The Digital Currency Forum
Wallet Security Subcommittee

セキュリティ検討報告書

ブロックチェーン接続パターンに応じた脅威と緩和策の検討

2024年
デジタル通貨フォーラムウォレットセキュリティ分科会

INDEX

第1章

本書について

01

CONTENTS

1.1　ウォレットセキュリティ分科会の目的と本書の位置づけ

ウォレットセキュリティ分科会では、DCJPYネットワーク、特にビジネスゾーンに参画する多種多様な企業が行うセキュリティ対策検討を支援するため、DCJPYネットワークを活用したシステムに対するセキュリティ要件の基本事項を整理することを目的に活動してきた。

本書は2020年12月～2024年3月までの活動の成果として執筆した「セキュリティ検討報告書【鍵管理編】」と「セキュリティ検討報告書【分散台帳編】」を再編したものである。本書の内容はDCJPYネットワークを構成する分散台帳の特徴を理解するために役立つとともに、今後より詳細なセキュリティ要件を検討するための道標となるものである。なお、検討対象のDCJPYネットワークはPoCのために設計・実装された仕様に基づいている。

1.2 背景

DCJPYネットワークは民間銀行をはじめとした金融業界のみならず、多種多様な企業や組織などが参加し、連携することにより維持されるプラットフォームである。複数の企業や組織が連携しながらプラットフォームを維持するためには、それぞれの企業や組織が管理するシステムに対する安全性について一定の基準を保ち、プラットフォーム全体としての安全性を高めていくことが不可欠である。

現在は様々な分野において分散台帳を用いたシステムの構築が検討されており、デジタル通貨フォーラムの各分科会においても「DCJPYネットワーク外で管理される分散台帳システム」と「DCJPYネットワーク」との連携を行うユースケースの検討や実証実験の実施が行われている。

DCJPYネットワークに参画する組織の中には、これまでも法規制や業界のガイドラインに基づき、高度なセキュリティ基準への準拠が要求されている事業もあれば、これから新規にデジタル通貨のビジネスに参入するため新たにシステム構築を検討する事業者もあり、安全対策に対する考え方の差異は様々であるが、どの事業者においてもDCJPYネットワーク固有の特性を理解したうえで安全対策を検討することが必要であり、DCJPYのビジネスゾーンの利用企業にはその対策が求められてくる。

分散台帳システムは業界や複数の主体によって管理される分散型・分権型の構造を持ち、業界や国境をも超えて運用されているものもある。分散台帳に関わる管理者やサービス提供者、ソフトウェア開発者、開発環境の提供者といった多数の関係者が関与することによって、多種多様なサービスやソフトウェアが次々に登場し、分散台帳のエコシステムが拡充されていくという期待がある反面、分散・分権型といった分散台帳技術の構造は従来の中央管理型のシステムとは性質が異なり、分散台帳技術を採用するシステムはその特性を考慮に入れ構築を行うことが必要となる。

特にセキュリティの観点では、分散台帳システムへ接続する特定のシステムの問題が分散台帳システムへ影響を及ぼす可能性や、分散台帳システムで発生した問題が別のシステムへ影響を与える可能性を想定することも必要となる。しかし、分散台帳技術は様々な機能や技術要素が含まれており、さらに、それらが複雑に関係しているため、セキュリティ上の脅威の要因も様々で理解しにくい。分散台帳技術に関わる要素を分析し、それらの要素に潜在する脅威とその脅威によるリスクの緩和策を考察することが必要となる。

そこで、外部事業者の分散台帳システムと接続するシステムを構築・運用するという観点に立ち、ビジネスゾーンのシステムにおけるセキュリティ課題と緩和策の検討を行うこととした。

1.3 想定読者

本ドキュメントの想定読者は以下の通りである。

1. DCJPYネットワークと外部事業者の分散台帳システムを接続する際のセキュリティ課題について理解を深めたいデジタル通貨フォーラム参加者
2. DCJPYネットワークを利用したビジネスゾーンのシステム構築を検討しているシステム開発担当者(特に分散台帳エンジニア)、セキュリティ担当者
3. DCJPYネットワークに接続する外部事業者の分散台帳システムの今後のセキュリティ指針等の検討を行う策定者

1.4 前提条件

ここでは、本書を読み進めていくにあたり前提となる条件をまとめる。

1.4.1 DCJPYネットワークについて

1.4.1.1 階層構造

DCJPYネットワークは、デジタル通貨（DCJPY）を発行・送金・償却を行うために、「フィナンシャルゾーン」と「ビジネスゾーン」の2つの領域を設け、両領域を連携させる仕組みを想定している（図1-1）。

フィナンシャルゾーンは、デジタル通貨の残高を記録する元帳を管理し、デジタル通貨発行のために各銀行のシステムと連携する仕組みを提供するなど、DCJPYネットワークで共通の機能を提供する。

一方、ビジネスゾーンは、各ユースケースに応じて構築されるものであり、ユースケースの要求に応じて開発されるプログラムが設定可能な領域となっており、各ビジネスゾーン間で独立性を有した領域となりえる。DCJPYネットワークの全体の構成や機能、特徴については2023年10月発行のホワイトペーパーを参照されたい。

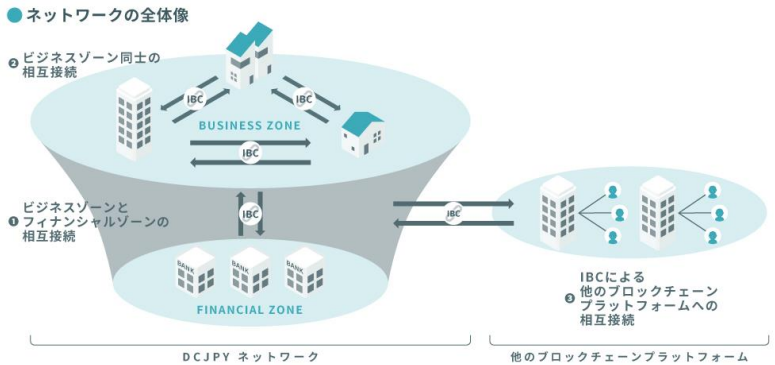


図1.1 DCJPYネットワークの全体像

●出典　デジタル通貨DCJPYの世界観を伝えるホワイトペーパー　（株式会社ディーカレットDCP発行）　https://amicsign.com/index.html

1.4.1.2 ネットワークシステム

DCJPYネットワークに用いられる分散台帳には現段階では『Hyperledger Besu』※が想定されており、ビットコインやイーサリアムといった、いわゆるパブリックブロックチェーン（パーミッションレス型ブロックチェーン）とは異なり、参加するノードが限定されたコンソーシアム型のブロックチェーンとなる。

また、インターネットを前提としたパブリックなオープンネットワークではなく、クローズドなプライベートネットワークが構築される。そのためパブリックブロックチェーンとは異なるセキュリティ要件が要求されることが想定される。

1.4.1.3 構成要素

DCJPYネットワークはコアパッケージと呼ばれるソフトウェア群と、それらを利用するためのデジタル署名用の署名鍵によって構成されている。コアパッケージはDCJPYネットワークに参画するそれぞれの企業や組織の環境下で実行され、それらの機能が協調動作することでDCJPYネットワークに関わる全般の機能が実現される。

DCJPYネットワークは分散化された構造を持っているため、一部の障害がただちにプラットフォーム全体の機能停止につながる可能性は低い。しかし、個々の企業や組織にセキュリティ上の問題が発生した場合には、その企業や組織の管理下にある情報資産や利用者に被害が及ぶことや、場合によってはDCJPYネットワーク全体に対する信頼を低下させることに繋がりかねない。安全・安心なデジタル通貨プラットフォームを実現するためには、それぞれの企業や組織が適切にプラットフォームのソフトウェア群や各種署名鍵を適切に管理することが求められる。

※2024年9月 LF Decentralized Trust 発足に伴い、Hyperledger Besu からBesuに名称変更

1.5 スコープ

本書は、外部事業者の分散台帳システムに接続して利用するビジネスゾーンのシステムのセキュリティ課題を抽出し、それらのリスク緩和策を検討する。
外部事業者の分散台帳システムとビジネスゾーンのシステムの関係と本書の考察の範囲を図1.2に示す。

- ビジネスゾーンのサービス提供事業者はDCJPYネットワークと接続してDCJPYの送金等を行う。
- DCJPYネットワークと連携したビジネスゾーンのアプリを図1.2において「DCJPYビジネスアプリ」とし、また、DCJPYネットワークと接続した処理系を「ビジネスゾーン接続システム」としている。
- DCJPYネットワークのフィナンシャルゾーンではDCJPYの発行・管理・償却に関わる処理を行う。
- ビジネスゾーン接続システム、フィナンシャルゾーン接続システム、DCJPYネットワークはDCJPYの処理を行うためのプライベートパーミッションド型の分散台帳システム（ブロックチェーン）を内包しているが、それらは本報告書の考察の対象外とする。

本書では、ビジネスゾーンのシステムはDCJPYの処理系とは別に、別の外部事業者による分散台帳システムと接続することを想定している。このような形態は、DCJPYの管理とは独立したデジタル資産の管理を外部の分散台帳システムで行う場合や、DCJPYの導入以前から既に稼働している分散台帳システムとの連携を行う場合などが考えられる。また、ビジネスゾーンのサービスを提供する事業者が、そのような分散台帳システムの管理者（の一部）である場合も考えられる。

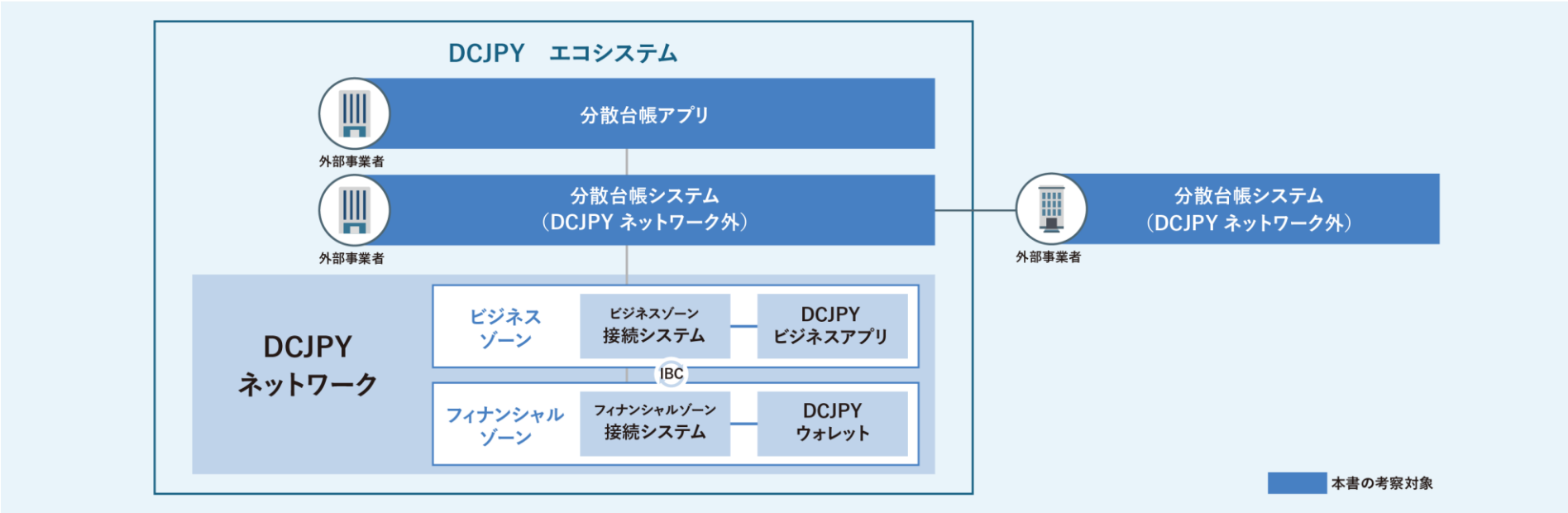


図1.2 本書が扱うシステムの対象

1.5 スコープ

本書では、ビジネスゾーンにおいて両者を連携したサービスやシステムを構築した場合に外部事業者の分散台帳システムがもたらすセキュリティ上の影響について考察する。セキュリティ課題は以下を含む。ただし、網羅性を保証するものではない。

- 分散台帳プラットフォームに潜在する可能性のある一般的なセキュリティ課題
- 分散台帳システムに潜在する可能性のある一般的なセキュリティ課題
- 分散台帳ノードを管理する場合の一般的なセキュリティ課題
- スマートコントラクトに関わる一般的なセキュリティ課題
- ビジネスゾーンのシステムの構築や運用に関わる課題

以下はスコープ外とする。

- ビジネスゾーンにおける事業者やビジネスゾーンのシステムの法的適合性
- デジタル資産に関する経済的リスク
- DCJPYネットワークの利用における安全策
- ビジネスゾーンのシステムの一般的なセキュリティ対策の詳細
- ビジネスゾーンのシステムの機能やプロトコル、プロセス等の具体的な設計

1.6 用語集

本書を読み進めるにあたり、把握しておくべき用語を一覧表にまとめた。

■ 用語集一覧

用語	意味
IBC	ブロックチェーン同士でデータや価値をやり取りする仕組みの一つ。
DCJPY	銀行発行デジタル通貨の一つ。
DCJPYウォレット	各銀行の管理するBPMシステムに接続し、ユーザー（口座所有者）が操作する個人向け画面（フィナンシャルゾーンアプリ）。
DCJPYビジネスアプリ	ビジネスゾーンをユーザーが操作するアプリケーション（事業者アプリ）。
DCJPYビジネスウォレット	各銀行の管理するBPMシステムに接続し、ユーザー（口座所有者）が操作する法人向け画面。
DCJPYネットワーク	DCJPYによる金流を担うフィナンシャルゾーン、商流を担うビジネスゾーンの２つのブロックチェーンをインターオペラビリティで連携するシステム。
ビジネスゾーン	DCJPYプラットフォームにおいて商流を担うブロックチェーン。
フィナンシャルゾーン	DCJPYプラットフォームにおいてDCJPYによる金流を担うブロックチェーン。
分散台帳プラットフォーム	分散の処理や保存、通信等の分散台帳の基本機能を提供するソフトウェア。
分散台帳システム	分散台帳プラットフォームを用いて、分散台帳を実装したシステム。ノードのネットワークで構成される。本書において、単に分散台帳システムと呼ぶ場合、スコープで記述した外部事業者の分散台帳システムのことを指す。
分散台帳ノード、または、DLTノード	分散台帳のネットワークに接続し、台帳の複製を保存するデバイスやプロセス。トランザクション作成の機能をDLTクライアントとして区別することもあるが、ここではトランザクション作成の機能も分散台帳ノードの機能の一つとして扱う。

第2章

想定される分散台帳との接続パターン

02

CONTENTS

2.1 本章について

DCJPYネットワークに接続する分散台帳システムの利用形態はユースケースごとに多種多様なものが考えられ、ビジネスゾーンのシステム内部の構成もユースケースごとに全く異なることが考えられる。デジタル通貨フォーラムの各分科会においても多様なユースケースが検討されており、今後も様々な形態のシステムが登場することが期待される。その一方で、共通のセキュリティ課題を洗い出し、その課題への対応策などの考察を深めていくためには、考察の対象となるシステムがより具体的であることが望ましい。そこで、考察の土台となるシステム構成の例示を行うこととした。

本章では、そのシステム構成の例について説明する。このシステムはあくまで例示であり、前述したように、ユースケースにより実際のシステム構成は異なるものと考えられる。システム構成が異なるケースにおいても、本節で示したシステム構成との差異を検証し、その差異がもたらすセキュリティ検討の相違について考察できるであろう。今回は、その利用形態の中でも実運用される可能性の高い3つモデルについて考察していく。

2.2 分散台帳システムの分類

この節では一般的な分散台帳システムの形態をISO 23257:2022 “Blockchain and distributed ledger technologies — Reference architecture”に基づき分類する。

分散台帳システムはパブリックとプライベートの区別と、パーミッションレスとパーミッションドの区別に分類することができる。

2.2.1 パブリックとプライベート

パブリックは図2.1に示すように分散台帳ネットワークに接続する全てのノードが台帳データ（台帳に記載されているトランザクションデータ）を読むことができるモデルである。

