ISACA認定試験受験者ガイド

目次

受験者ガイドの概要

このガイドをよくお読みください。このガイドには、ISACA試験の受験者が受験申し込みの前に知っておくべき重要な情報（スケジュール情報、受験資格、試験日の規則など）が記載されています。

このガイドではISACA認定試験受験に必要なすべての情報を、以下の4つの主要なセクションで説明しています。

- 公認情報システム監査人（CISA）
- 公認情報システムリスク管理者（CRISC）
- 公認情報セキュリティマネージャー（CISM）
- 公認ITガバナンス専門家（CGEIT）
- 公認データプライバシーソリューションエンジニア（CDPSE）

セクションI：はじめに

1.1 ISACAの概要と倫理規定

ISACAは、個人や事業体が技術のポジティブな可能性を達成できるよう支援する国際的な団体です。

ISACAは、専門家がキャリアを発展させ、組織を変革できるように、知識、資格、教育、コミュニティを提供します。

ISACAは、情報セキュリティ、ガバナンス、保証、リスク、プライバシー、品質などのデジタルトラスト分野で働く18万5千人以上の会員と、外郭団体のCMMI® Instituteの専門的能力を活用し、テクノロジーによるイノベーションの推進を支援しています。

ISACAは世界190か国で事業を展開し、全世界に230を超える支部を擁し、アメリカと中国に事業所を構えています。

ISACAの製品とサービス

メンバーシップ

ISACA会員になると会員限定特典を利用でき、認定試験、セミナー、受験対策資料などでISACA製品の割引を受けられます。

リソース

標準やベストプラクティス、新たなトレンドについて、最新の研究、ガイダンス、エキスパートの意見をご覧ください。

トレーニング

世界的に評価の高いISACAのトレーニングと認定プログラムは、自信を高め、キャリアアップと職場の改革に役立ちます。

COBIT 2019®

COBITは、事業体の情報技術ガバナンスの調整と規模の最適化に役立つ、ISACAの実績あるフレームワークです。

認定プログラム

ISACAの認定プログラムの一覧については、https://www.isaca.org/credentialingをご覧ください。

認定プログラム

IT監査、セキュリティおよびコントロールにおける経験と知識を実証し、キャリアアップと昇給を促進します。

CISA、CPA、CIAの保有者を対象とする、監査に特化した初の上級AI認定資格です。

上級管理者へのキャリアアップを促し、戦略的観点から事業体に貢献します。

CISMおよびCISSPの保有者を対象とする、AIを中心とした初のセキュリティ管理認定資格です。

事業体のIS/ITリスク管理およびコントロールの分野でキャリアを伸ばし、昇進と昇給を促進します。

プライバシーの専門家としてプライバシーを導入し、設計を実装する能力を評価します。

事業体の戦略的ガバナンスにおける専門知識を実証し、経営幹部レベルで存在感を示します。

サイバーセキュリティプロフェッショナルが雇用主に対して実践的な能力を証明できるようにします。

倫理規定

ISACAでは会員や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。

- 会員および認定された者は、ISACAの倫理規定を遵守する必要があります。
- これを遵守しない場合は調査が行われ、試験スコアの無効化や認定資格の取り消しなどの懲戒処分となる場合があります。

1.2 ISACA認定プログラムの概要

以下の表は、本ガイドで扱う5つのISACA認定資格の概要を示しています。

	CISA Certified Information Systems Auditor. An ISACA® Certification	CRISC Certified in Risk and Information Systems Control. An ISACA® Certification	CISM Certified Information Security Manager. An ISACA® Certification	CGEIT Certified in the Governance of Enterprise IT. An ISACA® Certification	CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification
説明	IT/情報システム監査人、コントロール、保証、および情報セキュリティの専門家向け	ITリスクマネジメント、および情報システムコントロールの設計、導入、監視、保守の経験を有する担当者向け	事業体の情報セキュリティ機能を管理、設計、監督、評価する担当者向け	事業体のITガバナンスの原則と実践（プラクティス）に関する知識を持ち、実務に応用してきた幅広い専門家を認定	データプライバシーのガバナンス、アーキテクチャ、ライフサイクルに関する技術レベルの経験を有する担当者向け
必要な経験	情報システム/IT監査、コントロール、アシュアランスまたはセキュリティで5年以上の実務経験を持つこと。 最大3年間の実務経験の免除の適用が可能です。	ITリスク管理と情報システムコントロールで3年以上の実務経験を持つこと。 適用可能な免除期間や代替条件はありません。	情報セキュリティ管理で5年以上の経験を持つこと。 最大2年間の免除の適用が可能です。	アドバイザーや監督の役割、または企業でのIT関連のガバナンスのサポートで5年以上の経験を持つこと。 適用可能な免除期間や代替条件はありません。	データプライバシーガバナンス、プライバシーリスク管理およびコンプライアンス、プライバシーエンジニアリング、および/またはデータライフサイクル業務で3年以上の経験を持つこと。 適用可能な免除期間や代替条件はありません。

ドメイン（%）	**ドメイン1** – 情報システム監査プロセス（18%） **ドメイン2** – ITのガバナンスと管理（18%） **ドメイン3** – 情報システムの調達、開発、導入（12%） **ドメイン4** – 情報システムの運用とビジネスレジリエンス（26%） **ドメイン5** – 情報資産の保護（26%）	**ドメイン1** – ガバナンス（26%） **ドメイン2** – リスクアセスメント（22%） **ドメイン3** – リスク対応および報告（32%） **ドメイン4** – テクノロジーとセキュリティ（20%）	**ドメイン1** – 情報セキュリティガバナンス（17%） **ドメイン2** – 情報セキュリティリスク管理（20%） **ドメイン3** – 情報セキュリティプログラム（33%） **ドメイン4** – インシデント管理（30%）	**ドメイン1** – 事業体のITガバナンス（40%） **ドメイン2** – ITリソース（15%） **ドメイン3** – 利益の実現（26%） **ドメイン4** – リスク最適化（19%）	**ドメイン1** – プライバシーガバナンス（20%） **ドメイン2** – プライバシーリスク管理とコンプライアンス（18%） **ドメイン3** – データライフサイクル管理（23%） **ドメイン4** – プライバシーエンジニアリング（39%）
試験言語					
試験時間	4時間（240分）、150問の多肢選択問題	4時間（240分）、150問の多肢選択問題	4時間（240分）、150問の多肢選択問題	4時間（240分）、150問の多肢選択問題	3.5時間（210分）、120問の多肢選択問題

受験料

受験料は、試験登録時の会員ステータスに応じて異なり、以下のようになります。

- ISACA会員：575米ドル
- ISACA非会員：760米ドル

受験登録料の払い戻しおよび譲渡はできません。

リソース

以下は、ISACA認定試験の受験者に役立つリンクとリソースです。

CISA認定

- CISA試験内容の概要
- CISA試験への準備
- CISA試験に関する情報
- CISAアプリケーション要件
- CISA保守要件

CRISC認定資格

- CRISC試験内容の概要
- CRISC試験への準備
- CRISC試験に関する情報
- CRISCアプリケーション要件
- CRISC保守要件

CISM 資格

- CISM試験内容の概要
- CISM試験への準備
- CISM試験に関する情報
- CISMアプリケーション要件
- CISM保守要件

CGEIT 資格

- CGEIT試験内容の概要
- CGEIT試験への準備
- CGEIT試験に関する情報
- CGEIT アプリケーション要件
- CGEIT保守要件

CDPSE 認定

- CDPSE試験内容の概要
- CDPSE試験への準備
- CDPSE 試験に関する情報
- CDPSE アプリケーション要件
- CDPSE 保守要件

セクションII：試験の登録と予約

2.1 登録する前に

ISACA認定試験はコンピュータを使用し、世界各地の認可されたPSI試験会場で、または試験官付リモート試験として実施されます。試験登録は継続的に行われています。つまり、受験者はいつでも登録でき制限はありません。受験者は受験料を支払って48時間後から試験の予約を行えます。

