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

## － 第3版 －

Cryptoassets Governance Task Force[1]

2022年03月22日

[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。本書で想定する暗号資産カストディアンの基本モデルは5章で示すが、この基本モデルとは異なる形態のシステム、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）等についても、参考とできる箇所については参考としていただくことを期待する。

また、本文書は網羅的に検討することを主眼において策定しているため、検討可能な項目のみを評価するのではなく、検討が難しい項目についても、技術の進化や状況の変化に応じて検討が再開できるよう、その理由を記録しておくことを期待する。

# 第3版の発行にあたって

第2版の発行後、幸いにして日本国内における暗号資産の流出事案は発生していない。このことは、第2版で整理した推奨事項が完全なものであることは意味していない。規制の粒度や範囲が異なるため一概には言えないものの、海外事業者で発生した流出事案の中には第2版までに記載した内容を充足していないと思われる事案もある。また、技術の進化や、実装方法の多様化によって、暗号資産を安全に保管するために必要な対策は多岐に渡ってきている。

このため、第3版においては、第2版までの記載内容のブラッシュアップとは異なり、以下の点を主に修正した。

1. 発生した事案の再発防止策とその考え方について明記（パブリックコメントの内容を反映）
2. 恣意的に本ドキュメントの一部のみ適用するのではなく、適用しない範囲についてはその理由を添えて適用除外とすることを明記
3. DEXをスコープ外としていた記載を削除し、適用可能な内容については適用できるように変更
4. 付録Aとしていた鍵管理の基本事項を本文中に記載

# 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ことが必要であると考える。
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（利用者や委託元）に対して、顧客の暗号資産アドレスから、業者が署名鍵を管理する業者の暗号資産アドレスに、暗号資産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得る社会的な影響

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（Webサイトの閲覧や、電子メールの送受信など）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
- LightningネットワークなどのLayer 2技術の利用

なお、暗号資産カストディアンのみならず、他の事業者等[2]にも参考になる内容を記載している。

# 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

アドレス ( Address )
　暗号資産を所有することを示し、ある検証鍵とひも付けされた識別子。

管理者 ( Administrator )
　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。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。

ブロック ( Block )
　ブロックチェーンの基本的な単位。ブロックチェーン上のトランザクションには、前のブロックの暗号学的なハッシュ値が含まれる。

[2] 自らの署名鍵を利用して（暗号資産以外も含め）資産の管理や移転を行う事業者。

承認( Confirmation )

コンセンサス・アルゴリズムによって定められた承認作業。ブロックやその中に含まれるトランザクションがマイナーや当該ブロックチェーンの利用者に承認された状態を指す。

暗号資産 ( Cryptoassets )

暗号技術を活用したブロックチェーン等の分散台帳または同様の技術によって実現された、電子的に交換または移転可能な電子的な価値の表現。

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業務 ( Cryptoassets Custody Service )

暗号資産の現物を管理する業務。例えば、暗号資産交換業や暗号資産ウォレットの管理などがある。

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。

暗号資産交換業者 ( Cryptoassets Exchange Service Provider )

暗号資産交換所を運営する事業者。

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。顧客の暗号資産を管理するため、暗号資産カストディシステムが含まれる。

デジタル署名 ( Digital Signature )

暗号学的に計算された値のことで、データの受信者が当該データの完全性を確認することができるように当該データオブジェクトと関連づけられたもの。

分散(型)台帳 ( Distributed Ledger )

暗号資産に関する、合意された処理に基づく分散データベース。

フォーク ( Fork )

ブロックチェーンが分岐すること。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 ( Accidental fork ) : 偶発的にほぼ同時間にブロックのマイニングが行われて、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 ( Soft fork ) : 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、ウォレットの実装に影響しないもの。ただし、マイナーの実装に影響する場合がある。
- ハードフォーク ( Hard fork ): 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。マイナー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暗号資産のことをフォークコインと呼ぶ。

ハッシュレート ( Hash Rate )
ノードが生成できる、単位時間あたりのハッシュ値の量。一般的には1秒あたりの値。

入庫（入コインともいう）( Incoming transaction )
他のアドレスから自己のアドレスに対する暗号資産の移転。

KEK ( Key Encryption Key )
署名鍵を共通鍵暗号方式で暗号化するために用いられる鍵データ。

マスタードシード ( Master seed )
決定性ウォレットにおいて、ひとつまたは複数の署名鍵を生成するための初期データ。

マイニング ( Mining )
Proof-of-Work や Proof-of-Stake などコンセンサスルールを利用し、トランザクションをバリデーションした上で、ノードで受信したトランザクションをブロックに追加するプロセス。

マイナー ( Miner )
マイニングを行う者。場合によりノードやソフトウエア実装を指すこともある。

操作員 ( Operator )
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。

出庫 ( Outgoing transaction )
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。

再収縮[リオルグ] ( Reorganization )
一時的に分岐された複数のチェーンから、何らかのアルゴリズムに基づいてひとつのチェーンに収束されること。

署名鍵 ( Signature Key )
検証鍵と対をなす鍵データで、デジタル署名を作成する際に用いられる。署名鍵の所有者は署名鍵を秘密に管理しておく必要がある。
暗号資産においては主にトランザクションに署名する際に用いられる。
秘密鍵、または署名用秘密鍵と呼ばれることもある。

スマートコントラクト ( Smart Contract )
ブロックチェーンネットワーク上で実装される、自動的に処理される機械的な手順。

トークン ( Token )

数量を示す汎用的な単位。意味合いは文脈によって異なり、価値の量を示すだけではなく、投票権や受益権の数やその他の数量を示すことがある。
また、（本ドキュメントではこの用法では用いていないが）API中に利用される認証用データのことを示すこともある。

トランザクション ( Transaction )
価値の移転などを示すデータの構造のこと。

バリデーション（検証）( Validation )
与えられたトランザクションやブロックの正確性や一貫性を確認すること。具体的には、デジタル署名が施されたデータの完全性や、他のトランザクションやブロックとの整合性を検証することが一般的である。トランザクションに対する検証を重ねることで、ブロックに対する検証を行うことが可能となる。

検証鍵( Verification Key )
署名鍵と対をなす鍵データで、デジタル署名の検証に用いられる。公開鍵と呼ばれることもある。

ウォレット ( Wallet )
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、かつ署名鍵が活性状態にあり、自動処理によって暗号資産を出庫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、かつ署名鍵が非活性状態にあり、操作員の明示的な操作がない限りは、出庫ができないウォレットのことである。

ホットウォレットとコールドウォレットという相異なる概念の間には、ウォレット自体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。

