SC

平成26年度　秋期
情報セキュリティスペシャリスト試験
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　スマートフォンに関する次の記述を読んで，設問1～4に答えよ。

K社は，従業員数5,000名の情報システム会社である。K社では，モバイルPCに加えて，スマートフォン（以下，スマホという）から，従業員が電子メールやグループウェアなどの社内システムへアクセスできるシステム環境（以下，Bシステムという）を昨年導入した。Bシステムの利用に先立ち，従業員が電子メール用やグループウェア用のアプリケーションソフトウェア（以下，アプリケーションソフトウェアをアプリという）をスマホにインストールする。また，Bシステムの導入に当たっては，スマホを遠隔で管理するシステム（以下，Mシステムという）を追加で導入し，スマホのOSやアプリのバージョンなどの構成情報の管理や，スマホの紛失時のデータ消去などのセキュリティ対策を実現した。さらに，“個人の所有物であるスマホからBシステムを利用する際は，事前に，利用者の氏名に加えてスマホの製品名や電話番号といった情報をK社に申請すること”などを定めたスマホ利用規程を策定した。

Bシステムの導入から1年が過ぎたので，K社では，セキュリティ対策及びスマホ利用規程が有効であったかについて確認することにした。その際に，スマホに関するセキュリティ対策を改めて議論することにした。

〔ルート特権の利用について〕

スマホのルート特権を利用者が利用できる状態にする行為（以下，ルート特権化という）について，セキュリティ上の問題がないかを検討することになった。スマホの多くは，利用者がルート特権をもたず一般利用者の権限だけで利用することを前提にしている。そのため，ルート特権をもつ個人のPCと違い，OSの設定の一部を自由に変更できないという制約や，スマホのベンダによってあらかじめインストールされているアプリを削除できないという制約などがある。そのような制約を嫌う利用者の中には，ベンダが想定していない手段で，ルート特権化を自ら行う者もいる。

K社で調査したところ，ルート特権化は，主に，バッファオーバフロー攻撃を用いて実現されることが分かった。

〔バッファオーバフロー攻撃の詳細と対策について〕

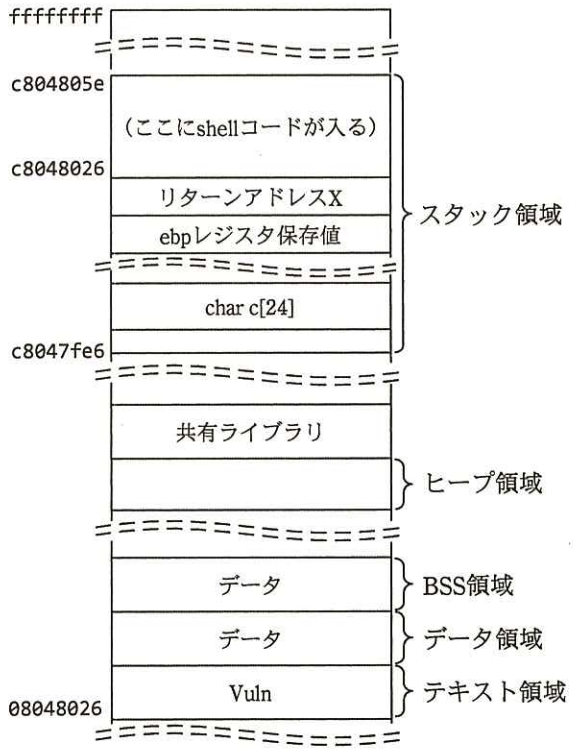
バッファオーバフロー攻撃に関するセキュリティホールは，スマホ用の OS だけではなく，PC 用 OS やサーバ用 OS においても報告されている。通常，OS やライブラリのセキュリティホールが公表された場合，PC やサーバを管理する者は，開発元から提供される［ a ］の適用やソフトウェアの更新によって，セキュリティホールに対処する。他方，Web サーバにおいては，［ a ］の適用やソフトウェアの更新をしなくても，①通信路上に IPS や WAF を設置することによって，インターネットから Web サーバへのバッファオーバフロー攻撃を防止することもできる。

バッファオーバフロー攻撃としては，スタックバッファオーバフロー攻撃，［ b ］バッファオーバフロー攻撃や，静的メモリ領域を対象としたバッファオーバフロー攻撃が知られている。いずれのバッファオーバフロー攻撃も，主に C や C++で作成されたプログラムが狙われる。スタックバッファオーバフロー攻撃は，スタック領域を破壊するので，スタック破壊攻撃とも呼ばれる。スタック破壊の挙動をプログラム実行時に検知して停止する機能（以下，スタック破壊検知機能という）を含むコードを生成するコンパイラも普及している。

