仮想通貨シリーズ（7）

業種別委員会実務指針第61号「仮想通貨交換業者の財務諸表監査に関する実務指針」の解説③

公認会計士　佐瀬（させ）　剛（たけし）

日本公認会計士協会（業種別委員会）は、2018年6月29日に業種別委員会実務指針第61号「仮想通貨交換業者の財務諸表監査に関する実務指針」（以下「本実務指針」という。）を公表している。

本稿では、解説①（本誌2018年11月号（Vol.507））、②（本誌2019年2月号（Vol.510））に続き、本実務指針を解説する。下記目次のとおり、「6 企業及び企業環境の理解と重要な虚偽表示リスクの評価」の「(3)内部統制の理解」を取り上げる。

目　次			
解説①	1	はじめに	
	2	適用範囲	
	3	仮想通貨交換業者の財務諸表監査における特質	
	4	監査契約の締結	
	5	監査チームの選任	
解説②	6	企業及び企業環境の理解と重要な虚偽表示リスクの評価	(1)仮想通貨交換業者の事業上のリスク等の理解 (2)仮想通貨交換業者に特有のアサーション・レベルの重要な虚偽表示リスク
解説③（本号）			(3)内部統制の理解
			(4)特別な検討を必要とするリスク
解説④	7	リスク対応手続	
	8	適用時期	

（全3回から全4回に変更している）

6　企業及び企業環境の理解と重要な虚偽表示リスクの評価

(3)　内部統制の理解

監査基準委員会報告書315「企業及び企業環境の理解を通じた重要な虚偽表示リスクの識別と評価」（以下「監基報315」という。）11項により、監査人は監査に関連する内部統制を理解することが求められている。仮想通貨交換業者における監査に関連する内部統制の理解においては、仮想通貨交換業者特有の内部統制を理解するとともに、取り扱う仮想通貨の種類ごとにその技術的特徴、アドレスの管理方法など仮想通貨の全般的な管理及び保有状況を理解することが重要であるとされている（本実務指針17項）。

本実務指針18項では、各仮想通貨の技術的特徴を理解するためには、十分な知識と経験を有する専門家の業務を利用することがあり、また、デリバティブ取引を行う仮想通貨交換業者においては、必要に応じてデリバティブ取引について十分な知識と経験を有する者に監査業務を担当させることもあるとされているが、仮想通貨やITに精通した専門家の関与は必須であろう。

仮想通貨交換業者において想定される内部統制の具体例は本実務指針の付録２にまとめられており、図表1として掲げている。

図表1　付録２ 仮想通貨交換業者において想定される内部統制の例示

仮想通貨交換業者において想定される具体的な内部統制の例は次のとおりである。

内部統制の例	関連する業務プロセス（筆者が追加）
(1) アドレス及び暗号鍵の生成に関する内部統制 仮想通貨交換業者が生成した全てのアドレス及び暗号鍵が、自己用・利用者用を区分した形でアドレス管理簿及び暗号鍵管理簿に記録されることを担保する内部統制	①アドレス生成
(2) 口座開設時における本人確認を含む利用者管理簿への登録に係る内部統制 例えば、登録内容としては、利用者ID、預金口座、受取アドレスなどが考えられる。 ① 取引時確認等の措置に関する内部統制 具体的には、仮想通貨交換業者の業務に関して、取引時確認等の措置を的確に実施し、テロ資金供与やマネー・ローンダリングといった組織犯罪等に利用されることを防止するための態勢（ガイドラインⅡ－２－１－２－２） ② 反社会的勢力との関係遮断を図るための内部統制 具体的には、反社会的勢力と一切の関係を持たないようにする態勢、関係を有してしまった場合に可能な限り速やかに関係を解消するための態勢、また反社会的勢力による不当要求に適切に対応するための態勢（ガイドラインⅡ－２－１－３－２）	②口座開設
(3) 利用者が預託した金銭及び仮想通貨を適切に分別管理するための内部統制（ガイドラインⅡ－２－２－２－２(1)①②） ① 分別管理に係る社内規則に、金銭・仮想通貨それぞれについて、分別管理の執行方法を具体的に定め、利用者との契約に反映させている。 ② 自己の固有財産である金銭・仮想通貨と、利用者が預託した金銭・仮想通貨が、上記の執行方法に基づいて明確に区分され、かつ、個々の利用者の持分について、直ちに判別できることとしている。また、その遵守状況について適切に検証することとしている。 なお、実務対応報告第３項において対象外となっている自己（自己の関係会社を含む。）の発行した資金決済法に規定する仮想通貨についても、分別管理の対象となることに留意する。	③仮想通貨の管理（金銭及び仮想通貨の分別管理）
(4) 利用者からの仮想通貨の受入れ及び利用者への引出しの事実が、ブロックチェーン等の記録上の有高と一致していることを確保するための以下を含む内部統制（ガイドラインⅡ－２－２－２－２(1)③） ① 利用者の仮想通貨の管理について、仮想通貨交換業者が管理する帳簿上の利用者財産の残高と、ブロックチェーン等のネットワーク上の利用者財産の有高を毎営業日照合している。 ② 照合した結果、利用者財産の有高が帳簿上の利用者財産の残高に満たない場合には、原因の分析を行った上、当該不足額に関しては、不足が生じた日の翌日から起算して５営業日以内に当該不足額を解消している。	③仮想通貨の管理（仮想通貨の分別管理）
(5) 利用者からの金銭について自己分と区分して管理するための以下を含む内部統制（ガイドラインⅡ－２－２－２－２(1)④⑤） ① 利用者の金銭の管理について、内閣府令第20条第１項第１号に規定する方法により管理する場合、仮想通貨交換業者が管理する帳簿上の利用者財産の残高と、利用者財産を分別管理している銀行等の口座残高を毎営業日照合している。 照合した結果、銀行等の口座残高が帳簿上の利用者財産の残高に満たない場合には、原因の分析を行った上、不足が生じた日の翌日から起算して２営業日以内に当該不足額を解消している。 ② 利用者の金銭の管理について、内閣府令第20条第１項第２号に規定する方法により管理する場合、内閣府令第21条第１項各号の要件を満たす利用者区分管理信託に係る契約に基づいて管理している。	③仮想通貨の管理（金銭の分別管理）
(6) 仮想通貨を管理・取引するために必要な暗号鍵等の適切な管理・保管に関する以下を含む内部統制（ガイドラインⅡ－２－２－２－２(1)⑥⑦） ① 自社の仮想通貨を管理・処分するために必要な暗号鍵等と、利用者の仮想通貨を管理・処分するために必要な暗号鍵等の保管場所を明確に区分して保管している。 ② 利用者の利便性等を損なわない範囲で、可能な限り、仮想通貨を管理・処分するために必要な暗号鍵等をインターネット等の外部のネットワークに接続されていない環境で管理している。	④仮想通貨に係るセキュリティ

