O-12

データ保護機能を有する電子保存システムの開発（２）
-ネットワーク対応データ保存システムの試作と評価-
Development of Data Strage System for the Personal Data Protection(2)
- Trial Manufacture and Evaluation of Network Strage System-

小尾高史[*1]、山口雅浩[*1]、大山永昭[*1]、谷内田益義[*1]、細田泰弘[*2]
Takashi Obi, Masahiro YAMAGUCHI, Nagaaki OHYAMA, Masuyoshi YACHIDA, Yasuhiro HOSODA

菅生清[*3]、佐藤能行[*4]、藤岡伸男[*5]、青野正宏[*6]、大賀哲二[*7]
Kiyoshi SUGO, Yoshiyuki SATO, Nobuo FUJIOKA, Masahiro AONO, Tetsuji OHGA

１．まえがき

インターネットの普及に伴い、ネットワークを通じての不正アクセスやコンピュータウイルスの被害が頻発している。本研究では、このようなネットワークからの不正アクセスやコンピュータウイルスの攻撃から重要なデータおよびドキュメントを保護するため、ユーザデータなどの重要なデータが格納されている保存装置を高機能化し、保存装置に対して不正アクセスが及ばない環境、ウイルスが動作しない環境を実現することで、ユーザデータの保全・復旧を可能とするシステムを開発することを目的としている[1]。現在までに我々は、現在用いられているコンピュータ処理機能を、ディスクドライバ，コンソール入出力機能，コミュニケーション機能，外部命令実行機能、及び残る機能を有するメイン機能の５つに分割し、これらの機能を外部などからロードしたプログラムの実行を許可するフロントエンドプロセッサと、信頼できるプログラムのみを登録し外部からプログラムをロードすることは許可しないバックエンドプロセッサに分担させる方法の基本アーキテクチャについて検討を行った[2,3]。本発表では、その検討結果をもとに試作した、ユーザデータに対する破壊・不正消去、改ざん、不正参照などの脅威からデータを守るデータ保存システムの概要と評価について報告する。

２．開発システム概要

全体システム構成を図１に示す。試作システムを開発する際に作成したソフトウェアは大別するとユーザ装置に組み込むソフトウェア、ホスト装置に組み込むソフトウェア、ホスト装置とデータ保存装置との連携ソフトウェア、ユーザ装置・ホスト装置及びデータ保存装置間の通信を行うソフトウェア、データ保存装置に組み込むファイル管理ソフトウェアとなる。それぞれのソフトウェアの機能を以下に示す。

ユーザ装置に組み込むソフトウェアは、ホスト装置から画面情報を受信し、ホスト装置の画面をリアルタイムにユーザ装置上に表示する機能、また、ユーザ装置から入力された、マウス・キーボードイベントをホスト装置へ送信する機能を有する。試作システムにおいては、本機能の実装にあたっては、ＡＴ＆Ｔのケンブリッジ研究所から配布されているＶＮＣ（Virtual Network Computing）を改良し、ＩＣカードを利用して相互認証・暗号化通信を行う機能を付加している。また、ユーザ（利用者）からの、「同期化」、「復元」、「一致確認」の操作に対し、ホスト装置、あるいはホスト装置経由で保存装置とコマンドの送受信を行い、制御を行なう機能、及びシステムの正常動作を確認するために、ホスト装置、さらにはデータ保存装置とホスト装置経由でセキュア通信を行なう機能を有する。これら機能を用いて、ユーザ装置自身でシステムの正常性を判断したり、仮にホスト装置がウイルス等に汚染された場合でもユーザの判断を仰ぐことが可能になる。

ホスト装置には、ユーザ装置に画面情報をリアルタイムに送信し、マウス・キーボードイベントを受信する機能、ホスト装置で行われたファイル作成や変更、削除等の処理を保存装置に伝える機能、ユーザ装置の指示に従い、システム正常性を確認するためのプログラム、ユーザ装置と耐ウイルス保存装置との情報の交換中継を行なうプログラム、ファイル破壊時に復元を行なうためのプログラムなどの機能を有するソフトウェアがインストールされる。

ホスト装置とデータ保存装置との連携ソフトウェアとしては、ホスト装置側に保存装置へのファイル入出力処理を行う通信ソフトウェアを実装した。試作システムでは、ホスト装置上の任意のディレクトリを監視し、ファイル情報に変更があった場合に、保存装置にその内容を伝えるデバイスドライバ代替機能としての実装を行ったが、今後ＯＳレベルで発生したファイルＩＯ命令を取得し、ローカルハードディスクならびに保存装置へファイル書き込みを行なうデバイスドライバを作成する予定である。

データ保存装置には、ＬＡＮによって接続されたユーザ装置、ホスト装置、保存装置から成る全体のシステム内で、

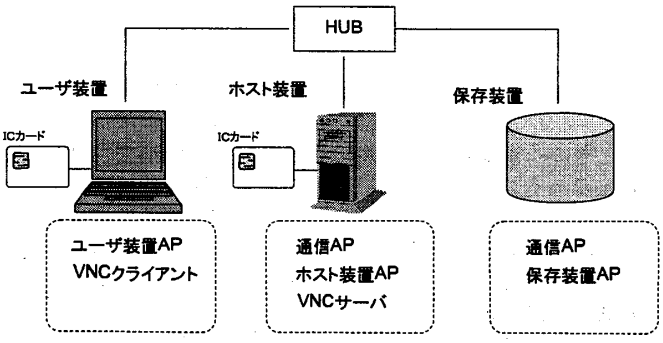

図１　データ保存試作システム構成図

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

ユーザのファイル操作・コマンド等によりホスト装置上のファイルを保存・復元するプログラムが実装される。ユーザ装置とデータ保存装置のプログラムはネットワーク経由で取り込んだ外部のプログラムが実行にされることはないため、ウイルス等がその上で実行されることはない。

