問2　特権 ID の管理に関する次の記述を読んで，設問 1～3 に答えよ。

Y 社は，従業員数 1,000 名の食品製造販売会社であり，一般消費者に食品を通信販売している。Y 社では，顧客情報管理システム（以下，Y システムという）を利用し，顧客情報を管理している。Y システムの保守作業は，開発元であるソフトウェア開発会社の S 社に委託している。保守作業のために，Y 社は S 社に対して，特権 ID の一部（以下，委託用特権 ID という）について使用を許可している。S 社に使用を許可した委託用特権 ID には，OS のシステム管理権限をもつ ID，DBMS の管理権限をもつ ID，及び DBMS 上のデータに対する操作権限をもつ ID（以下，それぞれ，システム管理 ID，DBMS 管理 ID，DBMS 操作 ID という）の 3 種類がある。

Y システムは，4 台の業務サーバ，1 台のデータベースサーバ（以下，DB サーバという）及び Y 社と S 社の PC から構成されており，業務サーバでは Y システムのサービスを提供するためのアプリケーションソフトウェア（以下，業務アプリという）が稼働している。各業務アプリは，DBMS 操作 ID を用いて，DB サーバから顧客情報を取得して Y 社の従業員にサービスを提供している。Y システムのサーバは，Y 社のグループ会社が運営するデータセンタ（以下，YDC という）に設置している。Y システムの構成を図 1 に示す。

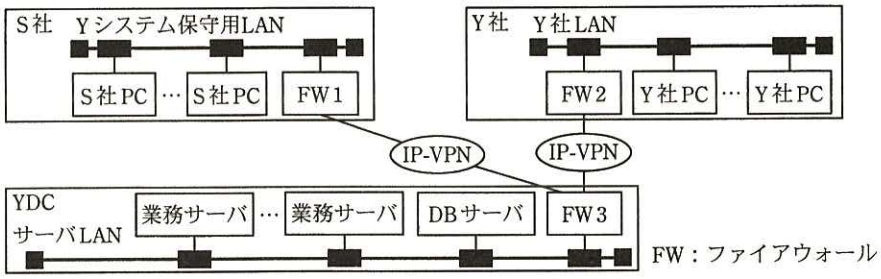

図 1　Y システムの構成

S 社に委託している保守作業は，機能追加などに際しての業務アプリの更新，Y システムに障害が発生した場合の原因調査，Y システムの設定変更などである。保守作業は，次の手順で依頼している。

1. Y 社の管理者が作業依頼書を作成し，S 社へ送付する。
2. S 社では，作業依頼書を受け取ると，S 社の保守チーム責任者（以下，保守責

任者という）が，保守チームメンバから作業担当者（以下，作業者という）を選任する。

3. 保守責任者が，担当する作業ごとに，作業者氏名，作業期間，作業対象サーバ及び作業内容を記載した作業計画書を作成し，Y 社に提出する。
4. 作業計画書が承認されて作業期間になると，Y システム保守用 LAN からサーバ LAN への接続が可能となるよう，YDC に常駐している Y 社のグループ会社の作業員（以下，YDC 作業員という）が，FW1 と接続しているネットワークケーブル（以下，ケーブル A という）を FW3 に結線し，S 社に通知する。ケーブル A は，保守作業時以外は結線されていない。
5. 作業者は，共用の ID を用いて S 社 PC にログインした後に，委託用特権 ID とパスワードを用いて，S 社 PC から作業対象サーバにアクセスし，作業する。システム管理 ID は，作業対象サーバごとに異なっている。
6. 作業終了後，保守責任者が，作業の完了を Y 社の管理者に連絡し，作業報告書を提出する。
7. 作業完了の連絡を受けて，Y 社の管理者は，ケーブル A を FW3 から取り外すよう YDC 作業員に依頼し，作業報告書によって作業内容を確認する。

システム管理 ID と DBMS 管理 ID のパスワードは Y 社が半年ごとに変更し，S 社に通知している。S 社 PC と FW1 は，S 社の資産である。Y システム保守用 LAN からサーバ LAN へのアクセスは，FW3 で保守作業に必要となるプロトコルだけに限定しているが，送信元 IP アドレスは限定していない。

