問3　保守作業の証跡確保のための対策検討に関する次の記述を読んで，設問 1～4 に答えよ。

M 社は，従業員数 900 名の保険会社である。M 社は損害保険業務を支援する保険システムを稼働させている。保険システムの利用者は，M 社の従業員である。M 社は，保険システムの開発をソフトウェア開発会社の Z 社に委託している。また，保険システムは M 社のグループ会社が運営するデータセンタ（以下，DC という）に設置し，主に M 社が運用と保守を行っているが，一部の保守作業については Z 社に委託している。保険システムは，20 台のサーバ（以下，保険サーバという）から構成されており，保険システムのサービス（以下，保険サービスという）を提供するための様々なソフトウェアが稼働している。保険システムの構成を図 1 に示す。

Z 社が請け負っている保守作業は，機能追加などに基づく保険システムのプログラムモジュールの更新，保険システムに障害が発生した場合の原因調査，本番システムへの設定変更などの作業が主である。Z 社は M 社から作業依頼書を受け取ると，保険システムを担当する 5 名の保守チームの中から当該作業担当者を 1 名選び，作業担当者氏名や作業期間などを記載した作業計画書を M 社に提出する。作業計画が承認されると，作業で使用するために，OS の特権 ID が使用可能な状態に有効化され，通知される。特権 ID とは，OS に対する全てのシステム管理特権を付与された利用者 ID のことである。作業担当者は通知された特権 ID を使い，Z 社 PC から保険サーバにリモートアクセスを行って作業を実施する。Z 社内の M 社保険システム保守用 LAN，M 社 LAN 及び DC 内の DCLAN は IP-VPN で接続されている。

なお，DC 内の保険サーバのコンソールからの操作や電源の操作は，M 社が実施している。また，保険サーバやネットワーク機器の時刻は全て同期している。

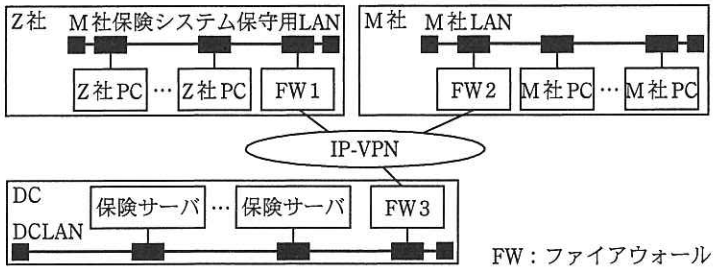

図 1　保険システムの構成

〔対策の検討と対策方針の策定〕

M 社の同業の C 社で情報漏えい事件が起きた。C 社の保守作業委託先の従業員が，保険加入者のデータを不正に持ち出して名簿業者に売却したと報じられた。事件は，C 社が事態をすぐに把握できなかった管理上の不備に対する指摘とともに，連日報道された。M 社の経営幹部は，C 社の事件をきっかけに，自社の保険システムにおいても同様の問題が起きる可能性はないか早急に調査するよう，情報システム部長に指示を出した。調査の結果，保険システムについても，Z 社の保守作業において，保険加入者の情報が保存されたファイル（以下，機密ファイルという）が，作業依頼書に指定した範囲を超えてアクセスされるおそれがあることが指摘された。そこで，情報システム部の L 主任がリーダとなり，対策を検討することになった。

検討を開始した当初は，Z 社の保守作業において機密ファイルへのアクセス制御を実施する案も出たが，M 社保守担当者から，特権 ID の運用が複雑になる上，保守作業には緊急性が求められる場合もあり，現実的な対策ではないといった意見があった。そこで，①L 主任は Z 社の作業担当者の保守作業の作業証跡を取得し，作業内容とは無関係な機密ファイルの操作（以下，機密ファイル操作違反という）を検知する仕組みを備えるという対策方針を立てた。本対策方針は経営幹部に報告された後，M 社役員会議で承認された。

