



# LPIC レベル2 技術解説無料セミナー

株式会社びぎねっと

宮原 徹

tmiyahar@Begi.net

# 講師プロフィール

- 株式会社びぎねっと 代表取締役社長兼CEO
  - 日本仮想化技術株式会社 代表取締役社長兼CEOでもある
- Linux・オープンソースに関するIT技術者教育を中心にビジネスを展開
- 現在は仮想化技術に関するソリューション提案を行っている (VMware・Xenなど)
- LPI-Japan発行 メールマガジン 執筆者



# 本日のアジェンダ

1. 出題範囲の確認と学習対策
2. ポイント解説
  - I. Linuxカーネル
  - II. セキュリティ



# 新出題範囲 (v3.0) について

- 2009年4月からリリース
- 主題が全体的にすっきりした
  - ニュース (NetNews) が無くなった！
  - PCMCIAが無くなった！
  - LVMがトピックとして独立
  - トラブルシューティングが1つにまとめられた



# 201試験の出題範囲(v3.0)

## 主題201:Linuxカーネル

201.1 カーネルの構成要素	2
201.2 カーネルのコンパイル	2
201.3 カーネルへのパッチ適用	1
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	2
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	3

## 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	4
202.2 システムを回復する	4

## 主題203:ファイルシステムとデバイス

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
203.3 ファイルシステムを作成して成する	2 オプションを構
203.4 udevでのデバイス管理	1

## 主題204:高度なストレージ管理

204.1 RAIDを構成する	2
204.2 記憶装置へのアクセス方法を調整する	1
204.3 論理ボリュームマネージャー	3

## 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とトラブルシューティング	4
205.3 ネットワークの問題を解決する	5
205.4 システム関連の問題をユーザーに通知する	1

## 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	4
206.2 バックアップ操作	3

## 主題207:ドメインネームサーバー

207.1 DNSサーバーの基本的な設定	2
207.2 DNSゾーンの作成と保守	2
207.3 DNSサーバーを保護する	2



# 202試験の出題範囲(v3.0)

## 主題208: Webサービス

208.1 Webサーバーの実装	3
208.2 Webサーバーの保守	2
208.3 プロキシサーバーの実装	1

## 主題209: ファイルとサービスの共有

209.1 Sambaサーバーの設定	4
209.2 NFSサーバーの設定	4

## 主題210: ネットワーククライアントの管理

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

## 主題211: 電子メールサービス

211.1 電子メールサーバーの使用	3
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

## 主題212: システムのセキュリティ

212.1 ルーターを構成する	3
212.2 FTPサーバーの保護	2
212.3 セキュアシェル(SSH)	4
212.4 TCPラッパ	1
212.5 セキュリティ業務	3

## 主題213: トラブルシューティング

213.1 ブート段階の識別と ブートローダーのトラブルシューティング	4
213.2 一般的な問題を解決する	5
213.3 システムリソースの問題を解決する	5
213.4 環境設定の問題を解決する	5



# 全体的な対策プラン(v3.0)

## サーバ構築でカバーされる範囲

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205: ネットワーク構成  
主題207: ドメインネームサーバー  
主題208: Webサービス  
主題209: ファイルとサービスの共有  
主題211: 電子メールサービス

じっくりと

## カバーされない範囲

主題201: Linuxカーネル  
主題204: 高度なストレージ管理  
主題206: システムの保守  
主題210: ネットワーククライアントの  
          管理  
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

しっかりと



# 学習の方法

- 出題範囲をしっかりと把握
  - 関連キーワードはすべて調べる
- 一般的なネットワークサーバ構築を学習
  - IPアドレス、DNS、Web、メール、ファイルサーバ等
- セキュリティについて学習
  - TCP/IPネットワークの知識を再確認すること
- トラブルシューティングの技法
  - 基礎知識の再確認
  - 自分なりによくあるトラブルをまとめてみる

