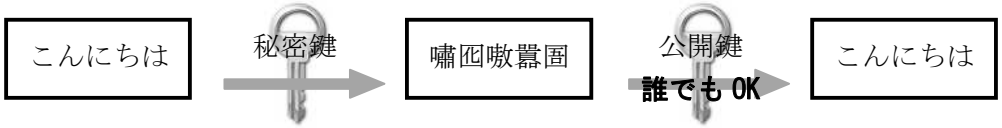
2007 年度 共通問題 解答例

注: このプリントは「解答例」であって「模範解答」ではありません。

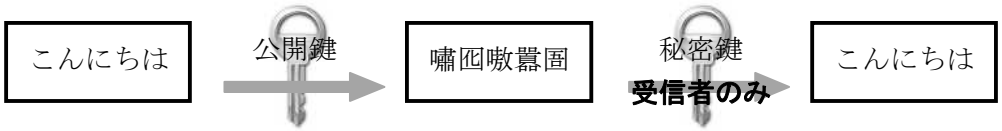
共通問題 1

(1) 公開鍵暗号では、**秘密鍵**を秘密にして**公開鍵**を公開する。

ここで、もし文章の暗号化に秘密鍵を使ったとしたら、復号には公開鍵が使われるので、誰でも復号できることになってしまう。〔下図〕



それでは困るので、復号は秘密鍵で行う必要がある。そう考えると、受信者が鍵を生成し、送信者が公開鍵を知っている状況が適切であると考えられる。〔下図〕



従って、答えは **受信者** となる。

(2) (1)で述べたとおり、(b)**秘密鍵と公開鍵**　(c)**公開鍵**　(d)**公開鍵**　(e)**秘密鍵**

(3) 〔例〕
- 秘密鍵は(a)受信者のみが知っている。
- 公開鍵で暗号化された暗号文は、秘密鍵でのみ復号できる。
- 公開鍵から秘密鍵を推測するのは困難である。

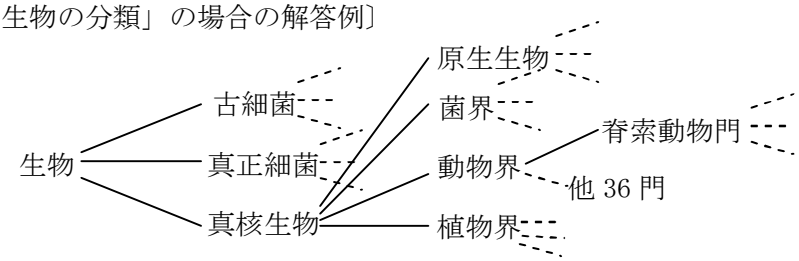
(4) 〔例〕
共通鍵暗号の場合は鍵は確実に相手のみに知らせないとその鍵で他者にデータを復号されてしまうのに対し、公開鍵暗号の場合は秘密鍵を知っている人しか復号できないので公開鍵は誰に知られても構わない。

共通問題 2

(1) 解答: 「**生物の分類**」または「**住所**」

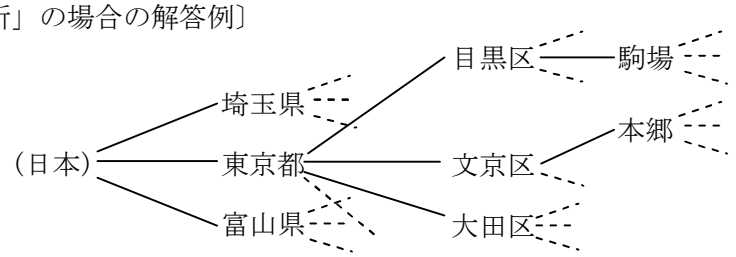
※「生物の分類」は諸説あるので、たぶん「住所」の方が確実です。

〔「生物の分類」の場合の解答例〕



上の生物の分類において、例えばヒトであれば 生物→真核生物→動物界→…→ヒト科→ヒト属→ヒト といったように、一意的に分類が定まる。この例では、各々の生物種はいずれか一つの属に属しており、各々の属はいずれか一つの科に属しており、…… というように、生物全体が階層的な構造を成している。このような構造を階層モデルという。

〔「住所」の場合の解答例〕



上図に示した通り、日本国内の場所であれば、都道府県→市・郡→区・町村→町名(字)→丁目→街区符号→住居番号などといったように、一意的に所在地の表示が定まる。例えば東京大学駒場Ⅰキャンパスであれば、東京都→目黒区→駒場→三丁目→8 番→1 号といった具合である。このように、日本の住所表示は階層的な構造を成している。このような構造を階層モデルという。

