# 平成１８年度　春期　システム監査技術者　午後Ⅰ問題

次の問 1，問 2 は必須問題です。

**問１**　個人情報保護への取組と内部監査に関する次の記述を読んで，設問 1～3 に答えよ。

E 社は，情報機器の販売などを行っている中堅企業である。約 1,200 名の正社員と派遣社員を抱え，業績を順調に伸ばしてきている。社長は，個人情報保護法の全面施行に先立ち，個人情報保護のための社内の仕組みやルールを整備する必要があると考え，総務担当の役員を個人情報保護管理者に任命し，個人情報保護への取組を開始した。取組を開始してから約半年が経過し，個人情報保護に関する内部監査が，監査部によって行われた。

〔E 社の組織と業務概要〕

E 社には，機器販売事業部，ソフトウェア事業部及び顧客サービス事業部がある。

・機器販売事業部は，情報機器の販売を担当し，PC とその周辺機器を取り扱っている。顧客は，主に中小企業であり，顧客数は 1,000 社を超えている。1 か月前から，Web を利用した情報機器の販売を開始した。
・ソフトウェア事業部は，機器販売事業部が販売した PC にインストールされた簡単な業務ソフトウェアを稼働させる事業からスタートし，現在では，ネットワークを利用した情報システムの開発・保守，及び各種ソフトウェアパッケージ(以下，パッケージという)の販売を行っている。顧客数は，パッケージ販売先を含めると 2,000 社を超えている。
・顧客サービス事業部は，機器販売事業部が販売した情報機器の保守サービスを行うとともに，2 年前から情報機器やソフトウェアに関するセミナを開催している。機器販売事業部及びソフトウェア事業部の顧客に対するダイレクトメール(以下，DM という)の効果もあって，セミナの受講者数は年々増加し，受講者名簿には 2,000 名以上が登録されている。

E 社が保有している個人情報によって識別される特定の個人の数は，5,000 人を超えており，E 社は，個人情報保護法における個人情報取扱事業者に該当している。

〔E 社における個人情報保護への取組〕

(1)　個人情報保護管理者に任命された総務担当の役員は，総務部を中心に個人情報保護推進事務局を設置した。
(2)　個人情報保護推進事務局は，約 2 か月間で，E 社の個人情報保護方針及び個人情報管理規程を作成し，社長の承認を得た。作成した個人情報保護方針を顧客向けホームページに掲載するとともに，個人情報管理規程を，役員を含む全従業者に通知した。
(3)　個人情報保護に関する社内文書は，個人情報保護方針及び個人情報管理規程のほか，個人情報取扱マニュアル，各種様式類及び記録類から構成されている。
(4)　個人情報管理規程では，各事業部とスタッフ部門に個人情報部門管理者を設置すること，及び取り

扱っている個人情報ごとに取扱責任者を定めることとしている。

(5) 個人情報取扱マニュアルは，取扱責任者が作成し，個人情報部門管理者が承認する手続になっている。

〔個人情報の特定〕

E 社では，個人情報管理規程に基づき，各事業部が取得・収集と保管を行っている個人情報を調査し，個人情報を含むファイル，データベース及び文書類を洗い出した。洗い出された個人情報は，各事業部において，管理台帳に登録し，個人情報として特定した。

現時点で特定されている個人情報は，表のとおりである。

表　特定されている個人情報

| 事業部名 | 特定されている個人情報 |
|---|---|
| 機器販売事業部 | 登録はがき，販売先の顧客データベース，販売実績一覧表，<br>見込顧客リスト，名刺データベース |
| ソフトウェア事業部 | 開発・保守先の顧客データベース，ユーザアンケートの回答，<br>パッケージ販売先の顧客データベース |
| 顧客サービス事業部 | 修理依頼書，保守契約先の顧客リスト，セミナ講師リスト，<br>受講者名簿，受講者アンケートの回答，セミナ案内データベース |

