PRESS RELEASE

報道関係各位

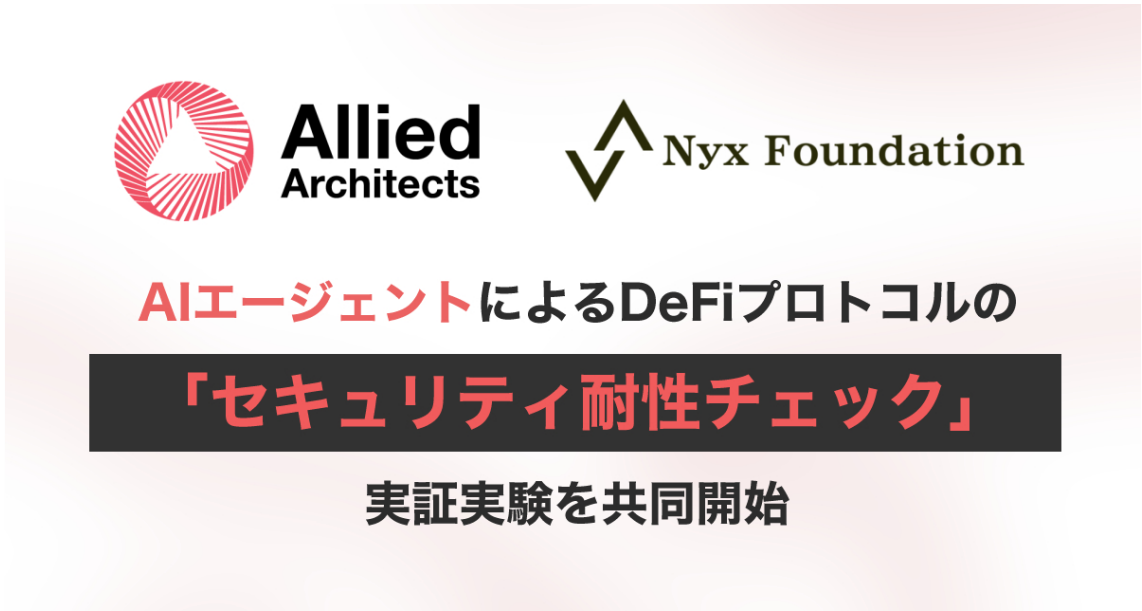
2026 年 6 月 10 日

アライドアーキテクツ株式会社

オンチェーン金融の安全性を高める ― AI エージェントによる DeFi プロトコルの「セキュリティ耐性チェック」実証実験を共同開始

AX の力で企業成長を実現するアライドアーキテクツ株式会社（本社：東京都渋谷区、代表取締役会長：田中 裕志、証券コード：6081、以下「当社」）は、Nyx Foundation と共同で、AI エージェントを活用して DeFi（分散型金融）プロトコルのセキュリティ耐性を検証する実証実験（Proof of Concept、以下「本 PoC」）を開始します。

