JAPAN
SMART
CHAIN

WHITEPAPER

バージョン **1.0.1** | 2025年 8月

免責条項:

このホワイトペーパー及びその内容はいかなるトークンの売買の申込み又は勧誘ではありません。本書面のいかなる内容も、JSC若しくはそのトークン（それがあれば）又はMizuhiki Protocolがどのように発展するのか、利用されるのか、又は価値を有するようになるのかについて、保証又は約束するものと判断又は解釈されるべきものではありません。Japan Smart Chain Foundation（JSCF）[及び/又はAltX Research 株式会社（AltX）]は現状の計画の概要を説明しているに過ぎず、当該計画は自らの裁量で変化しうるものであり、それが成功するかは、我々のコントロール外の様々な要因に依ります。そのような将来についての言及は必然的に既知又は未知のリスクを含むものであり、そのようなリスクは、将来、実際の成果や結果を、我々が本ホワイトペーパーにおいて記載し又は意味するものとは大きく異なるものにする可能性があります。JSCF[及び/又はAltX]はその計画のアップデートをする義務を負いません。実際の結果や将来の事象は大きく変わりうるため、本ホワイトペーパーのいかなる記載も、将来、正確であると判明する保証はありません。将来についての言及に過度の信頼を置かないようにお願いいたします。

はじめに

日本におけるブロックチェーンサービスの発展は、一時的な成長と停滞を繰り返してきました。ビットコインの初期時代には日本が世界をリードする立場にあったものの、現在のweb3時代においては他国に遅れをとっています。

グローバルに見ると、ブロックチェーン産業は成熟しつつあり、決済、分散型金融（DeFi）、実世界資産（RWA）、投票システムなど、スケールのある革新的なサービスが提供されています。

にもかかわらず日本での**web3**サービスの普及を妨げる主要な要因の一つは、日本の金融規制、データの国内保管、消費者保護に最適化されたブロックチェーンインフラの不足だと考えています。

これらの重要な要素が整備されると、日本の有力企業が長期的な投資を安心して行い、決済やロイヤルティ、実世界の資産など、ブロックチェーンを活用したコスト削減や顧客満足度の向上に貢献できるサービスを提供することが可能となるでしょう。

私たちのビジョンは、日本国内でバリデートされ、海外の政治的・地理的・社会的・技術的・経済的影響を受けない、パブリックなレイヤー1（L1）ブロックチェーンの構築です。

ひとことで言えば、**Japan Smart Chain**（**JSC**）は「日本主権型」のL1です。

JSCは日本のための自己主権ブロックチェーン[1]なのです。

[1] 日本のための自己主権ブロックチェーンの定義：

(イ) データはすべて日本国内に保存される。
(ロ) すべてのバリデータノードが日本国内で稼働し、その情報は公開される。
(ハ) 外国の規制当局（SECを含む）の干渉を受けない。JSCは日本のみの指針に従う。
(ニ) JSCのすべての運営が日本国内で行われる。JSCのリサーチラボと財団は、それぞれ株式会社と一般社団法人として日本に登録されている。

「日本のほぼすべての企業や政府機関は***web3***を活用したいと考えていますが、信頼性が高く、適切にガバナンスが行われ、評判が良く、さらに主権型のレイヤー***1***ブロックチェーンが存在しないため、実験や構築に踏み出せないでいます。」

伊藤 穣一
Japan Smart Chain

解決すべき問題

重要なインフラは「主権型」である必要があります。つまり、外部の政府や規制当局の干渉を受けないことが求められます。これまで、電力網、通信、交通ネットワークといった分野が重要インフラの典型例とされてきましたが、人工知能やweb3が進化するデジタル時代において、デジタル主権の重要性がますます明確になっています。

日本政府は最近、デジタル資産の利用やその推進に関する規制環境の整備に注力していますが、大手企業や大規模なサービスプロバイダーは依然としてweb3の活用に消極的であり、新たな消費者体験を提供したり、日本国民のために新たな価値を創出したりすることに踏み切れていません。

私たちが解決したい核心的な課題は、既存のブロックチェーンにおいて、サーバーが世界のどこに設置されているのか、またユーザーがどの国の規制に従うべきかという不確実性と、パブリックなブロックチェーンが提供する透明性、相互運用性、オープンソースの利点を両立させることの間にある緊張関係です。

私たちは、日本の高度なデジタルセキュリティ、プライバシー、安全性への需要に応えるため、外部の政府や規制当局、または単一障害点の影響を受けない主権型ブロックチェーンインフラの早急な開発が必要だと考えています。

ソリューション

「日本のデジタル新幹線」

Japan Smart Chain（JSC）は、日本国内で日本の産業リーダーによってバリデートされる、**Ethereum**完全互換のレイヤー1（L1）ブロックチェーンです。日本の法規制と消費者保護に最適化されており、外国の法規制や外部からの不当な影響を受けないように明確に設計されています。

JSCは外部の干渉を排除するだけでなく、日本のブロックチェーンエコシステムと顧客体験全体を効率化することにも注力しています。特に、アプリケーション層で顕在化する消費者の課題を、L1レベルでより効果的に解決することを目指しています。私たちの主なターゲット分野は、コストが高く、顧客に不便を強いる、または複数のアプリケーション間で繰り返されるプロセスです。

初期段階として、デジタル決済、分散型自律組織（DAO）、およびその他の規制されたオンチェーンユースケースにおけるeKYCの負担をアプリケーション層から軽減することを目指します。

さらに、効率化を図り、消費者に新たな満足を提供できる分野を継続的に模索していきます。

新幹線が既存の鉄道の枠組みを活用しながら、卓越した速度と世界クラスのサービスを提供しているように、**JSC**は**Ethereum**ブロックチェーン技術を基盤に、埋め込まれたデジタルプロトコルを活用することで、**JSC**の利用者が安全かつ合法的に、既存サービスを凌駕するコストでトランザクションを行える環境を提供します。

日本のための主権型Ethereum完全互換性

JSCのセキュリティとスケーラビリティの原則に基づく取り組み

JSCは、主権型**Ethereum**完全互換性の先駆けとして、Ethereumメインネットのセキュリティ、拡張性、技術革新を完全に踏襲しつつ、すべてのバリデータクライアントインフラが日本国内に所在し、名前が公開された状態で稼働する構成を実現します。

