
# CISM®試験問題作成ガイド

**2017 年 3 月改定**

## 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。東京支部は、「問題応募を会員にとって身近なもの」とするため本文書の日本語訳を２０１２年に実施し、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。今般、東京支部では5年ぶりに「CISM試験問題作成ガイド」について最新版を元に再度翻訳を行いました。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　東京支部理事（元会長） 坂本 正徳 CISA, CISM, CGEIT, CRISC, CISSP

協力　東京支部会長兼理事　田中 秀幸 CISA, CISM, CGEIT, CRISC

ISACA東京支部

2018-2019 会長兼理事　田中　秀幸

*Quality Statement:*
*This Work is translated into Japanese from the English language version of CISM Item Development Guide-Mar. 2017 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「CISM Item Development Guide-Mar. 2017」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。*

# CISM 試験問題作成ガイド

## 目　　次

# CISM 試験問題作成ガイド

## CISM 試験問題作成ガイドの目的

CISM 試験問題作成ガイド（以下、「本ガイド」という）の目的は、CISM 試験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 CISM 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。

## CISM 試験の構成

ISACA および CISM 認定委員会では、情報セキュリティマネージャー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、CISM 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、CISM 試験の青写真として提供されます。試験問題は、CISM の職務領域分析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 CISM の受験者です。試験問題は、望ましい CISM の受験者に求められる適切な経験レベル（3-5 年の情報セキュリティ管理の実務経験）に応じて作成されなければなりません。

情報セキュリティ管理はグローバルに展開されている職業であり、グローバルな立場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 CISM 試験問題は、国際的な情報セキュリティ管理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。

# CISM 試験問題作成ガイド

## 複数選択肢問題

CISM 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** CISM 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 CISM 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、Appendix B 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。このようにして受験者の経験の未熟さに訴えるような選択肢を誤答として用意できれば最適です。

**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** Appendix B 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(NOT, LEAST, EXCEPT といった単語を設問に用いる)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. 設問およびすべての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:**

# CISM 試験問題作成ガイド

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も不適切な選択を求める。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. 各設問に複数のコンポーネントがある、あるいはひとつの選択肢の部分がその他の選択肢の内容を含むようなことはさける。これらは「複合、複合選択肢」と考えられ、試験としては良くない。各選択肢は各々独立しているべきである。
7. 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、よい誤答とはらない。
8. 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。
9. 特定の標準やフレームワーク、マニュアル（例、COBIT, ISO）を個々に掲載するような試験問題は承認されない。しかしながら、最良の実践に関する知識を問うことは、全く承認および奨励されることである。
10. 「以下のいずれかが正しいか」といった正誤を試す設問は作成してはならない。
11. 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

CISM 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、質問型あるいは不完全文章型があり、以下に記されています。当該問題はサンプルとして問題作成用に作られたものであり、試験に出るものではありません。

***質問型:***

設問(Stem): Which of the following will **BEST** tie information security to business objectives?

選択肢(Alternatives):

A. Value analysis
B. Security metrics
C. Deliverables list
D. Process improvement model

注）設問は質問型である。

***不完全型:***

設問(Stem): The **PRIMARY** goal of a post-incident review is to:

選択肢(Alternatives):
A. identify ways to improve the response process.
B. gather evidence for subsequent legal action.
C. identify individuals who failed to take appropriate action.
D. make a determination as to the identity of the attacker.

注）当該設問への対応は以下の語句を伴い始まり、文章を完結させるように続き、回答は設問で始まる文を各々完成させるものである。

## 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と記載されているものです。これらの設問は、CISM 試験のプールにあるものではなく、いかなる試験でも使用されません。あくまで試験問題作成の練習目的のサンプルとして作られたものです。

***例 1:***

**設問(Stem)**: An intrusion prevention system does which of the following?

**選択肢(Alternatives):**
A. Prevents any attacks that occur from affecting the target system
B. Stops all network traffic that is part of an attack before it can get to the intended victim
C. Constantly modifies operating systems to make them a moving target
D. Launches attacks against attacking systems to bring them down or disable them

**正答(Key):** A

注）正解となる単語が設問に「prevention」と記されており、「prevent」が正答であることを導いています。正解が非常に明確になってしまうので、重要な類似語を設問および回答で使うことは避けて下さい。また、選択肢 B での「all」や、選択肢 C の「constantly」といった絶対的な言葉が使われていることで、容易にこれらが誤答であることが判って

