

情報 2015・2017・2018 年度共通問題

解答例&解説(文科向け)

共通問題 3 については問題 A のみ扱っています。2016 年度分は初っ端から現行教科書にないと思われる範囲が出て萎えたのでまだ作成していません。また、解説の教科書参照頁表記は、第 2 版第 3 刷のものになります。

2020 年 2 月 3 日 文科某クラス Mi

H27 (2015) 解答例

共通問題 1

- 1.1 (a)プログラム内蔵 (b)フォンノイマン (c)演算 (d)主記憶 (e)制御 (f)中央処理 (g) CPU
- 1.2 (1)自然言語は、日本語など、人間が特別な訓練なしに日常的に使用している言語であるのに対し、C 言語等のプログラミング言語は、人工的に作られた人工言語の一種で、計算の手順であるプログラムを記述するための種々の約束事をまとめたものである。
- (2)GUI は、Windows のように、捜査情報をアイコンなどを用いて視覚的に表示し、マウス等のポインティング・デバイスも用いて操作するインタフェースだが、CUI は、コマンドプロンプトのように、文字で情報を表示し、全操作をキーボードを用いて行うインタフェースである。
- (3)サーバは、ウェブサーバなど、ネットワーク上にあつて、もっぱら要求に応じてサービスを提供するプログラム、あるいはそれが稼働しているコンピュータを指すが、クライアントは、ウェブブラウザなど、サーバに対してサービスを要求するプログラムを指す。

共通問題 2

- (1)(a) $-\log_2(1/4) = 2$
- (b) $2 \times (1/4) \log_2 4 + 3 \times (1/8) \log_2 8 + 2 \times (1/16) \log_2 16 = 21/8 = 2.625$
- (c)フォルダ M と N の中で必要なデータが M の下のファイルにある確率は、 $(1/4) + (1/4) + (1/8) + (1/8) = 3/4$ だから、それを知る情報量を m とすると、 $m = -\log_2(3/4)$ 。また、同様にして、このときフォルダ P と Q の中でデータが P の下のファイルにあることを知る情報量を p とすると、 $p = -\log_2(2/3)$ 、ファイル A と B の中で A にあることを知る情報量を a とすると、 $a = -\log_2(1/2)$ である。 $m + p + a = -(\log_2 3 - 2) - (1 - \log_2 3) - (-1) = 2$
- m, p, a の和は、(a)で求めた情報量となっている。[これは、情報の加法性による。]
- (d)(ア)A (イ)B (ウ)C (エ)D (オ)E (カ)F (キ)G
- 平均時間 = $(1/3) \times 2 + (1/4) \times 2 + (1/8) \times 3 + (1/8) \times 3 + (1/8) \times 3 + (1/16) \times 4 + (1/16) \times 4 = 21/8$
- (2)(a)(ク)↓R (ケ)↓F (コ)↓G
- (b)フォルダとファイルの構成が木構造になっており、あるファイルまたはフォルダはより上位のフォルダを用いて一意に位置を表現できるという性質。

共通問題 3

問題 A

- (1) 物としての形を持つものとしては、絵画があげられ、形を持たない者としては、特許があげられる。
- (2) 著作権法の改正により、[ソースプログラム、オブジェクトプログラム、OS、アプリケーションプログラムの 4 種の]プログラムが、著作物として保護されるようになった。
- (3) ID や指紋による認証など、情報システムの管理者が、アクセスしてきた人間を、利用権者であるか識別する技術が個人認証技術であり、他人が購入者に成りすまして不正に書籍を読むのを、この技術の導入で防ぐことができる。

公開鍵暗号方式とは、送信者が、受信者が公開している暗号化専用の公開鍵を入手し、それで暗号化した結果を送り、受信者は自分の秘密鍵でデータを復号するという方式のことで、安全性が高い。各人に固有の正しい公開鍵を配布する認証局など、この方式を利用したセキュリティインフラストラクチャのことを、PKI という。購入者との通信に公開鍵暗号方式を利用することで、第三者に登頂により書籍の内容が漏れたり、購入者のパスワードが漏れて不正にアクセスされたりするのを防ぐことができる。

電子署名は、誰がどのデータに署名したかについて第三者の検証を可能とするもので、[公開鍵暗号方式において、秘密鍵で暗号化、公開鍵で復号を行う方法で実現される。] 書籍の購入の際のなりすましを防ぎ、本人確認が可能になる。

