文部科学省後援

情報システム試験

平成26年度後期 情報検定

＜実施　平成27年2月8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，解答欄の〇を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，電卓付腕時計等

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16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）での認証によるデジタル「合否通知」，デジタル「合格証・認定証」で行います。
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　次の在庫管理に関する記述を読み，各設問に答えよ。

在庫管理とは,企業が保管する製品の在庫量を適切にコントロールすることである。在庫量が少なすぎると品切れが発生するが，在庫費用は少なくて済む。また，在庫量が多すぎると品切れは発生しないが，在庫費用が多くなってしまう。したがって，この相反する在庫量を適切にコントロールすることが必要である。

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

在庫管理にかかる費用は［　(1)　］と［　(2)　］である。

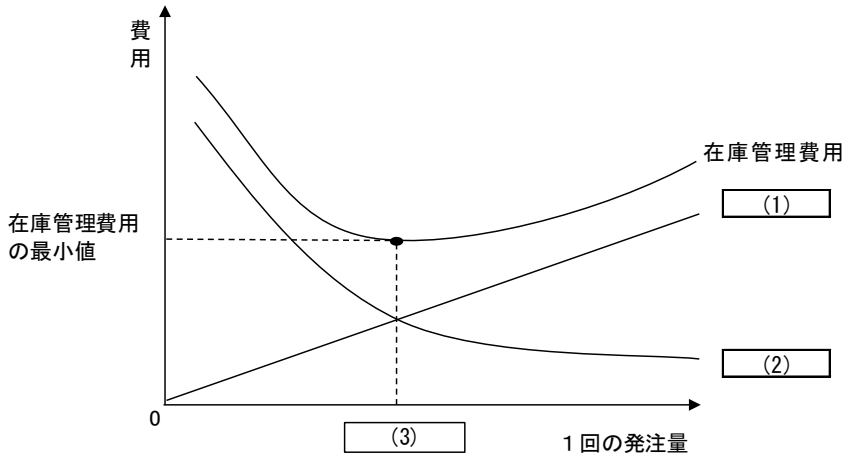

図　発注量と在庫管理費用の関係

［　(1)　］とは製品を保管するためにかかる費用であり，倉庫代や保管するための電気料金などが該当する。在庫量が多くなればなるほど増加する。

［　(2)　］とは発注するたびにかかる費用であり，発注のための通信費や配達費などが該当する。１回の発注量を少なくすると発注回数が多くなる。発注回数が多くなればなるほど［　(2)　］が増加することになる。

この二つの費用の和は在庫管理費用と呼ばれ，この和が最も小さくなる発注量を［　(3)　］とよび，次の式で表される。

$$\sqrt{\frac{2 \times \text{年間総需要量} \times \text{１回の発注費}}{\text{１個の年間保管費}}}$$

例えば，インクジェットプリンタのインクの販売量が15,000個/年であり，年間保管費が600円/個，１回の発注費1,250円の場合，発注１回当たりの［　(3)　］は［　(4)　］個となる。

(1) ～ (3) の解答群

ア．経済的発注量　　イ．在庫調整費
ウ．年間販売量　　エ．発注費用
オ．販売費用　　カ．保管費用

(4) の解答群

ア．10　　イ．100　　ウ．120　　エ．250

＜設問２＞　次の発注方法に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

在庫管理における発注方法には，［ (5) ］，［ (6) ］などがある。

［ (5) ］は，製品や商品を発注する時期をあらかじめ決めておくもので，次に発注するまでに品切れを起こさないように，需要を予測して発注量を決定する。

［ (6) ］は，在庫量があらかじめ決められた量（発注点）を下回ったら，一定量を発注する方法であり，発注時期は不定である。発注点は次の式で求められる。

発注点＝１日当たりの平均販売量×調達期間＋［ (7) ］

発注してから納品されるまでの期間を調達期間と呼ぶが，この調達期間が予定より長くなったり，調達期間に需要が急に増えて品切れが起こったりすることもある。このような品切れを起こさないレベルの在庫を［ (7) ］と呼ぶ。

ここで，インクジェットプリンタのインクの発注の場合，発注点は［ (8) ］となる。なお，1 日当たりの平均販売量は 42 個とし，調達期間は３日，［ (7) ］は 150 個とする。