しまいます。選択肢には絶対的あるいは主観的な単語は使用しないようにして下さい。

***例 2:***

**設問(Stem):** Which of the following is **MOST** important to writing good information security policies?

**選択肢(Alternatives):**

A. Ensure that they are easy to read and understand
B. Ensure that they allow for flexible interpretation
C. Ensure that they describe technical vulnerability
D. Ensure that they change whenever operating systems are upgraded

**正答(Key):** A

注）最初の3つの単語が各々繰り返されています。この問題では、より試験問題を簡潔に作り変えることが可能です。これらの3つの単語は設問の最後に、以下に続くものとして含めましょう。

**新しい設問(New Stem):** Which of the following is **MOST** important to writing good information security policies? Ensure the policies:

**新しい選択肢(Alternatives):New Alternatives:**

A. are easy to read and understand.
B. allow for flexible interpretation.
C. describe technical vulnerability.
D. change whenever operating systems are upgraded.

設問は、文章を完成させるような選択肢を伴う不完全型となります。

***例 3:***

**設問(Stem):** When building support for an information security program, which of the following should be performed **FIRST**?

**選択肢(Alternatives):**

A. Identification of existing vulnerabilities
B. Cost-benefit analysis
C. Business impact analysis
D. Formal risk assessment

**正答(Key):** A

この試験問題はタイミングの質問の例であり、主観に基づいてしまいます。選択肢 C および D は、組織内の状況によっては正しい回答となり得ます。プロセスの中で「最初の」段階を明確化しない限り、「最初に」すべきことは何か、という問いは良い問題ではありません。しかし、「最初の」段階を明確化すれば、設問としては簡単過ぎてしまいます。

***例 4:***

**設問(Stem):** Security awareness programs should be:

**選択肢(Alternatives):**

A. standardized throughout the organization.
B. customized depending on the target audiences.
C. avoided since key security vulnerabilities may be disclosed.
D. limited to IS personnel.

**正答(Key):** A

例 4 は、主観的な試験問題のもうひとつの実例です。組織のいくつかでは、セキュリティ啓蒙プログラムは標準化されたものとして義務付けられますが、一方ではプログラムをカスタマイズすることがより良い場合もあります。回答は組織のセキュリティニーズとプログラムによって変わるものです。

何がセキュリティ啓蒙プログラムとして良いのか、とか、役割と責任を試すといった、本来的に主観的になりがちな領域の設問を作成する際には、全ての状況において唯一の正答が存在するものかを注意深く確認することが必要です。全ての状況において適用される回答に自信がないものであれば、主観性を取り除くべく設問に更なる状況を付加するようにしましょう。例えば、組織の構成を記載できれば、経験ある情報セキュリティマネージャーは、どの型のセキュリティ啓蒙プログラムが実施するのに最良であるかが明確になります。

***例 5:***

**設問(Stem):** Record retention policies generally are driven by:

**選択肢(Alternatives):**

A. legal and regulatory requirements.
B. risk levels acceptable to the organization.
C. business goals and objectives.
D. audit and assurance requirements.

**正答(Key):** A

当該設問は、誤答が脆弱なために正答が明確すぎる場合を描いています。法規制の要件といった回答は、受験生を正答から誤答へ導く他の強力な選択肢の余地がないことから、設問を貧弱にしてしまいます。

以上の例は、試験問題が何故承認されなかったか、という最も一般的な理由を示すものです。その他に試験問題が返却される理由としては、技術的あるいは定型過ぎるといったものがあります。技術的な本質の試験問題を作成する際には、内容は情報セキュリティマネージャーの経験した知識を試す必要があること、技術者を試すものではないことを忘れないで下さい。また、CISM 試験は、個人の情報セキュリティ管理の知識の応用力を試す実務的な試験です。もし定型過ぎるという理由で返却される場合は、受験生に対して知識あるいはコンセプトをいかに応用するかということから乖離して、技術あるいはセキュリティ用語の定義を知っているかどうかを尋ねるだけの単純な試験問題になっている、ということが多いものです。

## CISM 職務領域とは

CISM の職務領域とは、セキュリティ、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 CISM 試験の設問の基礎となるものです。CISM 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。CISM 職務領域は、Appendix A 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。

