

# テクニカルエンジニア（情報セキュリティ）試験

## サンプル問題

- ・午後 試験サンプル問題：1 ページ～4 ページ
- ・午後 試験サンプル問題：5 ページ～14 ページ

### 〔出題形式と試験時間〕

項目	午前	午後	午後
試験時間	9:30～11:10 (100分)	12:10～13:40 (90分)	14:10～16:10 (120分)
出題形式	多肢選択式 (四肢択一) 55問出題して 55問解答	記述式 4問出題して 3問解答	論述式 (事例解析) 2問出題して 1問解答



独立行政法人 情報処理推進機構  
情報処理技術者試験センター

午後 試験サンプル問題

問 侵入検知システム（IDS）によるセキュリティ監視に関する次の記述を読んで、設問 1～4 に答えよ。

X 社は、インスタント食品や冷凍食品、缶詰、調味料などの製造と販売を手がける大手総合食品メーカーである。X 社では、5 年ほど前に自社製品を販売する Web ベースの EC サイトを立ち上げた。EC サイト専用のインターネット接続回線を用意し、その構成は、図 1 のようになっている。また、セグメント A に対するファイアウォールのフィルタリングルールを表 1 に示す。

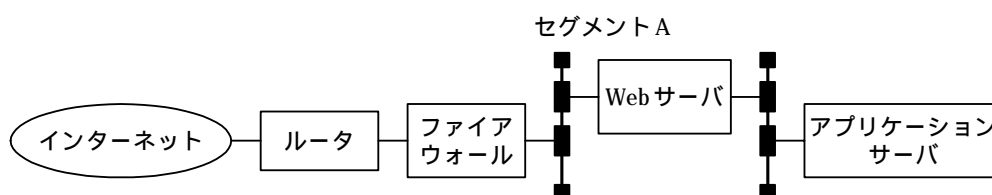


図 1 EC サイトの構成

表 1 セグメント A に対するファイアウォールのフィルタリングルール

プロトコル	送信元		あて先		動作
	IP アドレス	ポート番号	IP アドレス	ポート番号	
TCP	任意	任意	Web サーバ	80	許可 <sup>(1)</sup>
TCP	任意	任意	a	443	許可 <sup>(1)</sup>
b	Web サーバ	任意	ISP の DNS サーバ	53	許可 <sup>(1)</sup>
TCP	Web サーバ	任意	任意	25	許可 <sup>(1)</sup>
UDP	Web サーバ	任意	ISP の NTP サーバ	123	許可 <sup>(1)</sup>
上記以外					拒否

注<sup>(1)</sup> 動的フィルタリング機能によって、応答パケットも許可される。

EC サイトについての技術的な運用は、X 社の情報システム部に属する EC 運用グループが担当している。EC 運用グループには、現在、E 課長以下 5 名の社員が所属している。

〔 Web コンテンツの改ざんと復旧 〕

ある月曜日の朝、EC サイトの利用者からの通知によって、サイトのトップページの改ざんが発見された。EC 運用グループは、EC サイトを停止させるとともに、すぐ

さま復旧作業を開始した。その際に、次の仕様をもつトロイの木馬が仕掛けられていることが判明した。

- (a) Web サーバプログラムの機能拡張モジュールとしてインストールされる。
- (b) 外部から起動コマンドが送付されると、Web サーバの子プロセスとしてサーバプログラム（以下、木馬プロセスという）が起動する。
- (c) 起動コマンドは十数バイト程度の短いものであり、HTTP プロトコルが使われる。
- (d) 木馬プロセスは、自身が起動されたサーバマシン上の各種情報（パスワードファイル、コンテンツファイル、ユーザディレクトリ以下にある文書ファイルなど）を収集し、電子メール（以下、メールという）の添付ファイルとして特定のメールアドレスへ送信する。

