文部科学省後援

情報システム試験

平成21年度後期 情報検定

＜実施　平成22年2月14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），ポケットベル，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

財団法人　専修学校教育振興会

＜受験上の注意＞

１．この試験問題は15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．合否通知の発送は平成22年3月中旬の予定です。
①団体受験された方は，団体経由で合否の通知をいたします。
②個人受験の方は，受験票に記載されている住所に郵送で合否の通知をいたします。
③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１　次の経営戦略および経営組織に関する設問に答えよ。

＜設問１＞　次の経営戦略分析手法に関する次の記述を読み，最も適切な字句を解答群から選べ。

(1) 企業の経営環境を外部環境（機会と脅威）内部環境（強みと弱み）に分けて分析する技法。

(2) 市場の成長性と自社の市場占有率から４つのポジション（花形･金のなる木･問題児・負け犬）に分類し，今後の事業展開を分析する技法。

(1)，(2) の解答群

ア．PPM　　イ．PDCA　　ウ．PDS　　エ．SWOT　　オ．SLA

＜設問２＞　次の経営戦略および企業組織に関する次の記述を読み，最も適切な字句を解答群から選べ。

(3) 企業が自社の業務の一部を外部の業者に委託すること。社内で人員を育成するよりもコストがかからない場合に用いられる。

(4) 複数の企業間で提携して共同で事業を行うこと。資本関係があるかないかでその強さが決まり，最も強い関係が M&A（合併，買収）である。

(5) 競争相手が少ない限定された市場に特化してシェアを獲得する考え方。

(6) 最高経営責任者のことで，企業経営の最高責任者を指す。

(7) 最高情報責任者のことで，情報技術に関する責任者であり，情報戦略の策定などを行う人。

(3) ～ (5) の解答群

ア．コストリーダーシップ戦略　　イ．差別化戦略　　ウ．ニッチ戦略
エ．バリューエンジニアリング　　オ．アライアンス　　カ．アウトソーシング

(6)，(7) の解答群

ア．CEO　　イ．CFO　　ウ．CIO　　エ．COO　　オ．CISO

問題２　次のネットワーク技術に関する設問に答えよ。

＜設問１＞　次の LAN のアクセス制御に関する記述中の［　　］に入れるべき適切な字句を選べ。

LAN の中で，データを送受信するためのアクセス制御法の一つに CSMA/CD 方式がある。CSMA/CD 方式でデータを送信する手順を以下に示す。

① データを送信するコンピュータは，データに送信先アドレス，送信元アドレスなどを付加してフレームを作成する。
② 他のコンピュータがフレームを送信しているかを確認する。
③ 他のコンピュータがフレームを送信していれば，［　(1)　］。そうでなければ，フレームの送信を開始する。
④ 送信されたフレームは，LAN に接続されているすべてのコンピュータで受け取る。受け取ったコンピュータは，送信先アドレスと自分のアドレスを比較して一致していれば受信し，一致していなければ破棄する。
⑤ 複数のコンピュータがほぼ同時に送信を開始した場合，衝突が発生する。この場合，受信しているコンピュータはフレームを破棄し，送信しているコンピュータは［　(1)　］。

(1) の解答群

ア．いつも同じ時間を経過してから手順②へ
イ．いつも同じ時間を経過してから手順④へ
ウ．ランダムな時間を経過してから手順②へ
エ．ランダムな時間を経過してから手順④へ

＜設問２＞　CSMA/CD のアクセス制御は，OSI 基本参照モデルの何層に含まれるか解答群から選べ。

(2) の解答群

ア．物理層（第 1 層）
イ．データリンク層（第 2 層）
ウ．ネットワーク層（第 3 層）
エ．アプリケーション層（第 7 層）

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。

＜設問３＞　次の WAN を用いた LAN 間接続に関する記述中の［　　］に入れるべき適切な字句を選べ。

遠隔地の支店の LAN 同士で業務上の情報を送受信する場合，自社のデータしか扱わない専用線を用いると比較的高いセキュリティの上で送受信を行うことができるが，コストが高いという問題がある。これに対して，複数の利用者が共用しているネットワークをそのまま用いるとコストは安くなるが，覗き見による情報の漏洩やデータの改ざんなどのおそれがあり危険である。そのため，VPN（Virtual Private Network）という技術を用いて共用線内で「仮想的な専用線」を作り出し LAN 同士を接続する方法がある。

