本書の使い方

本書は，システム監査技術者試験の**午後対策**を**重点的に効率良く学習**できるよう**書籍の構成**と**付録**を工夫しています。

専門知識の確認 → **解法テクニック ＋ 問題演習** → **解法テクニック ＋ 問題演習**

第２部 午前Ⅱ試験の重点対策	第３部 午後Ⅰ試験の重点対策	第４部 午後Ⅱ試験の重点対策
午後試験にもつながる 専門知識を重点分野に 絞って解説！	問題概要分析に基づく **問題選択のコツ！！** ＋ 段階的にわかりやすい **解法説明と詳細な解説**！	出題パターンごと，設問ごとの **詳細な論述テクニック！！** ＋ **著者の出題予想**を基にした **全問オリジナル問題と論文事例！**
付録① **試験直前に役立つ** **キーワード集** 巻末のキーワード集で直前チェック！	付録② **予想配点付き解答用紙** 巻末の配点付き解答用紙を使って本番さながらに演習，自己採点で理解度の把握！	**付録③　付録④** **論文用紙・論文自己評価シート** ダウンロードサービスの論文用紙を使って本番さながらに演習，自己評価シートによる振り返り！！

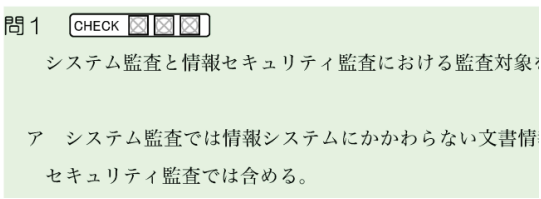
◆第２部◆

システム監査，法務，セキュリティ，サービスマネジメントの分野を重点的に学習します。

それぞれの章の構成は，**出題ポイントのまとめ**と**演習問題**の二つの構成になっています。

① **出題ポイントのまとめ**：その分野に出題される**重要なテーマ**について理解し，それぞれのテーマの**出題**ポイントを，確実に把握します。

② **演習問題**：問題を解くことで，**知識のさらなる定着**を図ります。収録した問題は過去の試験で実際に出題された問題の中から厳選しています。



CHECK ボックスを利用して理解度を確認しましょう。

☐ 自信あり
☒ 自信なし

◆第３部◆

① **「1-1 記述式問題の内容把握と選択体験」**：自分が何を判断材料に問題選択をしているのか，自分の傾向を確認！！

↓

② **「1-2 記述式問題の解き方」，「1-3 解答への具体的なアイディア」**：記述式の解き方のカギを習得！！

↓

③ **演習問題**：実際に問題を解く。　※巻末の解答用紙をコピーして活用してください。

↓

④ **演習実施後，各問の「解答作成のポイント」と「1.2.2　具体的な解答に当たって」で解答力アップ！**

⇒各問の「解答作成のポイント」と予想配点表で，**自分の解答内容をチェック！**

⇒1.2.2（1）解答作成の手順，（2）具体的な解答作成に当たってのプロセスを実際に踏んでいるか確認！（3）解答のレベルアップで，自分のレベルを **ABCD で自己評価！**

