サブドメインを運用するサーバの構築と管理

宮崎大学工学部教育研究支援技術センター
森　圭史朗

はじめに

学内では、総合情報処理センターに学科や講座単位のグループでサブドメインを登録することで、そのグループ独自のドメイン名を使用した DNS、メール、Web 等のサーバを構築し、運用することができる。サブドメインの管理・運用は、大学の情報セキュリティポリシーに基づき、そのドメインを管理するグループの責任で行うことになる。従って、外部からサブドメインへの不当なアクセスや攻撃に対する対策等は、ドメイン管理・運用者の責任で行い、サブドメインの内部から外部に対して不当なアクセスやその他の迷惑を及ぼす行為が行われないように運用することが必要となる。また、サブドメイン管理者は、トラブルが発生しないように日頃からログのチェックや保守管理作業も必要である。

そこで、学内でサブドメインを運用・管理するためのサーバの構築と管理について報告する。

キーワード：ネットワーク、ドメイン、サーバ

1. 目的

各サブドメインを管理しているサーバは、学科や講座によって提供されるサービスが異なっている。本稿では、学内でサーバとして多く利用されている Solaris の最新版（Solaris9_x86）用いて、各サブドメインで運用されているサーバ（DNS、メール、Web）の構築時の設定と日常のサーバ管理について述べる。また、サーバ構築や運用の際に必要なセキュリティ対策についても述べていくことにする。

2. ドメインとサーバの概念

2-1 DNS について

DNS とは、Domain Name Service の略で、IP アドレスとコンピュータの名前の変換を行う。ドメイン名から IP アドレスに変換することを「正引き」といい、逆に、IP アドレスからドメイン名に変換することを「逆引き」という。DNS のドメインはツリー状の階層構造に構成され、各ドメインにドメイン名が付けられる。インターネットでサービスを提供するメールサーバや Web サーバをはじめ、インターネットに接続されているすべてのマシンは、図 1 のようなドメインのツリー構造のどこかに位置付けられ、ドメイン名を使ってインターネット内のホストを選別する。

2-2. サブドメインとは

サブドメインとは、その言葉が示すとおり、あるドメインより下の階層にあるドメインのことという。例えば、「fuji.teng.miyazaki-u.ac.jp」というドメイン名の場合、「miyazaki-u」は「ac.jp」ドメインのサブドメインであり、また、「teng」は「miyazaki-u.ac.jp」ドメインのサブドメインとなる。

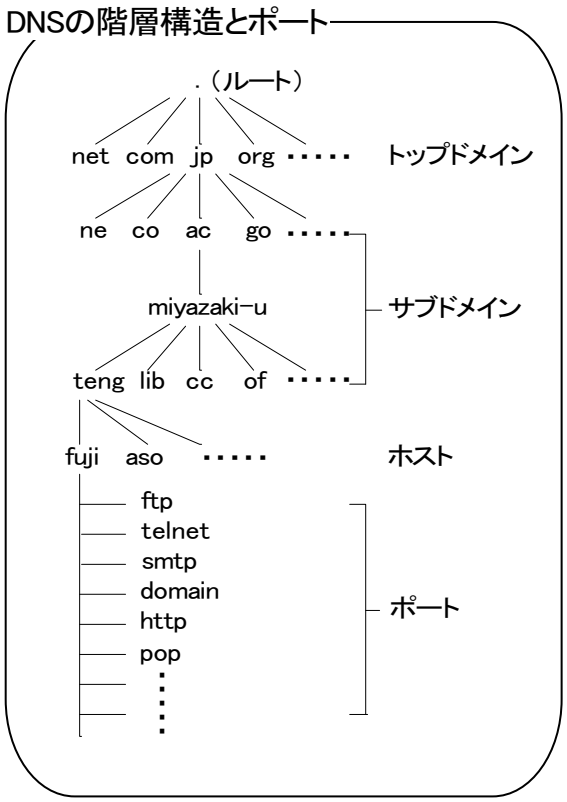

図 1

例）fuji.teng.miyazaki-u.ac.jp
［コンピュータ名］.［サブドメイン名］.［サブ

ドメイン名].[サブドメイン].[トップドメイン名]

2-3. ポートについて

図1にあるポートとは、インターネット上の通信において、複数の相手と同時に接続を行うために IP アドレス（ホスト）の下に設けられたサブアドレスのことをいう。ポートには、TCP と UDP があり、それぞれ 0～65535 までの数字がある。0～1023 までの TCP や UDP は、ftp の場合は tcp の 21 番、telnet の場合は tcp の 23 番というように各ポートで使用されるソフトウェアが決められている。

