

LPI-Japan 主催 LPICレベル2技術解説無料セミナー

スキルブレイン株式会社 所属OSS研修専任講師
コムソリュート株式会社 代表取締役兼CEO
大崎 茂



- 最近のLPICレベル2受験に必要なとされる知識・技術について
- 出題範囲全般における受験のポイントについて
- LPICレベル2における主要サーバソフトウェアへの取り組み方、考え方



A.LPICレベル2は、一体どれ位難しい試験なのか？

1) かなり難しくなった、問題の改変毎に難易度が増す。

Linuxの応用的なシステム管理やサーバ構築ができる知識
オペレーションレベルの知識 から 技術の根本的な理解へ

小中規模システムの管理者
小規模ネットワークの企画、
導入、維持、トラブルシュー
ティング

LAN server
Internet Gateway
Internet Server

2) ちょっと、ひねくれているモノも見受けられる。

普段利用しないようなオプションや滅多に利用しないオペレーションが問題となることも見受けられる
コマンドは必ずLinuxのオンラインマニュアルを確認する必要がある。



B. LPICレベル1とレベル2との差はどのくらい？

1) レベル1に必要とされる知識の2倍くらいの深さ。

たとえばコマンドは単一の機能を覚えるだけではなく、同じ様な機能を持つコマンドも必ずチェックする

試験対策テキストだけではなく、オライリー本などに目を通す必要がある。

2) それぞれの知識の複合形(広さ)を求められる。

たとえばカーネルのバージョンとモジュールの関係、カーネルが適切なモジュールを特定する仕組みにバージョンが関係している等、様々な知識の点と点を結び付けて線にすることが重要。



B. LPICレベル1とレベル2との差はどのくらい？

3)机上での勉強には限界があり、レベル2は必ず実機での実践が必要。

Level1では、実践がなくてもある程度覚える力があれば合格レベルを得ることは可能だったが、Level2はコマンド以外にサーバ等のマネージメントに関するスキルを試される為、実践は必須と考えるべきである。



201の試験範囲-1

201:Linuxカーネル

- 1) カーネルの構成要素
- 2) カーネルのコンパイル

カーネルのコンパイルの手順、.configファイル、makeのターゲットの違い、特にoldconfigの特殊性など

Initrdの意味をよく理解し、Initrdの中身がどういう構成になっているかを確認する。
併せて、cpio、gzip、unzipなどのコマンドの連携もチェック。

Initrdの覗き方の例、

Kernel2.4の場合、

```
# cp /boot/initrd /tmp/initrd.gz
```

```
# gunzip initrd.gz
```

```
# mount /tmp/initrd /mnt/ -o loop
```

Kernel2.6の場合、

```
# cp initrd.img initrd.gz
```

```
# gunzip initrd.gz
```

```
# cat initrd | cpio -i
```

Initrd(initramfs)はシステム起動時に、カーネルによってメモリー上に展開されるRAMディスク・イメージ。ハード・ディスクを備えないマシン上でもLinuxが利用できるようにするための仕組み。作成および内容の確認方法も合わせて理解を必要とする。

3) カーネルへのパッチ適用

パッチのオプションを理解する



201:Linuxカーネル

4) カスタムカーネルおよびカーネルモジュールのカスタマイズ、構築、インストール

カーネルとモジュールの連携の仕組みを理解する。カーネルバージョンとモジュールのインストールディレクトリ名の関係を理解する

`/usr/src/linux`内のMakefileの先頭の4行で構成されるカーネルの version
`/lib/modules/version`

カーネルのインストール方法を理解する。

5) 実行時におけるカーネルおよびカーネルモジュールの管理/照会

モジュールのロード、アンロードのコマンド、併せてKMODの仕組みを各コマンド、ファイルによる連携として仕組みを理解する。

つまりmodprobe, depmod, modules.dep, /etc/modprobe.conf等



202:システムの起動

1) システムの起動とブートプロセスのカスタマイズ

/etc/inittabの書式の特徴、アクション指示子はしっかり理解する。
ctldelなど/proc/以下のカーネルパラメータと関連するものもあるので
関連を深く理解する。特にrespawnアクション指示子の設定されているTTY(仮想ターミナル)の設定を
起動runlevelと共に理解を必要とする。

```
1:2345:respawn:/sbin/mingetty tty1
```

```
·  
·
```

サービスの起動に関わるルール、ファイルの仕組み、コマンドを理解する。

```
/etc/init.d/*
```

```
/etc/rc.d/*
```

```
chkconfig
```

```
等
```

