

エデュカーレ

情報

No. 24

特集 実践報告集 6



CONTENTS

- 情報 A ●
 - オリンピック開催地投票を題材にした問題解決..... 2
 - 座学と実習を取り入れた音のデジタル化の授業..... 6
- 情報 C ●
 - ネットワークとセキュリティについて具体的理解の試み..... 11
 - 副読本を利用した情報モラル教育..... 14
- 専門 情報 ●
 - 暗号化と復号..... 8

オリンピック開催地投票を 題材にした問題解決

福岡県立光陵高等学校 三池 司郎 先生

科目：情報A（必修2単位）

内容：問題解決

クラス：5クラス 各40名 1年生

時間：1時間

時期：本文参照（2009年度は7月に実施）

■ 1 ねらい

■実践のねらい

本校の教科「情報」の授業は、1年生で情報Aを2単位、3年生で情報C（2009年度までは情報B）を2単位履修というかたちで実施している。3年生は、文系3教科型クラスの選択科目として、フードデザイン・専門体育・情報Cから1科目を選択している。

全員実施の1年次の授業は、教室で講義形式の授業（毎週1時間）・PC教室で実習形式の授業（毎週1時間）というかたちで実施している。つまり、パソコンをまったく用いない授業も多い。そのなかで、教科書の内容に沿って用語などを説明しながら展開していく授業以外に、一話完結型の講義を開発する必要性を感じ、努力を続けているところである。

特に問題解決において、教科書では「品物購入」や「旅行計画」などの考察・演習が紹介されることが多いが、実際にはその立場にないのに、むりやりその立場となって考えるようなかたちであるので、個人的にはあまり魅力を感じない。世の中には問題解決を科学的におこなう手法が存在するので、それを紹介し、演習する授業を開発したいと考え、いくつか実践している（例としてはKJ法・ミニマックス法・ゲーム理論・対比較法など）。

問題解決の授業において、科学的手法を紹介することが本来の目的でないことは承知している。しかし、その手法を知ることにより、「こんな方法があるのか」「問題解決のための手法を人類はさまざまなかたちで求めているものだなあ」と生徒が思えるように、いろいろな手法を研究し、教材にできればと考えている。

今回の演習は科学的手法というわけではないが、戦略を考えることによる問題解決の演習問題である。

■全体のカリキュラムの中での位置づけ

この授業は、戦略を考えることによる机上の問題解決演習であり、一話完結型であるので、時期にとらわれずに実施してよいと思う。学期の終わりでもよいし、特に2009年のような実際にオリンピック開催地投票が

おこなわれた年は、その時期の近くでおこなうとおもしろいと思う。

■学習目標

戦略を考えることにより、問題解決を学ぶ。同時に、よりよい順位づけはどのようなものかも考察する。

■ 2 準備

・プリント3枚（問題・解答・解説1枚ずつ）

■問題を作成するにあたって注意するポイント

- ・オリンピック開催地投票のルールは、単純な多数決ではなく、「投票の結果、過半数の得票を得る候補地が出るまでは、得票最下位の候補地を1つずつ消していく」という独特のルールである。
- ・ここでは、4つの候補地の評価順位を、9人の選考委員がそれぞれ1位～4位とつけている状態をフィクションで設定した。9人という数は、適度に難しくなる最低限の数字で設定。4つの候補地というのは、平成21年度の開催地投票に合わせたものである。

■ 3 実践内容

■導入

- ・オリンピック開催地投票のルールの紹介
- ・普通の多数決（投票して、最多得票の候補地に決定する）との違いについて考えさせる。

■展開

問題プリント配布

①開催地がどこになるかを考えさせる（5～10分）

机間巡視し、3分の1くらいの解答が出たところで、周囲の生徒どうして確認しあう時間を少しとる。その後、解答できている生徒を指名して答えさせ、解説を加える（解答プリントはまだ配布しない）。

②「問1 東京が開催地になるための戦略」を考えさせる（5～10分）

9人の選考委員全員の評価順位を知っていると仮定したうえで、だれをどのように説得すればよいかを考えさせる。

問題解決について

問題（オリンピック開催地投票）

2016年オリンピックの開催地が、決定する日が来た。
最終選考に残った候補地は東京（日本）・リオデジャネイロ（ブラジル）・シカゴ（アメリカ）・マドリード（スペイン）であった。
A～Iの9人の選考委員が投票して決める。
ルールは「9人が開催地を一つずつ書いて投票し、過半数を超えた候補地が出たら決定。どの候補地も過半数を超えてないときは、得票の一番少ない候補地を落選とし、残りの候補地で再投票し、過半数を超える候補地が出るまで続ける。」である。
選考委員9人の四つの候補地についての評価順（1位～4位）は以下の通りとする。

	A	B	C	D	E	F	G	H	I
東京	2	3	2	4	4	4	2	2	1
リオデジャネイロ	3	4	1	1	1	1	4	4	3
シカゴ	1	1	4	3	3	2	3	3	2
マドリード	4	2	3	2	2	3	1	1	4

審査員は、選考対象の候補地の中で最も評価の高いところに投票するとする。
さて開催地はどこになるでしょう。

（前問と同じ条件）

選考委員9人の四つの候補地についての評価順（1位～4位）は以下の通りとする。

	A	B	C	D	E	F	G	H	I
東京	2	3	2	4	4	4	2	2	1
リオデジャネイロ	3	4	1	1	1	1	4	4	3
シカゴ	1	1	4	3	3	2	3	3	2
マドリード	4	2	3	2	2	3	1	1	4

問1 このままでは東京は負けてしまいます。
どうすれば開催地になれるでしょうか？

問2 リオデジャネイロが開催地になるにはどのような作戦がいいのでしょうか？

▲問題プリント

- ③指名して答えさせる。その後、全員で検証してみる
（第1回投票・第2回投票・最終投票の結果、東京が開催地になったかを教師が解説検証）
※間違った解答が多く出ることもある。その場合も、
どこが開催地になるかを確認する。意外な結果もあり得るので、間違った解答に期待する面もある。
- ④「問2 リオデジャネイロが開催地になるための戦略」を考えさせる

（②と同様に時間をとってもよいが、1時間完結にする場合は、2～3分時間をとった後、⑤に移る）

解答プリント・解説プリント配布

解答プリントで③④の確認をした後、解説プリントを読み、オリンピック開催地投票ルールの性質を説明

まとめ

オリンピックの開催地投票ルールと、通常の多数決との違いを考察させる

■4 生徒の反応

最初の問題は多くの生徒が解答できていたが、問1や問2になると、勘で答えを出すだけの生徒が多くなったようである。どのように解決すればよいかのポイント（その審査員にとって、より上位の候補地が選ばれることをねらった説得）がわかりにくかったようであるが、まあまあ楽しそうに考えていた。

