Press Release

報道関係者各位

2026 年 7 月 23 日
株式会社デジタルハーツホールディングス

AGEST、米 Lazarus 社との共同開発を通じた「自律型 AI による包括的サイバーセキュリティプラットフォーム『AGEST ZERO SHIELD』」の商用化に向けた PoC 提供を開始

株式会社デジタルハーツホールディングス(本社所在地：東京都新宿区、代表取締役社長 CEO：筑紫 敏矢、東証プライム：証券コード 3676) の子会社で、先端品質テクノロジーを活用してソフトウェアの品質・安全性向上を支援する株式会社 AGEST(本社所在地：東京都文京区、代表取締役 社長執行役員 CEO：二宮 康真、以下、「AGEST」)はこの度、2026 年 6 月 10 日にお知らせした米国の Lazarus Enterprises, Inc.(以下、「Lazarus 社」)との共同開発を通じた「自律型 AI による包括的サイバーセキュリティプラットフォーム」の商用化に向けた PoC を 2026 年 7 月末から開始することをお知らせいたします。

＜昨今のサイバーセキュリティ動向及び企業・組織の課題＞

先般発表された「Claude Mythos Preview(以下、「Mythos」)※1」に代表される高度な AI フロンティアモデルなどの登場に伴い、AI を活用した攻撃・防御の双方が高度化するなど、サイバーセキュリティを取り巻く環境は大きく変化しています。

企業や組織にとっての守備側の視点では、こうした新たなサイバー脅威への防御能力の継続的な強化が、事業継続や企業の信頼性を支える重要な経営課題となっています。

株式会社デジタルハーツホールディングス
〒163-1441 東京都新宿区西新宿三丁目 20 番 2 号 東京オペラシティビル 41 階
https://www.digitalhearts-hd.com/

その一方、高度な AI モデルを活用したセキュリティ対策では、
・API 経由でのソースコードの外部送信リスク(データ主権上の懸念)
・フルスキャン機会の増大などトラフィックの急増に伴う高額なトークン課金負担
・Mythos などフロンティア AI モデル利用のための条件ハードルや輸出規制などに伴う突然の利用停止リスク
・利用による高速／高頻度なアラートへの対応、アラート疲労リスク
などの課題を含んでいます。また、高度な AI を攻撃者が利用する一方で、守備側である企業や組織などでは幾重にも施された安全施策(ガードレール)に阻まれ、正規の手順では攻撃者視点でのコード検証が進まない非対称性が懸念されています。

＜『AGEST ZERO SHIELD』及び PoC 開始について＞

AGEST はこれらの課題を継続的に解決するソリューションとして「自律型 AI による包括的サイバーセキュリティプラットフォーム『AGEST ZERO SHIELD』」を Lazarus 社と共同開発し、その第 1 弾として、フロンティア AI 同様のゼロデイ脆弱性検知、発見された脆弱性に対するパッチまたはコード修正の提案機能を含めた「ゼロデイ脆弱性ハンティング」機能の 2026 年 9 月の商用化に向けた準備を進めています。

『AGEST ZERO SHIELD』の特徴
・オンプレミス／閉域環境設置によるデータ主権を確保しながらの利用が可能
※フロンティア AI などのように海外企業へのソースコード送信を行いません
・トークンベースではない、年間ライセンス固定課金方式
・サイバーセキュリティに特化した AI モデルを継続的にバージョンアップ提供予定

また Lazarus 社と AGEST による独自ハーネスと LLM チューニングによる高い脆弱性ハンティング機能を持ち、AGEST による検証では、Mythos の例でも挙げられる「FFmpeg H.264 のスライスカウンター脆弱性※2」、また一例として以下のような従来では発見できていなかった脆弱性を発見できています。

■実際に検知した脆弱性の一例

CVE	ANT-CVD	Date	CVSS	Lang	説明
CVE-2026-28208	ANT-2026-9VJ9JJXQ	2026/2/26	5.9	Java	Junrar has arbitrary file write due to backslash path traversal bypass in LocalFolderExtractor on Linux/Unix
CVE-2026-32316	ANT-2026-EBDTPNVH	2026/4/13	7.5	C	jq: Integer overflow in jvp_string_append() allows Heap-based Buffer Overflow
CVE-2026-40034	ANT-2026-6SNS6KMP	2026/5/26	7.3	Rust	gitoxide - Command Injection via Partial .gitmodules Override in gix-submodule
CVE-2026-27775	-	2026/7/3	8.8	Go	Gitea pre-receive hook permission cache allows full repository write access