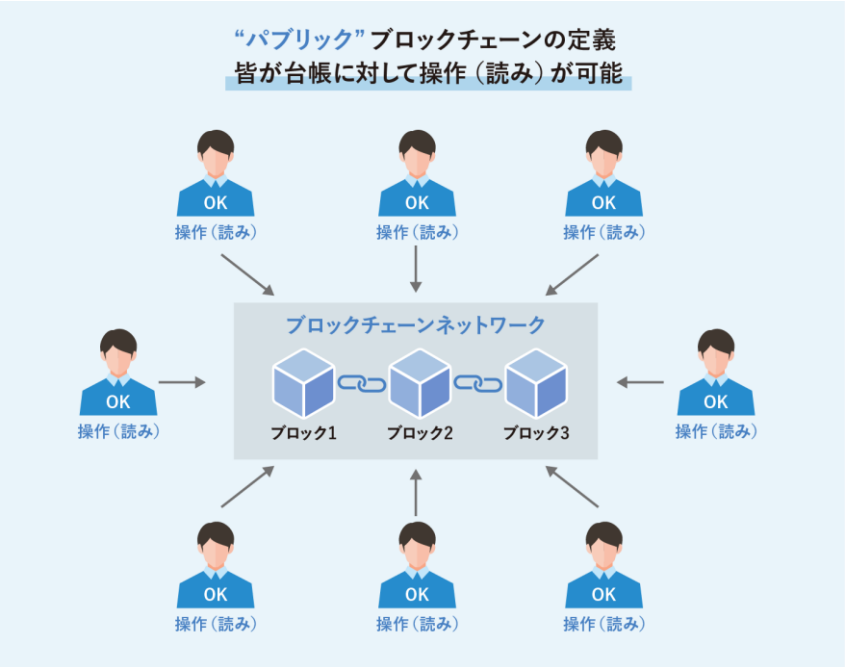


図2.1 パブリック型分散台帳の概念

対して、プライベート型分散台帳は特定のノードのグループのみが台帳データの閲覧が可能なモデルである（図2.2）。

プライベート型の分散台帳の実現方法の例としては、パブリック型の分散台帳プラットフォームを特定のノードのみが接続できる閉じられた通信ネットワーク内に配置することや、後述するパーミッションド型の分散台帳を用いてノードのアクセス制御を行うことが考えられる。

台帳データの書き込みについては、BitcoinのProof of Workのように全てのノードに対してオープンであるモデルや、特定のノードのみが台帳データの生成が可能なモデルが存在するが、このいずれの場合もパブリック型になりえる（後者については後述するパブリックパーミッションドを参照のこと）。

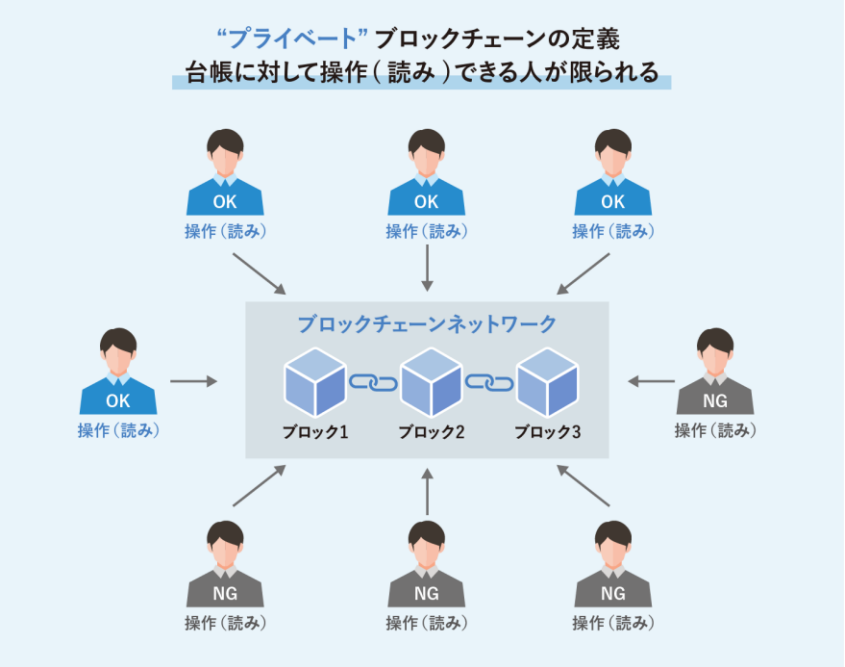


図2.2 プライベート型分散台帳の概念

2.2.2　パーミッションレスとパーミッションド

パーミッションレスとパーミッションドの区別は、分散台帳システムへの接続における許可の必要性に関するものである。パーミッションレス型の分散台帳プラットフォームではノードの接続に関してアクセス制御や許可の機能をもっていない（図2.3）。

対して、パーミッションド型では、接続の許可に関わる手続きやアクセス制御機能などを備えた仕組みとなっている（図2.4）。例えば、パーミッションドとして対応可能な分散台帳プラットフォームとして、Hyperledger FabricやHyperledger Besu、R3 Cordaが挙げられる。

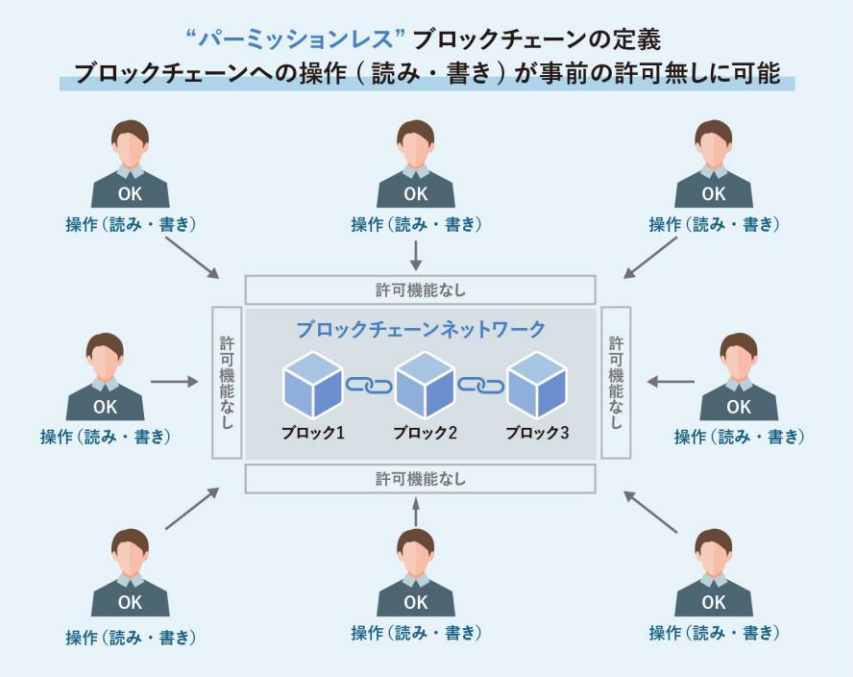


図2.3 パーミッションレス分散台帳の概念

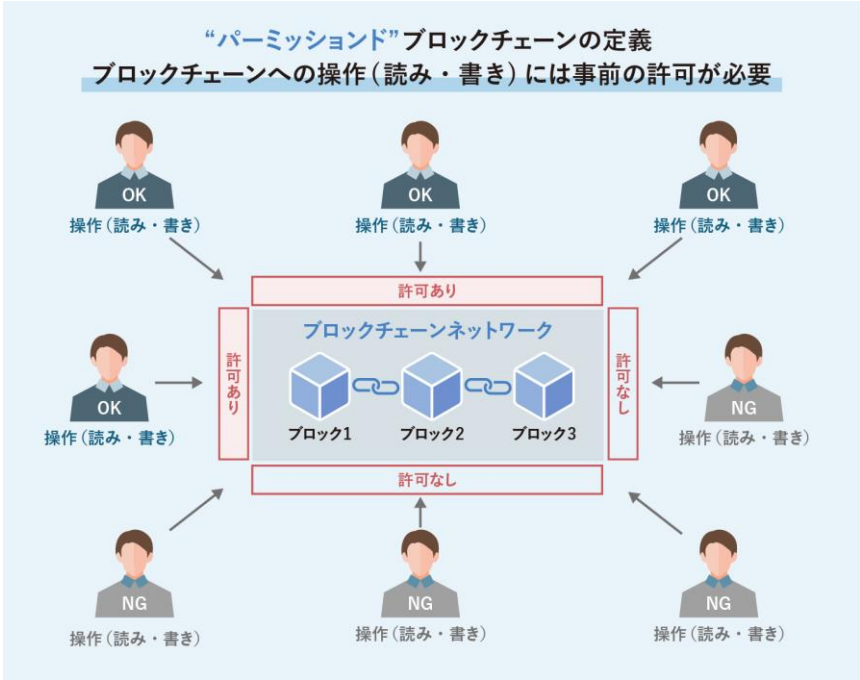


図2.4 パーミッションド分散台帳の概念

2.2 分散台帳システムの分類

パブリックとプライベートの区別と、パーミッションレスとパーミッションドの区別は独立したものとなっており、プラットフォームのアーキテクチャと導入方法によって両者の区別を組み合わせた形態がありえる。

■ パブリックパーミッションレス

誰もが台帳データの読み書き等の操作が可能なモデル。接続に関して事前の許可やアクセス制限等がない。例えば、世界中で使用されているBitcoinやEthereumのネットワークがこの分類となる。

■ パブリックパーミッションド

台帳データの閲覧は誰もが可能であるが、台帳データの書き込みは事前に許可された特定のノードだけに限定される。例えば、台帳データで食品トレーサビリティに関するデータを管理するとき、消費者として接続するノードは誰しもが台帳データに記載されている食品流通経路の情報が閲覧可能であるのに対し、台帳データへの書き込みは食品流通関係者のみに限定するようなケースである。

■ プライベートパーミッションレス

分散散台帳プラットフォームには接続されるノードへの許可やアクセス制御の機構を備えていないが、分散台帳プラットフォームを稼働させる環境等の制限によって、特定のノードのみが操作を可能とするモデル。例えば、BitcoinやEthereumのプラットフォームのソフトウェアを閉じられた通信ネットワーク上に配置して運用することで、限定されたノードのみが接続できる、独自の分散台帳ネットワークを構築することが考えられる。

■ プライベートパーミッションド

台帳データの操作に対する許可の機構を備えた分散台帳プラットフォームを用いて、特定のノードのみが操作できる分散台帳ネットワークを構築する。例えば、Hyperledger FabricやBesu等を用いて、ある業界内で使用する分散台帳ネットワークを構築するケースである。デジタル通貨プラットフォームのフィナンシャルゾーン・ビジネスゾーンの基盤となる分散台帳システムもこの形態である。

本書では、DCJPYネットワークに接続するビジネスゾーンのシステムが扱う外部の分散台帳システムの代表例として、「パブリックパーミッションレス」のケースと、「プライベートパーミッションド」のケースの2つに焦点を当てることとする。

前者は、既に世界中で多くの利用者が存在する暗号資産やデジタル資産のネットワークと連携するケースを想定しており、後者はビジネスゾーンの事業者間で、特定の業界向けに利用することを想定した分散台帳システムを構築し、DCJPYと連携することを想定したケースである。

残りのパブリックパーミッションドとプライベートパーミッションレスについては、本書が対象とした2つのケースと共通する課題が内包しているものと考えられ、本書の考察を元として検討することが期待できる。

2.3 分散台帳システムを利用するビジネスゾーンのシステムモデルの例

本書ではパブリックパーミッションレス型とプライベートパーミッションド型の分散台帳システムを利用したビジネスゾーンのシステムとして、以下の3つの異なる形態について考察を行う。本書ではビジネスゾーンの事業者として架空のXYZ社を想定し、XYZ社が管理するシステムを対象に考察を行っている。

- **想定システムモデル１**
  （パブリックパーミッションレス・カストディアルウォレット型）
  XYZ社がパブリックパーミッションレス型分散台帳システムを利用してデジタル資産とDCJPYの取引を行うケース。エンドユーザーのデジタル資産に関わる取引をXYZ社が代行するケース。

- **想定システムモデル２**
  （パブリックパーミッションレス・ノンカストディアルウォレット型）
  XYZ社がパブリックパーミッションレス型分散台帳システムを利用してデジタル資産とDCJPYの取引を行うケース。エンドユーザーのデジタル資産に関わる取引は、エンドユーザー自身のウォレットを介して行うケース。

- **想定システムモデル3**
  （プライベートパーミッションド）
  XYZ社が業界内で共同管理するプライベートパーミッションド型分散台帳システムを利用してデジタル資産の取引を行うケース。エンドユーザーに対してXYZ社がデジタル資産に関わるユーザーインターフェース等を提供する。

各考察において、以下の前提を置く。

【想定ユースケースの前提条件】

XYZ社のサービスについて

- XYZ社はデジタル資産の売買を行うオンラインサービスを提供する。
  このサービスを利用するエンドユーザー間でデジタル資産の売買を行う。
- XYZ社はビジネスゾーンの事業者に位置づけられる。
- XYZ社はDCJPYに基づいて発行されるビジネスゾーンの通貨XYZコインを使用する。
- デジタル資産の売買はXYZコインで行うことができる。エンドユーザーは、このサービス利用時にXYZ社が管理するサービス用アカウントを作成する。このサービスにログインするときには、そのアカウントIDを使用する。
- オンラインサービスはXYZ社が管理するビジネスゾーンのシステムによって提供される。
- ビジネスゾーンのシステムはDCJPYネットワークに接続し、XYZコインの送金指示を行う。ビジネスゾーンのシステムはDCJPYネットワークへの接続に必要な署名鍵を管理する（4.4.3 分散台帳ノードの鍵管理も参照のこと）。
- ビジネスゾーンのシステムはデジタル資産を管理する分散台帳システムに接続する。接続形態は想定システムモデル毎に異なる。
- 分散台帳システムにおいてスマートコントラクト実行やデジタル資産の交換を行う場合、その分散台帳システムの暗号資産等が必要になることも考えられるが、ビジネスゾーンのシステムはあらかじめ必要な暗号資産等を保有しているものと仮定する。暗号資産の管理はXYZ社の責任で行われ、暗号資産の移転に必要な署名鍵の管理もビジネスゾーンのシステムで行われる。ここではデジタル資産と暗号資産の交換、XYZコインと暗号資産の間の交換に関わる機能はスコープ外とする。

2.4 想定システムモデル1（パブリックパーミッションレス・カストディアルウォレット型）

想定システムモデル1は、デジタル資産を管理するパブリックパーミッションレス型の分散台帳システムにXYZ社のビジネスゾーンのシステムが接続し、ビジネスゾーンのシステムがデジタル資産の発行や移転等の操作を分散台帳システムに対して行う。したがって、XYZ社はデジタル資産の移転を行うトランザクションを作成するための署名鍵を管理することになる。

ここではイメージを容易にするためパブリックパーミッションレス型の分散台帳システムとしてEthereumを例に挙げているが、以降の考察はEthereumに限ったものではなく、他のパブリックパーミッションレス型の分散台帳システムにも該当するものと考えられる。

サービスの開始時においてビジネスゾーンのシステムは以下を前提とし必要な準備は完了しているものとする。

＜前提＞

- XYZ社のサービスとしてログインやデジタル資産取引実行のための認証手段をエンドユーザーに提供する。または、別の主体者によって提供される認証手段（別のデバイスの認証器など）を採用する可能性もある。
- エンドユーザーの登録プロセスが完了したのち、エンドユーザーはXYZ社のサービスを利用可能になる。
- ビジネスゾーンのシステムはエンドユーザーに対して、デジタル資産（NFT）のマーケットプレイスのユーザーインターフェースを提供する。
- 提供方法はWebアプリケーションやスマートフォンのアプリケーションなどの形態が考えられるが図2-5ではスマートフォンを例として記載している。

＜事前準備＞

- 分散台帳システムの接続に必要な署名鍵やブロックチェーンアドレス、アカウント等の作成。
- サービス実施に必要な暗号資産の取得。
- DCJPYネットワークを利用するための設定。DCJPYネットワークへの接続のための署名鍵の生成や登録など。
- エンドユーザーがサービス利用に必要なDCJPYのアカウント開設とDCJPYウォレットの設定（フィナンシャルゾーンによって提供される）。
- XYZ社のサービスに必要なアカウント登録手続き（DCJPYのアカウントやDCJPYウォレットの連携のための登録も含む）。

2.4　想定システムモデル1（パブリックパーミッションレス・カストディアルウォレット型）

図2-5は想定システムモデル1のイメージを示している。この図において取引を行うデジタル資産としてNFTを例としている。

ビジネスゾーンのシステムは分散台帳システムからデジタル資産に関する情報を取得し、売買可能なデジタル資産（NFT）の一覧を表示する。例えば、デジタル画像に対するNFTの場合には、NFTが参照するデジタル画像を取得して表示することも考えられる。

分散台帳システムへの接続はビジネスゾーンのシステム内の分散台帳ノードを通じて行われる。

分散台帳システムから取得した情報を元に事業者サーバーで、デジタル資産の権利を持つエンドユーザー情報（XYZ社が管理するアカウント）との対応関係や、デジタル資産の価格の判定等を行う。その結果をもとに、ビジネスゾーンのシステムのNFTマーケットプレイスの機能でユーザーに提示する表示の作成等を行う。

