2017年度

慶應義塾大学入学試験問題

環境情報学部

数学または情報

注意事項1

1. 試験開始の合図があるまで，この問題冊子を開かないでください．
2. 問題冊子は全部で 28 ページです．
   - 数学の問題 I〜VI は 3 ページから 11 ページです．
   - 情報の問題 I〜V は 12 ページから 27 ページです．

   試験開始の合図とともにすべてのページが揃っているか確認してください．ページの欠落・重複があった場合には，直ちに監督者に申し出てください．
3. 問題冊子の 2 ページに「注意事項 2」があります．試験開始後必ず読んでください．
4. 数学・情報のいずれか 1 つを選択し，解答用紙の選択科目名の欄に科目名を記入し，選択科目マーク欄にマークしてください．
5. 問題冊子は，試験終了後必ず持ち帰ってください．
6. 受験番号と氏名は，解答用紙の所定の欄に必ず記入してください．
7. 解答用紙の「注意事項」を必ず読んでください．

環

注 意 事 項 2

問題冊子に数字の入った $\boxed{}$ があります．それらの数字は解答用紙の解答欄の番号を表しています．対応する番号の解答欄の 0 から 9 までの数字または − (マイナスの符号) をマークしてください．

分数および分数式は約分した形で解答してください．ルート記号の中は平方因子を含まない形で解答してください．マイナスの符号は分母には使えません． $\boxed{}$ が 2 個以上つながったとき，マイナスの符号および 0 の使い方は，つぎの例のようにしてください．

例 $8 \longrightarrow \boxed{0}\boxed{8}$

$-3 \longrightarrow \boxed{-}\boxed{3}$

$1.4 \longrightarrow \boxed{0}\boxed{1}.\boxed{4}\boxed{0}$

$-\dfrac{3}{9} \longrightarrow -\dfrac{1}{3} \longrightarrow \dfrac{\boxed{-}\boxed{1}}{\boxed{0}\boxed{3}}$

$-\sqrt{24} \longrightarrow \boxed{-}\boxed{2}\sqrt{\boxed{0}\boxed{6}}$

$-a^2+6a-5 \longrightarrow \boxed{-}\boxed{1}\,a^2+\boxed{0}\boxed{6}\,a+\boxed{-}\boxed{5}$

$\dfrac{4a}{-2+2a} \longrightarrow \dfrac{-2a}{1-a} \longrightarrow \dfrac{\boxed{0}\boxed{0}+\boxed{-}\boxed{2}\,a}{1-\boxed{0}\boxed{1}\,a}$

情報－Ⅰ

以下、法制度に関しては、日本のものについて考えるものとする。

(ア) 次の文章を読み、空欄にあてはまる**正しい**ものを下の選択肢から１つ選び、その番号をマークしなさい。

[(1)] は、あらかじめウェブサイトにスクリプト（プログラム）を仕掛けておき、このサイトを閲覧したパソコンに当該スクリプトを実行させて、閲覧者が意図しない動作を強制的に行わせるものである。当該サイトを閲覧したパソコンから、別のサイトでネットショッピングを行わせたり、SNS や掲示板に書き込みを行わせるなどの動作をさせることが可能である。(出典：羽室英太郎、國浦淳編著『デジタル・フォレンジック概論』(東京法令出版、平成 27 年）P250、一部改変)

(1) ドライブ・バイ・ダウンロード攻撃

(2) 標的型メール攻撃

(3) クロスサイト・リクエスト・フォージェリ（CSRF）攻撃

(4) DNS 水責め攻撃

(5) フェイク・スクリプト攻撃

(イ) 次の文章を読み、空欄にあてはまる**正しい**ものを下の選択肢から１つ選び、その番号をマークしなさい。

[(2)] は、DNS サービスを提供しているサーバ（DNS サーバ）に偽の情報を覚えこませる攻撃手法である。攻撃が成功すると、DNS サーバは覚えた偽の情報を提供してしまうことになる。このため、ユーザは正しいホスト名の Web サーバに接続しているつもりでも、提供された偽の情報により、攻撃者が罠をはった Web サーバに誘導されてしまうことになる。(出典: IPA ウェブサイト)

