SC

平成22年度　秋期
情報セキュリティスペシャリスト試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. この注意事項は，問題冊子の**裏表紙**に続きます。必ず読んでください。
4. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
5. 問題は，次の表に従って解答してください。

問題番号	問1 ～ 問4
選択方法	2問選択

6. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に，**受験番号**を記入してください。正しく記入されていない場合は，採点されません。
   (3) **生年月日欄**に，受験票に印字されているとおりの**生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。
   (4) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。
   なお，○印がない場合は，採点の対象になりません。3問以上○印で囲んだ場合は，はじめの2問について採点します。
   (5) 解答は，問題番号ごとに指定された枠内に記入してください。
   (6) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問1，問3を選択した場合の例〕

選択欄	
2問選択	○問1
	問2
	○問3
	問4

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

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。

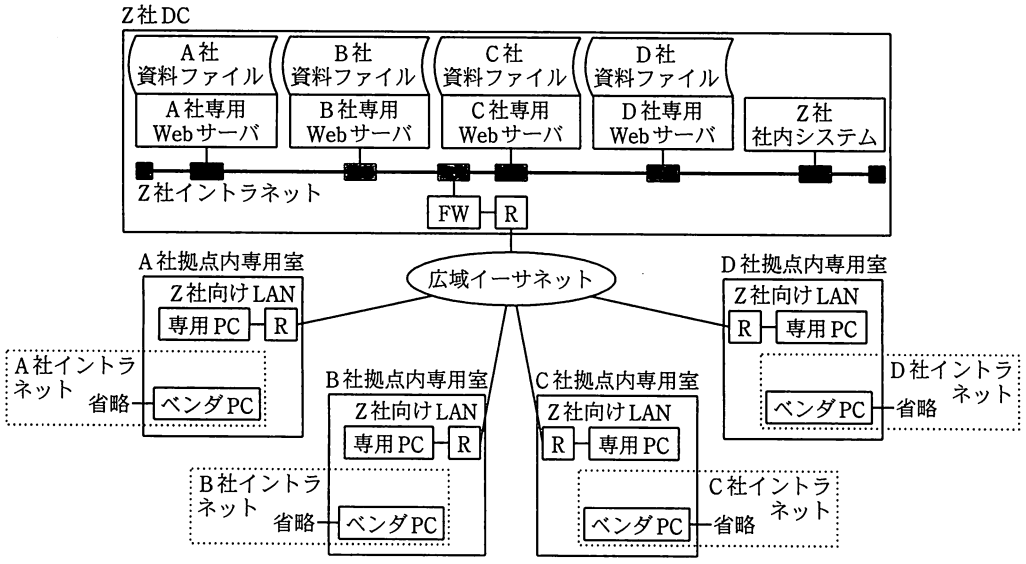
資料データは，業務アプリケーション，ネットワーク機器，サーバ機器，OS及びミドルウェアが出力する，ログ，内部トレースデータ，メモリダンプ及びネットワークトレースデータである。資料データは，Z社の秘密情報を含むことがあるので，Z社と各SIベンダとの秘密保持契約によって，他社への開示が禁止されている。例えば，A社の保守担当者は，取得した資料データを，B社，C社，D社及びその他の企業に開示することが禁止されている。

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。

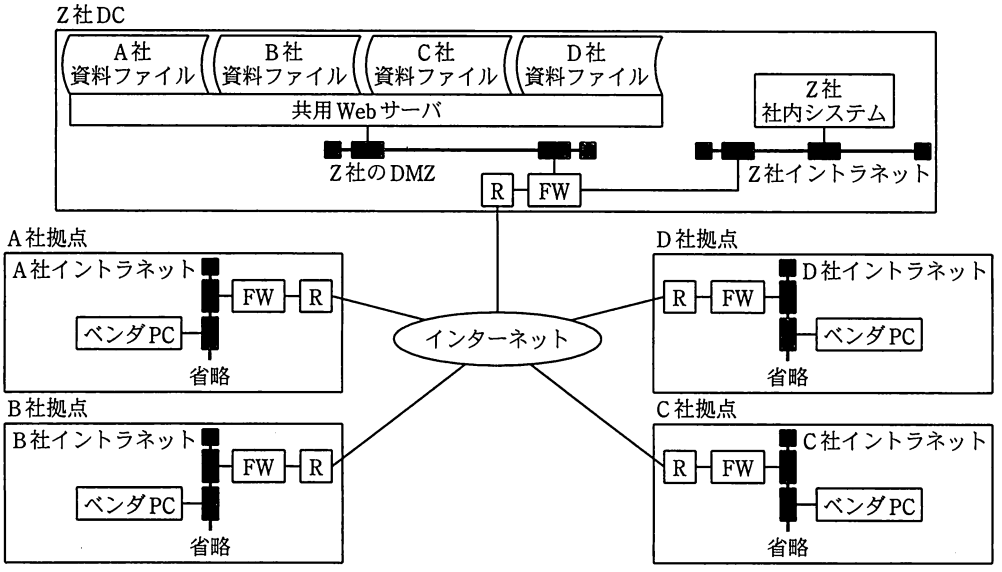


図2　案2におけるネットワーク構成

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。

問2　利用者IDのライフサイクル管理に関する次の記述を読んで，設問1～4に答えよ。

E社は，従業員数が500名，派遣社員数が常時200名程度の商社である。取扱商品分野ごとに事業部があり，メーカから商品を仕入れて販売店に卸している。E社には，販売管理，営業管理，会計，人事管理などの業務をそれぞれ支援する各サブシステムからなるシステム（以下，Eシステムという）がある。主要な業務は，Eシステムを使用しながら遂行されており，すべての従業員は，日常的にEシステムを使用している。他社に出向している従業員も，様々な手続のために頻繁にE社に出社してEシステムを使用する。休職者については，セキュリティの観点からすべてのサブシステムについて，アカウント管理者が利用者ID（以下，UIDという）を利用停止に変更することになっている。

