Whitepaper ver.0426 — Basic Edition

1. Abstract

分散型金融（DeFi）は過去数年で急速に成長し、Total Value Locked（TVL）は2026年初頭のピーク時に1,300億ドルを超えた（ETH建てでは過去最高水準）。同時に、AIエージェントが自律的に取引を執行する「Agentic Finance」が急速に台頭し、DeFiの参加者構造そのものを変えつつある。機関投資家、個人、そしてAI Agent——多様なアクターが流入し、新しい金融の主戦場がオンチェーンに形成されている。 しかしその裏側では、年間34億ドル規模のハッキング被害が発生し続けている（Chainalysis, 2025年）。根本原因は、DeFiの逆説的な構造にある。 ブロックチェーンは「全ての取引が公開される透明な金融」として設計された。しかし現実には、コントラクトのバイトコードは人間には読めず、Vaultの内部配分構造は不可視であり、トランザクションのcalldataは暗号の羅列にしか見えない。**透明性を標榜する金融が、最も不透明な金融になった**——これがDeFiの逆説である。 Agentic Financeはこの逆説をさらに深刻にする。AI Agentは自律的に判断し取引を執行するが、「何を判断し、なぜその取引を選んだか」は外部から見えない。人間がAgentに資産運用を委託しても、委託先の行動を監視する手段がない。**自律性を標榜するAgentが、最も説明責任を果たせない存在になっている**——これがAgentic Financeの逆説である。 Ninjaは、この二重の逆説を解消するAgentic Security Controlplaneである。Ninja Intelligence Coreは、3つのIntelligence領域（Entity / Action / Position）を通じて、コントラクトの信頼性評価、トランザクション意図の解析、ポジション全体の可視化を提供する。全てのIntelligenceは決定論的なLayer 1（事実の確定）とLLM補完によるLayer 2（人間語への変換）の2層構造に従い、再現性と説明可能性を両立する。さらに、ShoGun（統べる / 止める）がIntelligenceに基づくポリシー制御・自動アクションを実行し、「知る」だけでなく「止める」までを一気通貫で実現する。 Ninjaは「DeFiの透明性ツール」ではない。DeFiとAgentic Financeの透明性・セキュリティインフラである。 本ホワイトペーパーでは、Ninjaの技術アーキテクチャ、9,000万件超のEVMコントラクト・デプロイメントを対象にユニークバイトコード1,500万件以上を網羅的に解析したデータベース「not-so-smart-contracts」、プロダクトロードマップ、ビジネスモデル、及び競合環境について記述する。

---

2. Problem — DeFiとAgentic Financeの構造的不透明性

DeFiの成長は目覚ましい。ETH建てのTVLは過去最高を更新し、Morphoのような新興プロトコルは140万ユーザーを超え、急速な成長を遂げている。同時に、DeFAI（DeFi + AI）領域が急速に成長し、AIエージェントがオンチェーンで自律的に取引を行うAgentic Financeの時代が到来している。 しかしこの成長の陰で、4つの構造的な問題が解決されていない。 **1. コントラクトの信頼性が不明** ユーザーがDeFiプロトコルにアクセスする際、そのコントラクトが安全かどうかを判断する手段は極めて限られている。Verified済みかどうか、Proxy構造を持つか、OFACリストに該当するか、バイトコードの特性がexploitパターンと類似するか——これらを個人が逐

一検証することは現実的ではない。 **2. トランザクションの意図が不透明** 署名しようとしているトランザクションが実際に何を行うのかを、ユーザーは正確に理解できない。calldataの解析、コントラクト呼び出しの連鎖、承認額の妥当性——これらは専門知識なしには判断できず、フィッシングやapproval詐欺の温床となっている。 **3. ポジション全体像の不在** ウォレットの残高を表示するツールは存在する。しかし、Vault内部の配分構造、依存先プロトコルの健全性、資産全体のリスクプロファイルを統合的に把握できる製品は存在しない。ユーザーは自分の資産の全体像を知らないまま運用している。 **4. AIエージェントの行動が監視不能** AI Agentが自律的にDeFiプロトコルと対話し、取引を執行する時代が始まっている。しかし、Agentがどのコントラクトにアクセスし、どのような判断基準で取引を実行し、どのようなリスクを取っているかを、委託者である人間が把握する手段がない。2026年3月のResolv事件では、秘密鍵の侵害により約8,000万USRが無担保で鋳造され、約2,500万ドルの損失が発生した。さらに、周辺プロトコルの自動処理ロジックがデペグ後も機能し続けたことで二次被害が拡大した。Agentの自律性がセキュリティホールとなるケースが現実化している。 これらの問題が重なることで、年間34億ドルのハッキング被害、無数のフィッシング詐欺、そして機関投資家・AI Agent運営者のDeFi参入障壁が維持され続けている。

