全問が必須問題です。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1～3に答えよ。

T社は従業員数200名の建築資材商社であり，本社と二つの営業所の3拠点がある。このうち，Q営業所には，業務用PC（以下，PCという）30台と，NAS 1台がある。

PCは本社の情報システム課が管理しており，PCにインストールされているウイルス対策ソフトは定義ファイルを自動的に更新するように設定されている。

NASは，Q営業所の営業課と総務課が共用しており，課ごとにデータを共有しているフォルダ（以下，共有フォルダという）と，各個人に割り当てられたフォルダ（以下，個人フォルダという）がある。個人フォルダの利用方法についての明確な取決めはないが，PCのデータの一部を個人フォルダに複製して利用している者が多い。

Q営業所と本社はVPNで接続されており，営業所員は本社にある業務サーバ及びメールサーバにPCからアクセスして，受発注や出荷などの業務を行っている。

なお，本社には本社の従業員が利用できるファイルサーバが設置されているが，ディスクの容量に制約があり，各営業所からは利用できない。

T社には，本社の各部及び各課の責任者，並びに各営業所長をメンバとする情報セキュリティ委員会が設置されており，総務担当役員が最高情報セキュリティ責任者（以下，CISOという）に任命されている。また，情報セキュリティインシデント（以下，インシデントという）対応については，インシデント対応責任者として本社の情報システム課長が任命されている。さらに，本社と各営業所では，情報セキュリティ責任者と情報セキュリティリーダがそれぞれ任命されている。Q営業所の情報セキュリティ責任者はK所長，情報セキュリティリーダは，総務課のA課長である。

〔マルウェア感染〕

ある土曜日の午前10時過ぎ，自宅にいたA課長は，営業課のBさんからの電話を受けた。休日出勤していたBさんによると，Bさんの PC（以下，B-PCという）を起動して電子メール（以下，メールという）を確認するうちに，取引先からの出荷通知メールだと思ったメールの添付ファイルをクリックしたという。ところが，その後，画面に見慣れないメッセージが表示され，B-PCの中のファイルや，Bさんの個人フォルダ内のファイルの拡張子が変更されてしまい，普段利用しているソフトウェアで開くことができなくなったという。これらのファイルには，Bさんが手掛けている重

要プロジェクトに関する，顧客から送付された図面，関連社内資料，建築現場を撮影した静止画データなどが含まれていた。そこで，B さんは図 1 に示す T 社の情報セキュリティポリシ（以下，ポリシという）に従って A 課長に連絡したとのことであった。

A 課長は，B-PC にそれ以上触らずそのままにしておくよう B さんに伝え，取り急ぎ出社することにした。

8. インシデントへの対応

(1) 事象の発見と報告

当社の情報資産についてマルウェア感染，情報漏えいなどが疑われる事象を発見した従業員は，所属する拠点の情報セキュリティリーダに速やかに事象を報告する。報告を受けた情報セキュリティリーダは，速やかに事象を確認し，事象を当該拠点の情報セキュリティ責任者及びインシデント対応責任者（不在時は情報システム課員）に報告する。情報セキュリティ責任者は，情報資産の機密性，完全性，可用性に関する重大な被害が発生する可能性があると判断した場合には，インシデントの発生を宣言する。

(2) 被害拡大の防止

情報セキュリティリーダは，当該インシデントに係る被害の拡大を防止するための対策を当該拠点の従業員に指示する。

(3) 被害状況の把握，原因の特定及び影響範囲の調査

情報セキュリティリーダは，インシデント対応責任者と協力して，被害状況の把握，原因の特定及び影響範囲の調査を行う。

(4) システムの復旧

情報セキュリティリーダは，インシデント対応責任者と協力して，特定された原因の除去と，システムの復旧に努める。

(5) 再発防止策の実施

情報セキュリティリーダは，インシデント対応責任者とともにインシデントの再発防止策を検討し，実施する。

図 1　ポリシ（抜粋）

A 課長が Q 営業所に到着して B-PC を確認したところ，画面にはファイルを復元するための金銭を要求するメッセージと，支払の手順が表示されていた。A 課長は，B-PC がマルウェアに感染したと判断し，K 所長に連絡して，状況を報告した。この報告を受けた K 所長は，インシデントの発生を宣言した。また，B さんは，A 課長の指示に従って B-PC と NAS から LAN ケーブルを抜いた。

