ISACA
Trust in, and value from, information systems
Tokyo Chapter

CISM資格の紹介

ISACA東京支部 2013-2014年度

CISM委員会委員長　関　和正

ISACA
Serving IT Governance Professionals
Tokyo Chapter

1.CISM（(公認情報セキュリティマネジャー）について

（1）CISMとは？

情報セキュリティ管理の知識と経験を認定する国際的な専門資格。
Certified Information Security Managerの略です。
全世界で22,500名以上、日本で360名以上がCISMとして認定され、既に活躍しています。

(2)CISMになることの利点

知識と技能の向上

- 自分の知識と技能を向上させることに前向きな姿勢を示すため。

キャリアの向上

- 組織における自身の専門的な関与を経営者に示すため。
- 雇用者が求める資格を取得するため。
- 専門家としてのイメージを向上させるため。

世界的な認知

- 世界的に認知された専門家グループの一員となるため。

（3）CISMの特長

- 情報セキュリティマネジャーの職種を想定して考案された資格。
- 基準と試験問題は、情報セキュリティ管理実務担当者の意向を反映した実務分析をもとに開発。
- 情報セキュリティ管理に関する実務経験を要求。

ISACA
Serving IT Governance Professionals
Tokyo Chapter

（4）CISMに適した人材

会社の情報セキュリティプログラムを設計、実施、そして管理を担当する人材

- セキュリティマネジャー
- セキュリティ担当取締役
- セキュリティ担当役員
- セキュリティコンサルタント

（5）CISMの認知度

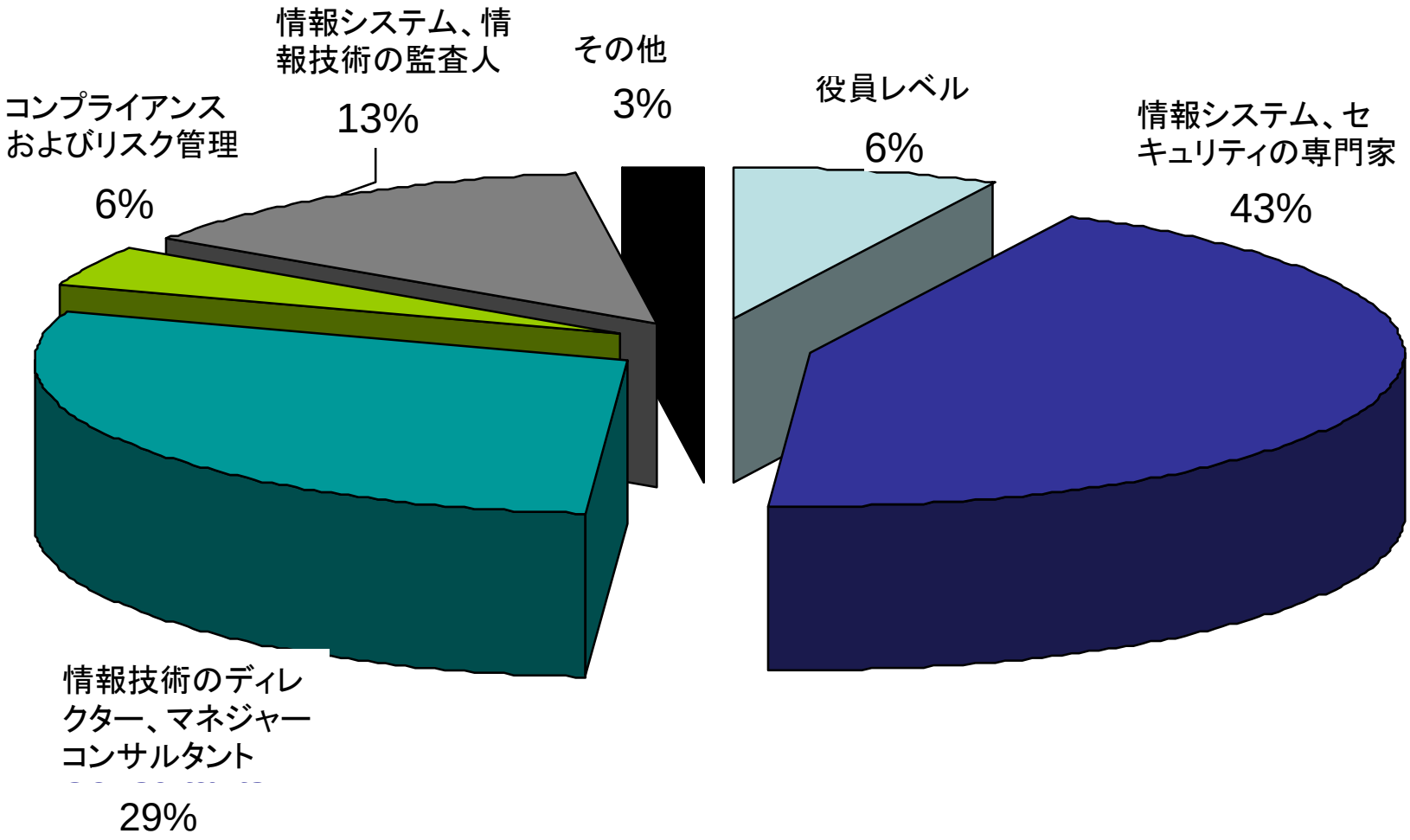
グローバルの情報セキュリティ業界では、CISMの知名度は非常に高くなっています。

