# 2019 春 情報処理安全確保支援士 全国統一公開模試 講評と採点基準

2019 年 3 月 25 日 (株)アイテック IT 人材教育研究部

## ■ 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 44.7 点，午後Ⅱが 41.9 点でした。問題別では，午後Ⅰの問 1 が 23.3 点，問 2 が 22.2 点，問 3 が 21.6 点で，問ごとの差は，ほとんどみられませんでした。また，午後Ⅱは，問 1 が 41.2 点，問 2 が 43.1 点で，問 2 の方が少し高くなりました。2018 年秋期の公開模試は，午後Ⅰの平均点が 42.4 点，午後Ⅱの平均点が 38.9 点でしたから，平均点で評価すると，午後Ⅰ，午後Ⅱともに，アップしています。また，今回の採点結果から判断すると，一部の受験者はかなり高い点数を上げていましたが，点数的にはまだまだ準備不足という受験者もかなり見られたという印象を受けました。

合格基準点をクリアするには，記述式の問題に対する取組み方が重要になってきます。記述式の問題の多くは，下線に関するものが出題されます。すると，解答を作成する際，どうしても下線部だけに注目しがちです。しかし，下線部だけに注目してしまうと，その前後にある条件などを見落としてしまい，的を射た解答をなかなか作成することができません。今回の模試でも，こうした解答が数多く見られました。設問で何が問われているかを十分に確認し，下線部の記述だけではなく，その前後における関係をよく把握した上で，解答を作成するようにしましょう。なお，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とよいでしょう。

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，問 1（IoT システムのセキュリティ）の選択者が 34.9%，問 2（Web サイトのセキュリティ対策）が 24.7%，問 3（マルウェア対策）が 40.4%で，例年に比較すると，問題ごとの選択者数に偏りが少なかったといえます。なお，本試験の午後Ⅰで出題される問題数も 3 問ですから，各自が得意とする分野の問題をいち早く見つけ出し，それに集中して取り組むことが必要になると考えられます。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知識が，まず必要とされます。本試験実施日までの期間で，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試験は，問 1（社内システムのセキュリティ対策）の選択者が 63.5%，問 2（セキュリティ対策の強化）が 36.5%でした。今回は，問 2 の方が少し技術的な要素が強い問題でしたから，問 2 の選択者数が少なくなったと思われます。午後Ⅱ試験は，様々なセキュリティ分野の知識が問われる総合問題として出題されることが多いので，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とよいでしょう。また，IPA 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 問とも手をつけ，かえって失敗することになってしまいます。

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到達していれば，問題文で記述された内容を基にして正解を導き出すことができます。しかし，受験者によっては問題文の記述内容をそのまま引用して解答を作成している例も多く見られます。単なる引用では正解になることは極めて少ないので，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論理的に考えていくようにしましょう。

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（あきらめずに）問題に取り組んで，ぜひ合格するようにしましょう。

## ＜午後Ⅰ＞

### 問1 IoT システムのセキュリティ

**【採点基準】**

**[設問1]**

（1）a，b は，解答例どおりに対し各 2 点。
（2）c，d は，解答例どおりに対し各 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 4 点。その他は，基本的に 0 点。
（4）解答例どおりに対し 4 点。
（5）機能，機器は，解答例どおりに対し各 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 4 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 4 点。その他は，基本的に 0 点。
（2）e ～ j は，解答例どおりに対し各 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 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 6 点。その他は，基本的に 0 点。

**【講評】**

平均点は 23.3 点（平均正答率は 46.6%）であり，午後 I の中では，最も高い点数でした。

設問 1 (1)，(2)は，少し専門知識が要求される用語選択問題でしたから，正答率はそれほど高くなかったようです。また，(3)～(5)についても，正答率は高くなかったと思います。(4)は，ポート番号と解答した受験者が見られましたが，ポート番号には宛先ポート番号と送信元ポート番号の二つが存在します。この両者のうち，どちらかを区別して答える必要のある問題については，宛先か送信元かを付けて答えるようにしましょう。ただし，TCP や UDP ヘッダにある情報などが問われている場合については，ポート番号と答えても構いません。(5)では，下線③について，実装すべき機能が問われています。このようなケースでは，必ず下線部を含む全体の記述を見ながら考えるようにしましょう。下線③を含む記述は，「そして，インターネットからの Web サーバにおける Web アプリケーション攻撃を防ぐためには，図 3 のあるネットワーク機器に対して，必要な機能を実装することが有効になると考えた」です。そうすれば，Web サーバにおける Web アプリケーション攻撃を防ぐための機能は何かを考えることができます。次に，その機能を実装すべきネットワーク機器を考えます。このように設問で問われている順に沿って丁寧に答えていけばよいのです。本試験でも，設問で問われていることを確認し，下線部だけに着目して解答を作成するのではなく，問題文の前後に記述されている内容を考慮しながら，解答を作成することを忘れないようにしましょう。