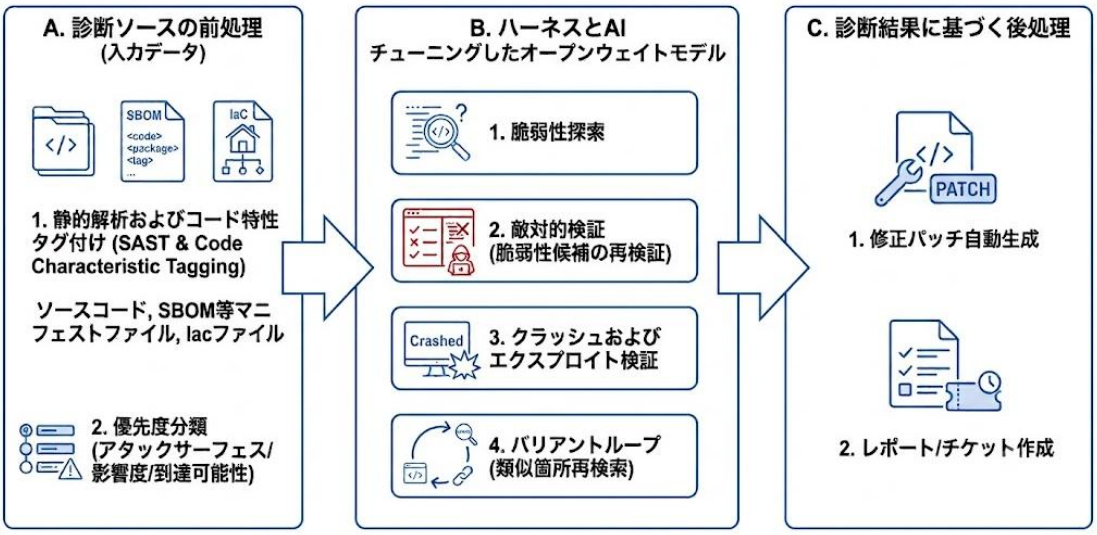
※CVE：CVE(Common Vulnerabilities and Exposures)は、システムやソフトウェアに一般公開されているセキュリティ上の脆弱性(欠陥)を識別するためにつけられる世界共通の識別番号

※ANT CVD:脆弱性を適切に修正・公開する制度である Coordinated Vulnerability Disclosure (CVD)識別番号であり、Anthropic PBC が発見した場合は ANT の識別子が付与されるが、単体の脆弱性情報として公開されない場合もある

株式会社デジタルハーツホールディングス
〒163-1441 東京都新宿区西新宿三丁目 20 番 2 号 東京オペラシティビル 41 階
https://www.digitalhearts-hd.com/

