

問2 情報セキュリティ管理状況の監査に関する次の記述を読んで、設問1～5に答えよ。

B社は、店舗での販売を主力事業としてきた百貨店である。しかし、最近はインターネットを利用した通信販売が普及してきたことから、3年前からインターネット通信販売システム（以下、通販システムという）を利用した通信販売を開始し、売上拡大に取り組んでいる。

B社では、通販システム運用開始時から保守業務をP社に委託している。今般、通販システムの保守業務を外部委託している同業他社の業務委託先で、顧客の決済情報が漏えいするという事故が発生した。B社の内部監査部長は、この事故から自社の通販システムについて情報セキュリティ管理の重要性を認識し、システム監査チームに対して管理状況を監査するよう指示した。

〔予備調査の結果（抜粋）〕

システム監査チームは今年3月に予備調査を実施し、次の事項を確認した。

- (1) B社システム部には、通販システム課（以下、通販課という）があり、課長1名と課員2名が配置されている。通販課は、通販システムの運用・保守を業務委託先の管理も含め、担当している。
- (2) B社の通販システムを担当するP社の保守業務担当（以下、P社保守業務担当という）には、P社の正社員及び契約社員から構成される従業員5名が配置されている。そのうち、正社員の一部は毎年4月に異動となり、契約社員の一部も契約更改時に入れ替わっている。
- (3) B社システム部は、P社との業務委託契約に基づき、毎月、P社の業務体制図を受領している。業務体制図には、P社保守業務担当の氏名、役割、着任年月、再委託先の社名などが記載されている。
- (4) 通販システムのクレジットカード決済機能の保守業務は、運用開始時にはP社からQ社に再委託されていたが、今年1月からは再委託先がR社に変更されている。
- (5) 通販システムの保守業務において使用されるテストデータは、表1のような手順で作成され、P社に送付されている。

表 1 テストデータ作成手順



担当	業務内容・手順
P 社保守業務担当者	① B 社通販課からの保守依頼に基づき、テストデータ作成依頼書（以下、データ依頼書という）を作成する。 ② P 社保守業務担当課長の承認を得て、B 社通販課に送付する。
B 社通販課員	③ B 社通販課長からの指示とデータ依頼書に基づき、専用ツールを用いて、顧客氏名、クレジットカード番号などを類推不能な英数字に置き換えるマスク処理を行う。 ④ マスク処理が正常に終了すると、テストデータ番号をファイル名とするテストデータが CD-R に出力され、テストデータ番号が記載されたマスク処理結果票が作成される。 ⑤ 記載されたテストデータ番号をデータ依頼書に記入する。
B 社通販課長	⑥ マスク処理が正常に終了したことを確認し、データ依頼書に確認印を押す。 ⑦ P 社に CD-R、データ依頼書、受領書を送付するように通販課員に指示する。データ依頼書の写しは、B 社通販課で保管される。
P 社保守業務担当課長	⑧ B 社通販課から受領した CD-R の内容を確認して、受領書にテストデータ番号を記入し、確認印を押す。 ⑨ B 社通販課に受領書を送付するように P 社保守業務担当者に指示する。
B 社通販課員	⑩ P 社から返送された受領書に対応するデータ依頼書の写しがあることを確認する。 ⑪ 受領書とデータ依頼書の写しを合わせて、受領書ファイルに保管する。

(6) 次のように、B 社の各部署は、業務委託先から提出される情報セキュリティ確認書によって、情報セキュリティ管理状況を確認している。

- ① B 社管理部が所管する外部委託管理規程では、業務委託先に対して一定の確認項目についての情報セキュリティ確認書を、B 社と業務委託先との契約締結時、及び年 1 回（毎年 12 月）B 社の各部署に提出させることを定めている。
- ② P 社からの情報セキュリティ確認書は、契約締結時、及び毎年 12 月に B 社システム部に提出され、情報セキュリティ確認書の確認項目ごとに B 社通販課長の確認印が押される。P 社が昨年 12 月に提出し、B 社が確認した情報セキュリティ確認書の一部は、表 2 のとおりである。
- ③ P 社から提出された情報セキュリティ確認書の添付資料の業務体制図、教育実施記録には、次のような内容が記載されている。