〔調査の実施と対策方針の策定〕

Y 社と同業の C 社で，C 社の保守作業委託先の従業員が個人情報を不正に持ち出して名簿業者に売却するという情報漏えい事件が起きた。持出しに特権 ID が不正に使用されたが，それを検知できなかったという C 社の委託先管理の不備が連日報道された。Y 社の経営幹部は，C 社の事件をきっかけに，自社においても同様の問題が起きる可能性がないか早急に調査をするよう，情報システム部長に指示した。表 1 に示す調査結果にあるように，Y システムにおいても委託用特権 ID を用いた保守作業に問題があることが判明し，情報システム部の L 主任がリーダとなって対策を検討

することになった。

表１　調査結果（概要）

項番	項目	内容
1	委託用特権 ID 使用者の特定	委託用特権 ID が共用されており，使用した者を特定できないおそれがある。また，作業者以外も委託用特権 ID を使用するおそれがある。
2	サーバへのアクセスの制限	Y システム保守用 LAN からサーバ LAN へのアクセスについては，サーバごとのアクセス制御をしていない。そのため，作業計画書に記載された作業対象サーバ以外のサーバにもアクセスできてしまう。
3	委託用特権 ID の操作のモニタリング	作業計画書とアクセスログを突き合わせる手順が定められておらず，委託用特権 ID を使ったアクセスが作業計画書どおりに行われたかをチェックしていない。

〔要件と実現方式の検討〕

L 主任は部下の N 君に次の要件を示した上で，対策を実現する方式の検討を指示した。

要件１：委託用特権 ID の使用を作業者だけに限定すること

要件２：委託用特権 ID を使用した者を特定可能にすること

要件３：作業対象サーバだけにアクセス可能とすること

要件４：許可された作業内容と実際に実施された作業内容を突き合わせ，不正な作業を検知可能にすること

N 君は，要件を満たすためには，委託用特権 ID のパスワードの S 社への通知の停止，個人ごとに付与され特権をもたない ID（以下，個人 ID という）の作業者への付与，及び特権 ID を管理するソフトウェアパッケージの導入から成る対策案を考えた。そこで，ソフトウェアパッケージとして製品 P 及び製品 Q を候補に選び，次の案を検討した。

案１：製品 P を利用する。製品 P は，管理用サーバにインストールするプログラム（以下，プログラム H という）と，PC にインストールするプログラム（以下，プログラム J という）で構成される。管理用サーバはサーバ LAN 上に設置する。作業者は，プログラム J に個人 ID でログインし，プログラム J から作業対象サーバにアクセスし，操作する。作業対象サーバへアクセスする際に使用する委託用特権 ID とパスワードは，プログラム H からプログラム J に転送さ

れ，ログインに際して自動入力される。

案 2：製品 Q を利用する。製品 Q は，管理用サーバにインストールするプログラム（以下，プログラム K という）だけで構成される。管理用サーバはサーバ LAN 上に設置する。作業者は，S 社 PC から個人 ID でプログラム K にログインした後に，プログラム K から作業対象サーバへ自動ログインによってアクセスし，操作する。

