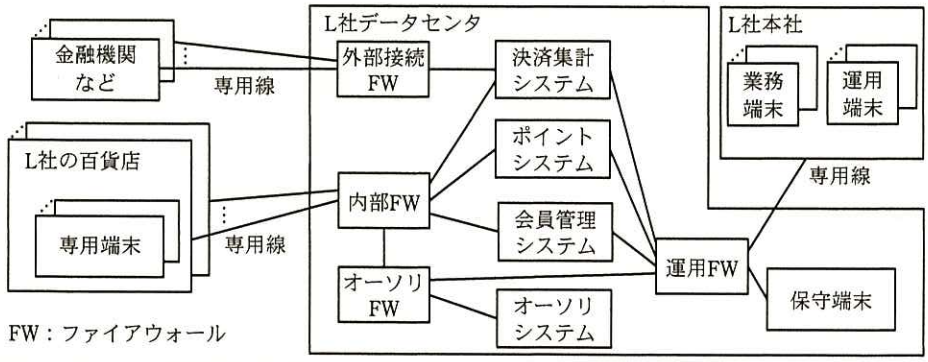
問1　百貨店事業におけるクレジットカード情報の安全な管理に関する次の記述を読んで，設問1～4に答えよ。

L社は，全国に百貨店事業を展開している従業員数3,000名の企業である。L社では，L社の百貨店だけで使用できるクレジットカード（以下，ハウスカードという）を発行している。ハウスカードは，顧客がハウスカード申込書を記入して，L社に提出し，審査に合格した後に発行される。ハウスカードを持つ顧客を会員と呼んでおり，会員がハウスカードを使用して支払ができるサービスと，ハウスカードを利用することでポイントが付与されるサービス（以下，両サービスを併せてハウスカードサービスという）を提供している。ハウスカードサービスでは，会員がハウスカードを使用して支払を行うと，会員にポイントが付与され，ポイントが一定数以上たまると，様々な商品と交換できる。ハウスカードの表面には，数字16桁のいわゆるクレジットカード番号（以下，PANという），会員名，有効期限などが表記されており，裏面にはハウスカードの不正使用を防止するために使用するセキュリティコードが表記されている。PANはハウスカードごとに異なる番号になっており，重複することはない。これらの情報の一部は，ハウスカードの磁気ストライプの中にも格納されており，各百貨店に設置されている専用端末で読み取ることができる。

〔ハウスカードサービスのシステム概要〕

ハウスカードサービスの主なシステムとネットワーク構成の概要は，図1のとおりである。



注記　L社本社の業務端末は執務室に，運用端末は運用ルームにそれぞれ設置されている。

図1　ハウスカードサービスの主なシステムとネットワーク構成の概要

L 社のセキュリティポリシによって，ハウスカードサービスのシステムを含め，全システムで，無線 LAN の利用が禁止されている。図 1 中の各システムの概要を表 1 に，各システムが利用しているデータベース（以下，DB という）の主なテーブルの構造を図 2 に示す。