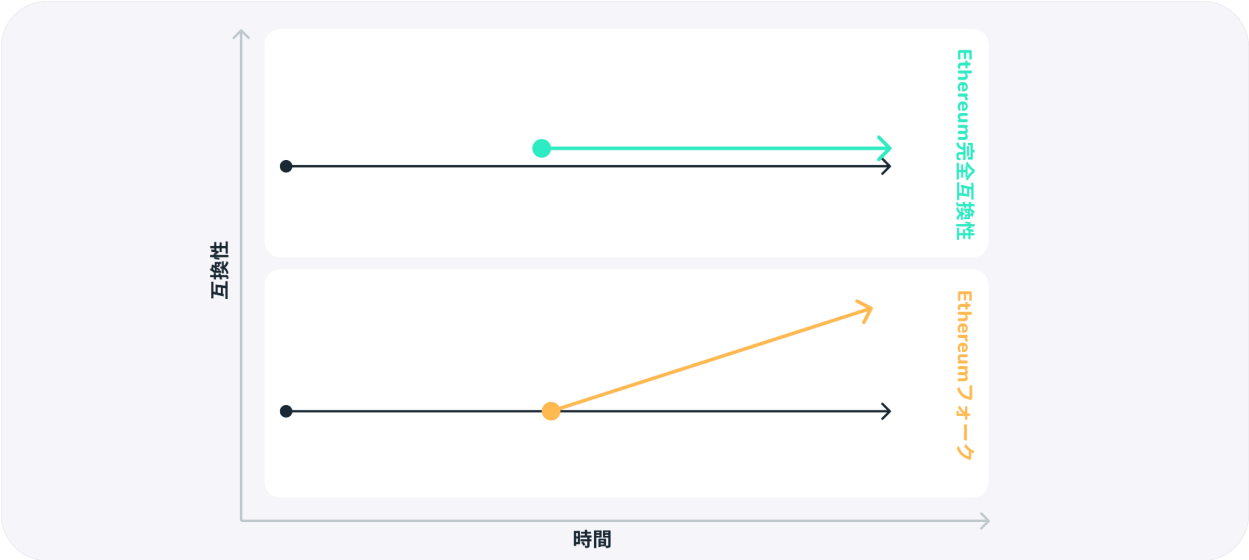
このアプローチは、AI分野の計算サービスにおける選択肢に似ています。共有クラウドサービスから専用リソース、そして最も機密性の高いユースケース向けの完全オンプレミス型インフラまで、多様な提供形態が存在する中で、JSCは日本国内オンプレミス型のパブリックでオープンなブロックチェーンです。

日本主権型ブロックチェーンインフラ

Ethereum完全互換性は、Ethereumの「フォーク」とは異なります。フォークでは、Ethereumのコードベースの一部または全部を変更しなければならず、独自のクライアントソフトウェア、プロトコル、セキュリティアップデートを維持・開発する必要があります。このため、フォークはクライアントの多様性に欠け[2]、既存・新規顧客をサポートする際に膨大なコストが発生しがちです。

[2] 集中リスクを回避するためには、ネットワーク上で複数の独立したブロックチェーンクライアントソフトウェアの実装が稼働していることが理想的である。Ethereum Mainnetでは5つ以上の独立したクライアント実装が維持されているが、多くのEthereumフォークでは1つの実装しか維持できていない。

JSCはEthereumのエコシステムに完全に互換性を持ち、過去・未来にわたるツール群のすべてに対応可能です。



*Ethereum*完全互換性とフォークの比較

JSCは、主権型かつ規制に準拠したブロックチェーンのニーズに対応しながらも、Ethereumとの相互運用性を損なうことはありません。主権型かつ規制準拠ブロックチェーンとしてのカスタマイズは現在も研究開発段階にあり、主な目的は (1) ブラックリストに登録されたトランザクションのブロックと、(2) ステーブルコインなど重要トランザクションの優先処理です。その他のJSC固有のネットワーク設定はジェネシスステートで一度だけ定義されており、これによりEthereumの大規模な仕様変更にも前方互換的に追随できます。

Ethereumや関連するブロックチェーン上でローンチされたプロジェクトは、即座にEthereum互換のJSC上でも展開可能です。この互換性は、Ethereumのレイヤー2（L2）ブロックチェーンエコシステム全体にも及びます。また、EthereumとJSCのオープンソース開発は互換性があり、どちらかのチェーンで行われた進化が相互に恩恵をもたらします。さらに、JSCは適切な場合、Ethereumの上流開発を支援することを予定しています。

JSCの指針となる4つの原則

JSCが日本でweb3の普及を促進するために独自に設計した枠組みは、以下の4つの指針に基づいています。

1. 主権
   主権とは、日本の統制下にあり、外部の規制機関や地政学的な影響を受けないことを意味します。これはJSCの根幹を成す重要な要素です。

   JSCは日本の主権型L1であり、日本の主要な産業リーダーによって日本国内でバリデートされています。JSCは、日本の法規制を遵守し維持するために設計されており、可能な限り外国の法規制や外部の干渉を排除しています。

2. 情報セキュリティ
   デジタル資産の安全性を確保することは、JSCの中核的な目標です。JSCは**Ethereum**完全互換であり、日本の優れたエンジニアリング力を活用して、Ethereumの優位性をさらに強化する堅牢なインフラを提供します。

3. 安全性
   規制対象のオンチェーンサービス（例：ステーブルコイン）の顧客は、アカウントが認証されていることや、日本のマネーロンダリング防止および反社会的勢力排除の方針がインフラ層に組み込まれていることを前提に、安心して他者と取引を行えます。

4. スケーラビリティ
   増え続ける顧客基盤のニーズに応える能力は、プラットフォームの発展に不可欠です。JSCはローンチ時から「L2 as a Service」を提供し、既存および将来のL2プロジェクトが大幅に低コストで準拠したインフラを採用できる環境を整えます。

Mizuhiki（ミズヒキ）スイート

安全性と主権の原則に基づくJSCの新しい基盤

JSCはインフラ層で消費者の課題を解決するというビジョンに基づき、革新的な**Mizuhiki** スイートを提供します。この包括的なスイートはユニバーサルな認証方法とeKYC[3]ツールとサービスを組み合わせたもので、**JSC**プロジェクトやエンドユーザーに対して無料で提供されます。

Mizuhiki スイートは単一で再利用可能なKYCプロセスを通じてユーザーの利便性を高め、消費者の時間を節約し、JSC上のアプリケーションにおけるコストを削減します。このプロセスにより、ブロックチェーンプラットフォームの新しい基準を確立し、日本におけるweb3の普及を妨げる2つの重要な課題、すなわちユーザーエクスペリエンスと情報セキュリティに直接対応します。

さらに、Mizuhiki スイートは、ステーブルコインの送金、金融取引、DAO管理、その他の規制対象活動において、日本の法規制を満たすブロックチェーンアプリケーション構築を支援します。ユーザーは必要な情報をアプリケーションに提供し、安全に取引を行うことができるだけでなく、アプリケーションの利用を中止したい場合には、検証可能な資格情報やオンチェーンの抽象化アイデンティティトークンを介して、いつでも情報へのアクセス権を取り消すことが可能です。

これらすべてのケースにおいて、個人識別情報（個人を特定できる情報）がオンチェーンで公開されることはありません。これは、従来の各アプリケーションに直接**PII**を共有する仕組みとは対照的です。

Mizuhikiは、JSCを利用するブロックチェーンアプリケーション開発者、ユーザー、企業に主な機能として以下を提供します。

- プライバシーの管理をユーザーの手に取り戻す：ユーザーは (イ) 必要最小限の個人情報だけをアプリケーションに共有し、 (ロ) 年齢や大学卒業資格などの証明を自然人のアイデンティティから抽象化し、 (ハ) **DID**や検証可能な資格情報（**VC**）へのアクセス権をワンクリックで取り消す、といった方法でMizuhiki統合スイートを通じて情報共有を細かく制御できます。
- シームレスな**KYC**と**AML**チェックの統合：JSCは最新のセキュリティおよびプライバシー基準を遵守するため、Mizuhiki統合スイートが提供するコンプライアンス／リスク管理

[3] 電子KYC（Electronic Know Your Customer）。本書では「Know Your Customer（KYC）」と同義として使用される。

ツールキットに、文脈に応じたKYC（顧客確認）およびAML（マネーロンダリング防止）などをプログラム的に組み込んでいます。

- 継続的なコンプライアンス：Japan Smart Chainは、プログラム化された継続的コンプライアンスにより、日本の法規制遵守と本人確認コストの削減を目指します。これにより既存・将来のイノベーションに必要なコンプライアンス費用を極小化し、本来はコスト面で困難だった新たなユースケースやビジネス機会を創出します。

