Skill Brain
スキルブレイン株式会社

Linux Professional Institute Japan LPI-JAPAN

LPI-Japan 主催
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
河原木　忠司

Agenda

Skill Brain

- セミナー・試験概要
- ver.3.5の試験範囲
- 201試験のポイント
- 202試験のポイント

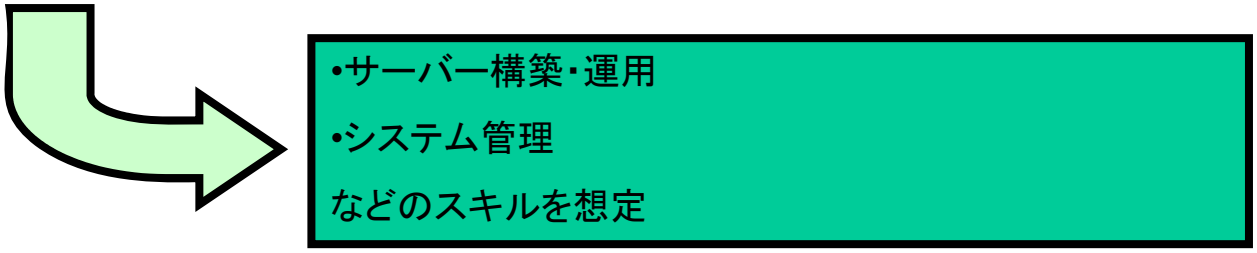
Linux Professional Institute

セミナー・試験概要

LPIC レベル2とは

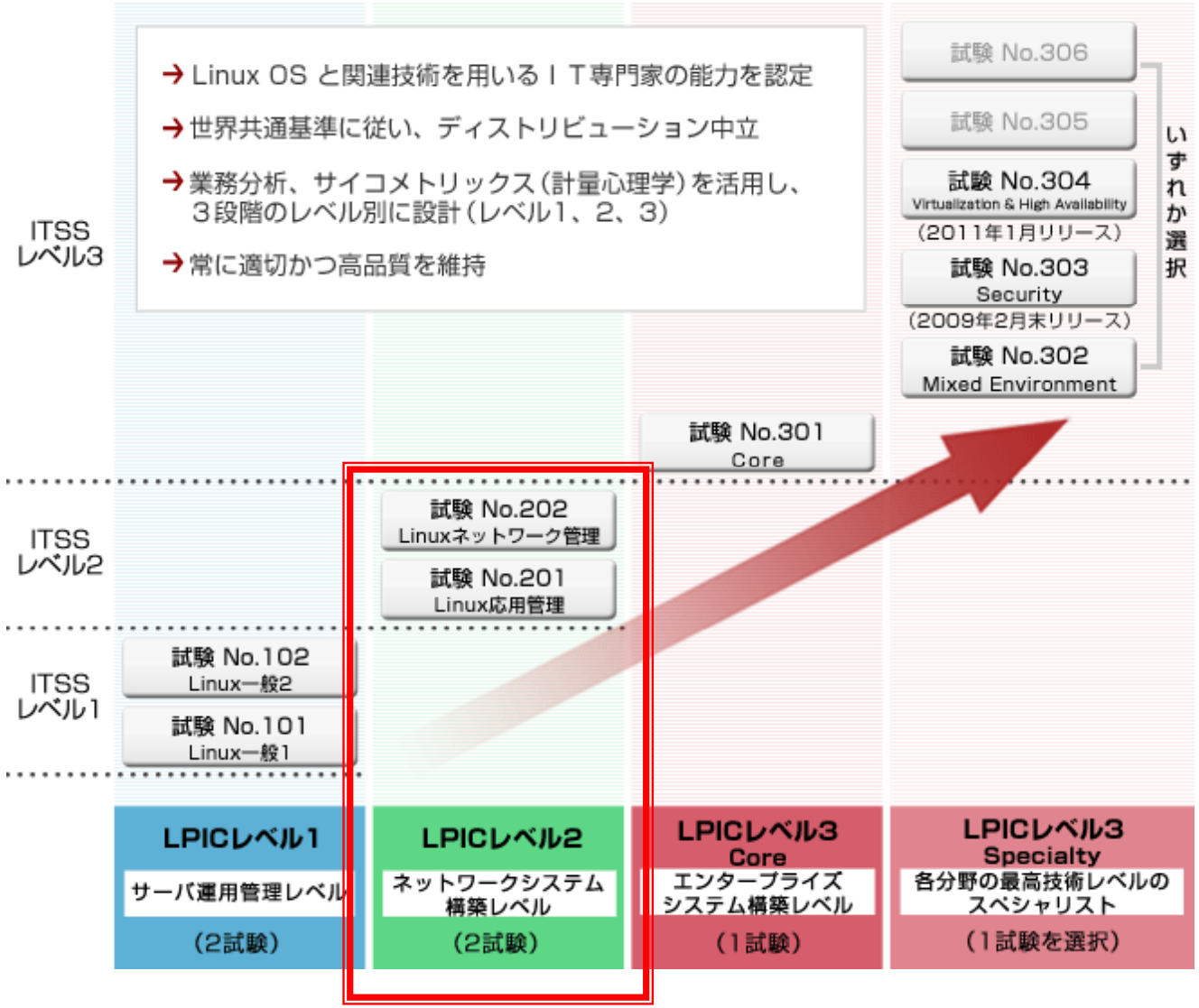
想定されるスキル

- 「アドバンストレベルLinux専門家」を認定
- 次のような小規模の混在 (MS、Linux) ネットワークの計画、実装、保守、一貫性の維持、セキュリティ設定、トラブルシューティングを行う
  - LANサーバ (Samba)
  - インターネットゲートウェイ (ファイアウォール、プロキシ、メール、ニュース)
  - インターネットサーバ (Webサーバ、FTPサーバ)



LPIC レベル2とは

Skill Brain



Linux Professional Institute

ver.3.5試験について

- 日本語試験では、10/1よりver.3.5試験になっております。
- 新傾向について
  - 201試験
    - カーネルが3.xベース
    - ファイルシステムがext4ベース。xfsdump, xfsrestoreも出題範囲に追加。
    - 暗号化ファイルシステム
  - 202試験は出題範囲の変更はありません。

http://www.lpi.or.jp/doc/20120620-101_102.pdf

201試験

- 主題201：Linuxカーネル
- 主題202：システムの起動
- 主題203：ファイルシステムとデバイス
- 主題204：高度なストレージ管理
- 主題205：ネットワーク構成
- 主題206：システムの保守
- 主題207：ドメインネームサーバ

特定のサービスではなく、システム管理系の内容が中心。

例外＞DNS

Lv1試験と関連する部分も多い。

202試験

- 主題208：Webサービス
- 主題209：ファイル共有
- 主題210：ネットワーククライアントの管理
- 主題211：電子メールサービス
- 主題212：システムのセキュリティ
- 主題213：トラブルシューティング

特定のサービスの内容が中心。

セキュリティについては、102試験の内容と重複する部分も。

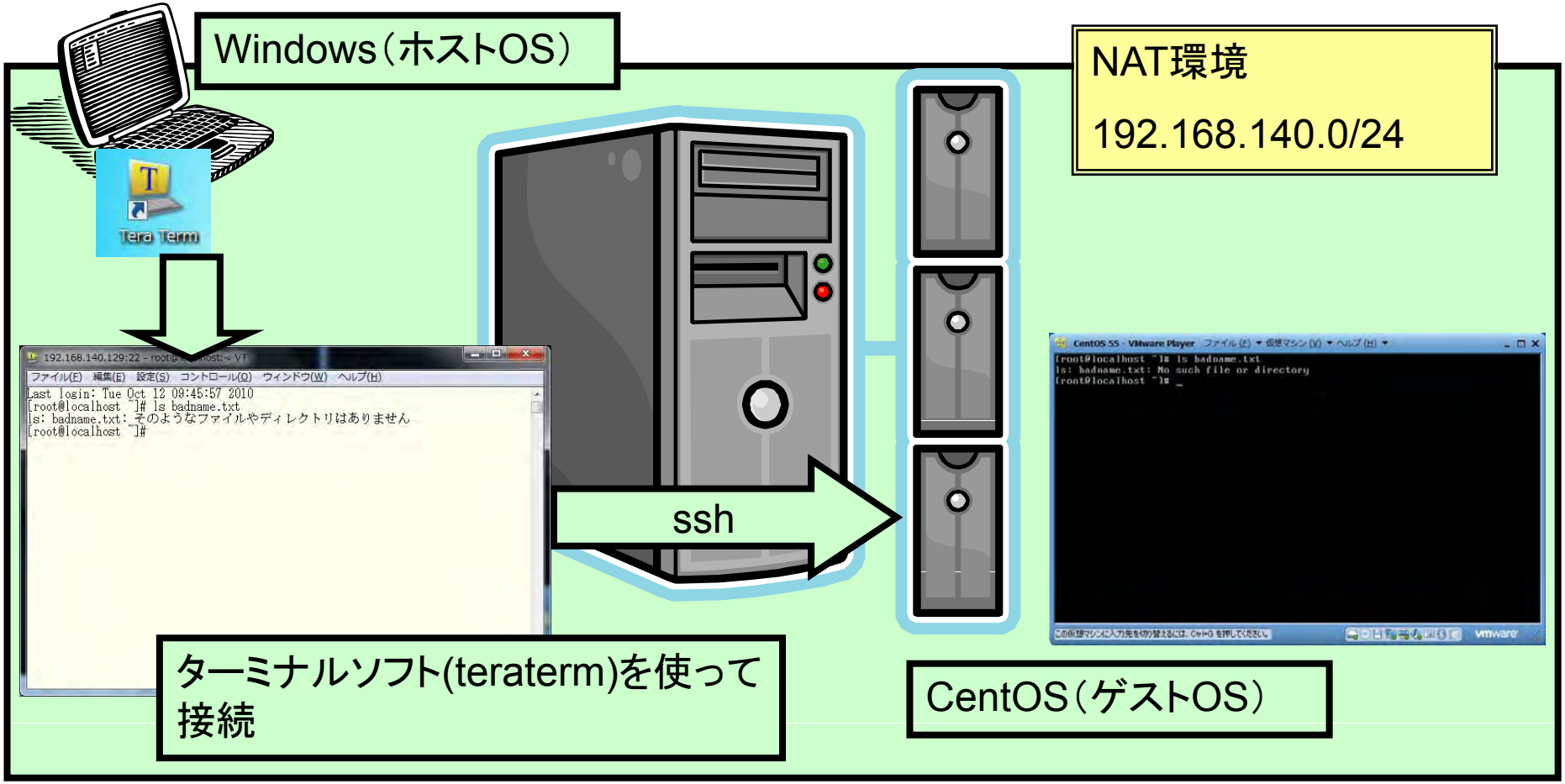
レベル2試験の傾向

Skill Brain

- レベル1試験よりも深い内容について問われる。
- 実際に設定を行った実務スキルについて問われる。
- 流れをつかんだ学習がしやすい
  - サーバーを構築
    →202試験のほとんどの範囲、201試験の一部を網羅できる

