

平成 19 年度 春期 テクニカルエンジニア（情報セキュリティ）試験 解答例

午後 I 試験

問 1

出題趣旨	
情報システムの構成要素は多岐にわたるが、中でも顧客の要求に応じて開発されるアプリケーションプログラムのセキュリティ脆弱性を少なくすることは、ソフトウェアエンジニアリングとしても重要な課題である。 本問では、システム開発の過程で脆弱性低減のために実施すべき作業についての知識を確認した上で、脆弱性を発生させないための具体的なプログラミングにおける技術的対策に関する知識・能力を問う。	

設問	解答例・解答の要点		備考
設問 1	a	スタック	
	b	val2	
	c	val1	
	d	権限昇格	
	e	関数呼出し	
	f	ヒープ	
設問 2	(1) ア	128	
	(2)	・攻撃者に読取り権限のない任意のファイルの内容が表示されてしまう。 ・プログラムが意図したファイル以外の任意のファイルの内容が表示されてしまう。	
	(3)	・最初のコマンドライン引数が 128 バイト未満であるという条件を論理積として加える。 ・ <code>if (argc > 1 && strlen(argv[1]) < 128) {</code>	
設問 3	・変数と戻りアドレス格納部分の間に特別な数値をあらかじめ埋め込んでおき、この数値がプログラム実行時に変更されていないことを確認する。 ・変数と戻りアドレス格納部分の間に乱数値をあらかじめ埋め込んでおき、この乱数値がプログラム実行時に変更されていないことを確認する。		

問 2

出題趣旨	
ネットワークの構築において、ネットワークセキュリティの確保は避けて通れない。ネットワークセキュリティには、ネットワーク境界を守るファイアウォール（FW）、不正な通信を監視する IDS、監視に加えて遮断まで行う IPS などの対策がある。 本問では、FW のフィルタリングルールの設計、IDS や IPS に関する技術的な知識、導入検討における判断力などを問う。	

設問	解答例・解答の要点		備考
設問 1	(1) a	任意 又は 社内 LAN	
		b 任意	
	(2) c	拒否	
設問 2	(1) d	SSH	
	(2)	パスワードが平文で送信されるから	
	(3)	DMZ 上のサーバを踏み台にして、社内 LAN にアクセスする攻撃	
設問 3	(1) e	統計	
	(2) 下線⑤	正常なものまでも攻撃として検知してしまうエラー	
		下線⑥ 検知すべき攻撃を検知できないエラー	
	(3)	・パケットのヘッダ情報だけで攻撃か否かを判断しているから ・ペイロードの内容を見ていないから	
	(4)	攻撃を発見してから防御手段が有効となるまでの間に通過したパケットによる攻撃が、成功する場合があるから	

問3

出題趣旨	
近年、企業の社会的責任（CSR）がますます重要視されてきている。企業における多くの情報システムでセキュリティ上の機能として利用者の認証アクセス制御は行っているが、監査ログのセキュリティ対策は十分に行われていない。 本問では、監査ログの設計・開発を主題とし、監査ログの設計要件から監査ログメッセージの正当性を実現するために、ハッシュ関数、タイムスタンプ技術などの技術的対策を適切に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)	a 役割ベース 又は ロールベース	
	(2)	盗聴によるリプレイ攻撃を防ぐことができるから	
設問2	(1)	・利用者の認証やアクセス制御のすべての動作を記録し、その記録の有効性を確認できる。 ・後日の監査において IT による統制が正しく遂行されたことを確認できる。	
	(2)	b 役割 c 権限	順不同
	(3)	監査ログデータ 監査ログデータが改ざんされていないこと	
		複数の監査ログレコード ・監査ログレコード間の順序性 ・監査ログレコードの抜けがないこと ・監査ログレコードが挿入、削除されていないこと	
設問3	(1)	d ハッシュ値	
		e タイムスタンプ局 又は TSA 又は タイムスタンプオーソリティ	
	(2)	・監査ログバックアップファイルがタイムスタンプ発行時に存在していたこと ・監査ログファイルがタイムスタンプ発行時に存在していたこと	

問4

出題趣旨	
セキュリティ機能を具備したシステムの設計においては、様々なアルゴリズムを適切に選択し、使用する必要がある。 本問では、社内アンケートシステムを題材に、公開鍵暗号に関する基礎知識、及びプライバシー保護を伴うセキュリティシステムの方式設計能力を問う。	

設問	解答例・解答の要点		備考
設問1	(1)	a 秘匿 又は 隠ぺい 又は 読めなく	
		b 8	
	(2)	全通りの回答について提出ファイルを作成し、回答者のファイルと比較する。	
設問2	(1)	① ・集計担当者以外はアンケートの回答を閲覧できないこと ② ・従業員が匿名でアンケートに回答できること ・部門の担当者が提出漏れをチェックできること ・アンケートの回答を1人1回答に制限できること	
	(2)	シリアル番号とその署名は各回答者しか知り得ず、また、シリアル番号の偽造は困難であるから	
設問3	(1)	シリアル番号から回答者を特定できないようにする必要があるから	
	(2)	・同じシリアル番号の回答がないかどうかをチェックする。 ・使用していないシリアル番号の回答がないかどうかをチェックする。	