Web コンテンツの復旧やトロイの木馬の削除などを含めて、復旧作業には 2 日を要した。トップページの改ざんは、金曜日の深夜に発生していたことが判明しており、月曜日の朝に通知を受けるまでの 2 日以上もの間、改ざんが検知されなかったことになる。また、土曜日の夜には、起動コマンドが送付されており、Web サーバ上で木馬プロセスが起動されていたことも判明している。ただし、Web サーバプログラムは限定的な権限をもったアカウントで動作しており、その子プロセスである木馬プロセスも同じ権限で動作するので、木馬プロセスによって社外へ送信されたのは、外部に公開しているコンテンツファイルだけであったと考えられた。

E 課長から今回の事故（以下、X 社事案という）の報告を受けた情報システム部の F 部長は、セキュリティ事故の発見が 2 日間も遅れた点や公開情報であるとはいえファイルが流出した点を問題視し、E 課長に改善を指示した。

#### 〔IDS の選定〕

E 課長は、EC 運用グループで主にセキュリティを担当している G 主任に、セキュリティ事故の早期発見のため、EC サイトに IDS を導入し、不審なアクセスを監視する体制を早急に検討するよう指示した。

G 主任は、IDS の選定と導入に先立って、IDS に関する調査を実施したところ、IDS は、大別して次の二つのタイプに分類されることが分かった。

- (1) 接続されたネットワークセグメント上のパケットを監視するタイプ（以下、NIDS という）
- (2) サーバ上にインストールされ、サーバに対するネットワークアクセスやサーバ上

のログを監視するタイプ（以下，HIDS という）

G 主任は，他社への導入実績が豊富な Z 社の IDS を選定し，NIDS 及び HIDS（以下，それぞれ Z-NIDS，Z-HIDS という）の機能を調査した。結果を表 2 に示す。

表 2 Z-NIDS と Z-HIDS の主な機能

	Z-NIDS	Z-HIDS
監視対象	ネットワーク上のパケット（同一セグメントに接続された機器全体を監視可能。ただし，暗号化されたパケットの監視は不可）	・サーバに対するネットワークアクセス（インストールした機器に対するアクセスだけを監視可能） ・サーバ上のログ ・ファイルの追加，変更，削除
検知時の通知方法	・コンソール画面へのメッセージ表示 ・指定したアドレスへのメール送信 ・SNMP トラップの発行 ・指定したプログラムの起動	同左
防御機能	RST パケットの送出による TCP セッションの切断	・同左 ・不審なパケットの破棄

少なくとも，X 社事案と同様の事故の発生を検知できる必要があるという点と，EC サイトでは SSL による暗号化通信を利用している点を考慮し，G 主任は，Z-NIDS と Z-HIDS の比較を表 3 にまとめた。その結果，EC サイトにおいては Z-HIDS を導入するのがよいと判断した。HIDS 導入の際の一般的な問題とされるインストールの手間については，監視対象が Web サーバ 1 台だけであるので問題にはならないと考えた。

表 3 Z-NIDS と Z-HIDS の比較

検討項目	Z-NIDS	Z-HIDS
X 社事案と同様の事故の検知		
Web ページの改ざん	c	d
トロイの木馬のインストール	e	f
起動コマンド	可（RST パケットは送信できるが， <u>防御は間に合わない</u> ）	可（該当パケットの破棄によって防御可能）
メールによるファイルの流出	不可（正常なメール送信との区別ができない）	同左
ファイアウォールを通過するプロトコルの監視	<u>一部のプロトコルは不可</u>	可

〔IDS の設定と運用〕

G 主任から IDS 選定の報告を受けた E 課長は、メールによるファイルの流出が検知できない点を問題視し、何らかの工夫によって検出できないか、G 主任に再検討を指示した。G 主任は、Web サーバから送信されるメールが注文内容の確認や会員情報の照会結果などの定型フォーマットのものだけであることから、次の方法によって、メールによるファイルの流出を検知することにし、E 課長の下承を得た。

