2019年第2四半期

DDoS攻撃者の武器

A10のセキュリティ調査による特別レポート

要旨

DDoS 攻撃の頻度、強度、巧妙さは増大し続けています。しかし、クラッシュを起こすような大規模攻撃を実施するために、ボットネットや脆弱なサーバーを利用するという配信手法は変わっていません。難読化によって攻撃の検知を逃れるような従来のセキュリティ対策とは異なりDDoS 攻撃は広範囲に分散される性質を持っているため、DDoS 攻撃者の武器の所在を重点的に把握することによって未然に被害を防ぐ可能性を生み出します。

反射型アンプ攻撃という武器

攻撃者は UDP プロトコルの脆弱性を利用して標的の IP アドレスを偽装し、サーバーの脆弱性を悪用して反射的なレスポンスを送りつけます。この方法では、最初のリクエストよりはるかに大きいデータサイズのレスポンスを生成することで攻撃を増幅します。

DDoS ボットネットという武器

マルウェアに感染したコンピュータ、サーバー、および IoT デバイスが、ボットハーダー（脆弱性のある多数のデバイスをボット化し、悪用するハッカー) に制御されて（通常は DDoS 攻撃請負サービスから）攻撃に利用されていますが、特に IoT デバイスの利用が増えています。これらで形成されるボットネットは、ネットワークレイヤーおよびアプリケーションレイヤーに対するステートフル / ステートレスな攻撃を仕掛けるために使用されます。

このレポートの主な見解

- IoT デバイスを悪用した COAP 反射型アンプ攻撃は、新しい端末とモバイルホットスポットの利用とともに幅広く増加
- UDP 1900 をソースポートとしない SSDP 反射型アンプ攻撃が増加
- Satori ボットネットを示すスキャンアクティビティの増加。マルウェアの観測を通して確認
- アップロードされた多くのマルウェアは前四半期とは異なったが、多くが Mirai と Gafgyt をベースとしている

DDoS 脅威インテリジェンス

DDoS 攻撃の攻撃元の特定と列挙

スレットリサーチャーは、ハニーポットを仕掛け、インターネットをスキャンし、コマンドアンドコントロール（C2）によって操作された攻撃エージェントを注意深く監視して DDoS 攻撃の武器に関する脅威インテリジェンスを収集します。A10 とパートナーのセキュリティリサーチャーはこれまでに、DDoS 攻撃で常用されている侵害されたホストの IP アドレスを数百万件収集しています。このデータは、数千万ものエントリを含む大量のフィードを作成するために使用されます。このデータを単なる情報から実用的な情報に変えるために、A10 のソリューションでは数百万のエントリから成るクラスリストに基づいて精度の高いブラックリストとホワイトリストを作成しています。