(5) ～ (7) の解答群

ア．２ビン法　　イ．安全在庫
ウ．過剰在庫　　エ．個別法
オ．定期発注法　　カ．定量発注法

(8) の解答群

ア．150　　イ．225　　ウ．250　　エ．276

問題２　次のシステム開発に関する各設問に答えよ。

＜設問１＞　次のソフトウェア開発に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ソフトウェア開発のモデルには，［　(1)　］モデル，［　(2)　］モデル，［　(3)　］モデルなどがある。

［　(1)　］モデルは，図(A)のモデルであり，川の水が滝を流れ落ちるように，上流工程から下流工程に向けて順に開発作業を進めていく。各工程では，作業が終了しないと次の工程には進めず，作業の結果は必ずドキュメントとして残さなければならない。また，ユーザの要望は，主に最初の工程であるシステム分析でまとめられる。

［　(2)　］モデルは，図(B)のモデルであり，早い段階で試作品を作成し，ユーザの意見や要望を取り入れながら開発を進める。

［　(3)　］モデルは，図(C)のモデルであり，システム全体を一斉に開発するのではなく，独立性の高い複数の機能に分割して，中心となる機能から順に開発を進めていく。機能単位での開発を繰り返しながら，徐々にシステムを大きくしていくため，同時に開発する規模が小さいので，開発要員の確保などが容易になる。

