文部科学省後援

情報システム試験

令和３年度前期 情報検定

＜実施　令和3年9月12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()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．試験後の合否結果（合否通知），および合格者への「合格証・認定証」はすべてＷｅｂ認証で行います。
①試験実施日の翌月より情報検定（J検）Webサイト合否検索ページ及びモバイル合否検索サイト上で，ディジタル「合否通知」，ディジタル「合格証・認定証」が交付されます。
②団体宛には合否結果一覧ほか，試験結果資料一式を送付します。
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　次の企業活動に関する記述を読み，各設問に答えよ。

企業がビジネス活動を行う上で関わる法律やガイドラインには,様々なものがある。

法律を守ることは，企業が存続していくための最低限の決まりごとである。一方，ガイドラインは法律ほど厳密なものではないが，ガイドラインに準拠することで業界や業種を一定以上の水準に保ち，共通の認識を持つことができる。

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

知的財産権は，著作権と産業財産権に大別される。

著作権は人の知的な創作活動の中で，芸術や文化的な創作物に関する権利であり，著作物を創作した著作者に与えられる権利である。著作権には，他人に譲渡したり，相続したりすることはできない一身専属的な［(1)］と著作物を市場に流通させることで発生する利益を保護する［(2)］があり，保護期間は著作者の死後［(3)］年である。また,著作物の伝達に重要な役割を果たしている実演家,音楽ソフト製作者,放送事業者等に認められる権利に［(4)］がある。

産業財産権は，特許権，実用新案権，意匠権，商標権の総称である。発明や創造の成果を保護し，産業や生活に応用できるように支援することを目的としている。産業財産権の概要は次のようになっている。

表１　産業財産権の概要

権利名	内容	保護法	保護期間
特許権	(5)	特許法	出願日から 20 年
実用新案権	(6)	実用新案法	出願日から 10 年(無審査)
意匠権	(7)	意匠法	設定登録日から 25 年
商標権	(8)	商標法	設定登録日から 10 年(更新可能)

(1)，(2)，(4) の解答群

ア．公表権　　イ．氏名表示権　　ウ．著作財産権
エ．著作者人格権　　オ．著作隣接権　　カ．同一性保持権

(3) の解答群

ア．10　　イ．20　　ウ．50　　エ．70

(5) ～ (8) の解答群

ア．産業上利用可能である発明を独占的に利用できる権利

イ．製品やサービスに関するものを識別する名称やシンボルなどを独占して利用できる権利

ウ．物品の形や模様，色，またはこれらのデザインに関するものを独占的に利用できる権利

エ．発明ほどではないが，物品の形状や構造または組合せに関する考案を独占的に利用できる権利

＜設問２＞　次の個人情報保護法(個人情報の保護に関する法律)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。

個人情報保護法は，情報化の発展により個人の権益が侵害される恐れがあることから，個人情報を取り扱う事業者に対して個人情報の取り扱いを定めた法律であり，何度かの改正を受けている。

従来の個人情報保護法で適用対象外となっていた取り扱う個人情報の数が 5,000 件以下の小規模取扱事業者も適用対象になった。また，個人情報について適切な保護を講ずる体制を整備している事業者等を認定する［ (9) ］という制度がある。事業者はこれを取得することで，個人情報保護法を順守していることを顧客や消費者に示すことができる。

また，IoT の普及により多くのデータが収集され，それを分析することは，マーケティングや商品開発に非常に有効である。しかし，データには他のデータと組み合わせることにより個人を特定できるものもあるため，個人の特定ができないよう次の表 2 のように，［ (10) ］を行い利用する。

表２　個人が特定できないように処理した例

	会員番号	氏名	購入種類	金額	日付
収集されたデータ	123456	J 検太郎	セーター	5,980 円	2021/10/3
変更後のデータ	削除	削除	衣料品	1 万円未満	2021/10

(9) の解答群

ア．プライバシーガイドライン　　イ．プライバシーシール

ウ．プライバシーマーク　　エ．プライバシーライセンス

(10) の解答群

ア．仕分け　　イ．匿名加工　　ウ．名寄せ　　エ．振り分け

問題２　次の構造化設計に関する記述を読み，各設問に答えよ。

＜設問１＞　記述中の［　　］に入れるべき適切な字句を解答群から選べ。

構造化設計では，システムの機能をいくつかのモジュールに分割して開発する。

モジュール分割の代表的な技法として，データの流れに着目してモジュール分割を行うSTS分割や［(1)］，データの構造に着目してモジュール分割を行う［(2)］や［(3)］などがある。

