問1　ランサムウェアへの対策に関する次の記述を読んで，設問1～4に答えよ。

B社は，従業員数300名の建築資材販売会社であり，本社，営業店10か所の他に倉庫がある。本社，各営業店及び倉庫のネットワークはIP-VPNで接続されており，インターネットとの接続は本社に集約されている。本社と営業店では，それぞれ，本社用PCと営業用PCから情報共有サーバ（以下，Gサーバという）を利用し，Windowsのファイル共有機能を使って資料を共有している。本社用PC及び営業用PCでは，一般利用者権限でログオンすると，自動的にGサーバへもその権限でログオンされ，Gサーバ上の共有フォルダが各PCのGドライブとして自動的に割り当てられる。Gサーバ上の共有フォルダの利用者データ，本社用PCの利用者データ及び営業用PCの利用者データは，それぞれ，各コンピュータのローカルディスク上に設けられた一般利用者権限ではアクセスできない領域に1時間に1回，毎時0分に開始されるジョブによって，バックアップされる。ジョブのログには，バックアップの開始と終了の時刻，総ファイル数，ジョブ実行結果などが記録される。

B社は，販売及び在庫管理を行うソフトウェアを独自に開発し利用している。受注から出荷までの業務を管理するWebアプリケーションソフトウェア（以下，業務APという）は，販売及び在庫管理用のWindowsサーバ（以下，Dサーバという）上で稼働している。B社の全てのPCは，ログオン時に，Dサーバへも一般利用者権限で自動的にログオンされ，Dサーバ上の共有フォルダがWindowsのファイル共有機能を使って各PCのDドライブとして自動的に割り当てられる。出荷業務は，倉庫に設置された作業用PCに，無線ハンディターミナル（以下，HTという）を接続して行う。各PCで用いるB社のWindowsアプリケーション（以下，Aアプリという）は，業務APにHTTP over TLSで接続する機能，及び出荷指示情報が記載されたファイル（以下，出荷指示ファイルという）を読み書きする機能をもっている。

B社のシステム構成を図1に，受注から出荷までの業務の流れを図2に示す。

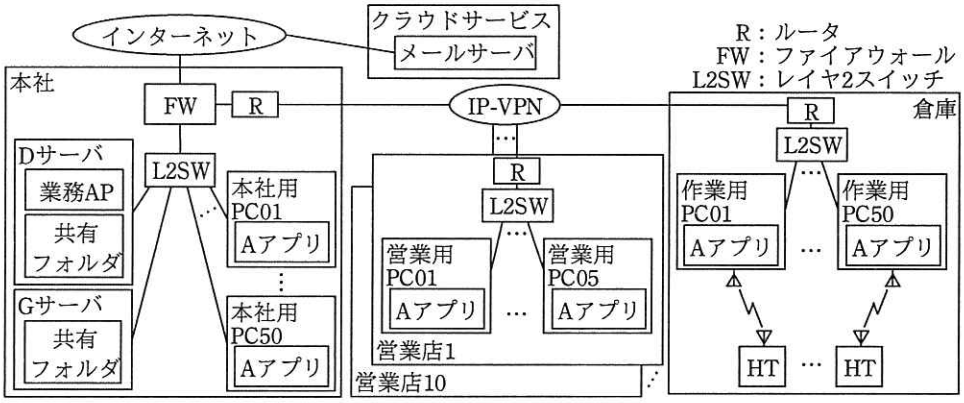

図１　B 社のシステム構成

1. 営業担当者が，自分の利用者 ID で営業用 PC にログオンし，A アプリを使って業務 AP に接続し，受注情報を登録する。
2. 本社スタッフが，自分の利用者 ID で本社用 PC にログオンし，A アプリを使って業務 AP に接続し，受注情報を基に出荷指示情報を登録する。
3. 業務 AP では，出荷指示情報が登録されると D サーバ上の共有フォルダに，出荷指示 1 件につき，CSV 形式による出荷指示ファイルを 1 ファイルとして出力する。全ての出荷指示ファイルは，出荷担当者が内容の確認と更新をすることができる。
4. 出荷担当者が，自分の利用者 ID で作業用 PC にログオンする。
5. 出荷担当者が，作業用 PC に HT を接続し，A アプリを使って D ドライブ上の自分が担当する出荷指示ファイルを“出荷処理中”にステータス更新した上で，出荷指示情報を HT に取り込む。倉庫内の商品に貼ってあるバーコードを HT で読み取りながら出荷を行う。
6. 出荷担当者は，出荷が完了すると，A アプリを使って D ドライブの該当する出荷指示ファイルを“出荷完了”にステータス更新する。
7. 営業担当者及び本社スタッフが，A アプリを使って D ドライブ上の出荷指示ファイルを閲覧し，最新の出荷状況を確認する。ただし，内容を確認するだけで更新はしない。

