２．コンピュータの技術要素

２．３　情報セキュリティ（１）（情報セキュリティの脅威（１））

問題１

“セキュリティの”におけるにする説明のうち、**でないもの**はどれか。

ア：　やがされたなどにするを、とぶ。

イ：　コンピュータをしてしてくるを、とぶ。

ウ：　にしてなをえるを、と呼ぶ。

エ：　のがとなるを、とぶ。

問題２

システムのながをうっかりえたとして、なデータがされてしまった。このようなをというか。

ア：

イ：

ウ：

エ：

問題３

をってのPCにし、データをみたり、したりするをというか。

ア：　クラッキング

イ：　ショルダハッキング

ウ：　トラッシング

エ：

問題４

セキュリティののうち、がにされるものはどれか。

ア：　によってサーバがし、がした。

イ：　からサーバにのデータをられて、サーバがした。

ウ：　がネットワークをして、のサーバにし、ファイルをした。

エ：　がメールのをえて、なデータがした。

問題５

システムのをげるへのにするのうち、なものはどれか。

ア：　からのをにできれば、アクセスへのとしてはない。

イ：　にしてはがなので、にってをじる。

ウ：　すべてのデータをバックアップしておけば、ほかのはとなる。

エ：　やコストとのトレードオフをして、なをじる。

問題６

ソーシャルエンジニアリングによるにびきやすいはどれか。

ア：　のセキュリティがい。

イ：　サーバののがわれていない。

ウ：　サーバへのアクセスがわれていない。

エ：　がされていない。

問題７

PCやハードディスクをしたりしたりするにしておくこととして、ハードディスクからのをぐ最もなはどれか。

ア：ハードディスクを16の00やFF、またはできをしておく。

イ：ハードディスクをフォーマットしておく。

ウ：ハードディスクのすべてのファイルやフォルダをごみにて、にゴミをにしておく。

エ：ハードディスクにパスワードロックをかけておく。

２　コンピュータの技術要素

２．３　情報セキュリティ（１）（情報セキュリティの脅威（１））

問題１　【解答：ウ】

とは、システムまたは、にをえるがあるもの（）である。は、、、にされる。

・ の（のはわない）がとなるである。

・ やがされたなどにするである。

・ のあるが、コンピュータをしてしてくるである。

なお、がえるには、にするなもまれているので、あえてセキュリティのに「」というはない（あるで、すべてのがである）。

問題２　【解答：ア】

・

：をえて、データをしたりしてしまうことである。（）をうっかりえたとしてしたなので、このにする（正解）

・

：のあるによる、などによって、がれてえなくなることである。

・

：がされているPCやUSBメモリなどを、にしてしまうことである。

・

：がされているPCやUSBメモリなどを、れたり、まれたりしてなくしてしまうことである。

問題３　【解答：ア】

・クラッキング

：をってのPCにし、データをみたり、したりするである。クラッキングをうをクラッカという。（正解）

・ショルダハッキング

：パスワードを入力しているのキーボードのやにされたを、からいてみるである。

・トラッシング（スキャンベンジング）

：ごみにてられたメモから、なをんだりするである。

・

：あるのやをターゲット（）としてするである。

問題４　【解答：ア】

ア：　というがなので、にされる。

イ：　のデータをりつけるというコンピュータをした（）なので、にされる。

ウ：　ネットワークをしてサーバにするというコンピュータをした（）なので、にされる。

エ：　がメールのをえるというがなので、にされる。

問題５　【解答：エ】

ア：　からのアクセス（アクセスをっていないが、ネットワークすること）もあるので、からのをするだけではとしてである。

イ：　する（、など）をして、バックアップサイトのやなバックアップのなどなをじるべきである。

ウ：　のやのなどのもあるので、データバックアップだけではとしてである。

エ：　のをし、それぞれのへの（など）をして、にをじておくことがである。よりもコストのがいような、あえてをじないということもある。

問題６　【解答：】

ソーシャルエンジニアリングは、なの一つであり、、なでをみるである。ごみにてられているメモからなをむ“トラッシング”や、が、あたかもであるかのようにって、やパスワードをきす“なりすまし”などがある。したがって、「のセキュリティがい」と、ソーシャルエンジニアリングによるにびきやすいであるといえる。