(1) フィッシング　(2) プロキシング　(3) DNS キャッシュポイズニング

(4) スキミング　(5) リバース・エンジニアリング

(ウ) 企業に対するサイバー攻撃に関し、**誤っている**ものを下の選択肢から１つ選び、その番号を [(3)] にマークしなさい。

(1) 企業からの情報流出は、技術的に防御システムを破るサイバー攻撃のみならず、人的なミスを起こさせることを狙うソーシャル・エンジニアリングの手法によっても発生する可能性がある。

(2) 企業からの情報流出においては、標的型メールを送付して対象組織のコンピュータにマルウェアを感染させる手法のほか、対象組織の構成員が良く閲覧するウェブサイトを改ざんし、当該ウェブサイトを閲覧することによってマルウェアに感染させる手法も存在する。

(3) 民間企業へのサイバー攻撃によって営業秘密を窃取する行為については、不正競争防止法によって、罰則をもって禁止されている。

(4) 民間企業へのサイバー攻撃によって情報流出が発生した場合、その企業が損害賠償責任を負う可能性があるが、セキュリティシステムを提供していた企業については、損害賠償責任を負う可能性はない。

(5) 民間企業へのサイバー攻撃が、ある特定国に存在するIPアドレスから行われたことが判明した場合であっても、必ずしもその国の者が攻撃してきたとは断定できない。

(エ) 著作権に関し、**正しい**ものを下の選択肢から1つ選び、その番号を $\boxed{\scriptstyle (4)}$ にマークしなさい。

(1) 著作権の保護期間は、原則として、著作者の生存年間およびその死後70年間とされている。

(2) 著作権で保護された音楽や映像を、ファイル交換ソフトを用いて自分で楽しむためにダウンロード（複製）した場合には、私的利用に該当するため、違法とはならない。

(3) 著作権のある著作物か否かを識別することは一般に難しいため、著作物には、外見上コピーライトを意味する表示をしておかない限り、著作権があるものとして保護されないこととされている。

(4) 既存のプログラムを解析し、アルゴリズムを抽出した上で、当該アルゴリズムを用いて別のプログラムを開発したとしても、アルゴリズムが同一である以上、「別のプログラム」の開発者に著作権は発生しない。

(5) ゲームソフトは著作権物であり頒布権も発生するが、一度新品として販売してしまえばその頒布権は消尽するため、中古ソフトの販売は自由におこなうことができるとするのが、日本の判例の立場である。

(オ) インターネット上の犯罪被害等に関し、**正しい**ものを下の選択肢から1つ選び、その番号を $\boxed{\scriptstyle (5)}$ にマークしなさい。

(1) インターネットバンキングにおいて、第2暗証番号をすべて入力するように求められた場合、本人確認のためにおこなわれているものなので、指示どおりに入力すべきである。

(2) 無線LANのアクセスポイントを利用してインターネットに接続する場合、「WEPで保護」と表示されているアクセスポイントの方が、「WPAで保護」と表示されているアクセスポイントよりもセキュリティ強度が強いので、どちらのアクセスポイントにもアクセスできる場合は、「WEPで保護」のアクセスポイントに接続する方が望ましい。

(3) インターネットショッピングを行う場合、既存のショッピングサイトによく似た偽サイトに誘導される危険があるため、サイトの画面だけでなく、URLが正規のものであるか否かにも注意を払うことが望ましい。

(4) スマートフォンにおいてアプリをダウンロードする場合、いわゆる「公式マーケット」から入手すれば、詐欺や個人情報窃取の被害にあう危険はない。

(5) アダルトサイトにアクセスしてしまっただけで、会員登録が完了して登録料を請求する旨の表示がなされた場合であっても、アクセスした本人に責任があるため、請求された登録料をいったん支払う必要がある。

(カ) 個人情報に関し、**正しい**ものを下の選択肢から1つ選び、その番号を (6) にマークしなさい。

(1) 過去の犯罪歴等の情報がインターネット上の検索によって明らかになることがないよう、検索エンジンによる検索結果から関連情報を削除すべきであるといういわゆる「忘れられる権利」は、我が国においても、最高裁判所の判例により、個人の権利として確立している。

(2) 顔認識データについては、個人の氏名、生年月日、住所等ではないため、個人情報保護法にいう個人情報には含まれておらず、議論はあるものの、これを含めるという法改正も行われていない。

(3) 自分自身のマイナンバーの取扱いは各人の自由であり、氏名や住所をインターネット上で公開することが自由であるのと同様、マイナンバーをインターネット上で公開しても、法律に触れる可能性はない。

