第４問　情報セキュリティにおけるリスクに関する次の記述を読んで、設問１，２に答えよ。

Ｔ君の所属するＫ社では、自社の情報セキュリティにおけるリスクを数値化して管理することになり、基準を設定して所有する情報資産のリスク評価を行うことになった。Ｔ君はこのうち、業務サーバのリスク評価を担当した。

［リスクの値の算出］

Ｋ社では、機密性、完全性、可用性のそれぞれについて、情報資産のリスク値を次の式で算出する。

リスクの値　＝　情報資産の価値　×　脅威　×　ぜい弱性

［情報資産の価値の評価基準］

Ｋ社では、機密性、完全性、可用性のそれぞれからみた情報資産の価値の評価基準と値を、表１～３のとおりに設定した。

表１　機密性の評価基準と値

| 評価基準 | 値 |
|---|---|
| 社外に開示可 | 1 |
| 社内だけに開示可 | 2 |
| 部門内だけに開示可 | 3 |
| 必要最小限の関係者だけに開示可 | 4 |

表２　完全性の評価基準と値

| 評価基準 | 値 |
|---|---|
| 業務への影響はない。 | 1 |
| 業務への影響は小さい。 | 2 |
| 業務への影響は大きい。 | 3 |

表３　可用性の評価基準と値

| 評価基準 | 値 |
|---|---|
| 年間24時間までの利用停止は容認される。 | 1 |
| 年間5時間までの利用停止は容認される。 | 2 |
| 年間１時間までの利用停止は容認される。 | 3 |
| 年間10分までの利用停止は容認される。 | 4 |
| 年間１分までの利用停止は容認される。 | 5 |

［脅威とぜい弱性の判断基準］

Ｋ社では、脅威とぜい弱性の判断基準と値を、それぞれ表４，５のとおりに設定した。

表４　脅威の判断基準と値

| 判断基準 | 値 |
|---|---|
| 発生の可能性が低い。 | 1 |
| 発生の可能性が中程度である。 | 2 |
| 発生の可能性が高い。 | 3 |

表５　ぜい弱性の判断基準と値

| 判断基準 | 値 |
|---|---|
| 適切な管理と対策がされている。 | 1 |
| ある程度の管理と対策がなされている。 | 2 |
| 管理と対策が不十分である。 | 3 |

［業務サーバ］

業務サーバでは、顧客情報のデータベースが稼働している。顧客情報とは、顧客コード、顧客名、住所、電話番号などである。

Ｔ君は、業務サーバの機密性、完全性、可用性のそれぞれからみた価値を評価するために、顧客情報に関する内容を次のようにまとめた。

［顧客情報に関する内容］

・顧客情報

①　取引があることをＫ社の競合他社に知られたくない顧客もいるので、社外には公開できない。

②　この情報は、顧客の個人情報であるので、誤りがあった場合、商品の配送ができず調達業務に与える影響は大きい。

③　社員が、電話番号の確認や、挨拶状の宛先ラベルの印字に利用しており、業務サーバが利用できない場合には、業務に支障をきたすことになるため、定期メンテナンス以外で年間１時間までの停止であれば許容する。

［脅威とぜい弱性の状況］

Ｔ君は、業務サーバがさらされている脅威とその脅威に対するＫ社のぜい弱性を調査し、表４および表５の判断基準に基づいて評価した。そのうちの主なものを、表６に示す。

表６　業務サーバの主な脅威とぜい弱性の値

| 脅威 | | ぜい弱性 | |
|---|---|---|---|
| 種類 | 値 | 種類 | 値 |
| ウイルス感染 | 3 | ウイルス対策ソフト未導入 | 3 |
| 不正アクセス | 3 | アクセスコントロール不備 | 2 |
| 故障 | 2 | メンテナンス不足 | 3 |
| なりすまし | 2 | パスワード管理の不備 | 2 |
| 盗聴 | 2 | 最新推奨暗号の未使用 | 1 |

［受容可能なリスク水準］

K社では、受容可能なリスク水準を、表７の通りに設定した。情報資産について各リスクの値がこれらの値以下であれば、そのリスクを保有し、そうでなければ、リスク対応を行う。

表７　受容可能なリスク水準

| | |
|---|---|
| 機密性 | 13 |
| 完全性 | 18 |
| 可用性 | 10 |

［業務サーバのリスク評価］

表１～５の基準、業務サーバの顧客情報と取引情報に関する内容の状況から、T君は、業務サーバに関する評価を行った。評価結果の一部を表８に示す。

表８　業務サーバのリスク評価（抜粋）

| 情報資産 | | | 脅威 | | ぜい弱性 | | リスク |
|---|---|---|---|---|---|---|---|
| 名称 | 価値 | | 内容 | 値 | 内容 | 値 | 値 |
| | 分類 | 値 | | | | | |
| 業務サーバ | 機密性 | (a) | ⋮ | | | | |
| | | | なりすまし | | パスワード管理の不備 | | (b) |
| | | | ⋮ | | | | |
| | 完全性 | (c) | ウイルス感染 | | ウイルス対策ソフト未導入 | | 27 |
| | | | 不正アクセス | | アクセスコントロールの不備 | | 18 |
| | | | なりすまし | | パスワード管理の不備 | | 12 |
| | | | ⋮ | | | | |
| | 可用性 | (d) | ⋮ | | | | |

注）網掛けの部分は表示していない。

設問１　表８中の空欄(a)～(d)に入れる正しい答えを、解答群の中から選べ。解答は、重複して選んでもよい。

解答群

ア　1　　イ　2　　ウ　3　　エ　4　　オ　5

カ　8　　キ　10　　ク　12　　ケ　14　　コ　16

設問２　表８の破線で囲まれた部分に関し、受容可能なリスクにするための対策として適切なものを解答群の中から選び、(e)に答えよ。

解答群

ア　ウイルス対策ソフトを導入する　　イ　パスワード管理を徹底する

ウ　アカウントごとのアクセス権の見直しを行う　　エ　暗号化ソフトを導入する　　オ　メンテナンス回数を増やす