注　上記以外に，人事部では役員を含む全従業者の個人情報を管理台帳に登録し，特定している。

個人情報ごとの取扱責任者が，管理台帳に，個人情報のタイトル名，利用目的，利用期間，保管場所などを記入し，個人情報部門管理者が，リスクの評価と対策の妥当性を確認することになっている。個人情報管理規程では，半年に 1 回，各事業部とスタッフ部門で個人情報を洗い出し，特定する手続になっている。

〔内部監査の実施〕

今回の個人情報保護に関する内部監査は，監査部でシステム監査を担当している F 課長がリーダとなって行われた。F 課長は，E 社にとって顧客の個人情報保護が重要であると考え，監査部長の承認を得て，各事業部における“個人情報の取得・収集と保管”及び“個人情報の利用と提供”についての点検と評価を監査テーマとした。今回の個人情報保護に関する内部監査で把握された事実は，次のとおりである。

〔個人情報の取得・収集と保管〕

(1) 機器販売事業部では，顧客からの登録はがきを基に，顧客情報をデータベース化していた。登録はがきには，“お客様の個人情報は，弊社の保守サービスに利用させていただきます”と記載されていた。データベースへの入力担当者は，登録はがきを地域別に五十音順に整理して入力していた。入力が完了した登録はがきはそのまま箱詰めにされ，来訪者が頻繁に通る廊下に置かれていた。

(2) 機器販売事業部では，Web を利用した機器販売システムによっても，個人情報の取得・収集を開始したが，管理台帳への登録はなく，個人情報部門管理者は，取得・収集の開始を認識していなかっ

た。E 社では，機器販売システムの運用を委託しているデータセンタの入退管理などの実施状況を確認したことはなかった。

(3) ソフトウェア事業部が実施しているパッケージ販売先のユーザアンケートには，“お客様の個人情報は，弊社にて大切に取り扱わせていただきます”と記載されていた。利用目的については，顧客向けホームページも含め，記載されていなかった。

(4) ソフトウェア事業部で，複数の開発プロジェクトの管理者数名にヒアリングを行った結果，プロジェクトによっては，顧客から預かった数千件の個人データを共有サーバに保管しているとのことであった。その共有サーバへは，プロジェクト関係者以外もアクセス可能であった。また，個人データを保存したフォルダへのアクセス制限も特に行っていなかった。ソフトウェア事業部の個人情報部門管理者は，顧客から個人データを預かっていることは知っていたが，個人情報の取得・収集と保管に該当するとは判断せず，事業部として管理対象外にしていた。

(5) 顧客サービス事業部が扱っている修理依頼書には，セミナ案内の送付希望の同意欄があり，同意が得られた顧客の個人情報をセミナ案内データベースに登録していた。セミナの受講者アンケートには，“弊社のセミナに関するご案内を希望者にお送りします”という記載があった。受講者アンケートの回答を基に，セミナ案内データベースに個人情報を追加登録していた。

〔個人情報の利用と提供〕

(1) 機器販売事業部では，顧客サービス事業部が個人情報を登録したセミナ案内データベースを利用して，PC 新製品のカタログを送付していた。

(2) ソフトウェア事業部では，パッケージ販売先のユーザアンケートの回答から作成した顧客データベースを利用して，ソフトウェアのパンフレットを送付していた。

(3) ソフトウェア事業部では，顧客データベースへのアクセス権限について，事業部内の正社員には個人単位に利用者 ID 及びパスワードを付与し，派遣社員には派遣元の会社単位に共用の利用者 ID 及びパスワードを付与していた。

(4) 顧客サービス事業部では，以前から，ほかの事業部の顧客データベースを利用して，セミナ案内の DM を送っていた。近年は，自事業部のセミナ案内データベースも利用して，セミナ案内の DM を送っていた。

