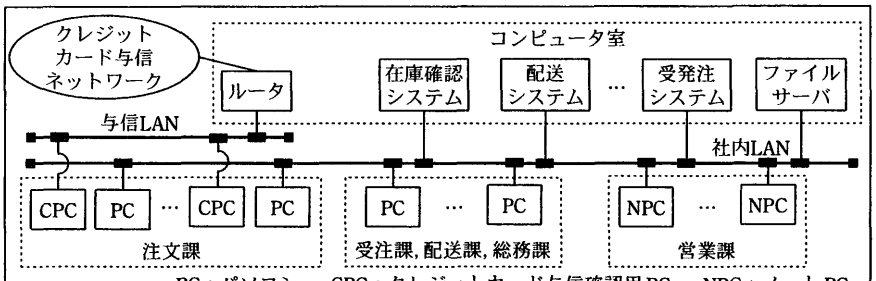
問1　情報漏えい防止システムの導入に関する次の記述を読んで，設問1～4に答えよ。

W社は，社員数40名の食料品の通信販売会社である。カタログ冊子には，常時1，000点以上の商品を掲載し，とじ込みの注文書をファックス又は郵送によって受け付け，商品を発送している。注文書には，注文商品番号，個数，注文者氏名，商品配送先，クレジットカード番号が記入される。一度注文を受けた顧客に対しては，ダイレクトメールを郵送しており，その効果もあって，最近では毎日平均1，000件を受注し，月間売上高は1億円を超え，業績を伸ばしている。

また，業務量が時期によって変動するので，アルバイトを活用している。アルバイトの採用，教育，管理は，各課の裁蔦に任せている。

オフィスは，雑居ビルの4階フロア全面を借りているが，エレベータホールや廊下はオープンスペースになっている。各課間で注文書を受渡しする際には，オープンスペースを経由するので，注文書の受渡しを確実に管理するために，授受簿に受渡しを記録している。各課の業務概要と情報システムの構成は，図1のとおりである。



PC：パソコン，　CPC：クレジットカード与信確認用PC，　NPC：ノートPC

受注課

(1)　受注課の受注係は，随時，ファックス及び郵便受けから注文書をピックアップする。

(2)　受注係は，採番表を用いてユニークな通し番号からなる受注番号を付与し，注文書に記入する。

(3)　受注係は，随時，注文書を束ね，授受簿に受渡しを記録して，受注課事務室を出てオープンスペースを通って注文課の事務室に行き，注文課の受付係に手渡しする。

注文課

(1)　注文課の受付係は，受注課の受注係から注文書の束を受け取り，内容を確認して授受簿に受渡しを記録する。

(2)　受付係は，注文係に注文書を割り振る。

(3)　注文係は，注文書ごとに在庫引当て及び請求処理を行う。この操作では，在庫確認システムにアクセスするPCと，社外のクレジットカード与信ネットワークにアクセスするCPCを同時に使用する。クレジットカード与信ネットワークは，社内LANと接続できない契約になっているので，注文係はPCとCPCを起動し，それぞれの画面を見ながら必要な情報を転記入力する。

(4) 在庫引当てが完了した後は，注文書の確認欄に商品手配済のチェック記号を記入し，受付係に手渡しする。
(5) 受付係は，注文書を点検し，授受簿に受渡しを記録して，注文課事務室を出て，オープンスペースを通って配送課事務室に行き，配送課の受付係に手渡しする。

配送課
(1) 配送課の受付係は，注文課の受付係から注文書を受け取り，内容を確認して授受簿に受渡しを記録する。
（省略）

総務課
(1) 総務課の文書係は，配送課の受付係から注文書を受け取り，内容を確認して授受簿に記録し，保管庫に入れて保管する。
（省略）

営業課
(1) 外出時には，社外秘情報をすべて消去した上でNPCを持ち出す。
（以下，省略）

図1 各課の業務概要と情報システムの構成

W社は，情報管理が適切に行われているかどうかについて，第三者の点検を受けることにし，セキュリティ評価で定評のあるB社に依頼した。B社のセキュリティコンサルタントであるZ氏は，依頼に基づいて，各課の実態を調査し，図2に示す点検報告書をW社に提出した。

