

ITプロ/ITエンジニアのための

# 徹底攻略

試験番号  
LPIC Level3 Specialty 303



Linux  
Professional  
Institute

LPI 出題範囲準拠教材  
ロゴ使用承認番号 LPI1120117

# LPI Level 3

[303 Version 1.0] 対応

# 問題集

金沢泳義 / 葛蒲淳司 著 森嶋秀樹 監修  
株式会社ソキウス・ジャパン 編

**303 Ver 1.0 試験** に対応した電子版!!

出題傾向を  
徹底分析した  
受験対策に最適な問題集です。

LPIC Level 3  
**303** Version  
**1.0**  
(Security Exam)  
対応

「最重要ポイント」  
がひと目でわかる。



試験対策

シリーズ

**100万部 突破!!**

インプレス

本書は、LPI認定試験（LPIC）レベル3の受験対策用の教材です。著者、株式会社インプレスは、本書の使用によるLPI認定試験（LPIC）レベル3への合格を一切保証しません。

本書の内容については正確な記述につとめました。著者、株式会社インプレスは本書の内容に基づくいかなる試験の結果にも一切責任を負いません。

「LPI出題範囲準拠教材」とは本書がLPIの出題範囲を網羅していることを出版元が示すものであり、LPIが本書の内容を認定し証明するものではありません。

Linuxは、Linus Torvaldsの米国およびその他の国における登録商標または商標です。

その他、本文中の製品名およびサービス名は、一般に開発メーカーおよびサービス提供元の商標または登録商標です。なお、本文中には™、®、©は明記していません。

## インプレスの書籍ホームページ

書籍の新刊や正誤表など最新情報を随時更新しております。

<http://book.impress.co.jp/>

Copyright © 2012 Socius Japan, Inc. All rights reserved.

本書の内容はすべて、著作権法によって保護されています。著者および発行者の許可を得ず、転載、複写、複製等の利用はできません。

## まえがき

最近ではテレビのCMなどでも「クラウド」という言葉がごく普通に使われています。ここ数年でクラウドに関する新たな商品やソリューションも多く見られるようになりましたが、その多くは既存の製品にセキュリティと仮想化技術を組み合わせたものです。本書で扱うLPIC試験のセキュリティ (LPIC-303) と仮想化・高可用性 (LPIC-304) は、まさに今の時代を反映した試験といえるでしょう。

現在はベンダーが提供する有償製品を利用したソリューションが大勢を占めている状況ですが、オープンソースだけでもここまでできるということを本書を通して少しでも実感し、そして無事試験に合格していただければ、著者としてこれ以上の幸せはありません。

本書の執筆にあたっては、効率的に試験対策ができるよう、次のような点に配慮しました。

### ●セキュリティ (LPIC-303)

この試験科目では既存技術をどのようにセキュアに扱うことができるかを問う問題が多いため、当パートではLPICレベル1、レベル2の出題範囲で扱う技術の内容については詳説せずに、セキュリティ面の考え方を中心に解説しています。

### ●仮想化・高可用性 (LPIC-304)

仮想化・高可用性はLPICで初めて出題される分野であるため、各技術の概要について文章だけでなく図も用いて、感覚的にも理解しやすいように解説しています。

### ●303/304共通

単なる問題と解答の羅列ではなく、問題を進めるにつれ段階的に知識が深まるよう構成に配慮して執筆しました。また、各コマンドの説明は、試験対策の面で特に重要なもののみを抜粋しています。本書に記載されていない部分については、実機の動作確認や公式マニュアルなどでの学習をおすすめします。

本書の内容、特に仮想化・高可用性は日進月歩の技術分野であり、日々進化し続けています。今までは実現できないとされていたことができるようになったり、必要とされていたコンポーネントが不要となったりすることもあるでしょう。しかし、本書で学んだ内容は決して無駄にはなりません。これを基礎として、新たな情報に目を向けて行くことが、より高い技術力につながると確信しています。

最後に、ソキウス・ジャパン坂田様をはじめ、本書の執筆に関わったすべての方々にも心よりお礼を申し上げます。

2012年1月吉日  
著者代表 金沢 泳義

本書は、2012年2月発行の『徹底攻略LPIC問題集 Level3 [303/304] 対応』のうち、303試験範囲の内容のみを抜粋し、新たに『徹底攻略LPIC問題集 Level3 [303 Version 1.0] 対応』として発行したものです。

## LPI認定試験について

LPIC(エルピック)はLPI(Linux Professional Institute:Linux技術者認定機関)が実施している世界共通のLinux技術者認定制度です。特定のLinuxディストリビューションに依存しない汎用性の高い認定資格制度であることが知られています。2016年1月時点では日本国内での累計受験者数は27万人を超え、9万6,000人以上が認定を取得している人気の資格です。

