極　秘　　取扱厳重注意

内閣情報調査室

分析部　科学技術分析室

技術評価報告書

自律型 AI エージェント経済基盤「Slonana」ブロックチェーンに関する分析

―― C++20 実装 Solana 互換レイヤー 1 の技術的妥当性および我が国への影響に係る評価 ――

文書番号：　内調/分析/令和 8 年/第 0156 号
作成日：　令和 8 年（2026 年）2 月 7 日
分類等級：　極秘（TOP SECRET）
有効期限：　令和 18 年 2 月 7 日（10 年間）
作成部署：　分析部科学技術分析室

配布先：

内閣総理大臣、内閣官房長官、国家安全保障局長、
金融庁長官、経済産業大臣、デジタル庁統括官、
防衛省情報本部長、警察庁警備局長

第 1 章　要旨

本報告書は、OpenSVM Research が開発する自律型 AI エージェント向けブロックチェーン基盤「Slonana」について、その技術的妥当性、経済的影響、および我が国の安全保障・産業政策上の含意を分析するものである。

Slonana は、C++20 で実装された Solana Virtual Machine（SVM）互換のレイヤー 1 ブロックチェーンであり、以下の特徴を有する。

- Tower BFT コンセンサスと Proof of History（PoH）による暗号学的時間順序保証
- 実測 185,000 TPS（トランザクション毎秒）、142μs 中央値レイテンシ
- ロックフリーアルゴリズムおよび NUMA 対応データ構造による設計目標 1,200,000 TPS 以上
- ベンチャーキャピタル（VC）事前配分を排した公正発行モデル（エアドロップ 10%、ステーキング報酬 90%）
- Model Context Protocol（MCP）ネイティブ対応による AI エージェント自律実行機構

評価結論：本プロジェクトは、自律型 AI エージェント経済の基盤インフラとして技術的に有意な提案を含むが、主張性能の一部は理論値であり実運用環境での検証が未了である。我が国の Web3 戦略およびデジタル円構想との関連で継続的な情報収集が必要である。

項目	**概要**
対象名称	Slonana（スロナナ）
開発主体	OpenSVM Research（代表：Rin Fhenzig）
公表時期	令和 8 年（2026 年）1 月 1 日
実装規模	C++20 ソースコード 87,453 行、506 ファイル
トークン	$SLON、総供給量 1 億枚、ファイナリティ 12.8 秒
技術的脅威度	中程度（監視継続を要する）

第 2 章　背景

2.1　国際的ブロックチェーン動向

令和 8 年現在、主要国においてブロックチェーン技術の国家戦略への組み込みが加速している。米国はデジタル資産に係る行政命令を発出し、欧州連合は MiCA 規制（Markets in Crypto-Assets Regulation）を施行している。中国はデジタル人民元（e-CNY）の大規模実証を継続し、シンガポール・UAE 等は暗号資産ハブとしての地位確立を推進している。

かかる状況下、既存のレイヤー 1 ブロックチェーンには以下の構造的課題が認められる。

1. **中央集権化**：Ethereum においてはステーキング上位 5 主体が全体の 64% を支配し、Solana のナカモト係数は 19 に留まる
2. **スケーラビリティの限界**：Ethereum は基盤層で約 30 TPS、Solana は実効 65,000 TPS であるが、AI エージェント経済の要求水準（100 万 TPS 級）には到達していない
3. **VC 支配構造**：多くのネットワークにおいて VC 事前配分がトークン総量の 20–40% を占め、ジニ係数 0.90 に至る富の集中をもたらしている

2.2　自律型 AI エージェント経済の台頭

大規模言語モデル（LLM）の急速な発展に伴い、自律的に経済活動を行う AI エージェントの実用化が進展している。DeFi 利回り最適化、自動裁定取引、コンピュートリソースの動的調達等、機械間（M2M）トランザクションの急増が予測される。

当該エージェントは人間と異なり、休止なく毎秒数千回の取引判断を行う能力を持つ。従来のブロックチェーン基盤では、このような大規模 M2M 経済の要求を満たすことが困難であるとの分析がなされている。

