J-043

ファイル位置と時間軸に着目したファイル変更管理情報の視覚化
Visualization of File System Integrity Based on File Location and Temporal Axis

中村　勲†　　奥野　拓‡
Isao Nakamura　　Taku Okuno

1　背景と目的

コンピュータに対する攻撃が発生し，コンピュータ内部に侵入された場合に調査を行う際は，異常発見が遅れるほど被害が増大するため迅速な対応が求められる．そのような状況でコンピュータ内にあるファイルが固有に保持しているファイル名やファイルサイズ，最終更新日などの変更状況を監視することで異常の検出を行う手法があるが，現状のテキストベースの調査法では変更されたファイル数が多くなると調査が困難になるという問題がある．

そこで本研究ではファイルの変更結果を視覚化することで不正侵入の発見を容易にすることを目的とする．この目的を達成するためにファイル同士の位置関係と時間軸に着目し，ファイル間の関連性を視覚化することで調査者の手間を軽減する

2. 関連研究

2.1　コンピュータセキュリティ

コンピュータに対する不正侵入への対策としては，接続元の制限やファイアウォール，IDS の設置などを行うことで外部からの攻撃を防止するのが有効である[1]．しかし，外部からの攻撃を全て防ぐことは非常に困難であり，内部からの攻撃の可能性も考えられるため，侵入に対する防御を強化するだけでは不十分である．そのため，実際に被害が発生した場合の事後対策も必要となる．そのような事後対策から収集した情報の法的な利用までを行うコンピュータフォレンジック[2]という分野がある．コンピュータフォレンジックでは，まず被害が発生した場合に行う初期対応であるインシデントレスポンスの作業が重要となる[3]．そのような作業は，被害の把握から範囲特定までをファイルの変更情報を監視することで行える．

2.2　ファイル変更管理システム

ファイルの変更状況を監視することで意図せぬファイルの変更を発見し，不正侵入を検出することを目的としたファイル変更管理システムというものがある．ファイル変更管理システムを用いることにより，ファイルの属性がどのように変化したのかがわかり，コンピュータの調査者はその情報を参考にして，変更が意図して行われたものかどうかを実際に判別することで疑わしい変更を発見することができる．

ファイル変更管理システムには様々なものがあるが，例えばオープンソースソフトウェアの Tripwire[4]では以下のようにファイルの変更を検出する．

1.各ファイルのファイル名，ファイルサイズや最終更新日，ハッシュ値などの属性をデータベースに記録する（図 1 参照）．
2.記録したそれらの情報を以前記録した情報と比較することで，ファイルが変更，追加，削除されたことを検出する．
3.その検出結果を人の目で確認することで，その結果が正当なものかどうかを判断する

現状のファイル変更管理システムの問題点としては，最終的なファイルの変更結果がテキストで出力されるため，確認作業のコストが高いことが挙げられる．基本的にはコンピュータ内の全てのファイルを管理対象にするため，場合によっては出力されるテキスト量が膨大となる．また，予期せぬファイル変更はシステムのどの部分においても発生する可能性があるため，データのフィルタリングをする場合には環境に応じた細かな設定が必要となり，その作業自体もコストが高い．

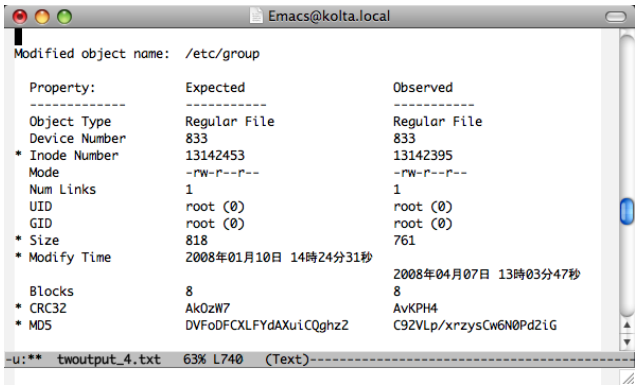

図 1　Tripwire によるファイルの変更履歴

2.3　情報視覚化

情報視覚化では視覚化する対象と目的によって様々な手法[5]が存在するため，着目する要素については慎重に検討する必要がある．本研究ではファイルの変更情報が記載されたテキスト情報を 2 つの要素に着目し視覚化することで，コンピュータ調査者の情報の理解度を向上させる．

3. 提案手法

本研究ではファイル同士の位置関係と時間軸に着目し，ファイル間の関連性を視覚化することにより容易に不正

†公立はこだて未来大学　システム情報科学研究科
‡公立はこだて未来大学　システム情報科学部

侵入調査を行うことを目的とする．以下に着目する情報の詳細を示す．

3.1 ファイルの位置関係に着目した調査

変更があったファイルの位置関係を視覚化することによって，コンピュータの調査者がファイル間の関連性を発見するための補助的な情報とすることができる．同ディレクトリや根が同じディレクトリには同じソフトウェアの設定ファイルや利用方法が似たファイルが存在する可能性がある．ファイルの位置関係を視覚化することで，調査者がそういった関連性を直感的に把握できるようになる．

