平成 28 年度秋期
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 年度秋期情報セキュリティマネジメント試験が 10 月 16 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、比較対象の IT パスポート試験は、10 月 16 日公開の問題を平成 28 年度秋期（H28 秋）として載せております。

＜午前問題＞

１．分野別出題構成比率

分野	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（H28 秋）	IT パスポート試験（H28 秋）
	H28 秋	H28 春		
テクノロジ系	66.0%（33 問）	68.0%（34 問）	62.5%（50 問）	46.0%（46 問）
マネジメント系	16.0%（ 8 問）	12.0%（ 6 問）	12.5%（10 問）	20.0%（20 問）
ストラテジ系	18.0%（ 9 問）	20.0%（10 問）	25.0%（20 問）	34.0%（34 問）

前回と比較して、“マネジメント系”が 2 問増え、“テクノロジ系”と“ストラテジ系”がそれぞれ 1 問減りました。

２．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（H28 秋）	IT パスポート試験（H28 秋）
		H28 秋	H28 春		
1	セキュリティ	60.0%（30 問）	60.0%（30 問）	12.5%（10 問）	18.0%（18 問）
2	法務	12.0%（ 6 問）	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）	2.0%（ 1 問）	3.8%（ 3 問）	2.0%（ 2 問）
4	データベース	2.0%（ 1 問）	2.0%（ 1 問）	6.3%（ 5 問）	4.0%（ 4 問）
5	ネットワーク	2.0%（ 1 問）	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）	2.0%（ 1 問）	5.0%（ 4 問）	8.0%（ 8 問）
7	サービスマネジメント	6.0%（ 3 問）	4.0%（ 2 問）	3.8%（ 3 問）	4.0%（ 4 問）
8	システム監査	8.0%（ 4 問）	6.0%（ 3 問）	3.8%（ 3 問）	4.0%（ 4 問）
9	システム戦略	2.0%（ 1 問）	2.0%（ 1 問）	5.0%（ 4 問）	5.0%（ 5 問）
10	システム企画	2.0%（ 1 問）	2.0%（ 1 問）	2.5%（ 2 問）	2.0%（ 2 問）
11	企業活動	2.0%（ 1 問）	4.0%（ 2 問）	5.0%（ 4 問）	9.0%（ 9 問）
その他				43.8%（35 問）	28.0%（28 問）

(1)　前回と比較して、“サービスマネジメント”と“システム監査”がそれぞれ 1 問増えました。

(2)　前回と比較して、“ネットワーク”と“企業活動が”がそれぞれ 1 問減り、“セキュリティ”、“法務”、“サービスマネジメント”、“システム監査”以外は、各 1 問のみの出題になりました。

(3)　前回と同様に、計算問題の出題は 1 問もありませんでした。

３．平成 28 年秋期基本情報技術者試験（試験開始時間が同じ）と同一の問題の出題

中分類	問番号	テーマ	基本情報技術者試験での問番号
セキュリティ	問 1	IC カードと PIN での利用者認証	問 40
	問 14	rootkit	問 41
	問 18	ウイルス検出におけるビヘイビア法	問 43
	問 20	CAPTCHA	問 36
	問 21	情報の“完全性”を脅かす攻撃	問 37
データベース	問 46	E-R 図	問 26
企業活動	問 50	マトリックス組織	問 76

(1)　基本情報技術者試験の“セキュリティ”10 問のうち、半数の 5 問が情報セキュリティマネジメント試験にも出題されました。この 10 問中 5 問の比率は、前回も同様でした。

