SC

平成21年度　春期
情報セキュリティスペシャリスト
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

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2
選択方法	1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。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。
   (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2を選択した場合の例〕

選択欄
問1
(問2)

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　公開鍵基盤の構築に関する次の記述を読んで，設問1～6に答えよ。

A社は，持株会社（以下，グループ本部という）を中心とした企業グループの中の一社であり，従業員数 1,200 名の中堅機械製造会社である。業務は，製造業向けの製造機械の製造である。A社には，製造部門以外に，人事総務部，商品管理部，営業部，配送部，情報システム部がある。商品管理部は，在庫管理が主な業務であり，受注状況によって，商品の製造指示を行っている。営業部は，販売推進とA社のグループ会社である販売会社（以下，グループ販社という）からの受注業務を行っている。受注業務には，電話とファックスを利用してきた。

グループ本部では，従業員のワークライフバランスに積極的に取り組んでおり，A社の経営者も，具体的な施策を段階的に実施してきている。ワークライフバランスへの取組の一環として，製造部門以外の部署を対象とするテレワーク環境（以下，Tシステムという）を提供することになった。

また，営業部における受注業務において，誤った商品の納品や，数量の誤りが年に数件発生し，損失と信用の失墜を招いていたので，受注誤りを減らすためのシステム（以下，Nシステムという）の構築もTシステム構築と同時に行うことになった。

両システムの構築は，情報システム部のX課長とZ主任が担当することになり，2人は検討を開始した。

〔Tシステムの検討〕

X課長とZ主任は，まず，Tシステムにおける，ネットワーク接続方法を検討した。次は，そのときの会話である。

X課長：まず，Tシステムの構築に当たって，利用形態や用途を洗い出し，どのようなネットワーク接続方法が適切かを考えてみよう。

Z主任：はい。最初にテレワークでの利用形態ですが，人事総務部のまとめによれば，現時点での対象者は，育児休職，介護休職を取得中で，在宅での勤務を希望する従業員です。その後，段階的に対象者の範囲を広げていくことになっています。勤務場所については，自宅以外にサテライトオフィスも検討されています。

X課長：作業の内容については，社内で行う作業のほとんどが対象となる。外部から無制限に社内のシステムにアクセスできることは，セキュリティ上の大きなリスクとなるから，何らかの制限をかける必要がある。どこから，どのシステムにアクセスする必要があるか，説明してくれ。

Z主任：はい。まず，場所ですが，従業員の自宅とサテライトオフィスからアクセスする必要があります。利用する社内システムには，二つの形態があります。一つは，Web システムの形態で，受注管理システム，発注管理システムとグループウェアがあります。もう一つは，クライアントサーバシステムの形態で，勤怠管理システムと電子メール（以下，メールという）があります。テレワークについての事前調査で，ほとんどの従業員は自宅でインターネットを利用できることが分かっています。サテライトオフィスについては，提供事業者に確認したところ，十分な帯域が確保されたインターネットが利用できるとのことでしたので，インターネットの利用を前提とすることは T システムの実現上，問題ないようです。

X課長：費用の面からも，公衆回線や専用線よりもインターネットを利用した方がよいだろう。インターネットを利用することになると，セキュリティ面での要件を検討する必要がある。

Z主任：そうですね。インターネットを利用することから，通信の盗聴や改ざんを防ぐことと，利用者を確実に認証することが必要になります。

X課長：それでは，当社のシステム構築を行っている C 社と相談して，T システムの通信はどのような仕組みにすべきか，検討してくれ。

Z主任：分かりました。

Z主任は，早速 C 社でセキュリティを担当している D 氏に連絡を取り，T システムにおける安全な通信方法について検討することにした。次は，そのときの会話である。

Z主任：T システムを，インターネットを利用して実現するために，IPsec を利用した VPN を構築したいと思いますが，どのようなことに注意する必要があるでしょうか。

D氏：テレワークで利用する PC（以下，テレワーク PC という）は，御社の社内ネ

ットワークに直接接続されるのと同様の状態になりますので，社内で使われているPC（以下，社内PCという）と同様の管理が必要になります。

Z主任：テレワークPCについては，社内PCと同じアプリケーションプログラム，ウイルス対策ソフトが導入されたものを貸与することにします。それでよろしいでしょうか。

D氏：それだけでは不十分です。例えば，御社では，ウイルス定義ファイルが，社内に設置されている配布用のサーバだけから自動的に配布されるようになっています。そのため，テレワークPCについては，①VPNで御社の社内ネットワークに接続されていないときに問題が起こる可能性がありますので，その対策が必要です。

D氏は，起こる可能性のある問題と，その対策方法について説明した。

Z主任：分かりました。対策を講じます。それから，不正な接続を防ぐために，信頼性の高い認証を行わなければならないと思いますが，どのような方法をとったらよいでしょうか。

D氏：利用者IDとパスワードによる認証ですと，総当たり攻撃などによって，正当な利用者以外の者が接続できてしまうリスクを無視できません。クライアント証明書を併用した認証方式を採用してはいかがでしょうか。

Z主任：そのようにしたいと思います。

数日後，Z主任はD氏との検討の結果を取りまとめ，D氏にも同席してもらい，X課長に報告した。

Z主任：Dさんと検討した結果，暗号化にはIPsec，認証にはクライアント証明書を利用することにしました。

X課長：分かった。運用上，秘密鍵とクライアント証明書の取扱いには注意が必要だ。そのことも考慮して，C社とともに作業に入ってくれ。

Z主任：そのように手配します。

X課長：ところで，現在広く使われている暗号方式には，暗号強度の問題や脆弱(ぜい)性の

問題がある，と聞いたことがあるのですが，どのようなことでしょうか。

D氏　：それは，米国国立標準技術研究所（NIST）が定めた，米国政府機関のコンピュータシステムの調達基準のことです。表に示す暗号アルゴリズムを利用したシステムなどの調達は2010年までしか認められていません。

