

問6 IT サービスマネジメントにおける個人情報の保護に関する次の記述を読んで、設問1, 2に答えよ。

X社では、約1万人の個人顧客向けに会員制の通信販売を行っている。注文はインターネットや電話で販売部が受け付け、商品と請求書を宅配便で発送する。顧客からの問合せなども、一括して販売部で受け付けている。顧客情報は、X社の基幹サーバで一括管理している。

X社の顧客管理部では、次の業務①～③を行っている。業務①は、顧客への定期的な取引状況の報告である。業務②及び③は、販売部での対応範囲を超えた問合せであり、顧客管理部に転送されてくる。

業務① 取引明細など顧客あて郵便物の印刷・発送

業務② 取引の詳細な内容や会員登録状況の照会など顧客からの問合せへの対応

業務③ 住所変更や退会など顧客からの訂正・削除・利用停止などの依頼への対応

業務①の印刷・発送の作業で使っている機器が老朽化し、最近では故障が増えている。X社の役員から“機器更新などの対応も含めて業務①～③の外部委託を検討するように”との指示を受けた顧客管理部長は、自身をリーダーとして、顧客管理部、システム部及びリスク管理部の管理者からなる委託検討プロジェクト（以下、プロジェクトという）を発足させた。

設問1 プロジェクトでは、まず委託元であるX社内での対応を検討することにした。

次の記述中の に入れる正しい答えを、解答群の中から選べ。

プロジェクトでは、“個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン”（以下、ガイドラインという）に沿った管理水準で検討を進めることにした。

個人データの取扱いの委託に当たっては、法とガイドラインに基づく安全管理措置（表にその概要を示す）を委託先に遵守させるために必要な a し、業務開始後は委託元が b する必要がある。

表 安全管理措置の概要

安全管理措置	安全管理措置の内容（概要）
組織的安全管理措置	・ 規程等の整備と規程等に従った運用 ・ 安全管理措置の評価，見直し及び改善
人的安全管理措置	・ 非開示契約の締結 ・ 教育，訓練の実施
物理的安全管理措置	・ 入退館，入退室管理の実施 ・ 盗難等の防止 ・ 機器・装置等の物理的な保護
技術的安全管理措置	・ 情報システムへのアクセス制御 ・ 不正ソフトウェア対策 ・ 情報システムの監視

業務①～③について，リスクに対する費用対効果の面から総合的に検討した。

その結果，業務①については機器の買換えではなく外部委託とすることにした。

一方，業務②及び③については社内処理を継続することにした。その理由として，例えば表の安全管理措置のうち技術的安全管理措置について，cなどの対応を考慮する必要があったことによる。

プロジェクトとしてこのように結論を出し，役員に報告した。

a, bに関する解答群

- | | |
|----------------|-----------------|
| ア 委託先の運用担当者を任命 | イ 委託先の従業者を監督 |
| ウ 契約を締結 | エ 個人データの取扱状況を監督 |

cに関する解答群

- ア X 社内の個人データを委託先からアクセスする際の安全性を確保するためにシステムを改修する
- イ X 社の管理水準を満たす専用作業室を委託先に新たに確保する
- ウ X 社の従業者が委託先の個人情報保護管理者となるために委託先で常駐する
- エ X 社の従業者が委託先のシステム運用方法の指揮・命令体制を整備する

設問 2 プロジェクトでは、次に委託先での安全管理措置の現状を調査することにした。

次の記述中の に入れる正しい答えを、解答群の中から選べ。

役員の承認を受けて業務 ① の外部委託が決まり、委託先は印刷・発送業の Y 社に内定した。また、Y 社での印刷・発送に必要なデータだけを、X 社の基幹サーバから抽出して Y 社のファイルサーバへネットワーク経由で暗号化して送信する方式とした。

個人データの安全管理措置は、現在の X 社での管理水準を Y 社においても維持する必要がある。そこで、プロジェクトでは X 社における規程や手続の要件を文書にまとめて Y 社の運用管理者に提示した。また、サービス開始前に Y 社の作業現場に行って現状調査を実施することで合意した。

後日、プロジェクトのメンバが Y 社の作業現場を訪問し、Y 社の運用管理者と一緒に現状調査を実施した。現状調査の結果、次の問題点 ①～④ が発見された。

〔問題点〕

- ① 印字不良などで廃棄する、個人情報を含む印刷物は、鍵の付いた個人情報専用の廃棄箱に入れて保管し、定期的に廃棄処分をしている。しかし、この廃棄箱の鍵の保管管理が十分でなく、管理者の帰宅後はだれでも鍵を使用できる状態にある。
- ② ファイルサーバに対する設定変更などの特権操作は、電算室内の運用管理者席にあるシステム保守用端末だけで実行できる。しかし、この端末で行われた特権操作の内容は記録していない。
- ③ ファイルサーバへのログインは利用者 ID とパスワードで認証しているが、認証後は、サーバ内のどのファイルも参照が可能である。
- ④ ファイルサーバへのログインは、すべて記録されるが、個々のファイルへのアクセスは、機能上の理由で記録していない。

プロジェクトのメンバと Y 社の運用管理者は、問題点について次のとおり確認した。

- (1) 問題点 ①～④ のうち、問題点 d を除くほかの三つの問題点は、技

術的安全管理措置の問題である。

(2) 問題点①について、この問題を放置しておくとき e というリスクがある。

(3) 問題点②及び④について、これらの問題を放置しておくとき f というリスクがある。

Y 社では、この現状調査の結果をガイドラインに沿ってまとめて改善計画を作成すること、及び改善計画の実施結果を X 社に報告することを確約した。

dに関する解答群

ア ① イ ② ウ ③ エ ④

e, fに関する解答群

ア 個人情報を含む媒体を持ち出せる	イ 誤操作や不正操作の発見が困難になる
ウ システム障害の原因となる	エ 利用者認証機能をう回できる