

## 令和元年秋期 情報処理安全確保支援士試験合格発表 分析コメントと今後の対策

(株) アイテック IT人材教育研究部 2019,12,20

10月20日(日)に行われた令和元年秋期の情報処理技術者試験について、応用情報技術者ほか高度系5試験の合格発表がありました。同時に発表された得点分布などの統計データの分析をもとに、情報処理安全確保支援士試験の合格発表コメントをお知らせします。

### ■情報処理安全確保支援士試験 (SC)

[令和元年秋期の情報処理安全確保支援士試験 統計情報]

応募者	21,237人
受験者	13,964人
合格者	2,703人
合格率	19.4%

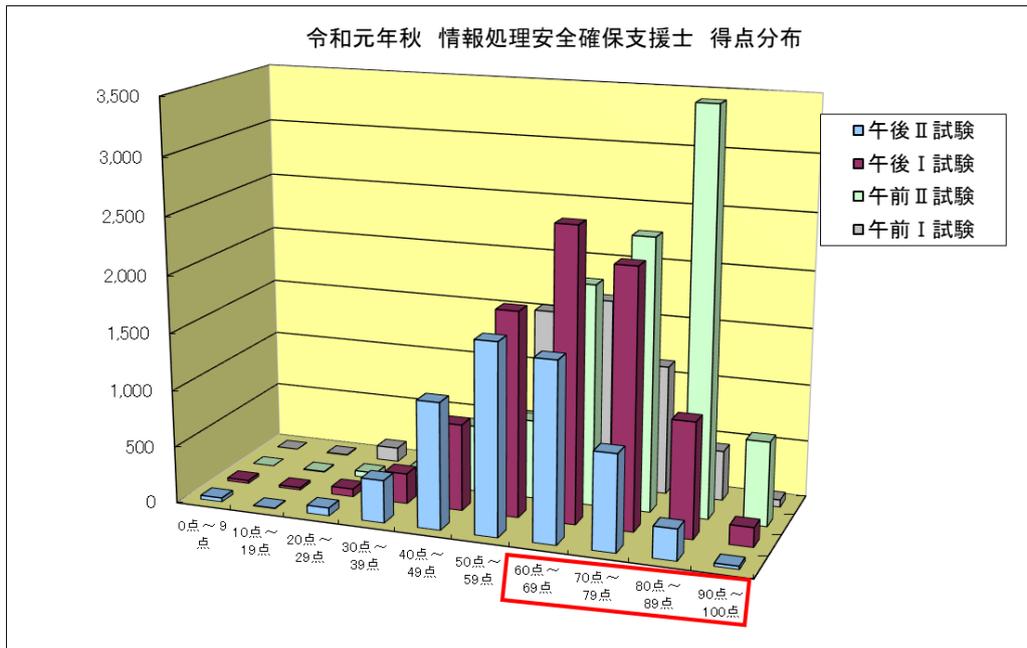
平成29年春期から始まった情報処理安全確保支援士試験は、内容的にこれまでの情報セキュリティスペシャリスト試験と変わらないものとして実施されています。今回の合格率は19.4%で、前回の18.9%より少し上がり、平成21年実施以降で最も高い合格率でした。

次に発表されたスコア分布の分析とグラフを示します。

(令和元年秋期 情報処理安全確保支援士試験 スコア分布)

得点	午前Ⅰ試験	午前Ⅱ試験	午後Ⅰ試験	午後Ⅱ試験	合格者
0点～9点	1	0	27	35	
10点～19点	5	6	22	5	
20点～29点	126	51	70	70	
30点～39点	394	132	267	373	
40点～49点	1,012	589	760	1,103	
50点～59点	1,536	696	1,789	1,663	
60点～69点	1,676	1,937	2,547	1,561	
70点～79点	1,140	2,380	2,250	841	
80点～89点	440	4,094	1,007	273	
90点～100点	64	737	171	28	
計	6,394	10,622	8,910	5,952	2,703
対前試験比率		166.1%	83.9%	66.8%	45.4%
午前Ⅰ免除者(概数)	7,570	54.2%			

合格者数	2,703	採点者数の割合	合格者数との差
午前Ⅰ60点以上合計	3,320	51.9%	617
午前Ⅱ60点以上合計	9,148	86.1%	6,445
午後Ⅰ60点以上合計	5,975	67.1%	3,272
午後Ⅱ60点以上合計	2,703	45.4%	0



午前Ⅰ試験免除対象の人も増えてきましたが、得点分布を分析してみると、今回午前Ⅰ試験の免除者は概算で7,570人(54.2%)おり、受験者の半数の人が午前Ⅱからの受験となっています。この午前Ⅰ試験で基準点60点以上取ることができた人は3,320人(受験者の51.9%)でした。