2.3　Slonana 白書の公表経緯

令和 8 年 1 月 1 日、OpenSVM Research の代表を名乗る Rin Fhenzig 氏により白書「Slonana: A High-Performance Solana Virtual Machine for Autonomous Agent Economies」が公表された。当該白書は、Tower BFT コンセンサス、公正発行モデル、MCP 対応等を主張する技術文書であり、オープンソースとして実装コードが公開されている。

第 3 章　技術的評価

3.1　コンセンサスメカニズム

3.1.1　Tower BFT

Slonana は Solana の Tower BFT コンセンサスアルゴリズムを採用している。Tower BFT は、Proof of History（PoH）によって確立された暗号学的時間順序の上に構築される投票ベースの BFT（Byzantine Fault Tolerance）プロトコルである。

安全性条件は、ビザンチン障害ノードの合計ステーク比率 α について以下のとおりである。

$$\alpha < \frac{1}{3} \implies \text{安全性保証} \tag{1}$$

ファイナリティは合計ステークの 2/3 超の投票により確定し、白書によれば 12.8 秒で達成される。この値は Solana 本体のファイナリティ時間（約 13 秒）と整合的であり、技術的に妥当である。

3.1.2　Proof of History（PoH）

PoH は SHA-256 ハッシュチェーンによる検証可能な時間順序機構であり、Slonana の白書では Solana と同等の実装が主張されている。PoH の暗号学的基盤は広く認知されており、その理論的妥当性に問題は認められない。

3.2　性能に関する分析

白書では以下の性能指標が主張されている。

指標	実測値	設計目標
スループット（TPS）	185,000	1,200,000+
中央値レイテンシ	142μs	—
RPC p95 レイテンシ	$\leq$15ms	—
トランザクション p95 レイテンシ	$\leq$50ms	—

評価所見：

1. 実測 185,000 TPS はテストネット環境における値であり、メインネット規模のバリデータネットワーク（数千ノード）での実証は未了である
2. 設計目標 1,200,000 TPS はロックフリーアルゴリズムおよび NUMA 対応アーキテクチャに基づく理論値であり、コンポーネントレベルのベンチマークにおいて部分的に検証されたに過ぎない
3. 142μs の中央値レイテンシは、ローカル SVM 実行のオペレーションレイテンシであり、ネットワーク伝搬遅延を含まない点に留意が必要
4. C++20 実装は Rust 実装（Agave/Solana）と比較して、メモリ安全性において固有のリスクを伴う。ただし、白書は AddressSanitizer・ThreadSanitizer による検証を主張している

3.3　実装の技術的特徴

3.3.1　C++20 による全面実装

87,453 行の C++20 コードによる実装は、以下の技術的選択を含む。

- simdjson による高速 JSON 解析（nlohmann::json から移行済み）
- RocksDB および ClickHouse によるハイブリッドストレージ
- BPF ランタイムの複数変種（標準、拡張、ロックフリー、JIT 対応）
- QUIC トランスポート層および Turbine ブロック伝搬プロトコル
- Gossip プロトコルによる CRDS（Cluster Replicated Data Store）実装

当該実装は Solana 公式実装（Agave、Rust 言語）との互換性を目指しており、独自のコンセンサスアルゴリズムを提案するものではない。Solana 互換クライアントの多様化という観点では、ネットワークのレジリエンス向上に寄与し得る。

3.3.2　MCP（Model Context Protocol）ネイティブ対応

白書の最も特筆すべき主張は、全てのオンチェーンプログラムが MCP インターフェースを実装し、AI エージェントが実行時にプログラム機能を自律的に発見・実行可能とする点である。

これは、ブロックチェーンと AI エージェントの統合において先進的な提案であり、従来の静的な ABI（Application Binary Interface）に代わる動的なプログラム発見メカニズムを提供する。ただし、セキュリティ上の含意（悪意あるプログラムの自己記述によるエージェント誘導等）については十分な分析がなされていない。

3.3.3　非同期 BPF 実行

自律的プログラム実行（Async BPF）は、エージェントがトランザクション署名なしにプログラムを起動できる機構である。これは従来のブロックチェーンパラダイムからの大きな逸脱であり、権限管理・認可モデルに関する精査が必要である。

第 4 章　経済的影響分析

4.1　トークンエコノミクス

Slonana のトークン設計は以下のとおりである。

項目	内容
トークンシンボル	$SLON
総供給量	100,000,000 枚（1 億枚）
エアドロップ配分	10%（既存 $slonana コミュニティ向け）
ステーキング報酬	90%
VC 事前配分	0%（なし）
チーム配分	0%（なし）

