コンピュータセキュリティ　1－9
（1998．5．29）

不正アクセスを考慮したシステムログ収集機能について

高田　寛　　佐野 晋
NECネットワーキング技術研究所

概要

コンピュータネットワークの普及にともない，ネットワークを介したシステム侵入・破壊などの犯罪も増えてきている．これに対しシステム管理者はファイアウォールの構築や各々のコンピュータのセキュリティ向上に努めている．しかしながら，現在ファイアウォールを構築するホストとして数多く使われているUNIXホストが通常有しているシステムログ機構は，侵入を受けた場合に侵入を検出したり，侵入元を特定するためには不十分である．また，侵入者がシステムの特権を得た場合には侵入した痕跡を残さないようにログを消去してしまう場合が多いため，侵入が判明した場合の解析が困難になるという問題もある．我々は実際に攻撃されたり侵入を受けた場合に役に立つシステムログ情報を記録するための機構を考案，実装を行なった．

The New Logging Feature Against Attackers for UNIX Systems.

Hiroshi TAKADA　　Susumu SANO
NEC Networking Systems Laboratories

Abstract

As computer networks are becoming utilized more widely, crimes such as breaking into or destroying computer systems are increasing. However, normal logging features implemented in many UNIX systems, which is widely utilized platform for fire wall servers, are insufficient. With normal logging feature. It is hard to detect an attack or to specify who the attaker is and how he is attacking. Besides, if attackers obtained root privilege, they often delete those logs to wipe away marks of their deed. In this case, it get even more difficult to analyze the intrusion when detected. This paper presents a new logging feature to be implemented on 'BSD' UNIX systems. Using this implementation, we'll be getting necessary data to analyze and intruders cannot delete log records. It will help you to analyze the attack.

1　はじめに

インターネットに代表されるような，広域コンピュータネットワークの発達，普及に伴い，ネットワークを悪用し，コンピュータシステムへの侵入やデータの破壊などの不正行為を行なう者（以下 侵入者）も増えてきている．ネットワークに接続されたシステムの管理者は侵入からシステムを守るためにファイアウォールの構築に代表される，侵入を防ぐための数々の設定を行なっている．しかし，侵入者により新しい攻撃や侵入手

法が開発されているため，すべての攻撃に耐えることは困難である．そのため侵入を前提とした対策，すなわち，侵入の検出，侵入方法や被害範囲の分析も重要となる．

侵入の検出や分析は，システムの利用履歴 (ログ) の内容を分析することによって行なう．そのため，ログは分析に十分な情報を含んでいることと，確実に蓄積されていることが必要不可欠である．

しかし，高度な技術を有している侵入者が侵入に成功し，特権を手に入れた場合，その多くはシステムが記録しているログから，侵入の痕跡を巧妙に消去するため，侵入されたことの検出や侵入方法の解析を困難にする．

また，システム全体が破壊された場合，ログも破壊され解析を困難にする．

我々は，既存のログ収集機能では記録されない侵入解析に必要な情報の収集と消去されにくい方法でログの蓄積を行なうことを目指し，その機構を開発した．

2 侵入者の侵入方法

まず，侵入者のシステムへの典型的な侵入方法について説明する．

- 侵入者はOSやアプリケーションのバグやセキュリティホールを利用してホストに侵入する．
- データの不正アクセス，改ざん，いたずらなどの不正行為をおこなう．
- 新たな痕跡を残さないようにするためにシステムロギングデーモン (syslogd) やアカウンティング機能 (acct) などを停止，もしくは，痕跡が残らないように改ざんしたものと置き換える．
- 侵入の痕跡の残ったログから自分が残した痕跡を消去する．

侵入の痕跡を消すために，ログ全体を消去することもあるが，侵入に係わる部分だけを消去することもある，前者の場合，ログ情報が大幅に欠落するため，その検出は比較的容易であるが，後者の場合，システム管理者は侵入そのものに気がつかない場合が多い．

