

問 6 入室管理システムの設計に関する次の記述を読んで、設問 1～5 に答えよ。

H 社は中堅の食品会社で、社内システムのデータベースの統合を検討している。現在、社内システムごとにデータベースのサーバを用意して運用しているが、関係データベース管理システム（以下、RDBMS という）のライセンスコストと運用コストを削減するために 1 台のサーバに統合し、各社内システムのデータベースは、統合したサーバの RDBMS でスキーマを分けて管理することになった。

〔社員情報の共用〕

全ての社内システムは、社員 ID や氏名などの社員情報を使用する。現在は、人事システムが管理している社員情報のマスタデータを月次処理で各社内システムに配布して運用しているが、最新の情報が反映されるのが翌月になること、月次処理の運用負荷が大ききことなどから改善が望まれている。今回、サーバを統合するに当たり、各社内システムにデータを配布するのではなく、人事システムが管理する社員情報に関連する実表を参照する方式に変更することを検討している。人事システムの社員情報に関連する実表を表 1 に示す。

表 1 人事システムの社員情報に関連する実表

実表名	列名
社員	社員 ID, 氏名, 勤務区分, 入社年月日, 生年月日, 社内メールアドレス, 社内電話番号, 自宅住所, 自宅電話番号, 役職, 所属組織 ID
組織	組織 ID, 組織名, 組織長の社員 ID, 上位組織の組織 ID

注記 勤務区分は、在職中、休職中、出向中、退職のいずれかを表す。

セキュリティの観点から検討した結果、人事システム以外の社内システムから社員情報に関連する実表を直接参照するのではなく、社員情報を使用する社内システムごとに必要な列だけをビュー表として公開し、ビュー表を参照する方式を採用することに決定した。

〔入室管理システム〕

会社内の特別な部屋の入退室管理を行う入室管理システムは、サーバ統合の対象となるシステムの一つである。入室管理システムで利用する主な実表とビュー表を表 2 に、E-R 図を図 1 に、入室に関する主なユースケースを表 3 に示す。

表 2 入室管理システムで利用する主な表

表名	種別	列名
入室管理用社員	ビュー表	社員 ID, 氏名, 勤務区分
室	実表	室 ID, 室名
入室許可	実表	社員 ID, 室 ID, 入室許可開始年月日, 入室許可終了年月日
入退室ログ	実表	社員 ID, 室 ID, 日時, 入退室区分, 許可区分

注記 ビュー表“入室管理用社員”は、表 1 の実表“社員”から入室管理システム用に社員 ID, 氏名, 勤務区分を射影したビュー表である。



図 1 入室管理システムの E-R 図（関連は未記入）

表 3 入室管理システムの入室に関する主なユースケース

ユースケース名	概要
入室申請	入室希望社員について、所属する組織の組織長が入室管理システムの管理者に申請書を提出する。申請書には、申請者（組織長の氏名）、入室希望社員の社員 ID, 氏名, 入室する室名, 入室許可開始年月日と入室許可終了年月日, 入室の目的を記入する。
入室許可登録	管理者は、申請書が届いたら、入室管理システムの入室許可登録画面で入室希望社員の社員 ID を入力し、表示された氏名が正しいこと、勤務区分が在職中であること、及び申請書の入室の目的が適切であることを確認して、問題がなければ入室を許可する。許可すると申請内容が実表“入室許可”に登録される。既に実表“入室許可”に同じ社員 ID, 室 ID, 入室許可開始年月日の行が存在する場合は、入室許可終了年月日を更新する。
入室	室の前に設置されているカードリーダーに社員証をかざすと、社員証から社員 ID を読み取る。実表“入室許可”で入室可否をチェックして、入室が許可されていれば、ドアを開錠し、実表“入退室ログ”に入退室区分が‘入室’、許可区分が‘OK’で記録する。入室が許可されていなければ、ドアを開錠せず、実表“入退室ログ”に入退室区分が‘入室’、許可区分が‘NG’で記録する。

