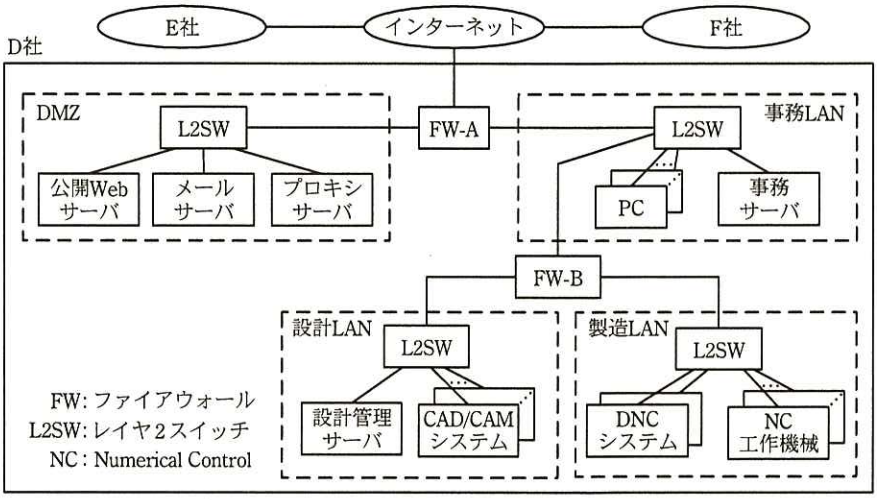
問2　金属加工業者におけるデータ管理に関する次の記述を読んで，設問1～5に答えよ。

D 社は，従業員数 200 名の金属加工業者である。CAD/CAM（Computer Aided Design/Computer Aided Manufacturing）システム及び DNC（Direct Numerical Control）システムを導入し，設計と製造に活用している。大型機械製造業や電気機器製造業の大手企業から委託を受けることも多い。特殊な加工が必要な場合は，専門の加工業者（以下，専門加工業者という）に再委託することもある。

〔D 社のネットワーク構成と機器〕

D 社のネットワーク構成を図1に示す。



注記　事務 LAN のデフォルトゲートウェイは FW-A である。

図1　D 社のネットワーク構成

D 社は，公開 Web サーバを運用し，そのコンテンツ作成を，コンテンツ作成業者の E 社に委託している。E 社の担当者は，E 社からインターネット経由で，FTP を使用してコンテンツを更新する。

また，D 社では，インターネットサービスプロバイダの F 社が提供するサービス（以下，F 社サービスという）のうち，次のものを使用している。

・DNS サービス

・インターネットと D 社との間の電子メール（以下，メールという）を中継するサ

ービス（以下，メール中継サービスという）

・メールのウイルス対策サービス及び迷惑メール対策サービス

D 社のネットワークに接続された機器には，固定 IP アドレスを割り当てている。

製造 LAN に接続された機器の運用は，製造課の担当者が行っている。それ以外の機器の運用は，情報システム課の J 課長の下，K さんが行っている。

〔取引時の情報管理〕

設計課の担当者は，委託元指定の安全性が確保された方法を用いて，設計図面を CAD データとして受け取る。その後，ウイルススキャンを行い，設計管理サーバに保存する。さらに，CAD/CAM システムを使用して，CAD データを NC 工作機械用の NC プログラムに変換し，設計管理サーバに保存する。製造課の担当者は，DNC システムを操作し，NC プログラムを設計管理サーバから NC 工作機械に取り込む。また，DNC システムを操作して，NC 工作機械の操作及び監視も行う。

CAD/CAM システムは，加工条件として工具の選択，加工順序などのデータベースを提供している。しかし，CAD/CAM システムが提供しているデータベースだけで全ての注文に対応できるわけではない。複雑な形状の加工の注文もあり，D 社が独自に作成した加工条件を使用することも多い。D 社独自の加工条件や NC プログラムは，D 社の重要情報であるので，情報漏えい対策に取り組んでいる。

専門加工業者に再委託する場合は，ウイルススキャンを行った後に暗号化した上で，次のいずれかの方法で CAD データを送付する。

・メールに添付して送付

・DVD-R などのメディアに記録して宅配便を利用して送付

復号用のパスワードは，CAD データとは別にメールで送付する。

経理課の担当者は，支払や入金の確認に U 銀行のインターネットバンキングサービスを利用している。U 銀行のインターネットバンキングサービスでは，EV SSL 証明書が使用されているので，担当者は，U 銀行のインターネットバンキングサービスにログインする前に，ブラウザのアドレスバーに表示される Web サイト運営者名が U 銀行であることを確認している。