STS 分割は，一連の処理をＳ(源泉)，Ｔ(変換)，Ｓ(吸収)の三つに分割し，それぞれを独立したモジュールで実現する。

［(1)］は，データの登録や修正のように，データの種類によって処理内容単位でモジュール分割を行う。

［(2)］は，入力データと出力データの関係からモジュール分割を行うもので，基本，連続，繰り返し，選択の図式を使って表現する。

［(3)］は，入力データの構造に着目してモジュール分割を行うもので，データが「いつ，どこで，何回」使われるかをもとに，順次・選択・繰り返しの制御構造で表現する。

(1) ～ (3) の解答群

ア．FP 法　　イ．共通機能分割
ウ．同値分割　　エ．ジャクソン法
オ．トランザクション分割　　カ．ワーニエ法

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

図１は，試験の答案を採点し成績一覧表を出力する処理を，STS 分割によりモジュール分割した例である。

STS 分割は，処理の最初から見て，入力したデータが徐々に形を変え，もはや入力データといえなくなる状態に達した点(図１中のα)である［(4)］と，処理の最後から見て，処理するデータが最初に出力データになる点(図１中のβ)である［(5)］を境にして分割し，それぞれを独立したモジュールで開発する。

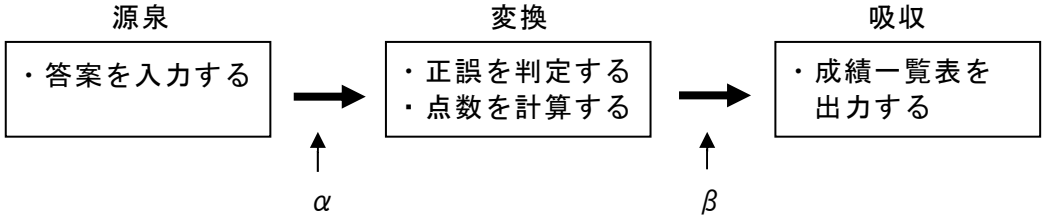

図１　モジュール分割の例

(4)，(5) の解答群

ア．最早結合点　　イ．最大抽象出力点

ウ．最大抽象入力点　　エ．最遅結合点

＜設問３＞　次のモジュールの強度に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

モジュールの強度とは，モジュール内部の関連性の強さを表すもので，モジュール内部の各要素の関連性が強いほど，モジュールの独立性が高くなり，強度も強いモジュールとなる。

