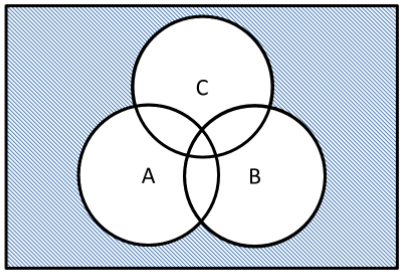
平成 27 年度 秋期 情報セキュリティスペシャリスト

＜午前 I　解答・解説＞

●問 1　正解：エ

そこに属する要素が一つもない集合のことを**空集合**という。

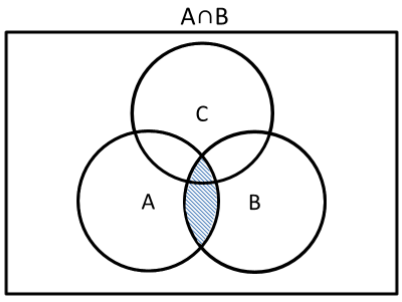
集合 A，B，C を次のベン図で表すと，網掛けの部分が空集合 $\overline{(A \cup B \cup C)}$である。

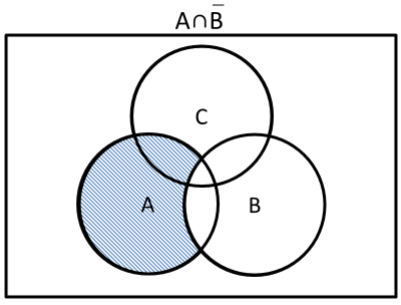


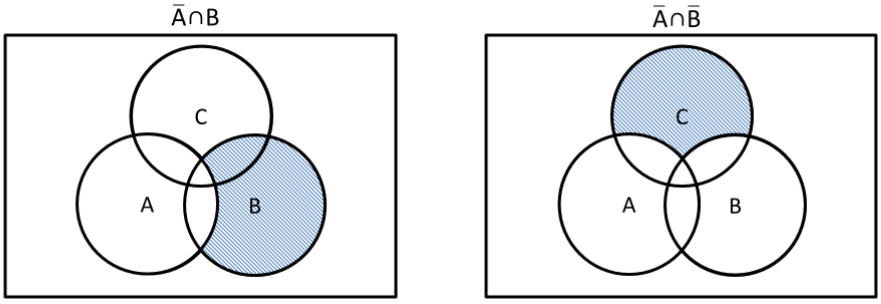
一方，**部分集合**とは，ある集合の全ての要素が他の集合に含まれることであり，例えば，集合 A の全ての要素が集合 B に含まれるとき，A は B の部分集合であり，次の式で表される。

$A \subseteq B$

解答群はいずれも C の部分集合を表す式となっているので，左辺が C の部分集合となるものをベン図を用いて確認する。







これにより，C の部分集合となるのは$\bar{A} \cap \bar{B}$であることがわかる。したがって**エ**が正解。

●問２　正解：ア

各行，列の 1 の個数が偶数もしくは奇数になるようにパリティビットの値を調整することにより，誤り箇所を特定するのがパリティビットによる誤り検出の仕組みである。問題文の方式では，1 ビットの誤り箇所を特定し，訂正することが可能である。同じ行に 2 ビットの誤りがあった場合，列のパリティビットでは誤りを検出できるが，行のパリティビットで誤りを検出できないため，誤り箇所を特定できない。また，異なる行，列に 1 ビットの誤りが 2 箇所あった場合には，誤りを検出できるが，誤り箇所を特定できない。したがって**ア**が正解。

●問３　正解：エ

「ASCII コードでは，昇順に連続した 2 進数が，アルファベット順にコードとして割り当てられている」ということなので，実際の ASCII コードを用いずとも，次のように小文字のアルファベットに 10 進数の 1 から 26 を順に割り当て，1 の位が同じ値となる組合せを見つければよい。

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

ア　a = 1，i = 9 であるため，衝突しない。
イ　b = 2，r = 18 であるため，衝突しない。
ウ　c = 3，l = 12 であるため，衝突しない。
エ　d = 4，x = 24 であるため，衝突が起こる。

