平成18年度　秋期
情報セキュリティアドミニストレータ
午後Ⅱ　問題

試験時間	14:10 ～ 15:40（1時間30分）

注意事項

1. 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。
2. 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。
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2
選択方法	1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) 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。2問とも○印で囲んだ場合は，はじめの1問について採点します。

〔問2を選択した場合の例〕

選択欄
問1
(問2)

   (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。

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アプリケーションのセキュリティ対策に関する次の記述を読んで，設問1～5に答えよ。

A社は，若者向け衣料の製造販売業を営む，社員数800名の中堅企業である。東京に本社があり，海外に工場をもつ。3年前に，一般消費者を対象として，Webによる受注を始めた。昨年からは，希望する顧客に対してメールマガジン（以下，メルマガという）の配信も行っている。商品購入の際の支払は，銀行振込と代金引換のいずれかを選択できるが，クレジットカードによる支払は扱っていない。図1は受注システムの構成である。受注システムは，Webサーバ上のJavaアプリケーションの開発やデータベース（以下，DBという）サーバのDB設計を含め，A社システム部が独力で構築した。

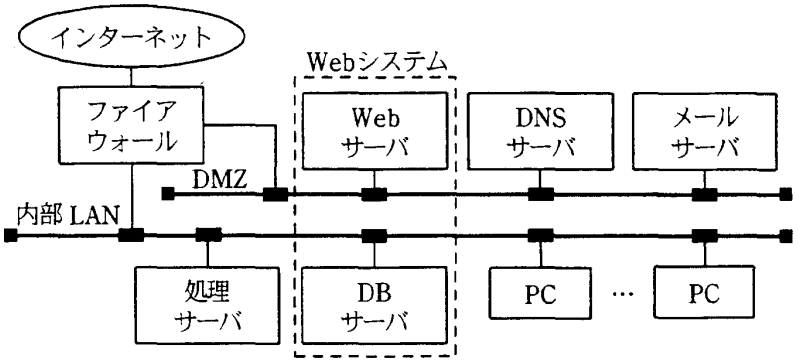

図1　受注システムの構成

図2はWebシステム設計書である。

1. サーバ構成
Webシステムは，DMZ上のWebサーバと，内部LAN上のDBサーバから構成される。Webサーバ上では，Webサーバプログラムと Java アプリケーションが稼働し，DBサーバ上では，DBMSが稼働する。DBには，Webページを生成するデータ（表示用DB）と，利用者がWebサーバに入力した情報を記録するデータ（入力用DB）が格納される。
2. Webページ構造
Webページは，内容が固定のページと，利用者からのアクセスの都度，内容を動的に生成するページから構成される。内容を動的に生成するページについては，Webサーバ上のJavaアプリケーションが利用者からの操作に応じて，表示用DBから必要なデータを読み出し，HTML文として組み立てる。
（以下，省略）

図2　Webシステム設計書（抜粋）

3年前は，システムの脆弱性を突いたホームページ書換え事故が多発した後であり，DMZ上のWebサーバの要塞化には特に注意を払った。現在も，Webサーバ上のJavaアプリケーションを除き，WebサーバとDBサーバのOS，Webサーバプログラム及びDBMSについては，セキュリティパッチを欠かさずに適用している。さらに，ウイルス対策ソフトを導入し，適切に運用している。

図3は，3年前に策定した，受注システムのセキュリティ対策方針である。受注システムの運用は，セキュリティの運用も含めてすべてA社内で対応し，外部業者には委託していない。

1. Webサーバ
   (1) Webサーバプログラムの脆弱性情報を継続的に入手し，脆弱性への対処を行う。
   (2) 外部からのリモート操作は禁止する。
   (3) 不要なサービスは停止し，不要なアカウントは削除する。
   (4) 公開を想定していないファイルは，公開用ディレクトリに格納しない。
   (5) 重要な情報を扱うページへのアクセスにはSSL通信を用いる。
2. Webアプリケーション
   (1) DBアカウントに適切な権限を与える。
   (2) Webアプリケーションへの攻撃事例に対して，適切な措置を講じる。
3. DBサーバ（省略）
4. ファイアウォール（省略）

図3　受注システムのセキュリティ対策方針

この3年間，受注システムは大きなトラブルもなく，Webによる受注件数は順調に伸びてきた。特に，この1年間の伸びは著しく，A社の総売上高の20％を占めるようになった。

最近，顧客の1人から“Webサイトの画面で入力を間違えたら，SQLの構文エラーメッセージが出てDBのテーブル名が表示された”といった情報が寄せられた。しかし，情報セキュリティ担当に指名されたばかりのA社システム部のC主任は，①安全上の問題に気付かず，何の処置も行わなかった。

