

# A10

## 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 .....	5
そもそも DDoS 攻撃とは? .....	5
攻撃者はなぜ DDoS 攻撃を仕掛けるのか? .....	6
第2章：事例とデータからわかる DDoS 対策が必要な組織 .....	8
世界と日本の事例で理解する DDoS .....	8
調査で理解する DDoS .....	9
第3章：デジタル化する社会インフラに忍び寄る DDoS 攻撃 .....	13
DDoS の脅威を知らしめた Mirai .....	13
脆弱な IoT デバイスによるボットネット .....	14
ダークウェブ市場で売買される DDoS 攻撃サービス .....	15
2019 年問題と 2020 年問題 .....	17
DDoS 攻撃が目当てじゃないスモークスクリーン .....	17
まとめ：デジタル化する社会インフラに忍び寄る脅威 .....	17
第4章：多様なインフラを狙う DDoS 攻撃の種類と実態 .....	19
狙われるレイヤーとそれぞれへの DDoS 攻撃の手法 .....	19

インフラレイヤー攻撃.....	20
ネットワークレイヤー攻撃.....	20
ネットワーク帯域レイヤー攻撃.....	22
アプリケーションレイヤー攻撃.....	23
まとめ.....	23
第5章：DDoS対策に不可欠なスクラビング機能のアーキテクチャー.....	24
DDoS対策に不可欠なスクラビング機能.....	24
DDoS対策のネットワークアーキテクチャ.....	24
まとめ.....	28
第6章：DDoS攻撃の対策方法（ネットワーク編）.....	30
ネットワークレイヤーを狙ったDDoS攻撃の対策.....	30
ネットワーク帯域レイヤーへの攻撃.....	32
DNSの仕組み.....	33
アンプ攻撃とリフレクション攻撃.....	34
DNSリフレクション・アンプ攻撃の対策.....	35
第7章：DDoS攻撃の対策方法・インフラ編.....	36

インフラレイヤーへの DDoS 攻撃とは.....	36
DNS 水攻め攻撃（ランダム DNS クエリー攻撃） .....	36
権威 DNS の DDoS 攻撃対策.....	37
キャッシュ DNS 側の対策 .....	38
DDoS 攻撃は大容量のトラフィック攻撃だけではない.....	39
第 8 章：DDoS 攻撃の対策方法・アプリケーション編 .....	40
ウェブサーバーを狙った攻撃 .....	40
HTTP フラッド攻撃の対策方法.....	40
スロー攻撃の検知.....	41
SSL への攻撃 .....	43
マルチベクトル型攻撃.....	43
第 9 章：DDoS 攻撃の対策方法・脅威インテリジェンス編.....	45
脅威インテリジェンスとは .....	45
脅威インテリジェンスの DDoS 防御への活用.....	45
第 10 章：ウェブサービスに対する DDoS 対策 .....	49
CDN による DDoS スクラビング .....	49

ウェブサービスの DDoS 対策で重要となる柔軟な IP 経路.....	51
第 11 章：DDoS 攻撃の対策（まとめ） .....	53
保護対象は何か？ .....	53
攻撃のタイプは？ .....	53
ウェブサーバーを想定した場合の保護策.....	54
通信経路から考える DDoS 対策.....	54
まとめ .....	55

## 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のでしょうか。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。