

平成 20 年度 秋期
情報セキュリティアドミニストレータ
午後 I 問題

試験時間

12:10 ~ 13:40 (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. この注意事項は、問題冊子の裏表紙に続きます。必ず読んでください。
4. 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。
5. 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 4
選択方法	3 問選択

6. 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、採点されません。
 - (3) 生年月日欄に、受験票に印字されているとおり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。
 - (4) 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。

なお、○印がない場合は、採点の対象になりません。4 問とも○印で囲んだ場合は、はじめの 3 問について採点します。

- (5) 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。
- (6) 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, 問 4 を選択した場合の例]

選択欄
問 1
問 2
問 3
問 4

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 Web 受注システムのセキュリティ対策に関する次の記述を読んで、設問 1～4 に答えよ。

X 社は、社員数 200 名の中堅製造販売会社である。東京に本社があり、首都圏近郊に物流拠点を兼ねた工場をもつ。10 年前に、一般消費者を対象とした通信販売事業を立ち上げ、5 年前からは、Web による受注を始めている。一般消費者が商品を購入した際の支払方法は、銀行振込か代金引換のいずれかである。X 社では、通信販売事業の効率向上を目的として、Web による受注に関連するシステム運用と開発業務を外部の 2 社に委託し、委託業務を X 社の通信販売事業部で管理している。

[Web 受注システムの概要]

図 1 に、X 社の Web 受注システムの構成を示す。Web 受注システムは、アウトソーシング事業者である Y 社のデータセンタに設置された、ルータ、ファイアウォール（以下、FW という）、Web サーバ、DNS サーバ及びデータベースサーバ（以下、DB サーバという）で構成されている。ルータ以外は Web 受注システム専用である。Web 受注システムでは、利用者はインターネットを介して Web サーバにアクセスし、利用者の端末と Web サーバ間のすべての通信は SSL によって暗号化されている。FW の管理、サーバのハードウェア保守とデータのバックアップ、OS とミドルウェアのバージョン管理・パッチ適用作業などの Web 受注システムの運用は Y 社に委託している。

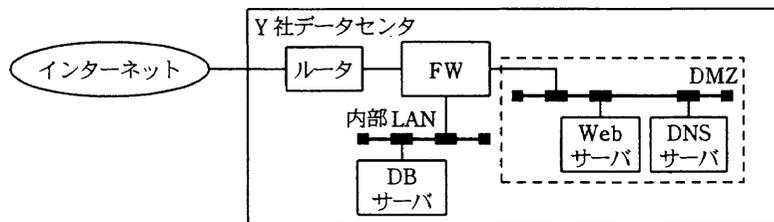


図 1 X 社の Web 受注システムの構成

Y 社には、利用者からの問合せ対応（以下、ヘルプデスクという）も委託している。ヘルプデスクでは、利用者からの操作上の質問や、システム不具合のクレームなどを受け付け、X 社が整備した対応マニュアルに基づいて対応するとともに、問合せ対応

の記録を X 社に提出している。

Web 受注システムで利用している Web アプリケーションプログラム（以下、Web 受注アプリという）の開発とバージョンアップは、ソフトウェアベンダである Z 社に委託している。納品された Web 受注アプリのインストールとデータベースの構成変更は、X 社の社員が行っている。Web 受注アプリの不具合については、ヘルプデスクから X 社に速やかに通報することを対応マニュアルに記載しており、X 社が主体となって対応している。

〔セキュリティ対策の見直しの契機〕

先月、通信販売事業会社である W 社の Web サイトが、Web アプリケーションプログラムの脆弱性を突いた攻撃を受けて、大量の個人情報^{ぜい}が漏えいしたことが、マスコミで大きく採り上げられた。その記事では、図 2 のような問題点が指摘されていた。

- | |
|--|
| <ol style="list-style-type: none">(1) 攻撃対象となった脆弱性については、以前からセキュリティ情報提供サイトで注意を喚起されていたが、W 社では対策を実施していなかった。(2) 利用者からの通報によって発覚した情報漏えいについて、対応状況は正しく記録された。しかし、W 社では対应手順が具体的に示されていなかったことが、対応を遅らせる一因となった。(3) (2)の通報以前にも、W 社は複数の利用者から、不審な支払請求が届いたとの問合せを受けていたが、いずれも利用者の操作ミスとみなしてしまい、セキュリティ事故として対策を開始するには至らなかった。(4) W 社では、過去に OS の脆弱性を突いた攻撃による情報漏えい事故が起きていたが、その際のノウハウは、次の事故の対策には生かされていなかった。 |
|--|

