情報セキュリティマネジメント

1.　はじめに

1.1　総評

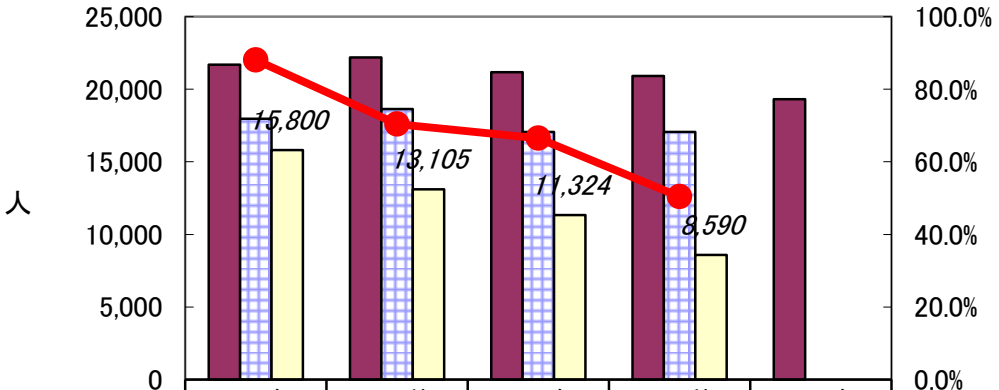
求められる知識・スキルの内容に大きな変化はなく，現場での運用を意識した内容が揃っていると評価できます。午後問題の全体的な構成も従来とさほど変わりません。

合格率の下がった前回（H29 秋）と比較すると，午前はほぼ同等，午後は同様～やや難と評価でき，受験者には同程度以上の水準が求められているかと評価できます。

1.2　受験者数

応募者数は 19,300 人で，前年春や前回と比べるとやや減少しています。

合格率は低下傾向が続いており，前回(H29 秋)の時点で 50%程度まで低下しました。試験の位置づけを考慮するとむしろこの水準が妥当(今までが高かった)とも言えますが，今後の推移に注目です。



	H28春	H28秋	H29春	H29秋	H30春
応募者数	21,691	22,186	21,162	20,907	19,300
受験者数	17,959	18,630	17,045	17,039	
合格者数	15,800	13,105	11,324	8,590	
合格率	88.0%	70.3%	66.4%	50.4%	

2. 午前問題の分析

全 50 問の内訳については，今回は以下のような枠組みでとらえてみました。問 1～30 の部分は前半 15 問程度を組織の ISMS に関する問題，後半 15 問程度を技術的な問題として大きく 2 ブロックに捉えることも可能ですが,問 9～問 23 の部分でマネジメント(ISMS)的な視点の問題と技術的な視点の問題がアトランダムに混在しており,明確な区分けがしづらい状況です。

全体的なテーマごとの出題数バランスは基本的に従来と同様といえます。

・問 1～8：情報セキュリティ管理

JIS Q 27001 や JIS Q 31000,“組織における内部不正防止ガイドライン”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：情報セキュリティ事象など

・問 9～23：各種脅威とその対策

各種攻撃の特徴やそれらに対する対策について，満遍なく問われています。特にネットワークにおける脅威・対策に関する言葉が多く登場しています。

新規出題用語：セキュリティバイデザイン，ドメイン名ハイジャックなど

・問 24～30：情報セキュリティ技術

暗号化技術と PKI(公開鍵基盤)に関するテクニカルな知識が，およそ半々の割合で問われています。

新規出題用語：リスクベース認証など

・問 31～36：法務に関する出題

セキュリティ関連の法規としては，サイバーセキュリティ基本法，刑法，個人情報保護法について出題されました。その他は知的財産権について 2 問，労働関連で 1 問が出題されました。