エンドユーザーおよび企業が直面する課題に対応するため、Mizuhiki　スイートは以下の3つのコアコンポーネントで構成されます。

(1) Mizuhiki アイデンティティ

eKYC済みのアイデンティティ、DID、検証可能な資格情報（VC）をユーザー自身が管理でき、ポータビリティとオンチェーンでの強制力を両立します。

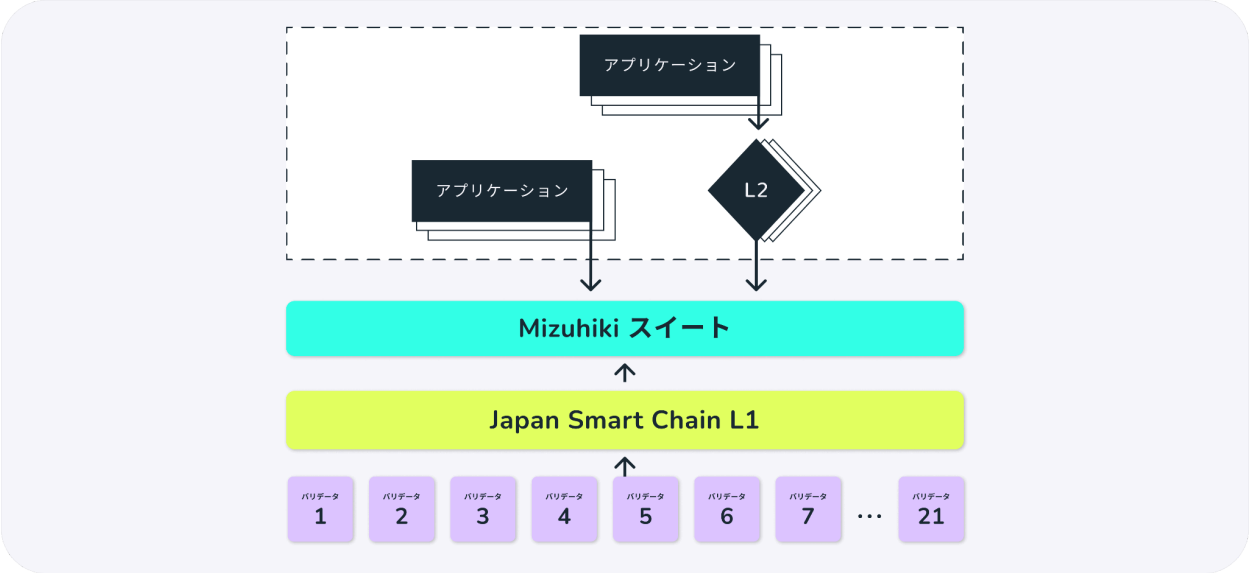
(2) Mizuhiki コンプライアンス

サードパーティによるコンプライアンス検証と保険を提供する「真実のソース」として、オンチェーン／オフチェーンのハイブリッド手法でコンプライアンスシグナルと証明を提示し、金融庁（JFSA）ルールなど外部規制を強制します。

(3) Mizuhiki リスクマネジメント

取引上限・アセットゲーティング・承認フローなど、外部規制を補完する企業独自の運用／取引ポリシーをコード化し、オンチェーンで強制することで効率性と透明性を実現します。

私たちの目標は、規制遵守を妥協することなく、ユーザーの満足度を向上させるとともに、金融ユースケースにおけるイノベーションの強固な基盤を築くことです。



JSCの構成要素の概要

ガバナンス構造

JSCエコシステムは、以下の2つの主要な運営組織によって構成されています。

- ジャパンスマートチェーン財団（**JSCF**）：JSCFは、日本の一般社団法人として設立された財団であり、JSCのガバナンス基準の維持およびエコシステムの発展を継続的に管理する法的主体です。この財団は、JSCのバリデータクライアントオペレーターや広範なコミュニティと密接に連携し、ネットワークの強化に努めます。
- **AltX Research**株式会社（**AltX**）： AltXはJSCブロックチェーンを開発するラボ企業として、JSCバリデータネットワークを構成する21のバリデータクライアントオペレーター（各オペレーターが1台のバリデータクライアントを稼働）の運営支援を担当しています。

トークノミクス

Japan Smart Chain（JSC）のネイティブトークンであるJSCトークンは、JSCエコシステム内で以下の2つの役割を果たします。

1. スマートコントラクトとブロックチェーンアプリケーションの実行：JSCトークンは、JSC上でのスマートコントラクトやブロックチェーンアプリケーションの実行を支えるネイティブトークンとして機能します。

2. ネットワークのセキュリティ確保：バリデータクライアントとステーカーは、JSCトークンをステークし、ネットワークのセキュリティを維持する役割を果たします。その見返りとして、JSCトークンで報酬を受け取ります。ネットワーク稼働開始から最初の10年間は、JSCユーザーが支払うトランザクション手数料に加えて、目標レートで発行されるJSCトークン報酬を獲得できます。

ステーキング・エコシステム

JSCのバリデータネットワークは、日本国内に配置された21のバリデータクライアントオペレーターで構成されています。

JSCは、デリゲート（委任）型ステーキングおよびリテール型ステーキングを通じて、数百万の企業や個人が参加する強固なステーキング・オーナーシップエコシステムの構築を目指しています。21のバリデータクライアントは、フルノード、デリゲート型ステーキング、リテール型ステーキングの3つのカテゴリに割り当てられます。

2025年メインネットローンチからの最初の5年間（2025-2030年）においては、21のJSCバリデータクライアントに対して、以下の表*1*のステーキングオプションが提供されます。

ノードタイプ	企業タイプ	割当てノード数	ノードあたりのステーカー数	最初の5年間の想定年利（APY）
フルノード	日経100企業	8〜10	1	20%
デリゲート型（信頼できるデリゲートパートナーによる運用）[4]	中〜大規模企業	8〜10	数百〜数千	約10%〜15%
リテール型（AltX Researchによる運用サポート）	中小企業および個人（国内外）	3〜5	最大数百万	変動金利
バリデータクライアント数計	–	21	-	-

表*1*：ステーキングエコシステム

[4] 日本国内の大規模企業および中小企業の多くは、高度なセキュリティを備えたブロックチェーンインフラの導入において、技術的な支援を必要とする場合がある。そのため、デリゲート型ステーキングは、堅牢で活発なステーキングエコシステムを構築する上で重要な要素となる。この仕組みにおいては、専門の第三者が技術的な課題や一部の会計業務を代行することで、企業がスムーズに参加できる環境を提供する。

トークン供給量

JSCトークンの初期総供給量は500億枚に設定されています。

以下の表2において、初期トークン供給量の配分表を示し、各グループへの割り当て、権利確定条件、およびロック解除スケジュールを説明します。

グループ	配分割合	トークン数（単位：百万枚）
バリデータクライアントオペレーター	21%	10,500
AltX Research	15%	7,500
JSCF - トレジャリー（コミュニティ基金）	25%	12,500
JSCF - パブリックセール	34%	17,000
JSCF - 開発者エンゲージメント	5%	2,500
Total	100%	50,000

表2：JSCトークン配分

バリデータクライアントオペレーター（21%）

各バリデータクライアントオペレーター（「オペレーター」）は、オペレーターになるための最低条件として、初期総供給量の1%に相当するトークンを購入しステーキングする必要があります。これらのトークンはバリデータスマートコントラクトにデポジットされ、ロックされたままとなります。

AltX（15%）

AltXへの割り当ては、JSCの創設者、株主、開発者、コアチームメンバーへのインセンティブとして設けられています。この割り当ては、プロジェクトの長期的な成功と成長への貢献を認識し、利害の一致を図ることを目的としています。

