文部科学省後援

情報システム試験

平成19年度前期 情報検定

＜実施　平成19年9月9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），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25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19年10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　次のプログラム設計に関する説明を読んで設問に答えよ。

Ｊ学園では，試験を行った後で学生に試験結果の成績票を配布している。このたび成績処理を行うためのプログラムを作成することにした。各科目担当の教員が採点結果をコンピュータに入力して，全ての科目の入力が完了してから学生用の成績票を出力する。

【試作プログラムの仕様】

・クラス数は３クラス（Ａ・Ｂ・Ｃクラス）で同一の授業内容である。
・人数は１クラス 30 人（欠員無し，出席番号は１番～30 番）である。
・科目数は英語・数学・国語・理科・社会の５科目である。
・各科目の担当教員が入力する内容は，科目・クラス毎に学生の得点のみである。（図１参照）
・成績票は各学生の５科目の平均点を算出して，平均点の高い順にクラス内順位を付加する。（図２参照）

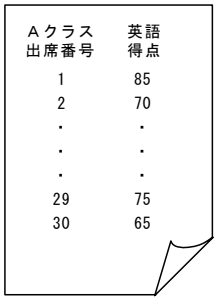


図１ 入力データ

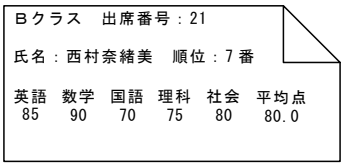


図２ 成績票（学生用）

業務のプロセス（処理過程）を明確にするために，DFD(Data Flow Diagram)を用いてコンテキストダイアグラムを作成した。

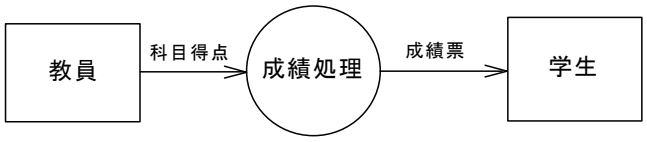


図３ コンテキストダイアグラム

＜設問１＞　次の DFD の説明文中の［　　］に入れるべき字句を解答群から選べ。

DFD では，データの流れ（フロー）を名前を持つ矢印で表現し，″□″（四角形）で［　(1)　］を表現し，″○″（円）で［　(2)　］を表現する。

(1)，(2) の解答群

ア．処理　　イ．源泉・吸収（外部）　　ウ．入力
エ．出力　　オ．変換

次に，図３の成績処理の詳細化を行うために，必要な機能を抽出した。

【抽出した機能】

・キーボードより入力した各科目の採点データを，成績ファイルに書き込む成績入力/保存機能。
・誤入力などのミスを発見した場合に行う成績訂正機能。
・成績ファイルから，学生配布用の成績票を作成する成績出力機能。

上記の各機能に基づくコンテキストダイアグラムの詳細化を行った。

なお，成績ファイルには，あらかじめ出席番号・氏名は記録されており，クラス別に３クラス分保存してある。

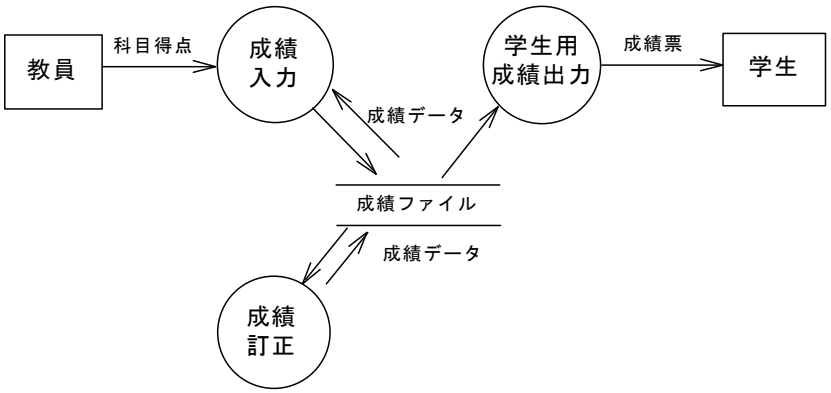
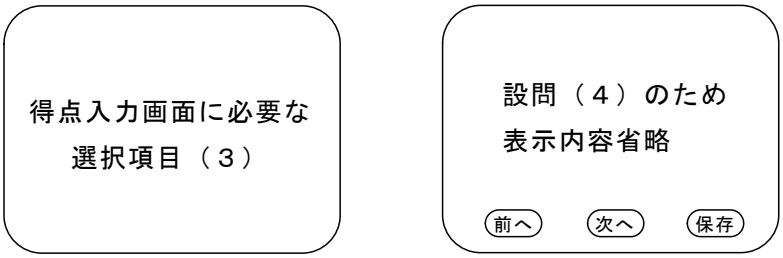


図４　詳細化したDFD

次に教員の入力画面（図５参照）を検討する。

図５①の問合せ画面で図１の入力データを教員が入力するために必要事項を選択させた後に,図５②の得点入力画面上で学生の出席番号に対応する得点だけを入力する。

得点入力画面は５人分を表示し,「次へ」「前へ」で表示の切り替えを行い,「保存」で得点入力を終了する。



①　問合せ画面　　②　得点入力画面

図５　入力画面の概要

＜設問２＞　次の入力画面の説明文に関する各問に答えよ。

(3) 図５①の問合せ画面に必要な選択項目として適切なものを解答群から選べ。

(3) の解答群

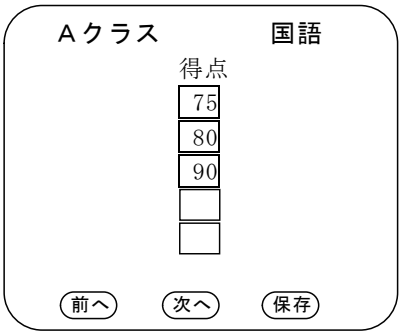
ア．クラス名　　イ．クラス名と出席番号

ウ．科目名　　エ．クラス名と科目名

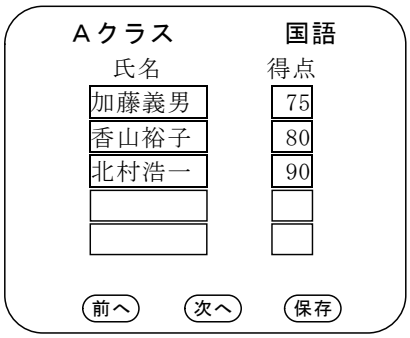
(4) 図５②の得点入力画面では，各科目の担当教員が成績の入力を行う。このとき，できるだけ担当教員の入力作業量と入力ミスを少なくするような配慮をする必要がある。画面のレイアウトとして最も適切なものを解答群から選べ。ただし，同姓同名はいないものとし，画面上の入力箇所は［　　］で示す。

