

ブロックチェーンビジネスにおいて求められる サイバーレジリエンスの構築

PwC Japan有限責任監査法人
リスク・アシュアランス部
パートナー 須田 真由



PwC Japan有限責任監査法人
リスク・アシュアランス部
マネージャー 望月 夕衣



はじめに

暗号資産をはじめとするブロックチェーン関連サービスは、投資・決済・資産保全を支える金融インフラとしての存在感を高めています。一方で、暗号資産はインターネット上で移転可能な財産的価値であり、攻撃が成功した場合には短時間での資産流出に直結し得るという特性があります。近年では、署名鍵の盗難にとどまらず、ソーシャルエンジニアリング、外部委託先への侵入、サプライチェーンを介した攻撃など、ブロックチェーン関連事業者を取り巻く脅威は一層高度化・複雑化しています。

加えて、生成AIをはじめとするフロンティアAIの進展は、攻撃者の能力を押し上げる可能性があります。脆弱性探索、攻撃経路の特定、フィッシングの高度化、マルウェア開発支援などが低コスト化・高速化することで、従来以上に迅速かつ実効性のあるサイバーリスク管理が求められます。

本稿では、改正金融商品取引法、フロンティアAIへの対応、経営陣の関与、リスクベースアプローチ、暗号資産業界特有の留意点の5つの観点から、ブロックチェーン関連事業者求められるサイバーレジリエンスの再構築について考察します。

なお、文中の意見は筆者の私見であり、PwC Japan有限責任監査法人および所属部門の正式見解ではないことをお断りしておきます。

1 拡大する暗号資産関連のビジネス領域とリスク

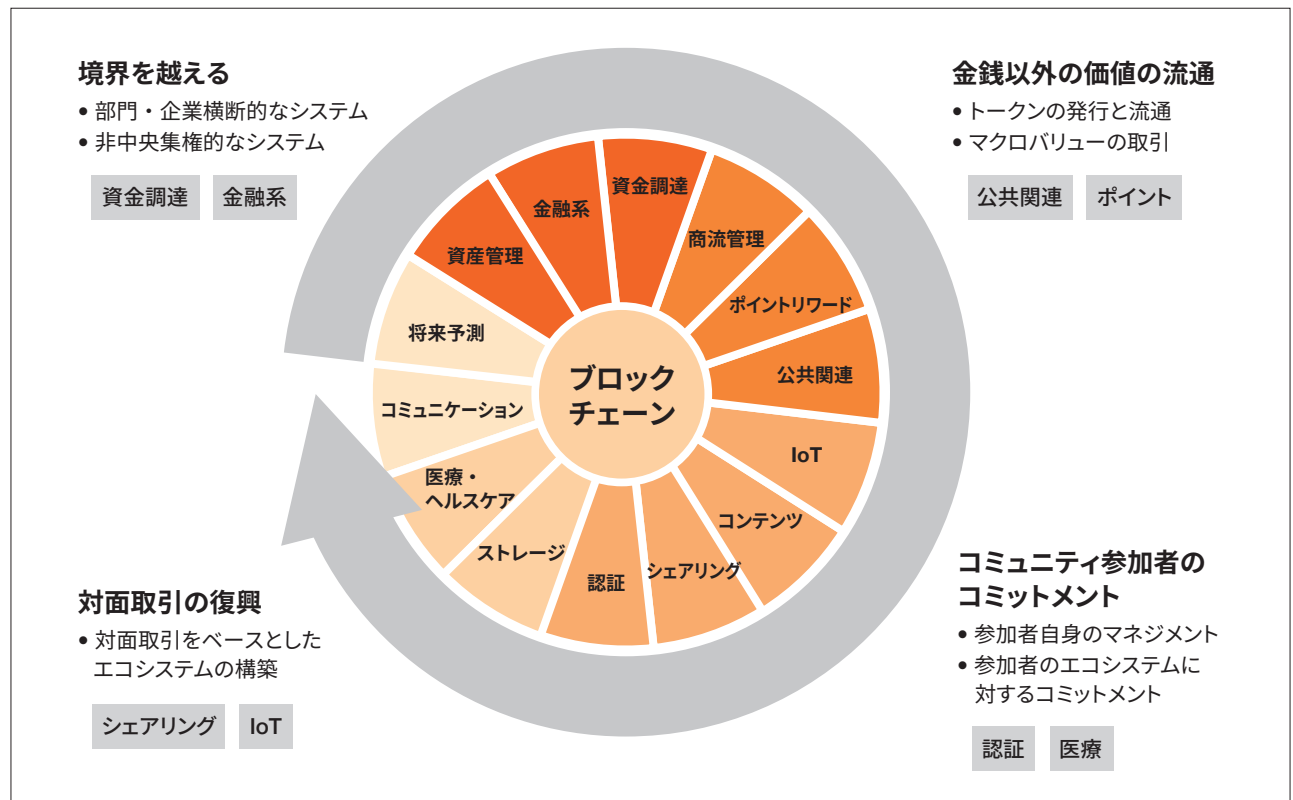
暗号資産をはじめとするブロックチェーン関連サービスは、ブロックチェーン技術を基盤とする新たな金融サービスとして発展してきました。近年では、暗号資産そのものに加え、トークン化、カストディ、DeFi（分散型金融）、ステーブルコイン、決済、投資商品など、関連するビジネス領域が広がっています（図表1）。こうした市場の拡大は、利用者の利便性や金融イノベーションの可能性を高める一方で、事業者には利用者資産の保護、市場の信頼確保、事業継続の観点から、より高度なリスク管理が求められることを意味します。