ちなみに、解説プリント（→p. 5）の最後の問題の答えは以下の通りである。

「まともにやるとシカゴになるよ」と言って、1位

票のなかでシカゴよりはマドリードがいいと思っているC、D、Eをマドリードに投票させ、早い段階でリオデジャネイロを落選させる。
（この答えはプリントに載せず、「各自、考えてみよう！」と言って終了）

○開催地はどこになるか？

(解答)

第1回目投票	東京・・・1 (I)	
	リオデジャネイロ・・・4 (C,D,E,F)	
	シカゴ・・・2 (A,B)	
	マドリード・・・2 (G,H)	(東京が落選)
第2回目投票	リオデジャネイロ・・・4 (C,D,E,F)	
	シカゴ・・・3 (A,B,I)	
	マドリード・・・2 (G,H)	(マドリード落選)
(東京がなくなったのでIは2位のシカゴに投票)		
第3回目投票	リオデジャネイロ・・・4 (C,D,E,F)	
	シカゴ・・・5 (A,B,G,H,I)	(シカゴに決定！)
(東京・マドリードがないのでG、Hは3位のシカゴに投票)		

(1) 東京オリンピック開催の秘策

(解答)

GかHのどちらか一人に、一回目から東京に投票してもらう。
 ○ マドリードの開催は不可能であると思われる。
 ○ このままではシカゴになる。それよりは2位の東京がよいのではないかと説く。

(仮にGを説得したとする。Gが一回目から東京に投票)		
第1回目投票	東京・・・2 (G,I)	
	リオデジャネイロ・・・4 (C,D,E,F)	
	シカゴ・・・2 (A,B)	
	マドリード・・・1 (H)	(マドリードが落選)
第2回目投票	東京・・・3 (G,H,I)	
	リオデジャネイロ・・・4 (C,D,E,F)	
	シカゴ・・・2 (A,B)	(シカゴ落選)
(マドリードがなくなったのでHは2位の東京に投票)		
第3回目投票	東京・・・5 (A,B,G,H,I)	
	リオデジャネイロ・・・4 (C,D,E,F)	(東京に決定！)
(シカゴがないのでAは2位の東京に投票)		
(シカゴ・マドリードがないのでBは3位の東京に投票)		

(2) リオデジャネイロオリンピック開催の秘策

(解答)

第一回目でC,D,E,Fの誰か一人がわざと東京に入れる。
 とにかくシカゴを早く消す。次に東京を消す。

(仮にCが第一回のみ東京に投票するとする。)

第1回目投票	東京・・・2 (C,I)	
	リオデジャネイロ・・・3 (D,E,F)	
	シカゴ・・・2 (A,B)	
	マドリード・・・2 (G,H)	(三つが同点)

(※ 注) 実はこのとき、どうするのかの本当のルールを私は知らない。まだリオデジャネイロも過半数を超えてないので決定にならないだろう。多分、リオデジャネイロ以外の3候補地の一つを落とす予備選挙が行われるのではないかとと思うので、ここではそのルールでいく。あしからず。

予備投票 (2票で並んだ3候補のうちの一つを落とす。)

ここでリオデジャネイロを除く3候補のうちの一つに投票するわけだがFは(リオデジャネイロを最終的に勝たせる目的により)シカゴを落とすためにあえて4位の東京に入れる。すると

東京・・・3 (C,F,I)	
シカゴ・・・2 (A,B)	
マドリード・・・4 (D,E,G,H)	(シカゴ落選)

▲解答プリント(p. 5 へ続く)

第2回目投票

リオデジャネイロの立場では今度は東京を落としたい。しかし今回は、特別に秘策を使わなくても大丈夫

東京・・・・・・2 (A,I)
 リオデジャネイロ・・・4 (C,D,E,F)
 マドリード・・・・・・3 (B,G,H)

(東京落選)

(シカゴがなくなったのでAは2位の東京,Bは2位のマドリードに投票)

第3回目投票

リオデジャネイロ・・・6 (A,C,D,E,F,I)
 マドリード・・・・・・3 (B,G,H)

(リオデジャネイロに決定!)

(東京・シカゴがないのでA、Iは3位のリオデジャネイロに投票)

▲解答プリント(p. 4 の続き)

このように、オリンピックの開催地を決める方法は最初の方は1位の多いほうが票を伸ばすが、最終決定の投票になると3、4位の少ないほうが優位になるルールである。結局、最後の投票でどの相手との戦いになれば勝てるかを考えて、秘策を練ることがポイントである。

例えば東京はリオデジャネイロには勝つが、シカゴ、マドリードには負ける。

	A	B	C	D	E	F	G	H	I
東京	2○	3○	2	4	4	4	2○	2○	1○
リオデジャネイロ	3	4	1○	1○	1○	1○	4	4	3

○・・・勝ち 東京5－4リオデジャネイロ

	A	B	C	D	E	F	G	H	I
東京	2	3	2○	4	4	4	2○	2○	1○
シカゴ	1○	1○	4	3○	3○	2○	3	3	2

○・・・勝ち 東京4－5シカゴ

	A	B	C	D	E	F	G	H	I
東京	2○	3	2○	4	4	4	2	2	1○
マドリード	4	2○	3	2○	2○	3○	1○	1○	4

○・・・勝ち 東京3－6マドリード

同様にリオデジャネイロは、マドリードには勝つが、東京、シカゴには負ける。

シカゴは東京、リオデジャネイロには勝つがマドリードには負ける。

マドリードは、東京、シカゴには勝つがリオデジャネイロには負ける。

よって、各候補地は最終投票の相手に

東京は・・・・・・リオデジャネイロ

リオデジャネイロは・・・マドリード

シカゴは・・・・・・東京かリオデジャネイロ

マドリード・・・・・・東京かシカゴ

を残すことを基本に作戦を立てなければならない。

ここで意外と苦しいのはマドリードである。最後の相手がリオデジャネイロでさえなければいいのだが、リオデジャネイロは1位票を四つも持っている。早い段階で落選させることが難しいからである。どうすればいいだろう？

▲解説プリント

座学と実習を取り入れた 音のデジタル化の授業

北海道帯広緑陽高等学校 前田 健太郎 先生

科目：情報A（必修2単位）
内容：情報の収集と問題解決
クラス：5クラス 各40名 1年生
時間：5時間
時期：9月～10月

1 ねらい

情報の授業をするうえで、生徒の興味・関心・理解度を高めるために、実習を活用することが効果的と考えている。しかし自分の勉強不足から、音のデジタル化については座学による説明が中心であった。

平成19年度におこなわれた研修で、札幌篠路高校の鶴間伸一先生から Acid Express というフリーソフトウェアを教えていただいた。生徒が実習を通して主体的に活動するなかで、このソフトウェアを使って、音のデジタル化の理解度をもっと高めることができるのではないかと考えるようになった。

