2008 春 テクニカルエンジニア（情報セキュリティ） 全国統一公開模試 講評と採点基準

2008 年 3 月 25 日 (株)アイテック 商品開発本部

■ 全体講評

テクニカルエンジニア（情報セキュリティ）試験は，４月の試験で第３回目の試験を迎えることになります。第１回，第２回の SV 試験の出題内容をみると，詳細な技術知識を問う問題が多かったように思います。そこで，今回の公開模試においても午後Ⅰ，午後Ⅱ試験の出題内容は，できるだけ技術内容を中心とした問題にしました。このため，正解率はかなり低くなるというように考えていました。しかし，採点結果から判断すると，午後Ⅰ試験の正解率は少し低めという印象がありましたが，午後Ⅱ試験では高得点者がかなり見受けられ，本番の試験に向けて準備がよくなされているという印象を受けました。本番の試験では，かなりの人が合格されるのではという期待が大きくなりました。

一方，今回の模試では，各自の得意とする分野と異なる分野の問題であったり，十分な準備ができないまま受験されたりした方もいらっしゃると思います。このような場合には，模試の判定にこだわることなく，４月 20 日の本試験に向け，十分にレベルアップを図って臨むようにしてください。例えば，試験日までの残された３週間前後を有効に使い，模試の解答・解説などをよく読んで，その内容を理解したり，関連する技術知識を含め，自分自身の観点から技術知識を十分に整理したりしてください。また，今回選択した以外の問題については，それを解くことによって，技術知識を整理するうえで役に立ちます。ぜひ，実施しておきましょう。

次に，午後Ⅰ試験と午後Ⅱ試験の状況を簡単に紹介しておきます。午後Ⅰ試験問題の選択状況は，問３が最も多く，問１が最も少ないという状況でした。問１は C++ に関するセキュアプログラミングの問題でしたから，選択対象から外した受験者が多かったと考えられます。また，過去２回の本試験の出題傾向から考えても，今回の試験でもセキュアプログラミングの問題が出題されることは間違いないでしょう。そこで，セキュアプログラミングの問題を選択するかどうかは，あらかじめ決めておくとよいでしょう。また，出題内容は C++，Java，Perl の３言語のうちから出題されますので，得意する言語以外は，選択しないことも一つの方法です。午後Ⅰ試験は，試験時間が１時間 30 分のため，臨機応変に対応するようにしてください。

午後Ⅱ試験における問１と問２の選択者の比率は，約２対１というような状況で，問１の選択者が多かったように思います。問１は設問数が多く，穴埋め問題は字句で解答するほか，DNS の動作，IPsec-VPN，SSL-VPN の技術知識を中心としたものでしたから，平均点でみると，問２よりも低いと考えられます。その半面，問２は設問１，設問２の正解率が高かったことから，全体的に点数が高くなっています。この結果，模試の総合評価は問１の選択者には厳しく，問２の選択者には甘くなる傾向があります。こうした事情もあり，模試の判定結果は一つの目安として考えるとよいでしょう。いずれにしても，４月の試験で最大限の力を発揮し，良い結果を残すことが大切です。

今回の模試の採点状況から判断すると，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。特に，記述式問題については，設問で何が問われているかを必ず確認し，解答を作成することが必要です。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も必要です。今回の模試でも，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，肝心の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。これらの点は，本番の試験では，ぜひ修正してほしいと思います。

試験日当日は，午前，午後Ⅰ，午後Ⅱの三つの試験が行われます。いずれの試験もスコア 600 点をクリアしなければ，合格できません。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＞

【採点基準】

[設問1]

a ～ e 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，例えば管理者権限が奪取されることを適切に指摘したものに対し６点。その他は，基本的に０点。

(2) バッファの最後がナル文字で終端しなくなるというキーワード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。内容が今一歩のものは３点。その他は０点。

［設問3］

（1）配布されるソフトウェアに改ざんがない旨のキーワードが適切に指摘されたものに対し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。

