平成 22 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
レースコンディションを発生させるバグは，通常の機能テストでの発見が困難である。さらに，レースコンディションに起因する脆弱性は，その原因の発見と対策に時間が掛かる。したがって，レースコンディションの正しい理解に基づいて，プログラムの設計及びコーディングの時点で十分な注意を払うことが必要である。 本問では，Web アプリケーション開発における脆弱性対策に必要な知識として，主にレースコンディションの仕組みとその対策についての理解を問う。

設問		解答例・解答の要点	備考
設問 1	a	バッファオーバフロー	
設問 2	(1)	インスタンス変数 tempPDF が複数のスレッドからほぼ同時に書き込まれたので，想定外の値となった。	
	(2)	・レースコンディション ・競合状態	
	(3)	インスタンス変数 tempPDF を doGet メソッドのローカル変数として定義する。	
	(4)	利用者 ID が異なる，多数の HTTP リクエストを，ほぼ同時に Web サーバに送信する。	
設問 3	(1)	他人の従業者番号を基に，勤務時間集計表の URL を推測し，ダウンロードを試みる。	
	(2)	b　PDF ファイル形式の勤務時間集計表	

問 2

出題趣旨
機密保護を実現する際には暗号化が有力な候補となるが，十分な検討を行わずに暗号化機能を導入すると，システム障害などが発生した際に，暗号化されたデータを復号することができず，結果として業務に支障を来してしまう可能性がある。 本問では，まず，暗号化とバックアップそれぞれについて，基本的な仕組みと，導入時に考慮すべき点を出題することによって，暗号化及びバックアップの導入に関する基本的な理解力を問う。続いて，暗号化とバックアップを同時に利用した場合に発生する問題と解決方法について出題することで，機密性と可用性の両面から施策を検討し，解決する能力を問う。

設問		解答例・解答の要点	備考
設問 1	(1)	a　ア	
		b　オ	
		c　カ	
	(2)	①　ウ	順不同
		②　エ	
	(3)	d　ア	
設問 2	(1)	バックアップテープを本社に宅配便で移送する際にテープが盗難に遭う。	
	(2)	・テープにデータをバックアップする際，暗号化する。 ・安全な移送サービスを利用する。	
設問 3	(1)	(b)	
	(2)	TPM が交換され，メールボックスファイル内の暗号化されたメールを復号するための秘密鍵が使えなくなったから	
	(3)	ファイル暗号化方式と S/MIME の鍵ペアを TPM 外で作成して安全にバックアップした後，TPM を用いて保管する。	

問３

出題趣旨
個人情報のように，送受信の際に暗号化が必要とされる情報を，企業間で安全に送受信するのは，容易なことではない。企業間の送受信において電子メールを暗号化することは難しい場合が多い。TLS（SSL）で保護されたWebページを利用するのも一つの方法であるが，正当な利用者であることを確認する必要がある。 本問では，暗号化，電子メール，パスワードなどに関する基本的な知識を前提として，具体的な状況に応じて解決策を提案できる能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	S/MIME 証明書	
		b	メール	
	(2)	証明書の正当性を確認できないから		
	(3)	紙媒体でフィンガプリントを入手する。		
	(4)	パスワードエラーが一定回数連続して発生したら，ログインを一定時間拒絶する。		
設問２	(1)	あて先に実在する求人企業の従業員からの申込みであることを確認するため		
	(2)	ランダムな文字列になるように生成する。		
	(3)	メールを盗聴し，利用者よりも先に再設定実行ページにアクセスする手口		
	(4)	パスワード再設定実行ページに，初期パスワードの入力を追加する。		

問４

出題趣旨
ウイルスには，ウイルス対策ソフトで検知，駆除ができないものもあり，その場合，そのウイルスに応じた対応が必要となる。 本問では，新種のウイルスの感染方法や感染後の動作の特徴などから，感染 PC の特定方法や，駆除手順，再感染防止策の立案について問う。

設問		解答例・解答の要点		備考
設問１		秘密情報の入ったファイルが攻撃者に盗まれる可能性		
設問２		a	ARP	
		b	IP アドレス	
		c	MAC アドレス	
		d	プロキシ	
		e	インターネット上の特定の Web サーバ	
設問３		X ウイルスに再び感染する。		
設問４	(1)	当該 PC と L2SW の間にファイアウォールを設置し，通信をパッチ配信サーバとの間に限定する。		
	(2)	f	管理者 ID のパスワードを推測しにくいものに変更する。	