■卒業製作
「破壊されたプログラムの発見(診断)」を指導して

ポリテクカレッジ茨城　情報技術科　福良　博史
（茨城職業能力開発短期大学校）

1．はじめに

当校は，産業界の高度なニーズに応えるために，実験・実習に重点を置き，高度の技能・知識を有機的に身につけたテクニシャン・エンジニアの養成を行うこと，および在職労働者等に対する高度の技能・知識を身につけるための職業訓練の実施，その他必要な各種援助を行うことを目的に平成５年４月に設立された。

高度職業訓練の専門課程（高等学校卒業者等を対象とした２年制の教育訓練）は，生産技術科，制御技術科，電子技術科，情報技術科，原子力科（各科定員20名）の５科から成り立っている。

今回は，情報技術科での卒業製作・研究（以下「卒研」という）の事例について述べる。

2．情報技術科の特徴

当校の情報技術科では，急速に発展する情報化社会におけるソフトウェア製品の設計・製造技術に関する技術・技能を教育訓練することにより，実践技術者の育成を行っている。

3．卒研への取り組み

情報技術科の卒研は，２年生の前期のゼミナールと，後期の卒業研究の２科目を合わせ，１年間通して卒研に取り組んでいる。前期のゼミナールでは，大きな方向づけを見定め，場合によっては小さな試作を行う。後期の卒研では，具体的な製作に入り，モノを作り上げる。

3.1　学生とテーマと指導担当教官の決め方

卒研は，学生の自主性を重んじ，まず自分が何をしたいのかを１年の終わりに各学生から第一希望，第二希望を提出してもらう。そのテーマについて，指導教官が受け入れ可能であれば，学生が選んだテーマにそのまま取り組むことになる。うまくテーマと指導教官がかみ合わない場合は，学生のテーマを軌道修正してもらうことになる。数回このようなやり取りを行うことにより，徐々に学生の希望テーマが収束していく。なお，似たようなテーマで，一人の教官のところに学生が集中する場合は，個別に学生と話し合い，何人かの学生には第二希望などのテーマを卒研として取り組むように指導していくことになる。

原則として学生が各人別々に独立して自分のテーマをこなしていくのが通常であるが，テーマによっては複数の学生が分担して，１つのテーマに取り組む場合もある。

ここに紹介する事例は，最初は，共同作業を行うことを考えていなかったのであるが，ゼミナールの最後に絞り込んだ製作テーマの規模が大きくなり，卒研の製作は４人の学生による共同製作となった。

3.2　前期「ゼミナール」での指導

ゼミナールは，自分の卒研テーマのイメージ（こ

んなモノを作ってみたい）周辺について情報収集する。この場合学生が自分自身でモノを作るにあたって，自分の実力と作業環境で，希望どおりのものが本当にできあがるかの実現性（つまり一種のフィージビリティ・スタディ）を検討し，指導担当教官と相談しながら具体的なテーマに絞り込んでいく。

絞り込むにあたっては，学生自身の能力として背伸びしすぎていないもの，実習室等施設内部の機器等で実現可能なもの，学生が納得してやる気が出せるものなどを考慮することになる。

今回のゼミナールでは，４人の学生が，近年コンピュータウイルスの話題が盛んになってきており，ウイルスの研究をしたいと考えていた。そして，モノづくりのテーマとしては，最初は漠然とコンピュータウイルスのワクチンソフトの開発をしたいという希望を持っていた。

このため，４人のイメージ合わせをするために，共通の基本的な情報を身につけるように指導する必要があると考えた。そこで，通産省の外郭団体である情報処理振興事業協会（略：IPA）が国としてのコンピュータ・セキュリティ関連の指導的役割を担っているので，IPAが公表しているシステム監査関連の各種基準（例，コンピュータウイルス対策基準等）に目を通し，コンピュータのユーザとして考えておかなければならないことにどのようなものがあるのかを学習した。なお，IPAからは，「コンピュータウイルス撃退・撲滅するために」というビデオがあるので，このビデオを通して各種ウイルスの実態を生々しく映像で確認することができた。

IPAの資料，ビデオなどから，全体のイメージを把握した後に，コンピュータウイルスには，どのようなものがあり，具体的にどのような仕組みになっているのかを各種文献にあたり調査・研究した。

最後に，「どのようなモノ」を卒研のテーマとするか，を考えてまとめることになる。夏期休暇の前には，まだ４人の学生は，ワクチンソフトの製作をしたいという考えがあったが，荷が重いと感じていた。

夏期休暇明けに学生たちとフリーディスカッションを行い，ソフトウェアのウイルスを撲滅するためのソフトウェアとは何か，ワクチンソフト以外にもあるのではないか，という方向で指導した。

