

# 令和06年 ITパスポートの新しくわかる教科書

## 実力アップ模試 解答・解説

### <問1～問17 ストラテジ(業務)系>

#### 問1 ITを活用して個々の学習者の効率・効果を高める仕組み

##### [正解]ア

正解は**アダプティブラーニング**<p.170> (ア)。アダプティブ (adaptive) は「順応して」という意味。記録した学習履歴などから、学習者ひとり一人の知識量や理解度に合った教材を判断して、進捗状況に合わせて最適なタイミングで提供するなど、修得効果の高い学習環境を提供する。

- イ：タレントとは、才能や適性のこと。**タレントマネジメント**<p.169>は、従業員が持つ技能・能力・経験値（職歴など）を記録し、集約管理することで、人材の育成や配置、評価（昇格・昇給）などに活用する管理方法。
- ウ：**ディープラーニング（深層学習）**<p.205>は、大量のデータから共通点・規則性などの特徴をコンピュータに発見させる機械学習で使われる技法。特徴などを発見するための判断を行う仕組みを多階層に重ねる（深層）ことで、より複雑な問題からの確な結果を導き出すことが可能になる。
- エ：ナレッジとは知識のこと。**ナレッジマネジメント**は、各従業員が持っている知識やノウハウなどを一元的に集約し、社内で情報共有するための管理活動。従業員の業務レベルの向上や技能修得にかかる時間の短縮と共に、業務全体の効率化を図ることを目的とする。

#### 問2 値が上限・下限を超えるものを検出する図法(管理図)

##### [正解]ア

キーワードは「品質管理」と「上限・下限の限界線」。正解は**管理図** (ア) <p.184>で、管理が必要な特性の値（部品のサイズ、製品の重さなど）を縦軸にとり、上側に上方管理限界を示す線、下側に下方管理限界を示す線を引く。要素の値でプロット（打点）した点が、限界線に接近したり超えた場合には、何らかの対策が必要だと判断できる。

- イ：**特性要因図**<p.184>は、いくつもの要因が複雑に絡んだ問題を整理するための図法。フィッシュボーンチャート（魚骨図）とも呼ばれる。
- ウ：**パレート図**<p.185>は、値の大きい順に並べた棒グラフと、棒の値の累積和を示す折れ線グラフを重ねて表す図法。要素が全体に占める割合がわかりやすいので、各要素の重要度の判断などに使われる。
- エ：**レーダチャート**<p.184>は、ある要素が持つ複数の特性を、中心から伸びる複数の軸にそれぞれ割り当て、値をプロットすることで、その要素の特徴を視覚的に表す図法。**クモの巣グラフ**とも呼ばれる。

### 問3 販売単価と変動費の差から計算する販売個数(計算問題)

#### [正解]エ

**変動費**<p.179>は、製造個数や販売個数に応じて金額が変わる費用で、原材料費などが含まれる。**固定費**<p.179>は、個数に関わらず一定の金額がかかる費用で、人件費や建物の賃料など。問題には「赤字にならない～少なくとも毎月何個」と書かれているが、これは「**売上高=費用**」となる**損益分岐点**<p.179>の販売個数を計算するということ(表中の販売個数は損益分岐点上の個数ではないので要注意!)

また、出題の暗黙のルールとして「製造された分はすべて販売される」として考え、変動費の合計額は「1個あたりの変動費×販売個数」で計算する(実際には、売れ残りが出るので「製造個数>販売個数」となる)。「損益分岐点での利益を計算する公式<p.179>」を変形して販売個数を求めてもよいが、もっと簡便な方法を探してみよう。

「**変動費**」は「**販売個数**」によって合計値が変わってくる。そこで、この2つの数値を使って計算することを考える。「販売金額800円/1個」と「**変動費**700円/1個」の差額は100円になる。この100円を仮の利益と考え、仮の利益で固定費の600,000円をまかなえれば赤字は出ない。固定費をまかなうために必要な販売個数は、以下の式で求められる。

$$\begin{aligned} & \text{固定費} \div (\text{1個あたりの販売金額} - \text{1個あたりの変動費}) \\ & = 600,000 \text{円} \div (800 \text{円} - 700 \text{円}) = 600,000 \text{円} \div 100 \text{円} = 6,000 \text{個} \end{aligned}$$

### 問4 資本活用の効率性を示す指標

#### [正解]ウ

「**～利益率**」は、その企業が利益を上げる力をどのくらい持っているかを表す指標。「**～比率**」は、財政がどれくらい安定しているかを表す指標。「**～回転率**」は、事業のために使った資産に対して、どれくらい効率よく利益を回収できているかを表す指標で、割合(%)で表す他の指標とは異なり、「1回転、2回転…」という単位で表現する。

- ア**：**売上高営業利益率**は「**営業利益**÷**売上高**(損益計算書<p.174>)」で求め、売上の中で費用などを除いた実際の利益となる割合を表すと共に、売上全体のうちで「本業で稼いだ割合」も示している。
- イ**：**自己資本比率**<p.177>は、「**純資産**(貸借対照表<p.173>)÷**総資産**(貸借対照表：資産の部の合計値)」で求め、**資産のうち自身が持つ資本(自己資本)の割合**を示す。この値が低い場合は、他人資本(借金など)が多く、財政が不安定な状態にある可能性も考えられる。
- ウ**：正解。**総資本回転率**は**総資産回転率**<p.178>とも呼ばれる。「**売上高**(損益計算書)÷**総資本**(総資産と同じ、貸借対照表の資産の部の合計値)」で求める。その企業が持つ資金や設備などの**経営資源を、どれくらい効率的に使って売上を作り出したか**を表す。値が低い場合は、せっかく保有している資産を事業に有効に使えていないことを示す。
- エ**：**損益分岐点比率**は、「**損益分岐点売上高**÷**売上高**(損益計算書)」で求める。損益分岐点売上高<p.179>は利益も損益もでない(売上高=費用)売上額のこと。この値が1(100%)ならば、赤字も黒字も出ていない状態。数値が低い(損益分岐点売上高<実際の売上高)ほど、現状でも利益が出ており、多少売上が減っても赤字にはなりにくいことを示している。

### 問5 著作権に関する正しい記述

#### [正解]イ

- ア**：日本の**著作権法**<p.220>では著作物の作成時点で自動的に権利が発生する。そのため、他の著作物と類似しているからといって直ちにどちらかの権利が否定されることはない。著作者は、類似する著作物による権利の侵害を訴えることができるが、もし裁判により「類似は偶然だった(意図的な模倣ではない)」と判断されれば、相手の著作権の行使を停止させることはできない。
- イ**：正解。日本の著作権制度では、著作物の作成時点で自動的に権利が発生し、出願等の手続きは不要。
- ウ**：著作権法は、元々は人が理解できる形で「**表現された作品**」を守るための法律。そのため、**技術的な思想やアイデア**など、表現としての形がないものは対象外。例えば、アルゴリズムや新たなビジネスモデルなども著作権法の対象外だが、アルゴリズム(営業秘密に該当)は不正競争防止法<p.223>、ビジネスモデルは特許法<p.222>の保護対象となっている。
- エ**：著作権の保護対象の要件として、**新規性(新しい技術やアイデア)を有する必要はない**(特許を取得する場合は新規性が不可欠)。

