

コンピュータウイ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イ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イルスが頻繁に届くようになりました。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ます。下記にその抜粋の再掲します。

平成13年7月25日

各 位

情報処理センター長 武富 敬

コンピュータウイルス情報（サーカム）

危険度の高い新種コンピュータウイルス{W32/Sircam（サーカム）}が出現しておりますので、ご注意ください。以下の1.にあるような電子メールを受け取ったら、絶対に添付ファイルを開かずに捨ててください。

1. 感染を避けるには
電子メールの添付ファイルをうかつに開かないようにしてください。このウイルスを含むメールには次のような特徴があります。
メール本文の1行目
Hi!Howareyou? または Holacomoestas? (スペイン語)
メール本文の最終行
Seeyoulater.Thanks. または Nos vemospronto.
gracias. (スペイン語)
2. 感染していたら
LAN接続を切り離し、パソコンを停止して、本センターにご連絡ください。このウイルスはメールだけでなく、LAN上での共有ドライブに対して自動的に感染する恐れもありますので、この事にも注意してください。
3. 感染の有無の確認
次にあげる点に該当する場合は感染している。
 1. sirc32.exe, scam32.exe, sircam.sys, scmx32.exe
のいずれかのファイルがある。
 2. c:\¥autoexec.bat の内容に @win¥recycled¥sirc32.exe
なる文字列がある。
4. 感染後の主な症状
 - ・ 自動的にそのウイルスを含むファイルを添付したメールを勝手に送信する。
 - ・ ファイルやフォルダが消去される。
 - ・ ハードディスクの残りを不要なファイルが占有する。
 - ・ OSやアプリケーションの動きが鈍くなる。
 - ・ 10月16日にCドライブのすべてのファイルとフォルダが削除される可能性がある。
5. このウイルスに関する情報を見るための URL
<http://www.ipa.go.jp/security/topics/sircam.html>
<http://www.symantec.com/region/jp/sarcj/data/w/w32.sircam.worm@mm.html>

平成 13 年 9 月 27 日

各 位

情報処理センター長 武富 敬

コンピュータウイルス情報（ニムダ）

すでに 9 月 20 日（木）に校内放送でお知らせしましたが、危険度の高い新種コンピュータウイルス { W32/Nimda（ニムダ）, W32.Nimda.A@mm, PE_NIMDA.A などともよばれる } が出現し、全世界で急速に被害が広がっています。電子メールの添付ファイルからだけでなく、ホームページ閲覧時にダウンロードされてしまう被害が多発しており、感染力が極めて高いもので、校内に感染した場合には深刻な混乱に陥る危険があります。最大の注意を払ってください。

1. 被害を被るコンピュータ

マイクロソフト社の Internet Explorer と Outlook/Outlook Express を使用している Windows パーソナルコンピュータおよび、マイクロソフト社の IIS バージョン 4、またはバージョン 5 を使用している web サーバー

2. 感染経路等

(1) 電子メールの添付ファイルから

readme.exe なるファイル名の添付ファイルを実行することにより感染する。特に、メーラとして Outlook または Outlook Express を使っている場合には、デフォルト設定のままだと、リスト上でそのメールを選んだだけで自動的に添付ファイルが実行されてしまう。

(2) 被害を受けたサーバ上のホームページから

既に全世界の多数のサーバに感染していると予想され、そのホームページにアクセスすると自動的にウイルスファイルをダウンロードしてしまう。あるいは、ダウンロードを促される。

(3) 被害を受けたパソコンとのディスク共有から

同じ LAN 上のパソコンに感染していた場合、そのパソコンが共有している他のパソコンのディスクにウイルスファイルを書き込む。

3. 症状

大量メール送信、ファイル改ざん、パフォーマンス低下、不正アクセスの補助等

4. 感染の有無の調査と予防策

感染予防の具体的な手引きとして大変分かりやすいホームページがありますので、これを参考にしてください。なお、このページの「Step 1 自分のパソコンが感染していないかチェックしましょう」ではオンラインスキャンという方法を使いますが、これにはブラウザとして Internet Explorer を使ってください。他のブラウザではプログラムがうまく動作しません。

ホームユーザー向け セキュリティ対策 早わかりガイド Nimda

コンピュータウイルスに関する情報

<http://www.microsoft.com/japan/enable/products/security/nimda.asp>

他にも感染の有無の調査と駆除が同時にできる Nimda 対策専用の駆除ツールがあります。下記 URL にアクセスして取得できます。

シマンテック社 W32.Nimda.A@mm 駆除ツール (Nimda 専用 検索と駆除)

