O-10

データ保護機能を有する電子保存システムの開発（3）
-利用者・機器間の認証方法の検討-
Development of Data Storage System for the Personal Data Protection (3)
-Consideration of a method of authentication among the complex which consists of users and equipments -

竹下孝幸[*1] 小尾高史[*2] 山口雅浩[*2] 大山永昭[*2] 谷内田益義[*2]
細田泰弘[*3] 菅生清[*4] 藤岡伸男[*5] 青野正宏[*6] 大賀哲二[*7]
Takayuki Takeshita Takashi Obi Masahiro Yamaguchi Nagaaki Oyama Masuyoshi Yachida
Yasuhiro Hosoda Kiyoshi Sugo Nobuo Fujioka Masahiro Aono Tetsuji Oga

1．まえがき

コンピュータシステムに対する脅威として一般的に考えられるカテゴリには、大きく分けて「不正アクセス」と「コンピュータウィルス」の２種類がある。「不正アクセス」では、攻撃する側は攻撃対象となるシステムを定めた上で、対象のセキュリティ上の弱点を試行錯誤的に調査し、しかるべき手段を選んで攻撃を加えるものである。

一方でコンピュータウィルス（以下、ウィルスと言う）は、活動の対象となるシステムの環境をあらかじめ想定した上で、一旦独立したデータ（ファイル）として作成され、ネットワークなどを通じて社会に拡散していく。したがってその攻撃対象は不特定であり、ウィルス作成者からみたその効果はある意味で成り行きに任せている面はあるが、インターネットの普及した近年の情報化社会にあっては、その被害や影響の深刻さは増すばかりである。

2．ウィルスによる被害

今日のウィルス被害の内容は、感染したコンピュータにおける利用者データの破壊や改竄のみならず、インターネット利用環境を前提とした利用者データの流出、不正なメールの送出、不正アクセスの環境を準備するものなど、巧妙でしかも利用者に甚大な悪影響を及ぼすものとなっている。他方、ウィルスの用いる手法の観点で見るならば、昨今ではマクロ型ウィルス、スクリプト型ウィルスなど、オペレーティングシステム（以下、OS と言う）やアプリケーションの高度化した機能の存在を前提として、それを感染や活動の手段として利用するものが主流となっている[1]。

このようなウィルスに対しては、その発見と防御を目的としたいわゆるウィルス対策ソフトウェア製品が種々出回っており、いずれも随時更新されるウィルス対策情報を利用者に頒布することにより、それまでに存在が確認されたウィルスに対しては網羅的によく対応できるようになっている。これらの製品はウィルスに対するセキュリティを確保するためには欠かせないものと言える。

しかし、更新されるウィルス対策情報は、ある程度社会に拡散した上で報告され、対策が開発されたウィルスに関するものであり、いわゆる後追いの情報でしかない。

[*1] 富士総合研究所
[*2] 東京工業大学
[*3] NTT コミュニケーションズ
[*4] リコーシステム開発
[*5] 日本電気
[*6] 東京工業高等専門学校
[*7] 三菱電機

すなわち、社会に存在するコンピュータシステムとそこで行われているウィルス対策を熟知した上で、それを欺くべく手法を新たにしたウィルスが絶えず出現している。

3．ウィルスの活動に関する考察

ウィルスが一般の OS におけるファイルの形式を採っているものであるならば、その活動の端緒は、利用者が

①そのファイルを実行形式として開くこと
②システムにインストールされているアプリケーションによってそのファイルを読み込むこと

以外にはない。利用者によるそのような操作は、必ずしも意識的、明示的に行われるものだけではなく、昨今の自動化の進んだ OS 環境やアプリケーションにおいては、一般の利用者が認識する範囲外で、実は数多くのファイル操作が、当該利用者のアカウントのもとで行われているものである。ウィルスがこのことを悪用して不正行為を働くことはすなわち、システムが厳密な意味での利用者の認証に失敗し、利用者本来の意思から外れて、システム資源の詐取を許してしまうことに他ならない。