- (1) Web サーバのメール送信プログラムの設定を変更し、送信メールのコピーを Web サーバ上に保存するようにする。
- (2) Z-HIDS のログファイル監視機能を利用して、送信メールのコピーをチェックし、定型フォーマットから外れた形式の場合に警告を発するよう設定する。

Z-HIDS が異常を検知した場合の通知方法として、G 主任は当初、担当者へのメール送信と SNMP トラップの発行を考えていた。しかし、E 課長から、監視対象となっているネットワークをイベントの通知手段として利用することには問題があるとの指摘を受けたので、Web サーバにモデムを接続して、担当者へのメールは、ダイヤルアップ回線経由で送信することにした。

G 主任は、選定した Z-HIDS を EC サイトに導入し、上記も含めた設定を施した後、運用を開始した。

設問 1 本文中の  ~  に入れる適切な字句を答えよ。  
なお、 ~  には“可”又は“不可”をそれぞれ選んで答えよ。

設問 2 表 3 について、(1)、(2)に答えよ。

- (1) 下線 の理由を 20 字以内で述べよ。
- (2) 下線 について、監視できないプロトコルを挙げ、監視できない理由を 20 字以内で述べよ。

設問 3 下線 について、送信メールを Web サーバ上に保存する際に注意すべき点を、アクセス権、保存場所、保存期間について、それぞれ 25 字以内で述べよ。

設問 4 下線 の理由を 45 字以内で述べよ。

## 午後 試験サンプル問題

問 安全な電子商取引システムの構築に関する次の記述を読んで、設問 1～5 に答えよ。

A 社は、衣類や生活雑貨、食品などを中心に扱う中規模の通信販売会社である。会員として登録された顧客あてに、カタログを四半期ごとに送付し、会員からの注文を電話、ファックス及び郵便で受け付ける。会員が注文した商品は、A 社からの指示に基づいて、その商品を取り扱う業者（以下、協力業者という）から注文した会員に直接送られる。

最近の業績は堅調に推移しているが、将来に不安を感じる傾向も見えてきている。A 社では、今後の成長戦略を検討し、多様な商品の迅速な提供を目的として、Web や電子メールの仕組みを使った電子商取引システム（以下、EC システムという）を新たに構築することにした。

EC システムは、電子カタログや広告などを掲載する Web サーバ（以下、掲載 Web という）、会員登録や注文などを受け付ける Web サーバ（以下、受注 Web という）、電子メールサーバなどから構成される。A 社は、会員の個人情報保護対策などの重要性を十分に認識しており、EC システムのセキュリティ確保を大きな課題として検討を始めた。

### 〔システム要件〕

顧客の獲得を目的として、不特定多数に情報を提供する掲載 Web のページと、会員が利用する受注 Web のページを用意する。会員が認証後にアクセスするすべての Web のページには、その会員の好みに合わせた商品ガイドを行うパーソナライズ機能をもたせる。会員認証は、安全で、かつ、会員の利便性を損なわない仕組みが必要である。また、電子メールは、A 社に対する各種の問合せに対応できるよう、不特定多数からの受信を想定する。

掲載 Web には、商品のアピールを目的として、商品購入者が評価や感想などを自由に書き込める掲示板機能を設ける。掲示板は、不特定多数の参照が可能であり、質問や苦情も書き込まれるので、A 社の信頼を確保することを目的として、これに迅速に対応することが非常に重要である。また、A 社は、協力業者ごとに担当の社員を定めており、各商品に対する問合せに担当の社員が回答する業務形態を採用している。各社員には掲示板に対する迅速な対応が求められるが、協力業者との協議や新たな業