図 2 W 社における問題点

X 社では、Web による受注件数が順調に伸びてきたことに伴い、個人情報漏えい事故の可能性を重く受け止め、セキュリティ対策の見直しを行うことにした。

〔セキュリティ対策の見直し〕

次は、通信販売事業部の T 部長と Web 受注システム担当の R 君がセキュリティ対策の見直しを行ったときの会話である。

T 部長：まず、Web 受注システムのセキュリティ対策の現状の問題点について説明してくれ。

R 君：Web 受注システムでは、不正アクセスを防止するために、a方式

の FW が設置されています。この方式の FW では、パケットの b に含まれる情報に基づいてパケットの中継及び破棄を行うだけであり、b 以降の部分に含まれる攻撃コードはチェックできません。したがって、マスコミの記事で採り上げられていたような攻撃は、この方式の FW では防御できません。

T 部長：それでは、Web アプリケーションプログラムや OS の脆弱性を突いた攻撃に対して、どのような対策が考えられるのか。

R 君：2 点の見直しを検討しています。まず、1 点目として、Y 社が提供しているセキュリティ強化サービスの導入を検討しています。このサービスは、FW ではなく、複数のセキュリティ機能が統合された機器（以下、UTM (Unified Threat Management) という）を設置し、セキュリティを強化するものです。Y 社が採用している UTM の機能は、表のとおりです。現状の FW 機能に比べ、複数の機能が追加されるので、OS の脆弱性を突いたある種のバッファオーバーフロー攻撃などを防止できる効果があります。既知のバッファオーバーフロー攻撃への脆弱性に対しては、使用している OS 及びミドルウェアのバージョンを最新にするとともに、最新のパッチを適用することが有効ですが、① これらの対策を実行に移すまでには時間が掛かるので、この間に攻撃を受けて事故につながるリスクへの対応が課題となっていました。UTM の導入によって、このリスクを低減することができます。FW よりも高価ですが、対応可能な攻撃の種類は増加します。

表 UTM の機能

機能の名称	機能の概要
FW 機能	アクセス制御ルールに基づいて、パケットの中継及び破棄を行う。
VPN 機能	暗号技術を用いて、仮想的なプライベートネットワークを実現する。
侵入防御機能	シグネチャとのパターンマッチングに基づいて、不正アクセスを遮断する。
バッファオーバーフロー攻撃遮断機能	入力パケット全体を検査し、バッファオーバーフローに結びつくアクセスを遮断する。

T 部長：UTM を導入するだけでは対応できない攻撃というのものもあるのかね。

R 君：はい。例えば、② 既知の攻撃であっても、Web 受注アプリへの攻撃を、この

UTM だけで検知することはできません。Web 受注アプリの脆弱性を突いた攻撃に対応するためには、Web 受注アプリへの対策が必要です。これが 2 点目の対策です。

T 部長：それは、どのような対策かね。

R 君：既知の脆弱性を Web 受注アプリに残存させないことが重要です。Z 社は、セキュアプログラミングを考慮した開発規約を策定し、この規約にのっとり Web 受注アプリを開発しているそうです。しかし、当社は、Web 受注アプリの納品を受ける際には、動作確認を実施しているだけで、セキュリティ面での確認が不十分でした。今後は、納品を受ける際に、③ Web 受注アプリの開発時にセキュリティ対策が適切に実行されたことを確認します。さらに、新たな脆弱性が発見された場合に備え、緊急の改修要請に対応してもらえよう、Z 社との契約を見直します。

T 部長：外部から発表される脆弱性情報に的確に対応するためには、どうするのかね。

R 君：部内にセキュリティ対策担当者を置き、外部機関やセキュリティベンダから発表されるセキュリティの脆弱性情報を収集して、当社に関係がありそうな場合は、Z 社などに対策を依頼することを考えています。

T 部長：W 社の事例を見ると、セキュリティに関する利用者からの問合せについても、漏れなく対応する必要がある。W 社と同じ失敗をしないように、④ 対応手順を具体的に対応マニュアルに記述するとともに、内容に漏れがないよう点検してくれ。

R 君：分かりました。

その後、Web 受注システムのセキュリティ対策の見直しは順調に進み、対策を実行に移した。

設問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 アプリケーションゲートウェイ | イ コンテンツフィルタ |
| ウ セッション | エ データグラム |
| オ パケットフィルタ | カ ヘッダ |

設問2 UTM の機能について、(1)、(2)に答えよ。

- (1) 侵入防御機能の効果を維持するために、UTM 導入後の日常運用として実行すべき事項を、25 字以内で述べよ。
- (2) 本文中の下線②の、攻撃を UTM で検知できない理由を、25 字以内で述べよ。

設問3 セキュリティ対策の見直しについて、(1)、(2)に答えよ。

- (1) 本文中の下線①の、対策を実行に移すまでに時間が掛かる X 社の理由を、45 字以内で述べよ。
- (2) 本文中の下線③の確認として、X 社が実行すべき事項を、35 字以内で述べよ。

設問4 本文中の下線④について、対応マニュアルに記載することが必要な項目を、35 字以内で具体的に述べよ。また、対応マニュアル作成時にその対応手順の適切さを検証する方法を、20 字以内で述べよ。

