CISM 資格認定申請書

2013 年から 2016 年までの CISM 試験に合格した申請者

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

CISM 申請者は過去 5 年以内の CISM 試験に合格している必要があります。
CISM 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/examreq

試験合格年度: _____

ステップ2. 実務経験報告

CISM の資格認定を受けるには、過去 10 年以内に 5 年以上の情報セキュリティ管理の実務経験を有していること。実務経験は、V-2 ページに記載されている 4 つの CISM 実務ドメインのうち 3 つを含めなければなりません。
セクション A の 5 年間の実務経験要件を満たしていない場合は、セクション B または C の技能による免除を申請することもできます。

セクション A：情報セキュリティ管理経験 *（必須）*

関連する実務経験を、現在も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。

		雇用日 *(MM/YY)*		CISMタスクの実務経験期間		CISM実務経験ドメイン *（該当のものをすべてチェック）*			
#	会社名	開始日	終了日	年数	月数	1	2	3	4
1									
2									
3									
4									

（4 つの実務ドメインのうちの 3 つの合計で最低 3 年間必須） **セクション A 経験合計：** _____

セクション B：一般的な情報セキュリティ技能による免除 *（任意）*

一般的な情報セキュリティ技能による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。最大 2 年間の免除が可能です。

		雇用日 *(MM/YY)*		経験期間	
#	会社名	開始日	終了日	年数	月数
1					
2					

（最大 2 年間） **セクション B 経験合計：** _____

セクション C：CISM 実務経験の代用 *（任意）*

セクション C の免除は **1 つ** のみで、請求した免除の（英文）証明書を提出しなければなりません。

- ☐ 2 年間免除－有効な CISA 資格保持
- ☐ 2 年間免除－有効な CISSP 資格保持
- ☐ 2 年間免除－MBA または情報セキュリティまたは関連分野の修士号
- ☐ 1 年間免除－固有のスキルまたは一般的なセキュリティ資格認定
- ☐ 1 年間免除－情報システム管理実務の経験 （満一年間従事した場合）

会社：_____ 開始日：_____ 終了日：_____

（最大 2 年間） **セクション C 経験合計：** _____

セクション D：経験総計：

認証を申請するにはセクション A・B・C の経験が総計 **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：** _____

CISM 資格認定申請書

2013 年から 2016 年までの CISM 試験に合格した申請者

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. 実務経験の証明

実務経験証明書（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名以上の場合、こちらから追加の実務経験証明書を入手してください：*www.isaca.org/cismapp*。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（いずれも英文）。

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/cismpay*

ステップ5. 資格認定条件の確認と署名

継続専門教育(CPE)方針
私はここに ISACA の方針と手順に従い、公認情報セキュリティマネージャー（CISM）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：資格条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解明や検証、または証明者への直接連絡を ISACA に許可すること；CISM 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、認定を取得し、維持するための要件を遵守すること；認定条件に応じられない場合、至急 ISACA 認定部門に知らせること；CISM の業務を遂行すること；獲得した認定の範囲内でのみ認定の要請をすること；そして CISM の認定やロゴ、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、あるいは試験規則や認定の要件に反した場合、認定の申請は棄却され、ISACA より与えられた、いかなる資格も喪失されることを理解し、了承する。全ての認定は 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、私はその認定を処分し、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
認定が付与された場合、私の認定状態は公開され、問い合わせがあった場合 ISACA により第三者に開示されると承認する。申請が承認されなかった場合、ISACA に連絡しアピールすることが可能だと理解する。資格試験受験者、認定申請者、または認定された人物のアピールは任意であり、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 に機密の認定申請と認定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、代理人および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。

私は自らの認定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。

私はこれらのステートメントを精読し理解し、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. 申請書の提出

申請書及び証明書等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、CISM 資格認定証、そして金属製の CISM ピンバッジが、以下の MyISACA プロフィール *www.isaca.org/myisaca* の第 1 住所宛に送られます。発送は 4 週間から 8 週間かかります。

CISM 実務経験証明書

2013 年から 2016 年までの CISM 試験に合格した申請者

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 CISM 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。

あなた（証明者）は申請書（ページ A-1）と CISM 実務ドメインと業務内容の申告（ページ V-2）に記述されている申請者の実務経験を立証しなければなりません。

この証明書を提出するため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: _____

証明者への質問

1. ページ A-1 に記述されている申請者の情報セキュリティ管理の実務経験を立証します。*（該当な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 3

☐ セクション A : 会社 2 ☐ セクション A : 会社 4

2. ページ A-1 セクション B に記述されている申請者の一般情報セキュリティの実務経験を立証します。*（該当なものをすべてチェック）* :

☐ セクション B : 会社 1 ☐ セクション B : 会社 2

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 で実務経験を立証する場合、ページ A-1/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

証明者の合意

私の知る限り、ページ V-1 と V-2 の情報が正しく、申請者が情報セキュリティマネージャーとして認められない理由はないと立証します。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: _____

