SC

令和３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〕

選択欄	
２問選択	○問１
	問２
	○問３

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　認証システムの開発に関する次の記述を読んで，設問1～4に答えよ。

現行システムの説明

S社は，従業員10名のベンチャー企業である。S社のファイル共有サービス（以下，Sサービスという）は機能が豊富であり，登録会員（以下，S会員という）の数を伸ばしている。

Sサービスでは，利用者認証されたS会員が写真などのファイルを自身に割り当てられたフォルダにアップロードできる。さらに，当該ファイルにアクセスするためのURLを電子メールなどで他者に示すことによって，当該ファイルを他者と共有できる。また，Sサービス内でメッセージや“いいね”を送信できる。

Sサービスの企画，開発及び運用は，CTOのF氏が取り仕切っており，そのうち，開発と運用は，F氏の指示の下，S社エンジニア2名が行っている。Sサービスは，外部セキュリティ企業による脆弱(ぜい)性診断を随時受けている。

〔Sサービスの改修〕

前回の脆弱性診断では，利用者IDとパスワードを用いて利用者認証するSサービスの認証モジュール（以下，S認証モジュールという）の認証方式を，多要素認証にする方がよいとのアドバイスを受けたが，その対処が課題であった。そこで，F氏は，認証及び認可を提供するSNS（以下，認証認可提供SNSという）のうち，多要素認証などの機能をもつT社のTサービスとSサービスとをID連携する改修をCEOのX氏に提案した。その改修によって，S認証モジュールを用いないS会員の登録と多要素認証の実現を目指す。ただし，今回の改修でのID連携では，既存のS会員は対象とせず，新規登録のS会員だけを対象とする。改修後も当面は既存のS会員の認証のために，S認証モジュールも継続して稼働させる。

1.1 と 1.2

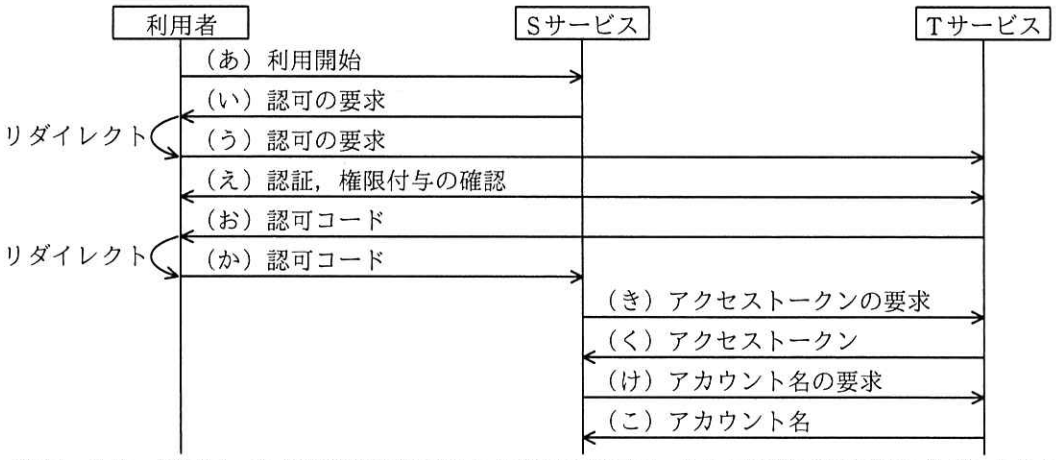
F氏は，①S認証モジュールの代わりにTサービスとのID連携を利用することにはどのような利点と欠点があるかをX氏に説明した。X氏は，ID連携技術に詳しい情報処理安全確保支援士（登録セキスペ）のY氏を外部から招聘(へい)して，実装の最終段階でのレビューを受けることを前提に，Sサービスの改修を承認した。

今回の改修では，OAuthのAuthorization Code Grantを採用する。OAuthは，認証認可提供SNSと認可情報を送受信するためのプロトコルの一つである。OAuthを用いた認可における三つの主体の説明を図1に，認可のシーケンスを図2に示す。

利用者　　：T サービスのアカウントをもち，S 会員の登録を希望する者（以下，S 会員登録希望者という）及び登録された S 会員である。 S サービス：T サービスでのアカウント名を要求する。 T サービス：認証認可提供 SNS である。図 3 に示す権限を提供する。