登録すると、受験者は6か月間の受験資格が得られます。つまり、登録日から6か月間（182日間）、試験を受けることができます。試験の予約と受験の前に、受験料をすべて支払う必要があることにご注意ください。

受験にさらに時間が必要な場合は、75米ドルで6か月間延長できます。受験資格の延長オプションは、受験資格の有効期限の30日前からダッシュボードに表示されます。試験が予約されている場合、受験資格を延長するには、試験日の48時間前までに試験をキャンセルしなければなりません。試験の延長は2回まで可能です。

予約した試験を受けなかったり、試験の時間に15分以上遅れたりなど、6か月間の受験可能期間に試験を受けなかった場合、受験資格がなくなり、受験料は払い戻しできません。

2.2 試験に登録する

以下の手順に従い、オンラインで試験登録を行ってください。

ステップ	アクション
1.	認定試験を選択します：CISA | CRISC | CISM | CGEIT | CDPSE
2.	ログインするかアカウントを作成します。 注：アカウント作成時の氏名は、試験日に提示する政府発行の身分証明書に記載した氏名と同じになるようにしてください。有効な身分証明書については、試験日の規則を参照してください。

ステップ	アクション
	試験に登録する前に、お近くのPSI試験会場に空きがあることを確認するか、リモート受験用の対応デバイスを用意する必要があります。デバイスをテストするには、この互換性チェックを完了してください。会社のデバイスを使用して受験する場合、IT部門の支援または承認が必要になる場合があります。
3.	登録プロセスを完了します。

注意：受験者は、試験の登録プロセス中に、ISACAの利用規約の第16項「試験」に同意しなければなりません。受験者は、本受験者ガイドに記載されている試験の実施、認定基準、試験結果発表に関する規定にも同意する必要があります。

受験料をすべて支払うまで、試験の予約はできません。受験料の**払い戻し**および**譲渡はできません。**

登録の確認

受験者には、登録および支払いの後、1営業日以内に**予約通知**Eメールが届きます。このEメールには、試験予約のスケジュール情報が表示されます。

特別措置

特別な試験措置を受けるには、登録手続き時に要求し、試験を予約する前にISACAの承認を得る必要があります。

特別措置受験をご希望の方は、次の手順に従ってください。

ステップ	アクション
1.	試験登録プロセスで、特別措置要求フィールドに*チェック*をつけてください。
2.	特別措置申請書を印刷します。
3.	ISACA特別措置申請書に必要事項を記入します。 **注：この申請書には、受験者本人と受験者の医療専門家が記入する必要があります。**
4.	フォームをISACA（support.isaca.org）に送信します。

特別措置の申請は、受験料をすべて払い終えるまで、検討されません。申請はすべて、ご希望の試験日の*4週間前までに*ISACAに送付する必要があり、その1回の試験にのみ有効です。

登録内容の変更

受験者が申請する一般的な登録内容の変更は次の3つです。

変更の種類	ステップ
氏名	ISACAアカウントに登録した名前は、試験のチェックインに使用するIDに記載する名前に一致しなければなりません。 名前を更新するには、次の手順を実行します。 1. www.isaca.org/myisacaでログインします。 2. 赤い「**MY ISACA PROFILE（自分のISACAプロファイル）**」ボタンをクリックします。 3. 必要な変更を行います。 4. 「**Save（保存）**」をクリックします。
試験言語	希望の受験言語を変更するには、次の手順を実行します。 1. https://www.isaca.org/myisaca/certificationsでログインします。 2. 「**Re-Schedule or Cancel Exam（試験の予約変更またはキャンセル）**」リンクをクリックして、PSIの予約ページに進みます。 3. 画面上の指示に従って試験予約をスケジュールします。（予約ガイドで、予約および予約変更に関する情報を確認できます。） **注：試験言語を変更する必要がある場合は、試験予約も変更する必要があります。**詳細は、試験の予約変更を参照してください。
試験の種類	試験の種類の変更をご希望の場合は、ISACAサポート（support.isaca.org）まですぐにご連絡ください。

すべての変更申請は、受験を予約した試験の48時間前までに完了する必要があります。

2.3 受験予約

資格

試験の予約および受験には受験資格が必要です。受験資格は、試験登録をすると得られ、6か月間（182日間）有効です。

試験を予約し受ける前に、試験登録と支払いを済ませる必要があります。受験料の払い戻しおよび譲渡はできません。

6か月間の受験資格期間中に受験予約して受験しないと、受験料を放棄することになります。資格の延期は、受験資格延期の支払い手続きを済ませない限り認められません。

受験予約

受験予約の主なステップは、次の5つです。

ステップ	アクション
1.	お使いのISACAアカウントにログインします。
2.	「**Certification & CPE Management（認定およびCPE管理）**」をクリックします。
3.	「**Schedule Your Exam（試験を予約）**」または「**Visit Exam Website（試験ウェブサイトにアクセス）**」をクリックします。これにより、PSIダッシュボードに移動します。
4.	PSIダッシュボードで「**Schedule Exam（試験を予約）**」をクリックします。
5.	予約ガイドに記載されている手順に従ってください。

試験予約が完了すると、no-reply@psiexams.comから試験予約の確認Eメールが届きます。追加のサポートが必要な場合は、予約ガイドをご覧ください。

試験予約は90日前にならないと行うことはできません。90日より前の受験可能な試験会場または試験日が分からない場合は、希望する試験日により近い日付を遡って確認してください。

それでも希望する受験可能な試験会場または試験日が分からない場合は、ISACAアカウントにログインして「Certification & CPE Management（認定およびCPE管理）」タブをクリックし、受験資格が期限切れになっていないことを確認してください。

試験の予約変更

当初予約した試験から48時間以上前であれば、ペナルティなしで、同じ受験資格期間内で予約を変更できます。予約した試験から48時間以内の場合は、受験する必要があります。受験しないと受験料を放棄することになります。試験予約を変更するには、ISACAアカウントにログインし、予約ガイドに記載されている予約変更手順に従ってください。

試験会場の緊急閉鎖

悪天候や緊急事態により、予約されていた試験のキャンセルが必要になった場合には、PSIは電話またはEメールにて受験者への連絡を試みます。ただし、ISACAは、www.psiexams.comにアクセスし、試験会場が閉鎖されていないか確認されることをお勧めします。試験会場が閉鎖されている場合、試験予約は追加料金なしで変更されます。

セクションIII：試験準備

3.1 試験の準備をする

試験準備

ISACAの多様な試験準備リソースには、グループトレーニング、自分のペースで進められるトレーニング、そして各国語の試験教材があり、認定試験の準備に役立てられます。

試験問題

試験問題は、実用的な知識と、一般的な概念や基準の適用を評価およびテストすることを目的として作られています。すべての問題は最適な解答を1つ選ぶように作られています。

- どの問題にも問題文と4つの選択肢があります。
- それらの選択肢から正しい解答または最適な解答を選んでください。
- 試験問題は、質問形式または記述の穴埋めの形式です。

シナリオが含まれる場合もあります。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。

試験問題の種類とその開発方法の詳細については、「項目記述要件およびリソース」を参照してください。

試験のヒント

- 各問題を注意深く読んでください。問題では、「MOST likely（最も可能性が高い）」や「BEST（最も適切）」などの修飾語に基づいて解答を選ぶことが求められる場合があります。
- 誤りと分かっている選択肢を消去し、最も適切な選択肢を選んでください。
- 試験会場にログインしてから試験開始までの間に、受験体験に関するチュートリアルが提供されます。重要な情報を見逃さないように、チュートリアルに細心の注意を払ってください。
- すべての問題に解答してください。

- 誤答に対するペナルティはありません。採点は正解した問題の総数のみに基づいて行われますので、解答を空欄にしないでください。
- 時間を配分してください。試験全体を完了できるように自分のペースで解答してください。CISA/CRISC/CISM/CGEIT試験の所要時間は4時間、CDPSE試験の所要時間は3.5時間です。