表 1　各システムの概要

名称	概要
決済集計システム	・ハウスカードの決済集計処理を行う。会員が L 社の百貨店でハウスカードを使用して支払をすると，専用端末から決済情報（店舗コード，金額，PAN，会員名，有効期限，暗証番号）を受信し，オーソリシステムにオーソリ処理要求を送信する。オーソリシステムから処理結果を受信すると，専用端末に処理結果を返信し，決済情報を決済集計 DB に書き込む。決済集計処理を行うために，PAN を保存する。 ・日次バッチ処理で，決済情報を集計し，会員管理システムと連携して，各会員の決済金額とポイントを集計する。集計結果をポイントシステムに送信する。 ・月次バッチ処理で，決済情報を集計し，会員管理システムと連携して，各会員の決済金額を集計する。外部接続 FW を経由して，集計結果を金融機関などに送信する。 ・決済ごとにステータスコードと呼ばれる属性をもち，決済処理の進捗情報を記録している。
ポイントシステム	・決済集計システムから日次バッチの集計結果を受信する。会員管理システムと連携し，ポイント倍率補正処理や，キャンペーンによるポイント補正処理を実行し，ポイント DB に書き込む。決済集計システムとの間でデータを関連付けるために，PAN を保存する。
オーソリシステム	・ハウスカードの信用確認処理を行う。決済集計システムからオーソリ処理要求を受信し，ハウスカードの与信枠，有効期限，暗証番号による認証などの信用確認処理を行い，処理結果を決済集計システムに返信する。信用確認処理を行うために PAN を保存する。 ・オーソリ DB にデータを登録するインタフェースをもち，一連のハウスカード発行処理の中でデータが登録され，その後，定期的に更新される。
会員管理システム	・会員情報を管理する。会員情報とは，会員名，住所，電話番号，性別のことで，会員管理 DB に保存される。会員管理システムは，決済集計システムやポイントシステムに対して，専用のインタフェース経由で会員管理 DB の情報を参照させることができる。決済集計システムとの間でデータを関連付けるために，PAN を保存する。 ・Web インタフェースをもち，会員からの入会申請時には L 社の担当者がブラウザから会員情報を入力することで，会員管理 DB に会員情報を登録することができる。同様に変更申請時は会員情報を変更することができ，退会申請時は退会処理をすることができる。

決済集計 DB：決済集計（<u>決済処理番号</u>，PAN，店舗コード，金額，日時，オーソリ結果，最終処理日時，ステータスコード）
ポイント DB：ポイント（<u>PAN</u>，ポイント値，最終更新日時）
オーソリ DB：オーソリ（<u>発行管理番号</u>，PAN，有効期限，セキュリティコード，暗証番号，与信枠）
会員管理 DB：会員管理（<u>PAN</u>，会員名，住所，電話番号，性別）

注記 1　下線は主キーであることを表し，主キーには索引が設定される。
注記 2　発行管理番号は，ハウスカードに対して，発行時に一意に割り当てられる番号である。

図 2　各 DB の主なテーブルの構造

ハウスカードサービスのシステムは，L 社のカードサービス部が運用している。カ

ードサービス部の各課の業務概要は表２のとおりである。

表２　カードサービス部の各課の業務概要

課名称	業務概要
会員サポート課	会員からの，ハウスカードサービス全般に関する質問や，会員情報の変更申請，退会申請を電話で受け付ける。会員を特定するために受付時に PAN，会員名，住所を聞き，会員管理システムで PAN をキーとして検索し，本人であることを確認の上，会員情報の参照や変更を行う。会員のうち，前年度の支払額が一定の金額を超える会員を VIP 会員と呼び，より質の高いサービスを提供している。VIP 会員の要望を受け，運用課を通して保守課に作業を依頼する場合がある。会員サポート課では，１人につき１台の業務端末が貸与されている。
マーケティング課	ハウスカードの新規会員を獲得するために，キャンペーンの企画といったマーケティング活動を行う。
カード発行課	ハウスカードの発行，会員へのカードの発送を行う。オーソリシステムへのデータ登録は，一連のハウスカード発行処理の中で自動的に行われる。
運用課	ハウスカードサービスのシステムの運用を行う。バックアップなどの定型業務に加え，システム障害への対応などの非定型業務を行う。作業指示書を作成し，作業を保守課に依頼することもある。
保守課	ハウスカードサービスのシステムの開発，構築，変更，リリースを行う。その他，運用課からの依頼を受け，特別作業と呼ばれる次の二つの作業を実施する。 ・特別作業-1: 暗証番号の変更作業 運用課から PAN，現在の暗証番号，変更後暗証番号が記載された作業指示書を受け取る。オーソリ DB のオーソリテーブルから，指示された PAN をキーに，該当する行の全てのカラムを表示する。表示される暗証番号が指示書の現在の暗証番号と同一であることを確認し，暗証番号を変更後暗証番号に更新する。 ・特別作業-2: ステータスコード確認作業 障害発生時に運用課から決済処理番号が記載された作業指示書を受け取る。決済集計 DB の決済集計テーブルから，指示された決済処理番号をキーに，該当する行の全てのカラムを表示する。表示されたステータスコードと最終処理日時を運用課に報告する。 特別作業-1 と特別作業-2 は，それぞれ別のチームが担当しており，両方の作業を実施する担当者はいない。担当者は，あらかじめ割り当てられている DB の利用者 ID を用いて，保守端末から DB に接続し，SQL 文を入力して作業を行う。DB への SQL 文によるアクセスは，オーソリテーブルは，特別作業-1 の DB の利用者 ID にだけ，決済集計テーブルは，特別作業-2 の DB の利用者 ID にだけ，許可されている。

