SC

令和４年度　秋期
情報処理安全確保支援士試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2 時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. 答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。
4. 問題は，次の表に従って解答してください。

問題番号	問１，問２
選択方法	１問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
   (2) 受験番号欄に受験番号を，生年月日欄に受験票の生年月日を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) 選択した問題については，次の例に従って，選択欄の問題番号を○印で囲んでください。○印がない場合は，採点されません。2 問とも○印で囲んだ場合は，はじめの 1 問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問２を選択した場合の例〕

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

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。

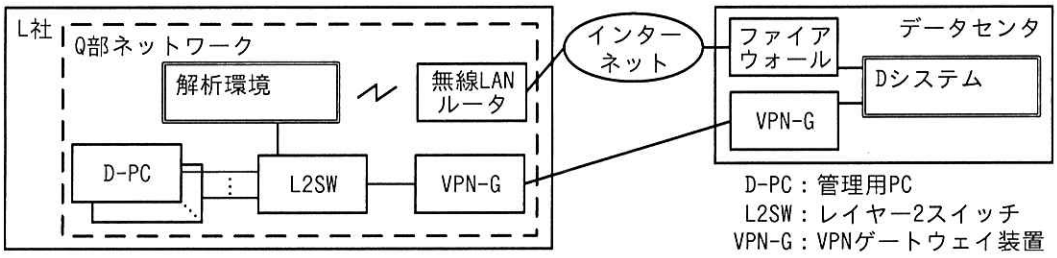


図 1　ネットワークの概要

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。

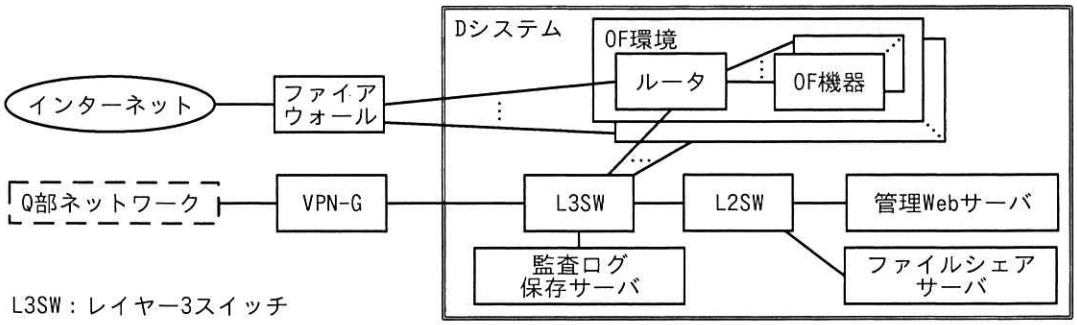


図２　Ｄシステムの概要

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。

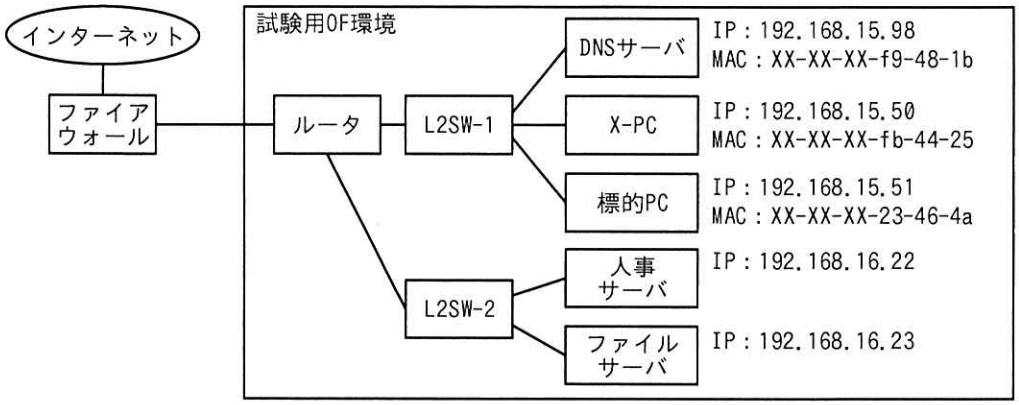


図 6　作成したネットワーク図

(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。

問2　インシデントレスポンスチームに関する次の記述を読んで，設問に答えよ。

K社は，従業員500名の輸入卸売業者である。拠点は，本社，営業所2か所，倉庫1か所の計4か所である。K社のネットワーク及び機器並びに関連する規程の整備は，情報システム課が担当している。K社のネットワーク構成を図1に，各サーバで取得しているログの内容を表1に示す。