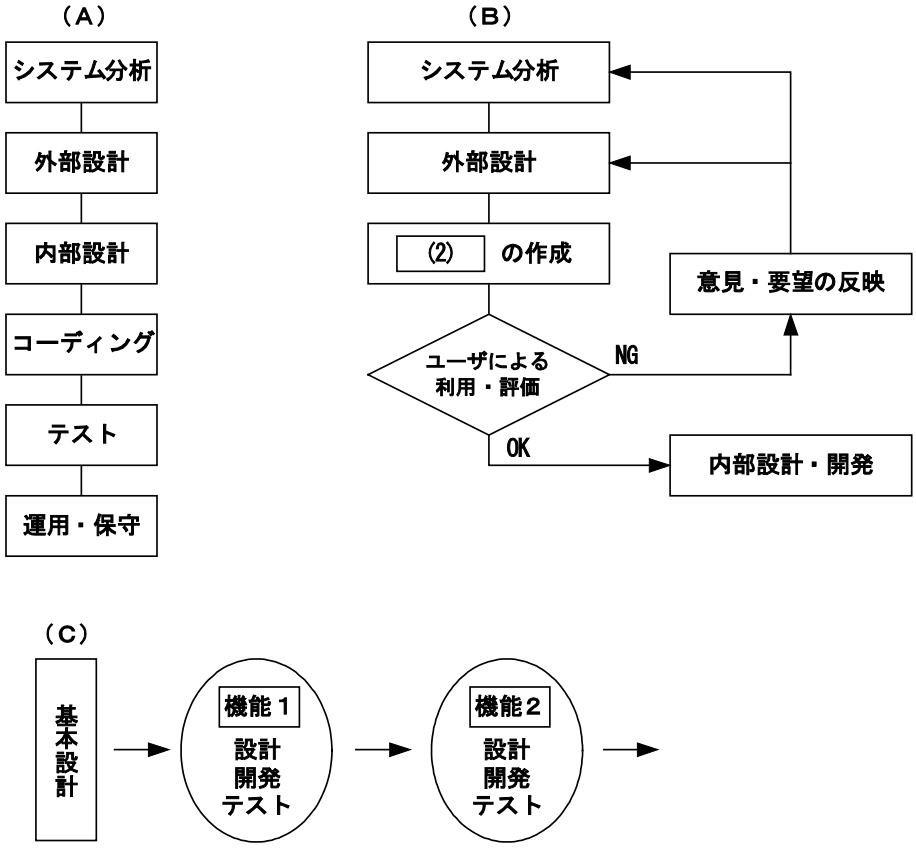

図　主なソフトウェア開発モデル

(1) ～ (3) の解答群

ア．インクリメンタル　　イ．ウォータフォール　　ウ．オブジェクト
エ．コンテキスト　　オ．データフロー　　カ．プロトタイプ

＜設問２＞　次のドキュメントは，図(A)のどの工程で作成されるものか。関係の深い工程名を解答群から選べ。なお，解答は重複して選んでもよい。

(4) 単体テスト仕様書
(5) 画面設計書(概要レベル)
(6) プログラム設計書
(7) 帳票設計書(概要レベル)
(8) 要求定義書

(4) ～ (8) の解答群

ア．システム分析　　イ．外部設計　　ウ．内部設計
エ．コーディング　　オ．テスト　　カ．保守・運用

問題３　次のネットワークに関する記述を読み，各設問に答えよ。

＜設問１＞　次のインターネットプロトコルに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

インターネットプロトコル体系は，表に示すように四つの階層に分けて定義されている。

表　インターネットプロトコル体系

第４層	アプリケーション層
第３層	トランスポート層
第２層	インターネット層
第１層	リンク層

ここで，トランスポート層の代表的なプロトコルとして［(1)］や［(2)］がある。［(1)］は，指定されたアプリケーションに，確実にデータを届けることを目的としている。そのために受信確認や再送処理を行うので，信頼性は高いが伝送効率は低い。これに対して［(2)］は，ライブ中継など，信頼性が低くても効率よくデータ転送を行いたいときに利用される。

また，インターネット層の代表的なプロトコルとして［(3)］がある。［(3)］は，発信者端末から受信者端末まで，ルータなどの中継機器と連携しながらデータを送り届けることを目的としている。これをルーティングと呼ぶ。

(1) ～ (3) の解答群

ア．DNS　　イ．FTP　　ウ．IP　　エ．SMTP　　オ．TCP　　カ．UDP

＜設問２＞　次のルーティングに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ルータは，複数のネットワークを相互に接続する装置である。一つのネットワーク内の通信機器は同じネットワークアドレスを持つ。

また，ルータは異なるネットワークへの通信経路の選択をルータ内のルーティングテーブルに基づいて行っている。ルーティングテーブルは，送信先ネットワークアドレス(パケットの宛先ネットワークアドレス),そのパケットの転送先ルータの IP アドレス,宛先ネットワークアドレスに到達するまでに経由するルータの数で構成される。ある LAN のネットワーク構成図を図１に，ルータ１のルーティングテーブルを表１に示す。

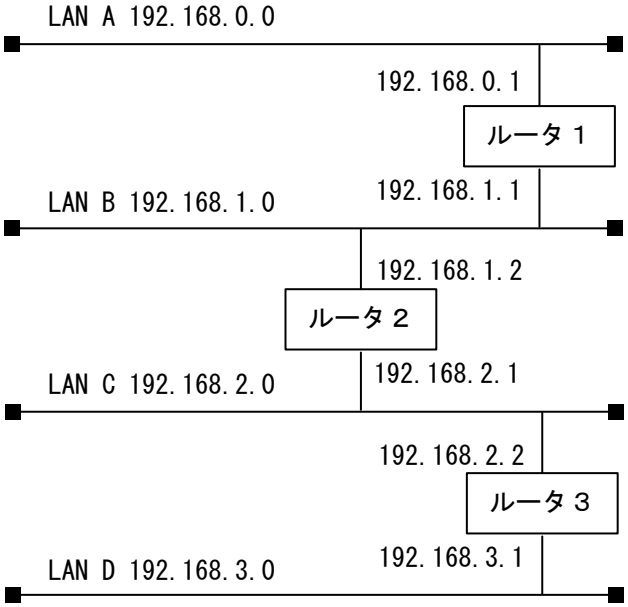

図１　ネットワーク構成図

表１　ルータ１のルーティングテーブル

送信先ネットワークアドレス	転送先ルータの IP アドレス	経由するルータ数
192.168.0.0	－	0
192.168.1.0	－	0
192.168.2.0	192.168.1.2	1
192.168.3.0	192.168.1.2	2

各ルータは,起動直後から 30 秒おきに自身が持っているルーティングテーブルの情報を全ての LAN に送信する。他のルータからの情報を受信したルータは，次のような動作で自身のルーティングテーブルを更新する。

