暗号資産ステーキングビジネスに関するベストプラクティス

初版　令和 8 年（2026 年）5 月 7 日 策定

一般社団法人 日本暗号資産ビジネス協会

目次

1. はじめに：本ベストプラクティスの対象と目的

本ベストプラクティスは、ステーキングを含む暗号資産関連サービスを既に提供している事業者、または今後当該サービスの提供を検討している事業者を主な対象とするものである。事業者がステーキングの仕組みおよびリスクの実態について理解を深めるとともに、サービス利用者（以下「利用者」という。）に対して正確かつ十分な情報提供および開示を行うことを促すことを目的とする。

これにより、利用者が十分な理解を持たないまま暗号資産ステーキングを行うことや、過度なリスクテイクに至ることを抑制し、暗号資産ステーキング市場の健全性および透明性の向上に資することを目指す。

なお、本資料は規制や拘束力を伴うものではなく、事業者が実務上の判断を行う際の参考指針および業務改善の目安として整理したベストプラクティス集である。また、本資料は特定の暗号資産、プロトコルまたはステーキングサービスの安全性や収益性を保証するものではない。本資料は、現時点における暗号資産ステーキングサービスの一般的な実務およびリスク構造を整理したものであり、すべてのプロトコルやサービス形態を網羅するものではない。

特に、本資料では PoS 型ブロックチェーンのコンセンサス形成メカニズムの一部として組み込まれているステーキングを対象とする。ステーキング資産に対応するトークンを発行し流動性を確保する仕組み（いわゆる Liquid Staking）など、トークン化されたステーキングサービスも存在する。また、「ステーキング」という用語が用いられるものの、PoS 型ブロックチェーンのコンセンサスに関与しないトークンステーキングや DeFi ステーキングも存在する。これらは、DeFi 特有のサービス構造やトークン設計といった追加的な論点を含むため、本資料では詳細な整理の対象とはせず、今後の検討課題とする。

また、ブロックチェーンの技術仕様、市場環境および規制環境は今後も変化する可能性があるため、本資料の内容は将来的に見直しまたは更新が必要となる場合がある。各事業者においては、自らが提供するサービスの内容および対象となるブロックチェーンの特性を踏まえ、適切なリスク評価および運用体制の整備を行うことが望ましい。

本資料の構成として、目次 1〜4 ではステーキングサービスの定義、類型およびリスク等について、利用者にも理解しやすい一般的な説明を行う。続く 5〜9 では、ステーキングサービスを提供する事業者向けの内容を扱う。

2. 用語の定義

2-1. プルーフ・オブ・ステーク（PoS）

PoS とは、ブロックチェーンにおけるコンセンサスアルゴリズムの一つであり、参加者が一定量の暗号資産をステークすることでネットワークにおけるトランザクションの正当性検証やブロック生成に参加する仕組みを指す。PoS では、ステークする暗号資産の数量やプロトコルのルールに基づいてバリデータが選出され、トランザクションの検証やブロック生成を行う。正しく検証活動を行ったバリデータは報酬を得ることができる一方、プロトコル違反や不正行為が発生した場合にはスラッシング等のペナルティが課されることがある。

2-2. ステーキング／ステーク

ステーキング／ステークとは、PoS を実装するブロックチェーン（PoS 型ブロックチェーン）において、ネットワークのコンセンサス形成に参加するために暗号資産を一定期間ロックし、トランザクションの正当性検証やブロック生成への技術的貢献の対価として報酬を受け取る仕組みを指す。ネットワークの安全性と運営を維持するための重要な技術的メカニズムであり、PoS 型ブロックチェーンの基本的な構成要素の一つである。

2-3. バリデータ

バリデータとは、PoS 型ブロックチェーンにおいて、トランザクションの正当性を検証し、ブロック生成を行うノードを指す。バリデータは一定量の暗号資産をステークすることでネットワークのコンセンサスプロセスに参加し、適切な貢献を行うことで報酬を得ることができる。

2-4. ロック

ロックとは、暗号資産を特定のブロックチェーンプロトコル上で一定期間移動または売却できない状態にすることを指す。ステーキングに参加する際には、ネットワークの安全性を担保するため、暗号資産が一定期間ロックされる仕組みが採用されることが多い。