さらに，A 課長が B さんに，他に連絡した先があるかを尋ねたところ，A 課長以外にはまだ連絡していないとのことであった。そこで，A 課長はインシデント対応責任者である情報システム課長に連絡したところ，情報システム課で情報セキュリティ

を主に担当しているS係長に対応させると言われた。そこで，A課長はS係長に連絡し，現在の状況を説明した。

S係長によると，状況から見て［　a　］と呼ばれる種類のマルウェアに感染した可能性が高く，①この種類のマルウェアがもつ二つの特徴が現れているとのことであった。A課長はS係長に，今後の対応への協力と当該マルウェアに関する情報収集を依頼し，S係長は了承した。その後，A課長が状況の調査を更に進めていたところ，昼過ぎにK所長がQ営業所に到着したので，A課長はその時点までの調査結果をK所長に説明した。調査結果を図2に示す。

- B-PC上のファイルと，B-PCから個人フォルダに複製したファイルがマルウェアによって暗号化されており，開くことができない状態になっていた。一方，Bさんは，顧客から送付されたデータを営業課の共有フォルダに複製していたが，そのデータに異常は見られなかった。
- B-PCに表示されたメッセージによると，BさんのファイルはAESとRSAの二つの暗号アルゴリズムを用いて暗号化されており，これが事実だとすると，復号することは極めて困難である。
- ［　a　］によっては，暗号化されたデータを復号できるツールがウイルス対策ソフトベンダなどから提供されている場合もあるが，今回のマルウェアに対応しているツールはない。また，［　a　］によってはOSの機能を用いると暗号化される前のデータがOSの復元領域から復元できる場合もあるが，今回のマルウェアは，OSの復元領域を削除していた。
- 今回のマルウェアは，金銭の受渡しに際して，②攻撃者の身元を特定できなくするための技術を利用している。
- B-PC以外のQ営業所のPCは全てシャットダウンされていた。

図2　調査結果

〔感染後の対応〕

K所長とA課長は，金銭の支払に応じるべきか否かはQ営業所だけで判断できることではないが，それぞれの場合に想定される被害及び費用の項目は一応把握しておきたいと考えた。そこで，“支払った場合にはデータを確実に復元できるが，支払わなかった場合にはデータを復元できない可能性が高い”という前提の下で想定される被害及び費用の項目を，表1のⅠ～Ⅲに分けてリストアップした。

表１　想定される被害及び費用の項目

Ⅰ．支払った場合にだけ，発生する又は発生するおそれがある項目	b
Ⅱ．支払わなかった場合にだけ，発生する又は発生するおそれがある項目	c
Ⅲ．支払っても支払わなくても発生する又は発生するおそれがある項目	（省略）

注記１　項目には，金額のほか，価値の喪失，損失といったものも含まれるものとする。
注記２　Ⅰ，Ⅱ，Ⅲは互いに排他的である。

折よく，当該マルウェアに関する情報収集を行っていた S 係長から，他社での対応事例の報告があった。これを受け，K 所長と A 課長は，表 1 作成時の前提を置かずに③対応について検討することにし，その結果を情報セキュリティ委員会に報告して CISO の判断を仰ぐことにした。

夕方になって，本社で調査を行っていた S 係長から A 課長に連絡があり，今朝のマルウェア感染以降，Q 営業所のネットワークから本社や外部への不審な通信は行われていないことが分かった。また，業務で利用している本社のサーバにも特に異常は見られなかったという。

これまでの調査から，被害は B-PC 及び B さんの個人フォルダ内のファイルだけであったと A 課長は判断し，B さん用の新たな PC を準備するよう S 係長に依頼した。