注記　T サービスのアカウント名は変更できない。

図 1　OAuth を用いた認可における三つの主体の説明



注記　S サービスは，S 会員登録希望者による利用の初回に，S 会員登録希望者がログイン中の T サービスから取得したアカウント名（以下，T-ID という）を S サービス内に登録する。T サービスにログインしていない場合はログインが促される。2 回目以降の S サービスの利用の場合，初回に登録された T-ID を確認する。

図 2　OAuth を用いた認可のシーケンス

3.1

（ア）　他の利用者の投稿に対し“いいね”を送信する権限 （イ）　他の利用者へのメッセージを送信する権限 （ウ）　利用者の代わりに投稿する権限 （エ）　利用者のアカウント名，電子メールアドレスなど登録情報を取得する権限

図 3　T サービスが提供する権限

1.3

図 2 のシーケンスにおいて，［　a　］は，［　b　］が提供するリソースにアクセスできる。それは［　c　］が，図3に示す権限を［　a　］に与えるからである。［　c　］は［　a　］に与える権限を図 2 中の［　α　］の通信の際に確認する。図 3 のうち，どの権限を要求するかは，［　a　］の実装者が決定する。S 社では，要求した権限のいずれか一つでも，［　c　］が与えることを拒否する場合は，シーケンスを止めるように実装することにした。

なお，S サービスでは，将来どの権限も利用すると考え，図 3 の全権限を要求する

ことにした。

次に，T サービスと S サービスとの ID 連携について，実装の最終段階で Y 氏のレビューを受けた。Y 氏はセキュリティ上の問題を三つ指摘した。

問題の想定

〔一つ目の問題〕

Y 氏は，一つ目の問題を，次の攻撃シナリオで説明した。

S サービスにログインしていない利用者が攻撃者の用意した罠(わな)サイトにアクセスすると，図 4 中に示すシーケンス X が走り，後に，②利用者が攻撃を受けているとは知らずに S サービスにファイルをアップロードすると，そのファイルを攻撃者にダウンロードされてしまうおそれがある。

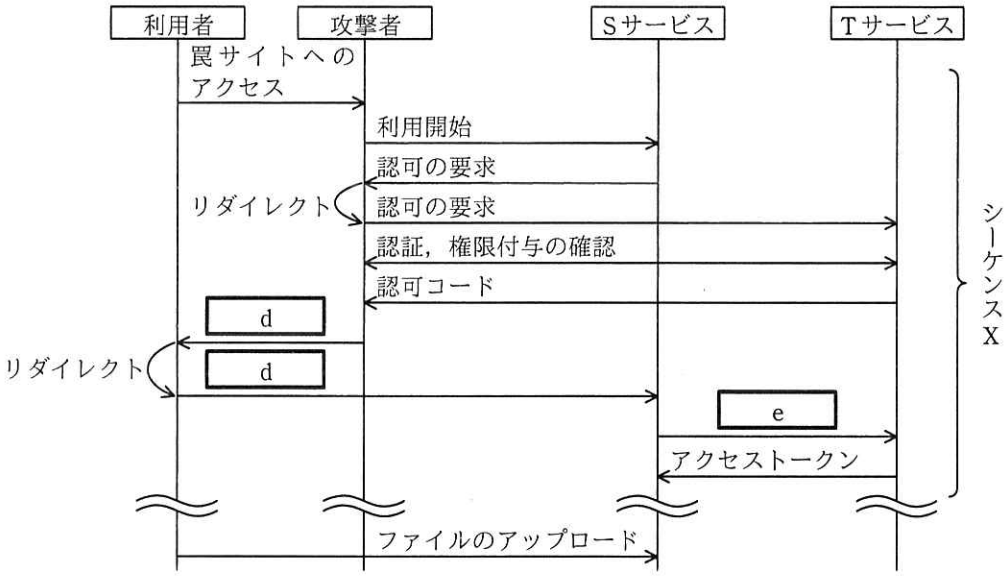


図 4　攻撃のシーケンス

この対策として，RFC 6749 は，図 2 のシーケンスで，推測困難な値である state パラメタを利用することを推奨している。S サービスは state パラメタを［　β　］を送信する際に付与する。S サービスは［　γ　］を受信する際に，そのセッションが，state パラメタを付与した際の［　β　］のセッションと同一であるか否かを確認する。同一である場合だけシーケンスを続ける。

