HI CORP.

Linux Professional Institute Japan LPI-JAPAN

LPIC Level2技術解説無料セミナー

～LPIC Level2試験に向けての準備とポイント解説～

2014/07/19

株式会社エイチアイ
末永貴一

自己紹介

株式会社エイチアイ 開発本部 システムデザイン部 部長
- 組込み機器向けソフトウェアの研究開発
  http://www.hicorp.co.jp

Linux関連文章の執筆
- LPIC Level1、Level2認定テキスト
- LPI試験 レベル1標準教科書（オーム社）
- LPI試験 レベル2標準教科書（オーム社）
- LPI-Japan コラム【Linux道場 入門編】
- @IT 「Linuxをいまから学ぶコツ教えます」
- @IT 「Linuxに触れよう」
- 日経Linux「Xと次世代「Wayland」を知る」
  など

本日のアジェンダ

HI CORP.

1. LPIC Level2試験とは
   - 試験概要と特徴
   - 主な試験範囲等
2. 201試験範囲とポイント
   - 各主題の確認とポイント解説
3. 202試験範囲とポイント
   - 各主題の確認とポイント解説

※間に10分間の休憩を挟みます。

Linux Professional Institute

LPIC Level2試験とは…

アドバンストレベルLinux専門家を認定する試験

- Level1 – ファーストレベルLinux専門家
- **Level2 – アドバンストレベルLinux専門家**
- Level3 – 市場価値の高いLinuxプロフェッショナル

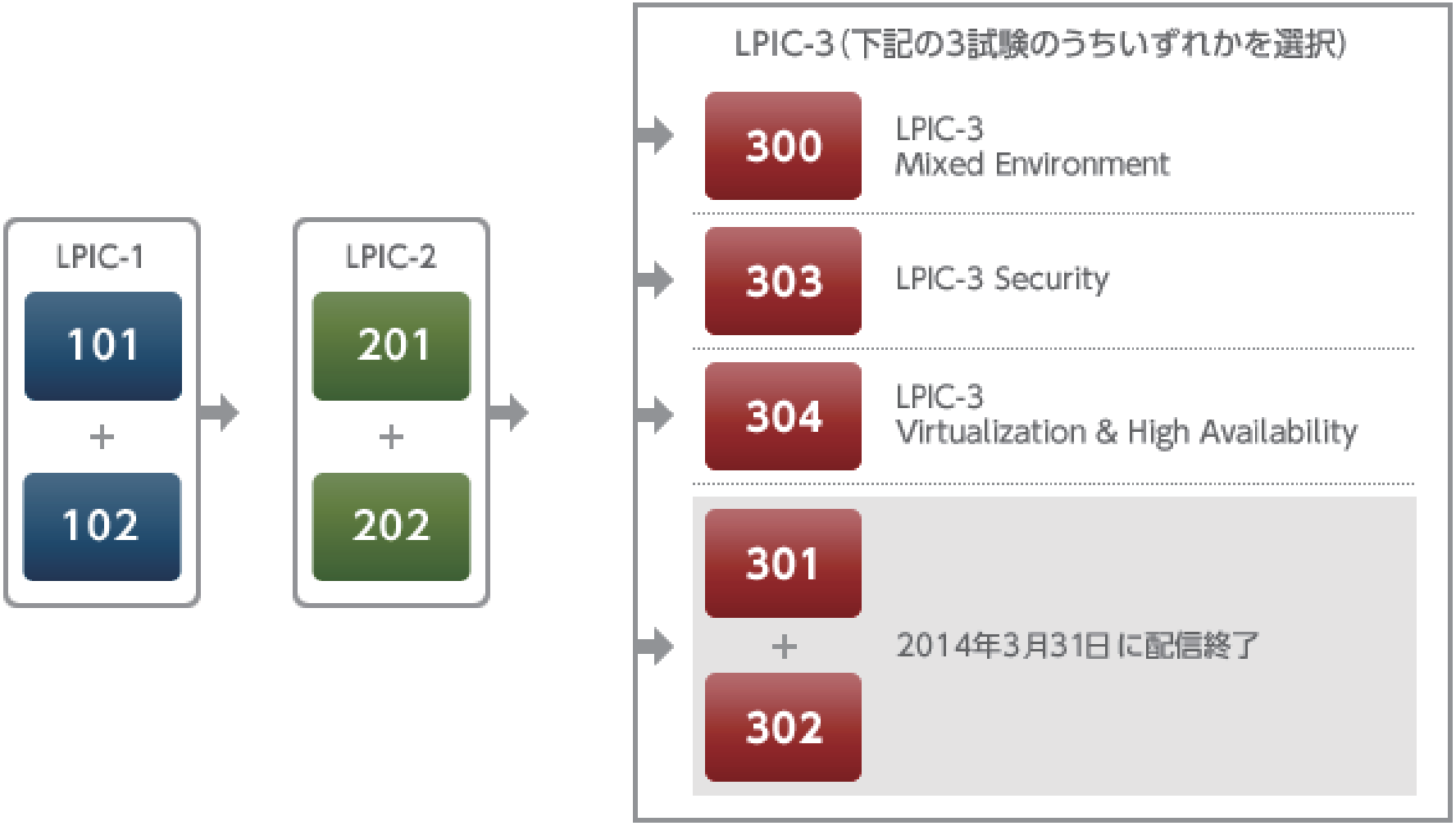
問われる知識

Linuxシステムの企画、導入、維持、トラブルシューティングができる。

カーネルからネットワークに関する事まで、構築・管理・修正ができる。

LPIC Level2試験とは

Level2認定を取得するためには、201試験と202試験両方に合格が条件



LPIC Level2 v4.0の主題目

201試験

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：システム保守

202試験

主題207：ドメインネームサーバ
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：システムセキュリティ

主にシステム管理、サーバ系に関する内容が中心

LPIC Level2がバージョンアップ

- **2014年1月1日よりLPIC2がv3.5 → v4.0に。**

→サーバ環境の変化、サーバの高性能化・大規模化が進み、LPIC-2のレベルのエンジニアに求められる技術力がより高度化したため。

- LPIC2 v4.0のポイント

201試験

サーバのスケーリング、メンテナンス、トラブルシューティング

202試験

主要なネットワークサービス、システムとネットワークセキュリティ

→ 詳細は http://www.lpi.or.jp/ver4/ を確認

LPIC Level2試験の傾向

HI CORP.