セミナーの内容

- 各主題のポイントとなる部分を紹介します。
- 仮想環境を利用し、デモで確認を行います。



201試験のポイント

主題201：Linuxカーネル

Skill Brain

- 201.1 カーネルの構成要素
- 201.2 カーネルのコンパイル
- 201.3 カーネルへのパッチ適用
- 201.4 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
- 201.5 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

例＞raiserfsを利用する

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/kernel
   wget http://www.kernel.org/pub/linux/kernel/v3.0/linux-3.4.14.tar.bz2
   tar xjvf linux-3.4.14.tar.bz2
3. カーネルのカスタマイズ
   make menuconfig
4. コンパイル
   make
5. カーネルモジュールのインストール
   make modules_install
6. カーネルのインストール
   make install
   installkernel 3.4.14 arch/x86/boot/bzImage System.map

xfsを利用できるように設定

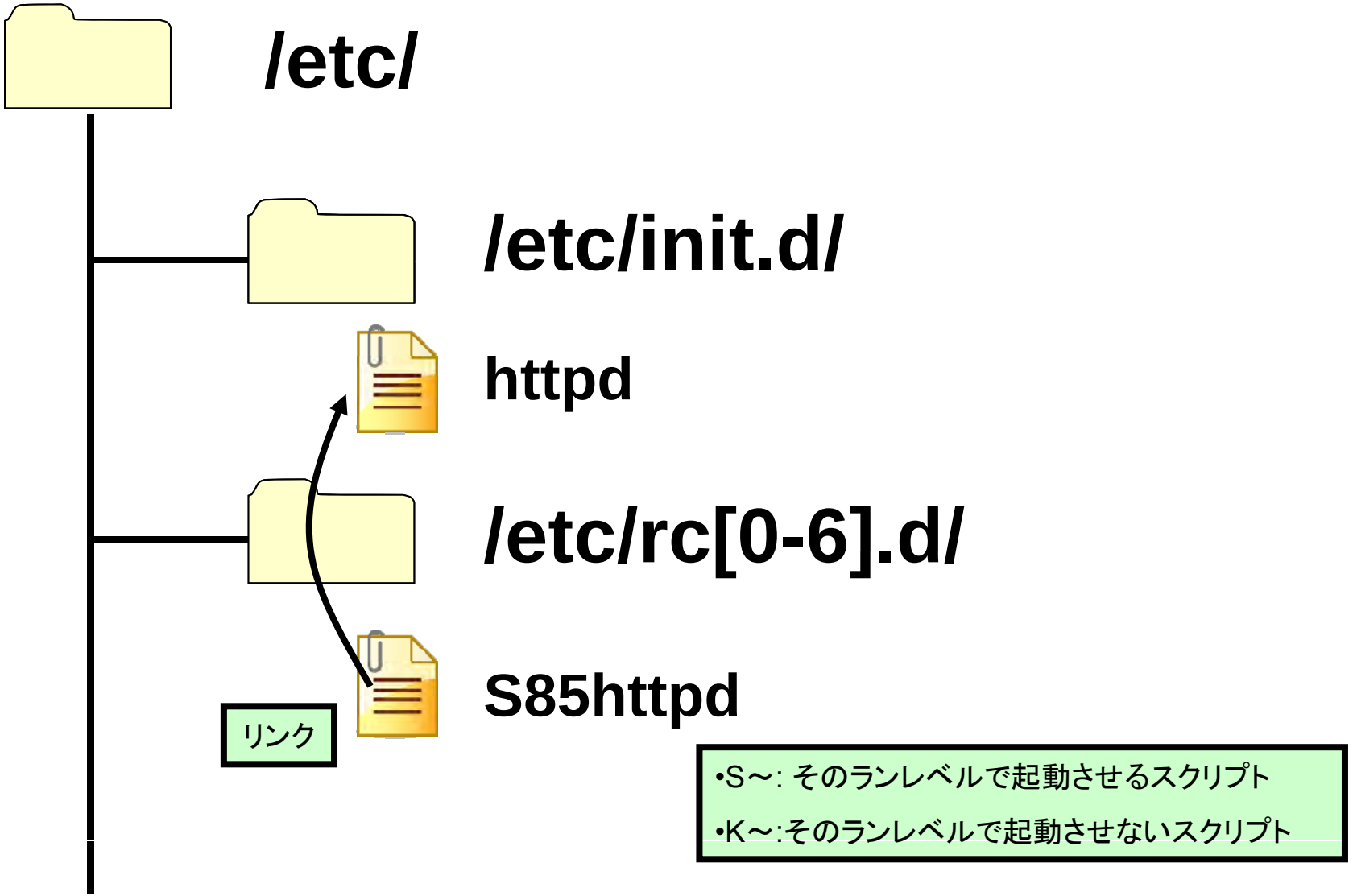
カーネルパラメータ

- カーネルの動作をチューニング
  例＞ブロードキャストICMPエコー要求を無視
  echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
- 設定方法
  - /proc/sys/ 以下のファイルを編集
  - sysctlコマンド
    sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
  - /etc/sysctl.conf

主題202:システムの起動

- 202.1 システムの起動とブートプロセスのカスタマイズ
- 202.2 システムを回復する

起動スクリプト



- S～: そのランレベルで起動させるスクリプト
- K～:そのランレベルで起動させないスクリプト

サービスの制御

- 現状のサービスを制御
  - /etc/init.d/
    - /etc/init.d/httpd start
- 次回起動時のサービスを制御
  - chkconfig (CentOS)
    - chkconfig httpd on
  - update-rc.d, sysv-rc-conf (Debian)
  - insserv (OpenSUSE)

- start:サービスの開始
- stop:サービスの停止
- status:サービスの状態を確認
- restart:サービスの再起動

主題203：ファイルシステムとデバイス

Skill Brain

- 203.1 Linuxファイルシステムを操作する
- 203.2 Linuxファイルシステムの保守
- 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
- 203.4 udevでのデバイス管理

ファイルシステム

- 101試験と重複する部分が多い
- 重複しない部分
  - xfs
    - xfsdump
    - xfsrestore
  - スワップ領域
    - swapon
    - mkswap
  - CD-ROMイメージ
    - mkisofs
  - UUID
    - /dev/disk/by-uuid/

xfs

- xfsdump：xfsファイルシステムのダンプ
- xfsrestore：xfsファイルシステムの復元
- XFSで構成されているパーティションのコピー

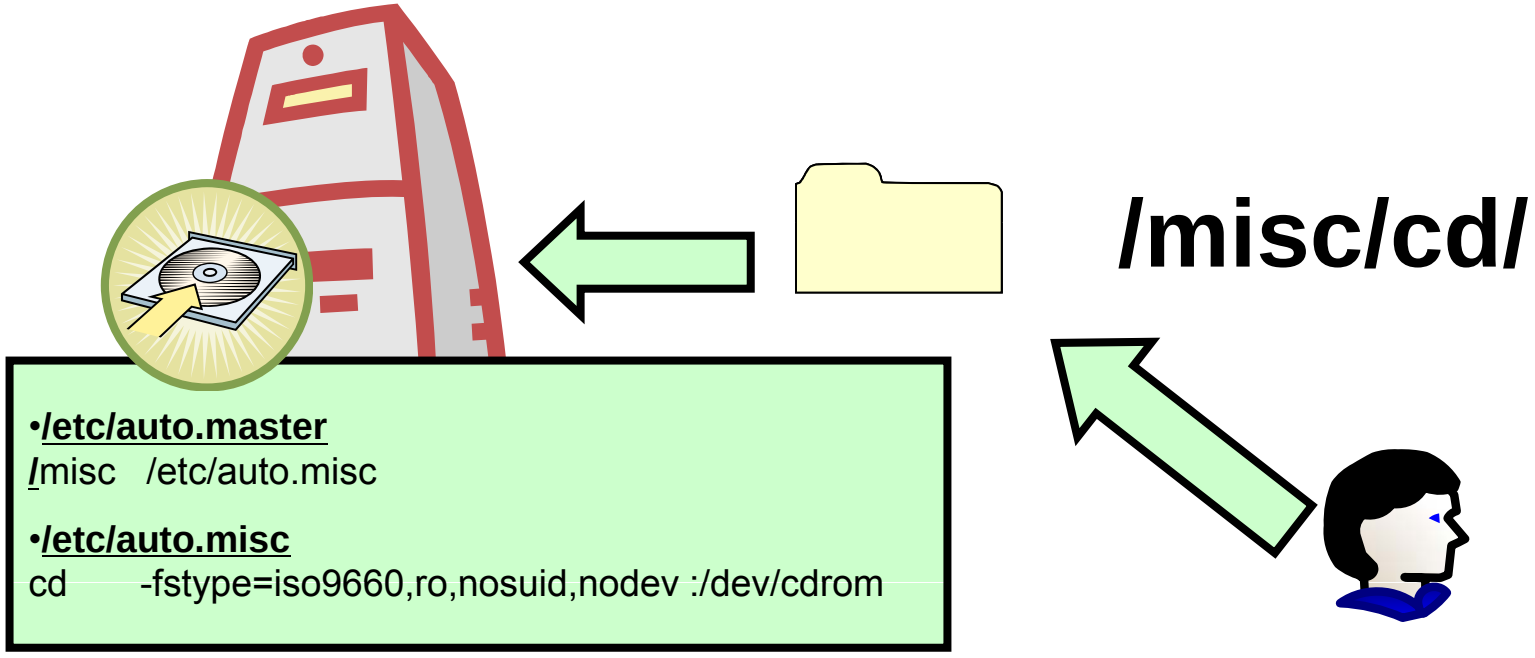
```
# xfsdump -J - /media/sda1 | xfsrestore -J - /media/sdb1
```

スワップ領域の利用


```
[root@centos ~]# dd if=/dev/zero of=/tmp/swapfile bs=1M count=10
[root@centos ~]# mkswap /tmp/swapfile
Setting up swapspace version 1, size = 10481 kB
[root@centos ~]# swapon /tmp/swapfile
[root@centos ~]# swapon -s
Filename                        Type            Size    Used    Priority
/dev/hda2                       partition       522104  60      -1
/tmp/swapfile                   file            10232   0       -2
```