(4) の解答群

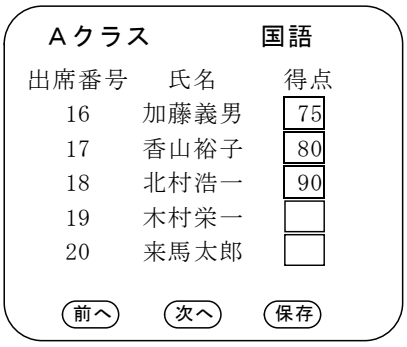
ア．得点だけを入力させる。



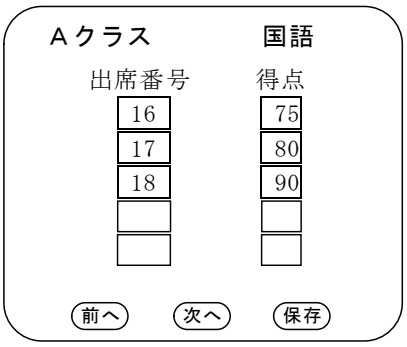
イ．氏名と得点をすべて入力させる。



ウ．出席番号と氏名を表示し，得点を入力させる。



エ．出席番号と得点を入力させる。



＜設問３＞　次の記述中の［　　］に入れるべき最も適切な字句を解答群から選べ。

次に，図４の学生用成績出力機能の詳細化を行うために，必要な機能を抽出した。

【学生用の成績出力機能の詳細化】

・成績出力対象のクラスを指定する機能。
・成績データの読込み機能。
・学生個人別の平均点計算機能。
・平均点の高い順にクラス順位をつける順位付け機能。
・出席番号順にクラスの学生全員の成績票を印刷する印刷機能。

図６に成績ファイルのイメージを示す。

出席番号	氏名	英語	数学	国語	理科	社会
1	青木 優子	８５	７０	６５	８３	７６
2	赤池 良男	６８	８０	７７	４５	６２

図６　成績ファイルの概要

学生用成績出力機能を詳細化したバブルチャートを図７に示す。このバブルチャートに STS 分割法を適用する。

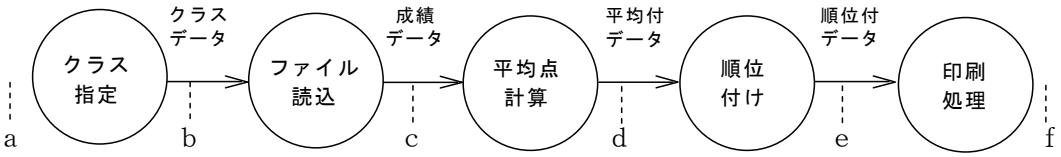


図７ 学生用成績出力機能のバブルチャート

STS 分割法では，データの流れに着目し，入力データがもはや入力データと呼べなくなる最大抽象入力点，出力データの形がはじめて見えるようになる最大抽象出力点を求め，それを基準にして，プログラムを源泉部分（入力処理），変換部分（データ処理），吸収部分（出力処理）の３つに分割していく技法である。

図７において，最大抽象入力点は［(5)］であり，最大抽象出力点は［(6)］である。

(5)，(6) の解答群

ア．a　　イ．b　　ウ．c　　エ．d　　オ．e　　カ．f

＜設問４＞　STS 分割の結果に基づき得られた次のモジュール構造図に関する［　　］に入れるべき適切な字句を解答群から選べ。解答は重複して選んでもよい。

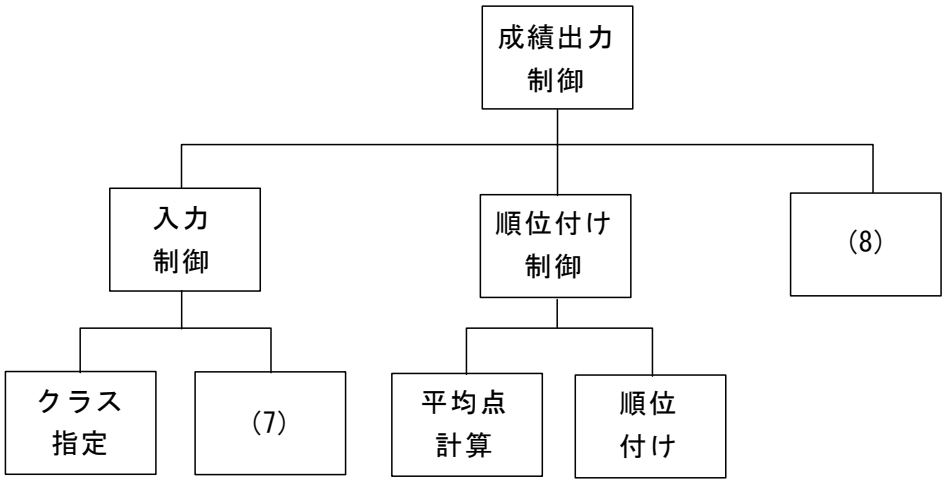


図８　モジュール構造図

(7)，(8) の解答群

ア．成績ファイル読込　　イ．出席番号入力　　ウ．成績票印刷
エ．成績ファイル保存　　オ．出席番号並べ替え

モジュールの独立性を示す尺度にモジュール強度とモジュール結合度がある。モジュール強度はモジュール内の命令同士の関連性の強さを表す概念であり，モジュール結合度はモジュール間の結合の度合いを表す概念である。

たとえば図８の平均点計算モジュールと順位付けモジュールを一つのモジュールにした場合，モジュール強度は［(9)］。

成績データをモジュール間で，図６に示したファイル概要の形式の２次元配列で受け渡しする場合，この２次元配列を大域変数として宣言すると外部結合となり，データ結合やスタンプ結合よりもモジュール結合度は［(10)］。

