ISACA

CISM Certified Information Security Manager® An ISACA® Certification

認定申請書

申請条件：2022年6月以降のCISM試験合格者

申請者情報

申請者の氏名 _____ ISACA ID _____

電子メール _____ 電話番号 _____

ステップ1. 試験合格

CISM申請者は、過去5年以内にCISM試験に合格している必要があります。CISM試験にまだ合格していない場合は、**isaca.org/credentialing/cism**でオンライン登録が可能です。

試験合格年 _____

ステップ2. 実務経験報告

CISM資格認定を取得するためには、申請書提出日から過去10年以内に、5年間の情報セキュリティマネジメントの実務経験が必要です。資格認定を取得する条件について、4つのCISMジョブ・プラクティスドメインのうち3つのドメインで実務経験を積む必要があります（V-2ページを参照）。セクション2Aに記載される5年間の実務経験の要件を満たしていない場合、セクション2Bおよび/または2Cに記載される実務経験の免除の提出を選択することもできます。以下のセクションAおよびBに記載される5年間の実務経験は、すべてステップ3で検証されなければなりません。

セクションA. 情報セキュリティマネジメント実務経験（必須）

下の欄に関連するご自身の実務経験を記入してください。現職または最も最近の職務から記入してください。日付は必ず記入してください。在職中の場合、終了日には現在の日付を記入してください。

		雇用日 *(月/年)*		CISM実務経験の期間		CISMジョブ・プラクティスドメイン *(該当するドメインすべてにチェックマークを付けてください)*			
No.	会社名	開始日	終了日	年数	月数	1	2	3	4
1									
2									
3									
4									

(4つのジョブ・プラクティスドメインのうち3つにおける最低3年間の実務経験が必須)

セクションA. 実務経験の合計年数： _____

セクションB. 一般情報セキュリティ実務経験の免除（オプション）

一般情報セキュリティ実務経験の免除を申請する場合、下の欄に詳細を記入してください。この実務経験は、セクションAに記載された雇用期間中に積んだものであってはいけません。この免除申請では、最長2年間の実務経験を記入できます。

		雇用日 *(月/年)*		実務経験期間	
No.	会社名	開始日	終了日	年数	月数
1					
2					

(最長2年間) **セクションB. 実務経験の合計年数：** _____

セクションC. CISM実務経験の申請（オプション）

セクションCでは、申請者は1つの免除申請しか記入できません。また、記入した免除申請の証明を提出しなければなりません。

- ☐ CISA資格が有効である場合は2年間の免除
- ☐ CISSP資格が有効である場合は2年間の免除
- ☐ 情報セキュリティ関連分野におけるMBAまたは修士号を取得している場合は2年間の免除
- ☐ 情報セキュリティ関連分野における学士号を取得している場合は1年間の免除
- ☐ スキルベースまたは一般セキュリティ認定を取得している場合は1年間の免除
- ☐ 情報システムマネジメントの実務経験がある場合は1年間の免除 *(通年であることが必須)*

会社名 _____ **開始日** _____ **終了日** _____

(最長2年間) **セクションC. 実務経験の合計年数：** _____

セクションD. 実務経験の合計年数

認定を申請するためには、セクションA、BおよびCの合計実務経験年数が5年以上なければなりません。

セクションA + セクションB + セクションC = 実務経験の合計年数 _____

*この申請書を電子媒体で記入する場合は、**Adobe Reader®**を使用してください。*

更新：v5 05-2022

ステップ3. 実務経験の証明

実務経験証明フォーム（本申請書のV-1**および**V-2ページ）を使用して、雇用主にステップ2の実務経験のすべての証明を依頼してください。複数の証明者が必要な場合、追加の申請フォームを記入できます（追加フォームのV-1およびV-2ページのみ記入してください）。セクションCに認定または学位を記入した場合は、認定証、学位記または成績証明書のコピーを送信してください。

ステップ4. 申請処理手数料の支払い

すべての申請者は、50USドルの申請処理手数料を支払わなければ、申請は完全に処理されません。支払いは**https://store.isaca.org**で行うことができます。

ステップ5. 同意条項の証明と署名

継続専門教育(CPE)ポリシー

私は、ISACAの手続きおよびポリシーを遵守し、それらに従い、公認情報セキュリティマネージャー(CISM)の認定をISACAに申請します。私は、認定申請書ならびに認定プロセスおよびCPEポリシーが記載された申請時に有効な継続専門教育(CPE)ポリシーに規定される条件を読み、同意しました。

