目　次

◆学習後のアンケートのお願い

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。

毎年，４月末，10 月末までに弊社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 円分をプレゼントしております。ご当選された方には，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。

ご入力いただきましたメールアドレスは，当選した場合の当選通知，賞品お届けのためのご連絡，賞品の発送のみに利用いたします。

なお，本書のアンケートのご回答期限は 2020 年 10 月末です。

https://questant.jp/q/fegogo20

第３部　知識の応用（テクノロジ系の選択問題）

第４部　知識の応用（マネジメント系・ストラテジ系の選択問題）

第５部　データ構造とアルゴリズム（必須問題）

第６部　演習問題 解答・解説

巻末資料

Part 2　第2章　Chapter 2

情報セキュリティ

出題のポイント

情報セキュリティ分野の問題として，過去には，ネットワークセキュリティ（平成 26 年度秋期），インターネットを利用した受注管理システムのセキュリティ（平成 27 年度春期），ログ管理システム（平成 27 年度秋期），Web サーバに対する不正侵入とその対策（平成 28 年度春期），販売支援システムの情報セキュリティ（平成 28 年度秋期），ファイルの安全な受渡し（平成 29 年度春期），SSH による通信（平成 29 年度秋期），Web サービスを利用するためのパスワードを安全に保存する方法（平成 30 年度春期），情報セキュリティ事故と対策（平成 30 年度秋期），クラウドサービスの利用者認証（平成 31 年度春期）といったテーマが取り上げられています

情報セキュリティの分野は必須問題なので，この分野に弱点を作らないように学習する必要があります。

(1)　アクセス制御

情報セキュリティを担保する上で必要となる，ファイアウォールによるパケットフィルタリング設定や，システムへのユーザアクセス権設定など，設定面での対策方法について学習しましょう。

(2)　暗号化・認証技術

情報セキュリティ技術の根幹となる，暗号化技術や認証技術要素について学習しましょう。

(3)　情報セキュリティマネジメント

情報セキュリティを企業として取り入れ，マネジメントする際に必要となるリスクマネジメント手法や，標準規格などについて学習しましょう。

演習問題　第２部　第２章　問１

販売支援システムの情報セキュリティに関する次の記述を読んで，設問 1〜3 に答えよ。

(H28 秋-FE 午後問 1)

中堅の商社である A 社では，営業員が顧客先で営業活動を行い，自社に戻ってから見積書を作成している。

この度，営業員がタブレット端末（以下，タブレットという）を携帯し，顧客先で要求を聞きながら，タブレットを使って見積書を作成し，その場で顧客に提示できる販売支援システムを構築することにした。

営業員は，タブレットの Web ブラウザからインターネット経由で HTTP over TLS（以下，HTTPS という）によって販売支援システムにアクセスする。このとき，営業員は，社員 ID とパスワードを入力してログインする。

〔販売支援システムの構成〕

(1) 販売支援システムは次のサーバで構成され，A 社のネットワークに設置される。
　① リバースプロキシサーバ（以下，RP サーバという）1 台
　② アプリケーションソフトウェアが稼働する Web サーバ 2 台
　③ 見積書作成に必要なデータを格納するデータベースサーバ（以下，DB サーバという）1 台

(2) Web サーバ 2 台はクラスタリング構成にして，1 台が故障してもサービスが継続できるようにする。

(3) DB サーバへのアクセスの監視は，PC と同じ LAN にある監視サーバで行う。

(4) インターネットから販売支援システムへの通信は，RP サーバを経由して行う。RP サーバは，HTTPS を HTTP に変換し，販売支援システムの他のサーバと，HTTP で通信する。

知識確認問題　必要な知識を確認してみましょう！

問　公開鍵暗号方式の暗号アルゴリズムはどれか。

(H29 春-FE 問 40)

ア　AES　　イ　KCipher-2　　ウ　RSA　　エ　SHA-256

解説

RSA は，アルゴリズムに大きな桁数の素数を掛け合わせた数値から，それを素因数分解して元となった素数を求めることは困難であるという数学的性質を利用した代表的な公開鍵暗号方式です。したがって，（ウ）が正解です。

ア：AES（Advanced Encryption Standard）……DES（Data Encryption Standard）に代わって，2002 年から米国政府の標準暗号として採用された共通鍵暗号方式です。NIST（米国国立標準技術研究所）が公募し，2000 年に選ばれたもので，DES に比べて更に安全性が高くなっています。

イ：KCipher-2……株式会社 KDDI 総合研究所が開発した共通鍵暗号のアルゴリズムです。

エ：SHA-256……SHA-2（Secure Hash Algorithm 2）の一つで，ハッシュ値として 256 ビットの値を出力するハッシュ関数です。SHA-1 のハッシュ値は 160 ビットであり，脆弱性が指摘されていることから，2016 年 12 月末までに SHA-2 へ移行することが推奨されていました。

