平成 30 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 30 年度秋期情報セキュリティマネジメント試験が 10 月 21 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 秋	H30 春	H29 秋	H29 春	H28 秋	H28 春
1	テクノロジ系	33	34	33	33	33	34
2	マネジメント系	8	7	8	8	8	6
3	ストラテジ系	9	9	9	9	9	10
	合計	50	50	50	50	50	50

(1)　前回と比較して、出題数が増えた分野は、“マネジメント系（+1 問）”でした。

(2)　前回と比較して、出題数が減った分野は、“テクノロジ系（−1 問）”でした。

2．中分類別出題数

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

(1)　前回と比較して、出題数が増えた中分類は、“サービスマネジメント（+2 問）”、“システム戦略（+1 問）”でした。

(2)　前回と比較して、出題数が減った中分類は、“法務（−1 問）”、“システム構成要素（−1 問）”、“システム監査（−1 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 年度秋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 1	CSIRT マテリアル	問 40
	問 14	ボットネットでの C&C サーバ	問 41
	問 17	セキュアブート	問 43
	問 20	アクセスポイント	問 44
	問 25	ディジタル署名	問 36
法務	問 37	ISMS 内部監査の監査報告書	問 58
プロジェクトマネジメント	問 43	WBS	問 51
システム企画	問 49	要件定義プロセス	問 65

(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 5 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 年度春期～平成 30 年度春期は同様に 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）、基本情報技術者試験（FE）、応用情報技術者試験（AP）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	過去問題
セキュリティ	問 1	CSIRT マテリアル	H29 春問 3　(SG)
	問 5	SaaS の情報セキュリティ管理	H28 春問 41　(FE)
	問 13	ゼロデイ攻撃	H27 秋問 42　(AP)
	問 14	ボットネットでの C&C サーバ	H28 秋問 12　(SG)
	問 18	NTP（UDP、ポート番号 123）	H28 秋問 19　(SG)
	問 19	ローカルホスト	H27 春問 45　(AP)
	問 22	サーバ証明書の正当性	H29 春問 37　(AP)
	問 26	AES	H27 春問 39　(FE)
	問 27	暗号方式の特徴	H29 春問 38　(AP)
	問 29	SSH	H26 春問 44　(AP)
	問 30	WAF	H29 春問 29　(SG)
法務	問 33	電子署名法	H29 春問 31　(SG)
	問 34	Web ページの著作権	H29 春問 78　(AP)
	問 35	ボリュームライセンス契約	H20 春問 80　(FE)
システム監査	問 38	外部委託管理の監査	H28 春問 60　(AP)
プロジェクトマネジメント	問 43	WBS	H28 春問 51　(FE)
システム戦略	問 48	ディジタルディバイドの解消	H26 春問 64　(FE)
システム企画	問 49	要件定義プロセス	H29 春問 66　(FE)
企業活動	問 50	リーダシップのスタイル	H25 秋問 74　(AP)

注記：問 1、問 14、問 43、問 49 は、“3．平成 30 年度春期基本…”の表中と重複します（平成 30 年度秋期基本情報技術者試験と平成 30 年度春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、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、分野を絞って演習することが効果的でしょう。

＜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）の午後問題については、前回の出題頁数に比べて、問 1 は 4 頁増えて 14 頁、問 2 は 1 頁増えて 10 頁、問 3 は 1 頁減って 11 頁となっています。前回に比べて全体で 4 頁増えましたが、文章量は前回と同等レベルといえます。問 1 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、問 2、問 3 を先に解き始めたことが、多少なりとも有利に働き合否に影響した可能性があります。

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「インターネットを利用した振込業務の情報セキュリティ」では、インターネットバンキングサービスの利用、サービス利用時の情報セキュリティリスク及びその対策などが出題されました。

問 2「リスク対応策の検討」では、リスク対策の脆弱性、情報処理安全確保支援士からの指摘事項に基づく対応方針の検討などが出題されました。

問 3「標的型メール攻撃への対応訓練」では、標的型メール攻撃対策の検討、訓練計画の実施案及び実施後の改善策などが出題されました。

全体のページ数では 4 頁増えましたが、文章量や設問数は前回同等であると考えます。また、技術的な要素の出題内容では、トークンやワンタイムパスワード、ネットバンキングユーザを狙ったサイバー攻撃である MITB（Man in the Browser）攻撃、ドメイン指定によるメールフィルタリングなどが出題されました。難易度的には、前回同様、初回から徐々に引き上げられている傾向は和らいでいるようです。