倫理規範

私は、資格認定要件を満たしていることの証拠を提供すること、ISACAが本申請に従って提出されたすべての情報の説明またはさらなる証明を求めることを許可すること（提出された情報を確認するために証明の専門家に直接連絡することを含むが、それに限定されない）、認定を取得し、維持するための要件を遵守すること（CISMのタスクを実行するための資格認定要件、ISACAの倫理規範、標準およびポリシーの遵守、更新要件を満たすことを含む）、私が認定要件を遵守できない場合、速やかにISACA認定部門に通知すること、認定が付与された範囲のみを対象として認定に関する異議申し立てを行うこと、誤解を与えたりISACAのガイドラインに反するような方法で、CISM認定またはロゴもしくはマークを使用しないことに同意します。

情報の真実性

私は、本申請書に私が記載した記述または回答が虚偽である場合、または私が試験規則もしくは認定要件のいずれかに違反する場合、認定申請が却下され、ISACAによって付与された資格が失効および没収されることを理解し、同意します。私は、すべての認定がISACAによって所有されること、および私の認定が付与された後に取り消された場合、私は認定証を破棄し、その使用を停止して、認定付与に対するすべての主張を撤回することを理解します。私は、ISACAが私の信用証明物および職業上の身分を証明するために必要とみなす、すべての照会および調査をISACAが行うことを承認します。

第三者との情報共有

私は、認定が付与された場合、私の認定状態が公開され、ISACAによって照会を行う第三者に開示される場合があることを認めます。私の申請が承認されない場合、私は、ISACAに問い合わせることで再審査を要請できることを理解します。認定試験受験者、認定申請者または認定された個人が行う再審査請求は、受験者または申請者の判断で自ら費用を負担して行うものとします。下の欄に署名することで、私はISACAが私の認定状態を開示することを承認します。この連絡先情報は、私の認定に関する照会および要求を満たすために使用されます。

問い合わせに関するポリシー

下の欄に署名することで、私は、記入した住所および電話番号にISACAが連絡すること、ならびに私が提供した連絡先情報が私自身の正確な情報であることを承認します。私は、法律によって要求される場合またはISACAのプライバシーポリシーに規定される場合、ISACAが秘密の認定申請および認定情報を公開することを承認します。このフォームで提供された情報をISACAがどのように使用するかに関する詳細は、ISACAのプライバシーポリシー(**isaca.org/privacy-policy**)をお読みください。

申請書の使い方に関する同意

私は、本申請、申請プロセス、私に対する認定証発行の不備、または認定証の没収もしくは再交付に対する要求に関連して、ISACA、その役員、理事長、試験官、従業員、代理人およびその支援組織の関係者のいずれかによる作為または不作為によって生ずる告訴、異議申し立てまたは損害から、かかる人物および団体を免責することに同意します。上記にかかわらず、私は、本申請により生ずる訴訟または本申請に関連する訴訟を起こす場合、米国イリノイ州クック郡の巡回裁判所に提出しなければならず、米国イリノイ州の法律が適用されるものとすることを理解し、同意します。

私は、私が認定を受ける資格があるかどうかに関する決定権をISACAだけが持ち、ISACAの決定が最終であることを理解します。

私は、本条項の記述を読んで理解し、本条項により法的に拘束されることに同意します。

申請者の署名 _____ 日付 _____

ステップ6.申請書の提出

申請書および証明フォームは、**isaca.force.com/support/s/application-submission**で送信/アップロードしてください。

ドロップダウンメニューから「**CISM**」を選択し、申請書をアップロードして「**Submit（送信）**」をクリックします。

送信された申請書の処理には、およそ2〜3週間かかります。承認されたら、電子メールでお知らせします。MyISACAプロフィール(**isaca.org/myisaca**)に入力された第一住所宛に、認定パック（承認レター、CISM認定証、金属製CISMピン）を郵送いたします。配達までに4〜8週間ほどお時間をいただきます。予めご了承ください。

CISM Certified Information Security Manager An ISACA® Certification

認定申請書 | *申請条件：2022年6月以降のCISM試験合格者*

申請者の詳細情報

申請者の氏名 _____ ISACA ID _____

証明者向けのフォーム記入手順

申請者（上の欄の記名者）は、ISACAによるCISM認定に申請します。ISACAでは、申請者の実務経験が真実であることを、勤務先の上司または管理者に独立して証明することを義務付けています。肉親または親戚が証明者になることはできません。また、人事部が証明者の代わりを務めることもできません。

このフォームを記入することで、あなたは申請者の実務経験が添付された申請フォーム（A-1ページ）に記載されるとおりであり、CISMジョブ・プラクティスドメインおよびタスクの記述（V-2ページ）の規定に従っていることを証明するものとします。