(9)，(10) の解答群

ア．強くなる　　イ．弱くなる　　ウ．強くも弱くもならない
エ．強くなるか弱くなるかどちらとも言えない

問題２　次のネットワークに関する設問に答えよ。

＜設問１＞　次の DNS の構造と動作に関する説明を読み，各問に答えよ。

インターネット上を流れるパケットは，その送り先を IP アドレスで指定している。しかし，Web での URL などではドメイン名を用いて指定することが一般的である。このドメイン名から IP アドレスに変換することを名前解決と呼び,そのために DNS が用いられる。これは，[a]分散型データベースの一種で，階層構造を持つ。最も上位のサーバをルートサーバと呼ぶ。これらのサーバを利用するクライアントのプログラムをリゾルバと呼ぶ。

ドメイン名は，インターネット全体で唯一となるようにユニーク性(一意性)を保証することが必要となる。そのために [b]ドメイン・ツリーと呼ばれる名前空間を構成している。頂点にある「.」が最上位のルートドメインで，ひとつ下に TLD (Top Level Domain)，その下に SLD (Second Level Domain)がある。

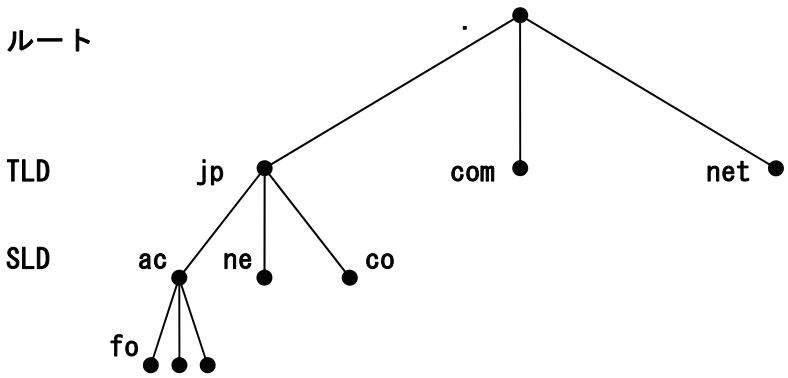


図１ ドメイン・ツリー

インターネットで用いられる www.fo.ac.jp のような表記を,FQDN (Fully Qualified Domain Name；完全修飾ドメイン名)と呼んでいる。FQDN の最後に本来はルートサーバを意味する「.」があるが，本問では省略されたものを用いる。なお，ホスト名を含めた www.fo.ac.jp をドメイン名と呼ぶこともある。

FQDN：　ホスト名 .ドメイン名　　(例: www.fo.ac.jp)

DNS の構造は「.」で表現されたルート(root)を頂点にして，下位の階層へと広がる階層構造である。それぞれの階層のノードには,「ネームサーバ」と呼ばれるデータベース機能が配置され,そのネームサーバに所属するホストのドメイン名と IP アドレスの対応関係を管理している。さらに，自分の下位に属するサブドメインの DNS サーバの IP アドレスも管理している。各ノードが管理対象とするデータ範囲を「ゾーン」と呼んでいる。サブドメインに所属するホストの情報などの管理は，サブドメインの DNS

サーバに権限委譲する。

図２は，DNS サーバ A の配下にあるクライアント PC から，www.fo.ac.jp を検索する動作を表す。

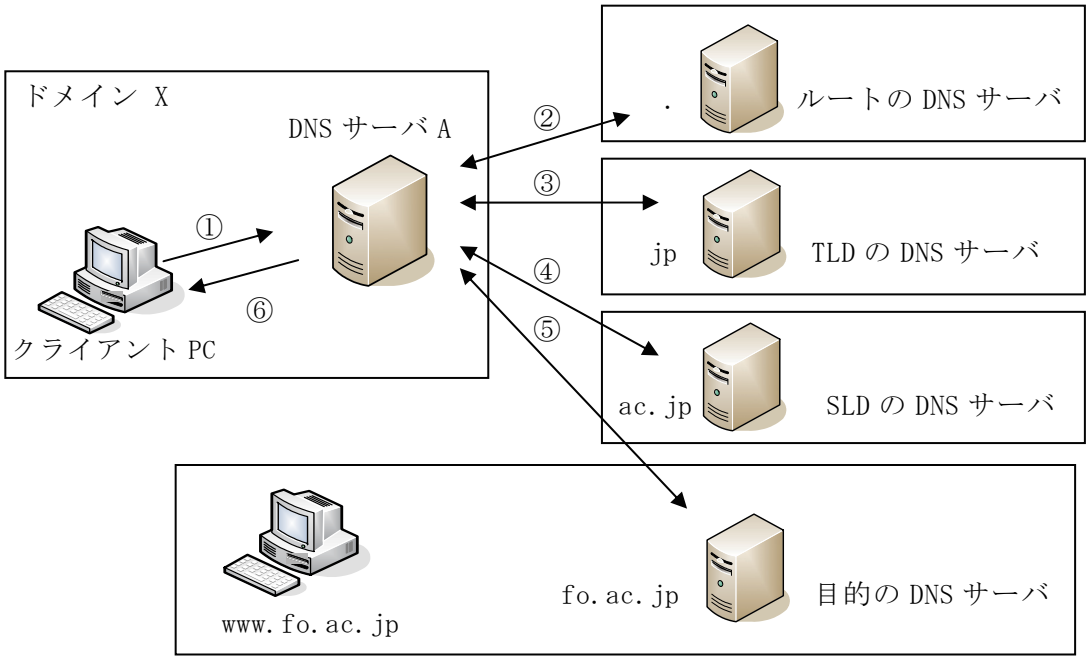


図２　www.fo.ac.jp の名前解決動作

名前解決の手順は，次のようになる。

① ドメイン X のクライアント PC は,DNS サーバ A に名前解決したい FQDN を送る。
② ドメイン X の DNS サーバ A は，ルートドメインを管理する DNS サーバに FQDN を送る。ルートサーバは，jp ドメインを管理する DNS サーバの IP アドレスを返す。
③ ドメイン X の DNS サーバ A は，jp ドメインを管理する DNS サーバに FQDN を送る。jp の DNS サーバは，ac.jp ドメインを管理する DNS サーバの IP アドレスを返す。
④ ドメイン X の DNS サーバ A は，ac.jp ドメインを管理する DNS サーバに FQDN を送る。 ac.jp の DNS サーバは，fo.ac.jp ドメインを管理する DNS サーバの IP アドレスを返す。
⑤ ドメイン X の DNS サーバ A は,fo.ac.jp ドメインを管理する DNS サーバに FQDN を送る。fo.ac.jp の DNS サーバは，自分のドメイン情報から www.fo.ac.jp の IP アドレスを返す。
⑥ ドメイン X の DNS サーバ A は，www.fo.ac.jp の IP アドレスをクライアント PC に返す。

