

事務局説明資料

2018年 5月22日
金 融 庁

I	仮想通貨・仮想通貨取引をめぐるプレイヤー	2
II	仮想通貨やそれに関連する技術についての 各国当局者等による指摘	6
III	補足資料（第2回研究会における質問に関して）	10

仮想通貨・仮想通貨取引をめぐるプレイヤー（1）

討 議 用
 ※ 本資料は討議の際の参考資料として作成したものであり、記載内容やデータの正確性・完結性を保証するものではありません。

- 仮想通貨・仮想通貨取引をめぐるのは、仮想通貨交換業者とその利用者に加え、新たな仮想通貨の考案者・開発者や、仮想通貨の取引記録を確定させるための計算を行う者（マイナー）など、グローバルに、様々なプレイヤーが関与している。

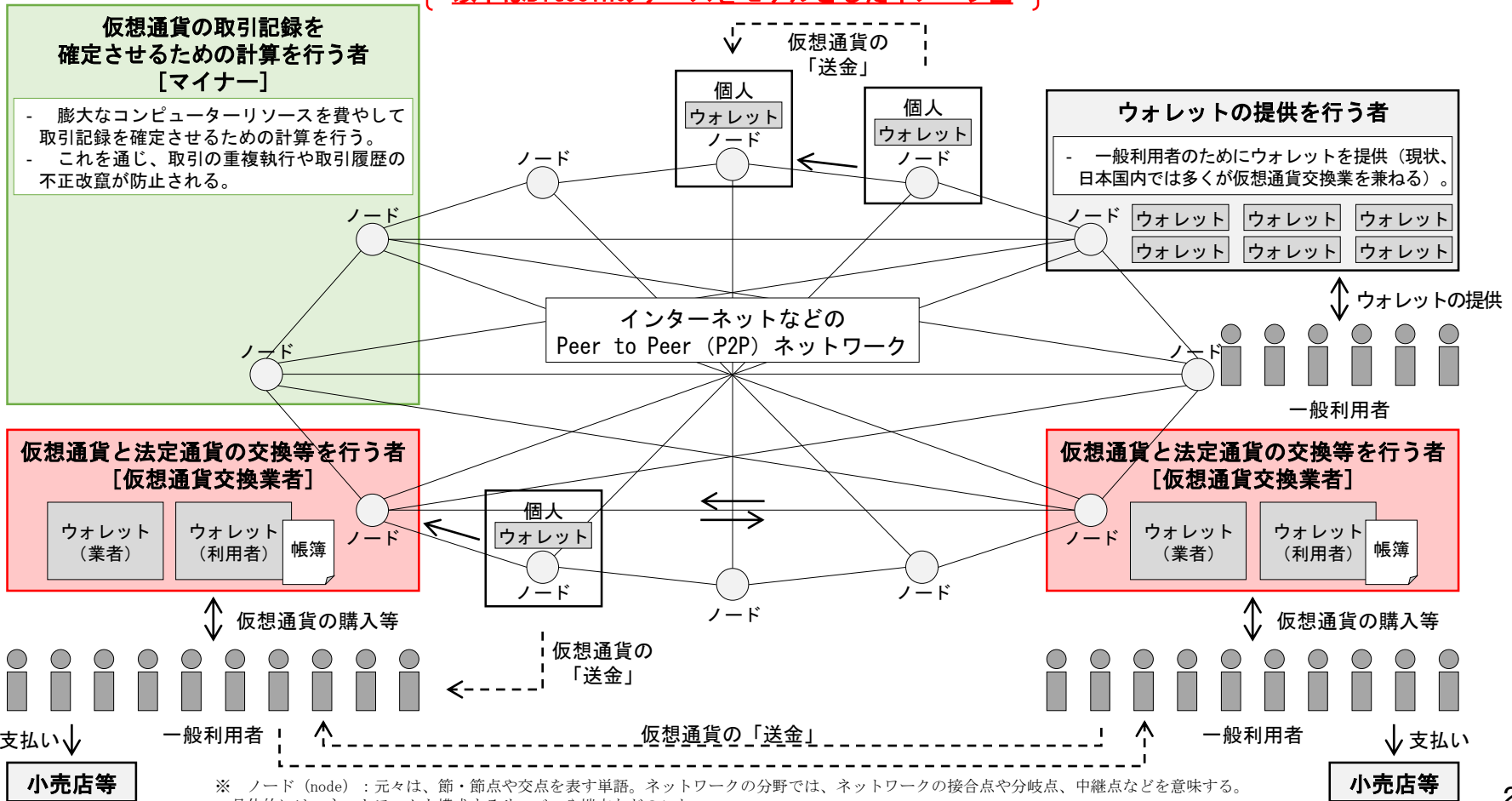
新たな仮想通貨の考案者・開発者

新たな仮想通貨について、①取引の即時性や安定性などを確保するためにどのような技術を用いるのか、②発行量の決定・調整メカニズムをどのようにするのか、などの仕様を検討・決定（仮想通貨の公開後も、仕様を随時変更することがある）。

仕様に基づき制作された新たな仮想通貨を公開

（以下はBitcoinのケースをモデルとしたイメージ図）

※ プレイヤーの構成や役割は、仮想通貨ごとに異なる。例えば、中央管理者が存在し、マイナーが存在しない場合もある。



※ ノード (node) : 元々は、節・節点や交点を表す単語。ネットワークの分野では、ネットワークの接合点や分岐点、中継点などを意味する。具体的には、ネットワークを構成するサーバーや端末などのこと。

新たな仮想通貨の考案者・開発者

- 新たな仮想通貨の考案者・開発者は、技術者個人の場合もあれば、営利企業の場合もある。
- 考案・開発の目的も様々であり、Etherのように、特定の技術的プラットフォームのための仮想通貨として開発されるものもある。

図表1 時価総額の大きな仮想通貨の概要

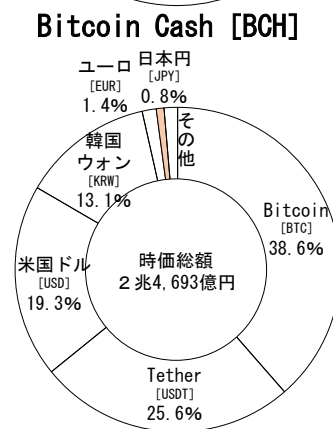
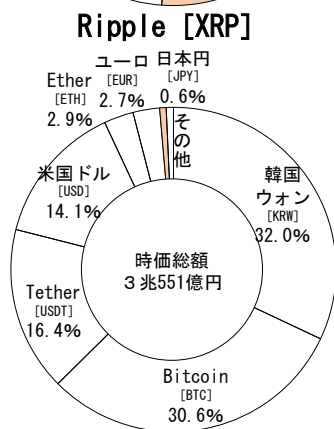
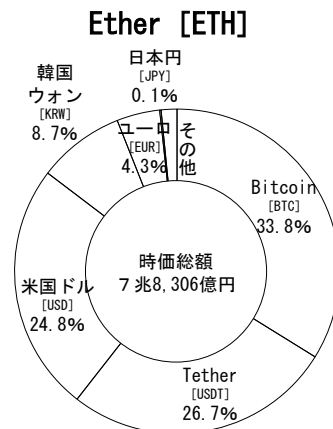
