工学部技術部ネットワークグループ活動報告
V　工学部サーバ機の運用について

第二技術系第四班　　中村　勝

1.内容

セキュリティ

TCP Wrapper (host.allow/host.deny) ,inetd

ログの監視 (system,web)

アップデート,パッチ

バックアップ

停電の時 (UPS)

HP のコンテンツの管理

運用マニュアルの作成

2.1.　セキュリティ

管理者として重要なこととして(1)システムをダウンさせない(2)セキュリティをしっかりしておくことが重要である。(2)に問題があれば、クラッカーと呼ばれる悪質なユーザーがサーバ機に侵入しデータを外部にもらしたり、データの書き換え、システムクラッシュ、他のマシンへの足場として利用されてしまう。

これらを未然に防ぐ方法として、ineted,TCP　Wrapper がある。これらの役割は、要求されたサービスを安全に実行するため、ログインとアクセス管理の機能を提供するものである。

2.1.1　TCP Wrapper (hosts.allow/hosts.deny) ,inetd

TCP　Wrapper は hosts.allow ファイル,hosts.deny ファイルを読み込み、許可されているホストと、禁止されているホストを判断する。許可されていれば、ftp や telnet でリモートログインできるが、禁止されていればできない。つまり hosts.allow ファイルに記述されていれば、サービスは提供されるが、hosts.deny ファイルに記述されていればサービスは提供されない。

hosts.allow ファイル,hosts.deny ファイルの適応順序は

(1) hosts.allow ファイルで記述されていれば許可する。

(2) hosts.deny ファイルで記述されていれば禁止する。

(3) どちらとも記述されていなければ許可する。

である。(3)に注意する必要がある。セキュリティ上の必要等で、特定のサーバを安全に運用したいなら、hosts.deny ファイルは以下のように設定する。

```
#
# hosts.deny    This file describes the names of the hosts which are
#               *not* allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
ALL:ALL
```

hosts.allow ファイルの設定例

hosts.allow ファイルに許可するサーバを記述する。

ineted はクライアントからのサービス要求があると動きだし(inetd.conf の読み込み)、対応したサーバプログラムを起動(inetd.conf に記述されている内容(この例では tcpd) を実行)する。ineted.conf 設定例を次に示す。

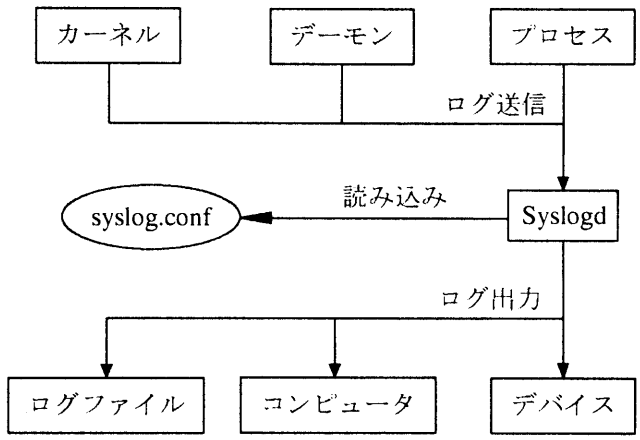
```
#
# inetd.conf    This file describes the services that will be available
#               through the INETD TCP/IP super server.  To re-configure
#               the running INETD process, edit this file, then send the
#               INETD process a SIGHUP signal.

ftp     stream  tcp     nowait  root    /usr/sbin/tcpd      in.ftpd -l -a
telnet  stream  tcp     nowait  root    /usr/sbin/tcpd      in.telnetd
```

ineted.conf の設定例

2.1.2　ログの監視(system,web)

もし侵入されたときや、侵入を試みられたとき、何らかの形で足跡がのこる。これを調べるためにログの監視を行う必要がある。

syslogd はカ--ネル、デ--モン、プロセスなどさまざまな記録をログとして出力する。そして、その記録は/etc/syslog.conf の設定にしたがってログの発行者、エラ--レベルなどによって分類され、多数のログファイルに書き出される。



syslogd のイメ--ジ図

syslogd の出力元

出力元	内容
kern	カ--ネルのメッセ--ジ
auth	login,su,getty 等のメッセ--ジ
daemon	ftpd,popd,named 等のデ--モンのメッセ--ジ
mail	sendmail のメッセ--ジ
user	ユ--ザ--のプロセスのメッセ--ジ

メッセージのエラーレベル(上にあがるほど重要)

レベル	内容
emerg	すべてのユ--ザ--への通知
alert	直ちに対処が必要な重大なエラ--
crit	ハ--ドウェアのデバイス・エラ--のような、致命的なエラ--
err	その他のエラ--
warn	警告メッセ--ジ
notice	致命的ではないメッセ--ジ
info	情報メッセ--ジ
debug	プログラムをデバッグするときに有益な情報
none	メッセ--ジを送らない

syslog.conf の内容を以下に示す。

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none                  /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                      /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  /var/log/maillog

# Everybody gets emergency messages, plus log them on another
# machine.
*.emerg                                                 *