者の開拓など、社外での業務も多い。

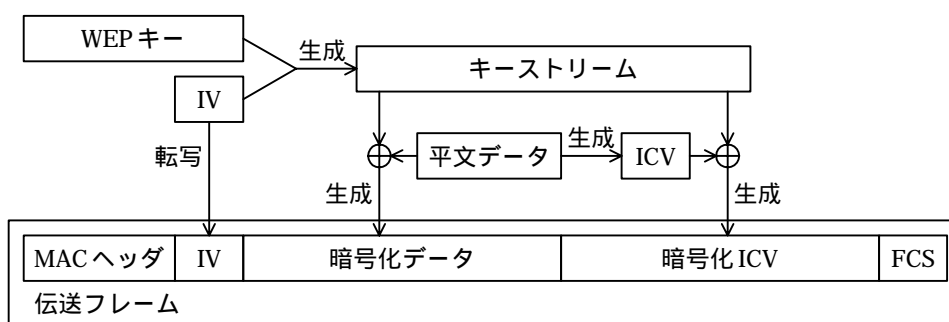
外出中にも迅速な対応が行えるように、社外から EC システムへアクセスすることを目的として、無線 LAN を使ったインターネット接続サービス（以下、無線 LAN サービスという）を利用したリモートアクセスを活用したい。社員は、掲示板の内容を変更したり削除したり、会員の情報へアクセスしたりする必要があり、リモートアクセスでの認証を厳格に行いたい。

〔リモートアクセスの検討〕

A 社から EC システムの構築を依頼された B 社の C 君は、セキュリティエンジニアの先輩である D 氏に指導を受けながら、無線 LAN サービスを利用する場合のセキュリティについて検討した。

C 君：無線 LAN サービスは、WEP (Wired Equivalent Privacy) を使用することによって、仮想的な専用線と同等なセキュリティが確保されるので、安全性が高まると思います。

D 氏：WEP を使用したとしても、仮想的な専用線と同様だと考えることには問題があります。この問題点は、WEP の仕組みと無線 LAN サービスの利用方法にあります。図 1 に、WEP の伝送フレームの概要を示します。



IV : Initialization Vector  
ICV : Integrity Check Value  
FCS : Frame Check Sequence

図 1 WEP の伝送フレームの概要

C 君：もし伝送フレームが盗聴されても、暗号化されているので安全だと思います。

D 氏：A 社が利用を予定しているプロバイダの無線 LAN サービスでは、WEP キーやローミングなどに利用される  に、利用者全員が同じ値を使用して、無線 LAN のアクセスポイントを使用しています。そのため、一定の条件が成立すると危険性が高まるのです。

C 君：もう少し詳しく説明してください。

D 氏：図 1 に示すとおり、WEP キーと IV から生成した  系列をキーストリームとして利用し、平文データとの排他的論理和を求めて平文データを暗号化します。同時に、平文データから伝送データの完全性を確保するために利用する ICV を生成して、同様に暗号化します。ここで、伝送フレーム数が  になると、同じキーストリームが使用される場合があるので、平文データを推定できる確率が高くなります。

C 君：なぜ、推定できる確率が高くなるのですか。

D 氏：同じキーストリームが使用された伝送データ同士の排他的論理和を求めると、 同士の排他的論理和が算出されるので、片方の  が推定できると、もう一方が簡単に特定できるからです。

C 君：標準的なプロトコルを使用していると、定型文字列 (“ http://www ” など) が伝送フレームに含まれるので、推定できる確率が高まるのですね。

D 氏：はい、そうです。ほかにも考慮する必要があります。例えば、暗号を解かなくても伝送フレームを  できる場合があります。つまり、WEP の伝送フレームを入手し、これに含まれる IP アドレスを変更して無線 LAN サービスのアクセスポイントに送ると、変更した IP アドレスあてに平文データを送信する攻撃（以下、パケット偽造攻撃という）が成立する可能性があります。

C 君：WEP だけを利用することでセキュリティを確保するには問題が多そうですね。

D 氏：はい。リモートアクセスを行う場合、WEP を使用する以外に、IPsec や SSL などのセキュアなプロトコルを併用すべきです。

C 君：社員が行う業務は、ブラウザを使用するので SSL を利用したいと思います。

〔社員認証の検討〕

パソコン（以下、PC という）とサーバの間は、SSL を利用してセキュアな通信路が形成される。利便性を多少犠牲にしても、セキュリティを重視する必要があるので、各社員に対して個別に発行された IC カードを利用して、社員を厳密に認証する。IC カードは、各自が IC カードに設定したコードを入力することで活性化される。C 君は、リモート環境での認証方式として、社員の IC カードと認証サーバに装着された IC カードの間での“チャレンジ/レスポンス認証”を用いることにした。