4.2　公正発行モデルの評価

白書はジニ係数のシミュレーション結果として、発行時の 0.88 から 48 ヶ月以内に 0.47 へ収斂すると主張している。一方、VC 支配型ネットワークではジニ係数が 0.90 に達するとされる。

$$G_{t+1} \geq G_t + \epsilon(r, \beta, k), \quad \epsilon > 0 \tag{2}$$

上式は VC 配分比率 β、ステーキング報酬率 r、VC 主体数 k の下でジニ係数が単調増加することを示す。Slonana の $\beta = 0$（VC 配分なし）設計は、理論上この集中化力学を回避する。**評価所見：**

1. 公正発行モデルは分散化の観点で理論的に優位であるが、初期バリデータの参入障壁（ハードウェア要件、技術力）が実質的な集中化要因となり得る

2. エアドロップの 10% 配分は既存ミームコインコミュニティ向けであり、投機的動機による初期ボラティリティが予想される

3. ステーキング報酬 90% モデルは長期的なインフレーション管理の具体的メカニズムが白書中に十分記述されていない

4.3　ゲーム理論的安全性

白書はナッシュ均衡の下でビザンチン攻撃者の行動を分析し、$\alpha < 1/3$ の条件下で全ての利益的逸脱が抑止されると証明している。攻撃コストは 10 億ドル（約 1,500 億円）超と推定されており、スラッシングペナルティがステーク利得を上回る設計となっている。

この分析は理論的に妥当であるが、ネットワーク初期段階（バリデータ数が少なくステーク総量が小さい時期）における安全性については追加的な検討が必要である。

第 5 章　我が国への影響

5.1　デジタル円構想との関係

日本銀行が推進する中央銀行デジタル通貨（CBDC）構想との関連において、以下の論点が存在する。

1. Slonana が主張する高速処理能力（185,000 TPS）が実現された場合、デジタル円の基盤技術としての検討対象となり得る。ただし、CBDC に求められる法的確実性・プライバシー保護・金融政策伝達機構との整合性については未検証である
2. AI エージェント経済基盤としての Slonana が普及した場合、デジタル円との相互運用性が金融政策上の課題となる
3. MCP 対応による AI エージェントの自律取引が大規模化した場合、既存の金融規制枠組み（資金決済法、金融商品取引法）の適用範囲に関する法的整理が必要となる

5.2　我が国の Web3 戦略への含意

政府が推進する Web3 戦略（令和 4 年 6 月「経済財政運営と改革の基本方針」閣議決定）との関連で、以下の事項に留意が必要である。

1. **技術的優位性の確保**：Slonana の公正発行モデルは、日本企業・開発者が初期段階から対等に参加可能な設計であり、VC 支配型ネットワークと比較して我が国にとって有利な参入環境を提供し得る
2. **産業競争力**：C++20 実装は日本の組込みシステム・ゲーム産業における技術的強みと親和性が高く、国内開発者の参画が見込まれる
3. **規制対応**：新規トークンの発行に伴い、金融庁における暗号資産交換業の登録要件、税制上の取扱い等について関係省庁間の調整が必要となる可能性がある

5.3　安全保障上の考慮事項

1. **AI エージェントの自律的経済活動**：MCP ネイティブ対応および非同期 BPF 実行により、AI エージェントが人間の介在なく大規模な金融取引を行う基盤が整備される。これは金融市場の安定性に対する新たなリスク要因である
2. **オープンソースの二面性**：コードの公開はセキュリティ監査を容易にする一方、敵対的行為者による脆弱性分析にも利用可能である
3. **分散型インフラの管轄権**：グローバルに分散したバリデータネットワークは、特定国の法的管轄に服さない可能性があり、マネーロンダリング・テロ資金供与対策（AML/CFT）の観点で課題となる
4. **量子コンピュータ耐性**：白書においてポスト量子暗号への移行計画は明示されておらず、Ed25519 署名に基づく現行設計は将来的な量子攻撃に対して脆弱となり得る

