Contents

目 次

Part 1　第1章　Chapter 1

応用情報技術者試験の出題範囲

独立行政法人　情報処理推進機構　情報処理技術者試験センター（以下，試験センター）から発表されている「情報処理技術者試験　出題範囲」によれば，応用情報技術者試験を「高度 IT 人材となるために必要な応用的知識・技能を問う」ものとしています。そして，この試験は多肢選択式（四肢択一）の午前試験と，記述式の午後試験によって行われることになりますが，午前，午後試験の目的は，それぞれ次のようになっています。

受験者の能力が当該試験区分における**期待する技術水準**に達しているか，
・午前試験…**知識**を問うことによって評価する
・午後試験…**技能**を問うことによって評価する

では，応用情報処理技術者に対する“期待する技術水準”を理解する前提知識として，まずは，応用情報技術者試験の対象者像を理解しましょう。

応用情報技術者試験は，旧試験制度のソフトウェア開発技術者試験の範囲を拡大した内容として位置付けられていますので，ソフトウェア開発技術者試験の対象像と比較したものを見てみましょう。

	対象者像
ソフトウェア開発技術者試験	情報システム開発プロジェクトにおいて，内部設計書・プログラム設計書を作成し，効果的なプログラムの開発を行い，単体テスト・結合テストまでの一連のプロセスを担当する者
応用情報技術者試験	高度 IT 人材となるために必要な応用的知識・技能をもち，高度 IT 人材としての方向性を確立したもの

ソフトウェア開発技術者試験の対象者像を見ると，一般に，内部設計やプログラム設計と呼ばれるソフトウェア開発作業を行っている人を対象とした試験であったことが分かります。

これに対して，応用情報技術者試験では，実際にソフトウェア開発作業を経

Part 1　第３章　Chapter 3

本書の学習方法

(1)　本書の構成

本書は，「午後問題の重点対策」という名前が示すように，午後試験に出題される問題を解くための着眼点や，解答の導き方を中心に解説する内容になっています。そして，午後試験の範囲である 13 の分野を，9 のテーマに再構成したものとなっていますが，情報セキュリティ，システムアーキテクチャ，ネットワーク，データベースの 4 テーマについては，午後試験特有のポイントがあるので，こうした部分を簡単に説明しています。そして，その他の分野を含めて，演習問題によって知識の理解を深め，解答のための着眼点，解答を身に付けられるように工夫しています。しかし，本書の目的はあくまでも午後試験の対策ですから，知識の復習部分については，あまり多くのページを割くことはできません。したがって，この部分で前提知識が不足していると感じた方は，その修得のために午前試験の対策書やテキスト，そして，専門書などで知識の整理をするようにしてください。

一方，その他の情報システム開発，プログラミング（アルゴリズム），組込みシステム開発，マネジメント系，ストラテジ系問題の 5 テーマについては，残念ながら前述した 4 テーマと違って出題範囲が広く，ポイントを絞り込むことが難しいので，演習問題による学習を中心に構成しています。

第 2 部については，前述の 4 テーマが，おおむね次のような構成になっています。

例　第 1 章　情報セキュリティ

〔学習のポイント〕
重要テーマごとに学習すべきポイントを解説しています。

〔例題〕
所々に例題と入った問題と解説があります。これは基礎知識を午前問題などで確認するためのものです。

〔演習問題〕
過去に出題された試験問題の考え方と解答を解説しています。

Part 2　第1章　Chapter 1

情報セキュリティ

学習のポイント

情報セキュリティに関することとしては，次のような内容が午後試験の出題範囲に挙げられています。

情報セキュリティポリシ，情報セキュリティマネジメント，リスク分析，データベースセキュリティ，ネットワークセキュリティ，アプリケーションセキュリティ，物理的セキュリティ，アクセス管理，暗号，認証，PKI，ファイアウォール，マルウェア対策（コンピュータウイルス，ボット，スパイウェアほか）不正アクセス対策，個人情報保護　など

平成 26 年度の春期試験から，午後問題の問 1 として，情報セキュリティをテーマとする問題が全受験者必須の問題になりました。必須問題になってから出題傾向が大きく変わったわけではありませんが，情報セキュリティに関する学習は，全受験者が避けては通れないものになりました。

