次の問1は必須問題です。必ず解答してください。

問1　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。

Z社は，従業員数が500の中堅SIベンダである。Z社では，プロジェクト開始前に，プロジェクトで扱う情報資産について，図1に示す自社で定めた手順に従って，リスクアセスメントを実施している。このたび，新規に受注したプロジェクトYに対して，リスクアセスメントを実施することになった。

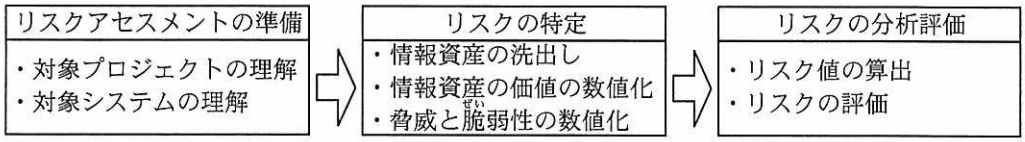

図1　Z社のリスクアセスメントの手順

〔プロジェクトYの説明（抜粋）〕

(1)　顧客が利用する購買システムを開発する。

(2)　開発で利用するテストデータは顧客から提供される。

(3)　顧客のテストデータを格納した顧客のUSBメモリを，プロジェクトメンバが顧客から受け取って自社に持ち帰り，顧客のテストデータを開発用サーバに複写後，USBメモリから削除する。

(4)　Z社から顧客の事務所を訪問するのに，電車で1時間30分ほど要する。

(5)　開発用PCでプログラムを開発し，適宜，開発用サーバにアップロードする。

〔Z社の開発環境（抜粋）〕

(1)　プログラムの開発には，開発用サーバと開発用PCを利用する。

(2)　開発用サーバは，施錠されたサーバルームに設置されている。

(3)　開発用サーバは，アクセス管理がされており，プロジェクトメンバとシステム管理者だけがアクセスできる。

(4)　開発用PCは，プロジェクト開始時にシステム部から各プロジェクトメンバに貸与され，プロジェクト終了時に返却される。

h26sp01情報セキュリティ_資産のリスクアセスメント.pdf

〔Z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) プロジェクト終了時に，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。

〔Z社のリスク値算出方法〕

Z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”とは情報資産が損なわれたときの影響の大きさを意味し，機密性（以下，Cという），完全性（以下，Iという），可用性（以下，Aという）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。“脅威”は，発生の可能性の大きさを1～3の値で評価する。“脆弱性”は，脅威が発生した場合に被害が顕在化する度合いの大きさを1～3の値で評価する。ここで，各1～3の値は大きい場合を3，小さい場合を1とする。

C，I，Aごとに算出したリスク値が全て12以下ならばリスクを受容し，そうでないならば追加のリスク対策を実施することにしている。

〔リスクの特定〕

① 情報資産の洗出し

プロジェクトYで扱う情報資産の洗出しを行った。その結果を，表1に示す。

表1 情報資産の洗出し結果

No.	情報資産	作成又は取得	保管場所	廃棄
⋮				
3	開発用サーバ上の開発中のプログラム	プロジェクトメンバが開発用サーバにアップロードする	開発用サーバ	プロジェクト終了時に削除する
4	顧客のテストデータ	顧客のUSBメモリで受領して，開発用サーバに複写する	顧客のUSBメモリ，開発用サーバ及び開発用PC	
⋮				

注記 網掛けの部分は表示していない。“…”は表示の省略を示している。

h26sp01情報セキュリティ_資産のリスクアセスメント.pdf

② 情報資産の価値の数値化

表 1 の各情報資産に対して，C，I，A のそれぞれについてその価値を評価した値と評価理由を，表 2 に示す。

表 2　情報資産の価値と評価理由

No.	情報資産	C	I	A	価値の評価理由
⋮					
3	開発用サーバ上の開発中のプログラム	3	3	3	(i) 開発中のプログラムが利用できない場合，プロジェクトの進捗に影響を与える (ii) 社外に漏れた場合，顧客からの信頼を失う (iii) 版管理が行われない場合，不整合によって，プロジェクトの進捗に影響を与える
4	顧客のテストデータ	3	2	1	
⋮					