5.4　金融システムへの影響

1. 国内暗号資産取引所における $SLON の上場が行われた場合、個人投資家保護の観点から金融庁による監視が必要となる

2. AI エージェントによる DeFi（分散型金融）取引の自動化が進展した場合、従来の市場監視手法では検知困難な市場操作リスクが発生する

3. 公正発行モデルが実際に機能し富の分散が実現された場合、既存の VC 支配型ネットワークからの資金流出（いわゆる「フェアローンチ・フライト」）が発生する可能性がある

第 6 章　提言

以上の分析を踏まえ、以下を提言する。

6.1　短期的対応（令和 8 年度内）

1. **情報収集の強化**：OpenSVM Research の開発動向、メインネット公開時期、バリデータネットワークの規模拡大状況について、技術的情報収集を継続すること
2. **技術評価の深化**：国立研究開発法人情報通信研究機構（NICT）および産業技術総合研究所（AIST）と連携し、主張性能の独立検証を実施すること
3. **関係省庁への情報共有**：金融庁、経済産業省、デジタル庁に対し、本報告書の内容を適切な分類の下で共有し、各省庁における対応準備を促すこと

6.2　中期的対応（令和 8–9 年度）

1. **規制枠組みの検討**：AI エージェントの自律的金融取引に対応する法的枠組みについて、金融審議会における検討を提言すること。特に MCP を介した自律的プログラム発見・実行メカニズムに対する規制の在り方を検討すること
2. **技術的知見の蓄積**：我が国独自の AI エージェント経済基盤の研究開発を推進し、海外技術への過度な依存を回避するための技術的知見を蓄積すること
3. **国際連携**：FATF（金融活動作業部会）における分散型金融および AI エージェント取引に関する国際基準の策定に積極的に関与すること

6.3　長期的対応（令和 10 年度以降）

1. **デジタル円との相互運用性**：Slonana を含む高性能ブロックチェーンとデジタル円の技術的相互運用性について、日本銀行と連携した検討を行うこと
2. **量子耐性の確保**：ポスト量子暗号への移行計画を含むブロックチェーンの長期的安全性について、暗号技術評価委員会（CRYPTREC）における評価を継続すること
3. **産業政策との統合**：AI エージェント経済が本格化した場合に備え、ブロックチェーン基盤の国内整備を経済安全保障推進法の枠組みにおける特定重要技術として位置付けることを検討すること

付記

分析手法

本報告書の作成にあたり、以下の情報源を分析した。

1. OpenSVM Research 公表白書（令和 8 年 1 月 1 日付、全文英語、数理的証明を含む技術文書）
2. 公開ソースコードリポジトリ（C++20 実装、87,453 行、506 ファイル）
3. Solana 公式実装（Agave）との比較分析（Rust 参照実装 17.4MB、2,281 ファイル）
4. 関連学術論文および技術標準（BFT コンセンサス、PoH、ゲーム理論等）
5. 暗号資産市場動向に関する公開情報

分析の限界

1. 本報告書は公開情報に基づく分析であり、非公開の開発計画・資金調達状況等については情報を得ていない
2. 性能指標の独立検証は実施しておらず、白書の主張値に基づく分析である
3. 開発主体（OpenSVM Research）の組織実態、所在地、資金源については追加的な調査が必要である
4. メインネット未公開の段階における分析であり、実運用後の状況変化に応じた再評価が必要である

用語定義

略語	定義
BFT	Byzantine Fault Tolerance（ビザンチン障害耐性）
PoH	Proof of History（歴史証明）
TPS	Transactions Per Second（毎秒トランザクション数）
SVM	Solana Virtual Machine（Solana 仮想マシン）
MCP	Model Context Protocol（モデルコンテキストプロトコル）
BPF	Berkeley Packet Filter（バークレーパケットフィルタ）
CBDC	Central Bank Digital Currency（中央銀行デジタル通貨）
DeFi	Decentralized Finance（分散型金融）
NUMA	Non-Uniform Memory Access（不均一メモリアクセス）
VC	Venture Capital（ベンチャーキャピタル）
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
CRDS	Cluster Replicated Data Store
QUIC	IETF 標準トランスポートプロトコル（RFC 9000）

令和８年２月７日
内閣情報調査室
分析部　科学技術分析室

（本文書は極秘に指定する。
取扱いは特定秘密保護法に準拠すること。）