- (4) 世に広く利益をもたらした具体例としては、データのバックアップが容易にできるようになったことで、重要な文書や写真が事件・事故で永遠に失われる可能性が低下したことがあげられる。リスクやコストをもたらした具体例としては、盗まれた機密データが容易に複製されて広まることで、情報の漏洩の際の危険性が増大したことがあげられる。これに対しては、データを暗号化して保管するなどの対策がとられている。
- (5) 過去には、活版印刷が聖書を大衆に普及させて宗教革命につながり、テレビの技術が社会主義国家の崩壊の遠因となった。情報技術は場所や時間の制約から人々を解放し、既存の社会を変革したが、過去の技術発展と違い、変化が 1 対 1 レベルのコミュニケーションの経路においても等しく起こっているため、地理的要素に依存した国家や地域共同体のような社会を相対化することとなった。

H27 (2015) 解説

共通問題 1

- 1.1 8 章の文型唯一の必修範囲、8.1～8.1.1 からの出題(pp.180－181)。平易。
- 1.2 (1) p.41 下の注釈と、現在(2019 年度)必修ではないが p.133 の内容と思われる。p.41 下の内容プラス、プログラミング言語の大まかな説明があればいいと思う。
- (2) 9 章 p.223。GUI と CUI についてはこれまでも何度か出題がる。違いを示すだけなので使いやすさとかは要るまい。
- (3) 2 章 p.16、4 章 p.81。これまでも何度か(以下略)。

共通問題 2

- (1)(a) p.65 メッセージの確率 p のとき情報量 $-\log_2 p$
(b) 平均情報量は文字通り平均、つまり情報量 \times 確率の和。 p.66
(c) 「Mにある」というのが決まってから「Pにある」というのを知っているので、Pにある確率は、P,Qのみ考えたときのものとなる。よって、 $(1/4)+(1/4)$ と $(1/8)+(1/8)$ を、和が1になるよう比で上手く処理して $2/3$ と $1/3$ 。AとBも同じ。情報の加法性への言及はいらなと思うが、無いとどうも作業ゲー感が...
(d) 要は、開く(=データがある)確率の高いものほど、短時間で開ければよい。ア、イは 2s、ウ、エ、オは 3s、カ、キは 4s で開けるので、順に A~G を割り当てると丁度いい。綺麗すぎて何か不安になるけども。
- (2)(a) 順番に辿ってゆく。ただの作業。
(b) p.170,(p.178)。木構造なので親は必ず 1 つ、という性質を説明すればよい(1 つの子に対し親が複数あると、「↑X」と書く必要が生じる)。教科書の言葉を使うと、解答例のようになる。

共通問題 3

問題 A

- (1) 本は果たして形を持つと言えるのか...? とか考えずに書いていいはず。ただ、絵画や建築のほうが安全ではある。形を持たないものは音楽などでもいいはずだが、CD はどうなのかと言われると...。それを言うの特許もあやしい。 pp.252-3。
(2) p.253 の(b)。実際に行われた調整としてはプログラムの権利のほうが書きやすい。
(3) 懇切丁寧に説明しているがもう少し簡単でよいはず。 p.259。ただ公開鍵はしっかり説明すべきだろう。PKI と電子署名の細かいシステムを書こうとすると沼にはまる。
(4) 著作権以外と言われると難しい。有識者求む。
(5) pp.247-249。「対比」なので違いも述べる。

H28 (2017) 解答例

共通問題 1

- 問 1-1 (1A)アナログ (1B)デジタル (2B)アナログ (2B)デジタル (3A)アナログ
(3B)デジタル
問 1-2 (4)文字 (5)キーボード (6)ポインティング (7)デスクトップ
問 1-3 (1) $-\log_2(3/4) \cong 0.42$
(2) $-(3/4)\log_2(3/4) - (1/4)\log_2(1/4) \cong 0.815 \cong 0.82$
(3) $-\log_2((1/2)\times(3/4) + (1/2)\times(1/4)) = -\log_2(1/2) = 1.00$

共通問題 2

問 2-1 (1) 8 枚

(2) 罫線を考慮しないとき、毎回の紙片数が最多となるようにするには、毎回すべての紙片を重ね、半分に切ればよい。このとき k 回切ると 2^k 個の紙片ができる。ここで $2^m 2^n = 2^k$ となるような k は、 m 、 n が 0 以上の整数ならば存在するから、先述の切り方で $2^m 2^n$ 個に分割できる。よって、先述の切り方で $m+n$ 回切ればよい。