追跡された DDoS 攻撃の武器（規模順トップ 5）

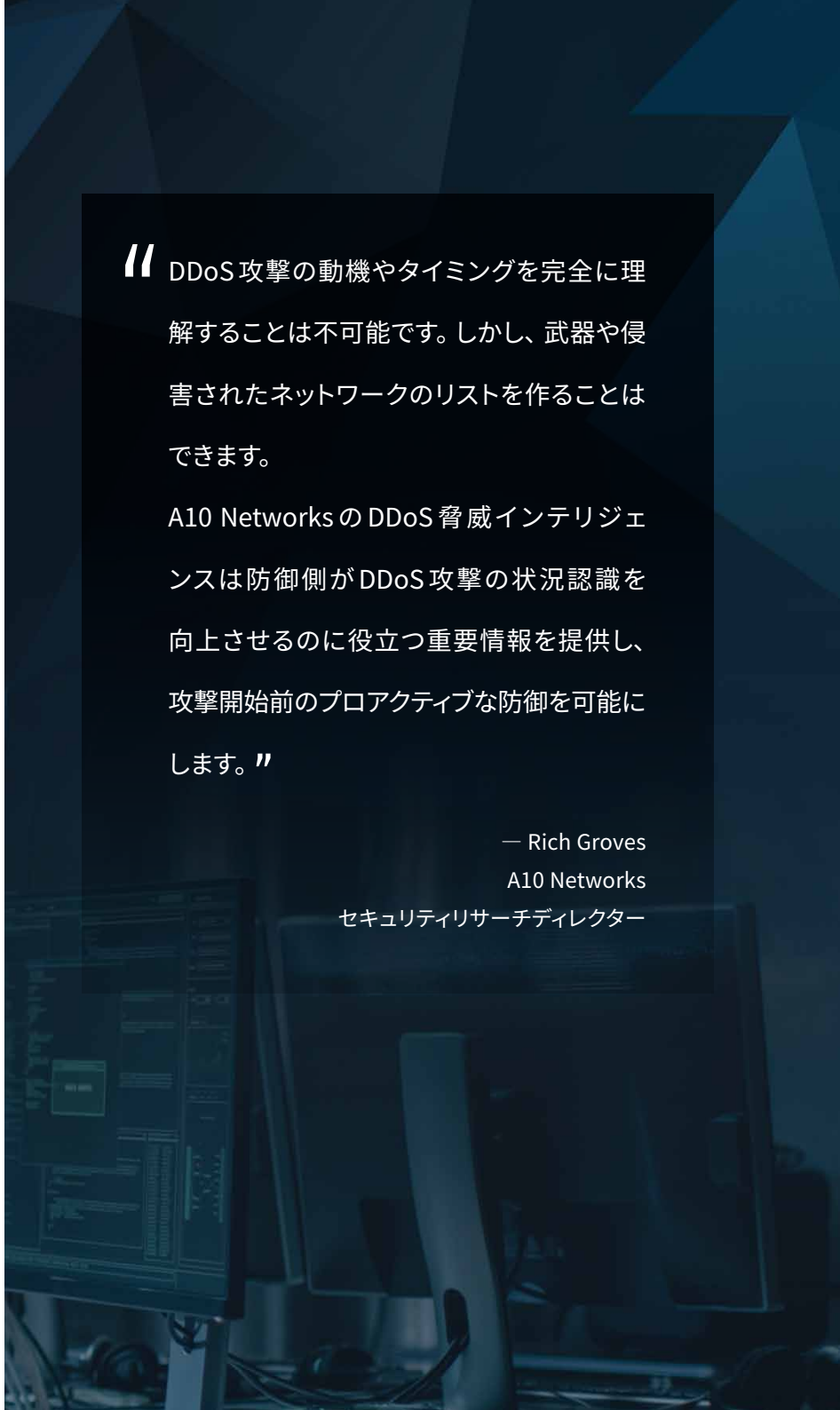
NTP：6,389,893

DNS リゾルバ：4,894,208

SSDP：3,321,269

TFTP：2,131,765

SNMP：1,897,221



"DDoS 攻撃の動機やタイミングを完全に理解することは不可能です。しかし、武器や侵害されたネットワークのリストを作ることはできます。

A10 Networks の DDoS 脅威インテリジェンスは防御側が DDoS 攻撃の状況認識を向上させるのに役立つ重要情報を提供し、攻撃開始前のプロアクティブな防御を可能にします。"

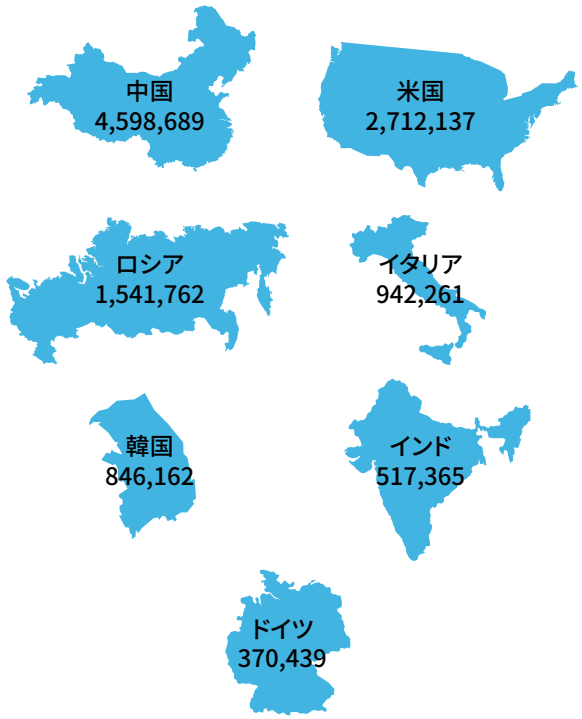
— Rich Groves
A10 Networks
セキュリティリサーチディレクター

