問２　データの取扱いに関する次の記述を読んで，設問 1～6 に答えよ。

V 社は，CM，プロモーションビデオなどのコンテンツを受託制作する従業員数 500 名の会社である。従業員はコンテンツの素材撮影のために国内外に出張する機会が多い。V 社は，コンテンツの制作の一部を他の事業者に委託している。委託先事業者（以下，委託先という）には個人で事業を行うデザイナやクリエイタも多い。

コンテンツの受託制作では，必要なデータを顧客から受け取り，その全部又は一部を委託先と共有して作業を進める場合がある。受け取ったデータだけでなく，当該データから派生した中間データ，及び，撮影又は作成された素材も含めて，適切な保護が必要である。

V 社では，従業員には，業務に応じてデスクトップ PC（以下，DPC という）又はノート PC（以下，NPC という）を貸与している。従業員の識別と認証に必要な利用者情報は，ディレクトリサーバ（以下，D サーバという）で管理している。D サーバは IT 部が運用している。

〔オンラインストレージサービスの導入決定〕

V 社では，業務効率の向上のために，クラウドベースのオンラインストレージの導入を決定し，IT 部の M 部長を導入責任者に任命した。オンラインストレージの用途は，次のとおりである。

・出張者と内勤者の間で，サイズが大きいデータを共有する。
・委託先と V 社の間で，データを共有する。
・デモやその他の目的のためにデータを取引先に送信する。
・NPC などにプレゼンテーション資料を配布する。

M 部長は，IT 部内のチームに複数のオンラインストレージサービスを比較検討させた結果，X 社の Q サービスを採用することにした。

〔Q サービスの概要〕

Q サービスの利用者は，インターネット経由で，Q サービスに任意のファイルを保管できる。Q サービスの概要を表 1 に，Q サービスの利用者用の専用アプリケーショ

ンソフトウェア（以下，同期アプリという）の概要を表 2 に，V 社における Q サービスの利用方法案を図 1 に，それぞれ示す。

表 1　Q サービスの概要

項目	説明
アカウント管理	・利用者に，個別のアカウントを割り当てる。 ・利用企業は，利用者のアカウントを自社で登録して管理するための機能（以下，管理者機能という）を利用できる。アカウントをもたない者も，Q サービスの一部の機能は利用できる（項目“ファイル管理”参照）。
管理者機能	・管理者は，アカウントの作成・停止・再開・廃止，パスワードの初期発行・再発行，ファイル及びフォルダへのアクセス履歴の閲覧，その他の管理のための機能を利用できる。
利用者識別・認証	・利用者 ID とパスワードを用いて利用者を識別・認証する。 ・利用者は，インタフェースを利用して，パスワードを変更できる。
ファイル管理	・各アカウントには，それぞれ専用のフォルダ（以下，ルートフォルダという）が与えられる。利用者が登録したファイルやフォルダは，ルートフォルダの下に配置される。 ・利用者は，インタフェースを利用して，次の機能を実行できる。 - ファイルの登録・更新・削除・取得・プロパティの閲覧 - フォルダの作成・削除・閲覧・プロパティの閲覧 - バックアップからのファイルの復元・取得・削除（補足説明 1 参照） - 他の利用者へのファイル又はフォルダのアクセス権の付与・変更（補足説明 2 参照） - ファイルにアクセスするための共有リンクの作成・削除（補足説明 3 参照） 【補足説明】 1. ファイルが更新又は削除された場合，元のファイルはバックアップとして保管される。利用者は，バックアップとして保管されたファイルのうち，バックアップから削除が行われていないものを，復元・取得できる。 2. 他の利用者に付与できる権限には“読み”と“読み書き”の 2 種類がある。“読み”は，ファイルの取得機能などの，ファイルやフォルダの変更を伴わない機能を利用する権限である。“読み書き”は，“読み”の権限に加え，ファイルの更新機能などの，変更を伴う機能を利用する権限である。 3. アカウントをもたない者にファイルを配布するための URL を“共有リンク”という。Web ブラウザで当該 URL にアクセスすると利用者認証なしにファイルを取得できる。 4. アカウントが廃止されると，そのアカウントで登録したファイルとフォルダが削除される。
インタフェース	・同期アプリ，Web インタフェース，API の三つのインタフェースがある。 - 同期アプリの機能については，表 2 に概要をまとめる。 - Web インタフェースを用いる利用者は，Web ブラウザで Q サービスの Web サーバ（w.example.com）にアクセスし，Q サービスの各機能を利用する。 - API を用いて，Q サービスと連携するアプリケーションソフトウェアを開発できる。
暗号化	・同期アプリと Q サービス間の通信，及び Web ブラウザと Q サービスの Web インタフェース間の通信は，TLS で暗号化される。 ・Q サービスは複数のサーバで構成されており，ファイルは，他の利用企業又は個人利用者のファイルと同じサーバに保管される場合がある。登録されたファイルは，暗号化して保管される。暗号鍵は，サーバごとに生成し，Q サービス内で管理する。利用者が Q サービスのインタフェースを利用してファイルにアクセスすると，Q サービスは，ファイルを復号した後に引き渡す。

