平成26年度 秋期 午前Ⅰ問題の解答・解説

□問 1	エ	□問 11	イ	□問 21	ウ
□問 2	イ	□問 12	ア	□問 22	エ
□問 3	イ	□問 13	ウ	□問 23	ウ
□問 4	エ	□問 14	イ	□問 24	エ
□問 5	エ	□問 15	ア	□問 25	エ
□問 6	エ	□問 16	イ	□問 26	エ
□問 7	ウ	□問 17	ア	□問 27	イ
□問 8	ア	□問 18	ウ	□問 28	エ
□問 9	ウ	□問 19	ウ	□問 29	エ
□問 10	エ	□問 20	ア	□問 30	ウ

問 1：正解エ

本問はカルノー図と等価な論理式を求める問題である。

論理演算はよく知っているものの，カルノー図には馴染みのない読者が多いと思われる。そこで，カルノー図の特徴を知らなくても解ける方法と，カルノー図の特徴を活かして解く方法の 2 通りを解説する。

●カルノー図の特徴を知らなくても解ける方法

本問のカルノー図は，縦軸（AB）が A，B の取り得る値の内訳であり，横軸（CD）が C，D の取り得る値の内訳である。各セルは，カルノー図と等価な論理式に，A ～ D の取り得る値の 1 組を代入したときの，式の値を示している。

例えば，左上のセルは，値が「1」である。このセルは，縦軸（AB）の「00」と，横軸（CD）の「00」が交わる位置にある。したがって，縦軸「A = 0，B = 0」，横軸「C = 0，D = 0」の組を論理式に代入したとき，式の値が「1」になることを示している。

1 個のセルは，A，B，C，D からなる項とみなすことができる。例えば，左上のセルは，「$\overline{A}\cdot\overline{B}\cdot\overline{C}\cdot\overline{D}$」という項に該当する。

カルノー図と等価な論理式は，すべてのセルの合計，すなわち，すべての項の論理和となる。もっとも，セルの値が「0」となる項を論理和の対象から外しても，カルノー図と等価な論理式の値（セルの合計値）は変わらない。そこで，求める論理式を簡略化するため，セルの値が「1」となる項だけを対象とする。つまり，カルノー図と等価な論理式は，セルの値が「1」となる項の論理和に等しくなる。

本問の図を，次の図「カルノー図のセルから項を抽出」の（a）に示す。この図には，値が「1」となるセルが 6 個ある。それらのセルを項として抽出したものを同図の（b）に示す。

AB＼CD	00	01	11	10
00	1	0	0	1
01	0	1	1	0
11	0	1	1	0
10	0	0	0	0

(a) 本文に掲載された図

A	B	C	D	項
0	0	0	0	$\overline{A}\cdot\overline{B}\cdot\overline{C}\cdot\overline{D}$

A	B	C	D	項
0	0	1	0	$\overline{A}\cdot\overline{B}\cdot C\cdot\overline{D}$

A	B	C	D	項
0	1	0	1	$\overline{A}\cdot B\cdot\overline{C}\cdot D$

A	B	C	D	項
0	1	1	1	$\overline{A}\cdot B\cdot C\cdot D$

A	B	C	D	項
1	1	0	1	$A\cdot B\cdot\overline{C}\cdot D$

A	B	C	D	項
1	1	1	1	$A\cdot B\cdot C\cdot D$

(b) セルの値が「1」になる項を抽出した図

図：カルノー図のセルから項を抽出

抽出した 6 個の項の論理和は，次の式となる。

$$\overline{A}\cdot\overline{B}\cdot\overline{C}\cdot\overline{D} + \overline{A}\cdot\overline{B}\cdot C\cdot\overline{D} + \overline{A}\cdot B\cdot\overline{C}\cdot D + \overline{A}\cdot B\cdot C\cdot D + A\cdot B\cdot\overline{C}\cdot D + A\cdot B\cdot C\cdot D$$

この式から共通項をくくり出して簡略化し，選択肢ア～エの中から等しい論理式を探せばよい。

1 ～ 2 番目の項は「$\overline{A}\cdot\overline{B}\cdot\overline{D}$」が共通項であり，3 ～ 6 番目の項は「$B\cdot D$」が共通項であることに着目すると，次のように簡略化できる。

$$\overline{A}\cdot\overline{B}\cdot\overline{D}\cdot(C + \overline{C}) + B\cdot D\cdot(A + \overline{A})\cdot(C + \overline{C})$$
$$= \overline{A}\cdot\overline{B}\cdot\overline{D} + B\cdot D$$

これは，選択肢**エ**の論理式と一致する。よって，これが正解となる。

さて，このようにして解を導くことはできるのだが，共通項をくくり出して「簡略化」する過程が結構大変である。実を言うと，この過程を簡単に成し遂げるのが，カルノー図の特徴を活かして解く方法なのである。

では，次にそれを解説しよう。

●カルノー図の特徴を活かして解く方法

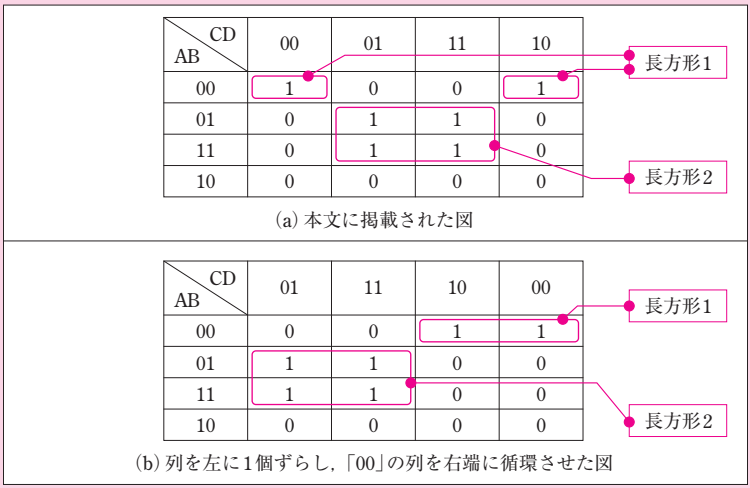
カルノー図では，値が「1」となるセルが連なって長方形になっている領域に着目することによって，簡略化された論理式を見つけることができる。

