

LinuC レベル2 技術解説無料セミナー

～LinuC レベル2 受験に向けての準備とポイント解説～

2019/06/30

株式会社アイエスエイ
木村 淳矢



本日のアジェンダ

1. はじめに
2. 各主題解説
 - 主題200 : キャパシティプランニング
 - 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
 - 主題208 : HTTP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
- ※60分の間に10分間の休憩をはさみます。



はじめに

■自己紹介

- ・木村淳矢
- ・ISA PCスクール ネットワーク関連講座講師

■所属会社

- ・株式会社アイエスエイ
- ・新宿、銀座、渋谷など関東圏に13校を展開する総合パソコンスクールです。
- ・新宿校は毎週土曜日にPearson Vueの試験会場となっています。
- ・LinuC Level2取得講座などを開講しています。

■内容

- ・LinuC Level2の試験に出るポイント



LinuC Level2試験とは

- LinuCレベル2に認定されるためには201試験と202試験の受験が必須です。LinuC レベル2は、「ネットワークを含むLinuxシステムの構築・運用・管理の専門家」を認定する資格試験です。
- 出題範囲のそれぞれの項目には、重要度として重み付けがなされています。重要度の範囲は概ね1～10であり、それぞれの主題の相対的な重要性を示しています。重要度が高い主題ほど、試験において多くの問題が出題されます。



■ Point

- ① CPU使用率、メモリ使用率などの計測

■ リソース使用率の特定をするコマンド

コマンド	説明
top	システムリソースの使用状況やプロセスの実行状態の確認
vmstat	メモリ、仮想メモリの詳細な状態を確認
netstat、ss	NICの情報を確認
sar	システム情報の統計を確認
uptime	システムの稼働時間やロードアベレージを確認
w	各ユーザのプロセス情報を表示
ps	プロセス単位でのシステムの情報を確認
pstree	プロセスの親子関係をツリー形式で表示
free	メモリの使用率を測定



■ Point

- ① カーネルバージョン ③ カーネルの管理
- ② カーネルモジュール

■ `uname` (カーネルのバージョン確認)

■ カーネルモジュールのコマンド

コマンド	説明
<code>lsmod</code>	ロードされているモジュールの表示
<code>insmod</code>	モジュールのロード
<code>rmmod</code>	モジュールのアンロード
<code>modprobe</code>	依存関係を解決してモジュールをロード、アンロードする
<code>modinfo</code>	モジュールの状態の表示



■ Point

- ① カーネルバージョン ③ カーネルの管理
- ② カーネルモジュール

■ カーネルのコンパイル

カーネルのコンパイル手順

1. カーネルコンパイル用のディレクトリを作成して、カーネルソースをDLする
2. カーネルソースを展開し、カーネルの設定をする
3. カーネルをコンパイルする
4. モジュールをコンパイルする
5. /bootディレクトリにカーネルをコピーする
6. RAMディスクの作成をする
7. ブートローダーの設定をする



■ Point

- ① ブートシーケンス
- ② サービスの自動起動
- ③ Systemd
- ④ GRUB
- ⑤ システムの回復

■ ブートシーケンス

1. BIOS・UEFI
メモリチェック、ハードウェア設定の読み込み、起動デバイスのチェック、ブートローダを実行
2. MBR・GPT
MBRにはブートローダーの一部、パーティションテーブル
3. ブートローダー（GRUB Legacy、GRUB2）
カーネルのロード
4. カーネルがルートパーティションをマウント、initを起動する



■ Point

- ① ブートシーケンス
- ② サービスの起動
- ③ Systemd

④ GRUB

- ⑤ システムの回復

■ サービスの起動

/etc/rc#.d ディレクトリに対象のランレベルで起動するサービスが入っている
サービスは/etc/init.d/へのシンボリックリンクになっている

■ systemd

systemdはinit/upstartの後継、unit単位で管理
systemctlコマンドでサービスを管理できる



■ Point

- ① ブートシーケンス
- ② サービスの起動
- ③ Systemd

④ GRUB

- ⑤ システムの回復

■ GRUB

GRUB LegacyとGRUB2がある

grub-install、grub2-installコマンドでGRUBをインストールできる

/boot/grub/menu.lstがGRUB Legacyの設定ファイル

/boot/grub/grub.cfgがGRUB2の設定ファイル

GRUB2では、grub2-mkconfigコマンドでgrub.cfgを作成

■ システムの回復

システムが起動しなくなった時にレスキューモードで起動しシステムを修復する

レスキューモードはルートファイルシステムが/mnt/sysimageなどにマウントされる



■ Point

- ① ファイルシステムの操作
- ② ファイルシステムの保守

■ /etc/fstab

ファイルシステムの情報が記載されている

- ファイルシステムのマウント、アンマウントにはmount、umountコマンドを使う
- スワップ領域の管理はmkswap、swapon、swapoffコマンドを使う
- ファイルシステムの作成

mke2fs	ext2、ext3、ext4ファイルシステムの作成
mkfs.ext4	ext4ファイルシステムの作成
mkfs.xfs	XFSファイルシステムの作成
mkfs.btrfs	B-treeファイルシステムの作成
mkisofs	CD/DVDの作成