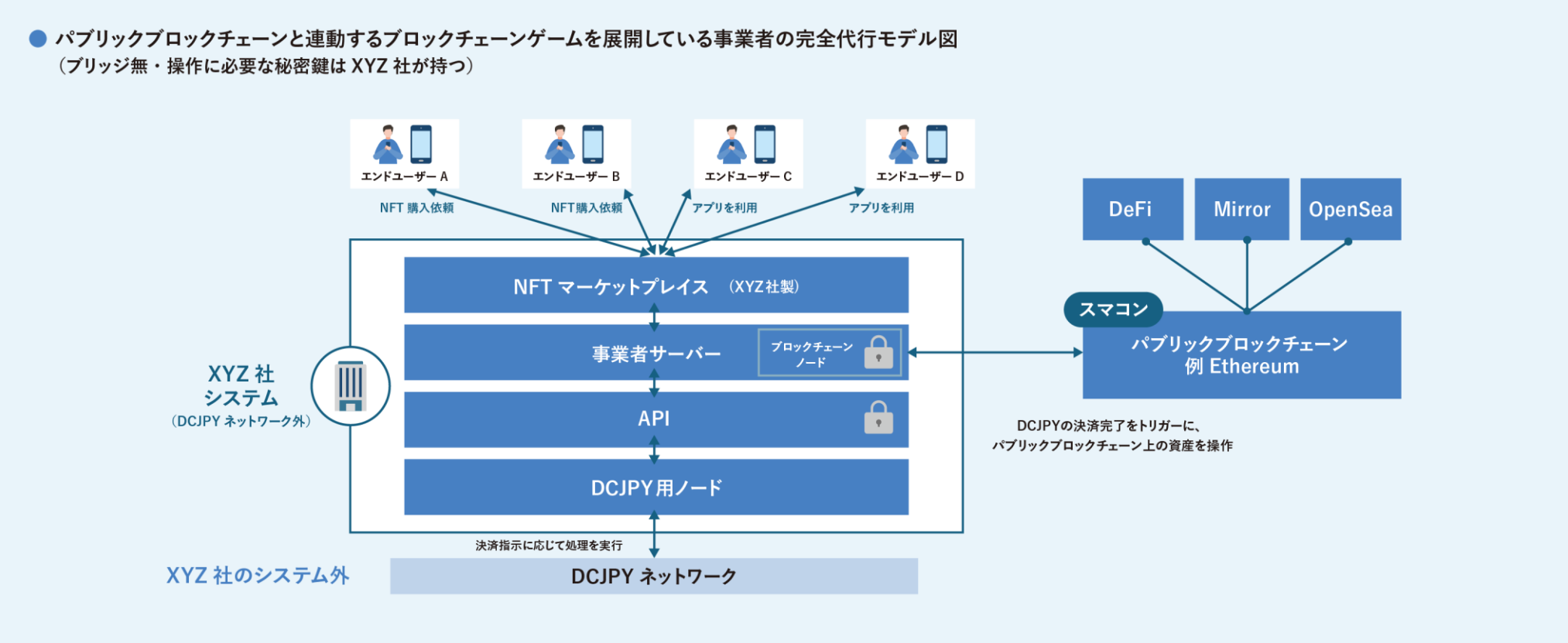


図2.5 想定システムモデル1

2.4　想定システムモデル1（パブリックパーミッションレス・カストディアルウォレット型）

エンドユーザーによるNFT購入時のフローの例を図2-6に示す。

ここでは単純に、XYZ社が新たに発行するNFTをエンドユーザーが購入するフローを示している。各工程は実際の設計によって前後することもある。

- エンドユーザーはNFTマーケットプレイスのユーザーインターフェースを通じてデジタル資産を購入する指示を行う。これらのリクエストはエンドユーザーのスマートフォン等を通じて、ビジネスゾーンのシステムが提供するNFTマーケットプレイスのユーザーインターフェースに対して行われる。NFTマーケットプレイスに行われたリクエストはビジネスゾーンサーバーで処理される。
- XYZコインの送金が必要な場合には、NFTマーケットプレイスを通じてエンドユーザーに送金操作の要求を出す。エンドユーザーはDCJPYウォレットの機能を用いて送金指示を作成する。送金指示はビジネスゾーンのシステムを通じてフィナンシャルゾーンに送られ（図2-6では省略）、送金処理が実行される。
- デジタル資産の移転など分散台帳システムに対して処理が必要なもの（NFTの発行指示とエンドユーザーのアカウントへの移転）は、トランザクションを作成し分散台帳ノードを通じて分散台帳システムに送信する。この際、分散台帳システムに配置されたスマートコントラクトを実行することも考えられる。このスマートコントラクトはXYZ社で開発される場合もあれば、サードパーティのスマートコントラクトを利用する場合も考えられる。事業者サーバーはスマートコントラクトの実行結果と連動し処理を行う。
- 事業者サーバーはXYZコインの送金処理とデジタル資産の移転処理の結果に基づき、デジタル資産の取引状態を更新し、エンドユーザーに結果を返却する。

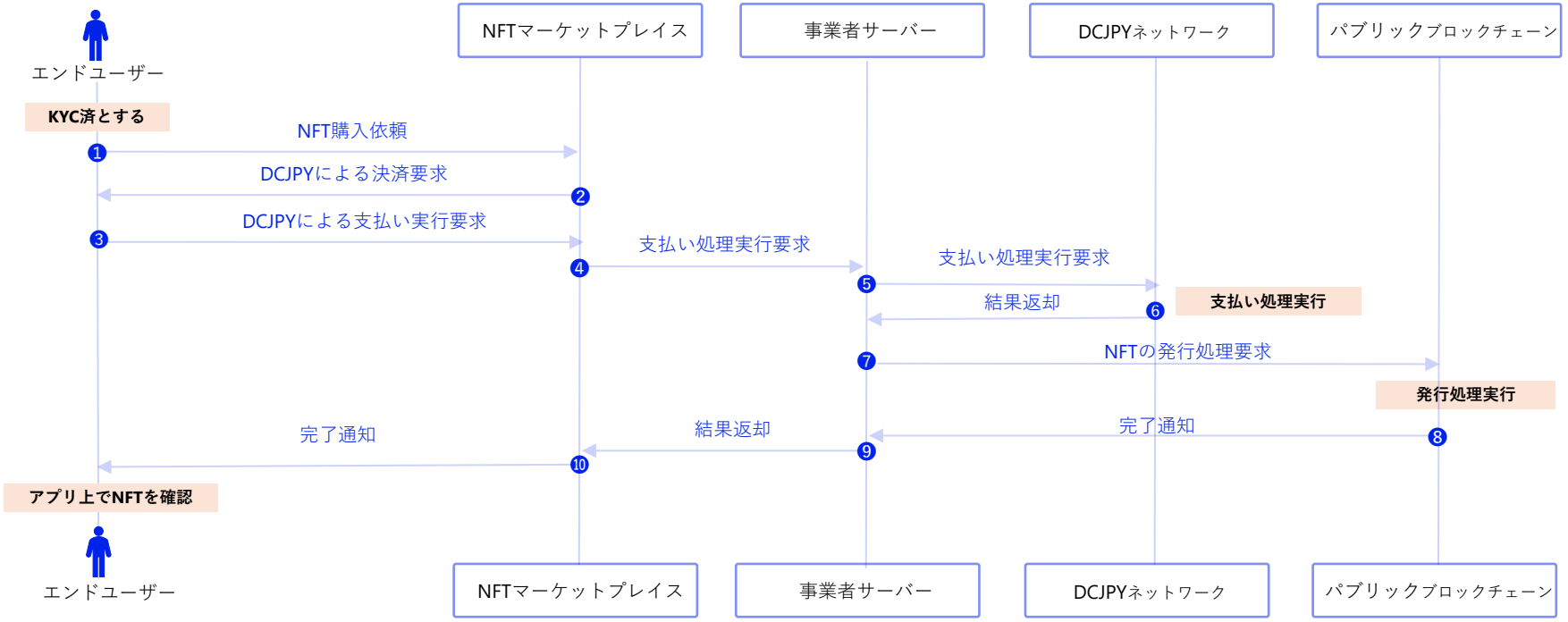


図2-6　想定システムモデル1のフロー例

2.5 想定システムモデル2（パブリックパーミッションレス・ノンカストディアルウォレット型）

想定システムモデル2は、エンドユーザーはデジタル資産の署名鍵を管理するデジタル資産ウォレットを自身で管理するケースである。デジタル資産の管理はパブリックパーミッションレス型の分散台帳システムが行う。XYZ社のビジネスゾーンのシステムではエンドユーザーのデジタル資産の署名鍵は管理せず、デジタル資産とエンドユーザーに関する情報を管理する。

ここではイメージを容易にするためパブリックパーミッションレス型の分散台帳システムとしてEthereumを例に挙げているが、以降の考察はEthereumに限ったものではなく、他のパブリックパーミッションレス型の分散台帳システムにも該当するものと考えられる。

サービスの開始時においてビジネスゾーンのシステムは以下を前提とし必要な準備は完了しているものとする。

＜前提＞

- エンドユーザーはサービス利用前にデジタル資産ウォレットの準備が完了しており、デジタル資産の移転のための署名鍵を管理しているものとする。
- DCJPYのアカウント開設とDCJPYウォレットの設定は完了しているものとする。
- DCJPYのアカウント開設とDCJPYウォレットの手続きはフィナンシャルゾーンによって提供されるものとする。
- XYZ社のサービスについて、アカウント登録の手続きがあるが、この過程には、デジタル資産ウォレット、DCJPYアカウント、DCJPYウォレットの連携のための登録が含まれる。
- デジタル資産ウォレットは様々な形態が考えられ、また、エンドユーザーによって選定されるため、デジタル資産ウォレットとXYZ社のサービスアカウントとの紐づけ方法もウォレットの種類によって異なる。本書では具体的な紐づけ方法の提示は行わず、抽象化したプロセスとして言及するのみとする。

＜事前準備＞

- DCJPYネットワークを利用するための設定。DCJPYネットワークへ接続するための署名鍵の生成や登録など。
- NFTマーケットプレイスと連動するスマートコントラクトを分散台帳システムに配置する。

2.5　想定システムモデル2（パブリックパーミッションレス・ノンカストディアルウォレット型）

図2-7は想定システムモデル2のイメージを示している。この図において取引を行うデジタル資産としてNFTを例としている。

XYZ社はサービスのログインやデジタル資産取引実行のための認証手段をエンドユーザーに提供する、または、別の主体者によって提供される認証手段（別のデバイスの認証器、デジタル資産ウォレットやDCJPYウォレットが提供する機能など）を採用する可能性もある。

エンドユーザーの登録プロセスが完了したのち、エンドユーザーはXYZ社のサービスを利用可能になる。

ビジネスゾーンのシステムはエンドユーザーに対して、デジタル資産（NFTなど）のマーケットプレイスのユーザーインターフェースを提供する。

提供方法はWebアプリケーションやスマートフォンのアプリケーションなどの形態が考えられる。図2-7ではスマートフォンを例として記載している。

ビジネスゾーンのシステムは分散台帳システムからデジタル資産に関する情報を取得し、売買可能なデジタル資産（NFT）の一覧を表示する。エンドユーザーから提供された情報(送金先アドレスや送金額など)に基づき、ビジネスゾーンのシステムが分散台帳システムからデジタル資産に関する情報を取得する。分散台帳システムから取得した情報を元に事業者サーバーで、デジタル資産の権利を持つエンドユーザー情報（XYZ社が管理するアカウント）との対応関係や、デジタル資産の価格の判定等を行う。その結果をもとに、ビジネスゾーンのシステムのNFTマーケットプレイスの機能でユーザーに提示する表示の作成等を行う。

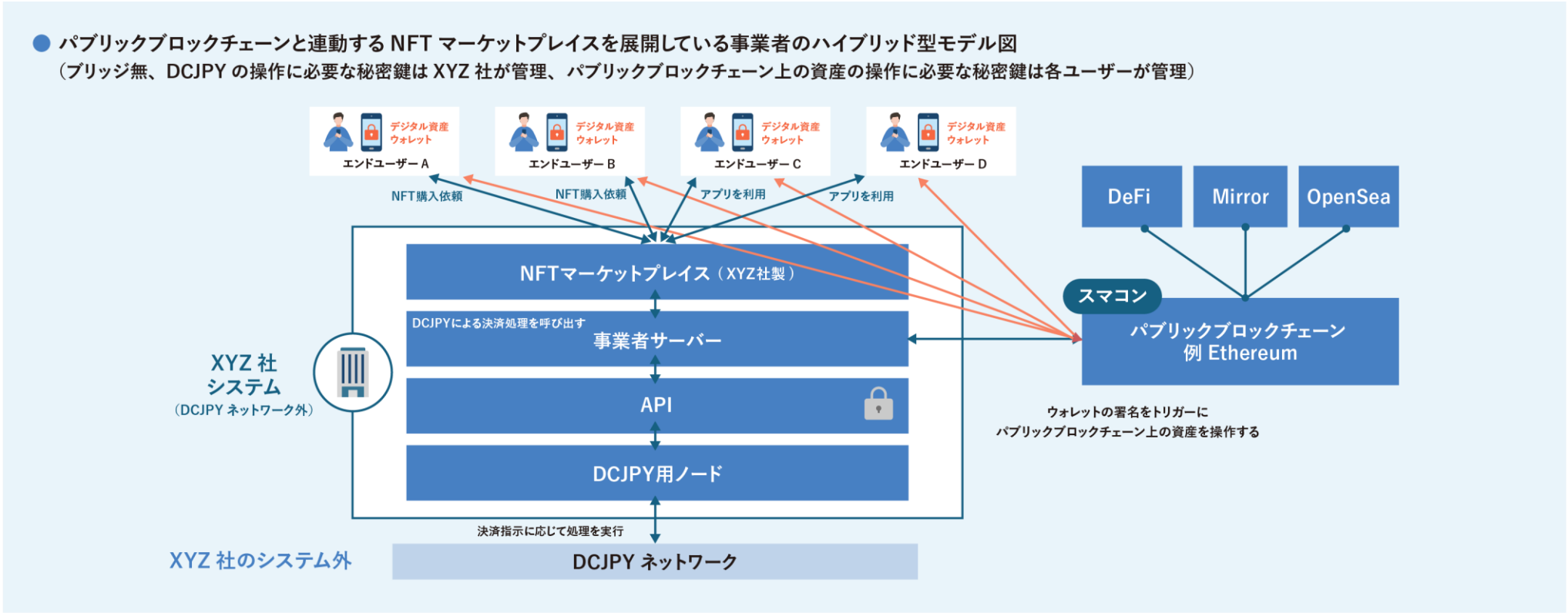


図2.7 想定システムモデル2

2.5　想定システムモデル2（パブリックパーミッションレス・ノンカストディアルウォレット型）

エンドユーザー間によるNFT購入時のフローの例を図2-8に示す。各工程は実際の設計によって前後することもある。

- エンドユーザー1が、エンドユーザー2の保有するデジタル資産を購入する。まず、あらかじめエンドユーザー2は自身のデジタル資産ウォレットを操作し、売却したいデジタル資産を分散台帳システムにあるスマートコントラクトに移転する。このスマートコントラクトはNFTマーケットプレイスと連動しており、ビジネスゾーンのシステムから操作できる。
- エンドユーザー１はNFTマーケットプレイスのユーザーインターフェースを通じてエンドユーザー2のデジタル資産を購入する指示を行う。これらのリクエストはエンドユーザーのスマートフォン等を通じて、ビジネスゾーンのシステムが提供するNFTマーケットプレイスのユーザーインターフェースに対して行われる。
- NFTマーケットプレイスに行われたリクエストは事業者サーバーで処理され、エンドユーザー1に対してデジタル資産に対するXYZコインの支払いを要求する。
- エンドユーザー1はDCJPYウォレットを通じて、エンドユーザー2に対してXYZコインの支払いを行う。
- NFTマーケットプレイスは支払いを確認したあと、スマートコントラクトに対して、エンドユーザー2のデジタル資産をエンドユーザー1の分散台帳アドレスへ移転するように指示を行う。
- 事業者サーバーはXYZコインの送金処理とデジタル資産の移転処理の結果に基づき、デジタル資産の取引状態を更新し、エンドユーザー1とエンドユーザー2に結果を返却する。

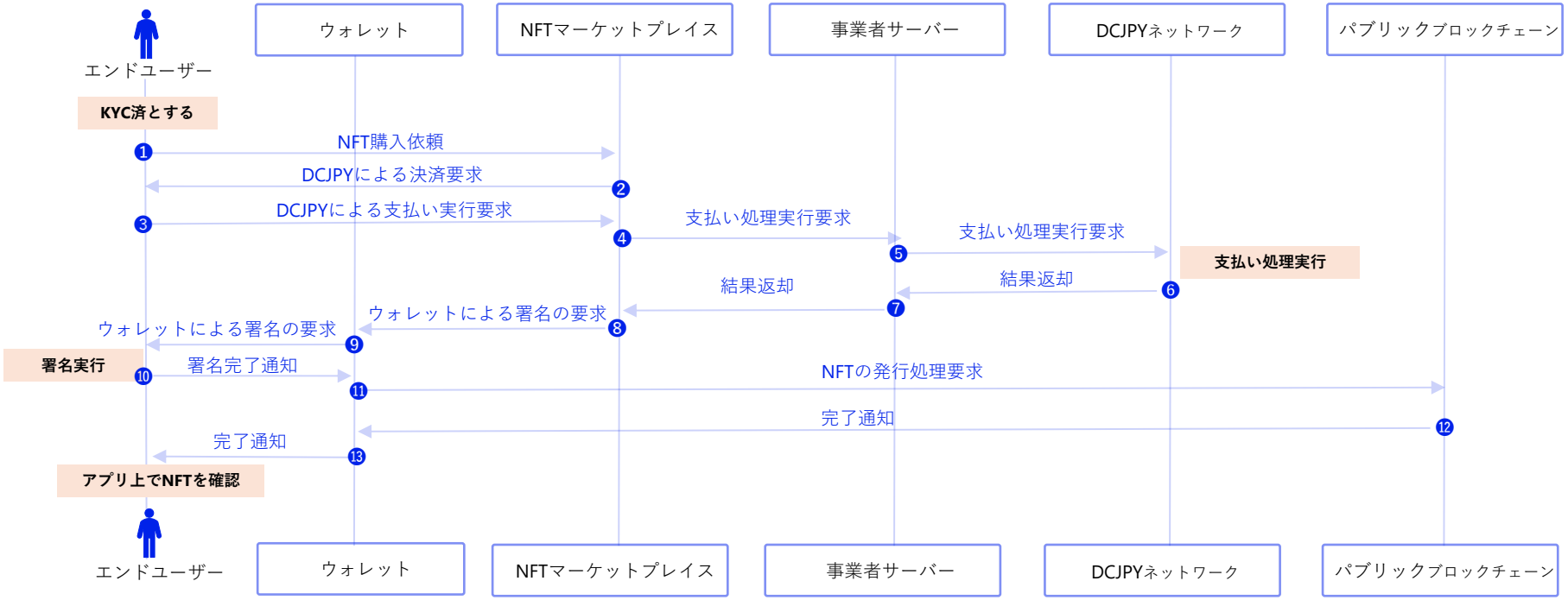


図2-8　想定システムモデル2のフロー例

2.5 想定システムモデル2（パブリックパーミッションレス・ノンカストディアルウォレット型）

この例では単純化するため、エンドユーザー1から直接エンドユーザー2へXYZコインの支払いを行っているが、取引における手数料の徴収や誤送金の防止、エンドユーザー間のプライバシー保護などの観点から、ビジネスゾーンの事業者のDCJPYアカウントへ送金し、ビジネスゾーンの事業者からエンドユーザー2へ送金を行うことも考えられる。