2) システムを回復する

リカバリーモードの手順を理解する。

ブートローダの仕組み、起動のパラメータを理解する。

設定ファイルのフォーマットを理解する。/etc/lilo.conf および /boot/grub/grub.conf (menu.lst)

bootセクタを含むデバイス名とrootファイルシステムのあるデバイス名の設定、defaultの設定など



203:ファイルシステムとデバイス

1) Linuxファイルシステムを操作する

/etc/fstabの書式、特にマウントオプションはよく理解を必要とする。

例、`async - sync , atime-noatime, exec - noexec , user, users, nouser`

ループバックデバイス

ファイルを、あたかもハード・ディスクなどのブロック型デバイスのように扱うための機能。パソコン上でイメージ・ファイルを直接操作したい場合などに用いる。

マウントオプションはループバックデバイス(-o loop)、NFSを関連させて理解する必要がある。同じく/etc/mntabの用途、/proc/mountsの意味、

swap関連コマンド、特にddコマンドを利用したswap領域を作る手順をよく理解する。

`dd if=/dev/zero of=/tmp/swapfile bs=1024 count=5120000; mkswap /tmp/swapfile`

2) Linuxファイルシステムの保守

ファイルシステムの構築に関わる手順を理解する。

同じように現状のファイルシステムの状態を把握する手段を理解する。

mke2fs、dumpe2fs、tune2fsはオプションを含めて確実に理解する。

特にファイルシステムの構造であるブロックグループ、iノード、スーパーブロックを関連させて理解する必要がある。

ハードリンク、ソフトリンクの根本的な理解も必要であり、コマンドラインのフォーマットをよく覚えておく



203:ファイルシステムとデバイス

3) ファイルシステムを作成してオプションを構成する

オートマウントの設定を設定ファイルの書式を併せて理解する。
CDRWなどのファイルシステムの構築コマンドの利用方法、また古いカーネルでの制限
つまりideデバイスをscsiデバイスとして使う仕組み等の理解。

4) udevでのデバイス管理

udevによって動的に管理されるデバイスファイルの仕組み、udevinfoコマンド
および /etc/udev/rules.d以下の設定ファイル



204:高度なストレージ管理

1) RAIDを構成する

RAIDの各タイプと必要なディスク容量の関係、ソフトウェアRAIDの構築方法を手順を含めて理解する。

2) 記憶装置へのアクセス方法を調整する

hdparm等のコマンドの理解。

PIO(programmed I/O)モードとDMA(Direct Memory Access)モードの切替

3) 論理ボリュームマネージャ

LVMの構築の手順、ならびにvgextend, vgreduceなどのメンテナンスコマンド全般を理解する。
RAIDとの組み合わせパターンを理解する。例 LVM over RAID5



201の試験範囲-5

205:ネットワーク構成

- 1) 基本的なネットワーク構成
- 2) 高度なネットワーク構成とトラブルシューティング
- 3) ネットワークの問題を解決する

ネットワーク構成時に使われるそれぞれのファイルの目的等を理解する必要がある。
Redhat系とDebian系両方のトラブルシュートに使われるコマンド類を理解しておく
参考書「ネットワークトラブルシューティングツール」オライリー発行

route、netstat、ifconfig、tcpdump等のコマンドの理解

```
# ifconfig eth0:1 192.168.1.10 / ifconfig eth0:sub1 192.168.1.10  
# tcpdump -nli eth1 'udp'  
# tcpdump -nli eth1 'icmp'
```

サーバとの連携で影響のあるファイルの理解、
resolv.conf の書式
nsswitch.conf
等

- 4) システム関連の問題をユーザに通知する

/etc/issue、/etc/issue.net、/etc/motd、wall、/sbin/shutdown などオプションも含め理解が必要



201の試験範囲-5

206:システムの保守

1) ソースからプログラムをmakeしてインストールする

Level1の内容を復習する必要がある。
インストールプロセスとパーミッションの関連等も併せて理解すること。

2) バックアップ操作

tarコマンドの用途、オプション、書式などよく理解する。その他バックアップに利用できるコマンドは一通り理解する必要がある。
ext2もしくはext3用ではあるが、dumpとresoreコマンドも理解をする。

207:ドメインネームサーバ(後述)



202の試験範囲-1

208: Webサービス(後述)

209:ファイル共有

1) Sambaサーバの設定

ウィンドウズのネットワーク環境下での「共有」に関連する設定。Linuxのユーザ認証とSambaのユーザ認証の差異を、仕組みの面と具体的な同期等の設定・手順の両方をよく理解する。Sambaに関する専門書を読む必要がある。