〔情報システム課が運用している機器の概要〕

情報システム課が運用している主な機器の概要を表1に示す。

表1　主な機器の概要

機器名	OS	概要
FW-A，FW-B	専用 OS	ステートフルパケットフィルタリング機能並びに通信の許可及び拒否のログを取得する機能がある。
公開 Web サーバ	UNIX	コンテンツ公開機能及びコンテンツ全文検索機能を提供している。コンテンツ更新は，FTP を用いて行う。
メールサーバ	UNIX	F 社のメール中継サービスのサーバとの間のメール転送機能及び PC との間のメール送受信機能がある。リゾルバ機能及び DNS キャッシュ機能がある。NTP サーバ機能があり，インターネット上の NTP サーバとの間で時刻同期している。
プロキシサーバ	UNIX	P 社のプロキシソフトを使用している。PC からインターネットへの Web アクセス通信中継機能，Web アクセス通信ウイルススキャン機能，URL フィルタリング機能及び HTTP over TLS（以下，HTTPS という）通信対応機能がある。HTTPS 通信対応機能とは，HTTPS 通信を復号し，Web アクセス通信ウイルススキャン機能及び URL フィルタリング機能を使用した後，再暗号化する機能である。プロキシソフトのウイルス定義ファイル及び P 社が提供する URL ブラックリスト（以下，P 社提供リストという）は，P 社の Web サーバから 1 時間ごとに直接ダウンロードし，更新している。D 社では，HTTPS 通信対応機能を使用していない。
事務サーバ	Windows	人事情報，経理情報などを格納する。Q 社のウイルス対策ソフトを導入している。NTP サーバ機能があり，メールサーバとの間で時刻同期している。
設計管理サーバ	Windows	CAD データ及び NC プログラムを格納する。Q 社のウイルス対策ソフトを導入している。PC との間の CAD データの送受信及び DNC システムの NC プログラム取込みのために，FTP サーバ機能がある。
CAD/CAM システム	Windows	設計図面の確認及び修正，並びに CAD データから NC プログラムへの変換を行う。Q 社のウイルス対策ソフトを導入している。

D 社では，社内で利用可能なソフトウェアを定めている。OS が Windows の場合は，Q 社のウイルス対策ソフトと R 社の画像閲覧ソフトの導入を必須としている。

D 社では年 3 回，FW-A，FW-B 及び DMZ に設置されたサーバに対して脆弱性修正プログラムを適用している。

事務サーバ，設計管理サーバ及び CAD/CAM システムでは，OS の脆弱性修正プログラムがリリースされた場合，その週末に OS ベンダの Web サーバからプロキシサーバ経由で脆弱性修正プログラムをダウンロードして，適用している。

従業員が用いる PC は，会社が貸与している。PC の OS は，Windows である。OS

の脆弱性修正プログラムは，リリースされると自動的に適用される。

DMZ に設置されたサーバ，事務サーバ，設計管理サーバ及び CAD/CAM システムのデータは，日次でバックアップを行っている。また，OS 及びプログラムのバックアップは，脆弱性修正プログラム適用前及び適用後に行っている。

PC，事務サーバ，設計管理サーバ及び CAD/CAM システムでは，ウイルス対策ソフトのウイルス定義ファイルを，起動時及び起動後 2 時間ごとに Q 社の Web サーバからプロキシサーバ経由でダウンロードし，更新している。

各サーバでは，サーバへのアクセス及びプログラムの動作をログとして取得している。各サーバのログの保存期間は 4 週間である。

FW-A のフィルタリングルールを表 2 に，FW-B のフィルタリングルールを表 3 に示す。

表 2　FW-A のフィルタリングルール

項番	送信元	宛先	サービス	動作	ログ
1	メールサーバ	インターネット	DNS，NTP	許可	取得しない
2	F 社[1]	メールサーバ	SMTP	許可	取得する
3	メールサーバ	F 社[1]	SMTP	許可	取得する
4	全て	公開 Web サーバ	FTP	許可	取得する
5	全て	公開 Web サーバ	HTTP	許可	取得する
6	PC，事務サーバ，設計管理サーバ，CAD/CAM システム	プロキシサーバ	代替 HTTP[2]	許可	取得する
7	プロキシサーバ	インターネット	FTP，HTTP，HTTPS	許可	取得する
8	事務サーバ	メールサーバ	NTP	許可	取得する
9	PC	メールサーバ	POP3，SMTP	許可	取得する
10	全て	全て	全て	拒否	取得しない

