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

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なので，復号鍵だけを秘密にする（ウ）ということは不可能です。

解答　イ

演習問題1

(H21秋-AP 午後問9)

公開鍵基盤を用いた社員認証システムに関する次の記述を読んで，設問1～4に答えよ。

販売業を営むX社は，社内業務で利用している電子メールで顧客情報などの個人情報や機密性の高い販売業務に関する情報を安全に取り扱うために，公開鍵基盤を用いた社員認証システム（以下，本システムという）を導入している。本システムを含む社内業務システムの概要を図に示す。

〔本システムの概要〕

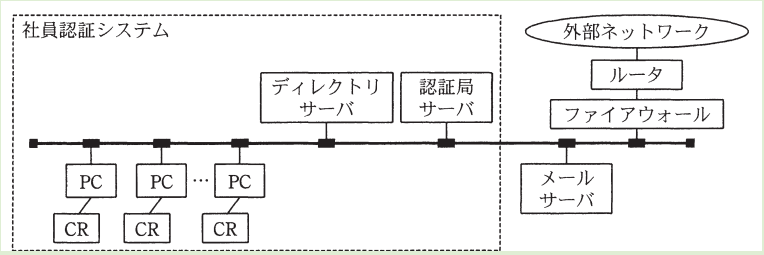
(1) 本システムは，ディレクトリサーバ，認証局サーバ，社員ごとのPC及びIC社員証カード（以下，ICカードという）から構成される。

(2) ディレクトリサーバでは，社員の公開鍵証明書や電子メールアドレスなどの属性情報の登録及び検索が行われる。

(3) 本システムでは，プライベート認証局を使用している。

(4) ICカードには，社員個人の秘密鍵，公開鍵証明書及びPIN（Personal Identification Number）が格納されている。社員が本システムを利用する際には，自分のICカードをPCのICカードリーダに挿入し，ICカードのパスワードであるPINを入力する。

(5) PCには，本システムにおける認証機能や暗号化機能及び電子メールのクライアント機能を提供するソフトウェア（以下，PCサブシステムという）が導入されている。



注 CR：ICカードリーダ

図　社内業務システムの概要

解説

公開鍵暗号方式によるメッセージ認証（送信者認証と改ざんされていないことの確認）については，例題で学習しました。この問題ではテーマとなっている公開鍵基盤について学習しましょう。

［設問1］

〔新規発行〕中の**空欄 a～d** に入れる**適切な字句**を解答群から選びます。同じ空欄が複数の箇所にあるので，それぞれの前後の記述から，解答を確定していきましょう。

空欄 a，b

空欄 a，b のある(1)の記述から，公開鍵暗号方式において，システム管理者が対を生成するのですから，公開鍵と秘密鍵であることは想像できると思います。**空欄 a** が(4)の記述にもあるので，そちらもヒントに考えます。(4)によると空欄 a の内容は新規の IC カードに記録されます。このことについては，**〔本システムの概要〕**(4)に「IC カードには，社員個人の秘密鍵，公開鍵証明書及び PIN（Personal Identification Number）が格納されている」と記述されているので，空欄 a は（キ）社員 A の秘密鍵です。一方の空欄 b は，社員 A の秘密鍵と対で生成されるのですから，（オ）社員 A の公開鍵です。

空欄 c，d

空欄 d のある(3)の記述から，空欄 d はディレクトリサーバに登録されることが分かります。このことについては，**〔本システムの概要〕**(2)に「ディレクトリサーバでは，社員の公開鍵証明書や電子メールアドレスなどの属性情報の登録及び検索が行われる」と記述されているので，空欄 d は（カ）社員 A の公開鍵証明書です。公開鍵証明書とは，個人の公開鍵について認証局がその正当性を証明するものです。認証局は証明のために公開鍵証明書に署名をしますが，その署名は，認証局しかもっていない，認証局の秘密鍵を使って行われます。したがって，空欄 c には（シ）認証局の秘密鍵が入ります。

FAQ　公開鍵証明書はなぜ必要なのですか。

公開鍵暗号方式では，本人（メッセージ）認証のために，送信者の公開鍵による復号を行います。このとき，公開鍵が本人のものではなく，第三者が勝手に公開しているものであったらどうなるでしょうか。認証の前提が崩れてしまいます。つまり，第三者が他人を騙（かた）って公開している公開鍵で本人認証を行う

