

平成 20 年度 秋期 情報セキュリティアドミニストレータ試験 解答例

午後 試験

問 1

出題趣旨	
社内システムの再構築など，システムの新規開発や更改に際しては，リスクアセスメントの実施と，その結果に基づくセキュリティ要件の検討が不可欠である。さらに，昨今では，金融商品取引法に基づく内部統制実現という視点も欠くことはできない。 本問では，情報セキュリティアドミニストレータが行うべき，リスクアセスメントとセキュリティ要件の検討を主題とし，情報セキュリティアドミニストレータが責任の一端を担うであろう，セキュアなシステム構築に求められる技術知識，マネジメント面での対応策の立案能力・実施能力・管理能力などを評価する。	

設問	解答例・解答の要点		備考
設問 1	(1)	a オ	
		b イ	
	(2)	c ・暗号化されたウイルス付き添付ファイルの復号時の感染 ・Web 経由でのウイルス感染 ・外部記録媒体経由でのウイルス感染	
		d ・パターンファイル更新のベンダによるばらつき ・特定ベンダのパターンファイル更新不備	
設問 2	(1)	利用者 ID の共用を廃止し，個人別に異なる利用者 ID を発行してログに記録する。	
	(2)	・発注担当者の入力した内容が，発注依頼票どおりであることを，上長がシステムの画面上で確認の上で承認し，発注を確定する。 ・電子化された発注依頼票の内容と，発注入力された内容を，上長が画面上で見比べて確認してから，システム上で発注を承認する。	
設問 3		・パスワードを本人に通知する過程で漏えいするリスクがあるから ・その利用者 ID を利用した者が，確実に本人であることを保証できないから	
設問 4	(1)	・発注担当者の利用者 ID ・発注品目 又は 品目 ・発注数量 又は 数量 ・取引先コード 又は 取引先名 ・発注番号	
	(2)	使用量を常時監視し，所定量に達したら自動的に外部記憶媒体に退避する。	
	(3)	・要さい化した専用のログサーバを設置し，ログを集約する。 ・接続可能なポートを制限したログサーバにログを集約する。	
	(4)	・取得したログの放置による不正行為の見逃ごしの回避 ・ログの見える化による不正行為検出率の向上 ・セキュリティ対策の不備を発見できる可能性の向上	
	(5)	利用者の不正行為を抑止することができること	
設問 5	(1)	権限が強すぎる特権 ID の共用	
	(2)	必要最小限の特権だけを付与した特権 ID を，利用者ごとに個別に付与する。	

問 2

出題趣旨	
適切な情報セキュリティ管理においては、情報セキュリティインシデントの予防措置に加えて、情報セキュリティインシデントが発生した場合の適切な対処の仕組みが欠かせない。後者においては、限られた時間での素早い対応や、組織の内外にわたる様々な部署との連携、通常時とは異なる権限管理や承認プロセスが必要となる。 本問では、情報セキュリティインシデントに対する不適切な対応への反省に基づいた情報セキュリティインシデントへの対応体制の整備を例に、情報セキュリティアドミニストレータとして理解しておくべきインシデント対応に関する知識、及び対応体制の整備についての知識と経験を問う。	

設問		解答例・解答の要点		備考
設問 1	ア	スクリプト 又は プログラム 又は コード		
	イ	インラインフレーム中にフィッシングサイトのコンテンツを表示させる HTML に差し替える		
設問 2	a	オ		順不同
	b	エ		
	c	ア		
	d	ウ		
設問 3	(1)	・ 収集した脆弱性情報が、自社のシステムに影響するかどうかを判断できるから ・ インシデント発生時に、影響を受ける範囲を速やかに判断できるから		
	(2)	インシデントの 対応側にとっての 利点	・ インシデントに関する情報を集約することで、インシデントの重要性を正確に判断できること ・ インシデントに関する問合せに対して、統一方針に基づいた対応ができること	
		社内の インシデント 発見者にとっての 利点	・ インシデントの内容に応じた報告先の変更をインシデント発見者が考える必要がないこと ・ インシデント発見者が、報告先を迷わずに済むこと	
設問 4		電子署名を検証し、署名者の証明書が Y 社のものであることを確認する。		
設問 5	(1)	・ 通販会員情報の漏えいにつながる可能性があるから ・ 利用者が多いので、被害の拡大が急速であるから		
	(2)	夜間又は休日に発生したインシデントが翌営業日まで対応されないこと		
	(3)	Z 社で対応すべきインシデントの範囲と対応方法		
	(4)	・ システム企画課の従業員及び IRT メンバに対する Z 社からの夜間及び休日の連絡方法 ・ システム企画課の従業員と IRT メンバを含めた、Z 社からの夜間及び休日の連絡網の整備		