



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



- 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/>



■ 201試験のポイント

- ・サーバのスケーリング、メンテナンス、そしてトラブ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

- ・主要なネットワークサービスのほかに、システムとネットワークのセキュリティ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

Skill Brain

- 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

Windows(ホストOS)



```
CentOS-6.5-20130905-1450-std [root@centos ~]# ls /etc
[...]
[root@centos ~]#
```

ssh

仮想環境

VirtualBox



sda : Linux
システム



sdb : RAID用



sdc : LVM用

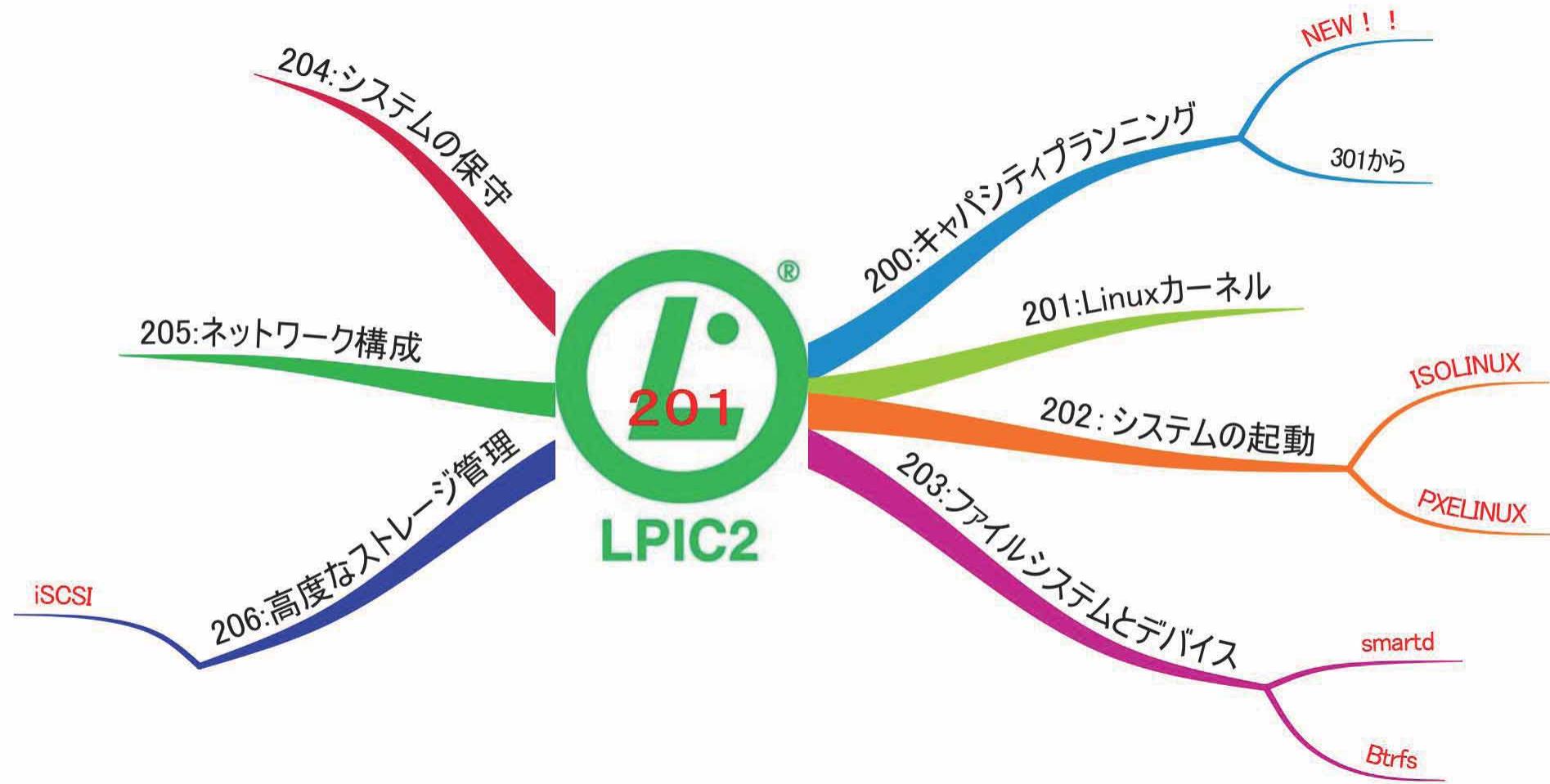
CentOS6.5(ゲストOS)

TeratermやPuttyを利用してsshで接続



201試験

Skill Brain



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



- 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: システムの各種情報を定期的に収集するデーモン
- Nagios: オープンソースのシステム監視、ネットワーク監視を行う
- MRTG: ネットワーク機器のトラフィックをグラフ化するプログラム
- Cacti: MRTGの代替となるソフトウェア。過去のグラフを参照できる





vmstatコマンドの見方

Skill Brain

```
[root@centos ~]# vmstat 1 5
procs -----memory----- ---swap-- -----io----- --system-- -----cpu-----
r b swpd free buff cache si so bi bo in cs us sy id wa st
0 0 0 236968 20304 205432 0 0 71 14 1019 31 0 0 99 0 0
0 0 0 236968 20304 205436 0 0 0 0 1003 20 0 0 100 0 0
0 0 0 236968 20304 205436 0 0 0 0 1013 32 0 0 100 0 0
0 0 0 236968 20304 205436 0 0 0 0 1004 19 0 0 100 0 0
0 0 0 236968 20304 205436 0 0 0 0 1011 24 0 0 100 0 0
```

vmstat 表示間隔(秒) 回数

r	実行待ちプロセス数	bo	送られたブロック
b	割り込み不可能なプロセス数	in	1秒当たりの割り込み
swpd	スワップサイズ	cs	1秒当たりのコンテキストスイッチ
free	空きメモリ	us	ユーザ時間
buff	バッファメモリ	sy	システム時間
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
so	スワップアウト	st	ゲストOSがCPUを割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



- 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。



- 必要なパッケージをインストール

```
yum install gcc kernel-devel kernel-headers ncurses-devel
```

- カーネルソース入手

```
cd /usr/src
```

現在のカーネルソース

menuconfigを起動するため必要

```
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
```

- カーネルのカスタマイズ

```
cp /boot/config-2.6.18-308.el5 ./config  
make menuconfig
```

以前のカーネルの設定を引き継ぐ

- コンパイル

```
make bzImage
```

新しい設定を組み込む

- 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
```



- 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
```

(再起動するところは無効になる)

- 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

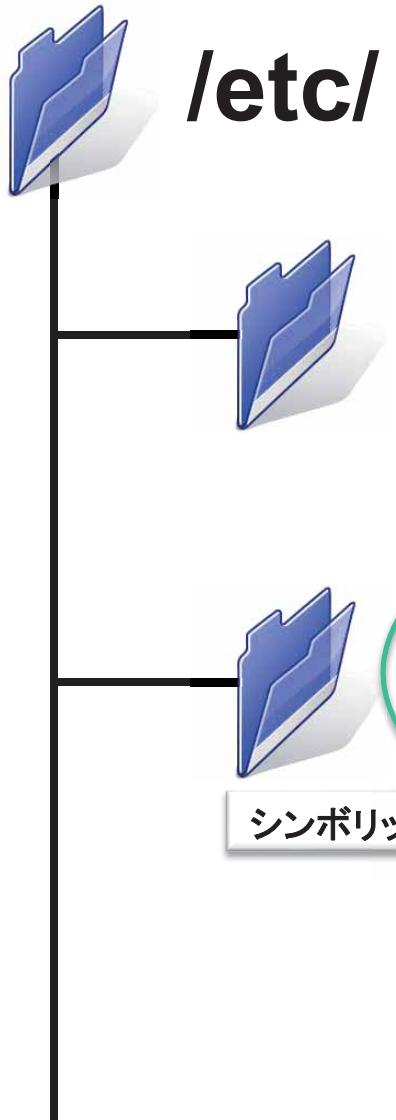
■202.2 システムのリカバリ 4

■202.3 その他のブートローダ 2

- SYSLINUX:FATファイルシステムからカーネルを起動する
- ISOLINUX:ISO9660ファイルシステムからカーネルを起動する
- PXELINUX:PXEを使用してネットワークブートをする

