CRYPTOASSETS GOVERNANCE TASK FORCE

暗号資産カストディアンのセキュリティ対策についての考え方（案）

Cryptoassets Governance Task Force[1]

2019年1月15日

本ドキュメントはIETFにおいて、インターネットドラフトとして標準化提案されます。
本ドキュメントに対するすべてのコメントはIETF知的財産権ポリシー(NOTE WELL)に同意したものとみなされます。
Be aware that all contributions to our work fall under the "NOTE WELL" terms therein.

[1] https://cgtf.github.io

本書の目的

この文書は暗号資産カストディアンが利用者の資産を保護する目的としてセキュリティを検討するための推奨事項を整理するものである。保護すべき資産のうち、特に暗号資産の署名鍵は従来の情報システムとは異なる特徴があり留意が必要である。本書では、暗号資産カストディアンが署名鍵を適切に管理し、不正な取引を防止するために留意すべき点を特に重点的に述べる。本書で対象とする暗号資産カストディアンの基本モデルは5章で示す。この基本モデルとは別の形態のシステム、例えば、利用者が提示する署名鍵を事業者が管理する業態（例：オンラインウォレット）等については別の補完的な文書あるいは本書の後の改訂で扱うものとする。

1. 本書のスコープ

本書が対象とする事業者は、暗号資産で使用される署名鍵を管理する暗号資産カストディアンである。暗号資産カストディアンにより、署名鍵の管理を他の事業者へ委託する場合も含む。その場合、署名鍵の管理を委託された事業者についても、本書が示す推奨事項の相当箇所が適用されるものと考える。
本書は以下の対象に対する脅威やリスクに関する考察を含む。

- 顧客（利用者や他のカストディアン）に対して、顧客の仮想通貨アドレスから、業者が署名鍵を管理する業者の仮想通貨アドレスに、仮想通貨の移転を受けて管理する方法で、暗号資産のカストディ業務を提供する暗号資産カストディシステム
- 暗号資産カストディシステムが管理する資産情報（暗号資産の署名鍵を含む）
- 暗号資産カストディシステムのセキュリティ対策の不備により及ぼしうる社会的な影響

本書は以下についてはスコープ外とする。

- 暗号資産カストディアンが日常業務に用いるシステムに対するセキュリティ対策
- 暗号資産の仕組みを提供するブロックチェーンや分散台帳自体に対するセキュリティ対策
- 暗号資産カストディアン自身の経営リスク
- 利用者と暗号資産カストディアンの資産の分離に関する具体的な要件

2 参照規格

ISO/IEC 27001:2013 (JIS Q 27001:2014) Information technology -- Security techniques -- Information security management systems -- Requirements
ISO/IEC 27002:2013 (JIS Q 27002:2014) Information technology -- Security techniques -- Code of practice for information security controls
ほかISO/IEC 27000シリーズ

3 用語

コイン
暗号資産

入庫
他のアドレスから対象のアドレスに対する暗号資産の移転。

出庫
自己の管理するアドレスから他のアドレスに対する暗号資産の移転。

ウォレット
暗号資産の検証鍵と署名鍵の鍵ペア、並びに検証鍵から生成されるアドレスを管理する機構である。ソフトウェアによるウォレットの実装を本文書ではウォレット実装と呼ぶ。

- ホットウォレット
  オンラインでネットワークに接続され、鍵が活性化されており、自動処理によって仮想通貨を出コインできるウォレットのことである。
- コールドウォレット
  通常時はネットワークから切断されて鍵が非活性化され、オペレーターの明示的な操作がない限りは、出コインができないウォレットのことである。出コインの頻度は制限されている。

ホットウォレットとコールドウォレットの間には、オンラインだがトランザクションの署名時などに手動での操作が必要なウォレット、オフラインだが運用が自動化されているウォレットなど、様々な中間的な形態が考えられ、ウォームウォレットなどと呼ばれることもある。

	自動処理	手動操作
オンライン	ホットウォレット	（ウォームウォレット等）
オフライン	（ウォームウォレット等）	コールドウォレット

フォーク
フォークとは、ブロックチェーンが分岐することである。ブロックチェーンの分岐は、偶発的に起こる場合と、仕様変更によって起こる場合がある。

アクシデンタルフォーク：アクシデンタルフォークとは、偶発的にほぼ同時間にブロックの採掘が行われて、一時的に複数のチェーンが併存している場合を指す。日常的に発生し、re-orgによって最も長いチェーンに収束する。

ソフトフォーク：ソフトフォークとは、ブロックチェーンの仕様変更によって生じる分岐のうち、採掘者の実装に影響する場合があるが、ウォレット実装には影響しない。

ハードフォーク：ハードフォークとはブロックチェーンの前方互換性のない仕様変更によって生じる分岐で、採掘者に加えてウォレット実装に影響する場合がある。

大多数のノードがハードフォークに追随することで仕様変更に留まる場合と、仕様の移行について開発者間の合意が成立せず、永続的に複数のチェーンが併存し続ける場合があり、後者をとくにスプリット（分裂）と呼ぶ。代表的なスプリットの例としては2016年のThe DAO事件におけるEthereumとEthereum Classicの分裂、2017年のBitcoinとBitcoin Cashとの分裂などがある。分裂によって生まれた新しいコインのことをフォークコインと呼ぶ。

操作員と管理者について

- 操作員
  通常業務として権限に基づいて定型的な業務をこなす要員である。
- 管理者
  システムの設定を変更できる権限を持って、システムの運用保守を実施する要員である。相互けん制の観点から、管理する対象によって、異なる権限を持った管理者が存在する。

暗号資産カストディ業務 (Cryptoassets Custody Service)
暗号資産の現物を管理する業務

暗号資産カストディアン (Cryptoassets Custodian)
暗号資産カストディ業務を運営する者

暗号資産カストディシステム (Cryptoassets Custody System)
暗号資産カストディ業務を担う情報システム

暗号資産交換所 (Cryptoassets Exchange)
法定通貨と暗号資産の交換、暗号資産同士の交換を行う機能

暗号資産交換業者 (Cryptoassets Exchange Service Provider)
暗号資産交換所を運営する事業者

秘密鍵 - Secret Key
私有鍵 - Private Key
署名鍵?
署名用秘密(私有？)鍵 (Private Signature Key:NIST, Signature Key:英訳)

4 略語集

HD - Hierarchy Deterministic (wallet)
DEK - Data Encryption Key
KEK - Key Encryption Key

5 暗号資産カストディシステムの基本事項

5.1 本章について

この章では、本書が対象とする暗号資産カストディシステムに関する基本的な構成要素や運用フロー、暗号に用いる鍵、ブロックチェーン・分散台帳の特性についてや運用フロー、暗号に用いる鍵、ブロックチェーン・分散台帳の特性について記載する。

5.2 暗号資産カストディシステムの基本モデルと各機能的要素

本書が想定する暗号資産カストディアンの基本モデルを図5-1で説明する。

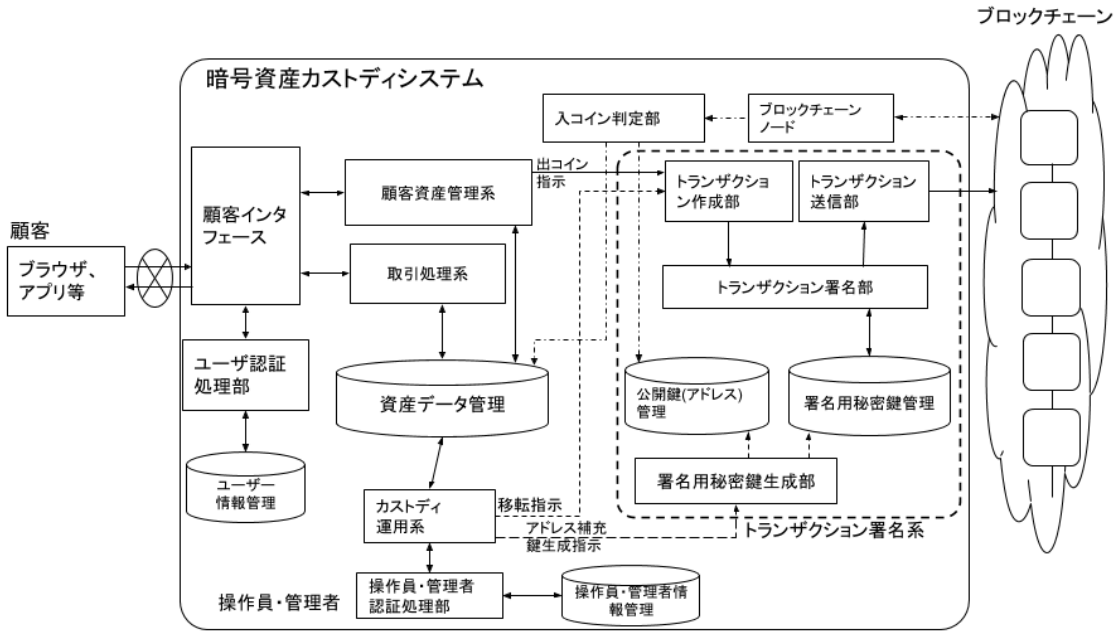

図5-1 暗号資産カストディシステムの基本モデル

機能的要素	概要
顧客インタフェース	顧客に対してログイン、口座管理（入出金指示など）、売買や移転指示などの画面表示や入力手段を提供する。WebアプリやAPIなど。
ユーザー認証処理部	暗号資産カストディシステムへのログインのためのユーザー認証の処理を実行する。
ユーザー情報管理	ログインに必要なIDとユーザー認証処理に関わる情報（例:パスワードの照合情報）を管理する。
顧客資産管理系	顧客の口座を管理する機能群。入金や出金（出コイン）の指示を受け、指示に応じた処理を行う。資産データ管理を参照・更新する。
ブロックチェーンノード	ブロックチェーンの他のノードに接続しブロックチェーンデータを取得する。
入コイン判定部	ブロックチェーンに格納されたトランザクションをチェックし、指定アドレスに入コインされていることを確認する。入コインされた内容に基づいて資産データを更新する。
取引処理系	顧客からの売買や移転指示を受け、暗号通貨の売買や移転に関わる処理を行う機能群。資産データを参照・更新する。

資産データ管理		法定通貨や暗号通貨の保有額を管理する。トランザクション署名に用いる署名鍵は含まない。顧客ごとに、取引所の資産と分離して管理される。
トランザクション署名系	トランザクション作成部	顧客資産管理系やカストディ運用系からの指示に基づいて、ブロックチェーンに送信するトランザクションを作成する。
	トランザクション送信部	署名済みのトランザクションをブロックチェーンに送信する。ブロックチェーンの他ノードと接続する。
	トランザクション署名部	指示されたトランザクション内容と署名鍵（のIDやアドレス）に基づいてデジタル署名を作成する。
	検証鍵(アドレス)管理	署名鍵とペアとなる検証鍵、あるいはアドレス（検証鍵や署名鍵から算出された値）などを管理する。
	署名鍵管理	暗号資産の署名鍵（トランザクションの署名に用いる鍵）を管理する。
	署名鍵生成部	署名鍵の生成を行う。生成した鍵は署名鍵管理へ、検証鍵やアドレスはアドレス管理へ登録される。
カストディ運用系		カストディの操作員や管理者が用いる機能群。管理者からの操作に基づいて、新たな署名鍵の生成や、暗号通貨の移転を指示する。
操作員・管理者認証処理部		操作員・管理者の認証を行う。
操作員・管理者情報管理		操作員・管理者の認証処理に係る情報を管理する。

各機能的要素は論理的に機能を区別するために定義したものであり、実際のシステム上の配置を示したものではない。

例えば、実際のシステムでは公開鍵(アドレス)と資産データ管理は一体のデータベースで管理されている場合もある。また、複数の機能的要素を一つにまとめて実装している場合や、トランザクション署名系の各機能的要素が顧客資産管理系と一体になっている場合、トランザクション署名系が別のシステムとして稼働している場合も考えられる。

また、bitcoin-coreのような既存の実装を用いている場合には、ビットコインウォレットはトランザクション署名系の機能をまとめて一つの実装として提供しているとも考えられる。

なお、トランザクション署名系の機能が外部の委託先のサーバーで提供されるという形態のように、一部の機能が遠隔の委託先で提供されている場合も考えられる。

5.3 トランザクション送信に至るまでのフロー

[入金フェーズ]

1. 顧客がカストディアン指定の銀行口座に送金する。
2. カストディは銀行口座に入金されたことを確認し、顧客の資産情報に反映させるために、資産データ管理部を更新する。

[入コインフェーズ]

1. 顧客がカストディアン指定のアドレスに暗号資産を移転する。移転は顧客が使用している暗号資産のウォレット等のツールやサービス（他のカストディアンやWebウォレットなど）を通じて行う。
2. 交換所は入コイン判定部で指定のアドレスに暗号通貨が移転されたことを確認し、顧客の資産情報に反映させるため、資産データ管理を更新する。

[取引フェーズ]

1. 顧客が顧客インタフェースにアクセスし、取引指示を行う。
2. 取引指示は資産データ管理の情報に基づき取引処理系によって処理される。取引処理系で処理された売買等の結果は資産データ管理に反映される。

[顧客からの出コイン指示]

1. 顧客が顧客インタフェースにアクセスし、自身が有する暗号資産をあるアドレスへ移転させる指示を行う（出コイン指示）。
2. 出コイン指示は顧客情報管理系で処理され、その後、指示内容に基づいてトランザクション作成部でトランザクションのメッセージ（移転先アドレスや仮想通貨の額など）が作成される。
3. トランザクションのメッセージはトランザクション署名部によってデジタル署名が付与される。
4. デジタル署名付きのトランザクションは、トランザクション送信部からブロックチェーンネットワークの各ノードに配信される。

[カストディ運用系からの移転指示]

1. 管理者がカストディ運用系のインタフェースを通じて、暗号資産をあるアドレスへ移転させる指示を行う。例えば、暗号資産の管理上の理由から、カストディシステム内で管理しているアドレス間で移転することが考えられる。
2. 管理者からの移転指示は、カストディ運用系での処理を通じて、その後、出コイン指示の手順2.～4.と同様に行われる。デジタル署名付きのトランザクションがブロックチェーンネットワークの各ノードに配信される。

5.4 署名や暗号に用いる鍵の種類について

5.4.1 鍵の種類について

分類	説明
署名鍵	トランザクションへのデジタル署名に用いる鍵。
検証鍵	トランザクションへのデジタル署名の検証に用いる鍵。トランザクションの宛先を指定するためのアドレスは検証鍵から生成されるユニークな値である。
署名鍵KEK	署名鍵を秘匿するために用いられる共通鍵暗号方式の署名鍵。
マスターシード	決定性ウォレットで署名鍵を生成するためのシード（ランダムな数値など）。