オートマウント

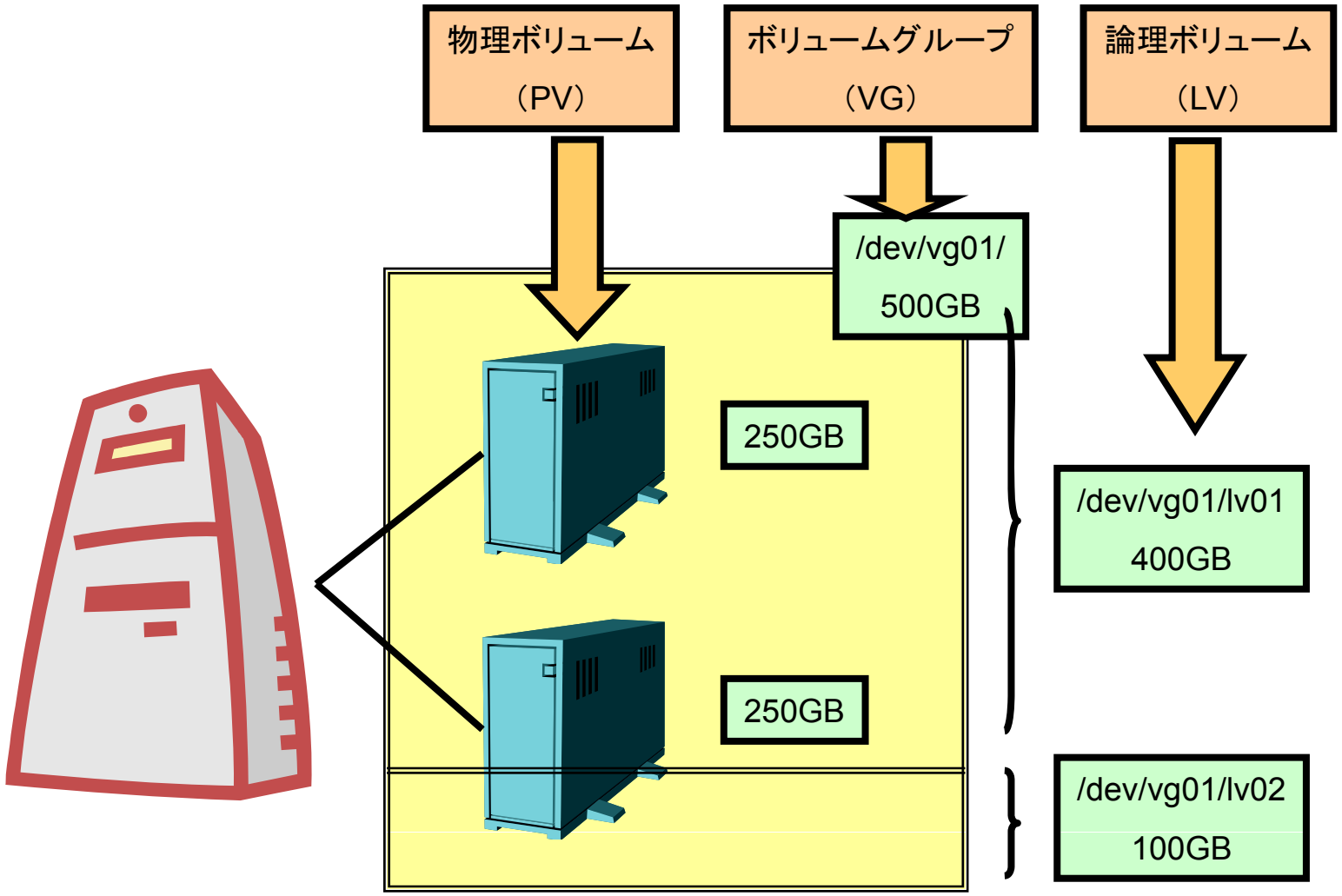
- 指定したディレクトリにアクセス→自動的にマウント
- 設定ファイル
  - /etc/auto.master
  - マップファイル



主題204：高度なストレージ管理

Skill Brain

- 204.1 RAIDを構成する
- 204.2 記憶装置へのアクセス方法を調整する
- 204.3 論理ボリュームマネージャ



LVMの構成

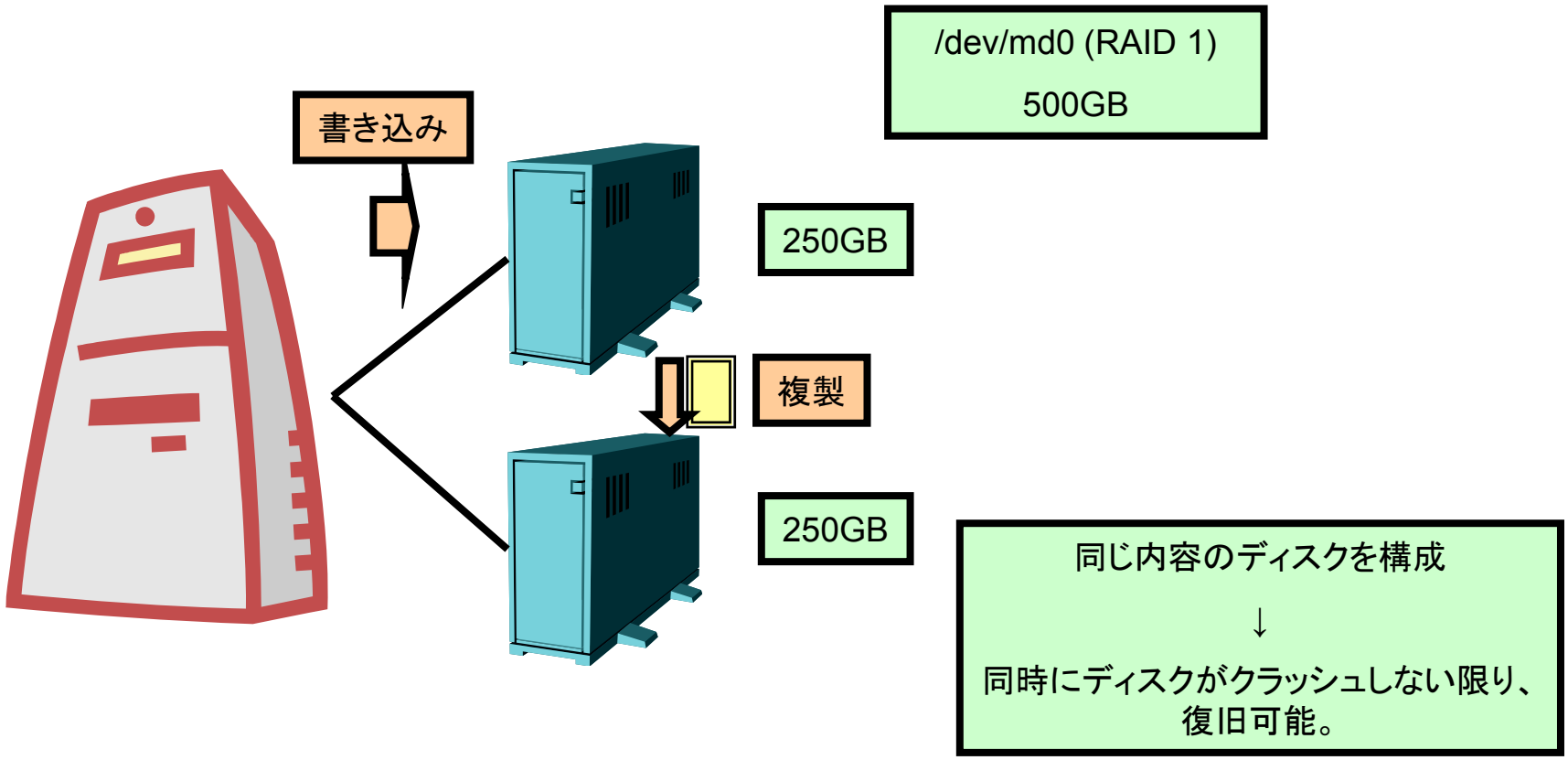

```
[root@centos ~]# pvcreate /dev/sdb2 /dev/sdc1
[root@centos ~]# vgcreate vg01 /dev/sdb2 /dev/sdc1
[root@centos ~]# lvcreate -L 12GB -n lv01 vg01
[root@centos ~]# mkfs -t ext3 /dev/vg01/lv01
[root@centos ~]# mkdir /lvmdir
[root@centos ~]# mount -t ext3 /dev/vg01/lv01 /lvmdir
```

/dev/sdb2と/dev/sdc1を用い、/dev/vg01/lv01という領域を作成

■LVM情報の表示

	全体を表示	各ボリュームを表示
PV	pvscan	pvdisplay /dev/sdb2
VG	vgscan	vgdisplay vg01
LV	lvscan	lvdisplay /dev/vg01/lv01

■ソフトウェアRAID（LinuxがRAIDを管理）が出題



RAIDの構成


```
[root@centos ~]# mdadm -C /dev/md0 --level=1 --raid-devices=2
  /dev/sdb3 /dev/sdc2
mdadm: array /dev/md0 started.
[root@centos ~]# cat /proc/mdstat
Personalities : [raid1]
md0 : active raid1 sdc2[1] sdb3[0]
      3911744 blocks [2/2] [UU]

unused devices: <none>
[root@centos ~]# mdadm --query /dev/md0
/dev/md0: 3.73GiB raid1 2 devices, 0 spares. Use mdadm --detail for
  more detail.
/dev/md0: No md super block found, not an md component.
```

/dev/sdb3と/dev/sdc2という2つのデバイスを用い、RAID1を構成

パーティションタイプの設定


```
[root@localhost ~]# fdisk /dev/hdd
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
領域のシステムタイプを 1 から fd (Linux raid 自動検出) に変更しました

コマンド (m でヘルプ): p

Disk /dev/hdd: 10.7 GB, 10737377280 bytes
16 heads, 63 sectors/track, 20805 cylinders
Units = シリンダ数 of 1008 * 512 = 516096 bytes

デバイス Boot      Start         End      Blocks   Id  System
/dev/hdd1               1        7751     3906472+  fd  Linux raid 自動検出
/dev/hdd2            7752       20805     6579216   83  Linux
```

8e : LVM
fd : RAID

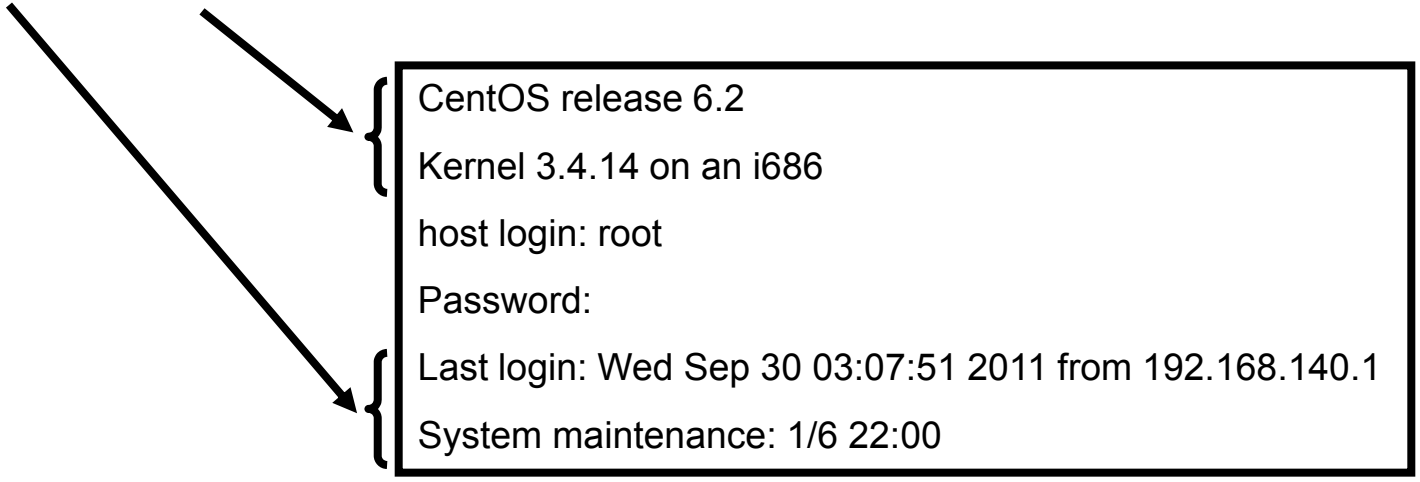
主題205：ネットワーク構成

Skill Brain

- 205.1 基本的なネットワーク構成
- 205.2 高度なネットワーク構成とトラブルシューティング
- 205.3 ネットワークの問題を解決する
- 205.4 システム関連の問題をユーザに通知する