試験会場での試験

試験会場での受験を予約した場合は、試験日の前に以下の準備を行ってください。

- 試験会場の住所と開始時刻を確認する
- 試験会場への経路を具体的に把握する
- 試験開始時間の30分前までに到着するよう計画する
- 所持品の保管方法を確認する

詳細は、試験日の規則を参照してください。

試験官付リモート試験

試験官付リモート試験に関する詳細は、リモート試験官ガイドをダウンロードしてください。

デバイスをテストするには、試験日の前に互換性チェックを完了しておいてください。会社のデバイスを使用して受験する際には、必要に応じて、セキュアブラウザをダウンロードするためにIT部門の支援または承認が必要になる場合があります。

身分証明書の提示

試験会場に入るか、オンライン試験にチェックインするには、所定の形式の身分証明書（ID）を提示する必要があります。所定の形式の身分証明書は、次の情報を含む、最新かつ有効の、政府発行の身分証明書の原本でなければなりません。

- 受験者の氏名。身分証明書に記載されている氏名は試験の登録に使用した名前と一致しなければなりません。一致しない場合、入場を許可されないことがあります。
- 受験者の署名（日本で発行された署名のない運転免許証は許容されます）
- 受験者の写真

すべての情報は、単一の身分証明書によって証明されなければなりません（コピーや手書きは認められません）。**デジタルIDは許容されません。**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、受験料は払い戻しされません。

許容されるID形式

許容されるIDの形式：

- 運転免許証
- 州発行の身分証明書（運転免許証以外）
- パスポート
- パスポートカード
- グリーンカード
- 外国人登録証明書
- 永住カード
- 国民IDカード

試験会場側は確認のため、追加の身分証明書の提示を求める権利を有します。受験者の身元に関して疑いがある場合、受験は拒否され、ISACAにその旨が通知されます。これは無連絡欠席と見なされ、受験料は没収されます。今後受験する際には、再登録を行い、受験料を再度支払う必要があります。

3.2 試験日の規則

試験規則は、試験中に認められることに関するガイドラインです。試験規則は、PSI試験会場および試験官付リモート試験で実施される試験に適用されます。どのISACA試験に登録する場合も、受験者は利用規約に同意しなければなりません。かかる利用規約に従い、ISACAはいずれかの認められない行動が確認された場合に試験スコアを無効にする権利を有します。

禁止事項

試験中は、他のすべての物品および教材を完全に自分の身の回りから排除しなければなりません。試験官が試験セッションを適切に監視できるように、試験中は画面に顔を向ける必要があります。

試験中に以下のものを持ち込むことは禁止されています。

- 参考資料、学習教材、白紙の用紙、メモ、メモ帳、辞書、またはその他の補助器具
- 電卓
- マルチモニター
- あらゆる種類の通信用、監視用、または電子/記録用機器（以下を含むがこれらに限定されない）：
    - 携帯電話
    - タブレット
    - スマートウォッチまたはスマートグラス
    - ヘッドホン/耳栓

- ハンドバッグ、財布、ブリーフケースなど、あらゆる種類の手荷物
- 武器
- たばこ製品または電子たばこ
- 飲食物（水を含む。会場受験および試験官付リモート試験の両方に適用）
- 訪問者

試験実施中に受験者がこのような通信用、監視用、または電子/記録用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（該当する場合）。試験結果画面を含め、試験のいかなる部分のスクリーンショットや写真も撮ってはなりません。

私物の保管

受験者は、試験会場に持ち込む所持品を、ロッカー等の指定された場所に保管するようにする必要があります。試験を完了して提出するまでは、所持品にアクセスすることはできません。

認められない行動

利用規約に基づき、以下の行為は禁止されています。

- 混乱を起こす
- メモ、紙片、その他の補助器具や、許可されていない学習教材を用いて他の受験者を助けたり、助けられたりすること
- 私語、大声で問題文を読み上げること、無言で問題文を読みながら唇を動かすこと
- 試験内容をコピー、撮影、録画、記憶またはその他の手段で保持もしくは再現しようと試みること、あるいは何らかの目的で他者が試験内容を保持、再現または再構築することを支援すること
- 代理受験をしようとすること
- 通信用、監視用、または電子/記録用機器（携帯端末、タブレット、スマートグラス、スマートウォッチなど）を持ち込むこと
- 試験前、試験中または試験後に、口頭、書面、またはその他の情報伝達手段（インターネット、Eメール、オンラインフォーラムなど）を用いて、直接的または間接的に、任意の人物または組織に対し、試験内容を販売、ライセンス許諾、配布、交換、譲渡、共有、コメント、開示または伝達すること
- 許可を得ずに試験会場を離れる（再入室は許可されません）試験官の許可を得た上で、10分以内の休憩を2回入れることは許可されます。許可された休憩中、試験は一時中断となりますが、タイマーは止められません。
- 試験が終了する前に私物保管場所に保管した私物に近づく

個人的にやむを得ない事情に関するガイドライン

個人的にやむを得ない事情で予約した試験に出席できない受験者は、受験料を放棄しなくても、予約を変更できる場合があります。これを行うには、次の手順を実行します。

ステップ	アクション
1.	予約の72時間以内にPSIに連絡します。
2.	欠席の理由を確認するための書類をPSIに提出します。

PSIに連絡するには、次の手順を実行します。

ステップ	アクション
1.	https://www.psionline.com/test-takers/candidate-support-numbers/にアクセスします。
2.	検索フィールドに「ISACA」と入力します。
3.	利用可能な連絡先電話番号の一覧を確認して選択します。

個人的にやむを得ない事情の例として、以下のようなものがあります。

- 本人の病気
    - 医師の診断書、緊急治療室への入室許可証明書などの書類が必要：
        - 医師免許を持つ医師による署名と受診の日付が記載されている必要がある
        - 医師免許を持つ医師の連絡先が記載されている必要がある
        - 病気や緊急事態に関する詳細は不要
        - 病気や緊急事態を鑑み、この受験者は受験するべきではないという医師からの指示が記載されている必要がある
- 配偶者、子供/扶養家族、親、祖父母、兄弟姉妹を含む直近の家族の死亡
    - 死亡日、故人の氏名、および故人との受験者の関係が書類に記載されている必要がある
- 交通事故
    - 書類には、警察による事故証明、整備士またはレッカー会社からの領収書（日付と連絡先が記載されているもの）などが含まれる

個人的にやむを得ない事情の申請が拒否された場合、受験者は再度登録を行い、受験料を全額支払う必要があります。

試験エリアを離れる場合

受験者は、試験会場から退場するには、試験監督官の許可を得る必要があります。試験官付リモート試験の場合は、指定された試験エリアを離れる際は、許可を得る必要があります。許可なく試験会場または試験エリアを離れると、試験終了となる場合があります。

試験官の許可を得た上で、2回の休憩が認められます。許可された休憩中、試験は一時中断となりますが、タイマーは止められません。

離れる理由	指示
緊急事態	• 試験は一時的に停止されます。 • 緊急時であると確認されたら、試験は終了します。
施設を利用するため	• チェックアウトしてチェックインする必要があります。 • 会場を離れている間、試験時間を止めたり、時間を延長したりはできません。 • 1回ごとの休憩時間は10分以内とします。

結果

受験者が利用規約または試験日の規則に違反したり、何らかの不正行為を行ったりした場合、以下の処分の対象となります。

- 失格または資格剥奪
- 試験の無効化
- ISACA会員資格と、現在取得しているすべての認定の取り消し
- ISACA試験受験の禁止

3.3 試験の実施

試験は、PSI試験会場で実施することも、試験官付リモートで実施することもできます。

PSI試験会場

試験は、他の受験者と一緒の部屋で実施されることがあります。多少の雑音が予想され、それが通常のことと見なされる点にご留意ください。

PSI試験会場体験のビデオをご覧ください。

3.4 オンラインリモート試験官サービス

前述のように、ISACAでは、オンラインリモート試験監督サービスによる在宅受験も提供しています。この提供サービスを利用して受験する前に、リモート試験官ガイドをご確認ください。