新規出題用語：要配慮個人情報 など

・問 37～50：その他の分野に関する出題

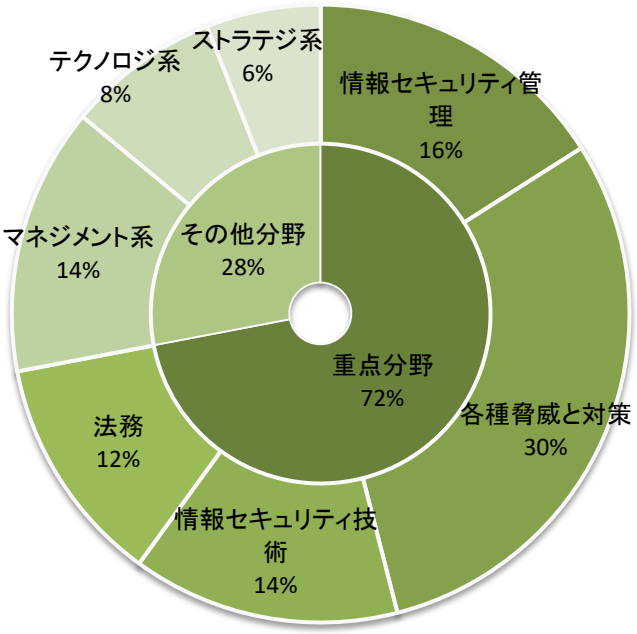
出題バランスは以下のようになっており，従来の形を踏襲しています。

・マネジメント系は前回から 1 問減って 7 問，うちシステム監査が 4～5 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：コントロールトータルチェック，PaaS 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
	情報セキュリティ管理	16 %	8
	各種脅威と対策	30 %	15
	情報セキュリティ技術	14 %	7
	法務	12 %	6
その他分野		28 %	14
	マネジメント系	14 %	7
	テクノロジ系	8 %	4
	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，平均並みまたはやや少なめと言えるでしょう。SG試験からの流用はまだ数問で，FE試験からの流用が多くなっています。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。

「SG 過去問題の演習のみで答えられるような単純な問題ばかりではない」という傾向は，継続しています。問 1～8 の部分は JIS Q 27001 などのガイドラインの内容をしっかり抑えておかないと答えづらい問題が並んでいました。

新規に登場した用語は前回よりも少なめですが，その代わり既出の概念に関する問題の内容が深化している部分が散見されます。たとえば SPF という言葉については，H28 秋の出題では「送信元の認証」という利用目的さえ理解していれば正解できましたが，今回は「ドメイン情報とサーバの IP アドレスを照合する」という具体的な認証手順を理解していないと正解できない問題になっています。

問 37 以降の「その他分野」については前回の分析における予測どおり，「数問程度は見慣れない問題が出てくる」という結果になりました。(問 45 の PaaS，問 47 の SMTP の処理など)

午前試験全体の難易度については，一部新規出題部分などの難易度が高い反面，定番部分は平易に答えられるものが多いことで相殺され，前回と同様あるいは微増になっていると評価します。

問	テーマ	難易度
1	サイバーレスキュー隊	B
2	リスクの回避	A
3	リスク評価	C
4	退職従業員の不正対策	B
5	情報セキュリティ事象	C
6	情報資産の機密性	B
7	特権的アクセス権	B
8	情報セキュリティの性質	B
9	LAN アナライザの利用	B
10	SPF	C
11	UPS	A
12	WAF	A
13	サーバ侵入対策	B
14	セキュリティバイデザイン	C
15	クラウドサービスのパスワード管理	B
16	ワーム検知方式	C
17	セキュリティパッチ	A
18	パケットフィルタリング	C
19	サイバーセキュリティ戦略	B
20	ドメイン名ハイジャック	B
21	ドライブバイダウンロード	A
22	バイオメトリクス認証	B
23	マルウェアの動的解析	B

24	メッセージ改ざん検知	B
25	リスクベース認証	C
26	暗号の危殆化	B
27	ブルートフォース攻撃	A
28	電子メールの暗号化	A
29	ディジタル証明書	A
30	認証局	B
31	サイバーセキュリティ基本法	C
32	マルウェア関連法規	B
33	個人情報保護	C
34	著作権	B
35	不正競争防止法	A
36	労働者派遣	C
37	コントロール手法	C
38	内部監査の要求事項	B
39	監査証拠	A
40	被監査部門の行為	B
41	事業継続計画	B
42	サービスデスク	B
43	アローダイアグラム	B
44	RAID	C
45	PaaS	B
46	DBMS のトランザクション制御	A
47	SMTP	C
48	外部委託	B
49	CSR 調達	B
50	損益計算	C

