痕跡に注目したログ収集機能の検討

6G－4

田口 篤[1]，女部田 武史[2]，浅香 緑[1]
情報処理振興事業協会セキュリティセンター[1]，(株)日本総合研究所セキュリティ事業推進部[2]

1. はじめに

不正侵入の結果，システムログに記録される様々な事象を一般に侵入の痕跡と呼ぶ．システムの管理者はこれらの痕跡を発見すると，更に情報収集，情報分析を行い最終的に侵入かどうかの判断を下す．そういった意味では，痕跡とは，侵入に繋がる可能性のある事象，侵入検出の初動となる事象，と捉えることもできる．現在，侵入検出システムにはAIDとMIDという2つの方式がある．それぞれ，AID方式はシステムへ負荷がかかり，MID方式は未知の不正アクセスには対応できないという欠点を持つ．痕跡検出を初動とした侵入検出システムは，これらの欠点を解消してくれるのではないかと期待している．本研究ではまず痕跡検出ツールを作成した．作成に先立ち，

・効果的な痕跡を検出するための収集するログの種類の検討
・収集したログから痕跡を抽出するためのフィルタリングルールの検討

を行った．本稿ではこれらの検討に関する報告を行う．

2. 痕跡の定義

痕跡とは，システムに残された侵入に繋がる可能性のある事象である．理想的な痕跡検出の条件とは，

・不正侵入に繋がる事象は痕跡として検出できる．
・不正侵入と関係のない事象は極力痕跡として検出しない．
・リアルタイムで検出できる．
・システムへの負荷は極力抑制される．

等が挙げられる．おそらく，大方のシステムログに痕跡は含まれているであろう．しかし，痕跡検出のために利用する情報は多ければ多いほどその精度も増すが，同時にシステムにかかる負荷も増大する．痕跡検出に用いるログは必要にして最小であることが望ましい．本研究では次の2種類のログから痕跡を抽出することを試みた．

・ファイルのread,writeに関するログ

侵入者の最終目的はシステム上，あるいは組織上重要な情報を記述したファイルの入手や改竄であることがほとんどである．そのためファイルアクセスに関するログの利用の検討を行った．

・ルートプロセスに関するログ

侵入者はその最終目的を達成するために，まずはシステムの特権ユーザモードを不正に入手しようとす

A Study of How to Find Marks of Intrusion from System Logs

Atsushi Taguchi[1], Takefumi Onabuta[2], Midori Asaka[1]
Information Technology Promotion Agency[1], The Japan Research Institute, Limited[2]
Bunkyo Green Court Center Office. 2-28-8, Honkomagome. Bunkyo-ku. Tokyo 113-6591.Japan

る．そのため特権ユーザのプロセスに関するログの利用の検討を行った．

3. 実装及び実験環境

今回は以下の環境で実装及び実験を行った．

機種： Sun Ultra10, Sun 4/10

OS ： Solaris2.5.1

ログ収集機能： SunSHIELD Basic Security Module

言語： Perl5.004

4. 実験方法

本研究ではログの収集機能に SunSHIELD Basic Security Module（以下 BSM）を使用した．これは，

・今回プラットフォームに指定した Solaris2.5.1 では OS のソースの提供が行われていない．

・ BSM はユーザ単位，システムコール単位で詳細なログを収集することができる．

・ BSM は Solaris の標準モジュールである．

といった理由からである．

4-1. ファイルの read,write に関するログ

open(read モード),create,ulink システムコールのログを収集した．このログを収集しながら，実際にシステムを使用し，その際のログを監視することによってフィルタリングルールの検討を行った．

4-2.ルートプロセスに関するログ

fork,fork1,execve システムコールのログを収集した．このログを収集しながら，複数の不正アクセスを実行し，その際のログを監視することによってフィルタリングルールの検討を行った．

5. 実験結果

5-1.ファイルの read,write に関するログ

open(read モード)はかなり余分なログまで記録する（ライブラリ等のバイナリファイルなど）．そこでフィルタリングルールは，ファイルの read に関してはこちら側で監視したいファイル名を指定，ファイルの作成と削除に関しては全てのログを痕跡として設定した．

5-2.ルートプロセスに関するログ

不正アクセスの手口を調査すると，そのほとんどが setuid されたコマンドを悪用したものであった．そこでフィルタリングルールは，所有者がルートで且つ setuid されたコマンドが実行された場合のログを全て痕跡として設定した．

6. 考察

ファイルの read,write に関するログ，及びルートプロセスに関するログはいずれも痕跡検出には有効であることが確認された．今回作成したツールだけでも，システム管理者のログ監視作業の軽減等それ相応に役立つと思われる．侵入検出システムで最も負荷の高い処理はログ解析だと考えられている．そこで，初めに痕跡を検出しておくことで，その後に更に続くログ解析作業に方向性を持たせ，制限できればその分負荷が軽減されるのではないかと考えている．また痕跡を初動とする侵入検出方法であれば未知の手口に対しても検出できる可能性があると思われる．今後，今回検出した痕跡を利用した侵入検出システムの作成を行っていく予定である．