

# 模擬試験

ITILF.JP

ITサービスマネジメント ファンデーション(ITIL®準拠)  
2007年11月版

## 目次

2	はじめに
3	模擬試験
12	解答集
29	評価



**EXIN International B.V.**

**Examination Institute for Information Science**

Janssoenborch, Hoog Catharijne

Godebaldkwartier 365, 3511 DT Utrecht

P.O. Box 19147, 3501 DC Utrecht

The Netherlands

Telephone +31 30 234 48 25

Fax +31 30 231 59 86

E-mail [info@exin.nl](mailto:info@exin.nl)

Internet [www.exin-exams.com](http://www.exin-exams.com)

## はじめに

これは ITサービスマネジメント ファンデーション(ITIL®準拠)です。

本試験は選択式の問題が40問で構成されます。各問題にはそれぞれ答の選択肢があり、その中の1つだけが正しい答となっています。

本試験では1問に正解する毎に1点が加算されます。最高得点は40点で、26点以上が合格となります。

本試験の制限時間は60分です。

この情報によって何らの権利が生じるものではありません。

ご健闘をお祈りいたします。

Copyright © 2007 EXIN

All rights reserved. No part of this publication may be published, reproduced, copied or stored in a data processing system or circulated in any form by print, photo print, microfilm or any other means without written permission by EXIN.

ITIL® is a Registered Community Trade Mark of OGC (Office of Government Commerce, London, UK), and is Registered in the U.S. Patent and Trademark Office.

## 模擬試験

### 第1問

コストを割り当てる仕組みを設けることに責任があるのは、どのプロセスですか？

- A. 可用性管理
- B. キャパシティ管理
- C. ITサービス財務管理
- D. サービスレベル管理

### 第2問

ITインフラストラクチャにおける全てのコンポーネントを記述し、登録する活動を含むのは、どのプロセスですか？

- A. キャパシティ管理
- B. 構成管理
- C. 問題管理
- D. サービスレベル管理

### 第3問

サービスマネジメントのイニシアティブ全体の一部としてサービスの可用性を管理することは、効率的サービスデリバリーにとって重要です。

サービスの可用性を管理する背景の理由を説明するのは、次のどれですか？

- A. ほとんどのサービス・プロバイダは顧客とのサービスレベル・アグリーメント(SLA)を持っており、可用性は保証されている。
- B. アウトソーシングは今日のITにとって今やより有効な選択肢であるため、サービスの可用性はアウトソーサの能力に委ねられている。
- C. サービスマネジメントのツールはリアル・タイムのパフォーマンス情報を提供するため、可用性を管理することには異論がある。
- D. コーポレートのゴールを満たすために、ビジネスはよりITへと依存しており、従って期待される可用性に到達することは必須である。

### 第4問

サービスデスクの活動ではないのはどれですか？

- A. 一時的修正を適用すること。
- B. インシデントを登録すること。
- C. インシデントを既知のエラーに関連付けること。
- D. 問題を解決すること。

## 第5問

インシデント管理において、技術的専門家の付加的な利用を何と呼びますか？

- A. 機能的エスカレーション
- B. インシデント分類
- C. 問題の分析
- D. インシデントの解決と復旧

## 第6問

リリース管理プロセスを確立する際、**最初**の活動は何ですか？

- A. コミュニケーション、準備とトレーニング
- B. リリース計画の実施
- C. 設計と構築、および構成
- D. リリース・ポリシーの確立

## 第7問

ITサービス継続性管理の責任ではない活動はどれですか？

- A. リスクの分析
- B. 復旧シナリオの設計
- C. 重大なインシデントのインパクト分析
- D. 復旧対策のテスト

## 第8問

キャパシティ・マネージャが、CPUが日中に過負荷とならないよう、ある活動が夜間に実施可能かどうか、アプリケーションのユーザに質問します。

これはキャパシティ管理プロセスのどの部分に相当していますか？

- A. アプリケーション管理
- B. アプリケーション・サイジング
- C. 需要管理
- D. モデル化

## 第9問

問題の診断が成功すれば、既知のエラーにたどり着きます。この既知のエラーに基づき、変更要求(RFC)が提起される場合があります。

いつ既知のエラーをクローズさせることができますか？

- A. 変更のレビューが満足のいく結果を導いたとき。
- B. 既知のエラーに関連するインシデントがもはや発生しないとき。
- C. RFCが変更管理に伴い記録されたとき。
- D. RFCが変更諮問委員会(CAB)に許可されたとき。

## 第10問

X社ではITインフラストラクチャの特定のコンポーネントが修正されました。これは他のコンポーネントに影響する場合があります。

これらの影響に正しい見解を提供するために、設けられるべきプロセスは何ですか？

- A. 可用性管理
- B. キャパシティ管理
- C. 変更管理
- D. 構成管理

## 第11問

ITサービス継続性管理では、大災害の間や後にサービスがデリバリされることを確実にするため、様々な予防的対策が取られています。非常用電源を設置することも一例です。

次のどのプロセスにおいて、この種の対策に着手する場合がありますか？

- A. 可用性管理
- B. キャパシティ管理
- C. 変更管理
- D. インシデント管理

## 第12問

導入後のレビュー(PIR)が開催されなければならないのはいつですか？

- A. 毎変更後
- B. 変更要求を提出した人が要求した時
- C. 非常時の変更の場合
- D. 変更実施後同じタイプの別のインシデントが再発する場合

### 第 13 問

インシデント管理の第一ステップは何ですか？

- A. 検知と記録
- B. カテゴリの決定
- C. 優先度の決定
- D. 初期サポート

### 第 14 問

サービスデスクでイベントが記録されたとき、おおよその順番でプロセスは実行されますか？

- A. 構成管理、インシデント管理、変更管理、リリース管理
- B. インシデント管理、変更管理、問題管理、リリース管理
- C. インシデント管理、問題管理、変更管理、リリース管理
- D. 問題管理、構成管理、リリース管理、変更管理