注[1]　F 社とは，F 社のメール中継サービスのサーバである。
[2]　代替 HTTP のポート番号は，8080 である。
注記　項番が小さいルールから順に，最初に一致したルールが適用される。

表 3　FW-B のフィルタリングルール

項番	送信元	宛先	サービス	動作	ログ
1	PC，DNC システム	設計管理サーバ	FTP	許可	取得する
2	設計管理サーバ，CAD/CAM システム	事務サーバ	NTP	許可	取得する
3	設計管理サーバ，CAD/CAM システム	プロキシサーバ	代替 HTTP	許可	取得する
4	全て	全て	全て	拒否	取得しない

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

FW-A 及び FW-B のログの保存期間は 4 週間である。

FW-A 及び FW-B のフィルタリングルールのバックアップは，ルール変更後に行っている。

〔公開 Web サーバのコンテンツ改ざんと対処〕

ある日，E 社の担当者から，“公開 Web サーバのコンテンツを更新しようとしたところ，あるファイルの更新日時が，前回の更新日時と異なっていることに気付いた。D 社で更新したのか”と K さんに問合せがあった。K さんが確認したところ，D 社では誰もそのファイルを更新していなかったので，J 課長に公開 Web サーバのコンテンツが改ざんされた可能性があることを報告した。J 課長が，情報システム担当の M 役員に報告したところ，情報セキュリティ専門会社に調査を依頼するようにとの指示を受けた。J 課長は，情報セキュリティ専門会社の G 社に調査を依頼した。

その日のうちに，G 社の情報セキュリティスペシャリストである A 氏が，D 社を訪問した。A 氏は，公開 Web サーバを①シャットダウンすると調査が困難になるので，調査が完了するまでそのままにしておき，公開だけは直ちに停止するようにと助言し，J 課長と K さんはそれに従った。さらに，A 氏が，FW-A 及び DMZ に設置されたサーバに対して，いつ脆弱性修正プログラムを適用したかを尋ねたところ，K さんは 2 か月前に適用したと答えた。

A 氏は，FW-A 及び DMZ に設置されたサーバで，必要なファイルを採取し，調査を開始した。1 週間後，G 社から J 課長と K さんに調査結果の報告があった。調査結果の概要を図 2 に示す。

1. コンテンツ改ざんについて
  1.1 コンテンツファイル改ざんの内容
    ・コンテンツファイル中に，不正なスクリプトが埋め込まれていた。
    ・不正なスクリプトは，ブラウザ表示の見かけには影響しないものであった。
  1.2 コンテンツファイル改ざんの手法
    ・改ざんは，公開 Web サーバのコンテンツ全文検索機能の脆弱性を悪用した可能性が高い。脆弱性情報は，調査開始日の 4 週間前に公表された。脆弱性修正プログラムは，調査開始日の 3 週間前にリリースされた。
    ・調査したログには，不審なアクセスの記録はなかった。調査開始日の 4 週間以上前に改ざんが行われた可能性が高い。
2. 不正なスクリプトについて
  ・改ざんされたコンテンツにアクセスすると，多くの PC ベンダがプリインストールしている R 社の画像閲覧ソフトの脆弱性を悪用し，攻撃者が用意した Web サーバから，新たなウイルスをダウンロードさせる。画像閲覧ソフトの脆弱性修正プログラムは，調査開始日の 3 週間前に，R 社の Web サーバからダウンロードできるようになっていた。
  ・不正なスクリプトは既知のものである。不正なスクリプトに対応したウイルス対策ソフトの定義ファイルは，調査開始日の 2 週間前にリリースされた。
  ・攻撃者が用意した Web サーバは，既に閉鎖されている。
3. 復旧方法及び再発防止策について
  ・②D 社の運用状況を考慮するとバックアップメディアからの復元ではなく，OS，Web サーバプログラム及びコンテンツ全文検索機能のプログラムの最新版をインストールし，コンテンツは E 社が納入したものを用いて復元することを推奨する。
  ・公開 Web サーバの運用再開前に，脆弱性検査を実施することを推奨する。
  ・FW-A，FW-B 及び DMZ に設置されたサーバに関する脆弱性情報の収集を強化する。
4. そのほかの推奨事項について
  4.1 コンテンツ改ざん事実の公表について
    ・コンテンツ改ざんの事実を，復旧後の公開 Web サーバに掲載する。
  4.2 PC，事務サーバ，設計管理サーバ及び CAD/CAM システムへの脆弱性修正プログラムの適用について
    ・脆弱性修正プログラムの適用対象を見直して，実行する。
  4.3 公開 Web サーバのコンテンツ更新方法について
    ・コンテンツ更新方法を見直す。
  4.4 プロキシサーバの設定について
    ・Web アクセスによるウイルス感染を減らすために，プロキシサーバの設定を見直す。
  4.5 ログの取得及び管理方法について
    ・トラブル調査の迅速化を目的に，ログの取得及び管理方法を見直す。
  4.6 DMZ に設置されたサーバのウイルス対策について
    ・DMZ に設置されたサーバにも，ウイルス対策ソフトを導入する。