---

3. Vision

Ninjaのビジョンは、DeFiとAgentic Financeにおけるセキュリティと透明性のControlplaneを構築することである。 「Controlplane」とは、個別のセキュリティ機能を提供するツールではなく、セキュリティに関する判断・ポリシー・対応を統合的に制御する基盤を意味する。ユーザーもAI Agentも、相手を知り（Entity）、行動を読み（Action）、資産を追い（Position）、その上でShoGunを通じてポリシーを定義し、自動化されたアクションを実行できる。 Ninjaは、個人DeFiユーザーの日常的な安全確保から、AI Agentの行動監視、機関投資家やプロトコルのセキュリティインフラまで、スケーラブルにカバーする。DeFiの「見える化」だけでなく、Agentic Financeにおける「説明責任の実装」を実現するインフラとなる。 **DeFi から Agentic Finance への連続性** DeFiは「責任主体の曖昧さ」ゆえに規制当局から敬遠されてきた。プロトコル運営者、フロントエンド提供者、個別ユーザー——誰が何に対して責任を負うのかが技術的に特定困難であったためである。しかし、この問題はAI Agentの登場により逆説的に解決へ向かう。AI Agentによる決定論的な行動ログと、Layer 1/Layer 2の2層構造に基づく説明可能性の実装は、「誰が・なぜ・その判断をしたか」を技術的に証明する基盤となる。DeFiはAgentic Financeへと進化する同じ流れの一部であり、金融の本質——可検証性・説明責任・透明性——に回帰する過程にある。Ninjaはその過程を支えるインフラである。

---

4. Architecture — Ninja の全体構造

Ninjaのアーキテクチャは、3つの層で構成される。

```
Ninja (Agentic Security Controlplane)
│
├── Ninja Intelligence Core（知る）
│   ├── Entity Intelligence  — 相手を知る
│   ├── Action Intelligence  — 行動を読む
│   ├── Position Intelligence — 資産を追う
│   └── Learning             — 学んで進化する
│
├── Ninja Delivery Layer（届ける）
│   ├── NinjaScan（Telegram Bot）
│   ├── Dashboard
│   ├── API
│   └── MCP
│
└── ShoGun（統べる / 止める）
    ├── ポリシーエンジン
    ├── ホワイトリスト管理
    ├── 承認フロー
    └── 自動アクション
```

Ninja Intelligence Core は、Ninjaプラットフォームの中核をなす知性エンジンである。3つのIntelligence領域（Entity / Action / Position）とLearningを通じて、判断の根拠となるIntelligenceを生成する。この分離により、Ninjaの解析結果はNinjaScan・Dashboard・API・MCPの全チャネルから一貫して利用でき、ShoGunのポリシーエンジンや自動アクションのトリガーとしても機能する。人間ユーザーだけでなく、AI Agentからの呼び出しにも同一のIntelligenceを提供する。 **Ninja Delivery Layer（届ける）** は、Ninja Intelligence CoreのIntelligenceをユーザーに届けるインターフェースである。Day1ではNinjaScan（Telegram Bot）を通じてOn-demand解析を提供し、Day2以降でDashboardとAPIを追加する。MCP（Model Context Protocol）はAIエージェントがNinjaをSSOTとして参照する標準インターフェースであり、Delivery Layerの一部として提供される。 **ShoGun（統べる / 止める）** は、Intelligenceに基づくセキュリティポリシーの定義と実行を担う。ホワイトリスト管理、承認フロー、自動アクション（アラート発報、ポジション凍結提案等）を含む。将来的にはAI Agentの行動ポリシー定義にも拡張される。