内部統制の例	関連する業務プロセス（筆者が追加）
(7) 仮想通貨のアドレス間で仮想通貨の移動を行う業務に関する内部統制 例えば、ホットウォレットからコールドウォレットへの移動等、仮想通貨交換業者が日々の業務で行う移動に関する内部統制	③仮想通貨の管理
(8) 利用者に対する取引明細及び残高報告の送付（電子的な方法を含む。）に関する内部統制	⑦利用者財産の管理
(9) 利用者又は利用者以外からの仮想通貨の誤入金について、自己用及び利用者用と区分した上で返金又は利用者財産の調整等の対応を行うための内部統制	③仮想通貨の管理
(10) 仮想通貨に係る時価を適時に入手し、期末の時価評価額を決定及び承認するための内部統制	⑧仮想通貨の評価
(11) 利用者の仮想通貨の管理を第三者に委託する場合には、委託先において自社で管理する場合と同様の管理体制が整備されていることを確認する内部統制（ガイドラインⅡ－２－２－２－２(1)⑧）	⑩ホワイトラベル
(12) 仮想通貨交換業に関する帳簿書類について、仮想通貨交換業者の業務及び利用者財産の管理の状況を正確に反映させること、分別管理監査の結果に関する記録を行わせること及び適切に保存させることに関する以下を含む内部統制（ガイドラインⅡ－２－２－３－２） ① 帳簿書類の作成について規定した社内規則等を定めた上で社内研修等により周知徹底を図っている。 ② データファイルのバックアップ等が毀損された場合に利用者ごとの金銭と仮想通貨の額を把握・復元できるようにしている。 ③ 記載内容の正確性について作成部署以外の部門において検証を行っている。 また、追加的に関連する内部統制として、例えば以下も考えられる。 ④ 金銭の分別管理に関して、利用者勘定元帳には、法定通貨の入出金及び差引残高についても記載している。 ⑤ 仮想通貨の分別管理に関して、利用者勘定元帳を作成する前提として、ブロックチェーン等のフロー情報から残高情報を作成・表示するシステムが存在する。 ⑥ ブロックチェーン等の記録における仮想通貨の取引記録と仮想通貨交換業者のシステム上の仮想通貨の取引記録との間にはタイムラグが生じ得るため、網羅的に仮想通貨の取引記録が仮想通貨交換業者のシステムに記録される内部統制を構築している。	⑨会計システムへの入力・帳簿作成
(13) 仮想通貨のポジションを保有する場合、第16項(5)で記述した価格変動リスク又は流動性リスクが生じることになるため、これらのリスクを適切に管理するための内部統制	③仮想通貨の管理
(14) 未承認の取引の実行、暗号鍵の不正使用、記録の改竄等を防止するためのアクセス・セキュリティに関する内部統制	④仮想通貨に係るセキュリティ

（表中のガイドラインとは、2017年3月24日に金融庁が公表した「事務ガイドライン（第三分冊：金融会社関係） 16 仮想通貨交換業者関係」である。なお、2019年9月3日に「事務ガイドライン（第三分冊：金融会社関係） 16 仮想通貨交換業者関係」は改正されているが、本実務指針は2017年3月24日公表のガイドラインを基礎としている。）

以下では、仮想通貨交換業者の下記の主要な業務プロセスごとに、図表1記載の内部統制の例と関連付けて解説する。一部の内部統制については、監査上の留意点も記述する。

主要な業務プロセス	
①	アドレス生成
②	口座開設
③	仮想通貨の管理
④	仮想通貨に係るセキュリティ
⑤	カバー取引
⑥	金銭（法定通貨）の管理
⑦	利用者財産の管理
⑧	仮想通貨の評価
⑨	会計システムへの入力・帳簿作成
⑩	ホワイトラベル
⑪	ハードフォーク

① アドレス生成

まず、図表1の「付録２」の(1)の内部統制を解説する。

● (1) アドレス及び暗号鍵の生成に関する内部統制

アドレスが勝手に作成されると、自社の仮想通貨が網羅的に把握できず、簿外資産が生じる等のリスクがあるため、アドレス生成に係る内部統制は重要である。

アドレスの生成時の承認手続、アドレス管理簿や仮想通貨の取引システムのアドレスマスターへの登録が適切に行われるための内部統制、定期的なアドレスの登録状況のモニタリングなどの内部統制が必要となる。前提として、アドレス生成の明確なポリシーがあり、無秩序にアドレスが生成されないようになっていることも重要である。

利用者（顧客）からの入金用アドレスを利用者ごとに設定することもある。その場合には生成アドレスが膨大になるため、口座開設時に仮想通貨の取引システムに利用者IDを設定すると自動で入金用アドレスを設定して利用者IDと紐づけられるような業務処理統制、その設定が変更できない業務処理統制なども考えられる。

付録２には「自己用・利用者用を区分した形でアドレス管理簿及び暗号鍵管理簿に記録されることを担保する内部統制」とあるが、各アドレスの役割（利用者からの入金用アドレス、出金用アドレス、利用者分の保管用アドレス、自己分の保管用アドレス等）を明確にすることも重要である。

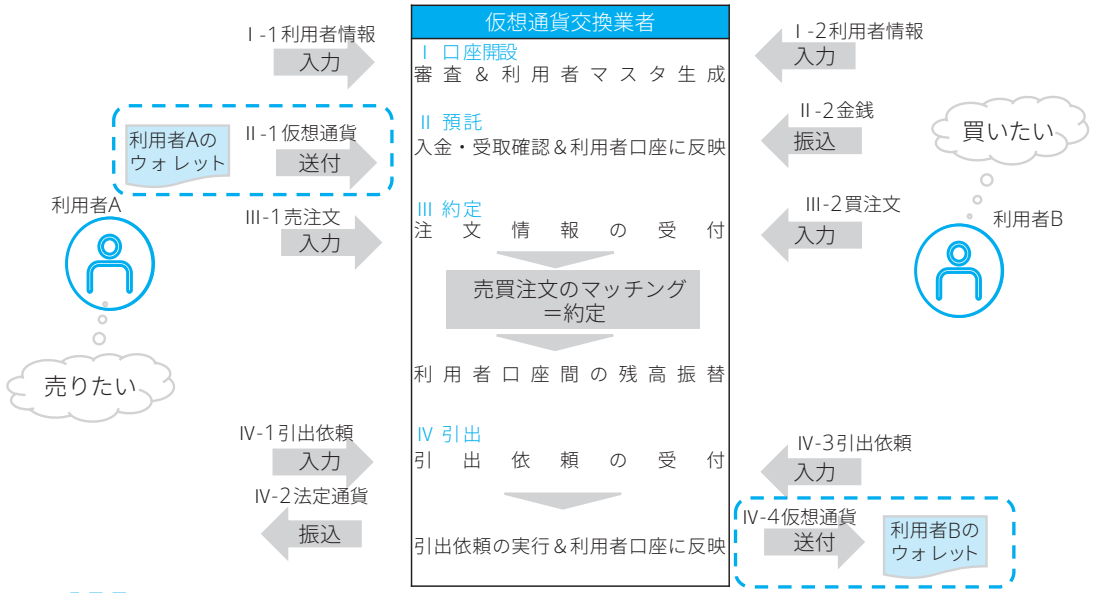
なお、一般的には、HD（Hierarchy Deterministic）ウォレットと呼ばれるアドレスを生成する機能を利用することが多いようであり、その理解も必要である。

