(2) 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のであるから、無効にする必要があるのは「パスワード認証」である。

(3) SSH Agent Forwarding とは、公開鍵認証方式が設定された SSH サーバへの接続時に、"ssh Agent"が秘密鍵に設定されているパスフレーズの入力を代行する仕組みである。J 社では、保守 PC から保守用中継サーバに SSH 接続した後、顧客管理サーバに SSH 接続して保守作業を行う方式である。このとき、接続に必要な秘密鍵とパスフレーズを保守 PC の"ssh Agent"に登録しておくことで、顧客管理サーバへの SSH 接続に用いる秘密鍵を保守用中継サーバに保存する必要がなくなる。これにより、保守用中継サーバが不正アクセスされたとしても、顧客管理サーバへの SSH 接続に必要な秘密鍵を不正利用されるのを防ぐことができる。

(4) 現状では、保守 PC-B, C に固定の IP アドレスが付与されていないため、保守作業時間帯は表 1 の項番 4 が送信元 IP アドレスの制限なく"許可"になり、第三者による不正アクセスのリスクが高まる。問題文では、保守 PC-B, C から保守用中継サーバへの接続を、VPN 装置を介して直接行う方式か、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アクセスさせる方式が検討されている。これらは、保守 PC-B, C の送信元 IP アドレスを固定にし、表 1 の項番 4 のルールを特定の IP アドレスのみ許可するよう変更することで、不正アクセスのリスクを低減させることを目的としている。

＜問２＞　システム開発での情報漏えい対策

●設問１

［試験センターによる解答例］
a：P パスワードの変更（9 字）
b：PC にコピー（6 字）

＜解説＞

a：プロジェクトメンバは P パスワードを知っているため、離任後であっても設計秘密にアクセスが可能である。離任後の元プロジェクトメンバが設計秘密にアクセスできないようにするためには、P パスワードを変更する必要がある。

b：〔設計秘密の管理〕にあるように、R 社の規則では、設計秘密は W ソフトを使って 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こととなっている。この規則に反して、プロジェクト参加期間中にプロジェクトメンバが設計機密を PC にコピーしていたとすれば、当該メンバは離任後も設計機密を参照できてしまう。

●設問２

［試験センターによる解答例］

(1) アカウント：ア、イ
　　操作：プロジェクト離任者の利用者アカウントをグループから削除する。(30 字)

(2) (ii)

(3) c：60
　　d：196

(4) e：辞書

(5) f：多要素認証 (5 字)

＜解説＞

(1) 図 1 にあるように、IRM-L では、利用者アカウントを 1 つ以上のグループに所属させることで、グループ毎にアクセス権を管理する仕組みとなる。ある利用者が作成したファイルは、当該利用者が所属するグループに利用権限が付与される。この仕組みであれば、プロジェクト離任者の利用者アカウントを全てのグループから削除することで、設計秘密の参照を禁止することができる。利用者アカウントをグループから削除できるアカウントは、アの IRM 管理はアカウントと、イのグループ管理者アカウントである。

(2) プロジェクト離任者の利用者アカウントを全てのグループから削除することにより、設計秘密ファイルへの全ての権限が失われる。したがって、図 1 の 5.の(ii)の処理でエラーが発生することになる。

(3) c：文字種が 64 種類で長さ 10 字であるから、P パスワードは 64 の 10 乗通りである。64 は 2 の 6 乗であるから、6×10＝60 で、P パスワードの推測には 2 の 60 乗の計算量が必要となる。

d：RSA-2048 を破るには 2 の 112 乗の計算量が必要とあるが、正誤表にあるように暗号化されたコンテンツ鍵は入手できないため、コンテンツ鍵を特定するには総当たりで最大 2 の 256 乗の計算量が必要である。一方、前述のように W ソフトによって暗号化されたファイルの解読には 2 の 60 乗の計算量が必要である。これらを比較すると、次のように、必要な計算量は 2 の 196 乗倍である。

$$2^{256} \div 2^{60} = 2^{256-60} = 2^{196}$$

(4) 推測が可能なパスワードを破るのに有効なのは辞書攻撃である。辞書攻撃とは、一般的な辞書に載っている英単語や、パスワードに使われそうな文字列が大量に登録されたファイル（辞書ファイル）を用いてログインを試行する手法である。

(5) 利用者 ID とパスワードによる認証だけで脆弱であり、それを解決するために変更する方式であるから、該当するのは多要素認証である。利用者の認証に用いられる要素には、生体情報（指紋、顔等）、所有物（IC カード、スマートフォン等）、記憶や秘密（パスワード、暗証番号等）があるが、これらの複数の要素を組み合わせて認証を行う方式が多要素認証である。