問2 検疫システムに関する次の記述を読んで、設問1～4に答えよ。

U社は、社員数500名の化粧品販売会社である。U社では、情報システム部で定めた仕様のPCを各部署で購入・管理し、社員1人に1台ずつ配布している。特に、営業部員の場合は、外出や出張が多いので、ノートPCを配布し、社外への持出しを許可している。

〔セキュリティ対策の実施状況〕

U社では、PCにウイルス対策ソフトを導入している。社内ネットワークに接続するときには、パターンファイルを定期的に更新する規則となっている。OSのセキュリティパッチ（以下、パッチという）は、情報システム部から正式に適用するようアナウンスがあったものを利用者が手動で入手し、適用している。

情報システム部では、営業部員がノートPCを長期間持ち出し、パターンファイルの更新やパッチを適用しないまま社内ネットワークに接続することを問題視していた。

〔ウイルス感染事故の発生〕

ある日、ウイルスに感染したノートPCが社内ネットワークに接続され、ほかのPCがウイルスに二次感染する事故が発生した。このノートPCは営業部員が社外に持ち出していたもので、営業部員はウイルス感染には気が付いていなかった。情報システム部のM君が中心となって調査したところ、ウイルスは、OSのRPCプロトコルの脆弱性を利用して、利用者の操作を介さずに、ほかのPCやサーバに侵入するタイプであることが分かった。また、この脆弱性に対しては、OSの開発元からパッチが提供されており、以前に情報システム部から適用するようアナウンスがあったが、感染したノートPC及び二次感染したPCは、ウイルス対策ソフトのパターンファイルが未更新で、かつ、パッチが未適用であったことが判明した。パターンファイルの更新やパッチの適用を適切に実施していたほかのPCやサーバは、感染していなかった。

事態を重くみた情報システム部のE部長は、再発防止策を策定することにした。そのために、M君に再発防止策の検討を命じた。

E 部長：今回の事故の調査結果を報告してほしい。

M 君：持ち出したノート PC は、パターンファイルが未更新で、かつ、パッチが未適用のまま、外出先でインターネットに接続したことが原因で、ウイルスに感染しました。また、二次感染については、パターンファイルが未更新で、かつ、パッチが未適用の PC が社内ネットワークに多数存在し、被害が広がりました。

E 部長：ノート PC へのウイルス感染の問題だが、ノート PC は社外へ持ち出して使うわけだから、パターンファイルの更新やパッチの適用の徹底は難しいのではないか。

M 君：はい。持ち出したノート PC の管理の徹底は確かに難しいので、社内ネットワークを通じてほかの PC やサーバに感染する“ウイルスの二次感染”を防ぐことが重要です。最近では、PC のパターンファイルやパッチの更新状況などを自動的に検査し、検査結果に応じて、サーバや PC への接続の制限及びパターンファイルやパッチの強制的な更新を行う仕組み（以下、検疫システムという）があります。

E 部長：検疫システムを導入すれば、どのようなウイルスに対しても二次感染を防止できるのかね。

M 君：パターンファイルが提供されているウイルスやパッチが提供されている脆弱性を悪用するウイルスは防止できます。しかし、開発元が製品の脆弱性に関するパッチを提供する前に、その脆弱性を悪用する攻撃、つまり a には対応できません。

E 部長：その場合は、根本的に防止策がないということで、リスクを受容するしかない。今回は、事故の再発防止策として検疫システムの導入を検討してみよう。また、社内 PC のパッチ適用の対策も併せて検討してほしい。

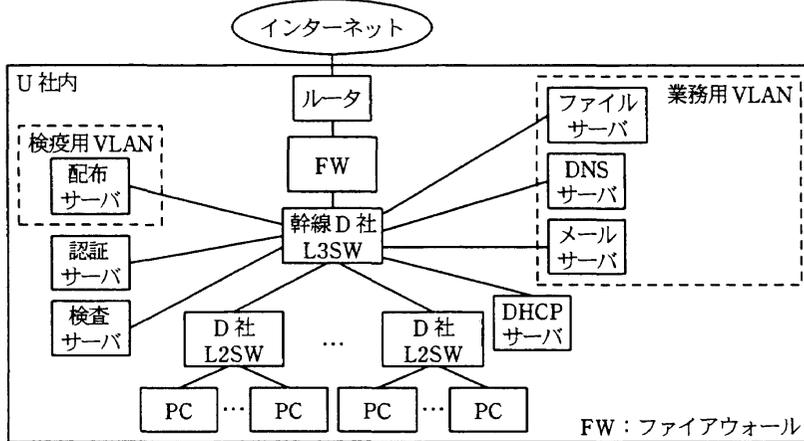
M 君：分かりました。

M 君は、市販の検疫システムを調査した。その結果、D 社検疫システムを選択し、その概要を図 1 のようにまとめ、E 部長に説明した。

1. ネットワーク構成

- (1) PC に接続するネットワーク機器を、D 社検疫システムに対応したレイヤ 2 スイッチ（以下、D 社 L2SW という）に置き換える。^(a)
- (2) PC のパターンファイルやパッチの更新が適切かどうかを検査するサーバ（以下、検査サーバという）、利用者を認証するサーバ（以下、認証サーバという）、パターンファイルやパッチを配布するサーバ（以下、配布サーバという）を、D 社検疫システムに対応したレイヤ 3 スイッチ（以下、

