令和元年度秋期
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

令和元年度秋期情報セキュリティマネジメント試験が 10 月 20 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	R1 秋	H31 春	H30 秋	H30 春	H29 秋	H29 春
1	テクノロジ系	33	33	33	34	33	33
2	マネジメント系	8	7	8	7	8	8
3	ストラテジ系	9	10	9	9	9	9
	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、“ストラテジ系（−1 問）”でした。

２．中分類別出題数

	中分類	R1 秋	H31 春	H30 秋	H30 春	H29 秋	H29 春
1	セキュリティ	30	30	30	30	30	30
2	法務	6	6	5	6	6	5
3	システム構成要素	1	1	1	2	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	1
6	プロジェクトマネジメント	2	1	1	1	1	1
7	サービスマネジメント	2	2	3	1	3	3
8	システム監査	4	4	4	5	4	4
9	システム戦略	1	2	2	1	1	2
10	システム企画	1	1	1	1	1	1
11	企業活動	1	1	1	1	1	1
	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、“プロジェクトマネジメント（+1 問）でした。

(2)　前回と比較して、出題数が減った中分類は、“システム戦略（−1 問）”でした。

3．令和元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 18	WPA3	問 37
	問 21	バックドア	問 39
	問 22	マルウェアの動的解析	問 36
	問 26	SMTP-AUTH	問 44
法務	問 33	シュリンクラップ契約	問 79
システム監査	問 39	アクセス制御の監査	問 60
プロジェクトマネジメント	問 44	アローダイアグラム	問 52

4．情報セキュリティマネジメント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	テーマ	過去問題
セキュリティ	問 3	リスクの受容	H28 春問 5
	問 4	組織における内部不正防止	H30 春問 4
	問 5	是正処置	H29 秋問 10
	問 7	SPF	H30 春問 10
	問 10	シャドーIT	H29 秋問 16
	問 11	ステガノグラフィ	H29 秋問 17
	問 15	ボットネットでの C&C サーバ	H29 秋問 21
	問 17	AES を使うときの鍵	H28 春問 28
	問 20	ディジタル署名に用いる鍵	H29 春問 22
	問 24	リスクベース認証	H30 春問 25
	問 27	PCI DSS	H29 春問 26
	問 30	ポートスキャンの利用目的	H29 春問 30
システム監査	問 37	データの正当性及び網羅性	H29 秋問 38

5．他の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	テーマ	過去問題
セキュリティ	問 16	DNS キャッシュポイズニング	H29 春 FE 問 36
	問 26	ハイブリッド暗号方式	H22 秋 FE 問 41
法務	問 34	プログラム著作権の原始的帰属	H30 春 FE 問 79
	問 36	労働法	H28 春 AU 前Ⅱ問 2
システム企画	問 49	RFP の作成と対応	H24 春 AP 問 65

注記　FE：基本情報技術者試験、AP：応用情報技術者試験、
AU 前Ⅱ：システム監査技術者試験 午前Ⅱ

6．今後の指導方法

⑴　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重要です。

⑵　情報セキュリティマネジメント試験の過去問題から多く再出題されていることから、過去問題の演習を徹底し、過去問題を十分にマスタする対策が得点力アップにつながります。

⑶　セキュリティや法務，監査などの最新情報に興味をもち、インターネットを活用して学習することも必要でしょう。

＜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、出題ページ数は、前回に比べて、問1は変わらず13ページ、問2も変わらず14ページ、問3は2ページ増えて14ページとなりました。全体では2ページの増加となりますが、前々回からは6ページの増加となっており、平成30年度秋期から3回連続の増加となりました。一方、文章量は、前回と同程度だったといえます。設問の数も前回と同程度でした。

また、今回の問題を問ごとに見ると、設問数はほぼ同分量で、難易度に大きな差はなかったと考えます。

今回も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」に関連した内容で出題されましたが、インシデント発生時の対応に関する問題や業務委託に関する問題など、「情報セキュリティマネジメントの運用・継続的改善」に関連した内容の出題が多くありました。

問1「EC サイトの情報セキュリティの改善」では、インシデント対応、原因・目的・対応策の検討などが出題されました。

問2「アカウント乗っ取りによる情報セキュリティインシデント」では、インシデントの発見、被害状況や被害範囲および原因の調査、対策の検討などが出題されました。

問3「業務委託先への情報セキュリティ要求事項」では、業務委託先および委託内容の検討、情報セキュリティ要求事項と評価などが出題されました。

技術的な要素の出題内容では、CAPCHA、HTTP over TLS などが出題されました。他に、難易度は高くないものの、午前問題の知識を必要とする内容は今回も随所に見られました。

