平成 29 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 29 年度春期情報セキュリティマネジメント試験が 4 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。

＜午前問題＞

１．分野別出題構成比率

	分野	H29 春	H28 秋	H28 春
1	テクノロジ系	66.0%（33 問）	66.0%（33 問）	68.0%（34 問）
2	マネジメント系	16.0%（ 8 問）	16.0%（ 8 問）	12.0%（ 6 問）
3	ストラテジ系	18.0%（ 9 問）	18.0%（ 9 問）	20.0%（10 問）
	合計	100.0%（50 問）	100.0%（50 問）	100.0%（50 問）

分野別出題数は、前回と同じでした。

２．中分類別出題構成比率

	中分類	H29 春	H28 秋	H28 春
1	セキュリティ	60.0%（30 問）	60.0%（30 問）	60.0%（30 問）
2	法務	10.0%（ 5 問）	12.0%（ 6 問）	12.0%（ 6 問）
3	システム構成要素	2.0%（ 1 問）	2.0%（ 1 問）	2.0%（ 1 問）
4	データベース	2.0%（ 1 問）	2.0%（ 1 問）	2.0%（ 1 問）
5	ネットワーク	2.0%（ 1 問）	2.0%（ 1 問）	4.0%（ 2 問）
6	プロジェクトマネジメント	2.0%（ 1 問）	2.0%（ 1 問）	2.0%（ 1 問）
7	サービスマネジメント	6.0%（ 3 問）	6.0%（ 3 問）	4.0%（ 2 問）
8	システム監査	8.0%（ 4 問）	8.0%（ 4 問）	6.0%（ 3 問）
9	システム戦略	4.0%（ 2 問）	2.0%（ 1 問）	2.0%（ 1 問）
10	システム企画	2.0%（ 1 問）	2.0%（ 1 問）	2.0%（ 1 問）
11	企業活動	2.0%（ 1 問）	2.0%（ 1 問）	4.0%（ 2 問）
	合計	100.0%（50 問）	100.0%（50 問）	100.0%（50 問）

(1)　前回と比較して、“システム戦略”が 1 問増えました。

(2)　前回と比較して、“法務”が 1 問減りました。

(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 29 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 2	サイバーセキュリティ経営ガイドライン	問 39
	問 10	タイムスタンプサービス	問 41
	問 17	DMZ を用いたサーバ設置方法	問 43
	問 23	ディレクトリトラバーサル攻撃	問 37
	問 30	サーバ検査でのポートスキャナ	問 45
システム監査	問 38	被監査部門と意見交換を行う目的	問 58
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
データベース	問 45	データマイニング	問 29

(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、前回及び前々回も同様でした。

(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。前回（H28 秋）は 7 問、前々回（H28 春）は 6 問であり，毎回 1 問ずつ増えています。

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 15	ディジタルフォレンジックス		H27 秋問 43
	問 16	パスワードの不正取得の対策		H25 秋問 44
	問 17	DMZ を用いたサーバ設置方法	H26 秋問 40	
	問 20	ハッシュ関数	H25 秋問 38	H24 春問 38
	問 22	ディジタル署名に用いる鍵	H22 秋問 39	H26 秋問 36
	問 23	ディレクトリトラバーサル攻撃	H26 秋問 44	H21 春問 42
	問 30	サーバ検査でのポートスキャナ	H26 秋問 45	
法務	問 31	電子署名法		H27 春問 80
システム監査	問 36	特権 ID の不正使用の発見		H25 春問 60
	問 37	システムテストの監査		H24 春問 58
サービスマネジメント	問 40	システムの運用テスト	H27 春問 55	
プロジェクトマネジメント	問 43	アローダイアグラム	H27 秋問 51	
システム戦略	問 47	中長期の経営計画	H24 春問 62	H21 秋問 63
	問 48	業務プロセスの抜本的な再設計	H27 秋問 62	
システム企画	問 49	受注管理システムの非機能要件		H26 秋問 64
企業活動	問 50	企業活動における BCP		H21 春問 75

注記：問 17、問 23、問 30、問 43 は、“３．平成 29 年度春期基本情報…”の表中と重複します（平成 29 年度春期基本情報技術者試験と平成 28 年度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 27001:2014、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

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、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、リスクの特定・分析・評価，リスク対応策の検討，リスク対応計画の策定がバランスよく出題されました。一見すると 1 題あたりの設問数が多いため、難易度が高めかと感じられますが、全体的な難易度は平成 28 年度秋期と同等、もしくは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」に関連した内容で出題されました。

問 1「マルウェア感染の対応」では、企業内においてランサムウェア（身代金要求型不正プログラム）に感染した事例を基に、調査分析の基本方針や企業としてふさわしい対応について考察します。問 2「クラウドサービスを利用した情報システムの導入と運用」では、メール送受信に関するクラウドサービスの導入事例を基に、外部サービス利用時のセキュリティ面での留意点、及び当該サービスにおけるアクセス制御（アクセス権の設定）について考察します。問 3「オフィスの物理的セキュリティ」では、オフィスレイアウトの変更を題材に、機密性確保の手段や共連れ対策、施錠方式について考察します。

