# ハッカーの手口　岡嶋裕史

・ボット

一昔前はいかに派手なことをするかが競われていたのですが、ここ最近のウイルスでそれは主流ではありません。いかに深く静かに潜行するかがクラッカの腕の見せ所になっています。

せっかく自分が作ったウイルスが他人のパソコンでひっそりと蟄居して、クラッカは何が楽しいのでしょう。実はこのウイルスはクラッカの指示を行儀よく待ち続けています。あるとき、クラッカが「迷惑メールを出せ」、「あのサーバを攻撃しろ」と指示を出すと、それを忠実に実行します。

こうしたウイルスを特に「ボット」と呼ぶことがあります。ロボットのようにクラッカのいいなりに動くからです。ボットに感染したパソコンはゾンビパソコン、ゾンビパソコンの集合体をボットネットといいます。

ボットネットは大きいにこしたことはありません。それだけ大規模な活動ができますし、同じことをするにしてもゾンビパソコンの負担を減らすことができます。

たとえば、クラッカが迷惑メールを１万通出す仕事を請け負った場合、ゾンビパソコンが１台しかなければ、そのパソコンから１万通の迷惑メールを出す必要があり、これはまず間違いなくウイルスの存在がバレます。

しかし、ゾンビパソコンが１万台あれば、１台のパソコンが出す迷惑メールは１通で済み、ウイルスの感染が発覚する確率を大きく下げることができます。

腕のいいクラッカは、自分の支配下にあるボットネットに数百万～一千ガ台のゾンビパソコンを持っていると言われています。それらは、普段おとなしくしてまったく感染を疑わせず、あるとき突然牙をむくわけです。

・3 ウェイハンドシェイクと DoS 攻撃

「3 ウェイハンドシェイク」をご存じでしょうか。堅気の生活をしていてご存じでしたら相当なマニアですが、ネットワーク上の通信の信頼性を向上させる手法の一つです。

といっても大層なことをしているわけではなく、通信を始めたいパソコンが、目的のパソコンに向かって「通信させてよ（SYN)」とメッセージを送ります。

これが無事に届くと、目的パソコンは「いいよ（ACK)。そっちこそ大丈夫なの？（SYN)」と返事を返してくれます。それに対し「もちろんだよ（ACK)」と返答することで、互いの通信準備やこれまでの通信に問題がないかを確認することができます。

この 3 回のやり取りが握手をしている様に似ているので、「3 ウェイハンドシェイク」というのです。メールを送ったり、ホームページを見に行ったりするとき、ふつうに使われているとても一般的な通信確認手段です。

ところで、「SYN」や「ACK」は一つの通信ですから、パソコンは自らの資源（CPU やメモリ）をこの通信に割り当てて処理を行っています。通信が終わるまで、CPU やメモリの割り当て部分はこの仕事に従事するわけです。もちろん、仕事が終われば、割り当てられていた CPU やメモリは解放され、別の仕事に振り分けられることになります。

ここでクラッカは考えるわけです。「通信に使っている CPU やメモリを解放させなければ、いつか資源が足りなくなってパソコンを機能不全に追い込めるのでは？」

では、具体的にどうすれば、一パソコンの資源を枯渇させることができるのでしょう？

3 ウェイハンドシェイクの場合は簡単です。まずクラッカは目標に定めたパソコンに SYN を送って、「通信しようよ！」と誘います。パソコンはあまり人を疑うことを知りませんから「どうぞどうぞ（SYN、ACK)」と返信します。それをクラッカは無視するのです。

3 ウェイハンドシェイクの正規の通信手順では、次にクラッカから最終確認である ACK 通信が返ってくるはずなので、パソコンは辛抱強くそれを待ち続けます。そのために CPU とメモリを使いながら。