### 第 15 問

サービスデリバリとそのセキュリティ管理との関係に関する合意は、どこに記録されますか？

- A. キャパシティ計画の中
- B. 構成管理データベース(CMDB)の中
- C. 確定版ソフトウェア保管庫(DSL)の中
- D. サービスレベル・アグリーメント(SLA)の中

### 第 16 問

サービスカタログに関する次の記述で、正しいのはどれですか？

- A. それはサービスレベル・アグリーメント(SLA)の代わりに利用可能です。
- B. それはITマネジメント組織により供給される、全てのサービスを記述します。
- C. それはサービスレベル・アグリーメント(SLA)にも含まれるサービスのみを記述します。
- D. それはサービスレベル・アグリーメント(SLA)を作成するためには必要ではありません。

### 第 17 問

承認された変更はどこで発表されますか？

- A. 変更諮問委員会(CAB)
- B. 構成管理データベース(CMDB)
- C. 将来的な変更スケジュール(FSC)
- D. サービス改善プログラム(SIP)

## 第 18 問

確定版ソフトウェア保管庫(DSL)の中身に関する説明で最も適しているのは、次のどれですか？

- A. インフラストラクチャ上で使用される全ソフトウェアの許可されたバージョン
- B. 全稼働環境のソフトウェア・プログラムのコピー
- C. 必要とされる全ソフトウェア・バージョンのコピー
- D. ユーザの受け入れテストを待つソフトウェア

## 第 19 問

ユーザから報告されたサービスの中断を分類するタスクは、どのプロセスにありますか？

- A. 変更管理
- B. インシデント管理
- C. 問題管理
- D. サービスレベル管理

## 第 20 問

あるスーパーのキャッシュ・レジスターでは、毎日午後4時から6時の間、ネットワークの中断を経験しています。

これらの困難を説明する責任は、どのプロセスにありますか？

- A. 可用性管理
- B. キャパシティ管理
- C. 変更管理
- D. 問題管理

## 第 21 問

変更要求(RFC)に対し、軽微、深刻/重要、重大といったカテゴリを決定する際、変更管理によって利用される基準は何ですか？

- A. 内容
- B. インパクト
- C. 優先度
- D. 緊急度

## 第 22 問

構成管理データベース(CMDB)から直接答えることのできないものは、次の質問のどれですか？

- A. 何のインシデントや問題がこのPCにあるのか？
- B. 特定のサービスはどの構成アイテム(CI)から成り立っているのか？
- C. X部門のスタッフのどのメンバがY部門に異動したのか？
- D. どの変更要求(RFC)が特定のサーバに対して提出されたのか？

### 第 23 問

組織は、どのようにしてサービスレベル管理プロセスの有効性を判断することができますか？

- A. サプライヤとの契約をチェックすることにより
- B. サービスレベルを定義することにより
- C. 顧客満足を測定することにより
- D. 全インシデントへの報告により

### 第 24 問

サービスデスクの活動ではないものは、次のどれですか？

- A. インシデントの検知と記録
- B. インシデントの調査と診断
- C. サービス要求の管理
- D. 所有、監視、トラッキング、コミュニケーション

### 第 25 問

サービスの設計、開発、デリバリーに対し、可用性管理の方法論やテクニックを適用することにより、そのサービスの可用性全体に影響しないものは、次のどれですか？

- A. コンポーネントへの支出
- B. インフラストラクチャの対障害弾力性
- C. サポート組織やサプライヤによるメンテナンスの品質
- D. コンポーネントの信頼性

### 第 26 問

問題管理の活動ではないものは、次のどれですか？

- A. 第三者のサプライヤとの関係維持
- B. 傾向分析を通じたインシデントのプロアクティブな予防
- C. 受容された時間枠を超過したインシデントの責任をとること
- D. サービスの可用性が合意されたレベルを確実に満足するよう、可用性管理と密接に働くこと

### 第 27 問

キャパシティ管理の活動は、次のどれですか？

- A. 保守性
- B. リソース管理
- C. セキュリティ
- D. サービス性

### 第 28 問

インシデント管理のゴールは何ですか？

- A. 将来のサービスの中断について顧客およびユーザとコミュニケーションすること
- B. 新規のインシデントを既知のエラーと照合すること
- C. サービスをできるだけ速く回復すること
- D. 既知のエラーのデータベース(KEDB)の中で、問題を追跡すること

### 第 29 問

セキュリティ管理プロセスにおける完全性の基本コンセプトを記述しているのは、次のどれですか？

- A. いつでもデータにアクセスすること
- B. 許可されていないアクセスと利用に対するデータの保護
- C. データの正確性を検証する能力
- D. データの正確性

### 第 30 問

構成管理のどの活動において、監査が定期的に行われますか？

- A. 識別
- B. 計画
- C. ステータスの監視
- D. 検証

### 第 31 問

顧客向けに設計したサービスレベル・レポートにおいて、在ると期待されない視点はどれですか？

- A. サービスデスクのスタッフの平均稼働率
- B. 実現された可用性のレベルと期間ごとの非可用時間
- C. 目標内で解決されたインシデントの割合
- D. 期間ごとの成功および切り戻された変更

### 第 32 問

キャパシティ管理と最も直接的関係もしくは相互依存性があるのは、次のどのプロセスですか？

- A. 可用性管理
- B. 構成管理
- C. ITサービス継続性管理
- D. リリース管理

### 第 33 問

プロセスはあらかじめ定義されたゴールに向かう、論理的に首尾一貫した一連の活動です。

プロセス・オーナーは何に責任がありますか？

- A. プロセスを記述すること
- B. プロセスを実装すること
- C. プロセス・レポートを提供すること
- D. プロセスを設立すること

### 第 34 問

電源障害によってITインフラストラクチャ全体が不能になりました。幸いにも、ITサービス継続性(ITSC)計画は利用可能です。

どの時点で危機管理チームに、ITSC計画を発動を依頼すべきですか？

- A. ITサービスが利用不可能となつてすぐ
- B. 障害がサービスレベル・アグリーメント(SLA)に定義された目標を超えて続きそうなとき
- C. インシデント・マネージャが必要と考えたとき
- D. 故障が解決されるべき時間を超えたとき

