情報セキュリティマネジメント

1.　はじめに

1.1　総評

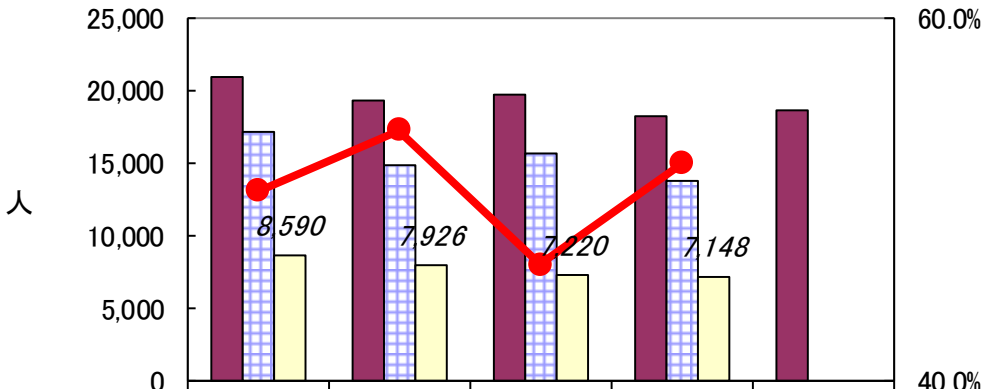
求められる知識・スキルの内容に大きな変化はなく，現場での運用を意識した内容が揃っていると評価できます。午後問題の全体的な構成も従来とさほど変わりません。

総合的な難易度は，前回(平成 31 年春)及び前々回(平成 30 年秋)とほぼ同等と評価できます。

1.2　受験者数

応募者数は 18,550 人で，前年の平成 30 年秋からは微減傾向です。

合格率については，難易度の高かった平成 30 年秋で 50%を下回りましたが，前回は再び 50%を超えました。



	H29秋	H30春	H30秋	H31春	R1秋
応募者数	20,907	19,300	19,692	18,129	18,550
受験者数	17,039	14,749	15,579	13,761	
合格者数	8,590	7,926	7,220	7,148	
合格率	50.4%	53.7%	46.3%	51.9%	

2. 午前問題の分析

全 50 問の内訳は以下のようになっていました。問 1～30 の情報セキュリティ分野については，従来と比較すると分野ごとに問題が固まって配置されておらず，ややランダムに配置されている印象を受けます。

・情報セキュリティ管理(基礎理念，各種ガイドラインなど)：7 問

従来傾向に沿った形で，JIS Q 27000 シリーズ，内部不正防止ガイドラインなどから用語の定義などが出題されました。今回は"中小企業の情報セキュリティ対策ガイドライン"からの出題はゼロでした。JIS Q 27017 がクラウドサービスに関する規格であることを知っているかなど，新たな観点からの出題もいくつか見られました。

・各種脅威とその対策：13 問

BEC(ビジネスメール詐欺)やリバースブルートフォースなど，トレンドに沿った初出の問題もいくつか見られますが，バックドアや C&C サーバなど，頻出テーマも同程度含まれています。電子メールや IoT を題材にした，インターネットを利用する際のネットワークセキュリティに関する問題が目立ちます。

・情報セキュリティ技術(暗号化，PKI，実装技術など)：10 問

やや出題数が増えている印象です。内容も VDI や SMTP-AUTH など，従来あまり聞かれていなかった踏み込んだものが少なからず含まれています。

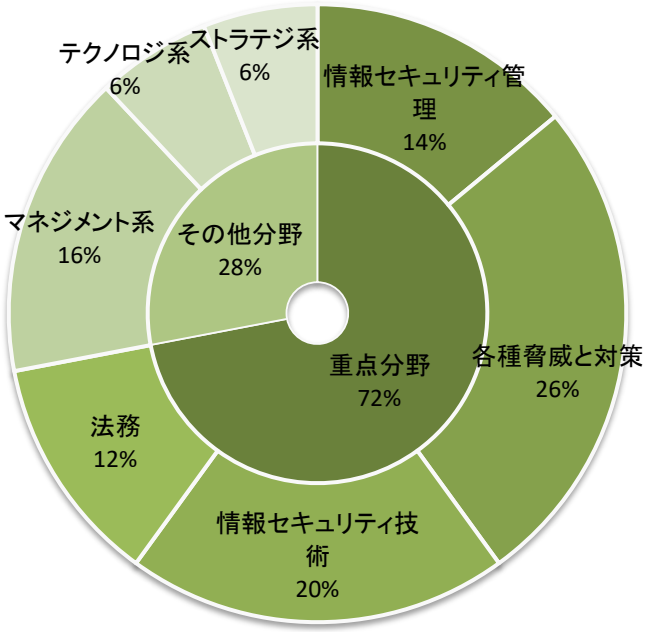
・法務　(6 問：問 31～問 36)

情報セキュリティ関連の法規に関する出題が少なく，派遣や就労規則などの労働に関する問題が目立つ構成となっています。初出の問題，及び上位区分(AP 試験や AU 試験など)から流用された問題については，難易度が高めになっています。

