2025 年 6 月 4 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai、DNS セキュリティとコンプライアンスの課題に対処する 業界初の DNS Posture Management

複数の DNS プロバイダーに渡り統合された可視性とリアルタイム監視を提供、 DNS ベースの攻撃を防ぐ

※本リリースは 2025 年 6 月 3 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, Inc.（NASDAQ：AKAM）は、Akamai DNS Posture Management を発表しました。これは、すべての DNS 資産に対して、複数の DNS プロバイダーにわたり統合された可視性を提供する、業界初のソリューションです。このエージェントレスなソリューションは、すべての主要な DNS プロバイダー上で企業が運用している DNS アセットに潜んでいるセキュリティ設定上の問題点について、リアルタイム監視と修復のためのガイダンスを提供します。セキュリティチームは、DNS ベースの攻撃、証明書のセキュリティリスク、脆弱性、および組織のセキュリティポスチャを弱体化する誤設定を迅速に検知し、対応することが可能になります。

DNS は、コンピューター、サービス、およびその他のリソースがインターネットや他の IP ネットワークを介して相互に検索し、接続できるようにする上で重要な役割を果たします。DNS はこれらのネットワークを運用する際に欠かせない部分です。しかし、残念ながら、DNS はサイバー攻撃の標的にもなっています。年初には、日本の複数の中央省庁、自治体のサイトで利用されなくなったサイトのサブドメイン名の設定が放置されたことにより、第三者に乗っ取られる可能性があったことが外部からの指摘で明らかになりました。同様の脆弱な設定の潜在的な問題は、日本国内の民間企業でも起きています。

多くの大規模な組織では、さまざまなベンダーの複数の DNS システムを管理して、インターネットのプレゼンスと企業が管理するドメインの名前解決をサポートしています。このような複雑さから、IT チームは、すべての DNS ソリューションがネットワークの変更に対応するように調整し、機能、パフォーマンス、セキュリティを適切に構成する必要があります。ただし、DNS 設定（およびレコードとゾーンデータ）が古くなると不完全になる可能性があり、ドメイン名を含む証明書が期限切れになったり、近い将来に耐量子化の観点からコンプライアンスを満たさなくなる可能性があります。

管理されていないアラートや DNS に関するコンプライアンス要件の数が膨大なため、セキュリティ担当者は重大なリスクに直面しています。自動化および合理化されたワークフローがなければ、優先度の高い問題も容易に見落とされてしまうことがあります。コンプライアンス評価を自動化し、その結果をインシデント管理に統合することが、セキュリティと効率性を維持する上で重要になります。

Akamai のインフラ・セキュリティ・ソリューション & サービス担当 SVP 兼 General Manager である Sean Lyons は「DNS セキュリティは見過ごされがちですが、ビジネスのセキュリティを確保し、円滑に事業を継続するために不可欠なものです」「多くの組織にとって、課題は DNS の設定作業ではなく、すべてのシステムが実際に正しく設定されており、セキュリティを十分に確保できているのかどうかを把握することです。このような組織にとって本当に必要なのは、DNS 環境全体で何が起きているかを把握して、迅速に対処するシンプルな方法です。これが、私たちが DNS Posture Management で解決しようとしている課題です。セキュリティ担当者は、優先順位の高い問題点を早期に特定し、コンプライアンスを維持し、ネットワークのパフォーマンスを最大限に高めるために役立つ、明確で統一されたビューを得ることができます」と述べています。

ドメインはしばしば、既知の高リスクの脆弱性や誤設定を外部に晒してしまいます。こうした弱点は、DNS の継続的な稼働と名前解決の信頼性に影響を与え、認証されていない SSL／TLS 証明書の発行や DNS スプーフィング、キャッシュポイズニングなどの重大な脅威に対する脆弱性を高めるおそれがあります。そして、脅威アクターが、詐欺、データ窃盗、フィッシングなどの目的で組織のブランドを模倣した偽の Web サイトを作成することを目的に、企業や組織が管理する DNS を乗っ取り、悪用する可能性があります。そのほか、攻撃者が DNS 全体を停止させ、ビジネスや顧客のネットワークサービスの停止を引き起こす脆弱性もあります。

これらの潜在的な攻撃ベクトルが DNS と証明書のセキュリティ衛生上の重大なギャップを浮き彫りにし、継続的なコンプライアンス監視の必要性が高まっています。Akamai の DNS Posture Management は、今日の企業が、拡大する規制要件に対応するために不可欠なコンプライアンス機能を提供します。NIST、PCI DSS、HIPAA などの重要なセキュリティフレームワークへの準拠を自動化することで、組織はセキュリティポスチャを強化しながら、コンプライアンスに関わるコストの大幅な削減を実現することができます。

Akamai DNS Posture Management は、デジタル証明書をドメイン名ごとに整理する Certificate Monitor を統合しており、期限切れ、誤設定、不正な証明書などのセキュリティリスクを特定して防止します。また、これらの証明書を使用しているドメインの HTTP ポスチャも提示します。

さらに、Akamai DNS Posture Management は、主要な DNS プロバイダー全て（Akamai Cloud、AWS、Microsoft Azure、Google Cloud Platform など）を含むゾーン、ドメイン、サブドメイン、レコードを把握するための総合的な視点を提供します。

Akamai は、オプションとして、専門知識を持ち、グローバルでスケーラブルな 24 時間年中無休で対応する社内チームを強化した Managed Security Service も用意しています。これは、組織が Akamai DNS Posture Management の価値を最大限に活用できるように支援するサービスです。

Akamai DNS Posture Management の詳細と、攻撃から組織を保護するために Akamai がどのように役立つかをご確認ください。

# # #

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 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。

※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