http://www.edu.pref.kagoshima.jp/ （通巻第1626号）

指導資料

鹿児島県総合教育センター

情報教育　第115号

―小，中，高，特別支援学校対象―

平成21年5月発行

学校におけるコンピュータウィルス対策

個人情報の保護に関する法律や条例等が施行され，学校における情報セキュリティへの取組が重要視されている。

一方コンピュータの利用範囲の拡大とともに，コンピュータに対する脅威も変化し続け，コンピュータウィルス（以下ウィルスという。）の感染による個人情報の流出などが問題となっている。

そこで本稿では，学校におけるウィルス対策について具体的に述べる。

1　最近のウィルス感染の傾向

ウィルスの感染経路が多様化し，外部記憶媒体（ＵＳＢメモリ等）を介して感染するウィルス（W32/Autorun）が増加（**図１**）するなど，注意すべき対象が増えている。

最近のウィルス感染の傾向を述べる。

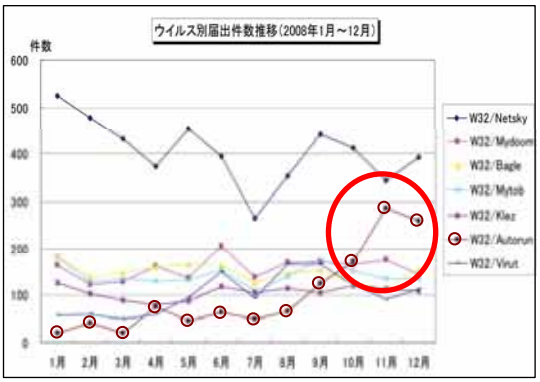

図１　ウィルス別届出件数の推移
（独立行政法人情報処理推進機構（IPA）「2008年のコンピュータウィルス届出状況」から）

(1)　ＵＳＢメモリ等を介した感染

ウィルスに感染したコンピュータに接続したＵＳＢメモリ等が感染し，それを別なコンピュータに接続することでウィルス感染が広がる事例が増えている。

本県の県立学校においても，ＵＳＢメモリ等を介したウィルス感染を防ぐことが課題となっている（**図２**）。

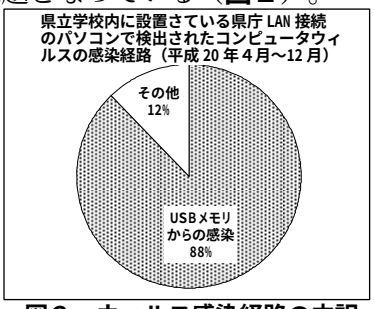

図２　ウィルス感染経路の内訳
（県教育庁高校教育課提供データから）

(2)　ＰＤＦや文書ファイルによる感染

これまでは，電子メールの添付ファイルの中にある実行ファイルからの感染が問題となってきたが，ＰＤＦや文書ファイルなどのデータファイルにウィルスが埋め込まれ，それを閲覧するソフトの脆弱性を悪用して感染が広がる事例もある。

(3)　Webサイトの閲覧による感染

Webサイトにウィルス感染の仕掛けが埋め込まれ，閲覧しただけで感染する。

有名な企業や組織のWebサイトが改ざんされ，利用者が感染した事例もある。

2　ウィルス感染による被害

ウィルスに感染すると，コンピュータの動作が不安定になったり，ファイルが破壊されたりする。また，使用者が知らないうちに，保存されているアドレス帳の宛先にウィルスが感染した添付ファイルを送信したり，他のコンピュータに不正アクセスを行ったりするなどの場合もある。

感染が拡大すると，完全に駆除するまでに膨大な時間や費用がかかるだけでなく，重要なデータがなくなったり，個人情報が流出したりするなど，大きな損害を受けることもある。

3　ウィルス感染を防ぐための対策

ウィルス感染を防止するためには，以下に述べる対策を，校務で利用するすべてのコンピュータに対して行わなければならない。１台でも未対策のものがあれば，そこから感染が広がることになる。