図 1 は，スタックバッファオーバフロー攻撃に対して脆弱（ぜい）なプログラム（以下，Vuln という）である。図 2 は，関数 foo が呼び出された後のメモリ配置である。ここで，図 2 中の shell コードは，攻撃者がスタックバッファオーバフロー攻撃によってメモリ上に配置するものである。スタック破壊検知機能を含めずにコンパイルした Vuln においては，攻撃を成立させるために挿入するデータ（以下，インジェクションベクタという）を変数 a に与えることによって，shell コードにプログラムの制御が移ってしまう。ここでは，図 3 が Vuln に対するインジェクションベクタである。その際，Vuln が実行時に②一定の条件を満たせば，あらゆる命令の実行が shell コードで可能となる。

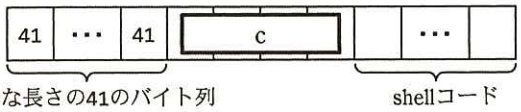
```
 1: (省略)
 2: int main(int argc, char *argv[]) {
 3:    char *a;
 4: (省略, ここで a がポイントする領域にインジェクションベクタが挿入される。)
 5:    foo(a);
 6: (省略, ここでその他の必要な処理をする。)
 7: }
 8: int foo(char *b) {
 9:    char c[24];
10: (省略)
11:    strcpy(c, b);
12: (省略, ここで c を利用する。)
13:    return 0;
14: }
```

図１　スタックバッファオーバフロー攻撃に対して脆弱なプログラム Vuln



注記　メモリアドレスは 4 バイトの 16 進数表記である。

図２　関数 foo が呼び出された後のメモリ配置



注記　表記は 16 進数である。

図３　Vuln に対するインジェクションベクタ

このスタックバッファオーバフロー攻撃を防止するため，指定されたメモリ領域でのコードの実行を禁止する機能（以下，データ実行防止機能という）が登場した。これは，CPU の機能を用いて実現されている。

しかし，プログラム実行時に共有ライブラリがメモリ上にロードされていることを利用して，データ実行防止機能を回避する新たな攻撃法が登場した。これは，共有ライブラリ内の関数であって，かつ，任意のプログラムを実行できる関数を，スタックバッファオーバフロー攻撃時に利用するものである。libc 共有ライブラリを利用する場合，この攻撃は［ d ］攻撃と呼ばれる。

最近の OS では，こういった攻撃が成功することを抑制するため，アドレス空間配置ランダム化技術が実装されている。アドレス空間配置ランダム化技術を用いると，スタック破壊検知機能を含めずにコンパイルしたプログラムであっても，スタックバッファオーバフロー攻撃の成功を抑制することができる。

〔K 社での対策〕

K 社の調査の結果，スマホの OS のあるバージョン（以下，バージョン V という）以降ではデータ実行防止機能及びアドレス空間配置ランダム化技術が実装されていることが分かった。また，バージョン V 以降では，その他様々な点でセキュリティ対策が強化されていることも分かった。

その上で，ルート特権化されたスマホから B システムを利用することについて改めて検討したところ，ルート特権化されたスマホは，ベンダの保守サポートの対象外になること，及び M システム用のアプリや B システム用のアプリが動作しなくなることが分かった。さらに，ルート特権化されていないスマホと違い，ルート特権化されたスマホでは，“データを盗み出すタイプのマルウェア”が侵入してしまうと，それがルート特権を取得して，③スマホ内に保存されているアプリのデータを不正に読み出してしまうリスクが高まることも分かった。そのため，K 社では，スマホ利用規程で，ルート特権化されたスマホからの B システムの利用を禁止することにした。

しかしながら，④それだけでは，従業員がスマホ利用規程を守ったとしても，“意図しないルート特権化”のリスクが残存する。K 社は，B システムのセキュリティを確保するために，スマホでは，バージョン V 以降の OS を利用することが必要であるとの結論に至った。そのため，⑤スマホの OS のバージョンを K 社が確認する運用策を実施することにした。

設問1　本文中の［ a ］，［ b ］，［ d ］に入れる適切な字句を，［ a ］は15字以内で，［ b ］は5字以内で，［ d ］は20字以内でそれぞれ答えよ。

設問2　Vulnへのスタックバッファオーバフロー攻撃とその対策について，(1)～(3)に答えよ。

(1)　図2のメモリ配置について，スタックバッファオーバフロー攻撃を防止するには，データ実行防止機能をどのメモリ領域に適用すればよいか。図2中の用語を用いて答えよ。

(2)　図3中の［ c ］に入れる適切なバイト列を解答群の中から選び，記号で答えよ。ただし，バイトオーダはリトルエンディアンとする。

解答群

ア　068004c8　　イ　08048026　　ウ　26800408　　エ　268004c8

オ　5e8004c8　　カ　c8048006　　キ　c8048026　　ク　c804805e

(3)　アドレス空間配置ランダム化技術は，攻撃者のどのような行為をできないようにすることによって，図3のインジェクションベクタによるスタックバッファオーバフロー攻撃が成功することを抑制するか。25字以内で具体的に述べよ。