C 君：IC カードを使用するので、その耐タンパ性を利用して、暗号で使うかぎと個体識別情報を安全に格納できます。これらの情報は、IC カードの外からは読み取ることができません。この特徴を利用して、すべての IC カードに同一の共通かぎを格納し、社員からのレスポンス生成に、対称暗号方式を適用したいと思います。

D 氏：まず、EC システムにおいて、暗号化や復号に使用するかぎは、IC カードに必ず格納することにしましょう。次に、社員が、IC カードを紛失した場合の対処を考えてみましょう。例えば、IC カードの消費電力を分析する攻撃などによって、IC カードの耐タンパ性が衰える可能性があります。

C 君：IC カードの紛失は、必ず発生するので、その対策が必要になりますね。

D 氏：はい。紛失の防止策もとても重要ですが、その検討は、情報セキュリティアドミニストレータの E 君に依頼してください。ここでは、紛失が発生してからの対策を技術的な側面から検討しましょう。

C 君：紛失に気が付いた社員の申告から始まると思いますので、紛失した IC カードの個体識別番号を使用不可とし、その IC カードが活性化されたとしても、認証サーバで拒絶します。

D 氏：紛失した IC カード自体の不正使用は防止できますね。問題は、対称暗号で使用する共通かぎの危たい化です。この対策として、チャレンジとレスポンスの生成には、非対称暗号方式を適用しましょう。

C 君：はい。暗号で使うかぎは、必ず IC カードに格納し、非対称暗号を使用することにします。ほかに注意する点はありますか。

D 氏：認証方式の考慮点として、チャレンジに対してレスポンスが異常な場合でも、決してリトライしてはいけません。

C君は、D氏の協力を得て、ICカードと非対称暗号を利用した認証方式を確立した。

図2に、ICカード活性化後の社員の認証方式を示す。

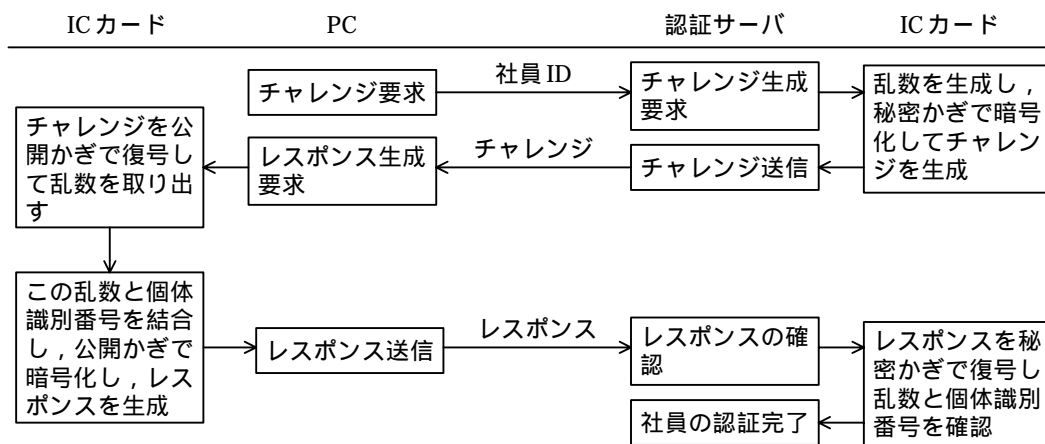


図2 社員の認証フロー

〔会員認証の検討〕

会員の認証は、利便性やコストを考慮する必要があり、会員IDとパスワードの対を使用する。会員IDは、会員の電子メールアドレスとし、認証用のパスワードは、会員自らが、氏名や住所などを登録するときに設定する。認証には、受注Webのサーバ証明書だけを使用したSSLを利用し、HTTPのベーシック認証を行う。会員がパスワードを入力ミスした場合、5回までのリトライを許可する。しかし、6回続けて入力ミスした会員の会員IDは使用不能とする。

