

## 問2 情報システムの運用段階における情報セキュリティに関する監査について

企業などでは、顧客の個人情報、製品の販売情報などを蓄積して、より良い製品・サービスの開発、向上などに活用している。一方で、情報システムに対する不正アクセスなどによって、これらの情報が漏えいしたり、滅失したりした場合のビジネスへの影響は非常に大きい。したがって、重要な情報を取り扱うシステムでは、組織として確保すべき情報セキュリティの水準（以下、セキュリティレベルという）を維持することが求められる。

情報セキュリティの脅威は、今後も刻々と変化し続けていくと考えられるので、情報システムの構築段階で想定した脅威に対応するだけでは不十分である。例えば、標的型攻撃の手口はますます高度化・巧妙化し、情報システムの運用段階においてセキュリティレベルを維持できなくなるおそれがある。

そこで、情報システムの運用段階においては、セキュリティレベルを維持できるように適時に対策を見直すためのコントロールが必要になる。また、情報セキュリティの脅威に対して完全に対応することは難しいので、インシデント発生に備えて、迅速かつ有効に機能するコントロールも重要になる。

システム監査人は、以上のような点を踏まえて、変化する情報セキュリティの脅威に対して、情報システムの運用段階におけるセキュリティレベルが維持されているかどうかを確かめる必要がある。

あなたの経験と考えに基づいて、設問ア～ウに従って論述せよ。

設問ア あなたが関係する情報システムの概要とビジネス上の役割、及び当該情報システムに求められるセキュリティレベルについて、800字以内で述べよ。

設問イ 設問アを踏まえて、情報システムの運用段階においてセキュリティレベルを維持できなくなる要因とそれに対するコントロールを、700字以上1,400字以内で具体的に述べよ。

設問ウ 設問イで述べたコントロールが有効に機能しているかどうかを確認する監査手続を、700字以上1,400字以内で具体的に述べよ。