したがって**エ**が正解。

●問４　正解：ウ

複数のデータ（Multiple Data）に対して，1 個の命令（Single Instruction）で同一の操作を同時並列に行う方式は，**SIMD** である。したがって**ウ**が正解。

ア　**MIMD**（Multiple Instruction Multiple Data）は，複数のデータに対して複数の命令を処理する方式である。
イ　**MISD**（Multiple Instruction Single Data）は，単一のデータに対して複数の命令を処理する方式である。
エ　**SISD**（Single Instruction Single Data）は，単一のデータに対して 1 個の命令を処理する方式である。

●問５　正解：ウ

ア　**ホットプラグ**とは，機器の電源を入れたままの状態で周辺機器を装着したり，交換したりすることである。
イ　再起動により処理が中断するため，信頼性を向上させる機能としては不適切である。
ウ　適切な記述である。これにより，利用者に障害の発生を感知させることなく代替ノードでアプリケーションを継続実行することが可能となる。
エ　**フェールバック**とは，障害から復旧したシステムを再稼働させるために代替システム等から処理を引き継いで元の状態に戻すことである。

したがって**ウ**が正解。

●問６　正解：ア

デマンド（demand）は「要求する」「必要とする」を意味する単語であり，**デマンドページング**とは，実際に必要が生じたとき（ページフォールトが発生したとき）に該当ページをメモリにロードする方式である。そのため，無駄なページをロードすることがなく，メモリ使用量を節約することができる。したがって**ア**が正解。

デマンドページングに対し，使用することが予測されるページを事前にメモリにロードしておく方式が**プリページング**である。プリページングではメモリの使用量は増加するが，ページフォールトの発生回数が減り，処理性能を向上させる効果がある。

イ　仮想記憶の容量比が大きくなるとページフォールトの発生頻度は高くなる。
ウ　プリページング方式の説明である。
エ　ページフォールトの発生頻度が極端に高くなればスラッシング状態に陥る可能性がある。

●問７　正解：エ

図より，発振器から発生した 15MHz の信号は PLL1 で 8 倍の 120MHz となり，さらに PLL2 で 2 倍の 240MHz になることがわかる。

分周器では，PLL1 が出力した 120MHz の信号を 115kHz にする必要があるので，次のように求めることができる。

$$\frac{120 \times 10^6}{115 \times 10^3} \fallingdotseq 1{,}043 \fallingdotseq 2^{10}\ (1{,}024)$$

であるから，次のように，分周器の値が $\frac{1}{2^{10}}$ であれば SIO に約 115kHz のクロック信号を供給することができる。

$$120 \times 10^6 \times \frac{1}{2^{10}} \fallingdotseq 115 \times 10^3$$

したがって**エ**が正解。

●問８　正解：ウ

問題文に該当するのはニモニックコード（Mnemonic Code）であり，**ウ**が正解。

ニモニックコード（表意コード）は，対象物が連想できるように，名称の一部や数値などを用いて表現したコードである。製品の型番やアセンブリ言語などで使用されている。

ア　**シーケンスコード**は，0001，0002，0003 というように，連続した番号を割り当てる方式である。

イ　**デシマルコード**（10 進コード）は，0～9 の 10 個のグループへの分割・分類を繰り返していく方式である。

エ　**ブロックコード**は，1000～1999，2000～2999，3000～3999 のように，一定の範囲に区切った番号を割り当てる方式である。

●問９　正解：ウ

問題文に該当するのは **H.264/AVC**（Advanced Video Coding）であり，**ウ**が正解。

以前から使用されてきた動画圧縮規格である「MPEG-2」と比較すると，2 倍以上の圧縮効率を実現しており，ディジタルハイビジョン対応のビデオカメラやワンセグ，インターネット上での動画配信等，様々な用途で使用されている。

