文部科学省後援

情報システム試験

平成30年度後期 情報検定

＜実施　平成31年2月10日（日）＞

システムデザインスキル

（説明時間　14：30～14：40）

（試験時間　14：40～16：10）

・試験問題は試験開始の合図があるまで開かないでください。

・解答用紙（マークシート）への必要事項の記入は，試験開始の合図と同時に行いますので，それまで伏せておいてください。

・試験開始の合図の後，次のページを開いてください。**＜受験上の注意＞**が記載されています。必ず目を通してから解答を始めてください。

・試験問題は，すべてマークシート方式です。正解と思われるものを１つ選び，解答欄の０をＨＢの黒鉛筆でぬりつぶしてください。２つ以上ぬりつぶすと，不正解になります。

・辞書，参考書類の使用および筆記用具の貸し借りは一切禁止です。

・電卓の使用が認められます。ただし，下記の機種については使用が認められません。

＜使用を認めない電卓＞

１．電池式（太陽電池を含む）以外の電卓

２．文字表示領域が複数行ある電卓（計算状態表示の一行は含まない）

３．プログラムを組み込む機能がある電卓

４．電卓が主たる機能ではないもの

＊パソコン（電子メール専用機等を含む），携帯電話（ＰＨＳ），スマートフォン，タブレット，電子手帳，電子メモ，電子辞書，翻訳機能付き電卓，音声応答のある電卓，電卓付き腕時計，時計型ウェアラブル端末等

５．その他試験監督者が不適切と認めるもの

一般財団法人　職業教育・キャリア教育財団

＜受験上の注意＞

１．この試験問題は19ページあります。ページ数を確認してください。
乱丁等がある場合は，手をあげて試験監督者に合図してください。
※問題を読みやすくするために空白ページを設けている場合があります。

２．解答用紙（マークシート）に，受験者氏名・受験番号を記入し，受験番号下欄の数字をぬりつぶしてください。正しく記入されていない場合は，採点されませんので十分注意してください。

３．試験問題についての質問には，一切答えられません。自分で判断して解答してください。

４．試験中の筆記用具の貸し借りは一切禁止します。筆記用具が破損等により使用不能となった場合は，手をあげて試験監督者に合図してください。

５．試験を開始してから30分以内は途中退出できません。30分経過後退出する場合は，もう一度，受験番号・マーク・氏名が記載されているか確認して退出してください。なお，試験終了５分前の合図以降は退出できません。試験問題は各自お持ち帰りください。

６．試験後にお知らせする合否結果（合否通知），および合格者に交付する「合格証・認定証」はすべて，Ｗｅｂページ（ＰＣ，モバイル）での認証によるディジタル「合否通知」，ディジタル「合格証・認定証」に移行しました。
①団体宛にはこれまでと同様に合否結果一覧ほか，試験結果資料一式を送付します。
②合否等の結果についての電話・手紙等でのお問い合わせには，一切応じられませんので，ご了承ください。

問題を読みやすくするために,
このページは空白にしてあります。

問題１　次の経営分析に関する各設問に答えよ。

＜設問１＞　次の PPM に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

PPM(Product Portfolio Management)は，自社の製品や事業の市場競争力を客観的に評価，分析するための手法である。PPM では，市場占有率と市場成長率をもとに「問題児」，「花形」，「負け犬」，「金のなる木」の４つに分類し，経営戦略を検討する。

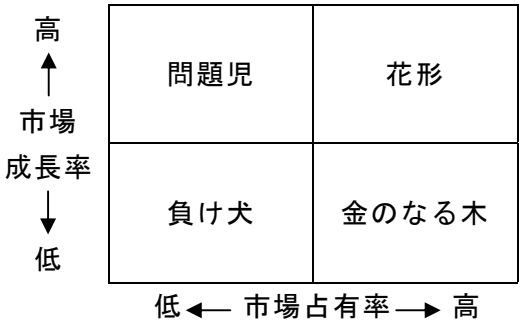

図１　PPM

①　問題児

成長市場であるのに市場占有率が低い。大きな投資を行うことにより市場占有率を高くできれば，［　(1)　］になる可能性がある。

②　花形

成長市場であるため高い利益が期待できるが，市場占有率を維持するための［　(2)　］が必要となる。

③　負け犬

市場成長率，市場占有率ともに低いので，資金を生み出す効果がないため，［　(3)　］を考える必要がある。

④　金のなる木

市場成長率は低くとも高いシェアを持つため［　(4)　］が少なく，［　(5)　］として位置づけられる。

(1) の解答群

ア．金のなる木　　イ．花形　　ウ．負け犬

(2)，(3) の解答群

ア．新規参入　　イ．多角化経営　　ウ．撤退　　エ．投資

(4) の解答群

ア．競合　　イ．顧客数　　ウ．市場の関心　　エ．資本金

(5) の解答群

ア．クレーム数減少の対策　　イ．コスト増加の要因

ウ．投資用の資金源　　エ．不良在庫の原因

＜設問２＞　次の国内で生産活動をしている子ども向けの食品メーカの事例(6)～(8)をSWOT分析したときのカテゴリを解答群から選べ。

SWOT 分析は，内部環境における強み(Strengths)と弱み(Weaknesses)，外部環境における機会(Opportunities)と脅威(Threats)の４つのカテゴリで分析する手法である。