※演習問題の CHECK ボックスを利用して理解度を確認しましょう。CHECK A B C D

↓

解答例との大きな差異がある場合は，要因を分析！

課題が明白になったら，「1-2 記述式問題の解き方」，「1-3 解答への具体的なアイディア」に戻りましょう。以前より内容が自分の中に入ってくるはずです！

◆第４部◆

① **出題傾向の把握**：どんなテーマの問題が出題されているのか傾向を把握。

↓

② **下書き論文作成**：午後Ⅱは，とにかく**論文を書くことに慣れること**が大切です。

「2-6 論文テンプレート：初めて論文を作成する方のために」の**テンプレート**を使って，**論文を設計**してみましょう。

↓

③ **２時間で論文作成**：「3-2 論文事例」を題材に，２時間で論文を書いてみましょう。

※第４部の演習問題は，全問著者の出題予想テーマを基にしたオリジナル問題です！

↓

④ **自己チェック**：**「論文自己評価シート」**を使って，自己評価しましょう！

↓

筆者が書いた論文事例と見比べて，自己添削後，課題を明確にし，どのように改善すべきか考えましょう。

Contents

目 次

本書をご購入いただき，誠にありがとうございます。

より分かりやすく，よりご満足いただける書籍作りをするために，お客さまのご意見やご要望をお聞かせいただき，改善に役立てたいと考えております。

学習後は，本書に関する簡単なアンケートにぜひご協力をお願いいたします。次のURL からご回答ください。

4 月末，10 月末までにアンケートにご回答いただいた方の中から抽選で 20 名様に，図書カード 1,000 円分をプレゼント！ いたします。

当選された方には，抽選後，ご登録いただいたメールアドレスにご連絡させていただきます（当選者の発表は，当選者へのご連絡をもって代えさせていただきます）。

なお，本書のアンケートのご回答期限は 2018 年 10 月末です。

URL https://www.itec.co.jp/books/2018au_jutentaisaku.html

Part 2　第1章　Chapter 1

午前Ⅱ(専門知識)問題の学習方法

1－1　午前Ⅱ試験の出題状況

午前Ⅱ（専門知識）は 25 問全問解答が必要な必須問題として出題されます。

図表 1-1 に「午前Ⅱ（専門知識）試験の出題分野と平成 26～29 年度の出題数」を示します。図表 1-2 に「平成 29 年度午前Ⅱ（専門知識）試験 25 問の出題内容と出題分野」を示します。

分類	大分類	中分類	レベル	出題数 26 年	出題数 27 年	出題数 28 年	出題数 29 年
テクノロジ系	技術要素	データベース	○3	1	1	1	1
		ネットワーク	○3	1	1	1	1
		セキュリティ	○3	3	2	3	3
	開発技術	システム開発技術	○3	2	2	2	2
マネジメント系	サービスマネジメント	サービスマネジメント	○3	2	2	2	2
		システム監査	◎4	10	12	10	10
ストラテジ系	経営戦略	経営戦略マネジメント	○3	1	2	1	2
	企業と法務	企業活動	○3	2	1	2	1
		法務	◎4	3	2	3	3
出題合計				25	25	25	25

※◎は出題範囲のうち，重点分野であることを示しています。またレベルの 3，4 は技術レベルを表し，4 が最も高度で，上位は下位を包含します。

図表 1-1　午前Ⅱ（専門知識）試験の出題分野と平成 26～29 年度の出題数

図表 1-1 に示すとおり，出題分野は重点分野◎として「システム監査」と「法務」が指定され，技術レベルも高度な「レベル 4」となっています。その他の分野は「レベル 3」となっており，午前Ⅰ試験と同じレベルです。なお，図表 1-1 の出題数は，次の図表 1-2「平成 28 年度午前Ⅱ（専門知識）試験 25 問の出題内

1－2　午前Ⅱ試験の出題傾向と学習方法

平成 29 年度午前Ⅱ試験について，出題分野別に整理した表を図表 1-3 に示します。

出題分野	出題数	出題比率
システム監査	10 問	40%
法務	3 問	12%
セキュリティ	3 問	12%
サービスマネジメント	2 問	8%
システム開発技術	2 問	8%
経営戦略マネジメント	2 問	8%
企業活動	1 問	4%
ネットワーク	1 問	4%
データベース	1 問	4%
合計	25 問	100%

図表 1-3　平成 29 年度午前Ⅱ（専門知識）試験の出題分野

(1)　出題傾向と分析

平成 29 年度午前Ⅱ試験の出題分野は，「システム監査」が 10 問でトップ，次いで「法務」，「セキュリティ」が 3 問，「サービスマネジメント」，「システム開発技術」，「経営戦略マネジメント」が 2 問でした。「システム監査」と「法務」は重点分野に指定されており，この 2 分野で 25 問中の 13 問（52%）を占めることになります。重点分野の「システム監査」と「法務」，システム監査関係分野の「セキュリティ」について，平成 22～29 年の出題数推移を図表 1-4 に示します。

出題分野	平成 22 年	平成 23 年	平成 24 年	平成 25 年	平成 26 年	平成 27 年	平成 28 年	平成 29 年
システム監査	14.5 問	10 問	11.5 問	11 問	10 問	12 問	10 問	10 問
法務	3 問	3 問	2 問	3 問	3 問	2 問	3 問	3 問
セキュリティ	1.5 問	3 問	1.5 問	1 問	3 問	2 問	3 問	3 問