〔事故発生〕

ある日，顧客の1人がA社のWebサイトにアクセスしたところ，ウイルスが検出されるという事故が発生した。事故の発生は，顧客からの苦情の電子メール（以下，メールという）が，A社の商品に関するお問合せ窓口に送られてきたことから露呈した。

苦情のメールの内容は，“A社が配信したメルマガ中に記載されているA社のWebサイトのURLにアクセスしたところ，ウイルス警告のメッセージが表示された”というものであった。

〔事故対応〕

顧客からの苦情のメールを受け，C主任は直ちに再現を試みたが，ウイルス警告のメッセージは確認できなかった。A社には，このような場合にどのように対応すればよいかが分かる社員がいなかった。C主任は考えあぐね，ウイルス対策関連サービス業者をインターネットで検索した。何社か選び電話で打診したところ，B社の技術力が高い印象を受けたので，電話に応対した技術担当のE氏に②苦情のメールをそのまま転送し助言を求めた。

E氏が問題のページにアクセスして再現を試みたところ，ウイルス警告のメッセージが表示された。そこで，E氏はC主任に対し，WebサーバのLANケーブルを抜き，すべてのサーバの電源を切らずにそのままにしておくことと，工事中画面が表示されるように設定されている予備のWebサーバに切り替えることを助言し，A社に駆け付けた。E氏の助言を受けたC主任は，上司のD部長の許可を得て，予備のWebサーバに切り替えた。

E氏が，警告のメッセージが表示されたウイルスをインターネットで検索して概要を調べた結果，ウイルスKの可能性があることが分かった。しかし，E氏が現場で調査した範囲では，不思議なことに，WebサーバからもDBサーバからもウイルスKは発見できなかった。また，WebサーバやDBサーバの設定，及びパスワードの設定も特に問題は見当たらなかった。

このような事態に初めて遭遇したD部長は，直ちに，社長名で情報セキュリティ委員会を開催し，自らリーダを務める緊急対応チームの編成を提案して，了承された。その日のうちに，B社に依頼した応援要員を含む緊急対応チームが招集され，原因究明を行う調査グループと顧客への対応を行う顧客対応グループの2グループが編成された。調査グループはウイルスKの感染経路の調査に当たり，顧客対応グループはメルマガ購読者に対する注意喚起メールの配信に当たった。注意喚起メールを配信した結果，“ウイルス警告のメッセージが表示された”との返信が3件あったが，幸いにして，ウイルスに感染して二次被害が発生したという報告はなかった。

調査グループが解析したところ，表示用DBの一部が不正コードに置き換えられていたことが判明した。この結果から，この事故は，次のような過程で顧客のPCにウイルスKを感染させようとしていたと推測できた。

(1) 何らかの攻撃によって，不正コードが表示用DBに書き込まれた。この不正コードは，ウイルスを感染させるために，攻撃者が用意したサーバを強制的にアクセスするように仕組まれていた。

(2) 受注システムのWebページの閲覧によって，不正コードを含んだページが生成され，顧客のPCにダウンロードされると同時に，不正コードが実行された。

(3) その結果，攻撃者が用意したサーバから顧客のPCにウイルスKがダウンロードされた。

すべてのサーバのログを分析した結果，不正コードはSQLインジェクション攻撃によって表示用DBに書き込まれていたことが分かった。A社ではすべてのサーバでログを採取していたものの，SQLインジェクション攻撃の警告を表示する仕組みはなかった。また，A社が導入していたPC用ウイルス対策ソフトは，この時点ではウイルスKに未対応で，顧客から指摘を受けるまで異常を発見できなかった。

このような外部からの攻撃が行われていたので，ほかにも攻撃を受け，顧客情報などが流出している可能性があり，事態は深刻であることが分かった。D部長は，緊急対応チームのメンバを総動員し，すべてのサーバのログを徹夜で精査したが，顧客情報などが流出したこん跡は特に見当たらなかった。

〔暫定対策〕

顧客からのWebサイト再開の要望が多かったこともあり，原因が判明したところで，Webサイト再開に向けて検討を急いだ。次は，そのときのC主任とE氏の会話である。

C主任：今回は，SQLインジェクション対策の不備を突かれてお客様に迷惑を掛けてしまいました。Webサイト再開に当たって，再度同様の攻撃を受けないように対処する必要があるので，どのような対策があり，最善策は何か，専門家の立場から助言してもらえますか。

E氏：対策としては，Webアプリケーションファイアウォールを設置する方法と

Webアプリケーションを修正する方法があります。後者は，エスケープ処理を施す方法と，DBMSの機能であるバインド機構を利用する方法が考えられます。SQLインジェクション対策のためのエスケープ処理とは，［ア］の場合に，例えば，“ ’ ”であれば“ ’ ’ ”のように“ ’ ”を二つ続けた文字列に置換する処理のことです。