<http://www.symantec.co.jp/region/jp/sarcj/data/w/w32.nimda.a%40mm.removal.tool.html>

5. このウイルスに関する詳しい情報を見るには

下記 URL にアクセスしてご覧ください。

情報処理振興事業協会 (IPA)

<http://www.ipa.go.jp/security/topics/newvirus/nimda.html>

マイクロソフト社

<http://www.microsoft.com/japan/technet/security/nimdaalrt.asp>

平成13年9月28日

各位

情報処理センター長 武富 敬

コンピュータウイルス情報(ニムダ)(その2)

先にお知らせしました「コンピュータウイルス情報(ニムダ)」の補足をいたします。

コンピュータウイルスに感染していると確認された、もしくは疑いがある場合には、すぐにLAN接続のケーブルを抜き取って本センターまでご連絡ください。ウイルスが Nimda や Sircam (サーカム) の場合には二次感染のための活動を自動的にしているはずだからです。

(1) Internet Explorer のバージョンアップ

感染予防のための Internet Explorer のバージョンアップは是非とも速やかに実行してください。これによりウイルスファイルの自動ダウンロードや自動実行(メール本文を見ただけで感染する)を防ぐことができます。Internet Explorer を利用していない場合でも Nimda はこの機能を使って感染するので、バージョンアップが必要です。

(2) Outlook Express の設定変更

上記バージョンアップをしていなくて Outlook Express を使用している場合には、少なくとも次のとおり設定を変更してメールからの自動的な感染を防いでください。

メニューバーの「ツール」の「オプション」を選択して、現れたボックスの中の「読み取り」タブを選択して、「メッセージの読み取り」の項目の「プレビューウィンドウで表示するメッセージを自動的にダウンロードする」のチェックを消してください。

平成13年10月4日

各位

情報処理センター長 武富 敬

コンピュータウイルス情報(サーカム)その3(10月16日に注意)

先日お知らせしましたコンピュータウイルス W32/Sircam (サーカム) の感染がまた校内で発見されました。ところが、この感染したパソコンでは感染後の症状(多数メールの発信など)が見られませんでした。このことから、他にも感染していても発見されていないパソコンがあるという疑いがあります。実は、このウイルスは10月16日にCドライブの全てのファイルやフォルダを削除するという時限爆弾的なプログラムを持っていることが分かっています。このウイルスの感染経路はメールのみならずLAN端末間の直接的な感染もあるので、校内のすべてのパソコン(Windows系のみ)について不安があります。

そこで、できれば10月の15日(月)と16日に特にこのウイルスに関する検査を実行しておくことをおすすめします。

具体的には、下記URLで専用の駆除ツールを取得し、これを実行してください。検査と駆除ができます。

<http://www.symantec.com/region/jp/sarcj/data/w/w32.sircam.worm@mm.removal.tool.html>

ファイルサイズは 80KB 程度とごく小さく、使用方法もとても簡単です。

平成13年11月22日

各 位

情報処理センター長 武富 敬

コンピュータウイルス情報 (Aliz)

昨日(11月21日)本校教官宛に届いたメール多数がウイルス付きであったことが確認されました。名前は W32.Aliz.Worm です。

感染力が極めて高く、最近全国で急激に被害が広がっていますので、ご注意ください。

下記URLに情報がありません。

<http://www.symantec.co.jp/region/jp/sarcj/data/w/w32.aliz.worm.html>

<http://www.ipa.go.jp/security/topics/newvirus/aliz.html>

平成13年12月12日

各 位

情報処理センター長 武富 敬

コンピュータウイルス情報 (バッドトランス)

新種コンピュータウイルス { W32.Badtrans.B@mm (バッドトランス) } が出現し、全世界で急速に被害が広がっています。既に本校職員宛にこのウイルス付きメールが届いており、多数の被害が発生しています。

最近の多くのウイルスと同じく、Internet Explorer のバージョンアップを怠っている
と、Outlook/OutlookExpress でのメールプレビュー時に自動的に添付ファイルが実行されて感染します。

InternetExplorer5.01,5.01SP1 または、
InternetExplorer5.5,5.5SP1 を使っている場合にはすぐに SP2 (サービスパック2) または ver.6 にバージョンアップしておいてください。

また、メールの添付ファイルをうかつに実行しないという常識を忘れて感染し、被害を広げる
(多数メール自動発信) 例が多いので、普段の通信相手であっても十分に警戒するようお願いします。

このウイルスに関する詳しい情報を見るには
下記 URL にアクセスしてご覧ください。

情報処理振興事業協会(IPA)