- SC Magazineは3年連続でプロフェッショナルアウォード部門の2013年”ベスト・プロフェッショナル認定プログラム”ファイナリストとしてCISMを選びました。CISMは、大手企業や大規模な公共部門の組織における最高情報セキュリティ責任者（CISO）のパネルでファイナリストに選ばれました。
- 複数の専門誌によりますと、CISMは高額収入の資格としてランクされています。
- 米国国防総省（DoD)情報保障担当要員能力向上プログラムにおいてCISMを承認資格(Approved Certificate)として認可しています。
- 国内でも政府機関、自治体の情報セキュリティ支援業務の提案に、CISM資格保有が業務従事者の要件の一つとされるようになりました。

参考：ISACA > Certification > CISM: Certified Information Security Manager
> What is CISM > CISM in the News

ISACA
Serving IT Governance Professionals
Tokyo Chapter

（6）CISM認定者の構成



ISACA
Serving IT Governance Professionals

Brocade Certified SAN Designer – BCSD (also known as Brocade Certified Fabric Designer, or BCFD)	120.77
Brocade Certified SAN Manager – BCSM	107.14
CAP	92.01
CCA	81.76
CCDA (Cisco Certified Design Associate)	95.16
CCDP (Cisco Certified Design Professional	105.96
CCEA	89.09
CCENT (Cisco Certified Entry Network Technician)	67.56
CCIE (Cisco Certified Internetwork Expert) Routing & Switching	120.33
CCNA (Cisco Certified Network Associate)	80.89
CCNP (Cisco Certified Network Professional)	91.87
CCVP (Cisco Certified Voice Professional)	97.83
Certified Ethical Hacker (CEH)	90.93
Certified Information Security Manager (CISM)	109.41
Certified Information Systems Auditor (CISA)	93.43
Check Point Certified Security Administrator (CCSA)	100.38
Check Point Certified Security Expert (CCSE)	102.61
Cisco Firewall Specialist	90.06
Cisco IDS Specialist	83.32
Cisco Information Security Specialist	85.12
Cisco IOS Security Specialist	82.73
Cisco IP Communications Express Specialist	103.56
Cisco IP Telephony Design Specialist	108.36
Cisco IPS Specialist	83.08
Cisco VPN Specialist	87.57
CISSP	98.87
CIW	57.78
GSEC – GIAC Security Essentials Certification	86.26
GSLC – GIAC Security Leadership Certification	89.69
GSNA – GIAC Systems and Network Auditor	94.39
Hitachi Data Systems Certified Professional (Foundations)	101.62
IBM Certified Application Developer / System Administrator – Lotus	77.85
IBM Certified Database Administrator / Application Developer - DB2	78.11
IBM Certified SOA Associate / Solution Designer	88.60
IBM Certified Solution Developer / System Administrator – WebSphere	78.33
IBM Certified Specialist – System x and BladeCenter	79.15
IBM Certified Specialist / Systems Expert - Power Systems (System p)	90.53
IT Architect Certification (ITAC)	109.00
Java Architect	95.16
Java Associate	59.49
Java Business Component Developer	70.82
Java Developer	86.90
Java Programmer	74.72
Java Web Component Developer	69.67
Master ASE (Accredited System Engineer)	96.76
Microsoft Certified Database Administrator (MCDBA)	86.02
Microsoft Certified Desktop Support Technician (MCDST)	63.91
Microsoft Certified IT Professional (MCITP)	76.72
Microsoft Certified Solution Developer (MCSD)	102.45
Microsoft Certified Systems Administrator (MCSA)	78.23
Microsoft Certified Systems Engineer (MCSE)	89.44
Microsoft Certified Technology Specialist (MCTS)	76.95

