CISM/AAISMのご紹介

- 公認情報セキュリティマネージャー
  （Certified Information Security Manager® （CISM®））
- ISACA Advanced in AI Security Management™ （AAISM™）

2026年2月14日 ISACA東京支部 CISM委員会 委員長 荒木 粧子

アジェンダ

- CISMについて
- CISM勉強方法
- CISMサンプル問題
- AAISMについて
- AAISM勉強方法
- AAISMサンプル問題

ISACA Tokyo Chapter

CISMについて

ISACA
Tokyo Chapter

CISM：公認情報セキュリティマネジャー

- 情報セキュリティマネジメントの知識と経験を認定する国際的専門資格
- 認定要件：
  試験合格＋実務経験＋倫理規定
  実務経験5年（情報セキュリティ3年以上）

戦略的なエンタープライズセキュリティリーダーになる

Become a Strategic Enterprise Security Leader

CISMは4つの分野をカバー

■ 多くの組織で課題となる4つの領域に特化した知識と経験にフォーカス

Domain 1

情報セキュリティ ガバナンス

ガバナンスの枠組み確立および維持により、情報セキュリティ戦略が組織の目標・目的と一致することを保証する

Domain 2

情報セキュリティ リスク管理

組織の目標と目的を達成するため、リスク選好度に基づき、リスクを許容レベルまで管理する

Domain 3

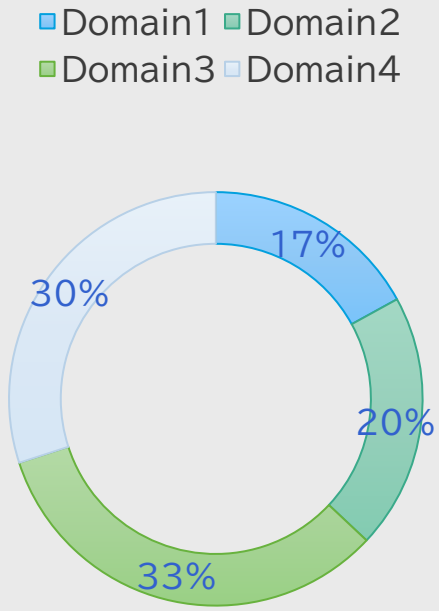
情報セキュリティ プログラム

組織の資産を識別、管理、保護し、情報セキュリティ戦略とビジネス目標に合わせて効果的なセキュリティの取り組みを支援するプログラムを開発し、維持する

Domain 4

インシデント管理

インシデントを検出、対応および回復させる機能を計画し、確立および管理することによりビジネスへの影響を最小限に抑える



CISM試験出題割合

CISM試験概要

- 四択問題：150問/4時間
- 試験資格は、登録から365日有効。試験日はほぼ通年。
- PSI試験会場 or 自宅PC（スペック要注意）にて受験可能
- 試験終了直後、その場で合否判定（暫定）
- 受験料：ISACA会員 $575 （非会員$760）
- 注意点：政府発行の写真付き身分証明書（パスポートや運転免許証等）必携 / 遅刻厳禁
  - 自宅受験の場合は、政府発行・英語表記・写真付きを満たす「パスポート」を推奨

CISMのキャリアパス

- 情報セキュリティ戦略をリードする力を証明する国際資格
  - CISMは経営視点でセキュリティ戦略を策定・運用できる能力を証明
- 現場担当からCISOクラスへ――
  キャリアアップしたい方に最適

- 一般的なキャリアパスと対象者：
  - CISOおよびCSO
  - セキュリティ担当マネージャー／コンサルタント
  - IT担当マネージャー／コンサルタント
  - コンプライアンス／リスク／プライバシー担当マネージャー

業界でも注目される資格

- 2025年SCアワード
  「最優秀プロフェッショナル認定プログラム」受賞
- CIO Magazine誌
  「2025年最も価値のあるIT認定資格」
  トップ15に選出

Press Releases 2025 ISACAs CISM Named Best Professional Certification Program in 2025 SC Awards

米国国防総省サイバー従事者に求める資格

CISMは、米国国防総省（DoD）が定める「DoD 8140 サイバーワークフォース資格フレームワーク」において、複数のサイバー／IT管理系ワークロールに対する承認資格（Approved Qualification）として位置づけられています。

DoD 8140 Qualification Matrices よりCISMを抜粋（2026年2月4日時点）
https://www.cyber.mil/dod-workforce-innovation-directorate/dod8140/qualification-matrices

