問2　マルウェア感染への対処に関する次の記述を読んで，設問1～4に答えよ。

A社は，従業員8,000名の化学素材会社であり，首都圏に本社，地方には六つの支社がある。素材の研究開発に関して古くから産学官連携をリードしてきた。A社は，VPNサーバ及び基幹システムを，ハウジング契約を結んでいるデータセンタ（以下，DCという）内に設置している。A社の電子メール（以下，メールという）は以前，基幹システム内に設置していたメールサーバを利用していたが，現在はクラウド上のWebメールサービス（以下，Bサービスという）を利用している。Bサービスへの移行に伴う通信量の増加によって，DCにある統合脅威管理（以下，UTMという）の処理能力は，ひっ迫している。従業員は，会社から貸与されたPC（以下，業務PCという）を業務に必要なWebアクセスやメール送受信などに利用する。

本社では，働き方の多様性を確保するためにテレワークを推進してきた。テレワークでは，従業員が業務PCを自宅に持ち帰り，自宅のネットワークからVPNサーバを介して，基幹システムや利用者LANにあるリソースにアクセスできる。テレワークでは，Bサービスなどのインターネットへの接続においても，同様にVPNサーバを介する。

図1にA社のネットワーク構成を，表1にその構成要素の説明を示す。

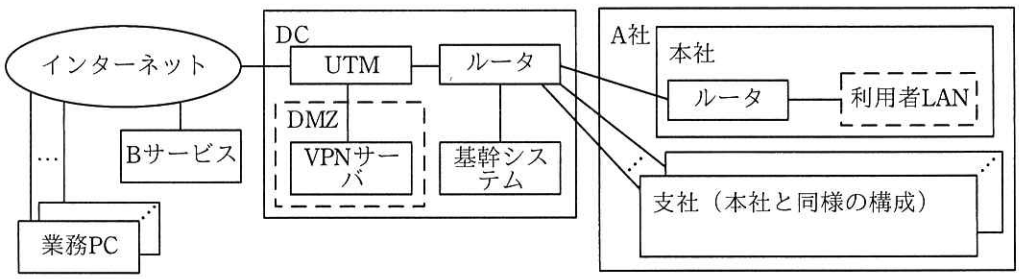

図1　A社のネットワーク構成（概要）

表1　構成要素の説明（概要）

構成要素	説明
基幹システム	共有ファイルサーバ，人事システム，経理システムなどから構成されている。
VPN サーバ	従業員がテレワークに利用する。業務 PC の VPN クライアントソフトウェアを起動すると，VPN サーバとの間に IPsec による通信路が確立する。VPN サーバへの接続の際に 2 要素認証を行う。
UTM	インターネットとの接続境界に設置され，グローバル IP アドレスをもつ。次の機能を備えており，そのうちファイアウォール（以下，FW という）機能と IDS 機能を有効にしている。 FW 機能：ステートフルパケットインスペクション型であり，送信元 IP アドレス，送信元ポート，宛先 IP アドレス，宛先ポートを指定して通信をフィルタリングできる。通信のログを取得する。 IDS 機能：全てのインバウンド通信をチェックし，不審な通信を検知した場合は，システム管理者に通知する。 DNS シンクホール機能：DNS クエリをチェックし，危険リストに登録されている FQDN の場合は，正規の名前解決を行わずに A 社があらかじめ用意した IP アドレスを応答する。危険リストは，日次で自動更新される。
利用者 LAN	従業員の業務 PC やネットワークプリンタといった OA 機器が設置されている。部ごとにセグメントを分けているが，本社と支社間も含めてセグメント間でアクセス制限はしていない。
B サービス	従業員ごとに払い出されたメールアドレス及びパスワードを入力すると利用できる。アクセス制限機能によって，アクセス元 IP アドレスが UTM のグローバル IP アドレスの場合だけアクセスが許可される。