注記　網掛けの部分は表示していない。“…”は表示の省略を示している。

③ 脅威の数値化

表 2 の情報資産のうち，情報資産 No.4（顧客のテストデータ）について，脅威の内容と脅威の値を，表 3 に示す。

表 3　情報資産 No.4 の脅威の内容と値

No.	脅威 ID	脅威の内容	値
4	T1	顧客のテストデータを格納した顧客の USB メモリを自社に持ち帰る途中で紛失する	3
	T2	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
	T3	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	2
	T4	開発用サーバに複写後，顧客の USB メモリから顧客のテストデータが漏えいする	3
	T5	テスト終了後，不要になった顧客のテストデータが開発用 PC から漏えいする	2
	T6	プロジェクトメンバ又はシステム管理者が顧客のテストデータを開発用サーバから取り出してサーバルームから持ち出す	1
	T7	開発用サーバから顧客のテストデータが滅失する	1

h26sp01情報セキュリティ_資産のリスクアセスメント.pdf

④　脅威に対する脆弱性の数値化

表3の各脅威に対する脆弱性の低減策と脆弱性の値を，表4に示す。脆弱性の値は，システム，規則又は運用で，二つ以上対策済みなら 1，一つだけなら 2，未対策は3とする。

表4　表3の脅威に対する脆弱性の低減策と値

脅威 ID	脆弱性 ID	脆弱性の低減策	値
T1	Z1	・顧客の USB メモリに顧客のテストデータを保存するときに暗号化してもらう	2
T2	Z2	・脆弱性に対する対策なし	3
T3	Z3	・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，ウイルス定義ファイルを自動更新する ・顧客の USB メモリをウイルスチェックした後に顧客のテストデータを開発用サーバに複写する	1
T4	Z4	・顧客の USB メモリ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	2
T5	Z5	・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	2
T6	Z6	・社員証による入退室管理を行う ・サーバルームに監視カメラを設置する	1
T7	Z7	・脆弱性に対する対策なし	3

〔リスクの分析評価〕

表2～4を基に情報資産 No.4（顧客のテストデータ）のリスクの分析評価を行い，リスク値を算出した結果を，表5に示す。

表5　情報資産 No.4 のリスク値

No.	情報資産の価値			脅威		脆弱性		リスク値			
	C	I	A	脅威 ID	値	脆弱性 ID	値	リスク値 ID	C	I	A
4	3	2	1	T1	3	Z1	2	R1	18	12	6
				T2	1	Z2	3	R2	9	6	3
				T3	2	Z3	1	R3			
				T4	3	Z4	2	R4			
				T5	2	Z5	2	R5			
				T6	1	Z6	1	R6			
				T7	1	Z7	3	R7			

注記　網掛けの部分は表示していない。

h26sp01情報セキュリティ_資産のリスクアセスメント.pdf

プロジェクト Y のプロジェクトマネージャは，リスクの分析評価の結果からリスク対応計画を作成した。その後，リスク対策を実施した。

設問 1　表 2 中の（ii），（iii）は，C，I，A のいずれかの観点から“情報資産の価値”を評価した際の評価理由である。（ii），（iii）に対応する C，I，A の組合せとして適切な答えを，解答群の中から選べ。

解答群

	(ii)	(iii)
ア	A	C
イ	A	I
ウ	C	A
エ	C	I
オ	I	A
カ	I	C

設問 2　情報資産 No.4（顧客のテストデータ）に対するリスクの分析評価の結果，追加のリスク対策が必要になる脅威の数として正しい答えを，解答群の中から選べ。

解答群

ア 1　　イ 2　　ウ 3　　エ 4

h26sp01情報セキュリティ_資産のリスクアセスメント.pdf

設問3　社内でのセキュリティ事故の発生と対策に関する次の記述中の［　　］に入れる適切な答えを，解答群の中から選べ。

プロジェクトYの終了後，新たに発足したプロジェクトXで利用している開発用PCに，プロジェクトYの顧客のテストデータが格納されている，とシステム部に連絡があった。調査した結果，このPCは，プロジェクトYで利用していた開発用PCであり，システム部に返却された後に，システム部からプロジェクトXに貸与されたものであることが判明した。そこで，Z社では，顧客のテストデータの漏えいというリスクに対処するために，［a］，［b］という対策を追加することにした。

解答群

ア　開発用サーバのアクセスログをシステム部が定期的に確認する

イ　顧客のテストデータを開発用PCにダウンロードして利用する場合は，管理台帳にダウンロード日，削除日，実施者を記入する

ウ　顧客のテストデータを開発用PCに保存する際に，警告メッセージが表示されるようにする

エ　プロジェクトごとに新たに開発用サーバを用意する

オ　プロジェクトメンバが開発用サーバ上の顧客のテストデータにアクセスする権限を参照だけに設定する

カ　返却された開発用PCは，システム部が全データを完全消去する工程を追加する

h26sp01情報セキュリティ_資産のリスクアセスメント.pdf