解答　ウ

問　X さんは，Y さんにインターネットを使って電子メールを送ろうとしている。電子メールの内容を秘密にする必要があるので，公開鍵暗号方式を使って暗号化して送信したい。そのときに使用する鍵はどれか。

(H27 秋-FE 問 38)

ア　X さんの公開鍵　　イ　X さんの秘密鍵
ウ　Y さんの公開鍵　　エ　Y さんの秘密鍵

Part 3　Chapter 3

第3章 データベース

出題のポイント

データベース分野の問題として，過去には，会員情報を管理する関係データベースの設計と運用（平成 25 年度春期），選手情報を管理する関係データベースの設計及び運用（平成 25 年度秋期），書籍を管理する関係データベースの設計及び運用（平成 26 年度秋期），自治会員の情報を管理する関係データベースの設計及び運用（平成 27 年度春期），電子部品の出荷データを管理する関係データベースの運用（平成 27 年度秋期），遊園地の入園者情報を管理する関係データベース（平成 28 年度春期），従業員の通勤情報を管理する関係データベース（平成 28 年度秋期），住民からの問合せに回答するためのデータベース（平成 29 年度春期），会員制通信販売事業者における会員販売データ管理（平成 29 年度秋期），小学生を対象とした，ある子供会の名簿を管理する関係データベース（平成 30 年度春期）などが出題されています。

(1)　正規化と SQL

データベース分野の午後問題のほとんどは，データベースの表定義における正規化や，データ抽出のための SQL を問う問題です。**データを矛盾なく効率的に格納する表形式や，WHERE 句，GROUP BY 句，ORDER BY 句を使った SQL 文，結合や副問合せを使った SQL 文**に慣れておく必要があります。

(2)　DBMS（データベース管理システム）

DBMS がもつ**トランザクション機能，つまり同時実行制御と回復処理のための機能**をテーマとした問題も，平成 23 年度春期（特別試験）や，平成 24 年度春期に出題されました。平成 25 年以降は出題がありませんが，トランザクションが備えるべき ACID 特性，や DBMS の備える排他制御（ロック制御），コミットメント制御を勉強する必要があります。

Part 4　第1章　Chapter 1

マネジメント系

出題のポイント

令和２年度春期試験から午後の試験の問５は，マネジメント系，ストラテジ系のどちらかの分野から１問だけが出題されることになりました。

マネジメント系の問題が，どのようなサイクルで出題されるか分かりませんが，IPA から発表されている項目は次のとおりです。しっかりと確認しておきましょう。

① **プロジェクトマネジメント**
　プロジェクト全体計画（プロジェクト計画及びプロジェクトマネジメント計画），プロジェクトチームのマネジメント，スケジュールの管理，コストの管理，リスクへの対応，リスクの管理，品質管理の遂行，見積手法　など

② **サービスマネジメント**
　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，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，変更管理ほか），サービスの運用（システム運用管理，運用オペレーション，サービスデスク）など

プロジェクトマネジメントでは，プロジェクトの実績管理を題材とした進捗管理，工数見積り，品質管理，コスト管理などがオーソドックスなテーマで出題されやすい内容といえます。午前問題で出題される知識を応用した問題になりますので，基本的な知識は整理しておきましょう。問題文を読んで内容の理解ができれば解答できる設問も多いのですが，短時間で迷わず解答するためにもこれらの知識の整理は重要となります。

サービスマネジメントでは，出題範囲の改訂で，サービスマネジメントの国内規格（JIS）の改正に基づき，この分野に含まれる項目や表記が大きく変更されています。分野構成や表記は見直されていますが，試験で問われる知識・技能の範囲が変わったわけではありません。問題事例を短時間に理解するためにも，これらの項目に関する知識を確実なものにしておきましょう。

Part 5　第3章　Chapter 3

基本アルゴリズム（整列・探索）

出題のポイント

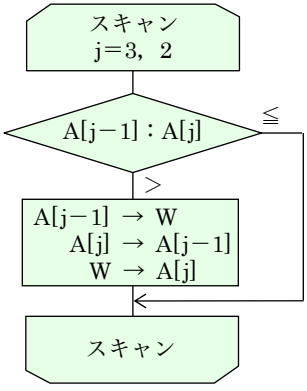
基本アルゴリズムとして，整列（ソート）と探索（サーチ）の代表的なアルゴリズムを学習します。具体的には，交換法と選択法及び挿入法による整列アルゴリズム，逐次探索と２分探索のアルゴリズムです。

