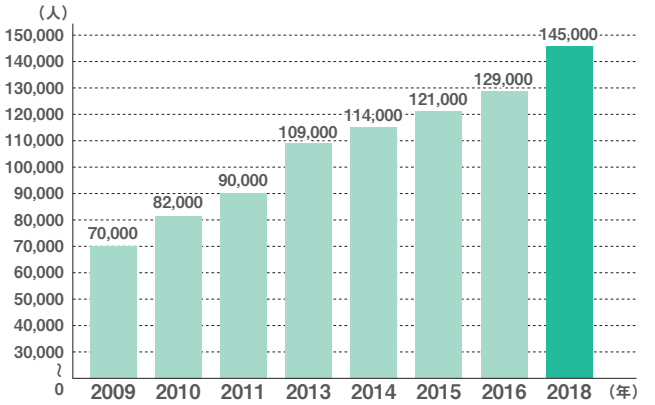
CISA®（公認情報システム監査人）とは

情報システム監査とは、情報システムの信頼性・安全性・効率性を検証し、評価することです。
ビジネス環境における情報システムの急速な普及によって、情報システムは企業の目標達成と存続に不可欠な要素として、ビジネスの根幹を支えています。
それは同時に、情報システムが様々なリスクに晒されていることを意味します。例えば、情報システム運用コストの肥大化、システム障害、情報の漏えいなどです。企業における相次ぐ個人情報の流失事件は、当該企業や社会に与える影響の大きさから、システム監査の重要性を認識させる契機となっています。
上記のリスクに対し、情報システム監査人は、ただチェックシートにマークをしていくだけでは職責を果たせません。経営者と同じ目線に立って監査し、経営者に改善を促す役目が求められています。

能力と専門性を証明する国際資格

公認情報システム監査人を意味するCISA®とは、"Certified Information Systems Auditor"の略称です。情報システム監査、セキュリティ、コントロールに関する指導的な役割を担うISACA®（情報システムコントロール協会）が認定する国際的な資格です。情報システム監査人の能力と専門性を証明することを目的に、1978年より開始されたCISA®資格認定試験は、約80の国で実施され、2018年時点で累計145,000人以上の資格認定者がいます。



CISA®累計認定者の推移

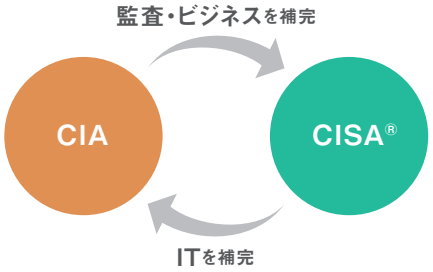
ISACA®（Information Systems Audit and Control Association：情報システムコントロール協会）

1976年にアメリカで設立。情報システム監査基準の作成、CISA®（公認情報システム監査人）などの資格認定を行い、ITガバナンス・コントロール・セキュリティおよび情報システム監査のための世界的な指導的役割を担う組織。現在、全世界で140,000人以上の会員を擁している。日本には東京・大阪・名古屋・福岡に支部があり、会員数は約3,700人。

column

CIA（公認内部監査人）とCISA®の関連性とは？

監査関連の資格として、CIA（公認内部監査人）をご存知の方は多いでしょう。2つの資格の関連性をご紹介します。
CIAでは、「監査+ビジネス」を主に学習します。ビジネスの一部にITも含まれますが、最低限の用語の理解にとどまりますので、ITに関わるリスクおよび監査の着眼点について深くは触れられていません。
一方CISA®では、CIAで不足する「ITに係るリスクおよび監査の着眼点」を中心に学習します。ただし、監査の学習量はCIAの方が多いです。また会計・ファイナンス・経営戦略についてはCISA®では取り扱いません。それぞれの資格で不足する部分を補完し合うのが、ダブルライセンスの魅力です。
CISA®取得を目指している方は、その後CIAの取得を、既にCIAを取得されている方は、CISA®の取得を推奨いたします。