2) NFSサーバの設定

デーモンの構成 portmap , nfsd , mountd

NFSの設定ファイル/etc/exportsファイルの設定フォーマット、

とくにroot権限でネットワークにアクセスするパーミッションなどをよく理解すること。

さらに、ソフトマウント、ハードマウントの違いを理解し、マウントオプションの内容も整理する必要がある。



202の試験範囲-1

210:ネットワーククライアントの管理

1) DHCPの設定

dhcpd.confファイルの設定を理解すること、特にsubnetの設定方法に注意すること。

2) PAM認証

設定ファイルならびにpamモジュールの格納場所(/lib/security)などの動作環境に関する理解が必要。実際の設定ファイルを読解するトレーニングも必要。

モジュールタイプ + コントロール + モジュールのパス、引数のフォーマット

・モジュールタイプ auth (ユーザ認証のタイプ), account(ユーザ認証を確認する、期限切れなど), password(パスワードの設定と変更を使う), session(ユーザ認証の前後の処理の設定、ログインのログ、ディレクトリのマウントなど)

・コントロール requisite,required,sufficient,optionalの違い

特に、requisiteとrequiredの使い方、特徴を理解する。requiredは同じタイプのモジュールの実行がすべて終わってから認証を拒否する。requisiteは失敗すると直ちに終了する。

3) LDAPクライアントの利用方法

LDAPの用語(DN,LDIFなど)を理解する。設定ファイルslapd.confの主要なディレクティブの記述は理解する。

特にslapd.conf内の rootdn “cn=root,dc=example,dc=com” の設定書式

ldapsearch、ldapadd、ldapdelete、ldappasswd等のクライアントコマンドは一通り覚える必要がある。



202の試験範囲-2

211:電子メールサービス(後述)

212:システムのセキュリティ

1) ルータを構成する

iptablesによるNAT、IPマスカレードの設定などを理解する。

```
#iptables -A INPUT -j LOG --log-prefix "ここに書き出すコメントを入れる "  
#iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j SNAT --to 12.34.56.78  
#iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -j MASQUERADE
```

/proc/sys/net/ipv4/ip_forwardカーネルパラメータとの関連、さらに設定の方法を理解する。
応用として、サービスとポートの関係を理解する。

2) FTPサーバの保護

anonymousFTPサーバを構築する場合の注意点を理解する。

/etc/ftppusersの目的、vsFtpdなどのchroot機能、chroot jailを施した場合の検証など

3) セキュアシェル(SSH)

sshd_confの設定は全般をきちんと理解をする。公開鍵方式の仕組み、鍵の生成、保管(パーミッション等)を理解する。さらにsshを使ったポート転送を理解する必要がある実機を使ったトレーニングが必要。

例、

秘密鍵ファイル~/.ssh/identityのアクセス権設定600とする、X接続の転送を許可する場合X11Forwarding yes



4) TCPラッパー

スーパーサーバの理解が必要。TCP_Wrappersは2つのファイルで管理する、つまり/etc/hosts.allow、/etc/hosts.deny、このファイルの書式を理解する。特に関連する主要なサーバ名をチェックする。

5) セキュリティ業務

セキュリティ用のツールの名称と用途は一通り理解する。さらに実戦的なnetstat、lsof、fuser等の使い方を理解する。

netstatはいろんな場面で使われているネットワークの状態を把握するコマンド、オプションが多く、なるべく詳しく覚えておく必要がある。



202の試験範囲-3

213:トラブルシューティング

1) ブート段階の識別とブートローダのトラブルシューティング

ブートローダ (lilo、GRUB) の違いを理解する。それぞれのブートローダの起動プロセスの理解が必要、さらにブートローダのオプションとその働き。201の範囲にある202:システムの起動1)システムの起動とブートプロセスのカスタマイズと併せて理解をすること。

例として、liloは、grubと違い物理的なディスク上の位置情報が必要なので、その位置に整合性が無いと起動できないトラブルが起きる、つまりmapファイルの更新の必要性を理解する。
またブート時の、それぞれのエラーメッセージに対してのトラブルシューティングをよく理解する。

2) 一般的な問題を解決する

サーバとログの関係も重要であり、どのサーバはどのログファイルをチェックすればいいのか？そのログから得る情報等の知識、運用の実践的なトレーニングが必要な部分でもある。