C主任：バインド機構を利用するというのはどういう方法ですか。

E氏：はい。これは，プレースホルダと呼ばれる一時的な特殊文字を使用してSQL文のひな形を用意しておき，後で実際の値（変数）を割り当ててSQL文を完成させる方法です。変数は［a］にエスケープ処理されるので，DBMSの種類によって異なるエスケープ処理を意識する必要がなくなります。

C主任：なるほど。

E氏：次にWebアプリケーションファイアウォールですが，これは［b］のルールを登録する，いわゆるホワイトリスト方式のシステムで，ルールにないアクセスを阻止することができます。しかし，今からハードウェアやソフトウェアを手配してルールの設定をチューニングするのは時間が掛かるので，Webサイトの再開がいつになるか分かりません。お勧めするのは，SQL文を構成するすべての変数にエスケープ処理を施す方法です。

C主任：部長からは，Webサイト再開を催促されているのですが，エスケープ処理には，どれぐらい掛かりますか。

E氏：すべてのWebアプリケーションプログラムをチェックして書換えを行うと，10日間は掛かると思います。

C.主任：それでは早速，プログラムの修正に取り組むように，部長に提案してみます。

Webによる受注件数が無視できない状況から，D部長は5日間でチェックと書換えを行い，終了次第Webサイトを再開すること，及び作業に当たっては修正漏れと間違いをなくすために，2人一組でクロスチェックを徹底することを指示した。

B社の支援の下に，緊急対応チームとは別に編成されたチームのメンバは，連日徹夜ですべてのWebアプリケーションプログラムのチェック，書換え及びテストを5日間で完了させた。引き続き，OSを初期状態から再インストールした後，最新のセキュリティパッチを適用し，エスケープ処理が施されたWebアプリケーションをイン

ストールして，6日目の夕方に，事故のおわびの一文を掲載して，Webサイトを再開した。

〔本格的対策〕

D部長は，暫定対策が一段落したことから，今回の事故の教訓を生かした今後の対応について，C主任と検討した。

D部長：ところで，今回の事故だが，なぜ，もっと早く手を打てなかったのか。

C主任：SQLインジェクション攻撃のことは聞いていたのですが，受注システム構築時点では，実際の被害事例がなく，予算の制約もあって，対策の優先度を下げたと聞いています。その後も，そのままになっていたようです。

D部長：最近は被害事例が少なくないのに，対処できなかったのはなぜか。

C主任：セキュリティ事故の情報がはんらんしており，すべてに対応することはできなかったからです。

D部長：すべてに対応する必要はない。言うまでもないが，受注システムの仕組みは，システムを構築した我々が一番よく分かっている。そのことを踏まえて，的確な行動ができるように考えよう。話は変わるが，事故対応に当たっては君も大変だったと思うが，反省点として思い付くことはあるかね。

C主任：はい。私が試行錯誤で対応せざるを得なかった点は問題だったと思います。万が一に備えた，緊急対応マニュアルの整備も必要だと思います。

D部長：そうか。その前に，今後このような事故が起きないように，受注システムのセキュリティを強化したい。これからは，特にWebアプリケーションのセキュリティ対策が重要だと思う。早速だが，検討に取り掛かってほしい。顧客には絶対に迷惑を掛けられないからな。

C主任：はい。早速，検討に取り掛かります。

C主任は，インターネット上のWebサイトや専門書籍に記載されている一般的な対策事項を抜き出して，受注システムのセキュリティ強化要求仕様書（初版）を作成し，D部長に提出した。提出したセキュリティ強化要求仕様書（初版）を，図4に示す。

これに対して，D部長は，③C主任がセキュリティ強化要求仕様書（初版）の作成工程で必要な作業を実施していないことを指摘した。

現在のA社の受注システムに関するセキュリティ対策強化のための要求事項

1. 入力検証及び不正データ入力時の無効化
   悪意のある文字列を組み込んでアプリケーションを攻撃しても，本来権限のないDBサーバにはアクセスできないようにすること。
2. 認証と承認
   なりすましや管理者権限の不正取得などができないような措置を講じること。
3. 適切なパスワードやセッション情報の設定
   パスワードやセッション情報を不正に使用されないように，適切な措置を講じること。
4. ログの採取
   事故が発生した場合に追跡できる基礎情報を取得するために，各種ログを確実に採取する対策を講じること。また，ログへのアクセスは，権限者だけに限定すること。

