「情報の科学」の指導例

愛媛県立丹原高等学校
山之内　統文

1　はじめに

本校は、各学年とも普通科３クラス、園芸科学科１クラスで編成されている。普通科は２年次から就職・進学型であるⅠ型（文系・理系）と国公立型であるⅡ型（文系・理系）に分かれる。

情報の科目については、普通科は１年次に「情報の科学」を履修している。普通科Ⅰ型では３年次に、他教科との選択科目として商業の「情報処理」を開講している。園芸科学科においては、農業の「農業情報処理」を３～７単位履修している。

2　「情報の科学」の授業関連データ

実施学年・学科　　１年・普通科
クラス数・生徒数　３クラス・各クラス 35、36 名
使用教室　　コンピュータ教室
使用教科書　　東京書籍「情報の科学」
副教材　　東京書籍「情報の科学 学習ノート」
　　東京書籍「Word Excel PowerPoint の基本操作」

3　年間指導計画の概略

学期	教科書（理論編）	実習内容
１学期	１章 コンピュータの仕組みと働き	ワードを用いた文書作成
２学期	１章 コンピュータの仕組みと働き ２章 問題解決とコンピュータの活用	エクセルを用いた表計算
３学期	３章 情報社会の科学的な理解	パワーポイントを用いたプレゼンテーション

4　授業形態

２時間連続の授業で、基本的に１時間目は教科書の内容の説明、２時間目は実習を行っている。１時間目は指導用のディジタル教科書を利用しながら、必要なことはホワイトボードに板書して説明している。時間の最後には「学習ノート」にまとめをさせるという形式で行っている。昨年６月の情報部会研究会で、「ＮＨＫ高校講座」も教材として利用できることを知り、「情報Ａ」と「社会と情報」の番組の中で「情報の科学」の内容と共通している部分を活用したいと考え、視聴を始めた。

5　授業実践例

(1) ＮＨＫ高校講座の活用

2013 年４月からＮＨＫテレビ高校講座「社会と情報」がスタートした。この番組は

東京書籍の教科書「社会と情報」のカリキュラムに沿って制作されている。１回の放送は 20 分間で、全 20 回である。番組はストリーミング配信で視聴でき、項目ごとにチャプター分けされているので、授業の中で必要なところだけ利用できる。１回の番組は６～７のチャプターに分けられており、１つのチャプターは１分程度のものから長いもので８分程度である。番組の概要を静止画や文章で確認できる「文字と画像で見る」というコンテンツが用意されており、授業計画を立てる際に参考にしている。また、番組の要点がコンパクトに整理されている「学習メモ」や、各回の内容理解をチェックする選択式の問題である「理解度チェック」なども用意されており、必要に応じて利用できる。

実際の授業では、個々の生徒のパソコンに映像を送り、個別に視聴する形態をとっている。授業では導入段階で利用することが多い。例えば、「情報のディジタル化」の授業で２進法や 16 進法を学習するときには、第４回放送の「情報のディジタル表現」の「２進法と 16 進法」（３分４秒）と「ビットとバイト」（１分 34 秒）のチャプターを視聴した後、教科書の内容を説明した。場合によっては、最後にまとめとしてもう一度視聴して理解を深めている。

第４回「情報のディジタル表現」		
1	今日のテーマ「情報のディジタル表現」	2’ 12”
2	音声のディジタル表現	8’ 37”
3	２進法と 16 進法	3’ 04”
4	ビットとバイト	1’ 34”
5	文字のディジタル表現	2’ 46”
6	エンディング	0’ 44”
7	今日のまとめ　３つのポイント	0’ 59”

また、「情報通信ネットワークの構成」の授業では、第８回放送の「インターネットって何？」の１～４のチャプターを２つに分けて視聴した。パケット通信の実演などもあり、生徒の興味・関心を引く分かりやすいものであった。

