問9　PCのマルウェア対策に関する次の記述を読んで，設問1～4に答えよ。

A社は，オフィス向け文具の開発，販売を手掛ける中堅企業であり，本社には企画部，開発部，営業部がある。全ての本社社員はデスクトップPCを1台ずつ所持している。さらに，営業部の社員は社外持出しのためにノートPCを1台ずつ所持している。

本社内のデスクトップPCは，社内LANに接続され，電子メール（以下，メールという）の送受信と保管，Web閲覧，ファイル共有，文書の作成・保管などに利用されている。

ノートPCは，社外に持ち出した場合にだけ使用され，メールの送受信と保管，Web閲覧，文書の作成・保管などに利用されている。

〔デスクトップPC及びノートPCにおけるマルウェア対策〕

A社では，デスクトップPC及びノートPCにおいて，次のマルウェア対策を実施している。

- デスクトップPC及びノートPCでは，OSやアプリケーションソフトウェアのアップデートを自動的に実施する設定を推奨している。
- デスクトップPC及びノートPCにウイルス対策ソフトウェアを導入し，ウイルス定義ファイルを毎日更新する設定を推奨している。
- メールサーバではメールの添付ファイルのウイルスチェックを行うとともに，①スパムメールをメールサーバ上で自動的に判定し，スパムメールと判定されたメールをメールサーバ上で隔離している。
- 社内LANからインターネット上のWebサイトを閲覧する際には，プロキシサーバを介する。②プロキシサーバでは，問題のあるWebサイトを登録しておくことによって，アクセス可能なWebサイトを制限するフィルタリング方式を利用している。問題のあるWebサイトのリストは，プロキシサーバ上でアクセス制限を行うソフトウェアのベンダから定期的に提供を受けている。

〔ノートPC持出し時の使用状況〕

営業部の社員がノートPCを社外に持ち出すときの使用状況は，次のとおりである。

・インターネットへアクセスするために，USB 接続の通信機器を使用している。
・メールアカウントは，A 社が契約している ISP のものを使用し，インターネット経由で利用している。
・ノート PC で作成した各種文書は，ファイルの暗号化を行い，ISP のメールアカウントを用いて，メールに添付して自社宛てに送信している。
・主に商品の紹介や在庫状況の確認のために，自社の Web サイトを参照している。また，顧客の Web サイトを参照して情報収集も行っている。

〔ウイルス感染の状況〕

A 社では，最近になって，デスクトップ PC やノート PC のウイルス感染が 3 件発生した。それぞれのウイルス感染の状況は，表 1 のとおりであった。

表 1　A 社におけるウイルス感染の状況

	利用部署	感染ルート	感染の状況
事例 1	開発部	USB メモリ	外注先から納品された USB メモリにウイルスが含まれており，デスクトップ PC が 1 台感染した。他のデスクトップ PC でもその USB メモリを使ったところ，ウイルスが検知された。感染したデスクトップ PC では，ウイルス定義ファイルが最新でなかった。
事例 2	企画部	メール	③打合せの日程確認が取引先担当者を詐称したメールによって送付された。そのメールに添付されていたファイルを開いたところ，デスクトップ PC が 1 台感染した。感染したデスクトップ PC では，ウイルス定義ファイルは最新であった。④アプリケーションソフトウェアのセキュリティパッチが提供される前のぜい弱性を狙ったウイルスであった。
事例 3	営業部	Web 閲覧	社外に持ち出したノート PC からインターネット上の Web サイトで情報検索をしていたところ，初めて閲覧した Web サイトに埋め込まれたマルウェアによって，ノート PC が 1 台感染した。感染したノート PC では，OS の最新のセキュリティパッチが適用されていなかった。

〔ウイルス感染に対する対策の検討〕

企画部の B 部長は，発生したウイルス感染と同様の感染が再発するのを防ぐ対策の検討を，C 君に指示した。C 君は，各事例を分析し，ウイルス感染のリスクをできるだけ減らすために，デスクトップ PC 及びノート PC における新たなマルウェア対策案を検討し，表 2 にまとめた。