〔社外との情報共有〕

A 社の研究部は，素材研究とその実用化に関する情報を共有する“化学研究開発コンソーシアム”という団体（以下，化学コンという）を運営している。化学コンには，研究機関や大学，企業など 40 組織が会員として加盟している。化学コンでは，月に 1 回，対面形式の連絡会議が開催され，会員の上位役職者が参加している。連絡会議では，研究開発における機密性の高い議事も扱われる。開催案内などの機密性のあまり高くない情報の共有はメールで行われるが，重要な情報は情報連携システムと呼ばれる SSH を用いたシステムで共有されている。

会員は，情報連携システム用の連携端末を設置する必要がある。化学コンは，会員に図 2 に示す連携端末設置ガイドライン（以下，ガイドラインという）を提示し，遵守を求めている。

1. 連携端末を設置し，別途定める要件を満たす機器，ソフトウェアを導入し，別途定める運用を行うこと
2. 連携端末からインターネットにアクセスするときのグローバルIPアドレスを化学コンに伝えること
3. 共有した秘密情報は，別途定める秘密情報管理規程に従って管理すること
4. 連携端末に関して，セキュリティインシデント（以下，インシデントという）が発生した場合は，化学コンと協力して解決すること

図2　ガイドライン（抜粋）

情報連携システムの構成を図 3 に，情報連携の手順と会員間で共有するファイルを格納する連携サーバの運用を図 4 に示す。

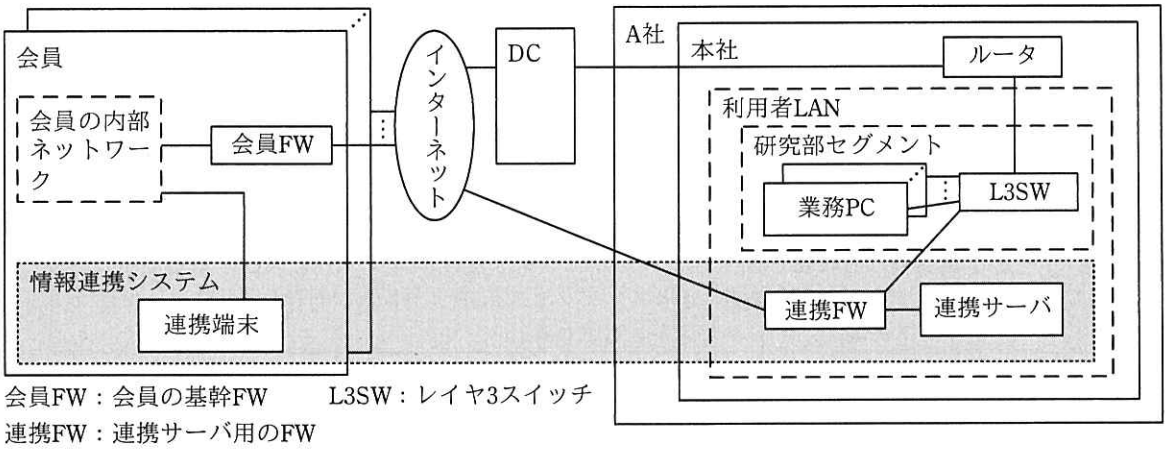

図3　情報連携システムの構成

[情報連携の手順]
・A 社の担当者は，共有したいファイルを連携サーバの共有フォルダに置く。連携サーバの共有フォルダは研究部セグメントの業務 PC から認証なしでアクセス可能になっている。
・連携サーバ及び連携端末には，SSH アプリケーションプログラムが導入されている。3 時間に一度，自動的に連携端末から連携サーバに SSH 通信を行い，認証に成功すると連携サーバの共有フォルダにあるファイルを，連携端末の所定フォルダにコピーする。
・会員の担当者は，随時，所定フォルダにあるファイルを連携端末上で閲覧する。
[連携サーバの運用]
・連携サーバは SSH による連携端末へのファイルのコピーが行われるとログファイルにログを出力する。ログファイルは日付を示す 8 桁の数字のファイル名で毎日生成され，60 日間保存される。61 日以前に生成されたログファイルは，毎日 0 時に起動する連携サーバの日次バッチ処理で自動削除される。
・ログファイルに出力されるログ項目は，SSH 接続ごとに，“接続日時，会員名，コピーファイル数，コピー成功/失敗ステータス”である。

