

CISA (公認情報システム監査人) 2009年12月度試験

ISACA東京支部 CISA委員会 委員長
関谷浩之, CISA, CISM, CIA, CCSA

CISAの要件と試験

1. CISAとは？

企業の情報システムにおける、システム監査、セキュリティ、コントロール(管理)分野の国際資格。Certified Information Systems Auditorの略です。

2. CISAになるには？

CISAになるには以下の条件全てを満たす必要があります。

- ISACA (Information Systems Audit and Control Association)

が主催するCISAの試験に合格すること。

- ISACAが制定している、職業倫理規定の遵守。

- 実務経験(最低5年間)

(受験の前提資格ではない。合格後、実務経験を積む事も可能。)

- ・CISA認定を維持するには、年間20時間、3年間で120時間以上の継続教育が必要です。

3. CISA試験とは？

- ・200問の多岐選択問題(4択)、試験時間は4時間。
- ・試験の内容は、システム監査、システム開発・管理等からの幅広い出題。
- ・今年(2009年12月度)の試験日は、12月12日(土)に全世界統一で実施。
- ・日本語での受験が可能。(試験は外部の専門テスト機関に委託。)
- ・日本では、東京、大阪、名古屋、福岡、沖縄で行われる予定。

受験手続(1)

4. スケジュール、受験手続(1)

- 受験願書を、郵送、FAXで本部に送付。または、Web(オンライン登録)
早期締切り: 8月19日(水)(消印有効)
最終締切り: 9月23日(水)(消印有効)
- 受験料(カード支払い可)
- 早期締切り: ISACA 会員 US \$ 395、 非会員 US \$ 525
最終締切り: ISACA 会員 US \$ 445、 非会員 US \$ 575
(但し、オンライン登録の場合、上記金額よりさらに \$ 50 の割引となります。)

詳細につきましては米国本部のWEBページ <http://www.isaca.org/>)でご確認ください

- 申込後、オンライン登録の場合は、受験地と言語についての確認が送られてきます。
もし、間違っていた場合は、examregistrant@isaca.org に連絡してください。
試験の2, 3週間前には、本部より admission ticket が郵送されてきます。(12月1日までに到着しない場合は、certification@isaca.org に連絡してください)
- CISA試験対策コースを10月に開催予定
(ISACA東京支部のWEBで 申込受付
東京支部のWEBページ <http://www.isaca.gr.jp/>)でご確認ください)

受験手続(2)

4. スケジュール、受験手続(2)

・受験が不可能な場合には、米国国際本部のwebサイト (www.isaca.org/examdefer) でキャンセルあるいは繰越の受付可能です。

- | | | |
|---------------|------------|----------------------------|
| 1) 受験のキャンセル | 10月9日迄... | ・キャンセル料US \$ 100を引いた差額を返還。 |
| 2) 受験の次年度への繰越 | 10月16日迄... | ・再登録料US \$ 50必要 |
| | 11月25日迄... | ・再登録料US \$ 100必要 |

留意事項)

- 試験そのものは日本語で受験可能。ただし、願書申請手続きは必ず英語で行ってください。
- オンライン申込については、最初にユーザID、パスワードの登録と、ISACAのWEBページ [利用規約への同意が必要になります。これはISACAへの入会申請ではありません。](#)
- FAXで申請を行う場合は米国国際本部(+1-847-253-1443)宛。
- 申込締切日間際は、FAXが込み合いますし、オンライン画面で問題が発生しないとも限りません。早めのお申込を推奨します。

受験手続(3)

5. 試験当日の主な注意事項 事前にお手元のeチケットを良く読んでおいてください

- ・ 受験票(eチケット)を忘れずに！！
- ・ 有効な身分証明書(顔写真付きの公的なもの)を必ず持参。 (パスポート、運転免許証等写真つき！！)
- ・ 時間的に余裕をもって会場に到着し、受付を済ませてください。
前回東京試験での例)7:30までに受付に出頭せよ。試験官が説明を8:30に開始したら、試験場への入室不可(受験はできない)！！払い戻しもなし

解説・・・> “8:10に会場に到着したが、受付が非常に混んで時間がかかり、試験官の説明開始の8:30までに入室できない(受験できない)場合でも当方は責任は負いませんよ”という事

- ・ 筆記用具、消しゴムを必ず持参。(貸し出しはありません)
- ・ 飲食物、バッグ、筆箱、参考資料、辞書、電卓、クロック等は、しまい込むこと。
- ・ 携帯電話、カメラ、コンピュータ、PDA等は、室内への持ち込みも不可とされています。