設問3　バッファオーバフロー攻撃について，(1)，(2)に答えよ。

(1)　本文中の下線①にある，インターネットからWebサーバへのバッファオーバフロー攻撃の対策として，IPSやWAFではどのような処理をするか。25字以内で具体的に述べよ。

(2)　本文中の下線②の条件を20字以内で述べよ。

設問4　〔K社での対策〕について，(1)～(3)に答えよ。

(1)　ルート特権化されていないスマホでは，本文中の下線③の不正な読出しを，OSのファイルシステムがどのような仕様で制限しているか。40字以内で述べよ。

(2)　本文中の下線④について，意図しないルート特権化がどのような状況で起こり得るか。25字以内で述べよ。

(3)　本文中の下線⑤について，確認方法を具体的に20字以内で述べよ。

問2　代理店販売支援システムに関する次の記述を読んで，設問1～3に答えよ。

L社は中堅の損害保険会社である。保険商品は，直営店でも扱っているが，多くは代理店を通じて販売している。L社では，10年前にインターネットを用いた代理店販売支援システム（以下，Pシステムという）を開設した。

Pシステムは，代理店に対して，顧客情報の新規登録，閲覧及び更新の機能，並びに商品説明書及び販売マニュアルの提示機能を提供する。代理店の担当者は，利用者IDとパスワードを入力してログインし，Pシステムを利用する。

Pシステムの開設以来，Pシステムへの不正ログインの試みと推測される事象が複数回確認されてきた。また，3年前には，競合他社において代理店から大量の顧客情報が流出する事件も発生した。これらの状況において，L社は代理店に対して，注意喚起，講習会の開催，年1回のセキュリティチェックレポート提出の要請などを実施してきた。

運用開始から10年目を迎えることを機に，L社では，Pシステムを全面改修・拡張して，新システム（以下，Qシステムという）を構築することにした。そのプロジェクトのリーダには，IT部門のB課長が任命された。プロジェクトの重要な目的の一つは，セキュリティの強化である。Qシステムのセキュリティ設計は，B課長の部下であるCさんが担当することになった。

〔Qシステムの設計方針〕

Qシステムは，Pシステムを拡張して構築する。2015年9月から10年間の稼働を想定している。Qシステムには，情報漏えいのリスクをできるだけ減らすことが求められている。B課長は，経営陣，代理店チャネル担当，情報セキュリティ室などの社内関係者及び社外の情報セキュリティの専門家に意見を求め，表1に示す情報漏えい防止設計方針を取りまとめた。

表１　情報漏えい防止設計方針（抜粋）

情報漏えい対策	設計方針
利用者の認証	・利用者 ID とパスワードだけでなく，多段階又は複数要素で利用者を認証することによって，なりすましによる不正アクセスを防止する。
端末の限定	・代理店の管轄下にある端末からのアクセスだけを許可する。
ガイドラインの作成	・顧客情報の取扱いや Q システムの利用要件についてガイドラインを作成し，その遵守義務を代理店契約に盛り込む。

C さんは，表１の設計方針のうち，利用者の認証及び端末の限定についての実現方法として，Q システムへのアクセス時に，従来の利用者 ID とパスワードでの認証に加え，SSL クライアント認証を行う方法を提案した。SSL クライアント認証では，あらかじめディジタル証明書（以下，証明書という）を代理店の端末に配布しておき，その証明書を用いた認証によって端末の限定を行う。

B 課長は，C さんが提案した方法について説明を受け，了承した。その上で，暗号技術について，情報セキュリティ室の R 主任に相談するよう助言した。

〔暗号技術の検討〕

次は，C さんが暗号技術について R 主任に相談したときの会話の一部である。

C さん：Q システムで使う暗号技術について，どのように検討を進めるのがよいでしょうか。

R 主任：SSL クライアント認証の場合には，まず，認証に使う公開鍵の鍵長，証明書に施されるディジタル署名の仕様，それから，通信の暗号化に使う共通鍵暗号の仕様などを選択する必要があるね。

C さん：何を基準にして選択すればよいのですか。

R 主任：表 2 は，米国国立標準技術研究所（NIST）が発行したセキュリティ文書を基に，攻撃の困難性の視点から，暗号アルゴリズムの安全性を整理したものだ。最も効率が良い攻撃手法で暗号を解読するときに必要な計算量を指標とし，同程度の耐性をもつものを同じ“セキュリティ強度”としている。また，“利用終了時期の目安”の行は，そのセキュリティ強度の暗号アルゴリズムについて，利用を終了することが望ましい時期を示している。

