Bulletin of Aichi Univ. of Education, 68 (Educational Sciences), pp. 103-108, March, 2019

低学年向け教育を意識した情報科学教材に関する一考察

松永　豊

情報教育講座

A Study on Information Science Teaching Material Conscious of Education for Low Grade Students

Yutaka MATSUNAGA

Department of Information Sciences, Aichi University of Education, Kariya 448-8542, Japan

１．はじめに

近年、コンピュータの急速な成長により、ありとあらゆる分野でコンピュータは利用されるようになった。また、安価なプログラマブル IC の登場により、ハードウェア分野においても一般ユーザへの垣根が大幅に下がり、情報科学的な専門用語がすっかり日常の会話に登場するまでになっている。AI, IoT, ビッグデータ, ドローン, ロボット, データマイニング, ブロックチェーン、公開鍵暗号、などは、本来なら専門性が高い用語であるのだが、単語を聞いたことがあるだけではなく、科学技術的な側面における知識を持つ人も多いかもしれない。(自分が従事している職業とは特に関係なく…、である。)

そこで、本研究では専門性が高い内容に対し、本質を残しつつ一般化する上での授業設計や教材開発についての議論を目的とする。現在、教育分野で広く利用されているアンプラグドをはじめとして、「１年前期情報基礎」授業での実践例を紹介するとともに、有効な点、扱うことが可能な範囲、問題点などについて議論する。

２．社会的背景について

本題に入る前に少しだけ社会的背景についても触れておく。専門用語（専門技術）の一般社会への浸透は、教育分野においても見ることができる。特に 2020 年度から小学校でプログラミングが必修になるなどが好例である。そもそも、プログラミングという単語自体がそれなりに専門的な単語と考えられるが、小学校で必修にせざるを得ないほどの事態に直面している［１］。情報分野においては、専門科目の低年齢化をじわじわと浸透するまで待つ余裕はなく、急ピッチで優先的な施行が求められていると言える。これは、すでに様々な研究等でも報告されているが、日本が海外の先進国に比べて大幅に遅れを取っていることや、第四次産業革命とも呼ばれる急激な社会変動により現存する多くの職業が近い将来存在しなくなる可能性が高いことなどが要因と考えられている［２］［３］。

実際のところ、人にしかできなかった分野においてもコンピュータ(ロボット)への代替が可能となれば、経営者にとって労働力という観点から極めて魅力的であることは自明の理である。長時間労働にも耐えうるし（一度、電源を入れればメンテナンス以外では半永久的に駆動可能など)、疲れによるうっかりミスなどは激減し、人件費を大幅に削減可能である。結果として、その職業に従事している（その職業を目指している）人間は困ることになるが、あらゆる意味で人間の労働力を凌駕するのであれば、職業そのものが消えてなくなることも仕方がないこととも言えるし、大幅に削減できた人件費を別の場所に回すことにより、新たな雇用が生まれるかもしれない。

AI の進化により人間からロボットに置き換わると考えられている職業は多種に渡るが、当然のことながらアルゴリズムが単純な場合や例外処理も含めてほぼすべてのパターンが網羅できる場合はロボット化される可能性が高い。例えば、無人運転の電車がすでに多数運用されていることは分かりやすい事例であろう。

一方、ロボット化が比較的難しい職種も当然存在する。その一つが教員であると考えられている。無論、e-learning をはじめとして教育の分野においても ICT 化（自動化や無人化等の要素を含む）の研究は広く行われているが、完璧な教育方法など存在しない（少なくとも現時点ではわかっていない）ことも多く、児童・生徒の振る舞いを完全に予測することも困難であり、また、一般的には有効と考えられている学習方法が一

部の特殊事情（家庭環境等）を持つ児童・生徒にとっては効果が期待できないなど、臨機応変に対処する必要があるという点では極めて人間的な職業であることが要因である。

ただし、そのような事情を鑑みても ICT が専門科目から一般科目へと範囲を拡大しつつあることは疑いようがなく、教員を目指す学生も知識として一定範囲身に付けておく必要がある。また、将来、低学年の児童・生徒等に教育する必要も生ずるため、ICT 活用指導力の観点からも様々なことを学んでおく必要があると考えられる。

