＊本資料は、2014 年 10 月 21 日に米国で発表されたプレスリリースを翻訳したものです。

報道関係各位

2014 年 10 月 27 日
アーバーネットワークス株式会社

# Arbor Networks Peakflow® 7.0 が、DDoS 攻撃検知とミティゲーションの時間を大幅に短縮

*サービス・プロバイダにネットワーク・インテリジェンスと DDoS 防御を提供する世界的なリーディング・プラットフォーム*

**米国マサチューセッツ州バーリントン**－エンタープライズやサービス・プロバイダのネットワーク向けに分散型サービス拒否（DDoS）攻撃や高度な脅威の対策ソリューションを提供するリーディング・プロバイダ Arbor Networks, Inc.（以下「Arbor Networks」）は、本日、Peakflow®プラットフォームの DDoS 攻撃検知とミティゲーション対応機能における画期的な強化を発表しました。Peakflow 7.0 を使用することで、サービス・プロバイダは、高速フラッド型の DDoS 攻撃をわずか 1 秒で検出し、30 秒以内にミティゲーションを開始できます。

攻撃を受けた場合、1 秒の違いで大きな差が生じます。高速フラッド攻撃は、わずか数秒でトラフィックが数百ギガバイトのサイズに膨れ上がり、プロバイダ・ネットワーク全体に大きな付随的損害を与える可能性があるため、サービス・プロバイダにとって、ミティゲーション開始までの時間の短縮は非常に重要です。2014 年における DDoS 攻撃の状況は、DNS、NTP、さらに最近では 簡易サービス発見プロトコル（SSDP）といったネットワーク・コンポーネントのリフレクション／増幅機能を悪用した非常に大規模な攻撃が主流となっています。Arbor Networks のデータでは、第 3 四半期末までに、100 Gbps を超える攻撃が 130 件以上発生しており、それ以前の四半期に比べて、ボリューム型攻撃が大幅に増加しています。

Arbor Networks プレジデントのマシュー・モイナハン（Matt Moynahan）は、「世界的なサービス・プロバイダの大多数が、Peakflow プラットフォームでネットワーク・インテリジェンスと DDoS 防御を実現しています。また 60 社以上のプロバイダが、Peakflow プラットフォームを利用した DDoS マネージド・サービスを顧客に提供しています。DDoS 攻撃検知とミティゲーションの領域における弊社の絶え間ない技術革新は、サービス・プロバイダのお客様に、自社のインフラストラクチャを保護し、より高度な DDoS マネージド・セキュリティ・サービスを提供するという 2 つの大きなメリットをもたらしました」と述べています。

**Arbor Networks Peakflow のポートフォリオ**

Arbor Networks の Peakflow DDoS 防御プラットフォームは、数多くの世界有数のクラウド事業者、ホスティング事業者、ならびにインターネット・サービス・プロバイダによって導入され、ボットネットやボリューム型およびアプリケーション・レイヤ型の DDoS 攻撃などの悪意のある脅威を積極的に排除し、サービスの可用性と品質を向上させています。

Peakflow プラットフォームは、Peakflow と Peakflow Threat Management System の 2 つの主要コンポーネントで構成されています。Peakflow は、ネットワークワイドの異常検知およびトラフィック・エンジニアリングと Peakflow Threat Management System のキャリア・クラスの脅威管理が一体化されており、他の業務のためのトラフィックを維持しながら、悪意のあるトラフィックのみを検知して自動的にこれを取り除きます。攻撃トラフィックのみをミティゲートできるため、プロバイダは攻撃

を積極的にミティゲートしながら、顧客向けサービスを中断なく提供できます。Peakflow プラットフォームはまた、世界有数のクラウドベースの DDoS マネージド・セキュリティ・サービスで数多く採用されています。

## Peakflow 7.0 の新機能

### 暗号化された攻撃をブロックする組み込み型の SSL インスペクション機能

インターネットで SSL 暗号化が普及するにつれ、DDoS 攻撃もまた悪意のあるトラフィックを暗号化して、防御をかいくぐるようになっています。Peakflow Threat Management System には、オプションでオンボックス SSL アクセラレーション・カードが用意されており、統合された 1 つのアプライアンス・ソリューションによって、暗号化されたトラフィックの DDoS 脅威の有無を検査します。DDoS 攻撃はリアルタイムでブロックされ、正規のトラフィックは中断されることなく通過します。これらはすべて、既存のネットワークやアプリケーション・インフラストラクチャを変更せずに実行されます。

### 攻撃に対する新しい強力な対応策

Peakflow Threat Management System には、ATLAS®インテリジェンス・フィードの一部として提供される機能アップした脅威防御機能が搭載されました。Arbor Peakflow 7.0 では、高度な HTTP、DNS、TCP 接続攻撃を阻止するための対応策が強化されました。今回のリリースで追加された新しい 2 つの対応策は、フラッド攻撃とサーバーを枯渇させる攻撃に対する強力な防御機能を提供します。

### ワークフロー、レポート、分析機能の改善

DDoS 攻撃アラート・ダッシュボードが一新され、地理的情報（攻撃元の国）、ネットワーク情報（攻撃元ネットワーク）、主な攻撃パターンの自動識別など、DDoS 攻撃の新しい分析データを豊富に表示できるようになりました。これによりサービス事業者は、攻撃をすばやく簡単に特定し、対処方法を把握することができます。

さらに今回のリリースでは、Peakflow の優れたネットワーク全体の可視性と分析機能がさらに向上しました。ユーザーは、新しい強力なレポート機能を使用して大量の Peakflow データを分析し、セキュリティチームやマーケティング部門、プロダクトマネージャー、経営陣にとって有用な情報を導き出すことができます。これにより、レポートならびに分析機能を「ユーザー対応」のためのツールとして利用できるようになりました。

### Arbor Networks について

Arbor Networks は DDoS 攻撃や高度化する脅威から世界の大手企業および大手サービス・プロバイダのネットワークを安全に守ることを支援しています。Arbor Networks は全世界のエンタープライズ、キャリア、モバイルの市場において DDoS 保護ソリューションを提供する世界をリードする主要ソリューションプロバイダです（Infonetics Research 社調べ）。高度化する脅威に対する Arbor Networks のソリューションは、パケットキャプチャと NetFlow 技術を組み合わせることで、ネットワーク全体を可視性し、マルウェアや悪意のあるインサイダーの脅威を迅速に検出し、駆除することを可能にします。Arbor Networks はまた、動的なインシデント対応、履歴分析、視認性、フォレンジクスについても市場をリードする分析機能を提供しています。Arbor Networks は、企業のネットワークやセキュリティの担当者がセキュリティのエキスパートになり、企業のセキュリティ強化を実現することを目指しています。Arbor Networks の目標は、お客様がセキュリティ問題を迅速に解決し、事業リスクを低減できるよう、ネットワーク上の脅威の視認性とセキュリティ・インテリジェンスの提供を可能にすることです。

Arbor Networks の製品およびサービスについて詳しく知りたい方は、Arbor Networks の日本語サイトを参照してください。また、業界唯一の革新的なインターネット監視システム ATLAS®のデータに基づく調査、分析および知見については、ATLAS セキュリティポータル（英文）をご覧ください。