デジタル通貨の送金が必要な場合には、NFTマーケットプレイスを通じてエンドユーザーに送金操作の要求を出す。エンドユーザーはDCJPYウォレットの機能を用いて送金指示を作成する。送金指示はビジネスゾーンのシステムを通じてDCJPYネットワークに送られ、送金処理が実行される。

デジタル資産の移転など分散台帳システムに対して処理が必要なもの（NFTの発行指示とエンドユーザーのアカウントへの移転）は、トランザクションを作成し分散台帳ノードを通じて分散台帳システムに送信する。この際、分散台帳システムに配置されたスマートコントラクトを実行することも考えられる。このスマートコントラクトはXYZ社で開発される場合もあれば、サードパーティのスマートコントラクトを利用する場合も考えられる。事業者サーバーはスマートコントラクトの実行結果と連動し処理を行う。

事業者サーバーはXYZコインの送金処理とデジタル資産の移転処理の結果に基づき、デジタル資産の取引状態を更新し、エンドユーザーに結果を返却する。

2.6 想定システムモデル3（プライベートパーミッションド）

想定システムモデル3は、プライベートパーミッションド型の分散台帳システムに接続すること以外、想定システムモデル1と類似している。

デジタル資産を管理するプライベートパーミッションド型の分散台帳システムにXYZ社のビジネスゾーンのシステムが接続し、ビジネスゾーンのシステムがデジタル資産の移転等の操作を分散台帳システムに対して行う。

プライベートパーミッションド型の分散台帳システムでは、システムへ接続する各ノードの実行環境に対するセキュリティ基準、ノード管理者の身元確認や認証認可の実施、意思決定方法の取り決めなどを含めたガバナンスの働きが期待できる。それにより、適切なガバナンスを前提に分散台帳システムやスマートコントラクトを設計することによって、関係当事者間だけの分散台帳情報の共有や、トランザクションや台帳や接続するノード等に問題が発生した際の停止や失効等の対応を管理者間の連携等によって実現できる可能性もある。

サービスの開始時において以下の準備は完了しているものとする。

<事前準備>

- 分散台帳システムに関わる設計と配置
  この分散台帳システムは目的やポリシーを共有する企業コンソーシアムで運用されている。コンソーシアムにはXYZ社以外にA社、B社、C社が参画し、それぞれ分散台帳ノードを管理している。コンソーシアム以外のノードは接続できない。

- ビジネスゾーンのシステムが分散台帳システムに接続するために必要な設定。例えば、ノードの認証クレデンシャル（署名鍵など）やアドレス、アカウント等の作成や登録。

- DCJPYネットワークを利用するための設定。DCJPYネットワークへの接続のための署名鍵の生成や登録など。

2.6　想定システムモデル3（プライベートパーミッションド）

このモデルのシステム例を図2-9に、NFT購入から送金に至るフローの例を図2-10に示す。
プライベートパーミッションド型の分散台帳システムとしてHyperledger Fabricを例に挙げているが、以降の考察はHyperledger Fabricに限ったものではなく、他のプライベートパーミッションド型の分散台帳システムにも該当するものと考えられる。

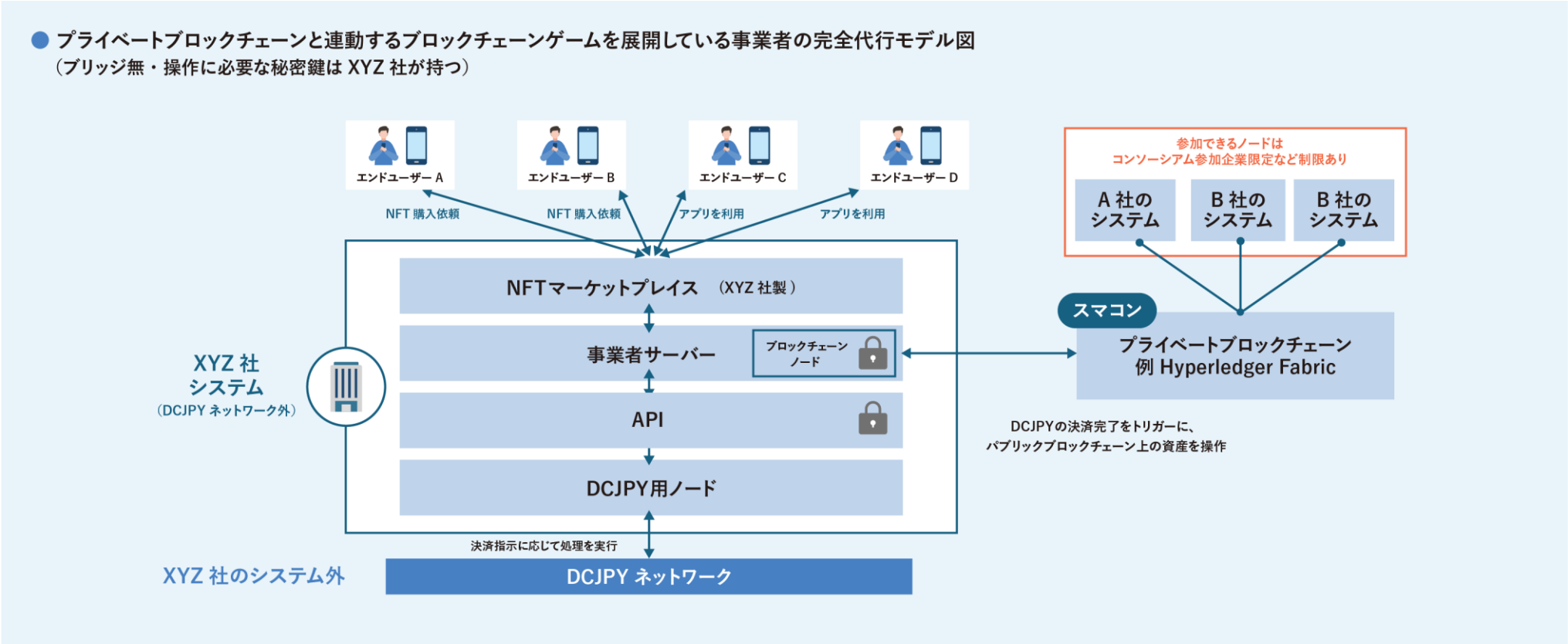


図2-9　想定システムモデル 3

2.6 想定システムモデル3（プライベートパーミッションド）

エンドユーザーの登録の工程と、デジタル資産の取引からXYZコインの送金に至る工程は想定システムモデル1 （2.3節）と同様である。

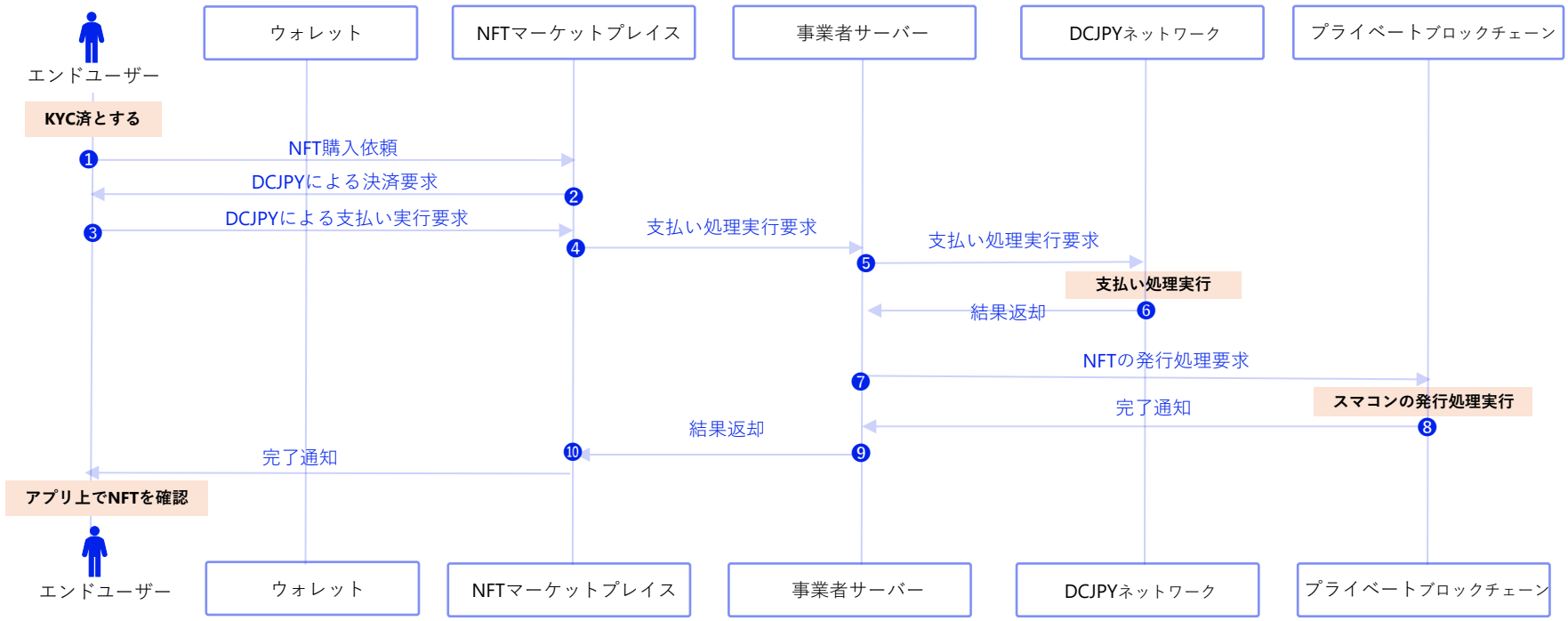


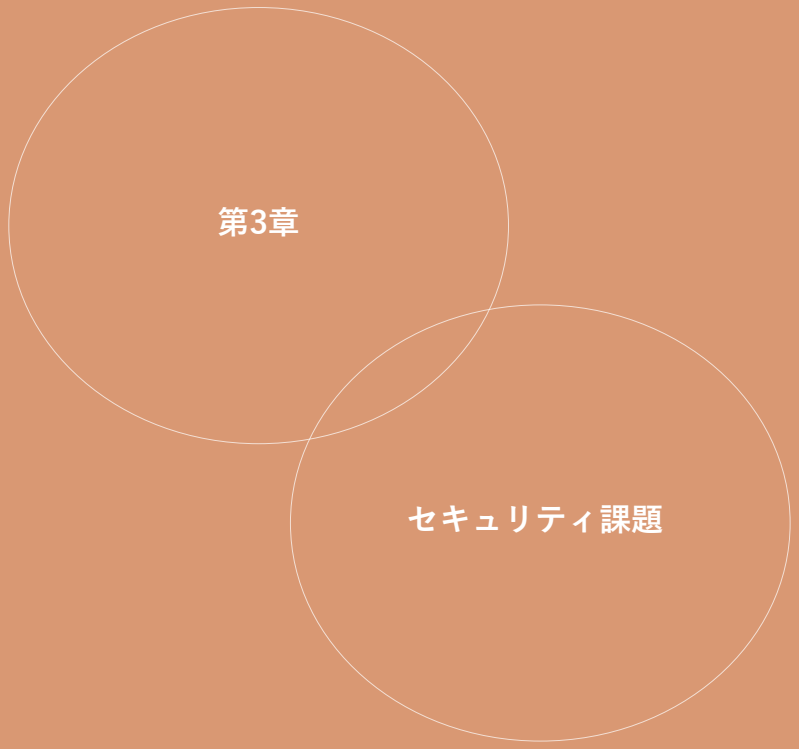
図2-10　想定システムモデル3のフロー例

第3章

セキュリティ課題

03

CONTENTS



3.1 本章について

本章では2章で述べた各システムモデルについて、
セキュリティに関わるリスクや課題について考察する。

3.2.1 本節について

本節では、想定システムモデル1からモデル3に対するセキュリティ課題を検討するため、分散台帳の基本機能を提供する分散台帳プラットフォーム、実際に構築され運用される分散台帳システム、分散台帳システムを構成する各ノードに関する一般的脅威について考察する。

3.2.2 分散台帳プラットフォームに対する脅威

3.2.2.1 分散台帳プラットフォームの考察点

ビジネスゾーンのシステムが接続する分散台帳システムの基本機能群を提供するソフトウェアをここでは「分散台帳プラットフォーム」と呼ぶ。分散台帳プラットフォームの例としては、Ethereum、Hyperledger Fabricがある。分散台帳プラットフォームのソフトウェアを実行する複数のノードが協調的に動作することで一つの分散台帳システムが構築される。

分散台帳システムは、分散台帳プラットフォームの機能や性能を拡張するレイヤー2と総称されるプロトコルや、サイドチェーンと呼ばれる補助的な別の分散台帳システムと共に用いることもある。レイヤー2は分散台帳システムの特定のノード間で適用することが考えられ、サイドチェーンの運用は基盤となる分散台帳システムとは別の主体（ノード群）が行うことが考えられる。レイヤー2やサイドチェーンのソフトウェアは分散台帳プラットフォームとは別の主体によって開発されうる。

この節では基盤となる分散台帳プラットフォームに着目して考察を行うが、その考察はレイヤー2やサイドチェーンのソフトウェアにも同様に適用することが考えられる。ここでは純粋に分散台帳プラットフォームに潜在する脅威の可能性について考察するが、各脅威が即座に実際の分散台帳システムを危殆化するものとは限らない。分散台帳プラットフォームに対する脅威が実際の分散台帳システムに対して現実化する可能性は、脅威の影響を受けるノードの全体に占める割合などにも関係する。分散台帳システムに対する脅威は3.2.3節で扱う。

基盤となる分散台帳プラットフォームには、一般的に以下のような機能や要素が含まれることがある。

- コンセンサスメカニズム
- 台帳管理
- トランザクションの生成と検証
- スマートコントラクトの生成と配置、実行
- ノード間通信
- ノードの認証や認可
- 暗号アルゴリズム

分散台帳プラットフォームの「設計や仕様に基づく脅威」と、それらの「実装に基づく脅威」がある。設計や仕様に基づく脅威では実装全体に影響を与えるが、実装方法に脆弱がある場合にはその方法を適用した特定の実装に対して影響を与える。

3.2.2.2 コンセンサスメカニズム

分散台帳技術では、様々なノードから生成されるトランザクションを検証し、台帳に格納すべきトランザクションを判定し、台帳に格納するといった台帳生成に関わる一連の処理を複数のノード間で協調して行うことが必要となる。台帳の整合性を維持するため、各ノード間で協調するメカニズムはコンセンサスメカニズムと総称される。コンセンサスメカニズムは複数の手法が提案されており、分散台帳プラットフォームごとに異なる。コンセンサスメカニズムの分類の例として以下のものがある（ISO 23257参照）。

- ラウンドロビン型
  複数の管理ノードを設定し、それらが持ち回りで台帳の生成を行う。
- PBFT(practical Byzantine Fault Tolerance)型 [1]
  複数の管理ノード間で台帳生成に関わる互いのメッセージを確認することで、整合性を維持する。ビザンチン障害耐性(Byzantine Fault Tolerance)をもつメカニズムでは、マルウェア等の感染により不正なメッセージを発するノードが存在しても、それを上回る正常なノード は正しいメッセージを共有できる。
- ナカモトコンセンサス型
  特定の管理ノードを規定せず、暗号資産の報酬等により自発的に各ノードが台帳の生成と協調に参加することを促す仕組み。代表的なものとして、BitcoinのProof of WorkやEthereumのProof of Stakeがある。

ビザンチン障害耐性ではなくノードの停止に対する障害（停止障害）耐性のみを持つ手法を適用する場合もある。

コンセンサスメカニズムは台帳生成と共有を行う分散台帳技術の重要な役割を担う。コンセンサスメカニズムの設計や仕様、実装に重大な不具合がある場合には、台帳データの不正な書き換え、不正な複製、台帳生成の機能停止や遅延によるトランザクションやスマートコントラクトの実行停止や遅延、台帳生成の役割を担うノードの支配などの脅威につながる可能性もある。

