問１　脅威情報調査に関する次の記述を読んで，設問に答えよ。

L 社は，従業員 200 名のセキュリティ関連会社である。L 社の脅威情報調査部（以下，Q 部という）は，国内で流行しているマルウェアを解析したり，攻撃者グループの攻撃手法を調査したりして，顧客にレポートを提供する事業を行っているほか，四半期レポートを作成して公開している。Q 部が管理するネットワークの概要を図 1 に，システムの概要を表 1 に示す。

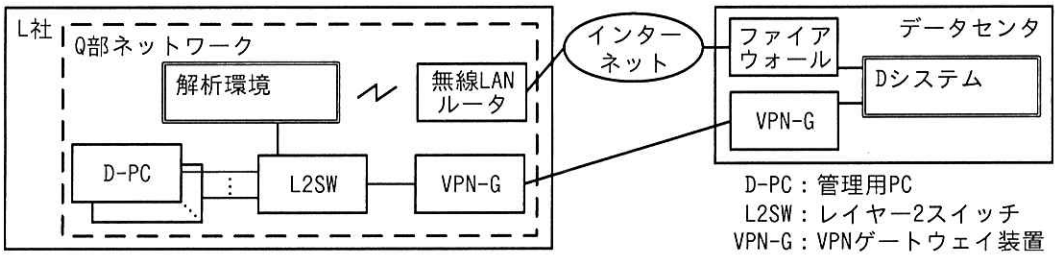

図 1　ネットワークの概要

表 1　システムの概要

項番	名称	概要
1	解析環境	マルウェアを実行して挙動を確認したり，マルウェアを簡易的に解析して機能を確認したりする環境である。サンドボックス用の複数の仮想マシンで構成されている。各仮想マシンは，動的解析中だけ無線 LAN ルータを経由して，インターネットにアクセスできる状態にする。
2	D システム	自社開発したハニーポット用のシステムであり，Q 部の事業に活用している。小規模オフィスから大規模オフィスまでの，疑似オフィス環境（以下，OF 環境という）10 組などで構成されている。各 OF 環境は，PC のほか，DHCP サーバ，メールサーバ，DNS サーバ，業務用各種サーバといった仮想マシン（以下，OF 機器という），及びルータで構成されている。必要に応じて，L2SW を含むこともある。各 OF 環境間の通信は全て禁止されている。
3	D-PC	解析環境及び D システムを操作する。Web ブラウザを起動し D システムにアクセスする。
4	VPN-G	Q 部ネットワークと D システムの間を IPsec-VPN で接続する。

