モバイルコンピューティングと
ワイヤレス通信 18－20
高度交通システム 6－20
（２００１．９．７）

耐ウイルスファイル保全方式の提案とモバイル機器

青野正宏[*] 谷内田益義[**] 小尾高史[***] 大山永昭[***] 山口雅浩[***]
[*]前三菱電機(株) 注1＜現東京高専＞ [**](株)リコー [***]東京工業大学

ファイル更新の履歴を H/W 的に自動的に収集する。コンピュータウィルスにファイルを破壊されたとき、そのファイル更新履歴から復元を図る。この方式を整理して、マルチプロセッサ構成によるコンピュータウィルス対策として概念をまとめた。この概念を基本に我々はファイル保全方式を設計・開発中である。このなかで、本稿ではコンピュータ単体で実現する方法に絞り、ウィルス攻撃を避けるための手段、効率的な履歴保全方式などを提案する。さらにモバイル機器へのファイル保全システムの適用を考察する。

Virus Tolerant File Preservation System and Mobile Eqipment

Masahiro Aono[*] Masuyoshi Yachida[**] Takashi Obi[***]
Nagaaki Oyama[***] Masahiro Yamaguchi[***]
*Mitsubishi Electric Corp. (Former affiliation)
＜Tokyo National College of Technology (Current Affiliation)＞
**Richo Corp. ***Tokyo Institute of Technology

When files are destroyed by a computer virus, the computer attempts to restore from the file update records. In this method, we established a concept of measure against the computer viruses by the multiprocessor system. Then, we are designing and developing file preservation methods against the viruses on the basis of this concept. In this paper, we select a method with a single computer system from the methods, and show the means to avoid attacks of the viruses, and an efficient record preservation method. Moreover, we consider applications of the file preservation system to the mobile equipment.

Key words: Computer Virus, File Preservation, Multiprocessor, Journal

１．はじめに

IT 革命の言葉に象徴されるように、インターネットを利用した情報通信は社会のインフラストラクチャーとしてなくてはならないものになった。インターネットは開かれた世界の情報交換の場となっており、不特定の相手との情報交換が行なわれている。しかも、単なるデータとしての送受信のみでなく、エージェントプログラムや オフィス・ソフトウェアのマクロ命令などのように、外部から入力されたデータに添付されたプログラムを実行することにより、木目の細かい処理を実現することが可能となっている。一般のユーザは外部から入力されたプログラムが実行されていることはほとんど意識していない。ところが、このようにオープンな情報交換が発展し、外部から送り込まれたソフトウェアを実行して、多様な使用方法が可能になると、逆にコンピュータシステムやシステムネットワークに害を与えるコンピュータ・ウィルス（以下、ウィルスと略する。）が跋扈する問題が生じてきている。ウィルスにより、コンピュータユーザが予期しないところで、ソフトウェアやデータベースが破壊されたり、ネットワークに混乱を与えたりしている。しかも、従来はフロッピーによる情報交換時に汚染されるケースが多かったが、最近はメールで簡単にファイルが送信できるため、メールによる汚染が広がって

注１ 通信・放送機構殿の助成を受け、本研究の基礎を行った当時の所属を示す。

おり、汚染拡大の速度が極めて速くなっている。新しいウィルスが発生すると、１日の間に全世界に広がるなど、その被害は深刻となっている[1]。

このウィルス問題に対して、ウィルスを事前に検出し駆除することを目指すワクチンプログラムによる対策がとられている。パターン・マッチング手法やルールベース方式，ソフトマイズ方式など、いくつかの方法が存在するが、いずれもウィルス防止方式としては、それだけで十分とは言い難い[1]。

ワクチンプログラムのように直接ウィルスと対決し、ウィルスを発見・駆除を目指す抗ウィルスの方法とは別に、ウィルスを直接発見・駆除することはできないが、ウィルスによる被害を最小限に抑える耐ウィルスの方式が考えられる。ウィルスによる被害で最も大きいのは情報の喪失である。OS や汎用ソフトウェアは再インストールにより復元できても、ユーザが収集や作成した情報は復元できない。

