暗号資産分野のサイバーセキュリティー強化に向けた対応方針

自助・共助・公助での対応へ、法改正を踏まえて市場の信頼確保

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

暗号資産交換業者等を狙うサイバー攻撃は高度化・巧妙化しており、利用者財産を直接脅かすだけでなく、国内の財産（国富）の流出にもつながり得る。金融庁は4月3日、こうした危機感の下、業界全体の防御力を高め、信頼ある市場を築くため、「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）を策定・公表した。本稿では、その背景と概要を紹介する。

繰り返されるサイバー攻撃の脅威

暗号資産に関連する技術と市場は、ビットコイン誕生以降、発展を遂げてきた。その一方で、暗号資産交換業者等を標的とするサイバー攻撃は国内外において繰り返し発生し、その手口も高度化・巧妙化している。

その対策について、コールドウォレットによる管理は、署名鍵のオンライン環境からの隔離という観点では重要であるが、それだけで十分とはいえない。近年、ソーシャルエンジニアリングや委託先・外部サービスへの侵入、開発・運用環境の侵害、認証情報の窃取・悪用、サプライチェーン攻撃など、必ずしも署名鍵の窃取を伴わない攻撃手法が用いられるようになっている。

実際、暗号資産交換業者等から多額の暗号資産が不正に流出する事案が複数確認されている。暗号資産の管理や移転に関わる業務プロセスを狙った攻撃による大規模な流出事案も発生した。これらの脅威アクターには、資金獲得等を目的とする国家を背景とするものも含まれており、彼らは組織的に攻撃やその試行を行っている。

暗号資産は、ひとたび不正流出が生じれば、短時間のうちに国境を越えて移転され得る。また、複数のアドレスやサービスを経由して移転され、事後的な追跡や回収は困難である場合も多い。このような暗号資産の性質から、暗号資産交換業者等は、資金獲得を目的とする攻撃者にとって格好の標的となっている。

従って、暗号資産交換業等のサイバーセキュリティーを強化し、その流出を未然に防ぐことは、利用者財産の保護に直結する課題である。国富の不正な流出を防ぎ、ひいてはわが国の安全を確保する観点からも重要になる。

もっとも、ここでいう暗号資産の性質に起因するリスクとは、必ずしも既存の金融分野でのサイバーセキュリティー対策によって対応できないようなリスクを意味するものではない。むしろ暗号資産交換業者等にも、まずは伝統的金融機関と同様に、経営管理やリスク管理、委託先管理、システム管理、インシデント対応等を含む総合的なサイバーセキュリティー管理態勢を構築することが求められる。その基礎の上に、暗号資産特有のリスクに即した追加的な対応を重ねる必要がある。

法改正と軌を一にする取組方針の策定

取組方針は、暗号資産交換業者等のサイバーセキュリティー管理態勢の強化に向け、金融庁として今後進める取り組みの方向性を示すものである。各事業者による自主的な態勢整備を基礎としつつ、自主規制機関・情報共有機関等を通じた業界全体の取り組み、さらに金融庁による支援と監督を組み合わせることが重要である。それにより、暗号資産交換業等におけるサイバーセキュリティー水準の底上げを図る考え方が示されている。

本方針の背景には、金融審議会「暗号資産制度に関するワーキング・グループ（WG）」における議論がある。WGでは、暗号資産制度の見直しに関する幅広い検討が行われたが、利用者財産の保護の観点から、サイバーセキュリティーの重要性があらためて確認された。

サイバー攻撃の手法は常に変化し、事業者のシステム構成や利用する技術も動的に変化する。そうしたことを踏まえ、WGでは、法令においては体制整備に係る基本的な義務を定めつつ、具体的な技術的や運用上の要件については、ガイドライン等により柔軟に対応していくことが適当であるとの方向性が示された。またWGのメンバーからは、暗号資産分野においてもサイバーセキュリティーを協調領域として捉え、業界全体で底上げを図ることの重要性等が指摘された。

暗号資産交換業者等においては、伝統的金融機関や他の重要インフラ事業者に当然に求められている標準的なセキュリティーマネジメントを着実に実施していく必要がある。ただ、十分なセキュリティー人材や管理態勢を単独で確保することが容易でない暗号資産関連事業者も存在する。こうした問題意識が、WGの議論の根底にある。

政府はWGの報告を受けて、4月10日に「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」を提出した。同法案は、暗号資産取引に係る規制を資金決済に関する法律から金融商品取引法に移管し、有価証券とは異なる金融商品として、暗号資産の性質を踏まえた規制を整備することを内容とするものである。

この中で、暗号資産等の管理については、暗号資産取引業者の善管注意義務や業務方法、委託先・システム提供者の適切な選定・指導等を新たに定めることとしている。暗号資産の管理

