Emerging Technology:

Using crypto and digital assets? 6 risks to consider when selecting a provider

暗号通貨・デジタル資産サービスプロバイダーの選定で考慮すべき 6 つのリスク

2022 年 12 月

PwC コンサルティング合同会社
PwC Intelligence　ディレクター　小林 峰司

イントロダクション

サマリー:

- **ビジネスリーダーは、特にデジタル資産に対して、サービスプロバイダーの選定や現行のオペレーションを監視する際のリスクを考慮しなければならない**
- **鍵となるリスクとして、オペレーション（運用）、テクノロジー、カストディおよびセキュリティ、マーケットアクセスおよびデータ、機密保持およびプライバシー、コンプライアンスおよび税務、の 6 つが含まれる**
- **SOC レポート（System and Organization Control report: 受託業務における内部統制状況を保証するための報告書）は、既に選定済みのデジタル資産サービスプロバイダーに対するリスク評価を支援するための有力なツールになり得る**
- **SOC1 は、財務報告に関する内部統制に特化**
- **SOC2 は、セキュリティ、可用性、機密保持、プロセスのインテグリティ、プライバシーに関する内部統制に特化**

暗号資産市場における昨今の混乱は、デジタル資産への投資や関与における重大なリスクを浮き彫りにしている。

暗号通貨や NFT（Non-fungible Token: 非代替性トークン）などのデジタル資産に投資や関与を行う場合、リスクの把握が重要であり、これには下記に該当するデジタル資産サービスプロバイダーに関連するリスクも含まれる。

- カストディ（ウォレットサービスなど、デジタル資産を管理・保管する業務）
- 取引所
- データソース（データの格納場所）
- インフラ提供事業者

加えて、これらのリスクが、自社ビジネスにおけるステークホルダーの信頼に与える影響を考慮すべきである。

Here are six key risks that you may consider when selecting a digital asset service provider – デジタル資産サービスプロバイダー選定において考慮すべき 6 つのリスク

1. オペレーショナルリスク（運用上のリスク）

自身がデジタル資産サービスプロバイダーにより提供されるサービスを理解しているか。かつ、そのプロバイダーが、関連するリスクを低減すべく堅牢な管理を行っているかどうかを理解しているか。関連する運用上のリスクの種類は、デジタル資産への投資アプローチやビジネスモデルによって異なる。いくつか例を挙げると、直接投資かどうか、先物取引かどうか、あるいは収入を得るためにデジタル資産をステーキング（保有している暗号資産に対し報酬を受け取ること）しているかどうか、といったことが挙げられる。また、運用上のリスクの例として、不正な取引活動、不正確もしくは不完全な帳簿や記録、カストディまたは（および）個々のブロックチェーンと一致しないデジタル資産の保有、といったことが含まれる。

2. テクノロジー

カストディ、レポーティング、調整（reconciliations）、その他デジタル資産のアクティビティといったサービスを提供するために、サービスプロバイダーが導入しているテクノロジーが信頼に値するものか。テクノロジーリスクには、重要なシステムに対する不適切もしくは許可されていない物理／論理アクセス、システムエラーの原因となる変更管理アクティビティ、極めて厳しい市場状況下で無力なレジリエンス（システムエラーからの回復力）、といったものが含まれる。

3. カストディとセキュリティ

資産保護のためにどのような管理が行われているか。ブロックチェーンベースの取引は取り消しできないため、ウォレットがセキュリティ侵害を受けた場合、デジタル資産は永久に失われる可能性がある。サービスプロバイダーは、オンボーディング、入出金、調整（reconciliation）といった従前からあるカストディ（ウォレット）機能だけでなく、秘密鍵のライフサイクルにおけるあらゆる段階――秘密鍵の生成から、配布、保管、セキュリティ、使用、ローテーション、破棄まで――を確実に管理する必要がある。

4. マーケットアクセスおよびデータ

市場が混乱している状況でも、戦略を実行することができるか。それぞれの分散型取引所とブロックチェーンを個別に接続するのか。それともインフラ提供事業者を活用し、集約してワンストップ・ショップとするのか。市場データと流動性を維持するためにも、サービスプロバイダーにて実施されている管理について理解する必要がある。

5. 機密保持およびプライバシー

ビジネスにおける詳細情報や個人情報といった機密情報は保護されるか。機密性とプライバシーの維持は、提供されるサービスにおける信頼を築き、ステークホルダーの期待に応える上での基礎となる。

6. コンプライアンスおよび税務

金融業界におけるスタンダードや規制――AML（アンチマネーロンダリング）や KYC（Know Your Customer: 本人確認手続き）など――を遵守するために、かつ／あるいは、納税申告の義務を果たすために、サービスプロバイダーはどのようなサービスやレポーティングを提供しているか。

Who’s responsible? Read the contract first – 責任の所在を明確に

どのデジタル資産サービスプロバイダーであっても、契約上の合意を確認の上で、義務と誰が何に対して責任を負うのかを正しく把握することが重要である。このことは、常に変化し続けるだけでなく、あらゆる曖昧さが潜在的にリスク管理を低下させ得るデジタル資産領域については、特に当てはまる。