受験者は、試験中にライブチャットツールを使ってリモートの試験官と英語でコミュニケーションを取ることができます。その他の言語は、リモートの試験官とのコミュニケーションには使用できません。

PSIオンラインリモート試験官サービス体験のビデオをご覧ください。

オンライン試験官サービスの試験規則

試験はオンライン、教科書持ち込み不可、リモート試験官付の方式で実施されます。試験官は、試験規則が守られていない場合、試験を中止します。いかなる形態の不正行為も容認されません。そのような行為を行った場合、試験は無効になり、返金は受けられません。

具体的には、試験中に下記の行為は許可されません。

- 試験中、室内に他の人がいること（他の人が立っていたり、試験エリアを通り抜けたりするなど）
- 休憩を取ること（試験官の許可なく離席するなど）
- カメラ、記録用機器、その他の電子機器（時計やメガネなどのスマートデバイスを含む）を使用すること
- コンピュータ画面や試験項目のスクリーンショットを撮ること
- 作業スペースに書類、本、メモなどの参考資料を持ち込むこと
- システムで他のプログラムやアプリケーションを使用すること（文書の表示、ブラウジング、リモートアクセス、Eメールへのアクセスなど）
- 試験の問題文を大声で読み上げたり、室内の他の人に話しかけたり、独り言を言ったりすること
- 試験内容をコピーしたり、書き留めたりすること
- カメラに覆いをかけたり、カメラの視界から離れたりすること（カメラの視野から少しでも外れると、試験官から警告がありますのでご注意ください）
- 飲食したり、ガムを噛んだりすること
- コンピュータ画面から目をそらすこと

注：上記の規則に従わない場合、試験は無効となり、受験料は没収されます。これらの要件についてご不明な点がある場合は、https://support.isaca.orgにアクセスしてISACAカスタマーエクスペリエンスセンターにお問い合わせください。

ISACAでは、各試験で室内スキャン後のミラーチェックを義務付けています。ミラーチェックの目的は、内蔵ウェブカメラを使った室内スキャンで映らなかった死角を試験官が確認できるようにすることです。ミラーチェックには、携帯用ミラーや携帯電話を使用できます。ミラーチェックでは、ウェブカメラにミラーをかざし、モニター/ノートパソコンの画面、キーボード、モニター/ノートパソコンの画面の四隅を映す必要があります。携帯電話を使用する場合は、ミラーチェックの終了後、試験用に指定された部屋の、手の届かない場所に携帯電話を置く必要があります。

セクションIV：試験終了後

このセクションでは、試験の採点と認定の申請について説明します。

4.1 試験の採点

得点の表示

受験者は、試験の完了直後に、暫定的な合否結果を画面上で確認することができます。試験結果画面を含め、試験のいかなる部分のスクリーンショットや写真も撮ってはなりません。正式な得点は、10営業日以内にEメールで送信されます。試験に合格した場合は、認定の申請方法に関する詳細が届きます。

- Eメール通知はプロファイルに記載されているメールアドレスに送信されます。
- オンライン結果は「MyISACA」>「Certification & CPE Management（認定およびCPE管理）」ページで確認できます。
- 試験の得点は、電話またはFAXでは提供されません。
- 問題別の結果は提供されません。

採点基準

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。段階評価の目的は、試験の異なるバージョン間で、結果を同じ基準で報告できるようにすることです。これによって、異なるバージョンを比較でき公平性が保たれます。

ISACAは評価スコアに200点～800点の共通基準を使用しています。ISACA試験は、採点項目とプレテスト項目で構成されています。プレテスト項目は、試験スコアの計算には使用されません。以下に、最低点、合格点、満点について概説します。

- 800点は全問正解の満点を表します。
- 200点は最低点を表し、少数の問題しか正解できなかったことを意味します。
- 受験者は、試験に合格するための最低合格基準として、450点以上のスコアを取得する必要があります。
- ドメインレベルごとの結果は参考用です。試験スコアは、ドメインに関係なく、正解した試験問題の総数に基づきます。ドメインごとの比率は、そのドメインの内容を反映する試験問題の割合を示すものであり、試験スコアの計算には使用されません。
- 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、認定申請することができます（詳細については「認定資格を取得するには」を参照してください）。

再採点の申請

ISACAは採点手順の完全性と妥当性に自信を持っていますが、試験に合格できなかった受験者は再採点を要請できます。再採点はPSIによって行われます。

受験者は、試験結果が公開されてから30日以内に、ISACAのサポートページから書面による再採点申請を提出する必要があります。

- 30日経過後の再採点申請は受理されません。
- すべての申請には、受験者の名前、ISACA ID番号およびEメールアドレスが必要です。
- 申請の際には、1回ごとに75米ドルの手数料がかかります。

4.2 再受験ポリシー

ISACAの認定試験の整合性を保護するため、ISACAは以下の再受験ポリシーを導入しました。

個人は12か月の期間内に、合格するまで4回試験を受けることができます。1回目の受験で合格しなかった受験者は、1回目の試験から12か月以内に、全部であと3回再試験を受けることができます。**受験者は、受験ごとに登録料を全額支払わなければならなりません。**つまり：

受験し、不合格になった後（1回目の受験）：

- 再受験1（2回目の受験）：受験者は、1回目の受験から30日間あける必要があります。
- 再受験2（3回目の受験）：受験者は、2回目の受験から90日間あける必要があります。
- 再受験3（4回目の受験）：受験者は、3回目の受験から90日間あける必要があります。

試験に合格した受験者は、5年間の申請期間の間、同じ試験を受験できません。

認定取得者は、認定を保持している間、同じ認定試験を受けることができません。

4.3 試験後のフィードバック

受験者は、試験完了後、試験後の調査でフィードバックを提供する機会が与えられます。皆様からのフィードバックは、試験体験と試験問題の質を向上させるために使用されます。

試験の実施に関する懸念

受験者は、ISACA（support.isaca.org）に試験終了後48時間以内に連絡して、試験日に関する問題、試験会場の状況、試験内容を含む、試験の運営管理に関するコメントや懸念事項を提出することができます。コメントを提出するには、次の手順を実行します。

ステップ	アクション
1.	ISACAサポートに連絡します。
2.	連絡する際には、以下の情報をお知らせください。 • ISACA ID番号 • 試験会場の場所 • 試験の日時 • 懸念事項に関する詳細な情報
3.	ISACAは、正式なスコアレポートを発表する前に、試験日や会場の懸念に関するコメントを確認します。

ISACAは、問題の更新に基づいてスコアを再発行することはありません。ISACAの各分野の専門家は、これらのコメントを今後の試験の改善に役立てます。

4.4 認定

認定資格を取得するには

ISACA認定試験を受験し合格することが、認定資格取得の最初のステップです。認定資格を取得するには、まず以下の要件を満たすことが必要です。

ステップ	アクション
1.	認定試験に合格すること。
2.	50米ドルの申請手数料を支払うこと。
3.	実務経験の要件を証明するための申請書を提出すること。
4.	職業倫理規程を遵守すること。
5.	継続的専門職教育ポリシーを遵守すること。

受験者は合格後5年以内に認定資格の申請をしなければいけません。追加のリソースは以下のとおりです。

- 試験の合格： CISA | CISM | CGEIT | CRISC | CDPSE
- 50米ドルの申請手数料の支払い： CISA | CISM | CGEIT | CRISC | CDPSE
- 認定申請書の提出：CISA | CISM | CGEIT | CRISC | CDPSE
- ISACA職業倫理規定、利用規約、およびプライバシー通知を遵守すること
- 継続専門教育（CPE）ポリシーを遵守すること： CISA | CISM | CGEIT | CRISC | CDPSE
- 情報システム監査基準を遵守すること（CISAのみ）

