平成 30 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 30 年度春期情報セキュリティマネジメント試験が 4 月 15 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。

＜午前問題＞

1．分野別出題数

	分野	H30 春	H29 秋	H29 春	H28 秋	H28 春
1	テクノロジ系	34	33	33	33	34
2	マネジメント系	7	8	8	8	6
3	ストラテジ系	9	9	9	9	10
	合計	50	50	50	50	50

(1)　前回と比較して、出題数が増えた分野は、“テクノロジ系（+1 問）”でした。

(2)　前回と比較して、出題数が減った分野は、“マネジメント系（−1 問）”でした。

2．中分類別出題数

	中分類	H30 春	H29 秋	H29 春	H28 秋	H28 春
1	セキュリティ	30	30	30	30	30
2	法務	6	6	5	6	6
3	システム構成要素	2	1	1	1	1
4	データベース	1	1	1	1	1
5	ネットワーク	1	1	1	1	2
6	プロジェクトマネジメント	1	1	1	1	1
7	サービスマネジメント	1	3	3	3	2
8	システム監査	5	4	4	4	3
9	システム戦略	1	1	2	1	1
10	システム企画	1	1	1	1	1
11	企業活動	1	1	1	1	2
	合計	50	50	50	50	50

(1)　前回と比較して、出題数が増えた中分類は、“システム構成要素（+1 問）”、“システム監査（+1 問）”でした。

(2)　前回と比較して、出題数が減った中分類は、“サービスマネジメント（−2 問）”でした。

(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 30 年度春期基本情報技術者試験（試験開始時刻が同じ）と同一の問題の出題

中分類	問	テーマ	基本情報技術者試験
セキュリティ	問 8	JIS Q 27000:2014　真正性	問 39
	問 10	SPF	問 40
	問 14	セキュリティバイデザイン	問 42
	問 18	パケットフィルタリング	問 44
	問 21	ドライブバイダウンロード攻撃	問 36
サービスマネジメント	問 42	ローカルサービスデスク	問 56
プロジェクトマネジメント	問 43	アローダイアグラム	問 51
ネットワーク	問 47	電子メールのヘッダフィールド	問 34

(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、過去 4 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は 8 問でした。なお、平成 29 年度秋期は 8 問、平成 29 年度春期は 8 問、平成 28 年度秋期は 7 問、平成 28 年度春期は 6 問でした。

4．情報セキュリティマネジメント試験（SG）、又は、基本情報技術者試験（FE）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	テーマ	SG 又は FE
セキュリティ	問 12	WAF	H28 秋問 42（FE）
	問 16	ワームの検知方式	H27 秋問 43（FE）
	問 19	サイバーセキュリティ戦略	H28 秋問 23（SG）
	問 22	バイオメトリクス認証システム	H20 春問 64（FE）
	問 27	ブルートフォース攻撃	H27 秋問 37（FE）
	問 28	S/MIME	H25 春問 43（FE）
	問 29	ディジタル署名	H26 秋問 37（FE）
	問 30	PKI における認証局	H26 春問 37（FE）
法務	問 31	サイバーセキュリティ基本法	H27 秋問 79（FE）
システム監査	問 38	ISMS の運用での内部監査	H28 秋問 37（SG）
	問 39	監査証拠	H24 春問 60（FE）
	問 41	事業継続計画の監査	H28 秋問 39（SG）
サービスマネジメント	問 42	ローカルサービスデスク	H27 秋問 55（FE）
プロジェクトマネジメント	問 43	アローダイアグラム	H24 秋問 52（FE）
データベース	問 46	排他制御	H28 春問 30（FE）
システム企画	問 49	CSR 調達	H28 秋問 65（FE）

注記：問 42、問 43 は、“3．平成 30 年度春期基本情報…”の表中と重複します（平成 30 年度春期基本情報技術者試験と平成 29 年度秋期以前の試験の両方で出題されています）。

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 27001:2014、JIS Q 27002:2014、JIS Q 31000:2010、JPCERT/CC “CSIRT ガイド（2015.11.26）”、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、前回の出題頁数に比べて、問 1 は 5 頁減って 10 頁、問 2 は 3 頁減って 9 頁、問 3 は変わらず 12 頁となっています。前回に比べて全体で 8 頁も減ったことから、文章量も減り読み解く時間が減少したといえます。ここで、問 1 の組合せ解答群の対応で解法時間を費やした場合、問 2 及び問 3 の解法時間への影響が発生した可能性があります。言い換えれば、組合せ解答群の対応における時間配分が合否を分けたと考えます。

また、IPA から発表されている午後の出題範囲に沿って、「情報セキュリティマネジメントの計画、情報セキュリティ要求事項」及び「情報セキュリティマネジメントの運用・継続的改善」に関連した内容でバランスよく出題されました。

問 1「個人情報の保護に関する法律への対応」では、個人情報の保護法、個人情報データにおける匿名加工情報を取り扱う上での留意点、情報セキュリティ対策の検討などが出題されました。

問 2「内部不正事案」では、内部不正事案に基づく調査、原因分析などが出題されました。

問 3「企業統合における情報セキュリティガバナンス」では、企業合併後の組織体制の立直し（内部統制）、メールの誤送信（ヒヤリハット）、シャドーIT などが出題されました。