３．専門知識と教育について

コンピュータ（いわゆる電子計算機）は今日では必要不可欠な道具であるが、発明されてからまだ１世紀すら経っておらず、極めて歴史が浅い。当然のことながら、コンピュータの仕組み等の教育や、コンピュータを使うことによる効果や応用事例などは、さらに歴史が浅い。

コンピュータの黎明期には、ジョン・フォン・ノイマンやアラン・チューリングなどが活躍しているが、設計に関わった多くの研究者が数学の研究者であったことはよく知られている。コンピュータの歴史は極めて浅いが、数学には長大な歴史がある。すなわち、コンピュータの仕組みやアルゴリズム等の教育において、様々な箇所で数学が登場する。そのため、コンピュータ自体を教育するための教材においても、数学の応用を使うシーンは多々ある。

また、ハードウェアにおいては、本格的な回路になると専門的な知識が必要不可欠となるが、デジタル回路の場合は 2 進数ベースでの設計が基本となるため、2 つの状態、0V か 5V か、電流が流れるか流れないか、など比較的扱いやすい世界となる。一例をあげれば、本来は増幅機器として使われるトランジスタも飽和状態で使えば単なるスイッチとみなすことができる、などである。この考えを基本にすると、オームの法則程度でもそれなりに回路設計が可能となる。

すなわち、コンピュータの歴史は浅いが、設計思想や物理的現象はあくまでも数学や物理に他ならないため、情報教育としての教材設計においても、数学（算数）教材や物理（理科）教材としても意識をする必要がある。

４．情報関連コースについて

本学の情報教育講座は、もともとは現代学芸課程の情報科学コースと教員養成課程の情報選修・情報専攻の学生に対するカリキュラムを提供してきた。この形態は現代学芸課程と教員養成課程を両輪とする構図で表すとわかりやすく、極めてうまく機能してきたと考えている。（図１参照）

両課程とも教育学部の中の課程ではあるが、現代学芸課程はいわゆるゼロ免課程（教員免許取得が卒業要件にはならない課程）なので、幅広い専門知識の取得が可能なコースとなっていた。

もともと、教員養成課程では多くの免許必須科目を取得する必要があるため、専門的な科目を取る時間は極めて限られている。しかしながら、情報科学の分野は広範囲に広がっているため、科目を限定させることが難しい。その点、ゼロ免の情報科学コースが存在する場合は、専門性の高い授業を情報科学コース向けに多数開講し、教員養成課程の学生にも提供することで専門性を高めた状態のまま選択肢を広げることができていた。（表１参照）

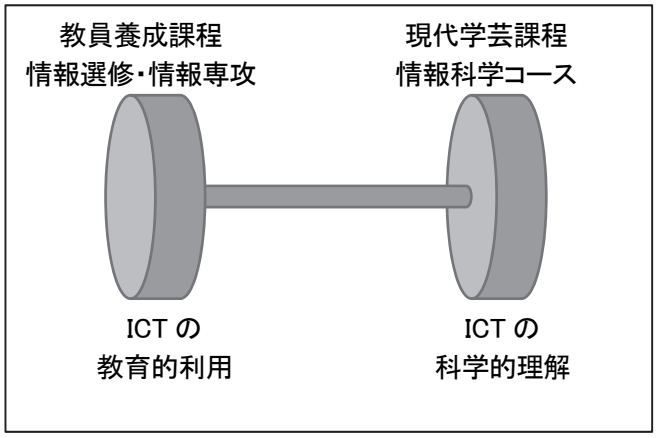

図 1　両輪を表す構図

学部	教育学部	
課程	教員養成	現代学芸
コース	情報選修 情報専攻	情報科学コース
免許	取得が卒業要件	ゼロ免
目標	情報に強い教員	専門知識の取得
就職	主に小学校・中学校の教員	主に企業就職

