CISA®試験問題
作成ガイド

（注）本書はガイドの翻訳であり試験問題は英語で作成することが必要です。

CISA試験問題作成ガイド

日本語訳に際しての謝辞

ISACAの各資格認定の試験問題は、世界の会員からの応募により作成されています。しかし、残念ながら、日本語を母国語とする会員からの問題応募は、過去は特定のケースに限られていました。東京支部は、「問題応募を会員にとってもっと身近なもの」とするため本文書の日本語訳を企画し、支部会員の有志の方々に協力をお願いしました。更に、これをテキストとした「試験問題開発ワークショップ」を実施しています。これらの活動は、全て参加メンバーの専門家としてのボランティア活動に支えられています。ここに、翻訳者並びに協力頂いた会員の指名を列記し、深く感謝の意を表する次第です。

翻訳　東京支部副会長兼理事　坂本 正徳 CISA, CISM, CGEIT, CRISC
協力　東京支部CRISC委員会委員長　田中 秀幸 CISA, CISM, CGEIT, CRISC

ISACA東京支部
2012-2013 会長兼理事　柴田　昭

Quality Statement:
This Work is translated into Japanese from the English language version of CISA Item Development Guide-2012 by the ISACA Tokyo Chapter with the permission of ISACA. The ISACA Tokyo Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.
品質について
本書は「CISA Item Development Guide-2012」を、ISACAの許可を得て東京支部が英語から日本語に翻訳したものです。翻訳の正確性および忠実性はISACA東京支部が責任を担います。

CISA試験問題作成ガイド

目　　次

CISA試験問題作成ガイド

CISA試験問題作成ガイドの目的

CISA試験問題開発ガイド（以下、「本ガイド」という）の目的は、CISA試験およびレビューマニュアルの品質を向上させる上で、試験問題作成者への支援を提供するものです。本ガイドでCISA試験問題の構成を十分説明することで、作成者が問題を作成・見直しにより習熟するよう支援を行ないます。

本ガイドを通じて試験問題作成の原則に留意して下さい。当該原則を適用することで、作成・提出した問題が承認される機会が増えることとなるでしょう。

CISA試験の構成

ISACAおよびCISA認定委員会では、情報システム監査の専門家にとって最新で必要なタスクおよび知識を決定するため、CISAの職務領域の分析を定期的に実施しています。当該分析の結果は、CISA試験およびCISAレビューマニュアルの青写真として提供されます。試験問題は、CISAの職務領域分析（AppendixA CISA職務領域）による確立されたプロセスと定義された内容の知識を、受験者に問うよう記述されていなければなりません。

試験問題作成の品質

問題を作成する際に最初に考えなければならないのは、対象者あるいはCISAの受験者です。試験問題は、望ましいCISAの受験者に求められる適切な経験レベルに応じて作成されなければなりません。当該経験レベルについては、CISA認定委員会では、以下のように定義しています。*「CISAはチームの一員として、特定の役割を独立して担い、必要なところでの指示を探索および実施できると共にその他領域では積極的であるという能力を持つべきである。CISAは、業務を計画し、ビジネス環境に存在する重要な関連課題を判断し、役割や要件を効果的に管理すると共に、必要に応じて計画を策定する、といった適切な知識と経験を持つべきである。CISAは一般的には、より熟練したスタッフメンバーあるいは管理者からの方向性を得て、技術の専門家からは複雑な技術的課題への支援を得て、業務を推進するものである」*

情報システム監査及び統制はグローバルに展開されている職業であり、グローバルな位置や環境を反映していないような個人の見識や経験といったものでないかどうか、試験問題を作成する際には、考慮しなければいけません。試験およびCISA試験問題は、国際的な情報システム監査および統制のコミュニティのために策定されなければならず、試験問題もグローバルで受け入れられている手法に柔軟に対応する必要があります。

CISA試験問題作成ガイド

複数選択肢問題

CISA試験問題は、複数の選択肢から構成されます。複数の選択肢は最も一般的に使用される認定試験のテスト設問のタイプです。

複数選択肢問題は1つの設問と4つの選択肢で構成されます。

設問:
設問は、評価しようとする知識に関連する状況あるいは背景を記述した導入の文章あるいは質問です。設問は、質問型であったり不完全な文章として記述されます。

選択肢:
回答の選択肢は導入の文章を完結させるもの、あるいは質問へ回答する形であり、1つの正答(Key)と3つの不正解あるいは誤答で構成されます。

正答:
正答は最新の実務を反映するものでなければいけません。正答は明示的に唯一、正しいものとして記述する場合と、相対的に提供された選択肢のなかで「最もそうであると思われる」ものを記述する場合があります。

