特定データの保護を目的とした ファイルアクセス監視システムの設計と実装

打田 悟志† 西山 裕之†† 溝口 文雄††

† 東京理科大学大学院理工学研究科

†† 東京理科大学理工学部

1 はじめに

近年，パーソナルコンピュータの普及や高速なネットワークインフラの整備により，コンピュータがインターネットに常時接続されている環境が一般的なものとなった．しかし，それに伴いコンピュータウイルスや不正侵入による個人情報の漏洩やデータの改ざんといった被害が増加している．SELinux(Security-Enhanced Linux)[1] はカーネルレベルでプロセスごとのアクセス制御が可能な Linux 上で動作するセキュア OS である．SELinux は強制アクセス制御 (MAC)，リソース (プロセス，ファイル，ソケット) ごとのアクセス制御 (TE)，root を含む全てのユーザに対するプロセス制御 (RBAC) によりセキュリティの高いシステムの構築を目的としている．しかし，情報漏洩やデータの改ざん等が行われた際，その追跡や復元が困難という問題がある．

そこで本研究では，コンピュータウイルス等からコンピュータおよび内部のファイル（実行ファイル，データファイル等）を保護することを目的とする．具体的には，コンピュータ内部のプロセス（アプリケーション）の動きやファイルアクセスを動的に監視することにより，不正なプロセスによる機密ファイルの移動の追跡，リアルタイムバックアップによるデータの保護を行う．

2 アクセス監視システム

2.1 システム設計

本研究はコンピュータ内を動的にモニタリングし，ファイルにアクセスしたプロセスごとにファイル管理を行う．本研究では不正なプロセスによるファイルの読み込みを検出し，個人情報等の機密ファイルのハードディスク内での移動及び，ネットワークを介した移動を追跡する．これにより情報漏洩の検知，防止とネットワークを介して外部に流れた際の迅速な追跡ができる．

Design and Implementation of the File Backup System using Dynamic Monitoring

Satoshi Uchita†, Hiroyuki Nishiyama††, Humio Mizoguchi††

{†Graduate School of Science and Technology, Tokyo University of Science, ††Department of Science and Technology, Tokyo University of Science}

*既存のデバイスドライバの前後に入り，通過する情報を収集したり，ドライバの動作を変更する中間ドライバ

更にファイルの更新時に，安全なプロセスによる更新はバックアップを作成，不正なプロセスによる更新はプロセスの除去及びバックアップからの自動復元を行う．この自動バックアップシステムにより，不正なプロセスによるデータの改ざんや破壊を自己修復することができる．

具体的には本システムを起動する際，コンピュータ内のファイルアクセス情報を取得するファイルアクセス監視エージェントを生成する．取得した情報から新たに，アクセスしたプロセスを確認するためのプロセス監視エージェントを生成する．

ファイルの読み込みを検知した際，プロセスを不正と判断した場合はプロセスを除去する．この際，除去したプロセスやその子プロセスがハードディスク内へのファイルの書き出しやネットワークへの接続を行っていないか確認することで，機密情報の漏洩の危険性をユーザに報告する．

ファイルの更新を検知した際，プロセス監視エージェントがプロセスを安全と判断した場合は，更新されたファイルも安全と判断してバックアップを作成する．ここで不正と判断した場合，更新されたファイルも同様に危険な可能性が高いと判断して削除する．その後，予め作成したバックアップファイルから復元を行う．この事後承諾システムによって，悪意のあるアプリケーションやユーザの誤操作によって，重要なファイルや本来安全であるアプリケーション本体とその設定ファイルが改ざんされるといった障害が発生しても半自動的に修復可能である．

ここで参照するホワイトリスト，ブラックリストは複数のユーザで共有することによって，グループ内で共通のセキュリティポリシーを策定可能である．ここで，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，管理者に通知し判断を仰ぐ．管理者が不在の際はユーザが一時的に安全か危険かを判断し，後に管理者に問い合わせることで処理を行う．ここまで述べたシステムの概要を図 1 に示す．

2.2 ファイルのアクセス監視

本システムは任意のファイルにアクセスしたプロセスとその種類（新規作成・書き込み・読み込み等），アクセスした時間等の情報を取得するために，Filemon[2] のフィルタドライバ* を利用する．フィルタドライバから情報を取得すると，プロセスと実行ファイルのフルパスをもとに「プロセス監視エージェント」にアク

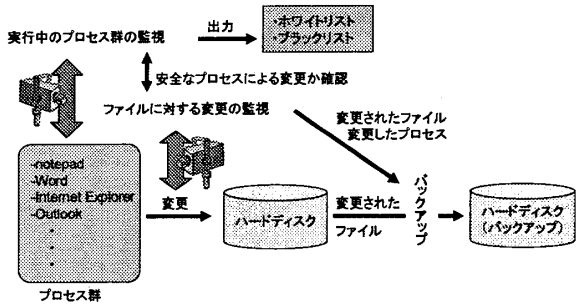

図 1: システムの概要

セスしたプロセスがホワイトリストに登録されているか，ブラックリストに登録されているかの確認を行う．その後，取得した情報を必要に応じて読み込みの際は「プロセス追跡エージェント」，ファイルの更新の際は「ファイルバックアップエージェント」に受け渡す．