授受簿による運用が適切に行われているか，そのほかに情報管理上の課題がないかどうかについて調査を行い，課題を次の(1)～(3)にまとめた。運用ルールの徹底を図るとともに，システム面での対策を検討すべきである。
(1) 授受簿の記録の不整合
文書の棚卸しを行ったところ，授受簿に受渡しの記録があるにもかかわらず原本が見当たらない“原本紛失”と，原本があるにもかかわらず授受簿に受渡しの記録がない“記録漏れ”が，それぞれ数件見つかった。ヒアリングによれば，繁忙期に業務が混乱したことが原因と推測される。
(2) PC管理の不備
①休憩時間などに，事務室を不在にしているにもかかわらず，PC，CPC，NPCがログインしたまま放置されていることがある。このような管理では，ほかの社員やアルバイト，来客などによるなりすまし及びのぞき見のリスクがある。
(3) アルバイトの情報セキュリティ意識の高低差
アルバイトの情報セキュリティ意識をアンケート調査したところ，各課間の高低差が大きいことが判明した。意識の低い課では，情報漏えいなどのリスクが大きい。

図2 点検報告書（要旨）

〔情報漏えい防止対策の検討と実施〕

報告を受けた社長は，情報管理の徹底を訓示するとともに，具体的な対策を検討するよう，情報セキュリティアドミニストレータのK君に指示した。K君は，対策の素案を次のようにまとめた。

(1) 物理的セキュリティ

すべての事務室の扉に電子錠を設置し，暗証番号を入力しないと入室できないようにする。

(2) 注文書の電子化

新たにイメージスキャナを導入し，受注課で注文書を受け付けた時点で，直ちにイメージスキャナで画像情報として電子化する。注文書の原本は，すぐに総務課で厳重に保管する。

(3) ワークフローシステムの導入

ワークフローシステムを既存システムに追加導入し，受注課から注文課，配送課及び総務課への注文書の手渡しと，各課間の受渡しを記録する授受簿は廃止し，ワークフローによって授受記録を管理する。

(4) IC カードの導入

IC カードを導入し，社員及びアルバイトに 1 枚ずつ配付する。すべての PC，CPC，NPC に IC カードリーグを接続し，IC カードを装てんした状態のときだけ使用できるようにする。

(5) ログイン情報管理サーバによる認証の一元化

ログイン情報管理サーバを新設し，社内 LAN に接続する PC，NPC は，このサーバと通信できる状態のときだけログインできるようにする。

(6) 操作制限，出力制限の実現

W 社内のすべての PC，CPC，NPC に対して，離席時の操作制限と外部記録装置やプリンタへの出力制限を行う。

(7) 情報漏えい防止システムの導入

上記（4）～（6）を実現するために，次の表に示す C 社製情報漏えい防止システムを導入する。

(8) 情報管理面での施策の弓削ヒ

②図 2 の点検報告書の課題 3 に対応するための施策を実施する。

表　C 社製情報漏えい防止システムの仕様

機能	仕様内容
ユーザ認証	ログイン時のユーザ認証は，IC カードの情報とディレクトリサーバの情報を照合するディレクトリサーバ認証方式と，パソコン内にあらかじめ導入された情報と IC カードの情報を照合するスタンドアロン認証方式のいずれかを選べる。ディレクトリサーバ認証方式は，ディレクトリサーバと通信できる環境の場合だけパソコンを起動できる。
ファイル暗号化	ファイルは自動的に暗号化され，IC カードを装てんしないと復号できない。これによって，パソコンが盗難に遭っても，情報漏えいのリスクを低減できる。
出力制限	フロッピー装置，CD-R 装置，USB メモリなどの記録装置への書込み，及びプリンタによる印刷を禁止できる。ただし，これらの禁止は，管理者の許可があれば，一時的に解除できる。
操作制限	IC カードをパソコンから外すと，パソコンの画面が暗転してロック状態になり，操作を禁止できる。