表　米国政府調達基準で現在調達可能で
2011年以降調達できなくなる暗号アルゴリズム

分類	名称
共通鍵暗号	2-key Triple DES
公開鍵暗号	鍵長 [a] ビットの RSA 及び DSA 鍵長 160 ビットの ECDSA
ハッシュ関数	[b]

D氏　：この理由の一つは，コンピュータの性能が上がることによって，数年後には，現在広く利用されている，鍵長 [a] ビットの RSA 公開鍵から秘密鍵が推測される可能性があり，②電子署名の対象のデータの改ざんやなりすましが行われる可能性があることです。これに対しては，鍵長を更に長くすることが求められます。もう一つは，ハッシュ関数として現在広く利用されている [b] には，ある条件下で [c] の衝突を意図的に起こすことができる，という脆弱性が発見されていることです。この脆弱性を攻撃されると，電子署名の信頼性が損なわれます。

X課長：なるほど。表の暗号アルゴリズムの問題には今から対策を講じておく必要があるわけですね。

D氏　：はい。日本でも政府機関に対して，内閣官房情報セキュリティセンターが2013年度までに対応するように求めています。

X課長：これらは政府機関の基準だが，我々のような民間企業でも，暗号アルゴリズムの問題を考慮してシステムを構築した方がよさそうですね。

D氏　：新規に構築するシステムですので，暗号アルゴリズムの問題を考慮した方がよいと考えます。

X課長：Z主任，この件についても，要求仕様を作る上で，十分に気をつけてくれ。

Z主任：はい，分かりました。

〔N システム要件の検討〕

続いて，X 課長と Z 主任は，受注誤りへの対応を行うために，営業部の Y 主任を交えて，N システムの要件を洗い出すことにした。次は，そのときの会話である。

X 課長：これまでの電話とファックスによる受注が，どのようなフローで行われているかを確認しよう。Y 主任，説明してくれ。

Y 主任：はい。まず，電話による受注処理ですが，営業部の従業員が電話を受け，その内容を注文票に記入します。注文票の内容を，同じ従業員が，社内システムの受注管理システムに入力します。商品管理部は，受注管理システムを参照して在庫情報を確認し，製造指示作業を始めます。次に，ファックスによる受注処理ですが，営業部の従業員が，受け取ったファックスの内容を，受注管理システムに入力するようになっています。以後は電話による受注処理と同じです。

X 課長：どのような受注誤りが多いのかね。

Y 主任：受注誤りで多いのは，受注管理システムへの型番や数量の入力間違いです。

X 課長：それでは，表計算ソフトを使って電子化した注文票を，送付してもらってはどうだろうか。そうすれば，受注管理システムとの連携は，比較的容易に構築できるだろう。

Z 主任：注文票には，グループ販社の担当者の氏名や電話番号，お客様の事業状況などがうかがい知れる項目が含まれていますので，グループ販社の発注担当者と当社営業部担当者間の機密性を確保することが必要です。

X 課長：それでは，電子化された注文票の送付方法について検討することにしよう。

電子化された注文票を安全に送付する方法について，再び，D 氏に相談することにした。次は，そのときの会話である。

X 課長：電子化された注文票は，注文票を作成したグループ販社と当社の者だけが，内容を知ることができるようにしたいと考えています。電子化された注文票を，インターネットを使って安全に送付する方法として，どのようなものがあるか教えてほしいのですが。

D氏　：送付する方法としては，メールを利用する方法と，Web システムを利用する方法があります。どちらの方法でも，暗号化を利用すれば，安全に送付することができます。

Z主任：Web システムを利用する場合は，SSL で暗号化された通信路を使って送付することになりますよね。メールを利用する場合は，どのような方法で行うのですか。

D氏　：はい，S/MIME という方法があります。これは，RFC で規定されており，多くのメールソフトが標準で実装しています。S/MIME を使うと，メールの暗号化と電子署名を行うことができます。

SSL も S/MIME も公開鍵基盤（PKI）の上で動作しますので，まず，認証局（CA）が必要となります。これには，認証事業者の CA（以下，商用 CA という）を利用することもできますし，御社で構築，運用する CA（以下，自営 CA という）を利用することもできます。利用者は，自分自身の秘密鍵と公開鍵の対（以下，鍵ペアという）を生成します。CA は，この公開鍵に対して公開鍵証明書（以下，証明書という）を発行します。御社での CA の設置運用状況は，どうなっていますか。

X課長：はい，グループ本部では，既に証明書ポリシと認証局運用規程（以下，CP/CPS という）を策定しており，ルート CA が自営 CA として設置されています。グループ企業はこのルート CA の利用が可能です。また，グループ企業独自のルート CA を設置してもよいことになっており，商用 CA と自営 CA のいずれで実現しても構わないことになっています。

Z主任：今回の場合，証明書の発行をタイムリに行う必要があると思うので，独自のルート CA を設置した方がよいと思います。

X課長：そうだな。グループ本部のルート CA を利用するのではなく，当社独自のルート CA を設置することにしよう。

D氏　：分かりました。

X課長：この場合，商用 CA を利用するか，自営 CA を利用するかは何を基準にして決めればよいのですか。

D氏　：まず，だれが証明書を利用するのかが基準になります。不特定の利用者を対象とする場合は，商用 CA を利用しなければなりませんが，利用者の範囲が

限られる場合は，自営 CA を利用しても構いません。次に，自営 CA の構築費用及び証明書発行費用を含む運用費用と，商用 CA の費用との比較によって決めるのが一般的です。

Z主任 ：今回の場合，利用者がグループ販社と当社に限定されるので，利用者の範囲という観点では，自営 CA でも問題なさそうですね。後は，費用と手間の観点での検討が必要ということですね。自営 CA を運用する場合，どのようなことをしないといけないのでしょうか。

D氏 ：構築段階では，自営 CA で発行する証明書の種類を決めたり，証明書発行の手順や運用体制を決めたりしなければなりません。これらを文書化して CP/CPS を策定する必要があります。運用段階の主な作業は，証明書の発行と証明書失効リストの発行です。