本規格は ITU-T が「H.264」として，ISO/IEC が「MPEG-4 AVC」として共同策定とな

ったため,「H.264/MPEG-4 AVC」「H.264 | MPEG-4 AVC」などと表記される場合もある。

ア　**AC-3**（Audio Code number 3）は，音声のディジタル符号化方式である。ドルビーディジタル（Dolby Digital）と呼ばれる。

イ　**G.729** は，電話帯域の音声を対象としたディジタル符号化方式であり，IP 電話やインターネット電話等で使用されている。

エ　**MPEG-1** は，データ転送速度が 1.5M ビット／秒程度の圧縮方式であり，CD-ROM などの蓄積メディアを対象とした規格である。

●問 10　正解：ウ

ロールフォワード（前進復帰）によって処理が復旧できるのは，システム障害発生前にコミットされたトランザクションであるため，T4 と T5 が該当する。一方，障害発生時に実行中であったトランザクションはロールバック（後退復帰）によって復旧する必要がある。したがって**ウ**が正解。

●問 11　正解：エ

端末 B の回線速度は端末 A の$\frac{1}{10}$であるため，10 倍の伝送時間を要することになる。

ホストコンピュータでの処理時間を X，端末 A のホストコンピュータへの片道の伝送時間を Y とすると, 端末 A, 端末 B のターンアラウンドタイムは次の式で表すことができる。

端末 A：X + 2Y = 100
端末 B：X + 20Y = 820

この二つの式から，Y の値は次のように求められる。

X = 100 － 2Y
100 － 2Y ＋ 20Y = 820
18Y = 720
Y = 40

したがって**エ**が正解。

●問 12　正解：ウ

公開鍵暗号方式の暗号アルゴリズムは RSA（Rivest Shamir Adleman）である。したがって**ウ**が正解。

RSA は，1978 年に開発された公開鍵暗号方式であり，開発者 3 人の名前の頭文字をとって RSA と名付けられた。桁数の大きな整数の素因数分解が困難であるということを安全性の根拠にしている。

ア　**AES**（Advanced Encryption Standard）は，米国標準の共通鍵暗号方式である。
イ　**KCipher-2** は，九州大学と KDDI 研究所により 2007 年に共同開発されたストリーム暗号方式である。
エ　**SHA-256**（Secure Hash Algorithm 256）は，256 ビットのハッシュ値を出力するハッシュ関数である。

●問 13　正解：ア

ゼロデイ攻撃（zero-day attack）とは，OS やサーバソフトウェア等にある脆弱性が発見された際に，それを修正するセキュリティパッチが提供されるよりも前に，その脆弱性を悪用して行われる攻撃のことである。したがって**ア**が正解。

イ　DDoS（Distributed Denial of Service）攻撃の特徴である。
ウ　フィッシング（Phishing）の特徴である。
エ　スパムメールの特徴である。

●問 14　正解：イ

ブルートフォース攻撃とは，鍵や文字列として考えられる全てのパターンを用いて暗号解読やパスワード破りを試みる攻撃手法である。総当たり攻撃とも呼ばれる。したがって**イ**が正解。

ア　セッションハイジャックの説明である。
ウ　キーロガーの説明である。
エ　リプレイ攻撃の説明である。

●問 15　正解：エ

ペネトレーションテストとは，コンピュータやネットワークに対して実際に侵入や攻撃を試みることで，セキュリティ機能の不備や設定ミス等の脆弱性（セキュリティホール）の有無や，その内容を確認する手法である。したがって**エ**が正解。なお，ア～ウの内容についてはペネトレーションテストで確認することはできない。

●問 16　正解：エ

DFD（Data Flow Diagram）とは，業務やシステムにおけるデータの流れに着目し，そ

の内容をモデル化して視覚的に表した図である。

データストアとは，データを蓄積・保存する場所であり，その実態はファイル，データベースのほか，紙媒体として蓄積される場合もある。

あるデータストアと他のデータストアが直接データフローで結ばれることはなく，必ず何らかの処理が介在する。したがって**エ**が正解。

ア　データが紙媒体で蓄積されるような場合もある。
イ　データストア自身がデータを作成したり変更したりすることはない。
ウ　データは必ずデータフローを通って流れる。

●問 17　正解：エ

共通フレームは，ソフトウェアの企画から設計・開発・運用・保守・廃棄までのライフサイクルプロセス全般に対して，共通の物差し（フレーム）を規定することによって，ソフトウェアの取得者と供給者間の取引を明確化することを目的としている。