ソフトウェア障害や誤操作により、ファイルの消失や改変がなされたとき、ファイルを復元可能とするため、ファイル更新の履歴をとるソフトウェアがある[2]。すなわち、ディスクに履歴領域を確保し、ファイルへの更新が実行されるたびに更新前のファイルの内容を履歴領域に記録する。ファイル復元の必要が生じたとき、履歴を逆に辿って順次復元することにより、履歴が記録されている範囲内では、任意の時点の状態まで復元できる。このソフトウェアは一般にウィルスによるファイル破壊に対しても有効である。しかし、ウィルス作成者がこのソフトウェアの存在を意識して履歴領域を破壊すれば、ファイルの復元に対して無効となってしまう。

ディスクへのファイルの入出力をすべてコンピュータのホスト CPU の制御により実行する方式に代えて、ファイルの入出力処理はホスト CPU の制御を受けて専用のティスク制御プロセッサが耐ウィルス保存装置として実行する。このファイルのディスクへの書き込み処理のとき、耐ウィルス保存装置は同時にファイル更新の履歴を自動的にとる。耐ウィルス保存装置のプログラムは ROM に書き込まれており、ホスト CPU からの命令では書き換え不能とする。このように構成すれば、ウィルスによるファイル破壊から防御することができる[3]。このアイデアを基本に通信・放送機構から助成を受け、平成 12 年度から東京工大と複数の企業でコンソーシアムを結成し、「耐ウイルス機能を持った情報通信システム構築に関する研究開発」を開始した[4]。本稿においては、平成 12 年度の研究成果のひとつとして耐ウィルス実現方式について検討した結果の一部を発表する。さらにモバイル機器への適用について考察する。

２．研究の前提条件

本研究の前提条件は次のとおりである。

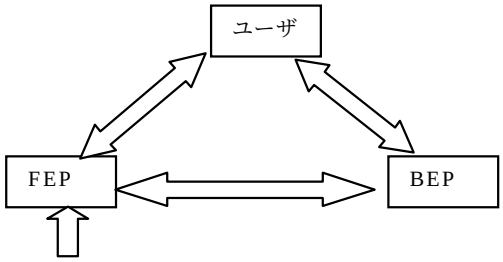
- 本研究の目的は、ウィルスによりユーザ・コンピュータの致命的なファイル破壊を防止する点にあり、ウィルスの検出や駆除は対象としていない。
- 本研究では、文書作成，文書閲覧，メール処理，インターネットアクセスなどのごく一般的用途のコンピュータを対象とする。
- ユーザの意志によらないファイルの更新や消去が発生すれば、ユーザはその変化に気がつくものとする。
- コンピュータのソフトウェアで実行できる機能はすべてウィルスにより実行される可能性があると考える。
- そのコンピュータで動作するソフトウェアの構造はウィルス製作者に知られてしまうものと考える。

３．耐ウィルス実現方式

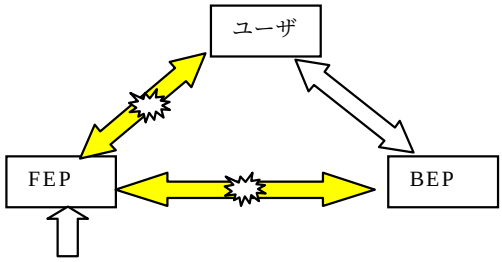
３．１ マルチプロセッサ構成

耐ウィルス保存装置の発想が先行したが、本節ではウィルス対策のシステム構成面からの対策を整理した。あるプロセッサがウィルスプログラムを読み込んだとしても、ウィルスプログラムに制御権を渡さなければ単なるデータに過ぎず、システムが悪影響を被ることはない。プロセッサにオリジナルに存在するインタプリタが外部からの入力プログラムを１ステップづつ、システムに悪影響を及ぼさないかどうか監視しつつ実行すればウィルスによる悪影響を避けることはできる。しかし、この方法はシステムの利便性を大きく損なう。

「ウィルスに汚染されていない物理的に隔離されたプロセッサに対しては、別のプロセッサに直接害を及ぼすとはできない。（通信指示により間接的に害を及ぼすことはできる。）」という点に着