D システムの概要を図 2 に，D システムの構成要素の説明を表 2 に示す。

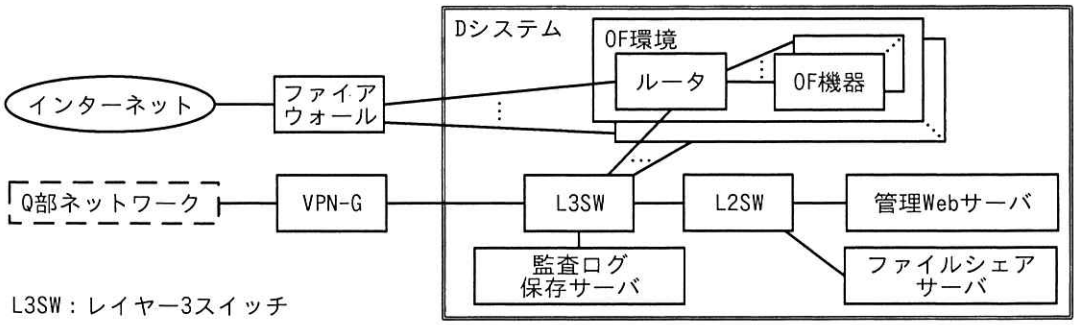

図2　Dシステムの概要

表2　Dシステムの構成要素の説明

項番	構成要素	説明
1	OF 機器	OF 機器での始業時のログインや終業時のログアウトといった利用者の日常的な業務を模した操作は，各 OF 機器上の専用プログラムによって自動的に行われる。各 OF 機器ではログも取得され，ARP テーブルの状態，CPU 使用率といったシステム情報も定期的に記録される。スナップショット機能によって OF 機器は定期的にディスクイメージが保存されており，OF 機器を任意の保存時点の状態に戻すことができる。
2	ファイルシェアサーバ	D-PC と各 OF 機器との間で転送するファイルを一時的に保存するための仮想マシンである。
3	監査ログ保存サーバ	OF 環境内の，各 OF 機器で記録された情報，並びにルータ及び L2SW でキャプチャしたパケットを集約して保存する。保存した情報を監査ログと呼び，解析業務などで利用する。
4	管理 Web サーバ	D-PC から D システムを操作するための Web インタフェースを提供する。D システムの各構成要素に対して行える操作は次のとおりである。 OF 機器：OF 環境内の全部又は個別の OF 機器に対する起動又はシャットダウン，各 OF 機器へのログイン OF 環境内のルータ：OF 環境ごとのインターネット及びファイルシェアサーバとの通信制御の切替え ファイルシェアサーバ：D-PC との間でのファイル転送 監査ログ保存サーバ：監査ログの閲覧

各 OF 環境内のルータには，“内部モード”と“公開モード”の二つのモードがあり，各モードでは，表 3 に示す通信制御のルールに従って各 OF 機器とそれ以外との間での通信制御が行われる。初期設定は内部モードである。

表3　OF 機器に対するモードごとの通信制御のルール

項番	送信元	宛先	通信制御	
			内部モード	公開モード
1	OF 機器	インターネット	禁止	許可
2	OF 機器	監査ログ保存サーバ	禁止	禁止
3	OF 機器	管理 Web サーバ	禁止	禁止
4	OF 機器	ファイルシェアサーバ	許可	禁止
5	OF 機器	Q 部ネットワーク	禁止	禁止
6	インターネット	OF 機器	禁止	許可
7	監査ログ保存サーバ	OF 機器	許可	許可
8	管理 Web サーバ	OF 機器	許可	許可
9	ファイルシェアサーバ	OF 機器	許可	禁止
10	Q 部ネットワーク	OF 機器	禁止	禁止

注記　通信制御はステートフルパケットインスペクションで行われる。

〔検体の解析作業〕

四半期レポートの作成チームのリーダーは Q 部の Y 主任であり，メンバーは新人アナリストの T さんである。T さんは，現在国内で感染が確認されている 3 種類の検体（以下，検体α，検体β，検体γという）の解析作業を担当する。T さんは，3 種類の検体を解析環境で実行し，挙動を確認するよう Y 主任から指示を受けた。T さんは，各検体を実行し，簡易的な解析を実施した。T さんが確認した挙動と簡易的な解析の結果を表 4 に示す。

表4　T さんが確認した挙動と簡易的な解析の結果

検体名	確認した挙動	簡易的な解析の結果
検体α	C&C サーバに接続し，プログラムコードをダウンロードした。	ダウンロードしたプログラムコードは，①ディスクには展開されずメモリ内だけに展開される。このプログラムコードは，キーボード入力を記録し，定期的に C&C サーバに送信するキーロガー機能をもつ。
検体β	PC 上の特定の拡張子をもつファイルを次々に暗号化した。暗号化完了後にデスクトップの背景を変更して終了した。	OS の言語設定を参照する。（省略）
検体γ	自身のデータの一部を削除して，すぐに終了した。	自身が仮想マシン上で動作していることを検知すると，システムコールを使用して自身のプログラムコード中の攻撃コードを削除した後，終了する。この機能は解析を回避するためのものであると考えられる。

