

On the Security of Computers in the CALL System : With Refernce to Kyushu University (In Honour of Professor Keiichi Onizuka On the Occasion of His Retirement)

Suzuki Yubun
九州大学言語文化部

<https://doi.org/10.15017/1354656>

出版情報 : 英語英文学論叢. 48, pp.1-16, 1998-02. 九州大学英語英文学研究会
バージョン :
権利関係 :

CALL 教室におけるコンピュータの セキュリティについて¹⁾

— 九州大学を例に —

鈴木 右 文

1 はじめに

かつて大学における外国語教育の中に聴解能力の向上を目指して LL 教室が導入されたように、昨今では効果的な学習と情報化の推進を旗印に CALL 教室 (CALL = Computer-Assisted Language Learning) の設置が全国の大学で始まっている。何分新しい展開であるから、CALL 教室を利用した授業の内容や教材からその管理運営方法に至るまで定番と言えるようなものは見当たらず、CALL 教室を導入した大学ではどこでも試行錯誤を繰り返しているものと思われる。また少なくとも九州大学では外国語の教員自らが管理運営にあたらなければならないので、非専門家なりにコンピュータと格闘して工夫していかなければならず、一層暗中模索の感がある。

本稿は、97年度4月からCALL教室の供用が開始された九州大学における前期6カ月間に渡る管理運営の研究の成果の一部であり、学生用コンピュータの管理強化の必要性を明確にし、その方法の実例を提示して、今後各地で更に普及していくであろうCALL教室の効果的な管理運営に資することを目的としている。²⁾

- 1) CALL 教室の管理運営にあたり、同僚の田畑義之助教授に並々ならぬ御尽力をいただいた。記して謝意を表す。また、筆者と田畑助教授は、97年度の九州大学言語文化 LL 委員会委員としてCALL教室の管理運営を分掌する立場にあったことを申し添える。なお、筆者のメールアドレスは yubun@rc.kyushu-u.ac.jp、ホームページの URL は <http://www.rc.kyushu-u.ac.jp/~yubun/> である。
- 2) CALL 教室で実施される授業の内容の検証なども含めたもう少し広く概論的な論考として、拙稿「CALL システムによる外国語教育とその諸問題 — 新規導入した九州大学の場合 —」『言語文化論究』第9号 (九州大学言語文化部, 1998年2月刊行予定) も参照されたい。

2 九州大学の CALL 教室の概要

九州大学の全学共通教育科目の多くが実施されている六本松キャンパスには従来から3つのLL教室があった。1997年4月にそのうちの1つが、CALLシステムと従来のLL教室の機能を合体させたCALL教室に更新された。

このCALL教室にはコンピュータ及びその関連機器だけが設置されているわけではなく、従来どおりのLL教室としての機能単独でも使用可能な設計となっている。LLシステムはソニー製 LLC-9000で、2名用の学生卓が32台、学生定員は64名となっている。1卓につき2台のLL用ブースレコーダ、2台のコンピュータ、2台のコンピュータ用モニターがあり、卓中央には1台の参照用モニター（学生2名で共用する）が設置されている。³⁾ 学生はこの参照用モニターと自分のコンピュータのモニターの2つの画面を見ながら授業を受けることになる。例えば、教員用のコンピュータの画面や特定の学生の画面をモデルとして学生卓中央の参照用モニターに提示し、学生にそれを見ながら自分のコンピュータを操作してもらうといった使い方がなされる。

学生用のコンピュータ本体は Apple の Power Macintosh 7200/120で、スクールトークの子機と共に学生卓のセンターコンソールの部分に収められている。キーボードは学生卓の内部にあり、卓上の一部がアクリル板になっている部分からのぞき込んでキーを操作する。⁴⁾

教員用コンピュータは Power Macintosh 7600/120で MO ドライブも追加してある。教員用と学生用のコンピュータはスクールトークによって接続され、ファイルの一括転送や出席の管理などができる。教員は学生のコンピュータの画面を手許に呼び出してアドバイスしたり、強制介入により遠隔操作したり、それをモデルとして学生卓上の参照用モニターに提示したりできる。各コンピュータは学内 LAN 経由でインターネットに接続されており、ネットワークサーバとしてソニー製 NEWS-5000X が設置されている。