(4) 企業等からの個人情報の流出事案が発生しているが、企業側は不正アクセス行為等の被害者であるため、損害賠償責任を負うことはない。

(5) 5,000人分以下の個人情報を取り扱う事業者は、個人情報保護法の適用対象外であったが、最近の情報通信技術の進展など環境が変化したことから、平成27年の個人情報保護法の改正により、同法の適用対象とされることとなった。

(キ) ドメイン名やDNSに関し、下の選択肢から**正しい**ものを1つ選び、その番号を (7) にマークし

なさい。

(1) ドメイン名は、商標登録と同様、法律により保護されており、特許庁が登録情報を管理している。

(2) 自由でフラットなインターネット空間においては、DNS サーバ相互間にも階層的な構造は存在していない。

(3) 日本においては、例えば他の事業者の商号と同一のドメイン名を、不正に利益を得る目的で用いるなど、ドメイン名の不正な利用について規制する法律は存在しない。

(4) 本来、組織内からの問い合わせを処理するための DNS サーバが、設定ミス等により、外部からの問い合わせにも応答する設定になっている場合、この DNS サーバを「オープンリゾルバ」という。

(ク) スマートフォン等のセキュリティに関し、**誤っている**ものを下の選択肢から１つ選び、その番号を $\boxed{(8)}$ にマークしなさい。

(1) スマートフォンで写真を撮影する場合、GPS 機能を利用して撮影場所の緯度経度が記録される機能があるので、その機能をオフにしておけば、自宅や学校を他人に特定される危険は減少するが、仮にオフにしていたとしても、撮影した画像を画像検索にかけることにより、背景などから、撮影場所を特定される危険は残る。

(2) スマートフォンでゲームアプリ等をダウンロードする場合、利用規約において、スマートフォン内のアドレス帳へのアクセスを認めるようなものについては、個人情報を窃取される危険があるので注意が必要である。

(3) スマートフォンがある種のマルウェアに感染した場合、そのスマートフォンがカメラや盗聴器として機能してしまい、私生活をのぞき見される危険があり、実際に、過去の交際相手のスマートフォンにそのようなマルウェアを感染させた事案も発生している。

(4) 一般に、オンラインゲームではアイテム等の課金をめぐるトラブルが起こりやすいが、テレビ CM 等で「無料」とうたっているゲームの場合は、消費者庁による厳格な広告規制をクリアしているので、そのようなトラブルが起きることはない。

(5) スマートフォンやゲーム機において端末同士が、短距離で自動的に通信を行ういわゆる「すれ違い通信」が可能となる場合があるが、特に未成年の場合、見知らぬ者とのコミュニケーションからトラブルに発展する危険がある。

情報－Ⅱ

(ア) 文字と2進数 (2進法で表された数) の対応付け (符号化) について述べた次の文章の空欄に入るもっとも適切な数字をマークしなさい。

A、B、C、D、Eの5つの文字を2進数に変換して、通信や保存に使うことを考える。たとえば、次のような方式で変換する。

A → 00、B → 01、C → 10、D → 110、E → 111

この方式を用いると、ADCは、0011010という7ビットに変換され、この7ビットから元のADCを一意に復元できる。この場合、元の文字列中の各文字の出現割合によって、変換後の2進数の元の文字1文字あたりの期待されるビット数は変化する。たとえば、A、B、C、D、Eの出現割合が、それぞれ等しかった場合は、出現割合を確率とみてビット数の期待値を計算すれば、ビット数の期待値は2.4ビットになる。

A、B、C、D、Eの出現確率が、それぞれ、

$$0.45, 0.25, 0.16, 0.09, 0.05 \qquad (1)$$

だった場合、変換後の1文字あたりのビット数の期待値は、(9).(10)(11)ビットになる。

A、B、C、D、Eの出現確率が、上と異なり、それぞれ、

$$0.05, 0.09, 0.16, 0.25, 0.45 \qquad (2)$$

だった場合、変換後の1文字あたりのビット数の期待値は、(12).(13)(14)ビットになり、効率が悪くなる。つまり、ある出現確率が与えられた場合、出現確率の高い文字に短い符号を割り当て、低い文字に長い符号を割り当てたほうが、期待されるビット数が小さくなることがわかる。

