SC

平成26年度　春期
情報セキュリティスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1，問2
選択方法	1問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を○印で囲んでください。○印がない場合は，採点されません。2問とも○印で囲んだ場合は，はじめの1問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問2を選択した場合の例〕

選択欄	
1問選択	問1
	(問2)

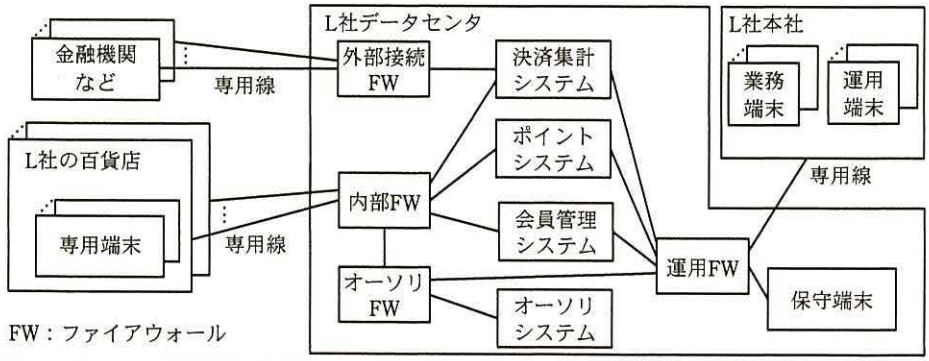
注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

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。

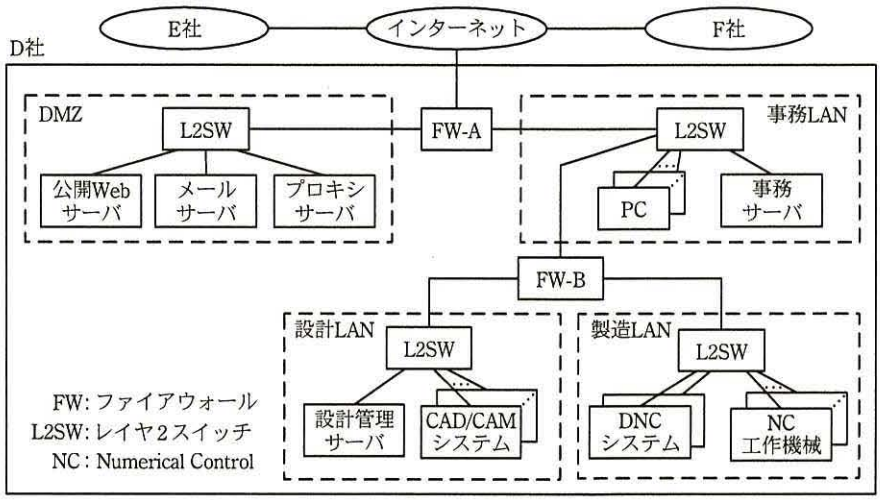
(2)　図8中の［　f　］，［　g　］に入れるテーブル構造を答えよ。
なお，主キーには下線を引くこと。

問2　金属加工業者におけるデータ管理に関する次の記述を読んで，設問1～5に答えよ。

D社は，従業員数200名の金属加工業者である。CAD/CAM（Computer Aided Design/Computer Aided Manufacturing）システム及びDNC（Direct Numerical Control）システムを導入し，設計と製造に活用している。大型機械製造業や電気機器製造業の大手企業から委託を受けることも多い。特殊な加工が必要な場合は，専門の加工業者（以下，専門加工業者という）に再委託することもある。

〔D社のネットワーク構成と機器〕

D社のネットワーク構成を図1に示す。



注記　事務LANのデフォルトゲートウェイはFW-Aである。

図1　D社のネットワーク構成

D社は，公開Webサーバを運用し，そのコンテンツ作成を，コンテンツ作成業者のE社に委託している。E社の担当者は，E社からインターネット経由で，FTPを使用してコンテンツを更新する。