OSは漢字トーク 7.5.3である。⁵⁾ ブラウザには「Netscape Navigator 3.01

- 3) このほか使用可能な LL 機材は、可変速（音質は変わる）のカセットデッキ1台、S-VHS方式のビデオデッキ1台、全世界対応ビデオ1台（後期から）、マルチディスクプレーヤ1台、教材提示装置1台、ミニディスクレコーダ1台、キャプション1台である。
- 4) このような設計にするとノートを取りながらキーボードを操作できるので便利であるが、主たる理由は広くない教室に64名（理系では定員で60名のクラスがある）の定員を確保するためである。

Gold)「Netscape Communicator 4」, エディタには「Jedit」「Simple Text」「SimpleTextKorean」をインストールしてある。入力メニューにはドイツ語、フランス語、スペイン語も追加した。更に、64台の学生用コンピュータのうち23台に「KoreanLanguageKit」をインストールし、朝鮮語環境にも配慮がなされている。この他、ファイル送受信や出席登録などのためのアプリケーションが「CALL SYSTEM」という名称のフォルダにまとめられている。

3 セキュリティ施策の重要性

公共の施設というものは、個人のものに比べて取り扱われ方が粗雑になりがちなものである。CALL 教室のコンピュータも次々と別の学生が使用する公共物であり、放っておけば個人用のコンピュータよりもトラブルが頻発することになる。

しかしながら九州大学に CALL 教室が設置されたとき、有償のソフトウェアを使用して強力なセキュリティ施策を図ることは検討されていなかったし、財政的にもその余裕があるとは言えなかった。外国語の教員にこのような教室での授業経験が欠如していたために、セキュリティに関して無策であることが極めて危険であるという認識がなかった。

当然の帰結として、1997年度前期の授業が始まって以来、様々の問題が生じている。学生用コンピュータのモニタが教員側から通常は見えないために、授業中に学生がコンピュータで遊んでいた、いたずらをしたりするケースが相次いだ。また、操作に不慣れな学生が誤った操作をしてしまうケースも目についた。

学生が遊ぶケースとしては、「アップルメニュー」の中の「ジグソーパズル」や「グラフ計算機」が挙げられる。この他、エディタを起動していたずら書きをしたり、アイコンを次々クリックしてハードディスク探検をしたりする。教員が学生用コンピュータをロックして使用できないようにすることはできるのだが、コンピュータを使用する課題を与えているときなどにはロックするわけにはいかない。

故意か誤操作かは別として、学生の操作が不都合を引き起こすケースで最も深刻なのは、必要なアプリケーションやファイルを「ゴミ箱」へ捨てて「ゴ

5) 後出のセキュリティソフトの FoolProof が漢字トーク 7.5.5までしか対応していないので、今のところ漢字トーク 7.6や MacOS 8へのバージョンアップはできない。

ミ箱」を空にしてしまうものだ。これはさすがに発生件数が極めて少ないが、発生した場合には授業に直接支障を来す。この他、以下のような様々のいたずらが発生した。

- 1) 必要なファイル等を「ゴミ箱」に捨て、「ゴミ箱」を空にはしない。次に使用する学生がゴミ捨てをするときに中身を確認しないと削除されてしまう可能性がある。
- 2) アイコンの上に別のアイコンをかぶせて見えなくしてしまう。次に使用する学生が目的のアイコンを発見できなくて困ることになる。
- 3) 「ゴミ箱」やハードディスクや「ツールバー」のアイコンをデスクトップの角に押し込んでほとんど見えない状態にする。次に使用する学生がなかなか戻せないで苦勞することになる。
- 4) アイコンのネームを全く別のものに変更したり、削除してしまったりする。こうなると目的のファイルを探すのに苦勞することになる。
- 5) 作成したファイルを勝手にハードディスクの中に残す。これはゴミ捨て操作に慣れていない学生がやむなく残してしまう場合もあるが、ゴミが溜まるとウィンドウが見にくくなるし、削除するメンテナンスの手間がかかる。
- 6) ファイル等を本来入っているべきフォルダ以外のフォルダへ移動してしまう。これも必要なときに迅速にファイルを探すことを妨げる。
- 7) 「デスクトップパターン」を変更してしまう。コンピュータを初めて扱う学生の中には、いつもと異なる画面を目にしただけでも教員に不具合ではないかと申し立てて授業が中断することもある。⁶⁾
- 8) 「スリープ」のタイマーをセットしてしまう。一定時間マウスやキーを操作しないとスリープし、「スリープ」を知らない学生がパニックを起こす。⁷⁾
- 9) 「ゴミ箱」を空にする際に警告のダイアログが出る設定をはずしてしまう。実際に、警告が出たとき念のために「ゴミ箱」を開いたらそれ以前に誰かが重要なファイルを捨ててあったことがあったので、この

