Computer Pest 検出システムの有効性の検証

Verification of the Validity of a Computer Pest Detection System

古屋 貴博 † 松田 勝敬 †† 永井 明 †††

Takahiro FURUYA, Masahiro MATSUDA, and Akira NAGAI

宇都宮大学総合情報処理センター ‡

Advanced Media Network Center, Utsunomiya University

概要

ウイルス／ワーム対策は一般的に行っているが，ウイルス対策ソフトでは検出できないウイルス／ワーム以外の不正プログラム被害が日本でも最近報告されており，対策が求められている．これらの不正プログラムはコンピュータペストなどと定義され，コンピュータペストを検出できるプログラムを教室系クライアント群の一部の端末に試験的に導入し，中規模な検証を行った．検証により検出されたコンピュータペスト，全ての教室系クライアント端末への導入方法の提案，問題点を報告する．

キーワード

センター運営，不正プログラム，コンピュータペスト，セキュリティ対策，利用者端末

1.はじめに

宇都宮大学総合情報処理センター（以後センター）では，以前からウイルス／ワームの検出・駆除に関して，積極的に対応してきた．不特定多数の利用者が使用することでウイルスが蔓延しやすい教室系クライアント群は，全ての端末でウイルス対策ソフトを導入し，利用者がログオンする時に最新パターンファイルのダウンロードを行いウイルス／ワームの監視を行うことで，ウイルスの被害を無くし，また教室系クライアント群から学内の他のクライアント端末や利用者の個人所有端末への 2 次感染による被害の拡大を防いできた．

しかし最近，ウイルス／ワーム以外の不正プログラムの被害が，世界的に報告されている．日本でもキー入力を記憶する「キーロガー」を利用し，パスワードを不正に入手することで，1600 万円を詐取される事件も発生している．「キーロガー」以外にも，端末内部の情報を勝手に盗み出す「スパイウェア」や広告等を勝手にブラウザなどに表示させる「アドウェア」，組み込んだ端末へ不正侵入し自由に操作できる「リモート管理ツール」などの被害も発生している[1].

そこでセンターでは「キーロガー」や「スパイウェア」「アドウェア」「リモート管理ツール」のセキュリティ対策として，これらの不正プログラムを検出できるシステムをメーカの協力を得て，教室系クライアント群の一部の端末に試験的に導入し，中規模な検証を行った．今回はこのシステムの有効な点や問題点，導入時の提案について述べる．

† furuya@cc.utsunomiya-u.ac.jp

†† mmatsuda@cc.utsunomiya-u.ac.jp

††† anagai@cc.utsunomiya-u.ac.jp

‡ 〒321-8585 栃木県宇都宮市陽東 7-1-2

Tel. 028-689-6340

2.コンピュータペスト

「キーロガー」「スパイウェア」「アドウェア」「リモート管理ツール」等のウイルス／ワーム以外の不正プログラムは「コンピュータペスト」などと定義されている[1].「コンピュータペスト」はウイルス／ワームのように自己増殖することは無い．しかし 2003 年 7 現在，ウイルス

図-1　ウイルス／ワームとコンピュータペストの関係

／ワームが約 63,000 種であるのに対し，コンピュータペストは約 72,000 種あるとされる．さらに 2002～2003 年にかけて 1.5 倍も増加しており，脅威となっている．コンピュータペストの主な例は以下のものである．

・キーロガー
　キー入力を記憶するツール．プログラマの作業履歴を残すために作られたプログラムだが，ID，パスワード，電子資産を盗むのに不正利用される．
・DDoS 用エージェント
　ターゲットシステムを同時に攻撃するツール．仕掛けられた側は被害者でもあり，加害者にもなりうる．
・スパイウェア／アドウェア
　端末内の情報を盗聴し，利用者の許諾なしに送信されてしまう．
・リモート管理ツール
　侵入者にコンピュータをリモートコントロールされ，さまざまな情報が漏洩してしまう．
・スニファ
　ネットワーク上に流れるメールの内容等の情報が漏洩してしまう．

　以上これらのコンピュータペストの侵入経路は主に次の三つである．
・外部より第三者によって組み込まれる
・電子メールの添付ファイルやウェブ・ブラウジング
・内部利用者によって組み込まれる

　また，コンピュータペストはインターネットのリンク集やネット通販，シェアウェアやハッキング本の付録等比較的簡単に入手可能であり，ウイルスのようにほとんどが海外から広まるのではなく，日本でも作られているらしい．

3.コンピュータペスト検出システム

　今回コンピュータペスト検出システムとして，株式会社アークンの協力により，「PestPatrol4.2 日本語版」[2]を使用させて頂いた．PestPatrol はコンピュータペストを検出・駆除・隔離することが可能であり，72,000 以上のコンピュータペストに対応し，既知コンピュータペストのデータベースを利用している．定義ファイルは週一回程更新されており，アップデート機能により定義ファイルである PPfile.dat，PPInfo.dat，Spyware.dat がダウンロードされ，これを用いてコンピュータペストの検出を行う．検出方法と機能の説明をする．