注記　Q サービスでは，“利用者”とは，アカウントをもつ者だけを指す。

表2　同期アプリの概要

項目	説明
ファイル管理	・表1の項目“ファイル管理”の機能を提供する。
同期機能	・同期アプリは，利用者のPCのローカルディスク上に特別なフォルダ（以下，同期用フォルダという）を作成する。 ・同期用フォルダには，利用者のアカウントのルートフォルダと，当該利用者がアクセス権をもつ他の利用者のファイル及びフォルダの複製が作成され，これらはQサービス上のそれぞれのフォルダ又はファイルと自動的に同期される。例えば，利用者が同期用フォルダ配下に複製されたファイルを更新した場合，更新内容は，Qサービスの該当ファイルにも適用される。また，更新されたファイルについて，他の利用者にアクセス権が付与されていた場合，他の利用者のPCの同期アプリがQサービスの該当ファイルを同期用フォルダにコピーする。
同期管理	・同期機能について設定を行う機能を提供する。自動的な同期を行わない場合は，その旨を設定できる。 ・同期の状況を表示する。
その他	・同期アプリは，QサービスのAサーバ（a.example.com）と通信し，各処理を行う。プロキシサーバを経由した通信もサポートしている。 ・同期アプリは，X社がインターネットで配布しており，誰でもダウンロードできる。

・Qサービスの利用に関する社内の管理はIT部が主管する。
・IT部は，業務上Qサービスの利用が必要なV社の従業員及び委託先の作業者に対してアカウントを作成する。

図1　Qサービスの利用方法案（抜粋）

〔Qサービスの試験導入〕

M部長は，Qサービスの導入に先だって，3か月間の試験導入をすることにした。オンラインストレージの利用が想定される部門の中から，試験導入への参加者を偏りなく選ぶことにし，最終的に30名の参加者を決定した。この中には，委託先の5名のクリエイタが含まれていた。試験導入では，次の項目を確認することにした。

・機能は，利用目的に照らし，必要十分で使いやすいか。
・管理は，シンプルで，実用に耐えるか。
・セキュリティ及びその他の問題点がないか。

以降，Qサービスについては，V社が利用する部分だけに限定して述べる。

〔Qサービスの試験導入において表出した問題〕

試験導入の結果，機能及び管理については大きな問題は発見されなかった。しかし，セキュリティについては，同期アプリが，マルウェア感染を拡散させるという問題が認識された。