(5) 顧客サービス事業部の受講者名簿及び受講者アンケートの回答を，受講者の同意を得ずに，講師及び講師の所属会社に提供していた。

**設問１**　E 社での個人情報の取得・収集と保管，利用と提供において，個人情報取扱事業者の義務に違反すると判断される事項を二つ挙げ，それぞれ 40 字以内で述べよ。

**設問２**　E 社の個人情報の取扱いにおいて，安全対策の不備について指摘すべき点を二つ挙げ，不備によって発生するリスクも含めて，それぞれ 60 字以内で述べよ。

**設問３**　E 社における個人情報の特定には，幾つかの問題点がある。監査指摘事項と考えられる問題点と，その改善策の具体的な内容を，それぞれ 40 字以内で述べよ。

**問２　ホスティングサービスにおけるシステム監査と ISMS に関する次の記述を読んで，設問 1～3 に答えよ。**

A 社はデータセンタを保有し，複数の顧客が共用のサーバ（以下，共用サーバという）を利用する形態のホスティングサービスを提供している。このサービスには，ホームページやメールサービスに加え，不正アクセス対策，ウイルス対策，ファイアウォールの運用管理などのセキュリティサービスも標準で含まれている。

A 社のホスティングサービスの顧客である M 社は，個人情報保護法の全面施行を契機に，セキュリティ対策の見直しを行っていた。M 社は，その一環として，自社の求めるセキュリティ要件を記載した質問票を A 社に送付し，回答を求めた。質問票には，個人情報の取扱いを含め，A 社が提供するホスティングサービスの運用と監査の実施に関する要求が含まれていた。

A 社では，質問票に掲げられた項目のうち，ホスティングサービスの運用に関する項目については，運用部門の B 部長が，部下に回答の作成を指示した。

監査実施に関する項目については，監査部長が，監査に精通している C 君と新人の D 君に回答の作成を指示した。監査部長は，運用部門の回答内容によっては，A 社が標準として提供しているサービスを超えた運用が必要になることも考えられるので，運用部門が作成した回答にも目を通しておくよう C 君に指示した。

〔ホスティングサービスの運用に関する M 社の要求事項と A 社の検討結果〕

(1)　M 社の要求事項

①　個人情報の削除

ホスティングサービスの契約が終了したときは，アクセスログに含まれる M 社の個人情報を含め，M 社にかかわるすべての個人情報を削除すること

②　個人情報の複製禁止

書面による事前承諾を得ることなく，M 社の個人情報を複写，複製又は加工してはならないこと

③　ログの保管期間

不正侵入検知システム（以下，IDS という）のログを 1 年間保管すること

④　障害時の対策

障害などでホスティングサービスが中断した場合，A 社は直ちにその旨を M 社に報告し，M 社の指示に従って対策を講じること

⑤　定期報告

ファイアウォール及び IDS のログを毎日確認し，不正アクセスされた形跡がないかどうかを日次で報告すること

(2)　A 社の運用状況及び検討結果

①　個人情報の削除

A 社は，サービス提供に際して，顧客の連絡窓口担当者と請求事務担当者の個人情報を取得している。A 社は，契約終了時に，これらの個人情報を顧客データベースから削除している。ログは IP アドレスで顧客を識別できるが，ファイアウォールのパラメタ設定や IDS のアラートレベルなどは顧客別ではない。したがって，ログも顧客別には管理しておらず，特定の顧客のアクセスログを削

除する運用は行っていない。

運用部門で検討した結果，M 社とのサービスの契約終了時には，共用サーバ内の M 社に関するログを消去することにした。

② 個人情報の複製禁止

A 社は，業務上の必要性から，顧客の連絡窓口担当者の個人情報を複製し，業務遂行にかかわる複数部署で使用している。

運用部門で検討した結果，業務遂行上，複製が必要である旨を明記した書面を作成して，M 社から承諾を得ることにした。

③ ログの保管期間

A 社は，IDS のログを 6 か月間保管している。

運用部門で検討した結果，IDS のログの保管期間を 1 年間に変更した。

④ 障害時の対策

共用サーバで運用しているので，ホスティングサービスにおいて障害が発生した場合の影響は，ホスティングサービスのすべての顧客に及ぶ。障害が発生した場合，A 社は直ちにその旨を顧客の連絡窓口担当者全員にメールで報告し，以降，障害の復旧まで適時報告を行っている。