	良い要因	悪い要因
内部環境	強み	弱み
外部環境	機会	脅威

図２　SWOT 分析

［食品メーカの事例］

(6) 原料の生産から流通・販売までを自社で行っているので柔軟な対応が可能。

(7) 消費者の国内生産品に対する志向が高まっている。

(8) 少子化の影響で子ども向け商品の販売数が減少傾向にある。

(6) ～ (8) の解答群

ア．機会　　イ．脅威　　ウ．強み　　エ．弱み

＜設問３＞　次のバランススコアカードに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

バランススコアカードは，財務の視点，顧客の視点，業績プロセスの視点，学習と成長の視点の４つの視点から業績を評価する考え方である。

① 財務の視点
株主や従業員など，ステークホルダの期待に応えるために財務的目標を設定する。
② 顧客の視点
企業のビジョンを達成するために，顧客に対して行動すべき指標を設定する。
③ 業務プロセスの視点
財務の視点や顧客の視点を達成するために，必要な業務プロセスを構築するための指標を設定する。
④ 学習と成長の視点
企業のビジョン達成するために，組織や個人としての能力向上を図るための指標を設定する。

例えば，自社製品をアピールするために行うキャンペーンは［　(9)　］の視点，社員の IT スキルを向上させるために研修会への参加を義務付けることは［　(10)　］の視点である。

(9)，(10) の解答群

ア．学習と成長　　イ．業務プロセス　　ウ．顧客　　エ．財務

問題２　次のオブジェクト指向設計に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

オブジェクト指向設計では，システム全体をいくつかのクラスで構成する。クラスとは，そのシステムに必要な″実態″のことで，属性(プロパティ)と操作(［(1)］)で構成される。属性と操作を一体化し，隠ぺいすることを［(2)］と呼ぶ。

実際に処理する場合は，定義されているクラスをひな形にしたオブジェクトを生成して利用する。この生成したオブジェクトを［(3)］と呼ぶ。オブジェクトの構造を知らなくても必要な操作ができるようにすることで，オブジェクトの独立性を高めることができる。このオブジェクトに対して処理を指示できる唯一の手段が［(4)］である。なお，異なるオブジェクトに同一の［(4)］を送った場合でも，それぞれのオブジェクトで特有の処理を行う事ができる。これを［(5)］と呼ぶ。

下図のようなクラス構造の場合，車クラスは，″バス″，″トラック″，″乗用車″の共通部分からなる［(6)］となる。車クラスで定義されている共通の属性や操作は，［(7)］に引き継ぐことができる。これを［(8)］と呼び，それぞれのクラスについて個別に定義しなければならない部分のみ定義し，共通部分は上位クラスから引き継ぐことにより，生産性を向上させている。

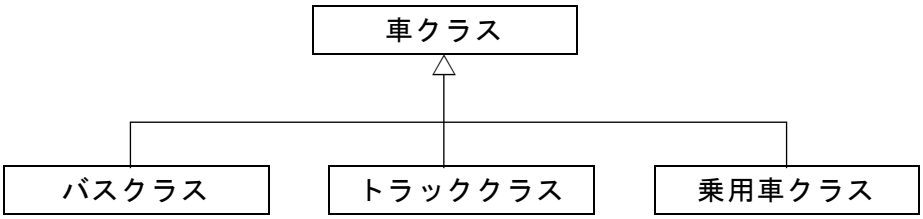

図　クラスの階層構造

なお，上図のクラスの関係は，［(9)］となる。

(1) ～ (5) の解答群

ア．インスタンス　　イ．カプセル化　　ウ．クラスタ
エ．スレッド　　オ．ポリモフィズム　　カ．メソッド
キ．メッセージ　　ク．ロール

(6) ～ (8) の解答群

ア．インヘリタンス　　イ．オーバライド　　ウ．サブクラス
エ．スーパークラス　　オ．デリゲーション　　カ．ベーシッククラス

(9) の解答群

ア．依存　　イ．集約／分解　　ウ．特化／汎化

問題３　次のネットワークに関する各設問に答えよ。

＜設問１＞　次の LAN 内のデータ通信に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

データ通信を実現するために，コンピュータが持つべき通信機能を 7 階層に分割し，国際標準化機構(ISO)が制定したプロトコル体系が OSI 基本参照モデルである。これに対して，インターネットで利用される TCP/IP 階層モデルでは，4 階層に分割して体系化している(図１)。