実際に発生した事件は次のとおりである。委託先のクリエイタがPCで編集していたファイルがマルウェアに感染した。そのことに気付かずにクリエイタがWebインタフェースを使って当該ファイルをQサービスに登録した結果，同ファイルにアクセス権をもつ複数の利用者のPCの同期アプリが，感染ファイルをQサービスから同期用フォルダにコピーした。本件では，それぞれのPCにインストールされていたウイルス対策ソフトが感染ファイルを検知したので，大事には至らなかった。しかし，V社では，事態を重く受け止め，対応について検討することになった。

〔Qサービス利用方法の見直し〕

M部長は，PCのウイルス対策ソフトだけではなく，複数の対策が必要だと考え，IT部のUさんに，情報セキュリティ室のR主任の支援を受けて，マルウェア感染ファイルの拡散について対応を検討するように指示した。

Uさんは，検討を進め，専用のサーバ（以下，同期用FSという）及び専用のディスク（以下，同期ディスクという）を介して，社内ネットワークに接続されたPCとQサービス間でのファイルの交換を行う仕組みを提案した。そのネットワーク構成を図2に，ファイル交換の仕組みの概要を図3に，同期用FSの機能の説明を図4に示す。

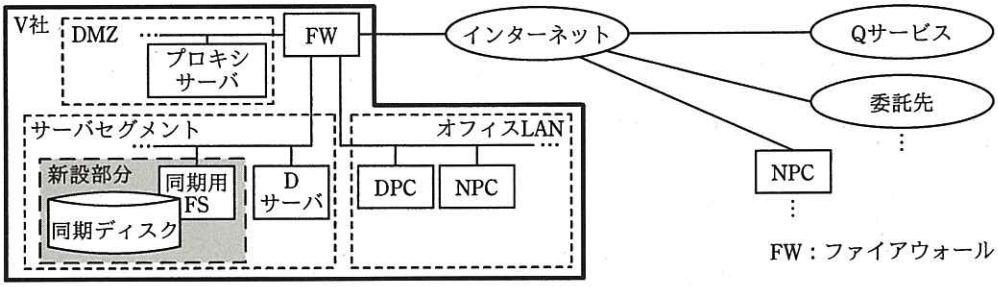

図2　ネットワーク構成

・同期用FSは，Qサービスに登録された利用者のアカウントのルートフォルダ及びその配下のフォルダ（以下，Qサービス利用者フォルダという）を監視し，新たに登録された又は更新されたファイルがある場合は，それを取得してマルウェアスキャンを行った後，同期ディスクに保管する。
・①同期アプリの利用を禁止する。
・同期用FSへのアクセスは，FWによって，オフィスLANからだけに限定する。

図3　ファイル交換の仕組みの概要

1. ファイルの同期
・ルートフォルダの複製を同期用 FS 内の同期ディスクに保持し，ファイルを同期する。同期は次のように行う。
A) Q サービス利用者フォルダにおいて，ファイルの登録又は更新があった場合は，当該ファイルを取得してマルウェアスキャンを行う。その結果，問題がなければ同期ディスクに反映する。マルウェアが検知されたら，Q サービス利用者フォルダにある当該ファイルを削除し，もし対応するファイルが同期ディスクに存在する場合はそれも削除する。登録・更新以外の変更があった場合は，同等の変更を同期ディスクに反映する。
B) 同期ディスクのファイルに変更があった場合は，Q サービス利用者フォルダにある対応するファイルに反映する。
2. フォルダの同期
・Q サービス利用者フォルダに変更があった場合は，同期ディスクの対応するフォルダに反映する。
・同期ディスクのフォルダに変更があった場合は，対応する Q サービス利用者フォルダに反映する。
3. アカウントとアクセス制御
・D サーバに登録された従業員の利用者情報と Q サービスのアカウントの対応表をもつ。
・同期ディスクにアクセスがあった場合，D サーバと連携して従業員を識別した後，前記の対応表を基に利用者のアカウントを判別する。この結果に基づいて，次の処理を許可する。
A) 判別されたアカウントの Q サービス利用者フォルダ又はそこにあるファイルに対応する同期ディスクのフォルダ又はファイル：全ての処理
B) 他の利用者のファイル又はフォルダに対応する同期ディスクのファイル又はフォルダ：判別されたアカウントに付与された権限内の処理
4. 補足事項
・Q サービスに保管されたバックアップのファイルについて，同期用 FS は一切処理を行わない。