C さん：なるほど。例えば，鍵長 256 ビットの AES アルゴリズムは，鍵長

[a] ビットの RSA アルゴリズムや，[b] ビットのハッシュ関数などと同じセキュリティ強度ということですか。Q システムの場合は，少なくとも [c] ビット安全性と同等又はそれ以上のセキュリティ強度をもつ暗号アルゴリズムを採用すべきですね。頂いたアドバイスを参考に，更に検討します。

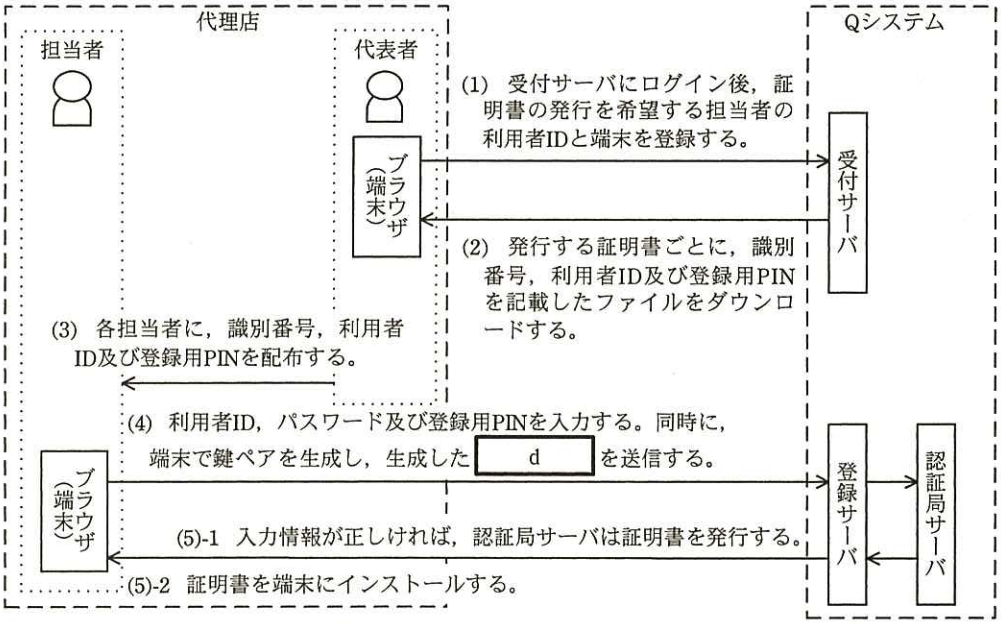
表 2　暗号アルゴリズムの安全性

項目＼セキュリティ強度		80 ビット安全性	112 ビット安全性	128 ビット安全性	192 ビット安全性	256 ビット安全性
共通鍵暗号		80	112	128	192	256
公開鍵暗号	素因数分解問題に基づくアルゴリズム	1,024	2,048	3,072	7,680	15,360
	離散対数問題に基づくアルゴリズム	1,024	2,048	3,072	7,680	15,360
	楕円曲線上の離散対数問題に基づくアルゴリズム	160	224	256	384	512
ハッシュ関数		160	224	256	384	512
利用終了時期の目安		2013 年	2030 年	2031 年以降	2031 年以降	2031 年以降

注記 1　暗号の各行の数値は，鍵のビット数である。
注記 2　ハッシュ関数の行の数値は，ディジタル署名とハッシュ単独利用の場合におけるハッシュ値のビット数である。

〔Q システムのセキュリティ設計〕

C さんは，R 主任のアドバイスを参考に，Q システムのセキュリティ設計について検討を進めた。証明書の新規発行手順案を図 1 に，証明書についての補足情報を図 2 に示す。代理店に遵守を求めるガイドラインには，顧客情報の取扱要件に加え，①Q システムにアクセスしていた端末を交換及び廃棄する場合に代理店が実施すべき処理などの事項を盛り込んだ。



受付サーバ：Qシステムの窓口となるサーバであり，アクセスにはSSLクライアント認証を必須とする。
登録サーバ：証明書の発行受付のための専用サーバである。SSLクライアント認証はない。
認証局サーバ：証明書を発行するサーバである。
代表者：代理店が指定し，L社に登録する。代表者は，必要な証明書の発行をL社に申請する。代表者に与える最初の証明書は，別途定めた手順に従って発行する。
担当者：代理店においてQシステムを利用する者を示す。
識別番号：個々の証明書の発行及び更新ごとに付与する一意な番号である。証明書の管理のために利用する。

注記 証明書には，証明書のシリアル番号，利用者ID，公開鍵，識別番号などを登録する。

図1 証明書の新規発行手順案

1. 証明書の利用停止手順

(1) 利用を停止する証明書の利用者である担当者が，受付サーバにログインし，利用を停止する証明書の [e] 又は識別番号を入力する。

(2) 受付サーバは，入力された情報で，ログインした担当者に発行された有効な証明書かを確認した後，当該証明書の識別番号を受付拒否リストと呼ばれるリストに登録する。