翌日の日曜日の朝，ウイルス対策ソフトの開発元から新たな定義ファイルが提供され，B-PC が感染していたマルウェアの検知と駆除が可能になった。そこで，その日の午後に T 社の全ての PC，サーバ及び Q 営業所の NAS に対してマルウェアのスキャンを行ったところ，B-PC 以外にマルウェアに感染していたものはなかった。また，暗号化されていた NAS 上のデータに関しては，NAS のデータのバックアップは実施されていなかったものの，NAS の復元領域から一部を復元できることが判明し，業務への影響はある程度抑えることができた。

〔対策の見直し〕

今回のインシデントを受けて，T 社の情報セキュリティ委員会が開催された。A 課長は，CISO から，今回のインシデントに関する問題点は何かと尋ねられた。A 課長は，④データの取扱い及びバックアップに関するルールの内容が不十分であったこと

が問題点であったと回答し，次のことを提案した。

・データの取扱い及びバックアップに関するルールを全面的に見直し，全社的なルールを定めること

・本社のファイルサーバの容量拡大を早急に実施し，全社共通の利用ルールを定め，それに基づいて各営業所からも利用できるようにすること

・営業所での NAS の利用は半年以内に廃止すること

・NAS の利用を暫定的に継続する間は，営業所では⑤今回の種類のマルウェアに感染することによってファイルが暗号化されてしまうという被害に備えたバックアップを実施し，あわせて⑥バックアップ対象のデータの可用性確保のための対策を検討すること

これらの提案は情報セキュリティ委員会で承認された。T 社はマルウェア感染を契機として情報セキュリティの改善を図ることになった。

設問 1　〔マルウェア感染〕について，(1) ～ (3) に答えよ。

(1)　本文中及び図 2 中の [a] に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

a に関する解答群

ア　アドウェア　　イ　キーロガー

ウ　ダウンローダ　　エ　ドロッパ

オ　ランサムウェア　　カ　ルートキット

キ　ワーム

(2) 本文中の下線①について，この種類のマルウェアの特徴を，次の (i) ～ (vii) の中から二つ挙げた組合せはどれか。解答群のうち，最も適切なものを選べ。

(i) OS やアプリケーションソフトウェアの脆弱(ぜい)性が悪用されて感染することが多い点

(ii) Web ページを閲覧するだけで感染することがある点

(iii) 感染経路が暗号化された通信に限定される点

(iv) 感染後，組織内部のデータを収集した上でひそかに外部にデータを送信することが多い点

(v) 端末がロックされたり，ファイルが暗号化されたりすることによって端末やファイルの可用性が失われる点

(vi) マルウェア対策ソフトが導入されていれば感染しない点

(vii) マルウェアに感染した PC の利用者やサーバの管理者に対して脅迫を行う点

解答群

ア (i), (ii)	イ (i), (iii)
ウ (i), (v)	エ (ii), (iii)
オ (ii), (iv)	カ (iii), (v)
キ (iii), (vii)	ク (iv), (vi)
ケ (v), (vi)	コ (v), (vii)

(3) 図 2 中の下線 ② について，当てはまる技術だけを挙げた組合せを，解答群の中から選べ。

解答群

ア Bitcoin，SSL-VPN，Tor

イ Bitcoin，Tor

ウ Bitcoin，ゼロデイ攻撃

エ Bitcoin，ポストペイ式電子マネー

オ SSL-VPN，Tor

カ SSL-VPN，ゼロデイ攻撃

キ SSL-VPN，バックドア，ポストペイ式電子マネー

ク Tor，バックドア，ポストペイ式電子マネー

ケ ゼロデイ攻撃，バックドア

コ ゼロデイ攻撃，バックドア，ポストペイ式電子マネー

設問２　〔感染後の対応〕について，(1)，(2) に答えよ。

(1)　表 1 中の [b]，[c] に入れる字句を，解答群の中から選べ。ここで，次の [項目 1] ～ [項目 5] は，解答群の [項目 1] ～ [項目 5] と対応するものとする。