X課長：自営 CA の構築はどのように行うのでしょうか。

D氏 ：自営 CA を構築する方法は幾つかあります。一つ目は，OS の機能やオープンソースソフトウェア（OSS）を使う方法です。二つ目は，アプライアンス製品を使う方法です。三つ目は，市販されている CA ソフトを使う方法です。

Z主任 ：OSS を利用すると，構築費用はかなり下げることができますね。ただし，そのソフトウェアに精通した技術者が必要になると思いますが。

X課長：そうだな。Z 主任，これらの情報を基に，電子化された注文票の送付方法をメールと Web システムのどちらにするか，CA は自営 CA と商用 CA のどちらにするか，また，自営 CA を利用する場合は，CA の構築方法も含めて検討してくれ。

Z主任 ：分かりました。

〔PKI 構築の検討〕

数日後，X 課長は，Z 主任の検討結果が適切であるかを，D 氏を交えて確認した。

Z主任 ：電子化された注文票の送付方法について検討したところ，Web システムを利用した送付については，Web システムの開発が必要ですので，すぐには開始できません。メールについては，証明書が用意できれば，すぐにでも開始できます。受注管理システムとの連携をスムーズに行うために，将来的には

Web システムを利用することにして，しばらくの間は，メールにすることにしました。

X課長：そうか。CAについてはどうかね。

Z主任：T システムと N システムを合わせると，発行する証明書がかなりの数になります。そのため，多数の証明書を一括して発行できる証明書発行プログラムが必要になりますので，その開発費用も含め，3 年間で掛かる総費用を算出してみました。なお，CP/CPS については，グループ本部の CP/CPS を流用することができますので，比較的容易に策定することができます。その結果，当社にとって最適な方式を採用した自営 CA を利用する場合が 359 万円，商用 CA を利用する場合が 654 万円となり，当社の場合，自営 CA を利用した方が安いとの結論に至りました。

D氏　：なるほど。しかし，証明書を発行するために，自営 CA の秘密鍵を使う必要があります。③自営 CA の秘密鍵が漏えいすると，グループ販社と御社に被害が及ぶことが想定されます。秘密鍵の漏えい防止対策を施すと，証明書発行に要する費用は，これよりは多くなると思います。

X課長：そのとおりだ。自営 CA の秘密鍵を安全に使うための手順を考慮して，証明書発行に要する費用を再度計算してくれ。

Z主任：分かりました。

Z主任は，自営CAの秘密鍵を安全に使うための手順を考慮した費用を計算し，X課長に提示した。

Z主任：秘密鍵を安全に使うための手順を見直したところ，鍵管理のアプライアンス製品を導入することで，秘密鍵を安全に管理できることが分かりました。この製品を使用した場合の 3 年間の総費用は 422 万円となり，やはり，自営CAを利用する方が安くなります。

X課長：それでは，自営 CA を利用することにしよう。Web システムになったとしてもCAは必要だからな。

Z主任：分かりました。ところで，利用者が証明書署名要求（CSR）を作成するためには，事前に，鍵ペアを生成しておく必要があります。また，CA で証明書

発行を行うためには，利用者からCSRをもらう必要があります。

X課長：証明書発行プログラムとは別に，鍵ペアの生成プログラムと，CSR 作成プログラムの開発が必要ということだな。ただ，今回の場合，証明書を T システムと N システムの利用に限定すれば，必ずしも CSR の作成までを，利用者に行ってもらう必要はないのではないでしょうか。

D氏　：おっしゃるとおりです。今回の PKI 構築の目的は，御社とグループ販社の担当者間のメールを，第三者が不正に閲覧することができなければよいわけですから，必ずしも，鍵ペアを利用者本人が生成しなくても，御社が生成すれば問題ないと考えます。鍵ペアを御社が生成するのであれば，CSR 作成も御社で可能です。鍵ペアの生成プログラムと CSR 作成プログラムは，証明書発行プログラムの一部として開発すれば，運用も容易になると思います。

X課長：そういうことだ。この方法を採用する方がよさそうだな。ただし，CP/CPSの中で，④利用者の鍵ペアの取扱いについて，きちんと決めておいた方がよさそうだ。Z 主任，D 氏とともに，テレワークを含め，証明書発行の運用フロー概要を作成してくれたまえ。

Z主任：分かりました。

翌日，Z主任は，証明書発行の運用フローをX課長に提示した。

Z主任：証明書発行の運用フローを，図 1 にまとめました。T システムで利用する証明書と，N システムで利用する証明書のいずれも，同じ CA で発行するようにしています。また，鍵ペアの生成及び CSR の作成は CA 運用者で行う方法を採用しています。