表3-1　ウォレットの形態の例

| | 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 |

# 4 略語集

本ドキュメントには定義すべき略語は本文初出時に正式名称を記載している。

# 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 本書が想定する基本モデルと各機能的要素

本書が想定する基本モデルを図5-1で説明する。なお、実際の機能的要素は業態や事業者によって異なることが考えられる。

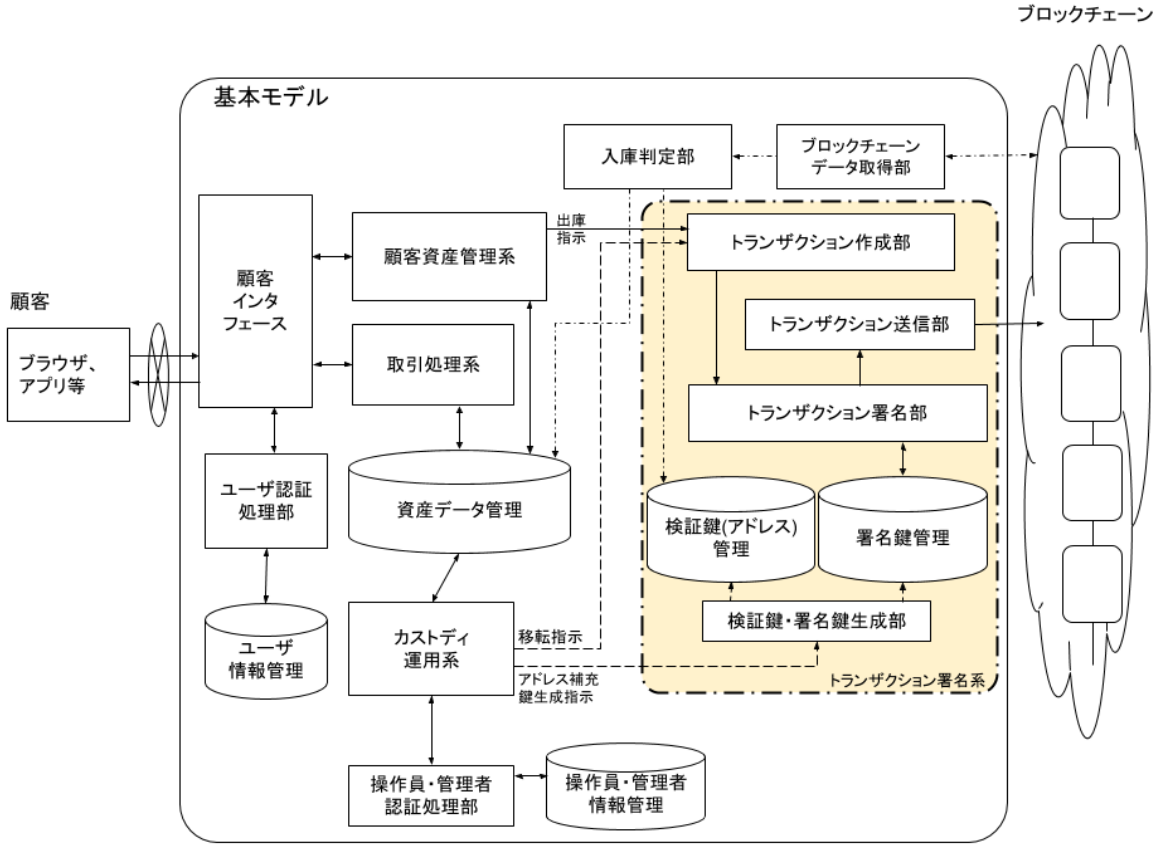


図5-1 本書の想定する基本モデル[3]

[3] ここではトランザクション署名系をオンラインで運用する場合のモデルを示している。トランザクション署名系の一部をオフラインで運用する場合については8.3.6.2項を参照のこと。

表5-1 機能的要素

| 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。入出金や入出庫の指示を受け、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。 |
| ブロックチェーンデータ取得部 | | ブロックチェーンネットワーク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。 |
| 入庫判定部 | | 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、指定アドレスに入庫されていることを確認する。入庫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、暗号資産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 | | 法定通貨や暗号資産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、事業者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。ブロックチェーンネットワークの他のノードと接続する。 |
| | 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。 |
| | 検証鍵・署名鍵生成部 | 検証鍵・署名鍵の生成を行う。生成した署名鍵は署名鍵管理へ、検証鍵やアドレスは検証鍵(アドレス)管理へ登録される。 |

| | |
|---|---|
| カストディ運用系 | 暗号資産カストディアンの操作員や管理者が用いる機能群。操作員・管理者からの操作に基づいて、新たな署名鍵の生成や、暗号資産の移転を指示する。 |
| 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検証鍵（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、ウォレットにトランザクション署名系の機能を集約して実装している場合もある。

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. 顧客が暗号資産カストディアン指定の銀行口座に送金する。
2. 暗号資産カストディアン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。

[入庫フェーズ]

1. 顧客が暗号資産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（他の暗号資産カストディアンやWebウォレットなど）を通じて行う。
2. 暗号資産カストディアンは入庫判定部で指定のアドレスに暗号資産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。

[顧客からの出庫指示]

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（出庫指示）。
2. 出庫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（移転先アドレスや暗号資産の額など）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. 操作員・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、暗号資産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. 操作員・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、出庫指示の手順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

暗号資産カストディアンが保護するべき鍵データとして、署名鍵がある。署名鍵の安全性に関連する情報として、署名鍵を保護するKEKや、署名鍵の生成に用いられるマスターシードがある。鍵には以下のようなものがある。基本モデルにおいて扱うそれぞれの具体的な利用形態もあわせて記載する。

表5-2 本基本モデルにおける鍵の種類

| 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。暗号資産を移転するトランザクションの作成には、暗号資産を所有するアドレスにひも付けされた検証鍵に対応する署名鍵を用いた署名が必要である。 |
| 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。 |
| KEK<br>( Key Encryption Key ) | 署名鍵を保護する共通鍵暗号方式における鍵データ。 |
| 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。 |

ブロックチェーンをベースとした暗号資産の説明において、トランザクションのデータ完全性を確保するための暗号技術として公開鍵暗号方式をベースとしたデジタル署名が用いられる。このとき、教科書的には「秘密鍵 ( private key ) と公開鍵 ( public key ) と呼ばれる2つの鍵で構成される鍵ペアを生成する」と説明されることが一般的である。他方、共通鍵暗号方式における暗号化 ( encryption ) において用いられる鍵データも秘密鍵 ( secret key ) と呼ばれている。日本語で利用用途が異なる secret key も private key も同じ訳語が利用されていると、読み手側が文脈に応じて解釈するため、混乱の原因となっている。

このため、本ドキュメントにおいてはデジタル署名に用いられる2種類の鍵データを署名鍵 ( signature key ) と検証鍵 ( verification key ) という用語に統一して説明している。つまり、公開鍵暗号方式における鍵データの名称を秘密鍵・公開鍵ではなく、それぞれ署名鍵・検証鍵と記載している。また署名鍵を保護する共通鍵暗号方式における鍵データの名称を、秘密鍵ではなくKEK ( Key Encryption Key ) と記載している。

### 5.4.2 鍵管理の基本事項

暗号鍵を扱う事業者は、そもそも暗号鍵管理全般について理解しておくことが求められる。そこで、暗号資産カストディアンが利用するだけではなく、広く一般に利用される暗号鍵管理全般について、特にその権限分離、状態や操作内容に応じた基本的な考え方と留意点を示す。なお、想定する対象としては、暗号鍵の管理システムおよびその運用設計に関わる要員としているため、必要に応じて他のドキュメントを参照する必要があることに留意すること。

原則として、暗号鍵を用いて管理する情報の重要性に応じて、状態や操作内容に応じたリスク対応策が求められる。リスク対応策としては、権限分離や活性状態の制御などが挙げられる。

鍵管理の基本的な考え方としては、
- 鍵の使用目的
- 鍵のライフサイクル

を事前に規定した上で、それらを前提とした
- 鍵管理のポリシの規定
- 鍵管理システムの設計

が求められる。

鍵管理のポリシとして規定すべき内容としては、責任者や管理者・操作者などの役割や権限の規定など体制面からの検討と、鍵管理システムへの脅威に対するセキュリティ策などサイバーおよび物理的な両面からの検討が必要である。
鍵管理システムで設計すべき内容としては、鍵生成や鍵管理を行う媒体やデバイス、鍵へのアクセス制御機構などである。この設計は前記ポリシを充足するように実施する必要がある。

こうした鍵の使用目的や鍵のライフサイクルにおける暗号鍵に対する脅威（例えば7.2節にある鍵の消失、漏えい・盗難、不正利用など）に対するリスク低減策を策定する必要がある。本項では、特に鍵管理の留意点として以下の4つを挙げる。

- 鍵管理における権限分離
- 鍵の真正性担保
- 活性状態の管理
- 承認操作と証跡の規定

- 鍵運用管理における権限分離

鍵管理においては、外部からの攻撃はもちろん、内部による不正利用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とするためには、適切な権限分離を設計する必要がある。

具体的には、鍵のライフサイクルにおいて、自動化してよいプロセスと意思決定を伴う明確な操作を必要とするプロセスに分けることが重要である。意思決定を伴う明確な操作を必要とするプロセスについて、権限分離の例を表5-3に示す。この例では、プロセスは鍵の生成、保管、活性状

態と非活性状態の切り替え（遷移操作）、署名(Signing)、破棄に分類され、操作はそれぞれの承認、実施、検査[4]といった一連の作業を指す(一般には承認→実施→検査の順序関係を持つ)。

表5-3 意思決定を伴う明確な操作を必要とするプロセスについての権限分離の例

| | | 鍵の生成プロセス | 鍵の保管プロセス | 鍵の活性状態・非活性状態の切り替え（遷移操作） | 署名(Signing)プロセス | 鍵の破棄プロセス |
|---|---|---|---|---|---|---|
| 管理者 | 運用責任者 | 承認 | 承認 | － | － | 承認 |
| | 署名責任者 | － | － | 承認 | （承認）[5] | － |
| 操作員 | 鍵操作員 | 実施 | 実施 | － | － | 実施 |
| | 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5-3のように、意思決定を伴う明確な操作を必要とするプロセスに対して承認、実施、検査の3種類に権限（操作）を分離するとともに、それぞれの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必要がある。鍵操作員・署名操作員は、それぞれに規定された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プロセスを完了させることができない。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、例えば操作員が操作を行うためには施錠された部屋で操作を行うことが必要で、運用責任者のみが解錠できる(あるいは運用責任者の指示によって他の操作員が解錠する)などによって、承認プロセスを物理的な制約と一体的に規定することが推奨される。