イ：　によるにびきやすいである。

ウ：　クラッキングによるにびきやすいである。

エ：　によるにびきやすいである。

問題７　【解答：ア】

ア：　ハードディスクを16の00やFF、またはできしておくと、データをにしたことになるので、をぐとしてもなである。（正解）

イ：　ハードディスクをフォーマットしてもデータをにしたことにはならないので、ハードディスクにされたをみられるがある。

ウ：　ファイルやフォルダをごみにててからからにしても、データをにしたことにはならないので、ハードディスクにされたをみられるがある。

エ：　ハードディスクにパスワードロック（にATAパスワードとばれる）をかけることで、をぐができる。しかし、このようなロックをするツールやスキルもしているため、をぐもなとはいえなくなっている。

２　コンピュータの技術要素

２．３　情報セキュリティ（１）（情報セキュリティの脅威（１））

問題１　【解答：ウ】

脅威とは、システムまたは組織、人間に損害を与える可能性があるもの（原因）である。脅威は、人的脅威、物理的脅威、技術的脅威に分類される。

・人的脅威 人間の行為（悪意の有無は問わない）が原因となる脅威である。

・物理的脅威 機器自体や機器が設置された建物などに対する脅威である。

・技術的脅威 悪意のある第三者が、コンピュータ技術を利用して攻撃してくる脅威である。

なお、今日が与える損害には、組織に対する経済的な損失も含まれているので、あえて情報セキュリティの脅威に「経済的脅威」という分類はない（ある意味で、すべての脅威が経済的脅威である）。

問題２　【解答：ア】

・誤操作

：操作を間違えて、データを消去したりしてしまうことである。処理（操作）をうっかり間違えた結果として発生した現象なので、この脅威に該当する（正解）

・破壊

：悪意のある第三者による妨害行為、破壊行為などによって、機器が壊れて使えなくなることである。

・破損

：情報が保存されているPCやUSBメモリなどを、使用中に壊してしまうことである。

・紛失

：情報が保存されているPCやUSBメモリなどを、置き忘れたり、盗まれたりしてなくしてしまうことである。

問題３　【解答：ア】

・クラッキング

：悪意を持って他人のPCに侵入し、データを盗み見たり、破壊したりする行為である。クラッキングを行う人をクラッカという。（正解）

・ショルダハッキング

：パスワードを入力している人のキーボードの操作や画面に表示された情報を、肩越しから覗いて盗み見る行為である。

・トラッシング（スキャンベンジング）

：ごみ箱に捨てられたメモから、重要な情報を盗んだりする行為である。

・標的型攻撃

：ある特定の組織や人間をターゲット（標的）として攻撃する行為である。

問題４　【解答：ア】

ア：　大雨という自然災害が原因なので、物理的脅威に分類される。

イ：　大量のデータを送りつけるというコンピュータ技術を利用した攻撃（脅威）なので、技術的脅威に分類される。

ウ：　ネットワークを介して社内サーバに侵入するというコンピュータ技術を利用した攻撃（脅威）なので、技術的脅威に分類される。

エ：　社員が電子メールの宛先を間違えるという誤操作が原因なので、人的脅威に分類される。

問題５　【解答：エ】

ア：　内部からの不正アクセス（アクセス権を持っていない第三者が、ネットワーク侵入すること）もあるので、外部からの侵入を阻止するだけでは事前対策として不十分である。

イ：　発生する自然災害（地震、洪水など）を想定して、バックアップサイトの準備や定期的なバックアップ計画の立案など適切な事前対策を講じるべきである。

ウ：　情報の漏洩や機器の紛失などの脅威もあるので、データバックアップだけでは事前対策として不十分である。

エ：　脅威の種類を理解し、それぞれの資産への影響（予想損失額など）を考慮して、事前に対策を講じておくことが大切である。予想損失額よりも対策コストの方が高いような場合、あえて事前対策を講じないということもある。