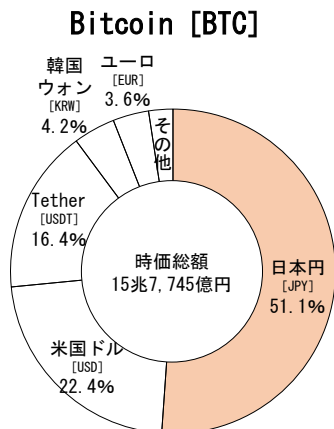
名称 [単位]	時価総額	公開等	考案者・開発者 [中心となった者]	特徴
Bitcoin [BTC]	15兆7,745億円	2009年	“サトシ・ナカモト” 他の技術者	<ul style="list-style-type: none"> ○ 中央管理者なしに運営されることとなった最初の仮想通貨とされる。中核技術である、いわゆるブロックチェーン技術とともに開発。 ○ マイナーが存在。
Ether [ETH]	7兆8,306億円	2015年	ヴィタリック・ブテリン（個人） イーサリアム財団	<ul style="list-style-type: none"> ○ イーサリアム財団などが開発する、スマートコントラクトの実行が可能な分散型プラットフォーム（“イーサリアム”）のための仮想通貨として開発。 ○ いわゆるブロックチェーン技術を利用。マイナーが存在。
Ripple [XRP]	3兆551億円	2013年	リップル社 （企業）	<ul style="list-style-type: none"> ○ リップル社が開発する、外国為替・送金・決済システム／ネットワーク（“リップル”）のための仮想通貨として開発。 ○ 取引記録を確定させるためのプロセスはBitcoinなどと異なっており、いわゆるマイナーは存在しない。
Bitcoin Cash [BCH]	2兆4,693億円	2017年	Bitcoinに携わる 技術者やマイニング プールの一部	<ul style="list-style-type: none"> ○ Bitcoinが持つ技術的な課題を解決することなどを目的として、Bitcoinから派生するかたちで開発された別の仮想通貨。 ○ いわゆるブロックチェーン技術を利用。マイナーが存在。
Litecoin [LTC]	8,703億円	2011年	チャーリー・リー （個人） 他の技術者	<ul style="list-style-type: none"> ○ 「Bitcoinが金（gold）であるなら、Litecoinは銀（silver）である」というコンセプトの下、取引の処理速度などについてBitcoinを改良。より多くの発行量を有する。 ○ いわゆるブロックチェーン技術を利用。マイナーが存在。

