平成 21 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
社内 LAN 上の異常を解析するツールとして，パケットモニタは有効である。ウイルスに感染した PC が外部と通信を行う際に DNS サーバを利用した名前解決を行うことが多く，DNS クエリに注目すると異常を特定しやすい。特に，スパムメールの踏み台になった PC の場合，メールの配送先を示す MX レコードを検索して，該当するメールサーバにスパムメールを送りつける。また，DNS 通信はステートレスな UDP プロトコルであるので，発信元 IP アドレスを詐称した DNS Reflection 攻撃の踏み台にされる危険性がある。 本問では，パケットモニタを利用して，このような異常を解析する手順と，DNS サーバの危険性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	**(1)**	**a**	(r)	
	(2)	**b**	ウ	
		c	詐称	
	(3)	**d**	イ	
	(4)	**e**	(Ⅱ)	
		f	(Ⅴ)	
		修正	インターネットからの A 社以外のドメイン上のアドレスに関する DNS クエリを拒否する。	
設問２	**(1)**	**不審な通信挙動**	・名前解決のために 3 台以上の DNS サーバと通信している。 ・A 社以外の DNS サーバに MX レコードを問い合わせている。	
		g	エ	
	(2)	ア，ウ		
設問３	**(1)**	・OS やアプリケーションが本来通信しないあて先ホストと通信するプロセス ・OS やアプリケーションが本来通信しないあて先ポートを利用するプロセス		
	(2)	ウイルス対策ソフトによるパターンファイルの更新確認パケット		

問2

出題趣旨
今日，システムの安全な運用を継続するためには，脆弱性情報の適切な取扱いと，修正プログラムの迅速な適用などの情報セキュリティ運用は，必須要件となっている。 本問では，コンピュータシステムの日常運用で必要とされる脆弱性管理のポイント，具体的には，日々公表される脆弱性情報に関して，その内容から自社システムにおいて必要な対応を決定するための判断，脆弱性が大きな問題となる Web サーバで使用される http の理解，OS，アプリケーションプログラムなどへ修正プログラムを適用する作業に関する理解について問う。

設問		解答例・解答の要点	備考
設問1	(1)	・攻撃者が指定したコマンドが実行されると，システムが全面的に停止するおそれがある。 ・管理者権限が奪われ，DB サーバ内の個人情報が漏えいする可能性がある。	
	(2)	・攻撃手法が公開されている。 ・Exploit コードを基にした攻撃が予想される。	
設問2	(1)	**a** form　又は　input	
	(2)	・Referer ヘッダにクエリストリングが記載されるので，リンク先などの外部サーバに入力データが送信されるおそれがある。 ・Web サーバのアクセスログにクエリストリングが記録されるので，ログから入力データが読み取られるおそれがある。	
	(3)	・X-Sender というフィールドを含んだ HTTP ヘッダを検出する。 ・HTTP ヘッダから X-Sender で始まる行を検出する。	
	(4)	**記号**　(f)	
		対策の内容　Web サーバプログラムの動作権限を必要最小限とする。	
設問3	(1)	**b**　・運用系から切り離す ・待機系にする ・スタンバイ状態にする	
	(2)	動作試験用システムで，修正プログラム適用後の動作の正常性を確認する。	

問3

出題趣旨
Web をベースとしたシステム開発が主流となっているが，アプリケーションレベルのセキュリティ対策は正しく実施されていないことがまだ多い。 本問では，Web アプリケーションに対する疑似侵入テストで，クロスサイトスクリプティング（XSS）への対応や，セッション管理の不備が見つかった状況，及び DB サーバに対する脆弱性診断で，格納しているデータ保護の不備が見つかった状況を想定し，それらの脆弱性に対する適切なアプリケーション設計，プログラミング手法，データベースセキュリティ対策などの理解を問う。

設問		解答例・解答の要点	備考
設問1	(1)	cookie にセットされたセッション識別子のうち，会員番号部分を他人のものに変える。	
	(2)	**行番号**　24	
		修正方法　・画像ファイルを相対パス名で指定する。 ・http の部分を https にする。	
	(3)	①　・タグの href 属性 ②　・タグのイベントハンドラ属性	
設問2	(1)	エ	
	(2)	・鍵付きハッシュ関数でパスワードからハッシュ値を算出して格納する。 ・パスワードとランダムな文字列を連結した文字列からハッシュ値を算出して格納する。	

問4

出題趣旨
近年，企業活動を支える情報システムの完全性を担保することが重要な課題となっている。特に上場企業においては，金融商品取引法の改正（いわゆる日本版 SOX 法）に基づき，重要なシステムの開発・運用プロセスにおける内部統制を評価，報告し，そのシステムが担う財務情報の適正性を立証することが求められている。システムの内部統制について理解し，評価や改善を行っていくためには，システムがもつ機能だけでなく，人による運用も含めた検討が必要であり，開発・運用にまたがる広範な知識とリスクに対する総合的な判断力が求められている。 本問では，システムの完全性を担保する重要な要素の一つである特権 ID の管理に焦点を当て，特権 ID 管理に関する知識と，機能と運用の両面から改善を行っていくための能力を問う。

設問		解答例・解答の要点		備考
設問1	**(1)**	イ		
	(2)	**a**	特権 ID の共用	
	(3)	**b**	ログのレビュー	
設問2	**(1)**	ア		
	(2)	**c**	syslog	
	(3)	**d**	ログサーバの特権 ID 使用者とほかのサーバの特権 ID 使用者を分離	
	(4)	特権 ID の認証が失敗したとき		
	(5)	**下線④**	システム管理者による不正行為の実行を抑止するため	
		下線⑤	・アラートの発生条件を回避しようとする行為を防止するため ・アラートが発生しないような不正使用方法を発見されないようにするため	
	(6)	**確認する内容**	・特権 ID で DB のデータを変更した処理のログに対応する特権 ID 利用申請書が提出されていること ・DB のデータを変更した処理が，すべて業務目的に基づいていること	
		立証しようとしていること	・DBMS 内の財務データが特権 ID によって改ざんされていないこと ・DBMS 内の財務データの完全性	