平成 23 年度　秋期　情報セキュリティスペシャリスト試験　採点講評

午後Ⅱ試験

問 1

問 1 では，医療情報システムを題材に，個人情報の取り扱い，ディジタル署名やタイムスタンプを用いたデータの完全性及び真正性，社会インフラにおける重要なシステムの事業継続について出題した。

設問 1(1)は，正答率が低かった。複数存在するアクタのうちどのアクタになりすますのかによって，発生するセキュリティ上のリスクが異なってくることを理解して解答してほしかった。(2)は，基礎的な技術に関する出題で，解答の多くは正しい技術用語で解答できていなかった。正しく理解し覚えてほしい。

設問 2(3)は，“アクセス主体”の意味を正しく理解していない解答が多かった。アクタ種別ごとのアクセス制御では不十分なことを踏まえ，“アクセス主体”を更に細かな単位で制御する必要があることに着眼してほしい。

設問 3(2),(3)は，正答率が低かった。タイムスタンプ技術の目的と適用方法について，曖昧なまま理解している解答が多いように見受けられたので，基本的な技術を正確に理解してほしい。(4)は，改ざん検知後，電子カルテを回復する場合，どの時点の状態に戻るのかを認識して解答してほしい。

設問 4(1)は，緊急時にはシステム環境などに関する制約がある中で業務遂行上の優先順位付が必要になることを認識した上で，実行性のある方式を具体的に解答してほしい。(2)は，非常時に医療情報システムを利用する者の識別及び資格の有無など，アクセスの許可を判断する上で必要となる手続などを具体的に解答してほしい。

問 2

問 2 では，複数種類のサーバからなる既存システムに対して，統一したログ管理システムを適用する際の設計について出題した。全体として正答率は想定どおりであり，実務経験をもつ受験者にとっては，正解を導きやすい問題であったと思われる。

設問 2(2)は，正答率が低かった。特権操作 1 に対して記録すべきデータ項目と製品 R の仕様とを比較することで，解答を導き出すことを期待したが，製品 R の仕様や本文中に記載されている条件を十分に理解していないと思われる解答が多かった。実装方法の検討においては，要件や制約の抽出及び整理を行う必要があることを再認識してほしい。また，設問の趣旨を誤解した解答も多かった。解答においては，設問の趣旨を十分に理解してほしい。

設問 2(4)では，システムを正しく選択できているのに，理由を正確に記述できていない解答が多かった。大量のディスク資源が必要になる真の理由は，製品 H の仕様上の制約の結果，必要のないログが大量に取得されてしまうことである。ログ管理においては，ログの保存や分析のために大量のディスク資源が必要になるので，必要なログだけを取得する必要があることを理解しておいてほしい。

設問 4(1)は，正答率が低かった。“管理端末に固定の IP アドレスを割り当てる”とした解答が多く，本文に記載されている，各特権操作に対して取得すべきデータ項目を，正確に理解していない受験者が多かった。ログ管理においては，どのようなデータ項目を取得し，どのような分析を行うかを要件として具体的に定義した上で，最適な実装方法を検討する必要があることを再認識してほしい。