次の問1は必須問題です。必ず解答してください。

問1　内部不正による情報漏えいの対策に関する次の記述を読んで，設問 1～3 に答えよ。

A 社は，小，中，高校生及び大学受験生向けに通信教育を行っている。A 社では，受講生の個人情報や受講履歴などを管理する受講生管理システムと複数の業務システム（以下，A 社の各種システムという）を E 社のデータセンタで運用している。A 社の各種システムの運用管理は，社内のシステム運用管理室で，F 社から派遣された技術者（以下，F 社技術者という）が行っている。A 社のネットワーク構成を図 1 に示す。

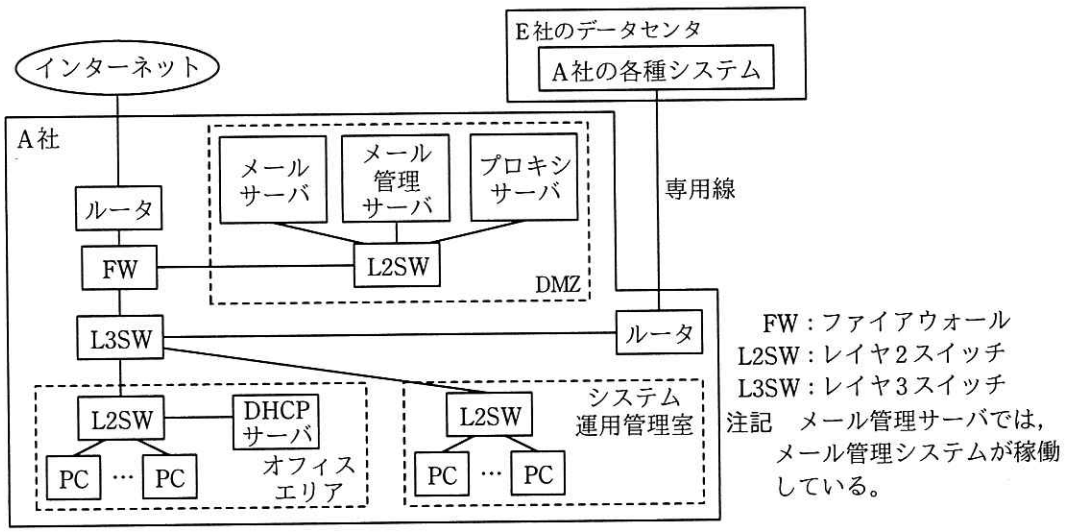

図 1　A 社のネットワーク構成（抜粋）

メール管理システムは，電子メール（以下，メールという）の誤送信を防止する目的で導入されている。PC から送信されたメールは，メール管理サーバで一旦保留され，送信者によって，宛先，メール本文及び添付ファイルに間違いがないことの確認操作が行われた後に，メールサーバに転送される。インターネットアクセスは，プロキシサーバ経由で行う。プロキシサーバでは，利用者認証は行っていない。PC には，DHCP サーバから IP アドレスなどの情報が付与されている。

A 社では，情報セキュリティ担当役員を委員長とする情報セキュリティ委員会によって，情報セキュリティ管理規程（以下，管理規程という）が整備されている。管理規程の内容を基に，次のように運用されている。

保有する情報には，管理規程に基づいて［ a ］区分を設定し，電子文書や書類に，区分に沿ったマークを表示又は押印して，誰でも判別できるようにし，区分に応じた取扱方法を定めている。F 社技術者を含む社員による，A 社の各種システムの操作に関しては，そのシステムの利用者だけに，業務上必要となる最低限の機能を利用できる［ b ］を付与している。利用者は，システムが保有する情報を，PC や許可された可搬型記憶媒体にダウンロードできる。資産価値又は重要度の高い情報の社外への持出しは原則として禁止されているが，持ち出すことが必要になった場合は，管理者である上司の承認を得た後に持ち出すことができる。社員は，社外の関係者との間で，添付ファイル付きメールの送受信を行っている。業務上不要な Web サイトへのアクセスやメールの私的利用は禁止されているが，徹底できていない。

昨今，正社員や派遣社員など，内部者の不正行為による個人情報や営業情報の漏えい事件の報道が後を絶たない。そこで，情報セキュリティ委員会では，内部不正による情報漏えいの追加の対策を実施することを決め，A 社の情報セキュリティリーダの B 主任に，情報システム部の支援を受けて対策案をまとめるように指示した。

