ホスティングサービスの利用によるサーバ更新と サーバ管理運用について

総合技術センター
計測・制御技術分野　飯田　仁 (Hitoshi Iida)

１．はじめに

長期間サーバシステムを運用しているとHDD等の各パーツの経年による故障発生の懸念が高くなってくる。そこで定期的に新しいサーバを準備し現在のシステムを新サーバに移行し，システムを停止させることなく継続利用できるようにする必要がある。今回，当学情報センターが運用している「ホスティングサービス」を利用して学内向け専用の新サーバを構築しシステムの移行を行ったのでその報告に加え，長期間運用していて気づいた便利な機能を紹介したい。

２．ホスティングサービスとは

ホスティングサービスとは，「自社施設に設置しインターネットに接続された情報発信用のコンピュータ（サーバ）の機能を，遠隔から顧客に利用させるサービス。顧客が自前の設備などを持たずにインターネット上で情報やサービスを配信するのをサポートするサービス」[1]とある。今回の場合，自社施設とは徳島大学・情報センターであり，情報センターのサーバ機能を利用（借用）してシステムを構築したことになる。この方法では高価なサーバ本体を購入することなく，サーバを構築することができる点に加え，停電時の電源バックアップに関する機能も具備している点が優れている。一方でサーバに関するスペックを選択できないことや，利用ポートに制限があるという点に不満を感じるかも知れないが，当学では情報センターとの協議によりメモリとHDD及び利用ポートに関しては柔軟な運用がされている。今回利用したスペックを表1にまとめる。

残念ながら当学のこのサービスは当学内限定のサービスであり，学外の方は利用できない。また，個人的な利用も認められていない。

現在の所，サーバの運用に係る費用（電気代など）は請求されていないので，無料で利用しているが，将来にわたって無料である保証はなく，筆者としてはこの状況が続くことを願うだけである。

表１　ホスティングシステムの基本構成

CPU	1Core
メモリ	4GB
HDD	50GB

今回はこのサービスを利用し，学内限定システムである
① 授業出席管理システム（中継サーバ）
② 工学部建物別使用電力確認システム
③ 講義室利用状況確認システム
以上のシステムを構築した。現在の所，旧サーバからは①の出席管理システムを完全に移行した。②と③については移行作業中である。

３．システムについて

ホスティングサービスでは，サーバのOSは管理者（筆者）が任意に選択することができるので，運用実績のあるRHEL互換であるScientific Linux7.0（以下SL）を選択した。SLは最少構成で導入し，新たに必要な機能が不足している場合にパッケージマネージャーyumを利用し追加する事とした。yumの自動更新機能は一部を除いて有効にしておくことは言うまでもない。前節で紹介した3つのシステムはWebサーバ機能で実現しているため，基本サーバソフトとして
A)　Apache2.4
B)　PHP5.4→PHP5.6
C)　PostgreSQL9.2
を導入した。上記のソフトは当初SLの標準パッケージを利用したがPHPは後日外部のサードパーティリポジトリ（remi）[2]を利用し最新バージョンに更新した。外部パッケージであ

るがセキュリティの対策・対応も早いのでこちらを利用する方が良いと判断した。

４．追加機能

ここでは構築したシステムで特別に必要となった機能のみを記載する。サーバ管理に必要な物は割愛する。

４．１　IP-sec

前述の出席管理システムでは，一部IP-secを用いて出席データの登録を実施している。以前のサーバではIP-secに関してRacoon2というパッケージを利用していたが，今回のサーバ構築時にはパッケージのメンテナンスがされていないことが分かり, strongSwanというパッケージに変更してIP-secの機能を実現した。この導入に関しても，外部サードパーティリポジトリであるEPEL[3]を利用した。前述したremiやEPELは通常のソフトウェア更新時に自動更新とならないように設定を行った。従って，追加したパッケージの更新は手動で行うことになる。

４．２　グラフ表示

工学部建物別使用電力確認システムではグラフ表示するためにJpGraph[4]というPHPの拡張ライブラリを追加した。非営利目的であるため指示[5]に従い画面表示を実施した。

５．サーバ運用について

５．１　通常の管理（ログ監視）

通常はlogwatchというパッケージを追加して，毎日様々なログから生成・送信されるメールを確認して通常とは異なる接続が無いかなどを確認する。最少構成でシステム導入を実施したため，このような管理ツールも追加する必要があった。