このとき、クラッカはきちんと ACK を返信して通信を始める気などさらさらないわけですから、「待ち」の状態に入っている CPU とメモリは無駄になっています。

これが一つや二つであれば問題ないかもしれませんが、クラッカは何千回も何万回も「通信しようよ（SYN)」と呼びかけては待ちぼうけをくらわせます。そのたび、少し

ずつ少しずつ資源を消費させられ、いつかは割り当てる資源がなくなって機能不全に陥るわけです。

これを回避する手段はあるでしょうか？　先ほどの ping のように「3 ウェイハンドシェイクを禁止してしまう」というのはどうでしょう？

できなくはないのですが、先ほども述べたように 3 ウェイハンドシェイクはとても一般的な通信確認手段です。メールもホームページを見せてもらう通信も、3 ウェイハンドシェイクを利用しています。「3 ウェイハンドシェイクは禁止！」と一律に決めてしまうと、メールのやり取りや、ホームページの閲覧ができなくなってしまいます。

1 台のコンピュータから短期間に何万回も SYN 要求がきていたら、それは明らかにおかしいですから、「クラッカかな？」と疑えますが、クラッカは例のボットネットを持っています。1 台 1 台のゾンビパソコンからの SYN 要求は常識的な範囲におさえつつ、攻撃することができるわけです。

「じゃあ、短期間に SYN 要求が集中したら、それがたとえたくさんのコンピュータから送られてきたものであっても拒否しちゃおうかな」という対策は可能です。しかし、たくさんのコンピュータからの SYN 要求が集中するというのは、日常の中でもあり得る話です。

新製品の発表があったり、ニュースで取り上げられたりして自社ホームページが急に見られるようになったとか、自分のブログにはっちゃけたことを書いてしまい炎上したとかいうことは、だれしも遭遇するかと思います。

そのとき、（……後者であれば遮断して苦かもしれませんが）前者の通信を遮断してしまっては大切な業務機会を失ってしまいます。

「ping」や「3 ウェイハンドシェイク」を利用した攻撃（それぞれ ping flood、TCP SYN flood という名前がついています）に代表される、普段ふつうに使っているしくみを巧みに利用してコンピュータを機能不全に追い込む方法を DoS 攻撃（サービス妨害攻撃）といいます。DOS 攻撃の場合、一つ一つは不正な通信とはいえない（普段メールやホームページをやり取りしているのと同じ手順）けれども、それを大量に行うことで相手のコンピュータに迷惑をかけるので、たとえば優良顧客が行うまっとうな通信ときちんと切り分けることが非常に難しいのです。下手に遮断してしまえば、大事なお客さんの通信も遮断してしまいかねません。非常に悩ましい、タチの悪い攻撃方法であるといえます。

・エストニアへの DOS 攻撃

2007 年 4 月、エストニアに対する DOS 攻撃が行われました。DOS 攻撃自体は珍しくありません。ちょっと名の知られた企業であれば毎日受けています。世の中には適当に標的を見つけて DOS 攻撃をしかけてまわるソフトウエアすらあるので、私のような何の取り柄もない個人の家のルータにすら、たまにお鉢が回ってきます。

しかし、エストニアのそれは量の面においてとんでもないものでした。国連加盟国の 4 分の 1 ほどの国に分散配置された膨大なゾンビパソコンからエストニアに向けて通信が放たれました。

通信はありとあらゆる手練手管によって、その量が増幅するよう工作されていました。これは飽和攻撃といってよい水準です。

飽和攻撃という考え方は昔から、あるいは戦争というもののパラダイムが変わる以前からありました。

・・・

エストニアに対して行われた攻撃は、サイバー戦における大規模を飽和攻撃でした。行政も金融も報道も通信も攻撃を受け、主要銀行 2 行が業務を停止しました。

エストニアは電子立国を標榜していた国なので、サイバー戦に対して無策だったわけではありません。しかし、このくらいの規模の攻撃になると、冗長化されたネットワークも侵入検知システム（IDS）も余裕を持ったキャパシティ計画も、ものの役に立ちません。単純な物量攻撃を前にして、すべてが無力化されます。

本書でも触れたように、DOS 攻撃自体に必要な技術水準はさほど高くありません。もちろん、それを準備するためのボットネットの構築や秘匿に尋常でないテクニックが要求されるわけですが、人海戦術が可能であれば頭数だけ揃えて今すぐにでも実行することができます。そのとき集める人たちには、パソコンをいじったことがある程度のスキルがあれば十分です。