OSI 基本参照モデル		TCP/IP 階層モデル
アプリケーション層		アプリケーション層
プレゼンテーション層		
セション層		
トランスポート層		トランスポート層
ネットワーク層		インターネット層
データリンク層		ネットワーク
物理層		インタフェース層

図１　OSI 基本参照モデルと TCP/IP 階層モデル

両モデルとも，データ送信時は上位層から下位層の順序で処理が施され，各層ごとにヘッダが付けられる(図２)。

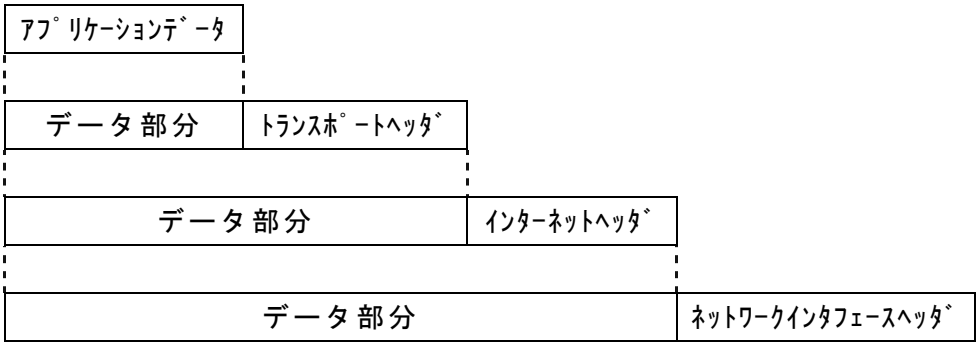

図２　TCP/IP 階層モデルの送信データの構造

社内 LAN に TCP/IP プロトコルを利用したイントラネットでは,ホスト間の通信において宛先や送信元として IP アドレスが利用される。IP アドレスは，インターネットヘッダに格納されるが，さらに下位層では［　(1)　］にカプセル化される。ネットワークインタフェース層の規格であるイーサネットを利用する場合，最下位層のヘッダでは,MAC アドレスが送信先や送信元のアドレスとして利用される。MAC アドレスは,NIC の ROM に格納されている 48 ビットのアドレスのことであり,8 ビットごとに 2 桁の 16 進数(00～FF)で表記し，それぞれの間をコロンで区切り，04:A2:8C:73:E5:BA のよう

に表す。

通常の利用において，IP アドレスを明示的に指定することはあるが，MAC アドレスを指定することはない。しかし，最下位層のイーサネットで使用する送信先や送信元のアドレスが MAC アドレスであることから，IP アドレスを基に MAC アドレスを得る必要があり，ARP(Address Resolution Protocol：アドレス解決プロトコル)が用いられる。

ARP の機能は，問合せとして「ARP 要求」を送信し，それに対する回答として「ARP 応答」を受け取ることで実現する。「ARP 要求」は，送信元の IP アドレスと MAC アドレス，MAC アドレスを得たいホストの IP アドレスを設定して［　(2)　］で送信する。「ARP 要求」を受け取った各ノードは，アドレス解決 IP アドレスが自身の IP アドレスと一致する場合に，自身の MAC アドレスを設定した「ARP 応答」を送信元に対して［　(3)　］で送信する。「ARP 応答」を受け取ったホストは，MAC アドレスをキャッシングして以降の送信に利用する。

(1) ～ (3) の解答群

ア．インターネットヘッダ　　イ．データ部分
ウ．トランスポートヘッダ　　エ．ネットワークインタフェースヘッダ
オ．ブロードキャスト　　カ．ユニキャスト

＜設問２＞　次の LAN 内のデータ通信に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

社内 LAN の一部を表した図３において，ホストＡは LAN 内のホストや LAN 間接続装置の全ての MAC アドレスをキャッシュしていないとする。この状態で，ホストＡがホストＣにデータを送信しようとするとき，ホストＡは［　(4)　］の IP アドレスに対する「ARP 要求」を送信する。また，ホストＡがホストＥにデータを送信しようとするとき，ホストＡは［　(5)　］の IP アドレスに対する「ARP 要求」を送信する。これで得た MAC アドレスをデータに付加し，送信する。