運用部門で検討した結果，現在もすべての顧客に対して障害発生時から復旧までの間，迅速に報告しており，現行どおりの運用で問題ないと判断した。

また，障害時の対策について M 社の指示に従っても問題はないと判断した。

⑤ 定期報告

不正アクセスが検出された場合は，A 社からすべての顧客に対して即時に報告されるが，不正アクセスがなかった場合の日次報告は行っていない。

運用部門で検討した結果，M 社に対してだけ日次報告することにした。

(3) 運用部門の作成した回答に対する C 君の検討結果

B 部長の部下は，ホスティングサービスの運用に関する M 社の要求事項は個別運用を徹底すれば実現可能なので，すべて受け入れる旨を B 部長に報告していた。しかし，C 君は，これらの要求事項を受け入れた場合の影響を運用部門が考慮しているかどうかを懸念した。C 君は，運用部門の検討結果に対して，想定し得る幾つかの問題を監査部長に報告した。

〔監査実施に関する M 社の要求事項と A 社の検討結果〕

(1) M 社の要求事項

① ホスティングサービスの運用について，年 1 回監査を実施すること

② 監査項目には，質問票に記載されている M 社の要求事項をすべて含めること

③ M 社に監査結果を報告すること

(2) A 社の監査の状況及び検討結果

A 社では，年度初めに監査部が監査基本計画書をまとめ，社長の承認を得る手続になっている。ホスティングサービスは A 社にとって重要なサービスなので，毎年監査の実施対象とされている。ホスティングサービスにかかわる監査項目は，個別計画において詳細を定めることになっているので，M 社の要求事項をすべて含めることは可能である。そこで，C 君は，M 社の要求には応じられると考えた。

C 君は，被監査部門である運用部門の B 部長に，年 1 回の監査の実施と M 社へ監査結果の報告を行いたい旨を伝え，同意を得た。C 君は，また，M 社の今回の要求に応じることに問題はないことを監査部長にも報告した。

(3)　昨年度の監査と B 部長が行った M 社への監査結果の提出

検討の過程で，昨年度，B 部長が M 社からの求めに応じて，ホスティングサービスの運用状況に関する内部監査報告書を提出していたことが分かった。

昨年度の監査は，A 社がホスティングサービスのサービスレベルとして顧客に開示している項目に関する準拠性監査であり，M 社に特定した監査ではない。内部監査報告書には，障害対処時における問題点やシステム変更作業の結果報告に対する承認漏れなどが指摘事項として記載されていたが，これらは顧客の業務に直接影響を与えるものではなかった。

M 社との間では，監査結果の開示に関する契約上の取決めはなかった。昨年度は B 部長の判断で内部監査報告書の電子データをフロッピーディスクにコピーし，書込み禁止やコピー禁止などの措置をせずに M 社に提出していた。

C 君は，昨年度，B 部長の判断で M 社に内部監査報告書が提出されていることを監査部長に報告した。さらに，監査結果の開示に関する規則が整備されていなかったことから，C 君は，監査結果の開示に関する社内規則案も併せて提案した。

(4)　ISMS 認証の利用の検討

この検討過程において，D 君は，A 社のホスティングサービスは ISMS 適合性評価制度の認証も取得しているので，M 社にその認証取得を示すことで，監査結果の報告に代えられるのではないかと考えた。D 君は，ISMS 認証基準では定められた間隔での監査実施が要件であること，及び ISMS 認証取得は外部機関の保証であることから，内部監査の結果よりも客観性があるのではないかと考えた。C 君も，ISMS 認証取得は，A 社のホスティングサービスの信頼性を顧客に示す方法の一つであると考えている。しかし，ISMS 適合性評価制度と内部監査との違いから，ISMS 認証取得を示すだけでは M 社の要求を満たすことができない理由を，D 君に説明した。C 君の説明内容は，監査部長の考えとも一致していた。

