SC

令和３年度　秋期
情報処理安全確保支援士試験
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. **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。**
4. 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３
選択方法	２問選択

5. 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，**生年月日欄**に**受験票の生年月日**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。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **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。○印がない場合は，採点されません。3問とも○印で囲んだ場合は，はじめの2問について採点します。
   (4) 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。
   (5) 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〕

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。

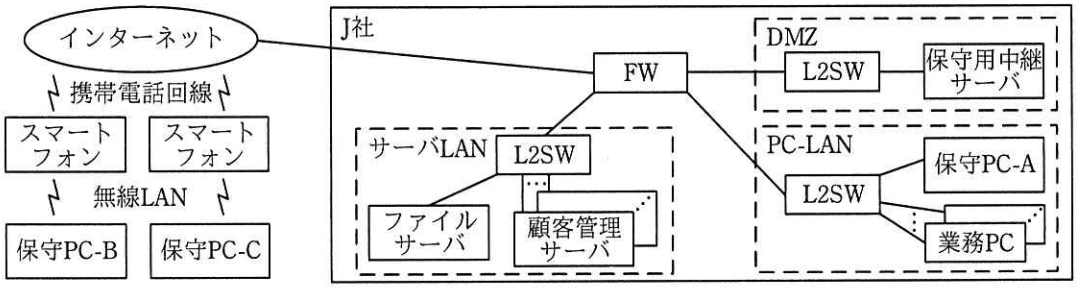
正　誤　表

情報処理安全確保支援士試験　午後Ⅰ　問題

ページ	問題番号	行	誤	正	訂正の内容
12	2	図2 下から 4行目	…，2 の 112 乗の計算量が必要だと言われている。	…，2 の 112 乗の計算量が必要だと言われている。しかし，暗号化されたコンテンツ鍵は入手できないと考えてよい。	下線部分を追加する。

問1　セキュリティインシデントに関する次の記述を読んで，設問1～3に答えよ。

J社は，従業員1,000名の小売業である。J社では，顧客情報を顧客管理サーバで管理している。J社のネットワーク構成を図1に示す。



FW：ステートフルパケットインスペクション型ファイアウォール　　L2SW：レイヤ2スイッチ
保守PC：顧客管理サーバの保守作業に使うPC
注記1　保守PC-A及びサーバLAN上のサーバには，固定のプライベートIPアドレスを割り当てている。
注記2　DMZ上のサーバには，固定のグローバルIPアドレスを割り当てている。

図1　J社ネットワーク構成（抜粋）

〔顧客管理サーバの保守方法〕

顧客管理サーバの保守作業は，図2に示す保守方法に従って行われる。

顧客管理サーバの保守はM社に委託している。M社の保守員2名（以下，保守員1，保守員2という）が，通常は保守 PC-A から，必要に応じて保守 PC-B 又は保守 PC-C から保守を行っている。

保守 PC-A

・未使用時はロッカーに保管している。

保守 PC-B，保守 PC-C

・M社が保守員ごとに貸与する。

接続経路と接続方法

・保守 PC のいずれかから保守用中継サーバに SSH 接続し，さらに，保守用中継サーバから顧客管理サーバに SSH 接続する。

・保守 PC-B 及び保守 PC-C は，M社が貸与するスマートフォンでテザリングし，インターネットに接続する。固定のグローバル IP アドレスは付与されない。

保守用中継サーバに初めて SSH 接続する際の接続先確認方法

1. 保守員が保守 PC-B 又は保守 PC-C を J 社に持参する。
2. 保守 PC-B 又は保守 PC-C をスマートフォンでテザリングし，インターネット経由で保守用中継サーバに SSH 接続する。
3. 接続したサーバのフィンガプリントが表示されるので，保守員は J 社のシステム管理者が紙に印刷しておいた保守用中継サーバのフィンガプリントと一致することを確認する。
4. 一致する場合は，次の確認メッセージに対して“yes”を選択する。
   “Are you sure you want to continue connecting (yes/no)?”
5. 当該接続先確認の手順が正常に完了すると，次回以降は確認メッセージが表示されなくなる。もし，SSH 接続する際に警告メッセージが表示され，接続が切断された場合，保守用中継サーバのフィンガプリントが変わったか，［ a ］という状況が想定されるので，J 社に確認する。