(Preboot eXecution Environment)





/etc/init.d/

/etc/rc[0-6].d/



httpd

(起動スクリプト)



S85httpd

ランレベルごとに
ディレクトリがある

Sで始まる: ランレベルのときサービスがスタート

Kで始まる: ランレベルのときサービスが終了

数字: 小さい数字から順に実行



■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
 - (Debian6からはupdate-rc.dに代わってinsservコマンドを使用)



■ 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

- S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology System)
ハードディスクに組み込まれている自己診断機能のこと
- Btrfs (B-tree file system) : Linux向けに開発中のファイルシステム

■ 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

NEW

NEW



スワップ領域の利用

Skill Brain

```
# dd if=/dev/zero of=/tmp/swapfile bs=1M count=10  
# mkswap /tmp/swapfile
```

Setting up swap space version 1, size = 10481 kB

```
# swapon /tmp/swapfile
```

```
# swapon -s
```

スワップ領域の確認

/dev/zero

0埋めするデバイス

Filename	Type	Size	Used	Priority
/dev/sda2	partition	530136	0	-1
/tmp/swapfile	file	10232	0	-2



■ オートマウントとは？

- ・ 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

① /mnt/auto ② /etc/auto.sdb2

- ・ マップファイル(/etc/auto.sda5)

① sda5 ② -fstype=ext4,rw ③ :/dev/sdb2

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



- 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(Internet Small Computer System Interface) 
TCP/IP上でSCSIプロトコルを利用可能にする仕組み。
安価にSANを構築できる。

- 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

Skill Brain

```
# fdisk /dev/sdb
```

システムタイプ
変更

コマンド (m でヘルプ): t

8e : LVM
fd : RAID

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

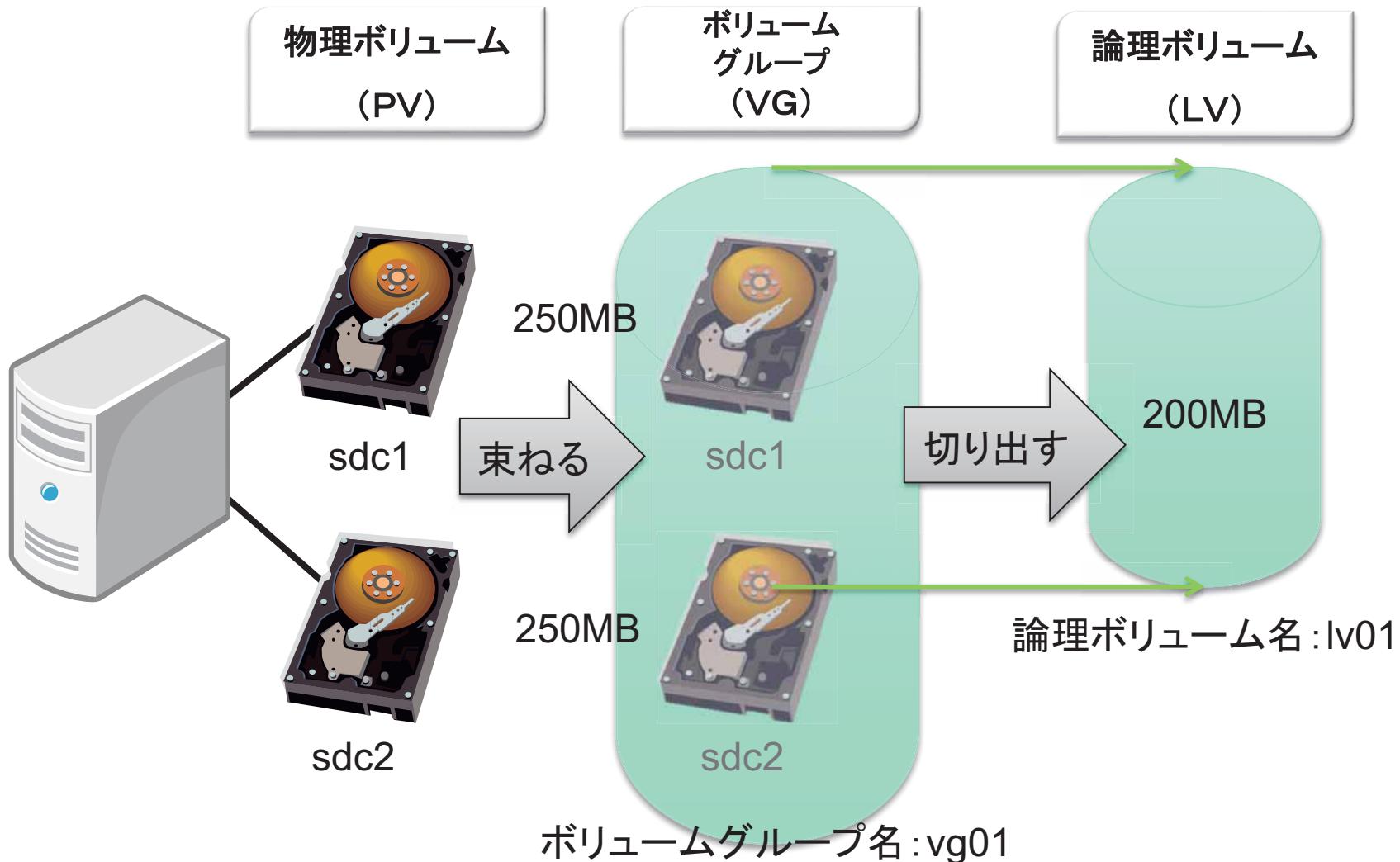
Disk /dev/sdb: 21.4 GB, 21474836480 bytes

