AU

平成29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	

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。

質問項目①，③～⑪は，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。

質問項目②は，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・運用業務の名称を記入してください。

問１　情報システムに関する内部不正対策の監査について

近年，従業員などの内部不正による，情報システムを対象とした情報漏えいなどが増えている。内部不正による損害には，情報漏えいなどに伴う直接的な損害に加え，組織の管理態勢の不備や従業員などのモラルの低さが露呈するなど，組織の社会的信用の失墜がもたらす損害も無視できない。

内部不正の動機は，組織，上司，同僚などへの不満，金銭目的など，様々である。また，従業員などが不正を行える環境や不正を正当化できる状況を組織が放置することも，内部不正を誘発する大きな要因になる。

情報システムに関する内部不正では，従業員などが業務を行うために有するアクセス権限を悪用して情報の不正窃取，改ざんが行われる場合が多く，外部の者や権限を有しない内部の者による不正アクセスよりも，その防止や発見が難しい。したがって，内部不正対策では，技術的対策に加え，組織的対策を適切に組み合わせることが重要になる。組織的対策には，例えば，規程の整備，労働環境の整備，内部不正が発生した際の対応手順の整備，規程・手順が遵守されるための各種施策の実施などがある。

システム監査では，内部不正を予防し，その被害を最小限にとどめるための技術的対策だけでなく，組織的対策が適切に行われているかどうかを確かめる必要がある。また，監査を行うに当たっては，当該対策が法令などに準拠して行われているかどうかという観点も重要になる。

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　あなたが携わった組織において，内部不正が発生した場合に重大な影響を及ぼす情報システムの概要と，その情報システムにおいて内部不正が発生した場合の影響について，800 字以内で述べよ。

設問イ　設問アに関連して，内部不正の技術的対策の実施状況を確認するための監査手続について，内部不正の特徴を踏まえた留意点を含めて，700 字以上 1,400 字以内で具体的に述べよ。

設問ウ　設問アに関連して，内部不正の組織的対策の実施状況を確認するための監査手続について，内部不正の特徴を踏まえた留意点を含めて，700 字以上 1,400 字以内で具体的に述べよ。

問2　情報システムの運用段階における情報セキュリティに関する監査について

企業などでは，顧客の個人情報，製品の販売情報などを蓄積して，より良い製品・サービスの開発，向上などに活用している。一方で，情報システムに対する不正アクセスなどによって，これらの情報が漏えいしたり，滅失したりした場合のビジネスへの影響は非常に大きい。したがって，重要な情報を取り扱うシステムでは，組織として確保すべき情報セキュリティの水準（以下，セキュリティレベルという）を維持することが求められる。

情報セキュリティの脅威は，今後も刻々と変化し続けていくと考えられるので，情報システムの構築段階で想定した脅威に対応するだけでは不十分である。例えば，標的型攻撃の手口はますます高度化・巧妙化し，情報システムの運用段階においてセキュリティレベルを維持できなくなるおそれがある。

そこで，情報システムの運用段階においては，セキュリティレベルを維持できるように適時に対策を見直すためのコントロールが必要になる。また，情報セキュリティの脅威に対して完全に対応することは難しいので，インシデント発生に備えて，迅速かつ有効に機能するコントロールも重要になる。

システム監査人は，以上のような点を踏まえて，変化する情報セキュリティの脅威に対して，情報システムの運用段階におけるセキュリティレベルが維持され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　あなたが関係する情報システムの概要とビジネス上の役割，及び当該情報システムに求められるセキュリティレベルについて，800字以内で述べよ。

設問イ　設問アを踏まえて，情報システムの運用段階においてセキュリティレベルを維持できなくなる要因とそれに対するコントロールを，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が有効に機能しているかどうかを確認する監査手続を，700字以上1,400字以内で具体的に述べよ。

〔 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。ただし，問題冊子を切り離して利用することはできません。

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（時計型ウェアラブル端末は除く。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。

試験問題に記載されている会社名又は製品名は，それぞれ各社又は各組織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。

©2017　独立行政法人情報処理推進機構