

## ■ 全体講評

今回の公開模試における午後Ⅰ、午後Ⅱ試験の平均点は、午後Ⅰが 33.7 点、午後Ⅱが 28.9 点でした。問題別では、午後Ⅰの問 1 が 16.6 点、問 2 が 11.9 点、問 3 が 18.3 点、問 4 が 19.6 点で、問 2 の平均点が最も低くなりました。また、午後Ⅱは、問 1 が 25.5 点、問 2 が 31.4 点でした。2011 年春期の公開模試では、午後Ⅰの平均点が 45.4 点、午後Ⅱの平均点が 35.1 点であったことを考慮すると、午後Ⅰ、午後Ⅱともに、平均点が大きく低下したことになります。一部、問題の難度が高くなったこともあります。午後Ⅰ、午後Ⅱとも想定していた平均点を下回る結果になりました。

次に、採点結果から受けた印象としては、問題で記述された内容、あるいは設問で指示されていることにあまり従わず、各自が持ち合わせている知識や先入観などに基づいて解答を作成していると思われる答案が数多く見られました。問題の記述内容や設問の指示に従って答案を作成することが、合格するための絶対条件となります。本番の試験では、こうした事項については改善していく必要があると思います。特に、記述式の問題においては、それぞれの設問で求める解答は基本的に一つの内容を答えさせるように条件が付けられています。このため、主語と述語、あるいは目的語は何かなどを明確にした上で解答を作成するようにしましょう。また、問題によっては、設問で具体的に述べよと指示されている場合があります。こうしたケースで、例えば、必要最小限の範囲に対してだけ権限を与えるなどを解答しても、それでは具体的と見なされません。権限が与えられるべき範囲を問題の記述から導き出し、それを具体的に表現することが必要です。

次に、問題ごとの選択状況を紹介しておきます。午後Ⅰ試験は、4 問の中から 2 問を選択するので、平均的な選択率は 25% になります。今回は、問 1 (電子文書管理システムの導入) の選択者が 40.3%、問 2 (ホスティングサービスの提供) が 12.3%、問 3 (データベースの情報保護と運用) が 39.3%、問 4 (Web アプリケーションの脆弱性対策) が 8.1% であり、多くの受験者が問 1 と問 3 を選択していました。午後Ⅰ試験では、得意とする分野の問題を早く見極め、その問題で、できるだけ多くの点数をあげることが必要です。例えば、得意分野の問題で 40 点近くの点数を獲得できれば、もう一つの問題で 20 点強を得点するだけで、午後Ⅰ試験はクリアすることができます。しかし、このようなことが可能になるには、問題の記述内容を十分に把握できるだけの技術

力が、まず必要とされます。本番の試験日までの期間で、より一層のレベルアップを図るようにしましょう。

午後Ⅱ試験では、問 1 (ネットワークセキュリティ) の選択者が 40.5%、問 2 (Web アプリケーションの再構築) が 59.5% という比率でした。午後Ⅱ試験では、様々な分野から総合問題になることが多いので、できるだけ各自が得意とする分野から構成されている問題を選択するようにしましょう。また、試験センターでは「試験結果に問題の難易差が認められた場合には、基準点の変更を行うことがあります」としています。このため、午後Ⅱ試験においては、問 1 と問 2 の難易差をあまり気にせず、一度選択すると決めた問題を最後までやり遂げることが大切です。問題選択に迷ってしまうと、2 問ともに手をつけて、かえって失敗してしまいます。

午後Ⅰ、午後Ⅱ試験の記述式問題の多くは、問題文の中に解答を導くためのヒントが記述されています。一定の知識レベルに達していれば、問題文で記述された内容に基にして考えることによって正解を導き出すことができます。設問で問われていることを十分に確認し、問題の記述内容と照らし合わせながら解答を導いていく訓練をしておくとい良いでしょう。

試験当日は集中力、精神力、体力の勝負になります。必ず合格するという強い意志をもって、午後Ⅱ試験の最後まで全力を出し切り(あきらめず)問題に取り組んで、ぜひ合格を目指してください。

