2008 春 テクニカルエンジニア（情報セキュリティ） 総合実力診断模試 講評と採点基準

2008 年 2 月 25 日 (株)アイテック 商品開発本部

■ 全体講評

総合実力診断模試は，４月のテクニカルエンジニア（情報セキュリティ）試験で合格するために必要な技術知識が，どれだけ身についているかを診断することを主な目的にしています。このため，電子メールの仕組みのほか，平成 17 年度および平成 18 年度に行われたテクニカルエンジニア（情報セキュリティ）とテクニカルエンジニア（ネットワーク）試験問題の中から出題し，どのような技術レベルに達成しているかを診ることにしました。そこで，現時点では午後Ⅰ，午後Ⅱ試験とも，どれだけ点数がとれたかということよりも，どれだけ理解できたかということに重点を置いて考えることが大切です。例えば，点数がとれなかった問題については，解説をよく読んだり，「テクニカルセキュリティ技術」や「テクニカルエンジニア情報セキュリティ記述式・事例解析の重点対策」などのテキストを参考にしたりしながら，自分自身の知識として吸収していけば十分だと思います。

その一方，情報セキュリティ試験で合格を目指すには，今回のような問題だけではなく，セキュアプログラミングやデータベースセキュリティに関する詳細技術のほか，ワンタイムパスワードや電子証明書を用いた認証方式，メッセージ認証などに関する認証技術全般，IPsec や SSL，IEEE802.1X などのセキュリティプロトコル，無線 LAN などのセキュリティ技術全般について幅広く理解し，本番の試験に臨むことが必要になってきます。それは，第１回および第２回のテクニカルエンジニア（情報セキュリティ）試験で出題された内容を評価すると，かなり高度な技術知識が要求される問題が出題されているからです。また，問題文で記述された条件，設問で問われている内容を的確に把握していくには，十分な技術力があってはじめて可能になるからです。しかし，こうした情報セキュリティ技術全般に関する正しい技術知識を身につけていくには，十分に学習していくことが必要です。つまり，情報セキュリティに関する本質的な仕組みをしっかり把握していない限り，情報セキュリティ試験で合格をかち取ることは，相当に難しいことだと考えておくべきでしょう。

総合実力診断模試の結果については，A 判定から E 判定という評価が行われます。すでに過去問の対策を十分に実施してきた受験者にとっては，午後Ⅰ，午後Ⅱとも正解率が８割以上という高得点を獲得することができるでしょう。このため，A または B の評価を受ける受験者が多いと想定されます。このように，総合実力診断模試の評価は，過去問の取組み状況に大きく左右されます。しかし，テクニカルエンジニア試験で出題されるテーマは毎年，異なるテーマが出題されます。すると，一度実施したことのある問題とは全く異なり，思うように解答が作成できないことがよくあります。そこで，今回の評価をそのまま鵜呑みにするのではなく，次に行われる公開模擬テストの成績などと合わせて総合的に判断していくことが必要であると考えられます。いずれにしても，これから本番の試験までに，情報セキュリティ技術全般の本質的な仕組みに対する理解だけではなく，問題文の読み方，設問で問われていることに，どれだけ適切に応えていくことができるかどうかなどが重要になってきます。４月の試験日を目指しさらにレベルアップをして，ぜひ合格するようにしましょう。

＜午後Ⅰ 問1＞

【採点基準】

［設問1］

ａ～ｋは，解答例どおりのみ各２点。ただし，ｃはセションというキーワードが記述されていればよい。

［設問2］

(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。その他は，基本的に０点。
②エラーメールがエンベロープの差出人に返される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) DNS プロトコルを使用し，MX レコードを問い合わせる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。

【講評】

午後Ⅰの４問の中では，正解率がそれほど高いというわけではありませんでしたが，平均点はおそらく 20 点（５割）程度と想定されます。この結果から判断すると，電子メールの基本的な仕組みは，その理解が進んでいると考えられます。

SMTP のヘッダ情報のうち，Received と Return-Path フィールドは，追跡者フィールドと呼ばれています。このため，これらのフィールドの読み方は，よく把握しておくとよいでしょう。

設問２(2)については,「DNS プロトコルを使用し，IP アドレスを問い合わせる」などの解答が比較的多く見られました。メールサーバが，あて先のドメイン名の名前解決を行うときには，通常 MX レコードを問い合わせるので，基本的な処理の流れについては，十分に理解しておくようにしましょう。なお，MX レコードを問い合わせると，優先度の値がついたメールサーバのホスト名が回答されるので，優先度の高いほうから順にメール送信を行うことも覚えておくとよいでしょう。

＜午後Ⅰ問2＞

【採点基準】

[設問1]

ａ～ｄは，解答例どおりのみ各２点。

[設問2]