6. 試験結果の通知

試験の合否通知については、約8週間でアメリカ本部より直接本人に郵送 されます。

合格基準は、スケールスコアで450点以上(200～800点中)。合格者にはスコアを記した合格証が送られます。(合格・不合格のいずれの場合も各章毎の得点内訳が送付されます。)

電話、メール等での個別の結果のお問い合わせには応じられません。

電子メールでの合否の通知をご希望の方は、願書No.10「電子Eメールアドレス」にご記入の上、NO.25を‘Y’とする。(certification@isaca.org をSPAMメールの対象から外すように)

試験内容(1)

7. 試験の分野 各ドメインの解説(1)

2006年6月度よりドメインが変更になっています。古いマニュアル等をお持ちの方はご注意ください。

- 1) 情報システム監査、コントロール、セキュリティの業務内容分野を示します。
- 2) カッコ内は、設問数の百分率及び出題数を示す。
- 3) 問題はランダムに出題されます。

ドメイン1. 情報システム監査のプロセス (10%)

組織の情報技術および業務システムが適切にコントロール、モニター、評価されていることを確認するため、一般に受け入れられた情報システムの標準やガイドラインに従って情報システム監査を行うプロセスの評価。

ドメイン2. ITガバナンス (15%)

情報システムの管理、計画、組織に関わる戦略、方針、基準、手続、および関連する実践内容の評価。

試験内容(2)

ドメイン3. システムとインフラストラクチャーのライフサイクル管理 (16%)

組織の業務目的を満たすことを確認するため、業務アプリケーション・システム開発、購入、導入、保守の方法論とそのプロセス、またリスクが組織の業務目的に従って管理されることを確認するため、業務システムとプロセスについての評価。

ドメイン4. ITサービスの提供と支援 (14%)

組織の技術上、運営上のインフラが適切に組織の業務目的をサポートすることを確認するため、その導入および継続的管理の効果と効率の評価。

ドメイン5. 情報資産の保護 (31%)

情報資産が許可無しに使用、開示、変更されたり、損傷、損失を受けないように保護するための組織上の業務要件を満たすことを確認するため、論理的、環境上、およびITインフラ関連のセキュリティの評価。

ドメイン6. 災害復旧と業務継続 (14%)

災害時の業務オペレーションと情報処理の継続に関する、文書化され、伝達され、テストされた計画を策定し維持するためのプロセスの評価。

サンプル問題(1)

経営陣へ監査結果を報告する前に、情報システム監査人がすべき事項は次のうちどれか。

- A. 被監査部門に、発見事項について確認する。
- B. エグゼグティブ・サマリーを作成し、被監査部門へ送付する。
- C. 提案事項を明確にし、監査委員会で発表する。
- D. 被監査部門より、発見事項および改善の対応について、同意を得る。

<解説> D

監査の終了後に、情報システム監査人は、被監査人と実施した監査の目的、テストや使用した評価技術、発見事項のテスト結果について、話し合わなければならない。情報システム監査人は、発見事項および被監査人が計画している改善対策について、同意または同意できない旨を確認しなければならない。

情報システム監査人は従業員退職時のコントロールについて監査を行っている。

下記選択肢のうち、レビューすべき最も重要な点はどれか？

- A. 退職について関連部署のスタッフに通知されていること。
- B. 退職者のユーザーIDとパスワードが削除されていること。
- C. 退職者の記録が現行の給与ファイルから除去されていること。
- D. 退職者に貸与されていた会社資産が返却されていること。

<解説> B

最もリスク高いのは、退職者による情報に対する論理的アクセスである。退職者のユーザーIDとパスワードが削除されていない場合、この種のアクセスの発生の可能性がある。ユーザーIDを無効あるいは削除していないと、退職者は物理的に会社に来なくとも情報へのアクセスが可能である。給与支払や会社資産の未返却に比べて、情報へのアクセスが発生した場合の潜在損失ははるかに大きい。

サンプル問題(2)

ISO - OSIのフレームワークの最上位レベル(アプリケーション層)で二つのネットワークを接続する装置は次のどれか？

- A. ゲートウェイ
- B. ルータ
- C. ブリッジ
- D. ブルータ

<解説> A

ゲートウェイは異なるプロトコルを使う二つのネットワークを接続するために使われる。接続は低位層の、名前で言えば、物理層、データリンク層、ネットワーク層、およびトランスポート層の接続をする。ルータは、ネットワーク層での装置であり、二つの接続されたネットワークは、同じネットワーク層のプロトコルでなければならない。ブリッジは、データリンク層で使われる。ブリッジは、トークンリングやイーサネットなどのネットワークを使うデータリンク層のプロトコルでなければならない。ブルータはいくつかのルータ機能を持ったブリッジである。