また、分散台帳システムの運用形態（2.2節の分類）やノードのネットワークの規模等によって、その脅威の実現可能性や、起きた場合の影響度が異なる。脆弱性の内容にもよるが、一般的に台帳生成に関わるノードの規模が大きいほど、特定の攻撃者が不正を実現させる可能性は低くなるものと考えられる。一方で、ネットワークの規模が大きい場合には、ソフトウェアの脆弱性や不正な台帳の修正を行う際の影響範囲はより大きいものとなると考えられる。

分散台帳プラットフォームが採用するコンセンサスメカニズムにどのような特性を持ち、台帳の生成や検証に関与するノードの存在など台帳の真正性担保がどのような信頼構造で成り立っているかを考察することは、分散台帳プラットフォームの安全性を評価するうえで大切なポイントとなる。コンセンサスメカニズムに意図せぬ不具合が存在しなかったとしても、その仕様上の特性を利用して、特定の者に台帳のコントロールを握られる脅威も存在する。それについては3.2.3.5節で扱う。

[1]手法により、例えば、不正なノードが全体の1/3未満であれば正しく動作するなど。

3.2.2.3 台帳管理

コンセンサスメカニズムを経て生成された台帳データは各ノードで複製され管理される。台帳データの全体を保持するノードはフルノードと呼ばれる。台帳の複製方法によって、ある瞬間において、あるノードが持つ台帳はその他のノードが持つ台帳の状態と一致しない状態にもなりえる。Proof of Workのような台帳データのファイナリティーのないメカニズムでは、一時的な台帳データの巻き戻し（reorg）が起こる可能性もある。各ノードの台帳データの不整合や、台帳データ管理の機構に不具合が生じた場合には、そのノードにおいて、台帳を参照したトランザクションの検証や確認（残高確認等）が正常に行えなくなる恐れがある。分散台帳プラットフォームの仕様や実装に問題があり、大規模に影響が及ぶ場合には、分散台帳システム全体において台帳データやトランザクションの転送や停止や遅延に繋がる可能性もある。

3.2.2.4 トランザクションの生成と検証

トランザクションの生成機能の不具合は、トランザクション処理の停止や遅延につながる可能性がある。また、生成機能の重大な脆弱性によって、攻撃者によるトランザクションの不正な生成（署名鍵の不正な利用）や、署名鍵の漏洩に繋がる場合には、大きな脅威となる。万が一、署名鍵が漏洩し、攻撃者に入手された場合には、当該トランザクション機能を修正したとしても、攻撃者はその署名鍵を使って別のノードから不正なトランザクションを生成することができる。

トランザクションの検証機能の不具合は、トランザクションの検証や確認の正常な実行を妨げることとなる。重大な脆弱性がある場合には、不正なトランザクションを受け入れてしまうことで攻撃の原因ともなりえる。大規模に影響が及ぶ場合には、分散台帳システム全体においてトランザクションやスマートコントラクトの実行の遅延や停止に繋がる可能性もある。トランザクションのデータフォーマットや、デジタル署名の生成や検証方法といった仕様上に原因がある場合には、不具合の影響度や修正の範囲、困難さがより大きなものとなりえる。

3.2.2.5 スマートコントラクトの生成と配置、実行

スマートコントラクトの生成と配置、実行に関わる機能群の不具合や脆弱性は3.2.2.4と同様にスマートコントラクトの正常な実行を妨げ、重大な場合には不正なスマートコントラクトの実行につながる可能性がある。分散台帳システムが管理するスマートコントラクト全般に影響が広がる可能性もある。スマートコントラクト自身が暗号資産などのデジタル資産を管理することがあること、また、他の分散台帳システムのスマートコントラクトと協調動作することが考えられることから、影響の度合いや範囲が大きなものとなりえる。

3.2.2.6 ノード間通信

ノード間ではトランザクションや分散台帳共有のためのメッセージを交換する。これらのメッセージ交換は例えばTCP/IPのような通信層の上で行われる。一般的にメッセージ交換のためのプロトコルや通信層の脅威では、メッセージ改ざんや、メッセージの再送攻撃、通信妨害、不正なノードへの接続の誘導などが考えられる。分散台帳プラットフォームのほとんどはメッセージにノードのデジタル署名を付すため、その署名鍵や署名生成処理が脆弱でなければ、改ざんへの耐性を持つものと考えられる。通信妨害については3.2.4.6節で後述する。メッセージ再送攻撃は、分散台帳技術のP2Pの特質を踏まえ、コンセンサスメカニズムを含めた台帳生成に至る一連のプロセスによって対策がなされているものもある。

ノード間の通信に関わる機能は、管理者の異なる外部環境のノードとの接点であるため、攻撃の起点となりやすい。分散台帳プラットフォームのノード間通信機能に深刻な脆弱性がある場合、ノードを稼働する個々の実行環境で任意の不正なコードを実行できる可能性もある。

3.2.2.7 ノードの認証や認可

ノードの認証や認可の機能はパーミッションド型の分散台帳が備えるものである。分散台帳システムへの接続を認めるノードを制限することや、台帳生成に関わる特権を有したノードを設定する場合に、分散台帳システムへ接続してきたノードが当該ノードであることを認証し、さらに、そのノードが行う操作が許可されたものであることを認可する。認証・認可メカニズムの機能は分散台帳プラットフォームが提供する。実際に、分散台帳システムで認証・認可を実施するためには、許可を行う主体（群）の決定、許可されるノードや操作の権限の決定、ノードの管理者等の確認方法などに関わる規定、その規定自身の決定方法、それらの決定や実施に責任を負う主体（群）の決定などの取り決め（まとめて運用ポリシーと呼ぶことにする）が必要となる。運用ポリシーは分散台帳プラットフォームを導入する分散台帳システムで決定することとなる。

ノードの認証や認可に関わる脅威は、分散台帳プラットフォームが提供する認証・認可メカニズムに関わる脅威と、分散台帳システムが決定する運用ポリシーが適切に実施されない場合の脅威（3.5章参照）がある。

分散台帳プラットフォームが備える認証・認可メカニズムの脅威の発生は、メカニズムの仕様の特性や、メカニズムの設計や実装における不具合、使用する暗号アルゴリズムや鍵サイズ等の強度の低下などに起因する。脅威としては、ノードのなりすまし、不正な操作の認可、与えられていない特権の不正な取得、特定のノードに対する妨害などの可能性が考えられる。

3.2.2.8 暗号アルゴリズムや暗号鍵サイズ

暗号技術は、台帳データの真正性や検証可能性といった分散台帳技術の基本概念を実現するために重要な役割を担っている。分散台帳プラットフォームにより使用する暗号技術や適用方法が異なる。一般的には、以下のような処理で使用されている。

- デジタル署名
  - ・トランザクションへのデジタル署名
  - ・台帳データへのデジタル署名
- （暗号学的）ハッシュ関数
  - ・トランザクションや台帳データの時系列を維持するためのハッシュツリーやチェーン
  - ・トランザクションやウォレットアドレスなどの識別子
  - ・デジタル署名の生成プロセス

上記のほか、プライバシー保護の理由からトランザクション情報の守秘を目的としゼロ知識証明や準同型暗号などを採用する分散台帳プラットフォームもある。

分散台帳プラットフォームにより、使用される暗号アルゴリズム[2]は様々である。デジタル署名として代表的なRSAやECDSA以外にも、Bitcoinが採用したSchnorr署名といったアルゴリズムもある。

暗号アルゴリズムは、その設計に不具合が発見される、実効性のある解読手法が発見される、計算機の飛躍的な性能向上などにより将来において脆弱化することが考えられる。アルゴリズムだけでなく暗号鍵のサイズ（鍵長）が十分な強度[3] を持たない場合にも脆弱化する。
また、選択されたアルゴリズムや鍵長が適切であっても、アルゴリズムの実装が適切でない場合では、その実装に対して攻撃が可能になることも考えられる。これらの理由により、デジタル署名及びハッシュ関数に深刻な脆弱性がある場合には、以下の脅威につながる恐れがある。

- **不正なトランザクションの生成**
- **不正な台帳データの生成**
- **過去の台帳・トランザクションの改ざん（入れ替え）**
  ノードのネットワークの規模や特性にも依存する
- **署名鍵の不正な複製（結果、不正なトランザクション生成につながる）**

守秘を目的とした暗号アルゴリズムや暗号鍵、実装が脆弱な場合、秘匿していたトランザクションの情報が暴かれる脅威につながる可能性がある。台帳に暗号化したデータを保存している場合には、過去のデータに対して脅威に晒されることになる。

安全性が評価された暗号アルゴリズムのリストとして各国の推奨暗号があるが、分散台帳プラットフォームでは、それらのアルゴリズムや鍵長が選択されているとは限らない。安全性の評価が明らかでないアルゴリズムが導入されている場合もある。分散台帳プラットフォームの安全性を評価するためには、選択されている暗号技術の安全性の評価と、その適用方法の安全性の評価が必要となる。

また、アルゴリズムや鍵長、実装が適切であっても、あるノードが持つ暗号鍵（署名鍵）の管理が不適切な場合には、そのノードになりすました不正なトランザクションや台帳データの生成等の脅威につながることになる。分散台帳システムの鍵管理については3.2.4節で記述する。

[2] 楕円曲線暗号においては分散台帳プラットフォームによって異なる曲線が用いられる場合がある
[3] アルゴリズム（楕円曲線パラメーター等含む）や鍵長を含めた暗号強度の指針としてビットセキュリティがある

3.2.3 分散台帳システムに対する脅威

3.2.3.1 分散台帳システムの考察点

分散台帳システムは分散台帳プラットフォームを実行する各ノードがネットワークを構成し、実際にトランザクションや台帳の処理を行うシステムである。ここでは分散台帳システムに対するセキュリティの脅威や課題を考察する。

- 分散台帳に配置されるスマートコントラクトに対する脅威
- 分散台帳システムと他システムとの接続に関わる脅威
- トランザクション承認と台帳生成に関わる脅威
- 分散台帳システムの支配への脅威

3.2.3.2 分散台帳に配置されるスマートコントラクトに対する脅威

スマートコントラクトは、分散台帳システムを利用するスマートコントラクト開発者によって開発され、分散台帳システムで共有される台帳データに配置される。

スマートコントラクトはビジネスゾーン事業者の責任において開発するケースと、他の開発者が作ったスマートコントラクトを呼び出して利用するケースがある。スマートコントラクトから別のスマートコントラクトの関数を呼び出すこともある。Ethereumのように、スマートコントラクト自身が暗号資産やデジタル資産を保有し管理することができる仕組みもある。スマートコントラクトの脆弱性により、スマートコントラクトの処理を不正に実行することが可能となる場合、最悪の場合には利用者が保有する暗号資産やデジタル資産の不正な移転、スマートコントラクトが保有する暗号資産やデジタル資産の不正な移転が可能となる恐れもある。

個々のスマートコントラクトの脆弱性だけでなく、スマートコントラクトで構築されたサービスの仕様に基づいた攻撃もありえる。

3.2.3.3 分散台帳システムと他システムとの接続に関わる脅威

分散台帳システムと別のシステムとの接続インターフェースとして、以下の2つを想定する。

- 相互システムインターフェース – 2つ以上の分散台帳システム間が直接接続するインターフェース
- 外部インターフェース – 分散台帳システムと外部の非分散台帳システム間の接続

相互システムインターフェースは別の分散台帳システムや、複数の分散台帳システムとの接続を仲介するブリッジとなる分散台帳システムとの接続を行う。

外部インターフェースは既存の中央管理型のシステムやDLTオラクル（本節下部の補足説明を参照）など非分散台帳技術によるシステムとの接続を行う。

これらのインターフェースに関わる機能に障害が発生する場合には、他システムとの接続が途絶え、分散台帳システムで実行する処理の停滞や停止につながる。また、インターフェース機能を提供するシステムへの悪意ある者の侵入やマルウェア感染によってインターフェース機能が乗っ取られた場合には、インターフェースに接続する分散台帳システム、他システムに対して意図しない不正な操作が実行されることや、不正な権限昇格が行われる危険性がある。インターフェースがネットワーク経由でアクセス可能な場合には、「3.2.2.6 ノード間通信」と同様の脅威の可能性がある。

各種インターフェースを通じて接続する他のシステムの安全性が、接続する分散台帳システムの安全性にも影響を与える。特にスマートコントラクトにより自動化され、他のシステムの動作が分散台帳システムの重要性の高い処理に連動する場合には、より慎重に評価を行うことが重要となる。分散台帳システムの動作に不具合がある場合には、接続するシステムやアプリケーションの機能停止や停滞、不正な処理の実行などの悪影響を及ぼす可能性があり、また、逆に接続するシステムやアプリケーションの不具合が分散台帳システムの動作に悪影響を与える恐れがある。

DeFiのように分散台帳システムが実行するスマートコントラクトで提供されるサービス間が連動する場合、そのサービス間の仕様の隙をついた攻撃（例：フラッシュローン攻撃）も存在する。

DLTオラクルの補足説明

DLTオラクルとは分散台帳システム外部の情報源から情報を取得して分散台帳システムに提供したり、分散台帳システムで発生するイベントに応じて処理を実行する機能を有するシステムである。分散台帳技術は各ノードでスマートコントラクトの処理を再現し検証可能にするため、一般的な分散台帳プラットフォームでは決定的な（Deterministic）スマートコントラクト[4]のみを実行可能にするという制約がある。この制約により、各ノードがスマートコントラクトの処理を行う際に、入力値以外の値を内部で発生（例えば乱数）させたり、各ノードが処理の過程で個別に外部リソースから取得した情報（取得時により変化する）に基づいて処理を行うといったことはできない。DLTオラクルはこの制約を補足するもので、分散台帳システムの外部システムより分散台帳システムのスマートコントラクトの実行に必要な外部リソースの情報を提供する。分散台帳システムの各ノードはDLTオラクルから入力された値に基づいてスマートコントラクトを実行することができる。DLTオラクルは特定の管理者によって運営されるシステムとして稼働するもの、特定の事業者のサービスとして提供するもの、複数の管理者による分散型システムなどの形態がある。

[4] 入力値が同じであれば必ず処理結果は同じになる処理。

3.2.3.4 トランザクション承認と台帳生成に関わる脅威

トランザクションの検証を行い、その結果に基づき台帳生成を行うノードはトランザクションの承認プロセスにおいて重要な役割を担う。これらのノードのソフトウェアに不具合がある、悪意ある者から攻撃を受ける、運用に障害がある等の理由により、トランザクションの承認や台帳生成に問題が発生することも考えられる。分散台帳技術では、コンセンサスメカニズムによって、あるノードに障害が発生した場合でも、他のノード群の働きによってその障害の影響を削減できるように設計されている。しかし、台帳生成や承認の役割を担うノードの数や配置によって、コンセンサスメカニズムの効果を適切に発揮できない場合もある。例えば、それらのノードが複数あっても、実質的に一か所に配置されているならば、その環境が攻撃を受けた場合、そこに配置されたすべてのノードが同じ脅威に晒される可能性がある。

3.2.3.5 分散台帳システムの支配への脅威

コンセンサスアルゴリズムの仕様上の特性を利用して、特定の利用者グループが分散台帳システムでの支配的な立場を取り、優位にふるまう可能性や台帳データの生成やトランザクションデータの検証が一部の利用者に都合の良い形で実施され、他の利用者のトランザクションやスマートコントラクトが実行されない、実行が停滞する等の影響を与える可能性がある。

分散台帳システムの維持のため、コンセンサスアルゴリズムに暗号資産獲得のインセンティブが与えられているメカニズムの場合、暗号資産の価値の低下が分散台帳システム参加への動機を低下させ、その結果、攻撃者が分散台帳システムの支配をより容易にする可能性がある。また、逆に、特定の利用者グループによる分散台帳システムの支配的な影響から、その分散台帳が提供する暗号資産の価値をより低下させることも考えられる。

3.2.4 分散台帳システムに接続するビジネスゾーンのシステムの脅威

3.2.4.1 ビジネスゾーンのシステムの考察点

ここでは分散台帳システムと接続するビジネスゾーンのシステムを対象に、モデル1～モデル3で共通のセキュリティの脅威や課題について考察する。以下の項目を含む。

- 分散台帳ノードの実行環境に対する脅威
- 分散台帳ノードにおける鍵管理に対する脅威
- 分散台帳アプリケーションとの接続に関する脅威
- 分散台帳プラットフォームの仕様変更に伴う台帳の不整合
- 分散台帳システムに対するDoS(Denial of Service)の脅威

3.2.4.2 分散台帳ノードの実行環境に対する脅威

分散台帳システムを構成する各ノードを実行するデバイス等の環境に悪意ある者が侵入する、または、マルウェアに感染することにより、ノードの機能の不正な実行、停止、不正な設定変更が行われる恐れがある。ノードが管理する署名鍵に対する不正アクセスや流出、署名処理前のトランザクションやスマートコントラクトに対する改ざん、トランザクションや台帳の検証などノードの機能の無効化、他のノードへのメッセージ転送の妨害、不正なメッセージ送信などに繋がる。特定のノードの異常な動作が分散台帳システム全体へ及ぼす影響はノードのネットワークの規模や、分散台帳システムにおけるそのノード役割の重要性に関わる。ノードが分散台帳システムにおいて重要な検証ノードとして大きな役割を占めている場合には、影響はより大きなものとなる。