ネットワーク構成

- 102試験と重複する部分が多い
- 重複しない部分
  - tcpdump
  - 無線LAN
    - iwconfig
  - ユーザーへの通知
    - /etc/motd, /etc/issue



tcpdumpの実行例(1)


```
[root@centos ~]# 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 192.168.140.1 > 192.168.140.134: ICMP echo
  request, id 1, seq 1, length 40
01:50:45.798984 IP 192.168.140.134 > 192.168.140.1: ICMP echo
  reply, id 1, seq 1, length 40
01:50:46.709473 IP 192.168.140.1 > 192.168.140.134: ICMP echo
  request, id 1, seq 2, length 40
01:50:46.709533 IP 192.168.14
  reply, id 1, seq 2, length 40
```

192.168.140.1から192.168.140.134宛にpingを実行している。
→echo requestを行い、echo replyが返ってくる

tcpdumpの実行例(2)


```
[root@centos ~]# tcpdump port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol
  decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
01:52:28.996817 IP 192.168.140.1.50372 > 192.168.140.134.http: S
  2890644170:2890644170(0) win 8192 <mss 1460,nop,wscale
  2,nop,nop,sackOK>
01:52:29.091640 IP 192.168.140.134.http > 192.168.140.1.50372: R
  0:0(0) ack 2890644171 win 0
```

192.168.140.1から192.168.140.134宛にhttpポート(80番ポート)宛の接続を行っている。
→IPアドレスの後ろの数値は通信ポート/プロトコル名

主題206：システムの保守

- 206.1 ソースからプログラムをmakeしてインストールする
- 206.2 バックアップ操作

ソースからインストール

1. tar xzvf software.tar.gz
2. cd software
3. ./configure　　→インストール環境の調査、Makefileの生成
4. make　　→コンパイル
5. make install　　→インストール

※インストール時は、root権限が必要

バックアップとリストア

Skill Brain

- バックアップの基本知識
  - オフラインサイトへのバックアップ
  - バックアップの種類（フル・増分・差分）
- ユーティリティ
  - tar
  - cpio
  - dd

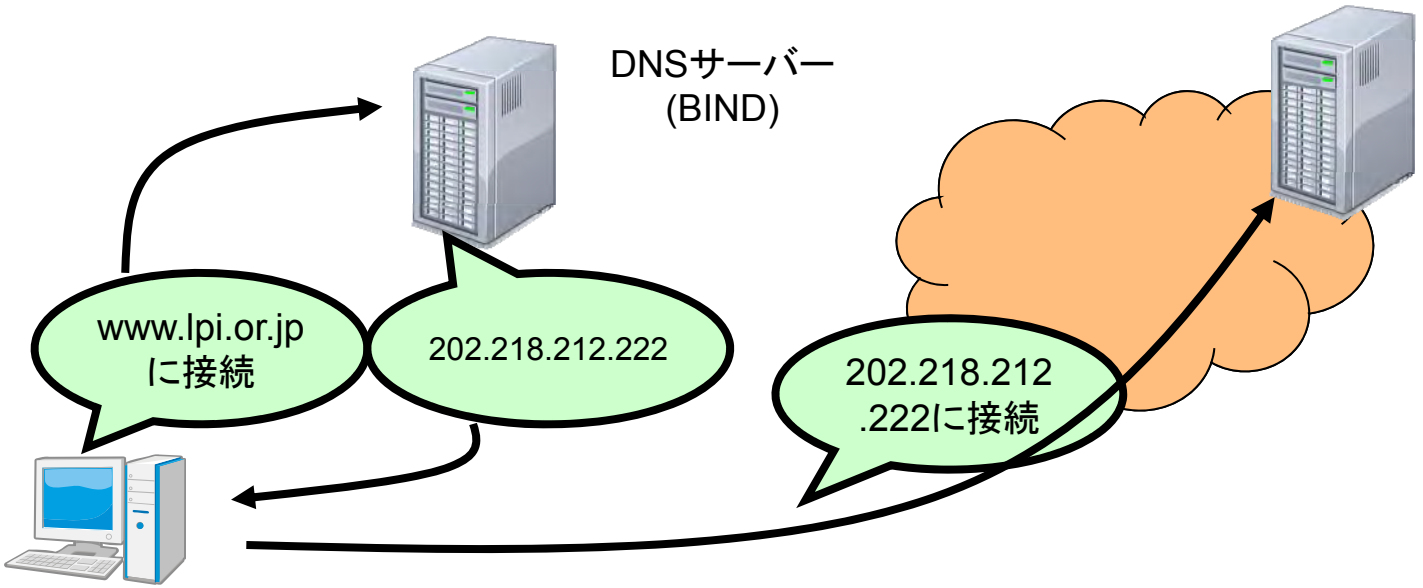
主題207:ドメインネームサーバ

Skill Brain

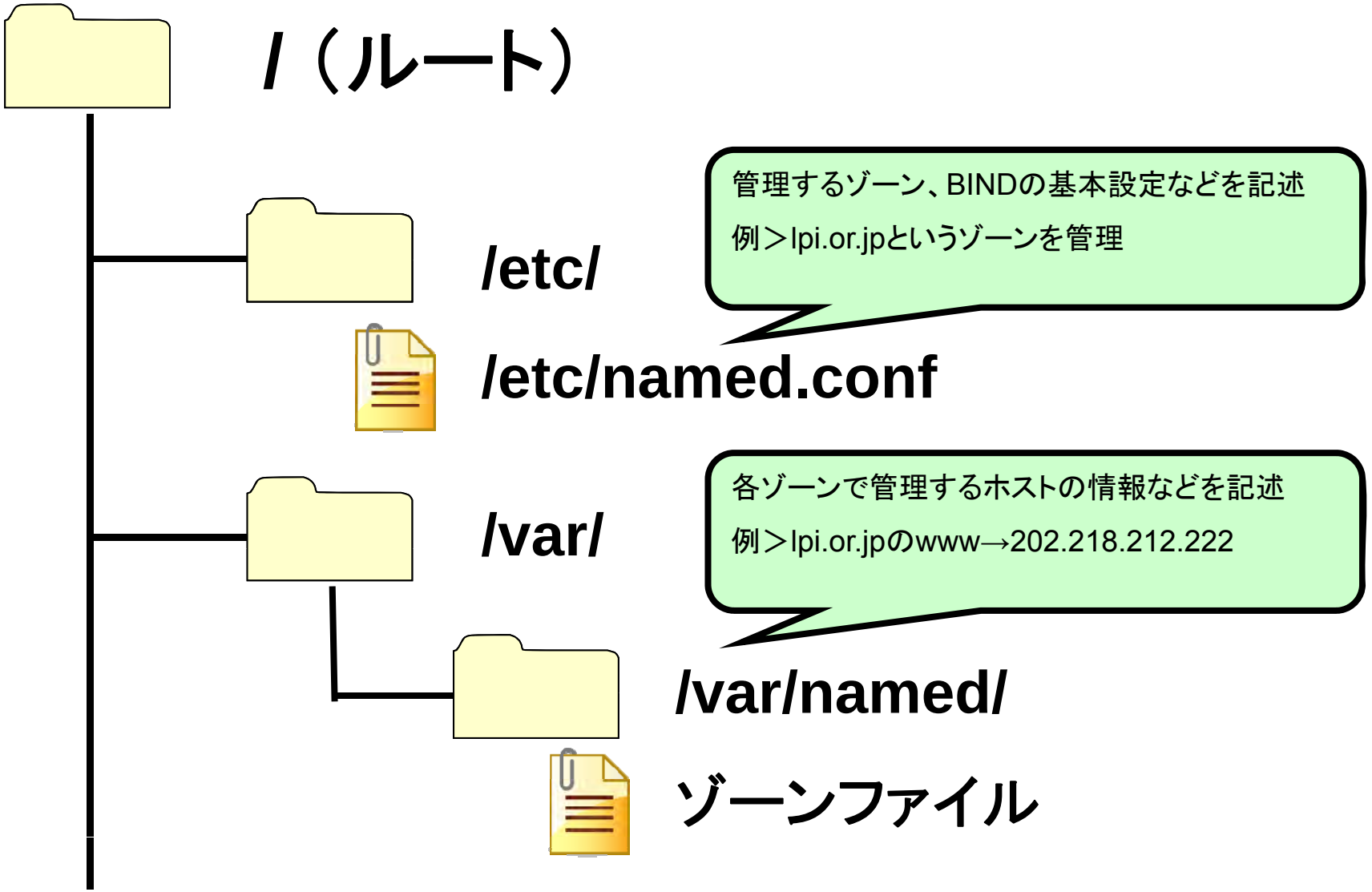
- 207.1 DNSサーバの基本的な設定
- 207.2 DNSゾーンの作成と保守
- 207.3 DNSサーバを保護する

DNSの基本

- 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
- BIND
  - 広く使われているDNSサーバーアプリ
- ゾーン
  - DNSサーバーが管理する名前空間の範囲



BINDの設定ファイル



named.conf

■namedの基本設定と管理するゾーンを記述

■設定例

```
options {
        directory "/var/named";
};

zone "example.net" {
        type master;
        file "example.net.zone";
};
```

ゾーンファイルの保存場所

/var/named/example.net.zone

※bind-chrootがインストールされていると
/var/named/chrootディレクトリ以下
→ /var/named/chroot/var/named/～.zone

ゾーンファイル

■設定例

```
$TTL 86400
@       IN      SOA     host.example.net.  root.example.net.  (
                        2012101101
                        86400
                        21600
                        864000
                        86400 )

        IN      NS      host.example.net.
        IN      MX  10  host.example.net.

host    IN      A       192.168.140.134
www     IN      CNAME   host.example.net.
```

- 基本的な構成
  名前 IN レコードの種類 値
- 特殊な記述
  @はゾーン名を表す
  名前が空欄の場合、上位のレコードの情報を参照
- ホスト名の記述
  後ろに「.」をつけない場合、ゾーン名が補完される。
- MXレコードの記述
  レコードの種類の右側に、プレフィックス値を記述。値の低いサーバを優先して参照。

