問040010問題

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。

Ｅ君の所属するＦ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。Ｅ君はこのうち，サーバＸ及びサーバＹのリスク評価を担当した。

なお，ここでは，試行のための仮の基準と値を扱うが，それぞれに“仮”を表す文言は用いない。

〔リスクの値の算出〕

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

リスクの値＝情報資産の価値×脅威×脆弱性

〔情報資産の価値の評価基準〕

Ｆ社では，機密性，完全性，可用性のそれぞれから見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
社外に開示できる。	1
社内だけに開示できる。	2
部門内だけに開示できる。	3
必要最小限の関係者だけに開示できる。	4

表２　完全性の評価基準と値

評価基準	値
情報の完全性が失われても，業務への影響はない。	1
情報の完全性が失われても，業務への影響は小さい。	2
情報の完全性が失われると，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
定期メンテナンス以外で年間24時間までの利用停止は容認される。	1
定期メンテナンス以外で年間５時間までの利用停止は容認される。	2
定期メンテナンス以外で年間１時間までの利用停止は容認される。	3
定期メンテナンス以外で年間10分までの利用停止は容認される。	4
定期メンテナンス以外で年間１分までの利用停止は容認される。	5

〔脅威と脆弱性の判断基準〕

Ｆ社では，脅威と脆弓引生の判断基準と値を，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　脆弱性の判断基準と値

判断基準	値
適切な管理と対策がなされている。	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

〔サーバＸ及びサーバＹ〕

サーバＸでは，調達先一般情報のデータベースが稼働している。調達先一般情報とは，調達先コード，調達先の正式な名称，略称，住所，電話番号などである。

サーバＹでは，取引情報のデータベースが稼働している。取引情報とは，調達先コード，購入品コード，単価，癖入履歴などである。

Ｅ君は，サーバＸ及びサーバＹの機密性，完全性，可用性のそれぞれから見た価値を評価するために，調達先一般情報と取引情報に関して，社内関連部門から聴取し，その内容を次のように

まとめた。

〔社内関連部門からの聴取内容〕

（１） 調達先一般情報

① 電話帳や各社のＷｅｂページで公開されている情報であるが，取引があることをＦ社の競合他社に知られたくない調達先もあるので，社外には公開できない。

② この情報は，調達先との間で行っているＥＤＩ（電子データ交換）では利用していないので，誤りがあっても調達業務に与える影響は小さい。

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いるが，サーバＸが利用できない場合には，代替手段での入手が可能である。

（２） 取引情報

① 競合する調達先をはじめ，Ｆ社の同業他社に知られてはならない情報である。また，社内でも，他部門には開示できない情報である。

② 情報に誤りがあれば，調達や支払などの業務に与える影響は大きい。

③ 営業時間内の調達オンライン入力処理，及び夜間のバッチ処理で利用されており，これらを処理するシステムは，メンテナンス以外では，年間４時間以上停止することは許されない。

〔脅威と脆弱性の状況〕

Ｅ君は，各サーバがさらされている脅威とその脅威に対するＦ社の脆弱性を調査し，表４及び表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 サーバＸ及びサーバＹの主な脅威と脆弱性の値

脅威		脆弱性	
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の不備	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〕

Ｆ社では，受容可能なリスク水準を，表７のとおりに設定した。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	15
可用性	10

〔サーバＸ及びサーバＹのリスク評価〕

表１～５の基準，聴取内容及びサーバＸとサーバＹの状況から，Ｅ君は，サーバＸ及びサーバＹに関するリスク評価を行った。Ｆ社では，評価に当たって，表１～３の評価基準では，該当する基準の値のうちで最も小さいものを選ぶことにしている。

評価結果の一部を表８に示す。

表８　サーバＸ及びサーバＹのリスク評価（抜粋）

情報資産			脅威		脆弱性		リスク
名称	価値		内容	値	内容	値	値
	分類	値					
サーバＸ	機密性		⋮				
			なりすまし		パスワード管理の不備		a
			⋮				
	完全性		ウイルス感染		ウイルス対策ソフト未導入		18
			不正アクセス		アクセスコントロールの不備		12
			なりすまし		パスワード管理の不備		8
			⋮				
	可用性		⋮				
サーバＹ	機密性		⋮				
			不正アクセス		アクセスコントロールの不備		b
			⋮				
	完全性		ウイルス感染		ウイルス対策ソフト未導入		c
			⋮				
	可用性	d	⋮				

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。

設問１　表８中の［　a　］～［　d　］に入れる正しい答えを，解答群の中から選べ。

ａ～ｃに関する解答群

ア　４　　イ　６　　ウ　８　　エ　９　　オ　１２

カ　１６　　キ　１８　　ク　２４　　ケ　２７　　コ　３６

ｄに関する解答群

ア　１　　イ　２　　ウ　３　　エ　４　　オ　５

設問２ 表８のサーバＸの完全性の破線で囲まれた部分に関し，Ｆ社の受容可能なリスク水準から判断されるリスク対応として適切なものを，解答群の中から選べ。

解答群

ア　ＩＤＳ（侵入検知システム）を導入する。

イ　ウイルス対策ソフトを導入する。

ウ　公開鍵暗号を利用する。

エ　定期メンテナンスの回数を増やす。

オ　パスワード管理を強化する。