問040010解説

◆解答

設問１　ａ　ウ　　ｂ　キ　　ｃ　ケ　　ｄ　ウ

設問２　イ

◆解説

情報セキュリティのリスク管理に関する問題である。

リスクアセスメントとリスク値の算出

情報資産の洗い出し（名称、管理責任者、価値、利用者の範囲、保管形態、保管場所、保管期間、処分方法など）、情報資産のラベリング、リスクアセスメント（管理状況、存在する脅威、資産の脆弱性、事業への影響度、リスクの評価など）を順次実施する

リスク値は次の式を用いて計算する。

リスクの値＝情報資産の価値×脅威の値×脆弱性の値

情報資産の価値：機密性、完全性、可用性の観点から評価した結果の数値化

脅威の値：要求される保証度合い以下に引き下げる潜在的な要因

脆弱性の値：情報資産や人員の管理方法に起因する弱点

情報資産の価値評価基準

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

情報セキュリティ確保の３条件

①　機密性

機密性はネットワーク上やコンピュータ内の情報を不適切な人間に見せないことである。盗聴や傍受、不正アクセスあるいは不正放置などによって、その内容が他者に漏れたときに、

持ち主にとって損失が発生する可能性がある。機密性の喪失は不適切な利用者にネットワーク上やコンピュータ内の情報を見られたり、メールサーバ内のメールの内容を見られることである。通信路上で無線周波数を合わせ、プロトコルアナライザを利用して容易に傍受したり、ハードディスクやフロッピーディスクの内容を他人に成りすましたり、セキュリティホールを利用して不当に読み出したりする行為である。

② 完全性

完全性はネットワーク上やコンピュータ内の情報が常に完全な形で保たれ、不正によって改ざんされたり破壊されないことである。完全性の喪失は、通信路上のデータ、ハードディスク内のデータ、フロッピーディスク内のデータの改ざんや破壊が行われたり、インターネット上の電子商取引において、金額情報の改ざんが行われたりすることである。長時間かけて蓄積、作成した情報源が破壊されると、その復旧に膨大な時間と金を必要としたり、時には復旧不能にもなる。交通システムに侵入され、制御情報を改ざんされると、生命の危険が生じかねない。

③ 可用性

可用性はネットワークやコンピュータ内の情報や資源がいつでも利用でき、資格を与えられたユーザが情報システムを適時に使用できる保証である。ハードウェア、ソフトウェア、データベースなど情報システムに関する構成物のすべてに関係する。可用性の喪失は、通信路やコンピュータパワー、コンピュータのディスクの不当な利用によって、ネットワークやコンピュータの機能、保存情報が使えなくなることである。

脅威と脆弱性の判断基準

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

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

リスクの発生要因

リスク発生の原因には脅威と脆弱性がある。

① 脅威

脅威は、顕在化すればシステムに損害を与える可能性のある要因である。地震や火災等の災害、機器の障害や誤操作、不正行為、景気変動などの外的要因が含まれる。

② 脆弱性

脆弱性は、脅威の顕在化を現実の損失あるいはその拡大に結びつけるシステムの脆さ、弱点である。ハード面、ソフト面におけるシステムの弱点、ネットワーク上の欠陥、バックアップ対策の不備、マニュアルの不整備などが含まれる。

サーバXおよびサーバYのリスク評価

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。

サーバXの完全性の場合のリスク値の計算要領

表６と表２、リスク値の計算式を用いて次のように計算できる。

① 脅威「ウィルス感染」＝３、脆弱性「ウィルス対策ソフト未導入」＝３、サーバＸでは一般情報は調達業務に与える影響は小さいため情報資産の価値＝２となる。

リスク値＝２×３×３＝１８

② 脅威「不正アクセス」＝３、脆弱性「アクセスコントロールの不備」＝２、サーバＸで

は一般情報は調達業務に与える影響は小さいため情報資産の価値＝２となる。

リスク値＝２×３×３＝１２

③　脅威「なりすまし」＝２、脆弱性「パスワード管理の不備」＝２、サーバＸでは一般情報は調達業務に与える影響は小さいため情報資産の価値＝２となる。

リスク値＝２×２×２＝８

設問１

ａは、サーバＸの情報資産の機密性のリスク値の計算問題である。脅威「なりすまし」＝２、脆弱性「パスワード管理の不備」＝２、機密性の評価基準は「社内だけに開示できる」＝２となり、リスク値を計算すると次のようになる。

リスク値＝２×２×２＝８

となり、求める答えはウとなる。

ｂは、サーバＹの情報資産の機密性のリスク値の計算問題である。脅威「不正アクセス」＝３、脆弱性「アクセスコントロールの不備」＝２、機密性の評価基準は「部門内だけに開示できる」＝３となり、リスク値を計算すると次のようになる。

リスク値＝３×２×３＝１８

となり、求める答えはキとなる。

ｃは、サーバＹの情報資産の完全性のリスク値の計算問題である。脅威「ウィルス感染」＝３、脆弱性「ウィルス対策ソフト未導入」＝３、機密性の評価基準は「部門内だけに開示できる」＝３となり、リスク値を計算すると次のようになる。

リスク値＝３×３×３＝２７

となり、求める答えはケとなる。

ｄは、サーバＹの情報資産の可用性の評価基準の値を求める問題である。処理システムではメイ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であるから、表３の可用性の評価基準と値から「定期メイ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」が適用されて値は３となる。求める答えはウとなる。

設問２

サーバＸに対して受容可能なリスク水準から判断されるリスク対応を求める問題である。リスク値は、ウィルス感染に関しては１８、不正アクセスに関しては１２、なりすましに関しては８であり、利用可能な完全性のリスク水準は１５であるから、リスク値がそれより大きい脅威に対しては脆弱性に対して対応を講じる必要がある。脅威「ウィルス感染」のリスク値は１８であるため、脆弱性の対応として「ウィルス対策ソフトの導入」を実施する必要がある。求める答えはイとなる。