また、この出現確率(1)に対して、変換後の1文字あたりのビット数を、(9).(10)(11)ビットよりも小さくすることが可能で、もっとも効率のよい2進数への割り当てを用いた場合、(15).(16)(17)ビットになる。

このような符号を作るためのひとつの考え方は、0で始まるすべての符号と1で始まるすべての符号の出現確率をできるだけ同じにすることであり、さらに、00、01、10、11で始まる符号の出現確率をできるだけ同じにすることであり、より長い符号についても同様の考え方で符号を構成することである。

たとえば、

$$0.25, 0.25, 0.25, 0.125, 0.125$$

という出現確率があった場合、0.125 を二つ組み合わせると、0.25 となって、他の 3 つと等しくなる。そこで、次のような符号を考える。

$$00, 01, 10, 110, 111$$

こうすると、00、01、10、11 で始まる符号の出現確率が同じになり、この 5 つの文字の符号の変換後のビット数の期待値は、2.25 ビットになる。このような割り当てに当てはまらない割り当て方、たとえば、

$$0, 100, 101, 110, 111$$

のように符号を割り当てたとすると、期待値は、2.5 ビットになって 2.25 ビットより大きくなってしまう。この場合、0 で始まる符号の出現確率は、0.25 であるが、1 で始まる符号の出現確率は 0.75 であり、大きく違っているからである。

このような考え方は、文字の種類が増えても同様に適用できる。たとえば、A、B、C、D、E、F、G の 7 つの文字を変換する場合、元の文字列中の各文字の出現確率が次のように与えられたとすると、もっとも効率よい 2 進数への割り当てを用いた場合、変換後の 1 文字あたりのビット数の期待値は、$\boxed{(18)}.\boxed{(19)}\boxed{(20)}$ となる。

$$0.33, 0.20, 0.16, 0.11, 0.08, 0.07, 0.05$$

(イ) 次の文章は、ある暗号方式の原理に関して説明したものである。空欄に入るもっとも適した数字をマークしなさい。

整数から別の整数へ変換する暗号方式を考える。ここで説明する暗号方式では、次のようにして、元の整数 a から、暗号化された整数 b を計算する。ただし、$x \pmod y$ は x を y で割った余りを表し、$z \equiv x \pmod y$ は x を y で割った余りと z を y で割った余りが等しいことを表している。

(1) 2 つの素数 p, q を選ぶ。

(2) 2 つの素数の積、$n = pq$ を求める。

(3) $(p-1)$ と $(q-1)$ の最小公倍数 L を求める。

(4) L と互いに素な、$e\ (3 \leqq e \leqq L-1)$ を選ぶ。

(5) $ed \equiv 1 \pmod{L}$ となる d を求める

(6) $a^e \pmod{n}$ を求めて b とする

b から a を得るには次のようにする。

(1) $b^d \pmod{n}$ を求める

したがって、暗号化するには、n, e の組がわかってればよく、復号するには、n, d の組がわかっていればよい。

実際には非常に大きな素数を用いるが、ここでは小さな値、$p = 13$ および $q = 17$ を用いて具体例を示す。まず、$n = 221$ が得られ、$L = 48$ が得られる。$e = 5$ とすると、積 ed を L で割ったときの余りが 1 になる d は $\boxed{(21)}\boxed{(22)}$ である。$e = 11$ の場合は、$d = \boxed{(23)}\boxed{(24)}$ となる。ここでは、$e = 5$ を用いて暗号化する。$a = \boxed{(25)}\boxed{(26)}\boxed{(27)}$ とすると、a の e 乗 (つまり 5 乗) を n で割った余りが b であり、$b = 15$ が得られる。復号するには、b の d 乗を n で割った余りを求めればよく、計算すると、$\boxed{(25)}\boxed{(26)}\boxed{(27)}$ が得られて、a の値になることがわかる。

$a^e \pmod{n}$ の計算は、桁数が多くなり、計算量が多くなるようにみえる。しかしながら、指数部を 2 進数で表現し、下位ビットに相当する部分の余りから順番に計算していく高速に計算できるアルゴリズムが知られており、a^e をそのまま計算する必要はない。