最後に、各装置間での通信を行うソフトウェアを実装した。保存装置間の通信にて行わなければならないのは、ユーザデータの伝送であるが、これを確実に実現するためには、安全性の高い伝送プロトコルと障害処理機能が必要である。また、将来的に保存装置を広域ネットワーク上に配置することを考えると、電送路上での攻撃に対しても考慮する必要がある。試作システムでは、伝送路上での攻撃として盗聴や改竄等を想定し、これらに対抗するために、暗号化機能やメッセージダイジェストを用いた改竄検出機能を持つプロトコルの設計・実装を行った。また、ホスト装置と保存装置間のデータのバックアップに必要な情報交換を安全に行う機能、保存装置のインタフェースを透過的にホスト装置へ見せるための機能を有している。

3. 評価実験

まず今回試作したシステムにおいて耐ウイルス機能が動作することを確認するための実験を行った。試作システムでは、ファイルドライバではなく、デバイスドライバ代替機能としての実装を行ったため、実際のウイルスを用いた評価ではなく、実際のウイルスが行うファイル操作を実行するプログラムを作成し、擬似的にウイルス被害を被らせ、動作検証を行った。想定したウイルスの動作は、「ファイル削除」、「ファイル書き換え」、「ファイル新規作成」、「退避領域食いつぶし攻撃」、「通信時のパケットロス・改ざん」である。

まず、ファイル操作を行うウイルスに対しては、同期化処理によりファイルが保護されることが確認された。次に、今回のシステムを対象とする攻撃である退避領域食いつぶし攻撃が生じた場合、大量の書き込みが行われた後に同期化を行う場合は、更新頻度監視機能の設定値を超えた場合、その場で同期化が中断され、ユーザ装置へ警告が発せられる。しかしながら、更新頻度監視機能の設定値を超えない程度にファイルの保存を繰り返すウイルスが存在する場合には、ユーザ領域の食いつぶしが起こり、評価点が低いバックアップファイルが順次消去されてしまうという現象が生じた。これについては、今後評価点の計算方法等の改良やユーザへの警告を行う時期等を今後検討する必要がある。さらに、通信データの改ざん等については、一時的に装置間の通信が行えなくなることを確認した。

次に通常の使用時における試作システムの評価を行った。試作システムでは、ファイルのバックアップ時に、チェックポイント評価点によってファイル毎の重要度を評価している。しかし、設定内容によっては、ユーザ領域が飽和したときに、重要なファイルのバックアップが消去される可能性のあることが明らかになった。更新速度監視設定を厳しく設定することで、不本意な消去を防ぐことはできるが、頻繁に警告メッセージが送られてくると、ユーザの使い勝手が悪くなるため、セキュリティレベルに応じた環境設定方法の検討が必要になると考えられる。

また、耐ウイルス保存装置での同期化処理の保存と、通常の PC からのネットワークを介してファイルを保存するのに要する時間を比較すると、表１のようになる。通常のファイル保存と、非圧縮の場合の同期化処理とでは、ほぼ同程度の処理時間であり、圧縮を行った場合でも、圧縮アルゴリズムを適切に選べば、処理時間大きく増加することはない。今後、さらに同期化処理を高速化するためには、同期化処理の際にファイルをすべて保存装置側へ複製せずに、変更した差分セグメントのみを複製、圧縮する方式を導入し、移動や圧縮するファイル数を減らすこと等が必要となる。

表１　保存に要する処理時間の比較

	処理時間
耐ウイルス保存装置による同期化処理（ＬＨＡ）	約２分 10 秒
耐ウイルス保存装置による同期化処理（ＺＩＰ）	約１分 50 秒
耐ウイルス保存装置による同期化処理（非圧縮）	約１分 40 秒
通常の保存	約１分 40 秒

4. まとめ

コンピュータウイルスなどの攻撃から重要なユーザデータを保護するため、保存装置を高機能化して、コンピュータウイルスが動作しない環境を実現することで、ユーザデータの保全・復旧を可能とする方法を提案し、データ保存システムの試作を行った。また、試作システムを用いた評価実験を行い、開発したシステムが、各種のコンピュータウイルスや不正アクセスからユーザデータを保護できることを確認し、提案方法の基本原理を確立した。今後の課題としては、今回の試作システムでは実装していなかった更新セグメント単位でのバックアップの実装やインターネット経由でのデータ保存装置の利用などが挙げられる。また、保存装置機能の小型化などを行い、個人が簡単に使える実用システムの開発へ向けて研究開発を継続する予定である。

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] 小尾高史 他、”耐ウイ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
[2]「平成 12 年度　産学連携支援・若手研究者支援型研究開発成果報告書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」 平成 13 年 5 月 通信・放送機構
[3]青野正宏 他、”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-、”FIT2002, 2002