SC

平成30年度　春期
情報処理安全確保支援士試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

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3
選択方法	2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。3問とも○印で囲んだ場合は，はじめの2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1，問3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　ソフトウェアの脆弱性に関する次の記述を読んで，設問1～9に答えよ。

V社は，従業員数100名のソフトウェア開発会社である。V社では，開発に関わる全員が情報セキュリティを意識した実装を行えるよう，開発経験が浅い従業員にセキュリティ教育を行っている。次は，任意の攻撃コードが実行され得る脆弱性について，開発チームのT主任が部下のUさんに教えていた時の会話である。

T主任：任意の攻撃コードが実行され得る脆弱性は幾つかある。確保済みメモリ領域を超えてデータを書き込んでしまう［　a　］と呼ばれる脆弱性の報告が以前から多かった。最近は解放したメモリ領域を後から使用してしまう［　b　］と呼ばれる脆弱性の報告も多くなってきている。

Uさん：［　b　］という脆弱性は具体的にはどのようなものなのですか。

T主任：例えば，図1のC++ソースコードからなるプログラム（以下，例示プログラムという）があったとする。例示プログラムは，図2に示すシステム構成の中で動作し，ノートと呼ぶメモ書き機能を実現するものであり，クライアントから利用者が自身の名前とメッセージを登録したり，それを他の利用者が参照したりする。例示プログラムでは，ノートはNote構造体で表現され，利用者の操作に応じて，NoteManagerクラスの各メンバ関数が個別に呼び出される。各メンバ関数では，ノートの生成（CreateNote），利用者の名前の登録（RegisterName），メッセージの登録（RegisterMsg），ノートの登録内容表示（DisplayNote），ノートの破棄（DeleteNote）を行う機能を実装している。例示プログラムにおいて，DeleteNoteメンバ関数内でm_noteの指すメモリ領域を解放しているが，仮にDeleteNoteメンバ関数が呼び出された直後にRegisterNameメンバ関数が呼び出されると，解放したm_noteの指すメモリ領域にアクセスできてしまう。これが［　b　］という脆弱性だ。例示プログラムでは，悪意をもつ利用者（以下，攻撃者という）の操作によって，任意の攻撃コードを実行され，サーバを乗っ取られてしまうおそれがある。

```
 1: #include <cstdio>
 2:
 3: struct Note{
 4:   char *name;
 5:   char *msg;
 6: };
 7:
 8: class NoteManager{
 9:   Note *m_note;
10: public:
11:   NoteManager(){ m_note = NULL; }
12:   void CreateNote(){
13:     if(m_note = new Note()){
14:       m_note->name = NULL;
15:       m_note->msg = NULL;
16:     }
17:   }
18:   void RegisterName(){
19:     if(m_note && !m_note->name) m_note->name = new char[8];
20:     if(m_note && m_note->name){
21:       printf("Input name: ");
22:       scanf("%7s%*[^¥n]%*c", m_note->name);
23:     }
24:   }
25:   void RegisterMsg(){
26:     if(m_note && !m_note->msg) m_note->msg = new char[100];
27:     if(m_note && m_note->msg){
28:        printf("Input message: ");
29:        scanf("%99s%*[^¥n]%*c", m_note->msg);
30:     }
31:   }
32:   void DisplayNote(){
33:     if(m_note && m_note->name) printf("Name: %s¥n", m_note->name);
34:     if(m_note && m_note->msg) printf("Message: %s¥n", m_note->msg);
35:   }
36:   void DeleteNote(){
37:     delete[] m_note->name;
38:     delete[] m_note->msg;
39:     delete m_note;
40:   }
41: };
42: (省略)
```

注記　メモリアドレスが32ビットの環境で動作させるものとする。

図1　脆弱性が存在するC++ソースコード

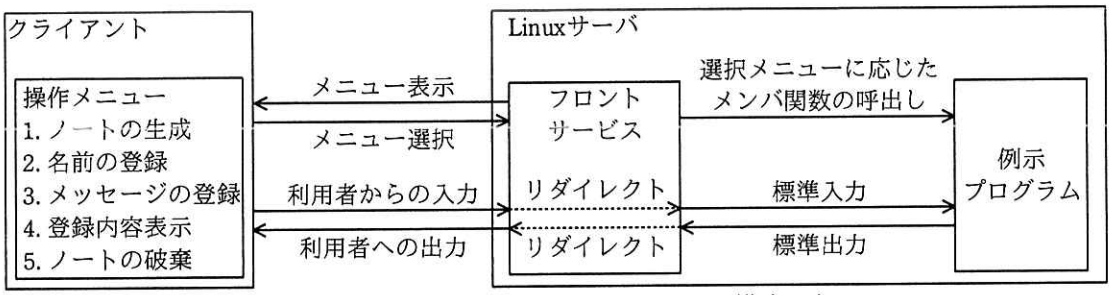
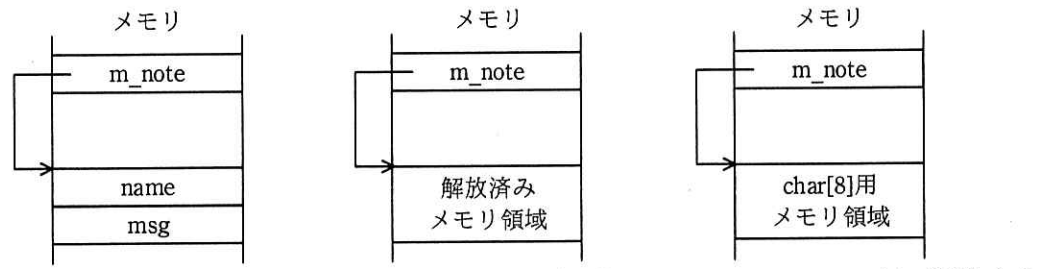