3. Solaris9_x86 のインストールについて

3-1. インストール前における注意点

Solaris9_x86 は、Linux や FreeBSD 等に比較して対応するハードウェアが少ないので注意が必要である。以下にある Sun の Web サイトを参考に、インストールするマシンのハードウェアがサポートされているか確認する。

HCL（Hardware Compatibility List）

http://www.sun.com/bigadmin/hcl/data/9/

基本的に、マザーボード、LAN カードは、intel のチップを搭載したものを使用し、ビデオカードは、ATI や Matrox 製の AGP や PCI を使用すると問題なく認識する。

3-2. スライス配置

Solaris のインストール時にスライス配置を自動配置にすると、OS のスライス構成は「/」、「swap」、「/export/home」の 3 つで構成されるので、表1のような使用目的別に分けて配置する。

表１　スライス配置の例

作成するスライス	使用目的
/	ファイルシステムの起点
swap	スワップ領域
/usr	ユーザーコマンド、システムコマンドなど
/var	システムログ、メールなど
/opt	アプリケーション
/export/home	一般ユーザー用のホームディレクトリ

3-3. OS 以外で必要なソフトウェア

Solaris では、Linux や FreeBSD と違い、コンパイラがインストールされていない。Solaris でソフトウェアをソースからインストールするためにコンパイラ「gcc」をパッケージよりインストールする。パッケージは、東京理科大の SunSite より入手できる。

導入するパッケージ　gcc-3.3.2

入手先

ftp://sunsite.tus.ac.jp/pub/sun-info/Solaris/intel/9/gcc3.3.2-sol9-intel-local.gz

4. サーバのセキュリティ対策

4-1. インストール直後の問題点

Solaris_x86 をインストールした直後の初期状態では、多くの TCP や UDP ポートが外部からアクセス可能となっている。サーバをさまざまな脅威から保護するためには、セキュリティ対策を行うことが必要である。そこで、次のような対策を行い、サーバのセキュリティ強度を高めることにする。

- 奨励・セキュリティパッチ導入
- inetd による不要なサービスの停止
- Tcp_Wrapper による inetd サービスのアクセス制限
- rc スクリプトによる不要なサービスの停止

4-2. 奨励・セキュリティパッチの適用

Solaris のインストールが完了した後、OS のバグやセキュリティ上の問題を修正するために奨励・セキュリティパッチを適用する。

奨励・セキュリティパッチは、Solaris9_x86 の場合、9_x86_Recommended.zip を以下のサイトから入手できる。

入手先

http://jp.sunsolve.sun.com/pub-cgi/show.pl?target=patches/summary&nav=pub-patches

パッチの適用方法は、シングルユーザーモードで unzip により 9_x86_Recommended.zip を展開し、9_x86_Recommended ディレクトリ内にある install_cluster を実行する。

4-3. inetd による不要なサービスの停止

inetd では、ftp や telnet など多くの TCP や UDP ポートが開かれる。inetd 経由で起動されるサービスは、/etc/inet.conf ファイルで設定する。管理業務において inetd によるサービスは、ftp と telnet

以外使用しないので、コメントアウト（「#」を行頭に付ける）して起動しないようにする。

/etc/inetd.conf の設定例

有効の場合

uucp stream tcp nowait root /usr/sbin/in.uucpd in.uucpd

無効の場合

#uucp stream tcp nowait root /usr/sbin/in.uucpd in.uucpd

4-4. Tcp_Wrapper によるアクセス制限

Tcp_Wrapper は、inetd の tcp で起動されるものに対してアクセス制限をかけることができるソフトウェアである。

導入するソフトウェア　tcp_wrapper-7.6

入手先

ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz

Tcp_Wrapper は、inetd から起動されるサービスを Tcp_Wrapper 経由で起動されるように設定する。

/etc/inetd.conf の設定例

変更前

telnet stream tcp nowait root /usr/sbin/in.telnetd in.telnetd

変更後

telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd

Tcp_Wapper は、/etc/hosts.allow と/etc/hosts.deny を用いてアクセス制限を行う。Tcp_Wrapper によるアクセス制限は、以下の順に適用される。