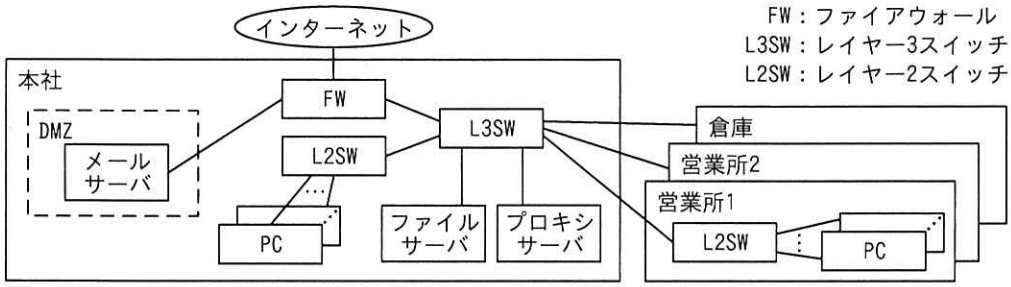


図1　K社のネットワーク構成（抜粋）

表1　ログの内容（抜粋）

サーバ名	ログに記録される項目
メールサーバ	イベントの発生日時，送受信メールの送信元メールアドレス，送受信メールの宛先メールアドレス，メール全体のサイズ，添付ファイルの名称，添付ファイルのサイズ
ファイルサーバ	イベントの発生日時，アクセスされたファイルのパス名，アクセス元のIPアドレス，読込み書込みの種別
プロキシサーバ	イベントの発生日時，アクセス元のIPアドレス，アクセス先のURL，転送したデータのサイズ，アップロードされたファイルのサイズ

〔マルウェアαの検知と対応〕

K社では，PCにマルウェア対策ソフトを導入しており，リアルタイムスキャンとスケジュールスキャンを実施している。マルウェア対策ソフトの管理サーバはクラウドサービス上にある。マルウェア定義ファイルは，PCを起動したときに更新される。スケジュールスキャンは，毎週月曜日の10:00に実施される。

ある月曜日，情報システム課のW主任がスケジュールスキャンの結果を確認したところ，10台のPCでマルウェアαが検出され，駆除されていた。W主任が，マルウェアαについてインターネット上で公開されている情報を調べたところ，次のことが

分かった。

・マルウェアαは，8日前に発見された。

・K社で利用しているマルウェア対策ソフトの定義ファイルにマルウェアαが登録されたのは，昨日だった。

・細工されたマクロ（以下，マクロGという）が仕込まれている，表計算ソフト（以下，Vソフトという）のデータファイル（以下，ファイルGという）を開いて，マクロGを実行してしまうと，攻撃者のWebサーバからマルウェアαがダウンロードされ，起動される。

・マルウェアαは，起動すると，PC上のメールフォルダにある電子メール（以下，電子メールをメールという）を読み出して，攻撃者が用意したWebサーバにアップロードする。その後，OS設定を変更して，OSログイン時にマルウェアαが自動起動されるようにする。

なお，K社で利用しているメールソフトでは，メールは1通が1ファイルとしてPCのメールフォルダ内に保存されている。

マルウェアαが検出されたPCのログと，プロキシサーバのログを調べた結果，これらのPCの中には，先週の水曜日以降，攻撃者のWebサーバのものと思われるURLにファイルをアップロードしていたPCがあったことが分かった。W主任は，調査の結果を上司のM課長に報告した。

M課長から調査と対応の指示を受けたW主任は，K社に機器を納入しているP社に支援を依頼した。依頼に応じたP社の情報処理安全確保支援士（登録セキスペ）であるU氏の協力を得て，W主任は，アップロードされたファイルの特定並びにマルウェアα及びファイルGの削除を進め，調査と対応を完了した。

〔定義ファイルに登録されていないマルウェアの検知〕

マルウェアαへの調査と対応が完了した後，W主任は，マルウェア対策ソフトの定義ファイルに登録されていないマルウェアも検知したいと考え，どうすればよいかU氏に相談した。U氏は，その用途に使用可能な製品として，EDR（Endpoint Detection and Response）があることを説明し，製品Cを提案した。製品Cは，各PCに導入し，クラウドサービス上の管理サーバから操作する。製品Cの機能を表2に示す。