ISACA
Serving IT Governance Professionals
Tokyo Chapter

ISACA　HPより

The Benefits of CISM

- CISM Impacts Your Career and Your Organization
- The demand for skilled information security management professionals is on the rise, and the CISM certification is the globally accepted standard of achievement in this area.
- CISMs understand the business. They know how to manage and adapt technology to their enterprise and industry.

CISM Certification:

- **Demonstrates your understanding of the relationship between an information security program and broader business goals and objectives**
- **Distinguishes you as having not only information security expertise, but also knowledge and experience in the development and management of an information security program**
- **Puts you in an elite peer network**
- **Is considered essential to ongoing education, career progression and value delivery to enterprises.**

ISACA
Serving IT Governance Professionals
Tokyo Chapter

- **ISACA HP より**
- CISM in the News
  »
- ISACA addresses security skills deficit
- CGEIT and CISM are among highest-paying certs
- Eight Emerging IT Certifications For 2013
- CIO magazine: CISM among IT certs that mean higher pay
- ISACA and SFIA Foundation Partner to Map CISA and CISM Certifications to Skills Framework for the Information Age
- Interview: CISM and CRISC in demand for 2012
- Certified Information Security Manager Exam Updated
- CISM Named a Top Certification for 2012
- ISACA's CISM Designation Named 2012 SC Magazine Awards Finalist for Best Professional Certification Program
- SC Awards Names CISM Finalist for Best Professional Certification Program Award
- Foote Partners Report: ISACA Certifications Earn Top Pay Premiums
- GovInfoSecurity.com shows CISM as one of the top 5 security certifications for 2011
- CSO Magazine Features CISM Certification
- CertMag Salary Survey Names CISM Third Highest-paying IT Cert
- SC Magazine UK Says CISM is Taking Off

ISACA
Serving IT Governance Professionals
Tokyo Chapter

2.CISMになるには？

CISM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CISM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:　受験の前提ではない。合格後実務経験を積むことも可能）

5年のうち3年は情報セキュリティ管理業務に従事していること。またCISMの4つのドメイン（7．参照）のうち、3分野での経験を積んでいるものとする。

業務経験の代替として、CISA認定者は2年分を代替できます。

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

ISACA
Serving IT Governance Professionals
Tokyo Chapter

3.CISM試験とは？

・200問の多岐選択問題（4問択一）、試験時間は4時間。
・試験の内容は、**情報セキュリティガバナンス、情報リスクの管理とコンプライアンス、情報セキュリティプログラムの開発と管理、情報セキュリティのインシデントの管理**からの出題。
・試験日は、6月、12月、(9月)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。

○「2013　説明パンフレット」 ・・・12月実施の試験案内
ISACA > Certification > CISM:・・・> CISM Bulletin of Information (BOI)

○2013年受験者のためのCISM試験と認定ガイド
ISACA > Certification > CISM: ・・・ > Prepare for the Exam

ISACA
Serving IT Governance Professionals
Tokyo Chapter

4. スケジュール、受験手続き(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: 2月下旬(消印有効)
  最終締切り: 4月下旬(消印有効)

- 受験料(カード支払い可)
- 早期締切り(2月下旬) :ISACA会員US＄485、非会員US＄660
  最終締切り(4月下旬) :ISACA会員US＄535、非会員US＄710
  (但し、**オンライン登録の場合、上記金額よりさらに＄75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、exam@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、exam@isaca.org に連絡してください)

