平成 23 年度　特別　情報セキュリティスペシャリスト試験　採点講評

午後 I 試験

問 1

問 1 では，C++におけるバッファオーバフロー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 3 は，正答率が低かった。図 6 では領域の境界をプログラムで管理する必要がないことは問題中の記述から読み取れる。その上で，なぜ必要がないのか，代わりにどのような仕組みで管理するのかという点を具体的に解答してほしかった。これは類似の脆弱性を回避するために重要な点であり，確実に理解しておいてほしい。

設問 4 では，開発標準ルールの具体的な記述を問うた。プログラム開発では，脆弱性対策だけでなく品質確保の面からも，開発標準ルールを決めることは重要である。具体的な開発標準ルールなどを参考に学習してほしい。

問 2

問 2 では，ソフトウェア資産管理に関連する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 2 は，正答率が低かった。全社としての調査で初めて把握できる内容を解答してほしかったが，各部門の調査でも把握できるような誤った解答が散見された。

設問 4(2)は，正答率が低かった。セキュリティパッチの提供が終了したソフトウェアを抽出することの意義として，“新たな脆弱性が発見されたら速やかに対処できる”という解答も見られたが，脆弱性が発見されたとしても，開発元からセキュリティパッチは提供されない。このような危険な状況は，直ちに回避する必要がある。

設問 5 は，正答率が低かった。権限の集中による不正行為を防ぐために，“権限分離”又は“相互けん制”という考え方に基づき，ソフトウェアの利用者以外の第三者が登録することを理解してほしかった。

問 3

問 3 では，PC や記憶媒体による情報の社外への持出しを題材として，情報漏えい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 2 は，正答率が低かった。PC の持運びに関する注意点を問うているにもかかわらず，持運び自体を禁止するといった誤った解答が散見された。設問で何が問われているのかを，落ち着いて把握するようにしてほしい。

設問 3(2)は，正答率が高かったものの，認証やアクセス制限，DMZ の設置による Web サーバ自体の防御といった誤った解答が散見された。これらは，いずれも不正アクセスを防ぐための方法であり，設問で問われている不正アクセス後の被害の拡大防止には寄与しない。各種の対策がどのようなリスクに対して効果をもっているのかを，改めて確認しておいてほしい。

設問 4 は，正答率が低かった。マルウェア対策が困難な理由を問うたが，Web サーバへの感染拡大といったウイルス感染後の事象を述べた誤った解答が散見された。感染後に何が起こるかは，感染対策が困難であることとは直接の関係がないことを理解した上で解答してほしかった。

問 4

問 4 では，Web サイトの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(3)は，正答率が低かった。パスワード認証方式の SSH は，活発なブルートフォース攻撃によって危険性が高くなっているので，公開鍵認証方式の理解が不可欠である。

設問 1(4)は，ログを保存するという趣旨だけの誤った解答が多く見受けられた。FW のドロップログを分析することで様々なインシデントやその予兆を検知できることを理解しておいてほしい。

設問 1(5)は，正答率が低かった。本来ならば必要のないスクリプトファイルへのアクセス権限を付与することでリスクは増大する。最小権限の原則を改めて意識してほしい。

設問 2 は，ログイン試行の時間，アクセス元，回数に関しては触れていたが，ログイン試行の結果（成功又は失敗）に関する条件が欠けている解答が多く見られた。結果に関する条件を明確にしないで検知しようとすると誤検知が大量に発生してしまうことを覚えておいてほしい。

©2011　独立行政法人情報処理推進機構