情報セキュリティマネジメント

1.　はじめに

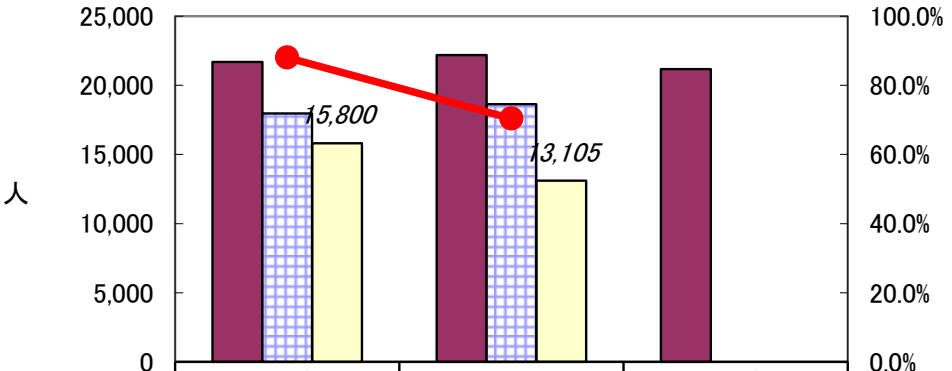
1.1　総評

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。

ただし，深い知識が必要とされる問題(設問)の割合が，従来よりもやや増している印象です。過去問題の傾向をふまえた対策で十分合格には到達できますが，全体的な難易度は午前・午後ともに若干上がっているのではないかと評価できます。

1.2　受験者数

3 月に IPA から発表された応募者数は 21,162 人で，前年度の H28 年春とほぼ同等(微減)です。前回及び前々回の合格率が高くリピート受験者がそれほど多くないことを考えると，十分に社会の関心を維持していると評価できそうです。



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

2. 午前問題の分析

2.1 出題テーマの特徴

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，±1 程度の誤差はありますが，前回及び前々回とほぼ同様でした。

・問 1～12：組織の ISMS に関する出題 （前回からの増減：＋１）

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：CSIRT マテリアル，RPO，リスクレベル など

・問 13～30：技術的な要素に関する出題 （前回からの増減：－１）

前回までは攻撃手法の特徴に関する問題が多い構成でしたが，今回はそれほど突出したテーマはなく，対策や認証方法などの理解も含めて各知識が満遍なく問われている印象です。

新規出題用語：NIDS，CRL，PCI DSS など

・問 31～35：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電子署名法が登場しました。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：電子署名法，36 協定 など

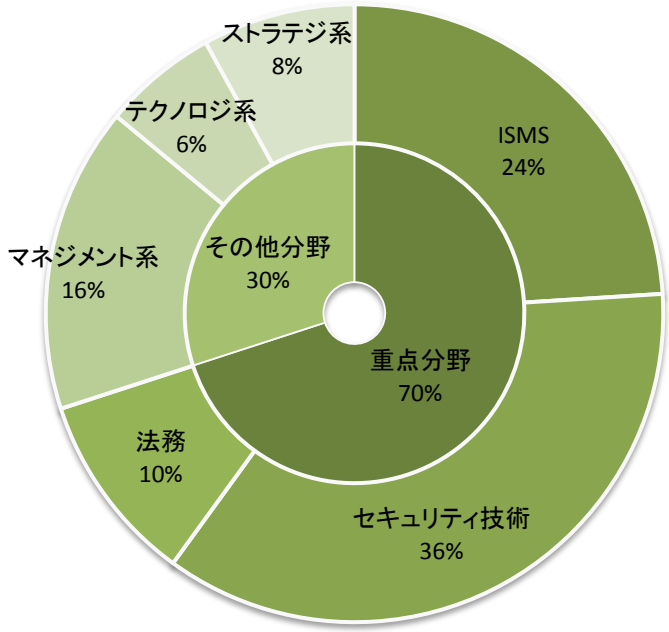
・問 36～50：その他の分野に関する出題 （前回からの増減：＋１）

マネジメント系は前回と同様 8 問出題されており，その他分野の中で重点的な位置づけを確保しています。その中でシステム監査が 4 問と，大きな重みをもつことも変わっていません。リスクコントロールはセキュリティの視点から重要なため，SG 試験としてはこの部分を重視するのは当然と考えられます。