DDoS攻撃用武器の主な供給源

DDoS攻撃は世界中に分布していますが、その攻撃元については興味深いデータが判明しました。

DDoS攻撃用武器が集中している国

DDoS攻撃用の武器は世界中に分散していますが、インターネット接続人口の密度が高い地域に集中していることがわかっています。



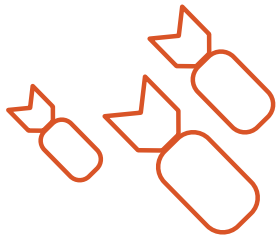
DDoS攻撃用武器が集中しているASN

ASNは、単一の管理オペレータの制御下にあるIPアドレスの範囲です。これらの企業または政府機関のオペレータは、彼らのユーザーに属する多数の武器が自ネットワークに接続したまま他のネットワークやコンピュータを攻撃できるようにします。

China unicom中国联通	1,969,582
中国电信 CHINA TELECOM	1,575,523
TIM	549,166
Rostelecom	444,717
kt	375,434

モバイルキャリアがDDoS攻撃の武器をホスト

DDoS攻撃の武器をホストするモバイルキャリアがレポート期間中に急増しています。



Guangdong Mobile Communication Co.Ltd

Shandong Mobile Communication Company Limited

China Mobile Communications Corporation

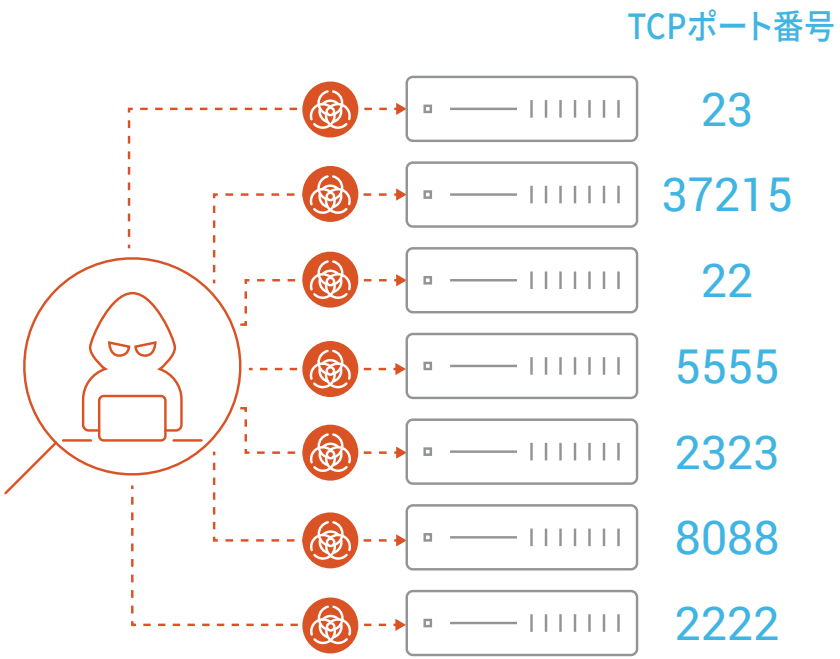
T-Mobile