特に、暗号資産の移転には不可逆性があるため、ひとたび不正送金が発生すると、金融機関における一般的な不正送金以上に事後的な回復が困難となるおそれがあります。そのため、暗号資産事業者におけるサイバーセキュリティは、単なるIT管理やシステム部門の課題ではなく、利用者保護、規制対応、経営戦略、企業価値に直結する経営課題として位置付ける必要があります。サイバー対策を、規制対応のためにチェックリスト的に文字通り対応するのではなく、経営として優先順位を付けて設計・運用すべきサイバーレジリエンスの課題として捉えるべきです。

2 規制対応を超えて問われる、暗号資産ビジネスの統制力

2026年7月に改正金融商品取引法（改正金商法）が成立しました。改正金商法への対応として、暗号資産関連サービス事業者は、業務管理態勢、内部管理態勢、コンプライアンス、リスク管理、サイバーセキュリティを一体として設計することがより重要となります。

図表1：ブロックチェーンの活用領域



出所：PwC作成

特に暗号資産関連サービス事業者は、中央集権的な運用主体と分散型基盤の双方のリスクを併せ持ちます。ブロックチェーンは透明性や耐改ざん性を備える一方で、実際のサービス提供では、取引所、カストディアン、ウォレット、フロントエンド、クラウド、API、外部委託先といったオフチェーン要素に大きく依存しています。

したがって、改正金商法対応においては、オンチェーンのコードやプロトコルだけでなく、オフチェーンの運用統制、外部依存関係、アクセス管理、署名プロセス、ガバナンス、インシデント対応、利用者保護を含めた包括的な統制基盤としてサイバー対策を設計する必要があります。

また、規制対応を進めるにあたっては、サイバーセキュリティを「個別規制への適合項目」として扱うだけでは不十分です。重要なのは、利用者資産の保護、重要業務の継続、重大インシデント時の意思決定、外部委託先を含むサプライチェーン管理といった経営上の論点と結び付け、実効性のある管理態勢として具体化することです。

3 フロンティアAIが変える、サイバー攻撃の速度と精度

生成AIをはじめとするフロンティアAIの進展により、

攻撃者は従来よりも低いコストで高度な攻撃能力を獲得できるようになっています。脆弱性探索の自動化、攻撃経路の特定、フィッシングメールの高度化、なりすまし、マルウェア開発支援、標的型攻撃の大規模化など、脅威環境は急速に変化しています。

暗号資産業界では、この影響が特に大きいと考えられます。攻撃が成功した場合、短時間で直接的な資産流出につながる可能性があるためです。特に、署名鍵、ウォレット、アクセス制御、CI/CD（ソフトウェア変更の自動化）、クラウドIAM/KMS（権限管理／鍵管理）、署名サービス等の運用インフラは、攻撃者にとって高い投資対効果を持つ標的となり得ます。

