問4　情報漏えい対策に関する次の記述を読んで，設問1～4に答えよ。

L社は，従業員数200名のソフトウェアパッケージ開発会社である。L社では，自社で開発したソフトウェアパッケージを，顧客ごとの要件に合わせてカスタマイズする業務を行っている。商談の早い段階から，開発部門，営業部門など各部門の関係するメンバ（以下，プロジェクトメンバという）でプロジェクトを編成し，プロジェクトマネージャの下で業務を行っている。

〔L社の情報システムの構成〕

L社の情報システムの構成を図1に示す。

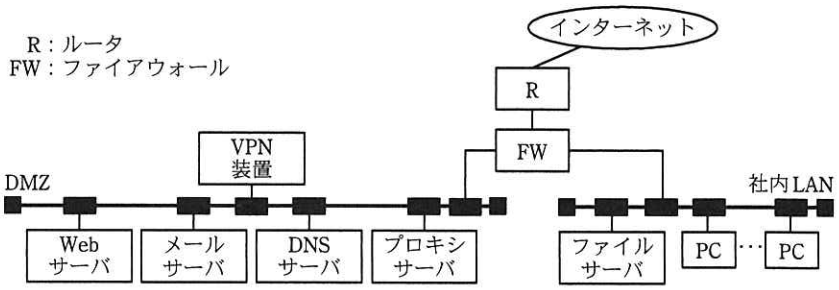

図1　L社の情報システムの構成

社内LAN上のPCからのインターネットの利用は，DMZ上のプロキシサーバ経由でのWebへのアクセスと，DMZ上のメールサーバ経由での電子メール（以下，メールという）の送受信の二つだけが許可されている。社内業務の多くは，社内LAN上のファイルサーバでファイルを共有して行われている。

〔機密情報の管理〕

L社内で扱う情報は，企業戦略上極めて重要で，かつ，ごく一部の関係者だけに開示される“厳秘”情報，関係者だけに開示される“秘”情報（以下，“厳秘”情報と“秘”情報を合わせて，機密情報という），通常の業務で使用する社内情報及び公知の情報に分類される。

L社では，①不正競争防止法に定められた営業秘密の3要件を文書管理規程に明示して，これを踏まえた分類と管理を従業員に求めている。また，機密情報にアクセス

できる者を制限するとともに，客観的認識可能性に配慮して，アクセスした情報が機密情報であるということを認識できるように管理することを求めている。

電子媒体の機密情報は，アクセス権を付与して管理している。紙媒体の機密情報は，表紙に“厳秘”又は“秘”の秘密区分を明記し，鍵が掛かるキャビネットで管理するという運用ルールを定めている。

〔情報システムのセキュリティ対策〕

L 社の情報システムでは，社内情報の保護のために図 2 に示す技術的セキュリティ対策が実施されている。人的セキュリティ対策としては，特に機密情報の管理に関して，入社時及び定期的な教育で周知徹底している。また，入社時に，セキュリティポリシ遵守の誓約書を提出させている。

1. 不正アクセス対策
   （省略）
2. アクセス制御
   (1) VPN 装置などの利用者 ID の管理　（省略）
   (2) ファイルサーバのアクセス権管理　（省略）
3. マルウェア対策
   （省略）
4. ログ管理
   （省略）
5. メールセキュリティ
   (1) 送受信メールのログ記録　（省略）
   (2) 送受信メールのマルウェア検査　（省略）
   (3) 送信メールの情報漏えい対策と誤送信対策　（省略）
6. Web フィルタリング
   (1) プロキシサーバ上でのフィルタリング
   インターネット上の Web メール，Web ストレージサービス，SNS などの Web サイトへの情報の書込みを全て遮断

（以下，省略）

図 2　L 社の情報システムの技術的セキュリティ対策

〔アクセス制御とログ管理〕

図 2 の 2.(1)及び 2.(2)は，情報システム部の社内情報基盤の運用担当者（以下，運用担当者という）が行う。機密情報を含むプロジェクトの全ての情報は，一つの専用フォルダで管理する。専用フォルダの使用開始・終了及びアクセス権の付与・解除は，

プロジェクトマネージャが運用担当者に申請する。運用担当者は，プロジェクト開始時に専用フォルダを作成し，申請されたプロジェクトメンバにアクセス権を付与する。プロジェクトメンバは，専用フォルダ内にサブフォルダを作成することができる。

プロジェクト終了時は，運用担当者が専用フォルダ内のファイルのバックアップを保管し，専用フォルダを削除する。また，従業員の退職時の運用ルールを図 3 に示す。従業員の退職時を含め，専用フォルダ内のファイルへのアクセスが不要になったときは，退職時の運用ルールなどに従って利用者 ID，アクセス権の管理を行う。