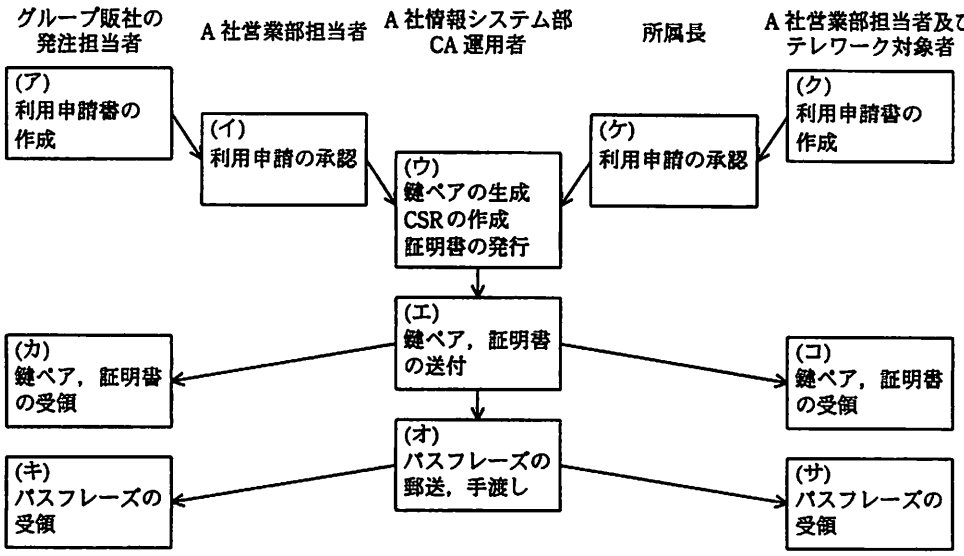

図１　証明書発行の運用フロー

X課長：ところで，利用者属性の真偽の確認は，どこで行うのかね。

Z主任：グループ販社の発注担当者の確認は，図１中の［　d　］で行います。テレワーク対象者の確認は［　e　］で行います。

X課長：登録局（RA）の役割を，利用申請者をよく知っている当社の従業員が担う形になるわけだな。鍵ペアと証明書は，利用申請者にどのような手段で渡すのかね。

Z主任：鍵ペアと証明書は，パスフレーズを使って暗号化し，メールで送付します。復号に必要なパスフレーズは，グループ販社の場合は郵送します。当社営業部担当者とテレワーク対象者の場合は，情報システム部に取りに来てもらいます。

X課長：分かった。ところで，実際の受注フローについては，どのようになるのかね。

Z主任：はい，図２にまとめました。

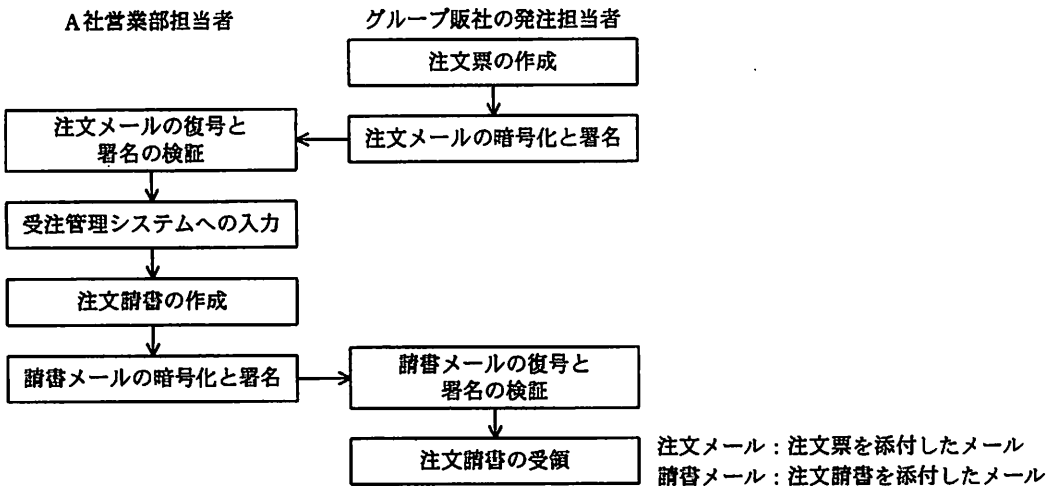

図２　受注フロー

X課長：グループ販社側で，注文メールの暗号化と署名，請書メールの復号と署名の検証に手間が掛かるが，最近のメールソフトでは，簡単な操作でこれらができるようになっているから，グループ販社にとっても，そんなに面倒な作業ではないだろう。受注管理システムへの入力は，注文票に組み込まれているプログラムで自動化することで，誤りが防げる。

ところで，当社営業部担当者の証明書をグループ販社の発注担当者に送っておく必要があるが，どのようにするのかね。それから，グループ販社と当社ともに，メールの暗号化と署名の検証を行う必要がある。そのときに必要となる当社の［ f ］証明書は，いつ，どこに，どのようにして導入するかを手順書として整備する必要があるな。

Z主任：すみません，それらのことを忘れていました。当社営業部担当者の証明書の送付方法と［ f ］証明書の導入については，手順書を作成して配布するようにします。また，グループ販社での導入を支援できるように，営業部員への教育を検討します。

X課長：CP/CPS についても，営業部員がきちんと説明できるようにしておいてくれ。それから，⑤グループ販社では，証明書を N システム以外の用途に使用しないように，徹底してくれ。

Z主任：分かりました。

その後，X課長とZ主任は，C社とともにTシステムとNシステムの構築を順調に終え，運用を開始した。

設問1　本文中の［　a　］～［　c　］及び［　f　］に入れる適切な字句を，8字以内で答えよ。

設問2　本文中の下線①について，どのような問題が起こるかを，45字以内で述べよ。また，その対策を，50字以内で述べよ。

設問3　Tシステムにおいて，テレワーク対象者は，他人が社内ネットワークへ不正にアクセスしないようにするために，自分のテレワークPCに関して，運用する上でどのような点に注意する必要があるか。秘密鍵の漏えい防止の観点から二つ挙げ，それぞれ35字以内で述べよ。

設問4　本文中の下線②について，秘密鍵の推測が成功したとして，どのようにすれば改ざんやなりすましができるか。その方法を，70字以内で述べよ。

設問5　PKI構築について，(1)～(3)に答えよ。

(1) 本文中の下線③について，どのような被害が考えられるか。50字以内で述べよ。

(2) 本文中の［　d　］と［　e　］に入れる適切な記号を，図1中の(ア)～(サ)から選んで答えよ。

(3) 本文中の下線④について，鍵ペアの取扱い上で注意すべき事項を，30字以内で述べよ。

設問6　本文中の下線⑤について，グループ販社の発注担当者が，証明書の使用制限に反して，第三者に対し，A社の自営CAで生成された秘密鍵を用いて署名したメールを送付した場合，メール受信者では，どのような問題が発生するか。また，その理由は何か。A社が自営CAを採用していることを考慮して，それぞれ20字以内，30字以内で述べよ。

問2　インターネット販売を行う企業の情報セキュリティ管理に関する次の記述を読んで，設問1～5に答えよ。

P社は従業員数500名の衣料小売業者であり，店頭販売やカタログ販売を行っている。これに加え，5年前からは社内に業務システム（以下，販売システムという）を構築し，一般消費者に対してクレジットカード決済を利用したインターネット販売を行っている。P社では情報セキュリティを確保するための取組を進めており，インターネット販売事業に関してISO/IEC 27001（JIS Q 27001）の認証（以下，ISMS認証という）を2年前に取得している。