Henan Mobile Communications Co.,Ltd

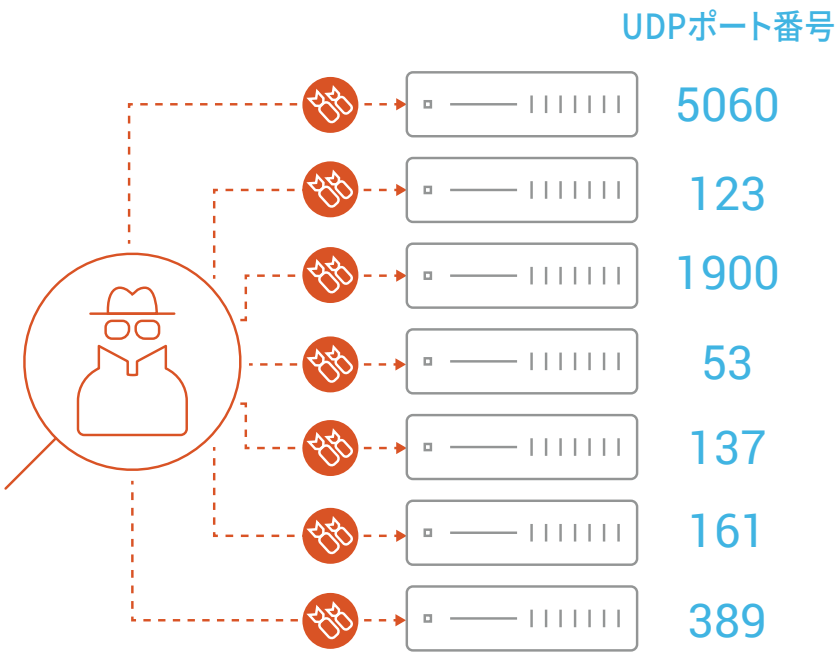
DDoS攻撃者による偵察

DDoS攻撃は、動機のある攻撃者、DDoS攻撃請負サービス、および武器を含む犯罪エコシステムから成り立っています。攻撃者は通常、利用可能なDDoS攻撃用武器のプールを備えたオーケストレーションプラットフォームを持っているDDoS攻撃請負サービスの力を借ります。DDoS攻撃請負サービスのボットハーダーは、継続的に武器のストックを補充するために、インターネットをスキャンして、無防備なTCPサービスを通じて脆弱なIoTデバイスを見つけるとともに、反射型アンプ攻撃に利用できるUDPサービスを探っています。

検索件数が多いTCPポート



検索件数が多いリフレクター

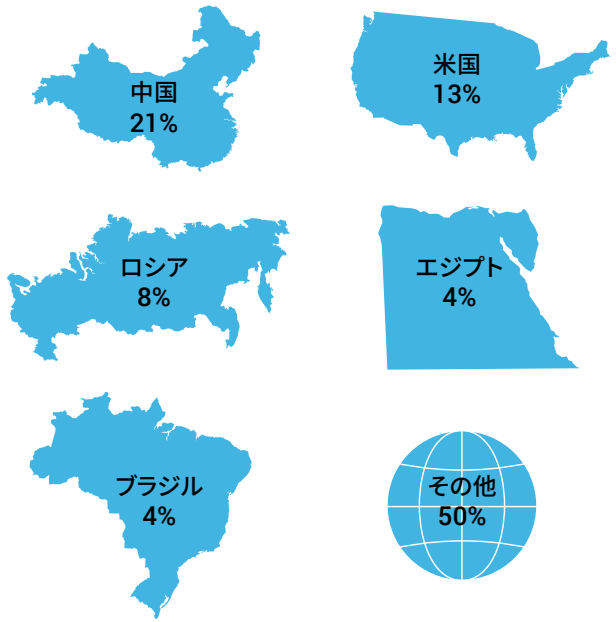


DDoS ボットネットエージェント

マルウェアに感染した攻撃者の制御下にあるコンピュータ、サーバー、ルーター、カメラおよびその他の IoT デバイスなどのノードは DDoS 攻撃の重要な武器になります。これらは一般的にボットまたはボットネットと呼ばれ、DDoS 攻撃を柔軟に仕掛けることができます。

セキュリティリサーチャーは、DDoS 攻撃で繰り返し使用されるホストの情報を蓄積し、マルウェア感染の特徴を示したホストを調査します。DDoS 攻撃が発生したら、その IP アドレスをさらに精査して慎重に対処します。