3 既存のログ収集機能

次に，UNIX が持つ侵入の検出，侵入方法の解析に利用可能な既存のログ収集機能について述べる．

3.1 wtmp

wtmp はユーザのログイン－ログアウトを記録するものであり，login コマンドや ftp デーモンなどによってファイルに記録される．wtmp が持つ情報は，TTY 名，ユーザ名，接続元ホスト名，時刻である．wtmp に記録される情報は，正規のユーザが，実際に利用した時間帯と記録された利用時間帯を確認することによって，侵入の検出に役立てることが可能であるが，次のような問題点もある．

- wtmp に記録を残すように始めから設計されているプログラムの記録しか記録できない．
- 直接ファイルに記録されるため，ファイル改ざんや破壊攻撃に弱い．

3.2 acct

acct(pacct) はアカウンティング情報の収集を目的とするもので，プロセス実行終了時にカーネルによってファイルに記録される．acct が持つ情報は，アカウンティングフラグ，終了ステータス，ユーザ ID，グループ ID，制御端末，実行開始時刻，ユーザ CPU タイム，システム CPU タイム，総実行時間，平均メモリ利用量，端末入出力バイト数，ディスク入出力ブロック数，コマンド名 などである．

acct は元来課金を目的として実装されたものであるため，侵入の検出，解析を行なうためには機能が不十分である．問題点を以下に示す．

- ログが記録されるのはプロセスの実行が終了した時点である．侵入者がシステムをハングアップさせたときは，その時点で動作していたプロセスの情報は記録されない．
- 記録されるコマンド名にはパス名が含まれていないため，実行されたコマンドを特定することはできない．

- プロセスの親子関係の情報が得られない.
- コマンドの引数が記録されない. 例えばrmコマンドが実行された場合でも, 実際に消去されたファイルは判別できない. またunlinkシステムコールを実行する別のコマンドやrmコマンドを別のコマンド名で起動された場合などは, acctの情報からではファイル消去を検出できない.
- 直接ファイルに記録されるため, ファイル改ざんや破壊攻撃に弱い.

3.3 syslog

syslogはsyslogライブラリを使用したアプリケーションのログをsyslogデーモン(syslogd)により収集する機能である.

syslogには以下のような問題点がある.

- 不正なアクセスが行なわれたことを類推するための情報は得られる場合があるが, 多くの場合, 解析に必要な情報は含まれていない.
- 得られるログは, アプリケーション開発者のスキルに依存する.

3.4 C2 audit

SunOSをはじめ, 多くの商用OSにはC2 auditを実現するためのセキュリティパッケージが実装されている. C2 auditを利用することによって, acctと比較すると多くの情報が得られるが, 以下のような問題点が残る.

- C2 auditを利用するように作られていないプログラムのログは記録されない.
- 直接ファイルに記録されるため, ファイル改ざんや破壊攻撃に弱い.
- 実装されているOSが限られている.

3.5 既存のログ収集機能の問題点のまとめ

システムが侵入を受けた場合には以下のような作業が必要である.

- 侵入を受けたホストの特定
- 侵入方法, 侵入経路の特定
- 生成, 改変, 消去されたファイルの特定
- 該当ホストからさらにネットワークを経由して他のホストに侵入した形跡の有無

これらの作業により, 侵入されたり影響を受けた可能性のあるホストを速やかにネットワークから切り離し, 侵入の証拠を記録し, 侵入方法の解析, 影響範囲を特定などを行なう必要がある.

既存のログ収集機能には, 下に示すような問題点がある.

- コマンドの引数が記録されないため, 生成, 改変, 消去されたファイルやtelnetコマンド使用時の相手先ホストの特定ができない.
- acceptシステムコールのログが記録されないため, ネットワーク経由での侵入の場合侵入元の特定が困難である.
- 直接ファイルに記録されるため, ファイル破壊に対して弱い.
- root権限を持つ侵入者により, 強制終了シグナルやコマンドによってログの収集そのものを停止される.

