問1　データ伝送のセキュリティ設計に関する次の記述を読んで，設問1～4に答えよ。

Z社は，従業員数10,000名の保険会社である。Z社は，100ある社内システムの構築をシステムごとにSIベンダのA社，B社，C社，D社のいずれかに発注している。各SIベンダは，ネットワーク機器，サーバ機器，OS及びミドルウェアを販売するとともに，業務アプリケーションの開発とシステムの構築を行い，運用をZ社情報システム部門に引き継いでいる。

Z社情報システム部門は，幾つかのシステムごとに1名の運用管理者と複数名の運用担当者からなる運用チームを編成して自社のデータセンタ（以下，DCという）内で社内システムを運用している。また，Z社情報システム部門は，システムの運用において，各製品の保守サービスに加えて，各SIベンダの拡張保守サービスを利用している。拡張保守サービスとは，障害時に業務アプリケーション又は製品の不具合が疑われる場合，保守担当者が派遣され，障害対応の支援を行うサービスである。派遣された保守担当者は，障害箇所を調査し，原因を分析するのに必要なデータ（以下，資料データという）を取得して可搬記憶媒体に保管し，社外への持出し手続をした上で自社に持ち帰る。保守担当者は，持ち帰った資料データを自社の業務アプリケーション開発部門又は製品開発部門にイントラネット経由で送付し，原因分析と対処方法の検討を依頼する。

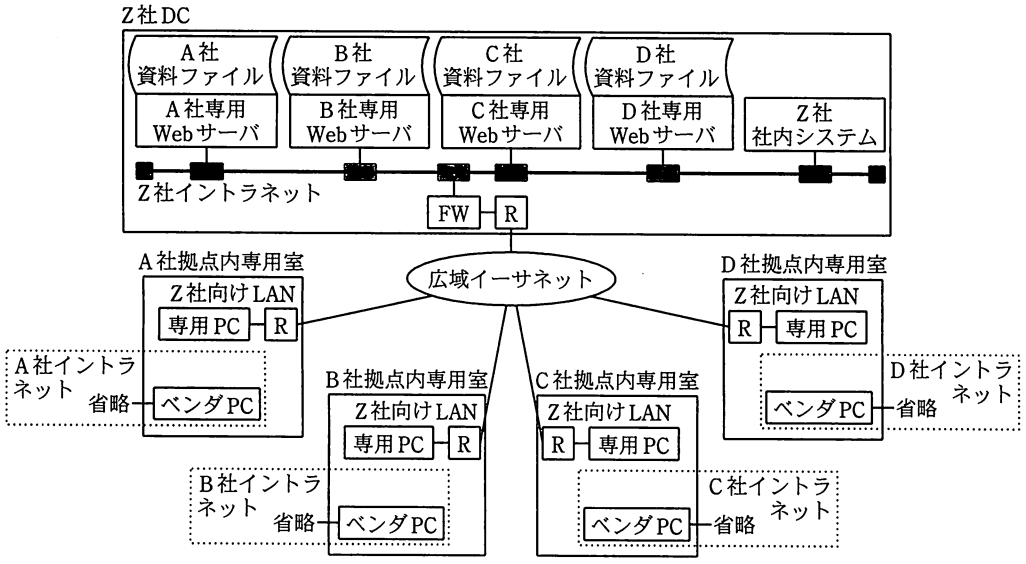
資料データは，業務アプリケーション，ネットワーク機器，サーバ機器，OS及びミドルウェアが出力する，ログ，内部トレースデータ，メモリダンプ及びネットワークトレースデータである。資料データは，Z社の秘密情報を含むことがあるので，Z社と各SIベンダとの秘密保持契約によって，他社への開示が禁止されている。例えば，A社の保守担当者は，取得した資料データを，B社，C社，D社及びその他の企業に開示することが禁止されている。