DDoS ボットネットエージェントが集中している国



DDoS ボットネットエージェントが集中している ASN

China unicom 中国联通

Rostelecom

中国电信 CHINA TELECOM

TE Data

Baidu 百度

IoT は DDoS ボットネットの温床

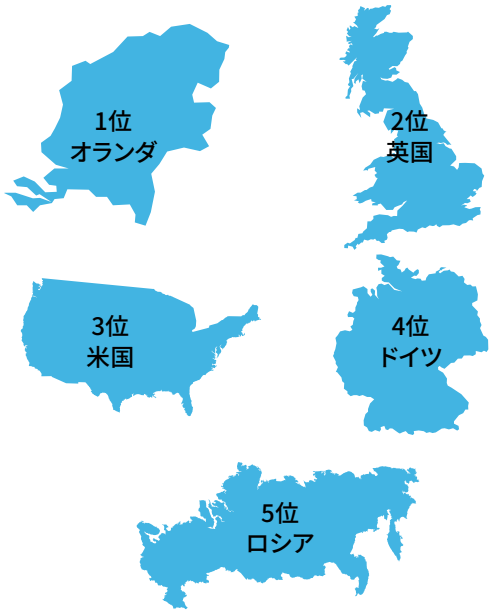
5G により攻撃ネットワークが大幅に拡大

インターネットの誕生からたった 25 年で、全世界人口 76 億人の 55% がネットに接続するようになりました。その人数は、1 秒あたり 4.6 人という増加率で直線的に増えました。1 秒あたり 127 デバイスが新たに接続されている IoT の成長率はこれを上回っており、さらに加速しています。5G（第 5 世代モバイル通信システム）の出現により、帯域幅速度の大幅な向上、超低遅延、そして地理的なカバー範囲の劇的な拡大がもたらされ、IoT の新たな使用形態の爆発的な増加と、接続されるデバイスの指数関数的増加が予測されます。5G により、脅威のすばやい検知と軽減のためには、機械学習と AI を使ったインテリジェントオートメーションが不可欠となります。Linux で動作する IoT デバイスは、すでに新種のマルウェアの標的になっており、これらのマルウェアは主に DDoS 攻撃に使用されています（Eurecom）[*1]。IoT は、ボットネットにとって完璧なホストです。彼らが残していったマルウェアを見てみましょう。

ドロップされた代表的な IoT マルウェア

ファミリー名	バイナリ名
Mirai	loligang.x86
Mirai	UnHAnaAW.x86
Gafgyt	Nakuma.x86

多くのマルウェアドロッパーがホストされている国



多くのマルウェアドロッパーがホストされている ASN

DigitalOcean
3WINFRA
COLOCROSSING
Selectel
Google Cloud

[*1] http://www.s3.eurecom.fr/docs/oakland18_cozzi.pdf (フランスに本拠を置く EURECOM)

最新のIoT脅威：COAP

IoTを悪用した新しいDDoS攻撃では、Miraiやマルウェアは使用されません。IoTデバイスのテクノロジはセキュリティが脆弱なため、何百万ものデバイスを武器に反射型アンプ攻撃を実行できます。新しい攻撃手法は、UDPで実装されたCoAP（Constrained Application Protocol）がベースです。このM2M（マシンツーマシン）の管理プロトコルは、スマートエネルギーやビルオートメーションなどのアプリケーションをサポートするIoTデバイスに導入されています。

CoAPはTCPとUDPの両方で実装され、認証を必要せず、DDoS攻撃者にとって小さなリクエストに対して大きなデータサイズのレスポンスを返すのに適したプロトコルです。

A10が特定した脆弱なIoTデバイスは50万以上（正確な台数：541,462）

96%

のレスポンスが350バイト以上

レスポンスの62パーセントが1KB以上

749バイト

レスポンスの平均サイズ

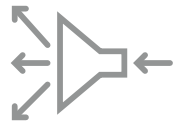
98%

が中国とロシアに存在している

UDPポート5683から任意の宛先ポートへの攻撃

4Kバイト

レスポンスの最大サイズ



平均増幅率：35倍

最大規模のDDoS攻撃の共通点 - アンプ（増幅）攻撃

反射型アンプ攻撃は、規模について言えば最大クラスに入ります。反射型アンプ攻撃とは、インターネット上の適切な設定がされていない無防備なサーバーに対して偽装したリクエストを送りつける、UDPプロトコルのコネクションレスな性質を悪用したDDoS攻撃の一種です。