- 鍵の真正性担保
  - 鍵の生成・バックアップ

    鍵が複製・漏えいされていないことや、鍵が完全に消去されたことを技術的・運用上確認できるのは、鍵の正当な所有者（あるいは所有者の指示により操作する者）のみである。それ以外の者が生成または所有した場合、その確認は難しくなる。このため、原則として正当な鍵所有者が鍵生成やバックアップを行う、あるいは他者が鍵生成を行う場合も、ICカードのように不正な複製が技術的に困難な鍵管理環境下で鍵生成した上で、鍵所有者に配付すること[6]が求められる。

    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ため、一定の強度を備えた暗号アルゴリズムと鍵長を備えた鍵を生成する必要がある。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。乱数生成機が、十分な乱雑性（探索空間における存在確立の均等性（randomness））[7]がなけれ

[4] ここでは後日に承認と実施の突合を行う証跡確認、いわゆるログ検査を想定しており、オンタイムの立会検査はスコープ外とする。
[5] 一部の限られた署名について承認を行うケースがある。詳細は後述。
[6] なお、ICカードなどの環境下で鍵生成したことを技術的に証明することは難しいため、所有者立ち合いのもとで生成する、あるいは一連のプロセスに外部監査を受けるなどの工夫が求められる。
[7] RFC 4086 “Randomness Requirements for Security”, June 2005

ば、解読に必要な探索空間も限定されること[8]になり、その下で生成された鍵の強度は十分ではない可能性がある。暗号学的に十分な乱雑性を持つ乱数生成器が利用できるのは、(例えばFIPS140-2/-3認証製品など[9])ごく一部の評価や認証を受けた実装環境に限られており、十分な乱雑性を持たない乱数生成器を用いた場合には、暗号学的に十分な鍵の強度を確保できていないことに留意する必要がある。

- 鍵の破棄

いわゆるHSM ( Hardware Security Module ) のような、鍵の管理や保管を行う装置を破棄する場合、管理していた鍵の破棄も合わせて所定の手続きを行うことが求められる。破棄処理が不十分な場合、保管箇所の残存磁気などから過去に管理していた鍵の復元や解読などが可能となり、破棄されたはずの鍵が、当事者の知らないうちに漏えい・盗難されることになる(特に暗号資産においては、その仕組み上検証鍵を無効化し、またそれを検証者に通知することが難しい)。従って、破棄した後に署名鍵が漏えいした場合や盗難された場合にも不正利用の脅威が存在することになる。このため、鍵破棄時には保管箇所からの復元が不可能となるよう、必要な処置[10]を執る必要がある。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締結することが必要と考えられる。

- 活性状態の管理

署名鍵が署名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。署名鍵の不正操作リスクを最小化するためには、活性状態の期間を最小限とすることのみならず、アクセスする人、デバイス、プロセスを含め、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。常に活性状態にあることが業務遂行上最も合理的ではあるが、明らかに不要な時間帯に活性状態としておくことは、不正利用のリスクを高めることになる。逆に、署名操作を必要とする度に活性状態と非活性状態を切り替えることは、操作頻度が高い場合には操作が煩雑となり、承認の形骸化や検査ログの肥大化を招くなど必ずしも合理的とは言えない。

制御の粒度や頻度は、業務の合理性と安全性のバランスによって決める必要があり、また利用者に開示可能な規定等によって、受容可能なレベルまでリスクの低減が確認できることが必要である[11]。

- 承認操作と証跡の規定

前項で権限分離の例を示したが、承認などの要否は業務のリスクに応じて設定する必要がある。例えば、暗号資産交換所においてはリスクの低いすべての取引に対してまで(署名の)承認操作を必要とすると、取引完了までの所要時間が延びるだけでなく、操作が煩雑となるためミスを誘発する遠因となる。

---

[8] 鍵が存在し得る数学的空間(探索空間)において鍵を探索、特定する行為のことを鍵を解読する、という。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、鍵の強度は探索空間の広さに依存することになるが、均等ではない場合、なんらかの手法を用いることで鍵の解読が容易になってしまう。

[9] 7.2.1.5節も参照のこと。

[10] 磁気記憶装置の記憶領域を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や、物理的な破壊等が挙げられる。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(フォレンジック可能なレベルも含めて)処理方法の詳細が異なる点に注意する必要がある。

[11] 例えばPKI認証局などにおいては、同様の規定(CP/CPS:Certificate Policy/Certification Practice Statement)の記述項目はRFC 3647として標準化されており、その標準に沿ってCP/CPSを公開することが求められている。

このため、事業者は、各プロセスに対する承認操作の要否を、ポリシとして規定しておくことが求められる。規定するにあたっては、業務合理性だけでなく操作が及ぼす影響や、承認不要とすることによって生じるリスク、暗号鍵に対する脅威などを考慮する必要がある。

承認の要否はプロセス単位に何らかの判断基準をもって規定することが考えられる。例えば、鍵の真正性を担保するために必要なプロセスである鍵の生成・保管・廃棄や、活性状態を管理する活性状態・非活性状態の切り替えについては一律に承認操作を必要とする、署名プロセスについては一部特定のリスクの高い取引の基準を設け、その基準に抵触した取引のみ承認を必要とする、承認を必要とするリスクの高い取引についても、その承認操作を規定しておくこと等が考えられる。

承認操作の証跡は、適正な権限者によって行われたものであることなどを後日ログ検査者が確認できるよう、適切かつ明確に残す必要がある。これにより、承認をもってリスクを受容したことを明確とする。

## 5.4.3 鍵生成と利用のフロー

### 5.4.3.1 署名鍵と検証鍵のライフサイクル

署名鍵と検証鍵の鍵ペアの管理に関するライフサイクルを図5-2に示す。

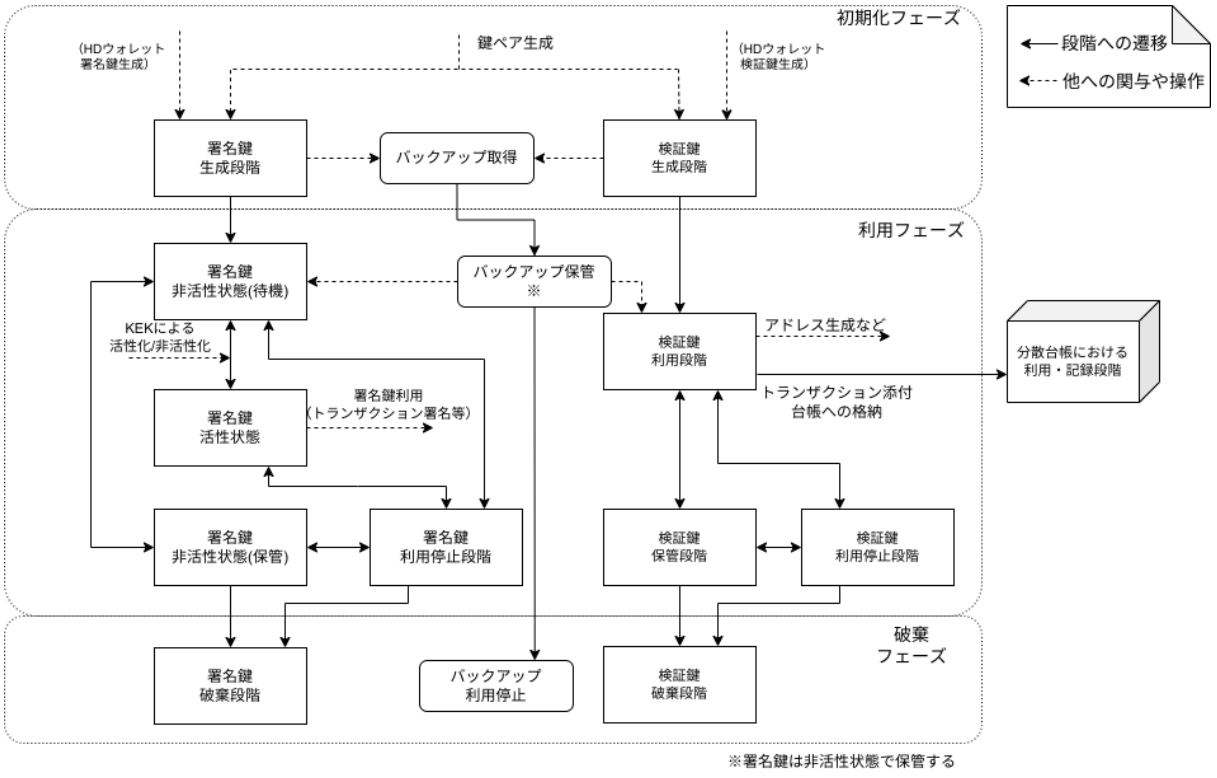


図5-2 署名鍵/検証鍵のライフサイクル

署名鍵や検証鍵の鍵ペアは乱数やマスターシード、あるいは、階層的決定性 ( Hierarchical Deterministic ) ウォレット（以下、HDウォレット）のようなケースではマスターとなる親の鍵ペアから生成される（後述するマスターシードのライフサイクルを参照のこと）。

