

情報 (2024年7月公開)

情報-1 次の問1と問2に答えなさい。

問1 図1(i)は高校Aに、図1(ii)は高校Bに、それぞれ通う男子生徒100名の身長(cm)に関するヒストグラムである。身長に関するヒストグラムでは、階級として135 cm から190 cm までの5 cm 刻みの区間を考え、各階級ごとに、その区間内の数値をとるデータの個数が度数として縦軸に示されている。高校Aに通う男子生徒100名の身長の中央値を含む階級は、 cm 以上 cm 未満の区間であり、第1四分位数を含む階級は、 cm 以上 cm 未満の区間である。ここで、四分位数とは、データを小さい順に並べたとき、それらのデータを四等分する位置の値のことをいい、小さい方から順に、第1四分位数、第2四分位数、第3四分位数と呼ぶ。第2四分位数は中央値でもある。同様に、高校Bに通う男子生徒100名の身長の中央値を含む階級は、 cm 以上 cm 未満の区間であり、第3四分位数を含む階級は、 cm 以上 cm 未満の区間である。

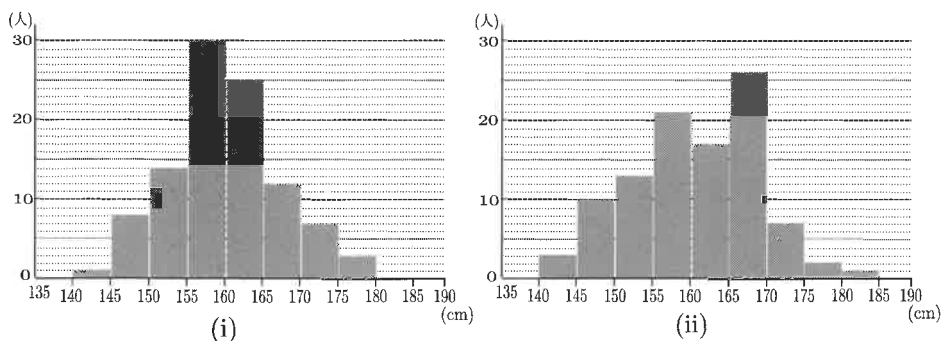


図1

図2は、高校Cに通う男子生徒100名の身長(cm)に関する箱ひげ図である。箱ひげ図では、データの最大値、最小値、第1四分位数、第2四分位数、第3四分位数が図2のように示されている。

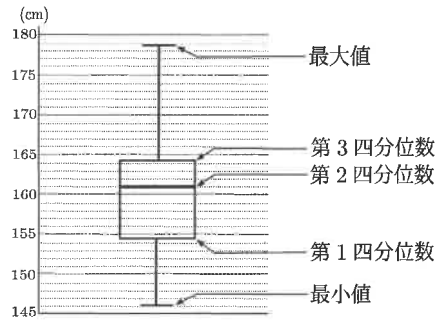


図 2

次の各問に答えなさい。解答紙には答のみを記入しなさい。ただし、男子生徒の身長はすべて異なるものとする。

(1) ~ にあてはまる適切な数値を答えなさい。

(2) 高校 C に通う男子生徒 100 名の身長 (cm) に関するヒストグラムとなり得るものを、図 3 に示すヒストグラム (a), (b), (c), (d) から一つ選び記号で答えなさい。

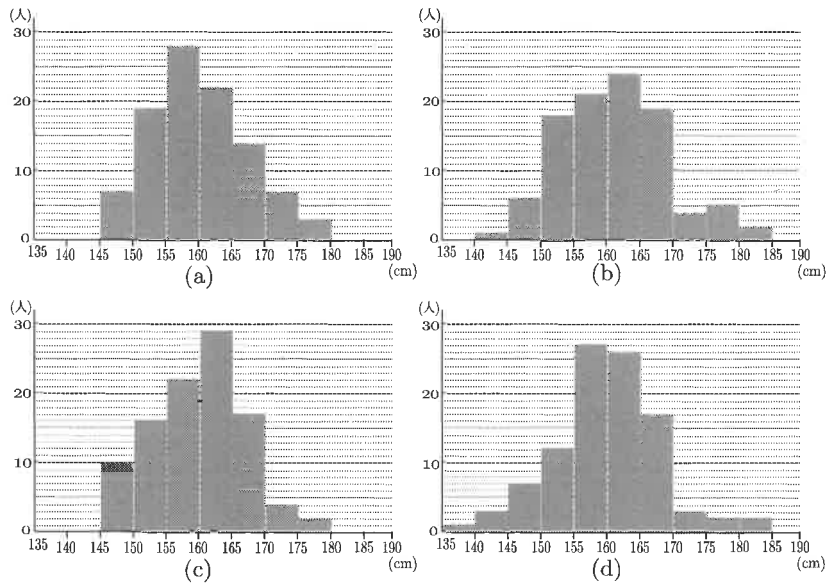


図 3

問 2 インターネットに接続された情報通信機器は、通信回線を用いて情報をやり取りしている。①電話回線を利用して通話をする際には回線交換方式が用いられるが、インターネットに接続する場合はパケット交換方式が用いられる。インターネットは、②アプリケーション層、トランスポート層、インターネット層、ネットワークインタフェース層の4つに階層化されており、それぞれの層では、通信を行うために必要なプロトコル（通信規約）が定められている。WWWは、インターネット上にあるWebページを閲覧するサービスで、③HTTPというプロトコルを用いて、Webサーバに保存されているWebページのデータをブラウザを利用して閲覧できる。