(1) 下線部 a の「分散型データベース」を用いる理由として，不適切なものを解答群から選べ。

(1) の解答群

ア．個々のドメインで，そのゾーンに関する情報だけ管理すれば良いので，管理をドメインごとに独立させることができる。

イ．ひとつの DNS サーバが持つ情報の量を少なくすることができる。

ウ．ある DNS サーバが停止しても，その管理下以外の名前解決に影響を与えないので，信頼性が向上する。

エ．複数の DNS サーバにアクセスが分散することで，アクセス速度が向上し，アクセス回数が減少する。

(2) 下線部 b の「ドメイン・ツリー」に関する記述として，適切なものを解答群から選べ。

(2) の解答群

ア．サブドメインの下に別のドメインが追加されても，そのノード内でのユニーク性が保障されれば，全体のユニーク性が保障される。

イ．それぞれのドメインが，自分の領域と，その下位にあるサブドメインの領域にあるドメイン名を管理することで,全体のドメイン名を管理することができる。

ウ．ドメイン・ツリーは，ルートドメインがすべてのドメイン名を管理する時に用いているディレクトリ構造のことである。

エ．トップレベルドメイン(TLD)がドメイン･ツリーの最も上位になるドメインである。

(3) 名前解決では，DNS サーバに対する問合せを FQDN の後ろから行っている(例えば，．→ jp → ac → fo の順)。このような動作を行う理由として，適切なものを解答群から選べ。

(3) の解答群

ア．それぞれのネームサーバは,自分の上位のネームサーバが登録されているので,検索も，同様に，下位から上位へサーバを探していくためである。

イ．ルートサーバから始めて，順にそのサブドメインにあるネームサーバを検索するためである。

ウ．ドメイン・ツリーを用いて，名前のユニーク性を保証しているので，ツリーを下から検索するためである。

エ．FQDN では，TLD を左端に記述し，その右に続けて，SLD の順にピリオドで区切って記述しているためである。

(4) 図２の名前解決動作に関する記述として，適切なものを解答群から選べ。

(4) の解答群

ア．DNS サーバ A は，クライアント PC に対してはサーバとして動作しているが，他の DNS サーバに対してはリゾルバとして動作している。

イ．DNS サーバ A は，問合せに対して，自分自身が管理しているゾーン情報にのみ返答し，ほかのサーバへ問合せは行わない。

ウ．すべての DNS サーバは，互いに協調して，対等の関係の水平分散型データベースとして動作している。

エ．すべての DNS サーバは，名前解決の問合せを受けると，自分の管理下にある DNS サーバに対して，名前解決の問合せを再帰的に行う。

このシステムでは，ルートサーバや TLD のサーバなどへアクセスが集中することになる。そこで，各 DNS サーバは取得した IP アドレスに関する情報をキャッシュすることで，アクセスを減少させている。例えば，図２の②の問い合わせ結果として，jp ドメインを管理する DNS サーバの IP アドレスがキャッシュされる。なお，ルートサーバは全世界で十数台あり，日本にも用意されている。ルートサーバの IP アドレスはあらかじめ，DNS サーバに設定されている。

(5) ドメイン X のクライアント PC による www.fo.ac.jp の IP アドレス問い合わせのために，DNS サーバ A が行う他の DNS サーバへの問い合わせの回数として，適切なものを解答群から選べ。ただし，キャッシュ機能は考慮しない。

(5) の解答群

ア．1　　イ．2　　ウ．3　　エ．4

(6) キャッシュ機能が有効な場合，ドメイン X のクライアント PC による www.fo.ac.jp の IP アドレス問い合わせのために，DNS サーバ A が行う他の DNS サーバへの問い合わせの回数として，適切なものを解答群から選べ。なお，DNS サーバ A は，すでに www.aa.ac.jp の問合せを行っているので，これに関する IP アドレスはキャッシュされているものとする。

(6) の解答群

ア．1　　イ．2　　ウ．3　　エ．4

＜設問２＞　次の DNS サーバの信頼性に関する説明を読み，各問に答えよ。

DNS サーバの障害対策として，同じ内容のサーバを 2 台以上設置する慣行になっている。追加したサーバをセカンダリ DNS サーバと呼び，もとのサーバをプライマリ DNS サーバと呼んでいる。このように，多重構成にすることで，名前解決の信頼性を向上させている。

セカンダリ DNS サーバの設定は，プライマリ DNS サーバの設定と一致することが必要である。この 2 台のサーバ間の同期を取るために，ゾーン転送が用いられる。セカンダリ DNS サーバは，定期的にプライマリ DNS サーバに接続し，ゾーン転送により，そのゾーン情報のコピーを取得している。この機能により，DNS サーバの管理者は，プライマリ DNS サーバにゾーン情報を設定するだけで，両者を管理することができる。なお，名前解決動作を行う時にプライマリ DNS サーバとセカンダリ DNS サーバの区別はない。

(7) 図２のネットワーク構成において，DNS サーバ A が使用不能になった場合に発生するクライアント PC への影響として，適切なものを解答群から選べ。

(7) の解答群

ア．IP アドレスで指定したアクセスができなくなる。
イ．ネットワークへのアクセスがまったくできなくなる。
ウ．ドメイン名を用いたアクセスができなくなる。
エ．自分のドメイン内へのアクセスは可能だか，ドメイン外へのアクセスができなくなる。

(8) プライマリ DNS サーバとセカンダリ DNS サーバに関する説明として，最も適切なものを解答群から選べ。

(8) の解答群

ア．クライアントのリゾルバにおける DNS サーバに関する設定で，プライマリ DNS サーバとセカンダリ DNS サーバの IP アドレスを設定する。
イ．セカンダリ DNS サーバの持つ情報を，プライマリ DNS サーバにゾーン転送して，両者のゾーン情報を同期させる。
ウ．ゾーン転送を効率化させるために，プライマリ DNS サーバとセカンダリ DNS サーバを同一マシン上で稼動させることが好ましい。
エ．プライマリ DNS サーバに障害が発生したときに，名前解決ができなくなる。