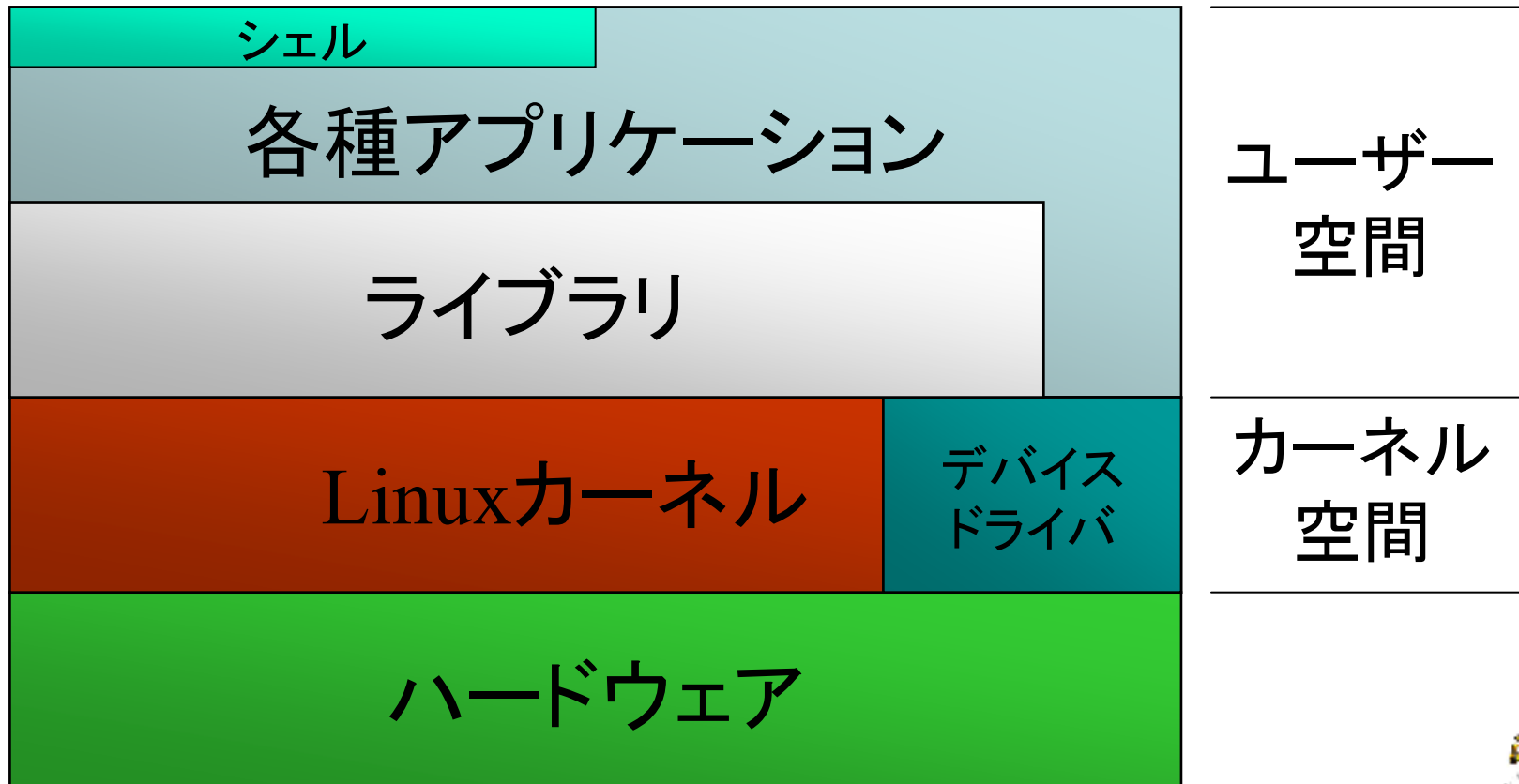


# ポイント解説 I

## カーネル



# Linuxの構造



# カーネル再構築(2.6系)

1. /usr/src/linuxにソースコードを展開(tar,gzip,bzip2等)
2. 必要に応じてパッチを当てる(patch -p0 < patch\_file)
3. (make mrproper 完全な消去)
4. make config カーネル設定
5. make clean 不要なものの消去
6. make **カーネルとモジュールの構築**
7. make modules\_install モジュールインストール
8. make install カーネルのインストールと  
ブートローダーの