（計算用紙）

情報－Ⅲ

文化祭の模擬店で、ココア、抹茶、ミックスの3種類のクッキーを作って売りたい。次の文章を読み、下の問に答えよ。

クッキーはオーブンの大きさや焼くのにかかる時間の都合から、同種のものを20枚単位でしか焼くことができない。それぞれのクッキーを20枚作るのに必要な材料と販売価格、材料の購入可能単位とその単価は次表のとおりである。ただし、薄力粉、バター、砂糖、卵などの共通の材料は省略してある。共通の材料の材料費や光熱費などの費用は、どのクッキーも1枚あたり10円である。共通の材料以外の材料は、購入可能単位の整数倍で購入しなければならない。共通の材料を含めて、材料を購入するための予算は7,000円である。

表1　クッキー20枚を作るのに必要な材料の量と販売単価

材料	ココア	抹茶	ミックス
ココアパウダー (g)	15	0	10
抹茶パウダー (g)	0	10	4
アーモンド (g)	20	5	10
販売単価 (円/枚)	40	50	45

表2　材料の購入可能単位とその単価

材料	購入可能単位 (g)	価格 (円)
ココアパウダー	640	1280
抹茶パウダー	50	650
アーモンド	300	960

(ア) ココア、抹茶、ミックスクッキーをそれぞれ$20n_c$枚、$20n_t$枚、$20n_m$枚作り、ココアパウダー、抹茶パウダー、アーモンドをそれぞれm_c、m_t、m_a購入単位購入したとき、全てのクッキーが売れた場合の利益を表す式として正しいものを次の選択肢から選び、その番号を $\boxed{(28)}$ にマークしなさい。ただし、n_c、n_t、n_m、m_c、m_t、m_aはそれぞれ0以上の整数とする。

【$\boxed{(28)}$の選択肢】

(1) $506n_c + 654n_t + 596n_m$

(2) $706n_c + 854n_t + 796n_m$

(3) $600n_c + 800n_t + 700n_m - 1280m_c - 650m_t - 960m_a$

(4) $800n_c + 1000n_t + 900n_m - 1280m_c - 650m_t - 960m_a$

情報

(イ) 次の (式 1) から (式 5) は、問題文にそった条件を表している。$\boxed{(29)}$から$\boxed{(32)}$にあてはまるものを、下の選択肢から選んでその番号をマークしなさい。

$15n_c + 10n_m \leqq 640m_c$ …(式 1)

$10n_t + 4n_m \ \boxed{(29)}\ 50m_t$ …(式 2)

$20n_c + 5\boxed{(30)} + 10\boxed{(31)} \leqq 300m_a$ …(式 3)

$200n_c + 200n_t + 200n_m + 1280m_c + 650m_t + 960m_a \ \boxed{(32)}\ 7000$ …(式 4)

$n_c, n_t, n_m, m_c, m_t, m_a \geqq 0$ …(式 5)

【$\boxed{(29)}$〜$\boxed{(32)}$の選択肢】

(1) $>$　(2) $<$　(3) $\geqq$　(4) $\leqq$　(5) n_c　(6) n_t　(7) n_m　(8) m_c　(9) m_t　(0) m_a

(ウ) 次の文章を読み、空欄に入るもっとも適切な数字をマークしなさい。ただし、$\boxed{(33)}$については、空欄にあてはまるもっとも適切な語を下の選択肢から 1 つ選び、その番号をマークしなさい。

まずは、ココアパウダー、抹茶パウダー、アーモンドの購入可能単位の制限が無く、1g 単位で購入可能な場合について考える。この場合、コスト 1 円あたりの利益が一番大きいのは$\boxed{(33)}$で、20 枚あたりのコストは$\boxed{(34)}\boxed{(35)}\boxed{(36)}$円である。よって、予算が 7,000 円だとすると、$20 \times \boxed{(37)}\boxed{(38)}$枚までのクッキーを焼くことができる。このときに必要となる材料の量を購入可能単位で用意しようとすると、ココアパウダー、抹茶パウダー、アーモンドはそれぞれ$\boxed{(39)}$単位、$\boxed{(40)}$単位、$\boxed{(41)}$単位ずつ必要となる。

ココアクッキーも抹茶クッキーもアーモンドが必要であるため、アーモンドはこれ以上減らすことができないことは明らかである。また、ココアパウダーは減らすことができるが、この場合は抹茶クッキーしか作ることができなくなり、ミックスクッキーより利益率が悪くなることが明らかである。このため、減らせる可能性があるのは抹茶パウダーのみとなる。抹茶パウダーの購入単位数を減らした場合、作れるミックスクッキーの上限は 20×12 枚となる。このとき、ココアパウダー、抹茶パウダー、アーモンドの余りはそれぞれ、$\boxed{(42)}\boxed{(43)}\boxed{(44)}$ g 、$\boxed{(45)}\boxed{(46)}\boxed{(47)}$ g、$\boxed{(48)}\boxed{(49)}\boxed{(50)}$ g となる。