ログの消去や改変を防止するために, ログを定期的に他のホストへコピーを行なう方法も考えられるが, 必要なログは侵入者が侵入しroot権限を得て, ログの消去や改変, 停止を行なったまさにその部分のログであり, 改変, 消去が行なわれた後のログがコピーされたり, 停止された後のログがコピーされていても意味をなさない.

もう一つの問題点は, 既存のログ収集機能は侵入者に知られているということである. acctやwtmpなどのログは多少の機能の違いやログが保存されるディレクトリの違いはあるものの, すべてのUNIXが備えているため, 侵入者はその存在や機能, 内部構造などを熟知している.

4 問題解決のための手法

上で述べたような既存ログ収集機能の問題を解決するには以下のような機能が必要である.

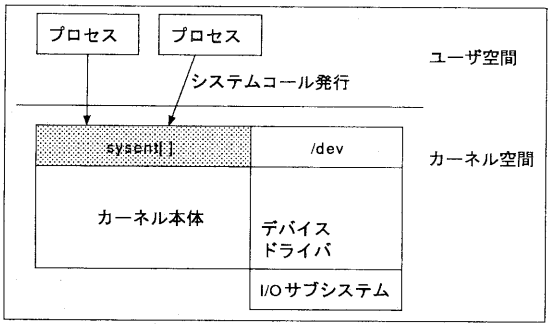

図 1: sysent

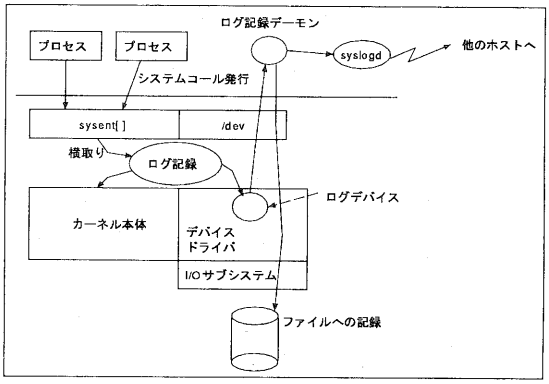

図 2: ログ機能の実装

- コマンドの実行やファイルの操作, シグナルの送信, ネットワーク経由の接続などを引数付きで記録できること
- 収集した情報を他の, より安全性の高いホストに記録できること
- ログ収集を停止することが困難であること

これらを実現するために我々は以下の手法を用いた.

- いくつかのシステムコールを引数付きで記録することにより, コマンド実行の引数や操作したファイルのパス, 侵入経路を特定するために必要な接続元ホストのアドレス等の記録を行なう.
- syslog ライブラリと syslogd を用いて, ログを他のホストに転送することによってログを消去から守る.
- 特定のプロセスに対する強制終了シグナルの送信を抑制する.

5 実装方式

BSD 系の UNIX ではカーネルのシステムコール呼び出し部分は, 各々のシステムコール関数へのポインタの配列 (sysent[]) として init_sysent.c 内に記述されている. init_sysent.c は, ソースコードが提供されていない OS(例えば SunOS) であっても, 独自のシステムコールを追加可能とするためなどの理由で, ソースコードとして附属している.(図 1)

我々は, init_sysent.c を書き換え, 本来のシステムコールを呼び出す前に, ログ情報を記録するための関数を呼び出すようにした. このような実装を行なうことによってシステムコール自体を改造することなく, 機能を追加することができる.

この方法は 4.3BSD,SunOS 4.x, BSD/OS, FreeBSD などの多くの BSD 系 UNIX で利用可能であり, 汎用性が高い.

できる限りカーネル内での処理を少なくすることと, 既存の機能を利用して新規開発コードを少なくするために, ログの記録, 指定されたプロセスに対するシグナルの抑止などを行なう関数および, ログのバッファリングとその内容をキャラクタデバイス経由で読み出せるようにするためのデバイスドライバのみをカーネル内に実装し, ログをファイルに記録する機能はデーモンプロセスとして実装した (図 2).