ア　個々のプロジェクトにより，アクティビティやタスクを取捨選択して適用する必要がある。
イ　プロセスの実施順序については規定していない。
ウ　特定の開発モデル，技法，ツール等には依存しない。
エ　正しい記述である。

したがって**エ**が正解。

●問 18　正解：ア

EVM（Earned Value Management）は，プロジェクトに進捗や作業のパフォーマンスを定量化（金額換算）し，プロジェクトの現状及び将来の状況を評価する進捗管理手法であり，コストとスケジュールが管理対象となる。したがって**ア**が正解。

●問 19　正解：エ

問題で示されている図は**アローダイヤグラム**もしくは **PERT 図**（Program Evaluation and Review Technique）とも呼ばれ，関連性のある複数の作業からなるプロジェクト等において工程管理を行うために用いられる。関連性のある作業とは，「ある作業が終了しないと次の作業が始められない」という関係のことを意味する。アローダイヤグラムでは，この関係を矢印（アロー）で表しており，凡例にあるように，各矢印が一つの作業を，各矢印の下の数字がその作業の標準日数を表す。

図の中で最も日数を要する経路を「**クリティカルパス**」と呼び，この経路上にある作業を短縮することで，プロジェクト全体の所要日数を短縮することができる。

問題文の PERT 図には次の三つの経路があり，クリティカルパスは「A→B→E→G」である。

A → B → E → G : 4 ＋ 6 ＋ 5 ＋ 5 ＝ 20（日）
A → C → G : 4 ＋ 8 ＋ 5 ＝ 17（日）
A → D → F → G : 4 ＋ 4 ＋ 4 ＋ 5 ＝ 17（日）

クリティカルパス上の作業 A に生じた 1 日の遅れを取り戻すには，クリティカルパス上の他の作業（B，E，G）を 1 日短縮する必要があるが，これらの中で増加費用が最も少ないのは E である。したがって**エ**が正解。

●問 20　正解：イ

IT サービスマネジメントの問題管理プロセスは，インシデントをはじめ，IT サービスにおける問題の根本原因を追究するとともに，恒久的な解決策を策定することを目的としている。したがって**イ**が正解。

●問 21　正解：エ

予備調査は，本調査に先立ち，監査人が監査対象を明確に把握するため，被監査部門から事前に入手した資料等を閲覧することによって行う調査活動である。したがって**エ**が正解。
ア～ウは個別計画策定において行う作業である。

●問 22　正解：ウ

ア　例外取引データに対する処理の正当性の確認にはなるが，起票された受注伝票が漏れなく，重複することなく入力されていることの確認にはならない。
イ　入力された受注伝票データの正確性の確認にはなるが，起票された受注伝票が漏れなく，重複することなく入力されていることの確認にはならない。
ウ　**プルーフリスト**とは，入力データをそのまま出力したものである。プルーフリストと受注伝票との照合が適切に行われているかどうかを監査することにより，起票された受注伝票が漏れなく，重複することなく入力されていることを確認することができる。
エ　**並行シミュレーション法**とは，監査人が用意した検証用プログラムと監査対象プログラムに同一のデータを入力して，両者の実行結果を比較する方法である。これによって受注伝票を処理するプログラムの論理の正当性を確認することはできるが，起票された受注伝票が漏れなく，重複することなく入力されていることの確認にはならない。

したがって**ウ**が正解。

●問 23　正解：ウ

経済産業省発行の「システム管理基準」の「Ⅰ．情報戦略－１．全体最適化－1.1 全体最適化の方針・目標」において，次の六つの事項を求めている。

(1)IT ガバナンスの方針を明確にすること。
(2)情報化投資及び情報化構想の決定における原則を定めること。
(3)情報システム全体の最適化目標を経営戦略に基づいて設定すること。
(4)組織体全体の情報システムのあるべき姿を明確にすること。
(5)システム化によって生ずる組織及び業務の変更の方針を明確にすること。
(6)情報セキュリティ基本方針を明確にすること。

したがって**ウ**が正解。

●問 24　正解：ア

RFI（Request For Information）とは，調達者である企業等が，業務委託や調達を行う際に，自社の要件を取りまとめるための基礎資料として，供給者候補となるベンダ等に情報提供を依頼するための文書である。したがって**ア**が正解。