**設問１**　M 社の要求事項に対する運用部門の検討結果に関して，C 君が監査部長に報告したと想定される問題点を二つ挙げ，それぞれ 55 字以内で述べよ。

**設問２**　昨年度，B 部長の判断で行われた M 社への内部監査報告書の提出には，幾つかの問題点がある。監査結果の開示に関して定めておくべき事項を二つ挙げ，それぞれ 35 字以内で述べよ。

**設問３**　C 君は，ISMS 認証取得を示すだけでは M 社の要求を満たせない理由を D 君に説明した。その理由について，ISMS 認証の審査と内部監査との基本的な違いを含め，80 字以内で述べよ。

次の問 3，問 4 については 1 問を選択し，答案用紙の選択欄の問題番号を○印で囲んで解答してください。
なお，2 問とも○印で囲んだ場合は，問 3 について採点します。

**問３　プログラム変更手続の監査に関する次の記述を読んで，設問 1～4 に答えよ。**

K 社は，中堅の証券会社である。K 社は早くから業務のコンピュータ化に取り組み，現在，多くの業務プロセスが情報システムによって支えられている。したがって，K 社においては，情報システムに障害が発生した場合，業務に多大な影響を及ぼす。そこで，K 社の内部監査部では，情報システムの監査を定期的に実施しており，本年度も監査計画に従って，既存情報システムのプログラム変更手続に関する監査を行うことにした。

〔K 社の情報システム部門と情報システムの概要〕

K 社の情報システム部門は，システム企画部，システム開発部及びシステム運用部の 3 部門である。システム企画部は，K 社全体の情報化戦略の策定，それに基づく情報システム中長期計画の立案，及び各年度におけるシステム開発計画の策定を主要な業務としている。システム開発部は，システムの開発及び保守が主業務であり，第一課と第二課の二つの課によって，担当するシステムを分けている。システム運用部は，既存システムのオペレーションや稼働監視などの運用業務を担当している。

K 社の主要な情報システムは，顧客からの売買注文を処理する注文・約定処理システム，顧客の預り資産を管理する顧客管理システム，各証券取引所や金融機関，顧客などのコンピュータとの接続を担う対外接続系システム，各種有価証券に関する情報や投資分析機能を提供する情報系システムなどである。これらのシステムは，すべてクライアントサーバシステムで実現されている。

〔K 社のプログラム変更手続の概要〕

プログラム変更は，システム開発管理規定に則って，次のように行われる。

(1)　システム改善依頼の申請

既存情報システムについて，機能の変更や追加ニーズが発生した場合に，システムオーナであるユーザ部門において，システム改善依頼書が作成され，部門長の承認後にシステム企画部に提出される。

(2)　対応時期の決定

システム企画部は，ユーザ部門から受領したシステム改善依頼書の内容を精査し，システム開発の年間計画との整合性を確認した後，対応時期を決定する。システム企画部は，その結果をユーザ部門に通知するとともに，システム改善依頼書をシステム開発部に回付する。

(3)　開発作業の実施

システム開発部は，ユーザ部門に詳細な要件を確認後，プログラム変更要件定義書を作成する。該当システムの開発を所管する課の課長がこのプログラム変更要件定義書を承認後，これに基づいてプログラム開発及びテストを実施する。

(4)　ユーザ承認

システム開発部におけるテストが終了後，依頼元であるユーザ部門が受入テスト（ユーザアクセプタンステスト：UAT）を実施し，受入可能と判断した場合は，ユーザ部門の部門長が承認する。この

とき，ユーザ部門の担当者によって，システム利用マニュアルや業務マニュアルの修正が行われる。ただし，システム開発部においてユーザへの影響度が小さいと判断された場合，UAT は省略され，システム開発部から該当ユーザ部門に対して，電子メールでプログラムのリリースが通知される。