【検出方法】
　PPfile.dat にはコンピュータペストのファイルストリング情報である MD5 値(デジタル署名にも使用されている一般的なメッセージ要約関数)，PVT 値(Pest Verification Token，PestPatrol 独自のファイルストリング値)およびコンピュータペスト名情報が含まれており，これらの情報はファイルを対象としている．PestPatrol によるスキャンによりファイル毎に MD5 値&PVT 値が算出され，この値は PPfile.dat 内にある値と比較され，一致すればコンピュータペストとして検知される．
　Spyware.dat は違う方法でコンピュータペストを検出する．Spyware.dat には"場所"の情報が入っており，あるファイルがあるディレクトリに存在すれば，このファイル（コンピュータペスト）は検知される．またあるレジストリエントリ（コンピュータペスト）が存在すれば，このレジストリエントリは検知される．Spyware.dat にはスパイウェア，スパイウェアクッキー，アドウェア，ブラウザ・ヘルパー・オブジェクトと一部のキーロガーの情報とそのコンピュータペスト名が入っている．

【機能】
PestPatrol は以下の機能を有している．
・PestPatrol
　GUI ベースによる手動検査機能
・PPMemCheck
　コンピュータペストの活動を監視するメモリ常駐機能
・Cookie Patrol
　スパイウェアクッキー検知機能
・PPUpdate
　定義ファイル自動アップ機能
・PPCL
　コマンドライン・プログラム機能　組織のセキュリティ要件に柔軟に対応可能である

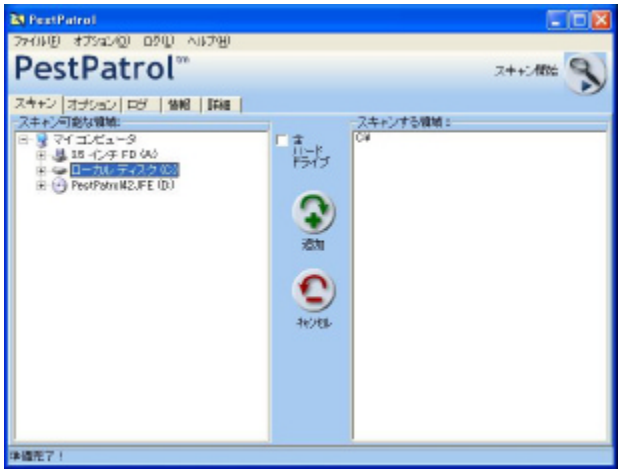

図-2　PestPatrol スキャン設定画面

4. コンピュータペスト検出システムの検証

【検証 1】利用後の端末ローカルドライブスキャン

センターが管理している教室系クライアント群の一部の端末（20 台）それぞれに PestPatrol4.2 をインストールし，1 日の利用時間が終了後に手動にて検査を行った．

5 日間検査を行ったが，すべての端末にてコンピュータペストの検出は無かった．

【検証 2】フリーソフトなどに含まれるコンピュータペストの検出

コンピュータペストはフリーソフトをインストールすることにより組み込まれることがある．インストール時に英語で説明があり，それとなく同意してしまいコンピュータペストまでもインストールされてしまっている場合がある．またシェアウェアのツールには，アドウェアがあらかじめ組み込まれているものもある．使用料を支払うことでライセンスキーを入手し，入力することで解除できるのだが，支払わないで使用している限りは組み込まれたままであり，これを駆除してしまうと，ツール自体使用できなくなる．

動画プレイヤーソフトとして広く使われているものの中には，インストール時にコンピュータペストを組み込む場合が見られる．これに組み込まれているコンピュータペストは，広告等を表示するアドウェアだが頻繁に表示される上に OS 起動時からプログラムがメモリに常駐しており，影響を及ぼしている．

このコンピュータペストは，PestPatrol にて検査を行い，検出することが可能であった．

【検証 3】PPCL 機能を用いたスキャン

センターが管理している教室系クライアント群の一部の端末（40 台）それぞれに PestPatrol4.2 をインストールし，PPCL 機能を用いて詳細設定を行った．

PestPatrol は administrator アカウントにて，インストールを行うため，最新の定義ファイルへ更新を行うと PPfile.dat，PPInfo.dat，Spyware.dat は administrator のファイル所有になってしまうため，利用者がログオンすると所有権が無くエラーが発生した．これを回避するため，everyone の読取と実行の権限付加を行ったが，この問題は，最新のバージョンでは解決されている．

詳細設定

・OS 起動時に PPMemCheck と Cookie Patrol を起動
・OS 起動後 3 分後に全スキャン開始
・CPU のアイドル時にスキャンを実行
・検出時に非通知（サウンド，ウインド）
・検出結果をメールにて送信

OS 起動後 3 分後に全スキャンを開始するのは，センターのシステムではログオンスクリプトが実行されており，CPU の負荷を増大しないために，CPU のアイドル時にスキャンを実行するよう設定を行った．