図表 1-4　重点分野の出題数推移

Part 2　Chapter 2

第2章 システム監査

2－1　システム監査とは

2.1.1　システム監査とは

システム監査は，情報システムを対象とする監査です。ここでは，参考として，監査と従来のシステム監査の定義を挙げておきます。

- 監査の定義：独立かつ客観的立場で監査対象を評価基準に照らして点検・評価し，その結果を監査報告書に取りまとめ，組織体の長に提出することである（プライバシーマーク制度における監査ガイドライン；2000）。
- システム監査の定義：監査対象から独立かつ客観的立場のシステム監査人が情報システムを総合的に点検及び評価し，組織体の長に助言及び勧告するとともにフォローアップする一連の活動（1996 年版システム監査基準Ⅱ．用語の定義(1)システム監査）。

現行の平成 16 年版システム監査基準にはシステム監査の定義の記載はありません。次に挙げる「システム監査基準Ⅱ．システム監査の目的」に記載されている内容がシステム監査の定義に該当するといわれています。

「システム監査の目的は，組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを，独立かつ専門的な立場のシステム監査人が検証又は評価することによって，保証を与えあるいは助言を行い，もって IT ガバナンスの実現に寄与することにある」

特徴については，システム監査基準解説書に次のように記されています。

- 情報システムにまつわるリスクに対するコントロールについて監査を実施すること
- コントロールがリスクアセスメントに基づいて適切に整備・運用されているかを検証又は評価すること
- 監査には，保証型又は助言型の監査があること
- 最終的には IT ガバナンスの実現に寄与すること

実際にはシステム監査と情報セキュリティ監査は共通する部分も多くあります。システム監査が任意監査を出発点とした助言型監査，情報セキュリティ監査は情報セキュリティマネジメントシステムが機能していることを保証するISMS認証などが中心になっているともいえます。

演習問題

問1　CHECK ☐☐☐　(H18春-AU 問52)

システム監査と情報セキュリティ監査における監査対象を説明したものはどれか。

ア　システム監査では情報システムにかかわらない文書情報を対象に含めないが，情報セキュリティ監査では含める。

イ　システム監査と情報セキュリティ監査は，ともにすべての情報資産を対象とする。

ウ　情報セキュリティ監査では情報システムにかかわる人を対象に含めないが，システム監査では含める。

エ　情報セキュリティ監査は情報システムを対象としないが，システム監査は対象とする。

解答解説

問1　解答－ア

システム監査と情報セキュリティ監査の監査対象についての知識を問う問題です。情報セキュリティ監査は情報資産が監査対象です。文書情報は情報資産ですので監査対象になります。システム監査は情報システムが監査対象ですので情報システムにかかわらない文書情報は監査対象にはなりません。したがって，（ア）が正解です。

イ：システム監査は，情報システムが監査対象であり，情報システム以外の情報資産は対象ではありません。

ウ：情報セキュリティ監査は，情報資産が監査対象であり，情報システムにかかわる人も情報資産に該当します。

エ：情報セキュリティ監査は情報資産が監査対象です。情報システムも情報資産の一つと考えられますので監査対象になります。

Part 3　第1章　Chapter 1

午後Ⅰ記述式問題の解法テクニック

1－1　記述式問題の内容把握と選択体験

記述式学習を始めるに当たって，記述式問題の内容を把握するため，過去 13 年間の記述式試験の内容を図表 1-2〜1-14 にまとめてみました。試験の概要に問題選択欄を設けましたが，みなさんには，実際にどのような問題を選択するかを体験頂きたいと思います。それは，問題選択に失敗したとのお話をよく聞くからです。

平成 17〜20 年は 4 問から 3 問選択，平成 21〜25 年は 4 問から 2 問，平成 26〜29 年は 3 問から 2 問選択する方式で出題されました。

