平成 26 年度　春期　情報セキュリティスペシャリスト試験　解答例

午後 I 試験

問 1

出題趣旨
ソフトウェア開発での脆弱性対策では，特にプログラム作成プロセスにおいて，不用意なコーディングによって脆弱性を作り込んでしまう可能性が高く，細心の注意が必要である。そのため，脆弱性の作り込みを予防したり，脆弱性を発見したりするためには，ツールによる対処に加えて，プログラム作成者及びレビュアのセキュアプログラミングに関する知識と能力が重要なポイントとなっている。 本問では，Web アプリケーションでのファイルアップロードを題材に，脆弱性についての知識及びソースコードレビュー（静的解析）によって脆弱性を発見する能力を問う。

設問			解答例・解答の要点		備考
設問 1	(1)		Referer		
	(2)		ブラウザの設定でスクリプトを無効化する。		
	(3)		Web アプリケーションで拡張子判定を行う。		
設問 2	(1)	a	整数オーバフロー		
		b	バッファオーバフロー		
	(2)		ヘッダ部の列数と各ピクセルのバイト数の積にパディングを加えたものと，行数の積が kMaxInteger を超える。		
設問 3			ア群	イ群	同じ群中の組合せとする
		c	kMaxInteger / fhBuf.rows	kMaxInteger / bytesOfRow	
		d	bytesOfRow	fhBuf.rows	

問 2

出題趣旨
標的型攻撃では，標的となる特定個人に対して電子メールのやり取りが行われる場合が多く，企業における標的型攻撃の入口対策として，電子メールに関する情報セキュリティ対策の継続的な実施と見直しが重要になっている。 本問では，迷惑メールの増加を題材に，電子メールの情報セキュリティ対策のうち，標的型攻撃に使用される電子メールを含む迷惑メール対策に関する設計及び運用についての能力を問う。

設問			解答例・解答の要点	備考
設問 1	(1)	a	syslog	
	(2)	b	-all	
設問 2			インターネットから迷惑メール対策装置を経由せずに送られていた。	
設問 3	(1)		メールサーバの IP アドレスが変更された場合	
	(2)		迷惑メールの送信者がドメインを正当に取得した場合	
	(3)	c	プロキシサーバ	
		効果	迷惑メールの拒否率向上	
設問 4			SMTP 通信を迷惑メール対策装置に振り分ける。	

問３

出題趣旨
マルウェアへのセキュリティ対策を講じるには，攻撃手法を正しく理解するとともに，講じるセキュリティ対策についても，どういった攻撃手法に効果のある対策なのかを正しく理解する必要がある。 本問では，インターネットバンキングを題材に，マルウェアの攻撃手法に基づいて適切な対策方法を立案する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	フィッシングサイト		
	(2)	攻撃者はクライアント証明書がなく，ログインできないから		
設問２	(1)	利用者のブラウザに表示される警告画面を見て気付くことができる。		
	(2)	a	123456	
		b	10000	
		目的	マルウェアKが書き換えた口座番号と送金額を利用者に隠すこと	
設問３	(1)	c	対策になる	
		d	対策になる	
	(2)	e	二要素	
	(3)	利用者の PC がマルウェアに感染した場合，HMAC 計算ツールの入力内容も改ざんされる可能性がある。		