ゾーン転送

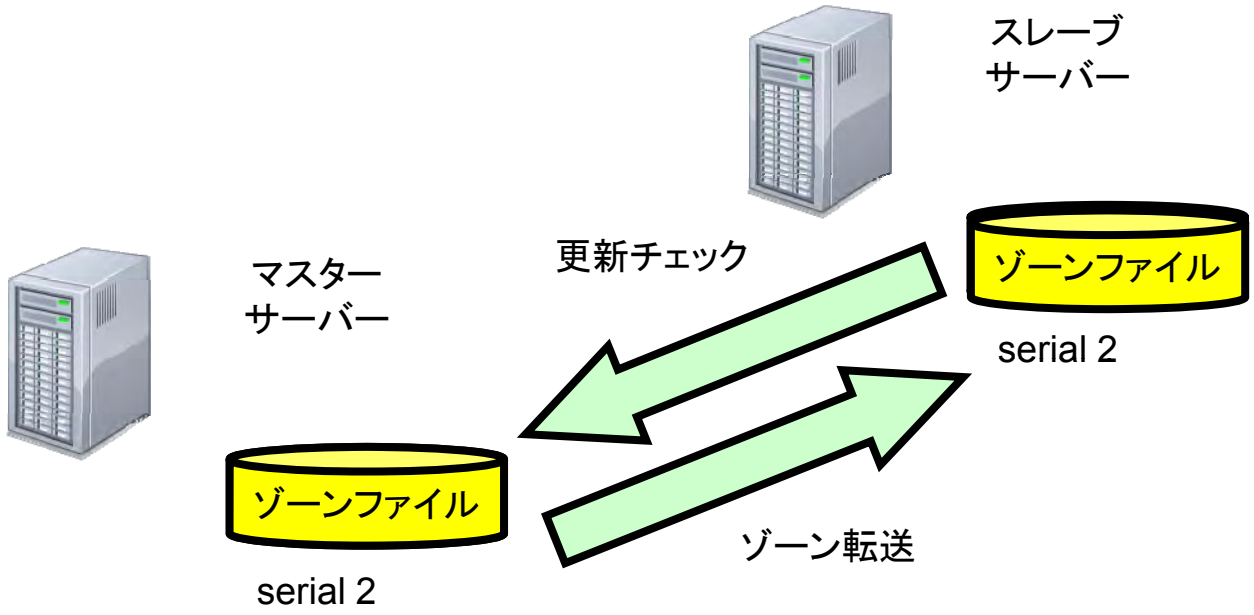
■設定例

マスターサーバーのnamed.conf

```
options {
    allow-transfer { 192.168.140.2; };
};

zone "example.net" {
    type master;
    file "example.net.zone";
};
```

スレーブサーバーのnamed.conf

```
zone "example.net" {
    type slave;
    file "slaves/example.net.zone";
    masters { 192.168.140.1; };
};
```



TSIG

■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 192.168.140.1{
    keys "example.net";
];

zone "example.net" {
    type slave;
    file "example.net.zone";
    masters { 192.168.140.1; };
};
```

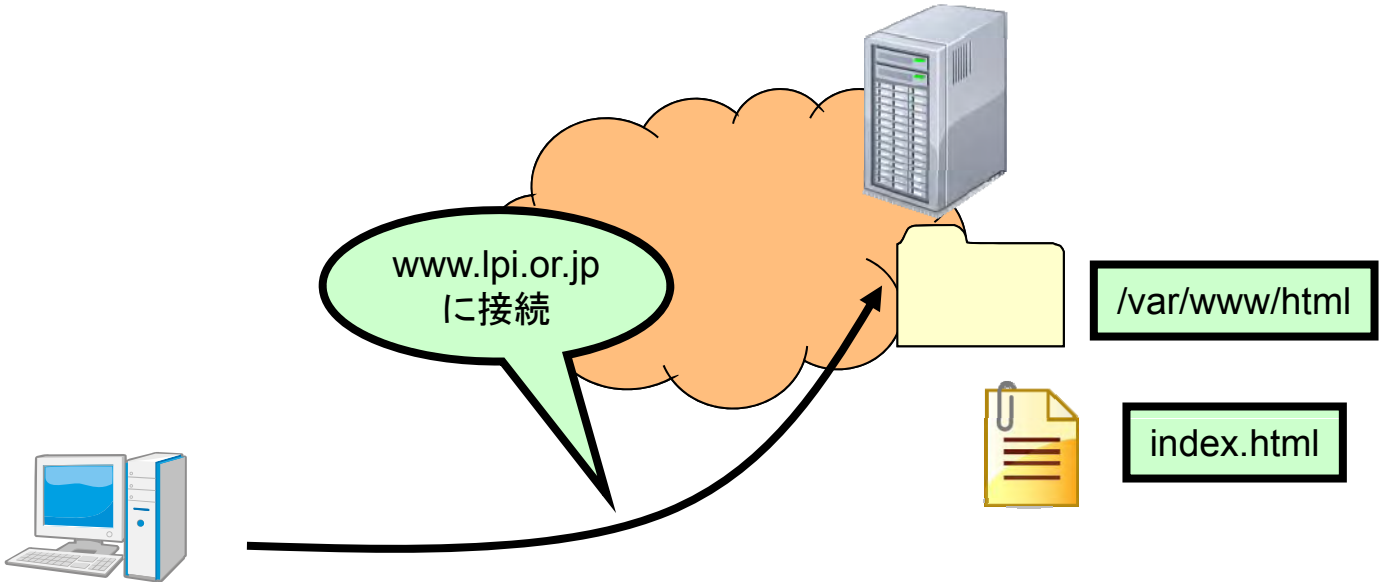
202試験のポイント

主題208：Webサービス

- 208.1 Webサーバの実装
- 208.2 Webサーバの保守
- 208.3 プロキシサーバの実装

Apache httpd

- 広く使われているWebサーバーアプリ
- 設定ファイル
  - httpd.conf
  - 「ディレクティブ名　値」という形で設定

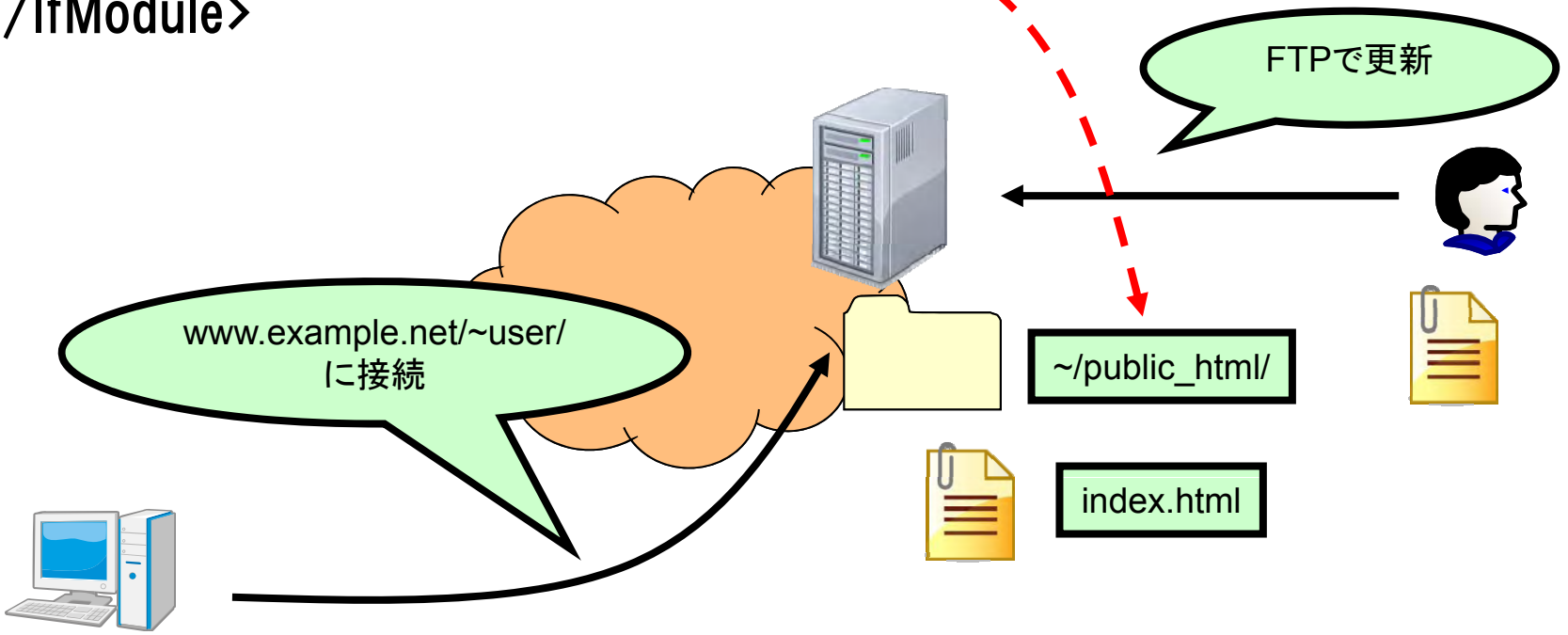


UserDir

■ユーザーごとに公開領域を設定

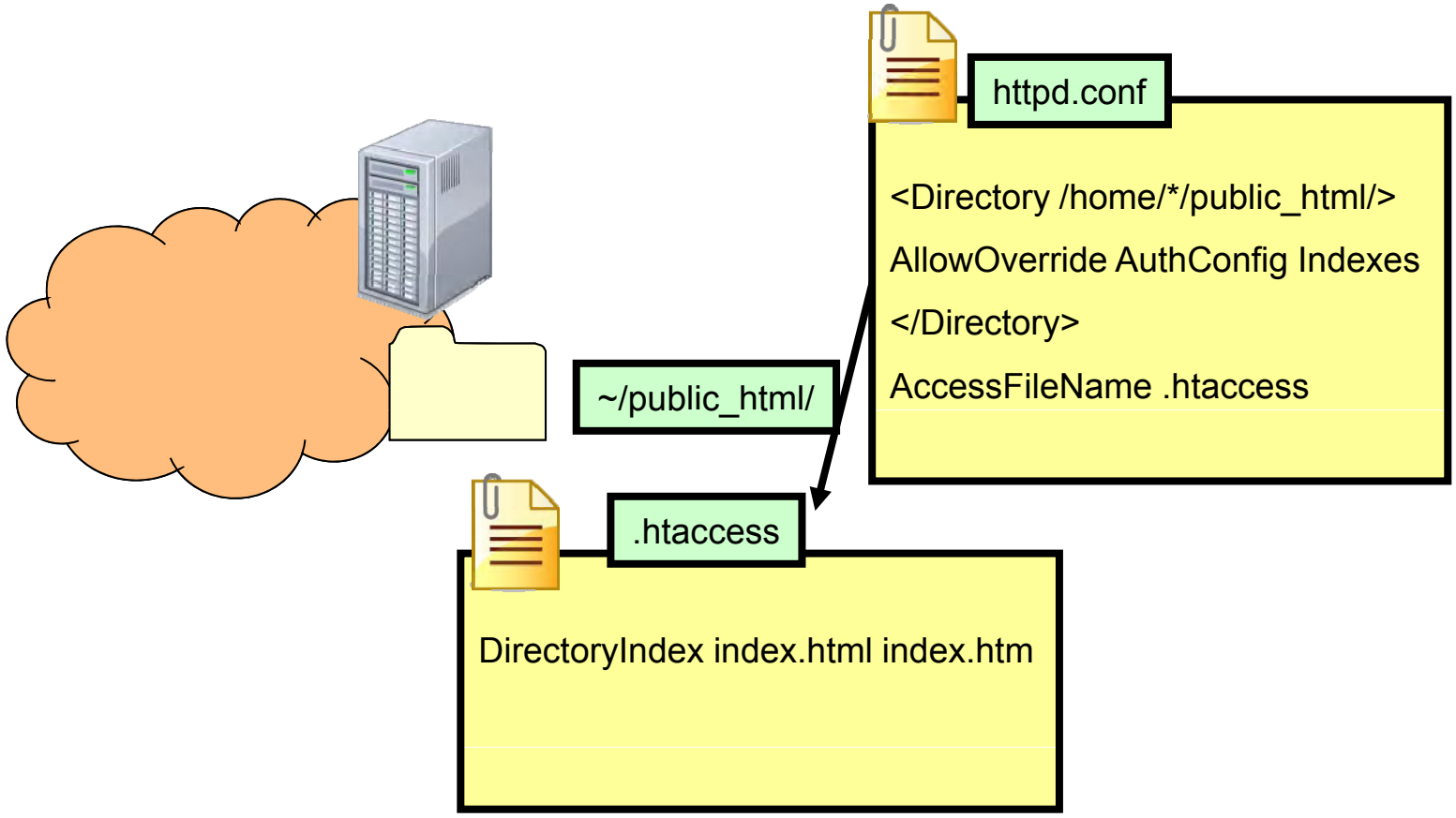
■設定例＞

