●平成26年度春期

午後問題 解答・解説

問1　情報資産についてのリスクアセスメント（情報セキュリティ）(H26春-FE 午後問1)

【解答】

［設問1］　エ

［設問2］　イ

［設問3］　a－イ，b－カ（a，bは順不同）

【解説】

リスクアセスメントに関する問題である。このテーマは，日常的に行う業務ではなく，問題文中で独自に定義されている用語の数が多い。難しいと感じた人もいるだろう。しかし，問題文を丁寧に読むことで，確実に正解にたどり着くことができる。

とはいえ，正解するには情報セキュリティに関する最低限の基礎知識が必要である。情報セキュリティの問題は必須問題である。最低限の基礎知識を学習しておくことで，いろいろな問題に対応できるようにしておきたい。

この問題を解くに当たり，いきなり設問を解くのではなく，問題文をきちんと理解してから設問を解いていくとよい。問題文は長文ではあるが，問題文には，設問を解くためのヒントが埋め込まれているからである。また，問題文をきちんと読み込むことで，リスクアセスメントの基本的な進め方と用語を理解することができる。

設問3は二つとも正解できないかもしれないが，設問1と設問2は確実に取りたい問題である。

［設問1］

まず，C，I，Aの定義を問題文にて確認する。Cは機密性，Iは完全性，Aは可用性を意味する。ここで，（ii）と（iii）がC，I，Aのどれに対応するかを考える。

まず，（ii）は，問題文に「社外に漏れた場合，顧客からの信頼を失う」とある。「社外に漏れ」という言葉から，機密として管理した情報が漏れるというリスクであること分かる。つまり，機密性のCが該当する。

次に（iii）であるが，「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」とある。「不整合によって」という言葉から，データの完全性が保たれないというリスクであることが分かる。つまり，完全性のIが該当する。

（iii）は，少し理解に苦しんだかもしれない。そんなときは，消去法も活用するとよい。

（i）を見ると，「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」とある。「利用できない場合」という言葉から，可用性が脅かされるリスクであることが分かる。つまり，Aの可用性が該当する。仮に（iii）が分からなかったとしても，（i）と（ii）の答えから（iii）を導き出すことができる。

したがって，正解は，（ii）がC，（iii）がIであることから，（エ）となる。

参考ではあるが，CIAのフルスペルは，機密性（Confidentiality），完全性（Integrity），可用性（Availability）である。

［設問2］

情報資産No.4（顧客のテストデータ）のリスクの分析評価は，表2～4を基に行うことが問題文に述べられている。また，その結果は表5にまとめられている。しかし設問の関係上，注記にあるように，網掛けの部分は表示されていない。この網掛け部分の具体値を計算することが解答に際して必要となるため，まずは表5を完成させる。

リスク値の求め方は，問題文に次のように解説されている。

リスク値　＝　情報資産の価値×脅威×脆弱性

これに従い，表5を完成させる。例えば，T3のリスク値Cで言うと，情報資産の価値は3，脅威は2，脆弱性は1である。よって，3×2×1＝6がリスク値となる。これを全ての脅威に対して計算すると，次のようになる。

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	6	4	2
				T4	3	Z4	2	R4	18	12	6
				T5	2	Z5	2	R5	12	8	4
				T6	1	Z6	1	R6	3	2	1
				T7	1	Z7	3	R7	9	6	3

設問では，「追加のリスク対策が必要になる脅威の数」が問われている。どんな場合に追加のリスク対策が必要になるのか，問題文で確認すると，「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」とある。

よって，作成した表5の中で，「リスク値が全て12以下」ではないものを探す。言い変えると，「リスク値が12より大きいものが一つ以上ある」リスクを探す。ここで，12の値は含まれないことに注意する。

リスクIDがT1とT4の二つは，Cのリスクが18であるため，追加のリスク対策が必要になる。したがって，（イ）の2が正解となる。

［設問3］

データ漏えいを防ぐための対策が求められている。一見すると，どの対策も有効のように見えるが，効果のあるものは二つだけである。

まず，今回の問題点を整理する。〔Z社の開発標準（抜粋）〕には，次の記載がある。

(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。

今回の問題は，このような開発標準があるにもかかわらず，(1)について，PCにダウンロードしたテストデータを削除しなかったことが問題である。また，(2)について，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きちんと確認しなかったことも問題である。この点を頭において解答群を見ていくと理解しやすい。

まず，（ア）であるが，「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」とある。しかし，アクセスログを確認したとしても，開発用PCの顧客データを削除することはできない。

次に（イ）であるが，「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」とある。この情報があれば，プロジェクトが終了したタイミングなどで，ダウンロードした実施者のPCから，データが削除されているかを確認できる。又は，削除日が入っていないPCに対し，テストデータを削除するように指示してもよい。つまり，情報漏えい対策として有効である。

（ウ）は，「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」とある。しかし，警告メッセージが表示されても，PCに保存してしまうことになるから，効果はない。

（エ）は，「プロジェクトごとに新たに開発用サーバを用意する」とある。こちらも，PCに保存されたデータを消すことには関係がない。

（オ）は，「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」とある。上書きなどの書き込み権限が付与されなかったとしても，参照できればデータを閲覧することができる。閲覧できればなんらかの方法で保存もできる。よって，データの漏えいのリスクは残る。

（カ）は「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」とある。この工程を追加することで，データの削除が確認できるので，データ漏えい対策として有効である。

以上のことから，（イ）と（カ）が正解となる。