L 主任は，Z 社が行う作業の操作ログを取得し，操作ログから Z 社の機密ファイル操作違反の可能性を自動検知する対策がよいと考えた。検知後に，作業者の機密ファイル操作違反前後の一連の操作を追跡することを想定した対策である。

〔対策実現に向けた要件と実現方式の検討〕

L 主任は部下の N 君に次の三つの要件を示した上で，実現方式の検討を指示した。

要件 1：保険サーバで Z 社の作業担当者が行うファイル操作を，ログサーバに記録できること

要件 2：特定のファイルのアクセスや，特定のプロセスの起動と停止などの検知ルールをあらかじめ定義でき，操作ログ上で検知ルールに一致したファイル操作ログが見つかったときに，管理者に通知できること

要件 3：操作ログの取得を実現する上で，保険サービスの可用性に影響を与えないこと

N 君は，操作ログが取得可能な製品の中でシェアの高い二つの市販ソフトウェアパッケージ製品 PP1，PP2 を候補とし，それぞれのパッケージ製品を利用した対策実現方式案（以下，それぞれ案 1，案 2 という）を表 1 のとおり取りまとめて，L 主任に報告した。

〔実現方式案の要件の確認〕

L 主任は最初に，案 1，案 2 が要件を満たしているかどうかを確認した。L 主任は，案 1 は，ログサーバがダウンしている場合，及び②作業担当者が保険サーバのネットワーク設定を不正に変更して操作ログの転送を妨害した場合において，③その後，作業担当者がある操作を実行すると，その前後のファイル操作について要件 1 及び要件 2 が満たされなくなると指摘した。

要件 3 については，L 主任は，特に案 1 について，保険サーバ内の [a] と既存ソフトウェアとの間で相互に悪影響を及ぼさないか，十分なテストを実施する必要があると考えた。

表1　案1及び案2の実現方式概要

案1	案2
・PP1を採用する。 ・操作ログを取得する各保険サーバにPP1のエージェントモジュールをインストールする。 ・ログサーバをDCLANに設置し，PP1のメインモジュールをインストールする。 ・Z社の保守作業におけるリモートアクセス手順に変更はない。 ・エージェントモジュールが取得するログ項目は，利用者ID，時刻（保険サーバの時刻）及び次のいずれかである。 (a) 実行されたコマンド (b) 操作対象ファイル名と操作（参照，コピー，更新，削除） (c) アプリケーションの起動と終了（エージェントモジュールの起動と停止も含む） ・PP1（メインモジュールとエージェントモジュール）の起動と停止には，インストールされているサーバの特権IDが必要である。 ・ログサーバはM社が管理する。 ・操作ログは，Z社の作業担当者が保険サーバにログインしてからログアウトするまでの間，取得する。	・PP2を採用する。 ・DCLANに中継サーバを設置し，中継サーバにPP2をインストールする。 ・操作ログは中継サーバで取得する。 ・ログサーバをDCLANに設置する。 ・Z社の保守チームには，担当者ごとに中継サーバの利用者IDを付与する。 ・Z社の保守作業におけるリモートアクセス手順は，リモートデスクトップ接続を行い中継サーバに一旦ログインして，さらにリモートアクセスを行い，各保険サーバにログインするように変更する。 ・取得するログ項目は，保険サーバの利用者ID，時刻（中継サーバの時刻）及び次のいずれかである。 (a) 保険サーバで実行されたコマンド (b) 保険サーバでの操作対象ファイル名と操作（参照，コピー，更新，削除） (c) 保険サーバでのアプリケーションの起動と終了 (d) Z社PCに表示されるリモートデスクトップ先（中継サーバ）のウィンドウ画面のスナップショット画像 ・中継サーバの利用者IDごとに，保険サーバへのリモートアクセスの許可と拒否の制御ができる。 ・PP2の起動と停止には，中継サーバの特権IDが必要である。 ・中継サーバ及びログサーバはM社が管理する。 ・操作ログは，Z社の作業担当者が中継サーバにログインしてからログアウトするまでの間，取得する。