5.4.2 鍵生成と利用のフロー

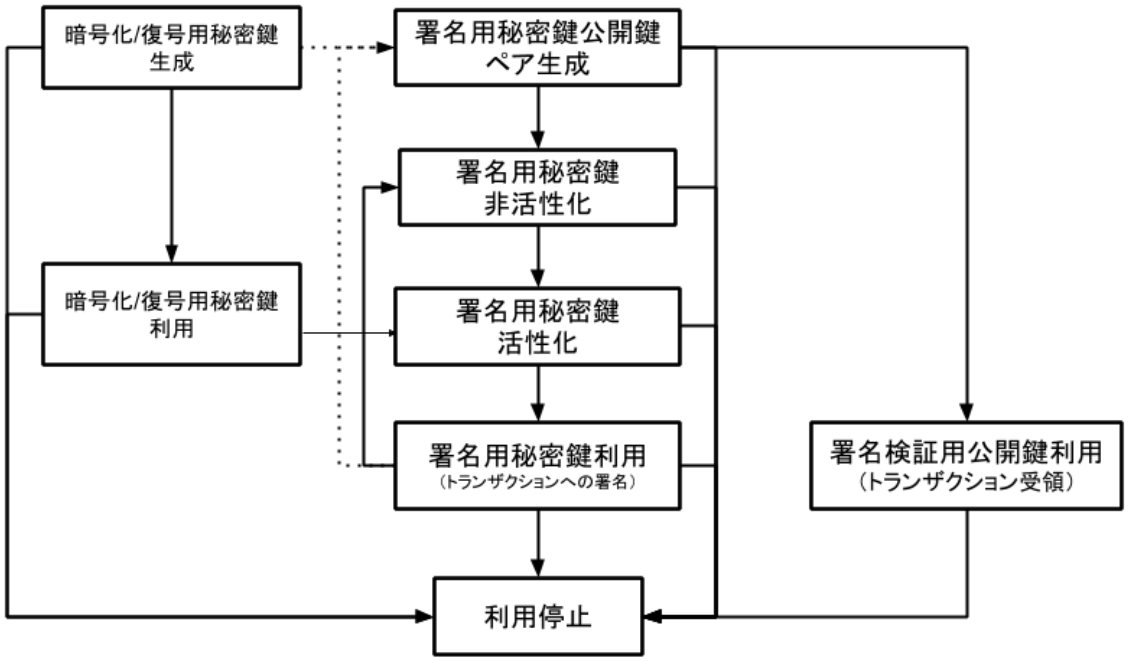

図5-2 署名鍵、署名検証用公開鍵、暗号化/復号署名鍵のライフサイクル

署名鍵と署名検証用公開鍵のペア（以降、署名用鍵ペア）を作成したのち、署名検証用公開鍵からトランザクションを受領するためのアドレスが生成される。暗号資産の送付元に対してこのアドレスを通知することで、送付元はそのアドレスに対して暗号資産を送ること（移転すること）ができる。そのアドレスが保有する暗号資産を別のアドレスへ移転する場合には、そのアドレスに対応する署名鍵で移転指示を記したトランザクションに署名する。

署名鍵の非活性状態とは、署名鍵が秘匿された状態で図5-1の署名鍵管理で保管されていることを想定している。
署名鍵の秘匿方法としては暗号化/復号用署名鍵（例えば、パスフレーズ等）による暗号化がある。図5-2では暗号化/復号用署名鍵によって暗号化されている状態を想定している。

署名鍵が復号用署名鍵によって復号され、署名演算が行える状態になっていることを活性状態と呼んでいる。活性化は図5-1のトランザクション署名部の機能として実行されることを想定している。

前述したように署名用鍵ペアを生成したあと、署名鍵はそのアドレスが保有する暗号資産を他のアドレスへ移転するまで必要としない。そのため、署名用鍵ペアを生成したのち、公開してよい署名検証用公開鍵やアドレスのみをオンライン上に置き、署名鍵をオフラインで安全に管理するという手法もある(7.3.6.2 参照)。

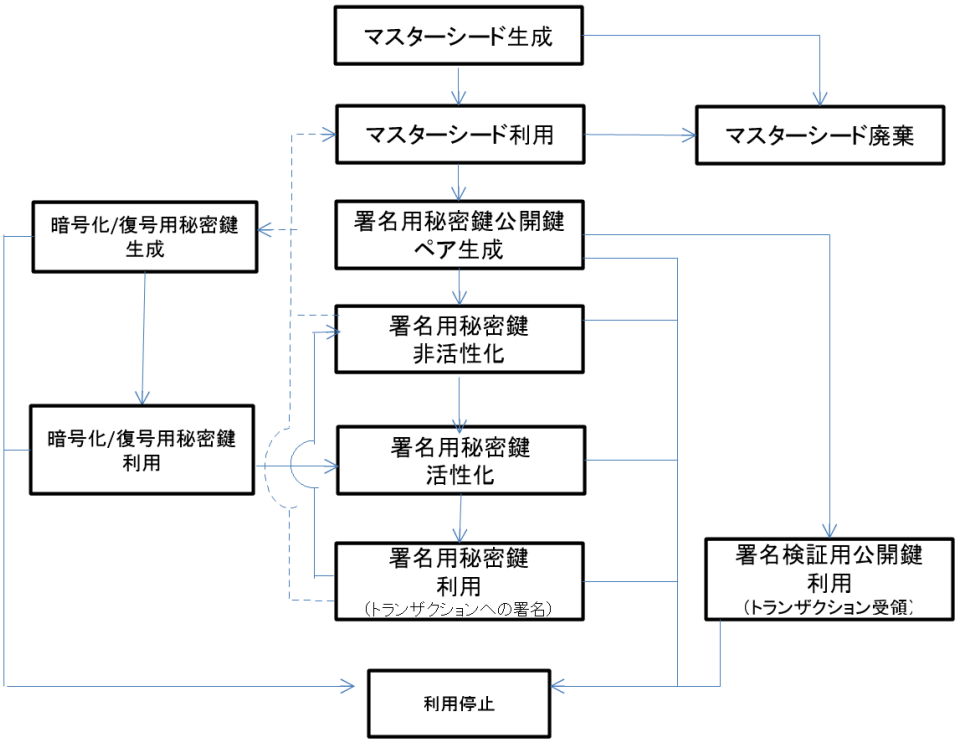

図5-3 決定性ウォレットを用いた場合のライフサイクル

決定性ウォレットとは一つのマスターシードを生成し、そのマスターシードから複数の署名用鍵ペアを生成する仕組みである。マスターシードをバックアップしておきリストアすることで、マスターシードから各署名用鍵ペアを再生成することができる。その反面、マスターシードの盗難にあった場合には、そこから派生して生成された全ての署名用鍵ペア（アドレス）が保有する暗号資産が盗難されうる。また、マスターシードを紛失した場合にも、そこから派生する署名用鍵ペアを再生成することが出来なくなる。決定性ウォレットの拡張として、階層型決定性ウォレット(HDウォレット)がある。HDウォレットの場合は、マスターシードから親となる鍵ペアを作成し、その鍵ペアから派生した子の鍵ペアを作成する。さらに、子の鍵ペアから孫の鍵ペアを作成するように階層構造で連鎖した鍵ペアを作成することができる。子の鍵ペア作成は、親となる鍵ペアから作成することができるため、マスターシードにアクセスする必要がない。暗号資産の中には、HDウォレットのマスター鍵に触れることなく新たな公開鍵を生成する機能については対応していない（原理的にできない）通貨ある。本書ではセキュリティ管理策の中で主に署名鍵の管理について言及しているが、マスターシードによる運用を行っている場合には、マスタシード署名鍵と同等かそれ以上のセキュリティ対策を行う必要がある。

5.4.3 複数の鍵の利用について

一般的な暗号資産の利用場面において、暗号資産の1ユーザが1つのアドレスを使うケースもあれば、1ユーザが多数のアドレスを使うケースもある。暗号資産カストディアンにおいても暗号資産の種類や管理の方法によって、管理対象となるアドレスおよび鍵ペアの数は異なる。例えば

RippleやNEMのように、トランザクションへのタグ付けができる暗号資産であれば、暗号資産カストディアンが1つのアドレスを複数の顧客に対応づけて管理し、個々のトランザクションに個別のタグ付けを行うことで顧客を識別する方法もある。一方、トランザクションのタグ付けが困難な暗号資産については、顧客ごとに個別のアドレスを割り当てて管理することになり、管理すべきアドレスおよび鍵ペアの数は膨大になりうる。また、暗号資産の種類だけでなく、ホットウォレットやコールドウォレットによる管理、暗号資産の額に応じた分散管理など、リスク評価の上で複数のアドレスおよび鍵ペアを使い分けることも考えられる。
なお、一般的な暗号資産の利用において、一度使った鍵ペアは再利用しないことを推奨されていることもある。しかし、これは個人利用において、取引を特定されにくくする目的が主であり、暗号資産カストディアンにおいて実効性や実用性がある手法とは考えにくい。暗号資産カストディアンではリスク評価と管理目的を考慮したうえで適切な管理策を実施することが必要である。

5.4.4 鍵の利用停止と破棄における注意点について

図5-2の鍵の利用停止はあくまでも交換所内での運用であり、暗号資産の仕組み上において一度送信したトランザクションの取消などを行うことはできない。また、利用停止以降においても署名鍵を破棄することが難しい場合がある。例えば、顧客が誤って、使用停止したはずのアドレスに対して入コインしてしまうこともあり、誤って入コインしたアドレスから元の顧客にコインを返却するためには、その署名鍵が必要となる。このような事態などを想定し、署名鍵の破棄は慎重に検討する必要がある。

5.5 ブロックチェーン・分散台帳における暗号資産の特徴について

5.5.1 本節について

ブロックチェーン・分散台帳を用いた暗号資産の取り扱いにおいて、一般的な情報システムにおける暗号の利用と比べて、より注意を必要とする機能や異なる特徴がある。6章以降に述べるリスク評価、それに基づくセキュリティに関する要件や対策を検討する場合には、これらの特徴に留意する必要がある。

5.5.2 署名鍵の重要性

5.3節で記したように、署名鍵を用いてトランザクションに署名することで、（署名鍵にバインドされたアドレスから）他のアドレスへ暗号資産の移転を指示することができる。このトランザクションが一度ブロックや台帳のデータに書き込まれ仮想通貨の移転が承認されてしまえば、元に戻すことや、失効手続き等により移転を無効化することは難しい。この性質は、金融機関のペイメントネットワークにおいて、送金の過程で複雑な事務手続きを要し、仮に不正な送金が発生しても、送金が着金するまで時間を要したり、送金の途中に処理を取り消し、組み戻すことができる場合があることとは対照的である。また、仮想通貨において署名鍵が消失した場合には、その署名鍵に対応したアドレスが保有する仮想通貨を他へ移転することはできなくなる場合がある。このような不可逆な性質を有する仮想通貨においては署名鍵の盗難や不正利用、消失に対して、より多くの注意を払う必要がある。

5.5.3 実装の多様性

暗号資産はビットコインをはじめとして様々なものが存在する。仕様も暗号資産ごとに大きく異なり多様である。例えば、ハッシュ関数や署名方式などの暗号アルゴリズム、トランザクションの生成方法や送信方法、署名鍵を保護するウォレットの実装方法などの違いがある。このような仕様の違いから、特定の暗号資産には有効な対策手段が、別の暗号資産の仕様では実施できないということも起こりうる。また、現状の暗号資産の過熱的な動向から、新たな暗号資産の登場や、既存の暗号資産の仕組みの機能拡張や仕様変更のスピードはとても早い状況にある。

5.5.3.1 暗号資産の暗号アルゴリズムについて

暗号資産では、安全性について十分にレビューされていない新しい暗号アルゴリズムが採用されることもある。通常の暗号利用において、設計者は科学的に検証され、数学的に安全性を証明され、公的機関によって承認された暗号アルゴリズムを利用する場合が多いが、暗号資産の設計者はしばしば未成熟で検証されていない暗号アルゴリズムを採用することがある。これは安全性証明や公的機関による承認などには時間がコストがかかること、一方技術として成熟度が低く、また競争と進化の著しいブロックチェーンにおいては、他の暗号資産との差別化やブロックチェーン固有の技術最適化などのために必要となるからである。これらのアルゴリズムは適切にレビューされた実装が存在しない可能性や、後からぜい弱性が発見され、危たい化するリスクが成熟したアルゴリズムと比べて高い。

5.5.4 ブロックチェーンが分岐する可能性

ビットコインに代表されるProof of Work等を用いたブロックチェーンでは、ソフトウェアの仕様変更などによりチェーンが一時的に分岐したり、分岐した状態が解消される（リオーガナイズ）といった状態が生まれうる。また、別のケースとして、開発コミュニティの分裂等により、ある時点からブロックチェーンが分裂し別々の暗号資産として運営されることもある。世の中には多種多様な分岐 (fork)、分裂 (split) があり、そのすべてに対応することは困難な場合があり、リスクに応じて対応策を検討する必要がある。

5.5.4.1 Re-orgによるロールバック

Re-orgによりチェーンが破棄される場合、破棄されたチェーンに含まれていたトランザクションの履歴は失われることになる。その場合、Re-orgの期間内に破棄されたブロック上のトランザクションはメインチェーンに反映されない場合がある。

5.5.4.2 分裂した暗号資産の扱い

ビットコインやイーサリアムなどの事例のように、ブロックチェーンが分裂し別の暗号資産として運営されていくことがある。分裂後の暗号資産も元の暗号資産と同じソフトウェアから派生している場合が多く、分裂する直前までのチェーンも同じデータとなっている。その性質を利用すること

で例えばリプレイ攻撃といったことが可能になる。リプレイ攻撃とは、元の暗号資産で使われたトランザクションを、トランザクション送信者には知らせることなくフォークコイン側でも再送し、結果としてフォークコインを不正に取得するといった攻撃である。このリプレイ攻撃は、トランザクション送信者側がフォークコインの発生を監視し、フォークコイン側に対しては自身の別アドレスにコインを戻すトランザクションを先んじて送付するなどの対策が必要となる。

その他、暗号資産カストディアンが保有する暗号資産にフォークコインが発生した場合、カストディアンのシステム内でその分裂後の暗号資産をカストディアンの利用者に割り当てない限り、利用者は利用できないという問題もある。

