平成 28 年度春期
情報セキュリティマネジメント試験　分析資料

株式会社ウイネット

平成 28 年度春期情報セキュリティマネジメント試験が初めて 4 月 17 日（日）に実施されました。

この度弊社では、弊社教材外部ライティングスタッフの皆様から、本試験出題内容に関するご意見を聴取させていただき、整理及び分析を行いました。今後のご参考として、今回の本試験分析をご報告させていただきます。なお、基本情報技術者試験は平成 28 年度春期、IT パスポート試験は 4 月 17 日公開（春期分）を比較対象としています。

＜午前問題＞

1．問題解答時間の比較

	情報セキュリティマネジメント試験	基本情報技術者試験	IT パスポート試験
レベル	レベル 2	レベル 2	レベル 1
問題数	50 問	80 問	100 問
試験時間	90 分	150 分	120 分
1 問当たりの平均解答時間	1.8 分	1.875 分	1.2 分

1 問当たりの平均解答時間は、基本情報技術者試験とほぼ同じ（やや短め）であり、IT パスポート試験の 1.5 倍です。

2．分野別出題構成比率

	情報セキュリティマネジメント試験	基本情報技術者試験	IT パスポート試験
テクノロジ系	68.0%（34 問）	62.5%（50 問）	45.0%（45 問）
マネジメント系	12.0%（ 6 問）	13.8%（11 問）	21.0%（21 問）
ストラテジ系	20.0%（10 問）	23.8%（19 問）	34.0%（34 問）

基本情報技術者試験や IT パスポート試験と比較して、“テクノロジ系”の構成比率が高く、“マネジメント系”と“ストラテジ系”の構成比率が低くなっています。

3．中分類別出題構成比率

	中分類	情報セキュリティマネジメント試験	基本情報技術者試験	IT パスポート試験
1	セキュリティ	60.0%（30 問）	12.5%（10 問）	18.0%（18 問）
2	法務	12.0%（ 6 問）	2.5%（ 2 問）	8.0%（ 8 問）
3	システム構成要素	2.0%（ 1 問）	3.8%（ 3 問）	2.0%（ 2 問）
4	データベース	2.0%（ 1 問）	6.3%（ 5 問）	4.0%（ 4 問）
5	ネットワーク	4.0%（ 2 問）	6.3%（ 5 問）	8.0%（ 8 問）
6	プロジェクトマネジメント	2.0%（ 1 問）	5.0%（ 4 問）	8.0%（ 8 問）
7	サービスマネジメント	4.0%（ 2 問）	5.0%（ 4 問）	4.0%（ 4 問）
8	システム監査	6.0%（ 3 問）	3.8%（ 3 問）	4.0%（ 4 問）
9	システム戦略	2.0%（ 1 問）	5.0%（ 4 問）	5.0%（ 5 問）
10	システム企画	2.0%（ 1 問）	1.3%（ 1 問）	2.0%（ 2 問）
11	企業活動	4.0%（ 2 問）	5.0%（ 4 問）	10.0%（10 問）
その他			43.8%（35 問）	27.0%（27 問）

“セキュリティ”だけで 60.0%を占めています。“セキュリティ”と“法務”の合計で、構成比率は 72.0%になります。なお、計算問題の出題は 1 問もありませんでした。

4．基本情報技術者試験で出題されている問題

“基本情報技術者試験で出題されている問題”と同一（非常に類似含む）の問題が次のように出題されています。

問番号	テーマ	基本情報技術者試験での出題
問 11	BYOD と情報セキュリティリスク	平成 28 年度春期・問 42
問 13	WAF	平成 28 年度春期・問 43
問 14	マルウェア対策	平成 25 年度秋期・問 42
問 16	ディジタルフォレンジックス	平成 28 年度春期・問 44
問 17	磁気ディスクの廃棄時の情報漏えい対策	平成 28 年度春期・問 45
問 24	認証局（CA）の役割	平成 28 年度春期・問 39
問 32	個人情報保護法	平成 25 年度秋期・問 80
問 35	不正競争防止法	平成 25 年度春期・問 78
問 43	レスポンスタイム	平成 11 年度秋期・問 52（第二種）
問 44	データウェアハウス	平成 22 年度春期・問 33
問 45	ルータの機能	平成 16 年度秋期・問 66
問 46	プロキシサーバ	平成 19 年度秋期・問 37
問 47	SaaS	平成 25 年度秋期・問 64
問 48	情報システムの調達手順（RFP）	平成 24 年度春期・問 66
問 50	コーポレートガバナンス	平成 28 年度春期・問 75

