~クラウドサービス時代を支えるOSS/Linux人材育成~





# LPICレベル2技術解説無料セミナー



LPI-Japanアカデミック認定校 スキルブレイン株式会社 インストラクター 三浦 一志

© LPI-Japan 2014. All rights reserved.



LPIC レベル2の概要

**Skill Brain** 

- ■小規模から中規模のネットワークシステムを管理できること。
- Linux、UNIX、Windowsが混在する小規模なネットワークの設計・運用・ 保守ができ、安定かつ安全な稼働を維持し、トラブルシューティングがで きること。
- ■アシスタントを管理できること。
- ■自動化および購入に関して管理者に助言できること。

#### ■2014年1月1日よりver4の新試験範囲が提供されている

http://www.lpi.or.jp/lpic2/range/





#### レベル2試験の概要

# ■201試験のポイント

・サーバの<u>スケーリング、メンテナンス</u>、そして<u>トラブ</u> ルシューティングに焦点を当てている

■202試験のポイント

- 主要な<u>ネットワークサービス</u>のほかに、<u>システムと</u>
   <u>ネットワークのセキュリティ</u>にも焦点を当てている。
- ■レベル1の試験範囲もかなり出題される
  - •復習が必要
  - ・レベル1より深い内容が問われる





#### 使用する環境



# ■各主題のポイントとなる部分を紹介 ■仮想環境を利用し、デモで確認を行う







ver3.5の「トラブルシューティング」は各主題に分配されました





主題200:キャパシティプランニング

# ■200.1 リソースの使用率の測定とトラブルシューティング 6

#### ■200.2 将来のリソース需要を予測する 2

- collectdを使用してITインフラの使用を監視する
- Nagios、MRTG、Cacti といった監視ツールを知っている







[root@cen	tos ~]# vmstat 1 5								
procs	memory	swap			syst	.em		-cpu-	
	wpd Tree butt cache	SI	SO I	0 k 71 1			s sy		a st
	0 230900 20304 203432	0	0		0 1002	31 ( 20 (		99 100	
	0 230908 20304 203430	0	0	0	0 1003	20 0		100	
	0 236968 20304 203430	0	0	0	0 1001	10 (		100	
ŏŏ	0 236968 20304 205436	Ő	ŏ	ŏ	0 1011	24 (		100	0 0
		· ·	~	Č.					
vmstat	表示間隔(秒) 回致								
r	実行待ちプロセス数		bo	送られ	ヽたブロッ	ク			
b	割り込み不可能なプロス数		in	1秒当	なりの割り	り込み			
swpd	スワップサイズ		CS	1秒当	自たりのコン	ノテキス	トス・	イッチ	
free	空きメモリ		us	그	ザ時間				
buff	バッファメモリ		sy	シスラ	テム時間				
cache	キャッシュメモリ		id	アイド	ル時間				
si	スワップイン		wa	入出	力待ち時間	5			
<b>SO</b>	スワップアウト		st	ゲストC	SがCPUを割り	り当てても	らえな	:かった	時間
bi	受け取ったブロック								







#### top

• システムリソースの使用状況やプロセスの実行状態

#### ■iostat

• CPUの利用状況とディスクの入出力

#### sar

- ディスク関連、ネットワーク関連、メモリとスワップ関連の情報
- sysstatパッケージに含まれている

#### free

• メモリの使用率





主題201:Linuxカーネル

201.1 カーネルの構成要素 2
201.2 Linuxカーネルのコンパイル 3
201.3 カーネル実行時における管理とトラブルシューティング 4





Active kernel releases

■カーネルの情報およびソースダウンロード先

http://www.kernel.org

■カーネルのバージョン

Prepatch	メインラインカーネルプレリリース版。
Mainline	メインラインツリー。すべての新機能が導入される。
Stable	メインラインカーネルが解放された後、それを「安定」と する。
Longterm	「長期保守」のカーネルリリース。重要なバグが修正さ れる。





