＊本資料は、2015 年 1 月 27 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

2015 年 1 月 28 日
アーバーネットワークス株式会社

Arbor Networks、第 10 版年次ワールドワイド・インフラストラクチャ・セキュリティ・レポートを発表。過去 10 年間で DDoS 攻撃の規模が 50 倍に増大

攻撃の規模、複雑性、頻度が継続的に増大。顧客のインフラストラクチャとデータセンターが主な攻撃のターゲットに

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、第 10 版となる年次ワールドワイド・インフラストラクチャ・セキュリティ・レポート（WISR）を発表しました。この年次レポートは、今日の通信事業者が直面する重要なセキュリティの課題について、独自の調査結果を提供するものです。WISR 調査は、今回で 10 年目を迎えます。本調査では、サービス・プロバイダと企業の両面で脅威と懸念事項について詳細な情報を提供しています。今回の年次レポートは、組織が直面する主な脅威と懸念事項、ならびに脅威に対処してミティゲートするための戦略について、主な傾向を報告します。

10 年間における脅威の状況の変化:

- DDoS 攻撃は、10 年前には多くが単発的な迷惑行為に過ぎませんでしたが、現在ではビジネスの継続性と最終利益に対する重大な脅威となっています。今日、DDoS 攻撃の多くは、複雑かつ長期にわたる高度な脅威活動を構成しています。
- 2014 年に報告された最大の DDoS 攻撃は 400Gbps でした。一方、10 年前に報告された最大の攻撃はわずか 8Gbps でした。
- 2014 年の調査では、90%の回答者がアプリケーション・レイヤ攻撃を経験しています。これに対し、10 年前の調査では最も一般的な攻撃ベクトルとして、90%の回答者が単純な「ブルート・フォース型」のフラッド攻撃を挙げていました。
- 人的要素は、防御能力を左右する要因の 1 つです。これは現在だけでなく、WISR レポートの 10 年間を通じて一貫しています。昨年度については、54%の回答者が、セキュリティ組織に熟練の人材を雇用し定着させることが困難であると答えました。

Arbor Networks は、信頼できるアドバイザーならびにソリューション・プロバイダとして長年にわたり築いてきた顧客関係と評価によって、この年次レポートを発行しています。Arbor Networks の第 10 版年次ワールドワイド・インフラストラクチャ・セキュリティ・レポートをご覧いただくには、こちら（英文、要登録）をクリックしてください。

Arbor Networks のソリューション・アーキテクト部長であるダレン・アンスティー（Darren Anstee）は、次のように語っています。「Arbor Networks は、過去 10 年間にわたって WISR の調査を実施することにより、初期のオンライン・コンテンツの出現時から今日の高度に接続された社会に至るまで、インターネットとその利用の進化を追跡してきました。2004 年当時、企業にとって最大の懸念は、その前年にネットワークに大きな被害を与えたスラマーやブラスターなどの自己増殖ワームでした。また、データ侵害の多くは、データ・ファイルに直接アクセスできる従業員によるものでした。今日、組織ははるかに広範で高度な脅威に対処しなければならず、より大きな攻撃サーフェスを防御する必

要に迫られています。さらには、攻撃や侵害を受けた場合、ビジネスに壊滅的な影響が生じる可能性があります。脅威のスケールは、10 年前の比ではありません。」

2015 WISR の調査結果の概要

攻撃の規模、複雑性、頻度が増大

- **リフレクション／増幅の使用による大量攻撃の開始**:2014 年の調査で最大規模の攻撃は 400Gbps であり、次いで 300Gbps、200Gbps、170Gbps の攻撃が報告されました。また、6 人の回答者が 100Gbps のしきい値を超える攻撃を報告しています。一方で、10 年前の調査における最大の攻撃は 8Gbps でした。
- **マルチベクトルやアプリケーション・レイヤ DDoS 攻撃の偏在化**:アプリケーション・レイヤ攻撃を受けたことのある回答者は 90%に上ります。また 42%の回答者が、1 回の継続的な攻撃の中にボリューム型、アプリケーション型、ステートを枯渇させる攻撃を含むマルチベクトル型攻撃を経験しています。
- **DDoS 攻撃の頻度の増大**:2013 年の調査では、1 ヵ月に 22 件以上の攻撃を観測した回答者は全体の 4 分の 1 強でしたが、2014 年にはこの割合が 38%へと増加しました。

