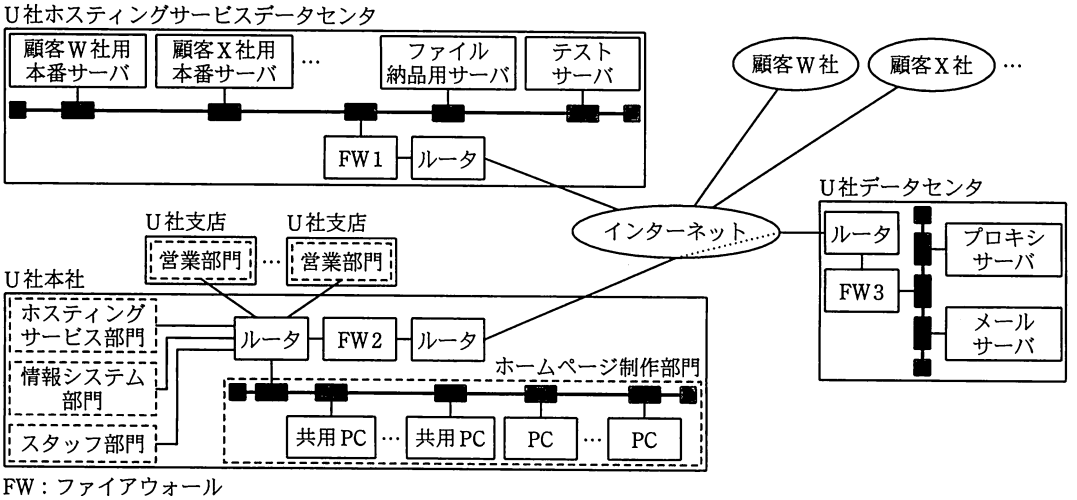
問4　マルウェア対策に関する次の記述を読んで，設問1～3に答えよ。

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。