

第13回情報セキュリティマネージャー
ISACAカンファレンス in Tokyo

CISM資格のご紹介

2025年2月15日 ISACA東京支部

Agenda

1. ISACA 資格およびCISM資格について
2. CISM資格の受験について
3. CISM資格関係のよくある質問

Agenda

1. ISACA 資格およびCISM資格について
2. CISM資格の受験について
3. CISM資格関係のよくある質問

ISACAの認定資格およびCISM資格について

資格				
専門領域	情報システムの監査 およびセキュリティ コントロール(1978-)	セキュリティマネジメント (2003-)	リスクマネジメントと コントロール (2010-)	ITガバナンス (2008-)
認定者	151,000+ (3,847)	48,000+ (848)	30,000+ (182)	8,000+ (92)

※カッコ内はISACA東京支部人数(2025年2月8日時点)

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*

米国国防総省(DoD)のサイバースペース従事者に求める資格

米国国防総省のDoD マニュアル 8140.03「サイバースペースワークフォース資格および管理プログラム」は、軍人、DoD サイバー従業員、請負業者など、部門のサイバースペース関連業務に従事する人々に関するポリシーと要件を規定しています。これには、教育、トレーニング、認定、経験、職務上の資格、環境固有の要件、継続的な専門能力開発など、これらの職位の資格要件が含まれます。

情報セキュリティマネージャー(CISM)は、このプログラムの一環として承認された職務の認定資格リストに含まれています。

DoD 8140 Qualification Matrices よりCISMを抜粋 (2025年2月6日時点)

<https://public.cyber.mil/wid/dod8140/qualifications-matrices/>

Acronym	Offering Type	Work Role Code	Work Role Title	Proficiency
CISM	Certification	541	Vulnerability Assessment Analyst	Advanced
CISM	Certification	611	Authorizing Official/Designating Representative	Advanced
CISM	Certification	612	Security Control Assessor	Advanced
CISM	Certification	652	Security Architect	Advanced
CISM	Certification	722	Information Systems Security Manager	Advanced
CISM	Certification	722	Information Systems Security Manager	Intermediate
CISM	Certification	723	COMSEC Manager	Advanced
CISM	Certification	723	COMSEC Manager	Intermediate
CISM	Certification	801	Program Manager	Advanced
CISM	Certification	804	IT Investment/Portfolio Manager	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>

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

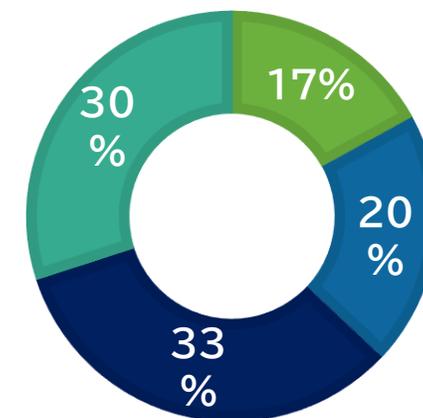
組織の資産を識別、管理、保護し、情報セキュリティ戦略とビジネス目標に合わせて効果的なセキュリティの取り組みを支援するプログラムを開発し、維持する

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

■ Domain1 ■ Domain2
■ Domain3 ■ Domain4



CISM試験出題割合

Agenda

1. ISACA 資格およびCISM資格について
2. CISM資格の受験について
3. CISM資格関係のよくある質問

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

ISACA認定試験受験者ガイド

https://www.isaca.org/-/media/files/isacadp/project/isaca/certification/exam-candidate-guides/2021/exam-candidate-guide_jpn.pdf

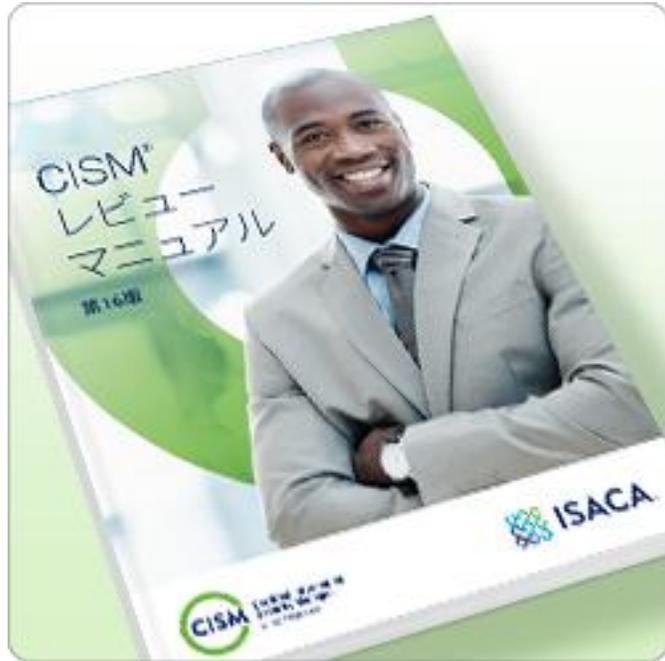
CISM関連Q&A

<https://isaca.gr.jp/cism/cismqa.html>

CISM試験準備方法

- ①自習用教材の利用
- ②日本のCISM委員会が主催するレビューコース
- ③国際本部が提供するオンラインコース（説明省略）
- ④国際本部が提供する試験準備コース（説明省略）

① 自習用教材(2022年6月改定反映後の最新版)



[CISMレビューマニュアル第16版\(Japanese\)](#)

会員価格 : \$109



[CISMサンプル試験問題解答解説第10版\(Japanese\)](#)

会員価格 : \$129

国際本部Webストアより購入可能です:

<https://store.isaca.org/s/store>

②CISM委員会による日本語でのレビューコース

- 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: 12CPEの証明書を発行(CISAなどにもCPE適用可能)
- 次回は、2025年3月8日(土)-9日(日)に開催予定

お申込み受付中:
<https://www.isaca.gr.jp/cism/index.html>

Agenda

1. ISACA 資格およびCISM資格について
2. CISM資格の受験について
3. CISM資格関係のよくある質問

よくある質問：CPE、費用

Q: CPEはCISA等と共用できますか？

ほとんど共有できます。

Q: 年間維持費は？CISAも持っていたら？

→本部\$135 + 東京支部\$30 + CISM\$45 = \$210

→本部\$135 + 東京支部\$30 + CISM\$45 + CISA\$45 = \$255

※上記は、2025年2月時点の、年会費更新時の費用です。
本部年会費は、更新は\$135、新規は\$145です。

よくある質問:どのような問題ですか？

<CISMサンプル問題①>

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ー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

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

正解はC

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)より

<https://www.isaca.org/credentialing/cism/cism-practice-quiz>

よくある質問:どのような問題ですか？

<CISMサンプル問題②>

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)より

<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
グローバルスタンダードを学べる
情報セキュリティマネジメントの国際資格です

詳細はISACA東京支部 CISM委員会まで
<https://www.isaca.gr.jp/cism/>

ISACA国際本部 CISM紹介ページ

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



ISACA®

Tokyo Chapter