ソリューション概要

Arbor Networks
DDoS 攻撃防御ソリューション

グローバルな視認性と脅威インテリジェンスを生かした
実証済みの DDoS 多層防御

DDoS 攻撃は明らかに、サイズ、頻度、複雑度の面で拡大の一途をたどっています。今日の DDoS 攻撃は、(1) 大ボリューム、(2) TCP ステート枯渇、(3) アプリケーション層の攻撃ベクトルを、動的に組み合わせています。

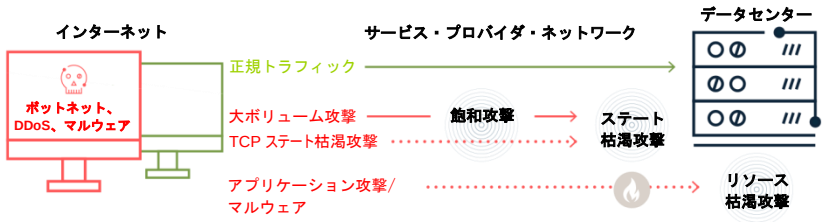

図 1：今日の DDoS 攻撃タイプ

DDoS 防御に対する業界のベスト・プラクティスは、多層防御か、DDoS 攻撃の多様なタイプと標的を考慮したハイブリッド型の手法です。インターネットの接続性を標的にした大ボリュームのフラッド攻撃については、この攻撃がローカルでの防御を圧倒する前に、意図した標的から離れたクラウド内でミティゲーションを行う必要があります。アプリケーション層攻撃とステート枯渇攻撃については、アプリケーションまたはサービスのロケーションに近いオンプレミスでの検知とミティゲーションが必要となります。

同じく重要事項として、動的なマルチベクトル型 DDoS 攻撃を阻止するために、最新の脅威インテリジェンスでサポートされたインテリジェントな形式の 2 層間通信を備えたソリューションである必要があります。Arbor Networks は、今日の DDoS 攻撃の阻止のために、インクラウドおよびオンプレミスの DDoS 防御に関する製品/サービスを完全に統合した、包括的なポートフォリオを提供しており、それらはすべて、継続的なグローバル脅威インテリジェンスを生かしています。

DDoS 攻撃は、サイズ（最大 800Gbps）、頻度（6 秒ごと）、複雑度（ボリューム、TCP ステート枯渇、アプリケーション層のベクトル型攻撃の動的な組み合わせ）の面で拡大し続けています。

ARBOR NETWORKS
The Security Division of NETSCOUT

主な特長

実証済みかつ信頼性の高いソリューション

Arbor Networks は 16 年間にわたり、DDoS 攻撃の防御ソリューションにおける圧倒的なリーダーであり続けています。Arbor Networks のソリューションは、世界のインターネット・サービス・プロバイダおよび大企業の多くから信頼を得ています。

あらゆる組織のための DDoS 防御

Arbor Networks の DDoS 防御は、あらゆる組織において、オンプレミスのアプライアンス、仮想マシン、Cisco ASR 9000 ルーター内のネットワーク組み込みソリューション、徹底的に管理されたハイブリッド型およびクラウドのサービススイートなど、導入、拡張性、予算に関するニーズを満たしています。

完全統合の多層防御

完全に統合化されたインクラウドおよびオンプレミスの DDoS 防御に関する製品/サービスは、今日の DDoS 攻撃に対する包括的な防御を備えています。

グローバルな視認性と脅威インテリジェンス

Arbor Networks の製品/サービスはすべて、ATLAS™ および Arbor Security Engineering & Response Team（ASERT）のグローバルな視認性と脅威インテリジェンスを生かしており、これによって組織は最新の DDoS 攻撃と高度な脅威を阻止できます。