注　IC カードは，多機能型が利用でき，入退室かぎ，クレジットカード，電子マネーなどと一体化して利用できる。

この素案に基づいて検討を行ったところ，〔情報漏えい防止対策の検討と実施〕の(4) に関して，③ある課では業務効率が著しく低下することから，導入が困難である

ことが分かり，特例的な運用によって解決することにした。

また，NPC と CPC のユーザ認証方式には［ a ］方式を適用できないことが分かったので，［ b ］方式を採用することにした。

W 社では，これらを踏まえて，情報漏えい防止システムの運用を開始した。

設問 1 本文中の［ a ］，［ b ］に入れる適切な字句を，表中の仕様内容の字句を用いて答えよ。

設問 2　本文中の下線②に該当する施策を，W 社のアルバイトの教育状況を踏まえ，35 字以内で具体的に述べよ。

設問 3　本文中の下線③について，(1)，(2) に答えよ。

(1) 導入が困難な課名を挙げ，該当する業務内容について，20 字以内で述べよ。

(2) 特例的な運用について，その内容を 40 字以内で述べよ。

設問 4　図 2 中の下線①の事態を抑止したい。そのための，C 社製情報漏えい防止システムの IC カードを活用した施策を，60 字以内で述べよ。

問 2　情報セキュリティ監査と改善に関する次の記述を読んで，設問 1～4 に答えよ。

L 社は，10 年前に設立された，社員数 200 名の書籍販売会社である。3 年ほど前からインターネットを利用した書籍販売を始めたところ，順調に売上げを伸ばし，現在では 10，000 人を超える顧客が会員登録をしており，1 日に平均して 500 件程度の注文がある。L 社の書籍販売システム（以下，E システムという）の構成は，図 1 のとおりである。

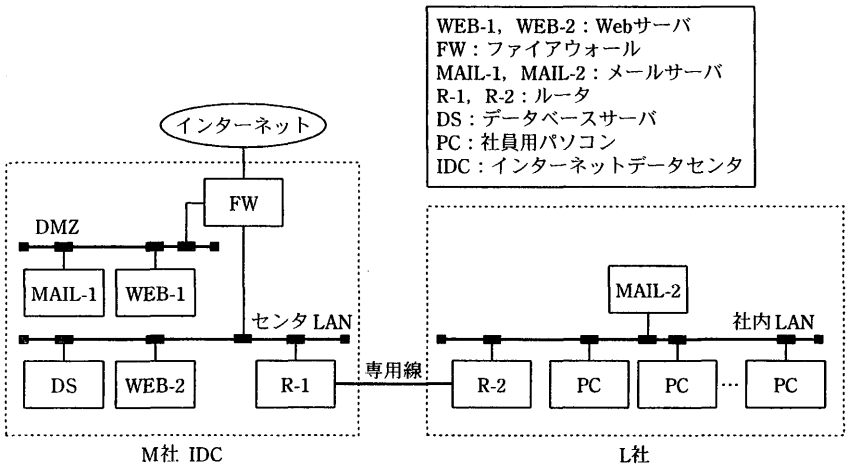


図 1　E システムの構成

〔E システムの概要〕

(1) E システムの MAIL-2 以外のサーバは，システム開発を委託した M 社 IDC のハウ

ジングサービスによって運用されており，FW 以外は L 社所有の機器である。

(2) 顧客は，インターネットを経由して WEB-1 にアクセスする。WEB-1 は，検索機能，書籍紹介情報の提示機能，発注機能及び決済機能を提供している。顧客データ，書籍紹介情報や在庫データは，すべて DS 上に蓄積されており，WEB-1 から随時，参照，更新される。

(3) WEB-2 は，営業部と仕入部の社員向けに販売管理機能を提供している。この販売管理機能は，受注管理機能，顧客管理機能及び在庫管理機能からなる。担当の社員は，社内 LAN から，R-1，R-2 で接続されている専用線を経由して WEB-2 にアクセスし，販売管理機能を用いて，DS 上に蓄積されたデータの取得や更新を 1 件ずつ行う。ただし，これらのデータの取得や更新が多い場合には，システム部にデータの一括取得や一括更新を依頼する。システム部の担当者は，FTP を使って DS にアクセスし，データの一括取得や一括更新を行う。

(4) 販売管理機能を利用する社員は，所属部長の承認を得た上で，販売管理機能の利用権限が設定された個別の ID（以下，SID という）をシステム部に申請し，取得する。また，取得した SID が不要となった場合には，同様にシステム部に削除を申請する。WEB-2 は，認証機能を備えており，SID とパスワードを用いてログインできる。営業部の社員は受注管理機能と顧客管理機能を，仕入部の社員は在庫管理機能をそれぞれ利用できる。

なお，ログイン時に使用するパスワードは，SID を取得した社員が管理する。

(5) 社内 LAN には，社員用の全 PC が接続されており，社内のメールは MAIL-2 を経由してやり取りされる。

〔情報セキュリティ監査の実施と対応策の検討〕

昨今の個人情報保護に対する社会的要請の高まりを受けて，L 社では E システムの情報セキュリティ対策について，外部監査を実施することにした。次は，システム部の担当者である V 主任と L 司の F 課長が外部監査について検討した際の会話である。

F 課長：今回の監査だが，どのようにすればよいか。

V 主任：個人情報の保護対策の確認が主眼になりますが，それ以外にも，当社の実情に見合った，情報セキュリティに必要な対策を明らかにしてほしいと考えています。そのために，今回は，情報セキュリティ監査制度に即した外部監査が望ましいと思います。