(2)　基本情報技術者試験と同一の問題の出題 7 問は、前回の 6 問よりも 1 問増えています。

(3)　“企業活動（問 50）”は、前回も基本情報技術者試験と同一の問題の出題でした。

４．基本情報技術者試験や応用情報技術者試験の過去問題と同一（非常に類似含む）の問題の出題

中分類	問番号	テーマ	基本情報技術者試験	応用情報技術者試験
セキュリティ	問 1	IC カードと PIN での利用者認証	H26 春問 38	
	問 3	JPCERT/CC		H27 春問 40
	問 9	残留リスク		H27 春問 41
	問 13	MDM	H26 春問 40	
	問 21	情報の“完全性”を脅かす攻撃	H26 春問 39	
	問 22	クロスサイトスクリプティング		H25 秋問 42
	問 25	ソーシャルエンジニアリング	H26 春問 41	
	問 26	パスワードリスト攻撃		H27 春問 39
	問 29	PKI での認証局の果たす役割	H26 春問 37	
法務	問 36	準委任契約	H26 秋問 80	
システム監査	問 39	事業継続計画についての監査		H27 春問 60
サービスマネジメント	問 41	システムの移行テスト	H19 秋問 51	
プロジェクトマネジメント	問 44	ステークホルダ	H27 春問 52	
データベース	問 46	E-R 図	H24 春問 28	
システム戦略	問 48	BPO		H24 秋問 62
システム企画	問 49	企画プロセス	H27 春問 66	

注記：問番号の問 1、問 21、問 46 は、“３．平成 28 年秋期基本情報…”の表中と重複します。

５．今後の指導方法

(1)　シラバスに記載されている用語例を完全にマスタすることが最も重要です。

(2)　基本情報技術者試験や応用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、これらの試験の過去問題を直前対策で徹底的に演習することが効果的でしょう。

(3)　JIS Q 27000:2014、JIS Q 27002:2014、JIS Q 31000:2010、ITIL 2011 edition、共通フレーム 2013 などの規格・標準に触れ、内容を理解しておくことが必要です。

＜午後問題＞

1．出題概要

現代の世相を反映する形で実施されることになりました、情報セキュリティマネジメント試験（以下、SG 試験という）の午後問題については、初回の出題内容と比べて、問 1 の出題ページ数が 2 ページ多くなっています。それだけ文章量が増え、読み解く時間が増したと考えます。ただし、3 問ともほぼ同等のページ数で、ある程度難易度も揃っていたようです。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初動対応、原因や影響、アクセス制御、再発防止策、被害の拡大防止策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ことから問題のボリュームが大きいと感じますが、全体の難易度としては、初回と同等もしくは若干高めでした。また、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を中心に出題されました。

問 1「オンラインストレージサービスの利用における情報セキュリティ対策」では、外部のストレージサービスの利用事例を基に、ファイルの共有設定に関する問題点を整理し、さらに、その対策を技術面と組織運用面の双方から考察します。問 2「情報機器の紛失」では、ノート PC の持出しに関する情報セキュリティインシデントを取り上げ、適切な初動対応の手順、実施すべき調査の内容、及び再発防止策について考察します。問 3「業務用 PC での Web サイト閲覧」では、Web サイトの改ざんに関する事例を基に、適切な調査手順及び改善点について考察します。

3 問ともに、運用上の不具合や外部からの攻撃を契機とした情報セキュリティインシデントに対し、初動対応からの問題の究明、必要な対策の考察までの流れを取り上げています。選択肢の組合せ解答群に基づく設問では、選択肢を絞り切れないやや難解な出題もありましたが、全体に影響を与えるほどではないようです。前回と比較しますと、すべての問題が情報セキュリティマネジメントの運用・継続的改善に基づく具体的な事例を中心に構成されていることもあり、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、計算問題は今回も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	オンラインストレージサービスの利用における情報セキュリティ対策（11 ページ） ・部門の情報システム利用時の情報セキュリティの確保 ・情報セキュリティインシデントの管理	3	設 1(1)　空欄選択 2・組合せ 設 1(2)　選択 1 設 2　選択・組合せ 設 3(1)　空欄選択 1 設 3(2)　選択・組合せ 設 4(1)、(2)　空欄選択 2×2 設 4(3)、(4)　選択 1、選択・組合せ	30 分程度 34 点
問 2	情報機器の紛失（10 ページ） ・情報資産の管理 ・部門の情報システム利用時の情報セキュリティの確保 ・情報セキュリティインシデントの管理	3	設 1　空欄選択 4 設 2(1)　選択・組合せ 設 2(2)　選択 1 設 2(3)　空欄選択 2・組合せ 設 2(4)　選択 1 設 2(5)　空欄選択 2・組合せ	30 分程度 34 点
問 3	業務用 PC での Web サイト閲覧(10 ページ) ・情報セキュリティリスクアセスメント及びリスク対応 ・部門の情報システム利用時の情報セキュリティの確保 ・情報セキュリティインシデントの管理	3	設 1(1)　選択・組合せ 設 1(2)　空欄選択 3・組合せ 設 1(3)　選択・組合せ 設 2(1)　空欄選択 4 設 2(2)　選択 1 設 3(1)　空欄選択 1 設 3(2)　選択 1 設 3(3)　空欄選択 1	30 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】オンラインストレージサービスの利用における情報セキュリティ対策