UID管理は，サブシステムごとに独自に行っているが，従業員と対応しないUIDがあったり，UIDの管理内容に全社的な統一性がなかったりするなどの問題があった。これらを抜本的に改善するために，E社では，新しくUID管理システムを構築することにした。UID管理システムでは，UIDの管理を徹底するためにUID管理を一元化するとともに，退職時にUIDを確実に削除できるように人事管理システムと連携させることにした。UID管理システムの構築のために，情報システム部が中心となってプロジェクトチームを立ち上げた。

はじめに，人事管理システムと連携させるために，入社や異動，退職といった人事上のイベント発生時（以下，人事イベント発生時という）の利用者情報に対する処理を表のとおり整理した。ここで，利用者情報の属性として“UID名”，“パスワード”，“UIDの状態”，“従業員名”，“従業員番号”，“UID発行年月日”，“所属部門名”，“出向フラグ”，“出向先名”，“休職フラグ”，“UID最終利用年月日”を定義し，“UIDの状態”の値（以下，状態値という）としては，“仮パスワード”，“有効”，“無効”，“一時利用停止”を定義した。一方，各サブシステムの利用権限については，引き続き各サブシステム側で管理することにした。

表　人事イベント発生時の利用者情報に対する処理内容

人事イベント	UID の発行と削除	状態値の設定，変更など	利用者情報の属性値の設定，変更など
入社，他社からの出向者受入れ	発行	“仮パスワード”に設定	必要な属性値の設定
異動	－	変更しない	属性値（所属部門名）の変更
他社への出向	－	変更しない	属性値（出向フラグ，出向先名）の設定
出向帰任	－	変更しない	属性値（出向フラグ，出向先名）の解除
休職	－	“ a ”に変更	属性値（休職フラグ）の設定
復職	－	“ b ”に変更	属性値（休職フラグ）の解除
退職，他社からの出向終了	削除	－	－

〔人事管理システム及び各サブシステムとの連携〕

プロジェクトチームでは，UID 管理システムと，人事管理システム及び各サブシステムとの連携を検討し，次のように決定した。

人事管理システムとの連携では，毎日，人事管理システムから従業員情報を取得し，UID 管理データベースに格納する。各サブシステムとの連携では，UID 管理データベースの変更のたびに各サブシステムに対して利用者情報を配布する。

これによって，利用者情報を一元的に管理する。パスワードの初期化及び変更は，各サブシステムではなく，UID 管理システムで行い，変更後のパスワードは各サブシステムに反映され，各サブシステム間のパスワードの同期がとられる。

〔従業員の UID 管理〕

プロジェクトチームでは，従業員の UID 管理を検討するために，E 社の情報セキュリティ規程から，UID に関する項目を抽出し，次のとおりにまとめた。

(1) システム管理者が利用する OS の特権 ID を除き，UID は利用者ごとに発行され，複数の利用者が共用することを禁止する。

(2) 情報システム部にアカウント管理者を置く。

(3) UID は，利用されない期間が，ある日数（以下，許容無使用期間という）を超えた場合に状態値を“無効”にする。許容無使用期間は 100 日とする。

(4) UIDに対応したパスワードは，次のルールに従わなければならない。

(a) 10文字以上

(b) 数字，英文字，記号が，それぞれ1文字以上

(5) UIDのパスワードを連続して5回間違えた場合，状態値を“一時利用停止”にする。

プロジェクトチームでは，UIDの管理のうち規程に明文化されていない部分について，次のように案をまとめた。

(ア) 人事イベント発生時におけるUIDの発行，状態変更及び削除，並びに初期化依頼に対するパスワードの初期化は，アカウント管理者が行う。

(イ) UIDの発行時には仮パスワードを設定する。

(ウ) 仮パスワードの発行を受けた従業員は，72時間以内にパスワードを設定しなければならない。パスワードを設定するまでは，各サブシステムを利用することはできない。仮パスワードのまま72時間経過した場合は，UIDを削除する。

(エ) “一時利用停止”の状態は，24時間後に自動的に解除される。ただし，緊急に利用しなければならない場合は，アカウント管理者の通常勤務時間内であれば，アカウント管理者にファックス，電話などの何らかの方法でコンタクトし，初期化依頼する。依頼を受けたアカウント管理者は，直ちにパスワードを初期化し，依頼者が指定する方法で仮パスワードを連絡する。