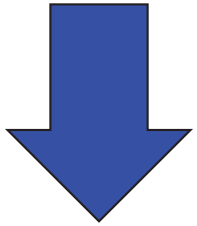
- LPIC1の知識は無論、前提知識となる。
- LPIC2ではシステム管理・運用、ネットワークサーバに関する知識範囲が広く問われる。
- Linux自体に関する知識以外にも、サーバ系の知識（主にプロトコル、サーバアプリケーション）が重要

LPIC1以上に広範囲な知識が必要

Linux Professional Institute

本セミナーの解説趣旨

・LPIC2の主題の概要とポイントを解説
・各主題のポイントをピックアップ



試験範囲を網羅的に確認し、
ポイントの一部を解説する

201試験

主題200 キャパシティプランニング

HI CORP.

含まれる試験範囲

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
200.2 将来のリソース需要を予測する

この主題のポイント

ハードウェアリソース、ネットワーク帯域幅の使用率を測定する知識。
問題を発見し、その問題解決ができる知識が必要なとなる。

top,vmstat等のコマンドを使用してシス無リソースの状況を把握し、
計測した情報から需要の分析ができること。

ピックアップ解説

・**vmstatでメモリ使用状況の確認**
$ vmstat [表示間隔（秒）] [表示回数]

・実行例

```
# vmstat 2 7
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   8576 222080 132344 535036    0    0     2    17    0     0   1   0  99   0   0
 0  0   8576 221840 132348 535032    0    0     0   272 1039   131   0   0  93   7   0
 0  0   8576 221716 132348 535032    0    0     0     0 1044    90   1   2  97   0   0
 0  0   8576 221896 132348 535036    0    0     0     0 1035    54   0   0 100   0   0
 0  0   8576 221896 132348 535036    0    0     0     0 1003    20   0   0 100   0   0
 0  0   8576 221896 132348 535036    0    0     0     0 1021    38   0   0 100   0   0
 0  0   8576 221896 132348 535036    0    0     0    80 1007    28   0   0 100   0   0
```

このような情報から現状を把握し、需要予測を行うことが基本となる。
予測に関しては一定の計測データ量が必要となり、ある程度計測に時間を要する場合も。

Procs
- r: ランタイム待ちのプロセス数
- b: 割り込み不可能なスリープ状態にあるプロセス数

Memory
- swpd: 仮想メモリの量。
- free: 空きメモリの量。
- buff: バッファに用いられているメモリの量。
- cache: キャッシュに用いられているメモリの量。
- inact: アクティブでないメモリの量 (-a オプション)。
- active: アクティブなメモリの量 (-a オプション)。

Swap
- si: ディスクからスワップインされているメモリの量 (/s)。
- so: ディスクにスワップしているメモリの量 (/s)。

IO
- bi: ブロックデバイスから受け取ったブロック (blocks/s)。
- bo: ブロックデバイスに送られたブロック (blocks/s)。

System
- in: 一秒あたりの割り込み回数。クロック割り込みも含む。
- cs: 一秒あたりのコンテキストスイッチの回数。

CPU

これらは CPU の総時間に対するパーセンテージである。
- us: カーネルコード以外の実行に使用した時間 (ユーザー時間、nice 時間を含む)。
- sy: カーネルコードの実行に使用した時間 (システム時間)。
- id: アイドル時間。Linux 2.5.41 以前では、IO 待ち時間を含んでいる。
- wa: IO 待ち時間。Linux 2.5.41 以前では、0 と表示される。
- st: 仮想マシンから盗まれた時間。Linux 2.6.11より前では未知。

主題201 Linuxカーネル

HI CORP.

含まれる試験範囲

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 カーネル実行時における管理とトラブルシューティング

この主題のポイント

Linuxカーネルの再構築やカーネルモジュール構築についての知識全般。makeやpatch等の知識やモジュール操作系コマンドが中心で、カーネル2.4系、2.6系の知識が必要となる。

また/procやsysctlを利用したパラメータ設定の知識も含まれ、パラメータの参照、設定も知っておく必要がある。

ピックアップ解説

・**カーネルバージョンの表記の変化**
旧：メジャーバージョン以降の数値の偶数奇数で安定版か開発版かを判断。
ex. 2.6.1（安定版）、2.5.1（開発版）
新：偶数奇数で開発・安定の区別はなくなり、rcN,gitNという表記になる。
ex. 3.2.1（安定版）、3.2-rc1、3.2-git1（開発版）

・**カーネルモジュールの操作**
modutiles系のmodprobeはオプションによる挙動が異なる
-a ：全てのモジュールをロードする
-l ：ロード可能なモジュールファイルの一覧表示
-c ：モジュールの構成表示
-r ：モジュールの削除
-t ：指定したディレクトリ内のモジュールを複数ロード

含まれる試験範囲

202.1 SysV-initシステムの起動をカスタマイズする
202.2 システムのリカバリ
202.3 その他のブートローダ

この主題のポイント

Linuxの起動シーケンス、initプロセスの仕組み等に関する知識。ランレベルや各種ブートローダの知識や操作なども含まれる。起動に関するトラブルシューティングの知識も必要。

特にinit関連ではinitパラメータやinittabファイルの知識が重要になる。

ピックアップ解説

・**ランレベル**
ランレベルの定義が複数ある場合があり、注意が必要。

ランレベル	動作内容
ランレベル0	システムの停止
ランレベル1、s、S	シングルユーザモード
ランレベル2	NFSファイル共有のないマルチユーザモード Debian：完全マルチユーザモード（GUIベース）
ランレベル3	完全マルチユーザモード（テキストベース）
ランレベル4	通常、未使用 Debian：完全マルチユーザモード（GUIベース）
ランレベル5	完全マルチユーザモード（GUIベース）
ランレベル6	システムの再起動

・**inittabファイル**

id:runlevel:action:process

id（識別子）、runlevel（ランレベル）、action（動作定義）、process（実行コマンド）

action	動作
boot	runlevelを無視して、全てのrunlevelでシステムブート中に実行する
bootwait	bootと同様だが、initはprocessフィールドの処理が終了するまで次の処理を開始しない
sysinit	boot、bootwaitと同様だが、boot、bootwaitより先に実行する
initdefault	デフォルトのランレベルの設定
wait	指定されたrunレベルになると一度だけ実行され、initはprocessフィールドの処理が終了するまで次の処理を開始しない
respawn	processフィールドの処理が終了したら再起動する
powerfail	UPSなどのバッテリ容量が少なくなったことを検出した場合、processフィールドの処理を実行する
powerokwait	powerfailと同様だが、initはこの行のprocessフィールドの処理が終了するまで次の処理を開始しない
ctrlaltdel	Ctrl-Alt-Deleteの同時押しを定義

主題203 ファイルシステムとデバイス

HI CORP.

