ログ管理の実例

新潟インターネット研究会
塩路 和彦
shioji@on.rim.or.jp/shioji@nisoc.or.jp

ログ管理の必要性

- 現在のネットワーク、システムの状態の把握
  - 気付いていないエラーが起こっていないか
  - 負荷は高くないか
  - 有効に利用されているか
- セキュリティのチェック
  - 不正アクセスがないか、踏み台にされていないか
  - ポートスキャンの形跡は
- diskの節約、有効利用
  - logの定期的な削除、移動

ログの種類

- デフォルト(?)でlogが出力されるもの
  - lastlog、utmp、wtmp
- syslog経由でlogが出力されるもの
  - /etc/syslog.confに従う
  - telnetd、ftpd、pppd、cronなど
- サービス（daemon)自体がlogを出力するもの
  - apache、squidなど

/etc/syslog.conf

- selectorフィールドとactionフィールドに分けられる
- selectorフィールドはさらにfacilityとpriorityにで構成される。
  - facility(メッセージを生成するサブシステム)
    - auth,authpriv,cron,daemon,kern,lpr,mail,mark,news,syslog,user,uucp,local0～local7
  - priority(優先度)
    - debug,info,notice,warning,err,crit,alert,emerg
- 詳細は/usr/include/sys/syslog.hを参照（Linux）

Facility

kern	カーネル用
user	ユーザプロセス用
mail	メールシステム用
daemon	システムデーモン用
auth	認証システム用
mark	タイムスタンプ用
lpr	ラインプリンタスプーリングシステム用
news	USENET news システム用
uucp	UUCP システム用
cron	cron/at システム用
authpriv	認証システム用(private)
local0～local7	ローカル用に予約

Priority（優先度）

- emerg　緊急事態発生メッセージ
- alert　アラートメッセージ
- crit　重大なエラーメッセージ
- err　通常のエラーメッセージ
- warning　ワーニングメッセージ
- notice　注意程度のメッセージ
- info　情報メッセージ
- debug　デバック用メッセージ

Action

- 通常のファイル
- 名前付きファイル
- ターミナルとコンソール
- リモートコンピュータ
- ユーザ名のリスト
- ログインしているもの

書式

Facility.Priority　　Action

- 基本は指定されたFacilityのPriorityより重要度が高いメッセージがすべてactionに沿って記録される。
- Linuxのsyslogはちょっと違う？（拡張されている）
  - アスタリスク(＊)、none、コンマ(，)、セミコロン(；)、イコール記号(＝)、エクスクラメーションマーク(！)

例（１）

```
#
kern.*          /var/adm/kernel
kern.crit       @alice
kern.crit       /dev/console
```

- FacilityがkernのメッセージはすべてVar/adm/kernel に出力。
- その内優先度がcritより高いものはすべてリモートのホストaliceへ送信。またコンソールにも表示する。

例（２）

```
#
mail.*;mail.!=info      /var/adm/mail
mail.=info              /var/adm/mail.info
```

- mailのlogはすべて/var/adm/mailに出力する。ただし優先度がinfoのものは除く。
- mailのlogのうち優先度がinfoもののみを/var/adm/mail.infoに出力する。

例（３）

```
#
*.emerg                 *
*.alert                 root,shioji
```

- 緊急事態発生のメッセージはログインしている全てのユーザに伝える。
- 優先度がalert以上のものはrootとshiojiがログインしていればその端末に表示する。

主なサービス（daemon）のlog

- inetd
  - telnetd、ftpd、tcp_wrapper、qpopper
  - syslogd経由で出力
- sendmail、INN
  - syslogd経由で出力
- Apache　access_log、error_log
- Squid　　access.log、cache.log、store.log

Logの活用(1)

- 多くのlogはテキストファイル
  - AWK、Perl等で簡単にグラフデータにしたり、統計処理できる。
  - 言語の勉強にもってこい？
- AccessWatch、WebStatなどのソフトを利用
  - 簡単に凝った(グラフィカルな)画面が作れる。
- cronを使えば自動化できる
  - logの削除や移動も同様

Logの活用(2)

- Logの管理とセキュリティは切り離せない。

- 定期の通知
  - cronを利用。
  - Site policyに従い頻度を設定。
- 異常発生時の通知
  - logにある文字列が記録されたとき報告する。
  - swatchを利用。

swatch

- ftp://ftp.stanford.edu/general/security-tools/swatch

- Logにある文字列が記録されたときリアルタイムに報告
  - mail or コマンドを実行