## 問6 不正アクセス禁止法の禁止行為に該当する事例

### [正解]ア

不正アクセス禁止法の禁止行為<p.224>に該当するかどうか、そのボーダーラインがどこにあるのかを理解しておこう。

- a: 他人のIDとパスワード(認証情報という)を無断で使っているため、不正アクセス禁止法の禁止行為に該当。もしログインをしなくても、他人のIDとパスワードを所持しているだけで禁止行為になるので要注意!
- b,c: 不正アクセス禁止法で禁止している「他人の認証情報を無断使用」「ネットワーク経由の不正アクセス」という要件に違反していないので、不正アクセス禁止法の禁止行為には該当しない。ただし、就業規則や倫理規定への違反行為として、勤務先から懲戒処分を受ける場合もある。特にcの事例はUSBメモリを無断で持ち出していることから、刑法の窃盗罪として処罰される可能性がある。

## 問7 個人情報保護法の定めで本人への通知が必要な項目

### [正解]ウ

個人情報保護法<p.225>では、次の2つの場合には予め本人の同意を得ること(本人に通知またはWebページなどで公表)が定められている。

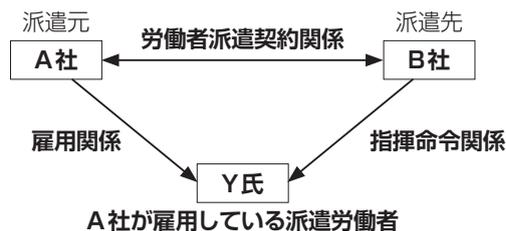
- ①: 情報を得る際に本人に通知した利用目的の範囲を超えて個人情報を利用する場合
  - ②: 収集した情報を第三者に提供するとき。ただし、個人情報保護法の改正により、個人が特定できないように加工したデータ(匿名加工情報)であれば、本人の同意を得ずに第三者に譲渡することも可能<p.226>。
- a: 情報を得た事業者が、利用目的の範囲内で利用するための業務委託であって、第三者への目的外の情報提供ではないため、同意は不要。
  - b: 利用目的の変更は、合理的かどうかを問わず範囲外利用になるため、本人の同意が必要。
  - c: 情報の削除に本人の同意は不要。なお、個人情報保護法では、不要になった情報は遅滞なく消去するよう努めることも定められている。

## 問8 労働者派遣法によって成り立つ関係

### [正解]エ

労働者派遣<p.229>は、雇用関係と指揮命令関係が派遣元と派遣先に振り分けられる雇用形態。もし混乱しそうだったら、配布されるメモ用紙に簡単に三者の関係を書き出すと、スッキリ整理できて誤答を防げる。

A社・B社・Y氏の関係



## 問9 プロバイダ責任制限法によりプロバイダの対応責任の対象となり得る事例

### [正解]ア

プロバイダ責任制限法<p.227>の対象となる事例はaのみ。この法律には、被害者の権利(書込みを行った発信者に関する情報開示の請求権)や、プロバイダが賠償責任を免れる条件(被害者の権利を侵害する情報の掲載を知らなかった場合に発生した被害者の損害に対する賠償、送信(公開)停止の可否を問う発信者への照会)に無回答だった場合に行った送信停止措置で発生した発信者の損害に対する賠償)などが定められている。

- b: マルウェア(ウイルス)の作成や配布を禁じる法律は、刑法のウイルス作成罪<p.228>。
- c: 他人の利用者IDやパスワードの無断使用は、不正アクセス禁止法の禁止事項<p.224>。

## 問10 企業提携と企業買収のデメリットの比較

### 【正解】エ

**企業提携(アライアンス)** <p.190>は企業どうして協力関係を結び、事業の特定部分で協力しあう戦略。

**企業買収(M&A)** <p.190>は相手企業の株を購入して、自社またはグループ企業として吸収し、経営の主導権を握る戦略。株主は保有株数に応じて株主総会の議決権を持つため、過半数の株を保有すれば取締役選任など経営陣の人事に介入でき、2/3以上なら事業の譲渡や会社の合併・分割などの重要案件も可決・成立が可能。

- a: ×提携の場合、相手は別会社なので、自社に合わせた「組織や業務プロセスの改革」は不要 ⇒ 企業買収の場合に生じるデメリット
- b: ○提携の場合、相手は別会社なので、事業戦略など相手企業的意思決定に踏み込むことはできない(そのため、相手方から提携関係を一方的に解除されるケースもある) ⇒ 企業提携の場合に生じるデメリット
- c: ×買収には相手企業の株式の大量取得(過半数または2/3)が不可欠で、買収する側には大きな財政上の負担がかかる ⇒ 企業買収の場合に生じるデメリット

## 問11 BSCを用いた戦略で目標ごとに明確化すべき事項

### 【正解】ウ

**バランススコアカード(BSC)** <p.196>は、戦略実現を目指して「目標設定と達成度の評価」を行うための手法で、4つの視点(財務・顧客・業務プロセス・学習と成長)から具体的な目標を設定する。問われているのは、「バランススコアカードを用いて設定した戦略目標ごとに明確化すべき事項」を指す用語。選択肢から一番フィットするものを探していこう。

**ア:** 企業倫理は**コンプライアンス** <p.234>とも呼ばれ、企業として遵守すべきルールやマナーのこと。

**イ:** **経営理念** <p.168>は、企業活動の指針となる考え方であり、社員・顧客・社会に対して、使命や存在意義を示すもの。

**ウ:** 正解。**重要成功要因(CSF)** <p.196>は、戦略目標達成のために不可欠で、最も重視すべき活動などの要因のこと。例えば、ITベンダがより高度なシステム構築技術を武器にした新規顧客獲得を到達目標とする場合、BSCの「学習と成長」の視点からはエンジニアの専門性の獲得が目標となり、専門エンジニアの採用や社内エンジニアのスキルアップ教育は、目標達成の鍵を握るCSFとなる。

**エ:** **ビジョン**(企業ビジョン)とは、企業が描く将来のあるべき姿、事業を通じて実現したい未来のこと。例えば、「企業としてどのような形で消費者の役に立ちたいか」など、具体的なイメージが示される。

## 問12 SCM導入による業務改善の事例として適切なもの

### 【正解】ウ

**SCM**(供給連鎖管理) <p.202>は、原材料や商品などの仕入れ先や製品などの販売先と情報を共有することで、企業間の物流や生産管理をスムーズに行うための仕組み。正解は売上情報を製造元と共有している**ウ**。

**ア:** ネットショップと実店舗など、複数の販売ルート(チャネルという)を持つことを**マルチチャネル** <p.195>という。さらに各チャネル間で在庫や顧客情報を共有し、商品を融通しあったり、一方の顧客に他方のチャネルの宣伝を送るなど、互いに活用しあって売上増を図ることを**オムニチャネル** <p.195>という。

**イ:** 営業情報やノウハウを共有しあい、営業活動を支援するシステムは**SFA** <p.203>。

**エ:** いろいろなシステムが考えられるが、このような事例としてよく出題されるのは、店頭での販売情報(商品名、販売数量、購入顧客情報など)を即時に本部へ送信する**POSシステム** <p.203>。これらの情報は、在庫・発注管理や商品開発に利用されている。