5.5.5 未承認トランザクションに対するリスク

5.5.5.1 本小節について

暗号資産の移転を指示するトランザクションをブロックチェーンのノードに送信しただけで暗号資産の移転が即座に反映されるわけではない。トランザクションが承認されるには、ある時間ごとに作成されるブロックに格納され、大多数のノードに受け入れられる必要がある。次に述べるような理由でトランザクションが承認されたことを確認しにくい事態も発生しうる。

5.5.5.2 承認されなかったトランザクションの扱い

分散台帳を用いる暗号資産には、トランザクション送信者がトランザクションを他ノードが処理するための費用(トランザクション手数料)を上乗せしたうえでトランザクションを送信するものがある。このトランザクション手数料はブロックを作成することでノードが獲得できるもので、トランザクション手数料が高いものほどブロックに格納されやすい（トランザクションをより早く承認されやすい）という性質をもつ。暗号資産カストディアンからブロックチェーンに送信するトランザクションのトランザクション手数料が少ない場合には、トランザクションの承認に時間がかかる、あるいは、承認されずに時間切れとなる恐れもある。トランザクション手数料が原因となる場合以外にも、5.5.4.1節のように一時的なチェーンの分岐により、一度承認されたはずのトランザクションが未承認状態になり暗号資産の二重使用が可能となる事象もある。実店舗におけるペイメントなど、即座に暗号資産の移転が求められる利用場面では、トランザクションが承認されたことを確認する時間を十分に取ることが難しいこともあり、未承認トランザクションのリスクを想定しておく必要がある。
この記述はProof of Work型の暗号資産を念頭に置いているが、実際にはそれぞれの暗号資産の特徴を理解し、リスクを洗い出した上で、正常系・異常系に対して適切に対策をとる必要がある。

5.5.5.3 仮想通貨の仕様や実装のぜい弱性から生じるトランザクションの障害

正確には未承認トランザクションのケースとは異なるが、ビットコインの過去の事例としてトランザクション展性(Transaction Malleability)と呼ばれるぜい弱性があった。このぜい弱性によりトランザクションを中継するノードに悪意がある場合、トランザクションを不正に操作することで、ブロックに格納されているトランザクションを発見できなくする（トランザクションのIDで検索できなく

する）ことも可能になる。その結果、承認済トランザクションをあたかも承認されていないように見せかけることが可能となり、取引相手から再度、暗号資産移転のトランザクション送信を要求することで二重取りする、という攻撃が可能となる。この攻撃は、トランザクションをノードに送信した以降に行われるため、送信者側が送信前にあらかじめ対策できないという点が特徴的である。トランザクション展性に関しては、現在のビットコインではSegWitの利用によって回避することが可能となった。しかし、この事例からの教訓として、ビットコインやその他の暗号資産の別のぜい弱性による障害や脅威に関して、暗号資産のトランザクション送信者や受信者となる暗号資産カストディアンだけでは有効な防御策が立てにくい場合もあることも想定しておく必要がある。

6 暗号資産カストディアンのリスク

6.1 本節について

ここでは、暗号資産カストディアンとして留意すべき主なリスクを、暗号資産カストディシステムに関するもの（6.2節）、暗号資産カストディアンのコントロール外にあるブロックチェーンなど外的要因によるもの（6.3節）に分類して列挙していく。暗号資産カストディシステムに関するリスクでは脅威と因子、脅威をもたらすアクターの観点で整理を行う。ブロックチェーンなど外的要因によるリスクでは、起こりうるインシデントの観点で整理を行う。これらのリスクの中には5.5節で述べた暗号資産の特徴や性質に起因するものがある。
その他、事業者毎に異なるシステムや運用に固有のリスクもあり得る。各事業者は、本節で示すリスクを参考にしつつ、事業者毎に異なるシステムの利用や運用を踏まえた上で対処すべきリスクを洗い出す必要がある。その後、各リスクが事業に与える影響などを評価することにより、管理策の優先度を決定することが望ましい。

6.2 暗号資産カストディシステムに関するリスク

ここでは暗号資産カストディシステムが保持する情報資産に対する代表的なリスクを挙げる。5.2節の基本モデルの中で、顧客の資産を保護する観点から特に重要な情報資産として署名鍵と資産データに着目する。

署名鍵の管理および運用が安全でなければ、不正なトランザクションを作成し分散台帳のノードに送信することも可能になる。一度、不正なトランザクションがノードに送信され、ブロックチェーンに書き込まれてしまえば、トランザクションを取り消すことはほぼ不可能である。したがって、不正なトランザクションが作成されないための事前対策が特に重要となる。署名鍵の管理や不正なトランザクション作成に関わるリスクを慎重に評価したうえで適切な安全策を検討する必要がある。また、署名鍵の消失についても考慮が必要である。署名鍵が消失した場合には、その署名鍵に対応するアドレスに蓄えられている暗号資産を使用することができなくなる。署名鍵に関するリスクについては5.2節の基本モデルを元に署名鍵とそれを取り巻く環境を含めて6.2.1節で考察する。

資産データについては、データの内容やデータ形式、管理形態、処理の詳細は暗号資産カストディアンごとに多様であるため、この文書ではモデルをより抽象化して考察している。保護すべき資産データの共通的な内容としては、顧客が暗号資産カストディアンに預け入れている暗号資産や法定通貨の総額、暗号資産カストディアンが保有する暗号資産や法定通貨の額、顧客の口座番号や暗号資産のアドレスなどが考えられる。このような資産データが悪意あるものによって不

正に書き換えられた場合、顧客に損害を与えることや、暗号資産カストディアンの業務に支障をきたすことにもなる。資産データについては6.2.2節で考察する。

トランザクション署名の署名鍵と資産データといった重要な情報の保護の観点以外にも、顧客が自身の資産を円滑にコントロールできるようにシステム停止などのリスクも配慮する必要がある。システム停止に関するリスクは6.2.3節で考察する。

本節で挙げた情報やリスク以外にも、暗号資産カストディシステム毎に個別に抱えるリスクや外部事業者との連携におけるリスクも考えられる。暗号資産カストディアンの実際のシステムに対して詳細なリスク評価を行う必要がある。

6.2.1 署名鍵に関するリスク

暗号資産の移転において、署名鍵の持つ役割とリスクは極めて大きい。その理由としては単に暗号資産の移転(transfer)を可能とするにとどまらず、暗号資産が有する匿名性により消失、漏えい・盗難に対し、署名鍵の失効(revocation)やトランザクションのロールバックによる対処が困難という性質による。本項では、署名鍵の消失、漏えい・盗難や、価値の毀損を招き得る不正利用のリスクについて示す。また、関連して署名鍵を扱うウォレットを導入する際のリスクとしてのサプライチェーンリスクなどについても示す。

6.2.1.1 署名鍵のリスク分析

リスク分析は、想定する脅威やシステム構成など脅威モデリングなどによってその結果は様々に異なる。本節では、一例として以下の想定にもとづくケーススタディを示す。

ここでは、署名鍵に関する脅威と、その脅威を起こし得る因子を表6-1のように想定した。また、5章の図5-1にもとづき署名鍵に入力を与える以下のものをアクターとして想定した。

表6-1　署名鍵の脅威とその因子、アクター

脅威	脅威の因子	アクター
● 消失 ● 漏えい・盗難 ● 不正利用	● 誤操作 ● 正当者の悪意ある行為 ● 正当者へのなりすまし ● 部外者の悪意ある行為 ● システムの意図しない挙動	● カストディ運用系 ● トランザクション署名系 ● 顧客資産管理系 ● 入コイン判定部

脅威の因子は、脅威となり得るものを大別したものであり、本稿では以下のように整理している。

誤操作：システムの正当な利用者(管理者なども含む)による意図せずに操作を示す。例えば、本来10万円分を出コインする操作を、誤って100万円分を出コインしてしまう操作など。

正当者の悪意ある行為：システムの正当な利用者(管理者なども含む)が、悪意を持って行う行為。例えば、内部不正による署名鍵の盗難や不正利用など。なお、ここでは因子となり得る行為の識別が目的であり、行為の目的やインセンティブなどは問わない。

正当者へのなりすまし：システムの正当な利用者以外が、正当な利用者認証情報を盗用して何かしらの操作を行う行為[2]。例えば、外部の攻撃者が顧客になりすまして暗号資産の売買・移転

[2] 正当な利用者認証情報の盗用によらないなりすまし行為(例えば権限昇格)や、認証情報の盗用行為そのものについては、次の「部外者の悪意」として扱う。

指示を行う、あるいは操作員や管理者権限を持たない内部犯が操作員・管理者権限でシステムにアクセスして資産移転指示やトランザクション生成・署名などを不正に行うなど。特に、ユーザについては初回登録時に本人になりすまして認証情報を盗用する可能性も十分に考慮する必要がある。

部外者の悪意ある操作：部外者のなりすまし以外の方法による悪意を持ったシステムに対する操作。例えば、システムのぜい弱性を利用して外部から不正侵入する、カストディ管理者への標的型メールなどを介してカストディシステムにマルウェアを混入させ外部から署名鍵(ないしトランザクション作成など)を不正に遠隔操作するなど。

システムの意図しない挙動：操作の意図とは無関係に、システムが設計者ないし運用者の想定しない挙動をすること。例えば、カストディ運用系システムのバグにより署名鍵が漏えいする、操作内容に関わらず間違った額のトランザクションが作成されるなど。

このうち、盗難と不正利用は明確な悪意を持った因子によってのみ発生し得る脅威と捉える[3]。この結果、想定すべきリスクは表6-2に示す。なお、正当者の操作指示と異なる動作や人間系の誤操作においても、複数の因子が重なった結果、盗難や不正利用が発生することは考え得る[4]。いずれも盗難や不正利用の管理策においてカバーされ得るものであり、ここではあくまでも分析のための整理である点に注意されたい。

表6-2 署名鍵において想定すべきリスク一覧

リスク	脅威の因子	消失	漏えい	盗難	不正利用
不当な操作（システムにとっては正常系）	エンドユーザ自身の悪意	Y	Y	Y	Y
	顧客資産管理系の管理者の悪意	Y	Y	Y	Y
	エンドユーザへのなりすまし	Y	Y	Y	Y
	カストディ内部犯 (管理者へのなりすまし)	Y	Y	Y	Y
外部からの不正侵入	トランザクション署名部への不正侵入	Y	Y	Y	Y
	入コイン判定部への不正侵入	Y	Y	Y	Y
	顧客資産管理系への不正侵入	Y	Y	Y	Y
	カストディ運用系への不正侵入	Y	Y	Y	Y
操作指示と異なる動作	トランザクション部の意図しない挙動 (バグなど)	Y	Y	-	-
	入コイン判定部の意図しない挙動 (バグなど)	Y	Y	-	-
	顧客資産管理系の意図しない挙動 (バグなど)	Y	Y	-	-
	カストディ運用系の意図しない挙動 (バグなど)	Y	Y	-	-

[3] 悪意のない盗難や悪意のない不正利用は想定し得ないことに起因する。
[4] 例えば、特定の正当な操作と連動して攻撃者に署名鍵を送信する、あるいはトランザクションの署名指示を改ざんするようなバックドアを仕込まれるなど。

人間系の誤操作	エンドユーザの誤操作	Y	Y	-	-
	顧客資産管理系の管理者の誤操作	Y	Y	-	-

Y：該当リスクあり、×：該当リスクなし

以下の節では各リスクについて概説する。各リスクに対応する管理策については7.3節で示し、各リスクと管理策の対応表は付録2に示す。

6.2.1.2 署名鍵の消失リスク

これらのリスクは、署名鍵への入力(操作指示)に着目し、消失を起こし得る可能性を持つ事象を列挙したものである。
典型的なリスクとしては、管理者の誤操作による署名鍵の消失が考えられる。

6.2.1.3 署名鍵の漏えい・盗難リスク

盗難は悪意あるものによる故意の操作が不可欠だが、漏えいは悪意がなくとも過失によって発生し得る。このため、漏えいリスクと盗難リスクは分けて整理する必要がある。

表6-2に示した漏えいリスクは、署名鍵への入力(操作指示)に着目し、過失も含め漏えいを起こし得る可能性を持つ事象を列挙したものである。典型的には、誤操作や意図しない挙動などによる漏えいリスクが考えられる。
同じく盗難リスクは、署名鍵への入力(操作指示)に着目し、何らかの悪意を持ったものによって起こされ得る可能性を持つ事象を列挙したものである。典型的には、内部犯や外部からの不正侵入などによる盗難リスクが考えられる。

なお、漏えいも盗難も、発生する事象は機微情報の外部への流出という点では同様であり、その管理策は共通である。これについては7.3.6節で後述する。

6.2.1.4 署名鍵の不正利用リスク

表6-2に示した不正利用リスクは、署名鍵への入力(操作指示)に着目し、何らかの悪意を持ったものによって起こされ得る可能性を持つ事象を列挙したものである。典型的には、外部からの不正侵入やなりすましによる不正利用リスクが考えられる。

署名鍵の不正利用は、直接的な操作指示だけでなく、トランザクション署名系に未署名のデータが入力される以前の各フローでの不正な操作もまた要因となりうる。例えば、以下のような方法による不正利用が考えられる。

- トランザクション署名部のプログラムが改ざんされて出コイン先や金額を変更されてしまう。トランザクション署名部で本来しているはずの検証処理が無効化されてしまう。
- トランザクション作成部が作成した署名前トランザクションデータが改ざんされて金額やアドレスが変更される。あるいは、本来は作成されるはずのない署名前トランザクションデータが作成され、トランザクション署名部への入力に挿入されてしまう。

- トランザクション作成部のプログラムが改ざんされて出コイン先や金額を変更されてしまう。トランザクション作成部に直接命令を出して署名前トランザクションデータを作成される。
- 管理者による内部不正、操作ミス、あるいは、なりすましによって、カストディ運用系からトランザクション作成部を経由して不正な金額や不正なアドレスが指定され送信されてしまう。
- 資産データを参照してトランザクション作成部に命令を出している場合、その資産データ自体を改ざんされてしまう（6.2.2節参照）。

このように署名鍵そのもので操作しなくても、攻撃者は暗号資産を不正取得することが可能となる。特に、各フローの処理が自動化されているシステムでは注意が必要である。こうした複合的なリスクに対策するためには、署名鍵のセキュリティだけでなく、7章で示すようにカストディアン全体としてのセキュリティ管理策を実施する必要がある。