また，D社では，インターネットサービスプロバイダのF社が提供するサービス（以下，F社サービスという）のうち，次のものを使用している。

・DNSサービス

・インターネットとD社との間の電子メール（以下，メールという）を中継するサ

ービス（以下，メール中継サービスという）

・メールのウイルス対策サービス及び迷惑メール対策サービス

D 社のネットワークに接続された機器には，固定 IP アドレスを割り当てている。

製造 LAN に接続された機器の運用は，製造課の担当者が行っている。それ以外の機器の運用は，情報システム課の J 課長の下，K さんが行っている。

〔取引時の情報管理〕

設計課の担当者は，委託元指定の安全性が確保された方法を用いて，設計図面を CAD データとして受け取る。その後，ウイルススキャンを行い，設計管理サーバに保存する。さらに，CAD/CAM システムを使用して，CAD データを NC 工作機械用の NC プログラムに変換し，設計管理サーバに保存する。製造課の担当者は，DNC システムを操作し，NC プログラムを設計管理サーバから NC 工作機械に取り込む。また，DNC システムを操作して，NC 工作機械の操作及び監視も行う。

CAD/CAM システムは，加工条件として工具の選択，加工順序などのデータベースを提供している。しかし，CAD/CAM システムが提供しているデータベースだけで全ての注文に対応できるわけではない。複雑な形状の加工の注文もあり，D 社が独自に作成した加工条件を使用することも多い。D 社独自の加工条件や NC プログラムは，D 社の重要情報であるので，情報漏えい対策に取り組んでいる。

専門加工業者に再委託する場合は，ウイルススキャンを行った後に暗号化した上で，次のいずれかの方法で CAD データを送付する。

・メールに添付して送付

・DVD-R などのメディアに記録して宅配便を利用して送付

復号用のパスワードは，CAD データとは別にメールで送付する。

経理課の担当者は，支払や入金の確認に U 銀行のインターネットバンキングサービスを利用している。U 銀行のインターネットバンキングサービスでは，EV SSL 証明書が使用されているので，担当者は，U 銀行のインターネットバンキングサービスにログインする前に，ブラウザのアドレスバーに表示される Web サイト運営者名が U 銀行であることを確認している。

〔情報システム課が運用している機器の概要〕

情報システム課が運用している主な機器の概要を表1に示す。

表1　主な機器の概要

機器名	OS	概要
FW-A，FW-B	専用 OS	ステートフルパケットフィルタリング機能並びに通信の許可及び拒否のログを取得する機能がある。
公開 Web サーバ	UNIX	コンテンツ公開機能及びコンテンツ全文検索機能を提供している。コンテンツ更新は，FTP を用いて行う。
メールサーバ	UNIX	F 社のメール中継サービスのサーバとの間のメール転送機能及び PC との間のメール送受信機能がある。リゾルバ機能及び DNS キャッシュ機能がある。NTP サーバ機能があり，インターネット上の NTP サーバとの間で時刻同期している。
プロキシサーバ	UNIX	P 社のプロキシソフトを使用している。PC からインターネットへの Web アクセス通信中継機能，Web アクセス通信ウイルススキャン機能，URL フィルタリング機能及び HTTP over TLS（以下，HTTPS という）通信対応機能がある。HTTPS 通信対応機能とは，HTTPS 通信を復号し，Web アクセス通信ウイルススキャン機能及び URL フィルタリング機能を使用した後，再暗号化する機能である。プロキシソフトのウイルス定義ファイル及び P 社が提供する URL ブラックリスト（以下，P 社提供リストという）は，P 社の Web サーバから 1 時間ごとに直接ダウンロードし，更新している。D 社では，HTTPS 通信対応機能を使用していない。
事務サーバ	Windows	人事情報，経理情報などを格納する。Q 社のウイルス対策ソフトを導入している。NTP サーバ機能があり，メールサーバとの間で時刻同期している。
設計管理サーバ	Windows	CAD データ及び NC プログラムを格納する。Q 社のウイルス対策ソフトを導入している。PC との間の CAD データの送受信及び DNC システムの NC プログラム取込みのために，FTP サーバ機能がある。
CAD/CAM システム	Windows	設計図面の確認及び修正，並びに CAD データから NC プログラムへの変換を行う。Q 社のウイルス対策ソフトを導入している。