これまでの午後試験には，暗号化，認証，セキュリティ攻撃と対策，アクセス制御，マルウェア対策などの問題が出題されました。今後もこのような傾向の問題が出題されると思いますが，情報セキュリティ分野の特徴は，変化が激しいことです。平素から，職場や学校，そして，インターネット上などにおいて，話題になっている情報セキュリティ関連の事柄に対して関心をもつことが大切です。また，セキュリティ対策の基礎となる，暗号化，認証技術，アクセス制御技術の基本について理解しておく必要があります。

(1)　暗号方式

暗号とは，データに対して何らかの処理を施し，第三者がその内容を見ても意味が分からなくすることです。しかし，意味が分からなくすることができても，当事者が，その内容から元のデータ内容を知ることができなくなってしまっては意味がありません。したがって，暗号方式は，データを暗号化できるの

と同時に，暗号化された内容を元に戻せる（復号）ものでなくてはなりません。ちなみに，暗号化される前のデータのことを平文（ひらぶん）と呼び，暗号化されたデータは暗号文と呼ばれます。

平文　→（暗号化）→　暗号文　→（復号）→　平文

暗号方式は，平文を第三者に分からないように加工し，その内容から元の平文が復元できればよいのですから，工夫次第でいろいろな方式を作ることができます。しかし，一般的には，暗号の強度（第三者による解読のしづらさ）などの関係から，幾つかの代表的な方式を使うことがほとんどです。方式が同じであれば，平文から暗号文を作り出す方法は同じなので，誰にでも解読されてしまいます。このため，暗号化には，“鍵”と呼ばれるデータが使われます。

例えば，数値データに対して，何らかの数を足すという暗号化方式があったとします。この場合，足すというのが処理方式です。そして，何らかの数というのが鍵に相当します。数を足すことによって暗号文にしたのですから，そのときに足した数を引けば，復号できますが，その足した数が分からなければ，復号できません。したがって，この足した数を鍵として当事者だけの秘密にしておけば，暗号方式として利用できるのです。まずは，暗号方式は，処理方法と鍵から成り立っているということを理解してください。

暗号方式は，鍵の性質によって，共通鍵暗号方式，公開鍵暗号方式に大きく分けられます。

①　共通鍵暗号方式

共通鍵暗号方式は，暗号化と復号とで同じ鍵を使います。同じ鍵を使うのですから，鍵の内容を第三者に知られてしまうと簡単に解読されてしまい，暗号としての意味がなくなってしまいます。したがって，鍵を秘密にしておかなくてはなりません。共通鍵暗号方式には，暗号化や復号の処理が比較的簡単なため，処理時間が短くて済むという長所があります。しかし，処理が簡単な分，解読されやすいという欠点があります。また，暗号を使ったデータ交換を行う当事者ごとに一つの鍵が必要となるため，鍵の数が多数必要となります。さらに，その鍵を秘密裏に受け渡し，その後も秘密に管理しなくてはなりませんから，鍵の管理が煩雑であるということも欠点とされています。

②　公開鍵暗号方式

公開鍵暗号方式では，暗号化の鍵と復号の鍵は違うものを使います。そして，暗号化の鍵からは，復号鍵の内容が分からないようになっています。暗号化では，暗号文が第三者に解読されることが問題なのであって，第三者が

その鍵を使って暗号文を作り出しても特に問題は発生しません。このため，第三者に復号されることのないように，復号鍵は秘密にしておかなくてはなりませんが，暗号化に用いる鍵は第三者に知られても問題は発生しません。公開鍵暗号方式を利用する場合には，暗号化の鍵を公開して，自分宛ての暗号化には全てこの鍵を使ってもらうことが可能となります。その結果，鍵の受渡しも容易になりますし，秘密に管理するのは自分の復号鍵だけになり，管理も単純になります。

公開鍵暗号方式は，共通鍵暗号方式に比べて強度も高く，鍵の管理も容易ですから，理想の暗号化方式のようですが，その分だけ処理が複雑で，現状では全ての暗号化にこの方式を採用するには，処理時間がかかりすぎるようです。このため，データ交換の都度，一時的な共通鍵を生成して暗号化を行い，復号に必要なその鍵だけを公開鍵暗号方式で暗号化して相手に渡すという，両方式を併用したハイブリッド暗号方式などが使われています。

例　題

(H11 春-SM 問 68)