## 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、CISM 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、Appendix A の「CISM 職務領域」を参照して下さい。***オンラインでの試験問題の提出する際には、種別は「Classifications」として関連付けられています。タスクは、「Primary Classifications」、知識の記述は「Secondary Classifications」として関連付けられます。***

## 試験問題の提出およびレビュープロセス

試験問題は、ISACA のオンライン試験問題作成システムを用いて提出しなければなりません。全ての試験問題は、英語で記載して提出する必要があります。試験問題には、設問（stem）、4つの選択肢（alternatives）、そして選択肢毎の論理的根拠が含まれなければなりません。

www.isaca.org/itemwriting 画面で試験問題作成に同意した首題の専門家は、試験問

題作成キャンペーン通知する電子メールを定期的に受け取ることになります。当該電子メールには、試験問題作成のシステムへのリンクも含まれます。キャンペーンに関する文書は、特定の重点領域、本ガイド、及び職務領域といったキャンペーンに関連する文書を適宜参照することができます。

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 CISM 試験問題評価委員会(Exam Item Development Working Group - EIDWG)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。$50 の謝礼金が承認された試験問題毎に授与されます。

# CISM 試験問題作成ガイド

# Appendix A

## CISM 職務領域 – 2017 年発効

試験問題の種別分担化を支援するために、当該職務領域に掲載する知識項目は、タスクを反映して関連付けられます。各知識項目の終わりには、最も良く適用するタスクが割り当てられています。所与の知識項目はひとつ以上のタスクと結び付けられ、知識の留意点（試すコンセプト）は、記述される特定のタスクに基づき、各々異なるべきものです。

**領域1—情報セキュリティガバナンス:** 情報セキュリティガバナンスのフレームワークと支援プロセスを確立および/または維持し、情報セキュリティ戦略が組織の目標と目的に整合していることを確実にする。

***タスクの記述:***

1.1 組織の目標及び目的とした情報セキュリティ戦略を確立および/または維持し、情報セキュリティプログラムの確立および/またはその継続する管理をガイドする。
1.2 情報セキュリティガバナンスのフレームワークを確立および/または維持し、情報セキュリティ戦略を支援する活動をガイドする。
1.3 情報セキュリティガバナンスをコーポレートガバナンスに統合し、組織の目標と目的が情報セキュリティプログラムによって支援されていることを確保する。
1.4 情報セキュリティポリシーを確立および維持し、企業の目標及び目的と整合した標準、手続き、およびガイドラインの作成をガイドする。
1.5 情報セキュリティへの投資を支援するビジネスケースを作成する。
1.6 組織への外部及び内部の影響を識別し（例えば新技術、ソーシャルメディア、業務環境、リスク許容度、法的規制事項、第三者の考察、脅威環境等）、情報セキュリティ戦略によってこれらの要素が対処されることを確実にする。
1.7 上級指導者層と他の利害関係者からの継続的な関与を得て、情報セキュリティ戦略を上手く実施できるよう支援する。
1.8 組織全体の情報セキュリティ責任（例えば、データ所有者、データ保護管理者、エンドユーザ、特権ユーザまたは高リスクユーザ等）と権限体制を定義し、伝達し監視する。
1.9 情報セキュリティの評価尺度の確立、監視、評価、報告を行い、情報セキュリティ戦略の有効性に関する正確かつ有意義な情報を経営陣に提供する。

***知識の記述:***

k1.1 情報セキュリティ戦略を開発するために使用する技術の知識（例えば SWOT[強み、弱み、機会脅威]分析、ギャップ分析、脅威研究等）(タスク: 1.1.1)
k1.2 情報セキュリティと、ビジネス目標、目的、機能、プロセスおよび実践の関係の知識 (タスク: 1.1.1, 1.1.3, 1.1.4, 1.1.6)
k1.3 利用可能な情報セキュリティガバナンスフレームワークの知識（タスク: 1.1.2, 1.1.3）
k1.4 情報セキュリティガバナンスと戦略の作成に関連した国際的に認識にされる標準、フレームワーク、および産業のベストプラクティスの知識 （タスク: 1.1.1, 1.1.2, 1.1.3）

