工学部技術部ネットワークグループ活動報告

サーバ機の移行からこれまでの運用について

中村　勝(第二技術系　第四班)　　伊藤　篤(第一技術系　第一班)

1.はじめに

サーバ機(事務部 mail&DNS,工学部 WWW)の移行作業,サーバのシステム監視,トラブル時の復旧方法と対策,セキュリティ,メンテナンス作業,トラブル事例の紹介等実際に行った作業を報告する。

2.移行作業

事務部 mail&DNS のパスワードファイル移行の問題点について述べる。また事務部 mail&DNS,工学部 WWW サーバ機のその他のファイル移行作業の手順について述べる。

2.1.問題点

従来機と新設機の比較表を図 1 に示す。注目したい点は OS が異なるという点である。

	従来機	新設機
サーバ機の設置場所	庶務係/機械工学科	サーバ室
ハードウェア	市販機(FMV/DEC)	自作機
OS	BSDI	TurboLinux Server 1.2
カーネル	BSD/OS 2.0 Kernel	Kernel 2.0.3.6
BIND	8.2.1 (但しbootファイルは4系)	8.2-2p5
Sendmail	8.8.8.4	8.9.3-16
CF	3.6W	3.7Wp12-1
Webサーバーソフト	CERN/Apache	Apache

図 1　サーバ機の比較表

2.2.mail&DNSサーバ

password ファイル

①従来機の/etc/master.passwd ファイルを新設機に ftp でコピー

②新設機にユーザのアカウント作成(パスワードなし)

③/etc/master.passwd ファイルのパスワードが暗号化された文字列の部分を、新設機の/etc/passwd ファイルのパスワード部分にコピー

④パスワードが変更されているかどうかログインしてチェック

sendmail

① sendmail.def の書き換え

② sendmail.cf の作成

home ディレクトリ

・従来機の/usr/home/以下を圧縮して新設機の/home/以下に展開
(old_home_town としてバックアップ)

mail スプール

・従来機の/var/home/ユーザアカウント名 ファイルを圧縮して新設機の/var/spool/mail/以下に展開

2.3.Webサーバ

機械工学科より移行に伴う変更作業にて

・ドメイン変更

http://www.met.mach.mie-u.ac.jp
/homepage2/index1.html
↓
http://www.eng.mie-u.ac.jp/index1.html

・URL 変更に伴うリンク先の変更

・横幅を 600 ドットに変更

・コンテンツの更新

を行った。

3.サーバのシステム監視

3.1.システム(プロセス)の稼働状況

システムは vmstat,ps,top コマンドを用いてプロセスの監視や状態,メモリの使用状況,ディスクのアクセス頻度,CPU の利用状況の監視をしている。

3.2.システム管理者へのメール配信による監視

システムよりログやエラーに関するメールが cron.hourly により一時間毎に送られてくる。これで不具合・不正ログインのチェックを行っている。

3.3.ログの採取、検証、ローテーション

syslog によるログの採取,logcheck による log の配信,cron による週に 1 回 log ファイル,メールスプールを圧縮,4 週に 1 回 logrotate 実行を行っている。今後テープへのログの自動保存を行う予定である。

4.トラブル時の復旧方法と対策

4.1.ポリシー

速やかに，ネットワークグループの誰もができるような体制としてマニュアルの作成中である。

4.2.システム復旧方法

万一の時の復旧方法として

・バックアップ機の準備
・データとログのバックアップ方法
・cron にて syslog とアクセスログの採取
・データ変更時にデータのバックアップ
・同リストア方法

・設定ファイルの保存
がある。

5.セキュリティ

提供するサービスや管理上必要なサービス以外のポートは閉め,またアドレスも制限している。被害時の対応策として
・サービスの停止
・ネットワークから切り離し
・データ、ログの隔離・保存
・被害状況の把握
・ユーザ,関係機関への通知
　　IPA・JPCERT・警察などへの被害届
・復旧手段の考慮
・設定の見直し
を考えている。

また,情報入手・調査場所として以下のサイトがある。
・コンピュータ緊急対応センター
　　http://www.jpcert.or.jp/
・情報処理振興事業協会
　　http://www.ipa.go.jp/
・警視庁　　http://www.npa.go.jp/
・TurboLinux　　http://www.turbolinux.co.jp/
・日本の Linux 情報
　　http://www.linux.or.jp/
・ネットエージェント
　　http://www.netagent.nd.to/
・有限会社長崎ネットワークサービス
　　http://www.nanet.co.jp/

6.メンテナンス作業

作業内容一覧を以下に示す。
・Web コンテンツの作成,更新
・三重大学における工学研究
　　・工学部長挨拶
　　・教職員
　　・国際宇宙科学会議（シンポジウム）
・リカレント教育
・Y2K 問題の対処
・セキュリティホールによるバージョンアップ及びパッチあて
　　・wu-ftpd2.6.1 へアップデート
　　・canna-3.5b2-24 サービスの停止
　　・BIND8.2.2-P5 へアップデート
・メールをメールゲートウェイに経由するように設定変更
・ネットワークに関する連絡事項を各係へアナウンス
・ユーザー登録,アカウント発行,グループの登録
・アカウントの削除
・事務ネットワークの管理 ,ネットワーク機器のメンテナンス
・IP アドレスの管理・発行,ネットワーク接続
・メールアドレスの管理・発行
・ウィルスチェック,バックアップ ,障害時対応,修理
・アプリケーションインストール

7.トラブル事例等の紹介

今まで起こったトラブル事例やアタック例を以下に列挙する。
・工事停電後の再起動時に勘違いで sendmail が自動起動せず
・落雷による停電時に UPS の設定ミスで所定の動作をしなかった
・就職情報室の HUB 故障（落雷?）
・学外(133.67 以外)からのアタック
・学内からメールの接続
・FDDI ケーブルとコネクタ部分の接合不良。60,eng ドメインが孤立
・Web に記載されていたメールアドレスと実際のメールアドレスが違っていた

8.サーバ運営

現在,ネットワークグループは 7 人がいるが,スキルある人が少ないので知識の共有とスキルアップのため担当者を
・就職情報室
・工学部 Web サーバ機
・工学部 mail,DNS サーバ機
の 3 グループに分け、必ずどこかのグループに属すようにしスキルアップを図っている。ただし,重要な変更点などはネットワークグループ全員で作業を行うようにしている。

9.おわりに

現在の OS1.2 からを安全なサーバーを構築するために必要とされるセキュリティ対策を充実した 6.1 へ変更,テープの追加,バックアップ機の作成を行う予定である。

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) Olaf Kirch 著　小嶋隆一,高尾哲康共訳 Linux ネットワーク管理　O'REILLY