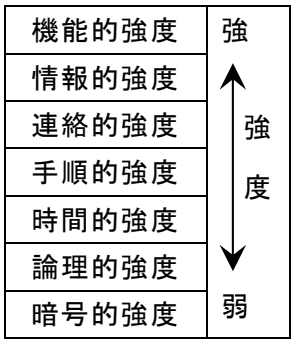

図２　モジュールの強度

それぞれの機能の関係により，モジュールの強度は次のようになる。

［(6)］：単にモジュールの大きさだけで分割し，モジュール内には関連性のない複数の機能が含まれている。

［(7)］：モジュール内の機能が一つの処理を実行するだけのもの。

［(8)］：関連のある複数のモジュールを一つにまとめ，どの機能が呼び出されるかは引数の値によって決まる。

(6) ～ (8) の解答群

ア．暗号的強度　　イ．機能的強度

ウ．時間的強度　　エ．情報的強度

オ．手順的強度　　カ．連絡的強度

キ．論理的強度

＜設問４＞　次のモジュールの結合度に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

モジュールの結合度とは，モジュール間の関連性の強さを表すものであり，他のモジュールとの関連性が弱いほど結合度は低くなり，モジュールの独立性を高めることができる。

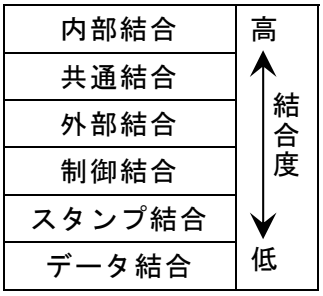

図３　モジュールの結合度

それぞれのモジュールの関係により，結合度は次のようになる。

［　(9)　］：複数のモジュール間で，必要なデータのみを引数として受け渡す。

［　(10)　］：他のモジュール内のデータを直接参照する。

(9)，(10) の解答群

ア．外部結合　　イ．共通結合　　ウ．スタンプ結合

エ．制御結合　　オ．データ結合　　カ．内部結合

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。

ネットワーク上で TCP/IP を利用した通信を行う場合，通信機器には IP アドレスが割り振られる。IP アドレスは従来から利用されてきた IPv4 アドレスの枯渇が問題となり，IPv6 という新しい規格の IP アドレスが利用されるようになってきた。

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

IPv4 の IP アドレスは［(1)］ビットであり，「192.168.0.20」のように 8 ビットずつ 10 進数に変換した値をドット(.)で区切り表記する。一方，IPv6 の IP アドレスは［(2)］ビットであり，「2008:00ab:3415:0000:0000:0000:cdef:7a6c」のように 16 ビットずつ 16 進数に変換した値をコロン（:）で区切って表記する。

なお，IPv6 には表記を短くするルールが二つあり，一つはすべて 0 のフィールドが連続する場合，１か所に限りダブルコロン(::)で 0 を省略できる。もう一つはフィールド内の先頭からの 0 は省略できる。このルールに従うと前述の IP アドレスは「2008:ab:3415::cdef:7a6c」のようになる。

(1)，(2) の解答群

ア．32　　イ．64　　ウ．128　　エ．256

＜設問２＞　次の IPv4 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。

IPv4 で利用される IP アドレスには，インターネットに接続する機器に世界中で重複しないように割り当てられる［(3)］IP アドレスと，LAN の中で利用する機器に割り当てられインターネット空間では利用できない［(4)］IP アドレスがある。

LAN からインターネットへアクセスするには，インターネットの出入り口にあるルータの持つアドレス変換機能を用いて，［(3)］IP アドレスと［(4)］IP アドレスの変換を行う。この機能を 1 対 1 で行うのが［(5)］である。しかし，1 対 1 では LAN 内の複数の PC から同時に要求があった場合に応えられないため，IP アドレスとポート番号を合わせて変換することで解決したものが［(6)］である。

(3)，(4) の解答群

ア．グローバル　　イ．プライベート

ウ．ブロードキャスト　　エ．マルチキャスト

(5)，(6) の解答群

ア．CIDR　　イ．NAPT　　ウ．NAT　　エ．NIC

＜設問３＞　次の IPv4 と IPv6 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。

現在は IPv4 から IPv6 への過渡期にあり，両方のネットワークが存在している。この二種類のネットワーク間は，そのままでは通信できない。そこで IPv4 の IP アドレスと IPv6 の IP アドレスを相互に変換する仕組みとして，NAT64 と DNS64 を組み合わせて利用する。一般的には，IPv4 の IP アドレスの先頭にウェルノウンプレフィックス「64:ff9b::/96」を付加して IPv6 の IP アドレスを得る。