表 1　情報コース

残念ながら、現代学芸コースがなくなることが決まったため、情報科学コースも在籍中の学生が全員卒業した時点で終了する。そのため、１年生の必修科目においても大幅な刷新が行われた。具体的には、教育寄りの内容へのシフトである。筆者が担当する１年前期の「情報基礎」もそのコンセプトに従って改造を行った授業の一つである。

５．情報基礎について

情報基礎という授業においては、基本的にはタイトル通り、情報の基礎を学ぶ授業である。情報科学コー

スでのカリキュラム（旧カリ）においては強いて言えば「コンピュータ通論」になるのだが（リカバリ学生用の代替科目になっている）、実際には内容を大幅に刷新した。ここでは導入したいくつかの演習事例を紹介する。

★事例１：仮想通貨におけるブロックチェーン

ビットコインで一躍有名となった仮想通貨だが、これらの仮想通貨においてはブロックチェーンの技術が使われている。いわゆる銀行のような特定の機関が通貨を保証するのではなく、マイニングという仕組みで通貨の安全性を担保しているのが特徴である。考え方は以下の通りである。

- 取引記録（いわゆる台帳）をある程度まとめてブロックデータとする。
- ブロックデータに何らかのキーワードを付加してからハッシュ値を計算するが、ハッシュ値がある条件を満たすまで付加するキーワードを探し続ける。（マイニング）
- ハッシュ値が条件を満たした場合、キーワードとハッシュ値を公開し、条件を満たしていることが確認出来たら、そのキーワードを採用し、最初にキーワードを見つけた人にだけ報酬を与える。（独り勝ち方式）

細かい部分ではもう少し複雑ではあるが、授業で使う分にはこの程度の手順で問題ない。まず、仮想通貨におけるブロックチェーンの仕組みやマイニングについてある程度話した後に、ハッシュについても説明する。体験学習の際にはどのハッシュアルゴリズムでも構わない。今回の授業では MD5 を用いることにした。

まず、ハッシュや MD5 について軽く説明した後に、入力文字列から MD5 を計算してくれるサイトを紹介し、適当な文字列を入れて 1 文字変えるだけでハッシュ値が全く異なることを体験させる。

次に基本となる単語（例：「apple」）を発表し、その単語に好きな数字やアルファベットを好きなだけ付加し、付加した文字列ごと MD5 を計算させる。

ここで、ハッシュ値に条件を設ける。今回は、ハッシュの最初の値が「0」から始まるものが条件を満たすことにした。学生はしばらくの間キーワードを変えながらひたすらハッシュの計算を行うが、0 から始まるハッシュ値が見つかった場合は手を挙げさせ、キーワードを発表させる。この時点で全員の作業を一旦中断させる。

例えば、「11」が条件を満たすキーワードであると発表があったと仮定する。発表したキーワードを付加した文字列「apple11」のハッシュ値が条件に合うか他の学生にも確認させ、条件を満たすことが確認できた時点で「11」を見つけた学生を勝者として報酬を与え、キーワード「11」を本採用する。勝者が決定したところで第一ラウンド終了である。

次に特定の記号（例：「＋」）を挟んだ後、２番目の単語（例：「orange」）を発表する。基本となる単語は「apple11+orange」となり、先ほどと同様に条件を満たす文字列を探すよう促す。

以下、同様にして最初に条件を満たすキーワードを見つけた学生を勝者とし、報酬を与えるとともに、キーワードを採用して、第二ラウンドは終了となる。

実際の仮想通貨においては、マイニングの成功報酬は仮想通貨そのものになるが、一定数マイニングが行われると条件レベル（始まる 0 の桁数等）を厳しくする仕組みが施されている。今回の例でいえば、「00」から始まるハッシュ値を条件にすれば、難易度は大幅に上がる。ただし、「00」からでは難易度が上がりすぎるため、授業では第三ラウンドで「一文字目が 0、二文字目が偶数」から始まるハッシュ値を見つけるように指示した。