ジャパンスマートチェーン財団 – トレジャリー（25%）

初期供給量の25%は、JSCFの財団トレジャリーに割り当てられ、コミュニティ基金として特別に指定されています。この割り当ては、コミュニティ主導のプロジェクト、イベント、取り組みを資

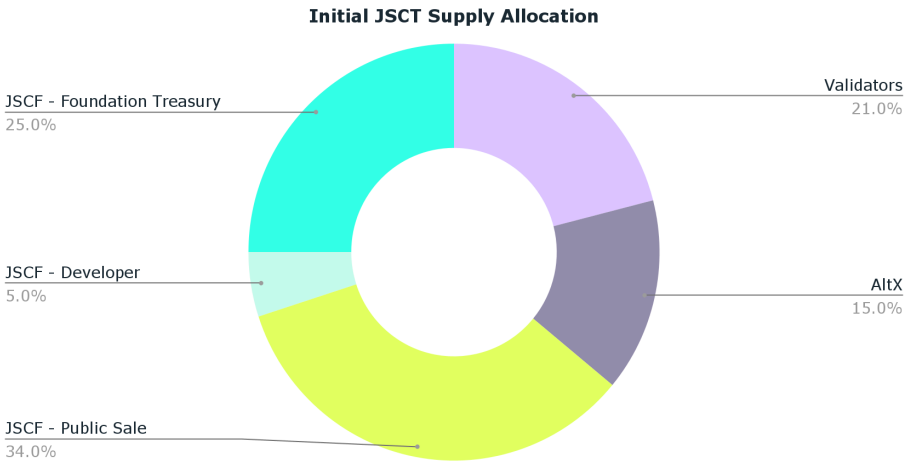
金援助することで、JSCトークンエコシステムの成長と発展を支援し、参加の促進、イノベーションの奨励、コミュニティメンバーの積極的な関与を誘発する財源として機能します。

ジャパンスマートチェーン財団 – パブリックセール（34%）

初期供給量の34%は、国内外の取引所でのパブリックセール用にJSCF準備金に割り当てられます。この公開販売分は、時間をかけてトランシェ方式で投資家に提供され、JSCトークンへのアクセスと流動性を確保します。販売は取引所リストや提供を通じて行われるため、このトークンには権利確定が設定されていません。

ジャパンスマートチェーン財団 - 開発者エンゲージメント基金（5%）

開発者エンゲージメント基金は、新規および既存のJSCコミュニティ開発者へトークンを配布し、JSC Layer 1の開発およびアプリケーション開発（例：Mizuhiki統合スイートやその他の日本特化型コンプライアンス技術）への参加を拡大します。また、トークン循環の促進、ロイヤリティ報酬の提供、そして開発者エンゲージメントのさらなる強化を目的としています。



トークン発行と報酬

JSCのステーカーは、ネットワークのセキュリティ確保に積極的かつ誠実に参加することで報酬を受け取ります。JSCの稼働開始から最初の10年間は、発行報酬とトランザクション手数料の両方で報酬を得ます。

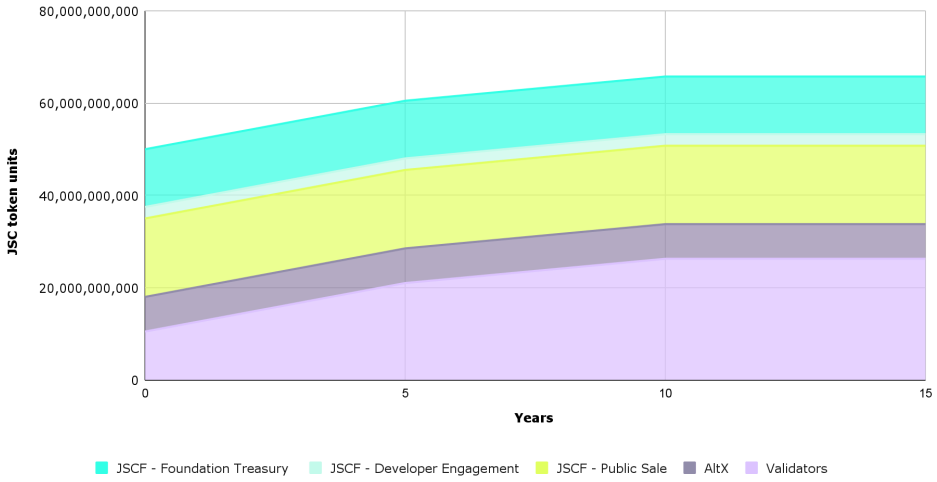
10年後には、トランザクション量が十分に増加し、トランザクション手数料のみでネットワークのセキュリティ確保に対する報酬がまかなえる状態を目指しています。

発行量は時間の経過とともに段階的に減少し、**10**年後にはゼロになるよう設定されています。

JSCのブロックタイムは6秒[5]であるため、1ブロックあたりの発行報酬は400 JSCトークンです。各バリデータクライアントが初期に5億JSCトークンをステーキングし、21のバリデータクライアント全体で105億JSCトークンがステーキングされていると仮定した場合、発行報酬は以下の通りです。

- 1～5年目：年利20%の発行報酬（年間21億JSCトークン発行）
- 5～10年目：年利10%の発行報酬（年間10.5億JSCトークン発行）

フルノードステーカー（すなわちバリデータクライアントオペレーター）は、自身のバリデータクライアントのステーキング報酬全額を受け取ります。一方、ステーキングプールに参加するステーカーは、プール内での保有割合に応じて報酬を受け取ります。