## 問13 画像認識システムでの機械学習の事例として適切なもの

### 【正解】イ

正解は**イ**。**機械学習** <p.205>の技術を使えば、大量の果物の画像データを比較し、その違いや類似性などを分析することで、「果物」に共通する特徴をコンピュータ自身が見つけ出すことができる。

- ア：瞳の虹彩の画像による認証の仕組みは、**バイオメトリクス認証(生体認証)**の一種<p.120>。
- ウ：タッチパネルから読み取られる指紋の画像と、スマートフォンに保存してある指紋の画像を比べて、合致しているかどうか(本人かどうか)を判断する認証方式は**指紋認証**と呼ばれ、バイオメトリクス認証の一種。
- エ：**チャットボット**<p.152>と呼ばれる仕組みのこと。文字入力や音声入力による会話形式でやり取りし、AIがユーザからの問合せに含まれるキーワードを検出して、予め保存してある適切な答えを選び出して回答する。

#### 問14 前工程と後工程の指示や納品書に電子タグを使う生産方式

**[正解]ア**

**サプライチェーン**<p.202>とは、製品の原材料調達から製造、顧客への納品(一般消費者への販売)までの、モノの流れ全体を指す用語。**内製**とは部品や原材料などを自社内で生産すること。また、電子式タグとは**ICタグ**<p.017>などのことを指す。

- ア：正解。昔は前工程から後工程への指示に、「看板」と呼ばれる指示ボードを使っていたことから、**かんばん方式**<p.210>と呼ばれるようになった。**ジャストインタイム生産方式**<p.210>は、「必要な時に必要な量だけ」部品や原材料が納入され、過剰在庫や欠品が生じないように管理することで、保管のための費用を抑えて生産の流れをスムーズにする管理方式。
- イ：**クラフト生産方式**<p.210>は、**ウ**のセル生産方式の一種。技術的に高度なものや工芸品に分類されるような製品を生産する場合に、一人の熟練工が最後まで作り上げる。
- ウ：**セル生産方式**<p.210>は、一人または数人のグループで製品の生産工程の始め～最後まで作り上げる生産方式。仕様が異なる少量多品種の製品に対応する**個別生産方式**<p.210>などで用いられる。
- エ：**見込み生産方式**<p.210>は、需要予測に基づいて生産量を決定する生産方式。これに対して、**受注生産方式**<p.210>は顧客からの発注があってから生産を行う。

#### 問15 IoTの事例として適切なもの

**[正解]ウ**

**IoT(IoTシステム**<p.026、208>)とは、ネットワークへの接続機能を持つ装置(IoTデバイス<p.027>)を活用する仕組みのことを指し、この問では**ウ**が該当する。実際に、服薬管理が難しい高齢者用に、一回分ごとに分けて薬を入れたケースにセンサを内蔵し、服薬の時間になると音と光で服薬を促し、患者が薬を取り出すとその記録が薬局に送られるというシステムなどが実用化されている。

- ア：インターネット経由で参加できるオークションは、**ライブオークション**と呼ばれる。
- イ：インターネット経由で利用できるのは、**クラウド型グループウェア**。
- エ：インターネットやPCを利用する教育形態は**e-ラーニング**<p.170>と呼ばれる。また、システムを使った学習者の進捗管理や、学習履歴から最適な教材を選択する機能などを含め、積極的に教育サービスにIT技術を活用することを**EdTech**<p.170>という。

#### 問16 RPAの適切な活用方法

**[正解]エ**

- ア：M&Aのような経営戦略に用いるのは**BIツール**<p.204>。BIツールは、専門知識がないユーザでも、利用目的に合った分析方法を使い、大量に蓄積された様々なデータを基に分析し、図表などを用いたわかりやすい分析結果を出すことができる。
- イ：一人ひとりの顧客に合わせたサービスやサポートを行う**ワントゥワンマーケティング**<p.202>を行うときに用いるのは、**CRM(顧客関係管理)システム**<p.202>。
- ウ：大量のデータから規則性を抽出するシステムは、**データ学習型AI**<p.205>。**機械学習**<p.205>の技術を使って学習や分析を行う。
- エ：正解。**RPA**<p.186>は、RPA自身が表計算ソフトやメールソフトなどを操作し、自動的に処理を進めていく機能を持つ。あらかじめ人がRPAに行わせる操作を設定・登録しておく必要があるため、その場ごとに判断が必要な用途には向かず、日常的に業務の中で繰り返されている定型的な事務処理などに適している。

## 問17 クラウドコンピューティングの説明

【正解】ウ

インターネット経由でコンピュータ資源（ハード・ソフト・システム・ストレージなど）を使うことを、**クラウドコンピューティング**<p.217>という（ウ）。なおウの文中にあるスケーラブルとは、「ユーザが必要としている容量や能力（その時々で変化する）に柔軟に対応できる」という意味。

- ア：汎用機などの高性能なコンピュータに処理のためのシステムとデータを集中させる形態は、**集中処理システム**<p.024>。
- イ：システムを利用する側（非エンジニア）の部門に所属するユーザ自身がコンピュータを扱って処理することを**EUC**（End User Computing：エンドユーザコンピューティング）という。昔のコンピュータは、操作が複雑で高度な知識が必要だったため、オペレータと呼ばれる専門の人員しか扱うことができなかった。最近のEUCの定義はさらに一歩進んでおり、ユーザ自身がアプリケーションを開発したり、システムの運用管理に積極的に関わることを指している。
- エ：複数台のコンピュータ（サーバ機など）に処理を分担させる形態のシステムを、**分散処理システム**と呼ぶ<p.024>。

## <問18～問27 マネジメント(管理)系>

### 問18 ブラックボックステストの考え方

【正解】エ

**ブラックボックステスト**<p.135>は、プログラムの中身はブラックボックスとして触れず、与えるデータ（入力）から正しい結果（出力）が導き出されているかを検証するテスト。正解はエ。

ア・イ・ウは、プログラム内部の構造や処理の流れを検証しているため、**ホワイトボックステスト**<p.135>の説明。

### 問19 新機能を迅速にリリースするために開発側と運用側が連携しあう取組

【正解】ア

正解はア。**DevOps**<p.138>は「Development and Operations（開発と運用）」を略した言葉。開発者と運用担当者がチームを組み、さらに移行ツールなどの自動化ツールを積極的に取り入れることで、新たなシステムやソフトウェアを素早くスムーズにリリースできるようにすることがDevOpsの目的。

- イ：**RAD**<p.138>は、**プロトタイプング**<p.136>を行いながら、少人数の開発チームで迅速にソフトウェアを作成する手法。「高速アプリケーション開発」とも呼ばれる。**RADツール**を使えば、アイコン等を使った視覚的な操作でプログラムを半自動生成したり、予め用意されている基本的な処理機能のモジュールを活用するなど、開発作業そのものを高速化することが可能だ。
- ウ：**オブジェクト指向開発（オブジェクト指向アプローチ）**<p.137>は、これまでの**プロセス中心アプローチ**（業務で行う「処理」に注目してシステムを構築）や**データ中心アプローチ**（業務に使う「データ」に注目してシステムを構築）とは異なり、データとそのデータに対して行う処理を一体化して扱うシステム構築の設計思想。
- エ：**テスト駆動開発（TDD**<p.138>）は、まず始めに、作成するソフトウェアの各機能に対して「何を検証するために、どんな内容でテストする必要があるか」を考えて、先にテストケースを作成。その上で、それらのテストをクリアできるようにプログラムを書いていく設計手法。テストケースを先に考えることで、プログラムに実装すべき機能を明確にすることが目的。