VPN には ISP が提供する IP ネットワークで実現する［(3)］とインターネットで実現した［(4)］がある。［(4)］の方がコストは安く済むが通信速度が不安定であることなど，さまざまな問題点がある。また，インターネットを用いる VPN では，［(5)］と呼ばれる方式もあり，これはクライアント側に VPN 装置を使う必要が無いのが特徴である。

VPN を実現するには，トンネリングと呼ばれる技術が必要になる。例えば，図１のような VPN を構築し，東京にある LAN 内のコンピュータ（以下東京 CP）が大阪にある LAN 内のコンピュータ(以下大阪 CP)を宛先とするとき,東京 CP は大阪 CP の［(6)］を指定する。

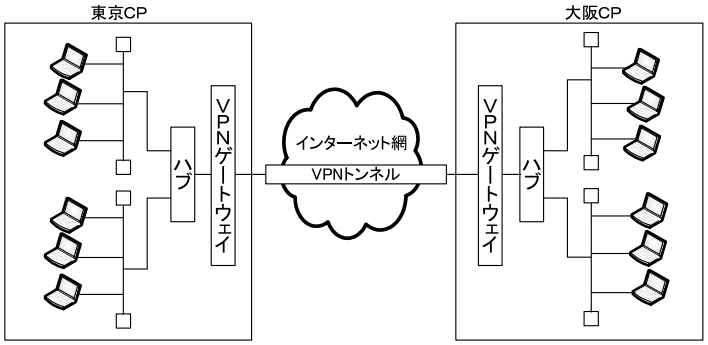

図１　VPN 図

しかし，［(6)］は大阪の LAN 内におけるコンピュータの宛先であり，共用線内における大阪の LAN そのものの場所を表すには，［(7)］が必要になる。そこで VPN 装置を用いて東京 CP が指定した［(6)］に自動的に大阪の LAN の［(7)］を付加することにより大阪 CP に接続することが可能になる。

また，VPN で重要になるのがセキュリティの問題である。セキュリティ対策には暗号化を行うことが有力な対策のひとつであるが，従来のようなアプリケーションごとに暗号化するのは効率的では無い。そこで，アプリケーションとは無関係に全ての通信データを自動的に暗号化する［(8)］というプロトコルが使われることが多い。［(8)］では利用する暗号化アルゴリズムを特定せずに，あらゆる暗号化アルゴリズムを利用できるようになっている。

(3) ～ (8) の解答群

ア．プロトコル	イ．レイヤ	ウ．IP マスカレード
エ．IP-VPN	オ．SSL-VPN	カ．グローバル IP アドレス
キ．インターネット-VPN	ク．IP パケット	ケ．プライベート IP アドレス
コ．IPsec		

問題３　次の図書館システムに関する記述を読み，設問に答えよ。

Ａ大学の図書館では，これまで手書きの貸出カードを使った書籍の貸出を行っていた。しかし，書籍管理や貸出管理にかかる手間が膨大になるため，コンピュータ管理による貸出システムを導入することにした。これまでの貸出カードによる方法に変えて，IC チップを埋め込んである学生証を用いた貸出方法となる。

この大学図書館の図書貸出規約の一部は，以下の通りである。

・一人で借りられる書籍は，5 冊までである。
・貸出期間は 2 週間である。
・返却予定日を過ぎても書籍の返却がない場合は，利用の停止期間を設ける。

［テーブルの形式］

○ 学生テーブル（＿＿は主キーである）

学生番号	氏名	…

学生の情報を管理するテーブルである。

○ 貸出テーブル（＿＿は主キーである）

学生番号	書籍コード	貸出日	返却予定日	返却フラグ

１件の貸出ごとに１件のレコードを生成する。返却フラグは，レコード生成時に 0 が入り，返却されたら 1 が入る。

○ 書籍テーブル（＿＿は主キーである）

書籍コード	書籍名称コード	著者コード

全ての蔵書を記録するテーブルである。同一の書籍名が複数ある場合は，それぞれにユニークな書籍コードを付ける。

○ 書籍名称テーブル（＿＿は主キーである）

書籍名称コード	書籍名

書籍名を管理するテーブルである。

○ 著者テーブル（＿＿は主キーである）

著者コード	著者名

著者名を管理するテーブルである。

○ 利用停止テーブル（＿＿は主キーである）

学生番号	回数	停止解除日

貸出停止の情報を管理するテーブルである。延滞があると，返却予定日から１週間の利用停止期間を設けるため，停止解除日にその日付を設定する。

＜設問１＞　次の貸出に関する記述中の［　　］に入れるべき適切な数値を解答群から選べ。

書籍の貸出を行う場合は，以下の 2 点を調べる。書籍を 1 冊借りようとしている学生の学生番号が G212001 で，今日の日付が 2009 年 12 月 1 日の場合は，次のような手順で SQL 文を実行する。