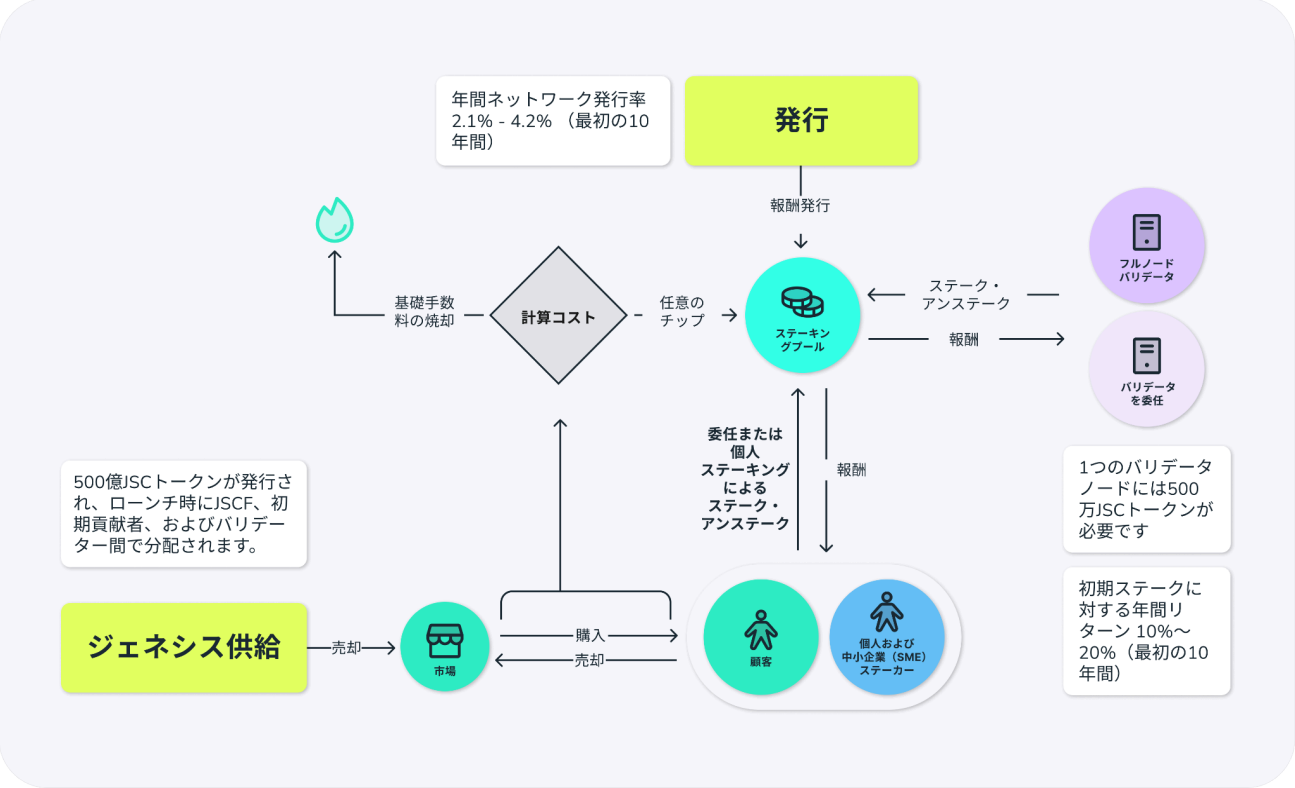


[5]平均ブロックタイムは初期設定で6秒に構成されており、これにより顧客のトランザクション速度と、21のバリデータ間での安全なデータ伝播のバランスが取れるようになっている。

JSCユーザーは、ブロックチェーン上のトランザクション処理のためにJSCトークンで手数料を支払います。Ethereumと同様に、トランザクションには処理費用を賄うための基本手数料と、トランザクション優先度を高めるための優先手数料（任意）が含まれます。基本手数料はバーン（焼却）され流通から除外されることで、バリデータと顧客の間の共謀[6]を防ぎます。

ジャパンスマートチェーン財団（JSCF）は、ステーブルコインやその他の重要なユースケースにおけるトランザクション手数料を、レイヤー1レベルに組み込まれたメカニズムによって補助する方法を積極的に研究しています。

以下のフローチャートは、JSCエコシステム内の経済的な動態を示しています。



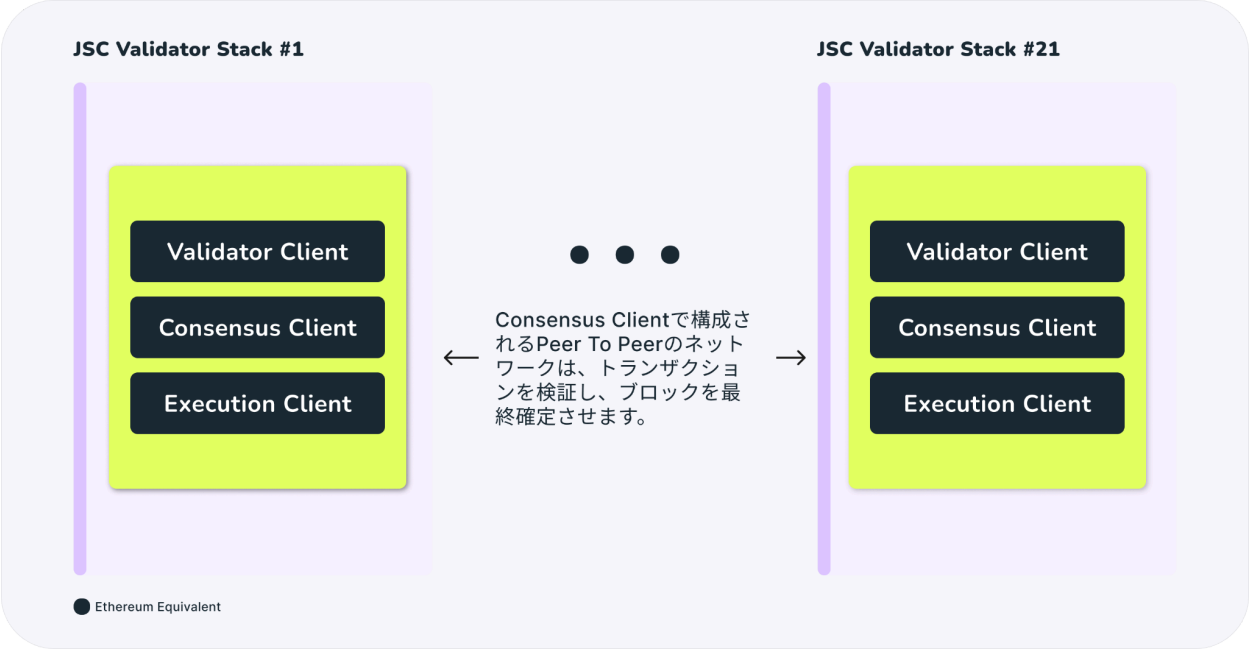
JSCトークノミクスの概要

[6] 出典：Roughgarden, Tim. "Transaction fee mechanism design for the Ethereum blockchain: An economic analysis of EIP-1559." *arXiv preprint arXiv:2012.00854* (2020)

技術的詳細情報

バリデータスタック・アーキテクチャ

JSCの「バリデータスタック[7]」アーキテクチャは、Ethereumの実行およびコンセンサスプロトコルの最新の進展と変更を取り入れながら、許可制バリデータクライアント群と基本的なコンプライアンス機能を両立できるよう設計されています。



JSCバリデータスタック・アーキテクチャ

JSCバリデータスタックは、実行クライアント（Execution Client）、コンセンサスクライアント（Consensus Client）、バリデータクライアント（Validator Client）の3つのコンポーネントで構成されています。実行クライアントとコンセンサスクライアントは標準的なEthereumソフトウェアコ

[7] EthereumがProof of Stakeへ移行して以来、「バリデータ」「バリデータノード」「フルノード」という用語が混用され、開発者や政策立案者の間で混乱を招いている。JSCでは「バリデータクライアント」「フルノード」「許可制システムオペレーター」を区別するために、実行クライアント・コンセンサスクライアント・バリデータクライアントの三つすべてを稼働させるインフラ構成を「バリデータスタック」と呼び、これを運営する許可制バリデータクライアント事業者を「バリデータクライアントオペレーター」と定義する。バリデータクライアントオペレーターに指定されていない者はバリデータクライアントを稼働できず、実行クライアントとコンセンサスクライアントのみをパーミッションレスで稼働できる。文法上、当面は固有名詞としてバリデータスタックを用いる。「バリデータクライアント」は引き続き個別ソフトウェアクライアントを指す語として使用し、混乱を避けるため単独で「バリデータ」という語を用いることは控える。詳細は付録Aを参照。

ンポーネントであり、バリデータクライアントオペレーターに指定されていない者でも、主に読み取り専用の形で個別に稼働できます。

- バリデータクライアント
  - JSCは、バリデータクライアントを実行できる主体をホワイトリストで限定し、高水準のトークン閾値を設定しています。
  - プロトコルは、ネットワークの安全性とコンセンサス維持に貢献した対価として彼らに報酬を付与します。
  - バリデータクライアントの主な役割はブロック提案、ブロックの妥当性アテステーション、およびライトクライアント[8]の同期支援です。