ファイルの位置関係に着目した場合の視覚化例を図１に示す．図１では各ファイルとディレクトリをツリー上に配置しており，各ファイルがどのディレクトリにあり，どのようなファイルと近い位置関係にあるのかが容易に判別できる．

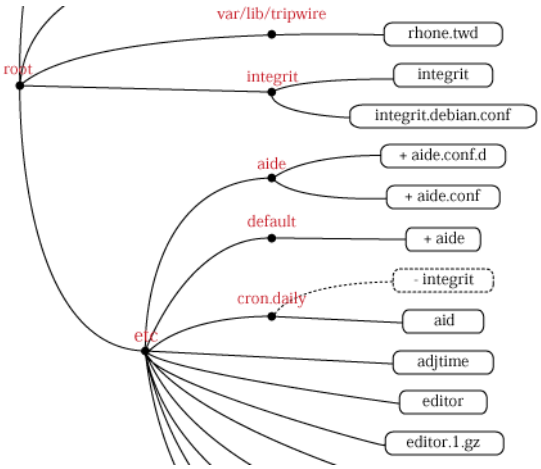

図２ ファイルの位置関係に着目した視覚化例

3.2 時間軸に着目した調査

ファイルの変更時間を視覚化することで，調査者の作業記憶と結びつけ，その時間帯の作業内容を想起することができる．例えば変更時間がほぼ同じファイルが複数あった場合にはソフトウェアのインストール作業の際などに生成された関連したファイル，変更時間が近いファイルは同一人物が行った作業の可能性がある．他にも普段作業を行わない時間にファイル変更があった場合には不正侵入による攻撃である可能性があるため，得られた情報を調査指針として対象ファイルを調査することができる．

他にも，ファイルが定期的に変更される場合にはコンピュータ内でどのようなサービスが動いているのかを知ることができる．

時間軸に着目し，変更時間が近いファイルを対象ファイルの周囲に表示した場合の視覚化例を図２に示す．図２では調査対象のファイル名をクリックすると，その周りに対象ファイルが変更されてから近い時間に変更があったファイルを同心円状に配置し，類似した時間帯に変更があったファイルが判別可能となる．

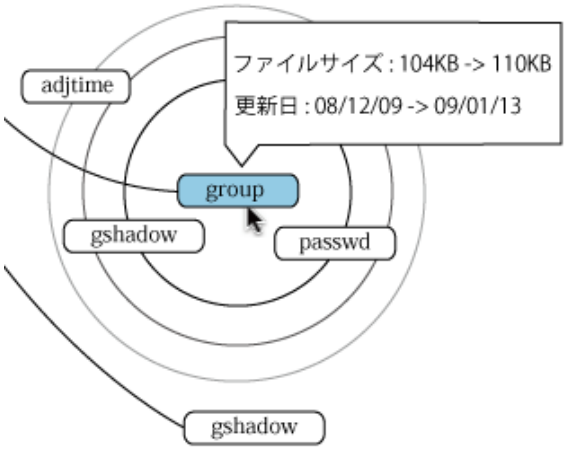

図３ 時間軸に着目した視覚化例

4 考察

ファイル変更管理システムを用いて不正侵入を検出する場合には外部からの侵入に対する防御を強化するだけでは検出できないようなものを対象としており，自動検出は困難であるため，最終的には人の目による確認作業が必要となる．

本研究では時間軸とファイルの位置関係の２点を着目要素として視覚化を行ったが，この方式の利点としては，コンピュータ調査者がファイルの変更内容を把握できる規模のコンピュータを調査する場合には，過去の作業記憶と結びつけることができるため，本研究のシステムは有用となる．しかし，企業などで用いるような大規模システムの場合には多数の変更が発生するため，さらにマクロな視点からの視覚化が必要となる．

本研究で考案したシステムの評価に関してはシステムの時間軸とファイルの位置関係に着目した場合について実験を行うことで効果を明らかにする．また，視覚化については様々な方法が考えられるため，その他の視覚化方法についても検討を行う予定である．評価実験は不正侵入されたと仮定した場合の仮想シナリオを用意し，関連性のあるファイルの発見率を測定することで行う．

参考文献

[1] Michael D. Bauer, Building Secure Servers With Linux, Oreilly & Associates Inc, 2002.
[2] K. Warren and H. Jay, Computer Forensics Incident Response Essentials, Addison-Wesley, 2001.
[3] M. Kevin and P. Chris, Incident Response Investigating Computer Crime, McGraw-Hill Companies, 2002.
[4] K. Gene and S. Eugene, Experiences with Tripwire, Using Integrity Checkers for Intrusion Detection: Computer and Communications Security, 1994.
[5] Edward R. Tufte, Envisioning Information: Graphics Pr, 1990.