D 社では，社内で利用可能なソフトウェアを定めている。OS が Windows の場合は，Q 社のウイルス対策ソフトと R 社の画像閲覧ソフトの導入を必須としている。

D 社では年 3 回，FW-A，FW-B 及び DMZ に設置されたサーバに対して脆弱性修正プログラムを適用している。

事務サーバ，設計管理サーバ及び CAD/CAM システムでは，OS の脆弱性修正プログラムがリリースされた場合，その週末に OS ベンダの Web サーバからプロキシサーバ経由で脆弱性修正プログラムをダウンロードして，適用している。

従業員が用いる PC は，会社が貸与している。PC の OS は，Windows である。OS

の脆弱性修正プログラムは，リリースされると自動的に適用される。

DMZ に設置されたサーバ，事務サーバ，設計管理サーバ及び CAD/CAM システムのデータは，日次でバックアップを行っている。また，OS 及びプログラムのバックアップは，脆弱性修正プログラム適用前及び適用後に行っている。

PC，事務サーバ，設計管理サーバ及び CAD/CAM システムでは，ウイルス対策ソフトのウイルス定義ファイルを，起動時及び起動後 2 時間ごとに Q 社の Web サーバからプロキシサーバ経由でダウンロードし，更新している。

各サーバでは，サーバへのアクセス及びプログラムの動作をログとして取得している。各サーバのログの保存期間は 4 週間である。

FW-A のフィルタリングルールを表 2 に，FW-B のフィルタリングルールを表 3 に示す。

表 2　FW-A のフィルタリングルール

項番	送信元	宛先	サービス	動作	ログ
1	メールサーバ	インターネット	DNS，NTP	許可	取得しない
2	F 社[1)]	メールサーバ	SMTP	許可	取得する
3	メールサーバ	F 社[1)]	SMTP	許可	取得する
4	全て	公開 Web サーバ	FTP	許可	取得する
5	全て	公開 Web サーバ	HTTP	許可	取得する
6	PC，事務サーバ，設計管理サーバ，CAD/CAM システム	プロキシサーバ	代替 HTTP[2)]	許可	取得する
7	プロキシサーバ	インターネット	FTP，HTTP，HTTPS	許可	取得する
8	事務サーバ	メールサーバ	NTP	許可	取得する
9	PC	メールサーバ	POP3，SMTP	許可	取得する
10	全て	全て	全て	拒否	取得しない

注[1)]　F 社とは，F 社のメール中継サービスのサーバである。

[2)]　代替 HTTP のポート番号は，8080 である。

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

表 3　FW-B のフィルタリングルール

項番	送信元	宛先	サービス	動作	ログ
1	PC，DNC システム	設計管理サーバ	FTP	許可	取得する
2	設計管理サーバ，CAD/CAM システム	事務サーバ	NTP	許可	取得する
3	設計管理サーバ，CAD/CAM システム	プロキシサーバ	代替 HTTP	許可	取得する
4	全て	全て	全て	拒否	取得しない

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

FW-A 及び FW-B のログの保存期間は 4 週間である。

FW-A 及び FW-B のフィルタリングルールのバックアップは，ルール変更後に行っている。

〔公開 Web サーバのコンテンツ改ざんと対処〕

ある日，E 社の担当者から，“公開 Web サーバのコンテンツを更新しようとしたところ，あるファイルの更新日時が，前回の更新日時と異なっていることに気付いた。D 社で更新したのか”と K さんに問合せがあった。K さんが確認したところ，D 社では誰もそのファイルを更新していなかったので，J 課長に公開 Web サーバのコンテンツが改ざんされた可能性があることを報告した。J 課長が，情報システム担当の M 役員に報告したところ，情報セキュリティ専門会社に調査を依頼するようにとの指示を受けた。J 課長は，情報セキュリティ専門会社の G 社に調査を依頼した。