〔二つ目と三つ目の問題〕

二つ目の問題は，③S サービスが T サービスに要求する権限が必要最小限のものになっていないことである。この問題については，要求する権限を一つだけにした。

三つ目の問題は，T サービスに深刻な脆弱性が報告された場合の対応方法を決めていなかったことである。この問題については，T サービスとの ID 連携を一時的に停止し，S 認証モジュールだけで認証することにした。ただし，このとき④一部の S 会員は S サービスを利用できなくなるので，対象の S 会員向けに代替策を検討することにした。

〔利用者認証の実現について〕

X 氏は，全面改修して S 認証モジュールを停止した後の利用者認証の実現方式について Y 氏に確認した。S サービスは利用者を直接認証していないが，⑤S サービスは，登録された S 会員をどのように利用者認証しているかを，Y 氏は X 氏に解説した。

S 社では，Y 氏から指摘された問題を解決した後，T サービスと S サービスとの ID 連携を開始した。

設問 1　〔S サービスの改修〕について，(1)～(4)に答えよ。

(1) 本文中の下線①について，S 社の課題に即した利点を 30 字以内で具体的に述べよ。

(2) 本文中の下線①について，可用性の観点での欠点を 30 字以内で述べよ。

(3) 本文中の［ a ］～［ c ］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　S サービス　　イ　T サービス　　ウ　利用者

(4) 本文中の［ α ］に入れる適切な字句を，図 2 中の（あ）～（こ）から選び，記号で答えよ。

設問2　〔一つ目の問題〕について，(1)～(3)に答えよ。

(1) 図4中の［　d　］，［　e　］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　アクセストークンの要求　　イ　アクセストークン

ウ　認可コード　　エ　認可の要求

オ　認証，権限付与の確認

(2) 本文中の下線②について，ファイルのアップロードと，ファイルのダウンロードは，それぞれTサービスの誰のアカウントによって行われるか。それぞれ6字以内で答えよ。

(3) 本文中の［　β　］，［　γ　］に入れる適切な字句を，図2中の（あ）～（こ）から選び，記号で答えよ。

設問3　〔二つ目と三つ目の問題〕について，(1)，(2)に答えよ。

(1) 本文中の下線③について，必要最小限の権限を図3中の（ア）～（エ）から一つ選び，記号で答えよ。

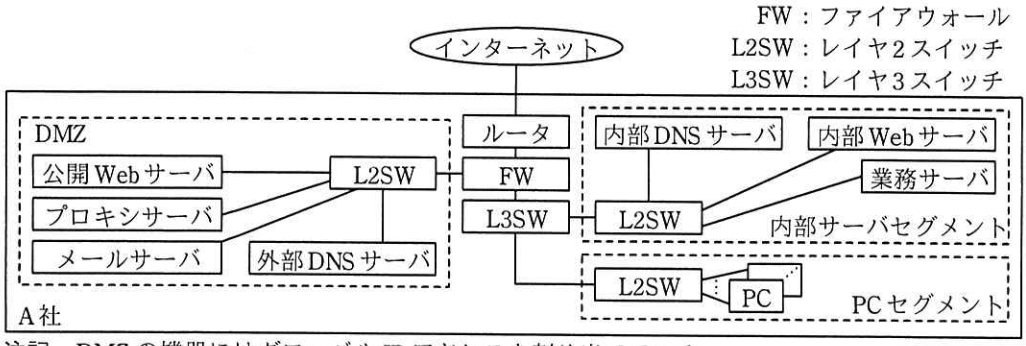
(2) 本文中の下線④に該当するS会員を，35字以内で述べよ。

設問4　本文中の下線⑤について，Sサービスは，Tサービスと連携して，どのように利用者認証を実現しているか。実現の方法を50字以内で具体的に述べよ。

問2　ネットワークのセキュリティ対策に関する次の記述を読んで，設問 1，2 に答えよ。

現行システムの説明

A 社は，従業員 500 名の中規模の小売業であり，インターネットを介して消費者向けに商品を宣伝している。A 社のネットワークは，同社の情報システム部（以下，情シ部という）の L 部長と M 主任を含む 7 名で運用している。A 社のネットワーク構成を図 1 に，図 1 中の主な機器とその概要を表 1 に示す。