- CISM試験受験者向けレビューコースを本試験直前に開催予定です。

(詳細については ISACA 東京支部のWEB サイトで適宜ご確認ください。)
東京支部のWEBページ http://www.isaca.gr.jp

ISACA
Serving IT Governance Professionals
Tokyo Chapter

4. スケジュール、受験手続き（2）

・下記の手続 (変更・キャンセル・繰越）が可能です。

1）受験会場・言語の変更	**変更依頼日により、無料、手数料US＄50必要、あるいは変更できない**
2）受験のキャンセル	**キャンセル依頼日により、キャンセル料US＄100を引いた差額の返却が可能**
3）次回の受験へ繰越	**繰越依頼日により、再登録料US＄50必要、再登録料US＄100必要、あるいは再登録できない 国際本部のwebサイト（www.isaca.org/examdefer）にて受付**

締切日の時刻： 米国イリノイ州シカゴの*5 p.m.*米国セントラル時間

留意事項）
・試験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。

ISACA
Serving IT Governance Professionals
Tokyo Chapter

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）を忘れずに持参してください。**
- **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。**
  試験が開始される約30分前に試験官が説明を開始したら、試験場への入室は不可となります。
  （この場合、受験は認められず、受験料の払い戻しもありません。）

- 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5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、スケールドスコアーで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。（exam@isaca.org　をSPAM　メールの対象から外すように）

7．各章の解説（1）

7．CISM試験 各ドメインの解説（1）

1）情報セキュリティマネジメントに係わる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します。
3）問題はランダムに出題されます。

ドメイン1ー情報セキュリティガバナンス(24%)

情報セキュリティガバナンスのフレームワークと支持プロセスを確立し維持して、確実に情報セキュリティ戦略が組織の目標と目的と調和し、情報リスクが適切に管理され、プログラム・リソースが責任を持って管理されるようにする。

ドメイン2. 情報リスクの管理とコンプライアンス（33%）

情報リスクを許容できるレベルまで管理して、組織の事業要件とコンプライアンス要件を満たす。

7．各章の解説（2）

ドメイン3．情報セキュリティプログラムの開発と管理　（25%）

情報セキュリティ戦略と調和するよう情報セキュリティプログラムを確立し管理する。

ドメイン4．情報セキュリティのインシデントの管理（18%）

情報セキュリティのインシデントの検知、調査、対応、および復旧を行う能力の計画、確立、および管理を行って、ビジネスへの影響を最小限にとどめる。

7．各章の解説（3）

上記の試験案内、試験ドメインの詳細につきましては米国本部のWEBページ

http://www.isaca.org/

ISACA Serving IT Governance Professionals Tokyo Chapter

8.CISM試験のサンプル問題（1）

1. 効果的なIT ガバナンスのために最も重要なのは、次のどれか？

A. ボトムアップアプローチの利用
B. IT 部門による管理
C. 問題の解決を組織の法務部門へ委任
D. トップダウンアプローチの利用

＜解説＞

D 効果的なIT ガバナンスは、明確なポリシ、目標及び目的を規定し、これらを継続的に監視する取締役会と経営管理者による、トップダウンの率先でなければならない。規制の問題や管理のプライオリティに重点を置くことは、ボトムダウンアプローチでは効果的に反映されないことがある。IT ガバナンスは組織全体に影響するもので、IT 管理者だけに関係する問題ではない。法務部門は、全体的なガバナンスプロセスの一部であるが、全責任を負うことはできない。

※出典　CQA10JS　T1-10

ISACA Serving IT Governance Professionals Tokyo Chapter

8.CISM試験のサンプル問題（2）

2. セキュリティコントロールを導入する際に、情報セキュリティマネージャーが最も重視しなければならないのは、次のどれか？

A. 業務への影響を最小限に抑えること
B. あらゆる脆弱性を排除すること
C. 同様の組織での利用
D. サードパーティによる認定

＜解説＞

A セキュリティコントロールは、ビジネスのニーズに合ったものでなければならない。あらゆる脆弱性を排除することは、実現可能ではない。同様の組織で利用されていたとしても、そのコントロールが適切であるとは保証されない。サードパーティによる認定は、重要だが、最も重視すべきことではない。

※出典　CQA10JS　T2-13

ISACA Serving IT Governance Professionals Tokyo Chapter

8.CISM試験のサンプル問題（3）

3. 企業ネットワークへのVPN アクセスに対し、情報セキュリティマネージャーが強固な認証を必要としている。ネットワークへのログオンが安全であることを保証する最強の方法は、次のどれか？

