column

DoS攻撃に対する警察の取り組み

田村研輔　中山毅彦（警察庁情報技術解析課）

DoS（Denial of Service）攻撃は，目新しい攻撃手法ではありませんが，比較的容易に実行でき，決定的な防御方法もないことから少々厄介な攻撃であると言えます．2012年6月には国際ハッカー集団「アノニマス」の関与が疑われるDoS攻撃により，政府機関等のサイトの閲覧に支障が出るなどの被害が発生しました．また，2012年9月には尖閣諸島に関する緊張状態の高まりの中，複数のサイトが閲覧困難な状況になったことが確認されています．

DoS攻撃では攻撃の発生を防ぐことは困難ですので，いかに被害を最小限に抑えるかが焦点になってきます．このコラムでは，DoS攻撃対策における警察の取り組みの一例を紹介したいと思います．

DoS攻撃とは？

DoS攻撃はサービス不能攻撃と呼ばれ，サーバ本来の機能を阻害する攻撃です．DoS攻撃には，多くの人が手動で一斉にデータを送信したり，ツールやボットネットを利用して自動的に大量のデータを送信することでサーバの処理能力や回線の許容量を超える負荷を与えてサービスの提供を困難にする方法があります（図-1）．

一方，サーバの脆弱性と呼ばれるプログラムの欠陥を悪用した特殊なデータを送信することにより，サービスの負荷を高め，サービスを停止させる方法もあります．後者については，修正パッチ等により脆弱性をなくすことで被害の発生を抑えることが可能ですが，前者については悪意のある「正常な通信」ですので対処が難しいところです．

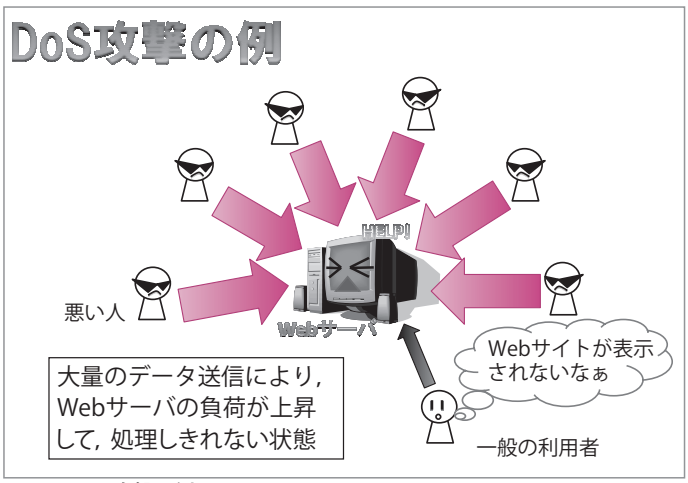

図-1　DoS攻撃の例

警察におけるDoS攻撃対処の例

それでは，DoS攻撃対処の例について，過去の実例を紹介しましょう．

2012年9月18日に中国を発信元とするDoS攻撃が発生したときのことです．警察庁では，9月12日頃から攻撃に関する情報を入手していました．このような攻撃情報の入手元は事案ごとにさまざまですが，このときの情報元は中国の大手チャットサイトでした．日本の複数の政府機関等へのサイバー攻撃を呼び掛けるメッセージが書かれており，実施日，方法，攻撃用ソフトウェアのダウンロード先や，使用方法を説明する動画へのリンク先等が記載されていました．

警察庁では攻撃対象とされたWebサイトに関する観測の強化を実施するとともに，攻撃に関する情報を収集し，攻撃対象として指定された政府機関や，Webサイトの閲覧に支障が生じた政府機関に対して，内閣官房と連携の上，DoS攻撃に関する注意喚起を実施しま

@police における情報発信について　http://www.npa.go.jp/cyberpolice/

警察庁では，情報発信用サイト「@police」をインターネットで公開しています（図 -2）．

@police では，OS やソフトウェアに関する脆弱性情報のような一般の人向けのセキュリティ情報の提供に加え，後述するリアルタイム検知ネットワークシステムによるインターネット観測・分析結果（図 -3）を技術者の人向けに公開していますので，興味のある方はぜひご覧ください．