- コンセンサスクライアント
  - PoSコンセンサスプロトコルに基づき、バリデータクライアントの「ビーコン」状態を管理し、フォークチョイスとファイナリティを担保します。
  - 複数のバリデータクライアントを調整し、メッセージの受け渡しやブロック提案などの職務割当を行います。
  - 他のコンセンサスクライアントとP2Pネットワーク上でコンセンサスメッセージを交換します。

- 実行クライアント
  - 他の実行クライアントとのP2Pネットワークで保留中トランザクションを受信およびゴシップします。
  - トランザクションをバリデータクライアントが提案するペイロードにパッケージ化します。
  - Ethereum Virtual Machine（EVM）上でブロックを実行し、ブロックチェーン状態を更新します。
  - JSON-RPC APIを公開し、ユーザーがトランザクション送信やエクスプローラーでのチェーン参照を行えるようにします。
  - EVMのロジックを保持します。

コンセンサスプロトコル - Proof of Stake

JSCは、Proof of Stake（PoS）コンセンサスプロトコルを採用したEVM互換のブロックチェーンネットワークです。このブロックチェーンは、ジャパンスマートチェーン財団（JSCF）が定める厳格なハードウェアおよびソフトウェア基準に従い、日本国内に設置された21のバリデータクラ

[8] ライトクライアントとは、実行クライアントまたはコンセンサスクライアント（あるいはその両方）の軽量版であり、ローカルにデータを保存する代わりに必要に応じてブロックチェーンからデータを取得する。そのため、フルの実行クライアントやコンセンサスクライアントを稼働させる場合に比べ、ライトクライアントのハードウェア要件は大幅に低い。

イアントオペレーター（各オペレーターがバリデータクライアントを稼働）によってバリデートされます。

JSCでは、許可制バリデータクライアントに対しコンセンサス業務が定期的に割り当てられ、正確かつ迅速に遂行した場合は報酬が与えられ、業務を怠るか誤って遂行したことが証明された場合にはペナルティが科されるPoS方式を適用しています。

Mizuhiki スイート：分散型識別子と検証可能な資格情報の活用

MizuhikiはJSCネットワーク向けに最適化されたユニバーサル・アイデンティティ・プロトコルです。この包括的なスイートの核となる「Mizuhiki ID」により、信頼できる Mizuhikiアテスターが利用者のブロックチェーンアドレスへ検証可能なプレゼンテーション（**VP**）[9]またはソウルバウンドトークン（**SBT**）を発行できます。

Mizuhiki アテスターは、日本の主権下でライセンスを受けたコンプライアンス準拠のアテスター網であり、個人・法人等の実世界のアイデンティティとデジタルアイデンティティを結び付ける「信頼の根」を形成します。アテスターは利用者の分散型識別子（DID）に検証可能な資格情報（VC）を発行できます。VCに含まれる個人データはオンチェーンに保存されず、**JSC**のクライアントオペレーターやバリデータからも不可視です。利用者はゼロ知識証明を提示することで個人情報を一切開示することなしにVCの有効性のみを開示し、必要なオンチェーンアクションの資格を証明することができます。これは**VP**または**SBT**、およびその両方の形をとります。

検証可能な資格情報（Verifiable Credentials, VC）はW3C勧告に基づく仕様で、分散型識別子と組み合わせて資格情報の発行・保持・提示・検証を行います[10]。資格情報には、大学の卒業証明書、運転免許証、身分証明書など、さまざまな文書が含まれる可能性があります。**Mizuhiki IDツールキット**には、日本国内で所定の KYC・スクリーニングを完了したことを示すオンチェーンVP「Mizuhiki Verified」 が用意され、規制対象アプリケーションとの相互運用を可能にします。

MizuhikiがVC・VP・SBT（VPの一形態と考えることができる）を活用できるのは、分散型識別子の採用によるものです。

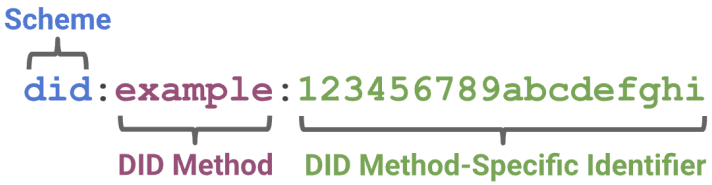
---

[9] 検証可能なプレゼンテーション（*Verifiable Presentations*）は、同一の検証可能な資格情報を場面に応じて異なる形で提示するための仕組みである。その一形態としてゼロ知識表現があり、資格情報の所有者は資格情報そのものを開示することなく、内容に関する主張が真実であることだけを証明できる。詳細は *W3C Candidate Recommendation Draft "Verifiable Credentials Data Model — Zero Knowledge Proofs"*（*2024*年*10*月）を参照。オンライン版：*https://www.w3.org/TR/vc-data-model-2.0/#zero-knowledge-proofs*

[10] 出典：*Verifiable Credentials Overview*, W3C Group Note, October 2024. [Online] https://www.w3.org/TR/2024/NOTE-vc-overview-20241022/

分散型識別子（Decentralized Identifiers, DID）は、分散環境での主体の認証可能な識別を目的に、W3Cワーキンググループ[11]によって推奨されたデジタル識別子です。

各DIDはURIとして構造化されており、識別子によって参照される文書を解決および検証するための方法に関する情報を含んでいます。



分散型識別子（*DID*）の一例[12]

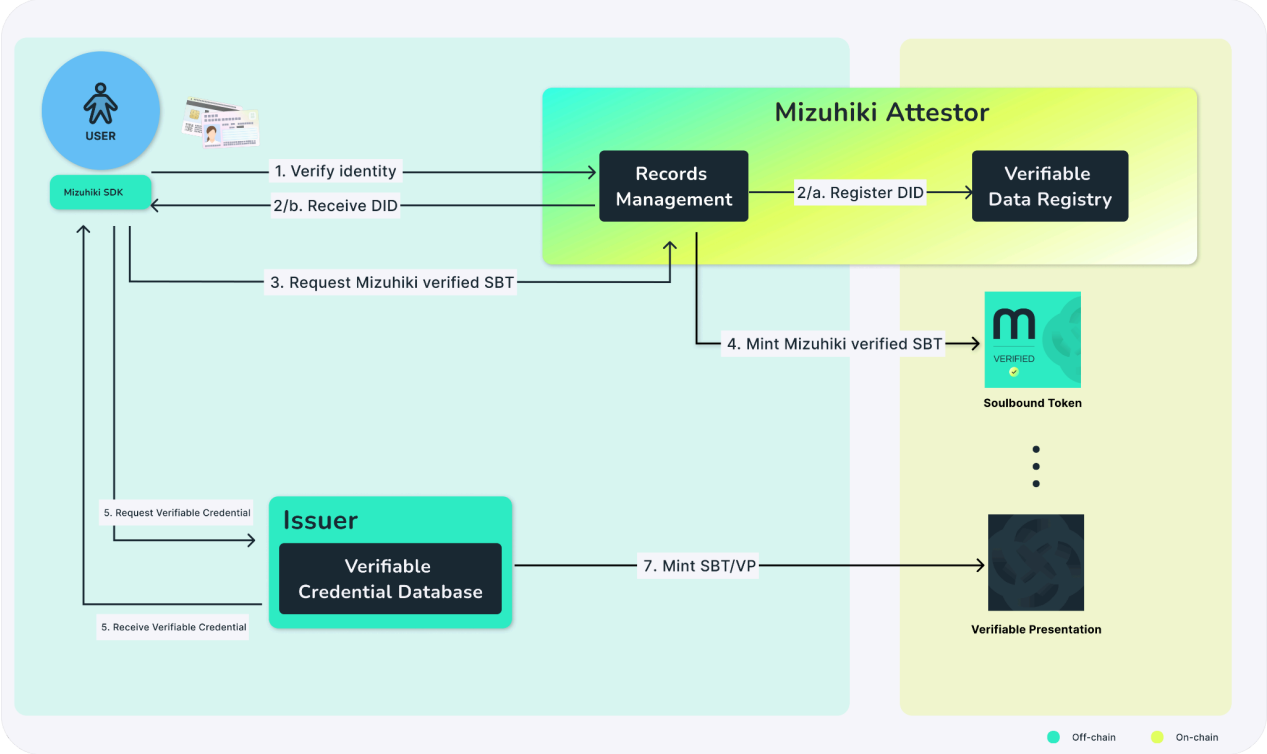
Mizuhiki スイートは、「Mizuhiki DID（Mizuhiki DID メソッド）」と呼ばれるW3Cの仕様に準拠した独自のDIDメソッドを備えています。このメソッドは、接頭辞`did:mizuhiki`で始まる分散型識別子（DID）およびそのDIDドキュメントに対し、構文・リゾルブ・検証・認可の各プロセスを規定します。