P社は先ごろISMS認証の維持審査に合格したが，この審査において四つの観察事項を指摘された。ISMS認証機関から提示された維持審査結果報告書を図1に示す。

維持審査結果報告書

ISMS認証機関　X株式会社

（省略）

[不適合]
ISO/IEC 27001:2005の要求事項に対する重大な不適合や軽微な不適合は特に認められませんでした。

[観察事項]　()内はISO/IEC 27001:2005の箇条を示す。
1. ISMSの適用範囲を定義する文書において社内組織の変更点が反映されていない部分がありますので，現行の組織体系に合わせた記述に修正することが望まれます。(4.2.1a，4.3.1b)
2. 販売システムの各サーバで利用している管理者パスワードの利用は適切なセキュリティ慣行に従うことが望まれます。(A.11.3.1，A.11.5.3)
3. Webアプリケーションの開発委託におけるセキュリティ要件を明確にすることが望まれます。(A.12.5.5)
4. 法的要求事項に関しては文書化されていますが，これを最新に保つための手法をご検討ください。(A.15.1.1)

（以下，省略）

図1　維持審査結果報告書

〔観察事項への対応〕

維持審査の結果を受け，P社では，情報セキュリティ責任者を兼務している情報システム部のG部長と，その部下で販売システムの管理を担当しているFさんが観察事項への対応に当たることになった。

次は，G部長とFさんの会話である。

Fさん：維持審査での観察事項への対応ですが，どのように進めていきましょうか。

G部長：不適合はなかったが，四つの観察事項への対応策を検討しよう。1.については適用範囲の定義文書を修正することで対応しよう。2.と3.は情報セキュリティポリシ（以下，ポリシという）の修正に加え，技術的な対応も必要になりそうだ。具体的にどの程度まで実施するのかが難しいね。

Fさん：4.については，新たな法律の制定や業界の動向を踏まえて社内のISMS運営事務局で法的要求事項の改訂案を検討し，［　a　］の場で承認を得るというルールを作るとよいと思います。クレジットカード業界に関しては新たな動きがありますね。

G部長：審査が終わってから聞いた話では，2008年6月に公布された改正割賦販売法が施行されると，クレジットカードの発行会社にはクレジットカード番号（以下，カード番号という）を含むカード会員データの保護が義務付けられるそうだ。当社のようなカードの加盟店を直接規制する法律ではないが，当社にもカード発行会社から何らかの対策が求められるかもしれない。

Fさん：カード番号の不正な取得や有償での提供を行った個人も処罰されるということでしたね。カード番号を悪用されると影響が大きいですからね。
そういえば，クレジットカード業界では加盟店に対して技術的な対応を含めた自主基準を定めていたようです。観察事項の2.と3.への対応のヒントになるかもしれませんので，調べてみます。

数日後，Fさんは G部長に調査の結果を報告した。

Fさん：先日の話ですが，国際クレジットカードブランド5社が共同で設立したPCI SSC（Payment Card Industry Security Standards Council, LLC）という国際協議会が，PCIデータセキュリティ基準（Payment Card Industry Data Security Standard，以下，PCI DSSという）という業界基準を設けています。この基準を参考にして対応を考えてはどうでしょうか。

Fさんは図2に示すPCI DSS（バージョン1.2）の要件をG部長に提示した。

安全なネットワークの構築と維持
　要件1　：カード会員データ(1)を保護するために，ファイアウォールをインストールして構成を維持すること
　要件2　：システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しないこと
カード会員データの保護
　要件3　：保存されたカード会員データを保護すること
　要件4　：オープンな公共ネットワーク経由でカード会員データを伝送する場合，暗号化すること
脆弱性管理プログラムの整備
　要件5　：アンチウィルスソフトウェア(2)またはプログラムを使用し，定期的に更新すること
　要件6　：安全性の高いシステムとアプリケーションを開発し，保守すること
強固なアクセス制御手法の導入
　要件7　：カード会員データへのアクセスを，業務上必要な範囲内に制限すること
　要件8　：コンピュータにアクセスできる各ユーザ(3)に一意のIDを割り当てる。
　要件9　：カード会員データへの物理アクセスを制限する。
ネットワークの定期的な監視およびテスト
　要件10：ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する。
　要件11：セキュリティシステムおよびプロセスを定期的にテストする。
情報セキュリティポリシー(4)の整備
　要件12：従業員および派遣社員向けの情報セキュリティポリシーを整備する。

出典：PCI Security Standards Council LLC, “Payment Card Industry（PCI）データセキュリティ基準 要件とセキュリティ評価手順 バージョン1.2”, 1ページ
（URL：https://www.pcisecuritystandards.org/pdfs/pci_dss_japanese.pdf（平成21年3月1日アクセス））

注(1)　カード会員データとは，カード番号，カード会員名，有効期限などを指す。
(2)　“アンチウィルスソフトウェア”は，問題文中の“ウイルス対策ソフト”と同じである。
(3)　“ユーザ”は，問題文中の“利用者”と同じである。
(4)　“情報セキュリティポリシー”は，問題文中の“ポリシ”と同じである。