---

5. Ninja Intelligence Core — 3 Intelligence + Layer 1 / Layer 2

5.1 設計原則：2層アーキテクチャ

Ninjaの全Intelligenceは、以下の2層構造に厳密に従う。 **Layer 1（決定論的層）**

- 事実を確定する。再現性100%。LLMを使用しない

- 同一入力に対して常に同一の出力を返す
- オンチェーンデータ、バイトコード解析、既知パターンマッチング等に基づく
- この層の出力が、全ての判断の基盤となる **Layer 2（LLM補完層）**
- Layer 1の出力を人間が理解しやすい形に変換する
- 事実の補完・説明を行うが、Layer 1の判定を上書きしない
- LLMが生成するのは「説明」であり「判定」ではない この設計は、セキュリティ製品において最も重要な再現性と説明可能性を確保するためのものである。LLMの出力は確率的であり、同一入力に対して異なる結果を返し得る。セキュリティ判定の基盤をLLMに委ねることは、誤判定の原因となるだけでなく、監査やインシデント対応において判定根拠の再現が困難になる。Layer 1で事実を確定し、Layer 2はその事実を人間にとって読みやすい形に変換するのみ——この原則が、Ninjaの信頼性の基盤である。 この2層構造は、AI Agentの行動監視においても重要な意味を持つ。Agentの取引を事後的にLLMで「解釈」するだけでは、解釈そのものが確率的で再現不能になる。Layer 1で取引の事実構造を決定論的に確定し、Layer 2でその事実を人間が監査可能な形に変換する——この構造が、Agentの説明責任を技術的に実装する基盤となる。

5.2 Entity Intelligence — 相手を知る

Entity Intelligenceは、コントラクトおよびアドレスの信頼性を多角的に評価する。 **Layer 1の評価項目：**

- バイトコードML分析：コントラクトのバイトコードから特徴量を抽出し、機械学習モデルで悪性パターンを検出
- Risk Score算出：複数の評価軸を重み付け統合したスコアリング
- ブラックリスト/OFAC照合：制裁リストおよび既知の悪性アドレスとの照合
- コントラクト属性検証：Verified状態、Proxy構造、デプロイからの経過時間等 **Layer 2 の補完：**
- 評価結果の自然言語サマリー生成
- リスク要因の優先順位付きの説明
- 類似コントラクトとの比較コンテキスト **動作モード：**
- **On-demand：** `/check` コマンドによるユーザー起点の即時評価

- **Continuous：** 依存先コントラクトに変更（アップグレード、オーナー変更等）が検出された場合の自動再評価

5.3 Action Intelligence — 行動を読む

Action Intelligenceは、トランザクションのcalldataを解析し、そのトランザクションが「何をしようとしているか」を判定する。人間が署名するトランザクションだけでなく、AI Agentが自律的に生成・実行するトランザクションも同一の解析パイプラインで処理する。 **Layer 1 の解析パイプライン（Action Intelligence Pipeline）：**

```
ParseCheck
→ TxIntentMapper（意図分類）
  → ContractArtifactResolver（コントラクト情報の解決）
    → 並列Check（複数の検証を同時実行）
      → Layer 1 Output（構造化された事実）
        → LLM補完（Layer 2）
```

1. **ParseCheck：** トランザクションデータの構文解析と基本検証
2. **TxIntentMapper：** calldataのfunction selectorから意図カテゴリ（13種）へのマッピング
3. **ContractArtifactResolver：** 対象コントラクトのABI、ソースコード、メタデータの解決
4. **並列Check：** 複数の検証ロジック（approval額検証、既知exploit署名照合、再入可能性検査等）を並列実行
5. **Layer 1 Output：** カテゴリ（13種）、アラートコード（17種）、信号機（SAFE / WARNING / DANGER）の構造化出力
6. **LLM補完：** Layer 1の構造化出力を人間が読める解析レポートに変換 **13カテゴリ：** Native Transfer、Token Transfer、Token Approve、Token Approve All、Permit、Permit2、DeFi Swap、Multicall、Multisig Exec、Ownership Transfer、Proxy Upgrade、Generic Call、Unknown **信号機システム：**