選択の考え方としては，平成 17 年〜20 年，平成 26〜29 年は，「どの問題を解答せずパスするか，選択しない 1 問を選択する」，平成 21〜25 年は「どの問題を選択するか，選択する 2 問を選ぶ」といった考え方で問題選択を体験してみてください。ただし，概要を読んで 5〜10 分程度で時間をかけずに実施してください。お時間のある方は実際に試験センターのホームページから試験問題を入手し，問題の内容を見るとよいでしょう。

年度	出題数	解答数
平成 29 年〜26 年	3 問	3 問から **2** 問選択
平成 21 年〜25 年	4 問	4 問から **2** 問選択
平成 17 年〜20 年	4 問	4 問から **3** 問選択

図表 1-1　出題数と解答数

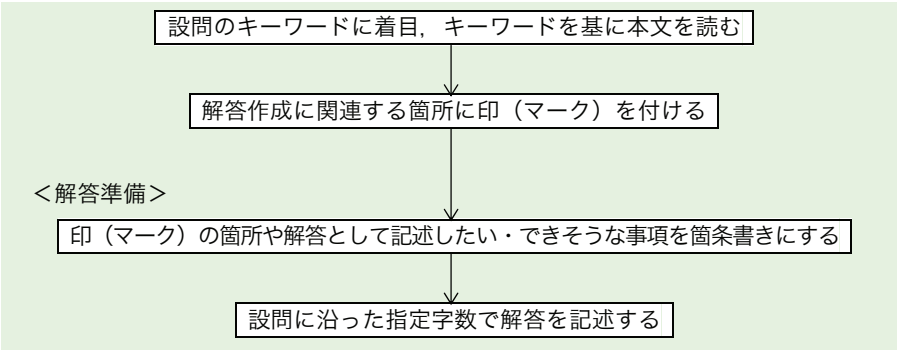
1.1.1 へ進む前に，次の出題内容について具体的に選択してみましょう。選択した問題については，**選択欄の問題番号を○印で囲んでください。**

1.2.2　具体的な解答に当たって

(1)　解答作成の手順

前述したように，具体的な解答を作成するに当たっては，冒頭の記述と設問を読んでから本文を読みにかかることになります。設問には，解答する上でのポイントとなるキーワードが必ず記述されているので，そのキーワードを基に本文を読み進むことです。そして，**解答に結び付く，又は解答に関連しそうな箇所にはアンダーラインなどの印（マーク）**を付けておくとよいでしょう。印（マーク）を付けておくことで，解答作成のために読み返したときに，迅速・的確に要点を把握できる場合も多いからです。ほとんどの場合，解答の手掛かりは本文中にあるといえます。

実際の解答は，「～について 40 字以内で述べよ」といった指定字数の解答が多いので，記述したい内容を箇条書きのメモにしてから，設問の指定に従って解答を作成しましょう。



図表 1-22　解答作成の手順

(2)　具体的な解答作成に当たって

①　1 問 1 問，着実に解答する

具体的に解答を作成する上で重要なことは，選択した 2 問について，着実に解答していくことです。選択した問題は必ず解答することを肝に銘じ，途中で最初に解答しないと決めた問題に移るようなことは絶対に避けるべきです。設問についても，着実に解答することが必要で，難しい設問に遭遇した場合も，「後で見直して解答しよう」という考え方はもたないようにすべきです。なぜなら，後で見直す時間がとれないことが多いからです。

Part３　Chapter４

第４章 テーマ別システムの監査に関する演習問題

テーマ別システムの監査は，第２章の情報システムのライフサイクル，第３章の適用業務システムを横断するテーマに関する監査の問題です。

クラウドコンピューティングは，平成 24 年 5 月のシラバス改訂に伴って，システム監査技術者試験の午後の出題範囲に位置付けられました。

平成24年度問１の「パブリッククラウドサービスを利用したシステムの監査」は，シラバス改訂に先だって出題されておりますし，平成 26 年度問 3 の「個人が保有するモバイル端末の業務利用の監査」は，BYOD の問題，平成 28 年度問 1 は CSIRT の問題，平成 29 年問 3 は，製油所の制御ネットワークの問題であり，新しいテーマや技術的システムのテーマにも注意しておく必要があります。