仮想通貨と法定通貨の交換等を行う者 [仮想通貨交換業者]

- いずれの仮想通貨についても、米国ドルやTether（米国ドルにペッグしたデジタル通貨）が、通貨別取引シェアの多くを占める。日本円は、Bitcoinの取引ではシェアが大きいと見られるが、他の仮想通貨ではその限りでない。
- 大規模な仮想通貨交換業者の中には、香港などアジアに拠点を有するものが多いと見られる。

図表2 時価総額の大きな仮想通貨の通貨別取引シェア

（以下は民間ウェブサイト（CoinMarketCap/CryptoCompare）の情報に基づき作成した参考資料である。記載内容やデータの正確性・完結性を金融庁が保証するものではない。



図表3 仮想通貨交換業者の取引額

（以下は民間ウェブサイト（Coinhills/各業者ウェブサイト）の情報に基づき作成した参考資料である。記載内容やデータの正確性・完結性を金融庁が保証するものではない。

名称	拠点	取引額 [24時間]
OKEx	香港（アジア）	2,471億円
bitFlyer	日本（アジア）	1,976億円
Binance	-	1,594億円
Huobi	シンガポール（アジア）	1,337億円
Bitfinex	-	894億円
Upbit	韓国（アジア）	814億円
bithumb	韓国（アジア）	751億円
HitBTC	香港（アジア）	327億円
Bit-Z	香港（アジア）	321億円
GDAX	米国（北米）	230億円

※ 「時価総額」はCoinMarketCap<https://coinmarketcap.com/>（2018年5月17日時点）のデータ、「通貨別取引シェア」はCryptoCompare<https://www.cryptocompare.com/>（2018年5月17日時点）のデータに基づき記載。 ※ 「通貨別取引シェア」は直近24時間におけるシェア。

※ Coinhills<https://www.coinhills.com/>（All Digital Currency Exchanges Volume Ranking）（2018年5月17日時点）のデータに基づき、取引量（BTC）①とBTC/JPYレート②を用いて「取引額」①×②を計算。 ※ 「拠点」は各業者ウェブサイト（2018年5月17日時点）の情報に基づき記載（ウェブサイトで拠点を明確に確認できなかったものは「-」とした）。

