[11]等の機能を強化し、自主規制の内容を不断に改善・強化できる体制の整備を求めていく。また、専門人材を活用した監査体制を整備し、各事業者のサイバーセキュリティ管理態勢について、定期的なオンサイト・オフサイトのモニタリングを実効的に行うことができているか、フォローアップを行っていく。

2. 情報共有機関の体制強化と参加の慫慂

暗号資産交換業者における強固なサイバーセキュリティ管理態勢の確保のためには、各事業者での脅威・脆弱性の検知や情報収集だけでなく、業界全体での協調的な情報共有の枠組みが不可欠である。特に、直近で多用される攻撃手法、一般的なシステムの脆弱性情報等を迅速に共有し、共同で分析・対応を検討する体制を整えることが求められる。

その際、既存の金融業界等で機能している ISAC[12]と同様、暗号資産業界においても、単なる形式的な組織体制の整備ではなく、企業のセキュリティ実務担当者同士が信頼関係を構築し、実効的な情報共有を行う文化を醸成することが極めて重要である。

また、サプライチェーン全体のサイバーセキュリティ管理態勢の強化を図る観点からは、委託先や関連事業者を含む幅広い主体との連携の在り方についても考慮する必要がある。加えて、暗号資産取引の国際性を踏まえ、海外機関との連携を通じて国外の最新の脅威・脆弱性情報にアクセスできる体制を確立することが望ましい。

こうした観点から、金融庁は、各事業者による JPCrypto-ISAC[13]など情報共有機関への積極的な参加を促すとともに、代表的な暗号資産交換業界における情報共有機関である JPCrypto-ISAC との間で実効的な情報共有機関の在り方について意見交換を重ね、業界全体のサイバーセキュリティ強化に向けて取り組んでいく。

---

[11] 一般社団法人日本暗号資産等取引業協会（JVCEA）組織体制図（https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/jvcea-sosiki20250601.pdf）

[12] ISAC（Information Sharing and Analysis Center）とは、同一産業に属する企業・団体が集まり、サイバー攻撃や脆弱性、セキュリティインシデント、ベストプラクティス等に関する情報を共有するための非営利組織。

[13] JPCrypto-ISAC 公式ウェブページ（https://crypto-isac.jp/）

Ⅳ. 公助

金融庁は、これまで、暗号資産交換業者を含めた金融業界全般に対して、「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」等のガイダンスの提供、モニタリングの実施、演習（Delta Wall）等、関係機関や業界と連携しながら、公助の取組を進めてきた。こうした取組を更に進めるべく、特に暗号資産交換業者向けには、以下の取組を実施する。

1. ブロックチェーン「国際共同研究」プロジェクト

金融庁は、2017 年度より、ブロックチェーン「国際共同研究」プロジェクト[14]を推進し、分散型金融システムに内在する根本的な技術リスクに関する知見を提供してきた。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。

こうした調査研究は今後も継続的に実施していくとともに、暗号資産交換業者や情報共有機関等へ結果を還元し、自助・共助の取組の強化に貢献していく。また、暗号資産の国際性を踏まえ、国内におけるこうした取組を国際的な場における議論の題材として提供していくことで、国際的な連携の深化を図っていく。

2. 金融業界横断的なサイバーセキュリティ演習（Delta Wall）

「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」では、金融機関等に対し、サイバーインシデント対応計画[15]及びコンティンジェンシープラン[16]の策定を求めている。これを踏まえ、金融庁では、暗号資産交換業者を含めた金融業界全体のインシデント対応能力の更なる向上を図るべく、「金融業界横断的なサイバーセキュリティ演習（Delta Wall）」[17]を実施している。演習を通じて明らかになった課題については、各事業者に還元し、必要な改善を促すことで、サイバーセキュリティ管理態勢の強化を図ってきた。

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たが、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い、より実践的な演習環境を確保していく。また、暗号資産交換業者には定期的な演習への参加を引き続き求め、3年以内に全社の参加を目指す。

3. 脅威ベースのペネトレーションテスト（TLPT）実証事業

---

[14] 分散型金融システムに関する技術リスク等の調査研究を継続して実施。これまでに、①令和３年度（2021 年度）「分散型金融システムのトラストチェーンにおける技術リスクに関する研究」、②令和４年度（2022 年度）「分散型金融システムにおけるオンチェーン／オフチェーンデータを活用した実態把握に関する研究」、③令和５年度（2023 年度）「金融セクターにおけるトークナイゼーションの進展とブロックチェーンの RegTech/SupTech への活用可能性に関する研究」などの成果を公表。

[15] インシデント発生時に必要な初動対応・封じ込め・根絶・復旧等を体系化した計画。

[16] 重大障害・緊急事態発生時に金融機関が重要業務を継続・復旧するための代替手段を定める計画。

[17] 金融庁が金融業界全体のインシデント対応力向上を目的に毎年実施するサイバーセキュリティ演習。名称は「自助・共助・公助」（Delta）と防御（Wall）に由来する。

各暗号資産交換業者による現在のサイバーセキュリティ対策が高度化する攻撃に耐えうるかを確認するには、脅威ベースのペネトレーションテスト（Threat-Led Penetration Testing（TLPT））[18]による検証が有効とされている。各事業者は、こうしたテストを通じて、技術面だけではなく、人及びプロセスの面を含む組織全体の弱点を把握し、適切に改善していく必要がある。

金融庁はこれまで、金融機関のサイバーレジリエンス強化のための政策として、金融機関における TLPT に関する事例還元や、地域金融機関等に対する TLPT 実証事業といった取組を進めてきた。

暗号資産交換業者についても、TLPT の有用性を実証することで、TLPT 実施の障壁を下げ、その普及を促す。具体的には、2026 年中に、全事業者のうち数組織に対して、実運用環境への TLPT を実施する。その上で、各事業者に評価結果を還元するとともに、抽出した共通課題を業界全体に還元[19]することで、暗号資産業界全体のサイバーセキュリティ強化を図る。

Ⅴ. 結び

本方針は、暗号資産を巡る脅威が一層高度化・多様化する中で、暗号資産交換業者等によるサイバーセキュリティ強化に向けた取組の方向性を示すものである。金融庁は、本方針に基づく各種取組を着実に実施するとともに、暗号資産を取り巻く技術動向や攻撃手法、国際的な議論の進展を踏まえつつ、必要に応じて不断に取組の見直しを行い、実効性の維持・向上を図っていく。

また、暗号資産交換業者、自主規制機関、情報共有機関、関係事業者、海外当局等との連携を継続し、官民一体となってサイバーセキュリティ強化に取り組むことが重要である。各暗号資産交換業者等においても、本方針を踏まえた主体的な取組を進め、我が国における暗号資産市場の安全性と信頼性の確保に向けて、引き続き積極的な役割を果たすことを期待している。

---

[18] 自組織が抱えるリスクを個別具体的に分析した上で、攻撃者が採用する戦術、手法を再現し疑似的な攻撃を仕掛けることで、侵入・改ざん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。レッドチームテストとも呼ばれる。（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（2025 年６月）https://www.fsa.go.jp/news/r6/sonota/20250630-2/01.pdf）

[19] 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（2025 年６月）第２章第２節 TLPT を実施するにあたっての推奨事項（https://www.fsa.go.jp/news/r6/sonota/20250630-2/01.pdf）