問2　ログの管理に関する次の記述を読んで，設問1～3に答えよ。

H 社は，200 名が勤務する高級化粧品の訪問販売会社である。H 社では，顧客の連絡先，訪問記録，購買履歴などの個人情報を管理する顧客管理システム（以下，B システムという）を利用している。B システムを利用しているのは，営業部の 1 課～5 課に所属する 140 名である。そのうち，営業を行っている 120 名は個人情報にアクセスする権限をもち（以下，有権限者という），担当顧客の情報を記録，参照している。残りの 20 名は，売上状況などを集計するためだけに B システムを利用しているので，個人情報にアクセスする権限をもたない（以下，無権限者という）。各営業部員は貸与された端末を社内で利用している。

最近，H 社の同業他社である C 社において，顧客の個人情報がシステムから漏えいするという事件があった。そこで H 社では，情報システム部の D 部長が中心となって個人情報漏えい対策を強化することになった。D 部長は，対策の検討に当たって部下の E 課長に対し，H 社のシステムの中で最も多くの個人情報を保有している B システムのアクセス管理の状況を確認するように指示した。

E 課長は，B システムの利用者 ID の管理状況を調査した。その結果，次の点を確認することができた。

- 利用者 ID の登録，変更及び削除は，申請に基づいて実施している。
- 3 か月ごとに利用者 ID と利用者名の一覧を営業部の各課長に提示の上，業務上の必要性について確認している。なお，利用者 ID と利用者は 1 対 1 に対応している。
- B システムのログを取得し，3 年間保存している。

E 課長がこれらの調査結果を D 部長に報告したところ，D 部長から，“利用者 ID の管理状況は分かったが，それだけでは B システムの利用が適切に行われているという保証にはならない。個人情報漏えいにつながるような不審な利用がないか，その予兆も含めて，ログを分析して確認するプロセス（以下，そのプロセスをモニタリングという）が必要である”と指摘された。

〔モニタリングの検討〕

指摘を受けた E 課長は，まず，B システムで取得しているログの種類を確認し，表 1 にまとめた。

表1　取得しているログ

ログを取得するイベント	取得する情報
ログイン成功	日付，時刻，機能番号(0001)，端末 ID，利用者 ID，成功(1)
ログイン失敗	日付，時刻，機能番号(0001)，端末 ID，ログインしようとした利用者 ID，失敗(0)
ログアウト	日付，時刻，機能番号(0099)，端末 ID，利用者 ID
ログインとログアウト以外の機能の利用成功	日付，時刻，機能番号(1000～9999)，端末 ID，利用者 ID，成功(1)
ログインとログアウト以外の機能の利用失敗 [1)]	日付，時刻，機能番号(1000～9999)，端末 ID，利用者 ID，失敗(0)

注 [1)]　利用権限のない機能もメニューに表示される。選択しても利用できず，ログが取得される。
注記 1　個人情報にアクセスする機能の機能番号は，8000 番台である。
注記 2　機能を使って読み出せる個人情報は 1 回当たり 1 人分である。
注記 3　集計機能では個人情報を読み出すことはできない。機能番号は 7000 番台である。

次に，E 課長は，B システムへのアクセスのうち，不審な利用及びその予兆とするものを表 2 にまとめた。

表2　不審な利用及びその予兆

記号	不審な利用及びその予兆
ア	他人の利用者 ID を使おうとして，推測した利用者 ID 又は推測したパスワードでログインを試みる。
イ	有権限者が，自分の利用者 ID を用いて，業務目的外で大量の個人情報にアクセスする。
ウ	普段，深夜・早朝に B システムを利用することがない有権限者が，オフィスに人がいない深夜・早朝に，業務目的外で個人情報にアクセスする。
エ	無権限者が，自分の利用者 ID を用いて，個人情報へのアクセスを試みる。

続いて，E 課長は，①営業部の F 部長にヒアリングを行い，ログから不審な利用者 ID を抽出するための条件（以下，モニタリング条件という）を検討し，表 3 にまとめた。

表3　モニタリング条件

条件名	抽出する利用者 ID	表 2 中の対応する記号
条件 1	1 週間で，ログイン失敗が 3 回以上の利用者 ID	ア
条件 2	1 週間で，8000 番台の機能の利用成功回数が 50 回を超えた利用者 ID	イ
条件 3	1 週間で，22 時～翌日 6 時に 8000 番台の機能の利用成功回数が 1 回以上の利用者 ID	ウ
条件 4	1 週間で，［ a ］の利用者 ID	エ