(オ) 各サブシステムのログイン履歴は，UID管理システムに送られる。

プロジェクトチームでは，上記(1)～(5)及び(ア)～(オ)に基づく，UID管理システムにおける従業員のUIDの状態遷移を，図のようにまとめた。

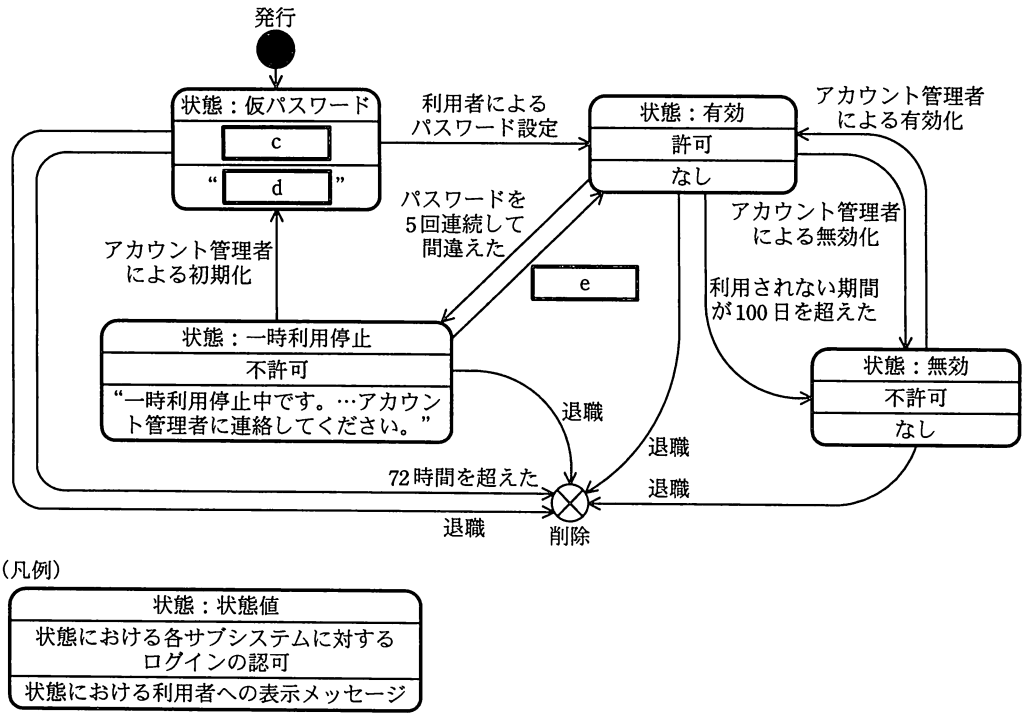


図　UID 管理システムにおける従業員の UID の状態遷移

〔派遣社員の UID 管理〕

プロジェクトチームでは，派遣社員の UID 管理を検討した。各サブシステムは，従業員のほか，派遣社員も利用する。派遣社員は，人事管理システムで管理されていない。そのため，派遣社員に関する契約期間に基づいて UID を管理することになる。

プロジェクトチームでは，派遣社員の UID 管理の内容を，従業員の UID 管理に準じて整理することにした。すなわち，情報セキュリティ規程や UID 管理システムの要件などにおいて，従業員の人事イベントを派遣社員に関する契約開始，契約終了（満了及び解除）に対応して読み替えることにした。例えば，表中の人事イベント“入社”を“契約開始”に，“退職”を“契約終了”に読み替えることにした。

派遣社員に関する契約は，各事業部が主体的に行っているが，契約開始時には，契約管理部の承認を得ている。E 社の契約内容に関する規程によって，契約開始日は月初日，満了日は月末日に限定すること，有期限の期間契約とすること，及び自動継続契約は行わないことが決められており，これらは，契約管理部によって厳格に確認されている。

どの事業部も，契約管理には，表計算ソフトや専用管理ソフトを利用しているが，それらのソフトウェアと UID 管理システムを連携させることは困難である。そこで，プロジェクトチームでは，UID 管理システムを利用して派遣社員の UID の発行及び削除を申請する仕組みを検討した。しかし，この仕組みは，各事業部が業務上の必要性に迫られる契約開始時における UID の新規発行申請には利用してもらえるとしても，契約満了時の削除申請には利用してもらえないだろうとの意見が出た。

このため，まず契約満了者の UID を確実に削除できる運用を検討した。第 1 案は，“無効”状態にある UID を，情報システム部が毎月初日に一括削除する運用である。第 2 案は，UID の発行申請時に設定する①属性を追加して，UID 管理システムが毎日その値を点検して自動的に UID を削除する運用である。第 1 案は，②UID の許容無使用期間と UID の一括削除の運用日程によって，契約満了後から削除されるまで一定の時間が掛かるという問題があった。また，契約満了後の UID が，削除されずに使い回されると，削除すべき UID が検出できない。そこで，第 2 案を採用することにした。

プロジェクトチームでは，これまでの UID 管理の検討結果をまとめ，情報システム部長に報告した。報告を受けた部長は，派遣社員の契約では契約満了前に契約解除となるケース（以下，満了前解除ケースという）がまれに発生することと，現状の従業員の UID 管理では，③何者かがなりすまして他者の UID のパスワードを不正取得できるリスク（以下，パスワード不正取得リスクという）があることを指摘した。