CISM 実務経験証明書

2013 年から 2016 年までの CISM 試験に合格した申請者

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。

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、証明者の確証を得る必要があります。

ドメイン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を確立および 維持し、情報セキュリティ戦略が組織の目標及び目的と調和して、情報リスクが適切に管理され、プログラムリソースが責任をもって管理されていることを確実にするプロセスを支援する。

業務内容の申告：

- 組織の目標及び目的と調和した情報セキュリティ戦略を確立および維持し、情報セキュリティプログラムの確立およびその継続する管理をガイドすること。
- 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維持し、情報セキュリティ戦略をサポートする活動をガイドすること。
- 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、組織の目標及び目的が情報セキュリティプログラムによってサポートされていることを確認すること。
- 情報セキュリティの基本方針を確立および維持し、経営層からの指示を連絡し、基準、手順、およびガイドラインの作成をガイドすること。
- 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。
- 組織への外部及び内部の影響を識別し（例えば、技術、業務環境、リスク許容度、地理的立地、法令及び法的規制事項等）、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認すること。
- 上級経営者からの関与及び他の利害関係者からのサポートを得て、情報セキュリティ戦略を正常に実施できる可能性を最大化すること。
- 組織全体の情報セキュリティの役割と責任を定義および連絡し、明確な説明責任及び権限体系を確立すること。
- 評価尺度の確立、監視、評価、および報告を行い（例えば、重要目標達成指標[KGI]、重要目標に対する成果達成指標[KPI]、主要なリスクインディケーター[KRI]）情報セキュリティ戦略の有効性に関する正確な情報を経営陣に提供すること。

ドメイン2 - 情報リスク管理とコンプライアンス

組織のビジネスおよびコンプライアンスの要件を満たすため、 情報リスクを許容レベルに管理する。

業務内容の申告：

- 資産保護のために講じる手段がビジネス価値に相当するように、情報資産のランク付けに対するプロセスを確立及び維持すること。
- 準拠違反のリスクを許容レベルに管理するための、法 的、規制、組織、及びその他の要件を特定すること。
- 組織の情報に対するリスクを特定するため、リスク評価、脆弱性評価、および脅威分析が定期的に一貫して実施されるようにすること。
- リスクを許容レベルに管理するための適切なリスク対応オプションを判別すること。
- 情報セキュリティコントロールが適切で、リスクを許容レベルにまで効果的に軽減するかどうかを判別するため、情報セキュリティコントロールを評価すること。
- リスクを許容レベルに管理するため、現在のリスクレベルとあるべきリスクレベルのギャップを特定すること。
- 組織全体で一貫した包括的な情報リスク管理プロセスを促進するため、情報リスク管理をビジネスプロセスとITプロセス（開発、購買、プロジェクト管理、合併、買収等）に統合すること。
- 変更を特定して適切に管理するため、既存のリスクを監視すること。
- リスク管理意思決定プロセスを支援するため、準拠違反及び情報リスクのその他の変更を適切な経営層に報告すること。

ドメイン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に沿った情報セキュリティプログラムを確立し、管理する。

業務内容の申告：

- 情報セキュリティ戦略と調和するよう情報セキュリティプログラムを確立し維持すること。
- 情報セキュリティプログラムとその他のビジネス機能 (人事[HR]、経理、調達、ITなど)との間で整合性を確実に取って、ビジネスプロセスへの組み込みを支援すること。
- 内部と外部のリソースの要件の把握、取得、管理、および定義を行って、情報セキュリティプログラムを実行すること。
- 情報セキュリティアーキテクチャ(人材、プロセス、技術)を確立し維持して、情報セキュリティプログラムを実行すること。
- 組織の情報セキュリティの基準、手順、ガイドライン、および他の文書の確立、伝達、および維持を行って、情報セキュリティ方針の遵守を支援し指導すること。
- 情報セキュリティの周知と研修のためのプログラムを確立し維持して、セキュリティで保護された環境と効果的なセキュリティ文化を推進すること。
- 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、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ベースラインを維持すること。
- 情報セキュリティ要件をサードパーティ(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ベースラインを維持すること。
- プログラムの管理と運用上の測定基準の確立、監視、および定期的な報告を行って、情報セキュリティプログラムの有効性と効率を評価すること。

ドメイン4 - 情報セキュリティインシデント管理

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

業務内容の申告：

- 情報セキュリティのインシデントの組織内定義と重大度の序列を確立し維持して、インシデントを正確に把握し対応できるようにすること。
- 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即座に対応できるようにすること。
- 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。
- 情報セキュリティの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、規制、および組織の要件に準拠しながら、適切に対応し原因を究明できるようにすること。
- インシデントのエスカレーションと通知のプロセスを確立し維持して、該当する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。
- 情報セキュリティインシデントに即座に効果的に対応するチームの編成、訓練、および準備を行うこと。
- インシデント対応計画を定期的にテストし見直して、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。
- 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。
- 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、是正処置を策定し、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。
- 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。