# カーネルの再構築

- **Skill Brain**
- 1. 必要なパッケージをインストール yum install gcc kernel-devel kernel-headers ncurses-devel
- 2. カーネルソースを入手 cd /usr/src wget ftp://ftp.kernel.org/pub/linux/kernel/v3.x/linux-3.11.10.tar.xz xz -dv linux-3.11.10.tar.xz tar xvf linux-3.11.10.tar
- 3. カーネルのカスタマイズ
   cp /boot/config-2.6.18-308.el5 ./.config
   make menuconfig
- 3. コンパイル make bzImage
- 4. カーネルモジュールのインストール make modules\_install
- カーネルのインストール make install

以前のカーネルの 設定を引き継ぐ

新しい設定を組み込む



カーネルパラメータ

#### ■カーネルパラメータの調整 → カーネルの動作をチューニング パケットの転送を有効にする(ルータ機能) echo 1 > /proc/sys/net/ipv4/ip\_forward

sysctlコマンド sysctl -w net.ipv4.ip\_forward =1

(再起動するとこれは無効になる)

#### ■設定方法

 ・再起動しても有効にするためには/etc/sysctl.confに記述する
 net.ipv4.ip\_forward =1





# ■202.1 SysV-initシステムの起動をカスタマイズする 3

## ■202.2 システムのリカバリ **4**

■202.3 その他のブートローダ 2

• SYSLINUX, ISOLINUX, PXELINUX











- ■現状のサービスを制御
  - /etc/init.d/
    - /etc/init.d/httpd start

Apacheの起動

- ■次回起動時のサービスを制御(CentOS)
  - chkconfig httpd on
  - chkconfig --list httpd

Linux起動時にApacheの起動 サービスの起動確認

## ■Debianの場合

- update-rc.d, sysv-rc-conf
- ■OpenSUSEの場合
  - insserv







#### ■203.1 Linuxファイルシステムを操作する 4 ■203.2 Linuxファイルシステムの保守 3

- SMARTデバイスの監視
- Btrfsを知っている 👥

■203.3 ファイルシステムを作成してオプションを構成する 2





# スワップ領域の利用

# dd if=/dev/zero of=/tmp/swapfile bs=1M count=10 # mkswap /tmp/swapfile Setting up swapspace version 1, size = 10481 kB # swapon /tmp/swapfile # swapon -s

スワップ領域の確認

/dev/zero 内容が何もないファイル

Filename Туре Size Used Priority 530136 /dev/sda3 partition 0 -1 0 -2 /tmp/swapfile file 10232





#### オートマウント

**Skill Brain** 

- ・指定したディレクトリにアクセスすると、自動的にマウントする
   ■設定ファイル
  - /etc/auto.master



マップファイル(/etc/auto.sda5)

1 2 sda5 -fstype=ext3,rw :/dev/sda5 ①マウントベース(ディレクトリがないときは作成する)
 ②マップファイルのパス

①マウントベースの下に置かれるディレクトリ
 ②マウントオプション
 ③デバイスファイル名

# ■オートマウントの実行

#/etc/init.d/autofs start

(auto.masterを変更したらautomountデーモンを再起動する)

確認:/mnt/auto/sda5に移動する



主題204:高度なストレージ管理

#### ■204.1 RAIDを構成する 3 ■204.2 記憶装置へのアクセス方法を調整する 2

• iSCSIのツールとユーティリティ 💷

■204.3 論理ボリュームマネージャ 3





パーティションタイプの設定



# fdisk /dev/sdb コマンド (m でヘルプ): t 領域番号 (1-4): 1 16進数コード (L コマンドでコードリスト表示): fd コマンド (m でヘルプ): p パーティション 確認

Disk /dev/sdb: 21.4 GB, 21474836480 bytes 255 heads, 63 sectors/track, 2610 cylinders Units = cylinders of 16065 \* 512 = 8225280 bytes

ここはレベル1の内容です

Device Boot	Start	End	Blocks Id System
/dev/sdb1	1	31	248976 fd Linux raid autodetect
/dev/sdb2	32	62	249007+ fd Linux raid autodetect
/dev/sdb3	63	93	249007+ fd Linux raid autodetect









#lvdisplay /dev/vg01/lv01







#### ■ソフトウェアRAID(LinuxがRAIDを管理)







#### RAIDの構成

# mdadm -C /dev/md0 --level=1 --raid-devices=2 --spare-devices 1 /dev/sdb1 /dev/sdb2 /dev/sdb3 mdadm: array /dev/md0 started. # cat /proc/mdstat Personalities : [raid1] md0 : active raid1 sdb3[2](S) sdb2[1] sdb1[0] 248896 blocks [2/2] [UU]

unused devices: <none> # mdadm --query /dev/md0 RAIDアレイmd0の状態を確認 /dev/md0: 243.06MiB raid1 2 devices, 1 spare. Use mdadm --detail for more detail. /dev/md0: No.md.super block found not on md.somponent

/dev/md0: No md super block found, not an md component.