〔現状の調査〕

B 主任は，まず，内部不正が発生する要因について調査した。内部不正は，不正のトライアングルと呼ばれる三つの要因（動機，機会，正当化）が揃ったときに，発生するおそれが増すと言われている。B 主任は，IPA の“組織における内部不正防止ガイドライン”に含まれる，“内部不正チェックシート”を利用して問題点の把握を行った。その結果，次の三つの問題があることが判明した。

(1) USB メモリなどの可搬型記憶媒体の運用が，管理規程どおりに行われていない。
(2) メールや社外の Web サイトの利用が，管理規程どおりに行われていない。
(3) 重要情報へのアクセス履歴及び利用者の操作履歴などのログの取得と管理が適切に行われていない。

これらの問題への対策を実施することによって，不正のトライアングルの要因の一つである機会が低減されることから，不正の抑止につながると考えられるので，これらの問題への対策について検討することにした。

〔内部不正に対する技術面での対策〕

問題の(1)については，可搬型記憶媒体の運用を管理規程どおりに行うことが必要である。しかし，許可されていない可搬型記憶媒体に情報をダウンロードするなどの悪意をもった行動に対しては，管理規程だけでは対処できない。そこで，PC の操作ログの取得機能や①デバイス制御機能をもつ PC 管理システムを導入することにした。

問題の(2)については，メール管理システムとプロキシサーバの設定の見直しで対処することにした。導入済みのメール管理システムの未使用の機能を図 2 に示す。

1. 情報漏えい対策機能 ・②添付ファイル付きメールに対して，指定された処理を行う。 2. メールアーカイブ機能

図 2　メール管理システムの未使用の機能（抜粋）

メール管理システムでは，新たに，図 2 中の情報漏えい対策機能を有効にする。プロキシサーバでは，URL フィルタリングを稼働させ，業務上必要な Web サイトをホワイトリストに登録してアクセスを許可し，その他の Web サイトへのアクセスは遮断する。ホワイトリストへの登録は，情報セキュリティ委員会による認定後に情報システム部が行う。ホワイトリストに含まれない Web サイトの中にも，業務上必要となるサイトが存在する可能性があるので，③当該サイトの利用を希望する者がとるべき手段を用意する。

〔ログの取得とメールのアーカイブ〕

問題の(3)の対策として，④プロキシサーバと PC 管理システムで全てのログを取得するとともに，新たに，図 2 中の，メールアーカイブ機能を有効にすることにした。

プロキシサーバのログでは，通信が行われた日時，⑤作業者の ID，アクセス先 IP アドレス，操作内容などが確認できるようになる。PC 管理システムのログでは，PC での全ての操作内容が把握できるようになる。メールアーカイブでは，送信されたメール本文及び添付ファイルの内容，送信者及び宛先が特定できるようになる。

B 主任は，これらの検討を基に，(a)PC 管理システムの導入，(b)メール管理システムの未使用機能の有効化，(c)プロキシサーバでの URL フィルタリングの稼働と設定

の見直し，(d)ログの取得と監視，の四つの対策案をまとめた。また，⑥これらの対策を社内に告知することによって，内部不正を抑止することが期待できるので，四つの対策の実施と対策内容を社内に告知することを情報セキュリティ委員会に提案し，承認された。

設問1　本文中の［　a　］，［　b　］に入れる最も適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　機能　　イ　権限　　ウ　ツール　　エ　取引　　オ　秘密

設問2　〔内部不正に対する技術面での対策〕について，(1)～(3)に答えよ。

(1)　本文中の下線①について，情報の不正持出しを抑制する方法を，35 字以内で述べよ。

(2)　図 2 中の下線②の“指定された処理”について，A 社の業務内容を考慮した場合，最も適切な処理の内容を解答群の中から選び，記号で答えよ。

解答群

ア　あらかじめ指定された上司に通知し，上司の承認後に送信する。

イ　一旦保留し，送信者によるメール内容の確認操作後に送信する。

ウ　添付ファイルを暗号化し，パスワードを別メールで送信する。

エ　添付ファイルを削除して，メールの本文だけを送信する。

(3)　本文中の下線③の手段について，20 字以内で答えよ。

設問3　〔ログの取得とメールのアーカイブ〕について，(1)～(3)に答えよ。

(1)　本文中の下線④について，ログやアーカイブなどによって法的な証拠性を明らかにすることは，一般に何と呼ばれているか。15 字以内で答えよ。

(2)　本文中の下線⑤の情報を基に作業者名を特定できるようにするために，プロキシサーバで新たに実施すべき処理について，6 字以内で答えよ。

(3)　本文中の下線⑥について，内部不正を抑止することが期待できるのはなぜか。その一つの理由を 30 字以内で述べよ。