Q 勝手に通信しているプログラムを見つけたい

パソコンを使っていない時間も、Wi-Fiルーターのランプが点滅しています。どうやら何らかのプログラムが、勝手に通信をしているようです。どのプログラムなのか、調べる方法はありますか？

A Windowsには、ユーザーが操作していないときも外部と通信をするプログラムがいくつかあります。Windows Updateなどがそうです。これらを簡単に見つける方法を紹介しましょう。なお、ウイルスはこれから紹介する方法で見つけることは困難です。不審に思ったらセキュリティ対策ソフトを活用しましょう。

2つのコマンドを使ってパソコンを調査する

netstat　TCP/IPによる通信状態を表示する

コマンドの書式

netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]
詳細は「netstat -?」を実行

実行するコマンド

netstat -a -n -o

-a	全てを表示
-n	IPアドレスをドメイン名に変換しない
-o	プログラムのプロセスIDを表示

tasklist　実行中のプログラムのリストを表示する

コマンドの書式

tasklist [/S システム [/U ユーザー名 [/P [パスワード]]]]
[/M [モジュール] | /SVC | /V] [/FI フィルター] [/FO 形式] [/NH]
詳細は「tasklist -?」を実行

実行するコマンド

tasklist

図1　パソコンの通信状態と、実行中のプログラムを調べるコマンドを使う。どちらも、コマンドプロンプトでキーボードから入力して実行する

今行われている通信は、「netstat」というコマンドで一覧表示できます（図1）。コマンドプロンプトで「netstat -a -n -o」と入力すると、5カラム目の「PID」に、通信中のプログラムのプロセスIDが表示されます（図2）。次に「tasklist」コマンドを入力します。するとそのプロセスIDを使っているプログラムのファイル名が分かります。

なおnetstatの出力のうち、「状態」が「CLOSE_WAIT」「TIME_WAIT」になっているものは通信が終了しています。「外部アドレス」は通信相手です。調査サイト「http://www.iplocationfinder.com/」などで調べるとよいでしょう。

（塩田 紳二＝テクニカルライター）

コマンドを実行してみる

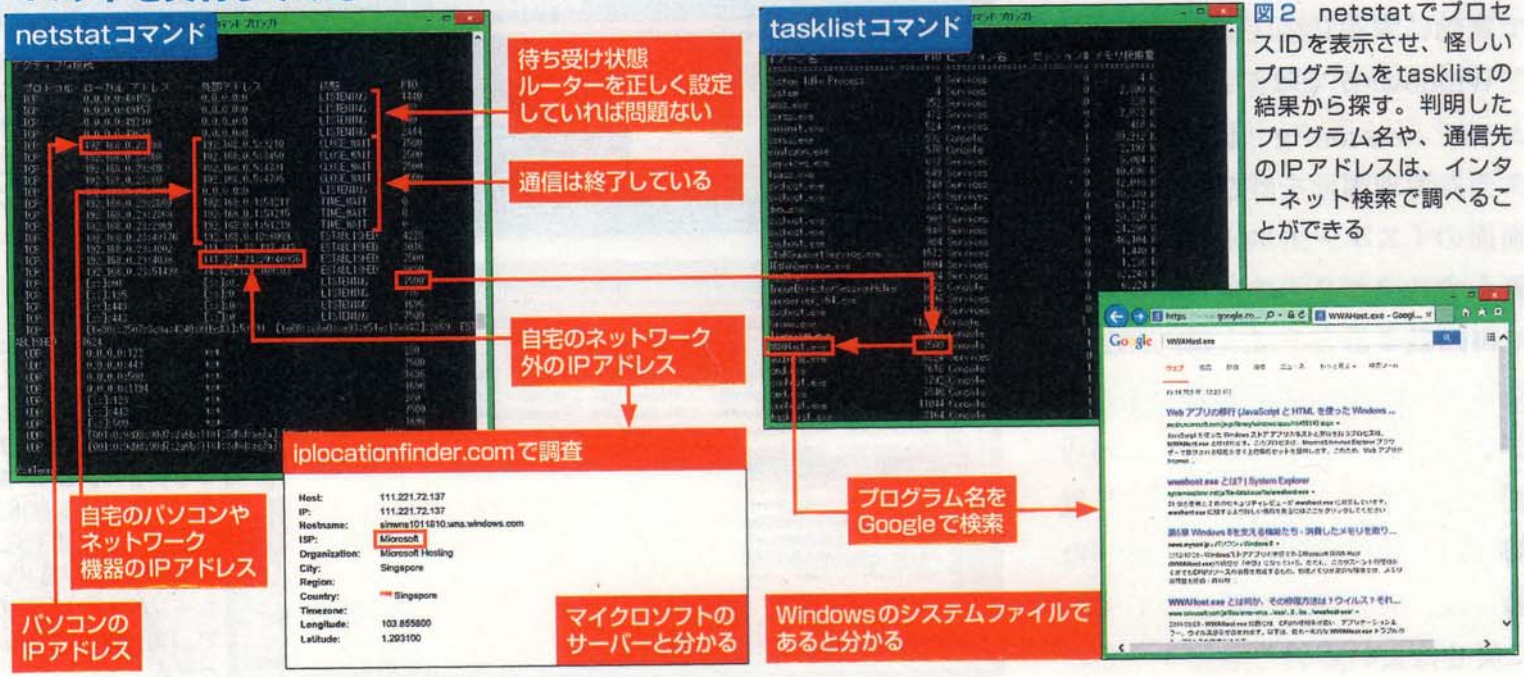

図2　netstatでプロセスIDを表示させ、怪しいプログラムをtasklistの結果から探す。判明したプログラム名や、通信先のIPアドレスは、インターネット検索で調べることができる