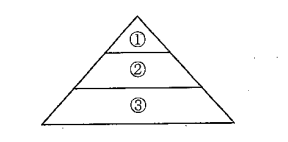
２．コンピュータの技術要素

２．３　情報セキュリティ（情報セキュリティ管理）

問題１

情報セキュリティの文書を詳細化の順に、右の図のように上から並べた場合、①~③に当てはまる用語の組み合わせとして、適切なものはどれか。

|  |  |  |  |
| --- | --- | --- | --- |
|  | ① | ② | ③ |
| ア | 基本方針 | 対策基準 | 対策実施手順 |
| イ | 基本方針 | 対策実施手順 | 対策基準 |
| ウ | 対策基準 | 基本方針 | 対策実施手順 |
| エ | 対策基準 | 対策実施手順 | 基本方針 |

問題２

情報セキュリティにおける“可用性”の説明として、適切なものはどれか。

ア：　システムの動作と出力結果が意図したものであること

イ：　情報が正確であり、改ざんされたり破壊されたりしていないこと

ウ：　認可された利用者が、必要な時に情報にアクセスできること

エ：　認可されていないプロセスに対して、情報を非公開にすること

問題３

ISMSの運用において、監査結果をインプットし、ISMSを継続的に改善するための是正処置及び予防処置を行うプロセスはPDCAサイクルのどれに当たるか。

ア：P

イ：D

ウ：C

エ：A

問題４

リスクマネジメントにおいて、リスクを資産ごとに洗い出すものはどれか。

ア：　リスク対策

イ：　リスク特定

ウ：　リスク評価

エ：　リスク分析

問題５

　組織で策定する情報セキュリティポリ氏に関するk医術のうち、最も適切なものはどれか。

ア：　情報えきゅりてぃ基本方針だけでなく、情報セキュリティに関する規則や手順の策定も経営者が行うべきである。

イ：　情報セキュリティ基本方針だけでなく、情報セキュリティに関する規則や手順も社外に公開することが求められている。

ウ：　情報セキュリティに関する規則や手順は組織の状況にあったものにすべきであるが、最上位の情報セキュリティに基本方針は業界標準のひな型をそのまま採用することが求められている。

エ：　組織内の複数の部門で異なる情報セキュリティ対策を実施する場合でも、情報セキュリティ基本方針は組織全体で統一させるべきである。

問題６

　組織の活動に関する記述ａ~ｄのうち、ＩＳＭＳの特徴として、適切なものだけを全て、挙げたものはどれか。

ａ：　一過性の活動でなく改善と活動を継続する。

ｂ：　現場が主導するボトムアップ活動である。

ｃ：　導入及び活動は経営層を頂点とした組織的な取り組みである。

ｄ：　目標と期限を定めて活動し、目標達成によって終了する。

ア：　ａ，ｂ

イ：　ａ，ｃ

ウ：　ｂ，ｄ

エ：　ｃ，ｄ

問題７

　ＩＳＭＳにおけるセキュリティリスクへの対応には、リスク移転、リスク回避、リスク受容及びリスク低減がある。リスク回避に該当する事例はどれか。

ア：　セキュリティ対策を行って、問題発生の可能性を下げた。

イ：　問題発生時の損害に備えて、保険に入った。

ウ：　リスクが小さいことを確認し、問題発生時は損害を負担することにした。

エ：　リスクの大きいサービスから撤退した。

２．コンピュータの技術要素

２．３　情報セキュリティ（情報セキュリティ管理）

問題１【解答：ア】

　情報セキュリティの文書を詳細化の順に上から並べると、次のようになる。

①　・・・情報セキュリティ「基本方針」

：組織としての統一的かつ基本的な考え方や理念を表したもの

②　・・・情報セキュリティ「対策基準」

：基本方針を実践するための村主事項や基準を記述したもの

③　・・・情報セキュリティ「対策実施手順」

：情報セキュリティ対策の具体的な実施手順を記述したもの

なお、基本方針と対策基準をまとめて、“情報セキュリティポリシ”という場合もある。

問題２【解答：ウ】

　情報セキュリティマネジメントシステムにおいては、情報セキュリティマネジメントの三大要素（機密性・完全性・可用性）を維持することが求められる。このうち、“可用性”は、必要な時に必要な資産（データ）に確実にアクセスができる特性である。したがって、「認可された利用者が、必要な時に情報にアクセスできること」が該当する。