を行うための重要なシステムの提供者に係る届け出制等なども盛り込まれた。同法案が成立した場合、法令上の基本的な規律と、監督・実務上の対応を組み合わせながら、高度化・巧妙化するサイバー攻撃の脅威に対応していくことになる。

取組方針は、こうした制度面の見直しと軌を一にしたものである。特にサイバーセキュリティーに関して、金融庁がどのように事業者、自主規制機関、情報共有機関等と向き合い、業界全体のサイバーセキュリティー管理態勢の高度化を促していくかを明らかにした。以下では、自助・共助・公助の枠組みに沿って、具体的な内容について解説する。

自助――経営責任としての態勢整備

自助とは、各暗号資産交換業者等が自らの経営判断として、サイバーセキュリティー管理態勢を継続的に高度化していくことである。サイバーセキュリティーは、単なるシステム部門の課題でも、最低限の規制対応でもない。利用者財産を保護し、事業の継続性を確保し、市場からの信頼を維持するための経営上の中核課題である。経営陣は、サイバーセキュリティーを単なるコストではなく、事業基盤を守るための戦略的投資として位置付ける必要がある。

暗号資産交換業者等に求められる自助の内容は広い。署名鍵管理やウォレット管理に加え、アクセス権限管理、ログ監視、脆弱性管理、開発環境の保護、委託先管理、サプライチェーンリスク管理、インシデント対応計画、経営陣への報告体制等が含まれる。

近年の攻撃は前述のとおり、必ずしも署名鍵そのものを直接窃取するものに限られない。ソーシャルエンジニアリングのほか、外部委託先や暗号資産交換業者等が利用する外部サービスへの侵入、開発・運用環境の侵害、認証情報の窃取・悪用など、攻撃の入り口は多様である。従って、特定の技術的措置を取れば足りるものではなく、多層的な防御態勢を構築し、組織全体として十分なリスク低減を図る必要がある。

金融庁は、この自助の取り組みを促す観点から、各事業者の実態把握を進めるとともに、事務ガイドラインの水準の引き上げを検討することとしている。具体的には、サイバーセキュリティーに係る人的構成、外部監査、外部委託先管理・外部サービスの管理等について、監督上の着眼点をより明確化し、暗号資産交換業者等に求められる管理態勢の水準を高めていくことが想定される。これは、個社の自律的な改善を促しつつ、業界全体として最低限確保すべき実務水準を引き上げるための重要な取り組みであり、金融庁としてはモニタリングを通じて、実効性について検証していく。

事業者も、こうした要請を形式的なチェックリストとして受け止めるのではなく、実効性ある管理態勢を設計することが重要である。自社の業務特性、預かり資産の規模、利用する技術、委託先・システム提供者との関係、インシデント発生時の影響等を踏まえた対応が不可欠である。

その際、サイバーセキュリティーは、専門部署だけで完結するものではない。経営や法務、コンプライアンス・リスク管理、システム、顧客対応が、経営陣のコミットメントの下に有機的に連携して初めて機能する。サイバーセキュリティーを実効的なものとするためには、経営陣がリスクの所在を理解し、必要な人材や予算、権限を適切に配分し、平時から態勢の有効性を検証し続けることが不可欠である。

共助――業界全体の底上げ

次に共助とは、業界全体としてサイバーセキュリティー管理態勢を高めるための仕組みである。この点、自主規制機関が技術的・実務的な知識を生かして規則やガイドラインを整備し、各事業者の順守状況を把握し、必要に応じて改善を促すことが重要である。ＪＰＣｒｙｐｔｏ－ＩＳＡＣ（ジェイピークリプトアイザック）などの情報共有機関が、脅威・脆弱性情報やインシデント・対応事例を集約・分析し、実務に資する脅威インテリジェンスとして業界に還元していくことも求められる。

サイバーセキュリティーの分野では、個社が単独ですべての脅威動向を把握し、十分な防御策を講じることには限界がある。攻撃者が強力な動機に基づいて組織的に活動している以上、防御側も業界横断的な連携を強化しなければならない。特に、このような情報の集約・分析・共有は、脅威動向に対処するために不可欠の取り組みである。

金融庁は、自主規制機関や情報共有機関の体制整備を促し、各事業者による積極的な参画を慫慂（しょうよう）することで、業界全体のサイバーセキュリティー水準の向上を図ることとしている。自主規制機関には、形式的な規則整備にとどまらず、技術的知見を有する人材の確保や実効的なモニタリング、事業者との継続的な対話、必要に応じた自主規制上の対応が期待される。

一方、情報共有機関には、迅速かつ実務に有用な情報の収集・分析・共有を通じて、各社の防御態勢と対応能力を高める役割が期待される。特にジェイピークリプトアイザックについては今後、多くの事業者が参加し、実務に有効な情報が集約されることで、暗号資産業界を代表する情報共有機関として発展していくよう、業界の英知の結集に期待したい。