2-5. アンステーキング

アンステーキングとは、ステーキングされた暗号資産のロックを解除する手続きを指す。

2-6. ボンディング期間

ボンディング期間とは、ステーキングの手続きを開始した後、当該暗号資産が報酬を獲得し始めるまでの待機期間を指す。多くの PoS 型ブロックチェーンでは、ネットワークの安全性を維持するため、ステーキングの申請後も直ちにステーキングが有効化されるのではなく、プロトコルのルールに基づき一定の待機期間を設ける仕組みが採用されている。なお、当該待機期間中は、一般に暗号資産はロックされ、移転や売却はできない。

2-7. アンボンディング期間

アンボンディング期間とは、アンステーキングの手続きを行った後、ロックされた暗号資産を引き出すことができるようになるまでの待機期間を指す。多くの PoS 型ブロックチェーンでは、ネットワークの安全性を維持するため、アンステーキングの申請後直ちに移転や売却が可能となるのではなく、プロトコルのルールに基づき一定期間はロックが継続する仕組みが採用されている。当該期間中は暗号資産の移転や売却はできないことが一般的である。

2-8. カストディ

カストディとは、暗号資産の秘密鍵を事業者が管理し、暗号資産の保管や移転、関連する金銭の管理などの業務を行うサービスを指す。カストディでは、利用者は自ら秘密鍵を管理する必要がなく、事業者がこれを行う。

2-9. セルフカストディ

セルフカストディとは、利用者自身が暗号資産の秘密鍵を管理する形態を指す。セルフカストディでは第三者に秘密鍵管理を委託せず、利用者が自身の管理するウォレットを通じて暗号資産を管理する。

2-10. デリゲーション

デリゲーションとは、ステーキングによって得られるブロックチェーンのコンセンサスプロセスに参加するための権限（投票力）を、バリデータを運用する第三者に委任する仕組みを指す。デリゲーションにおいては、通常、暗号資産そのものの秘密鍵は委任先に移転せず、資産管理は委任者が引き続き行う。委任者は自らノードを運用することなく、バリデータにステークを委任することでステーキング報酬を得ることができる。

2-11. レンディング

レンディングとは、利用者が保有する暗号資産を事業者に貸与し、事業者がその暗号資産を運用することで、利用者が一定の報酬を得るサービスを指す。多くの場合、契約形態は消費貸借契約となり、事業者が秘密鍵を管理し、暗号資産の運用を行う。

2-12. スラッシング

スラッシングとは、バリデータがプロトコル違反を行った場合に課されるペナルティを指す。例えば二重署名や長時間のノード停止などが発生した場合、ステークされた暗号資産の一部が没収されることがある。

2-13. 二重署名

二重署名とは、同一のブロック高またはエポックにおいて、矛盾する二つのブロックや投票メッセージに対して同じバリデータが署名してしまう行為を指す。これはブロックチェーンのコンセンサスルールに対する重大な違反行為であり、多くの PoS ネットワークではスラッシングの対象となる。

2-14. ステーキングサービスプロバイダ（SSP）

SSP とは、利用者の委任に基づき、バリデータノードの運用、ステーキングに関する手続きの実行、報酬の管理・分配、運用状況の管理等のステーキング関連サービスを提供する事業者を指す。SSP は、カストディ型またはセルフカストディ型のいずれのサービス形態においても介在する可能性がある。

3. ステーキングサービスの類型

3-1. 類型整理の基本的な考え方

ステーキングサービスは、技術的には同一の PoS メカニズムを利用するものであっても、利用者資産の管理主体や契約構造によってリスク構造および規制上の位置付けが大きく異なる。そのため、本資料ではまずサービス構造の違いに着目して整理を行う。

具体的には、カストディ型とセルフカストディ型を基本的な類型として整理する。なお、カストディ型における利用者資産の分別管理や保全については、ステーキングサービスに特有の実務上の論点との関係に限定して整理する。また、本資料におけるカストディ型およびセルフカストディ型の区分は、主として利用者資産の管理主体および移転権限の所在に基づき整理する。