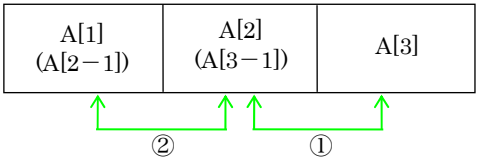
これらのアルゴリズムの考え方については，午前の試験でも出題されているので，既に学習していると思います。ここでは，考え方の説明は簡単にして，その考え方をどのようにアルゴリズムとしてまとめていくかということを中心に解説していきます。そして，ここで解説している論理的な考え方が身につけば，午後の試験のアルゴリズム対策の基礎訓練は終了です。

基本アルゴリズム自体が，午後の試験の出題テーマになることは少ないですが，整列と再帰処理の考え方を応用したマージソートやクイックソートの問題が出題されたことがあり，今後もアレンジした形で出題される可能性があります。

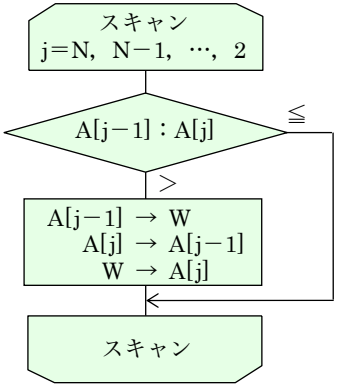
このような応用問題でも整列の考え方を理解していて，トレース（処理の追跡）が落ち着いてできれば，解答を導き出すことができますので，心配する必要はありません。また，整列や探索処理は，一般的なアルゴリズムの中の一部の処理として用いられていることもあるので，しっかり理解しておきましょう。

ここで説明するアルゴリズムの組立て方・考え方は，整列や探索だけに限定したものではありません。今後の学習の基礎となる大切な内容ですから，じっくり解説を読んで，しっかり理解してください。





実際に，スキャンで行うのは１番目～N 番目の比較・交換なので，右側の要素としては，N 番目，N−1 番目，…，２番目というように変わっていきます（最後が１番目でなく，２番目になります）。この内容を流れ図で表すと，繰返しの条件部分が変更されて，次のようになります。



（参考）擬似言語による表現

```
■ j: N, j ≧ 2, -1
   ▲ A[j−1] ＞ A[j]
      ・W ← A[j−1]
      ・A[j−1] ← A[j]
      ・A[j] ← W
■
```

注：擬似言語では処理を繰り返す条件（j≧2）を書きます。

ここまでで，内側の繰返し（スキャン）の部分にめどがたちました。次は，外側の繰返し，つまり，範囲の左端を一つずつ狭めながら繰り返す部分を考えます（このとき，スキャンの部分は中身を隠してまとめ，一つの箱として考えるのがポイントです）。さて，この繰返しでは，区間の左端を変えて範囲を狭めていくのですが，これは，具体的には，1，2，3，…，N−1 というように数字を増やしていくことになります。**最後が N ではなく，N−1 となります**（右端は N なので，左端も N の場合，要素が一つになり比較する対象がありません）。

演習問題　第５部　第５章　問５

次のプログラムの説明及びプログラムを読んで，設問１，２に答えよ。

(H29 春-FE 午後問 8)

副プログラム ShortestPath は，N 個（N＞1）の地点と，地点間を直接結ぶ経路及び距離が与えられたとき，出発地から目的地に至る最短経路とその距離を求めるプログラムである。最短経路とは，ある地点から別の地点へ最短距離で移動する際の経由地を結んだ経路である。副プログラム ShortestPath では，出発地の隣接地点から開始して，目的地に向かって最短距離を順次確定する。ある地点の隣接地点とは，その地点から他の地点を経由せずに直接移動できる地点のことである。

図１は，地点数Ｎが７の経路の例で，経路をグラフで表現したものである。図１において，丸は地点を示し，各地点には０から始まる番号（以下，地点番号という）が順番に割り当てられている。線分は地点間を直接結ぶ経路を示し，線分の上に示す数字はその距離を表す。また，経路上は，双方向に移動できる。

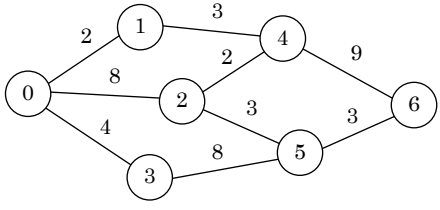


図１　地点数Ｎが７の経路の例

〔プログラムの説明〕

(1) 副プログラム ShortestPath の引数の仕様を，表１に示す。ここで，出発地から目的地までを結ぶ経路は，少なくとも一つ存在するものとする。また，配列の要素番号は，０から始まる。