Mizuhiki DID レジストリ は、犯罪収益移転防止法に基づくKYCを完了したユーザーの一意なDIDとDIDドキュメントのメタデータを記録するスマートコントラクトレジストリです。

KYC は「Mizuhikiコントローラー」により実施され、同コントローラーは登録済み JPKIサービスプロバイダーである必要があります[13]。

[11] W3C, *Decentralized Identifiers (DIDs)*, W3C Recommendation, v1.0, July 2022. [Online]. Available: https://www.w3.org/TR/did-core/
[12] 同書
[13] Japan Public Key Infrastructure（JPKI）公式ガイド. [Online]. Available: https://www.jpki.go.jp/jpkiguide/index.html

エンドユーザー向けMizuhiki ID利用手順



Mizuhikiエンドユーザー向けフロー

Mizuhiki IDプロセスを完了し、JSC 上で「Mizuhiki Verified」アドレスを取得するためのエンドユーザーのフローは以下のステップで構成されます。

DIDの生成と登録

1. ユーザーは**Mizuhiki** コントローラー（以下「コントローラー」）とともにMizuhiki ID確認プロセスを開始し、本人確認に必要な書類を提出します。プライバシー保護のため、コントローラーは本人確認と書類チェックを完全にオフチェーンで実施します。

2. Mizuhiki アテスターがMizuhiki SDK（開発中）を用いて、ユーザーのDIDをオンチェーンに生成・登録します。

Mizuhiki Verifiedソウルバウンドトークン

3. ユーザーはMizuhiki SDKまたは対応アプリ上で、該当DIDの所有者として認証された後、自身のJSCアドレスへ「Mizuhiki Verified」ソウルバウンドトークン（SBT）を発行できます。

4. ソウルバウンドトークンはMizuhiki コントローラーによって発行され、譲渡不可ですが、コントローラーまたはユーザー（またはその両者）によりバーンが可能です。重要な点として、ソウルバウンドトークンはDIDをはじめとした個人を特定できる情報（PII）を含みません。

検証可能な資格情報（Verifiable Credentials, VC）

5. ユーザーが追加の資格情報を管理したい場合、大学や登録済み団体などの信頼できる機関（「Mizuhiki アテスター」）にVCの発行を依頼しなければなりません。この機関はMizuhiki DIDメソッドと W3C VC 仕様に準拠している必要があります。

6. VCのリクエストを受けた後、Mizuhiki アテスターはオフチェーンでユーザーにVCを発行します。VCはユーザーのMizuhiki DIDに安全・非公開の形でひも付けられます。ユーザーはDIDのverification methodで認可を完了するとVCにアクセスできます。

VCには生年月日・GPA・住所など複数の主張（クレーム）が含まれます。必要に応じ、ユーザーはその一部だけをバリデータへ提示する「検証可能なプレゼンテーション（VP）」を作成できます。言い換えると、ユーザーは生年月日を非公開のまま年齢層を開示したり、居住地の住所を隠したままエリアを開示したりすることが可能です。

検証可能プレゼンテーション（Verifiable Presentations, VP）

7. ユーザーはMizuhiki SDKを通じて、保有する検証可能な資格情報（VC）を基に、JSCアドレスやJSC上の他アプリケーションへ — たとえばソウルバウンドトークン（SBT）形式で — オンチェーン互換の検証可能なプレゼンテーション（VP）を生成・発行できます。VPはVCを保持するユーザー自身、またはそのVCの発行者のいずれかが発行可能なものです。オンチェーンVPには、DIDを含むいかなる個人識別情報（PII）も含めることはできません。VPはオフチェーン形式でも提供でき、その場合はPIIを含むことがあります。

SBT／VC を用いたコンプライアンス＆リスク管理ルールエンジン

ユーザーがJSC上で規制対象の活動（例：金融取引）を行う場合、Mizuhiki スイートを介して自分のSBT／VCを提示し、当該規制サービスを提供するJSCアプリケーションに対して適格性を証明できます。

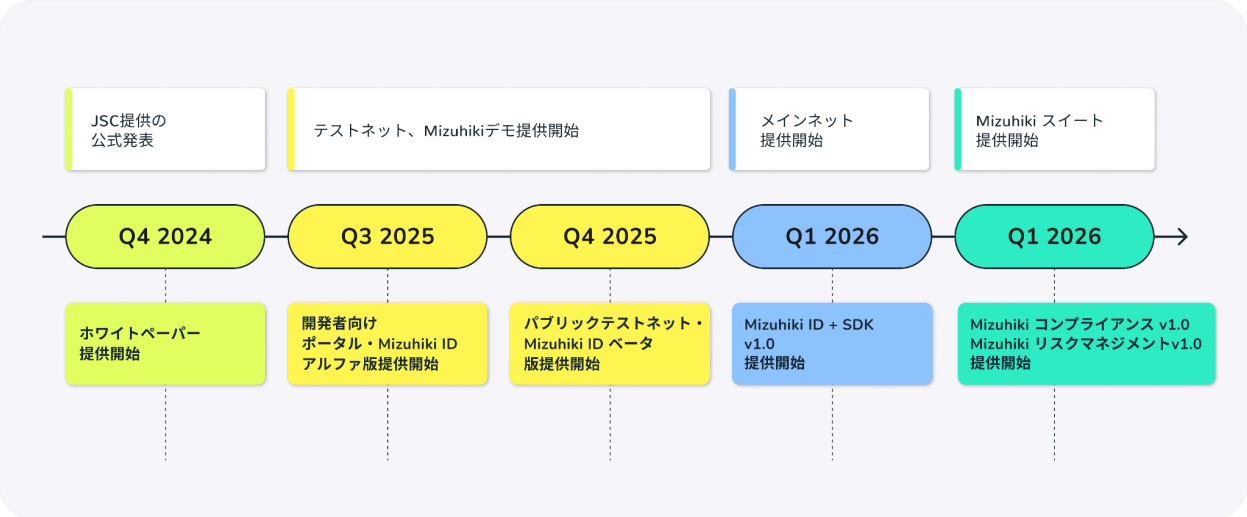
ロードマップ

このプロジェクトのロードマップは段階ごとに分かれており、まずはパブリックテストネット、開発者のオンボーディング、続いてバリデータダッシュボードやブロックエクスプローラーといった主要なツールの構築が行われます。