わけですから，悪意の第三者を本人として認証してしまうことになります。こうしたことがないように，信用のおける機関などが，自らの秘密鍵で署名した公開鍵証明書を発行することで，第三者による公開鍵の公開（配布）ができないようにしているのです。このように公開鍵証明書を活用することで，公開鍵暗号方式による本人認証が安心して行えるようにする仕組みが，この問題のテーマでもある公開鍵基盤（PKI；Public Key Infrastructure）です。

公開鍵基盤は，印鑑登録制度と似ています。印鑑登録制度は，実印のような大切な印鑑を勝手に使われないようにするために，あらかじめ区市町村役場などに印鑑を登録しておき，その印鑑を押印した文書に印鑑登録証明書を付して提出する制度です。このときに重要なのは，登録時の本人確認と，証明書の正当性確認です。登録時の本人確認は，受付担当者が身分証明書などをチェックすることで実現します。また，証明書の正当性確認には，登録機関の印鑑の押印や透かしなど使って実現しています。

公開鍵証明書の場合には，認証局と呼ばれる公的な機関などが証明書を発行することになりますが，証明書の発行を依頼するときには，本人証明となるような書類の提出などが必要となるので，第三者が証明書を発行してもらうことはできません。また，証明書の正当性については，公開鍵暗号方式による認証を利用します。つまり，発行元である認証局しか知らない認証局の秘密鍵で署名して，利用者が認証局の公開鍵を使って，その証明書を認証できるようにしています。

［設問２］

〔電子メールのメッセージの送受信〕《受信側》の処理の流れにある空欄 e ～g について，解答群から選びます。

この部分は，受信者である社員 B が社員 A から送られてきたメッセージを受信するための処理の流れで，空欄の前にある(1)には，「社員 B が IC カードと PIN による認証を受け，PC サブシステムにログインする」と記述されています。

次の手順が**空欄 e** ですが，**《送信側》**(5)によれば，社員 A から送信されたメッセージは，最終的に社員 B の公開鍵によって暗号化されていることが分かります。これに対して，解答群の内容は，**（ア）**社員 A の公開鍵証明書の取得と有効確認，**（イ）**社員 B の秘密鍵による復号，**（ウ）**社員 A の公開鍵によるメッセージ認証の三つです。この三つの内容をヒントに考えると，暗号化して送られてきたメールは，まず，復号してあげないと何もできませんから，**（イ）**が最初，つまり，空欄 e は（イ）ということになります。

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

他の分野と同様に，午後問題の目的は，知識を問うことではなく，技能や能力を問うことですから，各テーマについて，午前問題に出題されるような内容を理解していれば十分です。また，よく出題される内容については，演習問題の中で扱っていますから，正解できることだけを目標とせずに，解説をよく読んで知識を深めてください。なお，ITサービスマネジメントについては，第2章のシステムアーキテクチャ，プロジェクトマネジメントについては，第5章の情報システム開発と関連が深い内容なので，それぞれの分野についても一通り学習しておくとよいでしょう。

演習問題1

(H24 秋-AP 午後問 10)

プロジェクト計画に関する次の記述を読んで，設問 1～3 に答えよ。

文具類の販売を行う Z 社では，販売予算システムを開発することになった。販売予算システムは，予算登録，予算集計，承認ワークフローの三つのサブシステムから構成される。システム部の Y 君が，プロジェクトマネージャに任命され，スケジュールを立案することになった。

〔アクティビティリストとプロジェクトスケジュールネットワーク図の作成〕

プロジェクトでは，販売予算システム全体を対象に基本設計を行った後，各サブシステムの詳細設計を開始する。詳細設計では，サブシステムを構成する全てのプログラムの画面項目や処理内容の詳細仕様を決定し，最後にレビューを行う。詳細設計，プログラム作成・テスト，結合テストは，サブシステムごとに行い，サブシステム同士は同時並行に開発を行うことができる。全てのサブシステムの結合テストが完了すると，システム結合テストを開始する。

Y 君は，必要なアクティビティ，順序と所要期間を，表 1 のアクティビティリストにまとめた。

表 1　アクティビティリスト

記号	サブシステム	アクティビティ	所要期間（日）	先行アクティビティ
A	（システム全体）	基本設計	75	－
B1	予算登録	詳細設計	30	A
B2		プログラム作成・テスト	30	B1
B3		結合テスト	20	B2
C1	予算集計	詳細設計	25	A
C2		プログラム作成・テスト	25	C1
C3		結合テスト	20	C2
D1	承認ワークフロー	詳細設計	15	A
D2		プログラム作成・テスト	15	D1
D3		結合テスト	10	D2
E	（システム全体）	システム結合テスト	30	B3，C3，D3