## 問20 アジャイル開発の特徴

【正解】エ

アジャイルは「素早い」「機敏な」という意味。**アジャイル開発**<p.138>はシステムを機能単位に分けて作り、単位ごとに短期間で要件定義～リリース(実稼働)を繰り返すことで、全体を作り上げていくシステムの開発技法。ドキュメント(要件定義書や設計書)をしっかりと作成し、それを基に後工程で実現(プログラミングや構築)する、ドキュメント至上主義的な**ウォーターフォール**<p.131>とは異なり、頻繁にユーザとコミュニケーションを取って変化するユーザの要望に柔軟に対応していくのがアジャイル開発の特徴(**エ**)。

- ア・ウ：工程が一方通行で進むため全体の進捗は管理しやすいが、修正や変更が発生すると前工程に戻って作業(手戻り作業)を行うため、大きく時間・手間・コストが掛かってしまうのが**ウォーターフォール**の欠点。
- イ：**プロトタイプ**(試作品)の作成は、システム要件(必要な機能や性能など<p.132>)などをユーザが確認することが目的。そのため、**プロトタイプング**<p.136>では開発の初期段階でプロトタイプを作成。また、**スパイラルモデル**<p.137>の各段階で作成するのは本稼働用のソフトウェアで、プロトタイプではない。

## 問21 プロジェクト管理のプロジェクトスコープで定義すべき事項

【正解】イ

スコープとは「範囲」のこと。関連する問題が毎回必ず出る重要用語だ。

- ア：プロジェクトチームの役割や責任 ⇒ **プロジェクト憲章**<p.141>で定義。
- イ：正解。「プロジェクトで実施すべき作業」を意識すると「プロジェクトで行うべき作業範囲」。つまり、**プロジェクトスコープ**<p.142>を指す。
- ウ：各作業の開始予定日と終了予定日 ⇒ プロジェクトマネジメントの対象群「**時間**<p.143>」で策定。
- エ：実施に必要な費用⇒プロジェクトマネジメントの対象群「**コスト**<p.145>」で策定。

## 問22 PERT図を使った所要日数の計算

【正解】ウ

図のような所要日数の計算に用いられる**アローダイアグラム**(矢線図)のことを、**PERT図**<p.144>という。この問題では、作業Dが2日増加(遅延)し、作業Fが3日減少(前倒し)したことによる、全体の作業日数の変化を計算すればよい。全体の作業日数の計算は、矢印の作業を順にたどって合計日数を計算し、一番長い経路の合計日数がその作業全体の作業日数になる。

<作業予定の作成時>

A→C→F：2日+4日+5日=11日  
B→D→F：3日+1日+5日=9日  
B→E→G：3日+1日+5日=9日

<実際の作業日数>

A→C→F：2日+4日+2日=8日  
B→D→F：3日+3日+2日=8日  
B→E→G：3日+1日+5日=9日

予定時点での全体の作業日数は、A→C→Fの11日。実際の作業では、B→E→Gが一番日数が多く、予定に比べて2日減少しているので、答えは「2日前倒し(ウ)」

## 問23 ヘルプデスクの対応方法の合意に用いられる文書

【正解】エ

提供するITサービスの内容・方法・提供時間・品質などについて、提供側と利用者側で合意しておくための文書は**SLA(サービスレベル合意書)**<p.150>。

また、**チャットボット**<p.152>とは、利用者からのテキストや音声での質問に対して、会話形式でリアルタイムに回答していく対話型のシステムのこと。質問に含まれる言葉からキーワードを抽出し、蓄積されたデータの中から適切な返事を返すように作られている。

- ア：BCPはトラブル発生に備えて予め対応をマニュアル化しておく**事業継続計画**<p.168>。  
イ：NDAは知り得た秘密を外部に漏らすことを禁じる**守秘義務契約**<p.230>。  
ウ：RFPはシステム開発の委託先を検討する際に候補となる開発ベンダに提案の提出を依頼する**提案依頼書**<p.148>。

## 問24 自動応答技術でコミュニケーションを行うツール

### 【正解】エ

利用者の問合せ内容を判断し、**自然言語処理**<p.206>など技術を使い、簡単な会話形式の応答を行うツールは**チャットボット**<p.152>(問23の解説も参照のこと)。

- ア：**FAQ**<p.152>は問合せが多い質問の内容と回答をまとめたもの。同じ内容の質問であれば、ユーザ自らがFAQから解決策を探ることができる。  
イ：**RPA**<p.186>は事務作業の自動化を行うための仕組みやツールのこと。  
ウ：**エスカレーション**<p.152>は、サービスデスクの受付担当者では解決できない問合せの場合に、より上級の責任者や専門の技術者が代わって対応すること。

## 問25 ファシリティマネジメントの実施事項

### 【正解】イ

**ファシリティマネジメント**<p.156>は、装置や設備を適切で安全な状態に保つための管理活動。a～dの中で該当するのは、**a**の建物への入退出管理と、**d**の**無停電電源装置**<p.156>の設置なので、正解は**イ**。

なお、**b**のマルウェア対策ソフトの導入・更新は**セキュリティ管理**<p.161>や**ソフトウェア保守**<p.135>、**c**のソフトウェアのライセンス管理はサービスマネジメント(運用)の**構成管理**<p.151>の活動に該当する。

## 問26 システム監査人の所属として適切な組織

### 【正解】ア

**システム監査**<p.165>を行う**監査人**としては、「監査結果(評価)の良し悪しが、自身の利害に直接的に関係する人」は適切ではない。この問題の例では、メールサービスの運用(**イ**)・開発(**ウ**)・企画(**エ**)に携わっている人は利害関係者になるため、残っている**ア**の「社長直轄の品質保証部門」が正解になる。

## 問27 内部統制を目的として実装した機能の実現例

### 【正解】イ

**内部統制**<p.232>とは、企業の内部で不正や違法行為が行われることを防ぐための仕組みや活動のこと。「利用者IDとパスワードを入力させて、登録情報と一致しない場合は業務メニュー画面に遷移しない」という仕組みを実装しているので、実現している機能は「システムによるアクセス制御(**イ**)」。

### 問28 10進数から2進数への基数変換

**【正解】ア**

筆算で**基数変換**<p.035>する方法を覚えておこう。試験会場ではメモ用紙とシャープペンが配られるので、これを使って計算していく。

2進数では桁が増えるごとに、右隣の桁の値の2倍になる。10進数との対応を見ると一目瞭然だ。

$1_{(2)} = 1_{(10)}$ 、 $10_{(2)} = 2_{(10)}$ 、 $100_{(2)} = 4_{(10)}$ 、 $1000_{(2)} = 8_{(10)}$ 、 $10000_{(2)} = 16_{(10)}$ …