その日のうちに，G 社の情報セキュリティスペシャリストである A 氏が，D 社を訪問した。A 氏は，公開 Web サーバを①シャットダウンすると調査が困難になるので，調査が完了するまでそのままにしておき，公開だけは直ちに停止するようにと助言し，J 課長と K さんはそれに従った。さらに，A 氏が，FW-A 及び DMZ に設置されたサーバに対して，いつ脆弱性修正プログラムを適用したかを尋ねたところ，K さんは 2 か月前に適用したと答えた。

A 氏は，FW-A 及び DMZ に設置されたサーバで，必要なファイルを採取し，調査を開始した。1 週間後，G 社から J 課長と K さんに調査結果の報告があった。調査結果の概要を図 2 に示す。

1. コンテンツ改ざんについて
  1.1 コンテンツファイル改ざんの内容
    ・コンテンツファイル中に，不正なスクリプトが埋め込まれていた。
    ・不正なスクリプトは，ブラウザ表示の見かけには影響しないものであった。
  1.2 コンテンツファイル改ざんの手法
    ・改ざんは，公開 Web サーバのコンテンツ全文検索機能の脆弱性を悪用した可能性が高い。脆弱性情報は，調査開始日の 4 週間前に公表された。脆弱性修正プログラムは，調査開始日の 3 週間前にリリースされた。
    ・調査したログには，不審なアクセスの記録はなかった。調査開始日の 4 週間以上前に改ざんが行われた可能性が高い。
2. 不正なスクリプトについて
  ・改ざんされたコンテンツにアクセスすると，多くの PC ベンダがプリインストールしている R 社の画像閲覧ソフトの脆弱性を悪用し，攻撃者が用意した Web サーバから，新たなウイルスをダウンロードさせる。画像閲覧ソフトの脆弱性修正プログラムは，調査開始日の 3 週間前に，R 社の Web サーバからダウンロードできるようになっていた。
  ・不正なスクリプトは既知のものである。不正なスクリプトに対応したウイルス対策ソフトの定義ファイルは，調査開始日の 2 週間前にリリースされた。
  ・攻撃者が用意した Web サーバは，既に閉鎖されている。
3. 復旧方法及び再発防止策について
  ・②D 社の運用状況を考慮するとバックアップメディアからの復元ではなく，OS，Web サーバプログラム及びコンテンツ全文検索機能のプログラムの最新版をインストールし，コンテンツは E 社が納入したものを用いて復元することを推奨する。
  ・公開 Web サーバの運用再開前に，脆弱性検査を実施することを推奨する。
  ・FW-A，FW-B 及び DMZ に設置されたサーバに関する脆弱性情報の収集を強化する。
4. そのほかの推奨事項について
  4.1 コンテンツ改ざん事実の公表について
    ・コンテンツ改ざんの事実を，復旧後の公開 Web サーバに掲載する。
  4.2 PC，事務サーバ，設計管理サーバ及び CAD/CAM システムへの脆弱性修正プログラムの適用について
    ・脆弱性修正プログラムの適用対象を見直して，実行する。
  4.3 公開 Web サーバのコンテンツ更新方法について
    ・コンテンツ更新方法を見直す。
  4.4 プロキシサーバの設定について
    ・Web アクセスによるウイルス感染を減らすために，プロキシサーバの設定を見直す。
  4.5 ログの取得及び管理方法について
    ・トラブル調査の迅速化を目的に，ログの取得及び管理方法を見直す。
  4.6 DMZ に設置されたサーバのウイルス対策について
    ・DMZ に設置されたサーバにも，ウイルス対策ソフトを導入する。

図 2　調査結果の概要

J 課長と K さんは，図 2 に示された推奨事項について対処することにした。

まず，J 課長は，公開 Web サーバの復旧を，図 2 の 3. の方法で行うことを K さんに指示した。K さんは，OS，Web サーバプログラム及びコンテンツ全文検索機能のプログラムの最新版をインストールし，動作確認を行った。J 課長は，脆弱性検査を G 社に依頼し，脆弱性は発見されなかったという報告を受けた。J 課長は，M 役員の了承