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

ここで、次の②の前に、仮想通貨交換業者の利用者との取引に係る業務フローの概要について簡単に触れる。

仮想通貨交換業者の利用者との取引に係る業務フローには、利用者間の注文をマッチングする媒介モデルである「取引所」を前提とすると、図表2にあるとおり、主に、Ⅰ 口座開設、Ⅱ 利用者からの金銭・仮想通貨の預託、Ⅲ 約定（売買注文のマッチング）、Ⅳ 利用者による金銭・仮想通貨の引出等がある。以下の②、③では、これらに係る内部統制を解説する。

図表2　仮想通貨交換業者の基本的な業務フロー（利用者間の注文をマッチングする媒介モデルである「取引所」を前提）



✓ ［　］の部分がブロックチェーン上で記録される価値移転
✓利用者の売買記録はブロックチェーンに記録される訳ではなく、交換業者のシステム上で残高の付け替えが生じるのみ
✓利用者から送付されてきた仮想通貨は、仮想通貨交換業者が利用者用に設けたウォレットで保管される

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

②　口座開設

図表2の「Ⅰ 口座開設」に係る内部統制は、図表1の「付録２」の(2)に対応する。

●　(2) 口座開設時における本人確認を含む利用者管理簿への登録に係る内部統制

不正利用の防止（マネーロンダリング・テロ資金供与規制）という観点から重要であるのはもちろん、架空の口座でないかという観点からも監査上、重要である。

内部統制の例としては、

・口座開設時の審査担当者は本人確認書類、反社会的勢力でないことの確認等を実施し、仮想通貨の取引システムに利用者ID、利用者情報を登録する。

・上席者がその内容を確認して承認する。

等が考えられる。

また、事後的に利用者情報が改竄できないよう、利用者IDの削除や利用者情報の変更を制限する内部統制も考えられる。

なお、利用者によるアクセスの認証において、利用者本人によるアクセスを検証するための認証メカニズムが導入されていることが通常である。そのメカニズムとして、多段階認証や異なるIPアドレスからログインされた場合の確認等が考えられる。

③　仮想通貨の管理

図表1の「付録２」にあまり具体的には記載されていないが、図表2の「Ⅱ 預託」「Ⅲ 約定」「Ⅳ 引出」に係る内部統制は以下のようなものが考えられる。

●　Ⅱ　預託

仮想通貨の取引システムが、利用者からの入金用アドレスへの仮想通貨の入金を自動で検知して記録する業務処理統制が考えられる。

なお、利用者からの入金用アドレスを利用者ごとに設定せずに、1つのアドレスを利用者の入金用アドレスとしている場合には、仮想通貨の入金取引に付与されたメッセージから利用者を特定する必要があるため、それが適切に行われるようにする内部統制、不明入金の調査に係る内部統制が必要となると考えられる。

上記の状況でなくとも、実務上、不明入金が生じる可能性はあるため、その調査に係る内部統制、例えば、不明入金が生じた場合には調査し、必要な修正を行った上で、管理者が承認することが必要であると考えられる（本節③後述(9)も参照）。

監査上は、正確性の検証の観点から、ブロックチェーンと仮想通貨の取引システム上のデータを照合し、正確に利用者を識別して入金処理が行われていることを確認する。また、網羅性の検証の観点から、合計ベースでブロックチェーンと仮想通貨の取引システム上のデータを照合し、網羅的に処理されていることを確認する。

● III 約定

仮想通貨の取引システム上、仮想通貨の売買注文のマッチング（取引所の場合）、約定（販売所の場合）を適切に記録するため、仮想通貨の取引システムにおいて利用者の注文の有効性をチェックし、有効な注文のみを記録するという業務処理統制が考えられる。

また、取引手数料を仮想通貨の取引システムの設定条件に基づいて自動計算し、記録するという業務処理統制が考えられる。

● IV 引出

図表1の「付録２」の(7)に包含されると考えられる。

まず、利用者による引出、すなわち仮想通貨交換業者による出金は、仮想通貨交換業者により業務フローが異なるため、その理解が必要である。利用者からの引出依頼に基づき自動で出金処理をするケースもあれば、手動で出金処理をするケースもある。また、手動で出金処理を行う場合には、その頻度も仮想通貨交換業者により異なると考えられる。

なお、出金処理の違いは、出金用アドレスがホットウォレット（インターネット等の外部ネットワークと接続された環境）か、コールドウォレット（インターネット等の外部ネットワークと接続されていない環境）かの違いと関連する。ホットウォレットは自動出金が可能になるが、コールドウォレットは適時に出金処理ができないため、手動でまとめて出金処理を行うケースが多いと考えられる。また、ホットウォレット、コールドウォレットはサイバーセキュリティの観点から非常に重要であり、「④仮想通貨に係るセキュリティ」で後述する。

▶ ホットウォレットからの自動送金

利用者からの引出依頼に基づいて自動的に指定されたアドレスへ送金処理を行うとともに、仮想通貨の取引システムにおいて送金処理を記録する業務処理統制が考えられる。

▶ コールドウォレットからの手動送金

以下のような内部統制が考えられる。

・送金担当者が作成した送金ファイルについて、暗号鍵へのアクセス権を有する署名権限者が承認した上で電子署名を行う。
・別の担当者が、電子署名後の送金ファイルが利用者からの引出依頼と整合していることを確認してブロードキャストする。
・送金ファイルがブロードキャストされると、仮想通貨の取引システムにおいて自動的に送金処理を記録する。

▶ ネットワーク手数料（マイニング手数料）

一般的に、ブロックチェーンへの送金にはマイナーへネットワーク手数料を支払う。会社と利用者のどちらが負担するかは約款等により決められる。

以下のような内部統制が考えられる。

・仮想通貨の取引システムは、設定条件に基づいてネットワーク手数料を計算して送金処理を行う。
・仮想通貨の取引システムは、ネットワーク手数料を正確かつ網羅的に記録する。

また、毎営業日、利用者の出金依頼額と実際の送金額が一致しているかを確認する内部統制も考えられる。

ホットウォレットからの自動送金の場合、監査上は、正確性の検証の観点から、ブロックチェーンと仮想通貨の取引システム上のデータを照合し、正確に利用者を識別して送金処理が行われていることを確認する。また、網羅性の検証の観点から、合計ベースでブロックチェーンと仮想通貨の取引システム上のデータを照合し、網羅的に処理されていることを確認する。

コールドウォレットからの手動送金の場合、送金担当者と署名担当者の職務分掌の検証、送金ファイルの改竄防止に係る内部統制を検証する。

いずれの場合でも、利用者の出金依頼額と実際の送金額の一致を確認する内部統制の検証が考えられる。

図表1の「付録２」の(3)～(5)は分別管理に係る内部統制である。

(3)では、利用者が預託した金銭及び仮想通貨を適切に分別管理するための社内規則に分別管理の執行方法を定めること、個々の利用者の持分が直ちに判別できることとしていること、その遵守状況を適切に検証すること等が挙げられている。

(4)では、仮想通貨の分別管理のため、帳簿上の利用者財産の残高とブロックチェーン等のネットワーク上の利用者財産の有高を照合すること、不足がある場合にはそれを解消することが挙げられている。