2. 証明書の更新手順

(1) 担当者は登録サーバにアクセスし，更新前の証明書と，当該秘密鍵の保持を示す署名データを提示する。

(2) 登録サーバは，提示された証明書と署名データを検証し，認証局サーバが発行した証明書であること，証明書に対応する秘密鍵を端末が保持していること，及び有効期間の終了まで 60 日以内であることを確認する。全て確認できれば，端末に対して新鍵ペアの生成を要求する。

(3) 認証局サーバは，新鍵ペアに対して新しい証明書を発行する。

図2 証明書についての補足情報

3. 受付サーバにおける担当者及び代表者のログイン処理時の検証項目（順不同）
   ・入力された利用者 ID に対して，正しいパスワードが入力されたこと
   ・提示された証明書が，認証局サーバが発行した証明書であること
   ・証明書に対応する秘密鍵を，端末が保持していること
   ・証明書の有効期間内であること
   ・証明書中の識別番号が［ f ］に登録されていないこと
   ・［ g ］が，証明書中の［ h ］と一致すること
4. その他の補足事項
   ・証明書の有効期間内に更新が行われなかった場合は，新規発行手順で対応する。
   ・証明書に対応する秘密鍵は，端末から容易に抽出できないように設定する。

図２　証明書についての補足情報（続き）

〔セキュリティ設計の修正〕

C さんは，セキュリティ設計の検討結果について R 主任にレビューを依頼した。R 主任は，証明書の新規発行手順，利用停止手順及び更新手順について一つずつ問題を指摘した。

R 主任は，証明書の新規発行手順については，代理店の担当者が不適切な行為をした場合，表 1 中の“端末の限定”の設計方針が満たされず，代理店の管轄下にない端末で Q システムにアクセスできる可能性があると指摘した。②この問題については，Q システムでは対策をとらず，代理店側で対策をとってもらうように，代理店に要請することにした。

R 主任は，証明書の利用停止手順については，実際には行うことができない場合が多いと推測されるので，見直さなければならないと指摘した。C さんは，この問題について，表 3 に示す修正案を考えた。検討の結果，設計方針への適合性と運用の柔軟性確保の視点から，案(2)を採用することにした。

表３　証明書の利用停止手順の修正案

案	修正の概要	長所	短所
(1)	受付サーバへのログイン時に SSL クライアント認証を要求しない。	担当者本人による迅速な停止が期待できる場合がある。	情報漏えい防止設計方針と相違する部分がある。
(2)	役割と権限を見直し，［ i ］。	担当者が不在の場合にも，証明書の利用停止が可能である。	代表者の役割が拡大し，権限が集中する。

R 主任は，証明書の更新手順については，利用停止された証明書の取扱いを担当者が誤った場合などに，③本来発行されるべきでない証明書が発行される可能性があると指摘した。C さんは，この問題についても修正案を考えた。

C さんは，これらの修正案を基に図 1 及び図 2 の修正版を作成し，再度 R 主任のレビューを受けた後，B 課長に説明した。B 課長は修正版を了承し，Q システムの開発が進められることになった。

設問 1　〔暗号技術の検討〕について，(1)～(3)に答えよ。

(1) 本文中の［ a ］，［ b ］に入れる適切な数値を答えよ。

(2) 鍵長 3,072 ビットの RSA アルゴリズムと同等又はそれ以上のセキュリティ強度をもつと考えられるハッシュ関数を解答群の中から全て選び，記号で答えよ。