この法則を逆に使い、10進数の値を2で割っていき、出てきたあまりの値を書き連ねていくと、簡単に2進数へ変換することができる。

割られる数が「1」になったら、それを2進数の左端の桁(一番大きな桁)として、下から上にあまりの値を順に並べていくと、2進数の値が求められる。答えは10011011(ア)。

```

)155
)77 … 1 (155÷2=77 あまり1)
)38 … 1 (77÷2=38 あまり1)
)19 … 0 (38÷2=19 あまり0)
)9 … 1 (19÷2=9 あまり1)
)4 … 1 (9÷2=4 あまり1)
)2 … 0 (4÷2=2 あまり0)
)1 … 0 (2÷2=1 あまり0)
      1 (1÷2=0 あまり1)
      ↑
    
```

割られる数が「1」になったら、(これ以上は割れないので)最後の割り算を省略。

この「1」を2進数の左端桁(一番大きな桁)として値を並べていくと、2進数を求められる。

### 問29 ディープラーニングの説明

**【正解】イ**

正解は**イ**。この選択肢に書かれている「大量のデータ」「ニューラルネットワーク」「自ら規則性を見つけ」「推論や判断」は、どれも**ディープラーニング(深層学習)**<p.205>の重要キーワードなので、しっかり覚えておこう。

**ア**は**e-ラーニング**<p.170>、**ウ**は**エキスパートシステム**<p.205>、**エ**は**アダプティブラーニング**<p.170>のこと。

### 問30 CPUの性能を示す値とその性能がもたらす効果

**【正解】ア**

正解は**ア**。「データ長」とは、あるデータが持つ桁の長さのこと。コンピュータは全ての情報を2進数のビット列に変換して処理しており<p.032>、例えば「あ」という文字は16ビット(2進数16桁)のビット列として扱われている。

**32ビットCPU**はビット列の32桁のデータを一度に処理でき、**64ビットCPU**は64桁のデータを一度に処理できることを意味する<p.007>。そのため、64ビットCPUの方が、より長い(大きい)データを一度に扱うことが可能で、処理速度は速くなる。

**イ**：**キャッシュメモリ**<p.011>は、CPUと主記憶装置の間に置かれ、主記憶装置より高速(容量は小さい)で、一時的にデータを置いておくために使われる。CPUは、まずキャッシュメモリから目的のデータを探すので、キャッシュメモリの容量が「多い」ほど処理速度は向上する。

**ウ**：**クロック**<p.007>は、コンピュータに内蔵された各装置が同期して動作するための信号。この信号の周波数(1秒間の発生回数=**クロック周波数**)を「上げる」と、1秒間あたりのCPUの動作回数は増えるので、処理速度は向上する。

**エ**：**コア**<p.006>とはCPUの主要部分(制御装置と演算装置)のことで、**マルチコアプロセッサ**は複数あるコアの各コアに処理を振り分けて並行して動作させる。デュアルは2個、クアッドは4個のコアを持つため、クアッドコアの方が同時実行できる処理数を多くすることができる。

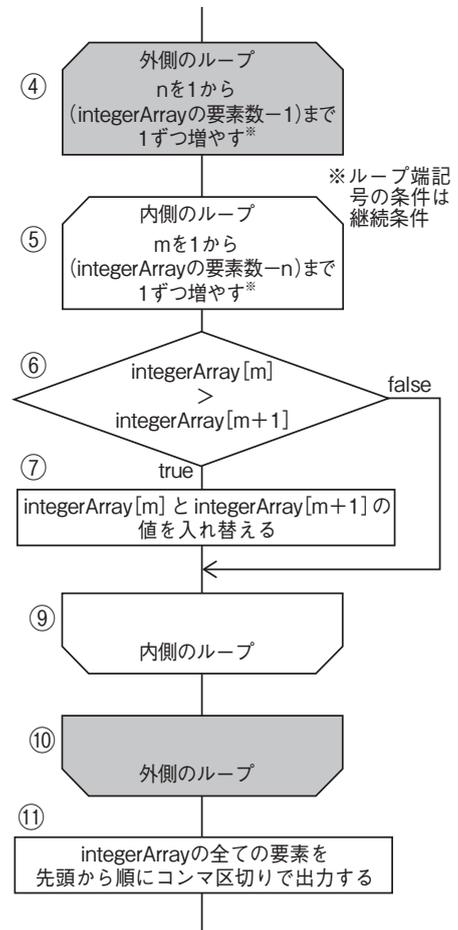
### 問31 for文の入れ子を使った繰返し処理

#### 【正解】ア

解説のために、左端に行番号を振ったプログラムを再掲する。このプログラムでは、**for文**<p.065>を使った繰返し処理が、4～10行目(外側)と5～9行目(内側)の入れ子で使われている。大まかな処理の流れを、流れ図で見ておこう(丸付き数字はプログラムの行番号)。

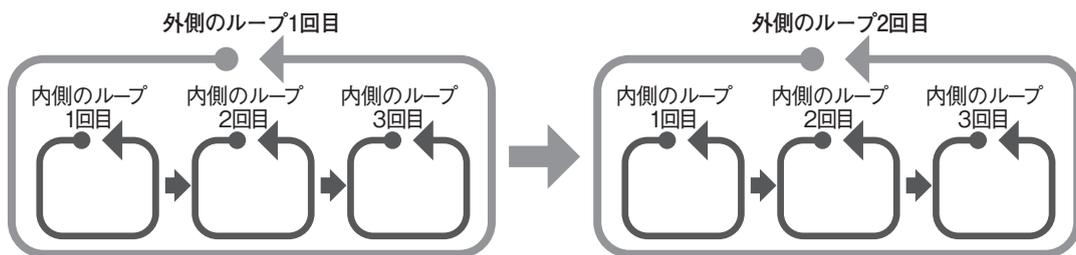
```

1  ○printArray ()
2  整数型: n, m
3  整数型の配列: integerArray ← {2, 4, 1, 3}
4  for (nを1から (integerArrayの要素数 - 1) まで
    1ずつ増やす)
5      for (mを1から (integerArrayの要素数 - n) まで
        1ずつ増やす)
6          if (integerArray[m] > integerArray[m + 1])
7              integerArray[m]とintegerArray[m + 1]の
                値を入れ替える
8          endif
9      endfor
10 endfor
11 integerArrayの全ての要素を先頭から順に
    コンマ区切りで出力する
    
```



#### ●入れ子の繰返し処理

入れ子の繰返し構造では、外側の繰返しの1回目でも内側の繰返しの各回が行われ、さらに外側の2回目でも内側の各回が行われ…、というように処理が進んでいく(図の例は、外側の繰返し2回、内側の繰返し3回の場合)。



#### ●配列integerArrayに対して行っている処理

複雑なfor文の入れ子の読み取りは後回しにして、配列の値の並べ替えを行っている箇所を先に見ておこう。

配列integerArrayの並べ替え処理は、6～9行目の**if文**<p.055>に書かれている。6行目では、配列の要素の値の大きさを比べている。比較する2つの要素の**要素番号**<p.063>を、[m]と[m+1]で指定しているが、これは配列の「ある要素」と「その右隣にある要素」という指定。要素の指定方法として、とてもよく使われるので、覚えておこう。

if文の内側の処理(7行目)に入る条件は、「左側の要素の値が右側の要素の値より大きい」となる。もし、左側>右側だった場合は、7行目の処理で左側(要素番号[m])と右側(要素番号[m+1])の値を入れ替える。「隣の要素と比較して入れ替える」という操作から、この処理は**バブルソート**<p.051>の並べ替えを行っているのではないかと予想できる。

