

## Akamai、NVIDIA の技術を活用した エージェントレス・ゼロトラスト・セグメンテーションにより 重要インフラのセキュリティを強化

Akamai Guardicore Segmentation と NVIDIA BlueField の統合により、  
エネルギー・製造・運輸セクターにおいて、  
これまで難しいとされてきたセキュリティ強化とシステム性能の両立を実現

※本リリースは 2026 年 2 月 23 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。

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、[Akamai Technologies](#) (NASDAQ : AKAM) は、巧妙化するサイバー攻撃から最も重要なシステムを保護するために、NVIDIA の技術を活用した新しいソリューションを発表しました。[Akamai Guardicore Segmentation](#) と [NVIDIA BlueField Data Processing Units](#) (DPU) を組み合わせることで、エージェントを導入できない産業機器、現代社会を支える重機や制御システムを含む、オペレーショナルテクノロジー (OT) および産業用制御システム (ICS) の全領域をサポートする方法を提供します。企業はこのハードウェアから分離された「エージェントレス」のセキュリティアプローチを実装することで、厳格な新しい規制要件への準拠や、サイバー保険におけるリスクプロファイルの改善を図ることが可能になります。

重要インフラの保護は、歴史的に困難な課題でした。多くのサイバーセキュリティツールは、コンピューターに「エージェント」と呼ばれる軽量なソフトウェアをインストールする必要があります。しかし、サイバー攻撃の脅威がミッションクリティカルな環境を標的にすることが増える中で、企業は水処理プラント、送電網、工場などで使用される特殊なコントローラーなどの重要な資産を保護するための、より優れた方法を模索しています。これらのシステムの多くは、追加のソフトウェアを実行するには古すぎるか、あるいは非常に繊細であるため、ソフトウェアを動かすとシステムダウンや生産速度低下のリスクを伴います。その結果、多くの組織は機密性の高いインフラを脆弱なまま放置せざるを得ない状況にありました。

この共同ソリューションでは、ユーザーが設定可能なセキュリティプロセスをホストシステムから NVIDIA BlueField DPU にオフロードすることで、脆弱なシステムやレガシーシステムにエージェントをインストールすることなく、ゼロトラストセグメンテーションを実現します。業務を中断することなく、システム、ネットワーク、およびアプリケーション全体にわたる詳細な「アウトオブバンド (帯域外)」の可視性を提供します。セキュリティポリシーをリアルタイムで適用し、重要な運用システムの周囲に強力な保護境界を構築することが可能です。その結果、運用アクティビティに対する信頼性の高いインサイトが得られ、全体的なサイバーレジリエンスが向上します。



セグメンテーションに加えて、このソリューションは異常なネットワーク接続や侵害の痕跡（IoC）を特定することもできます。エージェントレスのアプローチにより、ハードウェアレベルで脅威をフィルタリングし、侵害されたシステムを隔離できるため、施設のメインコンピューターが侵害された場合でも、脅威の拡散を抑制・阻止できます。NVIDIA BlueField が独立した「バンプ・イン・ザ・ワイヤー（ネットワーク経路上の独立した保護デバイス）」として機能するため、システムパフォーマンスや機械自体の稼働時間に最小限の影響で、機密性の高い産業機器をロックダウンできます。

Akamai の Enterprise Security 担当 Senior Vice President の Ofer Wolf は「水処理プラントを運営していようと、ハイパフォーマンス・コンピューティング（HPC）クラスターを運用していようと、最優先事項はシステムをフルスピードで動かし続けることです。セキュリティソフトウェアによってパフォーマンスに負荷をかけるわけにはいきません」「かつて、これらの環境を保護するのは極めて困難でした。マシンが従来のツールのオーバーヘッドに耐えられず、システムダウンや重要な計算のスローダウンを招くリスクがあったからです。Akamai と NVIDIA はそれを変えようとしています。セグメンテーションと可視化を DPU にオフロードすることで、CPU のパワーを本来の目的である重い処理に最大限活用しながら、攻撃を阻止する手段を提供します。」と述べています。

NVIDIA の Networking 担当 Senior Vice President である Kevin Deierling 氏は「AI はあらゆるビジネスを根本から再構築しており、自動化が拡大する中で、企業のデータとリソースを保護することは極めて重要です。しかし、セキュリティが稼働率やレジリエンスを犠牲にしてはなりません」「Akamai のセグメンテーション機能を NVIDIA BlueField に直接統合することで、企業はシステムの安定性や生産能力に影響を与えることなく、インフラ層でゼロトラストを適用し、最も機密性の高い業務を保護できるようになります。」と述べています。

Akamai と NVIDIA のこのコラボレーションは、極めて重要な時期に実現しました。米国連邦政府による[最近の評価](#)では、エネルギーおよび運輸セクターが、広範囲にわたる混乱をもたらそうとする攻撃者にとって主要な標的となっていることが強調されています。

この共同ソリューションは、2026 年第 2 四半期に全世界で提供開始される予定です。Akamai Guardicore Segmentation と NVIDIA BlueField の統合の詳細については、[Akamai のブログ](#)および[NVIDIA のブログ](#)をご覧ください。

## 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](https://akamai.com) および [akamai.com/blog](https://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。



※Akamai と Akamai ロゴは、Akamai Technologies Inc.の商標または登録商標です  
※その他、記載されている会社名ならびに組織名、ロゴ、サービス名は、各社の商標または登録商標です  
※本プレスリリースの内容は、個別の事例に基づくものであり、個々の状況により変動するものです