```
<IfModules mod_usermod.c>
    UserDir public_html
</IfModule>
```



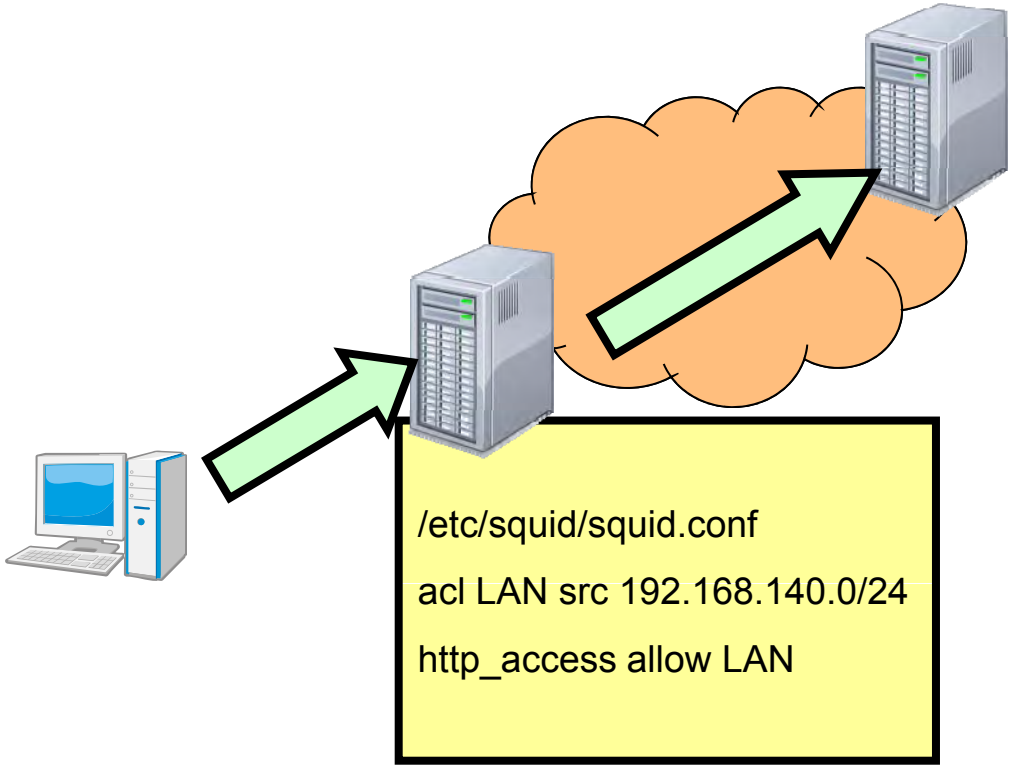
ディレクトリごとの設定情報

- .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。



squid

- Webプロキシ・キャッシュサーバー
- 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



主題209:ファイル共有

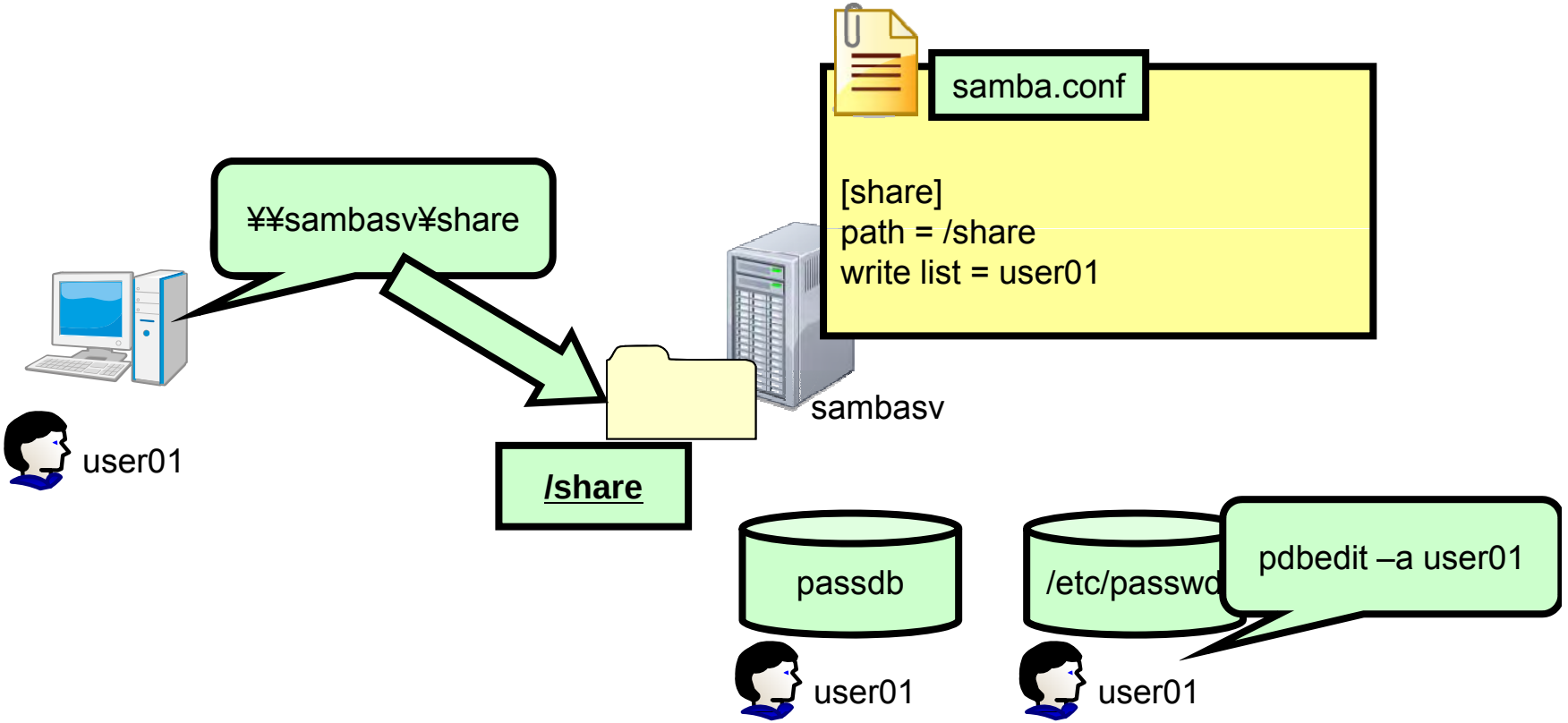
- 209.1 Sambaサーバの設定
- 209.2 NFSサーバの設定

Samba

- 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
  - 確認：testparm

Sambaの接続例

- 接続時にユーザー認証
- pdbeditでユーザー登録
  - 対応するUNIXユーザーも必要

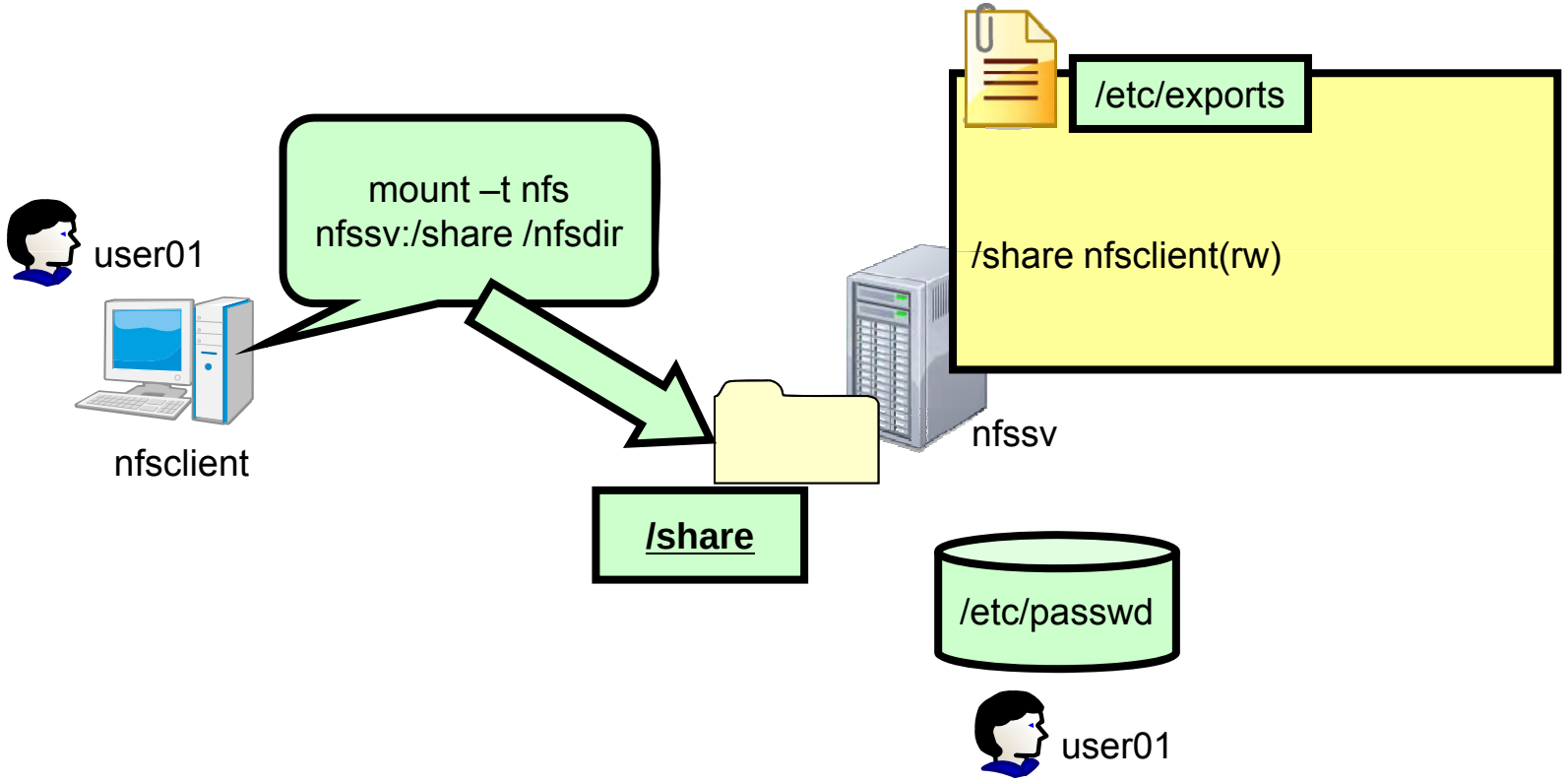


NFS

- 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
- サービス
  - portmap
  - nfsd
  - mountd
- 設定ファイル
  - /etc/exports
- ユーザー管理
  - ユーザー認証はなし
  - クライアント側でログインしたUIDを利用

NFSの接続例

- 認証はホストベース
  - ユーザー認証は行わない。
  - 接続元ホストでログインしているUIDを参照し、アクセス制御



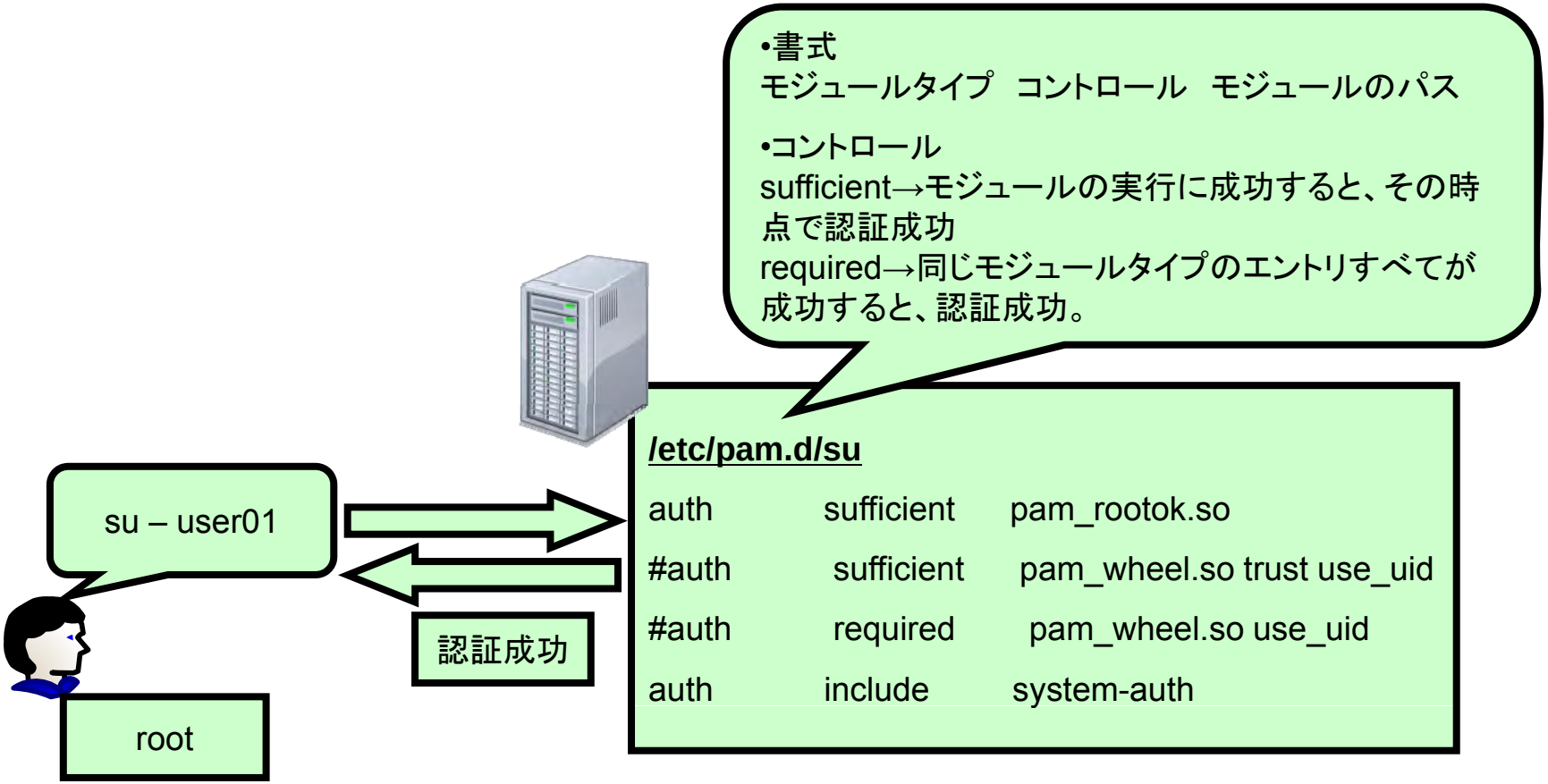
主題210：ネットワーククライアントの管理 Skill Brain

- 210.1 DHCPの設定
- 210.2 PAM認証
- 210.3 LDAPクライアントの利用方法

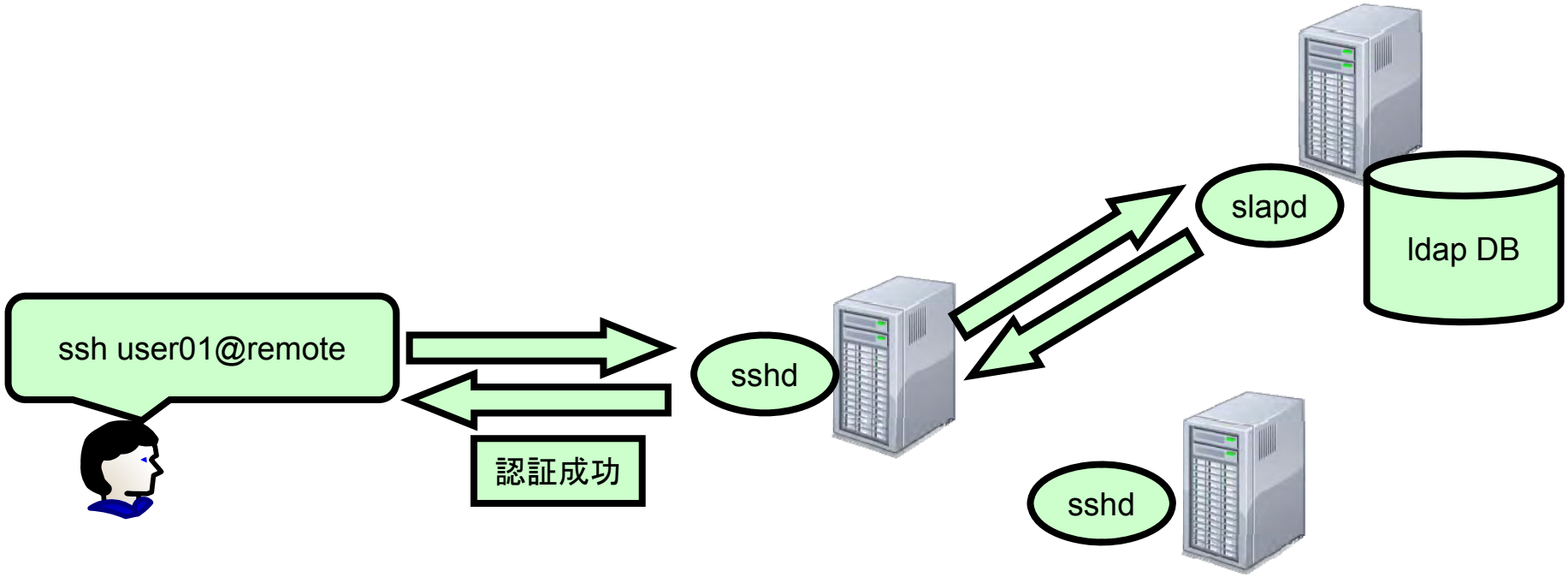
■設定ファイル：/etc/dhcpd.conf