関連性のイメージ

情報システム監査の専門家として幅広く活躍

CISA®が日本国内で注目されるようになった契機は、2009年3月期より導入された「金融商品取引法(J-SOX)」です。導入以前は主に監査法人やコンサルティング会社に在籍する方がCISA®を取得されていましたが、導入後は事業会社の内部監査部門に在籍されている方の取得が増えました。内部監査業務を遂行する上でシステムやシステム監査に関する知識が不可欠であったためです。そして現在、リスク管理という観点から、情報システム部門やセキュリティ部門に在籍されている方の取得が増えています。
欧米においては、特にリスク管理の必要性が高い金融機関などを中心に、CISA®資格者が情報システム監査の専門家として幅広く活躍しています。今後日本においても、CISA®資格者の必要性が様々な業種でより一層高まることが予想されます。

事業会社の場合	監査法人の場合	コンサルティング会社の場合
内部監査部門	IT監査部門	ITオペレーション
情報システム部門	リスク・マネジメント部門	セキュリティ
セキュリティ部門		コンプライアンス
コンプライアンス部門		

Message

システム監査に要求されるレベルは高くなり、責任も大きく変化
～CISA®の視点で企業経営をサポートする重要性～

「システム監査」という言葉を聞いたとき、どのように思われるでしょうか?

・監査は少数の専門家のための技術である
・私は別の部署(開発部門、運用担当など)なので関係が無い
・経営管理の立場なので報告だけ受ければ良い

などのご感想が多いかもしれません。実は私も米国企業でシステム総責任者をしていた頃、同じような思いでしたし、毎年やってくるシステム監査もほとんど気にしていませんでした。しかし2004年の米国SOX法の実施を受けてからは、要求されるレベルが非常に高くなり、責任も格段に大きくなったと痛感することが多くなりました。ちょうどその頃、内部と外部の監査人の多くがCISA®資格を持っていることを知り、同じ土俵で競争していくためにも、システム監査の方法論を学ぼうとCISA®を取得しました。実際、IT責任者また経営者として問題点の洗い出し・改善・提案等を行ううえで、CISA®として身に付けた監査の視点が大いに役立ってきたと実感しています。

近年、幾つかの企業がGRC(Governance Risk Compliance)の成熟度の低さから不祥事を起こしています。経営者・運用者・開発者が常に監査の視点を持ち、企業のGRCをモニターし評価することは企業の防衛や発達に不可欠と言えます。
また、現代においてIT技術無しで運営できる事業体はほとんどありません。そのためIT以外の経営層の責任として、企業全体のガバナンス機構にIT分野を統合して行くことは必要不可欠となってきています。さらにITの進歩や通信ネットワークの拡張によって、事業の活動がよりグローバルになっていることから、事業体活動をグローバルな基準に準拠して監査・モニター・評価・改善する事は、ますます重要になってきています。

このような中、ISACA®が提供する資格については、世界約190カ国以上で14万人余りの有資格者の皆さまが活躍されており、支部も日本の4支部(東京・名古屋・大阪・福岡)を含む世界210都市以上で展開しています。その結果、世界中の多様な企業や政府関連組織でCISA®資格が広く認知され高い評価を受けております。
CISA®の受験をきっかけに、ぜひ体系的な知識を修得され、グローバルな人脈を築いてください。

五島 浩徳氏

CISA®,CGEIT®,CISM®,CRISC®,ABCP ISACA®
東京支部2015-2017年度会長兼理事
ファイブ・アイLLC ITコンサルティングパートナー
Asia-Pacific CACS/ISRM 2014議長
DRI Japan 理事

CISA® 試験について

■試験内容と合格基準

CISA®試験は、最新のCISA®業務分析から生み出された、5つの実務領域(ドメイン)に関する150問の4択問題で構成されています。下記のドメインと割合は、試験に出る質問の重要度を示します。なお、本試験ではドメイン順ではなく、ランダムに出題されます。