- **SAFE：** 既知のパターンに合致し、異常なし
- **WARNING：** 注意を要する要素あり（高額approval、未検証コントラクト等）
- **DANGER：** 高リスク要素を検出（既知exploit署名、制裁アドレスとの関連等） **動作モード：**
- **On-demand：** `/scan` コマンドによるユーザー起点の即時解析
- **Continuous：** 監視対象ウォレットのトランザクションを自動検出・解析（AI Agentのウォレットを含む）

5.4 Position Intelligence — 資産を追う

Position Intelligenceは、ウォレットの全ポジションを検出し、Vault内部の配分構造を含む全体像を可視化する。 **主要機能:**

- 全ポジション検出：ウォレットが保有するトークン、LPポジション、Vaultシェア、ステーキングポジション等の網羅的検出
- Vault配分マッピング：Vault内部でユーザーの資産が実際にどのプロトコル・プールに配分されているかの構造解析
- 異常検知：ポジションの急激な変動、Vault戦略の変更、依存先の異常等の検出 **動作モード:**
- **On-demand:** ウォレット登録時の全ポジションスキャン
- **Continuous:** 定期巡回による変動検出とアラート

5.5 Learning — 学んで進化する

Ninjaは、3つのメカニズムを通じて継続的に進化する。

1. **ユーザー通報 → Ground Truth → モデル再学習:** ユーザーからのフィードバック（誤検知報告、不審トランザクション通報等）をGround Truthとして蓄積し、検知モデルの精度向上に活用する
2. **アラートコード蓄積:** 新たなインシデントが発生するたびに、そのパターンを分析し、新しい検知ルール（アラートコード）として追加する。検知対象は時間とともに拡大し続ける
3. **外部知見吸収:** Forta Network、GoPlus Security、DeFi Llama等の外部データソースから継続的に情報を取り込み、Ninjaの知識ベースを更新する

---

6. not-so-smart-contracts — 大規模EVMコントラクト解析DB

Ninjaは独自に構築した大規模EVMコントラクト解析データベース「not-so-smart-contracts」を保有している。具体的には、**9,000万件超のコントラクト・デプロイメントを対象とし、重複排除後のユニークバイトコード1,500万件以上を網羅的に解析**している(※ 同一バイトコードの再デプロイを統合した実解析対象数)。このデータベースの名称は、Trail of Bits（Crytic）が公開した同名のスマートコントラクト脆弱性パターン集（https://github.com/crytic/not-so-smart-contracts）に敬意を表して命名したものである。Trail of Bitsのリポジトリがパターン学習を目的とした教育リソースであるのに対し、Ninjaのnot-so-smart-contractsはEVMコントラクトを網羅的に解析したプロダクションデータベースであり、用途・規模ともに異なる。このデータベースは、Ninja Intelligence Coreを2つの方向で強化する。

6.1 Action Intelligence強化：selector_mappings.parquet

解析対象コントラクト群から抽出したfunction selectorとメソッド名のマッピングを `selector_mappings.parquet` に格納し、Ninja Intelligence CoreのAction Intelligenceが参照する `SELECTOR_METHOD_MAP` に統合している。 これにより、ABIが公開されていない未検証コントラクトのトランザクションに対しても、function selectorからメソッド名を高精度で解決できる。従来「Unknown」と判定されていたトランザクションの意図分類が大幅に改善され、Action Intelligenceのカバレッジが拡大した。

6.2 Entity Intelligence強化：contract_embeddings.npy

各コントラクトのバイトコードから特徴量を抽出し、ベクトル埋め込み（embedding）として `contract_embeddings.npy` に格納している。 これにより、新規コントラクトのバイトコードを既知のコントラクト群と類似度比較できる。例えば「過去のexploit対象コントラクト群と87%類似」といった判定が可能になり、Entity Intelligenceのリスク評価に定量的な根拠を提供する。未知のコントラクトであっても、過去のexploitパターンとの構造的類似性から早期にリスクを検出できる。

---

7. Product & Customer Roadmap — Day1 to Day5

Ninjaのプロダクトは、Day1からDay5までの5段階でリリースされる。各Dayはターゲット顧客・チャネル・Intelligence領域・動作モード・課金モデルが段階的に拡張される構造を持つ。