設問 2 は，全体的に正答率が高かったと思います。(2)の空欄 f は，SSH の認証方式を答えるものですが，パスワード認証と公開鍵認証の二つがあることは，よく理解されていると思います。(4)は，接続 IP アドレスを制限する方法ですから，ゲートウェイに対して SSH で接続する機器は何かを明確にすれば，具体的にどの装置が該当するかが分かりますので，送信元の装置を明確して具体的に答えるようにしましょう。

### 問2 Web システムのセキュリティ対策

**【採点基準】**

**［設問1］**

（1）a，b は，解答例どおりに対し各 3 点。

（2）c，d は，解答例どおりに対し各 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。

**［設問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

**［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。その他は，基本的に 0 点。

（2）e は，解答例どおりに対し 2 点。

**［設問4］**

（1）解答例どおりに対し 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各 4 点。その他は，基本的に 0 点。

（3）f は，解答例どおりに対し 3 点。指定されるデータは，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。その他は 0 点。

**【講評】**

平均点は 22.2 点（平均正答率は 44.4%）で，午後 I の 3 問の中では，問 1 に次ぐ点数でした。

設問 1 (1)は，個別の攻撃名称を答えるものでしたから，正答率は低くなると想定していましたが，比較的良かったと思います。(2)の空欄 c の正答率は，まずまずでしたが，SHA-1 を答える空欄 d の正答率は低かったと思います。(3)の記述式問題の正答率も低かったようです。SHA-1 の衝突問題は，異なるデータから同じハッシュ値が生成されることですから，こうした基本的な事項については，十分に理解しておいてほしいと思います。

設問 2 は，SSH の sftp コマンドを使用する旨の解答が多く見られました。ここでは FTP 通信の暗号化が問われていますので，TLS を使う FTP over TLS（FTPS）に気付いてほしかったと思います。

設問 3 (1)の正答率は高かったと思います。しかし，(2)の空欄 e に入れる字句は，アドレス変換の基本的な用語でしたから問題なく解答できると考えていましたが，ほぼ全員正解という状況ではなかったようです。

設問 4 (1)，(2)の正答率は高かったようで，これが，問 2 の平均点を押し上げる結果になったと思われます。(3)の空欄 f に入れる応答ヘッダフィールド名を選択する問題は，まずまずの正答率でした。そのヘッダで指定されるデータについても，比較的多くの受験者に理解されているようであり，想定よりも高い正答率だったと思います。

### 問3 マルウェア対策

**【採点基準】**

**［設問1］**

（1）a，b は，解答例どおりに対し各 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) c は，解答例どおりに対し 2 点。

［設問2］
(1) d，e は，解答例どおりに対し各 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) 有効に機能しないものは，解答例どおりに対し 2 点。理由は，有効に機能しないものが正解で，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 6 点。その他は，基本的に 0 点。

［設問3］
(1) f は，解答例どおりに対し 2 点。
(2) 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 4 点。その他は 0 点。情報は，解答例どおり（利用者 ID の指摘）に対し 4 点。
(3) g，h は，解答例どおりに対し各 2 点。

**【講評】**

平均点は 21.6 点（平均正答率は 43.2%）でした。午後 I の 3 問の中では，選択者数が最も多かった半面，点数は若干ですが，最も低い点数になりました。

設問 1 (1)の空欄 b は，MX などを選択した例も見られ，正答率はあまり高くありませんでした。(2)の正答率は高かった半面，(3)の正答率は低かったようです。

設問 2 (2)は，十分な知識を有していれば正解できますから，ほぼ想定どおりの正答率だったと思います。これは，サーバ証明書の検証に関するものですから，解説などをよく読んで理解を深めておくことが大切です。(3)は，URL フィルタリング機能と解答したものが多く見られましたが，図 1 と図 2 の違いは，プロキシサーバで HTTPS 通信を終端するかどうかの違いしかありません。プロキシサーバの中を通過するデータが暗号化されているかどうかですから，暗号化されているとウイルスチェックができないということになります。なお，Web ブラウザからプロキシサーバが受け取る HTTP リクエストについては，図 1 も図 2 も同じですから，URL フィルタリングの扱いについては，図 1 も図 2 も変わりません。(4)は，マルウェアがネットワーク上などで利用者 ID とパスワードを盗み取ることは，比較的よく理解されていたようです。