主題205:ネットワーク構成

205.1 基本的なネットワーク構成 3
205.2 高度なネットワーク構成 4
205.3 ネットワークの問題を解決する 4





#### # tcpdump icmp

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes 01:50:45.701512 IP 192.168.130.1 > 192.168.130.134: ICMP echo request, id 1, seq 1, length 40 01:50:45.798984 IP 192.168.130.134 > 192.168.130.1: ICMP echo reply, id 1, seq 1, length 40

> 192.168.130.1から192.168.130.134宛にpingを実行 している。 →echo requestを行い、echo replyが返ってくる







- ■206.1 ソースからプログラムをmakeしてインストールする 2
- ■206.2 バックアップ操作 3
- ■206.3 システム関連の問題をユーザに通知する 1





ソースからインストール

**Skill Brain** 

Apacheソースのダウンロード

\$wget http://ftp.riken.jp/net/apache/httpd/httpd-2.2.26.tar.gz

#### 1. \$tar xzvf httpd-2.2.26.tar.gz







#### ユーザへの通知

**Skill Brain** 

# ユーザーへの通知 /etc/issue → ログイン前にシステム情報やメッセージを表示 /etc/motd → ログイン後にメッセージを表示 wall → ログイン中のユーザへ通知















主題207:ドメインネームサーバ







- ■名前解決の種類
  - 正引き:ホスト名 → IPアドレス
  - 逆引き: IPアドレス → ホスト名

ペ → ホスト名 192.168.130.1

BIND ver9

• DNSサーバーのアプリケーション

■ゾーン

- DNSサーバーが管理する名前空間の範囲 (例: example.net)
- ■FQDN(Fully Qualified Domain Name:完全修飾ドメイン名)
  - ホスト名+ドメイン名の形式で表す

■インストール

#yum install bind bind-chroot

chrootを使用する場合



centos.example.net $\rightarrow$ 192.168.130.128
$192.168.130.128 \rightarrow \text{centos.example.net}$



BINDの設定ファイル







named.confの設定例



```
■/etc/namedの基本設定と管理するゾーンを記述
■設定例
options {
     directory "/var/named";
                                       ゾーンファイルのディレクトリ
};
                       管理するゾーン
zone "example.net" {
     type master;
     file "example.net.zone";
                                正引きゾーンファイルの名前
};
zone "130.168.192.in-addr.arpa" {
     type master;
     file "130.168.192.in-addr.arpa";
                                         逆引きゾーンファイルの名前
1.
Ì,
```



Institute





### ■設定例:/var/named/130.168.192.in-addr.arpa

\$TTL 86400

(a)	IN	SOA	centos.example.net. root.example.net.	(
			2014022301	
			86400	
			21600	
			864000	
			86400 )	
	IN	NS	centos.example.net.	
128	IN	PTR	centos.example.net 逆引き設定	

128.130.168.192.in-addr.arpa となる






## ■dnssec-keygenで鍵を生成 dnssec-keygen -a HMAC-MD5 -b 512 -n HOST example.net →生成した鍵により、スレーブサーバーを認証



```
マスターサーバーのnamed.conf

key "example.net" {

    algorithm hmac-md5;

    secret "n2W...xguJHugdACyg==";

];

options {

    allow-transfer { key example.net; };

};

zone "example.net" {

    type master;

    file "example.net.zone";

};
```

```
スレーブサーバーのnamed.conf

key "example.net" {

    algorithm hmac-md5;

    secret "n2W...xguJHugdACyg==";

];

server 192.168.130.1{

    keys "example.net";

];

zone "example.net" {

    type slave;

    file "example.net.zone";

    masters { 192.168.130.1; };

};
```