具体的に言うと，カルノー図の中で，次の条件を満たす長方形の領域に着目する。

1. 長方形の中のセルは，全て 1 である。
2. 長方形の中のセルの数は，2 の冪（2^N）である。

なお，この長方形の領域を見出すとき，図の上端と下端は連続していると考える。同様に，図の左端と右端も連続していると考える。

本問の図には，値が「1」となるセルが 6 個ある。それを次の図「カルノー図にある長方形の領域」の（a）に示す。



図：カルノー図にある長方形の領域

この図には，先ほどの条件を満たす長方形の領域が二つある。それらを「長方形①」「長方形②」と命名する。

この図では，長方形①の存在がやや分かりづらい。これは，図の左端と右端が連続していると考えて，領域を見出したものである。

参考までに，図（a）の列を左に 1 個ずつずらし，「00」の列を右端に循環させた図を，図（b）に示す。両端が連続しているので，このように循環させてもカルノー図の特徴は失われない。図(b)では長方形①の領域が連続して見えるので，その存在が分かりやすい。カルノー図に不慣れなうちは，このように行や列を循環させた上で領域を見出すとよいだろう。

長方形①の領域では，次の論理式（1）が真となる。

$$\overline{A}\cdot\overline{B}\cdot\overline{C}\cdot\overline{D} + \overline{A}\cdot\overline{B}\cdot C\cdot\overline{D} \qquad \text{式(1)}$$

長方形①は，行が「A = 0, B = 0」である。列はいずれも「D = 0」である。したがって，式（1）は，共通項「$\overline{A}\cdot\overline{B}\cdot\overline{D}$」でくくることができる。その結果，式（2）を得る。

$$\begin{aligned}&\overline{A}\cdot\overline{B}\cdot\overline{D}\cdot(C + \overline{C})\\ =\ &\overline{A}\cdot\overline{B}\cdot\overline{D}\end{aligned} \qquad \text{式(2)}$$

長方形②の領域では，次の論理式（3）が真となる。

$$\overline{A}\cdot B\cdot\overline{C}\cdot D + \overline{A}\cdot B\cdot C\cdot D + A\cdot B\cdot\overline{C}\cdot D + A\cdot B\cdot C\cdot D \qquad \text{式(3)}$$

長方形②は，行はいずれも「B = 1」である。列はいずれも「D = 1」である。したがって，式（3）は，共通項「$B\cdot D$」でくくることができる。その結果，式（4）を得る。

$$\begin{aligned}&B\cdot D\cdot(A + \overline{A})\cdot(C + \overline{C})\\ =\ &B\cdot D\end{aligned} \qquad \text{式(4)}$$

先ほど述べたとおり，カルノー図と等価な論理式は，セルの値が「1」となる項の論理和となる。したがって，式（2）と式（4）の論理和となる。これを求めると，式（5）となる。

$$\overline{A}\cdot\overline{B}\cdot\overline{D} + B\cdot D \qquad \text{式(5)}$$

これは，選択肢**エ**の論理式と一致する。よって，これが正解となる。

このように，カルノー図の特徴を活かした方法では，カルノー図の中から長方形の領域を見出し，それぞれの長方形の中で共通項をくくり出すことで，論理式の簡略化が容易になる。

問 2：正解イ

本問に登場する待ち行列のモデルは，M/M/1 である。この待ち行列の特徴を述べた箇条書きの 3 番目には，「1 件の伝票データの処理時間は，平均 T 秒の指数分布に従う」と記述されている。したがって，平均サービス時間は T である。

M/M/1 の待ち行列モデルに従うとき，平均待ち時間（W），平均サービス時間（T），利用率（ρ）の関係は，次の式で表される。

$$W = \frac{\rho}{1 - \rho} \times T$$

本問は，平均待ち時間 W が T 以上となる利用率を求めている。したがって，次の不等式を満たす ρ を求めればよい。

$$T \leqq \frac{\rho}{1 - \rho} \times T$$

これを解くと，$\rho \geqq 0.5$ となる。よって，正解は選択肢イとなる。

問 3：正解イ

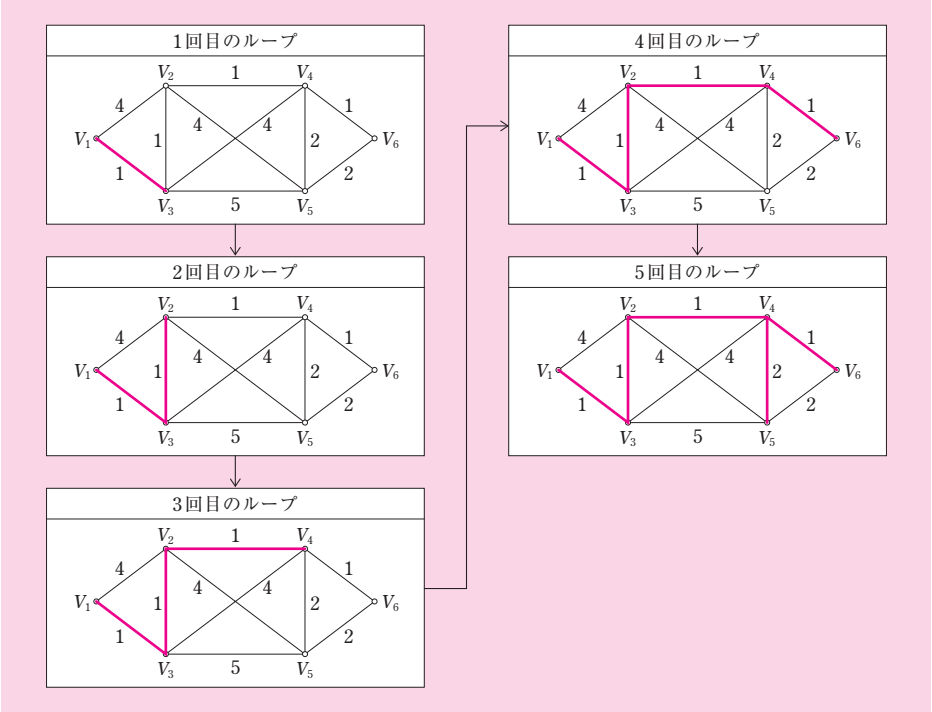
ダイクストラの最短経路アルゴリズムを用いて，頂点 V_1 から各点への最短経路を求めてみよう。