Z社では，運用管理者による事前承認を前提に，可搬記憶媒体を用いた社外への資料データ持出しを認めていたが，ある日，SIベンダの保守担当者が資料データの入った可搬記憶媒体を紛失する事故が発生した。Z社情報システム部門は，この事故の対応策として，Z社DCと各SIベンダ拠点との間で可搬記憶媒体を使わずにネットワーク経由で安全に資料データを伝送するシステムの検討を始めた。

〔資料データの伝送方式案〕

Z 社情報システム部門の H 部長は，部下の I 君と J 君に，資料データの伝送方式を検討し，伝送方式のセキュリティ設計についてセキュリティエンジニアの K 主任のレビューを受けるよう指示した。

I 君は，セキュリティを重視した資料データの伝送方式案（以下，案 1 という）を作成した。案 1 におけるネットワーク構成を図 1 に示す。



資料ファイル：資料データを圧縮して一つのファイルにしたもの
R：ルータ
FW：ファイアウォール
専用室：Z 社向け拡張保守サービス専用室
専用 PC：Z 社が貸与する拡張保守サービス専用 PC
ベンダ PC：各 SI ベンダが所有及び管理する PC

図 1　案 1 におけるネットワーク構成

案 1 では，資料ファイルを各 SI ベンダ専用の Web サーバ上にアップロードしておき，各 SI ベンダの複数の保守担当者が，自社の拠点に設けた専用室内の専用 PC から，広域イーサネット経由で Web サーバにアクセスし，資料ファイルをダウンロードする。専用 PC とベンダ PC はネットワークで接続されておらず，保守担当者は，資料ファイルをダウンロードした後，専用室内で可搬記憶媒体を介してベンダ PC に資料ファイルを移し，自社のイントラネット経由で開発部門に送る。必要となる機器のうち，ベンダ PC 以外の機器（Web サーバ，専用 PC，R，FW など）は，Z 社の遊休資産を使うことで購入不要であるが，広域イーサネットの敷設と専用室の設置に関しては，