イ　RFP（Request For Proposal）の説明である。
ウ　RFC（Request For Change）の説明である。
エ　SOW（Statement Of Work）の説明である。

●問 25　正解：ウ

環境省の環境表示ガイドラインに，「**環境表示**」について次のような記述がある。

「環境表示とは，製品の原料採取から製造，流通，使用，リサイクル・廃棄の段階において，環境に配慮した点や環境負荷低減効果等の特徴を説明したものをいい，説明文やシンボルマーク，図表などを用いて行われています」

したがって**ウ**が正解。

●問 26　正解：ウ

垂直統合とは，ある企業が，対象とするビジネスの上流から下流に関わる他の企業を統合することにより，事業を多角化することである。解答群の「製鉄メーカによる鉄鋼石採掘会社の買収・合併」がこれに該当する。したがって**ウ**が正解。

垂直統合のほか，同業他社を統合する「水平統合」，異業種の他社と統合する「混合型」

などがある。

ア　水平統合に該当する。
イ　水平統合に該当する。
エ　混合型に該当する。

●問 27　正解：エ

問題文に該当するのはデルファイ法であり，**エ**が正解。**デルファイ法**は，社会情勢や技術動向等のテーマに関する未来予測を行う場合等に用いられる意見収束技法であり，対象となるテーマについて専門家へのアンケートを実施し，その結果をフィードバックした後で再びアンケートを実施する，という作業を何度か繰り返すことによって意見を収束させていく。

ア　複数データ間の因果関係を分析することで，目的とする解を導き出す手法である。
イ　時間の経過によって変化する事象について，ある一時点で横断的に取得したデータを分析する方法である。
ウ　時間の経過によって得られたデータを回帰分析する手法である。

●問 28　正解：イ

かんばん方式とは，トヨタ生産方式における生産管理方式である。スーパーマーケットや量販店で用いられている，商品名，品番等が記載された商品管理用のカードから考案された「かんばん」と呼ばれる伝票を生産管理工程に使用したことからこの呼称がついた。

かんばん方式では，後工程が前工程に部品を調達しに行く際に「かんばん」を発注票として渡し，前工程は「かんばん」に基づいて必要な部品を生産する。前工程は，「かんばん」の指示量に備え，自工程の在庫を最小限に抑えながら生産しておく必要がある。したがって**イ**が正解。

ア　前工程の生産完了時ではなく，後工程が必要となった際に「かんばん」を発行する。
ウ，エ　前工程は部品の量を必要最小限に抑えながら生産する。

●問 29　正解：エ

ア　**混合戦略**は，複数の戦略を確率によって混合させて実施するものであり，適切でない。
イ　**純粋戦略**は，各計画の確率（不明な場合は均等とする）に基づいて期待利益を計算し，最大となる計画を選ぶ。これによって表の期待利益を計算すると，積極的投資で 233 万円，継続的投資で 200 万円，消極的投資で 283 万円となり，消極的投資に決定する。
ウ　**マクシマックス原理**は，各計画について，最善の場合の期待利益が最大となる計画を

選ぶ。これに従うと，積極的投資で 500 万円，継続的投資で 300 万円，消極的投資で 400 万円となり，積極的投資に決定する。

エ　**マクシミン原理**は，各計画について，最悪の場合の最低確保利益が最大（もしくは損失が最小）となる計画を選ぶ。これに従うと，積極的投資で 50 万円，継続的投資で 100 万円，消極的投資で 200 万円となり，消極的投資に決定する。

したがって**エ**が正解。

●問 30　正解：エ

サイバーセキュリティ基本法は，サイバーセキュリティに関する施策や戦略を明確に定め，総合的かつ効果的に推進することにより，経済社会の活力向上，持続的発展，国民が安全で安心して暮らせる社会の実現，国際社会の平和及び安全の確保，国の安全保障への寄与などを目的としている。サイバーセキュリティ基本法の第 2 条に次のような記述がある。

「この法律において『サイバーセキュリティ』とは，電磁的方式により記録され，又は発信され，伝送され，若しくは受信される情報の漏えい，滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ，その状態が適切に維持管理されていることをいう」

したがって**エ**が正解。