〔会員サポート課の業務内容〕

会員サポート課では，会員から暗証番号の変更要望を受けることがある。その場合，変更要望を断って，新規ハウスカードの発行手続を取るよう説明していた。暗証番号はオーソリシステムが保持しており，会員管理システムでは変更できない。これは，サービス設計当初，暗証番号の変更は原則受け付けずに新規にハウスカードを発行する運用を前提にしていたからである。

会員サポート課には，VIP 会員に対応する専門の担当者（以下，VIP 会員担当という）がいる。VIP 会員からの質問や要望は，VIP 会員専用の電話番号で受け付け，VIP 会員担当が，要望に対して柔軟に対応することで，VIP 会員の顧客満足度を高めている。VIP 会員担当は，特に電話の多い十数名の VIP 会員からの質問や要望に迅速に応えるために，そういった VIP 会員の PAN，会員名，過去の問合せ履歴などを PC 内の VIP ファイルというファイルに記録している。会員管理システムでも同様の記録や管理は可能であるが，VIP 会員担当は，VIP ファイルの方が使いやすいと感じており，VIP 会員から電話があった際には，ときどき，VIP ファイルを使用することもあった。また，VIP 会員担当が，VIP 会員から暗証番号の変更要望を受けたときに，断ることができず，運用課を通して保守課に依頼し，オーソリ DB のオーソリテーブル中の暗証番号を変更してもらうことが度々発生していた。

〔提携カードによる新サービス構想〕

近年，L 社は新規会員獲得のための様々な施策を実行しているものの，会員数は伸び悩んでおり，ハウスカードによる年間の支払総額は減少傾向にあった。そこで，L 社は，顧客のニーズや世の中のトレンドなどを調査し，世界各地で多くの加盟店をもつ H 社と提携した新しいクレジットカード（以下，提携カードという）による新サービスの提供を検討することにした。提携カードは，ハウスカードと異なり，L 社百貨店だけでなく，H 社の加盟店でも利用できる。L 社は，現行のハウスカードサービスのシステムを拡張し，提携カードによる新サービスを実現することにした。ポイント還元率の高いハウスカードと，多くの店舗でカードが利用できる提携カードの両方のサービスを提供することで，顧客の幅広いニーズに応えられると考えた。L 社は，H 社との交渉と提携カードによる新サービスの具体的な検討を進めるために，提携カード検討委員会を設置した。

H 社との交渉過程で，L 社のそれまでの PAN の取扱方針が不明確である点について，H 社から強い改善要求が示された。H 社は，PAN や，PAN に関連するデータについて，クレジットカードに関する情報を保護するセキュリティ基準として国際的に広く認知されている Payment Card Industry データセキュリティ基準（PCI DSS）に準拠するよう L 社に求めた。L 社は，提携カードによる新サービスを実現するためだけでなく，セキュリティの向上も期待できると考えて，改善要求を受け入れることにした。提携

カード検討委員会は，情報システム企画部のY部長に，PCI DSSへの準拠を検討するよう指示した。Y部長とその部下のN主任は，最初にPCI DSSの要件を調査した。

〔PCI DSS要件への準拠状況の調査〕

PCI DSSの要件は，PANや，PANとともに扱う会員名と有効期限，さらに磁気ストライプのデータ，セキュリティコードなどが，保存，処理又は送信される組織と環境にそれぞれ適用されることが分かった。また，PCI DSSの要件が適用される範囲（以下，適用範囲という）を最初に明らかにする必要があることも分かった。そこで，Y部長は，L社のPANの取扱方針を図3のように定めた。

