国家も揺るがす!? インサイバー攻撃を

国家の運営、企業のビジネスから私たちの生活まで、インターネットが不可欠になった今、新たな脅威となっているのがサイバー攻撃だ。一体どんな目的で、どんな攻撃をしかけてくるのか。攻撃を防ぐためにどんな対策が行われているのか、最前線を取材したゾ!

取材協力／独立行政法人情報通信研究機構 ネットワークセキュリティ研究所 サイバーセキュリティ研究室 井上大介室長
取材・文／塩野祐樹

井上大介

大学院博士課程後期修了後、2003年、独立行政法人通信総合研究所（現NICT）に入所。新世代モバイル研究開発プロジェクトでのセキュリティ研究を経て、2006年よりインシデント分析センターnicterを核としたネットワークセキュリティの研究開発に従事。工学博士。

日本に送られてくる不正なデータをリアルタイムに表示している最先端のサイバー攻撃分析システムの画面。世界中から攻撃を受けているようすが一目瞭然だ（提供：情報通信研究機構）

愉快犯から金銭目的へ

2011年4月、プレイステーションで有名なソニー・コンピュータエンターテインメントが大規模なサイバー攻撃を受けてオンラインサービスが一時停止、合計で1億件以上の個人情報が流出するという事件が発生した。さらに9月には三菱重工業のコンピューターが、10月には国会議員のコンピューターへの攻撃が報道され、システム情報やID、パスワードなどの流出が明るみになった。これらの事件は、新聞やテレビでも大きく報じられたので、覚えている人も多いだろう。

サイバー攻撃とは、他人のコンピューターに不正に侵入して情報を盗んだり、特定のウェブサイトに大量のデータを送りつけてサービス停止に追い込むなど、ネットワーク上で行われる攻撃のことだ。

一般家庭にパソコンが普及し始めた1980年～90年代は、コンピューターに悪さをするウイルスを、メールなどで不特定多数に送りつけて、モニター上にウイルス感染したことを表示させたり、パソコン内のデータを破壊したりといった攻撃がほとんどだった。攻撃者はウイルスをつくって広めるだけの愉快犯であることが多く、社会に大きな被害を及ぼすものではなかったといえる。

ところが2000年代に入ると、サイバー攻撃は主に金銭目的の組織的な犯罪となっていく。攻撃者はネットでビジネスを行う企業のウェブサイトをダウンさせて金銭を要求したり、コンピューターから盗み出した個人情報やクレジット情報などをブラックマーケットで売買して稼

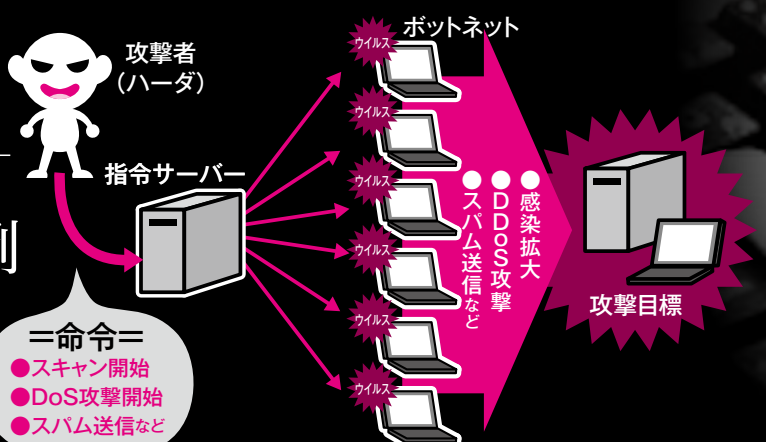

図1 ボットネットを使った
サイバー攻撃の例

ボットと呼ばれるマルウェアに感染したボットネット（一般のパソコンなど）は、攻撃者に操られてサイバー攻撃の加害者となってしまう。