（1）参照と更新という二つのキーワードが指摘されたものに対し８点。参照日時と参照者を特定するなど，参照だけに限定したものは４点。その他は０点。

（2）業務効率を著しく損なう旨のキーワード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]

機能は，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。

条件は，ハッシュ値の登録者を承認者（チームリーダ）に限定する旨を適切に指摘しているものに対し８点。ハッシュ値の作成者をチームリーダに限定するなどの今一歩の表現は４点。その他は０点。

【講評】

平成 18 年度春期のテクニカルエンジニア（情報セキュリティ）試験で出題された午後Ⅰ問２の問題です。すでに受験対策の準備が十分になされているようであり，40 点満点ないしは満点に近い方が多く見受けられました。この結果，平均点もかなり良い点数だと思われます。

個別の設問では，設問３の運用上の条件を述べる問題には，注意してほしいと思います。例えば，「チームリーダ承認後にハッシュ値を登録する」などの指摘については，０点にしています。このような解答は，登録する人が誰であるかが指摘されていません。このため，実際に登録する人が，別の設計開発文書とそのハッシュ値に差し替えて登録するというリスクが存在します。つまり，登録者が誰であるかを明確にすることが，この設問ではポイントになるということです。

＜午後Ⅰ問3＞

【採点基準】

[設問1]

ア～エは，解答例どおりのみ各２点。

[設問2]

（1）解答例と同様の趣旨が適切に指摘されたものに対し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たものに対し４点。その他は，基本的に０点。

[設問3]

（1）解答例どおりのみ２点。

（2）場所は，解答例どおりのみ２点。利点は，解答例のほか，「演算処理が高速にできる」旨を指摘したものに対し３点。その他は，基本的に０点。

[設問4]

（1）オ～ケは，解答例どおりのみ各１点。

（2）解答例と同様の趣旨が適切に指摘されたものに対し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たものに対し４点。その他は，基本的に０点。

（4）解答例のほか，「社外から内部 LAN のサーバへの接続を制限する」旨を指摘したものに対し４点。内容が今一歩のものは２点。その他は０点。

【講評】

平成 18 年度秋期のテクニカルエンジニア（ネットワーク）試験で出題された午後Ⅰ問３の問題です。問２と同様に，高得点者が多く見受けられ，平均点もかなり良い点数だと思われます。

記述式の問題は，一度取り組んだことがあれば，ポイントを押さえた解答を作成することができます。しかし，新たに取り組む問題については，なかなか思うように解答を作成できないことが多いので，本番の試験に向け，キーワードを明確にしながら解答を作成する訓練を行っておくとよいでしょう。例えば，「～について述べよ」と指示されている場合には，主語，述語を明確にして答案を記述するようにするとよいでしょう。

＜午後Ⅰ問4＞

【採点基準】

[設問1]

（1）解答例どおりのみ２点。

（2）ｂ，ｃは，解答例どおりのみ各２点。

[設問2]

（1）解答例どおりのみ２点。

（2）ｄ，ｅは，解答例どおりのみ各２点。

［設問3］
（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８点。内容が今一歩のものは４点。その他は０点。
［設問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各６点。その他は，基本的に０点。

【講評】

平成 18 年度春期のテクニカルエンジニア（情報セキュリティ）試験で出題された午後Ｉ問１の問題です。問２，問３と同様に，高得点者が多く見受けられ，平均点もかなり良い点数だと思われます。

設問の中で比較的正解率が低かった問題が，設問３(1)の空欄ｉに入れる数値です。Perl 言語の仕様を知らなくても，共通かぎが 30 文字（120 ビット）で表示されていることに気が付けば，１文字が４ビットで表示されているので，80 文字という解答を導くことができます。また，設問３(2)は，かなり難しい問題なので，正解者は極めて少数であると想定していました。しかし，過去問の対策が十分に行き届いていたためか，かなりの人が正解していました。一度，解いたことがある記述式の問題に対しては，簡単に正解を導いていくことができたとしても，最初から自分自身が持つ知識の範囲内から考える場合，思うように解答を作成できないことがあります。本番の試験に向け，さらに技術力レベルをアップさせるように努力していってください。

＜午後Ⅱ問1＞

【採点基準】

［設問1］
ア～キは，解答例どおりのみ各３点。ただし，イはファイルサーバと答えてもよい。
［設問2］
（1）解答例どおりのみ各３点。
（2）設置場所は，解答例どおりのみ２点。SW の設定内容は，パケット抽出装置を接続するポートを，社内用メールサーバが接続されるポートのミラーポートにする旨を適切に指摘しているものに対し 10 点。内容が今一歩のものは５点。その他は０点。
（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 10 点。内容が今一歩のものは５点。その他は０点。
［設問3］
（1）解答例どおりのみ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 10 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４点。その他は，基本的に０点。
（2）解答例のほか，「電子証明書の有効期限の管理」と同様の趣旨を適切に指摘しているものに対し各４点。その他は，基本的に０点。
（3）利用者認証のためのプロトコルが位置する層は，解答例どおりのみ３点。判断根拠は，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5］
（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。認証 SW 側の動作を指摘したものなどは，基本的に０点。
（2） ｂ， ｃは，解答例どおりのみ各２点。
（3）解答例のほか，「ICMP エコー要求に対する応答を確認する」旨を適切に指摘しているものに対し各４点。その他は，基本的に０点。
（4）解答例のほか，「消去されたメールを復旧できる」旨を適切に指摘し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８点。内容が今一歩のものは４点。その他は０点。