F 課長：その制度はどういうものか。

V 主任：情報セキュリティ監査制度は，情報セキュリティのマネジメント状況を監査するもので，監査の目的によって，［ a ］と［ b ］の監査を定めています。［ b ］は，主として改善を目的とした監査で，情報セキュリティマネジメント上の問題点を検出し，改善提言を行う監査です。

F 課長：その場合の監査項目はどのように決定されるのか。

V 主任：情報セキュリティ監査制度には，JIS X [c] の管理策から導出された約 [d] 項目のサブコントロールからなる情報セキュリティ [e] 基準があります。この [e] 基準の抜粋，変更，又は E システムのセキュリティ運用に関する規程類からの必要な項目の追加によって，E システムの管理項目を定め，それらを基に監査項目を決めることになります。

F 課長：分かった。これから検討を進めよう。

その後，V 主任と F 課長で検討を重ね，社外の監査サービス提供会社に監査を委託することにした。M 社でも監査サービスを提供しているが，E システムは，M 社が開発し，運用していることを考えると，[f] の観点から，M 社に監査を依頼することは問題があると判断し，実績も豊富な N 社に依頼することにした。

V 主任は，N 社の監査人と協議して監査項目を定め，ヒアリング対象として，L 社のシステム部，営業部と M 社のハウジングサービス担当部署を選定した。監査を効率良く実施するために，営業部と M 社に対して，①監査依頼書に依頼事項をまとめて通知した。

1 か月後，この依板の効果もあって，M 社 IDC 内での運用状況などをスムーズに監査できた。図 2 は，N 社による情報セキュリティ監査報告書である。

情報セキュリティ監査報告書

1. 検出事項

(1) 既に別の部署に異動して担当をはずれた元営業部所属の社員の SID が，利用可能な状態で残っており，その社員が顧客情報も閲覧可能な状態になっている。

(2) システム部，営業部，仕入部を含め，社員の異動が頻繁であるが，異動の情報は，人事部と該当部門だけがもっており，SID を管理するシステム部と情報が共有されていない。

(3) 社内 LAN からの E システム上の各サーバへのアクセスログは，OS レベルでのログインログ，メールサーバでのメール転送ログ，Web サーバへの HTTP アクセスログ，販売管理機能のログインログの取得にとどまっている。また，保管期間は 1 週間だけなので，情報漏えいなどの事故発生時に事実関係を十分に把握できない。

（省略）

2. 改善提言

(1) 現時点で不要な SID を，早急に削除すべきである。

(2) SID が不要になった際に，当該 SID の削除をより確実にするための施策を導入すべきである。

（省略）

(以下，省略)

図 2　N 社による情報セキュリティ監査報告書

図 2 の情報セキュリティ監査報告書を基に，V 主任と F 課長は対応策を検討し，システム部の H 部長に説明した。次は，その際の会話である。

V 主任：監査での検出事項に対応するための方針をまとめてみました。まず，不要な SID を洗い出し，その SID の削除をシステム部へ依頼するよう，営業部に指示します。また，アクセスログの保管期間については，今後は半年間にした

いと思います。

F 課長：もっと長期の保管についても考える必要があると思いますが，それは E システムの次の更新時に考えたいと思います。また，②少なくとも，大量の個人情報の流出事故に備えて，事実関係を把握するために，取得するログの種類も増やす必要があります。

H 部長：そうだな。情報セキュリティ監査報告書の改善提言（1）への対応としては，営業部へ不要な SID を削除するよう指示することでよいだろう。ただし，改善提言（2）への対応を考える必要があるな。③具体的な管理策を考えてくれ。

F 課長：はい，分かりました。

設問 1 本文中の [a] ～ [f] に入れる適切な字句を答えよ。

（1） [a] , [b] については，それぞれ 3 字で答えよ。

（2） [c] ～ [f] については，次の解答群の中から選び，記号で答えよ。

解答群

ア 130　イ 960　ウ 5070　エ 5080　オ 7799

カ ISMS　キ 安全性　ク 運用性　ケ 監査　コ 管理

サ 実施　シ 対策　ス 独立性

設問 2　下線①の監査依頼書では，M 社に対してどのような事項を依頼したと考えられるか。二つ挙げ，それぞれ 15 字以内で述べよ。

設問 3　下線②にあるように，現状の取得ログだけでは，情報セキュリティ対策としては不十分である。IDC に設置されている L 社所有の機器の範囲内では，どの機器でどのようなログを追加取得すべきか，25 字以内で述べよ。

