情報セキュリティマネジメント

1.　はじめに

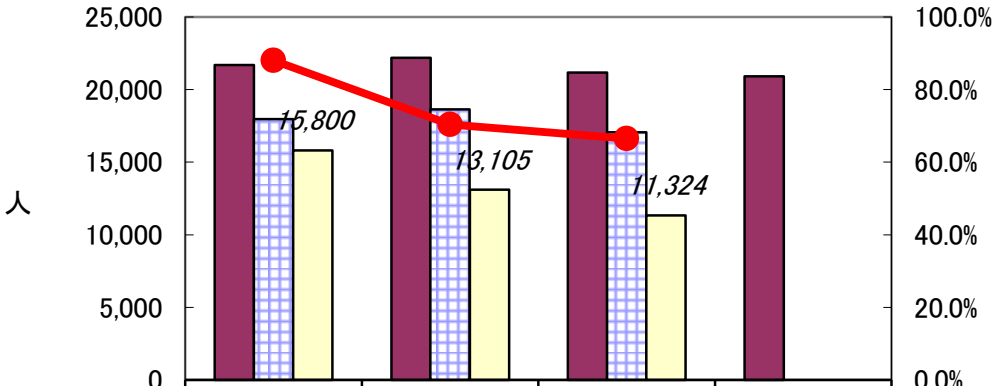
1.1　総評

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。

午前試験でガイドライン関連のやや難解な問題が多く出題された一方，午後試験は「時間をしっかり配分すれば解ける」部分が前回よりも多かった印象です。トータルで考えると，全体的な難易度は前回と同程度と評価できます。

1.2　受験者数

IPA から発表された応募者数は 20,907 人で，前年度の H28 年秋と比較するとやや減少です。しかし，前年が試験実施の初年度であったことや，リピート率が低い試験であろうことを考慮すると，一概に減少傾向ともいえないでしょう。情報セキュリティ管理の必要性に対する認識は高まっていくでしょうから，今後の推移に注目です。



	H28春	H28秋	H29春	H29秋
応募者数	21,691	22,186	21,162	20,907
受験者数	17,959	18,630	17,045	
合格者数	15,800	13,105	11,324	
合格率	88.0%	70.3%	66.4%	

2. 午前問題の分析

全 50 問は大きく分けて次の四つのブロックに分類できます。ブロックごとの出題数のバランスは基本的に従来と同様ですが，ISMS に関する部分がやや増え，技術的な要素に関する部分がやや減少しました。

・問 1～15：組織の ISMS に関する出題 （前回からの増減：＋３）

JIS Q 27001 や JIS Q 31000,“サイバーセキュリティ経営ガイドライン”など，標準的なガイドラインに拠った出題が多く含まれている傾向が継続しています。

新規出題用語：CRYPTREC，サポートユーティリティ，DLP など

・問 16～30：技術的な要素に関する出題 （前回からの増減：－３）

前回同様，突出したテーマはなく，攻撃方法や対策，認証方法など各知識が満遍なく問われている印象です。

新規出題用語：シャドーIT，C&C サーバ，ファジング など

・問 31～36：法務に関する出題 （前回からの増減：＋１）

セキュリティ関連の法規としては，個人情報保護法，特定電子メール法について出題されました。その他は売買契約や著作権法など，知的財産・労働などに関する標準的な問題が並んでいます。