実行環境のマルウェア感染は分散台帳システムに対する脅威だけでなく、任意のコード実行によるデバイス自身の不正なコントロールを可能にする恐れがあり、ネットワーク上の他のデバイスやシステムへの攻撃に利用されることに繋がる。

外部からの悪意ある攻撃者だけでなく、ノードを管理する組織内の内部不正によるノードの不正利用にも留意する必要がある。

3.2.4.3 分散台帳ノードにおける鍵管理に対する脅威

分散台帳システムの各ノードはトランザクションや台帳データに対するデジタル署名を生成するための署名鍵の管理が必要となる。トランザクション生成に用いる署名鍵はデジタル資産を移転するために必要であり、分散台帳システムに参加する多くのノードがそれぞれの署名鍵を管理する。また、台帳データ生成に用いる署名鍵は台帳データの真正性を担保するために重要であり、台帳データ生成の役割を担うノードがそれぞれの署名鍵を管理する。

署名鍵へ不正アクセスされた場合、悪意ある者によって不正なトランザクションや不正な台帳データが生成される恐れがある。また、署名鍵のネットワークを通じた漏洩や、署名鍵の格納された物理的な媒体の盗難は、分散台帳システムのネットワーク上にある別のノードから、その署名鍵を利用することを可能にする。したがって、署名鍵の漏洩や盗難によって起こりうる被害は、攻撃されたノードの機能停止では防ぐことができない。

一般的な分散台帳システム（特にパブリックパーミッションレス型）では不正なトランザクションが発覚しても、トランザクションが台帳上で承認された後に、システム上で取引を巻き戻したり失効することができないため、署名鍵への不正アクセスや漏洩、盗難の脅威による影響は大きなものとなる。

外部からの悪意ある攻撃者だけでなく、署名鍵を管理する組織内の内部不正による不正利用や漏洩、盗難にも留意する必要がある。

3.2.4.4 分散台帳アプリケーションとの接続に関する脅威

分散台帳アプリケーションとの接続インターフェースとして、以下の2つを想定する。

- ユーザーインターフェース
  ユーザーアプリケーションと分散台帳システム間の接続
- 管理用インターフェース
  管理者用アプリケーションと分散台帳システム間の接続

ユーザーインターフェースは分散台帳システムとユーザーの仲介役となる。例えば、分散台帳システムで扱うデジタル資産の取引操作や、デジタル署名の鍵を管理しトランザクションの生成処理の機能をもつユーザーアプリケーションとの接続を行う。ユーザーアプリケーションにはデスクトップやWeb、モバイルのアプリケーション、コンソールのコマンドラインツールなどの形態がある。
管理用インターフェースはノードの管理のための操作を提供する。ノードの設定、起動、停止、他のノードとの接続や分散台帳データの管理のための機能を提供することが考えられる。

これらのインターフェースに関わる機能に障害が発生する場合には、アプリケーションとの接続が途絶え、分散台帳システムで実行する処理の停滞や停止につながる。また、インターフェース機能を提供するシステムへの悪意ある者の侵入やマルウェア感染によってインターフェース機能が乗っ取られた場合には、インターフェースに接続する分散台帳システム、アプリケーションに対して意図しない不正な操作が実行されことや、不正な権限昇格が行われる危険性がある。インターフェースがネットワーク経由でアクセス可能な場合には、「3.2.2.6 ノード間通信」と同様の脅威の可能性がある。

インターフェースだけでなく接続するアプリケーション自身の不具合や脆弱性によって上記と同様の脅威に繋がる可能性がある。管理用アプリケーションとインターフェースは分散台帳システムやノードに対する特権的な操作が可能であるため、特に注意が必要となる。

3.2.4.5 分散台帳プラットフォームの仕様変更に伴う台帳の不整合

分散台帳プラットフォームの仕様変更において、分散台帳システムに接続する全てのノードやアプリケーションの更新が必要となるハードフォークは注意が必要である。ハードフォークに伴う台帳の分岐（スプリット）が発生するため、更新を行わない場合には古い台帳データのまま取り残され、正しくトランザクションを処理することができなくなる。仕様変更への対応について自己責任を負うパブリックパーミッションレス型の分散台帳では特に注意が必要となる。

3.2.4.6 分散台帳システムに対するDoS（Denial of Service）の脅威

分散台帳システムに接続するノードやシステム、アプリケーションから、特定のノードに対して、その処理能力を超える大量のリクエスト等の通信を発生させることで、特定のノードの正常な処理を妨げる。ビジネスゾーンのシステムが管理するノードが攻撃対象となった場合、ビジネスゾーンのシステムのサービスの正常な実施が妨害される。さらに、他ノードからの正常な台帳データ受信が妨げられることで、攻撃対象ノードで意図的な台帳の分岐（チェーンのスプリット）が発生する可能性や、デジタル資産の二重使用攻撃が可能になる等の脅威に繋がる恐れがある。DoSはTCP/IPなどの通信層のレベルで行われるものと、その上位で実装される分散台帳プロトコルのレベルで行われるものが考えられる。

3.3　想定システムモデル１（パブリックパーミッションレス・カストディアルウォレット型）に関するセキュリティ課題

システムモデル1はデジタル資産の移転に必要な署名鍵の管理をビジネスゾーンのシステムで行う。このモデルでは、ビジネスゾーンのシステムにおいて、デジタル資産に対する権利を持つエンドユーザーとデジタル資産（署名鍵）、デジタル通貨プラットフォームのアカウントの対応関係を管理することが重要となる。これらの管理について以下の課題が含まれる。

- **エンドユーザーの身元確認(Identity Proofing)と当人認証(Authentication)**

  エンドユーザーのなりすましの防止や、正常なサービスの提供、犯罪収益移転の防止など社会的な責任などの目的から、サービス提供にあたって適切なエンドユーザーの身元確認を行い、エンドユーザーに適切な認証手段を提供することが必要となる。デジタル資産に関連するサービス機能提供時の認証プロセスにおいて、その認証手段の強度が不十分な場合や脆弱性がある場合には、エンドユーザーのなりすましや不正な権限昇格などの脅威につながる可能性がある。

- **ビジネスゾーンのシステム全体のセキュリティ課題**

  一般的なシステムと同様に、ビジネスゾーンのシステム全体においてサイバー攻撃、システムを稼働するデバイスや施設に対する物理的攻撃、内部不正の脅威へ備える必要がある。モデル1におけるビジネスゾーンのシステムには特に以下に示す課題が含まれる。

  ○ 導入する分散台帳プラットフォームや接続する分散台帳システムに対する脅威

  3.2節で示したような分散台帳プラットフォームの不具合や脆弱性、分散台帳システムのインシデントがもたらす脅威に備える必要がある。ビジネスゾーン事業者からは直接コントロールできない、パブリックパーミッションレス型の分散台帳システムがもたらす脅威に備える必要がある。

  ○ デジタル通貨に関する署名鍵

  デジタル通貨プラットフォームに接続するための署名鍵の不正利用、漏洩、盗難によってデジタル通貨の不正な送金が行われる恐れがある。デジタル通貨プラットフォームには不正利用対策の仕組みが備わっているが、その対策を有効に働かせるために各ビジネスゾーンのシステムでの適切な署名鍵管理が必要となる。デジタル通貨プラットフォームに関わる署名鍵の管理については後述する「4.4.3分散台帳ノードの鍵管理」でも言及している。

  ○ デジタル資産に関する署名鍵

  デジタル資産に関する署名鍵の不正利用や漏洩、盗難は、署名鍵に紐づくデジタル資産の価値が大きいほど大きな損害をもたらすことになる。エンドユーザーやビジネスゾーン事業者が権利を有するデジタル資産の署名鍵について3.2.4節に示した脅威に備え、適切な鍵管理を行う必要がある。

  ○ デジタル資産とエンドユーザーの管理

  エンドユーザーのデジタル資産の権利を保護するため、エンドユーザーとデジタル資産の対応を適切に管理する必要がある。不適切な運用、操作ミス、外部からの攻撃、内部の不正などの理由により、この対応関係の管理に不整合が生じた場合には、エンドユーザーの資産が失われることになる。

3.4　想定システムモデル2（パブリックパーミッションレス・ノンカストディアルウォレット型）に関するセキュリティ課題

システムモデル2はエンドユーザーが自身で準備するデジタル資産ウォレットと、デジタル通貨プラットフォームが管理するデジタル通貨が連携するモデルである。このモデルはデジタル資産ウォレットが管理するデジタル資産とデジタル通貨の間の取引の整合性を維持することが重要となる。以下の課題が含まれる。

- **デジタル資産ウォレットのリスク**

  デジタル資産を管理するウォレットの形態は、デスクトップソフトウェア、モバイルアプリケーション、第三者が署名鍵を管理するサービス、ハードウェアなど様々である。デジタル資産ウォレットに重大な脆弱性がある場合には、エンドユーザーのデジタル資産の喪失につながる可能性がある。
  さらに、デジタル資産ウォレットを通じてデジタル通貨の送金が行われる場合には、デジタル通貨の被害に及ぶ可能性がある。デジタル資産ウォレットはデジタル通貨プラットフォームに関与しないサードパーティによって提供されるため、直接品質をコントロールすることは困難である。

- **エンドユーザーの身元確認(Identity Proofing)と当人認証(Authentication)**

  3.3節のモデル1の場合と同様に、サービス提供にあたって適切なエンドユーザーの身元確認を行い、エンドユーザーに適切な認証手段を提供することが必要となる。サードパーティが提供するデジタル資産ウォレットの認証手段を利用する場合には、その認証手段の安全性について留意する必要がある。

- **デジタル資産ウォレットとユーザーアカウントのバインディング**

  デジタル資産ウォレットを持つ正当なユーザーであることを確認し、ビジネスゾーンのシステムのサービスアカウント、デジタル通貨のアカウントと紐づけて管理する必要がある。このバインディングのプロセスに脆弱性がある場合には、不正なデジタル資産ウォレットや不正なユーザーとの紐づけを許し、デジタル資産の喪失、デジタル資産の不正な取引（監視を迂回した犯罪収益移転など）、デジタル通貨の不正な送金に繋がる恐れがある。

- **デジタル資産ウォレットの移行**

  デジタル資産ウォレットを別の形態のウォレットに移行することや、デジタル資産ウォレットが稼働するデバイスを別のデバイスに移行することがある。この移行のプロセスに脆弱性がある場合、デジタル資産ウォレットが意図しない別のユーザーやデバイスとバインディングされてしまい、結果としてデジタル資産の喪失やデジタル通貨の不正な送金の被害につながる可能性がある。

3.4　想定システムモデル2（パブリックパーミッションレス・ノンカストディアルウォレット型）に関するセキュリティ課題

● デジタル資産の移転操作

このモデルのフローの例では、エンドユーザー間のデジタル資産の移転の仲介を分散台帳システムに配置されたスマートコントラクトを用いて実行している。スマートコントラクトが脆弱な場合には、デジタル資産に対して不正な操作が行われ、深刻な場合にはスマートコントラクトが管理するデジタル資産の漏洩や喪失に繋がる場合がある。

この例とは異なる方法でスマートコントラクトを使用しない場合には、ビジネスゾーンのシステムでデジタル資産の移転とデジタル通貨の支払いの整合性を維持する仕組みを構築することになる。エンドユーザーがデジタル資産ウォレットを用いて分散台帳システムで実行するデジタル資産の移転処理と、デジタル通貨ウォレットを使用して実行されるデジタル通貨の送金の整合性を維持する必要がある。両者の処理に不整合が生じた場合には、デジタル資産やデジタル通貨の損失に繋がる。このプロセスが脆弱な場合、攻撃者によるデジタル資産やデジタル通貨の窃取の脅威に繋がる可能性がある。

● デジタル資産取引の監視

デジタル資産の移転はエンドユーザー自身の手によって行われるが、取引の仲介を行うビジネスゾーン事業者にも一連の取引に関する一定の責任を担うことになる。犯罪収益移転防止等の社会的な責任の観点から、デジタル資産の移転の監視が必要とされうる。

● ビジネスゾーンのシステム全体のセキュリティ課題

一般的なシステムと同様に、ビジネスゾーンのシステム全体においてサイバー攻撃、システムを稼働するデバイスや施設に対する物理的攻撃、内部不正の脅威へ備える必要がある。モデル2におけるビジネスゾーンのシステムには特に以下に示す課題が含まれる。

○ デジタル通貨に関する署名鍵

モデル1と同様にデジタル通貨プラットフォームに接続するための署名鍵を適切に管理する必要がある。デジタル通貨プラットフォームに関わる署名鍵の管理については後述する「4.4.3分散台帳ノードの鍵管理」でも言及している。

○ デジタル資産情報とエンドユーザーの管理

エンドユーザーの情報と、エンドユーザーが管理するデジタル資産の内容に関する情報を管理する。不適切な運用、操作ミス、外部からの攻撃、内部の不正などの理由により、この対応関係の管理に不整合が生じた場合には、デジタル資産の取引を適切に実行することができず、エンドユーザーとビジネスゾーン事業者に損害を与えることになる。

3.5　想定システムモデル3（プライベートパーミッションド）に関するセキュリティ課題

モデル3はデジタル資産の移転に必要な署名鍵の管理をビジネスゾーンのシステムで行う。このモデルはビジネスゾーンのシステムにおいてデジタル資産に対する権利を持つエンドユーザーとデジタル資産（署名鍵）を管理する点でモデル1と類似しており多く共通点があるが、デジタル資産を管理する分散台帳がプライベートパーミッションド型であるために前提が異なる部分がある。モデル3には以下の課題が含まれる。

- **エンドユーザーの身元確認(Identity Proofing)と当人認証(Authentication)**

  モデル1と同様にサービス実施のためのエンドユーザーの身元確認と認証手段の提供において、なりすましや不正な権限昇格などの脅威が存在する。

- **ビジネスゾーンのシステム全体のセキュリティ課題**

  一般的なシステムと同様に、ビジネスゾーンのシステム全体においてサイバー攻撃、システムを稼働するデバイスや施設に対する物理的攻撃、内部不正の脅威へ備える必要がある。モデル3におけるビジネスゾーンのシステムには特に以下に示す課題が含まれる。

  ○ 導入する分散台帳プラットフォームや接続する分散台帳システムに対する脅威

  3.2節で示したような分散台帳プラットフォームの不具合や脆弱性、分散台帳システムのインシデントがもたらす脅威に備える必要がある。プライベートパーミッションド型の分散台帳では台帳生成やトランザクションの承認に変わる特権を持ったノード（特権ノード）をあらかじめ決定して運用することが考えられる。分散台帳プラットフォームもそのような運用を前提にして設計されている場合があり、パブリックパーミッションレス型に比べ特定のノードの責任がより大きくなる傾向がある。複数の特権ノードが適切に分散配置され、それぞれが適切に運用されることが必要となる。

  ○ デジタル通貨に関する署名鍵

  モデル1と同様にデジタル通貨プラットフォームに接続するための署名鍵を適切に管理する必要がある。デジタル通貨プラットフォームに関わる署名鍵の管理については「セキュリティ検討報告書 【鍵管理】」（デジタル通貨フォーラム）を参照のこと。

  ○ デジタル資産に関する署名鍵

  デジタル資産に関する署名鍵の不正利用や漏洩、盗難は、署名鍵に紐づくデジタル資産の価値が大きいほど大きな損害をもたらすことになる。また、ビジネスゾーンのシステムが分散台帳システムへ接続するための認証や認可のための署名鍵、および、台帳生成やトランザクション承認に関わる特権ノードの役割を担う場合にはその操作に必要な署名鍵について厳重な管理が必要となる。署名鍵の不正利用、漏洩、盗難は不正な台帳の利用や、不正な台帳生成、不正なトランザクション承認につながり、分散台帳システム全体に影響を与える。

  ○ デジタル資産とエンドユーザーの管理

  エンドユーザーのデジタル資産の権利を保護するため、エンドユーザーとデジタル資産の対応を適切に管理する必要がある。不適切な運用、操作ミス、外部からの攻撃、内部の不正などの理由により、この対応関係の管理に不整合が生じた場合には、エンドユーザーの資産が失われることになる。

- **分散台帳システムの接続に関わる審査**

  プライベートパーミッションド型の分散台帳システムは接続するノードやシステム、アプリケーション、ユーザーなどに対して認証や認可を必要とする。認証や認可を行う前提として、接続するシステムや管理主体等に対して事前審査を行うことが考えられる。審査基準や実施方法に対して不備がある場合、不適切なシステムやアプリケーションとの接続や、不正なユーザーからの接続を許し、その結果、分散台帳システムへの不正操作や台帳データの汚染などの脅威に繋がる可能性がある。