乱数やマスターシードから鍵ペアが生成される場合には、署名鍵と検証鍵は同時期に生成されるが、HDウォレットのようなケースではペアとなる署名鍵と検証鍵が、それぞれ別のタイミングで生成されることがある。

署名鍵と検証鍵の鍵ペアを作成したのち、検証鍵からトランザクションを受領するためのアドレスを生成できる。暗号資産の移転元が、このアドレスを指定することで、そのアドレスに対して暗号資産を移転できる。アドレスAが保有する暗号資産を別のアドレスBへ移転する場合には、アドレスA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ことになる。

- 署名鍵のライフサイクルについて

  署名鍵が生成された後（「署名鍵生成段階」）、署名鍵データへのアクセス制御を行うために、例えば後述するKEKを用いた暗号化などの保護が行われることが一般的である。この署名鍵が保護された状態を非活性状態と呼び、さらにここでは、「署名鍵非活性状態（待機）」と「署名鍵非活性状態（保管）」と目的に応じて補記している。「署名鍵非活性状態（待機）」は署名鍵を利用するシステムに接続され、次に述べる「署名鍵活性状態」へ移行するために待機している状態である。「署名鍵非活性状態（保管）」については後述する。

  「署名鍵非活性状態（待機）」は、そのままでは署名鍵にアクセスできず、署名鍵を利用することができない状態にある。また、署名鍵を利用するために、KEKにより署名鍵を復号する等により、署名鍵を利用できる状態に戻すことができる。

  「署名鍵活性状態」は署名鍵を利用できる状態であり、トランザクション等への署名付与や、HDウォレットのような場合には、子の鍵ペア等の生成が行われる。署名鍵管理を行うハードウェアの内部で署名鍵が展開され、活性状態となっている署名鍵が他のプロセスから隔離されるケースもあれば、他プロセスも実行されているシステムのメモリ上で展開されるケースもある。後者のケースは署名鍵をソフトウェアで管理している場合に起こりうる。

  署名鍵の利用を終えた後に、再び「署名鍵非活性状態（待機）」へ戻すか、または「署名鍵利用停止段階」へ移行する。「署名鍵利用停止段階」は署名鍵を一時的に利用停止した状態である。署名鍵の利用停止を行う場合には、システム上で署名鍵への接続を閉じることや、実行メモリ上から署名鍵のデータを一旦消去するといった対応が考えられる。「署名鍵利用停止段階」へ移行するパターンとしては、例えば以下のようなものが考えられる。

  - 通常運用上の利用停止

    利用停止を行う場合は、運用上の規定に基づき、署名鍵によるトランザクションに対する署名演算を規定回数行った後に署名鍵の利用を停止する、といった対応が考えられる。利用停止後は、再度署名鍵の利用が必要となるまで、「非活性状態（待機）」や「非活性状態（保管）」に移行する。署名鍵を再度利用しない場合には、「署名鍵破棄段階」に移行する。

- 緊急時の利用停止
  不正アクセスの疑いや障害や災害などの緊急時に署名鍵の利用を停止にするケース。例えば、あるシステムで不正アクセスやマルウェア感染の疑いが生じた際に、そのシステムで利用されている署名鍵への接続を遮断することで利用停止にする。その一方で、不正アクセスされた痕跡や、マルウェア感染の疑いのない別のシステムで署名鍵を活性状態にし、安全なアドレスに暗号資産を退避するためのトランザクション作成を行い送信する、といったことが考えられる。

「署名鍵非活性状態（保管）」は非活性状態となった署名鍵がシステムから分離され、安全な媒体で保管されている状態である。署名鍵を必要とするまでの時間間隔が十分に確保できる場合には、署名鍵を利用するまで「署名鍵非活性状態（保管）」として維持される。保管媒体は適切にアクセス制御された設備や施設などで管理されることとなる。前述したように、署名鍵は生成されたあと、対応する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、署名鍵を生成したのち、検証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の「署名鍵非活性状態（保管）」の状態で安全に管理するという手法もある（8.3.6.2 参照）。

「署名鍵破棄段階」は署名鍵を以降利用することをやめ、署名鍵を復元できないように破棄された状態を指す。多くのブロックチェーンにおいては、署名鍵を破棄した場合に、その署名鍵に対応するアドレスが保有する暗号資産を移転することができなくなるため、署名鍵の破棄には慎重な判断を要する。仮に署名鍵を破棄した後でも、それに対応したアドレスはブロックチェーン上では有効性を維持するため、破棄した意図の有無によらず、そのアドレスへの暗号資産移転を拒むことはできない。署名鍵破棄後にアドレスに移転された暗号資産を無視するかどうか考慮する必要がある（5.4.5参照）。

- 検証鍵のライフサイクルについて

「検証鍵生成段階」で検証鍵が生成された後に、「検証鍵利用段階」に移行する。「検証鍵利用段階」では、検証鍵を用いたアドレスの生成や、署名検証用にトランザクションへの検証鍵の添付などが行われる。トランザクションに添付された検証鍵は「分散台帳における利用・記録段階」で、ネットワークの各ノードによるトランザクションのバリデーションに用いられ、ブロックチェーン・分散台帳に対してトランザクションと共に記録される。「分散台帳における利用・記録段階」は署名鍵・検証鍵の鍵ペアの管理主体のシステムからはコントロールできないブロックチェーン・分散台帳に記録された状態であるため、図5-2においては他の表記と異なる表記としている。

「検証鍵保管段階」では検証鍵は署名鍵やアドレスと共にデータベースで管理されるか、または、署名鍵とともに媒体等で保管される。「検証鍵利用停止段階」は、ここでは、「署名鍵利用停止段階」に連動し副次的に検証鍵の利用を停止するケースを想定している。暗号資産は署名鍵があれば移転可能である。また、検証鍵の利用を停止しても、対応するアドレスに対する暗号資産の移転を拒むことはできない。さらに、トランザクションに添付した検証鍵はブロックチェーン・分散台帳に記録され公開されている。このため、暗号資産カストディアンによる検証鍵単体での利用停止はあまり意味がない。

「検証鍵破棄段階」についても、システム上で「署名鍵破棄段階」と連動して破棄されることを想定している。システム上で検証鍵を削除しても、「分散台帳における利用・記録段