6.2.1.5 その他関連リスク

- ハードウェアウォレットのサプライチェーンリスク
  秘密鍵管理機能を備えた製品として、いわゆるハードウェアウォレットがある。多くのハードウェアウォレットは、PCなどの管理端末にUSB接続し、管理端末から鍵管理操作を行う。鍵管理機能を備えた製品のセキュリティ認定としてFIPS140-3などがあるが、暗号資産が扱う暗号アルゴリズムの多くは認定対象外となっていることから、暗号資産を対象とするハードウェアウォレットの安全性に関する第三者認定の仕組みは残念ながら不十分と言わざるを得ない。このため、市井に流通するハードウェアウォレットの中には十分な安全性を備えた製品がある一方で、安全性の不十分な製品もあることを認識しておく必要がある。
  さらに、一定の安全性を備えた製品であっても、流通経路上で細工を施されることによって安全性が毀損される場合がある。例えば、流通経路の途中でマルウェアを仕込まれたハードウェアウォレットは、たとえハードウェアウォレット内で購入者が新たに署名鍵を生成したとしても、攻撃者はハードウェアウォレットなしにその署名鍵を復元することが可能になる。

6.2.2 資産データに関するリスク

資産データは顧客やカストディアンが有する暗号資産や法定通貨の額などの資産を管理するためのデータである。ここでは、トランザクション署名系の署名鍵は含まないものとする（5.2節参照）。
前述したように、資産データはカストディアンごとに多様であるため、本書ではより抽象化したモデルとして考察している。実際のカストディのシステムが扱う資産データに対して詳細な脅威分析やリスク評価を行う必要があるため、ここでは簡単に考え方のみを示す。
資産データの主な脅威としては、不正な書き換え、消失、漏えいが考えられる。その因子としては、管理者による誤操作、正当者の悪意、正当者へのなりすまし、部外者の悪意、(システムの)意図しない挙動が考えられる。5.2節の基本モデルの例では、カストディ運用系、顧客資産管理系、入コイン判定部がアタック・サフェースである。
資産データの脅威のうち、不正な書き換えによるインシデントとしては次のような例が考えられる。

- 不正な資産データを参照した顧客資産管理系が不正なトランザクションを作成し、正常なプロセスを経てブロックチェーンに流れてしまう恐れ（6.2.1.4節）。例えば、資産データに記録されている保有額を書き換える、暗号資産移転先アドレスを変更する等が考えられる。
- 例えば、顧客にひもづいたアドレスのリストを書き換える等により、カストディアン内の資産データ内で顧客間あるいは顧客とカストディアンの間で保有額の不正な組み換えがなされる。その結果、ブロックチェーンにトランザクションとして結果が反映されることなく、ある顧客やカストディアンが有していたはずの資産が失われる。

資産データに関するリスクは、一般的な金融・決済システムと同様の問題と捉えることができるが、資産データに対する不正な書き換えの結果として、ブロックチェーンにトランザクションが書き込まれる事態となった場合に、トランザクションを取り消すことが出来ない性質を前提に検討する必要がある。

6.2.3 システムや業務の停止に関するリスク

暗号資産カストディのシステムとは、暗号資産カストディを構成するソフトウェア、ハードウェア、ネットワーク等が構成要素である。またカストディの業務とは、カストディシステムの運用監視、口座開設、送金指示、ウォレットの入出金など、人手を介して行われるオペレーションを指す。しかし、様々な要因によってシステムや業務が停止しうる。
システムや業務の停止に関するリスクは、一般的な金融・決済システムと同様の問題と捉えることができる。しかしながら仮想通貨交換所が一般に専用通信網ではなくインターネットに常時接続し、24時間365日で稼働していること、多くの暗号資産カストディがパブリッククラウド基盤上に構築されていること、暗号資産カストディの稼働状況が暗号資産価格に与える影響が大きく、攻撃の対象となりやすいことを前提に検討する必要がある。

6.2.3.1 ネットワークのふくそうに係るリスク

インターネットに接続されたシステムは、突発的な大量のアクセスや、サービス不能攻撃を受けることがある。サービス不能攻撃の対象としては、公表されているトップページ、APIエンドポイント等が一般的だが、攻撃者にシステム構成が知られ、インターネット上に業務システムや運用監視システムを置いている場合、これらシステムもサービス不能攻撃を受ける場合が考えられる。

6.2.3.2 システム基盤の停止によるシステム停止のリスク

システムを設置しているデータセンター、クラウド基盤などが停止し、暗号資産カストディシステムと業務が停止することが考えられる。天変地異による停電や通信の途絶、クラウド基盤事業者の運用ミスによる大規模障害、基盤運用のミスによる大規模システム障害、ソフトウェアのリリースの失敗など、様々な要因によってシステムは停止し得る。

6.2.3.3 要員に起因する業務停止リスク

システムそのものが稼働していても、運用監視や業務を担う要員の活動が阻害されると、業務が停止する可能性がある。例えば運用拠点における電源設備の定期点検や、天変地異やストライキ等による交通手段の途絶、抗議活動や取材記者の殺到によって建物の出入りが阻害されるといった様々な要因により、業務が停止する可能性が考えられる。
また要員が同じ交通手段を利用していたり、同じイベントに参加していたりする場合や、交通事故や食中毒など、同一の原因によって多くの要員が稼働できなくなるリスクが考えられる。

6.2.3.4 法的要因による業務停止リスク

暗号資産カストディが法定されて、免許制や登録制となっている国や地域においては、業務改善命令や業務停止命令、登録の抹消などによって業務が停止することが考えられる。

6.3 外的要因によるリスク

暗号資産カストディのシステムや業務を適切に運用していたとしても、暗号資産の稼働するブロックチェーン・ネットワークや、そのノード間の接続を支えるインターネット基盤が攻撃を受けた場合には、利用者に対してサービスを継続できなくなる場合や、適切に取引を処理できなくなる場合がある。

6.3.1 インターネットの基盤およびWeb PKI、端末環境に係るリスク

6.3.1.1 インターネットの経路制御および名前解決に対する攻撃

攻撃者が経路ハイジャック等、インターネットの経路制御や、ドメイン名前解決（Domain Name Service）に介入することで、暗号資産カストディへの到達性を妨げ、また偽の交換所に誘導したり、ブロックチェーンの同期を妨げて意図的に分岐を起こすことができる。この手法は悪意を持った攻撃者だけでなく、政府からの指示に基いてISP等が行うことも考えられる。

6.3.1.2 Web PKIに対する攻撃

多くの暗号資産カストディはWeb上でサービスを提供しており、利用者によるサイトの真正性確認と暗号化にTLSとサーバー証明書を利用している。サーバー証明書を発行する認証局が攻撃を受けた場合には、サイトのなりすましが可能となる。証明書をリボークされた場合には、サービスを提供できなくなることも考えられる。

6.3.1.3 メッセージングに対する攻撃

攻撃者がSMSや電子メール等のメッセージングシステムに介入することで、利用者とのやりとりやワンタイムパスワードの配送に使われる電子メールや携帯電話のSMS/MMSの詐取や遮断を行うことができる。利用者のメッセージを詐取された場合、利用者になりすましたログインやパスワードのリセットが可能となる。

6.3.1.4 端末環境の汚染に係るリスク

利用者の端末環境がマルウェア等によって汚染されている場合には、端末内のクレデンシャル等は全て詐取されるおそれがある。

6.3.2 暗号資産のブロックチェーンに起因するリスク

6.3.2.1 暗号資産ブロックチェーンのスプリット

開発コミュニティの間で合意が得られないまま仕様変更が行われ、ハードフォークによって台帳が分裂するケースがある。分裂前後の取引について、分裂前に取引が処理されて分裂後の双方の台帳に記録される場合と、分裂後の片方の台帳にしか記録されないケースがある。

6.3.2.2 51% attackやselfish miningによるBlockchainのRe-org

ネットワークの分断や51%攻撃によって過去に確定したブロックが破棄された場合、破棄されたブロックに含まれる取引はロールバックしてしまう場合がある。破棄されたブロックに含まれていた取引が、Re-orgの結果、他の取引と矛盾が生じる場合は破棄されて、その取引の対価として支払われた現金や暗号資産が詐取されるおそれがある。

6.3.2.3 ハッシュ関数および暗号アルゴリズムの危たい化

半導体の性能向上による計算能力の向上や、効率的な攻撃手法の発見によって、ハッシュ関数や暗号アルゴリズムが危たい化することが起こり得る。

6.3.2.4 ブロックチェーン仕様および実装の不備

合意アルゴリズムのバグを悪用して、偽の取引情報を特定のノードに送り取引相手に対して送金の有無を偽装することによって、送コインを装って対価を詐取する攻撃がある。例えば2014年のMt.GOX事件に於いては、便乗でTransaction Malleabilityを悪用した二重払い攻撃が多発したとされる。

実装の不備に起因して、ブロックの生成が止まってしまうリスクがある。Liskにおいてはトランザクションのタイムスタンプ値が、内部データベースで許容されない範囲の数値入力を許していた実装に起因して、各ノードがトランザクションを処理できずブロック生成が停止したという事例があった（https://github.com/LiskHQ/lisk/issues/2088）。問題発生から数時間後に修正され、参加ノードがクライアントソフトウェアをアップデートして順次ネットワークが回復したが、一定期間ブロックチェーンでトランザクションの処理ができない状態となった。

スマートコントラクトの実装の不備に起因して、トークン価値が崩壊する事例がある。Ethereum上で発行されていたERC20トークンのBeautychain Token(BEC)では、スマートコントラクトにオーバーフローを引き起こすぜい弱性があったことに起因して、発行量の上限を大幅に超えたトークンを引き出す攻撃があり、価値が崩壊したという事例がある。(CVE-2018-10299)

6.3.2.5 ハッシュレートの急激な変動

ハッシュレートが一時的に上昇したのちに急激に下がった場合には、残存ノードでブロックを生成するために非常に長い時間を要してしまうことが考えられる。

6.3.3 外部のレピュテーションに起因するリスク

6.3.3.1 銀行口座の凍結

AML/CFTの一環として、銀行が暗号資産カストディの業務に係る口座を凍結するケースや、規制当局からの指導や口座の事故に伴い、銀行が銀行口座を凍結するリスクがある。仮想通貨交換所の口座が凍結された場合には、利用者との法定通貨の入出金の業務が停止。

6.3.3.2 仮想通貨アドレス

AML/CFTの一環として、他の暗号資産カストディアンYの利用者が、暗号資産カストディアンXの暗号資産アドレスに送金する場合に、送金先アドレスが高リスク取引に当たらないかどうか他

の暗号資産カストディアンYが確認するケースがある。暗号資産カストディアンXの管理するアドレスが、問題あるアドレスとして登録された場合、暗号資産の交換を円滑に行えないリスクがある。犯罪者がかく乱のために盗んだ暗号資産を悪意ない第三者のアドレスに送金するケースはよくあることから、誤って暗号資産カストディアンYの管理するアドレスが高リスク取引先に分類されてしまうリスクがある。

6.3.3.3 Webサイトに対するフィルタリング・ブロッキング

暗号資産カストディのURLがネットワーク管理者によってフィルタリングされたり、ISPによってブロッキングされたりすることで利用者がアクセスできなくなってしまうリスクが考えられる。またマルウェア配布サイト等として認識された場合、検索結果として表示されなくなったり、ブラウザから閲覧できなくなったりするリスクも考えられる。

6.3.3.4 電子メール

迷惑メール対策として、メールサーバーの多くはレピュテーションに基づくメール配送拒否や迷惑メールの分類機能を提供している。暗号資産カストディアンの配信する電子メールがspamと判断された場合、利用者に対して連絡を取れなくなることが考えられる。

6.3.3.5 スマホアプリの審査

プラットフォームによっては、アプリによる暗号資産のハンドリングを制限するケースがある。スマホアプリの審査を通過できなかった場合、利用者は暗号資産カストディアンにアクセスするためのスマホアプリをダウンロードできず、サービスを利用できなくなることが考えられる。

6.3.4 利用者に対するID詐取

利用者本人になりすまして攻撃者が不正な操作を行うケースがある。攻撃の手法としては、IDに対するリスト型攻撃や、利用者の端末にマルウェアが仕込まれID・パスワード、その他のクレデンシャルを詐取する、APIアクセスに必要なトークンの詐取などが考えられる。
なりすましの目的としては不正な出金による現金または仮想通貨の詐取、他人名義の口座で暗号資産を現金化することによる資金洗浄、勝手に売買することによる相場操縦による利益移転などが考えられる。

7 暗号資産カストディにおけるセキュリティ管理策の留意点について

7.1 本節について

本節では6章に述べた各種リスクに対する管理策について基本的な考え方を示す。セキュリティ管理策については、項目の妥当性を議論しやすくする観点から、ISOにおける情報セキュリティマネジメントシステムの要求事項 ISO/IEC 27001:2013(JIS Q 27001:2014)および実践のための規範 ISO/IEC 27002:2013(JIS Q 27002:2014)を踏襲したものとしている。
本節では暗号資産カストディにおける特有の考慮点について記載している。特に、仮想通貨の署名鍵の管理は、他の情報システムと異なり、資産の裏付けがあることから、より強固な管理策を検討する必要がある。

その他のセキュリティ管理策については、類似の業務を行っている金融機関等で採用されている管理策を参考にすることが期待される。

セキュリティ管理策の策定にあたっては、適用範囲におけるリスク分析やぜい弱性診断の結果を受けて具体的な内容を検討する必要がある。また、セキュリティ上の脅威は常に変化するため、状況に応じて管理策を見直すことが重要である。

以下の個々の項目については、記載の補完や参考文献の記載が必要な部分があるため、今後拡充していくことが期待される。

7.2 セキュリティマネジメントに対する考え方の基本事項

一般的に、セキュリティマネジメントに関する要求事項としては、ISO/IEC27001:2013（JIS Q 27001:2014）、実践のための規範としてISO/IEC27002:2013（JIS Q 27002:2014）が存在する。仮想通貨交換所においても、これらの基準を参考に業務内容に応じた対策を検討したうえでセキュリティマネジメントを確立し、実施し、維持し、継続的に改善することが重要である。

具体的には、暗号資産カストディにおいては、顧客資産や自己資産に関する資産データ、顧客情報、さらに仮想通貨の署名鍵といった保護すべき資産があり、漏えいや紛失、改ざん、不正利用から保護される必要がある。また、暗号資産特有の考慮点として、ブロックチェーンやネットワークインフラなどの外部要因による資産の消失やシステムの停止といったリスクに適切に対処することが必要である。