【講評】

言語の詳細を問うような問題が一部，含まれていたためか，全体的な正解率は，ほかの問題に比較すると，若干低かったようです。

個別の設問では，設問３(1)のコードサイニング証明書によって保証されることについては，よく理解しておくことが必要です。答案の中には「発行元がＡ社であることが保証される」旨の指摘が多く見られました。しかし，このような内容では警告メッセージが出力されなくなることを指摘したことと等価です。したがって，この設問では，配布されるソフトウェアに改ざんがないことを保証する旨を解答することが必要となります。電子署名の基本的な内容は十分に理解されていると思いますが，少し形を変えて出題されると，的確に解答できないことがよくあります。もう少し突っ込んで考える姿勢が必要であるといえるでしょう。

また，コードサイニング証明書などの公開かぎ証明書は，基本的に有効期限が設定されます。なぜ，有効期限があるかという点についても，よく理解しておくことが必要です。答案の中には，電子証明書を偽造され，なりすまされるなどの答案も多く見られました。しかし，公開かぎ証明書は基本的に公開されているものですから，この指摘は正しいとはいえません。公開かぎ証明書の安全性が保証されるのは，公開かぎに対応する秘密かぎを解読することが極めて困難であるという原理に基づいています。そこで，同じ秘密かぎを長い間，使い続けると，それを解読されるという危険性があるので，一定の有効期限を設けているのです。問３の設問３と関連する問題です。なお，セキュリティ問題を考えるうえでは，秘密かぎのほか，パスワードなどの秘密情報は，その危たい化に注意することがポイントになります。

＜午後Ⅰ問2＞

【訂正とお詫び】

問題の表の「本社 VPN ルータのフィルタリングルール（抜粋）」において，誤記がありました。番号 7 の送信元 IP アドレス，番号 8 のあて先 IP アドレスが“172.16.21.*”となっていますが，正しくは“172.17.21.*”です。お詫びして訂正させていただきます。

会場受験以外の方は，正誤表が届いていないことから，採点にあたっては，次のようにいたしました。ご了承いただけますよう，お願い申し上げます。

「空欄 g，h については，相互に関係した問題であることから，空欄 g に正解された答案は，空欄 h も無条件に正解とします」

［設問1］

（1） a ～ c 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６点。なお，「ネットワークにパスワードが流れない」などの指摘は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。

［設問3］

（1） f ～ h は，解答例どおりのみ各２点。

（2）解答例どおりのみ２点。

【講評】

正解率は，想定していた以上によかったと思います。

用語の穴埋め問題に関して専門用語を答える問題は，その用語を知らなければ答えようがないので，あまり気にする必要はありません。しかし，設問３の空欄 g，h は，パケットフィルタリングの問題ですから，問題文の U 君と Y 君の会話に着目すれば，正しい解答が導けるはずです。また，本社にある IP 電話端末と PSTN-GW は，同一セグメントにあり，VPN ルータを介して接続されていません。このため，IP 電話端末と PSTN-GW 間の通信については，フィルタリングを行うことができません。このように，問題文を読んで正解できるものは，必ず正解することが合格のための必要条件となります。

＜午後Ⅰ問3＞

【採点基準】

［設問1］

（1）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。

［設問2］
（1） a～dは，解答例どおりのみ各２点。
（2）解答例どおりのみ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） R社が付与した時刻では客観的な証明力に欠ける旨のキーワード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］
「TSA の公開かぎ証明書の有効期間が短い」のキーワードが適切に指摘されているものに対し６点。なお，「電子署名の有効期間が短い」旨の指摘については，原則３点。その他は０点。

【講評】
記述式の問題が比較的よくできていたので，全体的に正解率は高かったようです。時刻認証やファイアウォールのセキュリティについては，よく理解されていると感じられました。その半面，予想外に正解率が悪かったのは，設問２(1)の語句選択問題です。全問正解者も少なかったようです。問題の記述内容を注意深く確認しながら選択していけばよいので，本番の試験の語句選択問題は全問正解するように心掛けましょう。

次に，電子署名と公開かぎ証明書の関係について，少し補足しておきましょう。端的にいえば，電子署名自体に有効期間が設定されるわけではありません。つまり，電子署名を検証するため，一般に公開かぎ証明書が使用されます。そこで，公開かぎ証明書の有効期間が過ぎてしまうと，電子署名の検証ができなくなります。このように，公開かぎ証明書に有効期限が設定されていることに起因する問題なのです。では，なぜ公開かぎ証明書に有効期限が設定されているかということです。問１の設問３とも関連しますが，同じ公開かぎをいつまでも使用し続けていると，公開かぎに対応する秘密かぎが解読されてしまうという危険性（秘密かぎの危たい化）があるからです。こうした内容は，セキュリティ技術の本質にあたることなので，よく理解しておきましょう。

