AU

# 平成27年度　春期
# システム監査技術者試験
# 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. **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) 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。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) |
|---|---|---|
| | 1問選択 | |

Ⅱ

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。

**“あなたが携わったシステム監査，システム利用又はシステム開発・運用業務の概要”の記入方法**

あなたの所属部門と，あなたが担当した主なシステム監査，システム利用又はシステム開発・運用業務の概要について記入してください。

①～⑪の質問項目に従って，記入項目の中から該当する番号又は記号を○印で囲むとともに，（　　）内にも必要な事項を記入してください。複数ある場合は，該当するものを全て○印で囲んでください。

## 問1　ソフトウェアの脆弱性対策の監査について

近年，ソフトウェアの脆弱性，すなわち，ソフトウェア製品及びアプリケーションプログラムにおけるセキュリティ上の欠陥を悪用した不正アクセスが増えている。ソフトウェア製品とは，アプリケーションプログラムの開発及び稼働，並びに情報システムの運用管理のために必要なオペレーティングシステム，ミドルウェアなどをいう。

ソフトウェアの脆弱性によっては，それを放置しておくと，アクセス権限のない利用者が情報を閲覧できるなど，アクセス権限を越えた操作が可能になる場合もある。例えば，不正アクセスを行う者が，この脆弱性を悪用して攻撃を仕掛け，情報の窃取，改ざんなどを行ったり，情報システムの利用者に，本来は見えてはいけない情報が見えてしまったりする。

ソフトウェアの脆弱性対策では，開発段階で，ソフトウェア製品及びアプリケーションプログラムの脆弱性の発生を防止するとともに，テスト段階で脆弱性がないことを確認する。しかし，テスト段階で全ての脆弱性を発見し，取り除くことは難しい。また，ソフトウェアのバージョンアップの際に新たな脆弱性が生じる可能性もある。したがって，運用・保守段階でも継続的に脆弱性の有無を確認し，適切な対応を実施していくことが必要になる。

システム監査人は，ソフトウェアの脆弱性を原因とした情報セキュリティ被害を防止するために，ソフトウェアの脆弱性対策が適切に行われるためのコントロールが有効に機能しているかを確認する必要がある。

あなたの経験と考えに基づいて，設問ア～ウに従って論述せよ。

**設問ア**　あなたが携わった情報システムの概要，及びその情報システムにおけるソフトウェアの脆弱性によって生じるリスクについて，800 字以内で述べよ。

**設問イ**　設問アに関連して，ソフトウェアの脆弱性対策について，開発，テスト，及び運用・保守のそれぞれの段階において必要なコントロールを，700 字以上 1,400 字以内で具体的に述べよ。

**設問ウ**　設問イで述べたコントロールの有効性を確認するための監査手続について，確認すべき監査証拠を含めて 700 字以上 1,400 字以内で具体的に述べよ。

## 問2　消費者を対象とした電子商取引システムの監査について

情報技術の発展に伴い，インターネットを利用して消費者が商品を手軽に購入できる機会が増えてきている。これらの消費者を対象とした電子商取引の市場規模はますます拡大し，その形態も企業対個人取引（BtoC），インターネットオークションなどの個人対個人取引（CtoC）など，多様化している。最近では，ソーシャルネットワーク，全地球測位システム（GPS）などの情報と取引履歴情報とを組み合わせたビッグデータの分析・活用によるマーケティングなども広がりつつある。

一方，BtoC 又は CtoC のビジネスは，不特定多数の個人が対象であることから，情報システムの機密性が確保されていないと，氏名，住所，クレジットカード番号などの個人情報が漏えいするおそれがある。

また，取引データの完全性が確保されていないと，取引の申込み又は承諾のデータが消失したり，不正確な取引情報を記録したりするなど，契約成立又は取引に関わる判断根拠がなくなるおそれがある。

さらに，可用性が確保されていないと，一度に大量の注文が集中して情報システムがダウンするなどして，取引が妨げられて販売機会を逃すことによる損失が生じたり，損害賠償を請求されたりする可能性もある。

システム監査人は，このような点を踏まえて，消費者を対象とした電子商取引システムに関わる機密性，完全性及び可用性のリスクを評価して，リスクを低減するためのコントロールが適切に機能しているかどうかを確かめる必要がある。

あなたの経験と考えに基づいて，設問ア～ウに従って論述せよ。

**設問ア**　あなたが関係する消費者を対象とした電子商取引システムについて，その概要とビジネス上の特徴，及び情報システムを運営する立場から重要と考えるリスクを 800 字以内で述べよ。

**設問イ**　設問アで述べた情報システムにおいて実施すべきと考える機密性，完全性及び可用性を確保するためのそれぞれのコントロールについて，700 字以上 1,400 字以内で具体的に述べよ。

**設問ウ**　設問イで述べたコントロールの適切性を監査する場合の手続について，監査証拠及び確かめるべきポイントを踏まえて，700 字以上 1,400 字以内で述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 解答に当たっては，次の指示に従ってください。指示に従わない場合は，評価を下げることがあります。

(1) **問題文の趣旨に沿って解答してください。**

(2) 解答欄は，“あなたが携わったシステム監査，システム利用又はシステム開発・運用業務の概要”と“本文”に分かれています。“あなたが携わったシステム監査，システム利用又はシステム開発・運用業務の概要”は，2ページの記入方法に従って，全項目について記入してください。

(3) “本文”は，設問ごとに次の解答字数に従って，それぞれ指定された解答欄に記述してください。

・設問ア：800字以内

・設問イ：**700字以上** 1,400字以内

・設問ウ：**700字以上** 1,400字以内

(4) 解答は，丁寧な字ではっきりと書いてください。

7. 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 | 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。

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。