表2　デスクトップPC及びノートPCにおける新たなマルウェア対策案

対象	新たなマルウェア対策案
デスクトップPC及びノートPC	【対策1】ウイルス定義ファイルの毎日の更新を強制的に実施する管理プログラムを導入する。 【対策2】OSやアプリケーションソフトウェアのセキュリティパッチを強制的に適用する設定を選択する。 【対策3】不審なメールの添付ファイルは安易に開かず，メールの送信者に確認し，そのようなメールが届いたことを社内に周知する，というルールを社内で徹底する。 【対策4】 a 【対策5】 b
ノートPC	【対策6】社外に持ち出す前に，ウイルス定義ファイルの更新や，OSやアプリケーションソフトウェアのセキュリティパッチの適用を確認することを義務付ける。 【対策7】社外に持ち出したノートPCから社内LANにVPN経由でアクセスできるようにして，Webサイトへのアクセスを社内LAN経由だけに制限する。

〔検討会議における指摘と対策〕

C君がまとめたマルウェア対策案に基づき，A社内で検討会議を開催したところ，表2中の【対策7】について，“社内LANにVPN経由でアクセスさせる方式は，導入までにコストと時間を要するので，短時間で対応可能な代替策を検討すべきである”との意見があった。

C君は，【対策7】の代替策として，アクセス可能なWebサイトを制限する仕組みをノートPCに導入する方法を提案することにした。ノートPCを社外で使用する場合にアクセス可能なWebサイトを制限する方式には，社内LAN上のデスクトップPC向けにプロキシサーバで実施していた方式ではなく，⑤あらかじめ指定されたWebサイト（自社のWebサイトや顧客のWebサイトなど）だけをアクセス可能にする方式を採用し，ノートPC上の常駐型ソフトウェアで実現することにした。

さらに，検討会議では“万が一ウイルスに感染してしまった場合の事後対策が不足している”との意見があったので，C君は次の項目について検討することにした。

(1)　感染したことを社内のインシデント対応部門に連絡し，社内周知によって感染の拡大を防ぐルールの策定と周知

(2)　感染したことによって情報漏えいが発生した場合の対応ルールの策定

(3) ⑥感染したことによってデスクトップ PC やノート PC が使用不能となった場合に備えるための対策の策定

設問 1 〔デスクトップ PC 及びノート PC におけるマルウェア対策〕について，(1)，(2)に答えよ。

(1) 本文中の下線①を実施した際に，メールの送信元や内容などで自動的に判定する基準が適切でないと，利用者がスパムメールを大量に受信してしまうことがある。その他に発生するおそれがある問題を 30 字以内で述べよ。

(2) 本文中の下線②のように，問題のある Web サイトを登録することによってアクセス可能な Web サイトを制限するフィルタリング方式の名称を，カタカナ 10 字以内で答えよ。

設問 2 〔ウイルス感染の状況〕について，表 1 中の下線③及び下線④のサイバー攻撃手法の名称を解答群の中から選び，それぞれ記号で答えよ。

解答群

ア DDoS 攻撃　　イ SQL インジェクション

ウ カミンスキーアタック　　エ 辞書攻撃

オ ゼロデイ攻撃　　カ トロイの木馬

キ 標的型攻撃

設問 3 〔ウイルス感染に対する対策の検討〕について，(1)，(2)に答えよ。

(1) USB メモリの利用に関する対策として，表 2 中の [a]，[b] 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 USB メモリに格納するファイルは全て暗号化する。

イ USB メモリの利用時にウイルススキャンを強制的に実施する仕組みとする。

ウ USB メモリは，マルウェア対策が実施済みで利用履歴が管理された専用のデスクトップ PC だけで利用可能とする。

エ 暗号化機能付きの USB メモリだけを利用可能とする。

オ 社外との情報の交換には自社保有の USB メモリだけを利用可能とする。

(2) 表2中の【対策7】によって期待される，Webサイト閲覧時の効果を35字以内で述べよ。

設問4 〔検討会議における指摘と対策〕について，(1)，(2)に答えよ。

(1) 本文中の下線⑤の方式をA社のノートPCで実施した場合でも，Web閲覧によってノートPCがウイルスに感染する可能性がある。それはどのような攻撃があった場合か。35字以内で述べよ。

(2) 本文中の下線⑥について，デスクトップPCやノートPCの利用者が実施可能な対策は何か。30字以内で述べよ。