・操作ログは，保険サーバ又は中継サーバで暗号化してログサーバに転送する。ただし，何らかの理由でログサーバに転送できない場合は，暗号化して，保険サーバ又は中継サーバのローカルディスクに一時保管し，定期的にログサーバへの転送をリトライする。
・PP1，エージェントモジュール，PP2を停止させた場合，停止操作の操作ログがログサーバに転送された後に停止動作が実行される。
・ログサーバ上の操作ログは付属する専用ビューアで閲覧する。
・ログサーバ上の操作ログについては，機密ファイル操作違反の隠蔽防止のために，④メッセージダイジェストを使用した［　b　］機能をもつ。
・保守作業を幾つかのパターンに分類し，パターンごとに作業内容に関係のある機密ファイルを決定し，検知ルールを定義しておく。そうすると，Z社の作業担当者が保守作業中に作業依頼書に指定した範囲を超えて機密ファイルにアクセスした場合，ログサーバでは転送された操作ログの記録内容を基に，あらかじめ指定されたメールアドレス宛てに電子メールを送信する。

〔要件以外の比較検討〕

次に，L 主任は要件以外の点についても検討を進めた。案 1 は導入に特に大きな支障はないと考えられた。

一方で案 2 は，中継サーバが導入されることから，Z 社の作業担当者の作業手順や，保険サーバなどのアクセス制御を見直す必要がある。例えば，案 2 を実現するには，[c] から保険サーバへのアクセスは禁止するが，[d] や M 社 PC からのアクセスは許可する必要がある。

また，案 2 の場合は，中継サーバを利用するための利用者 ID の付与と，保守作業ごとの各保険サーバの特権 ID の通知の 2 点の実施方法を考慮する必要がある。

しかし，L 主任は，案 2 の場合，中継サーバの利用者 ID を Z 社の保守チームの担当者ごとに作成するので，保守作業を作業計画書に記載された作業担当者だけに限定するという，より安全な仕組みが実現できると考えた。

〔対策の実施〕

L 主任は，以上の確認と比較検討の結果，Z 社の作業担当者の作業手順が変わる点などの不都合があるものの，要件を実現する上で案 2 の方が優れていると判断し，案 2 を選択することにした。その上で，保守作業の証跡を取得するためのシステム化計画を取りまとめ，経営幹部に報告し，M 社役員会議で承認を受けた。その後，システム化作業を行い，対策を実施した。

設問1　ログサーバ上の操作ログの安全な保管について，(1)，(2)に答えよ。

(1)　表1中の［　b　］に入れる適切な字句を答えよ。

(2)　表1中の下線④について，最も適切と考えられるアルゴリズムはどれか。解答群の中から選び，記号で答えよ。

解答群

ア　AES　　イ　SHA-1　　ウ　SHA-256　　エ　Triple DES

設問2　案1及び案2の実現方式について，(1)，(2)に答えよ。

(1)　本文中の［　a　］に入れる適切な字句を，表1中の用語を用いて答えよ。

(2)　本文中の［　c　］，［　d　］に入れる適切な機器名を，それぞれ図1中又は表1中の用語で答えよ。

設問3　操作ログのセキュリティについて，(1)～(3)に答えよ。

(1)　本文中の下線③のある操作とは，どのような操作か。30字以内で述べよ。

(2)　案1について，本文中の下線②のような操作ログの転送を妨害した上で行う方法以外に，Z社の作業担当者が保険サーバで，どのような操作を行うことによって，要件1の実現を妨害できるか。25字以内で述べよ。

(3)　上記(2)の操作をM社が検知するための，案1の機能を用いた有効な手段を35字以内で述べよ。

設問4　M社のセキュリティについて，(1)，(2)に答えよ。

(1)　本文中の下線①の対策方針を実現することによって，Z社の作業担当者の機密ファイル操作違反を検知することができる。さらに機密ファイル操作違反を抑止することを効果的に行うためには，M社は何を実施すべきか。40字以内で述べよ。

(2)　案2について，作業計画書に記載された作業担当者だけが特権IDを利用できるようにするために作業計画ごとに設定する制御を，60字以内で述べよ。