を得て，公開 Web サーバの運用を再開し，図 2 の 4.1 の対応を行った。

次に，J 課長と K さんは，図 2 の 4.2 に対応するために，③PC，事務サーバ，設計管理サーバ及び CAD/CAM システムについて脆弱性修正プログラムの適用対象を追加し，直ちに実行した。

J 課長と K さんは，A 氏の助言を受けながら，図 2 の 4.3～4.6 の推奨事項への対応を更に進めた。

〔公開 Web サーバのコンテンツ更新方法の見直し〕

J 課長と K さんは，公開 Web サーバのコンテンツ更新について，幾つかの方法を検討した。K さんが A 氏に相談したところ，A 氏は暗号や認証の技術を利用して，リモートコンピュータとの間でファイル転送や OS へのログインを安全に行うことができるプロトコルである［ a ］を用いたファイル転送ソフトの使用を推奨した。K さんは，E 社の担当者とも相談し，表 2 の項番 4 の項目のうち，サービスを FTP から［ a ］に変更することにした。加えて，④表 2 の項番 4 の項目をもう 1 か所見直した方がよいことに気付き，変更することにした。

K さんは，J 課長の承認を得て，これらの変更を直ちに実施した。実施後，E 社からコンテンツのアップロードができることを確認した。

〔プロキシサーバの設定の見直し〕

プロキシサーバの機能を表 4 に示す。

表4　プロキシサーバの機能

機能名	機能
Web アクセス通信中継機能	PC やサーバ（以下，PC とサーバを併せて接続元という）とインターネット上の Web サーバ（以下，接続先という）との間の Web アクセスの通信を中継する。
Web アクセス通信ウイルススキャン機能	接続元と接続先との間の通信内容に対してウイルススキャンを行う。HTTPS 通信のウイルススキャンを行うには，HTTPS 通信対応機能を有効にする。
URL フィルタリング機能	接続元，URL リスト及び動作を組み合わせた URL 制御ルールを用いて，URL フィルタリングを行う。URL 制御ルールの動作には許可又は拒否を指定する。接続元と URL リストの組合せのどれにも該当しない通信は，許可される。許可又は拒否にかかわらず，通信のログを取得する。URL リストには，P 社提供リスト及び利用者が定義するリスト（以下，ユーザ定義リストという）がある。サーバ管理者は，複数のユーザ定義リストを作成して URL を登録できる。P 社提供リストには，通信を拒否する URL が登録されているが，その URL の内容は開示されていない。HTTPS 通信の URL フィルタリングを行うためには，HTTPS 通信対応機能を有効にする。
HTTPS 通信対応機能	接続元とプロキシサーバとの間，及びプロキシサーバと接続先との間において，それぞれ独立の HTTPS 通信を確立する。HTTPS 通信確立前に接続先の証明書の検証を行い，検証が失敗した場合は，通信を拒否する。接続先のコモンネームを基に証明書を作成し，その証明書で接続元との間の HTTPS 通信を確立する。サーバ管理者は，HTTPS 通信対応機能を使用したくない URL を除外リストに登録できる。除外リストに登録された URL にアクセスした場合は，接続元と接続先との間で直接 HTTPS 通信が確立される。

J 課長と K さんは，URL 制御ルールの設定について検討した。現在の URL 制御ルールを表 5 に示す。

表5　URL 制御ルール

項番	接続元	URL リスト	動作
1	PC，事務サーバ，設計管理サーバ，CAD/CAM システム	P 社提供リスト	拒否

J 課長と K さんは，表 5 に対する修正案を作成した。その案を表 6 に示す。

表6　URL 制御ルールの修正案

項番	接続元	URL リスト	動作
1	事務サーバ，設計管理サーバ，CAD/CAM システム	ユーザ定義リスト 1	許可
2	事務サーバ，設計管理サーバ，CAD/CAM システム	ユーザ定義リスト 2	拒否
3	PC	P 社提供リスト	拒否