ア：　ソフトウェア製品の品質特性の一つである“機能性”の説明である。

イ：　“完全性”（資産（データ）の正確さ・完全さを保護する特性）の説明である。

エ：　“機密性”（認可されていない相手には、情報を非公開とする特性）の説明である。

問題３【解答：エ】

　情報セキュリティマネジメントシステム（ISMS：Information System Security Management System）は、“計画（Plan）”、“実行（Do）”、“点検（Check）”、“処置（Act）”のPDCAサイクルで進められる。

・P（計画[Plan]）

：情報セキュリティ基本方針などを策定する。

・D（実行[Do]）

：情報セキュリティ対策基準や情報セキュリティ対策実施手順を決めて運用する。

・C（点検[Check]）

：ISMSを開始/評価する。

・A（処置[Act]）

：導入したISMSを見通して改善する。（正解）

問題４【解答：イ】

・リスク対策

：リスクが発生したときの対応について優先順位を決め、損失と対策費用の関係（コストパフォーマンス）などから、リスクへの対応策を決定する。

・リスク特定

：資産を調査して、発生する可能性のあるリスクを資産ごとに洗い出す。（正解）

・リスク評価

：リスクが発生した場合の損失などによる、経営上の影響範囲などを評価する。

・リスク分析

：リスクの種類や発生頻度、強度（リスクに対する強さ）などを分析する。

問題５【解答：エ】

　情報セキュリティポリシは、情報セキュリティに対する組織としての考え方を明文化したものである。「組織内の複数の部門で異なる情報セキュリティ対策を実施する場合でも、情報セキュリティｋ本方針は組織全体で統一させるべきである。」

ア：　情報セキュリティに関する規則や手順は、情報システムや管理部門ごとに策定する。

イ：　情報セキュリティに関する規則や手順を社外に公開する必要はない。

ウ：　情報セキュリティ基本方針も組織の状況や業務内容に合わせるべきであり、業界標準のひな型をそのまま採用する必要はない。

問題５【解答：イ】

　ISMS（Information Security Management System）は、企業や組織が情報セキュリティマネジメントの三大要素（機密性・完全性・可用性）を確保・維持するために、情報セキュリティポリシに基づいてセキュリティレベルの設定やリスクアセスメントなどを継続して行い、情報資産を正しく、安全に運用するための枠組みである。

ａ：　“計画（Plan）”、“実行（Do）”、“点検（Check）”、“処置（Act）”のPDCAサイクルで進め、改善と活動を継続する。（正しい）

ｂ：　組織の経営層が情報セキュリティポリシを策定し、その基本方針に基づいて具体的な実施手順などを策定するトップダウンの活動である。

ｃ：　導入及び活動は経営層を頂点とし、組織的に取り組むべきである。（正しい）

ｄ：　改善と活動を継続し、終了することはない。

したがって、ISMSの特徴として適切なのは「ａ，ｃ」である。

問題６【解答：エ】

　リスク回避は、リスクを避けるために、リスクの発生源となるものの使用を中止するか、代替する対応方法である。したがって、「リスクの大きいサービスから撤退した」ことが、該当する。

ア：　リスク予防に該当する事例である。

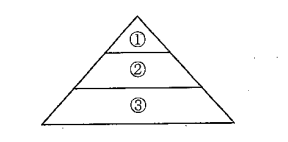
イ：　リスク移転に該当する事例である。

ウ：　リスク受容に該当する事例である。

２．コンピュータの技術要素

２．３　情報セキュリティ（情報セキュリティ管理）

問題１

セキュリティのをのに、ののようにから、①~③に当てはまるのみわせとして、なものはどれか。

|  |  |  |  |
| --- | --- | --- | --- |
|  | ① | ② | ③ |
| ア |  |  |  |
| イ |  |  |  |
| ウ |  |  |  |
| エ |  |  |  |