[項目 1]　攻撃者から要求されている金額

[項目 2]　再発防止に要する金額

[項目 3]　自力でのデータ復元の試みに要する金額

[項目 4]　犯罪を助長したという事実に起因する企業価値の損失

[項目 5]　マルウェアに感染したという事実に起因する企業価値の損失

b，c に関する解答群

ア　[項目 1]，[項目 2]

イ　[項目 1]，[項目 2]，[項目 3]

ウ　[項目 1]，[項目 2]，[項目 4]

エ　[項目 1]，[項目 3]

オ　[項目 1]，[項目 4]

カ　[項目 2]，[項目 4]

キ　[項目 2]，[項目 5]

ク　[項目 3]

ケ　[項目 4]

コ　[項目 5]

(2) 本文中の下線③について，支払に応じるべきではないと情報セキュリティ委員会で報告するとしたら，その理由は何か。次の (i) ～ (iv) のうち，適切なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) 金銭を支払うことによって，自社への更なる攻撃につながり得るから

(ii) 金銭を支払っても，ファイルを復号できる保証がないから

(iii) 外部業者にディジタルフォレンジックスを依頼すれば，暗号化されたデータを確実に復号できるから

(iv) 表 1 において，ⅠとⅡを比較した結果，Ⅰの方が，被害及び費用が小さいから

解答群

ア (i)，(ii)　　イ (i)，(ii)，(iii)

ウ (i)，(ii)，(iv)　　エ (i)，(iii)

オ (i)，(iii)，(iv)　　カ (i)，(iv)

キ (ii)，(iii)　　ク (ii)，(iii)，(iv)

ケ (ii)，(iv)　　コ (iii)，(iv)

設問３ 〔対策の見直し〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線④の直接的な結果として，何が起きたか。解答群の中から二つ選べ。

解答群

ア B-PC の OS の復元領域が削除されたこと

イ T 社の業務サーバ及びメールサーバが VPN で営業所と接続され，受発注や出荷などのデータが送受信されたこと

ウ Q 営業所で NAS のデータのバックアップが実施されなかったこと

エ 業務で利用するデータについて，何を NAS に保存するか，PC に保存するかが人によってまちまちだったこと

(2) 本文中の下線 ⑤ について，次の (i) ～ (iv) のうち，効果があるものだけを全て挙げた組合せを，解答群の中から選べ。

(i) NAS 上の特に重要なフォルダについては，定期的に BD-R にデータを複製し，BD-R は鍵が掛かるキャビネットに保管する。

(ii) NAS に定期的に別途ハードディスクドライブを追加接続してデータをアーカイブし，終了後にハードディスクドライブを取り外して保管する。

(iii) NAS にハードディスクドライブを増設し，RAID5 構成にすることによってデータ自体の冗長性を向上させる。

(iv) NAS にハードディスクドライブを増設して，増設したハードディスクドライブにデータを常時レプリケーションするようにする。

解答群

ア (i)	イ (i), (ii)
ウ (i), (ii), (iv)	エ (i), (iii)
オ (i), (iii), (iv)	カ (ii)
キ (ii), (iv)	ク (iii)
ケ (iii), (iv)	コ (iv)

(3) 本文中の下線 ⑥ について，次の (i) ～ (iv) のうち，効果があるものだけを全て挙げた組合せを，解答群の中から選べ。

(i) バックアップした媒体からデータが正しく復元できるかテストする。

(ii) バックアップした媒体を二つ作成し，一つは営業所に，もう一つは別の安全な場所に保管する。

(iii) バックアップした媒体を再び読み出せないようにしてから廃棄する。

(iv) バックアップする際にデータに暗号化を施す。

解答群

ア (i)	イ (i), (ii)
ウ (i), (ii), (iii)	エ (i), (iv)
オ (ii)	カ (ii), (iii)
キ (ii), (iii), (iv)	ク (ii), (iv)
ケ (iii)	コ (iii), (iv)