6) デスクトップの様子は、「コントロールパネル」の中の「デスクトップパターン」パネルで設定する。

7) 「スリープ」のタイマー機能は、「コントロールパネル」の中の「省エネルギー設定」パネルで設定する。

ダイアログは出るように設定してある。⁸⁾

- 10) 「アップルメニュー」に入れるエイリアスを勝手に削除したり入れたりする。学生に「アップルメニュー」からのアプリケーションの起動を指示しても発見できないということがある。⁹⁾
- 11) 「複製」や「新規フォルダ」の実行によって、余計なアイコンでウィンドウを満たしてしまう。
- 12) ローマ字入力ができないようにしてしまう。50音で入力するのに慣れていない学生が困ることになる。¹⁰⁾

前期の初期だけでもこのような様々のトラブルが発生したので、授業の円滑な進行とコンピュータの保護のためには何らかのセキュリティ施策を施す必要があると考えられた。しかし前期の授業期間に多額の予算を執行するのは困難なので、前期の間はフリーウェアを中心とした工夫でしのいだ。しかしこの体制ではメンテナンスにかなり労力を必要とするので、今後もこの状態のままでは到底無理と判断し、予算を獲得して、後期からは有償のセキュリティソフトウェアをインストールすることにした。

セキュリティ対策は、授業での使用だけを考慮しても必須の条件と思われるが、CALL教室の利用を前提とした宿題を課したり、せっかくの施設を学生の自学に対しても利用させようということでCALL教室を開放しようとするばななおさら不可欠のものである。¹¹⁾ 授業よりもむしろ学生が一人で使用した方がCALL教室の効果的利用にあたるという考え方もあり、何としてもセキュリティ施策が必要である。

以下第4章は前期に施したセキュリティ施策を振り返り、第5章では後期に施したセキュリティ施策を振り返る。第4章の場合は財政的に苦しい場合の工夫の仕方としての意味、第5章の場合はCALLシステムとセキュリティ

-
- 8) 警告のダイアログが出るようにするかどうかの設定は、「ゴミ箱」を選択して、「ファイルメニュー」から「情報を見る」を実行し、所定のクリックボックスをチェックすることによって行う。
 - 9) 「システムフォルダ」の中の「アップルメニュー」の中にエイリアスを入れることによって、アプリケーションを「アップルメニュー」から起動できる。
 - 10) 日本語入力のローマ字と50音の切り替えは、「コントロールパネル」の中の「キーボード」パネルで行う。
 - 11) 現在のところCALL教室の自習開放は行われていない。諸々の問題点をクリアしてなるべく早い時期に開放ができるようにと考えている。

ソフトウェアとの相性の研究としての意味に小さからぬものがあるものと思われる。

4 フリーウェアを中心にしたセキュリティ施策

マッキントッシュには Apple 純正の AtEase (Workgroups) というセキュリティに使えるソフトウェアがあるのだが、Power Macintosh には付属していないので、採用するとすれば別途購入しなければならない。ところが年度の早い時期での多額の予算執行は困難なので、このソフトウェアにしる他のソフトウェアにしる、前期冒頭から採用するということはできなかった。¹²⁾