識別・認証・認可方法

a. 保守用中継サーバ

・保守員の着任時に，利用者 ID として，保守員1には op1，保守員2には op2 を割り当てる。

・①当該利用者 ID には，一般利用者の権限を与える。

・パスワード認証を行う。パスワードは保守員自身が設定する。

・保守員の離任時，パスワードを J 社のシステム管理者が変更する。

b. 顧客管理サーバ

・保守員の着任時に，保守用中継サーバの利用者 ID と同じ名称の op1，op2 を割り当てる。

・当該利用者 ID には，特権利用者の権限を与える。

・パスワード認証を行う。パスワードは J 社のシステム管理者が設定し，安全な方法で保守員に伝える。

・保守員の離任時，パスワードを J 社のシステム管理者が変更する。

ログ

・SSH 認証について，成功と失敗が接続先のサーバ上に SSH 認証ログとして記録される。

・保守用中継サーバでのコマンド実行及びその結果，並びに顧客管理サーバでのコマンド実行及びその結果が，保守用中継サーバ上に操作ログとして記録される。

・SSH 認証ログ及び操作ログへのアクセスには特権利用者の権限が必要であり，それらのログの確認は J 社のシステム管理者が実施する。

備考

・保守員は，保守作業に当たって J 社への事前申請及び事後の作業報告が必要である。

図2　顧客管理サーバの保守方法

FWのフィルタリングルールを表1に示す。

表1　FWのフィルタリングルール

項番	送信元	宛先	サービス	動作	ログの記録
1	PC-LAN	インターネット	HTTP，HTTPS	許可	する
2	PC-LAN	サーバLAN	HTTP，HTTPS，SMB	許可	する
3	b	保守用中継サーバ	SSH	許可	する
4	c	保守用中継サーバ	SSH	拒否[1)]	する
5	保守用中継サーバ	顧客管理サーバ[2)]	SSH	許可	する
6	DMZ	インターネット	全て	拒否	する
⋮	⋮	⋮	⋮	⋮	⋮
15	全て	全て	全て	拒否	しない

注記1　項番が小さいルールから順に，最初に合致したルールが適用される。
注記2　項番7～14には，保守用中継サーバ，DMZ，SSHに関するルールはない。
注[1)]　保守PC-B又は保守PC-Cからの保守作業の際は，事前申請に記載された作業時間帯だけ，J社のシステム管理者が“許可”に変更する。
[2)]　複数台の顧客管理サーバそれぞれのIPアドレスが指定されている。

〔セキュリティインシデントの発生と対応〕

6月16日に，J社のシステム管理者であるFさんが，FWのフィルタリングルールに基づいて記録されたログ（以下，FWログという）から不審なログを発見した。調査したところ，暗号資産を採掘するプログラム（以下，プログラムHという）が保守用中継サーバで動作しており，②定期的にインターネット上のサーバに通信を試みていたことが分かった。そこで，外部の情報処理安全確保支援士（登録セキスペ）のS氏の助言の下，影響範囲及び原因の調査並びに対策方法の検討をすることにした。S氏からは，保守作業関連書類，FWログ，SSH認証ログ及び操作ログの調査並びに保守員へのヒアリングをするように助言があった。

翌日，Fさんは，S氏に図3に示す保守作業関連書類及び各種ログの調査結果並びに図4に示すヒアリング結果を報告した。

事前申請及びFWの設定変更
・保守員2から，顧客管理サーバの保守を，保守PC-Cを使って6月14日7時から9時30分に行うという事前申請が出されていた。事前申請に従って，J社のシステム管理者はFWの設定を変更した。
FWログの調査結果
・申請された保守作業時間帯に，二つのグローバルIPアドレスから保守用中継サーバにSSH接続されていた。
操作ログの調査結果
・6月14日8時に，op1がプログラムHを設置した。
・6月14日7時20分から9時10分の間に，op2による顧客管理サーバの保守作業の操作が行われた。操作内容は事前申請のとおりだった。
保守用中継サーバ上のSSH認証ログの調査結果
・op1は6月14日7時30分から認証の失敗が84回続き，7時40分に認証に成功していた。
・op2は6月14日7時20分に認証に成功していた。
保守作業報告
・保守員2から，6月14日7時20分から9時10分の保守作業について報告されていた。

図3　保守作業関連書類及び各種ログの調査結果

6月14日の保守作業に関するヒアリング結果
・保守員1からは，保守作業は実施していないと回答があった。
・保守員2からは，保守PC-Cを使い事前申請どおりに作業を行い，ほかの作業はしていないと回答があった。事前申請，操作ログ及び事後の作業報告と矛盾する回答はなかった。
そのほかの調査結果
・op1に設定されているパスワードが，推測の容易な文字列であることが分かった。

図4　保守員へのヒアリング結果

S氏は，この報告から，第三者がop1のパスワードを推測してインターネット経由で不正アクセスした可能性が高いと判断し，被害範囲の特定のために各種ログを追加調査するように助言した。Fさんによる追加調査の結果，FWログ，SSH認証ログ及び操作ログからは，保守用中継サーバにプログラムHを設置した記録は見つかったが，保守用中継サーバから顧客管理サーバを含む他機器へのアクセスの記録は見つからなかった。FさんとS氏は，これらの調査結果から，影響範囲は保守用中継サーバだけにとどまり，情報漏えいの被害もなかったと結論付けた。