【$\boxed{(33)}$の選択肢】

(1) ココアクッキー　(2) 抹茶クッキー　(3) ミックスクッキー

(エ) 利益が最大となる組み合わせが 2 組存在する。それぞれ、n_c、n_t、n_m はいくつになるか。$\boxed{(51)}\boxed{(52)}$、$\boxed{(53)}\boxed{(54)}$、$\boxed{(55)}\boxed{(56)}$および$\boxed{(57)}\boxed{(58)}$、$\boxed{(59)}\boxed{(60)}$、$\boxed{(61)}\boxed{(62)}$に答えよ。

情報－Ⅳ

次の文章を読み、下の問に答えよ。

慶應義塾大学湘南藤沢キャンパスの FabSpace には、多数のデジタルファブリケーションマシンが導入されている。この中で、キャンパスの学生たちは、授業の課題や研究のために必要なものを制作することができる環境が整備されている。

(ア) デジタルファブリケーションの説明としてもっとも適切なものを下の選択肢から1つ選び、その番号を $\boxed{(63)}$ にマークしなさい。

(1) 物体の3次元形状を物理的に成形する技術。

(2) コンピュータを用いて物体のデジタル形状データを取得する技術。

(3) 2次元平面の上で情報が3次元的に飛び出して見える印刷技術。

(4) コンピュータと接続された工作機械によって、デジタルデータをもとに物体を成形する技術。

(イ) 次の文章を読み、空欄に入るもっとも適切な数字をマークしなさい。

ある授業の課題で学生たちは、グループプレゼンテーションのために用いる模型を 3D プリンターで作成することにした。簡単のために、今回の条件を以下のように設定する。

条件 1 この授業の課題で使うことができる 3D プリンターは1台のみとする。

条件 2 この 3D プリンターで同時に出力できるデータは1つである。

条件 3 平均して30分に1人がランダムな確率で 3D プリンターに1つのデータを送る。

条件 4 3D プリンターにデータを入れてから造形が完了するまで平均して20分かかる。

条件 5 3D プリンターへの出力要求は待ち行列に入り、来た順に処理される。

この際、1時間当たりに 3D プリンターに送られるデータファイルの数 λ（個／時）と1時間に出力できるオブジェクトの数 μ（個／時）を用いて、3D プリンター利用率を示す指数 ρ は $\dfrac{\lambda}{\mu}$ として求められる。今回のケースでは ρ は $\dfrac{\boxed{(64)}}{\boxed{(65)}}$ と求められる。

ここで、学生が 3D プリンターの出力開始までに待つ時間の平均は $T\dfrac{\rho}{1-\rho}$（分）で表される（T は 3D プリンターの平均出力時間）。先ほどの値をもとに導出すると、データを送ってから 3D プリンターで出力し終えるまでの平均時間は、$\boxed{(66)}\boxed{(67)}$ 分と見積ることができる。

(ウ) 次の文章を読み、空欄に入るもっとも適切な数字をマークしなさい。

ある年、古くなった 3D プリンターを廃棄するタイミングで、FabSpace 内の機材を新たに購入することになった。利用できる予算額を鑑みると、以下の 2 つのプランが考えられることがわかった。なお、古くなった 3D プリンターは廃棄するものとする。

プラン 1 これまでの 3D プリンターと同じ性能のものを 2 台購入

プラン 2 これまでの 3D プリンターより 2 倍早く出力できる性能を持つプリンターを 1 台購入

授業で 1 時間当たりに学生が送るデータの数は（イ）と変わらないものとする。また、プラン 1 では学生は混み具合を考慮することなく、平均的にそれぞれの 3D プリンターにデータを送るものとし、3D プリンタ毎に待ち行列ができるものとする。

待ち時間の観点でこの二つのプランを比較すると、並べ始めてから出力が完了するまでの平均時間はプラン 1 では $\boxed{(68)}\boxed{(69)}$ 分、プラン 2 では $\boxed{(70)}\boxed{(71)}$ 分となる。