図 4　同期用 FS の機能の説明（抜粋）

U さんがこれらの検討結果を M 部長に報告したところ，②試験導入において表出した問題を踏まえると，同期用 FS には，マルウェア対策に関して追加すべき機能があると指摘された。U さんは追加機能を提案し，M 部長は，U さんの提案どおり対応を進めることを承認した。その後，Q サービスと同期用 FS の利用が，全社で開始された。

〔顧客からの要求〕

V 社で Q サービスの利用を開始してから 1 年が経過した頃，重要な顧客である J 社から，情報セキュリティに関して新しい要求の通知があった。J 社の別の委託先において，J 社が開示した新製品に関する CAD データが漏えいするという事件が発生し，対策の一環として，J 社が重要なデータを開示する全ての委託先に対して，新たな要求を課す方針になったとのことであった。J 社からの要求を図 5 に示す。

J社が開示する全ての重要な情報（以下，J社重要データという）について，次の措置を行うこと
・業務上，必要最小限の者しかJ社重要データにアクセスできないように管理する。
・J社重要データをインターネット上に送信する場合には，暗号化する。
・J社重要データを社外に保管する場合には，暗号化する。
・J社重要データを可搬型機器又は可搬型デバイスに保管する場合には，暗号化する。
・業務上不要となったJ社重要データは，直ちに，J社に返却するか，削除する。
・何らかの事故が発生した場合に備え，非常時の連絡体制・手順を確立する。
・J社重要データについて，法令による保護が受けられるように，十分に配慮して管理する。
・J社から受託した業務の一部を再委託する場合は，当該委託先に対して本要求と同等の措置を求め，かつ，その実施について監督する。

図5　J社からの要求（概要）

次は，J社からの要求に関する，M部長とUさんとの会話である。

Uさん：J社から受け取るデータの大半はJ社重要データですが，当社は，J社の要求を満たしていないと思います。

M部長：お客様のデータの保護は最優先事項だ。最近，J社以外にも，複数のお客様から，データの取扱いについての問合せや要求が寄せられている。この機会に，当社の現状を調査し，必要なら見直すことにしよう。

Uさん：分かりました。ところで，法律の規定との関係はどうでしょう。お客様のデータは，［　a　］で規定されている［　b　］に該当しますか。

M部長：［　a　］で規定されている［　b　］に該当するためには，当該データが，秘密として管理されていること，有用な情報であること，及び［　c　］こと，の三つの要件を満たす必要がある。秘密として管理されているというためには，その情報が，客観的に見て秘密として管理されている状態になっていなければならない。

Uさん：他の法令はどうでしょうか。

M部長：［　d　］の235条で規定されている窃盗罪は，他人の財物を窃取した場合に適用される。しかし，情報そのものは物ではなく，財物には当たらないので，適用は難しいという解釈があるようだ。思想又は感情を創作的に表現したと考えられるデータであれば，［　e　］の保護の対象となる。また，サーバなどの電子計算機に接続して行う不正行為に焦点を当てた［　f　］がある。ただし，［　f　］はネットワークを通じて行われる攻撃を対象としているので，攻撃対象の機器を直接操作するケースは

対象外だ。

Uさん ：ありがとうございます。教えていただいたことも参考に調査を進めます。

〔顧客データの取扱要件〕

U さんは，受託業務で顧客から開示を受けた重要なデータ（以下，顧客データという）の取扱状況を調査し，M 部長に報告した。M 部長は，調査結果を見て，顧客データの取扱いについて改善が必要だと判断した。M 部長は，U さんに，J 社の要求を満たすような顧客データの取扱要件及びその実装方法，並びにその他の必要な措置について検討して提案するように指示した。