仮想通貨の取引記録を確定させるための計算を行う者 [マイナー]

- マイナーは、膨大なコンピューターリソースを費やして仮想通貨の取引記録を確定させるための計算を行う。
- マイナーのうち必要な計算を最も速く完了した者が報酬（仮想通貨の新規発行分や送金手数料）を受け取ることができるため、マイナー同士の競争（「マイニング競争」）が生じている。

図表４ マイニング設備／マイニングプールの所在

以下は研究機関（ケンブリッジ大学）関係者が執筆したレポートの記載内容を仮訳したものである。記載内容やデータの正確性・完結性を金融庁が保証するものではない。

● 暗号通貨のマイニング設備の設置場所は、一般に、以下の3つの要因に基づいて決定される。

- ① マイナーが事業で利益を上げるためには、低コストで電力を得る必要がある
- ② ネットワーク上の他のノードとの間でデータを迅速に受け取り、発信するため、十分に高速なインターネット接続を確保する必要がある
- ③ マイニング装置が最適に機能するためオーバーヒートを避ける必要がある（冷却コストが低く収まることから、低気温地域への設置が潜在的に優位である理由）

● マイニングプール（注）（運営者）の58%は中国、16%は米国を拠点としている。マイニングプール運営者の所在は、そのマイニングプールにコンピューティングパワーを提供するマイナーの所在と、必ずしも一致しない。

（注）マイニングプール（Mining pool）：多数のマイナーのコンピューターリソースを結合することで、有効なブロックを発見する（報酬を受け取る）頻度や確率を向上するための枠組み。報酬はプール参加者によりシェアされる。

[Hileman, G. and Rauchs, M. (2017) *Global Cryptocurrency Benchmarking Study.*]

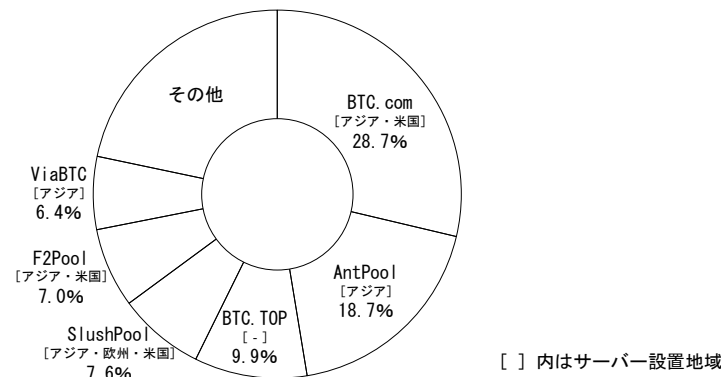
図表５ Bitcoinのハッシュレートの推移 [推計値]

以下（図表6を含む）は民間ウェブサイト（BLOCKCHAIN/CryptoCompare）の情報に基づき作成した参考資料である。記載内容やデータの正確性・完結性を金融庁が保証するものではない。

[ペタハッシュ/秒]（「ペタ」は 10^{15} （1,000兆））



図表6 Bitcoinの大規模マイニングプールのシェア [ハッシュレート分布]



※ 「Bitcoinのハッシュレートの推移」「大規模マイニングプールのシェア」はBLOCKCHAIN<https://www.blockchain.com/>（2018年5月17日時点）のデータ、「サーバー設置地域」はCryptoCompare<https://www.cryptocompare.com/>（2018年5月17日時点）の情報に基づき記載。 ※ 「大規模マイニングプールのシェア」は直近24時間におけるシェア。