(2) 〔例〕

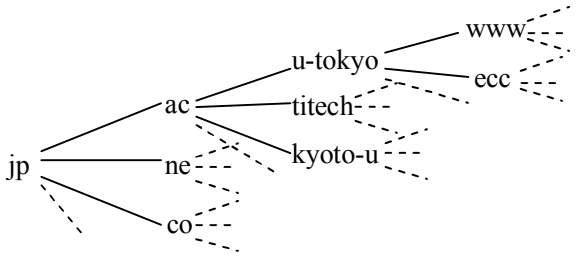
・フォルダの中にサブフォルダを作って細かい仕分けができる。

・すべてのファイルはある 1 つのフォルダに属しており、異なるフォルダ内のファイルが混ざることはない。

・フォルダを辿ることで、全てのファイル・フォルダに対して重複なく一度ずつ同じ処理を行うことができる。

・あるフォルダ内のファイル及びサブフォルダ全体に対して行う処理は、その最上位のフォルダに対する処理として代表して行うことができる。

(3) 〔例〕



上図のようにホスト名とドメイン名の構造は木構造と対応づけられ、ドメイン u-tokyo.ac.jp は ac.jp に属し、ac.jp は jp に属する、というように階層構造を成している。それ故、u-tokyo.ac.jp 以下のドメインは他のドメインとは関係なく東京大学が管理できるというように、ドメインの分散管理ができる。

共通問題３ 問題Ａ

(1) 〔例・著作権法〕

著作権法は、著作権の保護を目的とする法律である。この保護する対象が物質的媒体(CD・ビデオテープ・現像された写真・本・コピーなど)であった時は、その物質の市場・流通機構が存在し、その保有・所有についての概念は明確なものであった。しかし、情報技術の進んだ現在においては、電子情報(音楽・映像・画像・電子書籍・ソフトウェアなど)が保護されるべき著作物となっており、その保有・所有についての概念が曖昧なものとなっている。そこで、如何にして電子情報の所有を管理すべきかが問われ、DRM(デジタル著作権管理)が議論されるのである。このような中で、現在の社会制度である著作権法を固定した上で議論すべきか、それとも技術の進展とともに法を見直すべきか、ということが問題となっている。

〔例・個人情報保護法〕

個人情報保護法は、個人情報の有用性に配慮しながら個人の権利利益を保護することを目的とする法律である。情報技術の進歩により、以前では不可能であった個人に関する詳細な情報の収集が可能となった。ネットワーク経由で情報が交換される範囲は膨大であり、一旦ある個人の情報がコンピュータ上に記録されれば、別のコンピュータに転送可能である。その情報が売り買いされたり、無償で配布されたり、盗まれたりする。このような個人情報は、保護されなくてはならない。そこで制定されたのが、個人情報保護法である。この法律の制定により、個人情報の適切な扱いに関するルールが定められ、情報技術の時代における個人情報に関する権利が保障されるようになった。

……こんなに長く書く必要はないんじゃないかと思います。解答欄知りませんけど。

(2) 〔例〕

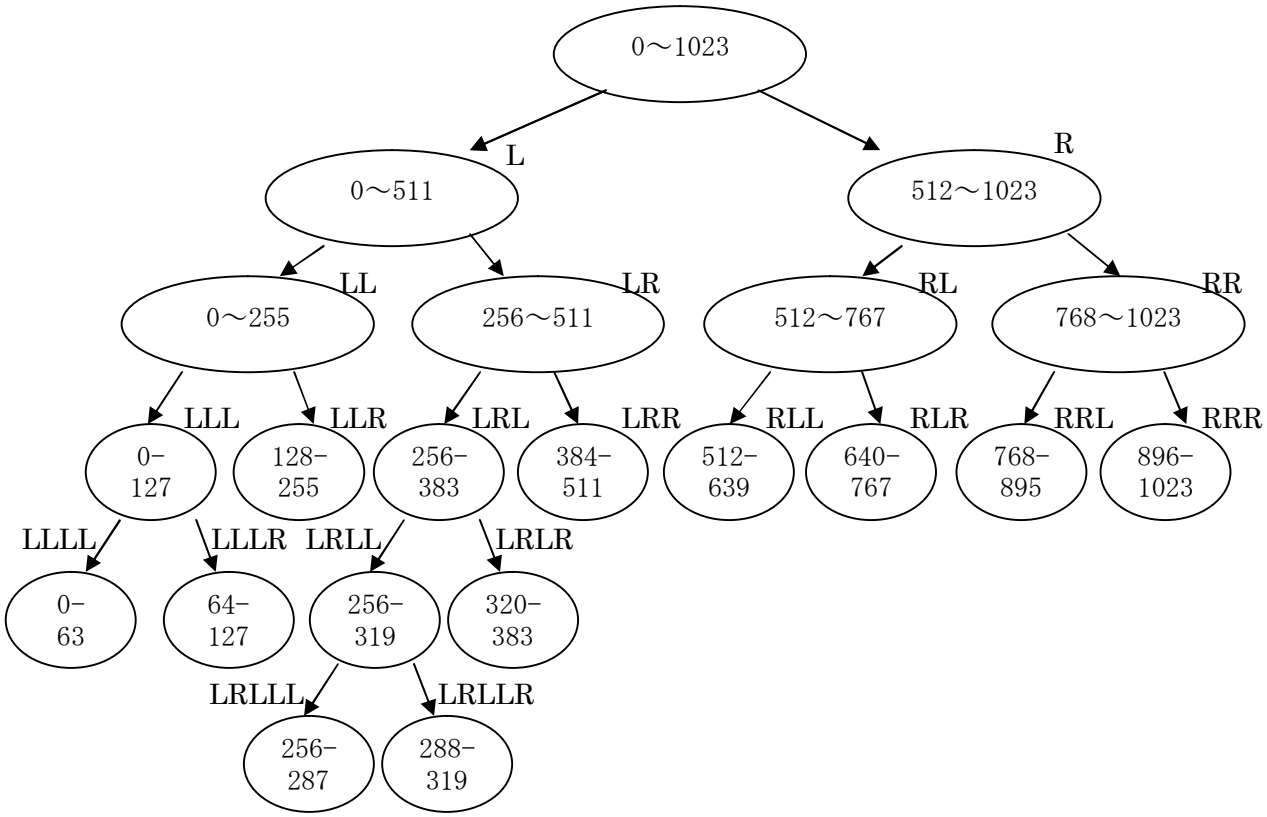
情報リテラシーとは、単なる情報機器操作能力ではなく、情報を主体的に選択・収集・活用・編集・発信する能力と同時に、情報機器を使って論理的に考える能力である。これには、情報を収集するときに、多様な情報手段を使って取捨選択できるか、情報機器を使って行う自分の行為がどのような影響を及ぼすかについての批判的考察などの、情報における批判的思考の能力も含まれる。