5．今後の指導方法

まずは、シラバスに記載されている用語例をマスタすることが最も重要です。また、基本情報技術者試験の過去問題から多く出題されることから、分野を絞って基本情報技術者試験の過去問題を直前対策で演習することも効果的でしょう。

＜午後問題＞

1．出題概要

現代の世相を反映する形で初めて実施されることになった情報セキュリティマネジメント試験（以下、SG 試験という）の午後問題に関しては、IPA より事前に発表されていた SG 試験のサンプル問題で提示されていたとおり、午前問題で問われる知識問題を具体的な事例に置き換えて、情報セキュリティインシデントの対応及び対策、アクセス制御、外部委託先の情報セキュリティ管理などを問う内容で出題されました。一見すると 1 題あたりの設問数が多いため、問題のボリュームが大きいと感じられますが、全体的な難易度は初回ということもあり、やや易しいと思われます。また、IPA から発表されていた午後の出題範囲及びシラバス（レベル 2）に沿って、〔要求される技能〕の情報セキュリティマネジメントの運用・継続的改善に関連した内容で出題されました。

問 1「標的型攻撃メールの脅威と対策」では、標的型攻撃メールの特徴、インシデント事例に基づく初動対応の問題点、管理規定及び運用の改善点、問 2「業務委託におけるアクセス制御」では、業務上の役割分担や規則に応じた適切な権限設定の検討、情報セキュリティ上のシステムの承認管理・運用、問 3「情報セキュリティ自己点検」では、監査部門の依頼に基づく CSA（統制自己評価）方式に基づく自己評価、及びその改善点について問われました。

すべての問題が情報セキュリティマネジメント運用・継続的改善に基づく具体的事例を中心に構成されていたこともあり、与えられた条件を基に限られた時間内で設問文を読み解くことができれば、理解しやすく、解きやすい内容であったと思われます。なお、計算問題はいっさい出題されていませんでした。

2．出題テーマ及び難易度 【難易度　5：高い、4：やや高い、3：並み（普通）、2：やや易しい、1：易しい】

	出題テーマ・要求される技能	難易度	出題形式・出題数	配分時間 ・配点割合
問 1	標的型攻撃メールの脅威と対策 ・マルウェアからの保護 ・情報セキュリティの意識向上 ・情報セキュリティインシデントの管理 ・情報セキュリティの教育／訓練	2	設 1(1)、(2)　空欄選択 3 設 1(3)、(4)　選択 2　（複数選択） 設 2(1)　選択 1 設 2(2)、(3)　空欄選択 2 設 2(4)、(5)　空欄選択 2	20 分程度 34 点
問 2	業務委託におけるアクセス制御 ・外部委託先における情報セキュリティの確保 ・利用者アクセスの管理 ・コンプライアンスの運用	3	設 1(1)、(2)　選択 2 設 1(3)　空欄選択 2 設 1(4) ～ (6)　選択 3 設 2(1)、(2)　空欄選択 4 設 2(3)、(4)　選択 2	30 分程度 34 点
問 3	情報セキュリティ自己点検 ・情報セキュリティの教育／訓練 ・情報セキュリティマネジメントの継続的改善 ・情報セキュリティ監査項目と改善計画	3	設 1　選択 1 設 2　選択 1（複数選択） 設 3(1) ～ (5)　選択 5 設 4(1)、(2)　選択 2（組合せ選択）	40 分程度 34 点

注記 1　得点の上限は 3 問合わせて 100 点として、合計 60 点以上を午後問題の合格点とする。

注記 2　配分時間は、受験者あるいは指導者が受験対策で想定している 1 問当たりの解法時間を示す。

3．出題傾向及び問題別分析

□ 問 1【必須問題】標的型攻撃メールの脅威と対策

ここ数年で、標的型攻撃メールによって企業などの組織の内部情報を搾取するインシデントが頻発しています。それによって、最初に標的とされた企業などの組織に限定されず、取引先や関連会社を狙うケースも増えてきており、情報システムの利用部門も含め誰もが狙われる可能性を秘めています。