仮想通貨やそれに関連する技術についての各国当局者等による指摘（1）

1. 英国中央銀行（BOE）総裁／金融安定理事会（FSB）議長 マーク・カーニー

- （暗号通貨（cryptocurrencies）は貨幣（money）の役割をどれだけ果たしているか、という問についての）
答えは、暗号通貨のエコシステム全体の機能 - （暗号）通貨自体を超えて、暗号通貨の売買ができる交換所や、新たなコインを作り出すとともに取引を検証して台帳を更新するマイナー、カスタディアンサービスを提供するウォレット提供者も含まれる - について判断されなければならない。冗長で寛容な答えは、暗号通貨は、せいぜい、一部の者だけにとって、しかも限られた範囲内で、貨幣としての役割を果たしているということだ。さらに、その場合であっても、伝統的な通貨と並行して、である。端的な答えは、暗号通貨は貨幣としての役割を果たしていないということだ。
- 暗号資産（crypto-assets）の根底にある技術、特に分散型台帳技術により、以下が可能となる。
 - データ管理の効率性を増大する
 - 複数の参加者が複製データや機能をシェアすることで中央の障害発生点を取り除き、復元力を向上する
 - 恒久的かつ変更不可能な即時記録の作成を通じて透明性（及び監査可能性）を強化する
 - 新しい情報を受け取り次第、自動的に更新され、適切な場合には支払いを行う「スマート・コントラクト」を含む、一貫したプロセスの利用が拡大する

[2018年3月2日付講演（英国中央銀行（BOE）総裁名）]

- 暗号資産（crypto-assets）は、不正活動を隠蔽するための用途や、マネーロンダリングやテロリストの資金調達に利用されるだけでなく、消費者や投資者の保護に関して多くの問題を引き起こす。同時に、暗号資産の根底にある技術は、金融システムと経済両方の効率性や包摂性を改善する可能性を有している。

[2018年3月13日付公開書簡（金融安定理事会（FSB）議長名）]

2. 国際通貨基金（IMF）専務理事 クリスティーヌ・ラガルド

- 暗号資産（crypto-assets）の裏側にある技術 - ブロックチェーン（技術）を含む - は、金融に止まらない分野を革命的に変化させることに役立つかもしれない、心躍る進展である。それは、例えば、銀行口座を持っていない人々に新しい低コストの支払手段を提供することにより、金融包摂の原動力になるかもしれない。また、その過程において、低所得国に住む何百万人もの人々に活力を与えるかもしれない。
 - 暗号資産 - あるいは暗号通貨（crypto-currencies）と呼ばれるもの - が非常に魅力的である理由が、同時に、それらを危険なものにしている。これらのデジタルな発行は、中央銀行を必要とすることなく、典型的には分散型の方法で行われる。これによって暗号資産の取引は、現金（cash）の取引とよく似た、匿名性の要素を帯びることになる。結果、マネーロンダリングやテロリストの資金調達のための新たな主要な手段となる可能性がある。
 - 暗号資産の急速な拡大や取引価格の極端に高いボラティリティ、従来型の金融の世界との不明確なつながりは、新たな脆弱性を容易に生じさせうるだろう。
- [2018年3月13日付ブログ]
- 暗号資産（crypto-assets）は、現金（cash）の利便性の一部を提供しながら、迅速かつ低コストの金融取引を可能とする。今日、一部の支払サービスは、海外送金に数日を要することなく、数時間で行っている。仮に民間が発行する暗号資産にリスクや不安定性が残るのであれば、我々が「国際金融安定性報告書」で論じるように、中央銀行がデジタル形態の通貨を提供することへの需要があるかもしれない。
 - 暗号資産の根底にある技術 - 分散型台帳技術（DLT） - は、金融市場の機能が一層効率的になることに資するかもしれない。

3. シンガポール金融管理局（MAS）長官 ラヴィ・メノン

- ブロックチェーン技術による主要な進歩は、分散型のシステムにおいて信頼を構築するという能力である。ブロックチェーン技術は、信頼できる中央組織なしに、多様な人々が協働できるようにした。（中略）分散型台帳技術（DLT）は、多くの産業や経済活動を転換する可能性を有している。

[2017年10月9日付講演]

