平成 29 年度　秋期　情報処理安全確保支援士試験　採点講評

午後 I 試験

問 1

問 1 では，ランサムウェアへの対策について出題した。全体として正答率は高かった。

設問 2(2)は，復元に利用するバックアップデータを選択する際の適切な判断について問う問題である。“バックアップの開始時刻”という誤った解答が見受けられた。バックアップの取得には時間が掛かるので，その間にランサムウェアが暗号化を行うと，バックアップファイルの中に暗号化されてしまったファイルが含まれ復元できなくなることを理解してほしい。

設問 3(2)は，暗号化に使う鍵について問う問題である。正答率は低かった。本文で示された共通鍵暗号と公開鍵暗号を組み合わせる方法での具体的な処理を理解した上で解答してほしい。

設問 4 は，脆弱性を悪用して他のサーバや PC に感染を広めるランサムウェアの被害について問う問題である。このランサムウェアの場合，管理者権限でファイルを暗号化するので，そのときの被害を想定して，対策の立案ができるようになることを期待したい。

問 2

問 2 では，Web アプリケーション開発におけるセキュリティ対策について出題した。全体として正答率は低かった。

設問 1(1)は，SQL インジェクションの脆弱性対策の問題である。設問 1(2)及び設問 1(3)は，クロスサイトスクリプティング脆弱性対策の問題である。これらについては，比較的よく解けていた。理解が進んでいると思われる。

設問 2(1)は，Cookie についての問題である。Secure 属性については理解されているようだが，それに比べると HttpOnly 属性については理解が進んでいないようであった。設問 2(2)は，正答率は低かった。Web アプリケーションでの認証後のリダイレクト機能に関する問題である。不適切な実装は，オープンリダイレクタの問題を招くことを確認するとともに，オープンリダイレクタの対策としては，ホワイトリストが知られているので，対策できるようになってほしい。

設問 3 は，ソフトウェア開発における検査及びリスク低減策に関する問題である。正答率は低かった。検査に Web ブラウザを用いることもあるので，最近の Web ブラウザの機能をよく理解しておいてほしい。

問 3

問 3 では，SSL/TLS を用いたサーバの設定と運用について出題した。全体として正答率は低かった。

設問 1(1)は，SSL/TLS が利用する暗号関連技術を問う問題である。SSL/TLS の安全性は一部これらの技術によっているので，SSL/TLS を安全に利用するために，正しく理解しておいてほしい。

設問 2(1)は，鍵の危たい化発生時の対応を問う問題である。危たい化が明らかとなった場合，被害の発生を最小にとどめるために，関係するサーバ証明書の利用を停止し，かつ当該サーバ証明書の失効を遅滞なく行わなければならない。設問 2(2)で採り上げたように，情報公開を適切に行うことも求められる。システム運用の現場において，危たい化発生時の対応についての検討が不足していることはないだろうか。受験者各位は，正しい知識を身につけ，現場に貢献してほしい。

設問 3(4)は，サーバ証明書の種類についての問題である。正答率は低かった。市場で販売されているサーバ証明書には複数の種類があり，適材適所がある。Web サーバの目的に照らして最適なサーバ証明書を採用できるように，サーバ証明書の仕様及び発行時の審査の違いを正しく理解しておいてほしい。