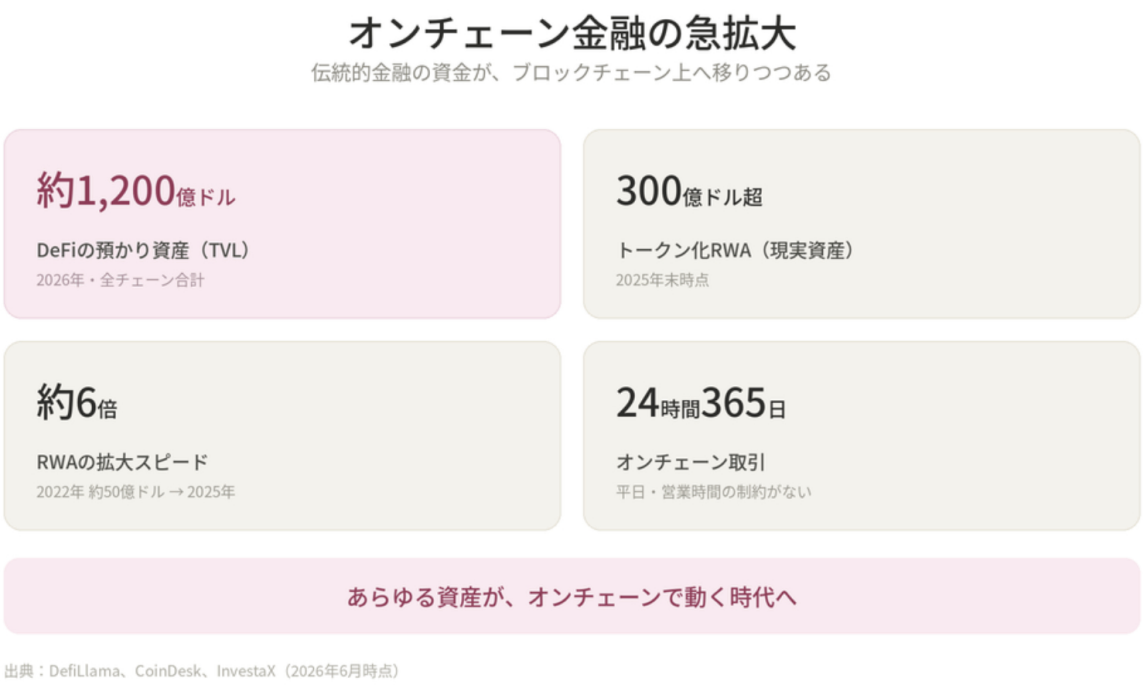
オンチェーン金融（ブロックチェーン上で完結する金融サービス）の市場が急速に拡大し、上場企業や機関投資家の参入も視野に入るなか、その安全性をいかに担保するかが重要な課題となっています。本 PoC では、代表的な DeFi カテゴリーを対象に、AI バグ発見システム「SPECA（Specification-to-Checklist Agentic Auditing）」と形式検証エージェントを用い、属人化せず再現可能な形で、コントラクトのロジックから運用・ガバナンスまでを対象とするセキュリティ評価を実施します。これにより、上場企業や機関投資家が安心してオンチェーン金融に参入できるだけの、客観的で説明可能な安全性の評価手法を確立することを目指します。



■ 背景

オンチェーン金融は近年急速に拡大しています。DeFi に預け入れられた資産（TVL：預かり資産の総額）は 2026 年に全チェーン合計でおおむね 1,000 億～1,700 億ドル規模で推移し、ドル連動のステーブルコインの時価総額は 2026 年 5 月に過去最高の約 3,200 億ドルへと達しました。さらに、トークン化された現実資産（RWA）も 2022 年の約 50 億ドルから 2025 年末には 300 億ドル超へと拡大しており、伝統的金融の資金がオ

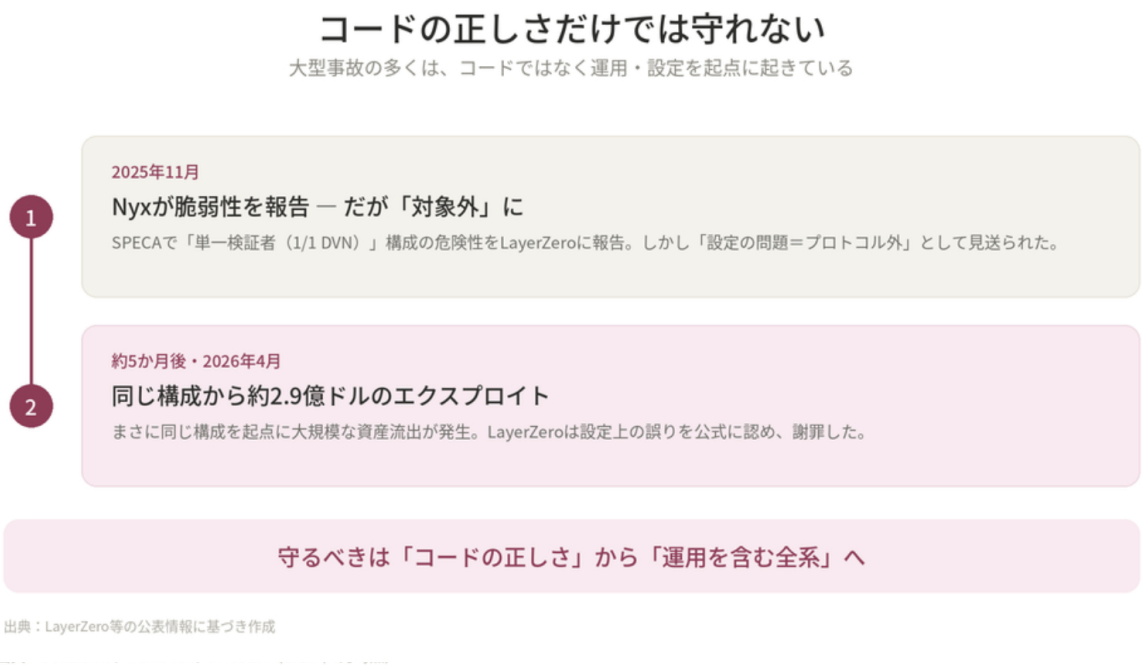
ンチェーンへ移りつつあります。扱われる金額が大きくなるほど、その安全性をいかに担保するかの重要性が増しています。