T さんは，これらの検体の挙動と解析の結果を報告書にまとめ，Y 主任に報告した。次は，報告後の T さんと Y 主任の会話である。

T さん ：今日は金曜日なので，解析環境の仮想マシンは帰宅前に全てシャットダウンして，週明けに改めて解析環境を使い，追加の調査をしようと思います。

Y 主任 ：近年の攻撃の傾向を考えると，②今日確認した検体αの挙動が，検体αを週明けに再実行した時には，攻撃者による変更によって再現できなくなる可能性がある。念のため，今の仮想マシンの状態を保存しておいてほしい。その上で，週明けに改めて解析環境で検体αを実行してみよう。

T さんは，指示に従って保存作業を実施した。週明け，T さんが改めて検体αを実行したところ，表 4 の挙動が再現できることを確認した。T さんは，追加の調査を実施し，Y 主任に最終報告をした。その後の Q 部内の会議で，検体αは D システムを用いて詳細に解析すること，検体βは詳細な解析を見送ること，検体γは現在の解析環境ではこれ以上解析できないので，③別の環境を構築して解析することが決定した。T さんが，検体αを D システム上で実行し，インターネットとの通信を解析することになった。

〔ファイル転送手順の改善〕

Q 部では，D システムに検体を持ち込んで実行する手順が図 3 のとおりに定められている。

1. D-PC で Web ブラウザを起動し，管理 Web サーバにアクセスする。
2. 解析に使用する OF 環境内のルータが内部モードであることを確認する。
3. 圧縮した検体を D-PC からファイルシェアサーバに転送する。
4. OF 環境内の解析に使用する OF 機器にログインし，圧縮した検体をファイルシェアサーバから OF 機器に転送する。
5. 使用する OF 環境内のルータを公開モードに切り替える。
6. OF 機器上で，検体を取り出し，実行する。

図 3　検体を持ち込んで実行する手順

検体の実行によって生成される OF 機器上のログやファイルなどは，監査ログ保存サーバでは収集されない。そこで，検体の実行後，図 4 に示すファイル転送手順によって D-PC に転送する。

1. D-PC で Web ブラウザを起動し，管理 Web サーバにアクセスする。
2. 使用した OF 環境内のルータを内部モードに切り替える。
3. 使用した OF 機器にログインし，ログ自動収集ツール [1)]が出力したファイル及び解析に必要な任意のファイル（以下，2 種類のファイルをあわせて解析ファイルという）を収集する。
4. 解析ファイルをファイルシェアサーバに転送する。
5. 使用した OF 環境内の全部の OF 機器をシャットダウンする。
6. ファイルシェアサーバ上でマルウェアスキャンを実行し，ファイルシェアサーバがマルウェアに感染していないことを確認した上で，解析ファイルを D-PC に転送する。

注 [1)] ログ自動収集ツールは，同ツールを実行した PC やサーバの主要なログ情報を自動で収集し，ファイルとして出力する。実行から収集完了までには，およそ 30 分～1 時間を要する。

図 4　ファイル転送手順

T さんは，図 4 の手順では，OF 環境で実行するマルウェアが，自律的に感染を広げる機能をもっている場合，ファイルシェアサーバに感染が及ぶ可能性があると考えた。万一，ファイルシェアサーバがマルウェアに感染すると，他の OF 環境での解析作業に影響を与えてしまう。そこで，次の方針で新しい手順を作成することにした。

・OF 環境内のルータごとに 1 台の検疫 PC を新たに設置する。
・解析ファイルの転送は，必ず検疫 PC を経由させる。
・解析ファイルの転送では，検疫 PC がマルウェアに感染していないことを確認する。
・検疫 PC は，表 3 の通信制御のルールについては，OF 機器として扱う。
・検体の実行後，検疫 PC 以外の OF 機器と，ファイルシェアサーバとは直接通信させない。
・検疫 PC は，パーソナルファイアウォール（以下，PFW という）の設定によって，検疫 PC と管理 Web サーバとの間の通信だけを許可しておき，解析ファイルの転送に必要な通信を転送時にだけ許可する。