なお，上記以外の事項に関しても，提案すべき対策などがあれば追加提案すること。

図4　セキュリティ強化要求仕様書（初版）

C主任は，D部長の指摘に従って作業方法の見直しを行い，1か月掛けてセキュリティ強化要求仕様書（第2版）を作成した。セキュリティ強化要求仕様書（第2版）は，D部長の承認を得た後，B社に提示された。

B社からは，A社の指定した期日に，図5のセキュリティ強化提案書が示された。C主任とD部長は提案書を詳細に評価し，提案がセキュリティ強化要求仕様書（第2版）を満たすものであることを確認し，B社に受注システムのセキュリティ強化対策の実施を発注した。

セキュリティ強化要求仕様書（第2版）に基づき，次のとおりご提案します。

第1ステップ

1. 入力検証及び不正データ入力時の無効化
   クロスサイトスクリプティング対策として次の強化を行う。
   (1) Webページに出力するすべての要素に対してエスケープ処理を施す。
   (2) ＜script＞... ＜/script＞要素の内容を含むWebページを動的に生成しない。
2. パスワード及びセッション情報の不正利用の防止
   セッション管理対策として，次の強化を行う。
   (1) セッション管理情報には［ c ］を使用し，クッキーに格納する場合は有効期限を設ける。
   (2) HTTPS通信で利用するクッキーには，secure属性を加える。
3. セキュリティ強化要求仕様書（第2版）に含まれていない重要事項
   3.1. ドメイン乗取りの防止
      ドメイン名を管理する［ d ］サーバが，正しく登録されているか，定期的に調査する。
   3.2. ファイル不正アクセスの防止
      (1) 外部からのパラメタに，Webサーバ内のファイル名を直接指定させない。
      (2) 外部からの入力値でファイル名を指定する場合は，［ e ］ディレクトリを指定し，かつ，ファイル名にディレクトリ名が含まれないようにする。

第2ステップ

（以下，省略）

図5　セキュリティ強化提案書

設問1　本文中の［　a　］～［　e　］に入れる適切な字句を答えよ。

(1) ［　a　］～［　c　］，［　e　］については，解答群の中から選び，記号で答えよ。

解答群

ア　異常系	イ　環境定数	ウ　擬似乱数	エ　固定
オ　自動的	カ　シリアル番号	キ　正常系	ク　選択的
ケ　代替	コ　同時	サ　プロセス番号	シ　ルート

(2) ［　d　］については，3字以内で答えよ。

設問2　A社が実施した事故対応について，(1)，(2)に答えよ。

(1)　E氏は，事故発生の相談を受けたとき，C主任にすべてのサーバの電源を切らないように助言した。電源を切ると原因究明にどのような支障があるか。30字以内で具体的に述べよ。

(2)　緊急対応チームの顧客対応グループが，メルマガ購読者に対する注意喚起メールの配信のほかに至急実施すべきことを，20字以内で述べよ。

設問3　本文中の［　ア　］に入れる適切な文章を，40字以内で答えよ。

設問4　C主任が取った行動について，(1)～(3)に答えよ。

(1)　本文中の下線①で，C主任が気付かなかった安全上の問題とは何か。また，その問題をどのように処置すればよかったか。それぞれ30字以内で述べよ。

(2)　本文中の下線②で，C主任が取った行動はどのような問題を引き起こす可能性があるか。二つ挙げ，それぞれ15字以内で述べよ。

(3)　本文中の下線③で，必要な作業とは何か。20字以内で述べよ。また，この作業を実施しないことによって生じる問題は何か。30字以内で述べよ。

設問5　A社では，セキュリティ対策が不十分だったので，SQLインジェクション攻撃への的確な対応ができなかった。今後の様々な攻撃に対し，必要性が生じたときに遅滞なく対処するためには，どのようなプロセスを実行すべきか。二つ挙げ，それぞれ30字以内で具体的に述べよ。

問2　旅行情報ネットワークシステムの情報セキュリティ自己点検に関する次の記述を読んで，設問1～4に答えよ。

J社は，売上高300億円，社員数300名の旅行業者で，パッケージ旅行や海外航空券などを販売している。J社では，設立時から販売業務を各営業所の窓口で行っているが，4年前に，会員制のインターネット予約販売（以下，Web販売という）を開始した。2年前には，Web販売を利用する会員数は1万人を超えた。

J社では，社員にPCを配布しており，旅行情報ネットワークシステム（以下，Rシステムという）を活用している。データセンタ事業者のY社と契約を結び，サーバなどは，Y社データセンタに設置している。現在のRシステムの構成を図1に示す。