含まれる試験範囲

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

この主題のポイント

Linuxのファイルシステムの基本的な知識を含むファイルシステムを利用するための設定の知識が問われる。マウント等の共通知識からext2,3,4等の各種ファイルシステムフォーマットの構築、保守等の操作系の知識も含まれる。またautomountの動作や設定についての知識も若干含まれる。

ピックアップ解説

・mountコマンドの-oフラグ以降のオプション

オプション名	機能
atime	アクセス毎にi-nodeのアクセス時間を更新する
auto	-aが指定されたときにマウントされる
noatime	ファイルシステムのi-nodeのアクセス時間を更新しない。 ディスクアクセスの高速化につながる
noauto	-aが指定されたときにマウントしない
nosuid	SUID,SGIDを無効にする
nouser	一般ユーザのマウントを禁止する
remount	すでにマウントされているファイルシステムを再マウント
ro	ファイルシステムをRead Onlyでマウントする
rw	ファイルシステムをWrite Readでマウントする
defaults	rw,suid,dev,exec,auto,nouser,asyncの同時指定

fstabのオプションとしても利用される

主題204 高度なストレージ管理

HI CORP.

含まれる試験範囲

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

この主題のポイント

RAID、HDDの設定、LVMをテーマにLinux上でファイルシステムをより使いこなすための知識が中心となる。

RAID、LVMは基本的な概要レベルの知識が前提となるため、それぞれの用語は前提の上で操作の知識等が問われる。

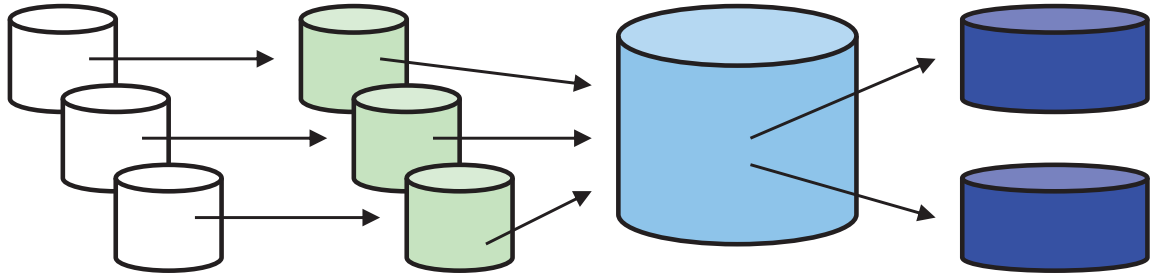
ピックアップ解説

- **各RAID Levelの機能**

  RAID-0：ストライピング。読み書きの高速化
  RAID-1：ミラーリング。書込みの二重化
  RAID-5：パリティ分散記録付ストライピング。専用パリティドライブを持たないため、信頼性とパフォーマンス向上が図れる。

- **LVMの構成要素**

  PV(Physical Volume)：LVM用に構成された、物理的なボリューム
  VG(Volume Group)　：1つ以上のPVを束ねて構成される、論理的なボリューム
  LV(Logical Volume)　：VGから実際に利用する領域を切り出した論理的ボリューム



fdiskからLVM用のパーティションを作成　PVの作成　PVを束ねてVGの作成　VGからLVを切り出す

含まれる試験範囲

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
205.3 ネットワークの問題を解決する

この主題のポイント

主にクライアント、サーバを問わないシステムローカルのネットワークに関する知識が中心となる。このため設定、トラブルシュートに関する知識もシステムローカルに関する知識となる。ディストリビューション非依存性が考えられているため、コマンドベースの設定や確認が重要になる。

またネットワーク設定にディストリビューション（Redhat系、Debian系）の知識も含んでいる。

ピックアップ解説

- **ネットワーク設定の基本コマンド**
  ifconfig、route、ping、arp、netstat等の基本的なネットワーク系のコマンドを把握しておく必要がある。

  例えば・・・
  # ifconfig *NIC名* *IPアドレス* パラメータ
  # iwconfig *NIC名* essid *ESS-ID*
  # route add –net *IPアドレス* gw *GWアドレス* netmask マスク *NIC名*

- **ディストリビューション依存のネットワーク設定ファイル**
  Redhat系：/etc/sysconfig/*
  Debian系：/etc/network/*

  /etc直下のファイル群は共通項

含まれる試験範囲

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
206.3 システム関連の問題をユーザに通知する

この主題のポイント

保守の中でもアプリケーションをソースからインストールする知識と
基本的なバックアップ方法に関する知識が中心となる。
インストールはmakeの基本的な操作が問われる。バックアップについては
ddやrsync等での単純なバックアップ作業が中心。

また/etc/issueなどを使って保守に関する情報をユーザに対して通知する
方法も含まれる。

ピックアップ解説

・**バックアップ**

LPIC2中で前提とされる基本用語

バックアップ形態	意 味
完全バックアップ	システム上の全てのデータを保存する
差分バックアップ	最新の完全バックアップ以後に変更、作成されたファイルだけを保存する
増分バックアップ	最新の増分バックアップを含むバックアップ以後に作成されたファイルだけを保存する

Amanda、Bacula、BackupPC等のバックアップ専用ソフトウェアのWebは簡単でいいので、チェック。

202試験

主題207 ドメインネームサーバ

HI CORP.