### 第 35 問

新しいワークステーションのリクエストを標準化するプロセスもしくは機能はどれですか？

- A. 変更管理
- B. インシデント管理
- C. サービスデスク
- D. サービスレベル管理

### 第 36 問

サービスデスクの役割を最もよく記述しているのはどれですか？

- A. サービスデスクは合意されたITサービスが利用可能になることを確実にします
- B. サービスデスクは電話要員が常に配置されることを確実にします
- C. サービスデスクはユーザに対する単一窓口です
- D. サービスデスクの最も重要なタスクは問題を調査することです

### 第 37 問

ITIL®を利用する利点は次のどれですか？

- A. 最終的にITサービスに対する請求が可能になります
- B. ITサービスを取り巻く組織をより速く設立することができます
- C. ITサービスの品質やコストをより効率的にコントロールすることができます
- D. ユーザがITサービスを提供するIT組織に影響を及ぼすことができます

### 第 38 問

変更管理において、変更要求(RFC)の受け入れから変更の完了までの間、多数の活動が行われます。

変更要求の受け入れ後**最初**に実施される活動はどれですか？

- A. 変更の構築とテスト
- B. 変更の緊急度の決定
- C. 変更の実装
- D. 変更要求のスケジューリング

### 第 39 問

構成管理データベース(CMDB)の文脈において「詳細レベル」という用語は何を意味しますか？

- A. データベース構造の深さ
- B. 構成アイテム(CI)の場所
- C. 保管される構成アイテム(CI)の量
- D. 異なった構成アイテム(CI)間の関係

### 第 40 問

次のタスクのうち、プロアクティブな問題管理の一部はどれですか？

- A. 傾向の分析
- B. 問題を解決する変更の作成
- C. 既知のエラーの管理
- D. 頻繁に発生するエラーの登録

## 解答集

### 第1問

コストを割り当てる仕組みを設けることに責任があるのは、どのプロセスですか？

- A. 可用性管理
- B. キャパシティ管理
- C. ITサービス財務管理
- D. サービスレベル管理

- A. 不正解。可用性管理はITサービスの可用性に責任があります。
- B. 不正解。キャパシティ管理は適切な時点での適切なキャパシティに対し戦略的責任があります。
- C. 正解。ITサービス財務管理はコストを割り当てる仕組みを設けることに責任があります。
- D. 不正解。サービスレベル管理はサービスレベル・アグリーメント(SLA)の管理に責任があります。

### 第2問

ITインフラストラクチャにおける全てのコンポーネントを記述し、登録する活動を含むのは、どのプロセスですか？

- A. キャパシティ管理
- B. 構成管理
- C. 問題管理
- D. サービスレベル管理

- A. 不正解。キャパシティ管理は適時適切なキャパシティに対し戦略的責任があり、問題や中断に対する責任はありません。
- B. 正解。構成管理は構成管理データベース(CMDB)に構成アイテム(CI)を登録する責任があります。
- C. 不正解。問題管理は(プロアクティブな)問題解決に責任があるプロセスです。
- D. 不正解。サービスレベル管理はサービスレベル・アグリーメント(SLA)の管理に責任があります。

### 第3問

サービスマネジメントのイニシアティブ全体の一部としてサービスの可用性を管理することは、効率的サービスデリバリーにとって重要です。

サービスの可用性を管理する背景の理由を説明するのは、次のどれですか？

- A. ほとんどのサービス・プロバイダは顧客とのサービスレベル・アグリーメント(SLA)を持っており、可用性は保証されている。
  - B. アウトソーシングは今日のITにとって今やより有効な選択肢であるため、サービスの可用性はアウトソーサの能力に委ねられている。
  - C. サービスマネジメントのツールはリアル・タイムのパフォーマンス情報を提供するため、可用性を管理することには異論がある。
  - D. コーポレートのゴールを満たすために、ビジネスはよりITへと依存しており、従って期待される可用性に到達することは必須である。
- 
- A. 不正解。SLAが公式、非公式にかかわらず、ITはビジネスのゴールを満たすためにサービスをデリバリーしなければいけません。
  - B. 不正解。サービスがアウトソースされていても、ビジネスのニーズを満たすことと同様に、サービスの可用性を管理することは重要です。
  - C. 不正解。ITがより多くのデータを収集できるからといって、収集されるべきであることも、全て価値があることも意味しません。可用性の管理はリアル・タイムのデータのインプットより、多くのことを要求します。
  - D. 正解。ITとビジネスの関係は今まで以上に重要です。そしてビジネスにとってそのゴールを維持するために、サービスは合意されたサービスレベルを満たすよう、デリバリーされなければいけません。

### 第4問

サービスデスクの活動ではないのはどれですか？

- A. 一時的修正を適用すること。
  - B. インシデントを登録すること。
  - C. インシデントを既知のエラーに関連付けること。
  - D. 問題を解決すること。
- 
- A. 不正解。問題管理はサービスデスクに、インシデントに対する一時的修正を供給することができます。例：PCのリブート。
  - B. 不正解。サービスデスクは全てのインシデントを登録します。
  - C. 不正解。サービスデスクはインシデントを既知のエラーに関連付けることにより、インシデントを解決しようとします。
  - D. 正解。問題を解決することは、問題管理のタスクであり、サービスデスクのタスクではありません。