(5)では、金銭の分別管理のため、帳簿上の利用者残高と利用者財産を分別管理している銀行等の口座残高を照合すること、不足がある場合にはそれを解消することが挙げられている。

ここでは、非常に重要な内部統制である(4)の仮想通貨に係る照合（いわゆるリコンサイル）を解説する。(5)の金銭の分別管理は後述する（「⑥金銭（法定通貨）の管理」参照）。

● **(4) 利用者からの仮想通貨の受入れ及び利用者への引出しの事実が、ブロックチェーン等の記録上の有高と一致していることを確保するための以下を含む内部統制（ガイドラインⅡ－２－２－２－２(1)③）**
① 利用者の仮想通貨の管理について、仮想通貨交換業者が管理する帳簿上の利用者財産の残高と、ブロックチェーン等のネットワーク上の利用者財産の有高を毎営業日照合している。
② 照合した結果、利用者財産の有高が帳簿上の利用者財産の残高に満たない場合には、原因の分析を行った上、当該不足額に関しては、不足が生じた日の翌日から起算して５営業日以内に当該不足額を解消している。

リコンサイルの方法は仮想通貨交換業者により異なる。自動処理によりリコンサイルを行う仮想通貨交換業者もあれば、手動で行う仮想通貨交換業者もある。

▶ 自動
仮想通貨の取引システムは、取引データを集計した残高数量と、ブロックチェーン上の数量を自動で照合し、差異が生じた場合には通知される。
差異が生じた場合には調査し、必要な修正を行った上で、管理者が承認する。

▶ 手動
送金担当者から独立した照合担当者が、仮想通貨の取引システム上の残高数量と、ブロックチェーン上の数量を照合し、管理者が承認する。
差異が生じた場合には調査し、必要な修正を行った上で、管理者が承認する。

監査上、リコンサイルのプロセスの検証、差異の調査結果をレビューすることは重要である。差異を調査し、適切に処理されていない場合には、虚偽表示が生じる可能性もある。
なお、仮想通貨交換業者が仮想通貨の取引システムに記録するに当たって、ブロックチェーン上のコンファメーション（ブロックチェーン上での承認）数を決めている場合がある。ブロックチェーン上の数量と照合する場合、当該コンファメーション数の方針によっても差異が生じる場合があるため、留意が必要である。

図表1の「付録２」の(9)にある誤入金は、上記の差異の調査にも関連する。

● **(9) 利用者又は利用者以外からの仮想通貨の誤入金について、自己用及び利用者用と区分した上で返金又は利用者財産の調整等の対応を行うための内部統制**

仮想通貨の不明入金、誤入金、不正出金等により差異が生じる。会計処理に影響することもあるため、差異が生じた場合の調査は非常に重要である。
例えば、不明入金が生じた場合には調査し、必要な修正を行った上で、管理者が承認することが必要であると考えられる。

上記「Ⅳ　引出」でも記述したが、仮想通貨の移動に係る内部統制も非常に重要である。

● **(7) 仮想通貨のアドレス間で仮想通貨の移動を行う業務に関する内部統制**
例えば、ホットウォレットからコールドウォレットへの移動等、仮想通貨交換業者が日々の業務で行う移動に関する内部統制

ホットウォレット、コールドウォレット、いずれからの出金であっても、管理者の承認に基づき実施する必要がある。

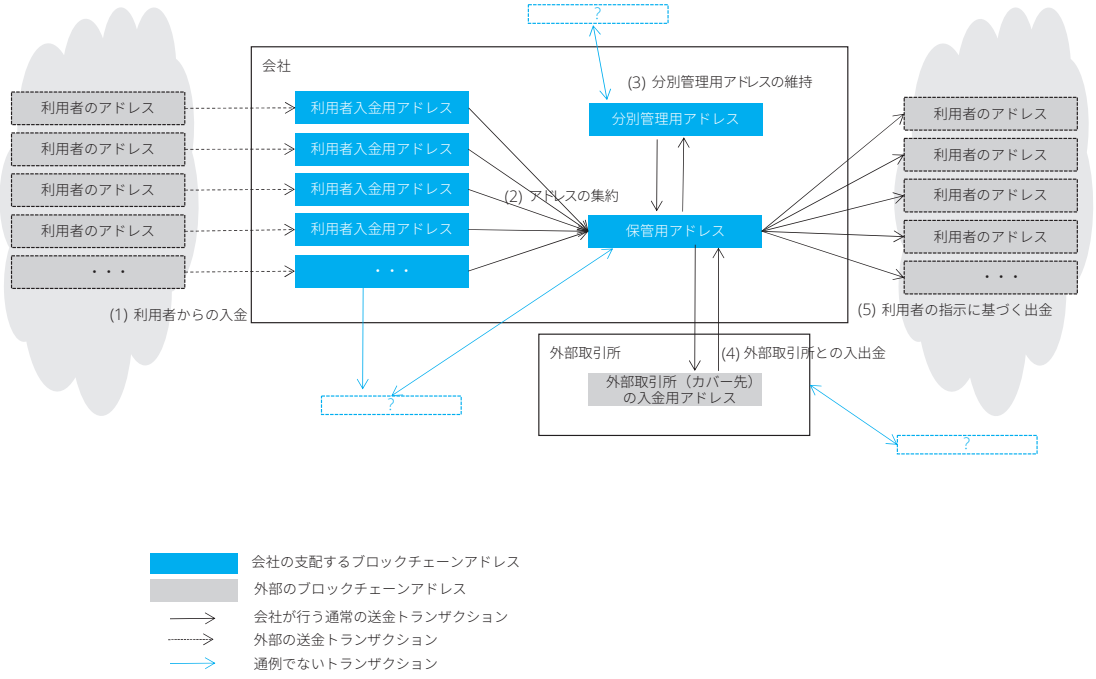
▶ ホットウォレットからの送金
・ウォレット間の送金は、管理者の承認に基づいて行われる。
・送金は担当者と別の承認者による承認がないと実行できないよう入力がコントロールされている。

▶ コールドウォレットからの送金
ウォレット間の送金は、管理者の承認に基づいて行われる。
送金は、仮想通貨の引き出しと同じ内部統制が適用される。

仮想通貨交換業者は複数のアドレスを保有するが、業務上、各アドレスの役割を明確にして使用していることが通常である。図表3は、保有アドレスの構成の例である。図表3では、利用者からの入金を受領する利用者入金用アドレス、保管用アドレス、分別管理のため利用者分の仮想通貨を保管する分別管理用アドレスを示している。
仮想通貨の流出を防ぐため、保管用アドレスから直接出金するのではなく、ホットウォレットの出金用アドレスを設けることもある。出金用アドレスを設け、保管用アドレスをコールドウォレットにして、セキュリティを高めることも可能となる。依然として、仮想通貨の不正流出事件が起こっているため、ホットウォレットの残高を最小限にする対応は非常に重要である。