- 幹線 D 社 L3SW という) に接続する。
- (3) PC のパターンファイルやパッチの更新状況の情報を収集し、それらの情報を検査サーバへ送信するためのソフトウェア (以下、エージェントという) を PC に導入する。



2. 検査から業務用 VLAN アクセスまでのシーケンス (b)

- (1) PC を起動すると、エージェントが自動的に起動する。
- (2) エージェントは、認証要求を D 社 L2SW へ送信する。
- (3) D 社 L2SW は、(2) で受け取った認証要求を検査サーバへ送信する。
- (4) 検査サーバは、(3) で受け取った認証要求を認証サーバへ送信する。
- (5) 認証サーバで認証を行い、認証に成功した場合、認証許可を検査サーバへ送信する。
- (6) 検査サーバは、(5) で受け取った認証許可を D 社 L2SW へ送信する。
- (7) D 社 L2SW は、(6) で受け取った認証許可をエージェントへ送信する。
- (8) エージェントは、パターンファイルやパッチの更新状況の情報を D 社 L2SW へ送信する。
- (9) D 社 L2SW は、(8) で受け取った更新状況の情報を検査サーバへ送信する。
- (10) 検査サーバは、更新状況の情報を検査し、問題がなかった (パターンファイルやパッチの更新を行う必要がない) 場合、PC を業務用 VLAN に割り当てるよう、D 社 L2SW に指示する。
- (11) PC は、業務用 VLAN へアクセスする。

3. 検査の結果、パターンファイルやパッチの更新を行う必要がある場合の処理

検査の結果、PC のパターンファイルやパッチを更新する必要がある場合、検査サーバは PC を検疫用 VLAN に割り当てるよう D 社 L2SW に指示し、PC は配布サーバにアクセスする。配布サーバは、PC にパターンファイルやパッチを配布する。PC は、配布されたパターンファイルを更新し、パッチを適用する。PC の再起動後、再び検査を行う。

(以下、省略)

注 (a) D 社 L2SW は、幹線 D 社 L3SW と連動し、1 ポートで一つの機器を隔離する。具体的には、ポートに接続されている機器の MAC アドレスとポートのマッピングテーブルを作成し、このテーブルを基に隔離する。マッピングテーブルは、電源の入った機器がポートに接続されている間保持され、保持しているマッピングテーブルの情報とは異なる MAC アドレスを認識した場合、そのポートを経由した通信はできなくなる。機器の電源をオフにした場合や機器をポートから外した場合、マッピングテーブルは削除される。

(b) PC と D 社 L2SW 間は EAP (Extensible Authentication Protocol) を利用し、D 社 L2SW と検査サーバ間及び検査サーバと認証サーバ間は RADIUS プロトコルを利用する。

図 1 D 社検疫システムの概要

E 部長：君が D 社検疫システムを選択した理由を説明してくれないか。

M 君：検疫システムには様々な仕組みがありますが、今回のような事故の再発を防止するためには、PC を直接接続するネットワーク機器で隔離する必要があります。D 社検疫システムではその仕組みを採用しているので選択しました。もう少し詳しく説明しますと、D 社検疫システムでは b による認証方式を採用していて、PC に直接接続された D 社 L2SW で PC 単位に隔離します。また、検査の間、PC は D 社 L2SW との間での EAP 通信しかできないので、ほかの PC やサーバにウイルスが感染することがありません。ただし、PC に直接接続されているすべてのネットワーク機器を D 社 L2SW に変更するので、コストや導入の手間が掛かります。

E 部長：ほかの検疫システムは、どのような仕組みになっているのかね。

M 君：例えば、業務用 VLAN のセグメントだけを二次感染から防止できればよい場合には、Web を利用した検査を行う、図 2 のような Q 社検疫システムがあります。このシステムは、検査サーバ上に Web サーバを動作させ、PC のブラウザ上で稼働するエージェントと検査サーバ間で、http 通信によって検査を行います。また、業務用 VLAN の隔離は幹線 Q 社 L3SW で行います。検査で問題がないことが確認された PC だけが、幹線 Q 社 L3SW によって、業務用 VLAN へのアクセスが許可されます。ただし、このシステムでは、今回の事故で起こったような①二次感染の可能性が残ります。