５．２　ログの出力先指定

前述のstrongSwan（IP-sec通信）は標準でログの出力先が/var/log/secureと/var/log/messageに出力される。接続ごとにログが発生し，1日でもかなりの量になってしまう。また，2つのファイルに分散されるので確認作業が煩雑になることに加え，他の重要なログがstrogSwanのログに埋もれ，見落とす可能性があるため，出力先を1つの専用ファイルに変更した。出力先の変更についてはrsyslogdの設定[6]により実施した。図１に設定内容を示す。出席管理システムで運用するcrotabの処理も通常とは異なるファイルに出力するよう設定を行った。

```
:syslogtag, contains, "charon" ¥
  /var/log/strongswan/strongswan.log
& ~
:syslogtag, contains, "strongswan" ¥
  /var/log/strongswan/strongswan.log
& ~
```

図１　rsysylogの設定例

５．３　Webサーバ（Apache）

前述した3つのシステムでそれぞれホスト名を変更し運用している。これに伴い，ヴァーチャルホストの設定で，接続ログなどもそれぞれ別ファイルになるようにしている。SSL証明書[7]を複数ホスト名で申請しhttps通信も実施している。

５．４　ポート変更

既知のポートを使用していると，不必要な利用者が訪問し安全性が脅かされることがある。気休めかもしれないが，以前のサーバからSSHのポートを変更して運用している。変更に際し，情報センターにポート利用の申請が必要になる。無条件で利用可能なポートは80, 443，3389であり，これら以外は申請の必要がある。

変更後の使用ポート番号であるが，慣例に従い49152～65535の範囲[8]で決めると運用時の不具合が少ない。図２にsshd.configファイルの変更例を示す。

```
Port xxxxx（←新しいポート番号）
AllowUsers user1 user2（←ユーザ限定）
PermitRootLogin no（←root ログイン禁止）
```

図２　sshd.configの変更例

５．５　ファイヤーウォール

不必要なネットワーク通信を遮断するために有効な機能で，使用しないポートは全て閉鎖（Reject）し，必要ポートのみ開放（Accept）

する設定としている。なお，ここで利用するポートは事前に情報センターに申請し開通手続きをしなければ利用できない。

５．６　停電作業

突発的な停電に対しては電源のバックアップ措置がなされているので心配はない。しかし，電気事業法に基づく年1回の計画停電がある。受電設備の検査や非常用発電設備が正常に動作することを確認するための停電で，この作業時にはサーバを停止する必要がある。しかし，可能な限りサーバは稼働させておきたいので，自動的に停止する方法を取った。これは単にcrontabを利用して，決められた時間に停止（shutdown）コマンドを実行するというもので停電開始時刻の10分前に設定している（図３）。この自動停止を実行する前に，深夜に問題無く再起動するか確認してから本番の設定を実施した。ただし，NTPなどによりサーバの時刻を正しく設定しておく必要がある。なお，停電からの復帰（復電）は情報センターの担当者がサーバの起動（電源ON）まで実施してくれるので，別途作業の必要はない。

以上で自動停止が実現できることを示したが，停電終了後にcrontabの設定はコメントアウトにて無効化する必要がある。

```
# [11/29 08:50]シャットダウン実施
50 8 29 11 * /sbin/shutdown -h now
```

図３　crontab設定

５．７　手動更新

前述のようにサードパーティリポジトリを追加して導入したソフトウェアに関しては念の為手動にて更新作業を実施している。特に日程を決めている訳ではないが，月１回程度は実施するようにしている。

５．８　バックアップ

サーバを運用していると不足の事態に備えデータのバックアップ作業が必要になる。従来から実施している方法は，外付けHDDにデータを圧縮して保存する方法で，HDDが異なるため内蔵（システム）HDDと同時に故障することは無いであろうとの考えからである。しかし，ホスティングサービスでは外付けHDDを接続できないため，旧サーバと連携[9]して旧サーバの外付けHDDにバックアップデータを保存するようにしている。以下にバックアップ処理の手順を示す。

1. 新サーバ本体のHDDに必要なバックアップファイルを作製
2. sftpを用いて旧サーバの外付けHDDにバックアップファイルをコピー
3. 新サーバ本体に作製したバックアップファイルを削除

一連の動作をシェルスクリプトにて記述し，crontabに毎日深夜に実行するよう設定した。

毎日のバックアップ処理では，Webサーバのコンテンツと，データベースに登録されているデータを対象とし，月3回（1日，11日，21日深夜）のバックアップ処理ではサーバの設定データ（/etc内）をバックアップ対象に追加している。バックアップスクリプトの概要を図４に示す。

```
# !/bin/sh
DIR=PATH
cd /home/www/html
/bin/tar –zcf ${DIR}/file_name.tar.gz ./XXXX
/bin/sftp -b sftp.bat -i key_file user@server
/bin/rm –f ${DIR}/file_name.tar.gz
```