＜設問３＞　次のドメイン fo.ac.jp の DNS サーバの設定に関する記述の［　　］に入れるべき適切な字句を解答群から選べ。

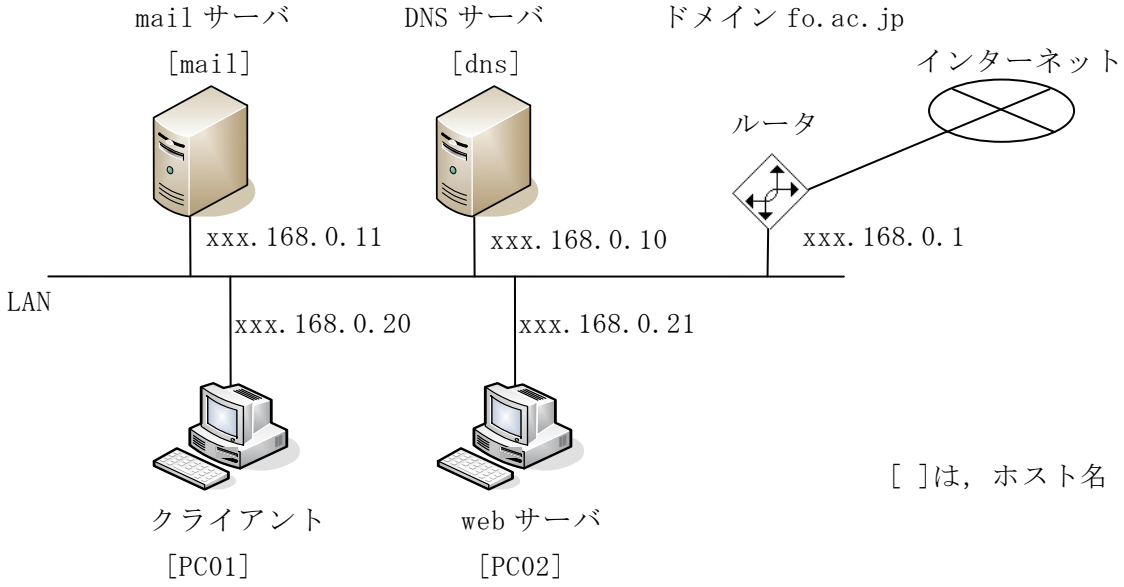


図３　ドメイン fo.ac.jp のネットワーク構成

各ノードが管理対象とするデータ範囲であるゾーンに登録されるレコードには，ホスト名から IP アドレスを得るための A レコードなどがあり，主なものを表１に示す。このレコードを用いて，図３の DNS サーバ［dns］を設定する例を表２に示す。

表１　主なレコード一覧表

レコードの種別	意味
A	ホスト名．ドメイン名に対する IP アドレスを指定する
NS	ドメインの DNS サーバ名を指定する
MX	ドメインのメールサーバ名を指定する
CNAME	ホスト名のエイリアス（別名）を指定する

【レコードの書式】

〈ホスト名．ドメイン名〉.	IN A	〈IP アドレス〉
〈ドメイン名〉.	IN NS	〈ネームサーバ名．ドメイン名〉.
〈ドメイン名〉.	IN MX　優先度	〈メールサーバ名．ドメイン名〉.
〈定義する別名〉.	IN CNAME	〈定義されたホスト名．ドメイン名〉.

表２　DNS サーバ［dns］の設定内容

fo.ac.jp.	IN	NS	(9)
fo.ac.jp.	IN	MX 10	(10)
dns.fo.ac.jp.	IN	A	xxx.168.0.10
mail.fo.ac.jp.	IN	A	(11)
PC01.fo.ac.jp.	IN	A	xxx.168.0.20
PC02.fo.ac.jp.	IN	(12)	xxx.168.0.21
www.fo.ac.jp.	IN	(13)	PC02.fo.ac.jp.

(9) ～ (13) の解答群

ア．A　　イ．NS　　ウ．MX　　エ．CNAME

オ．www　　カ．dns.fo.ac.jp.　　キ．mail.fo.ac.jp.

ク．xxx.168.0.10　　ケ．xxx.168.0.11　　コ．xxx.168.0.21

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３　次の情報セキュリティに関する設問に答えよ。

＜設問１＞　情報セキュリティの法規・制度に関する各問に答えよ。

(1) アクセス権限のない者のコンピュータ資源へのアクセスを禁止する「不正アクセス禁止法」において，処罰の対象となるものを解答群から選べ。

(1) の解答群

ア．ウイルス対策ソフトを稼動せずに，コンピュータを使用する。
イ．重要な個人情報を，暗号化されていないメールで送信する。
ウ．友人が購入したソフトを，自分のコンピュータにインストールする。
エ．友人のパスワードを無断で使用して，コンピュータにログオンする。

(2) 個人情報の不正な利用や流用を防止する「個人情報保護法」の説明として，適切なものを解答群から選べ。

(2) の解答群

ア．20 人前後の友人のメールアドレスを，データベースとしてコンピュータに保存すると，この法律の適用対象になる。
イ．ディジタルデータ以外の個人情報は，この法律の適用対象にはならない。
ウ．個人情報をコンピュータに保存するときは，必ず暗号化を行なわなければならない。
エ．収集した個人情報は，収集した目的の範囲内で使用しなければならない。

(3) ISMS 適合性評価制度は，企業など組織体の情報セキュリティに対する取り組みを第三者機関が評価して認定する制度である。ISMS の認定を受けた組織は，ISMS の運用状況を定期的に評価し，見直しや改善を行なう「PDCA サイクル」（Plan；計画，Do；実行，Check；評価，Action；改善)を実施する。PDCA サイクルの「Plan」の説明として，適切なものを解答群から選べ。

(3) の解答群

ア．企業などの組織体が全社的に取組むセキュリティポリシーを策定する。
イ．組織が運用している情報セキュリティシステムを評価・認定する。
ウ．組織の情報セキュリティシステムを構築・運用する。
エ．組織の中で発生した情報セキュリティに関する問題を分析する。

＜設問２＞　Webサイトのセキュリティに関する各問に答えよ。

インターネットの普及した今日では，Web サイトは単に情報発信をするだけではなく，利用者との間でさまざまな情報のやり取りが行なわれる。インターネットショッピングでは,買い物に必要な利用者の個人情報がWebサイトに送信されることになる。この個人情報を不正に入手するために，利用者を偽装のショッピングサイトに誘導して個人情報を入力させるという,悪質なWebサイトも少なからず存在する。SSL(Secure Socket Layer)と呼ばれるセキュリティプロトコルを用いることで,利用者(ブラウザ)とWebサイトとの間はセキュリティで保護された通信が行なわれる。インターネットで個人情報を入力するときは，SSL が適用されていることを，常に確認する必要がある。