そこで、プリントで作業しながら、デジタル化のしくみの理解度を高められるよう、授業内容を変更することにした。さらに、デジタル化された音声ファイルを編集して作品をつくり、その技術を本校の文化祭でおこなわれているパフォーマンス(創作ダンスのようなもの)の曲の作成にも活用できるようにした。

指導計画(計5時間)

音のデジタル化のしくみとデータ量	1時間
CDの取りこみと Acid Express による編集	3時間
MIDIのしくみと Sakura による作成	1時間

なお、本校ではこの授業の前に、コンピュータで扱う情報の量(単位)や、2進数について説明をしている。

2 準備

必要なソフトウェア

- ・ Windows Media Player
- ・ Acid Express(音楽編集ソフトウェア)
- ・ サクラ(作曲ソフトウェア)

生徒各自で用意するもの

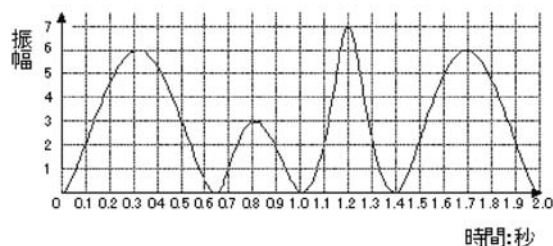
- ・ CD
- ・ イヤホンまたはヘッドホン

3 実践内容

(1) プリントによる音のデジタル化のしくみの理解と定着

音をデジタル化する方式の1つである PCM 方式では、標準化→量子化→符号化という流れでデジタル化していることを説明する。説明だけだと生徒の理解度を確認できないので、次のようなプリントで問題演習をおこない、理解度の確認をしている。

問：次のアナログ音声のデータをデジタル化しよう。ただし、周波数は10Hz、量子化のビット数は3ビットとする。



秒	振幅	ビット
0. 1		
0. 2		
0. 3		
0. 4		
0. 5		
0. 6		
0. 7		
0. 8		
0. 9		
1. 0		

なお、プリントの0.2秒の振幅の値は4と5の間であるが、この場合は4か5のどちらかになることも確認する。

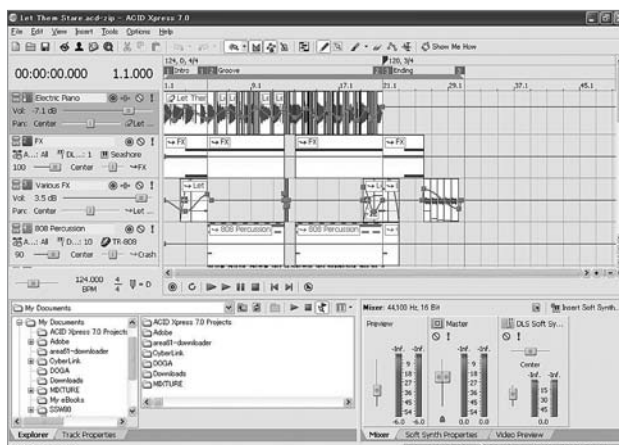
(2) PCM 方式の音声ファイル編集の実習

この実習を取り入れた理由は、デジタル化のしくみを座学だけで学んでも興味・関心をもってもらえないのではないかとということ、デジタル化したファイルは編集が容易で、先に述べたように文化祭で活用できると考えたこと、また作業画面から音を波形で見ることができるからである。

実習の作業は、まず Windows Media Player を利用して CD の曲を取りこむところからはじまる。なお、CD とイヤホン（ヘッドホン）は学校に必要な数がないので、生徒各自が持参する。事前に教員が編集した曲を聴かせておき、どのような曲がよいか、または編集したいか、生徒に考えさせておく。

なお、曲については、著作権があることやその例外規定（私的使用のためのコピーなど）があることを事前に指導している。今までこの件で問題を起こしていることはないが、今後はもっと詳しく指導する必要があるのではないかと考えている。

取りこんだ曲は Acid Express で編集する。例を通しておもな操作を生徒に見せるとともに、プリント 1 枚にまとめた操作方法の資料を配布し、後で生徒が操作方法を確認できるようにしている。



▲ Acid Express の画面

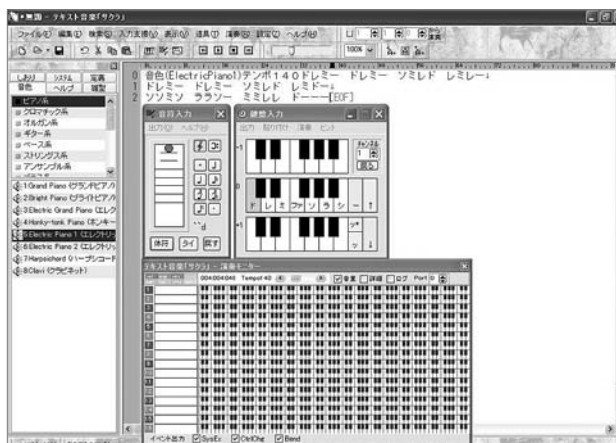
なお、編集の際に LoopSound（フレーズや曲の一部をパターン化した音声素材）のファイルがあるとアレンジが容易なことから、教員がいくつかのファイルを事前に用意するとともに、教育用であれば自由に使用できる素材が用意されたウェブサイトを紹介して、生徒がダウンロードして利用できるようにしている。

(3) MIDI 方式の音声ファイル編集の実習

次に MIDI 方式の音声ファイルについて、説明と実習をおこなっている。

MIDI を知っている生徒は少ないが、通信カラオケなどで現在も使用されていることを伝える。また、音源をコントロールして演奏できることや、音を数値化することでデータ量が小さくできるため、通信でデータを送るのに好都合であるという特徴を説明している。

生徒の実習では、音階や音符で入力できるサクラというフリーソフトウェアを用いている。また、打ちこむ曲として、だれでも知っていそうな曲（クラシックや校歌など）の楽譜を用意している。



▲ サクラの画面

4 結果と反応

デジタル化のプリントの演習では、一部の生徒が 10進数を 2進数に変換する方法を忘れていたので、その方法を復習した。また、考査では同様の出題をしており、正確な数値は調べていないが、8割程度の正解率だったのではないかと思います。

実習では、生徒はとても意欲的に取り組んでいる。なかには自宅でも趣味的におこないたいと希望する生徒もあり、関心の高さを感じている。

また、文化祭で使うときには、CD への保存方法以外では質問されることはなく、ねらいどおり活用されていると考える。

■ 評価基準

座学で学んだ音のデジタル化については、定期考査で出題して、理解（定着）度を評価に入れている。

実習では、Acid Express による編集では最低限の編集作業を、サクラによる打ちこみは、最低限の打ちこむ曲の範囲を指定して、その条件を達成していれば実習点を与えている。音楽の授業ではないことから、作品の出来については評価していないが、意欲的な態度で取り組んでいることを評価する方法も含むべきと感じている。しかし客観的な評価方法が確立できず、改善にはいたっていない。

