[特集] DoS攻撃

編集にあたって

寺田真敏（（株）日立製作所）

700Mbps

さて，何の数字であろうか？

本特集「**DoS/DDoS 攻撃**☆1**観察日記（2）～Antinny による ACCS サイトへの DDoS 攻撃～**」で取り上げた DDoS 攻撃のピーク時の通信トラフィックである．この観察日記によれば，2005 年 10 月時点で，www.accsjp.or.jp は常時約 4 万の攻撃被疑 IP アドレスから 200,000pps（400Mbps）の攻撃を受けていたとしている．

150 人

この数値は，2013 年 1 月 18 日，Telecom-ISAC Japan のサイバー攻撃対応演習ワーキンググループが主催した 2012 年度サイバー攻撃対応演習の参加人数である．国内大手通信事業者 8 社，重要インフラ事業者 2 社が参加し，DoS 攻撃，DNS サーバの長時間ダウンなどを想定した，約 2 時間半の演習が実施されたとのこと．詳細は，本特集「**DDoS 攻撃に対する通信事業者の取り組み**」に譲るとしても，通信事業者各位のインターネットのセキュリティに対する熱い想いが伝わってくる．

ここ数年の間にも，MITB（Man in the Browser）☆2，APT（Advanced Persistent Threats）☆3 など新たなセキュリティ用語が生まれている．さらに，サイバー攻撃による脅威は，情報システムだけではなく，制御システムなどへとフィールドも広がり，被害の形態も様相を変えてきている．特に，サービス不能攻撃，サービス拒否攻撃，サービス運用妨害攻撃と呼ばれる DoS 攻撃は，インターネット上の各種サービスの安定的な運用を脅かすものとなってきている．そこで，この特集では，DoS 攻撃を対象に，DoS 攻撃対策へのさまざまな取り組みを取り上げることとした．さまざまな視点からの報告を通して，DoS 攻撃対策について再考するきっかけにしたい．

本特集では，大きく 4 つの構成とした．

「**DoS/DDoS 攻撃とは**」では，用語を整理するために，DoS 攻撃手法，DoS/DDoS 攻撃の歴史などについて解説する．

「**DoS/DDoS 攻撃観察日記**」では，DoS/DDoS 攻撃に出会った研究者／通信事業者／サイト運用者の視点から事例を語ってもらう．「**DDoS は身内からもやってくる**」では，やや専門的な技術や用語が使われているところもあるが，DDoS 攻撃の発生原因を解きほぐしていく研究者の雰囲気が伝わると思う．「**Antinny による ACCS サイトへの DDoS 攻撃**」「**ボットネット PushDo による SSL 接続攻撃を振り返って**」は，日記形式で日々刻々と変わっていく対処の状況が描かれているので，読者の皆さんにも対処の雰囲気が伝わるの

☆1 DoS（Denial of Service）：サービス不能攻撃，サービス拒否攻撃，サービス運用妨害攻撃．DDoS（Distributed Denial of Service）：分散協調型 DoS 攻撃，分散 DoS 攻撃．
☆2 ブラウザを利用して，情報の窃取や改ざんなどの侵害活動を行う技術の総称である．
☆3 特定組織を対象とし（標的型），組織内ネットワークを活動基点とした（潜伏型）侵害活動のこと．標的型諜報攻撃とも呼ばれている．

ではないかと思う．**「DoS/DDoS 攻撃対策」**では，対策の前線にいる通信事業者／サイト運用者／研究者の視点から DoS/DDoS 攻撃対策について紹介してもらう．**「ISP における DDoS 対策の現在と課題」**，**「高度化する DDoS 攻撃と対策 サイトの視点から」**は，通信事業者とサイト運用者の視点から対策をまとめてほしいと執筆をお願いした．また，**「ダークネット観測網を用いたバックスキャッタ分析」**では，ダークネットという怪しそうなネーミングからも研究の匂いを感じてもらえると思うが，インターネットでの DoS/DDoS 攻撃活動の広域観測を実現する技術として，より技術的な視点からまとめられている．

「DDoS 攻撃に対する通信事業者の取り組み」，**「DoS 攻撃に対する警察の取り組み」**では，日頃，あまり表には見えてこない活動を取り上げた．インターネット上の各種サービスの安定的な運用が，いろいろな方々の日々の努力によって成り立っていることと，今後，何をしていくべきかについて考える機会となることを願って，特集のまとめとした．

執筆をお願いした方は，いずれも，DoS 攻撃対策に関する研究開発のみならず，実務部門でも非常に多忙を極められている方々ばかりであり，今回の機会に執筆いただいたことにこの場を借りて深く感謝申し上げる．

本特集がきっかけとなって，DoS 攻撃に関する理解が深まることを望んでいる．また，実効性の高い対策のためには，技術のみならず，各組織の持ち味を活かした連携のあり方についても議論を広げる必要があろう．ぜひ，皆の力を結束して，我々の利用するインターネットを安心で安全な環境にしようではないか！

本特集を組むことができたものテレコム・アイザック推進会議（Telecom-ISAC Japan）の活動にかかわりを持てたことにつきる．2006 年 10 月 16 日，Telecom-ISAC Japan は，「Antinny による ACCS サイトへの DDoS 攻撃」の対策活動が認められ，コンピュータソフトウェア著作権協会（ACCS）から感謝状を授与されたとのこと．人のつながりから始まった活動が，組織のつながりとしての活動に広がった．感謝状は，組織が連携した対策活動の証であり，今後のインターネットのセキュリティ対策活動に向けて，新たな一歩を踏み出したことを示している．

最後に本特集を読み進めるにあたり，DoS 攻撃，DDoS 攻撃の用語の使い分けについて解説しておきたい．本特集の原稿の中で，DoS 攻撃と DDoS 攻撃が混在して使われていることがある．この 2 つの用語の使い分けは，著者の方々がその時点で攻撃をどのように捉えるのかによるところが大きいが，次のような視点で，全体としての記述を合わせるようにした．

DoS 攻撃：発信元が 1 カ所からの攻撃事象の場合，攻撃手法そのものを説明する場合，攻撃事象そのものを説明する場合（発信元が 1 カ所か複数かを言及しない場合）

DDoS 攻撃：複数の発信元からの攻撃事象の場合

著者の方々が DoS 攻撃と DDoS 攻撃をどのように使い分けているのかについても目を向け読み進めていただければ幸いである．

（2013 年 3 月 11 日）