問 12　個人情報保護監査に関する次の記述を読んで，設問 1～3 に答えよ。

家具・日用品を販売している E 社は，以前から行っていた通信販売事業を拡大するために，2 年前にインターネット通信販売を開始し，その担当部門を，ネット事業部として，通信販売事業部から独立させた。同時に，インターネット通信販売用にネット通販システムを構築した。

E 社では，以前から個人情報保護の推進に取り組んでいる。JIS Q 15001 に準拠した個人情報保護規程（以下，規程という）を策定しており，1 年後を目標に，プライバシーマークの取得の準備を進めている。

E 社は，規程に基づいて，年に一度，個人情報保護に関する内部監査を行っており，今年は安全管理措置の実施状況を中心に監査を行う予定である。ネット事業部の監査については，内部監査部の F 君が監査主任を担当することになった。

〔ネット事業部の業務内容〕

ネット事業部では 10 名の社員が，会員管理とマーケティングの担当に分かれて，それぞれの業務を行っている。

(1)　会員管理業務

個人情報に関する問合せや訂正・削除の依頼などに応じて会員情報を管理する業務と，定型的な商品広告メールを定期的に送付するなどの会員サービス業務を行っている。

(2)　マーケティング業務

売れ筋商品の受注状況を分析し，キャンペーンなどの企画に反映させる業務を行っている。また，その分析結果を用いて，商品のアピール方法にきめ細かい工夫をしたメールマガジンの発行を試行している。

〔ネット通販システムの概要〕

ネット通販システムの概要は，次のとおりである。

(1)　会員管理

氏名，住所，電話番号，メールアドレスなどを保有する会員データベース（以下，会員 DB という）に対する，会員自身によるインターネット経由での入会・退会・

照会・更新の機能，及び，E 社社内の端末からの照会・更新・削除の機能をもつ。

E 社では，会員の個人情報の利用目的を，商品の送付と，受注・送付の連絡に限定する旨，個人情報保護方針で公表している。商品広告メールの送付は，①商品情報を提供するメールの送付に同意した会員に限定している。

(2) 受注処理

会員が注文を入力すると，ショッピングカートの注文内容を受注管理データベース（以下，受注管理 DB という）に格納するとともに，会員 DB を参照し，商品の送付先，支払方法などを確定する。受注データを後続の処理へ引き渡すとともに，受注が確定した旨のメールを注文した会員宛てに送付する。

(3) マーケティング用ファイル作成

受注管理 DB と会員 DB から，マーケティング業務で使用する受注分析ファイルとメールマガジン送付用ファイルを作成する。

受注分析ファイルは，注文ごとの商品情報と，注文した会員が登録した年齢層，性別，家族構成などの会員属性をもつ。会員個人が特定されないように，会員番号などはもたせていない。会員属性は商品の購買傾向との関連性の分析に使用される。

メールマガジン送付用ファイルは，商品情報を提供するメールの送付に同意した会員のデータだけを含むファイルで，会員の氏名，メールアドレス，及び会員属性をもっている。また，メールマガジン送付用ファイルは個人情報の管理対象データに指定されており，マーケティング担当者全員のユーザ ID にアクセス権が付与されている。

〔監査の実施〕

F 君は，ネット事業部の安全管理措置の実施状況を確かめるために，視察とヒアリングを開始した。

F 君は，視察の際，別の部屋での会議に出席していたマーケティング担当の G さんの PC が，会員の氏名とメールアドレスの一覧が画面に表示されたままになっていて，データの複写や印刷ができる状態になっていることを発見した。G さんにヒアリングしたところ，スクリーンセーバはネット事業部の情報セキュリティマニュアルどおり，5 分以内に起動する設定にしてあるので問題ないと思う，とのことであった。

規程では，PC で個人情報を取り扱っている途中で離席する場合は，必ず，パスワー

ドで保護された“コンピュータのロック”の状態にすることになっている。

F君は，GさんのPCの状況は，Gさん以外の人による不正な操作や，画面に表示された情報をのぞき見する行為などによって，個人情報が漏えいするリスクにつながると考え，今回の状況を②指摘事項にすべきと判断した。

次に，F君は，メールマガジン送付用ファイルのアクセス権リストを管理者から入手した。アクセス権が付与されたユーザIDと，マーケティング担当者の名簿を突き合わせたところ，1か月前にネット事業部から営業部へ転出し，個人情報を取り扱わなくなった社員のユーザIDにアクセス権が付与されたままになっていることが判明した。管理者にヒアリングした結果，ネット事業部の情報セキュリティマニュアルには，転出者の不要なアクセス権を削除せよと記されているので，半年ごとにまとめて実施しており，来月末に削除する予定である，とのことであった。

〔改善勧告〕

F君は，監査報告書に，転出した社員に対する，メールマガジン送付用ファイルのアクセス権管理の不備を指摘事項として挙げた。そして，ネット事業部の情報セキュリティマニュアルの，社員が転出する際の手続に③明記すべき具体的な記述の追加，及び，④その追加した記述どおりに実行されなかった場合に，それを検出できる対策の実施を，安全管理措置に関する改善勧告として挙げた。

設問1　〔ネット通販システムの概要〕において，E社が商品広告メールの送付先を，本文中の下線①に限定する理由は何か。個人情報保護法に基づいて，30字以内で述べよ。

設問2　〔監査の実施〕において，本文中の下線②の判断をする前に，F君が追加して実施すべきであった監査手続は何か。35字以内で述べよ。

設問3　〔改善勧告〕について，(1)，(2)に答えよ。

(1)　本文中の下線③の記述とはどのような内容か。30字以内で述べよ。

(2)　本文中の下線④の対策とは具体的にどのような内容か。30字以内で述べよ。