WRC	Work Role Title	Element	Acronym	Proficiency
422	Data Analyst	Data/AI	CISM	Advanced
541	Vulnerability Assessment Analyst	Cybersecurity	CISM	Advanced
611	Authorizing Official/Designated Representative	Cybersecurity	CISM	Advanced
612	Security Control Assessor	Cybersecurity	CISM	Advanced
652	Security Architect	Cybersecurity	CISM	Advanced
722	Information Systems Security Manager	Cybersecurity	CISM	Advanced
723	COMSEC Manager	Cybersecurity	CISM	Advanced
751	Cyber Workforce Developer and Manager	Cyberspace Enablers	CISM	Advanced
752	Cyber Policy and Strategy Planner	Cyberspace Enablers	CISM	Advanced
801	Program Manager	Cyberspace Enablers	CISM	Advanced
802	IT Project Manager	Cyberspace Enablers	CISM	Advanced
804	IT Investment/Portfolio Manager	Cyberspace Enablers	CISM	Advanced
805	IT Program Auditor	Cyberspace Enablers	CISM	Advanced

参考）CISA and CISM Recognized by U.S. Department of Defense 8140 as Approved Qualifications for DoD Cyber Workforce
https://www.isaca.org/about-us/newsroom/press-releases/2024/cisa-and-cism-recognized-as-approved-qualifications-for-dod-cyber-workforce

METI:サイバーセキュリティ体制構築・人材確保の手引き

■ 経済産業省の手引きにも「活用可能な試験・資格の例」として掲載

戦略マネジメント層	経営リスクマネジメント	CRISC	組織におけるリスクマネジメント（リスク認識・評価）や情報システムコントロールの設計・導入・運用に携わる人材	無	ISACA
	システム監査	公認情報システム監査人(CISA)	情報システムの監査および、セキュリティ、コントロールに携わる人材	有	ISACA
		システム監査技術者試験	監査対象から独立した立場で、情報システムや組込みシステムを総合的に点検・評価・検証して、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性などに対する保証を与える、又は改善のための助言を行う人材	有	IPA
	セキュリティ監査	公認情報セキュリティ監査人(CAIS)	情報セキュリティ監査の計画立案、監査実施、報告書の作成及び監査結果の被監査主体への報告等を担う人材	有	JASA
	セキュリティ統括	公認情報セキュリティマネージャー(CISM)	企業・団体等の情報セキュリティプログラムに係る、マネジメント、設計、監督を行う人材	有	ISACA
	デジタルシステムストラテジー	ITストラテジスト試験	企業の経営戦略に基づいて、ビジネスモデルや企業活動における特定のプロセスについて、情報技術（IT）を活用して事業を改革・高度化・最適化するための基本戦略を策定・提案・推進する人材等	有	IPA