Day1：Foundation — B2Cカスタマーベース獲得

- **ターゲット顧客：** B2C個人
- **チャネル：** NinjaScan（Telegram Bot）
- **Intelligence：** Entity Intelligence + Action Intelligence
- **コマンド：** `/scan`（Action解析・実装済・公開ローンチ済）/ `/check`（Entity評価・公開ローンチ直後に追加実装）
- **動作モード：** On-demand（ユーザー能動）
- **課金：** 基本無料のみ（Free 3回/日）。Day1の最大目的はカスタマーベース獲得であり、課金は次Dayから本格化する
- **並行施策：** Day1段階からB2Bパイロット1〜2社を確保し、Day2以降のB2B展開の前準備を並行進行する Day1の狙いは、NinjaScanという低摩擦チャネルで個人ユーザーのベースを

最速で積み上げることにある。技術差別化はLLMではなくML精度——Ninja Risk Engineのベンチマーク精度——で行い、Entity/Actionの二軸でNinjaの中核価値を無料体験させる。

Day2：Continuous Monitoring — B2C受動監視 + 課金開始

- **ターゲット顧客：** B2C個人（継続）
- **チャネル追加：** Dashboard
- **Intelligence追加：** Position Intelligence + Learning初期（オフチェーン通報データ統合）
- **動作モード追加：** Continuous監視（外部データ・通報データを含む受動アラート）
- **課金：** 本格開始。Free / Lite / Pro の3プラン。上位プランほど利用回数・機能が拡張される
- **前提条件：** Day1での有料化意思検証が完了し、B2Bパイロットが並行進行していること
  Day2はOn-demandからContinuousへの転換点であり、B2Cの課金が本格化するフェーズでもある。Dashboardの追加によりPosition全体像の視覚化が可能になり、外部データ・通報データを取り込んだLearning初期版が稼働する。

Day3：Protocol Expansion — B2B API + ShoGun + MCP対応

- **ターゲット顧客：** DeFiプロトコル運営
- **チャネル追加：** B2B API（Read / Monitor / Control APIの3階層構成）
- **機能追加：**
  - プロトコル個別監視項目（フラッシュローン対策、Vault戦略逸脱検知、ガバナンス提案分析）
  - ShoGun（統べる / 止める）初期（ポリシーエンジン、ホワイトリスト、承認フロー）
  - **MCP（Model Context Protocol）対応** — AIエージェントがNinjaをSSOTとして参照する標準インターフェース。Ninja Delivery Layerの一部として提供
- **Intelligence：** Learning本格稼働 Day3はNinjaがB2Bプラットフォームへと拡張するフェーズである。DeFiプロトコル運営チームを主要顧客とし、プロトコル固有の監視要件に応える。MCP対応は、Day5のAI2AI Controlplaneへの布石となる。

Day4：Institutional Control — ShoGun拡充

- **ターゲット顧客：** CEX・機関投資家・ファミリーオフィス・コンプライアンスチーム
- **機能追加：**

- 個別ガバナンスポリシーDSL
- 自動アクション拡充
- コンプライアンスレポートの自動生成

- **チャネル：** 機関向け専用Dashboard、SLA保証付きAPIライン Day4ではShoGun（統べる / 止める）が機関向けに拡充される。個別のガバナンスルールをDSLで定義でき、コンプライアンス要件に応じた自動アクションとレポーティングが可能になる。

Day5：AI↔AI Controlplane

- **ターゲット顧客：** AIエージェントプロバイダー、AI2AIエコシステム
- **機能：** Day3のMCP対応（AI→Ninja参照）から一歩進み、**AIエージェント同士のポリシー仲介・契約検証・インシデント隔離**を提供
  - Agent間取引ポリシー合意プロトコル
  - 行動ログの暗号学的証明
  - 異常Agent自動隔離
- **位置付け：** Agentic Finance時代の信頼性インフラとしての完成形 Day5はNinjaの長期ビジョンの完成形である。AIエージェント同士が自律的に取引・契約を交わす時代において、ポリシーの仲介者、契約検証者、インシデント隔離者として機能する。

統合ロードマップ表

フェーズ	主要顧客	チャネル	Intelligence	動作モード	課金
Day1 Foundation	B2C個人	NinjaScan	Entity + Action	On-demand	基本無料
Day2 Continuous	B2C個人	+ Dashboard	+ Position + Learning初期	+ Continuous（外部データ統合）	Free / Lite / Pro
Day3 Protocol	DeFiプロトコル	+ B2B API + MCP	+ Learning本格	+ ShoGun初期	B2B API課金
Day4 Institutional	CEX・機関	+ 専用Dashboard	（同上）	+ ShoGun拡充（ガバナンスDSL）	Enterprise課金
Day5 AI2AI	AI Agentプロバイダー	+ Agent間プロトコル	（同上）	+ AI2AI仲介	Agent課金