(3) (2)より、 $m+n$ 回である。

問 2-2

```
if  ${}^8n < 0$  then
     $n \leftarrow \underline{{}^9-n}$ 
endif
 $p \leftarrow 1$ 
while  ${}^{10}n > 0$  do
     $p \leftarrow p \times (-1)$ 
     $n \leftarrow n - 1$ 
done
return  $p$ 
```

<説明> 一般に、 n が偶数のとき $(-1)^{|n|} = 1$ 、奇数のとき $(-1)^{|n|} = -1$ となるのをを用いる。そこで、扱いやすいよう、与えられた数の絶対値をとる。以下、説明のため n の絶対値を m とする。次に、 m が 0 になるまで m から 1 ずつ引いていく操作を行うと、その回数は m 回となる。したがって、 p の初期値を 1 として、 p に $p \times (-1)$ を代入する操作を、先述の操作と同時に行うと、操作終了後の p は $p \times (-1)^m$ となるから、 n が偶数のとき解 p は 1、奇数のとき解 p は -1 となる。

共通問題 3

問題 A

問 A-1

- (1) 機密性とは、認可されたもののみ、情報にアクセスできるようにすることである。
完全性とは、情報が正確かつ完全であることである。
使用可能性とは、必要なときに必要な情報資源にアクセスできることである。
- (2) ①他人のアカウントやパスワードを無断で使用する、あるいはセキュリティほ一つを利用して侵入する、といった不正アクセス行為を禁止している。
②他人のアカウントおよびパスワードを無断で第三者に提供するという、不正アクセスを助長する行為を禁止している。
③情報システムの管理者が不正アクセス行為を防御する措置を講じるよう努めること[、及びこの防御措置に対する都道府県公安委員会による援助]について定めている。
[④不正アクセス禁止法の違反者に対する罰則を定めている。]
- (3) 機密性と関係する。不正アクセス禁止法では、不正なアクセス行為、つまり認可されていないものが情報にアクセスすることを禁じ、情報システムの管理者に、不正アクセス行為への対策を求めて

いるため、情報の機密性の向上を促進する。

問 A-2

- (1) 「地域の権力構造をひっくり返す」とは、地域内部でなら家柄などで事件を揉み消せるほどの権力を持っていた者や組織が、インターネットにより事件が全国的なものとなることで相対化され、従来の弱者が全国に味方されることで力を以て、従来の地域内部での力関係が大きく変わってしまうという意味である。この事件では、匿名性が人々に不可視性の感覚を与え、実名でなら批判などを恐れて行わないかもしれない、黒塗り部分の解析結果の発信や、激しい言葉での議論、及びそれに伴うネット炎上を引き起こしたことである。
- (2) まず、グローバルな多対多の通信射程により、動画は瞬時に、世界中から簡単に閲覧可能になり、事件が広く知られることにつながった。さらに複製可能性により、誰でも容易に動画をコピーして他の SNS やウェブサイトに掲載でき、動画の視聴者数の拡大が起こるとともに、ユニテッド工区による動画削除などの事件の収拾・隠蔽も困難にした。

H29 (2017) 解説

共通問題 1

問 1-1 ごく平易です。「デジタル」を「デジタル」と間違えるのを狙ったんですかね。

問 1-2 1回でも教科書を読んでいけばたぶんいけます。9章。

問 1-3 (1) p.65。

(2) p.66。(1)(2)は先・後がわかっているので、要は「Aさんの勝つ確率は $3/4$ 、Bさんの勝つ確率は $1/4$ 」と読みかえて構いません。

(3) 「A先勝」、「A先負」、「A後勝」、「A後負」。Aさん視点でこの4パターンがあり、それぞれの確率は $(1/2) \times (3/4)$ 、 $(1/2) \times (1/4)$ 、 $(1/2) \times (1/4)$ 、 $(1/2) \times (3/4)$ です。

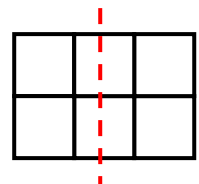
よって、Aさんの勝つ確率は「A先勝」+「A後勝」で、 $1/2$ 。

共通問題 2

問 2-1 (1) 情報というよりは数学の問題。(2)で述べているように、毎回すべて重ねて切るのが最多です。

「切る」という動作は「枚数を2倍にする」ということと同義なので、できるだけ多くの紙をまとめて2倍にしたほうが良い、ということです。

(2) 説明が下手ですが、要は、 $2m \times 2n$ なら罫線に沿って先述の延々2等分する方法ができるという話です。そうでないマス区切りの場合、途中で2分割できなくなるので注意(右図)。