## 第5問

インシデント管理において、技術的専門家の付加的な利用を何と呼びますか？

- A. 機能的エスカレーション
- B. インシデント分類
- C. 問題の分析
- D. インシデントの解決と復旧

- A. 正解。技術的により熟練した人を巻き込むことを、機能的エスカレーションと呼びます。
- B. 不正解。インシデントの分類はサービスデスクのスタッフまたはインシデント管理のスタッフが行います。
- C. 不正解。問題の分析は問題管理のスタッフが行います。
- D. 不正解。インシデントの解決と復旧はサービスデスクのスタッフないしは、インシデント管理のスタッフによってなされます。

## 第6問

リリース管理プロセスを確立する際、**最初の**活動は何ですか？

- A. コミュニケーション、準備とトレーニング
- B. リリース計画の実施
- C. 設計と構築、および構成
- D. リリース・ポリシーの確立

- A. 不正解。コミュニケーション、準備とトレーニングは、プロセスを実装する間になされます。
- B. 不正解。リリースの計画は、プロセスが実装され、運用できるようになった後に行う活動です。
- C. 不正解。リリースの設計、構築、および構成は、プロセスが実装され、運用できるようになった後に行います。
- D. 正解。プロセスのポリシー確立は、プロセスを確立する際の最初の活動です。

## 第7問

ITサービス継続性管理の責任では**ない**活動はどれですか？

- A. リスクの分析
- B. 復旧シナリオの設計
- C. 重大なインシデントのインパクト分析
- D. 復旧対策のテスト

- A. 不正解。リスク分析はITサービス継続性管理の一部です。
- B. 不正解。復旧シナリオの設計はITサービス継続性管理の一部です。
- C. 正解。重大なインシデントのインパクト分析はインシデント管理の一部です。
- D. 不正解。復旧オプションのテストはITサービス継続性管理の一部です。

## 第8問

キャパシティ・マネージャが、CPUが日中に過負荷とならないよう、ある活動が夜間に実施可能かどうか、アプリケーションのユーザに質問します。

これはキャパシティ管理プロセスのどの部分に相当していますか？

- A. アプリケーション管理
  - B. アプリケーション・サイジング
  - C. 需要管理
  - D. モデル化
- A. 不正解。アプリケーション管理は、組織によって利用されるアプリケーションの維持とサポートを行う、日々の活動です。
- B. 不正解。アプリケーション・サイジングは、新規ないしは変更されたアプリケーションをサポートするために、要求されるキャパシティを決定するために利用されます。
- C. 正解。需要管理は顧客のキャパシティのニーズを判断することと、ITサービスが利用可能な時間帯に最良のパフォーマンスをデリバリするために、利用可能なキャパシティの使用を管理することに利用されます。
- D. 不正解。モデル化は将来のキャパシティのニーズをサポートするために、要求されるキャパシティを決定することに利用されます。

## 第9問

問題の診断が成功すれば、既知のエラーにたどり着きます。この既知のエラーに基づき、変更要求(RFC)が提起される場合があります。

いつ既知のエラーをクローズさせることができますか？

- A. 変更のレビューが満足のいく結果を導いたとき。
  - B. 既知のエラーに関連するインシデントがもはや発生しないとき。
  - C. RFCが変更管理に伴い記録されたとき。
  - D. RFCが変更諮問委員会(CAB)に許可されたとき。
- A. 正解。変更の実装が成功し、問題が解決されると、既知のエラーをクローズすることができます。
- B. 不正解。これは問題が解決されたことを示しません。変更の実装が成功した後のみ、既知のエラーがクローズできます。
- C. 不正解。変更管理に伴い、RFCが記録されたとき、問題はまだ解決されていません。変更の実装が成功した後のみ、既知のエラーがクローズできます。
- D. 不正解。RFCが変更諮問委員会(CAB)に認可されたとき、問題はまだ解決されていません。変更の実装が成功した後のみ、既知のエラーがクローズできます。

## 第 10 問

X社ではITインフラストラクチャの特定のコンポーネントが修正されました。これは他のコンポーネントに影響する場合があります。

これらの影響に正しい見解を提供するために、設けられるべきプロセスは何ですか？

- A. 可用性管理
  - B. キャパシティ管理
  - C. 変更管理
  - D. 構成管理
- A. 不正解。可用性管理はITサービスの可用性に責任があります。
- B. 不正解。キャパシティ管理は適時適切なキャパシティに対し戦略的責任があります。
- C. 不正解。変更管理は変更の計画と実装に責任があるプロセスです。
- D. 正解。構成管理はITインフラストラクチャとそのコンポーネントおよびそれらの関係に関する情報を提供する責任があります。変更のインパクト評価を手助けするために、構成管理には適切なレベルの詳細さがなければなりません。

## 第 11 問

ITサービス継続性管理では、大災害の間や後にサービスがデリバリされることを確実にするため、様々な予防的対策が取られています。非常用電源を設置することも一例です。

次のどのプロセスにおいて、この種の対策に着手する場合がありますか？

- A. 可用性管理
  - B. キャパシティ管理
  - C. 変更管理
  - D. インシデント管理
- A. 正解。ITサービスの可用性に対し、可用性管理は通常の状態下でのサービスデリバリを確実にするために、一定の対策をとることができます。それらの1つは非常用電源の設置を開始することです。
- B. 不正解。キャパシティ管理は適時適切なキャパシティに対し戦略的責任があり、非常用電源を利用可能にすることにはありません。
- C. 不正解。変更管理はそれが変更であれば、非常用電源設備を据え付けることに責任がありますが、これらの対策を開始する責任はありません。
- D. 不正解。インシデント管理はできるだけ早くインシデントを解決することに責任があります。予防的対策をとることは、インシデント管理のタスクではありません。

