# 2009 秋 情報セキュリティスペシャリスト 全国統一公開模試 講評と採点基準

2009 年 9 月 20 日 (株)アイテック 商品開発本部

## ■ 全体講評

午後Ⅰ，午後Ⅱ試験とも，問題ごとのばらつきは少しありましたが，全体的に正答率は高かったようです。この調子を維持しながら，本試験までの残された期間を有効に利用し技術レベルをさらに向上させ，本試験では午後Ⅰ，午後Ⅱとも，合格基準点をクリアできるように努力していきましょう。なお，問題ごとの平均点は午後Ⅰ（50 点満点）の問 1 が 18.1 点，問 2 が 20.4 点，問 3 が 28.0 点，問 4 が 16.9 点で，午後Ⅰの平均点は 44.3 点になりました。また，午後Ⅱ（100 点満点）の問 1 が 46.4 点，問 2 が 43.8 点で，平均点は 45.4 点でした。

次に，問題の選択状況を紹介しておきます。午後Ⅰでは，受験者の約 49%が問 1 を選択していました。問 2 は 37%，問 3 は 78%，問 4 は 37%でした。問 3 は，情報セキュリティマネジメント系を中心とした問題ですから，多くの受験者が選択したと思われます。その一方，問 2（セキュアプログラミングを中心とした問題）と問 4（検疫ネットワークを中心とした問題）は，それぞれの専門知識が必要とされたり，難度が高かったりしたので，選択者が少なかったことは，予想どおりといえます。なお，午後Ⅰ試験は，4 問の中から 2 問の選択ですから，選択の自由度が高くなっています。できるだけ得意とする分野の問題を選択するようにしましょう。

午後Ⅱでは，問 1 の選択者が 60%，問 2 が 40%という割合でした。問 1 がデータベースを中心とした問題，問 2 がセキュアプログラミングを中心とした問題でしたから，ネットワーク系を得意とする受験者にとっては不利だったと思われます。なお，これまでのテクニカルエンジニア（情報セキュリティ）および第 1 回の情報セキュリティスペシャリスト試験の午後Ⅱの出題内容は，認証や暗号化などの情報セキュリティ系，ネットワーク系，データベース系，セキュアプログラミング系，情報セキュリティマネジメント系を組み合わせた問題となっています。そこで，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とよいでしょう。また，一度，選択した問題は最後までやり遂げることが大切です。一部，専門知識を有していなければ解答できない問題もありますが，多くの問題は，問題文で記述された内容に基づいて考察していけば，正解を導いていくことが可能なように出題が工夫されています。したがって，設問で問われていることを確認し，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ようにしてください。こうした地道な作業を続けていけば，ある程度，正解にたどり着くことができるはずです。後は，分かりやすい日本語で論理が通るように，指定された字数内で解答を作成していくようにしましょう。

今回の公開模試の採点状況から見ても，答案の中には問題の条件を考慮していなかったり，設問で問われていることに対し適切に解答していなかったりするものが多く見受けられました。また，不要な修飾語はできるだけ削除し，ポイントになる内容を分かりやすく記述することが必要です。今回の公開模試でも，設問で問われていること以外の内容を答えているものや，むだな修飾語が多く，肝心なことが記入できていないようなものも数多く見受けられました。これらの点については，本番の試験までには，ぜひ修正してほしい事項です。また，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持って，午後Ⅱ試験の最後まで全力を出し切り（あきらめず）問題に取り組み，ぜひ合格するようにしましょう。

## ＜午後Ⅰ＞

### 問1 認証技術の導入検討

**[採点基準]**

**[設問1]**

（1）a，b は，解答例どおりのみ各 2 点。ただし，空欄 b は，チャレンジレスポンス方式の代表例である S/KEY も正解としました。

（2）c は，解答例どおりのみ 4 点。

（3）「初期処理のパスワード（パスフレーズ）が盗聴される」旨が適切に指摘されているものに対し 4 点。内容が今一歩のものは 2 点。その他は 0 点。

（4）不正なサーバを用いた脅威，脅威が発生する理由とも，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 4 点。その他は，基本的に 0 点。

**[設問2]**

（1）d，e 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 4 点。その他は，基本的に 0 点。

（3）「盗聴されても元のデータは分からない」，「転送するデータ量が削減できる」旨のキーワード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。例えば，「盗聴を防止できる」，「固定長のデータになる」などの指摘は不正解としました。

（4）存在性証明，完全性証明について，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。
（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]**