図 2　例示プログラムが動作するシステム構成の例

U さん：解放したメモリ領域にアクセスされると，どのように攻撃コードが実行されるのですか。

T 主任：例示プログラムにおいて，図 3 に示す(1)~(3)の順でメンバ関数の呼出しが行われたとしよう。その場合，図 3 の(1)で確保されていた Note 構造体用のメモリ領域と，図 3 の(3)で確保された char[8]用のメモリ領域が同じアドレスに割り当てられる可能性がある。その場合，①RegisterName メンバ関数内で読み込まれる攻撃者からの入力値によって，元々Note 構造体用であったメモリ領域が上書きされる。このときの攻撃者からの入力値がうまく細工されていると，②次に RegisterName メンバ関数が呼ばれた際，その際に読み込まれる攻撃者からの入力値が，攻撃者の指定したアドレスに書き込まれることになる。このように，攻撃者からの入力値が攻撃者の指定したアドレスに書き込まれる場合には攻撃コードが実行され得る。



(1) CreateNoteメンバ関数実行後　(2) DeleteNoteメンバ関数実行後　(3) RegisterNameメンバ関数内のnew実行後

図 3　脆弱性を悪用する関数呼出しの過程とメモリマップ

Uさん：もう少し具体的に説明してください。

T主任：関数テーブルの例で説明しよう。ここでいう関数テーブルとは，プログラム中で呼び出している共有ライブラリに含まれる関数（以下，ライブラリ関数という）の実行コードの先頭アドレスが記録されたテーブルだ。ライブラリ関数の呼出し時には，図 4 に示すように関数テーブルに記録された実行コードの先頭アドレスの値を参照してライブラリ関数の実行コードに処理が遷移する。

図4　ライブラリ関数の呼出し時の動き

T主任：攻撃者が既に，攻撃コードをメモリ上に書き込んでいるとしよう。この状態で，例えば，攻撃コードが存在するアドレスを関数テーブルに書き込まれた場合，関数の呼出し時に関数テーブルが参照されると，攻撃コードに処理が遷移してしまう。

Uさん：例示プログラムを攻撃する場合だと，関数テーブルに書き込むアドレスは具体的にどのような値になりますか。

T主任：例えば，RegisterMsg メンバ関数の呼出しによって m_note->msg が指し示すメモリ領域に攻撃コードが書き込まれていて，その先頭アドレスが 0x0b123400 と分かっていたとする。その場合，関数テーブルが表 1 に示すようになっていたとすると，アドレス［　c　］番地に値［　d　］を書き込むことによって，次に CreateNote メンバ関数が呼び出された際，攻撃コードに処理が遷移することになる。

表1　関数テーブル

アドレス	値	値の意味
（ア）0x08049e30	（キ）0xf7cfcd70	delete の実行コードの先頭アドレス
（イ）0x08049e38	（ク）0xf7ce9370	scanf の実行コードの先頭アドレス
（ウ）0x08049e3c	（ケ）0xf7cd7670	printf の実行コードの先頭アドレス
（エ）0x08049e40	（コ）0xf7cff150	new の実行コードの先頭アドレス
（オ）0x08049e44	（サ）0xf7cff230	new[]の実行コードの先頭アドレス
（カ）0x08049e4c	（シ）0xf7cfcdd0	delete[]の実行コードの先頭アドレス

U さん：RegisterMsg メンバ関数の呼出しによって入力された攻撃コードは［　e　］領域に書き込まれるので，データ実行防止と呼ばれる機能が有効化されていた場合，実行されませんよね。

T 主任：確かにそのとおりだ。ただし，③関数テーブルに書き込むアドレスとして，例えば，共有ライブラリ内のメモリアドレスを選べば，データ実行防止が有効化されていた場合でも，攻撃者が任意の処理を実行できる可能性がある。例示プログラムにおいて，共有ライブラリ内のメモリアドレスが表 2 のようになっていたとすると，関数テーブルに書き込むアドレスを［　f　］番地にすることによって，データ実行防止が有効化されていた場合でも，/bin/sh を起動して任意のシェルコマンドを実行できる可能性がある。

表2　共有ライブラリ内のメモリアドレス

アドレス	内容
（ア）0xf7cc8da0	system の実行コード
（イ）0xf7cd7670	printf の実行コード
（ウ）0xf7ce9370	scanf の実行コード
（エ）0xf7cfcd70	delete の実行コード
（オ）0xf7cfcdd0	delete[]の実行コード
（カ）0xf7cff150	new の実行コード
（キ）0xf7cff230	new[]の実行コード
（ク）0xf7de99ab	"/bin/sh"の文字列

