問３　RDBMS のセキュリティに関する次の記述を読んで，設問 1～3 に答えよ。

B 社は，個人顧客を対象にした保険会社である。B 社では，顧客の個人情報の保護を強化するために，営業支援システムにおけるセキュリティに関する設計を見直すことにした。情報システム部の F さんがその見直しを担当した。

〔RDBMS のビュー及びセキュリティに関する主な仕様〕

(1) 実テーブル（以下，テーブルという）又はビューのアクセス権限（SELECT，INSERT，UPDATE 及び DELETE の各権限）をもつユーザは，テーブル又はビューにアクセスすることができる。

(2) ビューにアクセスする場合，そのビューが参照するテーブル又は別のビューのアクセス権限は不要である。

(3) テーブル又はビューのアクセス権限は，ユーザ ID，ロールに付与される。

(4) ロールは，ユーザ ID に付与され，別のロールにも付与されることがある。

〔営業部の組織・業務の概要〕

営業部の組織・業務の概要は次のとおりである。組織の一部を図 1 に示す。

(1) 営業部及び営業課は，部門番号で識別される。

(2) 社員は，社員番号で識別される。社員には，営業支援システムにログインするためのユーザ ID（社員番号を使用）が付与されている。

(3) 個人顧客（以下，顧客という）は，顧客番号で識別される。1 人の顧客は，一つの営業課によって担当される。

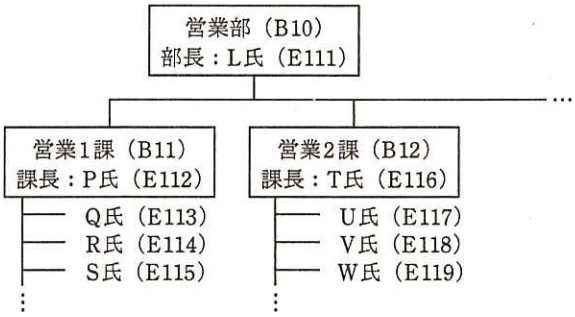
(4) 課長は，部下社員から成る少人数の営業チーム（以下，チームという）を複数編成する。経験豊かな社員については，複数チームに参加させることがある。

(5) チームは，顧客を訪問して面談し，保険に関わる様々な業務を行う。

(6) 各チームは，複数顧客を担当する。同じ顧客を複数チームが担当することはない。

(7) 課長は，随時，チーム編成を変える。チームに編成される社員が変わったり，チームから離れた社員が，また同じチームに戻ったりすることがある。

なお，チーム編成は，営業支援システムによって管理されていない。



注記　部門名の後ろのカッコ内は部門番号を表す。
　　社員名の後ろのカッコ内は社員番号を表す。

図１　営業部の組織（一部）

〔営業支援システムの概要〕

1. 主なテーブルの構造

営業支援システムで使用される主なテーブルの構造を図２に示す。

部門（部門番号，部門名，部門長社員番号，上位部門番号，所在地，…）
社員（社員番号，所属部門番号，社員名，電話番号，メールアドレス，FAX 番号）
顧客（顧客番号，担当部門番号，顧客名，生年月日，住所，電話番号，性別，…）
訪問予定（顧客番号，社員番号，訪問予定日，訪問予定時刻，訪問予定時間，訪問目的）
訪問実績（顧客番号，社員番号，訪問実施日，訪問開始時刻，訪問終了時刻，訪問結果）

図２　主なテーブルの構造（一部省略）

2. セキュリティ要件

B 社での顧客の個人情報（以下，個人情報という）とは，顧客名，生年月日，その他の記述などによって特定の個人を識別することができるものをいう。セキュリティに関する設計見直し後の個人情報に関するセキュリティ要件は，次の①～④のとおりである。