会員は、社員と異なり、認証された会員だけに関する購入履歴や住所など、該当する自分の情報しか参照させない。つまり、ほかの会員に関する情報の参照や変更、消去などを許可しない。

会員に対して的確な情報の提供を目的に、Webページのパーソナライズ機能を実装する。同一の会員が、掲載Webと受注Webを1回の認証で利用するためにクッキーを使用する。クッキーには、会員を特定できる情報を格納する。表1にECシステムのWebサーバのドメイン名を示す。

表1 ECシステムのWebサーバのドメイン名

Webサーバ名	ドメイン名
掲載 Web	www.catalog.a.co.jp
受注 Web	www.order.a.co.jp

クッキーは、掲載 Web と受注 Web の双方を連続してアクセスするときに、会員から送信してもらう設定を行う必要がある。しかし、この設定をクッキーに対して行うと、クッキー情報が漏えいする可能性がある。その対策として、不特定多数からのアクセスを許容している掲載 Web に対して、SSL を使ってもアクセス可能とし、必要な設定をクッキーに対して行った。

〔システム構成の検討〕

社員は、業務上必要な範囲に限って、会員情報や購入履歴情報などに対するアクセスが許される。その情報の実体はサーバ側に置かれ、PC へのダウンロードを禁止する。社員は、ブラウザを使用して、必要な会員に関する情報を 5 人分単位でアクセスする。また、一人の社員が、複数の会員に関する情報に対するアクセスを、短時間の間で行えないように注意する必要がある。

会員に対して、A 社が記録している情報に対するアクセス状況を説明したり、社員のアクセス履歴を残したりする必要がある。これらを実現するため、ログサーバ（以下、LS をいう）を用意し、各サーバのアクセスログを集中管理することにした。LS には、会員情報や購入履歴情報などをアクセスできる社員のアクセスを禁止する。また、各サーバのログファイルも同様なアクセス制御を施す。ログ収集は、LS の保護を目的に LS が各サーバに対してポーリングする。

会員管理を行うため、会員情報を格納するためのデータベース（以下、会員 DB という）が必要となる。個人情報保護の観点から、会員 DB は、非常に高いレベルの安全性が求められる。特に、多くの会員情報が、短期間で危険な状態になることを避けることが重要である。

社員に対しては、業務を遂行するために必要な、会員 DB に格納されている任意の会員情報へのアクセスを許可する。また、会員から電話や郵便などで、住所変更などの依頼を受けた際には、電話による本人確認を行ったうえで、必要な情報を更新する。