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





LVMの構成

Skill Brain

```
# pvcreate /dev/sdc1 /dev/sdc2
```

物理ボリューム作成

```
# vgcreate vg01 /dev/sdc1 /dev/sdc2
```

ボリュームグループ作成

```
# lvcreate -L 200M -n lv01 vg01
```

論理ボリューム作成

```
# mkfs -t ext3 /dev/vg01/lv01
```

ファイルシステム作成

```
# mount -t ext3 /dev/vg01/lv01 /mnt
```

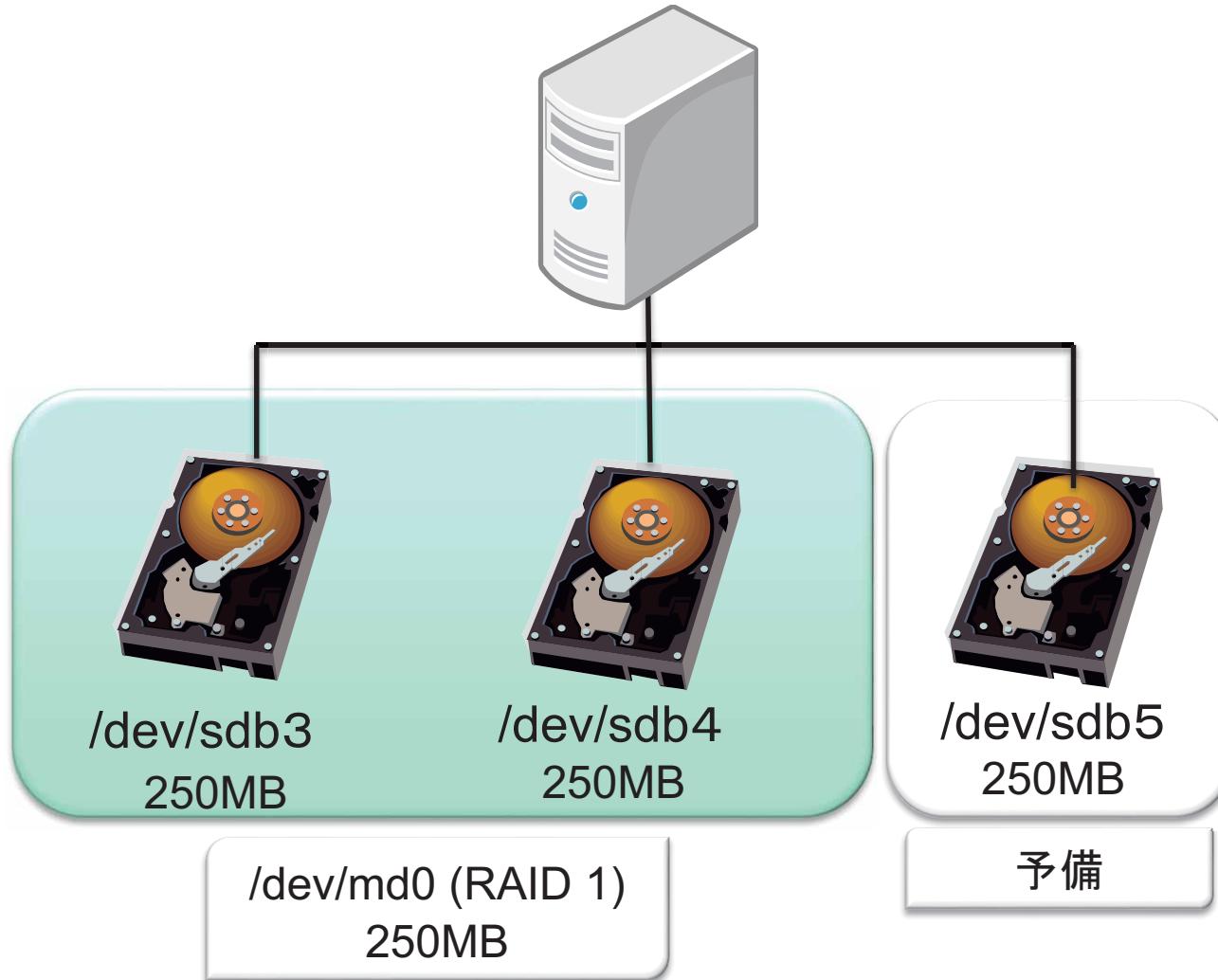
マウント

■論理ボリュームの確認

```
# lvdiskdisplay /dev/vg01/lv01
```



■ソフトウェアRAID(LinuxがRAIDを管理)





RAIDの構成

Skill Brain

```
# mdadm -C /dev/md0 --level=1 --raid-devices=2 --spare-devices 1  
/dev/sdb3 /dev/sdb4 /dev/sdb5
```

```
mdadm: array /dev/md0 started.
```

```
# cat /proc/mdstat
```

```
Personalities : [raid1]
```

```
md0 : active raid1 sdb5[2](S) sdb4[1] sdb3[0]  
      248896 blocks [2/2] [UU]
```

RAID1を作成
RAIDアレイmd0

RAIDアレイを確認

```
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 an md component.
```



- 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 192.168.56.1 > 192.168.56.128: ICMP echo  
request, id 1, seq 1, length 40
```

```
01:50:45.798984 IP 192.168.56.128 > 192.168.56.1: ICMP echo reply,  
id 1, seq 1, length 40
```

192.168.56.1から192.168.56.128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



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
2. \$cd httpd-2.2.26
3. \$./configure
4. \$make
5. #make install

インストール環境の調査、Makefileの生成

コンパイル

インストール

※インストール時は、root権限が必要



■ 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

/etc/issue

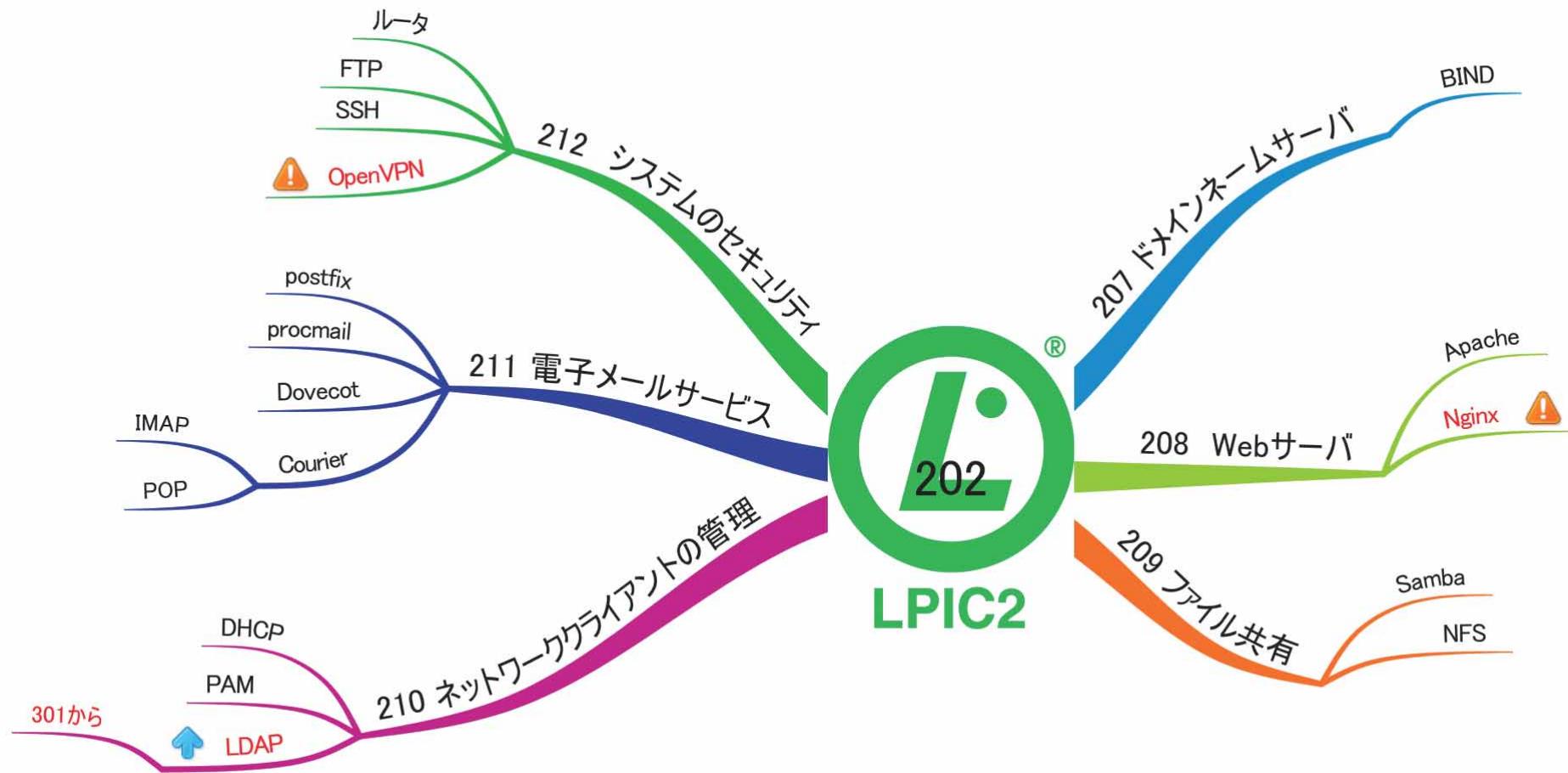
{ CentOS release 5.8
Kernel 2.6.18-308.8.2.el5 on an i686
centos login: root
Password:
Last login: Wed Sep 30 20:54:51 2011 from 192.168.56.1
System maintenance: Jun 30 22:00-23:00

/etc/motd



202試験

Skill Brain





- 207.1 DNSサーバの基本的な設定 3
- 207.2 DNSゾーンの作成と保守 3
- 207.3 DNSサーバを保護する 2



■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

centos.example.net → 192.168.56.128

192.168.56.128 → centos.example.net

■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）

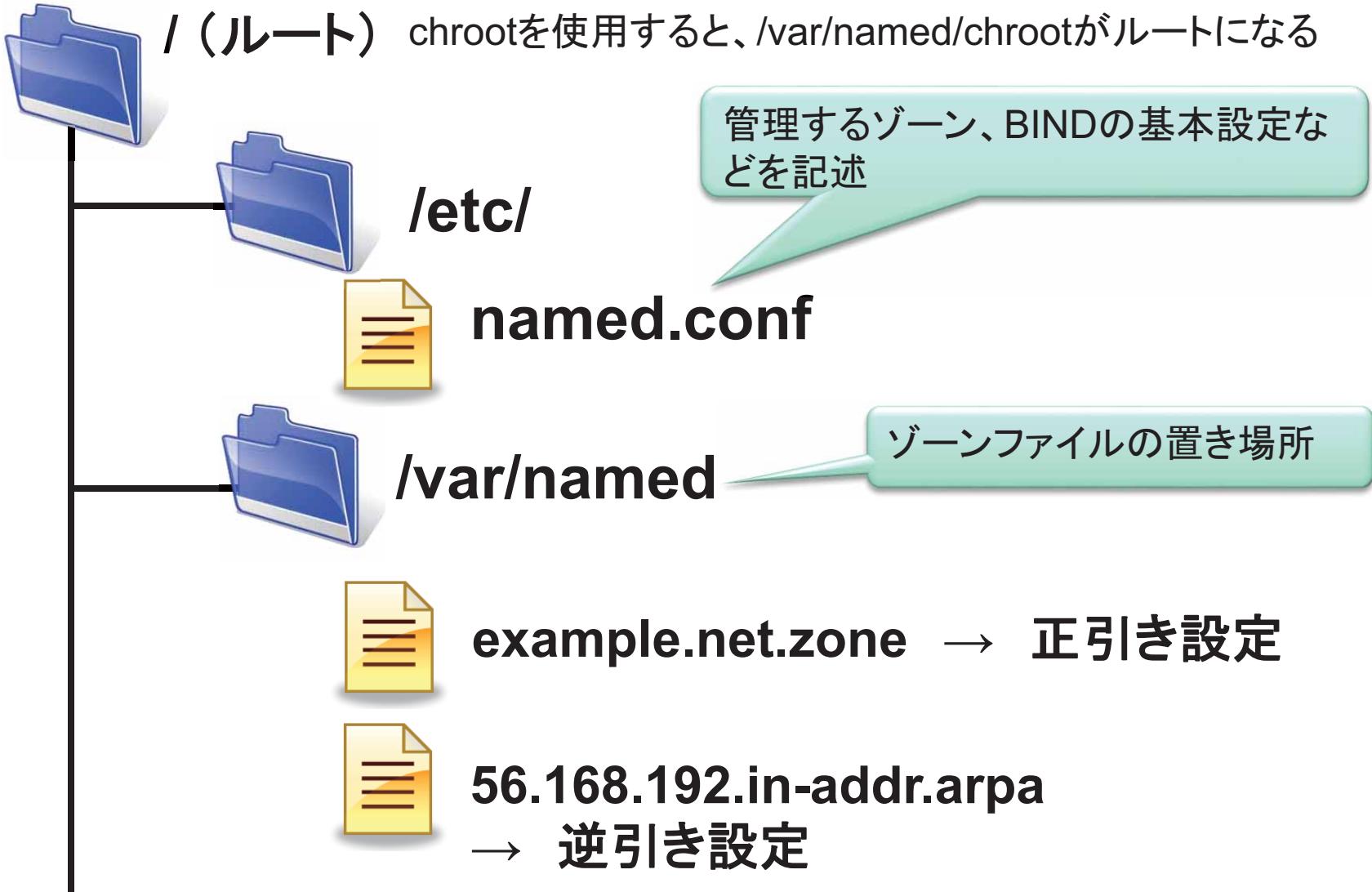
■FQDN(Fully Qualified Domain Name:完全修飾ドメイン名)

- ・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



そのほか、ループバック用ファイル、ルートDNSサーバ用ファイルが必要



■ /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