公開鍵暗号方式の暗号化鍵と復号鍵の関係として，適切なものはどれか。

	暗号化鍵と復号鍵の関係	暗号化鍵	復号鍵
ア	暗号化鍵≠復号鍵	公開	公開
イ	暗号化鍵≠復号鍵	公開	秘密
ウ	暗号化鍵＝復号鍵	秘密	公開
エ	暗号化鍵＝復号鍵	秘密	秘密

解説

公開鍵暗号方式では，暗号化鍵≠復号鍵でしたね。このため，暗号化鍵は公開できます。しかし，復号鍵まで公開してしまうと，誰にでも暗号文が解読されてしまいますから，こちらは秘密にします（正解（イ））。共通鍵暗号方式では，暗号化鍵＝復号鍵でしたね。したがって，(エ) のようにこの鍵を秘密にします。よく考えると，同じ暗号化鍵も復号鍵も同じものであれば，復号鍵だけを公開にする（ウ）ということは不可能です。

解答　イ

演習問題2

(H29 秋-AP 午後問 1)

個人情報保護の強化に関する次の記述を読んで，設問 1，2 に答えよ。

C 社は，服飾・雑貨のインターネット販売業者である。約 50,000 人の顧客が同社の会員制 Web サイトを利用している。会員制 Web サイトには HTTPS を使用してアクセスする必要がある。

顧客が会員制 Web サイトにログインするには会員番号が必要であり，会員登録時に，重複しない 6 桁の数字列をランダムに割り振っている。

C 社には，商品販売部門の他に，服飾類を扱う X 部門，生活雑貨を扱う Y 部門，そして輸入雑貨を扱う Z 部門の三つの商品開発部門がある。

〔C 社の現状〕

C 社の会員制 Web サイトは DMZ 内に設置してあり，セキュリティ専門会社に委託してインターネットからの不正アクセスの検知と対応を行っている。

C 社のネットワーク構成（抜粋）を図 1 に示す。

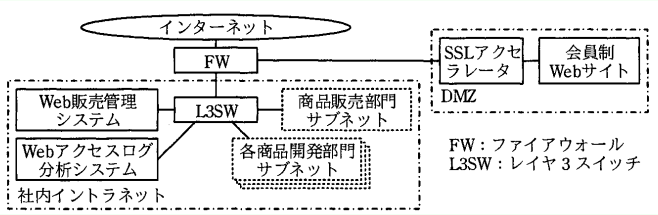

図 1　C 社のネットワーク構成（抜粋）

C 社の会員制 Web サイトで扱う顧客情報や販売情報は，社内イントラネット内の Web 販売管理システムに蓄積されている。Web 販売管理システムの顧客情報データベースには，顧客の会員番号をキーとして，氏名，メールアドレス，電話番号，性別，年齢，住所などが格納されている。また，Web 販売管理システムの販売情報データベースには，顧客の会員番号をキーとして，該当顧客の販売情報が格納されている。二つのデータベースは磁気テープを用いて，月次でフルバックアップを行い，日次で増分バックアップを行っている。C 社の方針で過去 1 年間のバックアップデータを保管している。

解説

個人情報保護の強化をテーマとした問題で，暗号化方式，ハッシュ関数の性質，セキュリティ攻撃の名称などが問われていますが，いずれも基本的な内容ばかりです。特に，ハッシュ関数については，午前試験であまり問われることがないので，この問題を通して理解しておきましょう。また，問題文の読み方や比較的文字数の多い記述の練習をしてください。

［設問1］

〔個人情報保護の強化〕について，(1)～(4)に答えます。

(1) 本文中の**空欄a**に入れる**適切な字句**を**4字以内**で答えるもので，空欄は次の記述中にあります。

> (4) 各商品開発部門の有資格者がWeb販売管理システムにログインした場合は，［a］情報に含まれる会員番号を同じ方法で仮IDに変換して提供する。

「会員番号を同じ方法で仮 ID に変換して提供する」とあるので，**会員番号の仮IDへの変換**に関する記述を探すと，直前の**(3)**に次のように記述されています。

> (3) Webサイト閲覧履歴は，その中に含まれる会員番号を，元に戻せない仮のID（以下，仮IDという）に変換してから，Webアクセスログ分析システムに転送する