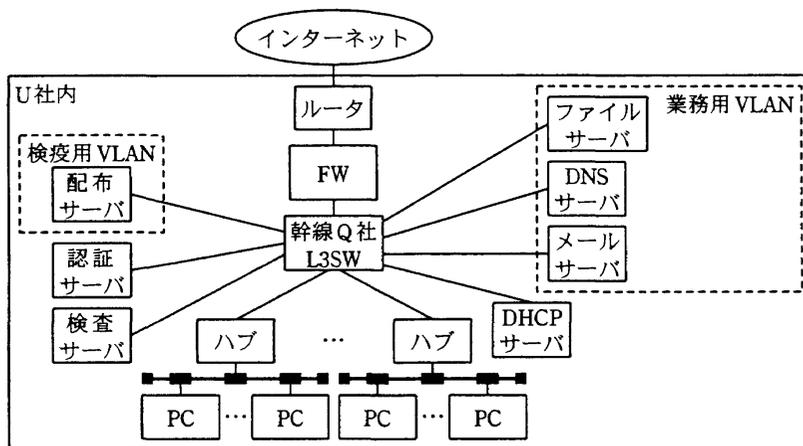


図 2 Q 社検疫システムの構成例

E 部長：そうか。D 社検疫システムを選択した理由は分かった。D 社 L2SW を使用してポート単位で隔離する場合、接続方法について制限事項があるが、それにも気を付けないといけないな。

M 君：はい。この制限に合った方法で接続しないと、そのポートを経由した通信ができないので、②そのような接続を行わないよう、周知徹底します。

M 君は、E 部長の指示に従い、D 社検疫システムの導入を開始した。

設問 1 本文中の , 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 IEEE 802.11b | イ IEEE 802.1X | ウ IEEE 802.3 |
| エ ゼロデイ攻撃 | オ トロイの木馬 | カ ポートスキャン |

設問 2 PC が DHCP サーバから IP アドレスを取得するのは、図 1 中の“2. 検査から業務用 VLAN アクセスまでのシーケンス”中のどの番号までに行う必要があるか。図 1 中の (1) ~ (11) の中から選び、番号で答えよ。

設問 3 本文中の下線①について、(1), (2) に答えよ。

- (1) 二次感染する可能性があるタイミング及び範囲について、それぞれ 30 字以内で具体的に述べよ。
- (2) 二次感染する可能性がある理由は何か。D 社検疫システムとの違いを考慮して、25 字以内で具体的に述べよ。

設問 4 本文中の下線②の接続方法について、その内容を 35 字以内で具体的に述べよ。

問3 生体認証による入退室管理に関する次の記述を読んで、設問1～4に答えよ。

A社は、社員数800名の中堅クレジットカード会社である。連結子会社を含めると社員数は3,000名を超える。本社、事務センタ及びコールセンタは東京にあり、営業所は全国に配置されている。また、データセンタは災害対策のために北関東と関西に分散配置されている。カード会員数は、現在1,500万人であるが、更にカード会員を獲得するために割引やボーナスポイントなどの様々な特典を用意するとともに、加盟店獲得にも積極的に取り組んでいる。

A社では、これまでも、社内に情報セキュリティ委員会を設置して情報セキュリティポリシーを策定し、個人情報の安全管理体制を整備してきた。事務室やコンピュータ室のドアは、テンキーによって解錠している。また、防犯のために、監視カメラで入退室画像を記録している。テンキーで入力する暗証番号は、部署ごとに管理している。最近では、3,000名を超える社員に加え、その2倍以上いる派遣要員やアルバイトなど、様々な勤務形態の従業員が入退室するようになった。暗証番号は、異動や退職があるたびに変わる規則なので、毎月のように変更を関係者に通知しなければならず、また、入退室の状況を正確に把握することも困難なことから、入退室管理の在り方を見直す時期にきていた。

[入退室管理の見直し]

前回の情報セキュリティ委員会で、だれが、いつ入退室したかを記録し、必要に応じて後で調査できるような、個人認証による入退室管理システムを導入することが決まった。即日、システム導入担当として、総務部のB課長と、情報セキュリティアドミニストレータのC主任が任命された。

B課長とC主任は、最初に、ICカードや生体認証などの個人認証方式について比較・検討を行った。A社では、従業員の入退室が頻繁なことから、行列を発生させないためには、高い が要求される。また、数日～数週間の派遣要員や短期雇用も多く、1か月間で各部署の要員が大きく入れ替わることから、そうした従業員に対する適用の容易さも必要となる。最終的に、これらの要件を満たす、非接触型ICカードを用いた入退室カードによる個人認証方式が全社的に導入されることになった。ただし、個人情報を扱う事務センタ及びデータセンタについては、入退室カードの不

正使用やなりすましを防ぎ、安全性を高める観点から、入退室カードだけでなく、生体認証を導入することになった。

次は、生体認証方式選定時のB課長とC主任の会話である。

B課長：いろいろな生体認証方式があるが、最適なのは何かな。

C主任：安全性を高めるには、高い が要求されます。指紋、虹彩、静脈などがこの条件を満たしていますが、今回のシステムでは、技術とコストの面から、指紋認証を用いたシステムが適当であると思います。

