O-11

データ保護機能を有する電子保存システムの開発 (1)
-基本アーキテクチャ-
Development of Data Storage System for the Personal Data Protection (1)
-Basic Architecture-

青野正宏[*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] 佐藤能行[*4] 菅生清[*5] 藤岡伸男[*6] 大賀哲二[*7]
Masahiro Aono Takashi Obi Masahiro Yamaguchi Nagaaki Oyama Masuyoshi Yachida
Yasuhiro Hosoda Yoshiyuki Sato Kiyoshi Sugo Nobuo Fujioka Tetsuji Oga

1. まえがき

最近ようやく、データは紙による記録・保存よりも電子データとして記録・保存する情報のペーパレス化が進展しつつある。データを恒久保存する場合は、ＤＶＤ・ＣＤなどの外部記録媒体に保存されるであろうが、データを最も活用する「ホット」な段階では即座に読み出し・書き込みが可能な磁気ディスク上に保存するのが一般的である。しかし、読み書きが便利なため、逆に誤操作やサイバー攻撃によりデータを紛失する危険性も大きい。OSやプログラムなどは再インストールすることにより復元を行うことが可能であるが、ユーザが作成したデータや収集したデータを復元するのは容易でない。提案する電子保存システムは、このようなディスク上のデータ紛失に対する耐性を備え、データの保全・復旧を図る。本稿ではその基本アーキテクチャとその拡張について紹介する。

2．実現基本方式

主として対象とするのは、ネットワークに接続されている汎用的なパーソナルコンピュータ（以下、PCと略す。）である。データ保護の実現方式の基本は次のとおりである。ディスク上のファイルが更新・消去されるとき、更新・消去前のファイルのデータを更新履歴情報として、対象PCのディスクにあらかじめ割り付けられた領域、またはネットワーク上の専用保存装置に退避する。誤操作、ソフトウェアのバグ、悪意あるコンピュータウィルス（以下、ウィルスと略す。）などにより、ファイルが破壊されたとき、更新履歴情報からファイルの復元を図る。このようなファイルの保全方式は、単一PC上のソフトウェア[1]、ネットワークサービス[2]として実現されている。

しかし、従来の実現方式では、ファイル保全を行うソフトウェア自身に対するウィルス攻撃に対しては考慮がなされていない。例えば、GOBACK[1]においては、ユーザファイルと同時に退避領域もウィルスで破壊されれば、ファイル復元は不可能である。また、InternetDisk[2]においては、ウィルスがファイル保全ソフトウェアを乗っ取り、ネットワーク上に偽の更新履歴を送り出しておいてから、ファイルを破壊すれば、復元は不可能となる。

本電子保存システムは、特にウィルス対策を意識し、ウィルスが本提案方式の仕組みを理解し、攻撃を仕掛けてきてもファイル保全が可能な対策を備えている。ウィルスに侵される可能性はあるが、利便性を重視して外部から取り込んだプログラムの実行を許すサブシステムと外部から取り込んだプログラムの実行を許さず、データの保全とユーザに対して正しい情報を伝える機能を持つサブシステムのマルチ構成で実現する。サービス用OSとセキュリティ用OSを持つマルチOS[3]の考え方に類似している点はあるが、マルチOSはソフトウェアで実現するため、ウィルスがOSの機能も乗っ取る危険はなくならない。本システムは物理的にウィルスを隔離するため、ウィルスの危険性は大きく減少する。単一のPCとして実現するスタンドアロン型とネットワーク上でファイルの保全を行うネットワーク型の２つの方式があるが、本稿ではネットワーク型に限定して説明する。

3．システム構成

本電子保存システムは、ホスト装置、ユーザ装置、耐ウィルス保存装置（以下保存装置と略す。）の3種類のサブシステムから構成する。ホスト装置は対象とするPCからユーザインタフェース機能を取り除いたものである。利便性を優先して外部からプログラムを取り込むことを許すためウィルスに汚染される危険性を持つ。ホスト装置においてファイルの更新・削除が発生すれば、ネットワーク経由で更新データを保存装置に出力する。保存装置は、対象となるホスト装置のファイルのコピーとホスト装置から送られてきたファイル更新履歴を記憶する。この装置のソフトウェアは外部からプログラムを取り込むことは行わない。機能は限定されるがウィルスに汚染されることはない。複数台のホスト装置に１台の保存装置を対応させることも可能で

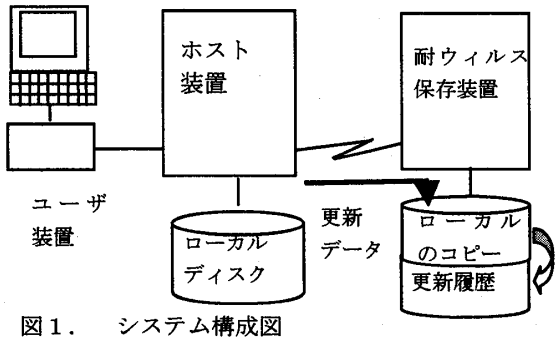

図１．　システム構成図

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

ある。ユーザ装置はホスト装置とユーザとの間にあって、モニター表示、キーボード入力などのユーザインタフェースを司る。この装置も外部プログラムの取り込みを行わないので、ウィルスに汚染されることはない。