階」でブロックチェーンデータや分散台帳データに記録された検証鍵は記録として永久に残ってしまう。

#### 5.4.3.2 KEKのライフサイクル

署名鍵または署名鍵を含んだウォレットを暗号化するKEKの管理に関するライフサイクルを図5-3に示す。

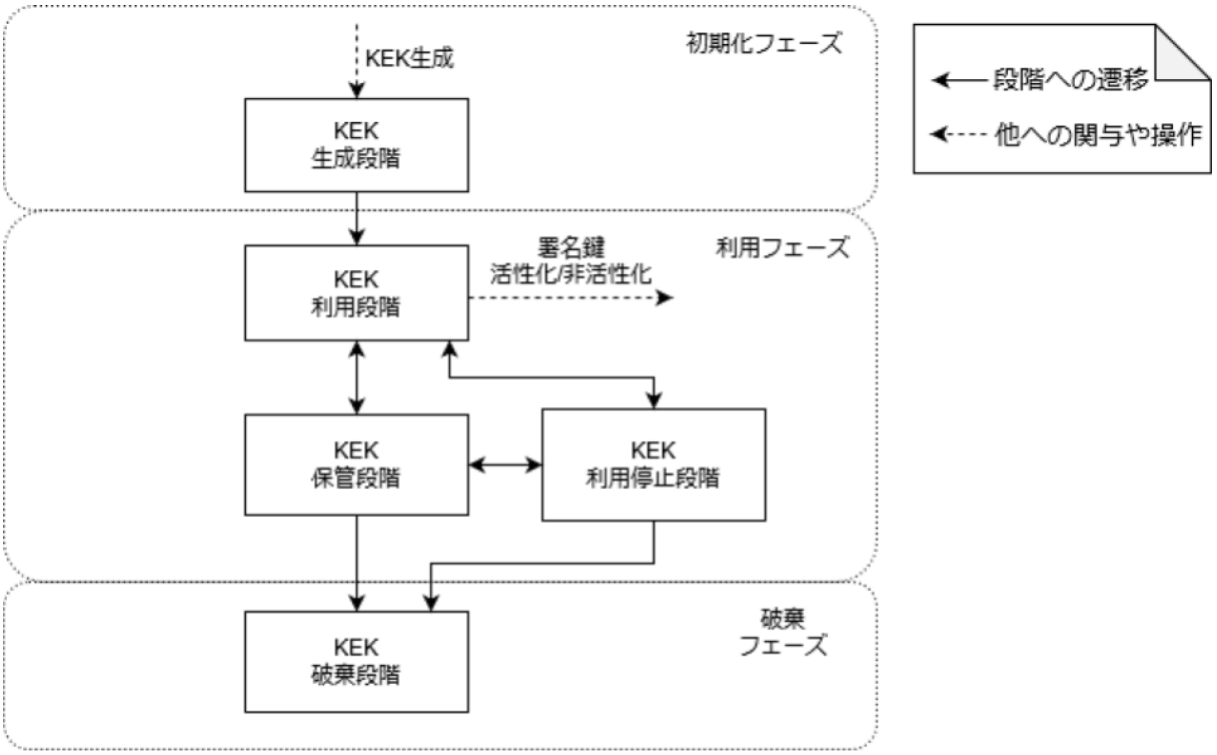


図5-3 *KEK*のライフサイクル

KEKの一例としてはパスワードから生成される共通鍵（共通鍵暗号方式における鍵）がある。

KEKは生成された後（「KEK生成段階」）、署名鍵の暗号化（署名鍵の非活性状態への遷移）および復号（同活性状態への遷移）のために利用される（「KEK利用段階」）。KEKの管理方法にもよるが、KEKを媒体で管理する場合には、利用後にその媒体を適切な設備や施設で安全に保管する必要がある。この保管されている状態が「KEK保管段階」である。KEKも署名鍵のライフサイクルと同様に、運用上の規定や緊急時の対応により「KEK利用停止段階」に移行することが考えられる。

新しいKEKに移行する必要がある場合には、新しいKEKを生成し（新しいKEKが「KEK生成段階」）、古いKEKにより署名鍵を復号したうえで、新しいKEKで再度暗号化することとなる。新しいKEKによる再暗号化が完了すれば、古いKEKは破棄することができる（古いKEKが「KEK破棄段階」）。また、あるKEKに関連する署名鍵を破棄する際に、KEKも破棄することも考えられるが、前述したように署名鍵の破棄については慎重な判断を要する。

#### 5.4.3.3 マスターシードのライフサイクル

非決定性ウォレットのように、署名鍵と検証鍵の鍵ペアが乱数をもとに生成され、各鍵ペア同士が関係を持たない場合もあれば、HDウォレット等の決定性ウォレットのようにマスターシードをも

とに関係を持つ複数の鍵ペアを生成する場合もある。決定性ウォレットでは、マスターシード、または、マスターシードに変換できる可読なニーモニックコードを用いることで、そこから派生した署名鍵と検証鍵を再生成することができる。以降、ニーモニックコードも含めてマスターシードと呼ぶことにする。マスターシードの管理によって、一般的な利用者にとって負担となる「多数の鍵ペアのバックアップといった管理負荷」を軽減することができる。しかし、その反面、マスターシードの盗難や不正利用により、そこから派生した署名鍵が入手され暗号資産が盗難される事態になりえる。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、マスターシードは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。マスターシードの管理上のライフサイクルを図5-4に示す。

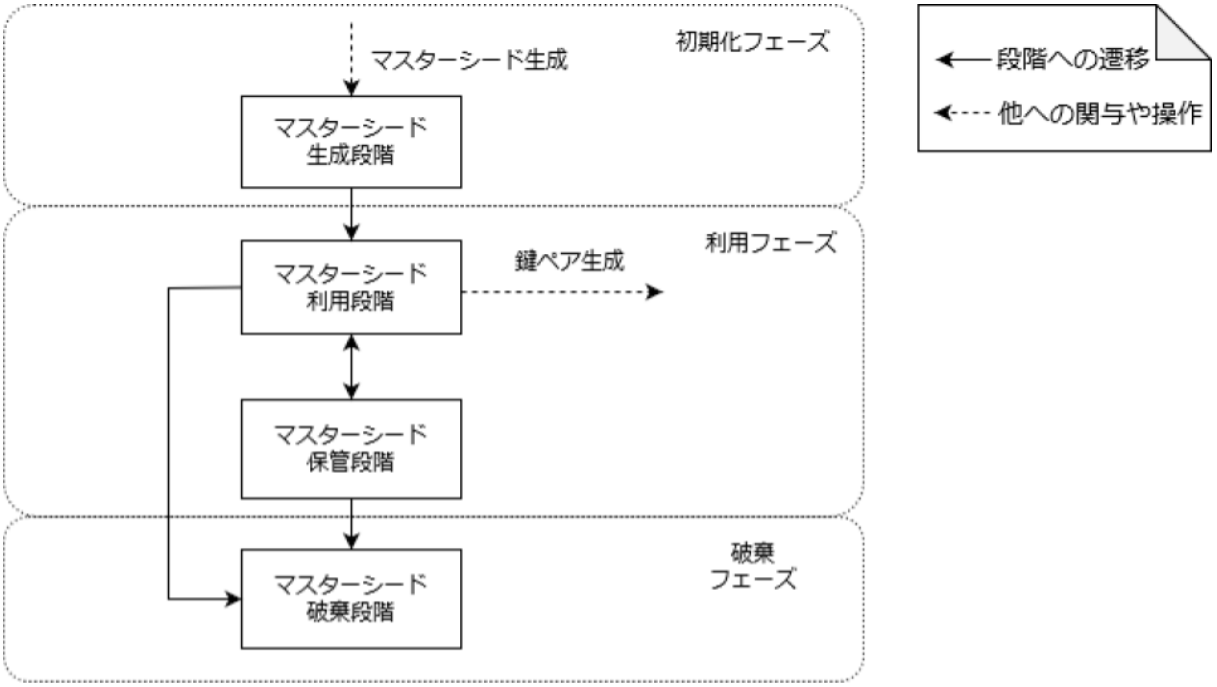


図5-4 マスターシードのライフサイクル

マスターシードは生成された後（マスターシード生成段階）、鍵ペア生成に用いられる（マスターシード使用段階）。マスターシードが使用されなくなった後に、マスターシードは媒体等に格納され、厳格に管理されることとなる（マスターシード保管状態）。マスターシードから派生した署名鍵の利用が終了するなど、マスターシードが不要になった場合には破棄されることとなる（マスターシード破棄段階）。しかし、マスターシードを破棄した場合には、マスターシードを用いて生成した署名鍵が復元できなくなるため、署名鍵のバックアップや署名鍵の消失のリスクなども考慮して、慎重に判断する必要がある。

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。HDウォレットの場合には、マスターシードと共にチェーンコード（chain code）と呼ばれるシードについても注意が必要である。暗号資産の中には、HDウォレットに対応していない（原理的にできない）ものがある。

#### 5.4.4.4 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。

### 5.4.5 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暗号資産カストディアン内での運用であり、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、破棄された署名鍵に対応するアドレスに対して、顧客が誤って入庫してしまうこともあり、誤って入庫されたアドレスから元の顧客に暗号資産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。

# 6. 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

## 6.1 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。7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。

## 6.2 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暗号資産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、暗号資産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暗号資産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暗号資産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。

## 6.3 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速い状況にある。

### 6.3.1 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。

## 6.4 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再収縮（Re-org）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。

### 6.4.1 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。

### 6.4.2 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（フォークコイン）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暗号資産を戻すトランザクションを先んじて送信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からフォークコインが分裂した場合、暗号資産カストディシステム内でフォークコインを暗号資産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。

## 6.5 未承認トランザクションに対するリスク

### 6.5.1 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得る。

### 6.5.2 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、6.4.1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。

### 6.5.3 暗号資産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[12]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。

[12] BIP-0141: Segregated Witness (Consensus layer)
https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

# 7 暗号資産カストディアンのリスク

## 7.1 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（7.2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（7.3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6章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。

## 7.2 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7.2.1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7.2.2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7.2.3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ごと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。

### 7.2.1 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。

#### 7.2.1.1 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7-1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7-1　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<br>● 漏えい・盗難<br>● 不正利用 | ● 誤操作<br>● 正当者の悪意ある行為<br>● 正当者へのなりすまし<br>● 部外者の悪意ある行為<br>● システムの意図しない挙動 | ● カストディ運用系<br>● トランザクション署名系<br>● 顧客資産管理系<br>● 入庫判定部 |

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（操作員・管理者なども含む）による意図せず行われる操作。例えば、本来10万円分を出庫する操作を、誤って100万円分を出庫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（操作員・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[13]。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、操作員・管理者への標的

[13] 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。

型メールなどを介して暗号資産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操作員・管理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、UIがわかりにくく、意図とは異なる挙動をしてしまう、などがある。