表 3 のユースケース“入室”で，入室可否をチェックし，否の場合は 0 を，可の場合は 1 以上を返す SQL 文を図 2 に示す。ここで，“:社員 ID”は指定された社員 ID を格納する埋込み変数，“:室 ID”は指定された室 ID を格納する埋込み変数，“:今日”は SQL 文実行時の現在日付を格納する埋込み変数である。また，ROOM は入室管理システムのスキーマ名で，表は“スキーマ名.表名”で表記する。

```
SELECT a FROM ROOM.入室許可 WHERE 社員 ID = :社員 ID
AND 室 ID = :室 ID
AND 入室許可開始年月日 <= :今日
AND 入室許可終了年月日 >= :今日
```

図 2 入室可否をチェックする SQL 文

〔各社内システムの RDBMS ユーザ〕

社内システムごとにデータベース管理者（以下，DBA という）が存在する。DBA は表の所有者であり，他のユーザに対して，自分が所有する表へのアクセス権限を付与することができる。DBA は，各社内システムのアプリケーションプログラム（以下，AP という）が表のデータにアクセスできるように AP 用のユーザに対して，適切な権限を付与する。各社内システムのスキーマ名と，DBA 用，AP 用の RDBMS ユーザ名を表 4 に示す。

表 4 各社内システムのスキーマ名と RDBMS ユーザ名（抜粋）

システム名	スキーマ名	DBA 用ユーザ名	AP 用ユーザ名
人事システム	HR	HR_DBA	HR_AP
入室管理システム	ROOM	ROOM_DBA	ROOM_AP

〔RDBMS の表のアクセス権限に関する主な仕様〕

使用している RDBMS の表のアクセス権限に関する主な仕様を（1），（2）に示す。

（1）表のデータに対して，所有者以外のユーザが参照，挿入，更新及び削除を行うためには，表に対して対応するアクセス権限（SELECT，INSERT，UPDATE 及び DELETE の各権限）を所有者から付与してもらう必要がある。

（2）ビュー表にアクセスする場合，そのビュー表が参照する表のアクセス権限は不要である。

〔入室管理システム用の社員ビュー表〕

表 2 のビュー表“入室管理用社員”を定義する SQL 文を図 3 に示す。

```
CREATE VIEW HR.入室管理用社員（社員 ID, 氏名, 勤務区分）AS  
SELECT 社員 ID, 氏名, 勤務区分 FROM HR.社員
```

図 3 ビュー表“入室管理用社員”を定義する SQL 文

このビュー表を入室管理システムの AP が参照だけできるように権限を付与する SQL 文を図 4 に示す。

```
GRANT b ON c TO e
```

図 4 ビュー表“入室管理用社員”を参照するための権限を付与する SQL 文

〔入室申請時の確認の強化〕

管理者は、“申請者が入室希望社員の組織長であること”を確認することになった。そのため、ビュー表“入室管理用社員”に組織長の氏名が必要となり、図 5 に示す SQL 文に変更した。

```
CREATE VIEW HR.入室管理用社員（社員 ID, 氏名, 勤務区分, 組織長氏名）AS  
SELECT T1.社員 ID, T1.氏名, T1.勤務区分, T2.氏名  
FROM HR.社員 T1, HR.社員 T2, HR.組織 T3  
WHERE f
```

図 5 変更したビュー表“入室管理用社員”を定義する SQL 文

設問 1 図 1 に適切なエンティティ間の関連を記入し、E-R 図を完成させよ。図 1 の凡例に倣うこと。

設問 2 表 2 に示した実表“入室許可”における、主キーを答えよ。

設問 3 図 2 中の[a]に入れる適切な字句を答えよ。

設問 4 ビュー表“入室管理用社員”について、(1)、(2) に答えよ。

(1) 図 4 中の[b]～[e]に入れる適切な字句を答えよ。

なお、表は“スキーマ名.表名”で表記すること。

(2) ビュー表を参照する権限を付与する SQL 文を実行するユーザ名を答えよ。

設問 5 図 5 中の[f]に入れる適切な式を答えよ。