・hosts.allow で許可

・hosts.deny で拒否

・hosts.allow と hosts.deny になければ許可

例として、すべての inetd サービスを学内から許可し、学外から拒否する場合は以下のように設定する。

設定例

/etc/hosts.allow

ALL:133.54.0.0/255.255.0.0

/etc/hosts.deny

ALL:ALL

Tcp_Wrapper は、tcpdchk や tcpdmatch によりアクセス制限内容を確認することができる。Tcp_Wrapper を設定後または修正後は、アクセス制限内容の確認を行う。

4-5. rc スクリプトによる不要なサービスの停止

rc スクリプトによるサービスは、デーモンで起動される。rc スクリプトによりポートが開いているものは、/etc/rc2.d、/etc/rc3.d にある起動スクリプトファイルを起動しないようにすることでサービスを無効化することができる。

rc スクリプトより起動されるサービスの停止方法は、不要な起動スクリプトファイルの先頭に「.」や「_」など付けることでサーバブート時に起動しないようにする。以下に/etc/rc2.d/S80lp を例にした設定例を示す。

/etc/rc2.d/S80lp 無効化の設定例

S80lp　→　_S80lp

4-6. ポートの確認

4-3 から 4-5 までの対策を行った後、不要な TCP や UDP ポートが開いていないかを確認する。確認方法は、netstat やポートスキャンツールの nmap を利用して確認することができる。

・nmap-3.70

入手先

http://download.insecure.org/nmap/dist/nmap-3.70.tgz

5. 各ソフトウェアの導入について

5-1. DNS サーバの導入

ネットワーク上でメールや Web などのサービスを利用するためには、ドメイン名と IP アドレスの名前解決を行うことが必要になる。この名前解決のサービスを提供するのが DNS サーバである。DNS サーバは、bind-8.4.4 を導入することにする。

導入するソフトウェア　bind-8.4.4

入手先

ftp://ftp.isc.org/isc/bind/src/8.4.4/bind-src.tar.gz

bind を稼働させるために必要な設定ファイルは、named.conf とゾーンファイルの 2 種類ある。named.conf ファイルは、bind の動作を設定し、ゾーンファイルは、ドメインの管理するホスト一覧を定義する。

設定に必要なゾーンファイルの種類

・localhost アドレスの逆引きファイル

localhost の逆引きを設定する。

・ルートキャッシュファイル

ルートサーバ一覧のキャッシュファイルである。ルートキャッシュファイルが更新された場合は、以下のいずれかのサイトか

ら入手する。

ftp://ftp.internic.net/domain/named.root

ftp://rs.internic.net/domain/named.root

・正引きゾーンファイル

管理するドメイン内のサーバ情報をドメイン名から IP アドレスに変換する。

・逆引きゾーンファイル

正引きと逆の変換を行う。（逆引きゾーンファイルが他の DNS サーバにある場合は不要）

DNS サーバは、基本的にアクセス制限をかけないが、外部にドメイン内の情報をすべて見せる必要はないので、named.conf ファイルにより次の 3 つの対策を行う。

・ゾーン転送は、スレーブサーバのみにする

・再帰的な問い合わせは、外部からは禁止する

・バージョン情報は、公開しない

OS が DNS クライアントとして名前解決を行えるようにするためには、nsswitch.conf と resolv.conf ファイルを設定する必要がある。

DNS クライアントの設定に必要なファイル

・nsswitch.conf

OS がホスト検索に DNS を使用できるようにする。

・resolv.conf

使用する DNS サーバを指定する。

5-2. メール環境の構築

ユーザーが、メールを利用するには sendmail と qpopper が必要である。

sendmail は、外部のメールサーバからメールを受信したり、ユーザーから送信されるメールを宛先のサーバへ送信することを行い、qpopper は、サーバに送られてきたメールをユーザーが受信するためのものである。

メールサーバは、sendmail-8.13.1 を導入することにする。

導入するソフトウェア　sendmail-8.13.1

入手先

ftp://ftp.sendmail.org/pub/sendmail/

sendmail.8.13.1.tar.gz

メールサーバを導入する上で必要なセキュリティ対策は、次の 3 つである。

・外部からのメールを中継させない

・バージョン情報を公開しない

・メールのメッセージサイズを制限する

メールサーバの設定ファイルは、/etc/mail ディレクトリ以下にある。

設定が必要なファイル一覧

・sendmail.cf

・local-host-names

・access

・DNS のマスターゾーンファイル

外部からのメール中継を禁止する設定は、access ファイルで設定し、バージョン情報とメールのメッセージサイズの制限は、sendmail.cf で設定する。sendmail.cf ファイルは、sendmail 付属の sendmail.mc ファイルから作成する。