共助を実効的なものとするためには、事業者自身も単に情報を受け取る立場にとどまらず、可能な範囲で知見や経験を還元していく姿勢が求められる。重大なインシデントや攻撃の兆候に関する情報を適切に共有できれば、他社における被害の未然防止につながり得る。サイバーセキュリティーについては、競争領域と協調領域を適切に区別し、業界全体で防御力を高めるという発想が重要である。

公助――金融庁による支援と監督

三つ目の公助とは、金融庁が行政として、個社および業界全体の取り組みを支えることである。これは、事業者の責任を肩代わりするものではない。サイバーセキュリティーの一義的な責任は、あくまで利用者財産を預かり、サービスを提供する各事業者にある。

公助の出発点は、業界に対する適切なモニタリングである。各事業者の態勢整備の状況、経営陣の関与、委託先や外部サービスの管理、インシデント対応能力等を的確に把握し、必要な対話を行うことにより、個社や業界全体の課題を明らかにする。その上で、金融庁は公助の取り組みを通じて、自助・共助が実効的に機能するよう後押しする役割を担う。

金融庁は、暗号資産交換業者等について国内外の攻撃事例やリスク、対応策に関する調査研究を行い、その成果を事業者や関係機関に還元することとしている。また、暗号資産交換業者等の実態を踏まえた演習・検証を通じて、各事業者の対応能力向上を促すこととしている。「金融業界横断的なサイバーセキュリティ演習」（Delta Wall）は、従来、伝統的金融機関を対象に実施してきたが、２０２５

年度に、暗号資産交換業者等に即したシナリオを取り入れた。今後、業態特有のリスクを踏まえた実践的な対応能力の向上が期待される。

さらに、現実の攻撃者の手法や行動を踏まえ、実運用環境に対して疑似的な攻撃を行い、組織の検知・対応能力を検証する取り組みが、「脅威ベースのペネトレーションテスト」（TLPT＝Threat-Led Penetration Testing）である。攻撃者がどのような経路で侵入し、権限を拡大し、重要資産に到達し得るかを想定し、これを模倣することで、防御側が現実の脅威に対応できているかを実践的に検証する。こうした取り組みを通じて、平時には見えにくい組織上・技術上の弱点を把握し、改善につなげることが可能となる。

加えて金融庁は、取組方針に示された基本的な考え方を軸としつつ、技術動向や攻撃手法、国際的な議論の進展等を踏まえ、モニタリングやガイドライン整備、業界との対話、調査研究、演習等の各施策を、環境の変化に応じて機動的に運用していく。その趣旨は、各施策の実効性を継続的に点検し、技術や脅威の変化に応じて、支援・監督の在り方を改善していく点にある。

信頼される市場に向けた事業者への期待

暗号資産交換業等のサイバーセキュリティー強化は、単なる規制対応ではない。利用者が安心してサービスを利用し、事業者が持続的に事業を営み、市場全体が信頼を得るために不可欠の前提である。変化し続ける脅威環境の下では、過去に有効であった対策が将来も十分であるとは限らない。重要なのは、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である。

今後、暗号資産交換業者等には、現物暗号資産の売買・管理に加え、暗号資産ETF（上場投資信託）に関連するカストディーや暗号資産以外のトークン化資産の取り扱い等の機関投資家向けサービスなど、より高度な役割が期待される可能性がある。こうした役割が拡大するほど、事業者が預かり、管理する財産的価値はいっそう大きくなり、社会的責任もより大きくなる。

暗号資産交換業者等は、単なる技術サービスの提供者ではなく、金融サービスの担い手であり、市場の信頼は自らの実践にかかっている。新たな市場機会を信頼あるかたちで担っていくためにも、サイバーセキュリティーを経営の中心課題として位置付け、強固で実効的なサイバーセキュリティー管理態勢を構築していくことは不可欠である。

金融庁としても、事業者、自主規制機関、ジェイピークリプトアイザックを含む情報共有機関その他の関係者との対話を重ねながら、暗号資産交換業等におけるサイバーセキュリティー管理態勢の高度化を促していく。繰り返しになるが、最終的に市場の信頼をかたちづくるのは、日々利用者と向き合い、利用者財産を守る各事業者の実践である。各事業者がこの課題を自らの責務として受け止め、形式ではなく実効性にコミットした取り組みを積み重ねていくことを期待する。

すぎの　たかや
18年金融庁入庁。23年ノースウエスタン大学ケロッグ経営大学院修了、23～25年ジョージタウン大客員研究員。25年7月から現職。

なす　しょう
21年早稲田大学大学院法務研究科修了。21年司法修習生、23年TMI総合法律事務所入所。24年9月から現職。