3) システムリソースの問題を解決する

dmesg、/sbin/lspci、/usr/bin/lshw、strace、ltrace、lsusb等のコマンドを理解する。

単独ではなく他の項目と複合的に理解する必要がある。

/proc以下のカーネルパラメータのうちシステムリソースにかかわる内容は把握しておく必要がある。

例、USBデバイスの状況を確認するためのファイル /proc/bus/usb/devices

4) 環境設定の問題を解決する

単独での項目ではなく他の内容と複合的に理解する必要がある。



スーパーサーバに関して -1

A.スーパーサーバ経由で起動するサービスとデーモンの関係を整理する

スーパーサーバを使う理由、デーモンを使う理由をよく理解する。

1) xinetd.dディレクトリ以下のファイルの設定項目の把握

各サービス用の設定ファイル内の設定値

たとえばaccess_times等

2) TCP_WRAPPERSとの関係を理解する

xinetdとlibwrapライブラリ

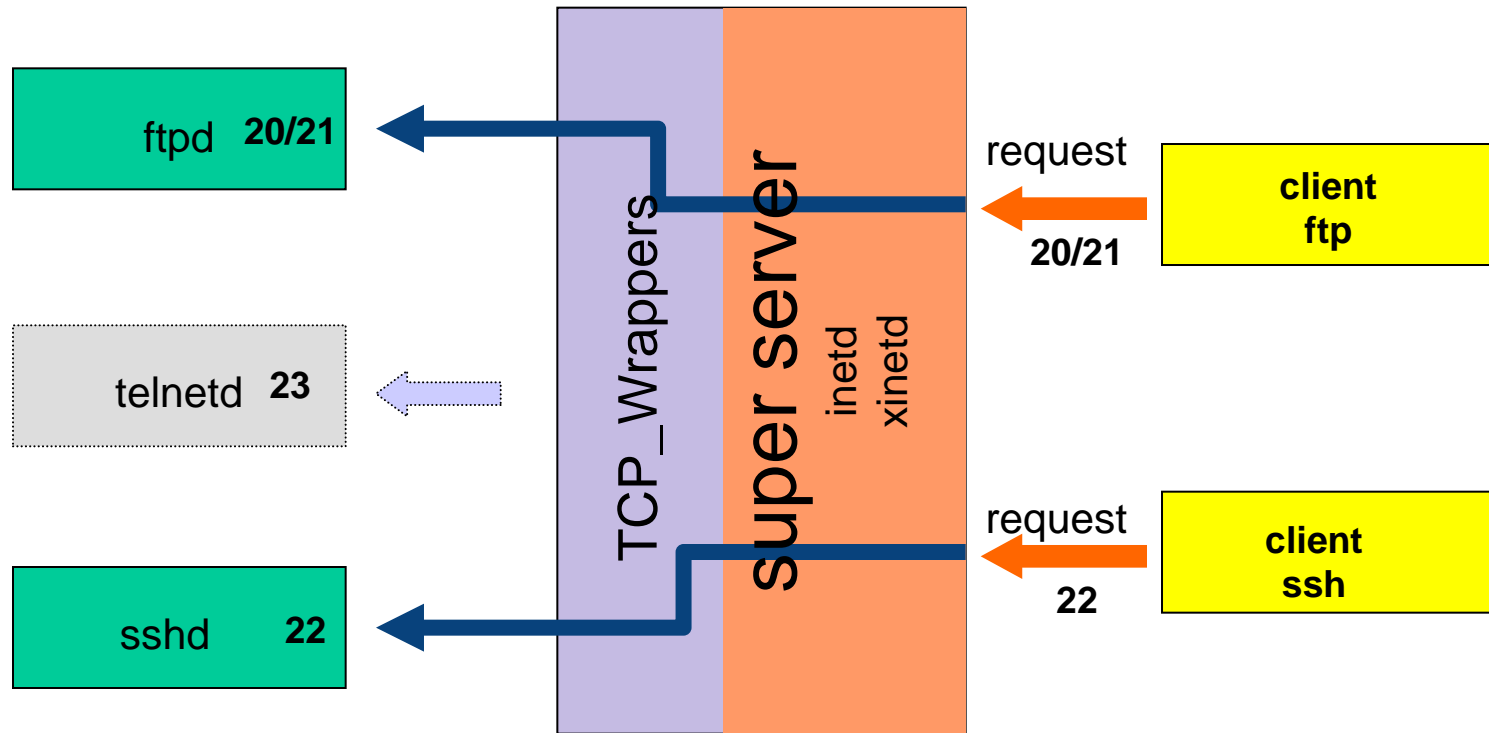
/etc/hosts.allowと/etc/hosts.denyの書式も併せて理解する(※ワイルドカードの使い方)