POP サーバは、qpopper-4.0.5 を導入することにする。

導入するソフトウェア　qpopper-4.0.5

入手先

ftp://ftp.qualcomm.com/eudora/servers/unix/

popper/qpopper4.0.5.tar.gz

qpopper のパスワード認証は、システムの平文パスワードで行うため、学外からのアクセスは避けるようにする。設定は、Tcp_Wrapper 経由で inet に追加し、Tcp_Wrapper によりアクセス制限を行う。

/etc/inetd.conf へ以下を追加する。

pop3 stream tcp nowait root /usr/sbin/tcpd

/usr/local/sbin/popper

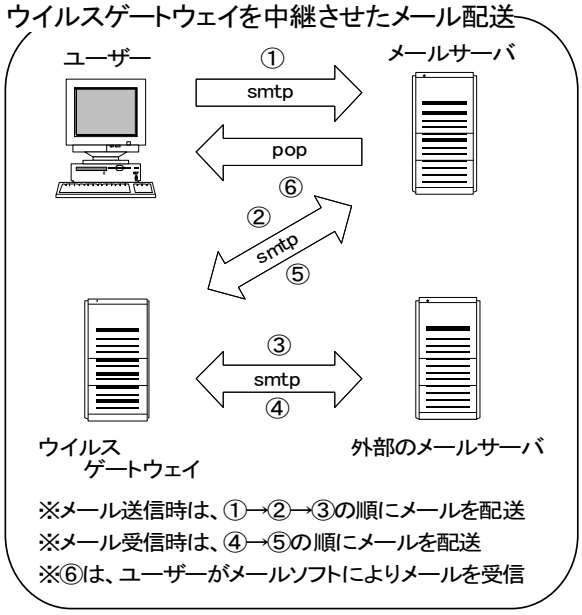

図２

ウイルスメール対策

パソコンのウイルス感染原因のほとんどはメールによる感染である。メールによるウイルス感染を最小限に押さえるため、総合情報処理センタ

ーのウイルスゲートウェイ２台を利用する。図２のようにメールの送受信を行う場合は、DNS の MX と sendmail.cf の設定によりウイルスゲートウェイを中継させるようにする。

5-3. Web サーバの導入

Web サーバは、apache-1.3.31 を導入することにする。

導入するソフトウェア　apache-1.3.31

入手先

http://www.apache.org/dist/httpd/apache_1.3.31.tar.gz

apache は、Netscape Navigator や Internet Explorer などの Web ブラウザでホームページを見ることができるようにするものである。apache を設定する上で必要なセキュリティ対策は次の通りである。

・サンプルの CGI プログラムは無効にする

・バージョン情報を公開しない

apache の設定は、httpd.conf で行い、外部に公開したくない部分は、.htaccess や access.conf ファイルでアクセス制限を行う。また、CGI や SSI 機能を利用した動的コンテンツは、セキュリティ上の問題を発生させてしまう可能性があるので、利用する場合は、最低限必要なディレクトリのみで実行可能にするなどの対策が必要である。

設定が必要なファイル

・httpd.conf

5-4. サーバ時刻の同期

ネットワーク管理を行う場合、サーバの時刻を正しい時刻に同期しておく必要がある。もし、サーバにトラブルが発生した場合、ログの時間が正確でないとログを解析するのが非常に困難になる。従って、ログ出力時間の信憑性を持たせるため、総合情報処理センターの NTP サーバとサーバの時刻を同期するようにする。サーバ時刻の同期は、Solaris 付属の xntpd を用いることにする。

設定が必要なファイル

・ntp.conf

5-5. 無停電電源について

無停電源装置（UPS）とは、落雷等による過電流に対しての保護や停電によるサーバへの電力を供給する予備電源である。また、無停電源装置（UPS）用の電源管理ソフトウェアを導入することで、長期間の停電に対してサーバを自動でシャットダウンできるようになる。

UPS： Smart-UPS

電源管理ソフトウェア： apcupsd-3.10.15

入手先

http://prdownloads.sourceforge.net/apcupsd/apcupsd-3.10.15.tar.gz

設定が必要なファイル

・apcupsd.conf

6. ログの管理

6-1. ログとは

/var ディレクトリ以下にあるログファイルには、サーバ起動時に検出したハードウェア情報や各種ソフトウェアに関する情報などが出力される。ログは、サーバを管理する上で非常に重要なメッセージとなるので、ログ出力は、できるだけ多くの情報を出力し、不要な情報の出力を停止するように設定を行う。また、いつトラブルが発生するかはわからないので、ログのチェックは定期的に行うようにする。