T さんは，検疫 PC を用いた新しいファイル転送手順案を考案し，Y 主任に説明した。後日，Q 部内の会議でこのファイル転送手順が，Q 部の正式な手順として採用された。新しいファイル転送手順を図 5 に示す。

1. D-PC で Web ブラウザを起動し，管理 Web サーバにアクセスする。
2. 使用した OF 環境内の OF 機器にログインし，解析ファイルを収集する。
3. [a]
4. [b]
5. 検疫 PC にログインし，マルウェアスキャンを実行して検疫 PC がマルウェアに感染していないことを確認した上で，以降の手順に進む。
6. [c]
7. [d]
8. ファイルシェアサーバから D-PC に解析ファイルを転送する。
(省略)

図 5　新しいファイル転送手順

〔模擬攻撃試験の受験〕

1 年後，T さんは模擬攻撃試験を受けることになった。模擬攻撃試験とは，年 1 回行われる社内試験である。2 日間の試験で，初日は，受験者だけがアクセスできる D システム内に作られた試験用 OF 環境にインターネットから接続し，事前に与えられたツール群とヒント情報を基に，秘密情報に見立てた文字列情報（以下，flag という）を 8 時間の間にできるだけ多く入手するという実技を行う。2 日目の午前は，flag の入手過程で確認した脆弱(ぜい)性，実行した攻撃手法などについて試験評価者（以下，評価者という）と討論する。午後は，flag の入手過程で確認した脆弱性について，運用面での改善提案を報告書にまとめ提出する。合否は 2 日間の総合成績によって決定する。L 社ではこの試験の合格が重要な業務を担当するための要件の一つになっている。

試験の初日は，試験用 OF 環境内のある PC（以下，X-PC という）が遠隔操作可能な状態から試験が始まった。T さんは，X-PC のシステム情報，X-PC に残っていた電子メールなどを収集し，X-PC から試験用 OF 環境内を探索して，flag の入手を試みた。初日の試験では，最終的に T さんは五つの flag の入手に成功した。試験 2 日目の討論では，T さんは，最初の flag の入手過程で ARP スプーフィングを使用したことから説明を始めることにした。

〔ARP スプーフィングの使用に関する説明〕

T さんは ARP スプーフィングの使用に関して次のように説明した。

(1) 与えられたヒント情報から，X-PC と同一セグメントにある別の PC（以下，標的 PC という）が送信するパケットを ARP スプーフィングによって盗み見できれば，最初の flag を入手できると考えた。

(2) 事前に与えられたツール群の中から ARP 関連のツールを探したところ，A ツールという広く流通する OSS の ARP スプーフィングツールがあり，表 5 に示す三つの機能をもつという情報を得た。

表 5　A ツールの機能

項番	機能名称	機能詳細
1	プローブ機能	OS 標準の機能を用いて同一セグメント内に ARP 要求を出し，応答を記録する。
2	ARP スプーフィング機能	標的の機器の IP アドレスを指定して実行すると，標的の機器が ARP 要求を出した際に，正規の ARP 応答が戻ってくる前に，自身の MAC アドレスを含んだ不正な ARP 応答を送る。
3	中継機能	ARP スプーフィング機能が成功した後，自身に送られてきたパケットを加工し，パケットの本来の宛先に転送する。

