平成 22 年度　春期　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，インターネットに公開されているサーバの導入における SSH サーバ，DNS サーバ及びメールサーバの情報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想定どおりだった。

設問 1(1)は，正答率が低かった。初めて SSH サーバに SSH 接続を行う際の，公開鍵の真正性を確認することの重要性について，よく理解しておいてほしい。

設問 2(2)は，正答率が高かったが，(1)及び(3)は，正答率が低かった。DNS キャッシュポイズニング攻撃についての理解は高いが，DNS サーバの設定に関する知識がまだ不十分であるための結果と思われる。DNS サーバには，DNS プロトコルの性質から様々な脆弱性が指摘されており，設定には細心の注意が必要であることを理解してほしい。

設問 3(2)は，選択肢形式であるにもかかわらず正答率が低かった。問題中の記述と図表をよく読めば正答を導けるはずである。インターネットに公開されているメールサーバでの迷惑メール対策についてよく理解しておいてほしい。

問２

問 2 では，ソフトウェア開発会社における情報セキュリティインシデント対応について出題した。全体として正答率は想定どおりだった。

設問 1(1)b は，正答率が低かった。JPCERT/CC はインシデント対応に関する様々な活動を行っており，有用な情報を Web サイト上で提供しているので，是非，目を通しておいてほしい。

設問 3(1)d 及び e は，正答率が低かった。d では“バッファオーバフロー”，e では“POST”や“PUT”といった解答が目立った。Web に関する脆弱性は多岐にわたるが，代表的なものについては，用語を覚えるだけではなく，その内容を掘り下げて理解しておいてほしい。

設問 5 では，インシデントが発生した原因だけに着目した解答が見られた。パッチの適用や，フリーのソフトウェアのダウンロードの禁止などのセキュリティ対策は，インシデント予防の面から極めて重要であることは言うまでもない。しかし，今回のインシデントの原因をそれらの対策によって除去できたとしても，それだけでは不十分である。全く異なる原因によってインシデントが発生する場合や，いわゆるゼロデイ攻撃など，既知の予防策のないインシデントが発生することも想定しておく必要がある。そうしたインシデントに対しても適切に対応できるよう，原因究明のための情報確保が重要であることに気づいてほしかった。

Copyright(c) Information-technology Promotion Agency, Japan. All rights reserved 2010