＜午後Ⅰ問4＞
【採点基準】
［設問1］
（1） a～dは，解答例どおりのみ各２点。
（2）攻撃名，サーバ名とも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2］
（1） e， f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】
この問題に対する正解率は，クッキー情報に関する詳細な技術知識を有しているかどうかによって決まったようです。

この問題の中で正解してほしかった問題は，設問１(1)の空欄c，dです。しかし，この２問とも正解した受験者は，極めて少数だったと思います。これらの問題は，暗号方式に関する基本ですから，どのように暗号化が行われているかを冷静に考えればよいのです。例えば，ASからクライアントに送られる信任状は，クライアントの秘密かぎで暗号化しなければ，クライアントは復号できません。また，その中の TGT にある暗号化データは，そのまま TGS に送信するので，TGS の秘密かぎで暗号化しておかなければ，TGS が復号できません。このような関係を論理的に考えていけば，正解を導くことができたと思います。

クッキー情報については，Web アクセスにおけるセション管理に使用される情報です。いくつかの属性が規定されていますが，これらの中では name（session_id），domain，path，secure，expires 属性の使用目的などをよく理解しておくとよいでしょう。

＜午後Ⅱ問1＞
【採点基準】
［設問1］
（1） a～c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） d～fは，解答例どおりのみ各２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。
［設問2］
（1） g～mは，解答例どおりのみ各２点。
（2）解答例どおりのみ４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3］

(1) ｎ～ｒ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。
(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。
(6) 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は，問２と比較すると，設問数などが多かったほか，IPsec や SSL-VPN の技術的なものが中心でしたから，正解率はそれほどよくなかったと思います。

午後Ⅱ問題に限らず，午後Ⅰ問題に取り組む場合には，必ず設問の指示に従うことを忘れないようにしてください。例えば，設問１(1)の空欄ａ～ｃには，「ルータ名を答えよ」と指示されているにもかかわらず，ルータ名で答えていない答案がかなりありました。本番の試験では，必ず設問の指示に従って，解答を作成していただきたいと思います。

技術的な観点からは，VPN 技術は重要です。前回の本試験で，IPsec のかぎ交換の仕組みなどが出題されましたので，今年４月の試験で同じような技術内容が出題されることは少ないと思われます。しかし，VPN 技術はネットワークセキュリティを考えるうえでは重要な仕組みです。このような問題を解くことによってセキュリティ問題の考え方を整理し，試験対策上，必要な技術知識をより多く身につけていきましょう。

＜午後Ⅱ問2＞

【採点基準】

［設問1］

(1) ア～ウは，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。

［設問2］

(1) ａ～ｇ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。

［設問3］

(1) ｈ～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８点。その他は，基本的に０点。
(3) 解答例と同様の趣旨（ただし，無線 LAN の盗聴を解答する場合は固定 WEP キー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（ただし，認証スイッチが HTTP リクエストを受信する旨が必要）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。

［設問4］

(1) ｋ，ｌ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。

【講評】

設問１，設問２は，情報漏えい対策などの基本的な問題でしたから，正解率はかなり高かったようです。しかし，穴埋め問題の正解率は，それほど高いというわけではありません。穴埋め問題は，本番の試験でも必ず出題されますが，専門用語を知らなければ正解が得られないものがあります。このため，穴埋め問題にあまり時間を費やさないようにしましょう。６割正解できればよしとし，記述式問題を考えるときの時間を十分にとるように心掛けてください。

設問３，設問４は，無線 LAN のセキュリティに特化した問題でしたから，解答作成に苦労するのではと想定していました。しかし，答案の中には，問題の記述内容をよく確認し，正解を導くように努力した跡が見られました。本番の試験でも，こうした姿勢を貫いて解答を作成することが必要です。なお，CRC-32 を RC4 などと同じ暗号方式と理解している答案もみられました。しかし，CRC-32 はデータの伝送誤りを検出するための生成多項式です。この際，理解しておきましょう。

以上