(3) (2)の答えで述べたとおりです。例えば4マス= $2^1 \times 2^1$ なら2回。

問 2-2 解答例を参照。絶対値をとるのに気付けるかがポイント。

「アルゴリズムを説明」は、どこまで何をどう説明すればいいのか不明。有識者求む。

共通問題 3

問題 A

問 A-1 (1) p.258 そのまんまです。各 1 行なので。

(2) p.258 そのまんまです。教科書では①、②まとめて 1 文ですが、内容的に分けても良いと思います。④は短いですが大事なので、①～④どれを選んでも良いと思います。...暗記ゲーです。

(3) 完全性・使用可能性と絡ませるのも不可能ではないでしょうが、教 p.258 で「機密性の管理に関しては」と明言してあるので、そうするのが無難です。というかこれが一番書きやすい。

問 A-2 (1) 自信がありません。助けて。後半は pp.268-9 のアレンジでどうにかなります。なお、大津の事件では、加害者が名家の子だったとか何とかいう話がありますが、それは教科書には無いので、曖昧にぼかしても可だと思います。

(2) 常識の範囲で書けばいいでしょう。pp.268-9。

H30 (2018) 解答例

共通問題 1

問 1-1 (A)クライアント (B)サーバ (C)URL (D)プロトコル (E)Cookie (F)防火壁

問 1-2 (ア)n (イ)log(n) (ウ)n (エ)n³

共通問題 2

問 2-1 (1) 平均情報量 = $-P_A \log_2 P_A - P_B \log_2 P_B - P_C \log_2 P_C - P_D \log_2 P_D$

(2) 購入者 X: $-(4/8) \log_2(4/8) - (2/8) \log_2(2/8) - (1/8) \log_2(1/8) - (1/8) \log_2(1/8)$
 $= 7/4 = 1.75$

購入者 Y: $-(4/16) \log_2(4/16) - (4/16) \log_2(4/16) - (4/16) \log_2(4/16)$
 $- (4/16) \log_2(4/16) = 2$

(3) 一般に、どの事象が起こるか予測がつきにくいほど平均情報量は大きくなるので、この場合購入ブランドの平均情報量が大きいほうが、次にどのブランドを買うか予測しづらい、つまりどのブランドも偏りなく買っているバラエティシーカだと考えられる。よって、購入者 Y をバラエティシーカとみなすのが適当である。

問 2-2 (1) “0”から“9”までの 10 種類の記号だけを使い、どれか 1 つの記号が必ず各桁に対応しているため、2 つの数の大小関係がひとめで測定でき、位取り記数法や筆算が可能である点。

(2) ア)50 イ)3061 ウ)604 エ)1496

共通問題 3

問題 A

問 A-1 (1) ウェブくもの巢のように人々を結びつけるというのは、階層的でないがゆえに「人民が権力を所有する」という民主主義の定義に合致する。

(2) 情報は力であるという考えに基づけば、インターネットは、多数者に情報という力を与える

ことになる。これも「人民が権力を所有する」という民主主義の定義に合致する。

- (3) 従来存在していた、巨大店舗や検閲機構といった機構による、団結に対する障壁を打ち壊すことで、弱者に力を与え、弱者だった人も含めた人民が等しく権力を所有する、新しい秩序を作る力を持つ。

問 A-2

- (1) インターネットはその匿名性や、対面せずに書き込みが行える性質から、電子会議室での荒らしのように、従来の対面での会議では起こりづらかった、話し合いや意見表明を妨害して民主主義のプロセスの邪魔をするような行為を促進する。
- (2) インターネットは匿名性ゆえに、なりすましが容易に行える。これは他者の権利を不正に利用し、一部の個人がなりすまして複数回投票するなどの減少につながり、人民が権力を所有するという民主主義の促進とは逆行する。

H30 (2018) 解説

共通問題 1

問 1-1 教 pp.80-82, p.92。読んでなくてもネット知識がちょっとあれば選べます。

問 1-2 教科書の「オーダー」の記述が不十分なのでちょっと難問。私の脳内整理もかねてゆっくり解説します。pp.118-121。要は、「何回計算するのか」がポイントです。