〔セキュリティインシデントの再発防止〕

S氏から，今回のセキュリティインシデントの再発防止について，幾つか提言があった。

一つ目の提言は，サーバに対する認証の強化である。保守用中継サーバ及び顧客管理サーバへの SSH 接続の認証方式を，パスワード認証から公開鍵認証に変更するというものである。F さんは，図 5 に示す公開鍵認証の初期登録手順を作成した。

保守用中継サーバへの SSH 接続に用いる公開鍵認証の初期登録手順
・公開鍵認証に使う鍵ペアは，各保守員が保守 PC ごとに作成し，管理する。
・③鍵ペアの秘密鍵には，十分な強度のパスフレーズを設定する。
・公開鍵は，J 社のシステム管理者が保守用中継サーバに登録する。
・SSH サーバの設定では，公開鍵認証を有効にするとともに，［ d ］を無効にする。

図 5　公開鍵認証の初期登録手順（抜粋）

次は，図 5 に関する S 氏と F さんの会話である。

S 氏　：万一，保守用中継サーバが不正アクセスされた場合を想定して，顧客管理サーバへの SSH 接続に必要な［ e ］を利用されないように，保守用中継サーバに保存しない運用にしましょう。SSH Agent Forwarding と呼ばれる機能を使うと，保守作業の SSH 接続に必要な［ e ］の全てを保守 PC にだけ保存する運用にできます。

F さん：承知しました。

二つ目の提言は，SSH の接続元の制限である。FW で接続元を制限することができれば，万一，SSH サーバソフトウェアで認証バイパスなどの脆弱(ぜい)性が発見されて悪用された場合にも有効な対策となる。

そこで，F さんは，保守 PC-B 及び保守 PC-C を，VPN 装置を介して又は直接，M 社内のネットワークに接続させた後に，インターネット経由で保守用中継サーバにアクセスさせることを考えた。このとき，［ f ］ことができれば，保守用中継サーバへのアクセスを表 1 の項番 4 のルールを変更することによって制限できる。そこで，これらへの対応を M 社に打診した。

そのほかの再発防止策についても，F さんは S 氏の提言について検討を重ね，保守用中継サーバ及び顧客管理サーバに関するセキュリティを強化した。

設問1　〔顧客管理サーバの保守方法〕について，(1)～(3)に答えよ。

(1)　図2中の［　a　］に入れる適切な字句を20字以内で答えよ。

(2)　図2中の下線①の設定にした目的を，“操作ログ”という字句を用いて25字以内で述べよ。

(3)　表1中の［　b　］，［　c　］に入れる適切な字句を，図1中の字句を用いて答えよ。

設問2　〔セキュリティインシデントの発生と対応〕について，(1)，(2)に答えよ。

(1)　本文中の下線②の通信は，表1のどのルールによってFWログに記録されるか。表1中の項番で答えよ。

(2)　今回のセキュリティインシデントにおいて，第三者が保守用中継サーバにSSH 接続可能だった期間は何月何日の何時何分から何月何日の何時何分までか。期間を答えよ。

設問3　〔セキュリティインシデントの再発防止〕について，(1)～(4)に答えよ。

(1)　図5中の下線③について，パスフレーズを設定する目的を30字以内で具体的に述べよ。

(2)　図5中の［　d　］に入れる適切な字句を10字以内で答えよ。

(3)　本文中の［　e　］に入れる適切な字句を5字以内で答えよ。

(4)　本文中の［　f　］に入れる適切な字句を20字以内で答えよ。

問2　システム開発での情報漏えい対策に関する次の記述を読んで，設問 1～3 に答えよ。

R 社は従業員 500 名の情報サービス事業者である。営業部門，システム開発部門及び管理部門があり，管理部門内の情報システム部が社内の情報システムを管理している。システム開発部門の従業員は，一つ以上のシステム開発プロジェクト（以下，プロジェクトという）に参加している。

同業他社でのシステム開発において，情報漏えいが発生したことから，情報システム部の K 部長は部下の Z 主任に，プロジェクトにおいて秘密として扱われている設計文書（以下，設計秘密という）の管理について，問題がないか調査するように指示した。

〔設計秘密の管理〕

R 社の規則では，設計秘密は次のように管理することになっている。

・設計秘密は，R 社指定の文書作成ソフトウェア（以下，W ソフトという）を使って PC 上で作成及び暗号化を行い，R 社のネットワーク内のファイルサーバだけに保管する。ファイルサーバでは，プロジェクト単位にディレクトリを分け，各ディレクトリにはプロジェクトメンバだけがアクセスできるように，各プロジェクトのマネージャがアクセス権限を設定する。

・W ソフトでは，パスワードを基に 256 ビットの鍵が生成され，その鍵を使って，ファイルが AES で暗号化される。ファイルを開くときには，パスワードの入力が求められる。設計秘密には，プロジェクト単位のパスワード（以下，P パスワードという）を使用する。