**Skill Brain** 

■208.1 Apacheの基本的な設定 4 ■208.2 HTTPS向けのApacheの設定 3



- ■208.3 キャッシュプロキシとしてのSquidの実装 2
- ■208.4 WebサーバおよびリバースプロキシとしてのNginxの実装 2







## Apache httpd

**Skill Brain** 











#### 「http://ホスト名/~ユーザ名/」でアクセス

(例)http://www.example.com/~centuser/





- ■.htaccessというファイルに設定を記述し、ディレクトリごと設定を上書き することができる。
- ■設定可能な範囲はAllowOverrideで許可されている範囲。











#### ■opensslを利用する

#### ■事前の設定

- ① 公開鍵と暗号鍵を作成
- ② 証明書発行要求書を認証局(CA)へ送る
- ③ 認証局からサーバ証明書を受け取る
- ④ サーバ証明書をWebサーバに設定する

#### SSLのモジュールをインストールしておく #yum install mod\_ssl

自分自身でCAを作成して自分自 身で証明書を発行することもでき る(自己署名証明書)







■/etc/httpd/conf.d/ssl.confに設定 LoadModules ssl\_module modules/mod\_ssl.so Listen 443 SSLでアクセスするとき のポート番号 <VirtualHost \_default\_:443> ErrorLog logs/ssl\_error\_log TransferLog logs/ssl\_access\_log LogLevel warn SSLEngine on

SSLProtocol all -SSLv2

SSLCertificateFile /etc/pki/tls/certs/localhost.crt

SSLCertificateKeyFile /etc/pki/tls/private/localhost.key </VirtualHost>

サーバ証明書



サーバ秘密鍵



# squid

**Skill Brain** 

#### ■Webプロキシ・キャッシュサーバー

■設定ファイル:/etc/squid/squid.conf

■http\_accessディレクティブで許可されていないと接続できない

• aclディレクティブで接続元アドレスなどを指定

■設定例

acl mynetwork src 192.168.130.0/255.255.255.0

http\_access allow mynetwork

aclで自身のネットワークを設定

自身のネットワークから接続を許可

■squidの起動 /etc/init.d/squid start







## ■Webサーバおよびリバースプロキシサーバ等の機能がある ■Apacheよりパフォーマンスが高い ■Apacheほど高機能ではない

• Apacheは高機能だが、使用しない機能が多いとも言える

#### ■リバースプロキシとは







rofessional

nstitute

## Nginxの設定例

**Skill Brain** 

# ■Webサーバとして動作させる場合

■設定ファイル:/etc/nginx/nginx.conf(パッケージからインストール)





# Nginxの設定例



```
■リバースプロキシとして動作させる場合
■設定ファイル:/etc/nginx/nginx.conf
■設定例
 server{
      server_name .example.net;
      root /home/eample.com/www;
      (省略)
      location / {
            proxy pass http://192.168.130.129:8080;
```









■209.1 Sambaサーバの設定 5
■209.2 NFSサーバの設定 3







#### ■Windowsネットワークにおけるファイルサーバー機能を提供

■サービス

smbd nmbd winbindd

■設定ファイル

- /etc/samba/smb.conf
- smb.confの構文にミスがないか確認 → testparm

■Sambaユーザの追加

#pdbedit -a centuser

smbclientで接続を確認する
 #smbclient -U centuser //samba3/public









**Skill Brain** 

■設定例:/etc/smb.conf



#### [public]

comment = Public Stuff browseable = Yes path = /home/samba/public public = yes writable = yes





# ■UNIX / Linuxネットワークにおけるファイルサーバー機能を提供 ■インストール

#yum install nfs-utils nfs-utils-lib portmap

■サービス

- portmap nfsd mountd
- ■起動方法
  - 1 /etc/init.d/portmap start
  - ② /etc/init.d/nfs start
- ■設定ファイル
  - /etc/exports