● for文で制御する配列の操作の範囲

5行目にある内側のfor文の制御記述から見てみよう。ここでは、繰り返すごとに、変数mの値が初期値の1から、ひとつずつ増えていく。変数mの値は配列integerArrayの要素番号を示すので（前ページ）、大小関係と比較する隣り合った2つの要素の位置が、配列の先頭から末尾側へと、内側の繰返し1回ごとにずれていくことになる。

外側のfor文の制御記述（4行目）では、「nを1から配列の要素数-1まで増やす」とある。配列integerArrayの要素数は4なので、繰り返すごとに変数nは1→2→3と変化する。

内側のfor文（5行目）では、変数nを「1から配列の要素数-nまで」と変数mの終値を計算するために使っており、これは値の大小を比べる範囲を、配列のどこまでにするのか（比較する範囲の右端）の指定になっている。外側の繰返しが進むと、変数nの値が増えるので、逆に変数mの値の幅は小さくなり、要素の値を比較する範囲が狭くなっていく。

●プログラムの処理の動き（下図を参照）

6～8行目のif文が行っている処理を、配列の要素の値の変化で追ってみよう（下図）。「左>右なら値を交換、左<右ならそのまま」という操作を繰り返して、配列の末尾まで処理を終えると、外側のfor文の1回目の繰返しの終わりに、この配列の最大値「4」が右端に移動してきた。

この例では、たまたま外側1回目で2番目に大きい「3」が右端から2つ目の要素に移動を完了している。しかし通常は、外側2回目で2番目に大きな値が右端から2つ目の要素に移動、3回目で3番目に大きな値が右端から3つ目の要素に移動…、という処理手順で進んでいくことを知っておこう。

予想していたとおり、このプログラムは隣りあう値の大小関係を整えながら、値を昇順に並べ替える「バブルソート」の処理を行っている。並べ替えの結果は図の通りで、正解は**ア**。

		要素番号	[1]	[2]	[3]	[4]		
			2	4	1	3		
<hr/>								
外側1回目、nは1 (4-1でmは3まで、比較の範囲は要素番号1~4)	内側1回目、mは1	[m]	[m+1]	2	4	1	3	
							2 < 4なのでママ	
	内側2回目、mは2	[m]	[m+1]	2	4	1	3	
						4 > 1なので入替え		
			2	1	4	3		
		内側3回目、mは3	[m]	[m+1]	2	1	4	3
						4 > 3なので入替え		
			2	1	3	4		
						最大値の「4」が ↑ 右端に移動してきた		
<hr/>								
外側2回目、nは2 (4-2でmは2まで、比較の範囲は要素番号1~3)	内側1回目、mは1	[m]	[m+1]	2	1	3	4	
							2 > 1なので入替え	
	内側2回目、mは2	[m]	[m+1]	1	2	3	4	
						2 < 3なのでママ		
			1	2	3	4		
		外側3回目、nは3 (4-3でmは1まで、比較の範囲は要素番号1~2)	[m]	[m+1]	1	2	3	4
						1 < 2なのでママ		

### 問32 1次および2次のキャッシュメモリに関する説明

【正解】ウ

以前は**キャッシュメモリ**<p.011>とは何かを簡単に問う問題だったのだが、1次キャッシュと2次キャッシュの違いなど、より詳しく問われることが多くなってきた。

CPUがメモリにアクセスする時の優先順位は、**1次キャッシュ→2次キャッシュ→メインメモリ(主記憶装置)**<p.010>の順(ウ)。問題文では、優先順位の高い側のメモリを「CPUに近い」「より上」と表現していることがある。

- ア：記憶できるデータの容量は、メインメモリ>2次キャッシュ>1次キャッシュの順に少なくなる。
- イ：読み書き(アクセス)の速度は、1次キャッシュ>2次キャッシュ>メインメモリの順に遅くなる。
- エ：データがキャッシュに存在すればその分処理は速くなるが、キャッシュになければメインメモリや補助記憶装置<p.010>(HDDやSSD)から必要な部分をその都度読み出すので、動作させることは可能だ。

### 問33 探索アルゴリズムの特徴

【正解】イ

ITパスポート試験でよく出題される探索アルゴリズムは、**線形探索**<p.050>と**2分探索**<p.050>だけなので、この2つの特徴をしっかりと確認しておこう。

**イ**と**エ**に出てくる**計算量**とは、結果を出すまでに掛かった処理の回数(ステップ数)のことで、計算量が多いほど処理時間も長くなる。計算量は、アルゴリズムやプログラムの効率性を示す数値として使われる。

- ア：探索対象となる配列の、「先頭から順に探索する」のは**線形探索**。
- イ：正解。**線形探索**では、先頭の要素から順に要素の値と検索値とを照合して探すので、計算量は値が一致する要素が配列のどの位置にあるのかで決まる。ただし、平均すると配列の要素数に比例しており、要素数が多くなるほど計算量も多くなる。
- ウ：事前に要素を「値の昇順または降順に並べ替え(ソート)しておく」必要があるのは、**2分探索**。
- エ：**2分探索**は、探索の範囲を真ん中から2分割して、分割したブロックの端の要素と検索値を照合する処理を繰り返す。そのため、もし検索値と同値の要素が先頭や末尾付近にあると、その要素がブロックの端になるまで分割を繰り返すので、分割の回数が増え計算量が増大する。これに対して、**線形探索**は先頭から順に探すため、もし先頭付近にあれば、要素の値と検索値の照合回数は少なくすむため、計算量も少なくなる。

### 問34 合否判定に用いる表計算ソフトの条件式

【正解】ウ

#### ●IF関数の構造

まず、選択肢に示されている**IF関数**<p.071>の構造を見ておこう。細かいところに違いはあるが、4つの選択肢の骨組みは同じになっている。

IF関数の条件式(式1)になっている**論理関数**<p.072>は、値が論理関数の条件を満たせばIF関数にtrue(真)を返し、値が論理関数の条件を満たさないときはfalse(偽)を返す。

なお、' 'は内側に文字列が入っていることを示す。この問題の選択肢のように、IF関数の式2と式3に'文字列'のみが書かれているときは、特に計算処理などは行わず、' '内の文字列を表示するだけの処理になる。

<b>IF(論理関数((A2+B2)≥120, A2=100, B2=100),</b>	式2: trueのときの処理 <b>'?合格'</b> ,	<b>'?合格')</b>
式1: IF関数の条件式(論理関数が使われている)		式3: falseのときの処理
論理関数からtrue(真)が結果として返ってくれば、式2の処理を実行		
論理関数からfalse(偽)が結果として返ってくれば、式3の処理を実行		

#### ●合格になる条件の整理と論理関数の式の意味

論理関数の( )内の、3つの条件式を詳しく見ていこう。

- ①(A2+B2)≥120 → 科目Xと科目Yの合計得点が120点以上
- ②A2=100 → 科目Xの得点が100点
- ③B2=100 → 科目Yの得点が100点

「合格」と表示する条件として、問題文の中に「合格判定条件(1)または(2)に該当するとき」と記述されていることを見落とさないようにしましょう。また(2)の条件式では、「少なくとも一つが100点」と書かれている。これらをまとめると、以下の3つの条件のどれかを満たせば、「合格」と表示することになる。