表 2　製品 C の機能（抜粋）

機能名称	機能詳細
イベントの記録機能	PC で起きたイベントを，表 3 に示すイベントの情報とともに記録する。
検知ルールの定義機能	特徴的なイベント又はその並びを，検知ルールとして登録する。複数の検知ルールを登録することができる。検知ルールの仕様を図 2 に，製品 C の製品出荷時に組み込まれている検知ルールを図 3 に示す。
検知機能	PC で起きたイベントが検知ルールに合致したときは，管理サーバから，事前に登録したメールアドレス宛てに警告をメールで送信する。
インシデントレスポンス機能	管理サーバを操作して，指定した PC を対象に，ネットワークからの切離し，OS 設定の変更又は OS コマンドの実行を行う。

表 3　イベントの情報

イベント種別	イベントの情報
ファイル操作	プロセス名，操作種別（読込み，書込み，上書き，削除など），操作されたファイルのパス名・ファイルサイズ・タイムスタンプ・種別（OS のシステムファイル，ログファイルなど）
ネットワーク動作	通信相手先の IP アドレス，サービス，通信の方向，通信データのサイズ，通信相手先の URL，動作種別（ファイルのアップロード，ファイルのダウンロードなど），アップロード又はダウンロードされたファイルのサイズ
プロセス状態の変化	変化種別（開始，終了），プロセス名
OS 設定の変更	変更された設定項目，変更前の値，変更後の値
USB メモリの操作	操作種別（装着，取外し），USB メモリの ID[1)]（以下，USB-ID という）
OS 起動・終了	操作種別（起動，終了）
ログイン操作	操作種別（OS ログイン，OS ログアウト），操作結果

注記　全てのイベントにおいて，発生日時及びイベントを起こした利用者 ID も記録する。
注 1)　USB メモリの識別番号

・検知ルールには，単純ルールと複合ルールの 2 種類がある。
・単純ルールには，一つのイベント内の各イベントの情報を条件として複数組み合わせて指定できる。条件として，値が一致する／しない，範囲内である／ない，列挙された値のいずれかに一致する／いずれにも一致しない，文字列として含まれる／含まれないが指定できる。
・複合ルールは，単純ルール又は複合ルールを組み合わせたものであり，次のようなルールを指定できる。
  - 指定した複数の単純ルールに合致するイベント全てが，指定した時間内に発生した。
  - 指定した単純ルール又は複合ルールに合致するイベントが，指定した時間内に，指定した回数以上発生した。
  - 指定した複数の単純ルール又は複合ルールに合致するイベントが，指定した時間内に，指定した順に発生した。
・複合ルール内で，複数のイベントの間でイベントの情報の値が一致することを条件として指定できる。

図 2　検知ルールの仕様

ルール 1：OS 設定である常駐ソフトのリストに，何らかのソフトウェアが追加された。
ルール 2：OS 設定である常駐ソフトのリストから，何らかのソフトウェアが削除された。
ルール 3：OS のシステムファイルが上書きされた，又は削除された。
ルール 4：ログファイルが削除された。
ルール 5：次の複合ルールが 1 時間以内に 10 回以上発生した。
　- 何らかのファイルが読み込まれた後，1 分以内に，同一のサイズのファイルが HTTP でアップロードされた。

図 3　製品 C の製品出荷時に組み込まれている検知ルール

例えば，マルウェアαは，PC で起きたイベントから製品 C を使って検知できる。マルウェアαの特徴的なイベントは，同じサイズのファイルに対する①ファイル操作のイベント及び②ネットワーク動作のイベント，並びにログイン時の自動起動に関する OS 設定の変更のイベントである。これらのイベントが，短時間のうちにこの順序で発生したことを検知すればよい。

続けて，U 氏は，P 社が提供可能な，製品 C に関連するサービスを表 4 を示して説明した。

表 4　製品 C に関連するサービス（抜粋）

サービス名称	主なサービス内容
解析サービス	・PC のイベントを解析し，解析結果を報告する。
運用サービス	・管理サーバを監視し，正常に稼働していることを確認する。 ・新たな攻撃手法に対応する検知ルールを登録する。
監視サービス	・警告を監視し，明らかな誤検知及び重複を除いて直ちに顧客に連絡する。

W 主任は，次の三つを軸とした EDR 導入案をまとめ，M 課長の承認を得た。

・社内の全 PC に製品 C を導入する。
・製品 C を使ったマルウェアの検知及び対応のための体制（以下，E 体制という）を立ち上げる。
・表 4 の解析サービスは必要に応じて利用するが，その他のサービスは利用しない。