特に主要なサーバを設定する場合の、デーモン名を理解する。

例えば、nfsはportmap、telnetはin.telnetd等、特殊なものは覚えておく必要がある。



スーパーサーバに関して -2



/etc/hosts.allow
/etc/hosts.deny



スーパーサーバに関して -3

inetd.conf / xinetd.conf ならびに xinetd.d以下の設定

#の付加でサービス行を無効にする。



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

```
service telnet
```

```
{
```

```
  disable= no
```

```
  flags= REUSE
```

```
  socket_type= stream
```

```
  wait= no
```

```
  user= root
```

```
  server= /usr/sbin/in.telnetd
```

```
  log_on_failure += USERID
```

```
  access_times : 20:00-22:00
```

```
}
```

← no : 有効にする
yes: 無効にする

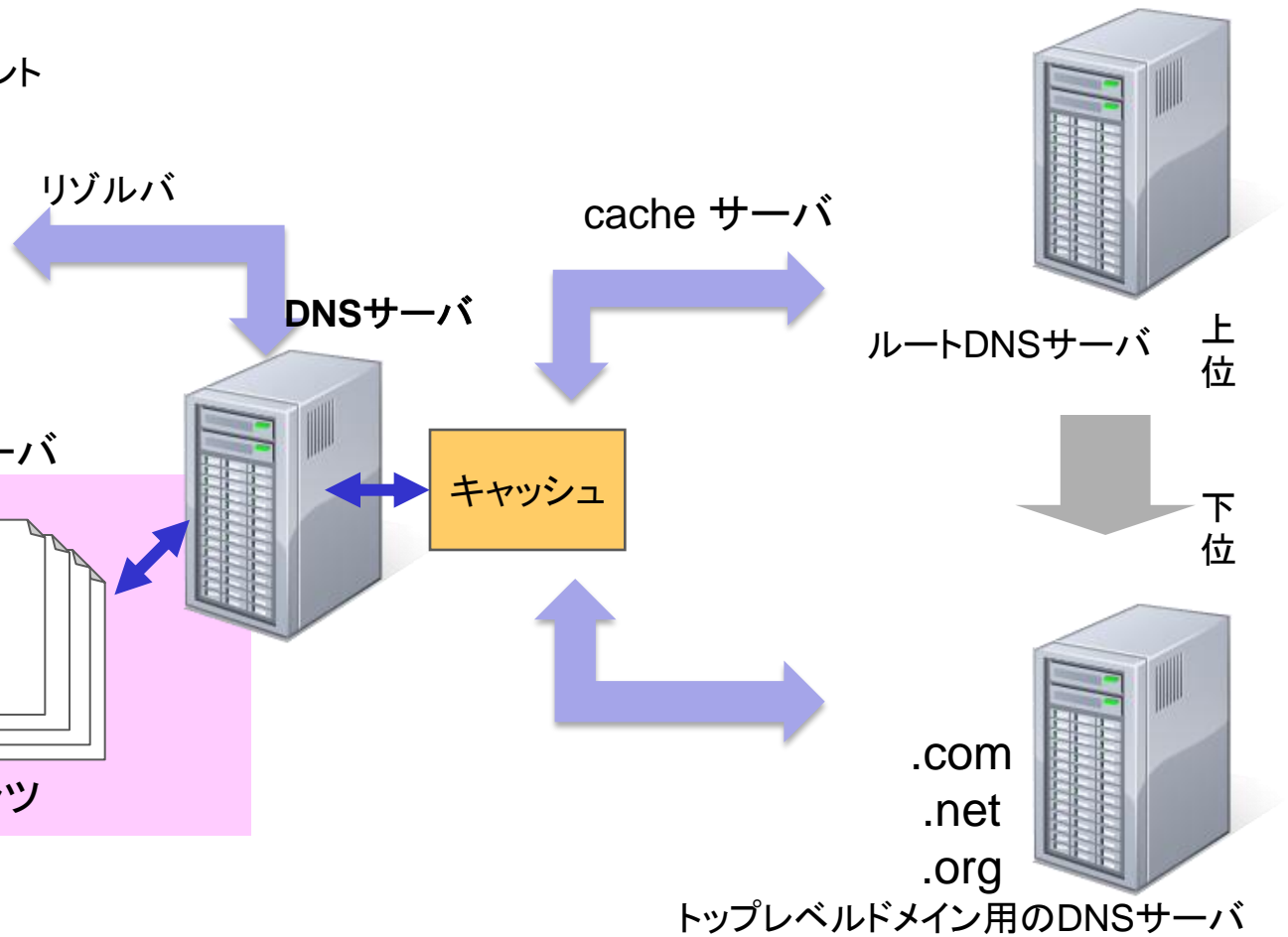
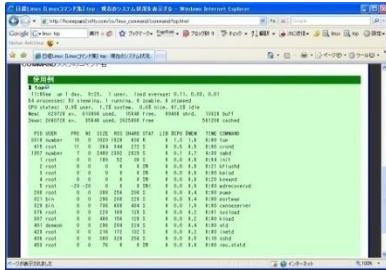
← 時間制限



DNSサーバに関してー 1

xxx.yyyy.com.