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：個人情報の保護に関する法律への対応

顧客情報の取得と取扱いについて，法律の内容を考慮しながらPCの運用対策を立案する問題です。

法規における個人情報の定義や，入手時に目的を「明示」するといったような文言を把握できているかで，かなり点数が上下する問題でした。

加えて，後半の設問では匿名加工という処理への理解も求められ，取捨選択に迷う部分が多く存在していました。この部分でつまずき時間をとられ，問2や問3に影響が出てしまった受験者もいたのではないかと推測されます。

問2：内部不正事案への対応

具体的な内部不正の発生例を題材に，原因究明及び再発防止策の考察を行う問題です。

設問2では“不正のトライアングル”の3要素，設問3では内部不正防止ガイドラインにおける“人的管理”や“職場環境”といった概念が登場しており，予備知識のある人は解きやすかったでしょう。ただしそれらを知らずとも，一般常識を用いて問題文を読解すれば解くことは十分に可能でした。

難問が並んでいるわけではありませんが，論点があまり多岐にわたっておらず少ないため，どこか一つの論点を見誤ると大きく失点する可能性もあります。

問3：企業統合における情報セキュリティガバナンス

業務ツールの利用を主題材に，トップダウン及びボトムアップアプローチで統制の構築を行う問題です。

メール利用やPC管理という見慣れた題材を扱っており，設問に関する部分だけ見ればストーリーもそれほど複雑ではありません。ただし，“シャドーIT”や“ヒヤリハット”，“BIOS”や“トップダウンアプローチ”といったように，用語の知識がしっかりしていないと解きづらいものが多く含まれていました。また，ルールを表す図表部分の情報密度がやや高いため，読解力が不足している受験者は整理にとまどったかもしれません。

ボリュームについては，各問とも 10 ページ前後で，かなり多めだった前回と比較すると従来のボリューム水準に戻りました。ただし問 3 に顕著なように，問題文部分の記述密度が高めなため，単純に時間負荷が減ったとは言い切れない部分もあります。

前回(H29 秋)の試験がどちらかというと「知識はさほど要求されず，原則が理解できていればあとは読解力で解答が可能」な色が濃かったのに対し，今回は法規や各種用語などに関する基礎知識がないと答えづらい部分が多い印象です。特に問 1 は個人情報保護法や匿名加工に対するしっかりとした理解が求められる部分が多く，ここでつまずいてしまった受験者も多いのではと考えられます。その意味では，2 回前の H29 春試験に近い性格をもっていると評価できます。

以上を考慮し，午後試験の全体的な難易度は「やや難」と評価します。

問	テーマ	難易度
1	個人情報の保護に関する法律への対応	C
2	内部不正事案への対応	B
3	企業統合における情報セキュリティガバナンス	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。ガイドラインの定義，脅威と対策，暗号化などの基礎技術といった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。

●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。特に

JIS Q 27000 / 27001，JIS Q 31000
組織における内部不正ガイドライン
サイバーセキュリティ経営ガイドライン

については，今後もよく取り上げられることが予想されます。

●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，各用語の意味をしっかりと整理しておきましょう。また，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。技術的に踏み込んだ面が聞かれないとも限りませんので，余力があれば各攻撃・対策に関する技術的な仕組みについても触れておきましょう。

●情報セキュリティ技術

まずは，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。

●法務について

傾向は変わっていませんので，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(派遣など)」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

重点テーマが “システム監査”と“サービスマネジメント”であることは変わりませんので，ここをしっかりと対策しましょう。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。

4.2　午後対策

テーマとしては

・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

・攻撃や内部不正のリスク分析と計画，その評価

などが考えられ，次回にどの題材が出るかはまだまだ流動的で傾向が読みづらい部分があります。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。過去問題の蓄積もだいぶ増えてきましたので，まずは過去問題を一通り演習することで，穴の少ない対策が可能になるかと考えます。

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，現状でそれに反しているものを探す

・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。

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。

リスク分析については，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。“機密性”などの項目ごとに評点を付けていくスコアリングの考え方も良く出ますので，慣れておくとよいでしょう。

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。前述した SG 試験の過去問題はもちろんのこと，できれば

・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。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。