ケーブル技術スタッフの機器チェック!

日々開発されるケーブルテレビ関連機器を、技術スタッフが厳しい目でチェック! 実用性に焦点を当てて報告します。

No. 67

ウィルスチェック

豊島ケーブルネットワーク(株) 技術部 部長　上山裕史

今回はウィルスを検知し削除されたかを確認するための便利な方法を紹介します。

ケーブルテレビ局では、ISP(インターネット接続プロバイダ)としてさまざまなウィルスチェック機器を使用しています。

インターネットのウィルスは、PCで悪意のある動きをするようにプログラムされたソフトウェアです。メールを読んだり、ホームページにアクセスすることで動作させるものです。これに対抗するためPCではウィルス検知ソフトをインストールし、ファイヤーウォールではウィルス削除をコマンドで指示します。ここで正常にウィルスを検知して削除するかを確認するために便利な方法を紹介します。

まず、確かにウィルスではありますが、悪さをせず、どんなウィルス検出ソフトでも検知される標準とも呼ばれるウィルスが図1です。「EICAR test file」でEuropean Institute for Computer Anti-Virus Researchという団体に由来するもので、ウィルス対策製品の検知を確認するためのツールです。短い英文字、数字の組み合わせからなります。

これは、PCにおいてcomファイルという実行ファイルの形でありながら、英数字で可読できる16進数です。WindowsのPCであれば、メモ帳で図1の文字列を間違いなくタイプして名前をつけて保存すれば、ウィルス検知ソフトが発見して削除するか、または削除済みであることを通知してくれます。これでインストールしたウィルス対策ソフトが正しく動作していることがわかります。

図2は、このようにして作成したEICARテストファイルを、ハードディスクの完全スキャンにより検出し、削除した様子がログとして記録されて様子を示します。ウィルス対策ソフトの仕様にもよりますが、zipで圧縮したファイルでも検出しているのがわかります。

ISPのウィルス対策機器の確認では、ウィルス対策ソフトをオフにして、EICARテストファイルをメールに添付してメール送信したとき、望む動きをファイヤーウォールやメールサーバが行うかの確認が出来ます。

ウィルス対策製品の動作確認のときに、有害なウィルスを所持していることはまずありません。動作確認が出来ず、実戦でウィルス検知されるまで待つのも不安が募ります。このようなとき、EICARテストファイルは便利に使用できます。

ウィルス検知ソフトを常に最新の状態に保つことも重要ですが、最初の一歩として検知できるようにインストールされているかの確認が大切になります。

予防保全の見地や確認の意味で、ウィルスチェックが確実に行われているか確認するのはとても必要なことです。

```
X5O!P%@AP[4¥PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

図1:どんなウィルス検出ソフトでも検知される、標準とも呼ばれるウィルス「eicar」

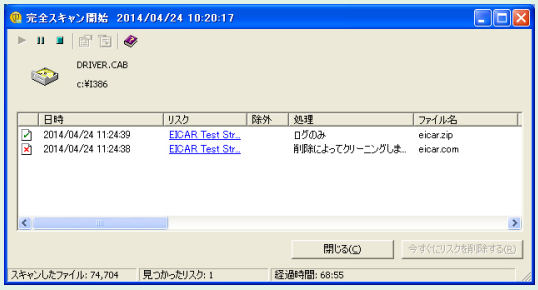

図2:EICARテストファイルを、ハードディスクの完全スキャンにより検出