(3) ネットワーク内の機器の情報を得たいと考え，表 5 中の項番 [e] の機能を実行した。実行後の X-PC の ARP テーブルは表 6 であった。

表 6　X-PC の ARP テーブル（抜粋）

IP アドレス	MAC アドレス
192.168.15.51	XX-XX-XX-23-46-4a
192.168.15.98	XX-XX-XX-f9-48-1b

注記　XX-XX-XX は同一のベンダ ID である。

(4) X-PC の ARP テーブル，X-PC 内のメール情報などを基にして，図 6 に示すネットワーク図を作成した。

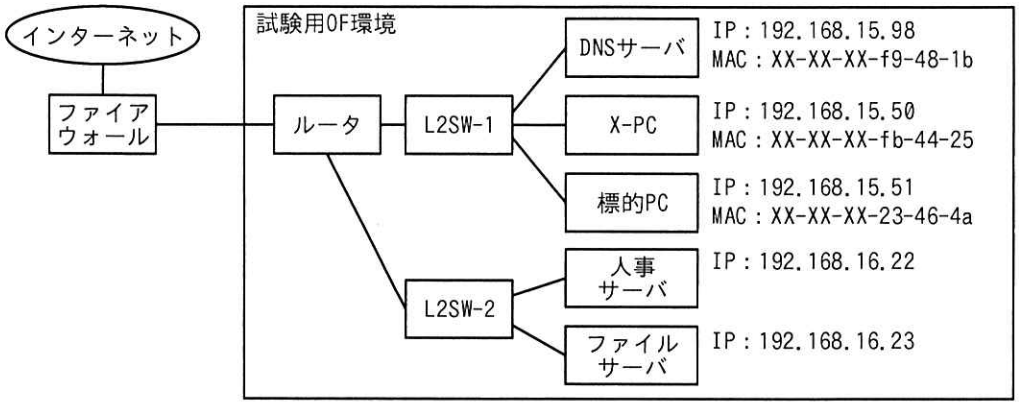

図 6　作成したネットワーク図

(5) ARP スプーフィング機能について，標的 PC の IP アドレスを指定して実行した後，DNS サーバの IP アドレスを指定して実行し，標的 PC から DNS サーバへの通信を盗み見する準備を整えた。この時の X-PC の ARP テーブルは表 7，標的 PC の ARP テーブルは表 8 のとおりであった。

表 7　ARP スプーフィング機能実行後の X-PC の ARP テーブル（抜粋）

IP アドレス	MAC アドレス
192.168.15.51	f
192.168.15.98	g

表 8　ARP スプーフィング機能実行後の標的 PC の ARP テーブル（抜粋）

IP アドレス	MAC アドレス
192.168.15.50	h
192.168.15.98	i

(6) ARP スプーフィングが成功している証拠を評価者に説明するために，監査ログ保存サーバに記録されていた，L2SW-1 を通過したパケットの記録を確認したところ，表 9 に示すとおりであった。

表 9　パケットの記録（抜粋）

送信元 IP アドレス	宛先 IP アドレス	サービス	送信元 MAC アドレス	宛先 MAC アドレス
192.168.15.51	192.168.15.98	DNS	j	k
192.168.15.51	192.168.15.98	DNS	l	m
192.168.15.98	192.168.15.51	DNS	XX-XX-XX-f9-48-1b	XX-XX-XX-fb-44-25
192.168.15.98	192.168.15.51	DNS	n	o

注記 1　ARP スプーフィングに関係するパケットだけを抜粋している。
注記 2　パケットは表中の上から順に送信された。

この後，T さんは，盗み見の成功から最初の flag 入手までの流れを評価者に説明した。評価者から幾つかの質問を受けたが，T さんは問題なく受け答えできた。次に，T さんは，2～4 番目に入手した flag についても同様の流れで説明した。最後に，5 番目の flag の入手に使用した人事サーバのパスワード解読に関して説明した。

〔パスワードの解読に関する説明〕

T さんはパスワード解読に関して次のように説明した。

(1) ヒント情報には，5 番目の flag を入手するためには，システム管理者の利用者 ID とパスワードを用いて Web ブラウザから人事サーバにログインする必要があると書かれていた。