テクノロジ系やストラテジ系が各分野ごとにほぼ 1 問ずつの出題となっていることも，従来と同様です。

新規出題用語：OLA，HTTP ステータスコード 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）		70 %	35
	ISMS(情報セキュリティマネジメントシステム)	24 %	12
	セキュリティ技術	36 %	18
	法務	10 %	5
その他分野		30 %	15
	マネジメント系	16 %	8
	テクノロジ系	6 %	3
	ストラテジ系	8 %	4



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 28 問程度で，前回(25 問程度)から見ると微増しています。ただし単純な流用ではなく，問題文の一部や選択肢を改変しているものも多く含まれていました。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は継続しています。

2.2 難易度の特徴

難易度については，前々回 → 前回 → 今回と少しずつ上昇してきた印象です。攻撃手法などの頻出用語を覚えていれば答えられる，という単純な問題がやや減少し，

・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

・RPO，NIDS，CRL 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

の割合が若干増えてきています。その他分野でも，HTTP ステータスの問題のように，利用者の視点から掘り下げて「FE 試験でもあまり問われていないような知識」について問う問題も散見されるようになってきました。

「FE 試験の対策に相当する水準の学習を進めていれば十分に合格点を獲得できる」という基本的な評価は変わりませんが，合格をより確実にする(高得点を見込む)ためには，AP 試験や SC 試験で用語問題として問われているような，やや高度な内容についても触れておくとより望ましい，という見方もできます。

2.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	ISMS のリーダーシップ（JIS Q 27001）	B
2	サイバーセキュリティ経営ガイドライン	B
3	JPCERT/CC のコンテンツ	C
4	RPO	B
5	リスクマネジメントの原則（JIS Q 31000）	B
6	リスクマネジメントの活動順序（JIS Q 31000）	B
7	リスクレベル	C
8	委託時のインシデント対応	B
9	暗号の危殆化	B
10	タイムスタンプサービス	B
11	組織労働者の認識 （JIS Q 27001）	B
12	JVN	C
13	ネットワーク型 IDS	B
14	内部不正による漏えい発見対策	B
15	ディジタルフォレンジックス	A
16	パスワード取得攻撃と対策	B
17	ファイアウォールとセグメント分割	B
18	2 要素認証	B
19	ディジタル証明書	A
20	ハッシュ関数	B
21	ソーシャルエンジニアリング	A
22	ディジタル署名の使用鍵	A

23	ディレクトリトラバーサル	B
24	真正性と信頼性（JIS Q 27000）	C
25	ディジタル証明書の失効	B
26	クレジットカードのセキュリティ技術	B
27	不正のトライアングル	B
28	ネットワーク層のセキュリティプロトコル	B
29	WAF のブラックリストとホワイトリスト	C
30	ポートスキャナ	B
31	電子署名法	B
32	売買契約	C
33	不正競争防止法	A
34	著作権法	A
35	労働基準法	C
36	特権 ID の使用統制	B
37	システムテストの監査	B
38	被監査部門との意見交換	B
39	障害管理の監査	B
40	運用テスト	B
41	運用レベル合意書(OLA)	C
42	問題管理	A
43	アローダイアグラム	B
44	ホットスタンバイ	B
45	ビッグデータ分析	A
46	HTTP ステータスコード	C
47	情報戦略立案	B
48	業務プロセスの再設計	B
49	非機能要件	B
50	BCP	A

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

3.1 問題テーマの特徴

午後問題3問の内容は次のようなものでした。

問1：マルウェア感染への対応

ランサムウェアに感染した事例を用いて，調査分析の考え方や企業としての対応について考察する問題です。当該マルウェアの基本的な特徴だけではなく，そこからの金銭授受の方法(Tor など)についても問われるなど，かなり掘り下げた内容も含まれていました。

問2：クラウドサービスの導入と運用

メール送受信に関するクラウドサービスの導入事例を用いて，外部サービス利用時のセキュリティ面での留意点，及び当該サービスにおけるアクセス制御(アクセス権設定)について考察する問題です。アクセス制御は定番テーマと言える内容なので，予想の範囲内の問題と言えます。