この演習は極めて簡単な手順で行うことができる割には、少々理解し辛い情報処理を体験的に実習できるため、興味深い学生の反応が出た。予備知識のほとんどない学生の反応は可もなく不可もなしだったが、仮想通貨やブロックチェーンについて多少勉強済みの学生には「マイニングの意味がようやく分かった」など、大変好評を得たのである。

なお、操作性の面において改善すべき点が見られた。MD5 を計算してくれるサイトは複数あるが、紹介したページにおいてはハッシュ値の計算の都度、元の文字列を入れたテキストボックスが初期化されてしまい、毎回、元の文字列を入力するのが面倒だったことである。この問題は、本演習のための専用のページを用意することで解決する。図２が作成したソフトである。今回作成したものは、基本となる文字列と追加文字列のテキストボックスを分離させて、追加文字列を書き換えると同時にハッシュ値を即座に計算するだけのものだが、使い勝手が大幅に向上したため、最低限、この程度は準備しておいた方が無難である。

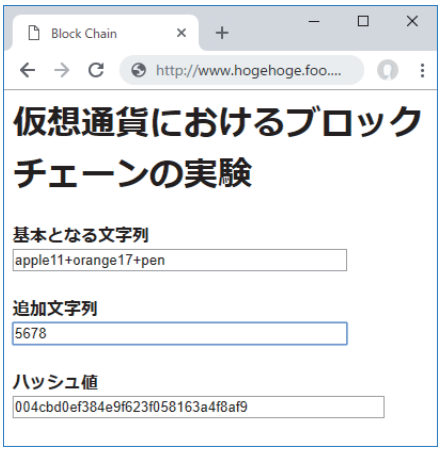

図 2　ブロックチェーンの実験

★事例２：手品の利用

本授業において手品（っぽいもの）を３回行ったのでそれについて紹介する。

【手品１】

まず、１５回の講義の前半で行った２進数のところで手品をしている。具体的には、8 枚のカードのうち学生が選んだカードを当てるというものであるが、数字を当てるものであれば割とよくあるが、8 つの漢字を用いているところに特徴がある。具体的には「非、求、米、元、臼、平、半、王」の８つの漢字を書いたカードをこの順に重ねておく。学生には８つの漢字のうち一つを選ばせ、筆者にはわからないように（筆者が後ろを向いている間に）どの漢字を選んだかクラス全員に共有するよう指示しておき、OK の合図で正面を向いて演技を開始する。

＜１回目＞

まず、8 枚の漢字カードを１枚ずつ交互に分けて２つのデッキを作成する。このうちの「王」の含まれるデッキの４枚の漢字カードを学生に見せ、選んだカードが含まれるか YES、NO で答えさせる。

含まれないと答えた場合は、間の途切れた水平線　－　－　を黒板に書く。含まれると答えた場合は、間の途切れない一直線の水平線　―――　を黒板に書く。

カードの順番が崩れないように揃えて、２つのデッキを重ねて１つのデッキに戻す。このとき、「非」と「王」が端になるように重なる。

＜２回目＞

１回目と同じことを行う。水平線は１回目の水平線の少し下に書く。

＜３回目＞

１回目と同じことをもう一度行う。水平線は２回目の水平線の少し下に書く。

３回終わったところで、線を１本か２本追加すると、元の漢字が浮き上がる。（図３参照）

図 3　漢字手品

8 枚のカードに対して 3 回の YES、NO の質問、すなわち、3bit の情報量なので、手品でも何でもないのだが、最後の線を追加するまでは漢字を書いているように見えないため、漢字になった瞬間に「おー！」といった歓声が上がっていた。無論、２進数を利用したものなので、種明かしの際には２進数の解説も行っている。

【手品２】

次に行った手品は、ECC メモリ(Error Check and Correct Memory)を扱った回である。ノイズが頻繁に混在するネットワーク通信とは異なり、メモリ上のビット反転エラーの発生は低頻度であり、２ビットが同時に反転するケースは極めて稀である。そのため、１ビットの反転エラーであれば自己修復の機能を持つメモリがサーバ等では使われている。

