平成１８年度　春期　システム監査技術者　午後Ⅰ　解答例

問１

設問１

・パッケージ販売先へのユーザアンケートに利用目的が明示されていない。
・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る。
・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 を送付している。
・受講者名簿及びアンケートの回答を受講者の同意なしに講師と所属会社に提供している。

設問２

・来訪者が頻繁に通る廊下に登録はがきが置かれており，来訪者などによって登録はがきが持ち出されるリスクがある。
・委託先の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がなく，個人データが漏えいするリスクがある。
・個人データを保存したフォルダへのアクセス制限を行わず，従業者が個人データを見たり持ち出したりするリスクがある。
・派遣社員に共用の利用者 ID 及びパスワードが付与されているので，不正利用した場合に派遣社員を特定できないリスクがある。

設問３

	a 群	b 群
問題点	・機器販売システムにおいて管理台帳に登録せずに個人情報の取扱いが始まっている。 ・Web での販売で個人情報を特定せずに新たに個人情報の取得・収集が始まっている。	・顧客から預かった個人データを個人情報と特定せず，管理対象外にしていた。
改善策	・個人情報を取り扱う際に，その個人情報の取扱責任者を漏れなく定めるルールを作る。 ・新たに個人情報を収集する際に，個人情報部門管理者に事前申請するルールを作る。 ・個人情報の洗い出しの頻度を現状の半年 1 回よりもっと多くする。	・個人情報部門管理者に対して，預託された個人情報を特定することを理解してもらう。 ・事業部として，預託された個人情報を管理対象として特定することを明確にする。 ・個人データを特定して管理対象とすることをプロジェクト管理者に徹底する。

※同じ群中の組合せとする

* ----------*

問２

設問１

・個別に顧客対応することによって提供サービスの標準運用が崩れ，コスト高となること
・個別に顧客対応することによって提供サービスの標準運用が崩れ，運用にミスが生ずるおそれが増すこと
・アクセスログの部分的な削除は，ログの連続性，完全性を損ねるので実施すべきではないこと
・M 社の指示に従うことがサービスを利用している他社に対して適切であるとは限らないこと

設問２

・開示先の可否に関する社内承認手続を定めること
・開示する範囲について社内承認手続を定めること
・開示する報告書の開示先における取扱条件を定め，書面で通知すること
・電子データで提供する場合は，修正ができないようにすること

設問３

・ISMS 認証の審査基準はあらかじめ定められているので，ISMS 認証では M 社の要求事項の実施状況が示されない。
・ISMS 認証はセキュリティレベルの高低を評価基準に含まないので，ISMS 認証では M 社の求めるセキュリティレベルの評価が得られない。

* ----------*

問３

設問１

・プログラム変更要件定義書についての承認が，開発部の課長だけで，該当ユーザ部門の承認がない。
・UAT の省略について，システム開発部の判断だけで実施しており，該当ユーザ部門の承認がない。

設問２

③・プログラムと仕様書の不整合が発生し，その後のプログラムの修正作業に誤りが起こりやすくなるリスク
・プログラムと仕様書の不整合が発生し，その後のプログラムの修正作業に時間がかかるリスク

④・開発担当者が不正なプログラムをリリース用ライブラリに移し，本番でそれが実行されてしまうリスク
・開発担当者が誤ってリリース用ライブラリを更新し，未承認のプログラムが本番で動いてしまうリスク

設問３

・システム開発部が使用した OS 及びデータベースに関するアカウントのパスワードを変更する。
・システム開発部が使用した OS 及びデータベースに関するアカウントを使用不能にする。
・アクセスログを調査し，システム開発部が不必要なリソースにアクセスしていないかを確認する。

設問４

・同一のプログラムに対する別作業での変更の有無が判断できるように，プログラム単位の修正の管理簿を作成して管理する。
・ライブラリ管理プログラムを導入し，修正中のプログラムに対する別の修正要件が発生した場合に，発見できるようにする。

*** ----------***

問４

設問１

・災害対応要員が，住所からバックアップセンタへの距離だけを基準に選定されている。
・災害対応要員の一覧表が，要員の異動や変更の都度，更新されていない。
・権限者不在時の，情報システムの切替えの判断及び承認の手順が考慮されていない。
・固定電話と携帯電話が両方使用できない場合の連絡方法が，考慮されていない。

設問２

・災害対応要員が，所定の時間内にバックアップセンタに集合できるかどうかがテストされていない。
・情報システムの切替作業で，バックアップセンタに保管されているデータ媒体が使用されていない。
・災害対応要員の大半が，情報システムの切替作業を実施していない。
・情報システムの切替作業について，手順書が使用されなかった部分の内容が適切かどうか確認されていない。

設問３

項目番号（1）…災害時対応計画のテスト計画書とテスト結果報告書をレビューし，テストごとにテスト結果報告書が作成されていることを確認する。
項目番号（2）…修正履歴とコンピュータセンタ及びバックアップセンタに保管されている災害時対応計画を比較し，修正箇所がすべて差し替えられていることを確認する。

注：この解答例に関するメールでのご質問には、応じかねます。あしからずご了承ください。