5 資料

Acid Express

（著作権者：Sony Creative Software, Inc.）

<http://www.acidplanet.com/>

サクラ（著作権者：クジラ飛行機）

<http://oto.chu.jp/tools/>

暗号化と復号

長野県須坂商業高等学校 原 周一郎 先生

科目：ビジネス情報（教科「商業」）
 内容：IT パスポート試験範囲
 情報セキュリティ 「暗号化と復号」
 クラス：情報スペシャリストコース 12名 2年生
 時間：1時間
 時期：6月中旬

1 ねらい

本校では2年次よりコース制を導入しており、この授業は「情報スペシャリストコース」の生徒を対象に実施したものである。情報スペシャリストコースは4科目9単位で授業を展開しており、ITパスポート試験の内容、表計算ソフトウェアやデータベースの利用などを中心に学習を進めた。

今回は、ITパスポート試験の範囲である「情報セキュリティ」「暗号化と復号」の授業を、科目「ビジネス情報」で実践した報告をおこなう。前時までに情報セキュリティに関する説明は終了しており、情報セキュリティポリシー、アクセス権、アクセス制御、ID、パスワードといった用語については説明済みであることを前提とする。

この「暗号化と復号」は理解に時間のかかる生徒が比較的多く、イメージをつかませながら授業展開をすることが必要である。したがって、授業で利用するスライドにもイラストや図解を多く用いるなどの工夫をしている。また、スライドと同様の授業用プリントを作成し、重要な用語や説明などを記入させ、書く・聞く・考えるという要素を多く取り入れることを意識して教材を作成した。さらには、授業の後半部分にITパスポート試験レベルの練習問題を準備し、その理解度を確認できるようにした。

2 準備

- ・授業用プリント（Microsoft Word で作成）
- ・授業用スライド（Microsoft PowerPoint で作成）
- ・プロジェクタ
- ・『ITパスポート学習テキスト』（実教出版）

3 実践内容

(1) 前回までの復習（3分）

前回までに学習したアクセス権やアクセス制御、ID、パスワードなどの内容について確認する。

(2) 暗号化と復号（5分）

インターネット社会における「暗号化と復号」の必要性・重要性について説明し、暗号化の意味やルールについて説明をする。

(3) 共通鍵暗号方式（秘密鍵暗号方式）（5分）

スライドのイラストを利用して、共通鍵暗号方式のしくみについて説明する。共通鍵暗号方式の特徴として、扱いが簡単であり処理速度が速い反面、相手ごとに固有の鍵を作成しなければならないこと、あらかじめ安全な方法で相手に鍵を渡さなければならないことから、限られた特定の相手とのやりとりに向いていることを理解させる。

(4) 公開鍵暗号方式（7分）

公開鍵暗号方式では公開鍵と秘密鍵のペアを使い、一方の鍵で暗号化した情報は、もう一方の鍵を使わないと復号できない点、公開鍵の共有は容易で、相手の数に関係なく公開鍵は1つでよいなど、鍵の管理が容易で安全性が高い点について理解させる。

また、電子証明書で公開鍵暗号方式の知識が必要になることにも留意して指導すべきである。

(5) 電子証明書（10分）

公開鍵暗号方式を利用した場合の、なりすましによる被害の危険性について説明し、信頼できる第三者（認証局）が間違いなく本人であると電子的に証明するものであることを理解させる。印鑑証明書にたとえられることが多い。

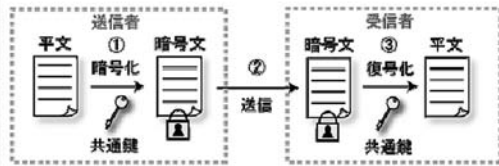
(6) 電子署名（デジタル署名）（10分）

紙文書における印やサイン（署名）に相当する役割をはたすものであることに留意させ、おもに本人確認、偽造・改ざん防止のために用いられることを理解させる。しくみが難しくなり、理解に時間のかかる生徒が増えることが考えられるため、説明には十分時間をかける必要がある。さらに、ハッシュやメッセージダイジェストのイラスト部分にアンダーラインを引かせるなど、生徒の手を動かす機会を増やしながら、そのしくみについても説明する。

共通鍵暗号方式(秘密鍵暗号方式)

共通鍵暗号方式では、暗号化と復号化に同じ鍵を用いる。
鍵の情報を秘密に管理することが重要。

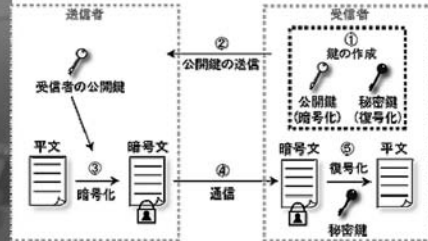
- ①暗号化する前の平文を用意し、共通鍵によって平文を暗号化する。
- ②暗号化された暗号文を相手に送信する。
- ③受信者は、暗号文を暗号化する際に用いた鍵と同様の共通鍵を用いることにより、暗号文を平文に復号化する。



公開鍵暗号方式

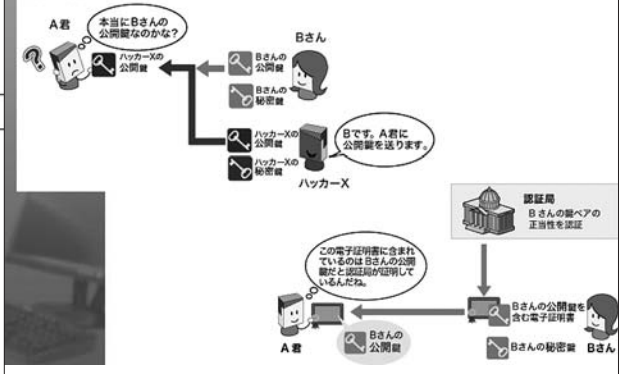
送信者は、受信者が公開した公開鍵で暗号化
受信者は、自分の秘密鍵で復号する。

- ①受信者は、作成した公開鍵を送信者に送信する。
- ②送信者は、受け取った受信者の公開鍵を用いて、平文を暗号化する。
- ③送信者は、公開鍵で暗号化した暗号文を受信者に送信する。
- ④受信者は、受け取った暗号文を、秘密鍵を用いて復号化する。



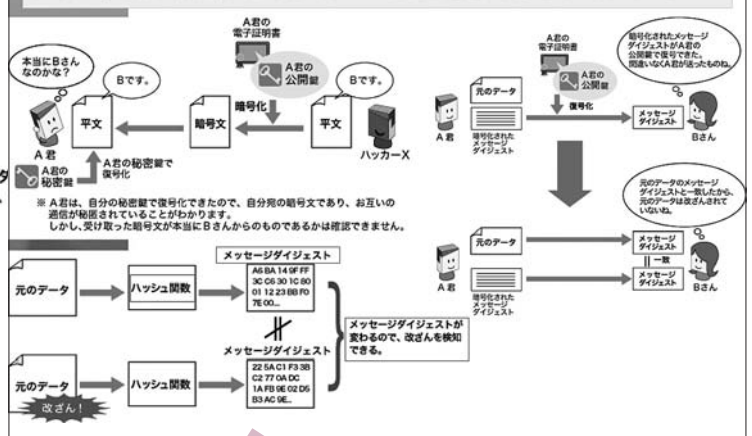
電子証明書

電子証明書を使わない場合...