ブラウザなどのクライアント





A. ネットワーク環境との関連を整理する

1) /etc/resolv.confの役割

どのDNSサーバをつかって名前解決を行うかを決める入口のファイル、/etc/nsswitch.conf内の優先順位も考慮する事

B. DNSに関して

1) キャッシュサーバとしての役割を検証する

2) そこに関連するoptionsステートメントの役割を整理する

ルートネームサーバから順番に問い合わせを行いサーバの場所を検索する動作は再帰的という言葉を使って表現されます。その再帰的な動作がキャッシュサーバとしてのDNSの動きにどういう影響があるか？
allow-query、allow-recursion、recursion、forward、forwarders等

悪意を持ったアクセスもしくは攻撃があった場合に、どう対処するかの特ラブルシューティングも含むと考えた方が良いでしょう。

3) マスタサーバ、スレーブサーバの違いを理解する

allow-update、allow-transfer等、named.confとゾーンファイルの記述に関してマスタとスレーブ間でゾーン転送を行うしくみとその安全性を理解する、その具体的なnamed.confでの記述はどうするのかをよく理解する必要がある。



4) DNSSEC、TSIGの目的を理解する

それぞれの用途を理解する。サーバ<>クライアント間で利用される仕組み=>DNSSEC、ホスト間やネームサーバー間でゾーン情報の認証を行う仕組み=>TSIG

5) chroot jailに関する理解

一般ユーザでのサービス起動、共有ライブラリへのアクセス等

6) メンテナンス、トラブルシューティング等

ゾーンファイルを編集し、CNAMEレコードを追加してファイルを閉じたが、ゾーン情報が他のDNSサーバに伝わらない。何をすればよいか？ -> SOAレコードのSerial値を増やす

ゾーンファイルの書式 -> FQDN記述の注意、`admin@lpic.example.com`.

digコマンドの使い方にも注意する。

digコマンドの結果には、クエリに掛った時間も出てくるのでDNSのパフォーマンスに関する情報も取得できる。



HTTPサーバに関してー 1

A. httpd.conf設定ファイル

1) Webサーバのパフォーマンスに関するディレクティブの理解

KeepAlive、MaxSpareServers、MinSpareServers、MaxClients等
数値を変更したことでどうなるのか？を検証し理解する事。

2) WebサーバとしてWebコンテンツを管理する構造に関するディレクティブの理解

DocumentRoot、UserDir、Alias、ScriptAlias等

NameVirtualHost、<VirtualHost ??></VirtualHost >、さらにDNSとの関連について

<Directory ??></Directory>、<Files ??></Files>、<Location ??></Location>

AccessFileName、Options

URLとサーバ内のローカルパスの関連を把握する、VirtualHostに関しては、一連の設定方法は実践で確認をする必要がある。Optionsに利用できるディレクティブを一通り覚える。

3) セキュリティに関しての理解

SSL関連のディレクティブ、Basic認証、Digest認証関連のディレクティブ

一連の設定方法は実践で確認をする必要がある。

また、htpasswdの使い方、オプションの特徴に関しても理解する。

4) squid プロキシサーバにおいて、

ACL関連を軸に理解を固める



HTTPサーバに関してー 1

5) その他

インストールによる設定ファイルの位置の違い

/etc/httpd/conf/httpd.conf

/usr/local/apache/conf/httpd.conf

MinSpareServers 5	リクエスト待ち可能な子プロセス最小起動数
MaxSpareServers 10	リクエスト待ち可能な子プロセスの最大起動数
StartServers 5	起動時の子プロセスの最小数
MaxClients	クライアント数の上限