Z 社が費用を負担する必要がある。また，広域イーサネットの敷設には申請から回線開通まで1～2か月の期間を要する。

一方，J君は，セキュリティを考慮しつつ，費用が安い伝送方式案（以下，案2という）を作成した。案2におけるネットワーク構成を図2に示す。

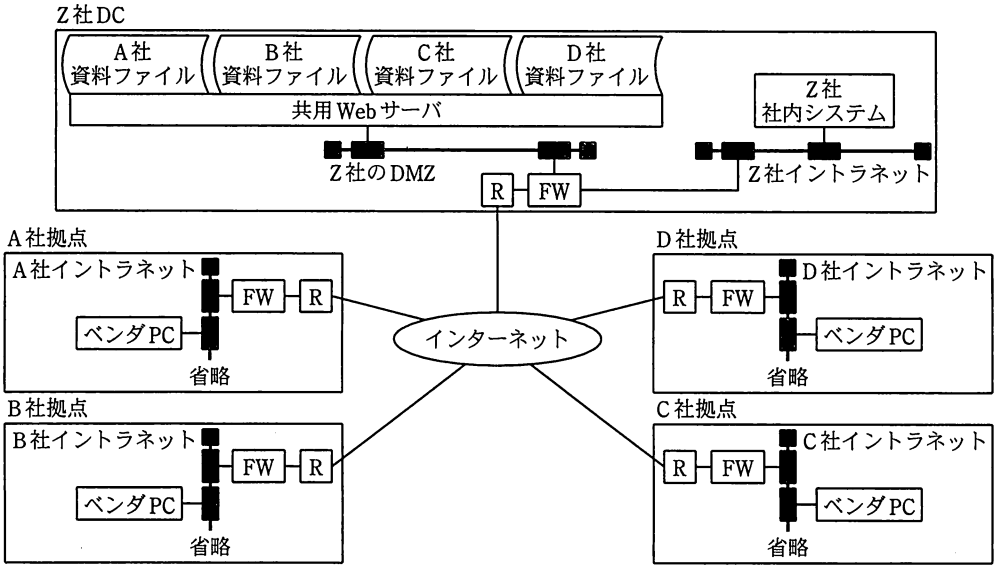


図2　案2におけるネットワーク構成

案2では，各SIベンダが既に所有している，イントラネット及びインターネット接続環境を利用する。各SIベンダの複数の保守担当者は，ベンダPCからインターネット経由で共用Webサーバにアクセスし，各SIベンダ専用のディレクトリ上にある資料ファイルをダウンロードする。Z社DC内で必要となる機器は，Z社の遊休資産を使うことで購入不要である。

〔資料データの伝送方式案におけるセキュリティ設計〕

I君とJ君は，伝送方式におけるセキュリティ設計のレビューと併せてどちらの案を選択すべきかをK主任に相談した。K主任は，資料データの伝送方式の運用手順を具体化した上で，データ保護と不正使用防止に必要なセキュリティ要件を業界ガイドラインから洗い出し，そのセキュリティ要件の各項目に対する実装方法をまとめるよう，I君とJ君に指示した。I君とJ君がまとめた，両案における資料データの伝送方式の運用手順を図3に，セキュリティ要件と実装方法を表に，それぞれ示す。

(1) 保守担当者が，Z 社社内システム上で資料ファイルを作成する。資料ファイルには，作成のたびに異なる一意なファイル名を割り当てる。
(2) 運用担当者が，Web サーバにログインし，資料ファイルを Web サーバにアップロードし，保守担当者に連絡する。複数の運用担当者が利用者 ID を共用する。
(3) 保守担当者が，自社の拠点から Web サーバにログインし，Web サーバ上の資料ファイルをダウンロードする。SI ベンダごとに，一つの利用者 ID を割り当てておく。
(4) 保守担当者が，運用担当者に資料ファイルのダウンロードが完了したことを連絡する。
(5) 運用担当者が，Web サーバ上の資料ファイルを削除する。
(6) 運用担当者が，作業報告書に，作業日時，運用担当者の氏名，保守担当者の所属と氏名，資料データの内容，資料ファイルのファイル名を記録する。
(7) 運用管理者が，作業報告書の内容を確認した後，確認印を押す。

図 3　資料データの伝送方式の運用手順

表　セキュリティ要件と実装方法

<table>
<tr><td colspan="2">業界ガイドラインにおける要件</td><td colspan="2">要件の対象</td><td colspan="2">実装方法</td></tr>
<tr><td>大項目</td><td>小項目</td><td>案 1</td><td>案 2</td><td>案 1</td><td>案 2</td></tr>
<tr><td rowspan="6">データ保護（漏えい防止）</td><td rowspan="2">相手端末確認（正規利用者への［a］の防止，及び誤接続の防止）</td><td>専用 PC（専用 Web サーバの相手端末）</td><td>ベンダ PC（共用 Web サーバの相手端末）</td><td colspan="2">(ア) SSL 通信によるクライアント認証（専用 PC 又はベンダ PC に［b］を設定する。）</td></tr>
<tr><td>専用 Web サーバ（専用 PC の相手端末）</td><td>共用 Web サーバ（ベンダ PC の相手端末）</td><td colspan="2">(イ) SSL 通信によるサーバ認証，並びにブラウザにおける Web サーバのブックマークへの登録及びブックマークからの Web サーバへのアクセス</td></tr>
<tr><td>蓄積データの漏えい（ファイルのコピーや盗難による漏えい）の防止</td><td>（省略）</td><td>（省略）</td><td>（省略）</td><td>（省略）</td></tr>
<tr><td rowspan="3">伝送データの漏えい（［c］による漏えい）の防止</td><td colspan="2">DC 内ネットワーク上の資料ファイル</td><td colspan="2" rowspan="3">SSL 通信による通信の暗号化</td></tr>
<tr><td colspan="2">DC から各 SI ベンダ拠点までのネットワーク上の資料ファイル</td></tr>
<tr><td>各 SI ベンダ拠点内 Z 社向け LAN 上の資料ファイル</td><td>－</td></tr>
<tr><td colspan="2">各 SI ベンダのイントラネット上の資料ファイル</td><td>（省略）</td><td>（省略）</td></tr>
<tr><td rowspan="5">不正使用防止</td><td rowspan="2">利用者認証</td><td colspan="2">運用担当者</td><td colspan="2" rowspan="2">Web サーバにおける，利用者 ID 及びパスワードによる利用者認証</td></tr>
<tr><td colspan="2">保守担当者</td></tr>
<tr><td>アクセス権限確認</td><td colspan="2">運用担当者の資料ファイルのアップロード権限及び削除権限
保守担当者の資料ファイルのダウンロード権限</td><td colspan="2">(ウ) Web サーバにおける，ディレクトリに対するアクセス制御</td></tr>
<tr><td>アクセス履歴管理</td><td colspan="2">運用担当者の，Web サーバへの資料ファイルのアップロード履歴及び削除履歴
保守担当者の，Web サーバ上の資料ファイルのダウンロード履歴</td><td colspan="2">(エ) Web サーバにおける，通信ログの取得及び保存</td></tr>
<tr><td>外部ネットワークからのアクセス制限</td><td>－</td><td>資料データの伝送以外のアクセス</td><td>－</td><td>FW による不要な通信の遮断</td></tr>
</table>