図表3　保有アドレスの構成の例

ブロックチェーン上のトランザクションフロー例示



アドレスの役割を踏まえた異常取引を把握する内部統制として以下が考えられる。

●　ブロックチェーンのフロー分析

分別管理のために利用者分の保管用アドレスと自己分の保管用アドレスを区分するため、図表1の「付録２」の(3)も関連する。

仮想通貨交換業者は通常、複数のアドレスを保有するが、各アドレスの役割と、それに基づく仮想通貨の流れを理解した上で、入出金を分析（フロー分析）し、想定外の仮想通貨の流れがないか、その流れが仮想通貨の取引システムのデータと整合しているかを確認する。

さらに、例えば、以下のような異常取引、異常なアドレスを識別する。

・会社の管理するアドレスの役割に鑑みて入出金が想定されないアドレスとの取引
・入出金が多額な取引
・入出金の頻度が多いアドレスに関連する取引
・残高が大きいが、長期間動きがないアドレスとの取引

なお、監査上、同様の視点での監査手続が非常に重要であることは言うまでもない。

図表1の「付録２」の(13)は、自己ポジションを保有する場合の自己ポジションの管理に係る内部統制と考えられる。

●　(13) 仮想通貨のポジションを保有する場合、第16項(5)で記述した価格変動リスク又は流動性リスクが生じることになるため、これらのリスクを適切に管理するための内部統制

販売所を営む場合、自己ポジションを保有するのが通常であるが、自己ポジションが多額である場合には、価格変動リスク等が高くなる。そのため、自己ポジションを一定に保つために、外部取引所（カバー先）との売買取引を自動あるいは手動で行うことがある。

このような取引が適切に行われるように、自動の場合には業務処理統制、手動の場合には承認手続等を整備、運用することが考えられる。

自己分の多額の保有を避けるという意味ではビジネスリスクへの対応が色濃いが、監査人が理解することは必要であろう。

④　仮想通貨に係るセキュリティ

すでに「③　仮想通貨の管理」までで業務処理統制にも触れているが、ここではITについて全般統制も含めて解説する。

仮想通貨交換業者の業務は、情報システムを利用して遂行されている場合が多い（本実務指針付録１参照）。監基報315第11項において、監査人は、監査に関連する内部統制を理解することが求められており、通常、仮想通貨交換業の業務で利用される情報システムについて理解するとされている（本実務指針20項）。

仮想通貨交換業の業務で利用される情報システムには、会計アプリケーション及び仮想通貨交換業の業務で利用される業務アプリケーションが含まれる。当該業務アプリケーションは、例えば、以下のような機能を有するものと考えられるとされている（本実務指針21項）。

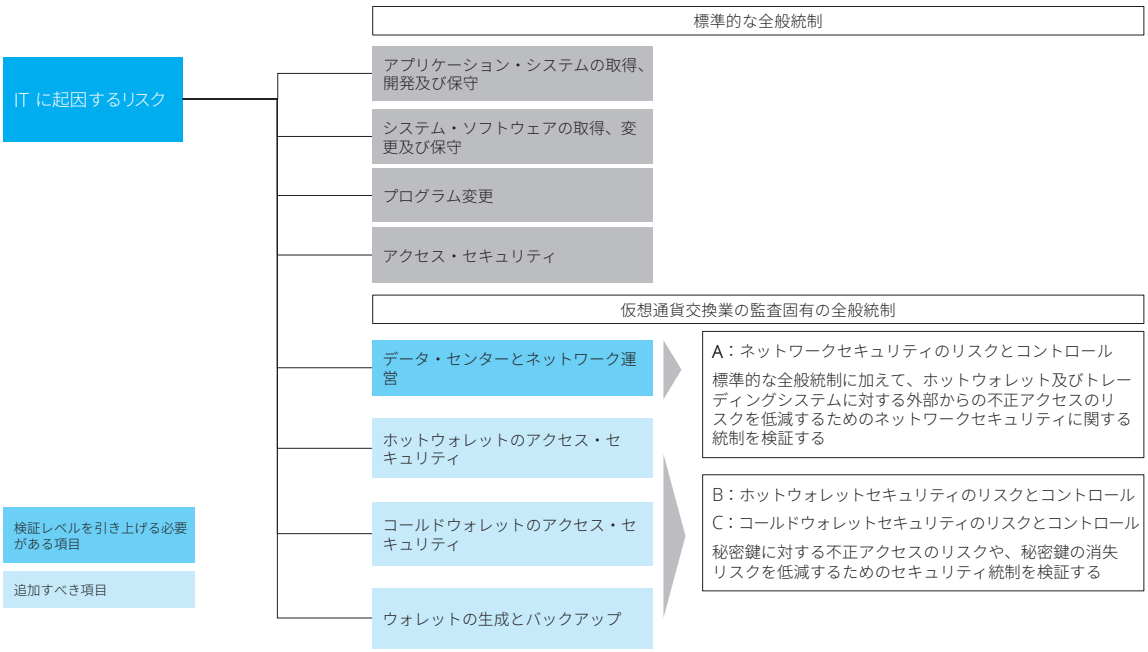
(1) 仮想通貨の交換及び売買取引
(2) 資金決済法第63条の13に規定される法定帳簿の作成
(3) 仮想通貨の外部との取引及び残高の検証（ブロックチェーン等の記録上への取引の記録、当該記録された取引データ及び残高情報の取得、当該取引データ及び残高情報の閲覧のための各仮想通貨のブロックチェーン等の記録の種類に対応したシステム等）
(4) 職務分掌を担保するアクセス・セキュリティ

上記(1)は「③　仮想通貨の管理」で解説した内容と関連する。(2)は法定帳簿の作成に係るもので後述する（⑨「会計システムへの入力・帳簿作成」参照）。(3)は「③　仮想通貨の管理」の中でもリコンサイルが関連する。(4)を含むITを中心とした内容を本節で解説する。

ITを利用した情報システムの理解については、IT委員会実務指針第6号「ITを利用した情報システムに関する重要な虚偽表示リスクの識別と評価及び評価したリスクに対応する監査人の手続について」等を参照するとされている（本実務指針22項）。

図表4は仮想通貨交換業者の全般統制の理解の例である。仮想通貨交換業者の特質を踏まえて、特に注意すべき項目を示している。言うまでもなく、仮想通貨交換業者の業務はITに依存する領域が多く、ITに係る検討は非常に重要である。

