2023 年 4 月 12 日

*Press Release*

アカマイ・テクノロジーズ合同会社

# Akamai Technologies、新たな脅威ハンティングサービスで ゼロトラストの導入を推進

## Akamai Hunt と Akamai Agentless Segmentation により、

### アタックサーフェスの縮小と修復時間の短縮を支援

※本リリースは 2023 年 3 月 7 日 (現地時間) 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。

オンラインライフの力となり、守るクラウド企業、Akamai Technologies, Inc.（NASDAQ：AKAM）は、Akamai Hunt セキュリティサービスを発表しました。これらは、Akamai がリーダーとして認知されているマイクロセグメンテーションに更なる価値を与える新機能です。このサービスにより、お客様は Akamai Guardicore Segmentation のインフラ、Akamai がもたらすグローバルな攻撃可視性、セキュリティ専門研究者を活用して、自社環境内できわめて巧妙に検知を逃れようとする脅威とリスクを能動的に検知し、迅速に対処することができます。Akamai は同時に、Agentless Segmentation もリリースしました。これを利用することで、Akamai Guardicore Segmentation のお客様はホストベースのセキュリティソフトウェアを実行できない接続された IoT デバイスや OT デバイスにゼロトラストの利点を拡張できます。

企業がデジタルトランスフォーメーションを推進し、ワークフォースが進化し続けている中で、ランサムウェアなどの高度な攻撃は依然として事業継続性やブランドの総合的な信頼に対する脅威となっており、2021 年だけでも 200 億ドルを超えるコストが発生しました。このような脅威に対処するために、IT 管理者はゼロトラスト・フレームワークとマイクロセグメンテーションによってネットワーク、知的財産、従業員を保護する新しいアプローチを採用し、ネットワーク内のラテラルムーブメント（水平方向の移動）を阻止する必要があります。

「マイクロセグメンテーションは、複雑で動的な環境においてアタックサーフェスを大幅に縮小することによって、ランサムウェアなどの攻撃を防ぐことが実証されています」と、Akamai の Enterprise Security 担当 Senior Vice President 兼 General Manager である Pavel Gurvich は述べています。「今回発表した Akamai Guardicore Segmentation のお客様向けの新しいサービスは、従来はセキュリティを確保することが困難だったデバイスにまで保護を拡張し、きわめて巧妙に検知を逃れようとする脅威を排除するために必要な可視性と分析を提供します」

**Akamai Hunt**

Akamai Hunt は、Akamai Guardicore Segmentation のセグメンテーション機能を、世界のインターネットトラフィックの多くを配信する Akamai が所有しているデータと組み合わせます。

これにより、お客様は自社環境内の脅威を排除し、仮想的に脆弱性にパッチを適用し、IT の安全性を向上させることができます。その他にも次のようなメリットがあります。

- **独自のデータセット：**顧客の環境からの豊富なテレメトリが優先的なグローバル脅威データと相互に関連付けられるため、Hunt は検知を逃れようとする脅威とリスクを見つけることができます。
- **ビッグデータ分析：**大量のデータを相互に関連付けてクエリを実行し、他のツールでは見逃す可能性のある疑わしい活動や異常な活動がないか分析します。
- **エキスパートの調査：**専任のセキュリティエキスパートが検知結果を調査し、フォールス・ポジティブ（誤検知）によってチームが混乱しないようにします。
- **アラートと月次レポート：**詳細アラートによって緩和のために必要な情報を提供し、月次レポートによってエグゼクティブサマリーを提供します。
- **緩和ガイド：**Hunt のエキスパートが脅威への対処、脆弱性に対するパッチ適用、および IT インフラの強化を支援します。

**Akamai Agentless Segmentation**

IoT デバイスと OT デバイスのセキュリティ確保は、従来から多くの企業にとって課題となっています。Akamai Agentless Segmentation を使用することで、企業はアタックサーフェスを縮小し、ホストベースのセキュリティソフトウェアを実行できないデバイスにもゼロトラストポリシーを適用できます。その他にも次のような機能があります。

- **継続的なデバイス検出：**新たにネットワークに接続されたデバイスを自動的に検出し、事前定義されたデバイス・オンボーディング・ワークフローを実行します。
- **統合デバイスフィンガープリンティング：**接続されているすべてのデバイスを特定、評価、分類し、適切なセキュリティポリシーが適用されていることを確認します。
- **エンタープライズ資産の可視化：**エンタープライズ全体の IoT デバイスと OT デバイス、トラフィック、さらにはエンドポイント、サーバー、クラウド資産とのインタラクションを確認できます。
- **エージェントレスのゼロトラスト・セグメンテーション：**ネットワーク制御ポイントと直接統合することで、エージェントレスの最小権限のセグメンテーションポリシーを適用し、疑わしいデバイスを隔離します。
- **ローミングデバイスの認識：**デバイスが有線ネットワークインフラと無線ネットワークインフラの異なる領域間を移動する際に、デバイスの可視性、コンテキスト、制御を維持します。

Akamai Agentless Segmentation は、2023 年第 2 四半期より Akamai Guardicore Segmentation のお客様向けに利用可能になります。

**Akamai について：**

Akamai はオンラインライフの力となり、守っています。世界中のトップ企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、いつでもどこでも、世界中の人々の人生をより豊かにしています。広範に分散したエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com/ja および akamai.com および akamai.com/blog をご覧いただくか、Twitter と 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しうるものです