3-2. 関与事業者の整理

ブロックチェーンにバリデータとして直接参加するためには、一定量の暗号資産をステークする必要があるほか、ノードの運用や監視など高度な技術的運用能力が求められる。そのため、多くの利用者は自らノードを運用するのではなく、事業者を介してネットワークに参加する形態が一般的となっている。

このような構造の下ではステーキングの仕組みには、ブロックチェーンプロトコル、バリデータ運用事業者、SSP、カストディまたはセルフカストディのサービス提供者および利用者といった複数の主体が関与し、それぞれ異なる役割を担っている。なお、実務上はバリデータ運用事業者と SSP が同一の事業者である場合が多い。

3-3. 類型の区分

ステーキングサービスは、資産管理方法の違いに応じて、カストディ型とセルフカストディ型に分類できる。さらに、資産管理主体とは別に、契約形態の違いによってサービス形態が異なる場合もある。レンディングはステーキングの類型ではなく契約形態の一種で

あるものの、日本国内ではステーキングと対比して論じられることもあるため、本項でも取り上げる。

3-3-1. カストディ型

カストディ型は、暗号資産交換業者やカストディ事業者が秘密鍵の管理権限を有し、利用者に代わってステーキングを実施するモデルである。このモデルでは利用者は技術的な運用を行う必要がなく、サービス事業者のプラットフォームを通じて簡便にステーキングに参加することができる。一方で、秘密鍵の管理を事業者に委ねることになるため、管理不備や内部不正などにより資産が流出するリスクや、事業者の運用リスクが利用者に影響を与える可能性がある。

3-3-2. セルフカストディ型

セルフカストディ型は、利用者自身が管理するウォレットからステーキングを行うモデルである。秘密鍵は利用者自身が保持するため、資産管理に関する事業者リスクは相対的に低減されるが、利用者には一定の技術的理解が求められる。

なお、利用者が秘密鍵管理を維持したまま第三者が運用するバリデータへステーク権限を委任する形態は、一般にデリゲーション型と呼ばれることがある。このような形態もセルフカストディ型の一形態と位置付けられる。また、利用者自身がバリデータノードを運用する場合もセルフカストディ型に含まれる。

3-3-3. レンディング

レンディングでは、利用者が暗号資産を事業者に貸与し、事業者がその資産をステーキングなどに活用するモデルである。この場合、契約形態は消費貸借契約となることが多い。秘密鍵の管理はレンディング事業者が担う。

4. ステーキングに伴う主なリスク

4-1. リスクの全体像

ステーキングサービスには、ブロックチェーン技術の特性および事業者の運用体制に起因する複数のリスクが存在する。これらのリスクには、秘密鍵管理やスマートコントラクトに関する技術的リスク、プロトコル設計やガバナンスに関するリスク、トークンエコノミクスや市場価格に関する経済的リスク、ならびに事業者や外部委託先に起因する運用リスクなどが含まれる。

4-2. 各リスクの内容

4-2-1. 秘密鍵管理リスク

まず、秘密鍵管理に関するリスクがある。カストディ型サービスでは、利用者資産の管理が事業者に委ねられるため、不正アクセスや内部不正、管理体制の不備などにより秘密

鍵が流出した場合、利用者資産が失われる可能性がある。一方、セルフカストディ型では秘密鍵の管理が利用者自身に委ねられるため、秘密鍵の紛失や漏えい等に起因するリスクは主として利用者が負担することとなる。

4-2-2. スラッシングリスク

また、PoS 型ブロックチェーンでは、バリデータがプロトコル違反を行った場合や長時間ノードが停止した場合に、ステークされた暗号資産の一部が没収される「スラッシング」と呼ばれるペナルティが課される場合がある。バリデータの運用体制や技術的管理が不十分な場合、利用者のステーク資産にも影響が及ぶ可能性がある。

4-2-3. スマートコントラクトリスク

さらに、ステーキングに関連して利用されるスマートコントラクトやブロックチェーンプロトコル自体に脆弱性が存在する場合、資産の損失やサービスの停止等の影響が生じる可能性がある。特に、スマートコントラクトを用いた資産管理や報酬分配の仕組みに不備がある場合には、利用者資産やサービス運営に直接的な影響が及ぶ可能性がある。