注記　DMZ の機器にはグローバル IP アドレスを割り当てている。

図 1　A 社のネットワーク構成

表 1　図 1 中の主な機器とその概要

機器	概要
公開 Web サーバ	消費者向けの商品の宣伝に使用されている。
プロキシサーバ	PC から公開 Web サーバ及びインターネット上の Web サーバへの HTTP 及び HTTPS 通信を中継している。
メールサーバ	社内外との電子メールの送受信に使用されている。
外部 DNS サーバ [1)]	A 社ドメインの権威 DNS サーバ及び再帰的な名前解決を行うフルサービスリゾルバ [2)] として使用されている。
内部 DNS サーバ [1)]	内部サーバセグメントのゾーン情報の管理に使用されている。
PC	A 社の従業員が使用している。Web ブラウザには，公開 Web サーバ及びインターネット上の Web サーバにアクセスできるように，プロキシの設定が適切にされている。

注記 1　A 社では，インターネットドメイン名 a-sha.co.jp を取得しており，レジストラとして X 社を利用している。

注記 2　公開 Web サーバ及びインターネット上の Web サーバの名前解決は，プロキシサーバが外部 DNS サーバに問い合わせる設定になっている。

注 1)　DNS サーバ用の OSS である D ソフトを使用している。

2)　フルサービスリゾルバとしては，プロキシサーバとメールサーバが使用している。

FW のフィルタリングルールを表 2 に示す。

表2　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
1	プロキシサーバ	インターネット	HTTP，HTTPS	許可
2	インターネット	公開Webサーバ	HTTP，HTTPS	許可
3	メールサーバ	インターネット	SMTP	許可
4	インターネット	メールサーバ	SMTP	許可
5	外部DNSサーバ	インターネット	DNS	許可
6	インターネット	外部DNSサーバ	DNS	許可
7	PCセグメント	プロキシサーバ	HTTP，HTTPS	許可
8	PCセグメント	メールサーバ	SMTP，POP3	許可
⋮	⋮	⋮	⋮	⋮
14	全て	全て	全て	拒否

注記1　FWは，ステートフルパケットインスペクション型である。
注記2　項番が小さいルールから順に，最初に一致したルールが適用される。
注記3　項番9～13には，DNSに関するルールは記述されていない。

問題の懸念

ある日，Dソフトの脆弱性を悪用したDoS攻撃で同業他社が踏み台になったというニュースが配信された。情シ部では，脆弱性情報が公開されると，CVSSの値を参考にして自社への影響を評価し，影響が大きいケースでは，早期に脆弱性修正プログラムを適用している。今回の攻撃に使われたDソフトの脆弱性に対する修正プログラムは既に適用されていた。A社では，今回のニュースを契機に，DNSにおけるリスクと対策の検討を，M主任を中心に行うことにした。

〔リスクと対策の検討〕

M主任は，まず，①A社の外部DNSサーバがサービス停止になった場合の影響を確認した。次に，外部DNSサーバが攻撃を受けるリスク及び外部DNSサーバにおけるその他のリスクを調査し，外部DNSサーバが攻撃を受けるリスクについて，主なものを三つ挙げた。

一つ目のリスクは，踏み台になるリスクである。表1及び表2の構成では，攻撃者は，②送信元のIPアドレスを偽装した名前解決要求を外部DNSサーバに送ることによって，外部DNSサーバを踏み台とし，攻撃対象となる第三者のサーバに対し大量のDNSパケットを送り付けるというDoS攻撃を行える。そこで，外部DNSサーバを廃止した上で，DNS-KとDNS-Fという2台のDNSサーバをDMZ上に新設し，権威DNSサーバの機能をDNS-Kに，フルサービスリゾルバの機能をDNS-Fに移行することを

考えた。これと併せて，FW のフィルタリングルールを表 3 のように変更することで一つ目のリスクへの対策となる。

1.3

表 3　変更後の 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
5	a	インターネット	DNS	許可
6	インターネット	b	DNS	許可

注記　項番 5，6 以外は，表 2 と同一である。

二つ目のリスクは，DNS キャッシュポイズニング攻撃によるリソースレコードの改ざんのリスクである。DNS キャッシュポイズニング攻撃が成功すると，攻撃対象のフルサービスリゾルバが管理するリソースレコードのうち，メールサーバの

1.4

c レコードの IP アドレスが，例えば攻撃者のメールサーバのものに書き換えられてしまい，電子メールが攻撃者のサーバに送信されてしまう。この攻撃への対策として，M 主任は，三つの対策を考えた。一つ目の対策は，一つ目のリスクへの対策を流用することである。二つ目の対策は，送信元ポート番号を