図2　PCI DSS（バージョン1.2）の要件

G部長：全部で12個の要件があるのか。観察事項に対応する要件は要件6，8辺りかな。これらの要件が更に細かく分かれているわけだね。

Fさん：そうです。例えば，観察事項として指摘されたパスワード管理に関しては，要件8の中に，図3に示すような詳細要件が定められています。

要件 8：コンピュータにアクセスできる各ユーザ(1)に一意の ID を割り当てる。
（省略）
8.5 すべてのシステムコンポーネントで，以下のように，消費者以外のユーザおよび管理者に対して適切なユーザ認証とパスワード管理を確実に行う。
8.5.1 ユーザ ID，資格情報，およびその他の識別子オブジェクトの追加，削除，変更を管理する。
8.5.2 パスワードのリセットを実行する前にユーザ ID を確認する。
8.5.3 初期パスワードをユーザごとに一意の値に設定し，初回使用後に直ちに変更する。
（省略）
8.5.9 少なくとも 90 日ごとにユーザパスワードを変更する。
8.5.10 パスワードに 7 文字以上が含まれることを要求する。
8.5.11 数字と英文字の両方を含むパスワードを使用する。
8.5.12 ユーザが新しいパスワードを送信する際，最後に使用した 4 つのパスワードと同じものを使用できないようにする。
（省略）

出典：PCI Security Standards Council LLC，“Payment Card Industry（PCI）データセキュリティ基準 要件とセキュリティ評価手順 バージョン 1.2”，37～40 ページ
（URL：https://www.pcisecuritystandards.org/pdfs/pci_dss_japanese.pdf（平成 21 年 3 月 1 日アクセス））
注(1) “ユーザ”は，問題文中の“利用者”と同じである。

図 3 パスワード管理に関する PCI DSS の詳細要件

G 部長：クレジットカード加盟店では，今後このレベルの管理が求められるということか。当社の現状からみるとかなり厳しい要件もあるが，クレジットカード決済を利用していくのであれば実施する方がいいのだろうね。
Web アプリケーションの開発時におけるセキュリティ要件については何か参考になりそうなものはあったかな。

F さん：Web アプリケーションの開発では，クロスサイトスクリプティングや SQL インジェクションなど，広く知られた脆弱性について対処する必要があります。そのため，詳細要件 6.5 では，安全なコーディングのためのガイドラインに従うことを推奨しています。PCI DSS では，その代表的なものとして，米国の団体が策定したガイドラインを挙げています。今後はこのガイドラインに沿って具体的なセキュリティ要件を発注の際の仕様に含めるとよいのではないでしょうか。

G 部長：そうだね。詳細については検討する必要があるが，今後 Web アプリケーションの改修を行うときや新規の開発を行うときには，①委託先に具体的なセキュリティ要件を提示することにしよう。

これらの検討を踏まえ，G 部長と F さんは観察事項への対応計画を作成した。この

対応計画は経営陣の承認を経て実行に移されることになった。

〔PCI DSS を参考にした ISMS の継続的改善〕

その後，G 部長が対応計画の完了を経営陣に報告したところ，PCI DSS で求められる要件をベースラインとして ISMS における技術面及び管理面の改善を図るようにとの指示が出た。そこで，G 部長と F さんは PCI DSS の要件に沿って販売システムの管理状況を確認することにした。次は，G 部長と F さんの会話である。

F さん：PCI DSS の各要件への対応状況ですが，私の考えで 12 個の要件ごとに現在の状況を表 1 のようにまとめてみました。

表 1　F さんによる PCI DSS の対応状況のまとめ

要件	対応状況 (1)	今後必要な対策
要件 1	○	ファイアウォール，ルータのルールセットのレビュー
要件 2	△	システム上での不要なサービスや機能の無効化，停止
要件 3	○	システム外でのカード情報の暗号化と難読化
要件 4	◎	対応済（SSL の導入）
要件 5	◎	対応済（ウイルス対策ソフトの導入）
要件 6	△	パッチ適用体制の見直し，既知の攻撃からの Web アプリケーションの防護
要件 7	◎	対応済（ポリシ，システムによるアクセス制限の実施）
要件 8	◎	対応済（パスワードポリシの修正，システムでの対応）
要件 9	△	カメラなどによるサーバ室の監視，安全なバックアップ媒体の保管
要件 10	×	監査証跡の自動取得と保護，ログの確認
要件 11	△	システムへの脆弱性スキャン，ペネトレーションテスト
要件 12	○	PCI DSS への対応に伴うポリシの見直し，インシデント対応計画の立案とテスト及び見直し

注(1)　対応状況は次の例による。
◎：各要件に含まれる詳細要件をすべて満たしている
○：詳細要件の一部について実施状況の見直しや確認が必要
△：詳細要件の一部について未実施
×：詳細要件の多くが未実施

G 部長：今の時点で対応できている要件はどれかな。

F さん：要件 4，5，7，8 は対応できていると思います。要件 4 はインターネットや無線 LAN などの公衆ネットワーク上でのカード会員データの暗号化を求めてい

ますが，販売システムでは無線 LAN は使用していませんし，インターネット経由でカード会員データを送受信する部分はすべて SSL で暗号化されています。要件 5 はシステムへのウイルス対策ソフトの導入ですが，ウイルス対策ソフトは販売システムに含まれるすべての PC とサーバに導入済です。

G 部長：②ウイルス定義ファイルの自動更新と定期スキャンも実施しているし，問題なさそうだ。

F さん：要件 7 はカード会員データへのアクセスを業務上必要な範囲内に制限するということですが，販売システムにはポリシ上も機能上も職責に応じて権限を与えられた担当者だけがアクセスできるようになっているので問題はありません。要件 8 は利用者ごとに個別の利用者 ID を割り当てるという要件で，パスワードポリシについては ISMS の観察事項に基づいて対応しました。それ以外の部分は以前から実施済です。

G 部長：この四つの要件に関しては対策が実施されているということだね。次に，要件 1，3，12 については見直しや確認が必要なところだね。

F さん：はい。要件 1 ではファイアウォールの設置を求めていますが，詳細要件 1.1.6 の，少なくとも 6 か月ごとに，ファイアウォール及びルータに関するルールセットのレビューを実施するという要件が現状では満たされていません。それ以外の詳細要件はすべて対応できています。

G 部長：ファイアウォールもルータも，設定についてのレビューは実施していなかったな。今の運用手順を改訂してレビューを行う必要があるね。

F さん：要件 3 はカード会員データの保護についてです。カード番号は販売システムのデータベースサーバ（以下，DB サーバという）の中では暗号化されていますが，詳細要件 3.4 によるとバックアップやログの中にカード番号が含まれている場合にはカード番号の一部を削除するか，あるいは暗号化やハッシュによって読めないようにする必要があります。