設問 1 の正答率が低かったことなどから，平均点では 18.1 点にとどまりました。

空欄 a では，「なりすまし」という答案がかなり見られました。問題文は「本人になりすまそうとする（a）攻撃……」となっているので，空欄 a にはなりすましが入ることはありません。穴埋め問題では，前後の関係から空欄に入れる字句をよく考えるようにしましょう。

設問 1 (3)では，パスワードが盗聴される旨の解答が多くありました。パスワードといった場合，初期処理のパスワードか，OTP 自体なのかが不明です。解答では何がということを明確に記述するようにしましょう。

時刻認証の仕組みについては，よく理解している受験者と，そうでない受験者に二分されました。この際，時刻認証とは何かを十分に理解しておきましょう。

最後に電子署名の検証方法について補足しておきます。電子署名の検証については，よく署名者の公開鍵で検証するといいます。しかし，これではどのように検証を行っているのかが分かりません。一般に，署名者の公開鍵で電子署名を復号すると，署名前のハッシュ値が現われてきます。一方，受信者は，送信されてきたメッセージから，署名者と同じハッシュ関数を使ってハッシュ値を求め，相互に比較することによって正しいかどうかの確認を行います。認証は，二つのものを比較することによって検証することが基本になっています。次に，時刻認証はどのように行われているかということです。TSA の電子署名は，時刻とハッシュ値を合わせたものに対し TSA の秘密鍵で暗号化します。このため，タイムスタンプ要求者は，TSA の公開鍵で電子署名を復号したものと，TST の中にある時刻とハッシュ値とを比較し，一致するかどうかを検証すればよいのです。

## 問2 プログラム開発におけるセキュリティ

**[採点基準]**

**[設問1]**

（1）a ～ e 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 4 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 4 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 4 点。その他は，基本的に 0 点。

**[設問2]**

（1）f ～ i 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 4 点。その他は，基本的に 0 点。
（3）解答例と同様の趣旨，または「接続先から送られてくる SYN/ACK に応答しない」旨が適切に指摘されているものに対し 4 点。その他は，基本的に 0 点。
（4）「タイムアウト時間を短くする」というキーワードが指摘されているものに対し 4 点。なお，「タイムアウトによって切断する」旨の指摘は，通常の処理と変わりないので，0 点としました。

**[設問3]**

（1）j は，解答例どおりのみ 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。

**[講評]**

平均点は 20.4 点で，公開模試で想定している午後Ⅰ問題のほぼ平均的な正答率になりました。

個別の設問では，strcpy と strncpy の違いを，よく把握しておいてほしいと思います。strcpy を実行すると，コピー元の文字列の中から，ナル文字が見つかるまでコピーします。このため，コピー元の文字列長が，コピー先よりも長い場合には，バッファオーバフローを発生させますが，コピー先には，ナル文字を含めてコピーされます。一方，strncpy は，コピー元の文字列長のうち，n 文字だけをコピーします。このため，n 文字以内にナル文字がない場合には，コピー先のバッファには，ナル文字が書き込まれないことになります。

なお，セキュアプログラミングの問題を選択する場合には，前もって IPA（情報処理推進機構）セキュリティセンターが公表している「セキュアプログラミング講座」を十分に学習されることをお勧めします。

## 問3 情報セキュリティ管理の検討

**[採点基準]**

**[設問1]**

（1）a，b は，解答例どおりのみ各 2 点。
（2）修正が必要な項番は，解答例どおりのみ 2 点。修正内容は，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。内容が今一歩のものは 3 点。その他は 0 点。

**[設問2]**

（1）c ～ e 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 4 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3]**

（1）f，g 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。内容が今一歩のものは 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に対し 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。

**[講評]**

平均点は 28.0 点で，午後Ⅰ問題の中では最も正答率が高くなりました。秋の試験は，従来の情報セキュリティアドミニストレータ試験の受験者が多く，マネジメント系の問題には強いという傾向があるためでしょうか。

個別の設問では，設問 2 (2)の正答率が低かったことが気になります。下線に関する理由を答える問題は，下線部だけではなく，その前後の記述を含め，幅広く検討していくことが必要です。この問題では，多くの答案は「暗証番号を毎回変更することは運用上容易ですが」という記述に着目したものが多かったように思います。入退室管理については，この下線の前にある W 課長の「誰がいつ入室したかの記録が必要だ」という発言までさかのぼることが必要です。

本番の試験では，下線の前後における記述を確認することはもちろんですが，もう少し全体的な関係から解答を考えていくとよいでしょう。本番の試験では，こうした観点に立って解答を作成するようにしてください。