正常時は FEP と BEP が協調して作業



FEP が汚染されていると、ユーザと BEP に一見正常と見せて悪影響を与えようと試みる。

図１．FEP と BEP の考え方
Fig.1 Concept of FEP and BEP

目する。ウィルスに汚染されていないプロセッサが､外部から入力された情報を厳重にチェックし、害を及ぼさないことを確認するか、または害かどうか不明であり外部からの指示を実行するにしても、復元が可能なように対策を施すことにより、耐ウィルス機能を実現しようとするものである。ここでウィルスに汚染される可能性があるプロセッサを、ウィルスに対して前線にあるのでフロントエンドプロセッサ（以下 FEP と略す。），汚染されないことを保証するプロセッサをバックエンドプロセッサ（以下、BEP と略す。）と呼ぶこととする。FEP は外部から入力されたファイルのマクロ命令等を実行することにより利便性を確保するが、ウィルスに汚染される可能性を持つ。BEP はシステム生成時を除き、外部から入力されたプログラムに制御権を渡すことはしない。また、FEP からの指示に対しては、上述のとおり耐ウィルス対策を施した上で実行を行なう。コンピュータユーザ，FEP，BEP をひとつのマンマシン系とすると、正常時は全ての要素が協力して動作するが、FEP がウィルスに侵されると、FEP はコンピュータユーザ及び BEP を可能な限り騙しにかかるという前提でシステムを設計する。FEP と BEP それぞれ１台づつで構成されている場合は、両者を合わせて、ひとつのコンピュータとみることができる。（図１参照）

３．２ 役割分担方式

FEP と BEP の役割分担については、いくつかの分割方法を提示する。まず、コンピュータの機能から、ディスクドライバー，コンソール入出力機能，通信制御機能，外部命令実行機能を抽出し、その他の機能をメイン機能として、５つの機能に分けるものとする。

(1) ディスク入出力命令代替方式

FEP は、ディスクへの入出力処理を除く全ての処理を実行する。FEP のソフトウェアは既存のままとする。BEP はディスクへの入出力処理とディスク・ファイルの破壊に備えてファイル更新の履歴をとる処理を行う。

(2) ファイル入出力命令代替方式

FEP は、ディスクへの入出力処理を除く全ての処理を実行するが、ファイル出力プログラムを BEP に情報を伝達できるよう入れ替える。BEP は、FEP から伝えられた情報を利用してディスク・ファイルの退避などの保護処理を行なう。

(3)機能分散方式

FEP は、ディスクへの入出力制御，コンソールディスプレイの表示，キーボード入力，マウス入力処理などを除いた処理を担当する。BEP は FEP で除いた処理を担当する。この分割の考え方は、テンポラリファイルやあらかじめ、BEP 側で指定されている自動ファイル更新を認める条件の場合を除いて、ディスクの更新・消去に対しては、その都度ユーザの意志を確認するものである。ウィルスによりユーザの意志を誤らせるような画面表示､情報入力などが行われないよう BEP 側において保護しなければならない。

(4) 外部プログラム分離方式

FEP は、ファイルに添付されたマクロ命令の実行など、外部から入力されたプログラムの実行のみを担当する。BEP は、FEP が改変できるディスク領域やメモリアドレスの範囲を限定する機能と、正規にインストールされたソフトウェアの