---

8. Competitive Landscape

DeFiセキュリティ、ポートフォリオ可視化、Agentic Financeのセキュリティ領域には複数の既存プレイヤーが存在する。本章ではそれらを機能の性質に基づいて3つの類型に分類し、Ninjaとの差を可視化する。

類型の定義

- **Security Alert**：危険検知・通知に特化し、Control機能を持たない類型。Blockaid, GoPlus, Hypernative, Forta等が該当する
- **Asset Visualization**：ポジション表示に特化し、セキュリティ評価を提供しない類型。Zapper, Zerion, DeBank, Exponential.fi等が該当する
- **Control Layer**：ポリシー実行・自動制御まで踏み込む類型。DeFi Saver（部分的）と**Ninja**が該当する

機能対応マトリクス

類型	サービス	Entity	Action	Position	LLM説明	アラート	ダッシュボード	B A
Security Alert	Blockaid	△	○	x	x	x	x	○
Security Alert	GoPlus	○	△	x	x	△	x	○
Security Alert	Hypernative	△	○	x	x	○	○	○
Security Alert	Forta	△	○	x	x	○	△	○
Asset Viz	Zapper	x	x	△	x	x	○	△
Asset Viz	Zerion	x	x	△	x	x	○	x
Asset Viz	DeBank	x	x	△	x	△	○	△
Asset Viz	Exponential.fi	x	x	○	△	x	○	x
Control Layer	DeFi Saver	x	x	△	x	○	○	x
Control Layer	**Ninja**	○	○	○	○	○	○	○

○ = 主要機能として提供　△ = 部分的に対応　x = 非対応 ### 各類型の解説と差別化 **Security Alert類型：** 「危険を知らせる」ことに優れるがControl Layerは持たない。Blockaid（累計調達\$83M）とHypernative（累計\$68M）は豊富な資金力を背景に広く採用されているが、Control LayerとPosition Intelligenceを持たない点はNinjaとの構造的な差である。 **Asset Visualization類型：** 「何を持っているか」の可視化に優れるが、セキュリティ評価は提供しない。Zapper/Zerion/DeBank/Exponential.fiはポ

ジションの見える化に特化しており、コントラクトの信頼性評価やトランザクション意図解析は扱わない。 **Control Layer類型：** 主要プレイヤーが極めて少なく、**AI向けControl Layerは現時点で需要検証段階の新興領域**である。Ninjaは3類型（Security Alert / Asset Visualization / Control Layer）を縦断統合（See → Detect → Control）し、AI向け対応までロードマップに明示的に含める先行プレイヤーの一つとしてポジショニングしている（※ 評価は2026年3〜4月時点の公開情報および営業ヒアリングに基づく独自判断）。 ### Ninjaの差別化ポイント

- 3類型（Alert / Visualization / Control Layer）を縦断統合する数少ないプレイヤーの一つ
- 決定論的Layer 1とLLM補完Layer 2の2層アーキテクチャによる再現性と説明可能性の両立
- Day5まで含むAI向けロードマップ（MCP対応 → AI2AI Controlplane）を明示している

留意点

AI向けControl Layer市場は現時点で需要検証段階にある。NinjaはB2C → B2Bプロトコル → AI向けへと段階的に展開する戦略を採用しており、各フェーズでの検証結果を踏まえて次フェーズの投資を意思決定する。

---

9. Business Model

Ninjaのビジネスモデルは、個人向けフリーミアムとB2B APIの2軸で構成される。

個人向け（B2C）

Free / Lite / Pro の3プラン。上位プランほど利用回数・機能が拡張される。

プラン	内容
Free	`/check` 3回/日 + `/scan` 3回/日
Lite	`/check` 拡張回数/日 + `/scan` 拡張回数/日
Pro	無制限 + 優先レスポンス + 詳細レポート出力