① 利用停止テーブルに登録されており,借りようとする日が停止解除日以降であるかを調べる。ここでは，レコード件数が 0 か 1 かで判断する。

```
SELECT COUNT(*) FROM 利用停止テーブル
 WHERE 学生番号 = 'G212001'
  AND  停止解除日 > '2009/12/01'
```

② 現在借りている書籍の冊数が 5 冊未満であるかを調べる。

```
SELECT COUNT(*) FROM 貸出テーブル
 WHERE 学生番号 = 'G212001'
  AND  返却フラグ = 0
```

①については［　(1)　］であり，かつ，②については［　(2)　］未満であれば貸出テーブルにレコードを追加する。

(1)，(2) の解答群

ア．0	イ．1	ウ．2
エ．3	オ．4	カ．5

＜設問２＞　次の書籍検索に関する SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。

図書館には，書籍検索を行う端末が設置されている。検索するときのキーワードとして，書籍名，または，著者名の一部を入力することで，該当する書籍のリストを書籍名称コードの昇順に表示するようになっている。表示する内容は，書籍名，著者名，貸出中かどうかである。これは，次の手順により作成する。

① 書籍テーブルから貸出中の書籍を除いた貸出可能ビューを作成する。

```
CREATE VIEW 貸出可能ビュー
  AS SELECT 書籍名称コード, 著者コード, 1 AS 貸出区分
       FROM 書籍テーブル S
     WHERE NOT EXISTS (
       SELECT * FROM 貸出テーブル K
        WHERE S.書籍コード = K.書籍コード
         AND  (3)  )
```

② 書籍テーブルと貸出テーブルから，貸出中ビューを作成する。

```
CREATE VIEW 貸出中ビュー
  AS SELECT 書籍名称コード, 著者コード, 0 AS 貸出区分
       FROM 書籍テーブル S, 貸出テーブル K
      WHERE S.書籍コード = K.貸出コード
       AND  (3)
```

③ ２つのビューを合わせて作業ビューを作成する。なお，UNION 集合演算子は，複数の問い合わせを１つに結合するものである。

```
CREATE VIEW 作業ビュー
  AS SELECT * FROM 貸出可能ビュー
     UNION
     SELECT * FROM 貸出中ビュー
```

④ 作業ビューと他のテーブルを結合して，表示に必要な情報を抽出する。なお，貸出中かどうかは，0（貸出中）と 1（貸出可能）として抽出し，ここでは，書籍名に'情報'が含まれている書籍を検索することとする。

```
SELECT V.書籍名称コード, 書籍名, 著者名, MAX(貸出区分)
  FROM 作業ビュー V, 書籍名称テーブル M, 著者テーブル T
 WHERE V.書籍名称コード = M.書籍名称コード
  AND  V.著者コード = T.著者コード
  AND  書籍名称 (4) '%情報%'
(5) V.書籍名称コード, 書籍名, 著者名
ORDER BY V.書籍名称コード
```

(3) の解答群

ア．返却フラグ = 0
イ．返却フラグ = 1
ウ．S.著者コード = K.著者コード
エ．S.書籍名称コード = K.書籍名称コード

(4) の解答群

ア．=　　イ．IS
ウ．EXISTS　　エ．LIKE

(5) の解答群

ア．GROUP BY　　イ．SET
ウ．HAVING　　エ．INTO

＜設問３＞　次の書籍返却に関する SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。

返却予定日を過ぎても書籍を返却しない学生は，利用停止テーブルにレコードを追加または，レコードの修正を行う。この作業は毎日午前 1 時にバッチ処理される。

バッチ処理をする時の日付が 2009 年 12 月 1 日である場合，利用停止テーブルにレコードの追加または修正を行うには，次のような手順で SQL 文を実行する。

① 貸出テーブルから，2009 年 12 月 1 日より前の日までが返却予定日になっているレコードの学生番号を抽出して学生ビューを作成する。

```
CREATE VIEW 学生ビュー
  AS SELECT DISTINCT 学生番号 FROM 貸出テーブル
    WHERE 返却予定日 [ (6) ] '2009/12/01'
     AND  返却フラグ = 0
```