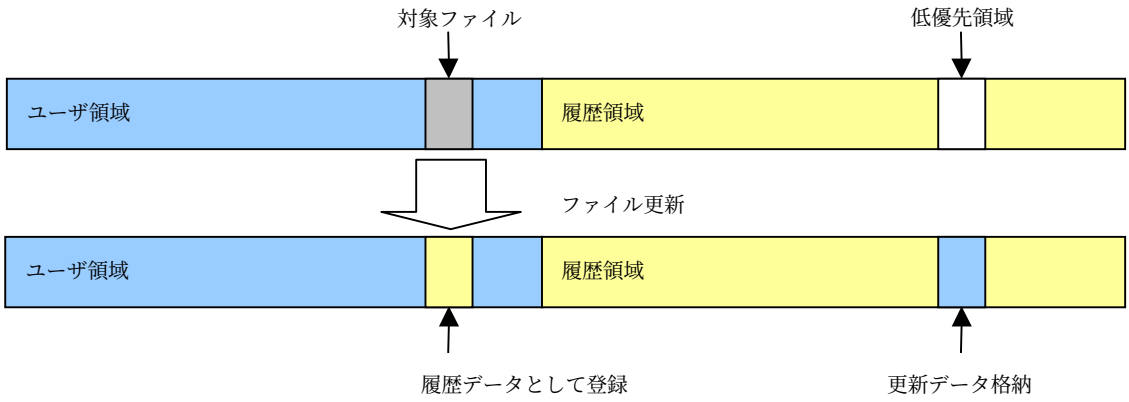


図 2 ファイル更新例
Fig.2 Example of File Update

実行を担当する。

提示した各方法のなかで、ディスク入出力命令代替方式とファイル入出力命令代替方式は最初に着想した耐ウィルス保存装置の考え方で、ウィルスによる活動そのものを封じ込めることはできず、被害を検出したときに復旧を図ることを狙った耐ウィルス対症療法である。それに対し、機能分散方式と外部プログラム分離方式はウィルスの活動を封じ込めることを目指した抗ウィルスの方法である。ところで、機能分散方式と外部プログラム分離方式は、システムの OS，メール，ワードプロセッサなど既存プログラムの改変を伴う。また、機能分散方式と外部プログラム分離方式は処理の分割方法が複雑であり、システム設計のバグによるセキュリティ・ホールの発生やマクロプログラム実行の利便性を損なうことを防止するための設計には慎重な検討が必要であり、実現は容易ではない。現実的には耐ウィルス方式が用意であるが、ウィルスが耐ウィルス機能を備えたプログラムを意識して攻撃をかけてくる場合には、対症療法のみでは無力となる場合もある。そのため、コンソーシアムにおける研究では耐ウィルス保存装置の方式を基本に実現を目指しているが、機能分散方式の考え方も一部（コンソール入出力機能をユーザ装置として分離）取り入れて検討している。全面的な機能分散方式と外部プログラム分離方式は今後の課題として挙げるにとどめておく。また、耐ウィルス保存方式のなかで、ファイル入出力命令代替方式はソフトウェアのみでプロトタイプシステム構築が容易なため、研究では本方式を中心に開発を進めている。しかし、ファイル入出力命令代替方式は OS に依存する。ディスク入出力命令代替方式は、ディスク制御装置の開発を必要とするが、OS に依存しない。本稿ではコンソーシアムにおいて概念設計としてのみ進めてきたこのディスク入出力命令代替方式を中心に説明する。

3．3 ディスク入出力命令代替実現方式

基本的な考え方は次のとおりである。現状のコンピュータにおいて、CPU，メインメモリなどで構成する装置を FEP としてホスト装置と呼ぶこととする。ホスト装置上のソフトウェアの基本構成は変更しない。ただし、既存ソフトウェアの構成上に新たな耐ウィルス処理ソフトウェアの追加が必要となる。現状のコンピュータ構成におけるディスク装置及びディスク制御装置を BEP としてこの章で検討する耐ウィルス保存装置に置き換える。耐ウィルス保存装置はホスト装置から物理的なディスク領域に対する読み出し命令，書き込み命令を実行する。このとき、読み出し命令はそのまま実行するが、書き込み命令は、その命令がウィルスまたはユーザの誤動作による不正な書き込み命令である場合に備えて、書き込まれる前の領域のデータを退避して履歴をとる。不正な書き込みがあることにコンピュータ・システムのユーザが気づいた場合、履歴データを利用してファイルの復元を図る。

耐ウィルス保存装置において、ホスト装置からのディスク領域への書き込み命令に対応して、該当する領域データの退避を行なうと、旧データの耐ウィルス保存装置メモリへの読み出し、履歴領域として割り付けたディスク領域への書き込み，新データの当該ディスク領域への書き込みが必要