1.5

d する対策である。D ソフトでも可能である。三つ目の対策は，

1.6

e という技術の利用である。この技術は，DNS サーバから受け取るリソースレコードに付与されたディジタル署名を利用して，リソースレコードの送信者の正当性とデータの完全性を検証するものである。ただし，この技術は，運用として，鍵の管理など新たな作業が必要になる。

三つ目のリスクは，中間者攻撃による DNS 通信内容の盗聴，改ざんのリスクである。この対策の一つとして，DNS 通信を暗号化する DNS over TLS（以下，DoT という）という技術が標準化されている。DoT は，f と g 間の通信を暗号化するために開発されたものである。

これらの調査と検討を踏まえ，M 主任は，外部 DNS サーバが攻撃を受けるリスク，外部 DNS サーバの機能を 2 台の DNS サーバに移行する対策案，及び送信元ポート番号を d する対策案を L 部長に報告した。

〔ホスティングサービス上に新設する DNS サーバの利用〕

M 主任は，外部 DNS サーバにおけるその他のリスクへの対策として，外部のホスティングサービス上に DNS サーバを新設して利用することを検討した。

M 主任は，DNS サーバの構成について，二つの案を考えた。

一つ目の案は，外部 DNS サーバを廃止した上で，DNS-K と DNS-F という DNS サーバを DMZ 上に，DNS-S という DNS サーバを X 社のホスティングサービス上に新設し，2.1 ③プライマリの権威 DNS サーバの機能を DNS-K に，セカンダリの権威 DNS サーバの機能を DNS-S に移行し，フルサービスリゾルバの機能を DNS-F に移行するものである。M 主任は，DNS-K と DNS-S のゾーン情報を同期するために，DNS-K でのゾーン転送の内容を示す設定ファイル，正引きゾーンファイル，逆引きゾーンファイルを設定することにした。M 主任が設定することにした DNS-K の正引きゾーンファイルを図 2 に示す。

なお，X 社のホスティングサービスに用いるドメイン名は x-sha.co.jp，DNS-S のホスト名は dns-s である。

2.2

```
@       IN      SOA     dns-k.a-sha.co.jp.   admin.dns-k.a-sha.co.jp.  (
（省略）
)
                IN      NS      dns-k.a-sha.co.jp.
                IN      NS      h
                IN      MX      10      i

dns-k           IN      A       x1.y1.z1.t1
www             IN      A       x1.y1.z1.t2
mail            IN      A       x1.y1.z1.t3
```

図 2　DNS-K の正引きゾーンファイル（抜粋）

DNS-K のホスト名は dns-k，公開 Web サーバのホスト名は www，メールサーバのホスト名は mail であり，各サーバの IP アドレスは x1.y1.z1.t1～x1.y1.z1.t3 である。

ゾーン転送では，ゾーン情報が流出するリスクがある。M 主任は，この対策として，DNS-K と DNS-S について，ゾーン転送要求に対する許可を必要最小限にするために，表 4 の設定にすることにした。

2.3

表 4　ゾーン転送要求に対する許可を必要最小限にするための設定

ゾーン転送要求元	ゾーン転送要求先	
	DNS-K	DNS-S
DNS-K		j
DNS-S	k	
上記以外の IP アドレス	l	m

二つ目の案は，外部 DNS サーバを廃止した上で，DNS-HK，DNS-S，DNS-HF という DNS サーバを X 社のホスティングサービス上に新設し，プライマリの権威 DNS サーバの機能を DNS-HK に，セカンダリの権威 DNS サーバの機能を DNS-S に，フルサービスリゾルバの機能を DNS-HF に移行するものである。DNS-K と DNS-F の DMZ への設置は実施しない。この案の場合，FW のフィルタリングルールを表 5 のように変更する必要がある。

2.4

表 5　二つ目の案の場合の 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
5	n	o	DNS	許可
6	p	o	DNS	許可

注記　項番 5，6 以外は，表 2 と同一である。

その後，A 社では，更に検討を進め，外部 DNS サーバを X 社のホスティングサービスに移行することにした。

設問 1　〔リスクと対策の検討〕について，(1)～(7)に答えよ。

(1) 本文中の下線①について，A 社の公開 Web サーバへの影響を，30 字以内で述べよ。

(2) 本文中の下線②の攻撃の名称を 20 字以内で答えよ。

(3) 表 3 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　DNS-F　　イ　DNS-K　　ウ　PC