図-3　PestPatrol 自動スキャン設定画面

PestPatrol4.2 をインストール以後 2 週間に検出されたコンピュータペストを図-4 に示す．

危険度の高い「キーロガー」や「リモート管理ツール」の検出は無かったが，利用者の許諾なしに情報を送出してしまう「スパイウェア」や「アドウェア」「Browser Helper Object」が検出された．

「Browser Helper Object」は，ブラウザで閲覧しているすべてのページをサーチしバナー広告を置き換え，行った行為をモニターし報告を行うコンピュータペストである[3]．

また「Hijacker」と呼ばれるブラウザの設定を勝手に変更してしまうコンピュータペストが多数検出された．

しかしこの検出結果は Web アクセスを簡単にするソフト「JWord」のモジュールの一部に PestPatrol の検出用パターンと同一なコード含まれているためにコンピュータペストとして検出されてしまうもので，コンピュータペストでは無いとの見解を得ている[4]．

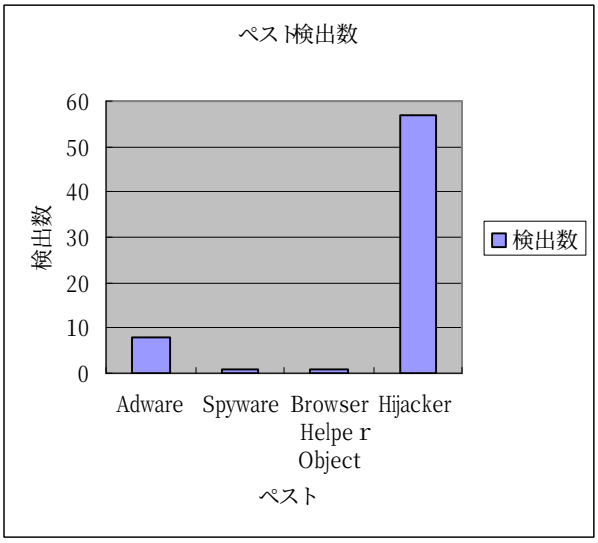

図-4　コンピュータペスト検出結果

5.コンピュータペスト検出システム導入方法の提案

今回の検証では，それぞれの端末に PestPatrol をインストールしていたが，センターで運用するにはすべてのクライアントを一括管理するのが望ましい．その為にドメインコントローラにて管理する方法を提案する．

現在センターでは，ログオンスクリプトを実行することにより，ウイルス対策ソフトのパターンファイル更新を行っている．同様に PestPatrol についてもログオンスクリプトを設定しておき，ログオン時に端末側で PestPatrol のモジュールである，PPMemCheck，Cookie Patrol，PPCL を実行する[1].

PPMemCheck，Cookie Patrol にて活動中のコンピュータペストを監視し，PPCL にて詳細設定を行い，端末のローカルドライブ，利用者個々のホームディレクトリをスキャンする．その時，検証時に行った設定以外に，コンピュータペスト検出時に管理者へメール通知をする設定や，検出ログをドメインコントローラへ自動転送するように設定しておく．

ドメインコントローラ上にて管理することにより，どの利用者のどの端末でコンピュータペストが見つかり処理を行ったかの確認をすることが容易であり，端末側にて定義ファイルの更新作業を行わないので，最新定義ファイルの更新を徹底し，全ての端末でコンピュータペストに対して共通の処理を行うことが可能である．

6.まとめ

センターでは，環境バックアップシステムにて毎日メンテナンスを実行していることで，そのマスターにコンピュータペストが存在していなければ，メンテナンス直後にコンピュータペストが検出されることが無い．しかしメンテナンス終了後から次のメンテナンス開始時にコンピュータペストを仕掛けられれば，これに対応することはできない．またコンピュータペストはウイルス対策ソフト，パッチ管理では対策が非常に困難である．

そこで，コンピュータペスト検出システムを導入することにより情報漏洩などに対する有効なセキュリティ対策が可能になる．

しかし全ての教室系クライアント群に導入するには問題も残されている．ログオンスクリプトで PestPatrol のモジュールを実行するため，多数の利用者が同時にログオンした時，ドメインコントローラ負荷やネットワーク負荷の調査検討は必要である．また 500 台以上もある教室系クライアント群から送られてくるログの管理をいかに負担無く行うかが検討課題である．但し，近日リリース予定の PestPatrol 専用管理ツール MCPP の使用により，ログの一元管理，定義ファイルの配信などの機能が利用できる開発が進んでいるそうである．

謝辞

今回の検証，実験は，株式会社アークン宮渕親二氏，斉藤純平氏をはじめ関係の方々の多大なるご好意により実現致しました．深く感謝致します．

参考文献

[1] 株式会社アークン第 1 回内部セキュリティソリューションセミナー資料　2003 年

[2] 株式会社アークン　PestPatrol 日本語版ユーザーズガイド　2003 年

[3] http://www.pestpatrol.jp/main_pestcategory.htm

[4] http://www.pestpatrol.jp/support/support_jword.html

[5]宇都宮大学総合情報処理センター電子計算機システム仕様書　1999 年