次の問1は必須問題です。必ず解答してください。

問1　マルウェア感染への対応に関する次の記述を読んで，設問1～4に答えよ。

J社は，従業員が100名の商社であり，各種工業製品用の部品・材料を取り扱っている。

J社のPCは，情報システム課で管理しており，業務に必要なソフトウェアをあらかじめインストールして各部署に配布し，社内LANに接続している。

コンピュータウイルスなどのマルウェアの感染を防ぐために，自社の情報セキュリティ規程に沿って，PCとサーバにウイルス対策ソフトを導入し，最新のウイルス定義ファイルとセキュリティパッチを自動的に適用している。サーバ上のファイルは，社内LAN上の共有ディスク装置に定期的にバックアップされている。

また，社内LANに接続されたPCからインターネット上のWebサイトを閲覧するときに，業務上閲覧することが不適切なWebサイトへの接続を制限する［　a　］を導入している。

〔モバイルPCの運用〕

J社には社内でだけ利用するPCの他に，営業課員が社外での営業活動時に携行するモバイルPCが用意され，社内では無線LANによって社内LANに自動的に接続できる。モバイルPCは，利用時以外は所定のキャビネットにおいて施錠管理されている。

モバイルPCには，OSと，業務に必要なソフトウェアだけがインストールされている。外出先で利用する文書ファイルなどは，モバイルPCの持出し時に営業課員が社内のファイルサーバからコピーする。また，モバイルPC利用後は，モバイルPC上にユーザがコピーした又は作成したファイル（以下，ユーザ作成ファイルという）を全て削除してから，所定のキャビネットに返却する。

〔モバイルPCのマルウェア感染〕

ある日，営業課のK君は，取引先での営業活動のために，ファイルサーバから新製品の提案書をモバイルPCにコピーして外出した。外出中に当該モバイルPCで営業日報を作成して，その日は帰宅した。翌日出社し，別の取引先を訪問するために営業情報をファイルサーバからコピーしようと当該モバイルPCを起動したところ，

金銭の支払を要求する警告メッセージが表示された。当該モバイル PC 上のファイルを確認すると，新製品の提案書と営業日報のファイル名の拡張子が特定の文字列に変更されていた。その拡張子を変更前のものに戻してからファイルを開いても，内容は文字化けして，判読できなかった。

K 君は，直ちに上司を通じて，情報システム課の Y 課長にこの状況を報告した。Y 課長は取り急ぎ，当該モバイル PC 本体の無線 LAN 機能を停止させて社内 LAN から切断し，当該モバイル PC にはそれ以上触らず，そのままにしておくよう K 君に指示した。Y 課長は，報告を受けた状況から見て［ b ］型の［ c ］に感染した可能性が高いと判断し，部下で情報セキュリティ担当の S 主任に状況の確認と対策の検討を指示した。

〔情報セキュリティ担当者による状況の確認〕

S 主任は，K 君から当該モバイル PC の直近の利用状況を聞き取った。

S 主任：このモバイル PC の利用状況について教えてください。

K 君：　昨日，営業で訪問した取引先の会議室において，当社が取扱いを始めた新製品のプレゼンテーションに利用しました。取引先では，インターネットを含めネットワーク接続をしていません。その時は特に異常はありませんでした。取引先を出た時には終業時刻を過ぎていたので，そのまま自宅に帰るつもりでした。営業日報だけ当日中に作成しようと，途中で最寄り駅近くの喫茶店に立ち寄って，このモバイル PC を利用しました。喫茶店では公衆無線 LAN でインターネットに接続し，営業日報を電子メール（以下，メールという）で上司に送信しました。

S 主任：何か他に利用しましたか。

K 君：　営業日報のメール送信後に，取引先で質問された情報を調べようと Web サイトを検索していたところ，突然警告メッセージのような画面が表示されました。Web サイトを閲覧中に時々表示される詐欺まがいの広告の類いだろうと思い，メッセージはよく読まずにすぐ Web ブラウザを閉じてモバイル PC をシャットダウンしました。今日，別の取引先との商談に，引き続きこのモバイル PC を利用する予定でしたので，必要なファイルを追加でコピーしようとして，今回の事象に遭遇しました。

