

# ARBOR CLOUD DDoS 防御サービス

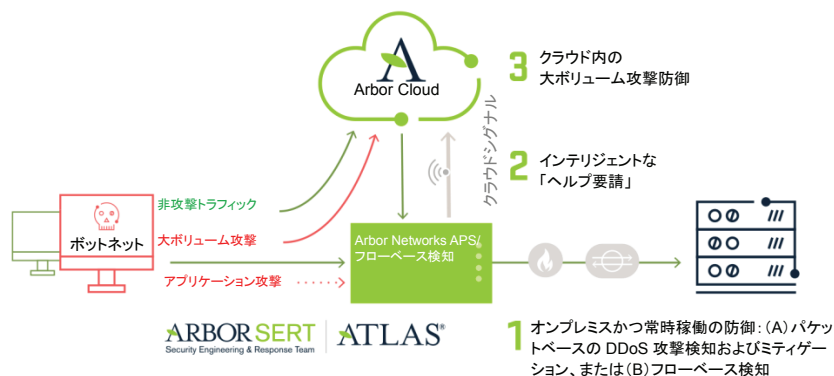
あらゆるDDoS攻撃に対する包括的な自動防御

脅威を増すDDoS攻撃は、企業にとって頭の痛い問題です。大ボリューム攻撃が増加傾向にあり、増幅/反射攻撃の普及も加わって、問題はますます複雑化しています。昨今のDDoS攻撃は、大ボリューム攻撃や、TCPステートを枯渇させる攻撃、アプリケーション・レイヤー攻撃など、攻撃ベクトルを組み合わせています。エンタープライズ向けArbor Cloud™ DDoS攻撃対策 (Arbor Cloud) は、オンプレミスのDDoSミティゲーションと密接に統合されたクラウドベースのトラフィック・スクラビング・サービスを提供します。DDoS防御に対するこの多層アプローチは、企業が昨今の動的なDDoS脅威のミティゲーションを行う上でのベストプラクティスとなります。

## 昨今の DDoS 攻撃に対する多層防御

Arbor Cloud は、DDoS 防御に対する多層アプローチの一部を構成するものであり、アプリケーションやサービスへのアクセスを妨げることなく、高度で大規模な DDoS 攻撃に対するクラウド内での防御を提供します。Arbor NetworksのDDoSセキュリティエキスパートが提供するArbor Cloudのオンデマンド・トラフィック・スクラビング・サービスによって、オンプレミスでミティゲーションを行えない規模の大ボリュームDDoS 攻撃に対する防御が可能です。

Arbor Cloud のオンプレミス・コンポーネントであるArbor Networks® APSは、DDoS攻撃に対して常時稼働のインライン型でパケットベースの検知とミティゲーションを実現します。Arbor APSは、あらゆるタイプのDDoS攻撃の検知と阻止が可能です。しかしながら、インターネット接続ネットワークやローカル防御を圧倒する大ボリュームのDDoS攻撃が発生した場合、Arbor APSは「クラウドシグナリング」という強力な機能を使用し、攻撃のミティゲーションを行Arbor Cloud のスクラビング・ロケーションへ自動的に通知し、攻撃トラフィックを再ルーティングすることができます。オンプレミスのArbor APS、クラウドシグナリング、Arbor Cloudを組み合わせ、今日のあらゆるDDoS攻撃に対する最も包括的な防御を実現しています。



1) アプリケーション・レイヤー攻撃に対する常時稼働のインライン防御を提供するオンプレミスのAPS、2) インテリジェントなクラウドシグナリング、3) より大規模な攻撃を阻止するArbor Cloud、という各要素を組み合わせた完全統合型のソリューション。ATLAS/ASERTのグローバル脅威インテリジェンスが一貫して装備されており、業界で最も包括的なDDoS防御ソリューションを実現。

## Key Features & Benefits

### グローバルな DDoS 防御

ワールドクラスのセキュリティ・インテリジェンスと業界をリードするDDoS防御製品により、単一のキャリアに依存しないグローバルなDDoS防御を1つのソリューションで実現します。