電子署名(デジタル署名)

デジタル署名は公開鍵暗号方式とハッシュの仕組みを組み合わせで作られている



スライドと内容を対応させたものを、生徒用に用意している。
生徒のようすを見ながら、必要に応じて、スライドの表示以外にも線を引かせたり、メモをとらせたりしている。

(7) SSL (3分)

SSLにより、インターネットで広く使われているWWWやFTPなどのデータを暗号化し、個人情報や、企業秘密などを安全に送受信できることを理解させる。

(8) 問題演習 (5分)

問題演習により授業の理解度ををはかる。生徒のようすを見ながら解答と解説をおこなう。

初級シスアド H20年春期 午前問題

公開鍵暗号方式を用いて、図のようにAさんからBさんへ、他人に秘密にしておきたい文章を送るとき、略号化に用いる鍵Kとして、適切なものはどれか。

ア Aさんの公開鍵
イ Aさんの秘密鍵
ウ Bさんの公開鍵
エ 共通の秘密鍵

```
graph LR
    A[Aさん] -- "鍵K2によって暗号化" --> Enc["'nd559f xj47 ac...'" ]
    Enc -- "ネットワーク" --> Dec["'nd559f xj47 ac...'" ]
    Dec -- "Bさんの秘密鍵 K1によって復号" --> B[Bさん]
```

初級シスアド H20年春期 午前問題

公開鍵暗号方式を採用した電子商取引において、取引当事者から独立した第三者機関である認証局(CA)が作成するものはどれか。

ア 取引当事者の公開鍵に対する電子証明書
イ 取引当事者のデジタル署名
ウ 取引当事者のパスワード
エ 取引当事者の秘密鍵に対する電子証明書

(9) まとめ (2分)

本時のまとめを簡単におこなう。

4 結果と反応

生徒が理解しにくい単元の授業であったため、説明に多くの時間を費やした。その結果、練習問題の正解率が高く、生徒の反応もよかった。しかしながら、この後、次の単元へと授業が進むにつれて理解度が低下してしまう生徒が多く、9月から情報処理検定1級「ビジネス情報」部門(全国商業高等学校協会主催)の学習をおこなった際には、再度、時間をかけて説明しなければならなかった。この時間内での問題演習のみでとどめてしまったが、定期的に問題演習をおこない、定着をはかる授業計画の必要性を感じた。

最後に、年間を通じた指導上の留意点などについて触れておく。本校ではコース制を導入しているため、1年次には「ビジネス基礎」「簿記」「情報処理」を必修科目として履修するが、2年次からは各コースの学習が中心となり、情報スペシャリストコース選択者は「会計」や「原価計算」「マーケティング」といった科目の学習をおこなっていない。ITパスポート試験は、商業高校で学ぶ簿記会計、経営情報をはじめとした多くの科目を網羅した知識が必要であり、その範囲は情報処理の学習だけにとどまらない。したがって、簿記会計や原価計算、マーケティングにいたるまでを指導計画に盛りこんでいく必要がある。また、論理的な思考力が必要とされる場面があるが、この点については表計算ソフトウェアやデータベースの学習を並行しておこなうことにより、ある程度養うことができたのではないかと考えられる。

5 参考資料

■参考文献

『ITパスポート学習テキスト』(実教出版)

『パソコン・IT用語辞典』(技術評論社)

■参考ウェブサイト

日本ペリサイン

<https://www.verisign.co.jp/>

共通鍵暗号方式と公開鍵暗号方式の概要

<http://mikilab.doshisha.ac.jp/dia/research/>

report/2005/0909/005/report20050909005.html

総務省 国民のための情報セキュリティサイト

http://www.soumu.go.jp/main_sosiki/joho_

[tsusin/security/](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/)

初級シスアドなどITのお役立ちサイト

<http://www.pursue.ne.jp/>

ネットワークとセキュリティについて具体的理解の試み

島根県立松江北高等学校 下垣 章裕 先生

科目：情報C（必修2単位）
 内容：ネットワークのしくみとセキュリティ
 クラス：普通科7クラス，理数科1クラス
 各40名 1年生
 時間：5時間
 時期：10月～12月

■ 1 ねらい

情報通信の技術が次つぎと開発され，めまぐるしく変化する情報社会では，ネットワークとセキュリティに関する知識が必要不可欠である。「情報C」はその入門書として優れた教材であるが，この分野は，生徒にとって関わる機会が少なく，イメージ化が困難で，教えるにくいところでもある。

そこで，実際に情報機器や部品を見せたり，さまざまな視覚に訴える教材をさがしたりして，基本的な概念の理解とイメージの取得を進める工夫を取り上げてみた。

本校では，1年次と2年次に1単位ずつに分けて情報Cを学ぶ。1年次では基礎的・導入的内容に絞り，飽きさせないように学期のなかに座学と実習を交互に取り入れている。座学については，生徒にとって身近で親しみやすい題材である，メール・パケットなどの情報通信に関わる内容からは始めている。

■ 全体のカリキュラムの中での位置づけ

1 学期	- 情報のデジタル化，効率的な情報通信 - 実習：ワードプロセッサ「タッチタイピングに挑戦」 - 実習：プレゼンテーションの基礎
2 学期	『ケーススタディ情報モラル』併用 - コミュニケーションモラル(おもにメール) - ネットワークのしくみとセキュリティ - 実習：表計算ソフトウェア(基本的な関数を中心に)
3 学期	『ケーススタディ情報モラル』併用 - 情報の管理と保護 - 演習：著作権

今回扱うのは，「ネットワークのしくみとセキュリティ」(配当時間5時間)である。その前に学習した「コミュニケーションモラル」の項で，パスワード・メール・パケットについてはすでに取り上げているので，教科書指導資料にある配当時間よりも少ない時間になっている。

■ 2 準備

- ・パソコン教室のパソコン・プリンタ，準備室のサーバ，UPS(無停電電源装置)
- ・ツイストペアケーブル，光ファイバケーブル，USBケーブル
- ・小型ハブ，スイッチングハブ，ルータ
- ・NIC(ボード式，カードスロット式)
- ・糸電話(糸，紙コップ)
- ・廃棄パソコン(デスクトップ式)
- ・コンピュータウイルスに関する映像教材(テレビ番組の特集を録画したVTR)
- ・レターBOX(レポート提出などに使う，引き出しが多数ついたもの)
- ・授業用プリント(教科書併用穴埋め問題と板書書き取りスペースのついたもの)