アルゴリズムの大要は，次のとおりである。

1. ［初期状態］始点以外の全ての節は，「未確定」とする。
2. 全ての「未確定」の点について，始点からの所要時間を求める。このとき，始点に隣接していない点は，所要時間を∞とする。
3. 「未確定」の点の中から，始点からの所要時間が最小の点を抽出し，この点を「確定」とする。
4. 全ての「未確定」の点について，これまでに「確定」した各点からの所要時間を求める。
   「確定」した点に隣接していない点は，所要時間を∞のままとする。
   「未確定」の点への所要時間を求めるとき，新たに確定した点を経由することで，所要時間が以前より小さくなることがある。そのときは，所要時間を更新する。
5. 全ての点が「確定」するまで，前記 3 → 4 をループする。

このように，ダイクストラの最短経路アルゴリズムでは，ループ（3 → 4）を繰り返しながら，「確定」する点を徐々に見つけていき，最短経路を求める。

本問のグラフでは，次の図に示すとおり，最短経路が確定していく。



図：V_1 から各頂点への最短経路

V_1 から，V_4，V_5，V_6 の各点への最短所要時間は，最短経路上の各区間の所要時間を合計して求める。

V_1 から V_4 の最短所要時間 = 1 + 1 + 1 = 3
V_1 から V_5 の最短所要時間 = 1 + 1 + 1 + 2 = 5
V_1 から V_6 の最短所要時間 = 1 + 1 + 1 + 1 = 4

最短所要時間を小さい順に並べると，V_4，V_6，V_5 となる。よって，正解は選択肢**イ**となる。

問 4：正解エ

キャッシュメモリへの書込み方式には，ライトスルー方式とライトバック方式がある。

ライトスルー方式では，データをキャッシュメモリと主記憶の両方に同時に書き込む。その結果，主記憶の内容は常に最新である。

ライトバック方式では，データをいったんキャッシュメモリにだけ書き込む。したがって，主記憶のデータは古いままであるが，低速な主記憶に逐一書き込む必要がないため，ライトスルー方式よりも速くなる。

ライトバック方式では，キャッシュメモリの内容を主記憶に書き込むケースが幾つかある。一つは，キャッシュミスが発生し，新たな領域を割り当てるときである。他には，キャッシュメモリの一貫性を保つときである。

ア：ライトスルー方式を使用する目的について述べたものである。
イ：ライトスルー方式を使用する目的について述べたものである。
ウ：ライトスルー方式の方が，キャッシュ管理が簡単になる。
エ：**正解**。ライトバック方式を使用する目的について述べたものである。

問 5：正解エ

解説の便宜を図り，2 台のプリンタを A，B と命名する。A の稼働率を「0.7」，B の稼働率を「0.6」とする。

この 2 台のいずれか一方が稼働していて，他方が故障している確率は，次の式で求まる。

A の稼働率 ×（1 − B の稼働率）+（1 − A の稼働率）× B の稼働率

A，B の稼働率を式に代入し，確率を求めると

$0.7 \times (1 - 0.6) + (1 - 0.7) \times 0.6 = 0.46$

となる。よって，正解は選択肢**エ**となる。

問 6：正解エ

カーネルとは，OS の基本機能を提供するソフトウェアを指す。カーネルが提供する機能

には，プロセス管理，メモリ管理，デバイス管理など，アプリケーションが動作するための機能がある。

Linux カーネルは，UNIX とほぼ同じ動作をするという特徴（UNIX ライク）をもち，GPL ライセンスで頒布されている。

ア：Linux カーネルには，GUI が組み込まれていない。

イ：Linux カーネルには，Web ブラウザ，ワープロソフト，表計算ソフトなどのアプリケーションソフトは含まれていない。

ウ：シェル（shell）は，カーネルを操作するコマンドや実行形式のプログラムを呼び出すソフトウェアである。シェルは，Linux カーネルの一部ではなく，Linux ディストリビューションの中でカーネルと共に提供されるものである。

シェルには，CUI（Character-based User Interface）で操作するコマンドライン型と，GUI（Graphical User Interface）で操作するグラフィカル型の 2 種類がある。とはいえ，Linux をはじめとする UNIX 系 OS において，「シェル」という語は，コマンドライン型のものを指す。

シェルの主な機能には，コマンドやプログラムの実行，環境変数の設定，リダイレクト（プログラムの出力先を指定），パイプ（あるプログラムの出力が別のプログラムの入力になるように指定した上で，それらプログラムを実行），などがある。更に，これら機能の実行を制御する構造（分岐，繰返し等）をもっており，構造化プログラムを記述したスクリプトをシェルのコマンドライン上で実行することができる。