問題６　【解答：】

ソーシャルエンジニアリングは、意表的な人的脅威の一つであり、日常的、一般的な手段で情報を盗み取る行為である。ごみ箱に捨てられているメモから重要な情報を盗む“トラッシング”や、第三者が、あたかも本人であるかのように装って、暗証番号やパスワードを聞き出す“なりすまし”などがある。したがって、「運用担当者のセキュリティ意識が低い」と、ソーシャルエンジニアリングによる被害に結び付きやすい状況であるといえる。

イ：　物理的脅威による被害に結び付きやすい状況である。

ウ：　クラッキングによる被害に結び付きやすい状況である。

エ：　盗聴による被害に結び付きやすい状況である。

問題７　【解答：ア】

ア：　ハードディスク全体を16進数の00やFF、または乱数で複数回上書きしておくと、データを物理的に削除したことになるので、情報漏洩を防ぐ方法として最も確実な方法である。（正解）

イ：　ハードディスクを論理フォーマットしてもデータを物理的に削除したことにはならないので、ハードディスクに記録された情報を読み取られる危険性がある。

ウ：　ファイルやフォルダをごみ箱に捨ててからからにしても、データを物理的に削除したことにはならないので、ハードディスクに記録された情報を読み取られる危険性がある。

エ：　ハードディスクにパスワードロック（一般的にATAパスワードと呼ばれる）をかけることで、情報漏洩を防ぐ効果が期待できる。しかし、このようなロックを解除するツールやスキルも存在しているため、情報漏洩を防ぐ最も確実な方法とはいえなくなっている。

２．コンピュータの技術要素

２．３　情報セキュリティ（１）（情報セキュリティの脅威（１））

問題１

“情報セキュリティの脅威”における分類に関する説明のうち、**適切でないもの**はどれか。

ア：　機器自体や機器が設置された建物などに関する脅威を、物理的脅威と呼ぶ。

イ：　コンピュータ技術を利用して攻撃してくる脅威を、技術的脅威と呼ぶ。

ウ：　組織に対して経済的な損失を与える脅威を、経済的脅威と呼ぶ。

エ：　人間の行為が原因となる脅威を、人的脅威と呼ぶ。

問題２

システムの正当な利用者が処理をうっかり間違えた結果として、重要なデータが消去されてしまった。このような脅威を何というか。

ア：　誤操作

イ：　破壊

ウ：　破損

エ：　紛失

問題３

悪意を持って他人のPCに侵入し、データを盗み見たり、破壊したりする行為を何というか。

ア：　クラッキング

イ：　ショルダハッキング

ウ：　トラッシング

エ：　標的型攻撃

問題４

セキュリティ事故の例のうち、原因が物理的脅威に分類されるものはどれか。

ア：　大雨によってサーバ室が浸水し、機器が停止した。

イ：　外部から公開サーバに大量のデータを送られて、公開サーバが停止した。

ウ：　攻撃者がネットワークを介して、社内のサーバに侵入し、ファイルを破壊した。

エ：　社員が電子メールの宛先を間違えて、重要なデータが流出した。

問題５

情報システムの安定稼働を妨げる脅威への事前対策に関する記述のうち、適切なものはどれか。

ア：　外部からの不正侵入を完全に阻止できれば、不正アクセスへの事前対策としては問題ない。

イ：　自然災害に対しては予測が困難なので、人的災害に絞って事前対策を講じる。

ウ：　すべてのデータをバックアップしておけば、ほかの事前対策は不要となる。

エ：　予想損失額や対策コストとのトレードオフを考慮して、必要な事前対策を講じる。

問題６

ソーシャルエンジニアリングによる被害に結び付きやすい状況はどれか。

ア：　運用担当者のセキュリティ意識が低い。

イ：　サーバ室の天井の防水対策が行われていない。

ウ：　サーバへのアクセス制御が行われていない。

エ：　通信経路が暗号化されていない。

問題７

PCやハードディスクを譲渡したり返却したりする前に実施しておくこととして、ハードディスクからの情報漏洩を防ぐ最も確実な方法はどれか。

ア：ハードディスク全体を16進数の00やFF、または乱数で複数回上書きをしておく。

イ：ハードディスク全体を論理フォーマットしておく。

ウ：ハードディスク内のすべてのファイルやフォルダをごみ箱に捨て、。最後にゴミ箱を空にしておく。

エ：ハードディスクにパスワードロックをかけておく。