誤答:
誤答は不正解な選択肢であるが、妥当で充分な知識を持っていない受験者が選択してしまうような内容とすべきものです。

試験問題作成の手順

手順1　CISA職務領域の中からトピックを選択します。試験問題は特定のタスクを実行するのに必要な知識を試すように記述されている必要があります。試験問題は、単一のトピックあるいは知識項目に焦点を当てるべきです。知識項目から記述された試験問題はより高い品質になると共に、実務に基づいた設問となる可能性が高いものです。Appendix AのCISA職務領域にあるタスクと知識の記述を参照して下さい。

トピックを選択した後は、以下の手順に従います。試験問題を作成する際には、ガイドラインとして試験問題作成の原則を参照し、AppendixBの試験問題作成チェックリストでレビューを行って下さい。

手順2　問題の設問と(選択肢Aに)正答を記述します。

手順3　もっともらしく見える誤答を作成します。誤答は単語や語句だけの記述をすべきではありません。誤答は経験が乏しい専門家にとっては正しい選択肢のように見えるようなものであるべきでしょう。試験問題作成のなかで、作者にとってよい誤答を作ることが最も難しい作業となります。当該作成に際して困難な場合は、経験者に相談すると良いでしょう。また経験の乏しいIT専門家が正しい回答と考えがちなものが何かを考えてみましょう。これらの経験の乏しい専門化は最良の誤答を生むことでしょう。

手順4　正答となる選択肢が何故正しく、各誤答が何故誤りであるかの説明を記入します。誤答が単に誤りだから、という書き方ではいけません。

手順5　参照したリソースを記入します。該当する参照先はISACAのウェブサイトにあります。– http://www.isaca.org/knowledge-center.

手順6　AppendixBの試験問題作成チェックリストを用いてレビューを行います。

手順7　作成した試験問題を仲間や同僚にレビュー、批評してもらいましょう。

試験問題作成に際しての一般原則

しなければならないこと:

1. 肯定的な文脈の試験問題を作成すること。否定的な文章は、それだけで書き直しが要求され、自動的に返却となる。
2. 各試験問題は、ひとつのコンセプトあるいは知識についてのみ問うこと。知識項目は当該目的で策定されている。対象となる知識項目はAppendixAの実務領域を参照のこと。
3. 設問および選択肢は共に関連性があること。例えば「最良の統制となりうるのは次のうちどれか」という設問であれば、全ての選択肢は統制についての記述とならねばならない。
4. 不要な文章や専門用語の使用を避け、可能な限り設問および選択肢は短くすること。設問に答える前の受験生に過大な情報を提供してコンセプトや理論を教えることがないようにしなければならない。これは試験であり授業ではない。
5. 正答や誤答ではなく、設問には一般的な単語あるいは語句を使用すること。
6. 全ての選択肢はだいたい同じ長さおよび形式に揃えて記述する。ITの知識や経験が乏しくとも上手な受験者は、最も短いあるいは選択肢の文を選んだり、正しいと思われる回答を選ぶことで正答を導くことになる。
7. 選択肢を作成する際には、問題の設問と文法的に一貫性を持たせて並列な文法形式とする。例えば正答が動詞で始まり「ing」で終わるのであれば、全ての誤答も動詞で始まり「ing」で終わるように作らなければならない。
8. 設問および選択肢には専門的に認められた言葉、あるいは専門用語を用いること。

してはいけないこと:

1. 試験問題の正答な単語あるいは語句を設問に入れないこと。経験豊富な受験者は、このような正答が設問にないかを探し回るからである。
2. 試験問題には、「frequently」「often」「common」「rarely」といった用語は、試験問題に主観的な概念をもたらすので使用してはならない。問題が主観的であると正答以外の選択肢も正答になってしまう可能性がある。試験問題が主観的であることは最も一般的な作成者への返却理由であり、試験において試されるものではない。
3. 設問には、「always」「never」あるいは「all」といった可能性を狭めて受験生に誤答の発見を容易にするような用語は使用してはならない。
4. 「least」「not」あるいは「except」といった用語は否定的であり、受験生に正解や望ましい選択を求めずに不正解や最低限の選択を求める。否定的な語句のテスト設問は良いものではなく、用いてはならない。

