問題５　次のセキュリティに関する記述を読み各設問に答えよ。

企業などの組織が情報セキュリティを確立するためのルールをセキュリティポリシーと呼ぶ。これに基づき，リスクに対する技術的な対策だけでなく，組織としてリスクへ対応するようにマネジメントし，自らのプランを持ってシステム運用することを ISMS(Information Security Management System)と呼ぶ。

ISMS を第三者機関が認定する制度が ISMS 適合性評価制度である。

＜設問１＞　次の ISMS に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ISMS の基本的な考え方として，情報資産に対する［　(1)　］性，［　(2)　］性，［　(3)　］性をバランス良く維持し改善することがある。

［　(1)　］性とは，アクセス権を持つ者に対してのみ，情報資産をアクセスさせることである。

［　(2)　］性とは，情報や処理方法が正確であること，および，情報が改ざんされていないことを保証することである。

［　(3)　］性とは，必要なときに情報資産へアクセスできることである。

ISMS 適合評価制度は，日本情報処理開発協会(JIPDEC)によって 2002 年から運用が開始されており，(a)企業などがこの認証を受けることで，情報セキュリティの運用が適切に行われていることを対外的にアピールし，信頼感を得ることができる。

企業を取り巻く環境は常に変化しているので，(b)ISMS の運用を定期的に評価し，必要に応じて改善や見直しをしなければならない。

(1) ～ (3) の解答群

ア．可能	イ．可用	ウ．完全
エ．危険	オ．機密	カ．保守

＜設問２＞　ISMS は３つのフェーズで確立する。各フェーズの順番を解答群から選べ。

表　ISMS のフェーズと内容

	フェーズ	内容
A	ISMS の適用範囲および基本方針の確立	事業内容および組織の規模，情報資産などを考慮して ISMS の適用範囲を決定する。
B	リスクアセスメントに基づく管理策の選択	組織が保護すべき情報資産に対するリスクを明確にし，そのリスクを受容するか，対応が必要かを判断する。
C	リスクについて適切に対応する計画を策定	管理策とその選択理由を適用宣言書として作成し，これを残留リスクとともに経営陣が承認する。

(4) の解答群

ア．A→B→C　　イ．A→C→B

ウ．B→A→C　　エ．C→B→A

＜設問３＞　設問１の下線（a）の企業が認証を受ける機関を解答群から選べ。

(5) の解答群

ア．JIPDEC　　イ．JIPDEC が認定した認証機関

ウ．経済産業省　　エ．地方自治体

＜設問４＞　設問１の下線（b）は下記の作業内容をどの順番で進めるべきか解答群から選べ。

［作業内容］

A 計画に従った情報セキュリティ対策を導入し運用する。

B 実施した情報セキュリティ対策を監視する。

C 情報セキュリティ対策に関する具体的な計画や目標を決定する。

D 情報セキュリティ対策を評価して改善や見直し行う。

(6) の解答群

ア．A→D→B→C　　イ．B→A→C→D

ウ．C→A→B→D　　エ．D→C→B→A

＜設問５＞　次のセキュリティの脅威に関する各記述に関係の深い字句を解答群から選べ。

(7) データベースを利用するプログラムの不備を利用して，データベースに不正アクセスする。

(8) Web サーバの処理能力を超えるようなリクエストを何度も送り，使用不能な状態にしてしまう。

(9) サーバに対して,どのサービスが利用できるかを調べるため接続口にアクセスし,侵入口となるかを調べる。

(10) データを一時的に蓄えるメモリ上に確保した領域を超えるデータを送ることで,他のプログラムで使うメモリ上の領域を上書きして誤動作させ，サーバの機能を停止させる。

(7) ～ (10) の解答群

ア．DoS 攻撃　　イ．SQL インジェクション
ウ．トロイの木馬　　エ．バックドア
オ．バッファオーバフロー　　カ．フィッシング
キ．ポートスキャン　　ク．ボット