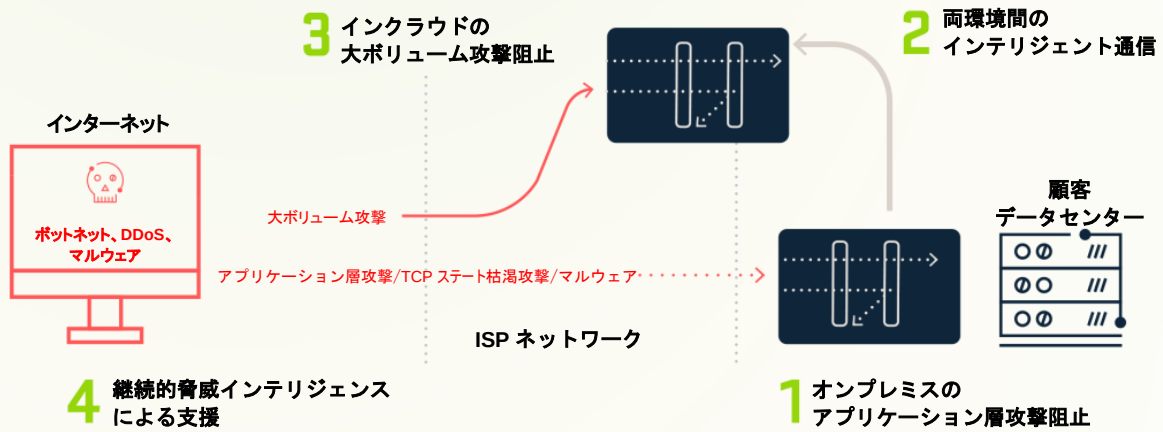

図 2：DDoS 多層攻撃防御

Arbor Networks の DDoS 攻撃防御ソリューション

オンプレミス防御

Arbor Networks は、より大規模なネットワークとより経験豊富な DDoS 攻撃ミティゲーションチーム向けのソリューションとして、Arbor SP および Arbor TMS を提供しています。

Arbor SP は、NetFlow、BGP、SNMP データの収集と解析によって、ネットワークに対する広範な視認性と、最短で 1 秒の DDoS 攻撃検知を実現します。攻撃を検知すると、攻撃トラフィックを Arbor TMS へ自動的に再ルーティングすることができます。Arbor TMS は、共有のスクラビング・センターに導入するか、Cisco ASR 9000 ルーターに組み込んで、あらゆるタイプの DDoS 攻撃に対して外科的なミティゲーション（最大 160Gbps）を行うことができます。また、Arbor SP および TMS のソリューションは、管理された DDoS 防御サービスを提供するためのプラットフォームとなるための機能も数多く備えています。

Arbor Networks は、いっそう自動化された DDoS 防御手法が求められる小規模ネットワークやセキュリティチーム向けに、Arbor APS を提供しています。

常時稼働のインライン型 DDoS 攻撃検知およびミティゲーション・ソリューションは、インバウンド/アウトバウンドの DDoS 攻撃などの高度な脅威を阻止できます。大規模な DDoS 攻撃が発生した場合、Cloud Signaling™は、上流またはインクラウドの DDoS 攻撃防御サービス（Arbor Cloud™など）にインテリジェントにリンクし、ミティゲーションを行います。

インクラウド防御

Arbor Cloud は、ISP に依存しないインクラウドの完全管理 DDoS 防御サービスです。米国、欧州、アジア全域に配置されたスクラビング・センターを介して、1Tbps を超えるグローバルなミティゲーション能力を実現します。企業は、オンプレミスの Arbor APS の防御を Arbor Cloud とシームレスに統合し、包括的な DDoS 攻撃防御を実現できます。サービス・プロバイダは、Arbor Cloud を使用することで、ミティゲーションに関するさらなる能力と専門性が得られます。

グローバルな視認性と脅威インテリジェンス

Arbor Networks Security Engineering & Response Team（ASERT）は、Arbor Networks の製品とサードパーティのインテリジェンス（別名 ATLAS）を 15 年にわたり世界中に導入してきた実績を生かし、グローバルな脅威アクティビティに対する優れた視認性を得ています。ATLAS/ASERT から得られたグローバルな洞察は、機能、統合ワークフロー、ATLAS インテリジェンス・フィード（AIF）として、すべての製品/サービスに継続的に反映されています。