5. 「he」「she」「his」あるいは「her」といった性別の代名詞を使用しない。
6. 選択肢に「all of the above」あるいは「none of the above」がある試験問題は作成者に返却される。受験生はこのような選択肢正解であることが非常に稀であることを周知しており、よい誤答とはならない。
7. ISACAはいかなるベンダー製品も支持するものではなく、ベンダー固有の製品に関する知識を問う設問は作成者に返却される。
8. 以下のような主観的なコンセプトを試すことは避ける。
    a. 特定の国際的あるいは各国の法規制
    b. グローバルあるいは全ての業界では適用されない文化や業界の問題に特化した情報
    c. 組織に特化した役割や責任

    CISA試験はグローバルで全ての業界で運営されていること、試されるコンセプトはグローバルおよび全ての業界で承認され認識された実務であることを忘れてはならない。

試験問題の実例(EXAMPLES)

試験問題には、質問型、不完全文章型、あるいはシナリオ型があります。

質問型:

設問(Stem): Which of the following concerns would BEST be addressed by the comparison of production application systems source code with an archive copy?

選択肢(Options):

A. File maintenance errors
B. Unauthorized modifications
C. Software version currency
D. Documentation discrepancies

注）設問は質問型である。

不完全型:

設問(Stem): The comparison of production application systems source code with an archive copy would BEST address:

選択肢(Options):

A. file maintenance errors.
B. unauthorized modifications.
C. software version currency.
D. documentation discrepancies.

注）当該設問への対応は文章を完結させるように続き、回答は設問で始まる文を完成させるものである。

最初に質問型で試験問題をドラフトするのは賢明です。より円滑で語句を繰返さないので、そこから不完全文章型に修正します。

シナリオ型

シナリオ型の設問を作成する際には多くの考慮が必要となります。
当該試験問題は、以下の問題についての導入情報（あるいはシナリオ）から構成します。

- o導入情報に関連して2問から5問の設問を設定します。
- o題材は特定の領域によるもので、関連および実践なければならず、受験生に仮定を強要することなく正答を導ける必要な情報を全て含まなければいけません。
- o関係する設問は順序立てて設定されているべきで、論理的な進行に従います。
- o各設問は他の設問とは独立して作成されているべきであり、ひとつ誤答したことが他の問題の回答に影響を及ぼしてはいけません。注意を払うのは、ひとつの設問が他の設問の正答を導くようになってはいけないことです。
- o新しい情報が関連する設問のなかにあってはいけません。設問への回答に必要な全ての情報はシナリオあるいは導入情報のなかに存在すべきものです。

最良のシナリオは業務上で生じた実際の状況が記述されたものです。また、法規制や役割と責任といったより主観的なコンセプトも、シナリオの中で記述すればよいものです。そこでは、法規制や特定の産業における組織の報告構造など、特定の要件を説明することができます。

試験問題を作成する際に避けなければならないこと

以下は、試験問題を作成する際に避けなければいけないことです。ガイドに掲載されているこれらの問題は決して試験用として承認されないことを念頭に置いて下さい。

例1:

設問(Stem): An IS auditor is reviewing an organization’s disaster recovery plan. Which of the following areas should the auditor review?

選択肢(Options):

A. Offsite data file storage
B. Fire fighting equipment
C. Backup UPS for the computer center
D. Access to the data center by backup staff

正答(Key):A

全ての選択肢は正答となり得ます。唯一の正答を選択し得る十分な情報が設問にはありません。情報システム監査人は、災害復旧計画をレビューする際には全ての選択肢にある事項を見なければなりません。

例2:

設問(Stem): A manager in the loan department of a financial institution performs unauthorized changes to the interest rate of several loans in the financial system. Which type of control could BEST have prevented this fraud?

選択肢(Options):

A. Functional access controls
B. Logging of changes to loan information
C. Senior management supervision
D. Change management controls

正答(Key):A

設問は職務の責任に関するものです。CISAの試験はグローバルになされますが、職務の責任は国や組織により定義が異なります。ある組織においては融資部のマネージャーがアクセスするかもしれません。

例3:

設問(Stem): Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job costing system. What is the BEST control to ensure that data entered into the job costing system is accurate?

