



CERTIFIED INFORMATION SYSTEMS AUDITOR[®]

2012 年受験者のための
CISA[®] 試験と認定ガイド

受験者のためのCISA® 試験と認定ガイド

2012年度CISA試験— 日付に関する重要情報

試験日—2012年6月9日

早期締切日:	2012年2月8日
最終締切日:	2012年4月4日
試験登録の変更:	4月14日～4月20日(手数料\$50)。2012年4月20日を過ぎてからはいかなる変更も認められません。

払戻: ~2012年4月13日(手数料\$100)。この日を過ぎると払戻はできません。

繰越: 2012年4月20日以前に受理された要求の場合、US \$50の手数料がかかります。2012年4月21日～5月24日に受理された要求の場合、US \$100の手数料がかかります。2012年5月24日を過ぎると、繰越は認められません。

試験日—2012年12月8日

早期締切日:	2012年8月15日
最終締切日:	2012年10月3日
試験登録の変更:	10月6日～10月12日(手数料\$50)。2012年10月12日を過ぎてからはいかなる変更も認められません。

払戻: 2012年10月5日(手数料\$100)。この日を過ぎると払戻はできません。

繰越: 2012年10月12日以前に受理された要求の場合、US \$50の手数料がかかります。2012年10月13日～11月21日に受理された要求の場合、US \$100の手数料がかかります。2012年11月21日を過ぎると、繰越は認められません。

すべての締切日の時刻は、米国イリノイ州シカゴの5p.m.(米国セントラル時間)に基づいています。

2012 受験者のための CISA® 試験と認定ガイド
本書は米国で印刷されています。

目次

概要.....	3
CISAプログラムがISO/IEC 17024:2003の 認証を更新.....	3
CISA試験.....	3
CISA試験の受験準備.....	4
CISA試験の管理運営.....	4
CISA試験の採点.....	6
CISA試験の問題の種類.....	6
CISAの資格申請.....	7
CISA資格の認定要件.....	7
CISA資格維持の要件.....	7
ISACA職業倫理規定.....	7
CISA資格の取り消し.....	7
CISAの職務と知識の記述.....	8

ISACA とは

ISACA (www.isaca.org) は、世界160か国95,000人をこえる会員から構成される団体で、情報システム(IS)のアシユアランスとセキュリティ、ITのエンタープライズ・ガバナンスおよび管理、そしてIT関係のリスクやコンプライアンスにおける、知識、資格認定、コミュニティ作り、支援活動、教育機会等を、グローバルに主導しています。ISACAは独立の非営利団体として1969年に設立され、国際会議の主催、「ISACA® Journal」の刊行、国際的な情報システム監査およびコントロール基準の策定に従事しており、情報システムの信頼性と利用する価値を明らかにしています。さらに、世界的に高く評価されているCertified Information Systems Auditor®(CISA®)、Certified Information Security Manager®(CISM®)、Certified in the Governance of Enterprise IT® (CGEIT®)、そしてCertified in Risk and Information Systems Control™ (CRISC™)などの資格認定を通じ、ITスキルと知識の向上と能力の証明を行っています。ISACAはCOBIT®を継続的に更新しており、これは、特にアシユアランス、セキュリティ、リスクとコントロールの分野において、IT専門家や企業の幹部のITガバナンスと経営責任、ビジネスの価値の向上に役立っています。

免責条項

ISACAおよびCISA認定委員会は、CISAの資格取得の指針として『2012年受験者のためのCISA®試験と認定ガイド』を策定しました。受験者が本書または他の協会の出版物を参照したことでCISA試験に合格することが保証されるものではありません。

権利の留保

Copyright © 2011 ISACA. 目的や形式を問わず、ISACAの事前の書面による許可なく、本書の内容を複製または保管することを禁じます。本書に関して、これ以外の権利ならびに許可は与えられません。全ての権利は留保されています。

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
電話: +1.847.253.1545
FAX: +1.847.253.1443
電子メール: exam@isaca.org
ウェブサイト: www.isaca.org