含まれる試験範囲

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

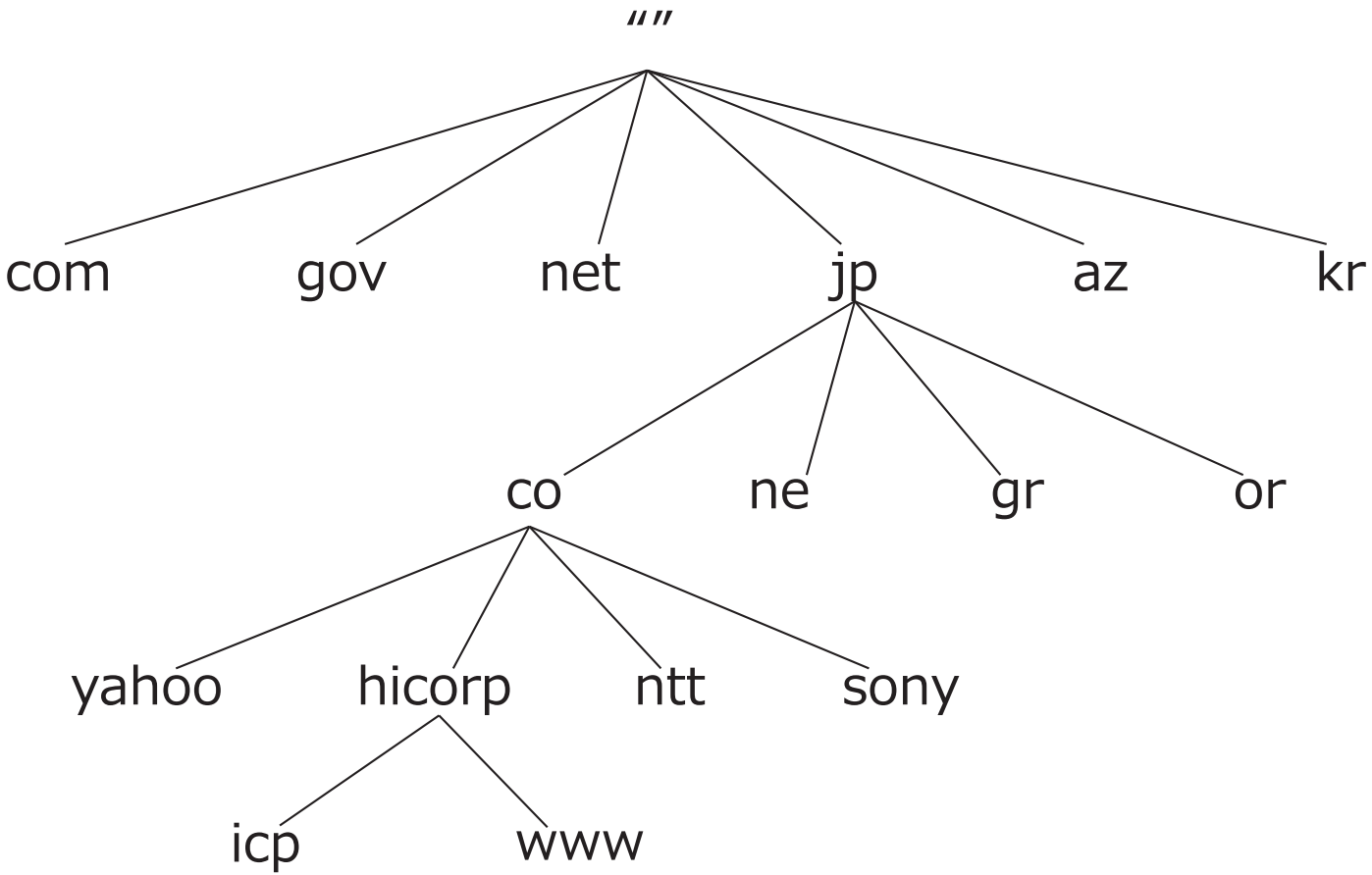
この主題のポイント

DNSサーバの構築、設定の知識が中心となる。DNSサーバアプリケーションはBIND（主にBIND 9系）を対象としている。キャッシュサーバの設定からゾーンファイルの記述、問い合わせ等の知識が問われる。

またDNSSECやchroot jail環境でのDNSサーバセキュリティについても含まれる。

ピックアップ解説

・DNSはinternet上で名前解決を行うための分散型DB



・DNS関連の設定ファイル群

ローカル名前解決	
/etc/resolv.conf	クライアントの問い合わせ先設定
BNID設定ファイル	
/etc/named.conf	BINDの設定ファイル
BIND dbファイル（named.conf中に記載）	
/var/named/named.ca	ルートネームサーバアドレス
/var/named/named.local	localhostの正引きファイル
/var/named/named.local.rev	localhostの逆引きファイル
/var/named/named.hosts	ゾーンホストの正引きファイル
/var/named/named.hosts.rev	ゾーンホストの逆引きファイル

dbファイルについては基本的にファイル名は任意

※ 上記dbファイル名は例としての名前

・正引きファイルの例

```
@           IN      SOA     ns.lpic.or.jp.      root.lpic.or.jp. (
                            2010103001          ; serial
                            3600                ; refresh(1H)
                            900                 ; retry(15M)
                            604800              ; expire(1W)
                            86400               ; negative TTL(24H)
                            )
                    IN      NS      ns.lpic.or.jp.
ns                  IN      A       192.168.0.1
lpic.or.jp.         IN      MX 10   ns.lpic.or.jp.
www                 IN      CNAME   ns
```

SOA：定義するドメインに関する情報
NS　：そのドメインのネームサーバの指定
A　　：ホストのIPアドレスの指定
PTR　：IPアドレスに対するホスト名
CNAME：ホスト名のエイリアス（別名）
MX *priority*：メールサーバの指定

含まれる試験範囲

208.1 Apacheの基本的な設定
208.2 HTTPS向けのApacheの設定
208.3 キャッシュプロキシとしてのsquidの実装
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