解答群

ア	Camellia	イ	ECDSA	ウ	MD5	エ	RC4
オ	SHA-1	カ	SHA-256	キ	SHA-512	ク	Triple DES

(3) 本文中の［ c ］に入れる適切な数値を答えよ。また，この数値は Q システムのどのような要件から導かれるか。20 字以内で述べよ。

設問 2　〔Q システムのセキュリティ設計〕について，(1)，(2)に答えよ。

(1) 本文中の下線①について，代理店が実施すべき処理を，30 字以内で具体的に述べよ。

(2) 図 1 中の［ d ］及び図 2 中の［ e ］～［ h ］に入れる適切な字句を，図 1 又は図 2 中の字句を用いて，それぞれ 10 字以内で答えよ。

設問 3　〔セキュリティ設計の修正〕について，(1)～(3)に答えよ。

(1) 本文中の下線②について，代理店がとる対策を，40 字以内で具体的に述べよ。ここで，代理店の代表者は不適切な行為をしないものとする。

(2) 表 3 中の［ i ］に入れる適切な内容を 30 字以内で述べよ。

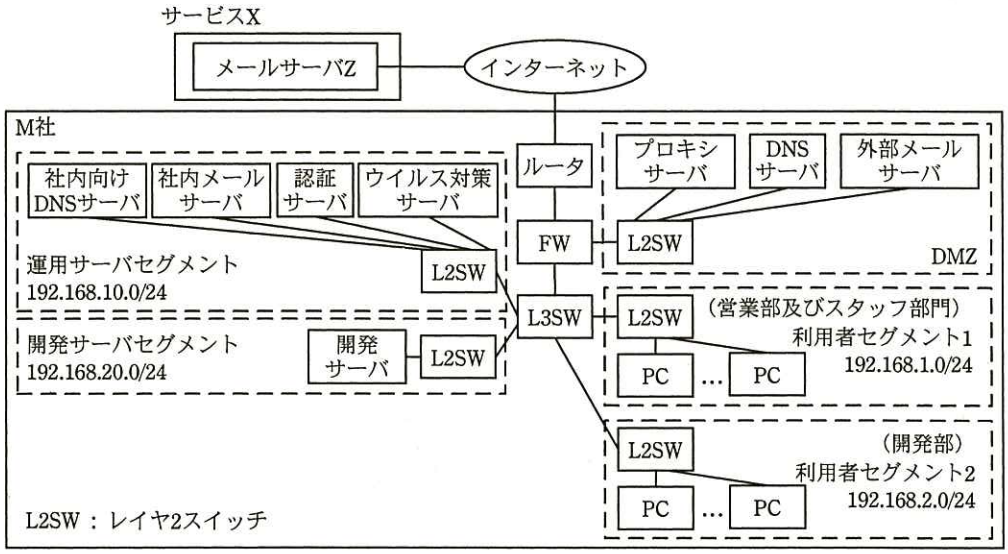
(3) 本文中の下線③のような証明書が発行されることを防ぐために，登録サーバにおける処理内容にどのような処理を追加すればよいか。40 字以内で述べよ。

問3　マルウェア感染への対応に関する次の記述を読んで，設問1～4に答えよ。

M社は，従業員数200名のソフトウェアパッケージ開発会社であり，開発部，営業部及びスタッフ部門がある。

開発部は，ソフトウェアパッケージの開発・保守を行っている。営業部は，顧客を訪問し，製品紹介，製品販売及び顧客管理を行っている。スタッフ部門は，M社のスタッフ業務全般を担当しており，総務部，経理部，情報システム部（以下，情シ部という）などから成っている。情シ部では，M社の情報システムの管理及び情報セキュリティインシデントへの対応を行っている。M社のネットワーク構成を図1に，M社のサーバの機能一覧を表1に示す。

M社のネットワークでは，ファイアウォール（以下，FWという）とレイヤ3スイッチ（以下，L3SWという）でネットワークのアクセス制御を行っている。FWのフィルタリングルールを表2に，L3SWのフィルタリングルールを表3に示す。



注記1　192.168.1.0/24，192.168.2.0/24，192.168.10.0/24及び192.168.20.0/24は，ネットワークアドレスを示す。

注記2　PCのブラウザは，ポート番号8080でプロキシサーバを経由してインターネットアクセスするように設定されている。

注記3　PCのデフォルトゲートウェイには，L3SWを設定している。

注記4　L3SWにおいては，DMZ及びインターネット宛てのパケットは，FWに転送されるようにルーティング設定が行われている。

図1　M社のネットワーク構成

表1　M社のサーバの機能一覧（抜粋）

サーバ名	機能
外部メールサーバ	・電子メール（以下，メールという）の中継機能 ・外部からのメールフィルタリング機能（現状は無効） －フィルタリングのルールとして，ホワイトリストに許可，ブラックリストに拒否の指定が可能である。 －ホワイトリスト及びブラックリストには，送信元メールサーバの IP アドレスのリスト及び送信ドメイン名のリストがある。 －ホワイトリスト及びブラックリストの両方にマッチした場合は，ホワイトリストを優先する。
認証サーバ	・利用者の氏名，所属及びメールアドレスの管理機能 ・利用者認証機能
ウイルス対策サーバ	・ウイルス定義ファイル配信機能 －半日ごとに最新のウイルス定義ファイルをプロキシサーバ経由でベンダからダウンロードし，他のサーバと PC に配信する。

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（ポート番号）	動作
1	プロキシサーバ	インターネット	全て	許可
2～7	⋮	⋮	⋮	⋮
8	ウイルス対策サーバ	プロキシサーバ	代替 HTTP（8080）	許可
9	PC[1)]	プロキシサーバ	代替 HTTP（8080）	許可
10	全て	全て	全て	拒否

注記1　項番の小さいものから順に，最初に一致したルールが適用される。
注記2　項番 2～7 は，SMTP 又は DNS に関するルールである。
注 1)　192.168.1.0/24 及び 192.168.2.0/24 の全ての IP アドレス