指摘を受けたプロジェクトチームは，④満了前解除ケースに対しても確実に UID が削除できるような運用を追加し，派遣社員の UID を確実に削除できるようにした。また，パスワード不正取得リスクに対しては，⑤具体的な手続を定めることで解決することにした。

以上の内容で情報システム部長の承認を得て，引き続いて UID 管理システムの構築に着手した。

設問 1　利用者情報に対する処理及び状態遷移について，(1)～(3)に答えよ。

(1) 表中の［ a ］，［ b ］に入れる適切な状態値は何か。図中の字句を用いて答えよ。

(2) 図中の［ c ］，［ d ］に入れる適切な字句を，［ c ］は 5 字以内で，［ d ］は 20 字以内で答えよ。

(3) 図中の［ e ］に入れる適切な字句を 15 字以内で答えよ。

設問 2　〔派遣社員の UID 管理〕について，(1)～(3)に答えよ。

(1) 本文中の下線①について，追加すべき属性を 15 字以内で答えよ。

(2) 本文中の下線②の一定の時間とは何か月か。整数で答えよ。

(3) 本文中の下線④の追加する運用とは何か。具体的な運用を 35 字以内で述べよ。

設問 3　本文中の下線③が起こるのはどのような場合か。65 字以内で述べよ。

設問 4　本文中の下線⑤で考えられる手続を 40 字以内で具体的に述べよ。

問3 Web アプリケーションファイアウォール（WAF）の導入に関する次の記述を読んで，設問1～4に答えよ。

R 社は従業員数 200 名の健康食品販売会社であり，消費者向けに電話受付による販売を行っており，5 年前からはインターネットを介した販売システムを利用した販売も行っている。

販売システムは，アウトソーシング事業者である Y 社のデータセンタに設置され，ルータ，ファイアウォール，負荷分散装置，Web サーバ，データベースサーバで構成されている。販売システムのネットワーク構成を図 1 に，販売システムの概略を図 2 に示す。

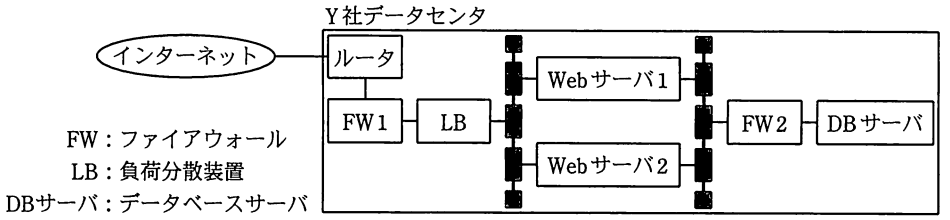


図1 R社の販売システムのネットワーク構成

(1) 利用者は，ブラウザでインターネットを介して Web サーバにアクセスし，販売システムを利用する。ブラウザからのアクセスは LB によって，Web サーバ 1 と Web サーバ 2 に負荷分散される。

(2) Web サーバ上では，HTTP による送受信を処理する Web サーバプログラム，ミドルウェア及びミドルウェア上で動作する Web アプリケーションが稼働している。Web アプリケーションは DB サーバと連携して動作する。

(3) Web アプリケーションの開発は，R 社のインターネット販売事業部で行っている。

(4) ルータ，FW 及び LB の管理，サーバのハードウェア保守，並びに OS のバージョン管理及び修正プログラム適用作業の運用は Y 社に業務委託している。

(5) FW は，パケットのヘッダ情報によってアクセスを制御するパケットフィルタリング型である。FW には，Web サーバへのアクセスを制御する FW1 と，DB サーバへのアクセスを制御する FW2 がある。

(6) 販売システムのログイン ID を保有している利用者は，Web アプリケーションのログイン画面で，ログイン ID とパスワードを入力することによってログインを行う。ログイン画面以降は，ブラウザと Web サーバ間で SSL 通信が行われる。また，ログイン時にミドルウェアがセッション ID を生成し，これをクッキーとして利用者のブラウザに格納することによってセッション管理を実現している。

(7) 販売システムのログイン ID を保有しない消費者向けに，R 社では電話による注文受付窓口を設置している。販売システムの商品紹介コンテンツは，ログイン ID を保有しない利用者でも閲覧できる。

図2 R社の販売システムの概略

〔脆弱性発見の情報〕

R 社は，情報セキュリティ専門会社からセキュリティ情報の提供を受けている。ある日，販売システムの Web サーバで稼働中のミドルウェアに脆弱性が発見されたとの情報が提供された。R 社インターネット販売事業部の S 主任がまとめた脆弱性の概要を図 3 に示す。

ミドルウェアによるセッション ID の生成に不備があり，利用者向けに発行されたセッション ID を第三者が推定できてしまう可能性がある。セッション ID は，利用者のログイン ID，ログインを行った年月日及び時刻の情報を基に生成される。この脆弱性によって，悪意のある第三者が，Web アプリケーションにログイン中のほかの利用者になりすまし，不正にアクセスできてしまう。

図 3　ミドルウェアで発見された脆弱性の概要

S 主任の調査の結果，ミドルウェアは開発元によるサポートが終了しており，修正プログラムが提供されないことが判明した。また，S 主任は，①販売システムの FW では，セッション ID の偽造を判別できないので，この脆弱性を悪用した攻撃を防御できないと判断した。

