2018 年 3 月 22 日
*Press Release*
アカマイ・テクノロジーズ合同会社

# Akamai の 2017 年第 4 四半期「インターネットの現状／セキュリティ」レポートを発表　ボットによる大量の不正ログインの継続を再確認

## 43%のログインがボットによる不正ログイン、新たに業界別の分析データを追加
## Mirai ボットの急成長の可能性と、仮想通貨マイニングに利用される脆弱なウェブを警告

世界最大、かつ最も信頼性の高いクラウド・デリバリー・プラットフォームを有するアカマイ・テクノロジーズ・インク（NASDAQ：AKAM、以下アカマイ）は、2017 年第 4 四半期の「インターネットの現状／セキュリティ」レポートを発表しました。1 か月間に発生した 7 兆 3,000 億件を超えるボットリクエストの分析結果が盛り込まれた新たな公表データから、ボットによる大量の不正ログイン（Credential Abuse）脅威が急増し、ログイン試行の 40% 以上を不正なアクセスが占めているという現状が、明らかになりました。
Ponemon Institute の調査では、不正ログイン関連（Credential Stuffing）による企業の損失は、年間で 270 万ドルに上ると予想されています。さらに、アカマイのデータは、DDoS 攻撃が依然として脅威であるだけでなく、Mirai ボットネットが急激に勢いを増す可能性があることを示しています。

アカマイの研究者は、ハッカーによる最近の活動が、エンタープライズシステムをボットネットの脅威の一部とするために、エンタープライズ向けのソフトウェアが持つリモートコード実行の脆弱性を悪用することへと移行してきていることを確認しています。たとえば、ハッカーは対象が 70 万以上存在すると推測される組込みシステム用の HTTP サーバーGoAhead と Oracle WebLogic Server の脆弱性を悪用するようになっています。また、今年初めに Spectre および Meltdown に関する情報の公開によってそれらの脆弱性が明らかになったことで、コンピューティングリソースを著しく消費する仮想通貨などの暗号化マイニングプログラムの不正インストールをはじめとする新たな攻撃が可能になりました。

アカマイの Martin McKeay（Senior Security Advocate 兼 Senior Editor）は、今回のレポートで「攻撃者の主な動機は、これまでと変わらず金銭的な利益を得ることです。ただし、ここ数年、その目的を達成するためにランサムウェアのような、より直接的な方法へと攻撃手法が移行してきているのを確認しています。暗号化マイニングの手法により、攻撃者は現金を攻撃者の暗号通貨ウォレットに即時入金するという最も直接的な方法で攻撃を収益化できるようになりました。」と述べています。

アカマイの調査結果から、前四半期（2017 年第 4 四半期）の DDoS 攻撃総数は、前年同期（2016 年第 4 四半期）から 14% 増加していることがわかりました。2017 年第 3 四半期までのレポートでは、Mirai ボットネットによる集中攻撃は緩やかになっていましたが、 11 月下旬に Mirai ボ

ットネットがインターネットでスキャンしたユニーク IP アドレスの数が 突然 100 万個近くまで急増したことで、Mirai がいまだに爆発的な力を秘めていることを示しました。

**数字による分析**

2017 年第 4 四半期の「インターネットの現状／セキュリティ」レポートのハイライト：

- サービス業界は、認証情報の不正アクセス攻撃の最大の攻撃対象となり、有害なボットネットによるログイン試行が全体の 82% を占めた。
- 金融業界では DDoS 攻撃の発生件数が急増し、前四半期は 37 の組織で 298 件の DDoS 攻撃が発生。
- GET、PUSH、POST フラッドなどのアプリケーションレイヤーを標的にした DDoS 攻撃は、第 4 四半期の発生件数が第 3 四半期から 115% 増加。
- 米国が攻撃元である DDoS 攻撃は、前年同期（2016 年第 4 四半期）と比較して 31% 増加。
- アカマイではボットトラフィック単独で 11 月に 146 ペタバイト、12 月には 145 ペタバイトのトラフィックを確認。これは約 550 Mbps の攻撃に匹敵。
- アカマイは 2017 年第 4 四半期に Prolexic Routed プラットフォームで 4,364 件の DDoS イベントを緩和。また、2017 年の 1 年間に確認された DDoS イベントの合計件数は 15,965 件。

**ボットアクティビティによる不正ログインという脅威の増加の要因**

アカマイは毎日 1 秒間に 2,750 件以上のボットリクエストを監視しており、その件数はプラットフォーム全体の純粋なウェブトラフィック（動画ストリーミングを除くトラフィック）の 30% 以上を占めています。そのようなボット活動の大半は正当なものですが、サイバー犯罪者がボットの活動を不正行為に利用する機会は増えています。たとえば、従来は DDoS 攻撃の原因となっていたボットネットの多くが、大量の不正ログインの目的で使われるようになっています。11 月と 12 月に Akamai プラットフォームで追跡された 170 億件のログインリクエストのうち、ほぼ半数（43%）が不正ログイン（Credential Abuse）に使用されていました。

「自動化とデータマイニングの進展で、ボットのトラフィックが大量に発生し、ウェブサイトやインターネットサービスにまで影響が及んでいます。そのようなトラフィックのほとんどはインターネットビジネスにとって有益ではあるものの、サイバー犯罪者は大量のボットを操作して不正に利益を得ようとしています」と McKeay は述べています。「各組織は、実際の人間を、良性ボットや悪性ボットと区別するために、自社のサイトにアクセスするユーザーを監視する必要があります。ウェブトラフィックやボットがすべて同じように作成されているわけではありません。」

2017 年第 4 四半期の「インターネットの現状／セキュリティ」レポートは、
akamai.com/stateoftheinternet-security から無料でダウンロードできます。

**手法：**

2017 年第 4 四半期「インターネットの現状／セキュリティ」レポートでは、アカマイのグローバルインフラストラクチャから収集された攻撃データをもとに、社内の多様なチームによる調査を行っています。このレポートでは、Akamai Intelligent Platform から収集したデータを使用して、現在のクラウドセキュリティと脅威の状況の他、攻撃傾向の知見について分析しています。「インターネットの現状／セキュリティ」レポートには、Security Intelligence Response Team（SIRT）、Threat Research Unit、Information Security、Custom Analytics グループなど、アカマイのさまざまな部署のセキュリティ専門家が携わっています。

**アカマイ について：**

世界最大、かつ最も信頼性の高いクラウド・デリバリー・プラットフォームを有するアカマイは、デバイスや場所に関係なく、最高、かつ最もセキュアなデジタル体験をお客様に提供します。アカマイのプラットフォームは 130 カ国に 20 万台以上という比類のないスケールで展開されており、お客様に優れたパフォーマンスとセキュリティを提供しています。ウェブ/モバイルパフォーマンス、クラウドセキュリティ、エンタープライズアクセス、ビデオ・デリバリー・ソリューションによって構成されるアカマイのソリューションは、優れたカスタマーサービスと 365 日/24 時間体制の監視によって支えられています。グローバルトップの金融機関、e コマース事業者、メディア・エンターテインメント企業、政府機関等が、アカマイを信頼する理由について、 www.akamai.com/jp/ja/または https://blogs.akamai.com/jp/および Twitter の @Akamai_jp でご紹介しています。



本プレスリリースに関するお問い合わせ先 ----------
●アカマイ・テクノロジーズ合同会社
マーケティング本部 広報担当：森（Mail: info_akamai@akamai.com）
●Akamai PR 事務局（プラチナム内）
TEL: 03-5572-6071　Mail: akamai@vectorinc.co.jp