また、攻撃者は「侵入する」だけでなく、認証情報、セッショントークン、フェデレーションアクセスを悪用して「ログインする」傾向を強めています。人間のアイデンティティだけでなく、サービスアカウント、APIキー、CI/CDパイプライン、クラウド権限、署名権限といった非人間アイデンティティを含めた管理が不可欠です。

フロンティアAI時代のサイバー対策では、従来型の境界防御だけではなく、侵害を前提とした検知・封じ込め・復旧能力が重要になります。加えて、AIを悪用した攻撃

の高速化に対応するためには、ログ監視、アラート対応、脅威インテリジェンス、演習、レッドチーム、外部評価などを組み合わせ、組織として継続的に防御能力を検証することが求められます。

4 サイバーリスクを経営のトップアジェンダに引き上げる

改正金商法対応とフロンティアAIへの対応は、いずれも暗号資産関連サービス事業者におけるサイバー対策の重要性を高めています。サイバーインシデントが発生した場合、利用者資産、事業継続、市場の信頼に直ちに影響が及ぶ可能性があるため、サイバーリスクはIT部門だけの管理課題ではなく、経営として優先的に管理すべきトップリスクのひとつとして位置付ける必要があります。

前述したように、暗号資産の移転には不可逆性があるため、ひとたび不正送金が発生すると、事後的な回復が困難となるおそれがあります。そのため、経営陣は重要資産、重要業務、重要委託先、重大インシデントシナリオを把握したうえで、予防、検知、停止、復旧を含む多層的な管理態勢を整備する必要があります。

また、経営陣の関与は、単に方針を承認することだけにとどまりません。リスクアパタイト、投資優先順位、KRI（重要リスク指標）、報告ライン、インシデント時の意思決定プロセスを明確にし、第1線、第2線、第3線が連携してサイバーリスクを継続的に管理する態勢を整えることが重要です。

特に暗号資産関連サービス事業者では、専門性の高い技術領域と、経営判断を要するリスク領域が密接に結び付いています。たとえば、ウォレット構成、署名方式、クラウド権限、委託先の運用、スマートコントラクトのアップグレード権限、緊急停止手続きなどは、技術的な論点であると同時に、利用者資産の保全や事業継続に直結する経営判断でもあります。

5 ガイドラインを出発点に、実効性あるリスク管理へ

現在、当局や関係機関から各種ガイドラインや指針が公表されています。これらは、金融機関に求められる管理態勢を整理するうえで役に立ちます。一方で、暗号資産関連サービス事業者が留意すべきなのは、ガイドラインをチェックリストとして機械的に充足するだけでは、実効的なセキュリティ態勢につながるとは限らないという点です。

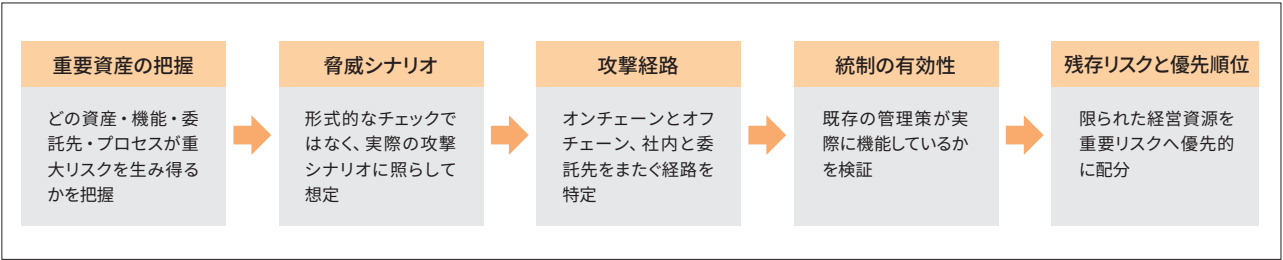
既存のガイドラインには、暗号資産関連サービス事業者における主要な脆弱性に対応する項目も含まれています。しかし、実際の管理策は、自社のシステム構成、委託関係、ウォレット・鍵管理方式、DeFiや外部サービスの利用状況に応じて具体化し、必要に応じて深掘りすることが求められます。

たとえば、同じ「アクセス管理」であっても、一般的な社内システムのID管理と、出庫承認、署名権限、MPC（マルチパーティ計算）運用、クラウドKMS、スマートコントラクトのアップグレード権限、CI/CD環境への本番反映権限では、リスクの性質も管理すべき統制も異なります。