エ：**正解**。Linux カーネルについて述べたものである。

問 7：正解ウ

問 7 で使用されている論理素子の表記ルールについて，問題冊子の 2 ページ目には次のように記されている。

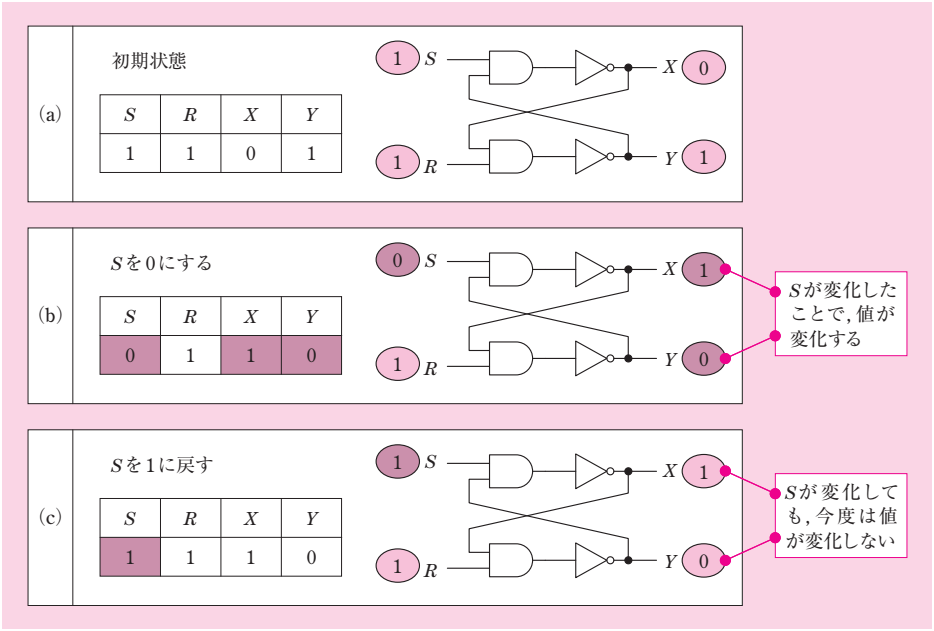
図記号	説明
	論理積素子（AND）
	論理否定器（NOT）

図：論理素子の表記ルール（一部）

問題の論理回路の出力点 X，Y は，次の式を満たす。

$X = \overline{S \cdot Y}$
$Y = \overline{R \cdot X}$

初期状態は，$S = 1$，$R = 1$，$X = 0$，$Y = 1$ である。この状態を，次の図「論理回路の各点の値の変化」の（a）に示す。（a）から，S を 0 にしたときの状態を同図の（b）に示す。更に，（b）から，S を 1 に戻したときの状態を同図の（c）に示す。



図：論理回路の各点の値の変化

図の（b）の状態では，X と Y の値がそれぞれ（a）から反転している。その後，図の（c）の状態に遷移しても，X と Y の値は（b）から変化しない。つまり，$X = 1$，$Y = 0$ となる。

よって，正解は選択肢**ウ**となる。

問 8：正解ア

顧客コードの文字種は，英大文字 A ～ Z の 26 種類である。26 文字で識別するには，対象となる顧客データの個数が，26 の何乗で収まるかが分かればよい。その指数が，求める桁

数となる。

現在の顧客の総数が 8,000 人で，毎年 2 割ずつ増えていくので，3 年後の人数は

$8000 \times 1.2^3 = 13{,}824$

となる。したがって，13,824 は 26^3（= 17,576）より小さいので，顧客コードが 3 桁あれば収まる。

よって，正解は選択肢**ア**となる。

問 9：正解ウ

本問は，与えられた関数従属性から得られる候補キーを問うている。そこで，候補キーについて，まずは解説する。次いで解を導こう。

●候補キー

候補キーは，一意性，極小の二つの性質を満たす属性集合である。

・一意性

一意性とは，関係の中で，「候補キーの値が重複するタプルは存在しない」ということである。別の言い方をすると，「候補キーの値が決まると，関係のタプルが 1 個だけ決まる」ということを意味する。

全ての属性の値が等しいタプルは存在しないので，一意性をもつ属性集合の値が決まると，全ての属性について，属性の値が一つだけ決まる。したがって，全ての属性は，一意性をもつ属性集合に関数従属している。

一意性をもつ属性集合→全ての属性

データベース基礎理論では，ここで述べた「一意性をもつ属性集合」のことを，「スーパーキー」という。

・極小

極小とは，「スーパーキーを構成する属性の中から，どれか一つでも属性を取り去るなら，残った属性集合はもはやスーパーキーでなくなる」ということである。

したがって，候補キーとは，「極小なスーパーキー」のことである。

●解の導出

与えられた関数従属性から，スーパーキーを求めてみる。

A → B　　式(1)
C → D　　式(2)
C → E　　式(3)
{A，C} → F　　式(4)

式（1）に増加律を適用して決定項と従属項に C を増加する。

{A，C} → {B，C}　　式(5)

式（2），（3）に合併律を適用して一緒にした後，これに増加律を適用して決定項と従属項に A を増加する。

{A，C} → {A，D，E}　　式(6)

式（4），（5），（6）に合併律を適用して一緒にする。

{A，C} → {A，B，C，D，E，F}　　式(7)

こうして得られた {A, C} に対し，関係 R の全属性が関数従属している。したがって，{A, C} は関係 R のスーパーキーである。

{A，C} から A 又は C を取り去っても，一意性を保つだろうか。式（4）を見ると，F は C にだけ関数従属してはいないし，A にだけ関数従属してもいないことが分かる。したがって，{A，C} から A 又は C を取り去るなら，スーパーキーとしての性質を失ってしまう。ゆえに，{A，C} は極小である。

以上より，{A，C} は極小なスーパーキーである。すなわち，候補キーである。

よって，正解は選択肢**ウ**となる。

問 10：正解エ

ア：ICMP（Internet Control Message Protocol）は，IP の上位階層のプロトコルである。ICMP は，アプリケーションのデータをペイロードにもつプロトコルではなく，IP ネットワークの制御のために使用されるプロトコルである。例えば，IP パケットの転送エラーを送信元ノードに通知する機能や，接続性を確認するエコー要求／応答メッセージを転送する機能をもつ。

イ：PPP（Point to Point Protocol）は，IP の下位階層に当たるデータリンク層のプロトコルであり，2 点間の通信に使用される。

ウ：TCP（Transmission Control Protocol）は，IP の上位階層に当たるトランスポート層のプロトコルである。コネクション型の通信を行うので，信頼性確保のための確認応答や順序制御などの機能をもつ。

エ：**正解**。UDP（User Datagram Protocol）は，IP の上位階層に当たるトランスポート層のプロトコルである。コネクションレス型のデータグラム通信を行うので，信頼性確保のための確認応答や順序制御などの機能をもたない。