試験内容

主題内容		割合	出題形式	問題数	試験時間
ドメイン1	情報システム監査のプロセス	21%	4択	150問	4時間
ドメイン2	ITガバナンスとITマネジメント	17%			
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	23%			
ドメイン5	情報資産の保護	27%			

合格基準

CISA®試験の得点は、200～800ポイントのスケールド・スコアに換算され、450ポイント以上で合格となります。

■試験制度

コンピュータ試験(Computer-based Testing:CBT)

テストセンターのコンピュータで解答します。自由度が高く、多忙なビジネスパーソンでも受験に取り組みやすくなっています。また、世界中で日本語による受験が可能です。

試験日程

テストセンターの空きがあれば、1年中いつでも受験できます。ISACA® Webサイトから申し込み後、1年以内に受験します。その1年以内であれば、予約した日程の48時間前までに、無料で試験日程のリスケジュールが可能です。

不合格になった場合、再受験は初回受験から30日以上あける必要があります(再受験2回目以降は前回の受験から90日後)。

※再受験は1年以内に3回までとなっています。
(再受験ごとに、出願手続きは必要です)

受験申込

ISACA® Webサイトからオンラインで申し込み手続きが可能です(英語のサイトになりますが、受講生の皆さまには日本語手続きマニュアルをご用意しております)。

受験資格

18歳以上であればどなたでも受験可能です。
学歴、実務経験などの要件はありません。

結果通知

受験したコンピューター画面上で、試験終了時に仮結果が表示されます。その後、本結果がメールで通知されます。

受験料

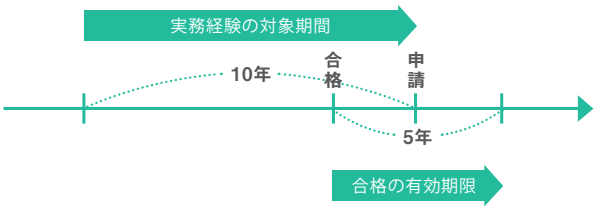
ISACA®会員	ISACA®非会員
U.S.$ 575	U.S.$ 760

※アビタス受講生は、アビタス経由の割安価格で申し込むことができます(バウチャー制度)。詳しくはスタッフまでお尋ねください。

※表示価格は2019年6月時点のもので、受験料は変動します。
必ずISACA® Webサイトでご確認ください。

■CISA®認定

CISA®と認定されるには、最低5年間の情報システム監査、コントロール、保証あるいはセキュリティ分野での実務経験を証明する必要があります(実務経験の詳細は次ページをご覧ください)。
これらの実務経験は、認定申請日からさかのぼって10年以内の経験に限ります。
合格の有効期限は5年間です。それまでに認定要件を満たさない場合は、失効してしまいますのでご注意ください。



以下の要件を満たすことで、実務経験に代替することができます(最大3年まで)。

- 最大1年間の情報システムまたは1年間の会計監査経験、業務監査経験は、1年間の経験に代替することができます。
- 取得した60〜120単位の大学の履修単位(2年または4年の学位相当)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年の経験に代替することができます。
- 情報セキュリティまたは情報技術の修士号は、1年間の経験に代替することができます。
- 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、1年間の経験に代替することができます。

■認定を維持する継続教育

CISA®認定を維持するには、所定時間以上の継続教育(CPE)が必要です。講義や研修などを受ける場合、1CPEは50分で、認定された翌年から1年で少なくとも20CPE、3年で120CPEを受講しなくてはいけません。
またCISA®維持手数料(ISACA®会員:$45、非会員:$85)の納入も必要です。

■ISACA® 入会費用(2019年6月時点)

入会費(初回のみ)	U.S.$ 30
国際会費	U.S.$ 135
支部費	東京:U.S.$ 50　大阪:U.S.$ 85 名古屋:U.S.$ 60　福岡:U.S.$ 80