なお，図３では CIDR で表記しており，末尾の[/24]がネットワークアドレスのビット数である。

(4)，(5) の解答群

ア．ブリッジＺ　　イ．ホストＡ　　ウ．ホストＣ
エ．ホストＥ　　オ．ルータＸ　　カ．ルータＹ

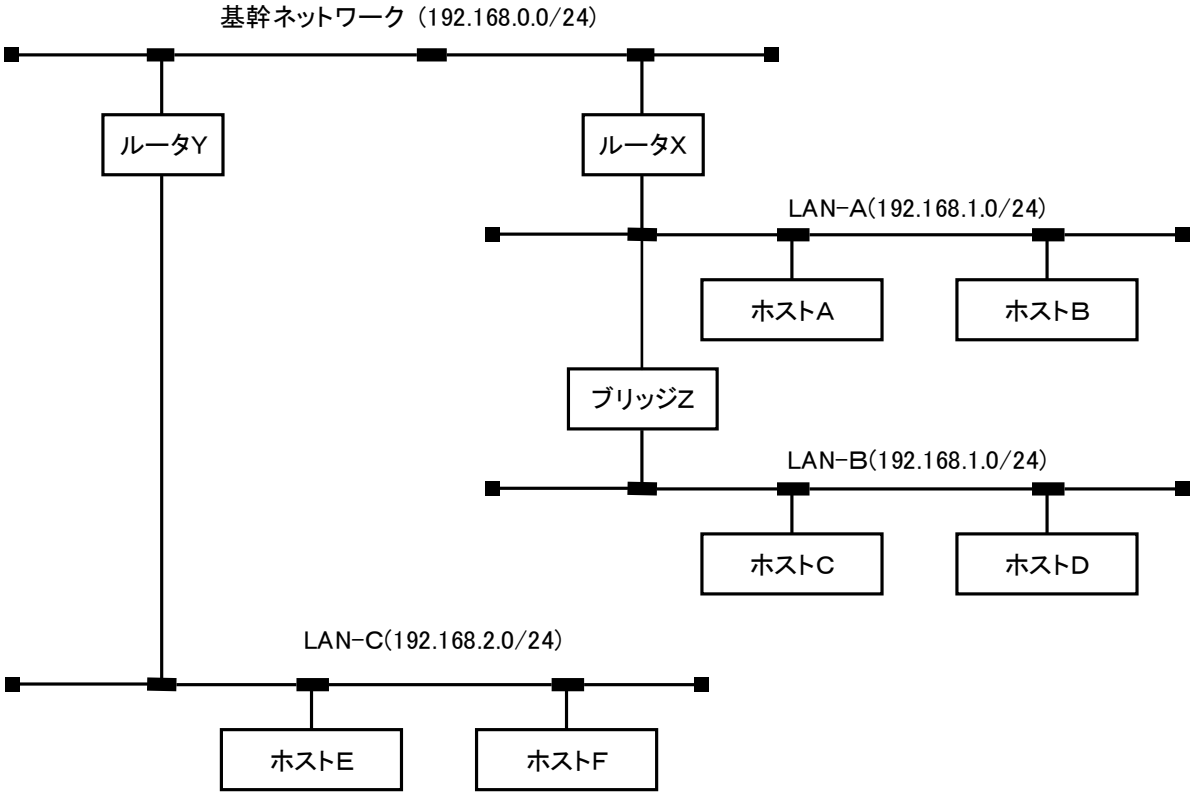

図３　社内 LAN の一部

＜設問３＞　次のサブネット化に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

クラス方式のホストアドレス部の一部をネットワークアドレスとして利用し，複数のサブネットワークを構築することをサブネット化という。このとき，サブネットマスクは，標準のネットワークアドレス部にサブネットワーク部を含んでネットワークアドレスとして指定する。

例えば，クラスＣの IP アドレスに対して，標準のサブネットマスク「［(6)］」を指定した場合，一つのサブネットワーク内には［(7)］個のホストアドレスを設定できる。また，ホストアドレスのうち３ビットをネットワークアドレスとして利用し，サブネットマスク「255.255.255.224」を指定した場合，一つのサブネットワーク内には［(8)］個のホストアドレスを設定できる。