図４　バックアップスクリプト概要

図４中のsftp.batファイルにはsftpで実行する処理を記述しておく。またkey_fileファイルはsftpをバッチモードで実行するために必要なパスワードの秘密鍵であり，公開鍵はバックアップ先サーバに登録しておく必要がある。図５にsftp.batの内容例を記載する。

```
cd SAVE_DIR
put backup_filename.tar.gz
exit
```

図５　sftp.batファイルの内容例

なお，エラーが発生しバックアップ処理が滞った場合には電子メールにてその旨の通知が届くようにしている。

５．９　HDDディスク容量

HDDの容量が少ないと，運用を開始するとディスク空き容量に余裕が無くなる。今回のサーバでは特に出席管理システムの出席情報の生データが1か月で約5GBとなるため，定期的に削除しなければHDDの空き容量が不足してしまう。このHDD空き容量確保のためのデータ削除作業はシェルスクリプトを用い手動で実施していた。この作業は不定期に実施していたがこの原稿執筆を期に，月初めに自動実行するように変更した。

５．１０　不具合について

今回構築した新サーバではないが，本原稿の執筆時に外付けHDDに起因する不具合が発生したので記載しておく。サーバにUSB接続の外付けHDDをバックアップ目的で接続しており，内蔵HDDにLinuxシステムを導入し起動ディスクとしている。前述の停電時にカーネル等の更新を実施し再起動をしたところ表２に示すようにデバイス名が変わっており，バックアップスクリプトの動作でHDDの容量が不足する不具合が発生した。これは前述のlogwatchにより停電の翌朝に届いた電子メールで確認できた。ただし/etc/fstabの/bootに関する記述がUUIDを用いていたため，デバイス名が変更になっても正常にサーバは起動しサービスを提供していたので，原因の確認と再発防止策の実施に時間的余裕があり，事なきを得た。

表２　デバイス名の変化

内／外	再起動前	再起動後
内蔵HDD	/dev/sda	/dev/sdb
外付けHDD	/dev/sdb	/dev/sda

このような不具合を防止するためにはデバイス名を固定することで回避することが可能である。この設定は/etc/udev/rules/以下に設定を追記し実施[10]した。図６は内蔵用HDDをsdaに固定するための設定。図７は外付けHDDをusbhdaに固定するための設定。図６と図７の内容は同じファイルに記述する。今回は参考URLに従い10-local.rulesというファイルに記述し再起動を行った。

```
SUBSYSTEMS=="scsi", ¥
ATTRS{unique_id}=="xxxxx",NAME="sda%n"
```

図６　内蔵HDDの設定

```
SUBSYSTEM=”usb”, ATTRS{serial}=”yyyyy″, ¥
NAME=”usbhdb%n”
```

図７　外付けHDDの設定

図６”xxxxx”と図７”yyyyy”の部分はHDDによって異なり，確認するためには“udevadm info -a -p $（udevadm info -q path -n /dev/sda（sdb））”というコマンドを利用した。

なお，この不具合原因の究明と対策に関しては情報センターに多大なるご支援を頂いたことをここに記しておく。

６．まとめ

学内限定サービスであるホスティングサービスを利用した新サーバ構築と，運用方法や過去に遭遇した不具合に関して記載した。サーバ購入という初期投資が不要なので今後このサービスの利用者も増加すると考える。

一方運用面では，学内専用サーバとはいえさらなるセキュリティ対策を要求されるので，管理技術の更新・向上が必要になる。今後も情報センターと連携してサーバ運用を実施して行く。

参考文献

[1] http://e-words.jp/w/ホスティングサービス.html
[2] http://rpms.famillecollet.com/
[3] https://fedoraproject.org/wiki/EPEL/ja
[4] http://www.asial.co.jp/jpgraph/
[5] http://www.asial.co.jp/jpgraph/download.php
[6] http://itmemo.digi2.jp/allCont/centos63/Centos63RsyslogSetting.html
[7] https://certs.nii.ac.jp/
[8] https://ja.wikipedia.org/wiki/TCPやUDPにおけるポート番号の一覧
[9] http://sonic64.com/2004-11-17.html
[10] http://www7b.biglobe.ne.jp/~shikabo/140.html