U さん：共有ライブラリ内のメモリアドレスは，表 2 のように前もって知ることができるものなのですか。

T 主任：共有ライブラリをメモリに読み込む際，それを配置するアドレスを毎回ラン

ダムに選ぶASLR（Address Space Layout Randomization）と呼ばれるセキュリティ機能がある。この機能が有効な場合，共有ライブラリ内のメモリアドレスを前もって知ることは難しい。しかし，例示プログラムにおいて，図3の(3)の状態をつくり出せれば，RegisterNameメンバ関数と［ g ］メンバ関数を利用することによって，ASLRが有効化されていた場合でも，共有ライブラリ内のメモリアドレスを特定できる可能性がある。データ実行防止やASLRなどは効果的な機能ではあるが，根本的な対策にはならない。やはり脆弱性そのものを修正することが重要だ。

U さん：では，［ b ］の脆弱性を修正するには，例示プログラムではどうすればよいのでしょうか。

T 主任：図1の39行目の直後に［ h ］という1文を加えればよいだろう。

U さんは，今回学んだことをコードレビューの観点として生かしていくことにした。

設問1　本文中の［ a ］，［ b ］に入れる適切な脆弱性名を，解答群の中から選び，記号で答えよ。

解答群

ア　CSRF	イ　SQLインジェクション
ウ　Use-After-Free	エ　クロスサイトスクリプティング
オ　コマンドインジェクション	カ　バッファオーバフロー
キ　フォーマットストリングバグ	ク　レースコンディション

設問2　本文中の下線②のようになるためには，本文中の下線①で読み込まれる攻撃者からの入力値はどのような値である必要があるか。攻撃者の指定したアドレスを0x12345678，改行コードを0x0aとした場合について，入力値の具体的なバイト列を14字以内の16進数文字列で答えよ。ここで，アドレスは32ビットであり，バイトオーダがリトルエンディアンのバイトマシンによって扱われるものとする。

設問3　本文中の［ c ］に入れる適切なアドレスを表1中の（ア）～（シ）から選び，記号で答えよ。

設問4　本文中の［ d ］に入れる適切な値を16進数で答えよ。

設問5　本文中の［ e ］に入れるメモリ領域の名称を答えよ。

設問6　本文中の下線③の理由を，45字以内で述べよ。

設問7　本文中の［ f ］に入れる適切なアドレスを表2中の（ア）～（ク）から選び，記号で答えよ。

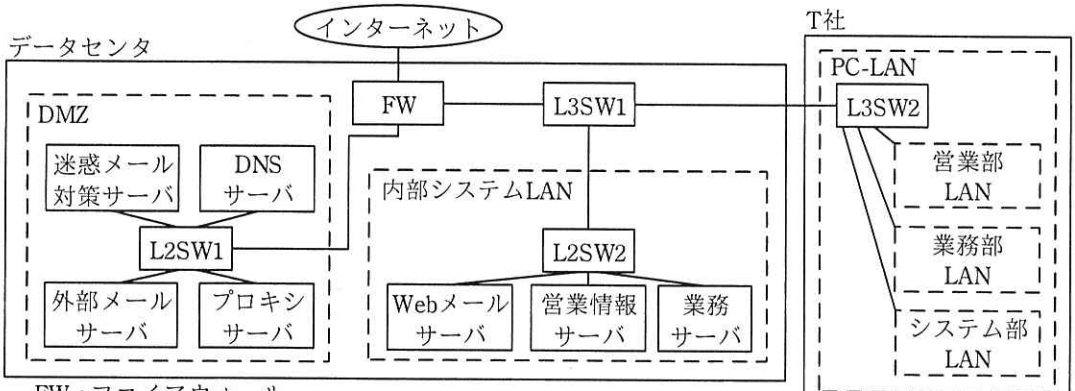
設問8　本文中の［ g ］に入れるメンバ関数の名前を答えよ。

設問9　本文中の［ h ］に入れる適切なソースコードを答えよ。

問2　情報セキュリティ対策の強化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300名の小売業者である。

T社のネットワーク構成を図1に示す。



FW：ファイアウォール
L2SW：レイヤ2スイッチ
L3SW：レイヤ3スイッチ
注記　PCの記載は省略している。

図1　T社のネットワーク構成

T社は，全ての従業員にPCを1台ずつ貸与している。PCは全て，営業部LAN，業務部LAN及びシステム部LANのいずれかに接続されている。PC及び内部システムLANのサーバには，固定のプライベートIPアドレスを割り当てている。

T社では，電子メール（以下，メールという）の送受信及びWeb閲覧にインターネットを利用している。T社のドメイン名は，t-sha.co.jp（以下，T社ドメイン名という）である。また，全ての従業員は，T社ドメイン名のメールアカウントをもつ。

T社では，PC及びサーバを導入する際，システム部がアプリケーションソフトウェア，L社製マルウェア対策ソフト及びOS（以下，これらを併せてT社標準ソフトという）のインストール，脆弱性修正プログラムの適用，並びにマルウェア定義ファイルの最新化を行う。導入後のPC及びサーバは，プロキシサーバ経由でT社標準ソフトの各ベンダのサイトに毎月1回自動で接続し，それぞれの脆弱性修正プログラムを適用している。マルウェア定義ファイルは，1時間おきに最新化している。