```
};
```

```
zone "example.net" {
```

管理するゾーン

```
    type master;
```

```
    file "example.net.zone";
```

正引きゾーンファイルの名前

```
};
```

```
zone "56.168.192.in-addr.arpa" {
```

```
    type master;
```

```
    file "56.168.192.in-addr.arpa";
```

逆引きゾーンファイルの名前

```
};
```

■ 設定例: /var/named/example.net.zone

\$TTL 86400

@ IN SOA centos.example.net. root.example.net. (

ゾーン名

DNSサーバのホスト

管理者のメールアドレス

time-to-refresh

2014022301

シリアル値

time-to-retry

86400

スレーブサーバに対する設定

time-to-expire

21600

minimum-TTL

864000

86400)

IN NS

centos.example.net.

DNSサーバ

IN MX

10 mail.example.net.

メールサーバ

プリファレンス値: 優先度

centos IN A

192.168.56.128

ホストのIPアドレスを指定

www IN CNAME

centos.example.net.

別名



■ 設定例 : /var/named/56.168.192.in-addr.arpa

\$TTL 86400

```
@      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

128.56.168.192.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

■設定例

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 192.168.56.1{
    keys "example.net";
};

zone "example.net" {
    type slave;
    file "example.net.zone";
    masters { 192.168.56.1; };
};
```



■ 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





■ Webサーバー用アプリケーション

■ 設定ファイル

- /etc/httpd/conf/httpd.conf

■ 「ディレクティブ名 値」という形で設定

■ 設定例 : /etc/httpd/conf/httpd.conf

ServerRoot “/etc/httpd”

設定ファイルの起点となるディレクトリ

Listen 80

待ち受けポート番号

ServerAdmin webmaster@example.net

管理者のメールアドレス

DocumentRoot “/var/www/html”

htmlファイルを置く場所



■ユーザーごとにページ公開領域を設定

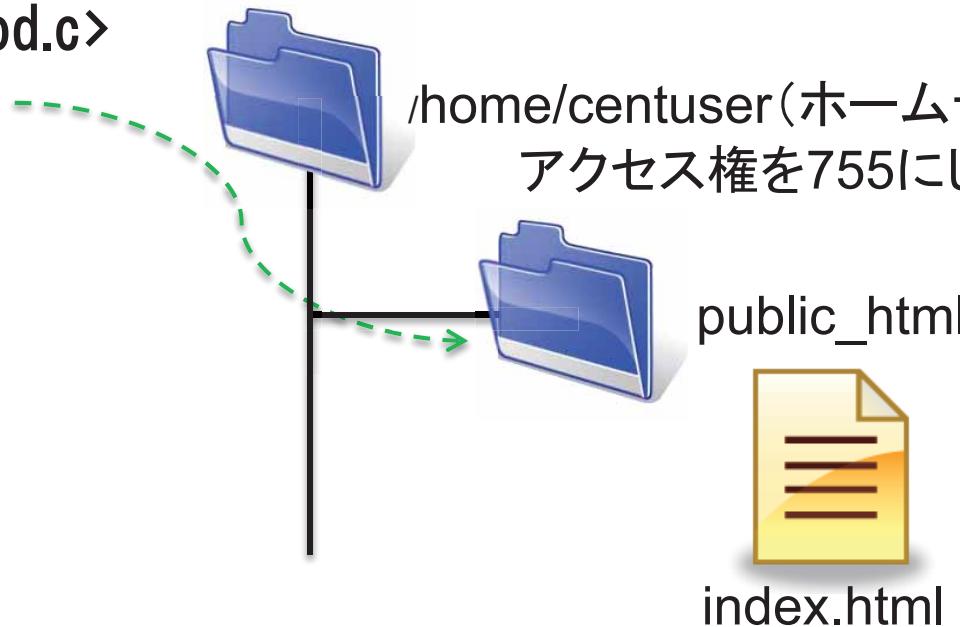
■設定

/etc/httpd/conf/httpd.conf ファイル内