特に、会員 DB に対するアクセスは、業務における必要最小限とする必要がある。

会員 DB の十分な保護を考慮し、図 3 に EC システムのネットワーク構成を示す。

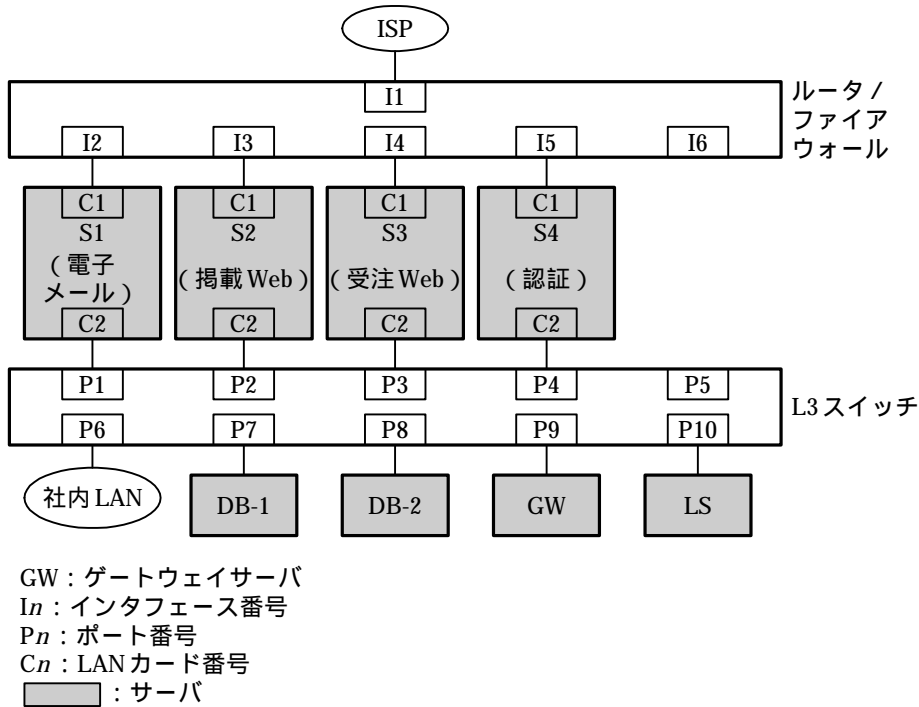


図 3 EC システムのネットワーク構成

S1 は電子メールサーバであり、SMTP と POP を使用している。社員は、L3 スイッチを経由して電子メールを使用する。S2 は掲載 Web であり、だれからでもアクセスできる。S3 は受注 Web であり、主に会員からアクセスされる。DB-1 は、カタログ情報が格納されているデータベースサーバであり、S2 から参照される。DB-2 には、会員 DB が構成されており、S3 から直接アクセスせず、GW を経由してアクセスされる。S4 は、社員の認証に用いる認証サーバであり、社員からだけアクセスされる。L3 スイッチでやり取りされる IP パケットは、あて先と送信元のアドレスがすべてプライベート IP アドレスを有している。また、ルータは、NAT やファイアウォール機能をもっている。

GW は、S3 と DB-2 の間の通信を定められたルールに基づいて中継する。S3 から会

員のパスワードを取得する命令が GW に送られても、GW はこれを DB-2 に中継しない。そのため、DB-2 には会員 DB 以外に、会員のパスワード処理機能をもたせる。また、会員情報を要求された場合でも、細心の注意を施したアクセス制御を行う。

各サーバ間の通信は、L3 スイッチが有する静的ルーティング機能を利用して、通信可能なサーバが限定されている。表 2 に L3 スイッチの仕様を示す。

表 2 L3 スイッチの仕様（抜粋）

ポート構成	100BASE-TX：10 ポート
スイッチング容量	9G ビット / 秒
スイッチング方式	ストア&フォワード方式
フィルタリング機能	次の条件を組み合わせて、IP パケットを通過又は破棄 (1) あて先及び送信元 IP アドレス (2) TCP ヘッダのあて先及び送信元ポート番号 (3) TCP ヘッダの SYN, ACK, FIN の各ビット
ルーティング機能	静的及び動的ルーティング
ネットワーク管理	SNMP
その他	ロギング機能を有する

SQL で制御される DB を利用する場合、サーバに侵入することなく、不正な SQL で DB を制御することが可能になる。例えば、会員がブラウザから入力した電子メールアドレスを、文字列としてプログラムが生成する SQL のパラメータに用いる。この場合、電子メールとして入力される文字列を細工することで、不正な SQL が生成される。

C 君：DB を使用しないシステム構成など考えられません。特に、個人情報などの重要な情報を格納する会員 DB は心配です。

D 氏：安全なシステムを構築するためには、システム側だけの対処では困難な場合がありますので、利用者にも協力を求める必要があります。例えば、電話番号を入力するところに着目してください。