3 か月後，製品 C を全 PC に導入し，E 体制を立ち上げた。E 体制のチームリーダは M 課長，メンバーは W 主任を含む情報システム課の課員 3 名である。

まずは，図 3 の検知ルールだけを用いて試験運用を開始した。

〔マルウェアβの検知〕

製品C導入から6か月ほど経ったある日，マルウェア対策ソフトのスケジュールスキャンの結果を確認したところ，3台のPC（以下，PC1，PC2，PC3という）で同一のマルウェアが検知され，駆除に失敗していた。図4は，製品Cが記録したPC1～3のイベントのうち，PC1～3に共通しており，特徴的と思われたVソフト及びUSBメモリに関するイベントを，OSログインのイベントとともに抜粋したものである。

PC1

```
5月19日(木)
 14:27 OSログイン
 15:03 USBメモリ装着
 15:15 ファイルコピー
   E:¥file1.v→C:¥file1.v
 15:16 USBメモリ取外し
 15:18 V-開始
 15:18 V-読込 C:¥file1.v
 15:18 V-読込 N:¥file2.v
 15:18 V-書込 N:¥file2.v
 15:25 V-書込 C:¥file1.v
 15:26 V-終了


5月20日(金)
 動作記録なし
```

PC2

```
5月19日(木)
 13:05 OSログイン
 13:15 USBメモリ装着
 13:16 ファイルコピー
   E:¥file3.v→C:¥file3.v
 13:17 USBメモリ取外し
 16:47 V-開始
 16:48 V-読込 C:¥file3.v
 16:49 V-終了
 17:12 V-開始
 17:25 V-読込 N:¥file2.v
 17:25 V-読込 C:¥file6.v
 17:25 V-書込 C:¥file6.v
 17:43 V-終了
5月20日(金)
 11:14 OSログイン
 11:15 V-開始
 11:15 V-読込 C:¥file6.v
 11:15 V-読込 C:¥file8.v
 11:15 V-書込 C:¥file8.v
 11:15 V-終了
 11:22 V-開始
 11:24 V-読込 C:¥file3.v
 11:43 V-終了
```

PC3

```
5月19日(木)
 09:57 OSログイン
 10:10 V-開始
 10:13 V-読込 N:¥file2.v
 10:25 V-書込 N:¥file2.v
 10:35 V-読込 C:¥file4.v
 10:40 V-終了
 16:30 USBメモリ装着
 16:35 ファイルコピー
   C:¥file4.v→E:¥file4.v
 16:39 USBメモリ取外し



5月20日(金)
 13:32 OSログイン
 14:36 V-開始
 14:39 V-読込 N:¥file2.v
 14:39 V-読込 C:¥file4.v
 14:39 V-書込 C:¥file4.v
 15:03 V-終了
 15:46 V-開始
 15:48 V-読込 C:¥file7.v
 16:23 V-終了
```

V-開始：Vソフトのプロセス開始　V-終了：Vソフトのプロセス終了
V-読込 ○○：Vソフトでファイル○○を読込み
V-書込 △△：Vソフトでファイル△△を書込み又は上書き
注記1 C:は，内蔵SSDに割り当てられたドライブ名である。
注記2 E:は，USBメモリを装着した場合に割り当てられたドライブ名である。
注記3 N:は，ファイルサーバ上の同じ共有フォルダに割り当てられたドライブ名である。
注記4 ファイルの拡張子“v”は，Vソフトのデータファイルの拡張子である。
注記5 PC1～3に装着されたUSBメモリは，それぞれ異なるUSBメモリである。

図4　製品Cが記録したPC1～3のイベント（抜粋）

W主任は，調査のためP社に解析サービスを発注し，図4のイベントの解析を依頼した。

P社は，推測した状況を表5のとおり報告した。

表5　P社による推測

発生順序	日時	事象
1	5月19日(木) [a]	USB メモリが，[b] に装着された。その USB メモリには，[c] というファイルが存在していたが，そのファイルにはマルウェアβという新種のマルウェアが潜んでいた。
2	(省略)	[c] が [b] の C ドライブにコピーされた。
3	(省略)	C ドライブ上の [c] を開いて，マクロを実行したところ，マルウェア β が起動した。その直後に，ファイル利用履歴の中から選ばれたと思われる [d] というファイルが開かれ，マルウェア β がマクロとして埋め込まれた後，直ちに上書き保存された。
4	(省略)	[e] 上で，利用者が [d] を開いて，マクロを実行したので，[e] にも感染が広がった。
5	(省略)	さらに，3台目の PC にも感染が広がった。
6	5月23日(月) 10:00	5月22日に更新されたマルウェア定義ファイルにマルウェア β が登録されたので，スケジュールスキャンによって PC1～3 の C ドライブでマルウェア β が検知された。(駆除失敗の理由については省略)