図表4　仮想通貨交換業者の全般統制の理解の例

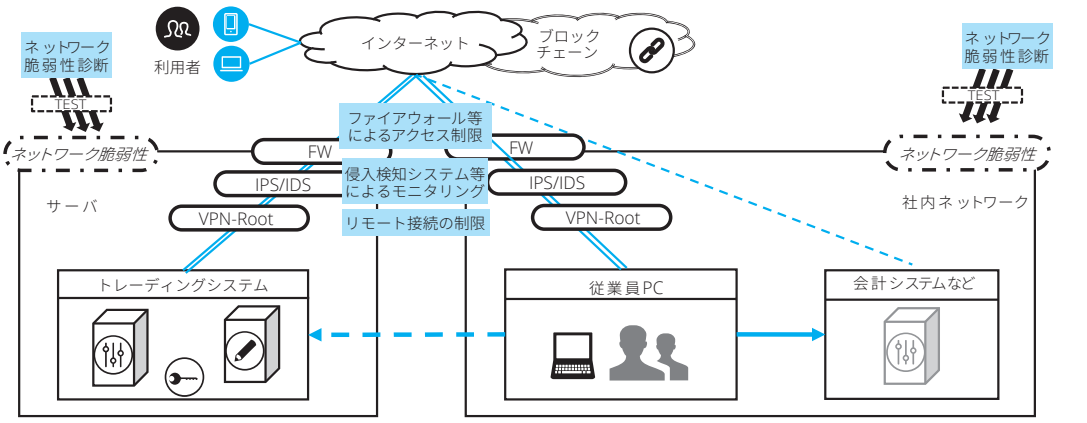


図表4にあるA～Cのリスクとコントロールを具体的に示すと、図表5～7のとおりである。

図表5のセキュリティリスクの検討に当たっては、サイバーセキュリティの専門家等を関与させることを検討することも必要であろう。

図表5　ネットワークのセキュリティリスクとコントロールの例

ネットワークのセキュリティリスクとコントロール



リスク

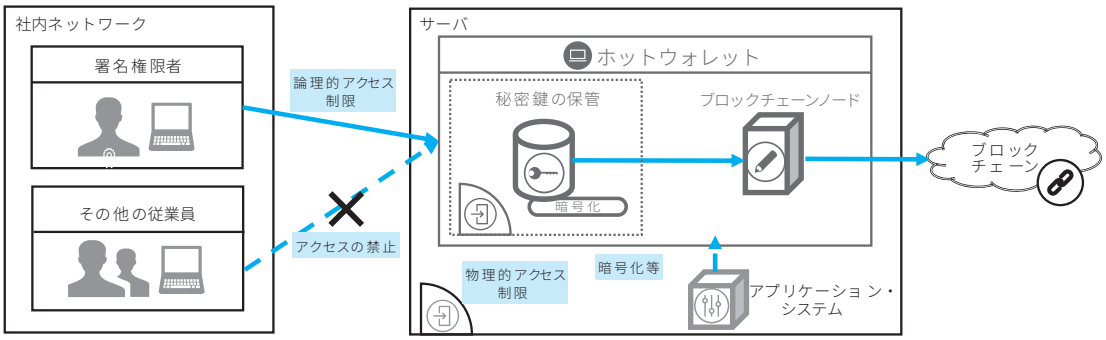
ネットワークセキュリティが十分に整備されていないことで、トレーディングシステムやホットウォレットに対する外部からの不正なアクセスが防止できず、不正な送金や秘密鍵の盗難が行われてしまう。

内部統制の例示

- 外部ネットワークと社内ネットワークの間には、ファイアウォールの導入や不要ポートの無効化等によるアクセス制限が実装されているか
- 侵入検知システム（IPS/IDS）によって脅威は定期的に警告が出されているか。また、これらの脅威は調査分析されているか
- 外部からのリモート接続（VPN）は承認された者しか行えないよう制限されているか
- ネットワークの脆弱性診断を定期的に行っているか

図表6　ホットウォレットセキュリティのリスクとコントロールの例

ホットウォレットセキュリティのリスクとコントロール



リスク

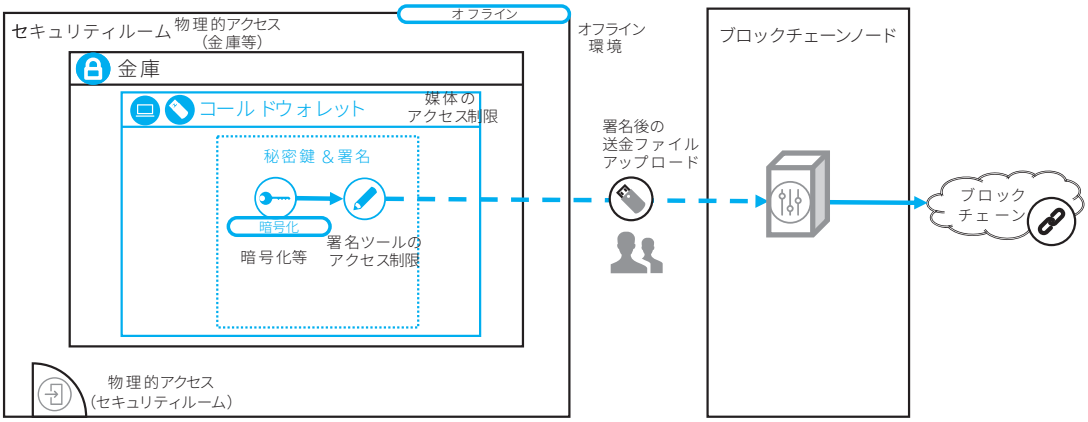
ホットウォレットのセキュリティが十分に整備されていないことで、マネジメントや従業員による不正なアクセスによって秘密鍵が盗難される・消失するリスク

内部統制の例示

- ホットウォレットへの論理的・物理的アクセス権は承認の上付与されているか、また適切に制限されているか
- ホットウォレットへの論理的・物理的アクセス権は適時削除され、定期的に棚卸されているか
- ホットウォレットへの論理的・物理的アクセスは必要に応じて記録され、適切な管理者によってアクセスの妥当性が点検されているか。
- ホットウォレットの秘密鍵は、暗号化等によってセキュアな状態で保管されているか

図表7　コールドウォレットセキュリティのリスクとコントロールの例

コールドウォレットセキュリティのリスクとコントロール



リスク

コールドウォレットのセキュリティが十分に整備されていないことで、マネジメントや従業員による不正なアクセスによって秘密鍵が盗難される・消失するリスク

内部統制の例示

- セキュリティルーム及び金庫への物理的アクセス権は承認の上付与されているか
- 秘密鍵の保管媒体への論理的アクセスは承認の上付与されているか
- 論理的・物理的アクセス権限は適時に削除され、定期的に棚卸されているか
- 論理的・物理的アクセスは必要に応じて記録され、適切な管理者によってアクセスの妥当性が点検されているか
- 秘密鍵はオフライン環境に、暗号化等によってセキュアな状態で保管されているか
- 秘密鍵のバックアップはコールドウォレットと同等のセキュアな環境で保管されているか

仮想通貨に係るセキュリティに関連する内部統制として、図表1の「付録２」の(6)、(14)が関連する。

●　(6) 仮想通貨を管理・取引するために必要な暗号鍵等の適切な管理・保管に関する以下を含む内部統制（ガイドラインⅡ－２－２－２－２(1)⑥⑦）

①　自社の仮想通貨を管理・処分するために必要な暗号鍵等と、利用者の仮想通貨を管理・処分するために必要な暗号鍵等の保管場所を明確に区分して保管している。

②　利用者の利便性等を損なわない範囲で、可能な限り、仮想通貨を管理・処分するために必要な暗号鍵等をインターネット等の外部のネットワークに接続されていない環境で管理している。

図表6、図表7に関連するものであるため、そちらを参照していただきたい。いずれにせよ、ホットウォレット、コールドウォレットの利用方針によりセキュリティに係るリスクは大きく変わるため、非常に重要である。