■ Point

- ① ファイルシステムの操作
- ② ファイルシステムの保守

- fsck、e2fsckコマンドでファイルシステムの整合性のチェックができる
- ext2、ext3、ext4のファイルシステムのパラメータを調整するためにはtune2fsコマンド



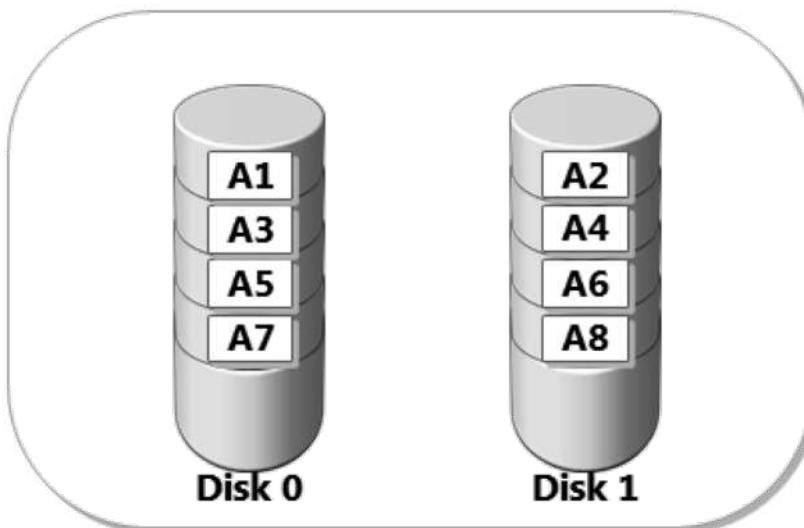
■ Point

- ① RAID
- ② LVM

■ RAIDはデータを複数のハードディスクに分散することで、性能と耐障害性などを確保するための技術

ソフトウェアRAIDの構成にはmdadmコマンドを使う

RAID0：パリティ、ミラーリングを持たないストライピング



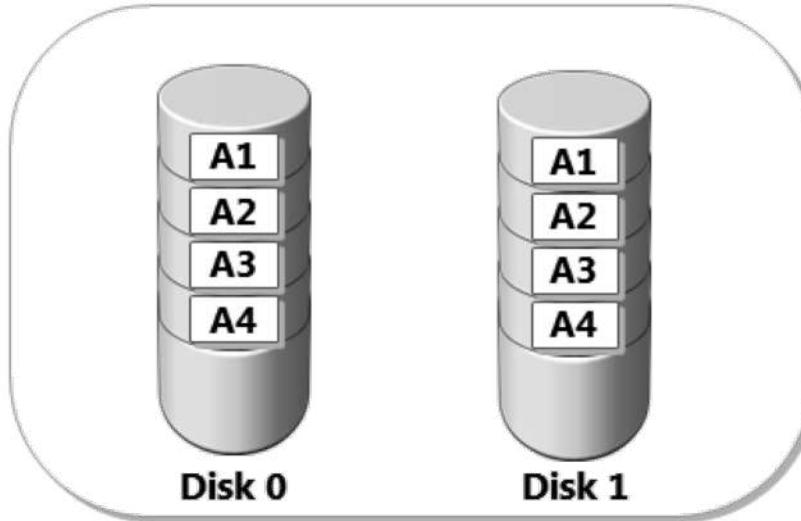


■ Point

- ① RAID
- ② LVM

■ RAIDはデータを複数のハードディスクに分散することで、性能と耐障害性などを確保するための技術

RAID1：ミラーリング



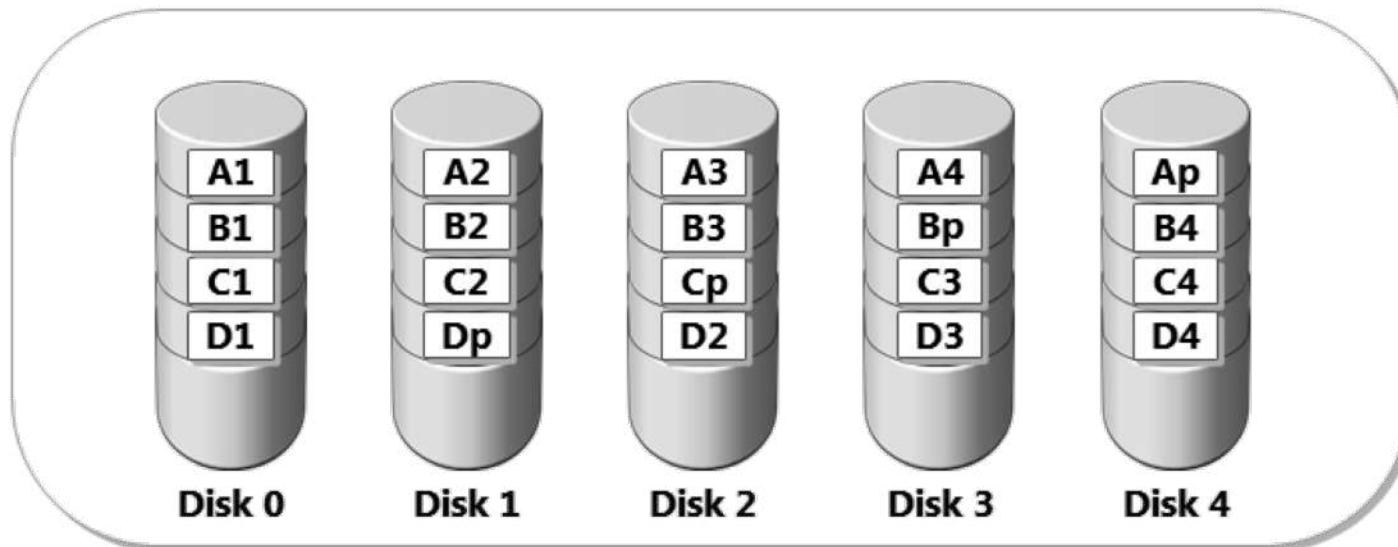


■ Point

- ① RAID
- ② LVM

■ RAIDはデータを複数のハードディスクに分散することで、性能と耐障害性などを確保するための技術

RAID5：3つ以上のディスクに分配されたパリティ情報を持つストライピング



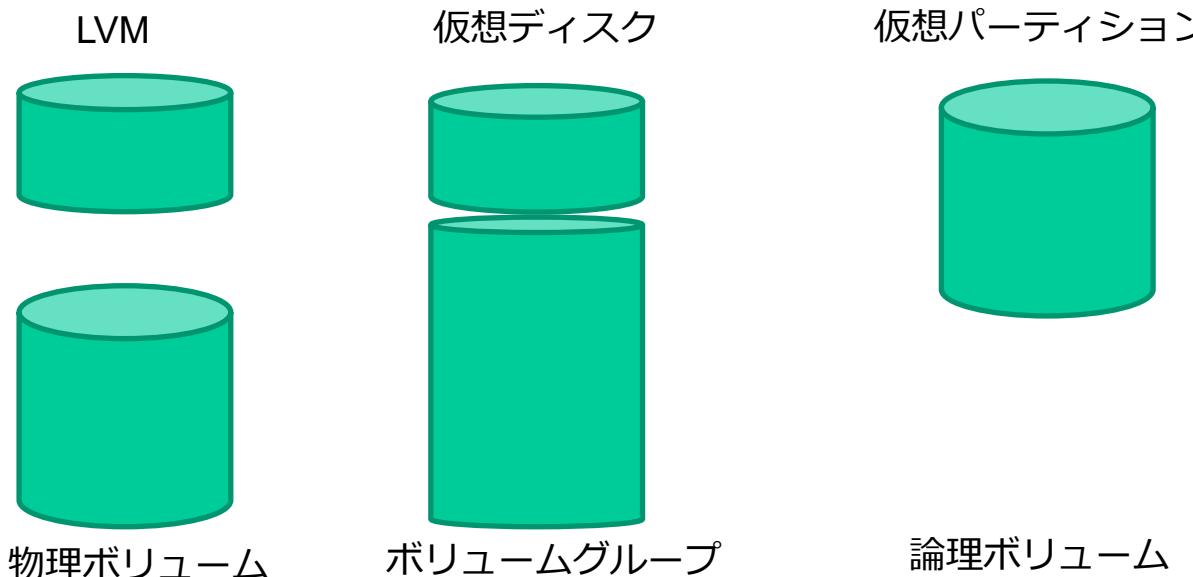


■ Point

- ① RAID
- ② LVM

■ LVM（論理ボリュームマネージャー）はディスクの管理をする機能

1. 1台のHDかパーティションを物理ボリューム（PV:Physical Volume）にする
2. 1つ以上の物理ボリュームからボリュームグループ（VG:Volume Group）を作る