また, 他のホストにログを転送する機能は既存の syslog ライブラリを利用し, ログ記録用デーモンプロセス側から syslog 関数を用いて syslogd へメッセージを送信し, syslogd が持つメッセージを転送する機能を用いて他のホストにも記録するようにした.

5.1 対象システムコールと収集する情報

本ログ収集機能では以下のシステムコールのログを収集する．収集する情報は，システムコール種別，プロセス ID，親プロセス ID，実 UID，実効 UID，実グループ ID，制御端末，およびシステムコールの引数である

execv	コマンドの実行
execve	コマンドの実行
fork	プロセスの生成
vfork	プロセスの生成
rexit	プロセスの終了
connect	リモートホストへの接続
accept	リモートホストからの接続
sysacct	アカウンティングの ON/OFF
unlink	ファイルの削除
open	ファイルのオープン
creat	ファイルの生成
utimes	時刻の取得，設定
kill	プロセスへのシグナルの送信
killpg	プロセスグループへのシグナルの送信

kill および killpg システムコールでは，設定された特定のプロセス ID に対してのシグナル送信を検出し，シグナルを送信したプロセスを含む同一プロセスグループのプロセスをすべて強制フリーズさせ，システム管理者に通知する．シグナル送信を抑制するプロセス ID はカーネル内に用意した変数に設定する．

収集したログは，デーモンプロセスを用いて読み出すため，バッファリングを行なう。カーネル内にリングバッファを設け，ロギング関数が書き込みを行なうようにし，リングバッファを記録用デーモンが読み出せるようにするためのデバイスドライバを実装した．

5.2 記録用デーモン

記録用デーモンには次の機能を実装した．

- デバイスからログを読み出し，時刻を付加した後，ファイルに記録する機能
- ファイルに記録するのと同時に，syslog ライブラリを用いて，syslogd にログを送信する機能
- ログを 1 日分ずつ記録し，前日のログを圧縮する機能

デバイスから読み出されたログは時刻情報を付加した後，ログファイルの名前に当日の日付が付加されたファイルに記録される．また同時に，syslog ライブラリを使用して syslogd に送信される．日付が変わったことを検出すると，新しいログファイルを生成して記録を継続するとともに，前日のログを圧縮し，ディスク容量の節約を図っている．

ログデバイスのデバイス名，ログを記録するディレクトリやファイル名，syslog 送信時の Facility,Priority の設定は設定ファイルに記述するようになっている．ログを記録するディレクトリや設定ファイルは root 以外が読み書きできないように設定する．

5.3 得られる情報

記録されるログに含まれる情報は，時刻,ident，シリアル番号，システムコール種別，PID,PPID，uid,ruid,rgid，制御端末の vnode 番号，引数である．シリアル番号は本ログ機能で収集されたログの一連番号であり，何らかの原因でログの書き込みに失敗した場合や，万一，侵入者に改ざんされた場合に役に立つであろう．ログの整合性を保ったまま，一部を書き換えることは困難である．