情報－V

ソーシャル・ネットワークの分野には「六次の隔たり」という言葉がある。これは、友人の友人の友人の…というふうにたどっていくと、世界中のほとんど誰とでも6回程度たどることでつながるという仮説である。

「六次の隔たり」が本当かどうかを調べるために、友人関係のデータが与えられた時に、その中の任意の2人がつながるためには最大何回たどる必要があるかを計算するアルゴリズムを考える。

与えられるデータは、人の集合 G と、すべての $x \in G$ に対して友人の集合 $F(x)$ である。$x, y \in G$ に対して、G の部分集合が x と y の経路であることを次のように定義する。

- $x = y$ の時、$\{x\}$ は x と y の経路である。
- $y \in F(x)$ の時、$\{x, y\}$ は x と y の経路である。
- すべて異なる $z_1, z_2, \cdots, z_n$ があり、$z_1 \in F(x)$ かつ $z_2 \in F(z_1)$ かつ $\cdots$ かつ $z_n \in F(z_{n-1})$ かつ $y \in F(z_n)$ の時、$\{x, z_1, z_2, \cdots, z_n, y\}$ は x と y の経路である。

問題を簡単にするために、このデータは次の性質を持つとする。

- すべての $x \in G$ に対して $x \notin F(x)$。
- すべての $x, y \in G$ に対して、$x \in F(y)$ ならば $y \in F(x)$ 。
- すべての $x, y \in G$ に対して、x と y の経路となる G の部分集合がただひとつ存在する。これを $P(x, y)$ と書く。

x と y の距離 $d(x, y)$ を、$d(x, y) = n(P(x, y)) - 1$ と定義する。ただし、$n(P(x, y))$ は $P(x, y)$ の要素の個数である。

与えられたデータの中の任意の2人がつながるためには最大何回たどる必要があるかは、次のようにして計算できる。

1. $s \in G$ を任意に決める。
2. すべての $x \in G$ に対して $d(s, t) \geqq d(s, x)$ となるように t を選ぶ。(条件 α)
3. すべての $x \in G$ に対して $d(t, u) \geqq d(t, x)$ となるように u を選ぶ。(条件 β)
4. $d(t, u)$ が求める値となる。

(ア) これをコンピュータで計算するための手順は次のようになる。空欄に入るもっとも適切なものを下の選択肢から選び、その番号をマークしなさい。なお、同じ選択肢を複数回使ってもよい。

$\boxed{(72)}\boxed{(73)}$ から任意の要素 s を取り出し、変数 M の値を $\{s\}$ とする
$\boxed{(74)}\boxed{(75)}$ が成り立つ間、次の処理 A を繰り返す
処理 A の始め
　変数 N の値を $\boxed{(76)}\boxed{(77)}$ にする
　すべての $x \in \boxed{(78)}\boxed{(79)}$ に対して、次の処理 B を繰り返す
　処理 B の始め
　　N の値を $\boxed{(80)}\boxed{(81)}$ にする
　処理 B の終わり
　M の値を $\boxed{(82)}\boxed{(83)}$ にする
処理 A の終わり
$\boxed{(84)}\boxed{(85)}$ から任意の要素 t を取り出し、M の値を $\{t\}$ とする
変数 i の値を $\boxed{(86)}\boxed{(87)}$ とする
$\boxed{(88)}\boxed{(89)}$ が成り立つ間、次の処理 C を繰り返す
処理 C の始め
　すべての $x \in \boxed{(90)}\boxed{(91)}$ に対して、次の処理 D を繰り返す
　処理 D の始め
　　M の値を $\boxed{(92)}\boxed{(93)}$ にする
　処理 D の終わり
　i の値を $\boxed{(94)}\boxed{(95)}$ にする
処理 C の終わり
$\boxed{(96)}\boxed{(97)}$ の値を結果として出力する

(11) G　(12) M　(13) N　(14) $M \subset N$　(15) $N \subset M$
(16) $M = G$　(17) $M \neq G$　(18) $N = G$　(19) $N \neq G$　(20) 空集合
(21) $M \cup N$　(22) $M \cup F(x)$　(23) $N \cup F(x)$　(24) $N \cup F(x) - M$　(25) $M \cup F(x) - N$
(26) i　(27) $i+1$　(28) $i-1$　(29) 0

(イ) また、上の計算方法が正しいことは、次のようにして証明できる。空欄に入るもっとも適切なものを下の選択肢から選び、その番号をマークしなさい。なお、同じ選択肢を複数回使ってもよい。