そこで我々は、費用をかけずに出来る範囲の小さな工夫の組み合わせで、不完全ながらもある程度の効果を持つセキュリティ施策を施すこととした。

4.1. マッキントッシュ側の対応策

最初に行ったのは、「アップルメニュー」の中から「コントロールパネル」のエイリアスを削除することだった。これにより、「アップルメニュー」から「コントロールパネル」を開き各種のパネルにアクセスして設定にいたずらを加えることは防ぐことが出来る。「アップルメニュー」から「コントロールパネル」を見ると、右側に様々のパネルのサブメニュー（「一般設定」「メモリ」「ランチャー」「デスクトップパターン」「モニタ」「カラー」「キーボード」「サウンド」「マウス」「表示」「TCP/IP」など）が表示されるので、学生はどうしても好奇心から中をのぞいてみたくなるものであり、この可能性を潰すだけでも幾分かはセキュリティの効果があろう。これで3章の12の問題のうち、(7)(8)(12)にある程度対応できることになる。但し、「アップルメニュー」から偶然に各種のパネルに興味を持つケースは防止できても、「システムフォルダ」を開き更に「コントロールパネル」を開けば各種のパネルのアイコンにたどり着いていたずらできるので、故意のパネル設定事項の変更を防ぐことができず、対策として万全とは到底言えない。

次に、「一般設定」による「システムフォルダ」と「アプリケーションフ

12) AtEase (Workgroups) は生産中止、後継ソフトウェアの予定なしとの回答を97年5月にアップルジャパンから得た。従ってそもそもこれを導入することができないことがわかった。当時生協連やパソコン店をかなりあたってみたが、64台分の在庫を持つところはなかった。

フォルダ」の保護が挙げられる。「コントロールパネル」の内部にある「一般設定」パネルを開くと設定画面が現れ、その左下に「システムフォルダの保護」「アプリケーションフォルダの保護」のチェックボックスが見える。デフォルトではこれらのボックスはチェックされていないが、チェックすることによって「システムフォルダ」と「アプリケーションフォルダ」の中にあるファイル等が外部へ移動できないようになる。外部へ移動できないのであるから、当然「ゴミ箱」に捨てることもできない。

これによって「システムフォルダ」「アプリケーションフォルダ」内の重要なファイル等を移動したりゴミ捨てしたりすることが、たとえ故意であっても不可能になる。また「システムフォルダ」と「アプリケーションフォルダ」からの取り出しは出来ないけれども、ファイル等をこれらのフォルダの内部へ移動することは出来るので、Netscape Navigator や SimpleText や CALL SYSTEM 関係のアプリケーション等のアプリケーション本体を「アプリケーションフォルダ」の中に入れた。これでこれらのアプリケーション本体をゴミ捨てすることが出来なくなる。こうして3章の(1)(6)について「システムフォルダ」と「アプリケーションフォルダ」に関係した部分につき幾分の解決をみた。

このように「システムフォルダ」と「アプリケーションフォルダ」の保護には誤操作による重要ファイル等の削除を防止する効果はあるのだが、故意のいたづらをブロックする上で、2つの大きな欠陥がある。

1つには、「システムフォルダ」と「アプリケーションフォルダ」の直接構成素を成すもの（すなわちどちらかのフォルダの中にあるが、これらのフォルダの中にある他のどんなものの中にもないもの）は確かに外部に移動できなくなるのだが、その移動できないものがフォルダである場合、そのフォルダの中にあるものは自由に「システムフォルダ」や「アプリケーションフォルダ」の外部へ移動出来る。従って、「システムフォルダ」や「アプリケーションフォルダ」の直接構成素であっても、一旦「システムフォルダ」や「アプリケーションフォルダ」の中の何らかのフォルダの中に入れば、次には一気にそのフォルダと「システムフォルダ」「アプリケーションフォルダ」を飛び越えて外部へ移動させることができるのである。「アプリケーションフォルダ」の中にアプリケーションのフォルダではなく本体をわざわざ入れたのは、フォルダごと入れた場合、本体が「アプリケーションフォルダ」の直接構成素とならず、「アプリケーションフォルダ」の外部へまともに移動

出来るからである。

もう一つの欠陥は、「一般設定」パネルを開けば、簡単に「システムフォルダ」と「アプリケーションフォルダ」の保護を解除できることである。これについては、次節の File Typer により若干改善出来る。