次の演習問題を収録しています。

演習問題の答案用紙と配点予想を巻末に掲載しています。コピーして活用してください。

演習問題　1

CHECK A B C D

問3　制御ネットワーク及び制御システムの監査に関する次の記述を読んで，設問 1～4 に答えよ。

(H29 春-AU 午後Ⅰ問 3)

D 社は，エネルギー企業グループ系列の中規模の石油精製会社である。東京に本社があり，東日本で製油所を操業している。

〔D 社ネットワークの統合〕

D 社では，老朽化した製油所の装置設備を，10 年前に改装した。その際，製油所の石油精製制御システム（以下，制御システムという）も刷新した。また同時に，制御システムが接続されている製油所のネットワーク（以下，制御ネットワークという）と，生産管理システムなどの各種業務システム（以下，業務システムという）が接続されているネットワーク（以下，本社基幹ネットワークという）を統合した。

D 社の現在のネットワーク構成（概要）を，図 1 に示す。

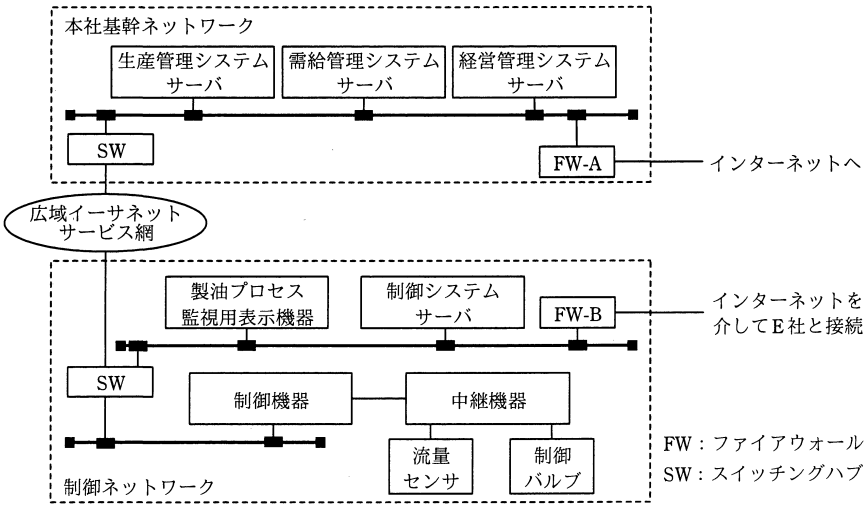


図 1　D 社のネットワーク構成（概要）

制御ネットワークは，広域イーサネットサービス網で本社基幹ネットワークと接続されている。また，制御システムの遠隔監視・保守のために，インターネットを

解答作成のポイント Point

＜解答の方針＞

本問は，エネルギー企業グループ系列の中規模の石油精製会社 D 社における他社制御ネットワーク及び制御システムへのセキュリティインシデント発生に起因する制御ネットワーク及び制御システムに関するセキュリティ監査の問題です。

冒頭の制御ネットワーク及び制御システムの監査と設問が 4 問あることを念頭に，図 1「D 社のネットワーク構成（概要）」，表 1「セキュリティ管理の相違点（抜粋）」を認識してページをめくり，設問 1〜4 を読み，各設問が次の内容であることを把握してから本文を読みます。

設問 1　〔本調査での発見事項〕(1)について，システム監査人が製油所安全管理規程と情報セキュリティ管理規程に関して確認すべき内容を，40 字以内で解答する。

設問 2　〔本調査での発見事項〕(2)について，システム監査人想定の“システム設定上の不備に起因するセキュリティインシデント”とは何か。50 字以内で解答する。

設問 3　〔本調査での発見事項〕(3)について，

(1) セキュリティ管理者によるセキュリティパッチ適用前の確認が行われていることを，システム監査人が確かめる場合，査閲すべき文書を二つ各 20 字以内で解答する。

(2) システム監査人が想定した“OS の脆弱性を突いたセキュリティインシデント発生に備えた補完的コントロール”を 20 字以内で解答する。

設問 4　〔本調査での発見事項〕(4)について，システム監査人が対策①，②の他に，制御ネットワーク側で遠隔監視・保守に伴う不正アクセスを防ぐための技術的対策が適切に講じられていることを確認するための監査手続を，50 字以内で解答する。