表3　L3SW 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	利用者セグメント 2	開発サーバセグメント	全て	許可
2	開発サーバセグメント	利用者セグメント 2	全て	許可
3	運用サーバセグメント	開発サーバセグメント	全て	許可
4	開発サーバセグメント	運用サーバセグメント	全て	許可
5	開発サーバセグメント	全セグメント[1)]	全て	拒否
6	全セグメント[1)]	開発サーバセグメント	全て	拒否
7	全セグメント[1)]	全セグメント[1)]	全て	許可

注記　項番の小さいものから順に，最初に一致したルールが適用される。
注 1)　全てのセグメントを示し，FW，DMZ 及びインターネットを含む。

情シ部員は，運用サーバセグメントの管理を，自席の PC のブラウザから行っている。開発サーバには，M 社の機密情報であるソフトウェアパッケージのソースコード

を保管している。

営業部では，SaaS 型クラウドサービスであるサービス X を利用して顧客管理を行っている。サービス X には，営業部の PC から，HTTP の CONNECT メソッドを使用してプロキシサーバ経由でアクセスしており，プロキシサーバからサービス X へのアクセスにはポート番号 2560 を使用している。また，サービス X 内のメールサーバ Z は，M 社専用であり，製品紹介のメールを M 社の顧客に対して自動送信すると同時に，メールの写しを M 社営業部員全員に送信している。送信の際には，送信者メールアドレスとして M 社のメールアドレスを使っている。

〔情報セキュリティインシデントの発生〕

営業部の D さんから情シ部の S さんに，D さんの PC でマルウェア Y が検出されたとの報告があった。S さんが確認したところ，マルウェア Y は，既に正常に駆除されていた。S さんは，マルウェア Y について調査した。マルウェア Y の特徴は図 2 に示すとおりであった。

1. マルウェア Y の動作
   - ブラウザ又は PDF 閲覧ソフトの脆弱(ぜい)性を悪用して感染し，PC の起動時に自身が起動されるようにシステム設定を変更する。
   - 攻撃者が用意した C&C（Command & Control）サーバと通信する。
   - リモートシェルの実行，キー入力操作情報の収集などを行う。
   - ネットワークで接続された，他の PC，サーバに感染を広げる。
2. マルウェア Y と C&C サーバとのバックドア通信
   次の 2 通りがある。
   - プロキシサーバを経由せずに，TCP ポート番号 8050 を使用して，アクセスする。
   - プロキシサーバに対して，HTTP の CONNECT メソッドを使用してアクセスし，プロキシサーバから C&C サーバへは，任意のポート番号でアクセスする。

図 2　マルウェア Y の特徴

〔情報セキュリティインシデントの調査〕

情シ部で，他の全ての PC とサーバを調査したが，マルウェア Y に感染したものはなかった。

次に D さんに確認したところ，送信者メールアドレスが総務部の F さんであるメールを受信した際に，マルウェア Y が検出されたことが分かった。ところが，F さんにはそのようなメールを送信した覚えはないとのことであった。そこで，当該メールのメールヘッダを調査したところ，当該メールは，送信者メールアドレスを F さんのメールアドレスに偽装した上，外部のメールサーバから送られてきたことが分かった。添付ファイルは，PDF ファイルに偽装したものであった。

今回のインシデントでは情報漏えいの被害はなかったものの，同様なマルウェアによって情報漏えいが発生した他社の事例もあり，マルウェア対策を見直すことになった。受信メールの制限，バックドア通信の遮断，及びマルウェアから社内のサーバへの不正アクセスリスクの軽減策をそれぞれ検討するとともに，サーバの脆弱性検査を実施した。

〔受信メールの制限〕

次は，受信メールの制限についての，情シ部の K 部長と部下でセキュリティ担当の S さんの会話である。

K 部長：送信者メールアドレスのドメイン名が当社のものに偽装されていた場合は，受信者は開いてしまう可能性が高い。良い対策はないだろうか。

S さん：外部メールサーバにある，外部からのメールのフィルタリング機能を使用しましょう。具体的には，フィルタリングルールとして，送信ドメイン名のブラックリストに当社のドメイン名を指定します。

K 部長：それだと，①正規のメールも一部届かなくなるね。

S さん：そうですね。②フィルタリングルールを追加します。

〔バックドア通信の遮断〕

続いて，K 部長と S さんは，マルウェア Y と C&C サーバとのバックドア通信の遮断について検討した。次は，そのときの会話である。

S さん：マルウェア Y は，2 通りの方法で C&C サーバとの通信を試みます。一つ目は，プロキシサーバを経由しない方法であり，既に③防ぐことができています。二つ目は，マルウェア Y が，HTTP の CONNECT メソッドで任意のポート番号を用いる方法です。これについては，表 4 に示すアクセス制御ルールをプロキシサーバに設定すれば，許可するポート番号以外の通信を防ぐことができます。