その他、以下のような内部統制も考えられる。

- ホットウォレットに保管された仮想通貨の残高が一定量を超過した場合に管理者へ通知され、残高を減少させる。
- 暗号鍵の消失に備えて、暗号鍵のバックアップを暗号化して保存する。

●　(14) 未承認の取引の実行、暗号鍵の不正使用、記録の改竄等を防止するためのアクセス・セキュリティに関する内部統制

アクセス・セキュリティは非常に重要であり、図表6、図表7も参照していただきたい。

その他、以下のような内部統制も考えられる。

- マルチシグ（マルチシグネチャーの略称。電子署名に複数の暗号鍵を必要とする）の技術を導入し、仮想通貨の送金処理において複数名の署名を必要とする。

なお、監査開始以前にアドレスを創業者等がすでに作成している場合、その創業者等は暗号鍵を知っていることになる。その後、内部統制を構築したとしても、創業者等が予め知っている暗号鍵を用いて不正等を行う可能性はゼロではなく、暗号鍵等の管理の限界が存在することは付言しておく。

⑤　カバー取引

ここでのカバー取引とは、特に仮想通貨交換業者が販売所である場合、利用者との取引の反対売買をして、ポジション（残高）を調整するための取引のことを指す。仮想通貨交換業者は、自己の仮想通貨のポジションを調整するために他の仮想通貨交換業者と取引をするのが通常である。ビジネス上は、自己の仮想通貨のポジションを調整し、自己ポジションの価格変動リスクを低減することがポイントと言われる。

図表1の付録2には明記されていないが、カバー取引に係る内部統制として以下のようなものが考えられる。

●　カバー取引

以下のような内部統制が考えられる。

・カバー先との取引を実施する際には、管理者が承認する。
　なお、自己ポジションの調整のために自動でカバー先と取引を行う場合もあるため、その場合には自動的にカバー先へ発注する業務処理統制が挙げられる。
・カバー先から入手した取引履歴と、自社の取引データを照合し、一致することを確認する。管理者はその確認結果を承認する。
　なお、カバー先と締め時間が異なる場合もあるため、留意が必要である。
・定期的にカバー先から残高明細を入手して、自社の残高と照合する。管理者はその確認結果を承認する。
・カバー先が仮想通貨の流出等により破たんするリスクもあるため、カバー先の信用リスクを継続的に評価することが必要である。

⑥　金銭（法定通貨）の管理

下記は、利用者からの金銭の預託、金銭の引出に係る内部統制である。

●　預託

金銭の預託は、自動処理、手動処理が考えられる。
以下のような内部統制が考えられる。

▶　自動処理
　仮想通貨の取引システムは、銀行の入金データに基づき、利用者を特定して入金処理を行う。

▶　手動
　担当者は、銀行の入金データに基づき、仮想通貨の取引システムに利用者別に入力する。管理者が入力結果を承認する。

また、いずれの場合でも、一定期間の銀行の入金データと仮想通貨の取引システムへの入力金額を照合する内部統制も考えられる。

監査上は、正確性の検証の観点から、銀行からの入金データと仮想通貨の取引システム上のデータを照合し、正確に利用者を識別して入金処理が行われていることを確認する。また、網羅性の検証の観点から、合計ベースで銀行からの入金データと仮想通貨の取引システム上のデータを照合し、網羅的に処理されていることを確認する。
手動処理の場合、担当者と管理者の職務分掌の検証等を検証する。

●　引出

金銭の引出も、自動処理、手動処理が考えられる。
以下のような内部統制が考えられる。

▶　自動処理
　仮想通貨の取引システムは、利用者が入力した引出依頼に基づき、利用者の銀行口座へ自動で出金処理を行う。

▶　手動処理
　担当者は、利用者が入力した引出依頼に基づき、仮想通貨の取引システムに利用者別に入力するとともに、銀行への支払依頼を作成する。管理者が入力結果を承認後に、入力結果を確定するとともに、銀行への支払指示を行う。

また、いずれの場合でも、一定期間の銀行への出金データと仮想通貨の取引システムへの入力金額を照合する内部統制も考えられる。

監査上は、正確性の検証の観点から、銀行への出金データと仮想通貨の取引システム上のデータを照合し、正確に利用者を識別して入金処理が行われていることを確認する。また、網羅性の検証の観点から、合計ベースで銀行への出金データと仮想通貨の取引システム上のデータを照合し、網羅的に処理されていることを確認する。
手動処理の場合、担当者と管理者の職務分掌の検証、銀行への出金データの改竄防止に係る内部統制を検証する。

図表1の「付録２」の(5)は、金銭の分別管理に係る内部統制である。

● **(5) 利用者からの金銭について自己分と区分して管理するための以下を含む内部統制（ガイドラインⅡ－２－２－２－２(1)④⑤）** **① 利用者の金銭の管理について、内閣府令第20条第１項第１号に規定する方法により管理する場合、仮想通貨交換業者が管理する帳簿上の利用者財産の残高と、利用者財産を分別管理している銀行等の口座残高を毎営業日照合している。** **照合した結果、銀行等の口座残高が帳簿上の利用者財産の残高に満たない場合には、原因の分析を行った上、不足が生じた日の翌日から起算して２営業日以内に当該不足額を解消している。** **② 利用者の金銭の管理について、内閣府令第20条第１項第２号に規定する方法により管理する場合、内閣府令第21条第１項各号の要件を満たす利用者区分管理信託に係る契約に基づいて管理している。**
以下のような内部統制が考えられる。 ・ 仮想通貨の取引システムにより集計された自己及び利用者の預金残高と、銀行口座の残高を照合する。 ・ 差異が生じた場合には調査し、必要な修正を行った上で、管理者が承認する。

⑦ 利用者財産の管理

ここでは、これまでに触れていない利用者財産の管理に係る内部統制を解説する。

● **利用者財産の管理**
以下のような内部統制が考えられる。 ▶ 取引残高報告書の利用者への開示 仮想通貨の取引システムは取引履歴データを集計して利用者財産の残高を計算して「取引残高報告書」等を生成し、利用者へ交付する。 監査上、正確性の検証の観点から、取引残高報告書と仮想通貨の取引システムを照合する。また、網羅性の検証の観点から、すべての利用者に対して取引残高報告書が交付されていることを確認する。具体的には、全利用者が取引残高報告書のデータへ容易にアクセスできることをプログラムの仕様の確認、実際に仕様通りであることを確認する等の手続が考えられる。 ▶ 取引の変更に関する内部統制 システムトラブル等の例外的な理由によって利用者の約定データや取引履歴データを修正する場合、管理者の承認を得る。 仮想通貨の取引システムの約定データや利用者財産の残高データを修正する権限は、職務分離ポリシーに従って特定の担当者に制限されている。 ▶ 取引の変更ログレビュー リスク管理部門等は、定期的に約定や利用者財産に対するデータの変更記録をレビューし、未承認のデータ変更が行われていないことを検証する。 ▶ 苦情処理結果のレビュー 利用者からの苦情処理の管理簿をレビューし、利用者財産の残高を修正する事象が生じていないかを確認する。