3. ボリュームグループを切り出して論理ボリュームにする



コマンド	説明
<code>parted</code>	LVMパーティションの準備
<code>pvcreate</code>	物理ボリュームの初期化
<code>vgcreate</code>	ボリュームグループの作成
<code>lvcreate</code>	論理ボリュームの作成



■ Point

- ① ネットワーク構成・確認コマンド
- ② ネットワーク関連のファイル

③ ネットワークのトラブルシューティング

■ ネットワーク関連のコマンド

ifconfig (NICの確認や設定)、ip (NIC、ルーティングテーブル、ARPテーブルの管理)

■ ネットワーク関連のファイル

ファイル名	説明
/etc/hostname	ホスト名を記述
/etc/hosts	ホスト名とIPアドレスを記述(名前解決)
/etc/nsswitch.conf	名前解決の順を記述
/etc/resolve.conf	DNSサーバやドメイン名を記述
/etc/sysconfig/network	デフォルトゲートウェイなどを記述
/etc/sysconfig/network-scripts/ (Red Hat系) /etc/network/interfaces (Debian系)	IPアドレスなどを記述



■ Point

- ① ネットワーク構成・確認コマンド
- ② ネットワーク関連のファイル

③ ネットワークのトラブルシューティング

■ ネットワークのトラブルシューティング

コマンド	説明
ping、ping6	疎通確認
traceroute、traceroute6	経路情報の確認
arp	ARPキャッシュの操作
tcpdump	NICの監視
netstat、ss	ソケット情報などの確認
nc	ポートスキャンの実行など



