

平成22年度 春期 情報セキュリティスペシャリスト試験 午後自己採点
(TAC/ITEC解答例を使用)

午後1

問2

設問1(1)a	ア	○	3
b	オ	○	3
c	カ	○	3
(2)	ア、イ	×	0
(3)	ア	○	3
設問2(1)	暗号化されていないバックアップを保存したテープを配送中に紛失する可能性	○	6
(2)	配送記録のある安全な宅配便サービスを利用する	×	0
設問3(1)	b	○	6
(2)	S/MIMEで暗号化されたものは、暗号化されたままバックアップされているため	△	2
(3)		×	0

問3

設問1(1)a	クライアント証明書	△	2
b	メーラー	△	2
(2)	ルートCAを利用できず、証明書の正当性を確認できないため	○	6
(3)	公的に信頼できる公開鍵登録サーバを用いて、対象相手を確認する	×	0
(4)	一定回数以上ログインに失敗したら、該当するアカウントを一時的に無効化する	○	6
設問2(1)	なりすましの不正な相手に送付しないように、公的に信頼できる情報を用いて郵送	○	6
(2)	擬似乱数を用いて、第三者が推測できないように生成する	○	6
(3)	パスワード再設定用のURLを含むメールを盗聴され、先に再設定される	○	6
(4)	パスワードの再設定をする際に、旧パスワードを入力させるようにする	×	0

合計点 60

午後2
問2

設問1(1)a	プライバシーマーク	○	4
b	CERT	×	0
(2)	連絡を迅速にできて、インシデントの原因究明を早急に行える点	○	6
(3)	当社が保守サポートを提供している対象に、異常、不具合が発生した場合	○	6
設問2(1)	ログは所定のタイミングでログ管理サーバにコピーする	×	0
(2)	社内にセキュリティ情報を提供する際に、発信者の正当性を示す目的	○	6
設問3(1)c	ログに記録	○	6
d	ディレクトリトラバース	○	4
e	TRANSFER	×	0
(2)	Webサーバが様々な攻撃の踏み台にされ	△	2
(3)理由	大量の警告メールに埋もれ、対応すべき深刻な脅威を見逃す可能性があるため	○	6
条件	X社では対策済みで、IPSで遮断しなくても問題が発生しない場合	○	6
設問4(1)	再起動により、インシデントの原因究明に必要な情報が失われる可能性があるため	○	6
(2)	インシデントの証拠収集に必要な情報を確実に保全するため	×	0
設問5問題(1)	証拠収集を行なう前に担当者がサーバをシャットダウン、電源を切断したこと	○	6
対応(1)	インシデント発生時はネットワークから切断し、証拠収集が済むまで操作しない	○	6
問題(2)	無断でサーバ機を開発系ネットワークに接続したこと	○	6
対応(2)	ネットワークに機器を接続する場合は、システムの構成情報に登録を済ませる	○	6

合計点 76