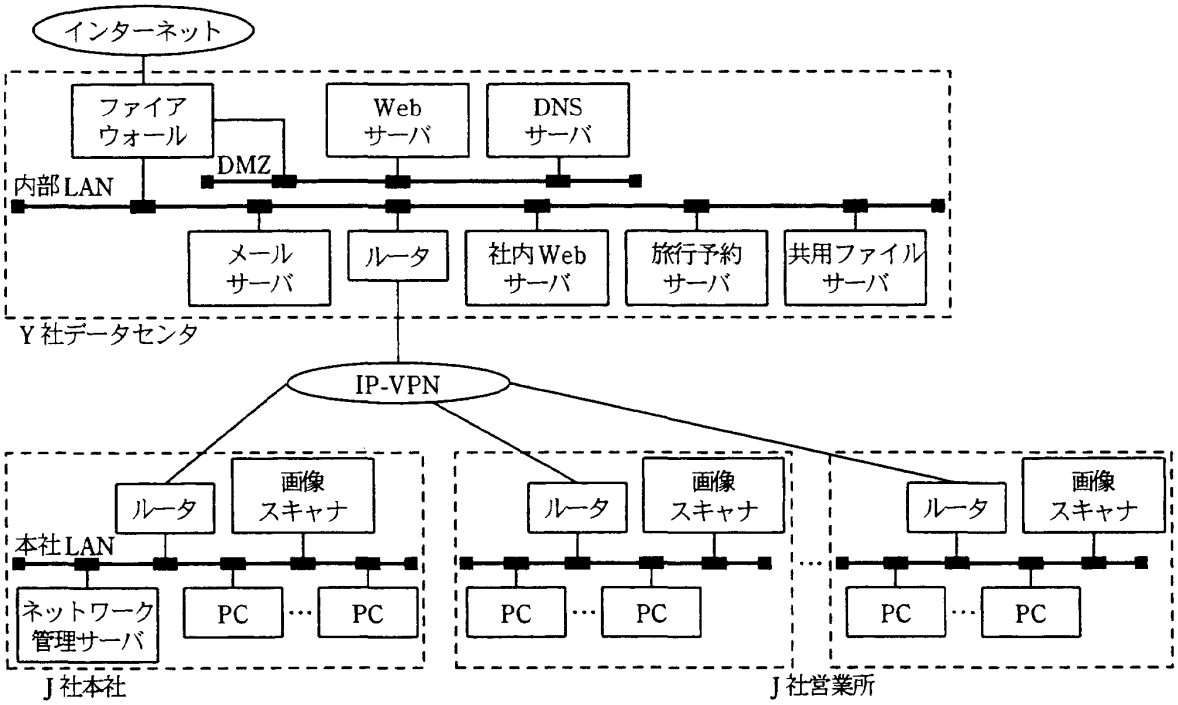

図1　Rシステムの構成

〔J社の業務内容と現在の情報セキュリティ体制〕

J社本社には，情報システム部，企画部，サービス部などがある。情報システム部では，Rシステムの運用管理業務の一部をベンダであるS社に委託している。S社は，Y社データセンタ及びJ社本社にSEを常駐させている。企画部では，パッケージ旅行の企画のために，大量の画像ファイルを扱うので，2年前にファイルサーバを独断で設置し，本社LANに接続した。取引先の各航空会社の営業担当者と共同で作成した企画書を，このファイルサーバに保存している。企画部を訪れる各航空会社の営業担当

者には，共通の利用者IDでファイルサーバを利用させている。サービス部では，会員の登録時に会員番号を付与し，J社だけで利用する条件で会員の同意を得た上で，パスポートを画像スキャナで読み込んでいる。J社本社や各営業所の窓口において，パッケージ旅行の航空券などを受け渡すときには，あらかじめ読み込んだパスポートの画像を参照して，本人確認をしている。また，サービス部では，取得した会員の個人情報はセキュリティ区画内だけで取り扱っている。このセキュリティ区画は，会員が出入りする接客区画とカウンタで仕切られている。

J社の主要3部署の業務内容を表1に示す。情報システム部のF君とサービス部のG君は，入社7年目の係長であり，本来の担当業務に加え，それぞれ所属する部署の情報セキュリティ対策の運用も担当している。