ある v, w について $d(v, w) > \boxed{(98)}\boxed{(99)}$ と仮定し、矛盾を示す。

もし $d(v, w') > d(v, w)$ となる w' があれば、w' をあらためて w とおくことができるので、すべての $x \in G$ に対して $\boxed{(100)}\boxed{(101)} \geqq d(v, x)$ としてよい。(条件 γ)

まず、$P(s, t)$ と $P(v, w)$ に共通部分があることを示す。

s と w の経路が存在するので、それが s と t の経路と分岐する箇所を a、v と w の経路と分岐する箇所を b とする。

$\boxed{(102)}$ より

$$\boxed{(103)}\boxed{(104)} = d(s, a) + \boxed{(105)}\boxed{(106)} \geqq \boxed{(107)}\boxed{(108)} = \boxed{(109)}\boxed{(110)} + d(a, b) + d(b, w)$$

となる。同様に $\boxed{(111)}$ より

$$\boxed{(112)}\boxed{(113)} = d(v, b) + \boxed{(114)}\boxed{(115)} \geqq \boxed{(116)}\boxed{(117)} = \boxed{(118)}\boxed{(119)} + d(a, b) + d(a, t)$$

となる。この 2 つの式の不等号の両辺を足して整理すると $0 \geqq \boxed{(120)}\boxed{(121)}$ となるが、距離は負にならないので $\boxed{(120)}\boxed{(121)} = 0$ となり、$P(s, t)$ と $P(v, w)$ には共通部分が存在することがわかる。

$c \in P(s, t) \cap P(v, w)$ とする。c は $P(s, v)$ か $P(s, w)$ のどちらかに含まれるが、$P(s, v)$ に含まれる場合は v と w を交換して考えることができるので、$c \in P(s, w)$ としてよい。

$\boxed{(122)}$ より

$$\boxed{(123)}\boxed{(124)} = d(s, c) + \boxed{(125)}\boxed{(126)} \geqq \boxed{(127)}\boxed{(128)} = d(s, c) + \boxed{(129)}\boxed{(130)}$$

であるから $\boxed{(125)}\boxed{(126)} \geqq \boxed{(129)}\boxed{(130)}$ となる。同様に $\boxed{(131)}$ より

$$\boxed{(132)}\boxed{(133)} = d(v, c) + \boxed{(129)}\boxed{(130)} \geqq \boxed{(134)}\boxed{(135)} = d(v, c) + \boxed{(125)}\boxed{(126)}$$

であるから $\boxed{(129)}\boxed{(130)} \geqq \boxed{(125)}\boxed{(126)}$ となる。この 2 つの式から $\boxed{(125)}\boxed{(126)} = \boxed{(129)}\boxed{(130)}$ となる。

$\boxed{(136)}$ より

$$\boxed{(137)}\boxed{(138)} \geqq \boxed{(139)}\boxed{(140)} = d(v, c) + \boxed{(125)}\boxed{(126)} = d(v, c) + \boxed{(129)}\boxed{(130)} = \boxed{(141)}\boxed{(142)}$$

となる。これは最初の仮定に反するので、証明された。

【$\boxed{\scriptstyle (102)}$, $\boxed{\scriptstyle (111)}$, $\boxed{\scriptstyle (122)}$, $\boxed{\scriptstyle (131)}$, $\boxed{\scriptstyle (136)}$ の選択肢】

(1) 条件 α　(2) 条件 β　(3) 条件 γ

【上記以外の解答欄の選択肢】

(11) $d(a, b)$	(12) $d(a, s)$	(13) $d(a, t)$	(14) $d(a, u)$	(15) $d(a, v)$
(16) $d(a, w)$	(17) $d(b, s)$	(18) $d(b, t)$	(19) $d(b, u)$	(20) $d(b, v)$
(21) $d(b, w)$	(22) $d(c, s)$	(23) $d(c, t)$	(24) $d(c, u)$	(25) $d(c, v)$
(26) $d(c, w)$	(27) $d(s, t)$	(28) $d(s, u)$	(29) $d(s, v)$	(30) $d(s, w)$
(31) $d(t, u)$	(32) $d(t, v)$	(33) $d(t, w)$	(34) $d(u, v)$	(35) $d(u, w)$
(36) $d(v, w)$				