●設問３

［試験センターによる解答例］
利用者がファイルを開いたとき、画面をキャプチャし、攻撃者に送信する動作（35 字）

＜解説＞
PC がマルウェアに感染すると、利用者が設計秘密ファイルにアクセスする際の ID とパスワードの入力内容が盗まれたり、ファイルを開いたときの画面をキャプチャされたりして、それらの情報が攻撃者に送信される可能性がある。前者については、送信されたとしても多要素認証によって不正なログインを防ぐことができるが、後者については防ぐことはできず、設計秘密の内容を攻撃者に不正に取得されてしまうことになる。

＜問３＞ PC のマルウェア対策

●設問１

［試験センターによる解答例］
(1) LAN から切り離す。（10 字）

(2) ディスクイメージ（8 字）

(3) a：最新のマルウェア定義ファイルを保存した DVD-R の使用（27 字）
b：マルウェア定義ファイルの更新（14 字）
c：マルウェア対策ソフトの画面の操作（16 字）

(4) Q 社内の全ての PC 及びサーバからのアクセス（21 字）

＜解説＞

(1) PC にマルウェアが感染した場合に感染拡大防止のために行う初動対応は、当該 PC を LAN から切り離すことである。

(2) ディジタルフォレンジックスによる調査は次のような手順で行う。

・対象 PC を隔離する等して保全する。
・対象 PC のディスクイメージを取得する。
・取得したディスクイメージを調査用のディスク上にコピーし、調査を実施する。

ディスクイメージとは、PC のハードディスク等の記憶装置の中身を物理的に完全にコピーしたものである。

(3) フルスキャンを実施する前にマルウェア定義ファイルを最新の状態に更新する必要があるが、PC-G は LAN から切り離されているため、マルウェア対策ソフトの画面の操作では更新できない。そのため、最新のマルウェア定義ファイルが保存された DVD-R を使用して更新する必要がある。一方、LAN に接続されている PC については、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最新の状態に更新する。
したがって、[a] には「最新のマルウェア定義ファイルを保存した DVD-R の使用」、[b] には「マルウェア定義ファイルの更新」、[c] には「マルウェア対策ソフトの画面の操作」が入る。

(4) 図 3 の(4)にあるように、プロキシサーバのアクセスログについては、PC-G からのアクセスを対象とした調査しか行われていない。PC-G 以外の Q 社内の PC やサーバからも C リストの URL にアクセスが行われた可能性があるため、Q 社内の全ての PC 及びサーバからのアクセスを対象として調査を行う必要がある。

●設問２

［試験センターによる解答例］
(1) 項番：3
送信元：総務部 LAN，営業部 LAN

項番：4
送信元：技術部 LAN

(2) d：V 社配付サイトの URL
e：全て

＜解説＞

(1) 表 2 の FW フィルタリングルールで F サーバ 1 と F サーバ 2 への通信に関するルールは項番 3, 4 であるため、これらが変更対象となる。現状では項番 3, 4 ともに「送信元が総務部 LAN, 営業部 LAN, 技術部 LAN」となっているが、項番 3 については送信元を「総務部 LAN, 営業部 LAN」に変更し、項番 4 については送信元を「技術部 LAN」に変更する。

(2) 表 1 の注記 2 にあるように、現状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ため、表 2 の項番 1, 2 により、サーバ LAN からは、プロキシサーバを経由し、V 社拒否リストに記載された URL 以外のインターネット上のサイトに広く HTTP, HTTPS 通信が可能である。しかし本来は問題文にあるように、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ため、UF ルールで V 社配付サイトへの通信のみを許可するように設定すればよい。したがって、 d には「V 社配付サイトの URL」、 e には「全て」が入る。

●設問３

［試験センターによる解答例］

(1) 登録した実行ファイルがバージョンアップされた場合（24 字）

(2) 登録した実行ファイルのマクロとして実行されるマルウェア（27 字）

＜解説＞

(1) Y ソフトでハッシュ値の登録変更が必要になるのは、元となる実行ファイルの中身に変更が生じたときである。そのため、実行ファイルがバージョンアップされた場合にはハッシュ値の登録変更が必要となる。

(2) Y ソフトで実行を禁止できないマルウェアは、実行ファイル形式ではなく、正規の実行ファイルによって使用される文書ファイル等に寄生する形で存在するタイプである。典型的なものとして、近年大きな被害を出した Emotet のように、MS Word の文書ファイルのマクロとして実行されるマルウェア（「マクロウイルス」とも呼ばれる）などがある。仮に Y ソフトで Emotet の実行を禁止する場合、MS Word 自体の実行を禁止する必要がある。