■ 3 実践内容

(1) 通信方式の移り変わり

- ・『ケーススタディ情報モラル』事例3「パケット代」でパケットの復習をしながら，パケット交換方式の利点について学ぶ。

(2) 情報伝達におけるプロトコル

- ・糸電話を使ってプロトコルの例を示す。
 - 1層：ネットワーク・インタフェース層
回線に使う糸は，どんな種類・太さにするか。
 - 2層：インターネット層(IP)
電話機として，どのコップ(紙製／ポリ製)を使うか。糸をどのように取りつけるか。コップをだれのところに置くのか。
 - 3層：トランスポート層(TCP)
「相手が話すときはコップを耳に当てて聞く」，「ひと通り話したら聞き手と交代する」などのマナー。
糸はピンと張って使う。一方が英語，他方が日本語を用いると会話が成立しない。
- ・『ケーススタディ情報モラル』のパケットの項が，教科書のTCPの項と結びつけて説明しやすい。

(3) LAN

- ・パソコン教室のしくみを見ながら、クライアントサーバシステムを説明する。
- ・「前日と異なるパソコンを起動してもなぜ同じ画面が出るのか」「パソコンは40台あるのに、どうしてプリンタは4台ですむのか。プリンタのケーブルは1本しかないけど大丈夫か」などの問いかけからはじめる。
- ・ツイストペアケーブル・光ファイバケーブルは、廃棄されたものの保護を切ってはがし、中身を見せる。
- ・NICの例として、廃棄パソコンから取り出したボードや、昔のカードスロットを見せるとわかりやすい。時間があればネットワークの歴史にも触れる。
- ・ハブとルータは予備の機器を見せる（実際に使用している場所を知らせるといわずらされる恐れがあるため）
- ・それぞれの機器などが、先に学んだプロトコルの、どの階層に対応するのかも考えさせる。

(4) インターネットのサービス

- ・教員用パソコンの画面を生徒全員に送信する。そのうえでプリンタのインストールを実行して、ポート

の選択画面の一部を見せ、IPアドレスによりLAN上に割り当てられていることを示す。

- ・メールのアカウント設定画面を見せて、メールアドレス、SMTP、POPを説明する。
- ・『ケーススタディ情報モラル』事例8「なりすまし」にヘッダの説明がある。復習を兼ね、これを利用してSMTPを説明する。
- ・SMTPとPOPの説明には、郵便局や宅配便、レターBOXを用いる。

(5) セキュリティの重要性

① パスワードの管理

- ・『ケーススタディ情報モラル』事例1「パスワード」を用いて、パスワードの復習をする。

② コンピュータウイルス対策

- ・生物の「ウイルス」とは異なり、害を及ぼすことを目的につくられたプログラムであることを、テレビ番組から録画したコンピュータウイルスの映像を見せることで示す。
- ・『ケーススタディ情報モラル』事例19「コンピュータウイルス/スパイウェア」をまとめに利用する。

ネットワークのしくみとセキュリティ(1)

ネットワークのしくみ P.72 ~ P.81

1 情報伝達におけるプロトコル

会話におけるコミュニケーションの場面を考えてみよう。お互いが理解しあうためには、いくつかの約束が必要である。このような、情報伝達における約束ごとを(1)プロトコルという。インターネットでは、(2)TCP/IP)とよばれる(1)プロトコル群にもとづいてデータの送受信を行っている。(3)TCP)と(4)IP)の2つの(1)プロトコル)を組み合わせた通信方法である。

(4)IP)の役割は、インターネットに接続するコンピュータや機器に固有で割り当てられた(5)IPアドレス)という番号を用いて、(6)ルーティング)（経路選択)を行い、(7)パケット)をやり取りすることである。ただし、(4)IP)は、通信途中で(7)パケット)が消失したり、データに(8)誤り)が発生しても、(8)誤り)を訂正することはない。

これに対して、(3)TCP)の役割は、データの正確性を保証することである。具体的には、送り出すデータを(7)パケット)に分割したり、受け取った(7)パケット)を順番どおりに並べ(7)パケット)の抜けやデータに誤りがある場合、データを再び送ってもらい、データを完全な形に仕上げる役割を果たしている。

2 LAN

学校や会社などの限られたせまい範囲で、コンピュータや周辺機器を接続したネットワークを(LAN)という。(1)LAN)では特定の業務に連したコンピュータに仕事を分散させて、効率よくコンピュータを利用する(2)クライアントサーバシステム)を構成している場合が多い。このシステムは、サービスを要求する(3)クライアント)というコンピュータと、(3)クライアント)からの要求に応じてサービスを提供する(4)サーバ)というコンピュータからなる。(4)サーバ)が提供するサービスにはいろいろな種類がある。また、(1)LAN)どうしをひろい範囲でむすんだものを(WAN)という。(5)WAN)では、(1)LAN)と(1)LAN)の間を一般に公衆回線で接続している。

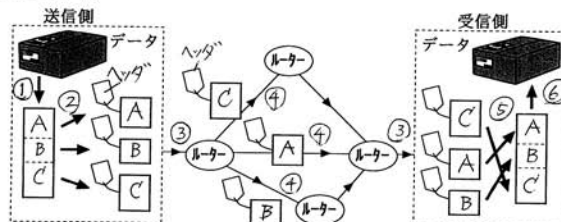
◎情報伝達の階層構造

プロトコル

系電話のプロトコル	
話す	話すときはコップを口に、聞くときは耳に。糸を張って話す
電話機	コップの種類、つなぎ方
回線	どんな糸にするか(種類、太さ)

4層 アプリケーション層	SMTP, POP, HTTP
3層 トランスポート層	TCP
2層 インターネット層	IP
1層 ネットワーク・インターフェイス層	

◎TCP/IP



TCPの役割

- ・データをパケットに分割(①, ②)。パケットと元のデータにもどす(⑥)。
- ・届いたパケットを並び変える(③)。
- ・エラーの検出・訂正。送受信のチェック

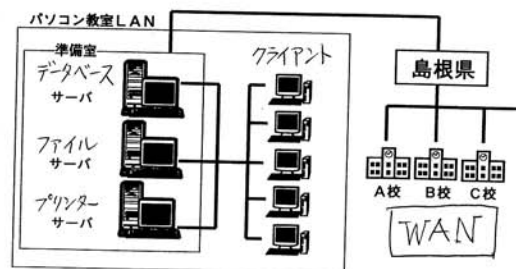
IPの役割

- ・パケットA, B, Cがどのルートを通るか選定(④)。
- ・パケットに宛先と送信側のアドレスを付けた(③)。

◎LAN

クライアントサーバシステム
クライアント：要求する人

サーバ：与える人、サービスする人



③情報の暗号化

- 教科書にある暗号化の例題は、アルファベットの文字を1つずつずらすというものである。これを実際に「鍵」ということを意識してやって見せる。
(例) 任意の8桁の2進数に、鍵となる2進数を加算する。