k1.5 ガバナンスの基本概念と情報セキュリティとの関係の知識 (タスク: 1.1.2, 1.1.3)
k1.6 情報セキュリティガバナンスフレームワークの評価、価値、作成および実施方法の知識 (タスク: 1.1.2, 1.1.3)
k1.7 情報セキュリティガバナンスをコーポレートガバナンスに統合する方法の知識(タスク: 1.1.3, 1.1.6)
k1.8 情報セキュリティポリシー策定に寄与する要因をパラメータ(例えば、組織の構造と文化、上級経験者への印象、関係等)の知識(タスク 1.1.4)
k1.9 ビジネスケースの内容およびビジネスケースを開発するための技術の知識 (タスク: 1.1.5)
k1.10 予算計画戦略及び報告方法の知識(タスク: 1.1.1, 1.1.5, 1.1.9)
k1.11 組織への外部及び内部の影響(例えば、新技術、ソーシャルメディア、業務環境、リスク許容度、法的規制事項、第三者の考察、脅威環境等)、それらが情報セキュリティ戦略にどのように影響を与えるかの知識(タスク: 1.1.1, 1.1.6)
k1.12 上級指導者層からの関与及び他の利害関係者からのサポートを得るために必要な主要情報の知識(例えば、情報セキュリティが組織の目標と目的をどのようにサポートするのか、成功裡な実施を決定する条件、ビジネスインパクト等)(タスク: 1.1.1, 1.1.5, 1.1.7)
k1.13 上級指導者層及び他の利害関係者との連絡の方法と考察の知識(例えば、組織の文化、伝達経路、情報セキュリティの重要な側面の強調等)(タスク: 1.1.7)
k1.14 情報セキュリティマネージャーの役割と責任の知識(タスク: 1.1.8)
k1.15 組織構造、権限体系およびエスカレーションポイントの知識(タスク: 1.1.8)
k1.16 組織にわたるスタッフの情報セキュリティの責任の知識(例えば、データ所有者、エンドユーザ、特権ユーザまたは高リスクユーザ)(タスク: 1.1.8)
k1.17 情報セキュリティの責任のパフォーマンス監視のためのプロセスの知識(タスク: 1.1.8)
k1.18 組織全体にわたる報告と伝達の適切な経路を新規に確立、または既存のものを利用する方法の知識(タスク: 1.1.8)
k1.19 主要な情報セキュリティの評価尺度(例えば、重要目標達成指標[KGI]、主要業績評価指数[KPI]、主要リスク指標[KRI]の選択、実施、および説明する方法の知識)(タスク: 1.1.9)

**領域2—情報リスク管理:** 組織の目標と目的に整合するリスク選好度に基づき、情報リスクを受容レベルで管理する。

***タスクの記述:***

2.1 資産保護のために講じる手段が確実に事業価値に釣合うようにするために、情報資産分類のプロセスを確立もしくは維持する。
2.2 準拠違反のリスクを受容レベルで管理するために、法的、規制、組織、その他の適用要件を特定する。
2.3 組織の情報に対するリスクを特定し評価するため、リスク評価、脆弱性評価、脅威分析が一貫して、かつ適切なタイミングで確実に実施されるようにする。
2.4 組織のリスク選好度に基づき、受容レベルでリスクを管理するために、適切なリスク対処/対応措置の選択肢を特定、推奨、実施する。
2.5 情報セキュリティコントロールが適切で、リスクを受容レベルで効果的に管理しているかどうかを判別する。
2.6 組織全体で一貫した包括的な情報リスク管理プログラムを実現するため、情報リスク管

理プログラムを実現するため、情報リスク管理をビジネスプロセスと IT プロセス（例えば、システム開発、調達、プロジェクト管理）に統合することを促進する。

2.7 既存または新しいリスクシナリオへの変更が特定され適切に管理することを確実にするために、リスクの再評価が必要となることがある内部および外部要因（例えば、脅威の状況、サイバーセキュリティ、地政学的状況、規則の変更）をモニタリングする。

