平成 27 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
近年，インターネット回線からのサイバー攻撃による被害が，大々的に報道されるようになった。現在，Web アプリケーションソフトウェアを利用するサービス事業にとって，サイバー攻撃への対策は必須である。Web アプリケーションソフトウェアの開発者には，脆弱性を作り込まないように，既知の対策を実施することに加えて，攻撃者が悪意をもって操作をした場合でも，問題が起きないような設計と実装を行うことが求められる。 本問では，よく知られた脆弱性である HTTP ヘッダインジェクション及びセッションフィクセーションを題材に，攻撃者の視点での攻撃方法を意識した，脆弱性の検出能力と，脆弱性への対策能力を問う。

設問			解答例・解答の要点	備考
設問１	(1)		画面 B	
	(2)		暗号化されない HTTP 通信において，セッション ID が送信されるから	
設問２	(1)	a	%0d%0a%0d%0a	
	(2)	b	ウ	
	(3)	c	・出力文字列に改行コードがあるとエラー画面を出力 ・出力文字列の改行コード以降の文字列を削除	
設問３	(1)	d	09　又は　17	順不同
		e	27	
	(2)	f	01234	
	(3)		攻撃者 J が取得したセッション ID で利用者 K にログインさせているから	
	(4)	g	新しいセッション ID によるセッションを開始する	

問 2

出題趣旨
近年，標的型攻撃又は新しいタイプの攻撃と呼ばれる外部からの攻撃が，業種や企業規模を問わず仕掛けられている。これらの攻撃ではソーシャルエンジニアリングと未知のマルウェアを組み合わせることによって，防御システムを回避して攻撃者が侵入し，長期間にわたりひそかに情報の窃取や破壊行為を行う。このような攻撃による情報漏えいインシデントの調査においては，情報漏えいを防ぎながら，侵入経路及び被害の特定を行う必要があり，適切な調査及び対策の計画立案及び実施が重要である。 本問では，運用担当者の PC へのマルウェア感染を題材に，未知のマルウェアによる情報セキュリティインシデントの調査及び対策を計画立案し，実施する能力を問う。

設問			解答例・解答の要点	備考
設問１	(1)		FW のログで当該通信の記録を確認する。	
	(2)	a	FW	
		b	プロキシサーバ	
		c	MAC アドレス	
設問２	(1)		DNS による名前解決ができず，TCP/IP 接続要求が出ないから	
	(2)		プロキシサーバで C&C サーバへの通信の URL をブラックリストに設定する。	
設問３	(1)		ファイル配信サーバからマルウェアを拡散する攻撃	
	(2)		V さんの利用者 ID の無効化	
	(3)		ログ管理サーバに保存されているログとの比較	

問３

出題趣旨
近年，ミドルウェアの脆弱性や Web アプリケーションソフトウェアの脆弱性を狙った攻撃被害の他に，Web サイトへの不正ログインの被害が多数報告されるようになった。こうした Web サイトへの不正ログインに対してセキュリティ対策を講じるには，Web サイト管理者と利用者のそれぞれが脅威を正しく理解する必要がある。 本問では，衣料品のショッピングサイトにおける不正アクセスを題材に，パスワード攻撃に対する正しい理解と，その脅威に対して適切な対策を講じる能力を問う。

設問		解答例・解答の要点		備考
設問１			多くの文字列のハッシュ値を計算したものと，漏えいしたファイル中のハッシュ値を突合し，パスワードを推測する攻撃	
設問２	(1)	a	32	
	(2)	b	単位時間当たりの同一 IP アドレスからのログイン試行数	
	(3)	c	多数の IP アドレス	
設問３		d	10^6	
		e	200	
		f	80^8	
設問４			他のサイトから流出した利用者 ID とパスワードの組合せによるパスワード攻撃	