4-2-4. プロトコルガバナンスリスク

そして、ネットワークの仕様や各種パラメータがガバナンスプロセスを通じて変更される場合がある。例えば、ステーキング報酬率、スラッシング条件、アンボンディング期間、バリデータ要件などが変更されることにより、ステーキングの経済条件や運用リスクが変化する可能性がある。また、ネットワークのアップグレードやハードフォークにより、ステーキングの運用方法や技術仕様が変更される場合もある。このため、事業者は対象となるブロックチェーンのガバナンス構造やアップグレードプロセスを把握し、これらの変更がサービス運営に与える影響について継続的に評価することが望ましい。

4-2-5. バリデータ集中化リスク

現在、Ethereum ステーキングなどで見られる現象として、特定のバリデータやステーキングサービスプロバイダにステークが集中することにより、ネットワークの分散性が低下する可能性がある。特定の事業者にステークが過度に集中した場合、当該事業者がステーク運用に関して十分な分散性やセキュリティ、冗長性を確保していない場合には、当該事業者の障害や運用不備がネットワーク全体の安定性に影響を与える可能性があるほか、ガバナンス投票等における影響力が偏在する可能性もある。このため、事業者は対象となるブロックチェーンにおけるバリデータ構成やステークの分布状況を把握し、集中度がサービス運営やネットワークの健全性に与える影響について考慮することが望ましい。

4-2-6. 報酬設計リスク（トークンエコノミクス）

さらに、PoS 型ブロックチェーンにおけるステーキング報酬は、ネットワークのトーク

ンエコノミクスおよびプロトコル設計に基づいて決定される。報酬率はネットワーク参加者数、ステーク総量、インフレーション設計、報酬分配ルール等により変動する可能性があり、将来的な報酬水準が保証されるものではない。また、プロトコル仕様の変更や市場環境の変化により、期待される報酬水準が変動する可能性もある。ステーキング報酬は、暗号資産ネットワークのプロトコル設計およびネットワーク参加状況等に基づき決定されるものであり、事業者が報酬水準を保証するものではない。このため、事業者はステーキング報酬の変動要因や報酬設計の仕組みについて十分に理解するとともに、利用者に対して適切な説明を行うことが重要である。

4-2-7. 価格変動リスク

加えて、暗号資産市場の価格は大きく変動する可能性があり、ステーキングによって得られる報酬が価格下落によって相殺される可能性がある。

4-2-8. 流動性リスク

また、多くの PoS 型ブロックチェーンでは暗号資産がボンディング期間、ステーキング期間、およびアンボンディング期間にわたりロックされる仕組みが採用されており、これらの期間中は資産の売却や移転が制限される場合がある。このため、利用者資産の流動性が制約される可能性がある。

4-2-9. カウンターパーティリスク

さらに、ステーキングサービスの提供にあたり、外部のバリデータ運用事業者、インフラプロバイダー、ウォレット事業者等を利用している場合には、これらの事業者の運用体制や信用状況に依存するリスクも存在する。外部事業者においてシステム障害、運用不備、セキュリティインシデント等が発生した場合、サービス提供や資産管理に影響が及ぶ可能性があるため、事業者はこれらのリスクを適切に管理する必要がある。

5. 運用要件・緊急時対応

5-1. 基本的な考え方

ステーキングサービスの信頼性は、技術運用体制の水準に大きく依存する。そのため、事業者はバリデータノードの運用、鍵管理、監視体制およびセキュリティ対策について、適切な技術的要件を整備するべきであり、基本運用としては各ブロックチェーンの公開されている技術仕様や推奨事項等を参考に運用するべきである。

5-2. 運用体制の整備

5-2-1. バリデータノードの安定運用

また、24 時間体制での監視および迅速な障害対応が可能な体制を整備する必要がある。ノードの稼働状況やネットワークパフォーマンスを常時監視し、異常が検知された場合に

は運用担当者に通知される仕組みを整備するべきである。また、ノード停止によるスラッシングリスクを低減するため、遠隔署名クライアント（Remote Signer）またはブロックチェーンノード自体の冗長化を行い、署名クライアントのフェイルオーバー構成やバックアップノードを整備することが有効である。また、スラッシングリスクの低減のためには、スラッシング条件への抵触を防止するための専用のソフトウェアおよび運用手法を用いてインフラを構築・管理することが有効である。