方針 1. PANの業務上不要な利用や保存はしない。業務上の利便性だけの理由による利用や保存も禁止する。
方針 2. 適用範囲を明らかにし，PCI DSSの要件を適用する。PANを保存する場合には，アクセス制御を行い，必要最小限の利用者だけに，必要最小限のアクセス権限を設定する。業務上PANの表示が必要な場合を除き，PANの表示はしない。

図3　L社のPANの取扱方針

Y部長とN主任は，図3の方針に従って検討を開始した。

方針1.について，カードサービス部の業務や表1の各システムにおける，PANの取扱状況を確認した。すると，会員サポート課の業務の中で，①方針1.に反する業務があることが分かった。Y部長は，会員サポート課に対する改善案を提言した。

方針2.については，PANや磁気ストライプのデータ，セキュリティコードなども考慮すると，図1中のL社本社の業務端末及び運用端末，各百貨店の専用端末，並びにL社データセンタ内のハウスカードサービスのシステム，ネットワーク機器及び端末が適用範囲であることが明らかになった。その上で，適用範囲中のシステムや端末などが，PCI DSSの各要件に準拠しているかどうかを調査した。すると，図4の要件3.4及び11.1に関して問題があることが分かった。

（省略）

3.4 以下の手法を使用して，すべての保存場所で PAN を少なくとも読み取り不能にする（ポータブルデジタルメディア，バックアップメディア，ログを含む）。
・強力な暗号化をベースにしたワンウェイハッシュ（PAN 全体をハッシュする必要がある）
・トランケーション（PAN の切り捨てられたセグメントの置き換えにはハッシュを使用できない）
・インデックストークンとパッド（パッドは安全に保存する必要がある）
・関連するキー管理プロセスおよび手順を伴う，強力な暗号化
（省略）

3.4.1 （ファイルまたは列レベルのデータベース暗号化ではなく）ディスク暗号化が使用される場合，論理アクセスはネイティブなオペレーティングシステムの認証およびアクセス制御メカニズムとは別に管理する必要がある（ローカルユーザアカウントデータベースや一般的なネットワークログイン資格情報を使用しないなどの方法で）。復号キーがユーザアカウントと関連付けられていない。
（省略）

11.1 四半期ごとにワイヤレスアクセスポイントの存在をテストし（802.11），すべての承認されているワイヤレスアクセスポイントと承認されていないワイヤレスアクセスポイントを検出し識別するプロセスを実施する
（省略）

出典：PCI Security Standards Council LLC, “Payment Card Industry（PCI）データセキュリティ基準 要件とセキュリティ評価手順 バージョン 3.0”，38～40 ページ及び 89 ページ
（URL：https://ja.pcisecuritystandards.org/minisite/en/pci-dss-v3-0.php（平成 26 年 3 月 6 日アクセス））
注記 1 “ユーザアカウント”とは，“利用者 ID”と同じである。
注記 2 要件 3.4 及び 3.4.1 は PAN だけに適用される。

図 4 PCI DSS 要件

〔PCI DSS 要件 3.4 への準拠〕

要件 3.4 には，PAN を保存する際の要件が書かれている。要件 3.4.1 には，ディスク暗号化に関する要件が書かれている。

Y 部長と N 主任は，DB に保存する PAN について，暗号化による対策を検討することにした。N 主任は表 3 に示す暗号化方式を選定し，検討を進めた。次は，その時の会話である。

表3　暗号化方式

方式名	概要	詳細
方式1	市販製品を利用したハードディスク暗号化	ハードディスク全体を暗号化する。OS の利用者 ID のログインに成功すると，ハードディスクの全てのデータがアクセス時に自動的に復号されるようになる。ネットワーク経由の OS へのログインについても同様である。
方式2	DB の機能を利用した表領域の暗号化	DB の表領域を暗号化する。DB へのログインは OS の利用者 ID とは別の DB の利用者 ID で認証される。DB へのログインに成功すると，復号された状態で DB を利用できる。
方式3	DB の機能を利用した列の暗号化	DB の表の指定した列を暗号化する。DB へのログインは OS の利用者 ID とは別の DB の利用者 ID で認証される。DB の利用者 ID ごとに，復号可能な列を権限として設定できる。暗号化された列を復号権限がない DB の利用者 ID で表示した場合，復号されずに表示される。索引を設定した列は暗号化できない。