2.3 実行中のプロセス監視

本システムは，プロセスの安全性を確認する際に，実行ファイルから一意に求まるハッシュ値 MD5 によるリストを用いる．

実行中のプロセス群を監視するには，新たに起動したプロセスを検知する必要がある．そこで，本システムは実行中のプロセス ID，実行ファイルのフルパスを取得するモジュールを定期的に呼び出すことで新たに起動したプロセスを確認する．プロセス ID と実行ファイルのフルパスを取得した後，フルパスからハッシュを生成しブラックリストを確認する．ブラックリストに登録されている場合，外部コマンドを実行することによって，プロセスの強制終了を行う．登録されていない場合は，通常の起動を許可する．

また，「ファイルアクセス監視エージェント」からプロセスが安全か問い合わせを受けた際，実行ファイルのフルパスからハッシュ値を生成し，ホワイトリスト，ブラックリストを参照し，登録されているかを返す．

2.4 プロセスの追跡

「ファイルアクセス監視エージェント」から得たファイルの読み込み情報を元に以下に示す処理を行う．不正なプロセスが指定した機密情報を読み込んだ際プロセスを除去する．その後，情報漏洩の危険がある子プロセスの起動，ハードディスク内へのファイルの書き出し及びネットワークへの接続を確認する．ハードディスク内へファイルの書き出しが行われた場合，「ファイルバックアップエージェント」と連携することで書き出されたファイルの除去もしくは復元を行う．ネットワークへの接続を確認した場合，即座にユーザに報告し追跡することにより，情報が漏洩した場合でも迅速な処置を行うことができる．子プロセスが起動されている場合，プロセスがホワイトリストに登録されている場合でもユーザに確認を行い，必要に応じてプロセスの排除を行う．ファイルの読み込みを行ったプロセスがリストに未登録の場合，読み込んだファイルに関連付けられたプロセスを確認し，異なる場合はユーザに警告する．

†不正なプロセスのルールは予め登録されているものとする

2.5 ファイルバックアップ

「ファイルアクセス監視エージェント」から得た情報をもとに以下に記す処理を行う．更新を与えたプロセスが安全な場合バックアップを作成する．

更新を与えたプロセスが不正な場合プロセスを除去し，予め作成された安全という保障があるバックアップファイルから復元を行い，更新されたファイルを解除する．バックアップファイルが複数ある場合は最も新しいファイルから復元を行う．この自動修復により，不正プロセスによるファイルの改ざんが起きた場合でも，コンピュータ内部の情報を保護する．

3 実証実験

本研究の有効性を示すために実証実験を行った．実験には WindowsXP を OS とする本システムを組み込んだ実験用端末を用意し，端末上でファイルへの読み書きと FTP によるネットワークを介したファイルの移動を確認した．

不正なプロセス† が新しいファイルを生成したり，既存のファイルを改ざんしたりした事を確認した際，プロセスを排除した後生成したファイル群を削除し，改ざんされたファイルを改ざん前の状態に復元することに成功した．

ユーザが指定したファイルを読み込んだプロセスが FTP によるファイルの送信を行った際，ファイルの送信を検知して送信先の IP アドレスの特定に成功した．これにより，万一機密情報が漏洩した場合でも迅速な追跡が可能である．

4 おわりに

本研究では，コンピュータの内部情報の監視による情報漏洩の検出と，リアルタイムバックアップを連動した総合セキュリティシステムの設計，実装を行った．実験により不正なプロセスに改ざんされたファイルの自動修復と，ネットワークを介した情報漏洩の追跡が出来ることを確認し，本システムにより安全なコンピュータ環境を構築することが可能であることを示した．また，免疫系ネットワークセキュリティ[3] と融合することにより，ローカルなマシン内部，ネットワーク双方が安全な環境が構築可能となる．

参考文献

[1] P. Loscocco and S. Smalley, "*Integrating Flexible Support for Security Policies into the Linux Operating System*", Proceedings of the FREENIX Track of the 2001 USENIX Annual Technical Conference, 2001

[2] ディビット ソロモン (著), マーク ルシノビッチ (著), David A. Solomon (原著), Mark E. Russinovich (原著), 豊田 孝 (翻訳) "インサイド Microsoft Windows 第 4 版 下", 日経 BP ソフトプレス, 2005

[3] 溝口文雄, 西山裕之, "免疫系によるネットワークセキュリティ", コンピュータソフトウエア, Vol.20, No.3, pp.88-94, 2003