受験者のためのCISA®試験と認定ガイド

概要

専門的な資格プログラムの優れた点は、達成したものに与えられる評価と認証にあります。1978年に開始されたISACA保有の公認情報システム監査人(CISA)プログラムは、情報システム(IS)の監査、コントロールおよびセキュリティの専門家が目指す世界的に認知された標準資格となっています。

CISAが推奨し評価する技術的なスキルや実務は、その分野で成功するための基本要素です。CISAの認定資格の保有は、熟練度の証明や専門分野の評価基準になります。情報システムの監査、コントロールおよびセキュリティのスキルを持つ専門家に対する需要の高まりを背景に、CISAは、世界中の個人や組織が求める資格プログラムへと成長しています。CISA資格は、企業で働く上での責任を意味し、卓越した専門職を表すものです。

CISAプログラムがISO/IEC 17024:2003の認証を更新

ANSI (American National Standards Institute 米国規格協会)は、CISA認定プログラムに対してISO/IEC 17024:2003(人に対する認証システムを運営する団体のための一般的要件)の認証を与えています。民間非営利団体であるANSIは、製品、システム、人材認定を行う第三者組織を認可する団体です。

ISO/IEC 17024は、特定の要件に対して個人を認定する組織が従わなければならない必要条件を指定しています。ANSIでは、ISO/IEC 17024を「資格コミュニティの世界的な標準化の促進、国間の流動性の向上、公共の安全性の強化および消費者の保護を推進するために大きな役割を担うもの」として評しています。



ANSI 認定プログラム
人材認定
#0694
ISO/IEC 17024

ANSIの認定:

- ISACAが提供するユニークな資格や専門性を促進する
- 認定に関する規準を保護し、法的な正当性を提供する
- 認定自体および認定資格の所有者に関して、消費者や公共の信用を高める
- 各種業界間の流動性を促進させる

ANSIによる認定は、ISACAの手順が、偏見のなさ、バランス、コンセンサス、適正な手続きなどに関して、ANSIの本質的な要件を満たしていることを意味しています。この認定によって、ISACAは、CISA資格所有者に対する優れた職業的チャンスが世界中でもたらされるものと予測しています。

CISA試験

CISA試験の開発/説明

CISA認定委員会は試験の作成を監督し、内容が最新であることを確認します。CISA試験の問題は、試験の品質を最大限向上させる包括的なプロセスを通じて開発されています。このプロセスでは、試験向上小委員会(Test Enhancement Subcommittee: TES)が問題の作成者と協力して例題の作成と精査を行います。この後、例題がCISA認定委員会に送られ、さらに審査が行われます。

実務は、試験の基本であり、CISA資格を取得するために必要な実務経験の要件になります。この実務は、5種類の分野(ドメイン)から構成され、定期的に更新されます。ドメインおよび付随する職務と知識の記述は、広範な調査と各国の当該問題の専門家によるフィードバックに基づいて作成されています。

職務と知識の記述は、CISAが実施する職務とその職務を実行するために必要な知識を表しています。受験者は、実施する職務に関連する実践的な知識に基づいてテストされます。

更新された実務領域分析のドメインおよびその割合を次に示します。

- 情報システム監査のプロセス(14%)
- ITガバナンスとマネジメント(14%)
- 情報システムの取得、開発および導入(19%)
- 情報システムの運用、保守およびサポート(23%)
- 情報資産の保護(30%)

注:ドメインと共に記載されているパーセント数は、各ドメインから出題される質問の割合ないし重要度を示しています。各ドメインの職務と知識の記述に関する説明については、8~11ページをご覧ください。


試験は、多肢選択方式の問題200問で構成されていて、6月と12月の年2回実施されます。試験時間は4時間です。受験者はいくつかの言語の中から1つの言語を選択して試験を受けることができます。現在対応している言語のリストについては、www.isaca.org/cisaterminologyをご覧ください。