① 営業課の社員は，その課が担当する顧客の個人情報にアクセスできる。

② 部門長は，部下がアクセスできる全ての情報にアクセスできる。

③ 個人情報が格納されているテーブルを隠蔽するために，社員にはビューを使わせ，テーブルには直接アクセスさせない。

④ 個人情報にアクセスする必要がなくなった社員については，そのことを反映するためのアクセス制限を直ちに実施する。

3. 操作及び処理の概要

社員が自分のユーザ ID を指定してログインした営業支援システムに対する操作，及び営業支援システムによる処理の概要は，次のとおりである。

(1) 社員は，顧客訪問の前に予定を登録し，予定の変更は，その都度，反映する。予定なしに顧客訪問することはない。

(2) 社員は，予定日に顧客訪問を実施後，その実績を登録する。

(3) 社員は，画面上でアクセスを許可されたテーブル名又はビュー名の一覧から一つを選び，選択・集計条件及び結果行の並び順を指定する。

(4) 営業支援システムは，(3)の指定に基づき，実行可能な SQL 文を動的に組み立てて実行し，その実行結果を画面に出力する。

〔ビュー及びロールの設計〕

F さんは，個人情報を含む営業課別ビューのうち，営業 1 課及び営業 2 課のビューを，表 1 の SQL1 及び SQL2 に示すように設計した。

表 1　営業 1 課及び営業 2 課のビューの定義

SQL	SQL の構文
SQL1	CREATE VIEW 営業 1 課ビュー AS SELECT 顧客番号，顧客名，生年月日，住所，電話番号，性別 FROM 顧客 WHERE 担当部門番号 = 'B11'
SQL2	CREATE VIEW 営業 2 課ビュー AS [redacted]

注記　網掛け部分は表示していない。

F さんは，ビューを用いることを前提に，次のようにロールを設計し，運用することに決めた。営業課別ビューのアクセス権限をロールに付与する手順を，表 2 に示す。

(1) 部門番号をロール名として，ロールを定義する。

(2) 営業課別ビューのアクセス権限をロールに付与する。

(3) ロールの付与・剥奪については，課長が 1 営業日前までにデータベース管理者（以下，DBA という）に依頼する。DBA は，課長からの依頼に基づいて，ロールの付与・剥奪を RDBMS に対して実施する。

表2　営業課別ビューのアクセス権限をロールに付与する手順（未完成）

SQL	SQL の構文
ア	GRANT ROLE [a], [b] TO [c] ;
イ	GRANT ROLE B10 TO E111 ;
ウ	GRANT ROLE B11 TO E112, E113, E114, E115 ;
エ	GRANT ROLE B12 TO E116, E117, E118, E119 ;
オ	CREATE ROLE B10 ;
カ	CREATE ROLE B11 ;
キ	CREATE ROLE B12 ;
ク	GRANT SELECT ON 営業1課ビュー TO [a] ;
ケ	GRANT SELECT ON 営業2課ビュー TO [b] ;

注記　セミコロンは，SQL 文の終端を示す。
　　ここで示した部門番号及び社員番号は，図1に示したものに限っている。

〔ビューの設計変更〕

F さんが，設計見直し前の営業支援システムの利用状況を分析したところ，動的に組み立てて実行された SQL 文の中に，“顧客”テーブルに直接アクセスする SQL 文，及び複雑でかつ実行回数が多い SQL 文があった。前者の例を照会 1 に，後者の例を照会 2 に示す。

照会 1　社員が過去に登録した訪問予定のうち，その社員が予定日に訪問しなかった顧客の顧客番号，顧客名，社員番号及び訪問予定日を出力する（表 3 の SQL3 を参照）。

照会 2　年初からの訪問回数が N 回以上の社員について，社員番号，社員名，訪問回数を出力する。ここで，N は実行時に与えられ，SQL 文の動的パラメタの？に設定される（表 3 の SQL4 を参照）。

F さんは，照会 1 についてはセキュリティ要件③を満たすために，照会 2 については SQL 文を簡単にするために，それぞれビューを使うことにした。

表3　営業支援システムで使用する主なSQLの構文（未完成）

SQL	SQLの構文
SQL3	SELECT K.顧客番号, K.顧客名, HY.社員番号, HY.訪問予定日 FROM 顧客 K [d] 訪問予定 HY ON K.顧客番号 = HY.顧客番号 [e] 訪問実績 HJ ON HY.顧客番号 = HJ.顧客番号 AND HY.社員番号 = HJ.社員番号 AND HY.訪問予定日 = HJ.訪問実施日 WHERE HJ.訪問実施日 IS NULL
SQL4	SELECT S.社員番号, S.社員名, COUNT(*) 訪問回数 FROM 社員 S INNER JOIN 訪問実績 HJ ON S.社員番号 = HJ.社員番号 WHERE HJ.訪問実施日 >= ISODATE('2016-01-01') GROUP BY S.社員番号, S.社員名 HAVING COUNT(*) >= ?
SQL5	SELECT 社員番号, 社員名, 訪問回数 FROM 社員別訪問回数ビュー WHERE

