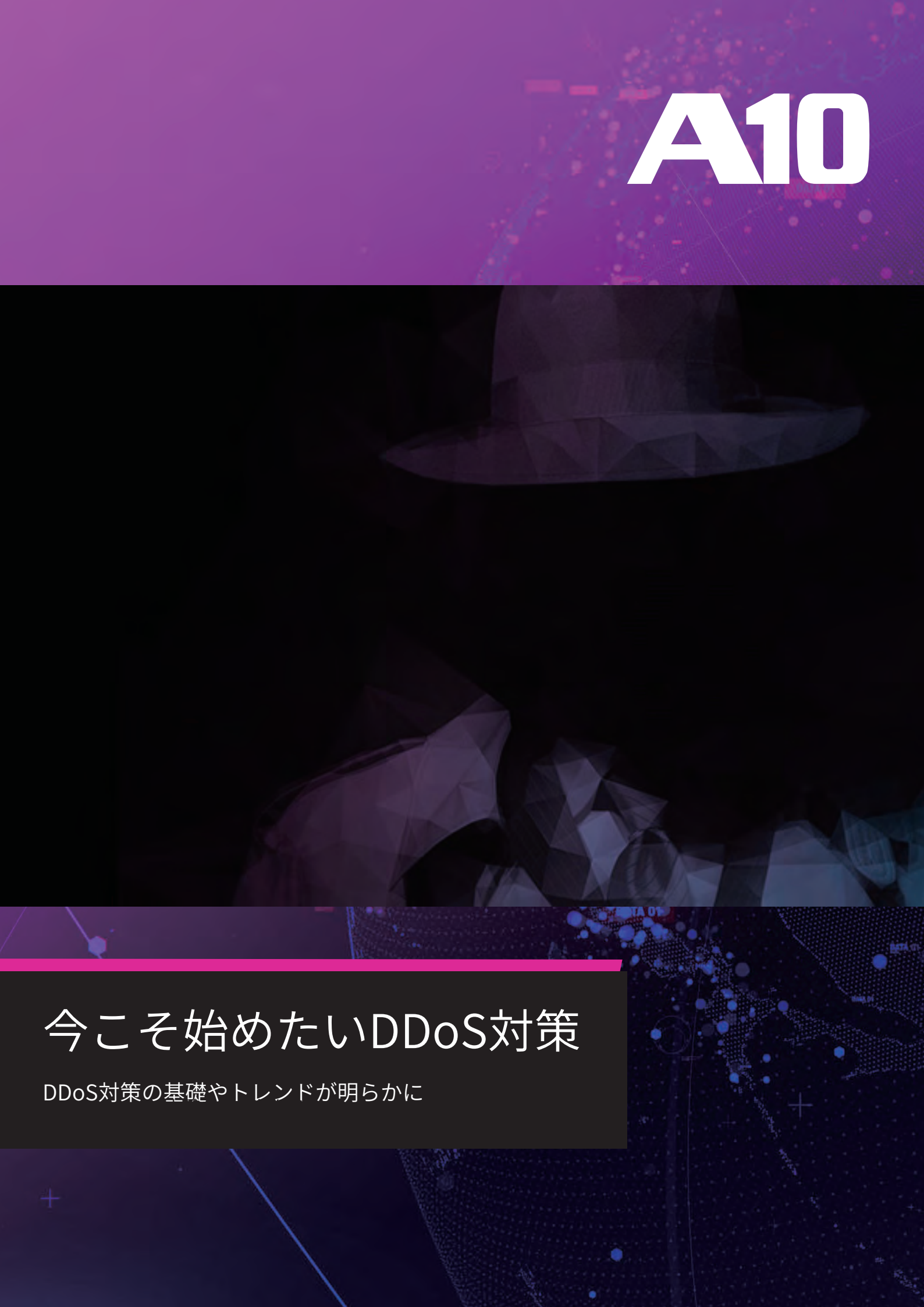

# 今こそ始めたいDDoS対策

DDoS対策の基礎やトレンドが明らかに

目次

# 第 1 章：なぜ DDoS 対策が必要なのか ― DDoS 攻撃が行われる理由

昨今、サイバー攻撃関連のニュースで DDoS 攻撃という単語を耳にする機会が増えてきているのではないでしょうか。他のサイバー攻撃同様に DDoS 攻撃による被害は拡大を続けていますが、筆者の所属する A10 ネットワークスによる 2016 年に首都圏上場企業 100 社に行った調査では“DDoS 対策を行っている企業は 55%”という結果となり、まだまだ対策を行えている組織が少ないのが現状です。本書では、DDoS 攻撃の基礎からその対策方法、最新トレンドなどを紐解き、DDoS 攻撃対策を行うのに参考となるような情報を届けます。

## そもそも DDoS 攻撃とは?

DDoS 攻撃は Distributed Denial of Service の略で分散サービス不能攻撃と訳されます。これは DoS 攻撃(サービス不能攻撃)の一種で、攻撃の目的はその名の通りサービスを不能にすることです。

外部から行われる DoS 攻撃は大きくわけて以下の 2 つに分類できます。

1. Exploit 型
   システムの脆弱性を突く攻撃（Exploit)をすることで攻撃対象のシステムが正常に動作しなくなり機能しなくなるタイプ
2. リソース枯渇型
   回線やアプリケーションや OS で処理できる能力を超えるようなコンピューターリソースへのリクエストを発生させて機能させるタイプ

１の Exploit 型はシステムが想定外の動作を行う攻撃に対応できず最終的に機能停止を及ぼす脆弱性がある場合に有効になります。特にネットワークから攻撃が有効な場合、簡単に攻撃が成立することもあります。

例：BSOD (Blue Screen of Death)を引き起こす Exploit

Microsoft 社の Windows が特定の脆弱性を突いた攻撃などにより Blue Screen 画面になりシステムが停止してしまうことを、一般的に Blue Screen of Death（日本では単にブルースクリーン）と呼びます。

この BSOD を引き起こす有名な脆弱性として、2015 年 4 月の MS15-034（CVE-2015-1635）で修正された HTTP.sys の脆弱性があり、CVSS スコア（脆弱性の深刻度）は最も高い 10 で評価されました。緊急の対応が求められ、セキュリティの現場を騒がせた一例になります。