受験者のためのCISA® 試験と認定ガイド

CISA 試験の受験準備

CISA 試験に合格するには学習計画に基づいた受験準備が必要です。受験準備を助けるために、ISACA では教材とレビューコースを受験者にご提供しています。試験の準備に役立つ ISACA 教材については、www.isaca.org/cisaguide をご覧ください。所在地や通関事情により配達に 1 週間から 4 週間を要する可能性があるため早めにご注文ください。最新の出荷情報は www.isaca.org/shipping でご覧ください。

ISACA では、CISA® オンライン・レビュー・コースも提供しています。このコースには、インタラクティブな課題、ケーススタディー、復習ツール、および練習問題が含まれます。詳細について、またはコースの概要については、www.isaca.org/elearning でご覧ください。

 学習を進めるために推奨される参考文献の総合的なリストは、「2012 年公認情報システム監査人 (CISA) レビューマニュアル」でご確認いただけます。

ISACA のウェブサイト www.isaca.org/cisaguide には、最もよく使用される専門用語のリスト（英語とその他の対応言語が対になっている）が記載されており、専門用語の学習に役立ちます。

ISACA では、共通の用語集や各資格に固有の用語集を保持しています。これらの用語集は、www.isaca.org/glossary から入手できます。

ISACA 並びに CISA 認定委員会は、これらの刊行物または他の協会の出版物及びコースが受験者の合格を保証するものではないことを明示します。

CISA 試験の管理運営

ISACA では、国際的に認知された専門の試験代理機関を利用して、CISA 試験の作成、管理および採点をしています。

受験者が試験の管理運営について意見がある場合、試験の最後で「試験の管理運営に関するアンケート」に記入できます。試験の管理運営に関するアンケートは問題冊子の裏面にあります。アンケートの回答は解答用紙の表面の特別コードセクション（グリッド No.4）の P ~ S 欄に記入してください。

試験会場の状態と試験自体を含む試験の管理運営に関してさらに意見または懸念事項がある場合は、書簡または電子メール (exam@isaca.org) にて ISACA 国際本部までご連絡ください。これらの意見または懸念事項は、試験日から 2 週間以内に ISACA に届くようにする必要があります。連絡する際には、受験者の ID 番号、試験会場、試験日、および特定の問題の関連情報を記入するようにしてください。試験実施後 2 週間以内に ISACA が受け取った意見のみが試験の最終採点プロセスで考慮されます。

受験票

CISA 試験日の大体 2 ~ 3 週間前に、ISACA から受験票および電子受験票 (e-ticket) が送付されます。受験者は、Web サイト (www.isaca.org) の MyISACA ページで受験票をダウンロードすることもできます。受験票には試験日、受付時間および試験会場、当日のイベントのスケジュールと CISA 試験に持参しなければならない物が記載されています。連絡先情報を変更する場合を除き、受験者は受験票に何も記入しないことになっています。

注: 受験票を受け取るには、受験料を支払う必要があります。受験票は、記録されている現在の郵送先と電子メールアドレス宛に、ハードコピーと電子メールで送られます。受験票、および政府機関によって発行されている有効な身分証明書を持つ受験者のみに受験が許可されます。さらに、受験票の氏名が政府機関によって発行されている身分証明書の氏名と一致している必要があります。ハードコピーの受験票、または印刷した電子受験票のいずれも有効です。住所および / または電子メールアドレスが変更になった場合、ISACA のウェブサイト (www.isaca.org) でプロフィールを更新するか、exam@isaca.org にご連絡ください。

受験票に記載されている所定の受付時間および試験開始時間を必ず確認してください。試験が開始される約 30 分前に主任試験官が口頭で試験の説明を始めると、試験会場への入場はできません。口頭での試験説明が始まった後で試験場に到着した受験者は受験することができず、登録料は払い戻しできません。受験票は指定された試験会場でのみ有効です。身分証明書は試験中に確認されます。