■ Point

- ① ソースからのインストール
- ② バックアップ

■ ソースからインストールする方法

1. ソースプログラムを含むアーカイブを入手して展開する
2. ソースプログラムをコンパイルしてバイナリファイルを作成する
3. バイナリファイルをインストールする

■ ソースからインストールするコマンド

1. 展開 : tar、gunzip、gzip、bunzip2、bzip2
2. ./configure
3. make install



■ Point

- ① ソースからのインストール
- ② バックアップ

■ バックアップで使われるコマンド

コマンド	説明
tar	ファイル、ディレクトリをまとめたり、展開したりする
cpio	ファイルをアーカイブファイルにコピーしたり抽出する
dump、restor	ファイルシステム単位でバックアップできる
rsync	ネットワーク経由で別のホストへバックアップをする



■ Point

- ① DNSサーバの基本的な設定
- ② DNSゾーンの作成と保守

■ DNS (Domain Name Server)の役割

- ・ホスト名からIPアドレスを解決（正引き名前解決）
- ・IP アドレスからホスト名を解決（逆引き名前解決）
- ・サービスの検索

■ DNS以外の名前解決

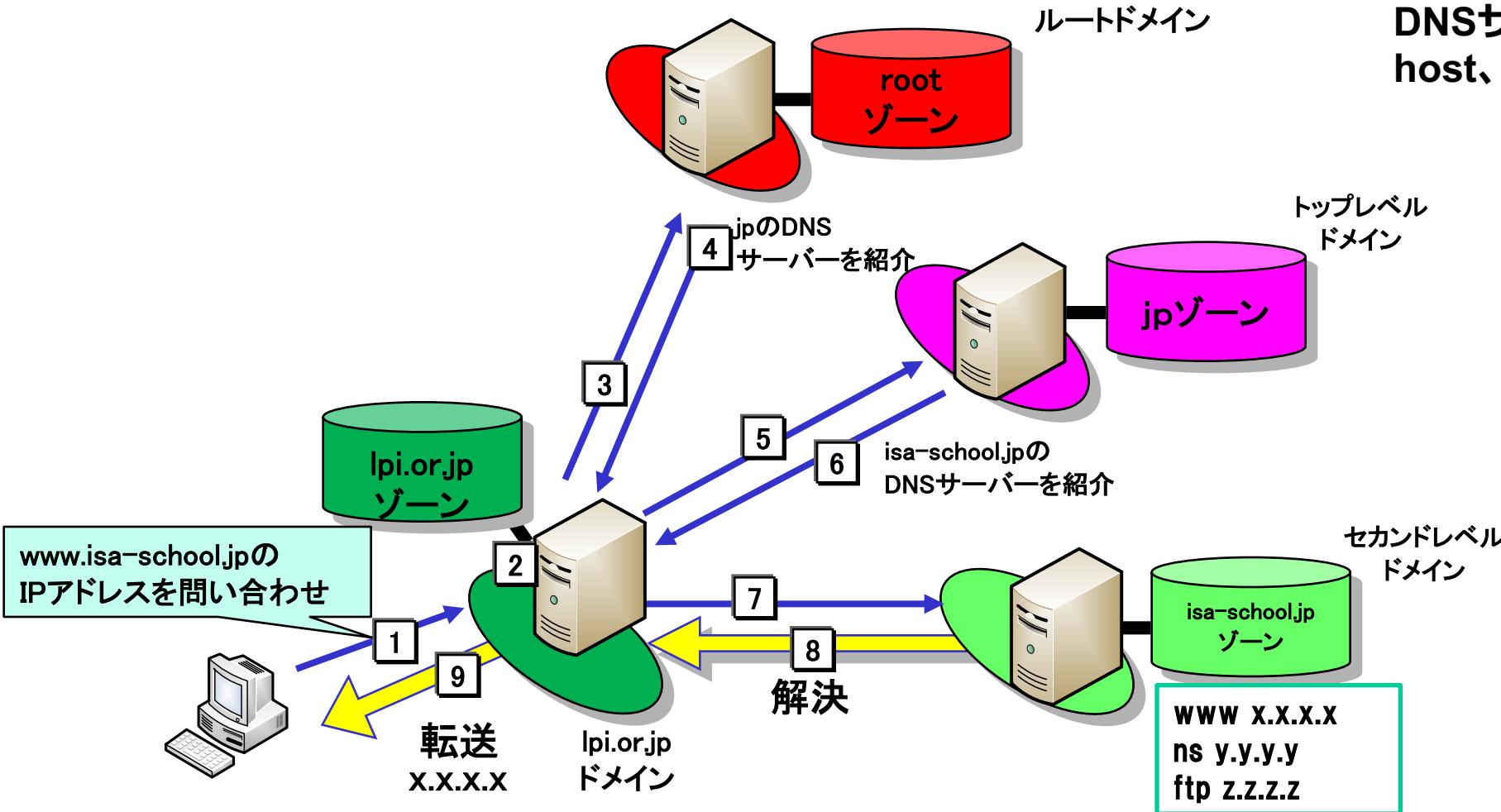
- ・/etc/hostsファイル
- ・DNS以前は/etc/hostsファイルに記載
- ・/etc/hostsファイルはIPアドレス、FQDN、ホスト名の順に記述