(2) ここまでの flag 入手の過程で得た情報を図 7 のように整理した。

1. ファイルサーバに保存されていた人事サーバの設計資料の情報
・利用者 ID に対してログイン失敗が 5 回連続した場合は，当該利用者 ID によるログインを 10 分間ロックする。
・利用者が設定したパスワードは，Blowfish 暗号を用いた，ソルトあり，④ストレッチングありのハッシュ関数を用いて出力した文字列（以下，H 文字列という）の形式で保存される。
例：$2b$05$AQHjx4ARKab2DrcdqO8tjuF2PvpI5NR5Xv/xjl/gZq.Q79vYF0w7C[1)]
2. 人事サーバに用いられている OSS の既知の脆弱性を悪用して閲覧できたデバッグログの情報
・デバッグログには，ログインした利用者 ID ごとの，セッション情報，H 文字列を含む認証情報，プログラムコードで用いられていると思われる関数名や変数の値などが出力されていた。
・デバッグログを解析したところ，システム管理者が直近のログインに成功した時に入力したパスワードに対して出力された H 文字列（以下，文字列 Z という）は次のとおりであった。
$2b$05$U/fzKvGOd//4E68fqvHJfOtrLcfj8LL5i7OziYaG8J5IS.vDpLJFy
3. パスワードについての推測
・ここまでに得た試験用 OF 環境に設置されているサーバのシステム管理者のパスワードは，いずれも“Admin[数字 5 桁]”であり，[数字 5 桁]にはサーバごとに異なる数字が設定されていた。このことから，人事サーバにおいても同じ形式のパスワードが用いられていると推測できる。

注[1)] 最初の 7 字はハッシュ関数のバージョンとストレッチング回数，その次の 22 字はソルト，その次の 31 字はハッシュ値を示す。

図 7　整理した情報

(3) 図 7 の情報から，システム管理者のパスワードを得るための攻撃手法を最初に二つ考えたが，いずれの手法も，表 10 に示すとおり，残りの試験時間内にパスワードを得ることは困難であると判断した。

表 10　攻撃手法と判断理由

項番	攻撃手法	困難であると判断した理由
1	人事サーバに対して，ツールを用いて，ブルートフォース攻撃によるログイン試行をする。	⑤ブルートフォース攻撃に対抗する機能があるから
2	文字列 Z に含まれるハッシュ値から平文を得るために，[p] 攻撃を行う。	文字列 Z の生成にはソルトが用いられているから

(4) 三つ目の攻撃手法を考えて試し，成功した。具体的には，図 8 に示すオフライン攻撃の流れをプログラムとして実装し，実行することによってシステム管理者のパスワードを解読した。

STEP1：整数型の変数 n に 0 を代入する。
STEP2：⑥システム管理者のパスワードとして n 番目の候補となる文字列を生成する。人事サーバの設計資料に記載されていたハッシュ関数を実行する。関数への入力は，n 番目の候補文字列，文字列 Z の中に記載されたハッシュ関数のバージョン，ストレッチング回数，ソルトである。出力は H 文字列である。
STEP3：STEP2 で出力した H 文字列と，文字列 Z とを比較し，一致していれば n 番目の候補文字列を出力してオフライン攻撃を終了する。一致しない場合は，STEP4 に進む。
STEP4：変数 n が最大値の場合はオフライン攻撃を終了する。それ以外の場合は，変数 n に 1 を加え，STEP2 に戻る。

図 8　オフライン攻撃の流れ

〔運用に関する改善提案〕

討論会を終えた T さんは，最後の試験課題である，報告書の作成に着手した。図 9 は，T さんが作成した運用に関する改善提案の報告書である。

ARP スプーフィングの有力な対策方法は二つある。一つ目の方法は，一部のスイッチがもつ Dynamic ARP Inspection 機能を有効化する方法である。二つ目の方法は，重要な PC や狙われやすいサーバについて，ARP スプーフィングが実行されていないか常時監視する方法である。例えば，各 PC 及びサーバの ARP テーブルを常時監視して，⑦ARP テーブルの不審な状態を確認した場合には，システム管理者が当該 PC 又はサーバ，及びネットワークを調査し，ARP スプーフィングが行われていないかどうかを確認する運用が考えられる。
（省略）
5 番目の flag の入手に使用したセキュリティ上の弱点を考えると，人事サーバについて，次の点の改善が望ましい。
(1) 脆弱性管理の観点
　OSS に対して，最新の脆弱性修正プログラムを適用すること。具体的には（省略）
(2) パスワードの観点
　各サーバのシステム管理者のパスワードには推測可能なパスワードの設定は避けること。具体的には（省略）
(3) ログの観点
　[q]。具体的には（省略）