U さんは，業務上の必要性のある従業員だけがアクセスできる場所への顧客データの保管，及び顧客データを NPC 又はオンラインストレージに保管する場合の暗号化について検討した。

〔NPC のディスクの暗号化〕

U さんは，顧客データの暗号化のため，NPC のディスクの暗号化，及びオンラインストレージに登録するデータの自動暗号化の導入を検討した。

U さんが検討した，NPC のディスクの暗号化方式を表 3 に示す。

表 3　NPC のディスクの暗号化方式

名称	説明
フルディスク暗号化方式	ディスク内の全ての領域を暗号化する方式。PC の全ディスクにこの方式を用いた場合，パスワードがないと [g] を起動できない。起動後，データの保護は，PC の [g] が提供する機能に委ねられる。本方式に対応する製品の多くは，PC が休止モードになる際にメモリの内容を書き出すハイバネーション用ファイルの [h] に対応している。
仮想ディスク暗号化方式	コンテナと呼ぶ仮想的な入れ物を用いて暗号化する方式。コンテナは仮想ディスクとして機能する。コンテナ内にアクセスする場合，利用者の認証が行われる。認証に成功すると，一定の間，通常のディスクと同様に，コンテナにファイルやフォルダを保管したり取り出したりすることができる。データは暗号化された上でコンテナ内に保管される。コンテナは，PC のデータディスク，USB メモリなどに置かれる。スワップ領域やハイバネーション用ファイルには [h] されていない状態のデータが存在する可能性があるが，これらは保護されない。
ファイル・フォルダ暗号化方式	ファイル単位・フォルダ単位で暗号化する方式。暗号化されたデータは，一つのファイルになる。当該ファイルへのアクセス権があれば，鍵情報を知らなくても，格納されたファイルやフォルダの名称及び他の属性情報を取得できる場合がある。

U さんは，検討した結果，フルディスク暗号化方式を採用することを提案した。

次は，暗号化製品に関する，Uさんと R 主任との会話である。

Uさん ：幾つかの暗号化製品の説明書に“暗号の利用モード”や“CBC モード”という記述がありました。これは何でしょうか。

R 主任 ：利用モードとは，ブロック暗号アルゴリズムを用いてブロック長よりも長いデータを暗号化する際に使われる技術のことだ。CBC モードは，よく使われる利用モードの一つだよ。

Uさん ：利用モードは他にもあるのですか。

R 主任 ：図 6 に代表的な暗号の利用モードがまとめられているので見てごらん。ブロック暗号アルゴリズムの利用時には，暗号化の目的や利用方法に合わせて，適切な利用モードを選ぶ必要がある。例えば，③ディスクやファイルの暗号化に ECB モードをそのまま用いるのは，セキュリティ上の問題がある。

利用モードによって，ランダムアクセス時の性能が大きく異なる場合もある。例えば，512 バイトの平文 P を，ブロック長が 128 ビットのブロック暗号アルゴリズムで暗号化した暗号文 C があり，この暗号アルゴリズムでは平文と暗号文の長さは同じとする。平文 P において 1,025 ビット目から始まる 1 ブロック分のデータを修正した場合，平文 P の修正に対応して暗号文 C を修正するためには，暗号化処理を，ECB モードでは [i] 回，CBC モードでは [j] 回実行しなければならない。

また，別の暗号文 C’ で，513 ビット目から始まる 1 ブロック分のデータを復号するためには，暗号化処理又はその逆処理を，ECB モードでは [k] 回，CBC モードでは [l] 回，OFB モードでは [m] 回実行する必要がある。