このミドルウェアを使用しないよう，販売システムを抜本的に改修するには，長期間を要する。そこで，R 社では，販売システムによる注文受付を一時的に停止し，注文は電話受付だけに限定する方針を決めた。また，インターネット販売事業部の P 課長は，脆弱性への早急な対策案の検討を S 主任に指示した。

〔WAF による対策の検討〕

S 主任は，図 3 の脆弱性への早急な対策案を，Y 社のセキュリティサービス担当の Q 氏に相談した。その結果，WAF の導入の提案を受けた。Q 氏が提案した WAF の主な機能を表に示す。

表　Q氏が提案したWAFの主な機能

機能の名称	機能の概要
シグネチャによる通信検査機能	HTTP による通信をシグネチャと比較し，一致した場合には攻撃として検知する。シグネチャには，脆弱性を悪用する攻撃に含まれる可能性の高い文字列が定義されている。シグネチャの更新情報は，WAF の開発元から定期的に配信される。シグネチャごとに有効化，無効化の選択ができ，有効化したシグネチャに対しては，検知時に通信を遮断するか，遮断は行わず通知だけを行うかを設定できる。独自のシグネチャも作成が可能である。
クッキーの暗号化機能	Web アプリケーションがブラウザに対してクッキーを発行した際，クッキーの値を暗号化して引き渡す。ブラウザからクッキーを受信した際，値を復号して，Web アプリケーションに引き渡す。
SSL アクセラレーション機能	SSL 通信の暗号化と復号を行う。
負荷分散機能	販売システムで利用中の LB と同等性能の負荷分散機能を有する。

次は，WAFによる対策の検討に関する，S主任とQ氏との会話である。

S主任：販売システムのミドルウェアで発見された脆弱性に対しては，WAF を使ってどのような対策が可能でしょうか。

Q氏　：②クッキーの暗号化機能によって，図 3 の脆弱性を悪用した攻撃への対策が可能です。この機能は WAF の導入後にすぐに利用を開始できるので，速やかに販売システムによる注文受付を再開できます。

S主任：分かりました。利用に際して，何か注意点はありますか。

Q氏　：③クッキーの暗号化では，クッキーに属性を付与している場合であっても，その属性の効果を維持できるように考慮されています。しかし，④ブラウザに格納されるクッキーが暗号化されたものになることから，Web アプリケーションによっては，動作に異常が生じる場合がありますので，販売システムでのクッキーの用途を事前に確認すべきです。

S主任：分かりました。確認しておきます。WAF にはシグネチャによる通信検査機能もあり，攻撃の遮断ができるようですが，どのような攻撃が遮断できるのでしょうか。また，この機能もすぐに利用が可能でしょうか。

Q氏　：クロスサイトスクリプティングや SQL インジェクションなど，既知の攻撃を検知して遮断することが可能です。シグネチャによる通信検査機能の利用に際しては，販売システムの可用性を維持するために，事前に十分な動作確認が必要です。販売システムを利用する上で必要な通信（以下，正常な通信と

いう）を WAF が攻撃として検知してしまうことで，利用者が販売システムを利用できなくならないよう，まずは［ a ］を減らすための検証期間を設けます。検証期間には，攻撃を検知しても通信の遮断は行わず，WAF 設定と Web アプリケーション設定のチューニングを行い，［ a ］が十分に減少した段階で，攻撃の遮断を開始します。ただし，チューニングに際しては，⑤正常な通信が攻撃と検知された場合であっても，不用意に，そのシグネチャを無効化するべきではありません。

S 主任 ：シグネチャによる通信検査機能によって，既知の攻撃を検知して遮断することが可能なので，安心して販売システムを運用できるのですね。

Q 氏 ：シグネチャによる通信検査機能では，攻撃がシグネチャに一致しなかった場合には，その攻撃を見逃してしまうので，必ずしも Web アプリケーションを防御できるとは限りません。

S 主任 ：なるほど。Web アプリケーションは，できるだけ脆弱性を除去して運用することが重要ですね。

Q 氏から説明を受けた S 主任は，販売システムでのクッキーの用途を確認した。その結果，WAF の機能によってクッキーを暗号化しても，販売システムの動作には異常が生じないことが分かった。そこで，S 主任は P 課長に WAF の導入を提案した。

〔WAF の導入〕

インターネット販売事業部では，S 主任の提案内容を検討した結果，販売システムへの WAF の導入を決定した。検討に際しては，クッキーの暗号化機能によって図 3 の脆弱性への対策が可能となる点に加えて，開発元によるサポートが終了したミドルウェアで，今後新たな脆弱性が発見された場合にも，シグネチャによる通信検査機能によって攻撃への防御を実現できる可能性がある点も評価された。

販売システムへの WAF の導入の際には，Web サーバへの負荷分散に WAF の負荷分散機能を利用することで，利用中の LB を WAF で置き換える方針とした。また，WAF の SSL アクセラレーション機能を利用し，⑥ブラウザからの SSL 通信は，WAF で終端させることにした。

インターネット販売事業部では，Q 氏の支援の下，WAF を販売システムに導入し，クッキーの暗号化機能を有効化した上で，販売システムによる注文受付を再開した。

その後，検証期間を終え，シグネチャによる通信検査機能の利用を開始した。そして，サポートの終了したミドルウェアを使用しないよう，販売システムの抜本的な改修に向けた検討を開始した。