〔内部システム LAN 上のサーバの概要〕

T 社の内部システム LAN とその LAN 上のサーバは，システム部の K さんが運用業務を担当している。内部システム LAN 上のサーバの機能の概要を表 1 に示す。表 1 に示す機能は全て有効にしている。

表 1　内部システム LAN 上のサーバの機能の概要（抜粋）

サーバ名	IP アドレス	機能の概要
Web メールサーバ	192.168.1.11	・SMTP で，迷惑メール対策サーバからのメールを受信するメール受信機能がある。 ・外部メールサーバに，SMTP でメールを転送するメール転送機能がある。 ・PC から Web ブラウザによってメールを送受信できるようにする Web メール機能，及びメールボックス機能がある。Web ブラウザとの通信プロトコルとして HTTP を用いる。 ・SMTP 通信及び HTTP 通信のマルウェアスキャンを行うマルウェアスキャン機能がある。 ・IP アドレス単位に，HTTP による接続を拒否することができる HTTP 接続拒否機能がある。その機能を用いて，内部システム LAN 上の他のサーバからの接続を拒否している。 ・送信メールについて，送信者メールアドレスをメールアカウントに対応付ける送信者メールアドレス詐称防止機能がある。 ・インターネットへの送信メールについて，送信者メールアドレスごとにインターネットへの送信の可否を設定できるインターネットメール送信制限機能がある。業務上，インターネットへの送信の必要がある者の送信者メールアドレスに対してインターネットへの送信を許可している。 ・DNS 機能がある。社内専用のドメイン名を管理する。インターネット上のドメイン名の名前解決は行わない。

運用業務において，内部システム LAN 上のサーバへのログインには，SSH を利用している。

〔DMZ 上のサーバ及び FW の概要〕

DMZ 上のサーバには，固定のグローバル IP アドレスを割り当てている。DMZ 上のサーバで，プログラムが異常停止するなどのエラーが発生した場合，迷惑メール対策サーバを経由してシステム部の運用担当者のメールアドレス宛てに通知している。

DMZ 上のサーバの機能の概要を表 2 に示す。表 2 に示す機能は全て有効にしている。

表 2　DMZ 上のサーバの機能の概要

サーバ名	IP アドレス	機能の概要
迷惑メール対策サーバ	x1.y1.z1.2	・受信したメールを Web メールサーバに SMTP で転送する機能がある。 ・インターネットからのメールの受信において，SPF（Sender Policy Framework）を用いてメールの転送を許可又は拒否する機能がある。 ・インターネットからのメールの受信において，メールの件名及び本文の内容によって迷惑メールと判定したメールを破棄する機能がある。
DNS サーバ	x1.y1.z1.3	・インターネット向けの T 社ドメイン名を管理する機能がある。 ・インターネット上のドメイン名の名前解決を行う機能がある。 ・オープンリゾルバ防止機能がある。
外部メールサーバ	x1.y1.z1.4	・転送されてきたメールをインターネットに SMTP で転送する機能がある。
プロキシサーバ	x1.y1.z1.5	・PC 及びサーバからインターネットへの HTTP 及び HTTP over TLS（以下，HTTPS という）通信を中継するプロキシ機能がある。HTTPS 通信の中継には，CONNECT メソッドを利用する。 ・送信元 IP アドレスごとにプロキシサーバへの接続可否を設定できる接続元制限機能がある。現在の設定は，T 社のネットワーク内の IP アドレスからの接続だけを許可している。 ・送信元 IP アドレスごとに接続可能な URL を制限するアクセス制限機能がある。現在は，全ての URL への接続を許可している。 ・プロキシサーバからの接続を許可する宛先ポート番号を設定するポート制限機能がある。現在は，1023 以下の宛先ポート番号だけを許可している。

運用業務において，DMZ 上のサーバへのログインには，SSH を利用している。

DNS サーバに登録されている，T 社ドメイン名に対する TXT レコードの設定内容を図 2 に示す。

```
t-sha.co.jp.      IN TXT "v=spf1 +ip4:[    a    ] -all"
```

図 2　T 社ドメイン名に対する TXT レコードの設定内容

FW は，ステートフルパケットインスペクション型である。そのフィルタリングル

ールを表3に示す。

表3　FWのフィルタリングルール

項番	送信元	宛先	サービス	動作	ログ取得
1	インターネット	b	SMTP	許可	する
2	b	c	SMTP	許可	する
3	c	d	SMTP	許可	する
4	d	インターネット	SMTP	許可	する
⋮	⋮	⋮	⋮	⋮	⋮
25	全て	全て	全て	拒否	する

注記1　項番が小さいルールから順に，最初に合致したルールが適用される。
注記2　項番5～24はSMTP以外のサービスに関するルールであり，PC及び内部システムLAN上のサーバと，インターネットの間の通信を許可するものはない。