第4章

セキュリティ課題への対応

04

CONTENTS

第4章

セキュリティ課題への対応

4.1 本章について

本章では3章で述べたセキュリティ課題に対して、考えられる対策や緩和策、対応方針について考察する。

4.2 分散台帳プラットフォームや分散台帳システムに対する課題への対応

分散台帳プラットフォームや分散台帳システムの安全性については以下の観点での評価がある。

- **分散台帳プラットフォームの設計・仕様に対する評価**
- **分散台帳プラットフォームの実装に対する評価**
- **分散台帳システムに対する評価**

分散台帳プラットフォームの設計・仕様、実装、分散台帳システムに対する評価は後述するように現状では非常に困難であり、特にビジネスゾーン事業者が個別に行うことは現実的ではない。評価が困難であることを前提にリスクを緩和することが必要となる。

分散台帳プラットフォームに対するセキュリティの評価は分散台帳プラットフォームの機能や要素、それらの組み合わせに対する安全性の評価が必要となる。

3.2.2.1節で述べたように、コンセンサスメカニズム、トランザクションの生成と検証の方法、スマートコントラクトの生成・配置方法、ノード間通信、ノードの認証や認可、暗号アルゴリズムといった機能や要素が含まれる。分散台帳プラットフォームはそれぞれ独自のコンセンサスメカニズムを採用したり、異なる暗号アルゴリズムなどを採用しており、各分散台帳プラットフォームに応じた評価が必要となる。コンセンサスメカニズムは、台帳が各ノードで一意となるために、ノード間での協調や競争を促すために報酬等のインセンティブと共に機能するものもあるため、インセンティブの設計も含めて評価が必要になる場合がある。コンセンサスメカニズムを含め分散台帳プラットフォームの基盤となる様々なメカニズムは学術界で安全性について評価されているとは限らない。また、分散台帳プラットフォームは複数の技術要素で構成されており、その実装も複雑になりえる。

分散台帳プラットフォームが提供する機能も多様であるため、分散台帳の分野における評価基準に統一的なものは現状無い。個別の分散台帳プラットフォームの実装コードに対する評価が必要となる。仕様変更の頻度の高い分散台帳プラットフォームもあることも、評価を難しくする要因である。

分散台帳プラットフォームが理論的に安全性の評価がされていても、そのプラットフォームを用いて実際に稼働しているシステムが安全であるとは限らない。3.2.3節や3.2.4節で述べたように分散台帳プラットフォームが前提とするノードの数や配置、署名鍵管理が期待通りでない場合には、その分散台帳システムの安全性が脅かされることになる。

特にパブリックパーミッションレス型の分散台帳に見られるように、実際のネットワークの構成を把握することが難しいことがあり、実態が分散台帳プラットフォームの設計時の想定と異なっていることも考えられる。実際の分散台帳システムの状況や発生する事案についても把握していくことが必要となる。

Bitcoinのように、そのシステムで発行される暗号資産の価値が分散台帳システムの安全性の維持に影響を与えることもあるケースでは、暗号資産の価値と台帳生成を担うノードの動向についても注意を払う必要がある。

プライベートパーミッションド型の分散台帳については接続されるノードが限定され、ノードの運用について一定の統制が可能であり、また、それを前提とした分散台帳プラットフォームのアーキテクチャが設計されている。上述した分散台帳プラットフォームの設計、仕様、実装の安全性と共に、分散台帳システムを構成するノード、特に台帳生成やトランザクション承認に関わるノードの数や配置、管理主体、管理運用方法について注意する必要がある。プライベートパーミッションド型の留意点は4.7節で扱っている。

4.2 分散台帳プラットフォームや分散台帳システムに対する課題への対応

分散台帳プラットフォームの設計・仕様、実装、分散台帳システムに対して安全性が評価されることは理想的であるものの、現実的には分散台帳プラットフォームで横断的で統一的な基準がなく、個別の分散台帳プラットフォームや分散台帳システムに対しても個別の機能要素ではなく全体としての安全性を評価することも難しい状況にある。学術界と分散台帳に関わる産業界、標準化団体等が連携し知見を高めることで、将来的に評価方法が確立されることが期待される。

その一方で、ビジネスゾーン事業者としては、分散台帳プラットフォームや分散台帳システムが抱えるリスクを想定し、以下の観点を含んだ緩和策を検討し、事案が発生した場合の対処を可能にしておくことが考えられる。

- **分散台帳プラットフォームや分散台帳システムに関する情報の収集、評価**

  分散台帳プラットフォームや分散台帳システムに関する情報を収集し、技術の特性、扱われるデジタル資産の特性、想定される脅威などについて理解する。また、分散台帳プラットフォームを導入する際には、分散台帳プラットフォーム、レイヤー2ソフトウェアやウォレットなどの実装について評価が伴うことが考えられる。この評価には第三者によるソースコード監査等を利用することも考えられる。

- **分散台帳プラットフォームの開発コミュニティに関する情報の収集**

  開発コミュニティの構成、仕様変更等の意思決定方法や関与の仕方、他のコミュニティとの関係を理解する。場合によっては、分散台帳プラットフォームの仕様変更に対して影響力を持つ開発者や運用者、ガバナンストークン保有者の存在や、その動向についても留意する必要がある。

- **分散台帳プラットフォームや分散台帳システムの最新動向の把握**

  仕様変更、不具合修正、脆弱性修正や大規模な移行計画などを把握し、ビジネスゾーンのシステムでの対応方法について検討する。分散台帳システムに接続するウォレットやアプリケーション、システムへの影響、分散台帳システムで稼働するスマートコントラクトへの影響も考慮する。

- **分散台帳システムの監視**

  実際に稼働している分散台帳システムの状態を監視し、異常を発見した場合には問題の分析や対処を行う。特定のノードの異常が想定される場合には、接続先の異なる複数のノードで監視を行うことも考えられる。

- **分散台帳ノードのアップデート**

  分散台帳プラットフォームの仕様変更や不具合修正、脆弱性修正のためのアップデートが行われる場合、そのアップデート内容の必要性に応じて、ノードのアップデートを検討し実施する。

- **対応体制の構築、対応策の検討と実施**

  上記の観点を含んだ分散台帳の問題に関わる対応体制を構築し、様々なリスクに対する対処法を検討する。分散台帳システムに異常が発生した場合の対応（脅威に応じた対応）、大規模な移行を行う場合の対応などが含まれる。具体的な対処方法を検討する場合には、分散台帳システムへの知識を有するエキスパートの関与が必要となる。

4.3 ビジネスゾーンのシステムの開発

4.3.1 基本方針

ビジネスゾーンのシステムは従来と同様のシステム開発に加え、スマートコントラクトや分散台帳アプリケーションの開発が必要となる。ビジネスゾーンのシステムの開発においては、採用する分散台帳プラットフォームや分散台帳システムの特性と、ビジネスゾーンのシステムにおいて想定される脅威（参考：3.2節）を踏まえた安全な設計と開発を行う必要がある。スマートコントラクトのリスク軽減については次節で基本的な考え方を述べる。

4.3.2 スマートコントラクトのリスク軽減

スマートコントラクトは一般的なソフトウェアと同様に、設計、仕様レビュー、セキュアコーディング、コードレビュー、テスト設計、テスト実施といった入念な工程が必要となる。

スマートコントラクト設計では、各関数を実行可能な権限を入念に検討する必要がある。スマートコントラクトでは一般的なプログラミング言語にスマートコントラクト特有の制約を設けたり、スマートコントラクト専用の言語を導入していることがある。スマートコントラクトの設計、レビュー、コーディング、テスト設計においては分散台帳プラットフォームが採用しているスマートコントラクトの言語仕様に対する知識が必要となる。スマートコントラクトの開発者コミュニティに参加することも知識を獲得するための有効な方法と考えられる。開発者の多いスマートコントラクト開発言語では、脆弱性のまとめやセキュアプログラミングにおいて留意すべき事項、脆弱性検査ツールなどが提供されているものもあり、それらの情報を参考にすることもできる。

レビューについては知識と経験が豊富な第三者によるスマートコントラクト監査や脆弱性診断を利用することも考えられる。第三者によって提供されているスマートコントラクトを利用する場合も、可能な限り、その仕様やコードのレビューを実施することが望ましい。

スマートコントラクトを実行するバーチャルマシンの環境は脆弱性対応を含んだアップデートが行われることがある。古いスマートコントラクトのコードはアップデートされたバーチャルマシンでは稼働しないこともある。古いコードが稼働しないことからバーチャルマシンをアップデートせず、脆弱性を含んだ古いコードを再利用することでセキュリティの問題が内在してしまうことも考えられる。新規の開発においては最新のバーチャルマシンの使用と共に、脆弱性対応された関数の使用を行う。また、スマートコントラクトの保守においては、バーチャルマシンの脆弱性対応のアップデート、それに応じたスマートコントラクトのアップデート、脆弱性を含んだ古いコードの再利用禁止などに注意し実施する。

スマートコントラクトは運用時に発覚した不具合の修正等に対応するため、分散台帳に配置した以降もアップデートできるようにすることが望ましいが、その機能が悪用され第三者による不正な機能修正や操作が行われないように十分に注意する必要がある。

スマートコントラクトは実運用されている分散台帳に配置される前に念入りにテストする必要がある。スマートコントラクトは分散台帳に配置せずにローカルな環境で試行することもできるが、実際に複数のノードで構成された分散台帳システムでテストを行うことも必要となる。スマートコントラクトのテスト環境としては、開発用として公開されているテストネットや自身で構築したプライベートの分散台帳を利用することが考えられる。

また、万一、スマートコントラクトの不具合が発生した場合に備え、不具合が発生した場合の運用上の対応や保険等などのリスク軽減策やリスク移転策を検討しておくことが望ましい。

4.4.1 情報セキュリティマネジメント

ビジネスゾーンのシステムはISO 27001やISO 27002に代表されるような一般的な情報セキュリティマネジメントに加え、4.2節で示したような分散台帳に特有のリスクに対応したセキュリティ体制を構築し実施することが考えられる。

分散台帳プラットフォームや分散台帳システムの特性や想定される脅威を踏まえ、ビジネスゾーンのシステムに対するリスク評価を行う。4.2節で示したような分散台帳に関わる対応を想定し、ビジネスゾーンのシステムのセキュリティに関わる全体の体制の構築とセキュリティ指針の策定、適切なアクセスコントロールの設計と実施、ネットワークやシステムの監視、インシデント対応、脆弱性対応等に対する体制の構築や対策の実施をする。

2章のシステムモデルは例としてNFTを挙げているが、ビジネスゾーンのシステムは別のデジタル資産を扱うこともありえる。デジタル資産の性質により、ビジネスゾーン事業者は法令の遵守が必要となる場合がある。法令や業界でシステムに対するセキュリティ基準が定められている場合には、ビジネスゾーンのシステムもその基準に準拠する必要がある。

4.4.2 分散台帳ノードに関するセキュリティ対策

ビジネスゾーンのシステムの他の要素と同様に、分散台帳ノードの実行環境について不正アクセスやマルウェア等のサイバーセキュリティ対策を行う。特に分散台帳ノードは外部のノードへ接続するため、外部からの攻撃に晒されやすいため、ビジネスゾーンのシステムの基幹との分離やネットワークの監視と異常の検知が必要となる。

また、分散台帳ノードの環境で操作可能な機能を必要最小限にする。分散台帳を参照するノードとトランザクション送信を行うノードの環境を分離することも考えられる。

また、ビジネスゾーンで管理しているブロックチェーンノードや外部のブロックチェーンノードが正常に稼働しているか確認することも必要となる。例えば、ブロックが生成されていることの確認、Mempoolが更新していることの確認などがある。DoS対策も含め、ノードの環境からの接続先を限定する等によって不必要な通信を遮断する。署名対象外のメッセージへの改ざん、盗聴や不正なノードへの接続等の対策として、ノード間でTLS（Transport Layer Security）に代表されるセキュアな通信が適用可能な場合にはその設定を行う。

分散台帳の整合性の維持や特定のノードの不具合等のリスクを軽減するために、異なるネットワークにある複数のノードで分散台帳を監視することも考えられる。

ビジネスゾーンのシステムにおいて、分散台帳システムと他のシステム（DLTオラクルや非分散台帳システムを含む）やアプリケーションと接続し連携する場合には、システムやアプリケーション間の双方で実行可能な操作や送信されるメッセージ、操作やメッセージ送信に必要な権限、認証や認証などの機構が適切に設計され実施されることが必要となる。また、必要に応じてDLTオラクル等の接続先のシステムに関する評価や監査を実施する。

4.4.3 分散台帳ノードの鍵管理

分散台帳ノードはトランザクションの生成のための署名鍵を管理する必要がある。さらに、分散台帳システムにおけるトランザクション承認や分散台帳の生成の役割を担う場合には、それに必要な署名鍵を管理する必要がある。トランザクション承認や分散台帳の生成に必要な署名鍵の不正アクセスや漏洩、盗難は分散台帳システム全体に影響が及ぶため、より留意する必要がある。

分散台帳では、トランザクションに署名を行う署名鍵（トランザクション署名）や、トランザクションや台帳データの承認のための署名を行う署名鍵（ブロック署名）など、異なる性格を持つ署名鍵が存在する。特に、トランザクションや台帳データの承認や、分散台帳システムの設定やスマートコントラクトの設定に関係する特権的な署名鍵が不正使用された場合は、分散台帳システムに関係するユーザーやシステム全体に影響を及ぼす。特権的な署名鍵はより慎重に管理することが求められる。

署名鍵の種類や性質を特定し、その署名鍵のライフサイクルを明確化することが必要である。デジタル資産を管理する分散台帳システムの場合には、署名鍵によって管理されるデジタル資産の価値や額についても考慮する必要がある。署名鍵の性質や扱うデジタル資産の価値によってリスクが異なるため、リスクに応じて要求される鍵管理のレベルを検討することとなる。署名鍵のライフサイクルには、署名鍵の生成、活性化、非活性化、使用停止、廃棄などの状態が含まれる。活性化は署名鍵の保護状態から署名鍵を利用可能な状態へ移行する。非活性化はその逆である。署名鍵のライフサイクルを明確化し、署名鍵の運用方針を検討する場合には、署名鍵に紐づくデジタル資産についても考慮する必要がある。デジタル資産を管理する分散台帳の場合には、新しい署名鍵を生成した場合、その署名鍵へデジタル資産を移動する運用が伴うことがある。また、古い署名鍵を廃棄する場合には、それ以降にその署名鍵へのデジタル資産が移転される可能性も考慮が必要になる場合がある。

署名鍵の性質に応じて署名鍵を管理する署名鍵管理システムを設計する。署名鍵の漏洩や不正アクセスを防ぐため、署名鍵管理システムに適切なアクセスコントロールを実施する。署名鍵管理システムは他のモジュールやシステムに署名鍵のデータ自体に直接アクセスさせることを防止することが望ましい。例えば、署名鍵管理システムは署名鍵を安全に管理し、要求されたデータに対し署名を生成して返却するのみとする。

署名鍵管理システムへ送られるトランザクションデータが不正な場合、署名鍵管理システムはそのトランザクションに対して署名処理を実行してしまうリスクがある。このリスクに対処する場合には、署名鍵管理システムへトランザクションデータが送られる前に、そのデータの妥当性を検証する必要がある。例えば、トランザクションの送付先が事前に登録された送付先（ホワイトリスト）に記されていることを確認する、トランザクションの金額など過去の振る舞いに基づいて異常を検知する等が考えられる。これらのリスク軽減策は署名鍵管理システムとは別に検討する必要がある。

厳格に署名鍵を管理する場合には、評価を受けたハードウェアセキュリティモジュール（HSM）を導入することも考えられる。分散台帳プラットフォームが採用する署名アルゴリズムはFIPS（CMVP）やCommon Criteriaなどの認証の範囲外である場合もある。その場合でも、HSMの署名鍵を保護する機構の考え方は適切な鍵管理を実施するために有効である。署名鍵を含んだモジュールやシステムが物理的なデバイスで稼働する場合には、物理的な破壊や盗難に対する対策も必要となる。物理的に保護されたモジュールや頑強な施設への設置や、入退出管理など物理的なアクセスコントロールの実施を検討する。また、署名鍵管理システムのモジュールや管理用端末に利用者認証等を行う場合には、認証クレデンシャルの管理も厳格に行う必要がある。

4.4.3 分散台帳ノードの鍵管理

署名鍵管理システムに対する運用ポリシーは、署名鍵管理システムを含んだ情報システム全体の情報セキュリティマネージメントの指針とポリシーに基づいて検討される。署名鍵管理システムの運用ポリシーでは、鍵管理体制を構築し、適切な役割と権限を定める。例えば、署名鍵管理に対する責任を負う鍵管理責任者、現場の責任を負う管理者、規定に従い署名鍵管理に関する操作を行う操作者、監査を行う監査者などがある。利害が相反する役割は兼務させないことや、特定の者に権限を集中させないため、適宜担当者を変更することが推奨される。また、特定の重要な操作においては内部不正や運用ミスを防止するため、2名以上の操作者による相互監視や、管理者や責任者による承認を行うことが考えられる。また、鍵に関わる操作のログを記録し、異常の監視や事後の監査を行う。また、異常発生時の報告や対処の方法を事前に規定することも重要である。

運用ポリシーではバックアップとリストア、アーカイブの運用方針も定める。署名鍵の消失に備えて署名鍵のバックアップを行うことが望ましいが、バックアップの管理も上記と同様に厳格な管理が求められる。バックアップデータの盗難や漏洩、不正操作などにより、署名鍵に対する不正が行われないように、バックアップデータの作成や保管、バックアップデータからの復旧（リストア）方法や手順、操作者の権限設定、アクセス制御を適切に定めて実施する。