P 社の報告を受けた W 主任は，③マルウェア β が埋め込まれたファイルの削除など必要な対応を完了した。P社がマルウェア β の検体を静的解析したところ，表5の発生順序3～5の事象について裏付けが取れた。また，マルウェア β は，追加のマルウェアをダウンロードする機能をもっていたが，ダウンロードに失敗していたことも分かった。その後，U氏は，“P社の運用サービスでは，このような場合は，すぐに検知ルールを作成し，登録します”と W 主任に提案した。

〔運用サービスの利用〕

K 社は，マルウェアをより早期に検知するために有効かどうかを確認しようと考え，表4のサービスについての当初の方針を変えて，3か月ほど試験的に P 社の運用サービスと監視サービスを利用することにした。P 社は，まず，④マルウェア β と同じ手段による感染の拡大を検知するための検知ルールを作成して製品 C に登録した。その後2週間，V ソフトの正常なデータファイルを開くといった，PC の通常利用に起因する誤検知が起きないか確認を続けた。

サービス利用開始から1か月後，ある従業員がメールに添付されていた V ソフトのデータファイルを開いて，マクロを実行した直後にマルウェア β の亜種を検知する

ことができた。さらに，E 体制のメンバーが直ちに必要な対応を指示することによって被害の拡大も防ぐことができた。

〔運用体制の組替え〕

試験期間が終了し，K 社は，運用サービス及び監視サービスを正式に利用することにした。それらに加え，インシデント対応を円滑に行うために，被害状況の把握及び侵入経路の特定を行う P 社のインシデント対応支援サービスも利用することにした。

インシデント対応支援サービスの利用には，インシデントレスポンスチーム（以下，IRT という）の整備が前提となっている。M 課長は，IRT の体制案をまとめ，経営層の承認を得た。IRT では，通常時は，1 名が通報窓口の要員として対応する。招集時は，情報システム課，営業所 1，営業所 2 及び倉庫の従業員計 10 名が参加する。

M 課長は，W 主任にインシデント対応の流れを整理して，必要となる規程及び通報窓口の要員が社内から通報を受けるための通報専用メールアドレスを整備するように指示した。また，規程を整備する際は，インシデントの重大さ（以下，レベルという）を定義し，レベルに応じて対応に必要な体制が変わることに注意するように付け加えた。