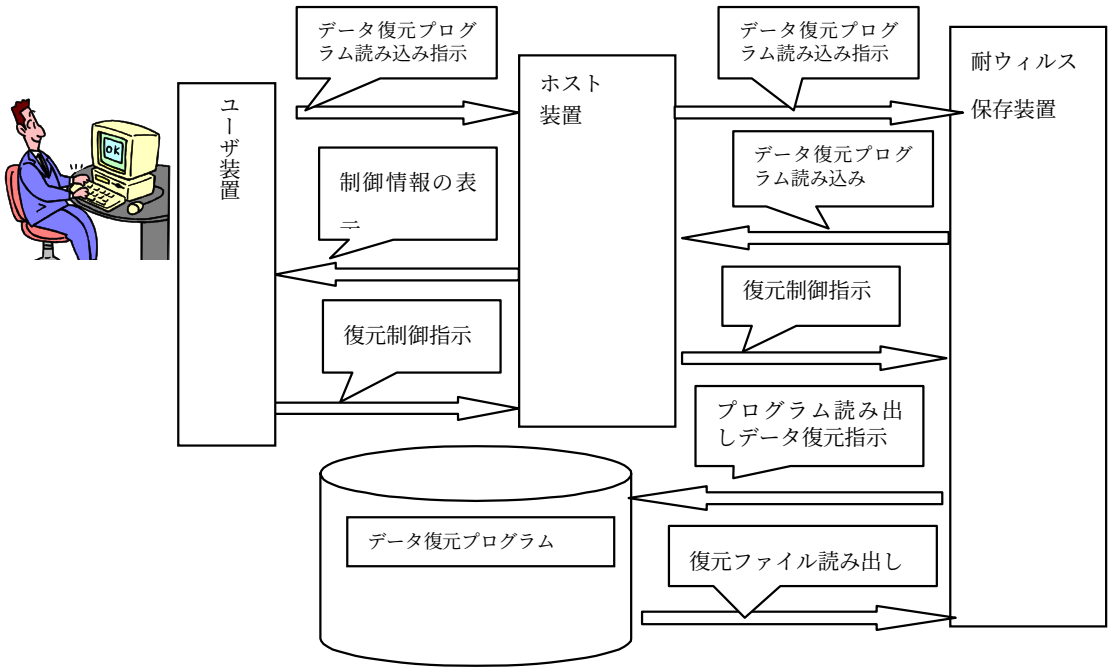


図３　データ復元の手順

Fig.3 Steps of File Recovery

となり、退避を行なわない場合に比べて約 3 倍の時間が必要となる。その対策としてまず、ディスク領域を一定の大きさに分割し、分割された一つの領域をページと呼ぶこととする。耐ウィルス保存装置内にページ単位に論理メモリと物理メモリの変換装置を設ける。これを論理／物理ページ変換装置と呼ぶこととする。ページの更新が発生すると、未使用ページを割り付けて更新データを書き込み､論理的な更新前ページアドレスとする。物理的な更新前ページは履歴領域として割り付け､新しい更新データのため割り付けた未使用ページ論理ページアドレスとする。この論理／物理変換装置は、不揮発性の高速アクセス／書き込みができる記憶装置が望ましい。(図２参照)

ホスト装置に書き込みを指定されたデータがページサイズと一致しない場合は、ページ単位でデータ更新がなされることを保証するため、更新データ書き込みで書き残されたページの残りに、相当する更新前ページのデータを書き込む。未使用論理ページがなくなれば、時間的に最も更新時刻が古い退避ページから解放し、未使用論理ページに戻す。この方法により、ディスクからの読み書きのアクセス時間を大きく抑制することが可能となる。また、コンピュータ・システムのユーザから見て、未使用領域とされるディスク領域は全て履歴領域とすることができるから、未使用領域の大きさに応じてデータ復元のため溯る時間を設定することができる。ただし、ファイルの断片化が進み易く、逆にファイルの読み出しに時間がかかる場合が生ずる副作用がある。しかし、耐ウィルス保存装置独自に自動デフラグ用のソフトウェアを組み込んでおき、ホスト装置からの入出力の指示がないときにデフラグ処理を行うことも可能である。

ページサイズは大きくとると、ページサイズに対する実際のデータサイズが小さくなり、データ未書き込み領域に対するページ単位更新を保証するための追加書き込み処理量が増大する。データ未書き込み領域が更新されれば、同様に当該ページに対して同様の処理を行なわねばならない。全体として履歴領域の確保の速度が大きくなり、データ復元が必要となったとき、過去に溯れる時間が相対的に小さくなる。ページサイズを小さくすると、論理／物理ページ変換装置のサイズが大きくなる。また、一回のホスト装置からのディスクへの書き込み処理に対し、書き込みを行なうページの数が増大する。どの程度の大きさが望ましいかは検討課題である。

４．ユーザへの情報表示とユーザからの入力

４．１ ファイルの復元

ディスクのファイルが破壊されていることにユーザが気づいた場合、履歴領域に残されているデータを用いてデータの復元を行わねばならない。通常は、主要なマンマシンインターフェイスの制御はホスト装置側にある。ファイルが破壊されている原因がウィルスによるものとしたら、単なるホスト装置による制御は危険である。しかし、ディスク領域の破壊が悪意のないソフトウェアのバグやオペレーションミスによる破壊もであり、単なる UNDO 機能として利用したい場合も考えられる。複雑な操作は好ましくないので、復元指示の制御もホスト装置で行なう方法が望まれる.。この場合の対処方法として、耐ウィルス保存装置が管理する非更新領域（書き込み禁止領域）にデータ復元プログラムを配置しこれを実行させるか、または、CD，フロッピーなど可搬性外部記憶装置から独立のプログラムを読み込んで実行させる方法が考えられる。いずれにせよ、データ復元プログラム自身が汚染させることがないよう、通常運用時のソフトウェアと独立させておくことが必要である。また、ウィルスがデータ復元プログラム機能を摸擬してホスト装置から耐ウィルス保存装置に偽のディスクデータ復元指示を出すことも考えられる。この対策が必要である。