(1)　基本的な対策

ア　ウィルス対策ソフトの活用

ウィルス対策ソフトをインストールし，常時ウィルスを監視する機能を有効にする。ウィルス対策ソフトがウィルスを検出するためには，ウィルス定義ファイルが必要であり，新種のウィルスに対応するために常に最新の状態に更新しなければならない。

ウィルス対策ソフトの多くは有効期限が定められており，期限を過ぎるとウィルス定義ファイルを更新できなくなるので注意が必要である。

イ　脆弱性の解消

基本ソフト(ＯＳ)やアプリケーションソフトには脆弱性が存在し，それを利用してウィルス感染が広がる。

脆弱性を解消するためには，これらのソフトを最新版に更新しなければならない。

(2)　新しいウィルスへの対策

ア　不審なファイルの取扱いについて

不明な送信者から届いた電子メールの添付ファイルは開かない。また，信頼できないWebサイトの閲覧やファイルのダウンロードはしない。

イ　セキュリティの警告について

Windows XPやWindows Vistaには，アプリケーションを実行しようとしたときに「セキュリティの警告」をする機能がある。警告が出たときは自分の意図した作業かどうかを確認し，判断できないときには実行しない。

(3)　ＵＳＢメモリ等の使用について

ＵＳＢメモリ等の外部記憶媒体を介したウィルス感染に遭わないために次のことに注意する。

ア　ＵＳＢメモリ等を接続したときの自動実行を停止する。

コンピュータのShiftキーを押しながらＵＳＢメモリ等を接続すると，自動実行されない。

イ　ファイルを開く前にウィルス検査を行う。

ウ　ＵＳＢメモリ等を信頼できないコンピュータに接続しない。

エ　コンピュータに信頼できないＵＳＢメモリ等を接続しない。

○　**ＵＳＢメモリ等をウィルス検査する方法**（ウィルスバスターコーポレートエディションの例）

①　Shift キーを押しながらＵＳＢメモリ等をコンピュータに接続する。

②　画面右下のウィルスバスターCorp.のアイコンをマウスで右クリックし，「ウィルスバスター Corp.メイン」を選択する（**図３**）。

図３　ウィルスバスターCorp.メイン画面の表示方法

③　メイン画面でＵＳＢメモリ等（**図４**のリムーバブルディスク）を選択し，「検索」ボタンをクリックすると「ウィルス検索中」の画面が表示される。

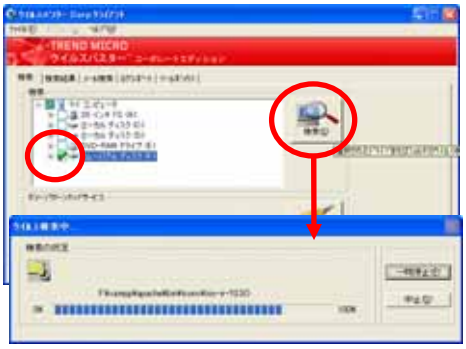

図４　ウィルスバスターCorp.によるウィルス検索画面

④　検査が完了してウィルスが検出されなければ次の画面が出る（**図５**）。

ウィルスが検出された場合はすぐにネットワークから切り離し，学校長及び情報セキュリティ管理担当者に報告する。

図５　検索終了後の画面

(4)　利用規定の策定状況及び利用者への情報提供

当教育センターが平成 19 年 11 月に実施した情報教育に関する実態調査によると，県内各学校における情報セキュリティポリシーの策定状況は次のとおりである（**図６**）。

