

H26

問1 情報システムの保守業務の監査に関する次の記述を読んで、設問1～4に答えよ。

S社は、保険会社の情報システム子会社である。S社で運用・保守を行っているシステムの種類は多く、ハードウェア、ミドルウェアも多岐にわたっている。一方で、親会社からは、運用・保守費用の削減を求められ、S社は保守要員を減らした。その結果、現在では、保守対象システムの多さに比べて保守要員が少ないことが、S社の課題の一つとなっている。

さらに、最近になって、保守を起因とする障害が連続して発生したこともあり、S社監査部のシステム監査チームでは、今年度の監査として、保守業務の品質確保の状況を確認するための監査を実施することになった。

[保守業務の状況]

S社におけるシステムの保守業務の状況は、次のとおりである。

- (1) 親会社の利用部門との調整、システムの企画・要件定義、プロジェクト管理などは、S社社員が主に担当している。プログラム開発などは、必要に応じて外部ベンダに委託している。
- (2) リリースから一定の年数を経過したシステムについては、開発に携わったS社社員が担当者として一人も残っていない場合が多い。
- (3) 5年以内に開発されたシステムの保守についても、費用削減のために、開発したベンダとは別のベンダに委託しているケースが多い。
- (4) 開発・保守を実施する部署とは別に、全システムに共通する開発標準及び開発・保守ツールの導入・更新については、S社の開発支援チームが担当している。
- (5) 保守ツールの一つとして、保守要件に伴う影響範囲の調査用ツールがある。調査用ツールは、ソースプログラム、JCL、データベース定義などに関して、項目名などから影響範囲を特定できる。

[予備調査の実施]

システム監査チームのT氏をリーダーとして実施した予備調査の内容は、次のとおりである。

- (1) 保守対象システムの内容、保守作業の状況を把握するために、表1に挙げた資料

を入手した。

表1 予備調査における入手資料

資料名	内容
システム一覧	稼働中のシステム名、利用しているハードウェア、ミドルウェア、OS、開発言語、委託先、及び担当者の一覧
保守業務の作業標準及びルール	保守作業において守るべき、全システム共通の作業標準及びルールを定めた文書
保守作業マニュアル	初心者でも間違いなく作業ができるように、作業の手順などを記載したマニュアル
障害報告レポート	担当部門別・システム別の障害発生件数、障害原因、問合せ件数などの集計資料
設計書類	システムごとの基本設計書、詳細設計書、プログラム仕様書、変更管理資料などのドキュメント
引継ぎ規程	新規にシステムを開発したときに、保守担当者に引き継がれるドキュメント、引継ぎ手順などを定めた文書

- (2) 保守作業マニュアルは、複数システムで共通のものもあるが、システムごとに作成されているケースが多く見られた。

- (3) 障害報告レポートをレビューし、システム別・障害原因別の発生状況を確認した。

- その結果、同一原因によるシステム障害が何度か発生していることが分かった。

- (4) 設計書・仕様書の整備状況を確認した。その結果、詳細設計書、プログラム仕様

- 書の一部が存在しないシステム、及び最新状態に更新されていないシステムが多く見られた。

- (5) 引継ぎ規程の内容を調査した。その結果、保守担当者への引継ぎに必要なドキュメントが網羅されていることを確認した。

[本調査の実施]

T氏は、予備調査の結果を基にリスクを洗い出し、リスクに対するコントロールを表2のとおりまとめた。

1/21はOK

内容は?

Q4

Q4 内容は?

Q4 内容は? 問題ない?

Q4 OK

範囲が十分
修正箇所のみ
テストしている

出
テラ範囲
図形記述
れ、
一般的
回答で考えた。

表2 リスクとコントロール

No.	観点	リスク OR	コントロール
(1)	影響範囲の調査	<ul style="list-style-type: none"> 基本設計書、詳細設計書などのドキュメントが不十分なので、システムの最新状態を把握するのが困難である。 ドキュメントに依拠した調査では、調査漏れが発生する可能性がある。 	<ul style="list-style-type: none"> a) ドキュメントの不備を補うために、調査用ツールを使用する。 b) リバースツールを使用して、ソースコードからプログラム設計書を作成し、ドキュメントの不足を補う。 c) 保守用のドキュメントを順次整備していく。
(2)	テストの実施対象範囲	<ul style="list-style-type: none"> テスト範囲が不十分で、不具合が残存している可能性がある。 	a) ①
(3)	障害時の対応	<ul style="list-style-type: none"> 障害報告書を作成していても、障害情報を共有していないと、障害が再発する可能性がある。 	<ul style="list-style-type: none"> a) ② b) 予防措置が可能なプログラムは修正しておく。
(4)	新規開発システムの保守担当者への引継ぎ	<ul style="list-style-type: none"> 引き継いだドキュメントが不十分だと、保守業務を実施する際にシステムの状況を把握できない。 	<ul style="list-style-type: none"> a) 引継ぎ規程に定められたドキュメントを作成し、保守担当者に引き渡す。 b) ドキュメントの作成に必要な工数を、開発時に確保する。

表2を基に監査手続書を作成し、次のような本調査を実施した。

- 表2の(1)のコントロールa)について、T氏は、保守担当者が実際に行った作業結果を記した“調査結果報告書”を査閲した。その結果、調査範囲は調査目的によって異なるので、保守担当者は、担当システムに関連するライブラリをその都度指定していることが分かった。T氏は、調査漏れを防ぐためにどのような対策を実施しているか確認した。
- 表2の(3)について、委託先の責任者にヒアリングを行い、障害時の対応結果を記した障害報告書を査閲した。最近発生していた障害の原因は、プログラム内部でもつテーブルの限界値を超えたことによる異常終了であった。障害報告書には、障害原因や当該プログラムの対応結果が記載されていただけであった。T氏は、障害報告書に記載すべき項目を追加する必要があると考えた。

Q3-2

2の他のシステムは
7-7-7-7の記述を
書いては、

横展開の
実施経路について

(3) 表2の(4)について、コントロールa)の運用状況を確認した。まず、サンプリングした幾つかのシステムについて、保守担当者に引継ぎ済のドキュメントの網羅性を確認した。次に、保守担当者に、引継ぎ時におけるドキュメントの内容確認のポイントをヒアリングした。Q4 ⇒ 網ろ性は確認済。

設問1 [本調査の実施]の(1)について、T氏が確認しようとした対策の具体的な内容を40字以内で述べよ。

設問2 表2の①として、T氏が考えた具体的なコントロールの内容を45字以内で述べよ。

設問3 表2の②に記載すべきコントロールを45字以内で述べよ。また、[本調査の実施]の(2)においてT氏が考えた、障害報告書に記載すべき項目を40字以内で述べよ。

設問4 [本調査の実施]の(3)において、T氏が保守担当者にヒアリングした、引継ぎ時におけるドキュメントの内容確認のポイントを45字以内で具体的に述べよ。

コントロールが
知っているか
確認済。

情報共有
については
内容から

先のコントロールについて
実施終了
がし

都度指定が
問題?
調査範囲は
調査目的に
おて

毎回、更新
ので
有識者に
レビューして

(1)のコントロールに
書き