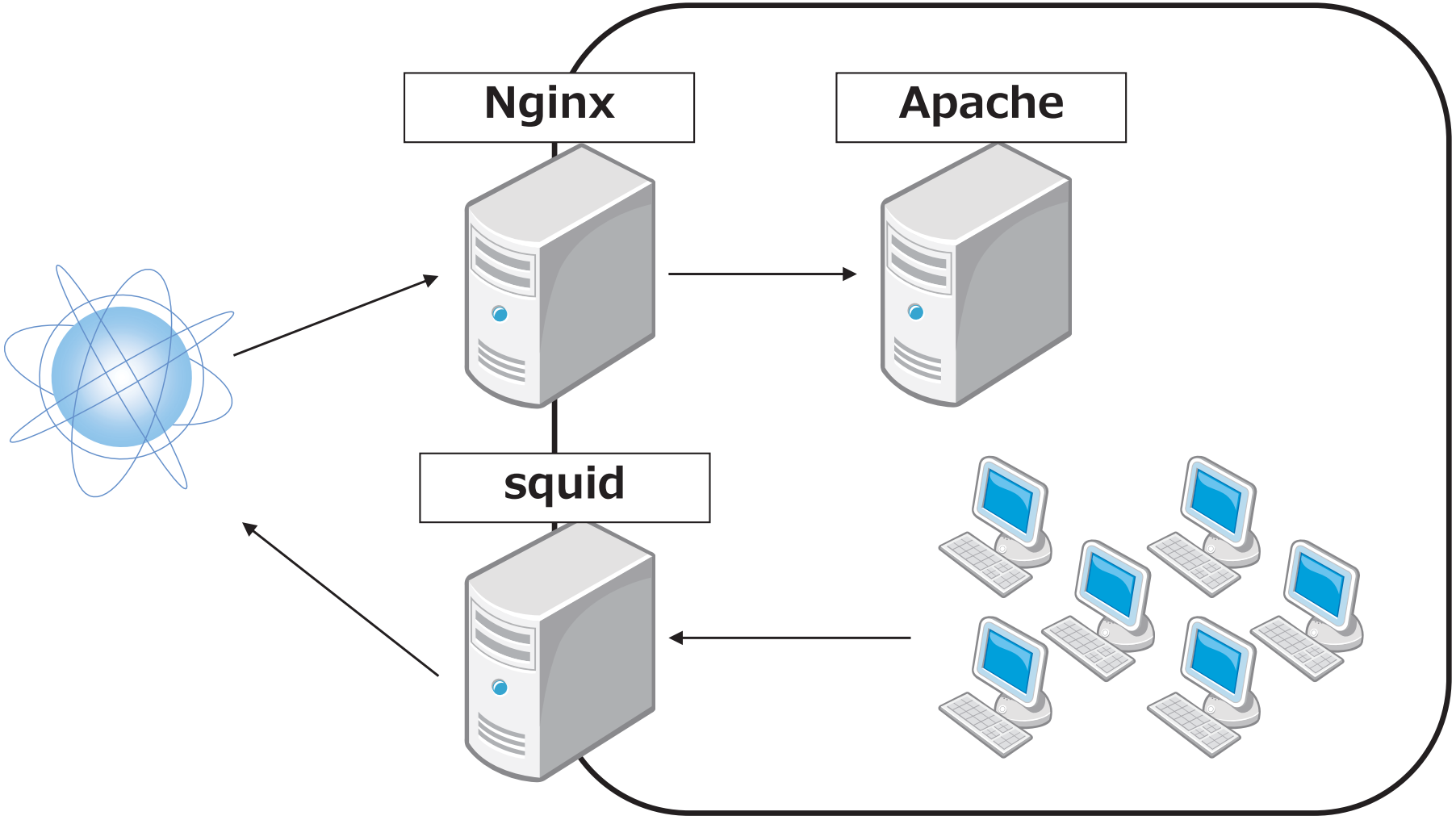
この主題のポイント

Webサーバの構築、設定の知識が中心となる。Webサーバアプリケーションはapache（主にApache 2系）を対象としている。スクリプト言語、クライアント認証（BASIC認証、ダイジェスト認証）、仮想ホスト、SSL設定等のhttpd.confの知識が必要。

プロキシサーバについては基本的なsquidの設定知識が必要。
ただしsquid.confのアクセスリストが理解できればよい。
リバースプロキシについてはnginx（エンジンエックス）の設定が対象。

ピックアップ解説

・主題208の全体像



ピックアップ解説

- **httpd.confの構造**
  httpd.confは大きく3つセクションに区分けされる
  - Global Environment：Apacheの動作環境の設定を行うセクション
  - ‘Main’ server configuration：Apacheの動作を設定するセクション
  - Virtual Hosts：1つのマシンで1つ以上のサーバを構築

- **設定の基本フォーマット**
  ディレクティブ　パラメータ

  <ディレクティブ>
  　ディレクティブ　パラメータ
  　ディレクティブ　パラメータ
  </ディレクティブ>

  代表的なディレクティブ
  ServerRoot：Apacheの配置ディレクトリPortApacheの動作ポート
  DocumentRoot：ドキュメント配置するルートディレクトリ
  DirectoryIndex：URLディレクトリパスでデフォルト表示されるファイル
  AccessFileName：アクセスコントロールファイル指定

- **認証設定（BASIC認証、Digest認証）**
  .htaccess等の設定ファイルに記述

```
AuthType Basic（or AuthType Digest）
AuthUserFile /etc/httpd/.htpasswd
AuthName “User Check”
<Limit GET>
        require valid-user
</Limit>
```

  パスワード生成のコマンドでIDと認証パスワードを設定する。
  BASIC認証の場合はhtpasswdコマンド、Digest認証はhtdigestコマンド

- **基本的なリソースの使用制限**
  MaxClients：リクエストを処理するために生成される子プロセスの最大数を設定
  MaxSpareServers：空きプロセスの最大数
  MinSpareServers ：空きプロセスの最小数

含まれる試験範囲

209.1 Sambaサーバの設定
209.2 NFSサーバの設定

この主題のポイント

Samba、NFSを利用したファイルサーバに関する構築、設定が中心となる。
両システム共にLinuxクライアントからの利用も知識範囲に含まれる。
その他、SambaではWindowsネットワークを想定したワークグループの設定やNFSではprotmapperやアクセスTCPwrapperでの制御が含まれる。

仕組みや設定ファイル、コマンド利用の知識が幅広く求められる。

ピックアップ解説

・smb.confの構造
- [global]セクションと[共有]セクションからなる。
- パラメータ = 設定

workgroup	Sambaサーバが所属するワークグループの指定
os level	ブラウザ選定に利用される優先度
domain master	ドメイン・マスタ・ブラウザの設定

設定はtestparamコマンドで文法チェックを行う

・sambaクライアント
- smbcliant　：コマンドベースのクライアント
- mount –t cifs：sambaファイルシステムをマウント可能

※smbfsはサポートされなくなったため、mountではcifsを利用する。

・NFSサーバの設定
/etc/exportsで共有設定
[共有したいディレクトリ] [公開する相手]([オプション]) ...
ex. /mnt/cdrom 192.168.0.0/255.255.255.0(ro)

ro	読み込みのみ許可
rw	読み込み、書き込みともに許可
root_squash	クライアントのroot権限を無効化する(デフォルト)
no_root_squash	クライアントのroot権限を無効化しない
all_squash	クライアントのユーザ権限を無効化する
noaccess	一切のアクセスを許可しない