設問 4　下線③に関して，SID の取得と削除の申請を行う営業部などのユーザ部門が実施すべき対策と，さらにその対策を補完するためにシステム部が実施すべき対策を，それぞれ 40 字以内で述べよ。

問 3　Web の私的利用に関する次の記述を読んで，設問 1～3 に答えよ。

Q 社は，従業員数 500 名の部品メーカである。早くからインターネットを利用して，業務に必要な情報の交換，収集を行っている。従業員が利用できるインターネットサービスは，電子メールと Web に制限している。本社では，従業員 1 人に 1 台ずつパソコンを配付しているが，工場では，複数人に 1 台配付し，共用させている。アカウントは，本社，工場とも 1 人一つずつ割り当てている。パソコンを利用する際には，ID とパスワードを入力し，ログインする。ログインのログは採取していない。Web を利

用する際には，必ずプロキシサーバを経由する。プロキシサーバでは，通信のログは採取していない。

なお，パソコンには固定の IP アドレスが割り当てられている。

Q 社のネットワーク構成を，図 1 に示す。

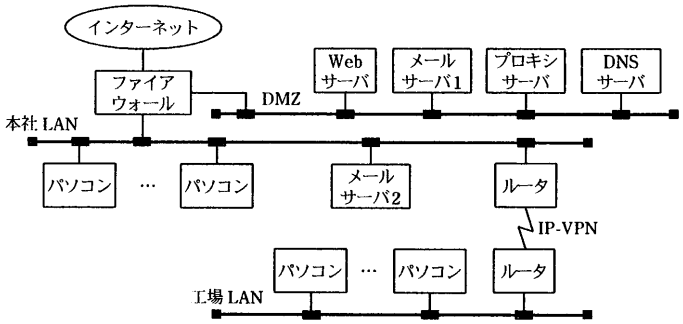


図 1　Q 社のネットワーク構成

〔私的利用の制限〕

Q 社は，2 年前に，情報システム部を中心とした情報セキュリティ委員会を設立し，情報セキュリティポリシ（以下，ポリシという）の策定を行った。情報セキュリティ委員会では，ポリシの制定や改正，情報セキュリティに関する施策実施の審議などを行う。ポリシに基づいた施策と現場の業務上の要求が相いれない場合は，情報セキュリティ委員会で，調整のための最終判断を行うこととなっている。

Q 社のポリシでは，業務目的以外のパソコンの利用を禁止しているが，Web に関しては，インターネットオークションや株取引など，一部で私的に利用されている。情報システム部の S 部長は，このような私的利用は就業規則に抵触すると判断し，早急に対処することにした。その対策として，Web について，フィルタリングソフトを導入してアクセス制限を行うこととし，情報セキュリティ委員会での審議を経て，経営陣の承認を得た。その際，S 部長は，必要ならば関連する社内規程も併せて修正するよう，情報セキュリティ委員会から指示され　情報システム部の T 君に検討を命じた。

T 君は，法律や公表されているガイドラインなどを点検し，既存のインターネット利用規程に，“利用の制限”と“管理者による利用状況の調査”の 2 項目を追加した（図 2)。これらの項目は，情報セキュリティ委員会での審議及び経営陣の承認を得た上で，従業員に周知された。

利用の制限
・フィルタリングソフトなどによるアクセス制限を行うことがある。
管理者による利用状況の調査
・管理者が，従業員のインターネット利用状況を調査する場合がある。
・管理者は，従業員のインターネット利用状況に関して，プライバシ保護の趣旨に反した調査を行ってはならない。

図 2　インターネット利用規程に追加した項目

〔フィルタリングソフトの導入〕

S 部長は，Q 社の業務にとって支障の少ないフィルタリングソフトを導入するよう，T 君に命じた。T 君による業務状況調査の結果，客先情報や業界の最新動向，技術情報など，不特定多数の Web サイトを通じて情報収集が行われているので，利用可能としておかなければならない Web サイトの特定は困難であることが分かった。このような状況を踏まえ，幾つかの製品を比較した上で，R 社フィルタリングソフトを導入し，稼働させた。R 社フィルタリングソフトの概要は，図 3 のとおりである。

