コンピュータウィルス等情報通知抜粋

平成１２年９月以来、しばしば校内でコンピュータウィルスに被害が発生するようになり、平成１３年度には電子メールの添付ファイルの形でウィルスが頻繁に届くようになった。平成１４年度からはセンターのサーバでウイルスを駆除できるように対策をとったが、ウイルスの脅威はなくなってはいない。本センターでは直接駆除にあたるほか、対策のための情報を電子メールで配布している。下記にそれらの抜粋を再掲する。

平成１４年５月１日

各　　位

情報処理センター長　長嶋　豊

コンピュータウィルス情報(Klez)

下記の新種のウィルスが急激に全国に広がっています。感染の広がりは Sircam, Nimda を凌ぐ勢いで、破壊力も強く危険です。
InternetExplorer のバージョンが低い(5.01-SP1・5.5-SP1 以下）と、 Outlook または Outlook Express で受信した場合に、リスト上のメッセージ見出しをクリック（シングル）しただけで添付ファイル（ウィルス）が実行されてしまいますので、次にあげる対策等をお勧めします。

対　策　等

１．Outlook または Outlook Express のユーザは InternetExplorer のバージョンを確認し、低ければバージョンアップをしてください。（下記ＵＲＬへアクセスしてファイルを取得できます）
http://www.microsoft.com/japan/ie/
このページの右上に「ダウンロード一覧」なる欄がありますので、ここから
InternetExplorer6
InternetExplorer5.5ServicePack2
InternetExplorer5.01ServicePack2
のいずれかを選択（クリック）し、更に「今すぐダウンロードする 」をクリックしてください。

２．市販のワクチンプログラムをインストールして最新のウィルスデータを取得していればほとんどのウィルスに有効ですので、是非とも購入をお勧めします。（約 5000 円）
例：　シマンテック社　ノートン　アンチウィルス 2002
　　ソースネクスト社　　ウィルススキャン　オンライン
ワクチンプログラムの有効性
・メールの受信時に即時に警告と駆除ができる
・ウィルスのスキャン（感染チェック）が自動的
・ウィルス定義データを自動更新

３．このウィルスに関する詳細な情報は
下記ＵＲＬをご参照ください。ここから更にワクチンメーカ等へのリンクがあります。
http://www.ipa.go.jp/security/topics/newvirus/klez.html

平成１４年7月１７日

各　　位

情報処理センター長　長嶋　豊

コンピュータウィルス対策のお願い

一昨日は最新のウィルス「Frethem.K」付きの電子メールが校内で多数受信されるという事態になりました。本校の電子メール集配サーバには既にウィルス対策用のプログラム（ワクチン）がインストールされているにもかかわらず、今回のケースではウィルスがあまりにも新しかったために、ウィルスの侵入を防ぐことができませんでした。ウィルスの拡散が速く、ワクチンメーカの対応を凌いでいたからです（現在は対応できています)。

同様のケースは今後も発生する可能性がありますので、ワクチンによる対策以外に下記の対策を講じておくことが必要です。最近のウィルスは、マイクロソフト社の通信ソフトのセキュリティホールを利用して電子メールの添付ファイルを自動実行させる手口を使っているからです。故に、電子メールの送受信ソフトとして Outlook Express,Outlook 以外のものを使う方が安全とも言えます。

対　　策

１．OutlookExpress と Outlook でメールのプレビューをさせないための処置
プレビューさせるとウィルスが自動実行されてしまうからです。「２.」に示すセキュリティーホールがある場合にこの処置が必要です。

Outlookexpress の場合
下記ＵＲＬに処置方法の説明があります。
http://www.trendmicro.co.jp/virusinfo/basic/winsecurity/winsec9.asp

Outlook の場合
メニューバーの「表示(V)」－「プレビューウィンドウ」と指定することにより、表示を交互に切り替えることができます。

２．InternetExplorer のセキュリティホールの確認と処置（バージョンの確認とバージョンアップ）
これで「１.」に述べた「プレビューさせるとウィルスが自動実行されてしまう」ことを防ぐことができます。

下記ＵＲＬに確認・処置方法の説明があります。
http://www.trendmicro.co.jp/virusinfo/basic/winsecurity/winsec8.asp

なお、上記「１．２.」の方法が分からない場合には本センターからお手伝いしますので、どうぞご遠慮なくご連絡ください。

平成１５年8月１９日

各　　位

情報処理センター担当技官　大渕　寛

コンピュータウィルス「エムエスブラスト」に対する緊急対策について

センター長が出張で不在のため、担当者から緊急にお知らせさせていただきます。

「エムエスブラスト」と呼ばれるコンピュータウイルスの感染が世界中に急激に広がっていることが報道

されています。身近では、すでに長崎大学で学生所有のパソコン１台から一気に感染が広がり、深刻な状況となっているそうです。長崎大学でも本校でも、外部とのインターネット通信に関してはファイヤーウォールを備えて、更にウィルスファイルの通過をチェックして駆除しておりますが、一旦校内のパソコンに感染した後はメール通信以外では無防備と言わざるを得ません。特に今回のものは LAN を介した感染力が非常に強いと言われています。また主な感染経路がメールではないことも特徴的です。