では，問題の概要を整理してみましょう。

(4)　操油部計装課：セキュリティ専門技術者不在
・FW-B 設定を E 社推奨ポリシに基づき E 社技術員が実施
・FW-B 経由遠隔監視・保守の不正アクセス対策：①，②実施を E 社に要請
対策①：遠隔監視・保守を行うため制御ネットワーク接続端末・利用者の限定
対策②：制御ネットワークへのアクセス状況記録，遠隔監視・保守以外の操作有無確認（製油所安全管理規程で定めた頻度での実施と異常発生時の報告）

＜設問１の解き方＞

設問１は〔本調査での発見事項〕(1)について，システム監査人が製油所安全管理規程と情報セキュリティ管理規程に関して確認すべき内容を問うています。

「D 社における全社的なセキュリティ管理の観点からは内容の確認が行われていない」の記載を踏まえ，安全管理規程と情報セキュリティ管理規程の整合性，管理レベルが同等で相互に不整合・矛盾しないことをベースに解答します。

＜設問２の解き方＞

設問２は〔本調査での発見事項〕(2)について，システム監査人想定の“システム設定上の不備に起因するセキュリティインシデント”とは何かを問うています。

管理対象として重視されていないセキュリティ領域のアクセス対策，論理アクセス制御やサーバのハードニングを踏まえ，内部者による不正アクセス（情報の持出し），外部不正アクセス（インターネット経由のサイバー攻撃など）を想定し解答することになります。

＜設問３の解き方＞

設問３は〔本調査での発見事項〕(3)について，

(1)はセキュリティ管理者によるセキュリティパッチ適用前の確認が行われていることを，システム監査人が確かめる場合，査閲すべき文書を二つ問うています。

セキュリティ管理者によるセキュリティパッチ適用事前確認事項として，
・表１項番５のセキュリティ要件満足についてのセキュリティ管理者の事前確認
・制御データ処理時の数値変動とタイミングの変化が定められた範囲内に収まるか確認

を踏まえ解答します。

(2)はシステム監査人が想定した“OS の脆弱性を突いたセキュリティインシデント発生に備えた補完的コントロール”を問うています。

「セキュリティパッチ適用の間隔が比較的長いこともあり，その間の OS の脆弱性を突いたセキュリティインシデント発生に備えた補完的コントロールが必要」という記載に着目し，侵入防御システムなどをベースに解答します。

＜設問４の解き方＞

設問 4 は〔本調査での発見事項〕(4)について，システム監査人が対策①，②の他に，制御ネットワーク側で遠隔監視・保守に伴う不正アクセスを防ぐための技術的対策が適切に講じられていることを確認するための監査手続を問うています。

E 社の推奨ポリシに基づく E 社技術者による FW-B 設定において不要なポートが開いていないかなどをベースに解答します。

〔解答例〕

［設問１］

両規程で定められたセキュリティ管理のレベルが同等であり，相互に矛盾がないこと（38 字）

［設問２］

不要なアクセス権をもつ社員などによる情報の持出しやインターネット経由の外部からの不正アクセス（46 字）

［設問３］

(1) ① セキュリティパッチ適用計画書（14 字）

② 制御データ処理時の影響調査結果報告書（18 字）

(2) 侵入防御システムの導入による防御（16 字）

［設問４］

ポリシを査閲し，遠隔監視・保守に必要なパケットだけを通過させる設定になっていることを確認する。(47 字)

Part 4　第1章　Chapter 1

午後Ⅱ論述式問題の解法テクニック

1－1　論述式試験を知る

1.1.1　平成29年度論文問題

平成 21 年度から新制度のシステム監査技術者試験が実施されています。新試験制度のシステム監査技術者試験の対象者像としては，情報システムに加え，組込みシステムが追加されました。平成 21 年度の論文試験では，組込みシステムについての出題はありませんでしたが，平成 22 年度問 1，平成 23 年度問 3，平成 24 年度問 2 で組込みシステムも含めた問題として出題されました。しかし，平成 25 年度以降は，組込みシステムの表記はなく，組込みシステムも含めた情報システムととらえているようです。平成 29 年度はどうだったでしょうか？