認定資格を取得すべき理由

ISACA認定は世界中で受け入れられ認識されています。ISACA認定は、試験の合格と、仕事の功績、そして学習経験を組み合わせることで受験者の信頼性を高めます。これはキャリアを進める上で必要なことです。認定資格を取得すると、企業の価値を高める資質を持っていることを雇用主に証明できます。実際、世界中で多くの企業や政府機関でISACA認定資格が求められたり、認識されたりしています。

独立した調査では、ISACAの認定はIT専門家が取得できる中でも最も見返りが大きく影響力の大きいIT認定資格とされています。ISACA認定の取得と維持

- 潜在的な能力の向上
- 採用プロセスへの組み込み
- 専門家としての信頼性と評価を強化

ISO/IEC 17024:2012準拠

米国国家規格協会（ANSI）は、*ISO/IEC 17024:2012: General Requirements for Bodies Operating Certification Systems of Persons*（*人材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*）に基づき、CISA、CRISC、CISM、およびCGEIT資格を認定しています。

ANSIによる認定を受けることによって、開示性、均衡、合意、および適正プロセスに関するANSIの要件をISACAの手順が満たしていることが示されます。

この認定を受けることにより、ISACAは、CISA、CRISC、CISM、およびCGEITの資格保持者に世界中で素晴らしい職業的機会がもたらされると考えております。認定の詳細は以下のとおりです。

ANSI認定プログラム
人事認定番号0694
ISO/IEC 17024
CISA、CISM、CGEIT、およびCRISCプログラム認定
ISO/IEC 17024:2012に基づいて更新済み

ANSIは、サードパーティの製品、システム、専門家の認証機関としての役割を果たす他の組織を認定する非営利民間団体です。

ISO/IEC 17024では、特定の要件に対して個人を認証する組織が従うべき要件が規定されています。

ANSIは、ISO/IEC 17024を「認証コミュニティの国際標準化の促進、国家間の移動性の向上、公共の安全の強化、消費者の保護において重要な役割を果たすことが期待される」と説明しています。

付録

付録A：CISA

CISA試験内容の概要

（2024年8月発効）

1	**情報システム監査プロセス**	**18%**
1A	計画	
1A1	情報システム監査基準、ガイドライン、機能、倫理規範	
1A2	監査、評価、レビューの種類	
1A3	リスクベースの監査計画	
1A4	コントロールの種類と考慮事項	
1B	実施	
1B1	監査プロジェクト管理	
1B2	監査テストおよびサンプリング方法	
1B3	監査証拠の収集技法	
1B4	監査データ分析（監査アルゴリズムを含む）	
1B5	報告およびコミュニケーションの手法	
1B6	監査プロセスの品質保証と改善	
2	**ITのガバナンスと管理**	**18%**
2A	ITガバナンス	
2A1	法律、規制、業界標準	
2A2	組織構造、ITガバナンス、IT戦略	
2A3	ITポリシー、基準、手順、およびプラクティス	
2A4	エンタープライズ・アーキテクチャ（EA）と考慮事項	
2A5	エンタープライズ・リスク・マネジメント（ERM）	
2A6	プライバシープログラムと原則	
2A7	データガバナンスとデータ分類	

2B	IT管理	
2B1	ITリソース管理	
2B2	ITベンダー管理	
2B3	ITパフォーマンスの監視と報告	
2B4	ITの品質保証と品質管理	
3	**情報システムの取得、開発、実装**	**12%**
3A	情報システムの取得と開発	
3A1	プロジェクトのガバナンスと管理	
3A2	ビジネス・ケースとフィージビリティ分析	
3A3	システム開発手法	
3A4	コントロールの識別と設計	
3B	情報システムの実装	
3B1	システムの準備と実装テスト	
3B2	実装構成とリリース管理	
3B3	システムの移行、インフラストラクチャの展開、データ変換	
3B4	導入事後評価	
4	**情報システムの運用とビジネスの回復力**	**26%**
4A	情報システムの運用	
4A1	ITコンポーネント	
4A2	IT資産管理	
4A3	ジョブスケジューリングと本番プロセスの自動化	
4A4	システムインターフェース	
4A5	シャドーITとエンドユーザーコンピューティング（EUC）	
4A6	システムの可用性と容量管理	
4A7	問題とインシデントの管理	
4A8	ITの変更、構成、パッチ管理	

4A9	運用ログ管理	
4A10	ITサービスレベル管理	
4A11	データベース管理	
4B	**ビジネスのレジリエンス**	
4B1	ビジネス・インパクト分析（BIA）	
4B2	システムと運用のレジリエンス	
4B3	データのバックアップ、保存、復元	
4B4	事業継続計画（BCP）	
4B5	災害復旧計画（DRP）	
5	**情報資産の保護**	**26%**
5A	**情報資産のセキュリティとコントロール**	
5A1	情報資産セキュリティポリシー、フレームワーク、基準、ガイドライン	
5A2	物理的コントロールと環境コントロール	
5A3	IDおよびアクセス管理	
5A4	ネットワークとエンドポイントのセキュリティ	
5A5	データ損失防止（DLP）	
5A6	データの暗号化	
5A7	公開鍵インフラストラクチャ（PKI）	
5A8	クラウド環境と仮想化環境	
5A9	モバイル、ワイヤレス、およびIoT（Internet-of-Things）デバイス	
5B	**セキュリティイベント管理**	
5B1	セキュリティ意識向上トレーニングとプログラム	
5B2	情報システム攻撃の方法と技法	
5B3	セキュリティテストのツールと技法	
5B4	セキュリティ監視ログ、ツール、技法	
5B5	セキュリティインシデント対応管理	
5B6	証拠収集とフォレンジック	

補助タスク

1. 情報システムが保護され、管理され、組織に価値を提供しているかどうかを判断するための監査を計画します。
2. 情報システム監査基準およびリスクベースの情報システム監査戦略に従って監査を実施します。
3. 監査プロセスにプロジェクト管理手法を適用します。
4. 利害関係者と情報交換を行い、監査の進捗状況、発見事項、結果、推奨事項に関するフィードバックを収集します。
5. 監査後のフォローアップを実施し、特定されたリスクが十分に対処されたかどうかを評価します。
6. データ分析ツールを活用して監査プロセスを強化します。
7. 組織における自動化および意思決定システムの役割や影響を評価します。
8. 品質保証および改善プログラムの一環として、監査プロセスを評価します。
9. 組織の戦略および目的との整合性についてIT戦略を評価します。
10. ITガバナンス体制およびIT組織構造の有効性を評価する。
11. 法的要件および規制要件の遵守を含め、組織のITポリシーおよびプラクティスの管理を評価します。
12. ITリソースとプロジェクト管理が組織の戦略と目標に整合しているかを評価します。
13. 組織のエンタープライズ・リスク・マネジメント(ERM)プログラムを評価します。
14. 組織がITリスク、コントロール、基準の所有権を定義しているかどうかを判断します。
15. ITの主要業績評価指標（KPI）およびIT主要リスク指標（KRI）の監視と報告について評価します。
16. 組織が事業運営を継続できる能力を評価します。
17. 組織のストレージ、バックアップ、復元のポリシーとプロセスを評価します。
18. 情報システムに関連するビジネスケースが事業目標を満たしているかどうかを評価します。
19. ITベンダーの選定および契約管理プロセスが、ビジネス、法律、規制の要件を満たしているかどうかを評価します。
20. ITリスク要因と完全性の問題に関してサプライチェーンを評価します。
21. 情報システム開発ライフサイクルのすべての段階のコントロールを評価します。
22. 情報システムの導入、および本番環境への移行の準備状況を評価します。