４．２ ウィルスによる履歴領域食いつぶし攻撃

ファイル更新履歴を記録することによる耐ウィルスのファイル保全対策に対し、ウィルスが大量の無効データを繰り返しディスクに書き込むことにより、コンピュータシステムのユーザがファイル破壊に気づく前に、履歴領域を食いつぶさせ、ユーザによるファイル復元を不能にする攻撃が考えられる。この攻撃に対処するため、単位時間あたり履歴領域を使用する頻度を監視する。しかし、新たなソフトウェアのインストールなど、一時に大量のディスク容量を正常に消費する場合もあり、大量ディスク消費が正常か異常かはシステムで一律には判断できない。そのため、ある閾値を越えて履歴領域が使用される場合は、ユーザに警告を発し、正常か否かの判断をユーザに求めるものとする。異常を検知した耐ウィルス保存装置がホスト装置への警告は、オリジナルのＯＳやユーザプログラムの操作の互換性を保つため、ディスクの入出力を模擬する経路とは別の接続方法で実現する。一般的に警告はマンマシンインタフェースとして画面に表示することが望ましい。画面制御はホスト装置で行われるので、耐ウィルス保存装置からホスト装置に警告を送信し、ホスト装置は警告を画面に表示する。ユーザが異常であると判断すれば､ここでシステムの動作を強制的に停止し、ディスクの保護を図るとともに、ウィルスの駆除やホスト装置のシステム再生成など、システムの保全を図る。ユーザがディスクの更新を正常と判断すれば、正常との判断情報をホスト装置経由で耐ウィルス保存装置に伝える。耐ウィルス保存装置はディスクデータ更新を再開する。

しかし、この方法のみでは、ウィルスが耐ウィルス保存装置からの受付回答処理を摸擬し、ディスクの更新を停止すべき場合に正常であると耐ウィルス保存装置に回答する恐れがある。

４．３ ユーザ装置

ファイル破壊に対するファイル更新履歴からの復元の実行や一時的な大量ファイル更新を防止の実行を行うのは BEP である耐ウィルス保存装置である。ところが、実行の可否を判断するのはユーザである。このため、安全に耐ウィルス保存装置からユーザに警告を発したり、ユーザから耐ウィルス保存装置に指示を与えたりしなければならない。ホスト装置とは別に、直接ユーザと耐ウィルス保存装置とインタフェースを持てば問題はない。しかし、操作性からすると通常のディスプレイモニタ，キーボード，マウスなどをシステムとユーザのインタフェースとしたいところである。このため、Ｘターミナルや WBT 装置と同様にユーザとのマンマシンインタフェースを司るユーザ装置を導入する。この装置は耐ウィルスに関する機能も合わせ持ち、外部プログラムを受け付けない BEP として動作させるものとする。

ユーザ装置は、ホスト装置と接続し、ホスト装置から指示されたとおりに情報をディスプレイモニタに表示する。また、キーボードやポインティングデバイスによる文字入力や位置入力の情報はホスト装置に伝えられる。それに加えて耐ウィルス保存装置からの入力をホスト装置からの表示指示に優先して表示したり、耐ウィルス保存装置へ情報を伝達したりする機能を持つものとする。