Day1は基本無料プランのみでカスタマーベース獲得に専念し、Day2からLite/Proを本格投入して収益化を開始する。Free層はDay1以降もユーザー獲得チャネルとして継続的に機能する。 ### B2B API Read API / Monitor API / Control API の3階層。上位階層ほど機能範囲が拡大し、価格も段階的に上昇する。価格レンジは他社の公開・推定価格（Hypernative \$3K–\$20K、Blockaid \$5K–\$50K、GoPlus Enterprise \$500–\$3K、Forta \$100–\$1K）を参考としたベンチマークに基づき、パイロット顧客との合意を経て決定する。

プラン	機能	対象カテゴリ（例）
Read API	Entity / Action Intelligenceの参照	キュレーター、ウォレットプロバイダー
Monitor API	+ Continuous監視 + アラート配信 + プロトコル個別監視項目	DeFiプロトコル、AI Agentプロバイダー
Control API	+ ShoGunポリシーエンジン + 自動アクション + ガバナンスDSL	機関投資家、コンプライアンス、CEX

※ Enterprise向けフルスイート（MCPインテグレーション、SLA保証、専用サポート）は個別対応とする。 --- ## 10. Team ### コアチーム - **CEO 金城：** Accenture 13年。金融機関向けAIプロジェクトを多数リード。戦略立案からテクノロジーデリバリーまでの一貫した経験 - **CTO 村上：** 大規模システム開発の技術リーダー。分散システム設計、パフォーマンスエンジニアリングに深い知見 - **恵上：** 暗号資産取引所およびFireblocks（機関向け暗号資産インフラ）での実務経験。セキュリティオペレーションの実践知識 - **大月 海（Kai Otsuki）：** B4TI（IEEE International Workshop on Blockchain for Decentralized Trust and Digital Identity）General Co-Chair。Ethereum Foundation貢献、IETF SD-JWT（RFC 9901）標準化への参画 - **CMO 菅沼：** 3言語（日本語、英語、中国語）対応。グローバルマーケティング・コミュニティ構築 ### アドバイザー - ICANN DNSSEC鍵管理者（Trusted Community Representative）。インターネットインフラの最も重要な暗号鍵管理セレモニーに参画する、世界で限られたセキュリティ専門家の一人（氏名非公開） --- ## 11. 市場環境と規制動向 ### 市場データ - **DeFi TVL：** \$130B超（2026年初頭ピーク時。ETH建てでは過去最高水準、出典: DefiLlama） - **Web3セキュリティ市場：** \$2.9B（2025年）→\$15.8B（2032年予測、CAGR 26.4%） - **年間ハッキング被害額：** \$3.4B（2025年、出典: Chainalysis） - **DeFAI（DeFi + AI）領域：** 急速に成長するセクター。AIエージェントによるオンチェーン取引が新たな市場カテゴリを形成 - **Morpho：** 140万ユーザー超。Vault型DeFiの急拡大を象徴 - **Resolv事件：** 2026年3月、秘密鍵の侵害により約8,000万USRが無担保で鋳造、\$25Mの損失。周辺プロトコルの自動処理ロジックがデペグ後も機能し二次被害拡大。Agentic Financeのセキュリティリスクを顕在化 これらの数値は、DeFiの成長と並行してセキュリティ需要が拡大していることを示している。特にAgentic Financeの台頭は、従来の「人間が署名するトランザクション」だけでなく、「AI Agentが自律的に実行するトランザクション」の監視需要を生み出している。 ### 規制動向 規制環境はDeFiセキュリティサービスへの需要を中期的に後押しする可能性がある。 **SEC DeFiフロントエンド不処分意見（No-Action Position）（2026年4月13日）** 2026年4月13日、米SEC取引・市場局（Division of Trading and Markets）は、DeFiフロントエンドおよび自己管理型ウォレットUI提供者に関する声明を発出した。一定条件を満たすDeFiフロントエンド提供者は、ブローカー・ディーラー登録を不要とするno-action letterの形式である。 主要条件（計11条件のうち以下の3点を要約）： 1. **ユーザーの自律性：** フロントエンドがユーザーの取引判断に介入せず、ユーザーが自律的に操作すること 2. **中立性：** フロントエンドが特定の取引や相手方を推奨・誘導しないこと 3. **透明性：** 利益相反の開示、サイバーセキュリティ対策の実施、MEV（Maximal Extractable Value）戦略の公開を行うこと 本措