表 4　プロキシサーバのアクセス制御ルール

項番	メソッド	ポート番号	動作
1	CONNECT	443	許可
2	CONNECT	全て	拒否
3	全て	全て	許可

注記　項番の小さいものから順に，最初に一致したルールが適用される。

K 部長：表 4 でアクセスを許可する通信をマルウェアが使用する場合の対策については，別途検討しよう。ところで，表 4 の設定では④業務に支障が出るので，⑤項番 1 と項番 2 の間に設定を 1 行追加する必要があるな。

〔マルウェアからサーバへの不正アクセスリスクの軽減策〕

次に，情シ部では，マルウェアから社内のサーバへの不正アクセスリスクの軽減策を検討した。開発サーバについては，現状，開発部の PC がマルウェアに感染してしまうと，そのマルウェアからアクセスされるリスクが高い。そのため，開発専用 PC を数十台，開発サーバセグメント内に置き，ソフトウェアパッケージの開発を開発専用 PC 及び開発サーバだけで行うようにし，かつ，⑥L3SW のフィルタリングルールを変更することによって，開発サーバがマルウェアからアクセスされるリスクを軽減することにした。さらに，開発専用 PC 自身がマルウェアに感染するリスクを軽減する対策も行うことにした。

一方，運用サーバセグメントのサーバについては，運用管理を行う PC がマルウェアに感染してしまうというリスクに絞って軽減することにした。具体的には，運用管理専用 PC を運用サーバセグメントに 1 台設置し，従来，情シ部の PC で行っていた運用サーバセグメントの管理を，そこで行うことにした。さらに，その運用管理専用 PC では，［ a ］を禁止することにした。

〔サーバの脆弱性検査〕

次に，情シ部で全サーバの脆弱性検査を行ったところ，OS のパスワード格納方法について，幾つかのサーバに脆弱性があることが分かった。これらのサーバでは，パスワードは，表 5 に示す二つのハッシュ値が格納される。OS の設定によって L2 ハッシュだけを格納することもできる。

表 5　L1 ハッシュと L2 ハッシュ

項目	L1 ハッシュ	L2 ハッシュ
パスワード文字種	英数字及び記号（合計 69 種）	英数字及び記号（合計 95 種）
パスワード長	1 字から 14 字まで	1 字から 127 字まで
文字列分割	8 字以上の場合は，前半 7 字と残りに分割 1)	なし
ハッシュ値のバイト数	16 バイト（生成された二つのハッシュ値を結合）	16 バイト
ソルトの使用の有無	なし	なし

注 1)　例えば，“1234567AB”というパスワードの場合，前半“1234567”と後半“AB”からそれぞれのハッシュ値を計算し，その 2 個の結果を結合して格納する。

次は，OS のパスワードの格納方法についての S さんと K 部長の会話である。

S さん：OS のパスワードのハッシュ値が入手できた場合に，14 字までのパスワードを総当たり攻撃で解析することを考えてみましょう。L1 ハッシュでは，前半 [b] 字までについて，最大で（$\sum_{i=1}^{[\ b\ ]}$ [c]）個のハッシュ値を求めれば，同じものを後半 [b] 字までについても使うことができます。一方，L2 ハッシュでは，最大で（$\sum_{i=1}^{[\ d\ ]}$ [e]）個となり，同一のパスワード長であっても，L1 ハッシュに比べ格段に増加します。

K 部長：なるほど。L1 ハッシュを格納しないように設定を変更しよう。ところで，表 5 にあるソルトを使用するとどのような効果が得られるのか。

S さん：ソルトを使用するとハッシュ値からパスワードを特定しにくくなります。

K 部長は，検討した対策案についての実施計画と，別途検討する項目についての検討時期を経営陣に報告し，対策を進めた。

設問 1　〔受信メールの制限〕について，(1)，(2)に答えよ。

(1)　本文中の下線①について，届かなくなるメールを 30 字以内で述べよ。

(2)　本文中の下線②について，追加するフィルタリングルールを 50 字以内で述べよ。

設問 2　〔バックドア通信の遮断〕について，(1)～(3)に答えよ。

(1)　本文中の下線③について，その理由を 30 字以内で述べよ。

(2)　本文中の下線④について，支障が出る業務を，本文中の用語を用いて 5 字以内で答えよ。

(3)　本文中の下線⑤について，追加すべき設定内容を表 4 に倣って答えよ。

設問 3　〔マルウェアからサーバへの不正アクセスリスクの軽減策〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑥について，L3SW でのフィルタリングルールの変更内容を 35 字以内で述べよ。

(2)　本文中の [a] に入れる適切な禁止事項を 35 字以内で具体的に述べよ。

設問4　〔サーバの脆弱性検査〕について，(1)，(2)に答えよ。

(1)　本文中の［ b ］～［ e ］に入れる適切な数式又は数値を答えよ。

(2)　ソルトを使用するとハッシュ値からパスワードを特定しにくくなるのはなぜか。その理由を35字以内で述べよ。

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。
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（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。