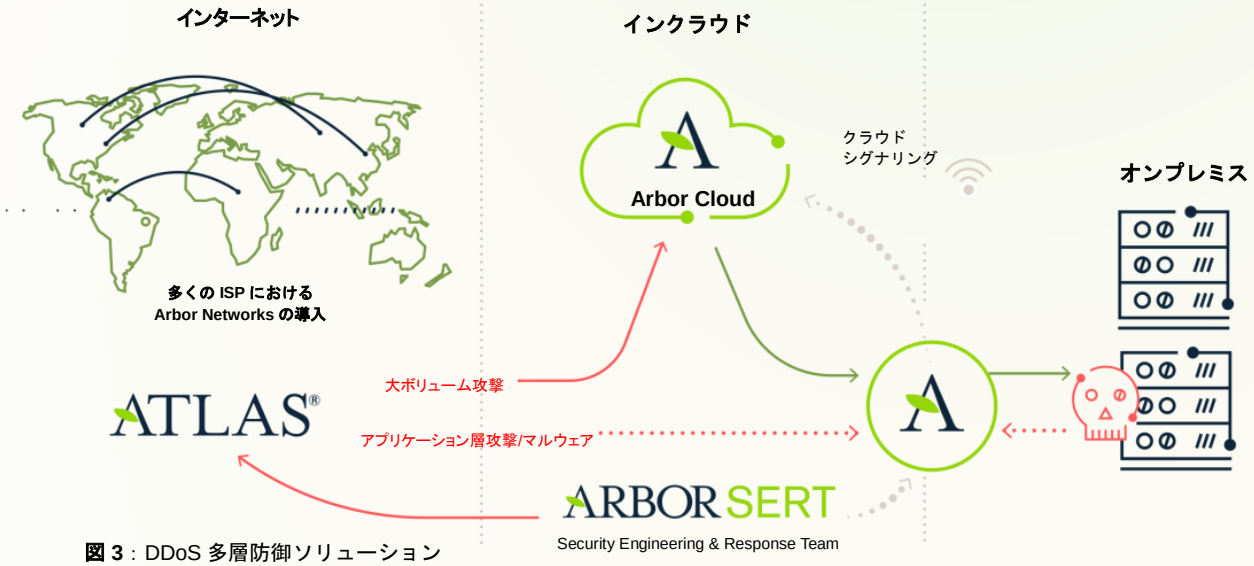

図 3：DDoS 多層防御ソリューション

Arbor Networks 製品

Arbor Cloud DDoS 防御製品/サービス

- インクラウドとオンプレミスを緊密に統合し、徹底的に管理された DDoS 防御。
- 米国、欧州、アジアに配置された 1Tbps を超えるグローバルなスクラビング能力。

Arbor APS

- 100Mbps 以下～40Gbps の範囲の DDoS 攻撃に対する、常時稼働のインライン型の検知とミティゲーション。
- クラウドシグナリングで Arbor Cloud とのインテリジェントな統合を実現。
- オプションのマネージドサービスにより、アプライアンスまたは仮想プラットフォームとして使用可能。

Arbor SP および Threat Management System（TMS）

- Arbor SP による、ネットワークに対する広範な視認性と DDoS 攻撃検知。
- Arbor TMS による、最大 160Gbps の DDoS 攻撃に対する、外部でのステートレスな外科的ミティゲーション。
- 6U シャーシ、2U アプライアンス、Cisco ASR 9000 ルーターの組み込みを網羅するプラットフォーム。

ATLAS インテリジェンス・フィード

- グローバルな視認性と脅威インテリジェンスをすべての製品/サービスに継続的に反映。

ARBOR NETWORKS

The Security Division of NETSCOUT

本社
76 Blanchard Road
Burlington, MA 01803 USA
米国内通話料無料：+1 866 212 7267
TEL：+1 781 362 4300

北米
米国内通話料無料：+1 855 773 9200

ヨーロッパ
T: +44 207 127 8147

アジア・パシフィック
TEL：+65 6664 3140

日本
〒101-0063
東京都千代田区神田淡路町 2-105
ワテラス アネックス 13 階
TEL：03 3525 8040
お問い合わせ japan@arber.net

arbornetworks.com

—

SB/DDoSATTACKPROTECTION/EN/0317-LETTER