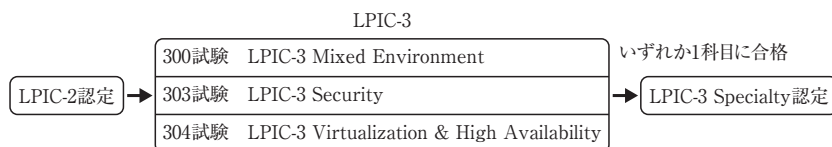
LPICのレベルには、「LPIC-1(LPICレベル1)」「LPIC-2(LPICレベル2)」「LPIC-3(LPICレベル3)」の3つがあります。2016年4月現在のLPIC資格体系は以下のとおりです。

### 【LPIC資格体系】

資格	試験 (バージョン)	認定されるスキル
LPIC-1	101試験 (4.0)	実務に必要なLinuxの基本操作とシステム管理が行えるエンジニアであること
	102試験 (4.0)	
LPIC-2	201試験 (4.0)	Linuxのシステムデザイン、ネットワーク構築において、企画、導入、維持、トラブルシューティング、キャパシティプランニングができるエンジニアであること
	202試験 (4.0)	
LPIC-3	300試験 (1.0)	Linux、Windows、Unixが混在するシステムの設計、構築、運用・保守ができるエキスパートエンジニアであること
	303試験 (1.0/2.0) *	セキュリティレベルの高いコンピュータシステムの設計、構築、運用・保守ができるエキスパートエンジニアであること
	304試験 (2.0)	クラウドコンピューティングシステム(クラウド)の設計、構築、運用・保守ができるエキスパートエンジニアであること

※ バージョン 1.0 は 2016 年 8 月 31 日 で配信終了

現在、LPIC レベル 3 に対応する試験は、「LPIC-3 Mixed Environment (300 試験)」「LPIC-3 Security (303 試験)」「LPIC-3 Virtualization & High Availability (304 試験)」の3つが実施されています。3 試験のうちいずれかに合格し、かつ、有意な LPIC レベル 2 の認定を持っていると、「LPIC レベル 3 Specialty」に認定されます。



## 303試験Version 1.0の概要

### ●試験概要

- ・ 試験名 : LPI303 Security Exam
- ・ 試験時間 : 90分
- ・ 問題数 : 約60問
- ・ 受験料 : 30,000円 (税抜き)

### ●出題範囲について

出題範囲は、「暗号化」「アクセス制御」「アプリケーションセキュリティ」「操作のセキュリティ」「ネットワークセキュリティ」の5つのカテゴリに分かれています。

主題 320 : 暗号化

- 320.1 OpenSSL
- 320.2 高度な GPG
- 320.3 暗号化ファイルシステム

主題 321 : アクセス制御

- 321.1 ホストベースのアクセス制御
- 321.2 拡張属性と ACL
- 321.3 SELinux
- 321.4 その他の強制アクセス制御システム

主題 322 : アプリケーションセキュリティ

- 322.1 BIND/DNS
- 322.2 メールサービス
- 322.3 Apache/HTTP/HTTPS
- 322.4 FTP
- 322.5 OpenSSH
- 322.6 NFSv4
- 322.7 syslog

主題 323 : 操作のセキュリティ

- 323.1 ホスト構成管理

主題 324 : ネットワークセキュリティ

- 324.1 侵入検出
- 324.2 ネットワークセキュリティスキャン機能
- 324.3 ネットワークの監視
- 324.4 netfilter/iptables
- 324.5 OpenVPN

### 【303 試験の出題範囲詳細 (Version1.0)】

<http://www.lpi.or.jp/lpic3/range/ver1.0/range303.shtml>

※ バージョン 1.0 と 2.0 では出題範囲が異なります。必ず上記で確認してください。

## ●試験方法

試験会場に用意されたコンピュータを使って行われます。試験問題のほとんどはマウスによる多岐選択方式ですが、キーボードから入力して解答する問題も一部出題されます。

## ●合否結果と資格認定

試験終了後、合否と得点が印刷されたスコアレポートが渡されます。試験に合格すると、約2カ月後にLPI本部（カナダ）から認定証が届きます。

# 受験申し込み方法

## ●LPI-IDの取得

LPI認定試験の受験を申し込むには、事務局が指定するWebページからLPI-IDを取得する必要があります。

・登録用Webページ：<https://bloom.lpi.or.jp/caf/Xamman/register>

## ●受験申し込み先

ピアソンVUEにWebまたは電話で受験予約をします。予約状況によっては希望どおりの会場や日時を選択できない場合もありますので、必ず予約状況を確認してください。また、予約時にLPI-IDが必要になります。LPI-IDを間違えると試験結果が反映されないことがありますので気をつけてください。