企業に対する容赦ない攻撃

- **DDoS 攻撃や高度な脅威の拡大**:回答者の 50%近くが調査期間中に DDoS 攻撃を観測し、そのうち 40%近くにおいて、インターネット接続が飽和状態になりました。
- **ファイアーウォールや IPS デバイスが、引き続き攻撃の対象に**:3 分の 1 以上の組織で、DDoS 攻撃の間にファイアーウォールや IPS デバイスが機能停止したか、機能停止の一因となりました。
- **攻撃の主要ターゲットはクラウド・サービス**:回答者の 4 分の 1 以上が、クラウド・サービスをターゲットとする攻撃を観測しています。
- **セキュリティ・インシデントの増加と企業による対応の立ち遅れ**:本年度、セキュリティ・インシデントが増加していると答えた回答者は全体の 3 分の 1 強に過ぎず、約半数が昨年度とほぼ同レベルと回答しました。セキュリティ・インシデントへの対策が非常に、もしくは十分整っていると感じている回答者は全体の 40%であり、対策を全く行っていないという回答は 10%でした。

データセンターはターゲットとして規模が大きく、影響も強い

- **データセンター事業者の 3 分の 1 以上が、DDoS 攻撃によるインターネット帯域幅の枯渇を観測しています。**これは、DDoS 攻撃がデータセンター事業者にとって常に重要な問題であることを示しています。データセンター事業者にとってダウンタイムはビジネス機会の損失に留まらず、クラウド内で顧客が運営するビジネスに不可欠なインフラストラクチャに付随的な損害を広がるためです。
- **データセンター事業者が DDoS 攻撃によって被る最大のコストは運用コストです。**これは、増加する攻撃への対応コストが増え続けており、また、データセンター事業者が DDoS 攻撃への対策を重視していることを示しています。
- **DDoS による収益の損失が急増**:データセンター事業者の回答者のうち、44%が DDoS 攻撃による収益の損失を経験しています。
- **半数弱の回答者が、DDoS 攻撃によってファイアーウォールがダウンしたか、ファイアーウォールダウンの一因となったと回答しています。**これは昨年度の 42%から増加しています。ロード・バランサーでも同様の問題があり、昨年度は回答者の 3 分の 1 以上が DDoS 攻撃によるロード・バランサーの機能停止を観測しています。

調査の範囲とデモグラフィックス

- 回答者数は 287 人（昨年度は 220 人）。回答者は、世界の Tier 1 ならびに Tier 2／3 サービス・プロバイダ、ホスティング、モバイル、エンタープライズとその他の種類の通信事業者で構成されています。
- 10 年前の WISR の回答者数は 36 人でした。現在の WISR のデータは、地理的にもネットワーク事業者の種類においてもより広い範囲からまとめられています。
- 本年度の回答者の 60%以上がサービス・プロバイダであり、約 30%が企業組織、教育機関、ならびに政府機関です。トラフィックに加え、サービス・プロバイダのネットワーク、サービス、顧客をターゲットとする脅威について、世界的な状況の把握が可能です。
- 本調査は、2013 年 11 月から 2014 年 10 月までのデータを対象としています。

追加リソース:

- レポートの全文をダウンロードするには、こちら*をクリックしてください（英文、要登録）。*
- WISR の図解については、Arbor Networks の Pinterest ページをご覧ください。
- WISR のプレゼンテーションをダウンロードするには、Arbor Networks の SlideShare ページをご覧ください。
- Arbor Networks の Facebook はこちらです。Twitter で@arbornetworks をフォローし、#WISR ハッシュタグを使用すると、詳細な調査結果をご覧いただけます。

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 防御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。

本件に関するお客様からのお問い合わせ

アーバーネットワークス株式会社
TEL: 03-3525-8040
Email: japan@arbor.net

本件に関する報道関係の方のお問い合わせ

フライシュマン・ヒラード・ジャパン株式会社 中原／友永
TEL: 03-6204-4309
Email: arbor-pr-jp@fleishman.com