ただし，各サブネットワーク内において，すべてのビットが「0」とすべてのビットが「1」のホストアドレスは設定できないものとする。

(6) の解答群

ア．255.255.0.0　　イ．255.255.240.0

ウ．255.255.255.0　　エ．255.255.255.240

(7) の解答群

ア．2^6　　イ．2^7-2　　ウ．2^8-2　　エ．2^8

(8) の解答群

ア．30　　イ．32　　ウ．62　　エ．64

＜設問４＞　次の図４の LAN 構成において，一般的に適切とされるサーバの設置場所を表した組合せを解答群から選べ。

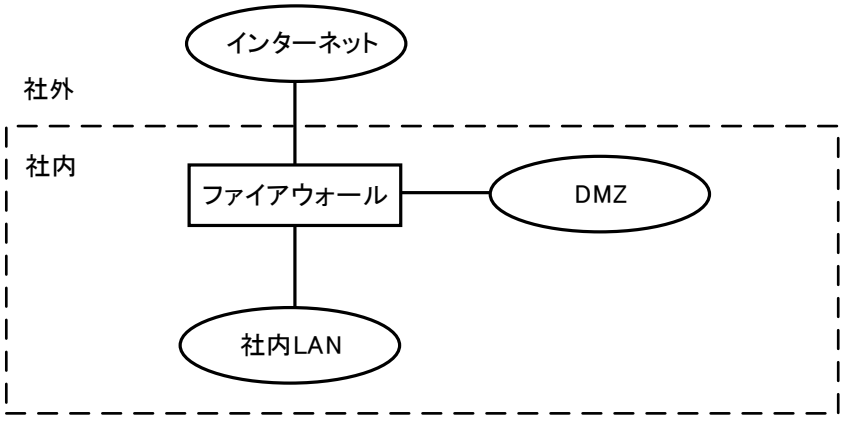

図４　LAN の構成例

(9) の解答群

	公開 Web サーバ	データベースサーバ	プロキシサーバ
ア.	DMZ	社内 LAN	社内 LAN
イ.	DMZ	DMZ	社内 LAN
ウ.	DMZ	社内 LAN	DMZ
エ.	社内 LAN	社内 LAN	社内 LAN

問題を読みやすくするために,
このページは空白にしてあります。

問題４　次のデータベースに関する記述を読み，各設問に答えよ。

Ｊ家具店は東京都内に本社と５カ所の店舗，３カ所の倉庫を持っており，200 種類の商品を取り扱っている。商品は各倉庫で保管されているが，必ずしもすべての商品を保管しているとは限らない。各店舗では１日平均 30 商品の在庫引当要求が発生するため，図１のような在庫引当票を作成し，毎日１回午後５時までに本社へ送付する。商品は翌日の午前９時までに各倉庫から各店舗に配送される。各商品の需要数は毎日ばらつきがあり在庫不足による販売機会の損失は各店舗の営業利益に影響する。なお，本社は引当処理などの事務作業のみで，販売は行わない。

・伝票番号は全社で一連の番号が付与される。
・店舗コードは全社で一意の値が付与されている。
・商品コードは全社で一意の値が付与されている。

在 庫 引 当 票

伝票番号　12345　　日付　20XX/XX/XX

店舗コード　1003
店舗名　中野店
電話番号　123-4567-8901
住所　東京都 XXXXX

商品コード	商品名	単価	数量	金額
ST03	学習机	92,000	2	184,000
HS05	ソファー	72,000	5	360,000
:	:	:	:	:
			合計額	904,000

図１　在庫引当票の例

＜設問１＞　データベースの正規化に関する次の記述中の［　　］に入れるべき適切な字句を解答群から選べ。

図１の在庫引当票をレコード形式にすると図２のようになる。これは非正規形と呼ばれ，在庫引当票をそのまま表現したものである。図２の下線が引いてある項目は主キーであり，一意の伝票番号によって在庫引当票の各項目を一意に特定できる。

図２　非正規形

次に，図２の非正規形を正規化する。なお，主キーの表示は省略している。

［第１正規化］

図２を第１正規化したものが図３になる。

第１正規化では，非正規形のデータから繰返し部分を排除する。また，導出項目を排除する。主キーは［　(1)　］の複合キーとなる。

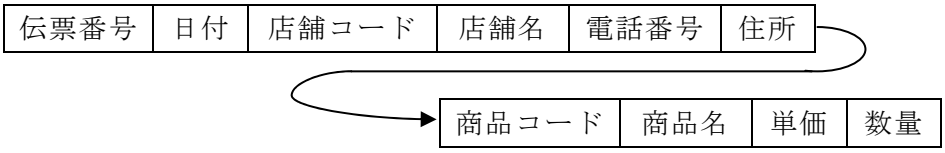

図３　第１正規形

第１正規化を行うことによって，レコード数は増加する。非正規形のレコード件数は全社で 1 日［　(2)　］件であるが，第１正規化を行うことによってレコード数は平均［　(3)　］件に増加すると予測される。

