アクセスモニタとファイルバックアップの統合による自己修復機構の設計

打田 悟志† 西山 裕之† 大和田 勇人†

†東京理科大学大学院理工学研究科

1 はじめに

コンピュータの普及やストレージの大容量化に伴い個人が扱うデータが増加する傾向にある．それに伴い，コンピュータウィルスに感染した際のデータの改ざんやユーザ自身の誤操作によるファイルの消失のリスクが高まっている．

そのようなリスクを回避するためには，バックアップソフトを使うことが有効である．Mac OS X Leopard に搭載された自動バックアップ機能 Time Machine[1] は，ファイルやフォルダを世代別にバックアップできる．保存された内容は Time Machine ブラウザで閲覧することができ，指定した日や時刻の状態に丸ごと戻したり特定のファイルを検索して呼び出したりすることができる．このような機能により，ファイルの改ざんや消失が起こった時間が分かればファイルを復元する事が可能となるが，ユーザ自身がウィルスによる改ざんの詳細を把握する必要がある．

ウィルスへの対策にはセキュリティソフトが最も有効である．しかし，一般的なルールベースのセキュリティソフトではルールの更新が間に合わず，新種のウィルスが 1 週間以上放置される危険性もある．この場合，ルールが更新されてもウィルスによる被害を完全に復元することは困難である．未知のウィルスに対しては Zhang らの研究 [2] のように，既知のウィルスのコードを基に類似点を検索し亜種を探す方法等があるが完全に検知することはできず，被害の復元もできない．

本研究では未知のウィルス等に感染した場合でも，コンピュータ内部のファイルの改ざんから自動復元できるソフトウェアの実装を目的とする．その手段としてコンピュータ内部の動きを監視することでファイルの更新を検知し，安全なプロセスに更新されたファイルはバックアップを作成し，悪意のあるプロセスに更新された場合は自動的に復元する．未知のウィルスにファイルを改ざんされた場合でも段階的にバックアップを行うことで，ウィルスと認識した時点で改ざんされたファイルを復元する．

2 自己修復システム

2.1 システム設計

本システムは，改ざんからの自動復元を行うためにリアルタイムバックアップと，ファイルを更新したプロセスのモニタリングを統合する．これにより必要となる機能を表 1 に示す．

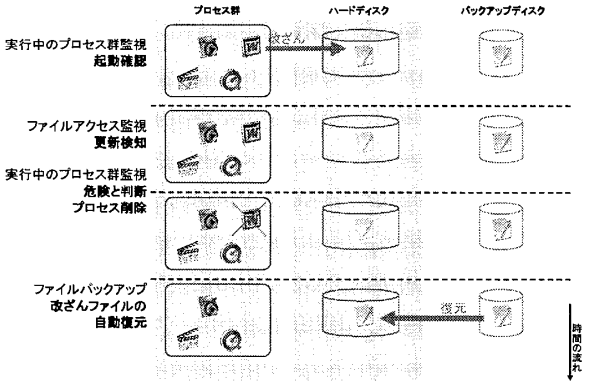

図 1: 悪意のあるプロセスによる改ざんからの自動復元

「プロセスの起動確認機能」がコンピュータ内部のプロセスの動きを,「ファイルアクセス検知機能」がファイルのアクセスを動的にモニタリングする.「ファイルアクセス検知機能」によるファイル更新の情報を基に「リスト管理機能」を呼び出しプロセスが安全かの確認を行う．安全なプロセスによる更新の場合は，ファイルも安全と判断して「ファイルバックアップ機能」により逐次バックアップを作成する．悪意のあるプロセスによる改ざんを確認した場合，図 1 のように「プロセス削除機能」により，実行されたプロセスの排除を行い，改ざんされたファイルのみを「自動復元機能」によりバックアップから復元する．

リストに登録されていない未知のプロセスを検知した場合，一時的にバックアップの作成を行う．その後，悪意があるプロセスであると判明した段階で，改ざんされた危険性があると判断し,「自動復元機能」により改ざんされたファイルのみを未知のプロセスによる更新前の状態に復元する．

表 1: 本システムの機能一覧

実行中のプロセス群監視機能	プロセスの起動確認機能 リスト管理機能 プロセス削除機能
ファイルアクセス監視機能	ファイルアクセス検知機能 アクセス情報のフィルタリング機能
ファイルバックアップ機能	自動バックアップ機能 自動復元機能

the Self-Repair System by Integrated Access Monitoring and File BackUp Function
Satoshi Uchita†, Hiroyuki Nishiyama†, Hayato Ohwada†
{†Graduate School of Science and Technology, Tokyo University of Science}

2.2 実行中のプロセス群監視機能

プロセスの識別のために，実行ファイルから一意に求まるハッシュ値 MD5 を用いてホワイトリスト・ブラックリストの作成，管理を行う．本システムでは実行中のプロセスの ID と実行フィルのフルパスを定期的に取得することでプロセスの起動を確認する．ブラックリストに登録されたプロセスを検出した場合，「プロセス削除機能」により該当プロセスを停止し，実行ファイルとその関連ファイルを削除する．リストに登録されていないプロセスを検出した場合，ファイルへのアクセスを行わない限り危険はないと判断し，次に示す「ファイルアクセス監視機能」の監視対象とした上で起動を許可する．

