2026 年 6 月 29 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai、NVIDIA との協業で AI ファクトリー内部にセキュリティを実装

Akamai Guardicore Segmentation と NVIDIA DOCA が、
NVIDIA Vera BlueField-4 STX 上で、AI ファクトリーのデータ、コンテキストメモリ、
およびエージェント型 AI ワークロードに対するリアルタイムのゼロトラスト制御を可能に

※本リリースは 2026 年 6 月 2 日(現地時間) 米国マサチューセッツ州ケンブリッジで発表されたプレスリリースの抄訳版です。

Akamai（NASDAQ：AKAM）は、NVIDIA と連携し、AI エージェントが普及するエージェンティック時代の基礎となる高度なセキュリティアーキテクチャを AI ファクトリーに導入します。

Akamai と NVIDIA は、セキュリティ面の連携を拡張し、NVIDIA DOCA ソフトウェアプラットフォームを基盤とする NVIDIA Vera BlueField-4 STX ストレージアーキテクチャに Akamai Guardicore Segmentation を組み入れることを発表しました。この連携は、ゼロトラスト・アーキテクチャのレイヤーを AI ファクトリー自体に組み込むことで、データ、コンテキストメモリ、自律型エージェントを保護することを目的としています。

この画期的なセキュリティ統合により、AI ファクトリーの運用者は、AI ワークロードが依存する GPU、CPU、またはストレージの処理サイクルに負荷をかけることなく、アクセラレーテッドコンピューティングの高速性を維持しながら、ワークロードを認識したセグメンテーションを適用し、エージェントのふるまいを監視し、脅威をインフラストラクチャ層で封じ込めることができます。

Akamai の Enterprise Security 担当 Senior Vice President、Ofer Wolf は「AI ファクトリーは企業にとって極めて重要な資産になりつつあり、特に最新のフロンティア LLM を悪用したサイバー攻撃がそのスピードと規模を増大させていることから、脅威の封じ込めを前提に設計される必要があります」「クロックサイクルが重要な環境において、従来のホストベースのセキュリティツールは、サーキット上のスピードバンプ（減速帯）のように速度低下の要因になってしまいます。ワークロードを認識するセグメンテーションを NVIDIA Vera BlueField-4 STX および NVIDIA DOCA に移行することで、AI ワークロード本来のスピードでゼロトラストを適用し、脅威がハイパフォーマンスな環境に拡散する前に、封じ込められるよう支援します」」と述べています

また、NVIDIA の Networking 担当 Senior Vice President、Kevin Deierling 氏は「データはエージェンティック AI ファクトリーの基盤であり、自律的な意思決定を支えるインテリジェンスの源泉です。企業にとってこれまで以上に堅牢な保護が重要になっています」「Akamai Guardicore エンタープライズ・セキュリティ・プラットフォームと NVIDIA Vera BlueField-4 STX は、インフラファブリックにゼロトラストの保護レイヤーを直接組み込み、AI ワークロードの大規模な通信をインテリジェントに制御することで企業データを保護します」と述べています。

高速処理で実現するセキュリティ

AI ファクトリーは、セキュリティ対策が追いつかないほどの速さで構築されています。これまで、AI のスピードと AI のセキュリティの間にはトレードオフが存在していました。しかし、もはやそのような妥協は許されません。

Akamai と NVIDIA の統合の拡張は、両社が今年 2 月に発表したアーキテクチャ合意に基づいて実現したもので、このトレードオフを解消するために設計されています。

Akamai Guardicore Segmentation は、世界最大規模かつ最も機密性の高い組織を保護しており、データセンター、クラウドインフラ、Kubernetes クラスター、エッジシステムを含むハイブリッド環境全体でワークロード、アプリケーション、およびデータがどのようにやり取りしているかを継続的にマッピングするインテリジェンスレイヤーを提供します。ポリシーは、静的なネットワークアドレスではなく、ワークロードのアイデンティティ、アプリケーションのコンテキスト、およびランタイムでのふるまいに基づいて定義されます。AI ワークロードのライフサイクル全体を可視化することで、異常なパターンや機微な情報への不正アクセスを明らかにします。

NVIDIA DOCA を介してプログラム可能な NVIDIA Vera BlueField-4 STX は、シリコン上で脅威検知レイヤーと適用レイヤーを構築します。セキュリティポリシーは、ホストではなくインフラストラクチャファブリック内のデータパスに、ラインスピードで適用されます。そして、ワークロード自体に近い場所でポリシー適用が行われるようになります。そのため、AI ファクトリーが依存する GPU、CPU、ストレージプロセッサーの処理を阻害することはありません。2 層のレイヤーが連携して、アイデンティティベースのゼロトラストを、追加製品ではなくインフラストラクチャそのものの特性として確立します。

統合の仕組み

この統合ソリューションは、ポリシーの適用に先だって、インテリジェンスを得る必要があるという原則に基づいて運用されます。

- **可視性**
  - Akamai Guardicore Segmentation は、データセンター、クラウド、Kubernetes、エッジシステム間の通信関係を継続的にマッピングします。エージェントレスのアーキテクチャにより、トレーニングパイプライン、推論サービス、データ・インジェスト・システム、オーケストレーションプラットフォームを含む AI ワークロードを、それらに干渉することなく監視します。

- **ポリシー**
  - ワークロードのアイデンティティ、アプリケーションのコンテキスト、およびランタイムでのふるまいを用いて、明示的な通信コミュニケーションポリシーを定義します。例えば、プリプロセッシングノードはデータセットおよびトレーニングサービスにアクセスできますが、その範囲を超えたアクセスはできません。研究環境は、本番環境の推論から明確に分離されます。ポリシーの境界を損なうことなくポッドをスケーリングし、サービスを進化させることが可能です。

- **適用**
  - NVIDIA DOCA は、これらのポリシーを、BlueField-4 が内蔵するシリコンのデータパスにラインスピードで適用します。セグメンテーション、テレメトリー、異常検知、感染したシステムの分離などのセキュリティ機能は、ホストではなくインフラファブリック内で実行されます。

- **封じ込め**
  - ワークロードが侵害された場合でも、その影響範囲は環境内の小さく特定されたセグメントに制限されます。AI ファクトリーの残りの部分は中断なく動作し続けます。

提供開始時期

NVIDIA BlueField および NVIDIA DOCA と統合された Akamai Guardicore Segmentation は、2026 年後半に、AI ファクトリーでのワークロード認識型セグメンテーションの実装向けに提供開始される予定です。また、Akamai と NVIDIA Vera BlueField-4 STX の統合ソリューションは、2027 年前半にストレージおよびインフラ・パートナー・プラットフォームで提供開始予定です。

Akamai について

Akamai は、オンラインビジネスの力となり、守るサイバーセキュリティおよびクラウドコンピューティング企業です。当社の市場をリードするセキュリティソリューション、優れた脅威インテリジェンス、グローバル運用チームによって、あらゆる場所でエンタープライズデータとアプリケーションを保護する多層防御を利用いただけます。Akamai のフルスタック・クラウド・コンピューティング・ソリューションは、世界で最も分散化されたプラットフォームで高いパフォーマンスとコストを実現しています。多くのグローバル企業が、ビジネスの成長に必要な業界最高レベルの信頼性、拡張性、専門知識を提供できる Akamai に信頼を寄せています。詳細については、akamai.com および akamai.com/blog をご覧いただくか、X や LinkedIn で Akamai Technologies をフォローしてください。