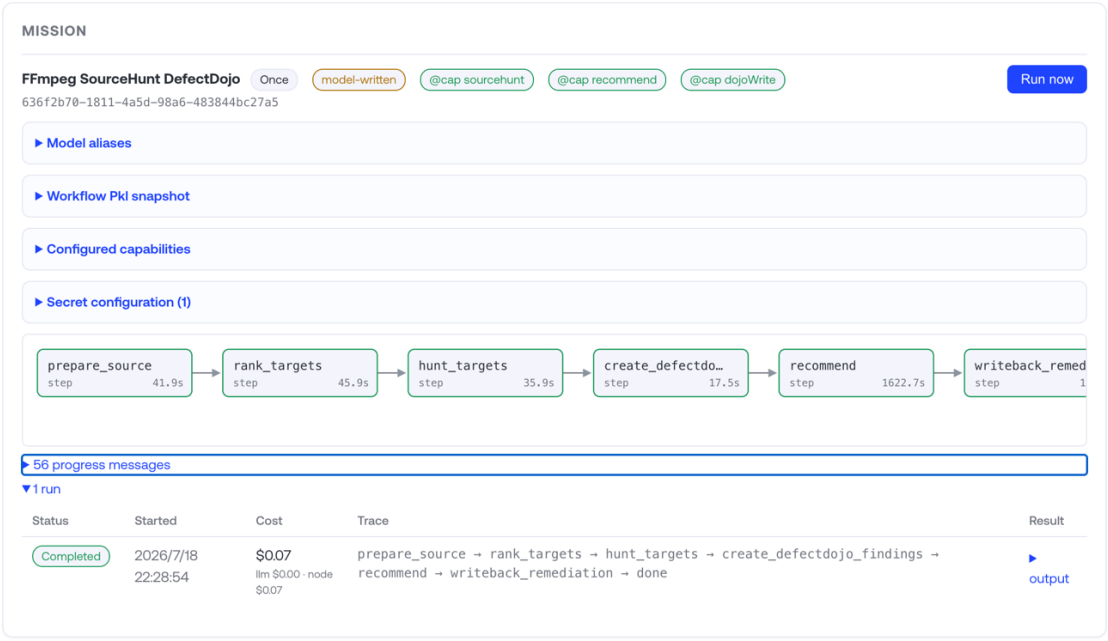
※CVSS: CVSS(共通脆弱性評価システム)は、情報システムやソフトウェアのセキュリティ脆弱性の深刻度を 0.0～10.0 のスコアで定量化する国際的な業界標準指標であり、スコアが高いほど危険度が増し、組織が脆弱性対応の優先度を判断するために活用される。近年エクスプロイトチェーン(Exploit Chain)と呼ばれる、攻撃者がシステムの制御権を奪うなどの最終目標を達成するために、複数の脆弱性(セキュリティホール)に対する攻撃コードを順番に連鎖(チェーン)させて実行するサイバー攻撃の手法が出現してきており、単体では脅威の低い軽微な脆弱性であっても、それらを巧妙に組み合わせることで、最終的にシステム最深部の権限を奪取できるなどの攻撃手法が明らかになっており CVSS スコアの脅威度だけで判断できなくなってきている

■ゼロデイ脆弱性ハンティングの流れ



各処理は複数回ループ処理することでハルシネーション抑止と再現性向上を担保します

■脆弱性検知画面のイメージ



株式会社デジタルハーツホールディングス
〒163-1441 東京都新宿区西新宿三丁目 20 番 2 号 東京オペラシティビル 41 階
https://www.digitalhearts-hd.com/

こうした成果を、実際のお客様環境へ導入し商用化に向けた様々な検証を行うため、AGEST ではこれまで協議を進めている国内主要 SIer 様を中心としたパートナー各社との PoC を今月末より開始いたします。

＜今後の取り組みについて＞

各社様から多くの引き合いを受け、今回実施予定の PoC については既に受付を終了しており、今後この PoC 実施や商用化に向けた継続的な協議を行い、『AGEST ZERO SHIELD』の導入を広く推進するための導入コンサルティングパートナー・ハードウェア調達パートナー様などのパートナーシップエコシステム構築を進めてまいります。

商用化のスケジュールや追加機能などの詳細については今後順次情報公開を行ってまいります。

＜追加予定機能＞

・ライブターゲットのモニタリング機能(CNAP 相当機能)
・ライブターゲットの各種ログ解析によるセキュリティ侵害の検出
・自律 AI によるペネトレーションテスト
・オフェンシブサイバー統制機能

※1　Anthropic PBC が限定提供している高度 AI モデルであり、特にゼロデイ脆弱性検出・脆弱性解析・攻撃経路生成などのサイバーセキュリティ領域に特化したフロンティアモデル

※2　Project Glasswing の成果として FFmpeg の H.264 スライスカウンターに 16 年間潜んでいた脆弱性を検出したもの(CVE 番号などは発番されておらず「h.264 slice counter mismatch または 0xFFFF sentinel collision」の名称で呼ばれる問題)

以上

※ すべてのブランド、製品名、会社名、商標、サービスマークは各社に権利が帰属します。

【AGEST について】
AGEST は、「先端品質テクノロジーで、すべての DX に豊かな価値と体験を」をビジョンに掲げ、先端テクノロジーの研究や最新技術に対応した QA テックリード人材の育成を推進し、次世代 QA ソリューションの提供を通じて、高度デジタル社会の発展に貢献しています。
https://agest.co.jp

【報道関係者からのお問い合わせ】
株式会社 AGEST　IR 広報室　広報担当
Mail:ml-pr@agest.co.jp
Tel: 03-6821-1753