近年、フロンティア AI の登場で「コードの脆弱性を見つける」作業は急速にコモディティ化する一方、大型事故の多くはコードではなく運用・設定・人間・外部環境を起点に起きています。防御の最前線は「コードの正しさ」から「運用を含む全系を継続的かつ数学的に保証できるか」へと移りつつあり、本 PoC はその最前線への具体的な一歩です。

実際、この問題は現実の事故として表面化しています。2025 年 11 月 Nyx Foundation は「SPECA」を用い、ただ一つの検証者の承認だけで通信が通ってしまう脆弱な「単一検証者（1/1 DVN）」に潜む、偽造メッセージ（正規になりすました不正通信）やリプレイ攻撃（過去の正当な通信を再送して不正処理を繰り返させる手口）の危険性を、異なるブロックチェーンをつなぐ主要な基盤インフラである LayerZero に報告しました。しかし、この指摘は「デプロイ設定の問題（プログラム本体ではなく運用時の設定に起因する＝プロトコル外）」として、対象外と判断されました。

その約 5 か月後の 2026 年 4 月、まさに同じ構成を起点に約 2.9 億ドル規模のエクスプロイトが発生し、LayerZero は設定上の誤りを公式に認め謝罪しています。原因はコードの欠陥ではなく構成・運用にあり、既存のバグバウンティでは捕捉できなかった実例です。



この LayerZero の一件は、コード中心の検証が運用・設定起点のリスクを取りこぼし、その損失規模すら事前に見積もれないことを示しています。そして、これは氷山の一角にすぎません。従来のセキュリティ監査には、より広く次のような構造的課題があります。

- 監査がスポット的・属人的になりやすく、バージョンアップのたびに品質を担保しづらい
- 個々のプロトコルを単体で評価するにとどまり、トレーダーが複数の DeFi を横断して取引する実態に即した「横断的な評価」が行われていない
- 上場企業・機関投資家が参入を検討する際に必要な「最大損失額の定量化（予見性）」や「第三者が検証可能な判断根拠（説明責任）」が十分に提供されていない
-

両社は本 PoC を通じて、「予見性（最大損失額の定量化）」「説明責任（第三者が検証可能な判断根拠）」、および継続的・再現可能な検証による属人性・スポット性の克服について、新たなアプローチの有効性を実証します。一方、複数の DeFi を横断した評価は、本 PoC で蓄積する検証パターンを土台に、次段階以降での確立を目指します。

■ 実証実験の概要

項目	内容
名称	AI エージェントを活用した DeFi プロトコルのセキュリティ耐性チェック実証実験（PoC）
目的	AI エージェントによる網羅的・再現可能なセキュリティ評価の有効性、および上場企業・監査の観点で求められる「予見性・説明責任・ガバナンス・事業継続性」の検証
対象	代表的な DeFi カテゴリーを選定し、一定の網羅性を確保
期間	2026 年内で完了予定
主な手法	AI バグ発見システム「SPECA」／形式検証エージェント／攻撃再現テスト（Red Teaming）

本 PoC で対象とする「代表的な DeFi カテゴリー」は、例えば以下のようなものです。

カテゴリー	内容	代表的なプロトコル例
分散型取引所（DEX／Swap）	トークン同士をその場で交換する	Uniswap、Curve など
レンディング（貸借）	暗号資産を貸し借りして金利を得る	Kamino、Aave など
利回り型ステーブルコイン／合成ドル	オフチェーン資産の利回りをオンチェーンに取り込む	Apyx（apxUSD／apyUSD）など
利回りのトークン化	将来の利回りと元本を分離して取引する	Pendle など