設問1　本文中の［　a　］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　フェールセーフ　　イ　フェールソフト

ウ　フォールスネガティブ（偽陰性）　　エ　フォールスポジティブ（偽陽性）

設問2　本文中の下線①について，判別できないとS主任が考えた理由を，30字以内で述べよ。

設問3　〔WAFによる対策の検討〕について，(1)～(4)に答えよ。

(1) 本文中の下線②について，クッキーの値を暗号化することで，図3の脆弱性を悪用した攻撃への対策が可能とQ氏が判断した理由を，40字以内で述べよ。

(2) 本文中の下線③について，販売システムへのログイン時に，次のSet-Cookieヘッダを Web アプリケーションが送信した場合，WAF がそれを暗号化した結果の Set-Cookie ヘッダはどれか。解答群の中から選び，記号で答えよ。解答群の中の“☆☆”は，暗号化後の文字列を表す。

（Web アプリケーションが送信した Set-Cookie ヘッダ）

```
Set-Cookie: session_id=uid20101017143045; secure; path=/874045/
```

解答群

ア　`Set-Cookie: session_id=☆☆; path=/874045/`

イ　`Set-Cookie: session_id=☆☆; path=☆☆`

ウ　`Set-Cookie: session_id=☆☆; secure; path=/874045/`

エ　`Set-Cookie: session_id=☆☆; secure; path=☆☆`

(3) 本文中の下線④の動作に異常が生じる場合とは，クッキーがどのように用いられる場合か。30字以内で述べよ。

(4) 本文中の下線⑤について，シグネチャを無効化しても問題ないと判断するためには，何を確認することが望ましいか。“シグネチャ”と“脆弱性”という字句を用いて，60字以内で具体的に述べよ。

設問4　本文中の下線⑥について，この措置を行う理由を55字以内で述べよ。

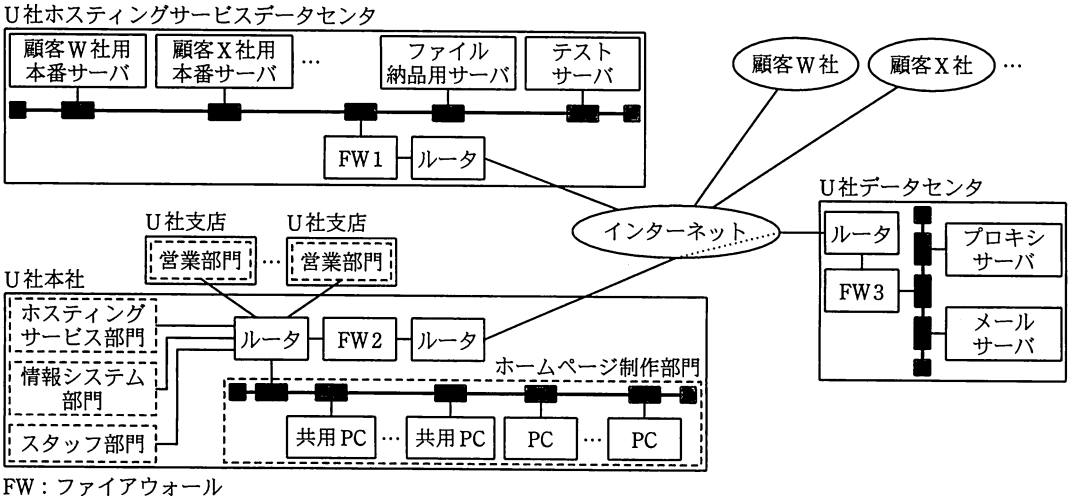
問4　マルウェア対策に関する次の記述を読んで，設問1～3に答えよ。

U社は従業員数 3,200 名の情報システム企業で，ホームページ制作部門，ホスティングサービス部門，営業部門，情報システム部門及びスタッフ部門からなる。

ホームページ制作部門には 150 名が従事し，そのホームページ制作事業は，洗練されたデザインと，検索エンジンによる検索結果の最適化に関する技術に定評がある。電話会議や Web 会議などの遠隔会議を活用して顧客との進捗確認を行うことで費用低減を図っており，全国各地から注文を受け付け，売上を伸ばしている。また，料金設定においても，同社のホスティングサービスの顧客には特別割引料金を提示するといった工夫を行っている。

〔ホームページ制作業務の流れ〕

U社は顧客との間で契約が成立すると，顧客から提供を受けた素材データを基にして，顧客に詳細なデザイン案を提示し，承認を得ると制作に取り掛かる。図 1 にホームページ制作事業関連のネットワーク構成を示す。



FW：ファイアウォール

注　インターネット内の点線はインターネット VPN を表す。FW2 と FW3 は VPN で接続されている。

図1　ホームページ制作事業関連のネットワーク構成

U社では，制作の段階から納品までの間，顧客が随時 HTTP でホームページデータを閲覧し，デザインを確認できるよう，ホスティングサービスデータセンタ内に全顧

客向けにテストサーバを設置している。顧客には，このテストサーバ内の自社向けデータ閲覧専用の利用者 ID とパスワードを提供している。U 社では，ホームページ制作部門からインターネットに向けた FTP アクセスは，プロキシサーバ経由だけに限定している。テストサーバへのホームページデータのアップロードもプロキシサーバ経由で FTP を利用して行っている。