## <午後Ⅰ>

### 問1 電子文書管理システムの導入

#### 【採点基準】

##### [設問1]

- (1) a, b は、解答例どおりのみ各 2 点。
- (2) 解答例どおりのみ 3 点。
- (3) c は、解答例どおりのみ 3 点。

##### [設問2]

- (1) d は、解答例どおりのみ 2 点。
- (2) e は、解答例どおりのみ 2 点。

##### [設問3]

- (1) f は、解答例どおりのみ 2 点。
- (2) 解答例と同様の趣旨、例えば、再署名というキーワードまでが指摘されているもの対し 6 点。内容が今一步のもの(上位管理者が修正した場合だけを指摘したものなど)は 3 点。その他は 0 点。
- (3) 解答例と同様の趣旨が適切に指摘されているもの対し 6 点。その他は、基本的に 0 点。

- (4) 手順 1, 手順 2 とも, 解答例と同様の趣旨が適切に指摘されているものに対し各 6 点。その他は, 基本的に 0 点。特に, 手順 2 は権限属性の変更ができる者が誰かという点が重要であり, 「設計文書の複製操作を許可に変更する」旨だけを指摘し, 誰が明確になっていない答案は 0 点にしました。
- (5) E システムの機能は, 解答例どおりのみ 2 点。理由は, 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は, 基本的に 0 点。
- (6) 上位管理者というキーワードが指摘されてものに対してだけ 2 点。

#### 【講評】

平均点は 16.6 点 (平均正答率は 33.2%) であり, 想定していた平均正答率 (40%弱) よりも, 低いものとなりました。

設問 1 の(1), (2)は情報セキュリティの基本的な問題でしたから, 大半の受験者が正解できると思っていました。全問正解者は, ごく一部の受験者に限られました。これは「文書の  と署名者の  を検証可能とする文書」だけに着目し, 空欄 a, b に入れる字句を考えたからではないでしょうか。この文書の前には, 「機密性」, 「電子文書の承認後」と記述されていますので, これらの字句との関連から考察していくことが必要です。極秘文書の承認については「…電子文書を承認し, 電子署名を付与する」と記述されていますので, 電子署名のもつ機能を答えればよいことが分かります。また, 情報セキュリティについては, 情報の機密性, 完全性, 可能性のほか, 真正性, 責任追跡性, 否認防止, 信頼性といった特性が基本になっています。これらの知識を基にすれば, 自ずと空欄 a, b に入れる字句は導き出せると思います。

設問 2 では, 公開鍵証明書の ITU-T 勧告名, CRL の正解率も高くなかったようです。SC 試験を受験するに当たっては, 基本的な用語を理解しておくことが要求されます。全体的にしっかり学習しておきましょう。

設問 3 は, 電子文書と承認文書との関係が少し複雑になっていましたから, 的を射た答案は少なかったように思います。記述式の問題では, 問題の記述内容に従って解答を作成することが基本ですから, 条件を整理しながら解答を考察していくようにしましょう。

## 問2 ホスティングサービスの提供

### 【採点基準】

#### [設問1]

- a ~ d は, 解答例どおりのみ各 3 点。

#### [設問2]

- (1) アは, 解答例どおりのみ 4 点。
- (2) L3SW に設定すべきものは, 解答例と同様の機能が指摘されているものに対し 4 点。VLAN を指摘したものは 2 点。その他は 0 点。理由は, 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。VLAN に関するものは 3 点。その他は 0 点。

#### [設問3]

通知する情報は, 解答例と同様の趣旨が適切に指摘されているものに対し 4 点。理由は, 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は, 基本的に 0 点。

#### [設問4]

- (1) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は, 基本的に 0 点。
- (2) 解答例と同様の趣旨が適切に指摘されているものに対し各 4 点。その他は, 基本的に 0 点。

#### 【講評】

平均点は 11.9 点 (平均正答率は 23.9%) と, 午後 I の 4 問の中では, 最も低い点数でした。IPsec で NAT を行うと, 通信ができなくなる技術的な理由を答えるものなど, 詳細な知識を問う問題も含まれていたため, 全体的に正答率が低くなったものと思われます。