サンプル問題(3)

システムのアクセスルールをレビューしたところ、コンピュータ上のすべてのデータやプログラムへの技術サポート要員によるアクセスが制限されていないことを、情報システム監査人が発見した。このようなアクセス資格に対応する記述は、次のどれか。

- A. 適切であるただし、アクセスはすべてログをとること。
- B. 適切である。技術サポート要員は、すべてのデータやプログラムにアクセスできるからである。
- C. 適切でない。アクセスは、その地位にかかわらず、「need-to-know: 必要最小限」の原則にもとづいて制限されるべきである。
- D. 適切でない。技術サポート要員は、システムを実行させる能力があるためである。

<解説> C

技術サポート要員は、他のコンピュータユーザと同様、職務遂行上、必要な情報にだけアクセス許可を制限すべきである。すべての資源にアクセスしたいことは、正当な理由ではない。

サンプル問題(4)

二社間の災害相互援助協定の監査中に、情報システム監査人が最初に関心を持つべき事項は次のどれか。

- A. 影響分析の根拠の確実性
- B. ハードウェアとソフトウェアの互換性
- C. 情報システムポリシーと手順の差異
- D. システムテストの頻度

<解説> B

相互援助協定が有効であるためには、二つのサイトのハードウェアとソフトウェアに互換性がなければならない。これを確実にする手順は適切でなければならない。D、システムテストの頻度は関心事ではあるが、これを考慮するのは、それがハードウェアとソフトウェアの互換性をテストするからである。Aは計画の手順を調査するときには問題となるが、相互援助協定を調査する上では問題にならない。各組織が異なったポリシーと手続きを有していても、災害時に互いのサイトでシステムが互換的に走るか否かわからないため、Cは当てはまらない。

サンプル問題(5)

次の記述のうち、ドキュメンテーションの標準化の観点から最も有効なものはどれか。

- A. 記入者の視点から書くべきである
- B. 読み易い自然な言葉使いで書くべきである
- C. 組織をベースに書くべきである
- D. 第一の権威をもつ記入者が最終的な発言者になる

<解説> C

ドキュメントは、記入者の視点ではなく読者の視点から書かれなければならない - 書くのは一度でも、読まれるのは何度もあるからである。しかし、正確性及び意図しないあいまい性の不足は重要なことであり、多くの事例に対して自然な言葉使いの使用を拡大することを意味してはいない。十分に定義された可視的なモデルが、多くのドキュメントとともに重要になりそうである。ドキュメントの代表的ユーザーは、目的の適合性及び、記入者だけで決定していないような重要な課題についてレビューすべきである。一般的な組織では、明快性の視点と参照の容易性により記入者と読者の双方を手助けする。

参考資料

9. 試験の参考資料

参考資料は全て 国際本部 の Bookstore で購入可能

< 参考書 >

CRM9J 2009年公認情報システム監査人 (CISA) レビューマニュアル
料金 非会員：US\$135.00、 会員：US\$105.00

< 参考問題集 ... 過去問ではありません >

QAE8J 2008年CISA 試験サンプル問題&解答・解説集 (600問)
料金 非会員：US\$130.00、 会員：US\$100.00

QAE9JS 2008年CISA 試験サンプル問題&解答・解説集 (追加) (100問)
料金 非会員：US\$60.00、 会員：US\$40.00

Web画面での受験登録

1. 国際本部のHPを開く (<http://www.isaca.org/>)
2. Certification をクリック
3. CISA Certification の Exam をクリック
4. Register Online をクリック
5. 以降、項目を選択または入力
6. 支払方法(クレジットカードなど)を入力
7. 終了

以上 ご清聴ありがとうございました。
ご健闘をお祈りします。

ISACA東京支部 入会のご案内

2009年 8月4日
CISA/CISM試験受験者説明会

ISACA Tokyo Chapter

年会費について

会員期間: 1月1日から12月31日まで
 会員ルール: 国際本部入会と同時に最寄の支部会員になる
 会費の構成要素: (国際本部 + 支部) 年会費 + 国際本部入会費