納品時は，本番サーバに FTP で納品物をアップロードする。ただし，顧客が U 社のホスティングサービスを利用せずにホームページを公開する場合は，U 社では，ファイル納品用サーバ又は外部記憶媒体を利用して納品する。

ホームページ制作部門の会議室には部門内で管理している共用 PC が常設されており，いつでも Web 会議を開催できるように環境が整備されている。基本的には Web 会議中に，共用 PC でホームページデータの修正を行うようにしているが，会議中に修正が完了できなかった場合でも，会議終了後 1 営業日以内には修正を行うようにしている。また，共用 PC からは納品時に本番サーバにアップロードすることもある。

〔ホームページ制作部門の情報セキュリティに対する取組み〕

U 社には，幹部，情報システム部門及び各部門の情報セキュリティ担当者からなる情報セキュリティ委員会が設置されている。全社の情報セキュリティ方針の立案，並びに全社共通システムのセキュリティ対策の検討及び実施は情報システム部門が担い，各部門のセキュリティ対策の検討及び実施は各部門の情報セキュリティ担当者が担う。ホームページ制作部門の情報セキュリティ担当者は F 課長と T 主任である。T 主任は，同業他社のセキュリティ事故事例を聞いて，ホームページ制作部門の PC 及び共用 PC への［ a ］の適用を徹底するために，2 年前に検疫システムの導入を情報セキュリティ委員会に提案したが，当時は，費用の問題で実現に至らなかった。その後，T 主任は重大な［ a ］が公開されるたびに部門内の従業員一人一人に呼び掛けて適用の徹底を図ってきた。

〔テストサーバ上のページ改ざん〕

2 か月前にホームページ制作を契約した顧客 W 社は，U 社にとって大口顧客である。W 社は大量の個人情報を取り扱っているので，自社内での情報セキュリティ対策を徹底している。W 社内のイントラネットからインターネットへのアクセスは制限されて

おり，アクセスが業務上必要でないと判断される URL を登録する［ b ］リスト方式の URL フィルタが導入されている。

ホームページ制作は順調に進んだが，1 週間前に W 社から，“テストサーバ上のページを閲覧すると U 社とは無関係と思われる Web サイトにリダイレクトされ，URL フィルタによってアクセスを遮断されるので調査してほしい”，との連絡があった。直ちにホームページ制作部門の担当者がテストサーバ上のホームページのコンテンツを確認したところ，見覚えのない JavaScript コードが埋め込まれていた。ホームページ制作部門の担当者は F 課長に連絡し，F 課長は T 主任に調査を指示した。

T 主任はテストサーバ上のページで見つかった JavaScript コードが，いつ，だれによって埋め込まれたかを調べた。テストサーバ上の FTP ログを見ると，FTP アカウントが U 社以外から使われた日があり，その FTP アカウントの正当な利用者である M さんに確認したところ，その日に作業をした覚えはないとのことだった。また，T 主任が毎日配信を受けている情報セキュリティ関連ニュースを調べた結果，ある攻撃（以下，G 攻撃という）への注意喚起を見つけた。図 2 は G 攻撃のシナリオを (1)～(4) の四つの攻撃フェーズに分けて説明したものである。

(1) 利用者 PC のブラウザから，改ざんされた Web サイトにアクセスすると，トロイの木馬型の不正プログラムを送り込む Web サイト（以下，不正プログラム送り込みサイトという）に強制的にリダイレクトされる。
(2) 利用者が気づかないうちに，不正プログラム送り込みサイトから，利用者 PC のブラウザ経由で不正プログラムがダウンロードされ，実行される。すると，利用者 PC 上のアプリケーションの［ c ］性を突いて不正プログラムに利用者 PC が感染する。悪用される［ c ］性は複数報告されている。
(3) 不正プログラムに感染した利用者 PC から，この利用者が管理する Web サイトに FTP でアクセスする設定となっていると，不正プログラムが，FTP サーバの IP アドレスや，FTP クライアントのパスワード保存機能から FTP アカウントの ID とパスワードを盗み出して，攻撃者のサーバに送付する。
(4) 攻撃者は，送付されてきた FTP サーバの IP アドレスや FTP アカウントの ID とパスワードを使って，利用者が管理する Web サイトに侵入してページを改ざんしたり，不正プログラム送り込みサイトに作り変えたりする。これによって，上記 (1) の改ざんされた Web サイトや不正プログラム送り込みサイトが増える。

図 2　G 攻撃のシナリオ（攻撃フェーズ）

ホームページ制作では，インターネット上の様々な Web サイトにもアクセスすることから，PC が G 攻撃によって改ざんされた Web サイトにアクセスして不正プログラムに感染した可能性がある。そこで，T 主任が，M さんの PC と，M さんが Web 会議中に使用した共用 PC について調べたところ，共用 PC が図 2 で説明されている不正プ

ログラムに感染していた。T 主任が情報セキュリティ委員会に報告すると，どの顧客に被害を与えたかを調査するよう指示があった。①T 主任は，ホームページ制作部門の共用 PC の不正プログラム感染によって被害を与えた顧客の範囲を調査した。調査の結果，被害があったのは W 社だけだったことが判明した。