ガイドラインは到達点ではなく出発点です。重要なのは、ガイドラインの各項目を文字通りに充足することそのものではありません。自社にとって、どの資産、機能、委託先、プロセスが重大なリスクを生み得るのかを把握し、限られた経営資源を重要リスクに優先配分することです。

そのためには、重要資産・重要業務を起点に、脅威シナリオ、攻撃経路、統制の有効性、残存リスクと優先順位を明確化する必要があります（図表2）。特に暗号資産関連サービス事業者では、オンチェーンとオフチェーン、技術と運用、社内と委託先が複雑に結び付くため、形式的なチェックよりも、実際の攻撃シナリオに照らしたリスク評価が重要になります。

図表2：重要資産・重要業務を起点としたリスク評価の流れ



出所：PwC作成

6 暗号資産固有の攻撃シナリオにどう備えるか

暗号資産業界では、一般的な金融機関と共通するサイバーリスクに加え、業界特有のリスクを踏まえた対策が必要です。特に、**図表3**に挙げた領域については、自社の事業モデルやシステム構成に即して優先的に確認することが重要です。

(1) 委託先は「外部」ではなくリスクの一部として管理する

暗号資産関連サービス事業者は、出庫、署名、鍵管理、ウォレット運用、CI/CD、クラウド基盤、監視、KYC/AML（顧客確認／マネー・ローンダリング防止）など、多数の重要業務を外部サービスに依存しています。そのため、委託先管理では、契約上のセキュリティ条項を確認するだけでは十分ではありません。

委託先のシステム構造、管理体制、アクセス権限、再委託関係、ログ監視、インシデント対応、プログラム変更管理、特権ID管理、要員管理、復旧能力を確認し、自社のリスク管理上不足する部分を補完することが重要です。

また、委託先の侵害が自社サービスや利用者資産に波及することを前提に、追加承認、利用上限、異常検知、自動停止、代替手段、緊急時連絡体制などをあらかじめ整備する必要があります。

(2) 正規の開発・運用プロセスが攻撃経路になり得る

暗号資産サービスでは、UI、API、CI/CD、スマートコントラクト、署名前トランザクション生成ロジック、本番環境プログラムが攻撃対象となり得ます。そのため、開発環境と本番環境の分離、コードレビュー、変更承認、署名

付きビルド、SBOM（ソフトウェア部品表）管理、脆弱性管理、リリース前検証、CI/CD権限管理、緊急変更の統制、開発者端末の保護を一体として設計する必要があります。

特に、正規の署名者が悪意あるトランザクションを承認してしまうリスクを踏まえると、署名前の内容検証、送金先アドレスの検証、異常な出庫パターンの検知、追加承認、自動停止、利用上限の設定が重要です。

(3) 不正送金を「起こさせない・止める」仕組みを設計する

暗号資産の不正送金は、発生後の回復が困難です。そのため、事前の防止と即時検知が重要となります。ホットウォレットとコールドウォレットの分離、出庫上限、複数者承認、MPCやHSM（ハードウェア・セキュリティ・モジュール）の適切な利用、承認者の職務分離、送金先アドレスのホワイトリスト管理、異常検知、オンチェーン分析、トランザクションモニタリング、緊急停止手続、インシデント時の連絡・封じ込め手順を整備することが求められます。

また、出庫プロセスでは、技術的統制だけでなく、オペレーション統制も重要です。画面表示、エラーメッセージ、例外処理、承認手順、担当者教育、複数名確認など、人的ミスや不審事象の見落としを防ぐ設計が必要です。

(4) スマートコントラクトとDeFiのリスクを運用レベルで捉える

DeFiやスマートコントラクトを利用する場合、従来型のシステム管理だけではリスクを十分に捉えきれません。スマートコントラクトの脆弱性、アップグレード権限、管理者権限、フラッシュローン攻撃、流動性リスク、ガバナ

