(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。