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	EC サイトの情報セキュリティの改善 (13 ページ) ・情報セキュリティインシデントの管理 （発見、分析、再発防止策の提案・実施）	3	設問 1(1)、(2)　空欄選択 設問 1(3)　空欄選択・組合せ 設問 1(4)　選択 設問 2　空欄選択 設問 3(1)、(2)　空欄選択 設問 3(3)　選択 設問 4(1)　空欄選択 設問 4(2)　空欄選択・組合せ 設問 5　空欄選択×3	30 分程度 34 点
問2	アカウント乗っ取りによる 情報セキュリティインシデント (14 ページ) ・情報セキュリティインシデントの管理 （発見、初動処理、分析、再発防止策の提案・実施）	3	設問 1(1)　選択 設問 1(2)　選択・組合せ 設問 2(1)　空欄選択 設問 2(2)　選択 設問 2(3)　空欄選択 設問 2(4)、(5)　選択 設問 3　選択・組合せ 設問 4(1)、(2)　空欄選択	30 分程度 34 点
問3	業務委託先への情報セキュリティ要求事項 (14 ページ) ・業務の外部委託における情報セキュリティの確保 （外部委託先の情報セキュリティの調査、外部委託先の情報セキュリティ管理の実施） ・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、残留リスク）	3	設問 1(1)　空欄選択 設問 1(2)　選択・組合せ 設問 2　空欄選択 設問 3(1)　空欄選択 設問 3(2)　空欄選択×2 設問 3(3)、(4)　選択・組合せ 設問 4(1)　選択 設問 4(2)　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】ECサイトの情報セキュリティの改善

インターネットなどを利用した商取引の増加に伴い、Webサイトなどへの不正ログインも増えており、サイト運営側はその対策として、複数の認証技術を組み合わせることによる認証の強化を行っています。ただし、利用者側の認証情報の使い回しも攻撃増加の一因であり、認証強化だけでは攻撃を防ぐことはできないため、監視の強化も重要となっています。

問1では、生活雑貨販売会社が運営するECサイトで発生した不正ログインをテーマとして、攻撃の方法や原因・目的を分析し、利用者認証の強化を含めた今後の対応策の検討を行い、追加対策としてログの監視を検討します。

具体的な出題内容は､受けてしまった攻撃および今回防ぐことができた攻撃について行った調査･分析の内容、今後の対応策としての利用者認証強化の方法や技術の導入に関する検討内容、問題点などを問います。また、攻撃を検知するための監視すべき値について問うています。

問題単体のボリュームとしては設問数がやや多めですが、各設問で問われている内容は基本的なものが多く、配分時間内で効率よ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】アカウント乗っ取りによる情報セキュリティインシデント

業務の効率化のために、外部サービスよるチャットサービスなどを利用する企業が増えていますが、秘密情報のやり取りが含まれることもあり得るため、より高度なインシデント対応能力が必要になっています。

問2では、食品メーカの営業所における諸連絡の煩雑化解消のために導入したチャットサービスが乗っ取られたことをテーマとして、被害状況の把握、被害範囲の調査、原因の調査、対策などを行います。

具体的な出題内容は、発見時の対応および被害拡大の防止策の考察、被害状況・範囲などの調査方法などに加え、被害の調査中における乗っ取られた従業員の業務への影響やその軽減策、今後の対応策における利便性の確保などについても問うています。

問題単体のボリュームとしてはページ数および設問数が前回と同じで、各設問で問われている内容も比較的平易であったため、配分時間内で効率よ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】業務委託先への情報セキュリティ要求事項

業務効率化の一環として外部に業務を委託する企業が増えています。委託先の従業員による委託業務に関する情報の不正持ち出しという事例も発生する中、委託元の情報セキュリティリスク対策が重要となっています。

問3では、データ通信サービスおよび通話サービスを提供している企業が業務の一部を外部に委託することをテーマとして、委託先の検討、委託元としての情報セキュリティ要求事項と評価、評価結果に対する委託先としての対応策の検討を行います。

具体的な出題内容は、暗号化された情報を限定した従業員のみが復号できることについて情報セキュリティ上期待できる効果、委託先からの提案における委託元としての選択理由、要求事項に対する委託先の対策について委託元が評価した根拠やリスク、委託先として行う要求事項に有効な対応策などを問うています。

問題単体のボリュームとしては前回よりも2ページ増加しました。各設問で問われている内容は比較的平易ですが、細かな状況設定を見落とすことなく配分時間内で効率よく整理し、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、前回同様、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、文章をよく読むことにより解答できる平易な問題が多く、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、毎回のことながら文章量は多く、特に、問3は委託元と委託先のそれぞれの企業の概要、業務状況の設定を読み込み、細部まで丁寧に理解し整理することが必要で、長文問題が苦手な受験者にとっては時間のかかる問題だった思います。過去問題を解き、問題を丁寧に読み込むなど、長文問題に慣れることが有効な試験対策といえます。

問題の難易度は一定のレベルで落ち着いてきていると考えますが、ボリュームについて、特にページ数については増加傾向が見られます。これらの傾向がこのまま次回以降に継続されるとは限りませんが、今後も注視するとともに、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ています。