2.8 リスク管理の意思決定プロセスを促進するため、準拠違反と情報リスクのその他の変更を報告する。

2.9 組織の目標と目的に対する潜在的な影響の理解を支援するため、情報セキュリティリスクが上級経営者に確実に報告されるようにする。

***知識の記述:***

k2.1 ビジネスの目的と整合性のとれた情報資産分類モデルを確立するための方法に関する知識（タスク: 1.2.1, 1.2.2）

k2.2 情報資産とリスクのオーナーシップアサインについての検討事項に関する知識（タスク: 1.2.1）

k2.3 情報資産とビジネスに対する内部または外部のイベントの影響を特定および評価するための方法に関する知識（タスク: 1.2.1, 1.2.7）

k2.4 内部または外部のリスク要因をモニタリングする方法に関する知識（タスク: 1.2.2, 1.2.7）

k2.5 情報資産の査定方法論に関する知識（タスク: 1.2.1）

k2.6 情報セキュリティに関連する法的、規則、組織、その他の要因に関する知識（タスク: 1.2.2, 1.2.7, 1.2.8）

k2.7 新たな情報セキュリティの脅威と脆弱性に関する、信頼できかつタイムリーな情報源の知識（タスク: 1.2.1, 1.2.3, 1.2.7, 1.2.8）

k2.8 リスクの再評価や、情報セキュリティプログラム要素の変更が必要となる可能性がある事象の知識（タスク: 1.2.1, 1.2.3, 1.2.7, 1.2.8）

k2.9 情報の脅威、脆弱性、露出（サイバーセキュリティを含む）とその発展性に関する知識（タスク: 1.2.3, 1.2.7）

k2.10 リスクシナリオおよび分析方法論に関する知識（タスク: 1.2.3, 1.2.4, 1.2.7）

k2.11 リスクシナリオおよびリスク対処/対応措置の選択肢の優先順位の決定に使用する方法に関する知識（タスク: 1.2.4, 1.2.5, 1.2.7）

k2.12 リスク報告要件（例えば、頻度、報告対象者、内容）の知識）（タスク:1.2.5, 1.2.8, 1.2.9）

k2.13 リスク対処/対応措置の選択肢（回避、軽減、受容または移転）およびそれらの適用方法に関する知識（タスク: 1.2.4, 1.2.5, 1.2.7）

k2.14 統制のベースラインと標準およびそれらのリスク評価との関係に関する知識（タスク: 1.2.3, 1.2.5）

k2.15 情報セキュリティコントロールとその効果の分析方法に関する知識（タスク: 1.2.4）

k2.16 情報セキュリティに関連するギャップ分析技術に関する知識（タスク: 1.2.3, 1.2.5）

k2.17 情報セキュリティリスク管理をビジネスプロセスと IT プロセスに統合するための技術に関する知識 （タスク: 1.2.5, 1.2.6）

k2.18 コンプライアンスの報告要件とプロセスに関する知識（タスク: 1.2.6, 1.2.8, 1.2.9）

k2.19 リスク対処の選択肢を評価するための費用対効果分析に関する知識（タスク: 1.2.4, 1.2.5）

# CISM 試験問題作成ガイド

**領域3—情報セキュリティプログラムの開発と管理:**情報セキュリティ戦略と事業目標に沿った、組織の資産を識別、管理および保護する情報セキュリティプログラムを開発および維持することで、効果的なセキュリティに対する姿勢を支援する。

***タスクの記述:***

3.1 情報セキュリティ戦略に沿った情報セキュリティプログラムを確立および/または維持すること。

3.2 情報セキュリティプログラムが確実に事業に付加価値を与えまたこれを保護するように、情報セキュリティプログラムと他のビジネス機能（人事[HR]、会計、調達、IT など）が持つ業務目標と連携させること。

3.3 内部と外部のリソースの要件の把握、取得、および管理を行って、情報セキュリティプログラムを実行すること。

3.4 組織の事業目標に沿って情報セキュリティプログラムが実施されるように、情報セキュリティプロセスとリソース(人員および技術を含む)を確立し維持すること。

3.5 組織の情報セキュリティの基準、ガイドライン、手順、および他の文書の確立、伝達、および維持を行って、情報セキュリティポリシーの遵守を支援し指導すること。

3.6 情報セキュリティの意識向上と研修のためのプログラムを確立、推進および維持して、効果的なセキュリティ文化を醸成すること。

3.7 情報セキュリティ要件を組織の各種プロセス（変更コントロール、合併および買収、システム開発、事業継続、災害復旧など）に組み込んで、組織のセキュリティ戦略を維持すること。