保存されているログを表 3 のモニタリング条件で分析したところ，どの条件に合致する利用者 ID も見つからなかった。E 課長は，F 部長へのヒアリング結果とログの分析結果を D 部長に報告した。

報告を受けた D 部長は，今後も表 3 の条件でモニタリングを行うように指示した。E 課長は，継続的にモニタリングを行うには，機械処理が必要と考え，ツールの開発を始めた。ツールの開発では，まず，モニタリング条件が，具体的かつ機械処理が可能なものになっていることを確認した。さらに，B システムのモニタリング手順を図 1 にまとめた。

手順 1. 毎週月曜日の朝 8 時に，過去 2 週間分（前週分と前々週分）のログを B システムから抽出し，モニタリング条件に合致する利用者 ID がログ中に存在するか確認する。
手順 2. モニタリング条件に合致する利用者 ID がログ中に存在した場合は，その利用者 ID を保有している従業員を調査の対象とする。②利用者 ID が B システムに登録されていない場合は，関係するログに記録されている端末 ID をもつ端末を貸与されている従業員を，調査の対象とする。
手順 3. 調査の対象になった従業員の上司に対してヒアリングを行う。個人情報漏えいにつながる可能性があると判断された場合は，更に詳細な調査を行う。

図 1　B システムのモニタリング手順

〔モニタリングの実施〕

B システムのモニタリング手順をまとめてから 2 週間後にツールが完成し，ツールによるモニタリングを開始した。D 部長は，③モニタリングの実施を社内に通達するよう指示した。ただし，④モニタリング条件はセキュリティ上の懸念から開示しないよう指示した。

モニタリングを開始してから 3 か月後に，化粧品の専門知識をもった従業員 4 名が，商品部から営業部 1 課に異動になった。4 名は，全ての顧客を対象として，顧客の購買履歴を基に，電話又は電子メールでアフターケアをする新サービスを担当することになった。4 名は，新サービスを行うために，1 人当たり毎週 200 回近く個人情報にアクセスすることになった。その結果，4 名は表 3 のモニタリング条件 2 に該当し，業務目的のアクセスであるにもかかわらず，営業部 1 課の課長が毎週ヒアリングを受けることになってしまった。そこで E 課長は，条件 2 の利用成功回数のしきい値を 50 回から 200 回に引き上げることを D 部長に提案した。

提案を受けた D 部長は，⑤条件 2 の利用成功回数のしきい値を引き上げると，適切

なモニタリングができなくなるので，再度検討するようにE課長に指示した。E課長は再検討の結果，改善案として，表3に示すモニタリング条件2を，表4に示す新たなモニタリング条件2′で置き換えることを提案した。

表4　新たなモニタリング条件2′

条件名	抽出する利用者ID	表2中の対応する記号
条件2′	[b]，かつ，8000番台の機能の利用成功回数が前の週に比べて2倍以上の利用者ID	イ

D部長は，当分はこの改良を加えたモニタリングを実施することを了承した。さらに，D部長は，“営業部の業務は今後も変化していくと考えられる。今回は，ヒアリングの実施件数が急増したことでモニタリング条件を見直すことになったが，モニタリング条件の見直しをせずにいると，モニタリングが有効に機能しなくなったり，非効率になったりすることがある”として，E課長に対し，⑥モニタリングの有効性と効率性を維持するための施策を検討するように指示した。

その後，H社ではその施策を踏まえたモニタリングを継続して実施している。

設問1　〔モニタリングの検討〕について，(1)～(3)に答えよ。

(1)　本文中の下線①を行わなかった場合に，表3を作る上でどのような情報が不足すると考えられるか。25字以内で具体的に述べよ。

(2)　表3中の [a] に入れる条件とは何か。具体例を一つ挙げ，25字以内で述べよ。

(3)　図1中の下線②について，調査の対象とする従業員を端末IDで特定しようとするのはどのイベントの場合か。表1中のイベントから選べ。

設問2　〔モニタリングの実施〕について，(1)～(4)に答えよ。

(1)　本文中の下線③について，どのような効果があると考えられるか。20字以内で述べよ。

(2)　本文中の下線④について，モニタリング条件の開示によるセキュリティ上の懸念とは何か。40字以内で述べよ。

(3)　本文中の下線⑤について，適切なモニタリングができなくなるのは，どのよ

うな従業員が，どのようなアクセスを行った場合か。本文中の字句を用いて 60 字以内で具体的に述べよ。

(4) 表 4 中の [b] に入れる条件とは何か。具体例を一つ挙げ，30 字以内で述べよ。

設問 3 本文中の下線⑥について，モニタリングの有効性と効率性を維持するための施策とは何か。50 字以内で具体的に述べよ。