```
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

         range dynamic-bootp 192.168.0.128 192.168.0.254;
         default-lease-time 21600;
         max-lease-time 43200;
}
```

- 認証機能を提供
- /etc/pam.d/ディレクトリに各種アプリ用の設定ファイルが用意されている。



- 標準仕様のディレクトリサービス
- 301試験で詳しく出題。202試験では基本が出題。
  - クライアントコマンド
    - ldapadd, ldapsearch, ldapdelete
  - 設定ファイル：/etc/openldap/slapd.conf

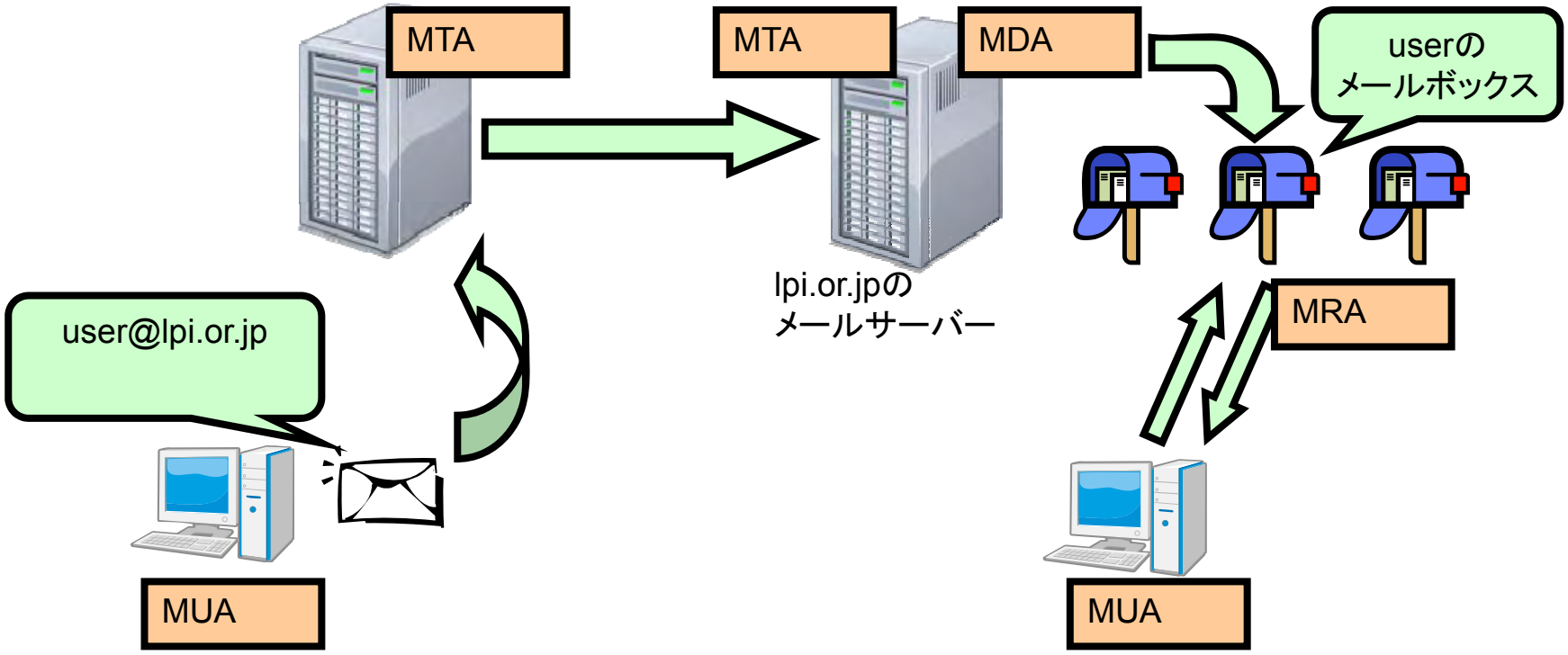


主題211：電子メールサービス

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

メールシステム

- 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, courrier IMAP】



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/mqueue/ (sendmail)
    - /var/spool/postfix/ (postfix)

■main.cfの設定例

