第４問　情報資産についてのリスクアセスメントに関する次の記述を読んで、設問１～３に答えよ。

K社は、従業員300名ほどの独立系SIerである。K社では、顧客から請け負ったシステム開発を一つのプロジェクトとして管理しており、プロジェクト開始前に、そのプロジェクトで使用する情報資産についてのリスクアセスメントを実施している。この度、新たに受注したプロジェクトSに対して、リスクアセスメントを行うことになった。

〔プロジェクトSの説明及び開発環境（抜粋）〕

(1) 顧客のテストデータは、メールに添付されプロジェクトメンバ共通のメールアドレス宛てに送付される。受信後、顧客のテストデータを開発用サーバに複写後、メールの添付ファイルは削除する。
(2) プログラム開発には、開発用サーバと開発用PCを使用する。
(3) 開発用PCは、プロジェクトごとにシステム部からプロジェクトメンバに貸与され、プロジェクト終了後に返却する。

〔K社の開発標準（抜粋）〕

(1) 開発時、プロジェクトメンバは顧客のテストデータのうち必要なものだけを、開発用サーバから自分の開発用PCにダウンロードし、不要になったら削除する。
(2) プロジェクト終了後に、プロジェクトマネージャは開発用サーバの顧客のテストデータを削除し、全ての開発用PCから顧客のテストデータが削除されていることを確認する。

〔リスクの特定及び、数値化〕

K社では、各情報資産のリスク値を、次の式で算出する。

リスク値　＝　情報資産の価値　×　脅威　×　脆弱性

ここで、“情報資産の価値”とは機密性・完全性・可用性の三つの観点に対して、影響の大きさをそれぞれ１～３の値で評価する。K社では、機密性・完全性・可用性ごとに算出したリスク値が10以下ならばリスクを受容し、一つでもそうでないものがあれば追加のリスク対策を講じることにしている。

① 情報資産及び価値の数値化

ここでは、顧客のテストデータについて、機密性、完全性、可用性のそれぞれについての価値を評価し数値化した。

表１　情報資産の価値

No	情報資産	機密性	完全性	可用性
1	顧客のテストデータ	3	2	1

② 脅威及び脆弱性の数値化

①の情報資産のうち、No.1について脅威の内容と脅威の値、脆弱性の低減策及び、脆弱性の値を表２に示す。ここで脆弱性の値は、二つ以上の対策が取られていれば１、一つだけなら２、未対策であれば３とする。

表２　情報資産No.1の脅威及び脆弱性の値

ID	脅威の内容	値	脆弱性の低減策	値
T-1	顧客のテストデータを添付したメールが誤って削除される	1	・メールのバックアップを取る	2
T-2	開発用サーバに複写後、メールの添付ファイルを削除し忘れ、誤送信されることにより漏えいする	3	・(a)	2
T-3	ウイルス感染によって顧客のテストデータの破壊又は漏えいが発生する	3	・開発用サーバと開発用PCにウイルス対策ソフトを導入し、パターンファイルを自動更新する ・受信したメールのウイルスチェックを実施してから、顧客のテストデータを開発用サーバに複写する	1
T-4	開発用サーバが外部から不正アクセスされて、顧客のテストデータが盗み出される	1	・対策はとっていない	3
T-5	テスト終了後、顧客のテストデータが開発用PCから漏えいする	2	・(b)	2
T-6	開発用サーバから顧客のテストデータが滅失する	1	・対策はとっていない	3

〔リスクの分析評価〕

上記の表を基に、情報資産No.1のリスク分析評価を行い、リスク値を算出した結果を、表３に示す。

表３　情報資産No.1のリスク値

No	情報資産の価値			脅威		脆弱性	リスク値		
	機密性	完全性	可用性	ID	値	値	機密性	完全性	可用性
1	3	2	1	T-1	1	2			
				T-2	3	2			
				T-3	3	1			
				T-4	1	3			
				T-5	2	2			
				T-6	1	3			

※網掛けの部分は、設問のため表示していない。

設問１　表２の空欄(a)，(b)に入れる正しい低減策を、解答群の中から選べ。

解答群

ア　添付されていた顧客のテストデータがメールから削除されていることをプロジェクトマネージャが確認する
イ　開発用PCから顧客のテストデータが削除されていることをプロジェクトマネージャが確認する
ウ　開発用PCから顧客のテストデータが削除されていることを開発者が確認する
エ　開発用サーバと開発用PCにウイルス対策ソフトを導入し、パターンファイルを自動更新する
オ　対策はとっていない

設問２　情報資産No.1に対するリスク分析評価の結果、受容可能なリスクの数として正しい答えを、解答群の中から選び、(c)に答えよ。

解答群

ア　１　　イ　２　　ウ　３　　エ　４　　オ　５　　カ　６

設問３　プロジェクトＳが終了後、別のプロジェクトで開発用PCを使用した際、顧客のテストデータが残っている事象が発生した。今後、顧客のテストデータが漏えいしないようにするために追加するべき対応はどれか。解答群より二つ選び、(d)，(e)に答えよ。

解答群

ア　アクセスログを取得し、定期的に確認を行う
イ　開発用PCは個人の物を使用するように変更する
ウ　管理台帳に、顧客のテストデータのダウンロード日、削除日、実施者を記入し、確認者の押印を必要とする
エ　開発用PCが返却された際に、システム部が全データの消去を実施する
オ　直前のプロジェクトで使用した開発用PCはすぐには使用せず、時間をおいてから別のプロジェクトに使用する