G-32

コンピュータウイルス作成の容易性と検出について

水村　有里[1]
Yuri Mizumura

1　概要

本論文では、近年インターネットの普及によって被害がもたらされているコンピュータウイルスの基本特性について考察する。また、実際にプログラミングによってウイルスを作成し容易に作成されることを検証することで、ウイルスの構造について考察する。

2 コンピュータウイルスの概要

コンピュータウイルスとは、1984 年に Fred Cohen[1]が発表した『他のコンピュータプログラムに自分自身の複製を寄生させるために、他のプログラムを修正して感染する機能を持ったコンピュータプログラム』に由来する。

2.1 ウイルスの分類

2.1.1 狭義のウイルス

感染機能・発病機能・潜伏機能を持つウイルスは**狭義のウイルス**と呼ばれ、以下 3 つの型に分類される[2]。

●ファイル感染型：「.com」「.exe」などの拡張子を持つ「実行ファイル」に感染するウイルス

●システム領域型：記憶デバイスのシステム領域に感染するウイルス

●マクロ型：Word や Excel などのデータ・ファイルにマクロ機能を利用して感染するウイルス

2.2.2 トロイの木馬とワーム

「トロイの木馬」や「ワーム」とは、プログラム単体で動作するウイルスを指す。トロイの木馬は有益プログラムと装いユーザーによって知らぬ間にダウンロードされパソコン内部に侵入する。ワームは、ネットワークを介して感染するウイルスである。次に、ウイルス検出方法について簡潔に述べる。

3 ウイルス検出方法[3]

3.1 パターンマッチング方式

既知のウイルスを検出する方法で、新しいウイルスが発見されるとその内容を分析し、過去に登録されたパターンと同一であるかどうか調べ検出を行う。

3.2 チェックサム方式

各ファイルのチェックサムを事前に保存しておき、ウイルス検査を行う際に計算されたチェックサムとの値を比較する。

3.3 ヒューリスティック(heuristic)法

ウイルスらしき動作を行うプログラムに対して検査を行う。この方法は未知のウイルスについても発見が可能だが、誤認する可能性が高くなる。

3.4 インテグリティチェック法(integrity check)法

暗号技術を利用した「デジタル署名」を作成し、検証時にも同じ方法で作成した値とデジタル署名から復号した値とを比較し、安全性を検証することでウイルス感染の有無を調べる。

4 疑似簡易ウイルス作成

Word に付随する Visual Basic Editor を用いて疑似ウイルスを作成した。

4.1 ウイルスプログラム基本の形

[1] 日大理工・学部・数学

下記は Word ドキュメントファイル開封時にウイルスコードを書き込み、ウイルスに感染させるスクリプトプログラムの雛型である[4]。

『Application.DisplayStatusBar = False』
ステータスバーを表示しない。

『ActiveDocument.ReadOnlyRecommended = False』
ドキュメント表示の際に読み取り専用を推奨させる。

『 System.PrivateProfileString("",_"HKEY_CURRENT_USER＼Software＼Microsoft＼Office＼11＼Word＼Security", _"Level") = 1&』※
セキュリティレベルを確認し無効にする。

『ElseIf DocActive.Lines(1, 1) <> "'SAMPLE" Then DocActive.DeleteLines 1, DocActive.CountOfLines』
標準プレートの 1 行目が[SAMPLE]でなければ全ての行を削除。

『 DocActive.InsertLines1,DocTemplateLines(1,DocTemplete.CountOfLines)』
現在開かれているドキュメントに標準プレートの全てのマクロを書き込む。

『ActiveDocument.Save』
現在開かれているドキュメントを保存する。

4.2 表示の変換

以下は、一単語変えるだけで表示のされ方が変化してしまうスクリプトの一例であり、図 1 のようなダイアログに新たにキャンセルが加わり図 2 のように表示される：

『MsgBox "テスト", vbInformation, "タイトル" 』
テスト、タイトルを表示させる。(図 1)

『MsgBox "テスト", vbOKCancel, "タイトル"』

5 ウイルス検出

マクロ機能を持つソフトウェアを利用する際、マクロプログラムの実行を無効にすることにより有害プログラムの実行を防ぐことができる。また、セキュリティレベルを最高に設定することも一つの方法である[3]。4.1 のプログラムで示したように、※の行で強制的にセキュリティレベルが無効にされている。このプログラムコードを記録させ 3.1 のパターンマッチング法に活かす。このような動作を遂時発見することで、ウイルス検出につなげていく。

5 終わりに

本研究では、Visual Basic Editor を用いた疑似ウイルスプログラム作成を通して、コンピュータウイルスが容易に作成できてしまうことを確認した。また、本論文で示されたような雛型を元にプログラムされることについて述べ、どのようにウイルスが検出されるのかを考察した。今後は他のウイルス形態や検出方法についても考察する予定である。

6　参考文献

[1]Fred Cohen,"Computer Viruses - Theory and Experiments",1987

[2]御池　鮎樹, “マルイウエア情報化社会の破壊者,” 工学社,2009 年 9 月

[3]内田　勝也,高橋　正和, “有害プログラム―その分類・メカニズム・対策,” 共立出版,2004 年 7 月

[4]CORD BRACK, “コンピュータウイルス製造ハンドブック,” 三協企画印刷,2002 年 6 月

[5]http://office.microsoft.com/ja-jp/help/HA010007210.aspx

図 1　テスト 1

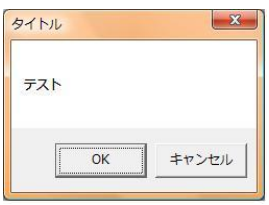

図 2　テスト 2