問題２

セキュリティにおける“”のとして、なものはどれか。

ア：　システムのとがしたものであること

イ：　がであり、されたり、されたりしていないこと

ウ：　されたが、なににアクセスできること

エ：　されていないプロセスに対して、をにすること

問題３

ISMSのにおいて、をインプットし、ISMSをにするためのびをうプロセスはPDCAサイクルのどれにたるか。

ア：P

イ：D

ウ：C

エ：A

問題４

リスクマネジメントにおいて、リスクをごとにいすものはどれか。

ア：　リスク

イ：　リスク

ウ：　リスク

エ：　リスク

問題５

　でするセキュリティポリシにするのうち、もなものはどれか。

ア：　セキュリティだけでなく、セキュリティにするやのもがうべきである。

イ：　セキュリティだけでなく、セキュリティにするやもにすることがめられている。

ウ：　セキュリティにするやはのにあったものにすべきであるが、のセキュリティにはのひなをそのまますることがめられている。

エ：　ののでなるセキュリティをするでも、セキュリティはでさせるべきである。

問題６

　のにａ～ｄのうち、ＩＳＭＳのとして、なものだけをて、げたものはどれか。

ａ：　のでなくとをする。

ｂ：　がするボトムアップである。

ｃ：　びはをとしたなりみである。

ｄ：　目標と期限を定めて活動し、目標達成によって終了する。

ア：　ａ，ｂ

イ：　ａ，ｃ

ウ：　ｂ，ｄ

エ：　ｃ，ｄ

問題７

　ＩＳＭＳにおけるセキュリティリスクへのには、リスク、リスク、リスクびリスクがある。リスクにするはどれか。

ア：　セキュリティをって、のをげた。

イ：　のにえて、にった。

ウ：　リスクがさいことをし、はをすることにした。

エ：　リスクの大きいサービスからした。

２．コンピュータの技術要素

２．３　情報セキュリティ（情報セキュリティ管理）

問題１【解答：ア】

　セキュリティのをのにから並べると、のようになる。

①　・・・セキュリティ「」

：としてのかつな考え方やをしたもの

②　・・・セキュリティ「」

：をするためのやをしたもの

③　・・・セキュリティ「」

：セキュリティのなをしたもの

なお、とをまとめて、“セキュリティポリシ”というもある。

問題２【解答：ウ】

　セキュリティマネジメントシステムにおいては、セキュリティマネジメントの（・・）をすることがめられる。このうち、“”は、なにな（データ）ににアクセスができるである。したがって、「されたが、なににアクセスできること」がする。

ア：　ソフトウェアのの一つである“”のである。

イ：　“”（（データ）のさ・さをする）のである。

エ：　“”（されていないには、をとする）のである。

問題３【解答：エ】

　セキュリティマネジメントシステム（ISMS：Information System Security Management System）は、“（Plan）”、“（Do）”、“（Check）”、“（Act）”のPDCAサイクルでめられる。

・P（[Plan]）

：セキュリティなどをする。

・D（[Do]）

：セキュリティやセキュリティをめてする。

・C（[Check]）

：ISMSをする。

・A（[Act]）

：したISMSをしてする。（正解）

問題４【解答：イ】

・リスク

：リスクがしたときのについてをめ、との（コストパフォーマンス）などから、リスクへのをする。

・リスク

：をして、するのあるリスクをごとにいす。（正解）

・リスク

：リスクがしたのなどによる、のなどをする。

・リスク

：リスクのや、（リスクにするさ）などをする。

問題５【解答：エ】

　セキュリティポリシは、セキュリティにするとしてのえをしたものである。「ののでなるセキュリティをするでも、セキュリティはでさせるべきである。」

ア：　セキュリティにするやは、システムやごとにする。

イ：　セキュリティにするやをにするはない。

ウ：　セキュリティものやにわせるべきであり、のひなをそのままするはない。

問題５【解答：イ】

　ISMS（Information Security Management System）は、やがセキュリティマネジメントの（・・）を・するために、セキュリティポリシにづいてセキュリティレベルのやリスクアセスメントなどをして、をしく、にするためのみである。

ａ：　“（Plan）”、“（Do）”、“（Check）”、“（Act）”のPDCAサイクルでめ、とをする。（正しい）

ｂ：　のがセキュリティポリシをし、そのにづいてななどをするトップダウンのである。

ｃ：　はをとし、にりむべきである。（正しい）

ｄ：　とをし、することはない。

したがって、ISMSのとしてなのは「ａ，ｃ」である。

問題６【解答：エ】

　リスクは、リスクをけるために、リスクのとなるもののをするか、するである。したがって、「リスクのきいサービスからした」ことが、する。

ア：　リスクにするである。

イ：　リスクにするである。

ウ：　リスクにするである。