図4　情報連携の手順と連携サーバの運用

連携サーバは，研究部が管理する連携FWを経由してインターネットに接続されている。連携FWでは，会員から伝えられたグローバルIPアドレス及び研究部セグメントから連携サーバへのアクセスだけを許可している。

〔テレワークの検討〕

2月2日，首都圏を中心とする感染症の急激な流行に伴い，A社は本社に勤務する従業員に対して，2月16日から原則，テレワークとする方針を決定した。また，より多くの従業員がテレワークに移行できるよう，テレワークWGを立ち上げた。テレワークWGには，情報システム部など関係する部の担当者が参加し，インフラ増強やルール整備を検討する。A社では，公的機関が発行したテレワークセキュリティガイドラインを参考に，図5に示すテレワークセキュリティ規程を作成し，本社に適用した。

役割を次のとおり定める。複数の役割を兼務する場合もある。
経営者：組織のあるべき姿を検討し，テレワークセキュリティ全般を考え，必要なリソースを確保する。
システム管理者：情報システムへの不正アクセス，マルウェア感染などのインシデント発生時の対処のルールを定める。
テレワーク勤務者：定められたルールを遵守し，データを安全に扱う。

[詳細]
1. [a] は，テレワークの推進に必要な人材・資源を確保するために，必要な予算を割り当てる。
2. [b] は，情報セキュリティポリシに従い，セキュリティ維持に必要な技術的対策を講じるとともに，定期的に実施状況を点検する。
3. [c] は，社内システムに，強度の低いパスワードが用いられないように制限を掛ける。
4. [d] は，パスワードの使い回しを避け，12桁以上の長さで他人に推測されにくいものを設定する。
5. システム管理者は，暗号化された通信路をテレワーク勤務者に提供する。その際，電子政府における調達の際にも参照される [e] 暗号リストを参照し，暗号化には危殆(たい)化していない暗号アルゴリズムを採用するものとする。

図5　テレワークセキュリティ規程（抜粋）

〔ネットワーク構成の見直しの検討〕

テレワークWGでは，支社でもテレワークの準備が必要であるという意見が出た。しかし，支社でのテレワークに本社と同様の方式を採用すると，UTM の処理能力を超過することが予想された。そこで，テレワーク WG は，新たなネットワーク（以下，新 NW という）の導入を検討することにした。図 6 に新 NW の内容，図 7 に新 NW の構成を示す。

・各支社に，新たにインターネット接続回線を敷設し，拠点 FW 及び拠点 DMZ を新設する。拠点 DMZ 内に拠点 VPN サーバを新設する。
・テレワーク時，支社のテレワーク勤務者には，所属する支社の拠点 VPN サーバに接続させ，基幹システムや利用者 LAN にあるリソースにアクセスさせる。拠点 VPN サーバ接続時には，本社と同様に 2 要素認証を行う。
・テレワーク時のインターネットアクセスは，一度，拠点 VPN サーバにアクセスさせ，DC を経由させる。ただし，①B サービスへのアクセスだけ，拠点 VPN サーバから，DC を経由させずに支社に敷設したインターネット接続回線を経由させる。