「サイバーセキュリティ体制構築・人材確保の手引き」（第2.0版）をとりまとめました（METI/経済産業省）

スキル標準（ISVマップ）

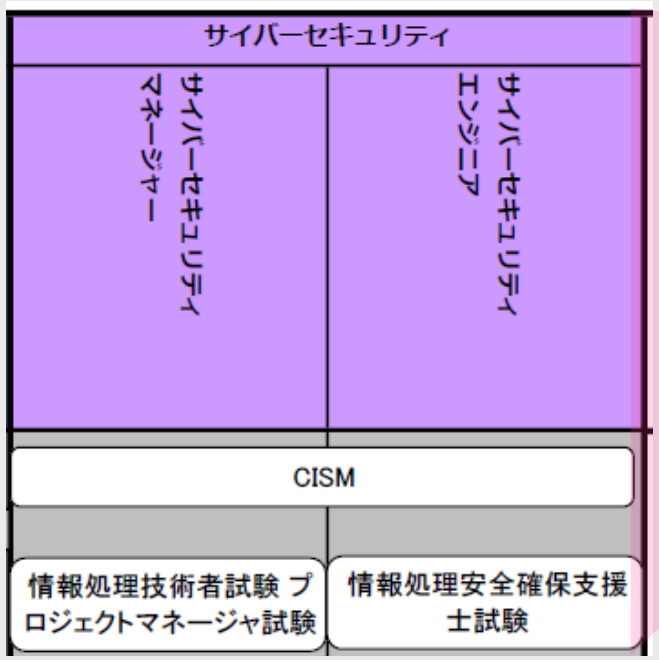
■ スキル標準 ISVマップとは？

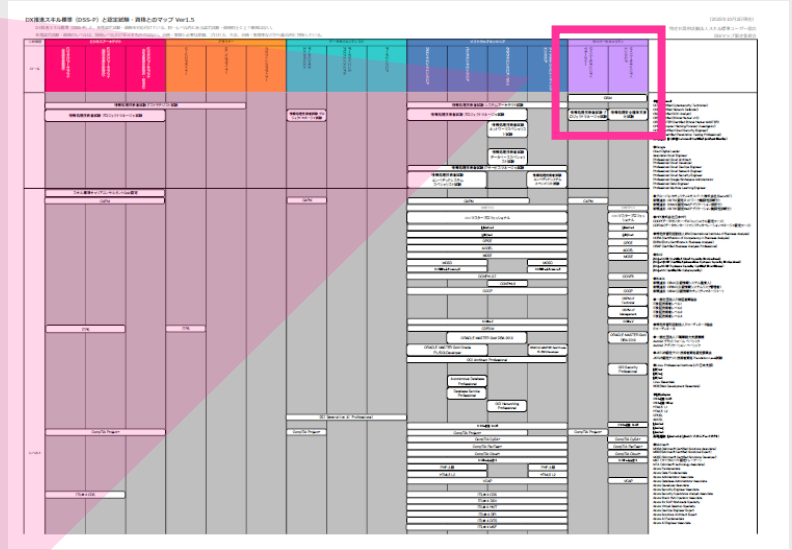
- スキル標準ユーザー協会で作成しているスキル標準マップ
- ISVマップは厚生労働省の人材開発支援助成金の対象資格としても参照される。

■ ISACA資格は ITSSレベル4相当として 2025年12月に正式追加

- CISA、CISM、CRISC

●ISACA
新規追加　CISA（公認情報システム監査人）
新規追加　CRISC（公認情報システムリスク管理者）
新規追加　CISM（公認情報セキュリティマネージャー）



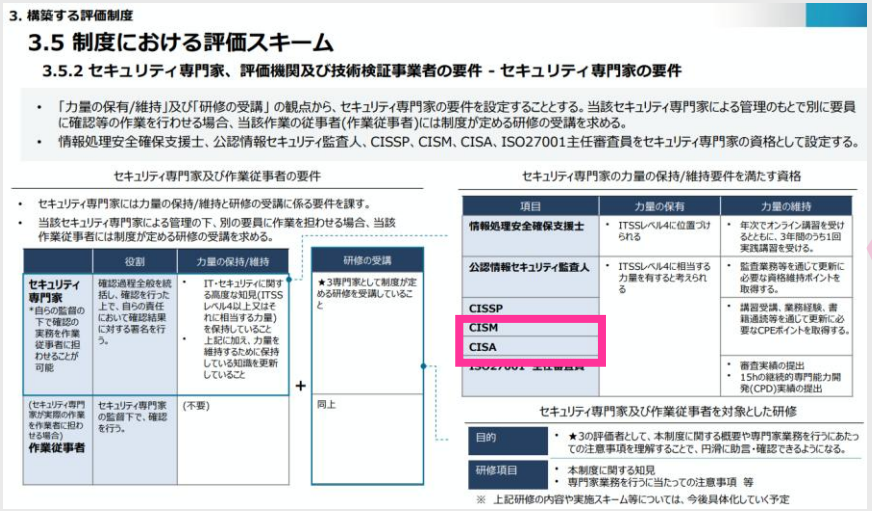


ISVマップ｜資格・研修関連情報｜スキル標準ユーザー協会 公式サイト

METI: サプライチェーンセキュリティ評価制度★3専門家

■ サプライチェーン強化に向けたセキュリティ対策評価制度

- 2026年度末の運用開始を目指す、セキュリティ対策のレベルを可視化する取り組み
- ITSSレベル4相当のCISMとCISAは、★3セキュリティ専門家に必要とされる資格となる見込み



3. 構築する評価制度

3.5 制度における評価スキーム

3.5.2 セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件

- 「力量の保有/維持」及び「研修の受講」の観点から、セキュリティ専門家の要件を設定することとする。当該セキュリティ専門家による管理のもとで別に要員に確認等の作業を行わせる場合、当該作業の従事者(作業従事者)には制度が定める研修の受講を求める。
- 情報処理安全確保支援士、公認情報セキュリティ監査人、CISSP、CISM、CISA、ISO27001主任審査員をセキュリティ専門家の資格として設定する。