```
<IfModules mod_usermod.c>
```

```
  UserDir public_html
```

```
</IfModule>
```



「http://ホスト名/~ユーザ名/」でアクセス

(例) http://www.example.com/~centuser/

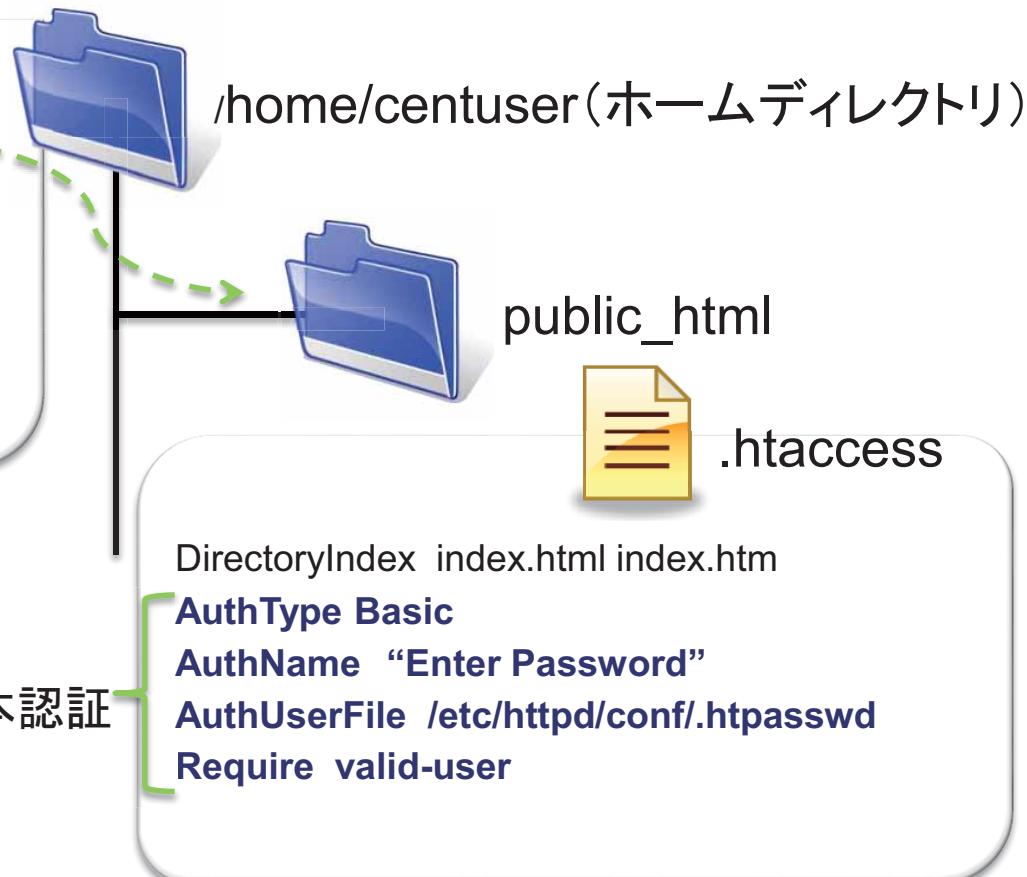
- .htaccess というファイルに設定を記述し、ディレクトリごと設定を上書きすることができる。
- 設定可能な範囲は AllowOverride で許可されている範囲。

/etc/httpd/conf/httpd.conf に記述

```
<Directory /home/*/*public_html/>
  AllowOverride AuthConfig Indexes
</Directory>
AccessFileName .htaccess
```

AuthConfig : 認証を有効にする
Indexes : DirectoryIndex を有効

基本認証





■ 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

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)

■ SSLのモジュールをインストールしておく

```
#yum install mod_ssl
```



■ /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

サーバ証明書

SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

サーバ秘密鍵

</VirtualHost>



- Webプロキシ・キャッシングサーバー
- 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 192.168.56.0/255.255.255.0
```

```
http_access allow mynetwork
```

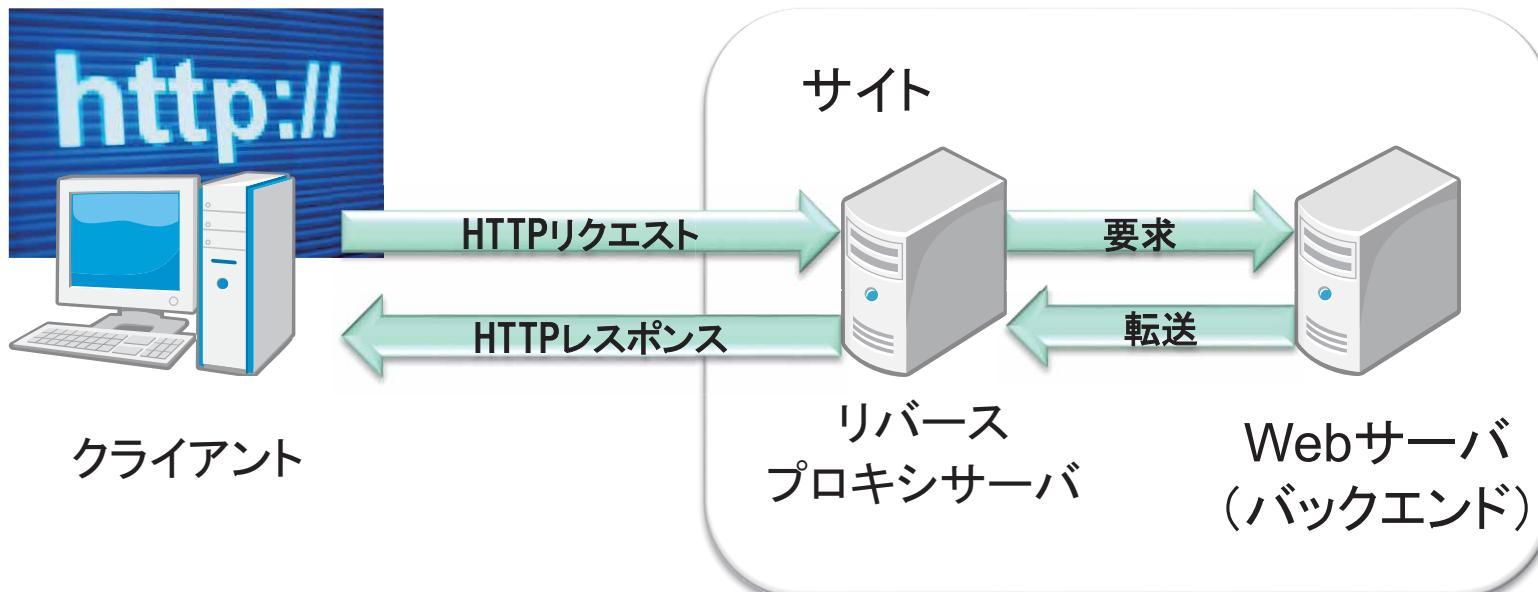
aclで自身のネットワークを設定

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





- 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の場合)

■ 設定例

```
server {  
    listen 80;                                待ち受けポート番号  
    server_name centos.example.net;            http://centos.example.netでアクセス  
  
    location / {  
        root /usr/share/nginx/html;             http://centos.example.net/に適用  
        index index.html index.htm;           DocumentRootと同じ  
    }  
}
```