つまり，**Webサイト閲覧履歴中の会員番号と同じ方法で，元に戻せない仮のIDに変換する**ということです。

空欄aには**“情報”**と続くので，問題文中から「○○情報」という名称で呼ばれるものを探すと，「顧客情報」，「販売情報」，「加工個人情報」の三つがありますから，それぞれに関連する記述を探します。すると，**図1の下の部分**に，次の記述が見つかります。

> C社の会員制Webサイトで扱う顧客情報や販売情報は，社内イントラネット内のWeb販売管理システムに蓄積されている。Web販売管理システムの顧客情報データベースには，顧客の会員番号をキーとして，氏名，メールアドレス，電話番号，性別，年齢，住所などが格納されている。また，Web販売管理システムの販売情報データベースには，顧客の会員番号をキーとして，該当顧客の販売情報が格納されている。

この記述から，顧客情報と販売情報には，会員番号が含まれることが分かりますが，これだけでは正解は分かりませんから，他の記述も探します。す

ると，〔**個人情報保護の強化**〕の上の段落に，次の記述があります。

> 顧客情報データベースは，各商品開発部門には公開していない。各商品開発部門の有資格者がWebサイト閲覧履歴と販売情報を関連付け，閲覧した商品と売れ筋商品を分析する。その際，性別や地域，年齢などを必要とする場合，システム部門は，顧客情報から必要がない個人情報の箇所をマスクしたデータ（以下，加工個人情報という）を提供している。

まず，顧客情報は**非公開**なので，**対象外**です。続く，販売情報については，Web **閲覧履歴と関連付けて分析に使う**ようなので，**正解の候補**ですね。そして，加工個人情報については，「顧客情報から必要がない個人情報の箇所をマスクしたデータ」ということですが，**マスクとは元の値が分からなくすること**なので，**対象外**と考えてよいでしょう。したがって，空欄aには販売（情報）が入ります。

ONE POINT　「4字以内」ということから，4文字の「加工個人」（情報）に飛びついた人も多かったのではないでしょうか。この試験では，文字数は多めになっていることがほとんどですから，文字数だけで正解を決めないように注意しましょう。

FAQ　正解を効率的に探すにはどうしたらよいでしょうか。

この設問のように，知識ではなく，問題文から読み解く問題は時間がかかります。問題文を効率的に読む練習をするしかないと思います。ただし，実際の試験では緊張などからどうしても見つからないこともありますから，時間の目安を決めて，時間内に見つからなければ後回しにするようにしましょう。ちなみに，私もなかなか正解が決められずに時間がかかりましたが，落ち着いて読み返してみると〔個人情報保護の強化〕の冒頭部分には「システム部門のF部長は，Web販売管理システムのデータベースにある情報や，PCに保存されているWebサイト閲覧履歴や販売情報，加工個人情報について，社内からの不正アクセスや従業員の人的ミスによる漏えいのリスクが高いと考えた」と記述されていて，これがヒントになっていたのかもしれません。

(2)　本文中の**空欄b，c**に入れる**適切な字句**を解答群の中から選び，**記号**で答えます。まず，**空欄b**があるのは，**D課長の報告の冒頭**の次の発言です。

Part 2 Chapter 8

第8章 マネジメント系の問題

学習のポイント

この章は，プロジェクトマネジメントに関すること，ITサービスマネジメントに関すること，システム監査に関することの三つの分野をまとめて扱っています。そして，それぞれの分野の出題範囲は，それぞれ次のようになっています。

プロジェクトマネジメントに関すること（演習問題1～5）
プロジェクト計画・プロジェクト管理（スコープ，工程，品質，予算，人員，調達，リスク，コミュニケーションほか） など

サービスマネジメントに関すること（演習問題6～10）
サービスマネジメントプロセス（サービスレベル管理，サービス継続及び可用性管理，サービスの予算業務及び会計業務，キャパシティ管理，インシデント及びサービス要求管理，問題管理，構成管理，変更管理，リリース及び展開管理ほか），サービスの運用（システム運用管理，仮想環境の運用管理，運用オペレーション，サービスデスクほか） など

システム監査に関すること（演習問題11～15）
IT統制，情報システムや組込みシステムの企画・開発・運用・保守の監査，情報セキュリティ監査，個人情報保護監査，他の監査（会計監査，業務監査ほか）との連携・調整，システム監査の計画・実施・報告，システム監査関連法規 など