G 部長：販売システム以外にもカード番号が存在するかどうかだね。具体的にカード番号がどの情報資産に含まれているか，それがどこに保管されているかについては，先日の維持審査の前に実施したリスク分析で明確にされているから対応はそれほど難しくはないだろう。

Fさん：要件12はポリシの整備が中心になっていますが，ここで対応すべき詳細要件としてはインシデント対応計画があります。PCI DSS では少なくとも年に一度のテストと見直しを求めていますが，インシデント対応計画についてはこれまでにテストも見直しも行ったことがありません。

G部長：この辺までは今までの対策の延長で対応できそうだが，更に修正が必要になるのが要件2，6，9，10，11だね。

Fさん：要件2は，システムのデフォルト設定を使ってはいけないという要件です。

G部長：サーバについては受入れ検査のときに③ポートスキャンツールを使って不要なサービスの有無を確認しているが，その後システムを変更しているからもう一度確認が必要だ。

Fさん：要件6は後回しにして，要件9は物理的アクセスの制限や媒体の取扱いについてです。詳細要件9.1.1では機密エリアはビデオカメラやその他のアクセス管理機器で監視し，少なくとも3か月間は監視データを保管することが求められていますが，現状では保管していません。

G部長：サーバ室とコールセンタはカメラで監視しているが，監視映像は保管していないから，追加投資が必要になりそうだ。

Fさん：ほかにはバックアップ媒体の保管の話があります。今は媒体を④サーバ室に保管していますが，外部の施設への保管も検討する必要があります。

G部長：これについては，先ほどのインシデント対応計画と同様に，ISO/IEC 27001の［　b　］計画でも対応すべきだろうね。

Fさん：要件11に移りましょうか。詳細要件11.2では，少なくとも四半期に一度，そのほかにネットワークに大きな変更があったときにシステムへの脆弱性スキャンを行うことが求められています。また，詳細要件11.3では，少なくとも年に一度と，そのほかにインフラやアプリケーションを大幅に変更した後にペネトレーションテスト（以下，Pテストという）を実施することが求められています。

G部長：Pテストは外部にお願いする必要があるのかな。Fさんに Pテストのスキルを身につけてもらった上で実施するのはどうだろう。

Fさん：社内で実施することは要件上認められていますが，私に Pテストのスキルがあったとしても，⑤私がPテストを実施するのは望ましくないですね。

G部長：そうだね。内部で実施するか外部で実施するかは別途考えよう。

Fさん：残っているのは要件6，10ですね。まず，要件10はアクセスの追跡と監視についてです。具体的には，各システム上でログを取得するだけではなく，改ざんされないように保護した上で少なくとも日に一度は確認することが求められます。

G部長：Web コンテンツへのアクセス状況は解析しているけれども，セキュリティ上のイベントについては特に何もしていない。日に一度の確認となるとかなり大変だから，今後は何らかの対応が必要だ。

Fさん：ほかにはシステムクロックを正確な時刻に保つことが求められていますが，社内のすべての機器は販売システム上の時刻サーバを介してインターネット上の標準時サーバと時刻を同期させています。これには通信の遅延を補正できる［　c　］というプロトコルを使っています。

〔Webアプリケーションの保護の手法〕

Fさん：技術的に最も対応が難しそうな要件6の対応状況は表2のとおりです。詳細要件6.2から6.5までは対応済ですが，残りの二つに関しては対応が必要になりそうです。特に詳細要件6.6ではWebアプリケーションの見直し又はWebアプリケーションファイアウォール（以下，WAFという）の導入が求められています。

表2　要件6の対応状況

詳細要件	対応状況(1)	今後必要な対策
6.1	○	最新セキュリティパッチのリリース後1か月以内の適用
6.2	◎	対応済（ベンダ，各種団体からの脆弱性情報入手）
6.3	◎	対応済（開発，テスト，本番環境の分離など）
6.4	◎	対応済（変更管理手順に基づくシステム変更の実施）
6.5	◎	対応済（コーディングガイドラインの導入）
6.6	×	Webアプリケーションの見直し又はWAFの導入

注(1)　詳細要件の対応状況は表1の注を参照。

G部長：詳細要件6.1はセキュリティパッチ（以下，パッチという）のリリース後1か月以内の適用ということだね。システムを停止できない場合も多いが，パ

ッチの運用体制を見直して対応するしかないね。

F さん：パッチの適用についてはリスクに応じて優先度をつけることも認められていますので，重大なものを優先させ，軽微なものは 3 か月以内に適用することができます。

G 部長：詳細要件 6.6 の Web アプリケーションの見直しというのはどんな方法で行うのかな。

F さん：Web アプリケーションの脆弱性を手動又は自動で評価するツール又は手法によって，Web アプリケーションをレビューすることが求められています。脆弱性はすべて修正し，修正後に再評価する必要があります。

G 部長：実施の頻度はどれくらいなのかな。

F さん：少なくとも年に一度実施することが求められています。そのほかに何らかの変更があった場合にも実施する必要があります。

G 部長：Web アプリケーションの見直し以外には WAF の導入も選択肢としてあるということだが，今導入している侵入防止システム（以下，IPS という）では対応できないのかな。

F さん：今使っている IPS はシグネチャベースの製品で，ネットワーク層に対する既知の攻撃を防御することに主眼を置いています。Web アプリケーションの脆弱性に対する攻撃にはそれほど効果はありません。

G 部長：WAF では Web アプリケーションへの攻撃をどうやって防ぐのだろう。

F さん：これには二つの考え方があるようです。一つはポジティブセキュリティモデルといって，正常な通信として定義されたもの以外の通信をすべて遮断するものです。どういった通信が正常なのかを定義するために個々の Web アプリケーションに対して細かい設定が必要になり，導入にも手間が掛かります。もう一つはネガティブセキュリティモデルといって，シグネチャや特定のパターンに合致した通信をアプリケーション層で遮断するものです。Web アプリケーションの脆弱性の性質から，⑥個々の攻撃に対してシグネチャを作成することが難しいというデメリットがありますが，特定の情報の漏えいを防ぐ観点からは，こちらのモデルの方が有効な場合があります。このため，PCI DSS では，この二つのセキュリティモデルを WAF に実装することが推奨されています。