K主任は，表に対して次の4点を指摘した。

指摘1　(ウ)に関して，特に案2においてはアクセス制御ルールの設計が必要である。

指摘2　(エ)に関して，通信ログの取得と保存だけでなく，運用担当者と保守担当者が行った作業の内容を事後確認する必要がある。また，事後確認を確実に行うために，図3の運用手順の修正と，通信ログとして取得するデータ項目の明確化が必要である。

指摘3　案2の場合，(ア)及び(イ)に関して，各SIベンダの情報セキュリティポリシと矛盾していないことを確認する必要がある。

指摘4　案2の場合，インターネットを利用することによってWebサーバの脆弱性をねらった攻撃を受けるリスクが大きくなるので，システム運用においてセキュリティパッチを遅滞なく適用する必要がある。

I君とJ君は，図3及び表の修正を行った。K主任は，修正後の案1と案2はどちらもセキュリティ要件を満たしていると判断し，両案におけるセキュリティ設計を承認した。また，K主任は，二つの案の選択に関してH部長の判断を仰ぐよう，I君とJ君に助言した。H部長は，資料データの伝送方式をSIベンダ以外の協業相手とのデータの受渡しにも適用することを考え，データの受渡し相手が増えた場合にも少ない費用と短い期間で対応可能な案2を選択することを決定した。Z社情報システム部門は，案2に基づいて資料データを安全に伝送するシステムの構築に着手した。

設問1　表中の［　a　］～［　c　］に入れる適切な字句を，それぞれ10字以内で答えよ。

設問2　指摘1について，(1)，(2)に答えよ。

(1)　アクセス制御ルールの設計が特に案2において必要な理由を，案1との違いを踏まえて，25字以内で述べよ。

(2)　案2において禁止すべきアクセスはどのようなアクセスか。アクセス対象とアクセス元の利用者を，それぞれ20字以内で述べよ。

設問3　指摘2について，(1)～(3)に答えよ。

(1) 事後確認の具体的内容として，何と何を突き合わせるべきか。突き合わせるべきものを二つ挙げ，それぞれ7字以内で答えよ。

(2) 図3の運用手順に対して行った修正内容を，40字以内で述べよ。

(3) Web サーバにおける通信ログとして取得しなければならないデータ項目を三つ挙げ，それぞれ7字以内で答えよ。

設問4　K主任が指摘3の内容を指摘した理由を，30字以内で述べよ。