なお，R 社フィルタリングソフト導入に際して，フィルタリング方式には，Q 社の業務状況から判断して，［ a ］方式を選択した。また，カテゴリの設定については，閲覧してよいかどうか判断しにくいものがあるので，各部署の意見を収集し，情報システム部で判断したカテゴリを設定することにした。その過程で，営業部から，“旅行”のカテゴリについては業務上必要であるとの要求があった。ポリシによれば，私的な旅行のための閲覧は制限すべきであり，情報システム部はこの要求を却下したが，営業部も譲らなかった。結局，情報システム部は，営業部の要求を認め，閲覧可能とした。

1. フィルタリング機能
次の(1)～(4)の項目の設定（フィルタリングルール）に基づいて，フィルタリングを行う。
(1) フィルタリング方式（必須）
次の二つの方式から選択する。
① ホワイトリスト方式：あらかじめ指定されたURL以外のアクセスを拒否する。
② ブラックリスト方式：あらかじめ指定されたURLだけアクセスを拒否する。
(2) フィルタリングを行うURLのカテゴリ指定（必須）
あらかじめ指定されたURLのリストをカテゴリ単位で指定する。(1)
(3) 送信元限定条件（任意）
特定の送信元からの通信をフィルタリングする。IP アドレス（群）又は利用者（群）を指定できる。指定しない場合，すべての送信元に適用される。(2)
(4) 時間帯限定条件（任意）
特定の時間帯の通信をフィルタリングする。指定しない場合，すべての時間帯で適用される。
2. ログ（任意）
ログを採取する場合，採取条件と採取項目を指定する。採取条件は，アクセス拒否された通信，アクセス許可された通信のいずれか，又は両方から指定できる。採取項目は，IP アドレス（送信元），あて先 URL，適用理由（適用したフィルタリングルール及びカテゴリ），時間，利用者 ID から任意に指定できる。ただし，利用者 ID は，送信元限定条件として，利用者（群）を指定された場合にだけ指定できる。
3. 管理方法
ブラウザによる設定の変更，稼働状況の確認などができる。
4. 運用形式
プロキシサーバ上で稼働する。

注 (1)
・URLのリストは，幾つかの分野（カテゴリ）ごとに分類されている。
・カテゴリとカテゴリ内の URL のリストは，ソフトウェア開発元の専門チームによって選定され，定期的に最新版に自動更新される。
・利用者は，独自にカテゴリの作成，URLのリストの追加ができる。

注 (2)
・利用者を指定した場合，フィルタリングソフトは，利用者を識別するために，ブラウザからのアクセスに認証済の利用者情報が含まれているかどうかを確認する。
・利用者情報が含まれていない（ブラウザ起動後の最初のアクセスなど）場合，利用者認証要求を返す。
・ブラウザから利用者 ID，パスワードを受け取り，利用者を認証し，フィルタリングルールに従ってフィルタリングを行う。
・利用者 ID，パスワードについては，本フィルタリングソフトで管理できる。

図3 R社フィルタリングソフトの概要

〔フィルタリングソフトの運用〕

S 部長は，業務目的以外のアクセス状況を把握するため，必要なログを採取するよう，T 君に指示した。T 君は，アクセス拒否された通信のログについて，IP アドレスと適用理由の項目を採取することにし，S 部長に相談した。S 部長は，その設定では，①利用者まで特定できない場合があるので，②設定変更するように指示した。

運用開始から数日後，営業部で業務目的以外に“旅行”のカテゴリに属する Web サイトを閲覧しているとの情報が寄せられた。情報システム部は営業部に対して調査を行い，寄せられた情報の事実確認を行った。この過程で，③閲覧の事実を確認するためのログが不十分であることと，“旅行”のカテゴリを閲覧可能とした④手続に問題があることを認識した。

これらの問題に対処するため，情報システム部が中心となって，運用を改善することになった。

設問 1 本文中の [a] に入れる適切な字句を，図 3 のフィルタリング方式から選び，10 字以内で答えよ。

設問 2　下線④の問題とは何か。Q 社の業務状況に基づいて，35 字以内で具体的に述べよ。

設問 3　フィルタリングソフトの設定について，(1) ～ (4) に答えよ。

(1) 営業部からの要求に応じて営業部だけ設定を緩和した。R 社フィルタリングソフトの機能を踏まえ，その設定方法を 35 字以内で述べよ。

(2) S 部長が下線①のように考えた理由は何か。Q 社の業務状況に基づいて，45 字以内で述べよ。

(3) 下線②の設定変更の内容を，30 字以内で具体的に述べよ。

(4) 下線③の問題に対し，どのように改善すべきか。R 社フィルタリングソフトの機能を踏まえ，30 字以内で述べよ。

問 4　SSL を利用した Web システムに関する次の記述を読んで，設問 1～4 に答えよ。

A 大学は，学生と教職員を合わせて，総数 4，000 人規模の理工系大学である。A 大学では，一昨年度，履修管理と成績管理を主な目的とした教務支援システム（図 1）を導入した。教務支援システムは，教職員の利用を前提として，操作の利便性に配慮し，標準的なブラウザでアクセスできるようにした。