5-2-2. 秘密鍵および署名鍵の適切な管理

秘密鍵管理については、セキュリティ確保の観点から極めて重要である。特に、暗号資産を管理するための秘密鍵と、ブロックチェーンのコンセンサスに参加するための署名鍵（Validator Key）は役割が異なるため、それぞれを適切に区別したうえで管理する必要がある。ステーキングサービスの類型（カストディ型、セルフカストディ型、デリゲーション型等）に応じて、これらの鍵の管理方法を適切に設計するべきである。秘密鍵の管理にはハードウェアセキュリティモジュール（HSM）やマルチパーティ計算（MPC）などの高度な暗号技術を利用することが推奨される。また、秘密鍵および署名鍵へのアクセス権限は厳格に管理し、アクセスログを記録し監査可能な状態を維持する必要がある。

5-2-3. スラッシング防止対策

モニタリング体制については、ノードの稼働状況、ネットワーク接続状況、報酬獲得状況、スラッシングリスク等を継続的に監視する体制を整備するべきである。

5-2-4. セキュリティ対策

セキュリティ対策としては、定期的な脆弱性診断およびセキュリティレビューを実施するべきである。また、ブロックチェーンノードソフトウェアや関連ミドルウェアについては、脆弱性情報やプロトコル更新に迅速に対応できるよう、ソフトウェア更新体制を整備する必要がある。さらに、インフラストラクチャの管理においては、設定変更やソフトウェア更新等の変更履歴を管理する仕組みを整備し、適用履歴を追跡できる状態を維持するべきである。これにより、障害発生時の原因分析やセキュリティインシデントへの対応を迅速に行うことが可能となる。

5-2-5. 外部委託先の管理

また、ステーキング運用の一部を外部事業者へ再委託または業務委託する場合には、再委託先または業務委託先に対して、自社が求めるセキュリティ・運用基準の遵守状況を確認し、必要に応じて契約上の統制や監査権限を確保するべきである。

5-3. 緊急時対応と事業継続性

ステーキングサービスを安定的に提供するためには、インシデント発生時の対応体制お

よび事業継続計画（BCP）の整備が不可欠である。

事業者は、ノード障害、ネットワーク障害、サイバー攻撃などのインシデントを想定し、障害検知から復旧までの手順を事前に定義する必要がある。また、重大なインシデントが発生した場合には、利用者に対して適切な情報提供を行う体制を整備することが求められる。さらに、災害や大規模システム障害に備え、データバックアップ、フェイルオーバー構成、ディザスタリカバリサイトの整備などを行うことが望ましい。

6. 情報開示・説明責任

6-1. 基本的な考え方

ステーキングサービスを提供する事業者は、利用者がサービス内容やリスクを適切に理解したうえで意思決定を行えるよう、十分な情報開示および説明を行うことが求められる。

6-2. 開示事項

6-2-1. 運用スキーム・収益源の開示

各事業者は、顧客との契約形態および運用スキームについて明確に開示する必要がある。例えば、顧客資産の運用契約であるのか、あるいは消費貸借契約に基づくサービスであるのかといった契約形態を明示することが重要である。

また、秘密鍵管理の方法についても、カストディ型サービスであるのか、またはセルフカストディ型サービスであるのかといった資産管理の形態については、利用者のリスク判断に大きく影響するため、明確に説明する必要がある。

外部のレンディング事業者やウォレット事業者などのサードパーティーを利用している場合には、その事業者の役割やセキュリティ認証、監査の有無についても開示することが望ましい。さらに、ステーキングサービスプロバイダ（SSP）においては、法人名や組織体制、運用体制、関連する認証、運用メンバーの経験や専門性などについても開示し、運用体制の透明性を確保することが重要である。