新規出題用語：オプトインとオプトアウト など

・問 37～50：その他の分野に関する出題 （前回からの増減：－１）

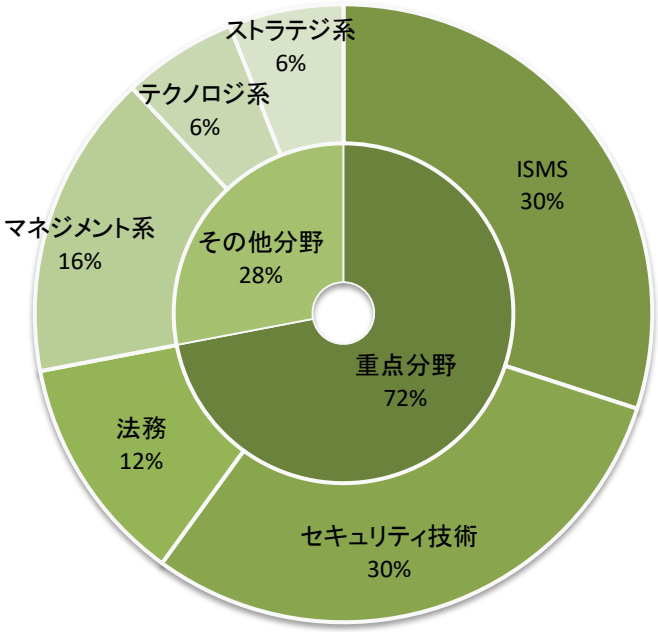
出題バランスは以下のようになっており，ほぼ従来どおりでした。

・マネジメント系は前回と同様 8 問，うちシステム監査が 4 問

・テクノロジ系やストラテジ系が各分野ごとにほぼ 1 問ずつ

新規出題用語：ビッグデータ(三つの V) など

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
	ISMS(情報セキュリティマネジメントシステム)	30 %	15
	セキュリティ技術	30 %	15
	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 25 問程度で，平均並みと言えるでしょう。ISMS 関連では新作が多く，技術的な要素やその他分野については流用が多いという傾向も継続しています。

難易度については，今までの「回を追うごとに少しずつ上昇」という傾向がまだ続いている印象です。前回同様，過去問題の演習のみで頻出用語を覚えていれば答えられる，という単純な問題は少なく，

・JIS Q 27001 などのガイドラインの内容をしっかり押さえておかないと答えづらい問題

・DLP，シャドーIT などの，FE 試験でもそれほど頻出ではない用語知識が求められる問題

の割合が多めになっています。特に，問 1～15 の ISMS に関する部分で，JIS Q 27000 シリーズで登場する用語や概念についてかなり多くの問題が出題されました。

問 37 以降の「その他分野」については，基本的には平易なものがほとんどです。ただしデータベース分野ではビッグデータ関連で新規の問題が登場しています。前回もネットワーク分野で HTTP ステータスについて問われたように，今後も数問程度は利用者視点での見慣れない問題が出てくるのではないかと推測できます。

問	テーマ	難易度
1	サイバーセキュリティ経営ガイドライン	B
2	JIS Q 27001 の要求事項と管理策	C
3	CSIRT	B
4	CRYPTREC	C
5	リスク特定	C
6	リスクファイナンシング	A
7	リスク受容可否の判断	B
8	リスク運用管理の責任主体	C
9	脅威と脆弱性	C
10	不適合原因の除去	B
11	否認防止	B
12	サポートユーティリティ	C
13	組織内の情報漏えい対策	C
14	SIEM	B
15	入退室管理	B
16	シャドーIT	C
17	ステガノグラフィ	B
18	パスワード認証	B
19	無線 LAN のアクセス制御	B
20	WAF	A
21	C&C サーバ	B
22	DNS キャッシュポイズニング	B
23	暗号アルゴリズム	A
24	ディジタル署名	A
25	データベースのアクセス制御	B

26	ルート認証局	B
27	トロイの木馬とワーム	A
28	公開鍵暗号方式	A
29	HTTPS	B
30	ファジング	B
31	個人情報保護法	B
32	特定電子メール法	C
33	著作権法	A
34	知的財産権	B
35	ソフトウェアライセンス	B
36	労働者派遣	C
37	スプレッドシートの正確性統制	B
38	入出金システムのコントロール	C
39	システム監査の目的	A
40	監査調書	A
41	PDCA	A
42	SLA と稼働率	B
43	逓減課金	B
44	ガントチャート	A
45	システム信頼性指標	B
46	ビッグデータ	C
47	NAT	A
48	業務プロセス改善	B
49	企画プロセス	A
50	CIO	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：リスクアセスメント

各種情報資産のCIAについて脅威，脆弱性を考慮した分析（重要度の算出）を行うとともに，各リスクへの対策を考察する問題です。“重要度×脅威×脆弱性”というリスク値の計算や，PCの紛失によってどんなリスクが発生するかなどが問われています。

問2：Webサービスの開発委託

Webアプリへの攻撃の分類と対策，開発委託時の留意点などについて考察する問題です。SG受験者にとっては見慣れないであろう名称のものも含めて攻撃手法が多数登場しますが，SQLインジェクションなどのポピュラーなものについて概要を理解していれば，多くの空欄は埋められるようになっています。また，パスワード運用についても問われます。

問3：スマートデバイスの業務利用

モバイル環境でスマートフォン等を活用する際のリスクと対策について考察する問題です。図が提示されていないため，ふだんモバイルワークについてあまり馴染みのない人はイメージがしづらかったかもしれません。内容自体は，紛失時のリモート操作など，定番といえるもので構成されています。

今回はインシデントへの事後対応に関する内容は少なく，事前のリスク分析及び対応策の考察に関する内容が割合として多くなっています。これまでの経緯をみると，特に全体的なバランスは固定せず，毎期ごとに様々なバランスの出題を試行しているという見方もできます。