## 第 12 問

導入後のレビュー(PIR)が開催されなければならないのはいつですか？

- A. 毎変更後
  - B. 変更要求を提出した人が要求した時
  - C. 非常時の変更の場合
  - D. 変更実施後同じタイプの別のインシデントが再発する場合
- A. 正解。PIRは毎変更後開催するべきです。  
B. 不正解。PIRは提出者が要求しているときだけでなく、毎変更後開催するべきです。  
C. 不正解。PIRは非常時の変更の場合だけでなく、毎変更後開催するべきです。  
D. 不正解。PIRは変更実施後別のインシデントが発生する場合だけでなく、毎変更後開催するべきです。

## 第 13 問

インシデント管理の第一ステップは何ですか？

- A. 検知と記録
  - B. カテゴリの決定
  - C. 優先度の決定
  - D. 初期サポート
- A. 正解。インシデントの検知と記録は、インシデント管理プロセスの第一ステップです。  
B. 不正解。インシデントのカテゴリの決定は、インシデント管理プロセスのステップですが、これはインシデントが検知され、記録された後に行われます。  
C. 不正解。優先度の決定はインシデント管理プロセスのステップですが、これはインシデントが検知され記録された後に行われます。  
D. 不正解。初期サポートはインシデント管理プロセスのステップですが、これはインシデントが検知され記録された後に行われます。

## 第 14 問

サービスデスクでイベントが記録されたとき、おおよその順番でプロセスは実行されますか？

- A. 構成管理、インシデント管理、変更管理、リリース管理
  - B. インシデント管理、変更管理、問題管理、リリース管理
  - C. インシデント管理、問題管理、変更管理、リリース管理
  - D. 問題管理、構成管理、リリース管理、変更管理
- A. 不正解。サービス障害への対応は構成管理で始まるのではなく、正式にはインシデント管理プロセスにおいて記録されます。  
B. 不正解。問題管理による根本原因の発見は、通常は変更を提出する前に行われます。  
C. 正解。  
D. 不正解。変更管理はいかなる変更も、リリース管理による実装の前に、評価し許可をします。

## 第 15 問

サービスデリバリとそのセキュリティ管理との関係に関する合意は、どこに記録されますか？

- A. キャパシティ計画の中
  - B. 構成管理データベース(CMDB)の中
  - C. 確定版ソフトウェア保管庫(DSL)の中
  - D. サービスレベル・アグリーメント(SLA)の中
- A. 不正解。キャパシティ計画は（将来の）キャパシティのニーズを記述します。
- B. 不正解。アグリーメントは構成管理データベース(CMDB)の中には記録されません。CMDBには全ITコンポーネント、構成アイテム(CI)、およびそれらの関係が記録されます。
- C. 不正解。確定版ソフトウェア保管庫(DSL)は許可されたソフトウェア・アイテムのみを格納します。
- D. 正解。顧客とのアグリーメントはサービスレベル・アグリーメント(SLA)に記録されます。

## 第 16 問

サービスカタログに関する次の記述で、正しいのはどれですか？

- A. それはサービスレベル・アグリーメント(SLA)の代わりに利用可能です。
  - B. それはITマネジメント組織により供給される、全てのサービスを記述します。
  - C. それはサービスレベル・アグリーメント(SLA)にも含まれるサービスのみを記述します。
  - D. それはサービスレベル・アグリーメント(SLA)を作成するためには必要ではありません。
- A. 不正解。サービスレベル・アグリーメント(SLA)は特定のITサービスに対する、交渉されたサービスのレベルを記述します。サービスカタログはサービスレベルの記述を伴わず、IT組織が提供できる全てのITサービスを記述します。
- B. 正解。サービスカタログは、IT組織が提供できる全てのITサービスを記述します。
- C. 不正解。サービスカタログはサービスレベル・アグリーメント(SLA)に含まれるより、多くのサービスを保持できます。
- D. 不正解。サービスカタログはIT組織が提供できる全てのサービスを記述するとともに、サービスレベル・アグリーメント(SLA)を作成する際に使用されるべきものです。

## 第 17 問

承認された変更はどこで発表されますか？

- A. 変更諮問委員会(CAB)
- B. 構成管理データベース(CMDB)
- C. 将来的な変更スケジュール(FSC)
- D. サービス改善プログラム(SIP)

- A. 不正解。変更諮問委員会(CAB)は、変更と変更要求に関して決定を行う人たちのグループです。
- B. 不正解。CMDBはITインフラストラクチャの全コンポーネントとそれらの関係を登録するために利用されます。
- C. 正解。将来的な変更スケジュール(FSC)において、全ての承認され、計画された変更は発表されます。
- D. 不正解。サービス改善プログラム(SIP)はITサービスを改善するために、サービスレベル管理によって利用されます。

## 第 18 問

確定版ソフトウェア保管庫(DSL)の中身に関する説明で最も適しているのは、次のどれですか？

- A. インフラストラクチャ上で使用される全ソフトウェアの許可されたバージョン
- B. 全稼働環境のソフトウェア・プログラムのコピー
- C. 必要とされる全ソフトウェア・バージョンのコピー
- D. ユーザの受け入れテストを待つソフトウェア

- A. 正解。ITインフラストラクチャで使用される、ソフトウェアの許可されたバージョンのみ、DSLに保管されます。
- B. 不正解。DSLには許可されたソフトウェアのコピーのみが入ります。稼働環境のソフトウェアは定義上許可されている必要性はありません。
- C. 不正解。DSLにはすでに利用されている許可されたソフトウェアのコピー（マスタ・コピー）のみが入ります。
- D. 不正解。DSLにはユーザの受け入れを待つソフトウェアは入りません。

## 第19問

ユーザから報告されたサービスの中断を分類するタスクは、どのプロセスにありますか？

- A. 変更管理
- B. インシデント管理
- C. 問題管理
- D. サービスレベル管理

- A. 不正解。変更管理は変更要求を分類し、変更を計画および実装する責任があります。
- B. 正解。サービスの中断は、ユーザがサービスデスクに報告するインシデントです。サービスデスクは中断を管理するために、インシデント管理プロセスに従事します。
- C. 不正解。問題管理は問題に責任があります。サービスの中断はインシデントなので、インシデント管理の責任です。
- D. 不正解。サービスレベル管理はサービスレベル・アグリーメント(SLA)を管理する責任があります。

