

電子的にこの申請書を記入する場合、アドビリーダーを使用してください。

申請者情報

申請者名: _____ ISACA ID: _____
 メールアドレス: _____ 電話番号: _____

ステップ 1. 試験の合格

CISA 申請者は過去 5 年以内の CISA 試験に合格している必要があります。
 CISA 試験に合格していない場合、以下のリンクでオンライン登録してください: www.isaca.org/examreg

試験合格年度: _____

ステップ 2. 実務経験報告

CISA 応募資格は、過去 10 年以内に 5 年以上の情報システム監査、コントロール、アシュアランスまたはセキュリティの実務経験を持つこと。当実務経験は、ページ V-2 記載の CISA 実務ドメインエリアで行われたものでなくてはなりません。セクション 2A の 5 年の実務経験要件を満たしていない場合、セクション 2B または 2C の経験免除を請求することができます (最大 3 年間まで)。

セクション A: 情報システム監査、コントロール、アシュアランスまたはセキュリティ職務経験 (必須)

関連の実務経験を、現在若しくは直近の職歴から記入してください。
 日付を空のままにしないでください。現在雇用されている場合、終了日に今日の日付を記入してください。

#	会社名	雇用日 (MM/YY)	開始日	終了日	年数	月数	CISA 実務経験ドメイン (該当のものをすべてチェック)				
							1	2	3	4	5
1											
2											
3											
4											

(最低 2 年間必須) セクション A 経験合計: _____

セクション B: 一般職務経験免除 (任意)

一般情報システムまたは一般監査実務経験免除を申請するには、下記の詳細を記入してください。
 当実務経験はセクション A の職務期間中に獲得したものであってはなりません。これは 1 年間の免除となります。

経験免除の種類 (該当のものを 1 つ選択してください) 一般監査 一般情報システム

会社名: _____ 開始日 (MM/YY): _____ 終了日 (MM/YY): _____

(最大 1 年間) セクション B 経験合計: _____

セクション C: 教育経験免除 (任意)

教育経験免除を申請するには、下の適切なボックスにチェックを入れて、該当の場合学校の情報を記入してください。

*学校の卒業証明書、成績証明書または手紙を添付してください (いずれも英文)。

**CIMA または ACCA 証書を添付してください。

- 1 年間免除 - 準学士号
- 2 年間免除 - 学士号、修士号または博士号 (分野問わず)
- 3 年間免除 - 情報システムまたは関連分野の修士号 *
- 2 年間免除 - CIMA (公認管理会計士教育機関) フル認定 **
- 2 年間免除 - ACCA (英国勅許公認会計士) 会員 **

学校名: _____ 学位: _____ 分野: _____

(最大 3 年間) セクション C 経験合計: _____

セクション D: 経験総計:

CISA 認証を申請するにはセクション A・B・C の経験が合計 5 年以上でなくてはなりません。

(セクション A + セクション B + セクション C) 経験総計: _____

電子的にこの申請書を記入する場合、アドビリーダーを使用してください。

ステップ3. 職務経歴証明

実務経歴証明書（この申請書のページ V-1 と V-2）を用いてステップ2の全ての経験を雇用者が証明してください。証明者が2名以上必要な場合、こちらから追加の実務経歴証明書を入手してください：www.isaca.org/cisaapp. セクションCの認証または学位の場合、認定証、卒業証明書、または成績証明書を提出してください。

ステップ4. 申請手数料

US\$ 50.00 の申請手数料の決済が完了次第、申請の手続きを進めさせていただきます。

決済はこちら：www.isaca.org/cisapay

ステップ5. 契約条件の確認と署名

継続専門教育(CPE)方針

私はここに ISACA の方針と手順に従い、公認情報システム監査人 (CISA) 資格認定を申請する。私は資格認定プロセス及び CPE 方針を含め、申請時に有効な資格認定申請と継続的専門教育 (CPE) ポリシーに記載されている条件を精読し、同意する。

倫理規定

私は以下のことを了承する：資格要件を満たす証拠を提供すること；申請の提出物についてのさらなる説明や検証、または証明者への直接連絡を ISACA に許可すること；CISA の業務を遂行するための資格要件、ISACA の倫理規定、基準とポリシーの遵守、更新要件の履行など、認証を取得し、維持するための要件を遵守すること；認証条件に応じられない場合、至急 ISACA 認証部門に知らせること；CISA の業務を遂行すること；獲得した認証の範囲内でのみ認証の要請をすること；そして CISA の認証やロゴ、マークを紛らわしい方法や ISACA のガイドラインに反して使用しないこと。

情報の真実性

私が提供した情報に偽りがある、あるいは試験の規則や認証の資格に反した場合、認証の申請は棄却され、ISACA に与えられた、いかなる資格も喪失されることを理解し、了承する。全ての認証は ISACA の所有物であることを理解し、獲得後取消になった場合、私はその認証を処分し、使用を中止し、資格を撤回する。必要とみなされた場合、私の資格情報や専門的立場についての ISACA の問い合わせと調査を認可する。