6-2-2. 月次運用レポート

事業者は、利用者に対して定期的に運用状況を報告することが望ましい。月次レポートなどの形で、ステーキング報酬の実績やスラッシングの発生有無、運用パフォーマンスなどを開示することにより、利用者がサービスの実績やリスクを継続的に把握できるようにすることが重要である。また、顧客向けの運用手数料や、手数料控除前後の数値を明確に区別して表示することが望ましい。加えて、過去のパフォーマンスの推移や、運用アーキテクチャに変更があった場合の報告などを行うことで、サービス運営の透明性を高めることができる。

6-2-3. 報酬水準表示の明確化

利用者に対して、運用手数料やその他の関連費用について明確に説明することが重要で

ある。また、ステーキング報酬が税務上どのように取り扱われる可能性があるかについて、一般的な説明を提供することも望ましい。ただし、具体的な税務上の取扱いは個別の事情に左右されるため、必要に応じて税理士等の専門家への相談が必要となる旨も併せて示すことが適切である。

6-2-4. リスク開示

事業者は、ステーキングサービスに伴うリスクについて利用者に対して十分に説明する必要がある。具体的には、スラッシングリスク、システム停止リスク、運用上のリスクなど、サービス利用に影響を与える可能性のあるリスクを明確に開示することが重要である。また、これらのリスクに対して事業者がどのような対策を講じているかについても説明することで、利用者がサービスの安全性やリスク管理体制を理解できるようにすることが望ましい。

6-2-5. ロック期間・アンボンディング期間の開示

ステーキングサービスにおいては、暗号資産が一定期間ロックされることに加え、ステーキングおよびアンステーキング申請後、それぞれステーキングが有効化されるまでの待機期間（ボンディング期間）および資産が引き出し可能となるまでの待機期間（アンボンディング期間）が存在する場合が多い。このため、事業者は利用者に対して、ステーキングに伴うボンディング期間およびアンボンディング期間について明確に開示する必要がある。

特に、アンステーキングの申請から実際に資産が引き出し可能となるまでのアンボンディング期間や、当該期間中に資産の売却や移転ができない可能性について、事前に説明することが重要である。また、ブロックチェーンごとにロック期間やアンボンディング期間が異なる場合には、その違いについても利用者が理解できる形で提示することが望ましい。

これらの情報を適切に開示することにより、利用者がステーキングサービスの流動性制約を十分に理解したうえで利用判断を行うことが可能となり、報酬水準の高さのみを強調した誤認や過度な期待を防止することにつながる。

7. コンプライアンス

7-1. 基本的な考え方

ステーキングサービスを適切に運営するためには、業務運営とリスク管理を分離した実効的なコンプライアンス体制を構築することが重要である。そのため、事業者は三線ディフェンス（Three Lines of Defense）モデルに基づき、事業部門、コンプライアンス・リスク管理部門、および内部監査部門からなる管理体制を整備するべきである。

7-2. 三線ディフェンスモデル

7-2-1. 第 1 線

第 1 線は事業部門であり、ステーキング業務を直接実施する部門が、バリデータノードの稼働状況、報酬管理、報酬算定、顧客資産の取り扱いなどに関する日常的なリスク管理を担う。

7-2-2. 第 2 線

第 2 線はコンプライアンスおよびリスク管理部門であり、業務プロセスが適切に設計・運用されているかを監督する役割を担う。具体的には、ステーキング報酬算定ロジックやルール設定の妥当性確認、運用上の逸脱の検知、内部不正リスクの監視、KYC/AML に関するチェックなどを実施する。また、スマートコントラクトやバリデータノード運用に関するオペレーショナルリスクについても評価を行う必要がある。

7-2-3. 第 3 線

第 3 線は内部監査部門であり、第 1 線および第 2 線の統制が適切に機能しているかを独立した立場から監査する役割を担う。監査においては、ステーキング報酬の分配の正確性、顧客資産管理の適正性、バリデータのダウンタイムやスラッシングリスクへの対応状況などについて確認を行う。内部監査部門は業務部門から独立した組織として設置され、経営陣に対して直接報告を行う体制を整備するべきである。

7-3. 内部監査および記録管理

また、年次監査計画を策定し、ステーキング関連業務プロセス、報酬管理、顧客資産の分別管理などを監査項目として明確にする必要がある。さらに、バリデータノード運用、ノードソフトウェアの更新、スマートコントラクトの変更管理などの IT 運用プロセスについても監査対象とすることが望ましい。加えて、ステーキング報酬計算や流動性状況などのログや記録について、証跡の保全および再現可能性を確保する仕組みを整備する必要がある。