4．耐ウィルスシステムの概要

以上の考察に鑑み本稿では、ネットワーク接続環境下にあるローカルなパーソナルコンピュータ（以下、PC と言う）について、ウィルスの活動による不正な動作を抑止し保護することを目的とした耐ウィルスシステムを提案する。このシステムでは、あらかじめ当該の利用者ごと、及び利用するアプリケーションごとに許可される周辺機器へのアクセスを定義し、これを逸脱したものを不正な動作として排除する。さらに周辺機器への即時的な不正行為もさることながら、メモリ上にしかるべきプロセスを常駐させ、時間などのシステム状態を監視しつつ、特定の条件の下で不正な活動を実行する、などの行為も併せて対処できるものを目指す。

システムの基本的な考え方としては、動作を保護すべき PC（以下、本体マシンと呼ぶ）とはハードウェア的に独立した別個の PC（以下、クローンマシンと呼ぶ）を用意する。またシステム内に存在するファイルについて、ウィルスに感染した可能性のないファイル（以下、認証ファイルと呼ぶ）と、それ以外のファイル（以下、非認証ファイルと呼ぶ）の概念を導入する。利用者がアプリケーションを利用する過程で、非認証ファイルを読み込む場合、その動作はクローンマシン上で行い、その結果として発生する事象、すなわちマシンプロセス及び周辺機器へのデータ入出力を監視して、不正なプロセスの発生の有無を確認する。

5．耐ウィルスシステムの構成

図１に示すシステム構成図において、ユーザ装置、本体マシンのプロセッサ及び保存装置は、通常の PC の構成要素である。ここでユーザ装置は、ディスプレイ、キーボード、マウスなどからなるユーザインターフェース装置を表す。プロセッサとは CPU、システムメモリ、各種コントローラなどの集合を表す。また保存装置はハードディスク装置などである。通常の PC では、各装置は相互に直接データ入出力を行うものであるが、本システムでは各装置の動作及び装置間の連携を制御するものとしてシステム制御装置を設定する。システム制御装置は、ユーザ装置入出力制御装置、プロセス制御装置、ディスク入出力制御装置からなる。

クローンマシンはシステム構成及びファイル構成を本体マシンと完全に同一のものとし、システムブート以降の両マシンの動作は同期している。

ユーザ装置に投入されたアプリケーション操作などのコマンドは、ユーザ装置入出力制御装置を経由して、両マシンのプロセッサに等しく伝達される。プロセス制御装置は、両マシン上のプロセスを常に監視し、プロセッサが保存装置とのデータ入出力要求を発行すると、ディスク入出力制御装置が介在して、データ入出力が行われる。ネットワークデバイスを経由して外部から取り込んだデータは、ディスク制御装置から一旦、両マシンの保存装置上に格納し、ファイルとして取り扱われる。

アプリケーションを操作する過程で、非認証ファイルの読み込み要求が発生した段階で、プロセス制御装置は本体マシン上のアプリケーションの実行を停止する。一方クローンマシン上では引き続き、当該ファイルを読み込んで以降のアプリケーションの実行を継続する。ただしプロセス制御装置は、利用者及びアプリケーションごとに、保存装置やネットワークデバイスに対する入出力に制限を設け、この内容をあらかじめプロセス許可テーブルに登録しておく。プロセス制御装置はこの制限を逸脱した入出力要求を検知した段階で、クローンマシン上のアプリケーションの実行を停止し、その旨を利用者に通知する。アプリケーションの終了時には、本体マシン上のプロセス状況をクローンマシンにコピーし、再度同期化させる。