この誤り訂正符号の一つであるハミング符号を用いた手品教材について紹介する。ここで用いるハミング符号では４ビットデータを７ビットの信号に変換することにより、高々１ビットのノイズが含まれた際に誤りを訂正できる。

まず、4 ビットの 2 進データに対し、各ビットを A、B、C、D で表し、パリティビットとして E=A+B+D、F=A+C+D、G=A+B+C をそれぞれ計算する（パリティビットの計算なのでここでの＋記号は排他的論理和とみなす）。この A～G の 7 つのデータにおいて、ビットが１になる数字のみを書き写した７枚のシートを作る。例えば、シート A には、8,9,10,11,12,13,14,15 か書かれていることになる。また、あとでエラー訂正の際に使うので、表の一番上の色のシールをシートに貼っておく。例えば、A 列のシートには赤青緑のシールが貼られていることになる。（表２参照）

数字	赤青緑	赤緑	青緑	赤青	赤	青	緑
	A	B	C	D	E=A+B+D	F=A+C+D	G=A+B+C
0	0	0	0	0	0	0	0
1	0	0	0	1	1	1	0
2	0	0	1	0	0	1	1
3	0	0	1	1	1	0	1
4	0	1	0	0	1	0	1
5	0	1	0	1	0	1	1
6	0	1	1	0	1	1	0
7	0	1	1	1	0	0	0
8	1	0	0	0	1	1	1
9	1	0	0	1	0	0	1
10	1	0	1	0	1	0	0
11	1	0	1	1	0	1	0
12	1	1	0	0	0	1	0
13	1	1	0	1	1	0	0
14	1	1	1	0	0	0	1
15	1	1	1	1	1	1	1

表 2　ハミング符号

実際の手品においては以下のように実演する。まず、１人代表の学生を選び、１から１５までの好きな数字を思い浮かべてもらい、筆者に分からないようにクラス全体に選んだ数字を共有してもらう。準備ができたら、以下のようにアナウンスする。

「今から、数字が書き込まれた７枚のシートを見せま

す。シートの中に選んだ数字が含まれているか聞きますので、含まれている、含まれていない、で答えてください。ただし、7 枚のうちの 1 枚だけはウソをついても構いません。どのシートでウソをついても構いませんし、全て正しく答えても構いません。数字が無いのにあると答えても、数字があるのに無いと答えても構いません。ただし、ウソの返事をするのは最大 1 回だけです。クラスのみんなは、代表者がどこでウソをついたか、2 回以上のウソをついていないかを観察しながら頭の中で確認しておいてください。」

さて、7 枚のシートに対して回答をもらう際、含まれている、と答えたシートだけを集めておく。7 枚すべての質問が終わった時点で、「含まれている」との回答を得たシートの色のシールをカウントし、赤、青、緑、それぞれの個数を計算する。もし 7 枚とも正しく答えている場合はそれぞれの色のシールが必ず偶数枚になるようになっている。仮に A,B,E に対して含まれていると答えたとしよう。その場合、赤 3、青 1、緑 2 となる。赤と青が奇数枚になっておかしいので、1 枚だけシートを移動させて正しくなるように調整すると、D のシートを「含まれている」に移動させれば矛盾がなくなることが分かる。すなわち、A,B,D,E に含まれて、残りのシートには含まれない数字が、学生が選んだ数字である。これを求める場合、A=8、B=4、C=2、D=1 として合計すればよい。ここでは A、B、D なので 8+4+1=13 が選んだ数字とわかる。

この手品を実演した回においては、誤り訂正符号に関する解説とともに、ハミング距離やパリティなどについても学習した。

【手品 3】

最後に行った手品は、公開鍵暗号の回に行ったものである。この回は比較的大きめの数字の因数分解やオイラーの定理など RSA 公開鍵暗号関連の実習およびコンピュータサイエンスアンプラグドの「子ども暗号」の実習を行った［4］。「子ども暗号」の際に配布したマップは「観光都市」に準ずるものであるが、基本的にはコンピュータサイエンスアンプラグドの手法を踏襲しているため、ここでは割愛する。