各問ともに 10 頁と情報量は従来どおり多めですが、各設問の説明文から“どの部分の記述から正答を導けばよいか”が比較的分かりやすく記述されており、解答に要する時間は前回よりも少なく済んだと予想します。

なお、個々の設問で問われる内容は午前問題をベースとした知識と論理的な考察を必要とするものも多く、求められるスキルのレベルは前回よりも向上した印象を受けます。また、“ Tor（匿名ネットワーク）”や“アンチパスバック（入室する際の認証記録がない不審者の退室を許可しない仕組み）”などの説明がなく、最新用語の知識が必要になる設問も出題されました。また、今回も計算問題は出題されませんでした。

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	マルウェア感染の対応（10 頁） ・部門の情報システム利用時の情報セキュリティの確保 ・マルウェアからの保護 ・情報セキュリティインシデントの管理 ・情報セキュリティリスクアセスメント及びリスク対応 ・情報資産管理	2	設 1(1)　空欄選択 1 設 1(2)、(3)　選択・組合せ 2 設 2(1)　空欄選択・組合せ 2 設 2(2)　選択・組合せ 設 3(1) ～ (3)　選択・組合せ 3	20 分程度 34 点
問 2	クラウドサービスを利用した情報システムの導入と運用（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 ・部門の情報システム利用時の情報セキュリティの確保 ・利用者アクセスの管理	3	設 1(1)　空欄選択 1 設 1(2)　選択・組合せ 設 1(3) 、(4)　空欄選択 2 設 2(1)　空欄選択 3 設 2(2)　選択・組合せ	30 分程度 34 点
問 3	オフィスの物理的セキュリティ（10 頁） ・情報資産に関する情報セキュリティ要求事項の提示 ・物理的及び環境的セキュリティ ・情報セキュリティリスクアセスメント及びリスク対応 ・情報セキュリティマネジメントの継続的改善	3	設 1(1)　空欄選択・組合せ 3 設 1(2)　選択 1 設 1(3)　選択 4 設 2　空欄選択・組合せ 設 3　空欄選択 4	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 点以上が午後の合格点となります。

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しています。

3．出題傾向及び問題別分析

□ 問 1【必須問題】マルウェア感染の対応

ここ数年、ランサムウェアによる被害が国内でも広がっています。

問 1 では、ランサムウェアへの組織における対策を題材にして、適切なバックアップによる感染時の被害の備え、リストア（リカバリ）手段の確認、及びバックアップ自体をランサムウェアから保護する対策、また、組織内の重要な情報資産の特定とその資産についてのリスク評価の定期的な実施、及びランサムウェア感染時の対応を主要なテーマとしています。

具体的な出題内容は、ランサムウェアの感染という情報セキュリティインシデントを事例として、情報セキュリティリーダに求められる適切な対応、及び管理・技術の両面からの情報セキュリティの改善施策の考察でした。

問題単体のボリュームとしては前回よりも 1 頁減りましたが、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】クラウドサービスを利用した情報システムの導入と運用

ここ数年、企業の業態や規模を問わず、業務の効率化及び生産性向上を目的としたクラウドサービスの利用が急速に拡大しています。

問 2 では、インターネット経由でアクセスするクラウドサービスを題材にして、昨今、クラウドサービスの利便性が高まる中で、適用業務に応じた利用者側の留意点を主要なテーマとしています。

具体的な出題内容は、クラウドサービスの導入・運用上での情報セキュリティの観点から留意すべき事項の考察、及び社内規程と適用業務を踏まえて、アカウントの付与及び操作権限の設定の考察でした。

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】オフィスの物理的セキュリティ

オフィスの情報セキュリティを確保するためには、オフィスごとの環境、レイアウト、取り扱う情報などに適した物理的セキュリティ対策が求められます。

問 3 では、各オフィスの情報セキュリティリーダの役割を題材にして、情報セキュリティリーダはそのオフィスの物理的セキュリティ対策が適切であるかを評価し、必要があれば改善案を提案します。また、物理的セキュリティ対策は、そのオフィスで働く全ての従業員に関わるため、業務への影響を考慮した改善策を主要なテーマとしています。

具体的な出題内容は、レイアウトが変更された後のオフィスにおいて、情報セキュリティ上の問題点の指摘、そして、その問題点に対する業務への影響を考慮した改善策の考察でした。

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。

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要素を含んだ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、マルウェア感染の対応（マルウェアに感染した事例に基づく調査分析の基本方針や企業としての対応）、クラウドサービスを利用した情報システムの導入と運用（外部サービス利用時におけるセキュリティ面での留意点、及び当該サービスにおけるアクセス権の設定）、オフィスの物理的セキュリティ（オフィスレイアウトの変更に基づく機密性確保の手段や共連れ対策、施錠方式）などといったように、世相を反映し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、基本情報技術者試験における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。

今回の難易度及び問題のボリュームバランスが、次の試験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。