選択肢(Options):

A. Reconciliation of total amounts by project.
B. Reasonableness of total amounts by project.
C. Validity checks, preventing entry of character data.
D. Display back of project detail after entry

正答(Key):A

情報システム監査人は当該質問に答えられるでしょうか。当該設問は情報システム監査人の概念を試すものでしょうか。情報システム監査人に必要とされる能力を問うものはありますが、これは境界的なコンセプトです。明確に情報システム監査人の能力を測るものであることが必要です。

CISA職務領域とは

CISAの職務領域とは、リスクおよび統制の領域で業務を遂行するIT専門家に関連するタスクと、これらのタスクを実行するのに必要知識を記載したものです。これらのタスクと知識はCISA試験の設問の基礎となるものです。CISA試験の目的は、タスクを実行するのに必要な知識を試すため、実務に基づいた設問を行うことです。CISA職務領域は、AppendixAに掲載されています。設問を作成する際には、ひとつの知識あるいは試験コンセプトのみ問うようにすることを忘れないで下さい。

CISA試験問題作成ガイド

種別化

全ての試験問題は領域が種別化されなければなりません。種別は、CISAのどのタスクおよび知識項目に最も関連しているかを示します。各種別では、2-3桁のタスクの番号および同様の知識の記述の番号が記載されます。種別はタスクと知識項目の前に記されます。試験問題を種別化する際には、AppendixAの「CISA職務領域」を参照して下さい。

試験問題の提出およびレビュープロセス

試験問題は、CISAitems@isaca.org に提出しなければなりません。全ての試験問題は、AppendixC – Item Construction Formの様式を使用し、英語で記載して提出する必要があります。しなければなりません。Item Construction Form内は、全項目に記載が必要です。空欄があればレビューされることなく返却されます。

*CISA Item Wrigting Application*を作成した首題の専門家は、CISA認定委員会が要請したCISA職務領域内のタスクおよび知識項目を連絡する電子メール（試験問題作成キャンペーン）を受け取ることになります。試験問題作成キャンペーンには、試験問題の提出に関する締切日も含まれます。

一次審査は、ISACAの事務局が、記載の完全性や「試験問題作成に際しての原則」への準拠について確認を行います。何か重大な欠陥があると判断された場合は、適切かつ建設的なフィードバックを付記して作成者へ返却されます。一次審査を通過した試験問題はCISA試験問題評価委員会(CISA Test Enhancement Subcommittee – TES)へ送られて試験問題プールに入れるべきかどうかの審査を行います。

評価委員会でレビューされた問題は、承認されるか返却されることになります。問題が作成者に返却される場合は、適切かつ建設的なフィードバックが付記されます。承認された場合には、当該試験問題はISACAが所有権を有するものとなり、作成者には2CPEの付与と共に謝礼金が支払われます。$100の謝礼金が重点領域で承認された各試験問題に授与され、重点領域以外で承認された各試験問題には$50が授与されます。

AppendixA

CISA職務領域 – 2011年6月以降

マーカーで記されたタスクと知識項目は、主観的な内容となることで、ひとつの正答を伴うグローバルに認識された設問を作成するのが難しくなりがちな項目です。試験問題作成者には、これらの主観的な領域を試すべく、シナリオ型の設問を作成されることをお勧めします。シナリオ型の設問では、作成者が主観的な情報および特別な背景を導入情報に含めることができるので、回答をする際に仮説を立てる必要がありません。例えば、組織の役割と責任について問う場合、組織の構成や特定の役割と責任をシナリオの中で定義することができます。複数の設問は、シナリオに含まれた情報を試すように作成されます。

また、知識項目の最後の数字は、これらの知識項目に対応する対応するタスクを表していることに注意して下さい。例えば、タスク1.1に記されたタスクを実施するためには、知識項目1.1, 1.2および1.6に記載された知識が個々に求められるものです。

ドメイン1 – 情報システム監査のプロセス: IT 監査基準に従い、組織における情報システムの保護および管理を支援するために、情報システム監査サービスを提供する。

タスク

1.1 主要な領域が含まれることを確実にするために、IT 監査基準に従って、リスクベースの IT 監査戦略を策定及び導入すること。
1.2 情報システムが保護され管理されているかどうかを判断するために特定の監査を計画し、組織にその評価を提供すること。
1.3 策定した監査目標を達成するために、IT 監査基準に従って監査を実施すること。
1.4 結果を伝えるとともに必要な場合は修正をもたらすために、主要な利害関係者に監査の発見事項の報告及び改善勧告を行うこと。
1.5 経営者によって適切な措置が時をとらえたやり方で取られていることを確認するために、フォローアップを実施すること、あるいは、状況報告書を作成すること。