図２　受注から出荷までの業務の流れ

〔セキュリティインシデントの発生〕

ある日の 9:50 に，出荷担当者の V さんから，IT システム担当者の L 君に A アプリの障害の連絡が入った。L 君が D サーバ上の共有フォルダを確認したところ，出荷指示ファイルが破損しており，A アプリで読込みエラーが発生していた。L 君は，原因究明よりも，業務の再開を優先するため，業務 AP の管理機能を使って出荷指示ファイルを再出力して復旧させた。このとき，L 君は，①破損した出荷指示ファイルを削除せず，別のフォルダに移動しておいた。後に，このファイルが，調査に役立った。

復旧させた直後，10:30 に，営業担当者の S さんから L 君に，暗号化されたファイ

ルを取り戻したければ手順に従うよう指示する脅迫文が，営業用 PC05 のデスクトップ画面に表示されているという連絡が入った。また，営業用 PC05 で一部のファイルを開くことができなくなっていた。L 君は，営業用 PC05 がマルウェアに感染したと判断し，営業用 PC05 をネットワークから切り離すよう S さんに指示した。

L 君は，D サーバの出荷指示ファイルも営業用 PC05 と同じように開くことができなくなっていたことから，D サーバも同じマルウェアに感染した可能性があると考え，一連の事象を上司に報告した。上司と相談した結果，業務を一時停止し，D サーバをネットワークから切り離し，従業員に注意喚起をした後，セキュリティ専門会社 U 社の J 氏に協力を依頼して，調査を行うことにした。

〔セキュリティインシデントの調査〕

L 君と J 氏は，感染経路と影響範囲を特定するために，営業用 PC05 と D サーバからログファイルやメモリダンプなどを収集して，表 1 のタイムラインを作成した。

表 1　セキュリティインシデントのタイムライン

No	時刻	事象	対象機器
1	7:50	PC が起動された。	営業用 PC05
2	7:51	営業利用者 05 でログオンされた。	営業用 PC05
3	7:51	営業用 PC05 から営業利用者 05 でログオンされた。	D サーバ
4	8:25	A アプリが実行された。	営業用 PC05
5	8:29	メール閲覧ソフトが実行された。	営業用 PC05
6	8:30	invoice.fdp.exe が実行された。	営業用 PC05
7	8:32	提案書.docx ファイルが暗号化された。	営業用 PC05
以降，9:11 までファイルの暗号化が繰り返された。			営業用 PC05
8	9:11	出荷指示_01_00001.csv ファイルが暗号化された。	D サーバ
以降，9:40 までファイルの暗号化が繰り返された。			D サーバ
9	10:10	脅迫文のファイルが作成され，画面に表示された。	営業用 PC05

受信した電子メールを調査したところ，PDF ファイルに偽装したマルウェアが添

付されていた。ファイル名に Unicode 制御文字の [a] が使われていたので，実際のファイル名は invoice.fdp.exe であるが，表示上は invoice.exe.pdf となっていた。S さんは PDF ファイルだと思って添付ファイルを開いたとのことで，開いたときにマルウェアのプログラムが実行されたと考えられた。差出人は B 社従業員になっていたが，メールヘッダの [b] フィールドで，経由したメールサーバを調べたところ，社外から送信されていたことが分かった。

S さんに割り当てられている営業利用者 05 に与えられているのは，一般利用者権限なので，営業用 PC05 では，OS のシステムファイルは暗号化されず，S さんが作成したファイルだけが暗号化されていた。L 君は，管理者権限を使って営業用 PC05 にログオンし，マルウェアを除去した上で，②複数世代のバックアップデータの中から，暗号化される直前の世代のバックアップデータを選択し，それを使ってファイルを復元した。

次は，マルウェアに関する，L 君と J 氏の会話である。

L 君：営業用 PC05 が感染したマルウェアはどのようなものなのでしょうか。

J 氏：今回のマルウェアは，ランサムウェア X と呼ばれるものです。ランサムウェア X は，アクセス可能なドライブをドライブレターのアルファベット順に探し，見つけたドライブ内のファイルを暗号化して上書き保存します。内蔵ドライブ，外付けドライブ，ネットワークドライブが対象です。暗号化の対象となるファイルは，文書ファイルなど約 60 種類の拡張子をもつファイルです。対象となるファイルを全て暗号化した後で，脅迫文を画面に表示します。

L 君：ファイルが暗号化されていたので，A アプリで読込みエラーが発生したわけですね。しかし，D サーバは，どのようにして感染したのでしょうか。

J 氏：ランサムウェア X によって，③D サーバ上のファイルが暗号化されたと考えられますが，D サーバ自体が感染した形跡はありません。

L 君：G サーバ上のファイルへの影響はどうでしょうか。

J 氏：D サーバ上のファイルの暗号化が完了した後で，G サーバ上のファイルを暗号化している可能性があるので調査が必要です。

G サーバを調査したところ，共有フォルダのファイルが暗号化されていることが分

かった。しかし，G サーバ上に取得しているバックアップデータを使って，ファイルを復元することができたので，大きな影響はなかった。

〔被害拡大防止策の実施〕

L 君は，PC がランサムウェアに感染した場合に備えて，サーバへの被害を最小限にする対策を講じることにした。D サーバ上の出荷指示ファイルを格納しているフォルダのアクセス権限が必要最小限になるよう，表 2 のとおりに見直しを行った。