・プロジェクトごとに，協力会社の T 社と秘密保持契約を結び，設計秘密を共有する。設計秘密は，T 社内でも R 社と同様の設備に保管し，アクセス権限を設定する。

・R 社と T 社の間で設計秘密をやり取りする際には，Web ブラウザからクラウドストレージサービスを利用する。R 社は，このクラウドストレージサービスでは，プロジェクト単位にディレクトリを分け，各ディレクトリには R 社と T 社のプロジェクトメンバだけがアクセスできるようにアクセス権限を設定する。

・プロジェクトを離任する者が出た場合には，ファイルサーバとクラウドストレー

ジサービスに保管しているプロジェクトの設計秘密に対して，離任者がアクセスできないようにする。

〔管理についての問題〕

Z 主任が，各プロジェクトのマネージャに，設計秘密の管理についてヒアリングしたところ，表1に示す問題があることが分かった。

表1　設計秘密の管理についての問題

名称	問題
問題1	ファイルを開くたびにPパスワードの入力が必要となり，作業負荷が高い。
問題2	Pパスワードの強度が十分でないおそれがある。
問題3	プロジェクト離任者が出た場合，Pパスワードが設定されている全てのファイルに対して［　a　］を行う必要があり，作業負荷が高い。
問題4	プロジェクトメンバが，プロジェクト参加期間中にR社の規則に反して［　b　］した設計秘密は，当該メンバであれば離任後も参照できてしまう。

〔問題への対策の検討〕

Z 主任は問題の解決に向けて，IRM（Information Rights Management）製品による対策を検討することにした。

Z主任は，導入実績の豊富なL社のIRM製品（以下，IRM-Lという）によって表1中の問題が解決できるかどうかを確認することにした。IRM-Lは，複数の利用者から成るグループ単位にアクセス権限の付与ができる。IRM-L は IRM クライアントと IRM サーバから構成される。IRM クライアントは，PC にインストールされ，ファイルの暗号化及び復号を行う。IRM サーバは，IRM クライアントの管理を行う。IRM-Lの概要を図1に示す。

1. IRM サーバ及び IRM クライアントの RSA 鍵ペア

IRM サーバをインストールする際，2048 ビットの RSA 鍵ペアが生成される（以下，IRM サーバで生成された公開鍵を IRM サーバ公開鍵といい，秘密鍵を IRM サーバ秘密鍵という）。IRM サーバ公開鍵は各 IRM クライアントに配付される。

IRM クライアントをインストールする際，2048 ビットの RSA 鍵ペアが生成される（以下，IRM クライアントで生成された公開鍵を IRM クライアント公開鍵といい，秘密鍵を IRM クライアント秘密鍵という）。

2. アカウントの種類

アカウントには次の 3 種類がある。

・利用者アカウント

利用者が使う。ファイルの保護及び保護されたファイルを開くことができる。利用者アカウントには利用者 ID，パスワード，メールアドレス，所属会社，所属部署，所属するグループなどの属性がある。

・グループ管理者アカウント

グループ管理者が使う。利用者アカウントをグループに所属させたり，グループから削除したりできる。

・IRM 管理者アカウント

IRM 管理者が使う。IRM サーバの設定，グループの管理，利用者アカウントの管理，グループ管理者アカウントの管理ができる。全てのグループに対して，グループ管理者アカウントと同様の権限をもつ。

3. 利用者とグループの管理

IRM 管理者は，IRM サーバ上にグループを作り，そのグループに対して，グループ管理者アカウントを作成する。

IRM 管理者は，IRM サーバ上に利用者アカウントを作成し，利用者 ID と初期パスワードを利用者に伝える。利用者は初回ログイン時に初期パスワードを変更する。

一つの利用者アカウントが，複数のグループに所属することもある。

4. IRM クライアントの起動とファイル保護の処理

IRM クライアントは，PC へのログイン時に自動起動される。利用者は IRM クライアントの起動画面に，利用者 ID とパスワードを入力する。IRM クライアントと IRM サーバとの通信は HTTPS で行う。

利用者がファイルの保護をするとファイルが暗号化され，ファイルの利用権限が自身の所属するグループのうち選択したグループに付与される。付与する権限は次から選ぶ。

参照：ファイルの参照だけを許可する。

編集：参照に加えて，ファイルの編集も許可する。編集後のファイルも IRM-L で保護される。

ファイルの保護では次の処理が行われる。

・ファイル単位に 256 ビットの AES 鍵（以下，コンテンツ鍵という）が生成され，ファイルはコンテンツ鍵で暗号化される。暗号化されたファイルには IRM-L 固有の拡張子が付与され，元のファイルと同じディレクトリに保存される。