4．更新履歴の退避と破壊からの回復

ホスト装置のファイルの書き込みはOSのファイル入出力命令を置き換える形で実現する。ホスト装置のローカルディスクに更新ファイルを書き込むと同時に更新データをネットワーク経由で保存装置に伝送する。保存装置は、送られてきた更新データから、ホスト装置のファイルのコピーを更新するとともに、更新前のファイルデータを退避して更新履歴を保存する。更新履歴の保存領域は有限であるため、更新履歴保存領域が不足すれば、更新履歴領域登録時刻または、ファイルの更新世代数などを条件にして優先順位の低い更新履歴から解放して、領域の余裕を作る。

ホスト装置へのファイル読み出しは、ホスト装置のローカルディスクから行い、保存装置は関与しない。

5．ウィルス攻撃と対策

ホスト装置がウィルスに侵された場合を想定する。ユーザがホスト装置のファイルが破壊されたことに気がつけば、ファイル保存装置のコピーファイルと更新履歴から任意の時点まで遡ってファイルの復元を行う。ウィルスは、コピーファイルと更新履歴を破壊することはできない。しかし、短期間に大容量のファイル更新を繰り返し行って保存装置の更新履歴領域を食い潰させ、しかる後、ユーザのファイルを破壊すれば、正常時のファイルの状態まで復元できない。この攻撃に対し、ファイル保存装置は、時間あたりの更新履歴量を監視し、一定量を超えれば保存装置からホスト装置を経由してユーザ装置に警告を送り、ユーザに正常か否かの確認を求める。ユーザが正常と判断すればファイル更新の許可をユーザ装置からホスト装置を経由して保存装置に返すが、異常と判断すればウィルスに汚染されていると判断し、システムを停止してウィルスの駆除を行う。

この警告と応答をホスト経由で行うため、ウィルスに乗っ取られたホスト装置は、ユーザ装置と保存装置間のメッセージ中継の妨害や改ざんを行う恐れがある。このため、警告と応答は暗号で行う。また、定期的にヘルシーメッセージを交換する。さらに、暗号文の内容を推定されないため、用いる暗号の鍵は毎回変化させるものとする。

次に考えられるウィルスの攻撃としては、保存装置に書き出す更新データの出力を妨害する。あるいは内容の改ざんを行うという手段が考えられる。ユーザには正常に動作していると思わせておいて、保存装置の機能を無効化し、その後ホスト装置のローカルディスクのファイルを破壊する。ユーザがファイル破壊に気がついて、保存装置から復元を図ろうとしても正しく復元できない。この対策として、ホスト装置のローカルディスクの内容と、保存装置にあるそのコピーの内容との一致の確認を行う。具体的方法は次のとおりである。ホスト装置は、ローカルディスクに記憶してあるファイル毎に一定の算式に則りハッシュ値を計算し、記録しておく。同様に保存装置も送られてきた更新ファイルのハッシュ値を計算しておく。ユーザ装置は定期的に、ホスト装置と保存装置に対し、ハッシュ値計算の要求を送る。要求を受けたホスト装置と保存装置はそれぞれ各ファイルのハッシュ値から総ハッシュ値を計算し、ユーザ装置に送る。保存装置からは、暗号化して送信するので、ホスト装置で内容の改ざんが行われる心配はない。ユーザ装置で両者のハッシュ値の一致を確認して保存装置が正しくホスト装置のファイルのコピーを保持していることを確認する。しかし、これだけであれば、次の抜け道も考えられる。ウィルスは保存装置に送り出した偽の更新データのハッシュ値を記憶しておく。ユーザ装置からハッシュ値計算の要求を受けたとき、ウィルスは、偽の更新データのハッシュ値から総ハッシュ値を計算して返す。この場合、両者からの総ハッシュ値が一致するため、ユーザ装置は異常を検出することはできない。従って、厳密には、定期的にウィルスに汚染されていないことが保証されている媒体からホスト装置を起動し、ファイルのハッシュ値を計算し、ユーザ装置に送る。ユーザ装置は保存装置にハッシュ値計算要求を行い、得られたハッシュ値結果を比較することで、両者のファイル内容の一致を確認する。この操作は自動的に行うことができず、オペレータの操作が必要となる。例えば、朝のホスト装置使用開始時にフロッピーディスクからチェックを行った後、OSの起動に進むなどの手順に進む方法が考えられる。なお、ホスト装置にローカルディスクを置かず、ファイルはすべて保存装置から読み出す方式をとれば、ファイルの読み出しに時間はかかるが、更新履歴を改ざんされる恐れはない。

6．電子保存システムの今後の拡張

ユーザがファイルの破壊に気がつけば復元を行うことは前記システムで可能であるが、特定のユーザファイルのみを破壊されている場合、気がつかないかもしれない。このため、ユーザファイルを更新消去する場合に保存装置から、ホスト装置とユーザ装置経由で、ユーザにファイル更新許可のコンファームを求める方法が考えられる。このとき、OSが求めるファイル消去などのコンファームと、二重に入力するのはユーザにとって煩わしい。OSからのコンファーム要求は削除できれば良い。

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.roxio.co.jp/products/goback3/index.html
[2] http://www.justsystem.co.jp/idisk500/toku_top.html
[3]佐々木他：マルチOS環境を利用したアクセス制御システムの実装と性能評価、情報処理学会研究報告、2001-CSEC-14、pp.157-163、2001年7月