23. システムの導入事後評価を実施し、プロジェクトの成果物、コントロール、要件が満たされているかどうかを判断します。
24. エンドユーザーをサポートする効果的なプロセスが実施されているかどうかを評価します。
25. ITサービス管理のプラクティスが組織の要件に合致しているかどうかを評価します。
26. 情報システムおよびエンタープライズアーキテクチャ（EA）の定期的なレビューを実施し、組織の目標との整合性を判断します。
27. IT運用および保守プラクティスが組織の目標をサポートするかどうかを評価します。
28. 組織のデータベース管理プラクティスを評価します。
29. 組織のデータガバナンスプログラムを評価します。
30. 組織のプライバシープログラムを評価します。
31. データ分類プラクティスが組織のデータガバナンスプログラム、プライバシープログラム、および適用される外部要件と整合しているか評価します。
32. 組織の問題およびインシデント管理プログラムを評価します。
33. 組織の変更、構成、リリース、パッチ管理プログラムを評価します。
34. 組織のログ管理プログラムを評価します。
35. 資産ライフサイクル管理に関する組織のポリシーとプラクティスを評価します。
36. シャドーITおよびエンドユーザーコンピューティング（EUC）に関連するリスクを評価し、補完的コントロールの有効性を判断します。
37. 組織の情報セキュリティプログラムを評価します。
38. 組織の脅威および脆弱性管理プログラムを評価します。
39. 技術的なセキュリティ・テストを活用して、潜在的な脆弱性を特定します。
40. 論理的、物理的、環境管理[統制・調節・規制]を評価し、情報資産オーナーの機密性、完全性、可用性を検証します。
41. 組織のセキュリティ意識向上トレーニングプログラムを評価します。
42. 情報システムの品質とコントロールを改善するために、組織にガイダンスを提供します。
43. 新技術、規制、業界プラクティスに関連する潜在的な機会とリスクを評価します。

付録B：CRISC

CRISC試験内容の概要

（2025年発効）

1	**ガバナンス**	**26%**
1A	組織のガバナンス	
1A1	戦略、ゴール、目標	
1A2	組織構造、役割、責任	
1A3	組織の文化と倫理	
1A4	ポリシーと標準	
1A5	ビジネスプロセスおよびレジリエンス（DRP、BCPなど）	
1A6	組織資産管理	
1B	リスクガバナンス	
1B1	エンタープライズ・リスク・マネジメント（ERM）	
1B2	ディフェンスライン	
1B3	リスクプロファイル	
1B4	リスク選好とリスク許容度	
1B5	リスクフレームワーク、法律、規制、および契約上の要件	
2	**リスクアセスメント**	**22%**
2A	リスク特定	
2A1	リスク事象	
2A2	脅威モデリングと脅威環境	
2A3	脆弱性の管理	
2A4	リスクシナリオの作成と評価	
2B	リスク分析	
2B1	リスクアセスメントの概念と標準	

2B2	ビジネス・インパクト分析（BIA）
2B3	リスク登録簿
2B4	リスク分析方法
2B5	固有および残存リスク
3	**リスク対応および報告** **32%**
3A	リスク対応
3A1	リスク対応オプション
3A2	リスクおよびコントロールオーナーシップ
3A3	ベンダー/サプライチェーンのリスク管理
3A4	問題、発見事項、例外、免除の管理
3B	コントロール設計と導入
3B1	コントロールのフレームワーク、種類、標準
3B2	コントロールの設計、選択、導入、分析
3B3	コントロールのテスト手法
3C	リスクモニタリングおよびレポート
3C1	リスク行動計画
3C2	データ収集、集計、分析、検証
3C3	リスクおよびコントロールの評価指標（KRI、KCI、KPIなど）
3C4	リスクおよびコントロールのモニタリング技法
3C5	リスクおよびコントロールの報告技法（ヒートマップ、スコアカード、ダッシュボードなど）
3C6	新たなリスクの監視と報告
4	**技術およびセキュリティ** **20%**
4A	技術原則
4A1	技術ロードマップとエンタープライズアーキテクチャ（EA）
4A2	運用管理（変更管理、資産、DevOps、問題、インシデントなど）

4A3 システム開発ライフサイクル（SDLC）

4A4 データライフサイクル管理

4A5 ポートフォリオおよびプロジェクト管理（アジャイルなど）

4A6 技術の回復力と災害対応/復旧

4A7 新しく出現した技術

4B 情報セキュリティ原則

4B1 セキュリティの概念、フレームワーク、標準

4B2 セキュリティ/リスク意識向上とトレーニング

4B3 データプライバシーおよびデータ保護原則

補助タスク

1. 組織のビジネスおよび情報システム環境に関する既存の情報を収集、レビュー、評価する。
2. 組織のビジネス目標および業務に対する情報システムリスクの潜在的影響または発現した影響を特定する。
3. 組織の人員、プロセス、技術に対する脅威および脆弱性を特定する。
4. 情報システムリスクシナリオを作成するために脅威、脆弱性、リスクを評価する。
5. 適切なレベルのリスクとコントロールオーナーシップを割り当て、検証することで説明責任を確立する。
6. 情報システムリスク登録簿を維持または確立し、事業体全体のリスクプロファイルに組み込む。
7. リスク選好および許容の閾値ならびに事業目標への影響度の選定において、主要な利害関係者を支援する。
8. セキュリティ/リスクに関する啓発およびトレーニングの開発と実施に貢献することで、リスクを意識する文化を育む。
9. 情報システムのリスクシナリオと事象を分析してリスクのスコア/格付けを生成することで、リスクアセスメントを実施する。
10. 既存コントロールの現状を特定し、情報システムリスク対応に対するその有効性を評価する。
11. 選好および許容の閾値を超えるリスクであるかどうかを判断して、対応オプションを推奨し、懸案事項を是正する。
12. リスクやコントロール分析の結果をレビューし、リスク環境の現状と望ましい状態とのギャップをアセスメントする。
13. リスク対応計画の策定に関してリスクオーナーと協力する。
14. コントロールの選択、設計、導入、維持に関してコントロールオーナーと協働する。
15. リスク行動計画に従ってリスク対応が実施されたことを検証する。
16. 重要リスク評価指標（KRI）を定義、導入、改良する。
17. 重要業績評価指標(KPI)および重要コントロール評価指標（KCI）の特定および改良に関してコントロールオーナーと協働する。

18. 重要リスク評価指標（KRI）、重要業績評価指標(KPI)、および重要コントロール評価指標（KCI）をモニタリングし、分析する。
19. コントロールアセスメント結果をレビューし、コントロール環境の適切性、有効性、成熟度を判定する。
20. リスクおよびコントロールデータの集計、分析、検証を実施する。
21. 該当する利害関係者に対して関連するリスクおよびコントロール情報を報告し、リスクに基づいた意思決定を促す。
22. 新しく出現した技術および環境に対する変更について、脅威、脆弱性、機会がないか評価する。
23. リスク管理フレームワーク、標準、規制に対するビジネスプラクティスの整合性を評価する。
24. リスクシナリオ、能力、対応におけるギャップを検証して特定するための机上演習を促進する。

付録C：CISM

CISM試験内容の概要

（2022年発効）

1	情報セキュリティガバナンス	17%
1A	事業体のガバナンス	
1A1	組織文化	
1A2	法律、規制、および契約上の要件	
1A3	組織の構造、役割、および責任	
1B	情報セキュリティ戦略	
1B1	情報セキュリティ戦略の策定	
1B2	情報ガバナンスフレームワークおよび標準	
1B3	戦略計画（例：予算、リソース、ビジネス・ケース）	
2	情報セキュリティリスク管理	20%
2A	情報セキュリティリスクアセスメント	
2A1	新たなリスクおよび脅威環境	
2A2	脆弱性とコントロールの不備分析	
2A3	リスクアセスメントおよび分析	
2B	情報セキュリティリスク対応	
2B1	リスク処理/リスク対応の選択肢	
2B2	リスクおよびコントロールオーナーシップ	
2B3	リスクモニタリングおよびレポート	
3	情報セキュリティプログラム	33%
3A	情報セキュリティプログラム開発	
3A1	情報セキュリティプログラムのリソース（例：人材、ツール、技術）	
3A2	情報資産の特定および分類	