・コンテンツ鍵は，IRM サーバ公開鍵で暗号化される。

・暗号化されたコンテンツ鍵は，暗号化後のファイルのハッシュ値及び付与された権限とともに IRM サーバに送信され，IRM サーバ内で保存される。

・IRM サーバへの送信後，PC 内のコンテンツ鍵と元のファイルは完全に削除される。

図 1　IRM-L の概要

5. 保護されたファイルを開くときの処理
保護されたファイルが開かれると，次の処理が行われる。
(i) IRM クライアントから利用者 ID，暗号化後のファイルのハッシュ値，及び IRM クライアント公開鍵が IRM サーバに送信される。
(ii) IRM サーバでは，暗号化後のファイルのハッシュ値が参照され，利用者アカウントがファイルに対する権限をもっている場合に，IRM サーバ秘密鍵でコンテンツ鍵が復号される。
(iii) IRM サーバでは，コンテンツ鍵が，IRM クライアント公開鍵で暗号化され，IRM クライアントに送られる。
(iv) IRM クライアントでは，送付されたコンテンツ鍵が IRM クライアント秘密鍵で復号される。
(v) IRM クライアントでは，コンテンツ鍵で対象ファイルが復号される。
(vi) 復号されたファイルに対しては，参照又は編集後に再びファイル暗号化の処理が行われる。

図 1　IRM-L の概要（続き）

Z 主任は，次のように IRM-L を利用することによって，表 1 中の問題を表 2 のとおり解決できると考えた。

・各プロジェクトにグループを一つ割り当てる。
・システム開発部門の従業員に IRM-L の利用者アカウントを割り当てる。
・設計秘密は，IRM-L で保護した上で，ファイルサーバに保管する。
・T 社のプロジェクトメンバも IRM-L を利用し，IRM-L で保護されたファイルを，クラウドストレージサービスにアップロードする。

表 2　設計秘密の管理についての問題に対する解決策

名称	IRM-L による解決策
問題 1	（省略）
問題 2	（省略）
問題 3	IRM-L では，ファイルの保護にパスワードを利用しない。また，①簡単な操作でプロジェクト離任者による設計秘密の参照を禁止できるので，従来と比較して大幅に作業負荷が減る。
問題 4	②プロジェクト離任者に対する操作を適切に行うことによって参照不可にできる。

問題 2 について，P パスワードの利用状況を調査したところ，英数字と一部の記号を用いた 10 字程度のパスワードの利用が多いことが分かった。それに基づいて，W ソフトによって暗号化されたファイルと IRM-L によって保護されたファイルの解読に必要な計算量を比較し，結果を図 2 にまとめた。

Wソフトによって暗号化されたファイルの解読：
鍵を総当たりで特定するには，最大で 2 の 256 乗の計算量が必要になる。また，その鍵を生成するためのPパスワードが文字種64種類で長さ10字とすると，Pパスワードの推測には最大で2の［ c ］乗の計算量が必要になる。
IRM-Lによって保護されたファイルの解読：
コンテンツ鍵を総当たりで特定するには，最大で 2 の 256 乗の計算量が必要になる。また，コンテンツ鍵を保護するIRMサーバ公開鍵は2048ビットであり，NIST SP 800-57によると，RSA-2048のセキュリティ強度は112ビットの共通鍵暗号と同等であることから，RSA-2048を破るには，2の112乗の計算量が必要だと言われている。

以上から，IRM-Lによって保護されたファイルの解読はWソフトによって暗号化されたファイルの解読と比較して 2 の［ d ］乗倍の計算量が必要になるので，より安全だと考えられる。

図2　比較結果

IRM-Lでは，一定時間当たりのログイン試行回数を制限する機能や，一定回数のログイン失敗でアカウントをロックする機能によって，攻撃者がログインに成功するリスクを下げることができる。しかし，利用者 ID とパスワードによる認証だけでは，推測が容易なパスワードを利用者が設定してしまうと，長さが 10 字であったとしても［ e ］攻撃に対して脆弱（ぜい）となるので，［ f ］への変更が可能か検討することにした。

〔社外とのやり取り〕

T社ネットワークからIRMサーバにアクセスするには，IRMサーバをR社のDMZに設置し，インターネットからアクセス可能にする必要がある。Z主任は，IRMサーバをDMZに設置した場合のリスクと対策を表3のとおりまとめた。

表3　IRMサーバをDMZに設置した場合のリスクと対策（抜粋）

リスク	対策[1)]
グループ管理者及びIRM管理者へのなりすまし	・［ f ］への変更 ・ログイン及びその試行の監視
IRM-L の既知の脆弱性を悪用したサーバへの侵入	・脆弱性修正プログラムの定期的な確認と適用 ・IPSの利用

注[1)]　T社の一部の事業所はIPアドレスを固定できないので，T社のIPアドレスだけからアクセスを許可するという対策は取れない。

IRM-Lの運用について情報システム部で検討した結果，ここまで検討した対策を全て採用した場合でも，③PC がマルウェアに感染してしまうと，設計秘密の内容を不正に取得されてしまう場合があることが分かった。そこで，マルウェア対策の強化も導入計画に盛り込んだ上で，IRM-Lの導入を進めることにした。その後，IRM-Lを導入し，設計秘密に対する情報漏えい対策を強化することができた。