表１　副プログラム ShortestPath の引数の仕様

引数	データ型	入出力	説明
Distance[][]	整数型	入力	地点間の距離が格納されている２次元配列
nPoint	整数型	入力	地点数
sp	整数型	入力	出発地の地点番号
dp	整数型	入力	目的地の地点番号
sRoute[]	整数型	出力	出発地から目的地までの最短経路上の地点の地点番号を目的地から出発地までの順に設定する１次元配列
sDist	整数型	出力	出発地から目的地までの最短距離

演習問題　第２部　第２章　問８

ファイルの安全な受渡し

(H29 春-FE 午後問 1)

(解答)

［設問１］　エ

［設問２］　a－イ

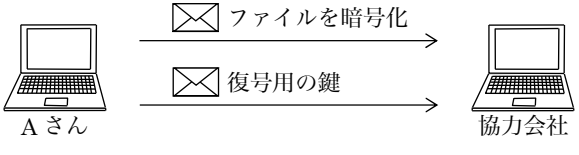
［設問３］　b－ウ，c－ア，d－オ

(解説)

複数の協力会社と協業して取り組むプロジェクトにおいて，各協力会社との間でのファイルの受渡しにおける安全な方式を選定することを題材にした問題です。一見すると暗号化方式等技術的な観点に特化した問題にも見えますが，利用シーンや費用といった観点も含めたトータルでの最適解を求める必要もあり，情報セキュリティマネジメント分野の問題といえます。

［設問１］

A さんが提案したファイル受渡し方法の問題点が焦点になっています。「E さんから“①A さんの方式は安全とはいえない”との指摘を受けた」理由が問われています。まず，A さんの方法を問題文から確認すると，「**ファイルを圧縮し，圧縮したファイルを共通鍵暗号方式で暗号化した上で電子メール（以下，メールという）に添付して送信し，別のメールで復号用の鍵を送付する方式**」とあります。



これは，多くの企業で採用されている，パスワード付 ZIP として添付ファイルを送り，後から別のメールでパスワードを連絡する手法のことと捉えてしまってよいでしょう。と同時に，**ファイルを添付したメールが盗聴できるのであれば，鍵を送付するメールも盗聴できるでしょうし，両者が揃えば，暗号化したファイルが復号できてしまいます。**

したがって，(エ) の「ファイルを添付したメールと，鍵を送付するメールの両方

演習問題　第５部　第５章　問４

Boyer-Moore-Horspool 法を用いた文字列検索

(H27 秋-FE 午後問 8)

(解答)

［設問１］　a－エ，b－カ

［設問２］　c－ア，d－オ，e－キ

［設問３］　f－イ

(解説)

Boyer-Moore-Horspool 法（以下，BM 法）を用いた，高速に文字列検索を行うアルゴリズムの問題です。午後試験のアルゴリズムの問題は非常に多くのテーマで出題されますが，文字列検索の難しいアルゴリズムかもしれないと不安に思った人がいたかもしれません。しかし，必須問題である以上，解かずに済ませるわけにはいきません。基本情報技術者試験のアルゴリズム問題は，**処理内容の説明と必要な考え方は問題文に全て記述されていると信じて（実際にそうです），説明を読み進めて行きましょう。**

最も単純な文字列検索処理は，検索対象の文字列（以下，対象文字列）の先頭から検索文字列と比較していき，不一致があれば，対象文字列の 2 文字目から同じ比較を行い，検索文字列の全てが一致したら検索終了とするものです。対象文字列を Text[]，検索文字列を Pat[]（パターン；pattern から）として，問題の図 1 の例でこの単純な文字列検索処理を行うと，図 A のように 11 回の比較が行われます。

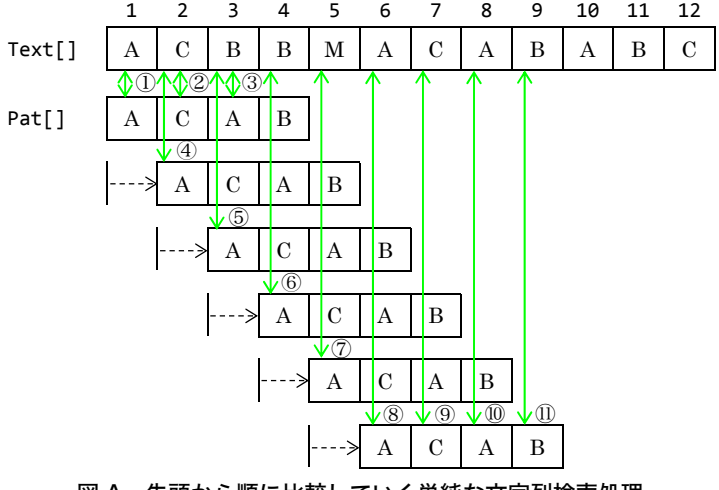


図 A　先頭から順に比較していく単純な文字列検索処理