検討の結果，N 君は，案 2 の方が製品の導入が容易であると判断し，案 2 による実現方式案をまとめて，L 主任に報告した。実現方式案の概要を表 2 に示す。

表 2　実現方式案の概要

項目	概要
ID の登録	・ a が，プログラム K の ID 登録画面において，委託用特権 ID をあらかじめ登録する。また，作業者の個人 ID をあらかじめ登録する。個人 ID は，プログラム K にログインするために付与される。
作業計画の入力と特権 ID の使用申請	・ プログラム K の作業計画入力・委託用特権 ID 使用申請画面において，保守責任者が，作業者の個人 ID，作業者氏名，作業期間，作業対象サーバ及び作業内容を入力し，委託用特権 ID の使用を申請する。
特権 ID の使用許可	・ a が，使用申請を確認した後に，委託用特権 ID の使用許可操作を行う。この操作によって，作業対象サーバでの委託用特権 ID の使用が可能になる。
作業対象サーバへのログイン	・ 作業者は，個人 ID を用いてプログラム K にログインし，作業対象サーバへの接続要求を行う。 ・ プログラム K は，作業者の個人 ID による委託用特権 ID の使用が許可されていることを確認する。確認できた場合は，委託用特権 ID とパスワードを用いて作業対象サーバに自動ログインする。
操作履歴の取得	・ プログラム K は，委託用特権 ID による操作履歴を入力コマンドはテキストで，操作画面は動画で記録する。 ・ 作業対象サーバでの操作履歴は管理用サーバに保存される。保存された操作履歴へのアクセスには管理用サーバのシステム管理権限が必要であり，Y 社内の限られた者だけがアクセスできる。 ・ 操作履歴のうち，入力コマンドのテキストは作業対象サーバにも保存される。
作業完了報告	・ 作業終了後，プログラム K の報告画面において，保守責任者が作業完了報告を行う。
特権 ID の使用解除	・ a が，作業完了報告を確認した後に，プログラム K の管理画面において，委託用特権 ID の使用解除操作を行う。 ・ 使用解除操作を行うと，作業対象サーバでの委託用特権 ID の使用が不可となる。
作業内容の確認	・ プログラム K の機能によって，操作履歴と委託用特権 ID の使用申請で入力された作業内容を突き合わせ，その結果をレポートに出力する。 ・ a が，レポートを確認する。

〔実現方式案の要件の確認〕

L主任はN君の対策案に対して，要件1と要件3について補足説明を求め，要件2と要件4について問題を指摘した。

要件1について，N君は，作業者以外は委託用特権IDを使用できないことを説明し，L主任の了解を得た。

要件2について，L主任は，次のように指摘した。

指摘1：製品Qの導入だけではこの要件を満たすのに不十分である。

指摘2：①使用される委託用特権IDによっては，DBサーバへアクセスした者をDBサーバ上のアクセスログから特定することができない。

指摘1に対してN君は，追加対策を検討すると回答した。また，指摘2に対しては，DBサーバ上のアクセスログを利用せずとも，DBサーバへアクセスした者を特定できることとその理由を回答した。

要件3について，N君は，[b]からは[c]へのアクセスだけを許可するようにFW3の設定を変更することによって，アクセス先を作業対象サーバに限定できると説明し，L主任の了解を得た。

要件4について，L主任は，作業者が作業対象サーバ上のアクセスログを書き換えると，作業計画の作業内容以外の操作，つまり不正操作が検知できなくなるのではないかと指摘した。これに対してN君は，②不正操作を検知できることとその理由を回答した。

〔追加対策の検討〕

N君は，要件2についての指摘1を踏まえて，次の追加対策をL主任に提案した。

・③S社におけるプログラムKの個人IDの管理状況をY社が確認する。

・④委託用特権IDを使った者が特定されることをプログラムKのログイン画面に表示し，作業者に周知させる。

最後にL主任は，案2を採用すべき理由を再確認した。N君は，要件を満たすためには製品を適切に運用するための資産管理が必要だが，Y社の状況においては⑤案1に比べて案2の方が必要な資産管理を実施しやすいと説明した。L主任は，案2に

よる実現方式案と追加対策を承認した。

〔対策の実施〕

案 2 による実現方式案と追加対策は，経営幹部に報告され，実施された。対策によって，保守作業時のケーブル A の結線と取外しが不要となった。

設問 1　表 2 中の [a] に入れる適切な字句を，10 字以内で答えよ。

設問 2　〔実現方式案の要件の確認〕について，(1)～(3)に答えよ。

(1)　本文中の下線①について，DB サーバへアクセスした者を特定することができない委託用特権 ID を 10 字以内で答えよ。また，特定することができない理由を 35 字以内で述べよ。

(2)　本文中の [b] ，[c] に入れる適切な機器名を答えよ。

(3)　本文中の下線②について，不正操作を検知できる理由を 35 字以内で述べよ。

設問 3　〔追加対策の検討〕について，(1)～(3)に答えよ。

(1)　本文中の下線③について，具体的には何を確認すべきか。35 字以内で述べよ。

(2)　本文中の下線④には，顧客情報の不正持出し対策として何と呼ばれる効果があるか。効果の名称を“効果”という字句を含めて 5 字以内で答えよ。

(3)　本文中の下線⑤について，案 2 の方が資産管理を実施しやすい理由を 40 字以内で述べよ。