下の例では root が /tmp の ls をした後，/tmp/xxx を削除し，成功している．vfork の場合の引数は PPID と親子の種別，exit の引数は終了ステータスである.(行末を PID フィールドの後で折り返している).

```
Tue May  5 18:05:27 1998  syscall: 602511 vf 26063
25274 0 0 0 1282 25274 1
Tue May  5 18:05:27 1998  syscall: 602512 ex 26063
25274 0 0 0 1282 /bin/ls ls /tmp
Tue May  5 18:05:27 1998  syscall: 602513 vf 25274
25270 0 0 0 1282 26063 0
Tue May  5 18:05:27 1998  syscall: 602514 op 26063
25274 0 0 0 1282 /tmp
Tue May  5 18:05:27 1998  syscall: 602515 exit 26063
25274 0 0 0 1282 0
Tue May  5 18:05:37 1998  syscall: 602516 vf 26064
25274 0 0 0 1282 25274 1
Tue May  5 18:05:37 1998  syscall: 602517 ex 26064
25274 0 0 0 1282 /sbin/rm rm /tmp/xxx
Tue May  5 18:05:37 1998  syscall: 602518 ex 26064
25274 0 0 0 1282 /bin/rm rm /tmp/xxx
Tue May  5 18:05:37 1998  syscall: 602519 vf 25274
25270 0 0 0 1282 26064 0
Tue May  5 18:05:37 1998  syscall: 602520 ul 26064
25274 0 0 0 1282 /tmp/xxx
Tue May  5 18:05:37 1998  syscall: 602521 exit 26064
25274 0 0 0 1282 0
```

また, ネットワークをからの接続は接続元のIP アドレスを含んだ情報が記録される.

下の例では PID が 115 のプロセス (この例では sendmail) に 192.135.93.194(0xC0875DC2) から接続されたことがわかる.

```
Tue May  5 18:39:27 1998  syscall: 602965 acpt 115
1 0 0 0 0 4 16 10020F5AC0875DC20000000000000000 0
```

5.4 性能

本機能を利用することにより, ファイアウォール上でサービスを行なうホストの性能は, 平均 7 %低下するが, 得られる情報の有用性から考えると, この性能低下は問題とならないであろう.

5.5 使用にあたっての注意事項

本ログ収集機構を利用した場合, 以下のような注意が必要である.

1. 本機能を利用して得られたログを解析することによって, 個々のユーザがいつ, 何をしたのかがわかるため, ユーザのプライバシに配慮する必要がある. 侵入者の行動を知るための機能を他の目的で使用するべきではない.

2. syslog ライブラリを用いてログの転送を行なっているため, ネットワークのモニタリングによりログの内容を取得可能である. 侵入者にネットワークをモニタリングされないことはもちろんだが, 1. の理由もあるため注意したい.

3. syslog によって転送されたメッセージを受けとるホストは, 外部からの侵入を決して受けないようにすることが重要である. ネットワークを利用するプロセスは syslogd 以外は動作させないようにし, 管理はコンソールから行なうべきである.

6 今後の課題

本機能には以下のような問題点があり, これを改善し, より確実性の高いログ収集機能とすることが今後の課題である.

- syslogd はメッセージの転送に UDP を使用しているため, 混雑したネットワークにおいてはパケットの喪失によりログが一部欠けるという問題が発生する. TCP を利用するか, UDP の場合でもハンドシェイクを行なうようなプロトコルを利用することによりこの問題を解決することが必要である.

- ログの記録, 転送時に暗号化を行なうなど, ネットワークのモニタリングによる情報の漏洩や, 権限のない者がログを目にすることのないようにする必要がある.

- 膨大なログの中から必要な情報を抽出する作業を現在は手作業や簡単なシェルスクリプトを用いて行なっているが, 解析用のツールの整備が必要である.

7 おわりに

このログ収集機能は 5 年程前に VAX8600 上で開発し, 現在までに SunOS 4.x, BSD/OS 2.x 3.x, 2.1.4 以上の FreeBSD に移植され稼働しており, 不正アクセスの検出および侵入経路の解析や影響範囲の分析に役立っている.

参考文献

1. Samuel J.Leffler, Marshall Kirk McKusick, Michael J. Kerels and John S. Quarterman, The Design and Implementation of the 4.3BSD UNIX Operating System, Addison-Wesley, 1989

2. DOD 5200.28-STD, Department of defence trusted computer system, evaluation criteria, 米国国防省, 1985.

3. CERT Coordination Ceneter Reports, http://www.cert.org/nav/reports.html

4. JPCERT/CC, JPCET/CC がうけた不正アクセス件数の推移, http://jpcert.or.jp/anm/status.html