G 部長：状況によっては両方のモデルを実装した WAF が必要ということか。

F さん：WAF には攻撃を検知する機能があるので，当社の対策に欠けている PCI DSS の要件を満たせるというメリットもあります。

G 部長：なるほど。ただ，⑦Web アプリケーションの見直しをせずに WAF を導入することには問題があるのではないかな。コスト面での制約はあるが，できるだけ併用する方向で検討しよう。

〔トランザクションログに対する代替管理策〕

その後，P 社では PCI DSS を参考に販売システムの改善を図っていったが，システムの制約上，対応が困難な詳細要件が存在することが分かった。次は，G 部長と F さんの会話である。

G 部長：ベンダに問い合わせてみたところ，DBMS が作成するトランザクションログについては暗号化を施してカード番号を判読困難にすることは難しいようだ。既存のログからカード番号を除去するのも現実的ではない。そうなると，詳細要件 3.4 を満たすことができない。できるだけ追加投資を必要とせずに対応する方法はないだろうか。

F さん：要件を満たせない場合でも，関連するリスクをほかの手段を適用することで［ d ］できる場合には，その手段を代替管理策とすることで，要件の目的を実現することが可能です。PCI DSS では，表 3 に示すようなワークシートを使って，要件が満たされないことに対するリスクを管理するそうです。まだ検討の途中ですが，このような形になるかと思います。

表3　詳細要件 3.4 に対する代替管理策のワークシート

必要な情報		P 社での状況
1. 制約	元の要件への準拠を不可能にする制約を列挙する。	DBMS が出力するトランザクションログの中にカード番号が含まれているが，ソフトウェアの制約によってトランザクションログを暗号化することができない。
2. 目的	元のコントロール(1)の目的を定義し，代替コントロールによって満たされる目的を特定する。	トランザクションログに含まれるカード番号を判読困難にすることによって，カード番号の露呈を防ぐ。
3. 特定されるリスク	元のコントロールの不足によって生じる追加リスクを特定する。	DB サーバにアクセス可能な従業員に対してトランザクションログに含まれるカード番号が露呈するリスクがある。
4. 代替コントロールの定義	代替コントロールを定義し，元のコントロールの目的および追加リスク（ある場合）にどのように対応するかを説明する。	[e]。 これによって，トランザクションログに含まれるカード番号の露呈を防ぐ。
5. 代替コントロールの検証	代替コントロールの検証およびテスト方法を定義する。	（未検討）
6. 維持	代替コントロールを維持するためのプロセスおよび管理を定義する。	（未検討）

太枠部分の出典：PCI Security Standards Council LLC, “Payment Card Industry（PCI）データセキュリティ基準 要件とセキュリティ評価手順 バージョン 1.2”, 62 ページ
（URL：https://www.pcisecuritystandards.org/pdfs/pci_dss_japanese.pdf（平成 21 年 3 月 1 日アクセス））

注(1)　“コントロール”は，問題文中の“管理策”と同じである。

G 部長：なるほど，表 3 の代替管理策を実施すれば詳細要件 3.4 の目的は実現できそうだ。残りの 5. と 6. についても検討してみてくれないかな。

F さん：分かりました。残りの部分についてもこれから検討します。

その後，P 社は PCI DSS を参考にして ISMS の取組を進め，技術面でのセキュリティ向上とポリシ面での継続的改善を図ることができた。

設問 1　〔観察事項への対応〕について，(1)，(2) に答えよ。

(1) 本文中の [a] に入れる適切な字句を，15 字以内で答えよ。

(2) 本文中の下線①について，Web アプリケーションの開発委託先に対してセキュリティ要件を提示していなかった場合，受入れ検査時に脆弱性の存在が判明したときにどのような問題が発生するか。60 字以内で述べよ。

設問2　〔PCI DSSを参考にしたISMSの継続的改善〕について，(1)～(5)に答えよ。

(1) 本文中の［ b ］，［ c ］に入れる適切な字句を，それぞれ5字以内で答えよ。ただし，［ b ］は漢字とし，［ c ］は英字の略称とする。

(2) 本文中の下線②について，自動更新と定期スキャンが確実に実施されていることをどのように確認するべきか。30字以内で述べよ。

(3) 本文中の下線③について，検査対象と同一のネットワークセグメントからポートスキャンツールを利用して検査を行う場合，不要なサービスがあるかどうかをどのような基準で判断するか。50字以内で述べよ。

(4) 本文中の下線④について，現状のままバックアップ媒体をサーバ室に保管する場合のリスクを，50字以内で述べよ。

(5) 本文中の下線⑤について，F さんが自身で P テストを実施することは望ましくないとした理由を，30字以内で述べよ。

設問3　〔Webアプリケーションの保護の手法〕について，(1)，(2)に答えよ。

(1) 本文中の下線⑥について，シグネチャを作成することが難しい理由を，50字以内で述べよ。

(2) 本文中の下線⑦について，Web アプリケーションの見直しをせずに WAF を導入することによって発生するセキュリティ上の問題点を，60字以内で述べよ。

設問4　〔トランザクションログに対する代替管理策〕について，(1)，(2)に答えよ。

(1) 本文中の［ d ］に入れる適切な語句を解答群の中から選び，記号で答えよ。

解答群

ア　移転　　イ　回避　　ウ　受容　　エ　低減

(2) 表3中の［ e ］に入れる代替管理策を，40字以内で述べよ。

設問5　PCI DSS を参考として技術面で新たな対策を追加していった P 社が，ISMS の活動として次回の審査に向けて実施すべき作業を，50字以内で述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

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	15:10 ～ 16:20

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。