図 2　調査結果の概要

J 課長と K さんは，図 2 に示された推奨事項について対処することにした。

まず，J 課長は，公開 Web サーバの復旧を，図 2 の 3. の方法で行うことを K さんに指示した。K さんは，OS，Web サーバプログラム及びコンテンツ全文検索機能のプログラムの最新版をインストールし，動作確認を行った。J 課長は，脆弱性検査を G 社に依頼し，脆弱性は発見されなかったという報告を受けた。J 課長は，M 役員の了承

を得て，公開 Web サーバの運用を再開し，図 2 の 4.1 の対応を行った。

次に，J 課長と K さんは，図 2 の 4.2 に対応するために，③PC，事務サーバ，設計管理サーバ及び CAD/CAM システムについて脆弱性修正プログラムの適用対象を追加し，直ちに実行した。

J 課長と K さんは，A 氏の助言を受けながら，図 2 の 4.3～4.6 の推奨事項への対応を更に進めた。

〔公開 Web サーバのコンテンツ更新方法の見直し〕

J 課長と K さんは，公開 Web サーバのコンテンツ更新について，幾つかの方法を検討した。K さんが A 氏に相談したところ，A 氏は暗号や認証の技術を利用して，リモートコンピュータとの間でファイル転送や OS へのログインを安全に行うことができるプロトコルである [a] を用いたファイル転送ソフトの使用を推奨した。K さんは，E 社の担当者とも相談し，表 2 の項番 4 の項目のうち，サービスを FTP から [a] に変更することにした。加えて，④表 2 の項番 4 の項目をもう 1 か所見直した方がよいことに気付き，変更することにした。

K さんは，J 課長の承認を得て，これらの変更を直ちに実施した。実施後，E 社からコンテンツのアップロードができることを確認した。

〔プロキシサーバの設定の見直し〕

プロキシサーバの機能を表 4 に示す。

表4　プロキシサーバの機能

機能名	機能
Web アクセス通信中継機能	PC やサーバ（以下，PC とサーバを併せて接続元という）とインターネット上の Web サーバ（以下，接続先という）との間の Web アクセスの通信を中継する。
Web アクセス通信ウイルススキャン機能	接続元と接続先との間の通信内容に対してウイルススキャンを行う。HTTPS 通信のウイルススキャンを行うには，HTTPS 通信対応機能を有効にする。
URL フィルタリング機能	接続元，URL リスト及び動作を組み合わせた URL 制御ルールを用いて，URL フィルタリングを行う。URL 制御ルールの動作には許可又は拒否を指定する。接続元と URL リストの組合せのどれにも該当しない通信は，許可される。許可又は拒否にかかわらず，通信のログを取得する。URL リストには，P 社提供リスト及び利用者が定義するリスト（以下，ユーザ定義リストという）がある。サーバ管理者は，複数のユーザ定義リストを作成して URL を登録できる。P 社提供リストには，通信を拒否する URL が登録されているが，その URL の内容は開示されていない。HTTPS 通信の URL フィルタリングを行うためには，HTTPS 通信対応機能を有効にする。
HTTPS 通信対応機能	接続元とプロキシサーバとの間，及びプロキシサーバと接続先との間において，それぞれ独立の HTTPS 通信を確立する。HTTPS 通信確立前に接続先の証明書の検証を行い，検証が失敗した場合は，通信を拒否する。接続先のコモンネームを基に証明書を作成し，その証明書で接続元との間の HTTPS 通信を確立する。サーバ管理者は，HTTPS 通信対応機能を使用したくない URL を除外リストに登録できる。除外リストに登録された URL にアクセスした場合は，接続元と接続先との間で直接 HTTPS 通信が確立される。