(4) 利用者を偽装のショッピングサイトに誘導する手口に該当するものを解答群から選べ。

(4) の解答群

ア．DHCPサーバを攻撃して，割り当てるIPアドレスの範囲を変更する。
イ．DNSサーバを攻撃して，該当するIPアドレスを書き換える。
ウ．利用者のウイルス対策ソフトを攻撃して，ウイルス検出機能を無効にする。
エ．利用者のファイアウォールを攻撃して，ファイアウォール機能を無効にする。

(5) セキュリティプロトコル SSL によって，「Web サイトの認証」と「通信データの暗号化」が行なわれる。「Web サイトの認証」によって保証されることの説明として，適切なものを解答群から選べ。

(5) の解答群

ア．Webサイトに接続しているユーザが，接続権限を持っていること。
イ．接続先のWebサイトがウィルスに感染していないこと。
ウ．接続先のWebサイトが信頼できるWebサイトであること。
エ．接続先のWebサイトと通信するメッセージが盗聴されないこと。

(6) ブラウザに表示されているページが，セキュリティプロトコル SSL で保護されているとき，ブラウザに表示されるURLとして適切なものを解答群から選べ。

(6) の解答群

ア．ftp://www.website.co.jp
イ．http://www.website.co.jp
ウ．https://www.website.co.jp
エ．ssl://www.website.co.jp

(7) 多くのショッピングサイトでは，個人情報を入力するページにSSLを適用し，それ以外の商品紹介ページなどではSSLを適用していない。この理由として適切なものを解答群から選べ。

(7) の解答群

ア．SSLを適用するとオーバヘッドが増加して応答時間に影響が出るから。
イ．SSLを適用するページはウィルスチェックが行なわれないから。
ウ．画像データにSSLを適用することができないから。
エ．複数のページにまたがってSSLを適用することができないから。

＜設問３＞　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。

我々の日常生活では，役所が発行する戸籍抄本や印鑑証明がその人の身元を保証してくれる。インターネット上では，認証局（Certification Authority：CA）が発行する「ディジタル証明書」が，その所有者の身元を保証する。なお，ディジタル証明書は「公開かぎ証明書」あるいは「サーバ証明書」とも呼ばれる。

Web サイト等を運用する組織は，必要な書類を揃えて認証局に申請を行なう。認証局は，所定の審査を行って申請者の身元を確認してから，申請者のディジタル証明書を発行する。このディジタル証明書には，申請者の「公開かぎ」の情報が含まれている。このように，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［　(8)　］という。

ディジタル証明書には，申請者のURLや公開かぎの情報が含まれている（図１参照）。そして，このディジタル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」が付加される。認証局のディジタル署名は，ディジタル証明書が正規の手続きを経て作成されたもので，決して偽造されたものではないことを保証する，重要な役割りを担っている。

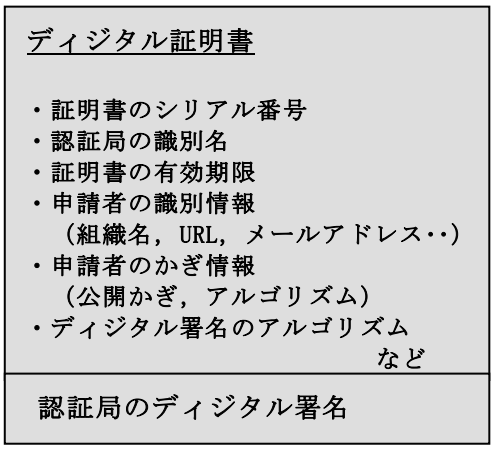


図１　ディジタル証明書の構成

認証局のディジタル署名は，ハッシュ関数と公開かぎ暗号方式の技術を用いて作成する。ハッシュ関数は，元のメッセージから特定のビット列を生成する関数で，元のメッセージが１文字でも変更されると，まったく異なるビット列を生成する。生成されたビット列のことを「ハッシュ値」または「メッセージダイジェスト」という。

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実現する。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。

認証局のディジタル署名は，申請者のディジタル証明書をハッシュ関数に入力してハッシュ値（ビット列）を生成し，それを［　(9)　］で暗号化することによって作成する。

ブラウザからWebサイトに接続要求が送られると，次の手順に従ってWebサイトの認証が行なわれる(図２参照)。

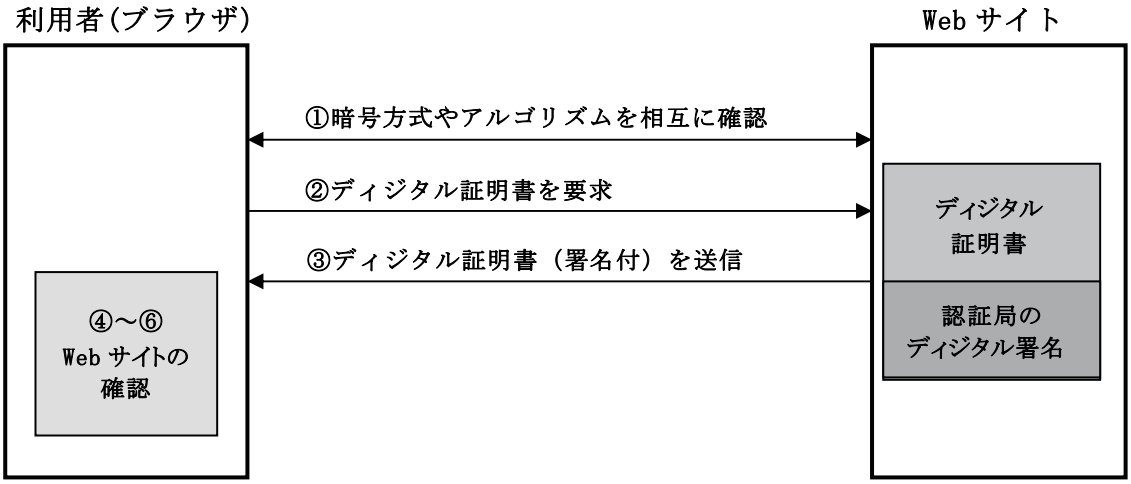


図２　Web サイトの認証手順

① ブラウザとWebサイトで，暗号方式やアルゴリズムを相互に確認する。
② ブラウザはWebサイトに，ディジタル証明書の送信を要求する。
③ Webサイトはディジタル証明書（認証局のディジタル署名付き）をブラウザに送信する。
④ ブラウザは受け取ったディジタル証明書をハッシュ関数に入力してハッシュ値 Aを得る。
⑤ ブラウザは受け取った認証局のディジタル署名を，［　(10)　］で復号してハッシュ値Bを得る。
⑥ ハッシュ値Aとハッシュ値Bの値を比較する。値が一致しないときは,［　(11)　］ので，接続しているWebサイトは信頼できないと判定する。