⑧ 仮想通貨の評価

図表1の「付録２」の(10)は、仮想通貨の評価に係る内部統制である

● **(10) 仮想通貨に係る時価を適時に入手し、期末の時価評価額を決定及び承認するための内部統制**
以下のような内部統制が考えられる。 ▶ 活発な市場の有無の判定 仮想通貨の種類ごとに、継続的に価格情報が提供される程度に十分な数量及び頻度で取引が行われているかを確認し、活発な市場が存在する仮想通貨に該当するかどうかを検討する。 ▶ 時価評価 仮想通貨の評価に利用したレートの適切性を、他社のレートと比較すること等により検討する。

⑨　会計システムへの入力・帳簿作成

ここでは会計システムへの入力に係る内部統制を取り上げる。

●　会計システムへの入力

会計システムへの入力に係る業務プロセスも仮想通貨交換業者により様々と考えられる。会計システムの入力は、手動、自動のいずれも考えられる。

▶　手動

手動の場合であっても、仕訳入力の基礎となるデータは、通常、仮想通貨の取引システムにより集計されると考えられる。そのため、その集計が適切に行われるための業務処理統制が必要となる。

なお、監査上は、その集計結果が適切であるかは慎重に検討する必要があろう。

▶　自動

仮想通貨の取引システムが自動的に会計システムと連携して入力処理される場合であっても、その入力データが適切に作成されるための業務処理統制が必要となるのは手動の場合と同じである。

また、以上の会計システムへの入力結果に問題がないかどうかを検証する内部統制も必要である。

・経理担当者は、勘定科目・通貨単位で残高テーブルと総勘定元帳等の照合を定期的に行い、仕訳が網羅的に記録されていることを検証し、管理者が承認する。
・差異が生じた場合には調査し、必要な修正を行った上で、管理者が承認する。

下記の図表1の「付録２」の(12)の内部統制は法定帳簿も含む帳簿を適切に作成するための内部統制である。

●　(12) 仮想通貨交換業に関する帳簿書類について、仮想通貨交換業者の業務及び利用者財産の管理の状況を正確に反映させること、分別管理監査の結果に関する記録を行わせること及び適切に保存させることに関する以下を含む内部統制（ガイドラインⅡ－２－２－３－２）

仮想通貨の取引システム等により自動で作成されることが多いと考えられるため、基礎データが適切に作成されていることを前提に、それを適切に集計するための業務処理統制が必要となる。

⑩　ホワイトラベル

ここでのホワイトラベルは、他社から仮想通貨の取引システムの提供を受け、自社ブランドでサービスを提供することを指している。

●　(11) 利用者の仮想通貨の管理を第三者に委託する場合には、委託先において自社で管理する場合と同様の管理体制が整備されていることを確認する内部統制（ガイドラインⅡ－２－２－２－２(1)⑧）

本実務指針では、ITを利用した情報システムの理解については、IT委員会実務指針第6号「ITを利用した情報システムに関する重要な虚偽表示リスクの識別と評価及び評価したリスクに対応する監査人の手続について」等を参照するとされている（本実務指針22項）。また、情報システムの管理、運用を外部に委託している場合については、監査基準委員会報告書402「業務を委託している企業の監査上の考慮事項」第10項に従って当該外部委託先の情報システムに関しても重要な虚偽表示リスクを識別し評価した上で、識別したリスクに対応するリスク対応手続を立案し実施することも考えられるとされている（本実務指針22項）。

ホワイトラベルの提供を受けて交換業を営む場合、システムや業務フローの大部分を外部委託することになる。そのため、これまで記述してきた内部統制も含めて、ホワイトラベルを提供する他社の内部統制、管理体制を十分に検討する必要がある。

なお、監査上は、外部委託先の内部統制の有効性に関する十分かつ適切な監査証拠を入手できないリスクがあり、特にITに関連する内部統制の検討にあたってはITの専門家を関与させて慎重に検討する必要がある。

⑪　ハードフォーク

ハードフォークは「仮想通貨シリーズ(6)　業種別委員会実務指針第61号「仮想通貨交換業者の財務諸表監査に関する実務指針」の解説②」（本紙2019年2月号（Vol.510））でも取り上げている。その内容を再掲しつつ、内部統制について解説する。

●　ハードフォーク

ブロックチェーンの分岐により保有する仮想通貨が異なる種類の仮想通貨に分裂するハードフォークと呼ばれる事象の発生等により、当初は想定しなかった価値及び数量の変動が生じる可能性があり、仮想通貨の実在性及び仮想通貨の評価に影響がある。

ハードフォークの取扱いについては、JVCEAにおいてその取扱いに関する指針を定めることとされているが、一般社団法人 日本仮想通貨事業者協会（現一般社団法人日本仮想通貨ビジネス協会。日本ブロックチェーン協会（JBA）とともにJVCEAの礎となった）が2017年11月10日に公表した「計画されたハードフォークおよび新コインへの対応指針の公表について（お知らせ）」は参考になると考えられる。

そこでは、ハードフォークにより組成された「新コインを支えるプログラムに欠陥がある場合や故意に不正なプログラムが組み入れられている場合には、新コインが価値を有せず、あるいは不適切なプログラムを介してオリジナルコインが奪われるなどの事態が生じる可能性」があるとされている。その欠陥には、「例えば、新コインはオリジナルコインの記録の複製によって組成されるため、新コインにオリジナルコインと識別するプログラムが組み込まれていない場合には、どちらのコインが移動したのか判別できずにブロックチェーンが機能しなくなり、あるいは二重移動や保有者の知らぬ間に移動されて抜き取られる（いわゆるリプレイアタック）などの不正行為が発生する可能性」が生じるとされている。

さらに、「このような行為や現象は、その対応を求められる仮想通貨交換業者の業務コストの上昇を引き起こすばかりではなく、顧客資産の安全管理や仮想通貨の資産価値そのものに深刻な影響を及ぼす可能性があることから、適切な仮想通貨としての条件を満たさぬ新コインについてはお客様に付与することなく、流通市場への参入を未然に防ぐ必要」があるとされている。

また、「計画されたハードフォーク及び新コインへの対応指針」において、顧客に新コインを付与する場合には、少なくとも以下の事項については十分に確認を行わなければならないとされている。

イ．新コインについて二重移転を防止する措置が講じられていること
ロ．新コインに顧客の資産を侵害する仕組みが講じられていないこと
ハ．新コインの有する機能が不法、不正な行為を誘引するものではないこと

さらに、当然であるが、利用者（顧客）の持ち分により生ずる新コインを会員が利用者に代わって自らが所有するものとして取得してはならないとされている。

内部統制としては、以上も踏まえて新コインが適切な仮想通貨であるかの検討を十分に実施すること、仮に新コインを取り扱う場合には仮想通貨の取引システムの準備を十分に行って、その整備・運用に問題がないことを確認することが必要と考えられる。

監査上は、これらが適切になされているか、慎重に検討する必要があると考えられる。

仮想通貨交換業者の内部統制はITへの依存度が非常に高いため、監査上、内部統制を検討するに当たっては、ITの専門家も関与し、サイバーセキュリティも含めて慎重に検討していくことが非常に重要である。

以上