A. バイオメトリクス
B. 対称暗号鍵
C. SSL ベースの認証
D. 二因子認証

＜解説＞

D 二因子認証は、単にユーザ認証の一つのタイプにとどまらない。バイオメトリクスは、ユニークな認証機能を提供するが、PIN(Personal Identifi cation Number) などの別の認証因子を一緒に使用しない限り、それ自体では強固ではない。バイオメトリクス認証も、それ自体はリプレイ攻撃の対象となる。対称暗号方式は、同一の秘密鍵によって、データを暗号及び復号するものだが、エンドユーザのための標準的な認証メカニズムではない。この秘密鍵は、解読される危険もある。SSL は、Web サーバとブラウザの間で暗号化されたリンクを確立するための標準のセキュリティ技術であり、認証メカニズムではない。SSL をクライアント証明書及びパスワードと一緒に使用すれば、二因子認証となる。

※出典　CQA10JS　T3-2

8.CISM試験のサンプル問題（4）

4. システムの脆弱性の連鎖結合から派生する集合リスクを測定し、優先順位付けするための最良の方法は、次のどれか？

A. 脆弱性のスキャン
B. 侵入テスト
C. コードのレビュー
D. セキュリティ監査

＜解説＞

B 侵入テストは、通常、脆弱性を順番に悪用することによって脆弱性を結合できる唯一のセキュリティ評価である。このテストにより、高度なリスクの測定と優先順位付けができる。脆弱性のスキャン、コードのレビュー、セキュリティ監査などのセキュリティ評価は、広範で十分なリスクと脆弱性の概要を把握するのに役立つが、複数の脆弱性が結合した最終的な結果をテストしたり実証したりすることはできない。侵入テストでは、新しい視点からリスクを捉え、一連のセキュリティの問題の最終結果に基づいて優先順位を付けることができる。

※出典　CQA10JS　T4-9

ISACA Serving IT Governance Professionals Tokyo Chapter

8.CISM試験のサンプル問題(5)

5. 失敗する可能性が最も高い復旧戦略は、次のどれか？

A. ホットサイト
B. 冗長サイト
C. 相互援助契約
D. コールドサイト

＜解説＞

C　相互援助契約とは、災害時に2 つの組織が互いにバックアップし合うことを可能にする契約である。このアプローチは、望ましいように見えるが、合意と計画を最新の状態に維持することが難しく、失敗する可能性が非常に大きい。ホットサイトは、ベンダによって処理能力とその他のサービスが十分に装備されているサイトのことなので、正解ではない。冗長サイトは、プライマリサイトとまったく同じように構成され、装備されているサイトのことなので、正解ではない。コールドサイトは、電気配線、空調設備、床などの基盤環境が整い、運用のために機器を受け入れる準備ができている建物のことなので、正解ではない。

※出典　CQA10JS　T5-10

受験準備(日本語の書籍)

教材は全て本部のBookstoreで購入可能※

＜参考書＞

○「2012年公認情報セキュリティマネージャー（CISM）レビューマニュアル」
（ CM12J ）　料金　非会員：US$115.00、　会員：US$85.00

＜参考問題集・・過去問ではありません＞

○「2012年CISM 試験サンプル問題・解答・解説集」（450問）

（ CQA12J ）　料金　非会員：US$90.00、　会員：US$70.00

○「2013年CISM 試験サンプル問題・解答・解説集（追補版）」(100問)
（ CQA13JS ）料金　非会員：US$60.00、　会員：US$40.00

受験準備（CISMレビューコース案内）

○CISMレビューコース募集案内

日本語CISMレビューマニュアル2012を教材に使います。各自購入願います。

・開催日程：4月、10月ごろの2日間（土、日）

・開催場所：日本教育会館
〒101-0003 東京都千代田区一ツ橋2-6-2

・申込締切・参加費用　　2013年11月実施の場合

申し込み区分	費用（2日分）
ISACA会員・早期申し込み	27,000円
ISACA会員・最終締め切り	32.000円
非会員	37,000円

※CISA/CISM/CGEIT/CRISCの認定取得者の継続教育の対象として、出席時間に応じてCPE時間(最大12CPE)を取得することができる。

9. Web画面での受験登録

国際本部のHPを開く
http://www.isaca.org/

次に、国際本部のトップページにて
“Certification”→”CISM” → “Register for the Exam”
Registerをクリックし、以後指示に従ってお進みください。
登録にはISACA IDが必要です。IDをお持ちでない方はオンライン上で作成いただけます。

是非受験し、合格をお祈り致します。