デジタル資産を管理するための署名鍵については、不正アクセス、漏洩、盗難のリスク軽減や障害時の可用性の確保のために、複数の署名鍵に分け、異なる場所で管理することも考えられる。分散台帳プラットフォームによっては複数の署名鍵によって運用可能なマルチシグなどの機能を備えており、それらを利用することもできる。スマートコントラクトによりマルチシグと同等の機能を実現するものもあるが、スマートコントラクトの場合はその安全性に留意する必要がある。分散台帳プラットフォームやスマートコントラクトでサポートされている機能を用いずに、秘密分散等を用いて署名鍵を複数のシェアに分割することも考えられるが、その場合は採用するアルゴリズムの安全性に留意する。複数の署名鍵で管理を行う場合、管理が不十分で安全性の低い署名鍵が存在する場合には、それが攻撃の対象となりえる。一定数に満たない一部の署名鍵の不正利用は即座にデジタル資産の不正利用に結び付くわけではないが、不正利用された署名鍵と同じ組を構成する署名鍵全体の安全性を下げることとなる。管理の不十分な署名鍵が存在する場合には、複数の署名鍵に分割した効果を適切に発揮できない。それぞれの署名鍵が同等のセキュリティ基準で運用されることが求められる。署名鍵に対する障害に備え、署名鍵のバックアップを行う際にも、バックアップに対しても本運用している署名鍵と同等の基準で管理を行う必要がある。

個々の署名鍵をマスターとなる署名鍵やシードから生成する場合、そのマスターの署名鍵やシードは個々の署名鍵と同等以上の基準で管理を行う。署名鍵以外の守秘等の用途の暗号鍵においても、その鍵の種別やライフサイクルに従い、上記と同様の方針で鍵管理体制を構築し実施する。

署名鍵の操作を監視し、不正利用の疑いに繋がる異常を検知した場合には、新たな署名鍵を生成し、デジタル資産をその署名鍵に対応したアドレスに速やかに移転することが必要となる（特にパブリックパーミッションレス型の分散台帳）。署名鍵を生成する機能を含んだシステムモジュールが攻撃者やマルウェアに制御されている可能性もあるため、新たな署名鍵生成とデジタル資産を移転するトランザクションの生成と送信は汚染の疑いのない環境下で実施することが望ましい。

4.5 モデル１に対するセキュリティ課題の対応

● エンドユーザーの身元確認と当人認証

このモデルのビジネスゾーン事業者はデジタル資産の管理を行うカストディアンとなるため、消費者の保護と犯罪収益移転等の防止のため、エンドユーザーに対し十分な身元確認を行う必要がある。

身元確認の基準については、デジタル資産の性質により、犯罪収益移転防止法の定める要件、業界で定められた基準、一般的な身元確認に関する標準規格としてNIST SP800-63-3 (63A)[5] を参照することが考えられる。身元確認はサービス開始時（オンボーディング）の実施と、取引リスクに応じた継続的な確認（オンゴーイング）を実施する。なお、身元確認においてはエンドユーザーのプライバシー保護のため不必要な情報の取得や保存を避ける。

ビジネスゾーンのシステムが提供するサービスへのログイン、デジタル資産の取引実行[6]などのプロセスにおいてエンドユーザーの当人認証の手段が必要となる。特にデジタル資産の取引実行においては適切な多要素認証の導入など安全性の高い手段が求められる。一般的な当人認証のレベルの基準としてはNIST SP800-63-3 (63B)がある。

● ビジネスゾーンのシステム全体のセキュリティ対策

4.2節から4.4節で述べたように、接続する分散台帳システムの特性を踏まえたビジネスゾーンのシステムのセキュリティマネジメントが必要となる。パブリックパーミッションレス型の分散台帳で発生するインシデントや、脆弱性の発見、仕様変更の動向については常に追従することが重要となる。分散台帳に深刻な問題が発生し、ビジネスゾーンのシステムにその被害が及ぶ可能性がある場合には、その分散台帳システムとの接続を切り離す等の対応も必要となる。

デジタル資産の移転に必要な署名鍵に対する脅威（3.2.4.3）のように、脅威の種類によっては、分散台帳システムとの接続を遮断することでは対処できないものもある。そのようなインシデントの発生に備え、デジタル資産を移転し保護する可能性や実現方法をあらかじめ検討し、対応方法を規定しておくことが必要となる。

また、エンドユーザーのデジタル資産を保護するため、エンドユーザーのデジタル資産や、デジタル資産の移転に必要な署名鍵を適切に分別管理することが考えられる。ビジネスゾーンのシステムで実行される処理や操作に関する記録は、ビジネスゾーンのシステムに対する異常を検知し即座に対応するための目的、事後の監査による異常の発見と原因の特定、セキュリティの強化のための目的があり、それらに適した事項を記録する。

● 取引に関する確認

ビジネスゾーン事業者はデジタル資産の取引が犯罪収益移転等の行為につながるリスクに対処することが求められる。リスクや必要性に応じて、デジタル資産取引の目的、デジタル資産の移転先の情報をエンドユーザーから取得し、記録し、疑わしい取引を検知する。

[5] 現在、SP800-63-4として改訂作業が行われており、ドラフト版が公開されている。
[6] デジタル通貨の決済における認証手段はデジタル通貨プラットフォームが提供するものであるためここでは扱わない。

4.6 モデル2に対するセキュリティ課題の対応

- **ビジネスゾーン事業者が負う責任の範囲の明確化**

エンドユーザーによって制御されるデジタル資産ウォレットの問題によって発生する損害に関してビジネスゾーン事業者が負う責任や保証の範囲を決定し、エンドユーザーに明示する必要がある。損害はビジネスゾーン　事業者が提供するサービス、エンドユーザーのデジタル資産やデジタル通貨を含む。ビジネスゾーンのシステムに技術的に接続可能なデジタル資産ウォレットを提示した場合であっても、エンドユーザーはそれらのウォレットをビジネスゾーン事業者が推奨し安全性を保証するものとして誤認することが考えられる。ビジネスゾーン事業者は自らの責任の範囲において、エンドユーザーが適切にデジタル資産とデジタル通貨を保護するための仕組みや適切なガイダンスを提供することが求められる。

- **エンドユーザーの身元確認と当人認証、ウォレットとのバインディング**

ビジネスゾーン事業者は取引を行う仲介業としての責任を果たすため、モデル１と同様にエンドユーザーに対し十分な身元確認を行う必要がある。身元確認と共に、そのエンドユーザーが当該ウォレットを確かに管理していることを確認し、エンドユーザーの情報とウォレットに関する情報を紐づけて管理することが必要となる。このプロセスでは、そのエンドユーザーが当該ウォレットをコントロールできることを確認することが必要となる。エンドユーザー情報とウォレットのバインディングの実現方法はウォレットの種類によって異なるが、ビジネスゾーンのシステムが提示した情報に対してエンドユーザーが付与したデジタル署名を確認する等のプロセスを含むことになる。このプロセスにおいてエンドユーザーが意図しないトランザクションに署名させられる危険性があるため、実際にデジタル資産の移転が可能な署名鍵をこのプロセスに用いることは望ましくない。

ハードウェアによって署名鍵が厳格に管理されているウォレットは、より高い確度のバインディングを実現できる可能性があるが、それ以外のウォレットではバインディングの過程における脅威やリスクをより慎重に評価する必要がある。

エンドユーザーはウォレットに対する認証や署名生成（署名鍵の活性化）のためのクレデンシャルを管理している。さらに、ビジネスゾーンのシステムが提供するサービスへログインするための認証クレデンシャルを管理することになる場合には、エンドユーザーの管理負担が増すことになる。エンドユーザーの負担軽減のため、ウォレットの認証メカニズムをビジネスゾーンのシステムのサービスの認証手段に用いようとする場合には注意が必要となる。バインディングにおける留意点と同じように、デジタル資産の移転を行う署名鍵を認証手段に用いることは避けるべきである。ウォレットが提供する認証手段の強度が適切であり、その認証手段がトランザクションへの署名とは別に提供されることが必要となる。オンラインのウォレットサービスの認証手段を用いて、ウォレットサービスと認証連携を行うことを検討する場合には、ウォレットサービスのアカウント登録時の身元確認方法と認証手段を含んだトラストフレームワークがビジネスゾーンのシステムのサービスに対して十分なレベルであることが必要となる。

4.6 モデル2に対するセキュリティ課題の対応

● 対応するウォレットの評価

デジタル資産ウォレットの安全性の評価としては以下の観点がある。

○ デジタル資産ウォレットの実装形態（ソフトウェア、ハードウェア、サービス）

○ デジタル資産ウォレットのセキュリティ対策

以下の項目を含む。

- 署名鍵の生成方法
  署名鍵生成のアルゴリズムや、署名鍵生成のための乱数生成方法
- 署名鍵の管理方法
  署名鍵の保存場所、署名鍵に対する操作、署名鍵のインポート/エクスポートの可否と方法、署名鍵のバックアップや複製の可否と方法、暗号化キーが存在する場合の管理方法など
- デジタル資産ウォレット及び署名鍵に対する操作における認証・認可方法
- デジタル資産ウォレットのインターフェースに対するセキュリティ対策
- デジタル資産ウォレットに対する物理的保護
- サービス型のウォレットの場合にはさらに以下を含む。
  - デジタル資産ウォレット提供事業者のセキュリティマネジメント、システムへのサイバー及び物理セキュリティ対策

○ 上記に関する第三者評価を受けている場合にはその評価の範囲上記の例のうち一部の機能や要素のみが評価対象である場合もある。

ビジネスゾーンのシステムに接続可能なデジタル資産ウォレットの安全性をビジネスゾーン事業が事前に評価できることが理想的であるものの、個々のビジネスゾーン事業者が評価することは現実的に難しい場合もある。将来的に業界団体や標準化団体等におけるデジタル資産ウォレットの評価基準が整備され、その基準に基づくデジタル資産ウォレットの安全性評価とその結果の共有がなされることが期待される。

● デジタル資産ウォレットの移行

異なるデジタル資産ウォレットに移行する、デジタル通貨ウォレットがインストールされたデバイスを移行する等のプロセスにおいて、異なるユーザー、デバイス、ウォレットに紐づけがされないように防止策を取る必要がある。ウォレットやデバイスの制約により、移行プロセスにおいて一貫性を維持できない恐れがある場合には、エンドユーザーの身元確認やバインディングのプロセスを再度行うことも考えられる。

4.6 モデル2に対するセキュリティ課題の対応

● ビジネスゾーンのシステム全体のセキュリティ対策

接続する分散台帳システムの特性を踏まえたビジネスゾーンのシステムのセキュリティマネジメントが必要となる。基本的な考え方はモデル1と同様であるが、以下の点に留意が必要となる。

デジタル資産とデジタル通貨による取引の整合性の維持

- デジタル資産の移転はエンドユーザーの制御下にあるデジタル資産ウォレットによって行われるため、デジタル資産を管理する分散台帳を確認し、ビジネスゾーンのシステムで行われるデジタル通貨の取引と矛盾がない状態にすることが求められる。なんらかの理由によりエンドユーザーによるデジタル資産の移転が実施されない場合には、デジタル通貨の送金停止や返金等の措置を行う。分散台帳の巻き戻しも想定し、定期的に分散台帳の情報を確認し、ビジネスゾーンのシステムが管理するデジタル資産情報の整合性を維持する。

● 取引に関する確認

デジタル資産の取引を仲介するビジネスゾーン事業者の社会的責任の観点から、他のモデルと同様に犯罪収益移転等の防止のための措置をとることが求められる。リスクや必要性に応じて、扱うデジタル資産の性質、デジタル資産取引の目的、デジタル資産の移転先の情報をエンドユーザーから取得、記録し、疑わしい取引を検知する。ビジネスゾーン事業者はデジタル資産の移転に関して直接コントロールするものではないが、エンドユーザーのデジタル資産を管理する分散台帳を監視し、ビジネスゾーンのシステムを通じて行われた取引に関して、その取引以降に行われたデジタル資産の移転についても一定期間監視すべきと考えられる。

4.7 モデル3に対するセキュリティ課題の対応

- **エンドユーザーの身元確認と当人認証**

モデル1と同様にビジネスゾーン事業者はデジタル資産の管理を行うカストディアンとなるため、消費者の保護と犯罪収益移転等の防止のため、エンドユーザーに対し十分な身元確認を行う必要がある。デジタル資産の性質によって、法規制で定められた要件、業界で定めた基準、ビジネスゾーン事業者としてのリスクを踏まえ、適切な身元確認と十分な強度を有した認証手段を提供する必要がある。

- **ビジネスゾーンのシステム全体のセキュリティ対策**

モデル1の場合と同様に接続する分散台帳システムの特性を踏まえたビジネスゾーンのシステムのセキュリティマネジメントが必要となる。基本的な考え方はプライベートパーミッションド型の分散台帳では、そのメカニズムを効果的に適用するために、各ノードが一定のセキュリティ基準を満たして運用されていることが期待される。ノードの稼働環境に対するセキュリティ対策と共にノードにあるデータの適切なバックアップを行う。台帳の閲覧やトランザクションの送信を行う一般的なノード（一般ノード）は少なくとも分散台帳システムに対する不正アクセスを防止する責任を負う。トランザクション承認や台帳生成の役割を持つノード（特権ノード）は、パブリックパーミッションレス型の分散台帳に比べて限定的な数となり、分散台帳システム全体の安全性維持を担うそれらのノードの責任の比重はより高くなる。

プライベートパーミッションレス型の各ノードの安全性を一定レベルに保証し、分散台帳システム全体のセキュリティを維持するため、各分散台帳システムにおいて一般ノードに対するセキュリティ基準、特権ノードに対するセキュリティ基準を定め、各ノードがそれらに準拠した運用を行うことが考えられる。また、必要に応じて基準への準拠性を第三者の評価を行うことが考えられる。この評価の結果が、当該分散台帳システムへの接続の可否の判断に影響することも考えられる。プライベートパーミッションド型分散台帳システムに接続する各ノードのセキュリティ基準を一定に維持することは、分散台帳システムに問題が発生した際に各ノードの管理者が連携して円滑に問題に対処することも可能にする。ノードを分散化することによる耐障害性やセキュリティを効果的にするため、ノードの物理的な配置についても考慮する必要がある。

- **取引に関する確認**

モデル１と同様にリスクと必要性に応じて取引に関する確認や監視を行う。

05

第5章

セキュリティ課題の解決や緩和に向けて

デジタル資産の取引や、重要なデータの活用や連携の基盤となりえる分散台帳のセキュリティはとても重要であり、分散台帳を運用する者も利用する者もその性質を理解して適切に扱うことが必要となる。しかし、これまで課題や対策で言及したように、分散台帳技術は暗号技術や分散処理技術など複数の技術要素を内包し複雑であり、それらの要素のある部分が脆弱な場合に、様々な影響を及ぼし、深刻な場合には分散台帳システム全体が機能不全に陥ることもありえる。

分散台帳の安全性は、個々の技術要素に対する安全性と、それらを組み合わせた場合の安全性、実際に多数のノードのネットワークで構成した分散台帳システムによってもたらされる安全性にかかっている。特にパブリックパーミッションレス型の分散台帳は安全性の維持に暗号資産やトークン発行による経済的なメカニズムが関わっているため、実際の評価はさらに困難な場合が多い。分散台帳技術そのものだけでなく、例えば、スマートコントラクトのフレームワークや署名鍵を管理するウォレットといった周辺の環境に対する安全性に考慮することも必要となる。

本書では技術的な観点で分散台帳の安全性に関わる要素を広範に考察し、分散台帳を利用するビジネスゾーンのシステムを設計し運用を行う際の留意点や緩和策について考え方を示した。これらの留意点は脅威の実現可能性や想定される被害の大きさ等の観点も含めて考慮されるものである。しかし、評価の難しさに加え、技術の進展も早いため、個別の事業者が様々な分散台帳プラットフォームや分散台帳システムに対する評価を行うことは現実的に困難である。より安全な分散台帳システムの活用を促進するために、デジタル通貨フォーラムや他の分散台帳に関わる業界団体、開発者コミュニティ、利用者コミュニティ、学術界、セキュリティ専門家、標準化団体などと連携し、分散台帳に関わる安全性や実際のリスク対応に関する事例の共有、より深い知見の蓄積、指針の策定、実装の評価、推奨される実装のリスト作成などの活動が推進されていくことが重要である。

参考文献

1. ISO 23257:2022 Blockchain and distributed ledger technologies
   Reference architecture
   https://www.iso.org/standard/75093.html

2. X.1401 : Security threats of distributed ledger technology
   https://www.itu.int/rec/T-REC-X.1401-201911-I/en

3. X.1402 : Security framework for distributed ledger technology
   https://www.itu.int/rec/T-REC-X.1402-202007-I/en

セキュリティ検討報告書
ブロックチェーン接続パターンに応じた脅威と緩和策の検討

編集・執筆　ウォレットセキュリティ分科会　幹事 セコム株式会社
セコム株式会社　IS研究所　佐藤雅史
セコムトラストシステムズ株式会社 近藤晴輝
ウォレットセキュリティ分科会　事務局　デジタル通貨フォーラム事務局（株式会社ディーカレットDCP ）

発行　デジタル通貨フォーラム事務局（株式会社ディーカレットDCP ）