図 6　新 NW の内容

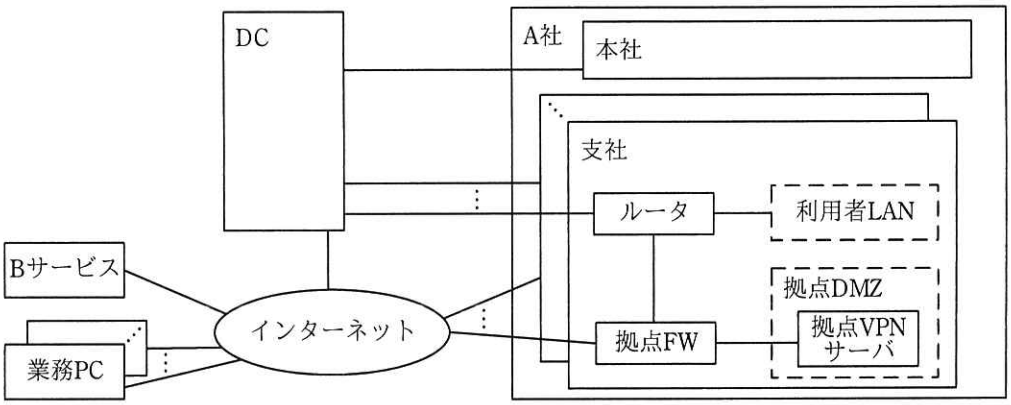

図 7　新 NW の構成

テレワーク WG は，新 NW の導入に先立ち，ある支社で新 NW をテストした。②その支社のテレワーク勤務者が，インターネットへはアクセスできたが，B サービスに接続できないというトラブルが発生した。B サービスの設定を変更することによってトラブルは解消でき，無事，テストが完了した。A 社は新 NW の導入を正式に決定し，6 月 15 日，各支社でもテレワークを開始した。

〔インシデントの発生〕

9月11日，情報システム部のシステム管理者であるCさんは，差出人が総務部のDさんと表記されたメールを受信した。メールの文面に違和感を覚えたCさんが，念のためDさんに電話で確認したところ，“そのようなメールは送信していない”という回答だった。Cさんは，すぐさまA社のCSIRTに報告した。報告を受けたCSIRT所属のEさんは，調査を行い，Dさんの証言やBサービスの利用履歴などからDさんのBサービスのアカウントが第三者に不正利用されている可能性が高いと判断した。Eさんは，情報システム部のCさんに，Dさんのアカウントの無効化措置を依頼した。その後，契約中のセキュリティベンダX社に所属する情報処理安全確保支援士（登録セキスペ）のP氏の支援を受け，9月16日に図8に示す初期調査結果をまとめた。

[タイムライン]
- 4月1日：情報システム部が新NWのテストでのトラブル解消のために，Bサービスの設定を変更した。
- 7月9日：攻撃者が，何らかの方法で入手したDさんのアカウントを使って，インターネットからBサービスに不正ログインした。
- 7月14日：攻撃者は，Dさんのアカウントを使って研究部のFさん宛にマルウェアαを添付したメールを送信した。Fさんがそのメールの添付ファイルを開いた結果，Fさんの業務PCがマルウェアαに感染した。同日中に，攻撃者の遠隔操作によって同業務PCがマルウェアβにも感染した。
- 7月28日から9月11日：攻撃者はDさんのアカウントを使って，Cさんなど数名の従業員宛にマルウェアβを添付したメールを断続的に送信した。
- 9月11日：Cさんから報告を受け調査を開始した。

[攻撃者の活動の特徴]
- 攻撃者は，メールの送信間隔を空けたり，マルウェアの拡散速度を遅くしたりしていた。感染した業務PCからA社内の情報を不正に取得していた。
- 攻撃者は，メールの送信をDさんに知られないよう，マルウェアを添付したメールを送信済みボックスから全て削除していた。
- 一部の業務PCでは，全てのイベントログが消去された痕跡があった。全てのイベントログが消去された後，イベントログにイベントログの消去を示すログが記録されていた。
- 攻撃者がDさんのアカウントを使って送信したメールは，タイムラインに示したA社内宛のメールだけであり，社外宛のメールはなかった。