3.8 情報セキュリティ要件をサードバーティ（合弁会社、委託業者、ビジネス・パートナー、顧客など）の契約と活動に組み込んで、組織のセキュリティ戦略を維持するため確立された要件の順守を監視すること。

3.9 プログラムの管理と運用上の測定基準の確立、監視、および分析を行って、情報セキュリティプログラムの有効性と効率性を評価すること。

3.10 セキュリティの成果について伝達するため、情報セキュリティプログラムと根底にあるビジネスプロセスの活動、傾向および全体的な有効性に関するレポートを編集し、主な利害関係者に提供すること。

***知識の記述:***

k3.1 情報セキュリティプログラムの要件と他のビジネス機能の要件を合致させる方法に関する知識（タスク: 1.3.1, 1.3.2）

k3.2 内部と外部のリソースの要件の把握、取得、管理、および定義を行うための方法に関する知識（タスク: 1.3.1, 1.3.3, 1.3.4）

k3.3 既存および新出の情報セキュリティ技術とその根底にある概念に関する知識（タスク: 1.3.3, 1.3.4）

k3.4 情報セキュリティコントロールを設計および導入する方法に関する知識（タスク: 1.3.7, 1.3.8）

k3.5 組織の事業目標に沿った情報セキュリティプロセスおよびリソース（人員および技術を含む）と、これらの適用方法に関する知識 （タスク: 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.3.7）

k3.6 情報セキュリティの基準、手順、およびガイドラインの策定および文書化する方法に関する知識（タスク: 1.3.5）

k3.7 情報セキュリティプログラムの開発と管理に関連した国際的に認められた規制、基準、

フレームワーク、およびベストプラクティスの知識（タスク: 1.3.7, 1.3.7, 1.3.8）
k3.8 情報セキュリティのポリシー、基準、手順、およびガイドラインを実装し伝達する方法に関する知識（タスク: 1.3.5, 1.3.6）
k3.9 情報セキュリティ要員用の研修、認定資格およびスキルセット開発に関する知識（タスク: 1.3.6）
k3.10 効果的な情報セキュリティ啓発と研修のプログラムを確立し維持するための方法に関する知識（タスク: 1.3.5, 1.3.7）
k3.11 情報セキュリティ要件を組織のプロセス（アクセス管理、変更管理、調査プロセスなど）に組み込む方法に関する知識（タスク: 1.3.1, 1.3.2, 1.3.3, 1.3.7）
k3.12 情報セキュリティ要件を契約や同意書およびサードパーティ管理プロセスに組み込むための方法に関する知識 （タスク: 1.3.2, 1.3.3, 1.3.8）
k3.13 サードパーティおの契約や同意書と、必要に応じてそれに付随する変更プロセスを監視および評価する方法に関する知識（Task: 1.3.3）
k3.14 情報セキュリティの運用上の測定基準の設計、実施、および報告を行うための方法に関する知識（タスク: 1.3.3, 1.3.9, 1.3.10）
k3.15 情報セキュリティコントロールの有効性および効率性をテストする方法に関する知識（タスク: 1.3.9, 1.3.10）
k3.16 情報セキュリティプログラムのステータスを主要利害関係者に伝達する技法に関する知識（タスク: 1.3.6, 1.3.10）

**領域4—情報セキュリティインシデントの管理:** 情報セキュリティインシデントの検出、調査、対応、及び復旧を行う能力の計画、確立、及び管理を行い、ビジネスインパクトを最小限にする。

***タスクの記述:***

4.1 情報セキュリティのインシデントの組織的定義と重大度の序列を確立し維持して、インシデントの正確な分類とカテゴリー可を行い、インシデントに対応できるようにすること。
4.2 インシデント対応計画を確立し維持して、情報セキュリティのインシデントに効果的かつ適時に対応できるようにすること。
4.3 各種プロセスを開発し実装して、ビジネスに影響を与える可能性のある情報セキュリティインシデントを適時に識別できるようにすること。
4.4 情報セキュリティインシデントを調査し記録するためのプロセスを確立し維持して、法令、規則、および組織の要件に準拠しながら、適切な対応と原因を決定できるようにすること。
4.5 インシデントの通知とエスカレーションのプロセスを確立し維持して、適切な利害関係者がインシデント対応管理に確実に参加できるようにすること
4.6 情報セキュリティインシデントに効果的に、かつ適時に対応するチームの編成、訓練、および準備を行うこと。
4.7 インシデント対応計画を定期的にテスト、評価および（該当する場合には）改定して、情報セキュリティインシデントに効果的に対応し、対応能力を向上できるようにすること。
4.8 コミュニケーションの計画とプロセスを確立し維持して、内部および外部の主体とのコミュニケーションを管理すること。
4.9 事後レビューを実施して、情報セキュリティのインシデントの根本原因を特定し、是正措置を策定し、リスクを再評価し、対応の有効性を評価し、適切な対策を実施すること。
4.10 インシデント対応計画、災害復旧計画、および事業継続計画の間の統合を確立し維持すること。