知識項目

1.1 I SACA IT 監査と保証の基準、ガイドライン、及びツールと技法、職業倫理規定、その他の適用基準に関する知識[1.1, 1.2, 1.3, 1.4,1.5]
1.2 監査におけるリスクアセスメントの概念、ツール及び技法に関する知識[1.1, 1.2]
1.3 コントロール目標、及び情報システム関連のコントロールに関する知識[1.2, 1.3]
1.4 監査計画及び監査プロジェクト管理の技法（フォローアップを含む）に関する知識[1.2, 1.3, 1.5]
1.5 IT 関連を含む基本的な業務プロセス（例: 購買、給与、買掛金、売掛金プロセス）に関する知識[1.2, 1.3]
1.6 監査の範囲、監査証拠の収集と保存、及び監査の頻度に影響を与える、適用法令及び規制に関する知識[1.1, 1.2, 1.3, 1.4]
1.7 監査証拠の収集、保護、及び保存に使用される証拠収集技法（例: 観察、質問、検査、インタビュー、データ分析）に関する知識[1.3]
1.8 様々なサンプリング方法論に関する知識[1.2, 1.3]

1.9 報告及びコミュニケーションの技法（例：ファシリテーション、交渉、紛争解決、監査報告書の構成）に関する知識[1.4, 1.5]
1.10 監査品質保証システムとフレームワークに関する知識[1.3]

ドメイン2 - IT ガバナンスとマネジメント:目標を達成し、組織の戦略を支援摺るために必要とされるリーダーシップ、組織構造、およびプロセスを備えているという保証を提供する。

タスク

2.1 IT に関する意思決定、方向性、パフォーマンスが組織の戦略と目標を支援しているかどうかを判断するためにIT ガバナンスの構造の有効性を評価すること。
2.2 IT の組織構造及び人材（人事）管理が組織の戦略の目標を支援しているかどうかを判断するために、それらを評価すること。
2.3 IT 戦略（IT の方向性を含む）、戦略の策定、承認、導入、及び維持のプロセスが組織の戦略と目標に整合しているかどうかを判断するためにそれらを評価すること。
2.4 組織のIT 方針、基準、及び手順と、それらの開発、承認、導入、維持、及びモニタリングのプロセスがIT 戦略を支援し、法令及び規制要求事項を順守しているかどうかを判断するために、それらを評価すること。
2.5 品質管理システムが費用対効果の高い方法で、組織の戦略と目標を支援しているかどうかを判断するために、その妥当性を評価すること。
2.6 IT に関する管理とコントロールのモニタリング（例：継続的モニタリング、品質保証[QA]）が組織の方針、基準、及び手順を順守しているかどうかを判断するために、それらを評価すること。
2.7 IT 資源の投資、活用、割り当ての業務（優先順位決定基準を含む）が組織の戦略と目標に整合しているかどうかを判断するために、それらを評価すること。
2.8 IT に関する契約戦略と方針、及び契約管理業務が組織の戦略や目標を支援しているかどうかを判断するために、それらを評価すること。
2.9 組織のIT 関連リスクが適切に管理されているかどうかを判断するために、リスク管理業務を評価すること。
2.10 取締役と上級経営者がIT パフォーマンスについて十分かつ適時な報告を受けているかどうかを判断するために、モニタリングと保証の業務を評価すること。
2.11 IT の障害発生期間中に、重要な業務の運営を継続できるかどうか組織の能力を判断するために、組織の事業継続計画を評価すること。

知識項目

2.1 IT ガバナンス、マネジメント、セキュリティ、及びコントロールフレームワークと、それに関する基準、ガイドライン、及び業務の知識[2.1, 2.4, 2.6]
2.2 組織のためのIT の戦略、方針、基準、及び手順の目的と、それぞれの重要な要素に関する知識[2.3, 2.4]
2.3 IT に関連する組織の構造、役割、及び責任に関する知識[2.6, 2.7]
2.4 IT の戦略、方針、基準、及び手順の策定、導入、及び維持のプロセスに関する知識
2.5 組織の技術の方向性及びIT アーキテクチャと、それらが長期の戦略的方向性の設定に与える影響に関する知識[2.3]
2.6 組織に影響を与える 関連法、規制、及び業界標準に関する知識[2.4]
2.7 品質管理システムに関する知識[2.4, 2.5]
2.8 成熟度モデルの活用についての知識[2.6, 2.9, 2.10]
2.9 プロセス最適化技法に関する知識[2.5, 2.6, 2.7]
2.10 IT 資源の投資と配分（優先順位決定基準を含む）に関する知識（例：ポートフォリオ管理、価値管理、プロジェクト管理）[2.7]
2.11 IT サプライヤーの選定、契約管理、リレーションシップマネジメント、及びパフォーマンスモニタリングプロセス（第三者委託先との関係を含む）に関する知識[2.1, 2.3, 2.8]