(3) 〔例〕

GUI は、情報が視覚的に表示されるため、直観的でわかりやすいという利点をもつ。その反面、CUI と比べて煩雑な操作が必要であり、また必要な処理が膨大となるなどの欠点がある。一方の CUI は、すべてのデータの入出力が文字列で為されるため、操作に慣れれば迅速な作業が可能である。しかし、GUI のような見た目のわかりやすさに欠け、初心者には扱いづらいという欠点がある。

共通問題 3 問題 B

(1) 下図の通り、LLLL: **0 から 63**, LRLLR: **288 から 319**



(2) ・0 について

(b) のように山を 2 つに分ける手順が 1 回為される毎にその山のカードの数は半分になるから、(d) が終わるまでにどのカードも 10 回 (b) のような操作が為される。($\because$ $1023 = 2^{10}$)
0 のカードは他のどのカードよりも番号よりも小さいので常に左側に置かれる。
従って、0 のカードの山は **LLLLLLLLLL**

・100 について

100 のカードは L(0～511) → LL(0～255) → LLL(0～127) → LLLR(64～127) → LLLRR(96～127) → LLLRRL(96～111) → LLLRRLL(96～103) → LLLRRLLR(100～103) → LLLRRLLRL(100～101) → **LLLRRLLRLL** (100) のように推移する。

・500 について

500 のカードは L(0～511) → LR(256-511) → LRR(384-511) → LRRR(448～511) → LRRRR(480～511) → LRRRRR(496～511) → LRRRRRL(496～503) → LRRRRRLR(500～503) → LRRRRRLRL(500～501) → **LRRRRRLRLL** (500) のように推移する。

(3) (b) のように山を 2 つに分ける手順が 1 回為されると、その時に左側の山に置かれたカードの番号はいずれも右側に置かれたカードの番号よりも小さい。また、その後の操作によって、このときに左側の山に置かれたカードが右側の山に置かれたカードよりも右に来ることはない。従って、(d) が終わった時点において、どの 2 枚を取ってみても右側のカードの方が番号が小さいことはない。すなわち、カードは左から番号の小さい順に並んでいる。

(4)（ア）$p(1)$ は 0 と 1 のカードに (a) から (d) の操作を行った時にカードをめくる回数だから、

$\underline{p(1) = 2}$

（イ）まず 0 から $2^n - 1$ までのカードを 2 つの山に分けるのにカードを 2^n 回めくる。

続いて、その 2 つの山のそれぞれのカードを $p(n - 1)$ 回めくって 1 枚ずつの山にする。

よって、**$\underline{p(n) = 2^n + 2\,p(n-1)}$**

（ウ）$$p(n) = 2^n + 2\,p(n-1)$$

$$\therefore \quad \frac{p(n)}{2^n} = 1 + \frac{p(n-1)}{2^{n-1}}$$

$$\therefore \quad \frac{p(n)}{2^n} = (n-1) + \frac{p(1)}{2^1} = (n-1) + \frac{2}{2} = n$$

$$\therefore \quad \underline{p(n) = n\,2^n}$$

説明が少なくてすみません。不備があったら関根まで。