そのディスカッションの結果，パソコンのハードディスクの中身が破壊されたか否かを調査するための支援ソフトというものが考えられないか，というアイデアに行き着いた。

この基本的な考えは，正しい環境の情報を保存しておき，何か異常が発生した場合は，その正しい環境の情報と比較し，相違点を検出し，診断情報を出力するというものである。この方法は，ウイルスに侵された場合以外にも，不正に悪意の第三者に破壊された場合の検出も行える。しかも，ワクチンソフトの場合は，基本的にウイルスごとにワクチンの開発を行う必要があるが，情報の比較となれば，新種のウイルスに対しても基本的には検出可能である。

このアイデアから出てきたテーマが標記の「破壊されたプログラムの発見（診断）」である。最初に考えていたワクチンの製造からすると二次的なテーマを発見したことになる。このテーマを卒研の製作テーマとした場合規模が大きく，結果として４人の共同製作となる。

3.3 「破壊されたプログラムの発見（診断）」の概要

ハードディスクに入っているプログラムやデータを破壊された場合，「サイズ」「日付」等が変化している。実行プログラム（拡張子がEXE，COM）の場合は，プログラム・ファイルの，特定のある約束で決められた箇所から実行プログラムが始まっている。通常のウイルスは，プログラムのこの箇所の命令を置きかえる（注：最近出現してきたマクロウイルスには，この考えは当てはまらない）。

このため，①はじめに，正しく動いている環境での，プログラムの「ファイル名」「サイズ」「日付」「命令部の開始箇所から一定の長さの情報」をすべて抽出しておく。そして，②異常が発生したときにその時点での上記情報を収集する。その後，③以前保存しておいた内容と今収集した情報とを突き合わせチェックし，「サイズ」「日付」「命令部」の変化，および「プログラム自身が消えていないか」，また

は「新しいプログラムが増えていないか」をチェックする。この考えは，通常の実行プログラムにウイルスが感染した場合には検出が可能である。また，悪意の第三者がデータを改ざんしたような場合も，ある程度チェックがかけられる。

以上の結果を以下のように，利点，弱点，実現可能性等を書き出し，納得し，後期の卒研に入ることになった。

① ウイルスの退治はできないが，どのソフトが怪しいのかを検出可能

② ワクチンソフトは，新種のウイルスには対応できない場合があるが，このソフトは新種のウイルスに対しても検出可能

③ ウイルス以外に悪意の第三者が改ざんした場合も検出できる（しかし，サイズが同じで日付時刻まで以前と同じ値にされてしまうと検出不可能）

④ 悪意の第三者がプログラムやデータを消去した場合は検出可能

⑤ 悪くないモノまで，捕捉する

⑥ 検出されたものについて，最終的には人間がプログラムやデータの内容を確認し，真偽をチェックしなければならない

⑦ ソフトの製作技術としては，日ごろの実習で経験ずみの技術の組み合わせで，基本的に可能である

◇

日ごろの実習のときに製作していたソフトで，どのようなことができるのか。不足している内容は何かのイメージを把握してもらうように説明指導することにより，学生たちがモノづくりへの自信を持て