DirectoryIndexと同じ



- 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/example.com/www;  
    (省略)  
    location / {  
        proxy_pass http://192.168.56.129:8080;  
    }  
}
```



バックエンドのWebサーバ



- 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 //samba01/public

//netbios名/公開ディレクトリ

■ 設定例 : /etc/smb.conf

workgroup = workgroup

ワークグループ名

netbios name = samba01

netbios名

hosts allow = 127. 192.168.56. 192.168.0.

アクセス制御

[public]**comment = Public Stuff****browsable = Yes****path = /home/samba/public****public = yes****writable = yes**

共有するディレクトリの設定



■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

必ずportmapから起動する
クライアントもportmapを起動

■設定ファイル

- /etc/exports

■ユーザー管理

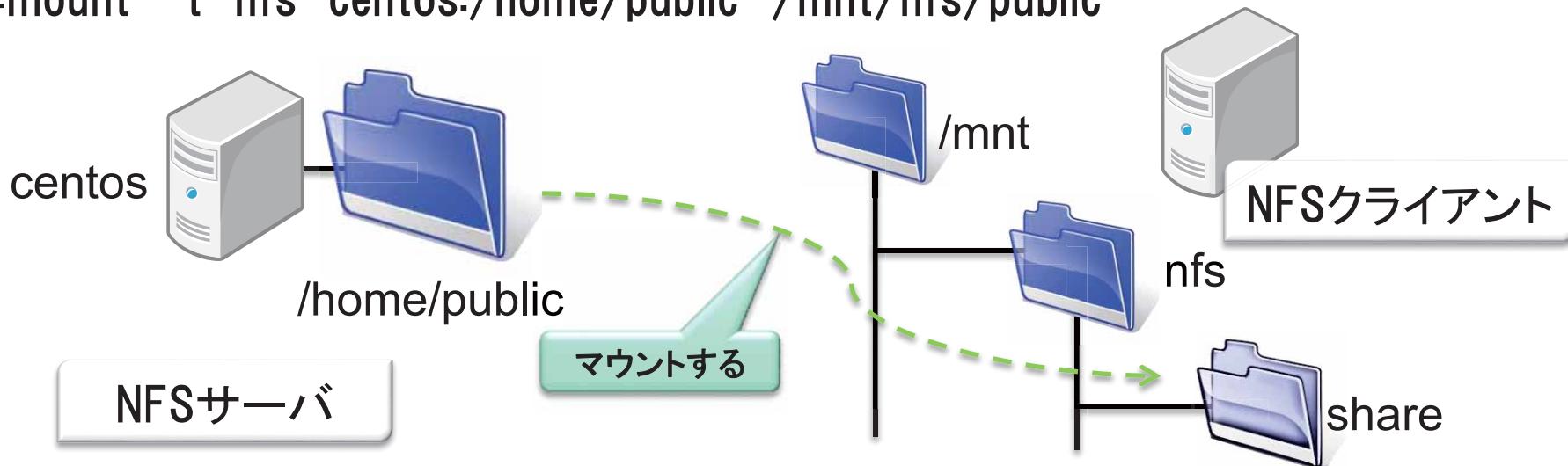
- クライアント側でログインしたUIDを利用

■ 設定例 : /etc(exports



■ クライアントからの接続

```
#mount -t nfs centos:/home/public /mnt/nfs/public
```





- 210.1 DHCPの設定 2
- 210.2 PAM認証 3
- 210.3 LDAPクライアントの利用方法 2
- 210.4 OpenLDAPサーバの設定 4 



■ 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;
```

```
subnet 192.168.0.0 netmask 255.255.255.0 {
```

```
    option routers
```

```
        192.168.0.1;
```

デフォルトゲートウェイ

```
    option subnet-mask
```

```
        255.255.255.0;
```

サブネットマスク

```
    option domain-name
```

```
        "example.net";
```

ドメイン名

```
    option domain-name-servers
```

```
        192.168.0.1;
```

DNSサーバ

```
    range 192.168.0.128 192.168.0.254;
```

割当て可能な
IPアドレスの範囲

```
    default-lease-time 21600;
```

デフォルトリース期間

```
    max-lease-time 43200;
```

最大リース期間

}



■ 固定のIPアドレスを割当てる

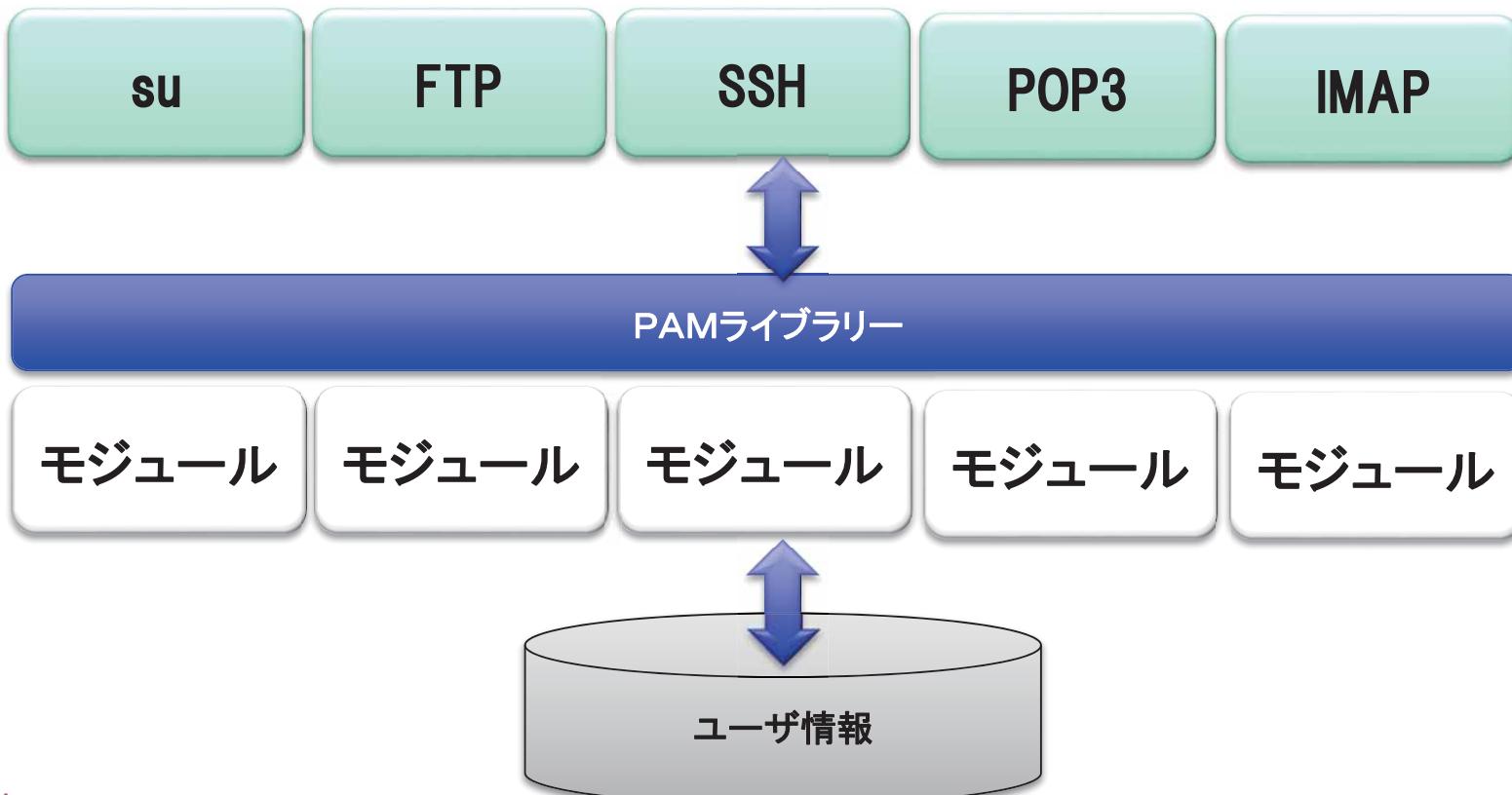
```
subnet 192.168.0.0 netmask 255.255.255.0 {  
    host debian7 {  
        hardware ethernet 00:0C:29:96:EE:5D;           MACアドレス  
        fixed-address 192.168.0.129;                  固定のIPアドレス  
    }  
}
```