［IPv4 の IP アドレスと IPv6 の IP アドレスの変換例］

IPv6 ネットワーク内の送信元から IPv4 ネットワーク内の jken.co.jp に送信する。

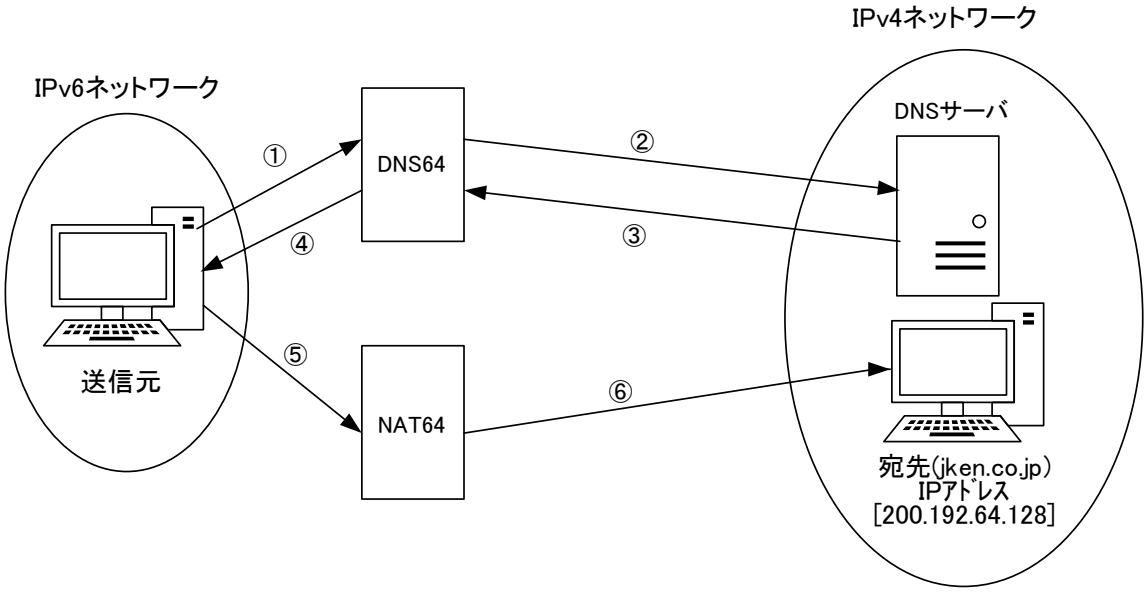

図　IP アドレス変換の仕組み

① DNS64 に，「jken.co.jp」の IP アドレスを問い合わせる。

② DNS64 は，IPv4 ネットワークの DNS サーバに，「jken.co.jp」の IP アドレスを問い合わせる。

③ DNS サーバは，「jken.co.jp」の IP アドレス「200.192.64.128」を DNS64 に送る。

④ DNS64 は，③の IP アドレスにウェルノウンプレフィックス「64:ff9b::/96」を付加した IPv6 形式の IP アドレス「［　(7)　］」を送信元に送る。

⑤ 送信元は，④で受け取った IP アドレスを宛先 IP アドレスにして NAT64 に送る。

⑥ NAT64 は，⑤で受け取ったパケットの宛先 IP アドレスを「200.192.64.128」に変更して IPv4 ネットワーク内の宛先 jken.co.jp に送る。

(7) の解答群

ア．64:ff9b::4080:c0c8　　イ．64:ff9b::4080:c8c0

ウ．64:ff9b::c0c8:4080　　エ．64:ff9b::c8c0:4080

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スーパーマーケットは，リレーショナルデータベースを使用して販売管理をしている。顧客がレジで会計を行う毎にレシートが一枚発行される。１日に何度か会計を行った場合は，そのつど異なるレシートNoのレシートが発行され，販売回数もそのつど加算する。

販売情報をもとに顧客の利用状況を分析することになった。

今回の処理で使用する表は次のようになっている。下線(実線)の項目は主キーであり，下線(破線)の項目は外部キーである。

［販売データ］

レシートNo	顧客ID	販売年月日

［販売明細データ］

レシートNo	商品コード	販売数量

［商品表］

商品コード	商品名	単価

［顧客表］

顧客ID	顧客名	フリガナ	性別	郵便番号	住所	電話番号

なお，レシートNo，顧客ID，商品コードはそれぞれ一意の値が付与されている。

今回SQL文で利用する関数である。

・CURRENT_DATE関数：参照時の日付をDATE型で返す日時値関数である

・DATEDIFF関数　　：(″d″，開始日，終了日)の組合せで引数を指定し，開始日から終了日の差分を日数で取得する

また，TOP句を使用すると指定した数のレコードを先頭から順番に取得することができ，ORDER BY句と組み合わせることで上位のレコードを取得できる。

＜使用例＞　成績表から得点上位３位までを抽出する場合，次のように記述する

［成績表］

学生番号	教科コード	得点

［SQLの例］

```
SELECT TOP 3 学生番号，教科コード，得点
  FROM 成績表
ORDER BY 得点 DESC
```

＜設問１＞　それぞれの集計表にデータを挿入する次の SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。なお，″:1 ヶ月前年月日″は，該当の値を格納する置換変数である。また，直近１ヶ月販売金額表，直近１ヶ月販売回数表，経過日数表は作成済みである。