暗号資産カストディのセキュリティマネジメントにおいて、特に考慮する必要がある事項は以下のとおりである。

- 利害関係者について（JIS Q 27001:2014「4 組織の状況」に関連）
  暗号資産カストディの直接の顧客に関する資産を保護すること。また、委託事業者（例えば仮想通貨の署名鍵の管理などセキュリティに関わるもの）との責任分界(Devision of responsibility)についても考慮が必要である。仮想通貨交換所が管理する資産の保護という観点とは異なるが、マネーロンダリングなど仮想通貨交換所の業務が社会に与える影響についても考慮に入れる必要がある。

- セキュリティ方針について（JIS Q 27001:2014「5 リーダーシップ」に関連）
  仮想通貨交換所はセキュリティ目的や管理策も含めセキュリティ方針を定める必要がある。特にセキュリティ方針については顧客等が判断できるように公開することが望ましい。

- 継続的なリスク評価と改善（JIS Q 27001:2014「6 計画」「8 運用」「9 パフォーマンス評価」「10 改善」に関連）
  仮想通貨交換所は一般的なセキュリティマネジメントの考え方に加え、本書5.3.2で述べたように仮想通貨が抱えるセキュリティリスクを常に監視する必要がある。状況の変化に応じて、セキュリティ管理策を継続的に評価し、改善することは特に重要である。

7.3 仮想通貨交換所システムのセキュリティ管理策に関する留意点

仮想通貨交換所では以下の全ての観点からセキュリティの目的や管理策を定める必要がある。

- 顧客資産となる資産データおよび仮想通貨の署名鍵の消失、盗難（漏えい）、不正利用の脅威に対する備え
- 事業上の要求事項
- 法令や規則の遵守

この節では6.2節で述べた仮想通貨交換所のシステムのリスクを前提としたセキュリティ管理策について留意すべき点を述べる。一般的な情報セキュリティ管理策の指針や手引きとしてJIS Q 27002:2014があり、仮想通貨交換所システムのセキュリティ管理策を考える上で参照することが期待される。以降の7.3.1節から7.3.14節ではJIS Q 27002:2014の項目を踏襲し、仮想通貨交換所システムで特に留意すべき事項について記述する。

7.3.1 情報セキュリティのための方針群

JIS Q 27002:2014の「5 情報セキュリティのための方針群」に準じて、情報セキュリティ方針を定める必要がある。

特に、仮想通貨交換所における情報セキュリティマネジメントの目的に、顧客資産の安全な保護、事業上の要件事項や法令や規制の準拠、社会的責任の遂行といった観点も含める必要がある。

また、情報セキュリティ方針群には、例えば、7.3.5の仮想通貨交換所システムのアクセス制御に関する方針、7.3.6の署名鍵など鍵管理策に関する方針、7.3.8の運用のセキュリティに関する方針、7.3.9の通信のセキュリティに関する方針など各管理策に関する方針を含む必要がある。

7.3.2 情報セキュリティのための組織

JIS Q 27002:2014の「6 情報セキュリティのための組織」に準じて、全ての情報セキュリティの責任を割り当てるとともに、実施と運用を行う組織体制を確立する必要がある。

特に、仮想通貨の取り扱いにおいては6章で述べたように署名鍵の不正取得やトランザクションの不正な作成などの脅威を特に慎重に考慮し、作成指示の承認等についての職務の分離を十分に検討する必要がある。（JIS Q 27002:2014「6.1.2 職務の分離」）。

7.3.3 人的資源のセキュリティ

JIS Q 27002:2014の「7 人的資源のセキュリティ」に準じる必要がある。

特に、仮想通貨交換所のセキュリティ管理策の検討や評価には、一般的な情報セキュリティに関する専門性が求められるとともに仮想通貨やブロックチェーン技術に関する専門性を有する専門性も必要である。
なお、雇用期間中においては、署名鍵を扱う操作員・管理者などは顧客資産も含め、高額資産を扱うことになるため、その倫理教育についても定められた間隔で適正に行う必要がある。

7.3.4 資産の管理

JIS Q 27002:2014の「8 資産の管理」に準じる必要がある。

特に交換所においては、情報資産として署名鍵をはじめとした顧客や資産に関する情報、資産の管理に必要な情報を含めることが必要である。
交換所がハードウェアウォレットを自ら運用する場合は、本項目に準じて、リスクに応じた適切な管理策を策定する必要がある（外部に委託する場合は7.3.11を参照すること）。また、顧客の資産を保護するため、規制および税務・会計などで要求される要件に対応できるよう、顧客の資産と交換所の資産を分別して管理することが必要である。

7.3.5 アクセス制御

JIS Q 27002:2014の「9 アクセス制御」に準じる必要がある。

特に、交換所のシステムへアクセスする者として、オペレーターや管理者といった交換所のシステム内で操作の権限を与えられた者（業務委託先含む）と、交換所のサービスを利用する顧客に大別できる。7.3.5.1節では特に交換所のオペレーターや管理者を対象としたアクセス制御の考え方を示し、7.3.5.2節では交換所のサービスを利用する顧客に対するアクセス制御について特記すべき事項を記す。

7.3.5.1 交換所内のオペレーターや管理者のアクセス制御

交換所のオペレーターや管理者については例えば以下のようなケースが考えられる。

- 交換所管理系を通じて操作を行うオペレーターや管理者。例えば、交換所管理系に接続する専用の端末やソフトウェアを用いて鍵生成の指示や、資産移転指示といった操作を行う等。
- システムの各要素が稼働している計算機やOS、データベース、ミドルウェア等のメンテナンスを行う管理者。

署名鍵に対する管理（活性化の操作、バックアップやリストアなど）、署名鍵の管理については7.3.6も参照のこと。

上記のようなオペレーターや管理者に対して適切な操作権限の割り当てとアクセス制御を実施する必要がある。アクセス制御には、例えば、交換所管理系に接続するリモート端末の認証と認可、交換所の機能の実現に外部サービスを利用する場合における外部サービスへの認証、交換所管理系にアクセスするユーザーの認証と認可、OSやデータベースに対するユーザーの認証と認可、交換所のシステムや操作端末が設置されている施設への入退出制限などが含まれる。また、アクセスの認可を判断する要因としては、例えば所定の業務時間帯(あるいは承認された作業時間帯)のみ、所定の端末に割り当てられたIPアドレスのみ、あるいは所定の端末や操作員からのアクセスであることをクレデンシャルを用いて確認するなどの方法が考えられる。各事業者のシステムに応じて、アクセス制御が必要なシステム要素や、オペレータや管理者などの役割や権限などを定めたアクセス制御方針を検討する必要がある。単に個々のアプリケーションのアクセス権設定にとどまらず、オペレーターや管理者が実行可能なソフトウェアや機能についても、同様に最小限に留めることが必要である。

6.2節で述べたように特に資産移転指示や署名鍵の管理については操作ミスや内部不正などにより重大な被害が生じうる。このような脅威を抑止するためにも、資産移転指示や署名用暗号鍵に対する操作など重要な操作を行う場合には、複数人のオペレーターや管理者による操作指示内容の確認や承認を経て実施することが望ましい。また、単一のオペレーターや管理者に全ての権限を集中させるのではなく、複数人で権限を分散させることが必要である。

7.3.5.2 顧客のアクセス制御（ユーザー認証やAPI提供について）

- 口座開設時の厳格な本人確認の実施
  顧客の口座開設に際しては、厳格な本人確認を実施して、本人確認を行った当人に対して適切に口座を払い出す必要がある。例えば公的機関の発行した身分証明書に基づいて本人確認を実施して、居所に対して転送不要郵便を送付する方法などが考えられる。各国法令や、それぞれの国が参加する国際協定（FATFなど）の要求する本人確認を実施することが求められる。
  本人確認に対する典型的な脅威として、身分証の写真の差し替えや、属性情報の改ざんなどがある。本人確認を厳格に行うため、典型的な攻撃手法を認識して、身分証明書画像が改ざんされているかどうかの目視やソフトウェアを使った解析による検証や、電子署名など改ざんの難しい電子的な方法を用いた身分証明書の真正性確認を行うことが必要である。クレデンシャルの管理・多要素認証の実施
  利用者の認証に当たっては、単一のクレデンシャルが漏えいしただけではなりすましできないように、複数の認証要素を用いる多要素認証や、通常とは異なる形態でのアクセス（経路や端末の特徴、時間帯が大きく異なるなど）に対して追加認証を求めるリスクベース認証を導入することで、なりすましや内部不正に対して効果が期待できる。
  なりすましや転送経路上での詐取のリスクがあることから、ワンタイムパスワードの配送に、電子メール等の保護されていない伝送路を利用することは推奨しない。SMSによる電話番号確認は、電話番号の所持・到達性の確認において有効であるとされていたが、多くの取引所でなりすましや中間者攻撃が発生しており、NISTでRESTRICTEDにされている事実を鑑み（NIST SP800-63b）、所有物認証などの本人認証技術や取引認証技術を施すべきである。アカウントリカバリに於ける要素のひとつとして利用できるが、実在確認や認証の手段にはならない点に留意する必要がある。
- ログイン時の多要素認証, リスクベース認証
  交換所の顧客になりすますことによって、預入金や預入仮想通貨を詐取したり、仮想通貨の現金化、資金洗浄などが行われることを抑止するために、顧客の登録とアクセス制御を厳格に行うことが必要である。
- 操作のリスクに応じた意思確認
  顧客の利便性とサービスの安全性とを両立するために、顧客の行う操作のリスクレベルに応じて、認証レベルに差をつけることが考えられる。例えば口座残高・取引明細の表示といった経済的被害のない低リスクの操作にはトークンによる単要素認証を認めてもよいが、コインの売買指示や住所変更・口座変更など、不正利用のリスクがある更新系の操作に対しては、追加的な認証を求めることが必要である。
  さらに出コイン・法定通貨の送金指示など、直接的な経済被害の発生する操作に対しては、金額や送金先といった個別取引のリスクに応じて、追加的な認証要求や、人手による取引意志の確認を求めることも考えられる。
- アカウント抹消時のデータ保全
  交換所は顧客の求めに応じて登録や保有個人データの抹消を行う必要があるが、攻撃者が不正アクセスに成功し、利用者の意に反してアカウントの削除などの操作を行うリス

クも勘案して対応する必要がある。こうした操作が行われ、後に利用者から不正アクセスの申し立てが行われた場合などに備えて、アカウント削除の操作に対して一定期間はロールバック可能な実装とすることが必要である。

- アドレス廃止時の署名鍵の保全
  仮想通貨アドレスに残高が残っていない場合であっても、アカウントに対応する署名鍵を削除すべきではない。外部者が任意のアドレスに対して自由に送金でき、技術的にそれを妨げることができない一般的な仮想通貨を前提とした場合に、過去に交換所が利用したことのある仮想通貨アドレスに対して送金が行われる可能性を想定して、適切に管理された仮想通貨アドレスに再送金できるように、利用を止めたウォレットの署名鍵も適切にバックアップしておくことが必要である。
- API提供時の留意点
  これら顧客の操作に対するアクセス制御に当たっては、Web上の対話的な操作に加えて、スマホアプリや外部システム等から接続するAPIについても同様に考慮する必要がある。APIの提供に当たっては、顧客からの明示的な認可作業が難しいケースなど、固有のリスクを考慮して実装する必要がある。またAPI固有の攻撃リスクを踏まえて、産業で共有されているベストプラクティスに準じることが必要である。
  参考として例えばOpenID FoundationのFinancial API[5]に準拠することが考えられる。

7.3.6 暗号（署名鍵の管理策）

JIS Q 27002:2014の「10 暗号」に準じることが必要である。

特に交換所固有の課題である署名鍵の管理策については、この章の他節（例えば、「アクセス制御」など）の管理策と密に関係するものがある。

ホットウォレットには、コールドウォレットからの引き出すために要する時間内で支払いを準備するために最小限の額のみを置くこととして、それらが流出することによって利用者への払い戻しに支障をきたさない金額にとどめておく必要がある。
署名鍵以外の暗号利用（例えば、データベースの暗号化など）については、一般的な情報システムと同様に、利用目的に応じて、客観的に安全性が評価された適切な暗号技術を選定すること。また、暗号鍵のライフサイクルを定め、適切な管理策を実施すること。

7.3.6.1 署名鍵管理の基本

仮想通貨に限らず、署名鍵管理の主な要件としては以下が挙げられる。

- 署名鍵は他の情報とは分けて管理し、厳格なアクセス制御を行うこと
- 署名鍵にアクセスする頻度はできるかぎり少なくすること
- 署名鍵の意図せぬ消失・破壊に備えること

これを実現するための、基本的な管理策として以下の3つを挙げておく。また、これら基本的な管理策に加えて、仮想通貨交換所システムとして考慮すべき主な管理策については、7.3.6.2項以降で述べていくことにする。

[5] OpenID Foundation, Financial-grade API (FAPI) WG
https://openid.net/wg/fapi/

1. 署名鍵の状態管理

   図5-2に示したように、署名鍵は一般に複数の状態を持ち、運用中においては主に活性/非活性状態のいずれかにある。署名(あるいは暗号文のための復号)演算を行うには、署名鍵の状態は活性化されている必要がある。非活性状態の署名鍵を活性化するには、何らかの秘密情報の入力を必要とすることが望ましい。これにより、非活性状態にある限りは、この秘密情報を合わせて入手しない限り署名鍵の不正利用は困難であり、漏えい・盗難に対しても同様である。

   また、署名鍵の不正利用リスクを最小化するためには、活性状態の期間を業務合理的な範囲で必要最小限に留めることが望ましい。最も業務合理的なのは常に活性状態にあることだが、明らかに操作不要な時間帯に活性状態としておくことは、漏えい・盗難も含めリスクを高めることになる。逆に、署名操作を必要とする都度に活性化/非活性化の操作を行うことは、操作頻度が高い場合には非合理的と言える。

   どこまできめ細かく制御するかは業務合理性と安全性のバランスによって決める必要があり、またそのようなリスク受容にもとづいて鍵管理が行われていることを、(鍵管理規程の掲載など)利用者が確認できることが望ましい。

2. 署名鍵管理に関する権限分離と相互けん制

   内部不正や誤操作を防ぐには、署名鍵を用いるクリチカルな操作に関して複数人による操作を必須とすることが基本となる。例えば署名操作を行う権限と、署名操作が可能な区画への入室を承認する権限を排他的に設定することで、単独犯が誰かに知られずに不正に署名を行うことは困難となる。さらに、例えば署名操作で複数名による立会いなど、リスクに応じて相互けん制措置を必須とすることは、内部不正や誤操作に対する有効な管理策となる。