### 数Tbpsのインクラウド防御

数 Tbpsのクラウドベースのトラフィック・スクラビング能力を活用し、大規模なDDoS攻撃をフィルタリングします。クラウド内でIPv4およびIPv6のミティゲーションをサポートします。

### インテリジェントな多層防御

Arbor Networks独自のクラウドシグナリング技術により、パケットベース検知のオンプレミスArbor APS、または、仮想フローベース検知とインクラウド防御を統合します。

### グローバル脅威インテリジェンスを活用

オンプレミスとArbor Cloud DDoS防御ソリューションは、Arbor Security Engineering & Response Team (ASERTが提供する最新のグローバル脅威インテリジェンスを自動的に活用します。

### マネージド APS (mAPS) サービス

業界最先端のArbor Networksの専門技術を駆使して、APSによるオンプレミスのDDoS防御の管理と最適化を行います。

**ARBOR**  
NETWORKS

The Security Division of NETSCOUT

## オンデマンドでクラウドベースの強力なトラフィック・スクラビング

攻撃が発生した場合、ビジネスの継続性を確保するためにはスピードと俊敏性が極めて重要になります。大ボリューム攻撃の際に、まずオンプレミスのAPSが防御の最前線で攻撃を検知します。APSは、攻撃が帯域幅容量の限界に迫っていることを検知すると、Arbor Cloudにシグナルを送信してその先の役割を託します。Arbor Cloud、Arbor Networksの4つのグローバル・スクラビング・センターのいずれかにインバウンドのトラフィックを再ルーティングし、そこでクラウドベースのミティゲーションが行われます。スクラビング・センターは数Tbpsを超えるDDoSミティゲーション能力を備えています。このような状況が発生した場合は、24時間365日対応のArbor Cloudセキュリティ・オペレーション・センター(SOC)がユーザーのセキュリティ/IT部門と連携し、悪意のあるDDoSトラフィックを素早くブロックしながら、正規のトラフィックをすべてユーザーのデータ・センターに戻します。

Arbor Cloudは、IPv4およびIPv6のグローバルなスクラビング能力を備えており、クリティカルなリソースや資産の可用性を脅かす昨今の大規模で複雑な攻撃にも対処できます。