(5)　プログラムの本番移行

UAT が終了し，ユーザ部門の承認を受けたプログラムは，プログラム開発担当者によってリリース用ライブラリに移される。また，UAT が省略されたプログラムについても，ユーザ部門への電子メールの通知後，プログラム開発担当者によってリリース用ライブラリに移される。システムの本番環境と開発環境は物理的に分離されており，リリース用ライブラリは開発環境に存在する。その後，システム運用部のライブラリアンが，リリース用ライブラリに移されたプログラムを，月に 1 回のシステム定例更新日に，本番環境のプログラムライブラリに移行する。

(6)　プログラムのバックアップ

本番環境への移行時には，移行前のプログラムのバックアップコピーがテープに取得される。バックアップコピーの保存期間は 1 週間である。プログラムは，移行作業終了後，直ちにリリース用ライブラリから削除される。

〔システム監査の結果〕

内部監査部は，上記プログラム変更手続に関して，関連する書類のレビューを実施し，システム企画部，システム開発部及びシステム運用部の担当者にインタビューを行った。その結果，次のような問題点が発見された。

①　緊急時のプログラム変更に関し，障害の原因となったプログラムのバグを修正した場合の原因調査からプログラム修正，本番移行までの手続が，明文化されていない。

②　月次バッチ処理など，プログラムによっては，本番移行後 1 週間以上たって初めて稼働するものがある。プログラムのバックアップコピーの保存期間を 1 週間としているので，プログラム稼働後にバグが見つかった場合に，リリース前のバックアップがなく，リリース前の状態に戻せない可能性がある。

③　プログラムを変更した場合に関連仕様書を修正すべきであることが，定められていない。

④　リリース用ライブラリに移行されたプログラムは，削除されるまでの間，システム開発部の開発担当者によって更新可能である。

内部監査部は，これらの問題点のうち，①が特に重大であると考え，追加調査を実施することにした。内部監査部が，担当者へのインタビューによって把握した緊急時のプログラム変更は，次のように実施されている。

〔緊急時のプログラム変更の現状〕

(1)　システム障害や誤作動などのトラブルが発生した場合，ユーザ部門又はシステム運用部などの発見部署からシステム開発部に連絡される。

(2)　システム開発部は，障害や誤作動の原因を本番環境において調査する。このとき，システム運用部が管理している OS 及びデータベースに関する原因調査用のアカウントとパスワードを使用する。

なお，本番環境へのアクセスは，すべてログに保存される。

(3)　アプリケーションプログラムが原因の場合は，システム運用部のライブラリアンが，該当プログラムを本番環境から開発環境にあるリリース用ライブラリにコピーする。
(4)　開発環境においてバグを修正し，テストを完了したプログラムは，開発担当者によってリリース用ライブラリにある修正前のプログラムと入れ替えられる。
(5)　ライブラリアンは，リリース用ライブラリに移されたプログラムを本番環境に移行する。これは月1回のシステム定例更新とは異なり，リリース用ライブラリにおけるプログラムの入替えが終了次第実施する。

内部監査部は，〔緊急時のプログラム変更の現状〕を評価する過程で，最近発生した障害において，次のような問題を発見した。

あるプログラムについて，ユーザ部門からシステム改善依頼書を受領して，開発環境において修正作業を実施中であった。この修正中のプログラムに，本番環境で重大なバグが発見された。システム開発部は，本番環境にある当該プログラムを〔緊急時のプログラム変更の現状〕の手順で修正し，本番環境に反映させた。その後，システム改善依頼に基づいて修正を完了した当該プログラムが，通常のプログラム変更手続に従って本番環境に移行された。しかし，移行されたプログラムには，緊急変更時に対応したバグの修正が実施されていなかったので，対応したはずのバグによるシステム障害が再発した。