上記の要件を満たせない場合、CISA®認定および合格実績が取り消されますのでご注意ください。

■ 実務経験

ドメイン1.情報システム監査のプロセス

- 情報システムが保護・管理され、組織に価値をもたらしているか否かを判断するため、監査を計画する。
- 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い、監査を実施する。
- 監査の進捗、発見事項、結果および提案を関係者に連絡する。
- 監査のフォローアップを行い、リスクへの対策が十分であるか否かを評価する。
- データ分析ツールを活用し、監査プロセスを効率化する。
- 情報システムの品質と統制を改善するため、組織にコンサルティングサービスおよびガイダンスを提供する。

ドメイン2.ITガバナンスとITマネジメント

- 組織の戦略および目的と足並みをそろえてIT戦略を評価する。
- ITガバナンス構造およびIT組織構造の有効性を評価する。
- 組織のITポリシーおよび実践手法の管理を評価する。
- 組織のITポリシーおよび実践手法が規制要件や法的要件に準拠しているかを評価する。
- 組織の戦略および目的と足並みをそろえてITリソースおよびポートフォリオ管理を評価する。
- 組織のリスク管理ポリシーおよび実践手法を評価する。
- ITマネジメントおよびコントロールのモニタリング体制を評価する。
- IT部門の重要目標に対する重要業績評価指標(KPI)を評価する。
- ITサプライヤの選別および管理プロセスがビジネス要件に準拠しているか否かを評価する。
- 組織のITポリシーおよび実践手法において、プロセスを改善する機会を識別すること。
- 新しいテクノロジー、規制、業界の実践手法に関連する潜在的な機会と脅威を評価する。
- 情報システムおよびエンタープライズアーキテクチャの定期レビューを実施する。
- 情報セキュリティプログラムを評価し、その有効性や組織の戦略および目標との整合性を検証する。
- ITサービスの管理実践手法がビジネス要件に準拠しているか否かを評価する。

ドメイン3.情報システムの調達、開発、導入

- 情報システムに対して提案した、変更のビジネスケースが、ビジネス目標を満たしているか否かを評価する。
- 組織のプロジェクト管理ポリシー、および実践手法を評価する。
- 情報システム開発ライフサイクルのあらゆる段階でのコントロールを評価する。
- 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する。
- 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否かを判定する。

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

- IT運営を評価し、それが効率的に管理され、組織の目標を支援し続けているか否かを判定する。
- IT保守の実践手法を評価し、それが効率的に管理され、組織の目標を支援し続けているか否かを判定する。
- データベース管理実践手法を評価する。
- データガバナンスのポリシーと実践手法を評価する。
- 問題/インシデント管理のポリシーおよび実践手法を評価する。
- 変更、構成、リリース、パッチ管理ポリシーおよび実践手法を評価する。
- エンドユーザーコンピューティングを評価し、プロセスが効率的にコントロールされているか否かを判定する。
- 組織がビジネス運営を継続する能力を評価する。
- 資産ライフサイクル管理に関連するポリシーおよび実践手法を評価する。

ドメイン5.情報資産の保護

- 組織の情報セキュリティおよびプライバシーポリシー/実践手法を評価する。
- 物理的コントロールと環境コントロールを評価し、情報資産が適切に保護されているか否かを判定する。
- 論理的セキュリティコントロールを評価し、情報の機密性、完全性、可用性を検証する。
- 組織の方針と該当する外部要件に合わせてデータ分類実践手法を評価する。
- 技術的セキュリティテストを実行し、潜在的な脅威と脆弱性を特定する。
- 新しいテクノロジー、規制、業界の実践手法に関連する潜在的な機会と脅威を評価する。

■実務経験の証明方法

実務経験の証明は、ISACA®Webサイトに用意されている定型フォーマットを用います。
右記のように該当するご経験にチェックを入れ、職場の上司からサインをもらうだけで終了です。書類一式を電子メールで送信してから、約8週間後に資格認定され、さらに約4週間経過すると認定証がお手元に届きます。
実務経験証明書は日本語で作成していただけます。

※実務経験の申請にあたり、$50が必要になります。


CISA 実務経験証明書
2019年6月以降の CISA 試験に合格した申請者
ISACA