## Arbor Cloud の仕様

Arbor Cloudセキュリティオペレーションセンター	
北米 (ヴァージニア州スターリング)	
クラウドベースのスクラビング・センター	パッケージ・オプション
<b>全クラウド・スクラビング能力 1Tbps 超:</b> <ul style="list-style-type: none"> <li>米国東海岸 (バージニア州アッシュバーン)</li> <li>米国西海岸 (カリフォルニア州サンノゼ)</li> <li>中欧 (オランダ・アムステルダム)</li> <li>アジア (シンガポール)</li> </ul>	<ul style="list-style-type: none"> <li>クライアントトラフィック・ベースの価格設定</li> <li>ミティゲーション: 72時間の利用率</li> <li>標準的なプロビジョニングの設定は無料</li> <li>別途指定がない限りすべての価格は月額制</li> </ul>
サービス・オプション	
<ul style="list-style-type: none"> <li>Arbor Cloud Connect: スタンバイ・クラウド・ミティゲーション・サポートを攻撃発生時に提供</li> <li>Arbor Cloud Essentials: リアルタイム・ミティゲーション・サポートを年間12回まで提供</li> <li>Arbor Cloud Essentials+: リアルタイム・クラウド・ミティゲーション・サポートを無制限に提供</li> </ul>	
柔軟なサービスパッケージ	リテナー・サービス・パッケージ
<b>クライアントトラフィックに基づくオプション:</b> <ul style="list-style-type: none"> <li>100 Mbps</li> <li>500 Mbps</li> <li>1 Gbps</li> <li>2 Gbps</li> <li>4 Gbps</li> <li>8 Gbps</li> <li>10 Gbps</li> </ul> <b>内容:</b> <ul style="list-style-type: none"> <li>年間12回のミティゲーション</li> <li>BGP: 1 戻し GREロケーションでの1/24の保護</li> <li>DNS: 5 ホスト名までの保護</li> <li>クラウドシグナリングのアラートと監視</li> <li>ASERTの脅威レポート、攻撃解析、警告</li> <li>レベル1、2、3のサポート・サービス(24時間365日対応)</li> <li>Arbor Networksの「ミティゲーション時間」SLA</li> </ul>	<b>クライアントトラフィックに基づくオプション:</b> <ul style="list-style-type: none"> <li>100 Mbps</li> <li>500 Mbps</li> <li>1 Gbps</li> </ul> <b>内容:</b> <ul style="list-style-type: none"> <li>低価格月額サブスクリプション</li> <li>年間1回のミティゲーション(2回目以降は別料金)</li> <li>BGP: 1 戻し GREロケーションでの1/24の保護</li> <li>DNS: 5ホスト名までの保護</li> <li>クラウドシグナリングのアラートと監視</li> <li>ASERTの脅威レポート、攻撃解析、警告</li> <li>レベル1、2、3のサポート・サービス(24時間365日対応)</li> <li>Arbor Networksの「ミティゲーション時間」SLA</li> </ul>
追加オプションの例	オンプレミスのオプション
<b>DNSオプション:</b> <ul style="list-style-type: none"> <li>追加ホスト</li> <li>SS 証明書(1 証明書ごと)</li> <li>緊急設定/変更(1 回ごと)</li> </ul> <b>BGPオプション:</b> <ul style="list-style-type: none"> <li>追加のGREトンネル・エンドポイント</li> <li>追加 /24</li> <li>1カ所または複数のArbor Cloudスクラビング・センターとの直接接続</li> </ul>	<b>Arbor APS</b> <ul style="list-style-type: none"> <li>常時稼働のインライン型でパケットベースの検知とミティゲーション</li> <li>最大40Gbpsの攻撃ミティゲーションが可能な2Uアプライアンス</li> <li>1G以下の攻撃を阻止できる仮想アプライアンス - サポートするハイパーバイザー: VMware、KVM、サポートするVNF</li> <li>オーケストレーション: Cloud-Init、Openstack</li> </ul> <b>Arbor Cloudフローベース検知</b> <ul style="list-style-type: none"> <li>仮想の自動フロー・コレクション、解析、DDoS攻撃検知</li> <li>Arbor Cloudへの自動クラウドシグナリング</li> <li>サポートするハイパーバイザー: VMware、XEN、KVM</li> </ul>

## Arbor Security Engineering & Response Team (ASERT)

ワールドクラスのセキュリティ研究者のチームであるASERTは、140Tbpsを超えるグローバルなリアルタイムのインターネット・トラフィックにアクセスし、分析を行います。ASERTは、攻撃データの収集、パートナーからの情報、分析といった各種ツールを巧みに組み合わせて活用します。これにより、インターネット上の新たな脅威を特定して分析し、ターゲットを絞った防御策を構築することで、最も高度かつ巧妙な攻撃からの防御を実現します。

ASERTは、Arbor Cloudポータルで毎週公開されるスレット・ブリーフを通じ、ユーザーにグローバルなインテリジェンスを提供します。

ポータルでは以下の情報を参照できます。

- ・グローバル脅威マップ
- ・スレット・ブリーフ (Arbor Cloud) : ポスト・インシデント・レポートとしてユーザー固有のインテリジェンスを提供
- ・トップ脅威ソース
- ・スレット・インデックス
- ・トップインターネット攻撃



The Security Division of NETSCOUT

米国本社

76 Blanchard Road  
Burlington, MA 01803 USA  
Toll Free USA: +1 866 212 7267  
T: +1 781 362 4300

アーバーネットワークス株式会社

〒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  
EMAIL: japan@arbor.net  
WEB: jp.arbornetworks.com

arbornetworks.com

©2017 Arbor Networks, Inc. All rights reserved. Arbor Networks, the Arbor Networks logo, ArbOS および ATLAS は Arbor Networks, Inc.の商標です。その他のブランド名は各社の商標または登録商標です。

DS/ACE/JA/1117-A4