〔セキュリティ対策の見直し〕

同業他社で，運用担当者のPCがマルウェアに感染し，サーバに格納されていた個人情報が大量に漏えいする事故が発生した。T社の経営陣は事態を重く見て，現状の対策の点検と見直しをシステム部のJ部長に指示した。J部長は，サーバの設定の点検及び見直し並びに運用担当者のPCの利用方法の見直しを行うようにKさんに指示した。さらに，セキュリティ専門業者に助言を求めることにし，情報処理安全確保支援士（登録セキスペ）のW氏が担当することになった。

〔サーバの設定の点検及び見直し〕

Kさんは W氏の支援を受けて，表4に示すサーバの設定のチェックリストを作成した。

表4　サーバの設定のチェックリスト（抜粋）

サーバ名	機能名	チェック内容
DNSサーバ	オープンリゾルバ防止機能	DNSサーバがeを許可するのは，DMZ上の他のサーバからだけであること
プロキシサーバ	接続元制限機能	DMZ上のサーバ，内部システムLAN上のサーバ及びPC-LAN上のPCだけが，プロキシサーバに接続可能であること
	ポート制限機能	接続を許可すべき宛先ポート番号を設定していること

表 4 に基づいて点検していたところ，プロキシサーバのポート制限機能に問題があることが分かった。次は，プロキシサーバのポート制限機能の利用方法に関する，W 氏と K さんの会話である。

W 氏　：プロキシサーバの設定をみると，CONNECT メソッドの悪用を防ぐ制限がなされていませんね。

K さん：CONNECT メソッドを悪用すると，どういう問題が生じるのでしょうか。

W 氏　：図 3 に示すように，CONNECT メソッドを悪用してトンネルを確立させることで，Web メールサーバの機能を回避できます。そして，①この回避によっていくつかの問題が生じます。

K さん：ポート制限機能に関する設計の見直しと設定変更案を作成します。

```
CONNECT x1.y1.z1.4:25 HTTP/1.1
```

図 3　CONNECT メソッドを悪用したリクエスト

K さんと W 氏は，サーバの点検を続け，他に問題がないことを確認した。

〔運用担当者の PC の利用方法の見直し〕

引き続き K さんと W 氏は，運用担当者の PC の利用方法の見直しを行った。

運用担当者は，運用担当者の PC からサーバに特権 ID でログインしているので，PC がマルウェアに感染した場合，サーバの重要な情報が窃取されるおそれがある。また，メールの送受信やインターネットの Web 閲覧は，マルウェア感染のリスクが高い。そこで，次の対策を実施することにした。

・運用担当者には，運用担当者の PC の他に，運用業務専用の PC（以下，運用 PC という）も貸与する。

・サーバの運用業務は，運用 PC だけで行うルールとする。

・運用 PC では，メールの送受信及びインターネットの Web 閲覧を技術的に制限する。

・L3SW2 に接続する運用 PC-LAN を新設し，そこに運用 PC を接続する。

その上で，次の設定を変更することにした。

・L3SW1 及び L3SW2 での IP アドレス指定によるフィルタリング設定

・②Web メールサーバの HTTP 接続拒否機能の設定

・③プロキシサーバのアクセス制限機能の設定

K さんは，運用 PC の利用方法案並びにサーバ及び L3SW の設定変更案を作成して，J 部長に説明し，了承を得た。K さんは，運用 PC の導入に着手し，サーバ及び L3SW の設定変更を行った。

設問 1　〔DMZ 上のサーバ及び FW の概要〕について，(1)，(2)に答えよ。

(1) 図 2 中の［ a ］に入れる適切な字句を答えよ。

(2) 表 3 中の［ b ］，［ c ］及び［ d ］に入れる適切なサーバ名を図 1 中の字句を用いて答えよ。

設問 2　〔サーバの設定の点検及び見直し〕について，(1)，(2)に答えよ。

(1) 表 4 中の［ e ］に入れる適切な通信の内容を 30 字以内で述べよ。

(2) 本文中の下線①について，回避によって生じる問題を二つ挙げ，それぞれ 40 字以内で具体的に述べよ。

設問 3　〔運用担当者の PC の利用方法の見直し〕について，(1)，(2)に答えよ。

(1) 本文中の下線②について，設定内容の変更点を 30 字以内で具体的に述べよ。

(2) 本文中の下線③について，設定内容の変更点を 55 字以内で具体的に述べよ。

問３　LAN 分離に関する次の記述を読んで，設問 1～4 に答えよ。

N 社は，新薬創出を事業内容とする，いわゆる創薬ベンチャ企業である。従業員は 10 名で，研究開発員が 5 名，その他の事務員が 5 名である。N 社のネットワーク構成を図 1 に示す。図 1 中の全ての機器には固定の IP アドレスを割り当てている。また，インターネット経由で N 社が利用しているクラウドサービスを表 1 に示す。