置は5年間の時限措置であり、2031年4月13日まで有効である。 これはSECスタッフによる不処分意見（法的拘束力を持つルールではないが市場への実質的シグナルとして機能する）であり、DeFiフロントエンドの増加はNinjaのようなセキュリティインフラの市場拡大に直結する。特に第3条件の「透明性」——利益相反開示、サイバーセキュリティ対策、MEV戦略公開——は、Ninja Intelligence Coreが提供する価値と直接的に一致する。DeFiフロントエンド提供者がSEC条件を遵守するためのインフラとして、NinjaのB2B APIは具体的なユースケースを持つ。 **その他の規制動向** - **MiCA（EU Markets in Crypto-Assets Regulation）： ** 暗号資産市場の包括的規制枠組み。2024年12月に全面施行済み（移行期間最終期限: 2026年7月）。DeFiプロトコルへの適用範囲は現時点では明確に定まっておらず、今後の細則策定を注視する段階にある。方向性としては、透明性とセキュリティへの要求が高まる追い風と捉えられる - **PSA改正法（2026年6月施行予定、日本）： ** 資金決済に関する法律の改正であり、主に暗号資産交換業者を対象とする。DeFiプロトコルや関連サービスへの適用範囲は不明確であるが、取引所を経由するDeFiアクセスにおけるセキュリティ要件の強化につながる可能性がある。また、2026年4月には金融商品取引法（FIEA）改正案が閣議決定され、暗号資産を「金融商品」として再分類する方針が示された。これはPSA（決済手段）からFIEA（金融商品）への根本的な制度転換であり、DeFi関連サービスへの規制環境にも中期的な影響を与える可能性がある - **EU AI Act（2024年8月発効済み、2026年8月に主要条項（ハイリスクAI要件、透明性義務等）が全面適用開始予定）： ** AI規制の包括的枠組み。Agentic Financeの文脈では、AI Agentの行動の説明可能性・監査可能性が将来的に規制対象となる可能性がある。Ninjaの2層アーキテクチャ（決定論的Layer 1 + LLM補完Layer 2）は、この規制方向性と整合する 総じて、これらの規制動向はDeFi及びAgentic Financeのセキュリティサービスへの需要を中期的に生むものと位置付けている。特にSECのDeFiフロントエンド不処分意見は、具体的な市場機会として捉えている。 --- ## References 1. DeFi Llama — Total Value Locked (TVL) Statistics. https://defillama.com/ 2. Chainalysis — 2025 Crypto Crime Report. Hacking losses data (\$3.4B). 3. Morpho Labs — Protocol metrics and growth data. https://morpho.org/ 4. Hypernative — Company information and product documentation. https://hypernative.io/ 5. Blockaid — Company information and product documentation. 6.3B+ transactions scanned. https://blockaid.io/ 6. GoPlus Security — API documentation and company metrics (\$4.7M revenue, Jan-Oct 2025). https://gopluslabs.io/ 7. U.S. SEC Division of Trading and Markets — Staff Statement on DeFi Front-End Providers (April 13, 2026). 8. European Commission — Markets in Crypto-Assets Regulation (MiCA). 9. Financial Services Agency, Japan — Payment Services Act amendments. 10. European Commission — EU Artificial Intelligence Act. 11. Forta Network — Decentralized threat detection. https://forta.org/ 12. Resolv Incident Report — March 2026. Compromised key exploit — unauthorized minting of 80M USR (\$25M loss). 13. Web3 Security Market — \$2.9B (2025) to \$15.8B (2032 projected, CAGR 26.4%). Source: Electronics Media / Market Research analysis (March 2026). 14. Model Context Protocol (MCP) — Anthropic (2024). https://modelcontextprotocol.io/ --- *Ninja — Agentic Security Controlplane for DeFi & Agentic Finance* *ShoGun — See Through DeFi, Control Agentic Finance* **Disclaimer:** 本ホワイトペーパーは情報提供を目的としたものであり、投資

助言、金融商品の勧誘、またはトークン販売の提案を構成するものではない。記載されている市場データ、競合情報、規制動向は、本稿執筆時点で公開されている情報に基づいており、正確性を保証するものではない。