特別措置

要求があれば、ISACA は文書による身体障害、宗教上の理由の証明のある受験者の申請に応じて受験方法に特別の措置をすることができます。こういった受験者は、試験の形式、説明方法、試験会場での飲食物、スケジュールに関して妥当な変更を希望できます。試験会場での飲食物の申請が医師の注意書きと一緒に提出される以外は、場内ではいかなる飲食も禁止されています。特別措置を申請する場合は、2012 年 6 月の試験では 2012 年 4 月 4 日までに、2012 年 12 月の試験では 2012 年 10 月 3 日までに、関連書類を添えて書面の申請書を ISACA の国際本部に提出してください。

注記

登録は、受験票に記載されている時間に各会場で開始されます。主任試験官が口頭で試験の説明を始めたときには、すべての受験者は受付を済ませており、試験会場内にいる必要があります。試験が開始される約 30 分前に主任試験官が口頭で試験の説明を始めると、試験会場への入場はできません。

受験者のためのCISA®試験と認定ガイド

必ず受験票を持参してください

受験票（電子受験票またはハード・コピーの受験票）は指定された試験会場でのみ有効です。有効な受験票と身分証明書（ID）がないと試験会場には入れません。有効な身分証明書とは、受験票にあるのと同じ氏名で政府機関によって発行されている、写真付きの有効なオリジナルの身分証明書です。手書きの ID 情報は認められません。上記の条件すべてが 1 つの身分証明書に含まれていなければなりません。例としては、パスポート、運転免許証、軍隊 ID、州発行 ID、グリーンカードやナショナル ID などがあり、しかしそれに限定されません。有効な身分証明書を持たない受験者は受験することができず、登録料金は払い戻しされません。

試験会場の規則の遵守

- 口頭での試験の説明が始まると、試験会場への入場はできません。
- 削ってある数本の HB(軟鉛)鉛筆とよく消える消しゴムを持参してください。試験会場には鉛筆と消しゴムは用意されていません。試験会場はさまざまに異なるため、各試験会場の受験票をダウンロードが快適になるようあらゆる努力が払われます。受験者は各自で都合のよい着物を準備してください。
- 参考資料、白紙の用紙、メモ帳、または言語辞書を試験会場に持ち込むことはできません。
- 試験会場への電卓の持ち込みや使用はできません。
- 受験者は、いかなる種類の通信機器（携帯電話、PDA、ブラックベリーなど）も試験会場に持参してはなりません。試験実施中に受験者がこのような機器を持っていることが確認された場合、受験は無効となり、直ちに試験会場から退去するように求められます。
- 同伴者は試験会場に入れません。
- 試験会場での飲食は禁止されています（ISACA から事前の許可を得た場合は除く）。

不正行為

試験実施中に助けを与える / 受ける、メモや書類その他の資料を使用する、他の人になりすまして受験する、携帯電話を含む各種の通信機器を使用する、あるいは試験会場から試験問題、解答用紙、メモを持ち出すなどの不正行為が発覚した場合、その受験者は受験資格を失うことになり、法的措置の対象となる場合もあります。受験者が許可なく、または試験官に同伴されることなく試験室を出た場合、その受験者は試験室に戻ることはできず、受験資格を失うこととなります。試験の代理機関は、そのような行為について ISACA の CISA 認定委員会に報告します。

所持品に関する規定は、www.isaca.org/cisabelongings をご覧ください。ISACA も試験の代理機関も、受験者の所持品について責任を負うことはありません。