設問 1 の穴埋め問題は, 技術的な知識を保有していることが必要ですから, 正答率は低かったように思います。なお, 本番の試験でネットワーク関連の問題を選択する場合には, TCP/IP 全体に関する技術を十分に理解しておくことが必要です。

設問 2, 設問 3 も, ネットワークの専門知識が必要な問題でしたから, 一部の受験者を除き, 正答率は低かったようです。

設問 4 (1)では, 下線③に含まれるタイムスタンプを付与するという記述に着目した答案が多かったように思います。もう少し全体の記述内容に着目し, ファイアウォールで顧客 PC の IP アドレスを, 一つの仮想 IP アドレスに変換しているということに気付いてほしかったと思います。特に, 下線部分に関する記述式の問題は, 下線の前後に記述されている文章, あるいは全体的な記述内容から考察することも要求されます。本番の試験では, もう少し全体的な関係を念頭に置きながら解答を作成していくようにしましょう。

## 問3 データベースの情報保護と運用

### 【採点基準】

#### [設問1]

- (1) a, b は, 解答例どおりのみ各 2 点。

- (2) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は、基本的に 0 点。
- (3) 解答例と同様の趣旨が適切に指摘されているものに対し各 6 点。その他は、基本的に 0 点。
- (4) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は、基本的に 0 点。

**【設問2】**

- (1) c, g は、解答例どおりのみ各 2 点。
- (2) e, f は、解答例どおりのみ各 3 点。
- (3) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は、基本的に 0 点。
- (4) d は、解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は、基本的に 0 点。

**【講評】**

平均点は 18.3 点（平均正答率は 36.6%）と、午後 I の 4 問の中では問 4 に次いで高くなりましたが、想定よりも若干、低くなりました。

設問 1 では、(3)、(4)の正答率が想定以上に良かった半面、(1)の空欄 b の共通鍵アルゴリズムを答える問題の正答率は低かったと思います。本番の試験で、このような基本的な問題にミスをする、致命傷になります。基本的な問題では、必ず得点できるようにしましょう。

なお、選択者の多かった問 1 と問 3 を比較して評価すると、問題の記述内容が複雑かどうかの違いが、そのまま正答率に反映されていると考えられます。このため、本番の試験で合格基準点をクリアするには、問題の記述内容が複雑になったり、高度になったりしても、正解を導いていくことができるようにすることが必要です。基本的な知識のほか、問題の読解力、全体の関係を相互に整理しながら考える洞察力などを、できるだけ磨いていくとよいでしょう。

**問4 Web アプリケーションの脆弱性対策**

**【採点基準】**

**【設問1】**

- (1) a ~ d は、解答例どおりのみ各 3 点。
- (2) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は、基本的に 0 点。
- (3) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は、基本的に 0 点。

**【設問2】**

- (1) \$country, \$street とともに、解答例どおりのみ各 4 点。
- (2) e, g は、解答例どおりのみ各 2 点。
- (3) f は、解答例どおりのみ 3 点。
- (4) 解答例と同様の趣旨が適切に指摘されているもの

に対し 5 点。内容が今一步のものは 3 点。その他は 0 点。

- (5) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は、基本的に 0 点。

**【講評】**

平均点は 19.6 点（平均正答率は 39.3%）であり、午後 I の 4 問の中では最も高い点数でした。その半面、選択者数は 4 問の中で最も低く、問題の後半部分が、セキュアプログラミングの問題であったことから、選択の対象外にした受験者が多かったものと思われます。

設問 1 (1)の穴埋め問題のうち、空欄 a は詳細な技術用語を問うものでしたから、正答率が低いのは仕方ありません。しかし、空欄 b ~ d は、想定していたよりも正答率は低かったようです。基本的な用語は、しっかり把握しておく必要があります。また、(2)は基本的な事項を答えるものですが、記述式で解答を求められると、思うように表現できないことがあります。日ごろから分かりやすい文章で解答を作成するようにしておきましょう。

設問 2 では、(1)、(5)の正答率はまずまずでしたが、(3)や(4)は、想定していたよりも低かったと思います。プレースホルダなどの用語は理解していたとしても、静的や動的といった字句と組み合わせられると、戸惑ってしまいます。問題文全体を考慮し、適切な字句は何かを考えるようにすることが必要です。