注記　ISODATE関数は，日付を表す文字列をDATE型に変換するユーザ定義関数とする。

〔セキュリティ要件の強化〕

営業支援システムのセキュリティを更に強化するために，セキュリティ要件①が，“チームの社員は，当該チームが担当する顧客の個人情報にアクセスできる。”に変更された。F さんは，営業課別のロールをチーム別のロールに変更するという対応（対応案A）も考えたが，次のような対応（対応案B）を採用することにした。

(1) 営業支援システムに，新たに“チームメンバ”テーブルを追加する。当該テーブルへのアクセス権限（DELETE 権限以外）を課長に与え，課長が次のような操作を行える機能を追加する。ただし，操作は各営業課内に限られるものとする。

(a) 営業課内で一意なチーム番号を付与する。

(b) 営業課内のチームの社員ごとに，担当開始日及び担当終了日を設定した行を登録する。担当終了日が未定の場合は，NULLを設定する。

(c) 担当開始日の当日又は前日までに，行を登録する。

(d) 担当開始日列又は担当終了日列を，いつでも変更することができる。

(e) 過去にどの社員がどのチームのメンバだったかを調べることができる。

(2) “顧客”テーブルにチーム番号列を追加し，営業課別だった表1のSQL1及びSQL2を，営業課共通にするために，表4のSQL6のように変更する。

表4　セキュリティ要件の強化後のビューの定義

SQL	SQL の構文
SQL6	CREATE VIEW 営業課ビュー AS SELECT 顧客番号, 顧客名, 生年月日, 住所, 電話番号, 性別 FROM 顧客 K INNER JOIN チームメンバ T ON K.担当部門番号 = T.部門番号 AND K.チーム番号 = T.チーム番号 WHERE T.社員番号 = CURRENT_USER AND T.担当開始日 <= CURRENT_DATE AND (T.担当終了日 >= CURRENT_DATE OR T.担当終了日 IS NULL)

設問1　〔ビュー及びロールの設計〕について，(1)，(2)に答えよ。

(1)　表2中の［ a ］～［ c ］に入れる適切な字句を答えよ。

(2)　表2のア～ケで示したSQL文を正しい順に並べ替えよ。

なお，正しい順は複数通りあるが，そのうちの一つを答えよ。

（　）→（　）→（　）→（　）→（　）→（　）→（　）→（ク）→（ケ）

設問2　〔ビューの設計変更〕について，(1)～(3)に答えよ。

(1)　表3中の［ d ］，［ e ］に入れる適切な字句を答えよ。

(2)　表3中のSQL4において，そのままビューの定義に指定できない箇所がある。その箇所を二重線で消せ。

(3)　(2)で指定できないとした箇所を除いてビューを定義する。定義したビュー構造を，社員別訪問回数ビュー（社員番号，社員名，訪問回数）とし，SQL4と同じ結果行を得るために，表3中のSQL5（未完成）を作成した。SQL5の空欄に適切な字句を入れて完成させよ。ただし，結果行の並び順については，考慮しなくてよい。

設問3　〔セキュリティ要件の強化〕について，(1)～(3)に答えよ。

(1)　“チームメンバ”テーブルの構造を示せ。主キーには実線の下線を付けること。

(2)　図1中の社員のうち，個人情報へのアクセスが許可されているにもかかわらず，表4のSQL6では期待した結果を得られない社員がいる。その社員の社員番号を全て答えよ。また，解決策として，“チームメンバ”テーブルに対して行うべき行の操作を，30字以内で具体的に述べよ。

(3)　セキュリティ要件④におけるアクセス制限の実施について，対応案Bが対応案Aに比べて優れている理由を，40字以内で具体的に述べよ。