内部監査部は，これを重大な問題と見なし，システム開発部に対して，解決の対応策をすぐに検討するように指示した。

**設問１**　K 社のプログラム変更手続には，〔システム監査の結果〕で挙げられたもの以外にも，幾つかの問題点がある。〔K 社のプログラム変更手続の概要〕に記述されている内容から，問題と思われる点を一つ挙げ，50 字以内で述べよ。

**設問２**　〔システム監査の結果〕で挙げられた③及び④の問題点について，このまま放置した場合には，どのようなリスクがあるか。それぞれ 50 字以内で述べよ。

**設問３**　〔緊急時のプログラム変更の現状〕によれば，システム運用部が管理している本番環境の OS 及びデータベースに関するアカウントとパスワードを，システム開発部が使用している。システム運用部は，この作業終了後に，開発担当者の不正防止の観点からどのようなコントロールを実施すべきか。最も効果的なものを一つ挙げ，50 字以内で述べよ。

**設問４**　〔緊急時のプログラム変更の現状〕を評価する過程において発見された問題点について，どのような対応策をとるべきか。60 字以内で述べよ。

**問４　災害時対応計画を対象としたシステム監査に関する次の記述を読んで，設問 1～3 に答えよ。**

X 社は，個人向け医療保険の通信販売を行っている保険会社である。X 社の経営者は，事業を拡大するためには情報システムの活用が不可欠と考えている。

X 社の主要な情報システムは，本社とは別の建物に設置されたコンピュータセンタで運用されている。また，災害の発生などによってコンピュータセンタが使用できなくなる場合を想定して，遠隔地のコンピュータ専用施設にバックアップセンタを確保し，災害時用の代替システムの機器を設置している。コンピュータセンタの管理と情報システムの運用は，X 社の情報システム部が行っている。一方，バックアップセンタには X 社の社員は常駐しておらず，コンピュータ専用施設の運営業者に管理を委託している。

情報システムに問題が生じると多くの業務に支障を来すので，X 社の情報システム部では，コンピュータセンタが被災した場合を想定した災害時対応計画を作成している。

〔災害時対応計画にかかわるシステム監査の実施〕

X 社の内部監査部は，自社の業務における情報システムの重要性を踏まえて，情報システムの開発と運用について，システム監査を定期的に実施している。今年度のシステム監査のテーマは，災害時対応計画が被災時に有効に機能するかどうかの評価とした。

監査担当者は，このテーマに基づいて，“災害時対応計画に記載されている情報システム切替えの方針”，“災害時対応計画のテスト実施状況”，及び“災害時対応計画の見直しと修正内容の周知”を中心に監査することにした。監査担当者は，これらの観点から，情報システム部の責任者へのインタビューと，災害時対応計画及びそのテストにかかわる文書のレビューを実施し，次の事項を把握した。

〔災害時対応計画に記載されている情報システム切替えの方針〕

災害時対応計画では，次のように定められている。

(1) 災害時対応計画は，被災によってコンピュータセンタを使用できなくなった場合，バックアップセンタに設置した代替システムを使用して，主要な情報システムを迅速に復旧することを主な目的とする。目標とする復旧時間は，災害の発生から 24 時間以内とする。

(2) 代替システムへの切替対象となる情報システムは，業務及び情報システムの重要度分析に基づいて情報システム部と利用部門との協議によって決定する。代替システムの機器は，切替後の運用に必要な処理能力を十分に確保できるように選定する。

(3) バックアップセンタには，代替システムがコールドスタンバイで用意される。また，バックアップセンタには，切替後のシステム運用に必要なデータを記録した媒体を定期的に搬送し，関連する資料及び備品を常備しておく。

(4) 情報システム部が，災害時対応計画のテストを定期的に実施し，その結果を評価して災害時対応計画を見直す。

(5) 被災時にバックアップセンタで作業を行う担当者（以下，災害対応要員という）は，担当業務や経験年数にかかわらず，自宅がバックアップセンタに近い者を優先して選定する。災害対応要員の一覧表は，災害時対応計画に記載され，毎年度末に更新する。