④悪意を持った人間が偽のサイトを構築して、メールなどで利用者をその偽サイトへ誘導し、利用者にログイン名やパスワード、クレジットカードの情報を入力させることで、個人情報を不正入手する方法を という。利用者が入力した情報を盗み取る方法以外にも、パスワードは、実際にはいろいろな方法で漏洩する。よく知られたパスワード解読方法として、可能な組合せを全て試す、総当たり攻撃という方法がある。表1はパスワードにおいて使用する文字ごとに、文字数と総パターン数との関係を示したものである。独立行政法人情報処理推進機構 (IPA) が 2008 年に行った試験によれば、総当たり攻撃によるパスワード解読には表2で示す時間が必要であった。

表 1: 文字数と総パターン数との関係

使用文字\パスワード長	1文字	4文字	6文字	8文字	10文字
数字のみ(0~9)	10	10,000	1,000,000	X	100億
英字(大小区別なし)	26	456,976	約3.1億	Y	約141兆
英字(大小区別なし)と数字	36	1,679,616	約21.8億	Z	約3656兆

表 2: 使用できる文字数と入力桁数によるパスワードの最大解読時間

使用文字\パスワード長	4文字	6文字	8文字	10文字
英字(大小区別なし)	約3秒	約37分	S	約32年

次の各問に答えなさい。解答紙には答のみを記入しなさい。

- (1) 下線部①について、パケット交換方式の利点を回線交換方式と比較して述べなさい。
- (2) 下線部②について、トランスポート層が主に担っている役割を説明しなさい。
- (3) 下線部③について、HTTP ほどの層のプロトコルか書きなさい。
- (4) 下線部④について、アにあてはまる語句を書きなさい。
- (5) 表1について、X, Y, Zとして適当な数字をそれぞれ {} 内から選びなさい。

X {1000万, 1億, 10億}

Y {約80億, 約400億, 約2100億, 約3兆2千億, 約36兆}

Z {約200億, 約3400億, 約2兆8千億, 約22兆, 約320兆}

(6) パスワードの最大解読時間は、総パターン数に比例した時間がかかるとして、表 2 中の S として適当な時間を { } 内から選びなさい。

S {約 6 時間, 約 40 時間, 約 6 日, 約 17 日, 約 200 日, 約 6 年}

(7) 表 2 について、現在のパスワード解読に必要な時間は、2008 年当時と比較してどのようになっていると考えられるか。理由とともに書きなさい。

(8) 総当たり攻撃によるパスワードの解読を防ぐために有効な対策方法を挙げ、その方法がどのように有効であるかを書きなさい。

情報 (2024年7月公開)

情報-2 以下に示すアルゴリズム 1 は 2 以上の正の整数 n が与えられたとき、 n 以下のすべての素数を求めるものである (1 は素数ではない)。アルゴリズム 1 が終了した際、配列 P の各要素は 0 か 1 であり、1 となっている要素の先頭からの位置を表す番号が素数となっている。なお、配列は複数の同じ形式の変数をまとめて 1 つの名前を付けたものであり、1 つひとつの変数を要素という。また、配列の要素の先頭からの位置を表す番号は 1 から数える。

アルゴリズム 1

文 1 n 個の要素を持つ整数の配列 P を用意する
文 2 P の先頭から 1 番目の要素に 0 を、その他の要素に 1 を代入する
文 3 整数の変数 i および変数 j を用意する
文 4 i に 2 を代入する
文 5 i が $n - 1$ 以下の間、以下の文 6~10 を指示に従って繰り返し、
それ以外は文 11 に進む
文 6 j に $i + 1$ を代入する
文 7 j が n 以下の間、以下の文 8~9 を指示に従って繰り返し、
それ以外は文 10 に進む
文 8 もし i が j の約数ならば、 P の先頭から j 番目の要素に
0 を代入する
文 9 j を 1 増やす
文 10 i を 1 増やす
文 11 終了する

次の各問に答えなさい。

問 1 n を 10 としてアルゴリズム 1 を実行し終了したときの、配列 P の各要素の値を示しなさい。以下の図の各四角を配列 P の要素として、そこに各値を書くこと。

先頭からの位置 1 2 3 4 5 6 7 8 9 10
 P

--	--	--	--	--	--	--	--	--	--

問 2 n を 10 としてアルゴリズム 1 を実行し終了するまで、文 8 は何回実行されるか答えなさい。ただし i が j の約数であるかないかに関わらず、実行が文 8 に到達するごとに 1 回と数える。

問 3 アルゴリズム 1 の文 11 を削除し、新たに文 11~17 を追加して、 n 以下の素数の個数を出力するようにしたい。以下の ~ に適切な表現を埋めてアルゴリズムを完成させよ。

アルゴリズム 1 の文 11 以降の変更, 追加

文 11 整数の変数 c および k を用意する

文 12 c に 0 を, k に 1 を代入する

文 13 もし k が n 以下ならば, 以下の文 14~15 を指示に従って繰り返し, それ以外は文 16 に進む

文 14 もし ならば

文 15

文 16 c を出力する

文 17 終了する

(以下余白)