平成 29 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 29 年度秋期情報セキュリティマネジメント試験が 10 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．分野別出題構成比率

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

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

(1)　前回と比較して、“法務”が１問増えました。

(2)　前回と比較して、“システム戦略”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	問番号	テーマ	基本情報技術者試験
セキュリティ	問 21	ボットネットにおける C&C サーバ	問 36
	問 22	DNS キャッシュポイズニング	問 37
	問 23	RSA	問 38
	問 24	ディジタル署名	問 40
	問 27	トロイの木馬とワームの比較	問 41
システム監査	問 40	監査調書	問 60
ネットワーク	問 47	NAT	問 33
データベース	問 50	CIO	問 75

(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 3 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、H29 春は 8 問、H28 秋は 7 問、H28 春は 6 問でした。

４．基本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
セキュリティ	問 18	パスワードによる利用者認証	H26 春問 42
	問 22	DNS キャッシュポイズニング	H24 秋問 37
	問 23	RSA	H23 春問 42
	問 24	ディジタル署名	H27 春問 38
	問 28	公開鍵暗号方式	H27 春問 40
	問 29	HTTP over TLS（HTTPS）	H25 春問 44
法務	問 33	著作権法	H28 春問 79
システム監査	問 39	システム監査を実施する目的	H28 春問 60
	問 40	監査調書	H25 春問 57
サービスマネジメント	問 43	逓減課金方式のグラフ	H25 秋問 58
ネットワーク	問 47	NAT	H22 春問 36
企業活動	問 50	CIO	H15 春問 74

注記：問 22、問 23、問 24、問 40、問 47、問 50 は、“３．平成 29 年度秋期基本情報…”の表中と重複します（平成 29 年度秋期基本情報技術者試験と平成 29 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、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、前回の出題内容に比べて、問 1 の出題頁数が 5 頁増えて 15 頁となり、問 2 及び問 3 も 2 頁ずつ増えて 12 頁となっています。文章量が大幅に増えたことで、読み解く時間が増したといえます。特に、問 1 で 30 分以上の解法時間を費やした場合には、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。

また、IPA から発表されている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」に関連した内容でバランスよく出題されました。ただし、インシデントへの事後対応についての内容は少なく、事前のリスク分析及び対策の考察についての出題内容が多くなったと分析しています。

問 1「情報セキュリティリスクアセスメント」では、各種情報資産の CIA（機密性、完全性、可用性）を基に、脅威、脆弱性を考慮した詳細なリスク分析を行うとともに、各リスクへの対策を考察します。

問 2「Web サービスでの Web アプリケーションソフトウェア開発委託」では、Web アプリケーションソフトウェア（以下、Web アプリという）への攻撃の分類と対策、開発委託時の留意点を考察します。

問 3「スマートデバイスの業務利用における情報セキュリティ対策」では、モバイル環境で NPC などを活用する際のリスクと対策を考察します。

各問においてページ数が増えたことによる文章量や設問数の増加が顕著で、前回までは技術的な用語の知識を問う設問がやや多かった印象を受けましたが、今回はそれほど多くの出題はありませんでした。また、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未だに続いているように思われます。

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・配点割合
問 1	情報セキュリティリスクアセスメント（15 頁） ・情報資産管理の計画 ・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 ・情報セキュリティの教育／訓練	4	設 1　空欄 1 選択 設 2　空欄 2 選択・組合せ 設 3(1)　空欄選択・組合せ×2 設 3(2)、(3)　選択・組合せ 設 3(4)、(7)　空欄選択 2・組合せ 設 3(5)、(6)　選択・組合せ 設 3(8)　選択・組合せ	30 分程度 34 点
問 2	Web サービスでの Web アプリケーションソフトウェア開発委託（12 頁） ・外部委託先における情報セキュリティの確保 ・情報セキュリティリスクアセスメント及びリスク対応	3	設 1(1)　選択 2 設 1(2)　選択 設 2(1)、(2)　空欄選択・組合せ×2 設 2(3)　選択・組合せ 設 3(1)　空欄選択 設 3(2)、(3)　選択 1×2 設 4(1)、(2)　選択 1×2	30 分程度 34 点
問 3	スマートデバイスの業務利用における情報セキュリティ対策（12 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 ・情報セキュリティの教育／訓練	3	設 1(1)　空欄選択 3 設 1(2)　空欄選択 2・組合せ 設 1(3)　選択 1 設 2(1)　空欄選択 2・組合せ 設 2(2)　空欄選択 1 設 2(3)　空欄選択 2 設 2(4)　選択 2・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】情報セキュリティリスクアセスメント