② 学生ビューに抽出された学生番号の中で,利用停止テーブルの中に含まれている学生については，回数と停止解除日を更新する

```
UPDATE 利用停止テーブル R
  [ (7) ] 回数 = 回数 + 1,
          停止解除日 ='2009/12/7'
  WHERE EXISTS (
      SELECT * FROM 学生ビュー V
      WHERE V.学生番号 = R.学生番号 )
```

③ 学生ビューに抽出された学生番号の中で,利用停止テーブルの中に含まれていない学生番号に関するレコードを追加する。

```
INSERT [ (8) ] 利用停止テーブル
  SELECT 学生番号, 1, '2009/12/7'  FROM 学生ビュー V
  WHERE NOT EXISTS (
       SELECT * FROM 利用停止テーブル R
        WHERE V.学生番号 = R.学生番号 )
```

(6) の解答群

ア．=　　イ．<>
ウ．<　　エ．>

(7)，(8) の解答群

ア．FROM　　イ．INTO
ウ．JOIN　　エ．SET
オ．HAVING　　カ．SELECT

＜設問４＞　次の書籍予約に関する SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。

学生からの要望で，書籍の予約に関する希望が出た。そこで，書籍検索の機能に予約の機能を追加することにした。

まず，予約テーブルを作成した。書籍検索画面で予約を行うと，レコードが生成されるようになる。

○ 予約テーブル（＿＿は主キーである）

書籍名称コード	学生番号	予約日	予約時間	貸出フラグ

・同じ書籍が複数あることから，予約する書籍の区別は書籍名称コードを用いる。
・貸出フラグは，予約をした段階で 0 が，予約をした学生が借りたら 1 が入る。
・同じ書籍に複数の予約が発生した場合は，予約日と予約時間の昇順に貸出を行う。

次に，設問２の SQL 文に，予約されている冊数を表示するための変更を行う。

① 貸出可能ビューと貸出中ビューの項目として，最後に予約数を追加し，初期値として 0 を設定する。

```
CREATE VIEW 貸出可能ビュー
  AS SELECT S.書籍コード, 書籍名称コード, 著者コード, 1 AS 貸出区分,
            0 AS 予約数
       FROM 書籍テーブル S
      WHERE NOT EXISTS (
        SELECT * FROM 貸出テーブル K
         WHERE S.書籍コード = K.書籍コード
          AND  [ (3) ]  )

CREATE VIEW 貸出中ビュー
  AS SELECT S.書籍コード, 書籍名称コード, 著者コード, 0 AS 貸出区分
            0 AS 予約数
       FROM 書籍テーブル S, 貸出テーブル K
      WHERE S.書籍コード = K.貸出コード
       AND  [ (3) ]
```

② 予約済ビューを作成する。

```
CREATE VIEW 予約済ビュー
AS SELECT 書籍名称コード, COUNT(*) AS 予約数
     FROM [ (9) ]
    GROUP BY 書籍名称コード
```

③ ２つのビューを合わせて作業ビューを作成する。

```
CREATE VIEW 作業ビュー
  AS SELECT * FROM 貸出可能ビュー
     UNION
     SELECT * FROM 貸出中ビュー
```

④ 予約済ビューの予約数で，作業ビューの予約数を更新する。なお，作業ビューは更新可能なビューである。

```
UPDATE 作業ビュー S
   (7)   S.予約数 = Y.予約数
  FROM 予約済ビュー Y
 WHERE S.  (10)  = Y.  (10)
```

⑤ 作業ビューと他のテーブルを結合して，表示に必要な情報を抽出する。なお，貸出中かどうかは，0（貸出中）と1（貸出可能）として抽出し，ここでは，書籍名に'情報'が含まれている書籍を検索することとする。

```
SELECT 書籍コード, 書籍名, 著者名, 貸出区分, 予約数
  FROM 作業ビュー V, 書籍名称テーブル M, 著者テーブル T
 WHERE V.書籍名称コード = M.書籍名称コード
  AND  V.著者コード = T.著者コード
  AND  書籍名称   (4)   '%情報%'
  (5)
```