/etc/hosts ファイルの例

```
127.0.0.1    localhost.localdomain localhost
::1          localhost.localdomain localhost
192.168.1.100  pc1.test.com      pc1
192.168.1.101  pc2.test.com      pc2
```



■DNSサーバの動作



DNSサーバーの情報は、`nslookup`、`host`、`dig`コマンドで確認できる。



■ Point

- ① DNSサーバの基本的な設定
- ② DNSゾーンの作成と保守

■ DNSサーバに必要な設定ファイル

- /etc/named.conf (BINDのメインの設定ファイル、ゾーンファイルの場所などを指定)
- hintファイル (ルートDNSサーバのIPアドレス一覧が記載されたファイル)
- 正引きゾーンファイル (ホスト名からIPアドレスの一覧の記載されたファイル)
- 逆引きゾーンファイル (IPアドレスからホスト名が記載されたファイル)

■ DNSリソースレコードの種類

種類	説明
SOA	ゾーンに関する設定情報
NS	DNSサーバをFQDNで指定
MX	メールサーバ

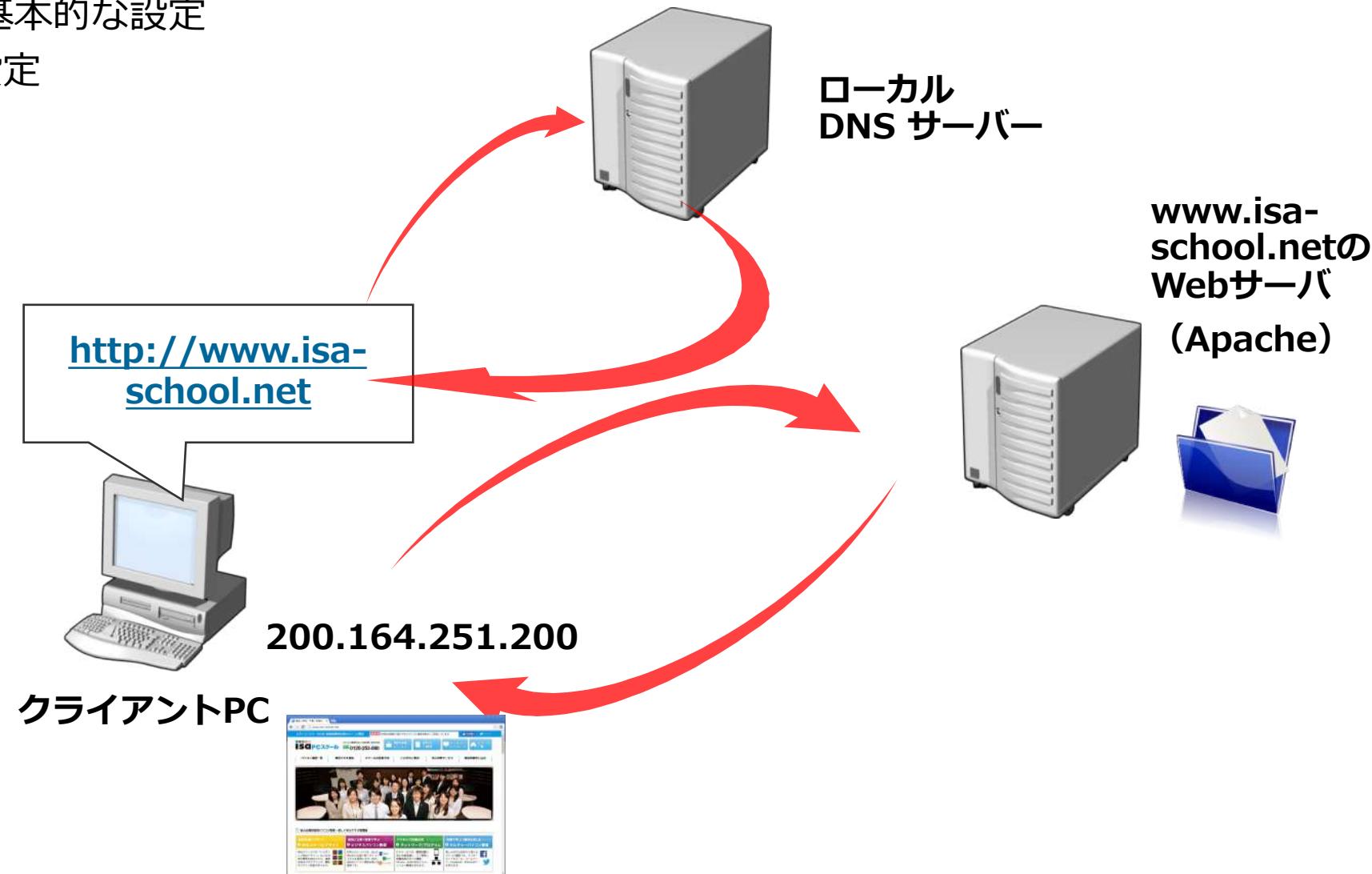
種類	説明
A	正引きホスト名(IPv4)
AAAA	正引きホスト名(IPv6)
CNAME	エイリアス