複数ブロックの並列処理は，[n] の場合，暗号化時は不可能だが，復号時は可能だ。[o] の場合は，鍵ストリームに相当するデータを事前に計算することができる。

ただし，一部の利用モードは，特定の攻撃に弱いので注意が必要だ。

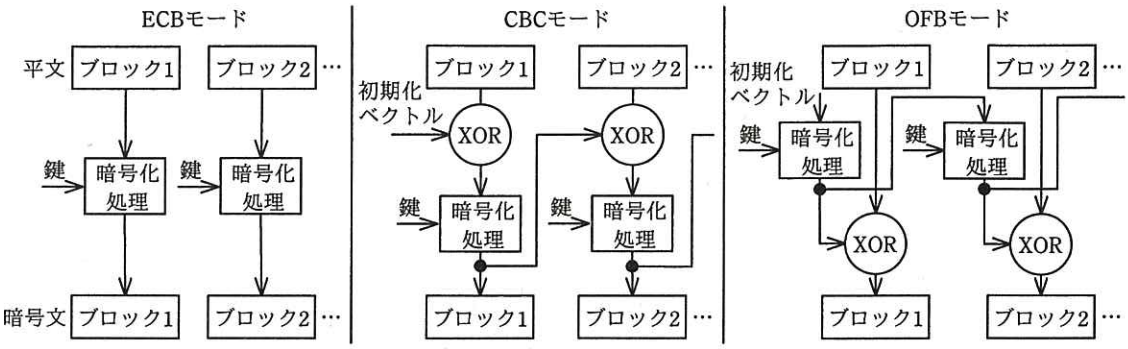

図 6　代表的な暗号の利用モード

〔同期用 FS の機能拡張〕

表 1 に示したように，Q サービスは，元々，登録されたファイルを自動的に暗号化する機能をもつ。しかし，Q サービスの暗号化機能は，④Q サービスに対するクラッキングや X 社自身のある種の行為に対して効果が期待できない場合があり，これを補完する措置が必要と考えられた。一方，V 社内では，Q サービスの有益性が高く評価されており，継続利用したい。そこで，U さんは，同期用 FS の機能を拡張し，Q サービスに登録する一部のファイルを自動的に暗号化する措置を提案した。同期用 FS の拡張機能を図 7 に，ファイルの暗号化と復号のフローを図 8 に，それぞれ示す。

1. 機密フォルダと暗号化フォルダの定義・導入
・利用者が同期ディスク中のフォルダに“_[c1]”で始まる名称を付けると，そのフォルダは機密フォルダになる。機密フォルダの同期先となるQサービス上のフォルダを暗号化フォルダという。
2. 機密フォルダにアクセスしたときの処理
・利用者が機密フォルダにファイルを登録した場合又は機密フォルダ内のファイルを更新した場合，同期用FSは，ファイルを暗号化した上で，Qサービス上の暗号化フォルダに登録するか，暗号化フォルダ内のファイルを更新する。
3. Webインタフェースを用いて暗号化フォルダにアクセスしたときの処理
・利用者は，暗号化フォルダにファイルを登録する場合又は暗号化フォルダ内のファイルを更新する場合，事前に，指定された鍵と暗号化ソフトを用いてファイルを暗号化する（“4. 暗号化のアルゴリズムと鍵”参照）。同期用FSは，暗号化されたファイルを取得してマルウェアスキャンを行い，マルウェアが検知されなければ，復号した上で，同期ディスク中の対応する機密フォルダに配置する。暗号化フォルダに平文のファイルが登録された場合又は平文のファイルで既存のファイルが更新された場合，同期用FSは当該ファイルを暗号化して更新した後，利用者に警告メールを送信する。また，暗号化された当該ファイルは，初めから正しく暗号化されたファイルで更新された場合と同様の手続で，同期ディスクに同期される。
・利用者は，暗号化フォルダからファイルを取得した場合，指定された鍵と暗号化ソフトを用いて復号した上で利用する。
4. 暗号化のアルゴリズムと鍵
・暗号化のアルゴリズムは鍵長128ビットのAES，暗号の利用モードはCBCモードとする。
・同期用FSは，機密フォルダ又は暗号化フォルダが作成された際に，作成されたフォルダごとに数字16文字のパスワードをランダムに生成し，さらにそれを基に鍵を生成する。⑤生成された鍵は，当該フォルダ内に登録されるファイルの暗号化と復号だけに利用される。ただし，名称が“_[c1]”で始まるサブフォルダがある場合は，そのフォルダを別の機密フォルダ又は暗号化フォルダとみなし，新しいパスワード及び鍵を割り当てる。
・同期用FSは，生成したパスワードを，当該フォルダの利用者に電子メールで通知する。
・暗号化ソフトは，暗号化と復号の機能をもつPC用ソフトウェアであり，利用者に配布される。

