

# 【インターネットの現状】 / セキュリティ

年間レビュー

○ エグゼクティブサマリー： 第4巻、第5号

## 編集者より

2017年11月以来、Akamaiの研究チームは、週平均1件を超えるペースで記事やブログを投稿し、論文を公開してきました。その範囲は、開催予定のイベントに関する記事から、新たな脅威に関するリスク情報、そしてこの「インターネットの現状 / セキュリティ」レポートシリーズまで、多岐にわたります。今回は、そうした記事や投稿を振り返り、この1年の大きなセキュリティストーリーの中でどのような位置付けになるのか確認したいと思います。そこで、AkamaiのChief Security OfficerであるAndy Ellisに、現在のトレンドを基にした2019年の展望についての考察を依頼しました。以下は彼のエッセイからの引用です。

## CSO室より

“ plus ça change, plus c'est la même chose  
(いくら見かけが変わっても、本質は変わらないものだ) –

Jean-Baptiste Alphonse Karr

インターネットセキュリティのトレンドについて唯一真実があるとすれば、それは毎年同じことが起こる点です。1998年、「砂漠のキツネ作戦」遂行中に、敵国はDDoS（分散型サービス妨害）攻撃とともにTeardropの脆弱性を利用し、USCENTAFネットワークの遮断を試みました（当時私は防御エンジニアを務めていました。攻撃を特定し、設定をテストし、境界セキュリティシステムに展開したときの興奮を覚えています）。これは、Security Operations Centerで私たちや他社が毎日行っている行動と戦略的には変わりません。当時と違うのはその規模とオートメーションだけです。

2019年の展望を考える場合、ここ数年継続しているパターンを指摘し、今後も継続することを示唆して、これまでとほとんど同じ形で今後も継続的に発展することは容易に推測できます。



## 総当たり DDoS

DDoS のトレンドは非常に安定しているため、スタート地点として DDoS は最適です。攻撃を、影響力と帯域幅という 2 つの異なる軸で考えると最も分かりやすいでしょう。**帯域幅**は、簡単に言うと、攻撃者が一定の時間枠で生成できるトラフィックの単位です。これまでの数字を見ると、最大の攻撃規模は四半期ごとに約 9% ずつ成長しており、2 年ごとに 2 倍になっています。ただし、興味深いことに、継続的には成長していません。9% の前四半期曲線に沿って新たなピークに達すると、Mirai や Memcached リフレクション攻撃のように、攻撃者がボットネットやリフレクションを構築する新たな手法を発見します。

新たなピークの間には、2 つの出来事が起こります。1 つ目は、攻撃を受けたシステム管理者や ISP オペレータなどが、攻撃対象となるシステムの数減らすという対策を取ることです。2 つ目は、攻撃者がこうしたリソースの管理を巡って争いを始めることです。ボットネットは断片化が進み、個々の攻撃は縮小していきます。

効果面を考えると、これは攻撃者にとって不利益にはなりません。一般に、DDoS の防御スタイルは、一定の割合で規模が拡大することはありません。最大規模の攻撃は、Akamai の Kona Site Defender や Prolexic Routed などのサービスが稼働するネットワークのエッジ部分で発生します。中間層の防御は ISP のコアで稼働し、「クリーンパイプ」サービスをサイトオーナーに提供します。最小規模の防御は、オンプレミスソリューションとして、対象となるデータセンター内でのみ稼働します。攻撃者のボットネットが小規模で、エッジベース防御を標的にできないとしても、データセンターベースの防御しか使用していないユーザーに対する攻撃は依然として有効です。たとえ数百人規模でも効果があります。

帯域幅ベースの DDoS 攻撃には多くの形態がありますが、攻撃の最大規模が 9% の前四半期成長曲線に制限されているのは興味深いことです。ただし、不可解な現象ではありません。これは自然発生的な制限ではなく、インターネット基盤の成長率がボットネット全体のキャパシティを制限していると解釈できるでしょう。インターネットのキャパシティは DDoS 攻撃全体の破壊力を減衰させます。ネットワークコンポーネントから標的が離れるほど、標的と攻撃ソース間の輻輳したリンクで発生するトラフィックは少なくなります。

DDoS、アプリケーションレベル攻撃、Credential Stuffing、ギグエコノミー、ブロックチェーンに関する Andy のその他の考察については、「[インターネットの現状／セキュリティ：年間レビュー](#)」レポート（第 4 巻、第 5 号）をダウンロードしてください。

## AKAMAI について

Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで全てを物理的に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、ウェブ／モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日/24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、[www.akamai.com/jp/ja/](http://www.akamai.com/jp/ja/)、[blogs.akamai.com/jp/](http://blogs.akamai.com/jp/) および Twitter の [@Akamai\\_jp](https://twitter.com/Akamai_jp) でご紹介しています。全事業所の連絡先情報は、[www.akamai.com/jp/ja/locations.jsp](http://www.akamai.com/jp/ja/locations.jsp) をご覧いただくか、03-4589-6500 までお電話でお問い合わせください。公開日：2018年12月。