B課長：了解した。ただし、指紋登録できる人の割合（対応率）を100%にすることが極めて難しいという問題への対策も忘れないように。

ところで、人工模造の指によるなりすましの話も聞くが、実際はどうか。

C主任：なりすましや誤作動を誘発する攻撃には、人工模造物以外にも様々な手段が使われています。それらの攻撃には、図1に示す対策が必要となります。また、対策済の機器を選定し、登録時や認証時の環境を整備するとともに、運用でのセキュリティ確保も行う必要があります。

B課長：そうだと、事務センタとデータセンタに①指紋登録担当者や運用担当者を配置する必要があるな。

1. なりすまし攻撃への対策

- ・指紋の登録に際し、登録者本人であることを社員証などで確認する。
 - ・センサの 検知機能によって、人工模造物による登録及び認証を防止する。
 - ・登録された指紋データから指紋を推測できないデータ登録方式を採用し、登録者の指紋データを保護する。
 - ・本人の登録操作に立会者を置き、本人以外の指紋登録を防止する。
2. センサの不正な設定や操作による攻撃への対策
- ・温度や湿度などの異常を検知する機能によって、異常な環境下での不正認証を防止する。
 - ・センサの調整は、運用担当者自身が行うか、又は、作業に立ち会う。
3. 認証判定しきい値の変更による攻撃への対策
- ・異常なしきい値の設定を禁止する機能を利用する。
 - ・しきい値変更は、運用担当者が行う。

(以下、省略)

注 指紋：指先の皮膚表面が形成する模様

指紋データ：指紋の照合に用いるデータ

図1 なりすましや誤作動誘発の防止対策

B課長：照合に用いる指紋データは、イメージ画像として指紋を読み取った後、どのような処理によって生成されるのか。

C 主任：よく使われている方式では、分岐点などの することによって生成されます。

B 課長：セキュリティレベルを高くすることも大切だが、操作性への配慮はどうか。

C 主任：入退室カードを読ませて指をセンサに置くだけで認証できます。ただし、入退室管理システムは、勤怠管理システムなどと異なり、なりすまし防止が重要なことから、安全性要件としては 率を低くすることよりも、 率を低くすることを優先する必要があります。

〔入退室管理システムの導入〕

C 主任は、見直し結果を、指紋認証による入退室管理システム（以下、S システムという）の概要、S システム運用規程及び S システム利用規程としてまとめ、B 課長に報告した。図 2 は S システムの概要である。

- | |
|---|
| <ol style="list-style-type: none">1. システム構成
入退室カード、入退室カード読取装置、指紋認証装置（ドア用）、指紋登録装置、入退室管理サーバ、電気錠、受付電話、UPS から構成される。
指紋認証装置は、入退室カード読取装置と並べて、室外（入室用）と室内（退室用）に設置する。2. 指紋登録
指紋登録装置を用いて、任意の 2 指の指紋を登録する。3. 登録された指紋データの削除
異動や退職に連動して削除される。4. 電気錠の開閉
指紋が認証された場合に解錠し、ドアが閉まったら施錠する。解錠後にドアが開閉されなかった場合は、一定時間後に自動的に施錠される。5. 入退室管理サーバのログ
入退室した個人を特定できるログを、所定期間保存する。6. 来訪者対応
受付電話によって室内にいる社員が解錠する。対応者は、来訪者の入室から退室までの間付き添う。7. 監視カメラとの連携
入退室画像を記録し、所定期間保存する。データセンタにおいては、室内の画像も記録し、所定期間保存する。 |
|---|

図 2 S システムの概要

B 課長：図 2 の S システムの概要に関しては、問題が二つある。一つは、6.の来訪者対応だ。入退室管理システム見直し時の方針から、②対応者が来訪者に付き添うだけでは不十分だ。もう一つは、1.のシステム構成を見る限り、私が以

前に指摘した、③生体認証が避けて通れない問題への対策がとられていないことだ。

C主任：そうでした。早速、適切な措置をとります。

B課長：ところで、Sシステムの導入だが、入退室カードによる全社レベルの入退室管理システムの展開と同期を取って、まず、事務センタから試験導入したい。早速、準備を始めてもらいたい。

C主任：了解しました。

C主任の準備が的確であったこともあって、Sシステムの事務センタへの試験導入は無事完了した。現在は、データセンタへの展開を計画中である。

設問1 図1中の 及び本文中の , 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 可用 イ 攻撃 ウ 差分 エ 障害
オ 生体 カ 他人受入れ キ 本人拒否