2009年8月7日から2010年5月31日までお申込みの場合

区分	国際本部	東京支部
入会費	US \$ 30	無料
年会費	US\$130	US\$80
合計	US\$160	US\$80

会費合計: US\$240

2009年6月1日から2009年8月6日までお申込みの場合

区分	国際本部	東京支部
入会費	US\$30	無料
年会費	US\$65	US\$80
合計	US\$95	US\$80

会費合計: US\$175

- ・学生の方は本部会費が割引になります。(申請の際に証明する書類が必要)
- ・会費における割引制度
 1. 2009年6月1日 - 2009年8月6日までの申込み - 本部会費半額(会員資格期限2009年12月31日)
 2. 2009年8月7日 - 2010年5月31日までの申込み - 2010年度の申込みとする。(会員資格期限2010年12月31日)
 3. オンラインで申込みをされる場合は会費合計から20ドル安くなります。

ISACA Tokyo Chapter

会員の特典

受験料・参考書類の割引(CISA)

	会員	非会員	差額
受験料	\$ 375	\$ 505	\$ 130
レビューマニュアル(2009年版)	\$ 105	\$ 135	\$ 30
問題集(2009年版)	\$ 100	\$ 130	\$ 30
追加問題集(2009年版)	\$ 40	\$ 60	\$ 20
合計	\$ 620	\$ 830	\$ 210
入会金・会費	\$ 240	-	\$30

- 注) 1. 受験料は、2009年8月20日までの早期割引適用を受けた場合の価格です。2009年8月21日 から9月24日までにお申し込みは会員 / 非会員ともに50ドルアップします。
2. オンライン登録が可能です。受験料がさらに50ドル安くなります。
3. 会員にご登録いただくと今月の月例会からご参加いただけます。

ISACA Tokyo Chapter

会員の特典

受験料・参考書類の割引(CISM)

	会員	非会員	差額
受験料	\$ 375	\$ 505	\$ 130
レビューマニュアル(2008年版日本語)	\$ 75	\$ 100	\$ 25
問題集(2008年版)	\$ 60	\$ 80	\$ 20
追加問題集(2008年版)	\$40	\$60	\$20
合計	\$ 550	\$ 745	\$ 195
入会金・会費	\$ 240	-	\$45

- 注) 1. 受験料は、2009年8月20日までの早期割引適用を受けた場合の価格です。2009年8月21日 から9月24日までにお申し込みは会員 / 非会員ともに50ドルアップします。
2. オンライン登録が可能です。受験料がさらに50ドル安くなります。
3. 会員にご登録いただくと今月の月例会からご参加いただけます。

ISACA Tokyo Chapter

会員サービスについて

- CISA/CISM試験の受験、CISA/CISM認定後の継続教育だけでなく、さまざまな情報収集の機会が得られます。
- 国際本部から
 - 国際会議の参加料の割引
 - ISACA刊行出版物の割引
 - IS Control Journal などの定期購読
 - KNET(ナレッジDB)の利用
- 東京支部から
 - 月例会、研究会への参加(無料)
 - 支部の各種委員会や会議への参加
 - ボランティア活動(翻訳など)
 - 支部Webサイト会員限定ページの閲覧
 - 会報誌「Control Community」(メルマガ)の配布

CPE(継続教育時間)
へのカウント

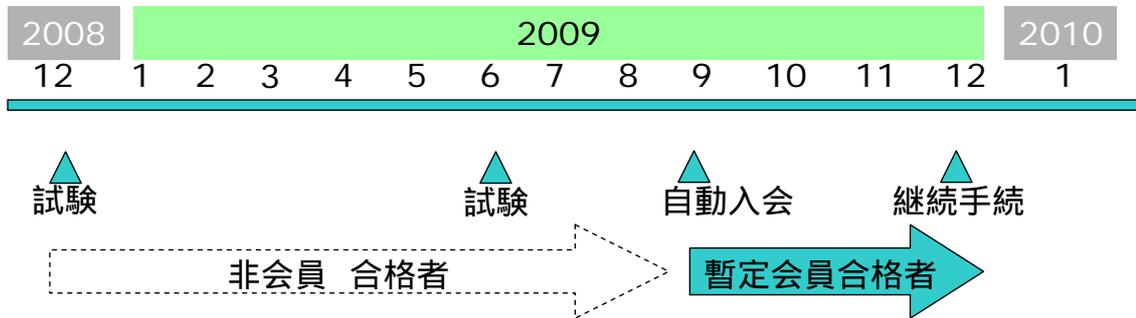
ISACA Tokyo Chapter

活動内容(CPEにカウントできます)