解答用紙の記入に関する注意点

- 試験開始前に、試験会場の主任試験官が口頭で解答用紙への ID 情報の記入について説明します。受験票に記載されている受験者の ID 番号などの必要な情報を正しく記入しないと、採点の遅延や間違いが発生する可能性があります。
- 各試験会場には、その他の主要言語を話せる試験官が配置されています。試験会場における主要言語以外の言語で受験することを希望しても、試験官がその言語に精通していない場合があります。ただし、書面による説明は受験する試験の言語で記載されています。
- 受験者は問題に解答する前にすべての説明をよく読んで理解するように指示されます。指示を読み飛ばしたり、速く読みすぎたりすると、重要な情報を見逃して不合格になる恐れがあります。
- 試験の解答は、解答用紙の適切な解答欄にマークする形式で行われます。1 問で複数の解答をマークしないように注意し、適切な解答行の問題に解答していることを確認してください。解答を変更する場合、間違った解答を完全に消してから新しい解答をマークしてください。
- すべての問題に解答する必要があります。解答を間違えても減点はされません。成績は正解した問題数でのみ計算されるので、未解答の問題がないようにしてください。
- 解答し終わったら、解答用紙と問題冊子を提出してください。

試験時間の配分

- 試験は 4 時間あるので、1 問につき 1 分強の時間があります。すべての試験問題に解答できるようにペース配分することをお勧めします。そのためには、1 時間あたり平均 50 問を解答する必要があります。
- 解答はすぐに解答用紙に記入してください。試験終了後に、問題冊子にマークした解答をマークして、後から解答用紙に転記するような時間はありません。

適切な行為

- 試験のセキュリティ保護や得点の正当性維持のために、受験者は解答用紙に署名する必要があります。
- CISA 認定委員会には、他人を助ける / 他人から助けを受ける、メモや書類その他の資料を使用する、他の人になりすまして受験する、試験教材やメモなどを試験会場から持ち出そうとするなどの不正行為または試験規則違反をしていることが発覚した受験者を失格にする権利があります。試験の代理機関は、そのような行為に関する記録を CISA 認定委員会に提出し、委員会による検討・裁定を待つものとします。

受験者のためのCISA® 試験と認定ガイド

失格または資格剥奪となる理由

- 試験会場に不正に入場する。
- 妨害行為や助けを与える / 受けるなどの行為を行う。
- 試験教材やメモなどを試験会場から持ち出そうとする。
- 他の受験者になりすまして受験する。
- 許可されていない物を試験会場に持ち込む。
- 試験実施中に受験者が通信機器（携帯電話、PDA、ブラックベリー® など）を所持している
- 受験者が許可を得ずに試験室から退去する

受験者が試験実施中に通信機器（例：携帯電話、PDA、ブラックベリー®）を所持していることが確認された場合、受験が無効となり、直ちに試験会場から退去するように求められます。

CISA 試験の採点

CISA 試験は多肢選択方式の 200 項目で構成されています。受験者の得点は段階評価スコアで通知されます。段階評価スコアは受験者の試験における実際の得点を共通の基準に変換したものです。ISACA は 200 点 ~ 800 点のスコアにより通知します。例えば、段階評価スコアで満点の 800 点は、すべての問題に正解したことを表し、最低点の 200 点は、ほとんどの問題に正解できなかったことを表します。試験に合格するには 450 点以上の得点が必要になります。450 点は安定した水準の知識が最低限あることを示す得点で、CISA 認定委員会により設定されたものです。合格点を得た受験者は、他の要件がすべて満たされていれば、これにより資格申請が許されます。

CISA 試験には研究および分析目的でのみ含まれている問題があります。これらの問題は他の問題と区別なく出題されていますが、最終的な得点の計算には使用されません。

試験日から約 8 週間後に、正式な試験結果が受験者に郵送されます。また、受験者が出願時に同意している場合、受験者に対し、合格の可否と得点を記した電子メールが送られます。この電子メールでの通知は、結果が最初に発表された時点で受験者のプロフィールに記載されているアドレスにのみ送られます。得点の機密を確保するために、電話あるいは FAX による試験結果のお問い合わせには応じられません。電子メールでの通知がスパムフォルダに入ってしまうのを防ぐために、アドレスブック、ホワイトリスト、または安全な送信者リストに exam@isaca.org を加えておいてください。