(1) の解答群

ア．伝票番号，店舗コード　　イ．伝票番号，電話番号
ウ．伝票番号，商品コード　　エ．伝票番号，数量

(2)，(3) の解答群

ア．3　　イ．5　　ウ．90　　エ．150
オ．200　　カ．450　　キ．600　　ク．1000

［第２正規化］

第２正規化では主キーが複合キーである場合，［　(4)　］を分離する。図３の第１正規形を第２正規化したものが図４である。

［引当］

伝票番号	日付	店舗コード	店舗名	電話番号	住所

［商品］

商品コード	商品名	単価

［引当明細］

伝票番号	商品コード	数量

図４　第２正規形

［第３正規化］

第３正規化では，［(5)］を分離する。図４の第２正規形を第３正規化したものが図５になる。

［引当］

伝票番号	日付	店舗コード

［店舗］

店舗コード	店舗名	電話番号	住所

［商品］

商品コード	商品名	単価

［引当明細］

伝票番号	商品コード	数量

図５　第３正規形

(4)，(5)の解答群

ア．キー項目以外の項目に関数従属する項目
イ．キー項目に従属する項目と導出データ
ウ．主キーと主キー以外の項目
エ．主キーに部分関数従属している項目

＜設問２＞　次の引当可能倉庫表を求める SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。

引当処理に必要な在庫表，距離表，倉庫表を次に示す。なお，引当処理は店舗と倉庫との距離やトラックの配車状況等も考慮され,在庫引当票が到着した順に行われる。

［在庫］

商品コード	倉庫番号	在庫数

［距離］

店舗コード	倉庫番号	距離数

［倉庫］

倉庫番号	倉庫名

各店舗から送られてくる当日の在庫引当票から，本社では店舗と商品ごとに翌日の商品配送が可能である倉庫を求める。引当可能倉庫とは，引当数量に在庫数が足りている倉庫とする。なお，引当可能倉庫表は，商品コードの昇順，距離の昇順に表示され，当日はホスト変数“:当日”に，引当店舗はホスト変数“:店舗コード”に格納されているものとする。

```
SELECT 引当.店舗コード, 引当明細.商品コード, 引当明細.数量, 在庫.在庫数,
       在庫.倉庫番号, 距離.距離数
  FROM 引当, 引当明細, 在庫, 距離
  WHERE [ (6) ]
    AND 引当.店舗コード = :店舗コード
    AND 引当.日付 = :当日
    AND 在庫.在庫数 >= 引当明細.数量
  ORDER BY 引当明細.商品コード, 距離.距離数
```

(6) の解答群

ア．引当.伝票番号 = 引当明細.伝票番号
　　AND 引当明細.商品コード = 在庫.商品コード

イ．引当.伝票番号 = 引当明細.伝票番号
　　AND 在庫.倉庫番号 = 距離.倉庫番号

ウ．引当.伝票番号 = 引当明細.伝票番号
　　AND 引当.店舗コード = 距離.店舗コード

エ．引当.伝票番号 = 引当明細.伝票番号
　　AND 引当.店舗コード = 距離.店舗コード
　　AND 引当明細.商品コード = 在庫.商品コード
　　AND 在庫.倉庫番号 = 距離.倉庫番号

＜設問３＞　次の商品引当一覧作成に関する記述を読み，SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。

引当状況を分析するため，指定された期間の商品別の引当一覧を作成する。引当一覧は，指定月の引当合計金額の多い順に表示する。ただし，引当合計金額が同じ場合は，合計数量の降順に表示する。なお，指定月の開始日と終了日はホスト変数“:指定月開始日”と“:指定月終了日”に格納されているものとする。

［指定された期間の商品引当一覧］

```
SELECT 商品.商品コード, 商品.商品名,
       SUM( (7) ) AS 引当合計金額, SUM(引当明細.数量) AS 合計数量
  FROM 商品, 引当, 引当明細
  WHERE 引当.伝票番号 = 引当明細.伝票番号
    AND 商品.商品コード = 引当明細.商品コード
    AND 日付 (8) :指定月開始日 (9) :指定月終了日
  (10) 商品.商品コード, 商品.商品名
  ORDER BY 引当合計金額 DESC, 合計数量 DESC
```

(7) の解答群

ア．在庫.在庫数 + 商品.単価　　イ．在庫.在庫数 * 商品.単価
ウ．引当明細.数量 + 商品.単価　　エ．引当明細.数量 * 商品.単価

(8) ～ (10) の解答群

ア．AND　　イ．BETWEEN
ウ．DISTINCT　　エ．EXISTS
オ．GROUP BY　　カ．HAVING
キ．IN　　ク．LIKE

問題５　次の情報セキュリティに関する各設問に答えよ。

＜設問１＞ 次の暗号化技術に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

データ通信では，伝送中にデータが盗聴される可能性がある。そこで，データの漏えいを防ぐためデータを暗号化し，盗聴されても復号できないようにする。暗号化技術には，大きく分けて二つの種類がある。