第三者との情報共有

認証が付与された場合、私の認証状態は公開され、問い合わせがあった場合 ISACA により第三者に開示されることを承認する。申請が承認されなかった場合、ISACA に連絡しアペールすることが可能だと理解する。資格試験受験者、資格認定申請者、または認定された人物のアペールは任意であり、費用は受験者や申請者の負担となる。下記に署名することで、私は ISACA が自らの資格認定状況を開示することを認可する。この連絡先は資格認定の問い合わせや要求のために使用される。

連絡ポリシー

下記に署名することで、私は ISACA に提供した連絡先での連絡を認可し、その連絡先は私自らのものであり正確である。法律によって求められた場合、或いは ISACA のプライバシーポリシーに沿って、ISACA に機密の認証申請と認証情報の開示を認可する。提供された情報の使用について詳しく知りたい方は、以下の ISACA プライバシーポリシーをお読みください：www.isaca.org/privacy.

使用に関する合意

私は ISACA、その役員、取締役、試験官、従業員、代理人、そして支援組織の代理人に対して、本申請および申請手続き、私に証明書を発行できなかった、または認定の没収または認定証の再配達、これらのいずれかの行為または不作為から生じる事項に関する苦情、請求または損害を与えないことに同意する。上記にも関わらず、私はこの申請に起因するまたはそれに関連するいかなる訴訟も、アメリカのイリノイ州クック郡巡回裁判所に提訴され、イリノイ州の法律に準拠するものと理解し、了承する。

私は自らの認証資格があるかどうかの判断は全て ISACA に委ねられ、ISACA の決断は絶対であると理解する。

私は契約条件を精読し理解し、ISACA に法的に拘束されることを了承する。

申請者署名： _____ 日付： _____

ステップ6. 申請書提出

申請書、（もし必要であれば追加の証明書等）や付属の書類を以下のリンクからオンラインで提出してください：

<https://support.isaca.org>

“Certifications & Certificate Programs”を選択し、“Submit an Application”を選択してください。

申請は約2週間から3週間かかります。承認後、Eメールでお知らせいたします。承認書、CISA 認証、そして金属の CISA ピンバッジが、ISACA プロフィールの第1住所に送られます。発送は4週間から8週間かかります。

電子的にこの申請書を記入する場合、アドビリーダーを使用してください。

申請者情報

申請者名: _____ ISACA ID: _____

証明者のための書式への記入方法

上記の申請者は ISACA を通して CISA 認証を申請している。ISACA では申請者の実務経験が、雇用の監督者または管理職によって証明される必要があります。証明者は直近の血縁や拡大家族、または人事部の者であってはなりません。このフォームの記入により、あなた（証明者）は申請書（ページ A-1）に記述されている申請者の実務経験、そして CISA 実務ドメインと業務内容の申告（ページ V-2）を立証します。

この証明書を提出するために申請者に返却してください。質問がある場合は、ISACA にご連絡ください：
<https://support.isaca.org> または +1.847.660.5505.

証明者情報

証明者名: _____

会社名: _____ 役職: _____

メールアドレス: _____ 電話番号: _____

証明者質問

1. 私はページ A-1 に記述されている申請者の職務経験を立証します（該当のものをすべてチェック）：

セクション A : 会社 1
セクション A : 会社 2

セクション A : 会社 3
セクション A : 会社 4

2. 私はページ A-1、セクション B と C の免除を立証します。（該当するものをすべてチェック）：

セクション B : 職務経験免除

セクション C : 学位

3. 私は申請者の以下の役割を務めていました：

監督者 マネージャー 同僚 クライアント

4. セクション A で職務経験を立証する場合、ページ V-2 に記述されている申請者の業務が、私の知る限り正しいことも立証します。

はい いいえ

証明者契約

私の知る限り、ページ V-1 と V-2 の情報が正しく、申請者が情報システム監査人として認められない理由はないと確証します。必要であれば、私は ISACA の上記の情報についての質問に快く回答します。

証明者署名: _____ 日付: _____

電子的にこの申請書を記入する場合、アドバイザーを使用してください。

実務ドメインの記入方法

申請者は対象となるドメインのすべてあるいは一部の業務を完了したことを確認し、証明者の確認を得る必要があります。

ドメイン1 - 情報システム監査のプロセス

IS監査基準に従い監査のサービスを提供し、組織の情報システムの保護と管理を支援すること。

業務内容の申告:

- 情報システム監査基準に従ってリスクベースの情報システム監査戦略を実施し、主要なリスク分野が確実に監査されるようにすること。
- 情報システムが保護され、管理され、組織に価値をもたらしているかどうかを判断するために特定の監査を計画すること。
- 策定した監査目標を達成するために、情報システム監査基準に従って監査を実施すること。
- ミーティングや監査報告書を通して主要な利害関係者に監査結果を連絡して推奨を行い、必要に応じて変更を促すこと。
- 監査のフォローアップを行い、経営者が適時、適切な措置を講じているか判断すること。