図8　初期調査結果（概要）

同日，X社からマルウェアの解析結果が報告された。マルウェアα及びマルウェアβのどちらにもA社を標的にしたと思われる識別文字列，A社固有のファイルパス，

並びに C&C サーバの IP アドレス及び FQDN のリストが埋め込まれていた。また，どちらも A 社が導入しているマルウェア対策ソフトでは検出されなかった。報告されたマルウェアの特徴を表 2 に示す。

表 2　マルウェアの特徴

名称	特徴
マルウェア α	PC 又はサーバが感染すると，C&C サーバと通信を確立し，攻撃者が遠隔操作できる状態になる。このとき，イベントログにマルウェア α の実行を示すログ（以下，α ログという）が記録される。
マルウェア β	次の(1)～(3)の機能をもつマルウェアである。PC 又はサーバが感染すると，いずれかの機能を，あらかじめ定められた確率でランダムに実行する。この実行は，1 週間の間隔を置いて繰り返され，遠隔操作機能の実行に成功すると，繰り返しの実行を停止する。 (1) 待機機能 何もしない。 (2) 横展開機能 感染した PC 又はサーバから到達可能なネットワーク内の機器をスキャンし，OS の脆弱(ぜい)性がある機器を発見すると，自身に感染させる。また，アクセス可能な共有フォルダを発見すると，細工された文書ファイルを生成し，その共有フォルダに置く。細工された文書ファイルを開いた機器はマルウェア β に感染する。 (3) 遠隔操作機能 当該 PC 又はサーバ内に保存されているクレデンシャル情報を収集する。C&C サーバと通信を確立し，収集した情報を C&C サーバに送信する。このとき，イベントログにマルウェア β の実行を示すログ（以下，β ログという）が記録される。以後，当該 PC 又はサーバの起動中は C&C サーバから攻撃者が遠隔操作できる状態を維持する。

A 社は重大なインシデントが発生したと判断し，社内規程に従い緊急対策本部（以下，対策本部という）を設置した。

〔インシデントへの対策の検討〕

このインシデントでは，D さんが B サービスに脆弱なパスワードを設定していたことに加えて，新 NW の導入に際しての B サービスの設定変更も攻撃が成功してしまった要因であることが分かった。

対策本部長（以下，本部長という）は，初期調査結果及びマルウェアの特徴をメンバと共有し，優先すべき対策を表 3 のように整理した。

表3　優先すべき対策（抜粋）

対策名	対策項目	暫定対策	恒久対策
対策1	C&C サーバへの通信の遮断	（省略）	（省略）
対策2	マルウェアα及びマルウェアβの駆除	（省略）	（省略）

次は，対策本部会議での，本部長，対策本部メンバの G さん及び P 氏の質疑である。

本部長：対策1については，どのように行うのか。

G さん：マルウェアαとマルウェアβには C&C サーバの IP アドレスと FQDN のリストが埋め込まれていました。その IP アドレス，及びその FQDN の DNS の正引き結果の IP アドレスの二つを併せた IP アドレスのリスト（以下，IP リストという）を手作業で作成しておき，IP リストに登録された IP アドレスへの通信を UTM で拒否します。

P 氏　：その対策だけでは，③攻撃者が行う設定変更によって，すぐにマルウェアαやマルウェアβの通信を遮断できなくなることが考えられます。④そこで，UTM での通信拒否に加えて，追加の暫定対策として，UTM の DNS シンクホール機能の有効化を推奨します。

本部長：では，両方の対策を実施しよう。次に，対策2については，どのように行うのか。

G さん：まず感染を確認するために，イベントログにαログ又はβログが存在するかどうかをチェックする確認ツールを作成してA社内に配布し，従業員に実行してもらいます。

P 氏　：イベントログに［　f　］が存在するかどうかもチェックする必要があると思います。さらに，確認ツールは暫定対策として有効ですが，全ての感染を確認できるわけではありません。⑤確認ツールを実行し，問題がないと判定された PC やサーバであっても，その後，別の PC やサーバに感染を拡大させることが考えられます。