セキュリティ専門家及び作業従事者の要件

- セキュリティ専門家には力量の保持/維持と研修の受講に係る要件を課す。
- 当該セキュリティ専門家による管理の下、別の要員に作業を担わせる場合、当該作業従事者には制度が定める研修の受講を求める。

	役割	力量の保持/維持	研修の受講
セキュリティ専門家 *自らの監督の下で確認の実務を作業従事者に担わせることが可能	確認過程全般を統括し、確認を行った上で、自らの責任において確認結果に対する署名を行う。	・IT・セキュリティに関する高度な知見(ITSSレベル4以上又はそれに相当する力量)を保持していること ・上記に加え、力量を維持するために保持している知識を更新していること	★3専門家として制度が定める研修を受講していること
(セキュリティ専門家が実際の作業を作業者に担わせる場合) 作業従事者	セキュリティ専門家の監督下で、確認を行う。	(不要)	同上

セキュリティ専門家の力量の保持/維持要件を満たす資格

項目	力量の保有	力量の維持
情報処理安全確保支援士	・ITSSレベル4に位置づけられる	・年次でオンライン講習を受けるとともに、3年間のうち1回実践講習を受ける。
公認情報セキュリティ監査人	・ITSSレベル4に相当する力量を有すると考えられる	・監査業務等を通じて更新に必要な資格維持ポイントを取得する。
CISSP		・講習受講、業務経験、書籍通読等を通じて更新に必要なCPEポイントを取得する。
CISM		
CISA		
ISO27001 主任審査員		・審査実績の提出 ・15hの継続的専門能力開発(CPD)実績の提出

セキュリティ専門家及び作業従事者を対象とした研修

目的	・★3の評価者として、本制度に関する概要や専門家業務を行うにあたっての注意事項を理解することで、円滑に助言・確認できるようになる。
研修項目	・本制度に関する知見 ・専門家業務を行うに当たっての注意事項 等

※ 上記研修の内容や実施スキーム等については、今後具体化していく予定

セキュリティ専門家の力量の保持/維持要件を満たす資格

項目	力量の保有	力量の維持
情報処理安全確保支援士	・ITSSレベル4に位置づけられる	・年次でオンライン講習を受けるとともに、3年間のうち1回実践講習を受ける。
公認情報セキュリティ監査人	・ITSSレベル4に相当する力量を有すると考えられる	・監査業務等を通じて更新に必要な資格維持ポイントを取得する。
CISSP		・講習受講、業務経験、書籍通読等を通じて更新に必要なCPEポイントを取得する。
CISM		
CISA		
ISO27001 主任審査員		・審査実績の提出 ・15hの継続的専門能力開発(CPD)実績の提出

「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針(案)」(SCS評価制度の構築方針(案))を公表しました (METI/経済産業省)

CISM：資格認定の申請について

■CISM委員会のFAQ（CISM関連FAQ）

https://www.isaca.gr.jp/cism/cismqa.html

■申請方法2種

- Webフォーム（英語のみ） or PDF（日本語版あり）をWeb提出

■5年間の実務経験報告

- 情報セキュリティマネジメント＝管理職位の意味ではありません。
  申請書をよくお読みください。
  CISA保有で2年間の免除などもあります。

CISM勉強方法

ISACA
Tokyo Chapter

CISM：勉強方法❶

- 印刷版の書籍（Print）と、オンライン閲覧が可能なデジタル版（Digital）の他、
  QAEは1年間のオンライン利用が可能なデータベースが提供されています。
- 詳細はISACA国際本部の Store > Exam Prep > CISMカテゴリをご参照ください。

CISM Review Manual, 16th Edition 2024 | Print | Japanese
$109.00　Member Pricing / $139.00　Non-member Pricing

CISM Review Manual, 16th Edition eBook 2024 | Digital | Japanese
$109.00　Member Pricing / $139.00　Non-member Pricing

CISM Review Questions, Answers & Explanations Manual, 10th Edition | Print | Japanese
$129.00　Member Pricing / $159.00　Non-member Pricing

CISM Questions, Answers & Explanations Database 2024 | Japanese
$299.00　Member Pricing / $399.00　Non-member Pricing

※この他、CISM Online Review Course 2024（英語のみ、11CPE）もあります
$795.00 Member Pricing / $895.00 Non-member Pricing

