１５．コンピュータウィルス

１．最近のウィルスの傾向

コンピュータウィルス（以下「ウィルス」という。）は、コンピュータに寄生して利用者の意図しない動作を行おうとする小さなプログラムです。

最近では利用者の意図しないうちにコンピュータのメール送信ソフトウェアを悪用し、自分自身のコピーを送りつけたり、ネットワークで共有されているフォルダに感染活動を試みる「ワーム」と呼ばれるタイプが多くなっています。

ウィルスに感染すると、コンピュータ内のデータを損傷する、データを外部にばらまく、あるいは複数の感染コンピュータを束ねてネットワークに過剰な負荷をかけるなど、**感染元だけでなく周囲を巻き込みます**。利用者本人が気がつかないうちに被害を受けてしまうことはもちろん、**ウィルスがきっかけで実生活の人間関係まで傷つけてしまうことがあります**。

２．ウィルスに感染されないための基礎知識

①ウィルス対策ソフトウェアをコンピュータにインストールし、最新の状態を維持します。情報科学室のコンピュータは導入済みですが、必ず自宅のコンピュータにも導入し、ネットワークに接続するたびに最新の状態にしておきましょう。また、コンピュータのセキュリティアップデート[7]が自動的に行われるようにしておきましょう。(大学のコンピュータは自動的にセキュリティアップデートされています。) AdobeFlash、AdobeReade、Java Runtime なども最新の状態に保つ必要があります。

②電子メールの添付ファイルやインターネットからダウンロードしてきたものは、必ずウィルスチェックをしてから開きましょう。

③万が一感染してしまった時の復旧作業のために、リムーバブルメディアなどに文書をコピー（バックアップ）しておきましょう。

常に新しいウィルスが現れており、対策ソフトウェアでも処理できないことがあります。次に紹介する Web ページや、ニュースに注意しておくことを強くお勧めします。万が一ウィルスに感染してしまっても、あわてずに行動してください。

どうしたらよいかわからない、また心配なときは情報環境センターに相談してください。

[7] Windows なら「自動更新」を有効にし、自動的に Windows Update されるようにします。MacOS なら「ソフトウェア・アップデート」のアップデートの確認期間を選択します。

３．主なウィルス・セキュリティ情報源

・情報処理振興事業協会セキュリティセンター　http://www.ipa.go.jp/security/
・トレンドマイクロセキュリティ情報　http://www.trendmicro.co.jp/vinfo/
・シマンテックセキュリティレスポンス　http://www.symantec.com/region/jp/avcenter/
・マカフィースレットセンター　http://www.mcafee.com/japan/security/

等々

４．情報科学室のウィルス対策

清泉女子大学ではトレンドマイクロ社の「ウィルスバスターコーポレートエディション（以下、「ウィルスバスター」という。）」とバラクーダネットワークス社の「Barracuda Spam Firewall（以下「バラクーダ」という。）」を使用しています。実際に情報科学室でウィルスが発見されたときの動きを確認してみましょう。