# CISM 試験問題作成ガイド

## *知識の記述*

k4.1　インシデント管理の概念と実務に関する知識（タスク: 1.4.1, 1.4.4）
k4.2　インシデント対応計画の要素に関する知識（タスク: 1.4.1, 1.4.2, 1.4.3, 1.4.10）
k4.3　事業継続計画（BCP）と災害復旧計画（DRP）およびそれらとインシデント対応計画との関係に関する知識（タスク: 1.4.1, 1.4.2, 1.4.4, 1.4.10）
k4.4　インシデント分類/カテゴリー化方法に関する知識（タスク: 1.4.1, 1.4.2, 1.4.3, 1.4.4）
k4.5　運営への悪影響を最小限に留めるための、インシデント封じ込め方法に関する知識（タスク: 1.4.1, 1.4.2）
k4.6　通知とエスカレーションのプロセスに関する知識（タスク: 1.4.1, 1.4.2, 1.4.5, 1.4.8）
k4.7　情報セキュリティインシデントの特定および管理における役割と責任に関する知識（タスク: 1.4.2, 1.4.3, 1.4.5, 1.4.6, 1.4.7, 1.4.8）
k4.8　インシデント対応チームで十分に備えておく必要があるトレーニング、ツールや機器の種類または供給源に関する知識（タスク: 1.4.4, 1.4.6）
k4.9　証拠の収集、保存、および提出のためのフォレンジックの要件と能力（証拠能力、証拠の品質、網羅性、分析過程の保全管理など）に関する知識（タスク: 1.4.2, 1.4.4, 1.4.6）
k4.10内部と外部のインシデント報告の要件と手順に関する知識（タスク: 1.4.2, 1.4.8, 1.4.9）
k4.11 根本原因の特定と是正処置の決定を行うための事後レビューの実務および調査方法に関する知識（タスク: 1.4.4, 1.4.7, 1.4.9）
k4.12 情報セキュリティインシデントによって報じる損害、費用および他のビジネスへの影響を定量化する技術に関する知識（タスク: 1.4.9）
k4.13 情報セキュリティイベントの検知、ログ作成、分析および文書化を行う技術とプロセスに関する知識（タスク: 1.4.3, 1.4.4）
k4.14 情報セキュリティのインシデントの調査に使用できる内部と外部のリソースに関する知識（タスク: 1.4.4, 1.4.5, 1.4.6）
k4.15 インシデント対応プロセス中に運用環境に対して行われた変更の潜在的影響を特定する方法に関する知識（タスク: 1.4.4）
k4.16 インシデント対応計画をテストする技法に関する知識（タスク: 1.4.1, 1.4.6, 1.4.7）
k4.17 適用される規制上、法律上および組織の要件に関する知識（タスク: 1.4.4, 1.4.9）
k4.18 インシデント対応計画の有効性を評価するための主な指標/評価尺度に関する知識（タスク: 1.4.4, 1.4.7, 1.4.9）

# CISM 試験問題作成ガイド

## Appendix B

### 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、CISM のコンセプトを、適切な経験レベル（3-5 年の情報セキュリティ管理）で、受験者を試そうとしていますか。

2 当該試験問題は、CISM 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「統制のうちどれが…」という設問であれば、全ての選択肢は統制に関するもの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. 試験問題には、正答となるような単語あるいは語句が設問の中に表現されていませんか。

9. 設問あるいは選択肢に「frequently」「often」「common」といった主観的な用語を使わないようにしていますか。

10. 設問あるいは選択肢に「all」「never」「always」といった絶対的な用語を使わないようにしていますか。

11. 「least」「not」「except」といった用語を使わないようにしていますか。