・その他の分野　(14 問：問 37～50)

分野ごとの出題バランスはほぼ従来どおりです。ストラテジ系において RPA やテキストマイニングなど，見慣れない用語がやや多く登場しています。

出題分野		出題率	出題数
重点分野（情報セキュリティ＋法務）		72 %	36
	情報セキュリティ管理	14 %	7
	各種脅威と対策	26 %	13
	情報セキュリティ技術	20 %	10
	法務	12 %	6
その他分野		28 %	14
	マネジメント系	16 %	8
	テクノロジ系	6 %	3
	ストラテジ系	6 %	3



従来と同様，複雑な計算や手順を必要とする事例問題はほとんどなく，

・用語や概念の定義を選ぶ問題

・簡単な状況判断や，技術の利用目的を考察する問題

で占められています。

過去試験からの流用は 50 問中 23 問程度で，ここ最近の中ではやや少なめです。ただし，過去の SG 試験からの流用数は 16 問と，逆に多くなってきました。特に平成 30 年春からは 6 問，平成 29 年秋からは 4 問が流用されており，ボリュームゾーンといえます。

その他分野は従来は流用が多めなのですが，今回は初出のものが目立ちました。

ここ数回の午前試験における「簡単に答えられる定番の用語知識問題はあまり多くなく，答えに迷いやすい内容が深化した問題が多い」傾向が継続しています。基礎的な知識だけではなかなか解きづらい問題の割合が多い印象です。

以上の点を重視し，難易度については，前回と同様にやや高めと評価しますが，前述のように「SG 過去問題の流用が増えてきた」ため，その部分については逆に対策が立てやすくなっているともいえます。過去問の演習をしっかり重ねていれば，かなり緩和できた面もあるでしょう。

問	テーマ	難易度
1	BEC	C
2	サイバー攻撃対策	B
3	リスク受容プロセス	B
4	退職従業員の不正対策	B
5	JIS Q 27000	C
6	IoT 機器への攻撃	C
7	SPF	B
8	VDI サーバの導入	C
9	JIS Q 27017	B
10	シャドーIT	A
11	ステガノグラフィ	B
12	セキュアハッシュ関数	B
13	トランザクション署名	C
14	フォールスポジティブ	C
15	C&C サーバ	A
16	DNS キャッシュポイズニング	B
17	AES	A
18	WPA3	A
19	リバースブルートフォース	B
20	ディジタル署名	A
21	バックドア	A
22	マルウェアの動的解析	B
23	メッセージ改ざん検知	B
24	リスクベース認証	B
25	ランダムサブドメイン攻撃	C
26	電子メールのセキュリティ	A
27	クレジットカードのセキュリティ	B
28	メール送信者認証	B
29	ハニーポット	A
30	ポートスキャナ	A
31	マルウェア関連法規	B
32	技術者活動関連法規	C

33	シュリンクラップ契約	B
34	プログラムの著作権	B
35	労働者派遣	B
36	労働法	C
37	正確性及び網羅性のコントロール	C
38	統制活動	B
39	システム監査技法	C
40	アクセス制御の監査	A
41	サービスマネジメント用語	B
42	エラープルーフ	B
43	プロジェクトライフサイクル	C
44	アローダイアグラム	B
45	応答時間	B
46	トランザクション	C
47	IP アドレスの問合せ	B
48	RPA	C
49	RFP	A
50	分析手法	B

注）　難易度は 3 段階評価で，C が難，A が易を意味する。

3. 午後問題の分析

午後問題3問の内容は次のようなものでした。

問1： ECサイトのセキュリティ改善

ECサイトにおける利用者IDとパスワードの運用について，複数の攻撃への対策を考察する問題です。複数種類のパスワードクラック手法が取り上げられています。

個々の論点自体は，午前試験で問われるパスワード管理の知識で十分に対応できるものです。ストーリーも読みやすく，あまり時間もかかりません。ここ最近の出題の中では，かなり平易に取り組める題材の問題だったと評価します。

問2：アカウント乗っ取りのインシデント対応

なりすましを題材に，調査分析の進め方などについて考察する問題です。

前半で提示されるシステムやサービスの仕様に関する情報が多く，この部分を整理するのに時間を費やします。それに関連して，いくつかの選択肢が「丁寧に個々の項目を洗い出し，取捨選択する」タイプのものになっており，じっくり考えないとミスしてしまうこともあるでしょう。

問3：業務委託におけるセキュリティ

コールセンタ業務を委託する際の，PC管理や物理的セキュリティなどについて考察する問題です。

委託契約に関する法規的な知識はさほど必要とせず，どちらかといえば「ロールごとのアカウント設定」や「フロアごとのアクセス管理」といった一般的なセキュリティ管理に関する内容となっています。個々の論点自体は深い知識を要求するものではありませんが，「組織の違い」や「フロアの違い」といった複数の要件を組み合わせて考察する場面が多く，かなり時間を要してしまう面もあります。