```
myhostname = host.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
                                →宛先として使用できる名前
mynetwork = 192.168.140.0/24, 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送先
mailbox_command = /usr/bin/procmail
                                →メール配送時の処理
```

Procmail

- 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
- 記述例

```
PATH=/bin:/usr/bin:/usr/sbin
MAILDIR=$HOME/Maildir/
LOGFILE=$HOME/.procmaillog
DEFAULT=$MAILDIR

:0
* ^Subject:.*SPAM.*
/dev/null
```

•レシピの記述ルール

:0 フラグ
* 条件
アクション

主題212:システムのセキュリティ

Skill Brain

- 212.1 ルータを構成する
- 212.2 FTPサーバの保護
- 212.3 セキュアシェル(SSH)
- 212.4 TCPラッパー
- 212.5 セキュリティ業務

Linux Professional Institute

システムのセキュリティ

Skill Brain

- 102試験と重複する部分が多い
- 重複しない部分
  - FTPサーバの保護
  - セキュリティ業務

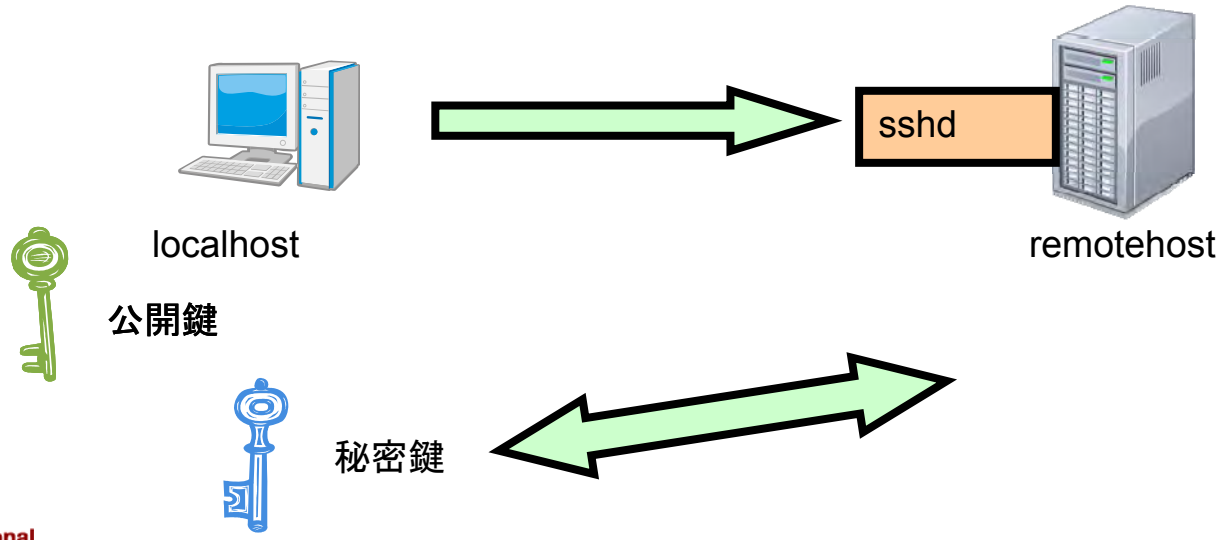
ssh認証（公開鍵認証）

```
[root@localhost ~]# ssh-keygen -t dsa
[root@localhost ~]# scp .ssh/id_dsa.pub remotehost:/root
                    [root@remotehost ~]# cat id_dsa.pub >> .ssh/authorized_keys
[root@localhost ~]# ssh remotehost
[root@remotehost ~]#
```

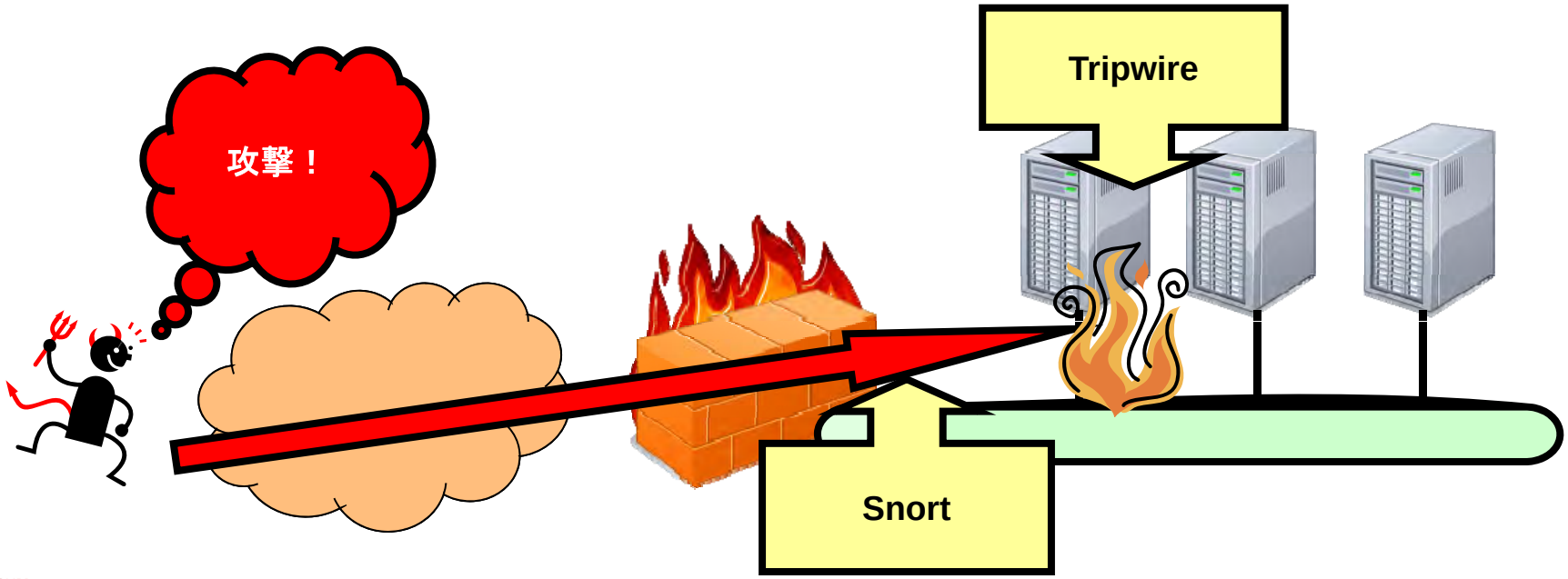
ssh-agent

秘密鍵利用時のパスフレーズを保存

```
[root@remotehost ~]# vi /etc/ssh/sshd_config
PasswordAuthentication no
```



Snort	IDS（侵入検知システム）。ルールセットに基づいて、ネットワーク上に流れる攻撃的なパケットを検知。
Tripwire	改ざん検知ツール。ファイルシステムを監視し、意図しない変更があった場合、通知。
OpenVAS	セキュリティスキャナ。脆弱性を検知。



主題213:トラブルシューティング

Skill Brain

- 213.1 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
- 213.2 一般的な問題を解決する
- 213.3 システムリソースの問題を解決する
- 213.4 環境設定の問題を解決する

トラブルシューティング

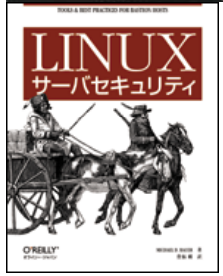
- これまで学習してきたコマンド・設定ファイル絡みでトラブルシュートに関わるものを総動員する。
  →201試験、主題201（カーネルパラメータ）、主題202（ブートローダ）など
- 新しく出題範囲となっているもの
  - strace, ltrace
    システムコール、ライブラリコールをトレース
  - /etc/login.defs
    パスワードの期限など、ユーザー登録時に参照する既定値を設定

参考資料

Skill Brain

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/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

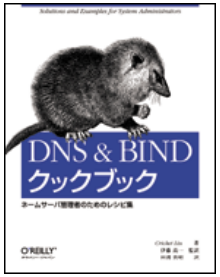
Linuxクックブック——Linuxを120%使いこなすレシピ集
Carla Schroder 著、林 秀幸 訳
2005/10発行
出版社: O'Reilly Japan
444ページ
定価3,780円
ISBN4-87311-248-6

Linux Professional Institute

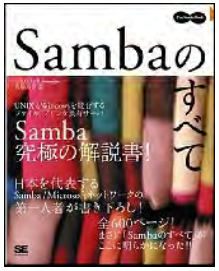
参考資料

Skill Brain

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（Ver1.0.2）
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 Professional Institute

スキルブレインの研修案内

Skill Brain

スキルブレインでは、社内研修・新入社員研修などの講師派遣も行っております。
経験・スキルともに豊富な講師陣とコンサルタントが技術や資格取得をサポートします。

- Linux 基礎
- LPIC レベル１ 試験対策
- Linux サーバー構築実践
- LPIC レベル２ 試験対策
- 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３試験対策
- TITL ファンデーション / エキスパート
- Cisco 認定 CCNA 講座
- Oracle 認定 JAVA 試験対策 (OCJ-A・P・WC)
- MCP 試験対策講座

※その他、企業様ごとにセミオーダー研修を承ります。

http://www.skillbrain.co.jp

info@skillbrain.co.jp

Linux Professional Institute

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
〒141-0031　東京都品川区西五反田8-2-6