第８回「インターネットって何？」		
1	IP アドレスとドメイン名	6’ 06”
2	ドメイン名の管理	5’ 30”
3	プロトコルとパケット通信	3’ 29”
4	回線交換とパケット交換	2’ 38”
5	トレースルート	1’ 15”
6	今日のまとめ　３つのポイント	1’ 00”

このように映像を視聴することで、授業で扱う内容の大まかな部分が理解できる場合も多く、単調になりがちな教科書の説明においても効果的である。ややくだけた内容の部分もあり、本校の生徒には適している。10 月に実施した「高校講座に関するアンケート」では、90％以上の生徒が「内容は分かりやすい」、「教科書の理解の助けに

なっている」と答えていた。ただ、授業以外で番組を視聴したことのある生徒は数名であった。授業で「高校講座」を視聴することについて、次のような意見や感想があった。

・番組を見るほうが、授業だけで学ぶよりも記憶に残って分かりやすかった。
・教科書では分からなかったところでも、番組を見て分かることが多いので、続けていってほしい。
・番組の雰囲気が楽しく、内容の難しいところなどが身近なものに例えられていて分かりやすかった。
・実演しながら説明してくれるので非常に分かりやすい。見ていて楽しい。
・あまり興味のなかった分野だったけど、もっと知りたいと思えるようになって、興味を持つことができた。
・２進法や 16 進法などの解説が分かりやすかった。
・私は情報が少し苦手ですが、少し好きになった。
・今まで情報の番組は見たことがなかった。高校講座を見て、理解する前に次に進んでしまうところがあったので、もう少しゆっくり説明してほしかった。でも、詳しかったので勉強になった。
・ときどきわからない語句が出てくるので、もう少し分かりやすくしてほしい。
・内容自体は良いと思うけど、画質が悪いので見づらい。

(2) 実習内容

ア　１学期「ワードを用いた文書作成」

４、５月は毎時間の初め 10 分間ほど、「Ｐ検（ＩＣＴプロフィシエンシー協会)」のインターネット版「ホームポジション」や「日本語入力」のソフトを利用して、タイピング練習を行った。その後、ビジネス文書実務検定２・３級問題集などの商業科の教材を利用して、文書入力の練習を行った。５月末には 10 分間の文書入力の実技テストを行った。６、７月は主に表の作成練習を行い、１学期末には簡単な時間割表を作成し、実技テストを実施した。

イ　２学期「エクセルを用いた表計算」

SUM、AVERAGE、MAX、MIN、IF、COUNTA、COUNTIF、INT、ROUND、RANK、VLOOKUP などの関数を用いた計算やデータの並べ替え、グラフ作成などを行い、10 月末には実技テストを実施した。２学期末には簡単な成績一覧表から個人票を表示させるところまで行った。

ウ　３学期「パワーポイントを用いたプレゼンテーション」

テーマは自由とし、６枚のスライドを作成した。作成時間は３～４時間である。自分の趣味や部活動紹介をテーマに選んだものが多かったが、中には地球温暖化などの環境問題を取り上げたものもあった。最後に、全員が持ち時間３分で発表し、10 項目について３段階で相互評価を行った。

(3) 数学との関連

ア　位取り記数法

新教育課程では、数学Aに「整数の性質」という分野が加わり、その中で「位取り記数法」について学習するようになった。「情報の科学」の「情報のディジタル化」の単元でも２進法や16進法について学習するが、先ず数学Aの教科書を用いて「位取り記数法」の部分を学習するようにした。位取りの基礎となる数（底）の変換に加えて、２進数の足し算・掛け算まで扱った。「ｎ進法」についてきちんとした形で学習しておいた方が、その後の定着も良い。なお、「新編 数学A」（数研出版）の教科書には、「ｎ進数の足し算・引き算」が課題学習として取り上げられている。