3. 署名鍵のバックアップ

   署名鍵が消失・破壊されれば、当該署名鍵による署名演算が不可能になるため、署名鍵のバックアップは重要な管理策である。一方で、バックアップした署名鍵の漏えい・盗難リスクもまた十分に考慮する必要があり、1)で述べた非活性状態での保管が欠かせない。

   また、不適切なバックアップの実施や、通常利用しないアドレスの不正利用を検知するため、当該アドレスからの出コインが実施されていないかブロックチェーンをモニタリングすることも有効である。

7.3.6.2 署名鍵のオフライン管理（コールドウォレット）

外部からの不正侵入による鍵の漏えい・盗難を防ぐために、システムを構成するネットワーク上に鍵を配置しない、いわゆるオフライン管理(コールドウォレットと呼ばれることがある)という手法がある。

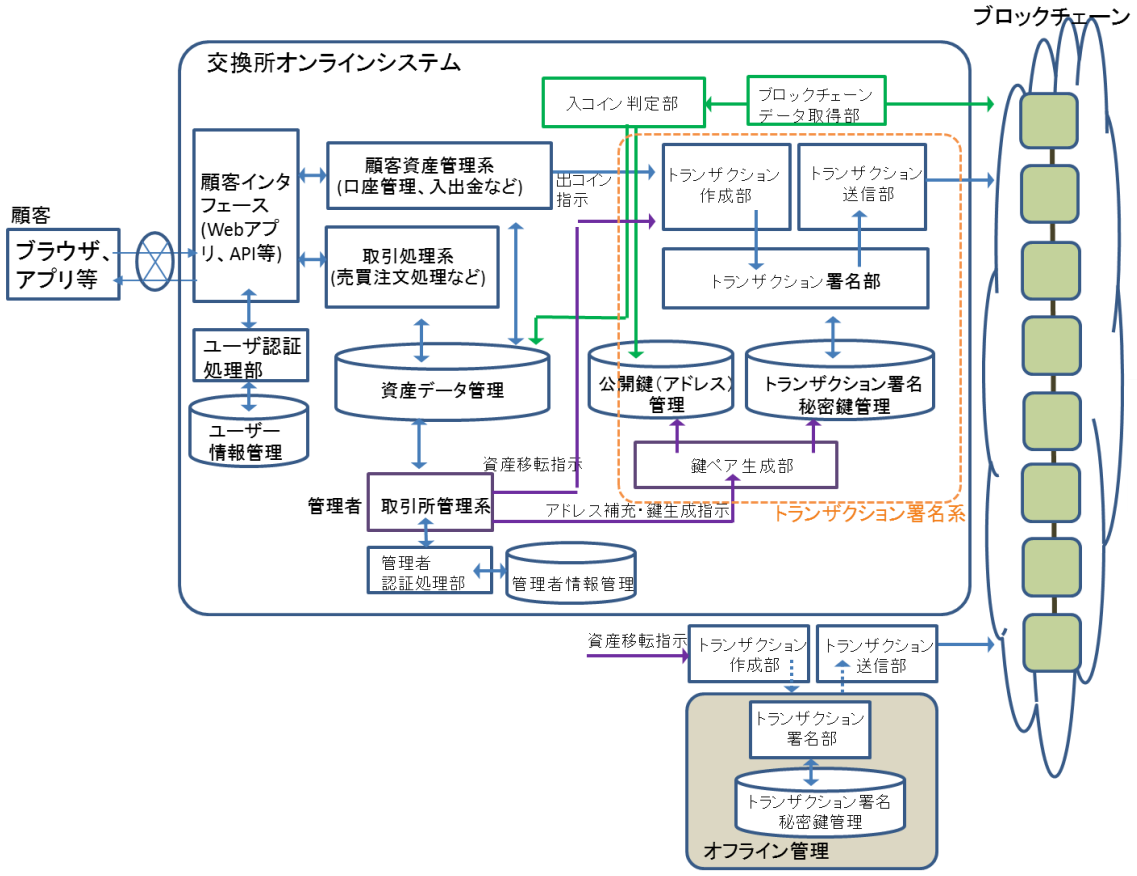

図9-1 署名鍵のオフライン管理のイメージ

この場合、システムが鍵を利用するには何らかのオフライン操作が必要となる。例えば、利用時のみ鍵をネットワークにつなげるために鍵を金庫から取り出してシステムに接続する、オンラインシステムとオフラインの鍵管理端末との間の入出力を、USBメモリ等可搬記憶媒体を介して行う、などが挙げられる。

この、鍵を利用するためのオフライン操作に対して明確な承認プロセスがなければ、例えば前述の高額取引も少額取引と同様に機械的に処理され、誤操作や不正利用だった場合に事前に止めることが難しくなる。即ち、鍵の漏えい・盗難は防ぐことができても、不正利用などに対する管理策には、明確な承認プロセスが欠かせない、ということになる。

7.3.6.3 署名鍵管理の権限分散 (承認プロセス)

署名鍵管理に関する権限分離と相互けん制が有効であることを7.3.6.1節で示した。これに加えて、ブロックチェーンに典型的な仕組みとしてマルチシグ[67]が挙げられる。これはトランザクションの生成に、複数のステークホルダーによる承認プロセスを必要とする仕組みで、各ステークホルダーの管理する署名鍵による署名を以て実現される。各ステークホルダーは、既に他者の署名

[6] BIP-0010: Multi-Sig Transaction Distribution
https://github.com/bitcoin/bips/blob/master/bip-0010.mediawiki

[7] BIP-0011: M-of-N Standard Transactions
https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki

がある場合には技術的にはその署名検証を、実務的にはトランザクションの内容の妥当性確認を行うことが求められる。
多段かつ複数組織の承認プロセスを必要とすることで、トランザクションの不正な生成に対する汎用的な対策として効果が期待できる。ただし、個別の署名鍵漏えい・消失といった脅威は別途対策する必要がある。マルチシグはブロックチェーンのソフトウェアによって提供されるものである。マルチシグの仕組みや実装方法もブロックチェーンのソフトウェアによって異なっている。例えば、イーサリアムにおけるマルチシグはスマートコントラクト上で実装されており、ウォレットソフトウェアごとに複数の実装方式が存在している。また、そもそもマルチシグをサポートしていない場合もあり得るため、仮想通貨の種類によってはこの管理策を適用することができない。

なお、権限分散に応用可能な類似の技術として秘密分散がある。こちらは署名鍵そのものを複数の部品(分散情報)に分割し、複数のシステムで分散管理するための技術で、単独の漏えいや盗難から鍵を守る有効な手段のひとつである。複数のステークホルダーが分散情報を個別に管理することで、トランザクションの不正な生成に有効な対策だが、承認すべき内容を各ステークホルダーが確認するには別途仕組みが必要となること、管理対象が署名鍵よりも実装に依存しやすい分散情報であることから、どちらかというとマルチステークホルダーより多拠点運用を行う単一ステークホルダーのための技術である点に留意されたい。

7.3.6.4 署名鍵のバックアップ

バックアップは、署名鍵の消失対策としてもっとも基本的かつ有効な手段であるが、一方でバックアップ媒体の漏えい・盗難等のリスクを抱えることになる。バックアップ媒体に格納する鍵の個数はここでは問わないものとする。
バックアップ媒体の漏えい・盗難等のリスクは媒体の種類によって異なるため、それぞれに適切なアクセス管理等を行う必要がある。
典型的なバックアップ媒体の概説と、その漏えい・盗難リスクについて以下に述べる。

- 耐タンパ性を有する鍵管理装置へのクローニング
  署名鍵が耐タンパ性を有する鍵管理装置(個体X)で管理されており、同装置が後述のクローニング機能を有する場合、同機能を用いて別個体Yに複製することは、もっとも安全性の高いバックアップ手段のひとつである。
  ここでいうクローニング機能とは、個体Xと個体Y以外のシステムに鍵を読み出すことなく鍵の複製を可能とするもの[8]で、同機能の安全性についてもCMVPやFIPS 140-3などの安全性評価を受けていることが望ましい。なお、耐タンパ性を有する鍵管理装置がサポートする暗号アルゴリズムはごく限定的であることから、すべてのシステムが本方式を採用できるとは限らないが、もっとも安全な方式のひとつとして挙げておく。
- 電磁記録媒体へのバックアップ
  DVDやUSBメモリなど電磁記録媒体へのバックアップを想定する。バックアップを、可搬性のある媒体等でオフライン保管するケースと、システムからアクセス可能な状態でオンライン保管するケースが考えられる。可搬性のある媒体で保管する場合は媒体自身の盗難容易性が高まるため、キャビネットや金庫など施錠管理できる場所に保管するとともに、キャビネット等に対するアクセス管理を厳格に行う必要がある。オンライン保管の場合は、鍵管理機能部(Management functional module)と同様の漏えい・盗難リスクを想定する必要がある。一般的には同機能部と同様の管理策を講じることが望ましいが、同

[8] 例えば個体XとYとしてUSBメモリ等を用い、PCを経由して複製を行うことは、これにあたらない。

機能部とは異なる制約(例えばバックアップ媒体は復元操作など非常時を除き非活性状態におくなど)があれば、それを考慮して管理策を講じることも許容され得る。また、バックアップ操作のために、署名鍵管理機能部の外に鍵を読み出すことが避けられない場合は、一時的と言えど読み出し先のメモリやディスクなどの残存磁気対策も合わせて考慮することが求められる。

- 紙媒体へのバックアップ（ペーパーウォレット）
  署名鍵を二次元バーコードなど機械可読な形式に変換して紙に印刷する。可搬性のある電磁記録媒体よりもさらに可搬性が高く、電磁記録媒体と比べて識別性に優れる。一方で、撮像という紙媒体特有の漏えい・盗難リスクを考慮する必要がある。
- 秘密分散法による冗長化
  署名鍵を複数の部品に分割し、複数のシステムで分散管理しておくことは、単独の漏えいや盗難から鍵を守る有効な手段のひとつである。ここでは複数の部品に分割する手法を指定しないが、秘密分散法など一定の安全性評価を持つ技術をベースに実装することが望ましい[9]。また、その場合も実装上のぜい弱性は排除できないため、セキュアコーディングやペネトレーションテストなど実装に関する管理策を合わせて実施するべきである。本手法はバックアップ媒体に対しても有効である。

7.3.6.5 ハードウェアウォレット等の調達

仮想通貨ウォレットを構築する場合、本来であれば既存のPKIサービス等で利用されているHSMのように技術的安全性が保証されている製品を用いることが望ましいが、現状では仮想通貨が利用する一部の暗号アルゴリズムに未対応である場合が多く、必ずしも利用できるとは限らない。このため、現状においてハードウェアウォレットを導入する場合は、その技術的安全性の不十分さを受容し、以下に示すような点に留意しながら運用していくことが望ましい。なお、市販のハードウェアウォレットのみを利用する場合は、7.3.4節 資産の管理に準じて管理を行う必要がある。

- 調達経路を信頼できないハードウェアは使用しない。
- 製造元が提供する最新のファームウェアやパッチを適用する。
- 初期化や鍵生成は安易に初期設定に頼らず、自身で確実に行う。
- ハードウェアウォレットに署名指示を行うソフトウェアが信頼できるか確認する。特にマルチシグ対応やオフラインコンピュータでの実行が可能であるかについて確認する。

一方でハードウェアウォレットは、こうした技術的な安全性を保証する第三者評価のスキームの創設、あるいは業界団体等による独自の評価スキームを確立し運用していくことが早期に求められる。

ソフトウェアウォレットを外部から導入する場合は、そこに不正なコードやぜい弱性、バグが含まれている可能性に留意する必要がある。

7.3.7 物理的及び環境的セキュリティ

JIS Q 27002:2014の「11 物理的及び環境的セキュリティ」に準じる必要がある。

[9] 例えばISO/IEC 19592-2:2017など

仮想通貨交換所システムでは特に以下の要素についても厳格な物理的保護策を検討する必要がある。

- 署名鍵が格納された媒体 (図5-1の署名鍵管理)
- コールドウォレット運用時に署名鍵が格納された媒体(図9-1のオフライン管理の署名鍵管理)
- コールドウォレット運用時に用いる管理用端末(図9-1のトランザクション指示や作成等を含んだ機能を有する端末)
- 署名鍵のバックアップデータを保存した媒体

上記の署名鍵が非活性状態で保存される場合において、活性状態にするための復号用署名鍵を別途管理する場合には、その復号用署名鍵が格納された媒体についても同様に厳格に管理する必要がある。
署名鍵が格納された媒体や、署名鍵を操作するために必要な情報が格納された媒体が保管される施設や環境は別途、物理的アクセスを制限することが必要である(7.3.6参照)。

なお、管理や操作を施設外から行う場合には、その操作端末についても遺失や盗難に対する対策を行う必要がある。物理的な保護手段やアクセス制御などその他の手段と併せて実施し、厳格に管理する必要がある。

7.3.8 運用のセキュリティ

JIS Q 27002:2014の「12 運用のセキュリティ」に準じる必要がある。特に仮想通貨交換所システムで言及しておくべき事項を以下に述べる。

7.3.8.1 マルウェアからの保護(JIS Q 27002:2014 12.2)について

マルウェアの検知策及び回復策については仮想通貨交換所システムの構成や環境、取り扱う情報に応じて適切に講ずる必要がある。

なお、マルウェア予防策として、仮想通貨交換所システムが稼働するOS、ミドルウェア等の環境についてセキュリティパッチの適用が考えられるが、パッチの重要度や緊急度に応じて、十分な確認を行った上で適用する必要がある。また、緊急度の高いパッチが提供された場合や、すでにぜい弱性に対する攻撃が開始されている場合のセキュリティパッチの適用及び試験手順やプロセスを事前に検討する必要がある。

7.3.8.2 バックアップ(JIS Q 27002:2014 12.3)について

バックアップの取得にあたっては、署名鍵やマスターシードなど漏えいによって重大な被害を受ける重要データについても、バックアップ対象のデータと同様に厳格に管理する必要がある(適切な保管場所の選定と厳格なアクセス制御の実施など)。7.3.6節で述べたような分散保管を実施することや、バックアップやリストアにおいて操作者や承認者(責任者)など適切な権限分離を行うこと、複数人による操作を行うことなども重要である。