この攻撃手法は、偽装した被害者のIPアドレスを使用して、大量の小さなリクエストが無防備なサーバーに送信されます。リクエストを受信した各サーバーは、増幅された大量のレスポンスを標的のサービスへ送信されます。このようなUDPサーバは攻撃を増幅させることができるため標的にされてしまいます。

この種の最も一般的な攻撃では、無防備なDNS、NTP、SSDP、SNMP、CLDAPのUDPベースのサービスを何百万回も利用できます。このような攻撃は、1.3 TbpsのMemcachedベースのGitHub攻撃など、記録的な巨大な量の攻撃となり、DDoS攻撃の大部分を占めています。

反射型アンプ攻撃の武器の主要な地理的分布

NTP

米国	1,318,982
中国	860,444
イタリア	635,071
ロシア	435,364
ドイツ	285,726

DNS リゾルバ

中国	1,202,306
米国	773,555
ロシア	296,374
スペイン	226,252
台湾	164,586

SSDP

中国	1,905,981
ロシア	289,011
台湾	115,220
米国	113,962
イタリア	93,536

SNMP

韓国	293,916
米国	266,637
インド	180,244
イタリア	106,900
中国	99,991

TFTP

中国	308,540
ロシア	260,354
米国	256,517
韓国	244,219
インド	82,877

5G でさらに大規模化する DDoS 攻撃

DDoS 攻撃の規模と巧妙さの進化は加速し続けています。新たな 5G ネットワークが稼働し始めるにつれて、攻撃の規模がこれまでの記録をはるかに超えて大きくなっていくと推測されます。5G によって、新たなスマートワールドの多種多様な IoT アプリケーションと使用形態が利用できるようになりますが、それに伴って攻撃者が利用できる DDoS 攻撃用武器も増えていきます。

エリクソン社は最近、携帯接続される IoT デバイスの数が 2024 年までに 41 億を超えるという予測を発表しました。これらのデバイスは、数が増えるだけでなくその通信速度も増大します。データ通信の高速化、低遅延を実現する 5G が、この急速な拡大を推進する要因となっています。サービスプロバイダーは、これらの増大する脅威に備えて急速に進化して、セキュリティの異常を瞬時に検知して軽減できるようにインテリジェントオートメーションを導入する必要があるでしょう。

> "プロアクティブなインテリジェンスの収集と適用には、攻撃者が使用するインフラストラクチャを攻撃者と同時に特定できるユニークな能力があります。"
>
> — John Bambenek 氏
> ThreatSTOP 社セキュリティリサーチ
> およびインテリジェンス担当 VP

DDoS 脅威インテリジェンス

高度な DDoS 脅威インテリジェンスと、リアルタイムの脅威検知、攻撃に対抗するシグネチャの自動生成を組み合わせることで、攻撃の発生元がどこであるかにかかわらず、最も大規模なマルチベクトル型 DDoS 攻撃に対しても防御を固めることができます。実用的な DDoS 脅威インテリジェンスは、DDoS ボットネットと DDoS 攻撃に利用されやすい脆弱なサーバーの IP アドレスの最新かつ正確なフィードに基づいてブラックリストを作成することで、プロアクティブな DDoS 防衛アプローチを可能にします。A10 Networks とパートナーのセキュリティリサーチャーが、この DDoS 脅威インテリジェンスの最前線に立っています。A10 は、サービスプロバイダーが全範囲における DDoS 攻撃対策を実現できる包括的で集約されたシステムを提供しています。

A10 Networks の DDoS 脅威インテリジェンスの詳細については、弊社の DDoS 脅威マップ https://threats.a10networks.com をご覧ください。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。A10 Networks は 2004 年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10 ネットワークス株式会社は A10 Networks の日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。　詳しくはホームページをご覧ください。

URL：http://www.a10networks.co.jp/
Facebook：http://www.facebook.com/A10networksjapan

LEARN MORE
ABOUT A10 NETWORKS

CONTACT US
a10networks.co.jp/contact

A10ネットワークス株式会社
www.a10networks.co.jp

Part Number: A10-EB-14115-JA-04　SEP 2019