

# システムログ調査

2003.01

## 1. システムログ調査の目的

ログ保存技術に関する研究・開発において、オープン系OSが実装しているログ機能で、どのレベルまで情報が収集できるか把握する必要がある。

そのために、OSが標準で提供しているログについて、その種類や内容、生成方法に関して調査を行い、OS標準ログの現状とその問題点についてまとめる。

## 2 . 調査対象ログ

以下の3つに分類し、ログの調査を実施した。

### システムログ

- ・RedHat Linux
- ・Solaris

### アプリケーションログ

- ・apache
- ・wu-ftp
- ・bind

### ネットワークログ

- ・iplog
- ・p0f
- ・gdd

### 3 . 調査結果

以下に、システムログ、アプリケーションログ、ネットワークログに関する一覧を示す。

#### RedHat Linux ログ

No.	カテゴリ	ファイル名	内容	備考	タイプ
1	syslog	/var/log/messages	一般的なシステムに関する情報	*.info; mail.none; authpriv.none; cron.none	テキスト
2		/var/log/secure	認証システムに関する情報	authpriv.*	テキスト
3		/var/log/maillog	メールシステムに関する情報	mail.*	テキスト
4		/var/log/cron	定期的に行われるプログラムに関する情報	cron.*	テキスト
5		/var/log/spooler	印刷やニュースに関する情報	uucp,nres.crit	テキスト
6		/var/log/boot.log	システム起動時に実行されるデーモン関連の情報	local7.*	テキスト
7	ハードウェアログ	/var/log/dmesg	システム起動時に Linux カーネルによって初期化されたハードウェアの情報	dmesg コマンドで参照されるログ	テキスト
8	ログインログ	/var/log/lastlog	ユーザが最後にログインした時間やアクセス元の情報	lastlog コマンドで参照されるログ	バイナリ
9		/var/run/utmp	現在ログインしているユーザの情報	whoコマンド、wコマンドで参照されるログ	バイナリ
10		/var/log/wtmp	ユーザのログイン・ログアウト時間やホスト名の情報	lastコマンド、acコマンドで参照されるログ	バイナリ
11		/var/log/btmp	ログインに失敗したユーザ名、アクセス時間の情報	lastbコマンドで参照されるログ。デフォルトでは有効になっていない為、touch /var/log/btmp でファイルを作成する必要あり	バイナリ
12	コマンドログ	/var/log/pacct	ユーザが実行したコマンド履歴の情報	lastcommコマンドで参照されるログ	バイナリ
13	RPMログ	/var/log/rpmpkgs	システムにインストールされている RPM パッケージのファイル名情報		テキスト

## アプリケーションログ

No.	カテゴリ	ファイル名	内容	備考	タイプ
1	アプリケーション ログ	access_log	HTTP サービスへのアクセス内容に関する情報	Apache が生成するアクセスログ	テキスト
2		error_log	HTTP サービスへのアクセスに関するエラーや警告の情報	Apache が生成するエラーログ httpd.conf 内でログファイルの設定を行うことにより、独自ログまたは、syslog ログを出力することが可能。	テキスト
3		xferlog	FTP サービスが処理したファイル転送に関する情報	Wu-ftp が生成するログ	テキスト
4		named.log	ゾーン転送の送受信やクエリを受信した際の情報	Bind が生成するアクセスログ named.conf 内でログファイルの設定を行うことにより、独自ログまたは、syslog ログを出力することが可能	テキスト

## ネットワークログ

No.	カテゴリ	ファイル名	内容	備考	タイプ
1	ネットワークログ	/var/log/p0f	受信した TCP(SYN) パケットに基づき、受動的に OS 種別の検知を行う	p0f プログラムで取得できるログ	テキスト
2		/var/log/iplog	TCP、UDP、ICMP の各種パケットを記録し、ポートスキャンやSmurf攻撃などの検知を行う	iplog プログラムで取得できるログ iplog.conf 内でログファイルの設定を行うことにより、独自ログまたは、syslog ログを出力することが可能	テキスト
3		/var/log/gdd/log	TCPセッション(telnet や ftp など)のストリーム通信を維持し、細切れになったパケットの再構築を行う	gdd プログラムで取得できるログ	テキスト

## 4 . 考察

Unixに保存されるシステムログの多くは `syslog` で管理されている。それに加え、主要なアプリケーションソフトでは、`syslog` をサポートしているものが多く、`syslog` を利用することで、システム上のログを一元管理することができる。

また、`syslog` では、ファシリティやプライオリティの設定変更を行うことで、ログレベルの変更や出力先をリモートホストにリダイレクトすることもできる為、利便性が高い。

Unixにおけるログ情報については、`syslog` を含めたOS上のログやアプリケーションログを利用することで、かなり詳細な情報を収集することができる。

但し、syslog には以下の様な問題点も指摘されている為、これらの問題点の解決策と標準ログで収集できない情報に関する検討も含め、ログ保存技術の研究・開発を行う。

- syslog が生成するファイルはテキストファイル
- syslog のログ転送はUDPプロトコルを使用
- syslog には認証機能やアクセス制御がない
- 時刻の情報に年やタイムゾーンがない