① 受信した情報に含まれる″経由するルータ数″に 1 を加える。
② ″送信先ネットワークアドレス″がルーティングテーブルに存在する場合は③-A，そうでない場合は③-B の処理をする。
③-A ″経由するルータ数″の値が①より大きければ，″経由するルータ数″を①の値に書き換え，″転送先ルータの IP アドレス″を受信したルータの IP アドレスで書き換える。
③-B 受信した″送信先ネットワークアドレス″と″転送先ルータの IP アドレス″，①の値をルーティングテーブルに追加する。

ここで，ルータ 1 を起動した時を基準として，その 10 秒後にルータ 2 を起動し，さらにその 10 秒後にルータ 3 を起動する。各ルータの起動直後のルーティングテーブルの内容を表 2 に示す。

また各ルータのルーティングテーブルの更新状況を，基準時からの経過時間とともに図 2 に示す。

表 2 起動直後のルーティングテーブル

	送信先ネットワークアドレス	転送先ルータの IP アドレス	経由するルータ数
ルータ 1	192.168.0.0	－	0
	192.168.1.0	－	0
ルータ 2	192.168.1.0	－	0
	192.168.2.0	－	0
ルータ 3	192.168.2.0	－	0
	192.168.3.0	－	0

経過時間	［ルータ１］	［ルータ２］	［ルータ３］
0秒後（基準）	・起動		
10秒後	・ルーティングテーブルにLAN Cの経路情報を追加 ←	・起動 ・経路情報送信	
20秒後		・ルーティングテーブルに (4) の経路情報を追加	・起動 ・経路情報送信 →
30秒後	・経路情報送信 →	・ルーティングテーブルに (5) の経路情報を追加	
40秒後	・ルーティングテーブルにLAN Dの経路情報を追加 ←	・経路情報送信	→ ・ルーティングテーブルに (6) の経路情報を追加

図２　ルーティングテーブルの更新状況の推移

図２の「40秒後」における，ルータ２のルーティングテーブルを，表３に示す。

表３　ルータ２のルーティングテーブル

送信先ネットワークアドレス	転送先ルータのIPアドレス	経由するルータ数
192.168.0.0	(7)	1
192.168.1.0	－	0
192.168.2.0	－	0
192.168.3.0	(8)	1

(4) ～ (6) の解答群

ア．LAN A　　イ．LAN B　　ウ．LAN C
エ．LAN D　　オ．LAN A と LAN B　　カ．LAN A と LAN D
キ．LAN B と LAN C　　ク．LAN C と LAN D

(7)，(8) の解答群

ア．192.168.1.1　　イ．192.168.1.2
ウ．192.168.2.1　　エ．192.168.2.2

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商会ではリレーショナルデータベースを使用し，健康食品の販売管理を行っている。次に販売伝票を示す。なお，各項目は次のように設定されている。

・販売コードは一回の販売ごとに一つ割り振られ，一意の連番が付与される。
・顧客コードは一意の番号が付与されている。
・商品コードは一意の番号が付与されている。
・商品によっては，営業担当者の裁量により若干の割引が認められている。

販売伝票

販売コード　01234　　日付　XXXX/10/22

顧客コード　9873
顧客名　健康　花子
住所　東京都千代田区　　担当者番号　6789
TEL　03-4444-5555　　担当者名　Ｊ検　太郎

商品コード	商品名	定価	数量	販売額
172911	トマトリコピン	780	2	1,560
173216	クロレラ	650	5	3,000
173173	グルコサミン	3,980	1	3,900
:	:	:	:	:
		合計金額		12,900

図１　販売伝票

＜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の販売伝票をレコード形式にすると次のようになる。これは非正規形と呼ばれ，販売伝票をそのまま表現したものである。下線が引いてある項目は主キーである。