図7　同期用FSの拡張機能（抜粋）

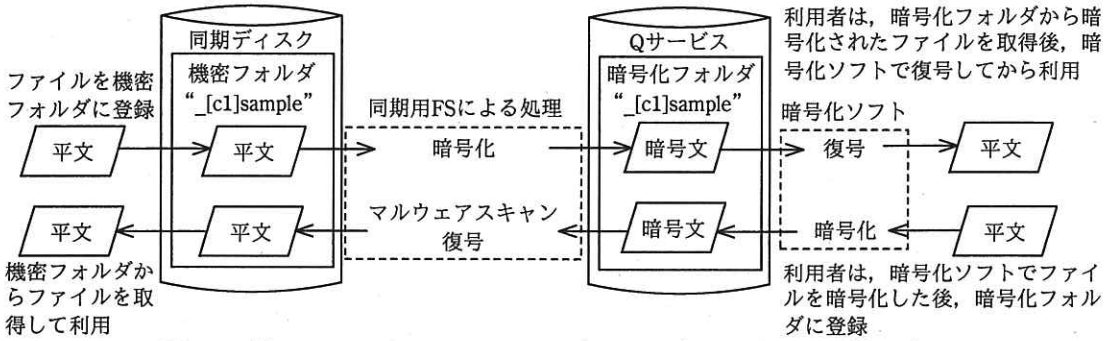

図8　同期用FSによるファイルの暗号化と復号のフロー（概要）

Uさんは，図7の方法では，⑥暗号化対象ファイルに関係する情報の一部は秘匿されないが，セキュリティ上容認できると考えた。

Uさんが図7のパスワードについてR主任に相談したところ，R主任は問題を指摘した。R主任は，図9を示し，数字16文字のパスワードの場合の数は，英数字 [p] 文字のパスワードの場合の数より小さいことを説明した。また，この場

合の数は，最近のコンピュータの能力向上を考慮すると，いつまでも安全とはいえないと指摘した。Uさんは，R主任の指摘を受けて，パスワードの構成を見直した。

英数字 x 文字のパスワードについて，その場合の数が，数字 16 文字のパスワードの場合の数より大きくなる最小の x を考える。ただし，大文字と小文字は区別する。

次の式から，求めるパスワードの文字数 x は [p] となる。

$$[\ q\ ]^{x} > 10^{16}$$

$$x > \frac{16\log_{10}10}{\log_{10}[\ r\ ]+\log_{10}[\ s\ ]} = [\ t\ ]$$

参考 $\log_{10}2 \fallingdotseq 0.301$，$\log_{10}3 \fallingdotseq 0.477$，$\log_{10}13 \fallingdotseq 1.114$，$\log_{10}31 \fallingdotseq 1.491$

図9　パスワードの検討

〔レビューと修正〕

Uさんは，IT部と情報セキュリティ室のメンバ（以下，WGという）に，顧客データの取扱要件とその実装方法の案についてのレビューを依頼した。レビューの結果，オンラインストレージについて，次の点が指摘された。