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	インターネットを利用した振込業務の情報セキュリティ（14 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） ・部門の情報システム利用時の情報セキュリティの確保（サイバー攻撃）	4	設 1、設 2　選択 設 3(1)、(2)　空欄選択×3 設 4(1)、(2)　選択 設 5(1)　選択 設 5(2)、5(3)　空欄選択 設 5(4)、5(5)　空欄選択×2	30 分程度 34 点
問 2	リスク対応策の検討（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） ・部門の情報システム利用時の情報セキュリティの確保（バックアップ） ・情報セキュリティの意識向上（情報漏えいの防止）	3	設 1(1)、(2)　選択 設 1(3)　空欄選択×2 設 1(4)、(5)　選択 設 1(6)　空欄選択×4 設 1(7)　空欄選択	30 分程度 34 点
問 3	標的型メール攻撃への対応訓練（11 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） ・情報セキュリティの意識向上（情報セキュリティの教育・訓練） ・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）	3	設 1　選択・組合せ 設 2(1)　選択 設 2(2)　空欄選択×2 設 3　選択 設 4(1)　選択・組合せ 設 4(2)　選択・組合せ 設 4(3)　空欄選択×2	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】インターネットを利用した振込業務の情報セキュリティ

インターネットバンキングサービスが普及する中で、何らかの手段を用いて取引に関する情報を入手し、金銭を詐取する詐欺事例が多発しています。企業の担当者に偽の電子メールを送り付け、詐欺を企てるために用意した口座に振り込ませるという手口は、被害額が年々多額傾向にあり、警戒が求められています。

問 1 では、BEC（Business E-mail Compromise：ビジネスメール詐欺）の被害に遭遇した企業を舞台に、振込手続、及び取引先との電子メールのやり取りを主要なテーマとしています。

具体的な出題内容は、インターネットバンキングサービスの利用、サービス利用時の情報セキュリティリスク及びその対策、サイバー攻撃の事例及び対策などを考察します。利用者のディジタル証明書と秘密鍵を IC カードに格納する目的、内部不正を事前に防ぐ手段、サービス利用時の情報セキュリティリスク（不正なログイン操作、不正な振込の承認、なりすましによる不正な振込の操作）及び対策、MITB の対策、ログ収集システムのログデータの活用などについて問います。

問題単体のボリュームとしては前回よりも 4 ページほど増加し、各設問で問われている内容も比較的難易度が高めでしたが、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 2【必須問題】リスク対応策の検討

情報セキュリティ対策は、リスク分析、情報システムの構成、対策の有効性、対策にかかるコストや運用コストなどを考慮して検討する必要があります。利用部門においては、情報セキュリティを推進する立場にある情報セキュリティリーダの役割も重要性を増しています。

問 2 では、情報セキュリティ点検を受けた結果を基に、改善を行っていく状況設定、複数の改善策の中の最も適切な改善策を主要なテーマとしています。OS の延長サポートの対応、退職者の従業員 ID の取扱い、ホワイトリストやブラックリストによるフィルタリング、ファイルサーバとそのバックアップなどについて問います。

具体的な出題内容は、リスク対策の脆弱性、指摘事項に基づく対応方針の検討、指摘事項の対応方針の問題点を考察します。

問題単体のボリュームとしては前回よりも 1 ページ増加しましたが、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】標的型メール攻撃への対応訓練

昨今、標的型メール攻撃が増加傾向にあり、マルウェアによる個人情報漏えい、金銭詐取といったトラブルが急増しています。企業内においては、標的型メール攻撃への対応訓練があります。その訓練では、組織の業務内容、社内メールシステム、情報セキュリティ対策の状況、訓練の目的などを明確にして計画を立案することが重要です。

問 3 では、派遣及び転職を支援する人材サービス会社における標的型メール攻撃への対応訓練を主要なテーマとしています。情報セキュリティリーダに必要となる、適切な訓練計画を立案する能力及び訓練で明らかになった課題に対する解決策を検討します。

具体的な出題内容は、標的型メール攻撃対策の検討、訓練計画（目的、不具合、理由、解決案、実施案、改善策）などを考察します。標的型メール攻撃対策の具体的な訓練内容、その訓練の目的、訓練用メールに実在する社名やアドレスを使用した場合の被害、ドメイン指定によるメールフィルタリング、不審メールの受信時の対応手順、不審メールの添付ファイルを開封した場合の予想される被害、標的型メール攻撃訓練の課題についての解決策やその実施案などについて問います。

問題単体のボリュームとしては前回よりも 1 ページ減少し、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。

4．午後問題の講評

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。

前回同様、問題の難易度アップ及びボリュームアップが和らぎつつあり、全体的に落ち着いてきていると考えます。こ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。