データシート

# A10 Defend Threat Control

## いま必要とされるプロアクティブなDDoS攻撃インテリジェンス

A10 Defend Suiteの構成要素の1つであるA10 Defend Threat Controlは、複雑さも規模も増大するDDoS脅威に対抗するために必要な機能です。DDoS武器のプロアクティブかつ詳細なリストを、組織にとって実用的なインサイトとして提供します。組織は、DDoS攻撃を開始または加担する可能性のある悪意のあるIPをブロックし、DDoS攻撃を阻止することができます。

## DDoS：エスカレートする脅威

DDoS攻撃を過小評価しないでください。誇大宣伝もなく話題にもなっていないかもしれませんが、DDoS攻撃は絶え間なく続いています。現在、IoTデバイスの普及、システムの稼働時間・可用性、企業ブランドの評判を維持することの重要性が急激に高まっていることもあり、DDoSはますます危険な脅威になりつつあります。組織の信用やシステムの中断のない可用性を確保するには、潜在的な攻撃を先回りして理解しておくことが重要です。

DDoS攻撃は、Carpet Bombing（絨毯爆撃）型攻撃などの斬新な攻撃手法の採用など、進化してきました。さらに、インターネットへの接続が世界的に急成長し、オンライン デバイスのネットワークが拡大しました。これは、DDoS攻撃の起点となりうるデバイスの数が増加することも意味します。

これらの進化したDDoS脅威を総合的に阻止するには、AI/ML、スケーラビリティ、自動化、および単なるレート制限以外の高度な技術およびその実装が必要です。DDoS防御には2つの追加機能が必要です。まず、多層防御です。多層防御は、セキュリティチームの負担を軽減し、クラウドスクラビングの使用を最適化し、DDoS攻撃の複雑さと規模に対抗し、TCOを削減します。次に、実用的なインサイトです。セキュリティチームは、保護された各インフラストラクチャの微妙な違いを考慮した実用的なインサイトを必要としています。これにより管理者は、DDoS攻撃の傾向と分析に基づいた調整が可能となります。A10 Defendは、徹底的な多層防御を提供するDDoS防御スイートです。その構成要素の1つであるA10 Defend Threat Controlが実用的なインサイトを提供します。

### SaaS

A10 Defend Threat Control

### 関連製品

A10 Defend Mitigator

A10 Defend Detector

A10 Defend Orchestrator

### お問い合わせ

https://info.a10networks.com/JP-WebContactUs.html

# プロアクティブなDDoSインサイトと防御

A10は、DDoS脅威に特化したインテリジェンスを提供します。A10独自のデータ収集、検証、分析を組み合わせ、実用的な防御ツールであるDDoS攻撃インテリジェンスプラットフォームを構築しました。インテリジェンスは万能薬ではありませんが、DDoS攻撃の規模と複雑さが増大する状況では、必要なサプリメントです。

A10 Defend Threat Controlのカスタマイズされたブロックリストにより、セキュリティチームは組織の特定のニーズに対応できます。従来のインテリジェンスは多くの場合クラウドソーシングであり、古く、そして広範囲をカバーしようとしています。A10 Defend Threat ControlはDDoS対策に特化したインテリジェンスです。ベンダー非依存であり、徹底的な調査、頻繁な更新、はるかに詳細なインテリジェンスです。

A10 Defend Threat Controlのカスタマイズ可能なブロックリストを活用して、組織特有のニーズにも対応できるようになります。また、このブロックリストは、既存のDDoS防御と併用でき、それらを強化するためにも利用できます。A10 Defend Threat Controlのカスタムブロックリストは、ほとんどの既存のセキュリティデバイスで利用可能です。

現在利用可能な他のツールには、False Positive（誤検知）やFalse Negative（見逃し）などの精度を犠牲にして利便性を提供するものも存在しますが、A10 Defend Threat Controlはそれらとは全く異なります。攻撃者、被害者、分析、ベクトル、傾向、その他の特性に関する実践的なインサイトは、DDoS攻撃を阻止するために調整されており、より堅牢で包括的なセキュリティ体制の確立に役立ちます。

# 主な利点

## コスト削減

ユーザがハイブリッドまたはクラウド型のDDoSソリューションを利用されている場合、A10 Defend Threat Controlが提供する正確なカスタマイズされたブロックリストを展開することで、クラウド上のDDoSソリューションへ向かうトラフィック量を減らしたり、クラウド上でのスクラブ容量を節約したりすることが可能です。専用ハードウェアや、高価なクラウドスクラビングサービスを必要とせずに、DDoS攻撃に対する信頼性の高い最初の防御層を確立することができます。既存のインフラストラクチャを十分に理解している管理者にとっては、A10 Defend Threat Controlが提供するインサイトを十二分に活用することができます。