問 11：正解イ

ホストが属するネットワークアドレスは，ホストの IP アドレスとサブネットマスクの論理積で求まる。

ホストアドレスが 172.30.123.45 で，サブネットマスクが 255.255.252.0 であるとき，ネットワークアドレスは，172.30.120.0 となる。

よって，正解は選択肢**イ**となる。

IP アドレス	172.30.123.45	10101100	00011110	01111011	00101101
サブネットマスク	255.255.252.0	11111111	11111111	11111100	00000000
ネットワークアドレス	172.30.120.0	10101100	00011110	01111000	00000000

図：ネットワークアドレスの算出

問 12：正解ア

ア：**正解**。SMTP-AUTH における，SMTP サーバの動作を説明したものである。クライアントの認証に成功したとき，SMTP サーバはクライアントから電子メールを受け

付ける。

イ：信頼できる認証局がクライアントに発行したディジタル証明書を用いた，サーバがクライアント認証を行うときの動作を説明したものである。

ウ：POP before SMTP における，SMTP サーバの動作を説明したものである。クライアントの認証に成功したとき，一定時間だけ，SMTP サーバはクライアントの IP アドレスを送信元とする STMP 通信を受け付ける。

エ：SMTP-AUTH は，利用者が電子メールを送信する際の，STMP サーバが実施する利用者認証である。利用者のメーラから STMP サーバに送信するパスワードを秘匿するため，SMTP-AUTH ではチャレンジレスポンスによる認証を行うことができる。したがって，選択肢エの「パスワードからハッシュ値を計算して」という記述は，誤りである。

問 13：正解ウ

DNS サーバ（フルサービスリゾルバ）は，クライアントから再帰的問合せを受けると，インターネット上の DNS サーバに対して反復的問合せを実行する。そこで得られた回答をクライアントに返信すると共に一定期間キャッシュする。クライアントからの再帰的問合せに対する回答が既にキャッシュされている場合は，反復的問合せを実行せずに，キャッシュされている回答をクライアントに返信する。

さて，あるホストの A レコードに対する反復的問合せを実行している間に攻撃者が偽りの A レコード情報をタイミングよく送信し，DNS サーバがこれを正規の回答であると誤って判断したとする。その結果，その偽りの回答がクライアントに返信され，かつ，一定期間キャッシュされる。この偽りの A レコード情報が DNS サーバにキャッシュされている限り，当該ホストの A レコードを問い合わせたすべてのクライアントは，本来とは異なるホストに誘導されてしまう。これが DNS キャッシュポイズニング攻撃である。

問題文の DNS サーバは「社内用」と記述されているので，フルサービスリゾルバであることが分かる。更に，「インターネット公開用」という記述は，外部から攻撃を受けるリスクがあることを示唆している。したがって，選択肢ウに記述されているとおり，「社内の利用者が，インターネット上の特定の Web サーバを参照する」という状況において，この Web サーバの A レコード情報が DNS キャッシュポイズニングの被害を受けていたとする。その結果，「本来とは異なるサーバに誘導される」という現象が引き起こされることになる。

よって，正解は選択肢**ウ**である。

DNS キャッシュポイズニング攻撃とその対処方法について，詳しくは《基礎編》の第 4 章「4.2.7　DNS キャッシュ汚染」を参照されたい。

問 14：正解イ

SQL インジェクションとは，アプリケーションが想定していない SQL 文を攻撃者が意図的に実行させることで，データベースを不正に操作する攻撃である。データベースと連携している Web サイトは，通常，Web フォームにユーザが入力したパラメータに基づいて動的に SQL 文を生成してデータベースに問合せを行う。攻撃者が入力値に SQL の構文を効果的に埋め込むことで，データベースを不正に操作することが可能となる。

SQL インジェクション攻撃に対処するには，SQL 文の組立てに静的プレースホルダを使用し，ユーザが入力したパラメータをそのプレースホルダに埋め込む方法が有効である。静的プレースホルダを使用すると，データベースは，静的プレースホルダを除外した状態で SQL 文を解析し，パラメータをリテラル値として静的プレースホルダに当てはめる。この結果，たとえパラメータに SQL の構文が含まれていようとも SQL 文の一部として解釈されることがなくなるため，SQL インジェクション攻撃が成立することはない。

静的プレースホルダを使用して SQL 文を組み立てる仕組みのことをバインド機構ともいう。

よって，正解は選択肢**イ**となる。

ア：OS コマンドインジェクションとは，アプリケーションが想定していない OS コマンドを攻撃者が意図的に実行させることで，OS を不正に操作する攻撃である。
Perl や PHP などのプログラム言語には，シェルを起動して OS コマンドを実行できる関数が存在する。Web アプリケーションのプログラムの中でそのような関数を不用意に使用しており，かつ，Web フォームにユーザが入力したパラメータをその関数の引数に渡すと，シェルが起動されてそのパラメータを OS コマンドとして実行してしまう。それゆえ，OS コマンドを効果的にパラメータに埋め込むことで，不正な操作が可能となる。
OS コマンドインジェクションの対策には，そのような仕組みをもつ関数を使用しないことなどがある。
選択肢に記述された「セッション ID を推測困難なものにする」という方法は，セッションハイジャックの対策として有効である。

ウ：クロスサイトスクリプティングとは，Web ページを閲覧した Web ブラウザ上で，悪意あるスクリプトコードを実行させる攻撃である。
掲示板などの Web ページは，ユーザが入力したパラメータに基づいて動的に HTML 形式のページを生成し，画面を表示する仕組みになっている。クロスサイトスクリプティング攻撃の代表的な手口は，このような Web ページで，悪意ある

スクリプトコードを入力データに埋め込んだ状態で画面表示させ，同 Web ページを閲覧した（第三者の）Web ブラウザ上でそのスクリプトを実行させるというものである。