パブリックテストネットのフェーズでは、ハードウェアおよびソフトウェアのセットアップに加え、レイヤー1での JSCブラックリスト有効化、Mizuhiki IDベータ版ツールの導入、そしてウォレットやステーブルコイン向けコンプライアンスエンジンのテストを通じて、JSCメインネットのローンチ準備を進めます。

次のフェーズでは、JSCメインネットがリリースされます。このフェーズでは、EIP（Ethereum Improvement Proposals）への対応やコアインフラコンポーネントの実装を継続的に行います。

最終フェーズであるMizuhiki スイートの完全リリースでは、オンチェーン検証コントラクト、ブロックチェーンアプリケーションのホワイトリスト化、Mizuhikiアテスターの移行などを実装し、Japan Smart Chainのビジョンを完全に実現します。各フェーズの詳細は下図の通りです。



Japan Smart Chain ロードマップ

付録A：用語集

- マネーロンダリング防止（**Anti-Money Laundering, AML**）
  金融機関やその他の規制対象機関が、金融犯罪、特にマネーロンダリング活動を防止、検出、報告するための政策と実践のセットを指す。
- ブロックチェーン（**Blockchain**）
  非中央集権型で分散されたデジタル台帳。多くのコンピュータでトランザクションを記録し、安全かつ不変の方法で保管する。
- 分散型自律組織（**Decentralized Autonomous Organization, DAO**）
  コンピュータプログラムとしてエンコードされたルールによって運営され、中央集権的なリーダーシップ構造を持たない組織。
- 分散型識別子（**Decentralized Identifiers, DID**）
  分散型環境における主体の検証可能な識別のために設計されたデジタル識別子。
- 電子**KYC**（**Electronic Know Your Customer, eKYC**）
  顧客の個人識別情報（Personal Identifiable Information, PII）を電子的に検証するプロセス。マネーロンダリング防止やその他の法規制に準拠するために使用される。一般的なeKYCの実装例として、スマートフォンやコンピュータのカメラを使用した顔認証等が挙げられる。
- イーサリアム仮想マシン（**Ethereum Virtual Machine, EVM**）
  Ethereumブロックチェーン上でスマートコントラクトを実行する仮想マシン。バイトコードの実行環境を提供する。
- イーサリアムメインネット（**Ethereum Mainnet**）
  Ethereumの本番環境「メインネットワーク」。
- **JSC**メインネット（**JSC Mainnet**）
  Japan Smart Chainの本番環境「メインネットワーク」。
- **KYC**／身元認証（**Know Your Customer**）
  企業やその他の団体が顧客の個人識別情報（PII）を検証し、マネーロンダリング防止（AML）やその他の法規制に準拠するプロセス。
- レイヤー**1**（**Layer 1, L1**）
  ブロックチェーンの中でも、トランザクションの決済とコアインフラの維持を行う基礎的なブロックチェーンネットワーク（例: Ethereum、Bitcoin）。

- レイヤー2（**Layer 2, L2**）
  スケーラビリティとトランザクションスループットを向上させるために、レイヤー1ブロックチェーン上に構築されたセカンダリプロトコル。

- **Mizuhiki** スイート（旧：**Mizuhiki**プロトコル）
  JSCが提供するユーザー制御型の識別ツールキットで、ユーザーの利便性、安全性、ネットワークセキュリティを強化する。

- **Mizuhiki** アテスター（**Mizuhiki Attestors**）
  JSCにおける「認証機関（Certificate Authority, CA）」に相当する存在。ワールドワイドウェブ（WWW）のパラダイムでは、CAは信頼された第三者として機能し、デジタル証明書の所有者（主体）およびその証明書に依存する者の双方から信頼されている。
  Mizuhikiアテスターは、Mizuhiki統合スイートのMizuhiki IDツールを実装する。

- **Mizuhiki** コントローラー（**Mizuhiki Controller**）
  JPKIに登録されたサービスプロバイダーであり、JSCFによって承認されたエンティティで、Mizuhiki DID と「Mizuhiki Verified」ソウルバウンドトークンを発行する権限を有する。

- 個人識別情報（**Personal Identifiable Information, PII**）
  氏名、生年月日、メールアドレス、生体情報など、個人を特定できる情報。

- プルーフオブステーク（**Proof of Stake, PoS**）
  一部のブロックチェーンネットワークがトランザクションを検証し、新しいブロックを作成するために使用するコンセンサスメカニズム。バリデータは暗号通貨をステーキングすることでコンセンサスのプロセスに参加すり。

- スマートコントラクト（**Smart Contract, SC**）
  事前に決められた条件が満たされた際に自動的に実行されるデジタル上のコントラクト（契約）／命令セット。ブロックチェーン上に保存される。

- ソウルバウンドトークン（**SBT**）
  譲渡不可能なノンファンジブルトークンであり、受領者または発行者のいずれかによって取り消すことができる。JSC では ERC-5484（Consensual Soulbound Tokens）規格を実装している。

- ステーブルコイン（**Stablecoin**）
  価格変動を最小限に抑えるよう設計された暗号通貨。しばしば米ドルやコモディティなどの安定した資産にペッグされる。

- ステーカー（**Staker**）
  JSCネットワークにJSCトークンをステーキングする個人や団体。

- シビル攻撃（**Sybil Attack**）
  単一の個人や団体が複数のアイデンティティを作成し、ネットワークに過度な影響を与えようとする攻撃。

- テストネット（**Testnet**）
  各チェーンのメインネットの動作をシミュレートする「テストネットワーク」。開発者や試験利用者が現実世界の金銭的影響を排除しながら、本番環境のプロセスやメカニズムを安全にテストできる環境。

- バリデータクライアントオペレーター（**Validator Client Operator**）
  バリデータクライアントオペレーター（以下「オペレーター」）はJSCネットワークの中枢を担い、主に日本の大手企業や確立された事業体が、バリデータクライアントの運用とネットワークインフラの維持を委託される。オペレーターは物理またはクラウドベースのインフラとコンセンサスプロセスを管理し、ネットワークのガバナンス決定にも参画する。

- バリデータスタック（**Validator Stack**）
  日本国内に設置されたブロックチェーンノードのハードウェアおよびソフトウェアインフラの組み合わせで、トランザクションを収集しブロックを生成してネットワーク全体へ伝播することでJSCブロックチェーンを実装・保護する責任を負う。バリデータスタックはコンセンサスクライアント、実行クライアント、バリデータクライアントで構成される。

- 検証可能な資格情報（**Verifiable Credentials, VC**）
  分散型環境で検証可能なデジタル資格情報。通常、認証には分散型識別子（DID）が使用される。

- 検証可能なプレゼンテーション（**Verifiable Presentation, VP**）
  認証可能な資格情報の一部または暗号的に抽象化された形式で、規制対象またはルールベースの活動を実行するために必要最小限の情報のみを開示するためのもの。

- **Verifiable Data Registry**（**VDR**）
  Japan Smart Chain上で検証可能な資格情報データを管理するレジストリ（個人を特定できる情報は含まない）。信頼できる発行者レジストリとも呼ばれ、Mizuhikiアテスターによって発行された検証可能な資格情報の正確な記録を表す。VDRは改ざん防止機能を備えており、Mizuhikiアテスターによって発行された検証可能な資格情報の正確な記録を保持する。

- ゼロ知識（**Zero-Knowledge, ZK**）／ゼロ知識証明（**~ Proof, ZKP**）
  ある主張が真であることを、追加情報を一切開示することなく証明する現代的な暗号手法。現代の暗号技術の一種であり、一方の当事者が、他方の当事者に対して、追加の情報を一切開示することなく、ある主張が真実であることを証明する方法を指す。