■ユーザー管理

• クライアント側でログインしたUIDを利用

必ずportmapから起動する

クライアントもportmapを起動









#### ■設定例:/etc/exports



■クライアントからの接続 #mount -t nfs centos:/share /mnt/nfs/share







# 主題210: ネットワーククライアントの管理 Skill Brain





fessional

**Skill Brain** 

## ■設定ファイル:/etc/dhcpd.conf

 ファイルは/usr/share/doc/dhcp\*/dhcp.conf.sampleをコピーして使用 ddns-update-style interim; ignore client-updates;







■DHCPサーバの起動 /etc/init.d/dhcpd start





nstitute

## PAM

**Skill Brain** 

**PAM**(Pluggable Authentication Modules)

■各アプリケーションに認証機能を提供

■/etc/pam.d/ディレクトリに各種アプリケーション用の設定ファイルが用 意されている







- sufficient:モジュールの実行に成功すると、上位でrequiredがすべて成功であれば認証成功。
- required:モジュールの実行に失敗したら、同じタイプのモジュールの実 行がすべて完了した時点で認証を拒否。
- ① rootユーザは認証なしでsuできる
- wheelグループに所属するユーザはsuでrootになるとき認証する。
  - その他のユーザはrootになるのを認証が拒否。
- ③ wheelのユーザだけsystem-authが認証する





#### ■標準仕様のディレクトリサービス

■識別名(DN:Distinguished Name)

• 例 dn: cn=Suzuki Ichiro, ou=People, dc=example, dc=net

■相対識別名(RDN:Relative Distinguished Name)

• 例 cn=Suzuki Ichiro

■設定ファイル:/etc/openIdap/slapd.conf







■LDIF(LDAP Data Interchange Format)形式: sample.ldif dn: cn=Takahashi Jiro, ou=People, dc=example, dc=net objectClass: person cn: Takahashi Jiro sn: Takahashi telephoneNumber: +81 3 1234 5678



```
■エントリの追加
 #Idapadd -x -D 'cn=Manager, dc=example, dc=net' -W -f sample.Idif
```



**Skill Brain** 





# クライアントコマンド

dapadd	エントリの追加
dapsearch	エントリを検索する
ldapmodify	エントリを変更する
dapdelete	エントリを削除する
dappasswd	エントリのパスワードを 変更する

■ 管理コマンド	
slapadd	エントリの追加
slapcat	データをLDIF形式で出力
slappasswd	パスワード値を生成する
slapindex	インデックスを再構築する
slaptest	slapd.confを構文テスト





主題211:電子メールサービス

211.1 電子メールサーバの使用 4
 211.2 ローカルの電子メール配信を管理する 2
 211.3 リモートの電子メール配信を管理する 2





#### メールシステム

**Skill Brain** 

MTA (Mail Transfer Agent):メールの転送【Sendmail, Postfix, qmail】
MDA (Mail Delivery Agent):メールの配信【Procmail】
MUA (Mail User Agent):メールクライアント【mailコマンド】
MRA(Mail Retrieval Agent):メール受信サービス





## postfix

■sendmailとの互換性と意識しながら、sendmail, qmailの長所を採用して 、作られたMTA

### ■主な設定ファイル

- /etc/postfix/main.cf
- /etc/postfix/master.cf
- ■関連ディレクトリ
  - ・メールスプール
    - /var/spool/mail/(メールボックス形式。1ユーザーにつき1ファイル)
    - ~/Maildir/(メールディレクトリ形式。1通につき1ファイル)
  - ・メールキュー
    - /var/spool/postfix/ (postfix)





**Skill Brain** 

■設定例:/etc/postifx/main.cf myhostname = centos.example.net →ホスト名 →ドメイン名 mydomain = example.net →@以降に補完する名前 myorigin = \$mydomain →接続を待ち受けるインターフェース inet interfaces = all mydestination = \$myhostname, localhost.\$mydomain, localhost, \$mydomain →宛先として使用できる名前 mynetwork = 192.168.130.0/24, 127.0.0/8→メールを中継するクライアント home\_mailbox = Maildir/ →メールディレクトリ形式の配送先 mailbox\_command = /usr/bin/procmail →MDAの設定









■定義したレシピに従い、メール配送を行うMDA

■レシピファイル

- ~/.procmailrc
- /etc/procmailrc

システム全体に設定

ユーザごとに設定

~/.procmailrcの記述例
 PATH=/bin:/usr/bin:/usr/sbin
 MAILDIR=\$HOME/Maildir/
 LOGFILE=\$HOME/.procmaillog
 DEFAULT=\$MAILDIR