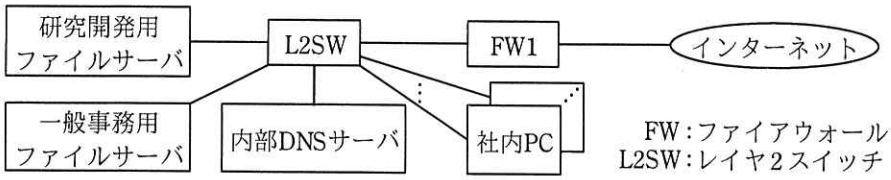


図 1　N 社のネットワーク構成

表 1　利用しているクラウドサービス

サービス名称	内容
電子メールサービス	社内 PC にインストールされた電子メールソフトからのアクセスに応じて，電子メールの送受信を行う。
Web プロキシサービス	社内 PC と社内のサーバからインターネット上の Web サイトへのアクセスを中継する。FW1 では，社内 PC と社内のサーバから，Web プロキシサービスを経由しないでインターネット上の Web サイトへアクセスすることを禁止している。
更新ファイル提供サービス	社内 PC と社内のサーバに，脆弱性修正プログラム（以下，パッチという）とマルウェア定義ファイル（以下，パッチとマルウェア定義ファイルを併せて更新ファイルという）を提供する。更新ファイルは，社内 PC 又は社内のサーバが，HTTP 通信を利用し，Web プロキシサービスを経由してこのサービスへアクセスし，取得する。

〔リスクアセスメント〕

N 社は，事業拡大のために，研究開発員を 30 名程度に増員する計画を立てた。これまで，情報管理を従業員の裁量に任せていたが，増員に伴い，社内の情報管理方法，特にファイルの漏えい防止対策を強化することになり，B 取締役がその責任者に，ネットワーク管理に最も詳しい R さんが担当者に，それぞれ指名された。社外の情報処理安全確保支援士（登録セキスペ）である A 氏の支援を受けることにし，漏えい防止対策の強化について検討を開始した。

次は，その時の会話である。

B 取締役：当社では情報資産の漏えい防止が重要な課題ですが，まずは有望な新薬候補に関するファイル（以下，新薬ファイルという）の保護に絞って見直そうと思います。

A 氏　：分かりました。新薬ファイルは，どこに保管しているのですか。

R さん：主に研究開発用ファイルサーバに保管していますが，一部は研究開発員が使用する社内 PC にも保管しています。

A 氏　：保護の見直しの最初に，サーバや社内 PC に保管中の新薬ファイルについてリスクアセスメントを行うことが必要です。JIS Q 31000:2010 及び JIS Q 31010:2012 では，リスクアセスメントは，［　a　］，リスク分析，［　b　］の三つのプロセスの順に進めると定義されています。まず，［　a　］のプロセスですが，ファイルに影響を及ぼす一般的なリスクの一覧を私から提供しますので，これを基に進めるとよいでしょう。

B 取締役と R さんは，A 氏の支援の下で［　a　］のプロセスを完了した。その結果，新薬ファイルに影響を及ぼすリスクの一覧として表 2 が得られた。

表 2　リスク一覧（抜粋）

項番	リスク	内容
リスク 1	インターネットからの不正侵入による新薬ファイルの漏えい	インターネット経由で，ファイルサーバに侵入されることによって，新薬ファイルがインターネットに流出する。
リスク 2	標的型攻撃による新薬ファイルの漏えい	電子メールによって N 社を標的としたマルウェアが送り込まれ，社内 PC 又は社内のサーバがマルウェアに感染することによって，新薬ファイルがインターネットに流出する。
リスク 3	従業員の故意又は過失によるインターネット経由の新薬ファイルの漏えい	従業員の故意又は過失によって，新薬ファイルが不適切な宛先に電子メールで送信される又は SNS に書き込まれることによって，インターネットに流出する。

続いて，リスク分析のプロセスとして，JIS Q 31000:2010 及び JIS Q 31010:2012 に沿って，［　c　］と，［　d　］を組み合わせてリスクのレベルを決定した。最後に，［　b　］のプロセスとして各リスクへの対応の要否を検討した。その結果，B 取締役は，表 2 のリスク 2 への対応が必要と判断した。

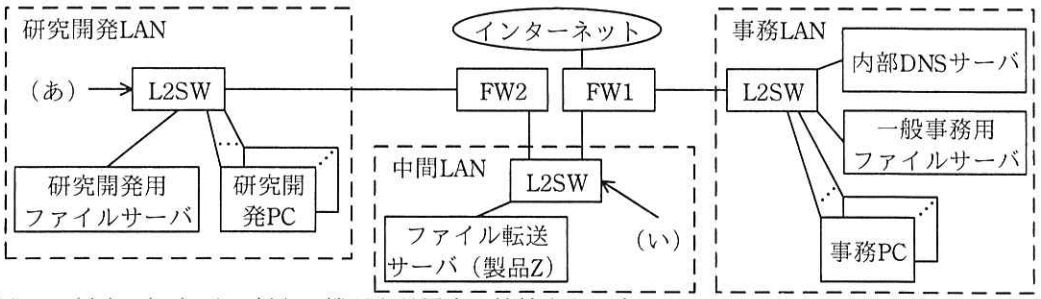
〔LAN 分離案の検討〕

B 取締役と R さんは，表 2 のリスク 2 への対応として，新薬ファイルを保管している機器を収容する LAN（以下，研究開発 LAN という）と，それ以外の機器を収容する LAN（以下，事務 LAN という）に分離する LAN 分離案を検討することにした。事務 LAN はインターネットとの通信を許可するが，研究開発 LAN はインターネットとの通信を一切許可しない。この LAN 分離に伴い，社内 PC は，研究開発 LAN だけに接続する研究開発用の研究開発 PC と，事務 LAN だけに接続する一般事務用の事務 PC に分かれる。研究開発員は，事務 PC と研究開発 PC の 2 台を利用する。