1000 1101 ……データ
+ 0000 0001 ……鍵

1000 1110 ……暗号

④管理者がすべきこと

- 教員用パソコンの画面を生徒全員に送信する。そのうえでウイルス対策ソフトのメイン画面を起動し、ファイアウォール・アクセス制御などが設定できるようになっていることを示しながら、説明する。
 - UPS(無停電電源装置)は実物を見せる。
- ※多数の専門用語が出てくるので、教科書併用副教材を利用して、穴埋めと板書記述スペースのあるプリントを作成し、それをノートがわりにして授業を進めている。

■ 4 結果と反応

同様のカリキュラムで授業を実施した2年前にくらべて、今年度は具体的な理解の試みを多く導入したため、生徒たちの反応もよく、大半の生徒が興味と集中を切らすことなく授業を送ることができたように感じる。定期考査においても、過去より難易度を上げたにも関わらず、得点結果はよかった。

生徒による授業評価の集計結果から、以下の質問項目に対して肯定的な解答(「そう思う」と「だいたいそう思う」)の占める割合を示す。

質問	割合
①授業を受けることで、学習内容への興味・関心が一層高まりましたか。	90%
②先生の板書やプリントなどは、見やすく整理されていますか。	72%
③総合的に考えて、この授業の内容を理解できましたか。	69%
④先生の取り組みは熱心で、授業に対する熱意を感じますか。	66%
⑤あなたは、この授業に意欲的に取り組んでいると思いますか。(先生の話を中心して聞く、質問する、きちんと質問に答えるなど)	64%

質問	割合
⑥先生がする実習や生徒実習はあなたの理解を深めることに役立っていますか。	64%
⑦先生の説明や指導方法には工夫が感じられますか。	61%
⑧先生の説明の仕方はわかりやすいですか。	51%

週1時間で、情報通信に関する多数の事項を扱う授業としては、まずまずの評価を得られたのではないかと考える。①と③を見ると、ねらい通りに生徒たちは最後まで興味を失うことなく取り組んでくれたことがわかる。しかし、時間をかけて工夫した⑦と⑧が、もっとも低い評価であったことは、十分に反省しなければならない。「これも知っておいてほしい」という思いが強い分、配当時間の割に内容が盛りだくさんになり、説明を急ぎすぎたことが原因と考えられる。また、私自身の問題として、専門である物理の授業と同じスタンスで授業を進めてしまったこともよくなかったと感じている。

■ 5 最後に

私は、校内の情報管理をまかされたことを契機に、初級システムアドミニストレータと基本情報技術者の資格を取得した。その受験会場で、さまざまな職種から実に多くの社会人が受験することに驚き、普通科高校で学ぶ生徒たちであっても、将来はネットワークとセキュリティに関する知識が、職種によらず必要になる可能性が高いと感じた。今回の実践報告には、この体験と強い反映されている。

ただし、資格を取らせることが目的ではない。ネットワークの発展にともない、新しいサイバー犯罪や不正行為が次つぎとあらわれている。これらに対して、対処療法的な指導に留まらず、生徒がみずから考え判断できる力を身につけるためには、きちんとした理解は必要不可欠だと考える。

■ 6 資料

- 『最新情報C』(実教出版)
 - 『ケーススタディ情報モラル』(第一学習社)
- 『ケーススタディ情報モラル』で扱う事例は、いずれも2学期の「コミュニケーションにおけるモラル」学習時に利用しているので、生徒には復習となり、親しみやすい。

副読本を利用した 情報モラル教育

大阪府立北野高等学校 中島 啓介 先生

科目：情報C（必修2単位）
内容：掲示板（情報発信の注意点）
クラス：8クラス 各40名 1年生
時間：35分(65分中)
時期：5月下旬

■ 1 ねらい

新入生に毎年実施しているアンケートによると、本校では、携帯電話の個人所有率と家庭でのパソコン所有率がほぼ100%である。この現状をふまえ、情報科では、授業の目的を以下の2つとしている。

- ①犯罪に巻きこまれない，犯罪を犯さないための知識の習得（安心・安全なネット生活のための知識）
- ②すべての教科で利用可能なスキルの習得

IT 機器が使われる犯罪は，基本的な知識があればほぼ防げ，意図せず加害者になることも回避できる。犯罪回避に使える知識は，できるだけ早くに身につける必要がある。

年間計画では，情報モラル教育を前期の柱としている。授業は自作プリントでおこない，必要に応じて教科書や副読本，ウェブサイトなどを参照している。

なお，本校は前後期制，1コマ65分授業のため，2週間で3コマの進度である。また，各時間は前半が講

義，後半は実習にあてることが多い。

2009年度の前期授業では，副読本（『ケーススタディ情報モラル』）を利用する機会が多かった。p.15の年間授業実績表中の参考事例番号は，副読本における対応事例番号である。

副読本を多用するのは

- ・新しい話題がある
- ・生徒に身近な例示がある
- ・漫画やイラストが多く親しみやすい
- ・見開き1テーマのため利用しやすい

ことなどが理由である。

改訂に時間がかかる教科書と異なり，プロフなどの新しいしくみの紹介もあるので，注意すべき点などを早めに指導できる利点がある。また，パスワードのつくり方の例があるなど，「～してはいけない」ではなく「～してはどうか」といった前向きな提案があり，指導しやすい。

過程	学習活動	指導内容	留意点
準備		掲示板の準備（匿名投稿可）	
導入 (5分)	開始前：タッチタイピングの自主練習 掲示板システムの提示 書きこみ経験の調査	掲示板に書きこんだ経験があるかを挙手で調査	
実習 (10分)	校内掲示板への書きこみ練習	「匿名」掲示板に1人最低1回は書きこむよう指示 書きこみがすぐに全員で共有できることを体験する 多数の人に意見表明できる道具としての有効性を認識 1つのテーマについて意見交換できる特性を確認	はじめに教師が書きこむ 書きこみ内容をこまめにチェック 書き込みが一巡し「なりすまし」などが発生しはじめたら，書きこみを中止させる
展開 (15分)	プリント配付	『ケーススタディ情報モラル』事例2，8，12を解説 ・匿名でも捜査令状により発信者を特定できるので，被害にあったら証拠保全をして被害届を出す （捜査令状によらないで情報を開示することはない） ・ネットで公開された情報は回収不能なので，軽い気持ちで書きこんだ内容も取り消せない ・たとえ真実であっても「名誉毀損」になり得る ・匿名の書きこみでも情報の断片をつなぎ合わせて発信者が特定される場合もある	匿名掲示板での書きこみでも逮捕される例をあげる （威力業務妨害など） 別人画像が流出した事件の紹介 「個人情報」「人格権」については次回の授業で取り上げる
まとめ (5分)		「本人に直接言えないことは書きこまない」 「軽い気持ちの行動が犯罪につながる恐れがある」 「書きこみは慎重におこなうこと」	画面の向こうには「人」がいることを意識させる