情報セキュリティに関わる新たな脅威は年々増加し、企業における情報セキュリティの重要性は益々高まっています。情報資産管理台帳の維持管理及び情報セキュリティリスクアセスメントを基に、経営資源を活用し、情報セキュリティ対策をどのように講じるかを日々検討します。

問 1 では、在宅勤務の導入に伴う IT 利用環境の変化を題材に、業務の現場で求められる情報セキュリティリスクアセスメント、詳細なリスク分析を主要なテーマとしています。

具体的な出題内容は、3 種類の在宅勤務形態の特徴、情報資産台帳におけるリスク値の再評価、在宅勤務の脅威や脆弱性の洗出し、表面化したリスクへの技術的な対応を考察します。

各設問で問われている内容は比較的平易であり、配分時間内で正答が得られたと予想します。ただし、問題単体のボリュームとしては前回よりも 5 ページほど増えたことから、難易度は例年よりもやや高いといえます。

□ 問 2【必須問題】Web サービスでの Web アプリケーションソフトウェア開発委託

Web サイトの脆弱性を突いた攻撃は増加傾向にあり、そのために個人情報や機密性のある情報などの漏えいが多々見られます。これらの攻撃への対策を Web サイトや Web アプリなどの開発委託先であるベンダにすべてを一任するのではなく、委託先への情報セキュリティ要求事項を委託仕様書及び契約書に盛り込み、検収時に脆弱性診断を行って、その結果を対策に反映させることで Web サイトの安全性の確保に努めます。

問 2 では、Web アプリ開発の外部委託を題材に、情報セキュリティ要求事項の検討、及び脆弱性診断結果を踏まえた対応、業務の継続性や情報セキュリティ上のリスクを考慮した上で、根本的な解決策と暫定的なリスク低減策の比較及び検討を主要なテーマとしています。

具体的な出題内容は、現行サービスの認証機能の強化対応、情報セキュリティ向上となる委託仕様書への適切な追加事項、脆弱性診断結果に基づく対応、WAF 導入のメリットを考察します。

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】スマートデバイスの業務利用における情報セキュリティ対策

ここ数年、取引先訪問のための外出中などにおいて、スマートデバイスを用いて、いつでも仕事ができる制度（以下，モバイルワークという）が注目されています。モバイルワークは、利益を追求するための競争力強化の可能性があることから、導入する企業が年々増えています。導入する企業にとっては、情報セキュリティのリスクや課題を想定し、事前に対策を検討しておくことが要求されます。

問 3 では、モバイルワークでのスマートデバイスの利用を題材に、情報セキュリティ対策を実施することによって、新たに発生する可能性のある課題を事前に洗い出し、その解決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、情報セキュリティ上のリスク分析と対策、その対策の実現に向けた調査を考察します。

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、RSA や AES の暗号化や復号の手順といった技術的な要素の高い出題は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、在宅勤務の導入に伴う IT 利用環境、Web アプリ開発の外部委託先への要求事項、スマートデバイスの業務利用といった、ここ数年で増加傾向にある業務形態における情報セキュリティの対策や安全確保の出題内容でした。

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。

今回の難易度及び問題のボリュームバランスが、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考えております。