［共通鍵暗号方式］

暗号化と復号に同じ鍵を利用する方式で，送信側は送信しようとするデータ(平文)に共通鍵を用いて,暗号文を作成して送信し,受信側は受信した暗号文を同じ鍵を使って平文に戻す。

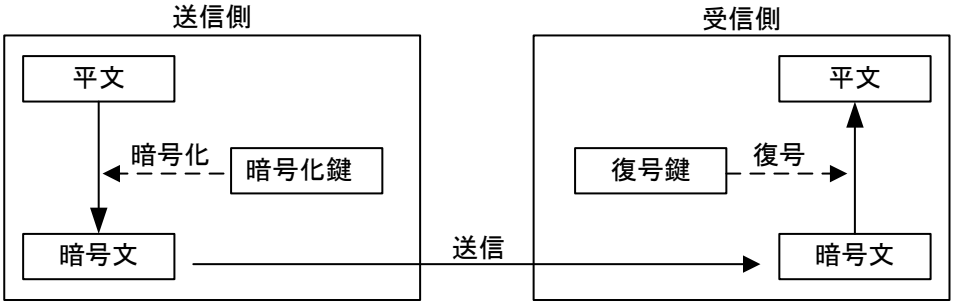

図１　共通鍵暗号方式を利用した送信

［公開鍵暗号方式］

対応する二つの鍵を作成し，一方の鍵で暗号化すると他方の鍵で復号できる方式である。一方の鍵を秘密鍵として自分で厳重に保管し，他方の鍵を公開鍵として公開する。一般的な公開鍵暗号方式では，送信側は［　(1)　］を使って暗号文を作り送信し，受信側は［　(2)　］で復号する。

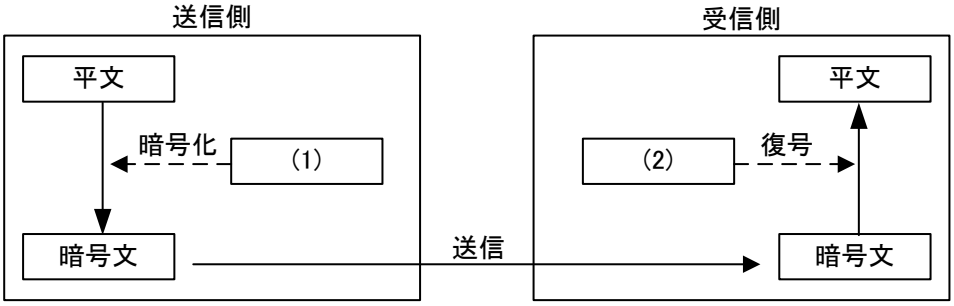

図２　公開鍵暗号方式を利用した送信

(1)，(2) の解答群

ア．受信者の公開鍵　　イ．受信者の秘密鍵

ウ．送信者の公開鍵　　エ．送信者の秘密鍵

＜設問２＞ 次のハイブリッド暗号方式に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ハイブリッド暗号方式は，共通鍵暗号方式と公開鍵暗号方式を組み合わせた暗号方式である。その仕組みを次に示す。