①　直近1ヶ月に販売した商品について,顧客ごとの販売金額合計を集計した直近1ヶ月販売金額表を作成する。

```
INSERT [ (1) ] 直近１ヶ月販売金額表(顧客 ID, 販売金額)
  SELECT 販売データ.顧客 ID, [ (2) ]
    FROM 販売データ, 販売明細データ, 商品表
   WHERE 販売データ.レシート No = 販売明細データ.レシート No
     AND 販売明細データ.商品コード = 商品表.商品コード
     AND 販売データ.販売年月日 >= :1 ヶ月前年月日
  [ (3) ] BY 販売データ.顧客 ID
```

②　直近１ヶ月に販売した商品について，顧客ごとの販売回数を集計する直近１ヶ月販売回数表を作成する。

```
INSERT [ (1) ] 直近１ヶ月販売回数表(顧客 ID, 販売回数)
  SELECT 顧客 ID, [ (4) ] FROM 販売データ
   WHERE 販売年月日 >= :1 ヶ月前年月日
  [ (3) ] BY 顧客 ID
```

③　顧客ごとに,最後に販売してから経過した日数を集計する経過日数表を作成する。

```
INSERT [ (1) ] 経過日数表(顧客 ID, 経過日数)
  SELECT 顧客 ID, [ (5) ] FROM 販売データ
  [ (3) ] BY 顧客 ID
```

(1)，(3) の解答群

ア．AND	イ．AS	ウ．INTO
エ．GROUP	オ．OR	カ．ORDER

(2)，(4) の解答群

ア．AVG(販売明細データ.販売数量)
イ．COUNT(*)
ウ．COUNT(販売明細データ.販売数量)
エ．COUNT(販売明細データ.販売数量 * 商品表.単価)
オ．SUM(販売明細データ.販売数量)
カ．SUM(販売明細データ.販売数量 * 商品表.単価)

(5) の解答群

ア. AVG(DATEDIFF("d", 販売年月日, CURRENT_DATE))
イ. MAX(DATEDIFF("d", 販売年月日, CURRENT_DATE))
ウ. MIN(DATEDIFF("d", 販売年月日, CURRENT_DATE))
エ. SUM(DATEDIFF("d", 販売年月日, CURRENT_DATE))

＜設問２＞　それぞれの上位 10 位以内の表を作成する次の SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。なお，設問１と同じ空欄には同じ字句が入る。また，各 TOP_10 表は作成済みである。

① 直近 1 ヶ月で販売金額の多い顧客を販売金額の多い方から 10 位まで抽出し,販売金額 TOP_10 表を作成する。なお,販売金額が同額の場合は,顧客 ID の昇順とする。

```
INSERT [ (1) ] 販売金額 TOP_10 表(顧客 ID, 販売金額)
  SELECT TOP 10 顧客 ID, 販売金額 FROM 直近 1 ヶ月販売金額表
  ORDER BY [ (6) ]
```

② 直近 1 ヶ月で販売回数の多い顧客を販売回数の多い方から 10 位まで抽出し,販売回数 TOP_10 表を作成する。なお，販売回数が同じ場合は，顧客 ID の昇順とする。

```
INSERT [ (1) ] 販売回数 TOP_10 表(顧客 ID, 販売回数)
  SELECT TOP 10 顧客 ID, 販売回数 FROM 直近 1 ヶ月販売回数表
  ORDER BY [ (7) ]
```

③ 最終販売日からの経過日数の短い顧客の経過日数の短い方から 10 位までの顧客を抽出し，経過日数 TOP_10 表を作成する。なお，経過日数が同じ場合は，顧客 ID の昇順とする。

```
INSERT [ (1) ] 経過日数 TOP_10 表(顧客 ID, 経過日数)
  SELECT TOP 10 顧客 ID, 経過日数 FROM 経過日数表
  ORDER BY [ (8) ]
```

(6) ～ (8) の解答群

ア. 経過日数, 顧客 ID　　イ. 顧客 ID, 経過日数
ウ. 顧客 ID, 販売回数 DESC　　エ. 顧客 ID, 販売金額 DESC
オ. 販売回数 DESC, 顧客 ID　　カ. 販売金額 DESC, 顧客 ID