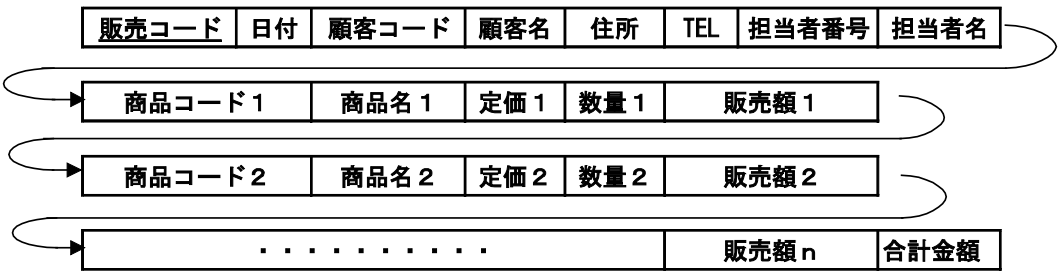

図２　非正規形

次に，販売伝票を正規化する。なお，問題の都合上，主キーの表示は省略している。

［第１正規化］

図３は，非正規形を第１正規化したものである。

第１正規化では，［　(1)　］。非正規形と同じキー項目ではレコードを特定することができなくなるので，主キーは［　(2)　］の複合キーとなる。

図３　第１正規形

［第２正規化］

図４は，第１正規形を第２正規化したものである。

第２正規化では主キーが複合キーである場合，［　(3)　］。

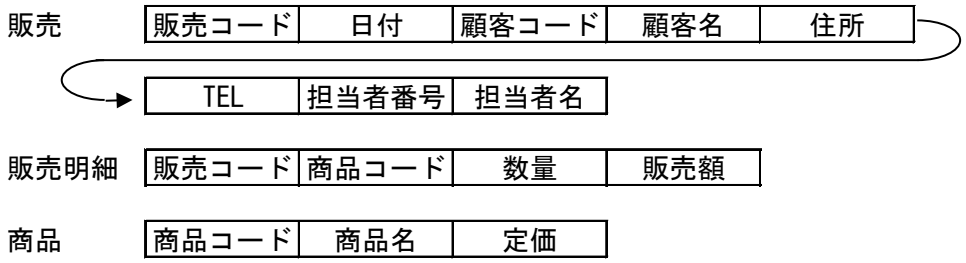

図４　第２正規形

［第３正規化］

図５は，第２正規形を第３正規化したものである。

第３正規化では，［　(4)　］。

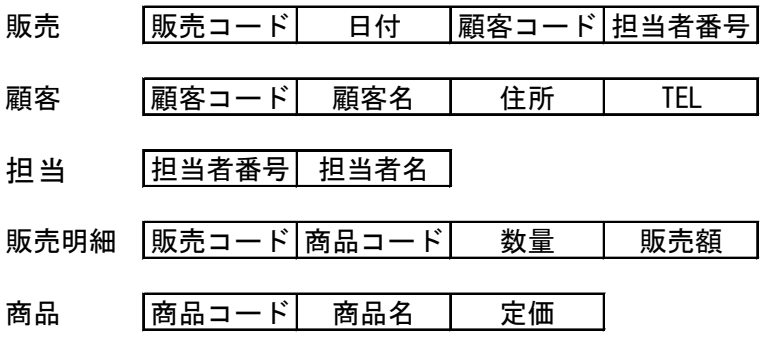

図５　第３正規形

(1)，(3)，(4) の解答群

ア．繰り返し構造を分離する

イ．主キー以外の属性間での依存関係を分離する

ウ．主キーとそれ以外の属性を分離する

エ．主キーを構成する各項目への部分的依存関係を分離する

(2) の解答群

ア．販売コードと TEL　　イ．販売コードと顧客コード
ウ．販売コードと商品コード　　エ．販売コードと担当者番号

＜設問２＞　月間売上優秀者を表彰するため，担当者ごとの販売総額を求める次の SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。なお，表示順は販売総額の降順とし，同額の場合は担当者番号の昇順とする。また，月の開始日，終了日はホスト変数":月開始日"，":月終了日"に格納されているものとする。

```
SELECT 担当者番号, 担当者名, [ (5) ] AS 販売総額
  FROM 担当 T, 販売 H, 販売明細 M
 WHERE T.担当者番号 = H.担当者番号
  AND  H.販売コード = M.販売コード
  AND  日付 BETWEEN :月開始日 [ (6) ] :月終了日
[ (7) ] 担当者番号, 担当者名
[ (8) ] 販売総額 DESC, 担当者番号
```

(5) の解答群

ア．AVG(数量*定価)　　イ．AVG(販売額)
ウ．SUM(数量*定価)　　エ．SUM(販売額)