設問2 本文中の , に入れる適切な評価事項を、それぞれ5字以内で答えよ。

設問3 指紋登録について、(1)、(2)に答えよ。

(1) 本文中の下線①の指紋登録担当者の作業内容を、40字以内で述べよ。

(2) 本文中の に入れる適切な字句を、15字以内で答えよ。

設問4 Sシステムの概要に関するB課長の指摘について、(1)、(2)に答えよ。

(1) 本文中の下線②に加えて行うべき、来訪者の入退室管理事項を、20字以内で述べよ。

(2) 本文中の下線③の問題に対する、Sシステムを活用した適切な措置を、50字以内で述べよ。

問4 Web サイトでの個人情報保護対策に関する次の記述を読んで、設問 1～4 に答えよ。

J 社は、社員数 250 名の市場調査会社である。J 社では、紙媒体を用いて街頭や郵送でのアンケート調査を実施していたが、昨年からインターネットを介する Web マーケットリサーチシステムを用いて、会員向けのアンケート表示・回答受付を開始した。Web マーケットリサーチシステムは、J 社の情報システム係が開発し、運用も情報システム係が担当している。

[セキュリティ強化の検討]

J 社では、アンケート調査のほかに、会員向けの Web ショッピングサービス事業も開始することにした。このサービスを提供するための Web ショッピングシステムは、Web マーケットリサーチシステムを改良することとし、図 1 のシステム構成を検討した。

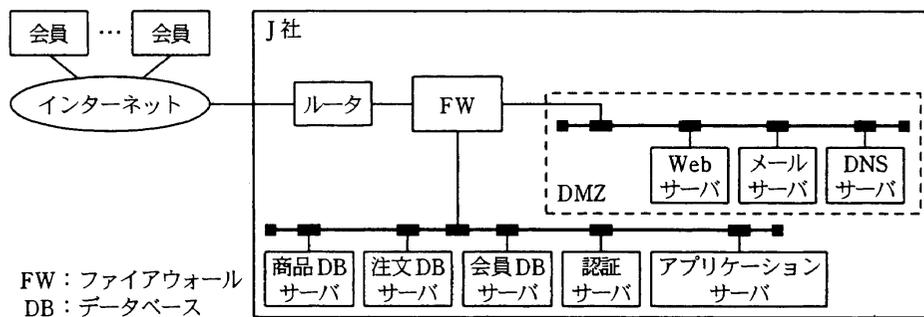


図 1 Web ショッピングシステム構成

これまで、会員の個人情報（以下、会員情報という）については、サービス内容の拡大時にはその都度会員の同意を得るなど、一定のレベルでの配慮を行ってきた。今後は、会員向けの Web ショッピングサービスを提供するために、技術的なセキュリティ強化を進めることにした。このセキュリティ強化について、システムインテグレータの H 社に相談することとし、窓口担当として、情報システム係の若手社員である N 君を指名した。

依頼を受けた H 社では、Web サイトにおける一般的な情報セキュリティ問題と対策について説明を行うことにし、情報セキュリティに詳しい K 氏が、次に示す表を用い

てN君に説明をした。

表 Web サイトにおける一般的な情報セキュリティ問題と対策

情報セキュリティ問題	対策（例）
・ 外部から内部ネットワークへの不正侵入	・ ネットワーク境界での不要な通信の遮断 ・ 適切なフィルタリングの設定
・ Web サーバの不適切な設定をねらった不正アクセス	・ 見慣れないファイルやプログラムがないことの確認 ・ 対象となるサーバの <input type="text" value="a"/> ・ 推測可能なパスワードの禁止 ・ 適切なアクセス制御の設定
・ Web アプリケーションの脆弱性をねらった不正アクセス	
（例1）SQL インジェクション攻撃	・ 悪意のある入力に起因する危険な SQL 文の実行を防ぐための、変数や演算結果の <input type="text" value="b"/>
（例2）ディレクトリトラバーサル攻撃	・ Web アプリケーションで用いる外部パラメタから <input type="text" value="c"/> する実装の回避
⋮	⋮
・ 業務運用及びシステム運用におけるオペレータの故意又は過失による情報漏えい	・ 業務運用及びシステム運用に伴うログの取得
（以下、省略）	（以下、省略）

N君は、表を踏まえた具体的なセキュリティ強化対策について、H社に提案を依頼した。

〔会員情報の保護への配慮〕

さらにN君は、Webショッピングサービスを安心して利用してもらうために、会員に対する注意喚起が必要であると考えた。そこで、注文受付サービスを行っている他社のWebサイトを参考にしながら、Webサイトに掲載するための“注意及びお願い”案（図2）を作成し、その内容についてH社に相談した。

会員の皆様へ

会員の皆様には、日ごろから御協力を賜り、厚く御礼申し上げます。このたび、皆様への新規サービスといたしまして、200x年mm月dd日から、Webショッピングサービスを提供させていただくことになりました。皆様の事前登録情報を安全に管理いたしますので、皆様にクレジットカードによるショッピングを安心かつ手軽にお楽しみいただくことができるようになります。

しかし、皆様も御承知のように、こうしたオンラインショッピングのWebサイトをターゲットに、利用者を不正なWebサイトに誘導して個人情報を詐取しようとする犯罪が後を絶ちません。