設問 3 (1)は，“a.b.0.10”などの解答が見られました。“a.b.0.10”から“x.y.z.10”への通信は FW を通過することがないので，空欄 f には当てはまりません。少し注意するだけで正解できる問題には，取りこぼししないようにしましょう。(2)の正答率は，あまり高くなかったようです。プロキシサーバで認証を行う際に取得できるログは，基本的に利用者 ID になります。

**＜午後Ⅱ＞**

**問1 社内システムのセキュリティ対策**

**【採点基準】**

［設問1］
(1) a ～ c は，解答例どおりに対し各 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 6 点。その他は，基本的に 0 点。

［設問2］
(1) d，e は，解答例どおりに対し各 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。

［設問3］
(1) f ～ i は，解答例どおりに対し各 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) 責任追跡性，認可とも，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。

［設問4］
(1) j は，解答例どおりに対し 4 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（CRL を発行というキーワードが必要）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 6 点。その他は，基本的に 0 点。

［設問5］
(1) k ～ n は，解答例どおりに対し各 2 点。
(2) 利便性の観点，信頼性の観点とも，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 6 点。その他は，基本的に 0 点。

**【講評】**

問 1 の平均点は 41.2 点で，問 2 より約 2 点低い点数でした。なお，問 1 を選択した受験者は，全体の約 65%を占めていました。

設問 1 の正答率は，全体として低かったと思います。特に(2)の PFS（Perfect Forward Secrecy）の意味や，(3)の Web サーバの URL とサーバ証明書の CN（コモン

ネーム）の整合性を検証する目的などについては，十分に理解しておくことが大切です。

設問 2 の正答率は高かったので，問題ないと思います。

設問 3 (1)は，表 1 の「○」，「×」ではなく，問題文の記述と照らし合わせながら考えるとよいでしょう。(2)の正答率は比較的良かったと思います。(3)の責任追跡性の問題を述べる方の正答率は高かったようですが，認可の問題を述べる方は，正答率が低かったと思います。認可は基本的にアクセス権限を意味しますので，認証とは区別して考えることが必要です。

設問 4 (1)は，図 5 を参考にすれば，空欄 j に入れる字句を解答できると思っていましたが，期待していたような正答率ではありませんでした。(2)～(4)は，まずまずの正答率だったと思います。

設問 5 (1)の空欄 n は，証明書という答案が多く見られました。署名を検証する際には，誰の証明書を用いるかが重要ですから，利用者なのか，サーバなのか，認証局なのかといったことをよく考えるとよいでしょう。

**問2 セキュリティ対策の強化**

**【採点基準】**

**[設問1]**

a ～ c は，解答例どおりに対し各 2 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各 4 点。その他は，基本的に 0 点。

(2) L2SW を利用して複製する場合，外部メールサーバで複製する場合とも，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 4 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。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 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) d は，解答例どおりに対し 2 点。目的は，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。

(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。

**[設問5]**

(1) e ～ g は，解答例どおりに対し各 2 点。

(2) h 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。

(3) セキュリティ規格，認証方式は，解答例どおりに対し各 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 7 点。指摘内容が今一歩のものは 4 点。その他は 0 点。

**[設問6]**

(1) i は，解答例どおりに対し 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。

**【講評】**

問 2 の平均点は 43.1 点であり，問 1 より約 2 点高くなりました。

設問 1 は，想定よりも低い正答率でした。日ごろから必要な知識を身に付けるように努力しましょう。

設問 2 は，全体として正答率が低かったと思います。タイムスタンプによる効果は，存在性証明と完全性証明の二つです。

設問 3 は，想定よりも少し高い正答率のようでした。一部の受験者は SPF や DKIM だけではなく，DMARC も理解されていたようです。

設問 4 (1), (3), (4)は，想定よりも高い正答率でした。これらは，問題の記述内容を把握して解答が作成されていたように感じられました。同じように(2)も，問題の記述内容を基にして答えるものでしたが，これは少し正答率が低かったと思います。

設問 5 の(2)は，正答率が低かったと思います。無線 LAN では，サーバに該当するものはアクセスポイントです。このため，無線端末で AP の認証を行わなければ，どのアクセスポイントに接続しているかが分かりません。攻撃者が設置したアクセスポイントに接続してしまうと，データを盗聴されるなどの危険性があります。(4)は，アクセスポイントの DNS 設定とは何かがよく理解されていないように感じられました。

設問 6 の正答率は，まずまずだったと思います。

本番の午後試験において合格基準点をクリアするには，問題の記述内容をベースにしながら，設問で問われていることを十分に確認し，素直に解答を作成していくことが必要です。本試験に向け，セキュリティに関する知識レベルを向上させ，解答の作成能力などに磨きをかけて，必ず合格するようにしましょう。

以上