2.3 ファイルアクセス監視機能能

本機能はファイルアクセスを監視し，アクセスしたプロセス，アクセスされたファイル，アクセスの種類等の情報を取得する．取得した情報に対してアクセスの種類に応じてフィルタリングを行う．ファイル更新が行われた場合，プロセスが安全かを「実行中のプロセス監視機能」に問い合わせ，その結果に応じた動作を「ファイルバックアップ機能」が行う．

2.4 ファイルバックアップ機能

プロセスによるファイルの更新が行われた場合，「ファイルアクセス監視機能能」から情報を受け取り以下に記す 3 種類の処理を行う．

2.4.1 安全な場合

更新を与えたプロセスが安全な場合，「自動バックアップ機能」により，更新ファイルのバックアップを元のディレクトリ構造を維持して作成する．バックアップファイル名は，バックアップを作成した時刻を用いることで管理する．この際，更新を与えたプロセスの実行ファイルの MD5 と，バックアップファイルをログに書き込むことで，安全と判断したプロセスが後に危険と判明した場合はバックアップファイルを削除し，バックアップファイルを安全な状態に保つ．

2.4.2 既知の脅威の場合

「実行中のプロセス群監視ツール」に検知される前に悪意のあるプロセスによる更新が与えられた場合，「自動復元機能」により，プロセスの強制終了と実行ファイルの削除を行う．その後，更新されたファイルを削除し，バックアップファイルから復元する．

2.4.3 未知の脅威の場合

リストに登録されていないプロセスの場合，管理者が判断を行うまでは更新は一時的にバックアップを作成して指示を仰ぐ．更新を与えたプロセスの MD5 と，更新されたファイルをログに保存することで，管理者が危険と判断した場合即座に「自動復元機能」により復元を行い，このプロセスによって作成されたバックアップファイルを削除する．本機能により，未知の脅威によるファイルの改ざんが行われた場合でも，気づいた時点で改ざんされたファイルのみを元の状態に復元することが可能である．

3 実証実験

3.1 実験環境

Windows OS 環境内でホワイトリストに 30 件のプロセスを登録した上で実証実験を行った．悪意のあるプロセスとして Winny を媒介とする Antinny[4] と USB メモリ等を媒介とする qvimi.exe[5] を使用した．動作を検証するために，ホワイトリストに登録したメモ帳による更新を行った場合，ブラックリストに登録した qvimi.exe が実行された場合，リストに登録していない Antinny が実行された場合の動作を検証した．

3.2 実証実験

・ホワイトリストに登録したプロセス Windows 標準のメモ帳を用いてテキストファイルの編集を行い，正常にバックアップされることを確認した．
・ブラックリストに登録したプロセス qvimi.exe を起動した際の動作を追跡した．C ドライブ直下に複製された qvimi.exe 本体とシステムファイル内に作成された mmvo0.exe，mmvo1.dll，juy.dll，IMM32.dll 等のウィルスファイルが削除された．
・未登録のプロセス Antinny を未登録の状態で起動させた後，ブラックリストに指定した際の動作を追跡した．未登録の状態では，Antinny が改ざんした win.ini や UpFolder.txt 等のバックアップが作成された．その後，管理者がブラックリストに指定することにより，Antinny によって改ざんされたファイルやそのバックアップを削除し，改ざん前の状態に復元されることを確認した．

以上より本システムを用いることでウィルス等による改ざんが起きても，通常のバックアップソフトのように全てのファイルを巻き戻す必要がなく，また Time Machine のようにユーザが復元するファイルを手動で選択する必要なしに，改ざんされたファイルのみを改ざん前の状態に戻すことが可能である．

4 おわりに

本研究では，アクセスモニタとリアルタイムバックアップの統合による自己修復システムの設計を行った．本システムを利用することで，未知のウィルスに感染した場合でもユーザが気づいた段階で改ざんされたファイルのみ復元することが可能である．実証事件によりシステムの有効性を示した．

参考文献

[1] “アップル Time Machine” http://www.apple.com/jp/macosx/features/timemachine.html

[2] Vyas Sekar et al.“A Multi-Resolution Approach forWorm Detection and Containment”, Proceedings of the 2006 International Conference on Dependable Systems and Networks (DSN 2006), pp.189-198, 2006

[3] Mark E. Russinovich et al.“Microsoft Windows Internals (4th Edition): Microsoft Windows Server 2003, Windows XP, and Windows 2000”, Microsoft Press, 2005

[4] “Symantec Antinny” http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.hllw.antinny.html

[5] “Trend Micro WORM_ AUTORUN.CEZ” http://www.trendmicro.co.jp/Vinfo/virusencyclo/default5.asp?VName=WORM_ AUTORUN.CEZ& VSect=P