【①合計得点が120点以上】 【②科目Xが100点】 【③科目Yが100点】

### ●論理関数の結果と合格/不合格の組合せ

いくつかの条件のうち、どれか一つでも満たせば(複数の条件を満たすときもOK) trueを返す論理関数は**論理関数**<p.072>となる(正解は**ウかエ**)。

また、論理関数からtrueが返ってくるのは「合格の条件を満たすとき」なので、IF関数の式2は「合格」。falseが返されるのは「不合格のとき」なので、IF関数の式3は「不合格」となる。したがって、正解は**ウ**。

## 問35 OSSの定義にあてはまる要件

【正解】ア

あるソフトウェアを**OSS**<p.022>とするには、「著作権は放棄されていない」「利用者を限定するような制限がない」「利用者が改変して再配布することも可能」などの要件を満たす必要がある。

- a: 正しい。OSSのソフトウェアでは、利用者が手を加えて再配布することも可能。
- b: 誤り。OSSのソフトウェアでは、有償サポートの強制など利用条件の制限はない。
- c: 誤り。OSSのソフトウェアの著作権は、著作権が保持している。著作権が放棄されているソフトウェアは、**PDS**(パブリックドメインソフトウェア<p.222>)。

## 問36 関係データベースで主キーを設定する理由

【正解】エ

**主キー**<p.079>とは、関係データベースの表で、表中のある1行(レコード)を特定するためのフィールドとして設定される列のこと。主キーに設定する列のフィールドの値には、「他の行と重複する値はNG(一意性制約)」「空値はNG(**NOT NULL**制約)」という制約がある。この2つの制約があるため、主キーを設定して、主キーのフィールドを検索の対象にすれば、「表中のレコードを一意に識別できるようになる(**エ**)」。

- ア**: 列を設定するときに、その列のフィールドに入れることができるデータの型(数値型、文字列型など)を指定するが、主キーを算術演算の対象外(=数値型以外の型)にしなければならないという制約はない。
- イ**: 特別な設定をしなくても、主キーも主キー以外の列のフィールドも検索の対象にできるため誤り。
- ウ**: 主キーは他の表からの参照のために設定するので、誤り(外部キーのルール<p.079>を参照)。

## 問37 関係データベースの表から、結合と選択で抽出される行数

【正解】イ

関係データベースの集合演算のひとつである**結合**<p.083>は、同じ意味を持つ列にあるフィールドの値を使って、複数の表を横につなげる操作。この問題では、両方の表に共通する部署コードを使って、部署表から部署名と所在地を入れ込んで結合する。

①結合: 部署表から「部署コード」の値が同じ行を結合させる

部署表から入れ込んだ部分

社員ID	氏名	部署コード	部署名	所在地	住所
H001	伊藤 花子	G02	営業部	神奈川県	神奈川県
H002	高橋 四郎	G01	総務部	東京都	神奈川県
H003	鈴木 一郎	G03	製造部	愛知県	三重県
H004	田中 春子	G04	開発部	大阪府	大阪府
H005	渡辺 二郎	G03	製造部	愛知県	愛知県
H006	佐藤 三郎	G02	営業部	神奈川県	神奈川県

また、関係演算のひとつである抽出(選択) <p.083>は、ある列のフィールドの値が条件に一致する行だけを取り出す操作。部署の所在地と社員の住所が異なるのは、H002とH003の2名(2行)なので、正解はイ。

②抽出(選択)：「所在地」と「住所」の値が異なる行のみを取り出す

社員ID	氏名	部署コード	部署名	所在地	住所
H002	高橋 四郎	G01	総務部	東京都	神奈川県
H003	鈴木 一郎	G03	製造部	愛知県	三重県

### 問38 データベースのトランザクション処理で、更新を確定すること

【正解】ア

トランザクション処理 <p.087>で、矛盾なく処理が完了したときのみデータベースの更新内容を「確定」することをコミット <p.087>という(ア)。

イ：スキーマとは、データベースの論理上の構造のこと。

ウ：ロールフォワード <p.088>は、トランザクション処理で障害が起こり、確定ができない場合に行われるデータの回復方法のひとつ。データの障害の程度が大きく、更新前の状態に戻すロールバック <p.087>では復旧できない場合に、前回のバックアップデータを基に、そのバックアップ以降に行われたデータの更新情報(変更履歴)を使って、データを復旧させる。

エ：データベースのロック <p.087>とは、あるユーザがそのデータにアクセスしたり更新している間は、別のユーザがアクセスできないように保護するDBMSの機能のこと。

### 問39 無線LANに使われている技術とその特性

【正解】イ

正しい記述はbのみ(イ)。同じ周波数帯を使った無線LANが近くにあると、電波の波が影響(干渉)しあって、伝送速度が遅くなったり、通信が切れてしまうこともある。

- a：伝送速度は、採用している無線LANの規格 <p.094>や、使っている通信機器の性能、bで起こるような通信環境の影響によって決まる。
- c：ESSIDは端末が検出した複数のAP(アクセスポイント：基地局)のどれが自分の属するLANなのかを区別するための識別子 <p.094>。無線LANであっても、メールの宛先など送信先の指定にはIPアドレスが使われる。

### 問40 LPWAの特徴として適切な説明

【正解】イ

LPWA <p.017>は無線通信の規格で、正しい説明はイ。最長50kmと通信距離が長く、省電力で電池で長期間運用できるため、例えば「山奥で頻繁にはメンテナンスに行けず、電源設備がない場所に設置してある装置」との通信などに使われている。

ア：コンピュータが大量のデータから新たな法則性やパターンを見つけ出す機械学習 <p.205>の説明。

ウ：暗号資産の台帳技術(改ざんのない正しい取引記録を保持する仕組み)で使われるブロックチェーン <p.214>の説明。

エ：無線LANで通信するデータの暗号化に使われるWPA2 <p.094>の説明。

## 問41 通信プロトコルの役割

### [正解]エ

それぞれの選択肢に示されているのは、**TCP/IP** <p.100>を使ったネットワークで用いられるプロトコル(通信規格)。

**ア** : **FTP** <p.101>は、ファイル転送に使うプロトコル。

**イ** : **POP** <p.103>は、メールサーバからメールのデータを取り出すためのプロトコル。

**ウ** : **SMTP** <p.103>は、端末からメールサーバにメールを送ったり、メールサーバ間でメールを転送するためのプロトコル。

**エ** : 正解。**TCP** <p.100>は、通信開始/終了の手続き、転送路の設定、パケットへの分割/組み立てや再送要求など、信頼性の高い通信を行うための機能を持つプロトコル。**IP** <p.100>は、IPアドレスを用いた転送/中継を行うためのプロトコル。2つを組み合わせることが多いため、**TCP/IP**と表記される。TCP/IPは、より上位にあるア～ウのようなプロトコルに、基本的な通信機能を提供する役割も持っている。

## 問42 128ビットのIPアドレスの名称

### [正解]ウ

インターネット上で宛先アドレスとして用いられている、128ビットに拡張したIPアドレスはIPv6 <p.097> (**ウ**)。ちなみに、旧来から使われてきた32ビットのIPアドレスはIPv4。