(8) の解答群

ア．VPN　　イ．公開かぎ基盤（PKI）
ウ．チャレンジレスポンス認証　　エ．ワンタイムパスワード

(9)，(10) の解答群

ア．Web サイトの公開かぎ　　イ．Web サイトの秘密かぎ
ウ．認証局の公開かぎ　　エ．認証局の秘密かぎ
オ．利用者の公開かぎ　　カ．利用者の秘密かぎ

(11) の解答群

ア．Web サイトにディジタル証明書がインストールされていない
イ．ディジタル証明書が暗号化されていない
ウ．ディジタル証明書が正規の手続きを経て作成されていない
エ．ブラウザが SSL プロトコルに対応していない

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４　次のデータベース設計に関する設問に答えよ。

システム設計時，データベースの設計図として ER 図（ERD）を利用する。ER 図では DBMS に依存しない標準的な呼び方として，実体（テーブル）をエンティティ，項目を属性，行（レコード）をオカレンスと表現する。オカレンスを特定するために用いる単一の属性や複数の属性の組合せを主キー(下線で表現)と呼ぶ。また，他エンティティで主キーとなっている単一の属性や複数の属性の組合せを外部キー(FK)として利用する。ここでは，図１に示す正規化された表の ER 図について考える。

学科表

学科コード	学科名

学生表

学生番号	学生氏名	学科コード(FK)

図１　正規化された表

図２の ER 図において，学科エンティティの主キーである学科コードと，学生エンティティの外部キーである学科コードによって関連が表現される。学生エンティティの外部キーである学科コードの値が決定すると，関連する学科エンティティの主キーである学科コードが関連付けられ，学科名が一意に決まることがわかる。

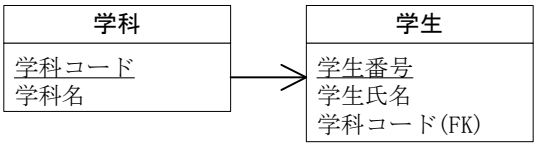


図２　学科・学生 ER 図

学科エンティティで学科コードはユニーク(唯一)であるのに対し，学生エンティティには同じ学科コードが複数存在する。この場合，「学科エンティティと学生エンティティは１対多の関連である」と表現される。エンティティ間は「1 対 1」，「1 対多」，「多対多」の３種類の関連があり，これを多重度(カーディナリティ)と呼び，ここでは図３のように表現する。

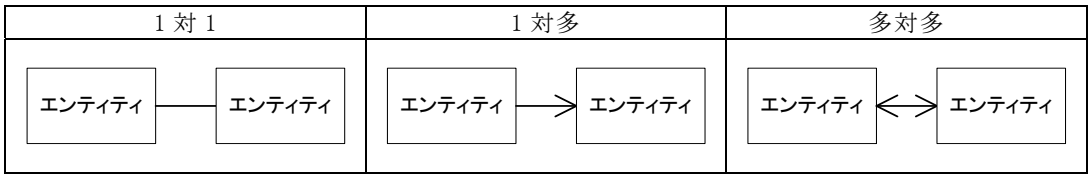


図３　カーディナリティの種類

＜設問１＞　次の［　　］に入れるべき最も適切な字句を解答群より選べ。

図２の ER 図の学生エンティティは，学生番号が主キーであるため，［　(1)　］。もしも，学科ごとに学生へ１番から連続した学生番号を付与したい場合には，学科を特定した後，学生個人を特定する必要がある。このときには，［　(2)　］ことで解決することができる。

(1) の解答群

ア．学生番号が未入力であっても問題は無い
イ．複数の学生に同じ学生番号を与えることはできない
ウ．異なる学科の学生に同じ学生番号を与えることができる
エ．データ型は数値型でなければならない

(2) の解答群

ア．氏名を主キーとする
イ．学生番号と氏名の複合項目を主キーとする
ウ．氏名と学科コードの複合項目を主キーとする
エ．学生番号と学科コードの複合項目を主キーとする

＜設問２＞　次の拡張した ER 図に関する各問に答えよ。

(3) 図４の ER 図の説明として誤っているものを解答群より選べ。なお，学生は１つの学科に必ず所属するものとする。

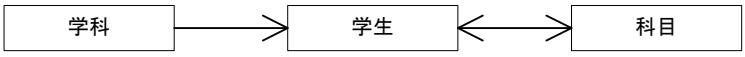


図４　拡張した ER 図

(3) の解答群

ア．同じ学科の学生は必ず同じ科目を履修する。
イ．同じ学科の学生は異なる科目を履修することもある。
ウ．学生は複数の科目を履修する。
エ．科目エンティティ，または学生エンティティを正規化する必要がある。

(4) 図４の ER 図のままでは，データベースの実装に不適切である。次の条件を満たす教員エンティティを追加すると同時に問題点を解決したい。教員エンティティとの関係として適切な ER 図を解答群より選べ。

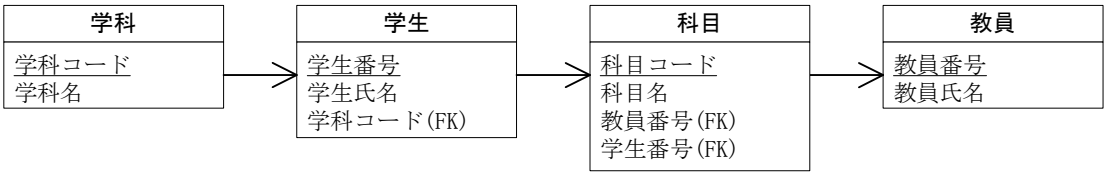
条件

① １つの科目は一人の教員が担当し，途中で科目を担当する教員が変更されることはない。
例） 国語 北海先生，数学 宮崎先生，英語 千葉先生，古文 北海先生

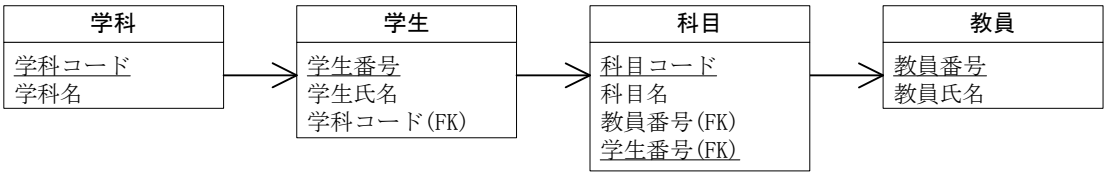
② 一人の教員が複数の科目を担当することもある。
例） 北海先生の担当科目：国語，古文