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[14]。この結果、想定すべきリスクは表7-2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[15]。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7-2 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） | 顧客(利用者)自身の悪意 | Y | Y | Y | Y |
| | 顧客資産管理系の操作員・管理者の悪意 | Y | Y | Y | Y |
| | 顧客(利用者)へのなりすまし | Y | Y | Y | Y |
| | 内部犯（操作員・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 |
| | 入庫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（バグなど） | トランザクション部の意図しない挙動 | Y | Y | - | - |
| | 入庫判定部の意図しない挙動 | Y | Y | - | - |
| | 顧客資産管理系の意図しない挙動 | Y | Y | - | - |
| | カストディ運用系の意図しない挙動 | Y | Y | - | - |
| 人間系の誤操作 | 顧客(利用者)の誤操作 | Y | Y | - | - |
| | 顧客資産管理系の操作員・管理者の誤操作 | Y | Y | - | - |

[14] 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。
[15] 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。

Y：該当リスクあり、ー：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8.3節で示す。

#### 7.2.1.2 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、操作員・管理者の誤操作による署名鍵の消失が考えられる。

#### 7.2.1.3 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8.3.6節で後述する。

#### 7.2.1.4 署名鍵の不正利用リスク

表7-2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庫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庫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てしまう。
- 操作員・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（7.2.2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、8章で示すように暗号資産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。

#### 7.2.1.5 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
  署名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証としてFIPS140-2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証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証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。

### 7.2.2 資産データに関するリスク

資産データは顧客や暗号資産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、資産データは暗号資産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。実際の暗号資産カストディ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、操作員・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、入庫判定部がアタック・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（7.2.1.4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、暗号資産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暗号資産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、ある顧客や暗号資産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。

### 7.2.3 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システムは、ソフトウェア、ハードウェア、ネットワーク等から構成される。また暗号資産カストディ業務には、暗号資産カストディシステムの運用監視、ウォレットの入出庫、業種や事業者によっては口座開設、送金指示など、人手を介して行われるオペレーションがある。このため、様々な要因によってシステムや業務が停止し得る。
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。しかしながら暗号資産カストディシステム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システム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アンのみならず、特に暗号資産交換所の稼働状況は暗号資産の価格に与える影響が大きいことから、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。

#### 7.2.3.1 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。

#### 7.2.3.2 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。

#### 7.2.3.3 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。

#### 7.2.3.4 法的要因による業務停止リスク

暗号資産カストディアンが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。なお、業務の停止を求められる原因は、免許条件や登録条件に違反する場合などが考えられるが、適用される法域

によって異なるため、予期せぬ業務停止命令や業務改善命令が発せられる[16]リスクが考えられる。

## 7.3 外的要因によるリスク

暗号資産カストディ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。

### 7.3.1 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

#### 7.3.1.1 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アンへの到達性を妨げ、また偽の暗号資産カストディアンに誘導したり、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。

#### 7.3.1.2 Web PKIに対する攻撃

多くの暗号資産カストディアンは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。

#### 7.3.1.3 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。

#### 7.3.1.4 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。

[16] 暗号資産の取扱いに関する違反に限らず、例えば個人情報の漏えいが確認された場合や、現地の労働法規に違反した場合など、業務を停止する命令が出る理由は法域によって異なる。

## 7.3.2 暗号資産のブロックチェーンに起因するリスク

### 7.3.2.1 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。

### 7.3.2.2 51% 攻撃やselfish miningによるブロックチェーンの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。

### 7.3.2.3 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。

### 7.3.2.4 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移転の有無を偽装することによって、入庫を装って対価を詐取する攻撃がある。例えば2014年のMt.GOX事件においては、便乗でトランザクション展性を悪用した攻撃が発生したとされる。また、2018年のモナコインにおいてもトランザクション展性を利用した攻撃が発生した。

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[17] 。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、暗号資産の価値が崩壊する事例がある。Ethereum上で発行されていた暗号資産である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 )。

### 7.3.2.5 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。

[17] Check INT_32 range for transaction timestamps, https://github.com/LiskHQ/lisk/issues/2088

### 7.3.3 外部のレピュテーションに起因するリスク

#### 7.3.3.1 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。口座が凍結された場合には、事業者の事業が継続できなくなる可能性、さらに暗号資産交換所の口座が凍結された場合は、利用者との法定通貨の入出金の業務が停止する可能性がある。

#### 7.3.3.2 暗号資産アドレス

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暗号資産を移転する場合に、移転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暗号資産を移転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。

#### 7.3.3.3 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アンの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。

#### 7.3.3.4 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。

#### 7.3.3.5 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。

### 7.3.4 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や、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暗号資産の詐取、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。

# 8 暗号資産カストディアンにおけるセキュリティ管理策の留意点について

## 8.1 本節について

本節では7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アンにおける特有の考慮点について記載している。特に、暗号資産の署名鍵の管理は、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。

## 8.2 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。暗号資産カストディアンにおいても、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アンにおいては、顧客資産や自己資産に関する資産データ、顧客情報、さらに暗号資産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アン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アン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（例えば暗号資産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。暗号資産カストディアン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暗号資産カストディアン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）
  暗号資産カストディアン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）
  暗号資産カストディアン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7章で述べたような暗号資産カストディアンが抱えるセキュリティリスクを継続的に把握する必要がある。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。

## 8.3 暗号資産カストディシステムのセキュリティ管理策に関する留意点

暗号資産カストディアン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暗号資産の署名鍵の消失、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7.2節で述べた暗号資産カストディ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、暗号資産カストディ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8.3.1節から8.3.14節ではJIS Q 27002:2014の項目を踏襲し、暗号資産カストディシステムで特に留意すべき事項について記述する。

### 8.3.1 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、暗号資産カストディアン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、8.3.5の暗号資産カストディシステムのアクセス制御に関する方針、8.3.6の署名鍵など鍵管理策に関する方針、8.3.8の運用のセキュリティに関する方針、8.3.9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。

### 8.3.2 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、暗号資産の取り扱いにおいては7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」)。

### 8.3.3 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、暗号資産カストディアン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暗号資産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。

### 8.3.4 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。

特に暗号資産カストディアンにおいては、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。
暗号資産カストディアン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8.3.11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、顧客の資産と暗号資産カストディアンの資産を分別して管理することが必要である。

### 8.3.5 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、暗号資産カストディシステムへアクセスする者として、操作員や管理者といった暗号資産カストディ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、暗号資産カストディアンのサービスを利用する顧客に大別できる。8.3.5.1節では特に暗号資産カストディアンの操作員や管理者を対象としたアクセス制御の考え方を示し、8.3.5.2節では暗号資産カストディアン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。

#### 8.3.5.1 暗号資産カストディアン内の操作員や管理者のアクセス制御

暗号資産カストディアンの操作員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。

- カストディ運用系を操作する操作員や管理者。例えば、カストディ運用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/非活性状態の遷移操作、バックアップやリストアなど)、署名鍵の管理については8.3.6も参照のこと。

上記のような操作員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、カストディ運用系に接続するリモート端末の認証と認

可、暗号資産カストディアン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、カストディ運用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、暗号資産カストディ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、操作員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、操作員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。

7.2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、複数人の操作員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、単一の操作員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。

#### 8.3.5.2 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、多くの暗号資産カストディアン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お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
  暗号資産カストディアンの顧客になりすますことによって、預入金や預入暗号資産を詐取したり、暗号資産の現金化、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単要素認証を認めてもよいが、暗号資産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。
  さらに暗号資産の移転、または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、数量・金額や移転先・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、人手による取引意思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
  暗号資産カストディアン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
  暗号資産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移転でき、技術的にそれを妨げることができない一般的な暗号資産を前提とした場合に、過去に暗号資産カストディアンが利用したことのある暗号資産アドレスに対して移転が行われる可能性を想定して、適切に管理された暗号資産アドレスに再移転できるように、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-grade API[18]に準拠することが考えられる。

### 8.3.6 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。

特に暗号資産カストディアン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。

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

#### 8.3.6.1 署名鍵管理の基本

暗号資産に限らず、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、暗号資産カストディシステムとして考慮すべき主な管理策については、8.3.6.2項以降で述べていくことにする。

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、署名鍵は活性状態にある必要がある。非活性状態の署名鍵を活性状態に遷移するには、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状態/非活性状態の遷移操作を行うことは、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、上記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庫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。

