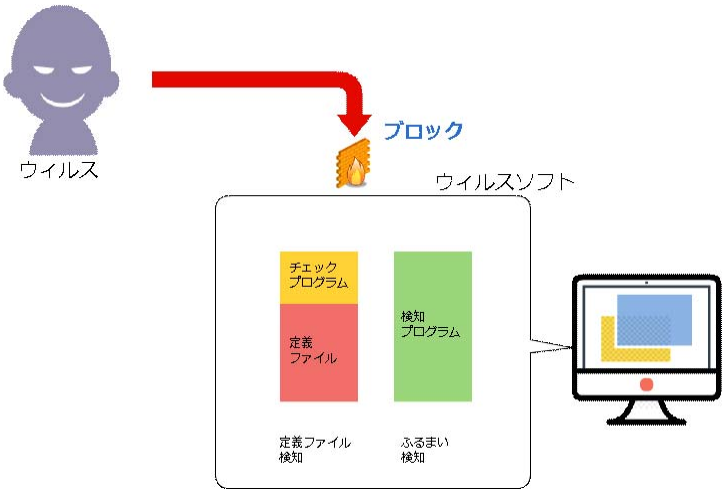
■ ウィルスソフトの仕組みをザクッと解説

ウィルスソフトの違いってなんですか？

「ウィルスソフトってたくさんあるけどどう違うの？」、「値段の高いのと安いのの違いってなんなのさ」という方はたくさんいらっしゃるのではないでしょうか。
今回のかわら版では、そこのところをザクッとご説明したいと思います。
最近はウィルスソフトもたくさんの機能をもつようになりました。とはいえ、ウィルスソフトの基本は「ウィルスの検知と駆除」です。下にウィルスソフトの検知方法を書きました。



図：ウィルスの検知方法

検知方法は大きく2つあります。
・定義ファイル検知　：　過去のウィルスデータベース（定義ファイル）をもとにチェックプログラムでチェックする。
・ふるまい検知　：　ウィルスっぽいデータの特徴から検知する。

最近は新種のウィルスが多く、「定義ファイル検知には限界がある」と考えられています。そこで脚光を浴びているのがふるまい検知です。

この「2種類の検知方法でウィルスをチェックできるか」がウィルスソフトの第1の違いです。ふるまい検知には「定義ファイル検知よりも速い」、つまり「パソコンがモッサリしない」という良い性質もあります。『高速』を売り物にしているウィルスソフトは、ふるまい検知に力をいれているソフトウェアと言えます。
ふるまい検知は比較的新しい技術ですが、定義ファイル検知も侮れません。というのも「古いウィルスを検知できるのか」というのが、ウィルスソフトの良否を決める第2のポイントだからです。古い定義ファイルをたくさん持つとパソコンが超遅くなってしまいます。ですので、安いウィルスソフトの中には古いウィルス定義をもっていないものがあります。
何年か前、ウィルス駆除を行ったときに、「nimda（ニムダ）」という 2001 年に流行したワーム（ウィルスの一種）が検出されて驚いたことがあります。中古のパソコンとかは危ないですよね。
上の2点を満足しているウィルスソフトが『ビジネスユースとして必要最低限の機能がある』といえます。