**<午後Ⅱ>**

**問1 ネットワークセキュリティ**

**【採点基準】**

**【設問1】**

- a ~ f は、解答例どおりのみ各 3 点。

**【設問2】**

- (1) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。
- (2) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。

**【設問3】**

- (1) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。
- (2) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。

**【設問4】**

- (1) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。
- (2) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。
- (3) 解答例と同様の趣旨が適切に指摘されているもの

に対し 8 点。その他は、基本的に 0 点。

- (4) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。

#### 【設問5】

- (1) 方式の名称は、解答例どおりのみ 2 点。理由は、解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。
- (2) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。

#### 【講評】

技術的な内容に重点を置いた出題でしたから、全体的に正答率は低く、平均点は 25.5 点でした。想定していたよりも、かなり低い結果に終わりました。

設問 1 は、全体的に正答率は低く、暗号化方式、ハッシュ関数、カプセル化の手法などに関する基本的な用語は、十分に把握しておくことが必要であると思われます。

設問 2 ～ 4 の記述式問題も、全体的に正答率は低かったように思います。特に、設問 3 (1)では、通信データの暗号化については AES-128 や 3-key Triple DES を使うので、安全性は確保されているにもかかわらず、解読される危険性があることを問うようにしていましたが、1,024 ビットの RSA には脆弱性が存在する旨の指摘にとどまった答案がほとんどで、通信データの暗号化を行う共通鍵を作成する情報が 1,024 ビットの RSA で送信されることに言及したものは、極めて少数でした。記述式の問題では、設問で問われていることの本質を考えて解答を作成することが必要であると思われます。また、設問 4 (1)は、メッセージ認証の基本的な問題でしたが、正答率は思ったほど、高くはありませんでした。

設問 5 (1)は、機器認証の基本的な問題ですが、正答率は、かなり低かったようです。SC 試験で合格を目指すには、一つ一つの知識を積み重ねていくことが重要ですから、努力を惜しまないようにしましょう。

## 問2 Web アプリケーションの再構築

### 【採点基準】

#### 【設問1】

- (1) a ～ c は、解答例どおりのみ各 3 点。
- (2) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。
- (3) 設定、操作ともに、解答例と同様の趣旨が適切に指摘されているものに対し各 6 点。その他は、基本的に 0 点。

#### 【設問2】

- (1) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。

- (2) 機密性、完全性、真正性の三つが適切に指摘されているものに対し 10 点。二つの要素が適切に指摘されている場合には 5 点。その他は 0 点。

- (3) 解答例どおりのみ 5 点。

- (4) 方式は、解答例どおりのみ 2 点。理由は、解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。

#### 【設問3】

- (1) d, e は、解答例どおりのみ各 3 点。
- (2) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。
- (3) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。
- (4) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。
- (5) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は、基本的に 0 点。

#### 【講評】

平均点は 31.4 点と、問 1 よりも若干、高くなりましたが、決して満足できるような点数ではありません。

設問 1 (1)は、Cookie に関する基本的な属性を問うものでしたから、正答率は高くなると想定していました。しかし、実際にはそうではなく、まだまだ基本的な知識が不足していると感じられます。(2)も、問題の記述内容を基にして解答を作成するのではなく、各自が思い付いた内容を述べているようなものも多く見られました。こうした点は、本番の試験に向けて改善していく必要があると考えられます。

設問 2 では、(4)は問題の記述内容を基にした答案が多く、まずまずでしたが、そのほかの設問は正答率が低かったように思います。このうち、(2)では、完全性、真正性の意味が正しく理解されていないような答案も見受けられました。

設問 3 は、ほかの設問に比較すると、正答率がやや高かったように思います。日ごろ、経験している事項などを解答するものが多かったのか、解答を作成しやすかったからではないでしょうか。つまり、情報セキュリティに関する知識レベルを保有していれば、それだけ解答を作成しやすいので、本番の試験に向けてできるだけ知識レベルを高めておくことが得策です。

また、午後 II 試験では、問題の記述内容を理解し、設問で問われていることに的確に対応していくことが必要です。本試験では問題の条件などを十分に考慮しながら解答を作成するように心掛けましょう。

以上