皆様におかれましては、こうした犯罪から個人情報を守るために、Webショッピングサービスの御利用の際には次の点に御留意ください。

- (a) お手元に配信された電子メール（以下、メールという）に記されているURLが、当社のWebショッピングサービスのURLであることを、アクセス前に御確認ください。(https://www.j-shop△△.co.jp/)
- (b) 仮にメールの送信元アドレスが当社であっても、このメールアドレスだけを信用して、メール中に埋め込まれたURLリンクをクリックしてアクセスしたり、会員IDやパスワードなどを入力したりしないようにしてください。アクセスを行う際には、過去に御自身が利用した際に登録したブックマークを利用することで、悪意のあるサイトへ誘導されることを回避できます。
- (c) アクセス中は、入力を促す画面のURLがhttpsで始まっていることと、アクセス中の情報秘匿を表す“鍵マーク”が表示されていることを御確認ください。この表示が見当たらない場合は、当社のWebショッピングサービスへのブックマークから接続し直してください。
- (d) アクセスしているWebサイトの安全性が確認できるまでは、個人を特定できる会員ID、パスワードなどの入力はお控えください。

注 図中のURL内の“△△”は、特定の文字列を表す。

図2 Webショッピングサービス利用の際の“注意及びお願い”案

次は、図2の“注意及びお願い”案に関するN君とK氏の会話である。

N君：他社のショッピングサイトを参考にして、会員の皆様への“注意及びお願い”案をまとめてみました。当社の会員をだまして、悪意あるWebサイトに誘い込んで情報を詐取する d への対策と考えています。これでよろしいでしょうか。

K氏：そうですね。例えば、(c)で鍵マークの表示を確認するように指示していますが、①鍵マークの表示それ自体は、会員が見ているWebサイトがJ社のものであることを示すものではありません。この部分は、追加の記述が必要です。

N君：なるほど。この部分は修正します。ほかにも問題がありますか。

K氏：会員が(b)を読むと、どうしてよいか分からず、J社のWebショッピングサービスが信用されなくなるおそれがあります。表現としても安心感を得られるように修正する一方で、信用してもらえらるための仕組みも構築すべきです。

N君：表現は修正します。仕組みの構築とは、具体的にはどうするのですか。

K氏：例えば、公開鍵暗号の技術を活用してメールの送信元を確認してもらう方法があります。メールに e を付与することによって、会員が必要な検証を行えるようにする、などの方法です。

図2の“注意及びお願い”案を修正したN君は、情報システム担当のG専務に内容を確認してもらうことにした。G専務は、会員が困ったときのヘルプデスクへの問合せについても追加記載しておくよう指示した。

次は、G専務の指示に関するN君とK氏の会話である。

N君：当社のG専務から、ヘルプデスクに関する記載を追加するよう指示を受けました。この点に関する注意事項はありますか。

K氏：会員が困ったときの照会用電話番号を明示することは、必要ですね。

攻撃者がJ社を装って会員に電話照会する可能性もあります。その場合、ソーシャルエンジニアリングによって、会員の情報が詐取される危険性があります。それに対する注意喚起も加えましょう。

N君：分かりました。では、②その点に関する注意も追加します。

N君はこれらの対策を盛り込み、G専務の承認を得た。N君の努力もあってセキュリティ強化も完了し、J社ではWebショッピングサービスの運用を開始することとなった。

設問1 表中の 及び本文中の , 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 環境対策	イ スキミング	ウ タイムスタンプ
エ 電子署名	オ 独立化	カ ハードニング
キ バックアップ	ク フィッシング	ケ メールヘッダ

設問2 表中の , に入れる適切な字句を、それぞれ10字以内で答えよ。

設問3 本文中の下線①について、(1)、(2)に答えよ。

(1) ブラウザの機能による鍵マークの画面表示によって担保されている内容を、20字以内で述べよ。

(2) 図2中の(c)に対して何を追加すべきか。追加内容を、60字以内で述べよ。

設問4 本文中の下線②について、J社を名乗る電話に対して、会員に注意を促すべき事項を、35字以内で述べよ。

7. 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	12:50 ~ 13:30
--------	---------------

8. 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。
9. 問題冊子の余白などは、適宜利用して構いません。
10. 試験中、机の上に置けるもの及び使用できるものは、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、黒鉛筆又はシャープペンシル、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、ティッシュ
これら以外は机の上に置けません。使用もできません。
11. 試験終了後、この問題冊子は持ち帰ることができます。
12. 答案用紙は、いかなる場合でも、すべて提出してください。回収時に提出しない場合は、採点されません。
13. 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。
14. 午後Ⅱの試験開始は 14:10 ですので、13:50 までに着席してください。

試験問題に記載されている会社名又は製品名は、それぞれ各社の商標又は登録商標です。

なお、試験問題では、® 及び ™ を明記していません。