■ DHCPサーバの起動

```
/etc/init.d/dhcpd start
```



- 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





■ 設定例 : /etc/pam.d/su

auth	sufficient	pam_rootok.so	… ①
auth	required	pam_wheel.so use_uid	… ②
auth	include	system-auth	… ③

モジュールタイプ

コントロール

モジュールのパス 引数

■ コントロール

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
- ② 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

①から③まで順に実行していく

■標準仕様のディレクトリサービス

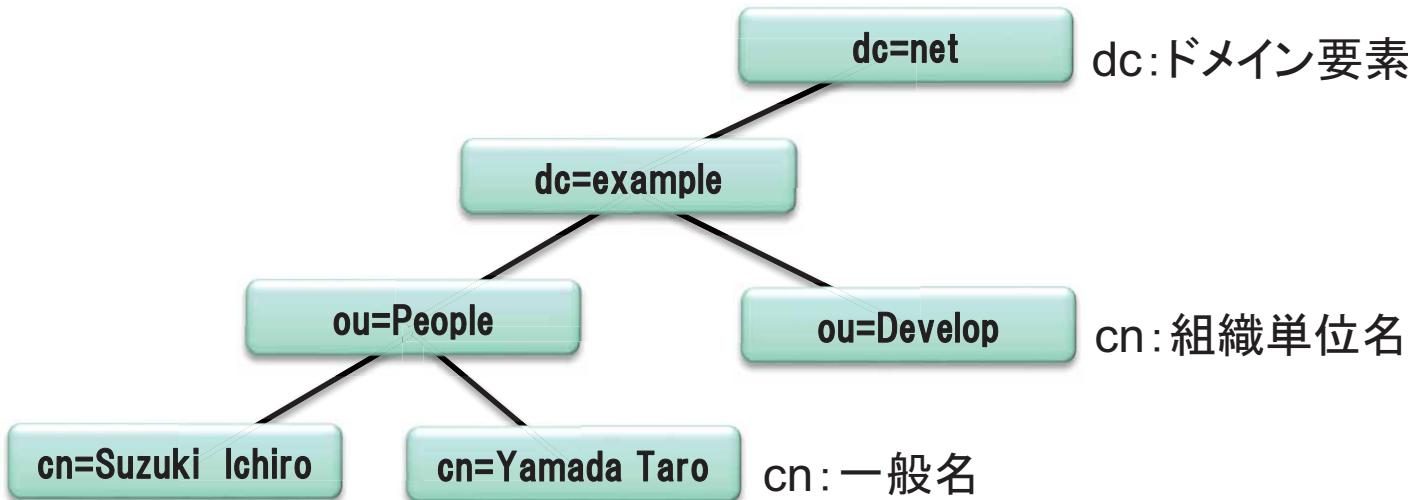
■識別名(DN:Distinguished Name)

- 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/openldap/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



sample.ldif

■ エントリの追加

```
#ldapadd -x -D 'cn=Manager, dc=example, dc=net' -W -f sample.ldif
```



■ クライアントコマンド

ldapadd	エントリの追加
ldapsearch	エントリを検索する
ldapmodify	エントリを変更する
ldapdelete	エントリを削除する
slappasswd	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

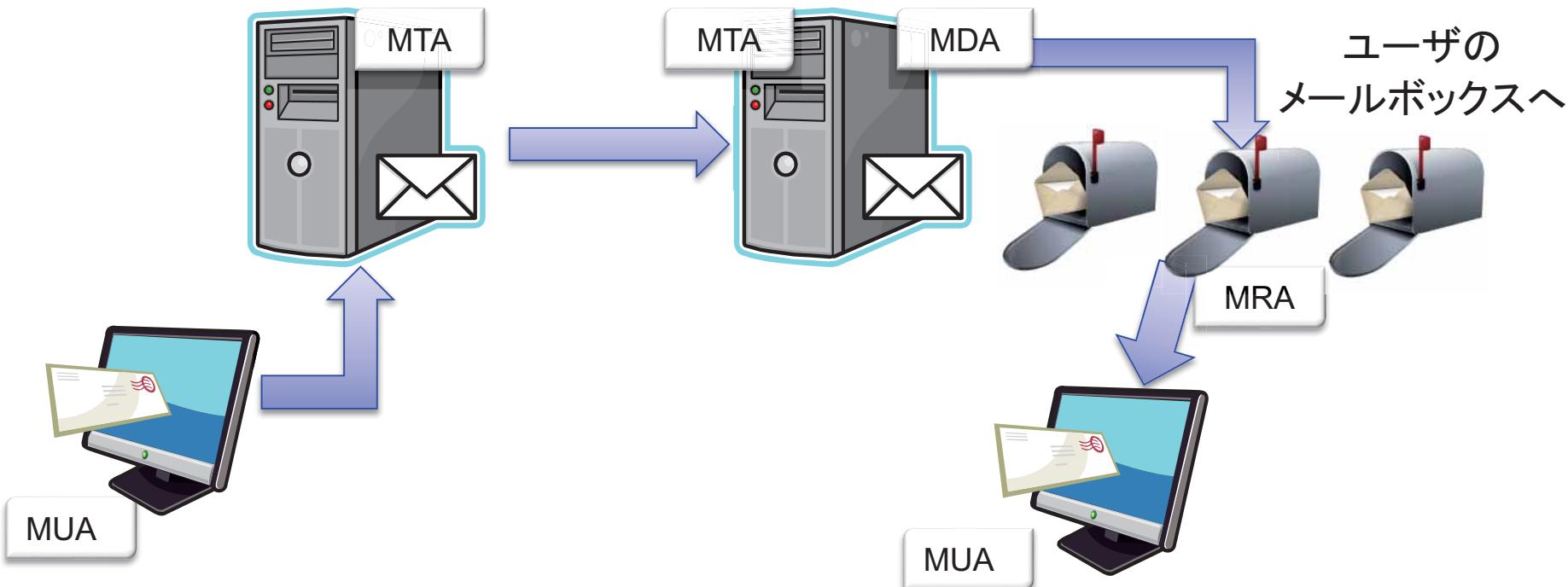


- 211.1 電子メールサーバの使用 4
- 211.2 ローカルの電子メール配信を管理する 2
- 211.3 リモートの電子メール配信を管理する 2

Sendmailの比率が減

- 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

【dovecot, courier IMAP】





■ 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)



■ 設定例 : /etc/postfix/main.cf

```
myhostname = centos.example.net          → ホスト名  
mydomain = example.net                   → ドメイン名  
myorigin = $mydomain                    → @以降に補完する名前  
inet_interfaces = all                   → 接続を待ち受けるインターフェース  
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain  
                                → 宛先の@以降につく名前を許可  
mynetwork = 192.168.56.0/24, 127.0.0.0/8  
                                → 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達先  
mailbox_command = /usr/bin/procmail  
                                → MDAの設定
```



■定義したレシピに従い、メール配達を行うMDA

■レシピファイル

- `~/.procmailrc` ユーザごとに設定
- `/etc/procmailrc` システム全体に設定

■`~/.procmailrc`の記述例

`PATH=/bin:/usr/bin:/usr/sbin`

`MAILDIR=$HOME/Maildir/`

`LOGFILE=$HOME/.procmaillog`

`DEFAULT=$MAILDIR`

・レシピの記述ルール

:0 フラグ

* 条件

アクション

:0
* ^Subject:.*SPAM.* } レシピ
/dev/null (フィルタリングのルール)

