■設問3

[試験センターによる解答例]

(1) 運用PCからの接続も拒否するように変更する。(22字)
(2) 運用PCから接続できるURLは，T社標準ソフトのベンダのサイトのものだけに制限するように変更する。(49字)

(1) 表1にあるように，Webメールサーバの HTTP 接続拒否機能は，IP アドレス単位で HTTP による接続を拒否することができる機能で，内部システム LAN 上の他のサーバからの接続を拒否している。Web メールサーバは，HTTP を用いて PC の Web ブラウザでメールを送受信できる機能を提供しているが，運用 PC についてはメールの送受信を制限する必要がある。そのため，Web メールサーバの HTTP 接続拒否機能により，運用 PC からの HTTP 接続を拒否するよう設定を変更する。

(2) 表2にあるように，プロキシサーバでは送信元 IP アドレスごとに接続可能な URL を制限するアクセス制限機能があるが，現在は全ての URL への接続を許可している。運用 PC はインターネットの Web 閲覧を制限する必要があるが，問題文の冒頭にあるように，T 社の PC 及びサーバは，プロキシサーバ経由で T 社標準ソフトの各ベンダのサイトに毎月1回自動で接続し，それぞれの脆弱性修正プログラムを適用している。運用 PC についてもこの対応は必要であるため，プロキシサーバのアクセス制限機能を用いて，運用 PC が接続できる URL を，T 社標準ソフトのベンダのサイトのものだけに制限するように変更する。

＜問3＞ LANの分離

■設問1

[試験センターによる解答例]

(1) a：ウ
　　b：エ
(2) c：ア
　　d：ウ
※c，dは順不同。

(1) JIS Q 31000:2010（リスクマネジメント－原則及び指針），JIS Q 31010:2012（リスクマネジメント－リスクアセスメント技法）では，リスクアセスメントを「リスク特定，リスク分析及びリスク評価のプロセス」としている。したがって，［ a ］にはウの「リスク特定」，［ b ］にはエの「リスク評価」が入る。

(2) JIS Q 31000:2010 ではリスクレベルを「結果とその起こりやすさとの組合せ」と定義している。この「結果」とは「リスクが顕在化したときの結果」であり，「起こりやすさ」とは「リスクの起こりやすさ」である。したがって［ c ］，［ d ］には，ア，ウが入る。（順不同）

■設問 2

［試験センターによる解答例］

(1) ファイル転送サーバから研究開発 PC への通信は FW2 で禁止されているから（35 字）
(2) e：利用者 ID（5 字）
f：パスワード（5 字）
g：アップロード用 URL（10 字）
※e，f，g は順不同。
方法：事務 PC の HTTP リクエストを監視する。（20 字）
(3) 研究開発 PC からファイル転送サーバにアクセスして，ファイルをダウンロードする必要があるから（45 字）

(1) ファイル転送サーバに感染したマルウェア α が研究開発 PC が感染を広げるには，FW2 を介して通信を確立させる必要があるが，表 3 にあるように，FW2 では研究開発 PC からファイル転送サーバへの必要な通信のみが許可されており，ファイル転送サーバから研究開発 PC への通信は禁止されている。そのため，A 氏は下線①のように判断したのである。

(2) 図 4 の 1 に「研究開発 PC の Web ブラウザからファイル転送サーバのアップロード用 URL にアクセスし，表示される画面で利用者ごとに異なる利用者 ID 及びパスワードを入力してログインする」とある。また，図 4 の注記に「事務 PC から研究開発 PC へのファイル転送時の操作手順は，図中の研究開発 PC を事務 PC に，事務 PC を研究開発 PC に，それぞれ置き換えて読むものとする」とある。したがって，事務 PC に感染したマルウェア β が不正なファイルをファイル転送サーバにアップロードするには，利用者 ID，

パスワード，アップロード用 URL，の 3 つの情報が必要であり，[e]，[f]，[g]にはこの 3 つの情報が入る。（順不同）

上記の事務 PC からファイル転送サーバへのアクセスは，事務 PC の Web ブラウザからの HTTP 通信で行われているため，事務 PC の HTTP リクエストを監視すれば，ファイル転送サーバにアクセスするために必要な情報を窃取することが可能である。

(3) ファイル転送サーバにアップロードされた不正なファイルが原因となって研究開発 PC が感染するには，N 社の研究開発員が研究開発 PC からファイル転送サーバにアクセスして，当該不正ファイルをダウンロードする必要がある。図 4 の 4 にあるように，ファイル転送サーバからファイルをダウンロードする際には，アップロードされたファイルの一覧を表示し，そこからファイルを選択する。このとき，マルウェアβがアップロードした不正なファイルが一覧に表示されたとしても，N 社の研究開発員が当該ファイルを選択してダウンロードする可能性は低いと考えられる。

■設問 3

［試験センターによる解答例］

h：高い
i：通信経路上に感染活動を遮断する機器が存在しないから（25 字）
j：低い
k：FW2 によって感染活動を遮断できるから（19 字）

表 5 より，研究開発 PC，配信サーバは OS-P を利用しているため，マルウェアγに感染する可能性がある。図 3 中の（あ）に配信サーバを設置した場合には，研究開発 PC と配信サーバの間は L2SW のみとなり，通信経路上にマルウェアγの感染活動を遮断する機器は存在しない。そのため，研究開発 PC から配信サーバに感染が拡大する可能性が高い。

一方，図 3 中の（い）に配信サーバを設置した場合には，研究開発 PC と配信サーバの間は L2SW だけでなく，FW2 がある。FW2 では，必要最小限の通信だけを許可しているため，マルウェアγの感染活動を遮断できると考えられる。したがって，研究開発 PC から配信サーバにマルウェアγの感染が拡大する可能性は低い。

■設問 4

［試験センターによる解答例］

ｉ：上長による承認（7 字）

図 4 の手順 2 にあるように，ファイルをアップロードする際にその正当性を確認する手順はなく，アップロードが完了すると即座にダウンロードが可能となる。そのため，研究開発 PC，事務 PC の双方にマルウェアが感染していた場合には，不正なアップロード，ダウンロードが行われ，インターネットへのファイルの流出に至る可能性がある。これを防ぐには，図 4 の手順 2 の後に上長による承認の手順を追加し，その手順の完了をもってダウンロードが可能となるようにするのが効果的である。