## 問43 別サイトから不正入手した認証情報を使って不正侵入を試みる攻撃

### [正解]ウ

**認証情報**とは、アクセス制御に用いるアクセスを許可された正当なユーザかどうかを判断するための情報(IDやパスワードなど)のこと。他のWebサイトなどから入手したこれらの情報を、別のサイトのログインに使って、不正なアクセスを試みる攻撃を**パスワードリスト攻撃** <p.115>という。同じIDとパスワードを別のWebサイトでも使い回すユーザが多いので、リストが手に入れば簡単にログインできてしまう。

**ア** : **DoS攻撃** <p.114>は大量のデータを送り付けるなど、攻撃対象となったシステムに過大な負荷を掛けることで、そのシステムが行っているサービスの提供を妨害する攻撃。

**イ** : **SQL**とは、データベースを操作するための簡易言語。**SQLインジェクション** <p.114>は、検索ウィンドウなどにユーザが書き込んだ文字列を基に、データベースにアクセスして結果を返す仕組みを持つサイトに、データの書換えや消去などを命令する有害なSQLの命令文を書き込む攻撃。

**エ** : **フィッシング** <p.115>は、嘘のメールで偽サイトへ誘導し、ユーザの個人情報やクレジットカード情報などを書き込ませて盗み取る攻撃。

## 問44 標的型攻撃に利用され、攻撃対象を遠隔操作する攻撃

### [正解]ア

特定の相手を狙って攻撃する**標的型攻撃** <p.115>に使われ、相手のコンピュータを勝手に遠隔操作できるようにしてしまうウイルスは**RAT** <p.113> (**ア**)。

**イ** : **VPN** <p.109>は、暗号化技術などを使い、公衆回線を仮想的な専用回線として使う技術。

**ウ** : **デバイスドライバ** <p.015>は、プリンタなどの周辺機器を制御するために用いられるソフトウェア。

**エ** : **ランサムウェア** <p.113>は、感染すると勝手にシステムをロックしたりデータを暗号化するなど操作不能にして、その解除のために金品を要求するウイルス。

## 問45 リスクマネジメントのリスク対応

【正解】ア

リスク特定・リスク分析・リスク評価は、リスクアセスメントのプロセスで行われる活動<p.159>。リスク移転・リスク低減・リスク回避・リスク保有はリスクへの対応方法<p.160>で、リスクアセスメントの次のプロセスになる**リスク対応**で決定。そのため正解は**ア**。**リスク移転**は**リスク発生時の損害を第三者に移転すること**。

イ：マルウェア対策ソフト（**ウイルス対策ソフト**<p.112>）の利用は**発生するリスクの影響を極力抑えるリスク低減**に該当するので、この部分は正しい。

ウ：**リスク回避**は**リスクの発生自体を避ける（プロジェクトそのものを中止するなど）対応方法**。

エ：**リスク保有**は**発生するリスクの影響が軽微だと予想される場合などで、積極的な対応を行わない対応方法**。

## 問46 情報セキュリティの三大要素の意味と特徴

【正解】ウ

情報セキュリティの要素について、特に重要とされる三大要素以外の特性も出題されるようになってきたため、本書では**情報セキュリティの7大要素**<p.162>として解説している。**情報セキュリティの三大要素**<p.162>のそれぞれの意味は次のとおり。

**機密性**：許可された者だけが情報資産を利用できること

**完全性**：情報資産の正確さや完全さが保護されていること

**可用性**：正当な利用者が必要としている場合には、滞りなく情報資産を利用できること

ア：情報漏えいのリスクを下げる＝**機密性**の確保

イ：利用者がいつでも利用できるように維持＝**可用性**の確保

ウ：正解。情報資産の保護を必要とする**機密性**と利用者の使い勝手を優先する**可用性**は、相反する性質を持っている。例えば、システムの機能やデータごとにアクセスできる人員が極力少なくなるように設定すれば、システムとしての機密性は高まるが、アクセス権限のない人員が増えてシステム全体の利便性は低下する。

エ：データの滅失や誤入力防止＝**完全性**の確保

## 問47 無線LANのアクセスポイントが端末の接続制限を行う仕組み

【正解】イ

無線LANの内部で、アクセスポイント（AP：基地局）と端末が通信を行う場合に相手を認識するには、その端末固有の識別情報である**MACアドレス**を用いる<p.092>。このため、特定の端末の接続制限を行うときには、その端末の**MACアドレス**で接続の可否を判断する**MACアドレスフィルタリング**<p.094>を用いる（イ）。

ア：**ESSID**は、検出した複数のAPのどれが自分の属するLANなのかを区別するための識別子<p.094>。

ウ：**VPN**は暗号化技術などを用いて、公衆回線を仮想の専用回線として使うための技術<p.109>。

エ：**WPA2**は無線通信などで通信するデータを暗号化するときに使われる暗号方式のひとつ<p.094>。

## 問48 公開鍵暗号方式で通信する場合に必要な秘密鍵の数

【正解】ウ

**公開鍵暗号方式**では、相手に渡す**公開鍵**と自身で保管（非公開）しておく**秘密鍵**のペアを生成して通信に用いる。一方の鍵で暗号化したデータはペアとして作られたもう一方の鍵でないと復号できないのが公開鍵暗号方式の特徴<p.122>。通常、データを相手に送る場合は、次の手順で送られる<p.123 図5-3-4参照>。

①受信者は公開鍵暗号方式の**公開鍵**と**秘密鍵**（鍵ペア）を作成

②受信者は予め送信者に**自分の公開鍵**を送信

③送信者は**受信者の公開鍵**でデータを暗号化して送信

④受信者は**自身の秘密鍵**で送られてきたデータを復号

問題のように4人で相互にデータを送る場合は、4人それぞれがまず鍵ペア（公開鍵と秘密鍵）を作成する。受信者の公開鍵で暗号化されたデータは、受信者本人が持つ秘密鍵（非公開）でないと復号できない。そのため、受信者は同じ公開鍵を何人の相手に渡してもOK（相手ごとに別の鍵ペアを作る必要はない）。各自がそれぞれ1つの鍵ペアを作ればよいので、非公開にする秘密鍵は4人分の合計で4つ。

#### 問49 ファイアウォールの設置で実現できる事柄

【正解】ア

ファイアウォール<p.118>で実現できるのは、aのDMZの構築とbの不正アクセスの防止（ア）。DMZ<p.118>は社外のネットワーク（インターネット）と社内LANの間に作り、メールサーバやWebサーバなど、外部とのやり取りが必要なサーバはDMZに置くことで、外部からは直接社内LANにアクセスできないようにするための緩衝地帯だ。

c： 入口に設置して入退出を管理する装置は、**ドアロックシステム**や**セキュリティゲート**<p.163>。

d： ユーザからの要求を複数のサーバに振り分けて、個々のサーバの過負荷を防ぐ仕組みは**ロードバランサ**と呼ばれる。

#### 問50 情報漏洩を防ぐHDDの廃棄方法

【正解】ア

HDDやSSD、USBメモリなどの記憶媒体では、ファイルを消去したり初期化（論理フォーマット）を行っても、データが書き込まれている位置などを記録している情報が消されるだけで、媒体に書き込まれているデータ自体は残っている（cの状態）。

aのデータ消去用ソフトウェアは、「消去」という名称になっているが、実際にはデータをすべてランダムな情報に書き換えて上書きするための専用ツール。HDDの廃棄では、消去用ソフトウェアでデータを全て書き換えてしまおうか、bのように物理的に読めないように破壊する方法が安全だ。