## 第20問

あるスーパーのキャッシュ・レジスターでは、毎日午後4時から6時の間、ネットワークの中断を経験しています。

これらの困難を説明する責任は、どのプロセスにありますか？

- A. 可用性管理
- B. キャパシティ管理
- C. 変更管理
- D. 問題管理

- A. 不正解。可用性管理は、問題や中断に対してではなく、ITサービスの可用性に戦略的責任があります。
- B. 不正解。キャパシティ管理は、問題や中断に対してではなく、適時適切なキャパシティに対し戦略的責任があります。
- C. 不正解。変更管理は、問題や中断に対してではなく、変更の実装に責任があります。
- D. 正解。問題管理は問題を解決する責任があります。これらのインシデントは日々発生し、問題に関係付けられます。

## 第 21 問

変更要求(RFC)に対し、軽微、深刻/重要、重大といったカテゴリを決定する際、変更管理によって利用される基準は何ですか？

- A. 内容
  - B. インパクト
  - C. 優先度
  - D. 緊急度
- A. 不正解。変更要求の内容は変更自体の記述です。
- B. 正解。インパクトは変更要求をカテゴリ化するために使用されます。インパクトは変更を実装するために、金銭、時間、キャパシティといった点でどの程度のリソースを必要とするか決定します
- C. 不正解。優先度はインパクトと緊急度に基づきます。
- D. 不正解。緊急度はいかに速く変更が実装されるべきかを示します。

## 第 22 問

構成管理データベース(CMDB)から直接答えることのできないものは、次の質問のどれですか？

- A. 何のインシデントや問題がこのPCにあるのか？
  - B. 特定のサービスはどの構成アイテム(CI)から成り立っているのか？
  - C. X部門のスタッフのどのメンバがY部門に異動したのか？
  - D. どの変更要求(RFC)が特定のサーバに対して提出されたのか？
- A. 不正解。インシデントや問題は構成アイテム(CI)に関係付けられ、CMDBに登録されます。
- B. 不正解。構成アイテム(CI)間の関係は、CMDBに登録されます。
- C. 正解。職員は人事部門によりトラッキングされ、この情報は直接CMDBの一部とはならないでしょう。
- D. 不正解。変更要求(RFC)はCMDBに登録されます。変更が実装されると、CMDBは更新されます。

## 第 23 問

組織は、どのようにしてサービスレベル管理プロセスの有効性を判断することができますか？

- A. サプライヤとの契約をチェックすることにより
  - B. サービスレベルを定義することにより
  - C. 顧客満足を測定することにより
  - D. 全インシデントへの報告により
- A. 不正解。サプライヤとの契約はサービスレベル管理プロセスの一部ですが、契約をチェックすることでプロセスの有効性を判断することはできません。
- B. 不正解。サービスレベルを定義することは、ITサービスをデリバリするために重要ですが、サービスレベル管理プロセスの有効性に関する情報は提供しません。
- C. 正解。顧客満足はサービスレベル管理の有効性を判断する最も重要な側面です。
- D. 不正解。全インシデントへの報告によりインシデント管理の有効性は判断できますが、サービスレベル管理の有効性はできません。

## 第24問

サービスデスクの活動ではないものは、次のどれですか？

- A. インシデントの検知と記録
- B. インシデントの調査と診断
- C. サービス要求の管理
- D. 所有、監視、トラッキング、コミュニケーション

- A. 不正解。これらの活動はサービスデスクの責任です。
- B. 正解。これらの活動はインシデント管理プロセスの責任です。
- C. 不正解。これらの活動はサービスデスクの責任です。
- D. 不正解。これらの活動はサービスデスクの責任です。

## 第25問

サービスの設計、開発、デリバリーに対し、可用性管理の方法論やテクニックを適用することにより、そのサービスの可用性全体に影響しないものは、次のどれですか？

- A. コンポーネントへの支出
- B. インフラストラクチャの対障害弾力性
- C. サポート組織やサプライヤによるメンテナンスの品質
- D. コンポーネントの信頼性

- A. 正解。コンポーネントのコストは、サービスの可用性全体に直接影響しません。
- B. 不正解。対障害弾力性は信頼性の一部であり、サービスの可用性全体に直接影響します。
- C. 不正解。サービス性と保守性は、サービスの可用性全体に直接影響します。
- D. 不正解。コンポーネントの信頼性は、サービスの可用性全体に直接影響します。

## 第26問

問題管理の活動ではないものは、次のどれですか？

- A. 第三者のサプライヤとの関係維持
- B. 傾向分析を通じたインシデントのプロアクティブな予防
- C. 受容された時間枠を超過したインシデントの責任をとること
- D. サービスの可用性が合意されたレベルを確実に満足するよう、可用性管理と密接に働くこと

- A. 不正解。これは問題管理により実施される活動の一部です。
- B. 不正解。これは問題管理により実施される活動の一部です。
- C. 正解。問題管理はリソースとしてインシデント管理をサポートするよう頼まれるかもしれませんが、オーナーシップはとりません。
- D. 不正解。これは問題管理により実施される活動の一部です。

## 第 27 問

キャパシティ管理の活動は、次のどれですか？

- A. 保守性
- B. リソース管理
- C. セキュリティ
- D. サービス性

- A. 不正解。保守性は可用性管理の活動です。
- B. 正解。リソース管理はキャパシティ管理の活動です。
- C. 不正解。セキュリティはセキュリティ管理の責任です。
- D. 不正解。サービス性は可用性管理の活動です。