この証明フォームは、申請者が提出するものであるため、申請者にお戻しください。ご不明な点がある場合は、ISACAまで電子メール(**support.isaca.org**)または電話(**+1-847-660-5505**)でお問い合わせください。

証明者情報

証明者の氏名 _____

会社名 _____ 役職 _____

電子メール _____ 電話番号 _____

証明者への質問

1. 私は、申請者が積んだ以下の情報セキュリティマネジメントにおける実務経験が、A-1ページに記載されたとおりであることを証明します。

   （該当するすべての項目にチェックマークを付けてください）

   ☐ セクションA：会社名1　☐ セクションA：会社名3

   ☐ セクションA：会社名2　☐ セクションA：会社名4

2. 私は、以下の一般情報セキュリティにおける実務経験が、A-1ページのセクションBおよび/またはCに記載されたとおりであることを証明します。

   （該当するすべての項目にチェックマークを付けてください）

   ☐ セクションB：一般IS実務経験の免除　☐ セクションC：IS管理実務経験の免除

3. 私は、申請者にとって以下の役職に就いていました。*（少なくとも1つに必ずチェックマークを付けてください）*

   ☐ 上司　☐ 管理者　☐ 同僚　☐ クライアント

4. 私は、セクションAに記載された実務経験を証明する場合、私は、申請者の業務内容が、私の知りうる限りにおいて、このフォームのV-2ページに記載されるとおりであることを証明できます。

   ☐ はい　☐ いいえ

証明者の同意

私は、私の知りうる限りにおいて、V-1およびV-2ページに記載された情報が正しく、申請者が情報システムマネージャーとして認定されてしかるべきであることを確認します。私は、必要であれば、上記の情報に関するISACAからの質問に答えることにも進んで協力します。

証明者の署名 _____ **日付** _____

CISM Certified Information Security Manager® An ISACA® Certification

認定申請書 | *申請条件：2022年6月以降のCISM試験合格者*

ジョブ・プラクティスドメインの説明

申請者は、一部あるいはすべてのタスクが完了しているドメインにチェックマークを付ける必要があります。

☐ ドメイン1. 情報セキュリティガバナンス

タスクの記述：

- 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。
- 組織の目標と目的に整合した情報セキュリティ戦略を確立し、維持する。
- 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。
- 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。
- 標準、手続、ガイドラインの策定の指針となる情報セキュリティポリシーを確立し、維持する。
- 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。
- 情報セキュリティ戦略を導入する支援のために、最高幹部や他の利害関係者からの継続的なコミットメントを得る。
- 組織、および権限系統全体において情報セキュリティの責任を定義、伝達、モニタリングする。
- 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。
- 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。

☐ ドメイン2. 情報セキュリティリスクマネジメント

タスクの記述：

- 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。
- リスクの特定、リスクアセスメント、リスク対処プロセスに参加し、監督する。
- 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。
- 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。
- 情報セキュリティコントロールが適切で、リスクを受容可能なレベルにまで抑えて効果的に管理しているかどうかを判別する。
- 情報リスクマネジメントをビジネスおよびITプロセスに統合することを促進する。
- リスクのリ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。
- リスクマネジメントに関する意思決定プロセスを促進するために、違反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。

☐ ドメイン3. 情報セキュリティプログラム

タスクの記述：

- 情報セキュリティプログラムの活動、傾向、全体的な有効性に関する報告書を作成し、主要な利害関係者に提出する。
- 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。
- 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、維持する。
- 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的にあわせる。
- 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、維持する。
- 組織の情報セキュリティポリシー、標準、ガイドライン、手続、その他の文書を確立、伝達、維持する。
- 情報セキュリティの意識向上およびトレーニング向けのプログラムを策定、推進、維持する。
- 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。
- 外部関係者が確立されたセキュリティ要件を遵守しているかモニタリングする。
- 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。
- 内部および外部の組織向けのコミュニケーション計画およびプロセスを確立し、維持する。

☐ ドメイン4. インシデント管理

タスクの記述：

- 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、維持する。
- 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。
- 情報セキュリティインシデントのタイムリーな特定を確実にするように、プロセスを開発し、導入する。
- 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、維持する。
- 封じ込め、通知、エスカレーション、根絶、復旧などのインシデントハンドリングプロセスを確立し、維持する。
- インシデント対応チームを組織、訓練し、装備を与え、責任を割り当てる。
- 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実施することで、インシデント管理計画を評価する。
- 継続的向上を促進するために、原因分析、学んだ教訓、是正処置、リスクの再評価などのインシデント事後レビューを実施する。

ISACA