図表3：暗号資産固有の攻撃シナリオへの5つの備え

1	2	3	4	5
委託先管理	開発・運用プロセス	不正送金の防止と停止	スマートコントラクト・DeFi	外部評価と脅威情報
委託先を「外部」ではなくリスクの一部として管理。再委託・特権ID・復旧能力まで確認し、自動停止や代替手段を事前整備。	UI・API・CI/CD・本番環境が攻撃経路になり得る。環境分離、変更承認、権限管理、署名前の内容検証を一体で設計。	ホット／コールド分離、出庫上限、複数者承認、MPC・HSM、ホワイトリスト、異常検知、緊急停止手続。	スマートコントラクトの脆弱性、ブリッジ等の固有リスクを評価。外部監査は範囲と時点を継続確認。	TLPT、レッドチーム、机上演習、第三者評価を組み合わせ、結果を経営報告・投資判断・改善計画へつなげる。

出所：PwC作成

ンス攻撃、プロトコル連携リスク、ブリッジリスクなど、暗号資産特有のリスクを評価する必要があります。

その際、外部監査を実施していることだけで安心するのではなく、監査範囲、監査時点、除外範囲、是正状況、運用変更後の再評価、依存プロトコルの変化などを継続的に確認することが重要です。

(5) 外部評価と脅威情報で、自社の実力を継続的に検証する

攻撃手法が高度化する中では、自社による点検だけでなく、外部評価や脅威インテリジェンスの活用が重要です。脅威ベースのパネトレーションテスト、レッドチーム演習、机上演習、インシデント対応訓練、第三者評価、クラウド設定診断、スマートコントラクト監査、ブロックチェーン分析、脅威情報共有機関からの情報収集を組み合わせることで、組織の実効的な防御・検知・対応能力を確認できます。

また、評価結果は単なる報告書として扱うのではなく、経営報告、改善計画、投資判断、KRI、訓練シナリオ、委託先管理の見直しにつなげることが重要です。

7 おわりに

改正金商法への対応とフロンティアAIの進展は、暗号資産関連サービス事業者に対して、サイバーリスクをトップリスクとして捉え、経営陣が強く関与することの重要性を示しています。

そのうえで求められるのは、ガイドラインへの形式的な適合にとどまらない対応です。自社のビジネスモデル、システム構成、委託関係、ウォレット・鍵管理方式、DeFiや外部サービスの利用状況を踏まえ、リスクベースで対策を具体化し、継続的に見直していくことが不可欠です。

特に暗号資産業界では、委託先管理、開発・運用プロセス、不正送金防止、スマートコントラクト・DeFi、外部評価と脅威情報の活用といった固有の論点を踏まえて、実効的なサイバー対策を設計する必要があります。

サイバーセキュリティは、もはや規制対応のためのコストではありません。暗号資産関連サービス事業者が社会的信頼を獲得し、金融インフラとして持続的に成長するための競争力そのものとして位置付けられるべきです。

須田 真由 (すだ まさよし)

PwC Japan 有限責任監査法人 リスク・アシュアランス部 パートナー
製造業、情報通信業および金融業（資金決済・暗号資産）を中心とした、IT領域において財務諸表監査、ならびに国内上場企業の内部統制監査を担当。また、米国証券取引委員会（SEC）登録日本企業、外資系企業の米国企業改革法に基づく内部統制監査業務にも従事。アドバイザー業務としては、財務報告に係るIT統制の構築および評価支援やフィンテックに関連するITガバナンス構築支援業務をリード。ブロックチェーン技術のセキュリティおよびガバナンスに関する講演も多数実施。

メールアドレス：masayoshi.suda@pwc.com

望月 夕衣 (もちづき ゆい)

PwC Japan 有限責任監査法人 リスク・アシュアランス部 マネージャー
証券会社での個人向け営業、金融機関向けシステム会社での開発・導入・管理フロー構築、外資系コンサルティングファームでのシステム監査やITガバナンス構築経験を経て2019年5月より現職。金融機関向けサイバーセキュリティ評価（NIST CSF、FFIEC CAT、CRI Profile、当局監督指針に基づく態勢評価、シナリオベースでのサイバー脅威に対する態勢評価〔技術的観点を含む〕など）やクラウドセキュリティ評価の経験を有する。その他、フィンテックに関連する内部監査支援、セキュリティ体制構築支援、法令対応支援等の各種支援提供実績を有する。また、各種金融機関を中心とする監査において、J-SOXのIT全般統制やIT業務処理統制等のITシステムを対象とする領域を担当。

メールアドレス：yui.mochizuki@pwc.com