J 課長と K さんは，URL 制御ルールの設定について検討した。現在の URL 制御ルールを表 5 に示す。

表5　URL 制御ルール

項番	接続元	URL リスト	動作
1	PC，事務サーバ，設計管理サーバ，CAD/CAM システム	P 社提供リスト	拒否

J 課長と K さんは，表 5 に対する修正案を作成した。その案を表 6 に示す。

表6　URL 制御ルールの修正案

項番	接続元	URL リスト	動作
1	事務サーバ，設計管理サーバ，CAD/CAM システム	ユーザ定義リスト 1	許可
2	事務サーバ，設計管理サーバ，CAD/CAM システム	ユーザ定義リスト 2	拒否
3	PC	P 社提供リスト	拒否

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

表 6 中のユーザ定義リスト 1 及びユーザ定義リスト 2 を表 7 に示す。

表7　ユーザ定義リスト1及びユーザ定義リスト2

URLリスト	URL
ユーザ定義リスト1	[b] のURL，[c] のURL，[d] のURL，…
ユーザ定義リスト2	全て

次に，J課長とKさんは，HTTPS通信対応機能の使用について検討した。A氏に相談したところ，次の助言を受けた。

・HTTPS 通信対応機能を使用すると，⑤インターネットを利用するD社の業務の一部に不都合が生じる。その不都合は，除外リストを使用すれば回避できる。

・HTTPS通信対応機能を使用するには，接続元にプロキシサーバのルート証明書をインストールしておく必要がある。

・HTTPS通信対応機能を使用すると，プロキシサーバの負荷が著しく上昇する。

J課長とKさんは，現在のプロキシサーバの性能では負荷の上昇に対応できないと判断し，HTTPS通信対応機能は，来年予定されているプロキシサーバの更新以降に使用することにした。

〔ログの取得及び管理方法の見直し〕

J課長とKさんは，公開Webサーバがウイルスに感染した場合に備えて，FW-Aでのログの取得方法を検討した。表2の項番10のログを“取得する”に変更すると，ログ取得数が増え，保存領域の不足が発生するので実現できない。しかし，表8に示すように項番5の後にルールを追加し，FW-Aのフィルタリングルールを修正すれば，攻撃者が用意したサーバへのウイルスからの通信を効率よく検出することができ，保存領域の不足が発生しにくくなることが分かった。

表8　FW-A のフィルタリングルールの修正案

項番	送信元	宛先	サービス	動作	ログ
⋮	⋮	⋮	⋮	⋮	⋮
5	全て	公開 Web サーバ	HTTP	許可	取得する
6	e	f	g	拒否	取得する
7	PC，事務サーバ，設計管理サーバ，CAD/CAM システム	プロキシサーバ	代替 HTTP	許可	取得する
⋮	⋮	⋮	⋮	⋮	⋮

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

同様に FW-B のフィルタリングルールの修正案も作成した。

続いて，各サーバのハードディスクの使用状況を調査した結果，ログの保存期間を1年にしても保存領域の容量不足は発生しないことが分かったので，これらのフィルタリングルールの修正案を適用することにした。

最後に，DMZ に設置されたサーバへのウイルス対策ソフトの導入について検討した。検討の結果，導入してもサーバの動作に悪影響がないことを確認できたので，導入することにした。

〔専門加工業者への CAD データの送信方法の検討〕

J 課長と K さんは，専門加工業者への CAD データ送信方法について，安全でかつ注文から納品までの時間を短縮できる電子的な方法を改めて検討することにした。現在使っているメールに添付して送信する方法では誤送信が問題になっていたが，誤送信を防止する確実な方法は見つけられなかった。そこで，他の方法を調査したところ，T 社が販売している，ファイル交換専用装置（以下，専用装置という）が見つかり，専用装置を DMZ に設置する前提で検討を進めた。