図 -2　@police の Web サイト

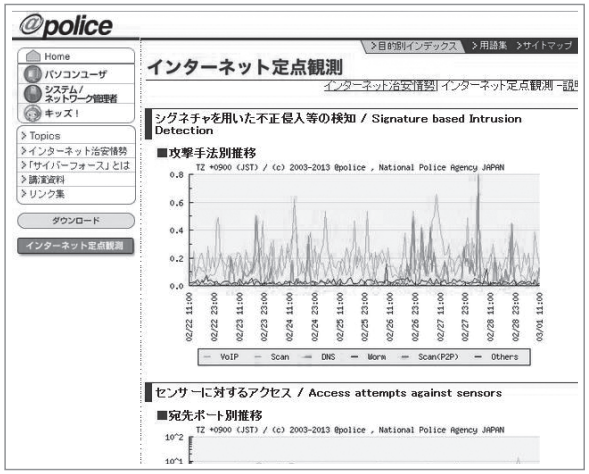

図 -3　リアルタイム検知ネットワークシステムによる観測データ

した．

また，DoS 攻撃等の被害の生じた事業者等に対し，必要な対処について助言するなどの被害拡大防止措置を講じました．

サイバーフォースセンターの活動

警察庁では，これらの攻撃に関する技術的な情報の収集や分析を，サイバーフォースセンターで行っています[1)]．サイバーフォースセンターは 24 時間体制でサイバーテロの予兆把握に努めるとともに，集約された情報を分析し，その分析結果を重要インフラ事業者等へ提供しています．

サイバーフォースセンターでは，インターネット上の攻撃等を認知するため，リアルタイム検知ネットワークシステムを運用しています（図 -3）．このシステムにより得られた技術的情報とその他の情報を調査・分析することにより，DoS 攻撃の予兆や発生を早期に認知し，それらへの対処を行います．ここではリアルタイム検知ネットワークシステムの機能とその活用について少し紹介します．

■ 定点観測による DoS 攻撃の検知

DoS 攻撃には，大量のパケットを送信する手法があることは冒頭にお話ししたとおりですが，その中でも発信元を詐称したパケットを大量に送りつけるタイプの攻撃が用いられることがあります．通常，Web ページの閲覧などを行う場合，閲覧を行う PC と Web ページを公開している Web サーバとの間で数回の情報のやりとりが行われます．このやりとりにはルールが決められていて，攻撃を受けたサーバは定められたルールに従い，発信元 PC に返答します．ところが，発信元の IP アドレスが詐称されている場合，詐称に使われた発信元の IP アドレスに返答を送ってしまいます（図 -4）．

リアルタイム検知ネットワークシステムの機能の 1 つであるインターネット定点観測ではインターネット上に設置された複数のセンサでこれらのパケット（跳ね返りパケット，または，バックスキャッタと呼ばれています）の状況を観測しています．同一のサーバからの跳ね返りパケットが大量に観測される場合は，そのサーバが大量の「発信元の IP アドレスを詐称したパケット」を送りつけられている，つ

まり DoS 攻撃を受けている可能性が高いと考えられるわけです．

発信元を詐称した攻撃パケットは一般的なインターネットサービスでは用いられることはないため，これらは攻撃専用のツールで行われていると考えられます．

■ ボットネットの C&C サーバの無害化措置

リアルタイム検知ネットワークシステムのサブシステムとしてボットネット観測システムがあります．ボットネットとは攻撃者の管理下に置かれたボットに感染した PC で構築されたネットワークです．ボットネットは C&C サーバと呼ばれる指令用のサーバで管理されており，ボットとなった PC は C&C サーバの命令で，所有者の意図にかかわらず DoS 攻撃等を行います．このため，ボットネットの活動を止めるには，指令塔である C&C サーバの活動を無害化する必要があります（図 -5）．

ボットネット観測システムでは，観測用の環境でボットを動作させ，ボットの動作を観測し，接続先や送信データ等の C&C サーバに関する情報を収集しています．その情報から国内に C&C サーバの存在が確認された場合には，当該サーバの管理者のもとに赴き，不正なプログラムの除去等を実施するなど，C&C 化されたサーバを無害化する措置を行っています．