図 9　運用に関する改善提案の報告書（抜粋）

T さんは報告書を完成させて提出した。数日後，試験の合格通知を受け取った T さんは，今後はより重要な業務を担当できることになった。

設問１　〔検体の解析作業〕について答えよ。

(1)　表 4 中の下線①の挙動を特徴とするマルウェアの種類を，解答群の中から選び，記号で答えよ。

解答群

ア　アドウェア　　イ　暗号資産採掘マルウェア

ウ　トロイの木馬　　エ　ファイルレスマルウェア

オ　ランサムウェア

(2)　本文中の下線②について，再現ができなくなるのは，攻撃者によって何が変更される場合か。攻撃者によって変更されるものを 15 字以内で答えよ。

(3)　本文中の下線③について，現在の解析環境との違いを 20 字以内で答えよ。

設問２　図 5 中の［　a　］～［　d　］に入れる適切な手順を，解答群の中から選び，記号で答えよ。

解答群

ア　検疫 PC にログインし，検疫 PC の PFW の設定を変更して検疫 PC と OF 機器との間の通信を許可する。解析ファイルを OF 機器から検疫 PC に転送する。

イ　検疫 PC にログインし，検疫 PC の PFW の設定を変更して検疫 PC とファイルシェアサーバとの間の通信を許可する。解析ファイルを検疫 PC からファイルシェアサーバに転送する。

ウ　検疫 PC を除く OF 機器をシャットダウンする。

エ　使用した OF 環境内のルータを内部モードに切り替える。

設問３　〔ARP スプーフィングの使用に関する説明〕について答えよ。

(1)　本文中の［　e　］に入れる適切な機能を，表5の中から選び，項番で答えよ。

(2)　表 7 中及び表 8 中の［　f　］～［　i　］に入れる適切な MAC アドレスを，解答群の中から選び，記号で答えよ。なお，同一の MAC アドレスが入る場合もある。

解答群

ア　XX-XX-XX-23-46-4a　　イ　XX-XX-XX-f9-48-1b

ウ　XX-XX-XX-fb-44-25　　エ　XX-XX-XX-ff-ff-ff

(3) 表 9 中の [j] ～ [o] に入れる適切な MAC アドレスを，解答群の中から選び，記号で答えよ。なお，同一の MAC アドレスが入る場合もある。

解答群

ア XX-XX-XX-23-46-4a　　イ XX-XX-XX-f9-48-1b

ウ XX-XX-XX-fb-44-25　　エ XX-XX-XX-ff-ff-ff

設問 4 〔パスワードの解読に関する説明〕について答えよ。

(1) 図 7 中の下線④について，どのような処理か。20 字以内で具体的に答えよ。

(2) 表 10 中の下線⑤について，どのような機能か。40 字以内で具体的に答えよ。

(3) 表 10 中の [p] に入れる適切な攻撃を，解答群の中から選び，記号で答えよ。

解答群

ア Pass the Hash　　イ SHA-1 衝突

ウ 既知平文　　エ レインボーテーブル

(4) 図 8 中の下線⑥はどのような文字列か。システム管理者のパスワードの特徴を踏まえ，40 字以内で具体的に答えよ。

設問 5 〔運用に関する改善提案〕について答えよ。

(1) 図 9 中の下線⑦について，どのような状態か。30 字以内で具体的に答えよ。

(2) 図 9 中の [q] に入れる適切な改善提案を，25 字以内で答えよ。