ISACA Tokyo Chapter

CISM：勉強方法❷

■ CISM試験レビューコース（四半期ごとに開催）

- 日本人講師による2日間（10時間）の解説コース
- 開催方法： オンラインでのライブ講習（Zoom）
- 料金： 東京支部会員 5,000円、それ以外の方 9,000円
- CPE証明： 12.25CPEの証明書を発行（CISAなどにもCPE適用可能）
- 次回は3月7日（土）・8日（日）に開催予定です：
  - https://www.isaca.gr.jp/cism/index.html#cism03

- 限られた時間でコンパクトに解説する、試験対策の短期集中コースです。
- 受験者ご自身の勉強に役立つ情報提供を目的としており、合格を保証するものではありません。
- 内容だけではなく、受験や認定申請に関するご質問にも可能な範囲でお答えしていますが、正式には国際本部にお問い合わせいただくことになります。
- CPE獲得や学び直しのための参加も大歓迎です、お気軽にご参加ください！

CISMサンプル問題

ISACA
Tokyo Chapter

CISMサンプル問題❶

- 組織の主要な提案された購入と新しいプロセスについて、リスク評価とビジネス影響分析（BIA）が完了した。情報セキュリティマネージャーと、結果の評価と特定されたリスクの責任を負う事業部門マネージャーとの間には意見の相違がある。情報セキュリティマネージャーの最善のアプローチは次のうちどれか？

- A. 企業へのリスクに関するビジネスマネジャーの決定の受け入れ
- B. 企業へのリスクに関する情報セキュリティマネージャーの決定の受け入れ
- C. 最終的なインプットのための経営幹部によるリスク評価のレビュー　　正解はC
- D. 不一致を解決するために、新しいリスク評価とBIAを作成します

経営幹部は、組織全体の全体像とセキュリティと機能の間のトレードオフを検討するのに最適な立場にあります。

国際本部　CISMサンプル問題（10問）をCISM委員会にて和訳。
https://www.isaca.org/credentialing/cism/cism-practice-quiz

CISMサンプル問題❷

- セキュリティインシデントの事後レビューにより、監視されていないプロセスがあったことが明らかになり、その結果、監視機能が実装された。この修正から最も期待できるのは次のうちどれか？

- A. 総インシデント期間の短縮
- B. リスク許容度の向上
- C. 識別の改善
- D. エスカレーションの促進

正解はC

主要なプロセスが監視されていない場合、その監視の欠如は、セキュリティの脆弱性または脅威が発見されないままになり、セキュリティインシデントが発生する可能性があります。一貫した監視が実装されると、脆弱性と脅威の識別が向上します。

国際本部　CISMサンプル問題（10問）をCISM委員会にて和訳。
https://www.isaca.org/credentialing/cism/cism-practice-quiz

公認情報セキュリティマネージャー（CISM）は
情報セキュリティマネジメントの
グローバルスタンダードを学べる国際的な資格

ISACA東京支部 CISM委員会

https://www.isaca.gr.jp/cism/

ISACA国際本部 CISM紹介ページ

https://www.isaca.org/credentialing/cism

AAISMについて

ISACA
Tokyo Chapter

AAISMについて

■ ターゲット

- AIセキュリティマネジメント特化の上位資格
- CISM/CISSPを保有するセキュリティ専門家が、AI特有の脅威環境におけるリスクプロファイルを適切に管理し、AIをセキュリティ運用に取り入れる能力を強化する。

■ 認定条件

- 有効なCISMまたはCISSP (ISC2)保有
- AAISM試験の合格
  - 90問、2時間30分、英語・スペイン語・日本語
- 申請手数料($50)、倫理規定・CPEポリシー遵守
  - 年間10CPE

ISACA Advanced in AI Security Management™ (AAISM™)は、経験豊富なITプロフェッショナルが企業のセキュリティ体制を強化し、AI特有の脅威から保護できるよう設計された、業界初かつ唯一のAI中心のセキュリティ管理認定資格です。AIに関連する進化するセキュリティリスクを管理し、ポリシーを適用し、組織全体でAIを責任を持って効果的に活用できるようになります。

- AAISM™—AI Security Management™
- ISACA AAISM FAQs
- AAISM紹介ウェビナー
  (2025/8/12開催、アーカイブ視聴は2026/8/12まで)

ドメイン構成

Domain 1 – AI Governance and Program Management (31%)