まず，平成 29 年度に出題された午後Ⅱ試験の問題を見てみましょう。

〔例題〕

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

(H29 春-AU　午後Ⅱ問 2)

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。

1.1.2　下書き論文の必要性

(1)　通常の資料との違い

読者の中には，実際に業務を遂行していく上で，企画・提案書，報告書，マニュアル，仕様書などの作成経験者も多いと思います。そうした通常の資料と論文は，どこが異なるのでしょうか。論述式試験での論文作成と通常の実務資料作成との相違をまとめたものが図表 1-2 です。これを基に説明します。

項目	当試験の小論文	通常の実務資料など
①　時間	２時間に限られている	ある程度自分で調整できる
②　タイミング	その場限り１回だけ	業務遂行上，連続性がある
③　作成対象者	出題（採点者）	顧客，ユーザ，上司，設計部門，開発部門，プログラマ
④　作成対象者との面識の有・無	ない	あるケースが多い
⑤　媒体	論文だけで説明	口頭で補足説明が可能
⑥　様式／書式	解答（原稿）用紙 800 字×５	標準書式が決まっている
⑦　用語	一般的で正確な記述	略語などが通用するケースが多い

図表 1-2　実務資料との違い

まず，第１に，**厳密に時間を制限されている**という点です。通常の業務で作成する資料に，これほど厳密に時間が制限されているケースはそう多くはないでしょう。もちろん，業務でも時間に追われ作成する場合も頻繁に見られますが，たいていは「前もって作成する」など，自分の裁量で対応できる部分が大きいと思います。

第２に，**出題者は皆さんを知らないということです。実務上の資料作成では，例えば企画・提案書やマニュアルならユーザや顧客，報告書なら上司，仕様書ならプログラマ，というように，該当資料を作成する対象を皆さんが知っている場合も多いでしょう。また，その場合には相手も皆さんのことを知っているのではないでしょうか。**

これによって補われる点は多いです。つまり相手は，単に作成した資料の情報にとどまらず，皆さんに関する情報を日々の業務の中で知り得る機会も多く，資料の中の説明不足などの点を知らず知らずのうちに補ってくれているのです。また，共通の用語や前提の問題も大きいです。皆さんは，逐一これらのことを説明

コラム　Column

担当の者がお答えします。

今回は今でもはっきり記憶にある，30 年前の監査についての出来事についてお話します。

わたしが新入社員として情報システム部に配属されたある日の朝礼でのことです。

部長：「今日は監査の日だ。余計なことは言わないように！」

わたしが怪訝な顔をしたからでしょうか。その後，

部長：「いいか，もし監査で質問されたらこのように答えなさい」

「担当の者がお応えします !! 」

「監査ではしゃべってはいけないんだ！」という印象が強く残ったのを昨日のことのように覚えています。

それは監査に対して監査を受ける側の意識として，「監査で摘発される」，摘発型監査，強制監査のようなイメージが非常に強かったからだと思います。

時が変わり，現在はわたしがシステム監査人でヒアリングする立場です。

システム監査のヒアリング時に，「担当の者がお応えします !! 」と回答されたらどうでしょうか。「公平で客観的なシステム監査はできない」と途方に暮れると思います。

システム監査は摘発型ではなく改善指向型監査ですので，私は監査のヒアリングの最初に，次のようにお話することにしています。

「システム監査は改善指向型監査です。摘発するために来たのではありません。皆さんの業務・組織を良い方向にと願ってのことですので，ありのままをお答えください」

〔事例6〕

ビッグデータ利用のシステム監査について　(865381)

情報通信技術の目覚ましい発展と進化を背景として，これまで考えられなかった巨大容量のデータの収集と分析が可能になった。既に蓄積された大量データから，価値がありそうな情報や仮説を引き出したり，フリーテキストを分析し，現状や予想傾向分析に利用されたりしており，更に最近のスマートデバイスやTwitter などの SNS の普及は，“ビッグデータ”の利用の可能性をますます高めることは間違いない状況といえる。

一方，本人が知らない間にスマートフォンの位置情報や電子メールのアドレス帳などの情報が漏えいしている状況も存在する。また，個人が特定されていないプライバシ情報が，各種情報とつながることによって，個人として特定され，個人情報の漏えいを引き起こしている状況も見られ，今後そうしたリスクは増大すると考えられる。