クロスサイトスクリプティングの対策には，ユーザが入力したパラメータを無害化（サニタイジング）してから HTML 形式のページを生成することなどがある。なお，HTML の文法上，パラメータが埋め込まれる位置によって無害化の方法が異なっている。ゆえに，無害化は，ページを生成するタイミングで行うのが適切である。

選択肢に記述された「外部から渡す入力データを Web サーバ内のファイル名として直接指定しない」という方法は，OS コマンドインジェクションやディレクトリトラバーサルの対策として有効である。

エ：セッションハイジャックとは，セッションを用いた通信を第三者に乗っ取られる攻撃である。

Web アプリケーションで用いられる HTTP セッションは，セッション ID で識別される。Web サーバは，クライアントからの HTTP リクエストを受信すると，Cookie や URL に格納されたセッション ID に基づき，これに該当するセッションの処理を行う。したがって，セッション ID が漏えいしたり推測されたりすると，セッションハイジャック攻撃が成立してしまう。

セッションハイジャックの対策には，セッション通信を SSL で暗号化して Cookie を盗まれないようにしたり，新しいセッションが生成されるたびに推測困難な ID を発行したり，セッションタイムアウトを設けて同じセッション ID を長期間にわたって使い続けないようにしたりすることがある。

選択肢に記述された「Web アプリケーションからシェルを起動できないようにする」という方法は，OS コマンドインジェクションの対策として有効である。

問 15：正解ア

WPA2 では，暗号化アリゴリズムに共通鍵方式の AES-CCMP を用いている。

よって，正解は選択肢**ア**となる。

問 16：正解イ

ブラックボックステストとは，テスト対象となっているモジュールが機能仕様どおりに作成されていることを評価するテスト技法である。具体的には，しかるべき手順に基づいて入力したときの結果が当該仕様と一致しているか否かを判定する。同値クラスとは，同じ結果

になる入力値の集合である。したがって，入力値の定義域を分析して同値クラスを見出せば，同値クラスの中から幾つかの代表値をテストデータとして採用できる。つまり，同値クラス分析の結果，テストケースの数を減らすことができる。その際，入力値の定義域が数列のような順序性をもつものである場合，隣り合う同値クラスの境界値をテストデータとして採用する。なぜなら，境界値はしばしば欠陥が発見される入力値であり，機能仕様を評価するという目的に適したテストデータだからである。

よって，正解は選択肢**イ**である。

ア：「無作為」ではなく，機能仕様に基づいてテストデータを作成する。

ウ：「発生頻度」にかかわりなく，定められた機能仕様を網羅するようにテストデータを作成する。

エ：ホワイトボックステストのテストデータ作成方法について記述したものである。ブラックボックステストでは，テスト対象となっているモジュールの内部構造は考慮しない。

問 17：正解ア

著作権法では，著作権は原則として著作者本人に帰属する。ただし，著作権は財産権の一種であるため，著作権の帰属先たる著作権者を契約で定めた場合や，著作者がもつ著作権（著作人格権を除く）の一部または全部を譲渡する旨を契約で定めた場合は，その定めが有効となる。

ソフトウェアの開発委託では，著作者は開発を行った法人となる。したがって，開発成果物の著作権の帰属先を委託元とする契約を交わさない限り，著作権法に基づき，著作権は著作者である委託先に帰属する。このとき，選択肢アに記述されているとおり，委託元は，開発成果物を著作者の許可なく使用することができなくなる。

よって，正解は選択肢**ア**となる。

問 18：正解ウ

ソフトウェア構成管理は，ソースコードの変更履歴を管理する機能をもつ。

構成管理機能をもつツールを使用することで，任意のバージョンのソースコードを復元することや，同じソースコードを複数の開発者が同時に編集してデグレードすることを防ぐことができる。

本問は構成管理の対象項目を問うている。これに該当するのは，選択肢ウの「プログラム

のバージョン」である。よって，正解は選択肢**ウ**となる。

問 19：正解ウ

PMBOK は，工期を短縮させるためにクリティカルパス上の作業に適用する技法として，クラッシングとファストトラッキングの二つを挙げている。

表：工期短縮のための技法

技法	説明
クラッシング	資源を追加投入してコストの増大を最小限に抑えながらスケジュールの所要時間を短縮する技法
ファストトラッキング	通常は順番に実施されるアクティビティやフェーズを並行して遂行するスケジュール短縮技法

注）各技法の説明は，『PMBOK 第 5 版』の 181 ページから引用。

選択肢の中でファストトラッキングに該当するのは，「全体の設計が完了する前に，仕様が固まっているモジュールの開発を開始する」（選択肢ウ）である。よって，正解は選択肢**ウ**となる。

残りの選択肢に記述された，「時間外勤務を実施」（選択肢ア），「生産性を高める開発ツールを導入」（選択肢イ），「要員を追加投入」（選択肢エ）は，資源を追加投入して工期を短縮させる方法なので，クラッシングに該当する。

問 20：正解ア

SLA（Service Level Agreement）とは，IT サービスに関する，IT サービス提供者と顧客との間の合意である。SLA を取り交わすときは，IT サービスの内容とそのサービスレベル目標を文書化し，IT サービス提供者と顧客が果たす責任について規定する。

したがって，選択肢の中で，SLA に記載する内容として最も適切なものは，選択肢**ア**の「サービス及びサービス目標を特定した，サービス提供者と顧客との間の合意事項」である。よって，これが正解となる。

問 21：正解ウ

目標復旧時点（RPO：Recovery Point Objective）とは，障害発生時点から遡って，どの時点までデータを復旧するかを定めた目標値である。

RPO を 24 時間に定めた場合，障害発生時点から 24 時間以内の業務データが，復旧の対

象となる。よって，正解は選択肢ウとなる。

● RPO を 24 時間に定めた場合の対策

広域災害を想定して RPO を 24 時間に定めた場合，その具体的な対策として，被災を免れる遠隔地に副系拠点を設け，主系拠点の 24 時間以内の業務データを副系拠点にバックアップしておく方法が考えられる。

