問6　ITサービスマネジメントにおける個人情報の保護（ITサービスマネジメント）（H22秋-FE 午後問6）

【解答】

［設問1］　a－ウ，b－エ，c－ア

［設問2］　d－ア，e－ア，f－イ

【解説】

この問題は個人情報保護の観点から，通信販売のX社における通信販売を事例に，個人情報についての管理・運用を主題とした問題である。

設問1では，委託先との契約や管理といった点からの個人情報の管理について問われている。通常の契約形態における義務・権利関係が分かっていれば比較的やさしい内容であろう。設問2では，プロジェクトにおける安全管理措置についての現状によって，与えられた問題点からリスクなどを検討する設問である。問われてる点については，迷うような選択肢が少なく，選びやすい解答群となっている。落ち着いて問題を読み進めていけば，正解が得やすい問題である。

［設問1］

自社の業務を外部委託した場合の委託元であるX社の対応について，委託先と結ぶべき契約や委託先への監督，安全管理措置の概要などを考える問題である。

・空欄a，b：空欄aは個人データの取扱いの委託に当たって，安全管理措置を委託先に遵守させるために必要なことが問われている。また空欄bは，業務開始後に委託元が実施する必要がある管理項目を考える。a，bに関する解答群から解答を考えていくと，まず空欄aの法とガイドラインに基づく安全措置を遵守させるという意味では，（ウ）の「契約を締結」することが肝要と考える。（ア），（イ），（エ）の担当者の任命や委託先の監督だけでは，委託先に対する法的拘束力が弱くなるため，解答としては適さない。また，空欄bの業務開始後に委託元が実施する必要がある管理項目については，より具体的に監督内容が示されている，（エ）の「個人データの取扱状況を監督」が適切である。（ア）の委託先の運用担当者の任命では，委託先に任せてしまう形となり，（イ）の委託先の従業者を監督では，監督内容が明らかではないことから，委託元の管理項目としては不十分である。したがって，空欄bは（エ）が適切である。

・空欄c：業務②，③について，外部に委託せず社内処理を継続することになった理由を，表の「安全管理措置の概要」から考えてみる。問題文には「表の安全管理措置のうち技術的安全管理措置について」とあることから，技術的安全管理措置の内容で，考慮すべき対応内容を解答群から考える。業務②，③の内容を見ると，いずれもX社の基幹サーバ内にある顧客データへのアクセスが必要である。表の安全管理措置の技術的安全管理措置には，情報システムへのアクセス制御が示されている。そこで解答群を考えてみる。（ア）は委託先からの個人データのアクセスについて，安全性を確保するためにシステムを改修するという内容である。業務②，③を外部委託すれば，委託先からのシステムへのアクセスは必然となる。そのためには，外部からのアクセスに対し，委託先からの限られた者からのアクセスのみを許可したり，不正な侵入を防ぐセキュリティ対策を情報システムに盛り込む必要がでてくる。したがって，（ア）が正解となる。ちなみに，（イ）の専用作業室を委託先に新たに設けることや，（ウ）のX社の個人情報保護管理者が委託先に常駐することは，システムへのアクセスとは関係ないので不正解である。また，（エ）のX社の従業員が委託先のシステム運用方法の指揮・命令体制を整備しても，システム的にアクセスを監視しなければ不正アクセスなどは防げないので，これも対応内容としては不完全である。

［設問2］

業務①のY社への外部委託が決定したことを受けて，X社の安全管理措置を管理水準としてY社にも維持してもらうために，規程や手続をY社の運用管理者に提示する。サービス開始前に，Y社の作業現場を現状調査した結果，浮き彫りとなった問題点について検討していく内容である。

・空欄d：問題点の中で技術的安全管理措置の問題ではないものを考える。問題点①は印刷物の取扱状況や廃棄箱の鍵の管理が問題点として挙げられている。ほかは実際にシステムを操作したり，アクセスしたりする状況での問題点で，技術的安全管理措置の問題といえる。したがって，（ア）の①が正解である。②～④に関しては，ファイルサーバアクセスに関しての問題点であり，技術的安全管理措置の中の情報システムへのアクセス制御に対する問題点となる。

・空欄e：問題点①を放置しておくことによって，起こるリスクについて問われている。問題点①では，個人情報を含む印刷不良の印刷物を入れる廃棄箱には鍵がかかっているが，その鍵の保管管理が十分でなく，誰でも鍵を使用できることが指摘されている。誰でも鍵を使用できるということは，その廃棄箱の鍵を開けて，個人情報を持ち出せるリスクが存在するということが考えられる。したがって，（ア）の「個人情報を含む媒体を持ち出せる」が正解である。（イ），（ウ），（エ）は，システムにアクセスする場合の問題点であり，システムの操作や機能にかかわる内容なので，物理的安全管理措置のリスクとしては当てはまらない。

・空欄f：問題点②，④を放置しておくと起こるリスクについて問われている。問題点②は，ファイルサーバに対する設定変更などの特権操作について，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が，この端末から行われた特権操作の内容が記録されていないことである。特権操作は，重要な操作であり，慎重な操作が求められる。どのような操作が行われて現状のシステムが稼働しているのか，また，システムトラブルが発生した際の誤操作の可能性なども考慮に入れなければならない。トラブルが起きた場合や特権操作が実行された際に記録（ログ）が存在しないのは，操作記録を追えないということである。また，操作記録がないということは，誰が操作したかは分からないということであり，裏を返せば，簡単に運用管理者が不正を働くこともできてしまうことになる。したがって，（イ）の「誤操作や不正操作の発見が困難になる」が正解である。特権操作記録がないことが，（ウ）のシステム障害の原因になったり，（エ）の利用者認証機能のう回になるとは言い難い。