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

表 6 中のユーザ定義リスト 1 及びユーザ定義リスト 2 を表 7 に示す。

表7　ユーザ定義リスト1及びユーザ定義リスト2

URL リスト	URL
ユーザ定義リスト1	b の URL，c の URL，d の URL，…
ユーザ定義リスト2	全て

次に，J 課長と K さんは，HTTPS 通信対応機能の使用について検討した。A 氏に相談したところ，次の助言を受けた。

・HTTPS 通信対応機能を使用すると，⑤インターネットを利用する D 社の業務の一部に不都合が生じる。その不都合は，除外リストを使用すれば回避できる。

・HTTPS 通信対応機能を使用するには，接続元にプロキシサーバのルート証明書をインストールしておく必要がある。

・HTTPS 通信対応機能を使用すると，プロキシサーバの負荷が著しく上昇する。

J 課長と K さんは，現在のプロキシサーバの性能では負荷の上昇に対応できないと判断し，HTTPS 通信対応機能は，来年予定されているプロキシサーバの更新以降に使用することにした。

〔ログの取得及び管理方法の見直し〕

J 課長と K さんは，公開 Web サーバがウイルスに感染した場合に備えて，FW-A でのログの取得方法を検討した。表 2 の項番 10 のログを“取得する”に変更すると，ログ取得数が増え，保存領域の不足が発生するので実現できない。しかし，表 8 に示すように項番 5 の後にルールを追加し，FW-A のフィルタリングルールを修正すれば，攻撃者が用意したサーバへのウイルスからの通信を効率よく検出することができ，保存領域の不足が発生しにくくなることが分かった。

表8　FW-A のフィルタリングルールの修正案

項番	送信元	宛先	サービス	動作	ログ
⋮	⋮	⋮	⋮	⋮	⋮
5	全て	公開 Web サーバ	HTTP	許可	取得する
6	e	f	g	拒否	取得する
7	PC，事務サーバ， 設計管理サーバ， CAD/CAM システム	プロキシサーバ	代替 HTTP	許可	取得する
⋮	⋮	⋮	⋮	⋮	⋮

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

同様に FW-B のフィルタリングルールの修正案も作成した。

続いて，各サーバのハードディスクの使用状況を調査した結果，ログの保存期間を1年にしても保存領域の容量不足は発生しないことが分かったので，これらのフィルタリングルールの修正案を適用することにした。

最後に，DMZ に設置されたサーバへのウイルス対策ソフトの導入について検討した。検討の結果，導入してもサーバの動作に悪影響がないことを確認できたので，導入することにした。

〔専門加工業者への CAD データの送信方法の検討〕

J 課長と K さんは，専門加工業者への CAD データ送信方法について，安全でかつ注文から納品までの時間を短縮できる電子的な方法を改めて検討することにした。現在使っているメールに添付して送信する方法では誤送信が問題になっていたが，誤送信を防止する確実な方法は見つけられなかった。そこで，他の方法を調査したところ，T 社が販売している，ファイル交換専用装置（以下，専用装置という）が見つかり，専用装置を DMZ に設置する前提で検討を進めた。

専用装置の仕様概要を図3に示す。

1. 利用者インタフェース及び認証方法について
・管理者並びに送信者及び受信者（以下，送信者と受信者を併せて利用者という）向けに Web インタフェースがあり，HTTP 及び HTTPS が使用できる。
・管理者は，利用者のメールアドレスを利用者 ID として登録する。
・管理者及び利用者の認証は，HTTP の場合はパスワード認証を，HTTPS の場合は，パスワード認証に加え，［ h ］認証を使用することができる。
2. データ送信方式について
利用者が使用するデータ送信方式として，URL 送信方式とデータ共有方式の 2 方式がある。
・URL 送信方式
送信者がファイルをアップロードすると，専用装置が，ダウンロード用のランダムな文字列を含む URL を受信者宛てにメールで送信する。ダウンロード後，ファイルは自動的に削除される。送信者は，ダウンロードの有効期間を指定できる。
・データ共有方式
管理者は，ファイル交換のためのフォルダを作成し，フォルダに対する利用者ごとの権限を設定する。
3. 他の機能
管理者は，次の機能を設定できる。
・上長承認機能
送信者の上長が承認した後に，ダウンロードが可能になる。管理者は，各利用者の上長及び上長代行者を登録する。
・アクセス制御機能
利用者ごとに IP アドレスを登録しておき，その IP アドレスからのアクセスだけを許可する。
・ログ機能
Web インタフェースへのアクセス，メールでの URL 送信，アップロード及びダウンロードのログを記録する。管理者は，Web インタフェースを使用して，ログをダウンロードする。
・ウイルススキャン機能
ウイルススキャン機能では，アップロード時及びダウンロード時にウイルススキャンを行う。