▲第5時指導案(前半：講義部分)

※中島先生は2010年4月より，海陽中等教育学校(愛知県)に勤務しております。今回の報告は，前任校の北野高校で実施されたものです。

時数	講義	実習	参考事例
1	・学校のネットワーク使用法について ・利用規程の解説など	・パソコン基本操作 パスワード変更，共有フォルダなど	事例1，19，25
2	・検索エンジンについて 検索エンジンの特徴，フィルタリング	・検索実習・タッチタイプ 検索エンジンの登録・タイピング練習	事例9
3	・VDT 作業時の注意事項 ・作業姿勢・環境整備	・プレゼンスライド作成実習1 文字入力，サイズ変更など	
4	・メディアについて 情報メディアの特性など	・プレゼンスライド作成実習2 画像の挿入，アニメーション効果など	
5	・掲示板について	・掲示板実習 ・プレゼンスライド作成実習3 トリミング，画像の圧縮，動画の貼り付け	事例2，8，12
6	・人権への配慮 人格権・個人情報について	・プレゼンスライド作成実習4 画面の切り替え効果，リンクボタンなど ・校内掲示板での書きこみ実習	事例5，6，7
7	・ネット犯罪の紹介 犯罪の解説と回避方法について	・プレゼンスライド作成実習5 配付資料，ワードプロセッサへの書き出し，テーマ決め	事例4，22，24
8	・知的財産権 知的財産権概説	・電子メール実習1 メールの操作実習	
9	・著作権1 著作権とは	・電子メール実習2 メールのマナー	事例10，13
10	・著作権2 著作権の制限	・プレゼンスライド作成実習6 テーマに沿ったスライド作成1	事例15，16，17
11	・産業財産権 特許権など		
12	・情報のデジタル化1 文字情報・音声情報のデジタル化	・プレゼンスライド作成実習7 テーマに沿ったスライド作成2	
13		・スライドの相互評価	
14	・情報のデジタル化2 画像情報のデジタル化	・情報のデジタル化実習 静止画や音声の取りこみ，加工	
15	・拡張子と圧縮形式 ・ファイル形式の特徴	・グループ発表実習1 発表テーマ決め，情報収集	
16		・相互評価の確認 ・グループ発表実習2 相互評価のコメントなどのフィードバック	
17		・グループ発表実習3 発表準備	
18		・グループ発表実習4 発表1，評価	
19		・グループ発表実習5 発表2，評価	
20	定期考査ガイダンス	・グループ発表実習6 ふり返り，プレゼン修正作業	

▲2009年度授業実績(65分授業：前期20コマ)

※架空請求詐欺ではIPアドレスなどを提示して個人の情報を取得したかのように錯覚させる手口があるが，IPアドレスやパケットなどのネットワークの知識は後期に講義をおこなうので，知識を得たうえで指導する。

■2 実践内容

大阪の府立高校では，校内だけで公開できる掲示板のシステムがある。このシステムを利用した授業を紹介する。

■第5時の指導目標

情報社会に参画するうえで，情報を得るだけでなく，「情報をつくり出す」姿勢が求められる。情報を提示できる場を用意することも，情報科の活動にとって重要なことである。

ネット社会では掲示板やブログにより，個人の意見を不特定多数の人に表明できる。携帯電話やネット上の掲示板に書きこみをしている生徒もいる一方で，まったく経験のない生徒もいる。学校内の閉じた掲示板で書きこみを経験し，あわせて書きこみ時の注意事項を確認する。

なりすましなどの問題は，掲示板だけでなくメールなど個人が情報発信する場合に共通するものであることを理解する。

■ 3 結果と反応

情報モラル教育は、ネットの「影」の部分を強調しがちであるが、まず「光」の部分を理解することが重要である。便利さや楽しさを経験させて情報を発信する態度を育成したい。

この意味で、掲示板を知っていても、書きこんだことのない生徒が、はじめはおそろおそろ書きこんでいたものの、しだいに書きこみ経験者に引っ張られるかたちで、書きこみを楽しんでいたのは、ねらい通りであった。

オープンなインターネットとは異なり、学校の閉じた環境では、自由に書きこませることができる。自由にさせると、経験上、必ずなりすましや誹謗中傷などの書きこみが生まれるが、クラスメイトの書きこみを通して、その場で指導ができるため、身近な問題として知識の定着をはかることができた。

具体的には、情報モラル教育では「～してはいけない」といった加害者にならない教育が主であるが、実際には被害者になるおそれの方が大きい。しかし、被害に遭ったときの対処方法をほとんどの生徒が知らないのが現状である。

印刷したり写真に撮ったりして、証拠を残したうえで警察に相談する(被害届を出す)といったことを、みずからの書きこみ経験を通して理解させると印象に残るようで、よく定着していることが定期考査でも確認できた。

自分たちの書きこみや、副読本の具体例を通して、軽い気持ちでの書きこみが、重大な結果(何年も残り、

回収不能)を引き起こすことに驚いていた。生徒にとっては書きこみはその場だけのことであり、会話と同じ感覚で書きこんでいるが、書きこみ記録が、場合によっては何十年も残るとは意識していない。今回の実習を通じて、メディアによる特性を意識させることができたのではないかと感じている。

■ 4 伝えたいこと

情報モラル教育全般を通して伝えたいのは、「誰も見ていなくても、してはいけないことはしない」ことである。

携帯電話や個人のパソコンで、一人でも悪いことが簡単にできる情報社会において、もっとも必要な態度であると考えている。

■ 5 さいごに

情報科の取り扱う内容は多岐にわたり、授業で十分に指導できないものが残る。このような部分については、教科書を開いて自学自習することがのぞましいが、実際にはなかなか期待できない。

副読本は、マンガやイラストが多く使われ、見開きで読み切りのスタイルなので読む負担も軽い。通学中やほかの勉強の合間に気軽に読んでもらえ、知識の定着が期待できる副読本の役割は大きいと感じている。

■ 6 資料

『ケーススタディ 情報モラル ver.3』(第一学習社)

エデュカーレ

[情報 No.24]

◆ご意見・ご提案・原稿をお待ちしております。

ホームページ <http://www.daiichi-g.co.jp/>

2010年6月1日発行
定価100円(本体95円)

東京：〒102-0082	東京都千代田区一番町15番21号	☎03-5276-2700
大阪：〒564-0044	吹田市南金田2丁目19番18号	☎06-6380-1391
広島：〒733-8521	広島市西区横川新町7番14号	☎082-234-6800
札幌☎011-811-1848	仙台☎022-271-5313	新潟☎025-290-6077
つくば☎029-853-1080	東京☎03-5803-2131	横浜☎045-953-6191
名古屋☎052-769-1339	神戸☎078-937-0255	広島☎082-222-8565
福岡☎092-771-1651	金沢☎076-291-5775	