Subjectに「SPAM」という 記述があると、 メールを破棄する





212.1 ルータを構成する 3
212.2 FTPサーバの保護 2
212.3 セキュアシェル (SSH) 4
212.4 セキュリティ業務 3
212.5 OpenVPN 2 (1)



**Skill Brain** 



# **Skill Brain**

#### ■vsftpdの設定

- /etc/vsftpd/vsftpd.conf
- ■設定例

local\_enable=YES ローカルユーザのログインを許可 write\_enable=YES 書き込みを許可

anonymous\_enable=YES anon\_upload\_enable=YES anon\_mkdir\_write\_enable=YES 医名FTPのアップロードを許可 医名FTPによるディレクトリ作成

を許可

■起動 /etc/init.d/vsftpd start





ofessional

stitute

**OpenVPN** 









# **Skill Brain**



Linux教科書 LPICレベル2 第4版 リナックスアカデミー 中島 能和 (著), 濱野 賢一朗 (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/Version 3.5 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教科書 LPIC レベル3
中島 能和 (著),高橋 基信 (著),濱野 賢一朗 (著)
単行本 (ソフトカバー):480ページ
出版社:翔泳社 (2010/2/19)
言語:日本語
ISBN-10:4798116556
ISBN-13:978-4798116556
徹底攻略LPI問題集 Level3
中島 能和 (著),ソキウス・ジャパン (編集)
単行本:256ページ
出版社:インプレスジャパン (2008/4/24)
定価 3,360円
ISBN-10:4844325647
ISBN-13:978-4844325642



Linuxサーバー構築標準教科書(Ver2.0.1) 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







# 質疑応答についてはお気軽にお声掛けください。

ご清聴ありがとうございました。



Skill Brain スキルブレイン株式会社

# http://www.skillbrain.co.jp







#### ■Linux 基礎 ■Linux サーバー構築実践 ■Linux サーバー管理・運用実践 ■Linux サーバーセキュリティ構築実践 ■LPIC(レベル1・2・3) 試験対策 ■OSS-DB (Silver/Gold) 試験対策 ■Oracle 認定 Java(OCJ)試験対策 ■ITIL® ファンデーション(シラバス 2011)研修 ■仮想化技術研修 ■セキュリティ(FW・IDS・ウイルス対策) ■階層別アセスメント研修 ビジネスマナー研修 ※その他、企業様ごとにセミオーダー研修を承ります。





**Skill Brain** 



#### 経験・スキルともに豊富な講師陣が技術や資格取得をサポート Skill Brain





#### 三浦 一志

サーバ管理者として8年以上の実務経験を積み、講師としても10年以上のキャリアを持つ。 法人向けにLPIC研修・Linuxサーバ構築・セキュリティ研修やITIL研修を主として担当。 ITIL認定講師 情報セキュリティスペシャリスト

#### 【担当講習】

・Linux/UNUX ・LPIC試験対策 ・セキュリティ ・Java ・PHP ・OSS-DB ・HTML5

#### 河原木 忠司

Linux・Windowsを使ったインフラ環境の構築・運用、セキュアなインターネットサーバーの 構築など、企業・官公庁向けの技術研修を担当。 MCT(マイクロソフト認定トレーナー) VoIP認定講師

【担当講習】 ・Linux ・Windows ・VoIP ・セキュリティ ・仮想化 ・LPIC試験対策 ・OSS-DB



#### 大崎 茂

OSS研修専任講師として、大手電機メーカー・通信キャリア・大手プロバイダー等、IT企業の LPIC対策研修ならびにOSSを中心とした技術研修などを専門に担当。

#### 【担当講習】

・Linux ・C言語 ・PHP ・Jaxa ・Ajax ・LAMP関連 ・LPIC試験対



#### 木村 祐

ITILV3 Expert ITILV2 Manager ITILV2 OSA・RCV・SOA・PPO EXIN認定インストラクター ISO20000 Consultant/Manager

【担当講習】 ・ITILファウンデーション ・ITILエキスパート ・ITILプラクティショナー