1. 退職する従業員は，所定の退職届用紙に記入・署名・押印した後，所属部門長が確認・押印して人事部に提出する。（人事規程から転載）
2. 所属部門長は，人事部から退職届受理の通知を受けると，退職する従業員のプロジェクト参画状況を確認した上で，該当する各プロジェクトマネージャに通知する。
3. 各プロジェクトマネージャは，速やかに“利用者 ID 停止・アクセス権解除申請書”を作成・押印し，運用担当者に送付する。
4. 運用担当者は，“利用者 ID 停止・アクセス権解除申請書”に従って，退職日終業時刻以降に，利用者 ID を停止し，アクセス権を解除する。

図 3　退職時の運用ルール

ファイルサーバの各フォルダへのアクセスログは，情報システム部の P 君が週 1 回分析している。例えば，短時間に大量のデータにアクセスするような不審なアクセスが見つかった場合には，上司の Q 主任，又は必要に応じて情報セキュリティ責任者である R 部長に報告し，指示を仰いでいる。

〔社外作業におけるセキュリティ対策〕

専用フォルダ内の情報は，顧客先でも必要になるので，社外持出し用 PC で社外からもアクセスできるようにしている。また，社外持出し用 PC でインターネットにアクセスして情報を収集できるようにしている。

社外からファイルサーバにアクセスする場合は，社外持出し用 PC を携帯電話網経由で L 社の VPN 装置に接続する。VPN 装置は利用者 ID とパスワードで認証を行い，社内 LAN への接続に対してリバースプロキシサーバとして動作する。

従業員が専用フォルダ内の情報をファイルサーバから社外持出し用 PC にダウンロードして使用する場合の情報漏えい対策としては，USB メモリなどの外部記録媒体へ

の書込みを禁止し，無線 LAN 機能を停止している。さらに，PC の管理権限を与えていない。また，社外持出し用 PC には，ウイルス対策ソフトを導入している。

〔インシデントの発生〕

ある日 P 君は，あるプロジェクトの専用フォルダが，その 4 日前の夜間に，外部から大量にアクセスされていたことに気付き，Q 主任に連絡した。Q 主任が確認したところ，1 週間前に退職した元従業員の利用者 ID が用いられていたことが分かった。

その利用者 ID はまだ有効であったので，Q 主任は，即座にその利用者 ID を停止することで VPN 接続ができないようにした上，②証拠を保存するために必要な措置を取り，調査を行った。当該プロジェクトのプロジェクトマネージャは 1 か月間の海外出張中で，利用者 ID の停止申請処理をしていなかった。

〔社内情報の保護対策〕

今回のインシデントの調査としてアクセスログを分析したが，機密情報への不正なアクセスは発見されなかった。しかし，事態を重く見た経営陣は，以前からセキュリティ上の懸念があった社外持出し用 PC も含め，機密情報保護の観点で，情報セキュリティ対策を見直し，速やかに改善するよう R 部長に指示し，Q 主任が対策をまとめることになった。Q 主任の検討結果の抜粋を図 4 に示す。

1. 退職者の利用者 ID の停止及びアクセス権の解除漏れ対策
   退職者などの人事情報を情報システムと連動させることで，確実に利用者 ID の停止とアクセス権の解除は可能になるが，情報システムの改修に時間が掛かるので，当面は運用改善による次の緊急対策を行うこととする。
   対策：［ a ］からの連絡を受け，運用担当者が利用者 ID の停止とアクセス権の解除を，［ b ］後，速やかに行う。
2. インターネットアクセスの情報漏えい対策
   社内からのインターネットアクセスと比較して，社外での社外持出し用 PC からのインターネットアクセスはセキュリティ上のリスクが大きいので，社内からのインターネットアクセスと同様の制限を課すために，次の対策を追加する。
   対策：社外での社外持出し用 PC からのインターネットへのアクセスは，［ c ］。

図 4　Q 主任の検討結果（抜粋）

Q 主任の検討結果をレビューした R 部長は，検討結果の対策を速やかに実施するよう指示した。さらに，R 部長は，これまでの L 社の電子媒体の機密情報に対する管理は，客観的認識可能性の点から不十分であると考え，Q 主任に，③運用上のルールを策定し，全従業員に周知徹底するよう指示した。

設問 1　本文中の下線①の営業秘密の 3 要件を，それぞれ 15 字以内で答えよ。

設問 2　本文中の下線②で利用する手法や技術のことを何というか。適切な用語を 15 字以内で答えよ。

設問 3　図 4 に示した Q 主任の検討結果について，(1)，(2)に答えよ。

(1)　1.の対策について，［ a ］，［ b ］に入れる適切な字句を，それぞれ答えよ。

(2)　2.の対策で想定しているセキュリティ上のリスクを，40 字以内で述べよ。また，［ c ］に入れる具体的な対策を，20 字以内で述べよ。

設問 4　本文中の下線③の運用上のルールの内容を，40 字以内で述べよ。