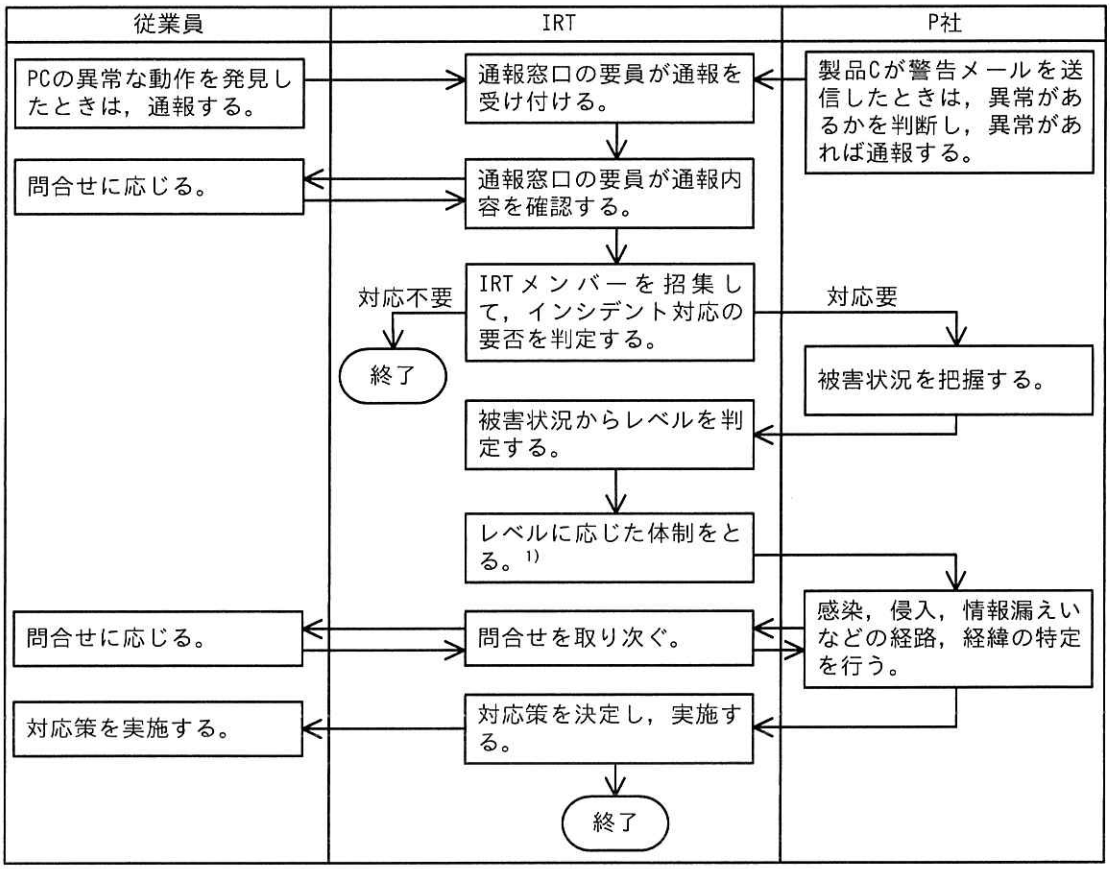
W 主任は，レベルの判定の際に使用する基準の案を図 5 に，マルウェアによる情報漏えいを想定したインシデント対応の流れの案を図 6 にまとめ，M 課長に提出した。M 課長は，図 5 と図 6 の案を承認して IRT の活動を開始した。

1. レベルは，緊急，重要，軽微の 3 段階とし，次の表によって判定する。

	影響の深刻さ：大	影響の深刻さ：中	影響の深刻さ：小
影響の広がり：大	緊急	緊急	重要
影響の広がり：中	緊急	重要	軽微
影響の広がり：小	重要	軽微	軽微

2. 影響の深刻さは，インシデントの事業への影響に基づいて判定する。
   大：一部の事業が継続できない可能性がある。
   中：一部の事業の継続に影響がある。
   小：事業活動でよく起きる程度の影響である。
3. 影響の広がりは，インシデントのシステムへの影響に基づいて判定する。
   大：サーバ複数台，又は PC 30 台以上が影響を受ける。
   中：サーバ 1 台，又は PC 10 台以上が影響を受ける。
   小：PC 1 台以上 10 台未満が影響を受ける。

図 5　レベル判定基準（案）



注 1) レベルが緊急の場合は，IRT 全員の体制とする。重要の場合は，IRT メンバー5 名の体制とする。軽微の場合は，IRT メンバー2 名の体制とする。レベルが緊急の場合は経営層に報告する。

図 6　インシデント対応の流れ（案）

〔秘密ファイルの流出〕

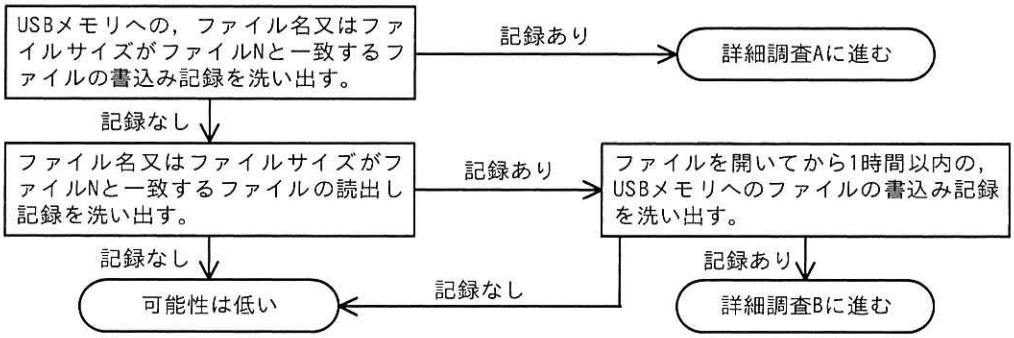
IRT の体制が整った 1 週間後の 9 月 29 日，社内からの通報専用メールアドレス宛てにある従業員からメールが届いた。そのメールの内容は，“S 社が提供するオンラインストレージサービスである S サービスにおいて，K 社の取扱商品の価格表（以下，ファイル N という）と思われるファイルが一般公開されていて，仕入原価も記載されていると 9 月 26 日に取引先から連絡があった”というものだった。メールを見た通報窓口の要員は IRT 全員を招集して会議を開催しようとしたが，日程調整が難航し，開催できたのは 10 月 4 日だった。10 月 3 日には，営業部門から，“顧客から，S サービスで公開されているファイルについて苦情が来ているので対応を急いでほしい”と，M 課長に抗議が来ていた。