問 1 では、標的型攻撃メールの対策検討、情報セキュリティインシデント対応、社員一人一人の意識向上の重要性を考慮した情報セキュリティ教育の実施を主要なテーマとしています。

具体的な出題内容は、標的型攻撃メールの受信が原因によるマルウェア感染というインシデント事例を用いて、各攻撃手法の特徴、初動対応の問題点、管理規定及び運用の改善点などを考察します。

問題単体としてのボリュームもそれほど大きくなく、各設問で問われている内容も平易であったため、配分時間内で高い正答率を得られたと予想します。

□ 問 2【必須問題】業務委託におけるアクセス制御

情報システムを活用して業務を行う職場において、その職場の社員に対する適切な権限設定の維持管理は、情報セキュリティ上、欠かすことができない管理業務です。したがって、情報システムの利用部門は、人事異動や組織変更の際に不要な権限設定の放置などのセキュリティ違反が起こらないよう、業務で利用する情報システムの特性を理解した上で、適切に権限設定の維持管理に努めることが重要です。

問 2 では、業務上の役割分担や規則に応じた適切な権限設定の検討、承認者の不在や要員の追加・交代といった日常的に起こり得る作業代行において情報セキュリティ上のリスクを考慮した対応を主要なテーマとしています。

具体的な出題内容は、販売業務システムを題材に、各ロール（役割）に設定する適切なアクセス操作権限、ユーザ ID も含めた管理・運用の方法などを考察します。

各設問の解答に際して予備知識はそれほど必要としないのですが、代わりに登場人物や使用するシステム、考慮すべき方針や要求事項が多数提示されているため、配分時間内で効率良く整理し読解することが求められます。

□ 問 3【必須問題】情報セキュリティ自己点検

情報セキュリティを維持するために、その評価は欠かすことができません。情報セキュリティの評価体系に CSA（統制自己評価）などの自己評価を適切に取り入れて、組織の情報セキュリティを効率的に維持することが重要です。

問 3 では、情報システムの利用部門が、簡易チェックリストを用いて自主的にチェックする仕組みを検討する際に、どのような評価項目が適しているかの検討、監査部門の依頼を基に CSA 方式によって自己評価を行う際に、情報セキュリティの実施状況の適切な評価、その結果に基づいて改善計画を策定することを主要なテーマとしています。

具体的な出題内容は、顧客情報の扱いを題材に、各種リスクの洗出し、自己評価に基づく問題点や改善点を考察します。CSA というやや難解な概念が掲載されており、その特徴を問う設問も出題されました。ただし、十分に理解できていなくとも、セキュリティ監査についての基礎的な知識があれば、一般常識と考え合わせて各設問に解答することは十分に可能です。

自己評価に基づく改善計画についての設問では、与えられた条件に基づいて適切に評価するだけでなく、その根拠との整合性も考察させるなどの出題があり、配分時間内で効率良く整理し読解することが求められます。

4．午後問題の講評

全体として、数値分析に基づく計算問題が 1 題もなく、RSA や AES の暗号化や復号の手順といった技術的な知識や技術を要する出題が少なかったと分析します。また、情報セキュリティの基本的な概念をベースに与えられた条件に基づき、問題文を効率良く整理し読解する能力が重視されています。今回の出題テーマでは、“インシデント対応”、“アクセス制御”、“リスク分析・対応”といったように、十分予想された標準的な出題内容でした。

全体的な難易度としては、基本情報技術者試験の午後問題対策を行っている受験者であれば、さほど難解ではない平易な問題であり、時間配分さえしっかり管理できれば午後試験の合格点に到達できたのではないかと予想します。ただし、マネジメント系やストラテジ系の読解力を要する長文問題が苦手な受験者にとっては、多少なりとも手強く感じられた可能性があります。

初回ということで、今回の難易度及び問題のボリュームバランスが次回も継続するとは限りませんが、引き続き注視するとともに、この SG 試験の継続的な実施にあたり受験者数の増加に期待したいと考えております。