■ BINDはrndcコマンドで操作できる



Point

- ① Apacheの基本的な設定
- ② HTTPSの設定





■ Point

- ① Apacheの基本的な設定
- ② HTTPSの設定

■ Apache

- ・世界で最も人気のWebサーバソフト
- ・モジュールをロードしたり、アンロードできる

■ Apacheの各種設定ファイル

Red Hat系の例

ファイル	説明
/etc/httpd/conf/httpd.conf	メインの設定ファイル
ssl.conf	SSLの設定

- .htaccessファイルを使うと、httpd.confの設定を上書き可能
- .htpasswdファイルを使うと、BASIC認証、ダイジェスト認証が可能
- バーチャルホストを利用すると、1台のサーバ上で複数のWebサイトをホストできる



■ Point

- ① Apacheの基本的な設定
- ② HTTPSの設定

■ httpd.confファイル

認証のモジュールの例

```
# Example:  
# LoadModule foo_module modules/mod_foo.so  
LoadModule auth_digest_module modules/mod_auth_digest.so  
LoadModule auth_basic_module modules/mod_authn_basic.so
```

■ .htaccessファイル

```
<Directory "/var/www/html/test">  
    AuthType Basic or Digest  
    AuthName "RestrictedArea"  
    AuthUserFile /etc/httpd/.htpasswd  
    Require valid-user  
</Directory>
```



■ Point

- ① Apacheの基本的な設定
- ② HTTPSの設定

■ SSL

SSLは公開鍵・秘密鍵を使ったセキュリティ技術

SSLを使うことでWebサイトとブラウザ間の通信を暗号化できる

■ SSL実装までの流れ

1. 公開鍵と秘密鍵を作成する
2. 公開鍵とCAに送付する
3. CAから証明書が発行される
4. 証明書をWebサーバにインストールする

■ 秘密鍵、CSRの作成コマンド

```
openssl genrsa -des3 -out ./ssl.key/ssl.isa.key 2048 (秘密鍵の作成)
```

```
openssl req -new -key ./ssl.key/ssl.isa.key -out ./ssl.csr/ssl.isa.csr (CSRの生成)
```

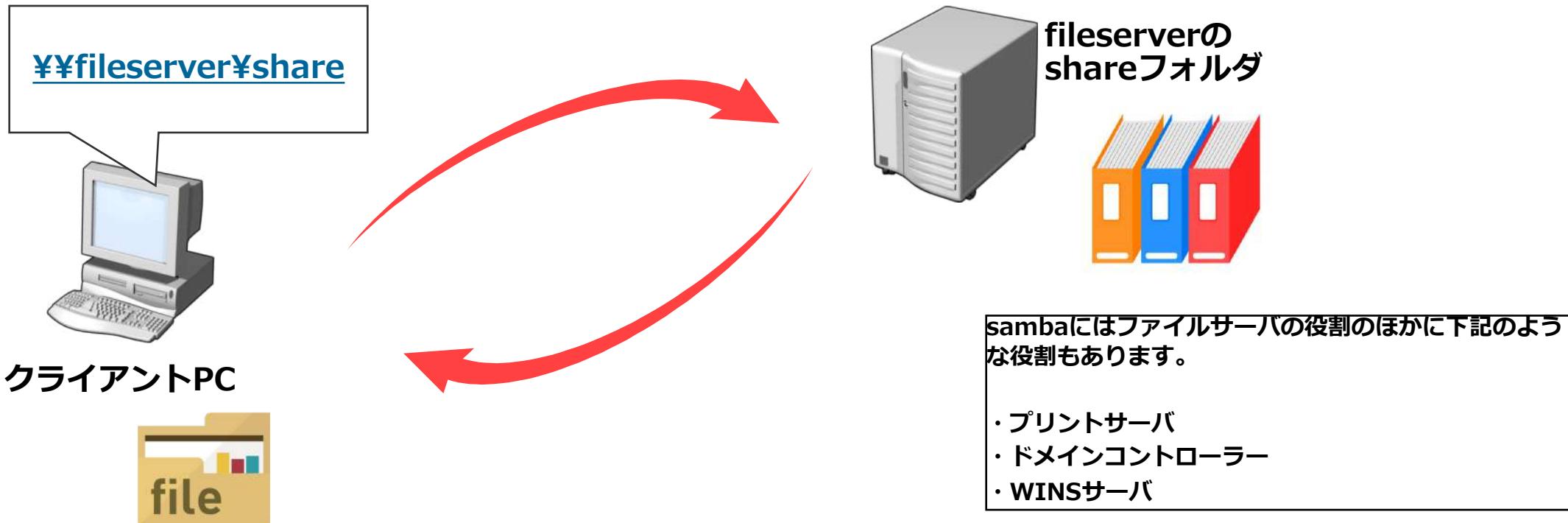


■ Point

- ① Sambaの設定
- ② NFSの設定

■ sambaの役割

Windowsでのファイル、プリンター共有などができるソフトウェア





■ Point

- ① Sambaの設定
- ② NFSの設定

■ smb.conf

/etc/samba/smb.confがsambaのメインの設定ファイル
smb.confは大きく分けると、全体の設定と共有定義に分かれている。
smb.confセクションに分かれている