更に、「アップルメニュー」のサブメニューを無効にした。これにより、「アップルメニュー」の中の「最近使った書類」「最近使ったアプリケーション」「最近使ったサーバ」が使用できなくなる。¹³⁾ こうしなければ、教員用コンピュータと何らかのコンタクトを行った際に、「最近使ったサーバ」に「教員用 Mac」がサブメニューとして残り、学生が Fetch などを持ち込まなくても簡単に教員用コンピュータに接続できてしまう。サブメニューの無効化は、「コントロールパネル」の中の「アップルメニューオプション」パネルで「サブメニュー」を「切」にすればよい。この「アップルメニューオプション」パネルは「サブメニュー」を「入」に戻すことが出来ないようにゴミ捨てした。しかしながら「アップルメニューオプション」パネルを入手して復活させればサブメニューが再び使用できるようになるわけで、対策としては抜け道を残すものと言わざるを得ない。

4.2. フリーウェアによる対策

上記の「一般設定」パネルのように学生に開かせたくないものは不可視にするという手がある。削除してしまっただけではその機能が使えず、残しておいては開くことができるので、存在はするけれどもアイコンを見えなくする（これを「不可視にする」と言う）というのが良い方策と言える。しかも、アイコンを不可視にするソフトウェアは構造が簡単で、フリーウェアもしくはシェアウェアとして比較的容易に入手できる。

数多くあるそういったソフトウェアの中から偶然知るところとなった FileTyper というフリーウェアを我々は採用することとした。¹⁴⁾ このソフトウェアは選択したフォルダやファイルを不可視にしたり可視に戻したりする機能を中心にした軽量のアプリケーションで、操作も単純明快である。

13) 「最近使った書類」「最近使ったアプリケーション」「最近使ったサーバ」を「アップルメニュー」から削除しても同じことである。

14) 他のソフトウェアとの比較検分を十分行ったわけではないが、FileTyper で機能は十分と判断した。また、FileTyper を最初に紹介してくださったのは佐賀大学文化教育学部の中中彰一助教授である。紙面を借りて御礼申し上げる。

FileTyper によってまず「一般設定」パネルを不可視とした。これにより「システムフォルダ」と「アプリケーションフォルダ」の保護を解除することは難しくなる。また、「アプリケーションフォルダ」には重要アプリケーションの本体を入れてあるが、これらの本体が元々入っていたフォルダには重要な付属ファイルが入っており、これらのフォルダも不可視とした。

しかし、使用されているフリーウェアが File Typer であることさえつきとめれば学生でも簡単に可視に戻すことができる。有名なソフトウェアを幾つか試用してみればわかることである。ここまでしていただずらをしてという学生は滅多にいるものでないと思うが、対策ができればそれはそれで望ましいことであろう。しかしそもそも「システムフォルダ」と「アプリケーションフォルダ」の保護にはもう1つの問題（直接構成要素でなければ外部への移動が可能であること）があり、こちらの解決を図らないと「一般設定」パネルを可視に戻せない方策をいくら考えてもあまり意味はない。

以上のような工夫により、ある程度のセキュリティ効果は期待できるものと思われる。だが、このような施策を施してもなお、3章の問題のうち(2)(3)(4)(5)(9)(10)(11)には全く対応できておらず、いずれ更に上級の施策を要する一時しのぎに過ぎない。

5 有償ソフトウェアによるセキュリティ施策

前章の費用をかけない対策は、3章の問題の多くを解決できないばかりか、解決できるように思える問題についても結局のところ抜け道を残すものであり、全体としてはお粗末と言わざるを得ない。対策としてより万全に近く、そしてハードディスクの中身に関してほとんどメンテナンスフリーという状態にまで持っていけるような確実なセキュリティ施策を施すためには、やはり有償の強力なソフトウェアの導入が必要である。

5.1 FoolProofの導入

前章冒頭で述べたように、AtEase(Workgroups)は利用することができない。我々が結局導入を決めたのは FoolProof というソフトウェアである。¹⁵⁾ このソフトウェアは下記に挙げるような数々の制約をコンピュータに課し、