(1)　履修者名簿の参照，変更
(2)　単位の取得状況と成績の参照，登録
(3)　オンラインシラバス (1) の作成，参照，変更

注 (1)　講義要領

図 1　教務支援システムの機能

〔教務支援システムの概要〕

教務支援システムは，基本的にオンラインですべての機能を利用できるように設計されている。ただし，教務支援システムが扱う対象には，プライバシに関するデータや機密データが含まれるので，技術面と運用面の両面からセキュリティを確保するための対策が施されている。例えば，学外からのアクセスも考慮し，SSL が導入された。特に，[a] 認証を行うクライアント認証モード（SSL の認証方式の一つ）を採用した。

ブラウザにインポートする必要がある“クライアント証明書”，“クライアント秘密

かぎ”と“A 大学の自己署名によるルート証明書”（以下，この三つを証明書セットという）は，教務支援システムを含めた学内のコンピュータネットワークを管理する情報センタが作成し，情報センタ職員が，ユーザである教職員の本人確認を行った後，フロッピーディスク又は USB メモリで手渡しすることになった。その際，情報センタ職員が利用方法を説明し，必要に応じて，ユーザに代わってパソコン上のブラウザなどに基本的な設定を行うことにした。さらに，教務支援システムサーバのアクセスログを長期間保存することなど，関連する事項を盛り込んだ運用手順書も定めた。導入後，順調に稼働し，教職員に好評であった。

〔ブラウザの設定〕

この 4 月に，X 教授が A 大学へ移籍してきた。そこで，情報センタ職員の Y 君が，X 教授が利用するノートパソコン（以下，ノート PC という）上の電子メールの設定と併せて，教務支援システムの説明と設定を行った。その際に交わした，ブラウザの設定に関するやり取りを，次に示す。

Y 君：証明書セットのインポートなどの基本設定は終わりました。これで，教務支援システムサーバに接続する際にパスワードを入力しなくても，すべての機能を利用できるようになります。また，証明書セットの入っているフロッピーディスクは必要ないので，情報センタに持ち帰ります。

X 教授：了解しました。今後は，URL を指定して接続するだけで，教務支援システムのメニュー画面が表示されるわけですね。

Y 君：はい。次に，セキュリティに関する設定について説明します。設定画面（図 2）を見てください。この設定画面で，SSL と TLS の有効／無効を選択します。

SSLv2	（有効・無効）
SSLv3	（有効・無効）
TLS	（有効・無効）

注　下線は選択されている状態を示す。

図 2　セキュリティに関する設定画面

X 教授：最近，SSL や TLS という言葉を耳にしますが，よく分からないので，教えてください。

Y 君：はい。SSL は，主に，Web サーバとブラウザ間の通信において，セキュリティを確保するための技術です。バージョン 2（SSLv2）とバージョン 3（SSLv3）がありますが，SSLv3 の方が多機能で安全とされています。教務支援システムでは，SSLv2 での接続の設定は，必ず“無効”を選択してください。

X 教授：分かりました。

Y 君：また，TLS は SSLv3 とほぼ同じものです。SSL や TLS によって，①真正性，

機密性，完全性を確保できます。別の言い方をしますと，教務支援システムサーバとの通信において，②“なりすまし”，“盗聴”，“改ざん”を防ぎます。

最後に，詳細設定は変更しなくてもよいのですが，せっかくですから，SSL の詳細項目に関する設定画面（図 3）を，簡単に確認してみましょう。

RSA 及び 128 ビットかぎと MD5 MAC による，RC4 暗号化	（有効・無効）
RSA 及び 168 ビットかぎと SHA-1 MAC による，3DES 暗号化	（有効・無効）
RSA 及び 56 ビットかぎと SHA-1 MAC による，DES 暗号化	（有効・無効）
RSA 及び 56 ビットかぎと SHA-1 MAC による，RC4 暗号化	（有効・無効）
RSA 及び 56 ビットかぎと SHA-1 MAC による，CBC モードの DES 暗号化	（有効・無効）