3A3	情報セキュリティに関する業界標準およびフレームワーク	
3A4	情報セキュリティポリシー、手続、およびガイドライン	
3A5	情報セキュリティプログラム評価尺度	
3B	情報セキュリティプログラム管理	
3B1	情報セキュリティコントロールの設計および選択	
3B2	情報セキュリティコントロールの導入および統合	
3B3	情報セキュリティコントロールのテストおよび評価	
3B4	情報セキュリティ意識向上およびトレーニング	
3B5	外部サービスの管理（例：プロバイダー、サプライヤー、第三者、第四者）	
3B6	情報セキュリティプログラムのコミュニケーションと報告	
4	インシデント管理	30%
4A	インシデント管理の準備	
4A1	インシデント対応計画	
4A2	ビジネス・インパクト分析（BIA）	
4A3	事業継続計画（BCP）	
4A4	災害復旧計画（DRP）	
4A5	インシデントの区分化/分類化	
4A6	インシデント管理のトレーニング、テストと評価	
4B	インシデント管理業務	
4B1	インシデント管理ツールおよび技法	
4B2	インシデント調査および評価	
4B3	インシデントの封じ込め方法	
4B4	インシデント対応に関するコミュニケーション（例：報告、通知、エスカレーション）	
4B5	インシデントの根絶および復旧	
4B6	インシデント事後レビューの実践	

補助タスク

1. 組織の情報セキュリティ戦略に与える内部および外部の影響を特定する。
2. 組織のゴールと目標に整合した情報セキュリティ戦略を確立し、維持する。
3. 情報セキュリティガバナンスフレームワークを確立し、維持する。
4. 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。
5. 情報セキュリティポリシーを確立し維持することで、基準、手順、およびガイドラインの開発を導く役割を果たす。
6. 情報セキュリティへの投資をサポートするビジネスケースを作成すること。
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に実施できるように支援すること。
8. 組織および権限系統全体における情報セキュリティの責任を定義、伝達しモニタリングする。
9. 情報セキュリティプログラムの活動内容、トレンド、および全体的な有効性をまとめてレポートを作成し、主要なステークホルダーに提出する。
10. 情報セキュリティ評価尺度を評価し、主要な利害関係者に報告する。
11. 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。
12. 情報セキュリティプログラムを、他のビジネス部門の業務目標にあわせる。
13. 情報セキュリティプログラムを実行するための情報セキュリティプロセスおよびリソースを策定し、修正していく。
14. 組織の情報セキュリティのポリシー、標準、ガイドライン、手順と他の文書を確立、伝達し維持する。
15. 情報セキュリティ意識とトレーニングプログラムの確立、推進、維持は重要であるが、比例した保護を達成するための主要な要素ではない。
16. 組織のセキュリティ戦略を維持するために、情報セキュリティ要件を組織のプロセスに統合する。
17. 情報セキュリティ要件を外部当事者との契約および活動に統合する。
18. 確立されているセキュリティ要件の外部者による遵守をモニタリングする
19. 情報セキュリティプログラム向けの管理および運用評価尺度を定義し、モニタリングする。
20. 情報資産の特定および分類に関するプロセスを確立し、維持する。
21. 法律要件、規制要件、組織要件、その他の適用されるコンプライアンス要件を特定する
22. リスクの特定、リスクアセスメント、リスク処理のプロセスに参加し監督する
23. 脆弱性アセスメントおよび脅威分析プロセスに参加し、監督する。
24. 組織のリスク選好度に基づき、受容可能なレベルまでに抑えてリスクを管理するために、適切なリスク対処および対応オプションを特定、推奨、導入する。
25. 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こと。
26. 情報リスク管理をビジネスおよびITプロセスに統合することを促進する。
27. リスクの再アセスメントを必要とする内部および外部の要因をモニタリングする。
28. リスク管理に関する意思決定プロセスを促進するために、非遵守や情報リスクの変更をはじめ、情報セキュリティリスクに関して主要な利害関係者に報告する。
29. 事業継続計画および災害復旧計画に沿ったインシデント対応計画を策定し、修正していく。
30. 情報セキュリティインシデントの区分化および分類化プロセスを確立し、維持する。

31. 各種プロセスを開発し実施して、情報セキュリティのインシデントを即座に把握できるようにすること。
32. 法令および規制の要件に従って、情報セキュリティインシデントを調査して文書化するプロセスを策定し、修正していく。
33. 封じ込め、通知、エスカレーション、根絶と復旧などのインシデント処理プロセスを確立し維持する。
34. インシデント対応チームを編成、トレーニング、準備し、責任を割当てる
35. 内部および外部の当事者向けのインシデントコミュニケーション計画およびプロセスを策定し、修正していく。
36. 机上演習、チェックリストレビュー、シミュレーションテストなどのテストおよびレビューを定期的に実施することで、インシデント管理計画を評価する。
37. 継続的向上を促進するために、根本原因分析、学んだ教訓、是正処置、リスクの再アセスメントなどのインシデント後のレビューを実施する。

付録D：CGEIT

CGEIT試験内容の概要

（2020年発効）

1	**事業体のITガバナンス**	**40%**
1A	ガバナンスフレームワーク	
1A1	ガバナンスフレームワークのコンポーネント	
1A2	組織の構造、役割、および責任	
1A3	戦略の開発	
1A4	法律および規制遵守	
1A5	組織文化	
1A6	事業倫理	
1B	技術ガバナンス	
1B1	ガバナンス戦略と事業体目標の整合性	
1B2	戦略計画プロセス	
1B3	利害関係者の分析と関与	
1B4	情報伝達および意識向上戦略	
1B5	エンタープライズアーキテクチャ	
1B6	ポリシーと標準	
1C	情報ガバナンス	
1C1	情報アーキテクチャ	
1C2	情報資産のライフサイクル	
1C3	情報の所有権および管理	
1C4	情報の分類と取り扱い	
2	**ITリソース**	**15%**
2A	ITリソース計画	

2A1	調達戦略	
2A2	リソース容量計画	
2A3	リソースの獲得	
2B	ITリソースの最適化	
2B1	ITリソースライフサイクルおよび資産管理	
2B2	人材能力の評価および開発	
2B3	契約サービスおよび関係の管理	
3	**利益の実現**	**26%**
3A	ITパフォーマンスと監督	
3A1	パフォーマンス管理	
3A2	変更管理	
3A3	ガバナンスモニタリング	
3A4	ガバナンス報告	
3A5	品質保証	
3A6	プロセス開発と改善	
3B	IT関連投資の管理	
3B1	ビジネス・ケースの開発および評価	
3B2	IT投資管理と報告	
3B3	パフォーマンス評価指標	
3B4	便益評価方法	
4	**リスクの最適化**	**19%**
4A	リスク戦略	
4A1	リスクフレームワークと基準	
4A2	エンタープライズ・リスク・マネジメント（ERM）	
4A3	リスク選好とリスク許容度	

4B	リスク管理
4B1	ITを活用した能力、プロセス、およびサービス
4B2	業務上のリスク、エクスポージャ、および脅威
4B3	リスク管理のライフサイクル
4B4	リスクアセスメント方法