＜設問３＞　優良顧客表を作成する次の SQL 文の［　　］に入れるべき適切な字句を解答群から選べ。

顧客の中から優良顧客を抽出する。優良顧客は，RFM 分析により判断する。ここでは，R(Recency：最後の購入日からの経過日数)を経過日数 TOP_10 表，F(Frequency：来店頻度)を販売回数_TOP10 表，M(Monetary:購入金額)を販売金額 TOP_10 表として，すべての表に含まれている顧客を抽出する。

```
SELECT * FROM 顧客表
 WHERE 顧客 ID  [ (9) ]
   (SELECT 経過日数 TOP_10 表.顧客 ID
      FROM (経過日数 TOP_10 表 [ (10) ] 販売回数 TOP_10 表
              ON 経過日数 TOP_10 表.顧客 ID = 販売回数 TOP_10 表.顧客 ID)
            [ (10) ] 販売金額 TOP_10 表
              ON 経過日数 TOP_10 表.顧客 ID = 販売金額 TOP_10 表.顧客 ID)
```

(9) の解答群

ア．EXISTS　　イ．IN

ウ．NOT EXISTS　　エ．NOT IN

(10) の解答群

ア．INNER JOIN　　イ．LEFT OUTER JOIN

ウ．RIGHT OUTER JOIN　　エ．UNION ALL

問題５　次の認証に関する記述を読み，設問に答えよ。

正当な利用者かどうかを確認する作業を認証と呼ぶ。重要な施設や部屋への入室時やネットワーク上のサーバに対するアクセス時など，様々な場面で必要となるセキュリティ対策の一つである。

＜設問１＞ 次の入室時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。

入室時の認証には，入口でパスワードを入力する方法や IC カードを利用して解錠させる方法がある。しかし，パスワードや IC カードは他人に盗まれて，入室される場合も起こり得る。そこで，正当な利用者の身体的特徴を利用して認証するのが［(1)］認証である。個人を特定できる身体的特徴としては，指紋を利用する指紋認証，手のひらや指先の血管のパターンを利用する［(2)］認証，眼球の黒目に現れるしわを利用する［(3)］認証などがある。

(1) の解答群

ア．相手　　イ．バイオメトリクス　　ウ．メッセージ

(2)，(3) の解答群

ア．顔　　イ．虹彩　　ウ．静脈　　エ．声紋

＜設問２＞ 次のアクセス管理に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ネットワーク上のサーバに対するアクセス管理の基本は，ユーザ ID とパスワードを使い正規のユーザであることを認証することである。同じパスワードを使い続けていると不正利用される確率も高くなり，重要なデータが攻撃されるリスクも増える。

そこで，ユーザとサーバ間で利用される対策の一つに［(4)］／［(5)］がある。ユーザはサーバにパスワード登録しておき，ユーザがサーバに対して認証要求を出すたびに，サーバはランダムに生成された数値列（［(4)］）を返信する。ユーザはこの数値列と本来のパスワードを組み合わせてハッシュ関数で演算した結果（［(5)］）をサーバに送る。サーバも先ほど返信した数値列とパスワードからユーザと同じハッシュ関数で演算しておき，ユーザから送られた演算結果と比較して認証する。

また，アクセスのたびに新たなパスワードを利用する［(6)］がある。［(6)］の一つに，初めに利用回数を決め一方向関数により利用回数分のパスワードを作成する方法がある。そして利用回数分使い終わった時点で改めて次の回数分のパスワードを作成する。

(4) ～ (6) の解答群

ア．コマンド　　イ．チャレンジ　　ウ．ライセンス
エ．リクエスト　　オ．レスポンス　　カ．ワンタイムパスワード

＜設問３＞　次のディジタル署名に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ディジタル署名は，公開鍵暗号方式を利用して送信者の正当性を保証するものである。このディジタル署名にメッセージダイジェストを利用することで，文書の改ざんの有無も合わせて証明できる。その仕組みを次に示す。

① 送信者は,送信文書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。

② メッセージダイジェストを［　(7)　］で暗号化し，ディジタル署名として送信文書に付加して送信する。

③ 受信者は受信した文書から,①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。

④ 受信したディジタル署名を［　(8)　］で復号したメッセージダイジェストと，③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文書が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。

(7)，(8) 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＞