会議の中で，S サービスで公開されているファイルが，秘密情報に該当するファイルNであることを確認した。ファイルNに含まれている商品の売上高は全社の売上高の 5%であった。IRT では，インシデント対応要と直ちに判断して，まず S 社にファイルの公開停止を依頼した。続いて，P 社に解析サービスを発注して PC のマルウェア感染の調査を依頼した。1 時間後，P 社から，“製品 C の記録を確認したが，マルウェアのものと思われるイベントは発見できない”との報告があった。これらの状況を基にレベルの判定を行おうとしたが，“影響の広がり”の区分のどれにも該当しないので，とりあえず“軽微”と判定した。その後，インシデント対応支援サービスを利用して，ファイルNの公開の経緯の特定を依頼した。

最初に P 社は，K 社のほかのファイルが S サービスで公開されていないかどうかを調査した。ファイルN以外に，価格表が幾つか公開されていたが，いずれも公開されても差し支えないものであった。これらは，アップロード日時からファイルNと同時にアップロードされたものだと推測できた。念のため，マルウェア α 及びマルウェア β の再感染も調査したが，その形跡はなかった。その後，ファイル N が公開された経緯として可能性の高いものを四つ，表 6 に示すとおりに想定して順に調査した。

表 6　ファイルNが公開された経緯の想定

項番	公開された経緯	調査方法
想定 1	従業員が，攻撃者にだまされた結果，又は意図的に，ファイル N を攻撃者のメールアドレスに送信し，攻撃者が S サービスにアップロードした。	メールサーバのログについて，［ f ］又は［ g ］が，ファイル N と一致するものを洗い出す。
想定 2	従業員が，攻撃者にだまされた結果，又は意図的に，HTTP で攻撃者のサーバにファイルNをアップロードし，攻撃者が S サービスにアップロードした。	プロキシサーバのログについて，ファイル N の［ h ］と，［ i ］が一致するものを洗い出し，その［ j ］が信頼できるサイトのものかどうか確認する。
想定 3	ファイルサーバが不正アクセスを受けて，何らかの方法で攻撃者のサーバにファイル N が送信され，攻撃者が S サービスにアップロードした。	ファイルサーバのログについて，製品 C の記録と突き合わせて一致しないものを洗い出す。
想定 4	従業員が，USB メモリにファイル N を書き込み，社外に持ち出してから S サービスにアップロードした。	図 7 に示す調査計画に従って各 PC を調査する。



注記　詳細調査 A 及び詳細調査 B は，想定 4 が実際に起きたかどうかを確認するための調査であり，PC 内のファイルの調査及びログの突合せを行うものである。

図 7　想定 4 の調査計画

P 社が調査を進めた結果，想定 1～3 の可能性は低いことが分かったので，想定 4 について調査を進めた。

調査の中間報告のために，U 氏が K 社を訪問した。W 主任は U 氏に，図 7 で“詳細調査 B に進む”と判定されるのは，従業員がどのような操作をして，どのようなファイルを USB メモリに書き込んだ場合が考えられるか聞いた。U 氏は，従業員がファイルを書き込む際に，［ k ］という操作をして，ファイル N と同じ内容が含まれるものの，［ l ］及び［ m ］が異なるファイルへと変換した場合が考えられると答えた。

〔原因の特定〕

図 7 に基づく調査では，従業員の J さんが使用している PC だけが詳細調査 A に進み，そのほかの PC は全て可能性は低いとの結果になった。P 社から報告を受けた IRT では，J さんに聞き取り調査を行った結果，公開可能な価格表ファイルを持ち出すために，個人所有の USB メモリにファイルをコピーした時に，誤ってファイル N もコピーしてしまい，その後 USB メモリを紛失していたことが分かった。