- 残念ながら、暗号トークン（crypto tokens）の匿名性が、それらを違法取引の促進に適したものにしている。（中略）暗号トークンが世界中で投機熱に火を付けた。桁外れに高い価格の危険なサイクルが、ますます多くの投資家を引き込み、更に急激な価格上昇に拍車をかけた。

[2018年3月15日付講演]

4. 欧州中央銀行（ECB）総裁 マリオ・ドラギ

- デジタル通貨（digital currencies）について言えば、ユーロ地域における利用量、利用者、その利用が実体経済に与える影響を見ると、それらはすべて、依然として非常に限定的であると考えられる。それは、まだ、中央銀行にとってのリスクを構成しうるものではない。しかしながら、より広く、（デジタル通貨に）使用されうるデジタル技術や分散型台帳技術（DLT）、その他の技術は、確かに、中央銀行や監督当局の興味を引くべき進展である。

[2017年11月20日付講演]

- ビットコインや他のデジタル通貨（digital currencies）は規制を受けておらず、従って非常にリスクの高い資産と見られるべきである、ということを理解しなければならない。仮想通貨（virtual currencies）は高いボラティリティにさらされており、それらの価格はまったく投機的である。銀行は、デジタル通貨を自身のポートフォリオに保有することのリスクを、適切に計測すべきである。

[2018年2月5日付声明]

5. 世界銀行グループ・国際金融公社（IFC）がとりまとめた公表物

- ラテンアメリカやアフリカの一部地域においてそうであるように、新興市場に関しては、（ブロックチェーン技術・分散型台帳技術を活用した金融の）エコシステムの採用に適しているように見える。（エコシステムは、法定）通貨の不安定性や政治リスクといった状況における、ビットコインや他の暗号通貨（Crypto Currency）を通じたヘッジ戦略のみならず、とりわけ、金融の面において排除されたセグメントの役に立つという、高い需要により推進される。金融の面において発展していない市場は、ブロックチェーン（技術）によるデジタルウォレットやモバイルペイメントがもたらす金融包摂に注目している。

[Niforos, Marina (2017) “Blockchain in Financial Services in Emerging Markets Part I: Current Trends,”
Fresh Ideas about Business in Emerging Markets.]

- アフリカ：人口の70%が銀行口座を有していないサブサハラ・アフリカは、伝統的な支払手段の代替として、ブロックチェーン（技術）に基づくソリューションを導入する大きな潜在的可能性を有している。頻繁に生じる政治的動乱の歴史や、高い通貨リスク、資本規制を伴う経済は、個人・家計が、取引の執行における潜在的なリスクへの恐怖を克服し、（伝統的な）システムの非効率性を迂回することを可能とするソリューションを採用する格好の場でもあるのだ。
- ラテンアメリカ：ラテンアメリカは、アフリカと比較して銀行口座を有していない人口の比率は低い（世界銀行フィンデックスによれば49%）が、周期的な政治的変動・（法定）通貨の変動にさらされており、現地通貨に対する信用は弱体化している。加えて、違法な活動（麻薬の密売やマネーロンダリングに関する活動を含む）が浸透していることにより、地域経済に対するディリスキング（de-risking）効果が増大し、伝統的な金融機関はコンプライアンス要件の強化や費用の増大を理由に、市場から撤退してきた。

[Niforos, Marina (2017) “Blockchain in Financial Services in Emerging Markets Part II: Selected Regional Developments,”
Fresh Ideas about Business in Emerging Markets.]

「事務ガイドライン」における仮想通貨交換業者の分別管理に係る監督上の着眼点

- 「事務ガイドライン」においては、仮想通貨交換業者における分別管理の方法に関して、例示として、以下のような着眼点を列挙している。
 - 利用者の金銭の管理について、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、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か。また、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、速やかに当該不足額を解消しているか。
 - 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か。また、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、速やかに当該不足額を解消しているか。
 - 仮想通貨の分別管理については、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か。
 - 利用者の仮想通貨について、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か。