本コラムでは警察の DoS 攻撃対策として活用しているシステムの機能の一部とその活用について紹介しましたが，このほかにもさまざまな情報収集や分析を行っており，これらを用いて DoS 対策に取り組んでいます．このような技術的な対策を考える上では，ネットワーク技術の進化や攻撃手法の巧妙化の影響が大きいため，これらの動向にも引き続き注意していく必要があると考えています．

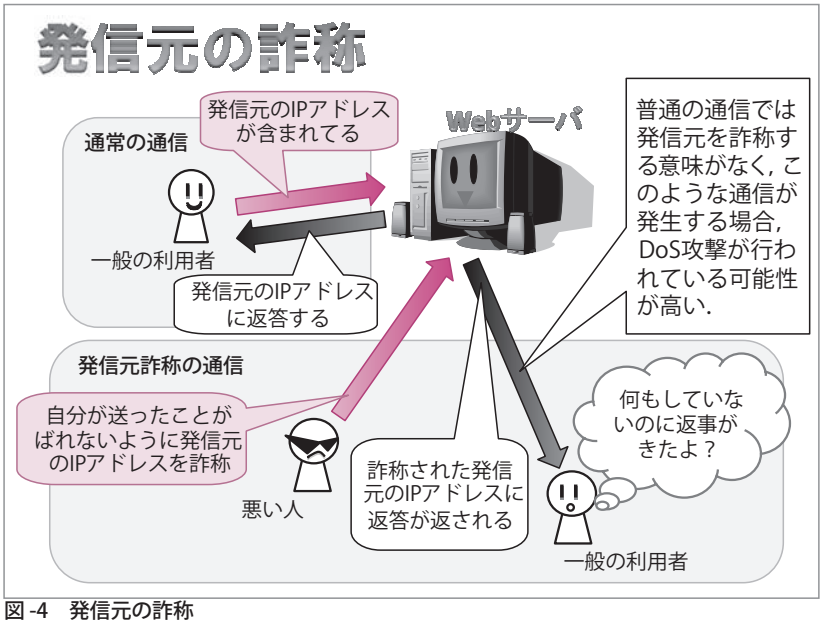

図 -4　発信元の詐称

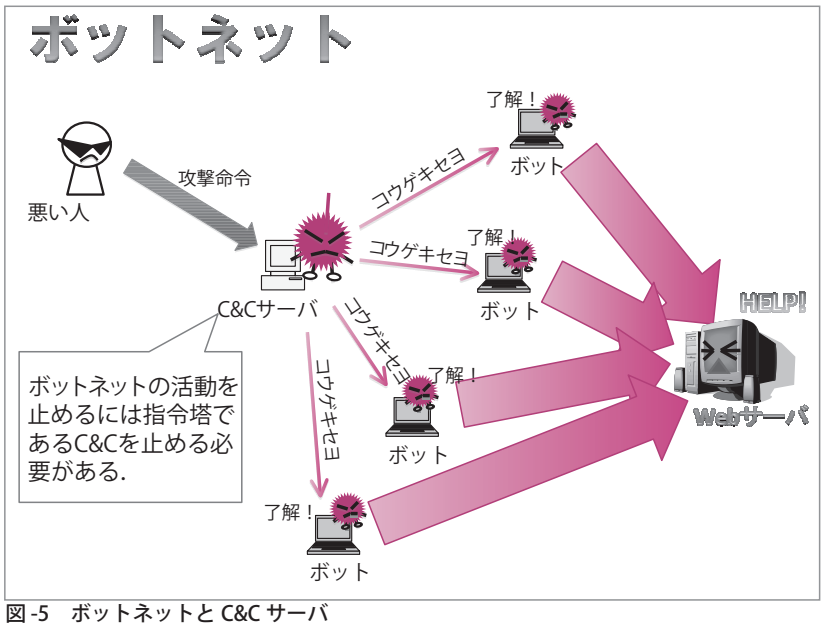

図 -5　ボットネットと C&C サーバ

2012 年 12 月 27 日受付）

参考文献

1）警察庁セキュリティポータルサイト @police, http://www.npa.go.jp/cyberpolice/index.html

■田村研輔
警察庁情報技術解析課に所属．

■中山毅彦
警察庁情報技術解析課に所属．