ページ数はそれぞれ13，14，14で，前回同様でした。問1がかなり平易なため，時間はかなり余裕があったでしょう。前回のレッドチームやCVSSのように高度な知識・理解が求められる場面は少なく，パスワードやアカウント管理，認証に関する基本知識があれば，あとはどの問題もパズルを解く要領で読み解くことができます。

以上を考慮し，午後試験の全体的な難易度は前回と同程度か，やや易しめと評価します。ここ数年で緩やかに難易度上昇を続けていた午後試験が，一定の水準で落ち着いてきたとみることもできるでしょう。

SG

問	テーマ	難易度
1	EC サイトのセキュリティ改善	A
2	アカウント乗っ取りのインシデント対応	B
3	業務委託におけるセキュリティ	B

注）難易度は 3 段階評価で，C が難，A が易を意味する。

4. 今後の対策

4.1 午前対策

出題バランスは従来と大きく変わっていませんので，基本的な対策学習方針を変える必要はないでしょう。各分野ごとにバランスよく知識を入れておくことが重要です。

過去問題の流用が占める割合が確実に大きくなってきていますので，過去の SG 試験問題演習の重要性が大きくなります。できれば全世代(平成 28 年春～)に目を通しておくのが望ましいでしょう。

●情報セキュリティ管理について

過去問題でよく取り上げられているガイドラインについて，できるだけ目を通しておくようにしましょう。可能であれば以下の文献は一通り眺めておきたいところです。

JIS Q 27000 / 27001 / 27002
組織における内部不正防止ガイドライン
サイバーセキュリティ経営ガイドライン
中小企業の情報セキュリティ対策ガイドライン

●各種脅威と対策について

サイバー攻撃や各種脆弱性について各用語の意味を整理し，それらに対して「何には何が有効か」という対策をイメージできるようにしておきましょう。

インターネット関連の技術的に踏み込んだ出題も増えてきています。IT 技術に苦手意識が無い人は，各攻撃・対策を実現するロジックについても触れ，事例問題にも対応できるようにしておくとよいでしょう。

●情報セキュリティ技術

暗号化技術と PKI(公開鍵基盤)の基本的な理論を最優先で理解するようにしましょう。比較的問われる内容が予測しやすい部分なので，しっかり対策して効果的に得点したいところです。

●法務について

「サイバーセキュリティ基本法」などのセキュリティ関連法規，知的財産権関連(著作権，不正競争防止法)，労働関連法規(派遣など)について概要を抑えておきましょう。

●その他分野について

出題数の多い “システム監査”と“サービスマネジメント”について，過去問演習を含めてしっかりと対策しましょう。テクノロジ系・ストラテジ系については基本的な用語知識をおさえ，得意な分野があればやや踏み込んで学習しておくという対応で問題ないと考えます。

4.2　午後対策

テーマとしては

・攻撃や内部不正のリスク分析と計画，その評価

・インシデントへの初動対応や原因究明，再発防止

・ファイルなど情報資産へのアクセス制御や管理運用

などいくつかが考えられますので，どれが出題されても慌てることのないよう，広くカバーする学習を行うのがよいでしょう。そのためにはまず過去問題の演習を一定量行うことが大事です。いずれもよく練られた事例ですので，演習を重ねて論点を確認することで，穴の少ない対策が行えます。最近のものだけでなく，できれば過去の出題全て(平成 28 年春～)に目を通しておきたいところです。各問題で共通する視点としては，

・組織のセキュリティ方針を整理し，守られていない点や課題を探す

・各方針や対策によって避けられるリスク，残るリスクを考える

・複数の組織が登場した場合に，それぞれの状況を混同せずに整理する

といったものが挙げられます。これらに留意しながら，提示された条件を読み解く訓練を地道に重ねていくことが重要です。

加えて，教材(講座テキストなど)や IPA 発行のガイドラインで紹介されている事例，ニュース記事などに触れておくと非常に参考になります。特に IPA 発行の各種ガイドラインは，具体的な手口や脆弱性が多く整理されており，目を通しておくことで大きな効果が期待できます。

(参考 URL)

IPA 情報セキュリティ対策　https://www.ipa.go.jp/security/measures/index.html

情報セキュリティ対策支援サイト https://security-shien.ipa.go.jp/

また，内容面での対策とは別に「長文問題を読み解く」ことに慣れておくのもポイントです。過去問題の演習だけでなく，ガイドラインの事例やニュース記事などに目を通すときも「何がどうした」といった要旨を整理する癖をつけておくとよいでしょう。それらの訓練が，本番で長文問題を素早く読み解く効果につながってきます。

問題演習の際には，目標時間内に最大限の効果(正答率)が得られるよう，たとえば

・最初の 10 分で，問題文を眺めて概要を把握する

・次の 10 分で，前半の設問に取り組む

・最後の 10 分で，後半の設問及び見直し

といったように自分に合った時間配分のイメージを作り，鍛錬を重ねていくことが望まれます。

以上のような要素を組み合わせて学習することにより，効果的に合格点を獲得する対策が可能になると考えます。