## 第 28 問

インシデント管理のゴールは何ですか？

- A. 将来のサービスの中断について顧客およびユーザとコミュニケーションすること
- B. 新規のインシデントを既知のエラーと照合すること
- C. サービスをできるだけ速く回復すること
- D. 既知のエラーのデータベース(KEDB)の中で、問題を追跡すること

- A. 不正解。コミュニケーションはインシデント管理をサポートするため、サービスデスクにより実施されるタスクないしは活動ですが、インシデント管理のゴールではありません。
- B. 不正解。インシデントのマッチングはインシデント管理のゴールではありません。それはインシデント管理の活動の一部です。
- C. 正解。これはインシデント管理のゴールです。
- D. 不正解。これは問題管理の責任です。

## 第 29 問

セキュリティ管理プロセスにおける完全性の基本コンセプトを記述しているのは、次のどれですか？

- A. いつでもデータにアクセスすること
- B. 許可されていないアクセスと利用に対するデータの保護
- C. データの正確性を検証する能力
- D. データの正確性

- A. 不正解。データのアクセシビリティは、「完全性」のコンセプトが意味する、データが正確であることを意味しません。
- B. 不正解。データの保護は「セキュリティ」と呼ばれます。
- C. 不正解。データの正確性を検証する能力ではなく、正確性自体が「完全性」と呼ばれます。
- D. 正解。データの正確性は、「完全性」と呼ばれます。

### 第30問

構成管理のどの活動において、監査が定期的実施されますか？

- A. 識別
- B. 計画
- C. ステータスの監視
- D. 検証

- A. 不正解。識別は構成管理データベース(CMDB)に追加されなければならない、ITコンポーネントの識別に関することです。
- B. 不正解。計画はプロセスの役割と責任を計画し、構成管理データベース(CMDB)の範囲とレベルを決定することを意味します。
- C. 不正解。ITコンポーネントのステータスをモニタリングすることは、「稼働中」、「修理」、「メンテナンス」、「アーカイブ」といったコンポーネントのステータスを見て、報告することを意味します。
- D. 正解。検証の一部は、構成管理データベース(CMDB)が最新で正確かどうか判断するために、レビューと監査を行っています。

### 第31問

顧客向けに設計したサービスレベル・レポートにおいて、在ると期待されない視点はどれですか？

- A. サービスデスクのスタッフの平均稼働率
- B. 実現された可用性のレベルと期間ごとの非可用時間
- C. 目標内で解決されたインシデントの割合
- D. 期間ごとの成功および切り戻された変更

- A. 正解。サービスデスクのスタッフの平均稼働率は、サービスレベル・レポートではなく、サービスデスク・レポートで報告されます。
- B. 不正解。サービスレベル・レポートはある時間枠における、実現された可用性を含みます。
- C. 不正解。目標内で解決されたインシデントの割合は、サービスレベル・レポートの一部です。
- D. 不正解。成功および切り戻された変更は、サービスレベル・レポートの一部です。

### 第 32 問

キャパシティ管理と最も直接的関係もしくは相互依存性があるのは、次のどのプロセスですか？

- A. 可用性管理
- B. 構成管理
- C. ITサービス継続性管理
- D. リリース管理

- A. 正解。キャパシティと可用性管理は共通のゴールを共有し相互補完します。理想的には可用性とキャパシティ管理は多くの相互依存があるよう整合するべきです。多くの依存が理由で、2つのプロセスは効果的に連携する必要があります。それらは両方ともコンポーネント障害インパクト分析(CFIA)や故障樹分析(FTA)など、多くの同じツールとテクニックを使用します。
- B. 不正解。構成管理情報はキャパシティに有用であり、概念的にはCDBはCMDBの部分集合です。最も強い関係は、その相互依存により、可用性とにあります。
- C. 不正解。これは価値のあるインターフェースですが、ITサービスの継続性はその設計活動を実施するために、より可用性管理に頼っており、キャパシティはそのキャパシティ要件のためです。最も強い関係は、その相互依存により、可用性とにあります。
- D. 不正解。リリース管理は投入オプション/計画の決定において、キャパシティと互いに影響し合いますが、キャパシティとの最も直接的関係は、その相互依存により、可用性にあります。

### 第 33 問

プロセスはあらかじめ定義されたゴールに向かう、論理的に首尾一貫した一連の活動です。

プロセス・オーナーは何に責任がありますか？

- A. プロセスを記述すること
- B. プロセスを実装すること
- C. プロセス・レポートを提供すること
- D. プロセスを設立すること

- A. 正解。プロセス・オーナーの主要な責任は、合目的性を確実にすることと、プロセスの範囲(記述)を提供することです。
- B. 不正解。プロセス・オーナーの主要な責任は、プロセスに関しハイレベルな見通しを持ち、プロセスの「よい状態」に最終的責任を持つことです。プロセスの実装は、プロセス・マネージャやプロセス・チームの責任です。
- C. 不正解。プロセスの報告は、プロセス・マネージャの責任です。
- D. 不正解。プロセス・オーナーの主要な責任は、運用の間プロセスに関しハイレベルな見通しを持つことです。プロセスを設立することは、プロセス・オーナーの指導下でのプロセス・マネージャの責任です。

### 第 34 問

電源障害によってITインフラストラクチャ全体が不能になりました。幸いにも、ITサービス継続性(ITSC)計画は利用可能です。

どの時点で危機管理チームに、ITSC計画を発動を依頼すべきですか？

- A. ITサービスが利用不可能となつてすぐ
  - B. 障害がサービスレベル・アグリーメント(SLA)に定義された目標を超えて続きそうなとき
  - C. インシデント・マネージャが必要と考えたとき
  - D. 故障が解決されるべき時間を超えたとき
- A. 不正解。ITSC計画はインシデントが起きた直後ではなく、あらかじめ定義された時間後に発動されます。
- B. 正解。ITSC計画はあらかじめ定義された時間後および、サービスレベル・アグリーメント(SLA)に定義された目標を満たすことができない時に発動されます。
- C. 不正解。ITSC計画はインシデント・マネージャの要請ではなく、あらかじめ定義された時間後に発動されます。
- D. 不正解。ITSC計画はあらかじめ定義された時間後および、サービスレベル・アグリーメント(SLA)に定義された目標を満たすことができない時に発動されます。障害を修理する時間が合意された最大の時間を超えた時、これはITサービス継続性計画を発動する直接的理由ではありません。