(9) の解答群

ア．作業ビュー　　イ．貸出中ビュー
ウ．貸出可能ビュー　　エ．予約テーブル

(10) の解答群

ア．書籍コード　　イ．書籍名称コード
ウ．著者コード　　エ．予約数

問題４　次の情報セキュリティに関する記述を読み，各設問に答えよ。

情報セキュリティはコンピュータの発展とともにもたらされた大きな課題である。1992 年 11 月に OECD（経済協力開発機構）は「情報システムセキュリティのためのガイドライン」を発表した。ここでは，「情報セキュリティの目的は，情報システムに依存するものを，(a) 可用性，機密性，完全性の欠如に起因する危害から保護することである」と定義した。その後，1997 年に見直され，さらに 2002 年の OECD 理事会で「情報システム及びネットワークのセキュリティのためのガイドライン　－セキュリティ文化の普及に向けて－」が採択された。ここでは，セキュリティマネジメントやセキュリティの設計及び実装などの 9 つの原則が提示されている。

ネットワークシステム上の情報セキュリティを考えるとき，その脅威として通信データの破壊や改ざん，ネットワークの不正使用などがある。それらの脅威への対策として，暗号化は有効な手段である。

＜設問１＞　下線部（a）の可用性，機密性，完全性の説明として適切な組み合わせを解答群から選べ。

［説明］

① データおよび情報が正確で完全であり，かつ正確性・完全性が維持されること。

② データ，情報，情報システムが適時に，必要な様式にしたがい，アクセスでき，利用できること。

③ 権限のある者が，権限のあるときに，権限のある方式にしたがった場合のみに，データおよび情報が開示されること。

(1) の解答群

	可用性	機密性	完全性
ア	①	②	③
イ	①	③	②
ウ	②	①	③
エ	②	③	①

＜設問２＞　暗号化方式には共通かぎ暗号方式と公開かぎ暗号方式がある。それぞれの特徴として適切な組み合わせを解答群の中から選べ。ただし，ディジタル署名は除く。

［特徴］

① 暗号化・復号の処理の負荷が小さく処理時間が短い。

② 暗号化・復号の処理の負荷が大きく処理時間が長い。

③ 通信相手ごとにかぎを使い分けるため，かぎの管理が煩雑になる。

④ 復号するためのかぎは通信相手に関係なく共通に使用することができる。

⑤ 暗号化するためのかぎから復号するためのかぎは推測することはできない。

(2) の解答群

	共通かぎ暗号方式	公開かぎ暗号方式
ア	①，④	②，③，⑤
イ	①，③	②，④，⑤
ウ	②，④	①，③，⑤
エ	②，⑤	①，③，④

＜設問３＞　次のディジタル署名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。

ディジタル署名では公開かぎ暗号方式とハッシュ関数を使用して，なりすましを防止することができる。

また，ここで用いられるハッシュ関数は任意の長さのメッセージをハッシュ化して短いメッセージダイジェストに変換する関数である。

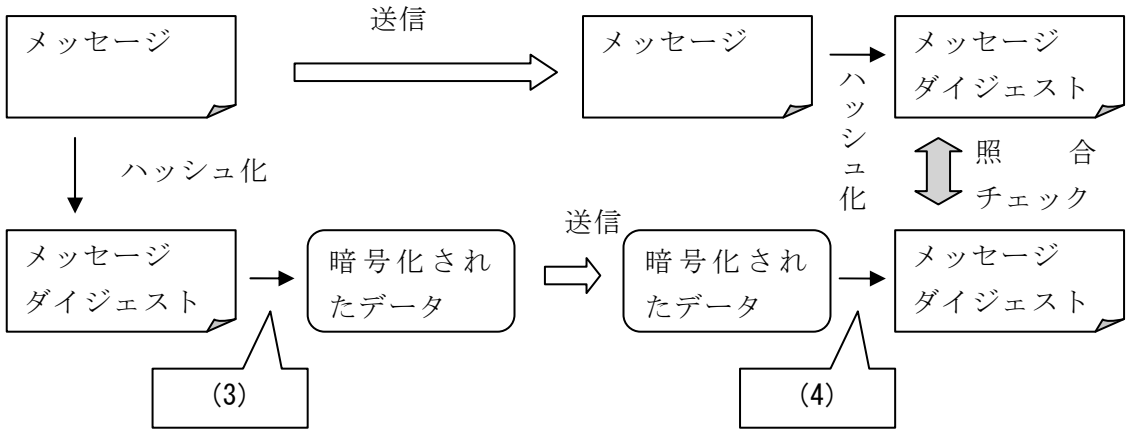

図１　ディジタル署名

(3)，(4) の解答群

ア．送信者の公開かぎで暗号化　　イ．送信者の秘密かぎで暗号化
ウ．受信者の公開かぎで暗号化　　エ．受信者の秘密かぎで暗号化
オ．送信者の公開かぎで復号　　カ．送信者の秘密かぎで復号
キ．受信者の公開かぎで復号　　ク．受信者の秘密かぎで復号