専用装置の仕様概要を図3に示す。

1. 利用者インタフェース及び認証方法について
   - 管理者並びに送信者及び受信者（以下，送信者と受信者を併せて利用者という）向けに Web インタフェースがあり，HTTP 及び HTTPS が使用できる。
   - 管理者は，利用者のメールアドレスを利用者 ID として登録する。
   - 管理者及び利用者の認証は，HTTP の場合はパスワード認証を，HTTPS の場合は，パスワード認証に加え，[h] 認証を使用することができる。
2. データ送信方式について
   利用者が使用するデータ送信方式として，URL 送信方式とデータ共有方式の 2 方式がある。
   - URL 送信方式
     送信者がファイルをアップロードすると，専用装置が，ダウンロード用のランダムな文字列を含む URL を受信者宛てにメールで送信する。ダウンロード後，ファイルは自動的に削除される。送信者は，ダウンロードの有効期間を指定できる。
   - データ共有方式
     管理者は，ファイル交換のためのフォルダを作成し，フォルダに対する利用者ごとの権限を設定する。
3. 他の機能
   管理者は，次の機能を設定できる。
   - 上長承認機能
     送信者の上長が承認した後に，ダウンロードが可能になる。管理者は，各利用者の上長及び上長代行者を登録する。
   - アクセス制御機能
     利用者ごとに IP アドレスを登録しておき，その IP アドレスからのアクセスだけを許可する。
   - ログ機能
     Web インタフェースへのアクセス，メールでの URL 送信，アップロード及びダウンロードのログを記録する。管理者は，Web インタフェースを使用して，ログをダウンロードする。
   - ウイルススキャン機能
     ウイルススキャン機能では，アップロード時及びダウンロード時にウイルススキャンを行う。

図 3　専用装置の仕様概要

J 課長と K さんは，図 3 の 1. については，通信の暗号化が必要であるので，HTTPS を使用することにした。また，[h] 認証を使用することにし，[h] 証明書の発行は，商用サービスを使用することにした。

次に，図 3 の 2. について検討した。専門加工業者から CAD データを受け取ることはないので，URL 送信方式がよいと K さんは説明した。J 課長は，K さんの説明に同意した。

さらに，図 3 の 3. については，各機能を使用することにした。

これらの検討の結果，⑥専用装置での CAD データの送信は，メールへの添付による送信と比べると，誤送信の防止や復号用パスワードの漏えい防止以外にも利点があることが分かった。

最後に，FW-A のフィルタリングルールに専用装置についてのルールを追加する案

を作成した。

J 課長は，検討した対策を M 役員に報告した。M 役員は，報告にある対策の他に，PC への対策を強化することを条件に承認した。

J 課長と K さんは，M 役員の指示について検討を行った。D 社のネットワーク構成を考慮して，⑦ウイルスの活動による PC からインターネットへの通信のうち，止めることはできないがログの分析によって検出できる通信と，⑧ウイルスの活動による PC からインターネットへの通信のうち，止めることはできるがログを分析しても検出できない通信に整理し，PC への対策の検討を開始した。3 か月後，PC への対策を完了した。

設問 1　〔公開 Web サーバのコンテンツ改ざんと対処〕について，(1)～(3)に答えよ。

(1)　本文中の下線①について，調査が困難になるのはなぜか。25 字以内で述べよ。

(2)　図 2 中の下線②について，バックアップメディアを用いてコンテンツの復元を行わない理由を 45 字以内で述べよ。

(3)　本文中の下線③について，追加した適用対象を 15 字以内で答えよ。

設問 2　〔公開 Web サーバのコンテンツ更新方法の見直し〕について，(1)，(2)に答えよ。

(1)　本文中の［　a　］に入れる適切なプロトコル名を，英字 6 字以内で答えよ。

(2)　本文中の下線④について，変更することにした項目の項目名を答えよ。また，変更後の内容を，図 1 中の字句を用いて答えよ。

設問 3　〔プロキシサーバの設定の見直し〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑤について，不都合が生じる業務を行う課を答えよ。また，不都合の内容を 45 字以内で具体的に述べよ。

(2)　表 7 中の［　b　］～［　d　］に入れる適切な接続先を答えよ。

設問 4　表 8 中の［　e　］～［　g　］に入れる適切な字句を答えよ。

設問 5　〔専門加工業者への CAD データの送信方法の検討〕について，(1)～(4)に答えよ。

(1)　図 3 中及び本文中の［　h　］に入れる適切な字句を 10 字以内で答えよ。

(2)　本文中の下線⑥について，利点とは何か。30 字以内で述べよ。

(3)　本文中の下線⑦の通信を二つ挙げ，それぞれ 50 字以内で述べよ。

(4)　本文中の下線⑧の通信を，35 字以内で述べよ。