受験者には、各ドメイン分野のサブスコアが記載されているスコア・レポートが送られます。合格者には、採点表と共に、CISA 認定の申込み方法の説明書が送られます。

サブスコアは、不合格者が試験を再受験する前にどの分野を勉強する必要があるのかがわかるので有用です。不合格の受験者は、段階評価スコアの合計がサブスコアの単純平均または加重平均で計算されていないことに注意してください。

不合格だった場合、自分の解答用紙を請求できます。この手続きにより、マーク・ミスや複数解答や、その他コンピュータの採点を阻害する要素がなかったことを確認できます。ただし、すべての得点は通知前に複数の品質管理チェックを受けることになっており、得点が変わる可能性は低いことをご理解ください。試験結果の発表から 90 日以内に書面で認定部門に採点内容を請求する必要があります。締切日を過ぎてから採点内容を請求しても処理されません。請求の際には、受験者の名前、試験の ID 番号およびメール・アドレスが必要です。要求の際には、1 回ごとに US \$75 の費用が必要になります。

CISA 試験の問題の種類

CISA 試験の問題は、実践的な知識と一般的な概念や基準の適応力をテストし評価することを目的に開発されています。すべての問題には 1 つの最適な解答が設定されています。

CISA の各問題は、問題文と解答の選択肢で構成されています。受験者は、正しいまたは最適な解答を選択肢の中から選びます。問題文は、質問形式または穴埋め形式になります。シナリオが記載されていることもあります。通常、このような問題には状況の説明があり、受験者は提供されている情報に基づいて 2 つ以上の問題に解答します。受験者は各問題をよく読んでください。CISA 試験の問題では、**最もふさわしい**や**最適**などの修飾語に基づいて適切な解答を選択しなければならないこともあります。どのような場合でも、受験者は問題をよく読み、不正解だとわかっている解答を消去し、最適な選択をする必要があります。CISA 試験の問題については、www.isaca.org/cisaassessment をご覧ください。

受験者のためのCISA®試験と認定ガイド

CISA の資格申請

受験者は試験に合格しただけでは、CISA 資格を取得できません。CISA 試験に合格したら、試験日から 5 年間以内に資格申請を行う必要があります。合格した受験者は、資格申請書を記入し、申請書の適切なフォームを使用して実務経験を証明する必要があります。記入済みの資格申請書の受領および承認が完了するまでは、受験者は認定されていないため CISA の認定資格を使用することはできません。認定申請が承認されなかった件に対する異議申立てのプロセスがあるため、申請に関する決定は最終的なものではないことに注意してください。認定却下に関する照会は、certification@isaca.org に送ることができます。CISA に認定されると、証明書と CISA 認定バッジが届きます。CISA のステータスを掲載、または別の方法で公表する権利（義務ではない）が ISACA にあることを申請時に承諾する必要があります。CISA の資格申請には、US \$50 の手数料が必要になります。

CISA 資格の認定要件

CISA 試験に合格し、次の実務経験の要件を満たすことで資格が認定されます。

資格を取得するには、情報システムの監査、コントロール、保証またはセキュリティの専門家としての実務経験が最低 5 年間は必要になります。実務経験の代替や免除は次のようにして得ることができます。

- 最高 1 年間の情報システムまたは 1 年間の非情報システム監査経験は、1 年間の経験の代替とすることができる。
- 取得した 60 から 120 単位の大学の履修単位（2 年または 4 年の学位）は 10 年以内という規則に制限されることなく、1 年または 2 年の経験の代替とすることができる。複数の学位がある場合でも、申告できるのは最大で 2 年間です。
- ISACA が後援するモデルカリキュラムを実施している大学の学士号ないし修士号は、経験 1 年に替えることができる。該当する大学のリストは、www.isaca.org/modeluniversities でご覧ください。3 年の経験代替と教育免除が既に申告されている場合、このオプションは利用できません。
- 認定された大学からの情報セキュリティまたは情報技術の修士号は、1 年間の経験に代替とすることができる。