セクション	説明
global	サーバ全体の設定
homes	接続してきたユーザのホームディレクトリを共有するサービスが自動実行される
printers	プリンター用の[homes]セクション

これ以降は任意の名前でセクションが作れる



■ Point

- ① Sambaの設定
- ② NFSの設定

■ smb.conf

smb.confの個々の設定はパラメータと呼ばれている

パラメーター	セクション	説明
hosts allow	global	アクセスを許可するIPを設定
workgroup	global	ワークグループ名の設定
smb passwd file	global	パスワード認証のファイルを設定
comment	共有	コメント
path	共有	共有フォルダへのパス
read only =Yes No	共有	読み取り専用
writable =Yes No	共有	書き込みの許可
guest ok =Yes No	共有	ゲストアカウントの許可
guest only =Yes No	共有	ゲストアカウントのみ許可

パラメーター	セクション	説明
path	printers	スプールファイルの場所
printable = Yes No	printers	印刷可能かどうかの設定



■ Point

- ① Sambaの設定
- ② NFSの設定

■ NFSとは

NFS (Network File System) とはネットワーク経由でファイルを共有する仕組み

■ NFSの設定

NFSサーバで共有を有効にすることをエクスポートと呼ぶ
対象のディレクトリは/etc/exportsに記述

/etc/exportのオプション	説明
ro	読み取り専用でエクスポートする
rw	読み書き可能な状態でエクスポートする
no_root_squash	rootでのアクセス時にroot権限になる
root_squash	rootでアクセスしても匿名アカウントになる(デフォルト)



■ Point

- ① DHCP
- ② PAM認証

- ③ LDAP

■ DHCPとは

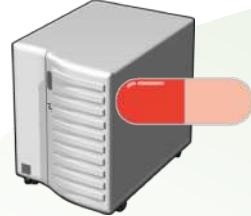
DHCP (Dynamic Host Configuration Protocol) とは、サーバ側で事前に設定しているTCP/IPの情報を自動的にクライアントに割り当てる技術

- IPアドレス
- サブネットマスク
- デフォルトゲートウェイ
- DNSサーバ

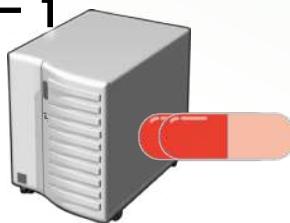


■DHCP (Dynamic Host Configuration Protocol) サーバの動き

DHCP サーバー 2



DHCP サーバー 1



DHCP クライアント

DHCP クライアントは DHCPDISCOVER パケットをブロードキャストする
DHCP サーバは DHCPOFFER パケットをブロードキャストする
DHCP クライアントは DHCPREQUEST パケットをブロードキャストする
DHCP サーバ 1 は DHCPACK パケットをブロードキャストする



■ Point

- ① DHCP
- ② PAM認証
- ③ LDAP

■ DHCPサーバの設定ファイル

DHCPサーバはdhcpd（DHCPデーモン）が利用されている
DHCPの設定ファイルは/etc/dhcpd.confで行う

dhcpd.confのオプション	説明
range	IPアドレスのプール
option domain-name	ドメイン名
option domain-name	DNSサーバ
option routers	デフォルトゲートウェイ
default-lease-time	デフォルトのリース期間(秒)



■ Point

- ① DHCP
- ② PAM認証

- ③ LDAP

■ PAMの仕組み

PAM (Pluggable Authentication Modules) とはLinuxにおいてユーザ認証を一元管理する仕組み

PAMの設定ファイル/etc/pam.dディレクトリに配置される

/etc/pam.dディレクトリにはユーザ認証を行うプログラムごとに設定ファイルがある

PAMの設定ファイルの書式：**モジュールタイプ コントロール モジュールパス 引数**

タイプ	説明
auth	ユーザ認証を行う
account	期限、有効性の確認
password	パスワードの設定と変更
session	ログの記録など

コントロール	説明
requisite	認証に失敗したら認証を拒否
required	認証に失敗しても以後の処理を継続
sufficient	認証に成功したら認証を成功とする
optional	認証の成否に関係なく処理をする
include	指定されたファイルの設定を読み込んで処理