(ア) 0 から 1 ずつ足して n までですから、n 回です。よって、n。

(イ) n を 2 で割り続けて 2 以下になるまでですから、回数を j 回とすると、 $n \times (1/2)^k \leq 2$ となるような最小の k が j です。

両辺の対数をとって $\log_2 n + \log_2 (1/2)^k \leq \log_2 2$

$$\log_2 n - k \leq 1$$

$$k \geq \log_2 n - 1$$

よって、 $k = \log_2 n - 1$ です。

計算量のオーダーでは、定数部分は基本無視し(p.120 中盤)、対数の底も結局定数倍の差に収まるので考慮しないため(p.119, 9 行目)、オーダーは $\log(n)$ になります。

なぜ定数無視するのかと言えば、n に **5000%** とか大きな値を入れたとき、底や定数はささいなもので、「 $\log(n)$ に比例」の部分のみ考えれば済むからです。

(ウ) 突然の b 登場ですが、慌てず計算回数を考えましょう。まず a は 0 から n までなので n 回です。そして、b も実は while(a<n)の中の計算なので、b=n の段階で a=n となって計算停止です。n+1000 まで行くことはありません。よって、合計で 2n 回ですが、係数はどうでもいいのでこれも n です。

(エ) c と d まで出てきました。というか a はどこ行ったんですかね。ともあれ b は、 $n^2 + j \geq n^3$ となる最小の j で、 $n^3 - n^2$ 回。d は $1000 - 2k \leq 5$ となる最小の k で 498 ですが、定数なので心底どうでもいいです。忘れましょう。

ということでオーダーは $n^3 - n^2 \dots$ ではありません。

p.120 の表からも分かるように、 n^3 は n^2 よりも非常に増加ペースが速い(n=1000 万のとき、

n^3 は3万年、 n^2 は27時間)ので、 n^2 はもはやゴミみたいなものです。よって、 n^3 だけに注目すればいいことになります。実質(n が大きければ)「3乗に比例する」と言っているという感じなわけですね。

...というのが教科書には明言されていないからか、選択肢では優しいことに「 n^3-n^2 」が含まれていません。安心して n^3 を選べます。

共通問題 2

問 2-1 (1) いつもの。pp.66-67。

(2) 問題文に、「購入した割合とその購入確率が等しい」とあるので、例えば計 8 本中 A を 1 本買っていけば、その人は $1/8$ で A を買うと見做していいことになります。それがわかれば作業です。計算もそれほど難しくありません。

(3) 解答例の通りです。p.67。この書き方で良いかは自身が無いですが、平均情報量の性質の利用は必須でしょう。

問 2-2 (1) 2014 年度共通問題 1 の 1-3 からほぼそのまま流用です。流石に露骨すぎませんか。

(2) 表から、 $D=500$ 、 $L=50$ 、 $M=1000$ 、 $C=100$ とわかります。後は足し算引き算です。

ア)50 イ)MMM+L+XI ウ)D+C+IV

エ)はちょっと注意です。IV(=4)などからわかるように、数の大きさが(小)→(大)と逆転して並んでいるときは、(大)引く(小)を示すと推察されます。

$$\begin{array}{ccccccc} M & C & D & X & C & & VI \\ 1000 & 100 & 500 & 10 & 100 & & 6 \end{array}$$

四角で囲んだのが該当箇所。よって、 $1000+(500-100)+(100-10)+5+1$ で 1496 です。この例でわかるかそんなん！という感じですが、並びがおかしいのに注目すべきだということでしょう、きっと。

共通問題 3

問題 A

解答用紙が無いので、(1)~(3)を分けて述べるのか、1つの答えにまとめるのかわかりません。読みやすさ重視で分けましたが、まとめる場合も単純につながれば済むと思います。

問 A-1 pp.264-265。こんなの暗記しないと無理です。とはいえ、覚えてなくても何かそれっぽく書けば点は貰えるのだと思います。(1)はあくまで「多対多」なので、p.264 中盤の手段云々はなくてもいいかと。(3)は教科書を写すとあまりにそのままなので、定義に絡めてアレンジしました。

問 A-2 p.265。教科書には無いですが、考えれば何か欠けると思われます。民主主義と絡めるのがやや力業。

(1)(2)ともに匿名性の関連なので、やはりまとめて書くものなのかもしれません。