資料3－1

情報セキュリティマネジメント資格運営について

CISM (Certified Information Security Manager)
公認情報セキュリティマネージャを中心として

2006年9月15日

ISACA 東京支部
CISM委員会

制度の沿革・概要

情報システムコントロール協会

(ISACA: Information Systems Audit and Control Association®)

2006年6月30日現在：100カ国に56,000名以上の会員/全世界で１７０以上の支部

日本国内会員数（東京：1,260名、大阪：151名、名古屋：50名）

- EDPAA (EDP Auditors Association) として1969年に協会設立
- 1978年 公認情報システム監査人(CISA) 資格認定を開始
- 1984年 4月 東京支部設立
- 2002年 **公認情報セキュリティマネージャ(CISM)資格制度**を創設

目的：*“情報セキュリティ管理者の職務と責務を立派に果たす知識と経験を有していることを保証すること。“*

- 2003年度よりCISM試験実施

2005年12月現在のCISM認定者は世界中で　5, 231名

（日本国内認定者数：104名 - 2006年7月6日現在）

資格を取得しようとする人材の傾向

企業・団体等の情報セキュリティマネジメントを担当する専門家

- セキュリティマネージャー　Security Managers
- セキュリティ担当役員　Security Directors
- セキュリティ担当役職者　Security Officers
- セキュリティコンサルタント　Security Consultants

受験者層

- 学生や社会人が個人的に受験
- 試験は年2回　-　6月と12月
- 日本語による受験も可能

資格制度の概要

- 情報セキュリティマネージャに特化した資格として設計。
- 資格認定の前提として、情報セキュリティマネジメントとしての経験が必要。
- 情報セキュリティマネージャの業務分析（5ドメイン）に基づく基準と試験問題を開発。

ドメイン1: 情報セキュリティ・ガバナンス

ドメイン2: リスク・マネジメント

ドメイン3: 情報セキュリティ・プログラム・マネジメント

ドメイン4: 情報セキュリティ・マネジメント

ドメイン5: レスポンス・マネジメント（対応管理）

資格取得者の品質維持

CISM認定までの流れ

- ＣＩＳＭ試験に合格する。 （200問の問題に解答。スケールドスコア７５点以上。）
- 情報セキュリティに関する５年以上の経験。
  (うち 3ドメインから 3年以上のセキュリティマネジメントの経験を有すること。)

資格の維持

- 国際本部に管理手数料を納入。
- ISACA職業倫理規則を遵守。
- 継続教育方針(CEP)を順守 (年間最低20時間取得。3年間で120時間以上。)
- 継続教育遵守状況の監査制度あり。監査要件を満たす証拠を提示できない場合資格は剥奪される。

運用にあたっての課題

ボランティア活動ゆえの限界

- 受験講習 - ISACA東京支部主催のレビューコース（受験勉強会）を年2回開催。
- テキストや関連資料の翻訳、受験希望者からの各種質問に応答など。
  → 近年の会員数増加のため、ボランティアベースでの活動は困難。

継続教育の機会提供

- 月例会、関連団体主催月例会、セミナー参加（平日主催のものが多い。）
  → 残業等により、思うように参加できない会員も存在。

月例会、セミナー参加費用

- 月例会、セミナー等は多くの場合有料。（但し、ISACA月例会は会員に限り無料。）
  → 継続教育費を自腹で負担している会員への圧迫。

各種資格との関係について

- **CISMの位置付け**：ビジネスサイドに立脚してセキュリティを管理し、経営者に適切な方針をアドバイスできる人材をターゲットとしている。
- 政府調達（入札時）の参加資格として官と民の類似資格を同条件で列挙していることに対する疑問。
- 情報セキュリティ関連資格が複数存在するため、それぞれの資格の特徴を明確にアピールする必要性。
- 各種セキュリティ資格運営団体間の情報交換の必要性。
- 各団体の創設趣旨の相違より、相互認証には限界が生じる可能性も。

セキュリティ人材の現状・評価

- 企業経営の立場より、リスクとコントロールを的確に判断できる人材が不足。
- セキュリティの流行用語に流されたり、リスク・マネジメントに疎い専門家が存在。
- セキュリティ対策についてあまり吟味せず無批判に導入する担当者が存在。
- 教育者側にも情報セキュリティに精通している人材が少ない。
- 海外の管理基準も頻繁に更新されるため、専門的能力や教材などをいかにして最新の状態に保っていけるかが問題。

制度に対する改善要望

- 情報システム技術者が豊かなセキュリティ知識を獲得できる仕組みが望まれる。
- 国家資格認定者にも継続教育要件を付加すべき。
- 類似した専門資格が複数存在する。競争で残るものと衰退するものが出てくるか。
  （サービス利用者側に混乱を生じさせない配慮が必要。）
- 政府入札時の参加者資格として資格制度を利用する場合の配慮。
  （各資格の創設趣旨の相違、認定される能力、継続教育義務の有無などを
  すべて考慮した上での公平な専門能力評価が可能か。）

以上。