【講評】

午後Ⅱ問題の問１と問２の選択者の比率は約６対４であり，問１の選択者が多かったように思われます。平均点を比較すると，問１のほうがやや低かったのではないでしょうか。

午後Ｉと同様に，午後Ⅱもこれまでの本試験で出題された問題を選んで出題したことから，高得点者が多く見られた半面，記述式の問題については，ポイントを押さえられた解答を作成できず，思ったほど点数がとれていない受験者も多かったように思います。

テクニカルエンジニア試験で合格するには，記述式の問題に対し的確な解答を作成していくことが求められます。そのためには，設問で何が問われているかを必ず確認するようにしてください。例えば，設問５(1)で問われていることは，認証サーバが認証 SW に対して行う処理内容です。認証 VLAN を利用した検疫ネットワークでは，検査に合格すると，検査サーバはその結果を認証サーバに通知します。すると，認証サーバは，認証 SW が検疫用 VLAN から業務用 VLAN に切り替えることが

できるように，業務用 VLAN の VLAN-ID を認証 SW に通知します。そして，認証 SW がその情報を受け取ると，PC の接続ポートに設定されていた検疫用 VLAN-ID を業務用 VLAN-ID に変更するので，検査に合格した PC は，業務用 VLAN にアクセスできるようになります。

以上のような処理の流れになるので，答案の中には，「検疫用 VLAN から業務 VLAN に切り替える」旨を指摘したものがかなり見られました。採点する側からいうと，このような内容では認証 SW が行う処理内容であって，認証サーバが認証 SW に対して行う処理内容を指摘していないと判断します。このため，検疫ネットワークの仕組みを理解していて，かつ設問で何が問われているかを確認すれば，正解できる問題に対しては，確実に点数をとることができます。特に，午後Ⅱ試験では，こうしたことを一つ一つ積み重ねていくことが大切です。本番の試験では，問題をよく読むほか，設問で何が問われているかを必ず確認したうえで，解答を作成するようにしてください。

＜午後Ⅱ問2＞

【採点基準】

［設問1］

（1）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。内容が今一歩のものは４点。その他は０点。

［設問2］

（1）ａ～ｊ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８点。内容が今一歩のものは４点。その他は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。内容が今一歩のものは４点。その他は０点。

(2)「自社に割り当てられていないディレクトリをアクセスする方法」，「任意のファイルをアクセスする方法」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 10 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）確認すべきことは，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。その目的は，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８点。その他は，基本的に０点。

【講評】

問１と同様に，過去問の対策を十分に行ってきた受験者は，高い得点をマークしていました。全体的にみても，設問１のほか，設問２(1)，(2)，設問４(1)などの正解率がよかったので，平均点も問１よりも高かったように思われます。

個別の設問では，設問２(3)のメールの送信者を確認する方法については，一部理解されていないようなところが見受けられました。例えば，答案の中には「J 社の調達担当者の公開鍵でディジタル署名を復号できることを確認する」旨の解答が多く見られました。送信者を確認する方法については，二つのものを比較し，それらが一致するかどうかによって判断する必要があります。復号しただけでは，それが正しいかどうかは全く判断できないということです。このため，送信者を確認するには，S/MIME によって添付された送信者のディジタル署名を検証することが必要です。しかし，このことが何を意味しているかをよく理解しておかなければなりません。ディジタル署名を検証するとは，まず，ディジタル署名を送信者の公開鍵で復号します。それと同時に，電子メールとして送られてきたメッセージ全体を，ハッシュ関数にかけてメッセージダイジェストを作成します。この作成したメッセージダイジェストと，公開鍵で復号した結果が一致すれば，メッセージ自体が改ざんされていないこと（データの完全性の確保）と，送信者の真正性が同時に確認できるのです。ここでのもう一つのポイントは，ディジタル署名が，送信者の秘密鍵によって作成されているということです。この行為自体は，秘密鍵の持ち主しかできない行為であることから，送信者の公開鍵で復号することが意味を持つことになってきます。

以上のように，情報セキュリティ技術の本質を理解していくには，こうしたことの積み重ねになります。着実にレベルアップを図りながら，試験での合格を目指すようにしていきましょう。

以上