補助タスク

1. 事業体のITガバナンスのフレームワークの目的を確立する。
2. 事業体のITガバナンスのフレームワークを確立する。
3. 事業体のITガバナンスのフレームワークに関して内外の要件を特定する。
4. 事業体のITガバナンスのフレームワークに戦略的計画プロセスを組み込む。
5. IT関連投資のためのビジネス・ケースの開発および利益実現プロセスが確立されていることを確認する。
6. 事業体のITガバナンスのフレームワークにエンタープライズアーキテクチャを組み込む。
7. 事業体のITガバナンスのフレームワークに情報アーキテクチャを組み込む。
8. 事業体のITガバナンスのフレームワークを全社的な共有サービスと整合させる。
9. 事業体のITガバナンスのフレームワークに包括的で反復可能なプロセスとアクティビティを組み込む。
10. 情報資産とITプロセスの役割、責任、および説明責任を確立する。
11. 事業体のITガバナンスのフレームワークを評価し、改善の機会を特定する。
12. 事業体のITガバナンスのフレームワークに関連する問題を特定および改善するためのプロセスを確立する。
13. ITと事業体の戦略的整合性をサポートするポリシーと基準を確立する。
14. IT関連のビジネス投資に関する意思決定に役立つ情報を提供するポリシーと基準を確立する。
15. 事業体のITガバナンスの価値を伝えるための情報伝達および意識向上プロセスを確立する。
16. IT戦略計画プロセスを評価、指示、および監視し、事業体の目標との整合性を確保する。
17. 利害関係者の関与を評価、指示、および監視する。
18. IT戦略計画プロセスと関連アウトプットを文書化して伝達する。
19. エンタープライズアーキテクチャがIT戦略計画プロセスに統合されていることを確認する。
20. 情報アーキテクチャがIT戦略計画プロセスに統合されていることを確認する。

21. 事業体のITガバナンスのフレームワークにITイニシアチブの優先順位決定プロセスを組み込む。
22. ITリソースおよび能力のライフサイクルを管理するためのプロセスが整備されていることを確認する。
23. 情報資産のライフサイクルを管理するためのプロセスが整備されていることを確認する。
24. 最適化とコントロールを確保するために事業体のITガバナンスのフレームワークに調達戦略を組み込む。
25. ITリソース管理プロセスと事業体のリソース管理プロセスとの整合性を確保する。
26. 情報ガバナンスと事業体のITガバナンスのフレームワークとの整合性を確保する。
27. ビジネスニーズに合致する人材の評価および育成のためのプロセスが整備されていることを確認する。
28. IT関連投資がその経済的ライフサイクル全体を通じて確実に管理されるようにする。
29. IT関連投資の所有権と説明責任を割り当てるプロセスを評価する。
30. IT投資管理プラクティスと事業体の投資管理プラクティスとの整合性を確保する。
31. IT関連投資、ITプロセス、およびITサービスの利益実現を評価する。
32. IT関連投資、ITプロセス、およびITサービスのパフォーマンス管理プログラムを確立する。
33. 改善イニシアチブが、パフォーマンス測定から導き出された結果に基づいていることを確認する。
34. 包括的なITおよび情報リスク管理プログラムが確立されていることを確認する。
35. ITおよび情報リスク管理のポリシーと基準の遵守を監視および報告するプロセスが整備されていることを確認する。
36. ITプロセスと事業体の法規制コンプライアンス目標との整合性を確保する。
37. ITおよび情報リスク管理とエンタープライズ・リスク・マネジメント（ERM）フレームワークとの整合性を確保する。
38. ITおよび情報リスク管理のポリシーと基準が策定および伝達されていることを確認する。

付録E：CDPSE

CDPSE試験内容の概要

（2025年発効）

1	**プライバシーガバナンス**	**20%**
1A	プライバシーガバナンス	
1A1	個人情報	
1A2	プライバシー原則（プライバシーバイデザイン、同意、透明性など）	
1A3	プライバシーに関する法規制	
1A4	プライバシーに関する文書（ポリシー、ガイドラインなど）	
1B	プライバシーオペレーション	
1B1	組織の文化、構造、および責任	
1B2	ベンダーとサプライチェーンの管理	
1B3	インシデント管理	
1B4	データ主体の権利、要求、および通知	
2	**プライバシーリスク管理とコンプライアンス**	**18%**
2A	リスク管理	
2A1	リスク管理プロセスとポリシー	
2A2	プライバシーに焦点を当てた評価（プライバシー影響評価（PIA）など）	
2A3	プライバシートレーニングおよび意識向上	
2A4	脅威と脆弱性	
2A5	リスク対応	
2B	コンプライアンス	
2B1	プライバシーフレームワーク	
2B2	証拠とアーティファクト	
2B3	プログラムのモニタリングと評価指標	

3	**データライフサイクル管理**	**23%**
3A	データ収集と処理	
3A1	データインベントリ、データフロー図、および分類	
3A2	データ品質（精度など）	
3A3	データ使用制限	
3A4	データ分析（集計、AI、データウェアハウスなど）	
3B	データの永続性と破棄	
3B1	データ最小化	
3B2	データの開示および転送	
3B3	データの保存、保持、およびアーカイブ	
3B4	データ破棄	
4	**プライバシーエンジニアリング**	**39%**
4A	技術スタック	
4A1	インフラストラクチャおよびプラットフォームテクノロジー（レガシー、クラウドコンピューティングなど）	
4A2	デバイスとエンドポイント	
4A3	接続	
4A4	安全な開発ライフサイクル	
4A5	APIとクラウドネイティブサービス	
4B	プライバシー関連のセキュリティコントロール	
4B1	資産管理	
4B2	IDおよびアクセス管理	
4B3	パッチ管理と堅牢化	
4B4	通信とトランスポートのプロトコル	
4B5	暗号化とハッシュ化	
4B6	モニタリングとロギング	

4C	プライバシーコントロール
4C1	同意タグ付け
4C2	トラッキング技術（クッキー管理など）
4C3	匿名化と偽名化
4C4	プライバシー強化技術（PETs）
4C5	AI/機械学習（ML）に関する考慮事項

補助タスク

1. 組織のプライバシープログラムを開発および保守するための内部および外部の要件を特定する。
2. プライバシー関連の法規制要件、業界のベストプラクティス（プライバシーバイデザインなど）、およびデータ主体の期待に整合するように組織のプログラムを見直す。
3. プライバシーに配慮したデータガバナンスを実現できるように、データライフサイクルポリシーおよびプラクティスについて助言する。
4. データ分類とデータライフサイクル要件に対処するための技術およびオペレーショナル・コントロールの実施を設計および評価する。
5. プライバシー影響評価（PIA）などのプライバシーに焦点を当てた評価を実施する。
6. 組織のニーズに応じた手順書や業務マニュアルの作成においてプライバシー原則（プライバシーバイデザインなど）を組み込むことに貢献する。
7. システム、アプリケーション、インフラストラクチャを設計、開発、および実装する際に、利害関係者と協力してプライバシー原則（プライバシーバイデザインなど）の遵守を促進する。
8. プライバシーに関連する脅威と脆弱性を特定および評価する。
9. 契約、サービスレベル合意書（SLA）、およびベンダーやその他の関係者のプライバシー慣行（プラクティス）の評価に貢献し、その後の遵守状況を監視する。
10. インシデント管理プロセスに参加し、プライバシーへの影響に対処して改善を支援する。
11. プライバシーコンプライアンスとリスク対応に利害関係者と協力して取り組む。
12. プライバシーバイデザイン原則とデータに関する考慮事項をサポートするため情報アーキテクチャの評価に貢献する。
13. 規制環境の変化、プライバシーに対する新たな脅威、およびプライバシー強化技術（PETs）を評価する。
14. 個人情報インベントリとデータフロー記録を最新かつ正確に保つためのプロセスと手順を設計、実施、および監視する。

15. リスクアセスメントとコントロールの実装を実現するため、個人情報のデータ分類について助言する。
16. プライバシープログラムのパフォーマンスを適切な利害関係者に報告するための評価指標を開発および監視する。
17. プライバシー体制と成熟度を組織目標に合わせて進歩させるよう提唱する。
18. プライバシーを意識する文化を促進するため、教育コンテンツの開発に貢献し、プライバシートレーニングを実施する。
19. データのライフサイクル全体を通じて説明責任、公平性、および透明性を促進する。