(6) の解答群

ア．AND　　イ．AS　　ウ．FROM　　エ．TO

(7)，(8) の解答群

ア．AND　　イ．EXISTS
ウ．GROUP BY　　エ．HAVING
オ．IN　　カ．ORDER BY

＜設問３＞　先月１ヶ月間の商品ごとの平均売上単価を求める次のSQL文の［　　］に入れるべき適切な字句を解答群から選べ。なお，先月の開始日，終了日はホスト変数“:月開始日”，“:月終了日”に格納されているものとする。

```
SELECT S.商品コード, 商品名, 定価, [ (9) ] AS 平均売上単価
  FROM 商品 S, 販売明細 M, 販売 H
 WHERE S.商品コード = M.商品コード
  AND  M.販売コード = H.販売コード
  AND  日付 BETWEEN :月開始日 [ (6) ] :月終了日
[ (7) ] S.商品コード, 商品名, 定価
```

(9) の解答群

ア．SUM(販売額/数量)　　イ．SUM(定価*数量)/SUM(数量)

ウ．SUM(販売額)/SUM(数量)　　エ．販売額/数量

問題５　次のセキュリティに関する各設問に答えよ。

＜設問１＞　次のWebサイトのセキュリティに関する記述を読み，各問に答えよ。

インターネットが普及している今日では，インターネットショッピングが日常の買い物手段として定着しつつある。

インターネット上のショッピングサイトで買い物をすると，個人情報がWeb サイトに送信される。この個人情報を不正に入手するために，偽装したWebサイトに利用者を誘導して個人情報を搾取する悪質なWebサイトも存在する。誘導する手口としては，(a)金融機関などを装ったメールからの誘導，SNSからの誘導などがある。

また，送信される情報が盗聴される恐れもある。そこで，(b) SSL（または TLS）を使用した通信を行い，送信する情報の保護を行う。

(1) 下線(a)に関係の深い字句を解答群から選べ。

(1) の解答群

ア．インジェクション　　イ．クラック
ウ．バックドア　　エ．フィッシング

(2) 下線(b)のSSLで処理する内容を解答群から選べ。

(2) の解答群

ア．ポップアップブロック　　イ．暗号化通信
ウ．スパイウェアからの保護　　エ．不正アクセスからの防御

(3) SSLを利用したWebサイトのURLで使用するスキームを解答群から選べ。

(3) の解答群

ア．http　　イ．https　　ウ．ssh　　エ．ftp

(4) ショッピングサイトでも商品紹介のように SSL を利用しないページが存在するが，その理由として適切なものを解答群から選べ。

(4) の解答群

ア．SSLを利用したページはレスポンスが悪いので表示に影響が出るから
イ．SSLが利用できるページ数はドメイン内で１ページに限定されるから
ウ．SSLを利用するページはコンピュータウイルスの検査が行えないから
エ．SSLは送信フォーム以外に利用することができないから

＜設問２＞　次の Web サイトの認証に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

認証局が発行する「ディジタル証明書」を持つことで，安全な Web サイトであることが保証される。このディジタル証明書を利用してインターネット上で通信相手を認証する仕組みを［　(5)　］という。ディジタル証明書には，証明書の正当性を保証するために「認証局のディジタル署名」が付加されており，ディジタル証明書が正規の手続きにより作成されたことを保証している。

Web サイトの認証では，ハッシュ関数と公開かぎ暗号方式の技術を用いる。

ハッシュ関数は一方向関数であり，入力されたメッセージからビット列（ハッシュ値）を生成するもので，メッセージが同じであれば生成されるハッシュ値は同じになる。また，ハッシュ値から元のメッセージに戻すことは不可能である。代表的なハッシュアルゴリズムに［　(6)　］がある。

公開かぎ暗号方式は，「公開かぎ」と「秘密かぎ」のペアでメッセージの暗号化と復号を行うものであり，公開かぎで暗号化したメッセージはペアの秘密かぎでのみ復号が可能であり，秘密かぎで暗号化したメッセージはペアの公開かぎでのみ復号が可能である。