設定



## 参考

# カーネル再構築(2.4系)

1. /usr/src/linuxにソースコードを展開(tar,gzip,bzip2等)
2. 必要に応じてパッチを当てる(patch -p0 < patch\_file)
3. (make mrproper 完全な消去)
4. make config カーネル設定
5. make dep 依存関係チェック
6. make clean 不要なものの消去
7. make bzImage カーネルの構築
8. make modules モジュールの構築
9. make modules\_install モジュールインストール
10. make install カーネルのインストールとブートローダーの設定



# カーネル設定

- カーネルの機能をON/OFF/モジュール化
  - ONにした機能はカーネル本体に組み込まれ、起動時にメモリにロードされる
  - モジュールは動的にロードされる
- 設定方法はconfig / menuconfig / xconfig
  - 2.6ではdefconfig / allmodconfig / allyesconfig / allnoconfigなども使用可能
- 設定ファイルは.configファイル
  - 以前のバージョンの.configを再利用したい場合にはmake oldconfigを実行



# 簡単カーネル設定方法

ディストリビューションで用意された.configを利用

1. カーネルソースパッケージをインストール
  - kernel-sourceやkernel-develなど
2. インストール先から.configを探す
  - 例: /usr/src/kernels/カーネルバージョン/.config
3. 新しいカーネルソースツリーに.configをコピー
4. make oldconfigを実行
  - 基本的にエンターキーを押しておけばいい
5. makeを実行



# モジュール関連

- 関連するファイル、ディレクトリ
  - インストール先: /lib/modules/[カーネルバージョン](#)
  - 設定ファイル: /etc/modules.conf・[modprobe.conf](#)
- 関連するコマンド
  - depmod 依存関係の調査
  - lsmod ロードされているモジュールの一覧
  - modprobe 依存関係を解消してロード
  - insmod/rmmodモジュールのロード/アンロード
  - mkinitrdRAMディスク作成