7-4. AML/CFT・トラベルルール対応

さらに、暗号資産関連サービスを提供する事業者は、AML/CFT およびトラベルルール対応の観点から、ウォレットアドレスに対するスクリーニング体制や取引モニタリング体制を整備する必要がある。具体的には、OFAC 等の制裁リストに掲載されたアドレスとの照合を行い、不正取引や制裁対象者との取引を防止する仕組みを導入することが求められる。また、トランザクションのリスク評価を通じて、不審な取引の検知および適切な対応を行う体制を整備することが重要である。加えて、トラベルルールの適用が求められる場合には、送受信者に関する必要情報を取得、管理および提供できる体制を整備することが望ましい。

8. 外部監査

8-1. 基本的な考え方

ステーキングサービスの信頼性および透明性を高めるためには、事業者内部の統制だけでなく、独立した第三者による保証や監査を活用することが重要である。外部監査は、サービスのセキュリティ、可用性、処理の完全性、情報開示の信頼性などについて客観的な確認を行う手段であり、利用者保護および事業運営の健全性を示すうえで有効である。特に、外部ベンダーや外部インフラに依存するサービス設計を採用している場合には、第三者による検証を通じて、統制状況を継続的に確認することが重要となる。

8-2. 外部監査の内容

8-2-1. 保証報告書の取得

SOC1/SOC2 や ISO27001 などの保証報告書・認証は、外部事業者または自社の統制状況を確認する手段として有効である。例えば、秘密鍵管理や資産移転に関する権限を外部ベンダーが保有する場合には、セキュリティ統制の有効性を確認する必要がある。また、バリデータの稼働要件を満たせないことによってスラッシングが発生する可能性がある場合には、可用性に関する保証が重要となる。さらに、預かり残高やステーキング報酬など、利用者への開示情報の正確性や信頼性が重要となる場合には、情報処理統制の観点からも保証報告書の確認が有効である。

8-2-2. スマートコントラクト監査

ステーキングサービスにスマートコントラクトを利用している場合には、スマートコントラクト監査を実施することが重要である。資産管理や報酬分配、ロック・アンロック処理などをスマートコントラクトに依存する場合、その設計やコードの不備が直接的に利用者資産やサービス運営へ影響を及ぼし得るためである。このため、スマートコントラクトの種類、利用目的、影響範囲に応じて、専門のブロックチェーン監査企業によるコードレビューやセキュリティ監査を受け、潜在的な脆弱性や設計上のリスクを把握することが望ましい。

8-2-3. ノード運用体制の外部評価

また、必要に応じて、バリデータノードの運用体制や関連システムについても外部専門機関による技術評価を受けることで、運用体制全体の信頼性を客観的に確認することができる。

8-2-4. ブロックチェーン関連システムのリスク評価

さらに、プライベートチェーン又は運営主体が主要なパラメータ変更権限を有するブロックチェーンを用いる場合には、当該運営主体の統制体制についても確認する必要がある。なお、ブロックチェーン自体の信頼性については、暗号資産が取引所等に上場する際の審

査プロセスにおいて一定の評価が行われている場合もあるが、サービスとして利用する際には、個別の運用リスクについて改めて確認することが重要である。

9. 税務・会計

9-1. 基本的な考え方

暗号資産に係る会計処理については、企業会計基準委員会が公表している実務対応報告第 38 号「資金決済法における暗号資産の会計処理等に関する当面の取扱い」において、暗号資産の保有および売買に関する基本的な取扱いが示されている。他方で、ステーキングについては、本実務対応報告の対象には含まれておらず、現時点ではステーキングに係る固有の会計処理に関する統一的な会計基準は存在していない。

そのため、ステーキングに関する会計処理は、関連する会計基準等の定めが明らかでない場合として、各企業において、提供するサービスの内容、契約条件、対象となるブロックチェーンの仕様その他の取引実態を踏まえ、合理的な会計方針を定める必要がある。例えば、ステーキングにより生じる報酬（以下、ステーキング報酬）については、実務上は、企業会計基準第 29 号「収益認識に関する会計基準」（以下、収益認識会計基準）を参考として、ステーキング報酬の収益認識方法を検討している例があると認識されている。