N 主任：暗号化に関して，検討を具体化するために，決済集計 DB の決済集計テーブルを対象に，テストデータと検証環境を用いて性能を測定しました。いずれの方式も SQL 文の処理性能はシステムに求める性能要件を満たすことが分かりました。そのうち，方式 2 が処理性能の劣化度合いが小さいので，方式 2 を採用すべきと考えています。

Y 部長：確かに，処理性能の面でいえばそうかもしれない。一方で，保守課では，②方式 3 を採用し，DB の利用者 ID ごとに権限を与えることで，③当社の PAN の取扱方針により一層従った状態で，作業できるようになる。ただし，④会員管理テーブルに方式 3 を採用することはできない。各方式で有意な差がないのであれば，処理性能を考慮点から除外し，PCI DSS の要件と当社の方針に基づいて，テーブルごとに最適な方式を採用しよう。

N 主任：分かりました，テーブルごとに最適な方式を検討します。

その後，N 主任は検討を進め，検討結果を Y 部長に報告した。提携カード検討委員会は，表 4 のように暗号化方式を決定した。

表4　決定した暗号化方式

テーブル名称	方式名
決済集計テーブル	a
ポイントテーブル	b
オーソリテーブル	c
会員管理テーブル	d

〔PCI DSS 要件 11.1 への準拠〕

N 主任は要件 11.1 についても検討を進めた。次は，要件 11.1 のワイヤレスアクセスポイントのスキャン（以下，W-AP スキャンという）に関する会話である。

N 主任：無線 LAN については，本社，各百貨店，データセンタのいずれでも使用していないはずです。なぜ，要件 11.1 では W-AP スキャンを実施することまで要求するのでしょうか。

Y 部長：⑤セキュリティ上の問題につながる事象が幾つか想定されるからね。それらの事象によって，例えば，情報漏えいなどが起きる可能性もある。W-AP スキャンを実施するには，専用のソフトウェアが必要になるが，それほど難しいことではないよ。実際に，当社の運用ルームで，W-AP スキャンを行ってみたらどうだろう。

N 主任は，実際に運用ルームで W-AP スキャンを行い，結果をまとめた。次は，その結果を Y 部長に報告した際の会話である。

N 主任：図 5 は W-AP スキャンの結果です。運用ルーム全体をカバーできるよう，部屋の中央に測定ポイントを設定しました。運用ルームは，測定ポイントから半径 5m 以内に収まり，かつ，検出されたワイヤレスアクセスポイントも測定ポイントからの推定距離が 12m 以上なので，運用ルーム内にワイヤレスアクセスポイントがないことを確認できました。

Y 部長：測定ポイントの設定や，推定距離の計算については問題ないと思う。ただし，無線 LAN の規格を考えると，例えば [e] の検査ができていない。

1. 検査結果

測定ポイントから 5m 以内の距離，つまり運用ルーム内にワイヤレスアクセスポイントは検出されなかった。

2. 確認日時及び検査方法

（省略）

3. 使用 PC，検査対象無線 LAN 規格，使用ソフトウェア

使用 PC：××× GP28
無線 LAN アダプタ：××× Network Connection
無線 LAN 規格：IEEE802.11 b/g
使用ソフトウェア：×××checker 3.1.6

4. 測定結果

次のワイヤレスアクセスポイントが検出された。

MAC アドレス	SSID	周波数帯(GHz)	推定距離(m)
××:××:××:00:08:0F	AbcD	2.4	16
××:××:××:00:74:B5	Emcad	2.4	12
××:××:××:10:2F:2A	AL45ioew4	2.4	15

図 5　W-AP スキャンの結果

〔準拠計画書の提出〕

その後も，Y 部長と N 主任は PCI DSS 要件への準拠性について確認を進め，問題がある要件については，対策計画を明確にした。また，継続的に適用範囲の正確性を確認するとともに，より限定していくという方針を定め，対策計画の内容と合わせて準拠計画書としてまとめた。準拠計画書は，提携カード検討委員会で承認された後，H 社に提出された。H 社からは，L 社の迅速な対応と準拠計画書の内容が高く評価された。