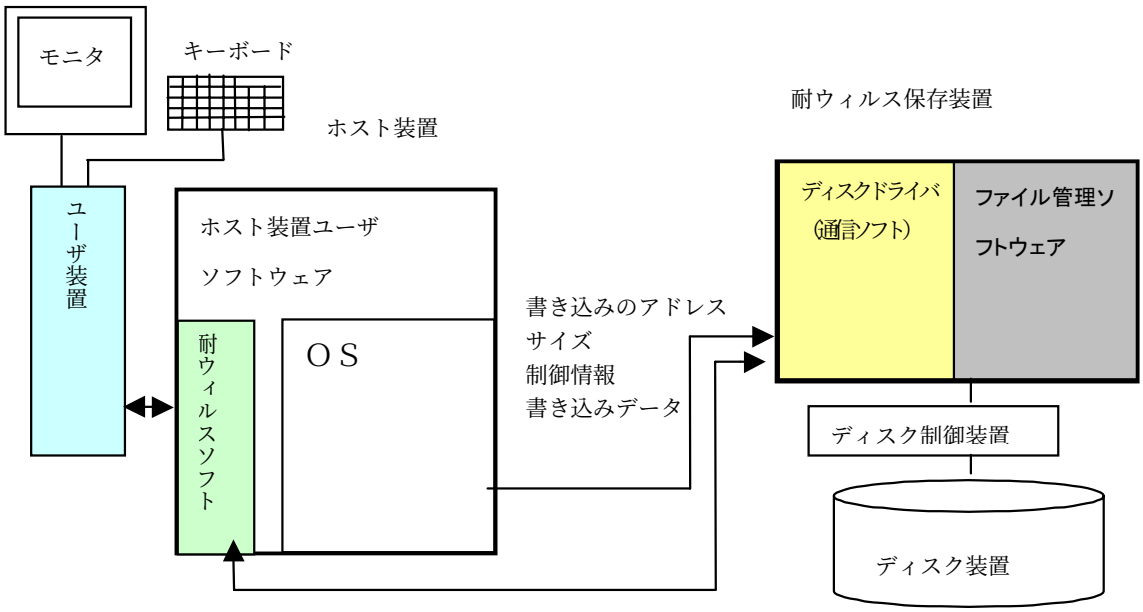


図４　耐ウィルスファイル保全システムの構成概要
Fig.4 System Configuration of File Preservation system

これらの機能は FEP であるホスト装置を経由して行う。ホスト装置にはユーザ装置と耐ウィルス保存装置との間の中継を行うソフトウェアをインストールする。そのとき、ホスト装置はウィルスに汚染されている可能性もあるので、正しく情報を中継するとは限らず、伝送を妨害したり伝送内容の改竄を行う恐れもある。

従ってユーザ装置と耐ウィルス保存装置間の情報交換は、正しくユーザ装置または耐ウィルス保存装置から入力されたことを証明する形で入力して送信されなければならない。そのため、暗号化して送信しなければならないが、暗号化形式を固定化すると、ウィルスに情報の形式を読み取られ､ウィルスに偽の応答を返される可能性がある。従って、形式が固定的な応答は不可である。次の手順が考えられる。鍵αを用いて情報βを暗号化した情報を Eα(β)で表す。ユーザ側と耐ウィルス保存装置で共通鍵 K1 を共有する。これは不特定相手との通信ではないので容易に行なうことができる。耐ウィルス保存装置は鍵 K2 と警告情報(Warning)を鍵 k1 で暗号化し、EK1(Warning＋K2）として送信する。ユーザはホスト装置経由で EK1(Warning＋K2）を、鍵 k1 を用いて警告情報と鍵 K2 を取り出す。K2 を用いて応答（正常の場合は継続<Continue>，異常の場合は停止<Halt>の要求）を暗号化し、EK2 (Continue or Halt)として、ホスト装置経由で耐ウィルス保存装置に送信する。耐ウィルス保存装置は鍵 k2 を用いて応答を得る。鍵 K2 は毎回変動させる。

次に、ウィルスによりホスト装置がユーザと耐ウィルス保存装置との通信を妨害することも考えられる。そのため、ユーザ装置から定期的にヘルシーメッセージをホスト装置経由で耐ウィルス保存装置に送る.耐ウィルス保存装置は応答をホスト装置に返す。各メッセージの長さを等しくしておけば、毎回異なるキーで暗号化しているのでホスト装置ではメッセージの中身は判断できない。ホスト装置が通信妨害を行うと、耐ウィルス保存装置には正しい応答が返らないのでタイムアウトとなり、耐ウィルス保存装置のディスク更新は無視され、ファイル破壊は防止できる。