2.12 企業リスク管理に関する知識[2.2, 2.4, 2.9]
2.13 IT パフォーマンスのモニタリングと報告の業務に関する知識（例：バランススコアカード、主要業績評価指標[KPI]）[2.6, 2.10]
2.14 事業継続計画の実行に使用されるIT 人材（人事）管理の業務に関する知識[2.2, 2.11]
2.15 事業継続計画（BCP）に関連するビジネスインパクト分析（BIA）に関する知識[2.11]
2.16 事業継続計画（BCP）の確立、維持及びBCP の検証方法に対する基準と手順に関する知識[2.11]

ドメイン3 – 情報システムの取得、開発および導入:情報システムの取得、開発、テスト、および導入の業務が組織の戦略と目標を満たしているという保証を提供する。

タスク

3.1 情報システムの調達、開発、保守、及びその後の廃棄への提案された投資が、ビジネス目標に合致しているかどうかを判断するために、そのビジネスケースを評価すること。
3.2 組織に対するリスクを管理しつつ、費用対効果の高い方法でビジネス要件が実現されるかどうかを判断するために、プロジェクト管理の業務とコントロールを評価すること。
3.3 プロジェクトが計画通りに進捗しているか、それが文書化によって適切にサポートされているか、及び状況報告が正確であるかを判断するためにレビューを実施すること。
3.4 組織の方針、基準、手順、及び適用可能な外部の要求事項を順守しているかどうかを判断するために、要件定義、調達、開発、及びテストの各フェーズにおける情報システムのコントロールを評価すること。
3.5 プロジェクトの成果物、コントロール、及び組織の要件が合致しているかどうかを判断するために、情報システムの導入及び本番への移行の準備状況を評価すること。
3.6 プロジェクトの成果物、コントロール、及び組織の要件が合致しているかどうかを判断するために、情報システムの導入後のレビューを実施すること。

知識項目

3.1 利益実現の業務（例: フィージビリティスタディ[実現可能性調査]、ビジネスケース、TCO[総所有コスト]、ROI[投資収益率]）に関する知識[3.1, 3.2]
3.2 プロジェクト管理のメカニズム（例: 運営委員会、プロジェクト監視委員会、プロジェクト管理室）に関する知識[3.2]
3.3 プロジェクト管理のコントロールフレームワーク、業務、及びツールに関する知識[3.2]
3.4 プロジェクトに適用されるリスク管理業務に関する知識[3.2, 3.3]
3.5 データ、アプリケーション、及び技術に関連するIT アーキテクチャ（例: 分散アプリケーション、Web ベースアプリケーション、Web サービス、n 層アプリケーション）に関する知識[3.1]
3.6 調達の業務（例: ベンダー評価、ベンダー管理、エスクロー）に関する知識[3.1, 3.5]
3.7 要件分析と要件管理の業務（例: 要件の検証、トレーサビリティ、ギャップ分析、脆弱性管理、セキュリティ要件）に関する知識[3.2, 3.5]
3.8 プロジェクトの成功基準とリスクに関する知識[3.2, 3.3]
3.9 トランザクションやデータの完全性、正確性、妥当性、及び承認を保証するコントロール目標と技法に関する知識[3.4]
3.10 システム開発手法とツール（例:アジャイル開発業務、プロトタイピング、ラピッドアプリケーション開発[RAD]、オブジェクト指向設計の技法）、及びそれらの長所、短所に関する知識[[3.2, 3.4]
3.11 情報システム開発に関連したテスト手法と業務に関する知識[3.4]
3.12 情報システムの開発に関連した、構成管理及びリリース管理に関する知識[3.4, 3.5]
3.13 システムの移行、インフラストラクチャの配置業務、データ変換のツール、技法、及び手順に関する知識[3.4, 3.5]

3.14 導入後のレビューの目的と業務（例：プロジェクト終了、コントロール導入、利益実現、パフォーマンス測定）に関する知識[3.6]