### 8.3.6.2 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。

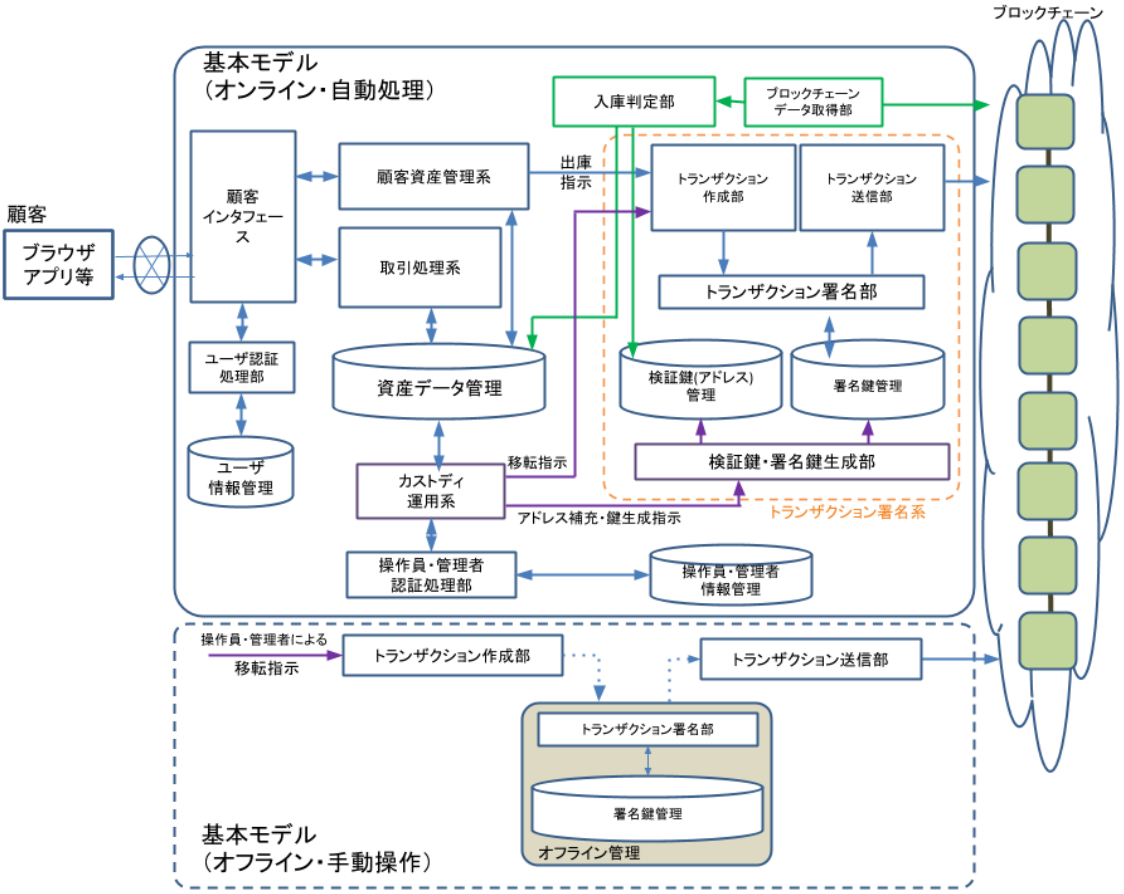


図8-1 署名鍵のオフライン管理のイメージ

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。

### 8.3.6.3 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8.3.6.1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[19] [20]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おり、プロトコル上に実装されているものや、イーサリアムのように、プロコトルでは対応していないが、スマートコントラクト上で複数の方式から選択してマルチシグを実現することが可能なものもある。また、そもそもマルチシグやスマートコントラクトによる実現をサポートしていない場合もあり得るため、暗号資産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。

また、権限分散に応用可能なマルチシグに類似の技術として秘密分散がある。秘密分散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。分散情報は単独では利用できず、分散情報を集約することで分割前の署名鍵を復元できる。複数の承認権限者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を防ぐ対策のひとつだが、署名鍵の生成・分割を行う者と、署名鍵の復元を行う者は単独で署名を行える立場となる。承認すべき内容（署名対象）を各承認権限者が確認することは実質的に難しく、また分散情報の管理は実装に依存することから、どちらかというと複数組織より単一組織における鍵の分散保管のための技術である点に留意されたい。

### 8.3.6.4 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。

バックアップに関する一連の考慮事項としては、以下のようなものがある。

1. 鍵のバックアップを生成する要件を検討すること
2. バックアップの生成後においては適正な保管や、定期的な点検（検証）を行うこと
3. バックアップを利用しなくなった場合には、鍵と同様に利用停止とすること
4. 上記のすべてにおいて、適切な手続きおよび運用を事前に設計すること

なお、暗号資産を保管・管理する場合には、バックアップされた署名鍵やマスターシードは、取引履歴など他の一般的なバックアップデータとは異なる厳格性をもって保管され、通常時には（システムが利用できない場合も含めた）適切な運用や事務手続きをもって、その存在を確認され、点検されるべきものと考えられる。

---

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

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

#### 8.3.6.4.1 鍵のバックアップを生成する要件の検討

##### 要件定義における論点

###### 鍵の分散の考え方

一般的に、不慮の操作や災害によるデータの逸失を防ぐためにバックアップを生成することが有効である。

そして、暗号資産を安全に保管するためには、鍵の分散管理（マルチパーティー計算や、秘密分散、マルチシグなどが含まれる）を行うことが、システム的な単一点の故障や漏えいを防ぐ観点から必要であると考えられる。しかし、バックアップを生成することで（生成した）データの逸失を防ぐことができる半面、バックアップデータが漏えいする新しいリスクが生じることになる。そのため、バックアップの生成から利用停止を行うまでのリスクについて十分に検討した上で設計することが必要である。

鍵の分散管理の方法には、1セットのマスターシードから署名鍵を複数生成する方法、複数のマスターシードからそれぞれの署名鍵を生成しマルチシグ等で分散する方法等がある。これらのいずれの場合においても、バックアップを生成したことで生じるリスク、保管するコスト、運用上の制約等を整理し、比較検討する必要がある。

現時点では、どの方法にも一長一短がある。最終的にはカストディアンがそれぞれに判断するべきものと考えられるが、いずれにしても、上記観点に基づいた十分なリスク分析が行われることを前提とすべきと考えられる。

###### バックアップからの復旧をしてはならない場合

上述のとおり、暗号資産にひもづく鍵のバックアップを行う主たる目的は逸失リスクの低減である。そのため、鍵の漏えい等のリスクが顕在化した場合には、生成したバックアップを利用することはできない。

例えば、既存の鍵が危たい化した場合には新しい鍵を生成する必要があり、新しく作成した鍵についても、バックアップを生成する必要がある[21]。なお、この場合、8.3.6.4.3に記載の通り、危たい化した鍵のバックアップは廃棄しないため、単純にバックアップ対象の数が増えることになる。

逆に、鍵をうっかり削除（消去）してしまった場合で、漏えいしていないことが保証できる場合などは、バックアップを利用して復旧することが可能である。。

いずれの場合であっても、鍵の生成時点では（いつバックアップが必要になるかわからないため）バックアップの生成が必要となるが、その復旧にあたっては、原因を確認する必要があり、原因によってはバックアップからの復旧をしてはならない場合があることに注意が必要である。

#### 8.3.6.4.2 バックアップの生成後は適正に保管し、定期的な点検（検証）を行うこと

##### 設計上の問題

署名鍵やマスターシードの生成や通常の運用にあたっては、その後の運用面を含めたリスク分析を行い、リスクに応じた実装やリスク対応策が検討されるのに対して、バックアップの作成や保管にあたってのリスク分析、およびリスク低減策については、その利用頻度の低さや、必要となるコストから、十分な検討が行われていない可能性がある。

バックアップの作成や保管にあたり、以下のような観点からの検討が必要と考えられる。

[21] アドレスを無効化できない暗号資産の場合、危たい化した鍵は廃棄することなく、利用停止に留めるよう、5.4.5に記載している。このため、バックアップも同様に利用停止に留める必要がある。

- バックアップの数量や個数の観点
    - バックアップ対象がどれくらいあるのか、バックアップをいくつ作成するのか、といった署名鍵やマスターシードの個数・量を見積もる必要がある。
- バックアップ媒体の観点
    - 生成する媒体を何にするのか、という観点のほかに、長期間の保管に耐えられない場合にはデータの移転を検討する必要がある。
- バックアップの保管主体の観点
    - バックアップの保管は誰が行うのか（自社のどの部門とするか、他社に委託するのか）、保管する主体を明確にする必要がある。また、委託する場合には委託条件を明確にする必要がある。
- バックアップの保管場所の観点
    - バックアップを論理的・物理的にどこに保管するのか、という観点の他に、物理的に保管する場合、復旧時や点検時には保管場所に出向く必要がある。
- バックアップの分散保管の観点
    - バックアップをどのように分散するのか、より具体的には、どの拠点にどのバックアップ（分散された場合のデータ片を含む）を保管するのか、1か所で鍵の復元が可能とならないよう、分散するバックアップの組み合わせを検討する必要がある。
- バックアップが利用可能であることの検証頻度
    - ISO27001:2013（JIS Q 27001:2014）のA12.3.1を採用している場合、バックアップデータは定期的に取得[22]され、かつ定期的に検査される必要がある。
- バックアップを所定の手続きにより速やかに利用可能とするための運用上の制約
    - 承認のための事務手続きや保管場所（地理的、または設備的なものを指す）へのアクセスについても、作業の承認にあたって権限が分離されており（権限分離）、かつ、複数名により実施する作業（相互けん制）のみとする必要がある。
- バックアップの保管場所、またはバックアップデータにアクセスされた場合の検知方法
    - 予期せぬアクセスに対する検知策が必要である。