AIガバナンスとプログラムマネジメント

- A–利害関係者の考慮事項、業界フレームワーク、および規制要件
- B–AI関連の戦略、ポリシー、および手続き
- C–AI資産とデータのライフサイクル管理
- D–AIセキュリティプログラムの開発と管理
- E–事業継続とインシデント対応

Domain 2 – AI Risk and Opportunity Management (31 %)

AIリスクと機会マネジメント

- A–AIリスク評価、しきい値、処置
- B–AIの脅威と脆弱性の管理
- C–AIベンダーおよびサプライチェーンの管理

Domain 3 – AI Technologies and Controls (38%)

AI技術とコントロール

- A–AIセキュリティアーキテクチャと設計
- B–AIライフサイクル(モデル選択、トレーニング、検証など)
- C–データ管理コントロール
- D–プライバシー、倫理、信頼、セキュリティコントロール
- E–セキュリティコントロールとモニタリング

※ 詳細は、以下をご参照ください:
https://www.isaca.org/credentialing/aaism

AAISM試験概要

- 四択問題：90問/2.5時間
- 試験資格は、登録から365日有効。試験日はほぼ通年。
- PSI試験会場 or 自宅PC（スペック要注意）にて受験可能
- 試験終了直後、その場で合否判定（暫定）
- 受験料：ISACA会員 $459 （非会員$599）
- 注意点：政府発行の写真付き身分証明書（パスポートや運転免許証等）必携 / 遅刻厳禁
  - 自宅受験の場合は、政府発行・英語表記・写真付きを満たす「パスポート」を推奨

AAISMの価値

■ AIセキュリティマネジメントを体系的に学べる

- ITシステムとは異なるAI特有のセキュリティリスクを学べる
- AIによって社会全体がアップデートされつつあるいま、AIのセキュリティリスクとマネジメントに関するグローバルスタンダードを学ぶことは大きな価値

■ 時代が求めるAIセキュリティマネジメントのスキルを国際的な資格で証明できる

- 明確に、AIセキュリティマネジメントにフォーカス
- CISMやCISSPの保有者を対象とすることで、前提となるスキルセットが明確

AAISMは、このような方に最適

- 情報セキュリティマネージャー
- サイバーセキュリティマネージャー
- AIセキュリティマネージャー
- セキュリティ/コンプライアンス担当ディレクター
- 情報セキュリティ担当VP/AVP
- 最高情報セキュリティ責任者（CISO）

AAISM勉強方法

ISACA
Tokyo Chapter

AAISM: 勉強方法

- 印刷版の書籍(Print)と、オンライン閲覧が可能なデジタル版(Digital)の他、
  QAEは1年間のオンライン利用が可能なデータベースが提供されています。
- 詳細はISACA国際本部の Store > Exam Prep > AAISMカテゴリをご参照ください。

ISACA AAISM Official Review Manual | Print | Japanese
$89.00 Member Pricing / $105.00 Non-member Pricing

ISACA AAISM Official Review Manual | Digital | Japanese
$89.00 Member Pricing / $105.00 Non-member Pricing

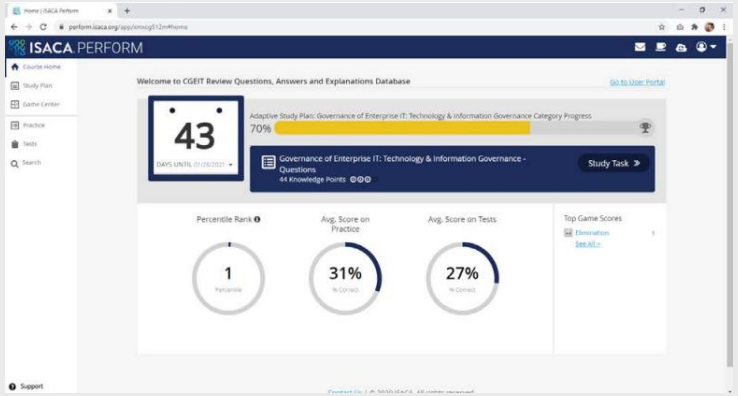
ISACA AAISM Questions, Answers, & Explanations, 12 Month Database | Japanese
$249.00 Member Pricing / $349.00 Non-member Pricing

※この他、ISACA AAISM Online Review Course(英語のみ、11CPE)もあります
$449.00 Member Pricing / $549.00 Non-member Pricing