ディジタル証明書を使った認証の流れは次のとおりである。

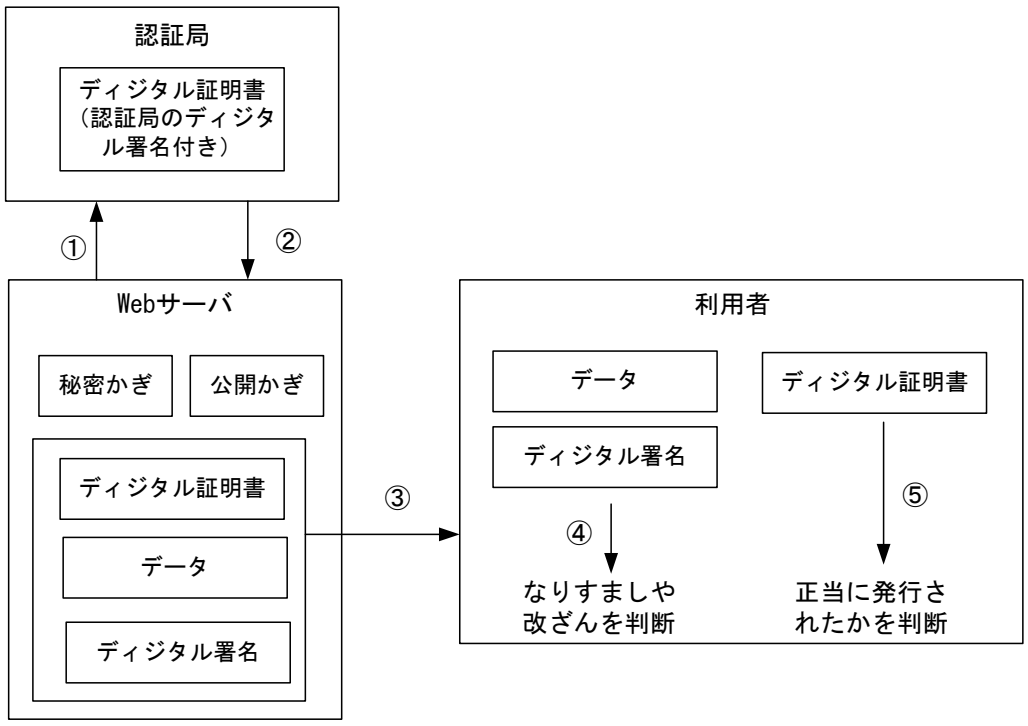

図　Web サイトの認証

［Webサイトがディジタル証明書を受け取るまでの流れ］

① Webサイトは，ペアとなる公開かぎと秘密かぎを作成し，公開かぎを認証局に送信してディジタル証明書の発行を依頼する。

② 認証局は，Webサイトの情報などから証明書を作成し，認証局のディジタル署名を付与してWebサイトに送信する。

［Webサイト認証の流れ］

③ Webサイトは，送信するデータから生成したハッシュ値を［ (7) ］で暗号化したディジタル署名とディジタル証明書をデータと一緒に利用者Xへ送信する。

④ 利用者Xは,ディジタル証明書に付与された認証局のディジタル署名を［ (8) ］で復号し，正当な手続きで発行されたディジタル証明書かどうかを確認する。

⑤ 利用者Xは,受信したディジタル署名を［ (9) ］で復号した値と,受信したデータから生成したハッシュ値を比較することで，なりすましや改ざんされていないことが確認できる。

(5) の解答群

ア．コールバック方式　　イ．チャレンジ・レスポンス
ウ．ワンタイムパスワード　　エ．公開かぎ基盤

(6) の解答群

ア．CA　　イ．PKI　　ウ．SHA-2　　エ．WPA2

(7) ～ (9) の解答群

ア．Webサーバの公開かぎ　　イ．Webサーバの秘密かぎ
ウ．認証局の公開かぎ　　エ．認証局の秘密かぎ
オ．利用者Xの公開かぎ　　カ．利用者Xの秘密かぎ

＜設問３＞　ディジタル証明書に含まれない情報を解答群から選べ。

(10) の解答群

ア．認証局の秘密かぎ　　イ．証明書の有効期限
ウ．認証局の名前　　エ．申請者の公開かぎ

＜メモ欄＞