U 社では，W 社に，テストサーバ上のページ閲覧時にリダイレクトされる原因が G 攻撃によるものだったことを報告した。W 社からは，強い懸念が表明され，再びテストサーバ上でページ改ざんが発生した場合には，本番サーバとして予定している U 社のホスティングサービスの利用を取りやめると通告された。U 社では，ホームページ制作部門だけでなくホスティングサービス部門にもまたがる全社的な問題となった。情報セキュリティ委員会は，この問題を全社で取り組むべき問題と受け止め，情報システム部門とホームページ制作部門とに再発防止策の検討の協力を要請した。

〔G 攻撃による被害の再発防止〕

情報システム部門とホームページ制作部門は，短期的及び中長期的な再発防止策を検討し，表のようにまとめた。

表　再発防止策

再発防止策	実施時期	対応する図 2 の攻撃フェーズ
(a)　U 社以外からのテストサーバへの FTP アクセス元 IP アドレスを制限する。	短期的	ア
(b)　PC を用途別に使い分け，FTP 専用 PC を用意し，FTP 専用 PC にはブラウザをインストールしない。FTP 専用 PC 以外の社内からの FTP アクセスを制限する技術的対策も実施する。	短期的	(1)，(2)，(3)
(c)　PC の OS 及びアプリケーションの更新状況，並びにブラウザ及びウイルス対策ソフトの状況を集中管理する。	短期的	イ
(d)　PC のブラウザで JavaScript 機能を無効化する。	中長期的	ウ
(e)　テストサーバへのデータアップロードを FTP 以外の方法に変更する。	中長期的	エ，オ

表の (b) の PC の使い分けはホームページ制作部門の業務効率に影響を与えるので，T 主任は慎重に検討した。T 主任が共用 PC の利用状況について調べると，アプリケーションのバージョンが古いままになっていたり，ウイルス対策ソフトの“常時スキャ

ン機能”が無効になっていたりした。情報システム部門によると，ほかの部門も同様の状況にあるとのことであった。両部門は，FTP 専用 PC 以外の社内からの FTP アクセスを制限する技術的対策の実施と，PC の管理強化を行うとともに，PC 利用時のセキュリティ意識を高めてもらうよう全従業員への通知も行うことにした。

両部門は，情報セキュリティ委員会に対して，表の再発防止策を提案し，了承された。セキュリティ意識向上の通知内容は，情報システム部門が文書化し，CIO の名前で全従業員に通知された。G 攻撃の手法は今後変化すると考えられることから，情報収集に努めて対策を打っていくことにした。

ホームページ制作部門は，W 社とのホームページ制作に関する話し合いを継続する中で，G 攻撃による被害の発生経緯と再発防止についての U 社の方策を説明し，W 社のホームページは無事にリリースされた。

設問 1　本文中の［ a ］，［ b ］及び図 2 中の［ c ］に入れる適切な字句を答えよ。［ a ］については 10 字以内で，［ b ］，［ c ］については 5 字以内で答えよ。

設問 2　〔G 攻撃による被害の再発防止〕について，(1)，(2)に答えよ。

(1) 表中の［ ア ］～［ オ ］を埋め，再発防止策を完成させたい。表中の (a)，(c)～(e) は，それぞれ図 2 中のどの攻撃フェーズに対応する再発防止策か。防止効果のある攻撃フェーズのうち効果の高いものを選び，項番 (1)～(4) で答えよ。

(2) 表中の (b) で，FTP 専用 PC 以外の社内からの FTP アクセスを制限する技術的対策は，どのサーバで行えばよいか。サーバ名を図 1 中から選び答えよ。ただし，U 社の各部門内は固定 IP アドレスを使用しているものとする。

設問 3　〔テストサーバ上のページ改ざん〕について，(1)，(2)に答えよ。

(1) 本文中の下線①で行った調査の具体的な内容を二つ挙げ，それぞれ 40 字以内で述べよ。

(2) 図 2 の G 攻撃による世の中の被害が拡大してくると，W 社と同じ方式の URL フィルタを採用してもテストサーバの改ざんを見過ごす場合がある。それはどのような場合か。図 2 中の字句を用いて 55 字以内で述べよ。

7. 途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

8. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
9. 問題冊子の余白などは，適宜利用して構いません。
10. 試験時間中，机上に置けるもの及び使用できるものは，次のものに限ります。
なお，会場での貸出しは行っていません。
受験票，B 又は HB の黒鉛筆又はシャープペンシル，鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能は使用不可），ハンカチ，ティッシュ
これら以外は机上に置けません。使用もできません。
11. 試験終了後，この問題冊子は持ち帰ることができます。
12. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
13. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
14. 午後Ⅱの試験開始は 14:30 ですので，14:10 までに着席してください。

お知らせ

1. システムの構築や試験会場の確保などの諸準備が整えば，平成 23 年 11 月から IT パスポート試験において CBT※方式による試験を実施する予定です。
2. CBT 方式による試験の実施に伴い，現行の筆記による試験は，廃止する予定です。
3. 詳細が決定しましたら，ホームページなどでお知らせします。

※CBT（Computer Based Testing）：コンピュータを使用して実施する試験。