イ　データの分析

新教育課程では、数学Ⅰに「データの分析」という分野が加わり、各種データの統計処理について学習するようになった。その最後に、「表計算ソフトによるデータの分析」を行う部分がある。「情報の科学」の「情報の分析」の単元でも各種の統計処理を扱う部分がある。両者の共通内容としてエクセルを利用して、分散、標準偏差、相関係数などを計算式入力と関数入力の２通りの方法で求め、表計算ソフトの有用性を理解させた。また、散布図を作り、相関係数との関係を確認した。

ウ　暗号について

数学Aの「整数の性質」では、約数と倍数、素因数分解、ユークリッドの互除法、ｎ進法などを学習する。「新編 数学A」（数研出版）の教科書の中に、「整数の性質を利用した暗号」というコラムがあり、「電子メールなどの通信において、情報を守るため暗号が利用されている。ある暗号の理論に、素数の性質や、ユークリッドの互除法が利用されている。そのようなものの１つに公開鍵暗号方式がある。・・・」という内容であった。同じ頃、情報の授業で「セキュリティの重要性」を学習していたとき、ＳＳＬやＴＬＳ、ディジタル署名などの言葉が出てきたが、自分自身がよく理解できなかったので少し調べてみた。そして、ＲＳＡ暗号については、数学Aの知識とエクセルの表計算を用いれば高校生でも理解できると思い、教材化を試みた。なお、「ＲＳＡ暗号は、“桁数が大きい正の整数の素因数分解は困難である。すべての正の整数は、その数をべき乗したものを素数の積で割った時、余りがその数と等しくなるようなべき乗数が必ず存在する”という数学的な性質を利用している」（「最新 情報の科学」実教出版）。

＜ＲＳＡ暗号の鍵の作り方＞

① 異なる２つの素数ｐ、ｑを選ぶ。　（例 ｐ＝11、ｑ＝13）

② ｎ＝ｐｑ を計算する。　（例 ｎ＝11×13＝143）

③ φ＝（ｐ－１）（ｑ－１）を計算する。　（例 φ＝(11－1)(13－1)＝10×12＝120）

④ φと互いに素である整数ｅを選ぶ。　（例 ｅ＝7）

（ｎとｅが公開鍵である）

⑤ ｅｄ≡１（modϕ） すなわち、ｅｄ＝ｋϕ＋１ となる整数ｄを求める。

（ｄが秘密鍵である） （例 ｄ＝103）

＜ＲＳＡ暗号の暗号化・復号化＞

平文をｍ、暗号文をｃとすると

⑥ 公開鍵 ｎ、ｅ を用いて暗号化 $c \equiv m^e \pmod{n}$

（例 平文を ｍ＝2014 とする。2 桁ずつに区切って、

$20^7 \equiv 136$、$14^7 \equiv 53 \pmod{143}$ から暗号文 ｃ＝136053 を得る。）

⑦ 秘密鍵 ｄ を用いて復号化 $m' \equiv c^d \pmod{n}$

（例 ｃを 3 桁ずつに区切って、

$136^{103} \equiv 20$、$53^{103} \equiv 14 \pmod{143}$ から復号文 m’＝2014 を得る。）

∵ $m' \equiv c^d = m^{ed} = m^{k\phi+1} = (m^{\phi})^k \cdot m \equiv m \pmod{n}$

※⑥、⑦において、エクセルで mod 計算のシートを作成しておけば合同式の値が求めやすい。なお、合同式については、数学Ａ「整数の性質」（「新編 数学Ａ」数研出版）で発展事項として扱われている。

6 おわりに

とても研究発表といえるものではなく、情報の授業に携わって約１年半でやってきたことをまとめてみただけである。教科書の内容についてもまだまだ分からないことも多く、その日暮らしの授業が続いているが、少しずつ改善していきたいと思う。

１学期末に実施した生徒による授業評価を見ると、昨年より概ね評価も上向いてきている。自己研鑽を積みながら、授業力向上に努めたい。

＜参考文献＞

「暗号がわかる本」（オーム社）

「最新 情報の科学」（実教出版）

「新編 数学Ａ」（数研出版）