## ●ピアソンVUE

URL：<http://www.pearsonvue.co.jp/>

TEL：0120-355-173 または 0120-355-583

FAX：0120-355-163

E-Mail：[pvjpreg@pearson.com](mailto:pvjpreg@pearson.com)

初めてピアソンVUEに申し込む場合は、受験者情報を登録する必要があります。その後、以下のいずれかの方法で申し込むことができます。

### ・Webからの申し込み

<http://www.pearsonvue.co.jp/>からログインして予約

### ・電話での申し込み

上記電話番号に直接申し込み（受付時間：平日午前9時～午後6時）

### ・テストセンターに直接申し込み

テストセンター一覧から受験希望のテストセンターを確認したうえで直接連絡

## LPI-Japanの連絡先

〒106-0041 東京都港区麻布台1-11-9 CR神谷町ビル 7F

TEL :03-3568-4482

FAX :03-3568-4483

E-Mail :[info@lpi.or.jp](mailto:info@lpi.or.jp)

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

最新の試験情報は、必ず上記のWebサイトで確認してください。

## 再受験ポリシーについて

2010年11月18日より、LPI認定試験に関する再受験ポリシーが下記のとおり変更になりました。最新の再受験ポリシーについては、必ずLPI-JapanのWebサイトで確認してください。

- ・ LPIC同一科目を再受験する際、2回目の受験については、受験日の翌日から起算して7日未満（土日含む）より可能
- ・ 3回目以降の受験については、最後の受験日の翌日から起算して30日未満より可能
- ・ 一度合格した科目については、受験日から2年間は再受験できない
- ・ 受験後2年間を経た場合、再受験ポリシーはいったんクリアになり、その後の同一試験の最初の再受験は一度目の受験としてカウントされる

## 本書の活用方法

本書は、カテゴリ別に分類された問題と解答で構成されています。

### ●問題

本書の問題は、LPI認定試験レベル3の試験科目である「303試験（バージョン1.0）」の合格に必要な知識を効率的に学習することを目的に作成したものです。解答していくだけで、合格レベルの実力が身に付きます。また、実際の試験に近い形式になっていますので、試験の雰囲気をつかむことができます。

#### 多岐選択式の問題

「選択肢から1つだけ選ぶもの」と「該当する複数の選択肢を選ぶもの」があります。複数の選択肢を選ぶ問題では、結果としてすべての選択肢を選ぶことになる場合もあります。

10. 保持している鍵の信用度や有効性を記録しているファイルとして適切なものを選びなさい。

- A. trustedkeys.gpg
- B. pubring.gpg
- C. trustdb.gpg
- D. secring.gpg

⇒ P26

#### チェックボックス

確実に理解している問題のチェックボックスを塗りつぶしながら問題を解き進めると、2回目からは不確かな問題だけを効率的に解くことができます。すべてのチェックボックスが塗りつぶされれば合格は目前です。

#### 解答ページ

問題の右下に、解答ページが表示されています。ランダムに解くときも、解答ページを探すのに手間取ることがありません。

#### キーボードから入力する問題

「説明文を読んでコマンド名やファイル名、用語などをキーボードから入力するもの」と「コマンドやオプションなどを入力して空欄をうめるもの」があります。

7. ファイルのACL情報を取得するコマンドを下線部に記述しなさい。

\_\_\_\_\_

⇒ P43

7. デジタル署名を用いて、ファイルが改ざんされていないことを検証したい。gpgコマンドのサブコマンドを記述しなさい。

gpg \_\_\_\_\_ gnupg-a. b. c. tar. gz. asc

### ●解答

解答には、問題の正解やその理由だけでなく、用語や重要事項などが詳しく解説されています。

**2. A**

opensslのコマンドのうち、メッセージダイジェストの計算をするコマンドは openssl dgst です (A)。

B. openssl genrsaコマンドは、RSA秘密鍵を生成します。

C. openssl reqコマンドは、X.509証明書署名リクエスト(CSR)を管理します。

D. openssl x509コマンドは、X.509証明書データを管理します。

#### 解説（選択肢）

正解である選択肢は(A)のように表記し正解の根拠を示しています。

#### 解説（用語）

重要な用語は、太字で表記されています。



## 目次

	まえがき .....	3
	LPI認定試験について .....	4
	303試験Version 1.0の概要 .....	5
	受験申し込み方法 .....	6
	本書の活用方法 .....	8
<b>第1章</b>	<b>暗号化</b>	
	問題 .....	12
	解答 .....	16
<b>第2章</b>	<b>アクセス制御</b>	
	問題 .....	32
	解答 .....	39
<b>第3章</b>	<b>アプリケーションセキュリティ</b>	
	問題 .....	56
	解答 .....	62
<b>第4章</b>	<b>操作のセキュリティ</b>	
	問題 .....	76
	解答 .....	79
<b>第5章</b>	<b>ネットワークセキュリティ</b>	
	問題 .....	86
	解答 .....	94
<b>第6章</b>	<b>総仕上げ問題</b>	
	問題 .....	116
	解答 .....	132