7.3.8.3 ログ取得及び監視（JIS Q 27002:2014 12.4）について

例えば以下のようなログを適切に取得、監視、記録することが求められる。

- 仮想通貨交換所システムが稼働する環境に関するログ
  稼働するコンピュータやOS、ミドルウェアなどが出力するイベントログを収集、監視することで稼働する環境の異常を検知する。また、記録したログはインシデント発生後の原因究明のためにも用いられる。
- 仮想通貨交換所システムが各要素で行われる処理に関するログ
  各要素の処理を収集し監視することで仮想通貨交換所システムでの異常を検知する。また、適切なログを記録することで仮想通貨交換所システムの処理が適切に行われていることの証明や、インシデント発生後の原因究明に用いられる。
- 署名鍵のアクセスログ
  署名鍵の活性/非活性状態の変更記録、活性化された署名鍵へのアクセス記録(署名作成の場合は署名対象のハッシュ値も含む)、バックアップ・リストアなどについて、日時、操作元端末、操作者(役割ではなく実際の操作員を特定できる情報)等を取得、記録するとともに、運用規程や業務時間・記録等との不整合がないか、週次点検などで定期的に確認すること。また、署名鍵をオンライン管理している場合等においても、操作者がトランザクション署名を作成するなどの操作は、同様に記録・確認すること。
- 自社が管理しているウォレットの操作ログ
  署名鍵やバックアップの意図しない漏えいにより操作があった場合を想定して、ウォレットの操作ログを安全に保管するとともに、分散台帳上の取引との整合性をリアルタイム監視する。意図しない操作が管理するアドレスで実施された場合には、素早く検知し対処できるようにする。
- 管理用リモート端末のアクセスログ
  仮想通貨交換所システムに対して管理用リモート端末からのアクセスを認めている場合、端末の認証・認可、操作者の認証・認可を行った上で、その日時、アクセス元IPアドレス、端末情報(端末ID、可能であれば端末の最新の安全性評価情報など)、操作者情報(操作者IDなど)、アクセス先IPアドレス(またはホスト名)などを取得、記録する。端末情報、操作者情報、アクセス先IPアドレス、アクセス日時などが許可された範囲内であることを確認すること。
- インターネットなど外部との接点における通信ログ
  インターネットなど外部からの仮想通貨交換所システムに対する通信は、9.2.9.1節で述べるように接続可能な外部ネットワークや通信可能なプロトコルなどを制限することが望ましい。制限されたネットワークからの通信や制限されたプロトコルを用いた通信はファイアウォールなどで遮断されるが、こうしたログを適切に記録することは不正アクセスから利用者を守る上では仮想通貨取引所固有の対策ではなく情報セキュリティ上有効である。
  仮想通貨取引所システムからインターネット・その他業務システムへの通信といった保護対象から発される通信については一般的には記録の対象となることは少ないが、こうした記録は署名鍵の不正な利用、署名鍵の奪取などのインシデント発生時における調査や、インシデント検知につながる端緒として有用であるため、プロトコル・通信先に応じて全取得やフロー情報による記録が望ましい。
- 顧客のアクセスログ
  顧客のアクセスログを取得し、不正ログインや不正なリクエストを検知することが望まし

い。これらは事後の証明ともなりうる。また、不正ログインを検知した際に、顧客に伝達することが望ましい。

- 利用者が不正アクセスに気づく端緒の提供
  ログイン時に電子メールやプッシュ通知などを用いて利用者に知らせること、利用者が後からログイン履歴を確認し、アクセス元の地域やIPアドレス、端末環境などについて把握できるようにすることは、事後的に不正アクセスを把握する上で有効である。また、普段と異なるアクセス元や端末からのログイン、同一IPアドレスからの他IDに対する連続したログイン試行などを検出し、利用者に警告を発したり、アカウントを保護する機能は、不正アクセスから利用者を守る上で有効と考えられる。

- 監視カメラの記録している画像・映像、入退館記録など
  監視カメラの記録している画像・映像や入退館記録を適切な期間保存することによって、インシデント発生時に物理的安全管理措置が適切に機能していたか、事後的に検証することができる。

上記のようなログを総合的に監視することで仮想通貨交換所システム全体の異常や、不正アクセス、マルウェアなどによる不正な処理の実行を検知することが重要である。また、これらの証跡を記録することは、内部不正抑止につながるとともに、有事の際に不正のない内部関係者の潔白を早期に証明するためにも重要である。上記に示したようなシステム監視のためにセキュリティオペレーションセンター(SOC)を運用することも考えられる。SOCの運用において脅威の検知と通知について信頼できる事業者に委託することも考えられる。

7.3.9 通信のセキュリティ

JIS Q 27002:2014「13 通信のセキュリティ」に準じる必要がある。

特に交換所においては、インターネット上からアクセス可能な状態で資産が管理されていることから、情報の流出防止策として、未然防止策、検知策、対応策、回復策をリスクに応じて検討する必要がある。

7.3.9.1 ネットワーク管理策(JIS Q 27002:2014 13.1.1)について

一般的なシステムに対するセキュリティ管理策と同様に、外部ネットワークとの境界を明確し、ネットワークへのシステムの接続の制限（ファイアーウォール等）、不要なサービスやポートの停止、ログ取得と監視、不正侵入検知などの管理策を検討し実施する。また、停止した場合に交換所システムの運営に大きな支障を与える機能（例えば、顧客インタフェース、トランザクション送信機能やブロックチェーンデータ取得機能など）は可用性を確保する目的から、例えば、アクセス過多での負荷分散や、DDoS攻撃を想定した対策が必要となる。

ログについては外部ネットワークとの接点における監視だけでなく、内部侵入を検知するために内部システムのログも監視する必要がある（7.3.8節に関連)。

交換所の機能の一部を提供するモジュールが遠隔配置されている場合には、モジュール間の通信の傍受や改ざんなどを防ぐため、SSHやTLSなどの標準的なセキュリティプロトコルを用いて、通信相手を適切に認証し適切に暗号化された通信を行い、当該通信に係るログを保存しておくことが望ましい。

7.3.9.2 ネットワークの分離(JIS Q 27002:2014 13.1.3)について

交換所のシステムがネットワーク経路での攻撃にさらされる危険性を低減させる目的から、インターネットや他のシステムとの接続を最小限に制限することは重要である。例えば、以下のようにネットワークの分離や接続制限について検討する必要がある。

- 交換所システムと他の情報系システムとの分離
    - 対策の目的:標的型攻撃など外部からのマルウェア感染により日常業務で用いる情報システムが踏み台にされ、交換所システムに接続されることを防止する。
    - 対策:日常業務で用いる情報系システムと交換所システムのセグメント分離やアクセス制限によってネットワークを分離する。
- インターネット接続箇所の分離
    - 対策の目的:インターネットに接続する要素を最小化して、他をインターネットからは分離することで、インターネット経由の攻撃により署名鍵等の重要な情報へアクセスされることを防ぐ。
    - 対策:トランザクション送信機能やブロックチェーンデータ取得機能の実行、あるいは交換所の機能の実現にインターネット上の外部サービスを利用する場合などは、ネットワーク接続を行う最小限度の機能をモジュール化し、DMZ(DeMilitarized Zone)に配置するなど他のシステム要素とネットワークを分離する。また、各モジュールが外部サービス等に接続する場合には、そのサービスへのアクセス制御を適切に実施すること。
- 交換所管理系で用いる端末の制限
    - 対策の目的:取引所管理系で用いる端末の乗っ取りによる不正操作を防ぐ。
    - 対策:取引所管理系を操作する端末や取引所管理系に対して操作を指示する管理ツールを稼働する端末など、交換所システムに接続できる端末を制限する。

7.3.10 システムの取得，開発及び保守

JIS Q 27002「14 システムの取得，開発及び保守」に準ずる必要がある。

取引所で取り扱われる仮想通貨は複数の事業者により取り扱われる流通量が高い仮想通貨から、新興な仮想通貨まで多岐に渡る。これら仮想通貨が用いるブロックチェーン・ネットワークの特性も様々であることから、JIS Q 27002に加え、システムの取得・開発、保守に係る危険性を低減させることは重要である。例えば以下のような手法は有効な対策である。

- ソフトウェア開発手法
  取引所システムのソフトウェアの開発では、セキュアコーディングやコードレビューといった堅ろうろうなソフトウェアの開発手法を用いる。開発部門だけでなく、運用部門も含めたコードレビューは、システム運用の観点からぜい弱性の検出につながるため有用である。
- ペネトレーションテスト
  ペネトレーションテストの実施は、システムに対する既知のぜい弱性の有無の検出につなつながり、攻撃者からの攻撃リスクを未然に削減することが可能である。
- ブロックチェーン・ネットワークも含めた結合テスト
  テストネットだけでなく、実ネットワークも用いたテストを実施する。本番環境でのテストは限界がある(負荷など)ことを理解し、リスク評価を実施する。

- 運用における権限分離
  コードレビューを経たソフトウェアのプロダクション環境への展開をシステム運用部門に限定するといった権限分離は、内部からの改ざん攻撃を防ぐために有用である。
- 機器のデフォルト（工場出荷時）値の使用禁止
  ハードウェア・ソフトウェア、開発環境・プロダクション環境に関わらず、工場出荷時に設定されたパスワードなどの認証情報を使用してはいけない。

7.3.11 供給者関係

JIS Q 27002:2014「15 供給者関係」に準ずる必要がある。

ウォレットに関連するサービスを外部委託先として利用する場合は、それ自体の技術的安全性が担保されていればよい選択肢となり得る。

マルチシグに利用する署名鍵を外部に委託していたり、交換所システムをクラウドサービス上に実装している場合などは、それぞれ委託先やクラウド事業者のセキュリティ管理についてJIS Q 27002:2014に沿った管理策を行うこと。

7.3.12 情報セキュリティインシデント管理

JIS Q 27002:2014「16 情報セキュリティインシデント管理」に準ずる必要がある。

サイバー攻撃は複雑化しており、特に交換所においては過去に例のない事故も起こりえる。事前に想定した脅威に対する備えとしての安全管理策に加え、未知の脅威によるインシデントが起きてしまった場合に備え緊急対応体制を整えておく必要がある。例えば、組織内CSIRT(Computer Security Incident Response Team)を設置し、外部機関との連携関係の構築が考えられる。

7.3.13 事業継続マネジメントにおける情報セキュリティの側面

JIS Q 27002:2014「17 事業継続マネジメントにおける情報セキュリティの側面」に準ずる必要がある。
困難な状況（災害や危機）における情報セキュリティの確保のため、要求事項を決定し、プロセス，手順及び管理策を確立し，文書化し，実施し，維持することが必要である。このとき、以下の内容を含むことが望ましく、対応策を実施する場合や困難な状況が発生した場合における管理策を定期的に検証しなければならない。また、状況によってはシステムを停止することも必要である。

- 設備（事務室等に利用しているものを含む）が利用できなくなった場合。
  - 停電
  - 建物の損壊
  - 天災（地震、火災（近隣の火災による放水を含む）、断水、水害等）
  - その他、法規制により立入が規制された場合や、設備が利用できなくなった場合
- システムの継続が困難になった場合
  - 自家発電装置の継続運転が困難になった場合

- 交通機関の長期間途絶、感染症のまん延、天災等による要員の不足
- 通信ネットワークの途絶
- 装置の損傷（故障）
- システム障害（プログラム障害、サイバー攻撃等の原因は問わない）
- ハードウェアウォレットやペーパーウォレット等の紛失
- 契約先事業者の事業停止
- 署名鍵の漏えい、消失

- 事業そのものが困難になった場合
  - 法規制による業務停止命令

7.3.13.2 システム可用性の確保

システム全体として、利用者数、取引のピーク日・ピーク時間や、レスポンスタイム、メンテナンスにかかる時間や頻度、運用要員の確保状況等を考慮し、利用者にとって十分な可用性を確保するよう、冗長性を持つ必要がある。また、一定のしきい値（ピーク時間の取引数、ピーク時間のメモリ使用率等）をもって、能力の拡充を行うことも検討する必要がある必要がある。

7.3.14 順守

各国の法令やガイドライン等を遵守すること（日本国内においては付録3参照）。

7.4 その他の仮想通貨交換所システム固有の留意点

7.4.1 メンテナンス時ユーザへの事前告知

定期的なメンテナンスを行う、特に深夜などにサービス停止を行う場合には、そのスケジュールを事前に公開することが望ましい。また緊急メンテナンス時にサービス停止する場合には、通常のWebサーバや電子メール等による告知方法だけではなく、Webサーバへのアクセス集中を回避するために他のFQDN/IPアドレスによるサービスから障害情報を提供することが望まれる。さらに電子メールやSMS、ソーシャル・ネットワークなど、実際にサービスされているサーバ群とは異なる他のチャネルによる告知を行うことが推奨される。

また突発的に起きうる外部からの攻撃などの事由によるサービス停止の場合には利用者保護の観点から影響範囲を最小に留めるよう努力することが望まれる。

8 今後の検討課題

(追記予定）
現行版はLayer 2ネットワークの利用や、分散交換所（Decentralized Exchange）はスコープ外としている。

付録1 鍵管理の基本事項

暗号鍵管理の基本

署名鍵管理、特にその運用について基本的な考え方を示す。
鍵に紐づけられる情報の重要性が高いほど、消失、漏えい・盗難を含め内外からの不正な操作を回避するための厳格なアクセスコントロールが求められる。
その手法として、権限分離や活性状態の制御、承認プロセスの介在などが挙げられる。

署名鍵が提供する機能(セキュリティサービス)は、情報源の認証(Source Authentication)、完全性の認証(Integrity Authentication)、および否認防止のサポート(Support for Non-Repudiation)である。[SP800-57Pt1]Table5
各機能を実現しつつ、またそれらを毀損する脅威(鍵の消失、漏えい・盗難、不正利用)を防ぐために、一般的な鍵管理の基本として以下の3つがある。
- 鍵運用管理における権限分離
- 活性化状態管理
- 明確な意思決定プロセス

- 鍵運用管理における権限分離
事業者における鍵管理においては、外部からの攻撃はもちろん、内部不正についても十分な対策が求められる。内部においても単独犯による不正を困難すとるためには、適切な権限分離を設計する必要がある。

鍵の主要な操作とその権限分離の例を表9-1に挙げる。

表9-1 鍵の主要な操作とその権限分離の例

	鍵生成	鍵バックアップ	鍵活性化	署名操作	鍵廃棄
運用責任者	承認	承認			承認
鍵操作員	実施	実施			実施
署名責任者			承認	承認	
署名操作員			実施	実施	
ログ検査者	検査	検査	検査	検査	検査

例えば、表9-1のように、主要な操作に対して承認、実施、検査の3種類に権限を分離するとともに、各権限を排他的に設定することで単独犯による内部不正を困難にする。鍵操作員・署名操作員は、各操作を実施する権限を持つものの、それぞれ運用責任者・署名責任者の承認がなければ操作の実施ができないものとする。承認の有無は必ずしも操作の技術的制限につながらない