ドメイン4 - 情報システムの運用、保守およびサポート:情報システムの運用、保守およびサポートが、組織の戦略と目標を満たしているという保証を提供する。

タスク

4.1 組織目標との整合が継続して維持されているかどうかを判断するために、情報システムの定期的なレビューを実施すること。
4.2 社内及び外部のサービス提供者のサービスレベルが定義され管理されているかどうかを判断するために、サービスレベル管理業務を評価すること。
4.3 組織が期待するコントロールレベルがサービス提供者によって順守されているかどうかを判断するために、外部業者管理(third-party management) 業務を評価すること。
4.4 計画された、および緊急のプロセスが完了するまで管理されているかどうかを判断するために、運用及びエンドユーザーの手順を評価すること。
4.5 情報システムの保守プロセスが適切に管理され、継続して組織の目標を支援しているかどうかを判断するために、情報システムの保守プロセスを評価すること。
4.6 データベースの完全性と最適化を確認するために、データ管理業務を評価すること。
4.7 IT サービスが組織の目標に合致しているかどうかを判断するために、容量及び性能監視ツールと技法の有効性を評価すること。
4.8 インシデント、問題、エラーが適時に記録、分析、解決されているかどうかを判断するために、問題管理及びインシデント管理の業務を評価すること。
4.9 組織の本番環境に対する計画された、および緊急の変更が適切に管理され文書化されているかどうかを判断するために、変更管理、構成管理、及びリリース管理の業務を評価すること。
4.10 処理を再開するために必要な情報が利用可能かどうかを確認するために、バックアップ及びリストア対策の妥当性を評価すること。
4.11 災害発生時に組織の災害復旧計画に基づいてIT 処理能力の復旧が可能であるかどうかを判断するために、組織の災害復旧計画を評価すること。

知識項目

4.1 サービスレベル管理業務とサービスレベルアグリーメント(SLA) の構成要素に関する知識[4.2]
4.2 外部業者(third-party) が組織の内部統制に準拠しているかどうかをモニタリングする技法についての知識[4.3]
4.3 計画された、および緊急のプロセスを管理するための運用およびエンドユーザーの手順に関する知識[4.3]
4.4 ハードウェアとネットワークの構成要素、システムソフトウェア、及びデータベース管理システムに関連する技術と概念に関する知識[4.5, 4.6]
4.5 システムインタフェースの完全性を保証するためのコントロール技法に関する知識[4.5]
4.6 ソフトウェアのライセンス及びインベントリ業務に関する知識[4.5]
4.7 システム高信頼化のツールと技法（例: 耐障害ハードウェア、単一障害点の排除、クラスタリング） に関する知識[4.5]
4.8 データベース管理業務に関する知識[4.6]
4.9 システム容量計画及びそれに関連する監視ツールと技法に関する知識[4.7]
4.10 システム性能監視のプロセス、ツール、及び技法（例: ネットワーク解析、システム利用状況報告、負荷分散） に関する知識[4.7]
4.11問題管理及びインシデント管理業務（例: ヘルプデスク、エスカレーション手順、追跡管理）に関する知識[4.8]
4.12 本番システムやインフラストラクチャに対する計画された、および緊急の変更を管理するためのプロセス（例: 変更管理、構成管理、リリース管理、パッチ管理の業務） に関する知

識[4.9]
4.13 データのバックアップ、保存、保守、保持、復元の業務に関する知識[4.10]
4.14 災害復旧に関する規制、法令、契約、及び保険の問題に関する知識[4.11]
4.15 災害復旧計画に関連するビジネスインパクト分析（BIA）に関する知識[4.11]
4.16 災害復旧計画の策定と維持に関する知識[4.10, 4.11]
4.17 代替処理サイトの種類（例：ホットサイト、ウォームサイト、コールドサイト）と契約された合意事項のモニタリングに使用される方法に関する知識[4.11]
4.18 災害復旧計画を始動する際に使用されるプロセスに関する知識[4.11]
4.19 災害復旧テストの方法に関する知識[4.10, 4.11]

ドメイン5 - 情報資産の保護:組織のセキュリティポリシー、基準、手順、およびコントロールが、情報資産の機密性、完全性、可用性を確保する保証を提供する。

タスク

5.1 情報セキュリティポリシー、基準、及び手順の完全性、及び一般的に受け入れられている業務との整合性について評価すること。
5.2 システム及び論理セキュリティコントロールの設計、導入及び監視を評価して、情報の機密性、完全性及び可用性を検証すること。
5.3 データ分類プロセス及び手順の設計、導入及び監視が組織の方針、基準、手順及び該当する外部要件と整合しているかどうかを判断するために、それらを評価すること。
5.4 物理的アクセス及び環境コントロールの設計、導入及び監視を評価し、情報資産が十分に保護されているかどうかを検証すること。
5.5 情報資産（例: バックアップメディア、遠隔地の保管施設、ハードコピー/ 印刷データ及びソフトコピーメディア）の保管、検索、移送及び廃棄を評価し、情報資産が適切に保護されているかどうかを検証すること。