５．　システム構成

ディスク入出力命令代替方式は、ホスト装置を現行のメインＣＰＵとし、耐ウィルス保存装置をディスク制御装置の位置づけとする。耐ウィルス保存装置はメイン CPU（ホスト装置）のデータバスを経由してディスクを制御するディスク制御装置を模擬する。耐ウィルス保存装置は耐ウィルス保存装置自身を動作させるプログラムを格納するメモリ，論理／物理ページ変換装置，運用系ディスク装置が必要である。また、タイマ，警報装

置も直接耐ウィルス保存装置から制御できることが必要である。さらに、ホスト装置から見て耐ウィルス保存装置を単なるディスク制御装置と見せるだけでは済まない通信については、直接、通信できる接続経路を設けておくことが求められる。ホスト装置には現行 OS やユーティリテイ，アプリケーションプログラムをそのまま実装する。加えて汎用 OS のアプリケーションとして耐ウィルス保存装置と直接通信ができるソフトウェアをインストールする。耐ウィルス保存装置のソフトウェアはホスト装置のシステム生成結果情報を得てインストールする。耐ウィルス保存装置のソフトウェアは運用中に更新されることはない。

６．モバイル機器への適用

モバイル機器がノート PC のように、固定ディスクなどの非揮発性メモリとメインメモリなどの揮発性メモリから構成され、プログラムの実行は一旦、揮発性メモリに読み出して実行する場合は本稿のディスク命令代替方式で対応できる。しかし、小型装置で小量のデータのみ記録する装置で非揮発性メモリから揮発性メモリに読み出す方式でなく、全て不揮発性メモリから、直接読み出し／書き込みする方式の場合、本稿の方式は採用できない。小量のデータとは言え、装置の所持者にとって重要な情報が、小型装置にエージェントの形で読み込んだウィルスにデータを消去されると問題である。ディスク命令代替方式のように不揮発性メモリに書き込みをかける前にデータ更新の履歴をとるわけにはいかない。

結局、定期的にデータのハッシュ値を定期的に検査することにより、データ内容の変化の有無を判断し、データ内容の変化があれば履歴を記録する方法となる。このとき、ウィルスによる影響を排除するため、小型装置の CPU とは別の BEP に相当するプロセッサで実行するか、通常レベルのプログラムからは移行することができないように特権モードを BEP 相当として設定する。別プロセッサまたは特権モード以外ではアクセスできない特定のメモリ領域を履歴領域とし、定期的に履歴の記録を行う。データの復元や履歴領域に対するウィルス攻撃への対処策も 4 章で示した方法で対処できる。あるいは BEP 相当のプロセッサや特権モードから専用の警報表示や入力機能を設ける方法も考えられる。これらの小型機器の場合、PC の場合と異なり既存の OS を基としてシステムを構築することは難しい。

７．まとめ

平成 12 年度において、着想に基づく PC でのデモシステム・プロトシステムの制作と、着想を展開したアルゴリズムとシステムの基本設計を行った。本稿で記述を割愛したネットワーク上に履歴領域を置く方式、履歴領域の消費を節約するためのチェックポイント法、世代管理、差分記録などの手法も検討している。本年度以降に設計アルゴリズムに基づいたモデルシステムの製作・評価などにより、システムの開発・検証を進めて行く予定である。また、本稿で少し触れたように PC 以外のモバイル機器やホーム機器へのウィルス対策も検討していく予定である。

謝辞

本稿は通信・放送機構殿による平成 12 年度産学連携支援・若手研究者支援型研究開発のひとつとして、東京工業大学・三菱電機（株）と協力いただいた NTT コミュニケーションズ（株），（株）リコー，NTT データセキュリティ（株），日本電気（株）とから成るコンソーシアムで実施した「耐ウィルス機能を持った情報通信システム研究開発」の成果にモバイル機器の観点から考察を加えたものである。協力いただいた東京工業大学山谷泰賀氏，鈴木裕之氏，NTT コミュニケーションズ細谷英一氏，NTT データセキュリティ日比亨氏，日本電気藤岡伸男氏，三菱電機芝田晃氏 他の皆様に感謝いたします。

参考文献

[1] http://www.ipa.go.jp

[2] http://www.roxio.co.jp/goback/index.html

[3] 小尾高史，山口雅浩他，「耐ウィルス機能を持つユーザ情報保存システムの開発」電子情報通信学会２００１年総合大会情報・システム講演論文集１, D-9-6, 2001

[4] 山口雅浩，小尾高史他，「耐ウイルス機能を持った情報通信システム構築に関する研究開発」，通信・放送機構平成 12 年度成果報告書，2001