(6) コンピュータセンタからバックアップセンタへの切替え，及びバックアップセンタからコンピュー

タセンタへの切替えは，情報システム部長の判断に基づき社長の承認を得て実施しなければならない。

(7) 復旧作業中は，公衆電話回線を使用した固定電話又は携帯電話を使用して，コンピュータセンタ，バックアップセンタ及びX社本社間で，随時連絡を取り合う。

〔災害時対応計画のテスト実施状況〕

(1) 災害時対応計画のテストは，ここ数年は年に1回実施されている。

(2) テスト対象の情報システムは，情報システム部と利用部門との協議によって選定されており，3年程度で，代替システムへの切替対象となる全情報システムを一巡するようになっている。

(3) 対象となる情報システムが選定されると，情報システム部がテスト計画書を作成する。

(4) 今年度のテストは，災害時対応計画で定められた時間内に，バックアップセンタに，災害対応要員全員が集合できたという前提の下に実施された。

(5) 今年度のテストでは，情報システムの切替えに必要なデータ媒体は，コンピュータセンタから搬送された。

(6) テスト対象の情報システムについて，バックアップセンタへの切替手順及びコンピュータセンタへの切替手順が，今年度を含め毎回確認されている。

(7) 今年度のテストは，X社の情報システム部で最も熟練した運用担当者が中心となって，情報システムの切替作業を実施した。

(8) 作業を実施した熟練者には，災害対応要員はほとんど含まれていなかった。情報システムの切替作業は，災害時対応計画の一部として用意されている手順書に従って実施することになっている。ただし，今年度のテストでは，熟練者が作業を行っているので，手順書を確認することもなく作業が進められた部分が多かった。

(9) 情報システムの切替作業は，コンピュータセンタとバックアップセンタ間で固定電話と携帯電話を使用し，随時確認を取りながら実施された。テストの結果，目標時間内に情報システムの切替えが可能であることが確認された。

〔災害時対応計画の見直しと修正内容の周知〕

災害時対応計画では，次のように定められている。

(1) 情報システム部は，災害時対応計画のテスト完了後，その結果を評価し，テスト結果報告書にまとめる。

(2) テスト結果報告書に基づいて，必要に応じて，災害時対応計画を修正する。修正内容と修正箇所は，災害時対応計画の修正履歴に記載する。

(3) 災害時対応計画は，イントラネットを利用して関係者に開示する。また，その印刷文書を，コンピュータセンタとバックアップセンタに保管する。

(4) 災害時対応計画を修正した場合，情報システム部の修正担当者がイントラネットで公開している災害時対応計画を差し替え，その旨を，関係者に電子メールで通知する。また，修正担当者は，災害時対応計画の修正ページを，コンピュータセンタとバックアップセンタの責任者に送付し，各センタに保管されている災害時対応計画の該当ページの差替えを依頼する。

監査担当者は，災害時対応計画に定められているとおりに見直しと周知が実施されているかどうかを

確認した。

〔監査担当者が設定した監査目的〕

(1)　災害時対応計画の内容を，規定どおりに見直しているかどうかを確認すること

(2)　コンピュータセンタとバックアップセンタに保管されている災害時対応計画が，適切に差し替えられているかどうかを確認すること

**設問１**　〔災害時対応計画に記載されている情報システム切替えの方針〕に記載されている内容には，幾つかの問題点がある。考えられる問題点を二つ挙げ，その内容をそれぞれ 40 字以内で述べよ。

**設問２**　〔災害時対応計画のテスト実施状況〕に記載されている今年度のテストの内容には，〔災害時対応計画に記載されている情報システム切替えの方針〕に規定されている情報システムの切替えの実効性を確認する上で不十分な点がある。不十分と考えられる点を二つ挙げ，それぞれ 50 字以内で述べよ。

**設問３**　〔監査担当者が設定した監査目的〕に記載されている(1)又は(2)のいずれかの項目番号を選択して解答欄に記入し，監査担当者が実施したと考えられる監査手続の内容を，70 字以内で述べよ。