本 PoC では上記のようなカテゴリーの中から代表的なプロトコルを選定し、評価の対象とします。

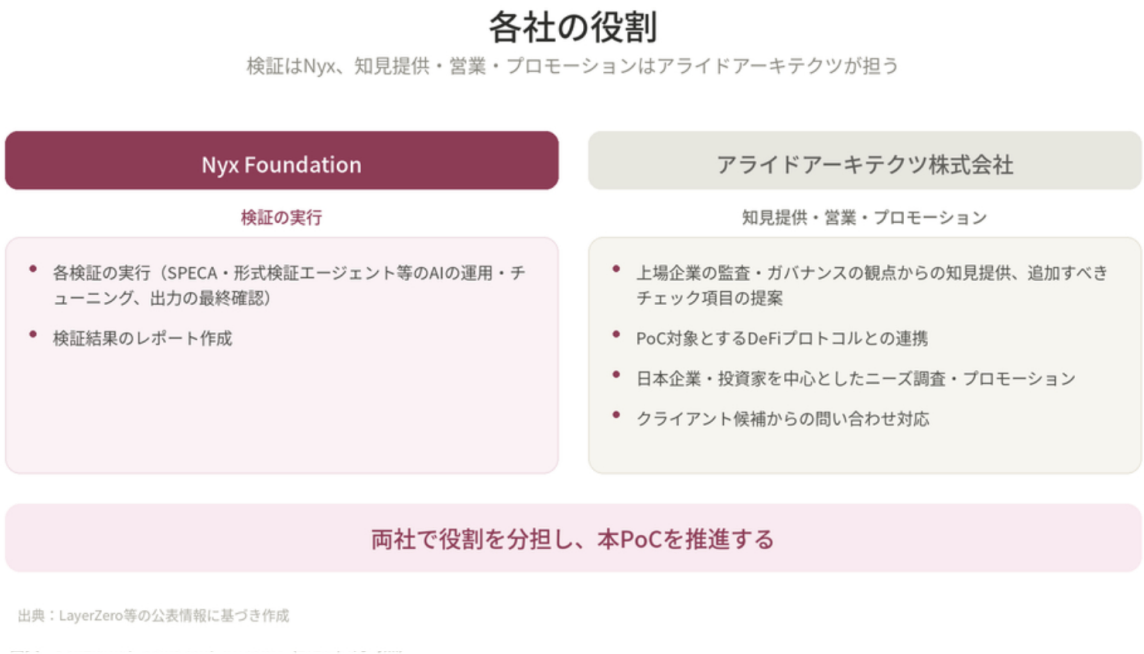
■ PoC におけるチェック項目

本 PoC では、AI バグ発見システム「SPECA」と形式検証エージェントを中心に、各種 AI エージェントを用いて以下の項目をチェックします。各チェックは、上場企業・監査の観点で求められる価値に対応しています。

チェック項目	内容	上場企業・監査の観点での価値
既知バグパターンとの整合性	既知の脆弱性パターンと一致する箇所がないかを確認（週 1 回もしくは月 1 回の定期実施）	継続性：更新のたびに同じ品質を担保し、属人化・単発化を防ぐ
コントラクトロジックの網羅的検証	対象として定義した範囲のプロセスパスを網羅的に検証し、その範囲を明示	網羅性：どこまで検証したかを明確にし、抜け漏れをなくす
ガバナンス・運用面の検証	マルチシグ運用、権限管理、緊急停止（サーキットブレーカー）など、SPECA の対象外となる項目を検証	ガバナンス：緊急時の権限と統制が事前に検証済み 事業継続性：24 時間 365 日でも異常を早期に止められる
形式検証（フォーマル・ベリフィケーション）	脆弱性が疑われる箇所を数学的に証明し、攻撃パターンごとに「証明書」を付与	説明責任：監査対応で「なぜ安全と言えるか」を第三者に示せる
テールリスク（最大損失額）の定量化	検証をすり抜ける攻撃が発生した場合の資産流出額を、発生確率と金額から期待損失として算定	予見性：想定最大損失を数値化でき、保険設計やリスク枠の根拠になる

各チェックの判断プロセスは JSON 形式のログとして記録し、第三者が検証可能な形で証拠化します（追跡可能性）。また、脆弱性が疑われる箇所は攻撃を再現するコード（Proof of Concept）で再現性を確認します。

なお、AI の出力は人間による最終確認を前提とし、最終的な責任は人間が負う体制とします。



■ 各社の役割

Nyx Foundation（検証の実行）

- 各検証の実行（SPECA・形式検証エージェント等の AI の運用・チューニング、および出力の最終確認）
- 検証結果のレポート作成

アライドアーキテクツ株式会社（監査やガバナンスの知見提供、営業、プロモーション）

- 上場企業の監査・ガバナンスの観点からの知見提供、および追加すべきチェック項目の提案
- PoC 対象とする DeFi プロトコルとの連携
- 日本企業・投資家を中心としたニーズ調査およびプロモーション
- クライアント候補からの問い合わせ対応