15) FoolProofは株クオリティの製品で、64台分では、学校向けパックの組み合わせで40万円強という価格設定である。

自らもパスワード防御されており、パスワードを知る以外に解除の方法はない。すべてのアイコンの移動を原則として禁じているので、この FoolProof 自体をゴミ捨てすることもできない。本体は「機能拡張フォルダ」に入っているが、「機能拡張マネージャ」は「コントロールパネル」に入っており、「コントロールパネル」は使用不可となるので、「機能拡張マネージャ」の設定を変更することで FoolProof をはずすこともできない。また、シフトキーを押しながら機能拡張をはずして再起動しても FoolProof の機能を止めることができないようになっている。¹⁶⁾

我々はまず、前章で示した施策のほとんどを一旦白紙に戻した。不可視にしたものは可視に戻し、「システムフォルダ」と「アプリケーションフォルダ」の保護を解除し、「アプリケーションフォルダ」の中からアプリケーションの本体をそれぞれが元々所属していたフォルダに戻した。更にハードディスクのウィンドウ内に置くフォルダやファイルの種類と位置を全コンピュータに共通となるように変更を加え、不要なファイル等を「ゴミ箱」に捨て、「アップルメニュー」の中にある不要なアプリケーションや「自動処理」をゴミ捨てした。

その上で FoolProof をインストールした。これの導入によって、下記のような望ましくない操作がフロッピーディスク以外の場所では禁止される。

- A) アイコンの移動
- B) アイコンのゴミ捨て
- C) アイコンのリネーム
- D) 新規フォルダの作成
- E) ファイルの保存
- F) 複製
- G) エイリアスの作成
- H) 「表示メニュー」の利用
- I) 「ラベルメニュー」の利用
- J) 「セレクト」の利用

16) 何もこれらの機能が FoolProof にしかない機能だと言っているわけではない。たまたま我々が FoolProof を採用しただけのことで、これが他の有償のセキュリティソフトウェアよりも優秀であると主張したり、FoolProof の利用を推奨したりする意図はない。

K) 「コントロールパネル」内のパネルの利用

(A) (B)によって3章の問題のうち(1) (2) (3) (6) (10)が解決され、(C)によって(4)が、(D) (F)によって(11)が、(E)によって(5)が、(G)によって(10)が、(K)によって(7) (8) (12)が解決をみる。こうなるとセキュリティ施策としては万全に近い。学生のハードディスクのウィンドウの中にあるものの種類と位置がそろえてあってどのコンピュータでも同一であり、また移動が不可能であるから、学生はどのコンピュータも全く同じ使い勝手で操作できるし、教員が学生に使用するアイコンを簡単な説明によって速やかに発見させることもできる。コンピュータリテラシーが皆無に近い学生も多くいるので、コンピュータの画面の均質性はぜひ確保したいところである。

(9)の解決のために、「情報を見る」も使用不能に設定したかったところであるが、そのようにしてしまうとアプリケーションへのメモリ割り当ての変更ができなくなるので、使用可能な状態のままにしておいた。学生用コンピュータはメモリが16MBしかないので、同時に複数のアプリケーションを使用させる場合に、メモリ割り当ての調整が望ましいケースも出てくる。

5.2. AppleScript の利用

FoolProofの導入はよいことづくめのように見えるが、これさえインストールしておけばよいというほど事態は単純なものではない。デフォルトではアプリケーションの使用によって生じた新規ファイルの保存先がフロッピーディスクだけに限られているので、フロッピーディスクの容量を越える大型のファイルを次の授業まで保存しておきたいときにこのままではその手だてがない。¹⁷⁾ そのままシステム終了してしまえば削除されてしまうが、FoolProofの機能を利用して保存先として使用できるフォルダを指定してそこに保存することもできる。そうすれば大きな容量のファイルも保存できるし、この指定されたフォルダと「ゴミ箱」の相互間ではアイコンの移動を許すことが出来るので、ゴミ捨てをすることもできる。そのようなフォルダを

17) 外付MOドライブを接続してこれに保存を許可するようにFoolProofを設定することはできるが、64台ものMOドライブを購入するとなれば相当な金額になる上、学生卓の鉄製のパネルをはがさないとコンピュータ本体裏のSCSIソケットに接続できない。はがしたままにしておく手も考えられるが、コンピュータ裏面をさらしてしまうのはかえってセキュリティ上問題がある。