表1　主要3部署の業務内容

部署名 / 項目	情報システム部	企画部	サービス部
業務概要	Rシステムの運用管理，情報セキュリティ対策支援	航空会社やホテルと提携したパッケージ旅行の企画	会員登録，会員に対するパッケージ旅行の販売，航空券の予約受付・販売
業務で扱う情報	社員などの個人情報，情報システム設計書	航空会社との共同作業による企画情報（機密情報を含む）	会員の個人情報（パスポートの情報，個人の機微情報を含む）
主管する情報システム	社内Webサーバ，メールサーバ，共用ファイルサーバ，ネットワーク管理サーバ	Webサーバ（広告，宣伝）	旅行予約サーバ（会員の個人情報，予約情報など），Webサーバ（Web販売）
責任者	M部長	（省略）	N部長
セキュリティ担当者	F君	（省略）	G君
セキュリティ区画	執務室，サーバ室	執務室	執務区画（接客区画と執務区画はカウンタで仕切られている）
入室制限	社員やベンダSEがサーバ室に入室する際に，虹彩による認証が必要	部外者が執務室に入室する際に，受付社員による本人確認が必要	会員は執務区画には入室不可
印刷出力	執務室の共用プリンタ，サーバ室の共用プリンタ	執務室の共用プリンタ	執務区画内の共用プリンタ
主な外部委託業務	Rシステムの運用管理・保守，利用者IDの登録・削除・変更など	パッケージ旅行のパンフレットの印刷	ダイレクトメール（以下，DMという）の発送
その他	Rシステムのネットワーク管理サーバはサーバ室に設置	企画部が独断で設置したファイルサーバのログは採取されていない	会員の個人情報の利用は，J社内部に限られている

J社は5年前に，社長を委員長，各部署の部長を委員とする情報セキュリティ委員会を設置し，コンサルタント会社の協力を得て，情報セキュリティポリシを策定した。情報セキュリティ委員会は2年前に，情報セキュリティポリシに対して，個人情報の記載の追加と外部委託管理項目の修正を行った。現在の情報セキュリティポリシを図2に示す。各部署では，情報セキュリティ対策を実施し，情報システム部では，全従業者に情報セキュリティポリシを認知させて遵守させること（以下，浸透という），及び各部署における情報セキュリティ対策の実施を支援することを役割としている。

情報セキュリティポリシ

社　長

Ⅰ．基本方針（省略）

Ⅱ．対策基準

1. 適用範囲

(1) 本基準は，社員（役員，管理職，一般職及び契約社員）及び派遣社員の全従業者に適用する。

(2) 本基準は，J社で利用するすべての情報資産（ハードウェア，ソフトウェア，ネットワーク，記録媒体及び情報（紙文書，電子化情報））を対象とする。

2. 資産管理

J社の情報は，重要度に応じてA（極秘情報），B（機密情報，個人情報），C（重要情報），D（公開情報）の四つに分け，その重要度に応じたラベルを付ける。

3. 人的資源セキュリティ

(1) 従業者は，毎年，新たな知識習得と意識向上のために，情報セキュリティ教育を受講する。

(2) 従業者は，雇用や契約の開始に際しては，情報セキュリティに関する条件に同意する。

(3) 従業者は，業務上の必要性があって，外来者に社内の情報システムを利用させる場合には，外来者に対して情報セキュリティポリシを遵守する旨の誓約書を提示し，同意を得て署名させる。

4. 物理的及び環境的セキュリティ

(1) 重要度A，Bの情報の作成，編集，保存及び印刷は，セキュリティ区画内で実施する。

(2) 従業者は，セキュリティ区画の出入りに，写真付きのICカードを用いる。

(3) セキュリティ区画に外来者を入室させるときは，訪問者用IDカードを携帯させ，社員が付き添う。

5. 通信及び運用管理

(1) Webサーバへのアクセスは，SSLで保護する。

(2) 重要度A～Cの情報は，定期的にバックアップを取得する。

(3) 重要度A～Cの情報の取扱いを外部委託する場合には，事前に情報セキュリティ要求事項を定め，管理の実施について契約を交わす。

(4) 情報資産を廃棄する際には情報漏えいに注意する。

6. アクセス制御

(1) 重要度A～Cの情報を扱う情報システムにアクセスする場合には，個人を特定できる利用者IDを用いる。

(2) 重要度Aの情報へのアクセスや印刷は，権限者だけが実施する。

(3) 重要度B，Cの情報へのアクセスや印刷は，権限者又は権限を委譲された者が，許可された機器で実施する。

(4) 重要度A～Cの情報へのアクセスや印刷の履歴はすべてログに記録し，権限者が許可内容に対する違反の有無を確認する。

7. 情報システムの取得，開発及び保守

社内の情報システムの設定は，所属長の承認の下，情報システム部の許可を得て実施する。

以上

図2　現在の情報セキュリティポリシ

〔情報セキュリティ自己点検の実施〕

M部長は，情報セキュリティポリシの浸透の度合い（以下，浸透度という）を調べることにした。そこで，F君と協力して，図3に示す情報セキュリティ自己点検（以下，自己点検という）の手順に基づいて，質問を作成した。