・NFSクライアント
mount –t nfs *NFS*サーバアドレス:公開ディレクトリ マウントポイント

showmount、nfsstat等の確認コマンドも

含まれる試験範囲

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
210.4 OpenLDAPサーバーの設定

この主題のポイント

LAN内のネットワーククライアントの管理に関して、DHCPによるアドレス管理、PAMによる認証管理、LDAPによるユーザ管理が知識の中心となる。
DHCPに関しては具体的な設定、保守まで含まれれる。
LDAPに関してはクライアントとしての利用とOpenLDAPを使った基本的なサーバ設定が知識として必要。
PAM認証はシステムローカルでの設定が問われる。

ピックアップ解説

・LDAPの仕組み

ディレクトリサービスとは、分散したネットワーク上の各種リソース（ユーザ、サーバ、アプリケーション、プリンタなど）を論理的な名前で管理しやすく系統立ててエンドユーザや管理者に提供する、情報データベースシステム。

→ LDAPはディレクトリサービスのプロトコル。

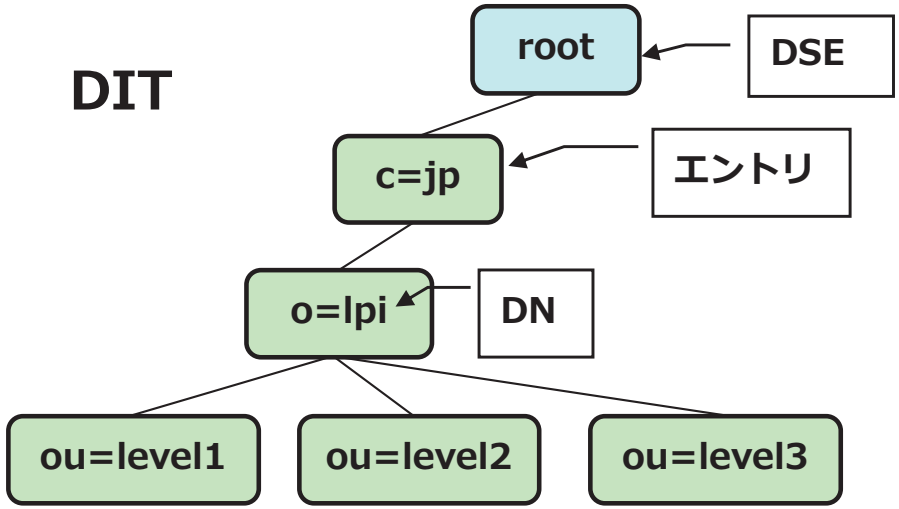
・LDAPの用語

エントリ：データオブジェクト

DIT(Directory Information Tree)：エントリを階層管理するための管理構造

DSE(Directory Service Entry)：ルートのエントリ

DN(Distinguished Name)：エントリの識別子

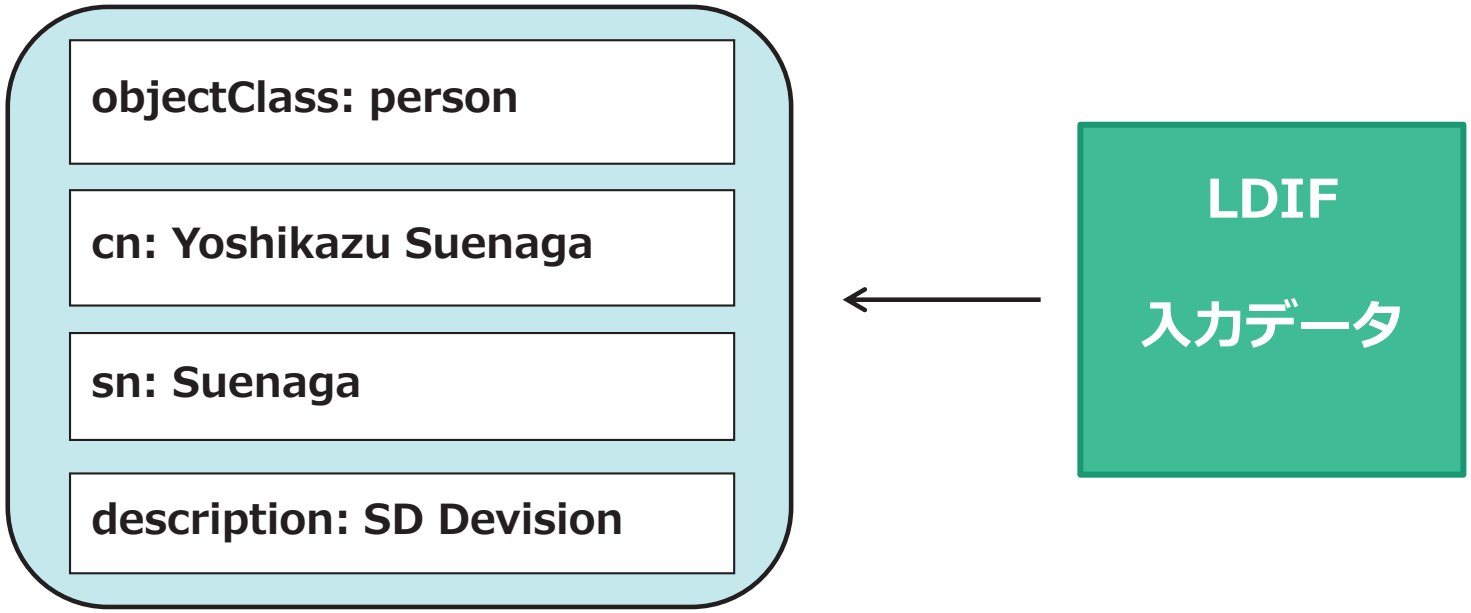


ピックアップ解説

・**LDAPの用語**

オブジェクトクラス：格納データの型
スキーマ：オブジェクトクラスの定義
LDIF(LDAP Data Interchange Format)：LDAPに入力するデータのフォーマット

エントリの中身



・**PAM認証**

設定ファイルは/etc/pam.d以下

・ファイルの基本フォーマット

<type> <control> <module-path> <module-arguments>

ポイント

type：**auth**、**account**、**session**

control：**requisite**、**required**、**sufficient**

auth ：認証

account：期限や有効性の確認

password：パスワード変更など

session：ログイン、ログアウト時の挙動

requisite：認証などに失敗したら以降の処理を行わずに失敗。

required：認証などに失敗しても、以降の処理を続行。

sufficient：認証などに成功したら、以降の処理を行わず成功と判断。

optional：成否に関係なく処理を行う

例えば・・・

```
auth sufficient pam_unix.so          ※1
auth required pam_deny.so            ※2
account required pam_unix.so         ※3
session required pam_unix.so         ※4
```