例外：関連した分野（例えば、コンピュータサイエンス、経理、情報システム監査）での 2 年間の常勤大学講師としての経験は、それぞれの分野における 1 年間の経験の代替とすることができます。

実務経験は、CISA の資格申請日から遡って 10 年以内、または試験の初回合格日から 5 年以内のものでなければなりません。試験の合格日から 5 年以内に CISA 認定資格の申請を行わないと、試験を再受験して合格する必要があります。

多くの方が実務経験の要件を満たす前に CISA 試験を受験しているという点にご注目ください。すべての要件を満たすまでは CISA の認定資格は得られませんが、こういった受験は認められており、また奨励されています。

CISA 資格維持の要件

CISA 資格保有者がその資格を維持するには、次の要件を遵守する必要があります。

- 年間最低 20CPE 時間を達成してその報告を行い、3 年間の報告期間で最低でも 120 CPE 時間を達成し、その報告を行います。詳細については、CISA CPE 継続プロフェッショナル教育 (CPE) 指針 (www.isaca.org/cisacpepolicy) を参照してください。
- ISACA 国際本部に CPE の年間継続維持料を全額支払うこと。
- 年次の監査対象に選ばれた場合、報告した時間を立証するために CPE 活動の必要書類を記入して提出すること。
- ISACA 職業倫理規定を遵守すること。

この一般要求事項を守れない場合には、CISA の認定資格が取り消されます。認定書はすべて、ISACA が保有します。ある受験者が認定を受けた後、資格を取り消された場合、認定書を破棄しなければなりません。

ISACA 職業倫理規定

ISACA では、協会の会員および / または当該資格保有者のプロフェッショナルまたは個人としての行動規範となる職業倫理規定を定めています。この職業倫理規定に違反すると、会員および / または資格保有者の行為が調査され、最終的に懲戒処分となる場合があります。ISACA 職業倫理規定は、www.isaca.org/ethics で確認できます。

CISA 資格の取り消し

CISA 認定委員会は、十分な検討の上で、以下のいずれかの理由から、個人の CISA 認定を取り消す権利を有します。

- CISA CPE 規則に違反した
- ISACA 職業倫理規定の条項に違反した
- 関連情報の改ざんまたは故意による隠蔽を行った
- 重要事実の虚偽表示を故意に行った
- CISA 試験または認定プロセスに関連する時期に、不誠実、不正または不適切な行為に関与したり、支援を行ったりした

受験者のためのCISA®試験と認定ガイド

CISA 職務領域の説明

CISA のタスクと知識項目

内容分野（ドメイン）
ドメイン 1：情報システム監査のプロセサー 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。
ドメイン 1：タスク項目
T1.1 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。
T1.2 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。
T1.3 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。
T1.4 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。
T1.5 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。
ドメイン 1：知識項目
KS1.1 ISACA 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
KS1.2 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
KS1.3 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
KS1.4 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
KS1.5 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
KS1.6 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
KS1.7 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
KS1.8 様々なサンプリング方法論に関する知識
KS1.9 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
KS1.10 監査品質保証システムとフレームワークに関する知識
ドメイン 2：IT ガバナンスとマネジメント 目標を達成し、組織の戦略を支援す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。
ドメイン 2：タスク項目
T2.1 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。
T2.2 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、それら进行评估すること。
T2.3 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进行评估すること。
T2.4 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、それら进行评估すること。
T2.5 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。
T2.6 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、それら进行评估すること。
T2.7 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、それら进行评估すること。
T2.8 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、それら进行评估すること。
T2.9 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。
T2.10 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。
T2.11 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。
ドメイン 2：知識項目
KS2.1 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
KS2.2 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
KS2.3 IT に関連する組織の構造、役割、及び責任に関する知識
KS2.4 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
KS2.5 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