# Save mail and news errors of level err and higher in a
# special file.
uucp,news.crit                                          /var/log/spooler
```

その他のログとして、lastlog、wtmp があり、lastlog は１人１人ユーザの最近のログインに成功した記録と失敗した記録を、wtmp はコネクト時間のアカウントの記録をログにする。
これらのログは、時々チェックしエラーが起きていないか、いつもと違うことが起きていないかをチェックする必要がある。クラッカーにより書き換えらてしまうこともあるので、外部媒体に定期的に点検しバックアップをとっておくなどの必要もある。

2.1.3　アップデート、パッチ

セキュリティに問題があるとか、２０００年問題に代表されるように正常に動作しないなどの対処をしなければならない。これを怠れば、正常に動作しなければならないはずのサーバ機が動かなくなったり、クラッカーの攻撃を受ける可能性がある。使用しているソフトウェア会社のサイトの情報を見ることで防げるが、こまめにチェックする必要がある。
工学部サーバ機に使用されている OS,アプリケーションは２０００年問題対応済みのものである。

2.2　バックアップ

もし、何らかの理由(ファイルの消失・クラッカーの攻撃等) により、サーバ機がダウンまたは正常に動かない場合には一刻も早く復旧する必要がある。また、どのような原因でトラブルが発生したのかを知り、繰り返しおこさせなくする事も必要である。

2.3　停電の時

今回、選定した UPS(無停電電源装置)は手動で電源を ON･OFF するタイプのものである。これは既知の停電(工事等)であれば、停電の前にコンピュータを終了しておけばよく、電気工事等の時に何度も停電するような場合、システムに負荷がかからないようにするためである。

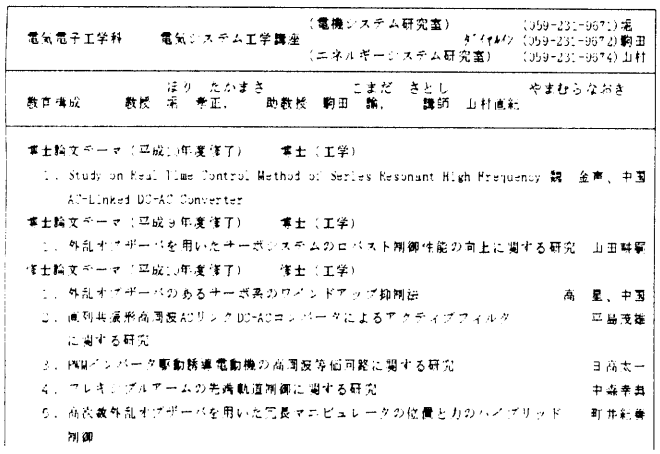
2.4　ホームページコンテンツの管理

業務内容一覧を以下に示す。

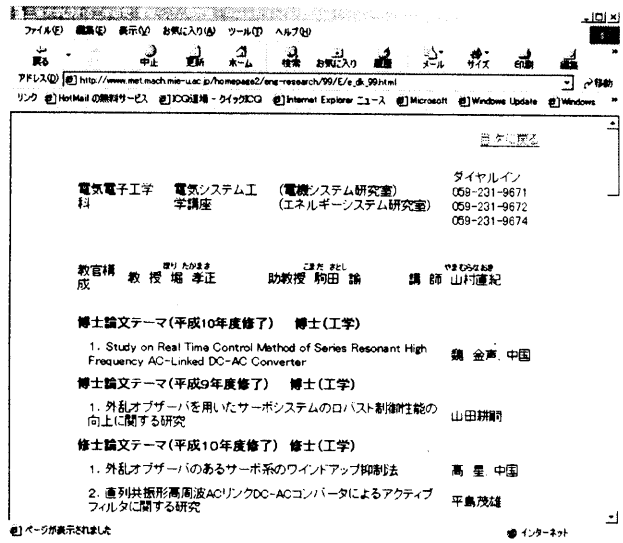
(1) アクセスログの解析・統計
(2) 入力作業：毎年更新が必要なもの
- 「三重大学における工学研究」の内容
- 「RESERCH REPORT」の目次
- 卒業生進路状況、学生現員表、入学状況、学部在学生出身地　　等

(3) 入力作業：随時更新が必要なもの
- 入試案内(学部,大学院,編入,留学生)
- 工学部のお知らせ(公開講座,記念事業)
- 職員(教官,事務職員)
- 工学部 HP へのリンク依頼の対応　　等

例として、今年度入力分が終了した「三重大学における工学研究」の元の提出原稿(一太郎にて作成)、html 変更後を以下に示す。これはすでに工学部のホームページにある。



元の提出原稿



html 変更後

2.5 運用マニュアルの作成

運用マニュアルがない場合の問題点とマニュアルのメリットについて

(1)運用マニュアルがない場合

- 動作のチェックミスや作業漏れ
- 作業効率の悪化
- サーバの復旧に時間がかかる　　等

(2)マニュアルのメリット

- 作業ミスの防止
  誰かの記憶を頼りにするとうっかりミスや間違ったまま記憶での作業ミスなどの防止。
- 作業の効率化
  作業手順のマニュアルがあれば、時間を無駄にすることなく作業を進めることができます障害児でも速やかに復旧できる。頻繁に行わない作業について効果がある。
- 作業方法の効率化
  不慣れな管理者でもマニュアルによって作業できるので、特定の管理者に負担をかけなくて済む。
- ノウハウの蓄積
  同じミスを繰り返すことが減り,作業能率の UP,新しい管理者に知識を引き継ぐこともできる。

3.まとめ

今後管理者として行わなければならない作業の下準備を紹介した。今後の予定は、サーバ機の設置される部屋が出来次第、サーバ機を運営することである。運営していく上で生じたトラブルなどは今後の技術発表会にて発表予定である。

参考文献

(1) AEleen Frisch 著　榊 正憲 訳：UNIX システム管理入門　アスキー出版局
(2)國安和廣,秀和システム出版編集部：フリー UNIX で作るネットワークサーバ構築ガイド　秀和システム
(3) http://linux.nikkeibp.co.jp/column/ash/：Linux サーバ運用マニュアル　日経 Linux ホームページ