午前Ⅱ試験で基準点以上の人は9,148人(受験者の86.1%)で、前回の79.8%からかなり増加しました。過去問題が基本的な内容で、得点の伸びた人が多かったと思われます。

午後Ⅰで基準点(60点)以上取れた人は67.1%で、前回の53.8%からかなり増えています。

午後Ⅱで基準点(60点)以上取れた人は45.4%で、こちらは前回の59.1%からかなり減少しています。

## ■令和元年秋期 情報処理安全確保支援士試験の出題内容について

### (午前Ⅰ試験(高度試験の共通知識問題))

高度試験に共通して出される問題30問は、従来どおり、すべて応用情報技術者試験(AP)から選ばれていて、テクノロジー系17問(57%)、マネジメント系5問(17%)、ストラテジ系8問(26%)という出題比率です。

問題内容は、文章問題は21問(前回17問から増)、用語問題は1問(前回3問から減)、計算問題が5問(前回3問から増)、考察問題が3問(前回7問から減)でした。これらは毎回増減があります。

- ・問題は出題範囲からほぼまんべんなく出題されますが、今回は、ヒューマンインタフェース、マルチメディア、技術戦略マネジメントなどからの出題はありませんでした。
- ・過去問題が毎回約7割ありますが従来よりもやや難問題が選ばれていたといえます。また、これまで出題されたことがない内容の新傾向問題が増え、全体としてやや難の試験だったと思われます。
- ・重点的に出題されるセキュリティ分野の出題数は前回と同じ4問でした。
- ・新傾向問題は次の6問で、これまで平均4問程度なので多く出題されたといえます。

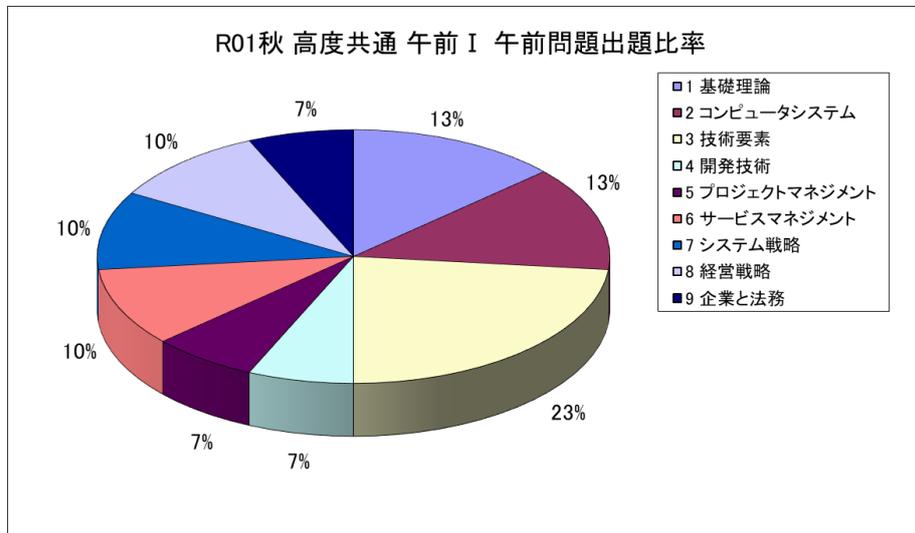
### (新傾向問題)