図３　専用装置の仕様概要

J 課長と K さんは，図 3 の 1. については，通信の暗号化が必要であるので，HTTPS を使用することにした。また，［ h ］認証を使用することにし，［ h ］証明書の発行は，商用サービスを使用することにした。

次に，図 3 の 2. について検討した。専門加工業者から CAD データを受け取ることはないので，URL 送信方式がよいと K さんは説明した。J 課長は，K さんの説明に同意した。

さらに，図 3 の 3. については，各機能を使用することにした。

これらの検討の結果，⑥専用装置での CAD データの送信は，メールへの添付による送信と比べると，誤送信の防止や復号用パスワードの漏えい防止以外にも利点があることが分かった。

最後に，FW-A のフィルタリングルールに専用装置についてのルールを追加する案

を作成した。

J 課長は，検討した対策を M 役員に報告した。M 役員は，報告にある対策の他に，PC への対策を強化することを条件に承認した。

J 課長と K さんは，M 役員の指示について検討を行った。D 社のネットワーク構成を考慮して，⑦ウイルスの活動による PC からインターネットへの通信のうち，止めることはできないがログの分析によって検出できる通信と，⑧ウイルスの活動による PC からインターネットへの通信のうち，止めることはできるがログを分析しても検出できない通信に整理し，PC への対策の検討を開始した。3 か月後，PC への対策を完了した。

設問 1　〔公開 Web サーバのコンテンツ改ざんと対処〕について，(1)～(3)に答えよ。

(1)　本文中の下線①について，調査が困難になるのはなぜか。25 字以内で述べよ。

(2)　図 2 中の下線②について，バックアップメディアを用いてコンテンツの復元を行わない理由を 45 字以内で述べよ。

(3)　本文中の下線③について，追加した適用対象を 15 字以内で答えよ。

設問 2　〔公開 Web サーバのコンテンツ更新方法の見直し〕について，(1)，(2)に答えよ。

(1)　本文中の［ a ］に入れる適切なプロトコル名を，英字 6 字以内で答えよ。

(2)　本文中の下線④について，変更することにした項目の項目名を答えよ。また，変更後の内容を，図 1 中の字句を用いて答えよ。

設問 3　〔プロキシサーバの設定の見直し〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑤について，不都合が生じる業務を行う課を答えよ。また，不都合の内容を 45 字以内で具体的に述べよ。

(2)　表 7 中の［ b ］～［ d ］に入れる適切な接続先を答えよ。

設問 4　表 8 中の［ e ］～［ g ］に入れる適切な字句を答えよ。

設問 5　〔専門加工業者への CAD データの送信方法の検討〕について，(1)～(4)に答えよ。

(1)　図 3 中及び本文中の［ h ］に入れる適切な字句を 10 字以内で答えよ。

(2)　本文中の下線⑥について，利点とは何か。30 字以内で述べよ。

(3)　本文中の下線⑦の通信を二つ挙げ，それぞれ 50 字以内で述べよ。

(4)　本文中の下線⑧の通信を，35 字以内で述べよ。

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。
9. 試験時間中，机上に置けるものは，次のものに限ります。
   なお，会場での貸出しは行っていません。
   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬
   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。

試験問題に記載されている会社名又は製品名は，それぞれ各社又は各組織の商標又は登録商標です。
なお，試験問題では，™ 及び ® を明記していません。

©2014　独立行政法人情報処理推進機構