R さんは，業務遂行のために必要な要件を研究開発員から聞き，図 2 にまとめ，ファイル転送のための中間 LAN を加えた図 3 の LAN 分離案を作成した。

1. 社外から届いた電子メールの添付ファイルを，研究開発 PC に転送できること
2. 社外の共同研究者とデータを共有するために，社外のファイル交換用 Web サイトから事務 PC にダウンロードしたファイルを，研究開発 PC に転送できること
3. 研究開発用ファイルサーバ内の新薬ファイルのうち，社外の共同研究者と共有するために承認を受けた新薬ファイルを研究開発 PC 上で編集した後，編集結果を事務 PC に転送し，事務 PC からインターネット上のファイル交換用 Web サイトにアップロードできること

図 2　業務遂行のために必要な要件



注記　（あ），（い）は，新たに機器を設置する接続点を示す。

図 3　LAN 分離案

この案では，研究開発 LAN と事務 LAN の間のファイル転送を行うために，ファイル転送サーバとして広く利用されている U 社製の製品 Z を導入する。図 3 中の FW1 と FW2 の設定内容を表 3 に示す。また，ファイルを転送する際の操作手順を図 4 に示す。

表3　FW1 と FW2 の設定内容

機器名	許可する通信	禁止する通信
FW1	・事務 LAN 上の機器から N 社が利用しているクラウドサービスへの必要な通信 ・事務 PC からファイル転送サーバへの必要な通信	・他の全ての通信
FW2	・研究開発 PC からファイル転送サーバへの必要な通信	・他の全ての通信

注記 1　研究開発 LAN 上の機器は，内部 DNS サーバを利用していない。
注記 2　FW1 及び FW2 は，ステートフルパケットインスペクション型である。

研究開発 PC から事務 PC へのファイル転送時の操作手順

1. 研究開発 PC の Web ブラウザからファイル転送サーバのアップロード用 URL にアクセスし，表示される画面で利用者ごとに異なる利用者 ID 及びパスワードを入力してログインする。
2. ログイン後に表示されるアップロード画面で，研究開発 PC 内のファイルを一つ選択して，アップロードする。アップロードが正常に完了すると，完了メッセージとともにアップロード画面が再度表示される。ここで次のファイルを続けてアップロードすることも，ログアウトボタンをクリックして，ログアウトすることもできる。
3. 事務 PC の Web ブラウザからファイル転送サーバのダウンロード用 URL にアクセスし，表示される画面で利用者ごとに異なる利用者 ID 及びパスワードを入力してログインする。
4. ログイン後に表示されるダウンロード画面では，その利用者 ID でアップロードされたファイルの一覧が表示されるので，ファイルを一つ選択してダウンロードする。ダウンロードが完了すると，サーバ内のダウンロードされたファイルが削除された後，完了メッセージとともにダウンロード画面が再度表示される。ここで次のファイルを続けてダウンロードすることも，ログアウトボタンをクリックして，ログアウトすることもできる。ダウンロードされなくてもアップロードしてから 4 時間たつとファイルは削除される。

注記　事務 PC から研究開発 PC へのファイル転送時の操作手順は，図中の研究開発 PC を事務 PC に，事務 PC を研究開発 PC に，それぞれ置き換えて読むものとする。

図4　ファイルを転送する際の操作手順

LAN 分離を進めると，研究開発 PC 及び研究開発用ファイルサーバは更新ファイルの提供を受けられなくなるので，新しい仕組みが必要になる。R さんは，更新ファイル提供サービスと同じ動作をするパッチ配信兼マルウェア対策管理サーバ（以下，配信サーバという）を用意することにした。

図 3，表 3 及び図 4 を見た A 氏は，幾つかのシナリオを仮定して図 3 の LAN 構成で想定されるマルウェア感染被害について表 4 のとおり評価した。表 5 に，各 OS を利用している機器を示す。

表4　マルウェア感染被害の評価（抜粋）

項番	仮定したシナリオ	想定される被害
1	・HTTP 通信を悪用して管理者権限を奪取できる脆弱性 v が発見されたが，パッチはリリースされていない。 ・事務 PC，研究開発 PC 及びファイル転送サーバには，脆弱性 v が存在している。 ・事務 PC が，脆弱性 v を利用して能動的に感染を広げるマルウェアαに感染した。	・事務 PC からファイル転送サーバが感染する。 ・脆弱性 v を利用して，ファイル転送サーバから①研究開発 PC が感染する可能性は低い。 ・配信サーバの設置位置によっては，配信サーバが感染する可能性がある。
2	・攻撃者が，N 社が製品 Z を使用していることを知っており，製品 Z のアクセス手順を組み込んだマルウェアβを作成し，電子メールを利用して N 社に送り込んだ。 ・事務 PC が，マルウェアβに感染した。 ・マルウェアβが，［ e ］，［ f ］，［ g ］の情報を窃取して，ファイル転送サーバにアクセスした。	・ファイル転送サーバに不正なファイルがアップロードされる。 ・その不正なファイルが原因となって②研究開発 PC が感染する可能性は低い。
3	・ファイル共有プロトコルを悪用して管理者権限を奪取できる脆弱性 w が，OS-P で発見される。 ・OS-Q には，脆弱性 w は存在しない。 ・事務 PC，研究開発 PC 又は配信サーバのいずれかが，脆弱性 w を利用して能動的に感染を広げるマルウェアγに感染した。 ・更新ファイルの提供に使用するプロトコルは，ファイル共有プロトコルではない。	・配信サーバの設置位置によっては，脆弱性 w を利用して，事務 PC，研究開発 PC 及び配信サーバの間で感染が拡大する可能性がある。