＜設問４＞　ディジタル署名に使用する代表的なハッシュ関数に MD5 と SHA1 がある。MD5 の説明として適切なものを (5) の解答群から，SHA1 の説明として適切なものを (6) の解答群から選べ。

(5)，(6) の解答群

ア．もとのメッセージをハッシュ化して，128 ビットのハッシュ値を生成する。RSA 暗号方式の考案者である Ronald　Rivest 氏らによって開発された。ハッシュ関数の逆関数を使用し，メッセージダイジェストからもとのメッセージを生成することができる。

イ．もとのメッセージをハッシュ化して，128 ビットのハッシュ値を生成する。RSA 暗号方式の考案者である Ronald　Rivest 氏らによって開発された。ハッシュ関数には一方向性関数が含まれており，メッセージダイジェストからもとのメッセージを生成することはできない。

ウ．もとのメッセージをハッシュ化して，160 ビットのハッシュ値を生成する。ハッシュ関数は一方向性関数であり，ハッシュ値からもとのメッセージを生成することはできない。1995 年に米国標準技術局(NIST)によって，米国政府の標準ハッシュ関数として採用された。

エ．もとのメッセージをハッシュ化して，160 ビットのハッシュ値を生成する。ハッシュ関数の逆関数を使用し，メッセージダイジェストからもとのメッセージを生成することができる。

＜設問５＞　インターネット上での認証に使用される PKI（公開かぎ基盤）の仕組みに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

インターネットのオンラインショップでは顧客が店舗の認証を図２のような手順で行う。

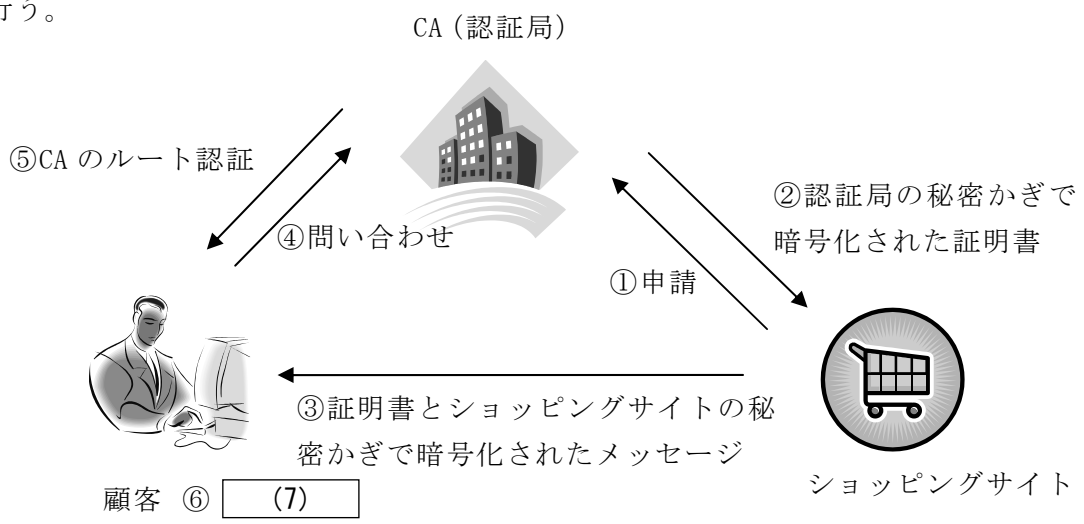

図２　PKI の仕組み

(7) の解答群

ア．証明書をCAの公開かぎで復号する。さらに，メッセージをショッピングサイトの公開かぎで復号することによりショッピングサイトの認証とメッセージが改ざんされていないことを確認する。

イ．証明書とメッセージをショッピングサイトの公開かぎで復号し，ショッピングサイトの認証とメッセージが改ざんされていないことを確認する。

ウ．証明書をCAの公開かぎで復号し，ショッピングサイトを認証する。メッセージはショッピングサイトの公開かぎで復号し，CAの信頼性を確保する。

エ．証明書をショッピングサイトの公開かぎで復号し，ショッピングサイトの認証を行い，メッセージはCAの公開かぎで復号しCAの認証を行う。

＜メモ欄＞

＜メモ欄＞