(4) の解答群

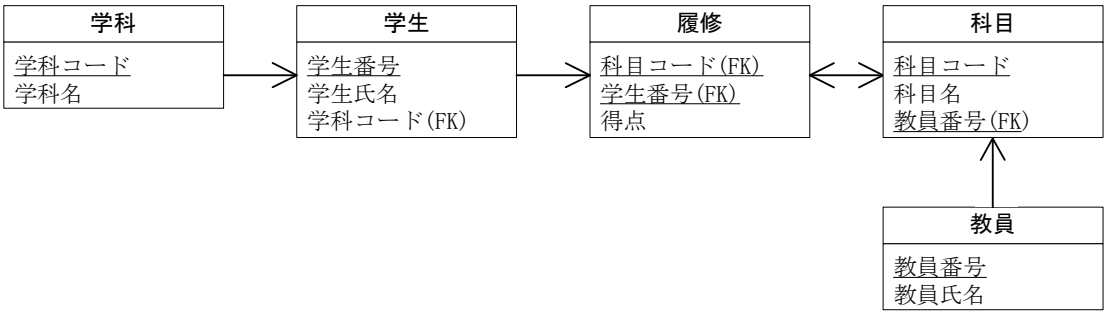
ア.



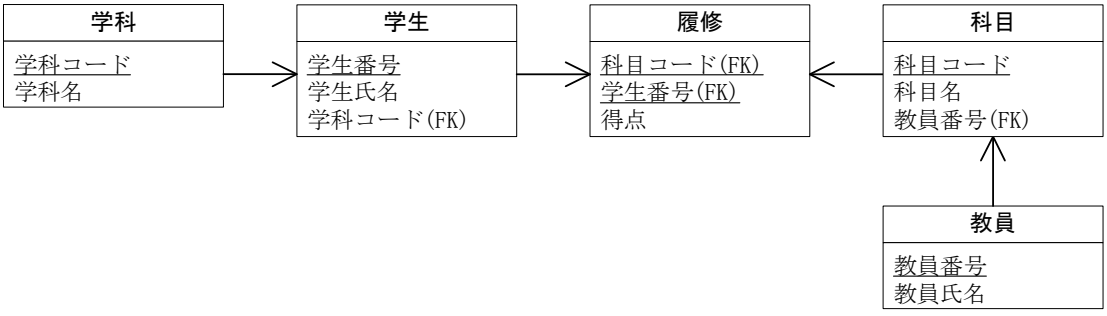
イ.



ウ.



エ.



＜設問３＞　①～⑤の SQL 文によって作成された各表を利用する，⑥～⑨の SELECT 文中の［　　］に入れるべき適切な字句を解答群より選べ。

テーブルを作成する SQL

① CREATE TABLE 学科表
(学科コード CHAR(2) NOT NULL,
学科名 CHAR(10),
PRIMARY KEY(学科コード))

② CREATE TABLE 学生表
(学生番号 CHAR(6) NOT NULL,
学生氏名 CHAR(10),
学科コード CHAR(2),
PRIMARY KEY(学生番号),
FOREIGN KEY(学科コード)
REFERENCES 学科表)

③ CREATE TABLE 教員表
(教員番号 CHAR(4) NOT NULL,
教員氏名 CHAR(10),
PRIMARY KEY(教員番号))

④ CREATE TABLE 履修表
(科目コード CHAR(8) NOT NULL,
学生番号 CHAR(6) NOT NULL,
得点 DEC(3),
PRIMARY KEY(科目コード,学生番号),
FOREIGN KEY(科目コード)
REFERENCES 科目表,
FOREIGN KEY(学生番号)
REFERENCES 学生表,
CHECK (得点 BETWEEN 0 AND 100))

⑤ CREATE TABLE 科目表
(科目コード CHAR(8) NOT NULL,
科目名 CHAR(10),
教員番号 CHAR(4),
PRIMARY KEY(科目コード),
FOREIGN KEY(教員番号)
REFERENCES 教員表)

⑥ 科目別の受講者一覧を科目コード順に表示する。

表示項目

科目コード	科目名	教員番号	教員氏名	学生番号	学生氏名	得点

```
SELECT A.科目コード,B.科目名,B.教員番号,C.教員氏名,A.学生番号,
       D.学生氏名,A.得点
  FROM 履修表 A,科目表 B,教員表 C,学生表 D
  WHERE
      A.科目コード = [ (5) ]
      AND B.教員番号 = C.教員番号
      AND [ (6) ] = D.学生番号
  ORDER BY A.科目コード
```

(5)，(6) の解答群

ア．A.科目コード　イ．B.科目コード　ウ．B.教員番号　エ．C.教員番号
オ．A.学生番号　カ．D.学生番号

⑦ 科目別に受講者人数を表示する。

表示項目

科目コード	受講者数

```
SELECT 科目コード, [ (7) ] AS 受講者数
    FROM 履修表
    [ (8) ] 科目コード
```

⑧ 科目別に得点の最高点と最低点を表示する。

表示項目

科目コード	最高点	最低点

```
SELECT 科目コード, [ (9) ] AS 最高点, [ (10) ] AS 最低点
    FROM 履修表
    [ (8) ] 科目コード
```

⑨ 受講者数が 20 名を超える科目を表示する。

表示項目

科目コード	人数

```
SELECT 科目コード,COUNT(*) AS 人数
    FROM 履修表
    GROUP BY 科目コード
    [ (11) ] COUNT(*) > 20
```

(7) ～ (11) の解答群

ア．AVG(得点)　イ．COUNT(*)　ウ．GROUP BY　エ．HAVING
オ．MAX(得点)　カ．MIN(得点)　キ．ORDER BY　ク．WHERE