が、例えば鍵操作が必要なエリアへの入退に必要な物理鍵の管理を運用責任者が行う(あるいは運用責任者の指示によって他の操作員が制御する)などによって、承認プロセスを物理的な制約に紐づけることが推奨される。

- 鍵の生成

署名鍵(公開鍵暗号における検証鍵)は、正当な鍵所持者のみが所持していることが前提となる。正当な鍵所持者以外が生成した鍵は、正当な鍵所持者以外による複製・漏えいの防止や鍵の消去などを保証することが技術的に難しい。このため、原則として正当な鍵所持者が鍵生成や複製を行う、あるいは他者が鍵生成する場合もICカードのように複製が技術的に困難な唯一性を保証できる鍵管理環境下で鍵生成した上で鍵所持者に配布されること[10]が求められる。

さらに、鍵生成にあたっては、そこで用いられる乱数生成器の実装が重要になる。鍵の強度は一般に暗号アルゴリズムと鍵長の組み合わせによって評価される。鍵を解読する行為は、鍵が存在し得る数学的空間において鍵を探索、特定する行為である。この探索空間において鍵が存在する確率が均等であれば、鍵強度は探索空間の広さに依存する。乱数生成器に十分な乱雑性(探索空間における存在確率の均等性)がなければ、解読に必要な探索空間も限定されることになり、一般的な鍵強度を有することができない。暗号学的に十分な乱雑性を持つ乱数生成器の実装は、ごく一部の認定された実装環境に限られており、それ以外の乱数生成器を用いた場合には、一般的に知られている鍵強度を維持できていないことに留意する必要がある。

- 鍵の廃棄

鍵管理装置を廃棄する場合、管理していた鍵も合わせて所定の廃棄手続きを行うことが求められる。廃棄処理が不十分な場合、記憶装置の残存磁気などから過去に管理していた鍵の解読などが可能となり、鍵の漏えい・盗難に直結する。特に仮想通貨においては、その仕組み上公開鍵を無効化することはできないため、廃棄した後に署名鍵が漏えい・盗難された場合にも不正利用の脅威は無視できないことになる。このため、鍵廃棄時には記憶装置に残存磁気が残らないよう、記憶装置のゼロ化[11]を行うこと、物理的なアクセスが不能となるよう(HDDであれは円盤の破壊、ICカードであれば接触端子の破壊など)装置そのものを物理的に破壊することが求められる。鍵管理機能を外部委託する場合には、同等の運用を保証する契約を確認するなどが望ましい。

- 活性化状態管理

暗号鍵が署名(または暗号化など)が可能な状態を活性状態、そうでない状態を非活性状態と呼ぶ。暗号鍵の不正操作リスクを最小化するためには、活性状態の期間を業務合理的な範囲で必要最小限に留めることが求められる。最も業務合理的なのは常に活性状態にあることはいうまでもないが、明らかに操作不要な時間帯に活性状態としておくことは、リスクを高めることになる。逆に、署名操作を必要とする都度に活性化/非活性化操作を行うことは、操作頻度が高い場合は非合理的と言える。

どこまできめ細かく制御するかは業務合理性と安全性のバランスによって決める必要があり、そのようなリスク受容にもとづいて鍵管理が行われていることは、(鍵管理規程の掲載など)利用者が確認できることが望ましい。

---

[10] ただしICカード上で鍵生成したことを技術的に証明することは難しく、現状こうした運用が法的に認められているのは電子署名法や公的個人認証法で認定されたごく一部の事業者に限られていることに留意されたい。

[11] 記憶領域を0x00や0xFFなどで上書きし、残存磁気などを利用した元データの読み取りなどを困難とする処理。記憶装置の集積度や物理媒体の違い(磁気ディスクかSSDか)などによって処理方法の詳細が異なる点に注意する必要がある。

- 明確な承認プロセス

鍵管理にかかわるいくつかの重要な操作(例えば鍵の廃棄や高額取引への署名など)については、明確な承認プロセスを必要とする。

承認プロセスには、当該操作を行うことのリスクを事業者が適切に認識・受容し、操作要求の正当性について一定の責任を負うことが求められる。このため、リスクの高い操作を明確な承認プロセスなしに行うことは責任放棄であり、承認プロセスはあるものの適切な判断や意思決定を伴わない場合は、一切の責任を事業者が負うことになる。リスクの高い操作とは、一概に規定することは難しく、鍵の安全性に限らず事業継続性に鑑みて識別する必要がある。鍵管理において強いて挙げれば、例えば鍵の廃棄や特定の署名(高額取引など)、一部の例外的な作業などが挙げられるが、高リスク取引のしきい値が一般の銀行取引と証券取引で異なるように、取引の内容に応じて適切に識別する必要がある。通常の取引操作に対しては機械的に処理しつつ、一定時間内の取引額が規定額を越えた取引に関しては例外処理として承認プロセスを求めるなどの運用が考えられる。前述の権限分離において承認と実施を分離することも、こうした意思決定の有無を明らかにすることを意図している。

付録2署名鍵に関するリスクと管理策の対応表

7.3.6で、署名鍵に関するリスクを示した。本項では、それらのリスクに対する主なセキュリティ管理策として、後述の13種類の管理策が挙げられる。各管理策が前述のリスクとどう対応するかについて、表1～4に示す。各リスクに対する管理策の有効性はあくまでも一般論であり、実効性は各システムおよびその運用の特性に応じて個別に評価する必要がある。また、システム構成や運用に応じて、ここに挙げた以外にも有効な管理策がある可能性があることを念頭に置かれたい。

表1　署名鍵の消失リスクとセキュリティ管理策の関係

リスク	署名鍵のバックアップ	署名鍵のオフライン化	秘密分散	マルチシグ	署名鍵へのAPI監視/アクセスログ監査	厳格なアクセス制御	ペネトレーションテスト	セキュアコーディング	多要素認証，リスクベース認証など	ダブルチェック、ツーパーソンオペレーション	オペレータによる確認・手動処理	署名鍵へのアクセスログと認証ログの整合性監査	追加認証、警告画面
エンドユーザ自身の悪意による消失	○										○	○	
顧客資産管理系の管理者の悪意による消失	○				○	○				○			
エンドユーザへのなりすましによる消失	○					○			○		○		
取引所内部犯(管理者なりすまし)による消失	○				○	○			○				
Tx署名部への不正侵入による消失	○				○	○	○						
入コイン判定部への不正侵入による消失	○				○	○	○						
顧客資産管理系への不正侵入による消失	○				○	○	○						
取引所管理系への不正侵入による消失	○				○	○							
Tx署名部の意図しない挙動(バグ)による消失	○				○			○					

入コイン判定部の意図しない挙動(バグ)による消失	○				○			○				
顧客資産管理系の意図しない挙動(バグ)による消失	○				○			○				
取引所管理系の意図しない挙動(バグ)による消失	○				○			○				
エンドユーザの誤操作による消失	○											○
顧客資産管理系の管理者の誤操作による消失	○				○					○		

表2　署名鍵の漏えいリスクとセキュリティ管理策の関係

リスク	署名鍵のバックアップ	署名鍵のオフライン化	秘密分散	マルチシグ	署名鍵へのAPI監視/アクセスログ監査	厳格なアクセス制御	ペネトレーションテスト	セキュアコーディング	多要素認証，リスクベース認証など	ダブルチェック、ツーパーソンオペレーション	オペレータによる確認・手動処理	署名鍵へのアクセスログと認証ログの整合性監査	追加認証、警告画面
エンドユーザ自身の悪意による漏えい		○	○								○	○	
顧客資産管理系の管理者の悪意による漏えい		○	○		○	○				○			
エンドユーザへのなりすましによる漏えい		○	○			○			○				
取引所内部犯(管理者なりすまし)による漏えい		○	○		○	○			○				
Tx署名部への不正侵入による漏えい		○	○		○	○							
入コイン判定部への不正侵入による漏えい		○	○		○	○	○						
顧客資産管理系への不正侵入による漏えい		○	○		○	○	○						
取引所管理系への不正侵入による漏えい		○	○		○	○	○						
Tx署名部の意図しない挙動(バグ)による漏えい		○	○		○			○					
入コイン判定部の意図しない挙動(バグ)による漏えい		○	○		○			○					
顧客資産管理系の意図しない挙動(バグ)による漏えい		○	○		○			○					

取引所管理系の意図しない挙動(バグ)による漏えい		○	○		○			○				
エンドユーザの誤操作による漏えい		○	○							○	○		○
顧客資産管理系の管理者の誤操作による漏えい		○	○		○							

表3　署名鍵の盗難リスクとセキュリティ管理策の関係

リスク	署名鍵のバックアップ	署名鍵のオフライン化	秘密分散	マルチシグ	署名鍵へのAPI監視/アクセスログ監査	厳格なアクセス制御	ペネトレーションテスト	セキュアコーディング	多要素認証，リスクベース認証など	ダブルチェック、ツーパーソンオペレーション	オペレータによる確認・手動処理	署名鍵へのアクセスログと認証ログの整合性監査	追加認証、警告画面
エンドユーザ自身の悪意による盗難		○	○								○	○	
顧客資産管理系の管理者の悪意による盗難		○	○			○				○			
エンドユーザへのなりすましによる盗難		○	○			○			○				
取引所内部犯(管理者なりすまし)による盗難		○	○			○			○				
Tx署名部への不正侵入による盗難		○	○		○	○	○						
入コイン判定部への不正侵入による盗難		○	○		○	○	○						
顧客資産管理系への不正侵入による盗難		○	○		○	○	○						
取引所管理系への不正侵入による盗難		○	○		○	○							

表4　署名鍵の不正利用リスクとセキュリティ管理策の関係

リスク	署名鍵のバックアップ	署名鍵のオフライン化	秘密分散	マルチシグ	署名鍵へのAPI監視/アクセスログ監査	厳格なアクセス制御	ペネトレーションテスト	セキュアコーディング	多要素認証，リスクベース認証など	ダブルチェック、ツーパーソンオペレーション	オペレータによる確認・手動処理	署名鍵へのアクセスログと認証ログの整合性監査	追加認証、警告画面
エンドユーザ自身の悪意による不正利用			○	○							○	○	○
顧客資産管理系の管理者の悪意による不正利用			○	○	○	○				○			
エンドユーザへのなりすましによる不正利用			○	○		○			○				
取引所内部犯(管理者なりすまし)による不正利用			○	○	○	○			○				
Tx署名部への不正侵入による不正利用			○	○	○	○	○						
入コイン判定部への不正侵入による不正利用			○	○	○	○	○						
顧客資産管理系への不正侵入による不正利用			○	○	○	○	○						
取引所管理系への不正侵入による不正利用			○	○	○	○							

付録3 各国における固有の要件

FATF加盟国

資金洗浄のリスク (Anti Money Laundering)

詐欺やランサムウェアの身代金、ダークマーケットでの取引などの犯罪に利用された仮想通貨を、現金化や資金洗浄する経路として、仮想通貨交換所が利用されるケースがある。取引所のアドレスに直接送金されるケースの他、利益移転などを通じて結果的に犯罪収益が現金化されるケースも考えられる。

テロ支援金融のリスク (Counter Financing of Terrorism)

金融機関に口座を開くことができないテロ組織が、仮想通貨による寄付を受け入れているケースがある。仮想通貨交換所からテロ組織に対する直接送金を止めることはできるが、仮想通貨交換所から利用者の管理する仮想通貨ウォレットに仮想通貨の現物を引き出し、そこからテロ組織に送金することを止めるのは難しい。

日本

犯罪による収益の移転防止に関する法律(犯罪収益移転防止法)
http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=419AC0000000022

資金決済に関する法律（平成21年法律第59号）
http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=421AC0000000059

資金決済に関する法律施行令（平成22年政令第19号）
http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=422CO0000000019

仮想通貨交換業者に関する内閣府令（平成29年内閣府令第7号）
http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=429M60000002007

事務ガイドライン第三分冊：金融会社関係
本文
https://www.fsa.go.jp/common/law/guide/kaisya/16.pdf

別紙様式
https://www.fsa.go.jp/common/law/guide/kaisya/y16.pdf

概要
https://www.fsa.go.jp/policy/virtual_currency/01.pdf

概要（英訳版）
https://www.fsa.go.jp/policy/virtual_currency/02.pdf

自主規制(日本仮想通貨交換業協会 http://jvcea.jp (認定自主規制団体))

（日本固有の要件、権利化されているため保留、犯収法改正に係る該当資料を参照し削除）
　なお、今後、郵送物なしで口座開設が一般的になると考えられ、利用者の顔写真／動画の登録を必須化すべきである。SNS等から窃盗した顔写真／動画による不正登録を防止するため「右を向いてください、口を開けてください」などランダムな指示をスマホから出し、利用者がその通りにすれば窃盗画像／動画でないと判定する方法が考えられる（JP-A-2018-18481）。生の顔写真／動画は強力な心理的防犯効果となり、逆にこれ以外の、身分証等は容易に偽造できるので証拠能力がなく犯人逮捕につながらない。

参考文献 (Bibliography)

1. ISO/IEC 27001:2013 (JIS Q 27001:2014) Information technology -- Security techniques -- Information security management systems -- Requirements
2. ISO/IEC 27002:2013 (JIS Q 27002:2014) Information technology -- Security techniques -- Code of practice for information security controls
3. Terminology I-D

Cryptoassets Governance Task Force

Security Working Group

- チェア
  - 楠 正憲 (Japan Digital Design株式会社)
  - 松本 泰 (セコム株式会社 IS研究所)
  - 崎村 夏彦 (株式会社野村総合研究所)
- エディタ
  - 佐藤 雅史 (セコム株式会社 IS研究所)
  - 島岡 政基 (セコム株式会社 IS研究所)
- メンバー
  - 川畑 雄補 (株式会社アプルーシッド)
  - 小宮山 峰史 (株式会社bitFlyer)
  - 志茂 博 (コンセンサス・ベイス株式会社)
  - 須賀 祐治 (株式会社インターネットイニシアティブ)
  - 杉井 靖典 (カレンシーポート株式会社)
  - 中島 博敬 (株式会社メルカリ)
  - 林 達也 (株式会社レピダム)
  - 樋田 桂一 (一般社団法人 日本ブロックチェーン協会)

Board of Trustees

- 岩下 直行 (京都大学)
- 上原 哲太郎 (立命館大学)
- 松尾 真一郎 (ジョージタウン大学)