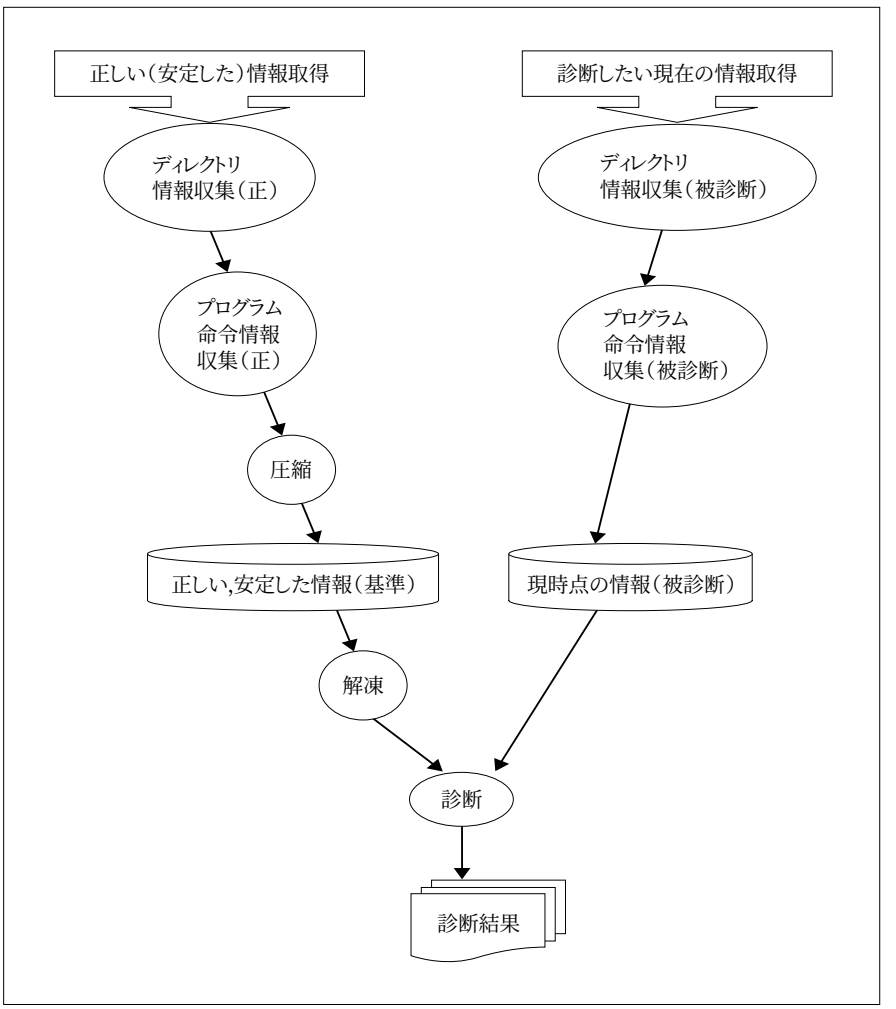

図１　製作したシステムの運用イメージ

るようになった。

3.4　後期「卒研」での指導

テーマが具体化した後は，学生が担当教官の指導のもとに製作活動に取り組むことになる。

今回のテーマの場合，全体のシステム構成は私がスケッチした。結果として製作するソフトは，

① 指定ディレクトリ情報をすべて収集するプログラム

② ①で収集した情報をもとに，識別子がEXEとCOMのファイル（実行プログラム）からは，実行開始位置からの命令部分の一定範囲を抽出するプログラム

③ 抽出結果を保存するために圧縮保存し，検査時点では解凍復元するプログラム

④ 以前に保存しておいた情報と，今回収集した情報の突き合わせ診断プログラム

以上の４本を作ることにした。プログラム言語はC言語を用いた（コンパイラはMicrosoft　Visual C++を使用）。

各々のプログラムは４人の学生が各自できそうなものを分担し，それぞれ製作に入った。

技術的に不明な点が発生するたびに個別に指導し説明した。しかし，技術的に皆が知っておいたほうがよいと判断した場合は，全員を集めて教室にて説明することもあった。

個別に製作し，個別のテストが完了した後すべてをつないで動かすと，お互いにインターフェースにズレが生じていて，学生同士でどちらをどう直したらよいか相談しながら結合作業を行った。このときどちらを修正したらいいか，またはどうしたらいいのか見当がつかなくなったときなどは，どうするのが良いかの判断の仕方を指導した。

今回製作した「診断プログラム」は，DOS環境で動かす。フロッピーにDOSと診断プログラムを入れておいて使用するという構成になっている。なぜなら，ウイルスに感染したシステムから隔離した状態で使用できなければならないため，このような構成とした。

3.5　ポリテックビジョンへの展示と学内での発表

今回の結果はポリテックビジョンにて展示を行った。

また，学内では，成果の発表と質疑応答を行う。発表前に，発表用資料の作成，発表練習，成果物を発表会場（実習用教室）に設置し稼動試験を行う。１年生も参加し，次年度の自分のテーマ探し，発表方法等の参考とする。

４．ま　と　め

今回の卒研は，１テーマ４人の共同作業となった。これが実際の製作現場の疑似体験をしたことになった。

① お互いのコミュニケーションの大切さを理解

インターフェースを変更したときには，必ず関係する人に伝えておくこと。知らされていないと相手は，以前のままのプログラムでよいと判断する。

② 本番環境とテストとの違いを理解

テストデータでのテストと，実際のハードディスクまるまる１個から情報収集したときに発生した各種トラブルと，その解決をとおして，テストデータの作成に対して思考しなければならないことの奥の深さを知る。

などを身をもって体験してくれたことは，卒業後の社会生活に役立ってくれることと思う。

〈参考文献〉

1） コンピュータウイルス対策基準，IPA.
2） コンピュータ不正アクセス対策基準，IPA.
3） コンピュータウイルス撃退・撲滅するために，IPA，セキュリティセンター，1997製作ビデオ.
4） 棟上昭男：ウイルス退治，共立出版.
5） 渡部章：コンピュータウイルス事典，オーム社.
6） MS-DOSエンサイクロペディア，Vol.1，システム解説編，アスキー出版局.
7） 出海勝富：86アセンブラ入門，工学社.
8） 奥村晴彦：Ｃ言語による最新アルゴリズム事典，技術評論社.