エ　内部 DNS サーバ　　オ　プロキシサーバ　　カ　メールサーバ

(4) 本文中の［ c ］に入れるDNSのリソースレコードのタイプ名を6字以内で答えよ。

(5) 本文中の［ d ］に入れる適切な字句を15字以内で答えよ。

(6) 本文中の［ e ］に入れる技術の名称を英字10字以内で答えよ。

(7) 本文中の［ f ］，［ g ］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 DNS Changer　　イ RADIUSクライアント

ウ RADIUSサーバ　　エ 権威DNSサーバ

オ スタブリゾルバ　　カ フルサービスリゾルバ

設問2 〔ホスティングサービス上に新設するDNSサーバの利用〕について，(1)～(4)に答えよ。

(1) 本文中の下線③を実施することによって低減できるリスクを30字以内で具体的に述べよ。

(2) 図2中の［ h ］，［ i ］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 dns-k.　　イ dns-k.a-sha.co.jp.　　ウ dns-k.x-sha.co.jp.

エ dns-s.　　オ dns-s.a-sha.co.jp.　　カ dns-s.x-sha.co.jp.

キ mail.　　ク mail.a-sha.co.jp.　　ケ mail.x-sha.co.jp.

(3) 表4中の［ j ］～［ m ］に入れる適切な内容を，“許可”又は“拒否”のいずれかで答えよ。

(4) 表5中の［ n ］～［ p ］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

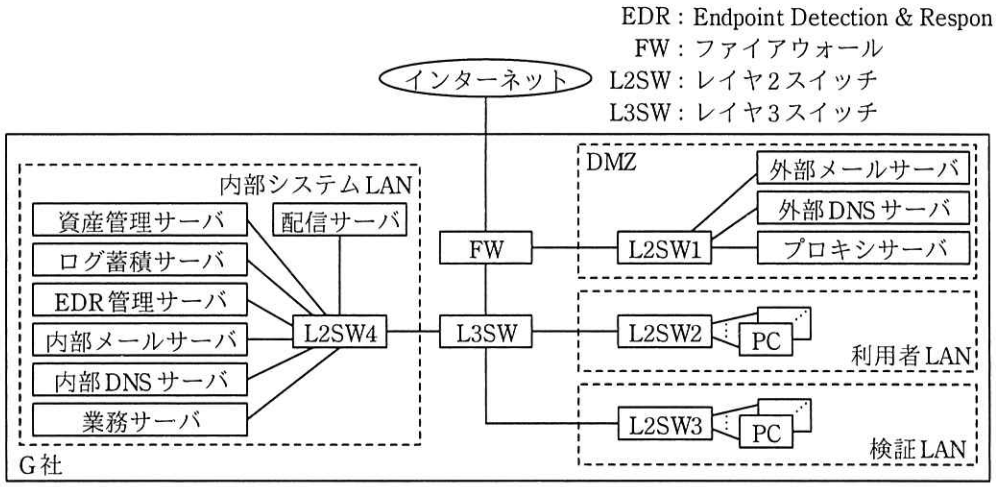
ア DNS-HF　　イ DNS-S　　ウ PC

エ 公開Webサーバ　　オ プロキシサーバ　　カ メールサーバ

問３　セキュリティ運用に関する次の記述を読んで，設問 1～4 に答えよ。

現行システムの説明

G 社は，従業員 1,500 名の製造業であり，研究開発に定評がある。従業員は，Web アクセスによる情報収集並びに電子メール（以下，メールという）による営業活動及び情報交換にインターネットを利用している。G 社では，情報セキュリティポリシを整備して運用している。G 社のシステム構成を図 1 に，機器及びソフトウェアの概要を表 1 に，OS の脆弱性修正プログラム（以下，セキュリティパッチという）の現状の配信手順を図 2 に示す。



注記 1　全ての PC 及びサーバには，固定 IP アドレスが割り当てられており，PC には，EDR のエージェントプログラム（以下，エージェントという）が導入されている。

注記 2　G 社の情報システム部（以下，情シ部という）以外の従業員には，PC の管理者権限を付与していない。

図 1　G 社のシステム構成（概要）

表 1　G 社の機器及びソフトウェアの概要（抜粋）

機器及びソフトウェア	概要
FW	・ステートフルパケットインスペクション型である。 ・フィルタリングルールをもち，送信元 IP アドレス，宛先 IP アドレス，ポートによって通信の許可と拒否を制御する。 ・パケットの送信元 IP アドレス，宛先 IP アドレス，ポート，データサイズと FW の動作を日時とともに FW のログとして取得し，ログ蓄積サーバに syslog で送信する。 ・インターネットとの間の通信を許可しているのは DMZ だけである。