# ポイント解説 Ⅱ

## セキュリティ



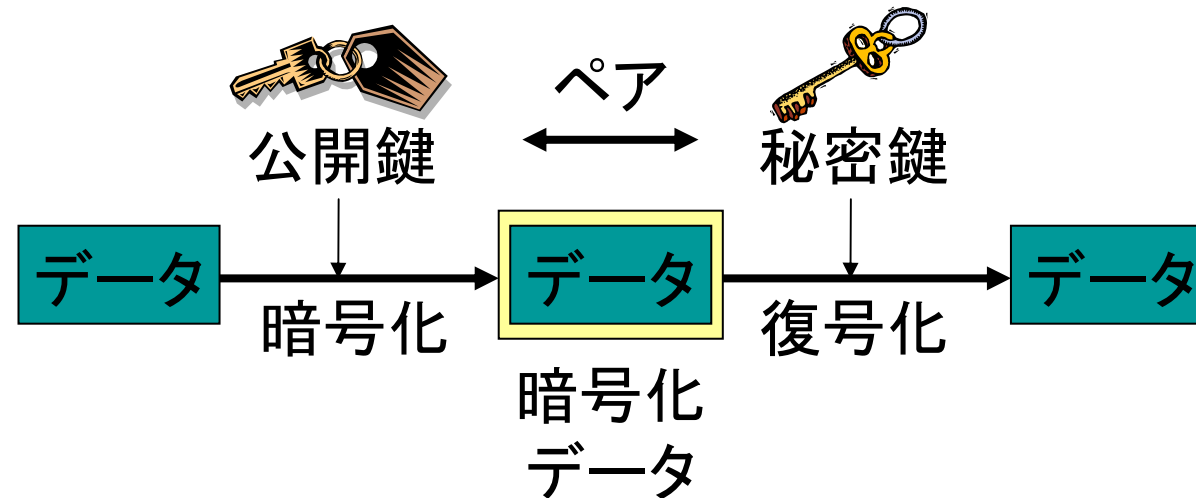
# SSHによる通信の暗号化

- 通信の暗号化を行うセキュアなリモートシェル
  - telnet, rlogin, rsh, rcpなどと置き換えが可能
    - コマンドラインターミナルとしての利用
  - 各種認証が可能
    - ホストベース認証/パスワード認証/公開鍵認証/S/Key認証 (One Time Password認証)
  - RSA暗号(SSH v1/v2)、DSA暗号(SSH v2)による公開鍵・秘密鍵暗号が利用可能
- LinuxではOpenSSHを使用
  - OpenSSHはOpenBSD開発グループが開発を行っているフリーなSSHソフトウェア