表 2　D サーバ上の出荷指示ファイルを格納しているフォルダのアクセス権限設定（抜粋）

利用者のグループ	見直し前		見直し後	
	読み	書き	読み	書き
出荷担当者グループ	可	可	c	d
営業担当者グループ	可	可	e	f
本社スタッフグループ	可	可	g	h

L 君は，G サーバについても，ファイルの被害が最小限になるように，G サーバ上の共有フォルダのアクセス権限を見直した。

L 君は，ランサムウェアによって暗号化されたファイルを，バックアップから復元する以外に元に戻す方法はないか J 氏に質問した。J 氏によると，ランサムウェアには，ファイルの暗号化に共通鍵暗号だけを使っているタイプと，共通鍵暗号と公開鍵暗号を組み合わせて使っているタイプが発見されている。それぞれファイルを復号可能なケースが報告されているとのことであった。共通鍵暗号だけを使うタイプでは，ランサムウェアのプログラム内にその鍵がハードコードされていれば，ランサムウェアの検体を解析することによって，その鍵を入手してファイルを復号できる可能性がある。一方，共通鍵暗号と公開鍵暗号を組み合わせて使うタイプでは，PC のメモリ上に一時的に作成する共通鍵で対象ファイルを暗号化した後，その共通鍵をプログラム内にハードコードされた公開鍵で暗号化した上で，メモリ上からは共通鍵を消去するので，④このタイプでは，検体を解析しても，ファイルを復号することは難しい。ただし，ランサムウェア X の場合，暗号化に使用した共通鍵をメモリ上から消去しないため，⑤PC をハイバネーション機能によって休止状態で保管しておくことによって，セキュリティベンダから復号ツールが提供されたときに，

復号できる場合があるとのことであった。

L 君は，ランサムウェアに感染した場合の対応手順やツールの整備を上司に進言した。

数日後，J 氏から，OS の新たな脆弱性を悪用する新たなランサムウェア Y が発見されたので，至急，セキュリティパッチ P を適用した方がよいという連絡があった。L 君が確認したところ，B 社のサーバと PC に影響する脆弱性であることが分かった。ランサムウェア Y は，⑥ファイルを暗号化するとともに，他のサーバや PC の OS の脆弱性を悪用し，管理者権限で次々と感染を広めるとのことであった。

L 君は，ランサムウェア Y に対処するために，全てのサーバと PC にセキュリティパッチ P を適用するとともに，セキュリティパッチ適用に関する運用の見直しを検討することにした。

設問 1　本文中の下線①のファイルについて，タイムラインを作成する際に用いたタイムスタンプ情報を解答群の中から選び，記号で答えよ。

解答群

ア　アクセス日時　　イ　更新日時

ウ　削除日時　　エ　作成日時

設問 2　〔セキュリティインシデントの調査〕について，(1)～(4)に答えよ。

(1)　本文中の [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　BOM　　イ　Content-Type　　ウ　CRLF

エ　Received　　オ　RLO　　カ　X-Mailer

(2)　本文中の下線②について，復元に利用するバックアップデータを選択する際，感染開始時刻と，何の時刻を比較すべきか。15 字以内で答えよ。

(3)　本文中の下線③について，感染していない D サーバも，ランサムウェア X によってファイルが暗号化された。その原因となる，営業用 PC の設定とランサムウェア X の特徴を，それぞれ 35 字以内で述べよ。

(4)　ランサムウェア X が起動した直後に感染を検知し，営業用 PC05 をネットワークから切り離していれば，今回の被害を一部防ぐことができたと考えら

れる。どのような被害を防ぐことができたか。25 字以内で述べよ。

設問３　〔被害拡大防止策の実施〕について，(1)～(3)に答えよ。

(1)　表 2 中の［　c　］～［　h　］に入れる適切なアクセス権限を，業務要件を踏まえて，可又は不可で答えよ。

(2)　本文中の下線④について，検体を解析してもファイルの復号が困難である理由を，30 字以内で述べよ。

(3)　本文中の下線⑤のように，PC を休止状態で保管しておけばファイルを復号できる可能性があるが，シャットダウンしてしまうとその可能性が低くなる。可能性が低くなる理由を，ランサムウェア X の動作を踏まえて 35 字以内で述べよ。

設問４　本文中の下線⑥について，セキュリティパッチ P を適用せずに放置した場合，営業用 PC がランサムウェア Y に感染すると，他のサーバや PC に感染が広がり，甚大な被害が生じるおそれがある。G サーバにおいて，ランサムウェア X では起きないが，ランサムウェア Y では起きる被害を，40 字以内で述べよ。