指定するかどうかは状況によって判断されるべきものであろうが、我々は一切余計なものを残さないことに重点を置いて、このようなフォルダの指定はしなかった。不便であるという現場の声が強い場合、方針を変更することはあり得る。

また、ファイル送信でネットワークを通じて送り込まれるファイルについてはシステム終了しても削除されないし、ゴミ捨てもできない。¹⁸⁾ 受信したファイルがどんどんハードディスクの中に滞積していく。定期的に64台ものコンピュータの FoolProof を解除して、フォルダをすべて開いて余計なものが溜まっていないかどうかチェックしていくのは負担の大きな作業である。

そこで我々は、FoolProof の機能よりも「AppleScript」による命令の方が優先されることを利用して、受信されたファイルがシステム終了時に自動的にゴミ捨てされる特別のプログラムを組んだ。FoolProof はゴミ捨てを禁止するが、AppleScript による命令にゴミ捨てが含まれていれば FoolProof が稼働中であっても必ず実行される。「Apple エクストラ」フォルダの中に「AppleScript」フォルダがあるが、この中にある「スクリプト編集」アプリケーションを利用して、コンピュータの起動時に作動するアプリケーションとシステム終了時に作動するアプリケーションを作成し、それぞれ「システムフォルダ」の中の「起動項目」と「システム終了項目」に入れた。¹⁹⁾

コンピュータの起動時に働くアプリケーションは「CALL SYSTEM」フォルダの中の「ファイル受信」²⁰⁾ のコピーを作り、新規フォルダ（ネームは「名称未設定フォルダ」のまま）をハードディスクウィンドウ内に作り、「ファイル受信のコピー」をこの「名称未設定フォルダ」の中に移動させて自動

18) スクールトークの機種によっては（例えば広島大学）、受信したファイルはデスクトップに現れ、RAM ディスクに入れられてシステム終了と同時に自動的に削除される（以上は同僚の田畑助教授の指摘による）。ソニーの説明によると、九州大学のスクールトークではこのような機能は実現できないとのことである。

19) AppleScript は FoolProof にとって脅威になりうるので、学生用コンピュータからは削除してある。もっとも、学生が AppleScript によっていたずら用のアプリケーションを作成して持ち込んだとしても、FoolProof の機能により、これをフロッピーからハードディスクにコピーすることはできない。

20) これは㈱日本電子計算が作成して我々の CALL システムに導入されたアプリケーションで（正式名称「ファイル一括転送 Ver. 2.0」）、TCP/IP により、教室内に置かれたサーバとスクールトークの力を借りて教員用のコンピュータにあるファイルを学生用コンピュータに一括転送するものである。学生は「ファイル受信」を起動し、ファイルの受入れ先を指定して、送信許可のボタンをクリックする。

終了する。²¹⁾

ファイル受信を実行するときは学生に「CALL SYSTEM」フォルダの中の「ファイル受信」ではなく「名称未設定フォルダ」の中の「ファイル受信のコピー」の方を起動させる。すると受信したファイルはデフォルトで「ファイル受信のコピー」の入っているフォルダ、すなわち「名称未設定フォルダ」の中に受信される。

システム終了時に働くアプリケーションは、この「名称未設定フォルダ」を「ファイル受信のコピー」及び受信されたファイルもろともゴミ捨てして削除してくれる。

このような仕組みにより、受信したファイルは必ずシステム終了と同時に削除されて、ハードディスクに残留することはない。「ファイル受信」のコピーを作って、システム終了時には削除されてしまうフォルダの中へ入れ、これを起動してファイル受信を行うという手順がミソであり、「CALL SYSTEM」フォルダ内の「ファイル受信」そのものはシステム終了となっても残存し、受信したファイルは「ファイル受信のコピー」と共にシステム終了と同時に削除されることになる。