Bridging the knowledge gap – 知識ギャップを埋める

幸運なことに、アセスメントの一助となる強力なツールとして、SOC（System and Organization Control）レポートがある。SOC1 レポートは財務報告書や財務諸表監査に関する内部統制の監査に最も有用であり、SOC2 レポートはトラストサービス原則をカバーし、セキュリティ、可用性、機密保持、プロセスのインテグリティ、プライバシーが含まれる。いずれもサービスプロバイダーの内部統制状況を理解する上で役立つ。

SOC レポートによって、透明性が高まるほか、ミスコミュニケーションや責任の所在に対する誤解により生じるリスクを軽減することができる。また、SOC レポートは CUECs（Complementary User Entity Controls: 相互補完的な内部統制）のリストを含んでいて、これにより責任の所在が明確となる。このリストは自らの義務ならびにデジタル資産サービスプロバイダーの責任に対する理解を補完し得る（ただし、完全に置き換えるものではない）。

SOC2 レポート（サービスコミットメントに関連するもの）では、従来 SOC1 でカバーしきれなかった、機密保持やプライバシー、可用性といった領域に関するシステム、プロセスおよび管理についての洞察を得られる。

また、SOC レポートでは、関連するサブサービス組織と補完的なサブサービス組織が実施すべき管理が開示されることから、取引先や第四者（フォースパーティー）による使用および失敗にさらされる可能性を特定することができる。

How to assess SOC reports – SOC レポートの評価方法

デジタル資産における業界標準が欠如していることは、現在の SOC レポートにも当てはまる。この領域は成長分野であることから、デジタル資産の発行主が誰なのか、そしてデジタル資産が保有しているものが何か、といった面において、一貫性が欠如している。デジタル資産の顧客は、受領した SOC レポートを評価するためにも、レポート

が取り扱う範囲（dimensions）について、サービスプロバイダーに質問することを検討すべきである。サービスプロバイダーは、これらの範囲（dimensions）に対処し、顧客の質問に回答することで、SOC レポートが顧客のニーズを満たしているかの判断に役立てることができる。

- **Type: どのような種類のレポートが存在しているか？**

  デジタル資産サービスプロバイダーにとって一般的な方法は、財務報告に関する内部統制に特化した SOC1 と、セキュリティ、可用性、機密保持、プロセスのインテグリティ、プライバシーに関する内部統制に特化した SOC2 の双方を発行することである。選定候補となるデジタル資産サービスプロバイダーのレポーティング能力に加え、レポートが顧客のニーズを満たすのに十分な詳細情報を提供可能かどうか、確実に理解すべきである。

- **Scope: SOC レポートが取り扱う範囲は適正か？**

  入手可能な SOC レポートは、重要なサービス、事業体（entities）、法域（jurisdictions）を網羅しているか。多くのデジタル資産サービスプロバイダーは、複数の法域で事業を運営するとともに、複数の事業体やサービスを保有している（e.g. プライム・ブローカレッジ取引業務に加えて、コールドウォレットサービスを提供する、など）。したがって、必要となる特定サービスを SOC レポートがカバーしていない可能性があるため、どの事業体・サービス・資産がレポートの範囲に入っているかを確実に理解すべきである。

- **Outsourcing: SOC レポートには、デジタル資産サービスプロバイダーの請負ベンダーに対する管理が示されているか？**

  ほとんどのデジタル資産サービスプロバイダーは、SaaS（Software-as-a-Service）プラットフォームや物理セキュリティ／ストレージといった領域にて、請負ベンダーを利用している。この構造により、サードパーティー（もしくはフォースパーティー）が有するオペレーション、テクノロジー、コンプライアンスのリスクに辿り着く可能性がある。SOC レポートは、これらのサードパーティーおよびフォースパーティに関連するリスクを把握するほか、アウトソースされたサービス全体を網羅すべく、これらの請負ベンダーごとにレポートを個別に取得する必要があるかどうかを理解するのにも役立つ。