知識項目

5.1 セキュリティ意識向上プログラムを含むセキュリティコントロールの設計、導入、及び監視の技法に関する知識[5.1, 5.2, 5.3, 5.4, 5.5]
5.2 セキュリティインシデントの監視及び対応プロセス（例: エスカレーション手順、緊急インシデント対応チーム）に関する知識[5.1]
5.3 権限が付与された機能やデータに対してユーザーを個人識別、認証及び制限するための論理アクセスコントロールに関する知識[5.2]
5.4 ハードウェア、システムソフトウェア（例:アプリケーション、オペレーティングシステム）、及びデータベース管理システムに関連するセキュリティコントロールに関する知識[5.2]
5.5 システムの仮想化に関連したリスクとコントロールに関する知識[5.2, 5.4]
5.6 ネットワークセキュリティコントロールの設定、導入、運用及び保守に関する知識[5.2]
5.7 ネットワーク及びインターネットセキュリティ機器、プロトコル及び技法に関する知識[5.2]
5.8 情報システムの攻撃方法と技法に関する知識[5.2, 5.4]
5.9 検出ツール及びコントロール技法（例: マルウェア、ウィルス検出、スパイウェア）に関する知識[5.2]
5.10 セキュリティのテスト技法（例: 侵入テスト、脆弱性検査）に関する知識[5.2]
5.11 データ漏洩のリスクとコントロールに関する知識[5.2, 5.3, 5.5]
5.12 暗号化関連の技法に関する知識
5.13 公開鍵インフラストラクチャ（PKI）の構成要素、及び電子署名技法に関する知識[5.2, 5.3, 5.5]
5.14 ピアツーピア・コンピューティング、インスタントメッセージング、及びWeb ベースの技法（例: ソーシャルネットワーキング、メッセージボード、ブログ）に関連したリスクとコントロールに関する知識[5.2]
5.15 モバイル及び無線機器の使用に関連したコントロールとリスクに関する知識[5.2]
5.16 音声通信のセキュリティ（例: PBX、VoIP）に関する知識[5.2, 5.4]
5.17 フォレンジック調査による証拠保全の技法及びプロセス（例: IT、プロセス、分析過程の保全管理）に関する知識[5.2]
5.18 データ分類基準及び対応手順に関する知識[5.3, 5.5]
5.19 認可されている設備に対してユーザーを個人識別、認証及び制限するための物理的アクセスコントロールに関する知識[5.4]

5.20 環境面の保護の為の機器及び対応業務に関する知識[5.4]
5.21 機密情報資産の保管、検索、移送及び廃棄に用いるプロセス及び手順に関する知識[5.3, 5.5]

AppendixB

試験問題作成チェックリスト

試験問題を提出する前に、以下の全ての質問に「はい」と答えられなければいけません。

1. 試験問題は、情報システム監査、統制あるいはセキュリティのコンセプトを、適切な経験レベル（3-5年の情報システム監査）で、受験者を試そうとしていますか。

2 当該試験問題は、情報システム監査、統制あるいはセキュリティに関するひとつのコンセプトだけを試していますか。

3. 試験問題は明確ですか。

4. 設問には、ひとつの正しい回答を導く十分な情報（シナリオ）がありますか。
受験生は、設問に情報が欠けていることにより、誤答を正しいものと推測するような解釈ができないように作られていますか。

5. いかなる状況や組織あるいは文化においても、設問に対するひとつの正答がありますか。設問に対応しない状況に基づき、ひとつ以上の正答がある場合に、試験問題の多くは状況によるという理由で、返却されています。

6. 設問および選択肢は相互に関連性がありますか。例えば「監査手続きのうちどれが…」という設問であれば、全ての選択肢は監査手続きであることが必要です。

7. 試験問題には妥当な誤答があり、ひとつだけの正答がありますか。

8. 設問には、正答となるような単語あるいは語句が表現されていませんか。

9. 設問あるいは選択肢に不要な文章や専門用語が用いられていませんか。

10. 設問あるいは選択肢に「frequently」「often」「common」といった主観的な用語が用いられていませんか。

11. 設問あるいは選択肢に「all」「never」「always」といった絶対的な用語が用いられていませんか。

12. 「least」「not」「except」といった用語を使った否定的な質問になっていませんか。

AppendixC

ITEM CONSTRUCTION FORM

Name:
ISACA ID:

Task Statement #:*(Refer to CISA Job Practice)*
Knowledge Statement #:*(Refer to CISA JobPractice)*

Testing Concept:(One sentence describing what is being tested)

Stem:

Options:

A. (Always make A the correct answer)
B.
C.
D.

Key:A

Justification:

A. (Why is A the correct answer)
B. (Why is Bincorrect)
C. (Why is Cincorrect)
D. (Why is D incorrect)

Reference(s): Provide references to enable independent review. Include the publication title, publication year, author and page.