IRT では，紛失した USB メモリを手に入れた何者かが，ファイル N を含む幾つかの価格表を S サービスにアップロードしたと推測した。今回のインシデントはこれ以上被害が拡大することはないと考え，インシデント対応は完了とした。体制不足もあり，取引先からの連絡から，インシデント対応完了までに 12 日間掛かった。

〔再発防止〕

M 課長は，ファイル持出しに起因する同様のインシデントの再発を防止するためには，個人所有の外部記憶媒体の使用制限を含めた対策が必要であると考え，必要な規程を策定するように W 主任に指示した。W 主任は，規程案を図 8 のとおりにまとめ，M 課長に提出した。

［業務で使用する USB メモリの指定］
・業務で使用する外部記憶媒体は，情報システム課が調達する USB メモリに限定する。調達した USB メモリの USB-ID は情報システム課が管理する。
・USB メモリは，必要時に情報システム課から借用し，利用終了後速やかに返却する。

［秘密ファイルの指定］
・秘密情報に該当するファイルは，ファイル名の先頭に“【秘密】”又は“(CONFIDENTIAL)”の文字列を付加する。

［秘密ファイルの持出し］
・秘密ファイルを社外に持ち出す場合は，暗号化した上で，情報システム課から借用した USB メモリに保存し，各部門で用意した秘密ファイル持出台帳に記録する。
・暗号化には，表計算ソフトなどの暗号化機能，又は AES を使用したファイル暗号化ツールを利用する。パスワードは十分な長さの推測困難なものを設定する。
・秘密ファイル持出台帳は，電子ファイルとしてファイルサーバに保管する。

図 8　規程案（抜粋）

M 課長は，この規程案を承認するとともに，情報システム課が管理する USB-ID を P 社に伝え，この規程に違反する持出しを製品 C で検知するように P 社に依頼した。P 社は，違反する持出し操作のうち製品 C で検知可能な操作について⑤新たな検知ルールを作成して，製品 C に登録した。一方，製品 C で検知できない操作については，別の対策を提案した。

〔事後評価〕

インシデント対応について，P 社と K 社が合同で見直しを実施した。この見直しの結果を受けて，M 課長は幾つかの修正を W 主任に指示した。W 主任は修正案を表 7 のとおりまとめた。

表7　インシデント対応についての修正案（抜粋）

項番	方針	具体的内容
1	IRTでの通報受付を早めるために，通報窓口を見直す。	n
2	図5中の“影響の広がり”の判定基準を見直す。	（省略）
3	インシデント対応の開始を早めるために，図6を見直す。	通報の受付時には，IRTメンバー全員の集合を待たず，最低限のメンバーが集合した時点で対応を開始するかどうかを決定する。
4	体制のとり方を見直すために，レベルの判定のタイミングを見直す。	o

M課長は，これらの案を承認し，後日正式な規程とした。

設問1　本文中の下線①，②について，検知するための単純ルールを，それぞれ30字以内で具体的に答えよ。

設問2　〔マルウェアβの検知〕について答えよ。

(1)　表5中の［a］～［e］に入れる適切な時刻，ファイル名又はPC名を答えよ。

(2)　本文中の下線③について，PC1～3の内蔵SSD及びファイルサーバから削除すべきファイルは何か。解答群から全て選び，記号で答えよ。

解答群

ア　PC1のC:¥file1.v　　イ　PC2のC:¥file3.v　　ウ　PC2のC:¥file6.v

エ　PC2のC:¥file8.v　　オ　PC3のC:¥file4.v　　カ　PC3のC:¥file7.v

キ　共有フォルダ内のfile2.v

設問3　本文中の下線④について，作成した検知ルールを60字以内で答えよ。

設問4　〔秘密ファイルの流出〕について答えよ。

(1)　表6中の［f］，［g］に入れる適切なログの項目名を，表1から選び答えよ。

(2)　表6中の［h］に入れる適切な字句を答えよ。

(3)　表6中の［i］，［j］に入れる適切なログの項目名を，表1から選び答えよ。

(4)　本文中の［k］～［m］に入れる適切な字句を，それぞれ10

字以内で答えよ。

設問5　本文中の下線⑤について，新たに作成した検知ルールを 60 字以内で答えよ。

設問6　表 7 中の［　n　］，［　o　］に入れる適切な字句を，［　n　］は 30 字以内で，［　o　］は 50 字以内でそれぞれ答えよ。

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

7. 問題に関する質問にはお答えできません。文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。