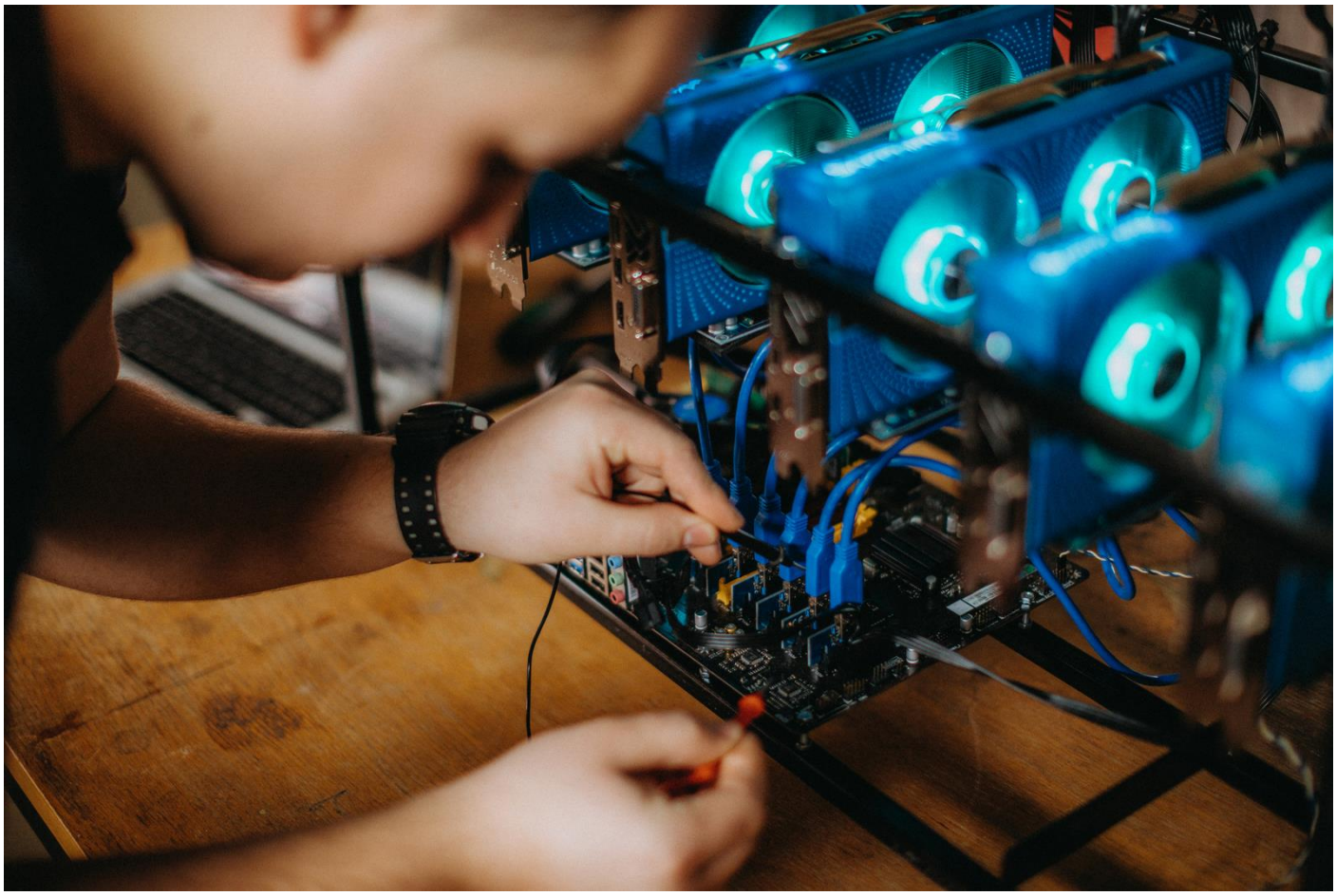
- **Completeness: SOC レポートは、顧客にとって最も重要なアクティビティを網羅しているか？**

  デジタル資産における業界標準の欠如を考慮すると、SOC レポートが取り扱う範囲はプロバイダーにより異なる傾向がある。例えばデジタル資産カストディの SOC レポートを見る場合、エコシステムのセキュリティにとって基本的かつ重要となる、秘密鍵のライフサイクル全体（鍵生成を含む）の管理に関する詳細を必ず確認すべきである。鍵生成のコントロールに欠陥があったり、独立した監査人によってテストされていなかったりすると、顧客のデジタル資産における脆弱性がより高まるためである。

Insights to domestic market – 日本市場に対する示唆

デジタル資産（暗号資産）を記録・管理するためのブロックチェーン。高い改ざん耐性・可用性・追跡可能性といった技術メリットを有する一方で、ブロックチェーンへの取引情報が不正確もしくは不完全な入力、あるいはデジタル資産（暗号資産）の所有者であることを実証するために必要な「秘密鍵」の不適切な管理・保管に起因する不正など、システム全体として信頼性を担保できなくなるリスクがある。

企業がブロックチェーンを活用する際、もしくは暗号通貨・デジタル資産サービスプロバイダーを外部委託先とする際には、運用面や技術・セキュリティ面でのリスク評価に加えて、委託先の内部統制状況を可能な限り理解した上で、信頼性・リスクを適正に評価することが求められる。デジタル資産サービスプロバイダーはグローバルプレイヤーであり、そのほとんどは日本国外に本社があるだけでなく、日本法人を含めた関連現地法人や、M&A によるグループ会社などがグローバルかつ複雑に結びついているケースが多い。したがって、（SOC1 の主題である財務報告に関連する内部統制状況の把握も含めて）SOC は有用となり得るものの、これを有力なツールとして活用するためには、グローバル全体での複雑な事業状況や SOC レポートのスコープといった現状を正確に把握した上で、整備・運用状況を適切に評価していく必要があると考えられる。



小林 峰司 | Takashi Kobayashi

ディレクター
エマージングテクノロジー
PwC Intelligence

PwC コンサルティング合同会社

〒100-0004　東京都千代田区大手町 1-2-1 Otemachi One タワー　Tel：03-6257-0700