### 管理・運用上の問題

一般的に、暗号資産カストディアンにおいては、署名鍵やマスターシードについては、最上級の機密情報として取り扱うことが求められ、その管理・運用についても十分なリスク分析を行った上で、残存リスクを最小化し、さらにその残存リスクに対する低減措置を実施する必要がある。

その一方で、署名鍵やマスターシードのバックアップについては、適切な媒体・保管場所[23]で確実に保管し、必要と判断された場合には（必要な手続きを経て）速やかに利用可能な状態にできることが必要である。また、保管場所に予期せずアクセスされた場合や、保管されているバックアップ（の一部）が予期せず利用された場合は速やかに検出することも必要である。

[22] 本ドキュメントではバックアップの「生成」としているが、JISの記載では「取得」となっているため、そのまま表記する。

[23] バックアップを1箇所に保管するのではなく、論理的、物理的に分散保管しておくことも考えられる。他方で、その場合には保管のためのコストや、検証時・利用開始時等における負担が生じるため、バックアップの保管場所には十分な検討が必要である。

#### 8.3.6.4.3 バックアップを利用しなくなった場合には、鍵と同様に利用停止とすること

管理・運用上の問題

本ドキュメントにおいては、鍵のライフサイクルにおいて、鍵を利用しなくなった場合でも、廃棄は行わず、利用停止とすることを求めている[24]。このため、バックアップにおいても同様に、廃棄することなく、鍵の利用停止と同時期に、バックアップも利用停止とする必要がある。つまり、利用を停止したことをもって、管理のレベルを変更してはならない。

なお、利用停止となった鍵のバックアップについては、最低限を残して廃棄することも考えられるが、最低限のバックアップの範囲については、利用停止が終了することがないことから、十分な検討が必要である。

#### 8.3.6.4.4 上記のすべてにおいて、適切な手続きおよび運用を事前に設計すること

管理・運用上の問題

一般的に、どのような事態でバックアップからの復元を行うのか、という判断はバックアップされたデータの汎用性と関連し、その際に必要となる手続きはバックアップデータの機密性と関連する。また、システムがすぐに利用できない場合における復旧を検討する場合には、コンピュータシステムに依存しない、手動運用も検討する必要がある。

しかし、特に暗号資産を保管・管理する場合には、バックアップされた署名鍵やマスターシードは、取引履歴など他の一般的なバックアップデータとは異なる厳格性をもって保管され、通常時には（システムが利用できない場合も含めた）適切な運用や事務手続きをもって、その存在を確認され、点検されるべきものと考えられる。

同様に、署名鍵やマスターシードのバックアップを利用する事態とは暗号資産を安全に保管することが保証できなくなった事態であり、一般的なバックアップデータを復元する場合とは異なり、より厳格かつ迅速に作業を行う必要がある[25]。

従って、上記の論点のすべてにおいて、作業の承認にあたって権限が分離されており（権限分離）、かつ、複数名により実施する作業（相互けん制）のみを認めることを運用設計として織り込む必要がある。

また、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[26]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。

---

[24] 鍵（アドレス）の失効という概念が存在しない暗号資産の場合、利用停止となったアドレスに対する入庫を防ぐことはできないため、入庫を検知した場合には速やかに安全なアドレスへ移転することを求めている。

[25] 8.3.6.4.1 に記載の通り、鍵が危たい化した場合など、バックアップを利用してはならない場合があることにも注意が必要である。

[26] 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。

- 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[27]。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。

#### 8.3.6.5 ハードウェアウォレット等の調達

暗号資産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、現状では暗号資産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、8.3.4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。

[27] 例えばISO/IEC 19592-2:2017など

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。

### 8.3.7 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。
暗号資産カストディ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5-1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5-1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KEK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（8.3.6参照）。

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。

### 8.3.8 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。特に暗号資産カストディシステムで言及しておくべき事項を以下に述べる。

#### 8.3.8.1 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暗号資産カストディ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、暗号資産カストディ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。

#### 8.3.8.2 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員や管理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。

#### 8.3.8.3 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。

- 暗号資産カストディ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。
- 暗号資産カストディ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暗号資産カストディ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暗号資産カストディ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（失敗も含む）、活性状態の署名鍵へのアクセス記録[28]、バックアップ・リストアなどについて、日時、操作元端末、操作員（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、操作員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
  暗号資産カストディ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、操作員の認証・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）、操作員情報（操作員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、操作員情報、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暗号資産カストディシステムに対する通信は、8.3.9.1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暗号資産カストディアン固有の対策ではなく情報セキュリティ上有効である。
  暗号資産カストディ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

[28] 署名作成の場合は署名対象のハッシュ値などを含めることが考えられる。

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暗号資産カストディ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。

### 8.3.9 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。
特に暗号資産カストディアンにおいては、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。

#### 8.3.9.1 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、停止した場合に暗号資産カストディ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（8.3.8節に関連）。
暗号資産カストディアン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。

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

暗号資産カストディ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。

- 暗号資産カストディ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、暗号資産カストディ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暗号資産カストディ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、あるいは暗号資産カストディアン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。
- カストディ運用系で用いる端末の制限
    - 対策の目的:カストディ運用系で用いる端末の乗っ取りによる不正操作を防ぐ。
    - 対策:カストディ運用系を操作する端末やカストディ運用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、暗号資産カストディシステムに接続できる端末を制限する。

### 8.3.10 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。

暗号資産カストディアンで取り扱われる暗号資産は複数の事業者により取り扱われる流通量が高い暗号資産から、新興な暗号資産まで多岐に渡る。これら暗号資産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
    - 暗号資産カストディ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
    - テスト環境だけでなく、本番環境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。

### 8.3.11 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、暗号資産カストディ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。

### 8.3.12 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、特に暗号資産カストディアン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。

### 8.3.13 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

#### 8.3.13.2 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。

### 8.3.14 順守

各国の法令やガイドライン等を遵守すること。

## 8.4 その他の暗号資産カストディシステム固有の留意点

#### 8.4.1 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。

#### 8.4.2 情報漏えいにより利用者に与えるリスク

暗号資産カストディアンから、利用者の出庫先ウォレットアドレスや、個人を特定できる情報の一部が漏えいした場合、利用者が自己で管理するウォレットアドレスやその残高、および利用者の住所等が特定可能[29]となりうるため、利用者および利用者ウォレットに対する犯罪が発生する可能性がある。このため、漏えいが発生した場合は利用者に対してその旨を速やかに周知するとともに、発生し得るリスクについても併せて伝えることが望ましい。

[29] 漏えいした情報だけでは特定不可能な場合であっても、他の事業者から漏えいした情報を組み合わせることで特定可能となる場合もありうるため、一部の情報が漏えいした場合であってもリスクは存在する。

# Cryptoassets Governance Task Force

## 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）

## Security Working Group

初版メンバー

- 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（ココン株式会社）
  - 樋田 桂一（一般社団法人 日本ブロックチェーン協会）

第2版メンバー

- チェア
  - 楠 正憲（Japan Digital Design株式会社）
- エディタ
  - 栗田 青陽（株式会社メルカリ）
  - 菅原 謙一（株式会社Neukind）
- メンバー（五十音順）
  - 川畑 雄補（株式会社アプルーシッド）
  - 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）
  - 須賀 祐治（株式会社インターネットイニシアティブ）
  - 中島 博敬（株式会社メルカリ）
  - 花村 直親（株式会社ExaProof）
  - 林 達也（株式会社イエラエセキュリティ/株式会社パロンゴ）
  - 森下 真敬（株式会社Ginco）

第3版メンバー

- チェア
  - 楠 正憲（デジタル庁）
- エディタ
  - 栗田 青陽（株式会社メルコイン/株式会社メルカリ）
  - 菅原 謙一（株式会社デジタルアセットマーケッツ）
- メンバー（五十音順）
  - 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）
  - 須賀 祐治（株式会社インターネットイニシアティブ）
  - 林 達也（株式会社パロンゴ/LocationMind株式会社）
  - 藤本 賢慈（株式会社Ginco）
  - 森下 真敬（株式会社Ginco）