設問1　表1中の［ a ］に入れる適切な字句を15字以内で，表1中の［ b ］に入れる適切な字句を10字以内でそれぞれ答えよ。

設問2　〔問題への対策の検討〕について，(1)～(5)に答えよ。

(1) 表 2 中の下線①について，操作を行えるアカウントだけを解答群から全て選び，記号で答えよ。また，操作を35字以内で具体的に述べよ。

解答群

ア　IRM管理者アカウント　　イ　グループ管理者アカウント

ウ　利用者アカウント

(2) 表2中の下線②について，参照不可になるのは，図1中の5.のどの処理でエラーになるからか。(i)～(vi)の記号で答えよ。

(3) 図2中の［ c ］，［ d ］に入れる適切な整数を答えよ。

(4) 本文中の［ e ］に入れる適切な字句を答えよ。

(5) 本文中及び表3中の［ f ］に入れる適切な字句を10字以内で答えよ。

設問3　本文中の下線③について，どのような動作をするマルウェアに感染すると不正に取得されるか。不正取得時のマルウェアの動作を 45 字以内で具体的に述べよ。

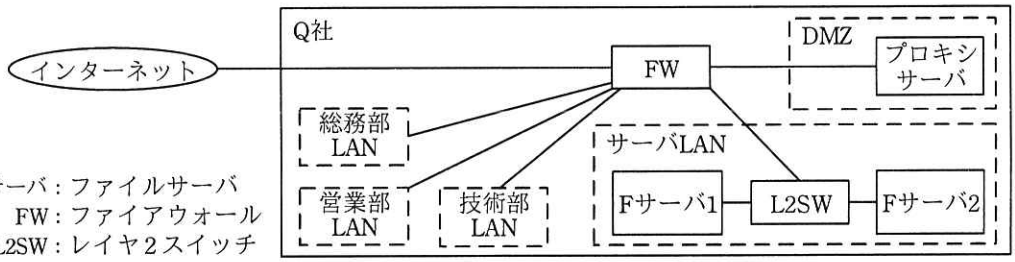
問３　PC のマルウェア対策に関する次の記述を読んで，設問 1～3 に答えよ。

Q 社は，従業員 100 名の金属加工会社である。Q 社には，総務部，営業部及び技術部がある。

Q 社では，全従業員に PC を貸与している。総務部員の PC は総務部 LAN に，営業部員の PC は営業部 LAN に，技術部員の PC は技術部 LAN に接続されている。業務に必要なソフトウェアを自らインストールして使用したいという各部からの要求に対応するために，貸与している PC の従業員の利用者 ID に管理者権限を付与している。

〔Q 社のネットワーク構成〕

Q 社の情報システムの管理は，総務部情報システム係の D 主任と E さんが行っている。Q 社のネットワーク構成を図 1 に示す。



注記 1　PC の記載は省略している。
注記 2　プロキシサーバには，グローバル IP アドレスを固定で割り当てている。
注記 3　総務部 LAN，営業部 LAN 及び技術部 LAN 内の各 PC，並びに F サーバ 1 及び F サーバ 2 には，プライベート IP アドレスを固定で割り当てている。

図 1　Q 社のネットワーク構成（抜粋）

F サーバ 1 及び F サーバ 2 には，PC 上の Web ブラウザを使ってアクセスする。利用者 ID 及びパスワードでログインした後，ファイルの格納及び取り出しが行える。F サーバ 1，F サーバ 2 及び PC のそれぞれの hosts ファイルには，プロキシサーバ，F サーバ 1 及び F サーバ 2 のホスト名と IP アドレスが登録されている。

プロキシサーバの機能概要を表 1 に示す。

表1　プロキシサーバの機能概要（抜粋）

機能名	機能概要
URL フィルタリング機能	・V 社の URL フィルタリングソフトが組み込まれており，URL フィルタリングルール（以下，UF ルールという）を用いて，指定した URL へのアクセスを許可又は拒否することができる。 ・UF ルールは，アクセス元の IP アドレス範囲ごとにそれぞれ別のルールを設定することができる。 ・一つの UF ルールは，次の三つのリストから成り，上から順に適用される。 －管理者許可リスト：管理者が設定できる，アクセスを許可する URL のリスト －管理者拒否リスト：管理者が設定できる，アクセスを拒否する URL のリスト －V 社拒否リスト：V 社が提供する，アクセスを拒否する URL のリスト ・管理者許可リストに，“全て”と記載すると，全ての URL へのアクセスが許可される。管理者拒否リストに，“全て”と記載すると，管理者許可リストで許可した URL 以外の URL へのアクセスが拒否される。管理者許可リストに何も設定しないと，そのリストはスキップされる。管理者拒否リストも同様である。 ・どの UF ルールにも該当しない場合は，アクセスは許可される。
ログ機能	・アクセスの日時，アクセス元 IP アドレス，URL 並びに，許可又は拒否の結果をアクセスログとして保存する。