このとき，ネットワーク回線を経由して業務データを副系拠点に転送するのであれば，転送の所要時間を考慮に入れて，バックアップ取得の間隔と頻度を計画する必要がある。

例えば，24 時間無停止で業務を行っている例を取り上げてみよう。主系拠点の 1 日分の業務データ（前日 0：00 ～本日 0：00 の直前）を毎日 0：00 から転送するものとし，その所要時間が 1 時間であるとする。転送している最中（0：00 ～ 1：00）に主系拠点が被災するならば，障害発生以前の全データが主系拠点で消失する可能性，及び，今まさに転送中の前日分データがネットワーク回線で消失する可能性がある。被災を免れているのは，副系拠点で安全に保管された一昨日までのデータなので，この方法では 24 時間という RPO を満たすことができない。

したがって，この例においては，バックアップデータの転送を 1 日 2 回以上実施する必要がある。

問 22：正解エ

データの網羅性とは，業務事象のデータが，漏れなく，重複なく，システムに記録されていることを指す。本問は，在庫管理システムを対象とするシステム監査において，当該システムに記録された在庫データの「網羅性」のチェックポイントを問うている。

在庫は，入庫及び出庫という業務事象が発生する都度，更新される。

システムが記録している入庫データ，出庫データは，当該事象の発生履歴の情報である。これらのデータの網羅性は，入庫，出庫の受払い記録と突き合わせることで判断できる（なお，ここでいう入出庫には，棚卸や廃棄など在庫数を増減させる業務事象をすべて含むものとする）。

一方，システムが記録している在庫データは，現時点の情報である。通常，在庫データの変更履歴は保存しないので，在庫データの網羅性が確保されていることを，在庫データだけから判断することはできない。

そこで，在庫データの網羅性は，入庫データと出庫データを用いてチェックする必要がある。すなわち，入庫データと出庫データの網羅性をチェックし，かつ，入庫及び出庫の記録が過不足なく在庫に反映されていることをチェックすることで，在庫データの網羅性を

チェックすることができる。

選択肢エに記述された「入庫及び出庫記録に対して，自動的に連番を付与していること」は，入庫データと出庫データの網羅性を監査するのに役立つ。システム監査では，工数の制約上，すべての記録をしらみつぶしに調べることは難しい。そこで，網羅性の監査では，連番が付与されていることを確認した上で，システムが採番した数と受払いの記録数とを突き合わせる方法を採ることがある。

したがって，選択肢の中で，在庫データの網羅性のチェックポイントとして最も適切なものは，選択肢**エ**となる。よって，これが正解となる。

問 23：正解ウ

企業は業績を伸ばすために投資している。このとき，財務の視点だけで投資を決定するなら，当面の利益を確保するといった短期的な目標を設定して，経営資源を配分してしまいがちである。財務の視点は大切であるが，それだけでなく，顧客との関係強化，業務プロセスの改善，人材の育成など，成果が出るのに時間がかかるような分野にも目を向け，バランスよく投資すべきである。

そこで，投資が効果的であるかどうかを評価するために，バランススコアカードを活用できる。

バランススコアカードとは，経営戦略の適合性に基づいて業績を評価する手法である。経営戦略を設定した後，おおむね次に示す手順で業績評価指標を設定する。

1. 「財務」「顧客」「内部業務プロセス」「学習と成果」という 4 つの視点から，経営戦略の実現に影響を与える要因（CSF：Critical Success Factor）を導き出す。
2. 上記 1 で得られた要因を掘り下げて，個人や部門が実施する目標（KGI：Key Goal Indicator）と，その業績を評価する指標（KPI：Key Performance Indicator）を設定する。

このように，バランススコアカードは，経営戦略に結び付く評価指標を複数の視点から設定している。したがって，これを用いることで，投資の効果性を多面的に評価することができる。

よって，正解は選択肢**ウ**となる。

ア，エ：「正味現在価値などのキャッシュフロー」（選択肢ア），「金融市場で使われるオプション価格付け理論に基づく，収益やリスクの期待値」（選択肢エ）は，財務の

視点である。バランススコアカードでは，「財務」だけでなく，「顧客」「内部業務プロセス」「学習と成果」という複数の視点から評価する。

イ：IT ポートフォリオ分析手法を説明したものである。

問 24：正解エ

ア：BPR（Business Process Re-engineering）について記述したものである。

イ：ERP（Enterprise Resource Planning）について記述したものである。

ウ：SLA（Service Level Agreement）について記述したものである。

エ：**正解**。SOA（Service-Oriented Architecture）について適切に記述している。

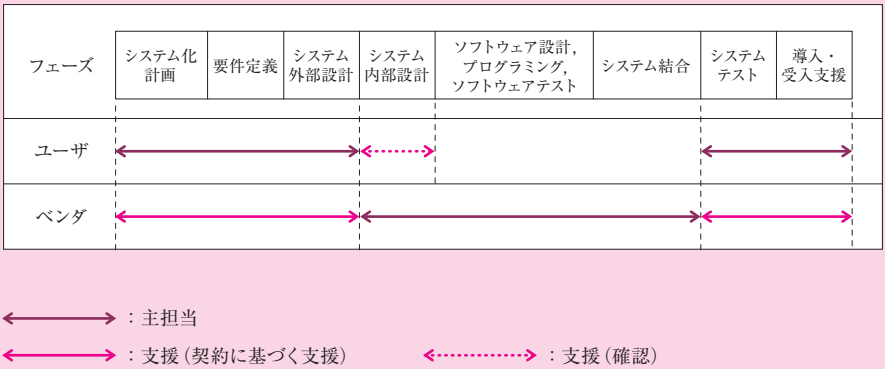
問 25：正解エ

「情報システム・モデル取引・契約書」とは，情報システムの信頼性向上と取引の可視化を目指して，取引と契約書のモデルを定めた文書である。経済産業省が，平成 19 年から 20 年にかけて公開した。

第 1 版（平成 19 年）は，対等な交渉力を有するユーザとベンダを契約当事者とし，ウォーターフォールモデルによる重要インフラ，企業基幹システム構築を前提条件とする取引と契約書について策定している。