内容としては，「技術的な知識はさほど要求されず，セキュリティマネジメントの原則が理解できていれば十分に解答が可能」な部分が大半を占めています。前回の一部設問のように，かなり深い用語知識や論理的な考察が求められる場面もそれほど多くありません(問2で数か所ある程度)。スキルのレベルという視点では，前回よりもやや下がり，昨年程度の水準に戻った印象を受けます。

その代わり，どの設問も問題文で提示された状況設定をしっかり読み解き，目的と手段の対応などを考察していかないと答えが出ないようになっています。上記の「スキルレベル的には難しくない」という評価の裏返しとして，「知識だけで素早く答えられる設問が少ない」という見方もできるでしょう。

時間的な負担の視点からページ数を比較してみると，

問 1：15 ページ　(問題文 7 ページ半，設問 8 ページ)

問 2：12 ページ　(問題文 6 ページ，設問 6 ページ)

問 3：12 ページ　(問題文 6 ページ，設問 6 ページ)

のようになっていました。設問のページ数はレイアウトにもよるので一概に何パーセント増したとは言えませんが，従来は 1 問当たり 10 ページ程度が標準的でしたので，かなり増えた印象を受けます。実際に受験していても，時間が足りないと感じた方は多かったのではないでしょうか。

特に問 1 は全部で 15 ページとなっており，小問の数も多かったため，ここで大きく時間を使ってしまうと残りの問題にも影響が出てしまうリスクがありました。

以上を総合し，午後試験の全体的な難易度としては，前回と同様，もしくはやや下がったと評価します。時間配分をしっかりできたかどうかが一つの鍵となったでしょう。

問	テーマ	難易度
1	情報セキュリティリスクアセスメント	B
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	B
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	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。傾向を考慮すると，一般的な情報セキュリティ技術の習得だけで安心するのではなく，規格などのガイドラインにしっかり目を通しておくことの重要性が高くなっているといえます。

●重点分野(情報セキュリティ，及び法務)について

情報セキュリティについてはシラバスに記載されている用語例を中心に，基本的な概念をしっかり把握しましょう。特に

・JIS Q 27001，JIS Q 31000，IPA 資料などの各種ガイドライン
・各攻撃手法とその対策
・認証技術

については重点テーマとして，しっかり学習することが重要です。特に JIS Q 27000 シリーズや JIS Q 31000 における，リスク関連の用語概念については注意が必要となるでしょう。

法務については，従来どおり

・個人情報保護法などのセキュリティ関連法規
・知的財産権関連法規(著作権，産業財産権，不正競争防止法)
・労働関連法規

について概要を押さえておくようにしましょう。

●その他分野について

まず，重点テーマである “システム監査”と“サービスマネジメント”についてしっかりと対策学習の時間をとり，基本的な考え方を理解しておくのがよいでしょう。特にシステム監査については，情報セキュリティ監査の概念を中心に，基礎をしっかり把握しておく必要があります。

残りのテクノロジ系・ストラテジ系の分野については,「分野ごとに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」という従来の対応で問題ないと考えます。

面倒な計算を伴ったり，複雑なデータの読み取りを要求する問題はそれほど多くは出題されないと推測できます。合格点の獲得に大きな影響はないので，それらの演習で大きく時間を費やすよりは，その時間を用語などの基礎知識の習得に振り分けたほうが得策となるでしょう。

4.2　午後対策

重点テーマが

・インシデント対応から対策までの流れ

・アクセス制御や管理運用

・リスク分析と計画，その評価

といった内容であることは従来と変わりません。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。

インシデント対応・対策については，教材(講座テキストなど)や IPA が発行しているガイドラインで紹介されている想定事例や，実際のインシデント事例を紹介するニュース記事・文献などに触れておくと非常に参考になります。

アクセス制御や管理運用については，「更新と承認の権限を分ける」「効果的なパスワード管理」などの基本的な考え方を，教材(講座テキストなど)でしっかり身に付けておきましょう。事例を扱った問題演習で具体的な適用のイメージをつかむことも重要です。

リスク分析については，「紛失の場合はどんなリスクがあるか」といったように，インシデントの種類に応じたリスク考察と対応をしっかり整理できるようにしておきましょう。

また，上記のような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。

・過去の IP 試験の中問

・FE 試験や AP 試験のマネジメント系の午後問題

など，類似したタイプの事例問題をしっかりと演習しておきたいところです。

特に今回のようなボリュームの大きい場合を想定すると，1 問ごとの時間配分がかなり大事になります。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。