## 新たな脅威を阻止

A10 Defend Threat Controlは、A10独自のデータ収集および検証方法を採用して、DDoS防御を大幅に強化できる正確で実用的かつインテリジェントなデータを提供します。攻撃ベクトル、攻撃手法、被害者の対応状況などについてのインサイトは、組織が既知および未知のDDoS脅威に備えるための、より包括的なDDoS防御スキームを開発するのに役立ちます。

## DDoS防御を強化

A10 Defend Threat Controlはスタンドアロンの SaaS プラットフォームです。専用ハードウェアを使用せずにDDoS防御を確立できます。また、A10 Defend Threat Controlが提供するブロックリストは、ルータやファイアウォールなどの既存のセキュリティデバイスでも使用することができます。カスタマイズされ自動化されたブロックリストは、DDoS防御の最初の防御層として機能します。最新かつ複雑な激しい攻撃ベクトルを特徴とする今日のマルチベクトル型DDoS攻撃を管理するのに特に効果的です。

# DDoS 脅威の状況調査

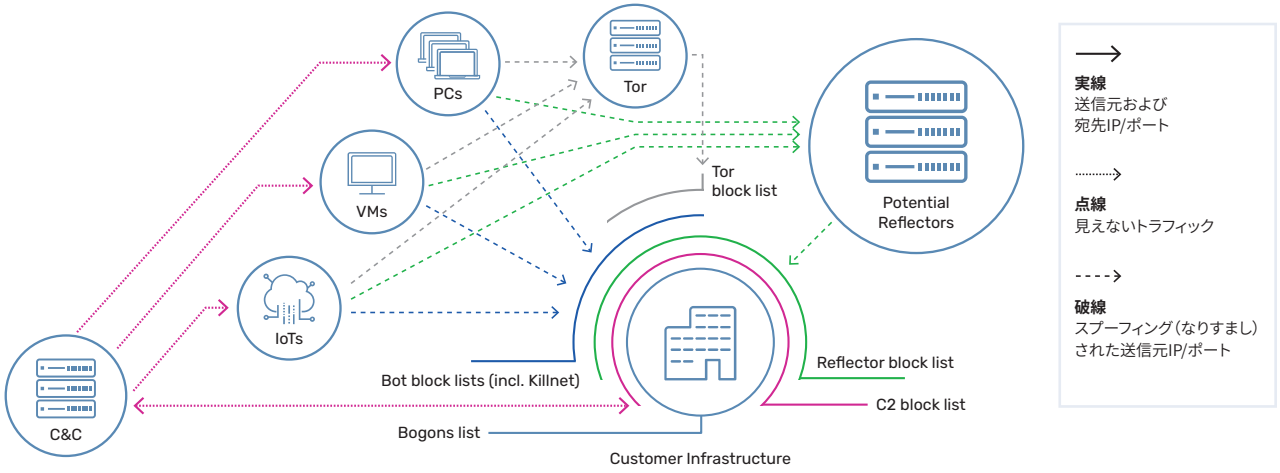


Figure 1: The expanding threat landscape

顧客インフラは、複数の攻撃元からの DDoS 脅威に対して脆弱です。マルウェアは、PC、仮想マシン、またはその他の IoT デバイス上で実行されている可能性があります。攻撃者が攻撃を管理および調整するための中心ハブであるコマンド&コントロールサーバ（C2 サーバ）が、攻撃の真の発生源です。インターネット上の正規の「オープンな」サーバは、さまざまな攻撃ベクトルを通じて侵害され、リフレクション攻撃を開始する可能性があります。Tor などのプロキシサーバは、攻撃をリダイレクトして、発信元を隠すことができます。

常に更新される 3 つの A10 独自のブロックリストが主な差別化ポイントです。

- C2 リスト：汚染されたシステム内のマルウェアは、ボットネット構築のために他のシステムを引き込もうとします。A10 の高度な分析は、そのマルウェアをリバースエンジニアリングして C2 サーバを特定します。この DDoS 攻撃対策に特化したリストはコンパクトで高い信頼性をもち、攻撃の発信元をブロックするのに役立ちます。この機能は、ボットネット全体を阻止するために重要です。根本原因を特定しないままで個々のボットを停止しようとすることは、勝ち目のないモグラたたきゲームをしているようなものです。

- Bot リスト：A10 独自のデータ収集および検証方法は、マルウェアに感染したシステムによって開始される攻撃の挙動と特性を分析します。A10 Defend Threat Control は、蓄積された膨大なデータの継続的な分析を通じて、ボットネットへ参加する可能性のあるエンティティのリストを生成します。