### 第 35 問

新しいワークステーションのリクエストを標準化するプロセスもしくは機能はどれですか？

- A. 変更管理
  - B. インシデント管理
  - C. サービスデスク
  - D. サービスレベル管理
- A. 正解。新しいワークステーションのリクエストは変更要求です。変更管理は全変更要求を管理し、それらに最も効率的な処理経路を割り当てます。この場合はサービス要求としてサービスデスクによって管理される、標準的な変更を作成することです。
- B. 不正解。新しいワークステーションのリクエストは変更要求です。インシデント管理はできるだけ早くインシデントを解決することに責任があります。
- C. 不正解。新しいワークステーションのリクエストは変更要求です。サービスデスクはユーザに対する最初の窓口です。
- D. 不正解。新しいワークステーションのリクエストは変更要求です。サービスレベル管理はサービスレベル・アグリーメント(SLA)を管理する責任があります。

### 第 36 問

サービスデスクの役割を最もよく記述しているのはどれですか？

- A. サービスデスクは合意されたITサービスが利用可能になることを確実にします
  - B. サービスデスクは電話要員が常に配置されることを確実にします
  - C. サービスデスクはユーザに対する単一窓口です
  - D. サービスデスクの最も重要なタスクは問題を調査することです
- A. 不正解。これは可用性管理の責任です。
- B. 不正解。サービスデスクで電話要員が常に配置されるよう確実にすることはもちろん重要ですが、サービスデスクの役割を最もよくは記述していません。
- C. 正解。ユーザに対する単一窓口であることはサービスデスクの主要な責任の一つです。
- D. 不正解。問題管理は問題の調査と解決に責任があります。

### 第 37 問

ITIL®を利用する利点は次のどれですか？

- A. 最終的にITサービスに対する請求が可能になります
  - B. ITサービスを取り巻く組織をより速く設立することができます
  - C. ITサービスの品質やコストをより効率的にコントロールすることができます
  - D. ユーザがITサービスを提供するIT組織に影響を及ぼすことができます
- A. 不正解。ITサービスを利用することに対する課金はITIL®を利用してもしなくても実施できます。
- B. 不正解。ITIL®を利用してIT組織を設立することは多くの利点がありますが、時間もかかりません。
- C. 正解。ITIL®を利用することにより、ITサービスは品質とコストの点でより効率的にコントロールできます。
- D. 不正解。IT組織に影響を及ぼすことはITIL®を利用してもしなくても実施できます。

### 第 38 問

変更管理において、変更要求(RFC)の受け入れから変更の完了までの間、多数の活動が行われます。

変更要求の受け入れ後**最初**に実施される活動はどれですか？

- A. 変更の構築とテスト
  - B. 変更の緊急度の決定
  - C. 変更の実装
  - D. 変更要求のスケジューリング
- A. 不正解。変更の構築とテストは分類がなされてから行われます。分類の一部は緊急度を決定することです。
- B. 正解。受け入れ後最初のステップは変更の緊急度を決定することです。
- C. 不正解。変更の実装は構築、テスト、スケジューリング実施後行われます。
- D. 不正解。変更要求のスケジューリングは分類がなされてから行われます。分類の一部は緊急度を決定することです。

### 第 39 問

構成管理データベース(CMDB)の文脈において「詳細レベル」という用語は何を意味しますか？

- A. データベース構造の深さ
- B. 構成アイテム(CI)の場所
- C. 保管される構成アイテム(CI)の量
- D. 異なった構成アイテム(CI)間の関係

- A. 正解。レベルは構成管理データベース(CMDB)の深さを意味します。
- B. 不正解。構成アイテム(CI)の場所は、それらの物理的場所です。
- C. 不正解。保管される構成アイテム(CI)の量は、構成管理データベース(CMDB)の中にある構成アイテム(CI)の総計です。
- D. 不正解。構成アイテム(CI)間の関係は、個々のCIの詳細とは別個です。

### 第 40 問

次のタスクのうち、プロアクティブな問題管理の一部はどれですか？

- A. 傾向の分析
- B. 問題を解決する変更の作成
- C. 既知のエラーの管理
- D. 頻繁に発生するエラーの登録

- A. 正解。傾向の分析はプロアクティブな問題管理の一部です。傾向の分析により問題管理は発生前にインシデント/問題を識別し、インシデント発生前に変更管理経由で適切な所に対策を実施することができます。
- B. 不正解。問題を解決する変更の作成はリアクティブであり、変更の管理は変更管理の責任です。
- C. 不正解。既知のエラーの管理は問題管理のタスクですが、プロアクティブなタスクではありません。
- D. 不正解。頻繁に発生するエラーの登録はインシデント管理/サービスデスクの一部です。

## 評価

### 模擬試験

以下の表は、この模擬試験の正解を示します。

番号	回答	点数	番号	回答	点数
1	C	1	21	B	1
2	B	1	22	C	1
3	D	1	23	C	1
4	D	1	24	B	1
5	A	1	25	A	1
6	D	1	26	C	1
7	C	1	27	B	1
8	C	1	28	C	1
9	A	1	29	D	1
10	D	1	30	D	1
11	A	1	31	A	1
12	A	1	32	A	1
13	A	1	33	A	1
14	C	1	34	B	1
15	D	1	35	A	1
16	B	1	36	C	1
17	C	1	37	C	1
18	A	1	38	B	1
19	B	1	39	A	1
20	D	1	40	A	1