情報セキュリティマネジメント試験合格講座 08

- 情報セキュリティの組織

1. NISC（内閣サイバーセキュリティセンター）
   （National center of Incident readiness and Strategy for Cybersecurity）
   内閣官房に設置され、我が国をサイバー攻撃から防衛するための司令塔機能を担う組織。

2. CRYPTREC（Cryptography Research and Evaluation Committees）
   電子政府推奨暗号の安全性評価、暗号技術の適切な運用、関連する情報の提供などを目的とするプロジェクト。総務省および経済産業省が共同で運営する暗号技術検討会などで構成されている。

   - ✓ Cryptography：クリプトグラフィ、暗号手法（内容を隠す技術）
   - ✓ Steganography：ステガノグラフィ、隠蔽手法（情報の存在を隠す技術）

3. JISC（Japanese Industrial Standards Committee、日本工業標準調査会）
   工業標準化法に基づいて、工業標準化全般に関する調査・審議を行っている審議会。経済産業省に設置されている。

4. IPA（Information technology Promotion Agency、情報処理推進機構）
   セキュリティに関係する調査・情報提供、「情報処理の促進に関する法律」に基づいて情報処理技術者試験を実施している独立行政法人。

5. JIPDEC（日本情報経済社会推進協会、旧：財団法人日本情報処理開発協会）
   情報セキュリティマネジメントシステム適合性評価制度、サイバーセキュリティマネジメントシステム適合性評価制度、プライバシーマーク制度、電子署名認証制度の運営などを行っている一般社団法人。

6. JPCERT／CC（Japan Computer Emergency Response Team Coordination Center）
   情報セキュリティに関連する事象の情報の収集、インシデント対応の支援、情報セキュリティ関連情報の発信などの活動をしている一般社団法人。

- 情報セキュリティの規格・制度

7. ISMS（Information Security Management System）
   ISO/IEC 27001（JIS Q 27001）シリーズの基となった規格。情報セキュリティを保つために、組織の情報資産の機密性、可用性、完全性を維持管理するためのシステムまたは管理方法。

8. ISO/IEC 27000 シリーズ
   国際標準化機構（ISO、International Organization for Standardization）と国際電気標準会議（IEC、International Electro technical Commission）が共同で策定する情報セキュリティ規格群。主な制定済みの規格は以下の通り。

   - ✓ ISO/IEC 27000:2009 ISMS 規格についての概要と基本用語集
   - ✓ ISO/IEC 27001:2005 組織の ISMS を認証するための要求事項
   - ✓ ISO/IEC 27002:2005 ISMS 実践のための規範
   - ✓ ISO/IEC 27003:2010 ISMS 実装ガイド
   - ✓ ISO/IEC 27004:2009 情報セキュリティの測定
   - ✓ ISO/IEC 27005:2008 情報セキュリティのリスクマネジメント
   - ✓ ISO/IEC 27006:2007 認証登録プロセスの要求仕様
   - ✓ ISO/IEC 27007:2011 ISMS 監査の指針（主にマネジメントシステム）
   - ✓ ISO/IEC 27014:2013 情報セキュリティガバナンスの枠組み
   - ✓ ISO/IEC 27032:2012 サイバーセキュリティの手引き

9. ISO/IEC 27001:2013（JIS Q 27001:2014）
   ISO のマネジメントシステム規格（MSS、Management System Standard）の共通要素を適用して開発された情報セキュリティマネジメントシステムの規格。情報セキュリティに不可欠な ISMS 固有の要求事項が規定されている。

   - ✓ ISO/IEC 27001:2013（JIS Q 27001:2014）の概要
     情報セキュリティマネジメントシステムの適用範囲、引用規格、用語の定義、組織の状況、リーダーシップ、計画、支援、運用、パフォーマンス評価、改善などに関する要求事項が規定されている。

10. ISO/IEC 27002:2013(JIS Q 27002:2014)
情報技術・セキュリティ技術・情報セキュリティ管理策の実践のための規範。
ISO/IEC 27001:2013 に基づく、情報セキュリティマネジメントシステムを実施するプロセスにおいて、情報セキュリティ管理策の選定、実施の手引、情報セキュリティマネジメントの指針を作成の指針・参考として用いられることを意図している。

✓ ISO/IEC 27002:2013(JIS Q 27002:2014)の概要
情報セキュリティマネジメントの実践のための規範として、主に以下の項目が提供されている。

- リスクアセスメントおよびリスク対応／セキュリティ基本方針(管理方針)
- 情報セキュリティのための組織(情報セキュリティのガバナンス)
- 情報資産の管理／人的資源のセキュリティ
- 物理的および環境的セキュリティ(コンピュータ機器の保護)
- 通信・運用管理／アクセス制御(機能やデータへのアクセス権制限)
- 情報システムの取得／開発および保守
- 情報セキュリティインシデントの管理／事業継続管理
- 順守(情報セキュリティポリシ／規格／法律／規定の順守の徹底)

11. ISMS 適合性評価制度
ISO/IEC 27001:2013(JIS Q 27001:2014)に基づく、組織が構築した情報セキュリティマネジメントシステムの適合性を JIPDEC が評価・認定する制度。

12. CSMS 適合性評価制度
産業用オートメーションおよび制御システムを対象としたサイバーセキュリティマネジメントシステムの適合性を JIPDEC が評価・認定する制度。

13. プライバシーマーク制度
JIS Q 15001 に基づき、個人情報について適切な保護措置を講じる体制を整備している事業者などを JIPDEC が評価・認定する制度。

14. CC (Common Criteria)／ISO/IEC 15408
情報技術に関連した製品およびシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格。1999 年に ISO 標準 (ISO/IEC 15408) 、2000 年に JIS 標準 (JIS X 5070) として制定されている。

15. TCSEC（Trusted Computer System Evaluation Criteria）
米国国防総省下にある NSA(国家安全保障局)の NCSC(米国コンピュータセキュリティセンタ)によるシステムのセキュリティを測定するための標準的な指標。表紙の色から「オレンジブック」とも呼ばれている。

16. JISEC（IT セキュリティ評価および認証制度）
（Japan Information Technology Security Evaluation and Certification Scheme）
ISO/IEC 15408 に基づいて、IT 関連製品のセキュリティ機能の適切性、確実性を評価する政府調達のためのセキュリティ要件の確認制度。

17. CVSS（Common Vulnerability Scoring System）
共通脆弱性評価システム。情報セキュリティの非営利団体 FIRST（Forum of Incident Response and Security Teams）が推進する情報システムに内在する脆弱性に対する汎用的な評価手法。脆弱性の深刻度を同一の基準で定量的に比較できる。

18. JCMVP（暗号モジュール試験および認証制度）
（Japan Cryptographic Module Validation Program）
電子政府推奨暗号リストなどに記載されている暗号化機能、署名機能など承認されたセキュリティ機能を実装したハードウェアやソフトウェア等から構成される暗号モジュールが、格納するセキュリティ機能並びに暗号鍵およびパスワード等の重要情報を適切に保護していることを IPA が認証する制度。

19. PCI DSS（Payment Card Industry Data Security Standard）
クレジットカード情報保護のためのセキュリティ対策フレームワーク。クレジットカード会員データを安全に取り扱う事を目的として策定された、クレジットカード業界のセキュリティ基準。

〔問題集〕

- ✓ 石川敢也(共著)「情報セキュリティマネジメント要点整理＆予想問題集」 翔泳社
- ✓ 情報セキュリティマネジメント試験合格講座 http://rakupass.com/security/