受験者のためのCISA®試験と認定ガイド


内容分野（ドメイン）
ドメイン 2：知識項目（続き）
KS2.6 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
KS2.7 品質管理システムに関する知識
KS2.8 成熟度モデルの活用についての知識
KS2.9 プロセス最適化技法に関する知識
KS2.10 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）
KS2.11 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（第三者外部委託先との関係を含む）に関する知識
KS2.12 企業リスク管理に関する知識
KS2.13 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]）
KS2.14 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
KS2.15 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
KS2.16 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
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。
ドメイン 3：タスク項目
T3.1 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。
T3.2 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。
T3.3 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。
T3.4 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。
T3.5 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。
T3.6 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。
ドメイン 3：知識項目
KS3.1 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
KS3.2 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
KS3.3 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
KS3.4 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
KS3.5 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
KS3.6 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
KS3.7 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
KS3.8 プロジェクトの成功基準とリスクに関する知識
KS3.9 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
KS3.10 システム開発手法とツール（例：アジャイル開発業務、プロトタイプング、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
KS3.11 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
KS3.12 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
KS3.13 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
KS3.14 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

受験者のためのCISA® 試験と認定ガイド

内容分野 (ドメイン)
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。
ドメイン 4：タスク項目
T4.1 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。
T4.2 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。
T4.3 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。
T4.4 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。
T4.5 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。
T4.6 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。
T4.7 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。
T4.8 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。
T4.9 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。
T4.10 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。
T4.11 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。
ドメイン 4：知識項目
KS4.1 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
KS4.2 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
KS4.3 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
KS4.4 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
KS4.5 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
KS4.6 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
KS4.7 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
KS4.8 データベース管理業務に関する知識
KS4.9 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
KS4.10 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
KS4.11 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
KS4.12 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
KS4.13 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
KS4.14 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
KS4.15 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
KS4.16 災害復旧計画の策定と維持に関する知識
KS4.17 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
KS4.18 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
KS4.19 災害復旧テストの方法に関する知識
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。
ドメイン 5：タスク項目
T5.1 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。

受験者のためのCISA® 試験と認定ガイド

内容分野 (ドメイン)
ドメイン 5: タスク項目 (続き)
T5.2 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。
T5.3 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、それら进行评估すること。
T5.4 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。
T5.5 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。
ドメイン 5: 知識項目
KS5.1 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
KS5.2 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
KS5.3 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
KS5.4 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
KS5.5 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
KS5.6 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
KS5.7 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
KS5.8 情報システムの攻撃方法及び技法に関する知識
KS5.9 検出ツール及びコントロール技法 (例: マルウェア、ウイルス検出、スパイウェア) に関する知識
KS5.10 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
KS5.11 データ漏洩のリスクとコントロールに関する知識
KS5.12 暗号化関連の技法に関する知識
KS5.13 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
KS5.14 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
KS5.15 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
KS5.16 音声通信のセキュリティ (例: PBX、VoIP) に関する知識
KS5.17 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
KS5.18 データ分類基準及び対応手順に関する知識
KS5.19 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
KS5.20 環境面の保護のための機器及び対応業務に関する知識
KS5.21 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



2012年度 CISA 試験の準備をしよう

2012年度公認情報システム監査人（CISA）試験の準備と職業能力の 開発のためのレビュー資料

Certified Information Systems Auditor®（CISA®）試験に合格するには、学習計画を立案すべきです。受験者が学習計画をうまく立案することができるように、情報システムコントロール協会は、学習のための資料とレビューコースを提供しています。以下のものが含まれます。

学習のための教材

- 2012年公認情報システム監査人(CISA®)レビューマニュアル
- 2011年CISA® 試験サンプル問題&解答・解説集
- 2011年CISA® 試験サンプル問題&解答・解説集(追補版)
- 2012年CISA® 試験サンプル問題&解答・解説集(追補版)
- CISA® Practice Question Database v12

ご注文はwww.isaca.org/cisabooks にて承ります。

レビューコース

- 支部主催レビューコース(www.isaca.org/cisareview)
- CISA® オンラインレビューコース(www.isaca.org/elearning)