C 君：電話番号を入力するところは、一つの欄にすべての電話番号を入力するのではなく、市外局番、市内局番及び加入者番号をすべて独立な欄に入力するのがいい。この程度なら、使用感も問題ないと思います。

D 氏：これは、任意に入力されるデータの範囲を限定したいからです。この場合ですと、数字しか入力されません。換言すると、数字以外の文字は受け付ける必要がありません。

C 君：なるほど、どんな値が入力されても、受注 Web を安全に動作させるために必要なのですね。

#### 〔システムの試験〕

これまでの検討結果を盛り込んで、安全な EC システムを構築し、ISP 接続を行わない状態での試験が完了した。次に、EC システムを ISP に接続し、外部との接続試験を行うことにした。まず、A 社に対する問合せを主な目的として使用する電子メールに関する試験を実施したところ、この試験において、スパムメールの踏み台にされる状況が発生してしまった。C 君が、S1 における SMTP の設定を調査した結果、S1 は、電子メールの不正な中継が可能であることが判明した。

C 君：S1 の設定を見直し、電子メールの不正中継対策を行いたいと思います。

D 氏：電子メールの不正中継対策を行うには、SMTP に関する設定を適切に行う必要があります。

C 君：不正利用者は、侵入したサーバから電子メールを自由に送信できるのに、なぜ、中継サーバを利用するのでしょうか。

D 氏：不正利用者の目的は、複数の相手に対して大量に電子メールを送信することです。電子メールの送信処理では、あて先サーバへのデータ転送に要する時間以外にも、必要な処理に多くの時間が費やされます。この時間は、複数の異なるあて先に対して電子メールを送信する場合、より多く必要になります。

C 君：SMTP に関する設定が弱いと、S1 がスパムメールの中継サーバとして利用されてしまうのですね。

D 氏：電子メールのあて先及び送信元のアドレスなどに着目して、電子メールを中継する条件を設定します。また、社外から S1 に対するアクセスに関して対処するルータのフィルタを適切に設定してください。

C 君は、S1 における電子メールの不正中継対策を無事に行った。ほかの試験も順調に完了し、A 社は、EC システムの稼働を開始した。

設問1 リモートアクセスについて、(1)、(2)に答えよ。

- (1) 本文中の  ~  に入れる適切な字句を答えよ。
- (2) 同一の WEP キーを使用した場合に暗号を解かなくとも、同じキーストリームを使っていることが判明してしまう理由を、20 字以内で述べよ。

設問2 会員の認証について、(1)、(2)に答えよ。

- (1) 会員がパスワードを入力する前に、受注 Web の証明書を確認しなければならない理由を、40 字以内で述べよ。
- (2) クッキーに設定すべき二つの属性を、それぞれ 20 字以内で述べよ。

設問3 システム構成について、(1)～(3)に答えよ。

- (1) S2 の静的ルーティング機能を利用せずに、L3 スイッチの静的ルーティング機能を利用している理由を、35 字以内で述べよ。
- (2) LS を守るための“P10”に設定すべきフィルタ内容を、35 字以内で述べよ。
- (3) 電話番号の入力時、会員 DB を保護するための入力値チェックが行いやすい理由を、25 字以内で述べよ。

設問4 電子メールの不正中継の回避について、(1)、(2)に答えよ。

- (1) S1 に設定すべき電子メールの中継に関するルールを、60 字以内で述べよ。
- (2) 社外から S1 に対するアクセスに関して対処するルータのフィルタとして設定すべき内容を、40 字以内で述べよ。

設問5 会員情報の保護について、(1)～(3)に答えよ。

- (1) 図 2 において、最初に C 君が提案した対称暗号方式に対して、D 氏が想定した問題点を、50 字以内で述べよ。
- (2) 正当な社員が、会員 DB をアクセスして会員情報を取得するときの制限事項を、35 字以内で述べよ。
- (3) 本文中で述べた会員情報の内部漏えい対策の妥当性を、社員認証と会員 DB のアクセス方法以外の観点から、50 字以内で述べよ。