- リフレクタリスト：リフレクタは、レスポンスを増幅するように構成されたシステムであり、元のリクエストよりも大幅に大きなレスポンスを生成します。リフレクタは、アンプ攻撃において重要な役割を果たします。アンプ攻撃の目的は、ターゲットに多数のリクエストを送り込むことではなく、少ないリクエストに対して不釣り合いに多量のレスポンスを引き起こしてターゲットを圧倒することです。潜在的なリフレクタを特定することは重要です。現時点では脅威ではないかもしれませんが、その構成と状態によっては悪用される可能性があります。

# 機能

## 多面的なダッシュボード

リアルタイムのDDoS攻撃マップとそれに付随する詳細情報は、攻撃者と被害者の両方の観点から、世界中のDDoS攻撃インシデントの状況を視覚化するのに役立ちます。時間経過に伴う攻撃傾向は、対数チャートと線形チャートによって表示されます。高度なフィルタリングも可能で、地域、期間、履歴データ、プロトコル、ポートなどの攻撃ベクトルのパラメータによって掘り下げることができます。これらのインサイトと調査結果は、PDF形式のレポートとしてダウンロード可能です。

## 被害者特定

DDoS攻撃は、上位2つか3つの攻撃ベクトルだけで実行されるわけではありません。新たな未発見の攻撃ベクトルや攻撃方法が常に探索されています。A10 Defend Threat Controlの実用的なインサイトは、リフレクタ、ボットネット、IoC（Indicators of Compromise: 痕跡情報）の前例のない可視性を提供します。これらのインサイトは、国、組織、その他の特徴によってさらに分類されます。追加のインサイトには、被害者のIP範囲、被害者のASN、上位のマルウェアハッシュ、スキャンされたポート、悪用されたプロトコル、分類別のDDoS武器の総数などの可視性が含まれます。インサイトには攻撃リサーチ/IP検索の結果として被害IPに対するアラートも含まれ、管理者はインフラを適切に構成・準備し、最新のより深刻なDDoS脅威から保護できるようになります。

## 柔軟性と利便性

A10 Defend Threat Controlは、SaaSとして、シングルサインオン、マルチテナント、通知管理、Web検索などの便利な機能を備えています。ユーザフレンドリな監査証跡は直感的であり、ユーザ、テナント、セッションの管理を簡素化できます。

## データの永続性

A10独自のデータ収集および検証により、劣化せず常に最新の状態を保ちます。攻撃ベクトルは常に進化しており、リスクにさらされる構成も常に変化するため、このことは重要です。リアルタイムの情報と更新がなければ、効果がなくなる可能性があります。

## ベースライン化とプロファイリング

A10 Defend Threat Controlは、インフラに対する攻撃者の視点も提示し、どの脆弱性が攻撃者によって悪用される可能性があるかをユーザが理解するのに役立ちます。IPアドレス/ネットワークで検索すると、ユーザはそれらが「攻撃を受けている」かどうか、または「武器化されている」かどうか、を確認できます。レポートとアドバイザリは、詳細な分析のためにこれらの洞察と同時に使用することができます。

## 有用なIPブロックリスト

A10 Defend Threat Controlは操作が容易です。ユーザは、新しいDDoS防御の展開や既存DDoS防御の強化を迅速かつ簡単に行うことができます。信頼性が高くカスタマイズ可能でDDoS攻撃対策に特化したブロックリストをボットネット、リフレクタ、C2用に生成可能です。Killnetボットネット、Torプロキシ、Borgonに対応したブロックリストも用意されています。ブロックリストは、既存のセキュリティデバイスまたは適切なSIEMデバイスに簡単に取り込むことができます。特殊なユースケースにも対応可能です。これらデータ・リスト全体を統合したい場合、A10 Defend Mitigatorには9,600万件のブロックリストを取り込むことができます。

### A10 Networks / A10 ネットワークス株式会社について

A10 Networksは、オンプレミス、ハイブリッドクラウド、エッジクラウド環境における、セキュリティ、インフラストラクチャの課題を解決するソリューションを提供しています。大手グローバル企業や通信、クラウド、Webサービス事業者まで7000社以上のお客様に導入いただいており、ビジネスに不可欠なアプリケーションやネットワークの安全性、可用性、効率性を高めています。A10ネットワークスは2004年に設立されました。米国カリフォルニア州サンノゼに本社を置き、世界中のお客様にサービスを提供しています。
A10ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。 詳しくはホームページをご覧ください。

• URL：https://www.a10networks.co.jp/ • X（旧Twitter）：https://twitter.com/a10networksjp • Facebook：https://www.facebook.com/A10networksjapan

Learn More
About A10 Networks

お問い合わせ
A10networks.co.jp/contact

**A10ネットワークス株式会社**
www.a10networks.co.jp



Part Number: A10-DS-15139-JA-01 Mar 2024