業務体制図 : P 社保守業務担当の氏名、役割、着任年月、再委託先の社名など
 教育実施記録 : 従業員氏名、教育内容、教育実施年月など

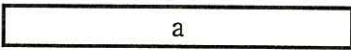
表2 P社から提出された情報セキュリティ確認書（抜粋）

項番	確認項目	回答	添付資料	確認印
1	受託業務を担当する全ての従業員に対して、情報セキュリティ教育を適時に実施しているか。	業務体制図に記載した受託業務を担当する従業員に対して、教育実施記録のとおり着任時に情報セキュリティ教育を実施している。	12月時点の業務体制図及び12月時点の教育実施記録	
2	受託業務を再委託している場合、再委託先の情報セキュリティ管理状況を確認しているか。	貴社に対して当社が提出している情報セキュリティ確認書と同一内容の確認書を、受託業務の再委託先から定期的に受領し、当社の保守業務担当課長が確認印を押している。	Q社から提出された情報セキュリティ確認書	

〔本調査の計画（抜粋）〕

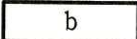
システム監査チームは、予備調査の結果に基づき、表3のような監査手続書を策定した。

表3 監査手続書（抜粋）

項番	監査要点	監査手続
1	B社通販課長は、業務委託先に送付するテストデータがマスク処理されていることを確認しているか。	データ依頼書の写しを閲覧し、B社通販課長の確認印が押されていることを確認する。
2		受領書ファイルに保管されたデータ依頼書の写しと、P社保守業務担当課長の確認印が押された受領書を照合し、テストデータ番号が一致していることを確認する。
3	B社システム部は、業務委託先における情報セキュリティ教育の実施状況を適切に確認しているか。	P社から提出された情報セキュリティ確認書を閲覧し、B社通販課長の確認印が押されていることを確認する。
4	B社システム部は、業務委託先を通じて、再委託先の情報セキュリティ管理状況を適切に確認しているか。	P社から提出された情報セキュリティ確認書に、再委託先からの情報セキュリティ確認書が添付されていることを確認する。次に、再委託先から提出された情報セキュリティ確認書に、P社保守業務担当課長の確認印が押されていることを確認する。

〔内部監査部長のレビュー（抜粋）〕

内部監査部長は、システム監査チームから予備調査の結果及び本調査の計画について報告を受け、次のとおり指摘した。

- (1) 表3 項番1の監査手続だけでは、監査要点の立証には不十分である。追加の監査手続（データ依頼書の写しと  の照合）を検討すること
- (2) 表3 項番3の監査手続だけでは、監査要点の立証には不十分である。

- ① 追加の監査手続（P 社から提出された情報セキュリティ確認書の添付資料である業務体制図と教育実施記録の照合）を検討すること
- ② P 社における通販システムの保守業務体制を考慮すると、P 社から提出された情報セキュリティ確認書の添付資料同士を照合するだけでは、監査手続として不十分であると考えられる。この点を踏まえて、追加の監査手続を検討すること

〔本調査の結果（抜粋）〕

システム監査チームは、監査手続を再検討した後、内部監査部長の承認を得て、今年 4 月に本調査を実施した。

表 3 項番 4 の監査手続を実施した結果、B 社システム部が現在の再委託先 R 社の情報セキュリティ管理状況を確認していないことが判明したので、次の改善提案を行った。

- (1) B 社システム部は、P 社を通じて、R 社の情報セキュリティ管理状況をできるだけ速やかに確認すること
- (2) B 社管理部は、業務委託先から提出される情報セキュリティ確認書に関して、外部委託管理規程を改定すること

設問 1 〔本調査の計画（抜粋）〕の表 3 について、a に入れる監査要点を 50 字以内で述べよ。

設問 2 〔内部監査部長のレビュー（抜粋）〕の(1)について、b に入れる監査資料を 10 字以内で答えよ。

設問 3 〔内部監査部長のレビュー（抜粋）〕の(2)の①について、監査手続において確認する事項を二つ挙げ、それぞれ 30 字以内で述べよ。

設問 4 〔内部監査部長のレビュー（抜粋）〕の(2)の②について、内部監査部長が“P 社から提出された情報セキュリティ確認書の添付資料同士を照合するだけでは、監査手続として不十分である”と考えた理由を、45 字以内で述べよ。

設問 5 〔本調査の結果（抜粋）〕の(2)について、外部委託管理規程の具体的な改定内容を、50 字以内で述べよ。