問3 AIの機械学習における教師なし学習

問11 フォワードプロキシの説明

- 問 18 PMO の役割の説明
- 問 22 システム監査手続で利用する技法
- 問 25 ファウンドリサービスの説明
- 問 28 RPA の説明

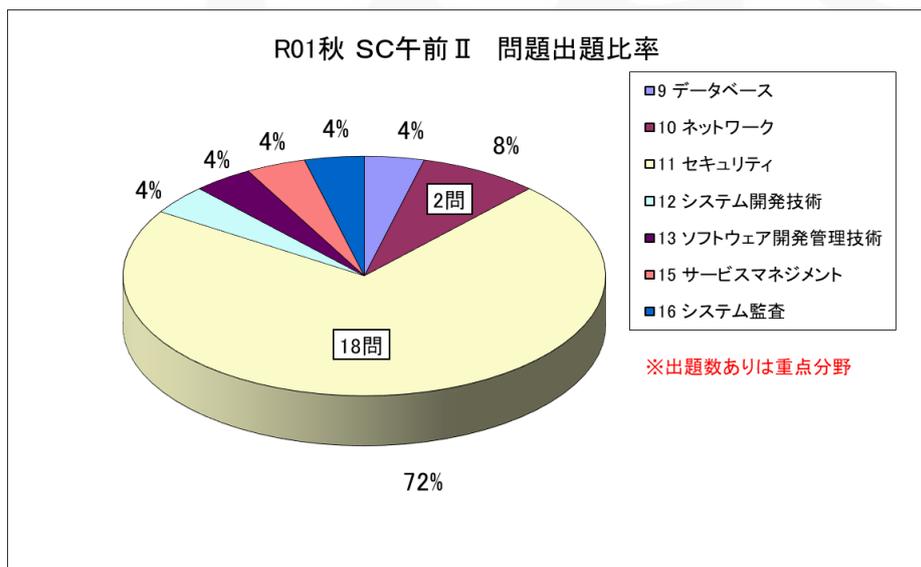
令和元年秋期の高度試験共通 午前 I 問題出題比率



(午前 II 試験 (専門知識問題))

午前 II 試験は基本的な問題が多く、セキュリティとネットワークの専門知識の出題数はそれぞれ 18 問と 2 問の合計 20 問でした。前回試験と比べて新傾向問題が増えています。過去問題は従来と同じで 7 割弱ありました。

令和元年秋期の情報処理安全確保支援士試験 午前 II 問題出題比率



過去の情報処理安全確保支援士試験問題の出題は 13 問ありました (前回 15 問)。この中で平成 30 年春期の問題が 6 問と最も多く出題されていました。新傾向問題といえる問題は次の 7 問で、前回の 5 問と比べて増えています。情報処理安全確保支援士試験の対策として、専門分野の

セキュリティについては、常に新しい技術を理解しておく必要があります。

- 問 1 FIDO UAF1.1 に基づく認証処理
- 問 10 BlueBorne の説明
- 問 14 常時 SSL/TLS のセキュリティ上の効果
- 問 15 専門知識がない攻撃者でも攻撃ができるもの
- 問 19 IP パケットの分割処理と再構築処理
- 問 21 JSON 形式で表現されるデータのデータベース格納方法
- 問 22 状態遷移図に追加すべき遷移

### 〔午後Ⅰ試験〕

・午後Ⅰ問題の出題テーマと設問概要は、次のとおりです。

今回の問 1 は電子メールのセキュリティに特化した技術要素の強い問題、問 2, 3 はマルウェア関連の問題で選択した人が多かったと予想されます。これまで定番の出題内容だった Web 関連セキュリティの内容がありませんでした。また、前回と比べて解答する小問数が増え、難易度は例年どおりといえます。

問 1 電子メールのセキュリティ対策（情報サービス事業者） 普通

送信ドメイン認証技術、SPF への対応状況、攻撃に対する効果、TXT レコード、DKIM 利用のシーケンス、DMARC のタグ、SPF 認証、デジタル署名の検証、DNS サーバ追加レコード、なりすまし方法

問 2 インシデント対応におけるサイバーセキュリティ情報の活用（金融事業会社） 普通

ネットワーク構成、FW のフィルタリングルール、構成機器、セキュリティ情報、攻撃の調査結果、C&C 通信への対策案、通信遮断理由、情報持出しの痕跡、共有すべき情報、証明書、攻撃種類

問 3 標的型攻撃への対応（ビッグデータ解析専門の調査会社） やや易～普通

標的型攻撃対策、システム概要、システム構成要素、インシデント対応手順、対応記録、マルウェアが実行したコマンド、対応手順の改善、マルウェアの活動、感染検知できない状態、感染の検知方法

### 〔午後Ⅱ試験〕

・午後Ⅱ問題の出題分野とテーマは次のとおりです。今回は偏りのないテーマで出題されました（前回は 2 問ともネットワークセキュリティの内容）。また、解答群付きの設問が従来よりも多かった問題でした。問 2 の方が問 1 と比べてやや易だったといえます。

問 1 ソフトウェア開発におけるセキュリティ対策（ネット広告事業者） 普通（11 ページ）

ネットワーク構成、サーバの FW ルール、フォレンジック調査、マルウェアの活動、ルートキットの動作、マルウェア対策、DevOps のセキュリティ向上策、システム変更手順、コンテナ技術活用

問 2 工場のセキュリティ（金属部品製造会社） 問 1 と比べるとやや易（13 ページ）

ネットワーク構成、セキュリティ規程、ランサムウェア感染、感染調査と対処、セキュリティの見直し、プロジェクトの進め方、APT 攻撃のステップ、工場の課題調査、課題解決案、見直し案の工場のネットワーク、安全なデータ転送の仕組み、評価結果、脆弱性管理のプロセス、規程の見直し

itec