追補版（平成 20 年）は，中小企業の取引の多数を占めるパッケージ，SaaS，ASP を対象とし，「重要事項説明書」を活用した取引モデルを前提条件とする取引と契約書について策定している。

本問は，「ユーザ（取得者）とベンダ（供給者）間」の請負型契約について問うている。第 1 版の「2. モデル契約プロセス」の「(4) ユーザとベンダの協力の重要性，役割分担」（42 ページ）では，フェーズごとのユーザとベンダの役割分担を次のように策定している。



注）「情報システム・モデル取引・契約書」の 42 ページの図「企画・要件定義段階，開発段階，運用段階の役割分担（全体像概略）」に基づき，著者が編集して作成。

図：ユーザとベンダの役割分担

これによれば，ベンダが主担当となるのは，システム内部設計からシステム結合までである。

この点を踏まえ，同文書の「(6) 請負と準委任」(44 ページ) は，「フェーズ毎に，契約類型として請負と準委任のどちらとするかを選択しなければならない」と定めており，その具体的な契約形態について次のように述べている。

> 請負ではベンダは仕事（受託業務）の完成の義務を負うのに対し，準委任ではベンダは善良な管理者の注意をもって委任事務を処理する義務を負うものの，仕事の完成についての義務は負わない。別の観点からいえば，請負に馴染むのは，業務に着手する前の段階でベンダにとって成果物の内容が具体的に特定できる場合ということになる。したがって，内部設計やソフトウェア設計などのフェーズは，請負で行うことが可能である。
>
> これに対して，システム化計画や要件定義のフェーズは，ユーザ側の業務要件が具体的に確定しておらず，ユーザ自身にとってもフェーズの開始時点では成果物が具体的に想定できないものであるから，ベンダにとっても成果物の内容を具体的に想定することは通常不可能である。そのため，請負には馴染みにくく，準委任が適切ということになる。

注）下線は著者による追加。

したがって，請負契約が適切であるとされているフェーズは，ベンダが主担当となるシステム内部設計からシステム結合までということになる。

よって，正解は選択肢**エ**となる。

問 26：正解エ

SCM（Supply Chain Management：サプライチェーンマネジメント）とは，購買，生産，販売に連なる「供給の連鎖」（サプライチェーン）を最適化することで，リードタイムの短縮，在庫コストや流通コストの削減などを目指す経営手法である。

よって，正解は選択肢**エ**となる。

ア：CRM（Customer Relationship Management）とは，企業内のあらゆる顧客チャネルの情報を管理し，顧客属性に基づく対応を行うことで，顧客満足度の向上と長期的な関係の構築を目指す取組みのことである。

イ：ERP（Enterprise Resource Planning）とは，企業の経営資源の有効活用による経営効率の向上を目指し，基幹業務を部門ごとではなく統合的に管理するための業務システムのことである。

ウ：MRP（Material Requirements Planning）とは，資材の手配を計画的に管理するため，製品の生産計画に基づいて製品の生産に必要な資材の正味所要量を展開し，資材の在庫数とリードタイムから適切な発注量と発注時期を算出する手法のことである。

問 27：正解イ

コア技術とは，企業の中核をなす技術のことである。例えば，競合他社がまねできないような独自技術は，コア技術であると言える。

選択肢**イ**に記述された「競合他社がまねできないような，自動車エンジンのアイドリングストップ技術」は，コア技術の事例と言える。よって，これが正解となる。

問 28：正解エ

コンカレントエンジニアリングとは，本来は順番に実行していた工程を，並行して実行することで，開発期間の短縮やコストの削減を目指す手法である。

これは，主に製造業で実施されている手法である。従来，製造業では，企画，設計，製造といった各工程を別々の部門が担当し，工程を順番に実行していた。

コンカレントエンジニアリングでは，部門間で情報を共有することで，前工程が完了する前から，自部門が担当する工程を開始する。このような取組みを通じて，開発工程全体で期間短縮を実現する。

よって，正解は選択肢**エ**となる。

問 29：正解エ

ア：アローダイアグラムは，複数の作業からなるプロジェクトについて，プロジェクトの開始から終了までの各作業の順序を表現した図である。

イ：パレート図とは，次に示す方法で作成した棒グラフと折れ線グラフを重ねた図である。

1. ある観点で分類された項目をグラフの横軸にする。その際，項目に含まれるデータ件数の多い順に左から並べる。
2. 上記 1 の項目を横軸とし，データ件数を縦軸とする棒グラフを作成する。
3. 上記 1 の項目を横軸とし，左の項目から順にデータ件数を累計した数を縦軸とする折れ線グラフを作成する。

ウ：マトリックス図とは，ある観点で分類された項目を縦軸に，それとは別の観点で分類された項目を横軸に置いて，縦軸の項目と横軸の項目が交わるセルに，両項目の関連性を記述した図である。

エ：**正解**。連関図の説明である。

問 30：正解ウ

不正競争防止法の第 2 条第 6 項は，営業秘密を次のとおり定義している。

① 秘密として管理されている［秘密管理性］
② 生産方法，販売方法その他の事業活動に有用な技術上又は営業上の情報である［有用性］
③ 公然と知られていないものである［非公知性］

この三つの要件全てを満たすことが法に基づく保護を受けるために必要となる。

問題本文には，「秘密として管理されていること」（秘密管理性），「事業活動に有用な技術

上又は営業上の情報であること」（有用性）が挙げられているので，残る要件は，選択肢ウの「公然と知られていないこと」（非公知性）である。

よって，正解は選択肢**ウ**となる。

●参考

企業の競争力の源泉となる営業秘密は，企業実態に即した実効的な管理が求められている。経済産業省は，企業実務において課題となってきた営業秘密の定義等（不正競争防止法による保護を受けるための要件）に関する考え方を文書化した「営業秘密管理指針」を公開している。平成 27 年 1 月に全面改訂されている。

同文書は法的拘束力をもつものではないが，イノベーションの推進，海外の動向や国内外の裁判例等を踏まえ，営業秘密の定義やその管理の在り方について具体的に説明している。