# 第

# 1

# 章

## 暗号化

- OpenSSL
  - GPG
- 暗号化ファイルシステム
  - LUKS

1. RSA秘密鍵を生成し、privkey.pemファイルに出力するコマンドとして適切なものを選びなさい。

- A. openssl req -out privkey.pem 1024
- B. openssl req privkey.pem 1024
- C. openssl genrsa -out privkey.pem 1024
- D. openssl genrsa privkey.pem 1024
- E. openssl ca -out privkey.pem 1024

→ P16

2. opensslのコマンドのうち、メッセージダイジェストを計算するコマンドとして適切なものを選びなさい。

- A. openssl dgst
- B. openssl genrsa
- C. openssl req
- D. openssl x509

→ P19

3. イントラネット上のサーバ「192.168.0.2」のポート番号443に接続できるか確認したい。下線部に当てはまるコマンドを選びなさい。

openssl \_\_\_\_\_ 192.168.0.2:443

- A. connection
- B. req -connect
- C. client -s
- D. s\_client -connect
- E. ca

→ P19

4. 外部の認証局で署名せずに自己署名するopensslコマンドのサブコマンドを記述しなさい。

openssl \_\_\_\_\_ -new -x509 -key server.key -out server.crt -days 365

→ P19

5. 公開鍵サーバに鍵を登録するgpgコマンドとして適切なものを選びなさい。

- A. gpg --gen-key
- B. gpg --delete-key
- C. gpg --sign-key
- D. gpg --send-keys
- E. gpg --recv-keys

⇒ P20

6. 以下のコマンドと、その説明の組み合わせとして誤っているものを選びなさい。

- A. gpg --send-keys — 鍵サーバに鍵を登録する
- B. gpg --recv-keys — 鍵サーバから鍵を読み込む
- C. gpg --search-keys — 鍵サーバの鍵を検索する
- D. gpg --refresh-keys — 鍵サーバの鍵情報を消去する

⇒ P24

7. デジタル署名を用いて、ファイルが改ざんされていないことを検証したい。gpgコマンドのサブコマンドを記述しなさい。

gpg \_\_\_\_\_ gnupg-a.b.c.tar.gz.asc

⇒ P25

8. デジタル署名の照合ツールとして適切なものを選びなさい。

- A. gpgsign
- B. gpgv
- C. gpgconfig
- D. gpgdiff
- E. opengpg

⇒ P25

9. GPGの秘密鍵を管理するコマンドとして適切なものを選びなさい。

- A. gpg-agent
- B. gpg-daemon
- C. gpg-management
- D. gpg-seckey
- E. gpg-pubkey

→ P25

10. 保持している鍵の信用度や有効性を記録しているファイルとして適切なものを選びなさい。

- A. trustedkeys.gpg
- B. pubring.gpg
- C. trustdb.gpg
- D. secring.gpg

→ P26

11. dm-cryptの暗号化ボリュームをセットアップするコマンドとして適切なものを選びなさい。

- A. cryptsetup
- B. cryptstart
- C. dmcryptsetup
- D. dmcryptstart
- E. dmcryptconfig

→ P26

12. LUKSパーティションを開くコマンドとして適切なものを選びなさい。

- A. cryptsetup luksAddKey
- B. cryptsetup luksClose
- C. cryptsetup luksDelKey
- D. cryptsetup luksOpen
- E. cryptsetup luksFormat

→ P27

13. システム上で暗号化されたファイルシステムのマウント、アンマウント、設定を行うコマンドとして適切なものを選びなさい。

- A. cryptmount-setup
- B. cryptconfig
- C. cryptmount
- D. cryptunmount

⇒ P29

14. cryptmountで利用できるすべてのターゲットの基本情報をリストアップするコマンドとして適切なものを選びなさい。

- A. /usr/bin/crypt/cryptmount --verbose
- B. /usr/bin/crypt/cryptmount --list
- C. /usr/bin/crypt/cryptmount --get
- D. /usr/bin/crypt/cryptmount --listup
- E. /usr/bin/crypt/cryptmount --target

⇒ P30

15. dm-cryptコマンドの暗号化モードとして適切でないものを選びなさい。

- A. CBC
- B. ESSIV
- C. LRW
- D. DMC
- E. XTS

⇒ P30