社内で構築・運用していた情報システムに代わり、インターネット上のストレージサービスを利用することが増加しています。安価で利便性の高いストレージサービスの情報セキュリティインシデントへの対応が重要です。

問 1 では、オンラインストレージ上のファイルの共有設定の誤りによる情報セキュリティインシデントを題材に、情報セキュリティリーダに必要な情報セキュリティの原因や影響を考察し、再発防止策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、オンラインストレージサービスの利用時における情報セキュリティインシデントの事例を基に、事故発生の原因追究、初期対応に対する評価、プロキシサーバの調査目的、ファイルの共有設定の個別ヒアリングの内容などを考察します。

問題単体のボリュームとしては前回よりも 2 ページほど増えたものの、各設問で問われている内容も比較的平易であったため、配分時間内で正答が得られたと予想します。

□ 問 2【必須問題】情報機器の紛失

企業活動において日常的に使用している情報機器の紛失・盗難は、会社組織が社外秘として管理している機密情報が社外に流出する危険につながります。また、情報機器を社外へ持ち出すことを前提とした営業活動は多くの会社組織で行われ、社外での情報機器の紛失・盗難への備えは情報セキュリティ管理上の重要な課題です。

問 2 では、従業員が外出中に携帯型の情報機器を紛失した情報セキュリティインシデントを題材に、各部門の情報セキュリティリーダが情報システム部門と協力し、情報セキュリティ被害の拡大防止のための初動対応などを主要なテーマとしています。

具体的な出題内容は、情報セキュリティインシデントの発生に伴い、迅速な報告書案の作成、その影響及び対応などを考察します。

問題単体のボリュームとしては前回と同等であり、各設問で問われている内容も比較的平易であったため、配分時間内で効率良く整理し読解することで、正答が得られたと予想します。

□ 問 3【必須問題】業務用 PC での Web サイト閲覧

自社の公開 Web サイトが改ざんされ、暗黙的にウイルス配布サイトにされてしまうことで、その Web サイトの閲覧者の情報機器がドライブバイダウンロードによってウイルスに感染させられてしまうケースが増加しています。情報システムの利用者の誰もが、ウイルス感染被害を受ける可能性があると考えられます。

問 3 では、情報システムの利用部門の情報セキュリティリーダによる情報セキュリティインシデントの対応、及び社内の関係者との協力体制に基づく感染原因の解明、及び再発防止策の検討を主要なテーマとしています。

具体的な出題内容は、情報セキュリティインシデントの発見と初動対応、調査結果の中間報告、課題の改善などを考察します。実際に不正プログラムによる被害を体験しなくとも、ウイルス対策ソフトの対策パッチの対応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。

情報セキュリティインシデントの発見と初動対応、調査結果の中間報告、課題の改善についての設問では、与えられた条件に基づいて適切に解答するだけでなく、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で、正答が得られたと予想します。

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知識・技術を要する出題が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、情報セキュリティインシデントの初動対応、原因や影響、アクセス制御、再発防止策、被害の拡大防止策などといったように、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、多少なりとも難しく感じられた可能性があります。

次回の難易度及び問題のボリュームバランスが、3 回目に継続され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。