“ビッグデータの利用”に当たっては，情報利用の利便性とプライバシ等個人の権利に配慮した管理が不可欠であり，システム監査としての貢献が期待される。

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　あなたが関係する組織の情報システムの概要と，ビッグデータの利用状況について，800 字以内で述べよ。

設問イ　設問アで述べたビッグデータの利用状況について，想定されるリスクと，当該リスクへの対策について，700 字以上 1,400 字以内で具体的に述べよ。

設問ウ　設問イで述べたリスクを踏まえて，ビッグデータの利用について，システム監査するとき，監査のチェックポイントと監査手続について，700 字以上 1,400 字以内で具体的に述べよ。

〔解説〕

本問は，「ビッグデータ利用のシステム監査」がテーマです。監査対象分野としては，テーマ別監査に分類される出題ですが，業務アプリケーションシステムがビッグデータを取り扱うケースもあることを考えると，アプリケーションシステムやシステム企画・開発・運用業務としても記載可能といえます。

設問アでは,「あなたが関係する組織の情報システムの概要とビッグデータの利用状況」が出題テーマです。見出し構成としては，次のようになります。

Ⅰ．情報システムの概要とビッグデータの利用
　Ⅰ.1　情報システムの概要
　　(1)　情報システムの構成
　　(2)　情報システムの特徴
　Ⅰ.2　ビッグデータの利用

設問イでは，設問アで述べたビッグデータの利用に係るリスクと対策についての記載を求めています。見出し構成としては，次のようになります。

Ⅱ．ビッグデータの利用に係るリスクと対策
　Ⅱ.1　ビッグデータの利用に係るリスク
　Ⅱ.2　ビッグデータの利用に係るリスクへの対策

設問ウは，組織としてのビッグデータの利用について，システム監査する場合の監査のチェックポイントと監査手続を求めています。ここでは，設問イで述べたリスクを踏まえた記述を求めており，設問イで記載した延長線上で論理を展開することになります。

Ⅲ．ビッグデータの利用のシステム監査のチェックポイントと監査手続
　Ⅲ.1　ビッグデータの利用のシステム監査のチェックポイント
　Ⅲ.2　ビッグデータの利用のシステム監査の監査手続

〔事例6　解答論文例〕

本文（設問ア）　800字以内で記述してください。

Ⅰ．コンテンツ提供システムの概要とビッグデータ利用

Ⅰ．1　コンテンツ提供システムの概要

私は情報サービス関連Y社に10年勤務し，現在はコンテンツ提供システムの運用・保守管理を担当している。

(1)　コンテンツ提供システムの開発目的

本システムは，画像・音声などの各種情報のコンテンツホルダに対し，インターネットをベースとするディジタルコンテンツ販売のプラットフォーム提供を目的に，約1年の開発期間を経て3年前にリリースした。現在10数社のコンテンツホルダが本システムを利用し，一般ユーザ向けにディジタルコンテンツを販売している。

(2)　本システムの概要

本システムは，コンテンツ販売サイト運営に必要な機能をワンストップで提供しており，コンテンツ販売サブシステム，ユーザ管理サブシステム，決済・売上管理サブシステムから構成される。

本システムの保守・運用は，私を含め4名のSEが担当しているが，コンテンツ購入者が不特定多数であり，個人情報を取り扱う点に特徴がある。しかも，オープンなインターネット上でデータを授受するため，セキュリティ管理は重要なポイントといえる。したがって，本システムで使用するサーバは，厳重な管理下にあるY社のデータセンタに設置しシステム運用部が管理している。

Ⅰ．2　本システムとビッグデータの利用状況

本システムは，稼働後3年を経過し，安定稼働している。この間のメールマガジンやキャンペーン情報，顧客のコンテンツ購入情報等の大量情報が蓄積されている。

現在，本システムの新機能として，蓄積データをベースに利用・分析した結果を次世代コンテンツ開発に生かすことや顧客ごとのきめ細かい販売促進情報に展開することが強く求められており，効果的なモデリング・分析ツールの開発に取り組んでいる。

100字　200字　300字　400字　500字　600字　700字　800字