**問4　検疫ネットワークの導入**

**[採点基準]**

**[設問1]**

（1）a ～ c は，解答例どおりのみ各 2 点。
（2）d は，解答例どおりのみ 2 点。

**[設問2]**

（1）e ～ h 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 4 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。
（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。
（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。

**[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 6 点。内容が今一歩のものは 3 点。その他は 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 6 点。その他は，基本的に 0 点。

**[講評]**

平均点は 16.9 点で，午後Ⅰ問題の中では最も低い点数となりました。この問題は，技術的に難度の高い問題でしたから，ある程度，仕方ないともいえます。

技術分野だけで問題を選択すると，技術的に難度の高い問題を選択することもあります。そこで，本番の試験で，こうした場合に遭遇すると，どのように対応したらよいかを考えてみましょう。例えば，設問 2 (2)では，下線①について，通信を妨害する方法が問われています。そこで，下線①を含む記述を確認すると，「PC がネットワークに接続されると，（a）の（e）検査を行うため，Gratuitous ARP を送信することに着目し，このプロトコルをシステム内の管理サーバが検出して通信を妨害するような手法が考えられています。ただし，この場合，妨害されるべき PC を特定するには，事前にシステム内の管理サーバに正規 PC の（f）アドレスを登録しておくことが必要です」となっています。そこで，この文章をよく読めば，「管理サーバが Gratuitous ARP に応答して妨害する」ということが分かります。このようにすれば，正解を導くことができます（それには，問題の記述内容を理解できるだけの必要最小限の技術知識が必要です）。本番の試験で，解答作成に困ったら，問題文の中から徹底的にヒントを見つけ出すようにしましょう。

**＜午後Ⅱ＞**

**問1　データベースのセキュリティ**

**[採点基準]**

**[設問1]**

（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。内容が今一歩のものは 3 点。その他は 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。内容が今一歩のものは 4 点。その他は 0 点。

**[設問2]**

（1）a ～ c は，解答例どおりのみ各 2 点。
（2）d ～ g は，解答例どおりのみ各 2 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。

**[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 10 点。内容が今一歩のものは 5 点。その他は 0 点。

（2）h ～ k は，解答例どおりのみ各 2 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）特定の可否は，解答例どおりのみ各 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各 6 点。その他は，基本的に 0 点。

**[講評]**

平均点は 46.4 点で，まずまずの正答率です。

個別の設問では，設問 1 に着目します。設問 1 (1)では，制限エリアに設置することは，物理的セキュリティ対策を実施することになります。答案の中には，「権限を持つ利用者だけに……アクセス制御を実施する」という技術的セキュリティ対策を指摘したものもありましたが，これでは不正解になります。一方，物理的セキュリティ対策の内容を指摘する場合には，「必要最小限の管理者だけが入室可能なエリアとする」というキーワードを解答することが必要です。大半の解答は「機密情報は制限エリアに保管する」旨を指摘していましたが，何が解答として求められているかをよく吟味していくとよいでしょう。また，(2)は設問で「運用管理者の種類と保護する情報分類を含めて」と指示されているので，こうした視点の解答を作成することがポイントです。

午後Ⅱ問題では，特に問題の記述内容，設問の指示に忠実に従うことが重要となります。本番の試験では，こうした姿勢を忘れないようにして問題に取り組んでいくことが大切です。

## 問2 Web システムのセキュリティ

**[採点基準]**

**[設問1]**

（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2]**

（1）「顧客の個人情報の漏えい」，「システムの脆弱性情報の漏えい」というキーワード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。

（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 6 点。その他は，基本的に 0 点。

**[設問3]**

（1）a ～ d 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 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4]**

（1）e，f は，解答例どおりのみ各 2 点。

（2）属性名は，解答例どおりのみ 2 点。方法は，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。

（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。

**[講評]**

平均点は 43.8 点で，問 1 よりも若干，下回りましたが，まずまずの正答率であったといえます。

設問 1 については，セキュリティ事故に遭遇した際，担当者独自が判断するのではなく，責任者に報告の上，その指示を仰ぐという視点は重要なことです。しかし，この問題では，エラーメッセージに関する内容を指摘したものだけを正解にしました。

セキュアプログラミングの問題については，ある一定の知識が要求されますが，問題の記述内容をもとにしながら設問 3 のような問題には，正解できるように技術レベルを向上させておくとよいでしょう。そうすれば，幅広い分野の午後Ⅱ問題に対しても対応することが可能となります。なお，設問 3 の正答率は，全体的に低かったようです。

また，クッキー情報に関するセキュリティは重要です。セッション管理の方法だけではなく，セキュアな通信を行うための属性などを含め，幅広く理解するようにしましょう。

以上