表5　各 OS を利用している機器

OS の名称	その OS を利用している機器
OS-P	事務 PC，研究開発 PC，配信サーバ，内部 DNS サーバ
OS-Q	研究開発用ファイルサーバ，一般事務用ファイルサーバ，ファイル転送サーバ

この結果から，図 3 の LAN 分離案は研究開発 LAN 内の新薬ファイルの漏えい防止に有効だとの結論を得て，B 取締役は社内ネットワークの変更を進めることにした。

さらに，表 4 の項番 3 について，マルウェアの感染が広がることを防ぐために，R さんは配信サーバの設置位置を，表 6 を用いて検討した。検討の際に，FW1 と FW2 の設定は必要最小限の通信だけを許可するものとした。

表 6　配信サーバの設置位置の検討内容

感染経路	図 3 中の（あ）に設置した場合	図 3 中の（い）に設置した場合
事務 PC から配信サーバへ	(省略)	結論：感染する可能性が低い。 理由：FW1 によって感染活動を遮断できるから
研究開発 PC から配信サーバへ	結論：感染する可能性が［　h　］。 理由：［　i　］	結論：感染する可能性が［　j　］。 理由：［　k　］
配信サーバから事務 PC へ	(省略)	(省略)
配信サーバから研究開発 PC へ	(省略)	(省略)

検討の結果，R さんは B 取締役に配信サーバの適切な設置位置を提案して，社内ネットワークを変更した。

〔不審な操作ログ〕

社内ネットワークの変更から半年ほどたったある日，ファイル転送サーバのログを調べていた R さんが，研究開発員の S さんの研究開発 PC がファイル転送サーバへ頻繁にアクセスしていたことを発見した。S さんの研究開発 PC を調査したところ，規程で利用を禁止しているリムーバブルメディアを利用した形跡があった。そのリムーバブルメディア経由で研究開発 PC がマルウェアに感染し，S さんが研究開発 PC を操作していない時に，マルウェアが研究開発 PC 内のファイルをファイル転送サーバにアップロードしていたことが分かった。ただし，ファイル転送サーバからダウンロードされてはいなかった。

このマルウェアの情報を調べたところ，次の機能をもっていることが分かった。

・図 4 の操作手順による，ファイル転送サーバへのファイルのアップロード
・図 4 の操作手順による，ファイル転送サーバからのファイルのダウンロード

今回，インターネットへのファイルの流出には至らなかったが，S さんの事務 PC もマルウェアに感染していた場合は直ちにインターネットへのファイルの流出に至るので，R さんはファイル転送サーバに何らかの対策が必要だと考えた。

R さんが A 氏に，この対策について相談したところ，“製品 Z には，正当なファイル転送であることを確認するために，図 4 の手順 2 の後に［ l ］の手順を追加し，その手順の完了をもってダウンロードが可能となる拡張機能が用意されているので，それを利用してはどうか”との回答を得た。R さんは，この拡張機能は効果があると考え，B 取締役の承認の下，導入した。

その後，N 社では情報管理上の大きな事故もなく，順調に事業を拡大している。

設問 1　〔リスクアセスメント〕について，(1)，(2)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　リスク回避　　イ　リスク対応　　ウ　リスク特定

エ　リスク評価　　オ　リスク保有　　カ　リスクモニタリング

(2)　本文中の［ c ］，［ d ］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　リスクが顕在化したときの結果　　イ　リスク対応の実践の優先度

ウ　リスクの起こりやすさ　　エ　リスク保有の利点

設問 2　〔LAN 分離案の検討〕について，(1)～(3)に答えよ。

(1)　表 4 中の下線①で，A 氏が低いと判断した理由は何か。40 字以内で述べよ。

(2)　表 4 中の［ e ］～［ g ］に入れる適切な字句をそれぞれ 15 字以内で答えよ。また，これら全ての情報をまとめて窃取する方法を，30 字以内で具体的に述べよ。

(3)　表 4 中の下線②で，A 氏が低いと判断した理由は何か。50 字以内で述べよ。

設問 3　表 6 中の［ h ］～［ k ］に入れる適切な内容を，［ h ］及び［ j ］については“低い”又は“高い”のいずれかで答え，［ i ］及び［ k ］についてはそれぞれ 30 字以内で述べよ。

設問 4　本文中の［ l ］に入れる適切な手順を，15 字以内で答えよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，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	13:10 ～ 13:50

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。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。