(1) 現在の情報セキュリティポリシの浸透度を調べるために，認知と実践についての質問を作成する。
(2) 社内Webサーバ上に，自己点検の結果を入力するための回答ページを用意する。
(3) 自己点検の実施を電子メール（以下，メールという）で全従業者に周知する。
(4) 従業者は，自己点検の結果を無記名で回答ページに入力する。
(5) 情報システム部が回答を確認して，結果をまとめる。

図3　自己点検の手順

M部長は，全従業者に対して，情報セキュリティポリシを参照しつつ自己点検を実施するように指示し，自己点検の結果を回答ページに入力させた。自己点検の質問と結果を表2に示す。

表2　自己点検の質問と結果（抜粋）

項目	項番	質問	結果(1)			
			会社全体	情報システム部	企画部	サービス部
情報資産管理	(1)	あなたは，情報を重要度に応じて分類するルールを知っていますか。	1.73	1.75	1.67	1.77
	(2)	あなたは，個人情報を重要度Bに分類していますか。	1.55	1.46	1.53	1.63
アクセス制御	(3)	あなたは，重要度B，Cの情報を印刷できるのは，権限者又は権限を委譲された者に限られていることを知っていますか。	1.14	1.31	0.93	1.00
	(4)	あなたの周りでは，重要度B，Cの情報を権限者又は権限を委譲された者が，印刷していますか。	0.86	1.15	0.60	0.63
入退管理	(5)	ア	1.78	1.69	1.80	1.88
教育	(6)	あなたは，情報セキュリティ教育を毎年受講しなければならないことを知っていますか。	1.55	1.46	1.60	1.56
	(7)	あなたは，昨年の情報セキュリティ教育を受講しましたか。	1.02	1.08	0.93	1.06
外部委託管理	(8)	イ	1.14	1.08	1.33	1.06

注(1)　結果は，各質問に“はい（該当する）”と回答した場合を2点，“いいえ（該当しない）”と回答した場合を0点，“部分的に該当する”と回答した場合を1点として，質問ごとの単純平均値を会社全体と部署別（主要3部署以外の記述は省略）に算出したものである。また，“分からない”と回答した場合については，0点とした。

M部長とF君は，自己点検の結果を見て，次のような議論を交わした。

F君：表2の結果から考えると，項番(3)，(4)，(8)に対応する情報セキュリティ対策基準の内容について，全社研修で周知徹底すべきだと思います。

M部長：いや，点数の高低だけで研修項目を決めるべきではない。研修テーマは，情報セキュリティに関する障害などの［ a ］と［ b ］，研修実施によって期待される教育効果の程度などを含めて総合的に判断する必要がある。

F君：研修による教育効果があるか否かは，どのように判断すればよいのでしょうか。

M部長：今回の自己点検の質問は，認知と実践などの観点から作成されている。認知については，従業者の知識不足が問題であるから，研修によって，ある程度の効果は得られると思う。また，実践の調査である項番(2)に“いいえ”と回答した場合には，対応する図2中のⅡ.2.について，意図的な未実施の場合と［ c ］の場合が考えられる。［ c ］の場合についても，研修による効果が期待できる。一方，意図的な未実施の場合については，研修以外の方法で浸透度向上対策を検討する必要がある。

〔各部署における情報セキュリティ対策のヒアリング〕

M部長は，自己点検の結果に情報セキュリティ上の問題が見受けられたことから，各部署を訪問してヒアリングを実施し，リスク対応の状況を確認した。最初にサービス部を訪問した。最近，サービス部では，提携代理店でも航空券を受け取れるサービス項目を追加している。次は，M部長とサービス部のN部長とG君の会話である。

M部長：表2の自己点検の結果を見ると，サービス部では，アクセス制御と外部委託管理の浸透度が低いようです。外部委託管理はどのように実施していますか。

N部長：販売促進のために，会員に対して毎月DMを送付している。その都度，複数の業者に発送作業を委託しているが，付き合いの長い業者ばかりで問題も起きていないことから，業者への立入調査は行っていない。

M部長：個人情報保護法では，委託先の［ d ］が条文に明記されているので，

DM発送の外部委託には十分に注意してください。

N部長：個人情報保護は，近年になって急に重要度が高まってきているにもかかわらず，DM発送の委託先とはそれ以前からの付き合いということもあって，リスクとしての認識が甘かったかもしれないな。

M部長：ところで，会員の旅行日程表や予約確認書などの個人情報を記した書類はどのように印刷しているのかね。

G君：外来者が近づきにくい執務区画にプリンタを設置して，許可された人だけが印刷しています。また，個人情報を扱う業務では，従業者は，PCから旅行予約サーバにアクセスし，そのサーバで実行されているWebアプリケーションを介してデータを取り出し，PCのJavaアプレットでレイアウトして，プリンタに送って印刷しています。このレイアウトの際，Javaアプレットが背景に“機密情報”という文字を挿入しているので，従業者に注意を喚起することができます。