注　下線は選択されている状態を示す。

図 3　SSL の詳細項目に関する設定画面（抜粋）

Y 君‥RSA は，［ b ］かぎ暗号方式の一種です。暗号化や［ c ］を目的に使われています。さらに，これらのほかに，［ c ］のために DSA，かぎ共有のために DH という組合せも用意されています。それから，RC4，3DES，DES は，それぞれ，［ d ］かぎ暗号方式の一種です。

X 教授：SSL や TLS では，両方の暗号方式を用いるのですか。

Y 君：はい。認証には公開かぎ暗号方式を，通信データの暗号化には共通かぎ暗号方式を用いています。ただし，公開かぎを用いたシステムを利用する場合は，③“ユーザやサーバの識別情報”と“その公開かぎ’との対応を保証するルート証明書が信頼できるものでなければなりません。図 3 で，MD5 と SHA-1 はメッセージダイジェストのアルゴリズムです。これらは主に，④メッセージ認証コード（MAC）で利用されます。また，128，168，56　ビットは［ d ］かぎ暗号方式のかぎ長を示します。一般に，同じ方式であれば，かぎ長は長い方が安全とされています。CBC は，［ e ］暗号の利用モードの一つです。現時点で教務支援システムを使う場合，ブラウザの詳細設定はこのままで結構です。

X 教授：難しいですね。普通に使っている分には知らなくてもいいことですよね。

Y 君：ええ。でも，将来，設定変更をお願いするかもしれませんので，記憶の片隅にとどめておいてください。詳細については，先日，情報センタにお越しいただいた際に，私がお渡しした運用手順書にも記載されています。

X 教授：分かりました。では，ブラウザのブックマークに教務支援システムサーバの URL を登録しておきます。

〔X 教授のノート PC の利用状況〕

X 教授は，今回，Y 君が設定したノート PC を，教務支援システムサーバへの接続だけではなく，研究発表のプレゼンテーションや論文作成などにも活用していた。ところが，セキュリティ意識は低く，これまで，ノート PC 起動時のパスワード認証を

設定していなかった。その点に関して，ある学生から指摘されたことがあった。しかし，普段，かぎの掛かる自室で利用することが多く，ノート PC から目を離すこともほとんどないので，大丈夫だと安心していた。

〔インシデントの発生と再発防止策〕

X 教授はその年度末，地方への出張が続いた。そんなある日，出張先でノート PC を紛失してしまった。X 教授は出張から戻った翌日に，別のノート PC を用意し，電子メールなどの再設定をしてもらうため，Y 君に連絡し，古いノート PC の紛失の経緯も併せて伝えた。それを聞いた Y 君が，念のため，教務支援システムサーバのアクセスログを調べたところ，紛失した日からこれまでに，⑤X 教授のユーザ ID のアクセスが数件記録されていた。幸い，プライバシに関するデータや機密データは，事務処理のため，紛失前に別のサーバへ移動していたおかげで大事には至らなかったが，情報センタは X 教授のアカウントを即座に無効にした。さらに，情報センタでは，このほかにも報告されていない PC 紛失などがあるかもしれないことを懸念して，当面は学外からの教務支援システムサーバへの接続を全面的に停止することにした。

その後，情報センタは学外との接続を再開するに当たって，インシデントの再発防止のため，教務支援システムサーバのアクセス制御方法や，接続するクライアントの設定などについて検討した。その結果，“PC（ノート PC を含む）起動時のパスワード認証を有効にすること“といった，PC 利用に関する一般的な項目だけではなく，⑥教務支援システムのユーザが利用するブラウザを対象とした新たな項目を，運用手順書に加えることにした。また，すべてのユーザの“クライアント証明書”と“クライアント秘密かぎを更新し，再配付した。さらに，教務支援システムサーバに接続する PC（ノート PC を含む）が盗難に遭った場合や紛失した場合，速やかに情報センタに報告すべきことを運用手順書に加えた。

設問 1　本文中の [a] ～ [e] 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　暗号スイート	イ　共通	り　公開
エ　ストリーム	オ　相互	カ　ディジタル署名
キ　バイオメトリクス	ク　復号	ケ　ブロック

設問 2　本文中の下線③のように，ルート証明書を信頼できるものとするために，A 大学ではどのような運用をしているか。40 字以内で述べよ。

設問 3　本文中の下線④のメッセージ認証コード（MAC）を用いる目的は何か。達成するための手段を含めて，20 字以内で述べよ。ただし，下線①と下線②から，それぞれ用語を一つずつ選択して記述すること。

設問 4　本文中の下線⑤のなりすまし L が発生した理由を考慮して，新たに運用手順書に追加されることになった下線⑥の項目を，40 字以内で述べよ。