〔新システム化計画〕

L 社内で提携カードによる新サービスの検討が進む中，N 主任は，提携カードの導入と合わせて，提携カードとハウスカードの表面に PAN，会員名，有効期限及び図 6 に示す仕様のお客様コードを表記し，会員管理テーブルの構造を図 7 のように修正して，お客様コードをキーに検索できるように会員管理システムを改修する案を Y 部長に提案した。

・10 桁の英数字で構成する。
・PAN とは異なるアルゴリズムで生成する。
・クレジットカードごとに一意に採番する。

図 6　お客様コードの仕様

会員管理 DB：会員管理（お客様コード，PAN，会員名，住所，電話番号，性別）

図 7　お客様コード導入後の会員管理テーブルの構造

N 主任は，“この改修によって，⑥会員サポート課の業務の一部の手順を，準拠計画書に含まれる方針に従って改善することも可能になる”と，お客様コードを表記するメリットを説明した。

Y 部長は，N 主任の提案に対し，“さらに，PAN とお客様コードを相互に関係付けるテーブルをもつ変換 DB を作成し，システムには，PAN から対応するお客様コード，お客様コードから対応する PAN を検索できるインタフェースを作り，各システムから利用できるようにすれば，L 社にとってセキュリティが考慮された DB のテーブルの構造を実現できる”と指摘した。N 主任は Y 部長の指摘を受け，図 8 に示す DB のテーブル構造案を作成した。また，合わせて他の必要な見直しも実施した。

決済集計 DB：決済集計（決済処理番号，PAN，店舗コード，金額，日時，オーソリ結果，最終処理日時，ステータスコード）
変換 DB：変換（PAN，お客様コード）
ポイント DB：ポイント（ f ）
オーソリ DB：オーソリ（発行管理番号，PAN，有効期限，セキュリティコード，暗証番号，与信枠）
会員管理 DB：会員管理（ g ）

図 8　お客様コード導入後の DB の主なテーブルの構造案

提携カード検討委員会は，Y 部長と N 主任の案を採用し，新システムでは，お客様コードを導入することを決定した。

その後，H 社との交渉は無事合意の方向で進み，Y 部長は，提携カードによる新サービスを実現するための新システム化計画を策定することになった。

設問1　本文中の下線①について，会員サポート課の業務の中で，どのような点が方針1.に反しているか。40字以内で具体的に述べよ。

設問2　〔PCI DSS 要件 3.4 への準拠〕について，(1)～(5)に答えよ。

(1)　本文中の下線②について，L社の方針に従った権限の付与を解答群の中から選び，記号で答えよ。

解答群

	特別作業-1 の DB の利用者 ID に対するオーソリテーブルの PAN 列の復号権限の付与	特別作業-2 の DB の利用者 ID に対する決済集計テーブルの PAN 列の復号権限の付与
ア	与える	与える
イ	与える	与えない
ウ	与えない	与える
エ	与えない	与えない

(2)　本文中の下線③について，保守課のどの作業を，どのような状態で，できるようになるか。それぞれ15字以内で答えよ。

(3)　表3の暗号化方式には，図4に示す要件を満たさないものがある。その方式名と満たさないPCI DSS要件の項目番号をそれぞれ答えよ。また，その方式のどの動作が，要件のどの内容に違反するのか。動作を40字以内で，内容を30字以内で，それぞれ具体的に述べよ。

(4)　本文中の下線④の理由を35字以内で具体的に述べよ。

(5)　表4中の［　a　］～［　d　］に入れる適切な方式名を表3の中から答えよ。

設問3　〔PCI DSS 要件 11.1 への準拠〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑤について，セキュリティ上の問題につながる事象を一つ，40字以内で述べよ。

(2)　本文中の［　e　］に入れる適切な字句を答えよ。

設問4　〔新システム化計画〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑥について，どの手順をどのように改善できるか。40字以内で具体的に述べよ。

(2)　図8中の［　f　］，［　g　］に入れるテーブル構造を答えよ。
なお，主キーには下線を引くこと。