■ Point

- ① DHCP
- ② PAM認証

- ③ LDAP

■ LDAP

LDAP (Lightweight Directory Access Protocol) はディレクトリサービスの提供者と利用者間のプロトコル

LDAPでは、情報をDIT（ディレクトリ情報ツリー）という階層構造で管理する

ディレクトリツリー内のオブジェクトを識別するには、識別名（DN : Distinguished Name）を使う

DNの例 : uid=user1,OU=users,dc=example,dc=com

オブジェクトクラスや属性の定義はスキーマで行う

LinuxでLDAPを使う場合は、OpenLDAPが使われる

■ LDAPクライアントコマンド

コマンド	説明
ldapadd	エントリの追加
ldapdelete	エントリの削除
ldapmodify	エントリの変更
ldapsearch	エントリの検索



Point

- ① 電子メールサーバの構成、管理

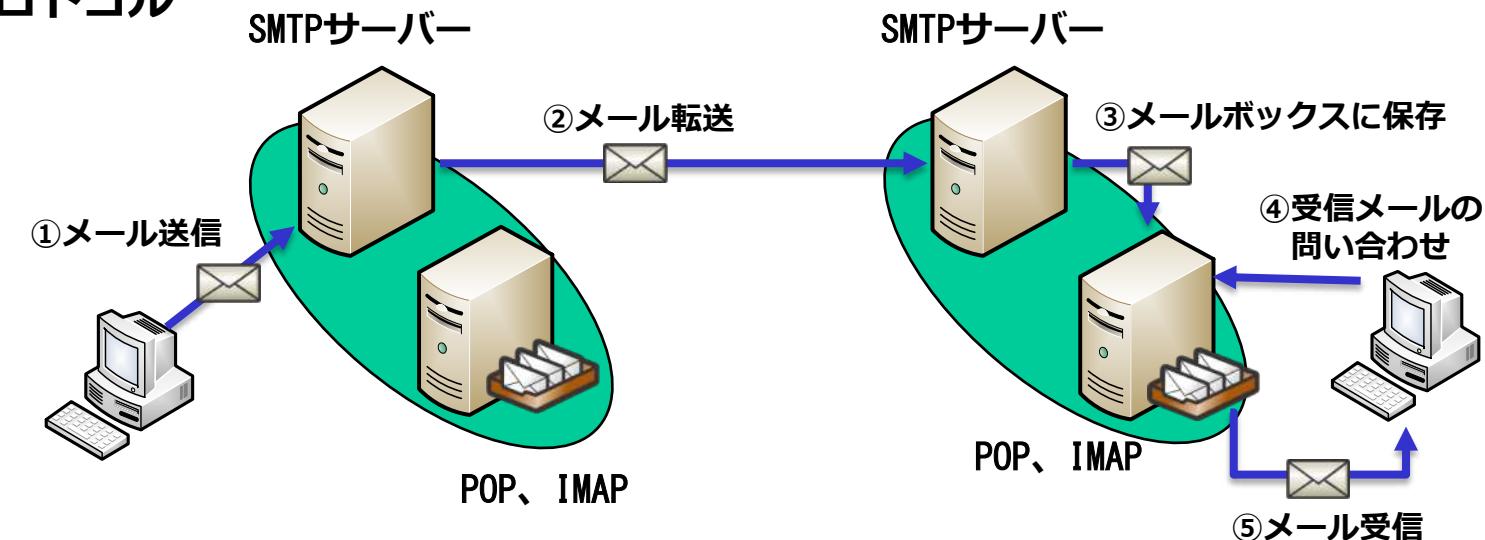
■ メール配送の仕組み

■ SMTP (Simple Mail Transfer Protocol)

- ・電子メールを転送するプロトコル
- ・Postfix、sendmailなど

■ POP (Post Office Protocol)

- ・電子メールを受信するためのプロトコル
- ・POP、IMAPなど





■ Point

- ① 電子メールサーバの構成、管理

■ Postfix

Postfixの設定ファイルは、/etc/postfix/main.cf
postconfコマンドでPostfixの全設定値が表示される

■ メールキューの管理

メールキューのディレクトリ

Postfix : /var/spool/postfix

Sendmail : /var/spool/mqueue

メールキューの表示はmailqコマンドを使う

■ Dovecot

POP3、IMAP4に対応しているMail Delivery Agent

/etc/dovecot/dovecot.confが設定ファイル

doveconfコマンドでDovecotの設定内容をデフォルト値も含めて表示できる



■ Point

① ルータの構成

② SSH

③ セキュリティ業務

■ ルーティング

ルーティングとは異なるネットワークにパケットを送信するときに最適な配達経路を決めること

ルーティングテーブルで管理されている

ルーティングテーブルを表示するにはroute、netstat -rコマンド

■ SSH

SSH (Secure Shell) はリモートホスト間の通信で認証と暗号化を行うことができる。セキュアなtelnet。

OpenSSHが使われている

/etc/ssh/sshd_configで設定ができる

■ ホスト認証、ユーザ認証

ホスト認証はSSHサーバの正当性を認証します

ユーザ認証はユーザの正当性を認証します

■ 鍵の作成

ssh-keygenコマンドで秘密鍵と公開鍵のペアを作成できる



■ Point

① ルータの構成

② SSH

③ セキュリティ業務

■ セキュリティツールで使えるコマンド

nmap、netstat、ss、lsof、fuserなどでポートの状態の確認をする

■ TCP Wrapper

TCP Wrapperは各種サーバプログラムへのアクセス制御を集中管理できる

アクセスを許可するファイル：/etc/hosts.allow

アクセスを拒否するファイル：/etc/hosts.deny

ワイルドカード	説明
ALL	すべてのホスト、サービス
x EXCEPT y	y以外のx
LOCAL	ローカルネットワーク内のホスト