6-2. ログ出力の設定

UNIX 系 OS では、ログは syslogd デーモンでログ出力が行われており、/etc/syslog.conf ファイルによりログ出力の種類と重要度を設定する。syslog.conf の基本構文は、以下に示す。

[ファシリティ].[メッセージレベル]<TAB> [アクション]

syslog.conf で用いられるファシリティとメッセージレベルについての一覧は、表２、表３に示す。

表２　ファシリティ一覧

ファシリティ	利用するプログラムの種類
auth	認証に関するプログラム
cron	cron による処理
daemon	各種デーモンプログラム
kern	カーネル出力
lpr	プリンタデーモン
mail	メールプログラム
mark	syslogd によるタイムスタンプ
news	NEWS システム
syslog	自分自身に関する出力
user	一般のユーザープログラム
uucp	UUCP プログラム
local0-7	任意のプログラムで使用可

表３　メッセージレベル一覧

レベル	意味
emarg	パニック発生
alert	緊急事態（システム破損）
crit	危険状況（ハードウェア障害）
err	通常のエラー
warning	警告メッセージ
notice	通知メッセージ
info	一般的な情報
debug	デバッグメッセージ
none	メッセージを出力しない

6-3. ログファイルのローテーション

ログファイルを放置した場合、時間が経つにつれて肥大化し、ディスク資源を浪費してしまう。ログローテーションは、一定の条件（サイズ、時間など）でログを別ファイルにバックアップしたり、圧縮したりする。apache などのログファイルは、放置すると肥大化するので、Solaris9 から追加された logadm を用いてログファイルのローテーションが行われるように設定する。

7. サーバ運用に必要な作業

7-1. 作業内容

サーバのセキュリティを維持するには、定期的な作業が必要になる。定期的な作業については以下の通りである。

・奨励・セキュリティパッチの適用
・各ソフトウェアの脆弱性への対策
・バックアップ

7-2. 定期的な奨励・セキュリティパッチの適用

サーバ構築時にセキュアなサーバを構築したとしても、新たな脆弱性が発見されれば、一転して脆弱なサーバとなってしまう。そこで、Solaris のバグや脆弱性に対してパッチを適用することにより修正する必要がある。奨励・セキュリティパッチの適用方法は、3-4 で述べたとおりである。ここで注意すべきことは、パッチ適用が原因で無効化した rc スクリプトが起動するようになっていたり、設定ファイルの内容が初期設定に戻っている場合がある。パッチ適用後は、提供されるサービスが以前と変わりがないか確認することを忘れないようにする。

7-3. ソフトウェアの脆弱性への対策

以下のセキュリティ情報サイトに掲載されるセキュリティホールは、早急に対策を行う必要がある。この情報サイトにサーバで使用している OS やソフトウェアのセキュリティホールが確認された場合は、該当するソフトウェアにパッチを適用するか、対策済みのバージョンに更新するようにする。

・情報処理推進機構　セキュリティセンター
　http://www.ipa.go.jp/security/
・JPCERT CC
　http://www.jpcert.or.jp/

7-4. バックアップについて

個人データやメールスプールは、トラブルによるハードディスク破損で失ってしまうことの無いよう定期的にバックアップをとっておく必要がある。バックアップは、バックアップ用スクリプトを作成し、定期的に crontab を実行してデータのバックアップをとるようにする。

8. 終わりに

サブドメイン管理者は、セキュアなサーバを構築するだけでなく、サーバを維持するための保守・管理作業も重要である。ネットワーク関連のセキュリティホールは、小さいものから含めると毎日のように報告されている。管理者は、その中でも対策が必要なものを選択し、OS やソフトウェア等の更新を行わなければならない。従って、管理者は、日頃からサーバのセキュリティ対策と新しいバージョンのソフトウェア導入方法などの技術力を上げる努力が必要である。また、サーバ運用の際は、外部にサーバ情報をできるだけ公開しないようにすることで、不正アクセスを未然に防ぐ対策も重要である。

参考文献

[1]　城谷洋司　Solaris システム管理　アスキー
[2]　中村敦司、新城靖、西山博泰、林謙一、他
　新 The UNIX Super Text【上、下】技術評論社