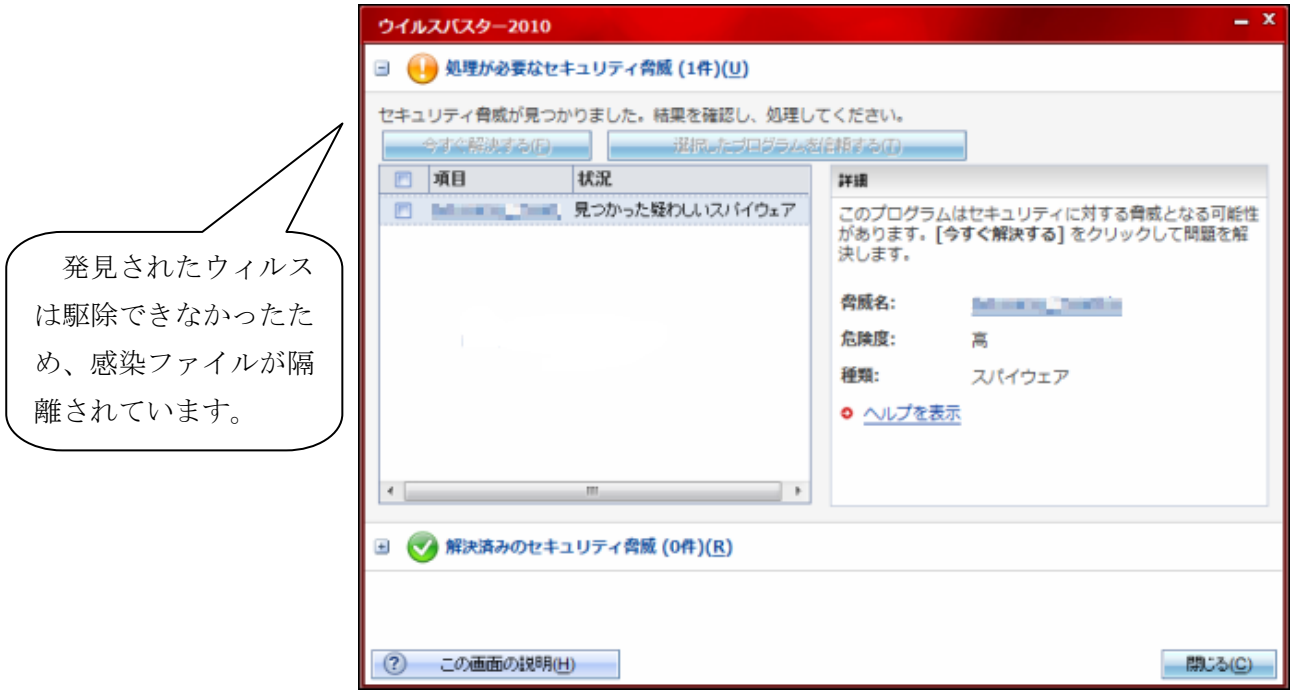
ウィルスバスターの動作

ウィルスバスターは、ウィルスを発見するとまず「駆除」できるかを調べます。駆除できるようなら、ウィルスを駆除して正常な状態に戻します。Word や PowerPoint などの文書がウィルスに感染しているようなら、ウィルス部分だけを駆除するように試みます。

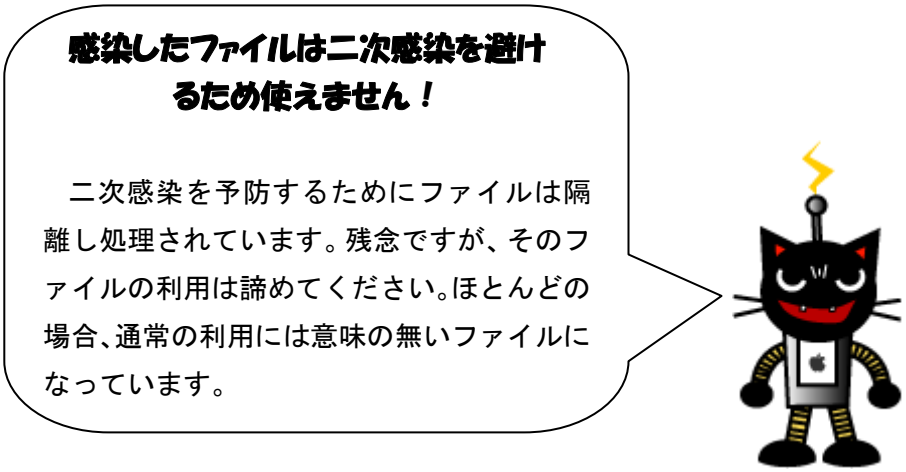
駆除できないウィルスであれば、感染の拡大を防ぐためにウィルス自身を「隔離」してしまいます。最近のウィルスは文書に感染するものよりも、意味のないメールにウィルス自身が添付されているものが多く、駆除されずに隔離されるものがほとんどでしょう。

自分のリムーバブルメディアが感染していたら？

ウィルスバスターは、ウィルスを検出する状況によって動作が異なります。インターネットからダウンロードしたファイルや、USB メモリ等に保存したファイルがウィルスに感染していると、次のようなメッセージが表示されます。



をクリックしてウィンドウを閉じると、パソコンの利用を続けることができます。発見されたのはウィルスだったため、このファイルを使うことはできません。



バラクーダの動作

バラクーダというシステムは迷惑メール（スパムメールとも言う）やウィルスを、大学にメールが届く前にチェックしてくれます。メールを機械的に分析し、迷惑メールやウィルスの可能性が高いと判定されれば、そのメールを隔離します。

しかし判定結果が必ずしも信頼できるとは限らず、安全なメールが迷惑メールだと勘違い判定されてしまうことも少なくありません。

この問題を解決するために、バラクーダは学習型フィルタ（または「ベインジアンフィルタ」）と言いう手法を採用しています。利用者が間違った判定を修正することで、利用者の傾向にあった判定ルールを「学習させる」ことができます。

５．学校のウィルス対策のまとめ

学校でウィルスに感染したファイルが、どのように処理されるかをまとめています。

【ウィルスの処理方法】

ウィルスの場所	処　理　方　法		
	検出タイミング	○駆除に成功	×駆除に失敗
マイドキュメントやUSBメモリの中	ファイルを開こうとしたとき	ウィルス駆除報告のメッセージが表示されます。	ウィルスが隔離報告のメッセージが表示されます。
ダウンロードファイルやメールの添付ファイル	メールサーバへ到着する前（バラクーダ）	バラクーダがネットワーク上の場所に隔離し、ユーザには届きません。	迷惑メールやウィルスであっても判定できなければユーザの下に届けられ、ウィルスバスターに委ねられます。
	利用者が受信するとき（ウィルスバスター）	サーバ上で自動的に駆除され、利用者には届きません。	サーバ上で自動的に隔離され利用者には届きません。