本校の場合の感染経路として最も心配されるものは次のとおりです。

１．校外で感染したノート型パソコンなどが校内に持ち込まれることによる感染
２．感染ファイルを持つ CD-ROM やフロッピーディスク等のメディアによる感染

したがって、最終的には個々のパソコンへのパッチあてやウィルス対策ソフトのインストールが必要となりますが、事態への対処が急を要しておりますので、次のとおり緊急対策を実施します。

緊　急　対　策
１．次にあげる例に該当がありましたら、ウィルス感染の有無をすぐに検査する必要がありますので、情報処理センター（内線２７１）までご連絡ください。
これは職員、学生を問わず必要な対策ですので、学生に関して各クラス担任や研究監督の先生から学生にお伝え下さい。

(1) 校外で使用したことがあるノートパソコンなどを校内で使用する場合。
(2) 校外で使用したことがある CD-ROM やフロッピーディスク等のメディアを校内で使用する場合。
(3) 特に学生がパソコンや記録メディアを新たに校内に持ち込むのを職員が気づいたときには、感染チェックを済ませたかどうかを確認してください。

ご連絡をいただけば速やかに感染の有無を調査いたします。感染のチェックは、ウィルス対策ソフトメーカが公開しているエムエスブラスト専用の駆除ツールを使って行います。既に方法をご存知の方は早めにご自身で実行願います。

平成１５年８月２１日

各　　位

情報処理センター長　長嶋　豊

コンピュータウイルス「エムエスブラスト」に対する緊急対策について（その２）

標記ウイルス対策につきましては、８月１９日付けの同名のメール通知でご案内したとおりですが、具体的な対策としては校外から持ち込まれた個々のパソコンやデータ（ＣＤ，フロッピーディスク、ＭＯなど）に対する処置が急務と考えられます。そこで、下記のとおり緊急対策の実施を願いいたします。

１．利用者各自での対策が可能な場合

・ＯＳ(Windows2000,XP,NT4)に対する修正パッチあて
各ＯＳごとに２種類(MS03-026,MS03-007)ありますので、下記のＵＲＬにアクセスして取得してください。
MS03-026:
http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS03-026ov.asp

MS03-007:
http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/MS03-007ov.asp

・ウイルス駆除ツールによる検査と駆除（ＯＳとデータに対するもの）下記のＵＲＬから取得できます。
http://www.symantec.com/region/jp/sarcj/data/w/w32.blaster.worm.removal.tool.html

２．本センターからの支援の場合
上記作業に要するツール（ＣＤ）を準備しておりますので、ご連絡ください。

長崎大学の例によりますと、僅かに１台の持ち込まれたパソコンが火種となり、学内全体に被害が拡大しておりますので、緊急の対策をお願いします。

３．当該ウイルスの各種呼び名について
当該ウイルスの呼び名は複数あり、以下のとおりです。
W32.Blaster.Worm,
W32.Blast.Worm
W32/Lovsan.worm
Lovsan
エムエスブラスター、
エムエスブラスト、
ラブサン等

平成１５年９月１２日

各　　位

情報処理センター長　長嶋　豊

MS-Windows の重大な脆弱性とその修正に関する情報

新手のコンピュータウイルス「エムエス・ブラスト」の出現から、ＬＡＮに接続しているだけで感染する「ネットワークウイルス」と呼ばれる新しいタイプのウイルスの脅威が注目されています。

つい昨日もこの種の脅威が心配される MS-Windows　が持つ脆弱性（セキュリティホール）とその修正パッチが公開されました。

この脆弱性を狙った新たなウイルスなどが出現する恐れが十分に予想されますので、該当するＯＳを使っている場合にはすぐに修正をお願いいたします。

該当するＯＳは下記のとおりです。
Microsoft Windows NTWorkstation4.0
Microsoft Windows NTServer4.0
Microsoft Windows NTServer4.0,TerminalServerEdition
Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows Server 2003

修正方法

１．「Windows Update」を実行する。

２．下記ＵＲＬにアクセスすることにより詳しい情報確認と修正パッチのダウンローができます。

「MS03-039: RPCSS サービスのバッファ オーバーランによりコードが実行される（824146)」に関する要約情報

http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/bulletin/ms03-039ov.asp

セキュリティホールを放置せず、本校「セキュリティポリシー」の遵守にご協力ください。

Windows の修正方法が分からない、ダウンロードがうまくいかないなどの場合には、本センターから作業の支援をしますので、ご連絡ください。