- 月例会
 - 先進的なテーマの講演など
 - メール及びHPにてご案内しています
- 研究会
 - 今期のテーマ:
 - 調査・研究委員会からアナウンス予定
 - 熱意のある方は参加も可能です。研究会活動にご興味のある方は担当委員にお問い合わせください。
(tkresearch@isaca.gr.jp)
- 委員会/ボランティア(最大10単位までカウント)
 - 教育/CISA/CISM/広報出版/翻訳など

ISACA Tokyo Chapter

会員になっていない方へ 暫定会員合格者の扱い



ISACAメンバーシップのメリット

- [COBIT 4.1](#) と関連製品の無料ダウンロード
- [COBIT Online](#) の基本機能が無料で利用でき、拡張機能の割引
- [CISA](#) および [CISM](#) 受験料と学習教材の割引
- 先端技術と管理者向けの [conferences](#) とワークショップの割引
- 現状や将来の技術や実践における記事や論文が掲載された隔月の [ISACA Journal](#), の定期購読と [Global Communiqué](#), メンバー刊行物
- グローバルITガバナンスのナレッジリソースである [K-NET](#) へのフルアクセス
- [research publications](#) および、専門家の意見にアクセスできる [Bookstore](#) 出版物の割引
- [IT Governance Institute](#) からのITガバナンスの視点での様々なドキュメントおよびプレゼンテーション
- 情報システム監査と統制のプロのための [Standards, statements and guidelines](#)
- メンバーのみがアクセスできるオンラインの資料には、専門家のリソースが含まれ、内部統制質問(ICQ)や、監査プログラムなどがあります
- プロテリティ社の KnowledgeLeader サイトへの年間アクセス権の割引
- IT 専門家に対する良い刺激を与える ISACA [boards/committees](#) を通じてリーダーシップとネットワーキングの機会

ISACAメンバーシップのメリット

- 継続教育プログラムや研究活動、および刊行物へのアクセス
- 定期的なチャプターの会議による情報交換の機会
- 支部のイベント、刊行物、研究活動に参加する機会
- 支部のイベントと機会を知らせるチャプターのコミュニケーション(ほとんどの領域)の行動
- 支部の委員会と委員会におけるリーダーシップ経験と、地元実業界での積極的に影響をあたえる機会

ISACA Tokyo Chapter

ISACAメンバーシップのメリット 専門的能力の開発

- ISACA eLibrary – ほとんどのISACA/ITGIの出版物に加え250以上の追加タイトルの包括的なライブラリ。メンバーは、いますぐISACA eLibraryへアクセス
- CISA, CISM, CGEIT 認定 — 試験と学習教材と登録費用の割引
- カンファレンスとトレーニング — 年間を通じて25以上のイベントの割引
- Webcasts と e-Symposia — 無料で月に3 CPEまで獲得できます
- 支部(チャプターレベル) 教育 — 通常の支部のミーティングやイベントを通じて割安なCPEプログラムへの参加や、情報交換ができます
- Bookstore — ISACA Bookstoreの出版物、調査資料の割引
- Career Centre Enhancements— さらに多くの仕事Access more jobs, including those posted on other job boards; more robust tools for job-seekers and, coming soon—a free job board for freelancers.
- My ISACA にアクセスし、プロフィールとCPE時間を更新しましょう

ISACA Tokyo Chapter



ISACAメンバーシップのメリット 専門的能力の開発



- ⑩ [ISACA Journal](#) — 隔月でのテクニカルジャーナルと無料CPEの追加情報
- ⑩ [GComm](#) — 月次のメンバーシップニュースレター, ISACAとITGIの最新情報をおとどけします
- ⑩ [COBITオンライン](#) — 無料の基本機能の利用と、フルアクセスの割引
- ⑩ [COBITクイックスタート](#) — 無料のダウンロード (\$55の価値)
- ⑩ [ダウンロード](#) — メンバーのみの調査ディスカウントもしくは、COBIT 4.1, Val IT, その他のITGIの出版物へのアクセス
- ⑩ [K-Net](#) — インターネットベースの6000以上の関連情報へのオンライン手データベースへのアクセス独占的なアクセス
- ⑩ [標準](#) — ISACAの情報システム監査標準ガイドラインと手続き
- ⑩ [監査プログラムと内部統制質問書 \(ICQs\)](#) — ベストプラクティスのためのガイドンスツール
- ⑩ [調査機会](#) — ITGIにおける研究のサポートでITガバナンス、コントロール、保証, アシュアランス、taburity専門家の製品開発