SAAJ
第 88 回月例研究会
講演記録

テーマ：「今日の企業情報システムにおけるウイルス対策監査」

講師：ＩＰＡ　情報処理振興事業協会
　　セキュリティセンター　　宮川　寧夫氏
日時：2002 年 6 月 26 日（水）18:30～20:30
場所：東京労働スクエア
　　（ワーカーズサポートセンター）701 号室

はじめに

標記の月例会において、宮川氏は最近のコンピュータウイルスが大規模なエンタープライズネットワークシステムに与える影響の現状を認識し、対策のベストプラクティスが変化しているのではないかという。

講演概要は以下のとおり。

(ゴシック体はスライド内容の抜粋、明朝体は解説、補足を表す)

No.148　木村裕一

目次：

１．ウイルス基礎知識の確認

ウイルスの種類をプラットフォーム別に、ＰＣ（Windows, DOS), PC（Macintosh)、他のプラットフォーム上のウイルスに分けた上で、ＰＣ（Windows, DOS）に関するウイルスを説明された。

１．１　ウイルスの種類

①ブートセクタ感染型ウイルス
②(実行)ファイル感染型ウイルス
③マクロ・ウイルス(スクリプト・ウイルス)
④トロイの木馬
⑤メール機能を悪用して感染するウイルス
⑥ワーム

ここではこの中の⑤について抜き出して紹介する。

１．２　メール機能を悪用して感染するウイルス

種類	感染を拡げる動作
W32/Ska (Happy99)	メール送信時にウイルスを添付したメールを同じ宛先に送信　便乗型
W32/MTX	
W32/ExploreZip	メールを受信時に送信者へウイルスを添付したメールを送信　返信型
VBS/LOVELETTER	登録アドレスにウイルスを添付したメールを送信　一斉送信型
W32/Navidad	受信トレイにあるメールを再利用して、ウイルスを添付したメールを送信
W32/Hybris	送受信メール、Web サイト等から取得したアドレス宛にウイルスを添付したメールを送信
W32/Sircam	登録アドレス、Web サイトから取得したアドレス宛にウイルスを添付したメールを送信

便乗型：正規のメールと思わせて開かせる。
返信型：勝手にメールを送信する。
一斉送信型：アドレス帳を引く MAPI 機能を持つ。
全般にこれらのウイルスは解析も面倒になっている。

１．３　具体例の紹介

当日のスライドからいくつかを紹介する。

（１）W32/Ska（俗称Happy99）(1999年2月届出)

添付ファイル名：「Happy99.exe」

添付ファイルを実行すると花火の画像

Skaに感染したパソコンで、メールを送信すると、ウイルスが、同じ宛先にもう１通、Happy.exeを添付した同じ件名で本文が空白のメールを送信

受信側：

同じ人からほぼ同時に２通のメールが届くため、うっかり添付ファイルを開きやすい

解説：「エンドユーザにセキュリティのための良い行動を求めることは難しい」

（２）VBS/LOVELETTER（2000年5月届出）

添付ファイル名：「LOVE-LETTER-FOR-YOU.vbs」

設定によっては、.vbs が表示されず、テキストファイルのように見える。（二重拡張子）

アドレス帳の登録アドレス全てにウイルスを添付したメールを送信

⇒メールサーバのシステムダウン

（３）W32/MTX（2000年9月届出)

メール送信時、同じ宛先にもう１通、件名、本文が空白で、ウイルスを添付したメールを送信

３１種類の異なる添付ファイル名を日替わりで使い分ける

（　3日）LOVE_LETTER_FOR_YOU.TXT.pif

(13 日)ALANIS_Screen_Saver.SCR

(30 日)zipped_files.EXE

感染すると初期化が必要で、被害は深刻

解説：最も届出数が多い。添付ファイル名称がころころ変わり、従来のように××に気をつけろという対策が通用しない。

（４）W32/Sircam（2001年7月届出)