両社共通

- SNS やイベント等を通じた、新たなセキュリティ耐性チェックの必要性についての啓発・周知

■ 今後の展開

両社は本 PoC の結果を踏まえ、検証パターンの蓄積を通じて、評価を標準化・量産化しながら対象プロトコルを広げ、精度を高めてまいります。あわせて、検証ログ（JSON）や攻撃再現コードを再利用可能な資産として積み上げ、第三者がいつでも検証・追跡できるライブラリとして公開していきます。

こうして安全性の根拠が誰にでも追える形になれば、利用者にとっては、預けた資産がどの程度のリスクに晒されているかが「証明書」として可視化され、より安心して使えるオンチェーン金融に近づきます。両社は、こうした透明性こそが企業・機関投資家・富裕層がオンチェーン金融に参入する際の前提になると捉えており、本 PoC で得た知見を、これらの利用者に向けた新たな事業機会へとつなげていくことを視野に入れています。

＜Nyx Foundation について － イーサリアム財団等と連携する世界水準の研究機関＞

一般社団法人 Nyx Foundation（所在地：東京都文京区）は、イーサリアムブロックチェーンに特化した日本の私設研究機関です。形式検証とセキュリティを専門領域とし、次世代プロトコルの安全性向上に取り組んでいます。活動資金はすべて寄付・研究助成金・スポンサーシップ（30 名超のスポンサー）によって支えられ、イーサリアム財団をはじめ国内外のブロックチェーン企業・大学との連携を進めています。

主な実績

- AI バグ発見システム「SPECA」の開発・公開：独自開発の「SPECA（Specification-to-Checklist Agentic Auditing）」が、イーサリアム財団プロトコルセキュリティ研究チームの助成プログラム「Integrating LLMs into Ethereum Protocol Security Research」に採択。論文・OSS としても公開（arXiv:2604.26495／github.com/NyxFoundation/speca）。
- 形式検証エンジン「Lean Atlas」の公開：形式検証エンジン「Lean Atlas」を論文・OSS として公開（arXiv:2604.16347／github.com/NyxFoundation/lean-atlas）。
- 監査コンペで報告件数 世界第 1 位：100 名超が参加するグローバルな Ethereum セキュリティ監査コンペ（次期大型アップグレード「Fusaka」公開監査コンテスト）において、11 種類のクライアント実装から 17 件の脆弱性を発見し、報告件数で世界第 1 位を獲得。Current Finance 監査コンペでも入賞。
- Ethereum 耐量子移行への参画：ポスト量子署名（XMSS 等）の性能改善・形式検証に貢献し、次世代クライアント「Verity」の開発を推進。
- イーサリアム財団との共同研究：MEV・プライバシー保護技術領域における共同研究を実施。
- 国際的な学術成果：Financial Cryptography 2026 DeFi Workshop での論文採択 など。
- アカデミアからの参画：京都大学 理学部 特定准教授／国立情報学研究所 LLM センター客員准教授の三内顕義氏が Principal AI Scientist として参画。

公式サイト：https://nyx.foundation/

＜アライドアーキテクツ株式会社 会社概要＞

・代表者 ： 代表取締役会長　田中 裕志
　　取締役社長　村岡 弥真人
・所在地 ： 東京都渋谷区恵比寿一丁目 19-15 ウノサワ東急ビル 4 階
・URL ： https://www.aainc.co.jp
・設立 ： 2005 年 8 月 30 日
・事業内容 ：マーケティング AX 支援事業・資産 AX 事業

＜アライドアーキテクツ株式会社とは＞

アライドアーキテクツ株式会社は、従来の事業構造を AI 前提で再設計する AX（AI トランスフォーメーション）を推進し、企業の持続的な成長を実現する AX カンパニーです。

AI を活用したデータ×クリエイティブでマーケティングを変革する「マーケティング AX 事業」と、オンチェーン経済圏における AX を通じて資産価値の向上を目指す「資産 AX 事業」を展開しています。

2005 年の創業以来、6,000 社を超えるマーケティング支援実績と、UGC をはじめとする顧客の声データ資産、独自開発の SaaS・AI 技術を蓄積。戦略立案からクリエイティブ、運用、開発までを担うデジタル・AI 人材を結集し、自らを変革し続ける企画者・創造者の集団として、「世界中の人と企業の創造がめぐる社会」を目指して、挑み続けています。

＊ 本プレスリリースに記載している会社名および商品・サービス名は各社の商標または登録商標です。

【リリースに関するお問い合わせ先】

アライドアーキテクツ株式会社　経営企画室　広報担当
TEL：03-6408-2791　　MAIL：press@aainc.co.jp