ここで独立したクローンマシン及びシステム制御装置を設ける理由は、単独のPCにファイル読み込みとプロセス監視機構を持たせることでは、ウィルス作成者がその構造を認識した上で、その監視機構を欺くウィルスを開発する可能性が考えられるからである。プロセス制御装置は外部から一方的に監視および制御を行うものであって、クローンマシン上のプロセッサに、ウィルスによるいかなる不正なプロセスが発生しても、プロセス制御装置自身がウィルスに制御を奪われる可能性はない。またディスク制御装置も、入出力するファイルを単なるデータとして転送するだけなので、同様に安全である。

6．現状と課題

本システムを実現する上での最大の課題は、ウィルスによる不正な動作を排除するための、プロセス許可テーブルの設定である。これはシステムが認証した利用者に対し、アプリケーションごとに利用できる周辺機器とその条件を定めるものであるが、アプリケーションの操作性を損なわず、しかも利用者の権限を厳正に定めるものとする必要がある。また現実的な運用を考えれば、認証ファイル・非認証ファイルをあらかじめ識別し、ファイル認証テーブルとして管理することも必要である。これらのことを踏まえて、現在この耐ウィルスシステムについて、実装に向けた詳細設計及びプロトタイプシステムの開発を進めている。

謝辞

本研究は通信・放送機構の委託研究テーマ「情報セキュリティ高度化のためのデータ保護技術に関する研究開発」により行なっている。

参考文献

[1] http://www.trendmicro.co.jp/virusinfo/basic/type.asp

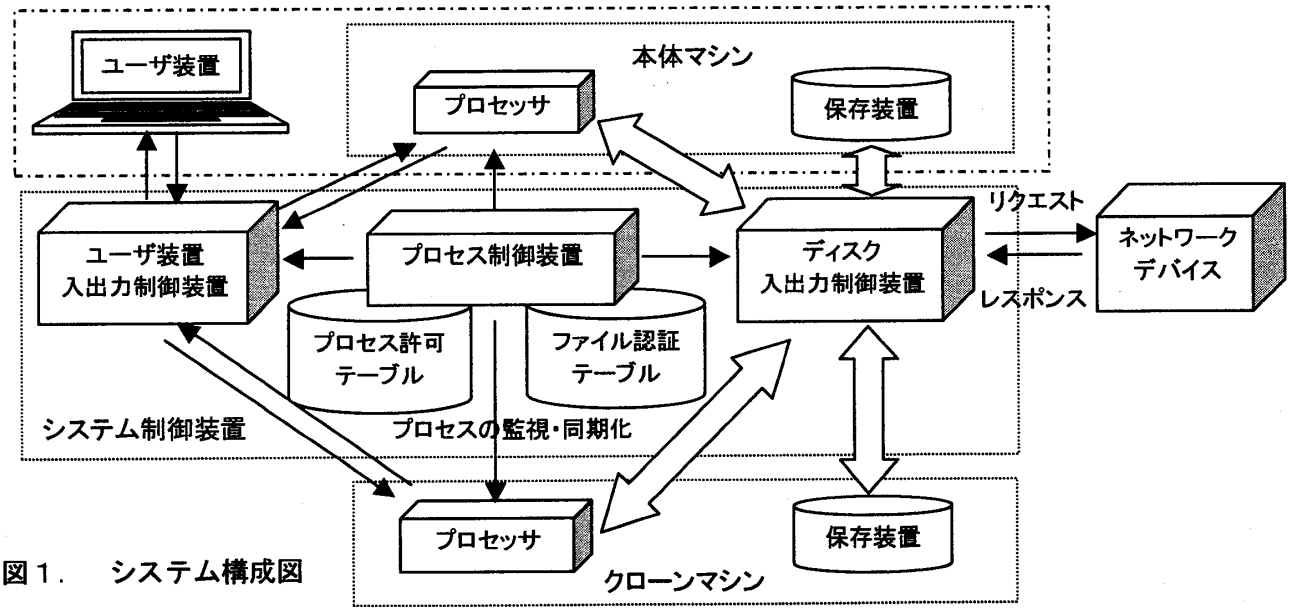

図１．　システム構成図