ウイルスに感染した添付ファイルを実行すると、

・Ｏｕｔｌｏｏｋ及びＯｕｔｌｏｏｋ　Ｅｘｐｒｅｓｓの登録アドレス全て
・Webサイトに掲載されているアドレス
に対し、ウイルスファイルを添付したメールを送信する

メール件名：添付ファイルを用いて作成
メール本文：Ｈｉ！Ｈｏｗ　ａｒｅ　ｙｏｕ？
Ｉ ｓｅｎｄ　ｙｏｕ　ｔｈｉｓ　ｆｉｌｅ　ｉｎ　ｏｒｄｅｒ　ｔｏ　ｈａｖｅ　ｙｏｕｒ　ａｄｖｉｃｅ
Ｓｅｅ　ｙｏｕ　ｌａｔｅｒ．　Ｔｈａｎｋｓ
添付ファイル：「マイドキュメント」フォルダのドキュメントファイル等のファイルから取得

企業情報漏えいの危険性

解説：この添付ファイルは実在するファイルの複製にウイルスを感染させて作成するので、既存の企業情報が漏洩する点からクローズアップされた。添付ファイル名は元のファイルとほとんど同じ。

その他、Ｗ32/ExploreZip、Ｗ32/Hybris、Ｗ32/Mypartyの例を紹介された。

２．最新のウイルスの傾向

この半年ほどにおけるウイルスの傾向を、具体例により注意事項を交え解説された。

２．１　傾向

・メール機能悪用　＋　セキュリティ脆弱性攻撃

メール本文を見ただけでも感染
OutlookExpressではプレビューだけでも感染

対策：従来の対策　＋　修正プログラムの適用

・セキュリティホールを攻撃・感染

W32/Nimda	サーバーを攻撃
W32/Aliz	ウイルスメールを送信
W32/Badtrans（亜種）	パスワード等の漏洩
W32/Klez（亜種）	ウイルスメール差出人を詐称

解説：セキュリティホールなどの脆弱性を攻撃するのがこの半年ほどの傾向である。エンドユーザに下線部の対応を求めるのは大変難しい。また、宮川氏の所に１日に来るメール 400 通のうち、１割ほどはウイルスに汚染されているとの事である。

２．２　具体例

（１）W32/Nimda（２００１年９月届出）

既知の
・ＩＩＳ（Ｉｎｔｅｒｎｅｔ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｒｖｉｃｅ）
・ＩＥ（Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ）
の脆弱性を悪用

標的

Ｗｅｂサーバ：ＩＩＳバージョン4、またはバージョン５

クライアント：Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ５.、５．５

ホームページを見ただけでも感染 メール本文を見ただけでも感染 サムネイル表示しただけでも感染

（２）W32/Aliz

既知のＩＥ（Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ）の脆弱性を悪用

ＯｕｔｌｏｏｋＥｘｐｒｅｓｓのアドレス帳に登録されている全てのアドレス宛に

ウイルスを添付したメールを送信する。

標的　・Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ５.、５．５

・Ｏｕｔｌｏｏｋ，ＯｕｔｌｏｏｋＥｘｐｒｅｓｓ

メール本文を見ただけでも感染 ＯｕｔｌｏｏｋＥｘｐｒｅｓｓではプレビューだけでも感染

（３）W32/Klez(亜種)（2001年11月届出）

既知のＩｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒのセキュリティ脆弱性を攻撃。

ウイルスメールの送信先アドレスを、アドレス帳や

感染したパソコン内のhtmlファイル等からも取得。

パソコン内から収集したメールアドレスを送信者（Ｆｒｏｍ）欄に

記述してウイルスメールを送信する。

標的　・Ｉｎｔｅｒｎｅｔ　Ｅｘｐｌｏｒｅｒ５.、５．５

・Ｏｕｔｌｏｏｋ，ＯｕｔｌｏｏｋＥｘｐｒｅｓｓ

メール本文を見ただけでも感染 メールアドレスを詐称 データの漏洩と破壊
本当の感染者に感染している旨の連絡がとれない 盗用されたアドレスにエラーや警告メールが届く

３．届出状況

３．１　ウイルスの届出状況

IPAへの届出ベースの数値（ＨＰで発表されているが、この届出数値が全てとは思わないという）を基に説明された。新種のウイルスの出現により1997年、1999年など届出件数が急増していること、メールで送信者を詐称するウイルスがありウイルスの感染を原因者に連絡することができず感染が止まらないウイルスがある等について解説された。