表1　G社の機器及びソフトウェアの概要（抜粋）（続き）

機器及びソフトウェア	概要
配信サーバ	・セキュリティパッチの適用及びソフトウェアの更新を管理する。 ・セキュリティパッチ及び更新用のソフトウェアを取得し配信する。 ・各PCは，セキュリティパッチをOSベンダのサイトから直接ダウンロードするのではなく，配信サーバからダウンロードする。
資産管理サーバ	・エージェントから情報を受け取り，ソフトウェアの資産管理を行う。 ・Wake on LAN（以下，WoLという）の起動パケットを送信する機能をもつ。
ログ蓄積サーバ	・FW，サーバ及びエージェントから送信されるログをsyslogで受信して保存する。
EDR管理サーバ	・エージェントを管理する。 ・社内外からマルウェアのハッシュ値を収集して登録する。
エージェント 4.2	・通信，ファイルの操作などのイベントをログとして保存する。ログは直ちにログ蓄積サーバに送信されるとともに，PCにも1週間は保存される。 ・EDR管理サーバで収集されたハッシュ値を基にマルウェアを検知し，検知したマルウェアの起動を抑止する。 ・PC上で起動する全てのプロセスを監視する。指定した時間帯に指定したコマンドが実行された場合，EDR管理サーバとの間の通信を除き，当該PCの全ての通信を遮断する機能をもつ。

(1)　OSベンダがセキュリティパッチをリリースした場合，情シ部のセキュリティパッチ担当者（以下，パッチ担当者という）は，そのリリースノートを確認する。
(2)　パッチ担当者は，セキュリティパッチを検証LANのPCに適用し，社内で利用しているアプリケーションプログラムを2日間動作させて［　a　］を確認する。1
(3)　さらに，パッチ担当者は，新たな不具合の情報が公開されていないことを確認した上で，セキュリティパッチを配信サーバに置く。
(4)　PCは，適用すべきセキュリティパッチが配信サーバに存在するかどうかを，起動時に配信サーバに問い合わせるように設定されている。もし，適用すべきセキュリティパッチがあれば，それをダウンロードし，適用する。起動中のPCは，適用状況を配信サーバに数時間ごとに通知する。

図2　セキュリティパッチの現状の配信手順（抜粋）

問題の懸念

〔同業他社の事例〕

ある日，情シ部のC主任は，同業他社のH社で発生したセキュリティインシデントの解説記事を見付けた。解説記事の要約を図3に示す。

(1) 8月，H社の1台のPC（以下，PC-Hという）がマルウェアQに感染していたことが分かった。
(2) 各種ログから，PC-Hは外部の不審なサーバに約50Mバイトのデータを送信していたことが分かった。PC-Hでは秘密情報が取り扱われていたことから，H社は，秘密情報が送信された可能性が高いと判断した。
(3) マルウェアQはOSの脆弱性を悪用して感染を広げる。当該脆弱性に対するセキュリティパッチ（以下，パッチQという）は，5月にOSベンダからリリースされており，H社では6月までに，PC-Hを除く全PCに適用されていた。
(4) PC-Hは1月から起動されておらず，7月にPC-Hを起動したときには適用すべきセキュリティパッチが多数あった。そのため，起動後，パッチQの適用完了までに時間が掛かり，その間にマルウェアQに感染したと推測された。
(5) 調査を外部の専門業者に依頼したが，マルウェアQの感染調査に必要なログが一部しか取得されていなかったので調査が難航し，10月まで掛かった。
(6) H社のセキュリティ運用には問題があることが分かった。

図3　解説記事の要約

心配になったC主任はログを調査した。その結果，1か月以上起動していないPCが30台あることが分かった。それらのPCをこのまま数か月起動しないでおくと，PC-Hと同様の問題が発生する可能性があった。図3の内容及びG社の状況を情シ部のB部長に相談した上で，必要な対策を図4のようにまとめ，情シ部のD君とともにそれぞれを具体化することにした。

対策1：マルウェア感染を確認したときに，感染経路及び外部に流出した情報を特定するための手段の導入
対策2：社内におけるセキュリティパッチの配信手順の改善

図4　必要な対策

〔対策1〕

C主任は，対策1については，L2SWのミラーポートに接続するタイプのパケット収集装置を導入し，J社のJサービスを利用して通信内容を分析すればよいと考えた。Jサービスは，インターネットVPN経由でパケット収集装置から必要なパケット情報を取得し，その内容からセキュリティ侵害を検知するサービスである。