<http://www.ipa.go.jp/security/topics/newvirus/badtrans-b.html>

シマンテック社

<http://www.symantec.co.jp/region/jp/sarcj/data/w/w32.badtrans.b%40mm.html>

平成13年12月19日

各 位

情報処理センター長 武富 敬

ウイルス被害急増 年末緊急警報

情報処理振興事業協会セキュリティセンター(IPA/ISEC)によると、12月に入ってからのコンピュータウイルス被害の届出件数が急増しており、月間の件数では過去最悪になる見込みとのこと
です。感染力の強い新種ウイルスの登場に加え、クリスマスと年賀のグリーティングメールが飛び交うこの季節は、受信側の警戒心が緩んでいるからだそうです。

IPA による警報通知文が下記 URL にありますので、是非ともご覧になることをおすすめします。
<http://www.ipa.go.jp/security/topics/alert131218.html>

平成 13 年 12 月 21 日

各 位

情報処理センター長 武富 敬

Internet Explorer 修正パッチインストールのおすすめ

先日からメール添付ファイルのウィルスの自動実行感染を防止するために Internet Explorer のバージョンを 5.01SP2 か 5.5SP2 または 6 にバージョンアップすべきであることをお知らせしたところですが、ここで新たに同 5.5SP2 と 6 についての重大なセキュリティホールが発見されました。この問題を放置しておくとならぬ新たなウィルスや罠が仕掛けられたホームページにアクセスしたときに被害を受ける恐れがあります。

そこで、このセキュリティホールを塞ぐために下記の URL にアクセスして修正用プログラムをダウンロードして修正を施すことをおすすめします。

http://www.microsoft.com/japan/technet/security/current.asp?url=/japan/technet/security/frame_prekb.asp?sec_cd=MS01-058

上記 URL のページ内の説明を読まれたうえで、「修正プログラム : この問題に対する日本語版修正プログラムは、次のサイトからダウンロードできます。」と書かれた行の次の行をクリックすればダウンロードのページにアクセスできます。修正プログラムは 5.5SP2 用と 6 用がありますので、選択してください。

平成 14 年 1 月 29 日

各 位

情報処理センター長 武富 敬

コンピュータウイルス情報 (マイパーティ)

下記の新種のウイルス (メールワーム型) が急激に全国に広がっています。件名 (subject 名) と本文が、以下の特徴のとおりですのですぐに分かりますので、絶対に添付ファイルを開かずすく消去してください。

1. 特徴

電子メールの添付ファイルとして届き、これを実行すると動作する。

メール件名 : new photos frommyparty!

メール本文 :

Hello!

My party... It was absolutely amazing!

I have attached my webpage with new photos!

If you can please make color prints of my photos. Thanks!

添付ファイル名 : www.myparty.yahoo.com

2. ウィルス名称

W32/Myparty (情報処理振興事業協会セキュリティセンターによる)

W32.Myparty@mm (シマンテック社による)

WORM_MYPARTY.A (トレンドマイクロ社による)

3. 詳しい情報がある URL

<http://www.ipa.go.jp/security/topics/newvirus/myparty.html>

<http://www.nai.com/japan/virusinfo/virM.asp?v=W32/Myparty@MM>

<http://www.symantec.com/region/jp/sarcj/data/w/w32.myparty%40mm.html>

平成14年2月19日

各 位

情報処理センター長 武富 敬

InternetExplorer 修正パッチインストールのおすすめ

先日の情報処理センター運営委員会でも話題にのぼりましたので、標記の件につき、通知を配布することにいたしました。

最近のコンピュータウイルスやハッキングは、マイクロソフト社のインターネット利用ツールのセキュリティホールを狙うものが最も多く、被害が頻発しています。パソコンのセキュリティを確保するためには InternetExplorer に常に最新の修正プログラムをあてておくことが必要です。これなしでは Outlook と OutlookExpress を安心して使うことができません。この最新の修正プログラムが Web 上で公開されていますので、下記 URL にアクセスしてダウンロードすることをおすすめします。

説明

http://www.microsoft.com/japan/technet/security/current.asp?url=/japan/technet/security/frame_prekb.asp?sec_cd=MS02-005

ダウンロード

下記ページの SelectLanguage: のメニューで Japanese を選んで「Go」ボタンをクリックしてください。その後 Internet Explorer のバージョンに合うものを選んでください。

<http://www.microsoft.com/windows/ie/downloads/critical/q316059/default.asp>

この修正プログラムの正式な名称は「2002年2月11日 InternetExplorer の累積的な修正プログラム (MS02-005)」です。

InternetExplorer のバージョンはウィンドウ上端メニューの「ヘルプ」から「バージョン情報」を選択して確認してください。