`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 



■ 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

匿名FTPを許可

anon_upload_enable=YES

匿名FTPのアップロードを許可

anon_mkdir_write_enable=YES

匿名FTPによるディレクトリ作成を許可

■ 起動

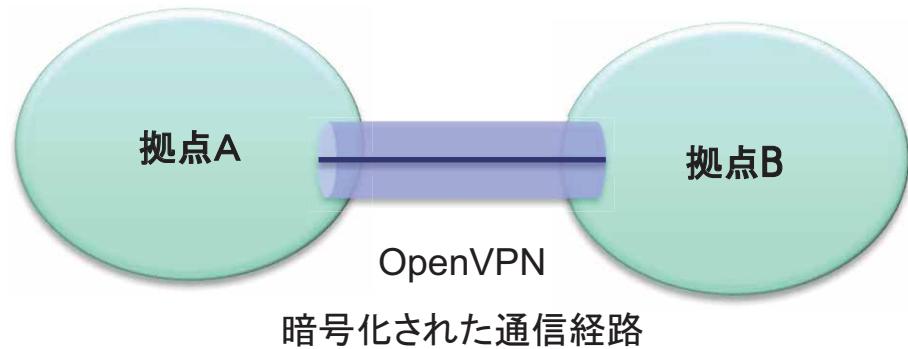
/etc/init.d/vsftpd start

■ VPN (Virtual Private Network) とは

- 拠点間の仮想的なネットワーク接続を可能にする

■ OpenVPNの種類

- トンネルモード (L3) VPN
 - ルーティング設定が必要
 - プロトコルは TCP/IP のみ
 - フィルタリングによるアクセス制御が可能
- ブリッジモード (L2) VPN
 - ルーティング設定が不要
 - TCP/IP 以外のプロトコルを使用可能
 - 通常の内部ネットワークと同様に、NetBIOS によるファイル転送が可能





■通信するホスト間を暗号化して、セキュアな通信を実現

■デフォルトのポート番号: 1194

■サーバ用設定ファイル

- /etc/openvpn/server.conf

事前にSSLの設定をする必要があります

■設定例

dev tap0(ブリッジモード) または dev tun(トンネルモード)

push "route 192.168.1.0 255.255.255.0"

push "dhcp-options DNS 192.168.56.128"

クライアントに経路情報を設定

クライアントにDNSサーバを設定

■クライアント用設定ファイル

- /etc/openvpn/client.conf

■設定例

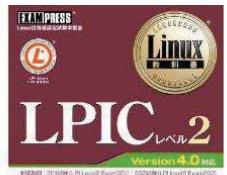
remote 192.168.56.128 1194

サーバのIPアドレス、ポート番号を指定

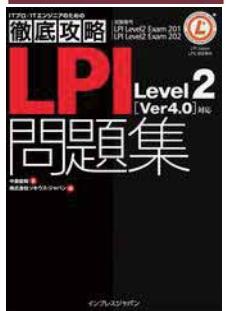


参考資料

Skill Brain



Linux教科書 LPICレベル2 version4対応
リナックスアカデミー 中島 能和 (著), 濱野 賢一朗 (監修)
2014/5/10発行
出版社: 翔泳社
597ページ
定価4,320円
ISBN-10: 4798137510 / ISBN-13: 978-4798137513



徹底攻略LPI 問題集Level2/Version 4 対応
中島 能和 (著), ソキウス・ジャパン (編集)
2014/4/4発行
出版社: インプレスジャパン
360ページ
定価3,456円
ISBN-10: 4844335758 / ISBN-13: 978-4844335757



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



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



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>

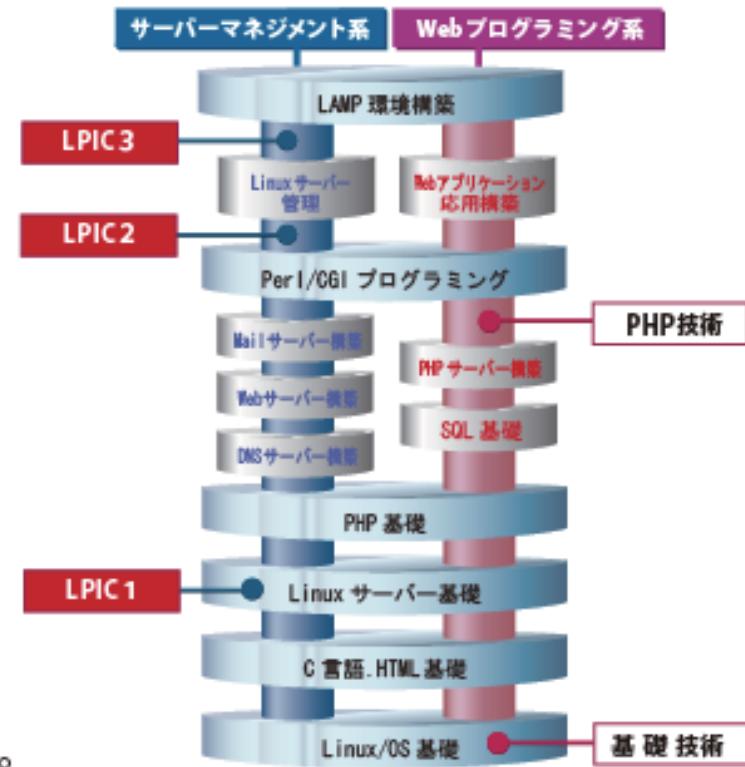


info@skillbrain.co.jp



■ OSS/Linux エンジニア研修

- 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。





経験・スキルと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/UNIX
- 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



各種オープンコース開催日程

Skill Brain

■オープンコース開催日程・特別価格一覧

※表示価格は消費税別途となります。

コース名	期間	受講料(税別) (通常価格)	受講料(税別) (特別価格)	開催日程	会場
VMware vSphere : Install, Configure, Manage [V5.5]	5日間	280,000円 ※受験料別途	220,000円 ※受験料別途	・2014/10/06 ~ 2014/10/10 ・2014/11/10 ~ 2014/11/14 ・2014/12/15 ~ 2014/12/19	品川 御殿山会場
ITILL®インターミディエイト認定 ケイパビリティ (SOA)	5日間	380,000円	285,000円	・2014/11/10 ~ 2014/11/14 ・2014/12/01 ~ 2014/12/05 ・2015/01/19 ~ 2015/01/23 ・2015/02/02 ~ 2015/02/06 ・2015/03/02 ~ 2015/03/05	麹町会場
ITILL®インターミディエイト認定 ケイパビリティ (PPO)	5日間	380,000円	285,000円	・2014/10/27 ~ 2014/10/31 ・2014/12/01 ~ 2014/12/05 ・2015/01/19 ~ 2015/01/23 ・2015/02/16 ~ 2015/02/20 ・2015/03/09 ~ 2015/03/13	麹町会場
ITILL®インターミディエイト認定 ケイパビリティ (RCV)	5日間	380,000円	285,000円	・2014/10/20 ~ 2014/10/24 ・2014/11/10 ~ 2014/11/14 ・2014/12/08 ~ 2014/12/12 ・2015/01/26 ~ 2015/01/30 ・2015/02/16 ~ 2015/02/20 ・2015/03/09 ~ 2015/03/13	麹町会場
ITILL®インターミディエイト認定 ケイパビリティ (OSA)	5日間	380,000円	285,000円	・2014/10/27 ~ 2014/10/31 ・2014/11/17 ~ 2014/11/21 ・2014/12/08 ~ 2014/12/12 ・2015/01/26 ~ 2015/01/30 ・2015/02/23 ~ 2015/02/27 ・2015/03/16 ~ 2015/03/20	麹町会場
ITILL®ライフサイクル全体の管理 (MALC)	5日間	380,000円	285,000円	・2014/12/15 ~ 2014/12/19 ・2015/03/16 ~ 2015/03/20	麹町会場
Cloud Essentials®コース	2日間	165,000円	125,000円	・2014/12/24 ~ 2014/12/25 ・2015/02/09 ~ 2015/02/10	麹町会場
PRINCE2®ファンデーションコース	3日間	270,000	210,000円	・2014/11/04 ~ 2014/11/06 ・2015/03/04 ~ 2015/03/06	麹町会場