なお、感染する前に発見するケースが増えていて、対策のレベルが上がっていると言う。

３．２　届出ウイルス名称

2001年に届出された主なウイルスの名称を紹介。

件数の多い第１位はW32/Hybrisで4915件、第2位はW32/Badtransで3281件、第3位はW32/Sircamが3017件と続く。

３．３　届出ウイルスの種類別割合の年別推移

ここではその一部を示す。

（2000 年、2001 年、2002 年(1～3 月)の各割合）

メール機能悪用（60.2%、58.8%、29.9%）

セキュリティホール悪用（4.6%、26.1%、63%）

マクロウイルス（30.5%、11.6%、5.5%）

かなりはっきりした傾向が見られる。

３．４　届出感染経路

メールによる割合がどんどん増え、2002 年は 97.5%である。

４．ウイルス対策

４．１　パソコンユーザのためのウイルス対策 7 箇条

パソコンユーザのためのウイルス対策 7 箇条
1．最新のウイルス定義ファイルに更新しワクチンソフトを活用すること
2．メールの添付ファイルは、開く前にウイルス検査を行うこと
3．ダウンロードしたファイルは、使用する前にウイルス検査を行うこと
4．アプリケーションのセキュリティ機能を活用すること
5．セキュリティパッチをあてること
――――――――――（※ここまでが感染防止対策）
6．ウイルス感染の兆候を見逃さないこと
7．ウイルス感染被害からの復旧のためのデータのバックアップを行うこと

解説：このＩＰＡが発表しているウイルス対策７箇条を改訂するのは容易であるが、通産省告示であるコンピュータウイルス対策基準を改訂するのはすごく大変である。この７箇条の解説をされた。

５．ウイルス対策のベストプラクティスの変化

４項の対策の実施について、エンドユーザが良い対策をきちんと実行してくれるであろうか（むつかしい)。従って、もっとシステム管理者の働き、ネットワーク設計に期待したいといい、次の２つの論点を展開した。

（１）情報システム運用論点

①エンドユーザに(ウイルス対策 7 箇条などを)期待するのは困難になってきている前提での検討

・ウイルス・データ・ファイルの更新

便利な機能が提供されている

（自動通知、簡単なインストール）

頻繁である（更新しなくなる）

・修正プログラム適用

便利な機能が提供されている

（インストールは簡単か？？）

頻繁である（更新しなくなる）

ユーザ数も（多い）

（２）情報システム構築・調達論点

①マクロ機能は本当に必要か

（Excel…　Word　？？

②構築：Web アプリケーション

・ブラウザさえあれば…

・ブラウザ指定システム：Internet　Explorer

③機能追加

・インターネット境界でのウイルス対策
　複数層での検査が建前…唯一有効な検査か？？

・修正プログラムの一斉適用は可能か？
　Windowsネットワークドメインにログインするタイミングで
　修正プログラムをあてさせるスクリプトを登録しておく
　（グループポリシーで設定可能。再設定手続を要求される）

6．システム監査への期待

（1）指導性

①システム運用に対する問題指摘だけでは

・エンドユーザに多くを期待しても

・システム管理者もつらい

②システム構築・ソフトウェア調達への参画
　理想と現実の間で
　コスト

（2）改善・フィードバックの役割

①機能追加でできること

・エンドユーザに多くを期待しなくても一定の効果がある対策機能を追加するよう指導する

解説:エンタープライズネットワークシステムの構築段階から対策機能を埋め込むような技術が利用可能になってきている。企業の中の対策としてはエンドユーザ教育のみを強調するのは適切でない。システム監査ではベストプラクティスの変化に応じた視点での指導性も必要でないかと言う。なお、ホームユーザが増加しているので、エンドユーザ教育の重要性がさがることはない。

7．Q＆A

Q＆Aには参加者から

・ウイルスを使ってばら撒いた人が逮捕されないのか、

・悪に正義は勝てるか、

・ウイルス対策のコストはどのくらいが適切と言えるか、

・プロバイダでウイルスを防止することが有効でないか、

等の質問が相次ぎ、技術論、法律論、倫理問題、実践面の多岐に亘っての質疑応答が行われた。

最後に宮川氏はＩＰＡの独立行政法人化の計画があることに触れ、それに関連してエンタープライズネットワークセキュリティに関するアンケートを考えていること、それへの協力などを希望するなどの話があって盛況の内に月例研究会を終えた。

月例会の記録として、各支部にビデオテープと資料を配布しております。また、ビデオテープは事務局で貸し出しが出来ます（有料、資料付）。