各サブシステムの作業は，表 2 のサブシステム作業要員リストに基づいて行う。

解説

プロジェクトスケジュールネットワーク図（以下，P・S・N図という）による，プロジェクト計画（日程計画）の問題です。これまでは，アローダイアグラム（PERT図）による出題でしたから，少し戸惑ったかもしれません。この図は，PMBOKにおいて，スケジュール計画のアウトプットとされているもので，午前問題に出題されています。基本的にはPERT図と同じ内容なので，この問題を通して理解しておきましょう。

図1の凡例から分かるように，P・S・N図では，アクティビティを四角で表し，その前後関係を矢印で結んでいきます。また，アクティビティを示す四角には，アクティビティの名称（記号）と，ES（最早開始日），EF（最早終了日），LS（最遅開始日），LF（最遅終了日）を記述します。

ONE POINT　ES, EF, LS, LFは，それぞれ，Earliest Start time, Earliest Finish time, Latest Start time，Latest Finish timeの略称です。

なお，この四つの日付については，PERT図にも記述することがありますから，知っている人も多いと思います。最早のES，EFについては，名前のままなので分かりやすいでしょう。最遅のLS，LFは，プロジェクト全体の作業日数を遅延させないためには，最も遅くともこの日付に始めなくては，終わらなくてはいけないという日付です。

凡例

ES		EF
	X	
LS		LF

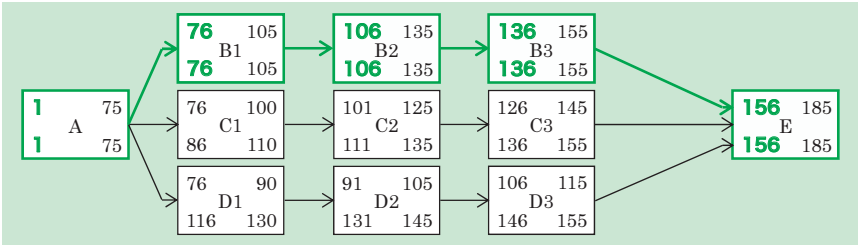
：記号Xのアクティビティ

ES：最早開始日　最も早く作業を始められる日付
EF：最早終了日　最も早く作業が終わる日付
LS：最遅開始日　最も遅く作業を開始してもよい日付
LF：最遅終了日　最も遅く作業が終了してもよい日付
⟶：アクティビティ間の順序関係

［設問1］

クリティカルパスを構成するアクティビティが問われています。クリティカルパスとは，全体スケジュールを遅延させないために遅れてはいけない，つまり，作業日数に余裕がないアクティビティを結んだものでした。P・S・N図では，最早と最遅が記述されていますから，クリティカルパスを容易に把握できます。

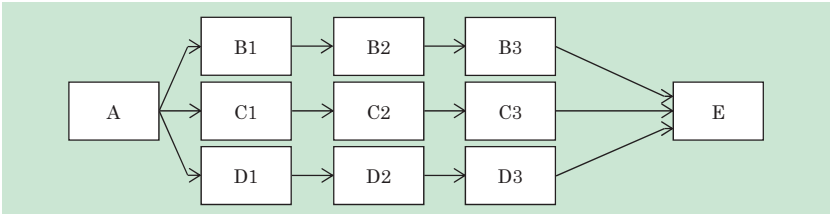
アクティビティの作業日数の余裕は，最早開始日と最遅開始日の差になります。したがって，この二つの日付の差が0（日付が同じ）ということは余裕がないことを示します。**図1**の場合，「A，B1，B2，B3，E」が該当しますから，これが正解です。



FAQ

この図の描き方を教えてください。

まず，アクティビティリストを基に，各アクティビティの前後関係を矢印で表現します。



次に，最早開始日，最早終了日を埋めていきます。最初のアクティビティ（A）の最早開始日を 1 として埋めていきます。次に，最早終了日を埋めますが，開始日にも作業は行われるので，開始日に所要日数の 75 を足した 76 ではなく，1 日少ない 75 であることに注意してください（以降も同じ）。

後続する B1，C1，D1 それぞれの最早開始日に，A の最早終了日の 75 の翌日である 76 と埋め，それぞれ作業日数を加えて最早終了日を埋めます。これを全てのアクティビティについて行い，最早開始日，最早終了日を埋めていきます。なお，E のように複数の先行作業があるときは，最も遅い終了日の翌日になることに注意してください。