6．考察

様々な教育を行う際に、コンピュータを使う手法とコンピュータを使わない手法があり、どちらも利点欠点が存在する。コンピュータを用いる場合、複雑な計算をミスすることなく実行するので、比較的短い授業時間の中で計算が必要な場合は大いに活躍するだろう［5］。これは、コンピュータの仕組みや情報技術を学習する際にも例外ではない。しかしながら、一方で計算そのものがブラックボックス化する可能性も生ずる。今回紹介したブロックチェーンの例でいえば、MD5 の計算がまさにそうである。今回の学習内容においては MD5 自体の計算については本題から外れるため純粋に計算速度を上げるために専用のページを使用したが、もしハッシュ値の計算過程に関する学習が必要になる場合は別の教育手法があるかもしれない。

また、コンピュータを使わずにコンピュータを理解させる方法、いわゆるアンプラグドコンピュータサインエスも極めて有効な教育手段であることは疑いようがない。先にも述べた通り、2020 年度に小学校でプログラミング教育が必修となるが、特に低学年の教育においてはアンプラグドが大変期待されている。とりわけ、教員養成課程の学生は将来児童・生徒に教えることになる可能性が高いため、大学生本人の教育レベルに合わせた授業設計や教材開発だけでなく、もっと低学年向けの教育レベルに関しても理解しておくことは極めて重要と考えられる。例えば、誤り検出訂正をテーマとして今回紹介したハミング符号化の手品教材は比較的複雑であるが、コンピュータサイエンスアンプラグドの「カード交換の手品」はもっと簡単な手法であり、小学生でも理解できる内容になっている。

なお、アンプラグド教材に関して言えばコンピュータを用いないわけだから、既存の教科における教材として考えられたものも多い。先にも述べたようにもともと数学や理科の教材として開発されたものをコンピュータの理解のために改造するケースも多々ある。例えば、誤り訂正符号の手品は、数学者の秋山仁氏が考案したものを踏襲している［6］。

その他、筆者は過去にも比較的専門性の高い科目を一般教養科目として再構築する取り組みを行っているが、その研究や授業運営において、比較的難易度が高いものであっても教材の提供の仕方で大きく左右されることが分かっている［7］。例えば、適切なタイミングで教材の機能を向上させる仕組みを導入すると、学習効率が極めて効果的なものになることが分かっており、この制御に関してはコンピュータを用いた教材の方が扱いやすいと考えている。

7．おわりに

本研究では低学年向け教育を意識した情報科学教材について意見を述べた。具体的には、専門知識を如何にして教育を踏まえた内容に移行できるかについて議論した。実際に授業の中で使用した事例をいくつか紹介したが、授業後の提出物の自由記述を読む限り、とりわけ手品に関してはどの内容においても極めて好評である。手品のタネを見破ってやろうとの意識が、いい感じに学習意欲をそそるのかもしれない。今後も様々な工夫をして、授業カリキュラムの向上について研究していきたいと考えている。

参考文献

［1］ 松永 豊, 磯部 征尊, 梅田 恭子, 齋藤 ひとみ, 小学校プログラミング教育におけるメンター育成および実践授業について，愛知教育大学教職キャリアセンター紀要 3，2018
［2］ 新産業構造ビジョン - 経済産業省 http://www.meti.go.jp/press/2017/05/20170530007/20170530007-2.pdf
［3］ 野村総研「日本の労働人口の 49%が人工知能やロボット等で代替可能に」 https://www.nri.com/jp/news/2015/151202_1.aspx
［4］ Tim Bell 他・監訳 兼宗進，コンピュータを使わない情報教育アンプラグドコンピュータサイエンス，イーテキスト研究所，2007
［5］ 松永 豊，教育方略に即した授業支援ツールの開発と実践，愛教大研究報告 67(1)輯（教育科学編），2018
［6］ https://ja.wikipedia.org/wiki/NHK/高校講座_数学基礎
［7］ 松永 豊，自作教材ソフトを用いたシミュレーション演習授業，愛教大学研究報告 61 輯（教育科学編）2012

（2018 年 9 月 25 日受理）