ドメイン2 - ITガバナンスとマネジメント

必要なリーダーシップと組織構造とプロセスが導入されていることを保証し、目標を達成させ組織の戦略を支援すること。

業務内容の申告:

- 組織の戦略や目標との整合性についてIT方針や戦略の開発、承認、導入や維持のプロセスを含め、IT戦略を評価すること。
- 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。
- ITの組織構造と人材（人事）管理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、それらを評価すること。
- 組織のIT関連リスクが識別、査定、モニタリング、報告、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。
- 組織のポリシー、基準と手順との準拠性について、ITマネジメント管理と統制のモニタリング（例：継続的モニタリング、品質保証[QA]）を評価すること。
- 組織のIT方針、基準、手順と、それらの開発、承認、リリース/発表、導入、維持プロセスがIT戦略を支援し、法規制の要件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。
- ITリソースの管理（投資、優先順位決定、割当、使用を含む）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。
- ITポートフォリオの管理（投資、優先順位決定、割当を含む）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。
- 経営陣が十分な情報を適時受け取っているかどうかを判断するために、ITの主要業績評価指標（KPI）のモニタリングと報告を評価すること。
- 組織がIT中断時に基本的な業務を続けられるかどうかを判断するために、IT災害復旧計画（DRP）とBCPの整合性を含め、組織の業務継続計画（BCP）を評価すること。

ドメイン3 - 情報システムの調達、開発、導入

情報システムの取得、開発、テスト、および導入の実務が組織の戦略及び目標に合致していることを保証すること。

業務内容の申告:

- 情報システムの取得、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。
- 組織のサービスレベルと必要なコントロールが確実に満たされるよう、ITサプライヤーの選定及び契約管理プロセスを評価すること。
- 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満たされているかどうかを判断するために、プロジェクト管理フレームワークとコントロールを評価すること。
- 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レビューを実施すること。
- 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、状況報告が適時かつ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。
- 組織のポリシー、基準、手順、及び適用可能な外部の要求事項を遵守しているかどうかを判断するために、要件定義、取得、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。
- 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移行の準備状況の評価すること。

ドメイン4 - 情報システムの運用、保守、サービスの管理

情報システムの取得、開発、検査と実装の実務が組織の戦略と目標に達していることを保証すること。

業務内容の申告:

- コントロールと組織の期待するサービスレベルが支持され、戦略目的が満たされているか判断するために、ITサービス管理フレームワークと業務（社内または第三者）を評価すること。
- エンタープライズアーキテクチャ（EA）内で組織の目標に継続して適合し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。
- IT運用が効果的に管理され、引き続き組織の目標をサポートしているか判断するために、IT運用（ジョブ・スケジューリング、構成管理、キャパシティおよびパフォーマンス管理など）を評価すること。
- IT保守プロセスが効果的に管理され、継続して組織の目標を支援しているか判断するために、IT保守プロセス（パッチ、アップグレード）を評価すること。
- データベースの完全性と最適化を判断するために、データベース管理業務を評価すること。
- 引き続き戦略目的を満たしているか判断するために、データ品質及びライフサイクル管理を評価すること。
- 問題とインシデントが適時、防止、検出、分析、報告、解決され、組織の目標を支持しているか判断するために、問題とインシデントの管理業務を評価すること。
- システムとアプリケーションの変更が十分に管理され文書化されているか判断するために、変更及びリリース管理業務を評価すること。
- エンドユーザーコンピューティング向けのプロセスが効果的に管理され、組織の目標を支持しているか判断するために、エンドユーザーコンピューティングを評価すること。
- IT継続性及び回復力が効果的に管理され、引き続き組織の目標を支持しているか判断するために、IT継続性と回復力（バックアップ/復元、災害復旧計画 [DRP]）を評価すること。

ドメイン5 - 情報資産の保護

情報資産の機密性、完全性、可用性を確実にするために、組織の方針、基準、手順および管理が確実であることの保証を提供すること。

業務内容の申告:

- 情報セキュリティおよびプライバシーポリシー、標準および手順の完全性、一般的に受け入れられている慣行との整合性、該当する外部要件への準拠性について評価すること。
- 物理的および環境的コントロールの設計、導入、保守、およびモニタリングを評価し、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。
- 情報セキュリティプログラムを評価し、その効果性や組織の戦略および目標との整合性を検証すること。
- システムおよび論理セキュリティコントロールの設計、導入、保守、モニタリング、および報告を評価して、情報の機密性、完全性および可用性を検証すること。
- データ分類プロセスおよび手順の設計、導入およびモニタリングを評価し、組織のポリシー、標準、手順およ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こと。
- 資産の保管、検索、移送および廃棄に使用されるプロセスおよび手順を評価し、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。