本部長は，確認ツールとは別に，より高い精度でマルウェアα及びマルウェアβ

を検出し，駆除できるツール（以下，駆除ツールという）の開発を X 社に委託することにした。P 氏は，開発する駆除ツールは，ディジタルフォレンジックスの経験を有する技術者だけが扱うことができるツールになることを説明した。

P 氏は，対策本部会議の恒久対策に関する質疑の際に，将来的には連携サーバを DC の DMZ に移設し，連携 FW を廃止する検討をした方がよいとの意見を述べた。その理由として，⑥インターネットから連携サーバが攻撃を受けたときに，より迅速な対応が可能であることを挙げた。

その後の対策本部会議の質疑の中で，連携サーバ自体が感染していなくても連携サーバ経由で，会員にもマルウェアβの感染を拡大させている可能性が指摘された。本部長は，E さんに，早急に連携サーバ経由の感染状況を確認し，感染拡大を防止するよう指示した。

〔連携サーバ経由の感染状況の確認と感染拡大防止〕

E さんは，まず，連携サーバをネットワークから切り離し，ディスクイメージを保全した。また，化学コンの運営責任者を通して，化学コンの全会員に連携端末を一時的にネットワークから切り離してもらうように連絡し，全ての会員で対応が完了したことを即日確認した。9 月 17 日，E さんは連携サーバの担当者にヒアリングを実施した。ヒアリングの際に，連携サーバに存在するログファイルを担当者に確認してもらったところ，最も古いものは 7 月 19 日に生成されたものであることが分かった。E さんは，マルウェアβの感染を拡大させている可能性があることから，会員でも何らかの対処が必要であり，会員によっては PC やサーバで，駆除ツールを実行しなければいけないと考えた。また，駆除ツールが扱える技術者を多数確保することは難しいので，全ての会員に対して一斉に対処をすることはできないと判断し，次の対処方針を定めた。

・感染調査手順書を作成し，各会員の担当者に調査を依頼する。その調査結果から，会員をグループ A とグループ B に分ける。
　グループ A：感染の疑いが強く，より早期に対処が必要な会員
　グループ B：それ以外の会員
・グループ A の会員には，P 氏と駆除ツールが扱える技術者が連携端末設置場所に赴き，駆除ツールを用いて連携端末上のマルウェアβを駆除する。さらに，マルウ

ェア感染に伴う会員側の被害を確認し，その対処をA社が支援する。

・グループAの全会員での駆除が完了した後に，グループBの会員に対して同様の手順で駆除を含めた対応を行う。

〔感染調査手順書のレビュー〕

Eさんは感染調査手順書案を作成し，P氏にレビューを依頼した。表4は感染調査手順書案に記載した感染調査項目，図9はP氏からのレビュー回答である。

表4　感染調査項目

調査名	調査内容	調査結果	判定
調査1	連携端末の対象期間[1]中のイベントログに，αログ，βログ又は［　f　］が存在するかどうか。	存在する	グループA
		存在しない	グループB

注[1]　対象期間：7月19日～調査日当日

感染調査項目に関して次の見直しを行う必要がある。
指摘1：対象期間の開始日は，本来は，保存されている最も古いイベントログの日付にすべきだが，せめて連携サーバに細工されたファイルが置かれていた可能性のある最も早い日付である［　g　］にする必要がある。
指摘2：マルウェアβの特徴を踏まえると，会員内での感染の広がりも考慮する必要がある。本来は，会員の全てのPCを確認してもらうべきだが，せめて会員FWのログの確認は追加で依頼する必要がある。

図9　P氏からのレビュー回答

Eさんは P氏の指摘2に対する改善案として，表5に示す感染調査項目を追加し，調査2の調査結果が“記録あり”である場合もグループAと判定することにした。

表5　追加した感染調査項目

調査名	調査内容	調査結果	判定
調査2	対象期間中の会員FWのログに，次に該当する送信元から宛先への通信記録が存在するかどうか。 送信元：任意のIPアドレス 宛先：［　h　］	記録あり	グループA
		記録なし[1]	グループB