※1：pam_unixはパスワードによるユーザ認証。成功すればsufficientで以降のチェックを行わずにauthが成功。
※2：pam_deny は無条件に失敗を返す。※1で失敗ならauth は必ず失敗 。
※3：パスワードの有効期限などを確認。required なので成功しないと、accountは失敗。
※4：セッション内（ログイン、ログアウト）でログ管理開始。

type、controlのそれぞれの意味と組合せを理解する。各項目の意味が理解できていれば、基本はOK。

現在のPAM認証設定はさらに項目が増えているが、上記オプションといくつかのmoduleを抑えていれば試験範囲としてはクリア。

含まれる試験範囲

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

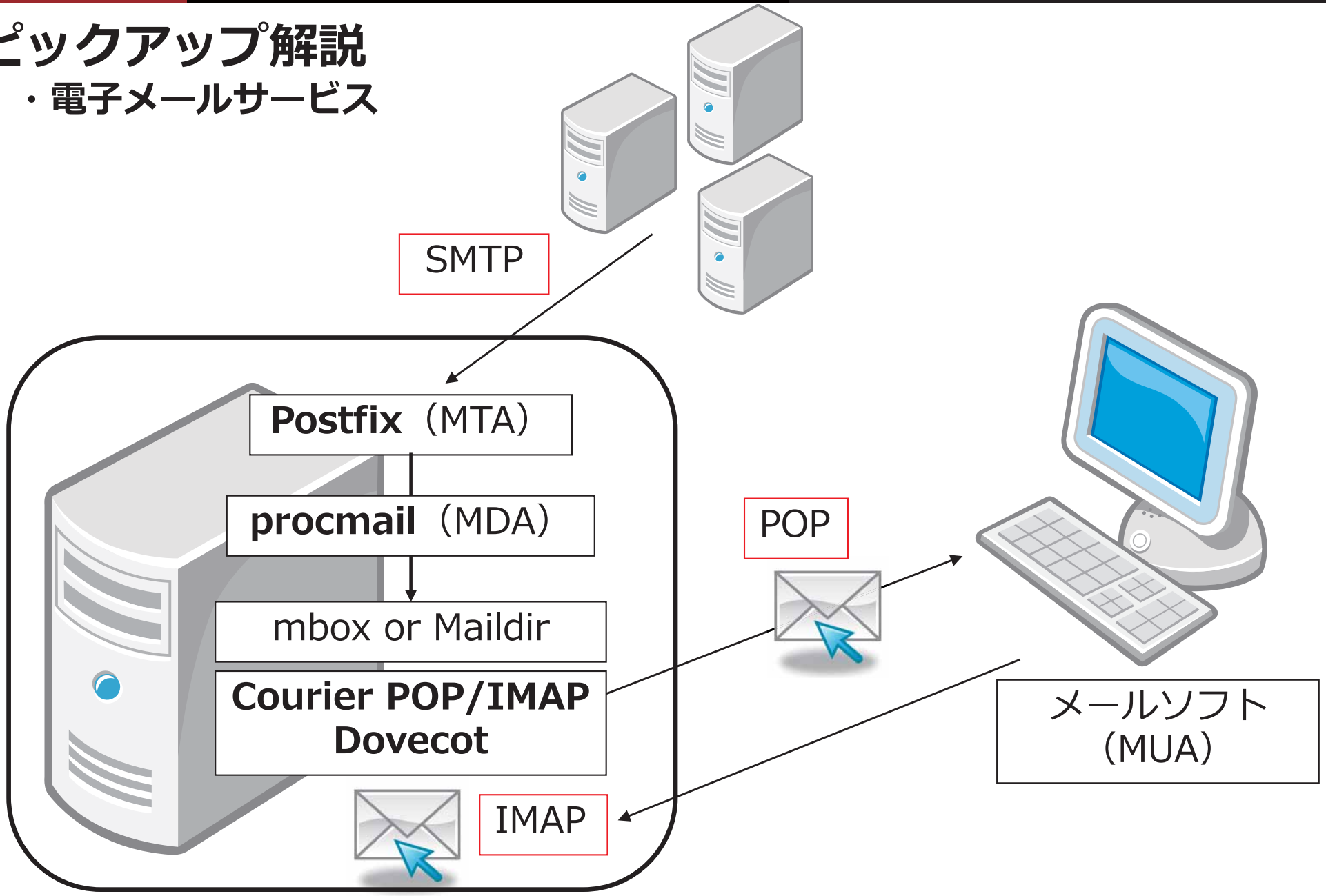
この主題のポイント

電子メールサービス全般に関する知識が求められる。SMTPの知識を前提にMTAはPostfixやsendmail、MDAはprocmailの知識が求められる。
サーバ設定ではPostfixが中心となるが、alias、mailコマンド等のsendmailで利用していた知識も含まれ、これはPostfixのsendmail互換機能によってカバーされている。

またメールクライアント側の知識も含まれ、POP3に加えてIMAP4も知識範囲となっている。サーバソフトウェアはCourierIMAP/POP、Dovecotが（IMAP/POPサーバ）対象。

ピックアップ解説

・電子メールサービス



- **Postfixの設定**
  main.cfが主な設定ファイルとなる。特別な転送設定等を行う場合には
  master.cfを変更することになるが、基本的には変更しなくて問題ない。

  - main.cfの文法
    「パラメータ = 値」で各設定を行う。

```
myhostname = my.lpic.jp
mydomain = lpic.jp
myorigin = $mydomain
mynetwork = 192.168.1.0/24, 127.0.0.0/8
home_mailbox = Maildir/
```

    postconfコマンドで設定内容を確認する。
    # postconf –n（デフォルト値から変更のあったものを抽出）

  - sendmail由来の転送設定
    /etc/aliases、.forward等も利用可能

- **procmailの設定**
  .procmailrcに記述。レシピは「:0」から始まるり、次の「:0」またはEOFまでが1つのレシピとみなされる。

```
:0 [フラグ][:lockfile_name]
* 条件文
アクション
```

レシピ構成要素	役割
フラグ	procmailへのメッセージの渡し方（省略可）
ロックファイル	メール処理中のロックファイル（省略可）
条件文	*で始まり、対象とするメールの条件を正規表現で記述
アクション	条件を満たした場合に実行される内容

lpic@hicorp.co.jp宛のメールを$MAIL/lpicに配信

```
:0
^From:.*lpic@hicorp¥.co¥.jp
$MAIL/lpic/.
```

主題212 システムのセキュリティ

HI CORP.