問3：オフィスの物理的セキュリティ

オフィスレイアウトの変更を題材に，機密性の確保手段や共連れ対策，施錠方式などを考察する問題です。日常業務に密接する内容であり，管理者経験のない受験者でも身近な話題として取り組みやすいテーマであったのではと考えます。

前回は「インシデントの初動対応から調査・対策まで」という一連のストーリーを追う問題が揃っていましたが，それと比較すると，インシデント対応が主題の問題や，リスク分析などの計画を主題にした問題などがミックスされ，全体としてはバラエティに富んだ構成になっていた印象です。

3.2 難易度の特徴

前回と同様，基本的には「技術的(テクニカル)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提示された内容を使って十分に解答が可能」な部分が大半を占めています。

ただし，一部の設問では

- ランサムウェアの金銭授受の手法(Tor など)
- アンチパスバックという共連れ対策の考え方
- シリンダ錠などの各種施錠技術の比較

など，しっかりした知識と論理的な考察を必要とするものがあり，求められるスキルの

レベルは前回よりも上がった印象を受けます。″Tor(匿名ネットワーク)″や″アンチパスバック″などは，FE 試験でもあまり問われていない知識です。「一つのテーマ（今回であれば，ランサムウェアやオフィス入退室)に対する理解がないと点を落としやすい」という意味では，前回よりも前々回(H28 年春)の問題セットに近い性格をもっているとも言えます。

時間的な負担の視点からページ数を比較してみると，

問 1：10 ページ （問題文 4 ページ半，設問 5 ページ半)

問 2：10 ページ （問題文 6 ページ，設問 4 ページ)

問 3：10 ページ （問題文 6 ページ，設問 4 ページ)

のようになっており，ほぼ従来どおりのボリュームとなっていました。各問とも情報量は従来どおり多めですが，今回は各設問の内容から「問題文のうち，どの部分の記述を重点的に読み返して考察すればよいか」が比較的分かりやすくなっており，どこを読み込めばよいのか迷う場面はあまり出ません。このため，解答に要する時間は前回よりも少なく済み，時間切れで得られるはずの得点を失った人は少ないのではないかと推定します。

以上を総合し，全体的な難易度としては，前回並みか，やや上がったと評価します。過去問題の演習だけでなく，IPA の資料などにしっかりと目を通した上で，最新の現場セキュリティ事情に関する情報を収集していないと，高得点は難しかったでしょう。

3.3 問題テーマ難易度一覧表

問	テーマ	難易度
1	マルウェア感染への対応	C
2	クラウドサービスの導入と運用	B
3	オフィスの物理的セキュリティ	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，基本的な学習方針を変える必要はないでしょう。ただし難易度の推移を考慮した場合，過去試験の合格水準で満足するのではなく，獲得する知識量の目標をより高くとっておくのがベターといえます。

●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 27001，31000，IPA の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。ガイドラインについては過去問題の演習だけでなく，一通り目を通しておくことで新規出題にも対応しやすくなります。

法務については，

・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

について概要を抑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，範囲も広いので，分野ごとに基本的な用語知識などをおさえておけば十分かと考えられます。得意な分野があれば，やや踏み込んだ応用知識について学習するのもよいでしょう。

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

これまでの傾向をふまえると

・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

といった内容が重点テーマと言えますので，これらの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，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。

アクセス制御やリスク分析については，「更新と承認の権限を分ける」「優先度や脅威の内容ごとに対策を立てる」などの基本的な考え方が理解できているかどうかが一番のポイントになります。教材(講座テキストなど)でしっかり考え方を身につけるとともに，事例を扱った問題演習で具体的な適用のイメージがつかめるようになっておくとよいでしょう。

さらに，今回のランサムウェアの金銭授受技術に見られるように，一部の要素についてはかなり踏み込んだ設問が登場することも予想されます。現場で遭遇しがちなインシデントについては，基本教材を眺めるだけでなく，事例集やニュース記事など，幅広くアンテナを張って情報収集に努めるのが望ましいといえます。

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。10 ページ前後の問題文を落ち着いて読解・整理する能力が非常に重要になりますので，

・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。その際，1 問ごとの時間配分にも気を配り，目標時間内に最大限の効果(正答率)が得られるような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。