注記1　V 社拒否リストは，V 社サイトから適時ダウンロードされる。
注記2　Q 社では，管理者許可リスト及び管理者拒否リストに何も設定していない。

Q 社では，PC 及びサーバに，V 社のマルウェア対策ソフトを導入し，リアルタイムスキャンを有効にしている。マルウェア定義ファイルは，PC では起動時及び毎朝 9 時に，サーバでは毎朝 9 時に，自動で V 社のマルウェア定義ファイル配布サイト（以下，V 社配布サイトという）に HTTPS で接続し，更新している。PC の利用者及びサーバの管理者は，マルウェア対策ソフトの画面の操作によってマルウェア定義ファイルを手動で更新することもできる。さらに，別の PC を用いてマルウェア定義ファイルを V 社配布サイトから手動でダウンロードし，そのファイルを保存した DVD-R を用いて更新することもできる。F サーバ 1 及び F サーバ 2 がインターネットと通信するのは，マルウェア定義ファイルの更新時だけである。

F サーバ 1 及び F サーバ 2 に，OS 及びアプリケーションソフトウェアの脆弱(ぜい)性修正プログラムを適用する場合，E さんが，各ベンダのサイトから脆弱性修正プログラムを PC にダウンロードして DVD-R に保存し，サーバに適用している。

E さんは，週次アクセスログ調査として，毎週月曜日の 10 時に，前週の月曜日から日曜日までの F サーバ 1 及び F サーバ 2 へのアクセスログを調査している。

FW は，ステートフルパケットインスペクション型である。FW では，アドレス変換機能を使用していない。FW のフィルタリングルールを表 2 に示す。

表2　FWのフィルタリングルール

項番	送信元	宛先	サービス	動作
1	プロキシサーバ	インターネット	HTTP，HTTPS	許可
2	サーバLAN，総務部LAN， 営業部LAN，技術部LAN	プロキシサーバ	代替HTTP[1)]	許可
3	総務部LAN，営業部LAN，技術部LAN	Fサーバ1	HTTPS	許可
4	総務部LAN，営業部LAN，技術部LAN	Fサーバ2	HTTPS	許可
⋮	⋮	⋮	⋮	⋮
9	全て	全て	全て	拒否

注記1　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。
注記2　項番5～8には，HTTP及びHTTPSに関するルールはない。
注1)　代替HTTPのポート番号は，8080である。

〔不審なログインの発見と対応〕

Eさんが，12月9日月曜日に週次アクセスログ調査をしたところ，12月6日の11時から13時にFサーバ1及びFサーバ2にログインを試みて失敗した記録が多数見つかった。アクセス元は，営業部のGさんのPC（以下，PC-Gという）であった。Eさんが，10時40分にGさんに電話で問い合わせたところ，12月6日は，Fサーバ1及びFサーバ2にはログインを試みていないとのことであった。Eさんは，PC-Gがマルウェアに感染したおそれがあると考え，①マルウェア感染拡大防止のためのPC-Gの初動対応をGさんに指示した。また，Gさんへの代替PCの貸出しとPC-Gの回収を行い，PC-Gについてはマルウェア感染への対応として，ディジタルフォレンジックスによる調査を行うことにして②必要な情報を取得した。

Eさんからマルウェア感染のおそれがあるという報告を受けたD主任は，PC-Gで［　a　］という方法を使って［　b　］をした後に，フルスキャンを実施するようEさんに指示した。さらに，図2に示すマルウェアへの対処をQ社全体に指示することにした。

(1) マルウェア対策ソフトによる対処について
　貸与しているPCで，［　c　］という方法を使って［　b　］をした後，フルスキャンを実施する。
(2) 報告について
　上記(1)の結果を情報システム係に報告する。

図2　マルウェアへの対処

Eさんは，PC-Gのフルスキャンで検出されたマルウェア（以下，マルウェアXという）の駆除を16時に完了した。Eさんは，マルウェアXへの感染の経緯を確認するために，Gさんに PC-Gの使用状況をヒアリングした。