［ハイブリッド暗号方式の仕組み］

① 共通鍵を生成する。

② 共通鍵を受信者の公開鍵で暗号化する。

③ 暗号化された鍵を送信する。

④ 暗号化された鍵を［ (3) ］で復号する。

以降の通信を次のように行う。

⑤ 平文を［ (4) ］で暗号化する。

⑥ 暗号文を送信する。

⑦ 暗号文を［ (4) ］で復号する。

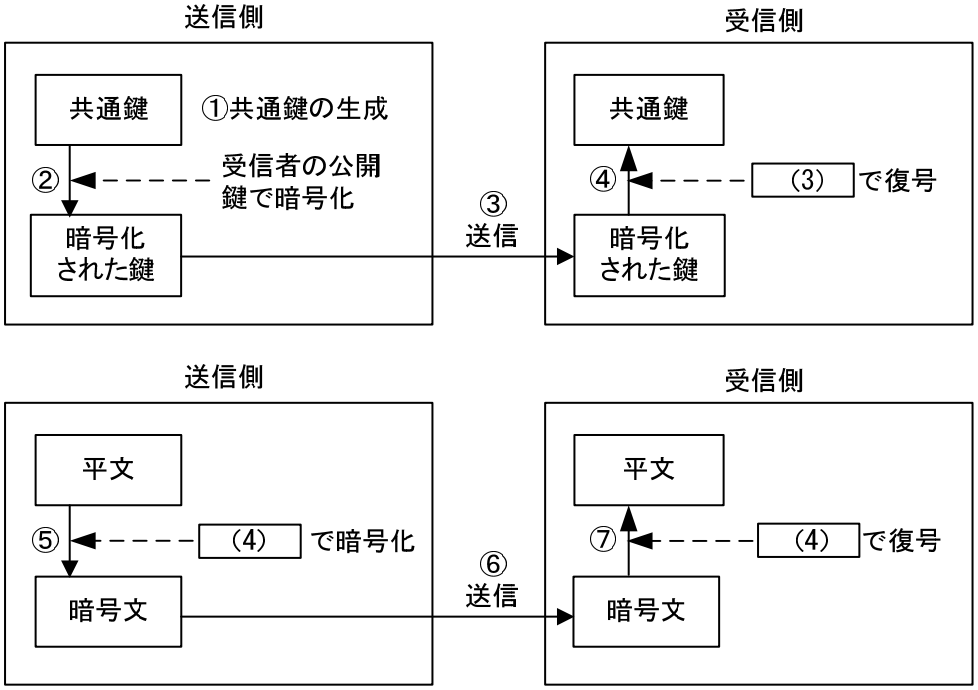

図３　ハイブリッド暗号方式の仕組み

(3) ～ (4) の解答群

ア．共通鍵　　イ．受信者の公開鍵
ウ．受信者の秘密鍵　　エ．送信者の公開鍵
オ．送信者の秘密鍵

＜設問３＞　次のなりすまし防止に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

なりすまし防止には，紙に記されるサインや押印と同じような役割を電子データで表し，送信データに付加する仕組みがある。これには，公開鍵暗号方式を利用した［(5)］があり，［(5)］にメッセージダイジェストを利用することで，送信者の正当性だけでなくデータの改ざんの有無も検知できる。

その手順を次に示す。

A 送信者は，平文のメッセージからハッシュ関数を利用してメッセージダイジェストを作成する。

B メッセージダイジェストを［(6)］で暗号化したものを［(5)］として利用し，平文のメッセージに付加して送信する。

C 受信者は受信した平文のメッセージから，Aと同じハッシュ関数を利用してメッセージダイジェストを生成する。

D 受信した［(5)］を［(7)］で復号して得たメッセージダイジェストと，Cで生成したメッセージダイジェストを比較する。比較結果が一致していれば受信したデータは改ざんされていないことと送信者の正当性を確認できる。

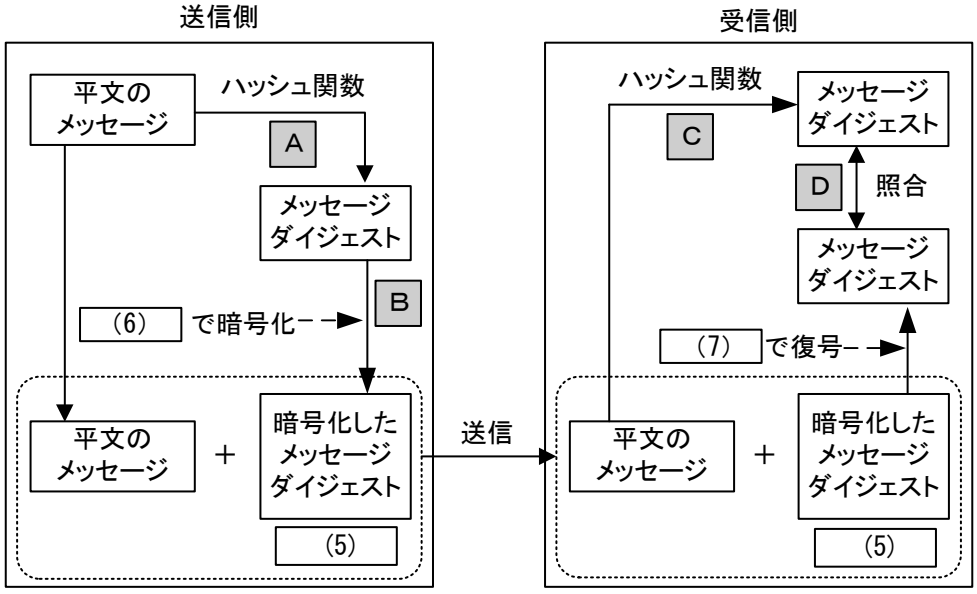

図４　なりすまし防止の仕組み

(5) の解答群

ア．サーバ証明書　　イ．ディジタル証明書
ウ．ディジタル署名　　エ．ルート証明書

(6)，(7) の解答群

ア．受信者の公開鍵　　イ．受信者の秘密鍵
ウ．送信者の公開鍵　　エ．送信者の秘密鍵

＜メモ欄＞

＜メモ欄＞