「ファイル受信のコピー」を作って「名称未設定フォルダ」に移動させなくても、「CALL SYSTEM」フォルダ内の「ファイル受信」をそのまま起動し、受信先を「名称未設定フォルダ」に指定すれば同じことであるように一見思えるのだが、「ファイル受信」は「CALL SYSTEM」フォルダの中であり、デフォルトでは受信先が「ファイル受信」を含むフォルダである「CALL SYSTEM」フォルダになるので、特に受信先を「名称未設定フォルダ」に指定する操作をしない限り、受信したファイルが「CALL SYSTEM」フォルダ内に堆積してしまうことになる。ところが、受信先をデフォルト以外の場所に指定する操作は慣れない学生にとって誤操作を招きやすいという報告が前期にファイル送受信を利用した教員から寄せられており、やはり「ファイル受信のコピー」を作成して「名称未設定フォルダ」に入れておく方が好ましいものと思われる。²²⁾ コピーの方を起動すれば受信先のデフォルト

21) 作成時に自動終了のチェックボックスをクリックしておかないと、いちいちダイアログが出て終了してよいかどうか聞いてくるので煩わしい。

22) 「ファイル受信」を「CALL SYSTEM」フォルダ内で起動させ、受信先のデフォルトを「名称未設定フォルダ」に指定することができればベストである。しかし株日本電子計算の担当者によると、受信先のデフォルトを特定の場所に設定し直すことはできない。

が「名称未設定フォルダ」となり、特段の受信先指定の操作を要しない。

但し、このようにしてもなお問題は完全に解決されたわけではない。まず第1に、教員の指示にもかかわらず学生が「名称未設定フォルダ」の中の「ファイル受信のコピー」ではなく「CALL SYSTEM」フォルダの中の「ファイル受信」を起動してしまうミスが考えられる。このようなミスが起これば、受信したファイルが「CALL SYSTEM」フォルダの中に溜まるのでシステム終了時に削除されないことになる。「CALL SYSTEM」フォルダを別のフォルダで包み込み、「CALL SYSTEM」の中の「ファイル受信」を起動する操作の手順が「名称未設定フォルダ」の中にある「ファイル受信のコピー」よりも多くて面倒になるようにするのも一つの手でないかとは思いますが、このミスを防ぐ有効な手だては今のところない。

また、マッキントッシュに頻発するフリーズ時に再起動すると、システム終了項目が実行されず起動項目だけが実行されることになる。この場合「名称未設定フォルダ」がゴミ捨てされないままに起動されるので、新規フォルダが作成されても名称が「名称未設定フォルダ2」となり、コピーされた「ファイル受信のコピー」は、再起動の前に作られた「ファイル受信のコピー」の中に含んでいる「名称未設定フォルダ」に移動されようとする。しかしここで「ファイル受信のコピーは既にあります」というダイアログが現れ、これに「OK」しても新しく出現したコピーは「CALL SYSTEM」フォルダ内に滞積し、「名称未設定フォルダ2」も削除されずに滞積することになる（ゴミ捨ての対象はあくまで「名称未設定フォルダ」であって「名称未設定フォルダ2」は対象外だから）。この場合の処置としては、フリーズ再起動したコンピュータの FoolProof を一旦解除した上でなるべく早く「ファイル受信のコピー」と「名称未設定フォルダ2」をゴミ捨てすることである。そうでないと起動時にダイアログが出続け、「OK」すれば先に進んでいつものようにコンピュータを使えることを知らない学生にいらぬパニックを引き起こすことになる。²³⁾

このトラブルはファイル受信の利用の有無にかかわらずフリーズ再起動した場合に必ず起きることである。しかし AppleScript を利用しない場合にもファイル受信実行ごとに受信されたファイルが溜まるわけで、64台のコンピ

23) また「ファイル受信」は他のアプリケーションと異なり、終了していない状態ではシステム終了が出来ない。学生に必ずシステム終了前に「ファイル受信」を終了させておくように徹底させなければならず、不便である。

ュータから受信したファイルをゴミ捨てる手間が要る。これらの2種類の手間のうち、どちらがより作業が軽くて済むかは、ファイル受信機能の利用頻度による。我々は、この機能は大いに利用すべきものと考え、AppleScriptを利用した施策を選択した。

6 終わりに

我々のスタッフには本当の意味でのCALLシステムによる外国語教育の専門家はいない。従って導入されたCALL教室を有効に活用していくためには、担当教員ひとりひとりがたとえゼロからであろうともこのシステムを研究していく必要がある。全国のそれぞれの部署の置かれている環境に合ったCALLシステムの応用のあり方が追究されていく上で、本稿が少しでも参考になれば幸いである。