問７　【解答イ】

VoIP（Voice over Internet Protocol）は，音声信号（アナログ信号）をディジタル信号に変換して，パケット単位に分割して伝送する技術である。VoIPを利用しているIP電話では，インターネットによるリアルタイム通話を実現している。

ア：SaaS（Software as a Service）などに関する説明である。

ウ：VPN（Virtual Private Network）に関する説明である。

エ：DNS（Domain Name System）に関する説明である。

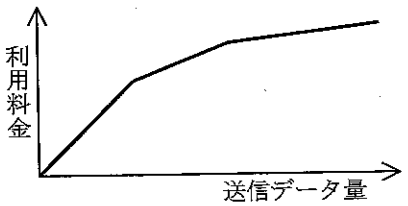
問８　【解答ア】

従量制は，送信データ量（パケット数）によって利用料金が決まる課金方式である。送信データ量が多くなるほど，利用料金も比例して高くなるので「a」のような右上がりの直線になる。

b：携帯電話の契約などで用いられる段階的定額制を表している。

c：定額制の課金方式を表している。

d：送信データ量が増えるほど，利用料金が少なくなるということはない。なお，コンピュータシステムの課金などでは，使用量が多くなるにつれて利用金額（単価）が安くなる逓減課金方式というものもある。逓減課金方式のグラフは，次のようになる。



2．3　情報セキュリティ(1)

問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，脅威が与える損害には組織に対する経済的な損失も含まれるので，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３　【解答ア】

・クラッキング

：悪意をもって他人の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，肩越しからのぞいて盗み見る行為である。

・トラッシング（スキャベンジング）

：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。（正解）

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５　【解答エ】

ア：内部からの不正アクセス（アクセス権をもっていない第三者が，ネットワークに侵入すること）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：情報の漏えいや機器の紛失などの脅威もあるので，データの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ほうが高いような場合，あえて事前対策を講じないということもある。（正解）

問６　【解答ア】

ソーシャルエンジニアリングは，代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つ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つきやすい状況である。

ウ：クラッキングによる被害に結びつきやすい状況である。

エ：盗聴による被害に結びつきやすい状況である。

問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，情報漏えい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ゴミ箱に捨ててから空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（一般にATAパスワードと呼ばれる）をかけることで，情報漏えい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，情報漏えいを防ぐ最も確実な方法とはいえなくなっている。

２．３　情報セキュリティ(2)

情報セキュリティの脅威(2)

問１　【解答ウ】

・アドウェア
　：広告を目的として配布される，一般的には無償のソフトウェアである。
・シェアウェア
　：一定の試用期間後に，利用を続ける場合に料金を支払う必要のあるソフトウェアである。
・マルウェア
　：悪意をもって作成されたソフトウェア（プログラム）の総称である。コンピュータウイルスや，ワーム，ボット，スパイウェアなどがある。（正解）
・ミドルウェア
　：OSと応用ソフトウェア（アプリケーションソフトウェア）の中間に位置付けられる，複数の応用ソフトウェアが共通して利用するOSの基本機能を提供するソフトウェアである。

問２　【解答エ】

マクロとは，処理手順をあらかじめ登録（定義）しておき，必要なときに呼び出して実行させる，ワープロソフトや表計算ソフトの機能である。マクロウイルスは，このマクロ機能を利用したウイルスであり，「ワープロソフトや表計算ソフトのデータファイルに感染する。」

ア：ボットに関する説明である。

イ：スパイウェアに関する説明である。

ウ：トロイの木馬に関する説明である。

問3　【解答エ】

・キーロガー

：キーボード入力を記録する仕組み（ソフトウェア）を利用して，他人が入力した情報（パスワードなど）を不正に入手する攻撃である。

・ゼロデイ攻撃

：ベンダ企業がソフトウェアの脆弱性（セキュリティホール）を公表した場合に，その修正プログラムが提供される前に脆弱性を悪用して行われる攻撃である。

・バッファオーバフロー攻撃

：長い文字列などを送り続け，プログラムが確保したメモリ領域（バッファ）をあふれさせることにより，プログラムのアクセス権を支配し，誤作動を起こさせる攻撃である。

・フィッシング

：実在する会社を装って偽電子メールを送ったり，DNSキャッシュポイズニング（DNSサーバのキャッシュ情報を改ざんする攻撃）を用いたりして，利用者を偽のWebページに誘導し，情報（パスワードなど）を入力させて不正に入手する攻撃である。（正解）

問4　【解答イ】

スパムメールとは，受信者の承諾なしに不特定多数に一方的に送りつけられる広告メールのことである。迷惑メールの一種で，広告や勧誘などを目的としたダイレクトメールなどが該当する。

ア：同報メールやメールマガジンに関する説明である。

ウ：オプトインメールに関する説明である。

エ：チェーンメールに関する説明である。チェーンメールも迷惑メールに分類される。

問5　【解答イ】

ランサムウェアとは，「感染すると勝手にファイルやデータの暗号化などを行って，正常にデータにアクセスできないようにし，元に戻すための代金を利用者に要求するソフトウェア」である。ランサムとは“身代金”を意味する言葉である。

ア：ウイルス対策ソフトに関する説明である。

ウ：OS（オペレーティングシステム）に関する説明である。

エ：日本語IME（Input Method Editor）に関する説明である。

問6　【解答エ】

DoS（Denial of Service）攻撃は，標的のサーバに大量のデータを送信し続け，サーバのCPU，メモリなどに過剰な負荷をかける攻撃である。その結果として，「サービスの提供が阻害される」という被害が生じることになる。

問7　【解答ア】

クロスサイトスクリプティング（XSS：Cross Site Scripting）は，悪意をもったスクリプトを，脆弱性のある標的サイト経由で利用者に送り，その標的サイトにアクセスした利用者にスクリプトを実行させて，情報を盗み出す攻撃である。Webサイトの運営者が意図しないスクリプトを含むデータであっても，利用者のブラウザに送ってしまう脆弱性を利用している。

イ：OSコマンドインジェクション攻撃に関する記述である。

ウ：パスワードリスト攻撃に関する記述である。

エ：IPスプーフィングに関する記述である。