含まれる試験範囲

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 セキュリティ業務
212.5 OpenVPN

この主題のポイント

主にネットワークアクセスのセキュリティに関しての知識が中心となる。
中心となるテーマはiptables、FTPサーバ（vsftpd、Pure-FTPd等）の
Anonymous設定、OpenSSH、OpenVPN。

テーマとしての範囲は広いが、ポイントはルーター設定とSSH。
その他の項目については概要的な知識が多い。

ピックアップ解説

- **ルーターの設定（iptables）**

パケットフィルタに関してはiptablesコマンドを利用する。
テーブル、チェイン、ターゲット、オプションの各項目と組合せを
理解し、どのような結果になるかを考える。

ex. 送信元アドレスが192.168.1.0/24のパケットをDROPするルールを
　　filterテーブルのINPUTチェインに追加

```
# iptables -t filter -A INPUT -s 192.168.1.0/24 -j DROP
```

ex. 外部からのSSH接続のみ許可する

```
# iptables –P INPUT DROP（すべて拒否）
# iptables –A INPUT –p tcp –syn –destination-port 22 –j ACCEPT
```

ex. SYN floodアタック対策

```
# iptables –A INPUT –p tcp –syn –j DROP
```

ピックアップ解説

・**SSH**
クライアント利用では公開鍵認証、トンネリングがポイント。
サーバ設定ではPermitRootLogin、PasswordAuthentication、
PubKeyAuthentication等の設定がポイントになる。

・公開鍵認証の設定（sshd_config）

```
PermitRootLogin no          （rootログインの拒否）
RSAAuthentication yes       （公開鍵認証）
PasswordAuthentication no   （パスワード認証のOFF）
```

・公開鍵の作成
ssh-keygen –t 暗号タイプ

公開鍵をもつユーザのみがログイン可能

勉強方法のTips

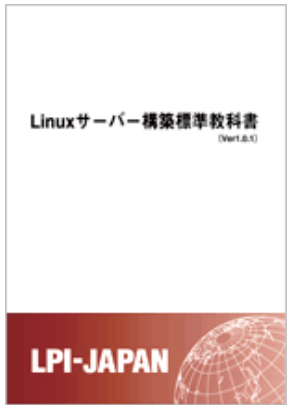
- 試験範囲をよく確認する
  知識範囲、キーワード、重要度をチェック
  重要度の高いテーマは掘り下げられる傾向がある

- 問題集は有効活用する
  問題数が多いテーマは出題傾向が高い
  解説をキーに各テーマを掘り下げる

- 詳細な情報は専門書やWebで調べる
  各テーマの専門書は活用する
  Webはアプリケーションの配布元

- 問題は更新されるため、問題集に頼り過ぎない

試験対策　参考文献



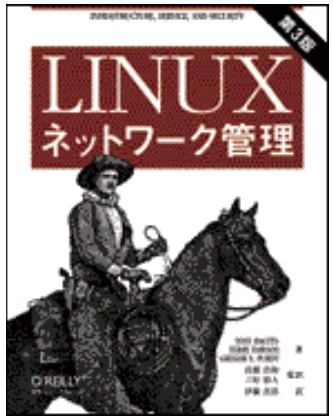
Linuxサーバー構築標準教科書
http://www.lpi.or.jp/linuxtext/server.shtml

Linux教科書 LPICレベル2 Version4.0対応
中島 能和 (著), 濱野 賢一朗 (監修)
出版社: 翔泳社 (2014/5/9)

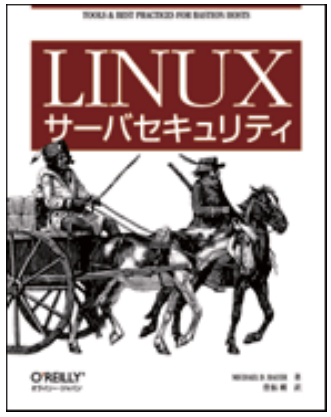
徹底攻略LPI 問題集Level2/Ver4.0 対応
中島 能和 (著),ソキウス・ジャパン (編集)
出版社: インプレスジャパン (2014/4/11)

その他　参考文献

Linuxシステム管理
ISBN978-4-87311-346-3

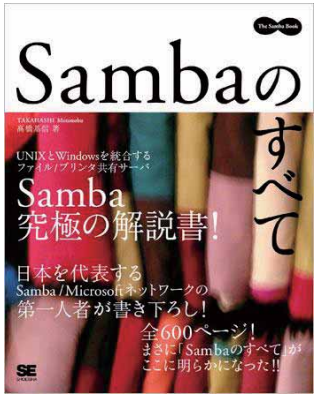


Linuxネットワーク管理 第3版
ISBN4-87311-247-8



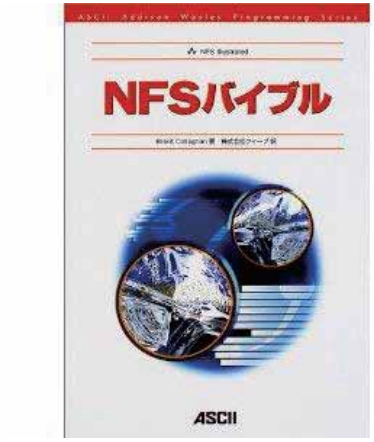
Linuxサーバセキュリティ
ISBN4-87311-149-8

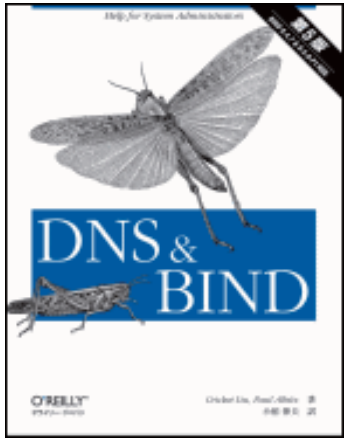
その他　参考文献



Sambaのすべて
高橋 基信 (著)
出版社: 翔泳社 (2005/6/30)
ISBN-10: 4798108545
ISBN-13: 978-4798108544

その他





HI CORP.

ありがとうございました。

株式会社エイチアイ

http://www.hicorp.co.jp

Linux Professional Institute