S 主任は K 君への聞き取りから，今回のマルウェアはインターネット上の Web サイトから，［ d ］によって当該モバイル PC に感染したものと推測した。

一方，S 主任は，今日，K 君が当該モバイル PC を社内 LAN に接続した時刻以降，社内のネットワークから外部への不審な通信が行われていないこと，①社内の他の PC やサーバに感染被害が拡大していないことを確認した。このことから，S 主任は，今回の被害の影響範囲は K 君が利用した当該モバイル PC だけに限られると判断した。

また，S 主任は，当該モバイル PC 上で変更されたファイル名の拡張子の文字列から，最近報告されたマルウェアの疑いが強いこと，当該マルウェアは最新のウイルス定義ファイルで駆除できることを確認した。S 主任は，今回の一連の状況及び調査結果をまとめ，Y 課長に報告した。

〔モバイル PC のセキュリティ管理上の問題点〕

モバイル PC には，社内の PC と同じウイルス対策ソフトが導入されている。しかし，ウイルス定義ファイルは，社内 LAN 接続中に手動又は不特定の時刻に自動で更新される仕様なので，モバイル PC の利用時にウイルス定義ファイルが最新になっていない可能性がある。

J 社の情報セキュリティ規程では，モバイル PC の利用時には，セキュリティパッチとウイルス定義ファイルを最新のものに更新するよう定めていた。しかし，今回，K 君はウイルス定義ファイルが最新になっていることの確認を怠ってしまった。

その後，J 社では，モバイル PC の利用に関する情報セキュリティ規程を遵守させるために，モバイル PC の持出し時の手順にチェックリストによる点検を新たに追加した。

〔マルウェアに感染した場合に備えた対策の検討〕

Y 課長は，S 主任からの報告を受け，今回のようなマルウェアがモバイル PC だけでなく，社内の PC に感染した場合にも備える必要があると感じた。マルウェア感染の被害を最小限にとどめる対策として，社内の PC 上のファイルのバックアップについて，S 主任に検討を指示した。

S 主任は，PC 上のユーザ作成ファイルは当該 PC には保存せず，ファイルサーバ

に保存するよう情報セキュリティ規程を改定し，さらに②ファイルサーバ上のファイルのバックアップについても，マルウェアに感染した場合に備えた対策を講じるための検討に着手した。

設問１　本文中の［ a ］～［ d ］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　URL フィルタリング　　イ　スパイウェア　　ウ　スパム対策
エ　端末ロック　　オ　ドライブバイダウンロード
カ　トロイの木馬　　キ　標的型攻撃　　ク　ファイル暗号化
ケ　フィッシング　　コ　水飲み場型攻撃　　サ　ランサムウェア

設問２　本文中の下線①について，マルウェアの感染被害が拡大していないことを，どのような方法で確認したのか。40 字以内で述べよ。

設問３　〔モバイル PC のセキュリティ管理上の問題点〕について，(1)，(2) に答えよ。

(1) モバイル PC のウイルス定義ファイル更新を確認する観点から，持出し時に確認すべき事項を 30 字以内で述べよ。

(2) モバイル PC のマルウェア感染の対策として，適切でないものはどれか。解答群の中から選び，記号で答えよ。

解答群

ア　情報セキュリティ規程の遵守を徹底するよう，従業員を再教育する。
イ　モバイル PC のウイルス対策ソフトを，インターネットからも直接，ウイルス定義ファイルを更新できる仕様の製品に切り替える。
ウ　モバイル PC は社内 LAN に一切接続せず，必要なファイルのコピーは USB メモリなど可搬性がある記憶媒体を介して行う。
エ　モバイル PC を，SIM カードによるデータ通信対応の端末に切り替え，公衆無線 LAN の利用は禁止する。

設問4　本文中の下線②について，(1)，(2)に答えよ。

(1) S主任が，検討に着手したファイルサーバ上のファイルのバックアップについて，マルウェアに感染した場合に備えた対策を必要と感じたのはなぜか。適切なものを解答群の中から選び，記号で答えよ。

解答群

ア　PC及びファイルサーバのハードディスクに対して暗号化を施していないから

イ　ファイルサーバのディスク使用量の増加に伴い，バックアップに要する時間が延びるおそれがあるから

ウ　ファイルサーバのバックアップ先にも，マルウェア感染の影響が及ぶおそれがあるから

エ　マルウェアの感染で，PC及びファイルサーバのシステム自体が破壊されるおそれがあるから

(2) バックアップに用いる共有ディスク装置の運用方法について，マルウェアの感染に備えた対策を，30字以内で述べよ。