9-2. 会計上の主要論点

以下では、バリデータノードの運用や、第三者に対するノード運用の委任（デリゲーション）等で利用者にステーキングサービスを提供する事業者を前提に、主にステーキング報酬について、収益認識会計基準を参考に会計処理を検討した場合に想定される主要な論点について記載している。

9-2-1. 契約関係および履行義務の整理

ステーキング報酬の会計処理を検討するにあたっては、まず、ステーキングサービスを提供する事業者が誰に対してどのようなサービスを提供しているのかを整理する必要がある。書面による契約に加えて、プロトコルの仕様、ホワイトペーパー、サービス約款等によって権利義務関係が定まる場合があるため、形式面のみではなく実態面からの検討が重要となる。

また、事業者が自らバリデータノードを運用しているのか、バリデータに対するデリゲーションなのか、あるいは利用者から暗号資産を預かって報酬の付与まで行う包括的なサービスを提供しているのかによって、誰が顧客に該当するかや、履行義務の内容等が異なる可能性がある。単なる資産の預かりにとどまるのか、ステーキングの実行や報酬分配まで含むのか、履行義務が単一か複数かを含めて、契約内容および取引実態に即して整理することが必要となると考えられる。

9-2-2. 本人取引・代理人取引の判定

収益認識会計基準を参考にする場合、ステーキングを本人取引として会計処理するか、代理人取引として会計処理するかが論点となる可能性がある。

例えば、自らバリデータノードを運用する事業者、すなわちバリデータについては、委任を受けた利用者の暗号資産を自己ノードにステーキングする場合に、ステーキング報酬のうち利用者に帰属する部分とバリデータ自身の報酬を区分し、本人取引か代理人取引のいずれに該当するかの検討が必要となる可能性がある。

また、暗号資産交換業者等が利用者の暗号資産を用いてステーキングサービスを提供する場合（SSP を利用する場合を含む）においても、利用者に対する役務が単なる預かりか、ステーキング実行・報酬受領・利用者への付与まで含む包括的サービスかを見極めたうえで、受領したステーキング報酬を利用者帰属分と自社の手数料等に区分し、本人取引か代理人取引のいずれに該当するかの検討が必要となる可能性がある。

本人取引か代理人取引かの判定にあたっては、契約条項のみならず、分別管理の有無、事業者の裁量の範囲、スラッシングが起きた場合の取り扱い等を含む経済的なリスクと便益の帰属関係などを総合的に考慮する必要がある。

9-2-3. 収益認識のタイミング

次に、ステーキング報酬をいつ収益として認識するかも論点となりうる。例えば、バリデータを前提とする場合、ブロックチェーンの設計やサービス条件によっては、バリデータとして検証・承認行為を行った時点、ブロックチェーン上で報酬が発生した時点、事業者が報酬を受領した時点、あるいは利用者への分配額が確定した時点など、複数の候補時点が考えられる。さらに、一定期間ごとに報酬が集計・算定される設計である場合には、一時点で認識すべきか、一定期間にわたり認識すべきかも論点となる可能性がある。

したがって、収益認識時点の判断にあたっては、対象ネットワークの報酬発生メカニズム、ロックアップやアンステークの条件、報酬分配に関する契約上の定め、実際の運用フロー等を踏まえ、履行義務の充足時期を慎重に検討する必要がある。

これらの論点については、事業者が提供するステーキングサービスの内容や、対象となるブロックチェーンの特性に応じて、事実関係を丁寧に整理したうえで会計基準への当てはめを検討することが求められる。最終的な会計処理の判断にあたっては、監査法人または公認会計士と十分に協議し、契約内容、実態、実務運用を踏まえた適切な会計方針を定めることが望ましい。

9-3. 税務上の取扱い

また、国税庁が公表している「暗号資産等に関する税務上の取扱いについて（FAQ）」（令和 7 年 12 月 26 日）によれば、ステーキング等により暗号資産を取得した場合には、その取得時点における時価が収入金額（法人税の場合は益金）として計上されるとされている。