Eさんは，図3に示す調査結果を，12月10日の13時にD主任に報告した。

(1) Gさんの PC-Gの使用状況
・12月6日9時に PC-Gを起動した。
・10時に，インターネットの検索サイトでファイル比較ツールを検索した。検索して見つかったサイト（以下，サイトPという）にあったツールPをダウンロードした。その後，管理者権限を用いてツールPをインストールした。
・11時にツールPを起動した。
・17時に PC-Gをシャットダウンした。
・12月6日は，Fサーバ1及びFサーバ2にはログインしていない。
・12月9日9時に，PC-Gを起動した。
(2) マルウェアXに関する情報
・V社のサイトに，マルウェアXに関する次の情報が掲載されていた。
- マルウェアXは，ツールPを装っている。
- C&Cサーバの URLのリスト（以下，Cリストという）がマルウェア中に保持されている。
- マルウェア中のパスワードリストを使って，hostsファイルに登録されている機器へのログインを試行する。ログインが成功すると，その機器からファイルをダウンロードし，C&Cサーバにアップロードする。
・V社は，マルウェアXに対応したマルウェア定義ファイルを12月9日10時にリリースした。
(3) V社拒否リストに関する情報
・Cリストに登録されている URLは，11月25日にV社拒否リストに追加されていた。
(4) プロキシサーバのアクセスログの調査
・アクセス元 IPアドレスが PC-Gであるアクセスを，プロキシサーバのアクセスログで，12月9日17時から3か月遡って調査した。調査の結果，Cリスト中の URLへのアクセスは，12月6日に1件だけであり，そのアクセスは URLフィルタリング機能で拒否されていた。
（省略）
(7) その他
・12月9日17時に，Q社全体でのフルスキャンでマルウェアは検出されなかったことを確認した。
・12月9日0時から17時までのFサーバ1及びFサーバ2のアクセスログに，ログインの失敗の記録はなかった。

図3 調査結果

報告を受けたD主任は，プロキシサーバに関して次の2点を指示した。

・Q社内からサイトPに接続できないようにするための管理者拒否リストの設定変更
・③プロキシサーバのアクセスログに関して調査すべき範囲の漏れをカバーするための追加調査

Eさんは，設定変更したこと，及び追加調査の結果，問題がなかったことをD主任に報告した。D主任とEさんは，図3，設定変更の実施及び追加調査の結果を総務部長に報告した。総務部長は，今回のマルウェアXの感染を踏まえ，追加のマルウェア対策の検討を指示した。D主任とEさんは，次の項目を検討することにした。

項目1：万が一マルウェアに感染した場合の被害拡大を防ぐ対策

項目2：マルウェア感染のリスクを低減する対策

〔項目1の検討〕

D主任とEさんは，PCがマルウェアに感染した場合，Fサーバ1及びFサーバ2にも影響があり得ると考えた。そこで，従業員が，所属している部以外のLANにPCを接続することを禁止した上で，FW及びプロキシサーバの設定変更の案を次のとおりまとめた。

・Fサーバ1の利用者を総務部員及び営業部員に，Fサーバ2の利用者を技術部員にそれぞれ振り分けて，④FWのフィルタリングルールのうちの二つのルールについて，送信元を変更する。

・サーバLANとインターネットとの間の通信を運用に必要なものだけにするために，アクセス元がサーバLANのUFルールを表3のとおりに設定する。

表3　アクセス元がサーバLANのUFルール

リスト	URL
管理者許可リスト	d
管理者拒否リスト	e
V社拒否リスト	（省略）

D主任とEさんは，設定の変更は直ちに実施できると考え，変更内容を総務部長に報告し，許可を得て設定を変更した。

〔項目2の検討〕

D主任とEさんは，マルウェア感染のリスクを低減するために，管理者権限の付与は，情報システム係の利用者IDに限定するのがよいと考えた。さらに，あらかじめ

登録した実行ファイルだけの実行を，ファイルのハッシュ値を比較することによって許可するソフトウェア（以下，Y ソフトという）の導入を検討することにした。E さんは，Y ソフトを利用する上で注意点はないのかと，D 主任に質問した。D 主任は，次のように答えた。

・⑤ハッシュ値の登録変更が必要になる場合がある。
・⑥ある種のマルウェアでは実行を禁止できない。

D 主任と E さんは，Y ソフトのメリットとデメリットの確認，及び導入案の作成を進めた。

設問 1　〔不審なログインの発見と対応〕について，(1)～(4)に答えよ。

(1)　本文中の下線①について，初動対応の内容を 15 字以内で述べよ。

(2)　本文中の下線②について，どのような情報か。10 字以内で答えよ。

(3)　本文中の［　a　］に入れる適切な方法を 35 字以内で，本文及び図 2 中の［　b　］に入れる適切な対応を 20 字以内で，図 2 中の［　c　］に入れる適切な方法を 25 字以内でそれぞれ述べよ。

(4)　本文中の下線③について，追加調査の範囲を 25 字以内で具体的に述べよ。

設問 2　〔項目 1 の検討〕について，(1)，(2)に答えよ。

(1)　本文中の下線④について，変更する二つのルールの項番と，それぞれの変更後のルールにおける送信元の内容を答えよ。

(2)　表 3 中の［　d　］，［　e　］に入れる適切な設定内容を答えよ。

設問 3　〔項目 2 の検討〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑤について，どのような場合か。30 字以内で具体的に述べよ。

(2)　本文中の下線⑥について，どのようなマルウェアか。35 字以内で具体的に述べよ。

6. 退室可能時間中に退室する場合は，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

7. **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。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，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，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬，マスク

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 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。
12. 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。
13. 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。