C主任は，1台のパケット収集装置を，[2]①マルウェア感染がDMZ又はどのLANで起きてもマルウェアからインターネットへの通信が通過することになるL2SWに接続することに決めた。

〔対策 2〕

次は，対策 2 についての D 君，C 主任及び B 部長の会話である。

D 君　：1 か月間起動していない PC を自動的に起動して，セキュリティパッチが適用されるようにすれば図 3 のようなセキュリティインシデントを防ぐことができます。良い仕組みはありませんか。

C 主任：当社の PC は，WoL に対応しています。WoL とは，WoL に対応した PC に対し，特定の起動パケットを送信すると，当該 PC が起動するという仕組みです。PC を利用者 LAN に接続しておけば，資産管理サーバから起動パケットを送信することによって，PC を自動的に起動できます。

B 部長：なるほど。では，WoL とセキュリティパッチ適用の動作検証を頼む。

D 君は，WoL の動作検証を開始した。まず，検証 LAN に接続された PC-X と PC-Y を用いて試すことにした。PC-X は起動しておき，PC-Y はシャットダウンしておいた。その上で，PC-X から PC-Y に対し，［ b ］に続けて，起動したい PC の［ c ］を 16 回繰り返したデータを含む起動パケットを送信し，PC-Y が起動することを確認した。その後，資産管理サーバから PC-Y の起動を試みたが，起動しなかった。C 主任に相談したところ，②L3SW の設定を変更する必要があるという助言を受けた。D 君は，L3SW の設定を変更し，資産管理サーバから PC-Y を起動できることを確認した。続いて，資産管理サーバから利用者 LAN に接続された PC を起動できることを確認し，セキュリティパッチが適用されることも確認した。

〔WoL を悪用するマルウェアの脅威〕

WoL について調べていた D 君は，図 5 に示すマルウェア R の記事を見付けた。

起動していない PC を WoL を使って夜間に起動させ，次の手順で感染拡大を試みる。
(1)　感染するとすぐに，③自身が動作する PC の ARP テーブルから下記(2)及び(4)の活動に必要な情報を読み取って保持しておく。
(2)　夜間に ARP テーブル中の PC 全てに ping コマンドを送信し，PC が起動しているかどうかを確認する。
(3)　起動している PC に感染拡大を試みる。
(4)　起動していない PC を発見したら，WoL を使ってそれらの PC を起動し，感染拡大を試みる。

図 5　マルウェア R の記事（抜粋）

D 君は，昼間は PC が不審な振る舞いをすれば発見し対処できる可能性があるが，夜間は多くの従業員が不在となり発見することは難しいと考えた。そこで，マルウェア R に限らない，WoL を悪用するマルウェアへの対策について，C 主任に相談した。

C 主任は，PC が夜間に不審な振る舞いをしたときに，当該 PC をネットワークから隔離するという対策（以下，対策 3 という）を助言した。D 君は，④対策 3 を G 社で導入済のシステムを用いて実現する方法を立案した。対策 3 は対策 1 及び対策 2 と併せて承認された。各対策は運用を開始し，マルウェア対策が強化された。

設問 1　図 2 中の［　a　］に入れる適切な字句を 20 字以内で具体的に答えよ。

設問 2　本文中の下線①の L2SW を，図 1 中の L2SW1～L2SW4 から選び，答えよ。

設問 3　〔対策 2〕について，(1)～(3)に答えよ。

(1) 本文中の［　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　00:00:00:00:00:00　　イ　00:00:00:FF:FF:FF

ウ　00:FF:00:FF:00:FF　　エ　FF:FF:FF:FF:FF:FF

(2) 本文中の［　c　］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　IP アドレス　　イ　MAC アドレス　　ウ　製造番号

エ　プロダクト ID　　オ　ホスト名

(3) 本文中の下線②に示す設定変更の内容を，30 字以内で具体的に述べよ。

設問 4　〔WoL を悪用するマルウェアの脅威〕について，(1)，(2)に答えよ。

(1) 図 5 中の下線③について，(2)の活動に必要な情報及び(4)の活動に必要な情報を，それぞれ 10 字以内で答えよ。

(2) 本文中の下線④の方法を，55 字以内で具体的に述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

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	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，マスク

   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。