注[1]　会員FWでログが取得されていない場合や，一部ログが欠けている期間があっても，ログが存在する範囲で通信記録がない場合は記録なしとする。

Eさんは，再びP氏のレビューを受けた。次は，再レビュー時のP氏とEさんの会話である。

P氏　：今回の感染調査の目的は，感染の疑いが強い会員を見つけることなので，調査2の内容は良いと思います。提案なのですが，仮に今回の感染調査の結果，大多数の会員がグループAと判定された場合，グループ分けの意義が薄れてしまいます。グループAと判定された会員の中から，更に対処を優先する会員を絞ってはどうでしょうか。

Eさん：対処を優先する会員をどのように絞ればよいのでしょうか。

P氏　：⑦連携端末からほかのPCやサーバへの感染拡大が明らかな会員に絞るのであれば，調査2に使う通信記録から絞ることができると思います。グループAと判定された会員企業であっても，この通信記録がなかった会員は，⑧既に行っている対応から考えて，感染を拡大させるリスクは相対的に低いと考えることができます。

Eさんは P氏の指摘や助言に従い感染調査手順書を修正し，会員に送付した。七つの会員がグループ A と判定されたものの，どの会員にも深刻な被害は確認されなかった。A社はその後もインシデント対応を進め，社内の詳しい調査を経て，攻撃者の活動は初期調査結果どおりだったことも確認した。対策1と対策2の暫定対策と恒久対策を完了した A 社は，対策本部を解散し，再発防止に向けた新たな取組の検討に着手した。

設問1　〔テレワークの検討〕について，(1)，(2)に答えよ。

(1)　図 5 中の［ a ］～［ d ］に入れる適切な役割を解答群の中から選び，記号で答えよ。

解答群

ア　経営者　　イ　システム管理者　　ウ　テレワーク勤務者

(2)　図5中の［ e ］に入れる適切な字句を英字8字で答えよ。

設問2　〔ネットワーク構成の見直しの検討〕について，(1)，(2)に答えよ。

(1)　図 6 中の下線①のネットワーク構成を示す用語を，解答群の中から選び，

記号で答えよ。

解答群

ア　OpenFlow　　イ　Software-Defined Networking

ウ　ゼロトラストネットワーク　　エ　ローカルブレイクアウト

(2)　本文中の下線②について，トラブルを引き起こした原因を，35 字以内で具体的に述べよ。

設問３　〔インシデントへの対策の検討〕について，(1)～(5)に答えよ。

(1)　本文中の下線③について，どのような設定変更か。40 字以内で具体的に述べよ。

(2)　本文中の下線④について，DNS シンクホール機能を有効化した場合でも，UTM での通信拒否が必要な理由を，マルウェアの解析結果を踏まえて 40 字以内で具体的に述べよ。

(3)　本文及び表 4 中の［　f　］に入れる適切な字句を，20 字以内で答えよ。

(4)　本文中の下線⑤について，問題がないと判定されるのは，PC やサーバがマルウェア β に感染後，マルウェア β がどのような挙動をしていた場合か。25 字以内で具体的に述べよ。

(5)　本文中の下線⑥について，可能である理由を 45 字以内で具体的に述べよ。

設問４　〔感染調査手順書のレビュー〕について，(1)～(4)に答えよ。

(1)　図 9 中の［　g　］に入れる適切な日付を答えよ。

(2)　表 5 中の［　h　］に入れる適切な字句を 25 字以内で答えよ。

(3)　本文中の下線⑦について，どのような通信記録があった会員が該当するか。通信記録の内容を 30 字以内で具体的に述べよ。

(4)　本文中の下線⑧について，どのような対応か。30 字以内で述べよ。