AAISM QAE DB/RM 補足情報

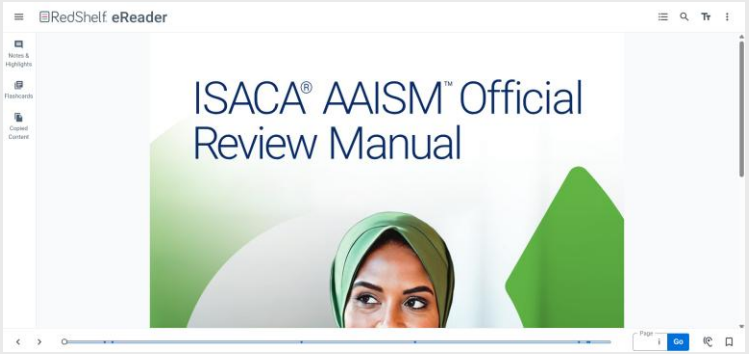
■ AAISM QAE DB（1年間）

- □ オンライン学習用の問題データベース
  - ● 学習スケジュールやクイズ、間違えた問題をチェックするなどの機能多数
- □ 全258問 ※2026年2月時点
- □ QAE DBのマニュアル：
  - ● Learning: How do I access my Question, Answer and Explanations (QAE) database?



■ AAISM Review Manual

- □ デジタル版は、RedShelfというWebアプリで閲覧する形で提供
  - ● Learning: How do I navigate the content in my eBook on ISACA's browser-based eBook platform?（動画あり）



AAISMサンプル問題

ISACA
Tokyo Chapter

AAISMサンプル問題❶

- AIガバナンスと組織の事業目標との整合性を確保するために最もよい最初のアクションは、次のうちどれですか？

正解はA

- A. 役割、目標、および監視の責任を定義するAI憲章を作成すること
- B. 生成AIツールに関する受け入れ可能な利用ポリシー（AUP）を作成すること
- C. すべてのAIガバナンス関連活動を管理するために内部監査人を割り当てること
- D. AI展開の倫理的影響を監視するための主要リスク指標を確立すること

AI憲章は、スコープ、役割、および責任を文書化することにより、ガバナンスの構造化された基盤を提供します。これにより、事業目標との整合性が確保され、AI監視の指針となる文書として機能します。

国際本部　AAISMサンプル問題（10問）をCISM委員会にて和訳。
https://www.isaca.org/credentialing/aaism/practice-quiz

AAISMサンプル問題❷

- ある病院が、希少疾患の診断を支援するために外部ベンダーからAIソリューションを導入します。このテクノロジーのセキュリティ要件の検証を最も示すのは、次のうちどれですか？

- A. 定期的な情報セキュリティレビューを規定する契約条項を要求すること。
- B. 必須のセキュリティAIソフトウェア更新の契約条項を事前に確認すること。
- C. AIシステムに対して定期的な詳細な脆弱性スキャンを実行すること。
- D. ヘルスケア規制に整合した機密データの要件を統合すること。 正解はD

機密の臨床データに関するセキュリティ要件を最初から統合することにより、病院は、セキュリティ・バイ・デザインの原則として、すべてのデータ処理とAI操作が規制（例：HIPAA、GDPR）に準拠していることを保証します。

国際本部　AAISMサンプル問題（10問）をCISM委員会にて和訳。
https://www.isaca.org/credentialing/aaism/practice-quiz

AAISMサンプル問題❸

■AIセキュリティアーキテクチャを設計する際に、敵対的トレーニングを使用する主な目的は何ですか？

■ A. 標準データセットでのAIモデルのパフォーマンスを向上させること

■ B. AIモデルの意思決定の公平性を改善すること

■ C. 攻撃に抵抗するための計算コストを削減すること

正解はD

■ D. AIモデルを潜在的な攻撃に対してより回復力のあるものにすること

敵対的トレーニングの主な目標は、トレーニング中にモデルを敵対的な例にさらすことにより、モデルが攪乱に抵抗することを学習し、意図的に操作された場合でも入力を正しく分類できるようにすることです。

国際本部　AAISMサンプル問題（10問）をCISM委員会にて和訳。
https://www.isaca.org/credentialing/aaism/practice-quiz

AAISM(Advanced in AI Security Management™)で エンタープライズAIの未来を守る

ISACA東京支部 AAISMご紹介
https://www.isaca.gr.jp/cism/index.html#aaism

ISACA国際本部 AAISM紹介ページ
https://www.isaca.org/credentialing/aaism