全体のページ数が減少したことで文章量や設問数の減少が顕著で、かつ、前回よりも技術的な要素の高い出題内容が減少しました。前回までの出題内容と比較した場合、個人情報の保護法や労働安全衛生法などの法律への対応、組織内部のインシデントの原因追究・対策・再発防止策などが重点的に出題されたと考えます。さらに、難易度的には、初回から徐々に引き上げられている傾向は今回で一旦和らいだようです。

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：やや低い、1：低い】

	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
問 1	個人情報の保護に関する法律への対応（10 頁） ・情報セキュリティリスクアセスメント及びリスク対応（リスク対応策の検討） ・業務の外部委託における情報セキュリティの確保	3	設 1　空欄選択×4 設 2(1)　選択・組合せ 設 2(2)　選択×2 設 2(3)　選択・組合せ 設 3(1)　選択・組合せ 設 3(2)　選択・組合せ	30 分程度 34 点
問 2	内部不正事案（9 頁） ・情報セキュリティインシデントの管理（発見、再発防止案の提案、証拠の収集） ・情報セキュリティの意識向上（内部不正による情報漏えいの防止）	3	設 1(1)　空欄選択 設 1(2)　空欄選択・組合せ 設 2(1)　空欄選択×4 設 2(2)　空欄選択×3	30 分程度 34 点
問 3	企業統合における情報セキュリティガバナンス（12 頁） ・情報資産の管理（情報セキュリティポリシの維持管理） ・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 ・情報セキュリティマネジメントの継続的改善	3	設 1(1)　選択 設 1(2)　空欄選択 設 2(1)　空欄選択 設 2(2)　選択 設 3(1)　選択 設 3(2)、(3)　選択・組合せ 設 3(4)　空欄選択×2 設 3(5)　空欄選択・組合せ	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 点以上を午後の試験の合格点とする。

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】個人情報の保護に関する法律への対応

個人情報保護法の大幅な改正に伴い、個人情報の保護が強化されたほか、個人情報をビッグデータと位置付けて再利用することが求められています。企業においては、個人情報を単なる保護データとして扱うのではなく、有効活用を図ることによって経営に最大限活用し、利益に貢献することが重要です。

問 1 では、個人情報保護法の改正の重要性を把握した上で、モバイル PC の導入に伴い発生する情報セキュリティリスクへの対策の立案を主要なテーマとしています。

具体的な出題内容は、ヘルスケア商品の販売代理店での営業スタイルの見直しを基に、個人情報の保護法、情報セキュリティ対策の検討、マーケティング計画の立案の検討、義務規定に基づく違反行為などを考察します。自社のマーケティング分析のニーズに合致する個人情報データにおける匿名加工情報の加工、及び匿名加工情報などを取り扱う上での留意点を問いています。

問題単体のボリュームとしては前回よりも 5 ページほど減少し、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。ただし、「要配慮個人情報」、「明示」、「労働安全衛生法」などの法規の用語は、事前に習得しておく必要がありました。

□ 問 2【必須問題】内部不正事案

顧客情報や製品情報などの重要な情報が、組織内部者による内部不正により持ち出される事案が多く発生しています。また、中小企業では、退職者による内部不正も多く、内部不正対策に関する方針やルールが未整備の企業も多いようです。

問 2 では、内部不正の防止策のために、「内部不正を生み出す 3 要因：不正のトライアングル」の理解や、組織の実態に応じてリスクを適切に把握し、「組織」、「人」、「技術」の 3 面からの原因分析を主要なテーマとしています。

具体的な出題内容は、保険代理店で発生した内部不正事案を基に、内部不正事案に基づく調査、原因分析を考察しています。

問題単体のボリュームとしては前回よりも 3 ページほど減少し、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】企業統合における情報セキュリティガバナンス

情報システムの利用者の業務実態を十分に調査・分析を行わないまま、情報セキュリティ対策を施すことで、現場での業務遂行に支障が生じる事例が多発しています。これが基となって、近年ではシャドーIT のようなルール違反が生じる要因となっています。

問 3 では、情報セキュリティ対策の向上だけを重視せずに、情報セキュリティガバナンスの原則である「利害関係者の要望を満たすとともに、利害関係者のそれぞれに価値を提供することが、長期的な情報セキュリティの成功のために不可欠である」という指標を目指して、経営方針に従い、使いやすい情報システムの実現を主要なテーマとしています。そのために、情報セキュリティリーダは、現場の改善要望のヒアリング、機能改善を通して、企画・調整・管理などを積極的に推進します。

具体的な出題内容は、企業合併後の組織体制を基に、法改正に伴い個人情報取扱事業者に該当する理由、内部統制、客先へのメール誤送信（ヒヤリハット）、シャドーIT、情報セキュリティポリシの違反・調査・対策・再発防止策などを考察しています。

問題単体のボリュームとしては前回と同じ頁数で、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。

4．午後問題の講評

今回の出題においても、数値分析に基づく計算問題が 1 題もなく、具体的なサイバー攻撃の内容、RSA や AES の暗号化や復号の手順、認証技術といった技術的な要素の高い出題は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。

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。

今回は、問題の難易度アップ及びボリュームアップが、前回までに比べて少し和らぎました。そのまま次回以降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ころです。