M部長：個人情報であるという注意は喚起されているが，だれが印刷したかは分からない。印刷物をプリンタのトレイに置き忘れて，別の従業者が取り違えるようなことはないのかね。

G君：はい。ある従業者が出力した印刷物を，ほかの従業者が自分の印刷物と一緒に取り出してしまい，別の会員に渡してしまったというミスが過去にありました。

M部長：最新のプリンタには，WebアプリケーションやJavaアプレットなどを変更せずに，①そのようなミスをなくすための仕組みを実現できるものがあるので，導入を検討してみてはどうかね。ところで，Web販売の海外航空券を提携代理店の窓口で手渡しできるようにするサービス項目の追加について，情報セキュリティ面から検討はしたのかね。

G君：Web販売では，会員からの入力データがSSLで保護されています。予約結果の確認は，平文のメールで会員に送っています。このメールには，予約番号，旅行者情報，旅行日程などが含まれています。このシステムは4年前から稼働しており，実績があるので，今回のサービス項目の追加によって情報セキュリティ対策を見直す必要はないと考えています。

M部長：今回のサービス項目の追加は，提携代理店での受渡しなのでリスクが変わる

はずだ。

G君：予約番号を示して海外航空券を受け取ることは従来と同じなので，リスクも変わらないと考えました。

M部長：それは違うはずだ。予約番号を不正に入手した者による［　e　］のリスクが高くなっている。提携代理店の窓口で海外航空券を手渡す場合には［　ウ　］を徹底するなどの対策が必要だ。

G君：分かりました。

次に，M部長は企画部を訪問し，アクセス制御の認知と実践についてヒアリングを実施した。企画部では，独断でファイルサーバを本社LANに接続したことに加え，ほかにも②情報セキュリティポリシへの違反が見受けられた。ファイルサーバについては，特にリスクが高いので，企画部による運用を中止させ，情報システム部が運用することにした。

M部長は，情報システム部についても自己点検の結果を見直した。外部委託管理の浸透度が低いことから，情報セキュリティ対策を追加する必要があると考え，F君に問題点を調べさせた。F君がRシステムの外部委託管理について調べたところ，S社への作業指示やJ社の管理に問題はないものの，部内でどのような外部委託管理が行われているかを知らない社員が多いことが分かった。そこで，F君は，情報システム部の外部委託管理の浸透度が低い問題は，部内での情報共有が不十分であることに起因していると結論付けて，M部長に報告した。M部長は，F君の報告を受けて，部内の各業務について情報交換会を設けることにした。

〔情報セキュリティマネジメントシステムの再構築〕

M部長は，各部署のヒアリング結果から，J社のサービス部や企画部では情報セキュリティマネジメントシステムが十分に機能せず，リスク対応が十分ではないことが分かった。これに対処するために，③情報セキュリティマネジメントシステムを再構築し，速やかにリスク分析を行ってリスク対応の遅れを最小限にとどめるようにした。

設問1　本文中の［　a　］～［　e　］に入れる適切な字句を答えよ。

(1)［　a　］，［　b　］については，解答群の中から選び，記号で答えよ。

解答群

ア　影響度　　イ　機密度　　ウ　信頼度　　エ　対応

オ　人気度　　カ　発生頻度

(2)［　c　］～［　e　］については，それぞれ5字以内で答えよ。

設問2　自己点検について，(1)，(2)に答えよ。

(1)　表2中の［　ア　］に入れる認知についての質問文を，50字以内で答えよ。

(2)　表2中の［　イ　］に入れる実践についての質問文を，60字以内で答えよ。

設問3　M部長が実施した，各部署における情報セキュリティ対策に関するヒアリングについて，(1)～(3)に答えよ。

(1)　本文中の下線①の実現に必要なプリンタの機能を，20字以内で具体的に述べよ。

(2)　本文中の［　ウ　］に入れる具体的な運用内容を，20字以内で答えよ。

(3)　本文中の下線②における違反とは何か。図2中のⅡ.6.の該当する項目の番号を(1)～(4)の中から二つ選べ。また，その違反内容を本文中の字句を用いて，それぞれ30字以内で述べよ。

設問4　本文中の下線③において，速やかにリスク分析を行いリスク対応の遅れを最小限にとどめるために，J社の各部署と情報システム部が担う役割を，それぞれ50字以内で述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 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	14:50 ～ 15:30

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. 電卓は，使用できません。
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，白紙であっても提出してください。
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。