Alias, ScriptAlias等を利用した場合のローカルなパスとURLの変換ルールをきちんと理解できているか？

UserDir site/html となっている時、

http://www.test.jp/~tom/index.htmlのファイルの実体をフルパスで記述

-> /home/tom/site/html/index.html

Perlに関して、CPANからモジュールをインストールする方法を理解する。

```
#perl -MCPAN -e shell
```

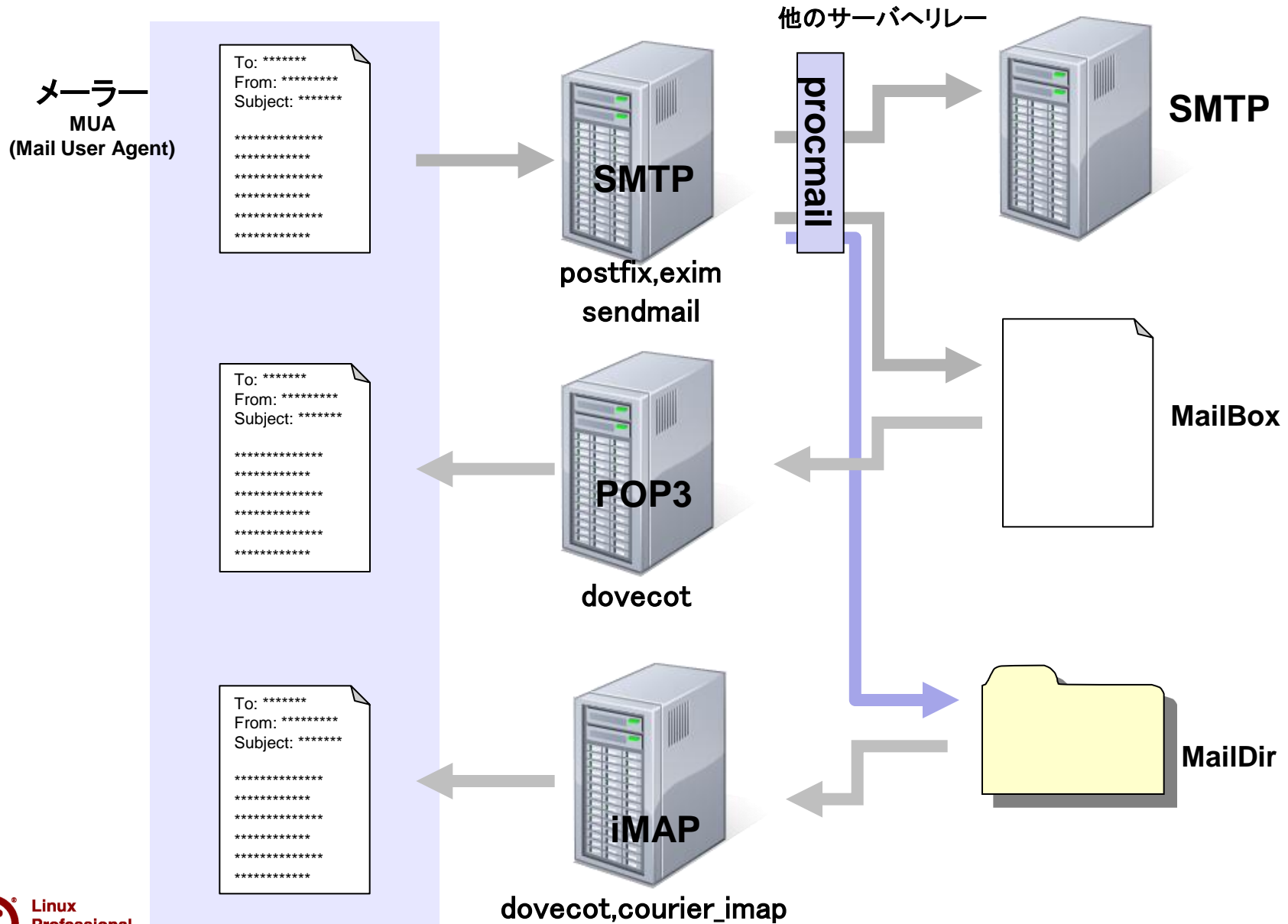
```
cpan>install Jcode
```

PerlモジュールAbc::defをインストールする方法として正しいものは

```
perl -MCPAN -e "install Abc::def"
```



Mailサーバに関してー 1





Mailサーバに関してー 2

A.Mailサーバに関して

1) postfixの設定ファイルの役割

main.cf と master.cf

それぞれのファイルの目的を理解する。とくにmaster.cfで設定する項目は一通り確認する必要がある。

2) postfixを構成するデーモンプログラムの役割

master、pickup、smtpd、cleanup、trivial-rewrite、qmgr、local、smtp、pipe、bounce

それぞれのデーモンの基本的な働きを覚える。特にキューの管理に関して

3) SMTPのtelnetを使ったテストを行う

25番ポートへ直接telnetを使ってメールの配信テストを実践にて、必ず確認する必要がある。

B.関連する機能に関して

1) procmailを実際に利用する

Mailサーバはサーバ本体より、そのMailサーバを取り巻く環境への理解度を求める傾向にある。

特にprocmail、aliasesの関連知識が重要。

procmailのレシピの記述と読解は重要なポイント、

~/procmailrcレシピの記述の実践が必要、フラグ、条件式(正規表現)などをよく理解する

条件式の記述における正規表現の記述の理解



procmailに関して

```

# SAMPLE
VAL=SAMPLE      ← 変数VALへの代入
:OB:           ← メールのBODY部のみ検査（ロックファイルを使う）
* ^$VAL        ← 分の先頭にVALの文字列    ※正規表現での記述
* < 5000       ← BODY部が5000Byteより小さい時
* > 4900       ← BODY部が4900Byteより大きい時
! aaa@test.jp  ← aaa@test.jp宛に転送する

```

条件(* から始る行)

! 条件の否定を意味する。

\$ 条件文に現れる(環境)変数をシェルの様に評価する。

? 指定したプログラムの終了コード(0:成功か1:失敗)を利用する。

< 長さが後に記述されたバイト数(10進)以下であれば実行する。

> 長さが後に記述されたバイト数(10進)以上であれば実行する。

変数名 ?? 指定された値と変数を比較する。