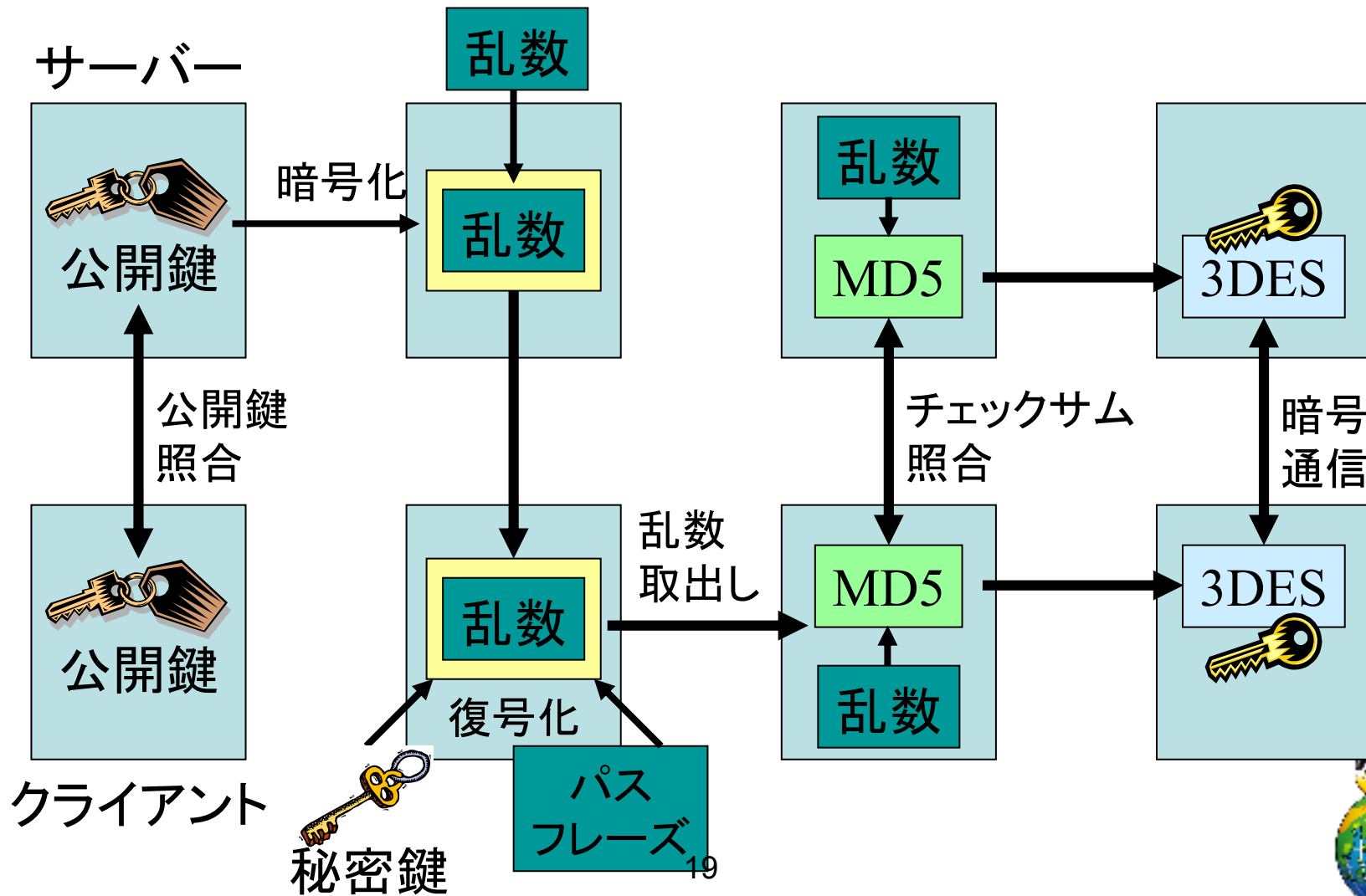


# 公開鍵・秘密鍵暗号

- 秘密鍵と公開鍵はペアで生成される
- 一方の鍵で暗号化されたデータは、もう一方の鍵だけが復号化できる



# 公開鍵認証



# 公開鍵・秘密鍵の生成

OpenSSHが使う公開鍵と秘密鍵のペアを生成

1. 鍵の生成にはssh-keygenコマンドを使用
  - -tオプションで使用する暗号化アルゴリズムを指定
  - ssh-keygen -t dsa (SSH v2・DSA暗号)
2. 実行時にはパスフレーズの入力が必要
  - 画面には表示されない
  - 2回入力が必要
3. 鍵は~/.sshディレクトリに生成される
  - 秘密鍵ファイル id\_dsa
  - 公開鍵ファイル id\_dsa.pub



# 公開鍵をサーバーに設置

1. 公開鍵を`~/.ssh/authorized_keys`に追加
  - 上書きを防ぐため、`cp`コマンドではなく`cat`コマンド+追加リダイレクト(`>>`)で行うこと
  - 他人の公開鍵の場合には事前に「指紋」で鍵の同一性チェックを行う(`ssh-keygen -l`)
2. `~/.ssh`ディレクトリと`authorized_keys`の所有者とパーミッションの確認と変更
  - `~/.ssh`ディレクトリ   モード700(`rwX-----`)
  - `authorized_keys`    モード600(`rw-----`)



# sshコマンドでサーバーに接続

1. 現在のユーザーの~/.ssh/ディレクトリに公開鍵・秘密鍵があることを確認
2. sshコマンドを実行
  - `$ ssh username@hostname`
3. ~/.ssh/known\_hosts2への公開鍵の追加
4. 公開鍵の照合に成功するとパスフレーズを聞かれる
  - パスワードを聞かれたら公開鍵認証失敗



# まとめ

- じっくりとサーバ構築などのスキルを学ぶ  
→ 幹作り
- 関連するトピックに対する知識を増やす  
→ 枝葉を伸ばす
- 実機を使用して1つずつ確認しながら
  - manコマンドが重要
- 問題集などでスキルチェック



# LPIメルマガのご紹介

- ・ 『LPI通信』
  - Linuxオープンソース関連ニュース
  - Linuxの利用に役立つTipsやテクニック
  - LPI合格者の声
- ・ 『LPIC Level2・Level3を受けてみよう！』
  - Level2・Level3の例題解説
  - Level2・Level3を取得するメリット、活用の事例など
  - Level1をお持ちでない方にも役立ちます

<http://www.lpi.or.jp/mail/>