マネジメント分野で出題される問題は，前提知識が少なくても問題文を読み進めていけば，解答できる内容となっています。前提知識がある場合には，問題の読解にかける時間を減らすことができますので，その時間を解答を検討する時間に回すことが可能となります。問われている知識は，午前問題と重なる内容が大半ですので，午前問題で蓄えられた知識を午後の演習問題を通じてさらに深めておきましょう。

(1)　プロジェクト計画・プロジェクト管理

パッケージソフトの導入を題材とした問題が頻出されます。ソフトウェア導入基準，発注先選定基準，発注内示書，機能要件，非機能要件，WBS（Work Breakdown Structure）の理解が必要です。

また，ブレーンストーミング，コストパフォーマンスベースライン，コンティンジェンシ，RFP（Request For Proposal;提案依頼書），CSR 調達（企業の社会的責任に基づく調達），グリーン調達（環境負荷を考慮した調達），ステークホルダといったプロジェクト管理用語の理解も前提知識として必要になっています。また，国際的に標準化されている PMBOK（プロジェクトマネジメント知識体系ガイド）や，共通フレーム 2013（SLCP-JCF 2013；Software Life Cycle Process - Japan Common Frame 2013）といった標準規格の枠組みを理解しておく必要もあります。その他のプロジェクトマネジメントとしては，プロジェクト資源マネジメント，プロジェクトコミュニケーションマネジメント，プロジェクトタイムマネジメント，プロジェクトスコープマネジメント，プロジェクトコストマネジメント，プロジェクトリスクマネジメントなどの知識エリアを確認しておきましょう。その他，EVM（アーンドバリューマネジメント），フィット＆ギャップ分析，といった実績評価手法が午後出題のテーマになっています。クラッシングや，ファストトラッキングといったプロジェクトスケジュール短縮のための手法も概要を押さえておくとよいでしょう。

(2)　サービスマネジメントプロセス・サービスの運用

SLA（サービスレベル合意），キャパシティ管理，インシデント管理，問題管理，変更管理，リリース及び展開管理，構成管理，UPS（無停電電源装置）と自家発電設備の違い，ハウジングサービス，QMS(Quality Management System；品質管理システム)，サービス継続及び可用性管理，ソフトウェアのライセンス管理などを把握しておきましょう。また，IVR（Interactive Voice Response;自動音声応答），サービスデスク，CTI(Computer Telephony Integration)，SPOC（Single Point of Contact; 単一窓口）といった用語の理解も必要になります。

(3)　IT 統制，情報・組込みシステムの企画・開発・運用・保守の監査

内部統制，業務要件とシステム要件の突合せ，ID 管理，アクセス権限管理，職務分掌の概要把握が必要になります。

(4) 情報セキュリティ監査，個人情報保護監査

情報セキュリティ監査に関連した内容では，セキュリティポリシとの整合性チェック，ハードディスクスキャン，JIS Q 15001 や ISMS 適合性評価制度，プライバシーマーク制度に準拠した個人情報保護規程の策定や運用などが出題されます。個人情報の取扱い，統計情報利用の際の匿名化についても押さえておく必要があります。

(5) システム監査の計画・実施・報告

システム監査のプロセスには，監査計画の立案から始まり，監査実施，評価，監査報告という流れがあります。システム監査の流れの中で使用される，監査計画，監査証拠，監査証跡，監査調書といった用語の理解が必要になります。使用される監査技法としては，基本的な監査技法（チェックリスト法，突合法・照合法，現地調査法）とコンピュータを利用したシステム監査技法（テストデータ法，ITF 法，スナップショット法，トレーシング法など）があります。また，システム監査を実施する監査人の要件（独立性，適格性）も午後試験では，設問の一部として問われています。

「システム監査基準」及び「システム管理基準」の改訂について

2018 年 4 月 20 日経済産業省から「システム監査基準」と「システム管理基準」の改訂版がリリースされています。
新しく改訂された基準につきましては，次のウェブページよりご確認ください。

・新「システム監査基準」（2018 年 4 月 20 日改訂）
http://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kansa_h30.pdf
・新「システム管理基準」（2018 年 4 月 20 日改訂）
http://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kanri_h30.pdf
・システム監査基準新旧対照表
http://www.meti.go.jp/policy/netsecurity/sys-kansa/h30kaitei_ref2.pdf
・システム管理基準新旧対照表
http://www.meti.go.jp/policy/netsecurity/sys-kansa/h30kaitei_ref3.pdf