・⑦マルウェア感染ファイルの拡散防止対策が不十分である。

・⑧暗号化フォルダに登録された一部のファイルが，平文のままQサービスに保管され続ける場合がある。

Uさんは，これらの指摘について検討し，修正案を作成した。修正案について，再度WGでレビューした結果，指摘は解決されていることが確認された。

〔M部長の最終確認〕

Uさんは，修正案及びその他の必要な措置について，M部長に報告した。

M部長：修正案は技術的に妥当であり，効果がある。当社は委託先との契約の中で，顧客データについて目的外利用の禁止と適切な管理を委託先に要求している。だが，事故の発生を防ぐ点で十分だろうか。

Uさん：当社の現状について調査した結果，委託先の管理が不十分だったので，IPAが公表している“組織における内部不正防止ガイドライン”を参考にして，技術的対策とは別に⑨対策をまとめました。

M部長はUさんの提案を承認し，提案どおり見直しが行われることになった。

設問1　〔Qサービス利用方法の見直し〕について，(1)，(2)に答えよ。

(1)　図3中の下線①について，この措置は，マルウェア感染ファイルの拡散がどのように起こることを想定したものか。40字以内で具体的に述べよ。

(2)　本文中の下線②について，同期用FSにどのような機能を追加すればよいか。追加機能の内容を，30字以内で具体的に述べよ。

設問2　〔顧客からの要求〕について，(1)，(2)に答えよ。

(1)　本文中の［ a ］，［ d ］～［ f ］に入れる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　刑法	イ　個人情報保護法
ウ　サイバーセキュリティ基本法	エ　情報公開法
オ　著作権法	カ　犯罪収益移転防止法
キ　不正アクセス禁止法	ク　不正競争防止法
ケ　マイナンバー法	コ　民法

(2)　本文中の［ b ］，［ c ］に入れる適切な字句を，［ b ］は5字以内で，［ c ］は15字以内でそれぞれ答えよ。

設問3　〔NPCのディスクの暗号化〕について，(1)～(4)に答えよ。

(1)　表3中の［ g ］，［ h ］に入れる適切な字句をそれぞれ5字以内で答えよ。

(2)　本文中の下線③について，セキュリティ上の問題を，45字以内で具体的に述べよ。

(3)　本文中の［ i ］～［ m ］に入れる適切な数値を答えよ。

(4)　本文中の［ n ］，［ o ］に入れる適切な暗号の利用モードを，図6中の三つの利用モードの中から選んで答えよ。

設問4　〔同期用FSの機能拡張〕について，(1)～(4)に答えよ。

(1)　本文中の下線④について，Qサービスの暗号化機能の効果が期待できないのは，Qサービスのどのような仕様によるものか。30字以内で述べよ。

(2)　図7中の下線⑤について，別の方法として，一つの鍵を全ての機密フォル

ダで共有して利用する方法がある。これらの二つの方法を比較した場合に，下線⑤の方法が優れている点は何か。35 字以内で具体的に述べよ。

(3) 本文中の下線⑥について，暗号化対象ファイルに関係するどのような情報が秘匿されないか。二つ挙げ，それぞれ 15 字以内で答えよ。

(4) 本文中又は図 9 中の [p] ～ [t] に入れる適切な数値を答えよ。[p] ～ [s] は整数で，[t] は小数第 2 位を四捨五入して，小数第 1 位まで求めよ。

設問 5 〔レビューと修正〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑦について，指摘に対応するには，図 7 の拡張機能をどのように修正すればよいか。修正内容を，50 字以内で具体的に述べよ。

(2) 本文中の下線⑧について，どのような場合にファイルが平文のまま Q サービスに保管され続けるのか。35 字以内で具体的に述べよ。また，この状況を防ぐには，同期用 FS の拡張機能にどのような修正を行えばよいか。修正内容を 30 字以内で述べよ。

設問 6 本文中の下線⑨について，U さんがまとめた対策を，35 字以内で述べよ。