¥ クォートします。¥/と記述することで該当箇所を変数MATCHに格納する。

フラグ(:0から始る行)

フラグの説明

H デフォルト(記述が省略された場合)の動作。メッセージのヘッダだけを条件文で検査する。

B メッセージの本体だけを条件文で検査します。HBメッセージのヘッダと本体の両方を条件文で検査する。

h アクション(実行部)にメッセージヘッダだけを渡す。

b アクションにメッセージ本体だけを渡す。

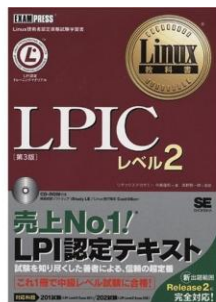
hb ※デフォルトの動作。アクションにメッセージのヘッダと本体の両方を渡す。

c 続くレシピのためにメッセージのコピーを残す。他のアドレスへのメッセージの送信、ブロック文で単一のメッセージに対して複数の処理を行う場合に用いる。

参考サイト: <http://www.jaist.ac.jp/~fjt/procmail.html>



参考資料について



Linux教科書 LPICレベル2 第3版
リナックスアカデミー 中島 能和 (著), 濱野 賢一郎 (監修)
2009/5/19発行
出版社:翔泳社
576ページ
定価3,990円
ISBN-10: 479811930X / ISBN-13: 978-4798119304



徹底攻略LPI 問題集Level2/Release2 対応
中島 能和 (著), ソキウス・ジャパン (編集)
2009/7/24発行
出版社:インプレスジャパン
288ページ
定価3,360円
ISBN-10: 4844327321 / ISBN-13: 978-4844327325



Linuxサーバセキュリティ
Michael D. Bauer 著、豊福 剛 訳
2003/10発行
出版社: O'Reilly Japan
464ページ
定価4,620円
ISBN4-87311-149-8



Linuxクックブック——Linuxを120%使いこなすレシピ集
Carla Schroder 著、林 秀幸 訳
2005/10発行
出版社: O'Reilly Japan
444ページ
定価3,780円
ISBN4-87311-248-6



ネットワークトラブルシューティングツール

Joseph D. Sloan 著、鷺谷 好輝 訳

2002年04月 発行

384ページ

定価4,095円

ISBN4-87311-080-7



DNS & BIND クックブック——ネームサーバ管理者のためのレシピ集

Cricket Liu 著、伊藤 高一 監訳、田淵 貴昭 訳

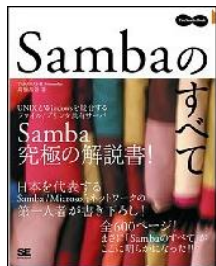
2003/04発行

出版社: O'Reilly Japan

256ページ

定価2,730円

ISBN4-87311-125-0



Sambaのすべて (The Samba Book)

著 高橋 基信

2005/6/30発行

出版社: 翔泳社

定価4,179円

ISBN-10: 4798108545 / ISBN-13: 978-4798108544



Linuxサーバー構築標準教科書 (Ver1.0.1)

詳しくは下記URLで

<http://www.lpi.or.jp/linuxservertext/>

発行: エルピーアイジャパン