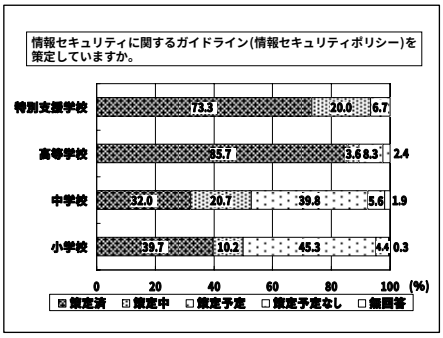

図６　県内公立学校の情報セキュリティポリシー策定状況

各学校は情報セキュリティポリシーの中でウィルス対策に関する項目を定め，全職員に周知するとともに，定期的に情報提供を行い，危機意識を高めることも必要である。

県立鹿児島南高等学校では次のような資料を作成し，全職員にウィルス対策を徹底している（**図７**）。

図７　ウィルス対策に関する情報提供の例（県立鹿児島南高等学校）

※　図７をクリックすると拡大表示されます。

4　ウィルス感染した場合の学校としての対応例

ウィルスは次々と新種や亜種（既存のウィルスをベースにした類似のもの）が発生しているので，これまで述べたような対策を取っているにもかかわらず，感染することがある。

万一感染した場合の対応例を以下に示す。

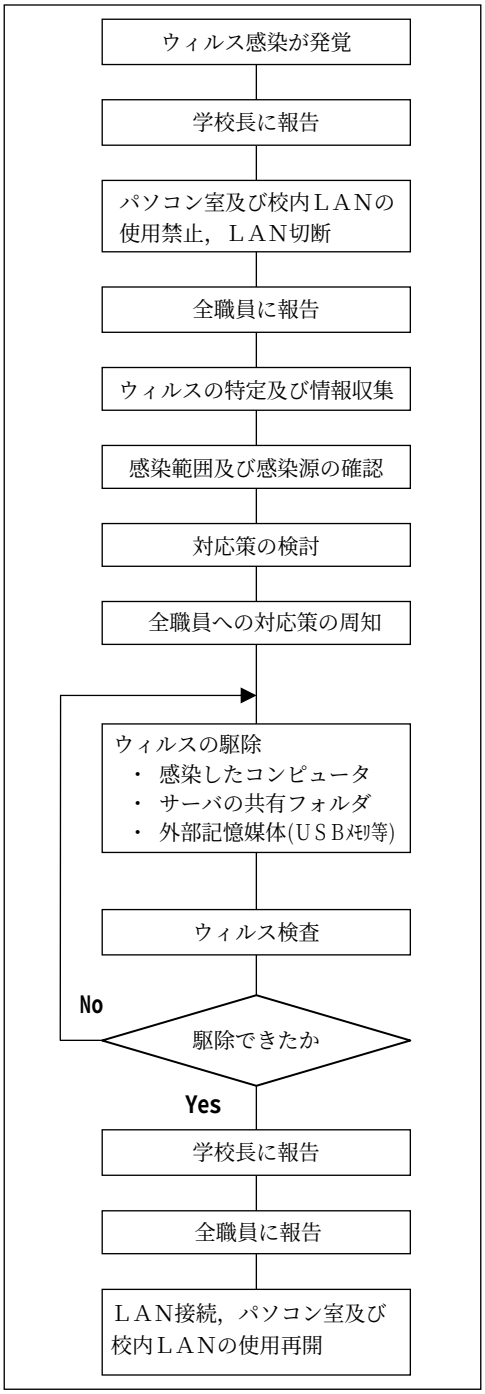

図８　ウィルス感染時の対応例

5　ウィルス及び情報セキュリティに関するWebサイトの活用

ウィルス対策や情報セキュリティについての対策や，最新情報を提供しているWebサイトの一部を紹介する。

○　総務省「国民のための情報セキュリティサイト」
http://www.soumu.go.jp/joho_tsusin/security/index.htm
○　独立行政法人情報処理推進機構「IPAセキュリティセンター」
http://www.ipa.go.jp/security/index.html
○　NPO日本ネットワークセキュリティ協会
http://www.jnsa.org/
○　マイクロソフト「セキュリティ ホーム」
http://www.microsoft.com/japan/protect/default.mspx

ＵＳＢメモリ等は大容量化と低価格化が進み，手軽に持ち運べる外部記憶媒体として普及しているが，その利用の際はウィルス感染に注意するだけでなく，学校の情報資産の管理等についても考慮する必要がある。情報セキュリティや個人情報保護に関することについては指導資料（通巻第1523・1603号）で述べているので併せて参考にしていただきたい。

【参考文献】

○「校内ネットワーク活用ガイドブック2005」
平成17年12月
社団法人日本教育工学振興会（JAPET）
○「ウィルス対策のしおり」平成20年５月
独立行政法人情報処理推進機構（IPA）

（情報教育研修課）